제 출 문

한국인터넷진흥원 원장 귀하

본 보고서를 “2019 글로벌 정보보호 산업 시장동향 조사”의 최종연구결과보고서로 제출합니다.

2019년 12월 13일

수 탁 기 관 :넥스텔리전스(주)
연 구 책 임 자 :연구위원/이사 김동진(넥스텔리전스)
참 여 연 구 원 :수석연구원 조현도(넥스텔리전스)
책임연구원 노은아(넥스텔리전스)
책임연구원 노재욱(넥스텔리전스)
선임연구원 성미연(넥스텔리전스)
선임연구원 김수연(넥스텔리전스)
선임연구원 장운현(넥스텔리전스)
연 구 원 남정현(넥스텔리전스)
KISA참여연구원:팀 장 송혜인(해외사업팀)
책임연구원 이승재(해외사업팀)
선임연구원 박형준(해외사업팀)

1. 글로벌 정보보호 시장 개요

시장 동향 및 전망

▶ 글로벌 정보보안 시장은 규모 면에서 IAM이 시장을 이끌고, 성장률 면에서는 암호화 분야가 시장을 견인 중인 가운데, 2023년까지 연평균 10.2%로 성장할 전망

- 2018년 정보보안 시장에서 솔루션은 866억 5,000만 달러, 서비스는 660억 600만 달러를 각각 기록했으며, 2023년에는 솔루션이 1,357억 6,000만 달러, 서비스가 1,125억 달러를 차지
- IoT 보안 시장은 시장 규모 면에서는 네트워크 보안, 성장률 면에서는 클라우드 보안 분야가 시장을 견인 중이며 2023년까지 연평균 33.7%의 성장률을 기록하여 351억 2,200만 달러의 시장을 형성할 전망
- 2019년 시점 북미 시장이 전 세계의 40% 이상을 차지하여 글로벌 인공지능 보안 시장을 주도하고 있으며, 전 세계적으로 2026년까지 23.3%로 성장하며 382억 달러 이상의 규모에 이를 전망

표 _ 전 세계 정보보안 시장 규모 및 성장 전망 (단위 : 십억 달러)

구분	2016년	2017년	2018년(e)	2023년(p)	연평균 성장률('18-'23)
시장규모	122.93	137.63	152.71	248.26	10.2%
성장률	13.0%	12.0%	11.0%	9.9%	

주) e: estimated, p: projected [출처] MarketsandMarkets(2018.9)

▶ 글로벌 물리보안 시장은 2018년 841억 5,000만 달러로, 2023년까지 연평균 7.3%로 성장하며 1,194억 5,000만 달러에 이를 전망

- 전 세계적으로 테러 활동의 증가가 물리보안 시장 성장의 동인으로 작용하고 있으며, 최근에는 클라우드 기반 물리보안 서비스가 새로운 시장을 창출 중

그림 _ 전 세계 물리보안 시장 규모 및 성장 전망 (단위 : 십억 달러)



[출처] MarketsandMarkets(2019.1)

2. 선진국 시장

시장 동향 및 전망

▶ 정보보안 시장에서는 선진국 시장 중 미국이 75억 2,400만 달러로 압도적인 비중을 차지하고 있으며, 일본이 연평균 15.6%의 성장률을 보일 것으로 예상됨에 따라 해당 시장에 대한 주목이 필요

표 _ 선진시장 주요국 정보보안 시장규모

(단위: 십억 달러)

국가	2016	2017	2018e	2023p	연평균성장률 (2018-2023)
미국	44.33	48.5	52.55	75.24	7.40%
일본	3.9	4.62	5.39	11.12	15.60%
영국	10.39	11.23	12.02	16.17	6.10%

[출처] MarketsandMarkets, Physical Security Market-Global Forecast To 2023, 2019

▶ 한편, 물리보안 시장규모는 2018년 미국의 경우 260억 달러 규모로 연평균 성장률(2018-2023) 6.2%로 성장할 것으로 전망하며, 영국은 40억 달러 규모, 일본은 26억 8,000만 달러 규모

표 _ 선진시장 주요국 물리보안 시장규모

(단위: 십억 달러)

국가	2016	2017	2018e	2023p	연평균성장률 (2018-2023)
미국	22.40	24.32	26.06	35.23	6.2%
일본	1.96	2.30	2.68	4.46	10.8%
영국	3.50	3.74	4.00	5.24	5.6%

[출처] MarketsandMarkets, Physical Security Market-Global Forecast To 2023, 2019

미국

▶ **(환경)** ITU 2018 'Global Cybersecurity Index(GCI)'에 따르면 미국의 사이버보안 지수는 0.926으로 영국(0.931)에 이어 2위를 기록했으며, 미주 권역에서는 2017년에 이어 연속적으로 1위를 기록

▶ **(시장 현황)** 2017년 미국 보안시장은 317억 달러 규모로, 전 세계 시장의 약 18% 이상을 차지하며 꾸준히 증가할 것으로 예상

- Ernst & Young (2017-18)의 글로벌 설문 조사에 따르면, 기업의 87%가 사이버 보안 예산을 50%이상 증가할 계획을 가지고 있으며 향후 기업들은 지속적으로 사이버 보안에 많은 비용을 지출할 전망
- 미국 연방 사이버 보안 시장은 인프라 강화 부문이 12%의 꾸준한 CAGR로 성장하면서 200억 달러 규모에서 안정적으로 유지될 것으로 예상
- 미국 보안 서비스 시장은 2023년에 286억 달러에 이를 것이며, 예측 기간 동안 연평균 8.2% 성장할 것으로 전망

▶ **(사업자 및 경쟁현황)** 전 세계 정보보안 시장의 40%를 차지하는 최대 시장인 미국은 연방정부가 적극적으로 투자 수요를 형성

- 매출 상위 15개사가 전체 시장의 27%를 점유하는 데 그쳐 특정 기업이 경쟁적 우위를 가지지 않는 경쟁적 시장 구도를 나타내고 있으며, 약 1만 730개의 기업이 존재
- 최근 클라우드 기반의 보안 솔루션 도입이 증가하면서 해당 시장의 경쟁이 심화되고 있으며, Cisco, Symantec, Zscaler, Forcepoint 등이 주도
- 2018년 사이버보안 분야의 스타트업 기업에 대한 투자 건수는 617건으로 2015년 대비 40% 가량 증가

▶ **(주요 동향)**

- 2019.7월 NSA는 사이버 공간에서 러시아와 중국과 같은 외국의 위협에 대처하기 위한 새로운 조직인 사이버보안국(Cybersecurity Directorate)을 발표하고, NSA의 외국 정보분석과 사이버 방어 임무 통합 및 국가 안보 시스템과 방위 산업 기반에 대한 위협의 예방·근절을 목표로 설정
- 샌프란시스코시는 경찰 당국과 다른 시 당국이 주민들에게 얼굴 인식 기술을 사용하지 못하도록 하는 조례를 승인(2019.5)
- 각각 독립적으로 발표된 Bitglass의 2019년 클라우드 보고서 및 Synopsys의 2019년 클라우드 보안 보고서에 따르면, 대다수의 조직이 클라우드 보안 상태에 큰 우려를 표시

▶ **(융합산업)** 미국 국립표준기술연구소(NIST)는 IoT의 사이버보안 및 개인정보보호 관리와 관련된 과제와

해결방안을 제시한 보고서인 'NISTIR 8228'를 발간(2019.6)

- 미국 국립표준기술연구소(NIST) 산하 국가사이버보안역량센터(NCCoE)가 소기업・가정용 IoT 기기 보안 가이드(안)발표(2019.4)
- 미국 하원에 초당적 법안인 2019 IoT 사이버보안 개선법 발의(2019.3)

▶ **(진출전략)** 정부 및 민간 등 다양한 분야에서 레퍼런스 확보가 시급하므로 신규 서비스 분야 발굴 및 현지기업과의 M&A, 투자유치 등을 통한 연계 진출 필요

일본

▶ **(환경)** 2020년 도쿄 올림픽을 앞두고 감시 카메라, 영상 종합 관리 소프트웨어, 드론 등 각종 보안 장비에 대한 물리보안 수요 환경이 개선되고 있는 중이며, 잦은 지진을 비롯한 자연재해에 자주 노출되는 일본 정보보안 시장에서는 데이터 백업을 위한 클라우드 컴퓨팅에 대한 수요가 지속적으로 상승 중

▶ **(시장현황)** 2018년 일본 정보보안 업계에서는 전년도의 'WannaCry'와 같은 대규모 보안 피해 사례는 발생되지 않으며 2019년 이후에도 소비세 증세에 따른 경기 후퇴 리스크로 시장 성장에 제약이 있을 것으로 예상

- 시장조사기관 후지케이자이(富士経済)에 따르면, 2018년 일본의 물리보안 시장 규모는 2017년 대비 3.6% 성장한 9,658억 엔으로 추정했으며, 2021년에는 1조 엔을 넘어서는 시장을 형성할 것으로 전망
- 일본네트워크보안협회(JNSA)에 따르면 2019년 정보보안 시장은 전년 대비 4.5% 성장한 1조 1,771억 엔의 규모에 이를 전망

▶ **(사업자 및 경쟁현황)** 2020년 도쿄 올림픽 개최에 따른 물리보안 신규 수요가 늘어날 것으로 예상되나, 저가 해외 제품의 일본 시장 진출에 따라 시장 경쟁은 더욱 격화되고 있는 양상

- 물리보안 시장은 Hitachi, Mitsubishi, NEC, Photosynth 등이, 정보보안 시장은 Trend Micro, Fujitsu, Hitachi, Vinx 등이 주요 업체로 활동 중

▶ **(주요 동향)**

- 2020년 올림픽 특수는 예상에 미치지 못할 것으로 예측되는 가운데 AI, IoT 등 혁신 기술을 활용한 물리보안 솔루션 응용에 대한 기대감이 커지는 중
- 글로벌 규제 환경 변화와 개인정보보호 기준이 강화됨에 따라 EU GDPR, NIST SP800-17 등의 데이터 보호 관련 규정의 제품 및 서비스 반영 수요 확산

▶ **(융합산업)** 총무성은 IoT 보안 취약점 강화를 위한 ▲체제 정비 ▲연구개발 ▲인재육성 강화 등을 도모하는 'IoT 보안종합대책(IoTセキュリティ 総合対策)'을 2017년 발표하고 매년 업데이트

▶ **(진출전략)** 유통채널, SI업체 등에 납품을 통해 시장 진출 가능성 높으며, 개발 및 2차 서비스 부분에서 우리 기업의 진출 가능성이 높음

영국

▶ **(환경)** 2019년 3월 발표된 '2018년 ITU의 사이버보안지수(Global Cybersecurity Index, GCI 2018)' 자료에 의하면 영국은 전 세계 1위로 한국(15위)보다 앞선 것으로 나타났으며, 최근 들어 사이버 공간을

통한 각종 침투공격과 테러 예방을 위해 국가 정보보호정책을 계속 강화하고 있는 추세로 관련 기기 및 솔루션, 소프트웨어 등의 수요가 계속 증가해 나갈 것으로 전망

▶ **(시장현황)** 2018년 기준 영국 사이버 보안시장 매출액은 전년대비 12.8% 증가한 6억6,640만 파운드로 추정

- 시장조사기관 IBIS World의 사이버 보안 소프트웨어 분석 보고서에 따르면 2013년부터 2018년까지 지난 5년간 영국의 사이버 보안 시장 매출액은 연평균 9.5%씩 증가했고, 시장 매출액은 향후 5년간 연평균 7.7%씩 증가하여 2023년 매출액이 9억6,740만 파운드에 달할 것으로 전망

▶ **(사업자 및 경쟁현황)** 자국 내 정보보호 산업도 높은 수준이지만 수요의 상당 부분을 수입에 의존하고 있어 글로벌 정보보호 기업 간 경쟁 강도가 치열

- 정보보안 시장은 다국적 사이버 보안 컨설팅사, 전문 ICT 서비스 사업자, 다국적 HW/SW 벤더, VAR 등이 얽혀 단독 혹은 컨소시엄 형태로 입찰에 참여하면서 치열한 경쟁 구도를 형성
- 물리보안 시장은 미국, 일본 등 유명 브랜드 제품이 선호를 받는 추세로, 기존에 가격경쟁력으로 시장 점유율을 확장해 오던 중국·대만·말레이시아 등의 제품 증가율이 다소 주춤해지고 있으나 여전히 중국산 등 저가 보안제품의 수요가 시장의 중심세력 구축 중
- 영국 사이버보안 스타트업들이 두각을 나타내고 있으며, 사이버 보안 스타트업의 진출 분야 산업 전 분야에 고르게 퍼져있다는 점에서 사이버 보안 시장의 건전성을 확인 가능

▶ **(주요 동향)**

- 브렉시트의 불확실성으로 건설업 경기가 7년 만에 최저수준으로 도달했는데 이러한 건설 프로젝트 사이클이 보안시장에 일부 영향을 미침
- KOTRA 런던무역관에 따르면, 영국은 전역에 425만대의 CCTV가 설치돼 있어 신규 CCTV를 설치할 여력이 없다는 의견과 기존 영상보안장비 업그레이드 및 고성능 장비로 교체 수요가 늘어날 수 있다는 의견으로 전망이 엇갈리고 있다는 분석

▶ **(융합산업)** 2019년 5월 2일, 영국 정부는 인터넷에 연결된 모든 기기를 '설계 단계부터' 사이버 공격으로부터 안전하게 보호하기 위한 소비자 IoT 보안 관련 신규 법안을 발의

▶ **(진출전략)** 법, 제도, 기술 등 한국과 비슷한 수준으로 경쟁관계에 있으나, 유럽시장 진출을 위해서는 협력 및 신규 서비스 분야에 공동 R&D 등 필요

3. 아시아 시장

시장 동향 및 전망

▶ 아시아 지역의 정보보안 시장은 2018년 211억 8,000만 달러로 추산되며, 이후 연평균 14.86%씩 성장하여 2023년경에는 423억 5,000만 달러에 이를 전망

표 _ 아시아 지역 주요국 정보보안 시장규모

(단위: 십억 달러)

국가	2016	2017	2018e	2023p	연평균성장률 (2018-2023)
중국	5.68	6.51	7.37	12.83	11.70%
기타 아시아*	9.84	11.72	13.81	29.52	16.41%
합계	15.52	18.23	21.18	42.35	14.86%

* 그 외 아시아 지역은 중국과 일본을 제외한 지역으로 호주, 한국, 말레이시아, 싱가포르, 홍콩, 뉴질랜드, 인도, 대만이 포함됨

[출처] MarketsandMarkets, Physical Security Market-Global Forecast To 2023, 2019

▶ 물리보안 시장규모는 2018년 중국의 경우 97억 2천만 달러 규모로 연평균 성장률(2018-2023) 9.2%로 성장할 것으로 전망되어, 시장규모와 성장률 면에서 아시아 지역을 전체적으로 견인

표 _ 아시아 지역 주요국 물리보안 시장규모

(단위: 십억 달러)

국가	2016	2017	2018e	2023p	연평균성장률 (2018-2023)
중국	7.56	8.60	9.72	15.12	9.2%
기타 아시아	4.48	4.97	5.44	7.85	7.6%
합계	10.08	11.27	12.48	18.5	8.2%

[출처] MarketsandMarkets, Physical Security Market-Global Forecast To 2023, 2019

중국

▶ **(환경)** 공업정보화부가 올해 6월 4대 이동통신사에 5G 영업허가증을 발급하는 등, 2020년 이후 5G 서비스가 상용화로 사물인터넷 시대가 본격적으로 열리면서 보안의 중요성이 높아짐에 따라 정보보호 시장의 성장세가 더욱 높아질 전망

▶ **(시장현황)** 중국정보통신연구원(CAICT)의 '2019년 중국 사이버보안 백서'에 따르면 중국 사이버보안 산업규모는 2018년 510억 9,200만 위안으로 전년 대비 19.2% 성장했으며, '19년에는 631억 2,900만 위안 규모를 형성할 전망

- IDC에 따르면 금년부터 2022년까지 중국 IT 보안 지출규모의 연평균 증가율은 25.6%에 달해 전 세계 평균을 크게 웃돌 전망
- 2019년 중국의 IT 보안 지출액은 약 73억 5,000만 달러로 예상되며, 2022년에는 중국 보안 솔루션 시장이 137억 7,000만 달러로 성장할 것으로 예상
- 중국안전방범제품산업협회에 따르면 2019년 중국의 물리보안 산업 매출규모는 7,412억 위안에 달할

전망

▶ **(사업자 및 경쟁현황)** 보안 SI 시장에서는 다수의 업체들이 치열한 경쟁 국면을 형성하고 있으며, 지역적으로나 산업적으로 파편화된 구조로 시장 집중도는 낮지만, 점차 핵심 기술력과 브랜드 인지도를 보유한 대형 기업들을 중심으로 재편될 전망

- 중국 영상감시설비 시장은 Hikvision, Dahua를 비롯한 상위 5개 업체의 시장 점유율이 50% 이상으로 시장 집중도가 매우 높은 편이나, 최근 샤오미, 360, 바이두 등 IT와 인터넷 기업들이 보안업체와 제휴해 인터넷 플랫폼을 통해 시장 진입이 활발해지면서 시장 경쟁이 격화
- 중국정보통신연구원에 따르면 2019년 7월 중국 정부가 상하이 증시에 기술주 전용 상장시장 커촹반(科创板 : Technology Board)을 개장하면서, 정보보호 스타트업들의 상장이 활성화될 전망

▶ **(주요 동향)**

- 국가인터넷정보판공실, 네트워크 안전심사방법 초안 발표(2019.05)
- 국가발전개혁위원회, 국가기술 안전관리목록 제도 제정 계획(2019.06)
- ZTE, 브뤼셀에 사이버 보안 연구소 설립(2019.7)
- Huawei, 향후 5년간 사이버보안에 20억 달러 투자 계획(2018.12)

▶ **(융합산업)** 중국 공업정보화부와 교육부, 인력자원사회보장부, 생태환경부, 응급관리부, 국가시장감독관리총국 등 10개 부서는 2019년 8월 '산업인터넷 보안업무 강화에 관한 지도의견'을 정식 발표하고 2020년 말까지 산업인터넷 보안을 위한 기본적인 체계를 구축할 계획

- 중국 중상산업연구원에 따르면 2018년 중국의 클라우드 보안 시장규모는 약 37억 7,600만 위안으로 전년 대비 45% 성장했으며, 2019년에는 50% 성장한 56억 1,000만 위안 규모를 형성할 전망
- 2018년 중국의 사물인터넷 보안 시장 규모는 전년 대비 35% 증가한 87억 위안을 기록했으며, 2019년에는 130억 위안, 2021년에는 50% 이상 증가한 300억 위안을 기록할 전망

▶ **(진출전략)** 중앙정부 및 지방정부의 다양한 수요를 대상으로 개별 수주는 가능 할 수 있으나, 자국제품 및 서비스 의무 조항, 판매허가 획득 어려움 등으로 현지 진출 시 중국법인과의 협력을 통한 진출이 필요하며, 환경이 매우 제한적일 수 있음

인도

▶ **(환경)** 모디 총리 집권 이후, 인도 정부의 IT 산업 육성 정책과 민간 기업의 투자가 맞물리며 인프라 구축을 넘어 5G, IoT 등 IT 산업이 급성장하였으나 이와 더불어 사이버보안 위협도 증가

▶ **(시장현황)** 인도 사이버보안 시장 규모는 2017년 492억 달러→ 2018년 552억(추산) 달러 → 2019년 598억 달러(추산)으로 성장 추세

- 2018년 사이버보안 시장을 제품별로 세분화하면, ▲네트워크 보안(48%) ▲신원 접속 관리(17.7%) ▲엔드포인트 보안(11.6%) ▲데이터 보안(5.5%) ▲기타(17.1%)로 구성
- 인도는 세계 최대 생체시장 중 하나로, 특히 지문과 홍채 중심의 생체인식 시장이 형성되어 있으며, 2018년 7억 달러에 달했던 인도 안면 인식・인증 소프트웨어 시장이 2024년까지 매년 35.9% 성장할 전망

▶ **(사업자 및 경쟁현황)** 인도의 정보보호 산업 시장은 다국적 기업의 영향력이 두드러지는 상황

- 인도의 보안 제품 소프트웨어 매출 기준 상위 10개 기업은 Symantec, IBM, McAfee, Check Point, Dell

Inc, F-Secure, Trend Micro, Kaspersky Lab, Hewlett Packard Enterprise, Forcepoint

- Honeywell과 Bosch Security India 등 글로벌 기업들은 가격경쟁력 확보를 위해 현지 업체를 통한 OEM 방식으로 물리 보안장비를 판매

▶ **(주요 동향)**

- 다국적 기업 Emerson이 인도 푸네(Pune)에 사이버보안 연구소를 개소('19.8)
- 프랑스 컨설팅 기업 Capgemini Research Institute에 따르면, 인도 기업들이 사이버공격 방어를 위해 인공지능 활용을 증대하는 추세
- ▲인도와 핀란드 간 사이버보안 분야 협력 양해각서 체결('19.1) ▲인도와 사우디아라비아의 사이버보안 협력 강화 합의('19.1) ▲인도-프랑스의 디지털 기술 및 사이버보안 로드맵 발표('19.8) 등 국제적인 안보협력 강화

▶ **(융합산업)** 인도 정부가 스마트시티 계획을 진행하면서 이와 관련해 대규모 IoT 시장이 창출되고 있으며, Nasscom에 따르면 2020년 인도의 IoT 시장이 글로벌 시장의 5%에 달하는 150억 달러에 이를 전망

- Barnes Report[1]에 따르면, 2019년 인도 자율주행 사이버보안 장비 시장 규모는 1억 8,570만 달러로 추정되며, 2025년까지 6억 2,409만 달러로 성장 전망
- 2019년 1월 인도 은행기술개발연구소(IDRBT)가 은행의 업무 효율화 및 사이버 위협 예방을 위한 블록체인 활용 로드맵을 제안

▶ **(진출전략)** 인도 정부조달시장을 통한 인도 보안시장 진출이 가능하며 이 경우 애프터서비스를 비롯해 정부가 요구하는 조건을 충족시키기 위해 인도에 사무실을 설립하는 것이 필요

인도네시아

▶ **(환경)** Digital 2019 Reports에 따르면, 인도네시아는 인터넷 사용 인구 증가에 있어서 인도·중국·미국에 이어 세계 4위이며 그만큼 관련 위협도 상당한 것으로 분석

- 2018년 한 해 동안 인도네시아에서 감지된 사이버 공격은 2억여 건으로 빈약한 사이버 시스템으로 인해 사이버 공격에 대한 노출 빈도가 증가

▶ **(시장현황)** BMI에 따르면 2018년 인도네시아의 ICT 지출은 총 117억 달러로, 부문별로는 ▲소프트웨어는 2018년 15억 달러(2022년 29억 달러) ▲IT 서비스는 68억 달러(2022년 118억 달러) ▲컴퓨터 하드웨어는 33억 달러(2022년 40억 달러)로 증가세를 이어갈 전망

- IDC는 2019년 인도네시아의 ICT 지출 규모를 332억 달러로 추산했으며, 2022년에는 인도네시아 보안 경보 장비의 10%가 인공지능에 의해 구동될 것으로 전망
- Barnes Reports에 따르면, 2018년 인도네시아의 보안 시스템 서비스 시장은 약 13억1,600만 달러 규모

▶ **(사업자 및 경쟁현황)** 인도네시아의 IT 및 정보보안 시장은 글로벌 기업이 주를 이루고 있는데, 이들은 주로 정부 및 금융기관 등 높은 수준의 정보보안을 요하는 기관을 중점 공략

- IT 솔루션 및 네트워크 분야에 진출한 기업은 EMC, HP, Cisco, VMware, Redhat, Radware, Sophos, 등이며 정보보안 분야 진출 기업은 Check Point, Trend Micro, Fortinet, McAfee 등
- 인도네시아 현지 보안서비스 제공업체 및 이동통신 사업자들은 SOCs 구축 경험 및 운용 역량을 갖춘

1 Barnes & Co., 2019 Global High Tech & Emerging Markets, 2019.5.26

글로벌 업체와의 파트너십을 통해 사이버보안 솔루션을 제공하는 추세

▶ **(주요 동향)**

- 인도네시아 보안업체 PT Professtama, 호주 Red Piranha와 파트너십 체결(2019.3)
- Facebook, Agence France-Presse(AFP)와 팩트 체크 파트너십 체결(2019.4)
- 자카르타 교통경찰국, AI 카메라를 도입해 전자교통단속시스템(ETLE)을 더욱 강화(2019.7)
- 인도네시아 수도 이전에 따른 인프라 개발과 관련해 ATISI는 4대 보안안전 기술, 즉 ▲도청 및 도난 방지 기술 ▲계층화된 보안 시스템 ▲CCTV 수량 및 품질(100㎢당 CCTV 100대 설치, 온도 센서 및 야간투시 기능 탑재) ▲안면인식 및 인공지능 기술을 권장

▶ **(융합산업)** 인도네시아의 인지보안(cognitive security) 장비 시장은 2019년 2,690만 달러에서 2020년 3,590만 달러로 33.6% 성장할 것으로 예측

- 인도네시아의 자동차 사이버보안 장비 시장은 2019년 8,670만 달러에서 2020년 18.6% 성장해 1억 290만 달러에 이를 것으로 예측

▶ **(진출전략)** 정부발주, 금융.통신 분야 발주, 주요 총판을 타깃으로 집중적 진출추진을 통해 지속적으로 레퍼런스 확대가 필요, 글로벌 기업(일본)과 경쟁하는 상황으로 전략적 접근 필요

베트남

▶ **(환경)** Kaspersky Lab은 2018년 말 기준 1억 건 이상의 온라인 공격과 4억 건 이상의 오프라인 사건 발생 등 베트남이 동남아시아에서 가장 많은 온라인 및 오프라인 공격을 받은 것으로 분석

▶ **(시장현황)** Ken Research의 자료에 따르면 베트남 사이버 보안 시장이 2023년 말까지 매출 기준 약 2억 1,500만 달러에 도달할 것으로 예상하며, 2019년~2023년 기간 동안의 사이버 보안시장 연평균성장률은 약 14.8%

- 베트남의 사이버 보안 산업은 ▲사이버 범죄 사건 수 증가 ▲기업 간 보안 솔루션에 대한 인식 제고 ▲소매· ICT 및 기타 최종 사용자 산업과 같은 분야의 성장 ▲디지털 보급 증가 ▲중소기업의 데이터 보안 솔루션 수요에 따라 더욱 확장될 전망
- 베트남 보안장비 시장은 매년 10% 이상의 성장률을 보이고 있는 가운데 최근 베트남 경제 회복과 함께 공공과 민간 분야의 투자 확대가 이어지고 있어 향후 수년 간 높은 성장성이 기대

▶ **(사업자 및 경쟁현황)** 글로벌 벤더들이 베트남 정보보호 시장의 주축을 차지하는 가운데, 안티바이러스 소프트웨어 등 일부 사업영역에서 BKAV, CMC 등 현지 기업들이 두각을 나타내는 상황

- 베트남 내 안티바이러스 소프트웨어 시장은 현재 Norton Antivirus(Symantec), Kaspersky, McAfee, Trend Micro, Bit Defender, Avira 등의 유력 해외 브랜드들과 BKAV, CMC 등 자국 브랜드 및 신규 기업들 간에 치열한 경쟁이 진행 중
- 물리보안 제품 역시 대부분 수입 제품이지만, 최근 Vantech, VDTECH, Questek, Seavision, Escort 등 현지 업체들이 점차 부상하고 있으며, 현지 업체들은 가격 면에서 훨씬 저렴하다는 이점을 보유

▶ **(주요 동향)**

- 베트남 정보통신부와 일본 국제협력기구(JICA)는 베트남의 정보 보안 및 법 집행 능력 보호에 대한 인식과 기술을 높이는 프로젝트를 지원하기 위해 공동 조정위원회의 첫 번째 회의를 개최 (2019.9)
- 베트남 정보통신부와 캄보디아 우정통신부가 우정/통신 서비스, 사이버보안, 디지털서명 등 3개

부문에서의 상호협력을 위한 협약 체결(2019.3)

- 한국의 삼성 SDS가 베트남 IT 서비스 기업 CMC의 주요 의사결정에 참여하는 전략적 투자에 합의(2019.5)
- 베트남 기반 사이버 보안 스타트업 689Cloud가 싱가포르 ICE71로부터 자금을 조달(2019.5)

▶ **(융합산업)** 베트남 정부가 2025년까지 현금 사용률 8% 미만 달성을 목표로 정책을 추진하고 있으며, 베트남의 많은 은행들이 지문인식 기술, 생체인식, QR코드, 모바일 POS기술, 토큰화 등을 적용하기 시작

- 2019년에 40억 달러 이상의 가치가 있는 하노이의 Dong Anh지역의 스마트시티 건설이 시작되었으며, 베트남의 BRG그룹과 일본의 Sumitomo 기업, 일본의 Nikken Sekkei Architecture 기업간의 조인트 벤처가 310헥타르 도시 설계를 담당

▶ **(진출전략)** 다양화되고 복잡해 져가는 보안 공격에 대한 위기의식 고조로 정보보호 기술 수요가 점차 높아지고 있기에 시장 선점 차원에서 진출을 강화할 필요가 있음

캄보디아

▶ **(환경)** 캄보디아는 열악한 통신 인프라 환경과 더불어 정보보호에 대한 인식이 매우 낮은 편으로, 사이버 공격도 빈번하게 발생

- 보안업체 Kaspersky에 따르면 2018년 한 해 동안 캄보디아에서 459만 건 이상의 사이버 공격이 발생해 인터넷 사용자의 30.5%가 피해를 입은 것으로 분석

▶ **(시장현황)** 캄보디아에서는 정보보안 제품을 비롯한 소프트웨어 산업 전반에서 설계/구현 기술이 내재화되지 않아 외국산 소프트웨어를 그대로 사용하는 것이 대부분이며, 레스토랑, 중소형 호텔 등 소기업용 응용 소프트웨어와 같이 단순한 형태의 개발이 주를 이룸

- 캄보디아 보안시장의 규모는 아직까지 협소한 편이지만 불안한 치안과 지속적인 경제 성장 및 건설 경기호황에 맞춰 CCTV, 금고, 도어록과 같은 보안 제품의 수요 증가가 예상
- 캄보디아 내 Dahua Technology의 독점 유통업체 Loxu Digital은 보안 시장의 성장률을 30~40%로 예상했으며, 중국과 홍콩, 일본의 주요 투자자들이 캄보디아 보안 수요를 뒷받침하고 있다고 언급

▶ **(사업자 및 경쟁현황)** 캄보디아 정보보안 시장은 저개발된 시장 특성상 경쟁강도가 낮고, 글로벌 보안업체들도 캄보디아에 직접 지사를 설립하지 않고 현지 SI 업체 등을 통해 제품을 공급

- 캄보디아의 물리보안 시장은 파편화되어 있으며, 관련 업체들은 솔루션 기반의 판매보다는 저가 제품 위주로 가격 경쟁을 진행

▶ **(주요 동향)**

- Visa, 캄보디아에서 '보안 로드맵' 공개(2019.09)
- 캄보디아, 디지털 도어락 도입 시작(2018.08)
- 중국, 캄보디아에서 열리는 주요 국제행사에 보안 장비 제공 계획(2019.09)

▶ **(융합산업)** 캄보디아 수도 중심에 싱가포르 민간자본을 통한 스마트시티 건설을 계획 중

- 캄보디아 국립은행이 해외로부터의 송금 편의성 확대를 위하여 지불수단으로서의 블록체인 활용에 착수

▶ **(진출전략)** 시장이 작고, 법제도, 협력, 조직 등 전분야가 미흡, 시장보다는 교육 등을 통해 역량 배양 먼저 실시하고, 장기적 접근과 ODA, EDCF 자금을 활용하여 진출 필요

태국

▶ **(환경)** ITU가 2019년 1월 발표한'Global Cybersecurity Index(GCI) 2018'에 따르면 태국의 사이버보안 지수는 0.796으로 글로벌 순위는 22위(2018년 지수는 35위)를 기록한 것으로 나타났으며, 동남아 권역에서는 싱가포르와 말레이시아에 이어 3위를 기록

▶ **(시장현황)** 태국의 정보보안 시장규모는 아직 크지 않으나, 정부 차원의 적극적인 정보보안 관련 정책 추진과 인프라 투자로 향후 빠르게 성장할 것으로 전망

- 2017년 태국의 물리보안은 시장은 37억 바트의 가치를 가지고 있으며 연간 성장률은 약 12%인 것으로 집계(MarketsandMarkets)
- 태국의 CCTV 시장은 2013년~2017년간 연평균 21.5%의 성장률을 보일 것으로 전망더;며, 태국 내 범죄율의 지속적인 상승과 보안 의식이 높아짐에 따라 물리보안 시장에 대한 수요도 급격히 증가할 것으로 예측(RNCOS)

▶ **(사업자 및 경쟁현황)** Trend Micro, McAfee, Check Point, Symantec, Sophos, Kaspersky 등 동남아 지역에서 활발한 사업을 벌이고 있는 글로벌 사업자들이 태국에서도 정보보안 시장을 주도하고 있으며, SafeComs, Nod32, BitDefender, Panda 등도 두각을 나타내고 있는 상황

- 태국의 정보보안 제품 수요자들 사이에서는 유명 글로벌 기업의 제품에 대한 의존도가 높게 나타나고 있으며, 저가 제품군을 형성하고 있는 중국 기업들의 제품에 대해서는 신뢰가 낮은 편

▶ **(주요 동향)**

- 사이버보안법(Cybersecurity Act) 발효('19.1)
- 2019 개인정보보호법 제정('19.5)
- Thailand Cybersecurity 2019 개최('19.6)

▶ **(융합산업)** Barnes Report에 따르면 태국의 커텍티드 카에 대한 보안(Automotive Cyber Security) 시장 규모는 2020년에 약 6천만 달러에 달할 것으로 예측

- 태국 국가방송통신위원회(NBTC)는 연말까지 사물인터넷(IOT) 장치 규제에 관한 초안을 발표할 예정

▶ **(진출전략)** 태국은 아시아에서 사이버 공격 대상국 중 상위권 국가로서 사이버 침해로 인한 피해액이 증가하고 있어 현지 유통가 개발을 통한 정부와 기업시장 진출이 필요

말레이시아

▶ **(환경)** MyCERT의 자료에 따르면 2018년 말레이시아 전역에서 기업 및 개인에 대해 10,699건의 사이버 보안 공격이 발생했는데 이는 2017년 대비 34% 증가한 수치

▶ **(시장현황)** A.T. Kearney analysis에 따르면, 2025년 까지 ASEAN 사이버 보안 시장 규모는 두 자리 숫자의 성장률을 보일 것으로 예상되며, 그 중 말레이시아는 연평균 성장률 15%를 보일 것으로 예상

- Gartner는, 말레이시아에서 정보기술(IT) 제품 및 서비스에서 소비는 2019년 652억 RM에 달하여 2018년 대비 4.6% 증가할 것으로 예상

▶ **(사업자 및 경쟁현황)** Kaspersky Lab, Avira 등 글로벌 IT 보안 서비스 공급자들은 말레이시아 국내

사업자들과 긴밀히 협력하여 시장에 참여하고 있으며, 가격 경쟁을 피하기 위해 국내 유통채널의 통합을 추진

- 글로벌 벤더에 대한 현지 플레이어들의 기술 의존도가 높아, 에이전트나 유통업체 및 리셀러 역할에 편중되어 있으며, 현지 플레이어들의 말레이시아 내 유통망 확보 역량이 기술력보다 중요하게 평가되는 상황
- 말레이시아에서 활동하는 정보보안 서비스 제공 사업자로 대표적인 업체는 AIMS, AKTI Consulting Group, ASK Pentest, Cyber Intelligence, DNex, Firmus, Kaapagam Technologies 등

▶ **(주요 동향)**

- 말레이시아 사이버보안청(CyberSecurity Malaysia)이 새로운 멀웨어 탐지 시스템 출시('19.9)
- 디지털경제공사(MDEC)는 사이버 보안 부문에 더 많은 여성이 참여할 수 있는 컴백 경력 프로그램을 개시('19.6)
- Asia Cybersecurity Exchange는 말레이시아를 세계 주요 사이버 보안 허브로 구축할 예정으로, 2019년 4,800만 달러 규모의 사이버보안 엑셀러레이터 프로그램을 계획

▶ **(융합산업)** 디지털 보안 전문기관인 CyberSecurity Malaysia은 '17년 12월부터 연방 정부의 행정 센터인 Putrajaya에서 사물인터넷(IoT) 및 스마트시티 개발의 기타 구성요소에 대한 취약성 평가 및 침투 테스트 시스템을 진행 중

- CyberSecurity Malaysia는 IoT 보안 실험실(IoT Security Laboratory)을 통해 취약점을 시뮬레이션하고 강화 단계를 테스트

▶ **(진출전략)** 대부분의 기업에서 사이버보안에 대한 인식이 고조되고 있으나, 아직 준비는 미흡한 상황으로서 점진적인 시장 확대를 기대할 수 있음, 과학기술정보통신부 정보보호 사업의 동남아 거점인 인도네시아의 주변국으로서 인도네시아 거점 사무국을 통해 현지 마케팅 역량을 강화

라오스

▶ **(환경)** ITU의 글로벌 사이버보안 지수(GCI)에서 라오스의 지수는 0.195로 전 세계 국가 중 120위, 아시아 지역에서는 22위로 하위권을 기록

▶ **(시장현황)** 라오스의 정보보호 시장은 시장 규모에 대한 통계도 존재하지 않을 만큼 낙후되어 있으며, 정보보호 수준을 향상시키기 위한 국가 전략도 부재하여 단기간 내 국가적 지원을 통한 성장 가능성은 제한적

- 라오스의 사이버보안 대응능력은 ASEAN 국가 중 캄보디아에 이어 최하위로 평가되며, 인구수도 적어 해외 보안업체들도 라오스에 직접 지사를 개설하기보다는 태국 등 주변국가의 지사에서 현지 유통업체를 거쳐 제품을 공급

▶ **(사업자 및 경쟁현황)** 2016년 10월 라오스 우정통신부 자료에 의하면 라오스의 ICT 관련 기업은 총 398개로 이중 ICT 보안업체로 분류된 업체는 단 한 개에 불과했으며, ICT 리셀러가 234개, ICT 설치 업체가 99개로 대부분을 차지

- KOTRA 라오스 현지 무역관에 따르면 라오스는 보안 소프트웨어나 CCTV 등의 보안 장비를 자체적으로 생산하는 업체가 없고 IT 유통업체들이 중국, 태국, 베트남 등 주변국에서 수입
- 물리보안 시장의 경우 낮은 소득과 안정적인 치안 환경으로 인해 개인 소비자는 보안장비에 대한

인식과 수요가 높지 않으며, 주로 기업과 기관, 임대사업자들을 중심으로 보안장비 수요가 형성

▶ **(주요 동향)**

- 라오스 보안장비 시장, 중국 업체들이 주도하고 있으며 특히 HikVision과 Dahua에 대한 선호도가 높은 상황('19.5)
- 주요 도시를 중심으로 부동산 등의 인프라가 개발되면서 라오스 디지털 도어락 시장이 성장 추세('19.5)
- 전자정부 서비스에 블록체인을 활용한 디지털 신원 서비스 도입을 추진('19.7)
- 라오스 최초의 디지털 포렌식 실험실 설립('19.8)

▶ **(융합산업)** 라오스는 핀테크 산업 발전 초기 단계로 은행이 주도하여 시장을 이끌고 있으며, 중국 관광객의 자국 내 소비를 촉진시키기 위해 중국 핀테크 기업의 라오스 시장 진입을 허용

4. 중남미 시장

시장 동향 및 전망

▶ 브라질과 멕시코가 견인 중인 중남미 지역의 정보보안 시장은 2018년 80억 9,000만 달러로 추산되며, 2023년경 143억 5,000만 달러에 이를 전망

표 _ 중남미 지역 주요국 정보보안 시장규모

(단위: 십억 달러)

국가	2016	2017	2018e	2023p	연평균성장률 (2018-2023)
브라질	2.77	3.11	3.46	5.6	10.10%
멕시코	1.9	2.18	2.49	4.59	13.00%
기타 국가	1.6	1.86	2.14	4.16	14.20%
합계	6.27	7.16	8.09	14.35	12.10%

[출처] MarketsandMarkets, Physical Security Market-Global Forecast To 2023, 2019

▶ 중남미 지역 국가들 중 브라질, 멕시코 및 아르헨티나에서 몇 년 동안 물리 보안 솔루션 및 제품에 대한 수요가 크게 증가하였으며, 이 지역의 산업 부문은 늘어나는 범죄 활동 대응을 위해 물리 보안 솔루션을 채택하고 있으며 이러한 지출은 향후 지속적으로 증가할 것으로 예상

표 _ 중남미 지역 주요국 물리보안 시장규모

(단위: 십억 달러)

국가	2016	2017	2018e	2023p	연평균성장률 (2018-2023)
브라질	1.05	1.17	1.29	1.89	7.90%
멕시코	0.84	0.96	1.09	1.72	9.5%
기타 국가	2.31	2.45	2.58	3.26	4.8%
합계	4.20	4.57	4.96	6.87	6.70%

[출처] MarketsandMarkets, Physical Security Market-Global Forecast To 2023, 2019

멕시코

▶ **(환경)** 멕시코는 1년 이내에 사이버 공격이 가장 많은 국가로 중남미에서 2위를 차지하였으며, 사이버 보안을 위한 전반적인 국가 관리 로드맵이 부재

▶ **(시장현황)** 2017년 멕시코 산업 수치에 따르면 보안 시스템 및 솔루션의 판매는 전체 경제에서 2% 성장을 훨씬 능가하여 10% 이상 증가

- 특히 스마트 홈 보안 부문의 수익은 2019년 1억 6,300만 달러이며, 29.6%의 연평균 성장률(CAGR 2019-2023)로 2023년까지 4억 6,000만 달러에 이를 것으로 예상
- 미국 상무부는 2017년 멕시코 보안시장 규모를 약 17억 달러로 추산하며 향후 시장규모가 더욱 확대될 것으로 예상

▶ **(사업자 및 경쟁현황)** 멕시코의 사이버 보안 부문은 글로벌 대기업이 가장 큰 시장 점유율을 확보

- Promexico에 따르면 멕시코의 사이버 보안 시장은 Cisco 및 Symantec이 주도하고, FireEye, ProofPoint, Fortinet 및 Palo Alto Networks 등의 업체가 SaaS의 하위 세그먼트를 계속 확장 중
- 물리보안 시장 중 비교적 높은 비중을 차지하는 디지털 도어록 시장에는 품질을 앞세운 LockState, Rocky Mountain 등의 미국 브랜드와 가격을 앞세운 다수의 중국 브랜드가 경합

▶ **(주요 동향)** 금융 기술 규제법(멕시코 Fintech 법)을 통해 정보 또는 금융 기관 등에 무단 접근하는 행위를 규제('18.3)

- '미국-멕시코-캐나다 협정(USMCA)'을 체결하고 사이버 보안 관련 조항을 신설('18.9)

▶ **(융합산업)** 2016년 멕시코의 스타트업 Dronix는 자동차 서비스 및 보안·경비 업체인 LoJack과 함께 범죄 예방을 위한 파트너십을 형성하고 드론을 이용한 범죄 예방프로그램을 가동

▶ **(진출전략)** 경제규모가 크고 ICT기술 수준이 중위권을 유지하고 있으나, 중남미 국가 중 가장 많은 사이버 침해사고가 발생하고 있어, 피해규모를 줄이려는 정부와 금융기관 등 대기업의 투자가 증가함에 의해 시장성장을 기대할 수 있음

코스타리카

▶ **(환경)** 코스타리카는 중남미 국가 중 정보보호 관련 제도가 비교적 잘 정비되어 있다고 평가되고 있으나, 주로 물리적인 측면의 보안 분야가 주도하고 있는 양상

▶ **(시장현황)** 최근 강도, 살인 등의 강력범죄가 증가하면서 많은 상업시설 및 기업들이 사설경비업체 고용 및 경비시스템 확충에 많은 비용을 투자하고 있으며 정부 역시 GDP의 평균 3.5%에 해당하는 예산을 공안부에 책정하며 시민 및 시민의 재산 보호에 주력

▶ **(사업자 및 경쟁현황)** 코스타리카의 정보보호시장은 아직은 전통적인 인적 물리보안 사업이 주류를 이루고 있고 최근 들어 일부 다국적 기업 현지 법인 및 지사의 참여가 시작된 정보보안 부문은 업체가 늘어나는 추세

- 2017년 6월 Control Pas에 등록된 사설보안업체 수는 737개이며 그 중 557개 업체가 실제 영업 중인 것으로 추정되며 2만 4천여 명의 사설보안요원이 있는 것으로 추정
- 코스타리카 현지 정보보호 업체는 없으며, 아카마이, IBM, HP 등 글로벌 기업이 진출하여 자체 SOC를 통해 고객사를 관제, 딜로이트는 정부기관을 대상으로 서비스를 제공

▶ **(주요 동향)**

- 최근 코스타리카에서는 5G, IoT, AI 등 신기술 확산에 따른 사회적 문제점을 해결하기 위한 Simulator(사회적 논의체)와 관련해 정치, 교육, 기술 등 관련 종사자들의 모임이 활성화('19.9)
- 코스타리카 대표단이 국가 및 지역 수준에서 발생하는 사이버 범죄의 유형을 파악하고 관리하기 위한 CSIRT 지역 회의에 참여('19.5)
- IBM, 2,100만 달러를 투자하여 코스타리카에 글로벌 IT보안서비스센터 설립 계획 발표('19.2)

▶ **(융합산업)** 2018년 11월 코스타리카의 전력 업체인 Conelectricas가 사물인터넷(IoT) 솔루션을 도입하여, 이를 활용한 스마트 그리드(Smart Grid) 사업에 나선다고 발표

▶ **(진출전략)** 중남미 국가 중 시장매력도를 보유한 국가로서 중남미 진출 거점지역으로 활용 중, 한국기업의 중남미 시장 진출 시 현지 교두보로 활용 필요

도미니카공화국

▶ **(환경)** 도미니카공화국은 국가 사이버보안 체계 등이 갖추어져 있지 않으며 기술수준 및 국민의 전반적인 보안 의식이 낮은 편

- 물리 보안 영역의 경우, 글로벌 인증기업 UL이 발표한 'UL Safety Index(2017 업데이트)'에서 59점을 기록하며 187개국 중 109위로 평가

▶ (시장현황) 물리 보안 영역에서는 도미니카공화국 곳곳에 범죄가 증가하고 있고 정부 주도의 치안 프로젝트를 추진함에 따라 앞으로 CCTV의 수요는 몇 년간 증가할 것으로 예상

- 도미니카공화국 관세청(Direccion General de Aduanas, DGA)에 따르면 도미니카공화국은 보안 카메라를 전량 수입 중으로 지난 5년간 도미니카공화국 보안 카메라 수입액은 4,960만 달러 규모에 이르며 2017년에는 전년 대비 37% 증가
- 미국 상무부에 따르면, 기술적인 진보는 보안 산업에 대한 접근 자체를 재구성하고 있는데 기존 인력을 이용한 서비스가 전자보안 장비, 알람, CCTV 등을 사용하는 방식으로 대체 중

▶ **(사업자 및 경쟁현황)** 도미니카공화국 내 카메라 등의 물리 보안 장비에서 Fertec(미국), Dahua(중국), Vivotek(대만), Kocom(한국), AV Tech(대만), Hivision(중국), Samsung(한국) 등의 브랜드가 경쟁 중

- 최근 3년간 보안 카메라 수입 시장 점유율은 미국이 68.4%로 1위를 차지했고 중국(19.9%), 파나마(3.2%), 푸에르토리코(2.3%), 한국(1.6%)의 순

▶ **(주요 동향)**

- 글로벌 보안 기업인 Symantec이 발간한 LATIN AMERICAN+CARIBBEAN CYBER SECURITY 보고서에 따르면 도미니카공화국의 가장 빈번한 사이버범죄는 신용카드복제, 이메일 및 소셜네트워크를 통한 명예훼손, 디지털 인증 도용, 피싱 및 전화를 이용한 사기 등
- 2018-2021 국가 사이버보안 전략 수립(Decreto 230-18, Establece y regula la Estrategia de Ciberseguridad 2018-2021)

▶ **(융합산업)** 도미니카공화국은 FITUR 2019박람회에서 동해안에 위치한 Bávaro-Punta Cana(바바로 푼타 카나)지역에 첫 스마트 시티를 조성할 계획이라고 발표

- Fintech Latin America 2018: Growth and consolidation 보고서에 따르면 도미니카 공화국 내 백만 명의 사용자가 핀테크를 이용 중이며, 평균 1,200만 건의 월간 거래를 이뤄지는 등 빠르게 성장하는 산업이라 평가

▶ **(진출전략)** 국가 전반적으로 보안 취약성이 높으므로 보안의식 강화에서부터 통합적인 정보 보안 제품, 단일품목의 물리보안 제품에 이르기까지 진출 고려

페루

▶ **(환경)** 페루의 정보보호 산업 환경은 아직 후진적 구조이나 법적 제도적 정비는 타 중남미국에 비해 양호한 편

- 정보보호 수요는 증가 추세지만, 자체 기술 수준, 조직적 체계, 역량구축 면에서는 열위 수준으로 제대로 정보보호 활동이 이루어지지 못하고 있는 상황

▶ **(시장현황)** 현재는 보안시장에서 물리보안 부문이 시장을 장악하고 있는 상황이지만, 최근 3년 전부터 사이버 범죄가 증가하면서 정보보안 수요 및 매출이 빠르게 증가 중

- 정보보안 업체 수 증가와 고용인원 측면에서는 2-3%대의 안정적 성장을 중이지만, 해당 기업의 매출액은 12-13%대의 고속 성장을 기록
- 미국 상무부에 따르면 페루의 안전 및 보안 시장 규모는 2017년 2억 9,690만 달러 → 2018년 3억 3,670만 달러 → 2019년 3억 4,980만 달러(추정)로 증가

▶ **(사업자 및 경쟁현황)** 정보보호 시장에서는 2,700개가 넘는 기업들이 전통적인 인적 물리보안 활동을 중심으로 활동하고 있으며, 최근 들어 대형 보안업체를 중심으로 ICT 기술을 활용한 고도의 정보보호 및 감시 활동을 강화해 나가는 추세

- 페루의 보안 장비 시장은 중국, 대만 등의 저가 브랜드 제품이 강세
- 페루 정보보호 산업을 기업 규모별 업체 수, 매출액 및 고용인원 별로 분석해 보면 영세기업 중심 구조

▶ **(주요 동향)**

- 소포스社에 따르면 현재 페루의 사이버보안 시장 규모는 소포스社 추산 1.8억불로 추산되며, 2021년까지 2.2억불로 성장할 것이라 전망
- 정부 부문 보안 관제 센터 구성 활성화

▶ **(융합산업)** 암호화폐는 페루의 인터넷 사용자들에게 가장 많이 알려진 핀테크 서비스(41.6%) 중 하나로, 2019년 초 ibitt는 페루에서 암호화 ATM 설치를 확장

- 2019년 5월 페루 정부가 블록체인 스타트업인 Stamping.io와 협력하여 투명한 계약 조달 시스템을 구축했다고 발표

과테말라

▶ **(환경)** 과테말라의 정보보호 산업 환경은 법적 및 제도적 정비가 제대로 갖춰지지 않은 후진적 구조

- 정보보호 수요는 증가 추세 이지만, 자체 기술 수준, 조직적 체계, 역량구축 면에서는 열위 수준으로 제대로 정보보호 활동이 이루어지지 못하고 있는 상황

▶ **(시장현황)** 과테말라의 주거용, 산업용, 사무용 보안장비에 대한 수요가 상승하는 추세로, 안전 및 보안 등 보안 제품의 총 수입이 2017년 2,374만 달러 → 2018년 2,534만 달러 → 2019년 2,567만 달러로 증가

- 치안상태가 최하위라고 평가되며 아직 해소되지 못하고 있는 빈부격차로 인한 민생범죄와 마약관련 범죄, 피싱 및 절도 등 다양화되고 있는 사이버 범죄 등으로 인하여 정보 보안 수요가 점차 증가

▶ **(사업자 및 경쟁현황)** 물리보안 분야는 중국과 미국이 시장을 장악하고 있으며 기업과 주택 소유자들은 보안 경보, 감시 카메라, 조명 등 예방 장비에 대한 관심이 높아지는 추세

- 중국 정부는 과테말라 보안 프로젝트에 대해 세제 혜택, 면제 및 무제한 자금 지원을 통해 카메라, 비디오 레코더 및 기타 보안 장비 제조업체를 지원 중

▶ **(주요 동향)**

- 기업과 시민들은 경찰이 사유재산권을 보호할 수 없다는 인식이 증가함에 따라 많은 사람들이 개인 보안을 선호하며 고용된 개인 보안과 보안 시스템에 대한 수요 증가 추세
- 심각한 살인율로 인해 민간 보안 부문이 빠르게 성장하고 있으며, 일반 기업 예산의 약 10-12%를 민간 보안에 투자

▶ **(융합산업)** 과테말라는 Salcajá시에 과테말라 최초의 스마트 시티 프로젝트를 착수

- 일본에 기반을 둔 암호 화폐 거래소 Bitpoint가 2019년 9월 과테말라에 암호 화폐 교환을 가능하게 하는 서비스를 개시
- 2019년 7월 통과된 '회사 설립 촉진을 위한 기업가 정신 강화에 관한 법률'에는 젊은 기업가들의 크라우드 소싱 및 암호 화폐 지원 정책이 포함

엘살바도르

▶ **(환경)** 엘살바도르의 정보보호 산업 환경은 라틴 아메리카와 카리브해 평균보다 현저히 낮으며, 정보보호에 대한 국가 수준의 정책이나 전략, 사이버 보안 관련 규제를 갖추지 못한 상황

- 인터넷 보급률은 약 34% 정도로 사이버 보안에 대한 인식도 저조

▶ **(시장현황)** 엘살바도르에서는 이동통신 시장의 강한 성장으로 인터넷 접속과 전자화폐, 모바일 결제 사용이 증가함에 따라 특히 금융, 통신 분야 정보보안 수요가 증가 될 것으로 예상

- 현재 경찰 역량으로 엘살바도르 전국 곳곳의 폭력조직이 벌이는 범죄를 통제하기 어려운 상황이며, 이로 인한 CCTV, 치안 시스템 등에 대한 수요가 존재

▶ **(사업자 및 경쟁현황)** 중앙아메리카의 주요 사이버 보안회사인 Soluciones Seguras가 엘살바도르 San Salvador에 사무소를 운영하며 사이버 보안 솔루션을 제공 중

▶ **(주요 동향)**

- 엘살바도르 공공안전부는 한국인터넷진흥원(KISA)이 운영하는 글로벌 사이버보안 협력 네트워크(CAMP) 회원으로 가입('19.4)
- 한국의 과학기술정보통신부와 한국정보화진흥원이 엘살바도르에 정보접근센터를 개소('18.12)

▶ **(융합산업)** conomist Intelligence Unit(EIU)의 2019년 자료에 의하면, 엘살바도르는 핀테크를 위한 감독 프레임워크를 개발 중

- 엘살바도르 시장에서 기능적으로 운용되는 전자화폐 Tigo Money 및 MoMo는 3,000명 이상의 에이전트와 1백만명 이상의 사용자를 보유하고 있는데, 이는 각 지방 자치 단체의 90% 및 성인 인구의 16%에 해당

5. 중동·동유럽 시장

시장 동향 및 전망

▶ 중동 지역의 정보보안 시장은 2018년 132억 2,500만 달러로 추산되며, 이후 연평균 12.8%씩 성장하여 2023년경 241억 5,000만 달러에 이를 전망

표 _ 중동 지역 정보보안 시장규모

(단위: 십억 달러)

2016	2017	2018e	2023p	연평균성장률 (2018-2023)
10.12	11.63	13.25	24.15	12.80%

[출처] MarketsandMarkets, Physical Security Market-Global Forecast To 2023, 2019

▶ 한편, 물리보안 시장규모는 2018년 77억 4,000만 달러로 추산되며, 이후 연평균 7.9%씩 성장하여 2023년경 113억 4,000만 달러에 이를 전망

표 _ 중동 지역 주요국 물리보안 시장규모

(단위: 십억 달러)

국가	2016	2017	2018e	2023p	연평균성장률 (2018-2023)
UAE	2.21	2.49	2.79	4.24	8.8%
사우디아라비아	1.26	1.52	1.66	2.69	10.1%
기타 국가	2.84	2.99	3.29	4.40	6.0%
합계	6.3	6.99	7.74	11.34	7.90%

[출처] MarketsandMarkets, Physical Security Market-Global Forecast To 2023, 2019

오만

▶ **(환경)** 2018 UN전자정부보고서에 따르면, 오만 전자정부 순위는 193개국 중 63위를 차지하여 아랍 국가 중 6위를 기록했으며 특히 보안 평가 지수는 글로벌 4위에 위치

▶ **(시장현황)** 오만의 경우 활발하게 정보보호 시장이 성장 중이지만, 인구수가 약 400만 명으로 작은 편이어서 시장 규모는 GCC 주요국 중 소규모인 7,000만 달러 수준

- GCC 타국가와 마찬가지로 CCTV 에 대한 수요가 많으며 시장 진출 역사가 오래된 유럽 및 일본 제품에 대한 선호도가 높은 편

▶ **(사업자 및 경쟁현황)** 물리적 보안 및 보안 시설 운영 분야는 다국적 기업들의 영향력이 큰 상황이며, 오만 국내 기업들의 정보보안 솔루션 제공이 증가 추세

- 하드웨어의 경우, Dell 및 Cisco를 중심으로 미국 회사 제품이 강세를 보이고 있으며 여기에 인도의 Cyberoam도 경합 중
- 오만 내에는 IT 보안 제품군을 생산하는 회사가 없어 해외 기업에 의존하고 있으며, 통상적으로 에이전트 또는 바이어에 의해 수입을 진행

▶ **(주요 동향)**

- 오만 로컬기업 Thawani Pay는 핀테크 기술이 적용된 Thawani Pay 플랫폼 기반의 서비스를 발족('18.3)
- 오만아랍뱅크(OAB)는 '17년 12월 디지털화로 변화 중인 금융서비스의 미래 비전을 위해 전자 지불 게이트웨이 서비스를 시행('17.12),

▶ **(융합산업)** 오만 보건부(MOH)는 모바일 애플리케이션을 통해 모든 환자들이 자신의 건강 기록과 상태를 온라인으로 볼 수 있는 스마트 서비스를 제공할 예정(2019.8)

- 오만 디지털 혁신 가속화를 위해 오만통신사 Omantel, 블록체인 솔루션 및 서비스(BSS)와 ITA e-government 부서와의 협력을 바탕으로 국가적 블록체인 프로젝트를 개시(2019.3)
- 2019년 4월 Duqm(두큼) 지역에 스마트 시티 조성 계획을 발표, 2020년부터 단계적으로 착공에 들어갈 계획

▶ **(진출전략)** 정부의 전자정부 개발과 주요 국가 인프라 개발 참여를 위해 시스템 구축, 교육훈련, 운영관리와 AS를 포함한 토탈 서비스 진출이 필요. 2016년부터 운영 중인 해외진출 거점을 중동지역 진출 교두보로 활용

UAE

▶ **(환경)** 2000년대 말부터 석유 및 가스 산업 의존도를 낮추기 위해 산업 ICT 산업을 위시한 다각화 정책을 추진하고 있으나, IT 도입과 보안에 대한 정부 투자 의지에도 불구하고, UAE가 외부의 보안 위협에 매우 취약한 상황이라는 분석과 사례가 등장

▶ **(시장현황)** SDI에 의하면, UAE 주요 기반시설 정보보호 시장은 2025년까지 22억 달러 규모를 형성, 2016년부터 2015년까지 연평균 3.2%의 지속적인 성장세를 실현할 것으로 전망

- 네트워크 보안 시장은 2025년까지 3.8% 성장하면서 전체 정보보호 시장 성장(3.2%)을 주도할 것으로 분석되는데, 이 같은 측면에서 향후 UAE 정보보호 관련 시장은 물리 보안 시장보다는 네트워크 보안 분야가 주도할 것으로 예상
- 미 상무부에 따르면 정부 주도의 프로젝트를 중심으로 고급 보안 솔루션에 대한 투자가 이어질 전망으로, 특히 주요 인프라 프로젝트에 대한 보안 위협 관리 수요가 상당히 증가할 전망

▶ **(사업자 및 경쟁현황)** Thales, IBM, UTC 등 글로벌 벤더들의 시장 점유율이 높은 편으로, 이들은 현지법인을 설립하여 직접 판매도 하지만, 복수의 에이전트를 통한 간접 판매에도 적극적

- 즉, 글로벌 벤더들에 대한 기술 의존도가 높아 현지 사업자들은 에이전트, 유통업체, 리셀러 역할에 편중
- UAE 사이버 보안 시장은 공공과 민간부문으로 나뉘며, 공공부문은 정부 프로젝트가 대부분으로 Thales(프랑스), Narus(Boeing의 자회사) 등의 유럽, 미국 기업이 선점하여 경쟁이 치열

▶ **(주요 동향)**

- UAE 통신규제청 '사이버보안 국가 전략 2019' 시행(2019.6)
- 미국 통신사 AT&T, 두바이 텔레콤 보안 얼라이언스 가입 (2019.3)

▶ **(융합산업)** UAE 보건부(Ministry of Health and Prevention, MoHAP)은 보건 데이터를 보관하고 공유하는 블록체인 시스템을 발표(2019.9)

- 현재 UAE의 블록체인 시장 규모 및 발전 수준은 아직 낮은 단계이나 정부의 개방적 정책으로 인해 다양한 산업에서 빠르게 활용될 것으로 기대

▶ **(진출전략)** 오만 등 전략 거점국가를 활용하여 운용, 시스템 구축, 교육훈련, 운영관리분야에 집중할 필요가 있으며, SOC, 디지털 포렌식 분야, 스마트 시티 보안 인프라 진출도 추진 필요, UAE 총판이 가능한 기업 발굴 모색

카타르

▶ **(환경)** 2022년 카타르 도하 월드컵을 앞두고 CCTV 감시, 화재 패널, 통신 시스템과 같은 여러 기술이 현지 시장에 계속 제공되고 있으며, 물리, 통신보안 분야에 대한 수요가 증가하며 안전과 보안문제가 대두됨에 따라 관련 시설 및 서비스에 대한 수요 또한 증가할 전망

▶ **(시장현황)** Markets and Markets의 최근 중동 지역 사이버 보안시장 보고서에 의하면, 카타르는 이 지역에서 가장 높은 비율로 성장할 것으로 예견

- 시장조사기관 Research And Market의 보고서에 의하면, 카타르의 관리형 보안(Managed Security) 시장은 2018년~2024년 동안 연평균성장률 47.8% 이상으로 상당한 성장을 보일 것으로 전망

- 미국 국제무역국 자료에 의하면, 2022년 월드컵에 대한 보안 요구사항과 국가 사이버 방위 인프라 개선의지로 인해, CCTV 감시 및 접근 제어, 사이버 보안, 통합 보안 시스템, 빌딩 관리 시스템, 침입 탐지 장비, 스포치 안전 및 보안, 전자 안전 및 화재 감지, 통신 시스템 등의 수요가 높을 것으로 추정

▶ **(사업자 및 경쟁현황)** 보안 서비스 시장 성장세로 인해 주변국들과 국제 기업들의 진출이 증대되는 중이나, 오만과 함께 5개국 중 가장 낮은 경쟁강도를 보유한 것으로 분석

- 카타르 CCTV시장에서 활동하는 주요업체는 Pelco, Hikvision Digital Technology, Axis Communications AB, Dahua Technology Middle East FZE, Honeywell 등이 대표적

▶ **(주요 동향)**

- 카타르 교통통신부, 사이버보안 프레임워크 개시('19.2)
- 카타르의 민간 항공국이 '항공 사이버 보안 가이드라인' 발표('19.6)
- 카타르 사이버 보안센터 등은 사이버 보안 분야 협력 및 훈련을 위해 Cisco와 계약 체결('19.7)

▶ **(융합산업)** 루사일(Lasail)시 주도의 스마트 시티 개발은 도하(Doha)로 연장하는 야심찬 도시 건설 프로젝트로, 첨단기술 솔루션을 기반으로 스마트 시티 관리 및 모니터링을 수행할 계획

▶ **(진출전략)** 한국과 공동연구 수요가 높으며, 공동연구 후 현지 진출가능 지역으로, 향후 대형 국제행사 등으로 건설 수요가 높으며 관련 시스템과 보안관련 프로젝트 가능성 높음. 인터넷진흥원과 카타르와의 민관워킹그룹 활동 활용이 필요하며, 중동거점을 통해 바이어, 총판 발굴 및 정부협력 추진 필요

사우디아라비아

▶ **(환경)** ITU 2018 'Global Cybersecurity Index(GCI)'에 따르면 사우디 아라비아의 사이버보안 지수가 0.881로 전 세계적으로 13위, 중동 국가에서 1위를 기록했으나, 사이버 공격 위험에 대한 일반적인 인식이 부재

▶ **(시장현황)** 2018년에서 2022년까지 사우디 아라비아의 전체 보안 지출은 CAGR 7.9%로 2019년 4억 5500만 달러에 도달할 것으로 전망

- 사우디 아라비아 물리 보안 시스템 시장은 2024년까지 3억 1300만 달러에 이를 것으로 예상
- U.S.-Saudi Arabian Business Council에 따르면, 사이버 보안 시장이 2022년까지 CAGR 15.3 % 성장할 것으로 예상

▶ **(사업자 및 경쟁현황)** 사우디 아라비아의 물리 보안 시장에서 활동하고 있는 업체는, GCC 대부분의 국가에서와 마찬가지로 글로벌 업체 및 국내 업체가 혼재

- 물리적 보안 시스템 시장에서는 Avigilon, Axis Communications, Bosch Security, Hikvision, Siemens, Honeywell Security 및 Samsung Techwin 등의 주요 업체가 활동
- 국토 안보 및 치안 시장에서는 Al Alameya, Axis Communications, Bristol, Drager, Genetec, NAFFCO, Nedap 및 ZMR 등의 업체가 주로 활동

▶ **(주요 동향)**

- 사우디 외교 안보국에 따르면 최근 이란, 카타르와의 외교적 갈등과 관련해 사우디 정부기관과 기업에 대한 사이버 공격이 지속

- UAE와 사우디아라비아 기관들은 여전히 사이버 보안 사고에 대응할 준비가 되어 있지 않으며, 응답자 31%는 사이버 보안 사고 대응 계획이 마련되어 있지 않다고 밝힘('19.5)

▶ **(융합산업)** 사우디 아라비아는 2018년 9월 현재 암호화폐의 제도적 기반은 마련되어 있지 않으나, 블록체인을 국가적 차원에서 도입하려는 의지를 보유

- 사우디아라비아 정부는 2025년까지 미국 뉴욕의 33배 크기에 달하는 초연결사회인 NEOM 건설 프로젝트 발표

▶ **(진출전략)** 시장 규모와 성장성 면에서 중요한 시장이나 글로벌 유력 보안 업체들이 이미 진출해 있어, 현지 유통 업체와의 파트너십을 통해 진출할 모색

이란

▶ **(환경)** 이란 정보보호 시장은 매우 열악하고 개인정보 유출이 심한 국가로 개인정보 당 최소 1리얄(0.0001달러)에 판매되고 있으며, 이로 인해 스팸, 사기 및 신원도용 등이 빈번히 발생

- 또한 이스라엘과의 정치적 대립으로 인한 분쟁이 지속되고 있으며, 사이버 테러를 이용한 범죄 발생 건수도 지속적으로 증가

▶ **(시장현황)** 이란의 정보보호 시장은 이스라엘 등 주변 국가와의 정치적 대립이 지속됨에 따라, 개인정보보호보다는 정부의 국방 및 안보를 보호하기 위한 정책적인 지원에 주력할 가능성이 높고, 관련 정보보안 시스템 구축에 집중 투자할 전망

▶ **(사업자 및 경쟁현황)** 이란에서 활동 중인 보안서비스 기업은 Arecont Visio, BCD Video, Nextchip, HID Global, Surveon Technology, Inc., DSX Access Systems, Inc., Anviz Global Inc. 등

▶ **(주요 동향)**

- 이란-미국 간 사이버공격 감행 정황을 포착했는데, 2019년 5월 호르무즈 해협를 중심으로 한 유조선 공격 사건이 발생하고 이란이 배후로 지목되면서 미국-이란의 갈등이 첨예하게 대립하는 가운데, 이란과 미국은 서로 사이버공격을 감행하고 있다고 보도('19.6)

▶ **(융합산업)** 이란 중앙은행, 은행 및 금융 부문을 위한 국가 블록체인 플랫폼 프로젝트 착수

- Borna 플랫폼으로 불리는 국가 블록체인 플랫폼 구축을 통하여 현재의 낙후된 시스템을 대체하고 디지털 금융경제로의 전환을 도모할 목적

루마니아

▶ **(환경)** ITU가 발표한 글로벌 사이버보안(GCI) 2018에 따르면 루마니아의 사이버보안 지수는 0.568로 단계로 글로벌 순위는 175개국 중 72위로 나타났으며, 유럽국가 권역에서는 46개 국가 중 38위를 낮은 수준을 기록

▶ **(시장현황)** 사이버 보안은 루마니아 ICT부문의 핵심 요소에 해당하며, 루마니아의 IT 시장은 중동부 유럽에서 가장 빠르게 성장하는 시장 중 하나로 IT 시장은 2017~2021년에 3.1% 성장하여 2021년 99억 RON(24억 7,000만 달러)의 가치에 이를 것으로 전망

▶ **(사업자 및 경쟁현황)** 루마니아에서 사이버보안 시장이 부상하고 있으며, 미국 공급업체와 같은 외국

업체에게도 사이버 보안 시장을 개방

- 현지 루마니아의 채널 파트너를 통해 판매하는 것이 해외 제조업체가 위험을 최소화하는 시장 진입 전략이며, 주요 사업자로는 Bitdefender, Safetech Innovations, Bit Sentinel, UTI Group, Mac Douglas Grup 등이 활동

▶ **(주요 동향)**

- 인도 대표 IT기업 Infosys는 루마니아 부쿠레슈티에 사이버보안센터 런칭을 발표('19.7)
- 루마니아와 이스라엘이 사이버보안포럼 추진을 위한 MoU를 체결('19.6)

▶ **(융합산업)** 2016년 트란실바니아 지방 Alba Iulia시에 루마니아 최초의 스마트 시티 구축 계획을 발표

- 스마트 조명, 디지털 교육, 공공 WiFi 설치, 의료 핫라인, 폐기물 관리, 불법 주차 모니터링 등 20개 이상의 개별 프로젝트가 진행, 2019년에도 프로젝트를 계속 이어갈 예정

▶ **(진출전략)** 시장 규모와 성장성 면에서 중요한 시장. 루마니아 지역의 기술 보안 업체들의 활동이 활발하므로, 현지 진출 시 사이버보안 지역협회(ANSSI)와 현지 업체와의 파트너십을 통해 진출을 모색

6. 아프리카 시장

시장 동향 및 전망

▶ 2018년 아프리카의 정보보안 시장은 36억 3,000만 달러이며, 이후 연평균 16.1%씩 성장하여 2023년에는 76억 7,000만 달러에 이를 것으로 전망

표 _ 아프리카 지역 정보보안 시장규모

(단위: 십억 달러)

국가	2016	2017	2018e	2023p	연평균성장률 (2018-2023)
아프리카 지역	2.61	3.09	3.63	7.67	16.10%

[출처] MarketsandMarkets, Security As a Service Market-Global Forecast To 2023, 2019

탄자니아

▶ **(환경)** 탄자니아 내 ICT 사용이 증가하면서 사이버위협도 함께 증대되고 있는데, Kaspersky Lab의 모바일 악성코드 관련된 보고서에 의하면 2018년 한 해 동안 탄자니아 모바일 사용자의 약 31.34%가 모바일 악성코드 공격을 경험

▶ **(시장현황)** 탄자니아의 경찰 1명당 서비스 인원은 1,049명으로 국제표준(1명당 450명)에

못미치는데, 이러한 적은 규모의 경찰력으로 인해 물리보안 시장이 점차 확대될 것으로 예상

- 2017년 기준 탄자니아 정보보안 시장 규모는 750만 달러 수준

▶ **(사업자 및 경쟁현황)** 탄자니아의 CCTV시장은 유럽제품과 중국제품이 경쟁하는 가운데 중국제품이 점유율을 크게 확대하고 있는 추세

- 주요 사업자는 Tera Technologies and Engineering Ltd., CATS Tanzania Ltd., NRD East Africa Ltd., Cyberoam, SCI, Softnet Technologies Limited, ComSec Security Systems Ltd. 등이 대표적

▶ **(주요 동향)**

- 탄자니아 통신규제청(TCRA)은 사기성 트래픽 추적 시스템 도입('19.1)
- 탄자니아 통신규제청(TCRA)은 남 아프리카 통신 규제 협회의 연례 총회를 주최하여 사이버 범죄에 대해 논의('19.3)
- 탄자니아는 보안 강화 및 사이버 범죄 방지를 위해 개인이 보유할 수 있는 휴대 전화 번호 수를 네트워크 당 한 개의 SIM카드로 제한할 계획('19.4)

▶ **(융합산업)** 2018년 7월 규제기관은 M2M/IoT 서비스의 사용 증가와 관련된 다양한 범위의 필요성에 대한 대응으로 번호 계획(numbering plan)에 대해 논의

- 규제기관은 ITU의 권고에 따라 15개의 숫자 범위를 사용하도록 제안하였고, M2M 장치의 활성화는 2018년 SIM 카드 등록 규제에 따라 적용
- BoT(Bank of Tanzania)는 즉시 지불 시스템(instant payment system)인 TIPS(Tanzania Instant Payment System) 개발 프로젝트를 2019년 2월 개시

▶ **(진출전략)** 사회적 기반이 취약한 나라이므로 시스템 구축, 교육훈련, 운영관리와 A/S 등 토탈 서비스 제공방식으로의 접근 활용. ODA, EDCF 자금을 활용한 프로젝트 발굴 필요

르완다

▶ **(환경)** ICT 발전과 함께 사이버 보안 위협과 범죄가 증가하고 있으며, ITU 'Global Cybersecurity Index 2018'에서 사이버보안 지수 0.697, 글로벌 순위 49위를 기록

▶ **(시장현황)** 르완다에서는 정부차원에서 ICT분야와 정보보안 분야 발전을 위한 종합계획을 발표하고 추진함에 따라 정보보안 수요가 증가할 것으로 예상

- 2017년 기준 르완다 정보보안 시장 규모는 280만 달러 수준

▶ **(사업자 및 경쟁현황)** 2019년 6월 르완다 정부가 결정한 2019-2020 회계 연도의 예산 2조 8천억 Rwf(약30억 3,100만 USD) 중에서 르완다 경찰이 공공 CCTV를 출시할 수 있도록 최소 50억 Rwf를 할당하여 경찰의 역량과 운영 향상을 도모

- 주요 사업자는 Pergamon Group Ltd., Fodey Security & Alarm System (FOSES) LTD., ISCO, Cyberteq, KK Security Ltd., Sekanyolya Systems Ltd., Highsec Ltd. 등이 대표적

▶ **(주요 동향)**

- 르완다 정부는 사이버 보안 및 개인정보보호에 관한 말라보 협약을 비준('19.7)
- 보안업체 Kaspersky Lab이 르완다에 사무실을 열어 동아프리카에서 사이버보안을 강화하며 사업을 확장('19.5)

- 보안 분야 기술회사인 Secure Services Mauritius이 르완다 보험 회사 및 금융기관의 사이버 보안 위협을 줄이기 위해 르완다 지사를 설립('19.3)

▶ **(융합산업)** 르완다 정부는 비전 2020개발 프로그램 및 2017-2024년 국가 전략의 일환으로 추진하는 주요 프로젝트로 Kigali 혁신도시 구축을 추진

- 르완다 정부는 금융 서비스에 ICT를 도입해 현금 없는 경제로 전환할 계획을 수립했으며, 르완다 중앙은행인 르완다 국립 은행(National Bank of Rwanda)이 자체 디지털 화폐 발행 방안을 모색 중('19.8.)

▶ **(진출전략)** 기 진출한 SOC, PKI 관련 추가 수주가 기대되며, 인력양성 사업에 관심이 높음. 정부간 협력관계 활용을 통한 추가 진출 및 Joint Venture 설립 등을 매개로 하여 현지기업과 아프리카 지역 공동진출 제안 필요

케냐

▶ **(환경)** African Cyber Security Report 2018 보고서에 의하면, 케냐의 멀웨어에 의한 피해가 지속적으로 증가하고 있으며, 사이버 범죄에 대한 노출 정도 역시 매우 높고, 금전적 피해도 심각한 것으로 분석

▶ **(시장현황)** 케냐 보안 시장은 IT서비스의 시장 성장과 더불어 함께 성장할 것으로 예상되나 현재 케냐 IT서비스 시장 자체는 여전히 작은 규모에 해당

- 케냐 2016년 IT서비스 시장 규모는 IT 전체 시장 중 21.5%로, 이집트의 28.4%, 남아프리카공화국의 40%에 비해 낮은 수준
- '17년 기준 케냐 정보보안 시장 규모는 2,330만 달러 수준으로 추정

▶ **(사업자 및 경쟁현황)** 인도 Cyberoam 등의 글로벌 네트워크 장비 기업이 현지 기업과 파트너십을 체결하고 현지 마케팅을 진행하고 있으며, 최근에는 네트워크 장비 위주의 보안에서 통합적으로 제공되는 보안 서비스 시장으로의 전환이 이루어지고 있는 것으로 분석

- 클라우드 서비스의 증가로 MSS(Managed Security Service) 등과 같이 아웃 소싱 및 서비스 형태로 기업에게 통합적인 보안 서비스를 제공하는 사업자도 증가
- 주요 사업자는 Safricom, Cyberoam, Symantec, AccessKenya, NetGuardians 등

▶ **(주요 동향)**

- 케냐 고등학교에서부터 사이버보안, 개인정보보호, 안전한 데이터 관리 교육을 추진할 예정('19.3)
- 케냐 2019년 1/4분기 사이버 위협, 전분기 대비 10.1% 증가('19.8)

▶ **(융합산업)** 케냐의 모바일 지급결제 시장은 2018년 기준으로 3조 9,844억 KES의 시장 규모를 형성하고 있으며, 모바일 금융 서비스 이용자수도 지속적으로 증가

- 케냐의 스마트 시티 계획이 진행되고 있는 콘자 지역의 개발과 관련해 중국 선전의 화웨이 캠퍼스 모델을 따라하겠다고 발표('19.9)
- 케냐 정부, 음식의 안전성을 제고하기 위해 블록체인 기술을 적용하기로 결정('19.7)

▶ **(진출전략)** 현재 시장은 크지 않지만 성장 가능성이 기대되므로 아프리카 거점을 활용하여 진출할 필요가 있음. 기반이 매우 취약한 나라이므로 시스템 구축, 교육훈련, 운영관리와 AS를 포함한 토탈 서비스 방식의 접근을 활용

세네갈

▶ **(환경)** 세네갈은 ▲사이버 보안 관리 체계적 구조 부재 ▲국가 사이버 보안 전략에 대한 공식 문서의 부재 ▲사이버 보안 사건을 관리하는 기관의 부족 등 취약한 사이버 보안 환경을 보유

▶ **(시장현황)** 세네갈은 공공 치안 문제로 인해 사설보안이 차지하는 비중이 매우 높은 국가로서, 물리보안 시장의 경우 정확한 통계를 통한 분석이 어려운 상황

- 2017년 기준 세네갈 정보보안 시장 규모는 430만 달러 수준으로 추정
- 사이버 보안 문제에 대한 일반적인 인식이 여전히 낮으므로, 사이버 보안 시장은 아직 완전히 개발되지 않고 있음

▶ **(사업자 및 경쟁현황)** 세네갈은 국내에서 생산되는 사이버 보안 제품이 없으며, Kaspersky Lab, McAfee, Panda, Trend Micro 등 글로벌 기업의 보안 제품을 사용하는 실정

- 이 밖에도 Abus, SPB securite privee, Axis 등의 유럽 기업뿐 아니라 ZKTeco, Hikvision, Dahua Technology(중국), Nec Xon(일본) 등의 아시아 기업 다수 진출
- 물리보안 제품으로는 주로 중국이나 프랑스 제품을 사용

▶ **(주요 동향)**

- 세네갈 수도 다카르에 아프리카 사이버 보안 학교 개설('18.11)
- 세네갈 정부와 한국정보화진흥원(NIA)이 협업해 ICT 정책 역량 및 관리·실행 능력 강화 지원을 도모('19.4)

▶ **(융합산업)** 2019년 11월 IoT 준비 및 개발 우선순위를 논하기 위해 이해관계자 워크숍을 개최하고, ▲세네갈의 IoT 보안 ▲우선 순위의 IoT 개발 ▲잠재적 위협 및 과제 등의 문제를 논의

- 세네갈 통신 업체인 Tigo Senegal은 디지털 시장을 가속화하기 위해 Ericsson과 함께 클라우드를 포함한 전국 네트워크의 현대화 프로젝트 진행('18.12)

▶ **(진출전략)** 경제성장률이 높다는 점에서 장기적으로 진출 의미는 있음. 서아프리카지역에서 가장 정보보호분야에 관심이 높은 국가로 ODA, EDCF 자금을 활용한다면 2~3년 내로 프로젝트 발주 가능성이 높음

에티오피아

▶ **(환경)** 이스라엘계 글로벌 보안 기업 Check Point에 따르면, 에티오피아는 아프리카에서 멀웨어 및 보안 위협에 노출된 상위 10개국에 속할 정도로 보안이 취약

▶ **(시장현황)** 시장조사기관 6Wresearch는 외국인 투자 급증으로 산업, 제조, 운송 및 전략 유틸리티 분야의 건설 프로젝트가 증가함에 따라 에티오피아의 비디오 감시 시스템 시장이 2019년~2025년에 증가할 것으로 예측

- 카메라, 레코더, 비디오 관리 소프트웨어는 향후 몇 년 동안 에티오피아의 비디오 감시 시스템 시장에서 시장을 지배할 것으로 예상

▶ **(사업자 및 경쟁현황)** 정보보안 시장에서는 IBM, CISCO, Fortinet, Check Point 등 글로벌 보안기업이 활동하고 있는 것으로 보이나 경쟁이 거의 없는 것으로 파악

- 에티오피아 네트워크 및 보안제품 대리점 MKTY는 SOPHOS 및 Cyberoam의 제품을 취급하고 있으며, 중소기업을 위한 UTM(Unified Threat Management)에서 Firewall, CCTV 등 물리보안 및 정보보안에 관한 다양한 제품을 현지에 공급하고 있음을 알 수 있음
- 물리보안시장은 중국 제품이 유럽 제품을 제치고 시장을 잠식 중

▶ **(주요 동향)**

- 에티오피아 대통령은 2020년 7월말 이전에 2개의 민간 회사에 통신 산업 부문 영업허가를 부여할 예정이라고 발표하였으며, Safaricom, MTN 그룹, Orange, Vodafone을 포함한 다국적 회사들이 라이선스 입찰에 관심 표명('19.10)
- 정부의 고위 공무원이 포함된 6명의 암살로 인해 에티오피아 전국적으로 인터넷 셧다운이 있었으며, 이후 10일만에 단계적으로 복원('19.6)

▶ **(융합산업)** 에티오피아 정부는 10년간 프로젝트 비용 최대 30억 달러 규모로 Amhara주의 Bahir Dar에 실제의 와칸다(Wakanda)라는 기술 도시를 건설하기 위해 2018년 8월 Hub City Live와 파트너십을 체결

- 모바일 플랫폼 대출업체 Equity Bank는 2019년 에티오피아 시장에 주목하며 시장 진출을 준비

▶ **(진출전략)** 정보보안시장은 현재까지는 시장규모가 매우 작으나, 경쟁이 저조하기 때문에 장기적 관점에서 시장진출의 기회는 풍부할 것으로 판단

지부티

▶ **(환경)** 지부티의 2017 ITU 글로벌 사이버보안 지수(GCI)는 0.99로 140위를 차지했으나 2018년 0.063으로 아랍지역국가 중 20위, 글로벌 순위는 159위를 기록하면서 큰 폭으로 하락

- 국가정보보호국(ANSIE)가 현재 국가 차원의 사이버보안전략을 마련하기 위한 초기 논의 단계에 있으며, 사이버보안 관련 법제를 개선할 방침

▶ **(시장현황)** 지부티에 자체적인 사이버 보안 및 물리 보안 제조사가 없어 글로벌 IT 솔루션 기업들의 제품이 시중에 판매되고 있는 것으로 파악

▶ **(사업자 및 경쟁현황)** 지부티 물리보안 시장에서 큰 비중을 차지했던 유럽 및 일본 전자보안기기보다 중국제품의 사용이 더욱 많아지고 있는 추세

- 네트워크 및 기본적인 글로벌 IT 솔루션 기업은 현지에 진출하거나 대리점을 통해 제품을 판매하고 있으며 Cisco는 네트워킹 보안 및 장비 교육 과정을 개설해 운영 중
- 주요 사업자는 정보보안 분야의 SDSI, Tech in Djib, Dis-pro Informatique, 물리보안 분야의 AGS Sécurité, Somelec, Alfa Mep 등

▶ **(주요 동향)**

- 지부티 중앙은행(BCD)은 세계은행의 지원을 받아 개선된 자동이체시스템(système de transfert automatique amélioré, ATS+)라는 국가결제시스템을 사용해 실시간으로 안전하게 은행간 결제 및 대량 송금이 가능하게 될 전망('19.2)
- 지부티 내무부는 세계적으로 증가하는 사이버 범죄를 방지하기 위해 법제를 강화할 방침이라고 발표('19.8)
- ICT 기술을 사용한 범법행위의 예방·퇴치를 위해 국가안보국(Direction Générale de la Sécurité

Nationale) 내에 디지털정보국(Direction de l'Intelligence numérique)을 신설('18.1)

배냉

▶ **(환경)** 서아프리카에서 나이지리아, 코트디부아르에 이어 가장 많은 사이버범죄행위가 일어나는 국가로, ITU의 'Global Cybersecurity Index'에서 175개국 중 80위(0.485)를 기록

▶ **(시장현황)** 베냉은 ICT 분야가 발전함에 따라 ICT기술을 사용한 범죄가 증가하면서 정부 및 민간 주도로 많은 토론회, 포럼 등이 개최되고 관련 법제, 조직 등이 정비되는 등 사이버 보안에 대한 의식이 제고되고 있는 상황이나 보안 시장 자체는 여전히 작은 규모이며 파악이 어려움

▶ **(사업자 및 경쟁현황)** 베냉은 자체 정보 보호 상품이 없고 글로벌 기업 상품을 사용하는 실정

- 나이지리아의 CCTV, 출입 제어, 화재 및 도난 경보 시스템 설치기업들이 베냉에 진출해 판매, 설치 및 유지·보수 서비스를 제공
- 주요 사업자는 ExperTIC, Sagam Sécurité Bénin, e-telecom, Sobitech 등

▶ **(주요 동향)**

- ANSSI-Bénin은 디지털 보안 국가 전략 마련을 위한 토론회를 개최하고 사이버 보안 이슈, 사이버 위협의 정의 및 종류, 국가보안전략의 필요성 및 목표, 주요 이슈 등에 대한 의견을 교환('19.4)
- ANSSI-Bénin은 사이버보안 관련 경쟁력을 강화하고자 제2회 해커랩 2019(Hacker lab 2019)를 개최('19.9)

▶ **(융합산업)** 베냉에는 아직 융합보안시장이 형성되지 않은 상태이지만, 핀테크, 스마트시티, 사물인터넷에 대한 관심 및 인식이 높아지는 상황

- Buddecomm의 자료에 따르면 1억 2,000만 달러가 투자되는 베냉 스마트 시티는 베냉 최초의 디지털 구역으로서, 육양국(ACE cable landing station) 주변의 12헥타르에 해당하는 면적에 건설될 예정이며 디지털 경제 개발 계획의 중심을 이룰 계획

CONTENTS

Ⅰ 개요

1. 조사 배경 및 목적 ····· 1
2. 조사 범위 ····· 7
3. 보고서 구성 및 전년도 보고서와의 차별점 ····· 8

Ⅱ 글로벌 정보보호 산업 권역 및 국가별 현황

1. 글로벌 정보보호 시장 현황 및 전망 ····· 9

2. 선진국 시장 ····· 17
   가. 미국 ····· 22
   나. 일본 ····· 67
   다. 영국 ····· 98

3. 아시아 시장 ····· 133
   가. 중국 ····· 139
   나. 인도 ····· 171
   다. 인도네시아 ····· 197
   라. 베트남 ····· 231
   마. 캄보디아 ····· 271
   바. 태국 ····· 289
   사. 말레이시아 ····· 318
   아. 라오스 ····· 352

4. 중남미 시장 ····· 367
   가. 멕시코 ····· 373

나. 코스타리카 ····· 397
다. 도미니카공화국 ····· 428
라. 페루 ····· 456
마. 과테말라 ····· 486
바. 엘살바도르 ····· 503

5. 중동·동유럽 시장 ····· 522
가. 오만 ····· 531
나. UAE ····· 553
다. 카타르 ····· 582
라. 사우디아라비아 ····· 610
마. 이란 ····· 633
바. 루마니아 ····· 650

6. 아프리카 시장 ····· 670
가. 탄자니아 ····· 675
나. 르완다 ····· 709
다. 케냐 ····· 748
라. 세네갈 ····· 781
마. 에티오피아 ····· 796
바. 지부티 ····· 819
사. 베냉 ····· 831

■ 참고문헌 ····· 844

Ⅰ. 개요

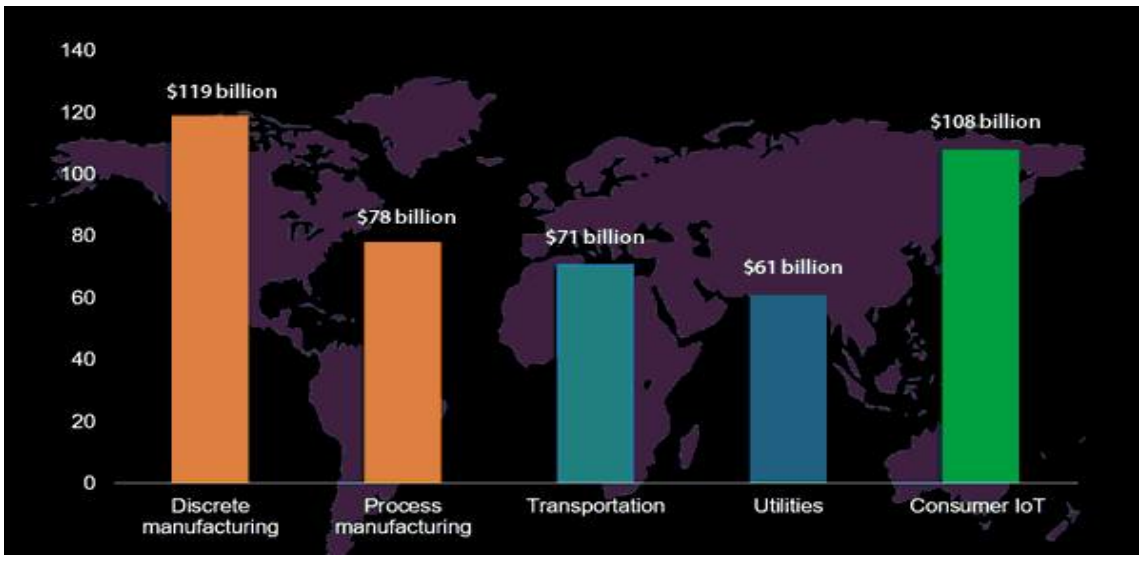
1. 조사 배경 및 목적

IoT, 5G, AI, 클라우드 등 신기술 확산에 따른 침해 사고 위협 증가

▶ IoT, 5G, 인공지능(AI), 클라우드 등 신기술이 급속히 확산되면서 다양한 비즈니스 기회가 창출되고 생산성이 상승하는 반면, 이에 따른 사이버보안 위협도 동시에 증대

- IT 조사기관 Gartner에 따르면, 전 세계 커넥티드 기기는 2019년 142억 개에서 2021년 250억 개까지 증가할 전망으로 이는 매일 127개의 새로운 IoT 기기가 인터넷에 연결되는 것을 의미
- IDC는 전 세계 IoT 지출이 2018년 6,460억 달러에서 15.4% 증가한 7,450억 달러에 도달할 것으로 예측했으며, 2022년에는 1조 달러를 상회할 것으로 전망

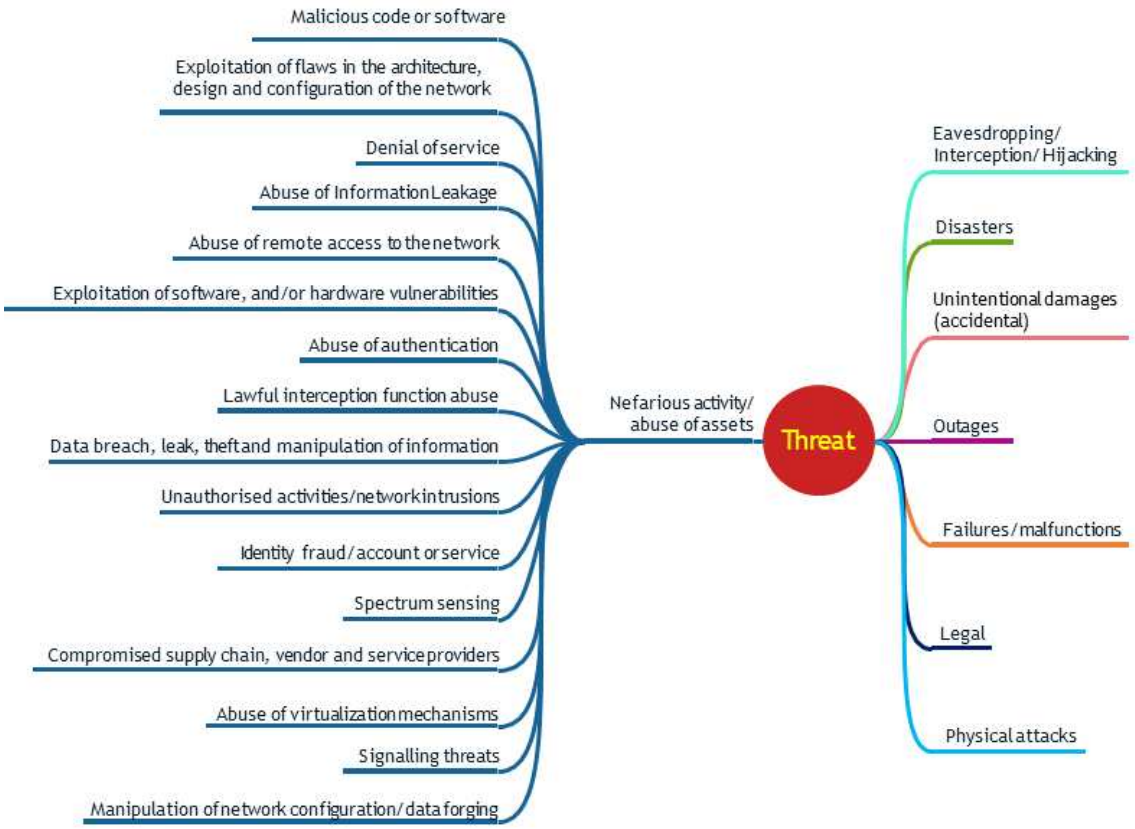
그림 _ 2019년 분야별 IoT 지출 비용 (단위: 십억 달러)



[출처] I-scoop(2019.6)

- 또한 미국, 중국, EU를 위시한 여러 국가들이 5G 구축 및 상용화에 박차를 가하는 가운데, 동 기술이 산업 분야의 기회를 창출하는 동시에 공급망 위험, 네트워크 보안 등 취약성에 대한 우려 대두

그림 _ 5G 위협 환경



[출처] ENISA(2019.11)

▶ 특히 전 세계적으로 주요 산업 분야에서 대규모 피해를 유발하는 사이버 침해 사고 발생

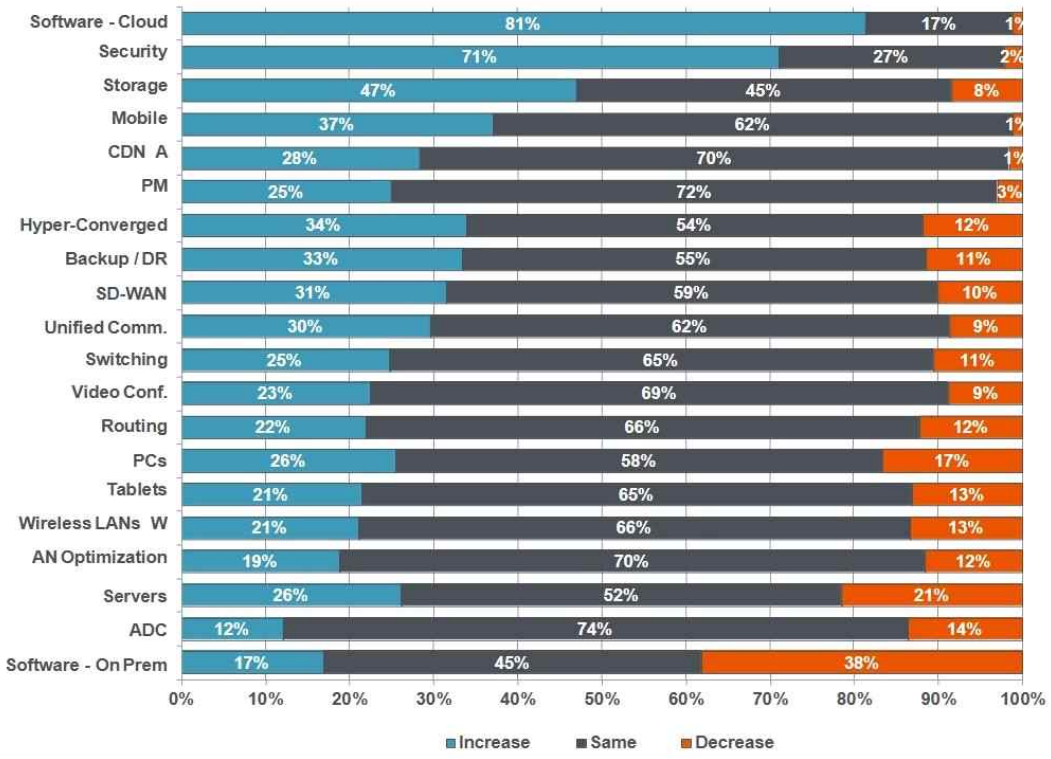
- (제조) 미국의 콘크리트 회사 Precast는 미 해군과 맺은 계약 내용을 해커에게 도난당했으며(2016년), 독일의 ThyssenKrupp는 철강생산 및 제조공장 설계부문 기술영업 비밀이 대규모 사이버 공격으로 해커에게 탈취(2016), 일본의 자동차 업체 Honda는 워너크라이의 침입으로 자동차 생산을 중단(2017년)하는 사고가 발생
- (보건의료) 미국의 병원간 협력체인 UnityPoint Health는 140만 명의 환자 기록이 피싱 공격으로 침해(2018년), 영국의 국민건강서비스 NHS는 오래된 시스템의 취약점으로 인해 랜섬웨어에 희생되어 일주일 간 전체 서비스의 약 1%에 해당하는 서비스가 중단(2017년)되는 사고 발생
- (교통) 미국의 공유차량 서비스 Uber는 해커에 의해 5,700만 명의 개인정보를 탈취(2016년), 샌프란시스코의 교통 시스템은 랜섬웨어 공격으로 3일간 무료 운행을 단행(2016년), 스웨덴 교통청은 DDoS 공격으로 열차 운행 지연을 초래(2017년), 영국의 British Airway는 고객 정보를 노린 사이버 공격으로 예약자 38만 명의 정보를 탈취 당하는 사고를 경험(2018년)

- (금융) 미국의 신용정보기관 Equifax는 해킹으로 인해 1억 4,600만 명의 개인정보를 유출(2017년), 미국의 버지니아 은행은 스피어 피싱 공격으로 해커에게 8개월 간 240만 달러를 빼앗겼으며(2017년), 일본에서는 인터넷 뱅킹용 악성 코드 DreamBot을 사용하는 일당이 해당 코드를 활용해 약 2억 4천만 엔을 훔친 것으로 조사(2017년)

▶ 사이버보안 위협이 다양화되고 대규모 피해가 잇따르자 산업계에서는 보안 분야를 우선 순위로 투자 강화

- 투자자문 기관인 Piper Jaffray가 미국 및 10개국의 110개 주요 기업 CIO를 대상으로 실시한 설문 조사에서 응답자의 71%가 2019년 보안 분야 투자를 전년 대비 늘릴 것으로 응답해 조직 내 IT 투자 중 두 번째로 높은 지출 필요성을 보임

그림 _ 2019년 주요 기업 CIO의 분야별 투자 계획



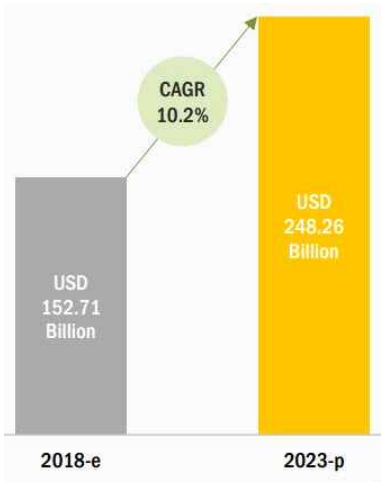
[출처] Piper Jaffray(2019.1)

사이버 위협에 대응하기 위한 투자 증가로 정보보안 시장 높은 성장세 지속

▶ 전 세계 정보보안 시장 향후 5년간 연평균 11.0%의 높은 성장세 전망

- 시장조사기관 MarketsandMarkets에 따르면, 전 세계 정보보안 시장은 2018년 1,527억 1천만 달러 규모에서 5년간 연평균 10.2%로 성장해 2023년에는 2,482억 6천만 달러 규모에 이를 전망

그림 _ 전 세계 정보보안 시장 성장 전망 (단위: 십억 달러)



[출처] MarketsandMarkets(2018.9)

▶ 정부 규제 준수 수요와 내외부 위협 요인 증대로 사이버보안 수요 강화

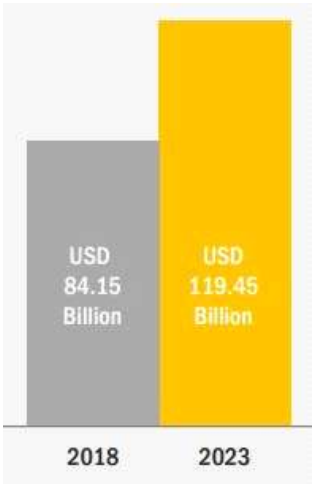
- DDoS 공격, 랜섬웨어, 멀웨어, APT(Advanced Persistent Threat) 등 다양한 기법을 활용한 사이버 해킹은 전 세계적으로 확산되고 있는 추세
- 정보보안 시장은 전 세계 정부들도 엄격한 수준의 컴플라이언스 요구 확산과 내외부 각종 위협에 따른 보안 침해 사례 증가 및 복잡성 심화 등에 적극적으로 대응 중
- EU의 일반 개인정보보호법(GDPR)과 미국을 중심으로 한 컴플라이언스 이니셔티브 및 데이터 보안 니즈 강화는 규제 요구 사항 준수에 특화된 기술인 레그테크(RegTech) 시장 활성화를 촉발
- 이에 따라 규제준수 프로세스 효율성 향상, 운영 리스크 완화 및 기업 리스크 관리 기능을 갖춘 솔루션에 대한 수요도 빠르게 확산
- 한편, 수직 산업별로는 의료, 은행·금융·보험·서비스(BFSI), 정부, 항공·우주·국방 부문 등 이 가파른 성장세를 기록할 것으로 기대

한편, 세계 곳곳에서 발생하는 테러와 치안 불안, IT 기술의 발달로 물리보안 시장도 높은 성장세를 유지

▶ 글로벌 시장조사기관인 MarketsandMarkets는 전 세계 물리보안 시장 규모가 2018년 841억 5,000만 달러 규모에서 2023년 1,194억 5,000만 규모로 연평균 7.3% 증가할 것으로 전망

- 물리보안은 자연재해, 화재, 도난, 강도, 테러 공격 등 내외부적인 물리적 위협으로부터 조직 및 구내 하드웨어, 소프트웨어, 네트워크 인프라 보호를 위한 안전 조치를 의미
- 물리보안은 화재, 테러, 기물 파손 및 도난 등 조직에 피해를 줄 수 있는 사건들로부터 소프트웨어, 인력, 하드웨어, 정보 및 네트워크를 보호
- 물리보안은 비디오 감시(CCTV), 액세스 제어 프로토콜, 침입자 경보, 서비스 등으로 구성

그림 _ 전 세계 물리보안 제품 및 서비스 시장 전망 (단위 : 십억 달러)



[출처] MarketsandMarkets(2018.9)

▶ IoT, 클라우드, 모바일 등과의 접목을 통한 첨단 물리보안 제품이 시장 성장 견인

- 물리보안은 사이버보안에 비해 상대적으로 단순한 기술 지식만으로도 공격 대상에 노출될 수 있어 빈번한 공격 대상이 될 수 있으며, 공격에 따른 피해 역시 치명적일 수 있음
- 최근에는 물리보안 분야 역시 IT 기술과 물리보안 시스템 간의 결합을 통한 다양한 첨단 제품들이 출시되고 있는 가운데, 수년 간 IP 기반 비디오 감시 카메라, 모바일 기반 접근 제어, IoT 기반 보안 시스템 및 클라우드형 물리보안 플랫폼에 대한 수요가 꾸준히 진작

IT 강국인 우리나라는 보안 분야가 내수 시장에 그치고 있어 적극적인 세계 시장 진출이 필요

▶ 우리나라는 세계 최고 수준의 정보보호 관련 기술과 제품을 보유하고 있어 분야별로 성공적인 세계 진출 품목이 많으나, 정보보호 산업은 여전히 내수 산업에 머물고 있어 전략적 수출 품목으로 육성이 필요

- 우리나라의 강점인 ICT 강국 위상, 침해 사고 대응 경험, 강점 보안 기술을 결합해 해외 보안 시장 진출을 강화
- 해외 진출에 필요한 주요국 현황을 국가별로 조사해 비교·분석하고 권역별 전략 거점을 선정해 해외 진출의 교두보로 삼고 점진적으로 수출을 확대

2. 조사 범위

조사 대상 범위는 정보보안 시장과 물리보안 시장

▶ 본 조사에서는 정보보호 산업 중 정보보안과 물리보안 산업을 조사 대상으로 삼음

- 정보보안은 정보 자산을 보호하는 것으로서 네트워크 보안, 콘텐츠 보안, 웹 보안, 메시지 보안, 엔드포인트 보안, 식별 및 접근 관리, 취약점 관리 등이 이에 속하며 관련 컨설팅과 시스템 구축을 포함
- 물리보안은 물리적 자산 및 인적 자산을 보호하는 것으로서 영상 감시, 출입 모니터링, 접근 통제 제품 및 시스템, 물리적 방호벽, 개인 보호 장비, 바이오 인식 제품 등이 이에 속하며 관련 컨설팅과 시스템 구축은 물론 보안 출동 경비 서비스 등을 포함
- 조사 대상 지역과 조사기관에 따라 정보보안과 물리보안 구분 기준은 다르게 적용될 수 있으며 또한 최근 융합기술과 융합산업이 급속도로 발달함에 따라 정보보안과 물리보안 어느 한 쪽으로 분류할 수 없는 융합보안 성격의 제품과 서비스들도 빠르게 증가하고 있는 상황

전 세계 주요국 30개국을 대상으로 조사

▶ 본 조사는 전 세계 시장을 크게 ▲선진국 시장 ▲아시아 시장 ▲중남미 시장 ▲중동·동유럽 시장 ▲아프리카 시장 등 5개 권역으로 분류했으며, 총 30개국을 조사 대상 국가로 삼음

권역	조사 대상국
선진국 시장(3)	- 미국, 일본, 영국
아시아 시장(8)	- 중국, 인도, 인도네시아, 베트남, 캄보디아, 태국, 말레이시아, 라오스
중남미 시장(6)	- 멕시코, 코스타리카, 도미니카공화국, 페루, 과테말라, 엘살바도르
중동·동유럽(6)	- 오만, UAE, 카타르, 사우디아라비아, 이란, 루마니아
아프리카(7)	- 탄자니아, 르완다, 케냐, 세네갈, 에티오피아, 지부티, 베냉

- 선진국 시장은 미국과 일본, 영국 3개국을 대상으로 했으며, 이들 3개국은 정보보호 최대 수요처이자 기술 보유국으로서 시장성과 협력 및 경쟁 관계 여부를 조사
- 아시아 시장은 세계 최대 단일 시장으로 도약하고 있는 중국을 비롯해 G3로 발전하고 있는 인도, 세계 4위의 인구를 보유한 인도네시아, 경제 발전이 빠르게 진행 중인 베트남, 이밖에 캄보디아, 태국, 말레이시아, 라오스를 조사

- 중남미 시장은 라틴아메리카 경제 2위국 멕시코, 우리나라와 FTA 협정을 맺어 교역을 확대하고 있으며 우리나라 ICT 기술에 관심을 보이는 코스타리카, 페루, 엘살바도르, 과테말라를 비롯해 도미니카공화국을 포함
- 중동·동유럽 시장은 다양한 분야에서 우리나라 전자정부 등 ICT 기술 도입을 추진하는 오만과 중동 지역 경제 산업 중심지 사우디아라비아, UAE, 2022년 월드컵 개최국으로서 정보보호 수요가 풍부한 카타르, 사이버보안 강국 이란 및 동유럽 국가로서 소프트웨어가 발달한 루마니아를 조사 대상국으로 선정
- 아프리카 시장은 최근 정보화 발전이 빠르고 정보보호에 사회적 관심이 증대되고 있는 탄자니아, 케냐, 르완다, 세네갈을 비롯해, 에티오피아, 지부티, 베냉을 중심으로 시장동향을 살펴보고 진출 전략을 도출할 예정

3. 보고서 구성 및 전년도 보고서와 차별점

글로벌 및 권역별 주요 보안 시장 현황과 전망, 30개 국가별 정보보호 시장 및 정책 현황을 제시

▶ (구성) 본 보고서는 크게 제1장 개요, 제2장 글로벌 정보보호 산업 권역 및 국가별 현황으로 구성

- 제1장 개요에서는 본 조사의 배경 및 목적, 조사 범위, 보고서 구성을 다룸
- 제2장 글로벌 정보보호 산업 권역 및 국가별 현황에서는 글로벌 정보보안 및 물리보안 시장 현황과 전망을 검토한 후 조사대상 30개국을 5개 권역별로 구분
  - 각 권역 현황에서는 권역별 주요 특징과 주요 보안 시장 현황 및 전망을 정리
  - 권역별 국가 현황에서는 국가별로 ▲정보보호 산업 개요 ▲정보보호 시장 현황 ▲정보보호 정책 및 기관 현황에 대한 조사 내용을 정리

▶ (차별점) 글로벌 및 권역별 보안 시장 현황을 대폭 강화하고 국가별 ICT 융합시장 및 정책 내용 추가

- 글로벌 및 권역 개요에서 정보보안 시장과 물리보안 시장 규모와 전망을 수록했으며, 세부 시장으로는 최근 주목 받고 있는 시장 중 IoT보안 시장, 서비스형 보안 시장 및 인공지능 보안 시장의 규모와 전망 데이터를 표로 정리해 각 시장별/권역별 규모와 성장성 비교가 가능하도록 함
- 30개 국가별 ICT융합 산업에 대한 시장과 정책 동향을 수록해 새롭게 부상하고 있는 신시장에 대한 자료로 활용(IoT, 스마트 의료, 자율주행차, 스마트 시티, 블록체인, 핀테크 등)

Ⅱ. 글로벌 정보보호 산업 권역 및 국가별 현황

1. 글로벌 정보보호 시장 현황 및 전망

정보보안 시장

▶ **(정보보안 일반)** 시장 규모 면에서는 IAM, 성장률 면에서는 암호화 분야가 시장을 견인 중이며 2023년까지 연평균 10.2%로 성장할 전망

- 전 세계 정보보안 시장은 2018년 1,527억 3,000만 달러로 추산되는 가운데 매년 10.2%의 성장률을 기록하며 2023년 2,482억 6,000만 달러를 형성할 것으로 전망

표 _ 전 세계 정보보안 시장 규모 및 성장 전망 (단위 : 십억 달러)

구분	2016년	2017년	2018년(e)	2023년(p)	연평균 성장률('18-'23)
시장규모	122.93	137.63	152.71	248.26	10.2%
연간성장률	13.0%	12.0%	11.0%	9.9%	

주) e: estimated, p: projected [출처] MarketsandMarkets(2018.9)

- 전 세계 정보보안 시장을 솔루션과 서비스로 구분할 경우 2018년 솔루션 시장은 866억 5,000만 달러, 서비스 시장은 660억 600만 달러를 각각 기록했으며, 2023년에는 솔루션이 1,357억 6,000만 달러, 서비스가 1,125억 달러를 차지

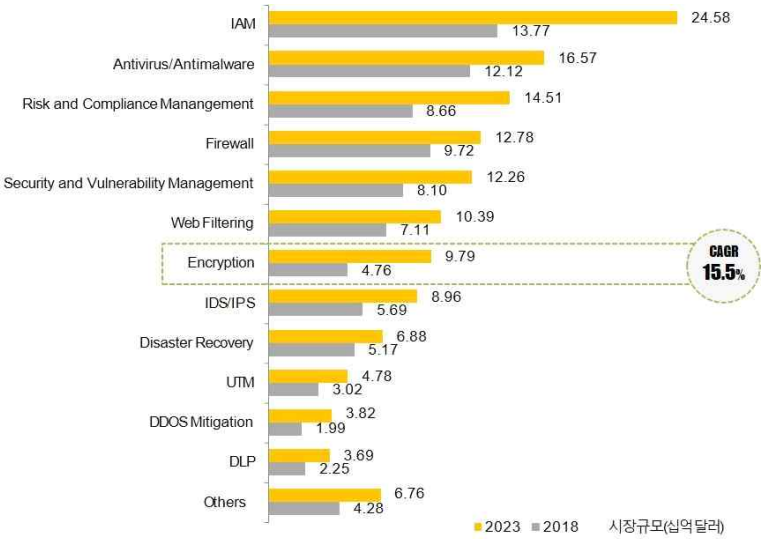
표 _ 전 세계 정보보안 구성 요소별 시장 규모 및 성장 전망 (단위 : 십억 달러)

구분	2018년(e)	2023년(p)	연평균 성장률('18-'23)
솔루션	86.65	135.76	9.4%
서비스	66.06	112.50	-11.2%

주) e: estimated, p: projected [출처] MarketsandMarkets(2018.9)

- 한편, 분야별로는 2018년 기준 IAM 시장이 137억 7,000만 달러 규모로 가장 큰 것으로 나타나고 있으며, 암호화 시장은 2023년까지 연평균 15.5%의 성장세를 보여 가장 높은 증가세를 보일 전망
- 두 번째로 큰 시장은 안티바이러스 및 안티 멀웨어 시장으로 2018년 121억 2,000만 달러 규모를 형성한 것으로 추산되며, 그 다음으로는 방화벽 시장이 97억 2,000만 달러 규모로 세 번째를 차지

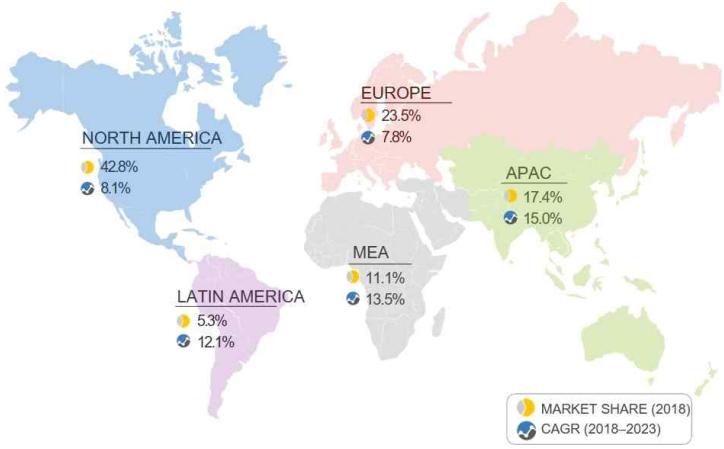
그림 _ 전 세계 정보보안 분야별 시장 규모 및 성장 전망



[출처] MarketsandMarkets(2018.9)

- 권역별로는 2018년 기준 북미가 42.8%로 가장 큰 비중을 차지하나 2023년까지의 성장률은 아태지역이 15.0%의 CAGR로 가장 빠른 성장을 보일 것으로 예상

그림 _ 전 세계 주요 권역별 정보보안 시장 비중 및 연평균 성장률



[출처] MarketsandMarkets(2018.9)

▶ **(IoT 보안) 시장 규모 면에서는 네트워크 보안, 성장률 면에서는 클라우드 보안 분야가 시장을 견인 중이며 2023년까지 연평균 33.7%의 성장률을 기록할 전망**

• 전 세계 IoT 보안 시장은 2018년 82억 2,000만 달러로 추산되는 가운데 매년 33.7%의 성장률을 기록하며 2023년 351억 2,200만 달러를 형성할 것으로 전망

표 _ 전 세계 IoT 보안 시장 규모 및 성장 전망 (단위 : 백만 달러)

구분	2016년	2017년	2018년(e)	2023년(p)	연평균 성장률('18-'23)
시장규모	5,241.7	6,550.0	8,220.0	35,152.2	33.7%
성장률	-	25.0%	25.5%	43.5%	

주) e: estimated, p: projected [출처] MarketsandMarkets(2018.9)

• 전 세계 IoT 보안 시장을 솔루션과 서비스로 구분할 경우 2018년 솔루션 시장은 52억 400만 달러, 서비스 시장은 30억 1,600만 달러를 각각 기록했으며, 2023년에는 솔루션이 210억 2,410만 달러, 서비스가 141억 2,810만 달러를 차지

표 _ 전 세계 사이버보안 구성 요소별 시장 규모 및 성장 전망 (단위 : 백만 달러)

구분	2018년(e)	2023년(p)	연평균 성장률('18-'23)
솔루션	5,204.0	21,024.1	32.2%
서비스	3,016.0	14,128.1	36.2%

주) e: estimated, p: projected [출처] MarketsandMarkets(2018.9)

• 유형별로는 2018년 기준 네트워크 보안 시장이 38억 1,600만 달러 규모로 가장 큰 것으로 나타났으며, 클라우드 보안 시장이 2022년까지 연평균 39.1%의 성장세를 보여 가장 높은 증가세를 보일 전망

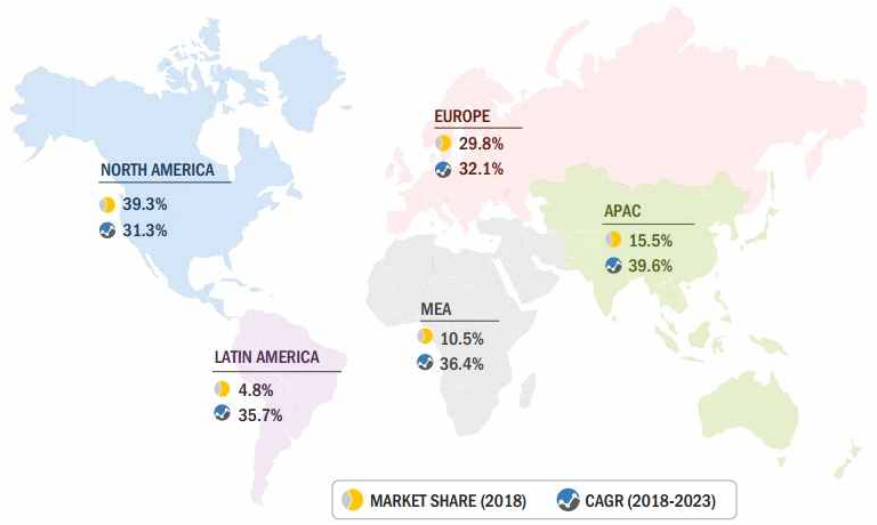
표 _ 전 세계 IoT 보안 시장 규모 및 성장 전망 (단위 : 백만 달러)

구분	2016년	2017년	2018년(e)	2023년(p)	연평균 성장률('18-'23)
네트워크	2,433.2	3,041.8	3,816.0	16,088.2	33.3%
엔드포인트	1,164.4	1,418.5	1,735.3	6,544.4	30.4%
애플리케이션	697.2	893.4	1,149.3	5,542.6	37.0%
클라우드	473.8	616.3	805.1	4,191.5	39.1%
기타	473.0	580.1	714.4	2,785.5	31.3%

[출처] MarketsandMarkets(2018.9)

• 권역별로는 2018년 기준 북미가 39.3%로 가장 큰 비중을 차지하나 2023년까지의 성장률은 아태지역이 39.6%의 연평균 성장률(CAGR)로 가장 빠른 성장을 보일 것으로 예상

그림 _ 전 세계 주요 권역별 IoT 보안 시장 비중 및 연평균 성장률



[출처] MarketsandMarkets(2018.9)

▶ **(인공지능 보안)** 2019년 시점 북미 시장이 전 세계의 40% 이상을 차지하여 글로벌 인공지능 보안 시장을 주도하고 있으며, 전 세계적으로 2026년경 382억 달러 이상의 규모에 이를 전망

• 전 세계 인공지능 보안 시장은 2019년 88억 90만 달러로 추산되는 가운데 매년 23.3%의 성장률을 기록하며 2026년 382억 2,740만 달러를 형성할 것으로 전망

표 _ 전 세계 인공지능 보안 시장 규모 및 성장 전망 (단위 : 백만 달러)

구분	2018년	2019년(e)	2020년(f)	2022년(f)	2024년(f)	2026년(f)	연평균 성장률('19-'26)
시장규모	5,783.6	8,800.9	11,542.2	18,872.5	28,059.4	38,227.4	23.3%

주) e: estimated, f: forecasteded

[출처] MarketsandMarkets(2019.4)

• 전 세계 인공지능 보안 시장은 유형별로 하드웨어, 소프트웨어 및 서비스로 구분할 수 있으며, 이 중 2019년 시점 소프트웨어가 59억 8,450만 달러로 전체 시장의 67.9%를 차지하며, 전체 시장을 주도

표 _ 전 세계 인공지능 보안 유형 별 시장 규모 및 성장 전망 (단위 : 백만 달러)

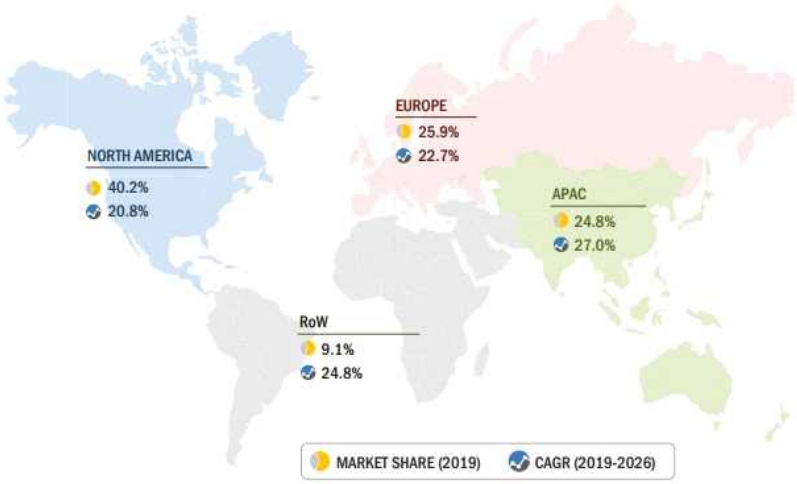
구분	2019년(e)	2026년(p)	연평균 성장률('19-'26)
하드웨어	2,641.3	10,492.7	21.8%
소프트웨어	5,984.5	27,080.8	24.1%
서비스	175.1	653.8	20.7%

주) e: estimated, p: projected

[출처] MarketsandMarkets(2019.4)

- 권역별로는 2019년 기준 북미가 40.2%로 가장 큰 비중을 차지하나 2026년까지의 성장률은 아태지역이 27.0%의 CAGR로 가장 빠른 성장을 보일 것으로 예상

그림 _ 전 세계 주요 권역별 인공지능 보안 시장 비중 및 연평균 성장률



[출처] MarketsandMarkets(2019.4)

물리보안 시장

▶ **(물리보안 일반)** 전 세계 물리보안 시장은 2018년 841억 5,000만 달러로, 2023년까지 연평균 7.3%로 성장하며 1,194억 5,000만 달러에 이를 전망

- 전 세계적으로 테러 활동의 증가가 물리보안 시장 성장의 동인으로 작용하고 있으며, 최근에는 클라우드 기반 물리보안 서비스가 새로운 시장을 창출 중

그림 _ 전 세계 물리보안 시장 규모 및 성장 전망



	2016	2017	2018(e)	2023(p)	CAGR (2018-2023)
물리 보안 시장	70.00	76.85	84.15	119.45	7.3%

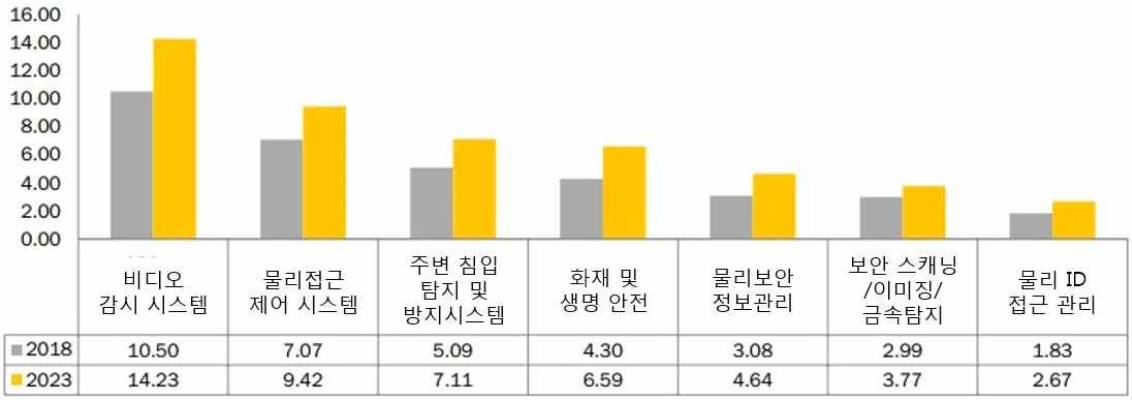
주) e: estimated, p: projected

[출처] MarketsandMarkets(2019.1)

▶ **(구성요소별 물리보안 시장)** 물리보안 시장은 시스템과 서비스로 구성되며 각각 전체 시장의 41%와 59%를 형성

- 물리보안 시스템 시장은 비디오 감시 시스템이 2018년 기준 105억 달러로 가장 큰 비중을 차지하며 이어서 물리접근 제어시스템(70억 7,000만 달러), 주변 침입 탐지 및 방지시스템(50억 9,000만 달러) 순
- 물리보안 서비스 시장은 보안 시스템 통합 서비스가 2018년 기준 256억 4,000만 달러로 가장 큰 비중을 차지하며 이어서 원격 모니터링 서비스(109억 3,000만 달러), 비디오 감시 SaaS(VSaaS, 50억 9,000만 달러), 접근 제어 SaaS(ACaaS, 49억 6,000만 달러) 순

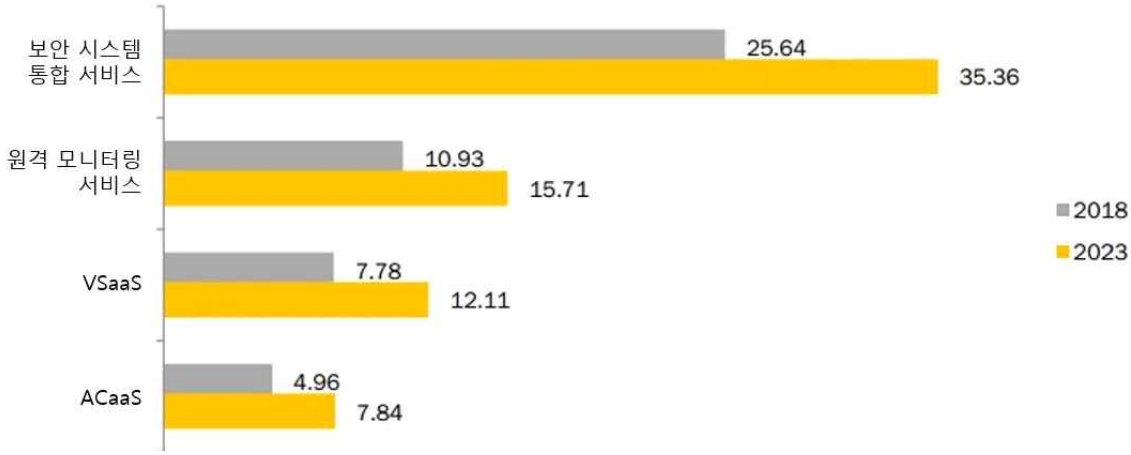
그림 _ 전 세계 물리보안 시스템 시장 규모 및 성장 전망 (단위 : 십억 달러)



	비디오 감시 시스템	물리접근 제어 시스템	주변 침입 탐지 및 방지시스템	화재 및 생명 안전	물리보안 정보관리	보안 스캐닝 /이미징/ 금속탐지	물리 ID 접근 관리
2018	10.50	7.07	5.09	4.30	3.08	2.99	1.83
2023	14.23	9.42	7.11	6.59	4.64	3.77	2.67

[출처] MarketsandMarkets(2019.1)

그림 _ 전 세계 물리보안 시장 규모 및 성장 전망 (단위 : 십억 달러)

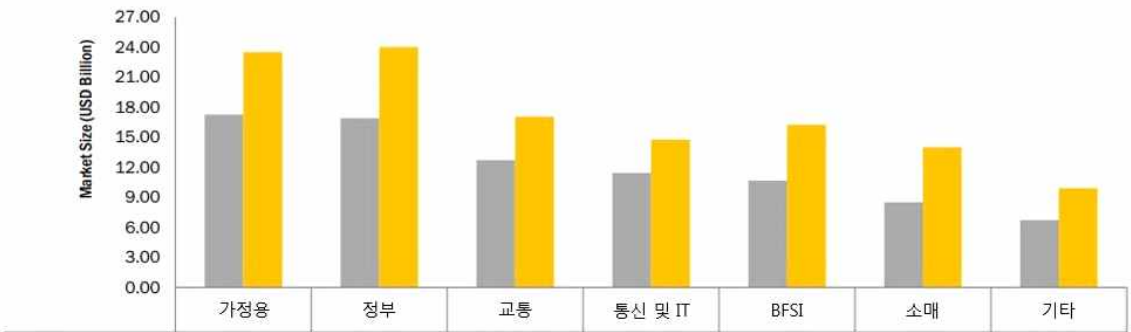


[출처] MarketsandMarkets(2019.1)

▶ **(산업별 물리보안 시장)** 물리보안 시장은 주요 산업별로 볼 때 가정용, 정부 및 교통 부문이 Top3 응용 분야를 형성

- 가정용 부문에서는 2018년 172억 7,000만 달러의 시장 규모를 달성한 것으로 집계되며 이어서 정부 부문이 168억 8,000만 달러, 교통 부문이 127억 달러 규모로 추정
- 세부 분야별 성장률 면에서는 2018-2023년 기간 동안 소매 부문이 10.5%로 가장 높은 성장이 기대되며, 은행·금융·보험·서비스(BFSI) 부문이 8.8%, 정부 부문이 7.3%의 성장이 관측

그림 _ 전 세계 물리보안 산업별 시장 규모 및 성장률 전망 (단위 : 십억 달러)



	가정용	정부	교통	통신 및 IT	BFSI	소매	기타
2018	17.27	16.88	12.70	11.42	10.66	8.51	6.72
2023	23.49	24.00	17.06	14.75	16.24	14.01	9.90
CAGR (2018-2023)	6.3%	7.3%	6.1%	5.3%	8.8%	10.5%	8.1%

[출처] MarketsandMarkets(2019.1)

2. 선진국 시장

선진국 시장 개요

▶ 미국과 일본, 유럽은 한국과 교역이 매우 활발한 지역으로 세계 경제의 핵심 축을 이루고 있음

- 미국의 GDP는 20조 5,130억 달러, 1인당 GDP 역시 62,517달러(2018년)로 가장 높은 수준이며, 영국은 프랑스, 독일과 함께 유럽의 빅 3로서 이들 국가의 경제규모 역시 세계 최상위권을 기록하고 있음
- 미국은 우리나라에게 있어서 중국에 이은 최대 교역국으로 우리나라는 미국과의 교역에서 높은 흑자를 기록하고 있음
- 일본, 영국도 우리나라의 주요 교역국이나 한국은 일본을 제외하고는 대체로 흑자를 유지함

표 _ 선진시장 주요국의 한국과의 관계(2018년 기준)

항목	수교일	우리나라 수출규모 (US$ 억)	우리나라 수입규모 (US$ 억)	우리나라의 주요수출품	우리나라의 주요수입품
미국	1948. 8.	727	589	승용차, 자동차부품, 집적회로반도체, 무선전화기, 제트유 등	원유, 집적회로반도체, LPG, 가축육류, 반도체 제조용장비, 천연가스
일본	1965. 12.	305	546	나프타, 기타정밀화학원료, 제트유 및 등유 등	반도체제조용장비, 집적회로반도체, 기초유분, 고철
영국	1884. 4.	64	68	승용차, 선박, 제트유 및 등유, 항공기부품, 자동차부품 등	승용차, 의약품, 주류, 원동기, 원유, 계측기, 합성수지 등

[출처] Kotra-국가정보(2019)

▶ 국제전기통신연합(ITU)은 인터넷 사용, 유무선 초고속 인터넷 가입자 등과 ICT 스킬(문맹률, 고등교육진학률) 등 측정항목에 가중치를 부여하여 종합적인 ICT 발전지수(ICT development Index, IDI)를 측정하여 국가 간 비교를 하고 있음

- 2017년 글로벌 ICT 발전지수(ICT Development Index, IDI)에 따르면 대부분의 북미·유럽 지역 국가들의 ICT 발전지수 순위는 세계 상위권으로 영국의 IDI는 8.65점으로 세계 5위, 일본은 10위를 기록

표 _ 선진시장 주요국 ICT 발전지수(IDI)

국가	IDI(2017년)		접근성(access)		이용성(use)		스킬(skill)	
	순위	지수	순위	지수	순위	지수	순위	지수
미국	16	8.18	17	8.27	20	7.67	3	9.05
일본	10	8.43	9	8.80	11	8.15	30	8.22
영국	5	8.65	4	9.15	7	8.38	33	8.17
한국	2	8.85	7	8.85	4	8.71	2	9.15

[출처] ITU, ICT Development Index 2017, https://www.itu.int/net4/ITU-D/idi/2017/index.html

▶ 국제전기통신연합(ITU)은 법적, 기술적, 조직적 대응 및 역량강화, 국제협력 등 5개 부문의 지수를 종합하여 글로벌 사이버보안지수(Global Cybersecurity Index, GCI)를 측정하여 국가 간 비교를 함

- 2018년 글로벌 사이버보안지수(GCI)에 따르면, 대부분의 유럽·북미 지역 국가들의 글로벌 사이버보안지수 순위는 세계 상위권으로 영국의 GCI는 0.931점으로 세계 1위, 미국은 2위, 일본은 14위를 기록함

표 _ 선진시장 주요국 글로벌 사이버보안지수(GCI) 주요 내용[2]

국가	GCI(2018년)		법적(Legal)	기술적 (Technical)	조직적 (Oranizational)	역량강화 (Capacity building)	국제협력 (Cooperation)
	순위	지수	지수	지수	지수	지수	지수
영국	1	0.931	0.200	0.191	0.200	0.189	0.151
미국	2	0.926	0.200	0.184	0.200	0.191	0.151
일본	14	0.880	N/A	N/A	N/A	N/A	N/A
한국	15	0.873	N/A	N/A	N/A	N/A	N/A

[출처] ITU, Global Cybersecurity Index(GCI) 2018,

▶ 유엔무역개발기구(UNCTAD)는 금융기관 또는 모바일 머니 서비스 제공업체의 계정 소유권, 인터넷을 사용하는 개인, 우편물 신뢰성 지수, 안전한 인터넷 서버 등 4개의 지수를 종합하여 B2C 전자상거래 지수(B2C e-Commerce Index)를 측정하여 국가 간 비교를 함

2 GCI 2018에서는 권역별 상위 3개국에 대해서만 평가항목별 점수를 제공해, 3위권 밖인 일본과 한국에 대해서는 평가항목 점수를 공개하지 않음

• UNCTAD의 2019년 B2C 전자상거래 지수에 따르면, 대부분의 유럽·북미 지역 국가들의 B2C 전자상거래 지수 순위는 세계 상위권으로 영국의 B2C 전자상거래지수는 94.4점으로 세계 5위, 미국은 13위, 일본은 21위를 기록함

표 _ 선진시장 주요국 B2C 전자상거래 지수

국가	전자상거래지수 (2019)		인터넷 사용하는 개인	계정 소유권	안전한 인터넷 서버	우편물 신뢰성 점수
	순위	지수	지수	지수	지수	지수
미국	13	91.3	87	93	95	90
일본	21	87.6	85	98	81	86
영국	5	94.4	95	96	88	98
한국	19	89.4	96	95	67	99

[출처] UNCTAD, B2C e-Commerce Index 2019, https://unctad.org/en/PublicationsLibrary/tn_unctad_ict4d14_en.pdf

▶ 글로벌 시장조사기관인 MarketsandMarkets가 발표한 물리보안 시장에 대한 보고서에서는 물리적 보안 시장 영역을 시스템 분야와 서비스 분야를 포함하여 시장 규모를 발표

• 시스템 분야에는 물리적 접근 제어 시스템, 비디오 감시 시스템, 경계 침입 탐지 및 예방, 물리적 보안 정보 관리, 물리적 신원 및 접근 관리, 보안 검색, 이미징 및 금속 탐지, 화재 및 생명 안전에 대한 시스템이 포함
• 서비스 분야에는 서비스 분야에서 서비스로서의 접근 제어, 서비스로서의 비디오 감시, 원격 모니터링 서비스, 보안 시스템 통합 서비스를 포함
• 물리보안 시장규모는 2018년 미국의 경우 260억 달러 규모로 연평균 성장률(2018-2023) 6.2%로 성장할 것으로 전망하며, 영국은 40억 달러 규모, 일본은 26억 8,000만 달러 규모임

표 _ 선진시장 주요국 물리보안 시장규모 (단위 : 십억 달러)

국가	2016	2017	2018e	2023p	연평균성장률 (2018-2023)
미국	22.40	24.32	26.06	35.23	6.2%
일본	1.96	2.30	2.68	4.46	10.8%
영국	3.50	3.74	4.00	5.24	5.6%

[출처] MarketsandMarkets, Physical Security Market-Global Forecast To 2023, 2019

▶ 글로벌 시장조사기관인 MarketsandMarkets이 발표한 정보보안시장 보고서에서는 선진시장 중 미국이 75억 2,400만 달러로 압도적인 비중을 차지하고 있으며, 일본이 연평균 15.6%의 성장률을 보일 것으로 예상됨에 따라 해당 시장에 대한 주목이 필요

표 _ 선진시장 주요국 정보보안 시장규모 (단위 : 십억 달러)

국가	2016	2017	2018e	2023p	연평균성장률 (2018-2023)
미국	44.33	48.5	52.55	75.24	7.40%
일본	3.9	4.62	5.39	11.12	15.60%
영국	10.39	11.23	12.02	16.17	6.10%

[출처] MarketsandMarkets, Physical Security Market-Global Forecast To 2023, 2019

▶ 글로벌 시장조사기관인 MarketsandMarkets이 발표한 서비스형 보안시장에 대한 보고서에서는 서비스형 보안은 클라우드 기반 모델이며, 보안 공급 업체는 클라우드 및 사내 환경에서 엔터프라이즈 네트워크, 애플리케이션 및 데이터를 보호하고 유지 관리함

- 서비스형 보안 시장규모는 2018년 미국의 경우 23억 3,760만 달러 규모로 연평균 성장률(2018-2023) 14.2%로 성장할 것으로 전망하며, 영국은 6억 3,200만 달러 규모임

표 _ 선진시장 주요국 서비스형 보안 시장규모 (단위 : 백만 달러)

국가	2016	2017	2018e	2023p	연평균성장률 (2018-2023)
미국	1,667.1	1,998.6	2,337.6	4,553.0	14.2%
영국	451.1	537.5	632.0	1,224.6	14.1%

[출처] MarketsandMarkets, Security As a Service Market-Global Forecast To 2023, 2019

▶ 글로벌 시장조사기관인 MarketsandMarkets이 발표한 IoT 보안시장에 대한 보고서에서는 IoT 보안 시장은 연결된 장치의 네트워크를 보호하고 연결된 장치의 위협 및 사이버 공격으로 인한 손실을 최소화하기 위해 제공되는 솔루션 및 서비스가 포함됨

- IoT 보안 시장규모는 2018년 미국의 경우 22억 5,720만 달러 규모로 연평균 성장률(2018-2023) 31.1%로 성장할 것으로 전망하며, 영국은 9억 7천만 달러 규모임

표 _ 선진시장 주요국 IoT 보안 시장규모 (단위 : 백만 달러)

국가	2016	2017	2018e	2023p	연평균성장률 (2018-2023)
미국	1, 485.2	1,828.2	2,257.2	8,752.7	31.1%
영국	639.7	786.0	970.0	3,807.4	31.5%

주) e: estimated, p: projected [출처] MarketsandMarkets, IoT Security Market-Global Forecast To 2023, 2019

▶ 선진국 시장의 주요 진출 전략은 다음과 같음

- 정부 및 민간 등 다양한 분야에서 레퍼런스가 시급한 상황으로, 스타트업 맞춤형 육성 프로그램, 조달시장 진출 방안 마련 등의 진출 전략이 필요함
- 시장 진출을 위한 협력 및 신규 서비스 분야에 공동 R&D 등 필요

가. 미국

'18년 GDP(십억달러)	20,494.10
'18년 인구수(천명)	327,170

■ ITU 글로벌 사이버보안 지수(Global Cybersecurity Index, GCI)

· 미국의 사이버보안 지수는 한국 대비 높은 수준으로 선도 그룹에 속함

국가명	2018		2017		전년대비 증감	
	지수	순위	지수	순위	지수	순위
미국	0.926	2	0.919	2	+0.07	-
대한민국	0.873	15	0.782	13	+0.091	-2

■ ICT 관련 주요 지수

· 미국의 전반적인 ICT 발전 수준은 전 세계 5% 이내의 최상위권을 유지하고 있음

지표명	미국		한국	
	점수	순위	점수	순위
IMD 국가경쟁력지수(2019)	-	3	-	28
IMD 디지털경쟁력지수(2019)	-	1	-	10
UNCTAD 전자상거래지수(2019)	91.3	5	89.4	19
ITU 글로벌 사이버보안 지수(GCI 2018)	0.926	2	0.873	15
UN 전자정부 지수(2018)	0.877	11	0.901	3

■ ICT 관련 주요 통계 (ITU, 2018년 말 기준)

· 미국의 유선·이동통신(ICT) 이용률 및 보급률은 세계 최고 수준으로 우리나라와 비슷함

항목	미국		한국	
	가입자수(천 명)	보급률(%)	가입자수(천 명)	보급률(%)
유선전화	116,724	35.68	25,907	50.63
유선브로드밴드	116,467	35.61	21,286	41.60
이동통신	404,577	123.69	66,356	129.67
인터넷 이용률	-		95.90%	

정보보호 산업 개요

1) 보안 환경

정보보안 환경

▶ ITU 2018 'Global Cybersecurity Index(GCI)'에 따르면 미국의 사이버보안 지수는 0.926으로 영국(0.931)에 이어 2위를 기록했으며, 미주 권역에서는 2017년에 이어 연속적으로 1위를 기록

- 해당 지수는 법적·기술적·조직적 대응 및 역량 강화, 국제협력 등 5개 부문의 지수를 종합한 것으로, 미국은 법적 및 조직적 대응의 2가지 측면에서 0.200의 최대 점수를 기록 (조직 측면에서 캐나다와 동점 기록)
- 특히, 법적 부문에서 가장 높은 점수와 순위를 동시에 차지하였으며, 사이버 범죄를 다루기 위한 실질적이고 광범위한 법적 조항을 보유

▶ 사이버 공격은 미국에서 가장 빠르게 성장하는 범죄로서 규모, 정교함 및 비용이 지속적으로 증가하는 추세임

- 2018년 미국 기업들이 경험한 사이버 공격은 ▲피싱(37%) ▲네트워크 침입(30%) ▲부주의한 공개(12%) ▲도난/손실된 장치 또는 기록(10%) ▲시스템 구성 오류(4%) 임
- Juniper에 의하면 사이버 범죄자들은 2023년에 약 330억 건의 정보를 탈취할 것이며, 전 세계 데이터 유출의 절반 이상이 미국에서 발생할 것으로 예상
- 미국은 표적 공격(Targetted Attack) 대상 1위(38%)로서 일부 공격은 개인 그룹에 의한 것이지만 국가가 지원하는 경우도 존재

물리보안 환경

▶ 시장조사업체인 MarketandMarkets과 Scalar Market Research 두 보고서에 따르면 전 세계적으로 발생하는 테러의 증가가 물리보안 시장의 성장을 이끄는 주요한 원인 중 하나임

- 기업 및 조직, 개인은 자산과 생명을 보호하기 위한 노력으로 최첨단 물리보안 시스템을 도입하는

추세

- 특히 사물인터넷(IoT) 기술이 물리보안 시장의 성장에 크게 기여할 것이라고 전망
- 출입통제·영상감시·재난예방 등의 물리보안 시장이 최근 테러 증가와 함께 사물인터넷(IoT) 기술과 융합되며 성장세를 기록
- 전 세계 지역 중 물리보안 시장은 현재까지 미국시장이 가장 크지만, 아태지역이 가장 빠른 속도로 성장해 미국시장과 함께 시장을 주도할 것으로 예상

▶ 미국 내 테러와 총기난사 등에 따른 경각심이 높아지면서 물리보안 제품에 대한 수요가 지속적으로 증가 추세

- 학교, 병원, 쇼핑몰, 오피스 등 상업시설에 첨단 보안시스템이 설치되고 포럼, 박람회 등 국제행사도 늘어나면서 다양한 보안시스템 구축
- 물리보안시장 사업자들은 IT기업과 업무제휴를 맺고 '스마트 시큐리티' 사업을 확대 중임

2) 인터넷 및 통신 환경

▶ 유선통신

- 2018년 5월 Leichtman Research Group의 분석에 따르면, 유선통신서비스(telephone) 가입자 수는 전년 동기 대비 325,000명 감소하였으며, 인터넷서비스는 전년 동기 대비 256,000명 증가한 것으로 조사
- 2016년 미국 유선 통신산업 규모는 1598억 달러로 전년대비 2.7% 감소했으며, 2021년까지 연 1.4% 감소 전망
- 유선 통신산업은 67.8%를 차지하는 가정, 개인 사용자와 32.2%를 차지하는 상업, 정부기관 사용자로 크게 나뉨
- 유선 통신산업의 하락의 주요 원인은 더 많은 가정에서 무선전화만 이용하는 경향이 증가하면서 유선전화 서비스에 대한 필요성의 감소에서 비롯되고 있으며, 그에 따른 유선통신시장과 무선통신 시장규모의 격차는 점점 벌어지고 있음

그림 _ 미국 인터넷 사용자 수와 보급률 (단위: 백만 명)

연도	인터넷 사용자	인터넷 보급율
2010	241	77%
2011	245	78%
2012	251	80%
2013	259	83%
2014	269	85%
2015	280	87%
2016	286	89%
2017	294	92%
2018	302	94%

[출처] BuddeComm based on internetlivestats data

▶ 브로드밴드

- 높은 브로드밴드 보급률에 따라 성장률이 감소하고 있으나, 가입자 수는 향후 5년 동안 지속적으로 증가할 것으로 예상
- 사업자 시장 점유율 측면에서 Comcast의 가입자는 시장의 약 20%를 점유하고 있고, AT&T, Charter Communications, Verizon 및 CenturyLink가 그 뒤를 따르고 있으며, 이들은 시장의 약 70%를 보유하고 있음

그림 _미국 브로드밴드 가입자 수와 보급률 (단위: 백만 명)

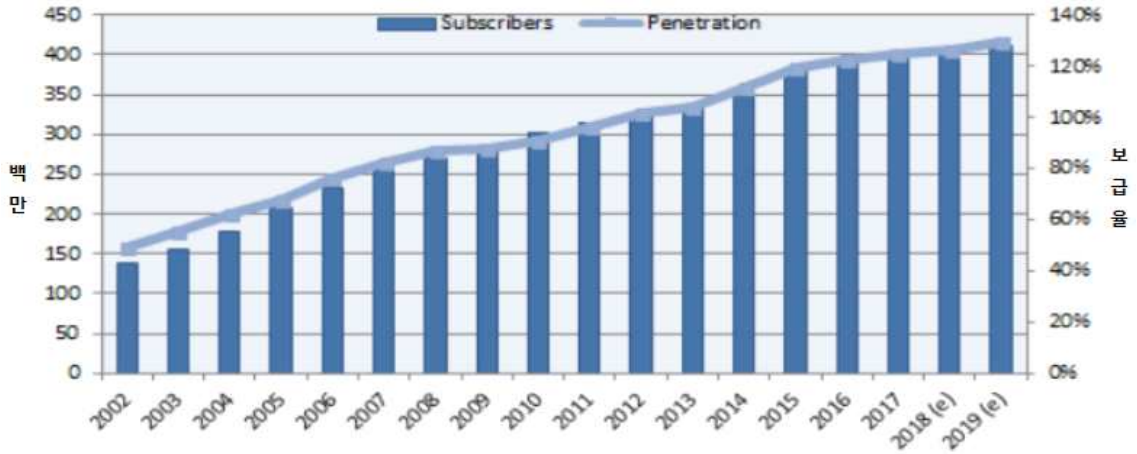


[출처] BuddeComm based on ITU and FCC data

▶ 이동통신

- 미국 모바일 부문은 최근 몇 년간 상당한 성장을 보이며 2018년 말까지 약 127%의 보급률에 도달
- 가입자 수의 꾸준한 증가와 모바일 트래픽의 상당한 증가에도 불구하고, 시장이 가격에 대한 경쟁에 반응함에 따라 2016년과 2017년 모두 모바일 산업 매출이 감소
- 향후 몇 년 동안 가입자 수는 계속 증가할 것으로 예상되나, 보급률이 높아짐에 따라 증가 속도는 느려질 것으로 전망
- 2019년 부터의 5G 기반 서비스 출시는 수백만 대의 장치를 연결하고 모바일 데이터 사용의 급속한 증가를 가져올 것으로 예상

그림 _미국 이동통신 가입자 수 및 보급률 (단위: 백만 명)



[출처] BuddeComm based on CTIA and industry data

▶ 5G

- Statista에 따르면, 미국 내에서의 5G 상용화는 2020년에서 2021년에 걸쳐 이루어질 것으로 전망
- 2020년에는 북미 지역에 약 1,800만 명의 사용자 수를 확보하고, 2021년에는 약 6,300만 명의 사용자 수를 확보할 것으로 예상
- 2019년 기준 향후 5년간의 사용자 증가 추세를 예견한 결과에 따르면 5G 사용자의 증가율은 매우 높은 편이며, 이는 5G 관련 산업 또한 미국 내에서 크게 성장할 것으로 전망함
- PwC 보고서에 따르면, 5G 네트워크가 기존의 4G/LTE보다 훨씬 빠른 속도의 서비스를 제공할 수 있음에도, 소비자들은 즉시 5G 기기로 바꾸어 5G 네트워크를 사용하고자 하는 경향은 아님
- 기기 업그레이드를 할 수 있을 때까지는 기존 네트워크 서비스를 사용하고자 함에 따라, 5G 서비스의 급격한 확산은 단기간 내에는 어려울 것으로 전망

그림 _ 2019-2024 세계 권역별 모바일 5G 이용자수 성장 예측 (단위; 백만명)



[출처] www.statista.com

정보보호 시장 현황

1) 시장 규모

시장 개요

▶ Ernst & Young (2017-18)의 글로벌 설문 조사에 따르면, 기업의 87%가 사이버 보안 예산을 50% 이상 증가할 계획을 가지고 있으며 향후 기업들은 지속적으로 사이버 보안에 많은 비용을 지출할 전망

- 또 다른 조사에서는, 조직의 78%가 2018년 사이버 보안 예산을 늘릴 계획이라고 응답하였으며, 미국의 비율은 86%로 더 높은 수치를 보이고 있음
- JP Morgan Chase는 연간 사이버 보안 예산을 2억 5,000만 달러에서 5억 달러로 두 배로 늘려 책정하였으며, Bank of America는 사이버 보안 관련 예산은 무제한임을 밝힘

▶ 미국 연방 사이버 보안 시장은 인프라 강화 부문이 12%의 CAGR로 꾸준히 성장하면서 200억 달러 규모에서 안정적으로 유지될 것으로 예상

- 미국 연방 정부의 연간 사이버 보안 지출은 전 세계 대부분 국가의 사이버 보안 지출 전체보다 크며, 단기 및 장기 연방 사이버 보안 투자가 추진될 전망
- 컴퓨터 상호 연결성의 급격한 확장과 정부 네트워크의 데이터의 기하 급수적인 증가로 인해, 사이버 공격의 수가 점점 늘어날 것으로 예측
- 정보기술에 높은 의존성을 가진 미국은, ▲기존 사이버 보안 접근 방식의 변화 ▲기술의 발전 ▲새로운 기술 출현 등으로 인해 사이버 보안 비용이 증가 추세

▶ 미국 물리보안 산업시장은 사용자층을 기준으로 주거용과 비주거용으로 분류되며, 전체 시장 대비 각각 1/3과 2/3 정도의 비율로 구성되어 있음.

- 비 주거용 사용자는 상업용 빌딩과 정부기관 등이 주를 이루고 있음
- 미국 물리보안 시장은 전 세계 시장의 18%를 차지하며 단일 규모 세계 최대로서, 산업제품 분야별 매출 기준으로 침입 탐지 부문과 비디오 감시 부문의 두 시장이 전체의 1/2을 차지하고 있음
- ▲범죄·테러에 대한 관심 증가 ▲기존 제품 업그레이드 수요 증가 ▲가격 인하에 따른 수요 저변 확대 등의 요인이 시장 성장을 견인

시장 규모 및 전망

▶ 2019 회계연도 예산은 사이버 보안 관련 활동에 150억 달러를 할당하며, 이는 전년도에 비해 4% 증가한 수치임

- 국방부는 약 85억 달러를 투자하여 가장 많은 자금을 조달하며, 국토 안보부는 약 17억 달러를 조달할 예정
- 미국 연방 정부의 연간 사이버 보안 지출은 전 세계 대부분의 국가의 사이버 보안 지출 전체보다 크다고 할 수 있음

▶ 글로벌 시장조사기관인 MarketandMarkets에 따르면, 글로벌 보안시장 규모는 2016년 2,475억 달러에서 2021년 4,565억 달러로 약 2배 가량 증가할 전망

- 2017년 미국 보안시장은 317억 달러 규모로, 전 세계 시장의 약 18% 이상을 차지하며 꾸준히 증가할 것으로 예상됨

▶ 스마트 홈 모니터링 및 보안 장치의 출하량은 2019년 말까지 1,132만대로 증가하여 2018년 8,890만 대보다 27.3% 증가할 것이며, 2023년 말까지 총 출하량은 2,495 만 대에 이를 것으로 전망 (CAGR 22.9% 예측)

- 스마트 홈 모니터링 및 보안 장치의 출하량은 2019년에 총 1억 2,330만 대에 이를 것으로, 2023년에는 CAGR 22.9%로 2억 4,950만 대로 증가 예상
- 홈 모니터링 및 보안 관련 응용 프로그램은 다른 대부분의 홈 응용 프로그램보다 지속적으로 더 많은 관심을 보이고 있음
- ▲DIY(Do-it-Yourself) 장치의 유입 ▲시간이 지남에 따른 가격 인하 ▲지능형 사람 및 음성 인식 서비스 등의 요인이 향후 수요를 주도할 전망

▶ 홈 모니터링 보안과 관련된 장치 유형별 예측 출하량은 다음과 같음

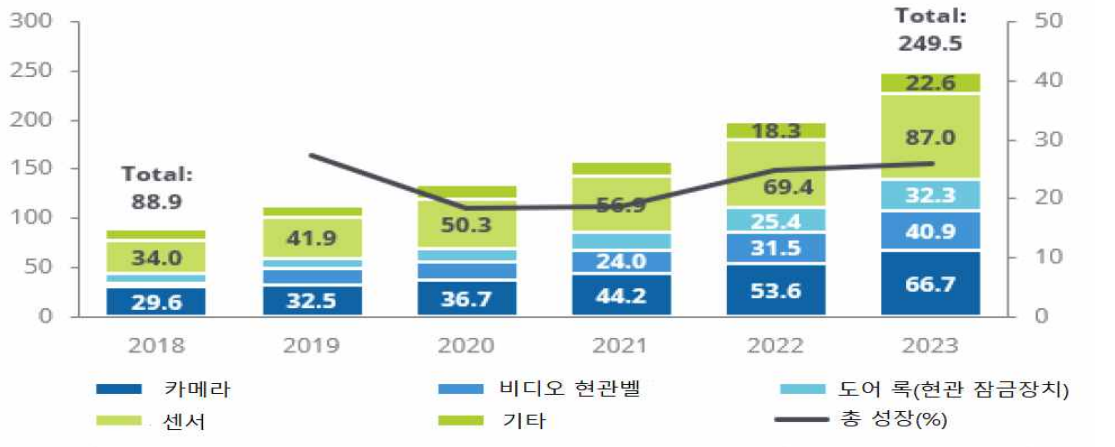
- 카메라 출하량은 2018년 2960만 대에서 2019년 3,250 만대로 증가하여 전년 대비 9.8% 성장할 것이며, CAGR 17.7%로 2023년에는 6670만대를 기록할 것으로 예측
- 카메라 시장은 ▲소비자 수요 증가 ▲가격 하락 ▲공급 업체 경쟁으로 인해 성장될 것이나, 개인 정보 보호에 대한 우려로 인해 시장의 성장이 제한될 것으로 예상
- 비디오 초인종 출하량은 2018년 470만 대에서 2019년 1,640만대로 전년 대비 245.4% 증가했으며,

CAGR 53.9%로 2023년 4억 9,900만 대의 증가 전망

- 비디오 초인종 시장은 ▲신규 공급 업체의 시장 진입 ▲장치에 대한 소비자 인식 증가 ▲손쉬운 설치 및 사용성에 따라 성장이 좌우
- 도어락 출하량은 2018년 900만대에서 2019년 970 만대로 증가하여 전년 대비 7.4% 증가 했으며, CAGR 29.1%로 2023년에 3,230만대로 증가할 전망
- 도어락 시장은 성장은 새로운 잠금 장치 설치 또는 기존 잠금 장치 개조와 관련한 복잡성 때문에 DIY 방식이 아닌 관리 서비스 제공업체가 주도
- 센서 출하량은 2018년 3,400만 대에서 2019년 4,410만 대로 증가하여 전년 대비 23.4% 증가했으며, CAGR 20.7%로 2023년에 8,700만대로 증가 예상
- 센서 시장은 DIY 제품의 유입과 저렴한 가격이 이 시장의 성장을 주도하고 있으며, 관리 서비스 제공업체는 번들링, 할인 및 설치 서비스를 통해 성장을 견인
- 시스템 허브 및 패널 등을 포함한 기타 장치 출하량은 2018년 1,160만 대에서 2019년 1,270만 대로서 전년 대비 9.7% 증가했으며, CAGR 14.3%로 2023년 2,260만 대로 증가 전망

그림 _ 미국 홈 모니터링 및 보안 출하량 현황

(단위: 백만 대, %)



[출처] IDC, 2019

▶ 지문, 홍채, 망막, 얼굴인식 등 보안 생체인식 시장은 CAGR 7.5%씩 성장하고 있으며, 국토안보부와 방위청 등 공공기관에서의 생체인식 시스템 도입과 생체인식 신분관리소 구축을 통해 투자 증가와 업계 수익이 증가함에 따라 2021년 94억 달러로 확대될 것으로 전망

- 제품별로는 지문 인식이 생체인식 스캔업계에서 50%을 차지하고 있으며, 체육관, 도서관 등에서 카드 대신 지문을 사용하고 있으나 망막 인식의 정확성과 용이성이 높아져 점유율이 감소할 전망

- 얼굴인식은 주로 정부에서 사용했으나 보안카메라, 얼굴사진을 통한 확인기술의 발달로 범죄수사에 많이 사용할 것으로 예상
- 3D 안면인식 등 혁신기술은 정확도가 낮은 것이 단점으로 지적되고 있으며, 손, 정맥, 음성 등을 활용한 생체인식의 시장 증가도 예상

2) 분야별 현황

정보보안 제품 및 서비스 시장

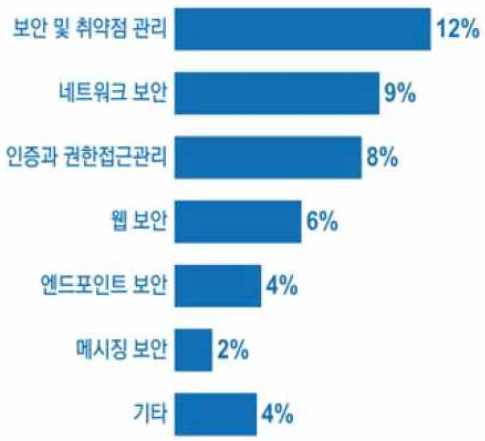
▶ 글로벌 사이버 보안 제품(서비스 시장 제외) 규모는 2016년 기준 약 330~360억 달러 규모로 추산되며, CAGR 6~7%의 성장을 지속할 전망

- IDC 따르면, 글로벌 '엔트 포인트 보안' 시장은 점차로 감소하는 반면, ▲보안 및 취약점 관리 ▲네트워크 보안 ▲인증 및 권한접근관리 시장은 수요가 증가하는 추세임

그림 _엔드 포인트 보안 글로벌 시장 전망



그림 _세부 시장별 연평균 성장률(CAGR)



[출처] Gartner, IDC, 2017

▶ 미국 보안 서비스 시장은 2023년에 286억 달러에 이를 것이며, 예측 기간 동안 연평균 8.2% 성장할 것으로 전망

- IT 컨설팅 및 시스템 통합은 예측 기간 동안 3.3%의 CAGR로 꾸준한 성장을 지속하여 2023년에는 110억 달러에 이를 것으로 예상되며, 지속적인 APAC 지역의 구축 및 신기술 확보에 따라 성장은 가속화될 것임
- 관리 보안 서비스 부문은 2023년에 169억 달러에 이를 것이며 예측 기간 동안 연평균 12.4%로 꾸준히 성장할 것으로 예상
- 교육 및 훈련 부문은 2023년에 89억 달러에 이를 것이며 예측 기간 동안 연평균 7.3% 성장할 것으로 예상

표 _ 분야별 미국의 IT 보안 서비스 시장 규모 및 전망(2017년~2023년)

(단위: 백만 달러)

분야	2017	2018	2019	2020	2021	2022	2023	2017–2023 CAGR (%)
IT consulting	3,767.3	3,922.3	4,132.1	4,364.7	4,586.2	4,821.6	4,821.6	5.2
Systems inte-gration	5,232.6	5,427.2	5,469.7	5,493.3	5,503.3	5,683.6	5,911.0	1.7
Managed sec-urity services	8,271.5	9,430.2	10,733.1	12,153.7	13,660.9	15,221.8	16,896.2	12.4
Education and training	582.2	623.9	667.8	717.3	771.9	829.0	887.1	7.3
Total	**17,853.7**	**19,403.6**	**21,002.8**	**22,729.0**	**24,522.3**	**26,556.0**	**28,756.8**	**8.2**

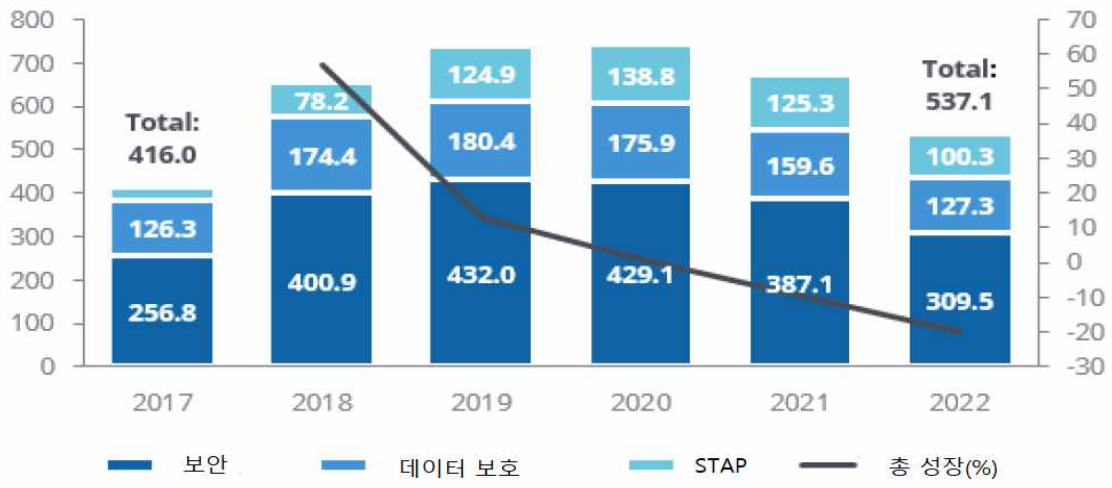
[출처] IDC, 2019.3

▶ 유럽연합(EU)의 일반 개인정보보호법(GDPR)이 미국 보안 제품 시장에 미치는 영향을 분석한 결과, 미국에서 EU의 GDPR 관련하여 시장이 형성되어 2017년에 4억 6,400만 달러가 창출되었으며, 2017-2022년 동안 CAGR 5.2%로 2022년에는 5억 5,700만 달러로 성장할 것으로 예상

- GDPR이 미국에 미치는 영향은 예상한 것만큼 크지 않을 수 있으며, 현재 미국 기업은 이미 GDPR을 준수하는데 필요한 솔루션을 구매하여 사용하고 있음
- 기업은 GDPR 위반 시 전 세계 매출의 4%를 과징금으로 부과받는 등의 행정처분으로 인해, 개인정보 보호 준수를 위한 관련 소프트웨어 시스템 활용 필요성 인식
- GDPR은 미국 시장 성장을 크게 이끌지는 못할 것으로 추측되나, 관련 소프트웨어 및 서비스 획득에 필요한 새로운 내부 프로세스를 개발해야 함

그림 _ 미국 GDPR 보안 제품 시장 현황

(단위: %)



* STAP: Specialized Threat Analysis and Protection

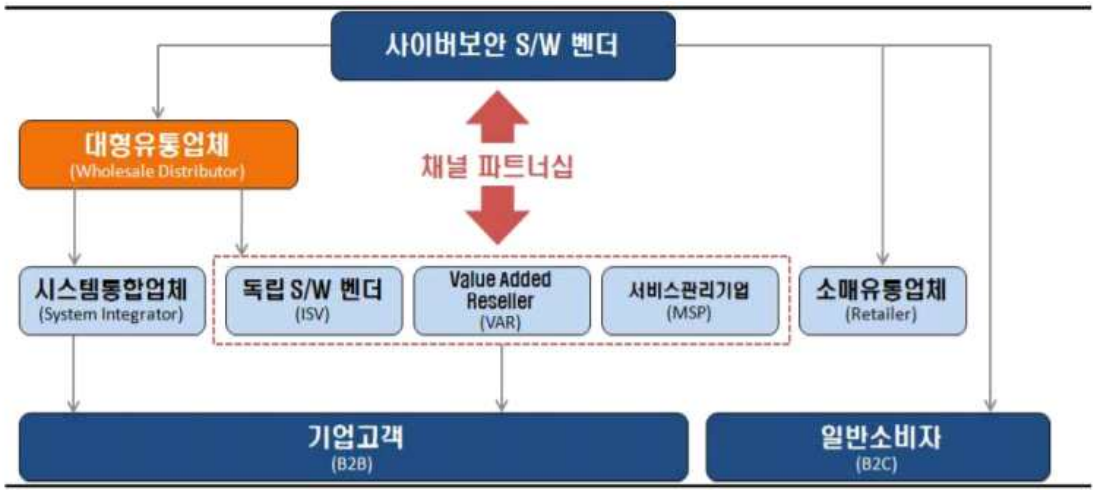
[출처] IDC, 2018

정보보안 제품 및 서비스 유통

▶ 미국 내 사이버보안 유통구조는 크게 벤더가 직접 온라인 등을 통해 소비자에게 판매하는 직접 판매 방식과 전문유통업체를 통한 간접 판매 방식으로 구분할 수 있음

- 일반 소비자를 대상으로 하는 경우, 소매 유통업체 및 온라인 등을 통한 벤더의 직접 판매 방식이 주요한 유통 경로
- 일반 소비자 대상의 소매 시장의 경우, 브랜드와 성능 이외에도 가격, 활용 용이성 및 소프트웨어의 업데이트 빈도 등이 경쟁력에 중요한 영향을 미치는 요소로 작용
- 전문유통업체를 통한 간접 판매 방식의 경우, Ingram Micro와 같은 대형유통업체를 경유하는 방식이 전체 유통의 70%를 차지
- 일반적으로 정부, 금융, 통신, 국방 분야의 대규모 프로젝트 경우는 시스템통합업체(SI)를 통한 방식이 보편적
- 대형벤더들의 경우 독립소프트웨어 벤더(Independent Software Vender, ISV), VAR(Value Added Reseller), 또는 서비스 관리기업(Managed Service Provider, MSP)등과 '채널 파트너십'을 체결하여 제품을 유통하는 방식이 급격히 증가하고 있음
- 미국 사이버보안 소프트웨어 부문의 주요 유통 구조 및 유통 업체는 다음과 같음

그림 _ 미국 사이버보안 스프트웨어 유통 구조



[출처] STRABASE / KOTRA 워싱턴무역관 분석 재구성

표 _ 미국의 대표적인 IT 및 소프트웨어 전문 도매 유통업체 현황

업체명	개요
Ingram Micro, Inc	세계 1위의 IT 컴퓨터 제품/서비스 공급자이자 시스템통합 솔루션, 마케팅, 유통 전문기업
Avnet, Inc.	미국을 본사로 둔 다국적기업으로 전세계의 전자기기, 부품, 데이터저장 장치 등 광범위한 IT생태계를 구축하고 있음
Tech Data Corp.	수백개 이상의 IT제품/솔루션을 전세계 십만개 이상의 IT 소매기업에게 공급
SYNNEX Information Technologies	세계수준의 IT전문유통업체로 VAR, SI, OEM 업체 등에 IT 하드웨어, 소프트웨어를 공급
Arrow Electronics, Inc	전세계 13,000개 이상의 리셀러와 협력을 통해 IT전자기기, 부품, 보안솔루션 등 제공
ScanSource, Inc	Automatic identification and data capture (AIDC) and point-of-sale (POS) 기술에 주력하여 전세계 리셀러에 공급
MA Labs	모델, 발전장비, 디지털장비, 보안장비, 네트워크 솔루션 등 전문 유통업체
D&H DISTRIBUTING	미국과 캐나다에 IT, 전자기기, 전자부품관련 도매유통업체로 주로 중소규모의 리셀러에 유통을 담당

[출처] KOTRA Global Market Report

물리보안 제품 및 서비스 시장

▶ 물리보안 시스템 서비스 시장은, 2018년 2,556억 달러에서 2019년 2,726억 달러로 CAGR 6.6%의 성장을 전망

- 이 시장은 ▲도난 및 화재 경보와 같은 보안 경보 시스템 판매, 설치, 수리 또는 모니터링하는 서비스와 이와 주로 관련된 시설 ▲전자 보안 경보 시스템의 원격 모니터링 서비스를 의미
- 2016년 2,225억 달러에서 CAGR 6.7%로 2020년 2,888억 달러로 성장할 것으로 예측
- 2019년 서비스 시장별로는, ▲보안 시스템 서비스 (61%) ▲침입 탐지 관리 및 모니터링 (30%) ▲화재 감지 및 모니터링 (2%) ▲보호 장비 및 안전 (4%) ▲폐쇄 감시 시스템 (3%) 서비스로 세분화 되어 있으며, 이러한 시장 비중은 2017년과 거의 동일하며 시장 판도에는 큰 변화가 없음
- 미국 주 별로는, 2019년 텍사스가 571억 달러로 가장 높은 순위를 보이고 있으며, 캘리포니아(381억 달러) 및 플로리다(353억 달러)가 그 뒤를 잇고 있음

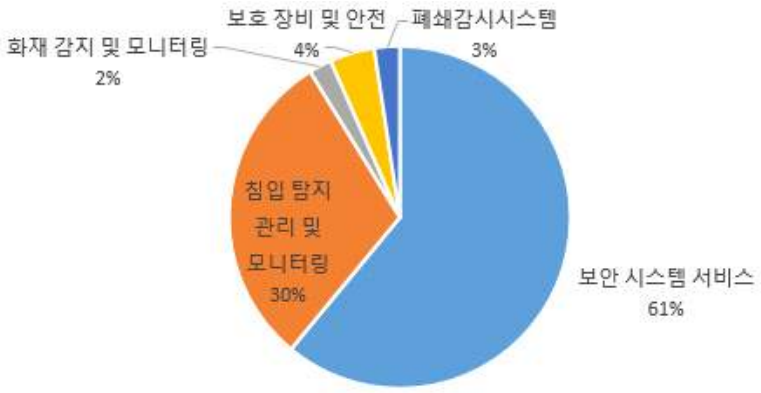
표 _ 미국 물리보안 시스템 서비스 시장

(단위: 개, 백만 달러, 명)

	2016	2017	2018	2019	2020
구축	24,765	25,783	27,041	28,193	29,592
매출	222,589	238,057	255,647	272,607	288,822
직원수	157,734	164,217	172,228	179,561	188,474

[출처] Barnes Report, 2019 U.S. Security Systems Services Industry-Industry & Market Report, 2019.1

그림 _ 미국의 물리보안 분야별 시장 규모와 현황(2019년)

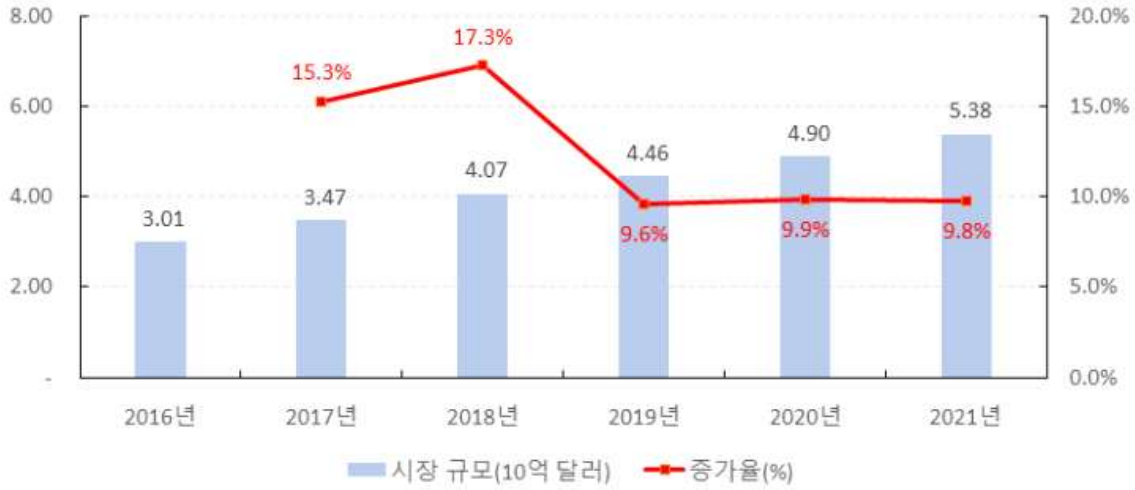


[출처] Barnes Report, 2019 U.S. Security Systems Services Industry-Industry & Market Report, 2019.1

▶ 2016년 기준 미국 동영상 감시 제품 시장 규모는 30억 1,000만 달러 규모로, CAGR 12.3%씩 증가하여 2021년 53억 8,000만 달러의 시장 규모를 형성할 것으로 전망

- 미국 정부는 국내 인프라를 범죄 및 테러 공격으로부터 보호하기 위해 동영상 감시 제품과 서비스를 적극적으로 도입
- 정부 및 공공분야뿐만 아니라 민간 기업들의 적극적인 투자가 시장 성장의 주요 견인 역할
- 향후 동영상 감시 시장은 클라우드 서비스, 빅데이터 분석 등 새로운 기술의 접목으로 지속적으로 증가할 것으로 예상

그림 _ 동영상 감시 시장 현황



▶ 경비원 및 순찰 서비스 시장은, 2018년 296억 달러에서 2019년 321억 달러로 CAGR 8.3%의 성장 추정

- 이 시장은 경비원, 보호 및 가드 서비스를 제공하는 시설을 의미
- 2016년 254억 달러에서 CAGR 8.2%로 2020년 348억 달러로 성장할 것으로 예측
- 2019년 주요 세부 서비스 시장별로는 ▲경비원 서비스 (40%) ▲보호 서비스 (22%) ▲가드 서비스 (18%)가 상위 점유율을 보이고 있음

표 _ 미국 경비원 및 순찰 서비스 시장

(단위: 개, 백만 달러, 명)

구분	2016	2017	2018	2019	2020
업체 수	36,087	37,122	38,483	39,909	41,666
매출	25,392	27,243	29,643	32,102	34,756
직원수	622,416	640,277	663,746	688,347	718,651

[출처] Barnes Report, 2019 U.S. Security Guards & Patrol Services Industry-Industry & Market Report 2018.10

물리보안 제품 및 서비스 유통

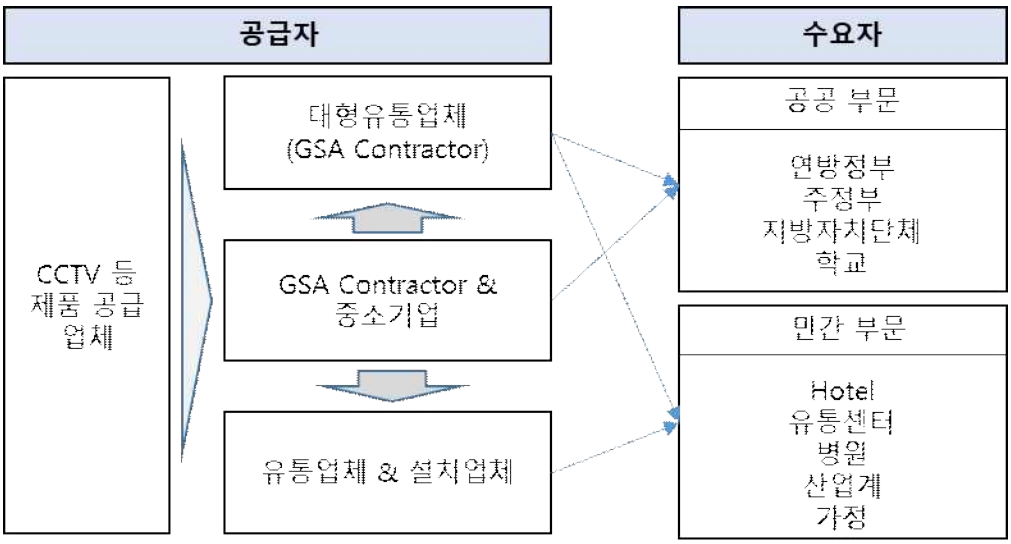
▶ 미국 물리보안 시장의 유통구조는 제품 및 서비스에 따라 시장이 여러 분야로 혼재되어 있어 복잡한 구조를 가지고 있음

- 하드웨어는 전문도매나 유통 딜러를 통하며, 직접 설치하는 업체에 판매되기도 하고 지역별 수많은 딜러를 통하게 됨
- 보안시스템 가치사슬(value chain)은 제조업체로 시작되며, 하드웨어 제품 개발 초기 단계부터 제조업체가 자체 개발하고 이를 적용해 생산하는 경우가 많음

▶ 공공시장은 연방정부, 주정부, 학교 등으로 구성되며, 미국 조달시장의 규칙을 따름

- 조달 시장에 공급하기 위한 기본 조건으로는 GSA contractor로 등록돼 있어야 하며, 이미 진출에 있는 대형 유통업체인 prime contractor와의 관계 형성이 중요
- 수요처 관점에서는, 공공부문과 산업계 등의 민간부문으로 나뉘며 두 시장 모두 대형 유통업체와의 관계 형성이 시장 진입의 중요 요소

그림 _ 미국 물리보안 유통채널 구조



[출처] STRABASE

▶ 물리보안 부문에서는 다양한 종합 유통 업체들과 전문 벤더들이 활약하고 있으며, 물리보안 제품과 정보보안 제품을 함께 취급하는 업체들도 다수 활동 중

- 물리보안 제품 공급 및 유통 업체 중에서는 ADT Security Service가 2018년에 이어 2019년에도 가장 규모가 큰 업체로 평가
- Ingram Micro 같은 대형 업체들은 물리보안과 정보보안 분야를 망라한 보안 제품을 유통

표 _ 미국의 대표적인 물리보안 종합 유통 업체 현황

업체명	개요 및 주요 취급 품목
ADT Security Service	- 안전 및 보안 관련 글로벌 최대 기업으로서 가정 및 비즈니스 분야 보안 서비스를 제공하며, 400군데 이상 인증 받은 딜러를 보유 - 미국 외에도 전 세계 200개 이상의 현지 법인 및 지사 보유
Stanley Convergent Security Solution	- Stanley Black and Decker 그룹 계열사로 보안 시스템의 디자인, 공급 설치 및 서비스 제공, 연방정부 및 주정부 보안 솔루션 공급업체
PELCO	- Schneider Electric의 보안 솔루션 전문업체이며, GSA 연방정부 공급 스케줄의 컨트랙트 홀더임. CCTV카메라, DVR 부문 담당
Ingram Micro	- 세계 최대 규모의 IT, 전자제품 전문 유통 업체로 세계 최대의 유통망을 보유 - 미국 본사를 비롯해 48개국에 162개의 지사와 물류 창고를 운영하며 150개국에 약 17만 개 도·소매업체(Best Busy, Future shop, Staples 등 리셀러)에 제품을 공급 - Sony, HP 등 대기업을 비롯해 약 1,400개의 제조업체에서 제품을 구매하며, 자체 브랜드를 OEM방식으로도 소싱
PELIKANCAM	- 미국 정부 기관 대상 전문 유통업체로서 GSA 컨트랙터로 활동 중 - 취급품목으로는 CCTV 카메라, 네트워크 DVR, IP 카메라 & 시스템이 대표적
A1 Security Cameras	- 보안 카메라 및 카메라 시스템 유통의 선도 기업 - GSA 컨트랙터로서 정부, 육해군, 은행, 주정부 등 대형 우량 고객 보유 - 온라인 사이트를 운용하며 글로벌 기업의 보안 카메라 라인업 보유

[출처] Wikipedia, Google Finance 종합

3) 주요 사업자 현황

시장 특성 및 경쟁 강도

❑ 정보보안 시장

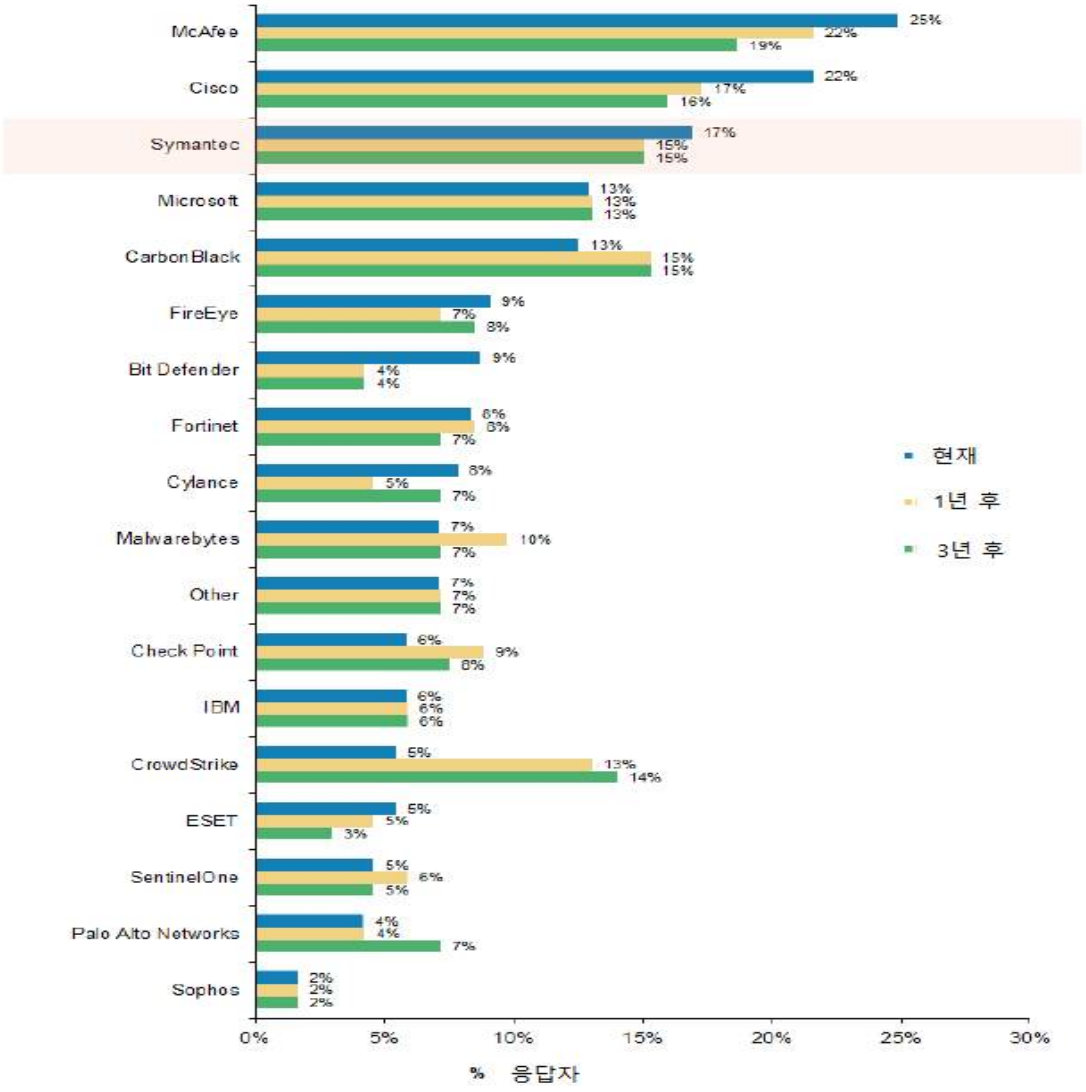
▶ 전 세계 시장의 40%를 차지하는 최대 시장인 미국은 연방정부가 적극적으로 투자 수요를 형성

- 매출 상위 15개사가 전체 시장의 27%를 점유하는데 그쳐 특정 기업이 경쟁적 우위를 가지 않는 경쟁적 시장 구도
- 주요 기업으로는 Symantec(15.9%), McAfee(13%), Check Point(3.9%) 이며, 기타 약 1만 730개의 기업이 존재
- 최근 클라우드 기반의 보안 솔루션 도입이 증가하면서 해당 시장의 경쟁이 심화되고 있으며, Cisco, Symantec, Zscaler, Forcepoint 등이 주도

▶ 2019년 Morgan Stanley에 따르면, 현재 및 향후 CSO가 도입하고자 엔드 포인트 보안 솔루션 업체 선호도 조사에서 McAfee, Cisco, Symantec이 상위를 차지하고 있으며, Microsoft, Carbon Black, Fireeye 등이 그 뒤를 잇고 있음

- Carbon Black은 향후 1~3년 내에 도입 선호도가 증가하여, 현재 3위인 Symantec과 시장 우위 경쟁을 할 것으로 나타남
- 현재 도입률이 5%로 14위인 Crowd Strike는 도입 선호도가 급격히 증가하여, 향후 3년내 3위 시장 경쟁에 합류할 것으로 예상됨

표 _ 미국 CSO가 도입 예정인 엔드포인트 보안 업체(2019~2022)



주) Survey of Chief Security Officers, n=61

[출처] Morgan Stanley Research(2019.1)

❑ 물리보안 시장

▶ 홈 오토메이션 산업에 새로 진입한 기업들은 보안을 강화할 뿐만 아니라 집을 통제하기 위해 노력하고 있으며, 각 세부 분야별로 미국 혹은 글로벌 업체들이 경쟁하고 있음

- 케이블업계 중에서는 Comcast, Cox, Spectrum이, 통신업계에서는 BCE Inc, AT&T (Digital Life)가 경쟁에 참여
- 기술/인터넷 분야에서는 Google(Nest), Amazon(Alexa, Ring), Samsung (SmartThings)이 주요 솔루션 제공
- DIY 분야에서는, Simplisafe, Arlo Technologies, Ooma Inc, Protect America, Frontpoint 등의 업체들이 서비스를 제공

▶ 2018년에 물리보안 업체의 인수 및 합병 활동은 총 73억 달러(2017년 16% 증가)로 새롭게 성장하고 있음

- 물리보안 업계의 구조는 수백 개의 소기업으로 인해 매우 세분화되어 경쟁하기가 점점 어려워지고 있는 추세임
- 합병 및 인수의 일반적인 추세와 가치는 향후 5년간 계속 증가할 것으로 예상

▶ 재난 및 보안 관련 시장은 물리보안의 서비스나 융합보안으로 구분되며, 시장의 성장은 물리보안의 성장과 동일 수준으로 성장

- 솔루션을 제공하는 업체들은 대부분 보안 시스템 회사나 보안기기 제품 생산회사들로서, 제품 개발 초기부터 병행하는 사례가 다수임
- 따라서 주된 경쟁사들은 현재는 바이어가 될 수도, 미래에는 경쟁사가 될 수도 있는 구조임

주요 사업자

❑ 정보보안 시장

▶ Symantec Corporation

- Symantec은 보안 영역을 포함한 세계 최대의 소프트웨어 기업으로서 현재 엔드포인트 보안, 데이터

보안, 이메일 보안, 인증서 등 신뢰서비스 분야에서 전 세계 시장 점유율 1위를 기록하고 있는 업체

- 2016년 6월 클라우드 보안 전문 업체 Blue Coat Systems를 인수함으로써 웹 보안 시장과 클라우드 보안 분야도 선도할 수 있을 것으로 주목받음
- 또한 지능형 지속 위협에 대한 보안 전략을 앞세워 차세대 엔드 포인트 보안, 이메일 보안, 원격 보안관제 서비스 등에 초점을 맞추고 이와 관련한 포트폴리오를 확대
- Symantec Mobile Security는 iOS, Android 및 Windows OS 기반의 모바일 단말을 각종 멀웨어 및 보안 위협으로부터 보호할 수 있는 앱 형태의 종합 솔루션을 지향
- 안티바이러스 기술, 방화벽, SMS 안티스팸 등의 기능이 기본으로 포함되어 있으며, Symantec Mobile Management Platform으로 복수의 모바일 단말 보안을 일원적으로 관리 가능
- 2016년 11월, 시만텍은 AI 기술이 적용된 엔드포인트 보안 솔루션 'SEP 14 (Symantec Endpoint Protection 14)'를 공개하고 실시간으로 올라오는 멀웨어 100개를 상대로 탐지 성능 데모를 시연해, 해당 멀웨어에 대한 시그니처가 갖춰지지 않은 상황에서도 90개 이상을 탐지함으로 AI 기반 보안제품 경쟁에 선두로 나섬
- 2019년 8월, Broadcom은 Symantec으로부터 LifeLock 브랜드와 Norton 안티바이러스 소프트웨어를 제외한 엔터프라이즈 보안 포트폴리오를 107억 달러에 인수

▶ SecureWorks

- 애틀랜타에 본부를 둔 인텔리전스 중심의 보안 솔루션 제공 업체로서, 2011년 Dell에게 6억 7,000만 달러에 인수됨
- 매니지드(Managed) 보안 서비스에 있어서 2018년 글로벌 시장 핵심 업체로서 AT&T, Symantec, IBM 등과 함께 해당 시장을 견인하고 있음
- 호스트 및 네트워크 기반 고급 위협 탐지를 위한 ▲AETD (Advanced Endpoint Threat Detection) ▲취약성 검색 ▲고급 위협 인텔리전스 서비스 제공
- 2019년 5월 Gartner의 전 세계 관리형 보안 서비스를 위한 Magic Quadrant 부문에서, 전체 공급 업체 중 비전과 능력 면에서 가장 높은 업체로 선정

▶ Carbon Black

- 매사추세츠에 본사를 둔 사이버보안 혁신 기업으로서 미국 정부의 보안 해커 팀의 전 구성원에 의해 설립되었으며, NSA와 CIA의 교육을 받은 설립자들은 엔드 포인트 보안을 위한 도구와 기술을 개발
- 고객이 가장 앞선 위협에 대비할 수 있도록 응용 프로그램 제어, EDR (Endpoint Detection and Response) 및 NGAV (Next-Generation Antivirus)를 포함한 다양한 엔드 포인트 보안 범주를 개발

- 필터링 되지 않은 고객의 데이터 위협을 분석하는 빅데이터 및 분석 클라우드 플랫폼인 PSC (Predictive Security Cloud)라는 기술을 활용
- Carbon Black은 2019년 8월 VMware에 21억 달러에 인수됨

▶ Cisco Systems

- 세계적인 네트워크 장비 업체로서 차세대네트워크, Service Provider Video, 데이터센터, 와이어리스, 사이버보안 등의 분야에서 활약
- Cisco Systems가 추진 중인 보안 비즈니스의 투자 방향은 2015년에 발표한 '모든 곳에서의 보안(Security Everywhere)' 전략이 바탕이 되고 있음
- 이 전략은 확장된 네트워크 환경에서 가시성과 제어능력을 높이고 사이버 공격이 발생하기 전(Before)과 공격이 이뤄지는 동안(During)과 공격이 이뤄진 후(After)에 이르기까지 전체 주기에 걸쳐 위협을 탐지하고 복구시간을 단축시키는 것이 특징
- 특히 클라우드 환경에 적절하게 대응하기 위해 2013년 Sourcefire와 2014년 Open DNS 등의 네트워크 보안 업체를 연달아 인수하고 2015년 통신장비 업체 Ericsson과 제휴를 체결했음
- 2015년 10월에는 모바일 기기 등 엔드 포인트에 대한 백도어 보안 솔루션 업체 Lancope를 인수해 보안 솔루션 사업부로 편입
- 2016년 8월 클라우드 보안업체 CloudLock 합병완료로 클라우드 보안 경쟁 강화
- 2018년 8월 보안 및 인증 클라우드 서비스를 제공하는 듀오 시큐리티(Duo Security)를 233억 달러에 인수할 것을 발표하였으며, 이를 통해 통합 액세스 및 다단계 인증 시장 진출에 발판을 마련

▶ Check Point Software Technologies

- 이스라엘에 본사를 둔 Check Point Software Technologies는 매출 기준으로 글로벌 기업보안 시장 점유율 4위를 기록
- 인터넷 정보보안 전문업체로서 전 세계 10만 개 이상의 대기업, 중소기업을 고객으로 확보
- 특히 네트워크 보안 어플라이언스, 엔드포인트, 모바일 안티 멀웨어 블레이드, 웹 게이트웨이 등 다양한 포트폴리오를 보유하고 꾸준한 성장세를 지속
- 고객들은 Check Point의 가상 시스템과 함께 방화벽, 가상사설망(VPN), 인터넷침입방지시스템(IPS), 애플리케이션 컨트롤, URL 필터링, 안티봇, 안티바이러스, ID인식 등 체크포인트 소프트웨어 블레이드를 선택해 가상화 보안을 강화할 수 있음
- Check Point는 현재 모바일, 클라우드 및 온-프레미스 네트워크에서 대규모 및 신속한 공격에 초점을 맞추고 있는 5세대 보안에 중점을 두고 있음

▶ Fortinet

- Fortinet은 고성능 네트워크 보안 제품과 서비스 공급회사로서 Unified Threat Management(UTM) 솔루션 분야의 주도 업체로 자리매김
- 통신업체, 데이터 센터, 엔터프라이즈, 분산 오피스 및 MSSP에게 네트워크 보안 어플라이언스 및 보안 구독 서비스를 제공
- 네트워크 보안 플랫폼, FortiGate는 방화벽, VPN, 멀웨어 방지, 침입 방지, 애플리케이션 관리, 웹 필터링, 스팸 방지, DLP, WAN 가속화, WLAN 관리 등 다양한 보안 및 네트워킹 기능을 제공하는 물리 및 가상 어플라이언스로 구성
- 대표 상품으로는 FortiGate라는 통합 네트워크 보안 방화벽을 내세우고 있으며, 전 세계 2만 여 개의 채널 파트너를 통해 서비스를 공급
- 2019년 2월 '모바일 월드 콩그레스 2019'에서 ▲핵심 모바일 네트워크(5G 포함)에 대한 보안 ▲MEC (Multiaccess Edge Computing) 및 IoT (Internet of Things) ▲SD-WAN 및 관리 형 보안 서비스 제공 업체라는 주제를 통해 자사의 보안솔루션을 소개

▶ Rapid7

- 2000년 Boston에서 설립된 보안 데이터 및 분석 솔루션 제공 업체로서, 자사의 Insight Cloud 솔루션에 의해 제공되는 가시성, 분석 및 자동화를 통해 고급 보안을 제공
- ▲IT 보안 데이터 ▲분석 소프트웨어 ▲글로벌 서비스를 통해 조직이 보안 침해 위험 감소, 공격 탐지 및 대응에 대한 효과적인 IT 보안 프로그램을 구축할 수 있도록 견인
- Gartner의 2018 보안 정보 및 이벤트 관리 부문 매직 쿼드런트 (Magic Quadrant)에서 비전 전문가로 선정
- 2019년 2월 NetFort사의 네트워크 모니터링, 트래픽 가시성 및 분석 기능을 Insight Cloud에 도입함으로써, 대량의 데이터 및 분석을 단일 플랫폼으로 통합
- 2019년 6월 AWS(Amazon Web Services) 보안 허브와 통합되어 우선 순위가 높은 보안 경보를 중앙 집중화하고, 보안 경보로 트리거 되는 작업에 대한 자동화 발표

▶ Imperva

- 2002년 캘리포니아에 설립되었으며, ▲웹 애플리케이션 보안 ▲데이터 보안 ▲위협 인텔리전스 및 애플리케이션 제공

- 보유 제품군인 Incapsula, SecureSphere 및 CounterBreach는 사이버 공격으로부터 웹 사이트, 응용 프로그램, API 및 데이터베이스를 보호하는 솔루션 제공
- Imperva Incapsula 솔루션은 웹 애플리케이션 방화벽 및 DDoS 규칙 엔진 등을 통해 트래픽을 필터링하며, 다중 계층 접근 방식을 사용하여 DDoS 트래픽을 차단
- 2009년 4월 봇 차단 솔루션 벤처 기업인 Distil Networks를 인수한다고 발표하였으며, Imperva의 애플리케이션 제공 플랫폼에 서비스를 통합 계획

❑ 물리보안 시장

▶ Allied Universal

- 펜실베니아에 본사를 둔 개인 소유의 시설 서비스 회사로서, 미국 내에서 가장 큰 규모의 보안서비스 회사
- 2016년 미국 유니버설 서비스 (Universal Services of America)와 얼라이드 바턴 (Allied Barton)의 합병을 통해 45억 달러의 매출을 기록한 시장 1위 업체
- ▲유인 보호 ▲위험 자문 및 컨설팅 ▲통합 기술 및 보안 시스템 솔루션 ▲인텔리전스 중심 보안 인력 관리 서비스를 제공

▶ Securitas

- 스웨덴 스톡홀름에 본사를 둔 Securitas AB를 모기업으로 하며, 보안 감시, 모바일 순찰, 모니터링 및 컨설팅 서비스 제공
- Securitas 운영 센터를 통해 북미에서 가장 큰 모바일 공간을 활용하여 Integrated Guarding 보안솔루션을 제공

▶ Vivint Inc.

- 미국에서 가장 큰 주택 보안 서비스 시스템 공급업체 중 하나로 가정용 보안 제품을 생산하고 공급하는 업체
- 주택 보안 시스템 서비스를 제공하면서 경쟁업체보다 저렴한 제품을 공급하는 것이 핵심 경쟁력이며, 미국 전역에 대규모 판매 및 서비스 오피스를 운영
- 주요 취급 품목은 터치스크린, 보조 터치 스크린 패널, 디지털 도어록, 스모크 알람, 유선 비디오 카메라 등이 대표적

▶ G4S

- 영국 런던에 본사를 둔 다국적 보안 서비스 회사로서, 해외 정부와 협력하여 정부에 대한 전체 사이트 또는 자산에 대한 통합 시설 서비스를 포함하는 '보안 시설 서비스' 제공
- 수익면에서 세계 최대 보안 회사로서 90개국 이상에서 사업을 운영하고 있음
- 훈련 및 선별된 보안 담당자를 제공하는 '무인 보안 서비스' 및 액세스 제어, CCTV, 침입자 경보, 화재 감지, 비디오 분석, 빌딩 시스템 통합 기술 등의 보안 시스템 제공

▶ FLIR Systems

- 오레곤에 본사를 두고 1978년 설립된 열화상 및 기타 센서, 시스템 설계 및 제조 업체
- 첨단 센서 및 통합 센서 시스템은 전 세계 민간 및 정부의 다양한 애플리케이션을 통해 중요 정보를 수집하고 분석할 수 있도록 지원
- 2016년 기준으로 감시(Surveillance) 제품의 매출 비중이 32%로 가장 큰 비중을 차지하고 있음

▶ FaceTec

- 캘리포니아에 본사를 두고 있으며, 최신 스마트 기기에서 모든 앱 암호를 완전히 대체할 수 있는 3D 얼굴 인식 솔루션 제공
- iPhone X에 탑재된 Face ID 기술을 뛰어 넘을 수 있는 방법을 성공적으로 시연함으로써 해당 분야를 기술적으로 견인
- Forge Rock, HYPR 및 기타 많은 시스템 통합업체가 생체 보안 수준을 높이고 사기 및 신원 도용 문제를 해결하기 위해 전 세계적으로 FaceTec의 솔루션을 판매

▶ Kastle Systems

- 비디오 감시, 엑세스 제어, 화재 및 방문자 관리를 포함한 통합보안 솔루션에 대한 설계, 운영, 관리, 모니터링 및 유지보수 제공
- 미국 전역의 수천개 기업에서 중앙 집중식 가시성 및 제어, 모바일 기능 및 시스템 백업을 통한 오프사이트 호스팅을 위해 kastle의 웹 기반 도구를 사용
- 2017년 괄목할 만한 성장을 기록하며, 미국 및 유럽의 더 많은 도시로 확장 계획

4) 주요 동향 및 이슈

▶ VMware는 엔드 포인트 보호 공급 업체인 Carbon Black와 합병하기로 결정했으며, 약 21억 달러를 합병 비용으로 지불하기로 함(2019.8)

- Carbon Black은 악성 행위 탐지 및 악의적인 파일이 조직을 공격하는 것을 방지하도록 설계된 클라우드 고유의 엔드포인트 보안 소프트웨어 제공
- '차별화된 고유 보안 클라우드'를 구축하려는 관점에서 빅 데이터, 행위 분석 및 AI를 통해 VMware는 엔터프라이즈 워크로드 및 고객을 보다 잘 보호할 수 있는 최적의 솔루션을 제공
- VMware 제품군에 Carbon Black 솔루션을 도입함으로써 보안을 강화하고, 워크로드, 애플리케이션, 네트워크를 관리 및 보호하는 엔터프라이즈급 플랫폼을 제공
- Carbon Black은 VMware 내에서 독립적인 사업 단위로 존재하며 VMware의 보안 사업에 편입될 전망

▶ NSA는 사이버 공간에서 러시아와 중국과 같은 외국의 위협에 대처하기 위한 새로운 조직을 발표(2019.7)

- 10월부터 운영될 사이버보안국은 Anne Neuberger*가 이끌 예정
  * 최근 크렘린 해커들의 위협을 관리하기 위해 설립된 러시아 중간 그룹 (Russian Small Group)으로 알려져 있으며 NSA 조직을 이끌었음
- 또한, 보안 전문업체인 Check Point와 Cisco Systems가 새로운 CTA 멤버로 합류함
- NSA의 외국 정보분석 및 사이버 방어 임무를 통합하고 국가 안보 시스템과 방위 산업 기반에 대한 위협을 예방하고 근절을 목표로 함
- 2020년 미국 대통령 선거를 방해하려는 외국 국가들의 시도가 있다면, 새로운 조직이 그에 대한 준비가 진행할 것이라고 강조

▶ 독립적으로 발표된 두 가지 보고서에서, 대다수의 조직이 클라우드 보안 상태에 매우 우려하고 있음을 발견(2019.7)

- Bitglass의 2019년 클라우드 보고서에서, 기관의 93%는 클라우드를 안전하게 사용할 수 있을 것인가에 대해 보통 정도의 우려를 갖고 있음을 언급
- Bitglass 보고서에 따르면, 조직의 75%가 여러 클라우드 솔루션을 활용하고 있으며, 20%만이 앱간 이상 동작에 대한 탐지능력을 확보하고 있음을 발표
- Synopsys의 2019년 클라우드 보안 보고서에 따르면 응답자 93%가 클라우드 보안에 관해서는 보통 또는 상당히 우려한다고 응답

- Synopsys 보고서는 조직이 광범위한 클라우드 보안 문제를 가지고 있으며, 가장 주목할만한 점은 조직은 데이터 손실 및 유출(64%), 개인 정보보호 및 기밀유지(62%)에 대해 우려하고 있다는 사실

▶ 샌프란시스코시는 경찰 당국과 다른 시 당국이 주민들에게 얼굴 인식 기술을 사용하지 못하도록 하는 조례를 승인(2019.5)

- 조례는 경찰이 사용하는 감시 기술*을 공개하는 프로세스를 포함하나, 얼굴인식은 주민의 시민자유권에 악영향을 미친다는 점을 고려

 * 주민의 이동을 추적 할 수 있는 Cell-Site 시뮬레이터, 차량번호판 리더 등

- 얼굴 감시 기술은 현재 심각한 오류율로 인하여 시민 자유에 큰 위험이 되고 있으며, 완벽하고 정확한 대량 감시가 이루어지면 이를 더욱 악화시킬 수 있다고 우려
- 캘리포니아의 오클랜드, 버클리 및 매사추세츠 주 서머빌을 비롯한 몇몇 다른 도시에서도 얼굴 인식 금지 고려
- 이는 개인정보보호 옹호자뿐만 아니라 법 제정자 및 일부 기술 업체가 지지하고 있으며, 마이크로소프트는 7월에 연방정부에 얼굴 인식 기술을 규제하고, 법 집행 기관에 판매하지 못하도록 연방정부에 요청

▶ Palo Alto Networks와 Demisto간의 최종 인수 계약이 체결되었으며(2019.1), 인수는 Palo Alto Networks의 회계연도 3분기에 종료될 것으로 예상

- 총 5억 6,000만 달러를 지불함으로서 Demisto 인수가 마무리 될 예정임
- Demisto는 Security Orchestration, Automation, Response (SOAR) 플랫폼을 제공하며, 머신러닝 기술 기반 사고 분석 및 조사를 지원
- Palo Alto Networks는 인공지능과 기계 학습을 추가함으로써 고객의 보안 운영에서 중요한 부분의 자동화 가능
- Palo Alto Networks는 보안팀에 보다 신속한 위협 예방 및 대응을 제공할 수 있게 될 전망

▶ 프랑스 규제 기관(National Data Protection Commission, CNIL)이 Google에 GDPR 위반에 대해 5,000만 유로(약 5,700만 달러)의 과징금 부과(2019.1)*

- Google은 데이터 처리 목적 및 데이터 저장 기간에 대한 정보를 제공하지 않았으며*, 때로는 사용자 정보를 얻기 위해 5~6회 클릭하도록 유도

 * 위반사항 : (투명성에 대한 의무 위반) 어떻게 데이터를 수집하고 타깃광고에 사용하는지에 대하여

사용자에게 적절히 공개하지 않음

- 프랑스에서 벌금이 부과 후, GDPR 위반 혐의로 스웨덴 규제기관 (Datainspektionen)에서도 추가 조사*

* 위반사항 : (위치정보 불법 수집) '위치 기록'과 '웹 및 앱 활동'을 통해 안드로이드 사용자의 위치 데이터 접근 및 수집

▶ 맥아피 보고서에 따르면, 해커그룹은 수개월 동안 전 세계 수십 개 기업의 기반시설을 대상으로 하는 글로벌 해킹 캠페인 진행(2018.12)

- 캠페인은 악성 코드를 사용하여 10월과 11월에 원자력, 방위, 에너지 및 금융 업계의 최소 87개 회사의 컴퓨터 시스템에 침투하려고 시도
- 대상 기업들을 밝히지 않았으며 대부분이 미국에 기반을 두고 있음
- 첨부 문서에는 Rising Sun이라는 백도어 악성코드가 포함되어 있으며, 사용된 악성코드는 북한 해킹 유닛인 Lazarus Group이 사용하는 코드와 굉장히 유사

5) 정보보호 스타트업 시장 현황[3]

시장 규모

▶ 미국 내 산업별 동향과 벤처캐피털 투자 동향으로 살펴본 결과 향후 IT분야로 집중적인 투자가 이뤄져 관련 스타트업이 성장할 전망

- 2018년 사이버보안 분야의 스타트업 기업에 대한 투자 건수는 617건으로 2015년 대비 40% 가량 증가
- 2018년 조사에 따르면, 스타트업 5000개 기업 분야 중 보안 분야 업체는 66개로 2017년 기준 약 770억 달러의 수익을 달성 (출처 Inc 5000)
- 미국 내 가장 빠르게 성장하는 스타트업 분야는 인공지능으로 향후에도 지속적인 성장세가 예상됨
- AI 스타트업 투자 금액은 2013년 11억 달러에서 2018년 93억 달러로 증가하였고, 투자 건수는 2013년 207건에서 2017년 533건을 기록하였으나 2018년 466건으로 소폭 감소

3 미국 스타트업 동향과 시사점, 한국 무역협회 뉴욕 지부, 2019.2

주요 사업자

▶ 스타트업 기업 전문 조사 기관인 CB Insights에 따르면, 2019년 사이버보안 분야 비상장 기업 중 태니엄(Tanium) 사는 가장 높은 기업 가치(65억 달러)를 가진 유니콘 기업[4]으로 평가

- 사이버 보안 스타트업 기업 중 노비포(KnowBe4)와 같이 유니콘 기업으로 평가되는 신규 업체가 증가하는 추세임

▶ 포춘(Fortune)에 따르면 사모 펀드는 초기 투자액 5,000만 달러를 발표한 지 불과 3개월 만에 3억 달러를 사이버 보안 인식(Cybersecurity Awareness) 회사인 KnowBe4에 추가로 투자(2019.6)

- KnowBe4는 2010년 설립된 회사로서 통합된 보안 인식 교육 및 시뮬레이션 피싱 플랫폼을 제공하며, 유명한 해커 Kevin Mitnick이 수석해킹담당자를 맡고 있음
- 2019년 10억 달러 시장가치를 인정받아 유니콘이 되었고, 브라질, 노르웨이 기반 2개 회사을 인수하고, 국제적으로 확장할 예정
- 규제가 엄격한 산업에서부터 글로벌 기관에 이르기까지 전 세계에 걸쳐 25,000 사용자 보유
- 보안 인식 교육에 대한 새로운 학교 접근 방식을 통해 랜섬웨어, CEO 사기 및 기타 사회 공학 기법에 대한 인식을 제고함으로써 회사가 인적 보안 문제를 해결하도록 지원

표 _ 미국 사이버 보안 주요 스타트업 기업 현황(2019)

주요 기업	본사	설립일	제공 솔루션
Tanium	캘리포니아 주	2007년	개인 엔드 포인트 보안 및 시스템 관리
Cloudflare	캘리포니아 주	2009년	CDN 서비스와 분산 네임서버를 이용하여 사이트 성능과 속도, 보안성 향상
Kaseya	뉴욕 주	2000년	IT 자동화 관리 서비스 플랫폼
Lookout	캘리포니아 주	2005년	모바일 앱 보안 및 분석
Illumio	캘리포니아 주	2013년	데이터 센터 및 클라우드 컴퓨팅 보안
Netskope	캘리포니아 주	2012년	클라우드 애플리케이션, 인프라 및 웹 보안
Auth0	워싱턴 주	2013년	웹, 모바일 및 레거시 애플리케이션을 위한 범용 인증 및 인증 플랫폼
KnowBe4	플로리다 주	2010년	보안 인식 교육 프로그램
Druva	캘리포니아	2008년	클라우드 데이터 보호 및 관리

[출처] 인터넷 기사 수집

4 기업가치 10억 달러 이상의 비상장사

주요 동향 및 이슈

▶ 미국 내 스타트업 생태계는 IT 기술 분야를 중심으로 활성화되고 있으며, 대도시권을 중심으로 투자가 활발히 이뤄지고 있음

- 실리콘밸리 내 인공지능(AI) 관련 스타트업 투자는 구글, 페이스북 등 거대 IT기업을 중심으로 이루어지며, 대표적으로 2018년 Microsoft가 AI 스타트업 Github사를 75억 달러에 인수함

▶ 뉴욕지역에 위치한 사이버 보안 스타트업들은 뉴욕 내 금융, 언론, 소매, 헬스케어 분야 기업들의 개인 데이터 관리에 대한 수요확대를 바탕으로 발전하고 있음

- 뉴욕에는 약 100개 이상의 사이버 보안 관련 업체들이 있으며 사이버보안 스타트업들은 2017년 약 10억 달러의 벤처캐피털(VC) 투자를 받음
- 대표적으로, 사이버 보안 관련 스타트업인 Mark43은 8,000만 달러, 소매 사기 방지 관련 스타트업 Forter는 5,000만 달러 투자금을 유치함

정보보호 정책 및 기관 현황

1) 관련 법령 및 정책

관련 법령 및 규제

▶ 트럼프 대통령, 정보통신 기술 및 서비스에 대한 위협에 대처하기 위해 ICT 공급망 보호에 관한 행정명령(Executive Order on Securing the Information and Communications Technology and Services Supply Chain)에 서명(2019.5)

- 미국 정부는 2018년 9월에 발표한 국가사이버전략에서 사이버보안 인력 개발을 정책 우선순위 중 하나로 설정
- 행정명령의 핵심사항은 ▲대통령배 사이버보안 연례 경진대회 개최 ▲사이버보안 전문성 증진을 위한 연방직원 직무순환 프로그램 개시 ▲사이버보안 인력 프레임워크 도입 확산 ▲사이버보안 적성 평가 실시 ▲시스템에 대한 보안 인력 부족 해소에 대한 내용을 담고 있음

▶ 트럼프 대통령, '사이버보안 인력 확충에 관한 행정명령'(Executive Order on America's Cybersecurity Workforce)에 서명(2019.5)

- 외국 적대세력의 위협으로부터 미국의 안보와 시민의 안전을 보호
- 미국내에서 공급 및 사용되는 ICT와 서비스의 보안성, 무결성, 신뢰성을 보장함으로써 안보 위협에 대처

▶ 미국 상원에 주 및 지방 정부의 사이버보안 역량 강화 지원을 위한 주(州)사이버복원력 법안 재발의(2019.4)

- 각 주정부의 사이버 복원력 조치 역량 강화를 위해 국토안보부에 교부금 프로그램 설치 및 운영 권한을 부여
- 교부금 설치 근거, 계획·실행 교부금 승인, 교부금 활용, 교부금 할당 및 교부금 검토 위원회의 구성과 역할 등을 규정
- 교부금 프로그램에 대한 실제 운영 관리는 국토안보부 산하 기관인 연방재난관리청(FEMA)이 담당

▶ 트럼프 정부는 미국이 직면한 나날이 증가하는 사이버위협에 대한 방어력을 강화하기 위한 '미국 국가사이버보안전략'을 발표(2018.9)

- 미국 국가사이버보안전략은 연방 네트워크 및 주요기반시설에 대한 사이버보안 강화를 목적으로 2017년 5월 발표된 '행정명령 제13800호'를 잇는 트럼프 정부의 사이버보안 핵심 정책으로서 '행정명령 제13800호'에 따라 진행된 각종 보고서들을 토대로 개발·수립
- 미 연방정부는 미국이 직면한 사이버위협으로부터 보호하고 연방정부의 사이버역량을 강화하기 위해 수행할 단계 제시
- 트럼프 정부의 '국가사이버보안전략'은 전임 오바마 대통령의 사이버보안 관련 정책(PDD-20)에 비해 사이버공격자에 대한 정부 대응 권한 강화
- 국가사이버보안전략은 ▲미국인, 국토, 시민의 삶에 대한 보호 ▲미국의 번영 촉진 ▲힘을 통한 평화 유지 ▲미국의 영향력 증대의 4개 전략영역(Pillar) 및 전략과제로 구성

2) 담당기관

▶ 국가안전보장회의(National Security Council, NSC)

- 1947년 제33대 트루먼 대통령 시절에 창설된 NSC는 미국 국가 안보와 외교 현안에 대해 조언과 자문을 구하고 대통령의 결정을 돕는 조직
- 대통령이 의장으로 있으며, 사이버보안과 관련해 산하조직으로 사이버보안국(Cybersecurity Directorate)을 두고 있음
- 오바마 정부 시기에는 사이버보안 컨트롤타워 역할로 대통령 직속 보좌관인 사이버보안조정관(Cybersecurity Coordinator)이 있었음
- 트럼프 대통령이 2018년 5월 업무 중복에 대한 효율성 제고와 관료주의 배제를 이유로 해당직을 해임한 후 컨트롤 타워 기능은 사이버보안국으로 옮겨져 두 수석 책임자가 공동으로 맡음

▶ 관리예산국(Office of Management and Budget, OMB)

- 대통령의 효율적인 행정발전과 유지계획을 지원하고 행정부의 조직을 관리하며, 예산관리의 감독과 통제, 법률안 제의에 대한 각 부처별 의견을 조정하기 위해 1970년 대통령실에 설치
- OMB의 사이버보안 관련 업무는 2002년 제정된 연방정보보안관리법(FISMA)에 따라 연방정부 및 정부기관이 지켜야 할 정보보안에 관한 정책, 원칙, 기준 및 가이드라인을 개발하고 그 실행을 감독
- OMB는 연방 정부부처와 기관들로부터 사이버보안 수준을 보고 받고 위험 요소 분석 및 실행계획을 수립

▶ 국가정보국(United States Director of National Intelligence, DNI)

- 9·11 테러 이후 지적된 미국 정보공동체 내에서의 관할 충돌과 협조체제 문제를 해소하기 위해 컨트롤 타워격으로 설치된 직책인 국가정보장(DNI)의 업무를 지원하는 조직
- 국가정보장과 국가정보국은 2001년 9·11 테러 사건 이후 정보기관을 개편할 필요성이 제기되어 2004년 12월 상원에서 통과된 '정보개혁 및 테러리즘 방지법'에 의해 설립
- 국가정보장은 군사와 관련된 정보활동의 예산을 제외하고 기존 국방부 장관이 관할하던 모든 정보기관에 대한 예산 관리 및 분배권을 책임
- 국가정보국은 백악관 직속이 아닌 외부의 독립기관이며, 국가정보장은 대통령의 정보 자문으로서 대통령과 국가안전보장회의에 직접 자문
- 국가정보국 산하의 사이버위협정보통합센터(CTIIC)는 자국 안팎의 사이버 위협과 사고를 수집 및 분석해 공공 및 민간 기관과 공유하는 업무를 담당
- 국가방첩안보센터(NCSC)는 국가정보장이 기존 국가방첩시행국(ONCIX)을 보안평가센터, 특수보안센터, 국가내부위협태스크포스와 결합해 2014년 11월에 설립한 조직

▶ 국토안보부(Department of Homeland Security, DHS)

- 미국 사이버보안 주무부처로서 2002년 6월 조지 W. 부시 대통령이 상원에 제출하여 통과된 '국토안보법'(Homeland Security Act)을 기반으로 설립된 부처
- 국토안보부의 목표는 테러방지 및 자연재해 등을 총집결시킨 총체적 재해.재난 관리체계를 구축하는 것으로, 이를 위해 국가기반보호계획을 수립
- 국토안보부의 업무 범위는 전 국가적인 국토안보를 실현하기 위하여 군사 부문 외에 민간 부문을 담당하는 것으로서, 여기에 사이버안보 및 사이버보안이 포함됨
- 2018년 11월 트럼프 대통령이 서명한 '사이버보안 및 기반시설보안청법'(Cybersecurity and Infrastructure Security Agency Act)에 의해 국토안보부 산하의 독립기관으로 설립
- 사이버보안 및 기반시설보안청(CISA)은 2007년에 설립된 국가보호프로그램부(NPPD)를 확대·발전시킨 기관
- 역할에 있어 NPPD와 크게 변화는 없지만, 독립적인 연방기관으로서 예산과 지침 행사력에서 더욱 강력한 권한을 부여받았다고 평가할 수 있음
- CISA 내의 사이버보안부는 국토안보부의 사이버보안 총괄부서 역할을 담당
- 사이버보안부는 하부 조직으로 ▲이해관계자참여 및 사이버기반시설 복원 부서 ▲국가사이버보안 및 통신통합센터 ▲연방네트워크복원 부서 ▲네트워크보안배포 부서의 4개 실무조직을 두고 있음

▶ 법무부(Department of Justice, DOJ)

- 미국 연방 정부의 법무 행정 주무 부처이며, 산하에 사이버보안 분야에서 범죄에 초점을 맞추어 수사와 단속하는 임무를 맡고 있는 연방수사국(FBI)를 두고 있음
- FBI는 12개 실(Office)과 6개의 지국(Branch)을 두고 있으며, 이 중 범죄, 사이버, 대응 및 서비스지국내 사이버부(Cyber Division)가 사이버 범죄 수사를 담당
- 2002년 설립된 FBI 사이버부는 컴퓨터 침입, 신분 도용, 인터넷 사기 범죄에 우선 순위를 두고 업무를 하고 있으며, 최근에는 온라인을 통한 아동 성적 착취와 지적재산권 침해 분야로 활동 영역을 확대

▶ 국방부(Department of Defense, DOD)

- 외부의 위협과 침략에 대해서 미국 국민 및 영토, 주요 방위 기반시설 보호를 주임무로 하는 부처
- 2010년 5월 국방부는 사이버공간에서의 작전 능력을 강화하기 위해 사이버사령부(Cyber Command, CyberCom)를 창설
- 사이버사령부는 미군의 통합전투사령부(UCC) 소속 부대 중 하나인 전략사령부(Strategic Command)의 소속 부대로, 사이버 상의 군사활동을 포함해 국방부 및 주요 군 시설의 네트워크 시스템 방어 등을 담당
- 사이버사령부는 임무별로 사이버 전투파견부대(Cyber Combat Mission Force), 사이버 보호부대(Cyber Protection Force), 사이버 국가파견부대(Cyber National Mission Force) 등으로 구성
- 육군, 해군, 공군 등 각 군마다 개별로 존재하는 사이버 방어 전담부대를 통해 직무를 수행
- 2018년 기준 사이버사령부에는 133개 팀이 있으며, 사이버사령부의 최고 책임자인 사이버사령관직은 국가안보국 국장이 겸직

▶ 상무부(United States Department of Commerce)

- 민간부문의 산업 육성을 지원하는 부처로서, 산하에 국립표준기술연구소(NIST)와 국가전기통신 및 정보청(NTIA)에서 사이버보안 관련 업무를 담당
- 국립표준기술연구소는 사이버보안 관련 연구개발과 표준화를 담당
- 국가전기통신 및 정보청은 인터넷 정책 태스크포스팀을 통해 사이버보안과 인터넷 경제의 혁신에 대한 포괄적인 연구를 수행

3) 규제 및 인증제도

▶ 2017년 7월, 의료기의 보안성 향상을 위해 사이버보안 평가표 작성과 판매 전 보안 테스트를 의무화하는 의료기기 사이버보안법((Medical Device Cybersecurity Act of 2017,S.1656)을 발의함

- 본 법안은 의료기기에 대한 사이버공격으로부터 환자의 안전을 보호하고 의료기기의 안정성을 개선하기 위한 취지라고 설명
- 기기의 보안성 확인을 위한 사이버보안 평가표(report card)를 작성하고 판매 전 보안 테스트를 의무화, 병원 내외에서 의료기기에 대한 원격접속 보호를 강화하고 의료기기 제조업체가 중대한 보안 패치나 업데이트를 무료로 제공할 것을 규정
- 사이버보안 평가표에는 ▲HIMSS[5]에서 개발한 의료기기 보안을 위한 생산자 공개문(MSD2) 최신 버전에 담긴 모든 기본적인 평가요인들에 관한 정보 ▲알려진 취약점을 해결하고 사이버보안을 개선하기 위한 보완통제[6] 방안 ▲기기 보안 테스트 등 사이버보안 평가 및 그 결과, 해당 평가를 진행한 기관 정보 등이 포함되어야 함

▶ 미국에서 판매되는 전자 및 보안 관련 제품에 대해 등록 및 인증 절차를 거치도록 의무화하여 관리

- 물리보안 제품들을 중심으로, 연방통신위원회(Federal Communications Commission, FCC)의 등록 요건과 UL(Underwriters Laboratory) 인증 조건에 대한 검토가 필요
- CC(Common Criteria)인증은 미국을 비롯한 주요 국가들이 보안 제품에 대해 공동으로 개발해 적용하는 국제 공통 평가기준

▶ 미 정부의 정보보호 인증제도는 예산관리국(Office of Management and Budget, OMB), 국립표준기술연구소(National Institute of Standards and Technology, NIST), 최고정보관리자협의회(Chief Information Officer, CIO)로 구성

- 예산관리국(OMB)은 정책결정 기관으로서 보안인증제도 추진을 총괄하며 최고정보관리자 협의회(CIO)가 작성한 보안항목에 대한 승인작업을 수행
- 국립표준기술연구소(NIST)는 보안기술을 개발하는 연구소로 환경에 따라 보안 설정을 적용/시험 할 수 있는 프로그램을 개발해고, 표준과 가이드라인을 개발하는 업무를 담당

---

5 Healthcare Information and Management Systems Society의 약자로 IT를 통한 건강 증진에 주력하는 세계 최대 규모의 비영리단체로, 의료기기의 사이버보안 수준을 평가하기 위한 측정도구로 MSD2를 제공
6 기존 보안 조치를 보완할 수 있는 추가적인 통제

• 최고정보관리자협의회(CIO)는 보안제도를 실행하는 기관으로서, 예산관리국(OMB)의 지시사항을 이행하기 위해 관련 업무에 대한 계획과 요구사항을 NIST와 함께 처리 및 진행

그림 _ 미 정부의 보안인증제도 구성 및 역할 개념도



[출처] KHNP

❑ FCC(Federal Communication Commission) 인증

▶ 미국 내에서 유통되는 모든 보안 제품은 미국 연방통신위원회(Federal Communications Commission, FCC)에 등록하고 등록번호를 부여받도록 규정

• 완제품이 아닌 보안 제품의 부품인 경우에도 FCC 등록 후 등록번호를 제품에 부착하도록 의무화
• 보안 제품 중 일부 카메라 제품, 데이터 저장을 위해 CD롬, DVD롬이 장착된 제품 등은 방사선(Radiation) 관련 FDA 등록이 필요
• 전파발생 장치에 대한 전파발생 기준을 설정하고 해당 제품을 그 기준에 의거하여 심사하고 인증
• 10KHz~3,000GHz의 주파수 대역을 유효하게 사용할 수 있도록 무선을 발사하는 각종 장치에 대해 승인하고, 무선을 이용한 통신장비에 대한 인증 및 불필요한 전자파장해(EMI) 등에 대한 규제와 승인업무 수행
• FCC 규정에 있는 기술적인 요구사항은 이동통신에 방해를 줄 수 있는 전파장애 크기를 제한하고 있으며, 몇몇 기기들에 대해서는 방해를 발생시킬 수 있는 잠재적인 성능까지 규제
• FCC 규정에 해당되는 대상 품목으로는 무선전화, 해상 구명장비 및 산업 /과학/의료용 고주파 장비,

송신기류, 저출력송신기, 수신기류, PC 및 주변기기, 방송수신기류, 전화선에 연결되는 장치(전화기, 팩스, 모뎀류) 등이 대표적

- 일반적인 디지털 도어록 제품은 제품인증 없이도 통관 가능하지만, 컴퓨터와 연결하여 출입 시에 카드를 사용하는 제품은 FCC 인증

▶ FCC 인증은 '인증'과 '검사확인' 등 두 가지 유형으로 구분되며 유형에 따라 요구 규정의 차이가 있음에 유의

- 첫째, 인증(Certification)은 제조자가 공인된 시험 장소에서 제품에 대한 검사를 받은 후 시험 보고서를 회로도, 블록다이어그램, 설명서 등과 함께 FCC에 송부하여 승인받는 제도
- 둘째, 검사확인(Verification)은 제조 및 수입업체가 공인시험소에서 검사를 통해 해당제품이 FCC 기준을 충족함을 확인하는 제도로서 시험보고서는 제조 및 수입업체가 자체 보관하도록 규정

▶ FCC 인증 절차는 다음과 같은 방식으로 진행

- 시험을 위한 적용 규격은 Communication Act(연방 통신법)와 Title 47 CFR(The Code of Federal Regulations: 연방법규집)이며, FCC 인증이 필요한 관련규정은 CFR(Code of Federal Register) 중 Title 47 (Telecommunications)에 설명
- 제품 검사는 FCC에서 공인된 시험소에서 실시되며, 불합격인 경우 FCC 신청이 불가
- FCC는 효율적인 인증관리를 위해 제품별로 FCC ID를 부착하도록 하고 있는데 동 ID 발급을 위해 Grantee Code 발급이 필요하며 인터넷을 통해 신청 가능
- 제품시험이 완료되고 FCC ID가 구성되면 인증신청 관련서류 등을 구비하여 FCC에 인증 신청 → FCC는 인증신청서류 검토 후 이상이 없으면 신청일로부터 4~6주 이후 인증서 발급

❑ UL(Underwriters Laboratory) 인증

▶ UL은 미국의 대표적인 비영리 안전시험기관으로서 UL이 제정한 UL규격은 미 연방정부의 강제 승인이 아닌 비강제 규격으로서 안전규격으로 사용하고 있으나 일부 주에서는 강제 규격으로 도입

- 시험 대상 품목은 가전기기 등 총 295개 품목이며, 제품을 시험한 후 해당 안전요구사항에 적합하다고 판정되면 UL은 제조자에게 UL마크 사용을 승인
- 사후관리 서비스 프로그램에 따라 주기적으로 공장검사를 통해 제품의 요구사항을 점검

▶ UL 인증의 효과 및 장점은 다음과 같이 요약

- UL은 오랜 기간 동안 축적된 경험을 통해 미국에서 안전시험 및 제품검정 증명 기관으로서의 확고한 위치를 차지
- 미국 내에서 UL의 신뢰성은 높이 평가되고 있으며, 소비자들의 선호도가 높기 때문에 생산업자, 판매상, 수입업자 대부분이 요구하고 있으므로 실제로 미국에 수출하기 위해서는 반드시 필요한 강제규격과 비슷한 효과를 발휘
- 미국 내 대형 소매업자 등은 UL 인증이 붙은 제품을 선호하고 있으며, 보험회사의 검사기관은 손해보험 위험도 평가에 있어서 UL마크의 유무를 확인

❑ CC(Common Criteria) 인증

▶ 이미 한 국가에서 평가받은 제품을 다른 평가기준을 사용하는 국가에 판매하기 위해서는 그 국가가 적용하는 평가기준을 활용하여 재평가 받아야만 수출을 할 수 있어, 이러한 번거로움을 해결하기 위해 미국을 비롯한 주요 국가들은 국제공통평가기준 CC에 합의

- 미국, 유럽 4개국(영국, 프랑스, 독일, 네덜란드), 캐나다는 각각 TCSEC(Trusted Computer Security Evaluation Center)(미국 1985년 제정), ITSEC(Information Technology Security Evaluation Criteria)(유럽 1992년 제정), CTCPEC(Canadian Trusted Computer Product Evaluation Criteria)(캐나다 1993년 제정) 등 자국의 평가기준을 사용하여 정보보안 제품을 평가해 왔음
- 평가 결과를 상호 인정하는 것을 목표로 단일화된 공통평가기준인 CC를 제정하여 적용하게 되면 평가과정 및 시간 절약, 평가비용의 절감에 따른 제품가격의 인하, 신속한 평가에 따른 새로운 제품개발의 가속화 등을 실현

❑ 연방정부 위험 및 인증관리프로그램(FedRAMP)

▶ 클라우드 업체가 클라우드 내 데이터에 충분한 보안 조처를 했는지 인증하는 제도로서 클라우드의 도입과 이용을 확산시키는 목적과도 연관

- 미 연방정부에 도입되는 클라우드 제품 및 서비스에 대한 보안성 평가 인증 및 지속적인 모니터링을 위해 도입
- 미 조달청(GSA)은 2012년 6월 공공분야 클라우드 보안인증 프로그램 FedRAMP (Federal Risk Authorization and Management Program)의 운영 및 게시 계획을 발표
- 클라우드에 특화된 보안 평가기준을 제시하여 신뢰성을 높이고 전문 평가 대행 기관(Third Party Assessment Organization, 3PAO)을 선정하여 일관성 있는 보안 평가 인증을 수행

- FedRAMP는 전문 평가 대행기관으로 연방정부 1곳과 민간 기업 8곳을 선정하고, 프로그램 운영을 시작

▶ 각 정부기관 및 민간분야와 학계가 협력해 개발한 FedRAMP 서비스는 기존의 보안인증 절차 간소화를 통해 인증 소요시간을 단축

- FedRAMP는 프로그램 운영을 맡고 있는 조달청과 NIST, CIO 위원회, 국방부, 국토안보부 및 관련 부처들 간에 2년 이상의 긴 협의 기간을 거치며 전체적 합의 도출에 성공
- 정부기관별로 수행하던 IT 시스템에 대한 보안성 평가를 클라우드에 한해 FedRAMP로 통합하여 비용, 시간 및 인력 절감을 기대

❑ USGCB(U.S. Government Configuration Baseline) 보안인증제도

▶ 연방기관에서 사용되는 모든 PC들이 안전한 보안 수준을 유지하도록 하기 위해 다양한 IT보안 침해행위로부터 연방기관내의 PC와 노트북 등을 보호하려는 PC보안 인증제도

- 사용자 접근권한 제한 등, PC의 설정항목을 표준으로 지정하여 보안수준을 향상 시키고 PC 공급에서 설정한 수준보다 엄격한 수준의 설정항목을 표준으로 사용하여, 위협과 취약점으로 인한 위험을 경감
- 접근권한 제한 등으로 인해 PC의 불필요한 동작이 감소하여 시스템 자원이 낭비되는 것을 방지하고 PC에 저장되어 있는 정보의 보안수준에 대해 구성원 모두가 신뢰하도록 함으로써 정부정보의 기밀성·무결성·가용성 확보에 대한 공감대 형성
- USGCB제도는 SCAP(The Security Content Automation Protocol)제도, FISMA(Federal Information Security Management Act) 제도 등 여러 IT보안 인증제도와 연계하여 미국 연방기관내의 IT기반시설 영역을 체계적이고 통합적으로 관리 및 감독

❑ 기타 부처 및 기관별 인증

▶ 미 국토부의 SAFETY 인증은 2002년 입법된 Homeland Security Act와 후속 법에 근거한 인증제도

- 테러 기반의 기술 판매를 억제하고 테러로부터 생명을 구할 수 있는 테러 방지 기술 개발 및 배포 제공처 혹은 기업을 인증
- 인증 신청 절차는 ①Applicant Account 생성→②Application 제출→③SAFETY Act가 요구한 정보 제출→④보험 인증→⑤패스워드 변경 후 완료의 순서로 진행

▶ 국가안전보장국(NSA)은 NIAP(National Information Assurance Partnership) 인증 제도를 통해 미 정부기관에 납품하는 정보보호제품관련 보안 규격 및 인증 테스트를 진행

- 기존의 보안성 평가는 정부기관의 사용 목적을 중심으로 진행되어 왔으나, 기술의 발전과 민간 분야에 사용되는 정보시스템에 대한 보증의 중요성을 반영
- 인증 신청 절차는 ①적용 보안 문제에 대한 서술→②보안 제품에 대한 설명→③인증 필요조건 교부→④인증 완료의 순서로 진행

4) 최근 정책 동향 및 이슈

▶ 미국 메릴랜드 주지사, 주 사이버보안 정책을 강화하기 위한 행정명령에 서명(2019.6)

- 2019년 5월 볼티모어 시 당국의 컴퓨터 시스템이 랜섬웨어 감염되면서, 시 당국의 서비스 대부분이 중단되는 사태를 초래
- 위 랜섬웨어 공격 발생 후 한 달여가 지난 시점에 메릴랜드 주지사가 사이버보안 강화를 위한 행정명령에 서명
- 해당 행정명령은 주정보보호최고책임자(SCISO)를 임명하고, 보안관리실 및 메릴랜드 사이버보안 조정 위원회(MCCC)를 신설하도록 지시

▶ 미국 트럼프 대통령은 2020년 연방 예산안에서 사이버 보안 개선에 약 110억 달러 요구(2019.3)

- 사이버 보안을 위해 요청된 예산은 부처 전체에 걸쳐 AI를 확장하고, 미국 사이버 전략 운영 및 통합노력을 계속하도록 독려를 목표
- 150페이지 분량의 문서 전체에서 사이버 보안은 여러 차례 나타났으며, 다양한 부문에서 국가 보안 카테고리로 분류
- 대부분의 예산은 국토안보부(DHS)와 국방부(DoD)에서 사용하나, 국방부의 상위 3개 사이버 임무에 거의 100억 달러 할당
- 예산은 최근 설립된 사이버 보안, 에너지 보안, 비상 대응 사무소를 위한 1억 5,600만 달러 규모 예산을 포함하여 여러 프로그램에 자금을 제공

▶ 새로 설치된 제 116대 의회는 사이버 보안 문제를 직접적으로 다루고 있는 법안이 하원에 30건, 상원에 7건 상정되어 있으며, 현재 5개 분야의 법안이 의제로 올라와 있음(2019.12)

- 정보 및 디지털 보안을 다루는 몇 가지 조항이 포함되어 있는 다른 법안들은 포함하지 않음
- 의회와 워싱턴에서 사이버 보안과 같은 복잡한 문제를 해결하는데 있어서의 핵심문제는 그 범위가 광범위하고, 상호 연결된다는 속성에서 기인하는 '확산된 책임'이라고 지적

입법 분야	관련 법
기반 시설 보안	• 민관 협력법을 통한 그리드 보안 강화 • 2019년 사이버 센스 법 • 에너지 비상 리더십법 • 파이프 라인 및 LNG 시설 사이버 보안 준비법 • 에너지 인프라 확보법
보안 인력	• 연방 교대 사이버 노동법 • 2019년 새로운 보안 관련 직업법
공급망 보안	• 중요 기술 및 보안 사무소를 설립하기 위한 법안
선거 보안	• 2019년 시민법 • SAFETi 법 • 글로벌 선거 교환법 • 조지아 지원법
버그 바운티[7]	• 국무부 해킹 법

5) 정보보호 스타트업 관련 정책 동향

▶ 미국 정부는 인공지능(AI) 분야의 연구 및 개발(R&D)에 투자를 확대하는 행정명령(Maintaining American Leadership in Artificial Intelligence)에 서명(2019.2)

- 동 행정명령 이후, 미 연방정부의 인공지능 연구개발 이니셔티브가 급속도로 강화
- AI R&D 전략 연구 우선순위는 기업이 해결하기 어려운 분야에 초점을 맞추고 있으며, 미국의 주도권 유지를 위한 R&D 투자를 강조
- 미 연방정부는 2016년 발표한 AI R&D 전략계획 발표 이후, 최근 AI R&D 이니셔티브를 지원하기 위해 해당 전략계획을 개정하여 ▲범용적 부문 ▲R&D 부문 ▲응용 부문의 총 3개 부문으로 구조화

7 기업이나 기관의 서비스 및 제품을 해킹해 취약점을 찾은 해커에게 보상금을 주는 제도

융합보안 시장 및 정책 동향

1) 융합보안 시장 현황[8]

▶ 미국 내 핀테크 관련 스타트업에 투자된 벤처캐피털(VC)은 2013년 24억 달러에서 2018년 109억 달러로 증가했으며, 투자 건수는 2013년 406건에서 2018년 627건으로 증가

▶ Forbes에 따르면, 2019년 미국의 블록체인 기술은 ▲모바일 결제 ▲공급체인망(SCM) 관리 ▲개인식별 정보 관련 보안산업 분야에서 활용도가 높아질 것으로 전망

- 벤처 및 스타트업 시장 분석 서비스 Crunchbase에 따르면, 2017년부터 2018년 2월까지 블록체인 스타트업 펀딩유치 국가별 순위는 미국(38%), 싱가포르(17%), 영국(8%) 등으로, 미국이 암호화폐 부문에서 압도적인 우위를 점하고 있는 것으로 조사됨
- 조사기관 Crypto Fund Research에 따르면 미국 내 블록체인 스타트업이 활성화된 도시로는 샌프란시스코, 뉴욕, 시카고, LA 등의 순으로 나타남

스마트 의료

▶ 1990년대 원격의료의 형태로 태동해 온 스마트 의료는 점차 성장해 오다가 ICT를 비롯한 첨단 정보통신기술이 결합되면서 급성장세를 보이고 있으며, 의료시장 중 핵심 분야로 자리매김

- 배경에는 넓은 국토 면적으로 인해 의료 접근성 문제가 심각하고, 의료 서비스의 수요-공급이 지나치게 불균형적인데다 대면 진료를 받기에는 비용이 턱없이 높고 대기기간이 길기 때문
- 미국의 스마트 의료 시장은 24시간 원격의료 서비스를 제공하는 텔라닥(Teladoc)을 필두로 아메리칸웰(American Well), 닥터온디맨드(Doctor on demand)와 같은 가상진료 서비스를 제공하는 기업과 매케슨(Mckesson), GE헬스케어와 같이 의료기기에 사물인터넷 기능을 탑재하여 병원과 가정을 연결하는 의료기기 및 솔루션 개발에 중점을 두는 기업 등으로 구분되어 발전을 거듭해 가고 있음[9]

자율주행차

8 미국 스타트업 동향과 시사점, 한국무역협회 뉴욕 지부, 2019.2
9 https://news.joins.com/article/22858910

▶ 미국의 국제자동차기술자협회 SAE international은 자율주행의 기준을 Level 0부터 Level 6까지 나누어 정의하고 있으며, 현재 Level3(조건부자율주행)에서 Level4(고급자율주행)로 발전해 가고 있는 중

- 무조건부자율주행에 해당하는 Level5에 도달하기까지는 다소 시간이 걸릴 전망
- 규제 완화 속도가 빨랐던 캘리포니아 주에서만 현재 구글·애플 등 60개가 넘는 기업이 자율주행차 상용화 경쟁을 하고 있으며[10], 구글의 웨이모(Waymo)의 경우 2018년 12월 애리조나 주에서 세계 최초로 자율주행 택시 서비스 시작[11]

▶ 자율주행차량은 차량 공유서비스보다 대형트럭에 먼저 적용되어 상용화될 가능성이 높음[12]

- 물류 트럭이 주로 운행되는 고속도로 구간은 일반 도로보다 돌발상황이 적은 편이며, 트럭 운전자를 대체할 수 있으므로 물류비의 절감 효과가 기대되기 때문
- 웨이모(Waymo)의 경우, 애리조나 주에서 2017년에 주행 테스트를 한 바 있으며, 샌프란시스코 및 애틀랜타에서도 테스트 중이며, 애리조나에서 테스트를 재개할 예정[13]

2) 융합보안 정책 현황

▶ 미국 국립표준기술연구소(NIST)는 IoT의 사이버보안 및 개인정보보호 관리와 관련된 과제와 해결방안을 제시한 보고서인 'NISTIR 8228'[14]를 발간(2019.6)

- 개별 IoT 기기와 관련된 사이버보안 및 개인정보보호 위험성에 대한 연방 및 기타 기관들의 이해·관리 증진을 지원하기 위한 목적
- IT 기기에 대비한 IoT 기기의 특성을 토대로 사이버보안을 위한 IoT 기기 단에서의 위기 고려사항과 과제 및 해결책을 제시
- 동 문서는 ▲IoT 기기 기능 ▲사이버보안과 개인정보보호 위기 고려사항 ▲IoT 기기의 사이버보안·개인정보보호 위기 완화를 위한 과제 ▲과제 해결을 위한 권고 사항 등으로 구성
- NIST의 사이버보안 프레임워크와 SP 800-53의 동반 문서(companion document)로서 IoT 보안 문제 해결을 집중적으로 다루고 있음

▶ 미국 국립표준기술연구소(NIST) 산하 국가사이버보안역량센터(NCCoE)가 소기업·가정용 IoT 기기 보안 가이드(안)발표[15](2019.4)

---

10 https://www.hankyung.com/economy/article/2019100935081
11 http://www.hani.co.kr/arti/economy/it/873694.html
12 https://www.cnbc.com/2019/11/22/self-driving-trucks-likely-to-hit-the-roads-before-passenger-cars.html
13 https://techcrunch.com/2019/05/29/waymo-is-bringing-its-self-driving-trucks-back-to-arizona/
14 https://csrc.nist.gov/publications/detail/nistir/8228/final

- IoT 기기의 이용 확산에 따른 보안위협에 대처하기 위한 제조사 사용설명서(이하 MUD) 접근법 적용과 주요 이점을 제시
- 소기업·가정용 MUD 명세서 적용의 논리적·기술적 구조를 도출
- 소기업 및 가정의 IoT 네트워크에 MUD를 구현할 때 고려할 보안 요구사항 및 MUD 이용 시의 주요 권고사항 제시

▶ 미국 하원에 초당적 법안인 2019 IoT 사이버보안 개선법 발의(2019.3)

- 과거 법안들은 NIST에 대한 가이던스를 제한된 수준에서 제시하였으며, 전반적으로 OMB의 가이드라인 제정에 보다 집중
- 2019년 법안은 IoT 기기의 사이버보안에 대한 NIST의 조치 강화 노력을 반영해, IoT 사이버보안 기능 구현을 위한 최저 요건을 중요하게 다루고 있음
- 법안은 크게 ▲IoT 기기 정의 ▲NIST 권고 사항 ▲부처 대응 정책 ▲가이던스 개발 등의 내용으로 구성

스마트 의료

▶ 각 주 별로 제도에 있어 어느 정도 차이는 있지만 일반적으로 대부분의 주가 원격의료와 관련해서는 적극적 장려 정책을 펼치고 있으며 대면진료와 동등한 의료행위로 간주하는 것이 특징[16]

- 대부분의 주가 원격의료동등법(Telehealth Parity Law)를 도입, 원격진료에도 대면진료와 동일한 보험 처리가 가능하도록 하여 환자로 하여금 원격의료를 손쉽게 선택할 수 있도록 함
- 원격의료에 활용되는 기기 및 진료 시스템 또한 일반적인 의료법의 적용대상이 되므로, 소프트웨어는 1996년 제정된 미국 의료정보보호법, 하드웨어는 식품의약국(FDA)의 501(k) 프로그램을 따르도록 하고 있음

자율주행차

▶ 주마다 차이는 있지만 자율주행 기술 자체를 금지하는 곳은 없으며, 주마다 다양한 수준의 자율주행 관련 정책을 가짐[17]

---

15 https://www.nccoe.nist.gov/projects/building-blocks/mitigating-iot-based-ddos
16 https://news.joins.com/article/22858910
17 https://www.lifewire.com/are-self-driving-cars-legal-4587765

- 아직 법제가 마련되지 않은 주, 자율주행 차량을 허용하지만 안전 요원 운전자가 동승하는 것을 조건으로 하는 주, 전면적으로 자율주행 차량을 허용하는 주 등으로 나뉘며, 전면적 자율주행을 허용하는 곳으로 캘리포니아, 애리조나, 플로리다 등을 들 수 있음

▶ 최근 주 정부를 중심으로 자율주행 대중교통을 시범 운행하는 파일럿 프로젝트가 진행 중[18]

- 미국 주요 도시에서 무인자동차 셔틀버스 서비스가 일반 대중을 대상으로 제공됨
- 2019년 11월 현재 디트로이트, 워싱턴DC, 오하이오 주 콜럼버스, 올랜도, 피닉스, 뉴욕-뉴저지 등에서 파일럿 프로젝트가 시행 중이거나 실시 예정
- 환경 친화적이며 출퇴근 시간대의 교통체증을 낮추는 등 경제성이 높아 자율주행차가 대중교통 시스템에 도입되는 현상은 더욱 가속화될 것으로 전망

18 https://news.kotra.or.kr/user/globalAllBbs/kotranews/list/781/globalBbsDataAllView.do?dataIdx=179116&column=&search=&searchAreaCd=&searchNationCd=&searchTradeCd=&searchStartDate=&searchEndDate=&searchCategoryIdxs=&searchIndustryCateIdx=&searchItemName=&searchItemCode=&page=9&row=10

나. 일본

'18년 GDP(십억달러)	4,972
'18년 인구수(천명)	126,785

■ ITU 글로벌 사이버보안 지수(Global Cybersecurity Index, GCI)

· 2017년 평가에 비해 지수는 0.1가량 큰폭으로 상승했으나 전 세계 순위는 다소 밀려나 일본이 14위, 한국이 15위를 각각 기록하며 올해도 10위권 밖에 머무름

국가명	2018		2017		전년대비 증감	
	지수	순위	지수	순위	지수	순위
일본	0.880	14	0.786	11	+0.094	-3
대한민국	0.873	15	0.782	13	+0.091	-2

■ ICT 관련 주요 지수

· 일본의 전반적인 ICT 발전 수준은 전 세계 약 10% 이내의 상위권을 유지하고 있음

지표명	일본		한국	
	점수	순위	점수	순위
IMD 국가경쟁력지수(2019)	-	30	-	28
IMD 디지털경쟁력지수(2019)	-	23	-	10
UNCTAD 전자상거래지수(2019)	87.6	24	89.4	19
ITU 글로벌 사이버보안 지수(GCI 2018)	0.880	14	0.873	15
UN 전자정부 지수(2018)	0.878	10	0.901	3

■ ICT 관련 주요 통계(ITU, 2018년 말 기준)

· 일본의 유선 및 이동통신(ICT) 이용 및 보급률은 세계 최고 수준으로 우리나라와 비슷

항목	일본		한국	
	가입자수(천 명)	보급률(%)	가입자수(천 명)	보급률(%)
유선전화	63,442	49.88	25.906	50.63
유선브로드밴드	40,910	32.16	21,286	41.60
이동통신	177,067	139.20	66,356	129.67
인터넷 이용률	84.59%(2017년 말 기준)		95.90%	

정보보호 산업 개요

1) 보안 환경

▶ 물리보안 시장 환경은 2020년 도쿄 올림픽을 앞두고 감시 카메라, 영상 종합 관리 소프트웨어, 드론 등 각종 보안 장비에 대한 수요 환경이 개선되고 있는 중

- 그러나 첨단 보안 기술을 응용한 장비 분야에서는 저가 해외 제품의 일본 시장 진출에 늘어나며 시장 내 경쟁 강도는 강화되는 양상

▶ 잦은 지진을 비롯한 자연재해에 자주 노출되는 일본 정보보안 시장에서는 데이터 백업을 위한 클라우드 컴퓨팅에 대한 수요가 지속적으로 상승 중

- 일본은 2009년부터 클라우드 컴퓨팅 산업 육성 정책을 실시해오고 있는 가운데, 2017년 말 시점 클라우드 보안 산업 시장 규모는 96억 엔을 형성했으며 2022년까지 18.0%의 연평균 성장률을 기록할 것으로 전망(IDC Japan, 2018.10)

▶ 2018년 이후 사이버보안법 개정안 확정 및 사이버보안전략 업데이트 등을 통해 사이버 보안전략본부의 기능 확대와 국가 정보보호 역량 결집을 위한 체계를 강화

- 주요기반시설과 정부 및 조직 단위에서의 각종 사이버보안 안전과 관련된 지침과 가이드라인 마련을 통해 구체적인 대응 요령이 확산

▶ IoT, 5G, 인공지능(AI), 클라우드와 같은 혁신적 기술의 보안 응용이 확대되면서 보안 시스템 분야의 새로운 수요가 지속적으로 형성

- 단순한 보안 기능 이외에 사회 인프라 솔루션이나 기업의 백오피스 업무 시스템과의 융합 등 새로운 시스템 서비스 개발이 진행되며 새로운 시장이 탄생
- IP카메라 분야는 동영상 해석 기술 도입이 가시화되며 AI 기술력을 보유한 기업들의 보안 시장 진출이 가시화
- 신기술의 도입은 광역 네트워크 스캔 방식의 경량화, 하드웨어 취약성 대응, 5G 네트워크 보안 기술, AI를 활용한 사이버 공격 검지 해석 기술 등에 대한 개발 수요를 촉발
- 또한 이러한 최신 기술의 도입을 위해 업종 간 제휴가 가속화되고 있어 업계 판도의 변화도 함께 발생

2) 인터넷 및 통신 환경

▶ 유선통신(고정형 브로드밴드)

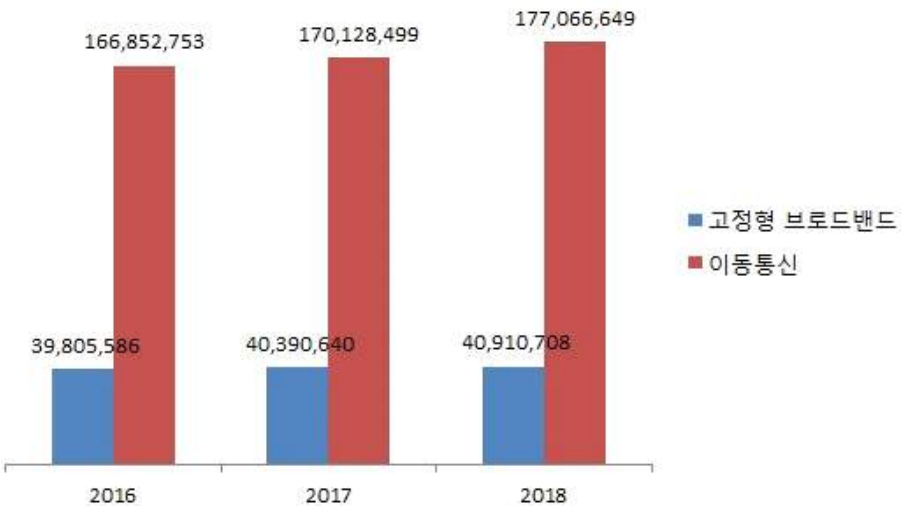
- 일본의 고정형 브로드밴드 가입 회선 수는 매년 미미한 증가세를 보이며 포화 상태에 근접 중
- ITU에 따르면, 2018년 말 일본 브로드밴드 인터넷 가입 회선 수는 4,091만 708회선으로 전년 대비 1.3% 증가
- 일본은 지진, 태풍 등 자연재해가 잦은 지리적·환경적 요인으로 인해 유선 대비 이동통신에 대한 기술 의존도가 높으며, 향후 이동통신 중심으로 투자가 확대될 것으로 예상

▶ 이동통신

- ITU에 따르면 일본의 이동통신 보급률은 2011년에 100%를 돌파했으며, 2018년 일본의 이동통신 가입자 수는 1억 7,706만 6,649명으로 보급률이 139.2%
- 높은 이동통신 보급률에도 가입자 수는 복수 단말 이용자 확대로 인해 매년 증가하고 있는 가운데, 2018년은 전년 대비 1.5%의 가입자 증가를 기록
- 일본 이동통신 시장 역시 국내와 마찬가지로 3G에서 4G LTE로의 이행이 신속히 이뤄졌으며, 5G는 2020년 중반을 전후로 각 통신사업자들이 개시할 전망
- 네트워크와 디바이스의 고도화에 따른 사물인터넷(IoT), 클라우드, 스마트 시티 등 ICT 융합 분야의 성장 토대가 견고하게 구축되고 있는 중

그림 _일본 인터넷 및 통신 환경: 2016-2018

(단위: 명)



[출처] ITU(2019.7)

정보보호 시장 현황

1) 시장 규모

시장 개요

▶ (물리보안) 2020년 도쿄 올림픽 개최에 따른 신규 수요가 늘어날 것으로 예상되나, 저가 해외 제품의 일본 시장 진출에 따라 시장 경쟁은 더욱 격화되고 있는 양상

- 시장조사기관 후지케이자이(富士経済)의 조사[19]에 따르면, 사회 정세 및 환경 변화에 따라 보안 대책(방범·방재·긴급 대응)에 대한 요구가 확대·다양화되어 가는 가운데, 보안 기기/시스템, 서비스 수요도 변화
- 최근 동영상 해석 기술이나 인공지능(AI), 클라우드와 같은 혁신적 기술을 보안에 응용하여 고도화된 보안 시스템을 구축
- 보안 분야뿐만 아니라 사회 인프라 솔루션이나 기업의 백오피스 시스템과의 융합을 통한 혁신적 시스템과 서비스 개발이 이뤄짐에 따라 새로운 시장이 탄생하며, 이에 따른 업종 간 제휴 가속화 및 업계 재편의 변화 조짐이 발생

▶ (정보보안) 2018년 일본 정보보안 업계에서는 전년도의 'WannaCry'와 같은 대규모 보안 피해 사례는 발생되지 않으며 2019년 이후에도 소비세 증세에 따른 경기 후퇴 리스크로 시장 성장에 제약이 있을 것으로 예상

- 2019년 G20 정상회의와 럭비 월드컵, 2020년 도쿄 올림픽/패럴림픽 등 국제 행사로 인한 사이버 공격 가능성 증대로 보안 관련 제품 및 서비스 수요가 늘어날 것으로 예상
- EU GDPR, 미국 정부 조달 관리 상의 중요 정보(CUI, Controlled Unclassified Information) 보호를 위한 보안대책 기준인 NIST SP800-171 등 해외에서의 데이터 보호 규제 강화에 따라 일본 보안 업계에서도 해당 기준 충족 요구가 높아지는 상황
- 또한 일본 개인정보보호법 개정과 관공서 퍼블릭 클라우드 서비스 활용 촉진 일환으로 미국의 FedRAMP(Federal Risk and Authorization Management Program)와 유사한 프로그램 추진을 검토 중
- 기술적으로는 AI, IoT, 로보틱스, AR/VR 등을 통해 디지털 혁신이 공공과 민간에서 가속화되고 있는 가운데, 데이터의 신뢰성 유지와 이를 통한 비즈니스 지속성 담보 중요성이 제기

---

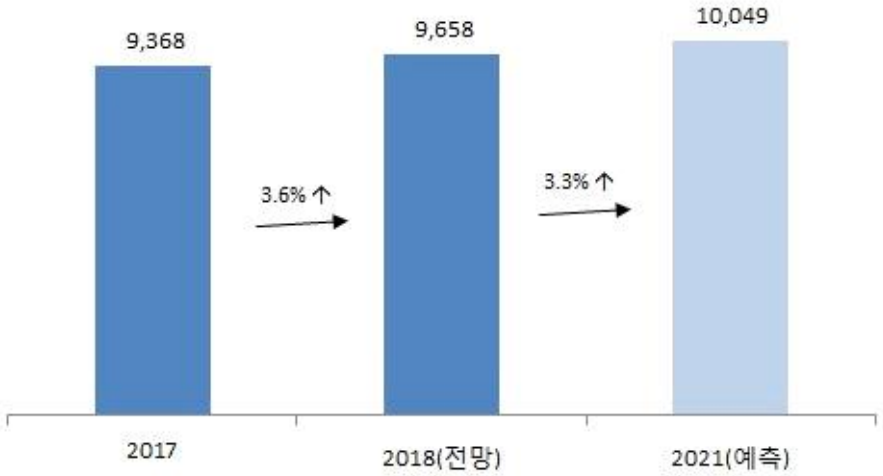
19 富士経済, 監視カメラ・アクセスコントロールシステム・緊急通報サービス・災害・防災関連機器/サービスなど国内のセキュリティ関連機器・システム・サービスの市場を調査, 2018.11

시장 규모 및 성장률

▶ 시장조사기관 후지케이자이(富士経済)에 따르면, 2018년 일본의 물리보안 시장 규모는 2017년 대비 3.6% 성장한 9,658억 엔으로 추정했으며, 2021년에는 1조 엔을 넘어서는 시장을 형성할 것으로 전망

그림 _ 일본 물리보안 시장 규모

(단위: 억 엔)



[출처] 富士経済(2018.11)

• 분야별로는 2018년 한 해 교체 수요가 활발했던 접근 제어와 재해·방재 관련 기기/서비스가 높은 성장을 보였으며 이외 감시 카메라 시스템, 자동차, 가정용 기기/서비스 분야 등도 3% 이상 성장

표 _ 일본 물리보안 하위 시장 규모(단위: 억 엔)

물리보안 시장 규모(단위: 억 엔)	2017	2018(전망)	2021(예측)
감시카메라 시스템	845	875	873
접근 제어	546	589	694
이벤트 감시/통보관련 기기	4,545	4,636	4,647
자동차	81	84	89
가정용 기기/서비스	2,389	2,465	2,598
재해 및 방재 관련 기기/서비스	963	1,008	1,149
보안 관련 비즈니스	9,368	9,658	10,049

[출처] 富士経済(2018.11)

• 2018년 이후에도 전반적으로 꾸준한 성장세가 예상되나 기대를 모았던 2020년 도쿄 올림픽과 관련된

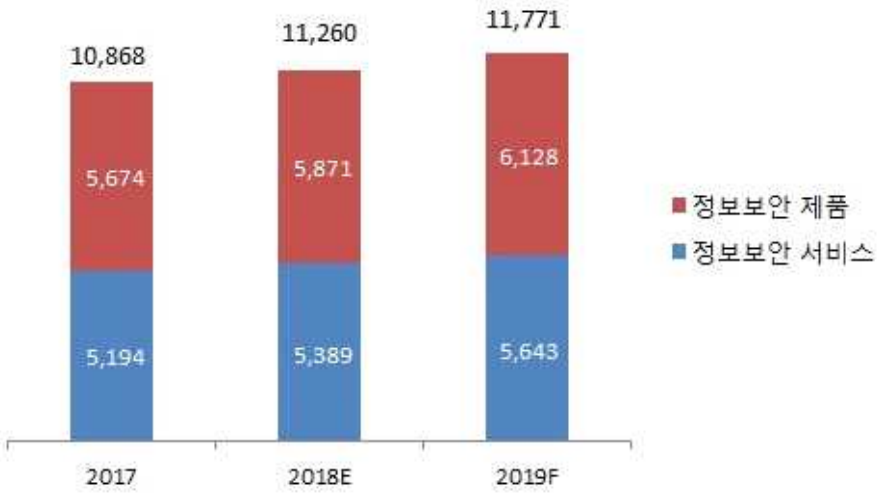
특수는 예상을 밑돌고 있는 상황으로, 향후 동영상 해석, AI, IoT 등의 기술혁신을 통한 새로운 분야에서의 수요 개척을 기대

▶ 일본네트워크보안협회(JNSA)가 일본 내 정보보안 제품과 서비스를 제공하는 사업자를 대상으로 한 조사[20]에 따르면, 2018년 일본의 정보보안 시장규모는 전년대비 3.6% 성장하여 9,658억 엔으로 추산

- JNSA에 따르면 2018년 정보보안 시장은 정보보안 제품 시장이 5,871억 엔, 정보보안 서비스 시장이 5,389억 엔을 기록하며 전년 대비 각각 3.5%, 3.8%의 성장하여 전체 정보보안 시장은 3.6%가 성장한 것으로 나타남
- 2017년 이후 일본 정보보안 시장은 1조 엔대의 규모를 형성한 가운데 2019년은 1조 1,771억 엔으로 성장할 전망

그림 _ 일본 정보보안 시장 규모 추이

(단위 억 엔)



[출처] 일본네트워크보안협회(JNSA)(2019.5)

- 정보보안 제품 시장은 통합형 어플라이언스, 네트워크 위협 대응 제품, 콘텐츠 보안 대응 제품, ID 액세스 관리 제품, 시스템 보안 관리 제품, 암호화 제품 등으로 구성
- 정보보안 서비스 시장은 정보 보안 컨설팅, 보안 시스템 구축 서비스, 보안 운용 관리 서비스, 정보 보안 교육, 정보 보안 보험 등으로 구성

▶ 2018년 정보보안 제품 시장에서는 콘텐츠 보안 대응 제품이 전체 시장의 37.7%(2,211억 엔)를 차지하며

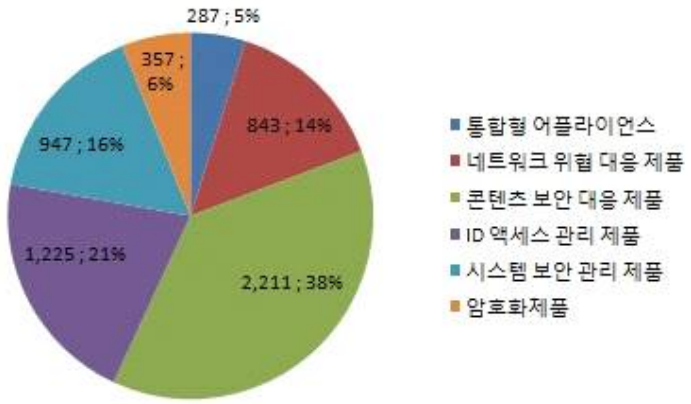
20 日本ネットワークセキュリティ協会(JNSA), 2018年度 国内情報セキュリティ市場調査, 2019.6

가장 큰 비중을 차지

• 이어서 ID 액세스 관리 제품(20.9%), 시스템보안 관리 제품(16.1%) 등이 높은 비중을 차지한 것으로 추산

그림 _ 2019년 일본 정보보안 제품 시장 구성 추산치

(단위 억 엔)



[출처] 일본네트워크보안협회(JNSA)(2019.5)

▶ 2018년 정보보안 서비스 시장에서는 정보보안 운용 관리 서비스가 전체 시장의 47.2%(2,542억 엔)를 차지하며 가장 큰 비중을 차지

• 정보보안시스템 구축 서비스(21.7%), 정보보안 컨설팅(20.3%) 등이 그 뒤를 따르는 것으로 추정

그림 _ 2018년 일본 정보보안 서비스 시장 구성 추산치

(단위 억 엔)



[출처] 일본네트워크보안협회(JNSA)(2019.5)

▶ JNSA에 따르면 2019년 정보보안 시장은 전년 대비 4.5% 성장한 1조 1,771억 엔의 규모에 이를 전망

- 정보보안 제품 시장이 6,128억 엔, 정보보안 서비스 시장이 5,643억 엔을 기록하며 전년 대비 각각 4.4%, 4.7%의 성장률을 기록
- 2019년 정보보안 제품 시장에서는 콘텐츠 보안 대응 제품이 전체 시장의 37.5%(2,299억 엔)를 차지하며 가장 큰 비중을 차지하며, 이어서 ID 액세스 관리 제품(21.1%), 시스템보안 관리 제품(16.2%) 등이 높은 비중을 차지할 것으로 예상

그림 _ 2019년 일본 정보보안 제품 시장 구성 전망치

(단위 억 엔)



[출처] 일본네트워크보안협회(JNSA)(2019.5)

- 2019년 정보보안 서비스 시장에서는 정보보안 운용 관리 서비스가 전체 시장의 47.3%(2,669억 엔)를 차지하며 가장 큰 비중을 차지하며, 정보보안 시스템 구축 서비스(21.4%), 정보보안 컨설팅(20.4%) 등이 뒤를 이을 것으로 예상

그림 _ 2019년 일본 정보보안 서비스 시장 구성 추산치

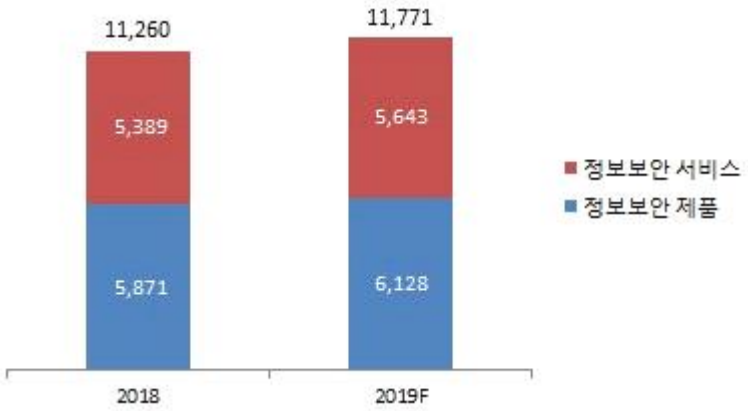
(단위 억 엔)



[출처] 일본네트워크보안협회(JNSA)(2019.5)

그림 _ 일본 정보보안 시장 규모 전망

(단위: 억 엔)



[출처] 일본네트워크보안협회(JNSA)(2019.5)

2) 분야별 현황

❍ 물리보안 제품 및 서비스

▶ 감시 카메라 분야

- 전체적인 IP카메라 시장은 확대 중인 가운데 아날로그 감시 카메라인 AHD와 HD-TVI 시장은 성장 중인 반면, 전통적 아날로그 CCTV 카메라 시장은 축소 중
- 영상 종합 관리 소프트웨어는 대규모 프로젝트 감소로 인해 시장이 일시적으로 축소했으나 2018년 이후 수요 회복 전망
- 가정용 감시카메라는 인지도 상승과 함께 제품 라인업을 강화하며 시장 확대 중
- 대형 감시 카메라 벤더들의 경우 동영상 해석 기술을 활용한 솔루션 서비스의 개발에 주력 중으로, 이상 발생 시 알람, 위험한 상황이나 사물의 검지, 매장이나 공장 내 사람의 행동 분석, 동선 분석 등에 해당 기술을 적용
- AI 기반의 감시 카메라 분석 기술은 아직은 고가의 장비 특성으로 인해 시장이 제한적이나, 향후 특정 시장에 겨냥한 특화된 시장을 중심으로 시장 저변을 점차 확대할 것으로 전망

▶ 접근 제어 분야

- 접근 제어 분야는 입·퇴실 관리 시스템의 경우 교체 및 증설 수요를 중심으로 꾸준히 수요가 확대

- 바이오 메트릭스 분야의 얼굴 인증과 정맥 인증은 2요소·다요소인증 확산과 새로운 용도의 시장 확대에 힘입어 시장 확대 지속

▶ 이벤트 감시/신고 분야

- 이벤트 감시/신고 관련 기기는 법인용 기계 경비 서비스나, 기계 경비 서비스 전용 침입센서 시장이 꾸준한 성장세를 유지
- 경비용 로봇/드론 관련 서비스 시장은 아직 개화되지 않은 상태이나 2020년 도쿄 올림픽을 위한 개발과 신제품의 투입이 가시화
- 이외 시장 규모 자체는 크지 않으나 동영상 해석과 AI 등의 기술 도입이 본격화될 것으로 예상

▶ 자동차 분야

- 일본 역시 최근 보복 운전(あおり運転)이 기승을 부리며 사회적 문제로 부각되고 있는 가운데 이에 대비한 업무용 주행 기록 기기 시장이 성장
- 후부 도난 방지 장치는 자동차 도난 건수 감소와 자동차 자체의 보안 기능 향상에 기여하고 있으며, 이와 동시에 2017년 2018년 블랙박스 기기 및 세트 판매도 꾸준히 확대

▶ 재난 방재 관련 기기/서비스 분야

- 화재예보 설비 시장이 교체 수요로 인해 순조로운 확산세를 보이고 있으며, 가스 누출 경보기는 설치 의무화 대상의 시설이 한정적으로 시장 정체 상황을 맞이
- 이외 긴급 지진 속보 대응 단말과 이재민 안부 확인 서비스는 아파트 시장을 중심으로 꾸준히 도입이 확산

▶ 가정용 기기/서비스 분야

- 가정용 기기/서비스가 전반적으로 안정적인 시장 확대를 이어가고 있는 가운데, 고령자 재실 안부 확인 서비스나 아동의 등하교 지킴이 서비스 등의 다양한 서비스 개발과 함께 꾸준한 성장을 유지
- 단독 주택이나 아파트 등 다양한 주거 형태에 걸쳐 전반적으로 수요는 꾸준히 증가 추세로, 사회 안전망의 강화로 인해 도둑이나 침입 건수는 크게 감소하고 있으나, 가정용 보안에 대한 잠재 수요는 여전히 높아 시장은 꾸준한 확대가 예상
- IoT 기능을 갖춘 주택의 관련 솔루션에 대한 잠재 수요가 있으나, 사용자의 편의성과 간편한 조작성 등이 주요 시장 과제
- 한편 주택 정보반이나 텔레비전 도어폰, 방범락 등의 주택용 방범 기기는 재구매 수요가 안정적으로 이어지는 상황

정보보안 제품

▶ 콘텐츠 보안 대응 제품

- 정보보안 제품군에서 가장 큰 비중을 차지하는 콘텐츠 보안 대응 제품은 2017년 실적치 기준으로 2,154억 엔을 기록하며 2016년 1,892억 엔 대비 13.9% 증가
- 콘텐츠 보안 대응 제품군 중에서는 엔터프라이즈용 바이러스/부정 프로그램 대책 소프트웨어가 735억 엔으로 가장 큰 비중(34%)을 차지했으며, 이어서 개인용 바이러스/부정프로그램 대책 소프트웨어와 데이터유출방지(DLP) 제품이 각각 446억 엔과 300억 엔으로 뒤를 이음
- 콘텐츠 보안 대응 제품 시장은 엔터프라이즈용 바이러스/부정 프로그램 대책 소프트웨어는 감소했으나, 개인용은 증가세를 보였으며, 특히 사무자동화 기업들로부터의 데이터유출방지 관련 제품 수요가 크게 증가

▶ 네트워크 위협 대응 제품

- 네트워크 위협 대응 제품 및 통합형 어플라이언스는 2017년 실적치 기준 826억 엔으로 2016년 766억 엔 대비 7.8%로 성장세가 둔화
- 이 제품군 중에서는 방화벽 어플라이언스/소프트웨어가 전체의 32%인 268억 엔으로 가장 큰 비중을 차지하며, 이어서 IDS/IPS 어플라이언스/소프트웨어와 VPN 어플라이언스/소프트웨어가 각각 192억 엔, 187억 엔으로 각각 23%대의 시장을 형성
- 매년 가장 두드러진 성장세를 보이고 있는 분야로는 웹애플리케이션 방화벽으로 2017년 실적치 기준 161억 엔으로 전체 시장의 20%선을 돌파

▶ ID 액세스 관리 제품

- ID 액세스 관리 제품은 2017년 실적치 기준 1,180억 엔의 규모를 달성하며 최초로 1,000억 엔대를 돌파한 가운데, 2016년 922억 엔 대비 27.9%의 성장을 기록
- 개인 인증용 생체인증 기기 및 시스템 수요의 경우 전년 대비 126.7%로 가장 높은 성장세를 보이며 258억 엔의 시장 규모를 달성
- 반면 PKI 시스템 및 기타 컴포넌트와 기타 아이디 액세스 관리 제품은 각각 –18.3%와 –67.2%로 시장이 감소

▶ 시스템 보안 관리 제품

- 시스템 보안 관리 제품은 2017년 실적치 기준 870억 엔으로 2016년 787억 엔 대비 10.5% 성장
- 하위 제품군 중에서는 보안정보 관리 시스템 및 제품이 359억 엔으로 전체 시장의 40%를 차지했으며, 이어서 정책관리·설정관리·동작감시·제어제품이 320억 엔(37%), 취약성검사제품이 164억 엔(19%)의

시장을 형성

- 2017년은 관리 계열의 기기에 대한 수요가 급증했으며 취약성검사제품 역시 동반 수요 확대
- 최근 표적형 공격 대책의 일환으로 내부 네트워크 트래픽의 이상을 상시 감시하기 위한 필요성이 증대하며 보안정보관리 시스템에 대한 수요가 늘어나고 있는 중

정보보안 서비스

▶ 보안시스템 구축 서비스

- 보안시스템 구축 서비스는 2017년 실적치 기준 1,155억 엔으로 2016년 1,273억 엔 대비 9.3%가 감소하며, 2014년 정점을 찍은 뒤 지속적인 마이너스 성장을 기록
- 이는 그동안 보안시스템 구축 중심의 시장이 클라우드 기반 운영 관리 중심으로 전환되고 있는 추세를 반영한 시장 다이내믹스의 변화에 기인
- 2017년은 SI 대기업의 대형 프로젝트 수주가 감소한 반면 중소 규모 수요는 증가
- 모든 업종과 업태에 걸쳐 IT 수요가 늘어나고 있는 추세로 2019년 이후 저가화와 수요량의 증가가 이뤄지며 시장이 새롭게 반전될 가능성도 존재

▶ 보안 운용 및 관리 서비스

- 보안 운용 및 관리 서비스는 2017년 실적치 기준 2,444억 엔으로 2016년 1,970억 엔 대비 24.0% 증가
- 동 서비스는 파편화된 다양한 하위 서비스들로 구성되어 있으며, 보안종합감시/운용지원 서비스가 497억 엔으로 이 시장의 20%를 차지하고 있으며, 이어서 취약성검사 서비스방화벽 감시·운용지원 서비스가 각각 369억 엔(15%), 306억 엔(13%)을 차지
- 최근에는 정보보안 컨설팅 및 보안시스템 구축으로부터 관리형 서비스로 수요 전환이 이뤄지며 운용 관리에 자금을 투입하는 기업이 늘어나고 있는 추세
- 전통적으로 동 시장을 견인해 온 SOC를 대신해 취약성검사, 정보제공, 전자인증, 사고대응 관련 서비스가 빠른 속도로 성장 중
- 컨설팅과 감사·교육 등의 수요 성장에 따라 취약성검사와 관련된 수요가 점차 보편화되고 있는 추세
- 이외 모바일/스마트 기기 시장에서의 전자인증 관련 수요도 본격적인 확장 조짐을 보이고 있는 중

▶ 정보보안컨설팅

- 매출 면에서 세 번째 규모인 정보보안컨설팅은 경영 관리 관점에서 전문가 지원을 활용하는 요소가 강하여, 경영 카운슬링의 개념과 유사하기 때문에 회계감사법인계, SI계, 독립계 등 다양한 사업자가 서비스를 제공 중

- 2017년 실적치 기준으로 정보보안컨설팅 시장 규모는 1,053억 엔으로 2016년 787억 엔 대비 33.8%의 성장을 기록
- 정보보안컨설팅 분야에서는 정보보안정책구축 지원/관리 전반 컨설팅이 2017년 기준 492억 엔으로 전체 시장의 47%로 가장 큰 비중을 차지
- 이어서 정보보안 진단/감사 서비스와 정보보안 관련 규격 인증 취득 지원 서비스가 각각 281억 엔(27%)과 183억 엔(17%)을 차지
- 전통적으로 일본 정보보안컨설팅 수요의 확대는 ▲2005년 4월부터 전면 시행된 개인정보보호법 ▲2008년 4월 회계연도부터 적용된 내부통제보고제도(J-Sox) ▲2004년 10월 니가타 현 주에쓰(新潟県中越)에서 발생한 대지진 및 신형 인플루엔자를 계기로 한 사업지속 계획(BCP) 등에 대한 관심에서 기인
- 이는 리스크 관리 계열의 컴플라이언스 전문가에 의한 컨설팅의 비즈니스 수요를 확대시켰으며, 프라이버시 마크(P마크)와 정보보호관리체계(ISMS) 인증에 대한 고객들의 니즈가 강화
- 최근 감소세를 보였던 정보보안 컨설팅 시장이 최근에는 모바일화 진전에 힘입어 관련 컨설팅 수요가 회복되는 양상
- 특히 진단감사, 규격인증, 심사 등의 분야는 전년 대비 시장 규모가 2배로 확대

3) 주요 사업자 현황

❑ 물리보안

▶ Mitsubishi Electric

- 일본의 대표적 물리보안 기업의 하나로, 입·퇴실관리, 감시카메라, 주변감시시스템, 전자차단 시스템을 포함한 토탈 보안 솔루션을 제공
- 물리보안 분야에서 확보한 다양한 제품 라인업과 기술력을 토대로 기술 간 융합을 통해 빌딩 및 에너지 관리 등 인접 사업 영역과의 시너지를 도모
- 특히 Mitsubishi는 사이버보안 기능과의 결합을 통해 통합 보안을 강화하기 위해 2018년 4월 원자력 발전소 등 주요기반시설의 제어시스템에 대한 공격 방어를 위한 통합형 보안 제어시스템 개발에 착수
- 최근 동사는 다요소 인증 및 클라우드 보안 솔루션 개발을 강화 중인 가운데, 2019년 10월 지문인증 솔루션 개발사인 DDS에 B2B용 다요소 인증 'EVE 시리즈'와 'Themis', 클라우드 인증 서비스인 '클라우드 본인 인증 마가타마 서비스' 및 'B2C용 차세대 온라인 인증 규격인 FIDO(Fast IDentity Online) 기반 '마가타마 플랫폼' 등을 공급

▶ NEC

- 정보보안과 물리보안 공히 시장 경쟁력을 갖추고 있는 NEC는 컴퓨터 등 주요 장비에 대한 액세스 제어를 위해 안면인식 등의 바이오 인증 소프트웨어 기술(NeoFace Monitor)을 활용
- 해당 기술은 통합형 PC 보안 소프트웨어인 'InfoCage PC Security'와 패키지 형태로 시장에 판매되고 있으며, 2019년 7월 입퇴실, 안면정보 확인 등의 관리 서비스와 연계한 서비스 제공에 착수
- 2017년 2월에는 IC카드 인증 인쇄가 가능한 모노크롬 레이저 리더인 MultiWrite 8300을 출시
- 2018년 3월에는 클라우드 기반 서비스인 NEC Cloud IaaS에 대해 미국국립표준기술연구소(NIST)의 보안 표준인 NIST SP800-171 대응을 완료한 바 있음

▶ Hitachi

- 히타치 산업 컨트롤즈는 2019년 10월 히타치 제작소가 자체 개발한 AI 영상 해석 기술을 이용하여, 역, 공항, 상업 시설·공공 기관 등의 감시·경비 업무 효율화와 고도화를 지원하기 위한 '고속 인물 발견·추적 솔루션'에 대한 판매에 착수
- 이 솔루션은 방범 카메라 등의 영상에 나타나는 인물의 성별, 연령층, 복장 등 100개 항목 이상의 전신 특징을 이용하여 특정 인물 발견을 지원

▶ Photosynth

- Photosynth는 2014년 스마트폰과 주택 도어록을 결합한 스마트 도어록 컨셉트를 개발하며 일본 내 해당 분야의 선도적 플레이어 역할 주도
- 동사의 대표적 제품인 Akerun은 기존의 자물쇠에 별다른 설치 작업 없이 특수 접착용 테이프를 부착해서 이용이 가능한 설치 상의 이점도 존재
- Akerun은 스마트폰 앱 조작을 통해 본인은 물론 특정인에게 특정 기간 동안 키 개방 폐쇄 권한 부여까지 가능
- 2018년 4월 미츠이부동산은 법인용 다거점 공유 사무실 서비스인 Work Styling 서비스에 Akerun의 입퇴실 관리 시스템을 채택하여 도쿄도 내 3개 사무실에서 적용
- 동사는 스마트 도어록 및 자동문의 클라우드화를 위해 문과 일체화된 'Akerun Controller'를 2019년 6월부터 제공하여 사무실 노동 시간 파악, 고유 오피스 및 피트니스 센터 등의 운영을 합리화

❑ 정보보안[21]

21 일본 정보보안 분야에서 대기업이나 공공기관 및 교육기관을 대상으로 영업을 하기 위해서는 유지 보수 등을 위탁하고 있는 NEC, Fujitsu, Hitachi와 같은 대형 SI 및 엔드투엔드 솔루션 기업이나 NTT, KDDI 등의 메이저 통신사업자 및 관계사와의 협력이 효과적임. 또한 IT 및 정보보안 솔루션 진출은 대기업이나 중소기업에 네트워크, 데이터베이스, 시스템 등 IT분야별로 특화된 전문 SI업체를 통해 추진되기도 하는데, 이 경우에도 대형SI 업체나 지역SI 업체를 거치게 되므로 복잡한 유통단계가 형성

▶ Trend Micro

- 1989년 미국에서 설립된 이후 1992년 일본 소프트웨어 회사를 인수하며 도쿄로 본사를 옮긴 글로벌 보안 소프트웨어 개발사인 Trend Micro는 서버, 클라우드 컴퓨팅 및 기업용 보안 소프트웨어로 일본 시장의 1위를 점하고 있는 기업
- 2016년 8월에는 랜섬웨어로부터 데이터 보호 기능을 강화한 토탈 보안 솔루션인 'VirusBuster'의 업그레이드 버전을 출시
- 2017년 8월 초에는 HITRUST와 협력하여 헬스케어 산업용 사이버 위협 관리 및 대응센터(HITRUST Cyber Threat Management and Response Center)를 구축키로 함
- 동 센터에서는 의료 분야의 사이버 위협 정보를 공유하는 조직들을 중심으로 구축이 확대되고 있는 HITRUST Cyber Threat XChange(CTX) 기능을 강화
- 창립 30주년을 맞은 2018년 3월 말 Trend Micro는 법인, IoT 및 소비자 3개 시장을 대상으로 보안 감시 센터 관련 제품과 서비스를 새로운 주력 사업으로 추진할 것으로 발표한 바 있음
- 한편 클라우드 보안 시장 대응 강화를 위해 동사는 2019년 10월 클라우드 인프라 설정 관련 보안 솔루션 개발사인 Cloud Conformity를 인수

▶ Fujitsu

- 일본 정보보안 업계의 Top 3중 하나인 Fujitsu는 클라우드 보안과 바이오인증 등 차세대 보안 기술에 대한 투자에 적극적으로 나서고 있음
- Fujitsu는 바이오인증 기술 개발에 대한 투자도 적극적인 가운데, 2015년 10월에는 데이터 암호화와 복호화에 지문인식, 망막인식, 손바닥 혈관 인식과 같은 바이오인식 기반 보안 시스템을 구현할 계획을 발표
- 실제 2016년 9월에는 'Fujitsu Biometric Authentication PalmSecure-F Pro'와 'Fujitsu Biometric Authentication Palm Vein Authentication Board'의 두 가지 기술 개발에 완료하여 다양한 응용 보안 분야로 바이오인증 기술 적용을 확대키로 함
- 2017년 7월에는 미국 국토안보부가 추진하는 사이버 위협정보 공유 체제인 Automated Indicator Sharing(AIS)에 공동 대응키로 합의
- Fujitsu는 2016년 8월부터 사이버 공격 대책으로써 조직 간 위협 정보를 공유하기 위한 시스템을 개발, 운영해 오고 있으며, 양 기관의 협력에 따라 AIS가 제공하는 사이버 위협 정보와 동사의 위협 정보 활용 시스템을 연계키로 함
- 2018년 5월 Futjisu는 사이버공격 예측 검지에서부터 시스템 복구까지의 라이프 사이클을 일원적으로 지원하기 위한 서비스인 Fujitsu Security Solution Global 관리 보안 서비스의 신규 라인업을 발표
- 동사는 자체적으로 개발한 'IoT 보안 맵'을 통해 IoT 시스템 전반의 보안 대응을 지원하고 있는 가운데,

Fujitsu Social Science Laboratory가 2019년 10월에 개시한 'IoT 보안 서비스'용 IoT 기기 보안 대책을 위해 개발부터 운용까지 전 과정에 이 IoT 보안 맵을 적용

- 한편, 동사는 2021년 말까지 IoT 보안 서비스를 통해 3억 엔의 매출 달성을 목표로 설정

▶ Hitachi

- 여타 일본의 메이저 보안 기업과 마찬가지로 엔드투엔드 보안 솔루션을 제공하고 있는 Hitachi는 바이오인증 분야에서 지정맥(finger vein) 인증 기술의 앞선 경쟁력으로, 동 분야에서는 Fujitsu와 함께 지문인증 시장 점유율을 앞지르고 있음
- Hitachi는 MS의 클라우드 정보 공유 협업 플랫폼인 SharePoint의 보안 기능을 강화한 SharePoint 온라인 익명화 솔루션을 2016년 10월 말부터 제공하기 시작
- 동 솔루션은 SharePoint Online 상에서 사이버 공격에 대응하고 시스템 운영자의 파일 내용 탐색을 막기 위해 모든 정보를 자동적으로 암호화함과 동시에 전문 검색에 이용되는 검색 인덱스도 암호화하여 안전한 파일 보존이 가능
- 한편, 동사는 해외 경쟁력 있는 솔루션에 대한 자국 유통 사업도 활발하게 전개 중으로, 2016년 4월부터 머신러닝으로 사이버 공격을 미리 차단하는 솔루션을 개발한 미국 스타트업인 Cylance의 AI 탑재 엔드포인트 보안 제품인 Cylance PROTECT의 일본 대리점 역할도 수행
- 이외 국내 기업으로는 잉카인터넷, 시큐어소프트 등이 Hitachi에 보안 솔루션을 공급한 사례가 있음
- 한편 Hitachi Systems는 2017년 3월에는 인터넷에 접속된 감시카메라와 자판기 등의 IoT 기기에 대응한 사이버 공격을 검지하기 위한 서비스를 개발
- 동 서비스 개발에는 피싱 대응 솔루션 전문 개발사인 Security Brain이 IoT 기기에 대한 사이버 공격 기법과 경향을 분석하고 개발하는 업무를 담당
- 한편 2017년 12월에는 NEC, Fujitsu와 공동으로 늘어나는 사이버공격에 공동 대응 일환으로 '사이버보안 인재육성 스킴 책정 공동 프로젝트'를 통해 2,000명의 사이버보안 전문가 육성에 협력키로 함
- Hitachi Solutions는 2019년 6월 공개키 암호 기반 기술을 응용한 생체인증기반 제품인 Biometric Signature Server 판매에 착수하며, IC카드와 스마트폰 상의 생체 정보 저장 인증 기능과 함께 생체정보로 작성된 공개키는 PKI를 이용한 기존 시스템과의 연계성을 지원

▶ Vinx

- IT 및 보안 솔루션 전문 에이전트로, 자국 내 해외 기술 유통뿐만 아니라 중국 및 아시아 시장을 중심으로 활발한 해외 에이전트 활동을 전개 중
- 현재 확보하고 있는 보안 솔루션으로는 차세대통합운용솔루션의 Hybrid Series 중 Hybrid Security를 통해 액세스 관리, 데이터베이스 감시, 데이터베이스 유출 차단 기능 등을 지원

4) 주요 동향 및 이슈

물리보안

▶ 2020년 올림픽 특수는 예상에 미치지 못할 것으로 예측되는 가운데 AI, IoT 등 혁신 기술을 활용한 물리보안 솔루션 응용에 대한 기대감이 커지는 중

- 시장에서는 2020년 도쿄 올림픽 개최에 따른 수요에 대한 기대가 과도하다는 평가가 이뤄지고 있는 가운데, 동영상 해석, AI, IoT 등 첨단 혁신 기술을 활용한 신규 수요 창출에 보다 기대
- 첨단 기술 수요 활용 니즈가 커짐에 따라 자금력과 기술력을 확보한 메이저 제조 기업을 중심으로 한 물리 보안 시장 확대가 예상되며, 물리 보안에 특화된 AI 기술 개발 스타트업의 시장 진입이 예상
- 특히 하이엔드급 IP 감시 카메라 시장에서는 AI 기술과 동영상 분석 기술을 응용한 수요가 니치 시장을 형성하며 점차 확산될 조짐을 보이고 있음
- Fujitsu, Hitachi, Mitsubishi, NEC, Oki, Panasonic, Toshiba, Sony 등은 일본 물리보안 시장의 주요 업체로 활동 중

▶ 최근 단품 솔루션 판매에서 통합관리 솔루션 제공으로 시장 비중이 이동 중

- 향후 IT 벤더, 경비회사, 빌딩관리 회사 간의 연계가 점차 강화되는 동시에 복수의 거점에 대해 동시 포괄적인 보안 체제를 구축하는 것에 대한 수요가 늘어날 전망
- 특히 올림픽을 앞두고 다수를 대상으로 한 인증 시스템 수요도 늘어나며, 인증과 관련된 다양한 기술 개발이 진전될 것으로 예상
- 다수 인증 시스템, 통합 보안 관리 및 인증 데이터를 활용한 키워드로 이용이 확대될 전망

정보보안

▶ 글로벌 규제 환경 변화와 개인정보보호 기준이 강화됨에 따라 EU GDPR, NIST SP800-17 등의 데이터 보호 관련 규정의 제품 및 서비스 반영 수요 확산

- 개인정보 및 데이터 관련 인증 제도 보완에 따라 정보보안 교육 분야의 신규 수요 증가

▶ 클라우드 서비스에 대한 공공 수요가 늘어남에 따라 대규모 클라우드 기반 보안 솔루션 분야에서의 시장 경쟁 강화

- 보안시스템 구축 서비스는 클라우드 확산에 따라 상대적인 시장 위축을 맞고 있으나 클라우드 서비스 도입 확산에 따른 정보보안 컨설팅 및 취약성 검사 등의 수요는 크게 확대

▶ 금융권, 공공기관을 중심으로 한 바이오인증은 정부와 기업의 적극적 후원 속에 도쿄 올림픽을 전후로 가파른 속도의 보급 확산을 보일 것으로 전망

- 지정맥 인증은 일본 ATM에 이미 80%나 적용되고 있을 정도로 보편화된 인증 수단
- 최근 Fujitsu 등이 앞장 서 개발 중인 손바닥 정맥 인식 기술은 인식에 소요되는 시간이 1초에 불과한데다 기타 인증을 위한 별도의 과정을 거치지 않는 간편성으로 인해 높은 기술적 가치를 평가받고 있음
- 이처럼 정맥, 지문 인증 등의 바이오 인식 분야는 정보보안 영역의 새로운 화두로 부각하게 될 전망

5) 정보보호 스타트업 주요 동향 및 이슈

시장 규모 및 주요 동향

▶ 일본의 2018년 한 해 벤처 기업의 자금 조달 총액은 전년 대비 22.4%가 증가한 3,880억 엔에 이른 것으로 집계

- 이 중 10억 엔 이상의 대형 자금조달에 성공한 스타트업도 80개사(2017년 58개사)에 이름

그림 _ 일본 벤처 기업 자금조달액 및 1개사



[출처] Japan Startup Finance 2018, KOTRA 재인용[22]

22 https://news.kotra.or.kr/user/globalBbs/kotranews/7/globalBbsDataView.do?setIdx=245&dataIdx=177214

▶ 일본의 스타트업계는 개발 성과물의 완성도에 대한 기업의 높은 기대 때문에 반짝이는 아이디어에 기반한 과감한 혁신적 비즈니스 모델보다는 생산성 향상 및 수익에 직결되는 모델에 대한 선호도가 높은 편

▶ 정책 측면에서는 Society 5.0 실현을 위한 핵심 기반으로 스타트업 생태계 육성에 주목하고 있으며, 개방적 혁신을 통한 산학 협력을 집중적으로 지원

주요 기업 동향

▶ Flatt Security는 화이트 해커가 Web 애플리케이션을 공격·진단하는 취약성 진단 사업과 보안 제품 개발을 추진하는 도쿄대 스타트업 기업

- 2019년 7월 2억 2,000만 엔의 투자 자금을 유치한 Flatt은 클로즈드 베타 버전으로 2019년 말 시점 개발 제품을 검증 중인 단계

▶ Safie는 Safie 대응 카메라를 인터넷으로 연결하여 원격지에서 스마트폰이나 PC를 통해 실시간으로 현지의 영상·음성을 확인하는 클라우드 기반 녹화 플랫폼을 개발

- 동사는 2017년 9월 2억 2,000만 엔의 투자 자금을 유치한 Flatt은 클로즈드 베타 버전으로 2019년 말 시점 개발 오릭스, 칸사이전력, NEC캐피털 등으로부터 9억 7,000만 엔의 자금 조달을 유치하며 누적 13억 5,000만 엔의 투자를 달성
- 기존 감시카메라의 경우 전용 녹화 기기나 별도의 소프트웨어를 필요로 했으며 카메라 한 대 당 수십만 엔이 소요
- Safie는 클라우드 환경으로 서비스 이용이 가능하기 때문에 카메라 이외의 전문 장비는 불필요
- 동사는 투자에 참여한 각 회사들과의 제휴를 통해 영업 기반 확대를 도모함과 동시에 동영상 해석 제휴 등의 기술개발도 촉진할 예정
- 향후 거리나 지역, 시설의 방범이나 안전 관리뿐만이 아니라, 비즈니스의 효율화나 마케팅 지원 등으로 응용 영역을 확대하여, 단순한 감시 카메라가 아닌 미래를 가시화하는 동영상 해석 플랫폼 제공을 주요 목표로 설정

정보보호 정책 및 기관 현황

1) 관련 법령 및 정책

관련 법령 및 규제

▶ 스마트폰 개인정보보호 가이드라인

- 2012년 8월, 총무성이 발표한 '스마트폰 개인정보보호 가이드라인'에는 스마트폰 이용자의 정보보호에 대한 인식 현황 및 사업자들의 개인정보 활용 가이드라인을 제공
- 동 가이드라인에는 ▲준법적 수단을 통한 개인정보 수집 ▲애플리케이션 및 서비스 제공 관련 개인정보보호 강화 ▲개인정보 수집 및 활용에 대한 투명성 확보 ▲개인정보 보유 관련 보안 강화 ▲개인정보 수집 및 활용에 대한 이용자 불만 접수 시 대응 강화 등을 포함

▶ 개인정보보호법 개정안

- 2014년 6월, 일본 정부 산하 IT종합전략본부가 마련한 개인정보보호법 개정 초안은 빅데이터 활용에 사용되는 스마트폰의 위치정보 및 웹사이트 이용 이력 등 데이터 관리에 대한 제도적 근거를 마련
- 일본의 개인정보보호법은 지난 2003년 성립됐으나 이후 IT의 발달로 인터넷 등에서 개인을 특정할 수 있는 데이터가 다수 생성되면서 IT종합전략본부는 법제도상 이들 데이터를 어떤 선상에서 다룰 것인지를 두고 논의를 거듭해 옴
- 2015년 9월 중의원 본회의에서 가결 및 성립된 개인정보보호법 재개정안에는 개인이 특정되지 않도록 하는'익명가공정보화'를 의무화하고 제3자에 개인정보를 제공하는 규정을 명확히 함
- 이와 동시에 개인정보의 이용과 활용을 촉진하여 신산업 . 신서비스의 창출과 국가안전 . 안심 향상을 실현할 수 있도록 규정을 정비
- 이후 일본 정부는 EU 등 해외와의 규제 일관성을 유지하기 위한 입법 개정을 추진해 왔으며, 2017년 5월부터 개정 개인정보보호법이 발효
- 개정 법 하에서는 사전 동의 없이 개인정보 취득 행위를 불허함으로써 개인정보 공개에 따른 부당한 차별이나 편견을 최소화시키고자 하였으며, 빅데이터 산업 지원과 규제를 위한 근거를 삼기 위해 익명가공정보에 대해 특정 개인을 식별할 수 없도록 개인정보를 가공하여 얻어지는 개인에 관한 정보에 대한 복원을 금지
- 이 같은 접근은 익명가공정보일 경우라도 데이터 가공 주체가 원본 데이터를 폐기하지 않은 이상 여전히 식별 가능성이 남아 있기 때문에 법률로써 이를 금지하여 익명성 보장을 담보하기 위한 것

- 또한 다양한 민간 빅데이터 서비스가 익명 가공을 통해 관광, 도시 계획, 안전 등 공적인 영역에서도 다양한 서비스에 활용되고 있기 때문에, 개정 법률안으로 인해 이 같은 서비스 응용은 더욱 탄력을 받을 것으로 예상

▶ 사이버보안기본법

- 2014년 11월, 일본 중의원 본회의에서 사이버 공격 대응에 관한 국가의 책무 등을 정한 사이버보안기본법이 통과되어 2015년 1월 9일부터 전면 시행
- 동법은 사이버보안에 관한 대응 전략을 국가 차원에서 종합적이고 효과적으로 추진하는 것을 목적으로 하며, 사이버 보안에 대한 기본 이념과 전략 및 국가의 책임을 정의
- 동 법을 통해 일본에서는 '사이버보안'이 '정보 시스템 및 정보 통신망의 안전성 및 신뢰성 확보를 위해 필요한 조치를 강구하고 그 상태가 적절하게 유지 관리되는 것'이라고 최초로 법률적 정의가 내려짐
- 정부의 사이버 보안 전략을 담당해 온 '정보보안 정책회의'를 격상시켜 '사이버보안전략본부' 설치를 결정
- 이외에도 동 법안에서는 연구개발의 추진 및 연구자·기술자의 육성, 경쟁기반의 정비 등에 필요한 시책, 국민에 대한 교육 및 학습을 위한 시책 역시 강구할 것임을 적시
- 그러나 사이버보안기본법 발효 이후 4개월 뒤인 2015년 5월에 일본연금기구가 외부로부터 송부된 이메일에 의해 약 125만 건의 개인정보가 유출되는 사건이 발생됨에 따라 기본법 보완에 대한 필요성이 재기
- 이에 따라 2016년 개정안에서는 ▲국가가 실시하는 부정한 통신의 감시, 감사, 원인 규명 조사 등의 대상 범위를 확대하는 것과 ▲사이버보안전략본부의 일부 사무를 정보처리추진기구(Information-technology Promotion Agency, IPA) 등에 위탁하고 국가자격제도(정보처리안전확보지원사)를 신설하는 것을 내용으로 한 조항이 새롭게 추가
- 이후 2020년 도쿄 올림픽을 앞두고 사이버공격의 지능화 및 대규모화에 대한 대응 차원에서 또 한 차례의 개정안이 발의
- 이 개정안에서는 사이버보안협의회 창설과 사이버보안전략본부 연락 조정 권한 부여 항목이 새롭게 추가
- 사이버보안협의회는 사이버보안에 관한 시책 추진에 관해 필요한 협의를 행하기 위해 설치되는 조직으로, 공공・민간 부문의 다양한 주체가 서로 연계하여 보안 정보 공유를 위해 노력하고 필요한 대책 등을 협의하는 것을 주요 목적으로 삼고 있음
- 또한 국내외 관민학에 걸친 사이버보안 통합 조정자 역할을 강화하기 위해 사이버보안전략본부에 대해 외부 기관들과의 연락 조정 권한을 강화
- 이 개정안은 2019년 중으로 시행될 것으로 예상

▶ 개인정보의 이용 및 활용 촉진과 소비자 신뢰성 확보의 양립을 위한 보고서

- 2017년 2월, 내각부 산하 개인정보보호위원회 사무국은 익명가공정보 안전관리조치 및 이용사례 및 가공방법 사례를 담은 "개인정보의 이용 및 활용 촉진과 소비자 신뢰성 확보의 양립을 위하여" 보고서를 발표
- 본 보고서는 2015년 9월 법안 통과되어 2017년 5월에 발효된 개정 개인정보보호법(個人情報の保護に関する法律)에 규정된 '익명가공정보' 활용에 앞서 제도 정비안을 마련하기 위한 목적으로 작성
- 주요 내용으로는 익명 가공 정보의 ▲정의와 취급 상의 유의사항 ▲생성 시 요구되는 가공 방법 ▲ 안전 관리 조치 ▲이용 상의 유의사항 ▲활용 사례 및 가공 예시 등을 언급
- 이외 인정 단체나 사업자 단체가 익명 가공 정보의 작성에 관한 규정을 검토하거나 민간 사업자가 실제로 익명 가공 정보 작성 시 참고가 되는 정보를 제공

주요 전략 및 정책

▶ 사이버보안전략

- 사이버보안전략은 2013년 6월 정보보안정책회의를 통해 최초로 도입되었으며, 2015년 1월 사이버보안기본법 시행 이후 사이버보안전략본부가 주무 부처 역할을 하고 있음
- 사이버보안전략은 현재와 향후의 사이버 위협에 대한 국가 차원의 대응 방안을 수립하고 공공과 민간의 관련 당사자들을 위한 전략적 대처 방안을 제시하는 기능을 담당
- 3년 단위로 정기적인 업데이트가 이뤄지고 있는 사이버보안전략은 2018년 6월 내각사이버보안센터(NISC)가 최신 전략 버전을 확정하여 공공의견 수렴을 거친 뒤, 2018년 7월 말 각료회의를 통해 해당 안을 승인
- 사이버보안전략 개정안에서는 대량의 데이터를 분석·활용하는 사례가 늘어나면서 사이버 위협 발생 시 실생활에 미치게 될 파급력이 커지고 있는 상황과 2020년 도쿄 올림픽, 장애인 올림픽 등 대규모 행사를 앞두고 향후 3년 동안의 새로운 사이버보안 시책 목표와 시행 방침을 명시
- 개정안에서는 주요기반시설 보호를 위해 정부와 민간의 일치된 협력과 대학에서의 연구 자료 보호를 위한 조치를 강화하는 내용이 추가
- 2020년 올림픽 준비와 대회를 통해 확보한 사이버보안 체계를 이후에도 지속성 있게 계승·발전시키는 내용 역시 새롭게 반영된 항목이며, 이외 2016년 미라이 봇넷 사태로부터 빚어진 위기의식을 반영하여 DDoS 등 대규모의 잠재적 사이버공격에 대한 대처 능력 강화를 위한 시책도 추가로 포함
- 전략 추진을 위해 사이버보안전략본부는 산하 내각사이버보안센터(NISC)를 중심으로 관계 기관의 역량 강화를 도모
- 센터는 각 부처 간의 종합적인 사이버보안 활동 조정과 산학 관민 연계 촉진을 위한 주도적 역할을

담당하며, 국가 사이버보안 위기관리 대응 역량을 더욱 강화해 나갈 예정

- 전략적 목표 달성을 위한 세부 정책은 사이버보안법의 기본적 지향 가치인 ▲경제 사회의 활력 향상 및 지속적 발전 ▲국민이 안전하게 살 수 있는 사회 실현 ▲국제사회의 평화 안정 및 국가 안전 보장 등을 달성하기 위해 하위 정책 실행 사항을 제시

표 _ 사이버보안전략 개정안 세부 실행 정책

1. 경제 사회의 활력 향상 및 지속적 발전	
① 새로운 가치 창출을 지탱하는 사이버 보안 추진	o 경영층의 의식 개혁을 촉진('비용'에서 '투자'로) o 투자를 위한 인센티브 창출(정보 제공 및 공시에 따른 시장의 평가, 보험 활용) o 설계 단계부터 보안 기능을 반영하는 'Security by Design'을 토대로 사이버 보안 비즈니스의 강화
② 다양한 연결에서 가치 창출 공급망의 실현	o 중소기업을 포함한 공급망(기기·데이터·서비스 등의 공급망)의 사이버 보안 대책 지침 마련
③ 안전한 IoT 시스템 구축	o IoT 시스템의 보안 체계 정비와 국제 표준화 o IoT 기기의 취약성 대책 모델 구축·해외 전파
2. 국민이 안전하게 살 수 있는 사회 실현	
① 국민과 사회를 지키기 위한 대응	o 위협에 대한 사전 방어(적극적 사이버 방어) 방안 수립 o 사이버 범죄 대책 마련
② 주요기반시설 보호를 위한 민간 공동 대응	o 안전 기준 개선과 확산: 주요기반시설 사업자 등을 대상으로 한 사이버보안 대책의 관계법령 정비 o 지방공공단체의 서비스 장애 시 대책 수립 등 보안 강화
③ 정부 기관 등의 보안 강화·충실	o 정보 시스템 상태의 실시간 관리 강화 o 첨단 기술 활용을 통한한 선제적 대응 과제 해결
④ 대학·대학연구기관의 안전한 교육·연구 환경의 확보	o 대학 및 대학공동연구기관(Inter-University Research Institute Corporation) 단위의 사이버보안 대책 강화 및 가이드라인 개발을 통한 연구 자산 보호
⑤ 2020년 도쿄 올림픽대회와 이후의 대응	o 사이버보안 대응 조정 센터(정부 올림픽 CSIRT) 구축: 관계부처, 대회조직위원회, 경기장 관할 지방 공공단체, 도쿄도, 주요기반서비스 사업자 간 사이버보안 리스크 대응 협조 체계 마련

	o 올림픽을 통해 갖춰진 사이버보안 대응 체제의 성과를 이후에도 지속적으로 계승 활용
⑥ 기존 틀을 넘어선 정보 공유·협력 체제 구축	o 정보 제공자 및 민간 전문 기관 등 다양한 주체의 참여를 통한 정보 공유·제휴 추진
3. 국제사회의 평화 안정 및 국가 안전 보장	
① 자유, 공정 및 안전한 사이버 공간 유지 강화	o 자유롭고 공정하고 안전한 사이버 공간 이념 전파 o 사이버 공간에서의 법질서 강화
② 국내 방어력·억제력·상황파악 능력 강화	o 강력한 국가 방어력(① 임무 보증 ② 국내 첨단 기술 및 국방 관련 기술 방어 ③ 사이버 공간상의 테러 조직 활동 대응) o 사이버 공격에 대한 억지력 향상(① 동맹국과의 협조와 관계 부처 연계 및 법집행기관·자위대 역량 강화를 통한 실효적 억제를 위한 대응 ② 국가 간 신뢰 구축 조치) o 사이버공간 내 위기 상황 파악 강화(① 관계 기관의 정보수집·분석 능력 향상 ② 위협 정보 공유·연계)
③ 국제 협력·연계	o 국가 간 사이버보안 정보 공유 및 정책 조정 o 사고 대응 등에 관한 국제 연계 강화 o 개도국 사이버보안 역량 구축 지원을 통한 글로벌 안보 환경 강화

[출처] NISC

▶ 주요기반시설 정보보안대책

- 일본 정부는 2000년부터 주요기반시설 보호를 위한 대책을 수립해 왔는데, 2000년 12월에 발표된 주요기반시설 사이버테러대책에 관한 특별행동계획(重要インフラのサイバーテロ対策に係る特別行動計画)에서는 정보보안 대책 추진 회의 등의 활동을 통해 사이버 테러로부터 정보통신, 금융, 항공, 철도, 가스, 전력 및 정부·행정서비스 등의 국민 생활과 사회 경제 활동에 중대한 영향을 미칠 수 있는 국가 기반 시설에 대해 보호 방안을 최초로 심의·정리
- 이후 정보보안정책회의에서는 2005년 12월 주요기반시설 정보보안대책에 관한 행동계획(重要インフラの情報セキュリティ対策に係る行動計画)의 최초 버전을 작성했으며, 이후 꾸준한 업데이트를 진행해 오며 2018년 7월 말 시점 사이버보안전략본부에 의해 4차 행동계획 개정안까지 업데이트된

버전이 공표

- 주요기반시설 정보보안대책에 관한 4차 행동계획에서는 ▲선도적 체계 확립 하의 추진 ▲도쿄 올림픽 대비 정보공유체제 강화 ▲위기관리 기반의 대처 태세 정비 추진 등의 3가지 중점 항목을 추진 계획으로 설정
- 동 계획의 주요 시책으로는 ▲안전 기준 정비 및 확산 ▲정보 공유 체제 강화 ▲정보 공유 체제 강화 ▲장애 대응 체제 강화 ▲위기 관리 ▲보호 기반 강화 등을 추진

▶ 주요기반시설 정보보안 안전기준 지침

- 내각사이버보안센터(NISC)는 주요기반시설의 사이버 방어 프로세스 전반에 걸친 대응 기준을 다룬 '주요기반시설 정보보안 안전기준 지침(重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針)을 적용 중
- 2018년 4월 4차 행동계획의 일환으로 동 지침의 최초 버전을 작성하였으며, 사이버 방어 계획 프로세스 전반에 걸친 각 단계별 검토 및 실행 사항을 제시
- 동 지침의 최신 버전인 제5판(2019.5)에서는 ▲자연재해로 인한 주요기반시설 서비스 장해 발생 관련 설비 설치 및 관리 ▲정부 대응과 국제 동향을 감안한 데이터 관리의 바람직한 방향 검토 ▲공항 분야 등의 내용이 새롭게 추가

2) 담당기관

▶ 총무성

- 총무성은 국가 정보보안 능력 제고를 위해 정보통신 업계관계자들이 실질적으로 고려해야 할 단기 및 중장기적인 대책이나 사업 개선의 방향성을 포함한 효과적인 국가 정보보안 정책 수립과 추진 방향에 대한 조언을 구하기 위해 자문위원회를 구성
- 총무성 산하 정보보안 자문위원회는 2013년 2월 15일 조직되어 3월부터 공식 활동을 전개

▶ IT종합전략본부

- 일본 정부는 정보통신기술의 발전으로 인한 세계적인 사회경제 구조 변화에 발 빠르게 대응하기 위해 2001년 1월 내각 내부에 '고도 정보통신 네트워크 사회 추진 전략 본부 (IT종합전략 본부)'를 설치
- IT종합전략본부는 내각관방 정보보안센터(NISC)와 연계해 국가 차원의 정보보안 정책을 지휘
- 내각관방 정보보안센터에서는 매년 정보보안 관련 각종 조사 및 연구를 수행하여 결과물을 홈페이지에 게재

▶ CSSC(Control System Security Center)

- 일본 경제산업성을 중심으로 이메일을 통해 침투하는 지능형지속위협(APT) 및 악성코드 정보를 공유하는 협의회로서 2012년 3월 설립되었으며, Hitachi, Toyota, Toshiba, Trend Micro 등 정보보호관련 업계 내 다양한 회원사를 보유

▶ 사이버보안 전략본부

- 사이버보안기본법에서는 현재 정부의 사이버보안 전략을 담당하고 있는 '정보보안 정책회의'를 격상시켜 범부처를 대상으로 한 사이버보안 정책의 사령탑 역할을 수행하기 위한 조직으로써 내각 산하에 '사이버보안 전략본부' 설치를 규정
- 기존에 정보보안 정책회의에서는 내각 관방 장관이 의장 역할을, 사무국 역할은 내각 관방 정보보안센터(NISC)가 각각 담당
- NISC는 총무성, 경제산업성, 국방성, 경찰청 등의 각 부처에서 파견된 인사들을 중심으로 구성되었으나, 법적 권한 제약과 전문 인력의 부족으로 인해 역할과 기능상의 한계를 노출함에 따라 사이버보안 전략본부에서는 민간 보안 전문가들을 기간제로 임용키로 결정
- 또한, 국가안전보장회의(NSC)와 IT종합전략본부의 의견을 토대로 '사이버보안 전략안'을 작성하고 지방자치단체들과 협력 체제를 구축
- 사이버보안 전략본부는 그동안 정보보안 정책회의가 추진해 온 보안 전략 및 정부 부처들의 보안 가이드라인 수립과 부처 내에서 발생한 보안사고 조사 등을 실시

▶ JPCERT 조정센터(JPCERT/CC, Japan Computer Emergency Response Team Coordination Center)

- 컴퓨터 보안 정보를 수집, 사고 대응 지원 및 컴퓨터 보안 관련 정보 제공을 하는 일본의 대표적인 컴퓨터침해사고대응팀(CSIRT, Computer Security Incident Response Team)
- 1996년 임의단체로 설립됐으나, 2009년 6월 이후 일반사단법인으로 전환한 상태
- 일본 최초로 국제 조직인 FIRST(Forum for Incident Response and Security Teams)에 참여한 CSIRT로, 아태 지역 내 CSIRT 조직인 APCERT 사무국을 운영
- 주요 활동으로는, 고정지점인터넷관측시스템(ISDAS, Internet Scan Data Acquisition System) 운영, 일본 내 사고 보고 대응 및 사고 정보의 국내외 네트워크 관리자 공유 활동 등을 수행
- 또한, 해외 CSIRT에서 수집된 취약성 정보를 일본 내 소프트웨어 개발사에게 제공하는 업무도 추진
- 이외 정보처리추진기구(IPA, Information-technology Promotion Agency)와 공동으로 일본 자국 내 소프트웨어 제품의 취약성 대응 상황 공개를 위한 'Japan Vulnerability Notes(https://jvn.jp/)'이라는 웹사이트를 운영

▶ 개인정보보호위원회

- 2015년 9월 개인정보보호법 개정에 따라, 2016년 1월에 개인정보 악용을 감시 . 감독하기 위한 제3의 독립기구인 '개인정보보호위원회'가 설립
- 기존에는 개인정보보호는 각 부처별 감독과 민간자율 규제에 맡겨져 왔으나, 보다 강력한 권한을 갖는 위원회가 출범
- 이에 따라 익명가공정보[23]를 취급하는 경우 '익명가공정보 취급사업자'라고 여겨지고 개인정보보호위원회 규칙으로 정하는 기준에 따라 당해 개인정보를 가공
- 또한 인정 개인정보보호단체는 개인정보보호 지침을 만들 때 소비자 등의 의견을 청취하고 개인정보보호위원회에 신고하여야 하며, 개인정보보호위원회는 그 내용을 공표

3) 규제 및 인증제도

▶ JISEC (정보보안평가인증제도)

- 일본 경제산업성은 2001년부터 'ISO/IEC 15408(SC27)'을 바탕으로 '정보보안 평가인증제도(Japan Information Technology Security Evaluation and Certification Scheme, 이하 JISEC)'를 운영 중
- 정보보안의 관점에서 보안 상품 및 시스템의 적합성을 공인하기 위한 표준으로써 CC(Common Criteria)를 채택
- 기관 및 민간 단체의 보안 솔루션 개발 프로세스, 제공, 사후관리 등의 측면에서 CC가 제시하는 기준 규격을 준수했는지 국가 차원에서 관리하기 위함
- 제 3의 민관기관에 평가 업무를 맡겨 공정성을 확보했으며 평가 이후 정보처리추진기구(IPA)가 인증을 처리
- 국제표준인 'ISO/IEC 15408'을 기준으로 하므로 'JISEC' 인증을 받은 제품은 해외에서도 기준을 통과한 제품으로써 인정받음

▶ 일본전기통신단말기기승인(JATE)

- JATE는 전기통신회선에 접속하는 단말기기가 관련 기술에 적합한지 검사해 인증하는 제 3자 인증기관으로 전기통신사업자가 정하는 기술적 조건에 단말기기가 부합하는지 확인하는 인증
- 주요 업무는 기술기준 적합 인증, 기술적 조건 적합 인증, 심사신청에 필요한 전기적 특성 등의 추정

▶ 일본공업규격 (Japan Industrial Standards, JIS)

---

23 특정 개인을 식별할 수 없도록 개인정보를 가공해 얻을 수 있는 개인에 관한 정보로서 당해 개인정보를 복원할 수 없도록 한 것. 개인정보보호법 개정안, 2015.9

- 일본공업표준화법에 따라 제정된 국가 임의규격으로, JIS 규격 기준 이상의 품질을 보유한 제품이나 가공품을 안정적으로 지속생산 할 수 있는 기술적 능력을 보유한 공장에 대해 일본 주무대신이 JIS 마크표시를 허가하는 제도
- 공장 전체를 하나의 시스템으로 파악하여 JIS에 적합한 제품 또는 가공품을 연속적으로 생산할 수 있는 기술적 능력을 검사해 JIS 마크 표시를 인정하는 '공장심사방식'을 취하고 있음
- 심사기준으로서 품질관리 및 품질보증에 관해 JIS Z 9902(ISO 9002)가 적용

▶ 일본자율안전인증(S-Mark)

- 일본의 임의 안전규격으로 전자제품 등에 대한 안전 확인을 받고자 하는 제조자, 수입자 등을 위한 인증으로 S-Mark 대상 전기용품에 대해 등록검사기관의 시험 및 공장심사를 거쳐야만 인증이 완료되며 이에 따라 제품에 S-Mark 표시를 하여 판매할 수 있음
- S-Mark는 의무적인 인증 제도는 아니나 전기제품의 안전도를 객관적 기준에 의해 확인받음으로써 판매업체 및 소비자에게 공신력을 확보하기 위한 수단으로 활용

▶ 클라우드 정보보안 감사 제도

- 표준적인 서비스를 다수의 고객에게 제공하는 클라우드 서비스의 특성에 입각하여 사업자가 준수해야 할 정보보안 관리의 '기본 요건'을 정하여, 정해진 요건에 따라 사업자의 실행 여부를 평가하고 안전성 확보 상태를 고객에게 명확하게 알려주기 위한 제도
- 감사 결과, '기본 요건'을 충족하고 있다고 인정된 경우 CS(Cloud Security) 마크가 부여되고 클라우드 사업자의 홈페이지 등을 통해서 이용자는 클라우드 사업자의 보안에 대한 대응 상황 확인이 가능

▶ IoT 인증 마크 제도

- 총무성이 2017년 10월 발표한 IoT 보안종합대책(IoTセキュリティ総合対策)에서는 IoT 기기의 설계・제조 단계에서는 프로세스 자체에 보안을 기본 요소로 반영하여 설계된 기기에 인증 마크를 부여할 계획을 밝힘
- 인증 마크는 관리자나 사용자가 보안 기준에 적합한 기기/서비스 이용 패턴을 유도하기 위해 설계 단계부터 이용 프로세스상의 보안을 강화할 수 있도록 ID/패스워드 설정, 펌웨어 업데이트 및 Wi-Fi 설정 사양을 설계 프로세스에 반영하도록 하며, 보안 기준을 충족한 제품에 대해 인증 마크를 부여
- 또한 IoT 기기 판매자는 기기 판매 후에도 신종 바이러스나 사이버 공격 기법 대응 현황을 정기적으로 감시 확인케 함으로써 IoT 기기 생애주기 전반에 걸친 보안 확보 방안도 함께 마련
- 총무성은 인증 마크 제도 도입을 위해 2018년 하반기 업계 내 의견을 수렴 중이며 이르면 2018년 했으며, 이를 토대로 2019년 10월 말부터 인증제도 적용에 본격 착수

4) 스타트업 관련 정책 동향

▶ 미래투자전략(2017.6)

- 아베 총리를 의장으로 한 '미래투자회의'에서 일본 정부는 Society 5.0 실현의 일환으로 2023년까지 유니콘 기업을 20개로 확대시킬 계획을 밝히며 주체별 성과 투자가 선순환 될 수 있는 시스템을 강조
- 대학, 국립연구개발법인, 기업·투자자 등의 공조를 통해 혁신 활동의 성과가 투자로 이어지는 선순환을 실현하기 위한 스타트업 생태계 구축을 실현

▶ 후쿠오카 시 글로벌 창업특구(2014.5)

- 일본 정부는 국가 전략 특구 제도를 활용하여 외국인 기업가 유치를 위해 최장 1년 동안 입국 체류를 인정하는 제도를 추진
- 후쿠오카 시는 2014년 5월 글로벌 창업 특구로 인정된 이후, 스타트업 법인 감세 및 외국인 창업 비자 발급 등의 정책을 전개

▶ 일본개방혁신·벤처창조협의회(2015.2)

- 기업의 개방적 혁신 추진을 목표로 민간 기업과 스타트업, 대학 등을 중심으로 일본 개방혁신·벤처창조협의회(JOIC, Japan Open Innovation Council)를 구성
- 국립신에너지산업기술종합개발기구(NEDO)가 동 협의회의 사무국 역할을 수행하며 스타트업 혁신을 위한 세미나(연 3회), 워크샵,(연 6회) 피칭(연 10회) 지원, 백서 발간 등의 작업을 수행
- NEDO는 향후 대학 벤처 육성에 초점을 맞춘 피칭 이벤트를 개최하고 기업 간 매칭 기능을 더 확대할 계획

▶ J-Startup(2018.6)

- 경제산업성은 세계 무대에서 경쟁할 수 있는 스타트업 기업 육성을 위한 지원 프로그램인 'J-Startup'을 운영을 발표
- 동 프로그램 하에서는 전문가가 추천한 성장 유망 스타트업 기업을 'J-Startup 기업'으로 선정하고 대기업, 벤처캐피탈, 엑셀러레이터 등의 'J-Startup Supporters'와 민관 공동 및 관계부처가 연계하여 선정 스타트업 기업을 지원
- 정책 지원 내용으로는 정부 시책 활용 시 우선제도와 가점제도 적용, 각종 보조금 지원 시책 우대, 절차 간소화 등이 있으며 이외 'J-Startup'로고 사용 권한 부여와, 홈페이지 개발, 국내외 언론에 대한 홍보 활동 등이 포함

5) 융합보안 시장 및 정책 동향

자율주행차량

▶ 일본 경찰청, 원격 자율주행차량 도로 실증실험 기준안(2019.9)

- 일본 경찰청은 2017년 4월 일본재흥전략의 일환으로 자율주행차량 주행 환경 정비를 위해 원격 조작 기반 자율주행차량의 도로 실증 실험을 위한 기준안을 마련
- 동 기준안에서는 주행 중 통신 환경이 두절되지 않고, 일반도로 이용자에게 현저한 지장을 미치지 않으며 원격 자율주행차량의 전후좌우에 원격으로 자율주행 중임을 알리는 표식을 장착하는 것을 의무화한 것 등의 조건을 허용할 경우 도로 실증 실험을 허용
- 차량 실험 대수는 원칙적으로 1대이며, 매회 1대씩 늘려갈 수 있고, 이 경우에는 복수의 차량 실험도 인정
- 실험에 사용되는 도로는 별도로 통제하지 않으며 경찰청의 허가 기간은 최대 6개월
- 2019년 9월에 개정된 원격 자율주행차량 도로 실증실험 기준안에서는 기존의 허용 조건 이외 최고 속도 기준 시속 20km를 넘지 않을 것으로 추가 규정으로 제정
- 또한 승객을 태우고 운행할 경우 원격 감시자는 2종 면허증 보유를 의무화

IoT

▶ IoT 사이버보안 액션 프로그램 2017(2017.1)

- 총무성은 2020년 도쿄 올림픽 개최와 IoT 인프라 확산에 대비하여, 현재 다양한 부처에서 제공되고 있는 사이버보안 시책을 통합한 'IoT 사이버보안 액션 프로그램 2017'을 발표
- 동 프로그램은 5대 실행 계획인 ▲사이버보안 태스크포스(TF) 회의 개최, ▲보안 인재 육성의 촉진(speed-up), ▲총리대신 표창제도 창설, 및 ▲국제 연계 강화 등으로 구성
- IoT 사이버보안 액션 프로그램 2017은 이미 일본 정부가 추진해 온 다양한 사이버보안 관련 시책의 연장선 상에서 이들을 통합한 성격
- 앞서 내각관방은 2015년 1월에 설치한 내각사이버보안센터(NISC)를 통해 이미 도쿄 지역을 중심으로 CYDER 추진을 비롯하여 다양한 사이버공격 대응 체제 활동을 수행
- 경제산업성 역시 2015년 12월에 수립한 사이버보안 경영가이드라인을 통해 기업 경영자 관점에서 사이버보안 대책 수립을 위한 지침을 제공

▶ IoT 사이버보안종합대책(2017.10)

- 총무성은 'IoT 보안종합대책(IoTセキュリティ 総合対策)'을 통해 자국 IoT 보안 취약점 강화를 위한 ▲체제 정비 ▲연구개발 ▲인재육성 강화를 도모
- (체제 정비) 일본 정부는 설계, 제조, 판매, 설치 및 운용 등 IoT 제품 사이클 전반에 걸친 보안 체제 마련을 위해 인증 마크 제도를 도입키로 했으며, 이에 따라 2019년 3월 총무성은 '단말 설비 등 규칙의 일부 개정안'을 통해 IoT 인증 제도 마련에 착수
- (연구개발) 정보통신연구기구(NICT)가 주축이 되어 정교화되고 고도화되는 사이버 공격에 대응하기 위해 AI 기술을 활용한 사이버보안 연구개발 추진
- (인재육성) 2018년 12월 총무성 산하 사이버보안 태스크포스팀 내 '사이버보안 인재육성 분과회'를 설치하여 지방 사이버보안 인재 육성 과제를 검토

핀테크/블록체인

▶ 핀테크, 미래투자전략 5대 전략 중 하나로 선정(2017.6)

- 2017년 6월에 발표된 '미래투자전략 2017'에서는 ▲의료/건강 ▲이동수단/교통 ▲공급망 ▲도시/건설과 함께 핀테크를 5대 전략 중 하나로 선정
- 핀테크 분야에서는 ▲오픈 이노베이션 ▲기업 성장 동력 강화를 위한 핀테크 활용 ▲캐쉬리스화 촉진 등을 중점 추진 항목으로 설정하며, 최근 일본 정부가 추진해 온 핀테크 정책을 망라하여 구체적인 목표치를 제시

표 _ 미래투자전략에서의 핀테크 관련 주요 정책

주요 정책	내용
오픈 이노베이션	• 핀테크 기업이나 금융기관의 혁신적 핀테크 실증 실험 추진에 따른 절차적인 문제를 해소하기 위해 '핀테크 실증실험 허브'를 구축 • 블록체인 시범 사업용 플랫폼을 통해 전자 기록 채권 거래 및 신분 확인, 결제·물류 정보 관리 등 금융 인프라 고도화를 위한 실증 실험 • 핀테크 기업의 금융 기관 제공 시스템 접속을 촉진시키기 위해 3년 이내 오픈 API 도입 은행을 80군데로 확대
금융 EDI 강화	• 금융 EDI(Electronic Data Interchange) 강화로 재무·결제 프로세스 전반에 걸친 고도화 도모 • 2018년부터 XML 신규 시스템을 가동하여 2020년까지 XML 전자문서로 전면 이행토록 하며, 2020년까지 상업용 유통 정보 항목의 표준화 확대와 업종을 넘어선 기업 간 EDI 협력 강화
캐쉬리스화 추진	• 신용카드의 안전한 이용 환경 정비를 통해 2020년까지 '신용 결제 단말기 IC 대응 100%'달성

[출처] 내각관방 未来投資戦略 2017 외 각종 자료

다. 영국

'18년 GDP(십억달러)	2,825.21
'18년 인구수(천명)	664,900

■ ITU 글로벌 사이버보안 지수(Global Cybersecurity Index, GCI)

· 영국의 사이버보안 지수는 0.931로 세계 1위를 차지

국가명	2018		2017		전년대비 증감	
	지수	순위	지수	순위	지수	순위
영국	0.931	1	0.783	12	+0.148	+11
대한민국	0.873	15	0.782	13	+0.091	-2

■ ICT 관련 주요 지수

· 영국의 전반적인 ICT 발전 수준 역시 최상위권을 유지하고 있음

지표명	영국		한국	
	점수	순위	점수	순위
IMD 국가경쟁력지수(2019)	-	23	-	28
IMD 디지털경쟁력지수(2019)	-	15	-	10
UNCTAD 전자상거래지수(2019)	94.4	5	89.4	19
ITU 글로벌 사이버보안 지수(GCI 2018)	0.931	1	0.873	15
UN 전자정부 지수(2018)	0.899	4	0.901	3

■ ICT 관련 주요 통계 (ITU, 2018년 말 기준)

· 영국의 유선 및 이동통신(ICT) 이용 및 보급률은 세계 최고 수준으로 우리나라와 비슷함

항목	영국		한국	
	가입자수(천 명)	보급률(%)	가입자수(천 명)	보급률(%)
유선전화	31,973	47.62	25,907	50.63
유선브로드밴드	26,586	39.60	21,286	41.60
이동통신	78,924	117.55	66,356	129.67
인터넷 이용률	94.90%		95.90%	

정보보호 산업 개요

1) 보안 환경

▶ 영국은 오랜 기간 동안 아일랜드 공화국군(IRA)의 독립 무력투쟁과 테러 행위로 정보보호 산업 및 서비스의 강화 필요성에 대한 인식이 이미 정착된 국가

- 전 세계에서도 미국과 일본 다음의 제 3위의 시장 규모를 형성하고 있으며 과거 EU 내에서는 최대 정보보호 시장을 형성
- 정보보안 시장뿐 아니라 사회불안 현상 야기로 물리보안 시장에서도 절도, 테러 등의 범죄예방을 위한 CCTV 설치 대수가 과거 EU 내에서 가장 많은 국가일 정도로 보안장비 수요가 매우 큰 시장

▶ 영국계 회계법인 PwC에 따르면, 지난 10년 동안 영국 내 사이버 공격은 꾸준히 증가함

- 영국 정부가 진행한 사이버 보안 침해 설문 조사에 따르면, 2017년에 영국 기업의 43%가 사이버 공격을 받았음
- 특히 직원 250명 이상이 근무하는 회사에서 침해 사례가 72% 증가한 것으로 나타났으며, 가장 흔한 사례는 사기성 이메일(48%)과 멀웨어(13%)로 조사됨

  * 멀웨어(Malware): 악성 소프트웨어(Malicious software)의 줄임말

▶ 영국 정부는 2016년 발표된 국가 사이버보안전략에 따라 19억 파운드(2조7천억원)를 사이버 보안 분야에 투자하고, 국가사이버보안센터(NCSC, National Cyber Security Cemtre)와 런던사이버보안혁신센터(LORCA, London Office for Rapid Cybersecurity Advancement)를 설립하여 사이버보안 인력을 양성하고 기업을 지원

- 필수서비스 사업자는 효과적인 사이버 보안조치를 실행하여 필수 네트워크와 인프라를 안전하고 복원력 있도록 해야 하며, 미흡한 경우 새로운 벌금이 부과될 예정
- 영국 교통부는 커넥티드카와 자율주행차의 사이버 보안을 위한 가이드라인을 발표하여 제조공급망에 관련된 모든 이해관계자들에게 일관성 있게 보안정책 제공

▶ 영국 정부는 사이버 보안 기업이 성장하기 좋은 비즈니스 및 투자 환경을 제공하고 있음

- 영국 정부에 따르면 800개사의 사이버 보안 기업이 영국에 본사가 있으며 89%는 중소기업으로 분류됨

2) 인터넷 및 통신 환경

❑ 개요

▶ 영국의 정보통신 발전 지수(IDI, ICT Development Index)

- 영국은 2022년을 목표로 전국에 광대역 인프라 설치를 위해 10억 파운드 투자 및 1GB/S의 인터넷 속도 달성을 위해 4억 파운드 투자를 추진하는 등 정보통신 환경을 지속적으로 개선하고 있으며 ITU의 정보통신 발전지수도 2010년 10위에서 2016년에는 5위로 상승했으며 현재까지 유지 중임
- 그 결과 인터넷 다운로드 속도가 급증하고 일반인의 정보통신 접근부문(Access)과 활용부문(Use)도 급격히 개선되었으나 정보통신 기술부문(Skills)은 2016년 기준 29위로 다른 분야보다 순위가 낮게 나타나, 이 부문을 강화하기 위한 정부의 정책적 노력이 요구됨

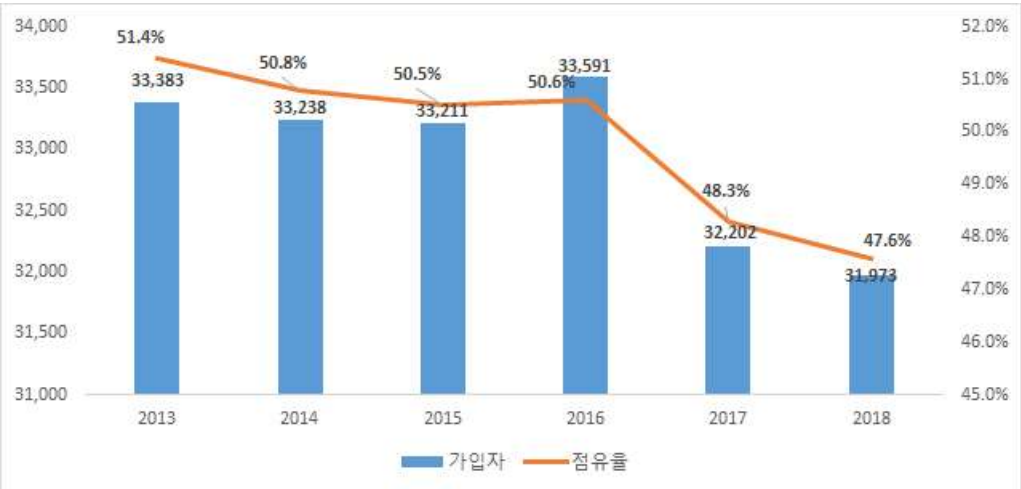
❑ 유선 통신

▶ 유선전화 통신망 보급률은 2017년 대비 0.7%p 감소

- IUT자료에 의하면 유선전화 보급률은 이동통신망과 인터넷 통신망 사용이 일반화되면서 2000년 이후부터 꾸준히 감소하여 2017년 48.3%에서 2018년 47.6%로 0.7%p 감소

그림 _ 영국 유선통신 가입 및 보급률 추이

(단위: 만 명, %)



[출처] ITU Statistics DB(2019.6)

- 유선통신 주요사업자로는 British Telecom(BT), KCom, Cable & Wireless가 있음
- British Telecom(BT)은 유선통신 사업자로 약 170개국에서 사업을 하며, 도매서비스에 점점 더 중점을 두며, 네트워크 기반의 IT서비스와 브로드밴드 서비스로부터 수익을 창출하고 있음

▶ 영국의 2018년 유선 브로드밴드 고속통신망 보급률은 94%에 이름

- 정책적으로 2022년도까지 10억 파운드를 투자하여 전국에서 고속 인터넷을 사용할 수 있도록 한다는 목표로 브로드밴드 고속 통신망을 가설 및 확장 추진 중
- 영국 정부는 2018년 말을 기준으로 전국의 94%에 고속통신망(30MB/s 이상의 다운로드 속도)을 가설했으며, 사용자의 6%에 해당하는 180만 가정과 기업이 최대 1Gbit/s까지 전송 가능한 광통신망 사용이 가능해져 2017년 84만 명에서 사용자가 크게 증가함

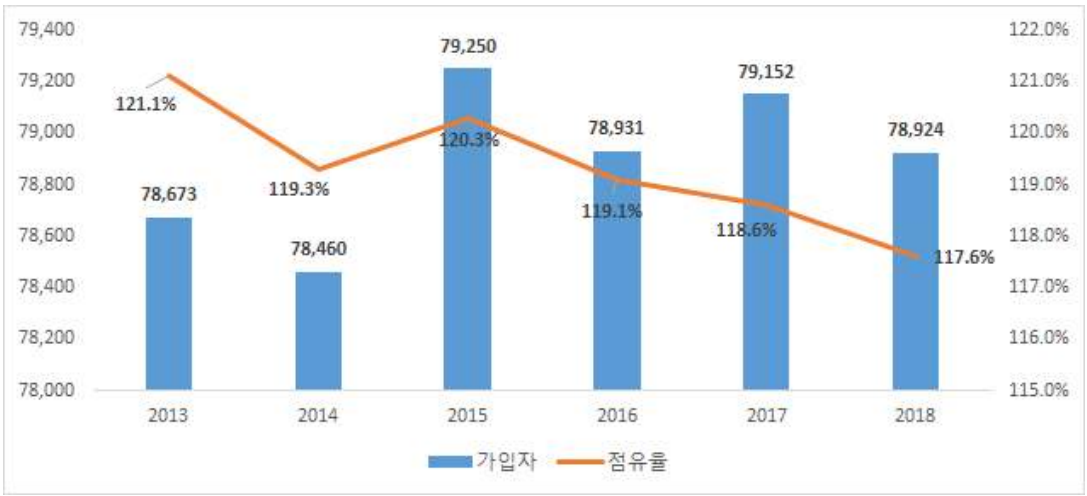
❑ 이동통신

▶ 이동통신 보급률

- ITU 자료에 의하면 영국은 2005년부터 이동통신 보급률이 100%를 넘어섰으며, 2018년 기준 이동통신 가입자 수는 2017년 대비 1.0%p 감소한 7,892만 4천만 명을 기록하며 보급률은 117.6%에 달했음

그림 _ 영국 이동통신 가입 및 보급률 추이

(단위: 만 명, %)



[출처] ITU Statistics DB(2019.6)

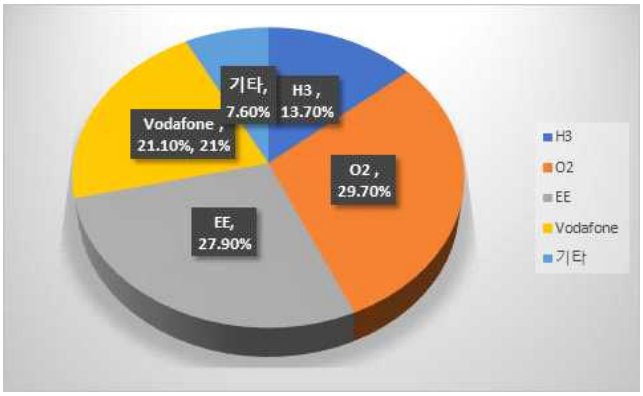
- 영국 4개 이통사(EE, Vodafone, Three, O2)의 LTE 커버리지는 서비스 제공지역의 64%, 실내 76%에

이르며 영국 정부는 2022년까지 무선통신 커버리지를 95%까지 확대할 예정임

- 각 이동통신서비스 사업자는 점차적으로 5G 서비스 지역을 늘리고 있으며, 2019년 8월 21일 기준 EE, Vodafone, Three 통신 3개사에서 5G 상용 서비스를 제공하고 있으며 O2는 10월 중 5G 서비스를 시작할 예정
- 2016년 기준, 이동통신 시장은 2개 업체 EE(29%), O2(27%)가 치열한 경쟁과 함께 시장을 주도하고 있으며 이 외 90개의 가상이동통신사업자(MVNOs, Mobile Virtual Network Operators) 존재

  * 영국 가상이동통신사업자 중 대부분은 IoT를 포함한 모바일 서비스 제공

그림 _ 영국 이동통신사별 시장 점유율(2016년 기준)



통신사	비율
H3	13.7%
O2	29.7%
EE	27.9%
Vodafone	21.1%
기타	7.6%
합계	**100.0%**

* EE는 2010년 이후 Orange와 T-Mobile의 합병으로 생성되어 BT가 2016년 인수 후 분리된 사업단위로 유지

** O2와 Vodafone의 경우 각사가 전적으로 소유한 MVNO인 GiffGaff(O2 소유), Talkmobile(Vodafone 소유)를 포함

[출처] Buddecomm(2019.8)

정보보호 시장 현황

1) 시장 규모

❑ 시장 개요

▶ 영국은 이슬람계 테러리스트과 극우집단의 테러행위 수준이 점점 증가하고 있어 물리보안이 발전함

- 2018년 11월 영국 정부는 국가감시카메라전략의 일환으로 CCTV 운영의 표준을 CCTV 산업 전반에 적용하기 전 시범으로써 사내모니터링 지침을 발표함[24]
- 사내모니터링 지침은 공공 CCTV 체계를 안전하게 관리하기 위한 최소 요구 사항을 제시함
- 2013년 발표된 감시카메라 행동강령의 후속 업데이트로 2018년 감시카메라 감독관은 구매자 툴킷, 공공 CCTV 시스템 이행 준수 자격증, 자체 평가, 정보보호 영향평가 등을 발표함[25]
- 2018년 3월 e-borders[26]으로 수집된 외국인 방문자 60만명에 대한 상세 정보의 외부 유출사건 발생으로 브렉시트 이전 IT 시스템의 재정비 필요성이 강조됨
- 영국 정부는 2018년 10월 런던 히드로 공항은 안면 인식 시스템을 도입하여 보안을 강화했으며 가까운 미래에 영국의 모든 공항에 전신 스캐너, 보딩패스 스캐너 등을 설치하고자 함

▶ 국가 안보 관련 산업 보호 강화[27]

- 영국 정부는 국가 안보와 투자(National Security and Investment) 백서를 발간하여 영국 정부에게 국가 안보를 위협할 수 있는 신규 프로젝트에 대한 사전 검토 권한을 부여할 수 있음을 발표함
- 국가 안보를 위협할 수 있는 신규 프로젝트에는 ▲인수합병 규모가 7000만 파운드 이상이거나 인수합병 이후 시장 점유율이 25% 이상이 되는 경우(2018년 6월, 법령 일부개정으로 군사 기술(또는 군민양용 무기제조업) ▲컴퓨터 하드웨어 기술 및 양자 기술(Quantum technology) 분야 기업의 경우 (인수합병 규모가 100만 파운드 이상일 경우에도 정부개입 가능)가 해당함

▶ 영국 정부는 2019년 2월, 중국 통신장비업체 화웨이 제품의 보안 위험을 완화할 수 있다는 결론에 도달

- 영국의 파이낸셜타임스(FT)에 따르면, 영국 국가사이버보안센터(NCSC)는 차세대 이동통신(5G)

24 Guidance launched for in-house monitoring centres, 2018.10.24
25 Surveillance camera guidance, tools and templates, 2018.10.3
26 경찰, 보안, 출입국 관리 목록에 대해 개개인 승객의 세부사항들을 전자적으로 수집하고 체크하는 시스템
27 "영국, 국가안보 관련 산업 보호 움직임", Kotra 해외시장 뉴스, 2018.10.11.

네트워크에 화웨이 통신장비를 사용하더라도 보안 위험을 줄일 수 있는 방법이 있다고 판단했다고 발표함

- 이러한 결론은 2018년 화웨이의 5G 네트워크 제품 배제 분위기와는 다소 달라진 것으로 화웨이 장비의 영국 도입 가능성을 시사함

▶ 2018년 7월 영국 화웨이 사이버보안평가센터(Huawei Cyber Security Evaluation Centre)는 화웨이의 5G 네트워크 제품의 보안 문제를 지적하는 보고서를 발표함

- 영국 화웨이 사이버보안평가센터의 보고서에서는 네트워크의 백도어를 통해 침투하는 사이버 공격을 제시하며, 이로 인한 화웨이 제품의 보안 문제를 지적함
- 보안 취약점 통계·분석 사이트인 CVE디테일에 따르면 2018년 6월 기준 화웨이 제품에서 드러난 보안 취약점이 152개로, 이는 2017년 보안 취약점 전체(157개) 개수와 맞먹는 수준임

▶ ITU의 글로벌 사이버 보안지수에서 영국이 글로벌 1위로 올라섬

- 2019년 3월 발표된 '2018년 ITU의 사이버보안지수(Global Cybersecurity Index, GCI 2018)' 자료에 의하면 영국은 전 세계 1위로 한국(15위)보다 앞선 것으로 나타남
- 2017년 조사에서는 유럽지역에서 에스토니아, 프랑스, 노르웨이에 이어 4위, 전 세계 순위는 12위였음
- 특히 최근 들어 사이버 공간을 통한 각종 침투공격과 테러 예방을 위해 국가 정보보호정책을 계속 강화하고 있는 추세로 관련 기기 및 솔루션, 소프트웨어 등의 수요가 계속 증가해 나갈 것으로 전망

▶ 영국의 정보보호 시장은 성장성이 큰 만큼 글로벌 기업 간 경쟁 강도가 매우 높음

- 자국 내 정보보호 산업도 높은 수준이지만 수요의 상당 부분을 수입에 의존하고 있어 글로벌 정보보호 기업간 경쟁 강도가 치열
- 고가 정밀 제품은 미국산 비중이 크나 중저가 물리보안시장 제품은 가격경쟁력이 높은 중국산이 강세

❑ 시장 규모 및 전망

▶ 2018년 기준 영국 사이버 보안시장 매출액은 전년대비 12.8% 증가한 6억 6,640만 파운드 추정

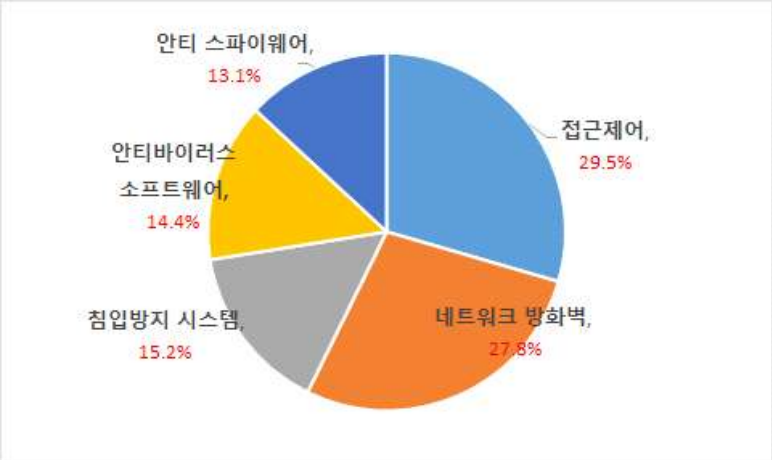
- 2017년 워너크라이(WannaCry*) 공격 등으로 영국 기업은 침입 방지 시스템에 대한 투자를 가속화하고 있으며, 영국 내 보안 소프트웨어를 개발하는 스타트업 수도 증가하고 있음

* 워너크라이(WannaCry) : 마이크로소프트(MS) 윈도 운영체제의 취약점을 노리는 랜섬웨어로 2017년 5월 12일부터 영국, 러시아, 중국 등 150여 개국에서 정부기관을 비롯해 글로벌 기업의 업무가 마비되는 등 20만여 건의 피해를 발생시킨 랜섬웨어(몸값(Ransom)과

소프트웨어(Software)의 합성어로 사용자의 데이터를 암호화해 접근할 수 없게 한 후 금전을 요구하는 악성 프로그램)

- 시장조사기관 IBIS World의 사이버 보안 소프트웨어 분석 보고서에 따르면 2013년부터 2018년까지 지난 5년간 영국의 사이버 보안 시장 매출액은 연평균 9.5%씩 증가했고, 시장 매출액은 향후 5년간 연평균 7.7%씩 증가하여 2023년 매출액은 9억 6,740만 파운드에 달할 것으로 전망
- 영국의 사이버 보안시장 점유율은 접근제어(29.5%)와 네트워크 방화벽(27.8%)이 절반 이상을 차지했고, 침입방지 시스템(15.2%), 안티바이러스 소프트웨어(14.4%), 안티 스파이웨어(13.1%) 순임

그림 _ 영국 정보보호 시장 분야별 점유율(2018~2019 추정치)



[출처] IBIS World, KOTRA 영국 런던무역관 재인용[28]

▶ 영국 디지털문화미디어스포츠부의 자료에 따르면 영국 사이버 보안 시장은 846개 회사가 활동하고 그 매출 규모는 56억 파운드로 추정[29]

- 영국 정부는 2016년에 새로운 5개년 전략을 발표하며 향후 5년간 사이버 보안 방위와 준비에 약 24억 달러를 투자할 예정이며, 투자 대상에는 새로운 국가 사이버보안센터(National Cybersecurity Centre)를 포함함
- 미국 상무부의 국제무역관리 자료[30]에 의하면, 영국 사이버 보안 시장은 약 50억 달러 가치를 지니며, 유럽에서도 가장 크고 가장 집중된 시장에 해당됨
- 2017년 영국 대규모기업의 73%가 사이버 공격&침해를 경험한 것으로 나타남
- 사이버범죄로 인한 영국의 피해는 약 30억 달러로 추정됨

---

28 https://news.kotra.or.kr/user/globalBbs/kotranews/782/globalBbsDataView.do?setIdx=243&dataIdx=171291
29 DMCS UK Cyber Sector Report, 2018.6
30 'United Kingdom – Cyber-Security' U. S. International Trade Administration(export.gov), 2019.8

▶ 소비자의 민감한 개인 정보를 다루는 금융기관과 기업 인트라넷에서 사용하는 소프트웨어 보안강화 등의 사이버 보안 관련 수요가 늘어나면서 해당 시장은 꾸준히 성장할 것으로 전망

- EU의 개인정보보호 일반규정(General Data Protection Regulations, 이하 GDPR)은 침해 보고를 의무화하고, 심각한 데이터 손실의 경우에는 글로벌 매출의 4% 또는 2천 5백만 달러까지 무거운 과징금을 부과함에 따라 사이버보안에 대한 지출을 촉진할 것으로 전망

▶ Homeland Security Research의 2017년 5월 자료에 의하면, 영국의 국토안보와 공공 안전부문의 2015-2020년 시장 연평균 성장률을 11.3%로 예상[31]

- 영국은 안보문제에 직면해 있으며, 극단이슬람(ISIS)의 테러위협은 감소할 조짐이 보이지 않음
- 영국 국토안보 시장연구에 의하면 2015-2020년 기간의 시장은 연평균 성장률 11.3%로 이전의 2010-2015년 기간의 연평균 성장률 2~3%보다 4배정도 크게 성장할 것으로 전망
- 이러한 시장성장은 국토안보출입국 강화 및 공공안전시장을 포함하며, 제품과 서비스는 현재와 유사한 부문에서 비즈니스 기회가 있을 것으로 예상됨

▶ HD급 CCTV의 수요가 급증하며 대세 인기품목으로 부상 중

- 주요 수요 품목은 IP CCTV, 모바일 CCTV, 자동차 번호인식, 안면 인식, 홍채 인식 등으로 신기술 제품 수요가 급증하고 있으며, 특히 CCTV 시장이 HD급 고화질 스크린 제품으로 급전환 중인 가운데 2016년 중 전체 CCTV 수요는 550만~600만 대 수준이 될 것으로 추정되었음
- 런던 히드로 공항은 2019년부터 안면 인식 시스템을 공항 전체에 도입하는 것을 목표로 5천만 파운드(약 736억 원)을 투자할 예정임

2) 분야별 현황

❑ 물리보안 제품

▶ 영국의 물리보안시장은 전통적으로 CCTV가 주력 제품

- 2007년에 들어 영국 CCTV시장은 공공수요 외에 증가세인 민간 수요가 가세하여 한 해 동안 400만대 이상이 판매되어 절정기에 도달했음
- 아날로그 CCTV는 2008년 금융위기 여파로 인한 경기침체 탓으로 2009년까지 수요가 28.2%나

31 Homeland security research, "UK Homeland Security & Public Safety Market – 2017-2022", May 2017.

감소하는 소강상태를 보였으나 2010년부터 수요가 다시 회복세로 회귀

- 낮은 규모(low-scale) 전자기기 보안에 대한 시장은 이미 포화상태이지만, 이들 사업자들은 각각 DVR, 접근제어, 생체인식, 전통적인 CCTV 등과 같은 특화된 프로세스로 전문화하는 경향을 보임

❑ 물리보안 서비스

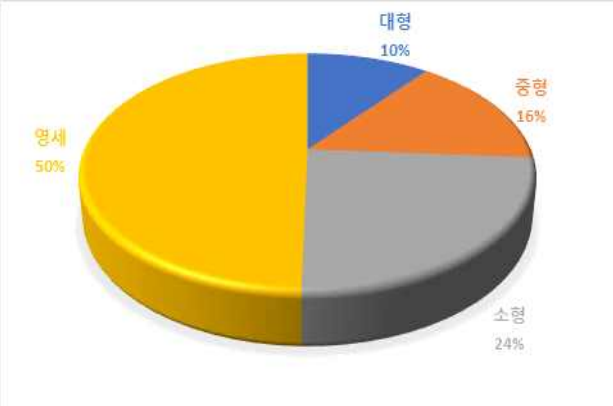
▶ 영국의 물리보안 서비스 업체는 4,800개 내외가 되는 것으로 집계되고 있고 연간 매출 규모는 26억 달러 수준이 되는 것으로 추산

- Barnes Reports에 따르면, 공식 등록업체 기준으로 70% 이상이 물리보안 업체로 파악되고 정보보안 서비스 전문 업체는 10%를 약간 넘는 492개 업체로 추정되는 정도로 물리보안 업체가 중심을 이루고 있는 상태

▶ 영국의 정보보호 서비스 업체들도 대부분이 소규모 업체로 구성

그림 _ 영국 정보보호 서비스 업체 규모별 비교

종류	기준	수	비율
대형회사	250명 이상	89개	11%
중형회사	50-250명 미만	132개	16%
소형회사	10-50명 미만	205개	24%
영세회사	10명 미만	420개	49%
합계	-	846개	100%



[출처] DMCS UK Cyber Sector Report, 2018.6

- 고용 규모 10명 미만의 영세회사가 전체 업체의 49%, 소형회사가 24%, 중형회사가 16%, 중소형회사가 전체의 89%를 차지함. 반면 250명 이상을 고용하는 회사는 89개로 전체의 11%뿐임

❑ 정보보안 제품 및 서비스

▶ 영국의 정보보안 시장은 기존 국방부 중심의 정부 각 부처의 국토방위 및 국가안보 관련 정보보안 수요가 중심에서 비즈니스에 심각한 타격을 받게 된 민간부문의 수요가 공공수요를 초과하여 급성장 중

• 영국정부는 국가 정보보안 역량 강화 특별 프로젝트로 2011-2015년 기간 중 사이버 보안 전문 업체인 BAE Systems를 통해 13억 달러를 투자하여 국가정보보안 프로그램(NCSP : National Cyber Security Programme)을 추진, 국가 정보보안 능력, 특히 네트워크 운영 기관의 보안역량 업그레이드 추진

표 _ 영국의 정보보안 시장 규모 추이

(단위 : 백만 달러, %)

구분	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025
규모	302	322	345	368	393	420	449	479	512	546	583
성장률	-	6.6	7.1	6.7	6.8	6.9	6.9	6.7	6.9	6.6	6.8

[출처] SDI, 'The Cyber Security Market in the United Kingdom to 2025: Market Brief'(2016.3)

▶ 물리보안 시장에 비해 정보보안 시장은 상대적으로 작은 규모를 형성

• 보안 전문 시장조사업체 SDI사에 따르면 영국의 정보보안시장은 2015년도의 경우 총 3억 200만 달러 규모로, 이중 인식 및 접근제어 부문이 가장 시장규모가 커 1억 3,500만 달러, 다음으로 네트워크 보안이 9,000만 달러, 데이터 보안은 5,000만 달러, 클라우드 보안은 2,700만 달러의 시장을 형성

표 _ 영국의 정보보안 시장 성장 전망

(단위 : 백만 달러)

구분	2015	2025	2015-25년 기간 중 총 시장규모	2015-25년 기간 중 연평균 성장률(%)
인식 및 접근제어	135	253	2,100	6.50
네트워크 보안	90	177	1.400	7.00
데이터 보안	50	94	774	6.50
클라우드 보안	27	58	449	8.00
합계	302	583	4,700	6.79

[출처] SDI, 'The Cyber Security Market in the United Kingdom to 2025: Market Brief'(2016.3)

3) 주요 사업자 현황

❑ 시장 특성 및 경쟁 강도

1) 물리보안 시장

▶ 유통 구조 및 시장 특성

- 영국의 물리보안 시장은 관련 제품의 국내 생산이 활발하기 때문에 유통 구조상 국내생산제품과 수입제품에 따라 다소 상이한 구조
- 이에 따라 가치사슬도 약간 상이한 구조를 가지며 전문 도매 유통업체는 특정 업체 및 브랜드의 독점 판매 에이전트 역할도 하지만 일반적으로 다양한 제품 및 브랜드를 국내의 다양한 지역의 소매상 및 SI 업체들에게 공급하는 패턴도 유지
- 최종 소비자 직전에 정보보안 컨설팅사가 개입하는 경우가 있는데, 이는 대기업, 유통업 등 다수의 매장을 운영하는 경우와 정부 조직 등에서처럼 더 전문적인 보안 제품과 시스템을 수요로 하는 경우

▶ 경쟁 강도

- 영국의 물리보안시장은 기존 가격경쟁 시장 구도에서 HD CCTV, 원격제어 감시 시스템 등 고도 기술제품으로 수요 중심이 전환되는 과정에 있으며 이를 충족시키는 미국, 일본 등 유명 브랜드 제품을 선호 하는 추세
- 이에 따라 가격경쟁력으로 시장 점유율을 확장해 오던 중국산, 대만산, 말레이시아 등 제품의 증가율이 다소 주춤해지고 있으나 여전히 중국산 등 저가 보안제품의 수요가 시장의 중심세력 구축 중

2) 정보보안 시장

▶ 유통구조 및 시장 특성

- 영국 정보보안 시장의 유통 구조는 ▲국토방위 및 정보기관, ▲정부 공공기관 ▲대기업, ▲중소기업 및 일반 소비자로 각각 카테고리 별로 특징이 구분되는 시장

① 영국 국방 및 정보기관 시장

- 국토방위 및 정보기관의 정보보안 수요는 공공입찰을 통한 정부조달시장을 통해 구매가 이루어지는데 사전 등록된 다국적 전문 방산제품 공급기업, 대형 컨설팅사, 다국적 HW/SW 벤더 등이 경쟁 입찰에 참가하여 공급

- 국방 및 정보기관 대상 정보보안 시장은 이미 보안상태가 검증된 공급업체가 아닌 한 신참기업이 참여하기도 어려운 자격요건을 요하므로 주로 미국 등 주요 선진국 다국적 기업들이 장악 중
- 시장규모는 2015년 기준 약 3억 7,600만 달러 정도로 추정되며 정확한 데이터는 기밀 사항으로 SDI사의 추정으로는 대략 2023년까지 연평균 12% 내외의 증가율을 보일 것으로 추산

표 _ 영국 국방부 정보보안 시장 추이

(단위 : 백만 달러)

구분	2015	2016	2017	2018	2019	2020	2021	2022	2023	연평균증가율
금액	376	411	453	498	548	613	687	790	908	12%

[출처] SDI, 'The Cyber Security Market in the United Kingdom to 2025: Market Brief'(2016.3)

- 2013년 통계를 기준으로 영국 국방 및 정보기관 정보보안 시장 중에서 가장 비중이 큰 부문은 정보보안에 가장 신경을 쓰고 있는 네트워크 보안으로 9,300만 달러 규모에 32%의 비중을 점유하였고 2023년도까지의 장기 전망으로는 시장 규모가 연간 2억 9,400만 달러에 이를 것으로 예상

표 _ 영국의 국방 및 정보기관 세부 정보보안 시장별 전망

(단위 : 백만 달러, %)

구분	2013	2023	'13-'23 합계	연평균 증가율
네트워크 보안	93	294	1,900	12.3
데이터보안	80	240	1,600	11.6
인식 및 제어	70	214	1,400	11.8
클라우드 보안	50	160	1,000	12.4
합계	293	908	5,900	12.0

[출처] SDI, 'The Cyber Security Market in the United Kingdom to 2025: Market Brief'(2016.3)

② 정부 공공기관 수요시장은 다양한 경로를 통해 조달하는 유통 구조

- 중앙 정부부처 및 산하기관 등은 엄격한 통제와 기밀을 요하는 국방 및 정보기관이 폐쇄적인 구매경로를 이용하는데 비해 정보보안 제품을 융통성 있는 경로를 통해 가격 경쟁력을 중시하는 구매패턴을 유지

③ 영국 정부 공공 정보보안시장은 중앙정부부처, 경찰, 지방정부/대학/건강보험 관련 조직 등 크게

세 카테고리로 구분

▶ 경쟁 강도

- 영국의 정보보안 시장은 유럽에서 가장 규모가 큰 시장으로 다국적 사이버 보안 컨설팅사, 전문 ICT 서비스 사업자, 다국적 HW/SW 벤더, VAR 등이 얽혀 단독 혹은 컨소시엄 형태로 입찰에 참여하면서 치열한 경쟁을 하는 경쟁강도가 높은 시장
- 특히, 일부 정보보안 중심기관들은 구매제품의 가격경쟁력보다는 해당 제품 공급사 및 브랜드의 보안성 및 신뢰도를 더 높게 보는 경향이 있어 지명도가 높은 다국적 기업들이 보다 유리한 입장

❑ 주요 사업자

▶ 정보보안 사업자

① G4S plc

- 세계 최고의 보안 회사로 보안컨설팅에서부터 전자기기 제품에 이르기까지 통합된 보안솔루션을 영국, 아일랜드, 아프리카, 아시아, 중동, 라틴아메리카, 유럽, 북아메리카에서 제공
- 주요 서비스는 설계, 구축, 통합시스템 뿐 아니라 분석과 지능, 기술과 소프트웨어, 컨설팅과 리스크 관리, 모니터링과 대응을 포함한 통합된 솔루션을 제공함
- 또한 현금관리 서비스, 전체적인 현금관리 전략과 현금 사이클 효율, ATM기 관리, 등에 대해 중앙은행과 상업은행에 자문 서비스 등 현금 솔루션을 제공
- 연락처 : Home Page - http://www.g4s.com/
  Tel.- 44(0)208-770-7000

② Exclusive Networks

- 이 업체는 영국계로 유럽 전역을 대상으로 정보보안 관련 VAD(Value Added Distributor)로 사업을 벌이고 있는 업체로 20여 주요 SW 벤더들의 제품을 취급하는 업체
- 20여 거래업체 중 정보보안 SW 벤더는 FireEye, Fortinet, SafeNet, Aerohive, Arbor, Aruba, Bit9, Palo, Alto 등 13개 업체
- 연락처 : e-Mail -info@exclusive-networks.co.uk
  Home Page - www.exclusive-networks.co.uk
  Tel. - 0845-521-7217, Fax - 01420-544799

③ Sophos

- 1985년에 설립된 영국의 대표적인 정보보안 업체로 영국 옥스퍼드셔와 미국 매사추세츠 두 곳에 본사를 두고 있는 기업
- 사업문야 : 통합위기관리(UTM : Unified Threat Management), 엔드 포인트, 암호화, 이메일, 웹, 모바일 보안 SW/HW 제공, 영국로컬 및 글로벌 기술 벤더로 1985년 안티바이러스와 암호화 제품을 출시하면서 정보보안 시장에 진출
- 중국, 일본, 싱가포르, 인도, 인도네시아 등 12개국, 1700여 명의 직원 고용 기업
- 연락처 : Home Page - http://www.sophos.com
  e-Mail : sales@sophos.com

④ Nexor

- 1989년에 설립된 기업으로 1992년도부터 본격적으로 정보보안 시장에 참여한 기업
- 주 사업 분야는 국방 및 정보기관, 발전소와 같은 중요한 인프라 보호를 위한 정보보안 분야이며 ISODE(ISO Development Environment) 연구개발 경험을 살려 군사정보전달체계(MMHS : Military Message Handling System)에 강점이 있는 기업
- 연락처 : Home Page - http://www.nexor.com/nexor-ukti
  Tel. -44(0)115-952-0500, e-Mail : info@nexor.com

⑤ Intercede

- 1992년도에 ID관리시스템 개발업체로 출범한 기업으로 대표 제품인 MyID를 현재 24개국에 수출하고 있는 기업
- 본사는 영국 Lutterworth 타운에 소재, 런던 증시에 상장 기업
- 주력제품인 MyID는 미국 조달청 GSA에서 최초로 인정한 전자 개인 ID 확인제품
- 주 기업 고객은 보잉, 록히드 마틴, 부즈 앨런 해밀턴 등이 있으며 미국, 영국 등의 주요 정부기관들도 ID 시스템으로 도입 사용 중
- 주요 비즈니스 파트너로는 BT, Gemalto, HP, Microsoft, Safenet, Symantec Thales 등
- 연락처 : Home Page - http://www.intercede.com
  Tel.- 44(0)1455-558-111, e-Mail – infor@intercede.com

▶ 물리보안 사업자

① Norbain

- 영국 전자보안업계에서 30년 이상 업력을 가지고 있는 영국 최대 보안장비 유통업체로서 17년 전부터 품질관리시스템인 ISO 9001.2000을 취득한 업체

- 활동지역은 전 세계 77개국에 진출하고 있으며 맨체스터에 있는 본사는 300명 이상의 인력을 고용
- 유럽 최대 유통망을 운영 중인 업체로 HID, GE, Panasonic 등 유명 브랜드 제품을 중심으로 취급, 기술력이 우수한 제품들을 선택, 유럽시장에 공급 중인 기업으로 2012년 투자기업 Newberry Investment Ltd.가 100% 지분을 인수
- 주요 취급 품목은 CCTV, IP 동영상 시스템, 접근 제어 통제 시스템, 침입자 감시 장비 및 시스템 등
- 연락처 : Home Page - www.norbain.co.uk
  Tel. - 0118-912-5000, Fax - 0118-912-5001

② ADI-Gardiner

- 50년간 보안장비 유통업을 해 온 영국 보안장비 업체의 대표 기업
- 전 세계 200여 개의 유통망을 통해 보안장비와 低 전력소비 제품 판매
- 국내 바이오 인식 솔루션 업체인 슈프리마의 바이오 인식제품 판매 업체
- 연락처 : e-Mail - websupport.uk@adiglobal.com
  Home Page - https://uk-eshop.adiglobal.com.
  Tel. : 01706-343-343, Fax : 44(0)207 902 7910

③ SSED Ltd. T/A Hunters Wholesalers

- 2005년에 설립된 전자 보안장비 전문 유통업체로 각종 화재경보, CCTV 보안 제어기기 등을 취급
- 다양한 벤더들의 제품을 취급하고 있는데, 예컨대 Honeywell MK, Honetwell ADE, Cooper Security, ICS Security, Fike, Klaxon, ESP UK, Visionic, Cytech Comfort Alarms, CDV, ICS Philex, Labgear 등이 주요 브랜드 임
- 연락처 : Home Page - www.hunters-wholesalers.co.uk
  e-Mail - sales@hunters-wholesalers.co.uk
  Tel. - 01628-669124, Fax - 01629-667710

④ Bosch Security Systems Inc.

- 독일의 보안제품 공급업체로 전 세계 CCTV, 침입방지 시스템, 음성인식 시스템 등 공급
- 영국 총괄대리점은 CSS Group PL
- 연락처 : Home Page -http://cssgroupplc.com/
  Tel. : 01489 566101, FAX : 01489 565375

⑤ Securitas

- 경호 보안업무가 주력이었던 Securitas는 2015년 10월 Diebold사를 인수합병하며 전자기기 보안

분야를 강화하고 보안 솔루션을 통합하였으며, 2016년 4월에는 CCTV, 접근 제어 등의 기술을 가진 독일의 Draht & Schutz을 합병하여 CCTV 부문의 기술을 강화함

- Securitas는 현재 전자기기 보안, 원격 보안 등 다양한 보안 제품을 제공하며 2015년에는 영국에서 민간 보안기업으로 매출액 기준 2순위를 차지함
- 연락처 : Home Page –http://www.securitas.uk.com
  e-mail: comms@securitas.uk.com

▶ 그 외 사업자

- **글로벌 정보보안 기술 벤더 및 시스템 통합(SI) 사업자:** IBM, HP와 같은 전 세계 IT시장을 주도하는 거대 IT 벤더들과 미국 CSC와 캐나다 CGI 그룹과 같은 IT 서비스 사업자들은 IT 인프라 구축과 함께 보안사업 비즈니스를 턴키로 수주하는 강력한 대형 사업자

▶ 방산 전문 업체

- 영국은 물론이고 전 세계 방위산업 시장은 특수시장으로 Thales, BAE Systems, Northrop Grumman 등 방산 전문 기업들이 참여
- 이들은 이미 영국 등 전 세계 방산 시장에 지명도가 높고 네트워킹이 구축되어 있는 기업들로 군용 SW나 솔루션만 판매하는 것이 아니고 다른 방산용 HW나 특수 목적 서비스를 담당하기도 함

① BAE Systems

- BAE Systems는 영국 런던에 기반하며 93,500명 이상의 직원을 가진 글로벌 방위 및 항공우주 시장에서 가장 큰 기업 중 하나에 해당
- 상업적인 사이버 성장 전략으로 2014년 Siversky를 인수하였고, 사이버와 지능 부문에서 시장에서의 존재와 역량을 더하기 위해 2010년 Stratsec Net Pty Ltd를 인수, 사이버 보안 등의 고객서비스와 지원 영역의 사업을 성장시키기 위해 2010년 SpecTal, LLC를 인수하였음

② Thales UK

- 프랑스에 기반한 Thales는 50여 개국에서 운영되고 있으며, 방위 계약자로 방위, 보안, 항공우주, 우주시장에서 정보시스템에 특화되어, 68,000명의 직원을 고용하고 있으며, 영국 시장은 1970년대 이후부터 운영해오고 있음
- Thales는 수익의 45%를 방위부문, 23%는 보안시장으로부터 얻고 있음
- 2013년 영국에서 새로운 사이버 통합 및 혁신 센터를 공개하였으며, 센터는 주요 국가 인프라, 정부, 상업적인 조직들의 보안의 향상을 지원하기 위해 설계된 사이버-보안 전투 실험실(battle lab)에 해당함

③ Northrop Grumman UK

- 미국에 기반한 Northrop Grumman은 글로벌 보안 회사로 전세계 정부, 상업적 고객에게 혁신적인 시스템, 제품, 항공우주 분야 솔루션, 전자기기, 조선, 정보시스템, 기술서비스 등을 제공함
- 영국에서 Northrop Grumman은 사이버보안과 정보 보증 서비스를 제공하며, 2012년에는 사이버보안과 보안 이동통신제품과 서비스를 제공하는 M5 Network Security Pty Ltd.를 인수하였음

4) 주요 동향 및 이슈

▶ 브렉시트(Brexit)의 불확실성으로 일부 건설 프로젝트 예산 승인이 지연되면서 정보보호 관련 수요가 일정 부분 영향을 받음

- 영국의 브렉시트 향방이 결정되지 않은 동안 보안 및 대테러 시장 동향은 큰 변화가 없었지만, 브렉시트의 불확실성으로 일부 건설 프로젝트 예산 승인 지연으로 수요에 일정 부분 영향을 받음
- 보안시장의 경우 건설 프로젝트 사이클의 영향을 받는 경우가 많은데, 시장조사기관 IHS Matkit에 따르면 2016년 브렉시트 국민투표 이후 영국의 건설업 경기는 7년 만에 최저수준으로 떨어진 상태임
- KOTRA 런던무역관에 따르면, 영국은 전역에 425만대의 CCTV가 설치돼 있어 신규 CCTV를 설치할 여력이 없다는 의견과 기존 영상보안장비 업그레이드 및 고성능 장비로 교체 수요가 늘어날 수 있다는 의견으로 전망이 엇갈리고 있다는 분석임

5) 정보보호 스타트업 시장 현황

▶ 영국 사이버보안 분야에서는 스타트업들이 두각을 나타냄[32]

- 영국의 사이버 보안 스타트업은 ID와 접속 관리 분야, 정보 보안과 협력 분야에 집중되어있음
- 사이버 보안 스타트업의 진출 분야가 산업 전 분야에 고르게 퍼져있다는 점에서 사이버 보안 시장의 건전성을 보여주고 있음
- 이와 같은 영국의 사이버 보안 스타트업체의 성장은 영국 정부의 큰 관심과 함께 대학과 협정된 투자의 증가가 뒷받침된 것으로 풀이

▶ 유망 사이버 보안 스타트업체들[33]

32 WaveStone, 2018 UK Cybersecurity Start-Up Radar, 2018.11.9.
33 Techworld, The UK's 13 most promising cybersecurity startups, 2017.7.11.
http://www.techworld.com/picture-gallery/security/uks-10-most-promising-cybersecurity-startups-2016-3634620/

① Darktrace(2013년 설립)

- 가장 성공한 영국 사이버 보안 스타트업으로, 사이버 침해사고 발생 전 범죄 패턴을 찾도록 인공지능기술을 사용하여 회사 네트워크 내 비정상적인 부분을 신속히 파악하는 시스템 보유
- 이러한 변칙을 탐지하는 기술은 현재 BT에 의해 재판매되고 있으며, Mike Lynch로부터의 투자를 받아 설립된 이후 2017년 7월에 7,500만 달러 투자를 받았으며 현재 가치는 8억 2,500만 달러에 해당함
- Darktrace는 캠브리지 수학과 출신학생들과 GCHQ(Government Communication Haedquarters) 출신들이 설립, 영국 캠브리지와 미국 샌프란시스코에 본사를 두고 있으며, 전 세계 23개 지사가 있음

② CybSafe(2015년 설립)

- 사용자의 실수에 의한 위험을 줄이기 위해 인간의 행동과학을 보안 이러닝 프로그램에 적용
- 직원이 제대로 훈련을 받지 못했거나 인식을 가지지 못한다면, 회사가 큰 위험에 처해있을 때 조직이 아무리 제때 좋은 기술을 가지고 있다 하더라도 이는 중요하지 않음을 전제로 함

③ ZoneFox(2010년 설립)

- ZonFox는 네트워크 동작을 조사하고, 실행 가능한 인사이트를 제공하며 의심스러운 활동에 경고를 보내기 위해 인공지능(AI)을 사용
- 최근 Archangels로부터의 투자를 이끄는 시리즈 A 펀딩 라운드가 완료되었고, ZoneFox는 에딘버그 본사를 3배 확대, 런던에는 한 개 팀을 구성할 계획임
- 고객으로 Rockstar Games, Zenith 은행을 포함하며, 비즈니스는 금융, 약학, 게임 부문으로 확대 중

④ StatusToday(2015년 설립)

- StatusToday는 '인공지능이 인간행동을 이해한다'는 브랜드를 사용하며, 기계학습을 사용하는 플랫폼은 직장에서 평범한 실수나 내부자의 공격 등의 인간 행동을 이해할 수 있게 함
- 2016년 2월에 Notion Capital을 포함한 벤처캐피탈 회사들로부터 seed 펀딩에서 1백만 파운드를 획득하였으며, 최근에는 영국 정보통신본부(GCHQ)의 인큐베이터 프로그램을 완료했음

⑤ Digital Shadows(2011년 설립)

- Digital Shadows는 특정회사에 대한 위협과 관련된 잡담을 수집하여 인터넷의 어두운 측면을 검색하는 데이터베이스 중심의 인식시스템에 기반을 둠
- 인식 시스템은 소셜미디어, 범죄 포럼, 깃허브(GitHub) 등을 포함하여 27개국 언어에서 1억 개에 해당하는 인터넷 소스를 검색함
- 시드 펀딩의 2차 라운드는 2011년과 2013년 총액 2백만 달러였고, 2015년 초 VC Storm Ventures에 의해 8백만 달러가 더 충원됨

정보보호 정책 및 기관 현황

1) 관련 법령 및 정책

❑ 관련 법령 및 규제

▶ 정보보호법(Data Protection Act 1998)

- 1998년 제정된 영국의 민감한 개인정보보호를 위한 기본법으로 몇 차례 개정된 가운데 최근 개정은 2018년 12월 17일 이루어짐[34]
- 개인정보보호법은 보호대상 개인정보 및 기타, 개인정보 관리자의 통보의무, 국가보안, 범죄 및 과세, 보건 교육 및 사회적 작업, 언론 문학 및 예술 관련 개인정보보호 예외 조항, 개인정보보호 효력 등에 대해 규정

▶ 컴퓨터 부정사용 방지법(Computer Misuse Act 1990)

- 법 제정일 및 코드: 1990. 06. 29일, 1990 Chapter 18
  수정법률 : Police and Justice Act 2006
- 주요 내용 : 승인받지 않은 자가 특정 컴퓨터 및 특정 프로그램 또는 데이터에 불법적으로 접속, 프로그램 변경, 해킹 등 부정한 방법으로 컴퓨터 악용을 방지하고 안전한 컴퓨터 사용 환경을 조성하려는 목적법
- 위반 시에는 12개월 이내 징역 및 법정 한도를 넘지 않은 범위 내의 벌금을 부과 처벌
- 승인받지 않은 자가 컴퓨터 시스템을 공격 또는 컴퓨터 내 자료를 변경하려 하는 경우는 형법에 정한 처벌 또는 만일 21세 미만인 자(잉글랜드 및 웨일즈는 18세)일 경우는 5년 이하의 징역 처벌 등 규정

▶ 조사권한 규제법(Regulation of Investigatory Powers Act 2000)

- 법 제정일 : 2000. 08. 01일 제정
- 범죄예방을 위해 규제기관인 공공 정보수사 조직에 대해 민간인 및 기업의 조사에 필요한 통신감청 및 모니터링 권한을 부여하는 것이 골자
- 총 5개장으로 구성되어 있고 인터넷 및 통신이용 내역, 개인 고객의 암호와 같은 개인정보에 대한 수사기관의 정보요구 권한 명시

▶ 사기방지법(Fraud Act 2006)

---

34 www.legislation.gov.uk 참조. http://www.legislation.gov.uk/ukpga/1998/29/contents

- 법 제정일 및 코드 : 2006. 11. 08일, 2006 Chapter 35
- 주요 내용: 직위 등을 사칭하거나, 정보공개 사기 행위나 직원 남용 등 관련 사기행위를 취한 자로서 약식 기소된 자는 12개월 미만의 징역형이나 법정 최고 기준 벌금형을 동시 부과하거나 선택적 처벌 조치(단, 북아일랜드는 6개월 징역), 정식 기소된 자는 10년 이하의 징역과 이에 상당하는 벌금을 병과 또는 선택적 부과

▶ 수사권법(Investigatory Powers Act 2016)

- 법 제정일 및 코드 : 2016. 11. 29일, 2016 Chapter 25
- 주요 내용 : 수사권법은 영국 수사기관에서 이동통신정보 등을 수집할 수 있도록 하는 근거를 마련, IT 기업들은 12개월간 이용자 데이터를 저장했다가 수사기관의 요청이 있을 때 그 데이터를 제공할 의무를 규정하였기 때문에 개인정보 침해 우려가 존재, 이를 보완하기 위해 일반적 개인정보보호 의무 규정을 삽입하여 개인정보 문제를 일부 완화[35]

▶ NIS 규정(The Network and Information Systems Regulations 2018)

- 법 제정일 및 코드 : 2018. 4. 19일, 2018 No. 506
- 주요 내용 : 2017년 2월 유럽네트워크정보보호원(ENISA, European Union Agency for Network and Information Security)은 'NIS 지침'에 대한 가이드라인을 발표하고, 정보보안 사고 발생 시 디지털서비스공급자(DSP, Digital Service Providers)에게 부과된 통지 의무 조항이 EU 전역에서 효과적으로 실행될 수 있는 방안을 제시
- 동 가이드라인은, 지침의 실행 과정에서 임시로 활용할 수 있는 개략적인 기술적 제안(Outline Technical Proposal)의 성격을 가지고 있음[36]

❑ 주요 전략 및 정책

1) 개 요

▶ 조직 체계

- 영국 정부는 2009년도에 정보보안체계 강화를 국가 최우선 과제로 지정하고 전략을 수립
- 내각부는 정보보호 정책 총괄 데스크 역할과 함께 각 정부 기관의 정보보호 활동 및 업무 조정 기능을 담당하고 산하에 사이버 및 정부 보안국(Cyber Government Security Directorate)을 두고 사이버 보안

35 http://www.legislation.gov.uk/ukpga/2016/25/contents/enacted
36 https://www.legislation.gov.uk/uksi/2018/506/made

업무를 감독

- 내각 각 부처의 담당 역할은 다음과 같음
  - 내무부(Home Office): 국가 주요 기반시설 보호
  - 외교부(Foreign & Commonwealth Office): 해외 정보보안 정보 수집 제공
  - 디지털문화미디어스포츠부(Department for Digital, Culture, Media & Sport): 문화, 미디어, 스포츠 및 디지털 분야 업무를 담당한다. 기존의 기업혁신기술부(Department for Business, Innovation & Skills)로부터 디지털 업무를 이관 받으며 사이버 보안 업무도 맡음
  - 국방부 산하 컴퓨터침해사고대응팀(Ministry of Defence, United Kingdom Computer Emergency Response Team) : 국가 사이버 보안 사고에 긴급히 대응하는 역할을 하는 국방부 산하 기관

2) 주요 정책 및 전략

▶ 영국의 사이버 보안 전략

- 영국정부는 1998에 제정된 정보보호법(Data Protection Act 1998)에 의거 정보보호관련 사항을 규제해 왔으나 컴퓨터 및 인터넷 사용 일반화에 따른 사이버 범죄의 확산추세와 개인정보보호, 민간부문의 사이버범죄 대응능력 제고를 위해 2009년 6월『사이버 보안전략』을 수립 발표한 바 있음
- 그 후 사이버 공격이 공공 및 민간 부문에 계속 증가함에 따라 보다 강력한 사이버 범죄 예방 및 퇴치를 위해 2011년 11월 新『사이버 보안전략』을 수립 발표

▶ 영국의 국가 사이버보안전략 2016-2021(National Cyber Security Strategy 2016-2021)[37]

- 영국은 2016년 11월 두 번째 국가사이버보안전략(National Cyber Security Strategy2016-2021)을 발표하였으며, 첫 번째 전략과 비교하여 영국을 온라인 사업을 하는 가장 안전한 곳으로 만들고자 함, 사이버보안에 대해 5년 동안 19억 파운드(약 23억 달러) 투자 계획
- 또한 방위와 보안에서 혁신적인 구매 지원을 위해 1억 6,500만 파운드를 방위 사이버 혁신 펀드(Defence and Cyber Innovation Fund)에 할당 계획
- 새로운 국가 사이버 보안전략의 비전을 실현하기 위해 ①방어(defend) ②억제(deter) ③개발(develop) 측면의 실천 목표 설정

▶ 영국의 민간 원자력 사이버보안 전략[38][39]

---

37 National Cyber Security Strategy 2016-2021, 2016.11.1.
38 Department for Business, Energy & Industrial Strategy, Civil Nuclear Cyber Security Strategy, 2017.2.14.
39 KISA, "영국, 민간 원자력 사이버보안 전략 발표", 2017.3.20.

- 2017년 2월 영국의 기업에너지산업전략부(Department for Business, Energy and Industrial Strategy, BEIS)는 디지털 위협으로부터 민간 원자력 부문을 보호하기 위해 민간 원자력 사이버보안 전략(Civil Nuclear Cyber Security Strategy) 발표
- 동 전략은 2016년 11월에 발표된 국가사이버보안전략에 대해 구체적으로 민간원자력부문에서 사이버위협에 대한 사이버안전과 복원력을 갖기 위한 전략에 해당하며, 안전한 클린 에너지 생산, 오래된 에너지시스템의 안전관리를 지원하고자 함

3) 주요 정책 내용

▶ Super-Connected Cities Programme 추진

- "Super-Connected Cities Programme"이란 영국정부가 시행하는 인터넷 환경 개선 프로그램으로 주요 22개 도시에 초고속 인터넷망을 보급하기 위해 추진 함
- 영국은 사업 추진을 위해 2011년에는 1억 파운드, 2012년도에는 5,000만 파운드의 예산을 투입하는 등 2017년까지 전국 95% 지역 이상에 초고속 인터넷 인프라망 구축을 완성하고 영국 전역에 무료 무선 인터넷을 보급하여 스마트폰, 태블릿 등 휴대용 통신기기 사용을 원활화시켜 나갈 계획

▶ 영국정부 "디지털 경제 전략 2015-18" 추진 중

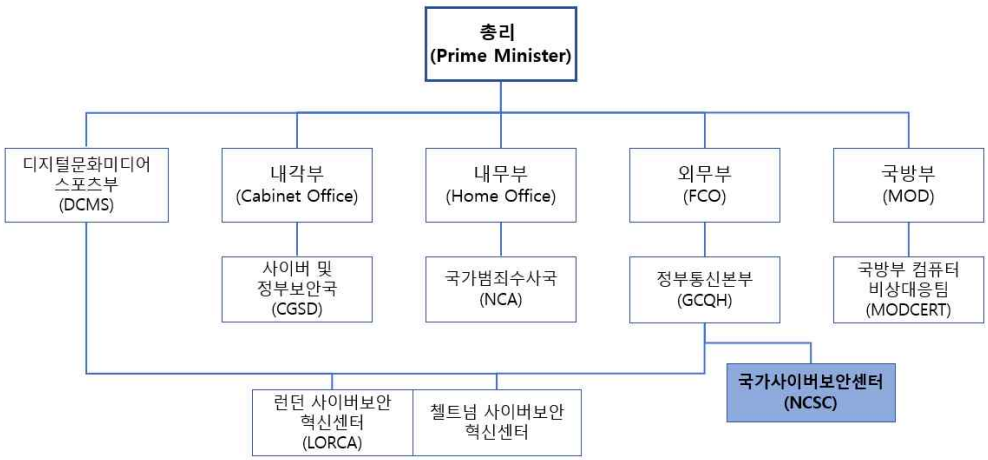
- 영국기술전략위원회(Innovate UK)SMS 2018년까지 디지털 혁신전략을 추진 중
- 동 전략은 2020년까지 영국 경제의 교통, 에너지, 헬스 분야의 혁신을 위해 이용자 편의 중심 디지털 솔루션 개발, 개인정보보호 및 데이터 보안 시스템 설계 지원 등 디지털 생태계 진입을 지원할 계획
- 4년간 매년 3,000만 파운드씩 총 1억 2,000만 파운드를 지원해 나가는 한편 관련한 혁신적인 비즈니스 프로젝트에 매년 1,500만 파운드씩 지원 계획

2) 담당기관

▶ 내각부(Cabinet Office)

- 2011년 시작된 영국의 사이버보안 전략은 내각부(Cabinet Office)를 중심으로 운영되고 있음
- 내각부는 정보보호 정책을 총괄하고, 정부기관의 정보보호 활동 및 업무의 조정을 담당하고 있음
- 내각부의 사이버보안 관련 산하기관으로는 사이버 및 정부보안국(Cyber and Government Security Directorate, CGSD)이 있음

그림 _ 영국 각 부처별 정보보안 관련 기구



출처 : 영국 내무부, 넥스텔리전스 가공, 2018.12

▶ 사이버 및 정부 보안국(CGSD, Cyber and Government Security Directorate)[40]

- 사이버 및 정부 보안국은 내각부 산하의 조직으로 국가사이버보안 프로그램 조정과 개인, 물리적, 정보 보안에 관한 정부와 국제적인 정책을 담당
- 사이버 및 정부 보안국의 목표로는 국가 사이버보안 전략(NCSS) 2016 - 2021 발표, 국가사이버보안 프로그램(NCSP) 2016 - 2021 5년간 운영, 국가사이버보안센터(NCSC) 설립 지원, 정부 보안을 위한 지속적인 정책 검토와 수립이 있음

▶ 영국방송통신우정청(Ofcom)

- Ofcom(Office of Communication) : 영국의 방송, 통신 및 우편산업 관리청으로 TV 및 라디오 방송, 통신 및 우편 분야에 막강한 권한을 가진 기관으로 2003년에 설립
- TV 라디오방송법, 일반적 권한법, 통신법, 영국 주파수배정규정 등에 의거 영국 내 방송 통신 우정분야의 안전 및 보안 업무 총괄

▶ 정보위원회(ICO : Information Commissioner's Office)[41]

- 영국의 공공이익 관련 정보접근권, 공공기관의 개방성 제고 및 개인정보보호 등을 담당하는 독립기관

40 https://www.gov.uk/government/groups/office-of-cyber-security-and-information-assurance

41 http://ico.org.uk/for-the-public

▶ 국가범죄수사국(NCA, National Crime Agency)

- 영국 정부는 지능화&국제화하는 중대 범죄에 대한 국가적 수사 대응력의 강화를 목표로 미국 연방수사국(FBI)과 같은 기능을 수행하는 국가범죄수사국을 2013년 10월에 창설. 국가범죄수사국은 연방수사국처럼 국가 차원의 중범죄 및 조직범죄의 수사를 담당하는 특별 수사기관임
- 국가범죄수사국은 '중대범죄수사국'의 기능과 조직을 흡수했으며 이에 더해 경제 범죄, 국제 인신매매, 사이버 범죄 등에 대한 수사 임무도 맡음. 그러나 테러대응 수사 업무는 런던경찰청과 국내정보국(MI5)에서 계속 수행함

▶ 정부통신본부(GCHQ, Government Communications Headquarters)

- 정부통신본부는 외무부 산하 통신정보기관으로서 전자기파, 음향, 그 밖의 설비로부터 나오는 방사물 등과 같이 정보자료와 관계되거나 이로부터 생산되는 정보를 획득/처리함.
- 이외에 정보 수집, 암호해독, 통번역, 전산망 상의 정보해독을 위해 수집된 정보를 국방부 소속 국방정보요원 등 전문가 집단에게 제공하고, 암호 관련 정책을 수립하여 지원하고 있음, 현재 산하에 전자통신 보안그룹(CESG, Communications-Electronics Security Group)을 두고 초현대식 감청시설을 보유 중

▶ 국가 사이버보안센터(National Cyber Security Center)

- 2016년 내각부가 발표한 국가사이버보안전략(NCSS)에 따라 영국 정부는 사이버보안 중추 기구로, 2016년 10월 국가사이버보안센터(NCSC)를 설립
- 국가사이버보안센터는 정부통신본부의 정보보증 담당 기구였던 전자통신 보안그룹(CESG), 영국컴퓨터침해사고대응센터(CERT-UK), 사이버평가센터(CCA) 및 내각부 산하의 국가기반시설보호센터(CPNI) 등 영국 사이버보안 관련 기구를 통합한 기관으로, 현재 영국의 사이버보안 정책 실무를 총괄하고 있음
- 국가사이버보안센터의 주요 임무는 국가 사이버보안 통합 담당기관으로서 ▲개인, 가정, 기업, 정부기관에 대한 사이버보안 대응은 물론 ▲사이버보안 관련 교육[42] ▲사이버보안 제품 및 서비스 인증[43] ▲사이버보안 기술 컨설팅 등 사이버보안 관련 폭넓은 영역을 담당
- 영국 산업계, 영국 정부 각 부처, 중요한 국가 인프라 및 민간중소기업 등을 대상으로 사이버 위협관련

---

42 국가사이버보안센터의 사이버보안 교육 프로그램으로는 11세~19세 학생 대상의 CyberFirst, 학사·석사·박사 학위 과정, 영국 내 세계적인 사이버보안 우수 대학 지원 프로그램(ACE-CSR), 사이버보안 학술연구 지원 프로그램, GCHQ 인증 교육 프로그램, 산업계 인력 교육 프로그램인 Industry 100, 전문가 인증 프로그램, 장기적인 사이버보안 전문가 개발 프로젝트인 CyBOK(Cyber Security Body of Knowledge), 사이버보안 기업을 지원하는 Cyber Accelerator 등이 있음

43 영국의 대표적인 사이버보안 프레임워크 보증(자격증 부여) 체계인 Cyber Essentials를 비롯해 사이버보안 관련 서비스, 제품 인증 제도, 사이버보안 전문가 자격증 제도 운영

신뢰할만하고 전문적이고 독립적인 가이드 제공
- 사이버 위협 및 취약점 심층 분석 및 사이버 보안관련 경고 발동

▶ 디지털문화미디어스포츠부(DCMS, Department for Digital, Culture, Media and Sport)
- 기존에 디지털 분야의 업무를 담당하며 사이버보안을 맡고 있던 주무 부처가 국가 산업 발전을 위해 정보보호 정책을 담당하는 기업혁신기술부(BIS)에서 문화미디어스포츠부(DCMS)로 변경되었다. 문화미디어스포츠부는 영국디지털전략(UK Digital Strategy)에 따라 디지털문화미디어스포츠부(DCMS)로 명칭을 변경하고 기업혁신기술부로부터 디지털 경제 정책 업무를 완전 이관 받음
- 산하에 런던사이버보안혁신센터(LORCA)를 두고 있음

3) 규제 및 인증제도

❑ 규제

▶ 핵심 내용[44] : 영국의 정보보호 관련 규제 내용은 EU 공동 규범을 적용 중

▶ 영국의 정보보호 규제는 하단의 EU 규제 내용을 포함
- 회원국은 네트워크 정보보안 전략 채택을 의무화하고 네트워크 정보보안 관련 위험과 사고에 대응하는 기관을 설립하고 적절한 자금과 인력을 제공할 것
- 회원국은 유럽 각 위원회 간 네트워크 정보보안 관련 위험과 사고를 대비하여 조기경보 공유 시스템을 구축할 것
- 금융, 수송, 전력, 건강보험 등 기간산업 사업자, 앱스토어, 전자상거래 플랫폼, 온라인 결제, 클라우드 컴퓨팅, 검색엔진, 소셜 네트워크 등 정보보안 서비스 제공업자 및 행정기관은 위기관리제도를 도입하고 핵심서비스의 보안 사고에 대한 보고를 의무적으로 이행해야 함

❑ 인증제도

1) 공공 인증기관

---

44 EC, Communication on a Cybersecurity Strategy of European Union, 2013.2.7.

▶ 담당 기관 : 국가사이버보안센터(NCSC : National Cyber Security Centre)

- 영국 정부기관 중 보안제품의 공식 인증업무는 2015년 11월에 내각부 산하에 설치한 국가사이버보안센터에서 담당

▶ 주요 담당 기능

- 상업용제품보증제도(CPA: Commercial Product Assurance)운영 : 동 제도는 상업용 제품 및 동 제품 개발자 등이 공지된 보안 및 개발 표준을 준수했는지 여부를 평가하고 인증기준인 상업용 보안규정을 준수한 제품인지 여부를 설명하는 평가등급(Foundation Grade)조건들을 충족하는 지를 평가하고 보증해주는 제도

▶ i-LIDS(Imagery Library for Intelligent Detection System)

- 영국 안전국 부설 CAST(Center for Applied Science and Technology)가 시행하는 지능형 CCTV 평가인증 시스템으로 수화물 검색, 주차차량 감시, 출입구 감시, 지역 감시, 열화상 감시, 다중카메라 등 6가지 분야에 대해 성능을 평가, 인증 수행

2) 비영리 민간기관

▶ 기관명 : 정보보안전문가연구원(IISP : Institute of Information Security Professionals)

- 영국의 공공 및 민간업계에 정보보안관련 전문적 표준을 제시하고 개별 정보보안 기술개발을 지도 및 지원하기 위한 네트워크를 제공하기 위해 설립된 비영리 민간기관
- IISP는 민간 및 정부부문에서 2,500여 개별 회원과 31개 기관회원 및 17개 학술 회원 보유

▶ 주요 기능

- IISP는 영국의 인증전문가기관을 이끄는 기구로 정보보안 및 인증업무 선도 기관
- IISP 기능의 핵심은 정보보안 전문가 역량 측정 표준으로 인정된 IISP 기술 프레임워크(IISP Skills Framework)
- 영국 정부의 외교부 산하 국가사이버보안센터(NCSC) 역시 정보시스템보안을 설계하고, 인증하는 공공부문 전문가들에게 요구되는 전문가적 역량을 키우기 위해 동 프레임워크를 채택

4) 최근 정책 동향 및 이슈

▶ 영국 정부는 최소사이버보안기준(Minimum Cyber Security Standard)을 발표(2018년 7월)

- 최소사이버보안기준은 정부 산하기관 및 군 관계기구와 유관 계약자들을 포함하는 모든 당사자들에게 적용되며, 당사자는 최소사이버보안기준을 준수하고 이를 초과할 정도의 보안수준을 유지해야 함
- 정부부처 및 조직들은 정부와 국가사이버보안센터가 함께 개발한 '최소한'의 기준을 반드시 충족하고, 가능한 그 기준을 넘어야함.
- 또한 향후 새롭게 나타나는 위협과 사이버취약계층을 보호하고, 신규 '적극적 사이버 방어' 정책을 사용할 수 있도록 최소사이버보안기준 정책은 계속해서 강화될 것으로 보임
- 최소사이버보안기준에는 ▲확인 ▲보호 ▲탐지 ▲대응 ▲복구의 총 5가지 범주의 10가지 분야가 명명되어 있음

▶ 영국 국립사이버보안센터는 기관을 위한 단계별 사이버보안 지침을 발표(2018년 5월)[45]

- 국립사이버보안센터는 사이버위협 증가에 대응하여 기관 자체적으로 시스템을 보호할 수 있도록 단계별 보안지침을 발표함. 단계별 사이버보안 지침은 즉시 조치사항, 수 주 내 조치사항, 사건발생시 조치사항으로 구분되어 대규모 기관에 적용됨
- 사고 발생 시 조치사항(If an incident occurs)으로는

2) 중대한 데이터 손실, 시스템 가용성 손상, 시스템 통제 상실

2. 접근권한이 없는 사용자의 IT시스템 무단 접근, IT시스템에 악성 소프트웨어 삽입 등이 있음

* 상기 상황 발생 시 NCSC 24/7 사고관리팀에 보고

▶ 영국 디지털문화미디어스포츠부(DCMS)는 소비자 IoT 제품의 사이버보안 개선을 위한 설계보안 보고서를 발표(2018년 3월)[46]

- 디지털문화미디어스포츠부(DCMS)는 소비자 IoT 제품의 보안성 보장을 위한 IoT 기회와 위협, 13개의 실천 강령(Code of Practice), 정부 및 산업계 실행방안, 국제적 공감대 형성 방안 등을 제시함
- 소비자 IoT에 대한 산업계 실천강령(13 지침)(Code of Practice for Industry on Consumer IoT)에는 기본 암호 사용 금지, 취약성 공개 정책 구현, 소프트웨어 최신성 유지 등의 13개 항목 존재

▶ 사이버보안이 미흡한 필수 서비스 운영자에게 새로운 벌금 부과 예정(2017년 8월)[47]

- 영국은 필수 네트워크와 인프라를 미래 사이버 공격의 위험에 대해 안전하고 복원력 있도록 만들려는

45 국가사이버보안센터(NCSC), 'Increased Cyber Threats: Security steps to take', 2018.5.16
46 DCMS, 'Secure by Design: Improving the cyber security of consumer Internet of Things Report', 2018.3.7.
47 Gov.UK, 'New fines for essential service operators with poor cyber security', 2017.8.8.

계획의 일부로서 제안된 내용은 필수서비스를 보호하기 위함

- 효과적인 사이버 보안 조치 실행에 실패한 필수서비스 사업자에 대한 벌금은 글로벌 매출의 4% 또는 1,700만 파운드 정도가 될 것임

▶ EU의 개인정보보호법 개정 주요 내용(2016년 5월)[48]

- 신법에 따르면 모든 가업들은 수집한 개인정보를 당사자 동의 없이는 공개할 수 없으며 소비자들의 사전 동의 받아야 개인정보를 사용할 수 있게 규정
- 해당 기업은 개인정보보호 사건이 발생하면 72시간 내에 신고하고 전문가의 조사를 받아야 하며, 조사결과 위법 사실이 발견되면 해당 기업은 전 세계 연 매출액의 4%까지 벌금 부과
- 또한, 개인정보보호법 의거 2018년 5월 25일부터는 잊힐 권리가 추가되어 이 시점부터 해당기업은 고객의 요구에 따라 개인정보를 삭제해야하며 신규 고개정보 수집할 경우는 정보의 삭제절차와 과정에 대한 사전고지를 해야 할 의무
- 개인정보보호의 책임주체는 해당 기업으로 해당기업은 해킹 및 악성 코드 삽입 등 사이버 범죄 방어 및 암호화 등 자체 정보보호 시스템을 구축하고 개인정보보호책임자(Data Protection Officer)를 두어야 하며, EU 역내에 서버를 두거나 영리 활동을 하지 않는 외국기업일지라도 인터넷을 통해 EU 시민의 개인정보를 취급하는 경우 자동적으로 이 법의 적용대상으로 간주

5) 정보보호 스타트업 관련 정책동향

▶ 영국은 사이버 보안 스타트업 지원을 위해 2018년 4월 1,350만 파운드를 투자하여 사이버보안혁신센터(Cyber Security Innovation Centre)를 설립

- 정부는 향후 3년 동안 최소 72개 기업이 사이버보안혁신센터를 활용하여 해당 시장 내 국제적인 지원을 받을 수 있도록 할 계획임

▶ 런던사이버보안혁신센터(LORCA, London Office for Rapid Cybersecurity Advancement)

- LORCA는 영국 정부(Department for Digital, Culture, Media & Sport) 기금으로 설립/운영되며 영국에 진출한 다수의 글로벌 보안 스타트업들을 선별해 컨설팅 전문기업 '딜로이트(Deloitte)', 영국 러셀그룹 명문대 '퀸즈 대학교 벨파스트(Queen 's University Belfast)' 등 다수의 기관으로부터 비즈니스 컨설팅과 엔지니어링을 제공하는 프로그램임
- 디지털문화미디어스포츠부(DCMS)가 총 1,450만 파운드를 투자해 런던 내에 신설한 기관. 국가사이버보안센터와

48 http://ec.europa.eu/justice/data-protection/ 및 KOTRA 런던무역관 시장동향 보고서(2016.05.16.)참조

더불어 사이버보안의 중심 기관임

- 디지털문화미디어스포츠부는 사이버보안 분야에 19억 파운드를 투자하는 계획의 일환으로 사이버보안 관련 스타트업 지원을 위한 프로그램을 실시함
- 운영기관으로 Wayra UK[49]를 선정하여 2016년 11월 사이버보안 스타트업 최종 선정 결과를 발표
- 한국기업 센스톤이 아시아계 스타트업으로는 최초로 LORCA에 공식 합격하여 프로그램의 지원을 받게 됨

▶ 국가사이버보안센터(NCSC)는 Wayra UK와 공동으로 차세대 사이버 보안 제품을 개발하기 위해 엑설러레이터 프로그램에 참여할 기업을 모집하는 프로그램을 개시함

- 2017년에 정부의 펀딩으로 설립된 NCSC는 기술 스타트업의 성장을 지원했으며 그 성과로 해당 프로그램의 이전 참여자기업은 2천만 파운드 투자금을 확보함

▶ 전 세계 우수한 재능을 보유한 인재들을 영국으로 유치하기 위한 노력의 일환으로 우수인재 비자(Tier 1 Exceptional Talent Visa) 정원을 기존 1,000명에서 2,000명으로 증가

- '인정된 리더(Recognised leader)' 자격으로 우수인재 비자를 발급 받은 경우 향후 영주권 신청 시 체류 기간 조건이 5년이 아닌 3년 적용하여 인재가 영국에서 체류하기 유리하게 개정

  * 우수인재 비자(Tier 1 Exceptional Talent Visa) : 과학, 공학, 인문학, 의학, 디지털 기술, 예술, 패션 분야에서 '우수한 재능(Exceptional talent)을 가졌다고 인정된 리더(Recognised leader)' 혹은 '특별한 가능성(Exceptional promise)을 지니고 있는 차세대 리더(Emerging leader)'에게 주어지는 비자

49 Wayra UK: 스페인의 대형 통신사 텔레포니카(Telefonica)가 스타트업을 지원하기 위하여 설립한 지원 기관

융합보안시장 및 정책 동향

자율주행차

▶ 영국 정부 스마트카의 사이버 보안 가이드라인 발표(2017년 8월)[50]

- 영국 교통부(Department for Transport)는 인터넷으로 연결된 커넥티드카와 자율주행차의 사이버보안을 위한 8대 원칙을 담은 가이드라인 발표
- 스마트카와 같은 글로벌 산업을 지원하기 위해 영국 교통부는 국가 주요기반시설 보호센터(Centre for the Protection of National Infrastructure, CPNI)와 함께 제조 공급망에 포함된 모든 이해관계자들에게 일관성 있는 가이드라인을 제공하고자 함
  - ① 조직의 보안은 이사회 차원에서 소유, 관리, 승격됨
  - ② 보안 위험은 공급망에 구체적인 것을 포함하여 적절하고 균형있게 평가되고 관리됨
  - ③ 조직은 시스템이 시스템수명에 걸쳐 안전하다는 것을 확신하기 위해 제품의 판매 후 관리와 사고 대응이 필요함
  - ④ 하청업체, 공급업체, 잠재적인 제3의 업체들을 포함한 모든 조직들은 시스템의 보안을 향상시키기 위해 함께 협력해야함
  - ⑤ 시스템은 심층방어접근방법을 사용하여 설계됨
  - ⑥ 모든 소프트웨어의 보안은 소프트웨어의 수명동안 관리됨
  - ⑦ 데이터 스토리지와 전송은 안전하고 제어될 수 있음
  - ⑧ 시스템은 공격에 대해 회복될 수 있고, 방어나 센서가 작동하지 않을 때 적절히 대처할 수 있도록 설계되어야 함

▶ 영국은 자율주행차 및 스마트카에 관한 책임을 보험회사에 부과하는 자율주행전기차법(Automated and Electric Vehicles Act) 실행[51]

- 영국 정부는 2021년까지 자율 주행차의 상용화를 목표로 3년간 법규 검토를 하고, 자율 주행차 관련 22개 기술 연구 프로젝트에 2200만 파운드를 투자하고, 자율 주행차와 친환경 자동차에 총 10억 파운드를 투자할 예정임
- 2018년 3월 영국 국가사이버보안센터는 사물인터넷(IoT), IP카메라 등 인터넷이 연결된 제품을 대상으로 한 가이드라인 발표함. 가이드라인에는 제품 출시할 기본 암호를 고유하게 설정도록 하는

50 Department for Transport, "The key principles of vehicle cyber security for connected and automated vehicles", 2017.8.6.
51 legislation.gov.uk, Automated and Electric Vehicles Act 2018, 2018.7.19

등 보안조치를 강화하는 내용이 담겼으나 법적 구속력이 없어서 실효성이 떨어진다는 문제점 존재함

사물인터넷(IoT)

▶ 2019년 5월 2일, 영국 정부는 소비자 IoT 보안 관련 신규 법안을 발의함

- 디지털문화미디어체육부 장관 마고 제임스가 인터넷에 연결된 모든 기기를 '설계 단계부터' 사이버 공격으로부터 안전하게 보호하기 위한 소비자 IoT 보안 관련 신규 법안을 발의
- 업계 전문가 및 이해 관계자들의 참여로 지금까지 3가지 방안이 제시되었다. 그중에는 영국 내 판매되는 스마트TV와 가전 등의 기기 전체에 '보안 인증' 라벨 부착을 의무화하는 방안도 있음
- 이 밖에 전 IoT 제품에 그 어떤 범용 공장 설정으로도 재설정될 수 없는 고유의 암호를 두라는 내용이 포함된 일반 지침과 실천 요강도 언급
- 여기에 따르면, 제품 제조사의 공개 연락처는 물론, 제품이 주기적인 보안 업데이트를 받을 수 있는 최소한의 기간을 명시해야 함

▶ 2018년 3월 영국 디지털문화미디어스포츠부는 소비자 IoT 제품의 사이버보안 개선을 위한 설계보안 보고서(Secure by Design: Improving the cyber security of consumer Internet of Things Report)를 발표함

- 디지털문화미디어스포츠부는 ▲소비자 IoT 제품의 보안성 보장을 위한 IoT 기회와 위협 ▲13개의 실천 강령(Code of Practice) ▲정부 및 산업계 실행방안 ▲국제적 공감대 형성 방안 등을 제시함

▶ 소비자 IoT 행동강령(Code of Practice for Consumer IoT Security)

- 법 제정일 및 코드 : 2018. 10. 14일
- 주요 내용

소비자 IoT 행동강령에는 소비재 제조업체들이 제품 제작에서 구현해야 할 13개의 지침들이 제시되어 있음.[52] 구체적으로 개인 데이터 안전 저장, 정기적 소프트웨어 업데이트, 데이터 삭제 용이, 디폴트

52 1. 기본 암호 사용 금지
2. 취약성 공개 정책 구현
3. 소프트웨어 최신성 유지
4. 크리덴셜 및 민감정보 안전한 저장
5. 안전한 통신
6. 공격표면 노출 최소화
7. 소프트웨어 무결성 보장
8. 개인정보보호
9. 정전에 대비한 시스템 복원력 확보
10. 원격측정 데이터 감시
11. 소비자의 개인정보 삭제 편의성

패스워드 제한 등을 규정. 유럽연합의 일반 정보 보호 규정(GDPR: General Data Protection Regulation)에 따라 데이터 보호법을 준수하는 방향으로 수정됐으며, 위반 시 최대 £1700만(220억원) 혹은 매출액의 4%의 벌금이 부과될 수 있음. 소비자 IoT 행동강령은 단기적인 보안성 향상을 위해 IoT 기기의 기본 비밀번호를 삭제하고, 독특한 비밀번호 설정, 취약성 공지를 위해 문제 발생시 보고해야할 공공 연락망을 제공하고, 정기적인 소프트웨어 업데이트 및 패치(Patch)를 설치하는 것을 최우선으로 함

스마트의료

▶ 의료기관은 데이터 및 기술에 적용되는 모든 규정을 준수해야 하며, 특히 데이터 보안 및 개인정보보호법을 위반하지 않도록 주의가 필요

- 2018년 5월부터 유럽연합 일반개인정보보호법(GDPR, General Data Protection Regulation)이 시행되었으며, 이를 통해 제3자에 의한 개인정보 사용에 대한 통제를 보다 효과적으로 할 수 있게 됨에 따라 의료 데이터보안 기능 또한 크게 강화됨

블록체인

▶ 영국 금융행위감독기관(FCA: Financial Conduct Authority), 암호화폐 자산에 대한 최종 가이드라인 발표

- 2019년 7월 31일, FCA는 암호화폐 자산 지침서에서 비트코인(BTC)를 규제하지 않겠다고 발표함
- FCA는 PS19/22: 암호화폐 자산에 대한 지침서(PS19/22:Guidance on Crypto on Cryptoassets)라는 제목의 문서를 통해 암호화폐 정책 최종 지침서를 발행, FCA는 2019년 1월 대중들의 의견을 위해 처음으로 암호화폐 자산 관련 문서를 발행했으며 디지털 자산의 기존 형태에 대한 규제 명확화에 목적을 두었음. 지침서에 따르면 FCA는 비트코인, 이더리움 등과 같은 주요 암호호폐를 교환 토큰으로 정의했으며 주로 탈중앙화되고 거래의 수단으로서 사용되는 암호화폐 자산의 형태라고 정의함. 또한 FCA는 이러한 디지털 화폐가 FCA의 규제 범주 안에 들지 않으나 증권형 토큰이나 유틸리티 토큰 등과 같은 디지털 화폐의 다른 두 형태는 규제의 대상이 된다고 구별함

스마트 시티

▶ 영국 스마트 시티 정책의 특징은 정부가 주도하거나 사회를 이루는 다양한 구성원들의 참여를 요구하는

---

12. 기기 설치 및 유지보수 용이성
13. 입력 데이터 유효성 검사

방식

- 정부가 주도하거나 정부 부처 중 한 곳이 정책을 이끄는 것이 아닌 지방차치단체, 대기업 및 스타트업부터 대학교 및 시민사회까지 계획에 동참시킴으로써, 영국 실정에 맞는 실질적인 스마트 시티의 모델을 구성해 가는 것에 중점을 둠

▶ 영국의 첫 스마트시티 계획은 2013년 Future of cities 프로젝트에서 구체화[53]

- 영국 정부 산하 조직 중 하나인 innovate UK가 프로젝트를 수행하면서, 여러 경쟁 도시 중 스코틀랜드 공업 도시인 글래스고를 선정하면서 글래스고가 영국 최초의 스마트 시티 프로젝트 도시가 됨
- 이후 보조금을 2,400파운드를 지원받고 도시 곳곳에 CCTV 설치, 인공지능 가로등 설치, 실시간 교통정보, 대중교통 도착시간 알림 앱 제공 등을 통해 시민들의 공공안전, 에너지 효율 증가, 편의성 증대 등을 이루어 내 영국의 대표적인 스마트시티로 꼽히고 있음

▶ 2015년 브리스톨 스마트 시티 추진[54]

- 브리스톨 시와 브리스톨 대학이 합작하여 만들어진 회사 '브리스톨 이즈 오픈(Bristol is Open)'이 추진한 스마트 시티 프로젝트
- 연구·개발(R&D) 단계에서의 스마트 시티 모델을 실질적인 비즈니스로 구체화 하여 상업화 단계로 유기적으로 옮겨 가는 정부 및 산학 협력 형태
- 여러 방면으로 수집한 정보를 공공데이터로서 대기업·스타트업 및 일반에 공개하여 실생활에서 활용할 수 있도록 함
- 2019년 9월, 기존 프로젝트의 일부 한계점을 개선하기 위해 6개의 주된 과제를 목표로 한 스마트시티 고도화 전략 발표[55]

▶ 2018년 Smarter London Together 계획을 통해 런던 스마트 시티 로드맵 발표[56]

- 2013년 발표한 Smart London Plan이 토대가 된 것으로, 기존 청사진에 대한 구체적인 계획에 해당
- 계속된 인구 집중으로 인구 1천만 명을 곧 초과할 것으로 전망되고, 부수적으로 대기 오염, 쓰레기 처리, 교통체증, 범죄 증가 등의 문제가 나타날 것으로 예상되면서, 도시 관리의 효율성을 높이고 시민의 삶의 질 향상을 위하여 스마트 시티 프로젝트를 추진
- 정부 주도가 아닌 지자체, 공공기관, 대학 및 시민들의 참여형 프로젝트로, 다섯 가지의 구체적인

---

53 http://smartcity.go.kr/wp-content/uploads/2019/08/1-201909_auri_%EB%9F%B0%EB%8D%98-%EC%8A%A4%EB%A7%88%ED%8A%B8%EB%8F%84%EC%8B%9C-%EA%B4%80%EB%A0%A8-%EC%A0%95%EC%B1%85%E3%86%8D%EC%A0%9C%EB%8F%842019.pdf

54 http://magazine.hankyung.com/business/apps/news?popup=0&nid=01&c1=1011&nkey=2018052101173000071&mode=sub_view

55 https://www.connectingbristol.org/strategy/

56 https://ubin.krihs.re.kr/ubin/wurban/maincitynews_View.php?no=1814&thema=%EC%98%81%EA%B5%AD&start=0

목표를 설정(▲사용자 친화적 서비스 디자인 ▲공공 데이터 활용 ▲세계적 수준의 연결성과 도로망 ▲디지털 리더십 및 기술 향상 ▲도시 전반의 협력 강화)[57]

- 매년 전 세계 스마트 시티 순위를 발표하는 스페인 바르셀로나 IESE 비즈니스 스쿨의 2019년 발표에서 런던이 1위를 차지

57 https://www.london.gov.uk/what-we-do/business-and-economy/supporting-londons-sectors/smart-london/smarter-london-together

3. 아시아 시장

아시아 시장 개요

▶ 아시아지역은 유라시아대륙에서 유럽을 제외한 부분으로 면적은 약 4,398만㎢, 세계 인구의 약 60%인 약 43억 명이 거주하며, 다양한 민족과 문화가 공존

- 아시아지역은 지리적·문화적 특성에 따라 다시 동아시아·동남아시아·중앙아시아·남아시아·서남아시아 로 구분
- 본 보고서의 아시아지역은 중국과 인도, 동남아시아 지역 국가를 중심으로 조사·분석을 실시하였고, 중동지역은 분리하여 다른 장에서 내용을 서술
- 베트남은 2018년 우리나라에게 중국, 미국에 이은 세 번째로 큰 수출규모를 보임

표 _ 아시아 시장 주요국의 한국과의 관계(2018년 기준)

항목	수교일	우리나라 수출규모 (US$ 백만)	우리나라 수입규모 (US$ 백만)	우리나라의 주요수출품	우리나라의 주요수입품
중국	1992. 8	162,125	106,489	집적회로반도체, 평판디스플레이, 합성수지	집적회로반도체, 기타정밀화학원료, 컴퓨터
인도	1973	15,606	5,885	집적회로반도체, 합성수지, 자동차부품 등	나프타, 알루미늄괴 및 스크랩, 기타정밀화학원료 등
인도네시아	1973	8,833	11,161	휘발유, 합성수지, 집적회로반도체, 등	유연탄, 천연가스, 기타금속광물, 신발
베트남	1992. 12.	48,622	19,643	집적회로반도체, 평판디스플레이	무선통신기기부품, 직물제의류
캄보디아	1997.10.	660	314	화물자동차, 음료, 편직물	편직제의류, 직물제의류, 신발
태국	1958.10	8,505	5,582	열연강판, 냉연강판, 합성수지	집적회로반도체, 당류, 보조기억장치
말레이시아	1962.2	8,994	10,206	경유, 집적회로반도체, 합성고무, 선박	천연가스, 집적회로반도체, 중유, 컴퓨터부품
라오스	1995.10 (외교관계 재개)	84	30	자동차부품, 화물자동차, 승용차, 원동기	기타목재류, 계측기, 커피류, 칼륨비료

[출처] Kotra-국가별 정보

▶ 국제전기통신연합(ITU)은 인터넷 사용, 유무선 초고속 인터넷 가입자 등과 ICT 스킬(문맹률, 고등교육진학률) 등 측정항목에 가중치를 부여하여 종합적인 ICT 발전지수(ICT development Index, IDI)를 측정하여 국가 간 비교를 하고 있음

- 아시아 국가들의 IDI는 국가별로 격차를 보이면서도 타권역에 비하여 비교적 양호한 수준을 보임
- 2017년 글로벌 ICT 발전지수(ICT Development Index, IDI)에 따르면 아시아 지역 국가들의 ICT 발전지수 순위는 국가 간 큰 격차를 보이고 있음
- 이번 조사국 중에서는 중국과 태국, 말레이시아가 IDI 종합 순위에서 100위권 안에 들어 있는 것으로 나타났으나, 인도 등 다른 국가들은 100위~140위 사이에 포진해 있음

표 _ 아시아시장 주요국 ICT발전지수(IDI)

국가	IDI(2017년)		접근성(access)		이용성(use)		(skill)	
	순위	지수	순위	지수	순위	지수	순위	지수
중국	80	5.60	89	5.58	69	5.27	81	6.28
인도	134	3.03	137	3.60	144	1.62	121	4.73
인도네시아	111	4.33	105	4.85	115	3.19	109	5.54
베트남	108	4.43	108	4.75	102	3.65	113	5.31
캄보디아	128	3.28	124	4.16	119	2.56	150	2.98
태국	78	5.67	91	5.48	68	5.33	70	6.72
말레이시아	63	6.38	62	6.93	48	6.17	101	5.70
라오스	139	2.91	140	3.47	132	1.90	136	3.78
한국	2	8.85	7	8.85	4	8.71	2	9.15

[출처] ITU, ICT Development Index 2017, https://www.itu.int/net4/ITU-D/idi/2017/index.html

▶ 국제전기통신연합(ITU)은 법적, 기술적, 조직적 대응 및 역량강화, 국제협력 등 5개 부문의 지수를 종합하여 글로벌 사이버보안지수(Global Cybersecurity Index, GCI)를 측정하여 국가 간 비교를 함

- 2018년 글로벌 사이버보안지수(GCI)에 따르면, 일부 아시아 국가들의 글로벌 사이버보안지수 순위는 세계 상위권으로 싱가포르의 GCI는 0.898점으로 세계 6위, 말레이시아는 8위, 호주는 10위를 기록

표 _ 아시아-태평양 지역 글로벌 사이버보안지수(GCI) 상위 3개국 주요 내용

국가	GCI(2018년)		법적(Legal)	기술적 (Technical)	조직적 (Oranizational)	역량강화 (Capacity building)	국제협력 (Cooperation)
	순위	지수	지수	지수	지수	지수	지수
싱가포르	6	0.898	0.200	0.186	0.192	0.195	0.125
말레이시아	8	0.893	0.179	0.196	0.200	0.198	0.120
호주	10	0.890	0.200	0.174	0.200	0.176	0.139
한국	15	0.873	N/A	N/A.	N/A	N/A	N/A

[출처] ITU, Global Cybersecurity Index(GCI) 2018,

▶ 유엔무역개발기구(UNCTAD)는 금융기관 또는 모바일 머니 서비스 제공업체의 계정 소유권, 인터넷을 사용하는 개인, 우편물 신뢰성 지수, 안전한 인터넷 서버 등 4개의 지수를 종합하여 B2C 전자상거래 지수(B2C e-Commerce Index)를 측정하여 국가 간 비교를 함

• 2019년 전자상거래 지수에 따르면, 대부분의 아시아 지역 국가들의 B2C 전자상거래 지수 순위는 세계 상위, 중위, 하위권으로 넓게 분포하고 있으며, 말레이시아의 B2C 전자상거래지수는 81.9점으로 세계 34위, 태국은 48위, 중국은 56위, 베트남은 64위, 인도는 73위를 기록함

표 _ 아시아시장 주요국 B2C 전자상거래 지수

국가	전자상거래지수 (2019)		인터넷 사용하는 개인	계정 소유권	안전한 인터넷 서버	우편물 신뢰성 점수
	순위	지수	지수	지수	지수	지수
중국	56	68.8	54	80	55	85
인도	73	57.0	34	80	48	65
인도네시아	84	50.1	40	49	64	48
베트남	64	61.1	70	31	66	77
캄보디아	122	30.8	40	22	41	20
태국	48	73.5	57	82	61	94
말레이시아	34	81.9	81	85	75	86
라오스	113	35.1	26	29	30	56
한국	19	89.4	96	95	67	99

[출처] UNCTAD, B2C e-Commerce Index 2019, https://unctad.org/en/PublicationsLibrary/tn_unctad_ict4d14_en.pdf

▶ 글로벌 시장조사기관인 MarketsandMarkets이 발표한 물리보안시장에 대한 보고서에서는 물리적 보안 시장 영역을 시스템 분야와 서비스 분야를 포함하여 시장 규모를 발표함

- 시스템 분야에는 물리적 접근 제어 시스템, 비디오 감시 시스템, 경계 침입 탐지 및 예방, 물리적 보안 정보 관리, 물리적 신원 및 접근 관리, 보안 검색, 이미징 및 금속 탐지, 화재 및 생명 안전에 대한 시스템이 포함
- 서비스 분야에는 서비스 분야에서 서비스로써의 접근 제어, 서비스로써의 비디오 감시, 원격 모니터링 서비스, 보안 시스템 통합 서비스를 포함
- 아시아지역 국가들이 제조업 기반이 증가하는 신흥 경제국이며 지 지역에 테러 위협의 지속적인 위험이 있어 물리보안 채택이 증가할 것으로 예상하며, 특히 인도와 중국의 안보 문제가 증가하여 높은 성장 잠재력을 갖고 있으며 이들 국가의 정부가 안보에 크게 투자하기 시작했음
- 물리보안 시장규모는 2018년 중국의 경우 97억 2천만 달러 규모로 연평균 성장률(2018-2023) 9.2%로 성장할 것으로 전망

표 _ 아시아 지역 주요국 물리보안 시장규모 (단위 : 십억 달러)

국가	2016	2017	2018e	2023p	연평균성장률 (2018-2023)
중국	7.56	8.60	9.72	15.12	9.2%
기타 아시아*	4.48	4.97	5.44	7.85	7.6%
합계	10.08	11.27	12.48	18.5	8.2%

주) 중국과 일본을 제외한 지역으로 호주, 한국, 말레이시아, 싱가포르, 홍콩, 뉴질랜드, 인도, 대만이 포함됨

[출처] MarketsandMarkets, Physical Security Market-Global Forecast To 2023, 2019

▶ 글로벌 시장조사기관인 MarketsandMarkets이 발표한 정보보안시장 보고서에 따르면, 아시아 지역의 정보보안 시장은 2018년 211억 8,000만 달러로 추산되며, 2023년경 423억 5,000만 달러에 이를 전망

표 _ 아시아 지역 주요국 정보보안 시장규모

(단위: 십억 달러)

국가	2016	2017	2018e	2023p	연평균성장률 (2018-2023)
중국	5.68	6.51	7.37	12.83	11.70%
기타 아시아	9.84	11.72	13.81	29.52	16.41%
합계	15.52	18.23	21.18	42.35	14.86%

[출처] MarketsandMarkets, Physical Security Market-Global Forecast To 2023, 2019

▶ 글로벌 시장조사기관인 MarketsandMarkets이 발표한 서비스형 보안시장에 대한 보고서에서는 서비스형 보안은 클라우드 기반 모델이며, 보안 공급 업체는 클라우드 및 사내 환경에서 엔터프라이즈 네트워크, 애플리케이션 및 데이터를 보호하고 유지 관리함

- 아시아 지역 국가들이 클라우드 기반 애플리케이션을 광범위하게 채택하여 클라우드 기반 보안 솔루션에 대한 수요가 높아지며 높은 성장세를 보임
- 서비스형 보안 시장규모는 2018년 중국의 경우 4억 9,960만 달러 규모로 연평균 성장률(2018-2023) 19.6%로 성장할 것으로 전망하며, 인도는 2억 5,220만 달러 규모임

표 _ 아시아 지역 주요국 서비스형 보안 시장규모

(단위: 백만 달러)

국가	2016	2017	2018e	2023p	연평균성장률 (2018-2023)
중국	314.6	399.6	499.6	1,224.6	19.6%
인도	148.1	194.8	252.2	699.1	22.6%
기타 아시아	405.6	522.0	661.4	1,703.6	20.8%

[출처] MarketsandMarkets, Security As a Service Market-Global Forecast To 2023, 2019

▶ 글로벌 시장조사기관인 MarketsandMarkets이 발표한 IoT 보안시장에 대한 보고서에서는 IoT 보안 시장은 연결된 장치의 네트워크를 보호하고 연결된 장치의 위협 및 사이버 공격으로 인한 손실을 최소화하기 위해 제공되는 솔루션 및 서비스가 포함됨

- 아시아 지역은 가장 높은 연평균 성장률(2018-2023)으로 성장할 것으로 예상되며, 주요 요인은

증가하는 정부 이니셔티브, 빠른 컴퓨팅, 가상화된 환경, 분석, 보안, 디지털화 및 대용량 네트워크에 대한 요구 증가, 전반적인 인터넷 속도와 응답성 향상을 들 수 있음

- IoT 보안 시장규모는 2018년 중국의 경우 5억 7,170만 달러 규모로 연평균 성장률(2018-2023) 39.8%로 성장할 것으로 전망하며, 인도는 2억 5,340만 달러 규모이고, 기타 아시아 국가들은 4억 4,820만 달러 규모임

표 _ 아시아 지역 주요국 IoT 보안 시장규모 (단위 : 백만 달러)

국가	2016	2017	2018e	2023p	연평균성장률 (2018-2023)
중국	335.3	436.9	571.7	3,051.3	39.8%
인도	149.0	193.9	253.4	1,324.1	39.2%
기타 아시아	260.8	341.2	448.2	2,363.3	39.4%

[출처] MarketsandMarkets, IoT Security Market-Global Forecast To 2023, 2019

▶ 아시아 시장의 주요 진출 전략은 다음과 같음

- 한국과 유사한 내용으로 현지 정부의 관련법령 제·개정 및 제도 도입을 지원·유도함으로써 국내기업에 유리한 시장환경 조성
- 국가별로 정부수요가 큰 관심분야를 선별하여 원조사업(ODA/EDCF)을 추진하거나, 타 산업과 연계를 통한 신규 프로젝트 중점 발굴
- 국내-현지 기업간 비즈니스 파트너십 구축 방식의 다변화 도모

가. 중국

'17년 GDP(십억달러)	13,608
'17년 인구수(천명)	1,393,000

■ ITU 글로벌 사이버보안 지수(Global Cybersecurity Index, GCI)

· 중국의 사이버보안 지수는 5계단 상승한 27위로 우리나라와의 간격이 줄어들고 있음

국가명	2018		2017		전년대비 증감	
	지수	순위	지수	순위	지수	순위
중국	0.828	27	0.624	32	+0.204	+5
대한민국	0.873	15	0.782	13	+0.091	-2

■ ICT 관련 주요 지수

· 중국의 전반적인 ICT 발전 수준은 ITU 조사국 167개국 중 중상위권 수준으로 성장

지표명	중국		한국	
	점수	순위	점수	순위
IMD 국가경쟁력지수(2019)	-	14	-	28
IMD 디지털경쟁력지수(2019)	-	22	-	10
UNCTAD 전자상거래지수(2019)	68.8	62	89.4	19
ITU 글로벌 사이버보안 지수(GCI 2018)	0.828	27	0.873	15
UN 전자정부 지수(2018)	0.681	65	0.901	3

■ ICT 관련 주요 통계(ITU, 2018년 말 기준)

· 중국은 각종 통신 서비스 보급률은 대체적으로 중하위권이나 이동통신 이용자 수는 세계 최고 수준

항목	중국		한국	
	가입자수(천 명)	보급률(%)	가입자수(천 명)	보급률(%)
유선전화	182,248	12.77	26,842	52.6
유선브로드밴드	407,382	28.54	21,195	41.5
이동통신	1,641,147	114.95	63,658	124.8
인터넷 이용률	54.30%(2017년 말 기준)		95.1%	

정보보호 산업 개요

1) 정보보호 산업 환경

정보보안 환경

▶ 최근 중국에서는 클라우드 컴퓨팅, 모바일 인터넷, 빅데이터 등의 신기술 발전으로 인터넷 의존도가 갈수록 높아지는 상황에서 각종 해킹, 보이스피싱 등 크고 작은 정보유출 사건이 빈번하게 일어나면서 정보보호가 전사회적 문제로 대두

- 중국 인터넷업체 텐센트에 따르면 2018년 중국 기업 10곳 중 2곳은 매주 컴퓨터 바이러스 감염 피해를 입은 것으로 나타났으며 특히 랜섬웨어와 채굴 바이러스에 의한 피해가 많았음
- 2018년 스마트폰을 겨냥한 바이러스 수의 증가세는 완화되었으나 여전히 심각한 상황으로, 텐센트의 모바일 보안랩에 따르면 지난해 800만 개에 달하는 모바일 바이러스가 탐지됨

▶ 중국 정부는 2013년 시진핑 주석 취임 이래 본격적으로 정보보호 관련 정책을 추진하면서 정보보호 산업 발전과 위협 대응에 나서고 있음

- 중국은 2013년 11월 국가안전위원회 신설에 이어 2014년 2월에는 시진핑 주석이 직접 수장을 맡는 중앙인터넷안전·정보화영도소조를 설립하는 등 정보보안을 국가전략의 우선순위로 삼고 있음
- 중국 정부는 2015년 새로운 국가안전법을 채택한 데 이어 2017년 6월부터 사이버공간 주권과 국가안보, 사회 공공이익을 지키기 위한 '네트워크안전법(통칭 사이버보안법)'을 시행하며 정보보호 강화를 위한 통제 방침을 강화하는 추세
- 네트워크안전법은 개인정보 및 데이터 처리 기준을 강화하여 외국 기업이 주요 정보 기간시설 운영자인 경우 개인정보와 중요 데이터의 중국 내 저장을 의무화하고 해외 전송 시 검사와 평가를 의무화하며 네트워크 운영자에 대해 수집한 이용자 정보 비밀유지를 철저히 하고 건전한 이용자 정보보호 제도를 수립할 것을 요구

▶ 한편, 2020년 이후 5G 서비스가 상용화로 사물인터넷 시대가 본격적으로 열리면서 보안의 중요성이 높아짐에 따라 정보보호 시장의 성장세가 더욱 높아질 전망

- 중국 공업정보화부는 올해 6월 4대 이동통신사에 5G 영업허가증을 발급했으며, 주요 통신사들은 연내 40개 도시에서 상용화 서비스를 개시할 계획

• 5G 보안의 핵심으로 꼽히는 양자암호통신에서 중국은 베이징과 상하이 사이의 1,200km 거리 구간에 양자암호 국가 시범망을 구축하는 등, 상대적으로 진보된 기술을 보유

표_중국 3대 이동통신사의 5G 상용화 추진 현황

이동통신사	주요 내용
China Mobile	• '19년 상용화, '20년 기지국 10,000개 이상 설치 목표 • 1개 도시당 100개 기지국 설립 예정 • 20개 단말기 기업과 파트너 관계 구축
China Unicom	• '19년 상용화 목표로 '5G 선도자 계획' 발표 • 5G 기반 시범사업 200개, 5G 오픈랩 50개, 5G 혁신 응용서비스 100개 추진 • 5G 활용 기준 20개, 협력 파트너 1,000개 추가로 확보
China Telecom	• 상용화 테스트 진행 중

[출처] 각종 언론 매체 종합

물리보안 환경

▶ 물리보안 부문에서는 중국 정부가 '안전도시(平安城市)', '스마트도시(智能城市)' 건설을 추진하면서, 보안시스템이 중요한 도시 인프라 중 하나로 각광받아 탄탄한 시장 수요를 형성

• 정부 정책의 시행은 보안 산업의 2~3선 도시로의 하향 발전을 촉진하고 보안기술의 혁신과 신제품 개발의 기폭제로 작용

• IDC에 따르면 중국의 스마트도시 프로젝트로 2020년까지 27억 6,000만 대의 CCTV가 설치될 예정으로, 첨단 기술을 활용한 영상 감시시스템 구축으로 CCTV를 통해 찍힌 사람들의 신원을 인공지능을 통해 식별 가능한 것으로 알려짐

▶ 물리보안 시장은 2018년 이후 인공지능과의 결합이 본격화되어 다수의 보안 업체들이 AI를 적용한 신제품을 출시하고 있으며, 인공지능과 기타 신기술의 도입으로 전통적인 보안업체뿐 아니라 인터넷 대기업 등 타 영역의 기업들이 보안 시장에 진출하면서 시장 경쟁이 격화됨

• 최근까지 지능형 보안 산업은 안면인식을 위주로 이루어져 왔으나 인공지능의 지속적인 발전으로 장치 응용 영역도 다양해질 전망

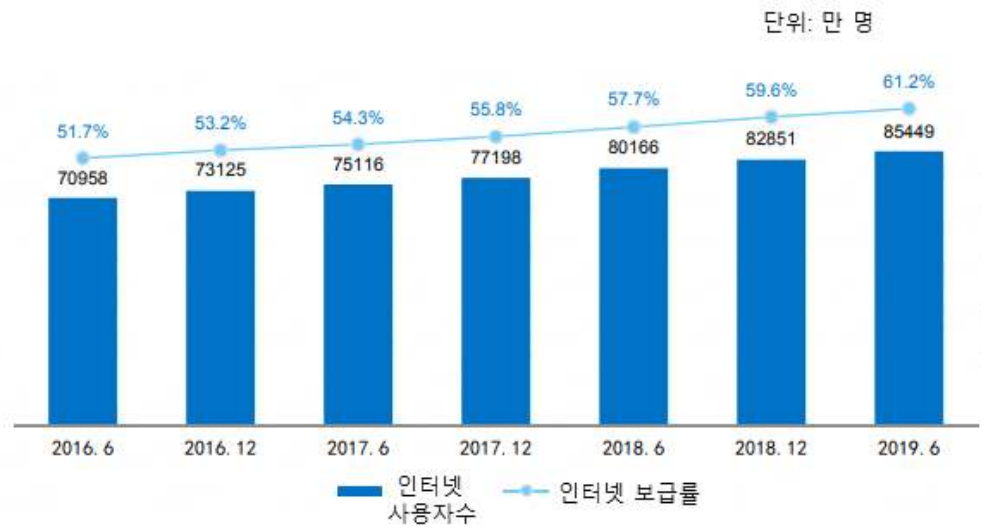
2) 인터넷 및 통신 환경

중국 인터넷 및 통신 시장 개요

▶ 2019년 8월 중국 인터넷네트워크정보센터(CNNIC, China Internet Network Information Center)가 발표한 제 44차 <중국인터넷발전현황통계보고>에 따르면 2019년 6월 30일 기준 중국의 인터넷 사용자는 8억 5,400만 명, 인터넷 보급률은 61.2%를 기록

- 휴대폰을 이용해 인터넷에 접속하는 사용자는 8억 4,700만 명으로 2017년 말보다 2,984만 명 증가했으며, 이는 전체 인터넷 사용자의 99.1%에 해당하는 수치임
- 연령별로는 10-39세가 전체 인터넷 이용자의 65.1%를 차지하는 주력층으로 나타났으며, 이중 20-29세가 24.6%로 가장 많은 비중 차지

그림 _ 중국 인터넷 사용자 규모 및 보급률(2013.6~2018.06)



[출처] CNNIC, '중국인터넷발전현황통계보고'(2019.8)

▶ 시장조사기관 BuddeCom에 따르면 2018년 기준 중국의 이동통신 가입자 수는 14억 9,600만 명으로 보급률은 106%에 달함

- China Telecom과 China Mobile은 2018년 한 해 동안 가입자 수가 각각 10% 증가하며 강한 성장세를 기록했으나, 시장 포화로 2023년까지 5년 간 성장 속도가 둔화될 전망
- 중국의 이동통신 보급률은 2020년 113%에서 2023년 121%를 달성할 전망으로, 2018년부터 2023년까지 연간 3.2%의 성장률을 기록할 것으로 예상됨
- 모바일 브로드밴드 보급률은 LTE의 보급과 스마트폰의 가격 인하에 힘입어 2013년 21%에서 2018년

92%로 급격히 상승

- 2020년 이후 5G가 본격적으로 보급되면서 2025년까지 중국은 전 세계 5G 연결건수의 3분의 2 이상을 차지하는 세계 최대의 5G 시장이 될 전망

인터넷 활용 현황

▶ CNNIC에 따르면 2019년 6월 기준 중국 인터넷 사용자들의 인터넷 프로그램 사용률에서 인스턴트 메신저가 96.5%로 가장 높은 비중을 차지했으며, 인터넷 동영상(88.8%)과 검색엔진(81.3%)이 그 뒤를 이었음

- 성장률 면에서는 온라인 교육 프로그램의 사용자가 6개월 전과 비교해 15.5% 증가해 가장 높은 성장률을 보였으며, 그 다음으로는 온라인 재테크 사용자가 12.1% 증가했음
- 모바일 애플리케이션(앱) 사용률에서는 인스턴트 메신저(96.9%)가 1위를 차지했으며, 검색엔진(78.2%)과 신문(78.0%), 쇼핑(73.4%)과 결제(73.4%)가 그 뒤를 이었음
- 인스턴트 메시지는 최근 기본적인 메시지 전달 기능 외에도 이용자의 생활서비스를 접목한 종합 플랫폼을 개발·구축하려는 시도를 하고 있음
- 검색과 인터넷 신문 역시 기본 기능 외에 사용자 개인 요구에 맞는 정보를 추천하거나 제공하는 플랫폼을 강화하는 추세

▶ 모바일 기기를 활용한 비즈니스 거래와 금융 서비스 등도 크게 확대되면서, 관련 앱과 이용자 규모가 크게 증가하고 있음

- 2019년 6월 기준 온라인 재테크 서비스 이용자 수는 1억 7,000만 명으로 전체 인터넷 사용자의 19.9%에 달함
- 온라인 지급결제 이용자 수는 6억 3,300만 명, 모바일 지급결제 이용자 수는 6억 2,100만 명으로 나타남

정보보호 시장 현황

1) 시장 규모

시장 개요

▶ 중국의 정보보호 산업은 고속 성장세를 유지하고 있으며, 특히 정보보안 산업의 경우 최근 3년간 20% 이상의 성장률을 기록

- 중국은 세계에서 온라인 보안 지출이 두 번째로 큰 국가로 성장했으며 빠른 성장세를 보이고 있음
- 그러나 아직까지 중국 정보보안 산업은 전반적인 IT 산업의 발전 수준에 비해 상당 부분 뒤처진 상태로, 전체 IT 투자액 대비 보안 지출 비율도 전 세계 평균 수준에 대비해 여전히 차이를 보임
- 시장 공급도 다수의 중소기업으로 이루어져 있어, 한동안 정부 정책 주도형의 발전 양상을 보일 전망

▶ 시장 수요 측면에서는 정부, 통신, 에너지, 군(軍) 등이 여전히 주축을 이루는 가운데 증권, 교통, 교육, 제조 등 신흥 시장이 새로운 동력으로 부상

- 특히 정보보호에 대한 정부의 높은 관심은 산업 발전의 강력한 동력으로 작용하고 있으며 중국 정부가 자체 정보보호 산업 육성을 위해 중국에서 개발된 제품을 집중 구매함으로써 중국 정보보호 업체들에게 안정적인 생존 및 발전환경을 제공
- 한편 인터넷 이용이 보편화되면서 기업 이메일과 기업 핵심정보 등 민감한 데이터를 보호하기 위한 기업들의 정보보호 제품 및 서비스 채택이 증가하면서 클라우드 기반 보안 솔루션에 대한 수요가 시장발전을 견인하고 있음
- 여러 정보보호 업체들은 클라우드 외에 빅데이터, 사물인터넷, 모바일 인터넷, 인공지능 등 신흥 기술을 활용해 제품과 서비스를 완비해가고 있으며, 전통적인 보안에서 차세대 보안으로 변모 중

▶ 물리보안 시장에서는 전통적으로 높은 수요를 보인 공공안전, 금융 분야 외에도 사람들의 안전 의식이 강화되면서 일반 가정용 보안 시장이 확대 추세

- 물리보안 제품군의 절반을 차지하는 영상감시 제품의 경우, 네트워크화 지능화, 고화질화의 방향으로 발전하고 있으며, '안전도시(平安城市)', '스마트도시(智能城市)' 건설 정책에 대한 중국 정부의 강력한 추진과 도시화의 가속화는 보안 산업에 대한 시장 수요를 뒷받침
- 또한, 중국 스마트홈 시장이 성장세를 보이면서 Hikvision, Dahua 등 전통적인 보안 기업뿐 아니라 Alibaba, Xiaomi, 360 등 인터넷 기업들도 스마트홈 보안 시장에 진출하는 추세

시장 규모 및 전망

❑ 정보보안 시장

▶ 중국정보통신연구원(CAICT)의 '2019년 중국 사이버보안 백서'에 따르면 중국 사이버보안 산업규모는 2018년 510억 9,200만 위안으로 전년 대비 19.2% 성장했으며, '19년에는 631억 2,900만 위안 규모를 형성할 전망

▶ IDC에 따르면 금년부터 2022년까지 중국 IT 보안 지출규모의 연평균 증가율은 25.6%에 달해 전 세계 평균을 크게 웃돌 전망

- 2019년 중국의 IT 보안 지출액은 약 73억 5,000만 달러로 예상되며, 2022년에는 중국 보안 솔루션 시장이 137억 7,000만 달러로 성장할 것으로 예상됨
- IT 보안 지출액 중 하드웨어가 차지하는 비중이 약 61.9%이며, 보안 관련 소프트웨어가 16.4%, 보안 서비스가 21.7%의 비중을 차지할 전망
- 업종별로는 정부와 통신, 금융이 중국 사이버 보안 시장에서 가장 지출액이 많은 3대 분야로 전체 IT 보안 시장의 60%를 차지할 전망

그림 _ 2017~2022년 중국 IT 보안 지출규모 예측



[출처] IDC 중국, 보안뉴스 재인용[58]

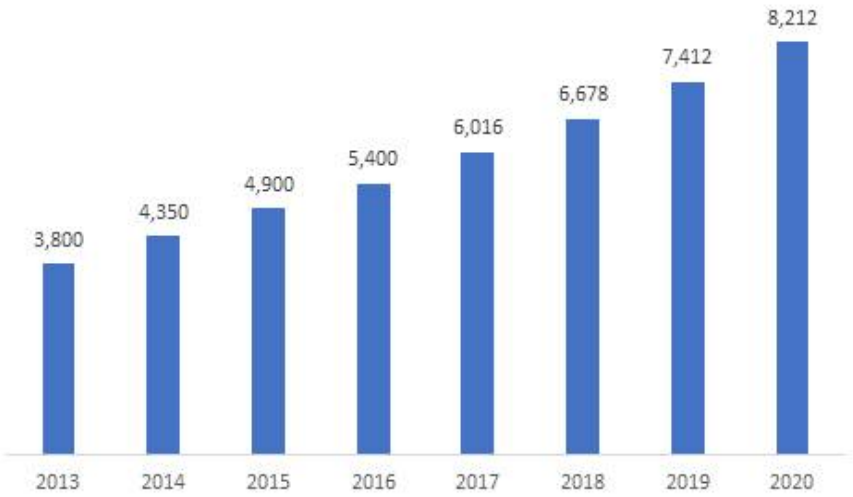
58 https://www.boannews.com/media/view.asp?idx=78784&kind=4

❑ 물리보안 시장

▶ 중국안전방범제품산업협회에 따르면 2019년 중국의 물리보안 산업 매출규모는 7,412억 위안에 달할 전망

- 향후 수년 간 국내외적으로 보안기술 제품에 대한 수요가 유지되는 한편, 시스템 교체 및 업그레이드 수요가 발생하면서 중국 보안 산업은 양호한 성장세를 유지할 것으로 예상됨
- 2020년까지 중국 물리보안 산업은 10-12% 사이의 성장률을 유지해, 2020년 시장 규모가 8,000억 위안을 돌파할 전망

그림 _ 2013~2020년 중국 보안 산업 규모(단위: 억 위안)



[출처] 중국안전방법제품산업협회, 중상산업연구원(2019.04)

2) 분야별 현황

정보보안 제품 및 서비스

▶ IDC China에 따르면 2018년 중국의 IT 보안 소프트웨어 시장 사업자들의 매출 규모가 9억 4,900만 달러로 전년 동기 대비 23.98% 성장

- IDC는 2023년까지 중국 IT 보안 소프트웨어 시장 사업자들의 매출 규모가 22억 9,000만 달러로 성장할 것이며, 향후 5년간 연평균 19.3%의 성장률을 기록할 것으로 예상
- 중국 정부의 정책적 지원과 디지털 경제의 성장, 기업 소비자들의 보안 의식 제고 및 기타 동인에

힘입어 중국이 IT 보안 시장은 빠른 성장을 유지하고 있으며, 클라우드 컴퓨팅의 급속한 발전과 함께 IT 보안 소프트웨어의 시장 응용도 광범해지고 있음

- 단말 보안 소프트웨어와 신원 및 디지털 신뢰 소프트웨어, AIRO(Analytics, Incident, Response, and Orchestration) 소프트웨어 시장이 전체 IT 보안 소프트웨어 시장을 주도

그림 _ 2018-2023년 중국 IT 보안 소프트웨어 사업자 매출규모 예측



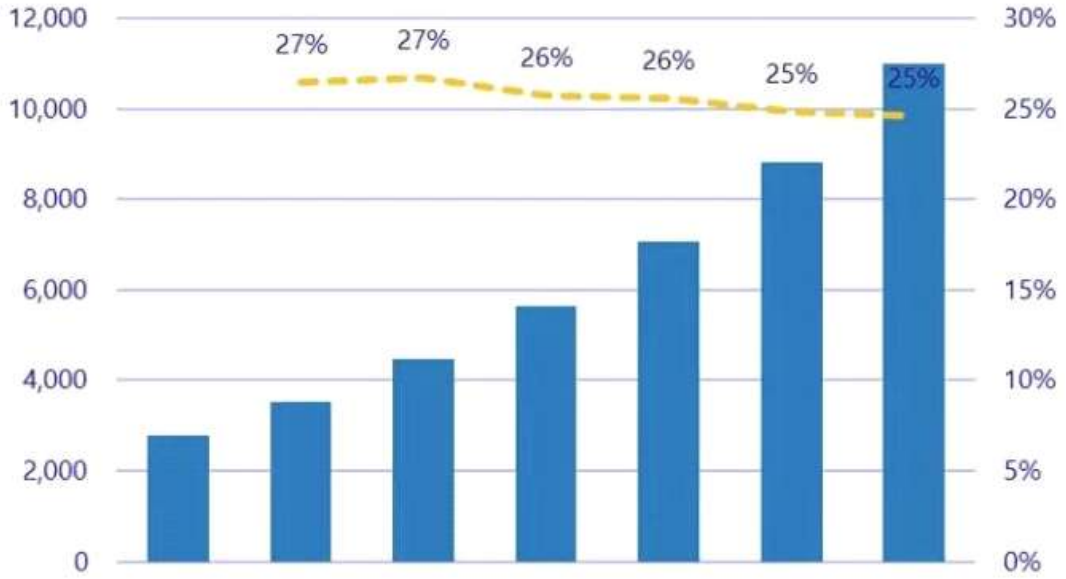
[출처] IDC China(2019.05)[59]

▶ 한편, 2018년 중국의 IT 보안 하드웨어 시장규모는 35억 3,000만 달러로 전년 대비 26.5% 성장했으며, 2023년에는 109억 9,000만 달러로 성장할 전망으로, 향후 5년간 연평균 성장률은 25.5%로 예상

- SCM(Secure Content Management), 방화벽, 침입 탐지 및 방어(IDP), 통합위협관리(UTM), 가상사설망(VPN) 등이 IT 보안 하드웨어 시장을 주도하고 있음

59 https://www.idc.com/getdoc.jsp?containerId=prCHC45106219

그림 _ 2018-2023년 중국 IT 보안 하드웨어 시장규모 예측



[출처] IDC China(2019.04)[60]

물리보안 제품 및 서비스

▶ CPS(中安网)에 따르면 2018년 기준 중국 보안 시장규모는 약 7,180억 위안으로, 중국 GDP의 0.8% 가량을 차지함

- 이중 영상감시시스템 시장 규모가 1,229억 위안, 출입통제 시스템이 341억 위안, 방범경보 시스템이 137억 위안 규모를 형성

▶ 최근 중국의 물리보안 제품 시장은 사물인터넷의 발달과 CCTV의 지능화에 따라 단순히 영상을 전달하는 역할을 넘어서 영상에 찍힌 사람이나 사물의 정체를 식별하고 행동의 특징을 분석하는 단계로 발전

- 영상감시 설비와 AI, 빅데이터 기술의 결합이 이루어지면서 물리보안 시장에 진입하는 인터넷 기업도 늘고 있으며, 정보보안과 물리보안의 경계도 흐려지고 있음

▶ 이와 함께 기술 업그레이드와 사용 범위의 확대는 물리보안 산업의 성장을 촉진하는 중요 요인으로, 영상감시 제품의 경우 IP화, 디지털화, 고해상도화 등 끊임없는 기술 업그레이드가 이루어짐

60 https://www.idc.com/getdoc.jsp?containerId=prCHC44980119

- 감시 카메라의 경우 고해상도 추세에 따라 720p, 1080p는 이미 주류가 되었으며, 2K, 4K까지 발전 중이며, 인터넷 발전으로 현재 지하철 감시 시스템, 안전도시 등 정부가 주도하는 대형 프로젝트는 모두 IP 네트워킹을 기본으로 하는 감시 시스템을 갖추고 있음
- 또한 과거에는 물리보안 제품이 군대, 정부, 교도소, 박물관 등 특수 분야에만 사용되었던 반면 최근에는 공장, 상점, 학교, 병원 등 대부분의 공공분야에 진출해 있으며, 방범 수요뿐만 아니라 사회 관리와 도시 관리로 수요가 확대되는 추세이며, 일반 가정에서도 물리보안 제품을 채택하는 사례 증가
- 정부 계획에서도 초기에는 범죄사건 해결률을 높이기 위한 목적에서 영상 감시 시스템을 구축하기 시작해, '안전도시'를 통해 도시 치안으로 사용범위가 확대된 이후, 현재는 '스마트도시' 계획으로 도시 치안뿐 아니라 교통 혼잡, 환경오염 등 각종 사회문제에 대한 종합적인 해결을 도모

3. 주요 사업자 현황

시장 특성 및 경쟁 강도

❑ 정보보안

▶ 중상산업연구원(中商产业研究院)에 따르면 중국의 정보보안 제품 시장은 제품군 별로 세분화되어 있어 서로 다른 업체들이 각 부문 별로 우위를 차지하면서 전체 시장의 브랜드 집중도는 낮은 편

- 중국의 정보보안 제품 시장은 장기적으로 통합 추세를 따르겠지만 확고한 시장 주도업체가 등장하거나 독점 체제가 이루어지기는 어려울 것으로 전망
- 정보보안 서비스의 경우, 서비스에 대한 사용자 인식 부족으로 인해 선진국 대비 보안 서비스에 대한 투자나 시장 규모가 미약한 편으로, 중국의 정보보안업체들은 주로 보안설계, 보안평가, 보안 운영관리, 보안기술 연구개발 등의 서비스를 제공
- 보안 SI 시장에서는 다수의 업체들이 치열한 경쟁 국면을 형성하고 있으며, 지역적으로나 산업적으로 파편화된 구조로 시장 집중도는 낮지만, 점차 핵심 기술력과 브랜드 인지도를 보유한 대형 기업들을 중심으로 재편될 전망

▶ 중국정보통신연구원에 따르면 2018년 기준 중국에서 사이버보안 분야에서 활동하는 업체 수는 총 2,8,98개로, 1년 간 새로 늘어난 기업이 217개로 양호한 발전 태세를 유지하고 있음

- 지역별로는 베이징의 기업이 975개, 광둥 기업이 975개, 상하이 기업이 288개 기업으로 1~3위를

차지함

- 2018년 상위 10대 상장업체들의 평균 매출규모는 15억 6,900만 위안으로 전년 대비 10.7% 증가함
- 상위 10대 상장 보안업체들은 2018년 평균 연구개발에 2억 6,700만 위안을 투자했으며, 이는 전년 대비 25.2% 증가한 수치

❑ 물리보안

▶ 중상산업연구원에 따르면 2018년 기준 중국 물리보안 기업 수는 약 22,000개로 이중 보안 제품 제조 기업이 4,900개로, 전체 기업의 23% 가량을 차지함

- 중국 영상감시설비 시장은 Hikvision, Dahua를 비롯한 상위 5개 업체의 시장 점유율이 50% 이상으로 시장 집중도가 매우 높은 편이나, 최근 샤오미, 360, 바이두 등 IT와 인터넷 기업들이 보안업체와 제휴해 인터넷 플랫폼을 통해 시장 진입이 활발해지면서 시장 경쟁이 격화

▶ 지능형 보안시스템 시장은 출입제어, 경보, 모니터링의 3개 부분으로 구성되며, 출입통제 영역에서는 전국에 약 500여개의 장비 제조업체가 있으며 주로 베이징, 광둥, 상하이에 집중됨

- 상위 10개 제조업체의 시장 점유율은 약 20%로 외국 기업으로는 Bosh, Honeywell, HID 등이 활동하고 있으나 가격 경쟁력 부족으로 시장 점유율은 낮은 편
- 중국 기업들은 시스템 관리 소프트웨어 개발 측면에서 일정한 우세를 보유하고 있으나, 출입통제 시스템의 핵심 기술 및 칩셋은 여전히 해외에 대한 의존도가 높음
- 도난방지 경보시스템의 경우 전국적으로 약 450개의 제조업체가 있으며, 상위 10개 업체의 시장 점유율이 30%로 Honeywell, 일본의 ALEPH, 이스라엘 EL 등의 외국 브랜드가 강세를 보임

▶ 한편, 중국 천풍증권(TF Securities)에 따르면 최근 Hikvision, Dahua 등 대형 기업들은 제품 공급업체에서 솔루션 공급업체로 사업구조를 전환하면서 시너지 효과 창출 및 더 높은 부가가치 창출을 이끌고 있음

- 일례로 스마트빌딩 솔루션에서 영상감시 장치의 비중은 15~20%에 불과하나, 솔루션 전체를 공급할 경우 도어록 제어, 출입 제어, 경보시스템, 소방시스템, 소프트웨어 플랫폼까지 포함해 한 프로젝트를 통한 매출이 4~5배까지 확대 가능

주요 사업자

❑ 정보보안

▶ NSFocus(綠盟科技)

- 기업용 인터넷 보안시스템 주요 개발업체로서 정부기관, 통신사, 금융, 에너지, 인터넷 등 분야의 기업고객을 대상으로 디도스 방지, 방화벽, 침입방지, 웹 보안, 위협분석, 데이터 유출 방지, 취약점 스캐닝, 보안 컨설팅 및 훈련 서비스 등을 제공
- NSFocus는 2014년 Kingsoft Security, Deepin 등 중국 정보보안 업체에 대한 인수합병을 통해 기업 규모를 확대했으며, 국가 정보보안표준화 작업의 회원사로서 다수의 국가급, 산업급, 기업급 표준화 작업에 참여
- NSFocus는 2019년 3월 글로벌 디도스 위협에 대한 실시간 인사이트와 상황인지를 제공하는 'Attack Threat Monitoring' 솔루션을 출시한 데 이어 5월에는 7Tbps 클라우드 디도스 방어 솔루션을 출시하는 등, 디도스 방지 솔루션을 잇달아 선보임

▶ Venustech(启明星辰)

- 중국 내 인터넷 보안업계의 대표기업으로 주력제품은 방화벽/UTM, 침입 탐지 시스템(IDS), 네트워크 보안, 비밀번호 인증 시스템 등이며 특히 방화벽/UTM, 침입 탐지 및 방어(IDS/IPS) 시스템, 안전 관리 플랫폼(SOC) 모두 시장점유율 1위
- 정부기관, 통신, 금융, 에너지, 교통, 군수, 제조업 등 분야의 기업고객이 선호하는 최우선 브랜드며 특히, 정부기관 및 군 시장 점유율이 80%에 달함
- 세계 500대 기업에 편입된 중국 기업 중 약 60%의 기업 고객에게 보안 시스템 및 서비스를 제공하며 동시에 정책성 은행, 국유은행, 대형 주식제 상업은행 시장의 보급률은 90%이며, China Mobile, China Telecom, China Unicom 등 3대 통신사에도 보안 서비스 제공

▶ Westone(衛士通)

- 2008년 중국 정보보안 업체 최초로 선전 주식시장에 상장된 바 있으며, 주력사업은 정보보안 하드웨어 제품 및 보안 시스템 개발생산, 주력제품은 암호장치, 암호 시스템, 보안 인증시스템, 방화벽 및 방화체계, 서버 및 데이터 보안시스템 등
- 2014년에 자산 구조조정을 통해 삼령성안, 삼령서통, 삼령가미 등 3개의 정보보안 전문기업을 인수하면서 칩에서 모듈까지, 단순 기기에서 시스템 개발까지 정보보안 분야에서 수직 계열화된 사업구조를 구축해 시장 경쟁력을 강화

▶ TopSec(天融信)

- 1995년 설립된 TopSec은 1996년 중국 최초로 자체 지적재산권을 보유한 방화벽 제품을 출시함
- 금융, 통신, 전력, 교육, 헬스케어, 에너지, 제조 분야의 기업들과 정부를 대상으로 VPN, 암호화 제품 및 보안관리 솔루션 등을 판매하고 있음
- TopSec은 자체 개발 및 혁신을 고수하며 해외 보안업체들의 기술력에 근접 내지는 추월했다는 평가를

받을 만큼 무서운 성장세를 보이면서 중국의 대표적인 보안 기업으로 성장

▶ Sangfor

- 2000년 설립된 Sangfor는 네트워크 보안과 관리, 최적화 솔루션에 특화된 보안업체로 3,000명 이상의 직원을 보유하고 있으며 미국 실리콘밸리와 중국 베이징, 선전, 후난에 R&D 센터를 보유
- Sangfor의 주요 제품과 서비스로는 차세대 방화벽, 위험평가, 보안 스캐닝, 침투테스트, 응급대응과 통합 보안시스템, 클라우드 컴퓨팅 솔루션 등이 있음
- 정부기관과 금융기관, 인터넷 서비스 사업자, 교육기관 등을 주요 고객으로 두고 있으며, 27개 중국 정부부처 중 24개 부처가 Sangfor 제품을 사용 중

❑ 물리보안

▶ Hikvision(海康威视)

- 중국 내 대표적인 영상보안장비 제조업체로서, IHS Markit의 '2018년 글로벌 영상감시정보서비스 보고서'에 따르면 Hikvision은 글로벌 영상감시 설비 시장에서 37.9%의 점유율로 1위를 차지
- Hikvision은 2018년 기준 CCTV 및 영상감시장비 부문에서 7년 연속 세계 최대 기업으로 입지를 강화해 나가고 있으며, 네트워크 카메라, 아날로그와 HD CCTV 카메라, DVR/NVR 및 영상 인코더를 포함해 거의 모든 개별 장비 부문에서도 글로벌 시장 1위 점유
- 백엔드(Back-end) 제품에서 프론트엔드(Front-end)로의 확장을 통해 종합 솔루션(Solution) 제공업체로 거듭났으며, 현재 HW와 SW를 결합한 솔루션 관련 사업의 매출비중은 50% 이상
- Hikvision의 해외사업은 미국과 유럽시장에서 빠른 성장세를 보이고 있으며, 2016년에만 카자흐스탄, 콜롬비아, 터키, 두바이에 지사를 추가 설립하며 해외지사를 25개로 확장
- 최근에는 가정 및 소형 매장을 대상으로 감시카메라 장비 판매 및 유지보수, 클라우드 서비스까지 하고 있으며 산업용 입체카메라와 CCD(Charge-coupled Device)를 개발해 머신비전(Machine Vision) 시장에도 진출
- 2017년 11월에는 딥러닝 기술을 내장한 듀얼렌즈 안면인식 DeepinView 카메라를 출시했으며, 특정 사람들의 신원과 이들의 얼굴 표정, 동작 등을 확인할 수 있는 기능을 탑재한 동 제품은 카지노, 금융기관, 혼잡한 공공장소 등에서 사용될 전망

▶ Dahua Technology(大华技术)

- 항주에서 2001년에 설립된 후 2008년 5월 상장했으며, IHS Markit에 따르면 2018년 기준 세계 영상감시시스템 시장에서 17%의 점유율을 기록하며 Hikvision에 이어 2위를 차지하고 있음
- 동영상 저장, 디스플레이 컨트롤, 스마트 교통시스템 등을 판매함. 보안, 금융, 교통, 에너지, 통신 등

핵심영역과 관련된 사업을 하며, 6자회담, 올림픽 운동장, 상해 엑스포, 영국 런던 지하철 등의 중대형 프로젝트에 참여

- 최근 2년 간 영업망을 대거 확충하면서 중국 내 성소재지 도시 중심으로 전국적인 체인을 갖췄고 아시아, 미주, 유럽, 중동, 아프리카 등 세계 전 지역에 35개 해외 지사를 보유
- 또한, HW에서 SW로 집중하면서 기술 강화를 위해 연구개발(R&D) 인력을 2011년의 700명에서 2017년 현재 6,000명으로 대폭 늘렸으며, 2014년부터 연간 매출의 10%를 R&D에 투자하고 있음
- 최근에는 영상보안 감시 장비 시장을 중심으로 머신 비전, 드론, 가상현실(VR), 증강현실(AR) 등의 신규 분야로 진출하고 있으며, 최근 중국 물리보안 업계에서 각광받고 있는 기업 및 일반용 보안 서비스로도 사업 확장 중

▶ Univew(宇视科技)

- 정보보안 업체 H3C의 스토리지 및 멀티미디어 사업부를 전신으로 2011년 설립된 Univew는 중국 IP 지능 형 감시카메라 및 네트워크 감시카메라 시장에 진출해 판매량 및 판매 성장률에서 중국내 선도적인 위치에 있으며, Hikvision, Dahua에 이어 중국 내 3위 영상감시 제품 사업자임
- 주요 제품으로는 IP 카메라, NVR, 인코더/디코더, IP SAN(Storage Area Network) 등이 있음
- Univew는 항저우와 선전에 R&D 시설을 설립하고, 매년 매출액의 15% 이상을 R&D에 투입하고 있으며, 2015년 기준 1,916명의 직원 중 절반이 R&D 인력임
- 2013년부터 해외 시장에 진출했으며, 2016년 5월에는 국내 보안기업 인콘과 제휴해 국내 시장도 공략

▶ Netposa(东方网力)

- 영상감시 플랫폼을 개발하는 솔루션 회사로서 10여 년간 도시 치안용 CCTV 플랫폼 건설에 주력해왔으며, 중국 내 영상감시 플랫폼 시장 점유율은 21%임
- 영상 클라우드 컴퓨팅이 핵심 기술이며 메모리장치, CCTV 카메라 등의 하드웨어를 통해 데이터 수집 회사와 최종 소비자에게 영상 서비스를 제공
- 회사의 제품은 영상수집, 네트워킹, 저장, 분석, 빅데이터 응용 등이 가능하며 도시 치안, 교통, 교육, 전력, 건물 관리, 기업고객용 및 개인 가정용 등으로 사용됨
- 주력 제품은 영상감시 관리 플랫폼 소프트웨어로서, Hikvision이나 Dahua와 달리 모든 방범(보안)용 장치를 제조하지 않고 영상감시 플랫폼의 소프트웨어 관련 부분에만 주력하고 있어 제품 수익성이 좋음

4) 주요 동향 및 이슈

▶ ZTE, 브뤼셀에 사이버 보안 연구소 설립(2019.7)

- ZTE가 중국산 통신 장비를 둘러싼 우려를 완화하고 투명성을 제고하기 위해 벨기에의 브뤼셀에 사이버보안 연구소를 개설
- ZTE에 따르면 연구소의 주요 목적은 규제당국과 잠재 고객이 5G 장비를 비롯한 ZTE 제품의 소스코드와 문서를 검토하고, 블랙박스 시험*과 침투 시험을 실시하도록 하는 것임
- 연구소는 ZTE의 5G 장비의 보안에 대한 심도 있는 연구도 실시하게 되며, 주요 보안 기관들과 협력해 연구를 진행할 계획
- ZTE는 2019년 5월 중국 난징과 이탈리아 로마에 사이버보안 연구소를 개설한 바 있음

▶ Huawei, 향후 5년간 사이버보안에 20억 달러 투자 계획(2018.12)

- Huawei가 향후 5년간 사이버보안 인력과 연구소 시설 업그레이드 등을 통해 사이버보안에 20억 달러를 투자하겠다는 계획을 발표
- 이는 전 세계적으로 제기되고 있는 Huawei에 대한 보안 우려에 대처하기 위한 조치로서, Huawei는 현재 미국과 호주, 뉴질랜드 등의 국가에서 5G 인프라 구축에서 제외됨
- Huawei는 기업과 정부의 특정 요구에 대응한 1회성 변경이 아닌, 소프트웨어 설계방식의 근본적 변화 및 연구개발 엔지니어의 훈련과 역량 강화에 20억 달러를 투자할 방침
- Huawei는 이를 통해 향후 3-5년간 정부와 기업 고객 양쪽에서 신뢰받는 제품 구축이 가능해질 것으로 기대

5) 정보보호 스타트업 시장 현황

시장 현황

▶ 중국정보통신연구원에 따르면 2019년 7월 중국 정부가 상하이 증시에 기술주 전용 상장시장 커촹반(科创板 : Technology Board)을 개장하면서, 정보보호 스타트업들의 상장이 활성화될 전망

- 현재 커촹반에 상장하거나 상장을 계획 중인 정보보안 스타트업은 총 6개로, 이들은 대부분 클라우드 보안과 IoT 보안, 빅데이터 보안 등 융합보안 사업 영역에서 활동 중
- 일례로 2011년 설립된 베이징 ABT Networks(安博通)은 IPv6 보안과 IoT 보안, 클라우드 보안, 보안 가시화 전문 기업으로 정보보호 기업 중 최초로 커촹반에 상장해 2억 9,800만 위안을 조달

▶ 물리보안 영역에서는 인공지능과 보안을 결합한 제품과 서비스를 개발하는 스타트업들이 다수 활동하고 있음

- Dahua를 비롯한 전통 보안기업이 보안 카메라와 도어록 등의 제품에 안면인식과 데이터 구조화, 딥러닝 기술을 접목하고 있다면, Sensetime과 Huohe Tech로 대표되는 스타트업은 안면인식과 행동분석 등 이미지 분석, 지문인식 보안 서비스 고도화에 주력 중

주요 사업자

▶ Baishan Cloud

- 2015년 4월 구이저우에서 설립된 Baishan Cloud는 클라우드 서비스 및 클라우드 보안 전문 기업으로 2017년 인공지능 기반 클라우드 보안 제품을 출시한 데 이어 2018년에는 데이터 애플리케이션 통합제품을 출시
- 2016년 미국에 지사를 설립하고 현지 시장 공략에 나섰으며, 현재 Microsoft, Xioami, Sina 등 400개 이상의 국내외 기업들에 서비스를 제공 중

▶ Pensees Technology

- 2017년 베이징에서 설립된 Pensees는 기업용 보안, 공공 보안, 스마트 커뮤니티, 스마트공장 등의 영역에서 다양한 AI 제품과 솔루션을 개발 및 구축하고 있으며, 주요 제품과 솔루션으로는 안면인식 시스템, 안면 빅데이터 분석 플랫폼 등이 있음
- Pensees는 2019년 7월 싱가포르에 AI 알고리즘 연구원, 시스템 연구원, 하드웨어 전문가와 엔지니어 등, 70명 규모의 연구소를 설립
- Pensees는 새로운 연구소를 통해 싱가포르 국립대학을 비롯한 현지 대학 및 전문가와 협력할 계획으로, 이미 싱가포르 국립대학과 AI 기반 카메라 시스템을 공동 개발하기 위한 협약을 체결

▶ SenseTime

- 2014년 설립되어 2018년 6억 달러 규모의 투자를 받으면서 2018년 말 기준 시가총액 45억 달러를 돌파한 센스타임은 AI 업계의 최대 유니콘 기업으로 성장한 스타트업으로 차이나 모바일과 화웨이, 정부기관 등 300여 개의 고객을 보유
- 2017년 AI 안면인식 시스템을 중국 광저우의 범죄자 추적업무에 도입하여 2,000여 명의 범죄자를 식별, 100여 건의 사건을 해결하고 800명을 입건하는 성과를 거두었음
- 현재는 얼굴과 이미지, 텍스트 인식과 의료 영상 및 비디오 분석, 자율주행 시스템으로 영역을 확장하여 보안분 아니라 금융, 의료, 자동차 등의 산업에 사용 가능한 AI 기술ㄹㄹ 개발 중

▶ Huohe Tech

- 2013년 베이징 중관춘에서 설립된 Huohe Tech는 2018년 2,000만 달러 규모의 시리즈 C 투자 유치에 성공한 스마트 도어록 전문 스타트업임
- Huohe Tech의 스마트 도어록 판매는 누적 100만 대를 넘어섰으며 2015년 이후 연 300%의 매출 증가율을 기록
- AI 지문 학습 알고리즘으로 0.3초 이내 360도 지문인식이 가능하도록 기능을 고도화하였으며, 스마트폰을 연동한 상시 출입기록 확인, 비밀번호 설정, 이상감지 자동 경보, 배터리 부족 알림 등의 기능을 탑재함

정보보호 정책 및 기관 현황

1) 주요 법령 및 정책

관련 법령 및 규제

표 _ 중국의 정보보호 관련 주요 법제도 현황

· 컴퓨터 정보시스템 안전보호조례(국무원-State Council, 1994.02)
· 컴퓨터정보망 국외 접속 안전보호 관리방법(국무원-State Council, 1997.12)
· 인터넷 안전 보호에 관한 결정(전국인민대표대회, 2000.12)
· 정보보안 업무 강화에 관한 의견(국가정보화지도소조, 2003.08)
· 해외 단체 및 개인의 재중국 암호제품사용 관리방법(국가암호관리국, 2007.03)
· 정보보안등급 보호관리방법(공안부/국가보밀국/국가암호관리국/국무원정보화판공실, 2007.06)
· 형법 개정안(전국인민대표대회, 2009.02)
· 통신네트워크 보안방법 관리방법(공업정보화부, 2010.01)
· 국가기밀유지법(전국인민대표대회, 2010.04) 개정안
· 신국가안전법(전국인민대표대회,2015.07)
· 사이버(네트워크·인터넷) 안전법(전국인민대표대회,2016.11)
· 핵심정보기반시설 안전보호조례 초안)국가인터넷정보판공실, 2017.07)
· 네트워크 안전등급 보호조례(공안부, 2018.06)

[출처] 각 부처 자료

▶ 신(新)국가안전법

- 중국 정부는 2015년 7월 1일 개최된 제12기 전국인민대표대회 상무위원회 제15차 회의에서 신국가안전법을 통과시킨 뒤 같은 날 공포, 시행함
- 신국가안전법 제1조는 "국가안전을 유지하고 인민민주독재 정권 및 중국 특색을 갖춘 사회주의 제도를 확립하며 인민의 근본적인 이익을 보호하고 중화민족의 부흥을 실현시키기 위해 동 법을 제정하였다"고 법률의 목적을 밝히고 있음
- 신국가안전법은 특히 사이버보안 강화에 중점을 두고 있으며, 국가가 네트워크와 정보 안전을 보장하는 체계를 구축하고, 네트워크와 정보안전 보호 능력을 향상시키며, 네트워크와 정보기술의 혁신 연구·개발 응용을 강화해야 한다고 명시

- 새 법은 또한 네트워크와 정보 핵심기술, 핵심 기초시설과 중요 영역 정보시스템 및 데이터의 안전에 대한 통제 가능성을 실현해야 한다고 강조
- 중국 정부는 신 국가안전법을 통해 인터넷 주권의 개념을 제시하고 사이버 공간에 대한 감독 강화를 명문화함으로써, 향후 중국 내 사이버보안과 관련해 국가와 개인 간 법익 충돌이 발생할 경우, 그 판단에 대한 법적 기준을 마련한 것으로 평가됨

▶ 네트워크안전법(일명: 사이버보안법)

- 중국 정부는 2016년 11월 전국인민대표대회에서 네트워크안전법(网络安全法)을 제정하여 2017년 6월 1일부터 시행
- (구성 및 내용) 네트워크안전법은 '사이버 공간 주권과 국가 안전 수호'를 입법 취지로, 모두 7장 68조항으로 이루어져 있으며, 네트워크 안전, 핵심 정보인프라 보호, 개인정보보호, 인터넷 모니터링, 법률 책임 등의 내용을 포함
- (집행 주체) 중국공산당 네트워크 안전 및 정보화 영도소조 판공실이 총괄 부처의 역할을 맡고, 공업정보화부와 공안부가 네트워크 보안, 사이버 불법콘텐츠 감독 업무를 집행
- 중국 정부는 향후 국가안전법과 네트워크 안전법을 토대로 네트워크 보안전략 기획, 집행, 감독, 위기상황 대응 등 종합적인 감독을 추진 계획

표 _ 중국 네트워크안전법 구성 체계 및 주요 내용

구분	주요 내용
제1장 총칙	· 목적, 적용대상, 국가의 역할, 국민의 책무 등
제2장 네트워크안전 지원 및 촉진	· 국가 네트워크 보안 전략 수립, 주무부처의 사이버 보안 계획 실행 · 표준 제정·시행, 기술 개발, 교육·훈련, 인재양성 등 촉진정책
제3장 네트워크 운영안전	· 네트워크 보안등급제도 실시 및 보안조치의무 · 네트워크 중요 설비 및 제품 인증·검사 및 제품목록 공개 · 인터넷 실명제 도입 및 국가의 전자신분 인증기술 연구개발 지원 · 핵심 정보인프라 지정·관리 및 보안조치의무 등
제4장 네트워크 정보안전	· 네트워크 운영자의 개인정보 보호조치 및 정보주체의 권리 · 불법정보 확산 방지를 위한 네트워크 운영자의 의무
제5장 네트워크안전 모니터링 경보 및 긴급대응	· 네트워크 보안정보 수집·분석·통보 관련 협조체계 구축 · 네트워크 보안 모니터링 경보 및 긴급 대응체계 구축
제6장 법률적 책임	· 금지행위 위반 시 처벌 규정 등
제7장 부칙	· 용어 해설 등

[출처] 공업정보화부

주요 전략 및 정책

▶ 국가 사이버보안 산업 발전 계획(国家网络安全产业发展规划)

- 2019년 6월 30일 개최된 '중국 소프트웨어 산업 발전현황'에 관한 기자간담회에서 '국가 사이버보안 산업 발전 계획'이 정식 발표되었으며, 중국 공업정보화부와 베이징 시정부가 국가 사이버보안 산업단지를 조성하기로 함
- 계획은 2020년까지 베이징 사이버보안 산업 규모 1,000억 위안(약 17조 원) 돌파, 사이버보안 산업의 국내총생산(GDP) 기여 규모 3,300억 위안(약 56조 원) 이상 달성, 연매출 100억 위안(약 1조 7,000억 원) 이상이 사이버보안 핵심기업 최소 3곳 육성 등의 목표를 설정
- 또한 2025년까지 국가사이버보안 전략 지원 기지, 국제적 수준의 사이버보안 연구개발 기지, 사이버보안 첨단산업 합동시범 기지, 사이버보안 인재육성 기지, 사이버보안 산업제도 혁신 기지 등 5개 기지를 건설한다는 계획

▶ 사이버공간 국제협력전략(网络空间国际合作战略)

- 중국 외교부와 국가인터넷정보판공실은 2017년 3월 1일 '사이버공간 국제협력 전략'을 공동 발표
- 앞서 시진핑 중국 국가주석은 2015년 12월 열린 제2회 세계인터넷대회 기조연설을 통해 사이버공간은 인류의 공동 활동영역이므로 세계 각국이 함께 관리해야 한다는 '사이버공간 운명공동체 수립'을 주창
- 사이버공간 국제협력 전략은 시진핑 주석이 주창한 사이버공간 운명공동체 건설을 목표로 국제 교류협력의 추진을 체계적으로 제안
- 중국 외교부는 이번 전략이 전 세계 사이버공간의 관리 문제를 해결하기 위한 중국의 방안을 제시하면서 사이버공간의 국제 교류와 협력을 이끌기 위한 전략성 문건이라고 설명
- 전략의 6대 목표는 ▲주권과 안전의 수호 ▲국제규칙체계의 수립 ▲인터넷 공평관리의 추진 ▲공민의 합법적 권익 수호 ▲디지털 경제협력 촉진 ▲인터넷 문화교류 플랫폼 구축 등임
- 또한 실행계획으로 사이버공간의 평화와 안정 촉진 ▲규칙 기반의 사이버공간 질서 형성 ▲사이버공간 협력관계 확대 ▲글로벌 인터넷 거버넌스 체계의 개혁 추진 ▲사이버 테러리즘과 범죄 단속을 위한 국제 협력 ▲프라이버시 등 공민의 권익 보호 ▲디지털 경제 발전 추진 ▲글로벌 정보인프라 건설과 보호 강화 ▲사이버 문화교류 제시

▶ 정보통신 네트워크 및 정보보안 규획 2016-2020(信息通信网络与信息安全规划)

- 2017년 1월 중국 공업정보화부는 '정보통신 네트워크 및 정보보안 규획 (2016-2020년)'을 발표
- 본 규획은 시진핑 주석의 사이버강국 전략 하에서 '혁신, 협력, 녹색, 개방, 공유'의 발전이념을 토대로

9개 방면의 중점 임무를 제시

- 주요 임무는 ▲네트워크 및 정보보안 법률법규 제도의 완비 ▲보안 관리감독 체계, 보안책임체계, 국내외 협력 체계 등을 포함해 새로운 네트워크 및 정보보안 관리체계 수립 ▲네트워크 및 정보보안 기술보장수준의 제고 ▲정보통신기반시설의 안전보장체계 수립 ▲네트워크(온라인) 데이터 및 이용자정보 보호 강화 등임
- 또한 인프라 자원 정보보안 관리에 더욱 힘쓰고 부가 통신서비스의 정보보안에 대한 감독 관리를 강화하며 새로운 인터넷 기술·업무에 대한 정보보안 평가를 심화할 계획
- 나아가 건전한 온라인 생태 환경을 적극 조성하는 동시에 온라인 보안 서비스 시장의 발전을 촉진한다는 방침

▶ 국가 사이버공간 안전전략(国家网络空间安全战略)

- 중국 국가인터넷정보판공실은 2016년 12월 27일 사이버 강국 실현과 사이버 공간 에서 국가 주권 및 이익 보호를 위한 '국가 사이버공간 안전전략'을 발표
- 인터넷정보판공실은 "정보기술의 광범위한 응용과 사이버 공간의 발전은 경제사회 번영과 진보를 크게 촉진하는 동시에 새로운 보안 위험과 도전도 초래"했다고 진단하고, 사이버 보안은 국가 안보와 관련되어 있다며 전략 마련의 배경을 밝힘
- '전략'은 국가 사이버 보안 업무의 주요 임무로 ▲사이버 공간 주권 수호 ▲국가 안보 수호 ▲핵심 정보인프라 보호 ▲사이버 문화 건설 강화 ▲사이버 테러와 불법 범죄 단속 ▲사이버 관리체계 완비 ▲사이버 보안 기초 마련 ▲사이버 공간 방호 능력 향상 ▲사이버 공간 국제협력 강화 등 9개 항을 명시

▶ 국가 정보화 발전전략 강요(家信息化發展戰略綱要)

- 2016년 7월 중국 국무원은 '국가 정보화 발전전략 강요'를 통해 오는 2050년까지 3단계의 인터넷 산업 발전 전략을 발표
- '강요'에는 향후 10년 동안 중국 정보화 발전을 지도하기 위한 내용이 담겨 있으며 인터넷 강국 건설이라는 최종 목표를 실현하는 과정에서 핵심 기술을 해외에 의존하는 국면을 탈피하고 기술 수준 향상, 산업 발전, 인터넷 보안이라는 중요한 목표를 실현함으로써 2050년대까지 인터넷 강국 실현, 세계 정보화 견인에 주도적인 역할을 해야 한다고 명시
- '강요'는 인터넷 보안을 '결코 간과해서는 안 되는' 전략적 목표로 강조함으로써 인터넷 보안에 대한 지원을 강화할 것이라는 정부의 의지를 표명
- 각종 테러 및 폭력 사건이 빈발하면서 이에 대한 사전 경보 및 예방의 중요성이 강조되는 가운데 업계의 전문가들은 인터넷 보안, 전용 통신 구축 등 부문을 발전 가능성이 있는 차세대 기술 부문으로 전망

2) 담당기관

표 _ 중국 정부부처별 정보보호 관련 수행 업무

정부 부처	수행업무	소관 부서/기관
중앙네트워크안전 정보화위원회	사이버보안 및 정보화 발전전략과 거시계획 및 법제의 연구제정	국가인터넷정보판공실
국가인터넷정보 판공실	인터넷 정보와 관련된 법령 제정과 인터넷 정보 내용에 대한 관리 강화 및 관련 기관에 대한 지도와 협조	
공업정보화부	통신과 인터넷 산업의 사이버보안 계획과 정책, 표준의 개발 및 시행, 통신과 인터넷 산업 사이버보안 심사 관련 업무, 신기술과 신사업의 안전평가 실시	- CN-CERT - 네트워크안전관리국
공안부	사이버 범죄의 조사 및 단속과 중국 내 인터넷에 국가안전과 사회질서 유지에 해로운 내용이 유포되는 것을 막기 위한 인터넷 검열 시스템 '만리방화벽' 운영	네트워크안전보위국

▶ 중앙네트워크안전정보화위원회

- 중국 공산당은 2014년 2월 당 중앙 직속으로 중국의 사이버보안과 정보화 업무 관련 최고 정책결정기구로서 중앙네트워크안전정보화영도소조 (中央网络安全和信息化领导小组)를 설립
- 영도소조의 조장은 시진핑 총서기, 부조장은 리커창 총리와 중국 공산당 당무를 총괄하는 류윈산 서기처 서기가 맡는 등 당·정·군 주요부서의 핵심 지도자 22명으로 구성됨
- 영도소조는 2018년 3월 위원회로 격상되어 위상과 권한을 더욱 강화함
- 위원회는 국가안전과 장기 발전을 위해 경제, 정치, 사회, 문화, 군사 등 각 분야의 사이버보안과 정보화 관련 중대 문제를 전반적으로 협의·조절하고 사이버보안 및 정보화 발전전략과 거시계획을 연구, 제정하며 국가 사이버보안과 정보화를 위한 법제 마련 등을 주요 임무로 함

▶ 국가인터넷정보판공실

- 2011년 5월 설립된 국가인터넷정보판공실은 2014년 2월 당 중앙 직속기구로 중앙네트워크안전정보화영도소조가 설립된 이후, 동 영도소조의 실무 집행기구 역할을 하면서 사이버보안 및 정보화 관련 권한과 역할이 대폭 확대되었음
- 국가인터넷정보판공실의 핵심 임무는 중국 내 인터넷에 대한 감시 및 검열 활동으로, 구체적으로는 인터넷 정보와 관련된 법령 제정과 인터넷 정보내용에 대한 관리 강화 및 관련 기관에 대한 지도와 협조, 인터넷 매체에 대한 심사허가 및 감독, 뉴스 제공 사이트의 규제 등임

▶ 공업정보화부

- 정보화 산업 발전을 위한 정책 및 기준의 입안 및 시행, 산업 운영의 조율과 모니터링, 주요 기술설비 제조업의 발전 및 혁신 촉진, 통신과 인터넷 산업의 규제, 정보기술 개발 및 응용의 가이드라인 제공 등의 역할을 수행함
- 공업정보화부 산하의 네트워크안전관리국은 통신과 인터넷 산업의 사이버보안 계획과 정책, 표준 등을 개발 및 시행하며, 통신과 인터넷 산업 사이버보안 심사 관련 업무, 신기술과 신사업의 보안평가 등을 실시

▶ 공안부

- 국무원 산하의 주요 중앙 부처로 범죄활동의 예방과 저지, 법과 질서 유지, 극단주의, 폭력, 테러의 예방, 국내 치안 유지, 관리 등록 업무(신원확인 서류, 출입국 허가 등)를 주 업무로 함
- 공안부 산하의 네트워크안전보위국은 보이스 피싱 등 경제사기 범죄와 테러, 분리주의자나 극단주의자 등 정치성 사이버 범죄를 조사하며, 전국에 사이버범죄 신고센터를 운영함

3) 인증제도

▶ 중국강제인증제도(CCC)

- 중국강제인증제도(CCC)는 2003년 8월부터 시행된 품질안전관련 인증제도로 음향 및 영상 주파수설비, 정보기술설비, 전신단말기설비, 안전기술 경비 제품 등 19개 유형 132개 제품으로 시작해 유형과 제품범위가 확대되고 있음
- 중국에서 해당 품목의 제품을 생산하거나 중국에 수출하는 업체들은 반드시 CCC 마크를 획득해야하기 때문에 CCC 제도는 수입제품에 대한 무역 장벽을 높여 수출입 비율을 조절하기 위한 수단으로 사용됨
- DVR을 비롯한 주요 물리보안 제품들도 CCC 인증 대상으로 DVR은 2012년 2월 말부터 CCC 인증에 포함되어 완제품으로 수입할 경우 반드시 CCC 인증서를 세관에 제출해야 함

▶ 정보기술보안강제인증제(ISSCC)

- 중국국가인증감독위원회(CNCA)는 2010년 5월부터 외국 기업이 납품하는 정부조달 IT 제품에 대한 정보기술보안 강제인증제(ISCCC) 시행을 발표
- 중국에서 전기·전자제품, 소방제품, 자동차 등 강제인증 대상품목에 포함된 제품은 반드시 관련규정에

따라 인증서를 취득해야 하는 동시에 CCC 인증마크를 부착해야만 중국 내 수입 및 판매가 가능

- 소비자 제품에 실시됐던 안전성 검증제도(CCC)가 통신안전, 데이터 안전, 콘텐츠 안전 등 8개 분야로부터 네트워크 해킹 스캐너 제품, 방화벽, 안전심사 제품 등의 정보보안 제품에까지 확대 시행

표 _ 중국 정보기술보안강제인증제 적용제품

분야	관련 제품	적용범위
경계안전	방화벽	· 방화벽 기능을 주로 하는 소프트웨어 및 하드웨어의 조합, 기타 네트워크 상품의 방화벽 모듈 (개인 방화벽 상품에는 적용되지 않음)
	네트워크 보안격리카드, 선로선택기	· 안전격리계산기(컴퓨터를 포함 디지털방식으로 사용되는 기기), 안전 격리카드, 안전격리 선로 선택기기
	보안격리, 정보교환	· 안전격리와 데이터 교환 상품, 안전격리와 단 방향 문서 전송 상품
통신보안	보안 라우터	· 범위는 IPSec/SSL에 통합되고, 방화벽 침입 탐지 시스템, 안전회계감사 등, 하나의 혹은 다중의 안전모듈의 공유기, 단 접이식 공용 공유기는 제외
신원감식과 출입통제	IC카드칩 운영 체제 (COS)	· 신분감식과 방문통제내의 IC카드칩운영체제(COS) 범위는 접촉 혹은 비접촉 작업방식을 채용한 지능카드의 COS
데이터 보안	데이터백업, 복구	· 독립적인 데이터백업과 회복관리 소프트웨어상품, 데이터 복제 상품과 지속 데이터보호상품은 포함되지 않음
기초 시스템	안전 데이터베이스 시스템	· 독립적 안전 데이터베이스 체계 소프트웨어 상품, 집약 혹은 내재된 안전 데이터베이스 체계 상품
	보안운영시스템	· 기초 플랫폼의 보안 조직체계, 적용되는 범위는 독립적 안전조직 체계 소프트웨어 상품, 집약 혹은 내제된 안전 조직체계의 상품
콘텐츠 보안	스팸차단	· 공개적 안티스팸게이트웨이, 안티스팸메일체계와 메일서비스일체, 안티스팸메일 서비스 시스템
평가심사 및 통제	침입탐지 시스템	· 네트워크 침입탐지 시스템, 주요기기 침입탐지 시스템
	네트워크해킹스캐너	· 네트워크 해킹 스캔상품 ※이 항목에 적용되지 않는 상품은 주요기기 해킹 스캔 상품, 데이터베이스 해킹 스캔상품, WEB 응용 해킹 스캔 상품
	보안심사	· 하드웨어, 서버, 네트워크, 데이터베이스와 기타 응용 시스템 등 하나 혹은 다중의 보안 심사 대상 상품
응용보안	웹사이트 복구	· 정지 상태의 홈페이지 문서, 동태 문서 목록 복구 진행 상품

[출처] KOTRA 상하이 KBC

▶ 모바일앱 안전인증

- 중국 국가인터넷정보판공실과 시장관리감독총국은 2019년 3월 모바일 앱의 이용자 정보를 수집 및 활용하는 관행을 규범화하고 개인정보 보호를 강화하기 위한 '모바일앱 안전인증 실시규칙'을 발표
- 중국네트워크안전심사기술인증센터가 앱 인증을 주관하고 검사기관은 인증센터가 인증업무의 필요성과 기술력에 따라 결정함
- 동 인증은 자율인증으로서 검색엔진과 앱스토어에 인증을 받은 앱에 대해 인증마크를 표시하고 우선 추천할 것을 권장
- 모바일앱 안전인증의 절차는 기술검증과 현장심사, 인증 후 감독으로 구성되며, 인증을 취득하려는 앱 운영자는 인증신청서와 앱 설명서, 인증 요구사항에 부합하는 자체평가 결과 및 관련 인증서류 등을 제출하면 됨
- 단, 관련법이나 규제를 위반한 전력이 있거나 12개월 내 중대 정보보안 사고가 발생한 기업 등은 인증 대상에서 제외함

4) 최근 정책 동향 및 이슈

▶ 2019년 중국 사이버보안 주간, 텐진에서 개최(2019.9)

- 2019년 9월 16일 중국 사이버보안 주간이 텐진에서 열린 가운데, 시진핑 주석은 사이버 공간의 개방성과 혁신성과 함께 안전성과 통제 가능성이 확보되어야 한다고 발언
- 시진핑 주석은 정부가 사이버 공간에서 개인정보의 안전과 시민의 합법적 권익을 보호해야 하며, 인공지능, IoT, 차세대 통신과 같은 신기술의 개발뿐 아니라 이러한 신기술의 응용이 법과 표준에 부합하도록 인도하는 것도 중요하다고 강조
- 사이버보안 주간은 2014년 처음 시작되어 사이버보안에 대한 국가적 의식을 고취하기 위해 매년 시행되고 있으며, 금년에는 사이버보안 전시회와 기술 포럼 등의 활동이 이루어짐

▶ 국가발전개혁위원회, 국가기술 안전관리목록 제도 제정 계획(2019.06)

- 중국 국가발전개혁위원회가 국가안전법 등 관련 법률법규에 의거해 국가안보를 위협하는 상황에 대응하기 위한 국가기술 안전관리목록 제도 수립을 추진 중
- 국가발전개혁위원회는 이번 제도가 국가 안보에 대한 위협을 효과적으로 예방 및 제거하고 국가의 혁신 드라이브와 양질의 발전을 위한 견고한 제도적 토대가 될 것으로 기대

- 인민일보에 의하면 국가기술 안전관리목록 제도를 통해 중국의 자주적인 혁신 능력 강화 및 통제 가능한 전략적 첨단기술과 중요 분야의 핵심 기술을 확보하기 위한 강력한 방화벽을 구축하게 될 전망

▶ 국가인터넷정보판공실, 네트워크 안전심사방법 초안 발표(2019.05)

- 국가인터넷정보판공실은 2019년 5월 '네트워크 안전심사 방법' 초안을 발표하고, 국내외 기업들의 IT 제품과 서비스가 자국의 중요한 핵심 정보기술 인프라와 국가안보를 해칠 가능성을 중점적으로 평가해 보안 심사를 통과하지 못한 IT 제품과 서비스의 구매를 금지하겠다는 방침을 정함
- 심사방법 초안은 국가인터넷판공실과 국가발전개혁위원회, 공업정보화부, 공안부, 국가안전부, 상무부, 재정부, 중국인민은행, 국가시장감독관리총국, 국가라디오TV총국, 국가보밀국, 국가암호관리국이 공동으로 마련함
- 총 21개 조항으로 구성된 심사방법 초안에 따르면, 네트워크 안전심사는 주요정보기반시설 운영자의 IT제품과 서비스 구매활동이 초래할 수 있는 국가 안보의 위험을 중점적으로 평가하게 됨
- 평가에서 고려되는 주요 요소는 △정치·외교·무역 등 비기술적 요인으로 인해 IT 제품과 서비스의 공급이 중단될 가능성을 포함해 IT 제품과 서비스의 통제가능성, 투명성, 공급망 안전 △국방과 군수산업시설, 주요정보기반시설과 관련한 기술과 산업에 대한 영향 △IT 제품과 서비스 제공자가 외국 정부의 자금 지원을 받거나 통제를 받는 등의 상황을 포함
- 주요정보기반시설 운영자는 구매하는 IT제품과 서비스가 국가 안보에 영향을 끼칠 수 있는 경우, 네트워크 안전심사방법에 따라 심사를 진행해야 하며, IT제품과 서비스 구매 시, 제품과 서비스 운영 이후 초래될 잠재적 보안 위험을 예측해 보고해야 함

5) 정보보호 스타트업 관련 정책동향

▶ 국가 사이버보안기지 인큐베이터, 우한에 설립(2018.09)

- 국가사이버보안기지 인큐베이터 기공식이 2018년 9월 우한에서 열렸으며, 투자규모는 30억 위안, 건축면적은 약 30만 평방미터로, 완공 후 중국 최대 규모의 사이버보안 영역 인큐베이터가 될 전망
- 2016년 9월 우한 린콩강 경제기술개발구역 내에 국가사이버보안 인재 및 혁신기지가 설립된 이래 지난 2년간 주요 프로젝트 계약이 성사됨
- 특히 TUS Cybersecurity(启迪网安)가 투자 및 건설하는 인큐베이터 프로젝트는 국가 사이버보안 기지의 중요 부분을 차지함
- TUS Cybersecurity는 이번 인큐베이터를 플랫폼으로 삼아 칭화대학교의 사이버보안 교육자원과

연구자원을 활용해 국내외 사이버보안 프로젝트 및 기업 유치에 나설 계획이며, 각종 과학기술 발전기금 및 공유 공간, 인큐베이터, 액셀러레이터 등을 건설해 사이버보안 산업 생태계를 형성한다는 계획

- 인큐베이터 프로젝트의 완료시기는 2020년경이 될 전망으로, 사이버보안 영역의 200개 기업을 유치해 스타트업 대상 전방위 서비스를 제공할 방침

▶ 사이버보안 인재 양성을 위한 일류 네트워크안전학교 시범 프로그램(2017.08)

- 중국 정부는 지난 2016년 사이버공간 안전 전략을 통해 사이버보안 인재 양성 프로젝트의 실시와 사이버보안 학과의 건립 강화, 일류 사이버보안 학부와 창의혁신단지 설립으로 인재 육성과 혁신 창업에 이로운 생태 환경을 만들겠다는 목표를 제시
- 이에 따라 교육부와 국가인터넷정보판공실은 2017년부터 10년에 걸쳐 사이버보안 인재 양성을 위한 참신한 아이디어와 체제를 탐색하고 다양한 정책적 지원을 통해 10년 내 국제적 영향력과 지명도를 갖춘 4~6곳의 네트워크안전학교를 건설하기로 함
- 시범 프로그램 계획에 따르면 사이버보안 인재 종합 양성을 위해 공학, 법학, 관리학 등을 포괄하는 학제간 프로그램을 수립할 방침
- 또한 사이버보안 분야에 전문 지식과 풍부한 교직 경험을 보유한 교수진을 모집하고 사이버보안 기술/관리 전문가를 겸임 교수로 초빙하며, 재학생들에게 창업혁신을 적극 장려해 인재양성과 기술혁신, 산업발전의 선순환 체계를 형성한다는 계획
- 일류네트워크안전학원 시범프로그램 신청서는 매 2년마다 수리하고, 시범프로그램에 참여하는 학교는 원칙적으로 10개 이내로 제한되며 매년 12월 31일 이전에 국가인터넷정보판공실과 교육부에 해당년도 시범 프로그램 완료 보고서와 차기 연도 계획을 제출해야 함

융합보안 시장 및 정책 동향

1) 융합보안 시장 현황

클라우드/사물인터넷 보안 시장

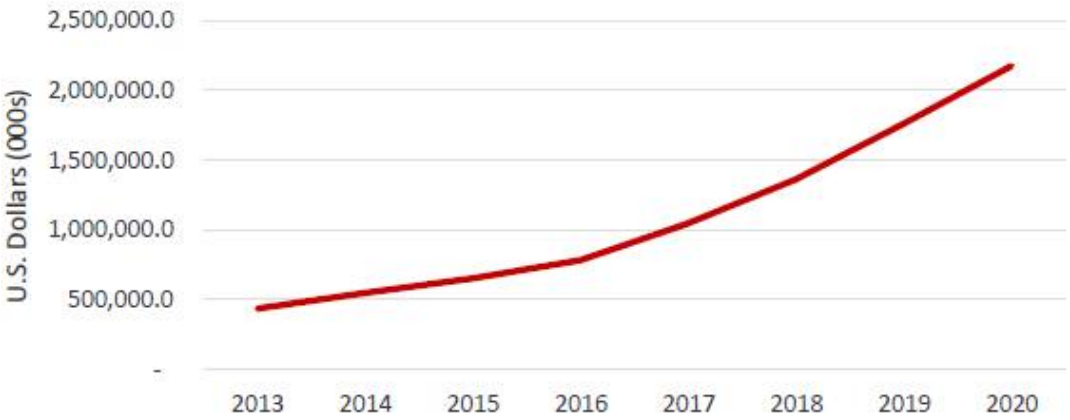
▶ 중국 중상산업연구원에 따르면 2018년 중국의 클라우드 보안 시장규모는 약 37억 7,600만 위안으로 전년 대비 45% 성장했으며, 2019년에는 50% 성장한 56억 1,000만 위안 규모를 형성할 전망

- 또한 사물인터넷이 생산과 소비, 안보 등 다양한 영역에 보급되면서 IoT 기기가 폭발적으로 증가 추세로, 이에 따른 보안 위협의 증가로 사물인터넷 보안 시장도 급속한 성장세
- 2018년 중국의 사물인터넷 보안 시장 규모는 전년 대비 35% 증가한 87억 위안을 기록했으며, 2019년에는 130억 위안, 2021년에는 50% 이상 증가한 300억 위안을 기록할 전망

자동차 사이버보안 시장

▶ Barnes Reports에 따르면 중국 자동차 사이버보안 시장 규모는 2019년 약 17억 5,850만 달러에서 2025년 62억 2,900만 달러로 성장할 전망이며, 2020-2025년까지 5년간 연평균 성장률은 37.3%를 기록할 것으로 예상됨

그림 _ 2013-2020년 중국 자동차 사이버보안 시장 규모



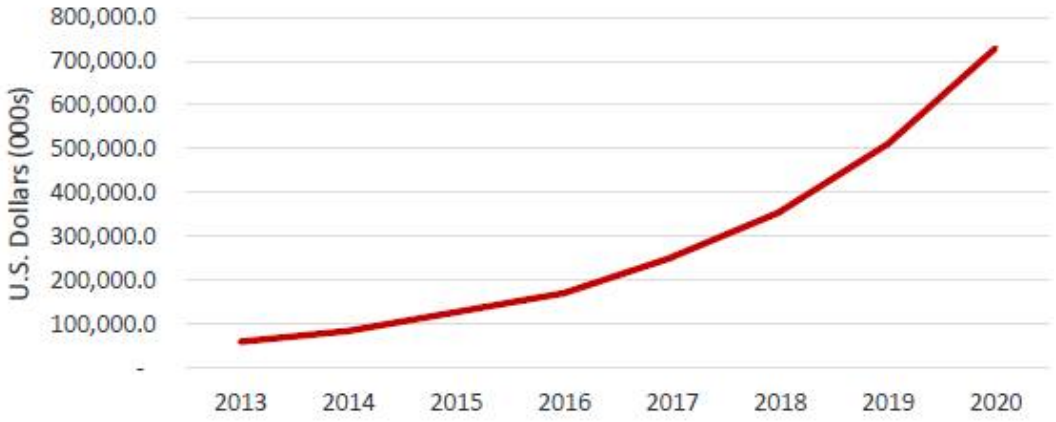
[출처] Barnes Report

인지보안 시장

▶ Barnes Reports에 따르면 중국의 인지보안 시장 규모는 2019년 5억 990만 달러에서 2025년 40억 3,730만 달러 규모로 성장할 전망

- 2020-2025년까지 5년간 연평균 성장률은 90.7%를 기록할 것으로 예상됨

그림 _ 2013-2020년 중국 인지보안 시장 규모



[출처] Barnes Report

스마트 의료

▶ 스마트 의료 시장은 중국의 의료산업 집중 육성 정책으로 매해 높은 성장을 기록 중[61]

- 배경에는 인구 고령화 및 높아진 의료 서비스 수요 대비 병·의원의 수가 모자라거나 대도시에 집중 분포해 있는 현상 때문으로, 온라인이나 거점 시설 등을 이용하여 원거리에서 진료를 받고자 하는 수요가 증가하였기 때문임
- 주로 3급 병원에 해당하는 대형병원을 선호하는 국민들의 선호도로 인해 진료를 위해 긴 대기 시간이 발생하여, 인터넷을 통한 간편한 의료 서비스를 받고자 하는 환자 비율이 증가한 것도 또 다른 요인
- 중국 정부의 완화된 의료산업 정책에 힘입어 기존 인터넷 플랫폼 회사들이 빅데이터·인공지능을 이용하여 스마트 의료시장에 새로이 진출하거나(알리바바, 텐센트 등) 대형병원이 온라인 병원을 설립(광동성 온라인 병원 등)하여 환자들에게 의료서비스를 제공하고 있음

61 https://www.kita.net/cmmrcInfo/rsrchReprt/rsrchReprt/FileDown.do?nIndex=2&nPostidx=1939&classification=5

2) 융합보안 정책 현황

관련 정책 및 규제

▶ 산업인터넷 보안 업무 강화에 관한 지도의견(2019.08)

- 중국 공업정보화부와 교육부, 인력자원사회보장부, 생태환경부, 응급관리부, 국가시장감독관리총국 등 10개 부서는 2019년 8월 '산업인터넷 보안업무 강화에 관한 지도의견'을 정식 발표하고 2020년 말까지 산업인터넷 보안을 위한 기본적인 체계를 구축할 계획
- 지도의견은 2020년 말까지 자동차, 전자정보, 우주항공, 에너지 등 주요 분야에서 최소 20개의 혁신적이고 실용적인 보안 제품을 마련하고 핵심 경쟁력을 갖춘 산업인터넷 보안 기업을 육성한다는 목표를 제시
- 2025년까지는 관련 체계의 개선과 기술수단 수준의 급격한 향상, 일정 규모 이상의 보안 산업 형성 및 상대적으로 완전하고 신뢰 가능한 산업인터넷 보안체계의 기본적 틀도 구축할 계획
- 지도의견은 이러한 목표의 실현을 위해 각지의 관련 부처가 현지의 산업인터넷 발전 현황을 바탕으로 정부 지원체계와 방식을 선진화하고 산업인터넷 보안 분야에 대한 지원 역량을 강화할 것을 요구
- 또한 정부와 산학연 등 다양한 관계자가 협력해 정책 연구, 연구개발, 표준 제정, 연맹과 포럼 결성, 인재 양성 등 다양한 분야를 아우르는 지지기반을 구축하고 산업인터넷 보안 산업 발전에 나서야 한다고 강조

▶ 클라우드 컴퓨팅 서비스 보안 평가방법(2019.07)

- 중국 국가인터넷정보판공실과 국가발전개현위원회, 공업정보화부, 재정부가 공동으로 공산당과 정부 소속 기관 및 핵심 정보인프라 운영업체가 도입하고 이용하는 클라우드 컴퓨팅 서비스에 대해 보안 평가를 의무화하는 규정을 발표하고 2019년 9월 1일부터 시행하기로 함
- 이번 평가방법의 제정 목적은 당과 정부기관 및 핵심 정보시설 운영자의 클라우드 컴퓨팅 서비스 이용에서 보안 통제 수준을 높이고 사이버 보안 위험을 낮추기 위한 것임
- 보안평가는 신고, 접수, 전문 기술 기관의 평가, 전문가 팀의 종합 평가, 보안평가 업무협조기제 심의, 국가인터넷정보판공실의 승인, 평가결과 발표, 지속적인 감독 등의 과정으로 구성됨
- 보안평가에서는 클라우드 서비스 업체의 신용정보와 경영상태 등 기본 상황과 클라우드 서비스 업체 소속인원의 배경과 신뢰성, 클라우드 플랫폼 기술과 제품, 서비스 공급사슬이 보안 실태 등을 점검
- 클라우드 서비스 업체는 당과 정부기관, 핵심 정보시설에 클라우드 컴퓨팅 서비스를 제공하는 플랫폼에 대해 보안평가를 신청할 수 있으며, 신설되는 클라우드 컴퓨팅 서비스 보안평가 업무협조기제판공실이 신청을 수리 후 보안평가를 실시
- 보안평가 결과의 유효기간은 3년이며, 평가 결과를 계속 유지해야 할 경우, 클라우드 서비스 업체는

최소한 유효기간 만료 6개월 전에 보안평가업무협조기제판공실에 재평가를 신청해야 함

▶ 블록체인 정보서비스 관리규정(2019.01)

- 국가인터넷정보판공실이 '블록체인 정보서비스 관리규정'을 발표하고 2월 15일부터 시행에 들어감
- 블록체인 정보 서비스는 블록체인 기술 또는 시스템을 바탕으로 인터넷 사이트, 애플리케이션 프로그램 등 형식을 통해 사회 일반 대중에 정보 서비스를 제공하는 것을 지칭
- 인터넷정보판공실은 블록체인이 신흥기술로서 변조가 불가능하고 익명성 등의 특징을 가지며 국가 발전의 기회이자 사회생활을 편리하게 하는 동시에 일정한 보안 위험을 초래한다고 규정 시행의 배경을 밝힘
- 규정에 따르면 블록체인 정보서비스 제공자는 정보 콘텐츠에 대한 보안 관리 주체로서 책임을 이행해야 하며, 서비스에 상응하는 기술 요건을 갖추고 관리규칙을 제정해 공개해야 함
- 블록체인 정보서비스 제공자는 새로운 제품과 애플리케이션, 기능을 개발해 출시할 때 유관 규정에 따라 국가와 성, 자치구, 직할시의 인터넷정보판공실에 보고해 보안 평가를 진행하며, 정보보안 위험이 발견될 경우 반드시 수정과 개선을 진행해야 함

스마트 의료

▶ 의료산업을 국가 집중 육성산업으로 분류한 후, 특히 인공지능과 원격의료 등에 있어 정책적 산업 육성 및 규제 완화를 통해 의료산업의 고도화를 추구함

- 2018년 1월 베이징시 위생계획출산위원회 주도로 발표된 '의료 서비스의 새로운 개선을 위한 행동계획 실시방안(2018-2020)'에서 원격의료를 제도권으로 도입하고 그 개념과 기준을 설정[62]
- 2019년 초 양회(兩會)에서는 "스마트+(智能+)" 전략을 발표하면서 인공지능을 의료 서비스 등 각 산업 분야에서 활용할 것임을 공표[63]
- 의료산업에 인공지능 및 빅데이터 기술을 적극 도입하면서, 일부 인터넷 대기업 등을 해당 분야의 대표 기업으로 공식 선정·발표하기도 함(예: 19차 공산당 전국대표대회에서 인공지능 대표 기업으로서 텐센트 선정)
- 의료산업에 빅데이터 및 인공지능를 도입하는 것은 개인정보 수집 및 취급 범위 문제가 결부됨과 동시에 의료사고가 발생할 경우 책임의 귀속에 대한 논란이 있을 수 있고, 또한 원격의료의 경우에도 책임 귀속 문제 및 보험 수가 산정 방식에 대한 논의가 필요할 수 있는데, 중국 정부는 제도를 선(先)시행하고 이후에 개선방안을 마련하는 방식을 견지해 옴

---

62 http://korean.china.org.cn/2018-05/07/content_51169798.htm
63 김윤희, [2019 중국양회 2] 정책 방향으로 본 유망산업, KOTRA 베이징 무역관, 2019. 3. 19., 박승혁 수석연구원, 2019년 중국 주요 정책방향과 시사점, 한국무역협회, 2019.2.26. No.5 Trade Brief

나. 인도

'18년 GDP(십억달러)	2,726
'18년 인구수(천명)	1,353,000

■ ITU 글로벌 사이버보안 지수(Global Cybersecurity Index, GCI)

· 인도의 사이버보안 지수는 2017년 대비 소폭 하락한 47위

국가명	2018		2017		전년대비 증감	
	지수	순위	지수	순위	지수	순위
인도	0.719	47	0.683	23	+0.036	-24
대한민국	0.873	15	0.782	13	+0.091	-2

■ ICT 관련 주요 지수

· 인도의 전반적인 ICT 발전 수준은 ITU 조사국 175개국 중 중하위권을 유지하고 있음

지표명	인도		한국	
	점수	순위	점수	순위
IMD 국가경쟁력지수(2019)	-	43	-	28
IMD 디지털경쟁력지수(2019)	-	44	-	10
UNCTAD 전자상거래지수(2019)	57.0	80	89.4	19
ITU 글로벌 사이버보안 지수(GCI 2018)	0.719	47	0.873	15
UN 전자정부 지수(2018)	0.566	96	0.901	3

■ ICT 관련 주요 통계(ITU, 2018년 말 기준)

· 인도의 유선통신 보급률은 매우 낮으며 매년 가입자 수도 줄어들고 있으나, 이동통신 보급률은 87%를 상회하며 양호한 편

항목	인도		한국	
	가입자수(천 명)	보급률(%)	가입자수(천 명)	보급률(%)
유선전화	21,868	1.62	25.906	50.63
유선브로드밴드	18,170	1.34	21,286	41.60
이동통신	1,176,021	86.94	66,356	129.67
인터넷 이용률	34.45%(2017년 말 기준)		95.90%	

정보보호 산업 개요

1) 정보보호 산업 환경 및 배경

▶ 인도 보안 시장은 범죄율 증가로 인한 대중들의 보안 인식 변화 및 급속한 도시화와 이에 따른 은행·현금 지급기의 증가를 바탕으로 보안 장비·서비스 산업에 대한 시장의 관심이 높아지는 추세

- 또한 소셜미디어 및 스마트폰의 증가와, 디지털화의 진전 등으로 이메일 기반 범죄·피싱·멀웨어 및 랜섬웨어·시스템 관련 취약점 악용 등의 사이버범죄가 급격히 증가
- 테러 위협 및 여성 대상 범죄의 증가로 인한 불안감 조성, 인구 대비 부족한 경찰 수도 주된 요인으로 평가
- 지난 몇 년간 꾸준한 경제 성장으로 인도 대도시의 쇼핑몰, 지하철역, 상업용 빌딩 등 공공장소에 은행 및 현금지급기 수가 증가

▶ 이에 안전장비, 가로등, 보안 솔루션 등 치안 서비스 강화를 위한 정부의 투자가 증가하고, 정부의 스마트 시티 조성 계획에 보안 관련 항목이 추가되는 한편, 일반 가정에서도 보안에 대한 수요가 확대되는 추세

- 인도 정부는 대중교통이 범죄에 취약하다는 지적에 따라 인도에서 운행하는 모든 버스에 비상버튼과 CCTV 및 GPS 시스템을 탑재하는 정책을 추진 중
- 향후 20년 동안 항공기 승객 수가 연간 5억 명으로 증가할 것으로 예상되면서 공항 보안에 대한 관심 증가하고 있으며, 과거 스리랑카 호텔 테러 등으로 인해 호텔 보안 분야가 지속적으로 성장할 전망
- 인도 내 스마트홈 성장과 더불어 가정 내 첨단 보안 카메라, 침입 방지 센서, 스마트 도어록 시스템 및 기타 감시 시스템 수요가 증가하는 추세

▶ 한편, 기업이 생산성에 영향을 미치는 멀웨어 및 사이버공격의 증가를 인지하면서 사이버보안 서비스 요구 또한 상승

- 정부의 디지털 인디아(Digital India) 정책 추진으로 사이버공격이 증가와 함께 잠재적 위협이 제기되고 있으나, 사이버보안 전문 인력에 대한 수요와 공급 간 격차가 뚜렷

▶ KOTRA에 따르면 모디 총리 집권 이후, 인도 정부의 IT 산업 육성 정책과 민간 기업의 투자가 맞물리며 인프라 구축을 넘어 5G, IoT 등 IT 산업이 급성장하였으나, 이와 더불어 사이버보안 위협도 증가

- 인도에서 IT 산업과 모바일 앱·뱅킹, 인터넷 뱅킹, 클라우드 서비스 사용이 급격히 증가함에 따라 모바일뱅킹·SNS·IoT 해킹 등 사이버 범죄 발생 가능성 및 범위가 지속적으로 확대
- 사이버보안 기업 Trend Micro은 2018년 인도 내 3,000만 건 이상의 멀웨어 위협을 확인
- 국가범죄기록국(National Crime Records Bureau)에 따르면, 정부에 보고된 사이버 범죄는 2014년

9,622건, 2015년 11,592건, 2017년 12,317건으로 꾸준히 증가 중

- 인도 컴퓨터긴급대응반(CERT-in)이 조사한 2018년 사이버 사건은 총 208,456건으로, 유형별로는 ▲네트워크 스캐닝/탐색(127,481건) ▲바이러스/악성코드(61,055건) ▲웹사이트 위변조(16,655건) ▲사이트 침입/멀웨어 증식(905건) ▲피싱(454건) ▲기타(1,906건)

2) ICT 시장/산업 개요 등

▶ 미국 상무부 산하 국제무역청(International Trade Administration)에 따르면, 인도의 ICT 산업은 국가 GDP의 13%를 차지하며, 인도의 디지털 경제는 매년 약 2,000억 달러의 경제적 가치를 창출

- KPMG는 현재 1,800억 달러로 추산되는 인도 ICT 산업이 2025년까지 3,500억 달러로 성장할 것으로 예측
- 인도 ICT 시장은 IT 서비스(52%), ITeS BPM (19%), 엔지니어링 및 R&D 소프트웨어(20%), 하드웨어(9%)로 세분화

▶ 인도의 모바일 시장은 지난 6년간 강력한 성장세를 나타내고 있는데, 모바일 침투율의 경우 2011년 72% → 2015년 76% → 2018년 91%로 증대

- 2018년 인도 이동통신 가입자는 전년 대비 5% 증가한 12억 3,100만 명 규모로 추산되며, 모바일 가입자 시장 침투율은 2017년 87%에서 4%p 상승한 91%로 예측
- 특히 VoLTE 기술이 출시되고 2020년까지 4G SIM의 활용이 예상됨에 따라, 2021년 회계연도에 4G 사용량이 최고조에 이를 전망
- 5G 보급 역시 진전을 나타내고 있는데, 인도 정부는 2019년 하반기 5G 시범사업을 진행하고, 연말 5G 대역 경매를 진행할 계획
- 5G 출시 이후, 2024 회계연도까지 5G 가입자가 총 가입자의 38%에 도달할 것으로 보이며, 4G・5G・AI・VR・IoT・M2M의 확장으로 통신 타워 산업 역시 급속히 성장 중

▶ 인도의 디지털 경제는 IT-BPM(비즈니스 공정 관리), 전자상거래, 국내 전자 제조, 디지털 결제, 디지털 통신 서비스 등을 통해 연간 2,000억 달러의 경제적 가치를 창출

- 인도의 디지털 기술 도입도 급속히 상승해, 지난 5년간 2억 700만 명 이상이 온라인에 유입되었고, 사용자 당 월간 고정회선 데이터 소비는 '14년 7.1GB에서 2018년 13.3GB로 증대
- 스마트폰 보급률은 2013년 100명 당 5.5에서 2018년 12월 기준 100명 당 26.2로 크게 증가하였고, 사용자 당 모바일 데이터 소비 역시 2016년 중반 이후 54배 이상 증가
- 전자상거래 및 결제 시장조사기관 yStats.com은 2022년까지 인도 스마트폰 사용자의 41%, 즉 약 1억 5,500만 명이 근접 모바일 결제(proximity mobile payment)를 사용할 것으로 예측

정보보호 시장 현황

1) 시장 규모

시장 개요

▶ 보안 서비스 시장에서 가장 빠르게 성장하는 국가로 인도와 중국을 꼽을 수 있는데, 두 국가가 글로벌 수익의 38%를 차지

- 인도 보안 및 안전(Security and safty) 산업 시장규모는 2018년 55억 9,400만 달러에서 2020년 61억 7,300만 달러로 성장할 전망
- 정보보안 시장에서는 플랫폼 소프트웨어 업체와 네트워크 설비업체 등이 보안 시장에 대한 투자를 지속적으로 확대하고 있는 추세이며, 네트워크 보안과 데이터 보안의 비중이 가장 높은 상황

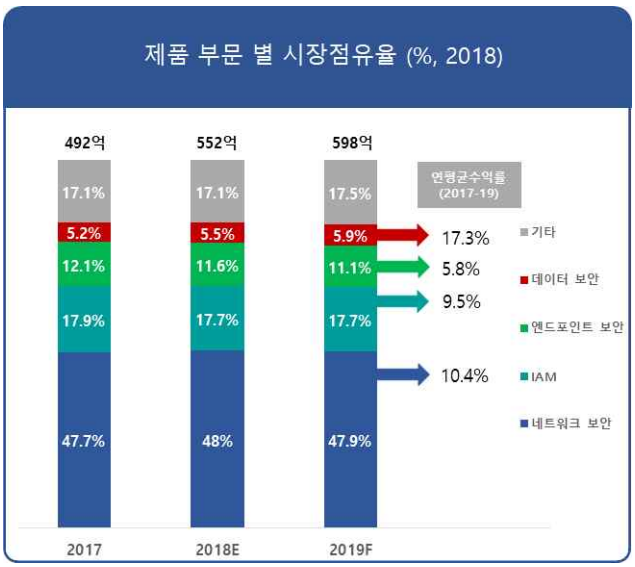
▶ 인도 물리보안 서비스 산업은 보다 고수준의 서비스 및 통합뿐 아니라 구체적인 솔루션을 제공하는 시스템으로 이동하고 있는데, JLL・Sodexo와 같은 통합 시설 관리 서비스 공급자나 G4S 등의 전용 보안 서비스 공급자가 대표적

- 또한 급속한 도시화에 따른 범죄율의 증가로, 홈 모니터링 카메라・스마트도어 잠금장치 등 보안 시장에 대한 관심이 확대되는 추세
- 현지 시장조사업체(Research Nester)는 디지털 도어록 시장 규모가 2016~2023년 기간 연평균 38.9% 성장할 것으로 예측하는 한편, 정부의 스마트시티 구축 계획이 진행되고 있는 만큼 보안에 대한 소비자 인식이 제고되면서 가정용 솔루션 수요 또한 견조하게 유지될 것으로 전망

▶ 인도 사이버보안 시장 규모는 2017년 492억 → 2018년 552억(추산) → 2019년 598억(추산)으로 성장 추세

- 2018년 사이버보안 시장을 제품별로 세분화하면, ▲네트워크 보안(48%) ▲신원 접속 관리(17.7%) ▲엔드포인트 보안(11.6%) ▲데이터 보안(5.5%) ▲기타(17.1%)로 구성
- 이중 차세대 방화벽과 차세대 이메일 보안 도입 및 통합 제품・솔루션에 대한 수요가 네트워크 보안의 성장을 견인
- 제로 트러스트(Zero Trust)가 주류로 자리 잡고 내부 위협이 증가할수록, 신원 접속 관리(IAM)의 성장이 지속될 것으로 예상

그림 _ 2017~2019년 인도 사이버보안 시장 구성



시장 규모 및 성장률

▶ 인도의 보안 서비스 시장은 2018년 5,930 크로레 루피에서 2019년 6,700 크로레 루피로 동기대비 13% 성장할 전망

- IT전문 시장조사기관 Gartner는 2019년 인도 기업 정보보안 지출이 전년 대비 12%가 증가한 18.6억 달러에 달하고, 2020년에는 20억 달러 규모에 이를 것으로 추산
- 한편, 인도상공회의소(FICCI)의 인도 민간 보안시장 보고서에 따르면, 2016년 인도의 사설 보안시장 규모는 88억 달러로, 2020년 152억 달러, 2022년 231억 달러에 이를 전망
- 인도의 2017년 보안 관제 서비스(Managed Security Service)는 디지털화 및 위협 증대로 전년대비 27.9% 성장하였으며, 2020년까지 연평균 18% 이상 성장할 것으로 전망
- 인도 데이터보호협회(DSCI)에 따르면, 2018년 인도의 사이버보안 시장 매출은 4억 5,000만 달러로, 연평균 25~30% 성장

시장 전망

▶ 시장조사기관 Barnes & Co.의 Barnes Reports는 2018년 인도 물리보안[64] 시장을 81억 3,400만 달러로 추산했으며, 2019년에는 9.7% 증가한 89억 2,400만 달러에 이를 것으로 전망

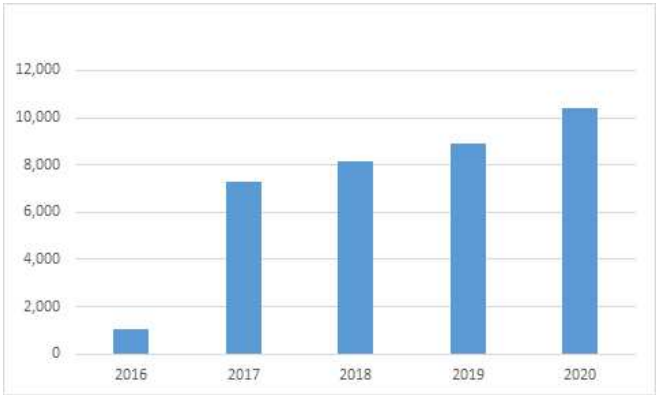
- Dataquest는 최근 몇 년간 인도 비디오 감시 시장이 연평균 27% 성장해, 2017-18년 5,467 크로레

64 보안 경비 및 순찰 서비스 시장 기준

루피에 도달한 것으로 추산하는 한편, 2018년부터 2024년까지 연평균 10.5% 성장할 것으로 예측

- 현재 아날로그 기반 감시 시스템이 전체 감시 시스템의 68%를 차지하고 있으나 IP 기반 감시 시스템 역시 IP 기반시설을 바탕으로 꾸준히 성장할 전망
- 지난 몇 년간 카메라 가격이 하락하고 관련 인식이 높아지면서, 1080p의 고해상도 CCTV 비디오 감시 솔루션에 대한 수요 역시 증가
- 한편 인도의 보안시스템 서비스 산업[65] 시장은 2017년 23억 2,500만 달러에서 2019년 30억 2,600만 달러로 성장 예상

그림 _ 2016~2020년 인도 물리 보안 시장 성장 전망 (단위: 백만 달러)



[출처] Barnes Reports (2018)

▶ 인도는 세계 최대 생체시장 중 하나로, 특히 지문과 홍채 중심의 생체인식 시장이 형성

- 정부 주도의 바이오정보 데이터베이스인 아드하르(Aadhaar)[66] 도입으로 생체인식 제품에 대한 수요가 증가 추세
- 리서치 기업 TechSci Research에 따르면, 2018년 7억 달러에 달했던 인도 안면 인식·인증 소프트웨어 시장이 2024년까지 매년 35.9% 성장

▶ DSCI에 따르면, 인도 기업들이 공급하고 있는 사이버보안 제품의 2018년 총 매출은 약 4억 4,500만 달러 이상으로, 2016~2018 회계연도 동안 연간 25~30%씩 증가

65 Barnes Reports, "2018 World Industry & Market Outlook - Security Systems Services Industry", 2017.12. Barnes Reports는 보안 경보 시스템 판매, 설치, 수리, 원격 모니터링 등을 보안시스템 서비스 산업으로 지칭
66 인도 정부가 추진하고 있는, 지문이나 홍채 인식을 통한 국민 식별 제도의 명칭

그림 _ 2016~2018년 인도 사이버보안 제품 기업 매출 추이



- 한편, 리서치 기업 Research and Markets은 현재 인도 사이버보안 시장을 38억 달러 규모로 추산하며, 2018~2023년까지 연평균 15~20% 성장할 것으로 전망

2) 분야별 현황

물리보안 제품

▶ 인도의 전자 보안 시장은 접근통제 시스템, 비디오 감시, 침입 경보 장치, 인터콤 감시 장비, 경보 시스템, 화재 감지 및 보호 시스템 등의 하위 분야로 구성

- 대표적인 유망 제품군으로는 IP CCTV 카메라, 센서 탐지기, 바이오 정보를 이용한 인증 방식(지문, 홍채 등), 소지품 엑스레이 스캐너, 고급 화재 경보기 등
- 전자보안장비·시스템 시장은 현재 인도시장에서 가장 전도유망한 부문으로서, 이 분야가 전체 보안시장에서 차지하는 비중은 약 20~25%를 기록
- 인도 보안 시스템 통합 시장의 경우, 2018년 4억 5,300만 달러에서 2024년 11억 7,000만 달러까지 성장할 것으로 전망

▶ 인도 감시 시장은 도시 감시, 호텔, 공항 보안, 소매, 제조, 대학 캠퍼스 등을 중심으로 가파른 성장을 보이고 있는데, 스마트시티 프로젝트 추진을 바탕으로 그 수요가 증가할 것으로 예상

- 이중 인도 비디오 감시 시장은 2017-18년 5,467 크로레 루피로 빠르게 성장하고 있으며, 2018~2024년간 연평균 10.5%씩 성장할 것으로 예측

- MarketsandMarkets 자료에 따르면 드론 등 모바일 비디오 감시 시장은 2017년 14억 달러에서 2023년 23억 달러로 연간 평균 8.77%의 성장률을 나타낼 것으로 전망

▶ 보안 장비 시장의 중심이 실내 보안에서 공공장소 보안과 감시로 이동하는 추세로 공항 보안, 대중교통 보안, 해안 경비와 관련한 장비 및 신기술 수요가 증대

- 공항 보안과 관련해서는 바이오인증 방식의 전자 접속 통제 기술, 공항 검색대, 수하물 대상의 폭발물 탐지 시스템 등이 주목
- 대중교통 보안과 관련해서는 자가진단 CCTV 시스템, 자동 무선 이미지 다운로드 기술, 혁신적인 승객용 보안 검색 기술 등에 대한 관심 고조
- 인도 정부는 중앙경찰부대(Central Armed Police Forces)의 장비, 기계, 차량 조달 등에 초점을 맞춰 2018~19년도 부대 예산을 전년 추정치 대비 14.2% 증가한 1,274 크로레 루피로 편성
- 또한 인도 내무부는 2018~19 예산 중 주립 경찰 현대화에 897.3 크로레 루피를 배정함으로써, 경찰 인프라, 범죄·범죄자 추적 네트워크 및 시스템, 전국적인 긴급 응급 대응 시스템, 경찰 통신 및 컴퓨터 서비스, 감시 시스템 등의 업그레이드를 지원할 계획
- 인도 중앙 및 주정부는 도시 감시, 국경 보호, 테러 대응, 경찰 현대화, 정보기관 등에 민간 영역을 활용할 계획으로, 이를 통해 약 27억 달러의 사업 기회가 창출될 것으로 전망

물리보안 서비스

▶ 인도의 민간 보안 산업은 지난 10년간 연평균 20% 성장하였으며, 이중 2018년 민간 경비 산업 규모는 81억 3,800만 달러로 집계

- 민간경비 서비스 부문은 인도 물리 보안 시장 중 75~80%의 점유율을 차지하는 등 보안시장의 주요 산업으로 자리매김
- Barnes Reports 2018에 따르면, 인도 민간 경비 산업은 지속적으로 증가할 것으로 예상되며, 2019년 약 89억 2,400만 규모로 9.7%의 증가율을 예상

정보보안 제품 및 서비스

▶ 시장조사기관 Gartner는 2019년 인도 기업의 정보 보안 제품 및 서비스 지출이 전년 대비 12.4% 증가한 18.6억 달러에 이르고, 2020년에는 20억 달러까지 성장할 것으로 예측

- 2019년 성장이 예상되는 기업 보안 지출 분야는 클라우드 보안 및 통합 위험 관리 부문으로, ▲클라우드 보안의 경우 2018년 대비 300% 성장한 400만 달러가 소요될 것으로 예상되고 ▲통합 위험 관리는 전년 대비 23.1% 성장 전망

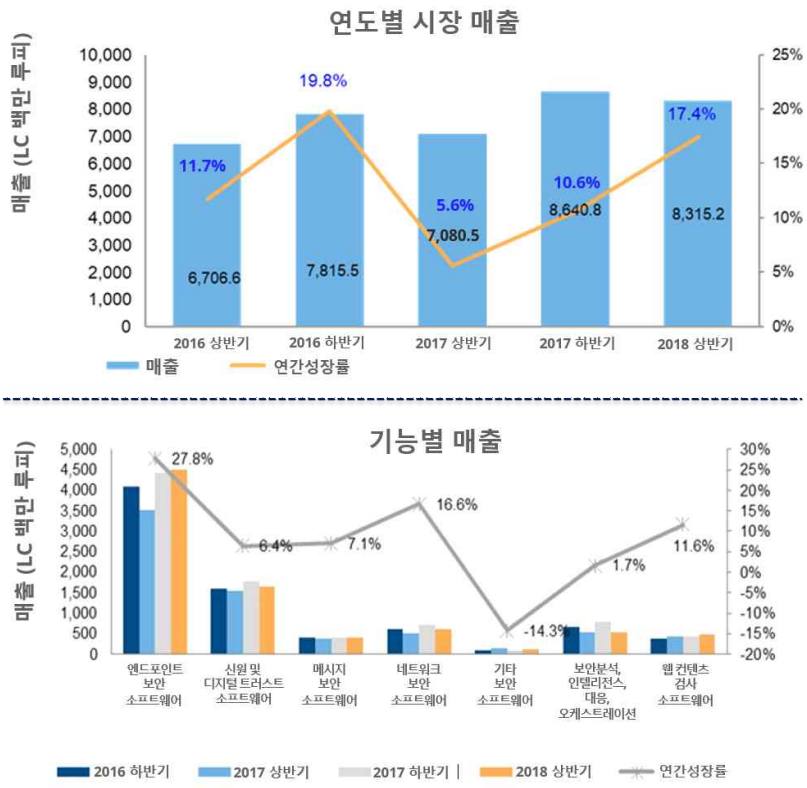
▶ 인도 보안 소프트웨어 시장은 2017년부터 2021년까지 연평균 11.3%씩 꾸준히 성장할 전망

- 인도 소프트웨어연합회(Nasscom)는 전 세계적으로 증가일로에 있는 사이버공격 및 데이터 보호 노력을 바탕으로 2025년까지 인도 내 350억 달러 상당의 매출 기회가 발생하고, 100만 개 이상의 일자리가 창출될 것으로 추정

▶ IDC에 따르면, 인도 사이버보안 및 위험 관리 부문의 사전 대응에 대한 비즈니스/IT 리더의 인식 수준이 높아지면서 2018년 상반기 보안 소프트웨어 시장에 대한 관심이 고조

- 2018년 상반기 다수 대기업의 보안 소프트웨어 구매 및 갱신 반복, 중소기업의 신규 도입으로 엔드포인트 보안에 대한 수요가 지속
- 디지털 인디아(Digital India) 프로그램 증가에 따라 조직이 신원 및 신뢰 소프트웨어를 채택하며, 해당 부문은 보안 소프트웨어 시장 중 두 번째로 큰 몫을 차지
- 다수의 방화벽/네트워크 업그레이드로 특히 금융 분야에서 네트워크 관리 소프트웨어 활용이 확대
- 제조업의 경우, IoT 구현과 디지털 혁신 이니셔티브에 비해 보안 인프라가 부족한 상황인 까닭에, 엔드포인트 보안 · 네트워크 보안 · 웹 검사 소프트웨어 등 보안 소프트웨어 수요가 증대

그림 _ 2016~2018년 인도 보안 소프트웨어 매출 추이



[출처] IDC, 'Market Analysis Perspective: India Security Software Market 1H18 Update'(2019.3)

3) 주요 사업자 현황

시장 특성 및 사업자 수

▶ 물리보안 시장에서 전자보안 장비 및 시스템 부문은 다국적 기업들의 영향력이 큰 상황이며, 보안 장비와 서비스를 통합 제공하는 추세가 두드러짐

- 현재 인도 전자보안장비·시스템 시장은 다국적 보안장비·서비스 기업들의 현지 주문자상표 부착생산(OEM) 방식을 통한 제품 생산과 건물보안 시스템이 주를 이루고 있음
- KOTRA에 따르면 인도 시장에서 조직화된(organized) 보안장비·시스템 업체는 약 700개로 확인되며, 비조직화된(unorganized) 업체의 수는 약 1,500개로 추산
- 보안업체들은 전자보안장비 설치, 감시, 관리 등 보안장비와 보안서비스를 통합한 복합 솔루션을 제공
- 글로벌 기업들은 Honeywell Automation India와 같이 가격경쟁력 확보를 위해 인도 현지기업과 협력한 주문자 상표부착 생산(OEM) 방식을 통해 보안장비를 판매

▶ 정보보안 시장에서는 IoT[67] 및 BYOD[68] 트렌드의 확산으로 인해 APT(Advanced Persistent Threats)[69]에 노출되는 기기와 애플리케이션이 급증

- 인도의 보안 제품 소프트웨어 매출 기준 상위 10개 기업은 Symantec, IBM, McAfee, Check Point, Dell Inc, F-Secure, Trend Micro, Kaspersky Lab, Hewlett Packard Enterprise, Forcepoint의 순
- 이외 매니지드 보안 서비스(MSS), 보안 취약성 관리(SVM) 및 네트워크 보안 역시 주목할 만한 시장
- 인도 소프트웨어연합회(Nasscom)에 따르면, 인도는 2025년 경 정보보안 분야에서 100만 명의 종사자를 창출하게 될 것으로 전망

주요 사업자

▶ Zicom Electronic Security Systems Ltd

- 인도 보안 솔루션 시장의 1세대 기업으로, CCTV 시스템, 침입경보 시스템, 지문인식 기기, 출입 통제 시스템, 화재경보 시스템, 비디오 도어 시스템, 원격보안관리 시스템 등 물리보안 제품과 서비스를 제공하는 한편 사이버보안 분야로 영역을 확장 중
- 2019년 5월 기준 연간 순매출 규모는 약 16.69 크로레 루피로, 전년 동기대비 36.38% 감소

---

67 IoT 즉 사물인터넷(Internet of Things)은 각종 사물에 센서, 통신 기능을 탑재해 네트워크로 연결하는 기술
68 Bring Your Own Device의 약자로, 개인 소유의 스마트 기기를 직장에서 활용하도록 허용하는 것을 의미
69 지능형 지속 공격(APT)은 타깃을 설정한 후 수 주~수 년에 걸쳐 지속적으로 공격하는 형태

▶ Zoom Technologies India

- 인도 정보보안 시장에서 네트워크 및 사이버보안, 포렌식 솔루션 업계의 대표 사업자 중 하나로 주목받고 있으며, 인도 전역에 보안 영업망을 구축
- Kaspersky Lab, NETASQ, egosecure 등 보안 제품과 솔루션을 유통하고 있으며, 관련 서비스 및 교육 사업도 진행
- 동 기업은 전방위적인 사이버 네트워크 보안 서비스 및 보안 기술 교육과정 제공 역량을 갖춘 것으로 평가

▶ Honeywell Automation India Ltd

- 2005년 인도에 진출한 다국적 업체로서 건물 내외의 CCTV 시스템, 원격보안관리 시스템 등 보안업무와 에너지관리 시스템을 취급
- 건물 복합관리 시스템 전문 기업의 특성에 따라, 방문자 관리 시스템, CCTV 시스템, 침입경보 시스템, 접근제어 기기, 에너지 관리를 위한 스마트그리드 시스템 등이 대표적인 상품
- 2019년 3월 기준 연간 매출 규모는 약 317억 3,400만 루피, 총수익은 151억 4,700만 루피

▶ Tyco Fire & Security India Private Limited

- 1991년 설립된 보안 전문업체로서 인도 350여 개 도시에서 보안 서비스를 제공하고 있으며, 인접 국가인 스리랑카, 방글라데시, 네팔, 부탄, 미얀마, 몰디브 등에도 진출
- 주요 취급 품목은 접근제어 시스템, 침입경보 시스템, CCTV 시스템 등 물리보안 서비스 부문

▶ Bosch Security India

- 오랜 전통을 자랑하는 산업 기술 전문 다국적 기업으로서 인도에서는 공항, 철도, 산업용 보안시스템과 건물 복합관리 시스템을 운영 중
- 주요 취급 품목은 비디오 감시시스템, 방문자관리 시스템, 접근제어 시스템, 침입경보 시스템, 화재경보시스템 등 물리보안 시스템 등

▶ Godrej Security Solutions

- Godrej Group 산하의 가정용 보안장비 업체로서, 다양한 소비재를 생산 및 유통하는 모기업의 특성에 따라 일반 사용자의 요구에 부합하는 소비자 중심의 제품들을 제공
- 주로 소비자의 니즈를 반영해 360도 회전형 CCTV, 지문인식 도어록 등 가정용 물리 보안 제품을 출시
- 2019년 9월 제품 혁신 역량 강화, R&D, 기업 브랜딩 등을 위해 향후 2년 간 100 크로레 루피를 투자하겠다는 계획 발표

▶ Aditya Infotech
- 인도의 보안장비 대형 유통업체로서 20여 개국에서 제조된 다양한 해외 CCTV 브랜드를 공급하고 있음
- 주요 취급 브랜드는 ACTi, Avtech, CP Plus, Cynix, D-max, Yoko, Eyeview, Honeywell 등이며, 이 밖에도 Canon, Panasonic, Sony, Eureka Forbes, Godrej, 한화(삼성) 테크윈 등의 CCTV 제품이 유통되고 있음

▶ Quick Heal Technologies Pvt. Ltd
- 인도 푸네에 본사를 둔 IT 보안 솔루션 제공 업체로, 1995년 컴퓨터 서비스 센터로 시작하였으며, 2007년 현재 기업명으로 변경
- 서버, 클라우드 컴퓨팅 환경, 중소기업 등을 위한 보안 소프트웨어를 제공

▶ SUPREMA ID
- 대한민국 기업인 슈프리마아이디는 인도 지문등록기기 시장점유율(40%) 1위 기업으로, 향후 인도 해외 영업지사를 설립하고 인증기기 시장을 확대할 계획
- 2018년 자사의 지문 인식 스캐너인 BioMini Plus 2가 인도 정부의 품질 인증인 STQC(Standardisation, Testing and Quality Certification) 레벨 0을 획득

▶ 그 외, ▲인도 첸나이에 본사를 둔 IT 보안 기업 K7 Computing ▲모바일 보안 소프트웨어를 출시한 Net Protector Research Lab ▲클라우드 데이터 보호·관리에 중점을 둔 druva 등이 있음

4) 주요 동향 및 이슈

▶ 2019년 8월 다국적 기업 Emerson이 인도 푸네(Pune)에 사이버보안 연구소를 개소
- 기존 에머슨 혁신 센터(Emerson's Innovation Center)에 위치하게 될 신규 사이버보안 연구소는 향후 900명의 인력을 고용하고, 사이버보안 전문가 훈련 및 관련 혁신 작업을 진행할 예정
- 또한 제조시설의 공장 운용, 네트워크 시스템, 데이터 자원 등을 보호함으로써 디지털 변혁 전략 도입을 지원할 계획
- 이와 관련해 연구소는 보안 요건 정의, 위협 모델 설계, 보안 실제 유지, 산업 환경에서의 사이버공격 시뮬레이션 등에 주력할 예정

▶ 2019년 3월 인도 국립증권거래소(NSE)의 연계회사인 NSEIT가 글로벌 사이버보안 기업 Aujas를 인수했다고 보도

- 2008년 설립된 Aujas는 정보 보안 컨설팅 및 IT 위험 관리 서비스 제공 기업으로, 전 세계 300개 고객을 보유
- NSEIT는 은행, 금융회사, 보험회사 등에 IT 서비스를 제공하고 있으며, 해당 분야에 대한 사이버보안의 중요성을 인식하고 Aujas 인수를 바탕으로 필요한 보안 인프라를 구축할 방침

▶ 프랑스 컨설팅 기업 Capgemini Research Institute에 따르면, 인도 기업들이 사이버공격 방어를 위해 인공지능 활용을 증대하는 추세

- Capgemini 서베이 결과, 인도 응답자의 2/3 이상이 AI 없이는 사이버공격에 대응할 수 없다고 응답
- 인도 조직은 네트워크 보안(71%), 엔드포인트 보안(71%), 신원 및 접근 보안(60%), 애플리케이션 보안(59%), 클라우드 보안(48%), IoT 보안(44%), 데이터 보안(55%)에 AI 기반 사이버보안 기능을 활용하는 것으로 조사
- 또한 응답자 중 2/3에 달하는 조직이 AI를 도입해 사이버방어를 강화할 예정이라고 응답

▶ 2019년 6월, 기술 기업 Tech Mahindra 및 인도 명문 공과대학인 IIT 칸푸르(Indian Institute of Technology Kanpur)가 사이버보안 분야의 공동 연구를 위한 양해각서를 체결

- 두 기관은 이번 파트너십을 통해 사이버보안 자동화 및 국가 주요기반시설의 디지털 복원력 향상 관련 환경 개발·육성 프로젝트를 위해 긴밀히 협력할 계획

5) 정보보호 스타트업 시장 현황

▶ 인도 스타트업이 공급하는 사이버보안 제품 2018년 총 매출은 8~9억 달러 가량으로, FY2016~FY2018 동안 연간 120% 성장하며 급속한 성장세를 시현

- 2012년 15개 가량 존재했던 인도 내 보안 스타트업이 2017년 20개 이상으로 증가했으며, 투자 금액 역시 2012년 100만 달러에서 2017년 1억 달러 이상으로 상승
- 인도의 보안 스타트업은 향후 10억 달러 규모로의 성장이 예견되고 있는 상황으로, 아카데믹 인큐베이터들이 스타트업에 대한 투자 및 제품 상업화를 지원

그림 _ 2016~2018년 인도 사이버보안 제품 기업 매출 추이



▶ 인도의 주요 사이버보안 스타트업으로는 Lucideus, Sequretek, Securitybulls, Seconize, Lakshya Cybersecurity Labs이 있음

- Lucideus는 최신 정보보안 서비스 및 AI-기계학습 기반 봔 플랫폼을 제공하며 2012년에 설립
- Sequretek는 AI 및 기계학습 기반 보안 도구 및 솔루션을 제공하며 2013년 설립
- Securitybulls는 모의침투 테스트, IT 보안 평가, 인프라 보안 서비스 등을 제공하며 2016년 설립
- Seconize는 클라우드 기반의 AI/기계학습을 지원하는 자동 보안 솔루션을 제공하며 2017년 설립
- Lakshya Cybersecurity Labs는 고객맞춤형 보안 솔루션을 제공하며 2017년 설립

정보보호 정책 및 기관 현황

1) 관련 법령 및 정책

관련 법령 및 규제

▶ 정보기술법(Information Technology Act) 및 시행령

- 인도 통신정보기술부(Ministry of Communications and Information Technology, MCIT)는 2011년 4월 개정된 정보기술법(Information Technology Act 2011)의 시행령을 고시
- 이에 따라 기업들에게 보안 활동과 민감한 개인정보의 보호를 관행과 절차를 요구하며, 이를 위한 산업표준((IS / ISO / IEC 27001)들을 적용하도록 규정
- 해당 산업표준 이외의 표준들을 따르는 경우, 해당 산업협회 등이 코드를 승인받고 중앙정부에 고지해야 하는 의무가 발생
- 해당 산업표준이나 기타 표준들을 따르는 기업들은 중앙 정부의 승인을 받은 독립 감독기구들로부터 감사 혹은 인증을 받도록 규정하는 한편, 연간 1회 이상의 감사 진행을 의무화(프로세스나 컴퓨터 소스 등에 대해 중대한 업그레이드가 이루어지는 경우에도 감사 필요)

▶ 인도 국가보안법(National Security Act)

- 1980년 제정된 인도의 '국가보안법(National Security Act of 1980)'은 중앙 정부와 주정부가 공공질서 유지를 위해 필요하거나 대외 관계에서 국가의 안보와 보안상의 위협이 될 수 있다고 판단한 경우, 공권력을 집행하는 식으로 대응 필요
- 이 법은 잠무(Jammu)와 카슈미르(Kashmir) 지역을 제외한 인도 전역에 적용

▶ 인도 개인데이터보호법안(Data Protection Bill) 발의

- 2018년 7월 27일 인도 개인데이터보호법안이 약 1년간의 의견 수렴을 거쳐 전기정보기술부(Ministry of Electronics and Information Technology, MeiTY)에 제출되었으며, 2019년 말 법제화 완결 전망
- 개인데이터보호법안은 유럽 일반개인정보보호 규정(GDPR)에 준해 ▲데이터 보호 의무 ▲개인 데이터의 처리 ▲민감 데이터의 처리 ▲미성년의 개인 데이터 ▲데이터 원칙 권리 ▲투명성 및 책임성 조치 ▲개인 데이터의 해외 이전 조항 등 112개 조항으로 구성
- 즉 ▲정보 열람권·이동권·잊혀질 권리 등의 데이터 원칙을 권리로 인정 ▲기관의 데이터보호담당관 선임 요구 ▲데이터보호청 설립 ▲기관이 보유한 데이터 현지화 ▲위반 시 금전적 제재 등의 사항을 규정

▶ 인도 전자상거래 규제안(Draft National e-Commerce Policy)

- 2019년 2월 인도 정부는 전자상거래 규제정책(안)을 발표했는데, 이를 통해 국경 간 데이터 이동 제한 프레임워크를 수립할 예정
- 즉, 해외에 본사를 둔 기업이 인도 내에서 사업하고자 할 경우 인도 내 사무소 및 데이터센터 설치를 의무화할 방침
- 2019.6월 경 정부는 향후 12개월 내 전자상거래에 대한 국가 정책 수립을 위한 제도적 틀을 마련할 예정이라고 언급

▶ 정보기술 중개자 가이드라인 규칙안 2018(Information Technology (Intermediary Guidelines) Rules 2018))

- 전자정보기술부(MeitY)는 2018년 12월 정보기술 중개자 가이드라인 규칙 2018을 발표하고 공공 의견을 수렴
- 이번 규칙안은 가짜 뉴스의 확산 방지, 인터넷 음란 정보 억제, 소셜 미디어 플랫폼의 오용 방지, 사용자에 대한 보안 제공 등을 골자로 정보 중개자의 책임을 제시하고 가이드라인을 개정

주요 전략 및 정책

▶ 국가사이버보안정책 2013(National Cyber Security Policy 2013)

- 인도 정부가 2013년 7월 발표한 '국가사이버보안정책 2013(National Cyber Security Policy 2013)'은 개인정보, 금융 및 뱅킹정보 등의 정보들에 대해 안정적인 보안 장치를 마련하기 위한 사이버 보안 정책 프레임워크임
- 전자정보기술부(MeitY)와 통신정보기술부(MCIT)가 공동으로 수립한 이 정책은 사이버보안과 관련해 인도 정부 차원에서 마련한 최초의 정책 사례라는 점에서 화제가 되었음
- 이 정책 프레임워크는 보안 생태계 형성, 개방형 표준 촉진, 규제 프레임워크 강화, 보안위협에 대한 조기경보 메커니즘 마련, 취약성 관리 및 보안위협대응 체제 구축 등을 주요 전략으로 내세우고 있음
- 특히 ICT 인프라스트럭처에 대한 위협과 관련해서는 전략적 정보를 확보하고 대응 시나리오를 마련하며, 위기발생시 관리 및 해결책을 실행할 수 있도록 24시간 가동 가능한 대응 및 복구 메커니즘을 마련하도록 함

▶ 디지털 인디아(Digital India) 전략

- 인도의 나렌드라 모디(Narendra Modi) 총리는 2015년 정보기술(IT) 산업 활성화를 도모하며 '디지털 인도(Digital India)' 전략 제시

- 특히, 전체 국민이 디지털 혜택을 누리고 디지털 기술을 국산화하는 것에 중점을 두고 있음
- 디지털 인도는 ▲디지털 인프라 (Digital Infrastructure) ▲수요를 기반으로 한 거버넌스와 서비스 (Governance & Services on Demand) ▲시민의 디지털 권리 강화(Digital Empowerment of Citizens) 등 3가지 영역으로 구성됨[70]
- 2019년까지 25만 개의 촌락을 초고속 인터넷으로 연결하는 것을 포함해, 전자문서와 전자서명제 도입, 원격진료 및 인터넷 병원 시스템 구축, 전국 주요지점 무선인터넷 중계기 설치, 사물인터넷(IoT) 연구소 설립 등의 계획 추진
- 정부는 2018-19년도 디지털 인디아 예산을 전년도 보다 2배 증가한 307억 3천만 루피 편성(2018.2)

▶ 국가 디지털통신정책 2018(National Digital Communications Policy 2018)

- 2018년 9월 26일 인도 내각이 통신부(Department of Telecommunications)의 국가 디지털통신정책을 승인
- 동 정책은 광대역 및 디지털 통신 기여도를 자국 GDP의 8%로 끌어올리겠다는 전략적 목표를 제시하는 한편, 외국인 투자 촉진을 목적으로 디지털 통신 부문에 1,000억 달러의 투자 유치, 혁신 주도 신생 기업 창출, IoT 생태계 확장 등의 계획을 제시
- 아울러 디지털 통신의 디지털 주권, 안전, 보안 역시 정책의 주요 영역 중 하나로, 디지털 통신을 위한 포괄적인 데이터 보호 체계 구축을 목표로 제시

▶ 사이버보안 인도 계획(Cyber Surakshit Bharat Yojana)

- 인도전자정보기술부(MeitY)가 2018년 발족한 민관 파트너십을 기반의 사이버보안 시스템 강화 계획
- 정부의 디지털 인디아(Digital India) 비전과 관련, 민간 파트너 기업과 협력해 사이버범죄에 대한 인식 제고, 조직 IT 부서·직원 등을 위한 보안 조치 역량 개발 등을 도모
- 사이버보안 인도 계획은 ▲교육 ▲인식 ▲활성화라는 3가지 원칙에 따라 운영되며, 때에 따라 전국적인 교육 프로그램을 진행
- 민간 파트너로는 인텔, 마이크로소프트, Redhat, Cert-In, NASSCOM 등이 대표적

▶ 2018-19년 전자정보기술부(MeitY)는 사이버보안을 위한 각종 시설 설립을 도모

- 자국 사이버공간을 위한 포괄적인 라이브 사이버작전 전용 연습 훈련 시설(Live Cyber Operations Specific Exercise Training Facility)을 설립했는데, 이는 조직이 시스템, 인프라, 프로세스, 인력을

70 첫째, 디지털 인프라는 광 인터넷 및 안전한 사이버 스페이스를 핵심으로 하며, 휴대전화와 은행 계좌를 활용한 디지털 금융서비스의 보급, 공공서비스센터의 간편한 접근, 공공 클라우드의 개발을 통한 사적 공간의 공유를 구축하는 것을 목표로 함. 둘째, 수요를 기반으로 한 거버넌스와 서비스는 수많은 행정기관과 사법체계를 포괄하는 통합적인 시스템 구축, 온라인 및 모바일 플랫폼에서의 실시간 서비스, 원활한 비즈니스를 위한 행정서비스의 디지털화, 금융거래 전자화 및 비현금화 등이 포함됨. 셋째, 시민의 디지털 권리 강화는 일반적인 디지털 해석력 및 디지털 서비스 자료를 인도 언어로 제공할 수 있도록 도모하는 협력적 디지털 플랫폼 구축, 모든 문서 및 증명서의 클라우드화 등을 핵심 내용으로 하고 있음

테스트함으로써 사이버공격에 대비할 수 있도록 지원

- 보안평가, 연구 및 탐색 테스트 센터 구축(Security Evaluation, Research and Exploratory Testing Centre) 프로젝트에 투자함으로써, 사이버보안 테스트 및 평가 개발을 지원
- 그 외 ▲사이버 포렌식 연구소(Cyber Forensic Lab) ▲Bihar주 사이버범죄 및 사이버 포렌식 자원센터 등을 추진

2) 담당기관

▶ 인도 컴퓨터 침해사고 대응팀(Indian Computer Emergency Response Team, CERT-In)

- 정보기술법(Information Technology Act)을 기반으로 만들어진 인도의 전문 IT 보안 기관으로서 정보보호와 관련된 전반적인 업무를 수행
- CERT-In은 ▲정보보안 품질서비스 ▲보안 인지 ▲리서치 분석 ▲사이버공격 감시 및 대응 등 4개 분야에서 30여 개의 서비스를 제공
- 사이버 공간 보안사고 발생 시 관련 정보를 수집, 분석, 배포하는 역할을 담당하고 있으며, 정보보안 실천 사항, 절차, 예방책, 대응책, 보고 등과 관련한 가이드라인 및 백서 발간 작업 등을 수행
- CERT-In은 2018.4~2019.3월 동안 ▲274,465건의 사이버사고 처리 ▲보안 알림 235건 ▲자문 48건 ▲Security Drills(보안 연습) 4건 ▲훈련 26건 등을 진행

▶ 국가 정보과학 센터 컴퓨터 긴급대응팀(NIC-CERT)

- 2017년 12월 인도 정부는 컴퓨터 침해사고 대응팀(CERT-In), 금융 분야의 Fin-CERT에 이어 국가 정보과학센터(National Informatics Centre)를 위한 NIC-CERT를 설립
- NIC는 인도의 전자 비즈니스 및 전자관리(e-governance) 기관으로, NIC-CERT는 NIC 내에 발생하는 사이버보안 사고 관리를 담당
- 사이버 위협에 대응해 인도 정부의 기반시설 및 NIC의 자산을 보호하기 위해 정기적인 위협 정보, 보안 경보, 관련 자료, 자문 등을 제공

▶ 국가 사이버 조정 센터(National Cyber Coordination Center, NCCC)

- 국가 사이버 조정 센터(National Cyber Coordination Centre, NCCC)는 인도의 정보보안 및 온라인 감시 활동을 담당하는 기관
- 2014년 9월 인도 정부에서 이 기관의 설립 필요성을 제기한 이후 2015년부터 2027년까지 1억 5,400만 달러를 투입해 신설

- 동 기관은 ▲사이버 범죄 예방 전략 ▲사이버 범죄 수사를 위한 훈련 ▲오래되어 실효성이 떨어지는 법률에 대한 검토 등을 담당하며, 사이버 공간에서 테러 집단들이 소셜 미디어 등을 악용한 활동을 벌이지 못하도록 인도 및 미국의 정보기관들과도 공조하고 있음

▶ 국가 재난 관리청(National Disaster Management Authority, NDMA)

- 내무부(Ministry of Home Affairs) 산하의 국가 재난 관리청은 자연 재해 혹은 인재 에 대한 대응을 조율하고 위기발생 시 이를 관리할 수 있는 역량을 강화함
- 재난관리법(Disaster Management Act)에 의거해 설립된 NDMA는 재난대응 정책의 프레임을 마련하고 가이드라인과 모범사례를 제시

▶ 국가 핵심정보 인프라 보호센터(National Critical Information Infrastructure Protection Centre, NCIIPC)

- 2014년 설립된 NCIIPC는 인도의 정보보안 강화를 위한 주요 역할을 담당하고 있으며, 다양한 정보보안 이슈를 조율하고 전력, 통신, 방위 등 국가 주요 인프라를 관장하는 정부기관으로 자리매김함
- 통신정보 기술부는 이를 지원하기 위해 전자 통신 및 메시지를 대상으로 한 중앙 모니터링 시스템(CMS) 프로젝트를 추진하고 있음
- 국가 통신망 보안 협동위원회(National Telecom Network Security Coordination Board, NTNSCB)를 통해 인도의 국가통신망 안전을 강화함

▶ 전자정보기술부(Ministry of Electronics & Information Technology, MEITY)

- 전자와 정보통신 부문에서 지속가능하고 포용적인 성장을 지원하기 위한 e-거버넌스를 촉진하고, 연구개발(R&D) 및 혁신을 추진하며, 디지털 서비스를 통한 효율성 향상과 안전한 사이버 공간 구축을 지원
- 디지털 서비스의 전달을 위한 전자 인프라스트럭처를 제공하고, 전자제품 하드웨어 제조와 ICT 산업을 지원하며, 사이버 공간의 정보보안을 강화하는 역할을 담당

▶ 인도 정보통신부(Department of Telecommunication, DoT)

- 정보통신부는 언제 어디서나 안전하고 안정적인 고품격의 통신 서비스를 제공받을 수 있도록 지원하고 이를 통해 사회경제적 발전을 도모하기 위해 설립됨
- 인도를 통신 장비 제조의 글로벌 허브로 육성하고, 국가적 요구사항에 부흥하는 새로운 통신 표준을 개발하며, 국내외 투자자를 확보하고 일자리를 창출하는 등의 목표를 추진

▶ 인도 방위사이버청(Defence Cyber Agency)

- 2018년 11월 인도 총리가 사이버 전쟁, 우주작전, 특수부대를 관리하기 위한 3군 사령부(tri-service

commands)인 방위사이버청(Defence Cyber Agency) 설립을 승인

- 방위사이버청은 중국이나 파키스탄 같은 해외 해커의 군사적 사이버위협에 대응하기 위한 것으로 민간 사이버범죄가 아닌 군사 사이버 사안에 집중할 것으로 알려짐
- 델리에 본부를 둔 방위사이버청은 최대 1,000여 명의 육군·해군·공군 인력 투입이 가능하며, 2019년 11월부터 본격적으로 운영될 것으로 전망

3) 규제 및 인증제도

▶ 인도에서 핵심 정보 인프라를 운영하는 모든 조직들은 보안인증에 관한 국제적인 표준인 ISO 27001 네트워크 보안 표준(Network Security Standard ISO 27001)에 의거한 정보 보안 관리 실천방침을 실행할 것을 권고 받고 있음

- 기타 표준을 준수하는 경우에는 해당 산업협회 등의 코드 승인을 받아 인도 중앙정부에 고지해야 함
- 모든 정부부처와 주요 기관들은 사이버 공격과 테러리즘에 대응하기 위해 위기 관리계획(Crisis Management Plan)을 수행해야 함

4) 최근 정책 동향 및 이슈

▶ 2020년 1월 경 국가 사이버보안 정책(National Cybersecurity Policy) 개정·발표 예정

- 국가 사이버보안 조정관 Rajesh Pant에 따르면, 새롭게 수립된 사이버보안 정책은 정부의 5조 달러 경제 구축 목표를 지원하게 될 예정
- 사이버보안·주요기반시설 보호·민간 파트너십 등을 감독하는 주요 정부부처 간 효과적인 협동 강화 등을 중점 추진할 전망

▶ 인도 전자정보기술부(MeitY)는 2018년 7월 사이버보안 제품에 대한 공공 조달 명령(Public Procurement (Preference to Make in India) Order 2018 for Cyber Security Products)을 공표

- 이는 정부의 '제조업 인도(Make in India)'정책을 장려하고, 인도 내 제품 및 서비스 제조·생산을 강화하기 위한 움직임
- 특히 사이버보안 분야를 전략 영역으로 설정하여, 조달 주체가 국내 제조/생산된 사이버보안 제품에 우선권을 제공하도록 규정

▶ 정부 차원에서 사이버보안 및 범죄에 대한 전략적 대응을 위한 다국 간 안보협력 강화
- 2019년 1월, 인도와 핀란드 간 사이버보안 분야 협력 양해 각서 체결
- 2019년 1월, 인도와 모로코 간 사이버보안 분야 협력 양해 각서 발표(체결은 2018년 9월)
- 2019년 1월 인도와 사우디아라비아가 종합적인 보안 회의를 수립함으로써 양국 간 사이버보안 협력을 강화하기로 합의
- 2019년 8월 인도-프랑스의 디지털 기술 및 사이버보안 로드맵 발표
- 2019년 8월 인도와 바레인은 사이버공간이 테러·과격화·사회 분열에 활용되는 것을 방지하기 위한 협력 증진을 위해 지속적으로 논의하기로 합의

5) 정보보호 스타트업 관련 정책동향

▶ 2017년 2월 인도 전자정보기술부(MeitY)가 Cyber Swachhta Kendra 프로젝트를 발족하고, 사이버보안 스타트업의 테스트 비용을 50% 감축하기로 결정

▶ 인도 정부는 전국 사이버보안 혁신 및 기업가정신을 촉진하기 위한 목적으로 스타트업을 위한 그랜드 챌린지(Grand Challenge for Start-up)를 계획
- 정부는 사이버보안 스타트업을 대상으로 제품 개발 수명주기 동안 멘토십, 재정 지원 등을 제공할 계획
- 현재 동 계획에 대한 정부 제안이 승인된 상태로, 인도데이터보안협의회(DSCI)가 파트너로 참여

▶ 2018년 6월 Telangana 주정부와 인도데이터보호협회(DSCI)가 사이버보안역량센터(Cybersecurity Centre of Excellence) 설립을 추진하기로 결정
- 민관 파트너십 모델을 기반으로 하는 위 역량센터는 혁신, 기업가정신, 역량 구축 등 전략 영역에 초점을 맞춰 관련 생태계를 강화할 예정
- 역량센터의 3대 중점 분야로 ▲혁신 생태계 구축 ▲기존 스타트업 인큐베이터와의 부합 ▲다양한 수준의 역량 구축을 제시

▶ Hyderabad Security Foundation이 구축한 인도 최초의 사이버보안 클러스터(Hyderabad Security Cluster, HSC)가 향후 5년간 인도 전역에 역량센터를 설립할 계획
- 첫 번째 역량센터는 2020년 2사분기 경 Engineering Staff College of India(ESCI)에 개설해, 연구개발·혁신 및 역량 구축·데이터 침해 조사 전문가 교육 등을 진행할 예정
- 또한 두 번째 역량센터 구축을 위해 National Industrial Safety Academy(NISA)와 논의를 진행 중

융합보안시장 및 정책 동향

1) 융합보안시장 동향

스마트시티

▶ 시장조사업체 모도인텔리전스(Mordor Intelligence)에 따르면, 2018년 기준 인도 내 스마트시티 프로젝트 수는 731개(약 46,366 크로레 루피)로, 이중 6.7%인 49개 프로젝트가 착수되었으며, 24개 프로젝트가 종결

- 정부가 진행 중인 스마트시티 계획으로 100개 이상의 스마트시티가 구축되면, 인도 인구의 약 40%를 포괄하고 2030년 GDP 75%에 기여하게 될 전망
- 반면, 센서 네트워크, IoT 기기, 클라우드 컴퓨팅 등의 스마트 솔루션을 기반으로 하는 스마트시티는 IoT로 인해 현저한 혜택을 누리는 동시에 개인정보보호, 보안, 신뢰 등의 사이버 위험 또한 대두
- 2018년 9월 PwC와 인도데이터보안협의회(DSCI)[71] 연구에 따르면, 스마트시티 서비스 중 가장 위험도가 큰 영역(Catastrophic zone)은 ▲감시 시스템 ▲원격의료 ▲e-거버넌스 부문

자율주행차(양자암호통신, V2X 등 포함)

▶ Barnes Report[72]에 따르면, 2019년 인도 자율주행 사이버보안 장비 시장 규모는 1억 8,570만 달러로 추정되며, 2025년까지 6억 2,409만 달러로 성장 전망

그림 _ 2013~2020년 자율주행차 사이버보안 시장 추이 (단위: 천 달러)



[출처] Barnes Reports (2019.5)

71 PwC, Creating cyber secure smart cities, 2018.9.
72 Barnes & Co., 2019 Global High Tech & Emerging Markets, 2019.5.26

표 _ 2013~2025년 자율주행차 사이버보안 시장 판매 변화 예측

시장판매(천단위) 연도 미국 달러		인도 루피
2013	45,170.0	2,732,873.4
2014	57,305.5	3,503,864.1
2015	69,357.0	4,540,696.0
2016	88,510.7	5,936,589.4
2017	113,124.9	8,009,944.7
2018	146,900.3	10,881,610.7
2019	185,743.0	14,679,049.5
2020	224,730.0	18,940,765.5
2025	624,092.4	68,425,495.1
연간변화	**미국 달러**	**인도 루피**
2013-2014	26.9%	28.2%
2014-2015	21.0%	29.6%
2015-2016	27.6%	30.7%
2016-2017	27.8%	34.9%
2017-2018	29.9%	35.9%
2018-2019	26.4%	34.9%
2019-2020	21.0%	29.0%
CAGR2020-2025	35.5%	261.3%

사물인터넷(IoT)

▶ 인도 정부가 스마트시티 계획을 진행하면서 이와 관련해 대규모 IoT 시장이 창출되고 있으며, Nasscom에 따르면 2020년 인도의 IoT 시장이 글로벌 시장의 5%에 달하는 150억 달러에 이를 전망

- 현재 인도 내 IoT 기업은 120개 이상으로, 2014년 이후 스타트업에 투자된 금액은 6,000만 달러를 상회
- 구체적으로 인도의 타타 커뮤케이션스(Tata Communications)는 스마트시티, 유틸리티, 시민 안전에 초점을 맞추고 IoT에 1억 달러를 할당하였으며, 인도 벤처캐피털 블룸(Blume) 역시 IoT 스타트업에 1억 달러의 기금을 투자

▶ PwC는 2019년 IoT 보안에 대한 이해 관계자의 관심이 높아질 것으로 예견

- 또한 2019년 클라우드 채택이 지속적으로 증가하면서, 클라우드 보안에 대한 조직의 관심이 높아지고 클라우드 공유 보안 모델에 대한 공격 역시 다양해질 것이므로, 클라우드 제공업체가 인프라 보호에 더 많은 자원을 투입해야 할 것으로 예측

블록체인(가상화폐 등 포함)

▶ 2019년 1월 인도 은행기술개발연구소(IDRBT)가 은행의 업무 효율화 및 사이버 위협 예방을 위한 블록체인 활용 로드맵을 제안

- IDRBT는 분산형 플랫폼을 통해 금융기관 간 상호작용을 강화할 수 있는 프로토콜 수립을 목표로 정부, 은행, 산업계와 협력 중

핀테크 등

▶ 핀테크 소프트웨어 시장 규모는 2020년 24억 달러에 육박할 것으로 예측

- 현재 인도는 은행 접근성이 없는 인구가 전체의 40%에 이르고 결제의 87%가 현금으로 이루어지는 미개발 시장을 보유한 데다, 2020년 모바일 전화 침투율이 85~90%까지 증가할 것을 예상되면서, 핀테크 솔루션 개발 및 시장 확대 가능성이 농후

▶ 2019년 3월 핀테크 전문매체 MEDICI 보고서에 따르면, 2019년 현재 인도에서 운영 중인 핀테크 스타트업은 총 2035곳으로, 이중 레그테크(RegTech)* 및 사이버보안 분야 스타트업은 단 58개로 집계

* 규제(Regulation)와 기술(Technology)의 합성어로 금융회사가 내부통제와 법규준수를 용이하게 할 수 있도록 하는 정보기술을 지칭

- 인도의 레그테크 및 사이버보안 분야 스타트업은 사기 예방, ID 인증, ID 관리, 디지털 서명 관련 솔루션 등에 주력
- 보안에 주력하는 스타트업 수가 58개로 저조한 원인으로는 관련 과제 해결에 필요한 스킬 및 지식, 자원의 부족 등이 지목

2) 융합보안정책 동향

스마트시티

▶ 2014년 모디 총리는 2022년까지 100개의 스마트시티를 개발하겠다는 '스마트시티(Smart City)'계획을 발표

- 2015~2016년 기간 중 '스마트 시티(Smart City)' 사업에 연간 9억 5,000만 달러의 예산을 지원하고 2022년까지 스마트시티 100곳을 건설한다는 계획으로, 중앙집권적 방식이 아니라 각 지방정부 및 현지 상황에 따라 사업 전반을 관리
- 2015년 6월 스마트시티 솔루션에 대한 가이드라인을 제시하며 핵심 인프라 시설에 "시민의 안전 및

보안" 항목을 제시하였고, 이에 따라 경쟁 참여기관은 '스마트시티 제안서' 내에 일자리 창출, 기업 유치, 공기질 및 수질 개선뿐 아니라 안전 및 보안 향상 부분도 포함시키게 됨

- 2016년 5월 도시개발부(Ministry of Urban Development)는 스마트시티의 사이버보안 모델 체계에 대한 가이드라인을 발표
- 2019년 4월 푼 스마트시티개발공사(PSCDCL)와 인도데이터보안협의회(DSCI)가 스마트시티의 취약점을 파악하기 위한 해커톤을 개최하였으며, 추후 푼 스마트시티 사이버보안 전략을 발표할 예정

사물인터넷(IoT)

▶ 2016년 10월 인도 전자정부기술부(MeitY)는 사물인터넷 정책 초안을 발표하고, 커넥티드 기기 수를 2020년까지 2억 개에서 27억 개로, 자국 IoT 산업 규모를 150달러까지 확대하겠다는 목표를 제시

- 이를 위하여 IoT 연구개발 기금을 지원하고, 국제IoT연구협력제도(International IoT Research Collaboration scheme, IIRC)를 통해 민간부문으로부터 R&D 투자를 유치할 계획
- 또한 IoT 관련 기업에 대한 벤처 펀드 장려, IoT 제조 기업에 대한 세금 해택, 관련 원자재 구입 시 세금 환급, IoT 교육 프로그램 개발 등을 제시
- IoT 보안과 관련해서는 표준 개발 추진을 위한 중심 기관 지정, 전문가 위원회 발족 등의 내용이 포함

스마트공장

▶ 인도 중공업부(Department of Heavy Industry)는 자국의 인더스트리 4.0 이니셔티브로 SAMARTH* Udyog Bharat을 발족

* Smart Advanced Manufacturing and Rapid Transformation Hub: 스마트 첨단제조 및 신속 변혁 허브

- 동 이니셔티브는 통해 인도 제조 산업 내 인더스트리 4.0에 대한 인식 제고하기 위한 목적으로 시연 센터 4곳을 운영 중

블록체인(가상화폐 등 포함)

▶ 인도 가상화폐 규제 강화

- 2017년 대규모 랜섬웨어와 같은 사이버 공격의 증가로 가상화폐에 대한 규제 강화 계획 발표
- 2018년 4월 인도 중앙은행(Reserve Bank of India)이 전 금융기관을 대상으로 가상화폐 서비스 제공을 금지
- 4개월 간의 유예기간을 거쳐 7월 5일부터 가상화폐 거래를 전면 중단하였으며, 이와 관련하여 2019년

8월 인도 대법원이 중앙은행에 암호화폐 금지령에 대한 민원 처리를 명령

▶ 2019년 8월, 인도준비은행(Reserve Bank of India)이 금융산업의 혁신을 촉진시키기 위한 '규제 샌드박스 활성화 프레임워크(Enabling Framework for Regulatory Sandbox)'를 발표

- 이로써 은행, 금융기관, 핀테크 스타트업 등이 혁신 제품과 서비스에 대해 실시간으로 테스트할 수 있는 규제 샌드박스가 구축될 수 있게 되었으나, 암호화폐·ICO 등은 배제
- 한정된 수의 참가 기업들이 제한된 시간 동안 자신들의 제품 및 서비스를 테스트할 수 있는 'End-to-End 샌드박스 프로세스' 형식의 소수 코호트(Cohort) 집단 단위로 운영될 예정
- 본 프레임워크는 규제 샌드박스에서 테스트될 수 있는 혁신 제품·서비스·기술을 적시하고 있는데, 스마트 계약, 데이터 분석 및 사이버보안 제품 등이 이에 포함

핀테크 등

▶ 2017년 전기정보기술부(Ministry of Electronics and Information Technology, MeiTY)가 IT Act 2000의 선지급 결제방식에 대한 규정안(Information Technology (Security of Prepaid Payment Instruments) Rules 2017 –Draft)을 발표

- 전자 선지급 결제방식(e-PPI)의 정보보안, 개인정보보호, 위험 평가 및 위험 통제, 고객 식별 및 인증, 종단간 암호화, 사이버사고 보고 등에 대한 요건 및 규정을 제시

▶ 2017년 인도 정부는 CERT-Fin은 금융 분야의 사이버사고 정보 수집·분석·유포 및 경보 발송, 대응 조치 실행 등을 담당하는 금융분야 컴퓨터침해사고대응팀 CERT-Fin 설립 계획을 발표

- 그 외 2016년 인도준비은행(Reserve Bank of India)이 자관 및 관련 기관의 사이버보안 수요 등 IT 요건을 관리하기 위한 준비은행정보기술유한책임회사(ReBIT, Reserve Bank Information Technology Pvt. Ltd.)를 설립

▶ 2019년 8월, 위 인도준비은행(Reserve Bank of India)이 발표한 규제 샌드박스 활성화 프레임워크에 핀테크 분야도 포함

- 규제 샌드박스 진입 신청대상은 스타트업, 은행, 금융기관, 관련 협력 기관 등을 포함한 핀테크 기업으로 규정
- 신청 기업이 반드시 준수해야 할 요건에는 ▲고객 개인정보 및 데이터 보호 ▲거래 보안 ▲이해관계자의 결제 데이터에 대한 안전한 접속 및 저장 등이 포함

다. 인도네시아

'18년 GDP(십억달러)	1,042.53
'18년 인구수(천명)	267,000

■ ITU 글로벌 사이버보안 지수(Global Cybersecurity Index, GCI)

· 인도네시아의 사이버보안 지수는 한국보다 낮으며, 중상위권 그룹에 속함

국가명	2018		2017		전년대비 증감	
	지수	순위	지수	순위	지수	순위
인도네시아	0.776	41	0.424	70	+0.352	+29
대한민국	0.873	15	0.782	13	+0.091	-2

■ ICT 관련 주요 지수

· 인도네시아의 전반적인 ICT 발전 수준 중위권을 유지하고 있음

지표명	인도네시아		한국	
	점수	순위	점수	순위
IMD 국가경쟁력지수(2019)	-	32	-	28
IMD 디지털경쟁력지수(2019)	-	56	-	10
UNCTAD 전자상거래지수(2019)	50.1	84	89.4	19
ITU 글로벌 사이버보안 지수(GCI 2018)	0.776	41	0.873	15
UN 전자정부 지수(2018)	0.525	107	0.901	3

■ ICT 관련 주요 통계 (ITU, 2018년 말 기준)

· 인도네시아의 유선통신 이용률 및 보급률은 하위권, 이동통신은 중상위권 수준을 유지

항목	인도네시아		한국	
	가입자수(천 명)	보급률(%)	가입자수(천 명)	보급률(%)
유선전화	11,208	4.19	25,907	50.63
유선브로드밴드	8,781	3.28	21,286	41.60
이동통신	320,770	119.84	66,356	129.67
인터넷 이용률	39.79%		95.90%	

정보보호 산업 개요

1) 보안 환경

정보보안 환경

▶ ITU가 발표한 '글로벌 사이버보안(GCI) 2018'에 따르면 인도네시아의 사이버보안 지수는 0.776으로 전체 194개국 중 41위에 올랐으며 아시아·태평양 권역에서는 9위를 기록

- 동 지수는 법적·기술적·조직적 대응, 역량 강화, 국제협력 등 5개 부문을 종합 평가한 것
- 전년도 실적(사이버보안 지수 0.424, 167개국 중 70위, 아태 지역 내 16위)에 비해 크게 발전

▶ Digital 2019 Reports에 따르면, 인도네시아는 인터넷 사용 인구 증가에 있어서 인도·중국·미국에 이어 세계 4위이며 그만큼 관련 위협도 상당한 것으로 분석

- 2018년 한 해 동안 인도네시아에서 감지된 사이버공격은 2억여 건으로 빈약한 사이버 시스템으로 인해 사이버 공격에 대한 노출 빈도가 증가
- 주요 공격 형태는 해킹이며, 국방부나 통신업체 등 정부 및 기업 웹사이트가 주요 표적
- 2017년 워너크라이 랜섬웨어 공격 당시 인도네시아 내 대학, 제조업체, 병원 등 12개 조직이 공격당함
- 최근 조사에 따르면 인도네시아 내 조직의 49%가 사이버공격을 경험했으며, 2018년 Frost & Sullivan는 사이버 공격으로 인한 인도네시아 기업의 직·간접 손실액에 대해 ▲대기업은 최대 670만 달러 ▲중기업은 33,500 달러로 집계
- 'Norton Cybersecurity Statistics Report'의 2017년 보고서에 의하면, 인도네시아 성인 중 사이버범죄의 희생자 수는 5,945만 명(세계 9위)으로 사이버범죄에 대한 낮은 인식 수준이 주요인

▶ 인도네시아 국가사이버암호청(BSSN)은 전국 6개 주에 설치된 21개 센서(HoneyNet)를 통해 수집된 데이터를 기반으로 '2018년 인도네시아 내 사이버공격 실태'에 대한 연간 보고서를 발표

- 사이버 공격은 연평균 15%씩 증가하고 있으며, 공격을 가장 많이 자행한 국가는 러시아(259여 건), 중국(187여 건), 미국(1,42만 여 건)의 순
- 한편 2019년 대선 기간 중 총선위원회(General Election Commission) 서버를 대상의 사이버 공격 시도는 2,880만 건
- 통신정보기술부(KOMINFO)에 따르면, 2019년 인도네시아령 파푸아(Papua)·웨스트파푸아(West Papua) 지역 내 반정부 소요사태와 관련한 거짓정보가 ▲소셜미디어를 통해 20여 개국으로 확산

▲사용된 URL은 약 55만 5,000개 ▲확산자 역할을 한 계정의 수는 10여만 개로 추산

- 이에 따라 정부는 8월 21일부로 해당 지역의 인터넷 엑세스 제한 조치를 단행

물리 보안 환경

▶ 글로벌 인증기관 UL(Underwriters Laboratories)이 발표한 'UL Safety Index(2018)'에서 인도네시아는 66점(글로벌 평균 60점)로 187개국 중 71위(전년 81위)를 기록

- 구체적으로 ▲기관 및 자원(Institutions & Resources) 부문 52점 ▲안전 체계(Safety Framework) 부문 60점 ▲장애나 사망 추정치 등, 안전 관련 수치(Safety Outcomes) 부문 93점
- UL Safety Index에 따르면, 인도네시아의 교통 상해의 주원인은 보행자・오토바이・트럭 사고 등이며, 작업장 내 위험으로부터의 인력 보호 면에서 저조한 것으로 분석

▶ 미 해외안보자문위원회(OSAC)의 'Indonesia 2019 Crime & Safety Report: Jakarta)'에서는 2018년 자카르타 경찰은 강간 31건, 가중폭행 801건, 강도 1,584건, 절도 637건, 차량 절도 1,226건을 보고

- 2018년 총 범죄 건수는 32,301 건으로 전년(총 34,227건) 대비 5.62 % 감소한 반면, 범죄 해결 건수는 28,316건으로 전년(총 27,084건) 대비 4.54% 증가
- 하지만 피해자가 신고를 꺼리는 분위기를 감안할 경우 실제 범죄율은 훨씬 높을 것으로 추정

▶ 한편 갤럽의 전 세계 142개국 거주자들을 대상으로 조사한 '2018 Law and Order Report'에서 인도네시아는 총 89점을 기록해 높은 수준의 법률 및 질서를 가진 국가 9위를 차지

- 동 보고서는 조사 대상자의 거주 지역 경찰에 대한 확신, 거주 지역 내 야간 도보의 안전성, 최근 12개월 내 재산 도난 경험 등에 근거해 조사

▶ 테러 사건 빈도는 정점에 이르렀지만, 이슬람 극단주의의 영향력 증대로 관리에 난항이 예상됨

- 2019년 5월 22일 대선 결과 발표 전후로 이슬람국가(IS) 추종세력에 의한 테러 가능성이 고조되었으며, 검거된 용의자는 대부분은 IS 연계 현지 테러조직 '자마 안샤룻 다울라(JAD)'의 조직원들로 판명
- 2019년 5월 西 자바 주 등에서 검거된 JAD 조직원들의 경우, 2015년 프랑스 파리 연쇄 테러 및 2016년 벨기에 브뤼셀 테러에서 사용된 고성능 폭발물질 TATP(트라이아세톤 트라이페록사이드)를 소지

전자상거래 환경

▶ 세계 4위 인구 대국인 인도네시아는 서남아시아의 B2C 전자상거래 시장의 선두주자이며, 현재 모바일 쇼핑 및 디지털 결제수단 활성화로 전자상거래시장이 역동적 성장을 구가

- 주목할 만한 트렌드로는 모바일상거래(M-Commerce)의 성장을 들 수 있으며,, Katadata Insight Center에 따르면 전자상거래 플랫폼 접속 수단 중 스마트폰이 94%를 차지
- 2018년 기준 인도네시아 전자상거래 시장 규모는 110억 유로로, 그 중 모바일상거래 부문이 60.2%를 차지하고 있는데 이는 영국(41.0%) 및 미국(39.6%)보다 높은 수치
- 한편 Google 및 Tamaseck은 2025년 인도네시아의 전자상거래 시장이 연평균 23.4% 증가해 460억 유로(530억 달러)에 달할 것으로 추정

▶ 2018년 9월 기준, 결제 수단은 계좌이체(69%), 현금결제(22%), 온라인뱅킹앱을 통한 신용/직불(12%), GoPay · Mandiri E-Money · T-Cash 등의 디지털 지갑(11%) 순으로 나타남

- 2018년 2분기 디지털 결제서비스 보급률은 46%였으며, 2020년 모바일 결제 시장은 280억 유로에 달할 것으로 전망

▶ 전자상거래 관련 현지 자료에 의하면, 인도네시아는 전자상거래 산업 보안 순위가 15개 국가 중 14위

- 결제 사기 · 신규계정 사기 · 계정탈취 사기 등 전자상거래 관련 사기가 빈발하며, 산업 발전을 위해서는 사이버 범죄에 대한 국민 의식 제고 및 보안 강화가 절실

2) 인터넷 및 통신 환경

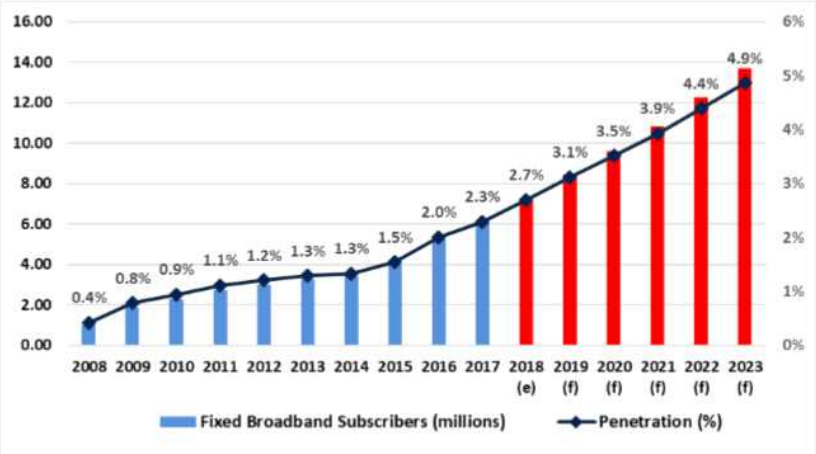
▶개요

- ITU에 의하면 2017년 기준 ▲인구의 99%가 모바일을 보유 ▲3G 네트워크 이용률은 93.8% ▲ 4G(LTE/WiMax)는 90.4% ▲컴퓨터 보유 가구 비율은 19.1% ▲인터넷 연결된 가구 비율은 57.3%
- yStats에 따르면 2018년 기준 인터넷 보급률은 42%로서 2022년에는 53%로 확대될 전망
- 2018년 인터넷 트래픽의 67.5%가 모바일폰에서 발생, 그 뒤를 이어 데스크톱(31.2%), 태블릿 1.2%
- 17,000여 개의 섬으로 구성된 인도네시아는 지리적 특성상 유선통신 인프라 구축이 어려우며, 브로드밴드 개발이 촉진되고 있음에도 고정 광대역 연결성은 2019년 기준 3%로 상대적으로 저조

▶유선 전화

- 유선 전화는 모바일 및 모바일 브로드밴드의 확산으로 꾸준히 감소하는 추세
- 유선 전화 이용자 수는 2012년 3,800만 명에서 2018년 1,630만 명으로 급감했으며 보급률은 4%

그림 _ 유선 브로드밴드 가입자 수와 보급률 전망(2008년~2023년)



[출처] Buddecomm(2019)

- 유선 회선 수 제한 및 모바일 플랫폼의 강세로 유선 브로드밴드 보급률이 상대적으로 저조
- 2018년 유선 브로드밴드 예상 가입자 수는 719만 명, 보급률은 2.7%로 전년 대비 19% 성장
- 시장 성장 동력은 FTTH 부문이며, 현재 Axiata · Biznet · Telkom Indonesia 등이 FTTH 서비스를 개시

▶이동통신

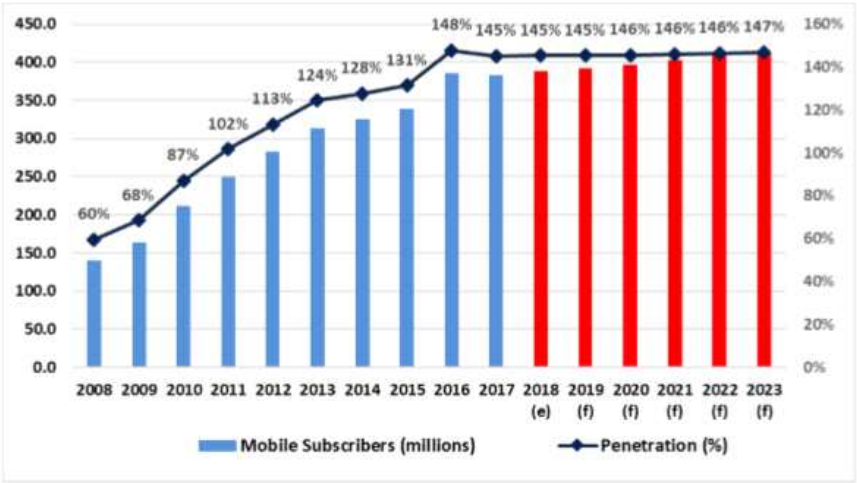
- 인도네시아 내 모바일 사업자는 Telkomsel, Indosat, XL Axiata, 3 Indonesia, SmartFren 등 7개사
- 상위 4개 업체가 시장의 약 90%를 점유하고 있으며, 그 중 Telkomsel의 가입자 수는 1억 9,300만 명(시장 점유율 50.4%)으로 전년에 이어 1위

표 _ 모바일 사업자 및 시장 점유율(2018년)

Operator	Subscribers (million)	Market Share
Telkomsel	193	50.4%
Indosat Ooredoo	64.1	16.7%
XL Axiata	52.9	13.8%
3 Indonesia	58	15.1%
SmartFren	10	2.6%
Bakrie Telecom	1	0.3%
Internux (Bolt)	3.9	1.0%
Total	382.9	100.0%

[출처] Buddecomm(2018)

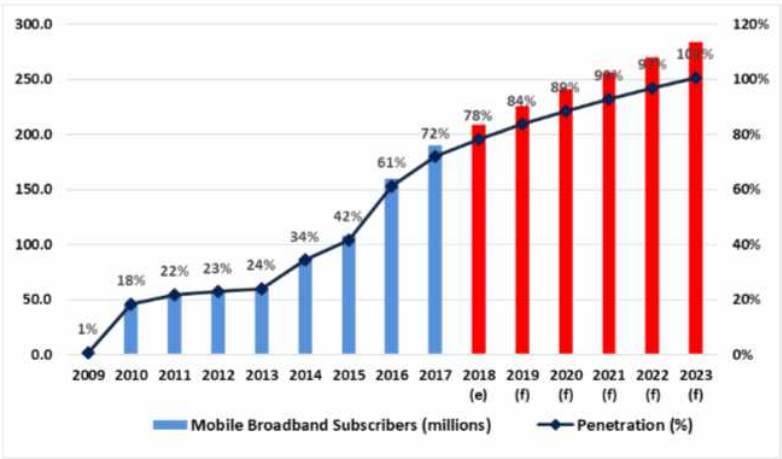
그림 _ 모바일 가입자 및 보급률 전망(2008년~2023년)



[출처] Buddecomm(2019)

- 모바일 가입자 및 보급률은 2016년을 정점으로 성장세가 다소 주춤한 상태
- 2018년 예상 가입자 수 3억8,750만 명, 보급률 145%,로 전년 대비 1.2% 성장
- 2019년~2023년까지 향후 5년 동안에도 연평균 성장률은 1.3%로 성장 둔화가 이어질 전망
- 한편 시장의 성장은 4G 및 5G 서비스에 의해 견인될 것으로 예상

그림 _ 모바일 브로드밴드 가입자 및 보급률 전망(2009년~2023년)



[출처] Buddecomm(2019)

- 모바일 브로드밴드 가입자 수 및 보급률은 2013년 이후 매년 급성장
- 2018년 모바일 브로드밴드 예상 가입자 수는 2억900만 명, 보급률 78%로 전년 대비 61.8% 성장

- 모바일 브로드밴드 시장은 아직 초기단계에 있으며, 이를 감안할 때 2019년~2023년까지 향후 5년 동안 연평균 6.3%의 높은 성장세를 보일 것으로 전망
- 현재 4G 모바일 서비스를 제공하는 모바일 브로드밴드가 강세이며, 이것이 유선 브로드밴드를 대체하는 추세

정보보호 시장 현황

1) 시장 규모

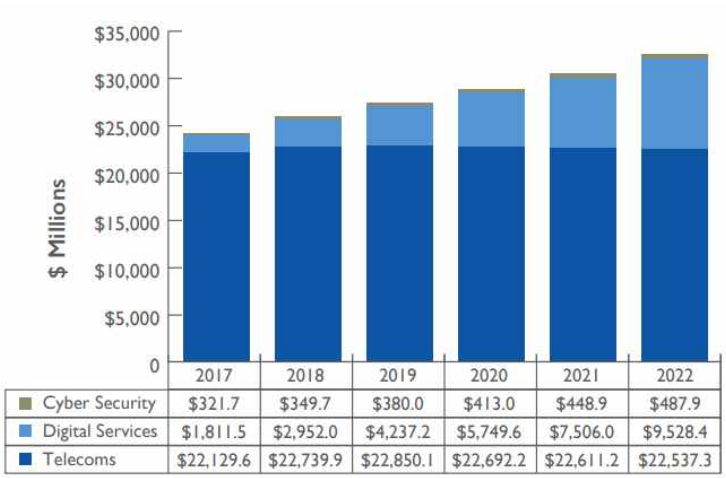
시장 개요

▶ 인도네시아는 중산층 증가와 함께 스마트폰 및 인터넷 사용자가 급증하고 있으며, 통신 네트워크 인프라 투자가 확대되면서 동남아시아 국가 중 가장 주목받는 정보통신 시장으로 부상

- BMI에 따르면 2018년 인도네시아의 ICT 지출은 총 117억 달러 규모로, 부문별로는 ▲소프트웨어는 2018년 15억 달러(2022년 29억 달러) ▲IT 서비스는 68억 달러(2022년 118억 달러) ▲컴퓨터 하드웨어는 33억 달러(2022년 40억 달러)로 증가세를 이어갈 전망
- 한편 IDC는 2019년 인도네시아의 ICT 지출 규모를 332억 달러 규모로 추산했으며, 2022년에는 인도네시아 보안 경보 장비의 10%가 인공지능에 의해 구동될 것으로 전망
- 인프라 부문에서는 위성 및 지상국, 광섬유 케이블 및 액세서리, 라스트 마일(3G 및 LTE 기지국, 기지국 제어기), IT 네트워크 장비, 모니터링 시스템·SCADA·NMS 등에서 수요가 커질 것으로 예측

▶ Frost & Sullivan은 2022년 인도네시아의 ICT 부문별 시장 규모와 관련해 사이버보안 4억 8,79만 달러, 디지털 서비스 95억 2,840만 달러, 이동통신 225억 3730만 달러로 전망

그림 _ 인도네시아 ICT 전체 시장 규모 추이(2017년~2022년)



	2017	2018	2019	2020	2021	2022
Cyber Security	$321.7	$349.7	$380.0	$413.0	$448.9	$487.9
Digital Services	$1,811.5	$2,952.0	$4,237.2	$5,749.6	$7,506.0	$9,528.4
Telecoms	$22,129.6	$22,739.9	$22,850.1	$22,692.2	$22,611.2	$22,537.3

[출처] Frost & Sullivan Indonesia Market Tracker, Statista(2018)

- 부문별 핵심 영역은 ▲사이버보안은 컨설팅 및 자문 서비스, 네트워크 보안 ▲디지털 서비스는 유료TV, 핀테크, 클라우드 ▲이동통신은 4G 연결성, 고정 무선접근 연결성

▶ 인도네시아의 ICT 전략 로드맵은 '국가개발플랜 2005-2025(National Development Plan 2005-2025)'의 일환으로, 국가 연결성 강화를 통한 경제 및 인프라 개발이 목적

- ICT 전략 로드맵은 인프라 및 보안, 채택 및 창조적 활용, 규제 및 법률, 펀딩 등 4개 축으로 구성

표 _ 인도네시아 ICT 전략 로드맵(2005-2025)의 부문별 핵심 목표

부문	핵심 목표
인프라 및 보안	• 2019년 고정브로드밴드 보급률을 도시 가구의 71%, 농촌 가구의 49%로 증대 • 고정브로드밴드 속도를 도시 지역은 1Mbps, 농촌지역은 10Mbps로 제고
채택 및 창조적 활용	• 2020년까지 800만 개 SMEs의 디지털화 달성 • 정부 네트워크 연결(e-government)
규제 및 법률	• 패시브 네트워크 공유 협정 확정 • 2016년 CDMA 셧다운 및 3G/4G 개발과 관련한 스펙트럼 관리
펀딩	• 인도네시아 브로드밴드 개발 플랜(IBP)의 핵심인 Palapa Ring 프로젝트 완료 • 충분한 수익 스트림 창조를 통한 자본비용(정부 투자 15억 달러) 회수

[출처] Frost & Sullivan(2018)

▶ 인도네시아는 모바일 인터넷 사용률이 높음에도 사이버보안 솔루션 시장의 규모는 작은 편

- 많은 조직들의 경우, 아직 정교한 사이버안보 솔루션 실행과 관련한 투자 및 스킬이 부족
- Gartner에 따르면 인도네시아는 GDP의 약 1.6%를 디지털 인프라 구축에 사용하고 있으며, 이는 인접국(싱가포르 6.6%, 말레이시아 4.5%)에 견주어 낮은 수치
- 2019년부터 5년간 ICT 지출을 GDP의 2.5%로 늘이고, 특히 네트워킹・보안・클라우드・데이터분석 등 10개 트렌드에 194억 7,000만~212억 4,000만 달러의 투자가 필요
- 인도네시아 내 ICT 및 소프트웨어의 60%는 외국산이며 자국 기업과 공동개발된 제품은 30% 정도로, 순수 인도네시아産 기술 및 솔루션은 소수에 불과

▶ 2017년 8월 정부는 전자상거래 육성을 위해 '국가 전자상거래 체계 로드맵 2017-2019 (Roadmap for the National Electronic Commerce System for 2017-2019)'을 대통령령(2017년 제74호)으로 공표

- 동 로드맵을 통해 전자상거래 운용 지침을 제시하고 있으며, 사이버보안 항목도 포함

표 _ 전자상거래 로드맵 주요 내용

자금 지원	▲자금 지원 및 대부, 자금 조달 계획 ▲양여금, 자금 지원, 보조금 계획 ▲양여금, 자금 지원 조달 대체 방안 ▲대체자금 지원 및 크라우드 펀딩 계획 ▲전자상거래 관련 정보통신 및 금융 분야 투자제한 리스트에서 해지 등
세금	▲납세의무 간소화 ▲전자상거래 비즈니스의 등록 절차 및 가이드라인 작성 ▲해외 전자상거래 기업에도 동등한 조세 부과 도모
소비자 보호	▲전자상거래에 대한 정부 규정 제정 ▲소비자 신뢰 구축 ▲인도네시아의 전자상거래에 대한 통합 결제 시스템(National Payment Gateway) 구축
교육 및 인적자원	▲소비자와 중소기업, 전자상거래 기업, 정책입안자를 위한 교육 프로그램 구축 ▲스타트업 인큐베이션 프로그램 제공 기관 설립 ▲전자상거래 교육 지원인력 양성 등
물류	▲물류 인프라 향상 ▲낙후지역 물류 시스템 개선 ▲물류 서비스 역량 강화 ▲중소기업을 위한 전자상거래 물류 시설 이전 등, 전자상거래의 발전에 따라 물류 서비스 공급자 증대
인프라	▲ICT 인프라 개선
사이버보안	▲전자상거래를 위한 사이버 범죄 감독 시스템 개발 ▲2018년까지 각 전자상거래 기업의 시스템 지원 요건 충족을 통해 전자상거래 보안성 향상
책임 기구	전자상거래 책임관리위원회 설립

▶ 물리 보안 영역에서는 테러 등 사회 불안 요소의 증가로 상업 및 공공 안전 제고에 역점을 두고 있으며, 안전 및 보안 장비에 대한 수요가 경찰청 등 정부 기관을 중심으로 민간으로 확대되는 추세

- 특히 사물인터넷(IoT)은 보안 관련 핵심 기술로서, IDC는 2019년 인도네시아 지방 정부의 20%가 도로, 가로등, 신호등 등의 인프라를 IoT로 구현할 것으로 전망

시장 규모 및 전망

▶ Barnes Reports에 따르면, 2018년 인도네시아의 보안 시스템 서비스 시장은 약 13억1,600만 달러 규모

- 부문별로는 ▲보안 시스템 서비스 8억 6,420만 달러 ▲도난경보 및 모니터링 4억 2,770만 달러 ▲보호 및 보안 장치 6,000만 달러 ▲감시 시스템 3,400만 달러 ▲화재 경보 및 모니터링 3,000만 달러 규모를 형성
- 보안 시스템 서비스 관련 기업은 총 29,287개로서 총 고용 인력은 142,243여 명
- 한편, 2018년도 인도네시아의 경비 및 순찰 서비스 시장 규모는 41억 400만 달러로, 2019년에는 전년 대비 7.8% 상승해 44억 2,400만 달러에 이를 것으로 예상
- 경비 및 순찰 서비스는 ▲경호 서비스 ▲도난 방지 서비스 ▲보안 서비스 ▲지문 서비스 등의 분야로 분류되며, 2018년 기준 관련 업체는 총 37,378개로 총 고용 인력은 238,000여 명

▶ 한편 Frost & Sullivan이 집계한 2018년 인도네시아 사이버보안 시장은 약 3억 4,900만 달러 규모이며, 2016~2022년 간 연평균 24.7%씩 증가해 2022년에는 4억 8,700만 달러에 달할 것으로 전망

- 2016년 사이버보안 시장에서 네트워크 솔루션 부문이 66.2%를 점유했으며, 주로 은행 및 정부 조직에 방화벽 • IDS(침입방어시스템) • IPS(침입예방시스템) • SSL VPN 등의 솔루션을 공급
- 뒤를 이어 보안 콘텐츠 관리 부문이 19.5%를 차지했고 2022년까지 연평균 13.4% 증가할 전망

그림 _ 인도네시아 사이버보안 시장 규모 전망(2016-2022)

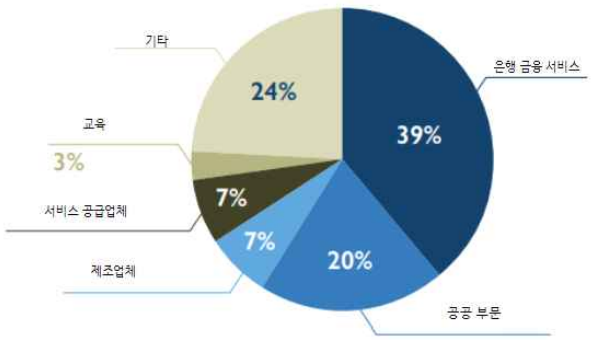
(단위: 백만 달러)



[출처] Frost & Sullivan, Digital Market Overview; Indonesia(2018)

- 고객별로는 해커들의 주요 공격 대상인 은행 및 금융 부문이 사이버보안 시장 매출의 39%를 차지

그림 _ 인도네시아 사이버보안 시장 지출 점유율(고객별)



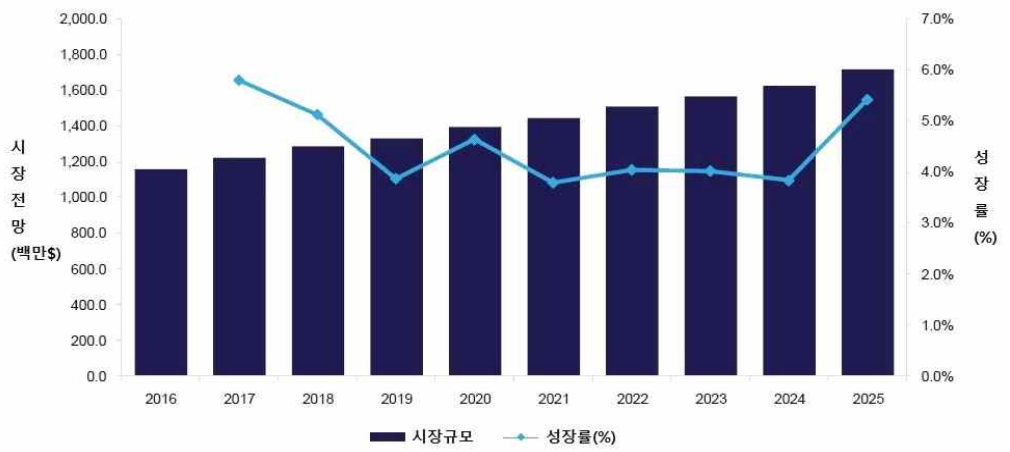
[출처] Frost & Sullivan, Digital Market Overview; Indonesia(2018)

▶ 한편 시장조사기관 6Wresearch에 따르면 보안에 대한 우려 증가, 정보의 보안 지출 및 IT 인프라 확대 등에 힘입어 인도네시아의 물리 보안 시장이 향후 강한 성장세를 나타낼 전망

- 6Wresearch는 인도네시아의 영상감시 시장이 2022년까지 2억 314만 달러로 성장할 것으로 예상
- 2016년 1월 자카르타 시내에서 폭탄 테러 이후 정부는 감시 시스템의 확대에 박차

▶ 글로벌 국방산업 조사 기관 SDI는 2025년 인도네시아의 국토안보 지출 규모(Homeland Security spending)가 17억 1,586억 달러에 도달할 것으로 예측

그림 _ 인도네시아 국토안보 지출 추이(2016-2025)



[출처] SDI(2016)

2) 분야별 현황

물리 보안 제품 및 서비스

▶ 경찰청 등 정부 기관, 또 항만·도로 인프라 구축 사업으로 인해 물리 보안 장비 수요가 증가

- 2025년에 인도네시아 인구의 70%가 도시에 거주할 것이라는 전망 속에서 인프라 개발에 따른 보안 장비 수요가 증대될 것으로 예상
- 한편 2017년 11월, 경찰은 범죄자의 얼굴을 탐지해 알람을 활성화시키는 첨단 CCTV 시스템을 개발 중이라고 발표했으며, 향후 경찰서·공항·항구 등에 배치할 예정

▶ 2014년 12월 '스마트시티 자카르타(Smart City Jakarta)' 이니셔티브 출범 후, 현재 반둥(Bandung) 등 기타 도시에서 스마트시티 정책이 진행 중

- ▲자카르트 외곽 신도시 메이카르타(Meikarta)의 경우 모든 대중교통 수단에 센서 및 CCTV를 탑재해 서로 연결되도록 설계 ▲반둥은 관제센터 구축 및 도로 상황 모니터링 시스템을 도입
- 현재 인도네시아에서는 출입제어 시스템, 알람 시스템, 영상감시 시스템, 금속 탐지기 등 하이테크 보안 장비는 물론, 통합 보안 솔루션이 요구되는 인프라 프로젝트 대부분 해외에 의존

정보보안 제품 및 서비스

▶ 시장조사기관 Kable에 따르면 2016~2019년 인도네시아의 보안 하드웨어 및 제품 시장이 연평균 6% 성장해, 2019년에는 약 292만 달러에 이를 것으로 전망

- 한편 보안 소프트웨어 시장은 2019년까지 매년 3.58% 성장 예상

표 _ 인도네시아 보안 하드웨어 및 제품 시장 추이

(단위: 백만 달러)

분야	2016	2017	2018	2019	CAGR
방화벽 및 VPN 게이트웨이	1.146	1.200	1.246	1.283	3.84%
암호화/SSL 액셀러레이터	0.494	0.528	0.562	0.595	6.40%
콘텐츠 필터링 및 스팸방지	0.431	0.472	0.516	0.560	9.17%
스마트카드 리더기	0.280	0.308	0.336	0.362	8.99%
스마트카드	0.108	0.116	0.122	0.128	5.72%
합계	**2.458**	**2.623**	**2.783**	**2.928**	**6.00%**

[출처] Kable(2016)

표 _ 인도네시아 보안 소프트웨어 및 제품 시장 추이

(단위: 백만 달러)

분야	2016	2017	2018	2019	CAGR
인증	0.2220	0.2335	0.2437	0.2525	**4.38%**
접근 제어	0.1452	0.1557	0.1663	0.1766	**6.75%**
방화벽/VPN	0.1356	0.1417	0.1469	0.1510	**3.64%**
보안 제품군	0.1279	0.1350	0.1416	0.1475	**4.88%**
보안 정보 관리	0.1202	0.1273	0.1340	0.1401	**5.22%**
스팸방지 및 콘텐츠 필터링	0.0969	0.1016	0.1057	0.1091	**4.05%**
안티바이러스 필터링	0.0949	0.0998	0.1044	0.1083	**4.52%**
접근 및 정보보호	0.0928	0.0984	0.1037	0.1086	**5.36%**

분야	2016	2017	2018	2019	CAGR
침입 감지 및 예방	0.0550	0.0572	0.0589	0.0602	**3.04%**
안티 멀웨어	0.0491	0.0473	0.0447	0.0415	**-5.44%**
SWG 소프트웨어 및 웹 안티 멀웨어	0.0458	0.0445	0.0425	0.0398	**-4.60%**
서버 보안	0.0430	0.0437	0.0439	0.0440	**0.76%**
애플리케이션 스캐너	0.0374	0.0380	0.0383	0.0385	**0.98%**
암호화	0.0357	0.0363	0.0366	0.0368	**1.00%**
기기 취약성	0.0356	0.0365	0.0371	0.0373	**1.59%**
포렌식 및 사건 조사	0.0241	0.0250	0.0258	0.0263	**2.99%**
보안 기기 시스템 관리	0.0172	0.0167	0.0159	0.0148	**-4.99%**
PKI	0.0123	0.0123	0.0125	0.0128	**1.42%**
합계	**1.3907**	**1.4505**	**1.5026**	**1.5456**	**3.58%**

[출처] Kable(2016)

▶ 인도네시아의 보안 제품 상당수는 글로벌 벤더의 제품으로 유통업체를 통해 수입되어 리셀러를 거쳐 최종 이용자에게 공급되는 구조이며, 주 수요처는 정부 기관 및 통신, 제조, 금융 업계 등

- 인도네시아 내 사이버 공격 대부분은 멀웨어와 피싱의 형태이며, 정부 기관 및 금융기관의 정보 시스템을 주로 겨냥하기 때문에 방화벽과 안티바이러스 제품이 주로 유통
- 한편 보안시장의 성숙도가 낮아 소프트웨어보다는 하드웨어의 비중이 높은 편
- 소프트웨어 시장의 성장이 더딘 이유 중 하나는 해적판의 범람으로, 2015년 비즈니스 소프트웨어 연맹(BSA) 조사에 따르면 ▲인도네시아 컴퓨터 이용자의 84%가 불법 소프트웨어를 설치 ▲해당 소프트웨어의 상업적 가치는 12억 달러
- 2019년 BSA는 해적판 소프트웨어의 리스크에 대한 인식 제고 및 정품 소프트웨어 사용의 유익 설파를 위해 인도네시아 · 태국 · 필리핀에서 'Legalise and Protect' 캠페인을 진행 중

3) 주요 사업자 현황

시장 특성 및 경쟁 강도

❑ 정보보안 시장

▶ 인도네시아의 IT 및 정보보안 시장은 글로벌 기업이 주를 이루고 있으며 기업 간 경쟁이 치열

- IT 솔루션 및 네트워크 분야에 진출한 기업은 EMC, HP, Cisco, VMware, Redhat, Radware, Sophos, 등이며 정보보안 분야 진출 기업은 Check Point, Trend Micro, Fortinet, McAfee 등
- 글로벌 기업들은 정부 및 금융기관 등 높은 수준의 정보보안을 요하는 기관을 중점 공략

▶ 정부 기관을 위시해 금융, 전자상거래 등 산업 전반에 걸쳐 사이버보안 서비스에 대한 투자가 이뤄질 전망이며, 특히 클라우드 기반의 서비스 채택에 있어서 SMEs가 주도적 역할을 할 것으로 기대

- 한편 정부 조직들은 하드웨어 기기 기반의 솔루션을 선호하며 DDoS 완화는 벤더 업체에 아웃소싱

▶ 현지 이동통신 사업자 및 보안 전문업체 등이 보안관제센터(SOCs) 자체 구축 및 사이버보안 홍보에 박차를 가함에 따라, 향후 사이버보안 서비스 채택률이 더욱 증대될 것으로 예상

- 인도네시아 현지 보안서비스 제공업체 및 이동통신 사업자들은 SOCs 구축 경험 및 운용 역량을 갖춘 글로벌 업체와의 파트너십을 통해 사이버보안 솔루션을 제공하는 추세
- 또한 Telcom Telstra 등 현지 기업들은 아웃소싱 서비스와 SOC 제공해 투자 회수 속도를 제고

표 _ 인도네시아 3대 현지 사이버보안 업체 전략(2017)

부문	주요 특징	성장 전략	핵심 부문
Telcom Telsta	• 자문 서비스를 통한 추천 채택 및 요구 조건에 기반한 맞춤형 서비스 실시	• Telkom의 국내 및 글로벌 네트워크 역량 및 인프라를 활용해 E2E 솔루션 포트폴리오 제공하기	• 금융 서비스 • 공공 부문 • 제조
Binaryworks	• 맞춤형 보안 시스템을 제공함으로써 네트워크 및 시스템 보안 증진에 역점	• 다양한 플랫폼에 활용 가능한 자체 제품 제작하기	• 헬스케어 • 금융 서비스 • 교통 • 제조
Xynexis	• 비즈니스 및 산업에 대한 심층 지식, 시연(hands-on) 기술 스킬, 고객에 특화된 액션 플랜에 기반한 정보보증(information assurance) 방법론을 구사	• 자회사 Noosc를 통해 새로운 보안 관제서비스(MSS)를 제공 • 동 서비스는 기관들로 하여금 SOC의 온전한 관리 및 모니터링 하도록 지원	• 공공 부문 • 금융 서비스 • 소매 • 제조

[출처] Frost & Sullivan

❑ 물리 보안 시장

▶ 인도네시아 물리 보안 시장에 진입한 글로벌 기업으로는 AvTech, Axis Communications, Bosch Security Systems, Dahua, Hikvision, Hanwha(구 Samsung) 등

- BitRefine가 조사한 2019년 1분기 인도네시아 내 CCTV 브랜드 점유율에 따르면, Axis(37.1%), Hikvision(18.6%), PROvision(11.4%), Ganz(10.0%), Dauha(8.6%), Lilin(8.6%), AVTech(5.7%)의 순

▶ 미국 상무부의 'Global Safety and Security Resource Guide'는 인도네시아에서는 중고급 보안 및 안전 장비 시장이 비교적 발달한 것으로 조사

- ▲중급 제품은 일본 · 한국 · 대만 · 중국 산 ▲고급 제품은 미국 · 유럽 산이 대부분 ▲인도네시아 자국 제품은 소화기, 자물쇠, 금고, 호신용품 등에 한정

주요 사업자

❑ 정보보안 시장

▶ Trend Micro

- 2018년 10월 자사의 보안제품 배포를 위해 인도네시아의 최대 유통업체인 ECS와 파트너십 체결
- 2019년 4월 Apex One이라는 최신 제품을 출시했으며, 이는 클라우드 기술에 기반해 디지털 비즈니스를 시도하는 기업을 위한 최고의 보안 솔루션

▶ Fortinet

- Unified Threat Management(UMT) 솔루션의 리더로서, Gartner의 '2019년 메직쿼드런트 보고서의 네트워크 방화벽 부문(Magic Quadrant for Network Firewalls)'에 10년 연속 등재
- Fortinet은 동남아 각국에 리셀러를 두고 있으며, 인도네시아 현지에 파트너 8곳을 통해 영업 전개

▶ Q2 Technologies

- 보안 솔루션에 주력하는 IT 솔루션 업체로서 ICE ACTIMIZE, Paladion, MarkAny, RSA Security, IBM, ACTIVE Identity 등의 보안 솔루션을 유통
- 2019년 8월 국제 사이버 보안 및 E-비즈니스 인증기관이자 CEH(Certified Ethical Hacker) 및 LPT (License Penetration Tester)로 유명한 EC-Council USA와 전략적 교육 파트너십을 체결

▶ PT. Piranti Nusantara Teknologi(PIRANUSA)

- IT 및 소프트웨어 전문 사업자이며 ZWCAD의 공식 총판이자 ZWSOFT, Microsoft의 파트너사

- 보안 분야에서는 Kaspersky Lab, Symantec의 솔루션을 판매

▶ Astra Graphia Information technology(AGIT)

- TELKOM, Microsoft, Ericsson, Cisco 등의 파트너로 시스템 모니터링 및 데이터 센터 솔루션을 공급
- 2019 인도네시아에서 가장 혁신적인 기업에게 주는 '혁신 기업상' 수상

❑ 물리보안 시장

▶ Bosch Security Systems

- 미국 기반의 보안 장비 업체로서 2008년 자카르타에 PT Robert Bosch라는 순 외자 법인을 설립
- 인도네시아 Surabaya, Bali 등에 지사 설립 및 Cikarang과 Bekasi에 자동화 제조공장을 운영
- Bosch Security Systems는 영상감시 시스템, 침입경보 및 화재 경보 시스템, 출입제어 시스템, 공항·철도·회의장 등을 위한 전문 보안 솔루션을 제공
- GSX 2019에서 신규 카메라, 녹화 및 관리 솔루션 등 50여 개의 신제품 출시 계획에 대해 발표

▶ PT. Handal Solusitama (Handal Security)

- 인도네시아 자카르트 기반의 PT. Handal Solusitama (Handal Security)는 전자보안 시스템 통합 제공업체로서, CCTV, EAS 및 리테일 매장용 알람 시스템, 접근 제어 시스템 등을 취급
- Handal Security는 Checkpoint Systems의 유일한 유통업체로 활동 중

▶ ADV International

- 중국 기반의 ADV **International은** 싱가포르에 유통 및 생산 조직을 두고 CCTV 제품만을 집중 취급
- 말레이시아, 인도네시아, 중국(심천) 및 홍콩 등에 CCTV 판매 지사를 설립

▶ Certis

- 싱가포르 기반의 Certis는 인도네시아 Jakarta, Bandung, Batam, Surabaya 등에 지사를 두고 있으며, 광범위하고 전문적인 통합 보안 솔루션 및 원스톱 서비스가 강점

4) 주요 동향 및 이슈

▶ 인도네시아 보안업체 PT Professtama, 호주 Red Piranha와 파트너십 체결 (2019.3)[73]

- Red Piranha는 차세대 방화벽 'Crystal Eye'를 개발한 호주 기반의 보안 스타트업
- Professtama 측은 동 파트너십을 통해 Crystal Eye를 비롯해 Red Piranha의 사이버보안 소프트웨어 및 서비스 솔루션을 인도네시아 기업 및 기관에 공급할 예정
- 특히 향후 1-2년 간 500만 달러 규모의 Crystal Eye 플랫폼을 인도네시아 시장에 독점 조달할 계획
- 양사는 자카르타 보안운영센터(SOC) 구축에 협력할 것이며, Red Piranha는 호주 교육 기관과 연계해 인도네시아 청년 전문가를 위한 사이버보안 전문지식 교환 프로그램을 지원할 계획

▶ Facebook, Agence France-Presse(AFP)와 팩트 체크 파트너십을 체결(2019.4)[74]

- Facebook은 인도네시아 대선 전에 국외에서의 정치 광고를 금지
- 한편 인도네시아 정부는 소셜미디어를 통해 유통되는 거짓정보가 선거전에 영향을 준다고 판단해 선거전 동안 80명으로 구성된 팩스체크팀을 구성

▶ 2019년 CCTV 시장 규모 15-20% 성장 전망 (2019.5)[75]

- Statistica에 따르면 2018년 인도네시아의 물리보안 시장 규모가 약 3억 5,000만 달러(USD)
- 연 평균 55.3% 성장하여 2022년에는 20억 1,000만 달러 규모에 이를 것으로 전망

▶ 자카르타 교통경찰국, AI 카메라를 도입해 전자교통단속시스템(ETLE)을 더욱 강화(2019.7)[76]

- 이 시스템은 2019년 7월 1일 기준 10곳의 신규 CCTV 카메라를 통해 작동 중
- 기존의 CCTV 카메라는 표지판, 도로 표지판, 신호등 위반 사항만 기록한 것에 반해, 동 카메라는 안전벨트 착용 및 운전자의 휴대전화 사용 여부, 가짜 번호판, 속도위반, 자동차 내부의 활동 기록 등 다양한 추가 기능이 탑재
- CCTV 카메라로 연결된 ERI 프로그램을 통해 교통법규 위반 차량의 번호 및 위치를 교통관리센터(TMC)에 통보하면, 센터에서 차량 및 차주 주소지로 스티커를가 발송

▶ 인도네시아 수도 이전 계획 및 보안기술 인프라 개발(2019.8)[77]

- 자카르타에서 1,300km 떨어진 보르네오섬 東 킬라만탄(East Kilimantan) 지역이 새 수도로 선정
- 높은 인구 밀도(3,000만여 명), 2040년 수자원 고갈 가능성, 지진 빈발 등이 수도 이전의 이유
- 새 수도 건설 공사는 2021년에 착수되며 총 440억 달러의 비용이 소요될 전망

---

73 Red Piranha, "Red Piranha signs US$5 Million Cyber Security capability partnership at Indonesia-Australia Free Trade Agreement Signing ceremony", 2019.3.4
74 The Asian Post, "Hoax busters: Fighting fake news in Indonesia", 2019.4.9
75 Marcomm, "UNV Targetkan Pangsa Pasar CCTV 20% di 2019", 2019.5.10
76 HanIn Post, "자카르타 교통국 인공지능 CCTV 카메라 설치", 2019.7.3
77 Tribunn News, "Empat Rekomendasi Teknologi Keamanan Canggih untuk Ibu Kota Baru dari ATISI", 2019.8.8.; ABC, "Indonesia picks Jakarta capital replacement in East Kalimantan province on Borneo", 2019.8.27

- 새 수도의 콘셉트는 '숲속 스마트시티(smart city in the forest)'이며 18만 헥타르의 정부 부지를 확보
- 인도네시아 보안산업 및 기술협회(ATISI) 등은 정부의 수도 이전 계획에 지지를 표명
- 수도 이전에 따른 기술 인프라 개발과 관련해 ATISI는 4대 보안안전 기술, 즉 ▲도청 및 도난 방지 기술 ▲계층화된 보안 시스템 ▲CCTV 수량 및 품질(100㎢당 CCTV 100대 설치, 온도 센서 및 야간투시 기능 탑재) ▲안면인식 및 인공지능 기술을 권장

5) 정보보호 스타트업 시장 현황

▶ 2019년 10월 기준 인도네시아에는 Gojek, Traveloka, Bukalapak, Tokopedia, OVO를 포함해 총 5개의 유니콘 기업이 있으며, 유니콘 대열에 합류한 정보보안 스타트업은 현재로서는 부재

- 한편 Nodeflux와 Avnos 등 현지 및 해외 기반의 정보보안 스타트업들이 맹활약 중

▶ 인도네시아의 비전 AI 스타트업 Nodeflux는 지능형 영상분석(IVA) 기술로 글로벌 기업으로 도약

- 동 사는 2016년 설립되었으며, 2019년 3월 텍사스에서 개최된 'FSXSW Festival 2019'에 참여함으로써 AI 기반의 지능형 영상분석(IVA) 기술 업체로서의 역량을 인정받음
- 현재 인도네시아 경찰청(POLRI) 및 인구・시민등록부(DISDUKCAPIL)의 승인 하에 안면인식과 딥러닝 기술을 바탕으로 IVA 기술을 구현 중으로, 두 기관의 대규모 데이터베이스를 추출해 CCTV 카메라에 포착된 인물・사물을 고도의 정확도로 인식
- 동 기술을 자카르타와 반둥 내 CCTV 카메라에 연결해 스마트시티 관리 및 공공안전을 지원
- 그 외, 2018년 아시안게임 및 IMF-World Bank 연례회의의 보안을 담당

▶ 한편 Avnos는 대표적 외국 스타트업으로서 아태지역 본사를 싱가포르에서 인도네시아로 이전

- 인도네시아 투자자로부터 시리즈 A에서 1,000만 달러의 투자금을 확보했으며, 향후 인도네시아의 사이버 R&D를 구축함으로써 인재 개발 및 사이버보안 인식을 제고할 전망
- 자사 제품 DSF/ Avnos 2.0(Avnos Decentralized Software-Defined Firewall)은 기업이 내부 네트워크 또는 공용 인터넷에 관계 없이 시간과 장소를 불문하고 자사 장치에 대해 보호 기능을 제공

Ⅲ. 정보보호 정책 및 기관 현황

1) 관련 법령 및 정책

관련 법령 및 규제

▶ 정부는 2008년 '전자정보 및 거래에 관한 법률(Law No. 11 of 2008)'를 제정해 사이버 범죄에 대응하고 있으며, 그 후 2016년 11월에 개정(Law No. 19 of 2016)

- **(Law No. 11 of 2008) 동** 법률은 전자정보 거래에 대한 적정 규제를 통해 정보기술 개발·유통·촉진·오용 방지를 도모
- 전자정보 거래에 관한 규정뿐 아니라, 이와 관련한 전자서명·지식재산권·개인정보보호·분쟁 해결·정부 및 공공 기관의 역할·형벌 규정 등을 총 망라
- (Law No. 19 of 2016) 동 개정법은 ▲'전자시스템 공급자(Penyelenggara Sistem Elektronik)'를 전자시스템을 공급·운영·관리하는 개인·공무원(state administrator)·기업·조직으로 그 의미를 구체화 ▲잊혀질 권리 및 정부의 접근 중단 권한을 인정
- 동 개정법이 개인의 프라이버시 권리를 강화시킨 반면, 표현의 자유 등 대중의 정보권을 제약할 수 있다는 점에서 논란

▶ '전자정보 및 처리에 관한 법률'에 근거한 '정보보호를 위한 시스템 운영 규정 (Ministerial Regulation No. 4 of 2016)'

- 동 규정은 공공 서비스 관련 전산 시스템을 리스크에 기반해 3개 범주, 즉 ▲공익 및 공공서비스·국방 및 안보 등에 중대 영향을 주는 전략적 전산 시스템 ▲특정 지역이나 영역에 한해 영향을 미치는 高 전산 시스템(high electronic system) ▲低 전산 시스템(low electronic system)으로 구분
- 그 중 전략적 전산 시스템 및 高 전산 시스템의 경우, '정보보호 경영 시스템 인증(Certificate of Management System of Information Protection)' 획득이 필수

표 _ 인도네시아 정보보호 정책 관련 법안 및 내용

법 안	내용
Mandate Act 36 of 1999 Article 39.	통신 분야의 보안 의무 언급
Government Regulation no. 52 of 2000 chapter 82.	통신 장애를 피하기 위해 모든 통신 네트워크, 장비, 인프라의 보안 시스템 필수 적용

법 안	내용
Law No. 11 of 2008	전자정보거래에 관한 규정 및 이와 관련한 전자서명, 지식재산권, 개인정보 보호 등을 망라
Ministerial Regulation No. 20 of 2016	전자 시스템에서의 개인정보 보호 관련 규정

[출처] ID-SIRTII

표 _ 인도네시아 전자정보법(Electonic Information Law) 위반 시 형벌 기준

위반 내용	징역 (또는 벌금)
불법 접근	징역 4~8년 (6억~8억 루피아)
전송 감청 (intercepion/wiretapping of transmission)	징역 6~10년 (8억~10억 루피아)
전자정보 또는 전자기록의 변경, 추가, 축소, 전송, 변경, 삭제, 이동, 은닉	징역 8~10년 (20억~50억 루피아)
조작, 파괴, 손상을 통해 만든 전자정보 및 전자문서를 원본인 것처럼 위장하거나 전자정보 프로세싱과 관련한 위반	징역 10~12년 (100억~120억 루피아)

[출처] Chambers

▶ 2016년 11월 인도네시아 통신정보기술부(KOMINFO)는 '전자 시스템의 개인정보보호에 관한 규정(Ministerial Regulation No. 20 of 2016)'을 공포

- 이는 ▲개인정보의 수집·처리·분석·저장·공개·이전·삭제 등 전자 시스템 내 개인정보 취급 단계별 활용 및 보호 방안 ▲불이행 시 경고처분·업무정지 등의 제재에 대해 명시

표 _ 전자 시스템의 개인정보 보호에 관한 규정 주요 내용

구분	주요 내용
수집	• 사전에 정한 특정 목적에 한해 개인정보 수집 가능 • 정보 소유자에게서 수집된 개인정보의 기밀 여부를 구체적으로 명시하고, 개인정보의 변경/추가/업데이트가 가능한 옵션을 제공 • 수집된 개인정보는 정확성 보장을 위해 검증이 필수 • 전자시스템 운영자는 상호운용성과 호환성 확보 및 적법한 소프트웨어 활용이 의무
처리 및 분석	• 개인정보 처리 및 분석은 공개된 범위로 제한하되 소유자의 동의를 기반으로만 가능 • 처리 및 분석된 개인정보는 정확성을 보장을 위해 검증이 필수

구분	주요 내용
저장	• 저장된 개인정보는 정확성 보장을 위해 검증이 필수 • 저장된 개인정보는 반드시 암호화된 데이터어야 할 것(최소 요구조건은 미명시) • 저장된 개인정보의 최소 보존 기간은 5년(명시된 경우는 제외) • 공공서비스 관련 전자 시스템 운영자는 자체 데이터 센터 및 재해복구센터를 구축
표시, 공개, 이전, 배포 및 접근 권한 제공	• 개인정보의 표시/공개/이전/배포/접근 권한 제공은 공개된 범위로 제한하되, 소유자의 동의가 필수 • 이러한 과정에 활용되는 개인정보는 정확성 보장을 위해 검증이 필수 • 데이터의 해외 이전은 통신정보기술부와의 조정 하에 진행 • 법집행기관의 유효한 요청에 근거한 법 집행 목적의 개인정보 접근권 제공이 가능
삭제	• 데이터 보유 기간 만료, 혹은 소유자의 요청이 있을 경우만 개인정보 삭제 가능 • 개인정보 삭제 시 정보의 소유자가 해당 개인정보 및 동의를 다시 제공하지 않는 한, 전자 시스템 상에 다시 표시될 수 없도록 전자적 및 비전자적으로 조치 필수
기타	• 그밖에 동의, 시스템 인증, 데이터 유출, 잊혀질 권리 등에 관한 내용 포함

▶ 현재 인도네시아에는 통신법 'Law No 36 of 1999', 의료행위 관련법 'Law No 29 of 2004), 전자정보 및 거래법 'Law No. 11 of 2008' 등 다수의 개인정보보호 규정들이 있지만 구체성이 부족한 실정

- 예를 들어, 통신 부문의 개인정보 관련법 'Law No 36 of 1999'의 제40조는 텔레콤 사업자에게 네트워크를 통해 전송된 가입자의 정보에 대해 비밀 유지를 요구하고 있지만, ▲현재까지 '텍스트 메시지'에 대한 권리 및 의무에 대한 세부 규정은 부재 ▲개인정보 보호를 위해 데이터 주체가 취할 수 있는 '추적금지' 고려사항이 미포함 ▲영상・텔레비전 등과 관련해 각각의 특별 조항을 마련하지 않고 그 대신 '전자문서'로 일괄 취급하는 등 구체성이 결여

주요 전략 및 정책

▶ 인도네시아의 사이버보안 정책은 2007년 수립된 인터넷 프로토콜 기반 통신 네트워크 애플리케이션 보안 법령인 'Regulation No. 26/PER/M.KOMINFO/5/2007'이 그 시초이며, 이는 네트워크 및 인터넷 보안 모니터링 기관 'ID-SIRTII/CC' 설립의 기초

- 그러나 정보보호를 위한 체계적 법령의 부재 등, 정보보호 정책은 전반적으로 미흡
- 정부는 정부 기관의 방화벽 강화, 모니터링, 향후 공격 방지를 위해 IT 모니터링 팀을 구축하는 한편, 핵심기반시설 보호(CIP) 강화, 국제 협력 강화, 신규 보안시스템 도입 등을 추진 중

▶ 2015년 5월 국가개발계획부 기술평가·적용처((BAPPENAS)는 '인도네시아 브로드밴드 플랜-사이버보안 전략'을 발표

- 주요 목표는 ▲사이버 범죄로부터 국가 ICT 인프라 보호 ▲브로드밴드 경제 활성화를 위한 연결성 인프라(Connectivity Infrastructure)와 관련해 투자자들로부터의 신뢰 획득 등

▶ 현 정부는 정보보호 및 사이버보안을 주요 정책과제로 선정했으며 '통신정보기술부(KOMINFO) 전략계획(2015-2019)'를 통해 그 의지를 확인

- 동 전략계획의 4대 우선순위는 ▲광대역 연결 ▲디지털화 ▲인터넷 거버넌스 ▲정부 PR

표 _ 통신정보기술부 전략계획(2015-2019)의 4개 우선순위

4대 우선 순위	주요 내용
광대역 연결	• 4G 서비스 포함한 광대역 인프라 개발 - 무선 주파수 스펙트럼 자원 정리 - 인도네시아의 위성 궤도의 연속성 유지를 통한 자국의 재산 및 통제권 유지 - 인도네시아 497개 지역 및 도시의 연결을 위해 국가 광섬유 백본 네트워크 (Palapa Ring) 배포 • 통신산업의 효율성 제고 - 통신 산업의 효율성을 위해 사업자 간 통합 장려 - 통신 인프라 개발비를 줄이기 위해 수동 공유 인프라(패시브 인프라 공유) 구축 • 통신도구 및 장치의 국산 콘텐츠 장려
디지털화	• 아날로그 TV에서 디지털로의 전환 프로세스의 속도 제고 • 디지털 TV로의 신속한 전환을 위한 정책 및 규정 개발
인터넷 거버넌스	• 정보 보안 개선 및 인터넷 거버넌스 최적화 - 전자 시스템 인증 구현 - 음전하 사이트 처리를 위한 패널 형성 - 전자 등록 시스템 제공 - PSrE 및 LSK 캔디 작성 및 비준 • 전자상거래 성장 촉진 - 5-10개년 전자 상거래 로드맵 확립 - 전자 상거래 확산 데이터 수집 • 불법적 콘텐츠 감소를 위한 DNS 구현 • 전자 정부 서비스 통합 - 전자정부 구현을 위한 마스터 플랜 개발
정부 PR	• 통신네트워크 기관 설립 • 정부 홍보(GPR) 규정 이행 준비 및 모니터링

[출처] KOMINFO

▶ 통신정보기술부(KOMINFO)는 'Born to Protect' 운영하고 있으며, 이는 매년 개최되는 국가 사이버보안 프로젝트로서 사이버보안 인력 배출이 주 목적

- 주관은 보안기업 PTXynexis이 맡고 있으며, 통신정보기술부를 비롯해 정보보안인증업체 EC-Council, RSA Security, Univerisity of Gunadarma 등이 지원
- 동 프로젝트의 진행 방식은, 자카르타(Jakarta), 메단(Medan), 반둥(Bandung) 등 10개 도시에서 보안 인재 1만여 명 모집→준결승전을 거쳐 1,000명 선별→'캡처더프래그(capture the flag)' 챌린지에서 최종 상위 100명을 선발→2주간의 '디지털 캠프'를 통해 사이버보안 전문교육 제공
- 준결승 통과자 1,000명에게 Certified Secure Computer User (C|SCU) 프로그램의 바우처, 최종 선발자 100명에게는 ANSI가 승인하는 Certified Network Defender (C|ND) 프로그램의 바우처를 수여
- 한편, KOMINFO가 2019년 1월에 발표한 바에 따르면, 인도네시아 전역의 기업, 공공기관, 중소기업에 필요한 사이버보안 인력은 연간 60만 명

▶ 2019년 9월 인도네시아 정부는 인터넷 프로토콜(IP) 상호연결 구현을 위한 로드맵을 발표

- 상호 연결 IP 기반 구현을 위한 로드맵에는 ▲목표 ▲IP기반 상호연결의 정의 및 모델 ▲기술적 표준(표준 코딩, 보안 기준, 표준 충전 및 결제) ▲상호연결 충전 및 청구 모델 ▲상호연결 벤치마크 ▲지역사회 준비도(광대역 보급, 광대역 서비스의 속도 및 요금) ▲상호연결 구현 계획 및 실행 단계 ▲관련 규제 ▲상호연결의 배치 등의 내용이 포함
- 2025년 4G/5G 액세스 네트워크가 전체 운영자 액세스 네트워크의 60% 이상에 도달하게 되면 모든 IP 기반의 상호연결 작업이 실행될 것으로 전망

2) 담당기관

▶ 국가사이버암호청(BSSN: Badan Siber dan Sandi Negara)

- 대통령령(Presidential Regulation No. 53 of 2017)에 기반한 것으로 2018년 1월 3일부로 설립
- 기존의 국방부 산하 국가암호청(LSN)을 모태로 통신정보기술부(KOMINFO)의 정보보호과 및 침해대응센터(Id-SITII/CC)를 통합
- 동 기관은 국가 사이버보안의 컨트롤타워로서, ▲정책 개발 ▲침해사고 탐지·대응 ▲유관기관과의 협력 및 조정 ▲사이버보안 마스터플랜 및 중장기 로드맵 등, 국가 전략·정책 수립 및 집행을 총괄 ▲사이버 공격에 대한 탐지·복구·예방·완화 조치를 수행 ▲내부 감독관을 통해 기술 규정을 수립·감독·평가 ▲소셜미디어 활동 모니터링를 통한 반국가적 이데올로기의 확산 억제
- 한편 BSSN은 사이버 공격에 취약한 10개 국가 핵심 인프라로 ▲사법기관 ▲에너지 및 광물자원 ▲금융 및 뱅킹 ▲보건 ▲ICT ▲농업 ▲국방 ▲비상대응(emergency response) ▲정수처리를 지정

▶ 통신정보기술부(KOMINFO)

- 정보통신서비스 보안을 위한 정책 수립, 제도 도입, 인력양성 등을 총괄
- 정부 네트워크 및 시스템 보안을 위한 Gov-CSIRT를 내부적으로 운영하고 있으나, 전자정부 수준이 낮고 소수의 인력만 배치된 까닭에 실질적인 기능 수행에는 한계가 뚜렷
- 대표적인 산하 조직으로는 민간 분야 네트워크 침해사고대응을 위한 Id-SIRTII/CC
- KOICA 자금으로 PKI 구축 및 네트워크 보안관제 시스템 개발을 추진 중
- 주요 정보통신기반시설 보호(CIIP)를 위한 인증, 심사 등 관련 제도 도입에도 관심을 표명

▶ 정치법률안보조정부(Kemenko Polhukam)

- 국가적 차원에서 사이버보안의 중요성이 강조됨에 따라, 대통령 지시로 국가 사이버보안 전담조직 설립을 위한 임시기구(DCN)를 부처 내 직할로 설립('2014년)
  ※ DK2ICN(Desk Ketahanan dan Keamanan Informasi Cyber Nasional)에서 DCN(Desk Cyberspace Nasional)로 명칭 변경('16.6월)
- 사이버보안에 직접적으로 관여하지는 않으나 통신정보기술부, 행정개혁부, 국방부, 검·경 등에 대한 조정 역할을 위임받았으며, 이로써 유관부처 및 기관에 대한 영향력을 행사

▶ 국가사이버위원회(Committee on National Security Systems, CNSS)

- 국가 전체의 사이버보안 체계 구축을 위한 법제 정비 및 마스터플랜 수립 등을 담당
- 한국이 주도하여 발족한 글로벌 사이버보안 협력 네트워크(CAMP) 가입 등, 활발한 국제협력 활동을 펼치고 있으며 사이버보안 전담조직으로의 독립 및 역량 강화에 주력

▶ Id-SIRTII/CC

- 통신정보기술부가 2007년 5월 4일 네트워크 및 인터넷 보안 모니터링 기관 'ID-SIRTII'를 설립
- 설립의 법적 근거는 2007년 제정된 인터넷 프로토콜 기반 통신 네트워크 애플리케이션 보안 관련 법령인 'Regulation No. 26/PER/M.KOMINFO/5/2007'
- 동 법령의 주요 내용은 ▲(산하조직) 통신정보기술부 산하 'ID-SIRTII'의 설립 ▲(인터넷을 이용하는 조직) 네트워크 실행 기록 파일의 보관 의무 ▲(통신 사업자) 데이터 보호 및 보안 등 모니터링 시스템 제공 의무 ▲(통신 사업자) 클럭 동기화(Clock Synchronization) 수행 의무 등
- Id-SIRTII/CC는 주요 ISP 네트워크 접속지점(NAP)에 센서 35개를 설치해 24시간 보안관제(모니터링/분석/대응)를 수행하고 있으며, 자국 내 인터넷 통신량의 50~70%를 커버
- 국가대표(National CSIRT)로서 ISP 등 사업자 및 각계 CERT에 대한 기술 지원, 조정 역할을 담당
- 그 외, 아태침해사고대응팀협의회(APCERT), 이슬람국가연합CERT협의회(OIC-CERT), 글로벌 사이버보안

협력 네트워크(CAMP) 가입 등을 통해 활발한 국제협력 활동을 수행

▶ ID-CERT(INDONESIA COMPUTER EMERGENCY RESPONSE TEAM)

• 1998년 설립된 ID-CERT는 인도네시아 민간 분야의 사이버 보안 커뮤니티로, ▲사이버 공격 및 위협에 대응 ▲자국 네트워크의 사이버 공격에 현황 보고서를 작성 및 배포 ▲국가 보안 시스템 개선에 대한 가이드라인 제공 ▲보안 취약성 개선 보고서 작성 ▲멀웨어 관련 보안 가이드라인 제공 등에 역점

표 _ 인도네시아 내 CSIRT 현황

National	• Id-SIRTII/CC (KOMINFO 산하기관)
Government	• 중앙정부 : Gov-CSIRT (KOMINFO 내부조직) • 지방정부 : 자바(Jawa), 자와티무르(Jatim), 족자카르타(Yogya) 지역별 CSIRT • 군(軍) : Mil-CSIRT
Community	• ACAD-CSIRT : 40개 대학의 CSIRT 연합 • ID-CERT : 민간 분야 CERT 연합
Private	• 주요 사업자(ISP, 통신사, 금융사 등) 별로 존재

[출처] 각종 자료를 토대로 KISA 재구성

▶ CISSReC (Communication & Information System Security Research Center)

• 2015년 설립된 비영리단체로 정보통신시스템 보안 관련 대중의 인식 제고를 위한 연구를 수행

• 민간의 ICT 보안 및 암호 분야 전문가들이 참여하고 있으며 ▲정보통신시스템의 보안 강화 및 암호 관련 각종 조사 및 학문적 연구 활동을 수행 ▲일반인 대상의 보안 교육 및 캠페인 실시

3) 규제 및 인증제도

▶ 인도네시아 시장은 국제보안인증인 ISO 27001:2013을 채택하고 있으며, 이를 기반으로 SNI ISO/EIC 27001:2009라는 명칭으로 보안 관리를 위한 인도네시아 국가표준을 지정

• 인도네시아 기술표준청(BSN)은 ISO 27001과 동일한 SNI ISO/IEC 27001 표준을 일반 기업, 정부, 비영리조직 등 모든 형태의 조직에 공통으로 적용

▶ 인도네시아는 보안 기술을 위해 ISO/IEC 15408로 알려진 공통 기준을 채택

- 즉, 소프트웨어를 포함한 IT 제품의 보안 속성 평가에 ISO/IEC 15408-1/2/3:2014를 활용

▶ 인도네시아 시장은 또한 정보보안 네트워크 등의 제품에 대한 CC 인증도 인정
- 인도네시아 시장에 진출한 글로벌 기업들은 대부분 국제 CC 인증을 취득하여 시장에 해당 제품의 공신력과 기술력을 입증
- CC(Common Criteria) 인증은 한국·미국·영국·캐나다·호주 등 세계 20개국에서 사용하는 정보보호 제품의 평가 기준으로, 최고 등급은 EAL 5등급임
- 국내의 보안 업체는 CC 인증 취득을 통해 인도네시아를 비롯한 동남아 시장에 진입하면서 공신력 및 기술력을 입증하는 마케팅 전략으로 활용

4) 최근 정책 동향 및 이슈

▶ 통신정보기술부(KOMINFO)는 28개 대학・22개 과학기술학교・5개 글로벌 기업(CISCO, AWS, Google, Dicoding, Microsoft)과 협력을 통해 디지털 인재를 양성하는 4개 아카데미 운영 계획을 발표(2019.1)[78]
- 각 아카데미별 역점 분야는 ▲Fresh Graduate Academy는 사이버보안, 빅데이터 분석, AI, 클라우드 컴퓨팅, IoT, 머신러닝 ▲Vocational School Graduate Academy는 네트워크 관리자, 웹 개발자, 모바일 프로그래머, 그래픽 디자인, 중급 애니메이터 ▲Coding Teacher Academy는 코딩 강사 양성 ▲Online Academy는 사이버 운용 및 CCNA 보안, AI, 프로그래밍 운용, 디지털 기술/정책, 빅데이터 등

▶ 인도네시아 통신정보기술부(KOMINFO), 개인정보보호법 초안 완료(2019.5)[79]
- 동 개인정보보호법 초안은 2016년 12월 공포된 '전자시스템 개인정보 보호 규정'에 기반
- KOMINFO 산하의 통신감독청(BRTI)은 개인정보 매매를 형벌 및 벌금이 부과되는 위법 행위로 규정
- 위 두 기관은 전자상거래 및 소셜미디어 플랫폼 공급자에게 개인정보 거래 관련 홍보물・ 광고 등을 내릴 것을 요구
- 동 법안은 종교・헬스・육체 및 정신 질환・性 질환・개인 금융 등 특별 보호를 요하는 민감정보 및 개인정보를 다루고 있으며, 개인 데이터의 보안 제고와 데이터 조작 방지에 역점

▶ 사이버보안 핵심 이슈 해결을 위한 'Indonesia Security Summit' 개최(2019.9)[80]

---

78 KISA, "정보보호 해외진출 전략거점 1월 주요동향", 2019.2.12
79 Tempo.com, "Kominfo Preps Draft Bill on Personal Data Protection, 2019.5.17
80 ITSP Magazine, "Accelerating Cyber Security For A Safer Indonesia | ISS 2019", 2019.9.4

- 9월 3-4일 자카르타에서 '보다 안전한 인도네시아를 위한 사이버 보안 가속화'라는 주제로 개최
- 이는 정부 인사, CISO, CIO, CTO, 포렌식 전문가, 사이버 법률가 등을 위한 지식 공유 플랫폼
- 2019년은 ▲인도네시아 사이버 범죄 현황 ▲사기·위반 방지를 위한 최신 기술에 역점

▶ 9월, 인도네시아 최초의 사이버보안법 공표 예정(2019.9)[81]

- 인터넷 사용자 수 세계 5위 인도네시아에서 2019년 5월 발생한 사이버공격만 190만여 건으로, 사이버위협에 대한 기민한 대처를 위해 사이버보안법의 통과가 절실한 상황
- 동 법안에는 사이버암호청(BSSN)을 정부, 군·경 등 유관기관과의 협력을 총괄하는 기관으로 지정
- 기존에 수립된 '전자정보 및 거래법(Law on Electronic Information and Transactions)'과 '전자시스템 및 거래에 대한 정부 규정(Government Regulation on the Implementation of Electronic System and Transaction)'은 사이버 위협에 대해서는 다루지 않음
- 법안 통과의 시급성에도 불구하고, ▲사이버암호청이 여타 법 집행기관 위에 군림할 가능성 ▲과다한 권한 부여 ▲사이버암호청의 업무 모니터링에 대한 상세 방안 부재 등이 논란을 야기
- 비평가들은 정부가 동 법에 기반해 반정부 콘텐츠 감시 및 언론의 자유를 탄압할 가능성을 제기

5) 정보보호 스타트업 관련 정책 동향

▶ 정부는 2020년까지 1,000개 스타트업을 창조하겠다는 이니셔티브를 전개

- 그런 가운데 Alibaba Cloud가 2018년 초 데이터센터 1호점에 이어 2호점을 개소했으며, Google Cloud와 Amazon AWS도 인도네시아로 클라우드 사업 확장을 발표
- 이로써 정부의 스타트업 이니셔티브가 더욱 탄력을 받을 것으로 전망

81 The Conversation, "Indonesia needs to fix 'authoritarian' clauses in bill on cyber security before passing it into law". 2019.9.4.

융합보안시장 및 정책 동향

1) 융합보안시장 동향

스마트시티

▶ '자카르트 스마트시티 이니셔티브'는 2014년 12월에 출범했으며 스마트환경, 스마트 모빌리티, 스마트 경제, 스마트 인물, 스마트 정부, 스마트 생활 등 6개 핵심 요소를 포함

- 자카르타의 스마트시티 구축 과정을 보면, 기본 데이터분석을 위한 서버 구현->로컬 스타트업 생태계와 협력해 모든 사람이 휴대 전화 및 인터넷으로 다운로드해 사용 가능한 공개 애플리케이션 개발->시민 불만 사항을 실시간 모니터링 할 수 있는 관제센터 및 모니터링 시스템 구축->시민 불만 처리 소요 시간 등을 평가->분석 지원을 위한 빅데이터 분석 플랫폼 구현 및 개발의 순

▶ 위 애플리케이션과 관련해, 2016년 설립된 스타트업 Qlue가 자체 앱을 개발해 인도네시아 최초로 '스마트 시티' 개념 구현에 기여

- 이로써 자카르타 주민은 Qlue 플랫폼을 통해 정부와 직접 소통하게 되었으며, ▲2018년 한 해 동안 Qlue 앱을 통해 접수된 불만은 총 10만여 건 ▲후속 조치가 취해진 비율은 82%

핀테크

▶ Frost & Sullivan에 따르면 2017년 인도네시아의 핀테크 시장의 규모가 2억 3,770만 달러이며, 그 후 연평균 39.54%씩 성장해 2022년에는 12억5천만 달러에 이를 것으로 전망

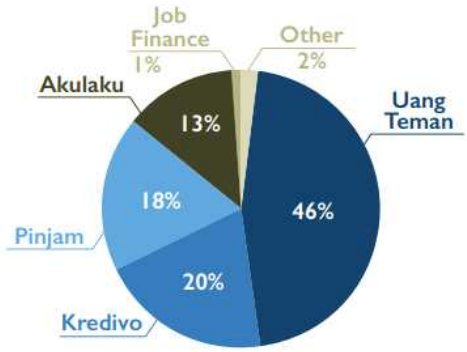
- International Finance Corporation의 2014년 조사에 의하며, 인도네시아의 전체 마이크로 중소기업 중 ▲신용서비스에 대한 접근성 보유 및 지속가능한 규모로의 성장 가능성을 갖춘 기업은 12%에 불과 ▲은행 등 금융기관으로부터의 자금 지원을 못 받는 기업은 45%
- Palapa Ring 프로젝트로 인터넷 보급률이 증대되면 핀테크 서비스 수요도 동반 상승할 것으로 예측
- 특히 디지털 지불 결제 및 P2P(Peer-to-Peer) 대출 서비스 영역이 인도네시아의 개인 및 기업에게 금융 상품 및 서비스에 대한 접근성을 제고할 것으로 기대
- 2018년 기준 인도네시아 중앙은행에 등록된 핀테크 기업은 PT Toko Pandai Nusantara(Toko Pandai), PT Privy Identitas Digital(PrivyID) 등 총 49개
- 한편 Statista의 데이터에 의하면, 2018년 기준 인도네시아의 핀테크 시장은 지불결제 시스템(38%),

대출(31%), 개인재산 관리(8%), 상품비교97%), 인슈어테크(6%), 크라우드펀딩(4%) 등의 순

▶ 핀테크 부문 중 P2P 대출 서비스는 상대적으로 새로운 영역이며, 따라서 시장 주자들 대부분은 스타트업으로서 2019년에는 그 수가 39% 증가될 것으로 전망

• 업체별 시장 점유율은 Uang Teman이 46%로 1위이며 그 뒤를 이어 Kredivo, Pinjam, Akulaku의 순

그림 _ 인도네시아 P2P 대출 시장 업체별 점유율(2016년 기준)

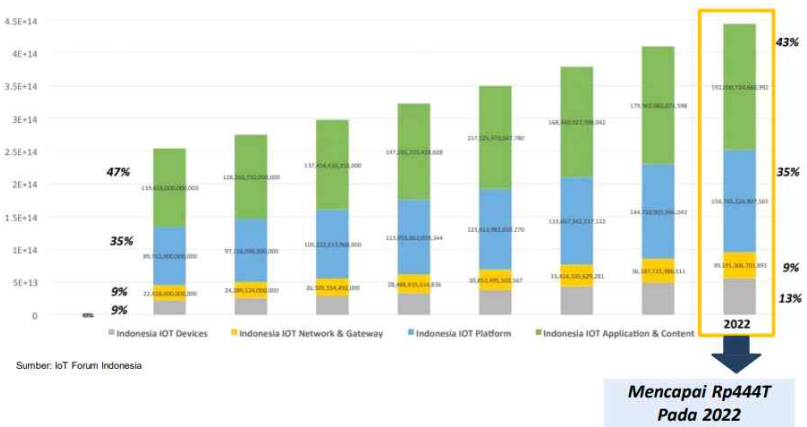


[출처] Frost & Sullivan(2018)

사물인터넷(IoT)

▶ 인도네시아의 2022년 IoT 시장 규모는 444조 루피아에 이를 것으로 전망

그림 _ 인도네시아 IoT 시장 규모 전망(2015-2022)



[출처] IoT Forum Indonesia

- 부문별 점유율은 IoT 애플리케이션 및 콘텐츠 43%, IoT 플랫폼 35%, IoT 장비 13%, IoT 네트워크 및 게이트웨이 9%의 순
- 2018년 말 기준 IoT를 구현하거나 IoT 관련 투자를 한 기업은 250여 개

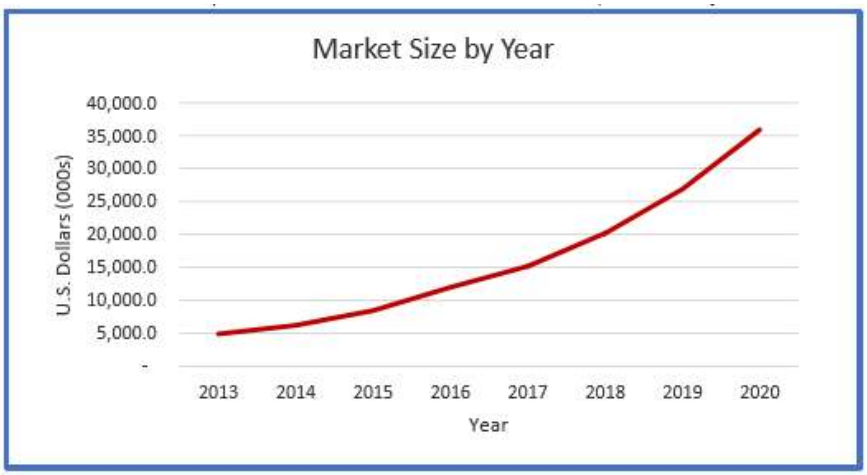
인지보안

▶ 인도네시아의 인지보안(cognitive security) 장비 시장은 2019년 2,690만 달러에서 2020년 3,590만 달러로 33.6% 성장할 것으로 예측

- 그 후 2020부터는 연평균 60.7%씩 성장해 2025년에는 14,480만 달러에 이를 것으로 전망

그림 _ 인도네시아 인지보안 시장 전망(2013-2020)

(단위: 천 달러)



[출처] Barnes Reports(2019)

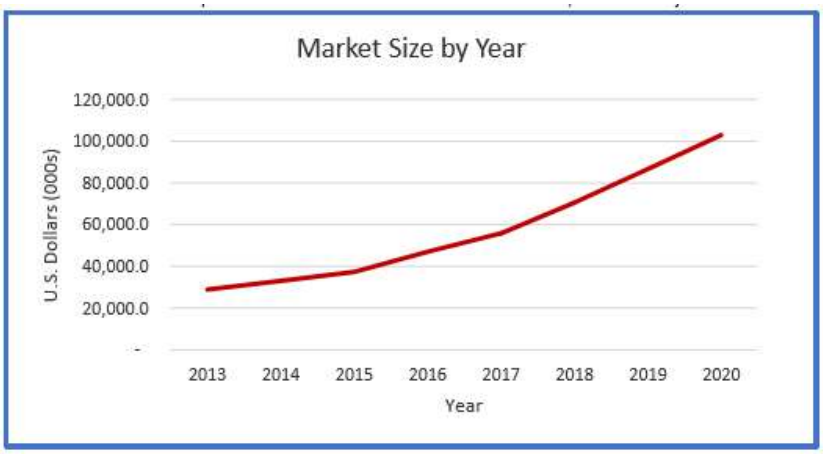
자동차 사이버보안

▶ 인도네시아의 자동차 사이버보안 장비 시장은 2019년 8,670만 달러에서 2020년 18.6% 성장해 1억 290만 달러에 이를 것으로 예측

- 그 후 2020년부터는 연평균 27.9%씩 증가해 2025년에는 2억 4,670만 달러에 이를 것으로 전망

그림 _ 인도네시아 자동차 사이버보안 시장 전망(2013-2020)

(단위: 천 달러)



[출처] Barnes Reports(2019)

블록체인(가상화폐 포함)

▶ 인도네시아 농업에 블록체인 기술을 접목하여 작물 환경 개선 및 빈농 타개[82]

- 국가의 빈곤층 대부분을 차지하는 농민층에서 활발하게 이용 중으로, HARA社의 블록체인 플랫폼을 활용하여 '데이터 민주화(democratize data)' 환경 구축
- 즉, HARA에 데이터를 제공하는 사람들(주로 농촌의 청년층)이 ▲농부의 신원 ▲재배 품목 ▲농법 ▲비료 ▲경작지 모양·면적 등의 정보를 자발적으로 HARA의 스마트폰 앱에 등록하면 데이터 제공에 따른 보상을 받고, 이 데이터를 은행, 보험회사, 비료회사 등의 기업들이 사들여 자신들의 사업 확장에 활용하며, 농부는 플랫폼에서 HARA가 제공하는 금융상품을 기존 고리의 사채 대비 저리(低利)로 이용하여 빈곤한 경제 상황에 활용

2) 융합보안정책 동향

스마트시티

82 https://news.chosun.com/site/data/html_dir/2019/08/12/2019081201712.html

▶ 통신정보기술부 및 국가개발계획부(BAPPENAS)는 2019년까지 스마트시티 100여 곳을 개발하기 위한 '100 Smart City Movement' 이니셔티브를 출범

- 자카르타, 수라바야, 반둥이 1세대 스마트도시들이며, ▲반둥은 정부 및 관련 기관의 데이터를 통합 ▲수라바야는 교통문제 해결을 위해 감시 카메라에 기반해 교통 상황을 모니터링 ▲스마트시티 생태계의 핵심 도시 자카르타는 도시 내 도로 전역에 CCTV를 설치 외 스마트 조명·스마트 주차·폐기물 관리·커넥티드 맨홀 등 다양한 프로젝트를 탐색 중

핀테크

▶ 2018년 9월 인도네시아 금융감독청(OJK)은 혁신적이고 신속하고 저렴한 금융서비스 지원, 금융 포용성 및 투자 증대를 위해 핀테크 기업에 대한 금융 혁신 규제 'No 13/POJK.02/2018'을 발표

- 주 내용으로는 ▲(규제 샌드박스 절차) 핀테크 업체는 OJK에 등록을 필해야 하며 규제 샌드박스 테스트 통과 후 그 결과에 따라 해당 시스템의 권장 여부를 결정 ▲(포함 및 교육) 사용자에게 정보 제공의 의무 ▲(사용자 안전성) 시스템 투명성, 공정한 서비스, 개인정보보호 등 안전성 제공의 의무 ▲(Fintech Indonesia Center) 인도네시아 핀테크센터를 구축해 규제 샌드박스 프로세스 지원 ▲(자금세탁 및 테러리즘) 자금세탁 및 테러리즘 지원 금지

그림 _ 인도네시아 핀테크 관련 주요 법규

법규	주요 내용
인도네시아 중앙은행법 PBI No. 18/40/2016	• 지불거래처리 기관 관련 규정 • 주요 소관 업무는 거래전 단계, 승인, 청산, 정산, 사후 처리
인도네시아 중앙은행법 PBI No. 19/8/PBI/2017	• 국가 지불결제 시스템 관련 규정 • 기술 발전에 따른 전자상거래 증대로 안전성, 효과성, 신뢰성을 갖춘 국가 통합 지불 결제 시스템 실현을 목적으로 제정
인도네시아 중앙은행법 PBI No. 19/12/PBI/2017	• 핀테크 조직에 대한 규정 • 핀테크 사업자의 정의, 활동 범위, 중앙은행의 승인 획득의 의무, 규제 샌드박스에 대한 내용이 포함
인도네시아 중앙은행법 PBI No. 20/6/PBI/2018	• 전자화폐 관련 규정 • 전자화폐의 정의, 유형, 최대 예치규모, 외국인 지분율 제한 등의 내용 포함
금융감독청 OJK No 77/POJK.01/2016	• 기술 기반 펀드 대부 서비스(P2P 대출 서비스) 관련 규정 • P2P 대출 서비스 제공에 대한 규제 사항, P2P 대출업자 자격요건 등이 포함
금융감독청 OJK No 13/POJK.02/2018	• 금융 서비스 부문의 디지털 금융혁신에 대한 규정 • 디지털금융혁신(IKD, Inovasi Keuangan Digital)을 위한 핀테크 규정 • IKD의 정의 및 범위, 금융감독청 인허가 절차, 정보보안 및 데이터 보호, 규제 샌드박스 등의 내용이 포함

[출처] 인도네시아 중앙은행 등

사물인터넷(IoT)

▶ IDC의 조사에 따르면, 2019년까지 인도네시아 지방 정부의 20%가 도로, 가로등, 교통 신호등의 인프라에 IoT를 구현할 예정[83]

블록체인(가상화폐 포함)

▶ 블록체인 기술을 연구하는 국가적 전담팀을 구성, 국가 산업의 전반적인 데이터 관리 문제 극복 도모[84][85]

- 인도네시아는 데이터 기록 및 관리에 있어 전문적인 지식과 자원이 부족하여 정확한 기록을 일정하게 유지하는 데에 어려움을 겪어 왔음
- 그러나 블록체인은 중앙 집중식이 아닌 분산형 네트워크로부터 지속적으로 업데이트되는 정보를 공유하는 형태로서, 정부의 데이터 처리 및 세금의 투명한 사용에 획기적인 발전 가능성을 제공
- 예컨대, 농촌에 주어지는 정부 보조금은 전년도 수확량을 기준으로 책정되는데, 다수의 수령자가 매년 수확량의 과장을 통하여 과다하게 보조금을 수령하는 경우가 발생해 옴
- 블록체인 기술을 활용하게 되면 수확량 기록의 정확도가 높아지며 보조금 수령자의 정보 확인도 수월해지게 되므로, 불필요한 보조금의 지급을 줄여 국가 재정 지출의 정확성 및 투명성을 높일 수 있음

---

83 ASMAG, Smart IoT Indonesia 2019 ready to unveil latest IoT trends, 2018.12.19

84 https://www.reuters.com/article/us-indonesia-blockchain/indonesia-looks-to-blockchain-to-fix-its-dodgy-data-challenges-idUSKBN1I503R

85 http://www.dcoinnews.net/%EC%9D%B8%EB%8F%84%EB%84%A4%EC%8B%9C%EC%95%84-%EA%B3%B5%EA%B3%B5-%EB%B0%8F-%EB%AF%BC%EA%B0%84-%EB%B6%80%EB%AC%B8%EC%97%90%EC%84%9C-%EB%B8%94%EB%A1%9D%EC%B2%B4%EC%9D%B8-%EC%9A%A9%EB%8F%84-%EC%97%B0/

라. 베트남

'18년 GDP(십억달러)	244.95
'18년 인구수(천명)	95,540

■ ITU 글로벌 사이버보안 지수(Global Cybersecurity Index, GCI)

· 베트남의 사이버보안 지수는 한국보다 낮은 수준이며, 중상위권 그룹에 속함

국가명	2018		2017		전년대비 증감	
	지수	순위	지수	순위	지수	순위
베트남	0.693	50	0.245	101	+0.448	+51
대한민국	0.873	15	0.782	13	+0.091	-2

■ ICT 관련 주요 지수

· 베트남의 전반적인 ICT 발전 수준은 중위권 수준을 유지하고 있음

지표명	베트남		한국	
	점수	순위	점수	순위
IMD 국가경쟁력지수(2019)	-	-	-	28
IMD 디지털경쟁력지수(2019)	-	-	-	10
UNCTAD 전자상거래지수(2019)	61.1	64	89.4	19
ITU 글로벌 사이버보안 지수(GCI 2018)	0.693	50	0.873	15
UN 전자정부 지수(2018)	0.593	88	0.901	3

■ ICT 관련 주요 통계 (ITU, 2018년 말 기준)

· 베트남의 유선통신 이용 및 보급률은 10%대 수준이며, 이동통신(ICT) 보급률 150%에 근접

항목	베트남		한국	
	가입자수(천 명)	보급률(%)	가입자수(천 명)	보급률(%)
유선전화	14,296	14.96	25,907	50.63
유선브로드밴드	12,994	13.60	21,286	41.60
이동통신	140,639	147.20	66,356	129.67
인터넷 이용률	70.35%		95.90%	

정보보호 산업 개요

1) 보안 환경

▶ 정부기관에서 10,000개 이상의 사이버 보안 취약점 발견(2019.9)[86]

- IT & Network Security Centre에 따르면 10,000개 이상의 사이버보안 취약점이 2013년 이후 정부기관에서 발견되었음
- 총 100개의 멀웨어에 도메인 이름 '.gov' 가 포함되었고, 정부기관의 2,100개 이상 이메일 계정이 공격당함
- Kaspersky Lab의 보고서는 2018년 말 기준 1억 건 이상의 온라인 공격과 4억 건 이상의 오프라인 사건으로, 베트남이 동남아시아에서 가장 많은 온라인 및 오프라인 공격을 당한 것으로 분석
- 한편, Spanhaus Project에 따르면, 베트남이 세계에서 최악의 봇넷 국가 중 3위로 905,000개 이상의 스팸봇이 발견되었다고 발표
- 컴퓨터 바이러스는 베트남 사용자에게 15조 동(VND)(약 6억 4,000만 달러)의 손실을 일으켰음
- Bkav회사의 통계에 따르면 베트남에서 기관과 기업의 60% 이상이 암호 화폐 채굴 악성 코드에 감염되었음
- 전문가들은 낮은 수준의 네트워크 보안 정책과 안전하지 않은 장비 및 IT 서비스의 사용으로 사이버 공격이 발생했다고 언급하며, 또한 해커가 IT 인프라를 마비시키기 위해 고급 위협을 사용할 가능성이 높아짐에 따라 사이버 공격이 점점 더 위험해지고 감지하기가 더욱 어려워짐
- IT & Network Security Centre의 소장은 AI 기반 멀웨어 공격의 새로운 트렌드로 전자상거래 사이트, 은행 및 금융 부문의 사용자 개인 정보 유출에 대해 우려를 표명

▶ 베트남 정보통신부는 2019년 상반기에 약 3,159건의 사이버 공격이 발생했으며, 이는 전년 대비 45.9%가 감소한 결과임

- 사이버 공격 중 피싱공격(1,556건), 홈페이지 위변조(968건), 악성코드(635건)이 발생하였음
- 정보통신부는 2018년 악성코드 제거 및 관련 교육을 통해 사이버 보안 및 안전성이 향상되었다고 밝혔으나, 지난 2019년 5월~6월 사이에 악성코드에 감염된 PC 수가 137만 개를 기록하며 직전 4월의 85만 개보다 증가함
- 정부기관의 경우 2018년 같은 기간에 비해 2배 이상의 악성코드 공격이 증가해 상대적으로 정보보호에 대한 대응이 부족한 것으로 나타남

---

86 VNISA, Over 10,000 cyber-security vulnerabilities found in government agencies, 2019.9.30.

▶ MS, IDC가 2019년 상반기에 발간한 최근 보고서에 따르면 베트남 소비자 중 32%만이 디지털 서비스 기업들의 개인정보보호 방식을 신뢰하는 것으로 나타남

- 현재 베트남은 정부기관, 은행 및 소매업체 등에서 디지털화가 빠르게 진행되고 있어 소비자들의 사이버범죄와 개인정보보호에 대한 위험 인식도 높아지고 있음
- 그러나, 대부분의 소비자들은 디지털 정보를 취급하는 기업들을 신뢰하지 못하고 있는 실정이며 관련 설문조사에서 사이버보안(90%)과 개인정보보호(89%)가 디지털 서비스 이용에 중요한 요소라고 응답함
- 동 설문조사에서 응답자의 73%가 가격이 높더라도 신뢰성 높은 디지털 서비스를 이용 및 추천하겠다고 응답함

▶ ITU가 2019년 3월 발표한 'Global Cybersecurity Index (GCI) 2018'에 따르면 베트남의 사이버보안 지수는 0.693으로 전 세계 순위 50위, 아시아-태평양지역에서 11위를 차지한 것으로 나타났으며, 2017년 전 세계 순위 100위에 대비 대폭 상승한 순위임

- 당초 베트남은 70위권을 목표로 했으나, GCI의 5개 평가 분야에서 고른 성적을 나타내며 초과 실적을 달성하였으며, 베트남 정보통신부는 2019년에는 20위권으로 도약하기 위해 '지속적인 솔루션'을 운영 중이라고 밝힘

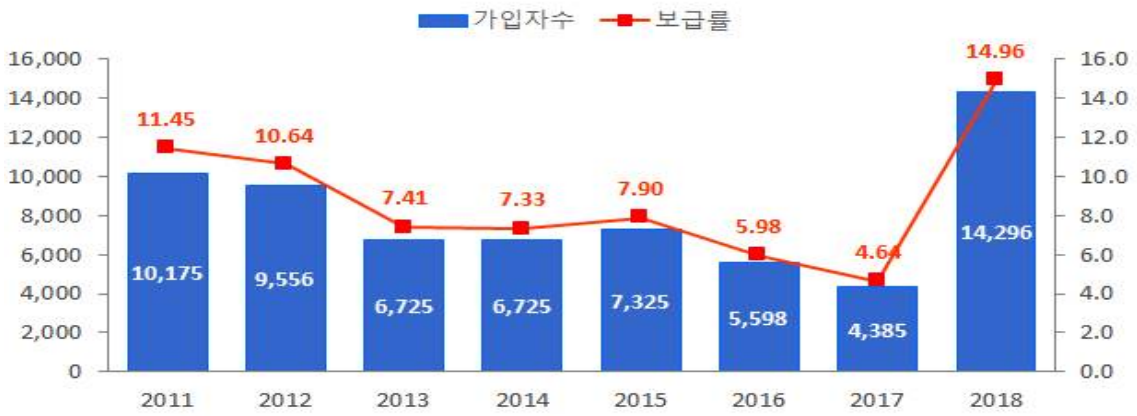
2) 인터넷 및 통신 환경

▶ 유선통신

- ITU에 의하면 2018년 말 기준, 유선통신 가입회선 수는 약 1,429만 회선을 기록, 보급률은 14.96%이며, 2017년 보급률 4.64% 대비 10.33%p. 증가하였음
- 베트남의 유선 통신시장 보급률은 2009년 20%로 최고치를 기록한 후 이후 계속 감소하는 추세를 보이다가 2018년 약 15%로 상승함
- 유선 사업자로는 국영기업인 VNPT(Vietnam Post and Telecommunications Corporation), 군부 소속 기업인 Viettel, FPT Telecom, VNPT의 자회사인 VTC, 현지 IT 기업인 CMC, GTel이 있음
- 2017년 VNPT-Vinaphone은 유선 네트워크를 구리선에서 광섬유로 전환하였음

그림 _ 베트남 유선통신 가입자 수 및 보급률 추이

(단위: 천 명, %)



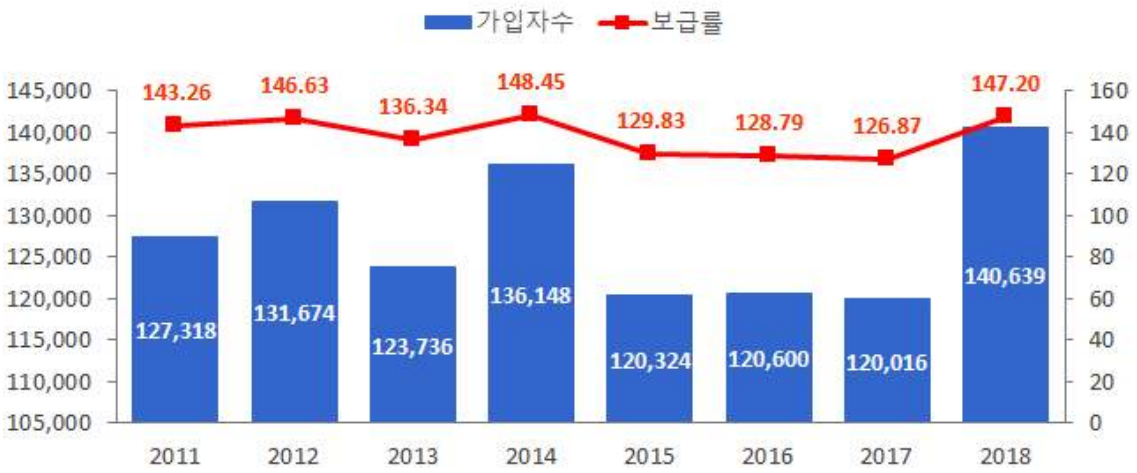
[출처] ITU Statistics DB (2019.6)

▶ 이동통신

- ITU의 자료에 의하면 2018년 기준 이동통신 가입자 수는 2017년 대비 약 17% 증가한 약 1억 4,000만 명으로 보급률은 147.2%였으며, 2014년 148.45%로 최고의 보급률을 기록
- 보급률은 2015년부터 3년간 성장이 정체되었다가 2018년 다시 소폭 상승하였지만, 이동통신 시장이 성숙하고 포화되어 시장 성장력은 제한되어 있음

그림 _ 베트남 이동통신 가입 및 보급률 추이

(단위: 천 명, %)

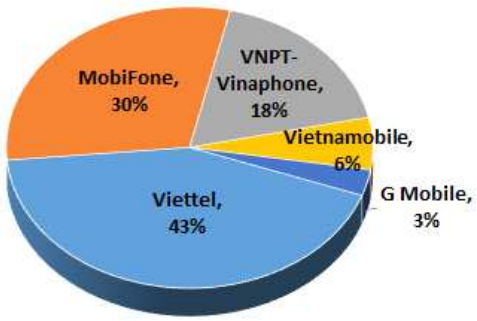


[출처] ITU Statistics DB (2019.6)

- 2018년 이동통신 시장은 Viettel(43%), MobiFone(30%), VNPT-Vinaphone(18%)가 전체 이동통신 시장의 91%를 차지하고 있으며, 이외에도 Vietnamobile가 6%, G Mobile이 3%를 차지하는 것으로 나타남

그림 _ 베트남 이동통신사별 시장 점유율(2018년 기준)

통신사	가입자 수 (백만명)	비율
Viettel	62.5	43%
MobiFone	43.0	30%
VNPT-Vinaphone	25.6	18%
Vietnamobile	9.2	6%
G Mobile	4.1	3%
전체	**144.4**	**100%**



[출처] BuddeComm (2019.5)

- 주요 모바일 사업자로는 VNPT-Vinaphone, Mobifone, Viettel, Vietnamobile, G Mobile이 있으며, 2019년 베트남 최초의 MVNO인 Itelecom(Indochina Telecom Company)가 시작되었음[87]
- 베트남 정부가 2016년까지 라이선스를 발행하지 않아 4G를 출시하는데 시간이 걸렸지만, 그 이후 2017년까지 5개 주요 이동통신 사업자 모두 4G 라이선스를 발급받았으며 2018년 초까지 4G 출시가 잘 진행되었음
- Mobifone은 2016년 다낭, 하노이, 호치민시에서 시범 LTE-A 네트워크를 시작하였고, 2016년 10월 경쟁사들과 함께 4G 라이선스를 받았으며, Mobifone은 2017년 1월 한국의 SK텔레콤과 계약을 맺어 2020년까지 전국에 LTE 네트워크를 설계 및 구축할 수 있는 솔루션을 제공받으며, 5G 및 IoT를 포함한 추가 서비스 개발에서 운영하고 있음
- Vinaphone은 Phu Quoc 섬을 시작으로 2016년 11월에 베트남 최초의 4G LTE서비스 제공업체가 되어 2017년 말에는 Gia Lai 지방으로 확장하였으며, 2018년 12월에 4G 기지국을 21,000개로부터 2019년까지 30,000개로 증가할 목표를 발표함
- Vietnamobile은 2017년 12월 4G LTE 서비스를 위한 라이선스를 받았으며, 2024년 9월 15일까지 유효함
- G Mobile은 2016년 10월에 4G LTE 서비스를 위한 라이선스를 받음
- 2019년 베트남 최초의 MVNO인 Itelecom은 초기 운영 단계에서 9개 시도의 산업 지역 노동자가

87 BuddeComm, Vietnam – Telecoms, Mobile and Broadband - Statistics and Analyses , 2019.5.29

서비스를 이용할 수 있게 됨

- Viettel은 2017년 4월 인구 커버리지 95%에 달하는 4G LTE 네트워크의 상용 개시를 발표하였음
- 베트남 정부는 2020년에 5G 상용 네트워크를 시작하기 위해 전국 이동통신 사업자에게 5G 테스트 라이선스를 2019년 1월에 제공하기 시작하였으며, 파일럿 5G 서비스가 하노이와 호치민시에서 수행될 예정이며 2020년까지 전국적으로 모바일 네트워크를 업그레이드할 계획임
- 2019년 1월 Viettel은 정보통신부(MIC)로부터 5G 이동통신 서비스를 시험할 수 있는 최초의 라이선스를 받았으며, 테스트 허가는 2020년 1월 21일까지 1년 동안 유효하며, 하노이와 호치민시에서 이 기술을 시험할 수 있음
- Viettel은 최대 73개 위치에서 5G를 테스트할 수 있지만 서비스를 테스트하는 사용자에게 요금을 청구할 수는 없음

▶ 전자상거래 및 결제시장 전문 조사기관 yStats에 의하면[88] 베트남의 비즈니스에서 2018년 1년간 온라인 사기 손실이 증가하였다는 답변이 50%로 나타났으며, 손실이 다소 줄었다는 답변은 44%, 손실이 같은 수준이라는 답변은 6%로 나타남

- 2018년 실시된 설문조사에 따르면, 인터넷 사용자의 17%가 보안 문제로 온라인 쇼핑을 하지 않은 것으로 나타났으며 이는 2017년 22% 대비 줄어듦
- 2017년 온라인 쇼핑을 하지 않는 이유로는 보안 문제 22%, 늦은 배송 11%, 배송 비용 10%로 상위 다섯 가지 요인이 주를 이룸
- 2018년 11월 인터넷을 통한 구매에 대해 베트남 온라인 쇼핑객의 대다수인 80%가 배달 시 현금을 지불하였으며, 직불카드/신용카드 결제는 8%, E-Wallet은 6%, 은행 이체가 5%에 해당함
- 2017년 디지털 방식으로 구매할 때 베트남 쇼핑객이 고려하는 주요 요인 중 하나는 지불방법이라는 응답이 41%로 나타남
- 2017년 온라인 쇼핑객 중 18%는 배달 지연으로 온라인 구매를 취소했으며, 2016년 13% 대비 5%p. 증가함
- 2018년 3월 베트남에서 가장 큰 인터넷 트래픽은 모바일이 70.6%을 차지했으며, 이후 데스크톱 25.4%, 태블릿이 4.0% 순으로 나타남
- 인터넷 사용자의 높은 스마트폰 보급률은 모바일 쇼핑의 성장을 이끌고 있으며, 2017년 인터넷 사용자의 86%가 스마트폰을 통해 온라인에 접속함
- 2017년 온라인 쇼핑객의 53%는 스마트폰에서 모바일 브라우저를 통해, 52%는 모바일 앱을 통해 디지털 구매를 했으며, 2016년에는 각각 47%, 40%에 해당함
- 2017년 6월 기준, 전자상거래 웹 사이트 트래픽의 모바일 점유율이 72%를 차지함

88 yStats, "Global E-Commerce Intelligence, Fraud and Security in Global Online Payments 2019", 2019.7.

▶ 베트남의 전자상거래는 호황을 누리고 있지만 통제가 어려움[89]

- 국가 운영위원회(National Steering Committee) 389 상무국장은 성명서에서 베트남의 전자상거래는 성장하고 있지만 많은 개인과 기업은 온라인 플랫폼에서 품질이 좋지 않은 제품을 판매하여 고객에게 해를 끼치고 있다고 발표
- 당국은 전자상거래 부문에 대한 규제가 부족하여 온라인 플랫폼에서 사기를 통제할 수 없었고, 또한 법적 체계는 기술 개발에 뒤처져 제재는 위반을 저지하기에 충분히 강력하지 않았음
- 2018년 독일 시장 조사기관인 Statista가 발표한 자료에 따르면, 베트남의 전자상거래 수익은 약 22억 7천만 달러에 달하며, 가장 발전된 6개 전자상거래 국가 중 하나였음
- Nielsen Vietnam과 Miniwatts Marketing Group이 집계한 통계에 따르면, 베트남 소비자는 하루 평균 7시간을 온라인으로 보내며, 도시 인구의 90%와 농촌 인구의 50%가 스마트폰을 사용함
- 베트남 전자 상거래 지수 2019 보고서[90]에 따르면, 베트남의 2017-2019년 전자상거래 성장률은 평균 25%~30% 사이이며, 이런 성장을 유지한다면 2025년 시장은 인도네시아와 태국에 이어 동남아시아에서 3위를 차지할 전망임
- 산업무역부 산하 시장관리국 대표는 전자상거래 비즈니스 활동이 가치와 규모면에서 강력한 발전을 보였으며, 많은 비즈니스와 개인을 끌어 들이고 있다고 말함
- 그러나 전자상거래의 성장은 또한 금지 및 위조 상품의 거래도 확대되어 당국은 소비자 보호를 위해 위조품, 가짜, 밀수품과의 싸움에 전념하고 있음
- 브랜드가 있는 전자상거래 플랫폼은 소비자를 보호하기 위한 조치가 있으나 소셜 네트워크에서 운영되는 개인 및 비즈니스 관리는 소비자 보호 조치 적용이 매우 어려운 상황임

▶ 인터넷 이용 환경

- ITU의 자료에 따르면 베트남의 인터넷 이용자 보급률은 2018년 70.35%로 전년의 58.14%에서 12.21% 증가하였음

89 The Phnom Penh Post, VN e-commerce booming but hard to control, 2019.9.22.
90 Vietnam e-Commerce Association, Vietnam E-Business Index 2019 Report, 2019.

그림 _ 베트남의 인터넷 보급률



[출처] ITU Statistics DB(2019.6)

- BuddeComm 자료에 의하면 전체 인구에 대한 모바일 브로드밴드 보급률은 2018년 추정치는 57%이며, 전체 인구에 대한 유선 브로드밴드 보급률은 2018년 13%에 해당하는 것으로 추정[91]

표 _ 베트남의 브로드밴드 보급률(2018년 기준)

구분	이용자 수	보급률
모바일 브로드밴드	54,900,000	57%
유선 브로드밴드	12,850,000	13%
전체	**67,750,000**	-

주: 데이터는 2018년 추정치에 해당함

[출처] BuddeComm(2019.5.)

- 베트남은 다른 아시아 국가에 비해 고정 회선 및 고정 브로드밴드 보급률이 낮고, 모바일 브로드밴드 보급률이 중간수준에 속함
- 기존 유선사업자인 VNPT와 2014년 VNPT로부터 공식적으로 분리된 네트워크 사업자인 Mobifone의 관리는 정보통신부(MIC)를 대신하여 국가 자본관리위원회(Committee for the Management of State Capital, CMSC)로 2018년 11월에 이전되었으며, 이는 사업자의 효율성과 경쟁력을 향상시키고 비즈니스를 위한 새로운 개발 계획을 세우는 것을 목표로 함

▶ 유선 브로드밴드

- 유선 브로드밴드 보급률은 주로 제한된 유선 회선수와 모바일 플랫폼의 지배로 인해 여전히 낮지만, 최근 FTTH 시장에 의해 2013년 6%에서 2018년 13%까지 보급률이 상승함

91 BuddeComm, Vietnam – Telecoms, Mobile and Broadband - Statistics and Analyses , 2019.5.29

- 유선 브로드밴드는 광범위한 DSL(Digital Subscriber Line) 기반으로 구축되었으며, 최근에는 광섬유 기반 서비스에 중점을 두어 광섬유 기반 가입자 증가가 강세를 지속함
- 통신 사업자 VNPT는 베트남 유선 브로드밴드 시장을 주도하고 있으며, 2017년~2018년 동안 FTTH서비스를 위해 전국 네트워크 인프라 및 전송 시스템을 확장하는데 투자하였으며, NGN(Next Generation Network) 개발의 일환으로 크게 수행하고 있음
- Viettel은 동일한 인터넷 회선에서 FTTH이외에 케이블 TV 서비스를 포함하여 여러 서비스를 제공하고 있으며, Viettel은 FTTH 가입자 수를 약 20~25%까지 늘리고, 전국 코뮌(commune)의 커버리지를 2016년 말 기준 46%에서 70% 커버리지로 증가할 계획을 2017년 발표함
- 또한 하이노, 호치민 등 기타 대도시에는 무료 WiFi 핫스팟이 널리 보급되어 있음

▶ 모바일 브로드밴드

- 베트남은 3G 및 4G 모바일 가입자의 증가로 인해 지난 5년간 모바일 브로드밴드 보급률이 매우 빠르게 증가하여, 보급률이 2013년 19%에서 2018년 57%로 증가하였음
- BuddeComm의 자료에 따르면 모바일 브로드밴드 시장은 상대적으로 개발의 초기 단계에 있어 향후 5년간 강한 성장이 기대되어 2018년~20203년 기간 동안 연평균성장률 9.2%로 2023년에는 84% 보급률에 달할 것으로 전망함[92]

92 BuddeComm, Vietnam – Telecoms, Mobile and Broadband - Statistics and Analyses , 2019.5.29

정보보호 시장 현황

1) 시장 규모

시장 개요

▶ 베트남 소프트웨어 및 IT 서비스 협회(VINASA)에 따르면 베트남 정보통신기술(ICT) 시장 규모는 2010년 20억 달러에서 2015년 30억 달러로 성장했으며, 소프트웨어 매출은 10억 달러에서 16억 달러로 증가
- 베트남 정보보호 시장 역시 정부와 기업 양쪽에서 보안에 대한 관심이 증가하면서 매년 10%가 넘는 고성장을 유지하고 있음

▶ 특히, 해외투자진흥법 도입은 과거 20년 간 베트남 정보보호 시장 성장의 촉매 역할을 해 왔음
- 1996년 해외투자진흥법(Foreign Investment Law) 입법 이후 베트남 기획투자부 (Ministry of Planning & Investment) 산하 해외투자국(Foreign Investment Agency)은 총 9,500건 이상(980억 달러)의 해외투자 프로젝트를 유치
- 로컬 시장에서 집행된 투자 프로젝트는 산업 전반에 걸쳐 확산 중인데, 특히 보안장비 분야에서 매우 높은 투자 유치율을 보이며 수혜를 받음
- 또한 과거 베트남의 보안장비 수입 관세는 30~35% 수준이었으나, 2006년 WTO 가입 이후 관세 장벽을 완화하고 있으며 이는 해외 진출 기업들에게는 중요한 메리트로 부각

▶ 베트남 정보보호 시장에서는 글로벌 벤더들이 주축을 차지하는 가운데, 안티바이러스 소프트웨어 등 일부 사업영역에서 BKAV, CMC 등 현지 기업들이 두각을 나타냄
- 베트남 정부는 정보보안 자주권 실현을 위해 자국 제품의 점유율 50% 달성을 목표로 자국 정보보안 산업에 세금 인센티브 제공 등의 정책적 지원 방안을 모색 중

시장 규모 및 전망

▶ Ken Research의 자료에 따르면 베트남 사이버 보안 시장은 2023년 말까지 매출 기준 약 2억 1,500만 달러에 도달하여, 2019년~20203년 기간 동안 사이버 보안시장은 연평균 성장률 14.8%로 예상함[93]
- 베트남 정보통신부에 따르면 2019년 1분기에 약 4,770건의 사이버 공격이 목격됐으며, 이는 전년에

보고된 총 사건수의 절반 이상에 해당함

- 또한 베트남 소매 시장은 이 분야에 대한 투자가 증가함에 따라 향후 5년간 26%의 성장률로 증가할 것으로 예상되며, 이로 인해 신용카드 거래 수가 증가하여 이 부분에서 효율적인 사이버보안 솔루션의 필요성도 높아짐
- 베트남의 ICT산업은 베트남 경제의 성장과 변화를 위해 ICT 파워로 전환하려는 베트남 정부의 요구로 인해 빠른 속도로 성장할 것으로 예상됨
- 베트남의 사이버 보안 산업은 사이버 범죄 사건의 수가 증가하고, 기업간 보안 솔루션에 대한 인식이 높아지고, 소매, ICT 및 기타 최종 사용자 산업과 같은 분야가 성장하고, 디지털 보급 증가와 중소기업의 데이터 보안 솔루션에 대한 수요가 증가함에 따라 더 확장될 것으로 예상함

▶ 베트남 보안장비 시장은 매년 10% 이상의 성장률을 보이고 있는 가운데 최근 베트남 경제 회복과 함께 공공과 민간 분야의 투자 확대가 이어지고 있어 향후 수년 간 높은 성장성이 기대됨

- 2016년 베트남 소방전시회(Secutech Vietnam)에 참가한 보안 기업들은 2016년 평균 15%의 매출 성장을 기대했으며, 이는 베트남 국민들의 보안 인식 제고와 함께 정부와 민간 분야의 지출 증대에서 기인
- 현지 SI 업체 Techpro에 따르면 최근 정부가 보안을 매우 중시하고 있으며, 과거 정부기관들은 보안 인력에만 의존했지만 최근 신축되는 정부 건물들은 모두 비디오 감시와 접근통제 시스템을 갖추고 있음

▶ 시장조사기관 6Wresearch에 따르면 베트남의 영상감시 시장은 2016~2022년까지 12.4%의 연평균 성장률을 기록할 전망

- 보안에 대한 우려가 증가하면서 영상감시 시스템에 대한 수요가 증가하고 있으며, 베트남 재정부가 ATIGA(ASEAN Trade in Goods Agreement) 협정에 따라 주요 수입품에 대한 관세를 인하하면서, 다양한 영상 감시 시스템의 부품가가 하락하며 시장이 확대되고 있음
- 6Wresearch에 따르면 베트남에서 아직까지는 저가의 아날로그 방식 영상감시 시스템 비중이 가장 높지만, IP 영상감시 제품이 매출액 기준으로는 가장 높은 비중을 차지하며, 엔드유저 사이에서 아날로그 HD 카메라에 대한 수요가 커지면서, 하이엔드급 아날로그 카메라 시장이 더욱 성장할 전망
- 2016~2022년 사이 IP 영상감시 시스템은 정부 및 교통, 은행과 금융 산업을 중심으로 도입될 전망이며, 그밖에 일반 사무실과 헬스케어 및 접객 산업 역시 향후 6년간 성장의 주요 동력이 될 것
- 특히 베트남 남부 지역은 상업 및 소매 산업의 핵심 건설 프로젝트 덕분에 베트남 영상감시 시장의 최대 매출원이 되고 있음

---

93 CISION PR News, Vietnam Cyber Security Market is Expected to Reach about USD 215 Million in Terms of Revenue by the Year Ending 2023: Ken Research, 2019.9.2.

2) 분야별 현황

물리보안 제품 및 서비스

▶ 베트남 물리보안 시장은 크게 출입통제, 탐지 및 화재 장비로 구분

- Barnes Report에 따르면 2015년 기준 보안시스템 매출 규모는 약 1억 9,600만 달러로, 이중 일반 보안 시스템/서비스 매출이 1억 1,500만 달러, 화재 경보 시스템이 5,700만 달러, 안전 장비가 800만 달러, 구금시설 감시시스템이 500만 달러의 매출을 기록

표 _ 보안장비군 별 유망 제품

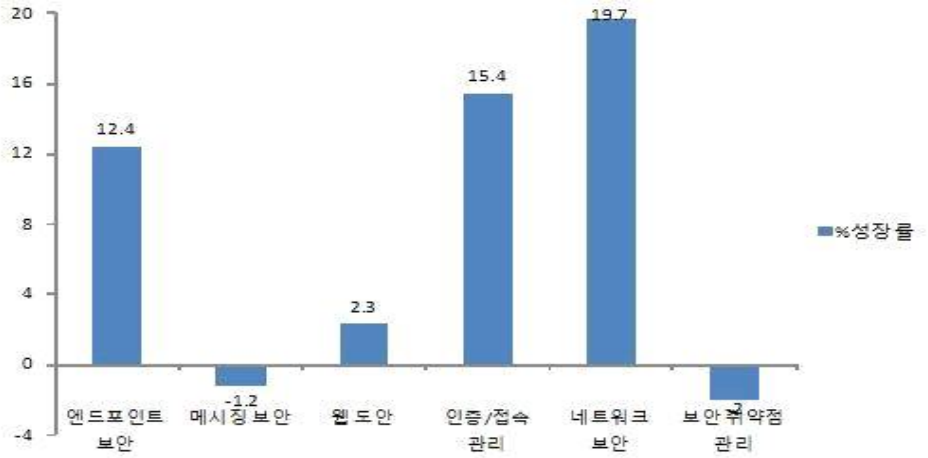
보안장비군	주요 유망 제품
출입통제 장비	도난방지, 침입방지 모니터링 시스템, 출입제어 및 감시시스템
탐지 장비	수하물/신체 스캐너, 금속 탐지기
화재 장비	화재경보 시스템, 제어패널, 소화분무기, CO2 및 불활성 압축가스 시스템 및 가스 탐지 시스템

정보보안 제품 및 서비스

▶ 시장조사기관 IDC에 따르면 2014년 베트남의 보안 소프트웨어 매출 규모는 1,660만 달러로 전년 대비 11.9% 증가했으며, 클라우드 컴퓨팅 기반 애플리케이션의 성장으로 2015년에도 10% 대의 성장을 달성한 것으로 추산

- IDC는 베트남 기업들이 웹과 메시징 보안에 대한 지출을 줄이는 대신 엔드포인트와 네트워크 보안에 집중하고 있다며, 2014년 엔드포인트 보안 시장이 정부기관 및 통신사들의 구입에 힘입어 12.4% 성장했다고 밝힘
- 웹과 메시징 보안 시장은 2014년 전년 대비 각각 2.3%와 1.2% 감소를 기록했으며, 식별/접근 관리 시장은 15.4% 성장했음
- 2013년과 비교해 보안 및 취약점 관리 소프트웨어 시장은 은행 및 통신 분야와 같은 핵심 엔드유저층의 지출 둔화로 2% 감소를 기록
- 한편 2014년 하반기 공공 클라우드 상의 엔드포인트 보안 시장이 74% 성장하면서, 전통적인 방식의 라이선스 소프트웨어 판매에 크게 의존하는 유통업체들에게 위협 요인이 되고 있음

그림 _ 2014년 베트남 보안 소프트웨어 분야별 성장률



[출처] IDC, Vietnam News, 'Businesses spend more on data security'(2015.6.13.) 재인용

▶ 베트남 보안 소프트웨어 시장에서는 콘텐츠 보안 및 위협 관리 솔루션(Secure Content and Threat Management Solutions, SCTM)이 가장 큰 비중으로 보이고 있음

- 이어서 통합 계정 및 권한 관리(IAM, Identity Access Management), 보안 및 취약성 관리(SVM, Security and Vulnerability Management) 순

▶ 베트남에서는 26개 이상의 보안 벤더들이 활동 중이며 특히 가장 높은 매출을 보이고 있는 SCTM 시장에서는 경쟁이 치열한 상황

- 벤더들은 각각의 제품군에서 다양한 가격대와 성능을 갖춘 신규 솔루션들을 지속적으로 출시 중
- 또한 이들 기업들은 제품 개발 이외에도 마케팅이나 파트너십 활동 등을 병행 노력
- 최근 기업들은 엔드포인트 솔루션에만 국한하지 않고 가상화, 데이터센터, 모바일 기기, 소셜 네트워크 등 다양한 보안 분야를 겨냥한 솔루션 개발로 시장 경쟁은 점차 다이내믹해지고 있는 상황

3) 주요 사업자 현황

시장 특성 및 경쟁 강도

❑ 정보보안 시장

▶ 베트남 정보보안 시장은 매출 규모 면에서 Symantec, IBM, McAfee, Cisco의 4대 메이저 보안 기업이

시장의 절반가량을 차지하고 있으며 로컬 기업들의 비중은 10% 내외 수준

- 이들 글로벌 기업들은 주로 대규모 정부 프로젝트나 기업 부문의 매출 비중이 높은 반면, 로컬 기업들은 안티바이러스 소프트웨어를 중심으로 한 일반 소비자 시장을 주요 매출원으로 하고 있음

▶ 베트남 내 안티바이러스 소프트웨어 시장은 현재 Norton Antivirus(Symantec), Kaspersky, McAfee, Trend Micro, Bit Defender, Avira 등의 유력 해외 브랜드들과 BKAV, CMC 등 자국 브랜드 및 신규 기업들 간에 치열한 경쟁을 펼치고 있음

- 2009~2010년 사이 많은 안티바이러스 분야 국내외 기업들이 베트남 시장에 진출했으나, 상당수가 소비자의 관심을 끌어내지 못하거나 제품의 치명적인 오류 등으로 인해 현재 10개 내외의 플레이어들만 시장에서 활동 중
- 현지 기업으로는 CMC와 BKAV 두 기업이 대표적으로 현지 소비자들에게 인기를 얻으며 해외 기업들과 경쟁하고 있음

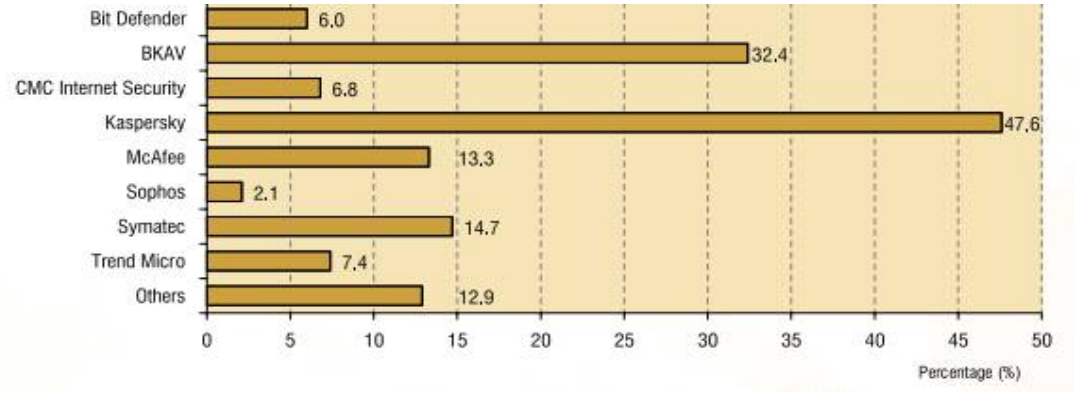
▶ 한편, 다수의 해외 정보보안 업체들은 베트남 중소기업을 대상으로 한 보안솔루션 서비스를 지속적으로 확대하고 있음

- 2013년 7월 미국의 스토리지 솔루션 기업 EMC는 베트남 중소기업을 대상으로 IT 보안솔루션 세미나를 개최하며 대기업 위주의 고객을 중소기업으로 확대하기 위해 노력 중
- Symantec도 최근 베트남 중소기업을 대상으로 한 터미널 서비스 보안, 온라인 사기 방지 및 이메일 안티바이러스 등 다양한 보안솔루션을 제공 중

▶ 베트남 정보통신부가 2013년 베트남 전역의 600개 정부기관 및 기업들을 대상으로 실시한 설문조사에 따르면 안티 바이러스 시장에서 가장 많이 사용되는 소프트웨어는 Kaspersky(47.6%)로 나타났으며, BKAV(32.%), Symantec(14.7%), McAfee(13.3%)가 그 뒤를 이었음

- CMC와 함께 베트남의 대표적인 로컬 정보보안 업체인 BKAV에 따르면 2013년 1분기 기준 베트남 내 컴퓨터 중 안티바이러스 소프트웨어를 탑재한 컴퓨터의 비중은 50% 미만
- 안티바이러스 시장은 글로벌 벤더들이 시장에 진입한 2010년 대비 역동성이 더욱 줄어들었으며, 이는 정품 소프트웨어에 대한 지출을 꺼리는 로컬 기업들 및 소비자들로 인한 것

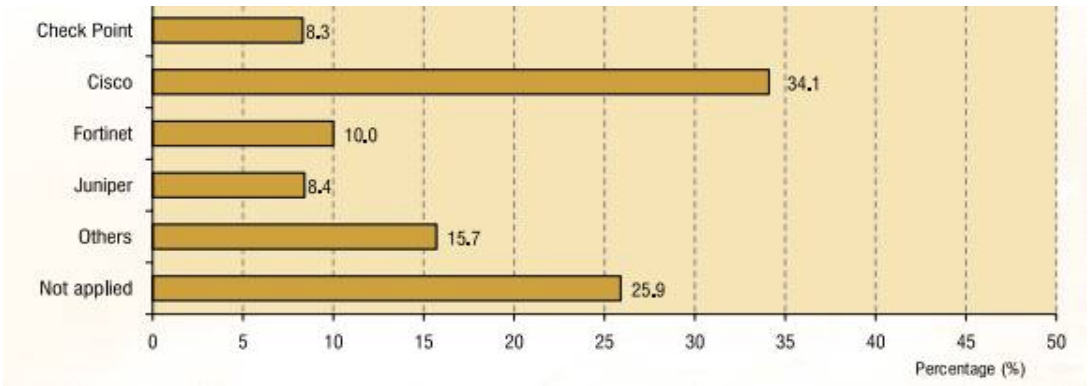
그림 _ 베트남 안티바이러스 소프트웨어 브랜드별 사용률



[출처] MIC, 'Vietnam Information and Communication Technology White Book 2014'

▶ 방화벽 소프트웨어 시장에서는 Cisco가 34.1%로 가장 높은 사용률을 나타냈으며, Fortinet(10.0%)와 Juniper(8.4%), Check Point(8.3%)가 그 뒤를 이었음

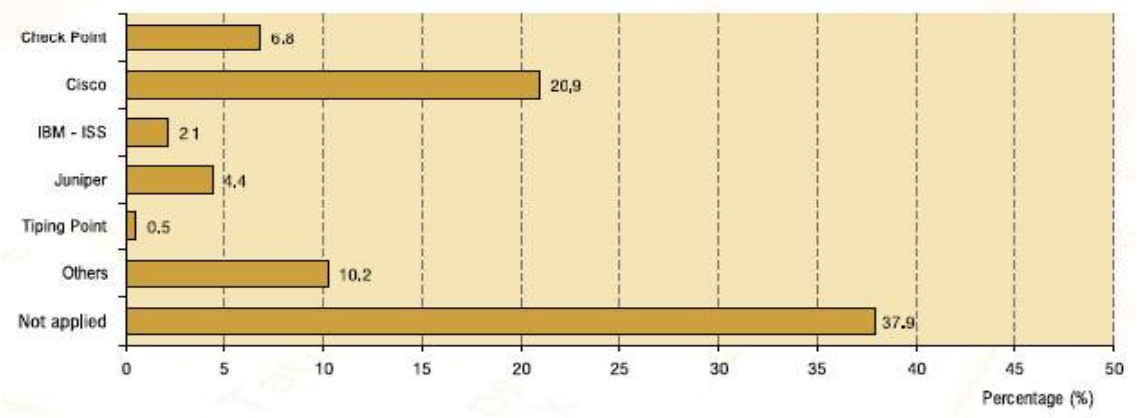
그림 _ 베트남 방화벽 소프트웨어 브랜드별 사용률



[출처] MIC, 'Vietnam Information and Communication Technology White Book 2014'

▶ IDS/IPS 소프트웨어 시장에서는 Cisco를 사용하는 비율이 20.9%로 가장 높았으며, Check Point(6.8%)와 Juniper(4.4%)가 그 뒤를 이었으나, IDS/IPS를 사용하지 않는 기업 비율이 37.9%에 달했음

그림 _ 베트남 IDS/IPS 소프트웨어 브랜드별 사용률



[출처] MIC, 'Vietnam Information and Communication Technology White Book 2014'

▶ 베트남 모바일 보안시장에는 로컬 기업과 해외 보안 기업을 포함 총 10개 이상의 사업자들이 활동 중

- 주요 사업자로는 해외업체로 Kaspersky, Trend Micro, Symantec, Bitdefender 등이 있으며 현지 업체로 BKAV, CMC가 대표적

❑ 물리보안 시장

▶ 베트남에는 약 1,000개 이상의 전자식 물리보안장비 및 서비스 업체가 있으며, 화재 안전 업체가 1,000~2,000개, 보안경비 업체가 약 700~800개로 추산

- 베트남에서는 많은 업체들이 시스템 통합과 유통, 설치 업무를 동시에 수행함
- 베트남 보안 제품들은 대부분 수입 제품이지만, 최근 Vantech, VDTECH, Questek, Seavision, Escort 등 현지 업체들도 점차 부상하고 있으며, 현지 업체들은 가격 면에서 훨씬 저렴하다는 이점이 있음

▶ 보안장비 중 CCTV는 베트남 내에 생산 기반이 없어 해외 벤더들에 대한 의존도가 특히 높은 분야로 중국/대만의 업체들이 높은 시장 장악력을 보이고 있으며, 이어서 국내 업체(20~25%), 일본 업체(10% 내외) 순의 시장 점유율을 기록

- 베트남 영상감시 시장의 주요 업체로는 Avigilon Corporation, Axis Communications, Bosch Security Systems, Hikvision, Hanwha(구 Samsung) Techwin, Panasonic, Sony, Pelco by Schneider 등이 있음
- 비교적 시장 진입 장벽이 낮은 CCTV 제품군의 특성 상 현지에는 300개 안팎의 IP 및 아날로그 CCTV 제공업체들이 활동 중인 것으로 추정

▶ 베트남 보안장비/시스템 시장은 95% 이상이 수입품일 정도로 해외 공급업체에 대한 의존도가 높으며, 로컬 제조업체들은 열쇠, 금고, 안전 장갑, 로프 등 로엔드 보안장비 제품 생산에 주력

- 따라서 베트남 로컬 업체들은 글로벌 선도 기업들의 공급 에이전트 역할에 치중
- 특히 IP 기반 CCTV 시스템, 통합보안시스템, 전자카드 출입통제 시스템, 스마트카드 기술, 침입탐지 장비 등 하이엔드급 자동 보안 시스템에 대한 해외 수요가 높은 편

주요 사업자

❑ 정보보안 시장

▶ BKAV

- 베트남의 대표적 보안 소프트웨어 기업으로 BKAV의 안티바이러스 소프트웨어는 베트남 정보보안 협회에 의해 5년 연속 가장 인기있는 제품으로 선정되었으며, 고객 수는 약 1,000만 명에 달함
- BKAV 소프트웨어 제품은 1) 대부분 Tran Anh과 같은 유통 채널을 통해 시장에 공급되거나, 2) Pico나 Nguyen Kim 같은 가전 매장을 통해서도 일부 공급이 이뤄지고 있으며, 베트남 북부 지역에서는 BKAV 소프트웨어 제품이 Gia Long과 An Phat의 양대 유통 업체를 통해 공급
- BKAV의 구매층은 대부분이 정보 기술에 대한 지식이 많지 않은 학생이나 일반 가구로 구성되며, 하노이나 호치민 등의 대도시에서 매출의 80% 가량 발생
- BKAV는 베트남 내 26개 도시에서 전자정부 프로젝트를 수행했으며, 스마트홈 시스템과 스마트폰 Bphone 제조도 하고 있음

▶ CMC

- 베트남의 대표적인 IT 기업으로서 자회사로 CMC SI, CMC Software, CMC Telecom, CMS, CMC Infosec 등을 두고 있음
- 이 중 2006년 6월 설립된 CMC Infosec은 정보보안 솔루션 R&D에 특화된 기업으로, 개인 및 모든 분야의 기업을 대상으로 합리적인 가격에 보안 솔루션 제공을 목표로 함
- 보안 관련 제품으로는 CMC Mobile Security, CMC Internet Security, CMC Endpoint Security, CMC Antivirus 등이 있으며, 그 외 보안서비스 및 시스템통합 서비스 등도 제공
- 주요 고객사로는 HP, Honda, Dell, Cisco, Emerson, Acer, APC 등이 있음

▶ Symantec

- 안티바이러스 분야 해외 기업 가운데 가장 높은 브랜드 파워를 보유하고 있으며, 2008년 이후 Security Management 제품 및 솔루션 분야 공략 강화
- Thakral One, FPT, Ingram Micro 등이 베트남 내 Symantec 제품 유통 담당

▶ Kaspersky Lab

- 안티바이러스 프로그램으로 베트남 시장 진입에 성공했으며, 최근에는 기업 시장으로 영역 확대 중이며, 2013년 4월 Kaspersky Lab과 베트남 유통업체인 Nam Truong Son Group은 기업 보안 솔루션(Kaspersky Endpoint Security for Business)을 새롭게 도입
- 同 솔루션은 IT 보안 관리를 단순화하고 다양한 규모의 기업들을 위한 고성능 보안 기능을 구현하기 위한 기술로, 모바일 보안, 디바이스 관리, 데이터 암호화 기능, 엔드포인트 컨트롤 툴, 시스템 관리, 안티 멀웨어 방지 등의 다양한 기술 제공

▶ IBM

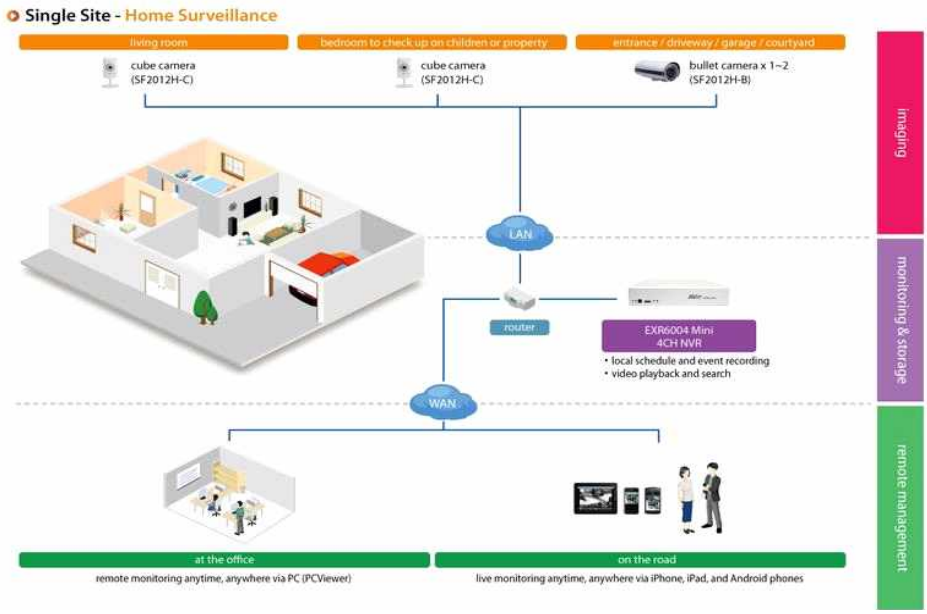
- 정부, 국영기업, 대기업을 대상으로 클라우드 기반의 통합 보안 솔루션을 중심으로 높은 기술력 과시
- 베트남우정통신공사(Vietnam Post and Telecommunication Corporation, VNPT)의 데이터통신 자회사인 VDC(Vietnam Datacommunication Company)는 IBM의 SmartCloud Managed Backup 시스템(V-Backup)을 도입
- 해당 시스템은 클라우드 기반의 온/오프 사이트 기업 데이터의 보안성 강화와 관리 보호 기능을 제공하며, 양사는 V-Backup 시스템이라는 브랜드로 베트남 내 중소기업을 위한 중저가 보안 서비스도 지원
- 현지 법인과 유통업체인 FPT를 통해 자사 솔루션 및 제품 판매

❑ 물리보안 시장

▶ AVer

- 2008년에 설립된 대만 소재 영상 기술 전문 기업으로 전 세계 100개국 이상에 자사 제품 수출
- 감시 장비 분야에서는 ABM Distribution Vietnam을 베트남 유통 파트너로 두고 현지 시장 개척 중
- Maritime Bank, SeABank 등 금융 기관용 ATM을 중심으로 아날로그 감시 솔루션 업그레이드 사업 확장 중
- 아날로그 카메라와 IP 카메라를 단일 DVR로 연동시키기 위한 AVer hybrid DVR(HD NVR) 제품 시장 호평

그림 _ AVer HD NVR 구성도



[출처] AVer 홈페이지

▶ ACTi

- 대만 소재 IP 영상감시 전문 기업으로 하드웨어와 관리 소프트웨어를 포함한 엔드투엔드 솔루션을 제공하며, 베트남 Chinfon Cement Corporation에 25프레임 풀 D1(720x576) MPEG-4 IP 제품 공급
- 베트남 현지 협력 파트너인 LOIKHA를 통해 시장 진출

▶ Honeywell

- 빌딩, 가정 및 산업용 보안 통제 기술 분야의 세계적 선도 업체로 2005년 하노이와 호치민에 법인 설립
- 정유(PetroVetnam), 항공(Vietnam Airlines), 빌딩자동화, 화학단지 등 다양한 산업 분야에서 Honeywell 장비 채택하고 있으며, CCTV 시스템, 스캐닝 장비, 센서 등의 솔루션 제공
- 2010년 Honeywell의 베트남 매출은 3,000만 달러를 넘어섬

4) 주요 동향 및 이슈

▶ 한국의 삼성 SDS는 베트남 IT 서비스 기업인 CMC의 주요 의사결정에 참여하는 전략적 투자에 합의(2019.5)[94]

- 베트남 2위 IT 서비스 기업인 CMC의 2018년 매출은 약 2,615억 원이며, 주요 사업으로 SI, SW개발, 클라우드, IT 인프라 운영 등임
- 양사는 2018년 6월 스마트팩토리와 사이버보안 분야에서 공동 사업을 위한 협약을 체결한 데 이어 이번에 전략적 파트너십 관계를 구축하게 되며, 삼성 SDS의 투자금은 500억원대로, CMC 지분 중 약 25%를 인수하게 됨
- 삼성 SDS는 AI, IoT, 빅데이터 분석 등과 함께 특히 스마트팩토리, 클라우드, 사이버보안 등의 분야에서 CMC의 현지 영업망과 인지도를 결합하여 베트남에서 강력한 시너지 효과를 창출할 것으로 전망함

▶ 2017년 사이버 바이러스로 인한 피해액이 5억 달러를 넘는 것으로 밝힘(2018.1)[95]

- 온라인 보안 업체 BKAV에 따르면 2017년 사이버 공격으로 인한 피해액이 5억 달러에 달한다고 발표, 이는 전년 대비 18% 증가한 수치
- 2017년 5월 랜섬웨어 Wannacry의 글로벌 공격 당시 베트남은 1,900대 이상의 컴퓨터가 감염됨
- 암호 화폐 채굴 멀웨어(cryptojaking)의 경우 23,000대의 컴퓨터를 감염시킴
- 2018년에도 베트남을 향한 사이버 공격이 있을 것이며, 보안이 아직 취약한 베트남은 손실을 감수해야 할 것이라 발표함

▶ 각종 사이버 범죄에 노출된 베트남 (2018.7)[96]

- BKAV에 따르면 2018년 7월에만 BrowserSpy라는 스파이웨어에 56만대의 PC가 감염되었다는 것을 확인함
- 바이러스 감염의 주원인은 USB로, 80%의 베트남 USB들은 최소 1년에 한번 바이러스에 감염되는 것으로 밝혀짐
- 2018년 6월 BKAV는 120만대의 PC가 W32.XFileUSB 바이러스로 인하여 데이터를 잃어버렸다고 발표함
- 2018년 4월 베트남 정보통신부는 전 세계 멀웨어 IP와 도메인을 방문한 1,300만개의 베트남 IP를 기록하였으며, 국제기구 블랙리스트에 38만개의 베트남 IP가 등록되어있다고 밝힘
- 응우옌 다이 부(Nguyen Dai Vu) 입법부 국회 부의장은 네트워크 인프라에서 최종 사용자에 이르는 전체 컴퓨터 시스템을 보호하기 위한 중앙 정보 보안 통제가 필요하다고 주장함

▶ 베트남 호스팅 업체, 싱가포르 클라우드 보안 업체와 데이터 보호 파트너십 체결 (2018.6)[97]

---

94 삼성SDS, 동남아 진출 박차...베트남 IT기업에 500억 투자, RayThe, 2019.5.27
95 Vnexpress, "Vietnam loses $542 million to cyber viruses in 2017", 2018.1.2.
96 Vnexpress, "Virus alert: 80 percent of USBs in Vietnam are infected", 2018.6.14.
Vnexpress, "Spyware attacks half a million plus computers in Vietnam", 2018.7.27.
97 PrWeb, "Dropsuite and Mat Bao Join Forces in Southeast Asia to Partner On Data Protection", 2018.6.25.

- 싱가포르 클라우드 보안 기업 Dropsuite Limited와 베트남 호스팅 제공 기업 Mat Bao가 데이터 보호 파트너십을 체결함
- Mat Bao는 2002년에 설립된 인터넷 인프라 서비스 기업이며, 현재 베트남 최고의 호스팅 제공 업체임
- Dropsuite는 회사 정보를 백업, 복구, 보호를 주력으로 하는 클라우드 보안 기업으로, 베트남의 Mat Bao 뿐만 아니라 100 개국 이상의 기업들에게 서비스를 제공 중
- 베트남의 온라인 쇼핑 소비자는 약 3,500만 명. Mat Bao의 클라우드 백업 기술을 전면 도입함으로 베트남 사이버 보안이 안전해지는 계기가 될 것으로 예상
- Mat Bao는 Dropsuite의 이메일 백업 서비스, Office 365의 문서보존 서비스를 베트남어로 현지화 하여 제공 할 수 있게 됨

5) 정보보호 스타트업 시장 현황

▶ 베트남 기반 사이버 보안 스타트업 689Cloud는 싱가포르의 ICE71로부터 자금지원을 받음 (2019.5)[98]

- 싱가포르 기반의 사이버보안 기업가 허브인 BLOCK71(ICE71)에 현신 사이버보안 생태계는 ICE71 엑셀레이트 프로그램을 통해 자금을 조달한 10개의 스타트업을 공개하였음
- 스타트업들은 싱가포르에서 개최되는 ICE71 엑셀러레이트 데모데이에 소개되어 투자자와 사이버보안 리더에게 아이디어와 기술을 피칭할 기회를 가짐
- ICE71 엑셀레이트의 두 번째 모집된 스타트업에는 베트남 기반 사이버보안 스타트업 689Cloud는 권한 관리 기술을 사용하여 외부 공유 디지털 문서에 대한 접근 권한을 보호, 추적, 제어하여 데이터 유출 및 기밀 데이터의 무단 재배포를 방지함

▶ 베트남 주요 엑셀러레이터 중 하나인 Topica Founder Institute(TFI)는 2018년 현지 스타트업에 유치된 투자금이 8억 8,900만 달러(92건)에 달하는 것으로 추산함 (2019.5)[99]

- 해당 금액은 전년대비 3배 정도 크며, 현지 스타트업의 성장 가능성에 대한 투자자들의 기대가 지난 1년 사이 크게 높아진 것으로 반영됨
- 투자 금액이 집중된 분야는 핀테크, 전자상거래, 물류테크 등이며, 투자자들의 관심을 이끈 스타트업의 대부분은 AI 같은 기술을 결합한 솔루션을 구축했으며 모바일 기반의 서비스를 제공함
- 베트남의 스타트업 시장은 아직 성장 초기단계로 시리즈B 투자 단계에 들어선 스타트업 수도 많지 않음

98 689Cloud, '689Cloud – Vietnam-based Cybersecurity Startup receive funding from Singapore's ICE71', 2019.5.10.
99 Kotra 해외시장뉴스, 베트남 스타트업 화두는 "Tech", 2019.8.22.

정보보호 정책 및 기관 현황

1) 관련 법령 및 정책

관련 법령 및 규제

▶ 인터넷 정보보안법

- 베트남 국회는 2015년 11월 19일 개인정보보호 강화 등에 대한 조항을 포함하는 인터넷 정보보안법을 통과시켰으며, 해당 법안은 2016년 7월 1일부터 시행됨
- 동법은 총 8장 54조로 이루어져 있으며, 인터넷 정보보호, 인터넷 정보보호를 위한 기관·단체·개인의 권리와 책임, 인터넷 정보보호에 관한 기준·표준, 인터넷 정보보호 사업, 인터넷 정보보호 사업에 종사하는 인재의 육성, 인터넷 정보보호에 관한 정부 관할 관청의 관리 책임 등을 규정
- 동법에서는 인터넷에서 정보 전송을 불법적으로 방해·간섭하는 것, 정보 시스템의 활동을 불법으로 방해하여 이용자의 합법적인 사용에 영향을 주는 것, 인터넷 정보보호 시스템을 불법 공격하고 불법으로 탈취하는 것, 스팸 메일 악성 코드를 유포하는 것, 사기·위조된 정보로 네트워크를 구축하는 것, 타인의 개인 정보를 불법으로 수집·이용·유포하는 등의 행위가 일체 금지됨
- 또한 제2장 제 31조 등에서는 테러 활동에 있어서 인터넷의 악용 방지 등에 대해서도 규정하고 있음

▶ 사이버보안법(Law on Cybersecurity)

- 베트남 국회는 2018년 6월 12일 국가 사이버 보안 강화 등에 대한 조항을 포함하는 사이버보안법을 통과시켰으며, 해당 법안은 2019년 1월 1일부터 시행됨
- 동법은 총 7장 43조로 이루어져 있으며, 사이버 공격 예방, 보안사고 대응, 네트워크 보안 역량 강화, 사이버 공간에서의 아동 보호에 관한 법률과 책임을 규정함
- 공공질서를 어지럽히거나 반국가적 콘텐츠, 거짓 선전 선동을 담은 게시물은 제공해서는 안 되며, 서비스 제공 기업들은 이러한 게시물들을 걸러낼 수 있는 메커니즘을 개발하여 적용해야 함
- 사용자 정보를 기밀로 유지하되, 해당 사용자가 사이버 보안에 관한 법률을 위반했다고 판단될 경우, 서비스 제공 기업은 당국과 협력하여 사용자에 대한 정보를 제공해야함
- 당국이 요청할 경우, 법령을 위반한 콘텐츠는 24시간 이내로 삭제해야 함
- 사용자 개인정보와 사용자의 서비스 이용 기록은 특정 기간 동안 저장되어야 함
- 외국 업체가 베트남에 서비스를 제공하기 위해서는 베트남에 지사 혹은 사무소를 설립하여야 하며, 베트남 사용자의 정보를 베트남 현지에서 보관할 수 있는 시설을 마련해야 함

주요 전략 및 정책

▶ 베트남 정부는 2016년 1월 '광대역 개발 계획'을 발표

- 광대역 인프라를 개선하여 2020년까지 인구의 40%가 혜택을 받을 수 있도록 함
- 또한 인터넷 연결의 적어도 60%가 최소 25Mb/s 속력을 유지하는 것을 목표로 하며, 공공장소 인터넷 접속 지점의 적어도 50%가 최소 50Mb/s의 인터넷 연결 속력으로 업그레이드 하는 것이 포함됨
- 모바일의 경우, 주거 지역의 최소 95%가 3G 또는 4G 네트워크를 구축하여 도시지역에서 최소 속력 4Mb/s, 농촌지역에서는 2Mb/s의 속력을 제공하는 것을 목표로 함
- 전자정부, 전자상거래, 재난 방지 같은 ICT 서비스와 디지털 콘텐츠의 애플리케이션을 홍보하는 것에도 중점을 둠
- 이 계획은 특히 민간 기업 부문이 브로드밴드 인프라 개발에 투자하도록 장려하고 통신 기업이 브로드밴드 라이선스를 보다 쉽게 받을 수 있도록 장려함
- 이러한 개혁의 일환으로 경쟁을 촉진하고 국유 및 민간 통신 서비스 제공업체를 통합한 관리 메커니즘이 도입되었음
- 정부는 기술 회사가 브로드밴드 장비를 국내에서 제조하거나 조립하여 생산 비용을 최소화하도록 권장함

▶ 베트남은 정보보호 강화를 위해 베트남 전자상거래협회(Vietnam E-commerce Association)와 공업무역부(Ministry of Industry and Trade)가 현지 전자상거래 웹사이트에 대해 'TrustVn' 라이선스를 발급

- TrustVn 라이선스는 APEC 회원국들과 비즈니스를 하는 베트남 기업들 중 개인정보보호 정도, 방문자 수, 체결된 계약의 모니터링 등의 결과를 기초로 발급
- 베트남 정부정보보안위원회(Government Information Security Commission, GISC)는 정부 기관 간 온라인 거래 시 보안 강화를 위해 2012년 6월부터 2015년까지 15만 건의 디지털 서명 제공을 발표
- 이를 위해 정부정보보안위원회(GISC)는 2,500~3,000억 동(약 1,200~1,440만 달러)을 투자할 계획

▶ 2020년까지의 베트남의 사이버보안 전략(2016-2020)

- 베트남은 2020년까지의 사이버보안 전략(Vietnam's Cybersecurity Strategy by 2020)을 2016년 5월에 마련함
- 베트남은 사이버보안법에 대한 준수와 국가 전반의 사이버위협 대응력 강화를 위해 사이버보안전략을 수립
  - 국가사회 전반의 사이버보안 준수에 대한 의식 제고
  - 사이버보안 제품·서비스 시장 창출 및 진흥과 중요 시스템 보안 강화

- 국가 차원의 사이버보안을 강화하고, 적응력과 유연성 등 강화

• 사이버보안전략(2016~2020)은 다음의 4대 목표를 위해 추진함

① 사용자 인식 미흡, 부주의 등으로 인한 사이버보안 손실 발생률을 50% 미만으로 축소

② 베트남의 전자거래 명성을 높이면서, 전 세계에서 최악의 악성코드 및 스팸 감염률을 보이는 20개 국가 목록에서 베트남이 제외되도록 함

③ 사이버보안의 기술 규정, 표준체계, 검증 및 평가 체계 마련

④ 국내 시장에서 널리 사용되는 베트남 브랜드의 사이버보안 제품 5개 이상 창출, 베트남 기업이 사이버보안 시장에서 주도적 역할 수행

• 사이버보안전략의 추진과제와 기관별 역할은 다음과 같음

표 _ 사이버보안전략 중점과제

구분		주요과제
중점과제 (Duties)	국가 차원의 사이버보안 보장	• 국가 중요 정보시스템에 대한 최소한의 사이버보안 요구사항을 개발하고, 사이버보안 보장 투자를 강화하며, 국가 중요 정보시스템에 대한 사이버보안의 정기적 검증 및 평가 • 사이버보안에 관한 국가 기술 규정 및 표준 체계 마련, 국제 관행에 따른 사이버보안 관리체계 모델 개발 및 보급 • 사이버보안을 보장하는 기술역량을 향상시키기 위해 다음과 같은 플랫폼 시스템 개발에 투자 - 베트남 사이버 공격 처리 시스템 - 사이버보안 평가 및 검증 시스템 - 국가 전자인증 시스템. • 국가 차원에서 사이버보안 침해대응협력 네트워크 역량 향상 및 효과적 운영 - 사이버보안을 보장하고 국제 사이버훈련에 참여하기 위해 정기적인 사이버훈련 조직 • 악성코드 방지 및 통제 능력을 향상시키고 전자거래 활동에서 국가의 신뢰성 향상
	조직 및 단체의 활동에서 사이버보안 보장	• 조직 및 단체의 활동에서 사이버보안을 보장하기 위해 규정 및 정책을 개발, 발행 및 정기적으로 현행화 • 조직 및 단체 활동의 기술 규정 및 표준에 부합하는 사이버보안 관리체계 적용 • 사이버보안 책임자를 지정하고 책임부서/연락창구(PoC) 지정 • 관리자와 공무원을 위한 사이버보안 인식제고, 담당공무원 대상 사이버보안 교육훈련 실시 - 정보시스템의 사이버보안 기술 역량 강화에 투자 • 사이버보안 사고 대응계획을 개발하고, 정보시스템에 대한 주기적인 사이버보안 검증, 평가 및 훈련, 국가적인 교육 및 사이버훈련

구분		주요과제
		프로그램에 참여 및 협력 • 단체 및 조직의 지속적인 활동을 보장하기 위해 비상사태 및 데이터 백업 계획을 개발하고, 사이버보안 침해사고 발생 후 시스템의 정상적 활동을 위한 복원 준비
	사이버보안 제품과 서비스 시장 촉진	• 연구개발 및 파일럿 프로젝트를 추진하고, 과학기술 예산으로 국내 사이버보안 제품 개발 • 사이버보안 분야 중소기업을 위한 인적자원 투자 촉진, 교육 및 역량 강화 지원 • 국제거래 홍보, 시장 확대, 브랜드 개발을 지원하고 베트남 브랜드의 사이버보안 제품 및 솔루션의 사용 장려 • 일부 국내 사이버보안 제품 및 서비스에 대한 개발 지원 - 사회경제적 활동에서 공공 전자서명 적용을 장려하고, 기업의 사이버보안 서비스의 아웃소싱 강화
기반과제 (Solutions)	정책개발 및 법제정비	• 지속적인 법적 규범 문서 검토 및 발행하고, 사이버보안 법적 체계 마련 • 사이버보안 보장에 직접 관련된 높은 수준의 정책을 개발하여 관리자와 기술자에게 보급
	국내/국제 협력	• 사이버보안을 보장하기 위해 관련 국가기관과 국내외 기업 간의 정보와 경험을 공유하고, 학제 간 협력을 강화하기 위한 메커니즘 개발 • 사이버보안 분야의 지역 및 국제기구, 포럼에 참여하고, 세계 각국, 특히 포괄적 전략적 파트너, 전략적 파트너, 전통적인 베트남 파트너인 국가와의 협력 및 경험 교류 촉진
	인력양성	• 사이버보안 활동을 구현하기 위한 부처 간, 산업 간, 지역 간 운영 및 협력 체계 마련 • 사이버보안 전문가 그룹을 조직하고 유지하여 국가 전반의 사이버보안 대응계획 관련 관할 당국을 지원하고, 자문하며 권고사항 제시 • 교육훈련을 강화하여 베트남의 사이버보안 인적자원 개발
	인식제고	• 사이버보안에 대한 전파, 보급 및 인식 제고, 책임 부여 등의 활동 수행
과제이행 역할분담	정보통신부	• 타 부처, 부문 및 인민위원회, 중앙정부 운영 도시 및 관련 조직 및 단계와 협력하여 사이버보안전략 적용, 촉구, 주기적 이행평가 등 수행하며, 이행 결과에 대해 총리에게 보고하고, 필요할 경우 사이버보안전략의 내용을 수정하거나 추가 권장 • 집행위원회를 조직하여 정보통신부의 관리자들과 함께 사이버보안 조정, 촉구, 검사, 지침 제공 등 수행 - 집행위원회 위원장과 상임위원회는 정보통신부의 비상설 조직으로 구성 • 국방부와 공공안전부와 협의하여 부처, 산업, 지방의 사이버보안 연례 점검을 위한 학제적인 실무그룹을 구성하고, 부처, 부문 및 기업과 협력하여 악성코드에 대한 분석 및 대응을 위한 신속한 대응그룹 구성

구분		주요과제
		• 베트남 정보보안협회와 협의하여 정보보안 제품 및 서비스의 품질을 분류 및 평가하고, 매년 조직 및 단체의 사이버보안 수준을 조사 및 평가
	공공안전부	• 공공안전부의 활동에서 사이버보안 수행 • 부처 담당 기능과 의무에 따라 국가의 중요한 정보시스템에 대한 사이버보안을 수행하기 위해 관련 기관과 협력
	국방부	• 국방부의 활동에서 사이버보안 수행 • 부처 담당 기능과 의무에 따라 국가의 중요한 정보시스템에 대한 사이버보안을 수행하기 위해 관련 기관과 협력 • 암호에 관한 법률의 규정에 따라 정치 조직과 단체의 사이버시스템에 대해 특수한 전자서명 및 정보보안 적용을 장려하기 위해 정보통신부 및 관련 부처 및 부문과 협력 • 관련 단체와 협력하여 국가 조직 및 단체의 주요 정보기술 네트워크의 정보보호 감시시스템을 효과적으로 보급
	과학기술부	• 과학기술부는 정보통신부와 협력하여 관련 업무 수행
	재무부 및 기획투자부	• 재무부, 기획투자부는 사이버보안전략 과제를 수행하기 위한 규정에 따라 국가예산, 반복 지출, 개발 투자 지출의 균형 유지
	중앙 및 지방의 기관	• 지정된 부처, 부문 및 지방의 관리 하에 국가의 중요한 정보 시스템에 대한 사이버보안을 수행하기 위해 정보통신부, 공공 안전부 및 국방부와 협력 • 경영진의 관리 하에서 그룹, 기업 및 기업의 정보통신시스템, 산업제어시스템 및 기업이 관리, 운영 및 이용하는 기타 중요한 정보시스템에 대한 사이버보안 강화 검토, 평가, 조치 수행 • 부처, 산업 및 지역의 활동에서 사이버보안을 보장하기 위한 업무를 수행하며, 사이버보안 활동을 정보기술 애플리케이션, 전자정부시스템 개발 등과 연계 • 담당하는 기능과 의무에 따라 사이버보안전략에 명시된 관련 활동을 수행하기 위해 정보통신부와 협력
	정당, 대통령실, 의회, 법원원 등	• 정당, 대통령실, 이회, 법원 등은 해당 조직에 관련된 사이버보안 업무 수행 • 당중앙사무국, 대통령실, 국회실, 최고인민법원, 국가감사원, 베트남 조국전선 중앙위원회, 베트남 노동총연맹, 호치민 공산주의 청년연합중앙위원회, 베트남농민협회, 베트남 전쟁 참전용사협회, 베트남 여성연합중앙위원회는 사이버보안전략 내용에 따라 조직과 단체에서 사이버 보안을 수행
	정보보안, 정보처리, 인터넷,	• 정보통신부 당국과 협력하여 사이버보안전략 내용을 이행 • 사이버보안에 대한 제품 및 서비스 및 솔루션을 적극적으로 연구, 개발, 생산 및 제공하기 위해 회원 및 기업의 참여를 독려하고, 기업의

구분		주요과제
	전자거래 등 관련협회	사이버보안에 제품, 서비스, 솔루션을 우선 사용하도록 기관과 조직에게 권장
	통신사, 인터넷서비스공급자 등 정보통신 관련 기업	• 정보기술 및 통신 분야에서 운영되는 그룹, 기업, 국유기업, 통신기업, 인터넷서비스를 하는 기업 등은 사이버보안전략 내용에 따라 기업 활동에서 사이버보안 활동 수행

2) 담당기관

▶ 공안부(Ministry of Public Security)

- 공안부는 인민 공안군(People's Public Security Forces)의 산하 기관으로 국가 보안과 사회 질서 유지를 담당
- 인민 공안군은 인민 보안군(People's Security Force)와 인민 경찰(People's Police Force)로 구성
- 또한 공안부 산하 기관으로는 중심 운영 도시 담당 안보 부서, 지역 안보 사무실, 최소 행정구역 담당 안보 사무실 등이 있음
- 베트남 내 물리보안 분야의 정책을 총괄하며 당과 국가에 국가 안보 정책 건의, 사회 질서 및 안전 유지, 폭동 예방 및 각종 범죄 예방을 담당

▶ 정보통신부(Ministry of Information and Communications, MIC)[100]

- 통신 및 IT 부문을 책임지며 산업 규제에 주요한 역할을 담당하고 있으며, 2007년 MPT가 MIC로 되면서 역할이 확장되어 TV 및 방송 부문까지 커버함
- MIC는 정책 결정 및 규제 기관으로 설립되었으며, 언론, 출판, 우편, 통신 및 인터넷, 전송, 라디오 주파수, 정보기술, 전자 기기, 방송 및 국가 정보 인프라, 정부를 대신하여 관련된 공공서비스 관리 등의 책임을 가짐
- 정보기술, 전자기기 분야에서 IT 산업, IT 사용 및 정보 보안영역이 포함되며 정보보안에 대한 내용은 다음과 같음
  - 정보 보안을 규제하고 관리함: 정보 시스템과 인터넷에 대한 정보 보안을 보장, 정보 기술

100 정보통신부(MIC) 홈페이지: english.mic.gov.vn

애플리케이션의 운영에 대한 정보 보안 보장, 스팸 방지, 전국적인 컴퓨터 문제해결의 관리, 조정을 조직함

- 정보보안 제품 및 서비스의 생산, 판매, 수입 및 수출을 규제하고 관리, 정보보안에 대한 라이선스를 인증, 평가 및 발급함
- 정보보안 보장을 위한 시스템 구축 및 운영, 정보보안에 대한 교육, 육성, 인식 제고

• 또한 정보통신 인프라 분야에 관련된 정보보안 내용은 다음과 같음

- 정보통신 인프라에 대한 정보보안 보장에 관한 지침을 제공하고 법적 규칙을 구현함
- 정보통신 인프라에 대한 보안보증 및 안전에 대한 솔루션을 보급하며, 공유 정보 및 통신 인프라 사용에 대한 메커니즘, 정책, 규정을 제공함
- 장비, 통신 인프라의 안전을 관리하고, 통신 및 정보기술 분야에서 국가 안보와 관련된 주요 작업에 대한 정보보안을 보장하기 위해 공안부(Ministry of Public Security), 국방부(Ministry of National Defense)와 협력함

▶ 베트남 컴퓨터침해사고대응팀(Vietnam Computer Emergency Response Team, VNCERT)

• 베트남 통신법 제339항에 의해 설립된 베트남 컴퓨터침해사고대응팀은 자국 내 인터넷 네트워크 및 컴퓨터 보호 업무 담당
• 2005년 12월 20일, 베트남 정보통신부(Ministry of Information and Communication)의 직속 산하 기관으로 설립
• 베트남의 네트워크 보안 경고, 컴퓨터 보안 기술 표준 개발 및 조정, 공공기관 또는 기업의 중앙 컴퓨터침해사고대응팀 지원 담당
• 또한 컴퓨터 네트워크 보안 위험 감지 및 조기 경보 기능 수행, 인터넷 안전과 관련된 정보 수집 및 컨설팅 업무 수행하며, 이외에도 외국 컴퓨터 비상 대응(CERT) 기관과의 협력을 통한 컴퓨터침해사고대응팀 구축 담당
• VNCERT는 자국의 디지털 주권과 정보보안을 확립하기 위해서 자국 제품의 점유율이 50%를 달성해야 하며, 이를 위해 자국 정보보안 기업들에 Symantc, Kaspersky, McAfee 등 글로벌 벤더들과 경쟁할 수 있도록 세제 상 인센티브를 제공할 것을 제안

▶ 베트남 정보보안협회(Vietnam Information Security Association, VNISA)

• VNISA는 2011년 11월 17일, 정보보안 산업의 진흥을 위한 비영리 정보보안 기관으로 설립
• 협회 회원은 정부기관 책임자, 은행 및 재무 관련 회사 대표, 통신사 대표, 솔루션 제공업체, 정보보안 분야 종사자, 컨설턴트, 보안 전문가 등 각 분야 전문가로 구성
• 보안 인력 양성, 국가 단위 정보 보안 대회, 컨퍼런스 및 세미나 개최, 정보 보안 관련 설문조사 수행, 정보보안 발전과 협력을 위한 기관 및 사업체간 회의 개최 등을 담당하며, 이외에도 정보 보안 컨설팅

서비스를 제공

▶ 베트남 정부정보보안위원회(Government Information Security Commission, GISC)
- 국방부(Ministry of National Defence) 산하 특별 기관으로서 국가 안보와 관련된 국가 기밀 정보보호를 담당하며, 각 정부 기관에 전자 서명을 발행하는 유일한 기관
- 베트남 정부정보보안위원회(Government Information Security Commission, GISC)는 2012년 6월부터 2015년까지 15만 건의 디지털 서명을 발행했으며, 이는 정부 기관 간의 온라인 거래 시 보안 강화를 위한 조치

▶ 네트워크보안국(Department of Network Security)
- 2014년 9월 인터넷 보안을 강화하기 위해 하노이에서 공식 설립된 기관으로, 네트워크 보안 관련 기관의 보안 기준을 종합적으로 개선하는 것을 핵심 목표로 함

3) 규제 및 인증제도

▶ 베트남 기업의 소프트웨어 및 보안 인증은 금융 및 IDC 분야에 국한 적용
- 베트남 정보통신부의 최근 조사에 의하면, 자국 내 10대 소프트웨어 기업조차 소프트웨어 인증에 대한 필요성 절감하지 못하고 있는 상황
- 로컬 시장에서 활동하는 기업들 중 불과 1%만이 ISO 27001 표준을 준수하고 있으며, 이 중 대부분은 은행, 금융기관 및 데이터센터에 집중

▶ 열악한 재무 환경과 보안 전문가 부재가 베트남 인증 확산의 주요 걸림돌
- 베트남 내 소프트웨어 및 보안 인증 보급이 더딘 배경으로는, 인증 채택 시 수반되는 베트남 기업들의 재무적인 부담과 베트남 내 ISO 표준 전문가가 거의 전무한 상황을 꼽을 수 있음
- 특히, ISO 27001 준수를 위해서는 외국으로부터 전문가를 영입해야 하는 상황

▶ 베트남 정보통신부는 현상 타개를 위해 ISO/IEC 27001:2005 표준 전문가 양성 프로그램에 착수
- 베트남 정보통신부는 2013년 2월, 자국 내 소프트웨어 기업의 ISO 27001 인증과 소프트웨어 품질 보증 기준의 하나인 CMMI(Capability Maturity Model Integration) 획득을 지원하기 위해 1백만 달러의 자금 지원 계획 발표
- 향후 ISO 27001 적용 기업에게는 매 기업 당 최대 2만 달러까지 지원 계획

- 베트남 정보통신부는 2014년까지 CMMI/소프트웨어 개발과 ISO 27001 인증 확산을 위해 각각 18개의 연수 프로그램을 출시할 계획으로, ISO 27001의 경우 40개 기업에 대해 인증 획득을 지원 예정

▶ 한편, 글로벌 인증 에이전시 SGS가 1989년부터 베트남에 진출해 영향력을 발휘하고 있으며, 보안과 관련해서는 ISO 20000 기반의 인증 제도를 지원하고 있음

- ISO 20000(IT 전반에 대한 인증), ISO 22301(비즈니스 지속성 관리), ISO 27001:2005(정보보안 관리 시스템), ISO 28000(공급체인 보안 관리 시스템), ISO 31000(위기관리), ISO 50001(에너지 관리 시스템), ISO 9001(품질 관리 시스템) 등의 인증을 지원

표 _ SGS Vietnam 기본 정보

회사명	SGS Vietnam Ltd.
주소	SGS Building 119-121 Vo Van Tan, District 3 Ho Chi Minh City, Vietnam
연락처	Tel: 848 3935 1920 Fax: 848 3935 1921
홈페이지	http://www.sgs.vn/

4) 최근 정책 동향 및 이슈

▶ 베트남 정보통신부와 프랑스 디지털 사무국과의 회의 (2019.10)

- 정보통신부 차관과 프랑스 디지털 사무국장과의 회의에서 정보기술 및 사이버보안 분야에서 프랑스와 베트남 간의 양자 협력에 대해 높이 평가함
- 베트남과 프랑스 양측은 베트남의 전자정부 건설, 디지털 혁신, 디지털 경제 개발 및 정보보안과 관련된 내용에 관심을 갖고 개발을 위한 안전한 환경을 조성하고 있음
- 베트남 정보통신부는 프랑스와 같은 전자정부 및 사이버보안 구축의 주요 국가 출신인 국제 경험이 풍부한 파트너와의 협력 활동을 환영하고 지원하며, 이번 회의를 통해 양국은 디지털 혁신과 사이버 보안 분야에서 베트남과 프랑스간의 협력을 계속 강화하길 희망함

▶ 베트남 정보통신부와 일본 국제협력기구(JICA)는 베트남의 정보보안 및 법 집행 능력 보호에 대한 인식과 기술을 높이는 프로젝트를 지원하기 위해 공동 조정위원회의 첫 번째 회의를 개최 (2019.9)

- 일본 국제협력기구(Japan International Cooperation Agency, JICA) 베트남 사무소 대표이사와 일본대사관 대표, 일본 사이버 보안 전문가들이 이 회의에 참석함
- 또한 최근 몇 년간 베트남 정보통신부의 사이버보안 부서는 일본측과 긴밀히 협력하여 경험을 공유했으며, 특히 베트남의 정보보안에서 법 집행 역량 및 정보보호에 관한 인식 및 스킬을 높이는 프로젝트에서 경험을 공유했음
- 이번 회의에서 양측은 프로젝트 이행 과정을 보고하고 어려움과 아이디어 및 해결책을 교환했음

▶ 베트남 정보통신부와 캄보디아 우정통신부는 상호협력을 위한 협약 체결 (2019.3)

- 베트남 정보통신부(MIC) 장관과 캄보디아 우정통신부(MPT) 장관은 캄보디아 프놈펜에서 양자회담을 가진 후 우정/통신 서비스, 사이버보안, 디지털서명 등 3개 부문에서의 상호협력을 위한 협약 체결
- 동 협약을 기반으로 향후 베트남 정부는 캄보디아의 사이버보안 모니터링 센터 설립을 지원하고, 캄보디아 우정/통신 기술연구소 학생을 대상으로 총 27,000 달러 규모의 장학금을 제공할 예정임
- 캄보디아 정부는 베트남 IT기업들의 캄보디아 시장진출 확대를 위한 지속적인 지원 및 투자를 약속함
- 양국은 앞으로 전자상거래, 전자정부 및 스마트시티 개발은 물론 사이버보안 분야의 인프라 확충 및 생태계 구축을 위한 협력을 지속해 나가기로 합의함

▶ 베트남 사이버보안법 시행령안 발표(2018.11)

- 베트남 공안부(Ministry of Public Security)는 2018년 6월 신규 제정된 사이버 보안법의 시행(2019년 1월 1일)을 앞두고 세부사항들에 관한 시행령(안)을 발표
- 시행령안의 주요 내용은 다음과 같음
- 서비스제공자인 기업이 저장/보관해야 하는 정보 규정

<table>
<tr><th>정보의 유형·종류</th><th>저장기간</th></tr>
<tr><td>• 성명, 생년월일, 출생지, 국적, 직업, 직위, 거주지, 이메일주소, 전화번호, 신분증 번호, 개인식별번호(가족등록번호 대신), 시민권 번호, 여권번호, 사회보장카드번호, 신용카드번호, 건강 상태, 의료 기록 및 생체인식정보 등 이용자의 개인정보</td><td>서비스 종료시까지 (최소 12개월)</td></tr>
<tr><td>• 모든 종류의 장치에서 업로드, 동기화 또는 가져오기를 통해 생성되는 정보</td><td rowspan="2">서비스 종료시까지 (최소 36개월)</td></tr>
<tr><td>• 친구, 연결그룹 등 이용자의 관계 정보</td></tr>
</table>

- 사이버보안법 적용대상 기업 규정: 통신 네트워크, 인터넷을 통해 베트남의 고객에게 서비스를 제공하는 국내외 모든 기업
  - 전기통신서비스, 호스팅서비스, 국내·외 도메인네임 제공, 전자상거래, 온라인결제(중개결제 포함), 운송서비스, 소셜네트워킹/미디어, 온라인 비디오게임, 이메일서비스

- 기업은 공안부 장관의 요청을 받은 날부터 12개월 내 베트남에 지사 또는 대표사무소를 설립하고 데이터를 보관해야 함

• 사이버 상에서의 불법 콘텐츠 및 행위 규정

불법 콘텐츠 및 행위 유형	관련조항
• 반국가적 선동, 역사 왜곡, 성 차별, 종교적 범죄, 인종차별, 허위정보 게시, 인신매매 등 금지행위 • 네트워크 테러, 사이버 범죄, 국가 안보에 중요한 정보 시스템에 대한 네트워크 공격	제8조
• 베트남 공산주의에 반하는 정치선전, 폭력적 소요 유발, 치안 방해 또는 공공질서 교란 • 명예훼손 또는 비방 • 경제적 관리 명령 위반	제16조
• 사이버 간첩행위, 국가기밀 유출 • 업무/영업/개인/가족 비밀 및 사생활 침해	제17조
• 국가안보, 공공안전 및 질서를 위반하는 정보기술 또는 전자적 수단의 사용	제18조
• 사이버 공간에서의 아동 보호에 위반되는 행위	제29조

• 저장할 이용자 정보의 기간범위 및 정보의 국외이전 제한과 같은 문제는 추가 후속 시행령 등을 통해 구체화 될 예정

▶ 사이버보안에 중점을 두는 베트남 전자정부 (2018.8)[101]

• 베트남 총리 응우옌 쑤언 푹(Nguyen Xuan Phuc)은 전자정부의 IT 서비스 및 사이버 보안을 감독하는 프로젝트를 허가함

• 베트남 컴퓨터침해사고대응팀(VNCERT)이 운영하는 국가 사이버보안 모니터링 센터, 주요 지방과 도시, 인터넷 서비스 제공업체들이 사이버 공격에 대응하는 능력을 2025년까지 보강하는 것이 프로젝트 목적

• 장관급과 지역구 책임자들은 전자정부 시스템을 이해하는 사이버보안 인력을 육성해야 함

• 사이버보안 위기가 발생할 경우 모든 부처들은 협력 및 정보를 공유하여 최고 책임자인 총리에게 보고하는 시스템을 갖춰야 함

• 모니터링 시스템은 6개월에 한 번씩 검사할 예정

• 2018년 4월 23일에 발표된 Government's Decree No61/2018/ND-CP는 행정절차를 다루는 단일 창구 메커니즘의 이행에 관한 내용으로, 각 부처, 부문 및 지역은 시민과 기업이 편리하게 이용할 수 있는 단 하나의 집중된 온라인 포털을 제공해야 함

101 Vietnamnews, "e-Gov't focuses on cyber security", 2018.8.17.

▶ ASEAN-Japan 사이버보안 훈련을 개최한 베트남 (2018.5)[102]

- ASEAN-Japan 사이버보안 훈련에 100여 개의 IT업체, 정부부서 등에서 온 300여 명의 대표단과 기술진들이 참가함
- 정보통신 부차관보 응우옌 탄 흥(Nguyen Thanh Hung)은 분산 서비스 거부(DoS/DDoS) 공격은 날마다 증가하고 있으며, 이에 대비한 정보보안 훈련이 정기적으로 조직되어야 한다고 밝힘
- 이 훈련은 국제 기관, 국내 기관, 핵심 부서간의 공조가 목표이며, 이중 핵심 부서들이 직간접적인 공격을 제일 많이 받으므로 이에 대비하는 것이 핵심

▶ 베트남과 한국 정부, 전자정부 MoU 체결 (2018.5)[103]

- 2018년 5월 전자정부 협력 강화를 골자로 한 MoU 체결
- MoU 체결에 앞서 전자정부 협력회의를 통하여 전자정부 인프라 정비, 국가 데이터센터 구축, 데이터베이스 통합 및 표준화, 사이버보안 관련 경험 공유 등을 논의함
- 정부 청사 장관 마이 티엔 둥(Mai Tien Dung)은 대한민국의 전자정부 전략과 해결책을 배우기를 원하며, 양측이 정보를 교환하고 장기적이고 효과적인 협력을 기대한다고 밝힘

▶ 베트남 정부는 사이버보안법 위반 관련으로 페이스북과 갈등 고조 (2018.2)

- 베트남 정부는 페이스북에 반정부 활동 페이지에 대한 삭제를 요청했으나 페이스북은 해당 콘텐츠가 커뮤니티 규정을 위반하지 않았다는 이유로 거부하였고, 보안기관의 '사기계정(Fraudulent Accounts)' 정보 제공 요청도 거부함
- 정보통신부 장관은 페이스북이 반정부, 음해 및 명예훼손 관련 게시물을 허용하고 있으며, 베트남 사이버보안법과 인터넷 서비스 이용에 관한 규정을 심각하게 위반하는 것이라 비난함
- 페이스북의 행위에 대한 위법여부 판단이 추후 이루어질 예정이며, 정보통신부는 페이스북의 플랫폼 광고수입(2018년 약 2억 3,500만 달러)에 대해 세금을 부과하는 것도 고려함

5) 정보보호 스타트업 관련 정책동향

▶ 베트남은 IT 중점 지역 19개 추가 확보[104]

---

102 VOV, "Vietnam hosts 2018 ASEAN-Japan cyber security", 2018.5.24.
103 보안뉴스, "한국 전자정부, 베트남 시작으로 신남방지역 본격 진출", 2018.5.25.
VOV, "RoK helps Vietnam build e-government system", 2018.5.25.

104 BuddeComm, Vietnam – Telecoms, Mobile and Broadband - Statistics and Analyses , 2019.5.29

- 베트남 정부는 IT개발에 대한 마스터 계획(20205년을 향한 비전을 갖고 2020년까지)을 준비하였으며, 이 계획에 따라 베트남은 IT 중점 지역의 19개를 추가함
- 2014년 8월까지 IT 중점 지역의 구축을 10년 동안 수행한 후 베트남은 7개 지역(사이공 하이테크 파크, 사이공 소프트웨어 파크, Quan Trung 소프트웨어 파크, 하노이 IT 훈련 센터, 다낭 ICT 인프라 개발 센터, 호치민 시의 IT 파크의 국립 대학교, Can Tho 대학교 소프트웨어 센터)이 있음
- 이 부문은 디지털 콘텐츠 서비스, 비즈니스 프로세스 아웃소싱(BPO), 해외 시장에 아웃소싱, IT 인력 교육 및 공급, 데이터센터 구축 및 관리, 임베디드 제품 및 국내 소프트웨어 비즈니스 컨설팅 및 인큐베이션이 포함됨
- Quang Trung 소프트웨어 파크는 미국, 일본 및 여러 유럽 국가를 포함하여 20개 국가에 108개 IT 비즈니스 아웃소싱이 가장 두드러지며, 이 파크는 2013년 총 매출에서 약 2.9조 동(VND)으로 2012년 대비 36% 증가함

▶ 베트남 정부가 최근 현지 스타트업 시장 활성화를 위해 Vietnam Silicon Valley 같은 엑셀러레이터 및 인큐베이터 프로그램을 마련[105]

- 베트남 내 과학기술분야 기업은 특정조건하에 법인 설립후 4년간 법인세가 면제되며 이후 9년간 50% 감면받을 수 있음
- 베트남 기획투자부는 '4차 산업혁명 국가전략' 초안을 통해 현지에서 유니콘 기업을 2025년까지 5개, 2030년까지 총 10개를 만들겠다는 목표를 제시함

105 베트남 스타트업 화두는 "Tech", Kotra 해외시장뉴스, 2019.8.22.

융합보안시장 및 정책 동향

1) 융합보안 시장 현황

사물인터넷(IoT)

▶ 일본 통신그룹 KDDI의 베트남 사업부는 북부 항구 도시 Haiphong의 산업 지역에 LoRaWAN 네트워크 기술 기반의 스마트 계량 시스템(smart metering system)을 구축할 계획을 2018년 5월에 발표[106]

- KDDI 베트남은 LoRaconnected 파워 미터를 통해 실시간 원격 모니터링을 구현하여 약 4km 떨어진 LoRa 게이트웨이로 데이터를 전송하여, 미터를 읽고 하드웨어 작동 상태를 확인하기 위해 현장을 방문할 필요가 없게 됨

스마트시티

▶ 통신사 Viettel은 첫 5G 서비스 제공을 호치민 시에 시작하여 사물인터넷 인프라 운영을 시작함(2019.9)[107]

- Viettel은 호치민시 10지구의 12구에서 시험적으로 5G 네트워크를 공식적으로 제공하며, 수백만 개의 IoT 장치를 연결하는 커버리지 영역을 만들어 운송, 전기, 수도, 애플리케이션 및 서비스와 같은 모든 사회 활동을 지원함
- 호치민시는 10,000개 이상의 정보기술 사업이 있으며 5G 애플리케이션은 기업이 서비스를 개발할 수 있는 기회를 제공할 것으로 기대하며, 하이테크파크와 IT비즈니스가 있는 Quang Trung 소프트웨어 파크, 5G 애플리케이션이 필요한 대학 등의 영역에 5G 애플리케이션의 점차적인 확장을 요구함
- Viettel은 9월내에 하노이에서 NB-IoT 커버리지를 완료하고, 향후 2년내에 전국의 모든 지역으로 확장할 계획임
- 호치민시는 2019년 상반기동안 도시의 전자정보 기술산업이 28% 이상 성장하여 산업 부문의 성장보다 4배 증가하였음

▶ 스마트 시티 민간 협력 부문[108]

---

106 BuddeComm, Vietnam – Telecoms, Mobile and Broadband - Statistics and Analyses , 2019.5.29
107 정보통신부 뉴스(VNISA), HCM City becomes first locality in Vietnam to get 5G service, 2019.9.23

- VNPT와 Mocrosoft는 2017년 12월 호치민시와 하노이에 스마트시티 개발 플랫폼을 공동으로 구축하기 시작함
- 또한 글로벌 ISP인 Trilliant Networks는 호치민시 전력공사(EVN HCMC)와 파트너 관계를 맺고, Saigong HiTech Park에 베트남 최초의 스마트 시티 통신 플랫폼 파일럿을 구축함
- 호치민 시 2지구내에 한국의 롯데 그룹이 자금지원하는 Thu Thiem Eco Smart City 프로젝트는 무역 및 금융 센터, 호텔, 오피스 타워, 서비스 및 주거용 빌딩을 갖춘 7.4ha 프로젝트임
- 하노이에서 Microsoft는 전자정부, 헬스케어, 교육, 관리를 위한 데이터 수집과 같은 스마트 도시를 위한 기술 개발에서 도시를 지원하기 위한 협력각서에 서명하였으며, Viettel, VNPT, FPT 그룹, Nhat Cuong와 같은 현지 회사들도 이 계획에 지원함
- 하노이를 스마트시티로 개발하는데 추정되는 예산은 2018년에 약 30억 달러임
- 2019년에 40억 달러 이상의 가치가 있는 하노이의 Dong Anh지역의 스마트시티 건설이 시작되었으며, 베트남의 BRG그룹과 일본의 Sumitomo 기업, 일본의 Nikken Sekkei Architecture 기업간의 조인트 벤처가 310헥타르 도시 설계를 담당하였음

핀테크

▶ Standard Chartered Bank는 모바일 지갑을 이용한 결제를 베트남에서 시작[109]

- Standard Chartered Bank는 M_Service가 운영하는 모바일 머니 서비스인 MoMo와 제휴하여 Straight2Bank Wallet 결제를 베트남에서 시작하였으며, 회사, 정부 및 개발 조직을 이것을 사용하여 은행 및 비은행 개인과 현금 없이 거래할 수 있음
- M_Service는 비은행 인구를 위한 모바일 지갑을 제공하는 State Bank of Vietnam이 허가한 베트남 최초의 회사임

▶ 통신사 VNPT는 전자결제 수단인 EPAY를 통해 국제 송금 서비스 제공[110]

- 통신사 VNPT는 VNPT의 EPAY를 BICS 글로벌 송금 허브와 연결을 통해 고객에게 국제 송금을 허용하는 서비스를 제공
- 이 협력을 통해 VNPT의 EPAY는 베트남 최초로 모바일 기반의 해외 결제 서비스를 도입한 것에 해당함
- 이전에 VNPT EPAY는 국내 시장으로 제한되어 6개 지역 은행과의 관계를 유지했으며, BICS와의 거래를 통해 영국과 벨기에 사람들은 베트남에 있는 VNPT 가입자의 모바일 지갑에 거의 즉시 자금을 송금할 수 있으며, 이 서비스는 주로 해외에서 일하는 베트남인을 대상으로 함

---

108 BuddeComm, Vietnam – Telecoms, Mobile and Broadband - Statistics and Analyses , 2019.5.29
109 BuddeComm, Vietnam – Telecoms, Mobile and Broadband - Statistics and Analyses , 2019.3.1
110 BuddeComm, Vietnam – Telecoms, Mobile and Broadband - Statistics and Analyses , 2019.3.1

- 새로운 서비스에 의해 부과되는 전송요금은 국가마다 다르지만 일반적으로 전통적인 송금 서비스에 의해 청구되는 것보다 낮음

자율주행차

▶ 베트남 FPT 그룹, 베트남 최초의 자율주행 운행에 대한 승인을 교통 당국에 허가 요청[111]
- 베트남 최초의 자율주행 자동차 파일럿 프로젝트에 해당하며, 시험 운전 중 교통 보안에 대해 책임을 지도록 지시 받음
- 미국 자동차 기술자 협회의 분류에 따르면 자율 주행 시스템 단계 중 2단계에 해당하는 것으로, 자율 운행 기능이 완벽히 작동하지만, 시스템이 작동하지 않을 경우를 대비하여 1-2명의 운전자로부터 부가적인 도움이 요청되는 상태를 뜻함

▶ 베트남 FTP 그룹은 일본 야마하 모터, 베트남 도시개발업체 에코파크와의 제휴로 자율주행 전기자동차 개발에 착수[112]
- 자율주행차 기술 도입 가속화 및 베트남 향후 대중교통의 비전 실현을 목표로 함
- 인공지능과 레이다 기술을 사용하는 야마하 전기 골프카트로부터 자율주행 소프트웨어를 개발할 예정으로, 에코파크는 물류 및 효율적인 인프라를 제공하며 야마하는 도로 자율주행 테스트 중 기술 지원 및 차량 컨설팅을 제공

2) 융합보안 정책 현황

사물인터넷(IoT)/스마트팩토리

▶ 당 중앙위원회의 경제위원회 회장은 산업 4.0에 대한 결의 발표를 통해 정부의 적극적 참여 계획[113]
- 2019년 10월 3일 베트남 하노이에서 열린 산업 4.0 정상회의(Industry 4.0 Summit 2019)와 국제 박람회에 2,500명의 정부 지도자, 대사관, 국제기구, 지역 및 기업 대표자들이 참여하였으며, 해당 행사는 당 중앙위원회의 경제위원회, 정보통신부, 산업통상부, 베트남 은행 및 기타 관련 부처와 기관이 공동으로 개최
- 당 중앙위원회의 경제위원회 경제위원회의 의장은 베트남이 그 동안 디지털 기술로 인해 생산, 비즈니스, 문화, 사회생활, 국방 및 안보를 포함한 거의 모든 부문에 중대한 변화가 있었고, 디지털

111 https://kr.saigoneer.com/%ED%85%8C%ED%81%AC/11982
112 http://www.irobotnews.com/news/articleView.html?idxno=16904
113 Viet Nam News, Việt Nam ready to embrace Industry 4.0, 2019.10.4.

경제 규모도 크게 성장하였음을 언급함

- 산업 4.0에 참여를 통해 베트남의 경제 성장에 긍정적인 결과를 가져올 것을 기대하며, 당과 국가는 모든 수준과 부문에 과학, 기술 및 혁신의 적용을 장려하고 산업 4.0에 적극적으로 참여하는 연구활동을 강화하도록 지시했음
- 포럼에서 의장은 Politburo의 결의(No. 52-NQ/TW)를 발표했으며, 이 보고서는 산업 4.0에 적극적으로 참여할 수 있도록 다양한 지침과 정책으로 발표되었음
- 이 결의에 따라 국회, 정부, 부처 및 부문, 지방자치단체가 구체적인 프로그램을 구현하는데 공동으로 참여하여 전국적으로 산업 4.0을 추진할 계획임
- 이를 통해 베트남 정부는 2025년까지 글로벌 혁신 지수(GII) 순위에서 3대 아세안 국가에서의 지위를 위해 노력하고 디지털 경제는 GDP의 약 20%, 노동 생산성은 평균 7% 증가시키고자 함
- 또한 2030년까지 GII 순위에서 세계 40대 국가 중 하나가 되며, 디지털 경제는 GDP의 30% 이상, 노동생산성은 평균 약 7.5%까지 증가시키고자 함
- 정부는 산업 4.0 속도를 높이기 위해 최근 산업 4.0에 대한 국가 디지털 혁신 프로그램을 작성했으며 승인을 위해 총리에게 제출되어 올해 발표될 것으로 예상함
- 정부는 또한 모든 지역의 긴밀한 참여가 필요한 생산 모델 및 신제품에 대한 시범 산업 4.0 프로젝트를 발표할 것이라고 밝힘

스마트시티

▶ 건설부(MoC)는 스마트시티 개발 계획을 제안[114]

- 건설부(Ministry of Construction, MoC)의 도시개발부(Urban Development Department)는 2030년까지 비전을 갖고 2025년까지 스마트시티 개발 계획을 2018년 제안함
- 2020년까지 적어도 세 개의 스마트시티를 갖기 위해 정부 또한 디지털 산업, 스마트 관광, 스마트 농업 및 통신 인프라의 개발에 우선순위를 두는 정책을 시작함

▶ 호치민시는 2018년 베트남 최초의 스마트시티가 됨[115]

- 2018년에 호치민시는 클라우드 컴퓨팅 인프라, 빅데이터, 데이터 웨어하우스/데이터센터 및 보안 모니터링 센터 구축, 2020년 목표를 달성하기 위한 오픈데이터 생태계 개발에 중점을 둔 베트남 최초의 스마트시티가 되었음
- 또한 도시는 건강관리, 식품 안전, 교육, 교통 관리, 홍수 통제, 법 집행에 스마트 솔루션을 도입할 계획임

114 BuddeComm, Vietnam – Telecoms, Mobile and Broadband - Statistics and Analyses , 2019.5.29
115 BuddeComm, Vietnam – Telecoms, Mobile and Broadband - Statistics and Analyses , 2019.5.29

- 호치민시 인민 위원회(People's Committee)는 2018년 Can Gio 지구를 스마트 도시 지역으로 개발할 계획을 발표했으며, 도시의 모든 지구는 2020년까지 스마트 개발 계획을 가질 것으로 예상됨
- 양해각서가 체결되었으며, Can Gio에 대한 파일럿이 1, 12지구, 2지구의 Thu Thiem지역에서 시작되었음
- 또한 2018년 미국 상공 회의소는 호치민시 정부와 국제 금융 공사(International Finance Corporation, IFC)간의 협력을 통해 스마트시티 시스템, 특히 2, 9지구와 많은 양의 제조 및 기술이 현재 집중화되고 있는 Thu Duc 개발을 위한 편드에 PPP(Public-Private-Project) 방식을 도입
- 또한 도시는 교통 혼잡을 완화하고 배출량을 줄이며, 교통 안전을 개선하기 위해 Thu Thiem과 같은 새로운 도시 지역에 스마트도시 교통 네트워크를 계획함

▶ 하노이는 2030년까지 스마트시티가 되는 것을 목표로 의료, 교육, 교통 및 관광의 4가지 주요 부문에 중점을 둠[116]

- 이미 주차장을 검색하여 모바일 기기를 통해 요금을 지불할 수 있는 주차 시스템을 구현했으며, 2019년 말까지 모든 지역에서 주차시스템을 출시할 계획이며, 또한 대중교통을 관리하기 위한 디지털 교통 지도를 개발하고 있음

스마트의료

▶ 전자 건강 기록 서비스 출시[117]

- 2018년 전자 건강 기록(electronic health record, EHR)이 파일럿 기간 동안 8개 주와 도시에서 구현되고 점차 완성되어 2019년 7월부터 전국 규모로 출시될 예정임
- 전자 건강 기록(EHR)은 출생에서 사망에 이르는 개인의 건강 의료 기록을 관리하는 시스템으로 평생 개인 데이터 관리, 의료 정보 시스템간 데이터 공유 및 기록의 안전, 개인 정보 보호를 보장함
- 2019년까지 하노이는 건강 관리 시스템에 전자 문서를 최초로 도입한 도시가 되며, 9십만개의 기록을 보유함
- 2020년까지 핵심 인프라 및 스마트 애플리케이션 개발에 중점을 두며, 2020~2025년 기간 동안 두 번째 단계인 솔루션 운영에 중점을 둘 것임

핀테크

▶ 베트남 정부 2025년까지 현금 사용률 8% 미만 목표로 정책 추진[118]

116 BuddeComm, Vietnam – Telecoms, Mobile and Broadband - Statistics and Analyses , 2019.5.29
117 BuddeComm, Vietnam – Telecoms, Mobile and Broadband - Statistics and Analyses , 2019.5.29

- 베트남 중앙은행을 비롯한 BSI(Banking Strategy Institute)등이 주최한 '현금 없는 경제'를 주제로 세미나가 2019년 5월 30일 베트남 하노이에서가 개최되었음
- 베트남 중앙경제위원회, 국가 경제위원회, 금융 감독위원회, 세계은행 등 각 유관부서와 국제기관이 참가하여 베트남의 현금 사용 현황에 대한 진단과 향후 방향에 대한 논의가 진행됨
- 베트남 중앙은행에 따르면, 현금 없는 결제는 2018년 기준 총 660만 건의 거래로 전년 대비 242%가 성장하여 거래금액은 19억 달러 규모에 이름
- 주요 현금 없는 결제 수단으로는 인터넷 결제, 전자지갑을 통한 결제, 모바일 결제 등이 있으며, 2018년 기준 사용 건수는 각각 32%, 28%, 25%의 비율을 차지함
- 또한 베트남의 많은 은행들이 지문인식 기술, 생체인식, QR코드, 모바일 POS기술, 토큰화 등을 적용하기 시작함
- 현금 없는 거래를 위한 결재 중개서비스 또한 증가하고 있는 추세이며, 2019년 2월 베트남 중앙은행에서 발표한 지불 결제 사업자로 라이선스 등록된 업체는 총 29개사이며, 현지의 34개 은행과 협력하여 지불 결제 서비스를 제공함
- 한편, 상당수의 베트남 소비자들 사이에서 전자결제의 정보보안에 관한 신뢰도는 여전히 구축되지 않고 있다고 베트남 산업무역부는 전함

그림 _ 베트남의 비현금 수단별 결제 건수 추이

(단위: 건)



[출처] 베트남 중앙은행 자료를 인용한 Kotra 해외시장뉴스(2019.6)

118 Kotra 해외시장뉴스, 베트남, 현금없는 미래를 꿈꾸다, 2019.6.25

마. 캄보디아

'18년 GDP(십억달러)	24.57
'18년 인구수(천명)	16,250

■ ITU 글로벌 사이버보안 지수(Global Cybersecurity Index, GCI)

· 캄보디아의 사이버보안 순위는 131위로 하위권에 속함

국가명	2018		2017		전년대비 증감	
	지수	순위	지수	순위	지수	순위
캄보디아	0.161	131	0.283	92	-0.222	-39
대한민국	0.873	15	0.782	13	+0.091	-2

■ ICT 관련 주요 지수

· 캄보디아의 전반적인 ICT 발전 수준은 하위권을 유지하고 있음

지표명	캄보디아		한국	
	점수	순위	점수	순위
IMD 국가경쟁력지수(2019)	-	-	-	28
IMD 디지털경쟁력지수(2019)	-	-	-	10
UNCTAD 전자상거래지수(2019)	30.8	122	89.4	19
ITU 글로벌 사이버보안 지수(GCI 2018)	0.161	131	0.873	15
UN 전자정부 지수(2018)	0.375	145	0.901	3

■ ICT 관련 주요 통계 (ITU, 2018년 말 기준)

· 캄보디아의 유선통신과 브로드밴드 이용자 수는 미미하며, 이동통신 중심으로 통신을 이용

항목	캄보디아		한국	
	가입자수(천 명)	보급률(%)	가입자수(천 명)	보급률(%)
유선전화	88	0.54	25,907	50.63
유선브로드밴드	166	1.02	21,286	41.60
이동통신	19,417	119.49	66,356	129.67
인터넷 이용률	40.00%		95.90%	

정보보호 산업 개요

1) 보안 환경

정보보안

▶ ITU가 2019년 3월 발표한 'Global Cybersecurity Index(GCI) 2018'에 따르면 캄보디아의 사이버보안 지수는 0.161로, 아시아 지역에서는 27위, 글로벌 순위는 131위로 하위권으로 나타남

- Cisco와 Gartner Research가 2018년 발표한 Global Digital Readiness 지수에서 캄보디아의 지수는 8.6으로, 전 세계 평균인 11.96에 미달하는 하위권을 기록

▶ 캄보디아는 열악한 통신 인프라 환경과 더불어 정보보호에 대한 인식이 매우 낮은 편으로, 사이버 공격도 빈번하게 발생

- 보안업체 Kaspersky에 따르면 2018년 한 해 동안 캄보디아에서 459만 건 이상의 사이버 공격이 발생해 인터넷 사용자의 30.5%가 피해를 입었음
- NTT Communications의 Marith Khi 캄보디아, 라오스, 미얀마 지역 부책임자에 따르면 2018년 11월 디도스 공격으로 캄보디아의 주요 인터넷 서비스 사업자들이 피해를 입어 인터넷 속도가 느려지는 사고도 발생
- 그에 따르면 캄보디아 기업들 사이에서 사이버 보안에 대한 의식이 점차 형성되고 있으나, IT 보안 수준과 기업들의 투자가 더욱 확대될 필요가 있음

물리보안

▶ 물리보안 시장의 경우, 불안한 치안과 건설경기 호황으로 보안제품 수요도 증가하고 있으며, 최근 일반 가정집에서도 무인전자경비 서비스 가입이 증가하고 있는 추세

- 미국 해외안보자문위원회(Overseas Security Advisory Council)의 '2019년 캄보디아 범죄 및 안전 보고서'에 따르면 2018년 현재 범죄행위는 지속적으로 높은 수준을 유지하고 있으며, 무장 강도와 같은 강력 범죄도 수도 프놈펜을 중심으로 빈번하게 발생
- 보안 전문 매체 asmag.com에 따르면 제조업과 기반시설, 관광 시장이 강한 성장세를 보이면서 관련 프로젝트에 투자하는 외국인 투자자들의 보안 수요도 성장세를 보이고 있음

2) 인터넷 및 통신 환경

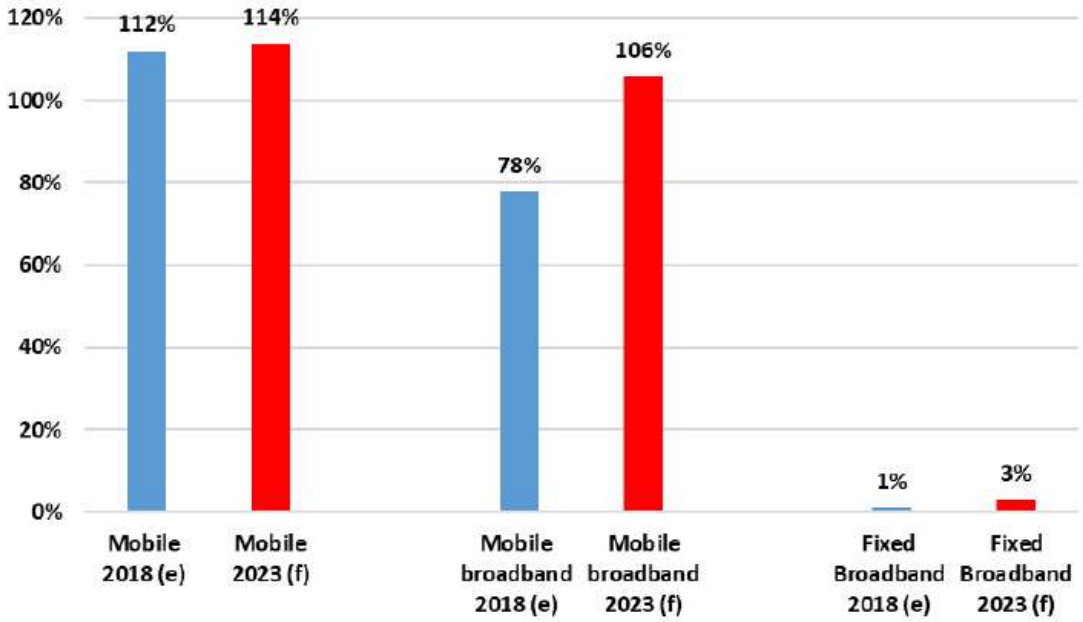
▶ 시장조사기관 BuddeComm에 따르면 2019년 현재 캄보디아는 여타 아시아 국가들과 비교해 매우 낮은 유선 및 유선 브로드밴드 보급률을 기록

- 유선통신 보급률은 모바일 보급률이 확대되며 감소되는 추세로 2014년 2.3%에서 2018년에는 1.2%까지 감소했음
- 유선 브로드밴드의 발전도 매우 낮은 수준으로 지난 5년간 보급률은 소폭 감소해 2012년 0.2%에서 2018년에는 1.1% 수준에 머무름
- 캄보디아 유선 인터넷 시장은 현재 다수의 상용 접속 장비를 사용해 저가로 제공되는 저품질 서비스가 주도하고 있으며, 2019년 기업용 인터넷 사업자 SINET이 전국 규모의 FTTH 네트워크 구축 계획을 밝히며 변화가 예상됨

▶ 캄보디아 이동통신 시장은 2015년 보급률 134%를 기록하며 정점에 올랐으나 이후 시장 포화 및 주요 사업자간 시장 통합, 심카드 등록 관련 규제 강화로 2018년 112%까지 보급률이 낮아짐

- Smart Axiata가 최대 600Mbps의 속도를 지원하는 LTE-A 서비스를 출시했으며, Viettel Cambodia(Metfone)도 2018년 LTE-A(4.5G) 서비스를 출시
- 캄보디아는 현재 5G 서비스 출시를 준비 중으로 2019년 중국 통신장비 업체 Huawei와 5G 인프라 구축 계약을 체결하여, Smart Axiata가 연내 5G 상용화에 나설 계획
- 4G에서도 Huawei 장비를 사용 중인 Smart Axiata는 수도 프놈펜에서 9월 5G 시범 서비스를 개시했으며, 향후 3~5년에 걸쳐 5G에 총 1억 달러를 투자할 계획
- Viettel Cambodia도 2019년 7월 프놈펜에서 5G 장비 설치와 점검을 완료하고 연내 5G 서비스를 출시할 계획
- BuddeComm에 따르면 2023년까지 이동통신 시장은 성장세를 회복할 전망으로, 5년간 1.8%의 연평균 성장률을 기록해 2023년에는 가입자 수 1,990만 명에 보급률 114%를 기록할 것

그림 _ 2018~2023년 캄보디아 모바일, 모바일 브로드밴드 및 유선 브로드밴드 보급률



[출처] BuddeComm(2019.05)

▶ 전자상거래 시장과 관련해, 국제 마케팅 조사업체 'We are Social'에 따르면 2019년 1월 기준 금융기관에 계좌를 보유한 캄보디아 인구는 전체의 22%, 신용카드 보유율은 0.6%, 모바일 머니 계정을 보유한 인구는 5.7%에 불과했으며, 온라인 구매나 결제 비율도 3.8.%에 그쳤음

- KOTRA 캄보디아 무역관에 따르면 2019년 현재 스마트폰 보급과 인터넷 사용 증가, 모바일 결제 시스템의 확산과 전자상거래에 대한 인식 제고 등으로 전자상거래에 유리한 환경이 조성되고 있으나 아직 시작 형성 초기 단계임
- 캄보디아는 아세안 국가 중 유일하게 전자상거래법이 아직 제정되지 않았으나, 정부가 연내 전자상거래법 통과를 목표로 법안을 검토 중에 있으며, 법안이 통과되면 전자상거래 시장이 한층 활성화될 전망

정보보호 시장 현황

1) 시장 규모

정보보안

▶ 캄보디아의 정보보호 시장은 시장 규모도 제대로 파악되지 않을 만큼 낙후되어 있으며, 정보보안 수준을 향상시키기 위한 구체적인 정책이나 법안도 마련되지 않아 당분간 국가적 지원을 통한 성장 가능성은 제한적

- 2018년 11월 NTT Communications의 Marith Khi 캄보디아, 라오스, 미얀마 지역 부책임자에 따르면 사이버보안에 대한 의식 수준이나 투자 부족으로 은행과 정부기관이 종종 사이버 범죄의 주요 표적이 되고 있음
- 금융권의 경우 사이버 위협의 위험을 인식하고 연간 감사 및 침투테스트를 실시하고 있으나 보안에 대한 모니터링과 인적 자원에 대한 투자가 한층 강화될 필요가 있음

▶ 그러나 2016년 IDC에 따르면 캄보디아 소프트웨어 시장에서 향후 5년 동안 보안 소프트웨어 분야는 빠른 성장세를 보일 전망

- 종업원 500명 이상의 현지 대기업들은 IT 지출을 늘릴 의향을 갖고 있으며 IT 서비스 지출 가운데 보안 강화는 중요한 비중을 차지하고 있음
- 2015년 캄보디아의 IT 서비스 지출은 전년 대비 5.8% 증가한 2,892만 달러를 기록했으며, 향후 은행과 정부 부문을 중심으로 하드웨어와 소프트웨어 서비스 구축 및 보안 서비스에서 활발한 지출이 예상됨

물리보안

▶ 글로벌 보안업체 Robert Bosch SEA 측에 따르면 캄보디아 현지의 물리보안 시장의 연간 성장률은 10% 수준으로 금액으로는 400만 달러에 상당하며, 건설 경기 호황과 관광 시장 성장에 힘입어 향후에도 지속적인 성장이 예상됨

- 2019년 1월 보안 전문 미디어 asmag.com의 보도에 따르면, 캄보디아에서 Dahua Technology의 독점 유통업체 Loxu Digital은 보안 시장의 성장률을 30~40%로 예상했으며, 중국과 홍콩, 일본의 주요 투자자들이 캄보디아 보안 수요를 뒷받침하고 있다고 설명

2) 분야별 현황

정보보안 제품 및 서비스

▶ 캄보디아에서는 정보보안 제품을 비롯한 소프트웨어 산업 전반에서 설계/구현 기술이 내재화되지 않아 외국산 소프트웨어를 그대로 사용하는 것이 대부분이며, 레스토랑, 중소형 호텔 등 소기업용 응용 소프트웨어와 같이 단순한 형태의 개발이 주를 이룸

- 소프트웨어 설계/구현 시 체계적 방식을 적용하는 회사는 캄보디아 1위 SI 업체 First Cambodia 등 극히 일부 회사에 국한되며, 이마저 SAP, Microsoft 등 외국 기업의 방식을 그대로 차용하고 있는 실정
- 또한 캄보디아는 소프트웨어 개발 속도가 빠른 편이나 개당 2, 3달러에 판매되는 불법 복제 소프트웨어의 만연으로, 해외에 지사를 둔 업체를 제외하면 정식 라이선스를 받은 업체를 찾아보기 어려움

물리보안 제품 및 서비스

▶ 캄보디아 보안시장의 규모는 아직까지 협소한 편이지만 불안한 치안과 지속적인 경제 성장 및 건설 경기호황에 맞춰 CCTV, 금고, 도어록과 같은 보안 제품의 수요 증가가 예상됨

- 최근 일반 가정집에서도 무인전자경비 서비스 가입이 증가하고 있는 추세로 앞으로 보안관련 제품의 수요가 꾸준히 증가할 것으로 전망됨

▶ 캄보디아의 물리보안 시장은 파편화되어 있으며, 관련 업체들은 솔루션 기반의 판매보다는 저가 제품으로 가격 경쟁을 위주로 하고 있음

- 현지 건설업체 NKDesign Cambodia의 Sovan Hok 기술 매니저는 캄보디아 고객들은 품질보다 가격을 우선하기 때문에 저가의 중국산 제품들이 가장 인기 있고, 기타 브랜드 제품에 대한 인지도는 제한적이라고 설명
- 현지 보안업체 FLIR Systems의 Eric Lee 매니저는 예산 제약과 빈약한 네트워크 인프라로 인해 고급형 제품들이 도입되지 못하고 있다며, 캄보디아 내 IP 기반 영상감시시스템 비중이 15% 정도에 불과하고 나머지는 아날로그 제품이라고 설명

3) 주요 사업자 현황

시장 특성 및 경쟁 강도

❑ 정보보안 시장

▶ 캄보디아 정보보안 시장은 저개발된 시장 특성상 경쟁강도가 낮고, 글로벌 보안업체들도 캄보디아에 직접 지사를 설립하지 않고 현지 SI 업체 등을 통해 제품을 공급하고 있음

- 정보보안에 특화된 현지 업체는 찾아보기 어려우며, 대부분 IT 관련 종합적인 서비스의 일환으로 정보보안 서비스를 제공하는 형태

❑ 물리보안 시장

▶ KOTRA 현지 무역관 조사에 의하면, 2014년 기준 캄보디아의 보안업체는 40여개로, 이중 CCTV를 직접 수입하고 유통하는 업체는 30여개로 파악됨

- 2011~2013년까지 캄보디아 보안 관련 제품 수입통계에 따르면 현지 소비자들은 CCTV의 경우 아시아 제품보다 미국, 독일의 제품을 선호하며, 금고 및 도어록의 경우 말레이시아, 대만 등의 제품을 선호하는 경향
- 캄보디아 소비자는 가격에 민감해 주요 수입국이 자주 바뀌는 양상을 보이며, 현재 캄보디아에서 유통되는 CCTV는 대부분 15~50달러의 보급형 저가 모델임

주요 사업자

❑ 정보보안 시장

▶ CambodiaSoft

- CambodiaSoft는 2005년 설립된 IT 서비스 기업으로, 소프트웨어 개발, 웹 디자인, 사이버보안, 보안 카메라 설치, 서버 유지관리 등의 서비스를 제공
- 사이버보안 부문에서는 보안 컨설팅, 시스템 내 침입이나 해킹 조사 및 추적, 법적 조언 등을 제공

▶ First Cambodia

- First Cambodia는 시스템 통합 및 정보통신 솔루션 전문 기업으로 은행, 보험, 통신, 정부기관 등을 주요 고객으로 두고 있음
- 주요 제휴사로는 Cisco, Temenos, Thales, IBM, HP, SAP, Oracle, Checkpoint 등이 있으며, 이중

정보보안과 관련된 업체는 프랑스의 방위산업체 Thales와 방화벽 장비 부문에서 선두 업체인 Checkpoint가 대표적

▶ Trust Global Service

- 중소기업(SMB) 시장에서 높은 명성을 누리고 있는 SI 기업으로, IT 서비스보다는 하드웨어와 소프트웨어 매출의 비중이 높음
- 주요 고객군은 은행, 정부 및 소매업으로, 보안 관련 제품 및 서비스로는 네트워크 방화벽 외 스팸, 스파이웨어, 안티바이러스 등의 제품을 공급하며, Kaspersky와 제휴해 소비자와 기업 대상으로 판매를 담당

❑ 물리보안 시장

▶ GES Cambodian

- GES Cambodian은 2010년 설립된 캄보디아의 대표적인 IT 전문 유통업체로, 제품 공급뿐 아니라 종합 IT 서비스 및 솔루션도 제공
- 특히 보안 분야에서는 CCTV 시스템, 화상회의 시스템, 접근제어, 화재경보 시스템 등을 제공하며, 호텔, 은행, 컨벤션 센터, 정부, 카지노, 헬스케어, 리테일 등의 부문에 특화된 솔루션을 제공
- GES Cambodian이 취급하는 주요 보안 벤더로는 BOSCH, Dahua, Samsung 등이 있으며, 특히 접근제어, CCTV, 화재경보, 침입방지 등 보안 관련 전 부문에서 BOSCH의 제품을 중점으로 취급

▶ PROTEK Cambodia Security Company

- PROTEK은 1996년 6월 설립된 캄보디아 물리보안 업체로, 현재 프놈펜, 시엠립, 시아누크빌, 캄폿 등 4개 지역에서 약 2,000여명의 직원을 보유
- 동사는 공공 및 민간 영역에서 종합적인 물리보안 서비스를 제공하며, 은행, 공항, 항공사, 호텔, 공장, 보험사, 국제학교, 창고 등을 고객으로 확보
- 주요 서비스로는 CCTV, 보안 훈련, 무장/비무장 보안요원, 현금수송 등이 있음

▶ CY Tech

- 2009년에 설립된 CCTV 설치 및 유지관리 전문 기업으로, 최근 지문, 접근제어 시스템, GSM 경보 시스템 등의 영역으로 확장하는 추세
- CY Tech는 저가 CCTV 제품을 주력으로 취급하며, 중국 Safer의 제품이 대표적

▶ ADTECH

- 캄보디아 기반의 시스템 통합업체로, 침입 방지, 접근제어, 영상감시시스템 등의 보안 서비스와 빌딩

자동화, 통신 시스템, 화재감지 시스템 등을 설치

- ADTECH는 콘도미니엄과 5성급 이상 호텔 등 고급 건축물에는 Salto와 한화테크윈 등 한국과 서구 브랜드의 고가 보안장비를 시공

4) 주요 동향 및 이슈

▶ Visa, 캄보디아에서 '보안 로드맵' 공개(2019.09)

- Visa가 캄보디아에서 디지털 결제의 안전성을 보장하고 캄보디아의 캐시리스 경제 전환을 지원하기 위한 이니셔티브로 '보안 로드맵(Future of Security Roadmap)'을 발표
- Visa의 Shivakumar Siraman 동남아시아 부문 최고위험관리임원은 보안 로드맵을 발표하며, 이번 로드맵이 소비자들이 지불하는 방식을 변화시키는 기술과 같은 속도로 보안의 발전을 이끌기 위한 것이라고 설명
- 보안 로드맵은 데이터 보호와 금융사기에 앞서 이를 확인하기 위한 데이터 활용, 금융사기에 대응한 소비자 지원 등에 초점을 두고 있음
- 결제와 관련된 소비자들의 태도에 대한 Visa의 조사 결과, 동남아시아 소비자들의 67%는 모바일 결제 시 개인정보의 안전을 우려하는 것으로 나타났으며, 캄보디아 소비자들은 휴대폰 분실이나 도난, 휴대폰 해킹이나 데이터 탈취, 멀웨어나 바이러스 공격 등에 우려를 표시

▶ 캄보디아, 디지털 도어록 도입 시작(2018.08)

- KOTRA 캄보디아 무역관에 따르면 디지털 도어록 등 스마트홈 제품은 아직 시장 형성 초기 단계로 소수의 제품군만 시장에서 판매되며, 보안 장비와 서비스 업체, 컴퓨터 용품점, 가구점 등에서 디지털 도어록을 일부 판매하거나 향후 판매를 계획하고 있음
- 과거에는 일부 고급 호텔이나 한국이 투자한 주거단지에 제한적으로 스마트 도어록이 설치되었으나 최근에는 캄보디아 사무실, 콘도, 아파트 건설 붐과 생활방식의 현대화로 수요가 조금씩 증가 추세
- 2017년까지 캄보디아의 디지털 도어록 수입규모는 7만 달러 이하였으나, 2018년 상반기 수입액이 2017년 전체 수입액을 넘어서, 금년도 수입액은 10만 달러를 넘어설 전망
- 캄보디아의 도어록 제품은 모두 수입산으로 한국 브랜드에서는 삼성의 고가(300~500달러) 제품이 주로 판매되며, 기타 해외 브랜드로 Yale, PHGlock, Molilock, ZKBIO 등이 있음

▶ Te Aikhong, Kepstar Data Center와 Fourtitude Asia, 캄보디아 프놈펜 근처에 최대 데이터 센터 건설 계획(2018.06)

- 이 시설은 약 7천만 달러의 비용이 소모되며 18개월 안에 사업을 시작할 것으로 예상
- 캄보디아는 이 프로젝트를 통해서 타이완, 말레이시아, 싱가포르와 같이 기술적으로 진보된 이웃 나라들 대비 뒤처지는 것을 방지하는 한편, 신뢰할 수 있는 데이터 센터가 설립됨으로써 캄보디아에 더 많은 투자자들을 유치할 수 있을 것을 기대
- 캄보디아 정부는 "우리는 전자 거래, 지불 및 데이터 저장 촉진과 사이버보안을 강화하는 데 주력해왔다"라고 밝히며 데이터 센터 건설 계획에 대한 포부와 중요성을 밝힘

5) 정보보호 스타트업 시장 동향

▶ 캄보디아 최초의 스타트업 보고서 발간(2019.04)

- 캄보디아 국립우편통신ICT연구소(National Institute of Posts, Telecoms & ICT, NIPTIC)와 Smart Axiata의 의뢰로 Mekong Strategic Partners와 Raintree가 캄보디아 테크 스타트업 보고서를 발표
- 보고서에 따르면 2019년 현재 캄보디아의 스타트업은 300여개로, 2015년에서 2018년 사이 스타트업에 대한 공개 투자는 두 배로 증가했으며, 향후 수년간 시장 기회 증가와 디지털 수요 확대로 스타트업 숫자도 두 배로 늘어날 전망
- 업종별 스타트업 조사 결과에 따르면, 정보보호와 직접적으로 관련된 스타트업은 없는 것으로 나타났으며, 핀테크 분야의 스타트업이 50개 이상으로 가장 많고 디지털 미디어와 광고(40개 이상), 전자상거래와 물류(30개 이상)이 그 다음을 차지함
- 보고서에 따르면 캄보디아의 스타트업들은 전문 기술을 갖춘 인력의 부족과 뛰어난 기술적 지식이나 경험을 갖춘 멘토의 결핍으로 어려움을 겪는 것으로 나타남
- 보고서는 스타트업 발전을 위해서는 관련 지원 정책의 수립과 최적의 사업 환경 구축, 기술 스타트업 생태계의 인재 양성 등 다양한 관계자의 협력을 통한 해결책 마련이 필요하다고 강조

그림 _ 캄보디아 스타트업의 업종별 현황



[출처] Raintree(2019)

정보보호 정책 및 기관 현황

1) 관련 법령 및 정책

관련 법령 및 규제

▶ 캄보디아는 정보보호와 관련된 별도의 법령을 보유하고 있지 않으며, 2014년 4월 캄보디아 정부가 2년 여간 준비해 온 '사이버 범죄법(cybercrime law)' 초안이 유출된 바 있으나, 해당 법안이 언론의 자유를 침해한다는 비판이 제기되면서 한동안 보류되다가 2019년 7월 현재 초안 검토가 진행되고 있음

- 해당 법안은 온라인 불법행위에 대처하기 위한 것으로 해킹 및 자료 절취, 음란물 제작 등을 불법화
- 그러나 유출된 법안 내용 제 28조에는 "캄보디아의 주권과 통합성을 저해하는 온라인 콘텐츠"나 "정치적 분열과 불안을 조장하는 자료를 발행하는 행위" 등을 범죄로 규정하면서 표현의 자유를 침해한다는 비판 제기
- 이에 2014년 12월 캄보디아 정부는 사이버범죄법 초안을 폐기하고 한동안 추진하지 않을 계획이라는 입장을 발표
- 그러나 2017년 7월 캄보디아 우편통신부 ICT 보안국의 탄 소피크(Tan Sopheak) 국장은 현지 언론에 우편통신부의 지원을 받아 내무부에서 사이버범죄법 초안 작업을 진행 중이라고 밝힘
- 2019년 7월 The Phnom Penh Post의 보도에 따르면 내무부와 법무부 관계자들이 사이버범죄법 초안을 검토 중에 있으며, Chin Malin 법무부 대변인은 외국의 유사 법 시행현황을 연구할 필요가 있다고 발언
- 내무부 관계자에 따르면 사이버범죄법 초안은 7장 48개 조항으로 구성되며, 현재 실무그룹이 처벌 조항에 대한 개요 작업을 진행 중

관련 정책

▶ 2020년 통신/ICT 개발 정책(Policy on Telecom/ICT Development 2020)

- 2016년 4월 발표된 2020년 통신/ICT 개발 정책은 캄보디아의 통신과 ICT 발전을 위한 비전과 정책 프레임워크, 제도적 장치 마련, 통신과 ICT 분야의 구조적 난관 해결과 사업 및 투자환경 개선, 필요에 따른 구체적인 조치의 지원 등을 위해 개발됨
- 2020년 통신/ICT 개발 정책의 3대 목표는 ①통신 인프라와 사용률 개선, ② ICT 인적 역량 개발 ③ ICT 산업 다변화와 ICT의 응용 확대임

표 _ 2020년 통신/ICT 개발 정책의 3대 목표

목표	세부 목표
통신 인프라와 사용률 개선	• 도심 지역 100% 브로드밴드 커버리지 확보 • 농촌 지역 80% 브로드밴드 커버리지 확보 • 이동통신 보급률 100% 달성 • 인터넷 보급률 80% 달성 • 브로드밴드 보급률 50% 달성 • 가정용 인터넷 보급률 20% 달성 • 가정용 컴퓨터 보급률 26% • 사물인터넷 보급률 10% 달성
ICT 인적 역량 개발	• 국가공무원의 ICT 문해율 95% 달성 • 지방공무원의 ICT 문해율 75% 달성 • 고등학교 졸업자 100%가 ICT 기초역량 보유 • 여타 역량 대비 ICT 역량을 보유한 인적 자원 비율 15% • 100만 명 당 30명의 ICT 연구개발 전문가 확보 • 100만 명 당 10명의 ICT 연구원 확보
ICT 산업 다변화 및 ICT 응용 확대	• 통신/ICT 등록기업 비율 65% 달성 • 정부기관의 이메일 사용률 100% 달성 • 정부기관 웹사이트 보유율 100% 달성

[출처] 캄보디아 우편통신부(2016)

▶ 국가전략개발계획(National Strategic Development Plan, NSDP) 2014~2018

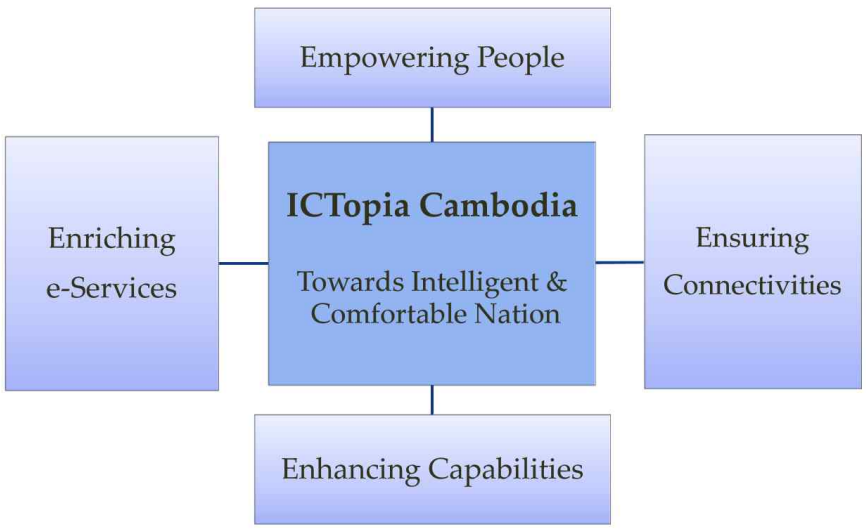
- 캄보디아 계획부는 2014년 9월 '국가전략개발계획(이하 NSDP) 2014~2018'을 발표했으며, 해당 계획은 NSDP 2009~2013의 성과에 기반을 두고 향후 신정부의 "사각전략" 제 3단계에 규정되는 목표 달성을 위한 액션플랜을 포함
- "사각전략"은 2004년 수립된 훈센 총리 정부의 국가발전전략으로서 ▲급속한 경제성장 달성,▲ 빈곤완화 및 새천년개발목표(MDGs) 등에 규정된 여타 사회적 목표 달성, ▲상기 두 가지를 위한 거버넌스 제도 창출 등이 포함
- 정보보호와 관련된 내용도 NSDP가 ICT 부문에서 우선 추진하는 하기 정책의 일부로 포함되어 있음
  - · 모든 사회적 경제적 측면과 부합하는 ICT 발전을 위한 국가 정책 개발
  - · 통신법 채택과 사이버범죄, 전자상거래를 포함한 관련 법안의 준비
  - · 국가브로드밴드 계획의 준비 및 시행

· 백본 인프라의 커버리지 확대 및 효율성 강화
· ICT 분야의 공공 문해력 수준 향상 및 빠르게 발전하는 현대 기술에 대응한 인력 자원 개발 도모
· 전자정부의 추가적 발전
· 브로드밴드 인터넷, 클라우드, 소프트웨어를 포함한 첨단 기술에 대한 민간 분야의 투자 촉진

▶ ICTopia Cambodia 2014~2020

- ICTopia Cambodia는 캄보디아 정부가 한국 KOICA의 원조를 통해 수립한 ICT 마스터플랜으로, 지적이고 편안한 국가를 비전으로 하며, 이를 위해 ▲권한 부여(Empowering People) ▲연계성 보장(Ensuring Connectivity) ▲능력 함양(Enhancing Capabilities) ▲e-서비스 강화(Enriching e-Service) 등 4대 전략적 목표를 수립
- 권한 부여와 관련된 실행목표로는 국가 ICT HRD 시스템 구축, 정부 및 산업계 종사자 훈련, ICT 교육 강화, ICT 활용 고취를 위한 사회적 환경 수립 등이 있음
- 연계성 강화와 관련된 실행목표로는 국가 백본망 구축, 국가 정보네트워크 가속화, 디지털 디바이드 해소, 디지털 TV 강화, 전자정부법 실행, 사이버보안 강화 등이 있음
- 능력 함양과 관련된 실행목표로는 ICT 생태계 토대 마련, ICT 생태계의 선별적 및 점진적 산업화, 국가표준기구 설립, ICT 연구개발을 위한 담당기관 및 정책 수립 등이 있음
- e-서비스 강화와 관련된 실행목표로는 전자정부 서비스 확대, 전자상거래 환경 개선, e-뱅킹 및 금융 네트워크 강화, e-러닝 서비스 실행 등이 있음

그림 _ ICTopia 2020 비전 및 전략적 목표



[출처] Cambodia's ICT Masterplan 2020

2) 담당기관

▶ 캄보디아 우정통신부(Ministry of Posts & Telecommunication, MPTC)

- 캄보디아 우정통신부는 캄보디아 전역의 우편, 통신, ICT 분야에서 효율적인 네트워크 인프라 연결성과 접근 가능한 서비스를 증진하여 사회경제적 발전과 빈곤 감소에 기여한다는 목표 하에 통신 산업 전반에 걸친 정책 수립을 맡고 있으며, 정보보호 정책도 여기에 포함됨
- 우정통신부는 산하에 ICT보안국(Department of ICT Security)을 두고 보안 정책을 수립하고 있음

▶ CamCERT(Cambodia Computer Emergency Response Team)

- CamCERT는 캄보디아 국가정보통신개발청(National ICT Development Authority, NIDA)의 산하기관으로 2007년 12월 설립되어 2008년 10월부터 정식 운영을 시작
- CamCERT는 IT 보안전문가들로 구성된 비영리 조직으로, 캄보디아 정부 및 인터넷 서비스 사업자들, ICT 업체 등과 긴밀히 협력해 정보보안과 관련된 조언을 제공
- CamCERT의 주요 과제는 ▲사이버범죄 수집 및 조사, 대응, ▲ IT 보안에 대한 훈련 및 홍보 개선, ▲국내외 CERT와의 협력 ▲전국 네트워크 감시센터 설립 ▲IT 보안 표준 수립 ▲사이버 보안 플랫폼 개발 등이 있음

3) 최근 정책 동향 및 이슈

▶ 중국, 캄보디아에서 열리는 주요 국제행사에 보안 장비 제공 계획(2019.09)

- 중국 정부가 캄보디아가 주최하는 국제 행사에 앞서 보안 장비와 경험을 지원하기로 함
- 캄보디아 경찰청의 Neth Savoeun 경찰청장은 양국간 보안 협력을 논의하기 위해 중국을 방문해 국제 행사에 대한 지원을 요청
- 캄보디아는 2020년 아시아-유럽 회담과 2023년 동남아시아 게임을 주최하며, 국제 행사 경험이 풍부한 중국이 각 행사의 보안을 유지하기 위한 경험과 장비를 제공하기로 함

▶ 제 4 회 아시아 태평양 사이버 보안 정상 회의 캄보디아에서 개최(2018.09)

- 매년 개최되는 이 컨퍼런스는 기업의 최고 연구원 및 경영진이 아시아 태평양의 주요 사이버 보안 이슈를 이 지역의 11 개국에서 온 기자들과 청중들에게 제시함
- 이번 컨퍼런스는"Balkanization(발칸화): 보안은 고립되어서는 안된다"를 테마로 아시아 국가들과

관련된 사이버 위협의 개요와 함께 인터넷의 탈세계화의 위험성을 강조했음

▶ 일본, 캄보디아 포함 아세안 6개국의 사이버보안 강화 훈련 지원(2017.03)

- 캄보디아 우편통신부의 관리들은 2017년 2월 20일부터 3월 3일까지 인도네시아, 라오스, 필리핀, 미얀마, 베트남 등의 아세안 국가 관리들과 함께 일본 현지에서 사이버보안 훈련을 받음
- 일본국제협력기구(JICA)가 후원하는 이번 프로그램은 3년간 지속되며, 정부기관에 대한 모의 공격을 통해 사이버 공격에 대비하려는 목적을 갖고 있음
- JICA는 이번 훈련으로 진화된 사이버 공격에 대응해 사이버보안 사고대응에 필요한 조직, 기술, 절차, 인력을 이해하는 인적 자원 개발이 가능해질 것이라고 설명

4) 정보보호 스타트업 관련 정책 동향

▶ 캄보디아, 스타트업 양성 위한 스타트업 센터 설립(2019.04)

- 캄보디아 정부 후원으로 스타트업을 양성하기 위한 스타트업 센터(Techo Startup Centre)가 설립됨
- 스타트업 센터는 젊은 기업가들에 대한 지원 및 캄보디아를 디지털 경제로 전환하고자 하는 정부 계획을 지원하게 됨
- 캄보디아 정부에 따르면 스타트업 센터의 임무는 새로운 기술 스타트업과 중소기업들에 대한 지원 프로그램을 통해 창업을 활성화하는 것임
- 스타트업 센터는 학생들에게 인턴십 지원 및 멘토 연결 등을 지원할 계획이며, 대학과 고용 시장 및 민간 분야를 연계하는 중개 역할을 맡게 됨
- 한편, 지난 3월 캄보디아의 훈센 총리는 캄보디아 기술 스타트업 분야를 강화하기 위해 연간 500만 달러의 기금을 조성한다고 발표하기도 했음

융합보안시장 및 정책 동향

1) 융합보안시장 동향

스마트시티

▶ 캄보디아 수도 중심에 싱가포르 민간자본을 통한 스마트시티 건설 계획[119]

- 싱가포르 기업 Limestone Network는 수도 프놈펜 중심부에 스마트 시티를 건설할 계획
- 규모는 100 헥타르이며, 주거용 주택, 사무실 건물, 쇼핑몰, 상점, 학교, 컨벤션 센터 등이 세워질 예정으로 총 1만 개의 기업과 약 20만 명의 인구를 수용할 전망
- 블록체인 인프라 기반의 스마트 시티로 건설될 예정으로, 디지털 여권을 통하여 이곳에 등록된 주민들로부터 정보가 수집되고, 수집된 정보를 통하여 주민들의 활동과 요구사항을 쉽게 파악 가능

핀테크

▶ 핀테크 시장은 아직 발전 초기단계이나 급격한 발전을 보이고 있음[120]

- 기존의 유선 전화망보다 모바일 통신망의 품질이 우수하여 100%에 육박하는 국민들이 스마트폰을 소지하게 된 것이 발전의 배경을 이룸
- 초기의 원거리 단순 송금기능을 넘어 모바일 결제, 금융상품 이용, 세금 및 공과금 납부 등의 형태로 시장이 확장 중
- 현재 약 10개사의 핀테크 기업(wing, payway, pi pay 등)들이 캄보디아 핀테크 시장에 진출, 경쟁에서 우위를 차지하려고 노력
- 19년 국내 시중은행들도 핀테크 시장에 직접 진출하거나 기존 핀테크 기업과 협력을 통하여 캄보디아로의 사업 영역 확장을 모색 중[121][122]

---

119 https://www.khmertimeskh.com/50634713/singaporean-company-plans-to-build-smart-city-in-cambodia/

120 http://news.kotra.or.kr/user/globalAllBbs/kotranews/album/2/globalBbsDataAllView.do?dataIdx=169565&searchNationCd=101073

121 https://www.yna.co.kr/view/AKR20190801149500053

122 http://it.chosun.com/site/data/html_dir/2019/03/17/2019031701591.html

2) 융합보안정책 동향

블록체인(가상화폐 포함)

▶ 캄보디아 국립은행, 해외로부터의 송금 편의성 확대를 위하여 지불수단으로서의 블록체인 활용 착수[123][124]

- 캄보디아 국립은행은 말레이시아 Maybank와 MOU 체결을 통하여 Maybank의 블록체인 기술 도입 및 양국 간의 해외 지불에 직접적으로 관여 노력 중
- 실제로 많은 국민들이 인근 국가에서 근로를 통하여 벌어들인 수입을 정기적으로 본국으로 송금하고 있는데, 높은 수수료와 지나치게 긴 송금처리 기간으로 불편을 겪고 있음
- 지속적인 인근 국가들과의 협력을 통해, 블록체인 기술을 활용하여 지불의 효용성을 높이고 해외거래 비용을 줄일 수 있을 것으로 기대

123 https://www.cnbc.com/video/2019/10/22/how-cambodia-is-using-blockchain-for-payments.html
124 https://www.asiablockchainreview.com/cambodia-national-bank-tests-blockchain-for-cross-border-payments/

바. 태국

'18년 GDP(십억달러)	504.993
'18년 인구수(천명)	69,429

■ ITU 글로벌 사이버보안 지수(Global Cybersecurity Index, GCI)

· 태국의 사이버보안 지수 순위는 35위로 전년 대비 15위가 하락

국가명	2018		2017		전년대비 증감	
	지수	순위	지수	순위	지수	순위
태국	0.796	35	0.684	20	+0.112	-15
대한민국	0.873	15	0.782	13	+0.091	-2

■ ICT 관련 주요 지수

· 태국의 전반적인 ICT 발전 상황은 전 세계 중상위권에 속하는 것으로 나타남

지표명	태국		한국	
	점수	순위	점수	순위
IMD 국가경쟁력지수(2019)	-	25	-	28
IMD 디지털경쟁력지수(2019)	-	40	-	10
UNCTAD 전자상거래지수(2019)	73.5	43	89.4	19
ITU 글로벌 사이버보안 지수(GCI 2018)	0.796	35	0.873	15
UN 전자정부 지수(2018)	0.654	73	0.901	3

■ ICT 관련 주요 통계(ITU, 2018년 말 기준)

· 태국은 유선통신 기반이 취약하나, 이동통신 보급률은 상당히 높은 것으로 조사됨

항목	태국		한국	
	가입자수(천 명)	보급률(%)	가입자수(천 명)	보급률(%)
유선전화	2,929	4.22	25.906	50.63
유선브로드밴드	9,189	13.24	21,286	41.60
이동통신	125,098	180.18	66,356	129.67
인터넷 이용률	56.82%		95.90%	

정보보호 산업 개요

1) 정보보호 산업 환경 및 배경

정보보안 환경

▶ ITU가 2019년 1월에 발표한'Global Cybersecurity Index(GCI) 2018'에 따르면 태국의 사이버보안 지수는 0.796으로 글로벌 순위는 22위(2018년 지수는 35위)를 기록한 것으로 나타났으며, 동남아 권역에서는 싱가포르와 말레이시아에 이어 3위를 기록

- 해당 지수는 법적 대응, 기술적 대응, 조직적 대응, 역량강화, 국제협력 등 5개 부문의 지수를 종합한 것으로, 태국은 5개 부분에서 비교적 High 그룹에 속하고 있음.(High 그룹 상위 53개 국가, Medium 그룹 54개 국가, Low 그룹 87개 국가)

▶ Symantac Internet Security Threat Report 2018에 따르면 2017년 사이버보안 위협 지수에서 태국은 아시아 태평양 지역에서 7위를 기록하였는데, 이는 9위를 기록했던 2016년 보다 두 단계 상승한 것임

▶ 태국, 세계 2위 사이버 범죄 위험 국가로 사이버 범죄의 표적이 되고 있다고 알리안츠(Allianz Global)가 분석[125]

- BitDefender의 연구에 의하면 태국은 아시아에서 5번째, 전 세계적으로 11번째 사이버 고위험 국가(아시아 지역에서는 인도, 인도네시아, 중국, 베트남 다음)[126]로 분류
- 2016년 8월 1일부터 8일까지 악의적인 해커들이 정부저축은행(Government Savings Bank) 소유의 ATM을 공격하여 약 346,000달러를 탈취
- 디지털경제부(Ministry of Digital Economy) 산하 전자거래개발청(Electronic Transactions Development Agency, ETDA)[127]에 따르면 ThaiCERT의 통계를 인용하여 2018년에만 약 2,520회의 사이버 공격이 있었던 것으로 보고되었으며, 주로 사기성 스캠(Scam) 공격이었던 것으로 밝혀짐
- 사이버 범죄에 따라 손실을 입었다고 보고된 약 20% 정도 기업의 경우, 손실이 10만 달러에 달했으며 그 중에도 약 4% 기업 경우에는 약 100만 달러에서 1억 달러에 달하는 손실을 본 것으로 드러남
- 인터넷 사용자와 모바일 이용자도 폭발적으로 늘어나고 있지만, 위험에 대한 대비 부족, 프로토콜에

125 Bangkokpost. 2016.6.8.
126 TECHINASIA, 2017.4.10
127 태국의 ICT, 전자상거래 및 사이버보안 담당 기관

대한 교육의 부재 등으로 멀웨어를 포함한 각종 바이러스 노출위험이 증가하고 있음

- 동남아 지역은 피싱(Phishing) 공격의 온상이 되고 있다고 보안전문 기업인 Kaspersky가 밝히고 있음.[128]

  동 기업이 밝힌 공격 회수를 보면 태국에서 2019년 상반기에만 약 150만 건의 사이버 공격 시도가 있었던 것으로 조사되었다고 언급하면서, 이러한 공격에 의해 감염된 컴퓨터 또는 컴퓨터 시스템의 감염률은 11.972%로 지난해 같은 기간 10.9%보다 높은 것으로 나타남

- 특히 모바일 사용자가 많은 태국과 같은 지역에서 오래된 방식이지만 여전히 효과적인 피싱과 같은 공격에 대한 교육이 필요함을 강조

▶ 태국, 여전한 정보 유출 사고

- 태국에서는 2018년 3월 두 번째로 큰 모바일 네트워크 사인 True Corp. 에서 45,000명의 개인 정보가 유출 된 것으로 보고됨. 동 유출 사고로 인해 32GB 분량의 개인정보가 유출된 것으로 소비자의 스캔한 개인문서, ID 운전면허, 여권 스캔 자료가 탈취당한 것으로 나타남
- 2018년 8월 태국 중앙은행이 언급한 내용은 2개의 상업은행에서 123,000명의 소비자 정보가 유출된 것으로 알려짐
- 2019년 3월에는 태국과 베트남에서 동시에 토요타 자동사 현지 법인의 자료에 불법적인 접근이 감지되어 현재 조사 중인 것으로 나타남

물리보안 환경

▶ 국가의 3개 핵심지표(Institutions and Resources, Safety Frameworks, Safety Outcomes)로 안전성을 평가하는 UL Safety Index (2018) 기준, 태국은 물리보안 영역에서 글로벌 평가 56위를 차지하였으며, 주요 동남아시아 국가 중 싱가포르와 말레이시아 다음으로 높은 순위임

▶ 물리보안 영역의 경우, 태국 정부가 추진하는 Thailand 4.0 계획과 연안동부지역 경제개발에 따른 스마트 시티 등 대규모 인프라 투자로 인해 수요 급증

- 태국 정부는 관광 도시 푸켓과 치앙마이를 스마트시티로 변모시키고, 동부회랑 경제특구(Eastern Economic Corridor)을 위한 대규모 프로젝트를 시행
- ▲도시 내의 첨단 IT 인프라 구축과 주민의 안정성 및 편의성 증대 ▲첨단 교통관제 시스템, 여행객들의 여행정보 검색 및 안전한 여행을 위한 인프라 증대 추진으로 향후 물리보안 시장 규모가 증가할 전망

▶ 통계 포털 Statista에 따르면 2018년 태국 물리보안 시장 규모는 약 800만 달러이며, 연 평균 60.2%씩

128 SecurityBrief, 2019.9.7

성장하여 2022년에는 시장규모가 4,600만 달러에 도달 할 것으로 전망

2) ICT 시장/산업 개요

▶ 국제 마케팅 조사업체 'We are Social'에 따르면 2019년 1월 기준 총 6,924만 명의 태국 인구 중 인터넷을 사용하는 인구는 5,700만 명으로, 전년에 비해 변동이 없는 것 나타남

- 모바일 가입자 수는 9,233만 명으로 133%의 보급률을 보이고 있으며, 이는 전년 동기대비 약 1.7%의 증가율을 보이고 있음
- 한편, 태국에서는 인터넷 사용자들의 대부분이 소셜미디어 서비스를 이용하는 것으로 나타남
- 휴대폰을 통한 인터넷 접속인구는 5,501만 명으로 전체 인구의 약 79%가 모바일을 통해 인터넷을 사용하는 것으로 나타남

그림 _ 태국 인터넷 및 모바일 사용 인구 현황



[출처] We are Social (2019.1)

▶ 태국은 모바일과 인터넷 속도는 전 세계적으로 가장 느린 국가 중의 하나

- Speedtest Global Index에 따르면 2019년 8월 기준 태국의 다운로드 속도는 20.20Mbps로 전 세계 145개국을 대상으로 한 모바일 광대역 속도 측정에서 94위를 차지하여, 111Mbps로 1위를 차지한 한국과 큰 차이를 보이고 있음

- 한편 유선인터넷에 있어서는 88.78Mbps로 176개국 중에서 26위를 차지한 것으로 나타남(한국의 경우는 160Mbps로 3위를 기록)

▶ 태국 통신 시장

- 태국은 아직까지 GSM이 지배적인 시장으로 정부의 강력한 디지털 경제로의 전환 추진에 따라 빠르게 4G 5G 통신으로 소비자들이 전환할 예정
- 2012년 태국방송통신위원회(NBTC)는 15년 기한의 3G 라이선스 입찰을 완료하였고, 태국의 주요 3개 통신사(AIS, DTAC, True Corp)는 2013년 6월부터 상업적인 3G 네트워크 사업을 시작
- AIS사는 2016년에 4G 광대역 서비스를 실시계획을 밝히고, 4G LTE와 LTE-A 서비스를 방콕과 42개 지역으로 서비스를 늘려갈 계획
- 2017년 9월에는 퀄컴기술을 LTE-A 서비스에 적용하여 4.5G 네트워크 서비스를 개시
- DTAC사는 2012년 5월 4G LTE 모바일 시험서비스를 실시하였고, 2014년에 Ericsson 장비를 도입하여 4G 네트워크를 전개하였음. 이는 향후 5G 서비스로의 전환을 염두에 둔 것임
- 또한 DTAC사는 2018년 7월 노키아와 함께 TD-LTE 네트워크를 전개하기로 협력 파트너십을 체결
- 국영 통신사인 TOT와 CAT는 3G 네트워크 도매사업으로 수익을 거두고 있지만, 만성적인 재정적인 어려움으로 인해 정부 측으로부터 두 회사의 합병에 관한 권고가 있었으며, 2018년 CAT 이사회가 이를 승인함으로써 양사간 합병이 이루어질 전망
- 현재 태국은 4G 서비스로의 전환이 급격하게 이루어지고 있어, 향후 시장은 4G, 5G 서비스 시장 경쟁으로 재편될 예정

▶ 태국 5G 시험 전개

- 2019년 6월 태국의 디지털경제사회부는 공공 및 민간부문의 40개 사와 5G 서비스 시험운용에 관한 계약을 체결하였으며, 동부경제회랑(EEC) 촌부리(Chon Buri) 지역의 카셋삿(Kasetsart) 대학 Siri Racha 캠퍼스 내 테스트 센터(5G Testbed@Sriracha)를 테스트베트로 활용할 계획
- 디지털경제사회부와 동 대학은 2019년 2월부터 5G 인프라 개발을 추진하여 왔으며 태국 최초의 이용사례 테스팅을 실내외에서 진행

▶ 디지털 경제 추진을 위한 투자 계획

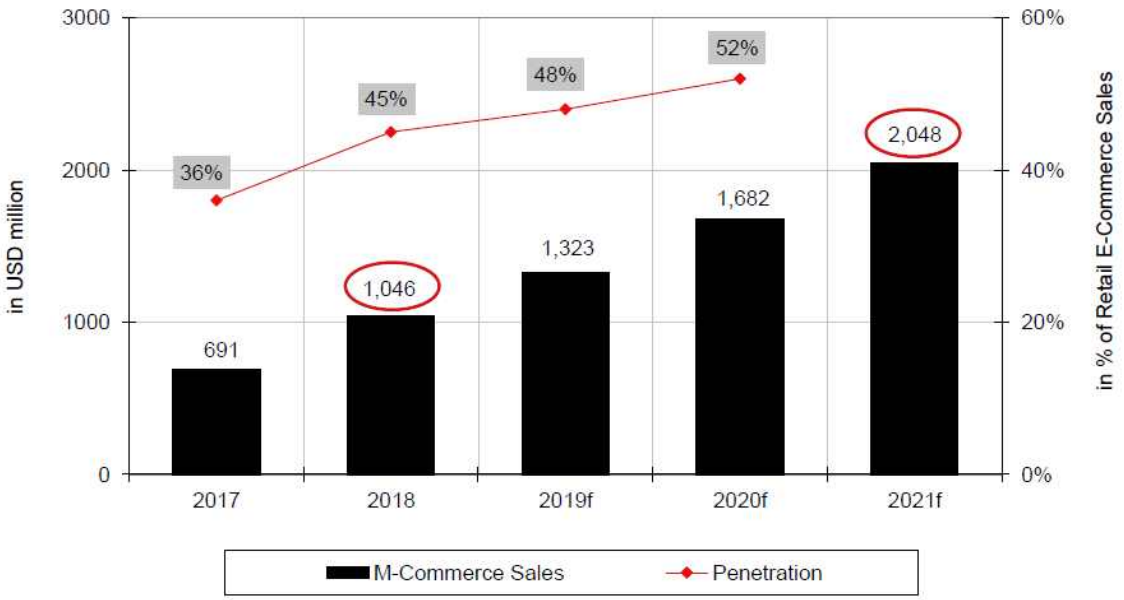
- 태국 정부는 향후 10억 바트를 투자하여 국가 통신 인프라를 개선할 예정이며, 향후 3년 이내, 인터넷을 이용하는 인구를 4천만 명까지 늘릴 목표
- 2015년 10월 CAT 텔레콤사는 태국을 2020년까지 동남아 디지털의 허브로 만들기 위한 '국가인터넷 게이트웨이' 프로젝트를 제안. 이 프로젝트의 핵심의제는 해저케이블을 통해 국제적인 인터넷 게이트웨이(IIG)를 증가시키는 것임

- 디지털 시장 전망(digital market landscape), 디지털 인프라(digital infrastructure), 디지털 혁신 생태계(digital innovation ecosystem)가 태국 디지털 경제에서의 주요 투자 영역임

▶ 전자상거래 활성화

- 태국의 전자상거래 시장은 매년 두 자리 수의 증가율을 보이고 있으며, 특히 태국의 경우 SNS를 통한 전자거래가 활발한 것으로 나타남
- yStats의 조사에 의하면 태국은 인도네시아와 베트남을 이어 동남아시아에서 3번째의 활발한 전자상거래가 이루어지고 있는 것으로 나타나고 있지만, 소셜미디어를 통한 상거래가 활발하여 이를 합칠 경우, 인도네시아에 이어 2번째로 큰 시장을 형성하고 있는 것으로 나타남
- 태국의 전자상거래 시장은 소셜미디어 판매를 제외하고 2018년에는 약 23억 유로, 2023년에는 70억 유로를 기록할 것으로 예측. 소셜미디어 판매를 포함할 경우 2018년에 약 26억 유로 규모로 증가

표 _ 태국의 모바일 거래 시장 규모



출처: yStates.com

- 스마트폰은 태국 국민들아 가장 빈번하게 인터넷에 접속하는 도구(95%)로 나타나고 있어 스마트폰을 통한 모바일 거래(M-Commerce)는 동남아시아에서 가장 활발한 것으로 나타남. yStats에 따르면 스마트폰 전자상거래 규모는 2018년 9억 유로(약 9억 8,500억 달러)에서 2021년에는 18억 유로(약 19억 7천만 달러)로 늘어날 것으로 예상
- 태국 정부는 전자상거래를 중심으로 디지털 사회로의 전환을 목표로 하고 있으며 국가 전자상거래

전략(National e-Commerce Strategy)를 개발하여 2021년까지 현재 규모의 2배까지 전자상거래를 확대시킬 예정(ETDA)

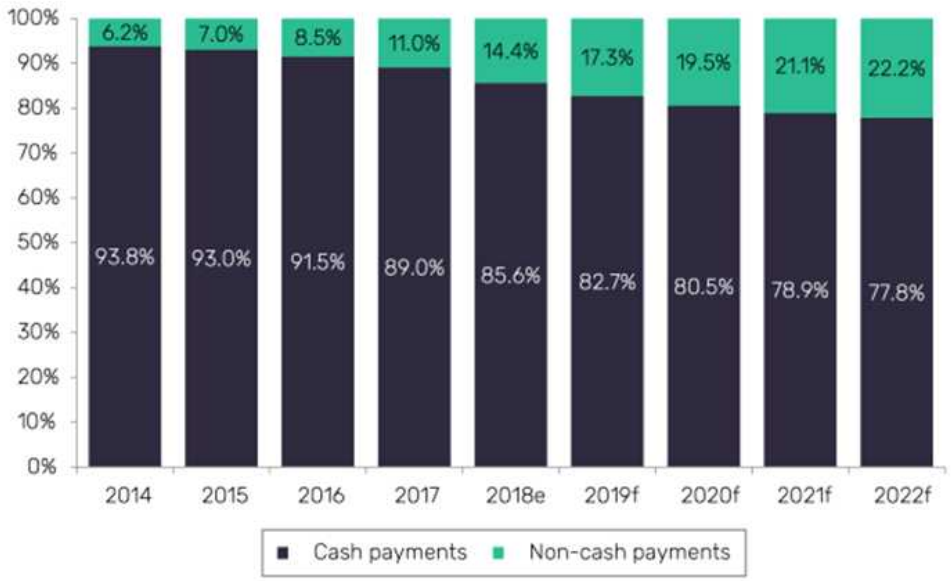
- 전략1: 기업 확대, 전자상거래 품목 및 표준 개발 등
- 전략2: 전자상거래 생태계 강화 및 거래용이성 확보 등
- 전략3: 정보 인프라의 효율성 증진, 정보·데이터·지식의 이용 풀 확대, 펀딩자원 접근성확대 등
- 전략4: 모두를 위한 신뢰성 확보, 자기 규제 강화, 소비자 보호 등

▶ 전자거래 지불 시스템 (e-payment) 구축

- 태국 정부는 P2P 거래와 세금납부, 복지수당 지급 등의 용도로 쓰일 e-Payment 시스템인 PromptPay 시스템을 2016년 8월부터 도입
- PromptPay 시스템은 비공식적인 경제 활동을 은행 시스템 안에 통합하고 현재의 사회복지 정책에서 투명성을 확보겠다는 목표로 추진
- 등록된 고객들은 모바일을 통해 전화번호나 주민번호 등으로 자금을 이체할 수 있으며 사회보호, 연금, 세금 환급 등도 이를 통해 받을 수 있게 됨
- 태국 정부는 중국의 전자상거래 영업체인 Alibaba와 협력하여 중국기업이 태국의 중소기업이나 개인 간 거래에 사용할 수 있는 전자거래 지불 시스템에 대한 교육 훈련을 시작
- 한편, 태국 정부가 소유하고 있는 태국 기간 통신사 CAT Telecom은 한국의 SK텔레콤, NHN KCP와 파트너십을 체결해 e-Payment 관련 합작 사업을 시작
- 2018년 8월 기준, 일인 당 e-payment 평균 거래량은 50건이며, 태국은행 (The Bank of Thailand)은 사용자 1인당 평균 e-payment 거래량이 150건으로 늘어날 것으로 예상
- PromptPay, QR 코드, electronic data capture (EDC) 사용의 증가로 태국 내 e-payment 거래량은 예상보다 빠르게 증가하고 있음
- 2019년부터 발효된 전자지불법(e-payment law)에 따라 온라인 판매자들에 대한 소득세 징수가 2020년 1월 1일부터 시작될 예정. 온라인 판매자들에 대한 징수는 전체 수입금액에 대한 0.5% 일괄 과세로 징수될 것으로 예상[129]
- 한편 GlobalData에 따르면 태국의 현금결제 규모는 점차 적으로 줄어들고 있으며, 비 현금 결제 규모는 2018년 전체 결제 규모의 약 14.4%를 차지한 것으로 나타남
- 이는 태국 정부가 추진하고 있는 현금없는 사회를 지향하는 마스터 플랜에 따라, 소매점들에게도 POS 설치를 장려하고, 세금 감면 등의 혜택을 주고 있기 때문

129 Bangkok Post, 2018.12.8

표 _ 태국의 현금거래와 비현금 거래 규모 추이



출처: GlobalData

- 태국 내에서 전자결제 관련 모바일 결제는 2016년부터 모바일 결제 시장에 뛰어든 LinePay와 더불어 SamsungPay, PromptPys 등이 있음

정보보호 시장 현황

1) 시장 규모

시장 개요

▶ 태국의 정보보안 시장 규모는 아직 크지 않으나, 정부 차원의 적극적인 정보보안 관련 정책 추진과 인프라 투자로 향후 빠르게 성장할 것으로 전망

▶ AES 그룹의 CEO, Henny Beeber에 따르면, 태국의 보안 시장은 계속해서 성장하고 있지만 이 전과 비교해 다소 느린 성장률을 보이고 있다고 밝힘

▶ Fit IT and Solution의 CEO인 Wissawat Chotbenjakul에 따르면 태국 정부의 프로젝트와 외국 투자가 적은 것이 태국 보안 시장의 하락의 이유라고 밝힘. 프로젝트에 대한 엄격한 규제 또한 시장 발전을 저해한다고 밝힘

시장 규모 및 전망

▶ 태국 물리보안 장비 시장의 규모는 약 3억 달러 수준으로 동남아시아 전체 물리보안 시장의 약 30%를 차지하고 있으며, 매년 약 30%의 고성장을 기록하고 있음

- 시장조사기관 RNCOS에 따르면 태국의 CCTV 시장은 2013년~2017년간 연평균 21.5%의 성장률을 보일 것이라고 하며, 태국 내 범죄율의 지속적인 증가와 보안에 대한 의식이 높아짐에 따라 물리보안 시장에 대한 수요도 급격히 증가할 것으로 예측
- 아울러 철도, 지하철 건설과 공항확장과 같은 인프라 건설이 지속되면서 새로운 물리보안에 관한 수요가 점증

▶ MarketsandMarkets 조사에 따르면 태국의 2017년 보안 솔루션시장 규모는 약 37억 바트(약 1억 1천만 달러)에 달하며, 2018년에는 약 10~12% 성장할 것으로 추정

▶ 글로벌 시장 리서치 회사인, MarketsandMarkets에 의하면, 2017년 태국의 물리보안은 시장은 37억 바트의 가치를 가지고 있으며 연간 성장률은 약 12%인 것으로 집계됨

2) 분야별 현황

물리적 보안 시장 주요 사업자

▶ 캐나다의 보안기업인 Genetec에 따르면 태국에서 동사의 물리적 출입통제 관련 프로젝트는 2016-21년간 연간 약 6.6% 평균 성장률을 보일 것으로 예측

- 이에 따라 태국의 보안시장에서 벌어들일 수익 규모는 2016년에 2170억 달러에서 2021년에는 약 2920억 달러에 달할 것으로 예측
- Genetec사는 주로 인터넷 기반 출입통제, CCTV, 자동화된 출입인식증 등을 제공하는 기업으로 제3자 통합 보안 서비스 제공자

▶ Arecont Vision

- Arecont Vision은 선도적인 메가픽셀 기술로 선진화된 이미지 기반 보안 적용 애플리케이션을 제공하는 기업으로 메가픽셀 관련 기술과 제품을 제공
- 제품은 CCTV 시스템 관련 IP camera, CCTV 카메라 렌즈, CCTV 조명 등

▶ Delta Scientific Corporation

- Delta Scientific Corporation은 차량 입출입 통제 시스템 관련 제품을 생산하는 기업으로 차량을 통제하는 바리케이드 시스템을 주로 납품
- 주요 제품은 차량방지용 말뚝(Bollard), 바리케이드, 방호문, 경비초소 등

▶ Segate Technology

- 하드 디스크와 저장장치의 보안 솔루션을 제공하는 기업으로 감시 시스템의 신뢰성을 보장하며, 감시 시스템의 수명은 늘리고, 보안 시스템의 경비를 낮추며 비디오 분석을 지원
- 주요 제품은 10TB SkyHawk Surveillance Hdd 등

▶ IDIS

- IDIS는 최첨단 비디오 감시 솔루션을 제공하는 한국 업체로 비디오 감시 장비를 제조하며, 인공지능과 딥러닝을 통한 차세대 분석 솔루션을 통해 감지 및 분류, 침입 등을 감시하는 시스템 제공
- 주요 제품은 DirectIP 카메라, CCTV용 비디오 카메라 등

▶ Dahua Technology Ltd.

- Dahua Technology는 비디오 감시 솔루션을 제공하는 업체로 전 세계적인 감시장비 시장에서 2위를 차지하는 것으로 나타났으며, 세계에서 첫 번째로 8채널의 실시간 디지털 비디오 기록장치를 출시
- 주요 제품은 네트워크 카메라, 건물 관리 감시 카메라, 얼굴인식 기기 등

▶ Vanderbilt

- Vandervilt Industries는 출입통제, 침입감시, 비디오 관리 시스템을 제공하는 보안 업체로, 보안관련 통합 시스템 환경을 제공하며, 하드웨어뿐만 아니라 통합 관리 소프트웨어도 제공

▶ Vicon

- Vicon Industries 는 비디오 시스템과 관련 보안과 감시, 안전과 통제 목적으로 사용되는 제품을 생산하며, 비디오 관리 소프트웨어와 메가픽셀 IP 카메라 등도 제공

▶ FLIR Systems

- FLIR Systems는 인지기능과 감지기능을 증강시키는 기술을 개발하여 센싱분야 통합 솔루션을 제공하는 기업으로 열화상 이미지, 비디오 분석, 가시광이미지(Visible-light Imaging) 등을 통해 위험요소를 감지하는 시스템을 제공
- 주요 제품은 열화상 카메라, 감시용 모바일 보안경, 실외용 IP 카메라 등

▶ BCDVideo

- BCDVideo는 IP Video 감시 시스템에 관한 통합 솔루션을 제공하는 업체로, 감시 저장 서버, 환경적으로 안전한 서버, 스위치, 네트워킹, 온 사이트 서비스 등을 제공

3) 정보보안 주요 사업자 현황

정보보안 시장

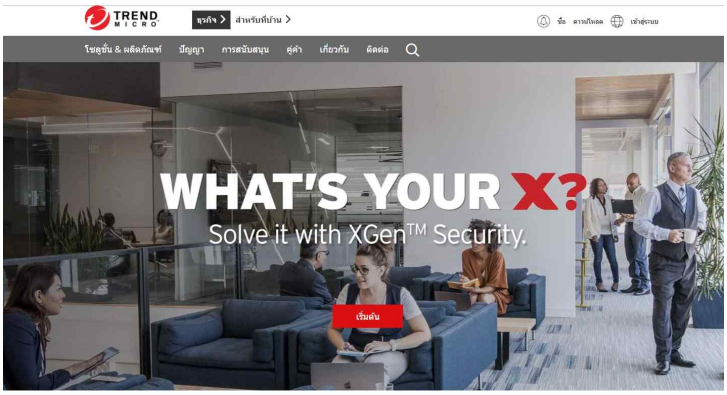
▶ Trend Micro, McAfee, Check Point, Symantec, Sophos, Kaspersky 등 동남아 지역에서 활발한 사업을 벌이고 있는 글로벌 사업자들이 태국에서도 정보보안 시장을 주도하고 있으며, SafeComs, Nod32, BitDefender, Panda 등도 두각을 나타내고 있는 상황

▶ 태국의 정보보안 제품 수요자들 사이에서는 유명 글로벌 기업의 제품에 대한 의존도가 높게 나타나고 있으며, 저가 제품군을 형성하고 있는 중국 기업들의 제품에 대해서는 신뢰가 낮은 편임

▶ Trend Micro

• 글로벌 보안 솔루션 기업인 Trend Micro는 동남아시아 주요국 (말레이시아, 태국, 인도네시아, 베트남 등)에 지사를 보유하고 있으며, 태국어 웹사이트를 통해 PC의 보안 수준을 체크할 수 있는'Threat Meter'를 제공 중

그림 _ Trend Micro 태국 홈페이지



ผลิตภัณฑ์ความปลอดภัยที่ชาญฉลาด ดีที่สุด และเชื่อมโยงกัน
สำหรับโลกที่เชื่อมโยงกันของคุณ

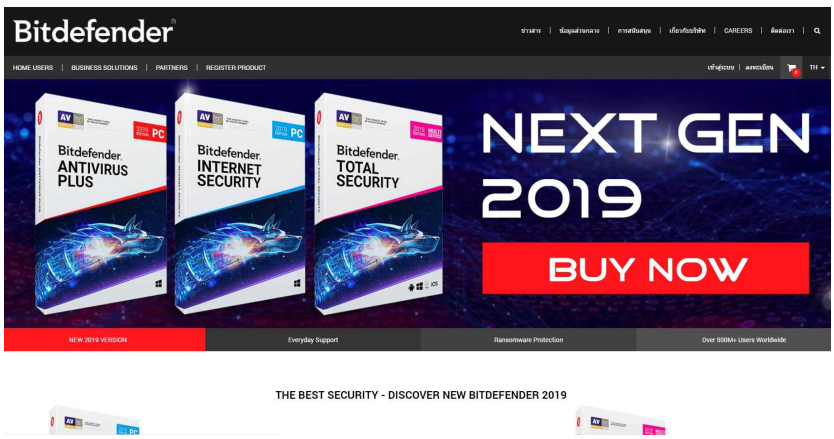
[출처] TrendMicro.co.th

▶ Bitdefender

• 루마니아계 글로벌 정보보안 솔루션 기업 Bitdefender는 태국 내 별도의 지사 없이 태국어 홈페이지만을 운영하고 있으며, 정보보안 제품 유통업체인 Freelance Engineering을 통해 유통되고 있음

• 주요 제품군 및 서비스 : 안티바이러스, 안티 스파이웨어, 안티피싱, 안티스팸, 방화벽, 네트워크 보안 등

그림 _ Bitdefender 태국 홈페이지



[출처] Bitdefender.co.th

▶ SafeComs

- SafeComs는 2004년 태국 방콕에 설립되었으며, 호주의 보안 관련 전문 인력들로 구성
- 주로 중소기업 대상의 솔루션을 제공하고 있으며, 고객사의 약 90%가 태국 및 기타 아시아 지역에 소재한 글로벌 기업의 해외 지사
- 주요 제품군 및 서비스: 인터넷 보안 솔루션, 데이터 보안, 드라이브&데이터 복구, 보안 컨설팅 서비스

▶ Fortinet

- Fortinet은 태국 최대의 온라인 게임 제공사인 AsiaSoft의 안티바이러스 방화벽 시스템과 BAAC(Bank of Agriculture and Agricultural Cooperatives)에 네트워크 보안 솔루션을 제공 중
- 주요 제품군 및 서비스 : 안티 스파이웨어, 웹 보안, 안티바이러스 등

▶ Cyberoam

- Cyberoam은 동남아시아 전역에 걸쳐 파트너 및 리셀러를 보유하고 있으며, 태국 지역에서는 E-Rong Consultant Co., Ltd와 파트너십을 체결하고 ITessential, Infrotonic 등의 리셀러를 확보하고 있음
- Cyberoam은 IDC, Gartner 등 IT 전문 시장조사기관이 주목하는 정보보안 기업으로 떠오르고 있으며, Kaspersky Lab과 제휴를 맺고 바이러스 감지 기능을 강화하는 등 최근 혁신을 위한 노력을 거듭하고 있음
- 주요 제품군 및 서비스 :·방화벽, IPS, 안티바이러스, 안티스팸, VPN 등 정보 보안 전 분야에 걸친 제품 라인업을 보유

▶ SIMENSE

- ISA-99, IEC62443, DHS, BSI 등 규격 획득에 대한 컨설팅 진행
- 통합 Portal 서비스를 통해 네트워크 보안과 시스템 통합에 관한 보안 서비스 제공
- 네트워크에 대한 방화벽 및 VPN 채널에 대한 무단 침입보호 서비스

▶ Fujitsu

- Fujitsu는 24시간 운용하는 보안운영센터(SOC)를 통해 정보관리 서비스를 제공
- 바이오 인식 기반 솔루션, PalmSecure ID Match 기술을 통한 물리적 출입관리 등의 솔루션 제공

▶ BAE Systems

- 보안운영센터(SOC)를 통한 보안관리서비스(MSS) 제공
- 오픈 소스를 통한 공격에 관한 정보를 자동 탐지하여 취약성을 평가하고 검색하는 서비스 제공

▶ HIP Global

- HIP Global은 태국 보안 시장의 60%의 시장 점유율을 차지하고 있으며, 보유하고 있는 공공 그리고 개인 고객 수가 2,000에 다다름
- 원스톱(one-stop) 서비스와 보안 상품은 지문, 얼굴 스캔, 주차, 접이식 게이트, 서스펜션 게이트, 개찰구, 플립 게이트 등이 포함됨

▶ Hanwha Techwin

- Hanwha Techwin은 구 삼성 테크윈으로서 CCTV 카메라 등 보안 기술 제품 및 솔루션을 공급
- 아날로그 및 IP 네트워크 IP CCTV 시스템을 이용한 CCTV 제품을 제공

4) 주요 동향 및 이슈

▶ 태국 정부가 추진하는 'Thailand 4.0'은 정보화 사회로의 목표를 가속화시킬 것임

- 2016년 5월에 전격 개시된 Thailand 4.0은 디지털 태국을 위한 핵심 캠페인으로서 태국 정부는 중공업 기반에서 기술기반 국가로 점차 옮겨가고자 노력 중
- Thailand 4.0의 궁극적인 목표는 디지털 부분의 성장뿐만 아니라 전체적인 경제 구조를 기술 지향적으로 변환시켜 기존 대비 4~5%의 경제성장을 이루어내고 중진국의 함정에서 벗어나는 것임
- 동 캠페인은 일련의 수퍼 클러스터를 건설하고자 하는 계획으로, 전자부품, 전기/통신 클러스터, 디지털 클러스터, 친환경 화학 및 플라스틱 클러스터, 식품혁신센터(Food Innopolis), 우주항공 클러스터, 로봇 클러스터, 의학 클러스터 등의 산업이 이에 포함됨
- 아울러 태국 정부는 ICT 기술 발전을 통해 태국이 외국 기술의 소비시장이 아닌 자체적인 기술 및 서비스 시장을 보유한 국가고 발전하는 것을 추구함
- Thailand 4.0 하에, 태국 정부는 전국의 모든 마을을 대상으로 광대역 네트워크를 구축하기 위한 예산을 배정함. 이는 전자상거래 채널을 통해 디지털 격차를 해소하고 디지털 경제 발전을 촉진시킬 것

▶ 사이버보안 관련 인력의 부족

- 태국은 'Thailand 4.0' 전략을 추진하는 데 있어 사이버보안 관련 인력의 부족으로 인한 곤란을 겪고 있음
- 태국의 전자상거래개발청(ETDA)에 따르면 매년 사이버 공격이 10% 이상씩 늘어나고 있으며, 멀웨어, 랜섬웨어 공격이 증가하고 있지만 이에 대응하는 사이버 보안 인력은 태부족인 상황

※ 현재 태국에는 국제공인 정보시스템 보안전문가(CISSP, Certified Information System Security

Professional) 자격을 취득한 인력이 약 200명 있는 것으로 알려지고 있으며, 이는 한국의 약 2,800여 명, 싱가포르의 1,600여 명에 비해 상당히 부족한 수준

- ETDA의 Surangkana Wauparb 청장에 따르면 증가하고 있는 사이버 위험에 대응하기 위해서는 CISSP 전문가들이 적어도 800명 이상이어야 함
- 이를 위해 태국 정보보안협회(Thailand Information Security Association)와 협력하여 새로운 IT 보안 전문가를 위한 훈련과 전문인증자 제도를 발전시키기로 하였으며, CISSP 전문가들을 2017년 말까지 약 500여 명, 2022년까지 1,000여 명을 확보할 목표
- 보안 전문가, 보안 인력 1,000명의 보안 능력 향상을 위해 ETDA는 Cisco Thailand와 협업, Cisco는 또한 보안 지식을 태국 컴퓨터침해사고대응팀(ThaiCERT)에 제공하기로 함
- ETDA 산하의 ThaiCERT는 사이버보안 위협 경보를 받아 볼 수 있으며, 전 세계 포진되어 있는 Cisco의 인지, 교육, 가이던스 센터의 정보에 접근할 수 있게 됨

▶ 동남아시아 사이버보안 센터인 아세안-일본 사이버보안 능력 배양 센터 (The Asean-Japan Cybersecurity Capacity Building Centre)가 태국에 2018년 9월 14일 자로 설립, 이는 아세안 국가에서 사이버 공격에 취약한 지역을 돕기 위한 인력을 훈련시키는 것이 목표

- 동남아시아 내 약 700명의 인력이 일본이 구상한 프로그램을 이수할 것으로 기대됨. 이는 사이버 방어, 디지털 포렌식(digital forensics), 악성코드 분석을 포함

▶ Thailand Cybersecurity 2019 개최

- 태국 방콕에서 태국 전자거래 개발원(ETDA)는 2019년 6월 19-20일에 공공과 민간부문이 태국의 디지털 전환에 따른 사이버 위험에 대응할 수 있는 역량을 강화하기 위하여 Thailand Cybersecurity 2019를 개최함
- 동 행사는 사이버보안 관련 B2B 네트워킹 플랫폼인 CyberTechAsia 2019와 RSAC Unplugged와 함께 열려 사이버보안 관련 새로운 트렌드와 기술을 교환하고, 새로운 사이버 위험 관련 정보 교환이 활발하게 이루어짐

▶ IBM Think Thailand 개최

- 태국 방콕에서 2019년 8월에 IBM와 태국의 Samart 사는 사이버보안 솔루션 개발 협력을 위한 컨퍼런스를 개최
- 동 컨퍼런스에서는 양사가 SECUREiNFO라는 포괄적인 사이버보안 솔루션 서비스를 도입한다고 밝히고, Cyber Security Operation Center(CSOC)를 태국에서 처음으로 설립할 예정이라고 밝힘
- 동 센터는 클라이언트에게 최고 수준의 보안을 제공하기 위해 IBM의 인공지능 Watson 기술을 사용할 것이라고 밝힘

정보보호 정책 및 기관 현황

1) 관련 법령 및 정책

관련 법령 및 규제

▶ 2019년 2월 28일 정부에서 제출된 디지털 보안 관련 사이버보안법(Cybersecurity Act, CSA)와 개인정보보호법(Personal Data Protection Act, PDPA)이 국가입법회의(NLA)를 통과함

- 두 개의 법은 정부공보지에 5월 27일 게재되어 효력 발생
- 두 법이 효력을 발생함에 따라 태국에서는 새로운 두 개의 기구, 즉 국가사이버보안위원회(National Cyber Security Committee, NCSC)와 개인정보보호위원회사무국(Office of Personal Data Protection Board)이 태국의 사이버보안과 개인정보보호에 관한 업무를 맡게 될 예정
- 이 외에도 함께 통과된 디지털경제 활성화를 위해 통과된 법들은 전자거래기관구조개혁법(Electronics Transaction Organisation Restructuring Act), 디지털신원법(Digital ID), 디지털경제사회위원회법(Digital Economy and Society Council Act), 전자거래관리자법(Electronics Transaction Officer Act) 등임
- 6개의 디지털 관련 법들은 태국 정부의 Thailand 4.0과 디지털 정부를 위한 동력을 제공할 것이며, 정부의 빅데이터, 데이터센터, 클라우드 서비스, 원스톱 플랫폼과 같은 필요한 인터넷 인프라 개발을 선도하고 감독할 것임

▶ 사이버보안 법안 'Cybersecurity Act'(2019)

- 이번에 제정된 사이버보안법은 조항의 내용이 모호하고 정부가 인터넷 트래픽을 모니터링하고 검열에 대한 우려가 있다는 점 때문에 많은 시민 운동가들이나 외국 기업들의 우려를 표하는 가운데 통과되어 발효되었음
- 법안에 따르면 '사이버보안'의 개념은 국가안보, 경제안보, 국방안보, 사회질서에 영향을 미치는 국내외 사이버 공격의 위험을 방어하고, 통제하고, 감소시키는 방법과 절차를 수립하는 것이라고 정의 또한 '사이버 위험'은 컴퓨터나 컴퓨터 시스템, 컴퓨터 데이터, 기타 관련 데이터에 위해를 가하기 위해 고의적으로 수행하는 행위나 불법적인 조치라고 규정
- 동 법안에 따르면 사이버 위험의 수준은 ① 덜 위험한 수준의 사이버 위험(Non-critical level), ② 위험한 수준의 사이버 위험(Critical level) ③ 심각한 수준의 사이버 위험 수준(Crisis level)으로 나누고 있으며, 민간 기관에 대한 권한과 명령은 위 수준에 따라 달라짐

- 동 법의 대상이 되는 기관은 주요 정보 기반시설 기관(Critical Information Infrastructure Organization, CII)과 기타 민간 기관이 모두 포함될 수 있는데 주요 정보 기반시설 기관은 국가안보, 공공안전, 공공의 이익을 위한 기본 인프라를 운영하는 목적으로 컴퓨터나 컴퓨터 시스템을 사용한 민간 기관, 기타 민간 기관은 주요 정보 기반 시설 기관이 아닌 민간 기관으로 다음과 같은 의무를 부과함
  - 주요 정보 기반시설 기관은 ① 회사 소유자(들), 컴퓨터 소유자(들), 컴퓨터 시스템을 감시하는 사람(들)의 이른과 연락처 정보 제공 ② 실행규범(Code of Practice)과 최소한의 사이버보안 기준 준수 ③ 위험에 대한 평가 ④ 사이버 위험 즉각적인 보고 등의 의무가 있음. 아울러 기타 민간 기관에 부여하는 의무도 부과됨
  - 동 주요 정보 기반시설 기관은 다음의 업무를 수행하는 기관을 지칭함: 국가안보, 공공재화 서비스, 재정 및 금융, 정보기술 및 통신, 수송과 물류, 에너지 및 공공시설, 공중보건, 기타 국가 사이버 보안 위원회가 지정한 기관 등
  - 주요 정보 기반시설 기관이 아닌 민간 기관인 경우에도 사이버 위험이 있을 경우, 관련 감독기관이 ① 사이버 위험을 예방하기 위해 필요한 경우에 관련 컴퓨터 데이터 또는 컴퓨터 시스템을 감시할 수 있도록 조치 ② 컴퓨터 또는 컴퓨터 시스템에 대한 감시 허용 ③ 관련 공무원이 컴퓨터 또는 컴퓨터 시스템의 운용을 테스트하거나 컴퓨터 또는 컴퓨터 시스템, 또는 기타 장비를 압수 또는 동결하도록 허용할 의무가 있음
- 동 법에 따라 태국의 사이버보안 총 감독기관이 되는 국가 사이버 보안 위원회(NCSC)가 설립될 예정이며, 동 위원회는 총리가 의장, 국방부와 디지털경제사회부 장관은 당연직 위원이 될 것임
  - 사이버 위험이 2단계 위험한 수준과 3단계 심각한 수준의 경우, 동 위원회 사무총장은 지속적으로 사이버 위험과 관련된 당사자들에게 실시간으로 정보를 요구할 수 있고, 당사자들은 협력해야 함
  - 특히 사이버 위험이 심각한 수준일 경우, NCSC 사무총장은 치명적 사이버 위험이 발생한 현장에 가서 정보에 접근하고 컴퓨터 프로그램을 복사하고, 컴퓨터나 컴퓨터 시스템을 테스트 하거나 압류하여 사이버 위험을 예방하고 처리하며 완화하게 할 수 있음. 이는 법원 명령을 받기 이전에도 시행할 수 있으며, 사후에 지체 없이 법원에 이러한 행위에 대해 보고하여야 함

▶ 개인정보보호법 'Personal Data Protection Act'(2019)

- 이번에 도입된 개인정보보호법은 태국 최초로 법률에 의해 개인의 프라이버시가 보호되는 법률로 국내외 적용성, 정보주체에 대한 알림, 동의 필요, 미성년자 동의, 정보의 수집·이용·공개의 제한과 예외, 개인정보의 국외 전송, 민감한 정보에 대한 명시적인 동의와 예외 조항, 정보 주체의 권리, 보안대책, 정보 유출에 대한 통고, 데이터 컨트롤러 또는 프로세서 지정, 정보보책임자(DPO) 지정 등에 대한 내용을 담고 있음
  - 동 법에서 정의하고 있는 '개인정보'는 직간접적으로 개인을 식별할 수 있는 정보로 규정하고 민간사업자, 사망자에 관한 정보는 제외

- 또한 '민감정보'는 인종, 특정 소수인종, 정치적 견해, 종교적/철학적 믿음, 범죄경력, 노동조합원, 유전정보, 생체정보, 건강 관련 정보, 자연인의 성적 지향 또는 성생활에 대한 정보를 포함하며, 이러한 정보에 대해서는 특정상황(긴급 의료 상황이나 법에 의한 필요)의 예외를 제외하고는 개인의 동의 없이 수집이 금지됨
- 정보컨트롤러: 개인정보의 수집, 사용, 공개에 대한 결정을 내리는 권한을 가진 자연인 또는 법인
- 정보프로세서: 정보컨트롤러의 지시에 따라 개인정보의 수집, 사용, 공개를 진행하는 자연인 또는 법인
- 동의: 정보주체의 동의는 기본 필요조건으로 법은 이러한 동의를 명확히 하여야 하며 정보주체를 오도하지 않는 방법으로 획득하여야 함을 명기. 단 명시적으로 핵심적인 이익, 개인적 이익, 법률적 의무, 또는 당사자들 간의 계약에 의한 의무에 구속되는 경우에는 동의의 의무가 면제됨
- 정보컨트롤러와 프로세서의 의무: 정보관리자에게 법적 수단이나 목적 내에서 정보를 수집하는 것을 포함하는 것에 대한 의무를 부과하며, 정보관리자는 정보주체에게 정보주체의 개인정보를 수집하는 것에 대한 내용을 알려야 하며, 동의를 획득하여야 함. 정보관리자는 정보의 유출 방지, 불법적인 활동에 의한 정보의 변경 등을 방지하기 위한 적절한 보안조치를 실행하여야 함
- 담당 기관은 정보컨트롤러로 하여금 정보의 수집, 이용, 공개, 처리 활동을 포함하여 이러한 절차를 감독하도록 의무를 부과함
- 개인정보의 유출이나 개인정보 침해의 사건이 발생하였을 경우 72시간 이내에 개인정보보호 위원회 사무국에 고지하여야 함

• 유의하여야 할 점은 고용주가 인력을 아웃소싱하여 외부 인력파견 회사에 서비스를 받는다고 하더라고 서비스 제공자가 위법한 행위를 하게 되면 고용주도 같은 책임을 지게 된다는 점임
- 즉 개인정보보호법 위반의 경우, 고용주나 인력파견 서비스 제공자나 모두 민사상 배상책임을 받을 수 있으며 법원은 징벌적 손해배상을 내릴 수 있음
- 또한 고용주는 형사적 책임도 면할 수 없음. 이럴 경우 6개월의 실형을 받거나 50만 바트까지의 벌금에 처할 수 있음
- 만일 형사나 민사처벌과의 함께 행정처벌도 받을 수 있으며 이럴 경우 침해 정도에 따라 50만 바트에서 500만 바트까지의 벌금 처분을 받을 수 있음

• 동 법에 의한 개인정보 수집 제한과 관련하여, 데이터 컨트롤러는 정보주체로부터 온라인상이나 문서상으로 개인정보 처리 이전에 동의를 받아야 하며, 개인정보와 민감정보를 저장하기 위해서는 충분한 보안조치를 마련하여야 하고, 개인정보의 제3국 전송에 대한 제한, 정보 유출에 대한 고지 의무, 태국 밖에 있는 데이터 컨트롤러는 태국 내에 대표를 지명하여야 하며, 이 대표는 법에 의한 권리와 의무를 지니고 있어야 함

주요 전략 및 정책

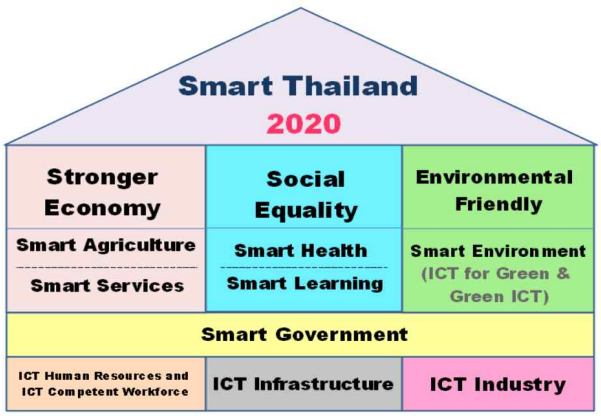
▶ 태국 정부는 현재까지 신기술 부문 발전을 위해 IT2010, ICT Master Plan(2002-2006), ICT Master Plan Extended(2007-2008), ICT Policy Framework 2020(2011-2020, ICT2020), National Digital Economy Policy and Plan(2016-2020) 등을 차례로 계획하여 실천해 오고 있음

- IT2010은 ▲태국의 'Technology Achievement Index(TAI)' 등급을 'dynamic adopters'에서 'potential leader'로 올리는 것과 ▲태국의 지식노동자들을 2010년까지 전체 노동력의 30%까지 확대하는 것, ▲GDP의 50%까지 지식기반 산업에서 나오게 하는 것 등의 목표를 가지고 있었음
- 이러한 계획을 바탕으로 정보통신기술부(MICT)에서는 향후 10년 간의 ICT 정책의 목표와 전략을 구상한 ICT2020을 발전시켰음

▶ ICT2020 전략은 현재 태국이 추진하고 있는 ICT 정책의 근간이 되는 계획으로 여러 가지 목표와 전략을 표방하고 있음

- IT2010 계획의 후속으로 태국의 정보통신기술부는 ICT2020 정책을 구상하여 향후 10년(2011-2020)의 정보통신정책 목표와 전략을 전개
- 동 전략의 원칙은 사회, 경제, 환경 차원의 균형 발전, ICT가 모두에게 이익이 되는 기회 제공, 현대적인 사회 유지 및 함께 경제발전에 있어 국가 능력에 맞는 개념을 고려, 지난 정책과의 연계성, 공공부문에의 민간 참여 등임

그림 _ ICT 2020의 비전과 목표



ICT 2020 Framework

[출처] 정보통신기술부(MICT)

- ICT는 '스마트 태국 2020(Smart Thailand 2020)'을 이루기 위한 기반 인프라가 될 것이며, 사회를 평등과 지속가능한 경제로 이끌 핵심 전력이라는 것이 ICT2020의 기본 프레임워크임
- ICT2020은 목표를 이룩하기 위한 7가지 전략을 제시하고 있음
  - 첫째, 보편적이고 안전한 광대역 인프라 구축 : ICT 인프라는 모든 사람들이 접근 가능한 보편적인 국가 기본 시설로서 세계적 수준의 보안을 유지하여야 하며, 유무선 고속 네트워크 투자에 민간 참여를 보장하고 자유롭고 공정한 경쟁을 보장하며, 이를 통해 디지털 생태계를 창조함
  - 둘째, ICT 관련 인력 확대와 경쟁력 있는 ICT 노동력 확보 : 다양한 분야에서 필요로 하는 인력을 위한 기술 수준 발전을 위한 국가적 차원의 계획을 마련함
  - 셋째, ICT 산업의 경쟁력을 확보하고 아세안 통합에 대비 : ICT 산업현장에서의 기존 인력과 신규 인력에 대한 지속적인 인력을 개발하고 국제적인 시장을 목표로 ICT 상품과 서비스 질을 발전시키고 브랜드를 개발. 특히 아세안 시장 통합과 관련하여 산업 발전을 위해 지역적 협력을 강화하고, 태국 기업들이 아세안 국가들과 상품 개발, 서비스 마케팅에 있어 상호 협력하도록 지원함
  - 넷째, 스마트 정부를 환경 조성을 위해 정부 서비스 혁신과 거버넌스를 개선 : 우선 전자정부를 책임질 중앙기관을 설치하고, 중앙과 지방 정부의 ICT 표준에 대한 가이드라인을 제시. 정부의 CIO 위원회를 강화하며 정부의 각 부서나 지방 정부에도 CIO를 설치. 또한 열린 정부 정책에 따라 e-서비스를 발전시키도록 하며 투명성과 책임성, 공공부문과 민간부문의 협력 강화 및 정부 서비스 개발을 위한 R&D 강화함
  - 다섯째, 태국의 비교 우위의 상품과 서비스의 혁신과 창조성, 지식을 창조하는 추진력으로의 ICT 전략을 추진 : 기존의 제조업 강화를 위해 물류와 공급 망에 대한 ICT 기술 발전을 강화하고, 태국이 장점이 있는 서비스 부분에 대한 R&D 지원을 위한 책임기관을 설립함
  - 여섯째, 사회 평등을 보장하는 ICT의 추진 : 정보 인프라를 균등하게 배분하여 도시나 지방에서 모든 국민이 초고속 네트워크에 접근 가능하도록 함. 디지털 미디어도 모든 사람들이 매일 접근할 수 있으며, 교육 TV 지역 언어 방송에도 할당. 아울러 e-정부 서비스도 모든 사람이 매일 서비스 받을 수 있도록 다양한 채널로 공급. 어떤 경우에든 사회경제적인 불평등을 줄일 수 있도록 ICT를 제공하고 발전시킴
  - 일곱 번째, Green ICT를 추진: 녹색경제와 녹색사회 발전 추진을 위한 ICT 발전전략을 추구하며, 에너지 절약과 환경보호의 수단으로서 ICT 사용 증진

▶ 2014년 군사 쿠데타를 통해 집권한 군사정부도 ICT2020에 기초한 새로운 ICT 발전을 도모해 '경제와 사회를 위한 디지털 발전 계획'(Digital Development Plan for Economy and Society(2016-2020))을 추진

- 동 계획은 국가 디지털 경제 마스터플랜(National Digital Economy Master Plan)으로서 인프라 발전과 혁신, 정보기술 발전, 노동력 개발, 여타의 자원개발 등에 있어 디지털 기술을 사용토록 유도하고,

디지털 기술을 통한 국가경제 및 사회 발전을 목적으로 함

- 마스터플랜은 향후 20년간 디지털의 기초를 형성 및 활용하여 모든 산업을 디지털화하고 궁극적으로 태국을"Digital Thailand"로 만들어 나아가겠다는 전략임
- 현재 동 계획의 일환으로 디지털 경제관련 법안들도 과도의회의 승인을 기다리고 있으며, 2001년의 전자거래법에 관한 개선안, 사이버 범죄, 사이버 보호, 개인 프라이버시와 같은 것들이 논의되고 있음

▶ 디지털 경제 발전을 위한 SIGMA

- 태국의 디지털경제사회부는 태국의 디지털 전환을 위한 기본 5원칙으로 SIGMA 프레임워크를 제안하고 이에 기반한 Thailand 4.0을 추진할 예정이라고 밝힘
- SIGMA 원칙은 ① S(Cybersecurity): 개인정보와 조직 및 인프라를 사이버 위험으로부터 보호, ② I(Digital Infrastructure): 사회 불균형을 감소시키는 정보 인프라의 중요성 강조 ③ G(Digital Governement): 민간기업이 공공부문에 더 쉽게 접근할 수 있는 다양한 전략 ④ M(Digital Manpower): Thailand 4.0 추진을 위한 핵심인력 개발 ⑤ A(Digital Application): 태국 경제가 새로운 비즈니스로 개방하는데 도움이 되는 매체 개발 등임

2) 담당기관

▶ 디지털경제사회부(Ministry of Digital Economy and Society: MDES)

- MDES는 2016년 컴퓨터 범죄법을 개정하기 위한 제안(Draft CCA 2016)에 의해 정보통신기술부에서 부서 명칭을 디지털경제사회부로 변경하여 설립된 내각부서
- MDES는 태국 내 경제와 사회의 디지털화를 촉진하기 위한 정책과 계획을 수립하고, 태국의 정보통신 네트워크의 관리와 통신 인프라의 개발을 촉진하기 위한 업무를 담당
- 또한 디지털 기술을 활용하는 산업의 활성화와 정부 내 디지털 거버넌스의 담당기관
- 각종 법안과 규제를 통해 사이버보안을 총괄하고 있음
- 2019년 7월 10일 개각을 통해 장관으로 붓티퐁 푼나칸(Buddhipongse Punnakanta)이 지명되었으며, 부장관으로는 Nawin Chochaiyathip, 사무차관으로는 Ms. Ajarin Pattanapanchai이 지명됨
- 산하에 전자상거래 발전과 사이버 보안에 관한 집행기관인 전자상거래개발청(Electronic Transaction Development Agency: ETDA), 전자정부 집행기관인 전자정부청(Electronic Government Agency: EGA), 소프트웨어 산업 발전과 지원을 위한 디지털 경제진흥청(Digital Economy Promotion Agency: DEPA), 기상국(Meteorological Department), 국가통계실(National Statistical Office) 등이 있으며, 공공기관은 태국전화공사(Telephone Organization of Thailand, TOT), 태국통신공사

(Communications Authority of Thailand, CAT)를 두고 있음

▶ 전자상거래개발청(Electronic Transaction Development Agency: ETDA)

- 2010년 정보통신기술부 산하에 전자상거래를 활성화하기 위해 설립된 ETDA는 전자상거래 활성화를 위한 인프라 개발과 기술적인 서비스를 제공하는 업무 담당
- EDTA의 주 서비스 영역은 전자상거래 관련 정책 및 기획, 국가 전자상거래 통계 작성, 전자상거래 관련 법제, 전자상거래 보안 및 표준화, 전사상거래 관련 핵심 인프라 개발 등임
- 또한 침해사고대응팀(ThaiCERT)이 ETDA 산하로 들어오면서 보안 관련 사이버보안 분야에 있어서도 정부 및 금융기관, 일반 기업 등에 대한 보안 교육을 강화하고 있음
- ETDA 대표는 Surangkana Wayuparb이며, 이사회 의장은 Jirawan Boonperm이 맡고 있음

▶ 태국 컴퓨터침해사고대응팀(Thailand Computer Emergency Response Team: ThaiCERT)

- ThaiCERT는 태국 내 유일한 침해 사고 관련 긴급대응 공공기관임
- 2000년에 과학기술부 산하 국가전자 및 컴퓨터기술센터(National Electronics and Computer Technology Center)에 설립되었다가 2011년에 ETDA 산하로 소속이 변경됨
- ThaiCERT의 주 업무는 컴퓨터 네트워크에 발생하는 모든 사건에 관련 당사자들에 대한 조정과 필요한 정보를 전파하는 것임. 정부, 민간단체, 학계 등과 연계해 사이버 공격에 대응하고 있으며, 보안사고대응팀 포럼(Forum of Incident Response and Security Teams: FIRST), 아시아태평양 컴퓨터 침해사고대응팀(Asia-Pacific Computer Emergency Response Team: APCERT)에 참여하여 정보보안 체계에 관한 국제적 협력 관계를 구축
- 또한 디지털 포렌식 서비스도 제공

▶ 국가방송통신위원회(National Broadcasting and Telecommunication Commission, NBTC)

- NBTC는 태국의 주파수 관리 및 라이선스 제공 기구로 통신 분야 비즈니스 규제 기관으로 소비자 보호와 네트워크 관리 기구
- 2010년에 관련법에 따라 설립되었으며, 주요 업무로는 주파수 라이선스 규제, 통신업무 및 민간 비즈니스의 공정성 및 품질 관련 규제, 통신 번호 규제, 네트워크 접근 및 상호연결의 기준 및 절차 규제, 통신 서비스 요금 규제, 통신서비스 표준 및 기술 사양 설정, 보편적인 통신서비스 확대, 소비자 보호, 통신서비스의 감시 등의 업무를 수행
- 현재 위원장은 Sukit Khamasundara 장군이 부위원장으로는 군인인 Natee Sukonrat 박사와 Settapong Malisuwan 박사가 맡고 있음

▶ 최근 통과된 개인정보보호법과 사이버보안법에 따라 개인정보보호 관련하여서는 개인정보보호위원회

(Personal Data Protection Committee, PDPC)와 사이버보안과 관련하여서는 국가사이버보안위원회(National Cyber Security Committee, NCSC)가 각각 설립되어 담당업무를 맡을 예정

3) 정보보호 인증제도

▶ 태국 시장은 정보보안 네트워크 등의 제품에 대한 국제 인증을 인정

- 태국 정부는 보안 제품에 대한 로컬 인증을 따로 실시하고 있지 않으며, 태국 시장에 진출한 글로벌 기업들은 대부분 국제 CC 인증을 취득하여 시장에 해당 제품의 공신력과 기술력을 입증하고 있음

▶ CC(Common Criteria) 인증은 한국·미국·영국·캐나다·호주 등 세계 20개국에서 사용하는 정보보호제품의 평가 기준으로, 최고 등급은 EAL 5등급임

- 외국 보안 업체는 CC 인증 취득을 통해 태국을 비롯한 동남아 시장에 진입하면서 이를 자사제품의 공신력 및 기술력을 입증하는 마케팅 전략으로 활용할 수 있음

4) 최근 정책 동향 및 이슈

▶ 태국, 사이버보안 강화 위해 사이버보안 담당 기관 설립 예정 발표[130](2018.5)

- 2018년 5월, 태국의 IT분야 담당기관인 전자거래진흥청(ETDA)에 따르면 태국의 Prrayut Chan-ocha 총리가 처음으로 사이버보안에 관한 국가 안전보장 회의를 주재
- 회의에서 총리는 사이버보안 대응 측면에서 태국이 세계 톱 20 국가에 진입하는 것을 국가 목표로 제시
- 또한 사이버보안 강국이 되기 위해 다음의 4가지 핵심 포인트를 언급
  - 사이버보안 위협의 위험을 보호하고 예방 및 감소시킬 수 있는 국가 정책 프레임워크의 중요성 강조
  - 주요정보기반시설(CII)의 사이버보안과 관련된 긴급 상황 처리를 위해 지침 및 표준 운영 절차(SOP) 작성: 태국은 CII로 ▲국가 안보 및 공공서비스 ▲운송 및 물류 ▲금융 ▲에너지 및 유틸리티 ▲공중보건 ▲통신 6대 분야를 지정
  - 사이버보안 인력 개발: 공공부문에서 1,000명의 사이버보안 인력 양성

130https://www.opengovasia.com/thailand-plans-to-set-up-cybersecurity-agency-to-boost-cybersecurity-preparedness/

- 사이버보안 문제를 조정하고 이에 대응하는 책임을 맡을 사이버보안청(CSA, CyberSecurity Agency) 설립: EDTA와 태국컴퓨터긴급대응팀의 인력으로 구성

• 태국 정부는 사이버보안을 위한 예산 3억 5,000만 바트를 디지털 경제 기금에서 마련할 계획

▶ 태국 정부는 일본의 지원을 받아 태국 현지에 아세안-일본 사이버보안 역량 구축 센터 (ASEAN-Japan Cybersecurity Capacity Building Center, AJCCBC)를 2018년 9월에 설립

• 동 사이버보안 센터는 사이버 위험에 대한 아세안 국가들의 인력을 훈련시키기 위한 목적
• 약 700여 명의 인력이 일본식으로 디자인된 프로그램으로 교육받을 것으로 예상
• 교육 프로그램은 사이버 방어, 디지털 포렌식, 멀웨어 분석 등이 포함될 예정

▶ 개인정보보호법 및 사이버보안법과 함께 디지털 관련 법률들이 통과되어 태국 정부의 디지털 전환을 위한 동력을 제공할 것으로 예상됨

• 동 법률들은 전자거래기관구조개혁법(Electronics Transaction Organisation Restructuring Act), 디지털신원법(Digital ID), 디지털 경제사회위원회법(Digital Economy and Society Council Act), 전자거래관리자법(Electronics Transaction Officer Act) 등임

▶ 태국 외무부는 DGM 컨소시엄(Gemalto, Thales Company, Data Products Toppan Forms, MultiCert)의 도움을 받아 매우 보안성이 높은 전자여권(e-passport)를 도입할 예정[131]

• 전자여권 프로젝트는 2019년에 외무부와 컨소시엄간 계약이 체결되어 태국 시민 약 1,500만 명에게 새로운 여권이 제공될 예정
• 생체정보가 포함된 새로운 64페이지짜리 전자 여권은 얇고 소지자의 얼굴 이미지가 들어간 폴리카보네이트 커버 페이지를 포함
• 동 전자여권은 국제민간항공기구(ICAO)가 제시하는 최고 수준의 보안 표준을 준수하여 만들어질 것이며, 임베디드 소프트웨어를 통해 빠른 시간 국경을 통과할 수 있을 것임
• 현재 22개의 여권 갱신 사이트에서 기존 여권을 갱신할 수 있으며, 15개 새로운 사이트를 신설하여 시민의 편의를 제공할 예정임

131 HELPNETSECURITY, 2019.8.29

융합보안시장 및 정책 동향

1) 융합보안 시장 현황

▶ Barnes Report에 따르면 태국의 커텍티드 자동차에 대한 보안(Automotive Cyber Security) 시장 규모는 2020년에 약 6,000만 달러에 달할 것으로 예측

- 동 보고서에 따르면 태국의 자동차 사이버보안 장비 시장 규모는 2019년에 약 5,070만 달러에 달하며, 2020년까지 약 18.9%의 성장률을 보일 것으로 예측
- 또한 동 시장규모는 2025년이 되면 약 1억 4,600만 달러에 이를 것으로 예상

표_태국과 전 세계 자동차 보안시장 규모 예측(단위: 백만 달러)

구분	2017	2018	2019	2020
세계시장	3,564.5	4,438.6	5,446.4	6,557.2
아태시장	1,764.7	2,247.2	2,824.8	3,431.4
태국시장	32.5	41.1	50.7	60.3

출처: Barnes Report(2019)

스마트시티

▶ 방콕, 2019년 전 세계 스마트시티 지수에서 102개 도시 중에서 75위 차지

- 태국 방콕이 스위스 IMD 경영대학원 산하 세계경쟁력센터의 스마트시티연구소(Smart City Observatory)와 싱가포르기술대학이 공동으로 개발한 'IMD Smart City(SCI) Index 2019'에서 평가를 받은 102개 도시 중에서 75위를 차지
- SCI Index는 도시를 '스마트하게' 만들기 위한 노력의 범위와 정도뿐만 아니라, '경제적 및 기술적' 발전과 '인간적 차원(Human dimension)'의 균형을 맞추고 있는지 여부을 중점적으로 평가
- 태국 IMD 경영대학원 관계자는 방콕이 대중교통의 온라인 예약이나 승차권 같은 분야는 양호하나, 모빌리티와 대기환경 분야, 녹지, 일반 문화 활동 분야에서는 상당한 이슈와 선결과제가 있다고 지적

자율주행차

▶ 자율주행 3륜차에 대한 테스트 진행

- 태국 일반 거리의 통상적인 교통 수단이 되고 있는 3륜차 'tuk-tuk'에 대해서 자율주행 기술을

접목시키고자 하는 민관 협력 차원의 프로젝트가 진행

- 자율주행차 스타트업 Airovr, 투자업체인 Siri Ventures, 태국 정부가 방콕 시내 특정 지역에서 자율주행 'tuk-tuk'에 대한 테스트를 진행하고, 여기에서 도출될 결과를 바탕으로 향후 미니버스와 대형 차량에도 자율주행 기술 적용할 방침

사물인터넷(IoT)

▶ 중국 화웨이, 태국 NB-IoT 시장 공략에 주력 발표

- 2019년 8월초 중국 화웨이가 '태국 IoT 산업 서밋 2019' 행사를 개최하고, NB-IoT 기반 사물인터넷 사업을 강화하고 있다고 발표
- 화웨이는 태국이 NB-IoT 방식의 사물인터넷 네트워크가 구축된 주요 국가이며, '스마트시티', '스마트인더스트리', '스마트라이프' 등 3개 분야 중심의 사물인터넷 사업 추진 계획을 공개

스마트공장

▶ 스마트팩토리, 태국 제조업 활성화의 주요 대안으로 주목

- 태국 제조업이 증가하는 제품 수요에 부응하는 생산량을 증대시키지 못하고 있는 상황에 처해 있으며, 이를 해소할 대안으로서, 스마트팩토리 또는 인더스트리4.0의 추진이 필요하다는 주장 제기
- 방콕 소재 IoT 및 인더스트리4.0 업체인 '어드밴텍(Advantech)'는 2016년 이후 태국 제조업에서 생산되는 제품에 대한 수요가 증가하고 있다고 분ㄴ석
- 또한 인더스트리4.0 솔루션 도입을 희망하는 태국 제조업체들의 50% 이상이 IoT 게이트웨이, IoT 인프라 등 스마트팩토리 도입을 희망하고 있다고 언급

블록체인(가상화폐 포함)

▶ 태국 상공업은행(JSCCIB), 블록체인 기반 수출입 거래 플랫폼 구축

- 2019년 11월 태국 상공업은행(The Joint Standing Committee of Commerce, Industry and Banking, JSCCIB)이 블록체인 기술을 활용한 거래 플랫폼을 구축했다고 발표
- 해당 플랫폼의 구축은 태국에서 진행 중인 국가디지털거래플랫폼((National Digital Trade Platform, NDTP) 개발 프로젝트 중에서 민간 분야 사례로 추진
- NDTP는 거래 처리 비용과 시간을 줄임으로써 거래 효율성을 높이고, 이중 금융 및 사기성 문서를 억제하고 중소기업 금융 접근성을 향상시키는데 기여할 수 있을 것으로 예상

핀테크 등

▶ 태국 은행업계, 핀테크 사업 위한 자회사 분리 시도
- 태국 자산 규모 3위에 해당하는 Siam Commercial Bank가 10억달러 이상 가치를 내는 유니콘 기업으로 육성하겠다는 목표하에 내부 핀테크 사업 조직을 별도의 자회사로 분리하는 조치 단행
- 현재 Siam Commercial Bank를 포함해서 태국 은행 업계는 대출 사업 마진 감소 속에서 스타트업과의 핀테크 분야 경쟁을 위해 관련 투자에 나서고 있는 상황

2) 융합보안 정책 현황

▶ 태국 국가방송통신위원회(NBTC)는 연말까지 사물인터넷(IOT) 장치 규제에 관한 초안을 발표할 예정
- 동 규제는 ① 넘버링과 ID ② 스펙트럼과 기술표준 ③ 주파수 통신에 대한 허가와 경쟁 ④ 보안과 프라이버시 ⑤ 데이터 구조 및 상호운용성 등에 대한 내용이 포함될 예정
- NBTC는 각 분야별 규제 사항을 담당할 5개의 소위원회를 지명하였다고 밝힘

▶ 태국 공중보건부(MOPH)가 제시한 eHealth 전략(eHealth Strategy 2017-2026) 프레임워크[132]
- 동 프레임워크는 3개의 전략을 제시하고 있으며, 그 중 전략3: 건강정보 표준, 효과적인 데이터 통합 및 상호 운용성의 부문에서의 세부 실행계획으로 ① 효율적인 상호운용성을 확보를 위한 데이터 공유를 위해 건강정보 표준 설정 ② 국가 건강정보 저장공간 개발 ③ 건강정보 보안 기준 개발 ④ 건강 시스템의 효율성 지표에 대한 모니터링 개발 ⑤ 건강시스템 예측 등과 같은 관측 시스템의 개발 등을 들고 있음
- 이와 관련 동 전략의 목표를 달성하기 위한 가장 기초적인 인프라로 연결성(Conentivity), 저장(Storage), 보안(Security), 표준(Standards), 컴퓨팅 등이 될 것으로 설정하고 있음

▶ 태국 5개 대형 상업은행들은 2019년 4/4분기 내에 보안 강화를 위해 QR 코드 지불방식을 도입할 예정
- 태국의 5개 상업은행, Siam Commercial Bank, Kasikornbank, Bangkok Bank, Krungthai Bank, Bank of Ayudhhya 등은 MyPrompt QR 지불 방식을 토한 모바일 지불 시스템을 도입할 예정이라고 밝힘
- 표준화된 MyPrompt QR 기술은 소비자들에게 더욱 편리하면서 빠르고 한층 더 높은 수준의 보안을 제공하게 될 것이라는 점을 강조
- 동 기술은 태국의 중앙은행과 민간 지불 시스템인 PromptPay 플랫폼이 공동 개발한 것으로, 향후

132 Ministry of Public Health, eHealth Strategy(2017-2026), 2017

캄보디아, 라오스, 미얀마, 베트남 등지로 확대될 가능성이 있다고 밝힘

- 향후 약 5백만 개 상점에서 월간 약 10억 바트 규모의 거래가 MyPrompt QR로 거래될 것으로 예상
- 5개의 상업 은행 이 외에도 다른 4개 은행은 2020년도에 동 시스템 활용에 가입할 예정

스마트시티

▶ 태국 정부가 2020년까지 24개주 30개 도시를 스마트시티로 전환하고, 2022년까지 전국 100개 도시를 스마트시티로 전환하는 프로젝트를 추진

- 정부 주도 스마트시티 담당 관청인 디지털경제진흥청(Digital Economy Promotion Agency, Depa)에 의하면, 2019년 7월말 현재, ▲푸켓 ▲치앙마이 ▲콘캔 ▲방콕 ▲촌부리 ▲라용 ▲차청 사오 ▲얄라 및 ▲나콘 라차 시마 등 9개주 20개 도시가 스마트시트 프로젝트에 신청서를 제출
- 태국 정부는 ①명확한 지리적 경제와 스마트시티 구축의 명확한 목표, ②인프라 투자 및 발전 계획, ③개방적이고 안전한 데이터플랫폼 설계, ④스마트시티 솔루션 확보, ⑤지속가능한 관리 모델 등 5개 기준을 충족시켜야 스마트시티 프로젝트 추진 도시로 선정될 수 있다고 발표

스마트의료

▶국가 디지털 헬스케어 인력개발 이니셔티브(WDI) 개시

- 태국에서 의사와 간호사 인력의 부족 상황이 발생하면서, 초고속인터넷, 모바일 기기, 애플리케이션, IoT, 인공지능, 가상현실 등이 결합된 원격의료와 디지털 헬스케어의 중요성 증대
- 디지털 헬스케어 기술은 농촌 또는 비도심 지역의 시민과 응급 치료의 수준을 높여, 의료 서비스 및 삶의 질 개선에도 기여할 것으로 기대를 모으고 있음
- 2019년 10월 17일 HIMSS AsiaPac 2019 컨퍼런스에서 발표된 디지털 헬스케어 인력 개발 이니셔티브(Thailand National Digital Healthcare Workforce Development Initiative(WDI)는 향후 3년간 디지털 헬스케어 서비스 개선과 헬스케어 산업 육성에 투입될 보건의료 인력의 디지털 역량 향상에 초점을 맞춘 프로그램임.

블록체인(가상화폐 포함)

▶ 태국 세무당국, 2020년까지, 블록체인 기반 세금 환급 시스템을 2020년 중반까지 구축 계획

- 태국 소비세청(Excise Department)이 2020년 중반까지 블록체인 기술을 활용한 세금환급 시스템을 구축하겠다고 발표

- 국영은행인 크룽타이 은행(Krungthai Bank)과 협력하여 구축하는 해당 시스템은 석유수출 관련 업무에 적용될 것으로 보임

핀테크 등

▶ 홍콩과 디지털 토큰(token) 분야 협력 체결

- 태국과 홍콩의 통화금융 당국이 핀테크 기반으로 양국간 자금 이체를 위한 프로세스의 일부로서 2계층(two-tier) 디지털 토큰을 출시할 계획을 추진
- 양국의 2계층 디지털 토큰 시스템은 지난 2019년 5월 HKMA와 태국 중앙은행(Bank of Thailand) 간 핀테크 협력 체결을 통해 11월 시작된 'LionRock-Inthanon' 프로젝트에서 한 단계 발전한 양상
- 블록체인 기반 디지털 토큰의 사용은 양국간 보다 신속한 통화 결제를 가능하게 할 것이며, 홍콩 달러와 태국 바트화를 거래하는 기업과 은행에도 긍정적 영향을 미칠 전망

사. 말레이시아

'18년 GDP(십억달러)	354.35
'18년 인구수(천명)	31,530

■ ITU 글로벌 사이버보안 지수(Global Cybersecurity Index, GCI)

· 말레이시아의 사이버보안 지수는 한국과 거의 비슷한 수준이며, 선도 그룹에 속함

국가명	2018		2017		전년대비 증감	
	지수	순위	지수	순위	지수	순위
말레이시아	0.893	8	0.893	3	-	-5
대한민국	0.873	15	0.782	13	+0.091	-2

■ ICT 관련 주요 지수

· 말레이시아의 전반적인 ICT 발전 수준은 상위권을 유지하고 있음

지표명	말레이시아		한국	
	점수	순위	점수	순위
IMD 국가경쟁력지수(2019)	-	22	-	28
IMD 디지털경쟁력지수(2019)	-	26	-	10
UNCTAD 전자상거래지수(2019)	81.9	34	89.4	19
ITU 글로벌 사이버보안 지수(GCI 2018)	0.893	8	0.873	15
UN 전자정부 지수(2018)	0.717	48	0.901	3

■ ICT 관련 주요 통계 (ITU, 2018년 말 기준)

· 말레이시아의 유선통신 보급률은 20%로 다소 낮으며, 이동통신(ICT) 보급률은 세계 상위권을 유지

항목	말레이시아		한국	
	가입자수(천 명)	보급률(%)	가입자수(천 명)	보급률(%)
유선전화	6,433	20.41	25,907	50.63
유선브로드밴드	2,696	8.55	21,286	41.60
이동통신	42,413	134.53	66,356	129.67
인터넷 이용률	81.20%		95.90%	

정보보호 산업 개요

1) 보안 환경

▶ ITU가 2019년 3월 발표한 'Global Cybersecurity Index (GCI) 2018'에 따르면 아시아-태평양 지역에서 싱가포르와 함께 일찍부터 사이버 보안을 주도해온 말레이시아의 사이버보안 지수는 0.893으로 전 세계 순위 8위, 아시아-태평양지역에서 2위를 차지한 것으로 나타남

- 해당 지수는 법적·기술적·조직적 대응 및 역량강화, 국제협력 등 5개 부문의 지수를 종합한 것으로, 말레이시아는 조직적인 부분(0.2)과 역량강화(0.198) 부문 그리고 기술적 부문(0.196)에서 높은 지수를 나타내고 있으며, 국제협력 부문(0.120)이 상대적으로 낮은 지수를 나타냄
- 특히 말레이시아가 국가사이버보안청(National Cyber Security Agency, NACSA)를 설립하여 사이버보안 분야에서 국가 최고의 전문가와 자원을 조정하고 통합으로써 모든 국가 사이버 보안 문제를 주도하고 감독하고 있음을 강조
- 말레이시아의 경우 산업계와 협력하여 보안서비스 및 클라우드 보안 실무를 위한 모범 사례 지침을 개발하였으며, 클라우드 보안 인증 체계를 수립하기 위해 클라우드 보안 실무가 준비 중임
- 온라인 금융 사기와 싸우기 위해 현지 금융기관, 말레이시아 통신 및 멀티미디어 위원회(Malaysian Communications and Multimedia Commission, MCMC), 사이버보안 말레이시아(CyberSecurity Malaysia, CSM), 왕립 말레이시아 경찰로 구성된 인터넷 뱅킹 태스크 포스(Internet Banking Task Force)가 설립됨
- 디지털 포렌식 연구소를 운영하는 모든 법 집행 기관으로 구성된 디지털 포렌식 실무 그룹(Digital Forensics Working Group)이 만들어지고 있음
- CNII(Critical national information infrastructure) 기관은 사이버 보안 기술 분야의 모범 사례 및 정보 공유에 대해 논의함
- MCMC 네트워크 보안 센터(Network Security Centre) 및 방위 보안 센터(Defense Security Centre)를 포함한 다른 사이버 운영 센터에 연결된 국가 사이버 조정 및 명령 센터(National Cyber Coordination and Command Centre, NC4)는 모든 CNII 기관에 기술 자문을 제공함
- 국가 사이버 훈련(X-Maya)은 사이버 사고를 처리하기 위해 CNII IT 직원의 기술 능력을 테스트하고 개선하고 있으며, CMERP(Coordinated Malware Eradication and Remediation Project)는 국가 차원에서 멀웨어 위협을 해결하기 위한 파일럿 프로젝트를 시행함
- 말레이시아는 CCRA(Common Criteria Recognition Arrangement)의 회원이며, CC(Common Criteria Information Technology Security Evaluation)의 인증서-인증(certificate-authorizing) 회원임

- MS ISO/IEC 27001:2013 표준 준수에 대한 조직/기관 자체 평가를 위한 ISMS(Information Security Management System) 비즈니스 프로세스 자동화 도구에 추가하여 SCADA(supervisory control and data acquisition) 보안 테스팅 시뮬레이션 랩이 설립되어 있음
- 또한, NC4는 CyberSecurity Malasia와 MCMC가 설정한 허니팟(honetpots)에서 데이터를 제공받음

▶ 약 2만 명의 말레이시아 환자에 대한 의료 기록을 지금까지 세계 최대 규모의 데이터 결함 중 하나로 전 세계 온라인상에서 무료로 이용할 수 있다고 하여 보건부에서 위반을 조사 중[133]

- 독일에 기반을 둔 사이버 보안 회사인 Greenbone Networks는 52개국에서 이 문제를 확인하여 2019년 발표하였는데, 엑스레이, CT 및 MRI 스캔 이미지와 함께 환자의 이름, 생일, 검사일 등과 같은 환자 개인 데이터를 온라인에서 사용할 수 있었음
- 말레이시아의 경우 19,922개의 환자 데이터 레코드가 3개의 아카이브 시스템으로부터 공개적으로 접속이 가능했으며, 이 레코드와 관련된 120만 개의 이미지가 있었음

▶ 경찰에 따르면, 2019년 상반기 7개월 동안 8,808건의 사이버 범죄 사례로 인해 3억 3,100만 RM에 달하는 손실을 기록함[134]

- 이 사이버 범죄에는 러브 스캠, e-Trade(온라인 구매), 통신 사기 등이 포함됨

▶ MyCERT의 자료에 따르면 2018년 말레이시아 전역에서 기업 및 개인에 대해 10,699건의 사이버 보안 공격을 기록했으며, 이는 2017년 대비 34% 증가하였음[135]

- 2018년 사기(5,123건), 침입시도(1,805건), 악성코드(1,700건), 침입(1,160건), 사이버 괴롭힘(356건), 스팸(342건), 콘텐츠 관련(111건), 취약점(92건), 서비스 거부(10건)이 포함됨
- 특히 사기 사건은 2017년 대비 34% 증가하였고, 침입시도는 578% 증가, 악성 코드는 109% 증가하였음

133 channelnewsasia, Almost 20,000 medical records of Malaysian patients found to be freely available online, 2019.9.18.
134 thesundaily, CSM-ACE the right platform to address cyber security issues: Gobind, 2019.9.23.
135 www.mycert.org.my

그림 _ 말레이시아 유형별 사이버 사고



[출처] www.mycert.org.my (2017, 2018 자료 재구성)

- 봇넷 드론과 멀웨어 감염 사고는 2018년에 321만 건 이상이 기록되었으며, 이는 MyCERT에 기록된 사례일뿐 아니라 당국에도 보고된 공격으로 보고되지 않은 숫자는 더 클 수 있음
- 사이버 범죄로 인한 손실은 2018년 7,200만 달러(약 3억 RM)이상임[136]

▶ 2017 Unisys Security Index에 따르면 말레이시아 국민들의 88%는 은행, 카드 사용에 대해 걱정하고 있으며, 87%는 무단으로 개인 정보에 접근하거나 이를 오용하는 것에 대해서도 우려하고 있음

- 조사 대상 국민의 77%는 바이러스나 원치 않는 전자메일 또는 해킹과 관련하여 컴퓨터와 인터넷 보안에 대해 우려하고 있는 것으로 나타남

▶ Limelight Networks의 사이버 보안 보고서에 따르면, 말레이시아 소비자 중 오직 18.72%만이 기업이 사이버 범죄 보호에 대한 충분한 조치를 취하고 있다고'매우 확신'하는 것으로 나타남

- 사이버 범죄의 증가에도 불구하고 소비자의 온라인 활동은 지속되고 있으며, 말레이시아 소비자의 92.36%가 전자상거래 및 기타 활동 전에 사이트 보안을 확인하는 것으로 나타남
- 웹사이트의 해킹 전적이 브랜드의 명성과 신뢰성에 직접적인 영향을 주는 것으로 밝혀짐. 사이버 공격을 받은 웹사이트에 대해 말레이시아 소비자들의 70% 이상이 브랜드에 대한 의견이 전과 변화됨
- 말레이시아에서는 거래를 할 때, 스마트폰이 선택의 대상이며, 2위는 노트북으로 나타남

▶ 사이버보안 위협이 말레이시아 기업에 122억 달러의 비용을 발생시킬 수 있다고 나타남

- 보안 사고로 인한 아시아 태평양 지역의 잠재적 경제적 손실은 2017년, 1조 7천 4백억 달러로 전체

136 Digital News Asia, FUTURE OF CYBERSECURITY CONFERENCE TO ADDRESS INDUSTRY CHALLENGES, 2019.6.12.

GDP의 7%에 해당하는 수치임

- 말레이시아의 경우, 122억 달러는 엄청난 금액으로, 말레이시아 총 GDP의 4%를 차지하는 수치임

▶ 마이크로소프트가 발표한 보고서 Global Security Intelligence Report(SIR) 22호에 따르면, 말레이시아는 멀웨어 발생이 증가하고 있는 나라 중 하나라고 밝힘

- 2017년 1분기, 말레이시아 마이크로소프트의 실시간 보안 제품이 실행되는 컴퓨터의 평균 12.9%에서 멀웨어 발생이 보고되었는데, 이는 전 세계 평균인 9%보다 높은 수치임

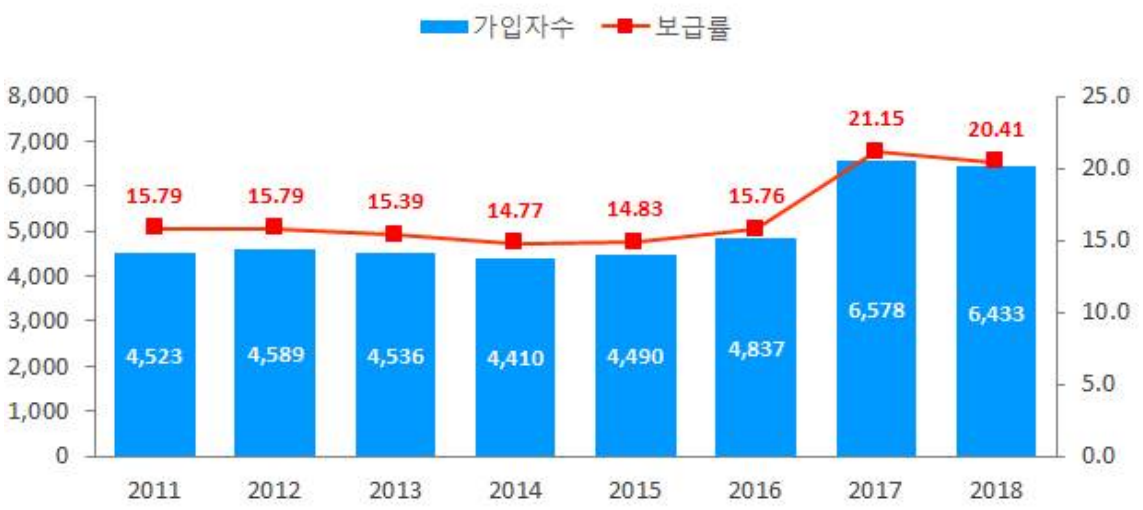
2) 인터넷 및 통신 환경

▶ 유선통신

- ITU에 의하면 2018년 말 기준, 유선통신 가입회선 수는 약 64만 회선을 기록, 보급률은 20.41%이며, 2017년 보급률 21.15% 대비 0.74% 감소하였으며, 이는 모바일 부문이 시장을 확장함에 따라 유선 보급률은 감소함
- 말레이시아에서 대표적인 유선 사업자인 Telekom Malaysia는 유선 시장에서 98% 시장점유율을 차지함

그림 _ 말레이시아 유선통신 가입자 수 및 보급률 추이

(단위: 천 명, %)



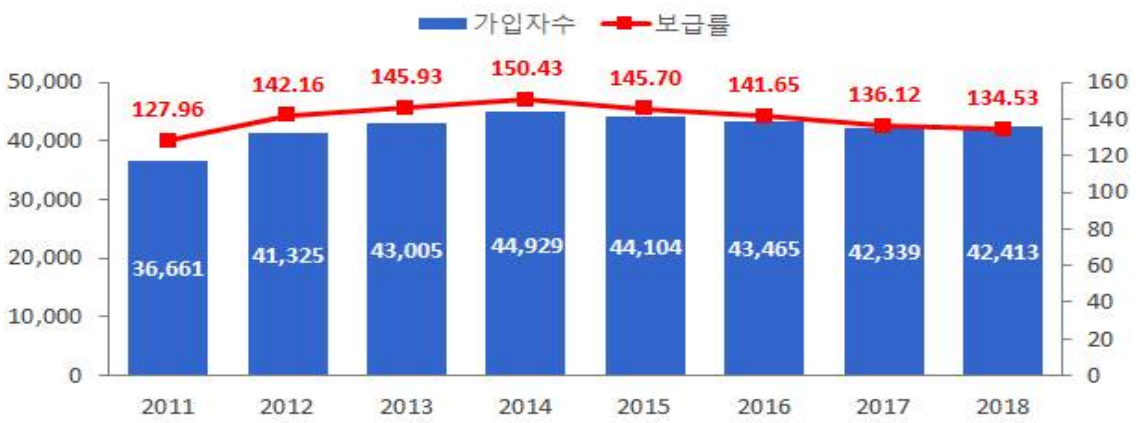
[출처] ITU Statistics DB (2019.6)

▶ 이동통신

- ITU의 자료에 의하면 2018년 기준 이동통신 가입자 수는 2017년 대비 약 0.17% 증가한 약 4,241만 명으로 보급률은 134.53%였으며, 2014년 150.43%로 최고의 보급률을 기록
- 2014년 이후 보급률이 다소 감소하는 추세를 보이는데, 이는 말레이시아의 이동통신 시장은 다른 아시아 시장에 비해 상대적으로 발전했지만 시장이 포화 상태에 달했기 때문으로 풀이
- 1993년에 설립된 Maxis는 2013년 말레이시아에서 최초의 4G LTE 네트워크를 시작하였으며, 2017년 초 4G LTE기반 네트워크의 인구 커버리지는 88%에 달함
- DiGi는 2013년에 브로드밴드 및 태블릿 요금제에 대한 LTE 서비스를 시작하였으며, 2014년 3월 스마트폰을 위한 LTE 서비스를 시작하였고, 2017년 2월 DiGi의 LTE 네트워크의 인구 커버리지는 85%에 달함
- U Mobile은 2007년 3G 서비스로 말레이시아에 진입하였으며, 2015년 8월 ZTE는 5G 모바일 브로드밴드 기술 개발에 중점을 둔 U Mobile과 연구 개발 파트너십을 체결하였고, U Mobile은 2015년 5월 LTE 출시를 위해 Telekom Malaysia의 광섬유 백홀을 제공받는 계약을 체결함
- BuddeComm 보고서에 의하면, 2022-2023년까지 5G가 말레이시아에서 널리 사용될 것으로 예상하며, Ericsson은 2016년부터 Universiti Teknologi Malaysia 및 2017년부터 Celcom Axiata Bhd와 협력하여 5G 구현에 대한 기초 연구를 수행했음
- 2017년 5월 Celcom Axiata는 말레이시아 최초의 5G 시험을 수행했으며, 이는 2월에 서명한 Ericsson과의 5G 양해각서의 일부에 해당함
- Alatel-Lucent가 이끄는 5G NOW 프로젝트는 2015년 9월에 완료되었으며, 이 공동 프로젝트는 차세대 모바일 네트워크의 유연성 및 장치 지원 요구사항에 중점을 둠

그림 _ 말레이시아 이동통신 가입 및 보급률 추이

(단위: 천 명, %)

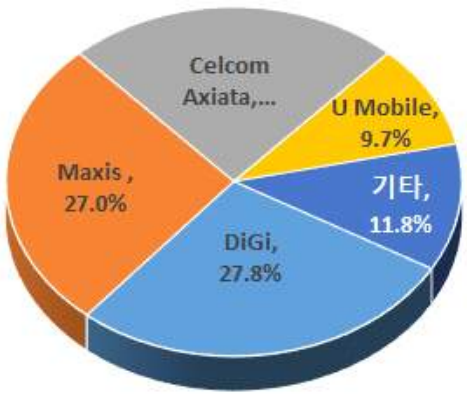


[출처] ITU Statistics DB (2018.6)

- 말레이시아에는 주요한 3개의 이동통신 사업자인 Maxis, Celcom Axiata, DiGi가 있으며, 이외에도 U Mobile 등과 함께 다양한 군소 사업자가 경쟁하고 있음
- 2018년, 이동통신 시장은 주요 3개 업체인 DiGi(27.8%), Maxis(27.0%), Celcom Axiata(23.7%)가 전체 이동통신 시장의 78.5%를 차지하고 있으며, U Mobile은 9.7%, 기타 여러 업체들의 점유율 합이 11.8%에 해당함

그림 _ 말레이시아 이동통신사별 시장 점유율(2018년 기준)

통신사	가입자 수 (백만명)	비율
DiGi*	11.6	27.8%
Maxis	10.9	27.0%
Celcom Axiata	9.6	23.7%
U Mobile*	3.8	9.7%
기타*	6.9	11.8%
전체	**42.8**	**100%**



* DiGi, U Mobile, 기타의 값은 추청치
[출처] BuddeComm (2019.8)

▶ 말레이시아의 전자상거래(B2C) 시장은 상당한 규모의 인구(3,100만 명)와 비교적 높은 소득 수준(2018년 1인당 GDP 27,736달러), 높은 인터넷 보급률(전체 가구의 79%) 및 잘 발달한 물류 인프라를 바탕으로 성장 가능성이 높음

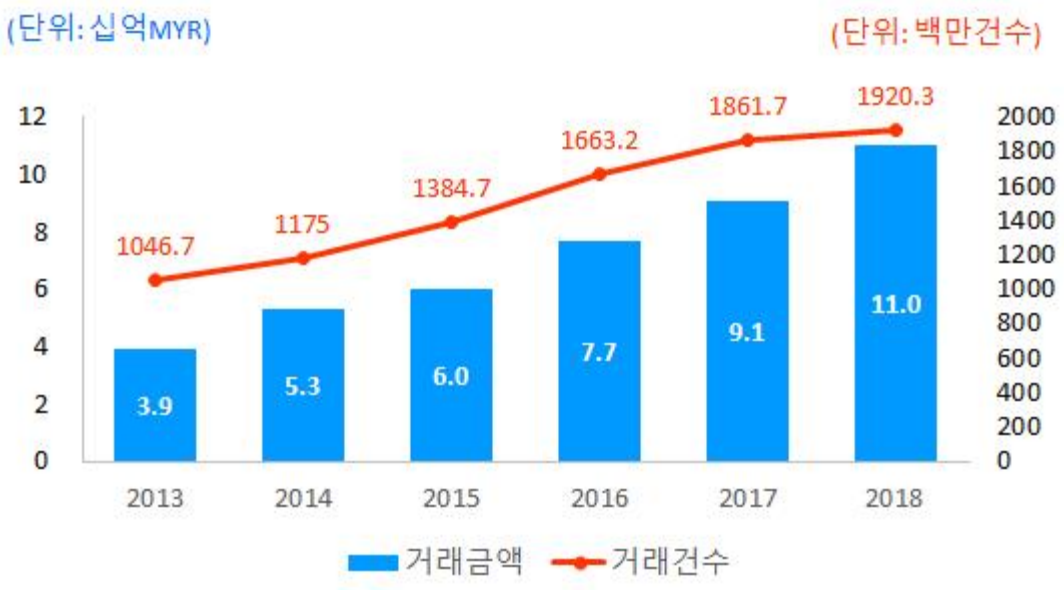
- 2018년 기준 말레이시아는 1억 5,300만 명의 온라인 쇼핑객 (인구의 50%)과 모바일 기기 사용자의 62%가 온라인 쇼핑을 하고 있음
- 말레이시아 정부는 2020년까지 전자상거래 부문이 GDP에 대한 기여도를 두 배로 끌어 올리겠다는 목적에서 6개 분야 11개 추진 프로그램으로 구성된 국가전자상거래 전략 로드맵(2016 National eCommerce Strategy Roadmap)을 발표하였음
- 전자상거래 활성화를 통해 2015년-2020년간의 전자상거래 분야 성장률을 매년 두 자리 숫자로 유지하여 국가 GDP 성장에 기여하겠다는 목적임
- IT시장 조사기관 eMarketer에 의하면 말레이시아는 서비스를 포함하여 소매 전자상거래 판매액 분야에 있어 동남아에서 5번째를 기록

▶ 전자상거래 및 결제시장 전문 조사기관 yStats에 의하면[137] 말레이시아의 비즈니스에서 지난 1년간

온라인 사기 손실이 증가하였다는 답변이 57%에 해당하며, 손실이 다소 줄었다는 답변은 24%, 손실이 같은 양이라는 답변은 19%로 나타남

- 2018년 실시된 설문조사에 따르면, 인터넷 사용자의 24%가 보안 및 개인정보보호 문제로 온라인 쇼핑을 하지 않고, 응답자의 50%는 보안문제와 사기에 대한 두려움으로 전자지갑(E-Wallet)을 사용하지 않는 것으로 나타남
- 2019년 2월 기준 삼성 페이가 사용 가능하며, 또한 2018년 8월에 위챗 페이(WeChat Pay)는 말레이시아에 등록된 위챗 사용자가 위챗의 지갑 서비스를 사용할 수 있도록 시작하였으며, 결제 거래의 37%는 2022년까지 현금 없이 될 것으로 예상됨
- 2018년 비현금(non-cash) 결제 방법을 사용하는 소비자의 8%가 모바일 지갑으로 지불했으며, e-Money 거래는 20%이상 증가하여 23억 유로까지 증가하였으며, 사용된 모바일 결제 서비스는 GrabPay(27%), Touch 'n Go eWallet(19%), Boost(19%), Maybank QRPay(16%), WeChat Pay(7%)순서로 나타남
- 말레이시아의 e-Money 거래 건수는 2018년 기준 19억 건에 달하며, 2013년 대비 거의 두 배로 증가하였으며, 2018년 기준 거래 금액은 110억 MYR에 달함

그림 _ 말레이시아 e-Money 거래금액 및 거래건수 추이



[출처] yStats(2019.7)

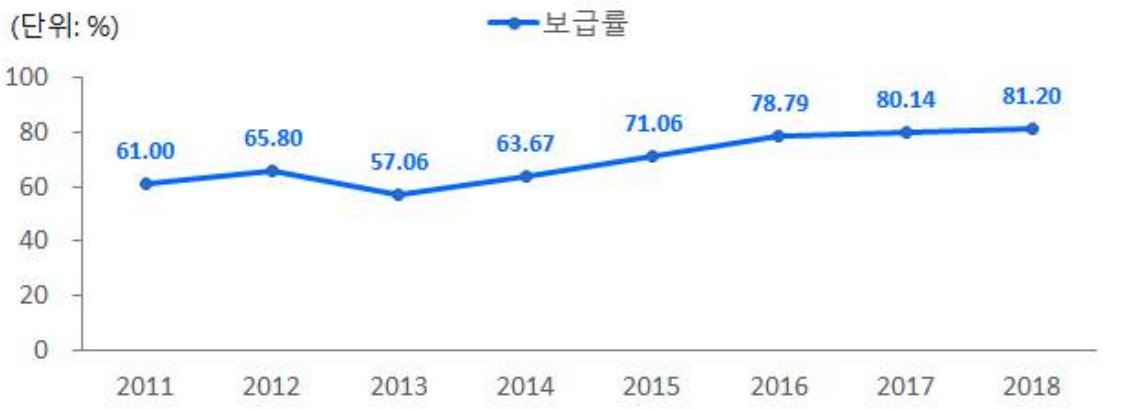
137 "Global E-Commerce Intelligence, Fraud and Security in Global Online Payments 2019", yStats, 2019.7.

- 2017년 설문조사에 따르면, 말레이시아 온라인 쇼핑객의 주요 관심사는 높은 배송비와 긴 배송시간임
- 인터넷에 접속하는 주요 장치인 스마트폰의 인기는 말레이시아에서 모바일 상거래의 성장을 견인하고 있으며, 2018년 3월 말레이시아 전체 웹 트래픽의 절반 이상(54.5%)이 휴대전화이며, 태블릿은 3%를 차지함
- 설문조사에 따르면 2017년 8월 기준 온라인 쇼핑객의 51%가 스마트폰을 사용하여 가장 최근 전자 상거래 주문을 한 것으로 조사되었으며, 2017년 6월 기준 인터넷에 접속하는 주요 기기는 모바일폰이 97%에 해당되며, PC가 51%에 해당됨
- 2017년 6월 기준 전자 상거래 웹사이트 트래픽의 모바일 점유율이 74%에 해당함

▶ 인터넷 이용 환경

- ITU의 자료에 따르면 말레이시아의 인터넷 이용자 보급률은 2018년 81.2%로 전년의 80.14%에서 1.06% 증가하였으며, 2013년 이후 꾸준히 증가 추세를 보임

그림 _ 말레이시아의 인터넷 보급률



[출처] ITU Statistics DB(2019.6)

- 말레이시아는 4G 모바일 가입자의 증가와 높은 데이터 용량으로 인해 지난 5~6년간 모바일 광대역 보급률이 급격히 증가하였음
- BuddeComm의 자료에 의하면 전체 인구에 대한 모바일 브로드밴드 보급률은 2017년 98%이며, 2018년 103%로 추정한[138] 반면, 전체 인구에 대한 유선 브로드밴드 보급률은 2017년 8.5%이며, 2018년 8.5%로 추정함[139]

138 BuddeComm, Malaysia - Mobile Infrastructure, Broadband, Operators - Statistics and Analyses , 2019.8.8
139 BuddeComm, Malaysia – Fixed Broadband Market – Statistics and Analayses, 2019.8.24

표 _ 말레이시아의 브로드밴드 보급률(2017년 기준)

구분	이용자 수	보급률
모바일 브로드밴드	31,000,000	98%
유선 브로드밴드	2,688,000	8.5%
전체	**33,688,000**	-

[출처] BuddeComm(2019.8.)

- 말레이시아의 유선 브로드밴드 시장은 여전히 저개발 상태이며, Telekom Malaysia은 FTTH, ETTH, VDSL2 기술을 사용하여 라스트 마일 접속 네트워크를 출시하였음
- 말레이시아 정부는 2017년 발표된 NFP(Nationwide Fiberisation Plan)에 따라 국가의 유선 브로드밴드 인프라를 확장하여 소비자의 이용 속도를 높이고자 하며, 이 프로그램은 2019년까지 운영되며, 농촌 지역의 2백만 개를 포함한 총 6백만 개의 부지에 연결되는 광섬유 인프라에 해당함
- Telekom Malaysia와 Tenaga National Berhad(TNB)는 정부의 NFP를 이행하기 위한 이행계획을 공동 개발하기 위해 2018년 1월 양해각서(MoU)에 서명함
- Telekom Malaysia는 2018년 말까지 Wi-Fi 핫스팟 수를 1만개에서 10만개로 대폭 늘리는 전략을 발표
- Telekom Malaysia는 2014년 8월 4G 브로드밴드 서비스를 Kedah주의 Alor Setar시에서 시작했으며, 2014년 말 4G WiMAX 서비스에 대해 65%의 인구 커버리지를 달성함

▶ 네트워크 기술업체 Akamai의 State of the Internet 2017 보고서에 따르면 말레이시아의 인터넷 평균 속도는 2017년 1분기에 8.9Mbps로 아시아 태평양 지역에서 10위를 차지, 이는 전 분기에 비해 9.1% 증가한 것이며 작년 1분기에 비해 40% 성장한 것임

- 한국의 인터넷 속도가 28.6Mbps로 1위를 차지했으며, 홍콩 21.9Mbps, 싱가포르 20.3Mbps, 일본 20.2Mbps, 대만 16.9Mbps 등이 그 뒤를 따름

▶ 영국계 통신분야 시장조사 업체 Kable의 분석에 의하면 말레이시아 정보통신 부문 시장은 매년 가파르게 성장하여 2019년경에는 약 7억 4,137억 달러에 이를 것으로 전망

그림 _ 말레이시아 정보통신 부문 시장 성장률

(단위: 백만 달러)



[출처] Kable(2016.8)

- 이를 부문별로 나누어 보면 기업통신서비스 부문이 가장 큰 비중을 차지하지만, 성장률의 경우는 클라우드 서비스 부분이 가장 높은 성장세를 보일 것으로 전망
- 기업통신서비스 부분은 연평균 성장률(CAGR)이 8.21%, 클라우드 서비스 부문은 47.2%에 이를 것으로 나타남

표 _ 말레이시아 정보통신 분야별 시장 성장 전망

Segment	2016	2017	2018	2019	CAGR 2016-19
Enterprise Communications Services	162.72	178.07	193.65	206.18	8.21%
IT Hardware	160.69	170.74	180.20	188.83	5.52%
IT Services	129.36	136.12	143.83	153.55	5.88%
Software	43.68	47.24	50.82	54.38	7.58%
Cloud Services	37.79	56.98	83.77	120.31	47.12%
BPO Services	13.46	15.03	16.60	18.12	10.43%
Total	547.69	604.19	668.86	741.37	10.62%

Source: Kable ©Kable

[출처] Kable(2016.8)

정보보호 시장 현황

1) 시장 규모

시장 개요

▶ 사이버 보안은 점증하는 사이버 위협과 광범위한 공격 형태로 인해 말레이시아 대부분의 기관에서 IT와 함께 핵심적인 비즈니스가 되어 가고 있으나 대부분의 기관에서는 아직 이에 대비한 사이버 보안 준비가 부족한 상황

- 대부분의 기업은 사이버 보안의 중요성을 인식하고 전문적인 서비스를 아웃소싱하는 것에 큰 관심을 보이고 있음
- IDC의 '2017 Annual Business and IT Services Survey'에 따르면 설문 조사 대상 말레이시아 기업의 65%는 보안관리 서비스 제공에 대해 큰 관심을 보이고 있으며, 협업을 원하고 있음
- 강력하고도 최신 기술에 대응하는 규제의 부족, 자국 내 보안 전문 서비스 기관의 능력 부족, 수준 높은 보안 전문가의 부족 등은 말레이시아가 당면한 사이버 보안 관련 도전 과제임

▶ 글로벌 사이버 보안 시장 참여자들의 경쟁상황

- 글로벌 IT 보안 서비스 공급자들은 말레이시아 국내 사업자들과 긴밀히 협력하여 시장에 참여 하고 있음
- 또한 가격 경쟁을 피하기 위해 국내 유통채널의 통합을 추진
- 세계적인 SI업체와 컨설팅 업체들은 데이터센터나 클라우드 서비스와 같은 솔루션을 제공하고 있음
- 보안관리 서비스 업체들은 서비스 영역을 확대해 가면서 사고대처, 포렌식, 위기정보 제공, 빅 데이터 분석 등의 분야에 투자를 진행하고 있음

시장 규모 및 전망

▶ Statista의 자료에 의하면[140], 말레이시아 스마트홈 보안 부문에서의 수익은 2019년 1,600만 달러에 이르며, 매출은 2019년~2023년 기간 동안 연평균성장률이 25.5%로 2023년에 4천만 달러에 이를 것으로 예상함

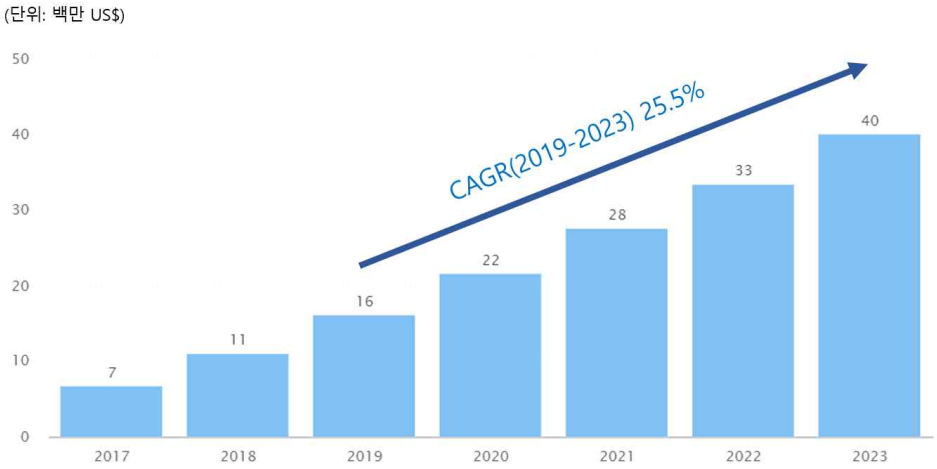
- 여기서 스마트홈 부문 보안에는 건물 및 부지의 네트워크 접속 제어 및 관리를 위한 장치 및 서비스

140 statista, Smart Home Report 2019 – Security, 2019.4.

판매가 포함되며, 감시제품(예: 보안카메라 및 관련 데이터 저장 및 전송 서비스, 모션 센서, 프로그램 가능 및 원격 제어 도어 잠금 장치) 및 위험 모니터링 장비(연기 감지기 및 습도 센서 연결)가 포함됨

- 이러한 보안부문 2019년 가계 보급률은 1.3%이며, 2023년에는 4.1%에 이를 것으로 예상하며, 보안부문의 스마트홈 당 평균 수익은 186.47 달러임

그림 _ 말레이시아 보안 부문 수익 성장 전망



[출처] statista(2019.4)

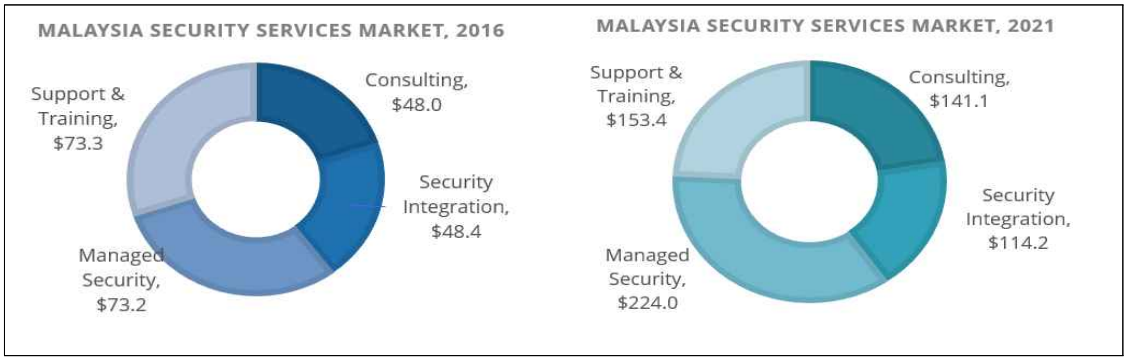
▶ 통신멀티미디어부에 따르면 말레이시아는 2025년까지 지역 사이버 보안 서비스 시장 점유율의 75%를 기여하는 3대 아세안 국가 중 하나임[141]

- 최근 Frost & Sullivan 디지털 인재 연구를 인용하면서, 통신멀티미디어부 장관은 말레이시아에서 사이버 보안 인재에 대한 수요가 2020년까지 10,500명에 달할 것으로 봄

▶ IDC 조사에 따르면 말레이시아 사이버보안 서비스 시장은 2016년 2억 4,290만 달러 규모에서 향후 5년간 연평균 21.1%로 증가해 2021년 6억 3,260만 달러 규모에 달할 것으로 보임

141 Bernama, ICT industry sees bright prospects in 2018-2019, 2018.12.24.

그림 _ 말레이시아 사이버 보안 시장 규모 예측



[출처] IDC(2017.8)

- 부문별로는 보안관리 서비스(Managed Security Service) 부문이 2016년 7,320만 달러 규모에서 2021년에는 2억 2,390만 달러로 증가하여 연평균 증가율 25.1%를 기록하며 두드러진 성장세를 보일 것으로 전망
- 말레이시아의 보안 소프트웨어 시장은 여러 조직들이 IT 보안 인프라 개선을 위해 자금을 할당하면서 앞으로 수년 간 계속 성장할 것이라고 IDC 말레이시아의 SW 시장 분석가 Linda Chuna가 밝힘
- IDC 설문 조사에 따르면 말레이시아의 조직 중 24%가 클라우드, 이동성, 사물인터넷 등과 같은 디지털 기술로 인한 변화에 대응하여 사이버 보안 솔루션을 채택하거나 변형할 계획이라고 나타남

그림 _ 부문별 말레이시아 사이버 보안 시장 성장 전망



[출처] IDC(2017.8)

▶ A.T. Kearney analysis에 따르면, 2025년까지 ASEAN 사이버 보안 시장 규모는 두 자리 숫자의 성장률을 보일 것으로 예상되며, 그 중 말레이시아는 연평균 성장률 15%를 보일 것으로 예상

▶ Gartner는, 말레이시아에서 정보기술(IT) 제품 및 서비스에서 소비는 2019년 652억 RM에 달하여 2018년 대비 4.6% 증가할 것으로 예상함[142]

▶ 말레이시아 ICT 협회(National ICT Association of Malaysia, Pikom)에 따르면, 2010년에서 2017년 기간동안 연평균성장률(average annual growth rate, AAGR)이 7.8%에 해당하며, ICT산업의 국내 총생산 기여 가치는 2018년 1,920억 RM에 달하는 것으로 추정됨[143]
- 전자상거래는 2010년부터 2018년까지 12.5%의 연평균성장률(CAGR)에 기반하여 2018년 965억 RM을 기록하는 공격적인 성장세를 계속할 것으로 추정함

2) 주요 사업자 현황

정보보안 시장 유통 구조

▶ 글로벌 벤더들의 시장 장악력이 높은 말레이시아 시장에서는 현지 법인 설립을 통한 직접 판매와 현지 플레이어들에 의한 글로벌 벤더 솔루션의 간접 판매 방식 유통 구조가 지배적
- Kaspersky Lab, Avira 등 글로벌 규모의 기업들은 현지 법인을 설립해 직접 제품 및 솔루션을 판매하기도 하지만, 다양한 유통 채널 확보를 위해 복수의 에이전트를 두고 간접적인 유통망 활용에도 적극적
- 간접 판매는 도매업자/배급업자(1차), 리셀러(2차) 등의 유통 경로로 구성

▶ 현지 플레이어들은 글로벌 벤더들로의 기술 의존도가 높아, 에이전트나 유통업체 및 리셀러 역할에 편중돼 있음
- 현지 플레이어들의 경쟁력은 기술력보다는 말레이시아 내 유통망 확보 역량이 중요하게 평가됨

정보보안 시장 주요 사업자

1) 글로벌 보안 SW 벤더

142 NST Business, Malaysia IT spending to reach RM65b in 2019, 2018.11.13
143 Bernama, ICT industry sees bright prospects in 2018-2019, 2018.12.24.

▶ 말레이시아는 Kaspersky Lab, Symantec, Websense, Clearswift, Trend Micro, Panda Security 등 다양한 글로벌 업체들이 진출해 있는 시장으로, 현지 기업의 활동은 대부분 에이전트나 유통업체 역할에 그침

- 전통적으로 동남아 지역에서는 싱가포르가 IT시장의 중심지 역할을 수행해 왔으나 Kaspersky Lab을 필두로 최근 Panda Security 등 글로벌 기업들이 시장 거점 다변화 전략을 구사하면서 싱가포르와 함께 말레이시아가 동남아 시장의 새로운 중심지로 부상 중
- 유력 글로벌 기업 이외에도 후발 벤더인 Websense, Clearswift, ConSentry Networks 등의 업체들도 현지 지사를 보유하고 있거나 유통망을 보유하고 있음
- 국내 기업으로는 하우리, 어울림정보기술, 웨어밸리 등의 국내 업체들도 통신사, 대학교를 중심으로 제품을 공급하며 브랜드 인지도 상승을 위해 노력을 기울이고 있음

▶ Kaspersky Lab

- 안티바이러스 부문에서 말레이시아 내 70%에 달하는 점유율로 시장 독주 중
- Kaspersky는 또한 네트워크 보안 업체인 Tech Titan Ltd와 파트너십을 체결, T-Drive Pro는 세계 최초의 휴대형 USB 안티바이러스 솔루션인 Tech Titan T-Drive Pro with USB KAV를 출시 중으로 8GB 용량의 T-Drive Pro는 55달러 선에 판매되고 있음
- Kaspersky는 2010~2012년 사이 65~70%의 매출이 중소 비즈니스 고객으로부터 발생

▶ Websense

- 미국 소재 통합 웹 보안 및 데이터 보호 전문 업체인 Websense는 동남아 지역을 중심으로 최근 마케팅 공략 강화 중
- Websense는 통합 웹보안, 이메일 보안, 모바일 보안 및 데이터손실방지(DLP) 기술력을 기반으로 글로벌 시장을 확대하고 있는 기업
- 앱 기반 소프트웨어나 SaaS 기반 클라우드 서비스 제공을 위한 유통 네트워크를 구축 중인 Websense는 급증하는 다양한 보안 위협과 멀웨어, 기밀정보 손실 방지 및 인터넷 정보보호 정책 기술 개발력을 강화하며, 시장 영향력을 확대 중

▶ Avira

- 워크스테이션 및 모바일 보안 프로그램으로 말레이시아 현지법인(Avira Sdn Bhd) 이외에도 다양한 유통법인들과의 제휴 전략을 통해 말레이시아 내 정보보안 시장 장악력을 강화 중
- Avira는 임직원 500명에 전 세계적으로 1억 명의 이용자를 보유하고 있는 독일계 글로벌 보안 기업
- 개인 워크스테이션용 솔루션을 비롯, 다양한 계층의 네트워크 이종 시스템 보호를 위한 워크스테이션, 파일, 메일 및 웹서버용 솔루션과 PDA, 스마트폰 및 임베디드 기기용 보안 프로그램 제공

- 2013년 6월 이후, 리눅스 기반 OS용 안티바이러스 제품 개발을 중단하고, Mac OS X와 Windows 라인용 제품 개발에 보다 주력 중

▶ Cyberoam

- ID 기반 UTM 솔루션과 안티스팸 분야의 선도적 기업으로 통신 솔루션 기업인 Elitecore Technologies를 주요 고객으로 두고 있음
- Cyberoam Anti Spam Engine은 메일의 스팸 여부 판단을 위해 메일 헤더를 사용하여 로컬 캐쉬와 Spam Detection Center 간의 통신과 이메일 메시지 수신을 수행
- 동사의 Spam Detection Center에서는 독자적으로 개발한 RPD(Recurrent Pattern Detection) 기술을 통해 스팸 탐지, 식별, 분석 및 발생 유형을 분류
- 말레이시아에서는 Secure One을 유통 업체로 선정하여 현지 시장 공략 확대 중

2) 정보보안 서비스 제공 사업자

▶ AIMS

- 데이터센터 운용 기업. 말레이시아에 기반을 둔 외국 통신사업자의 80% 이상과 모든 아시아/태평양의 국내 호스팅 업체에 있어서도 선도 기업
- 보안관리서비스(MSS)를 통해 실시간 보안관리와 긴급대응, 신원 모니터링 등과 같은 업무 수행

▶ AKTI Consulting Group

- 브뤼셀에 본사를 두고 있는 정보보안과 컴퓨터 포렌식에 특화된 정보보안 서비스 제공 기업으로서 2009년부터 전 세계적으로 300여개의 글로벌 클라이언트에 대해 접근관리, 가이드, 보안영역에 관한 회사 내부 방법론 제시
- 보안관리 서비스 프로그램(MSSP)를 통해 기관들이 보안과 사건에 대응하는 정책 디자인에 관한 컨설팅 제공

▶ ASK Pentest

- 보안 전문가들이 설립한 정보보안 컨설팅 기업
- 네트워크와 시스템의 취약성과 보안에 관한 정보를 제공하고 보안 강화에 관한 컨설팅 제공
- 대규모 보안 관련 조사와 대응 방법 및 해킹에 관한 모의실험 실시

▶ Cyber Intelligence

- 말레이시아의 정보보안 서비스 제공에 관한 선도 기업이며, CyberSecurity Malaysia와 국제 이슬람

대학과의 협업을 통해 사이버 보안 관련 정보 수집 및 사이버 전략게임 수행

- 프로젝트의 계획, 평가, 온라인 학습, 현지 워크숍, 보고 등을 포함하는 광범위한 보안 의식 제고와 행태관리 솔루션 제공

▶ DNex

- 보안관리 서비스를 위해 보안운용센터(SOC)를 포함하는 자문서비스를 포함해 최종 소비자에게까지 이르는 전 경로에 대한 보안 서비스 제공
- FORTRESS Managed Service를 통해 보안관리서비스와 기업보안에 대한 끊김없는 패키지 솔루션을 제공하고 24시간 운용하는 SOC 서비스 제공

▶ Firmus

- 2008년부터 보안관련 서비스와 컨설팅을 수행하고 SI 서비스를 제공
- OSSTMM 기반 기술과 시험 시행 표준과 침투 테스팅 체제(Test Execution Standard and Penetration Testing Framework)를 통한 네트워크 침투 테스트를 진행하고 평가하며 소스 코드 관리를 통해 웹사이트나 모바일 앱의 보안 관련 점검 수행

▶ HeiTech

- 시스템과 상품의 전 생애과정을 포함하는 통합 솔루션과 서비스를 제공하는 말레이시아의 선도적 ICT 기업
- 보안관리 서비스 제공, Tier4 데이터센터 소유와 운영
- ISO 27001, ISO 9001-2001, ISO 20000-2011에 관한 기술적 인증서 제공

▶ Kaapagam Technologies

- MSS, SOC, 자문, 심사, 컴플라이언스, 침투테스트, 리스크 관리 등을 통한 광범위한 보호 서비스 제공
- VALARI: 웹 애플리케이션 방화벽과 웹 애플리케이션에 적합하게 디자인된 보안관리 서비스를 제공
- VALAI: 레이어 7 침투 감지 및 방어, 웹 필터링 등에 관한 통합 보안 게이트웨이 솔루션을 제공

▶ LGMS

- 말레이시아뿐만 아니라 미국, 유럽, 아프리카, 대만, 싱가포르, 베트남, 인도네시아 등지에서 전문적인 보안 서비스를 제공하는 업체
- 침투테스트에 특화 서비스. 디지털 포렌식, 컴퓨터 범죄 조사 수행. LGMS는 보안 관련 컨설팅과 인증받은 포렌식 분석을 통해 민간기업과 법률 사무소 등에 전문적인 지원 업무 수행

▶ Mesiniaga

- 1981년에 Bumiputera(말레이시아 원주민)이 참여하는 산업을 증진시키기 위한 말레이시아의 NEP 정책에 부응해서 설립
- 인프라부터 소프트웨어, 서비스에 이르기까지 전 과정에 대한 보안 서비스 제공. 24시간 SOC 서비스 제공

▶ NetbyteSEC

- IT 및 보안 서비스 제공 기업
- 보안 모니터링, 침투 감지, 사건 대응 및 포렌식 서비스. 대규모 사이버 훈련 실시하여 각 시설들의 대응형태와 운영에 있어서의 문제점에 해결방안 제시

▶ Nexagate

- ISMS/ISO 27001에 대한 컨설팅을 제공하는 말레이시아 보안 컨설팅 기업. 보안 대응 태세평가(SPA), 정보유출 보호(DLP) 등의 서비스 제공
- 고객에 특화된 데이터 유출 보호(DLP), 클라우드 기반 웹사이트 보안 솔루션, 웹사이트에 접근 제한 엔진

▶ Quann

- 과거 e-Cop의 이름으로 싱가포르 기반 MSSP와 'CISCO 인증' 지원을 수행했던 기업이며 2016년에 이름을 Quann으로 변경해 활동
- 사이버 훈련과 통제, 데이터 획득에 관한 보안 서비스 제공. 보안 관리 모니터링 서비스인 특허 받은 'Cyclops'라는 이름의 SIEM 플랫폼 소유권자

▶ VADS

- 중소기업, 대기업 정부 기관에 이르기까지 물리서버와 클라우드 기반 MSS 서비스 제공
- 통합 위기관리(MUTM): 단일 플랫폼에 바이러스, 트로이 목마, 스파이웨어나 다른 악성 프로그램에 대한 다차원적 보안을 특색으로 함
- 웹 애플리케이션 관리 방화벽(MWAF): 웹 애플리케이션이나 서버에 대한 보안 서비스를 제공

3) 주요 동향 및 이슈

▶ 말레이시아의 KPMG는 사이버 챌린지 2019를 통해 실제 비즈니스 사례 시나리오에서 테스트(2019년

9월)[144]

- KPMG는 다섯 번째 사이클인 사이버 챌린지 2019(Cyber Challenge 2019)를 통해 전국의 대학생 팀이 기술적 스킬, 대인관계 기술 및 분석적 사고 역량 모두를 테스트하며 2019년 9월 마무리함
- 이 경쟁은 21개 대학교에서 300명 이상의 대학생이 참여한 사이버 보안 챌린지와 사이버 기술 챌린지의 두 가지 과제로 구성됨
- 사이버 보안 챌린지에서 학부생들은 역 공학(reverse engineering), 스테가노그래피(Steganography), 암호기법(cryptography), 프로그래밍, 네트워크 분석, 인프라 해킹, 웹 애플리케이션 보안, 디지털 포렌식 기술을 테스트하는 연습에 참여하였으며, 또한 참여자들은 실제 디지털 사기(fraud) 시나리오에 배치될 때 비즈니스를 생각하는 것으로 함
- 사이버 기술 챌린지는 블록체인, 위협 인텔리전스, 운영 기술에 중점을 둔 세 가지 과제를 거침
- KPMG의 사이버 챌린지는 대학생들이 실제 비즈니스 문제에 노출될 수 있고, 기업이 요구하는 지식과 기술을 갖추는 플랫폼으로, 말레이시아의 사이버 보안 전문가에 대한 요구에 대해 차세대 기술 지원 인력을 강화하고자 함
- 이번 행사는 전략적 파트너인 Netpoleon과 엔지니어링 기술 연구소(Institution of Engineering and Technology, IET)와 함께 하며, 말레이시아 디지털 경제 공사(MDEC)와 Al-Rajhi Bank가 지원함

▶ 보안회사 Kaspersky는 말레이시아 사이버보안청(CyberSecurity Malaysia)과 협력하여 아시아 태평양 지역에 첫 번째 투명성 센터(Transparency Centre)를 개설함(2019년 8월)[145]

- Kaspersky의 동남아본부가 이미 말레이시아에 위치해 있으며, 취리히, 마드리드에 이어 세 번째로 개설하는 말레이시아 Cyberjaya에 위치하는 투명성 센터는 회사의 파트너와 정부 이해당사자가 Kaspersky의 솔루션의 소스 코드를 와서 확인할 수 있는 신뢰할 수 있는 시설이 될 것임
- 새로운 센터는 고객이 Kaspersky의 엔지니어링 및 데이터 처리 관행에 대해 더 많이 배울 수 있는 브리핑 센터의 역할을 하게 됨
- Kaspersky의 정부 규제 기관 및 기업 고객은 위협분석, 보안 검토, 응용프로그램 보안 테스트 프로세스를 포함한 회사의 솔루션 및 서비스 검토를 요청할 수 있음
- 이와 같은 제 3자 검증을 통해 민간기업과 공공기관이 팀을 구성하여 사이버범죄로부터 사용자를 더 잘 보호할 수 있다는 사실을 입증할 수 있게 됨

▶ 말레이시아의 경우, 대부분의 기업이나 기관들이 사이버 보안보다는 네트워크 확대에 우선순위를 둠

- 말레이시아는 전반적으로 혁신이 낮은 수준이며, 규제 당국자도 시장의 변화를 따라가지 못하고 있음

144 Digital News Asia, KPMG CYBER CHALLENGE 2019 TESTS UNDERGRADS IN REAL BUSINESS CASE SCENARIOS, 2019.9.27.
145 Digital News Asia, KASPERSKY SET TO OPEN FIRST TRANSPARENCY CENTRE IN ASIAPAC IN CYBERJAYA, 2019.8.19.

※ 예를 들어 Negara 은행은 핀테크와 크라우드소싱 관련 사업을 2016년에 승인 받음. 규제 당국은 바이오인식, 빅데이터, 핀테크, IoT와 같은 신기술을 반영하는 정보보호에 관해 새로운 정책이 필요한 상황

- 말레이시아의 개인정보보호법(Personal Data Protection Act 2010)은 유럽의 정보보호 규정(European Data Protection Directive)과 유사하다고는 하나 개인정보보호 관련 데이터 유출에 관한 보고의무 조항이 없어 시급히 개정을 요구됨
- 말레이시아에서는 제3자에 의한 보안관리 서비스 공급자(MSSPs)들과의 보안운용 센터(Security Operation Center)의 중요성이 높아지고 있으며 위험정보 전파나 리스크 평가에 대한 관심의 증가도 이러한 경향을 높이고 있음

▶ 기업의 전반적인 리스크 관리전략의 일환으로 사이버 보험에 대한 중요성이 높아지고 있음

- 이는 기업들의 데이터 유출에 대한 책임, 이에 따른 비즈니스 중단, 벌금과 조사, 재난관리, 신뢰성, 프라이버시 침해 등에 대비하기 위한 전략으로 풀이됨
- 글로벌 사이버 보험 관련 회사들이 말레이시아의 국내 기업들과 협력하여 맞춤형 보험 서비스와 함께 해당 기업의 사이버 복원력을 평가하여 이에 적합한 보험을 개발하는 형식의 사이버 보험 사업을 전개
- AIG 보험은 2016년 9월 Dimension Data와 협력을 통해 클라이언트에게 종합적인 맞춤형 사이버 보안 솔루션을 제공하기로 했으며 또한 Dimension Data의 사이버 보안 능력과 AIG의 보험 경험을 통합한 서비스 제공하기로 함
- Symantec은 사이버 복원성 평가 상품을 출시하여 기업들이 스스로 자신들의 사이버 관련 복원력에 대한 평가를 할 수 있도록 서비스 제공하기로 했으며 보안서비스는 미국계 보험사 Chubb와 협력하여 소규모 기업에 대해 사이버 보안 툴을 통합한 보험을 제공

4) 정보보호 스타트업 시장 현황

▶ Asia Cybersecurity Exchange는 말레이시아를 세계 주요 사이버 보안 허브 중 하나로 만들어 인재를 세계적 수준의 플레이어로 성장시켜 전 세계 조직에 새로운 수준의 사이버 보안 전문 지식을 제공하고자 하며,[146] 2019년 4,800만 달러 규모의 사이버보안 엑셀러레이터 프로그램을 계획

- ASIACYBERX 라고도 불리는 Asia Cybersecurity Exchange는, 현지 인재와 기업가의 역량을 강화함으로써 말레이시아의 사이버 보안 생태계를 높이고자 하며 또한, 사이버 보안 생태계의 주요 촉매제 역할을 함

146 ASIA Cybersecurity Exchange 웹사이트: asiacyberx.com

- ASIACYBERX는 스타트업 엑셀러레이터 프로그램, 사이버보안 인재 개발, 교육 및 멘토십, 이벤트 조정, 취업 시장, 사이버보안 스타트업을 위한 공동작업(Co-working) 사무소에 중점을 두며, 정부기관, 기술 파트너, 글로벌 파트너, 지역 파트너, 기업 및 학계의 조직이 포함된 커뮤니티로 구성됨
- 2019년 4월, 현지 인재를 발굴하고 육성하기 위해 2억 RM(4,800만 USD) 규모의 사이버보안 엑셀러레이터 프로그램을 계획을 발표함[147]
- 해당 프로그램은 스타트업의 성장 잠재력이 높은 비즈니스를 개발하고, 광범위한 사이버 보안 인재 풀을 구축하려는 장기 계획의 일부에 해당하며, 말레이시아의 전반적인 디지털 경제 활성화에 도움이 될 것으로 기대함
- 해당 프로그램은 현지 스타트업과 기업가가 그들의 솔루션과 제품을 상용화하는 것에서부터, 비즈니스 모델을 미세 조정하며, 20명 이상의 멘토, 기업가, 산업계 전문가의 기존 네트워크 내에서 자금 및 네트워킹 기회를 확보 할 수 있도록 적극적인 멘토링을 강조함
- 해당 프로그램은 통신멀티미디어부, 국가사이버보안청(NACSA), 통신멀티미디어위원회(MCMC), 디지털경제공사(Malaysia Digital Economy Corporation, MDEC), Bank Negara Malaysia를 포함한 여러 주요 정부기관에 의해 지원되며, 2018년 4월에 시작된 세계 수준의 사이버보안 자원 허브로 말레이시아의 전환을 지원하기 위해 증가하는 사이버보안 생태계를 강화하고자 함
- Asia Cybersecurity Exchange는 LE Global Services Sdn Bhd(LGMS)와 다각화된 투자 대기업인 ACE Group의 파트너십을 통해 형성된 ACE Accelerator Network Sdn Bhd가 단독으로 소유하고 있으며 LGMS는 현재 말레이시아에서 가장 큰 전문 보안 테스트 회사임
- 프로그램은 순수한 사이버 보안 플레이어로 제한하지 않고, IT보안, 빅데이터 분석, 사이버보안 관련 솔루션 스타트업에게 개방됨

정보보호 정책 및 기관 현황

1) 관련 법령 및 정책

관련 법령 및 규제

▶ 개인정보보호법(Personal Data Protection Act 2010)

- 2013년에 발효된 말레이시아 개인정보보호법은 전자상거래 및 비즈니스의 거래 촉진을 위해

147 ASIACYBERX offers RM 200M to local talent, Focus Malaysia, 2019.4.19.

제정되었으며, EU의 원칙과 유사한 데이터 보호 원칙을 기반으로 하고 있음

- 그러나 동 법의 적용 범위에 연방정부 및 주정부와 신용보고 기관이 제외되어 있어서 제한적 적용이라는 지적이 있음
- 각 기관들은 기술적으로 보호 방안을 설립하여 개인 식별 정보를 보호해야 하며, 국제 표준인 ISO/IEC 27001 정보보호관리체계(ISMS)를 따라야 하고, 각 산업이나 부문별로 개인 정보를 취급하는 행동강령(code of conduct)마련하여야 함
- 개인정보보호에 관한 주무 기관은 통신미디어부(Ministry of Communication and Multimedia) 산하 개인정보보호국(Department of Personal Data Protection)이며 개인정보의 상업적 거래 절차에 관한 내용과 개인정보 오용에 관한 사항을 감독함
- 일반 원칙으로는 정보소유자의 동의 없이 정보를 사용하는 것을 금지하고 있으며, 이러한 동의는 명시적인 것이어야 함
- 아울러 정보사용이 직접적으로 합법적인 목적을 위한 것이 아닌 한 정보처리를 금지하고 있음
- 또한 개인정보의 사용에 관해서는 정보소유자에게 사용됨을 알려야 하고, 관련 부분 장관의 승인이 없는 한 정보의 해외 유출은 금지됨
- 개인정보를 이용하는 다음의 11개 분야는 개인정보보호국에 등록하여야 함
  - · 은행업과 금융업
  - · 보안업
  - · 정보통신업
  - · 공익시설사업
  - · 보건업
  - · 접객업 및 관광
  - · 교육
  - · 부동산과 개발업
  - · 직접판매업
  - · 법률/회계/경영컨설팅/앤지니어링/건축/고용중개기관/수송의 서비스업
  - · 소매 및 도매 판매업

▶ 통신과 멀티미디어법(Communications and Multimedia Act 1998)

- 통신과 방송, 컴퓨터 관련 산업이 통합되어가는 현상을 반영하여 규제체계를 확립하기 위해 제정됨
- 이 법을 기반으로 말레이시아 통신미디어 위원회(Malaysian Communications and Multimedia Commission MCMC)가 규제체계를 담당하는 기관으로 등장
- 최근 네트워크 보안 문제를 포함, 윤리적이고 긍정적인 인터넷 사용을 촉진하고 거짓 뉴스의 확산을 억제하는 자율규제를 규정하는 새로운 요소가 반영된 개정안을 발표

▶ 새로 제안된 사이버 보안 관련 단일 법률안

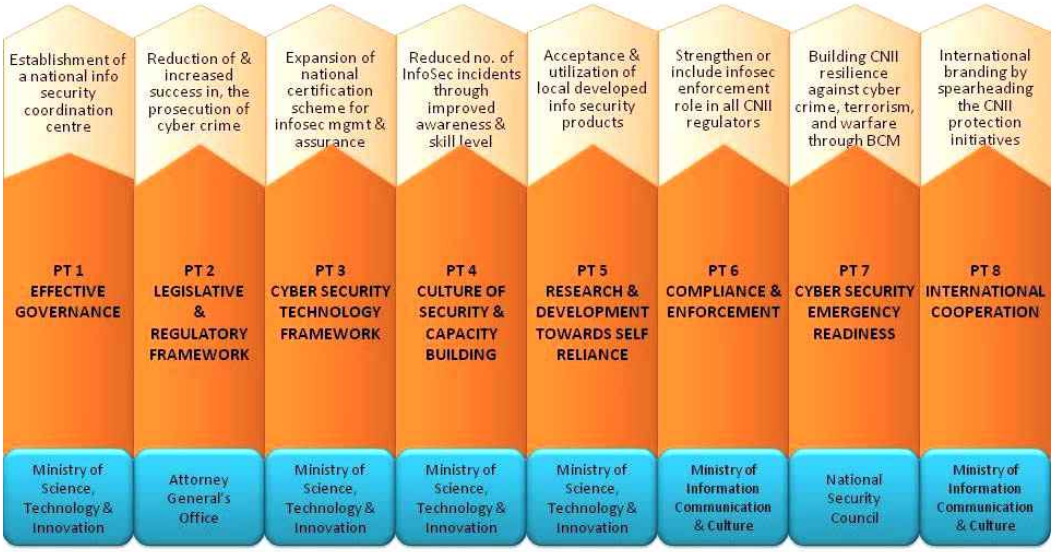
- 말레이시아는 최근 점증하는 사이버 보안뿐만 아니라 미래의 위협에 대처할 수 있는 토대를 마련하고자 새로운 강력한 법률안을 제정할 예정
- Ahmad Zahid Hamid 부총리는 법률안이 공개되지는 않았지만, 극단주의 단체들의 온라인 모금활동을 금지하고 돈세탁과 온라인 도박 등과 관련된 예방조치를 담고 있다고 함
- 그 동안 말레이시아에는 특별히 사이버 보안에만 집중된 법이 별도로 없어서 국가사이버보안청(National Cyber Security Agency, NCSA) 등과 같은 기구들이 기존의 통신· 미디어법(Communication and Multimedia Act 1998), 명예훼손법(Defameation Act 1957), 선동법(Sedation Act 1948) 등과 같은 법률에 기반을 두고 활동했으나, ICT 기술의 진보가 빠르고 점증하는 사이버 공격이 정교해지면서 이를 따라가지 못하고 있음
- 2017년 2월에 설립된 국가사이버보안청(NCSA)은 동 법이 제정되면 국가안전보장위원회(National Security Council, NSC) 산하로 이관되며, 기존의 사이버 보안 사고의 보고를 담당해 왔던 CyberSecurity Malaysia의 권한을 포함하여 말레이시아 국가 전체에 사이버 보안 관련 정책 조정의 단일 기구가 됨

주요 전략 및 정책

▶ 말레이시아 사이버 보안 정책(NCSP, National Cyber Security Policy)

- 말레이시아는 동남아 국가들 중 가장 먼저 사이버 정책을 구상한 국가 중 하나로서 사이버 보안 정책의 중심은 국가의 주요 정보통신 기반시설(CNII)에 대한 위협에 대응하는 차원에 있음
- 동 전략에 의해 말레이시아의 주요 정보통신 기반시설로 규정된 카테고리는 10개 분야로서, 국방과 보안, 교통, 은행과 금융, 보건서비스, 에너지, 정보와 통신, 수자원, 긴급서비스, 정부, 식량과 농업임
- 동 전략에서 추진하려고 하는 과제들은 정부기관-규제기구-민간분야 간 협력의 고양, 정보교환 메커니즘의 증진과 개발, 법률과 규제체계 관련 정보보안을 광범위하게 적용, 정보보안 필수 요소에 대한 의무조항과 강제조항의 최소화, 질 높고 경험 많은 정보보안 전문가와 규제 인력의 능력 배양, 정보보안 교육과 경각심 프로그램의 확대, 정보보안 R&D의 조정 강화, 외국기술에의 의존 점진적인 축소, 비즈니스를 위한 위험관리 체계의 표준화, 정보보안 사건 발생의 보고와 대응 강화 등임
- 말레이시아 정보 보안 정책은 국가 주요 정보통신 기반시설(CNII)의 보안, 복원성, 자기신뢰성을 확보해야 하고, 이를 위해 보안에 관한 문화가 확산되도록 하며, 이를 통해 사회적 웰빙과 부를 창출하여야 함을 비전으로 하고 있음
- 사이버 보안 정책 8가지 정책 추진 방향과 관련 부서를 정리하면 다음과 같음

그림 _ 말레이시아 사이버보안 정책(NCSP)



PT – Policy Thrust

① 효과적인 거버넌스 체계 마련 – 과학기술혁신부
② 법률과 규제체계의 사이버 범죄 – 법무부
③ 사이버 보안 기술 체계와 정보보호 관리 – 과학기술혁신부
④ 보안관련 사회적 토대 마련과 능력배양 – 과학기술혁신부
⑤ 자국 내 사이버 보안 관련 산업 개발과 보호 – 과학기술혁신부
⑥ 핵심정보인프라에 대한 정보보안 강제 및 강화 – 통신미디어부
⑦ 사이버 보안 긴급 대응과 핵심정보인프라의 복원력 회복 – 국가안전보장위원회
⑧ 국제협력 – 에너지녹색기술수자원부

▶ 말레이시아 전자상거래 전략 로드맵(National eCommerce Strategic Roadmap)

- 2016년 10월 말레이시아 총리는 전자상거래 전략 로드맵을 발표하면서 국경 없는 상품 및 서비스 거래 시대에 전자 상거래 활성화를 통해 국가경제발전을 도모하고자 하는 정책을 수립
- 이는 2020년까지 전자상거래 부문이 GDP에 대한 기여도를 20%이상 올리겠다는 목표를 가지고 있음

그림 _ 전자상거래 전략 로드맵을 통한 국민성장에의 기여 목표

	2015 Current	2020f Business as Usual	2020f With Intervention*
E-Commerce (B2C and B2B) Contribution to GDP, in MYR billion	68	114	>170
E-Commerce Sales Growth CAGR, in %	+12.8% (2012-2015)	+10.8% (2015-2020f)	+20.8% (2015-2020f)

- 이 로드맵을 추진할 기구로 여러 기관이 참여하는 국가전자상거래 위원회(National eCommerce Council, NeC)을 설립하였고, 6개의 추진전략과 11개의 프로그램을 수립하였음
- 6개의 추진전략은; 첫째, 전자상거래 판매자 확대, 둘째, 거래에 있어 전자조달 시스템 도입 확대, 셋째, 비관세 장벽 제거, 넷째, 경제적 인센티브 조정, 다섯째, 일부 전자상거래 기관에 대한 전략적 투자, 여섯째, 국경 간 전자상거래에 있어 국내 브랜드 프로모션 등임
- 또한 이 추진체계 안에서 알리바바와 같은 민간 기업들과 협력하여 디지털 자유 통상지역(Digital free trade zone)을 만들 계획이며, 이 통상 지역에는 e물류 허브, 위성서비스 허브, e서비스 플랫폼 건립들을 포함하고 있음

2) 담당기관

▶ 국가사이버보안청(National Cyber Security Agency, NACSA)[148]

- NACSA는 2017년 2월 사이버 보안 문제의 국가 주도 기관으로 공식적으로 설립되었으며, 사이버 공격의 위협에 직면한 말레이시아의 복원력을 강화하고 보장하기 위한 목적으로, 사이버 보안 분야에서 국가 최고 전문가와 자원을 조정하고 통합함
- NACSA는 또한 국가 차원의 사이버 보안 정책 및 전략을 개발하고 구현하며, CII(Critical National Information Infrastructure)를 보호하고, 사이버 위협에 대응하기 위한 전략적 조치를 취하며, 사이버 보안 인식을 주도하고, 축적 및 역량 구축 프로그램을 수립함
- 또한 사이버 범죄 퇴치, 조직의 사이버 위험 관리에 대한 조언, 기관 간 공유 자원 개발 및 최적화,

148 National Cyber Security Agency 홈페이지: www.nacsa.gov.my

사이버 보안에 관심있는 단체간의 건설적인 지역 및 글로벌 네트워크 육성에 대한 전략적 접근 방식을 수립함

▶ 말레이시아 사이버보안청(CyberSecurity Malaysia, CSM)

- CyberSecurity Malaysia은 과학기술혁신부의 외청격인 기구로 설립되어 사이버 보안서비스와 핵심 정보인프라에 대한 사이버 위협에 대응하기 위해 2009년에 설립된 독립 기관임
- 주 업무는 사이버 보안 긴급대응 서비스, 사이버 보안 관리 서비스, 사이버 보안 전략관련 연구조사 업무를 수행함
- MyCert(Malaysia Computer Emergency Response Team): 사이버 사건 관련 조사와 멀웨어 조사를 담당하며, Cyber999 Help Centre를 운영하여 컴퓨터 보안 관련 사항에 대한 긴급대응 서비스 시행
- Digital Foresics(CyberCSI): 컴퓨터 관련 범죄 사건의 디지털 소스에 대한 증거를 제시, 수집, 확인, 식별, 분석, 해석하는 서비스 제공
- MySEF(Malaysian Security Evaluation Facility): 말레이시아의 Common Criteria 평가와 인증을 담당. ICT 제품과 시스템에 대한 보안 평가 업무.
- 정보보안 인증 기구(ISCB): 국제적인 기준과 가이드라인에 대한 인증서비스 제공. 이를 통해 2008년부터 약 179건의 인증서를 사이버 보안 서비스를 제공하는 국내 기업이나 글로벌 기관에 발행하여 왔음
- 최근 Cybersecurity Malaysia는 현지 판매회사에 대해서 종합적인 평가 방법을 포함한 인증 과정을 개발함

▶ 에너지, 과학, 기술, 환경 및 기후변화부(MESTECC)[149]

- 에너지, 과학, 기술, 환경 및 기후변화부(Ministry of Energy, Science, Technology, Environment and Climate Change, MESTECC)는 2018년 제 14차 총선(GE14) 이후, 과학기술혁신부(MOSTI)의 전체 구성요소, 에너지 녹색 기술 및 수자원부(KeTTHA)의 에너지 및 녹색기술부문, 천연 자원 환경부의 환경관리 및 기후 변화 부서가 MESTECC를 형성하기 위해 재구성됨
- 기존의 과학기술혁신부(MOSTI)는 말레이시아의 ICT 보안과 사이버 보안에 관한 정책을 수립하는 기관으로서 특히 말레이시아 사이버 보안 정책의 8개 추진 전략 중에서 4개를 담당하였음
- 기존의 과학기술혁신부(MOSTI)는 ICT 관련 보안 정책 수립과 사이버 보안 관련 기술발전 전략에 관한 정책을 추진하고 있으며, 주요 정보통신 기반시설(CNII) 보안에 관한 사항을 담당함
- 기존 과학기술혁신부(MOSTI) 산하에 말레이시아 사이버보안청(CyberSecurity Malaysia)을 두고 있어, 말레이시아의 사이버 보안 관련 대응과 사건 보고에 대한 사항을 관장함

149 MESTECC 홈페이지: www.mestecc.gov.my

▶ 통신미디어부(Ministry of Communications and Multimedia Malaysia, KKMM)

- 방송과 통신관련 정책을 수립하는 기관으로서 사이버 보안과 관련하여서는 개인정보보호국(Department of Personal Data Protection)을 통해 개인정보 보호에 관한 정책과 집행을 하는 기관임. 법에 따라 11개 개인정보를 취급하는 부분의 영업을 영위하기 위해서는 이곳에 등록을 해야 함
- 아울러 산하의 통신멀티미디어위원회(Malaysian Communications and Multimedia Commission)를 통해 방송통신관련 소비자 보호와 정보 보호 네트워크 평가를 담당하고 있음

▶ 통신멀티미디어위원회(Malaysian Communications and Multimedia Commission, MCMC)

- 방송, 통신, 온라인 서비스의 융합 산업을 규제를 위해 설립('98년)된 통신멀티미디어부(KKMM) 산하기구임
  * 총 9명(위원장1, 정부3, 민간5)의 위원으로 구성
- 방송·통신 사업자 인·허가, 요금 관리 및 불공정행위 규제, 분쟁조정 등 소비자보호 활동 수행
- 통신 주파수 할당, 방송·통신 분야 기술표준 개발, 이용자 대상 교육 및 인식제고 프로그램 운영
- 멀티미디어(인터넷 포함) 콘텐츠의 활성화 및 유해콘텐츠 규제를 담당하며, 방송통신 융합에 따라 점차 영역 확대를 도모
- 사업자 규제와 관련하여 경찰, 국립은행(BNM), 보안위원회(SC), 기업위원회(SSM) 등과 긴밀히 협업 중
- 통신사·ISP 감독 및 규제의 측면에서 인터넷 네트워크 침해사고 관제 및 보안을 담당. 이용자 보호 관점에서 개인정보 및 스팸 문제를 다룸
- 일부 역할·기능에서 과학기술혁신부(MOSTI) 및 CyberSecurity Malaysia와 중첩될 여지가 있으며, 상호 교류·협력은 미미

3) 규제 및 인증제도

▶ MyCC(Malaysian Common Criteria Evaluation & Certification

- ICT 상품을 국제적 기준인 ISO/IEC15408에 따라 평가하고 인증하는 것
- MyCC 체계에는 MySEF(Malaysian Security Evaluation Facility)로 알려진 기관 평가 구조도 함께 포함되어 있음

▶ CSM27001(CyberSecurity Malaysia Information Security Management System Audit and Certification)

- 이 인증은 국제적으로 ISO/IEC27001로 잘 알려진 ISMS에 기반한 기관의 보안관리 시스템에 대해 인증하는 것

▶ Malaysia Trustmark for Private Sector(MTPS)

- e-Business 관련 웹사이트의 보안과 준법여부, 그리고 우수 e-Business 거래를 인증하는 것으로 아시아/태평양의 인증마크 연합(Trustmark Alliance)의 기준에 기반한 인증

4) 최근 정책 동향 및 이슈

▶ 말레이시아 사이버보안청(CyberSecurity Malaysia)은 새로운 멀웨어 탐지 시스템 출시(2019.9)[150]

- 국가 사이버 보안 기관인 말레이시아 사이버보안청(CyberSecurity Malaysia)은 새로운 멀웨어 탐지 및 알람 시스템인 CMERP(Malware Eradication and Remediation Platform)을 발표하며, 조직, 특히 중요한 국가 정보 인프라부문에 대한 멀웨어 위협의 영향을 크게 줄일 수 있을 것으로 예상함
- CMERP은 민관 협력을 통해 현지 전문지식을 사용하여 개발되었으며, 스마트 보안 기능을 통합하여 사이버 위협을 자동으로 탐지, 경고 및 완화할 수 있어 사이버 보안 표준을 높이고 데이터 및 정보의 안전성을 향상시킬 것으로 예상됨

▶ 말레이시아 사이버보안청(CyberSecurity Malaysia)하의 말레이시아 컴퓨터 비상대응팀(MyCERT)이 호주에서 개최된 CTF(Asean Capture the Flag) 대회에서 전체 챔피온으로 부상함(2019년 6월)[151]

- 호주 사이버 보안 센터(Australian Cyber Security Centre, ACSC)에서 주최한 CTF 대회는 참가자들이 영향을 받은 시스템의 포렌식 분석을 수행함으로써 컴퓨터 보안 문제를 해결하도록 도전하기 위해 고안되었음
- 이번 대회는 사이버 사고 예방 및 대응 역량과 스틸을 강화하기 위해 동남아시아 10개국의 실무자 수준의 사고 대응 전문가들이 참여하였으며, 또한 사이버 사고 대응자가 호주 사이버 보안 센터(ACSC)에 대한 통찰력을 얻을 수 있는 기회를 제공했으며, 호주와 아세안 국가의 사고 대응자간 실무 수준의 관계를 구축할 수 있는 기회를 제공함
- 이번 사고 대응 도전은 시뮬레이션 된 사건에서 수집된 인공물 분석에 관한 것으로, 여기서 제기된 도전에 대한 답을 찾아야만 하였음
- 이번 대회의 우승으로 인한 역량 인정과 함께 말레이시아 사이버보안청은 전문성과 기술을 최고 수준으로 강화시키며 지속적으로 안전한 사이버 공간 환경을 만들어 나가고자 함

150 the Sun daily, CSM-ACE the right platform to address cyber security issues: Gobind, 2019.9.23.
151 Digital News Asia, CYBERSECURITY MALAYSIA WINS INTERNATIONAL COMPETITION, 2019.7.4.

▶ 말레이시아에서 데이터 유출 사고가 증가함에 따라, 개인 정보가 도난당한 경우, 말레이시아 기업이 데이터 유출을 공개하도록 강요하는 법률의 필요성이 제기됨

- IBM의 사이버 보안 및 개인 정보 보호 프로그램 책임자인 Gant Redmon은 회사가 위반을 선고해야하는 지 여부를 결정할 수 있는 확실한 법률을 마련할 것이라고 밝힘
- 하지만 CMS의 CEO인 Amirudin Abdul Wahab 박사는 보안 위원회가 금융 회사에게 특정 상황에서 공개를 요구하지만 말레이시아 기업은 데이터 유출을 선언할 의무가 없다는 입장임
- 사이버 공격이 계속 증가하고 있고, 이는 지난 7년 동안 MyCERT에 보고된 데이터의 약 절반을 차지함. 하지만 위반 선언이 의무가 아닌 것을 감안하면, 이 수치는 축소 보고되었을 가능성이 있음

▶ Huawai와 CyberSecurity Malaysia는 사이버 보안을 증진시키고 발전시키는 것을 목표로 MOU를 체결함. Huawai는 2001년부터 말레이시아의 ICT 분야 산업을 지원해왔음(2017.11)

- 이 MOU를 토대로, Huawai는 CyberSecurity Malaysia Collaborative Partner(CCP) 프로그램을 통해 사이버 보안 업계의 현지 플레이어를 지원하고 개발할 것, 또한 연수 과정을 통해 보안 문제에 대한 지식과 시스템을 공유할 것임
- 이는 말레이시아의 국내 및 국제 수준의 사이버 보안 문제에 대한 인식을 증진시킬 것임

5) 정보보호 스타트업 관련 정책동향

▶ 디지털경제공사(MDEC)는 사이버 보안 부문에 더 많은 여성이 참여할 수 있는 컴백 경력 프로그램을 시작함(2019년 6월)[152]

- 디지털경제공사(Malaysia Digital Economy Corporation, MDEC)는 새로운 '사이버 위험 관리 프로그램의 여성 역량 강화(Empowering Women in Cyber Risk Management Programme)'에 여성의 지원을 장려함으로써 여성이 사이버 보안 인력의 일원이 될 수 있도록 함
- 이 프로그램은 산업 4.0시대에 여성들이 수요가 많은 직업에 필요한 기술을 개발할 수 있도록 하며, 사이버 보안 분야에서 인재를 육성하고, 여성들이 복귀하는데 필요한 기술을 제공하기 위한 전략적인 지속적인 노력의 부분임
- 성공적인 지원자는 CIMB, PwC Malaysia, Cisco Systems, Asia Cybersecurity Exchange 등과 같은 프로그램의 업계 파트너와 함께 3개월 교육 기간을 거치게 될 것임
- 직장에서 스킬을 향상시키고, 사이버보안 부문에서 통찰력을 개발하는 방법에 대한 교육을 받을 것이며, 또한 글로벌 인증 프로그램에 등록되어 이 분야의 일부가 되기 위해 필요한 것을 갖고 있음을 보여줄 것임

---

152 The Star Online, MDEC launches comeback career programme for more women to join cybersecurity sector, 2019.6.20.

- 훈련 기간 동안 연수생에게는 다양한 월별 수당이 지급되며, 신청자에게 교육하고 고용을 제공하기 위한 산업 파트너에게 10,000RM의 인센티브가 제공됨
- MDEC는 50개 지점으로 첫 교육 강좌를 시작하며, 많은 수의 응용 프로그램을 받을 수 있도록 준비함
- 이 프로그램은 여성가족 및 지역사회 개발부(Ministry of Women, Family and Community Development), 국가사이버보안청(National Cyber Security Agency, NACSA), Jabatan Pembangunan Wanita(JPW)와의 파트너십으로 진행됨

융합보안시장 및 정책 동향

1) 융합보안 시장 현황

핀테크

▶ 2018년 말 말레이시아는 현금을 대체하고 직불 카드를 보완하기 위해 높은 휴대 전화 보급률을 이용한 e-payment 전환을 도입하고 있음[153]

- 예를 들어 Bank Negara Malaysia는 상호운용가능한 신용 전환 프레임워크(Interoperable Credit Transfer Framework, ICTF)를 구현하고 있으며, 이 서비스를 통해 지불인은 자신의 기관이 수혜자에게 자금을 송금할 수 있도록 지시할 수 있음
- QR(Quick Response) 코드를 사용하여 디지털 결제에 대한 원활한 사용을 지원함
- 은행과 비은행 고객 모두 수신자의 휴대전화 번호와 신분증 번호를 참조하거나 수신자 스마트폰의 QR코드를 스캔하여 네트워크를 통해 원활하게 자금을 이체할 수 있음
- 중소기업은 최대 5,000RM까지 즉시 이체 거래를 하거나 받는데 수수료가 부과되지 않음

2) 융합보안 정책 현황

스마트시티

▶ 디지털 보안 전문기관인 CyberSecurity Malaysia은 연방 정부의 행정 센터인 Putrajaya에서 사물인터넷(IoT) 및 스마트시티 개발의 기타 구성요소에 대한 취약성 평가 및 침투 테스트 시스템을 2017년 12월에 시작함[154]

- 이 프로젝트는 2년 이상 걸리며 공공 WiFi 및 CCTV와 같은 7개 범주로 나뉘며, 신호등, Putrajaya 호수 수질 모니터링, Putrajaya 댐 모니터링, 공동 유틸리티 트렌치(Common Utility Trench, CUT) 및 날씨 모니터링을 처리하는 스마트 시스템의 디지털 보안 측면을 검토함

사물인터넷(IoT)

▶ 국가 사물인터넷 전략 로드맵(National Internet of Things (IoT) Strategic Roadmap)[155]

---

153 BuddeComm, Malaysia – Fixed Broadband Market – Statistics and Analayses, 2019.8.24
154 BuddeComm, Malaysia – Telecoms Infrastructure, Operators, Regulations - Statistics and Analyses, 2019.8.24
155 BuddeComm, Malaysia – Telecoms Infrastructure, Operators, Regulations - Statistics and Analyses, 2019.8.24

- 말레이시아의 과학기술혁신부(Ministry of Science, Technology and Innovation)와 응용연구기관인 MIMOS는 2015년 7월 국가 사물인터넷 전략 로드맵(National Internet of Things (IoT) Strategic Roadmap)을 발표하였으며, 말레이시아의 IoT 구현을 위한 가이드라인으로 사용될 것임
- 정부는 IoT 구현으로 2020년까지 국가 총소득에 약 95억 MYR을 기여하고, 산업계는 2020년까지 14,000명의 고숙련 고용기회를 창출할 것으로 기대함

▶ IoT 보안 실험실(IoT Security Laboratory)는 취약점을 시뮬레이션하고 강화 단계를 테스트함[156]
- CyberSecurity Malaysia는 중요한 정보 시스템 및 기술에 대한 취약성 평가 실험실을 보유하는 것이 중요하다는 사실을 인식함
- 그러므로 실험실(테스트베드)은 평가를 수행하고 일반적이고 잠재적인 취약점을 식별하며 완화 방법을 조사함

스마트공장

▶ 말레이시아는 더 높은 생산성, 기여, 혁신, 숙련된 노동력을 통해 제조부문 중소기업의 참여를 높이기 위한 전략적 접근법인 산업 4.0에 대한 국가 정책인 Industry4WRD[157]를 2018년 10월 31일에 시작함[158]
- 산업 4.0에서 산업 통신은 확장되고 강하게 연결되므로 디지털 보안은 산업환경에서 중요한 측면이며, 기존의 사이버 보안 방식으로는 보호할 수 없는 연결된 장치와 환경으로 구성되어 더욱 복잡해짐
- 그러나 산업 4.0 애플리케이션을 보호하는 사이버 보안 솔루션을 제공하는데 현지 기능 및 역량이 부족함
- 또한 제조 및 공급망을 따라 원활한 디지털 흐름을 가능하게 하는 중요한 장벽은 데이터 및 지적 재산 모두에 대한 표준, 상호 운용성 및 거버넌스가 부족함
- 전략에서 규제적인 측면으로 데이터 무결성, 표준 공유 및 보안을 향상시켜 제조가치 사슬의 완벽한 통합을 촉진하고 효과적인 산업 4.0 프로그램을 위한 정부부처간 조정을 지원하며, 이를 위해서 표준과 보안 프로토콜의 개발과 부처와 기관간의 통합이 필요함
- 행동계획 및 프로그램으로 말레이시아의 광범위한 사이버 보안 기능 개발의 일환으로 산업 4.0에 대한 일련의 사이버 보안 및 IoT 보안 지침 수립함

▶ 2018년 정부 예산 발표에서 말레이시아 정부는 4차 산업혁명(Industry 4.0)에서 투자 및 비즈니스 활동을 지원하기 위해 스마트 제조 서비스를 업그레이드에 국내 투자 전략 기금(Domestic Investment Strategic

---

156 CyberSecurity Malaysia, Staying ahead of emerging security challenges in digital industrial revolution - Malaysia's perspective, 2019.5.16.
157 Ministry of International Trade and Industry(MITI), Industry4WRD, National Policy on Industry 4.0, 2018.
158 Ministry of International Trade and Industry 홈페이지: www.miti.gov.my

Fund)에서 2억 4,500만 RM의 보조금을 제공함[159]

블록체인(가상화폐 포함)

▶ 말레이시아 재무장관은 증권으로 암호 화폐(cryptocurrency) 및 초기 코인 제공(ICO)을 규제하는 명령의 발표를 발표함(2019년 1월)[160]

- 암호화 서비스 제공업체와 거래소는 국가 증권 위원회(Securities Commission, SC)으로부터 승인을 받아야 하며, 중앙 은행과 협력하여 규정을 준수해야 함
- 증권 위원회의 규정에 따라 증권으로 디지털 통화 및 디지털 토큰을 인식하는 명령이 발효될 예정이며, 이에 따라 암호화폐, ICO 및 관련 활동은 관련 증권법을 준수하고 위원회의 승인을 받아야 함
- 증권 위원회는 디지털 자산의 제공 및 거래를 규제하기 위한 지침을 마련할 것임
- 해당 지침에는 거래 규칙 및 고객 자산 보호에 있어 발행자 및 거래 운영자의 적합성 등을 결정하는 기준을 수립하며, 디지털 자산을 취급하는 사람은 자금 세탁 방지 및 테러자금 조달 규칙, 사이버 보안 및 비즈니스 연속성 조치를 취해야 함

핀테크

▶ 2006년부터 비은행 업체인 핀테크 기업의 해외 송금 개방[161]

- 일본 2010년, 우리나라는 2017년에 이르러서야 허용된 것과 비교해 매우 개방적인 정책 펼침
- 이를 계기로 핀테크 업체의 시장 점유율은 2006년에는 10%에 불과했지만 2014년에는 50%를 웃돌게 됨

▶ 규제 완화 및 특구 조성으로 스타트업들의 시장 참여 기회를 폭넓게 부여[162]

- 말레이시아 중앙은행은 2018년 4개의 핀테크 기업에 규제 샌드박스를 적용하여 사업을 허가하였고, 중앙정부는 알리바바그룹과 함께 e-허브 디지털자유무역지구(DFTZ) 구축 추진

159 BuddeComm, Malaysia – Telecoms Infrastructure, Operators, Regulations - Statistics and Analyses, 2019.8.24
160 Bitcoin, Malaysia Starts Regulating Cryptocurrencies Today, 2019.1.15.
161 https://www.hankyung.com/economy/article/2019112772321
162 https://www.asiae.co.kr/article/2018061011555888114

아. 라오스

'18년 GDP(십억달러)	18.13
'18년 인구수(천명)	7,060

■ ITU 글로벌 사이버보안 지수(Global Cybersecurity Index, GCI)

· 라오스의 사이버보안 지수는 0.195로 하위권에 속함

국가명	2018		2017		전년대비 증감	
	지수	순위	지수	순위	지수	순위
라오스	0.195	121	0.392	77	-0.197	-44
대한민국	0.873	15	0.782	13	+0.091	-2

■ ICT 관련 주요 지수

· 라오스의 ICT 발전 수준은 대부분 100위권 이하로 전반적으로 하위권에 속해 있음

지표명	라오스		한국	
	점수	순위	점수	순위
IMD 국가경쟁력지수(2019)	-	-	-	28
IMD 디지털경쟁력지수(2019)	-	-	-	10
UNCTAD 전자상거래지수(2019)	35.1	113	89.4	19
ITU 글로벌 사이버보안 지수(GCI 2018)	0.195	121	0.873	15
UN 전자정부 지수(2018)	0.305	162	0.901	3

■ ICT 관련 주요 통계 (ITU, 2018년 말 기준)

· 라오스의 이동통신(ICT) 보급률은 50%대로 아직 국민의 절반 가량이 이용하지 않음

항목	라오스		한국	
	가입자수(천 명)	보급률(%)	가입자수(천 명)	보급률(%)
유선전화	1,482	20.99	25,907	50.63
유선브로드밴드	45	0.64	21,286	41.60
이동통신	3,662	51.86	66,356	129.67
인터넷 이용률	-		95.90%	

정보보호 산업 개요

1) 보안 환경

정보보안

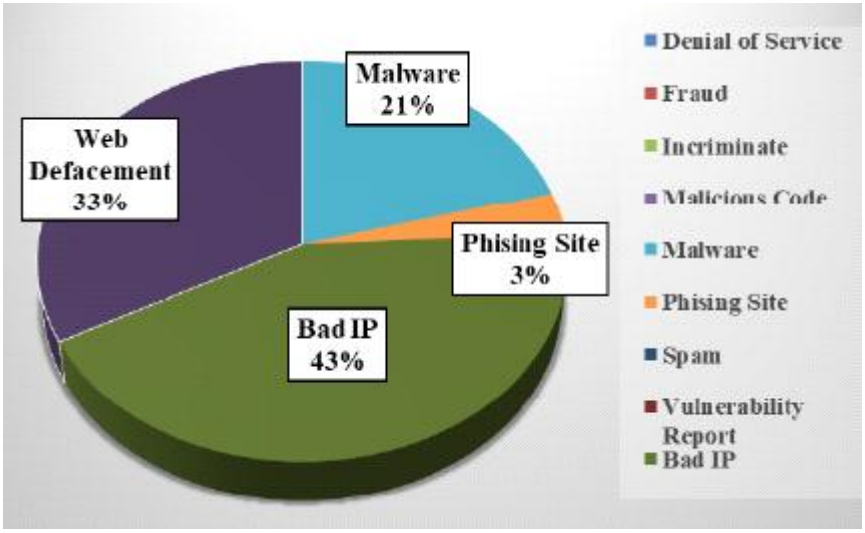
▶ ITU의 글로벌 사이버보안 지수(GCI)에서 라오스의 지수는 0.195로 전 세계 국가 중 120위, 아시아 지역에서는 22위로 하위권을 기록

▶ 국제 사이버 정책센터(International Cyber Policy Center)의 '아시아태평양 지역 사이버 성숙도 2017(Cyber Maturity In the Asia-Pacific Region 2017)'보고서에 따르면 라오스의 사이버 성숙도는 30.3점으로 전체 25개국 중 19위로 하위권

- 동 조사는 거버넌스, 사이버범죄, 군사, 기업 활동, 사회의 5개 방면에서 성숙도를 평가한 것으로 라오스는 2016년에는 23개국 중 20위로 2017년과 비슷한 순위를 유지
- 라오스는 사이버범죄에 대처할 기관 및 금융과 관련된 사이버범죄 법제 면에서 5점 만점에 1점을 받았으며, 사이버보안과 사이버정책에 있어 군의 역할 면에서도 1점으로 낮은 평가를 받았음
- 사이버 문제와 관련된 정부 조직과 사이버 이슈에 관한 법제/규제, CERT와 같은 사이버보안 지원기관의 존재 여부 등에서는 각각 4점으로 비교적 높은 평가를 받았음
- 사이버 문제에 관한 정부와 기업 간의 교류 현황에서는 4점을 받았으며, 사이버 문제에 대한 대중의 인식 수준과 인터넷을 이용하는 개인의 비중은 각각 3점을 기록

▶ 라오스 침해사고대응팀(LaoCERT)에 따르면 2018년 기준 라오스의 사이버 침해사고 유형은 악성 IP의 비중이 43%로 가장 높게 나타났으며, 웹 변조(33%)와 멀웨어(21%), 피싱 사이트(3%)가 그 뒤를 이었음

그림 _ 2018년 라오스 사이버 침해사고 현황



[출처] LaoCERT(2018)

물리보안

▶ 미국 해외안보자문위원회(Overseas Security Advisory Council, OSAC)의 '2018년 라오스 범죄 및 안전 보고서'에 따르면 라오스의 치안 상태는 양호한 편으로, 무기를 이용한 강력 범죄의 발생 확률은 희박함

- 이처럼 안정적인 치안 환경으로 인해 보안 장비에 대한 수요는 주로 기업이나 정부기관에 집중되어 있으나, 최근 라오스는 연평균 6% 후반대의 빠른 경제 성장을 지속하고 있어 소득 증가와 함께 치안에 대한 관심도 늘어날 전망
- 라오스 현지의 보안 제품 유통업체들에 따르면 아직까지 개인의 보안장비 수요는 적은 편이나, 일부 소비자들이 스마트홈이나 보안제품에 관심을 보이고 있어 시장의 점진적 성장이 예상됨

2) 인터넷 및 통신 환경

▶ 국제 마케팅 조사업체 'We are Social'에 따르면 2019년 1월 기준 총 701만 명의 라오스 인구 중 인터넷을 사용하는 인구는 전년 대비 13% 증가한 270만 명으로, 보급률은 39% 수준

- 이동통신 가입자 수는 565만 명으로 전년 대비 2.8% 증가했으며, 인구 대비 보급률은 81%를 기록

- 이동통신 가입자 중 선불제 가입자의 비중이 96%에 달하며, 3G와 4G 인터넷을 지원하는 서비스의 가입자 비중은 57%임
- 모바일 인터넷 이용자 수는 260만 명으로, 전체 인구 대비 모바일 인터넷 사용자 비율은 37%이며, 모바일 인터넷 평균속도는 22.75Mbps로 나타남
- 전자상거래 관련 지표의 경우, 금융기관에 계좌를 보유한 사람은 전체 인구의 29%, 신용카드를 보유한 사람은 0.6%에 불과하며, 온라인 구매 경험이 있는 사람의 비율도 7.1%에 그쳤음

그림 _ 라오스 인터넷 및 모바일 사용 인구 현황

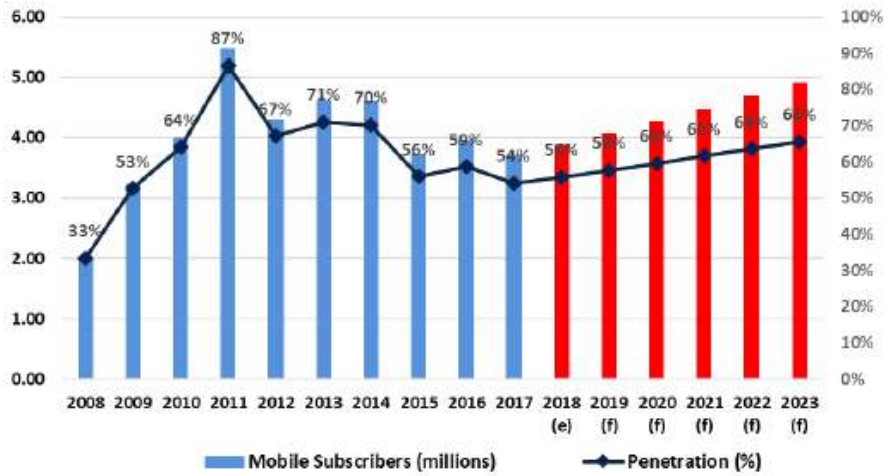


[출처] We are Social(2019.1)

▶ 라오스의 이동통신 시장에는 Lao Telecom, ETL, Beeline, Unitel 등 4개 사업자가 있으며, Unitel이 시장 점유율 45%로 1위 사업자이며, Lao Telecom(38%)이 그 뒤를 잇고 있음

- 시장조사기관 BuddeComm에 따르면 라오스의 이동통신 시장은 2023년까지 완만한 성장을 이어나갈 전망으로, 정부의 엄격한 규제로 인해 시장 발전이 제한되고 있으며, 네트워크 유지와 업그레이드에 대한 통신사들의 투자도 부족한 상황
- 라오스의 이동통신 보급률은 2020년 60%에서 2023년까지 66%로 늘어날 전망이며, 2018-2023년 사이 4.8%의 연평균 성장률을 기록할 것으로 예상됨

그림 _ 라오스 이동통신 가입자 수 및 보급률 추이(2008~2023년)



[출처] BuddeComm(2019.3)

▶ BuddeComm에 따르면 라오스의 유선 브로드밴드 시장 보급률은 2012년 0.1%에서 2018년 0.4%로 매우 미미하게 성장하였으며, 앞으로도 성장세는 이어가겠지만 전체적인 시장 보급률은 큰 변화가 없을 전망

- 반면 모바일 브로드밴드 시장은 이동통신 사업자들이 4G 서비스를 시작하면서 빠르게 확장되고 있음
- 라오스에서는 2012년 LTC가 처음 4G 서비스를 출시했으며, Unitel은 2015년 6월 수도 비엔티엔에서 4G 서비스를 개시하여 현재는 사바나켓, 루앙프라방, 참파삭 등의 주요 도시에서 4G 서비스를 제공
- 2018년 기준 3G 통신망의 인구 커버리지는 78%, 4G LTE/Wimax의 인구 커버리지는 약 40%임
- 2018년 기준 라오스의 모바일 브로드밴드 가입자 수는 전년 대비 12% 증가한 246만 명으로 추정됨
- 라오스 모바일 브로드밴드 시장은 2018-2023년까지 7%의 연평균 성장률을 기록하며 2023년까지 보급률 46%에 가입자 수 345만 명을 기록할 전망
- 이동통신 가입자의 꾸준한 증가와 통신사간 경쟁으로 인한 가격 인하 및 4G 서비스 보급에 따른 속도 향상이 모바일 브로드밴드 시장의 성장을 견인

▶ 한편, 라오스에서 5G는 이제 논의가 시작되는 단계로, 라오스 우정통신부 주파수관리국은 2019년 5월 인터넷 사업자들과 가진 워크숍을 통해 주파수 정책과 네트워크 장비 수요를 논의

- 라오스 정부관계자는 5G 네트워크 도입 여부는 시장 수요에 달려있다며, 정부가 현재 교육, 의료, 농업 분야에서 5G의 잠재적 이익을 고려중이라고 밝힘

정보보호 시장 현황

1) 시장 규모

정보보안

▶ 라오스의 정보보호 시장은 시장 규모에 대한 통계도 존재하지 않을 만큼 낙후되어 있으며, 정보보호 수준을 향상시키기 위한 국가 전략도 부재하여 단기간 내 국가적 지원을 통한 성장 가능성은 제한적

- 라오스의 사이버보안 대응능력은 ASEAN 국가 중 캄보디아에 이어 최하위로 평가되며, 인구수도 적어 해외 보안업체들도 라오스에 직접 지사를 개설하기보다는 태국 등 주변국가의 지사에서 현지 유통업체를 거쳐 제품을 공급

▶ 2016년 10월 라오스 우정통신부 자료에 의하면 라오스의 ICT 관련 기업은 총 398개로 이중 ICT 보안업체로 분류된 업체는 단 한 개에 불과했으며, ICT 리셀러가 234개, ICT 설치 업체가 99개로 대부분을 차지하고 있음

물리보안

▶ KOTRA 라오스 현지 무역관에 따르면 라오스는 보안 소프트웨어나 CCTV 등의 보안 장비를 자체적으로 생산하는 업체가 없고 IT 유통업체들이 중국, 태국, 베트남 등 주변국에서 수입함

- 물리보안 시장의 경우 낮은 소득과 안정적인 치안 환경으로 인해 개인 소비자는 보안장비에 대한 인식과 수요가 높지 않으며, 주로 기업과 기관, 임대사업자들을 중심으로 보안장비 수요가 형성
- 개인은 주로 가격이 저렴한 중국산 제품을 선호하며, 기업이나 정부는 첨단 기술제품과 유명 브랜드를 선호하는 경향

2) 주요 사업자 현황

▶ TTiT-Solutions

- 라오스 수도 비엔티엔에 위치한 TTiT-Solutions는 글로벌 보안 시스템 업체 Robert Bosch Limited의

공식 딜러로서 CCTV 시스템, 접근통제 시스템, 화재 경보 제품과 시스템, 빌딩관리 시스템 등을 취급

- Bosch 제품 외에도 중국 보안업체 Dahua의 접근통제 시스템과 CCTV, 삼성전자의 CCTV도 함께 취급
- 물리보안 제품 외에 엔드포인트 보안, 방화벽과 VPN, 침입방지시스템, 이메일 보안 등의 네트워크 보안 제품도 취급

▶ Kerberos Security

- 2006년 설립된 라오스 현지의 보안 전문업체로 안전 시공, 보안 감시와 설계, 보안 컨설팅, 시스템 통합 등의 영역에서 활동
- Kerberos Security는 라오스 프랑스 대사관의 CCTV와 접근통제, 통신 시스템 시공과 미국 대사관의 차량 출입통제 시스템 등을 수주한 바 있음
- Kerberos Security가 제공하는 보안 솔루션으로는 펜스 시스템, 접근통제와 신원관리, 아날로그 및 고해상도 디지털 CCTV, 침입 탐지 및 경보 시스템, 빌딩 자동화, 화재 경보 시스템, 차량 모니터링과 보호 시스템 등이 있음

▶ Trivico Computer Sole Co., Ltd

- 라오스 비엔티엔 소재의 IT 종합 유통업체로, 보안 관련 제품으로는 중국 업체 Hikvision의 CCTV와 Kaspersky 및 Trend Micro의 안티바이러스 소프트웨어, 경보시스템 등을 취급

3) 주요 동향 및 이슈

▶ 라오스 보안장비 시장, 중국 업체들이 주도(2019.05)

- 보안 전문 매체 ASMAG.com에 따르면 라오스의 보안 시장은 저가를 무기로 한 중국 기업들이 주도하고 있으며, 특히 HikVision과 Dahua의 인기가 높음
- 라오스 에너지와 광산 분야에 대한 중국의 투자규모는 100억 달러에 이르며, 중국 정부는 라오스 정부에 50억 달러를 원조하는 한편, 라오스에 투자하는 중국 기업들에게 50억 달러를 지원
- 라오스에 투자하는 중국 기업들은 자신들의 자산과 사무실, 시설 등을 보호하기 위해 중국산 보안 제품을 선택하며, 정부 기관이나 교통 프로젝트에도 Dahua를 비롯한 중국 보안제품이 선호됨

▶ 라오스 디지털 도어록 시장 성장세(2019.05)

- KOTRA 라오스 무역관에 따르면 경제 발전에 따라 주요 도시를 중심으로 부동산 등의 인프라가

개발되면서 디지털 도어록 등 보안장비에 대한 수요가 증가 추세

- 비교적 안전한 치안, 주택 위주의 주거 형태, 낮은 소득 등의 영향으로 일반 가정의 도어록 수요는 많지 않으나, 최근 아파트 등 신식 주거건물이 증가하면서 일반 가정의 수요도 점차 증가 추세
- 과거 일부 3성급 이상의 호텔, 외국인 전용 주거단지 등에 국한되었던 디지털 도어록 수요는 상업용 부동산, 신축 관공서 건물로 확대되고 있음
- 라오스는 낮은 소득 수준으로 인해 제품 구매 시 품질과 기술보다 가격을 더 우선시하는 소비 경향을 보이나, IoT 기술을 활용한 스마트 도어록 등도 최근 시장에 선보이기 시작하여 공유 주택과 호텔, 소수 고소득층을 대상으로 시장 테스트 및 초기 마케팅이 이루어지고 있음
- 라오스 디지털 도어록 시장에서는 Colt(태국), Yale(다국적), HAFELE(다국적), Hikvision(중국) 브랜드가 보편적으로, 시장 규모가 작은 라오스의 기업들은 판권을 지닌 태국 유통기업으로부터 다국적 브랜드 제품을 수입, 판매함
- 라오스 소비자들은 기능 대비 가격이 저렴하고 설치와 사후 기술지원이 용이한 태국 제품 및 태국에서 유통하는 다국적 기업 제품을 선호하는 경향

▶ 라오스, 국제공항에 첨단 보안시스템 도입 계획(2016.10)

- '첨단 승객처리시스템(Advance Passenger Processing system, APP)'라는 명칭의 새로운 시스템은 출입국 절차를 간소화하는 동시에 보안을 강화하기 위한 것으로, 시스템 도입을 위해 라오스 이민경찰국은 태국의 국가보안 시스템 업체 SOMAPA IT와 MOU를 체결
- 시스템 상에서 수집된 승객 정보는 라오스 내 이민경찰국과 승객이 향하는 목적지의 이민관리국에 곧바로 전송되어 테러 예방에 효과적
- 또한 동 시스템은 블랙리스트에 등재된 승객을 확인할 수 있어, 해당 승객이 수속하는 경우 잠재적 보안 위험을 차단 가능
- 시스템을 구축할 SOMAPA IT에 따르면 동 시스템은 아세안 국가 중 미얀마와 태국에 이어 라오스에 세 번째로 도입되는 것으로, 태국에서는 2015년 12월부터 테러와 기타 범죄 예방을 위해 시행 중

정보보호 정책 및 기관 현황

1) 관련 법령 및 정책

관련 법령 및 규제

▶ 사이버범죄 예방 및 대응법(Law on Prevention and Combating Cyber Crime)

- 라오스에서는 사이버범죄 예방 및 대응법이 2015년 7월 발효되었음
- 사이버범죄 예방 및 대응법은 국가 안보와 사회질서를 보장하기 위해 데이터베이스와 서버 시스템, 컴퓨터 데이터 및 정보의 보호와 사이버범죄에 대한 예방 및 대응을 위한 원칙과 규제, 대응 조치 마련을 목표로 하고 있음
- 동 법의 적용 대상은 라오스 국경 내에서 컴퓨터 시스템과 컴퓨터 데이터 및 정보를 운영 및 처리하는 국내외 기업과 개인임
- 동 법의 주요 원칙은 아래와 같음

표 _ 라오스 사이버범죄 예방 및 대응법의 주요 원칙

주요 원칙
1. 국가 정책과 법률, 전략 계획 및 사회경제 계획에 부응 2. 국가 문화와 전통, 국가 안보와 평화, 사회질서를 준수 3. 국가 및 조직, 개인의 기밀 보호 4. 통일성과 안전성, 신속성과 공정성을 보장 5. 법률과 규제에 의거해 서비스 사업자의 합법적 권익과 소비자의 컴퓨터 시스템 서비스와 컴퓨터 데이터 및 정보를 보호 6. 사회의 참여를 보장 7. 라오스가 참여하는 국제협약 및 조약의 준수

[출처] Law on Prevention and Combating Cyber Crime, LaoCert

- 사이버범죄 예방 및 대응법은 비인가 컴퓨터 접속 및 시청각 자료의 비인가 편집, 컴퓨터 정보의 비인가 탈취와 온라인 소셜미디어를 통한 피해 유발, 음란물 유포, 컴퓨터 시스템 간섭, 컴퓨터 데이터 및 정보의 위조와 파괴 등을 불법으로 규정
- 또한 사이버보안 사고 발생 시 통지 및 긴급대응 계획을 규정하고, 우정통신부가 사고를 통지받아 필요한 기술적 조치를 취할 것을 요구

- 우정통신부는 사이버범죄에 대한 의식 향상을 위한 대국민 홍보활동과 관련 당국과 인원의 훈련, 긴급사고 모니터링과 사이버범죄 관련 통계와 데이터베이스 시스템 개발 등을 실시해야 함
- 사이버범죄 예방 및 대응법은 또한 라오스 침해사고 대응팀(LaoCERT)의 권리와 의무를 규정하고, LaoCERT에 사이버범죄의 예방 및 대응을 위한 규제방안의 연구개발과 컴퓨터 시스템 보안 인력의 개발과 훈련, 사이버보안 사고의 모니터링과 점검 등을 실시할 것을 요구

▶ 전자 데이터보호법(Electronic Data Protection Law)

- 라오스 정부는 2017년 5월 12일 전자데이터보호법을 발효했음
- 동 법은 전자데이터를 출처를 밝힌 한 누구나 회람 및 사용할 수 있는 일반 데이터, 그리고 소유주의 허락 없이 회람될 수 없으며 국가 정보와 개인/민감 정보를 포함하는 특정 정보로 분류

주요 전략 및 정책

▶ 제8차 2016-2020년 사회경제개발 5개년 계획(8th Five Year National Socio-Economic Development Plan 2016-2020)

- 라오스 정부는 ICT 약소국의 지위를 벗어나기 위해 ICT 분야의 발전과 관련 환경 조성에 많은 노력을 기울이고 있으며, 2011-2015년 제7차 라오스 사회경제개발계획을 통해 인터넷, 통신, 우정 사업의 환경 개선을 위한 인프라를 구축
- 2016년 발표된 제8차 2016-2020년 사회경제개발 5개년 계획은 더 나아가 정보통신기술을 사회 전반에 적용하기 위한 토대 마련을 강조하면서 ICT 발전방향을 아래와 같이 설정함

  ·기초 통신 및 전자정보 인프라 개발 촉진, 서비스 부문의 현대화 지원을 위해 고속·고품질 서비스 제공, 전자상거래 촉진, 사회경제개발 강화, 국제 표준에 부합하는 ICT 발전을 위한 중심축이 될 수 있도록 통신환경 업그레이드

표 _ 제8차 2016-2020년 사회경제개발 5개년 계획 중 ICT 주요 목표

달성 기간	주요 내용
2016년	국가인터넷서비스코드(la.) 관리 및 서비스 시스템 구축 완료
2018년	북부 및 중부지역에 인터넷 백업센터 구축
	라디오 주파수 관리센터 2곳 설립 및 해외 위성 대신 라오스 위성 사용 장려
	공공 및 민간 부문의 전자기록 취합을 위한 국가 데이터 센터 구축
	정부기관, 구역 및 마을의 50%를 연결하는 인트라넷 및 원격회의 시스템 구축

달성 기간	주요 내용
	정부기관의 50%에 대한 전자 관리 및 서비스의 점진적 개발
2020년	ICT 기술응용학습센터를 마을 규모 단체에 2곳, 구역 규모 단체에 2곳 설립
	e-거버넌스 지원을 위한 인프라 일환으로 공중 및 지하 광섬유 네트워크를 1만 킬로 확장하여 전국적으로 각 시당국과 수도 비엔티엔에 연결
	고품질·고효율·저비용 3G 및 4G 송수신국 확장으로 전 지역 서비스
	연간 GDP 성장률 8% 달성 위해 우정통신 분야의 매출 확대

[출처] 라오스 기획 투자부(2016.6)

▶ 2030년을 향한 ICT 비전 (ICT Vision 2030)

- 2015년 10월 라오스 우정통신부는 ICT 환경 조성을 위해 7가지 목표를 세우고 2030년까지 달성하겠다는 계획을 발표
- 7가지 세부 목표는 인적 자원 개발, 우편 부문 현대화, 사이버보안 강화, ICT 산업의 발전, 전자정부 구축, ICT 혁신 등임
- 우정통신부의 Thansamay Kommasith 장관은 2018년 비엔티엔에서 열린 라오스 ICT 엑스포 개회식에서도 2030년까지 라오스를 디지털 사회로 변모시키겠다는 비전을 다시금 확인했음
- 라오스는 그밖에 전자정부 개발계획 2013-2020, 2025년을 향한 ICT 전략 계획, 국가 ICT 정책 2015-2025 등을 추진 중

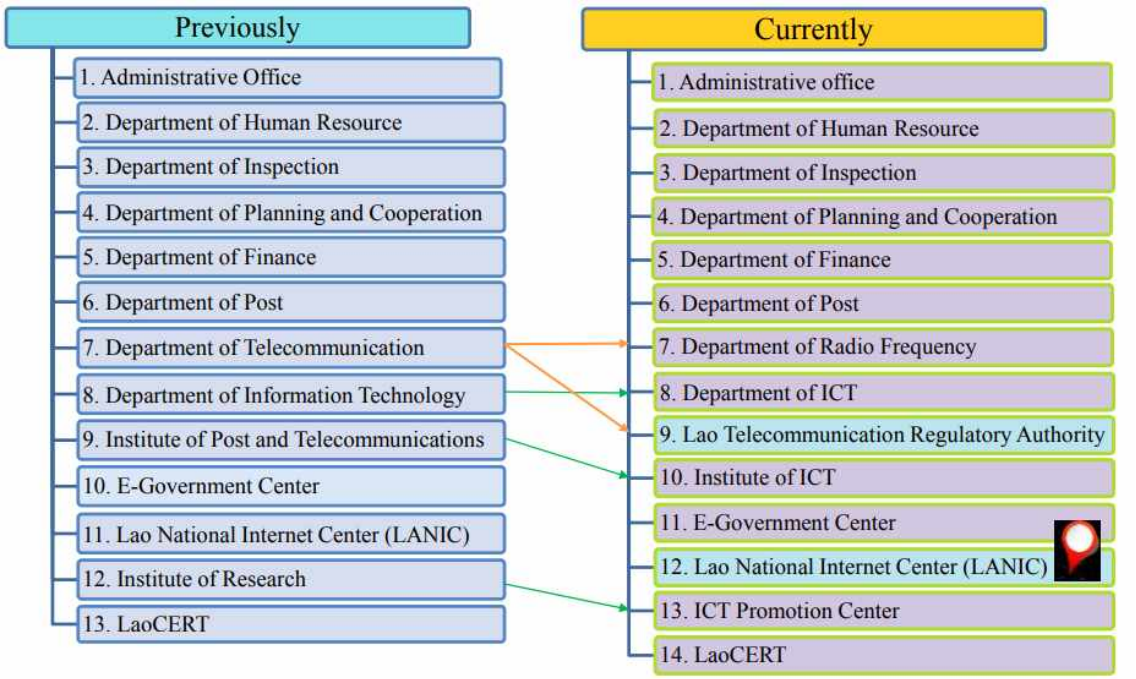
2) 담당기관

▶ 우정통신부(Ministry of Posts and Telecommunications, MPT)

- 2007년 10월 우편 및 정보통신 정책 추진을 위해 총리실 직속 기구로 설립된 라오스 국가우정통신청(National Authority of Post and Telecommunications)이 2011년 9월 우정통신부로 기관명을 변경함
- 우정통신부는 라오스의 우편 및 정보통신, 방송 정책과 규제를 총괄하고 있으며 전자정부 사업 실무 추진, 정보통신 관련 교육 실시 등을 주로 담당
- 우정통신부는 2017년 1월 조직 개편을 통해 기존의 통신국을 폐지하고 라오스 통신규제청(Lao Telecommunication Regulatory Authority)과 무선주파국(Department of Radio Frequency)를 신설함

• 또한 산하의 연구소(Institute of Research)를 폐지하고 ICT 증진센터(ICT Promotion Center)를 신설

그림 _ 라오스 우정통신부 조직도



[출처] 라오스 우정통신부

▶ 라오스 침해사고 대응팀(Lao Computer Emergency Response Team: LaoCERT)

• LaoCERT는 2012년 9월 라오스 우정통신부 산하 국가인터넷센터(Lao National Internet Center, LANIC) 산하기관으로 설립되었으며, 2016년 6월 LANIC에서 독립되어 우정통신부 직속기관이 되었음

• LaoCERT는 아시아태평양 CERT(APCERT)의 멤버이자 2016년 5월 카네기멜론대학으로부터 CERT 명칭의 사용을 정식으로 허가받았음

• 2018년 현재 LaoCERT의 직원 수는 총 32명으로, 조직 구조는 관리 및 국제협력국, 연구개발국, 사고대응국, 행정인사국의 4개로 구성되어 있음

• LaoCERT는 주요기반시설 보호를 위한 국가 사이버 전략의 수립 및 ICT 분야의 발전을 위한 법제 수립의 역할을 담당하고 있으며, 사고 처리와 대응, 경보발령, 네트워크 취약점 스캐닝, 기술 조언, 보안 의식 제고 등의 역할을 수행

그림 _ LaoCERT 조직도



[출처] LaoCERT(2018)

3) 최근 정책 동향 및 이슈

▶ 라오스, 전자정부 서비스에 블록체인 도입 계획(2019.07)

- Boviengkham Vongdara 라오스 과학기술부 장관이 베트남 기업 LINA NETWORK와 MOU를 체결하고 블록체인을 활용한 디지털 신원 서비스 도입을 추진하기로 함
- MOU에 의하면 LINA NETWORK는 블록체인과 사물인터넷, 빅데이터, 인공지능 기술을 활용해 라오스 정부에 블록체인 애플리케이션 개발을 위한 솔루션을 제공하기로 함
- LINA NETWORK는 또한 5년 내 블록체인 연구개발센터 설립 및 정부 애플리케이션 개발을 위한 블록체인 기술 연구 등을 위해 과학기술부에 50만 달러의 자금 원조를 제공하기로 함

▶ 라오스 최초의 디지털 포렌식 실험실 설립(2019.08)

- 라오스 공안부 산하 경찰국에 라오스 최초의 디지털 포렌식 실험실이 설립되었으며, 국제연합 마약범죄국((United Nations Office on Drugs and Crime, UNODC)이 노르웨이 정부의 자금 후원을 받아 실험실 설립을 지원함
- 디지털 포렌식 실험실은 초국가적 조직범죄와 사이버 범죄를 포함한 범죄조사에서 수집된 디지털 증거 분석 작업을 담당하게 됨

▶ 라오스-베트남, 전자정부와 사이버보안 협력 합의(2019.03)

- 라오스 우정통신부와 베트남 정보통신부가 사이버보안과 전자정부, 우편 서비스 개발 면에서 협력을 지속하기로 합의함
- 이번 합의는 응유엔 마잉 훙(Nguyen Manh Hung) 베트남 정보통신부 장관이 라오스를 방문한 동안 체결되었으며, 양국은 앞서 주파수 관리와 모터링, 인터넷 브로드밴드, 클라우드 컴퓨팅과 소셜 미디어 관리 면에서도 협력을 지속해 왔음

▶ 라오스 우정통신부, 전자상거래 발전계획 추진(2018.03)

- 2018년 3월 라오스 우정통신부는 향후 10년간 핵심적인 전략 목표 중 하나로 전자상거래 발전을 제시
- 우정통신부는 2025년까지 정보통신기술 기초 인프라의 구축을 완료하고 전자상거래 지원을 위한 법제화를 이끌어내겠다는 계획을 발표
- 정보통신 인프라와 법제가 완비되면 국내외 기업들은 온라인 거래에 대한 법적 보호를 받을 수 있어 온라인 거래도 활성화될 전망
- 우정통신부는 또한 현재 대부분 ASEAN 국가들보다 비싼 인터넷 서비스 비용을 인하하겠다는 계획도 발표
- 라오스 인터넷 사업자들에 의하면 기간통신사업자가 아닌 주변국으로부터 대역폭을 구매하기 때문에 요금이 높게 형성되고 있으며, 주변국들과 협상을 통해 비용 절감 필요

▶ 캄보디아·라오스·미얀마·베트남(CLMV) 아세안 4개국 사이버보안 관련 워크샵 개최(2016.12)

- 2016년 12월 스위스 ICT 평화재단의 지원으로 라오스 비엔티엔에서 열린 CLMV 국제 사이버보안 정책 및 외교 워크샵에서 CLMV 4개국은 사이버보안 규범과 역량 강화 등에 관해 협의
- 각국은 사이버보안 협력을 통해 광케이블 백본망과 글로벌 은행 간 결제네트워크 등의 주요정보기반시설 보호 및 아세안 커뮤니티의 성장 지원을 꾀할 방침
- 라오스 우정통신부의 Thansamay Kommasith 장관은 라오스의 발전과 생활수준 향상을 위해 ICT가 매우 중요하다고 발언
- 그는 또한 ICT가 많은 새로운 기회를 창출하는 동시에 그로 인한 사이버 공격 등의 보안 위험성도 높아지는 만큼, 이러한 위협에 대응해 국제적 보안 의무를 이행해나갈 것이라고 강조

4) 정보보호 스타트업 관련 정책 동향

▶ 한-라오스 ICT·스타트업·농업 협력 양해각서 체결(2019.09)

- 한국과 라오스 정부는 9월 5일 정보통신기술과 스타트업, 농업 등 제반 분야에서 양국간 협력을 강화하는 내용의 양해각서(MOU)를 체결함
- 양국 정상은 방송·통신 분야에서의 디지털 전환과 첨단 기술 분야에서의 협력 확대를 위해 정부 간 협력체계를 구축하는 내용의 '한-라 ICT 협력 양해각서', 스타트업·혁신 정책 및 프로그램에 대한 경험을 공유하고 설립 예정인 '스타트업 국제기구'에 공동 협력하는 내용의 '한-라 스타트업 협력 양해각서' 등을 체결
- 아울러 양국 정부는 이날 대외경제협력기금(EDCF) 기본약정을 체결, 우리 정부가 2020년부터 2023년까지 라오스 측에 총 5억달러 규모의 기금을 지원하기로 함

융합보안 정책 및 시장 현황

핀테크[163]

▶ 라오스는 핀테크 산업 발전 초기 단계로 은행이 주도하여 시장을 이끌고 있음

- 2017년 12월 라오스 최대 은행 BCEL((Banque pour le Commerce Exterieur du Lao))이 모바일뱅킹 앱 'BCEL One'을 론칭한 것이 계기가 됨
- 산업 발전 초기 단계로서, 다양한 금융분야 지불 서비스 중 휴대전화 요금 충전, 공과금 납부, QR코드 결제시스템을 이용한 지불·송금 수준에 그침
- 결제시스템의 경우 BCEL의 결제시스템 'One Pay'의 QR코드를 이용하여 이루어짐

▶ 중국 관광객의 자국 내 소비를 촉진시키기 위해 중국핀테크 기업의 라오스 시장 진입을 허용

- 2019년 9월부터는 중국의 알리페이, 위챗페이도 BCEL 가맹점에서 이용할 수 있도록 서비스를 도입하였는데, BCEL이 가진 자체 가맹점은 전국 1만여 곳이 넘음

163 http://news.kotra.or.kr/user/globalAllBbs/kotranews/album/781/globalBbsDataAllView.do?dataIdx=178519&column=&search=&searchAreaCd=&searchNationCd=&searchTradeCd=&searchStartDate=&searchEndDate=&searchCategoryIdxs=&searchIndustryCateIdx=&searchItemName=&searchItemCode=&page=4&row=10

4. 중남미 시장

중남미 시장 개요

▶ 중남미 지역(Latin America and the Caribbean)은 아메리카대륙에서 캐나다와 미국을 제외한 중앙아메리카 8개국과 남아메리카 12개국, 카리브 제도의 13개국과 식민 도서를 지칭

- 총면적은 약 2,055만㎢, 인구는 약 6억 4천만 명, GDP 5조 4,000억 달러의 대형 시장
- 중남미 지역은 풍부한 자원과 노동력을 기반으로 중국을 잇는 신흥국으로 부상하고 있음
- 경기 활성화를 위한 노력을 기울이고 있으나, 천연자원에 대한 지나친 수출의존도가 높은 사회 범죄율은 경제발전의 걸림돌로 지적되고 있음

표 _ 중남미 시장 주요국의 한국과의 관계(2018년 기준)

항목	수교일	우리나라 수출규모 (US$ 백만)	우리나라 수입규모 (US$ 백만)	우리나라의 주요수출품	우리나라의 주요수입품
멕시코	1962.1	11,458	5,090	자동차부품, 평판디스플레이	원유, 기타금속광물
코스타리카	1962.8.	168	139	승용차, 철강, 화물차	의료기기, 반도체기기, 커피
도미니카 공화국	1962.6	258	155	승용차, 배전 부분품	의료용전자기기, 기타의료위생용품
페루	1963.4.	803	2,474	승용차, 화물자동차	천연가스, 동광, 아연광
과테말라	1962.10.	237	67	화물자동차, 승용차, 편직물	커피류, 과실류, 폐건전지
엘살바도르	1962.8.	166	24	자동차, 섬유제품, 전기	커피, 당류, 고철 등

[출처] Kotra-국가정보, 외교부 국가/지역정보, stat.kita.net

▶ 대부분 중남미 국가들의 ICT 발전지수(IDI)는 열악하지만, 일부 국가에서는 빠르게 호전되고 있는 추세이며, 정부차원의 ICT개발 정책이 추진되면서 IT시장 전망은 매우 밝음

- 2017년 글로벌 ICT 발전지수(IDI)에 따르면 대부분의 중남미 지역 국가들의 IDI 순위는 세계 50위권 밖으로 이 지역의 ICT 경쟁력은 전반적으로 낮은 수준이지만 최근 수년간 중남미 IDI는 높은 증가율을 보임

표 _ 중남미 시장 주요국 ICT발전지수(IDI)

국가	IDI(2017년)		접근성(access)		이용성(use)		스킬(skill)	
	순위	지수	순위	지수	순위	지수	순위	지수
멕시코	87	5.16	94	5.28	76	4.65	95	5.93
코스타리카	60	6.44	74	6.40	47	6.18	63	7.05
도미니카 공화국	77	5.69	75	6.34	75	4.78	84	6.23
페루	96	4.85	102	4.90	90	3.96	75	6.54
과테말라	125	3.35	115	4.52	135	1.78	130	4.13
엘살바도르	119	3.82	109	4.75	124	2.25	118	5.11
한국	2	8.85	7	8.85	4	8.71	2	9.15

[출처] ITU, ICT Development Index 2017, https://www.itu.int/net4/ITU-D/idi/2017/index.html

▶ 국제전기통신연합(ITU)은 법적, 기술적, 조직적 대응 및 역량강화, 국제협력 등 5개 부문의 지수를 종합하여 글로벌 사이버보안지수(Global Cybersecurity Index, GCI)를 측정하여 국가 간 비교를 함

- 2018년 글로벌 사이버보안지수(GCI)에 따르면, 대부분의 중남미 지역 국가들의 글로벌 사이버보안지수는 세계 중위권 및 하위권이며, 아메리카 지역에서 캐나다의 GCI는 0,892점으로 세계 9위, 우루과이는 51위를 기록함

표 _ 아메리카 지역 글로벌 사이버보안지수(GCI)

국가	GCI(2018년)		법적(Legal)	기술적 (Technical)	조직적 (Oranizational)	역량강화 (Capacity building)	국제협력 (Cooperation)
	순위	지수	지수	지수	지수	지수	지수
미국	2	0.926	0.200	0.184	0.200	0.191	0.151
캐나다	9	0.892	0.195	0.189	0.200	0.172	0.137
우루과이	51	0.681	0.120	0.124	0.186	0.131	0.120
한국	15	0.873	N/A	N/A	N/A	N/A	N/A

[출처] ITU, Global Cybersecurity Index(GCI) 2018

▶ 유엔무역개발기구(UNCTAD)는 금융기관 또는 모바일 머니 서비스 제공업체의 계정 소유권, 인터넷을 사용하는 개인, 우편물 신뢰성 지수, 안전한 인터넷 서버 등 4개의 지수를 종합하여 B2C 전자상거래 지수(B2C e-Commerce Index)를 측정하여 국가 간 비교를 함

- 2019년 전자상거래 지수에 따르면, 대부분의 중남미 지역 국가들의 B2C 전자상거래 지수 순위는 세계 중하위권에 넓게 분포하고 있으며, 코스타리카의 B2C 전자상거래지수는 64.1점으로 세계 61위, 도미니카공화국은 67위, 페루는 90위, 멕시코는 91위, 과테말라는 108위, 엘살바도르는 110위를 기록함

표 _ 중남미시장 주요국 B2C 전자상거래 지수

국가	전자상거래지수 (2019)		인터넷 사용하는 개인	계정 소유권	안전한 인터넷 서버	우편물 신뢰성 점수
	순위	지수	지수	지수	지수	지수
멕시코	91	47.5	68	37	50	36
코스타리카	61	64.1	74	68	63	51
도미니카 공화국	67	60.4	75	56	45	66
페루	90	47.8	53	43	51	45
과테말라	108	37.5	65	44	41	0
엘살바도르	110	37.2	34	30	42	42
한국	19	89.4	96	95	67	99

[출처] UNCTAD, B2C e-Commerce Index 2019, https://unctad.org/en/PublicationsLibrary/tn_unctad_ict4d14_en.pdf

▶ 글로벌 시장조사기관인 MarketsandMarkets이 발표한 물리보안시장에 대한 보고서에서는 물리적 보안 시장 영역을 시스템 분야와 서비스 분야에서 시장 규모를 발표함

- 시스템 분야에는 물리적 접근 제어 시스템, 비디오 감시 시스템, 경계 침입 탐지 및 예방, 물리적 보안 정보 관리, 물리적 신원 및 접근 관리, 보안 검색, 이미징 및 금속 탐지, 화재 및 생명 안전에 대한 시스템이 포함
- 서비스 분야에는 서비스 분야에서 서비스로써의 접근 제어, 서비스로써의 비디오 감시, 원격 모니터링 서비스, 보안 시스템 통합 서비스를 포함

- 중남미 지역 국가들 중 브라질, 멕시코 및 아르헨티나에서 몇 년 동안 물리 보안 솔루션 및 제품에 대한 수요가 크게 증가하였으며, 이 지역의 산업 부문은 부적절한 범죄 활동을 처리하기 위해 물리 보안 솔루션을 채택하고 있으며 이러한 지출은 앞으로 몇 년동안 증가할 것으로 예상됨
- 물리보안 시장규모는 2018년 멕시코의 경우 10억 9천만 달러 규모로 연평균 성장률(2018-2023) 9.5%로 성장할 것으로 전망하며 그 외 중남미 국가들은 25억 8천만 달러 규모에 해당

표 _ 중남미 지역 주요국 물리보안 시장규모

(단위: 십억 달러)

국가	2016	2017	2018e	2023p	연평균성장률 (2018-2023)
브라질	1.05	1.17	1.29	1.89	7.90%
멕시코	0.84	0.96	1.09	1.72	9.5%
기타 국가	2.31	2.45	2.58	3.26	4.8%
합계	4.20	4.57	4.96	6.87	6.70%

[출처] MarketsandMarkets, Physical Security Market-Global Forecast To 2023, 2019

▶ 글로벌 시장조사기관인 MarketsandMarkets이 발표한 정보보안시장 보고서에 따르면, 중남미 지역의 정보보안 시장은 2018년 80억 9,000만 달러로 추산되며, 2023년경 143억 5,000만 달러에 이를 전망

표 _ 중남미 지역 주요국 정보보안 시장규모

(단위: 십억 달러)

국가	2016	2017	2018e	2023p	연평균성장률 (2018-2023)
브라질	2.77	3.11	3.46	5.6	10.10%
멕시코	1.9	2.18	2.49	4.59	13.00%
기타 국가	1.6	1.86	2.14	4.16	14.20%
합계	6.27	7.16	8.09	14.35	12.10%

[출처] MarketsandMarkets, Physical Security Market-Global Forecast To 2023, 2019

▶ 글로벌 시장조사기관인 MarketsandMarkets이 발표한 서비스형 보안시장에 대한 보고서에서는 서비스로서의 보안은 클라우드 기반 모델이며, 보안 공급 업체는 클라우드 및 사내 환경에서

엔터프라이즈 네트워크, 애플리케이션 및 데이터를 보호하고 유지 관리함

- 중남미 지역 국가들은 디지털화 및 클라우드 기반 기술 채택이 증가함에 따라 보안 필요성이 증가할 것으로 예상되나 리소스 부족 및 기술 정책을 처리할 전문가 부족으로 서비스로서의 보안에 대해 입문 단계에 있음
- 서비스형 보안 시장규모는 2018년 멕시코의 경우 1억 8,060만 달러 규모로 연평균 성장률(2018-2023) 18.8%로 성장할 것으로 전망하며, 그 외 국가들은 1억 6,260만 달러 규모임

표 _ 중남미 지역 주요국 서비스형 보안 시장규모

(단위: 백만 달러)

국가	2016	2017	2018e	2023p	연평균성장률 (2018-2023)
멕시코	116.7	146.1	180.6	428.0	18.8%
기타 국가	103.1	130.4	162.6	399.0	19.7%

[출처] MarketsandMarkets, Security As a Service Market-Global Forecast To 2023, 2019

▶ 글로벌 시장조사기관인 MarketsandMarkets이 발표한 IoT 보안시장에 대한 보고서에서는 IoT 보안 시장은 연결된 장치의 네트워크를 보호하고 연결된 장치의 위협 및 사이버 공격으로 인한 손실을 최소화하기 위해 제공되는 솔루션 및 서비스가 포함됨

- 중남미 지역은 브라질과 멕시코가 IoT 보급률에서 이 지역의 다른 국가와 비교했을 때 가장 빠르게 성장하고 있어 IoT 보안 시장도 함께 성장함
- IoT 보안 시장규모는 2018년 멕시코의 경우 1억 1,990만 달러 규모로 연평균 성장률(2018-2023) 36.1%로 성장할 것으로 전망하며, 기타 중남미국가들은 1억 10만 달러 규모임

표 _ 중남미 지역 주요국 IoT 보안 시장규모

(단위: 백만 달러)

국가	2016	2017	2018e	2023p	연평균성장률 (2018-2023)
멕시코	73.6	93.8	119.9	560.4	36.1%
기타 국가	61.3	78.1	100.1	468.9	36.2%

[출처] MarketsandMarkets, IoT Security Market-Global Forecast To 2023, 2019

▶ 중남미 시장의 주요 진출 전략은 다음과 같음

- 사이버보안 초기구축모델의 전파 : 페루·엘살바도르·도미니카공화국·과테말라
  - 인터넷침해대응센터 구축운영, 사이버보안 역량강화 등 사이버보안 초기구축모델을 활용한 진출전략을 바탕으로 최초레퍼런스의 확보가 시급한 상황
  - 기획재정부 KSP사업 또는 미주개발은행(IDB, Inter-American Development Bank) 타당성조사 사업 등을 활용한 협력수요 발굴이 필요

가. 멕시코

'18년 GDP(십억달러)	1,224
'18년 인구수(천명)	126,190

■ ITU 글로벌 사이버보안 지수(Global Cybersecurity Index, GCI)

· 2018년 멕시코의 사이버보안 지수는 세계 63위로 하락하였으며, 우리나라와의 격차 심화

국가명	2018		2017		전년대비 증감	
	지수	순위	지수	순위	지수	순위
멕시코	0.629	63	0.660	28	-0.031	-35
대한민국	0.873	15	0.782	13	+0.091	-2

■ ICT 관련 주요 지수

· 멕시코의 전반적인 ICT 발전 수준은 ITU 조사국 175개국 중 중하위권 내에서 하향

지표명	멕시코		한국	
	점수	순위	점수	순위
IMD 국가경쟁력지수(2019)	-	50	-	28
IMD 디지털경쟁력지수(2019)	-	49	-	10
UNCTAD 전자상거래지수(2019)	47.5	95	89.4	19
ITU 글로벌 사이버보안 지수(GCI 2018)	0.629	63	0.873	15
UN 전자정부 지수(2018)	0.681	64	0.901	3

■ ICT 관련 주요 통계 (ITU, 2018년 말 기준)

· 멕시코는 이동통신을 제외한 나머지 통신 및 인터넷 지표 항목 전반에 걸쳐 여전히 낮은 보급률을 유지

항목	멕시코		한국	
	가입자수(천 명)	보급률(%)	가입자수(천 명)	보급률(%)
유선전화	21,361	16.93	25.906	50.63
유선브로드밴드	18,478	14.64	21,286	41.60
이동통신	111,367	93.01	66,356	129.67
인터넷 이용률	65.77%		95.90%	

정보보호 산업 개요

1) 보안 환경

▶ ITU 2018 'Global Cybersecurity Index(GCI)'에 따르면 멕시코의 사이버보안 지수는 0.629로 전 세계적으로는 63위, 미주 국가에서는 미국, 캐나다, 우루과이에 이어 4위를 기록

- 해당 지수는 법적·기술적·조직적 대응·역량 강화 및 국제협력 등 5개 부문의 지수를 종합한 것으로, 멕시코는 2017년 GCI 지수 0.660으로 미주 3위, 전 세계적으로 28위였으나 2018년에는 순위가 현저히 하락함
- 멕시코에는 사이버 보안을 위한 전반적인 국가 관리 로드맵이 부재
- 상업, 산업, 공공 및 개인 정보 보안과 관련된 문제의 증가(2013년~2018년)를 해결하기 위해, 멕시코 정부는 정보 보안에 대한 국가 전략 수립을 위한 전문화된 정보 보안위원회를 설립

표 _ 미주지역 주요국가 GCI

국가명	GCI 지수	지역 순위	글로벌 순위
미국	0.926	1	2
캐나다	0.892	2	9
우루과이	0.681	3	51
멕시코	**0.629**	**4**	**63**

[출처] ITU, Global Cybersecurity Index 2018

▶ 멕시코는 1년 이내에 사이버 공격이 가장 많은 국가로 중남미에서 2위를 차지

- KPMG에 따르면 멕시코의 CEO 중 약 58%가 기업의 사이버 보안 준비에 대해 확신하고 있지 않음
- 멕시코의 사이버 공격은 IoT, 모바일 및 인터넷 보급률 증가 등으로 인해 국가가 취약해짐에 따라 점점 빈번해지고 이로 인한 비용이 증가하는 추세임
- 멕시코의 금융 사이버 범죄도 증가하고 있는 추세로, 멕시코 금융 기관의 60%~70%가 침해 위협을 받고 있으며, 금융 사이버 범죄로 인해 2015년부터 2017년까지 약 1,300만 달러의 손실이 발생

▶ 멕시코 치안 불안으로 보안 용품 시장이 확대될 것으로 전망하며 특히 CCTV, 종합 안전 시스템과 같은

예방 보안 솔루션 시장의 확대가 기대

- 멕시코 내 치안 불안 체감률이 증가하고 있어 주요 범죄 예방을 도와주는 영상보안 시장 및 생체인식, 통합관제 등이 가능한 통합보안솔루션 시장이 성장할 것으로 전망
- 2019년 멕시코 통계청이 조사한 도시 공공안전에 관한 설문조사(Encuesta Nacional de Seguridad Publica Urbana)에 따르면 멕시코에서 치안 불안을 느낀다고 답한 응답자 비율은 74.6%로 2015년 대비 6.7%포인트 증가
- 이와 같은 치안 불안 증가로 인해, 개인 호신용품에 대한 관심도 높아지고 있음

▶ 멕시코 물리 보안시장은 대테러보다는 자국 내 범죄 방지에 더 초점을 두고 있음

- 멕시코 범죄조직은 납치와 상인 대상 현금 갈취 등 다양한 방식으로 수입원을 늘려가고 있으나 공권력이 조직범죄에 대응하는 방법은 제한적
- 이에 따라 사설 경비업체 등 민간 보안시장이 점점 활성화되고 있으며, 2013년 대비 2016년에 멕시코 보안시장 규모는 60%가량 성장
- 상기 기간 동안 수입 규모는 약 37% 증가했으며, 융합보안 부문까지 시장이 확대되고 있는 추세임

2) 인터넷 및 통신 환경

▶ 멕시코 통신 시장은 모바일 및 광대역 부문 주도하에 2005년에서 2007년 사이에 주로 성장했으며, 2008년 이후 글로벌 금융 문제로 인해 성장이 둔화되었으나, 이후 많은 글로벌 시장, 특히 유럽 시장과 비교할 때 강세를 유지하고 있음

- 미국 연방 통신위원회 (Cofetel)가 개발한 통신 부문 생산 지수(ITEL)에 따르면, 2012년 통신 부문은 위성 TV, 국제 장거리 및 모바일 트래픽의 성장에 따라 2010년 10.6%에 비해 12.2% 성장
- 2019년 현재 멕시코의 통신 시장은 Telmex가 주도하는 유선 부문과 자매 회사인 Telcel이 주도하는 모바일 시장으로 여전히 집중되어 있음
- 멕시코 정부는 지배력을 50% 미만으로 낮추기 위해 AT&T의 시장 진입을 장려하는 등 규제 완화 노력을 기울이고 있으며, MVNO의 경쟁적 역할도 확대되고 있음
- 규제 기관이 향후 5G 서비스에 600MHz 스펙트럼을 할당함에 따라 모바일 광대역 부문에서의 급격한 발전이 예상

▶ 유선통신은 수년간 성장이 둔화되었으나, 2015년 이후 유선 전화 밀도는 약 18.4%로 일부 성장이

진행되고 있음

- 멕시코 시티의 가계 전화 밀도는 약 85%인 반면, 치아파스와 같은 주에서는 13%에 불과하여 성장의 여지가 여전히 남아 있음
- 반면 모바일 부문과의 경쟁이 치열한 Telmex의 인프라 우위는 유선 가입자 증가를 계속 제한할 것으로 전망
- DSL 광대역 서비스에 대한 수요가 유선 통신에 대한 수요를 유발하고, 규제 개혁이 새로운 진입 및 투자에 대한 인센티브를 창출한다면, 전화 밀도가 증가할 수 있을 것으로 예상
- 케이블 VoIP가 모멘텀을 얻음에 따라 케이블 광대역이 크게 성장 가능
- 유선통신의 가구 보급률은 2018년 9월까지 약 60%에 도달했으며, Telmex, Axtel, Alestra, Maxcom 및 Marcatel이 이 부분의 주요 사업자로 활동 중임

▶ 최근 인터넷 시장은 멕시코 통신 부문에서 가장 빠르게 성장하는 부문 중 하나가 되었으며, 시장 규모 측면에서 브라질 다음으로 중남미에서 두 번째로 큰 인터넷 시장임

- 광대역 보급 측면에서, 멕시코는 이 지역에서의 보급률이 상대적으로 낮으며 35개 OECD 국가 중 가장 낮은 비율을 차지
- 유선 전화 보급률이 14%를 약간 상회하는 반면, 인구의 30% 이상은 정기적으로 인터넷을 사용 중
- ISP 서비스를 제공하기 위해 수년 동안 등록한 350여 개 업체와 달리 현재 약 20개의 주요 ISP만이 운영되고 있음
- Telmex/Prodigy는 여전히 주요 통신 업체이자 ISP의 로컬 회선 및 상호 연결 링크를 제공하는 주요 공급 업체로서 활동 중임
- Telmex는 신규 사업자로 인해 시장 점유율은 점차 감소하고 있으나 가입자의 약 73%는 여전히 DSL 시장을 차지하고 있으며, 2018년 3월 기준으로 유선 광대역 시장에서 53%의 점유율을 보이고 있음
- Cablemas와 Cablevision을 통합한 Grupo Televisa는 22.7%의 점유율을 가지고 있으며, Megacable은 15.5%로 그 뒤를 잇고 있음

표 _ 인터넷 사용자 및 연간 변화 (2016~2018)

연도	사용자 수	점유율
2016 (e)	64,500,000	52.4%
2017 (e)	66,500,000	54.3%
2018 (e)	68,100,000	56.1%

[출처] BuddeComm based on regulator and INEGI data

그림 _ 유선 브로드밴드 가입자 (2003-2017)



[출처] BuddeComm based on regulator and ITU data

▶ 멕시코는 브라질 다음으로 중남미에서 두 번째로 큰 모바일 시장을 가지고 있으며, 모바일 가입자 수는 2000년 중반 유선 사용자 수를 넘어섬

- 2002년 Telefonica Moviles Mexico (TEM Mexico)가 Movistar라는 브랜드로 운영되면서 모바일 경쟁이 점차로 증가하기 시작함
- 2019년 초 모바일 보급률은 94%에 도달했으며, 가입자의 84%가 선불 서비스에 가입되어 있음
- 멕시코 모바일 시장에는 현재 Telcel, Movistar 및 AT&T Mexico의 3개 주요 사업자가 시장의 대부분을 점유하고 있음
- Telcel은 시장 점유율이 약 65%인 확실한 시장 리더이며, Movistar는 약 23%로 2위, AT&T Mexico가 12%의 점유율로 3위를 기록
- 모바일 가입자는 3G에서 4G LTE로 점차 이동하고 있으며, 이러한 이동은 약 2020년부터 5G 플랫폼으로 유사하게 진행될 것으로 예상

표 _ 주요 사업자에 따른 모바일 시장 점유율

연도	Telcel	Movistar	AT&T Mexico
2016	64.9%	23.3%	10.7%
2017	64.2%	21.4%	13.0%
2018 (9월)	63.3%	21.0%	14.3%

[출처] BuddeComm based on industry and regulator data

그림 _ 모바일 가입자 및 점유율 (2007-2019)



[출처] BuddeComm based on company and State Statistics data

▶ 4G LTE 인프라에 대한 상당한 투자에 따라 LTE 네트워크 가입자 수는 꾸준히 증가하는 추세임

- 2018년 3/4 분기 LTE 네트워크는 모바일 데이터 트래픽의 70%를 차지했으며 2G는 0.3 %에 불과
- Telcel은 2012년 말 9개의 도시를 포함하여 서비스를 시작했으며, 2013년 5월까지 인구의 약 65%를 차지하는 26개 도시로 확장
- Ericsson은 제어 신호 및 트래픽을 처리하는 주요 장비 공급 업체로서 2018년 3월 LTE 서비스보다 최대 10배 빠른 속도로 데이터를 제공할 수 있는 '4.5G' 서비스를 시작
- Movistar는 2012년 말 서비스를 시작했으며, 2018년 말까지 300개 도시로 LTE 인프라의 범위를 확장하기 위해 2억 2,500만 달러를 투자

▶ 5G

- GSMA 연구소에 따르면, 5G는 2025년경 중남미 인구의 40%에게 서비스를 제공할 것으로 전망
- 2016년 이후로 현지 통신업체들은 브라질, 멕시코, 아르헨티나, 콜롬비아, 칠레, 페루 등의 국가에서 5G를 실험 중에 있으며, 이 중 멕시코는 가장 빠른 시기인 2020년에 상용화를 할 것으로 예측
- 멕시코에 5G 네트워크를 구축하는 것은 인구가 3%인 제한된 지역에서만 가능하나, 2025년에는 14%, 약 1,800만 개의 연결이 채택될 것으로 예상
- 멕시코는 5G 주파수 계획을 발표하였으며, 이는 스펙트럼을 3.6GHz로 재정렬하고 현재 해당 밴드의 주요 세 업체인 Telmex, Axtel, AT&T가 향후 5G에서 사용이 용이하도록 함
- 이를 통해 멕시코는 3.4GHz 및 밀리미터 주파수와 같은 5G 대역의 스펙트럼 개발에 대한 확립된 로드맵을 가진 최초의 중남미 국가가 될 것으로 전망

정보보호 시장 현황

1) 시장 규모

시장 개요

▶ 중남미 사이버 보안 시장은 전체적으로 CAGR 12.3%로 2023년까지 206억 5,000만 달러로 증가할 것으로 예상

- 2016년 중남미는 사이버 보안 시장에서 전 세계 매출의 7.9%를 차지
- 현재 취약한 사이버 보안 인프라를 가진 중남미 시장은 대부분의 보안 소프트웨어 제공 업체들에게는 중요한 시장으로 부각
- 중남미는 인구 증가와 함께 인터넷 연결이 증가하고 지역 경제의 디지털화가 발전함에 따라, 2020년까지 이 지역에만 6억 대 이상의 연결된 스마트 폰이 있을 것으로 추정되며 이로 인한 보안 시장이 확대될 것으로 예측

▶ Europole의 보고서에 따르면, 멕시코의 조직화된 사이버 범죄는 민간 및 공공 기관뿐만 아니라 민간인들에게도 위협을 가하고 있으며, 멕시코는 브라질 다음으로 중남미에서 가장 많은 사이버 공격을 당하고 있음

- Symantec은 멕시코를 이메일을 통해 유포된 악성 링크가 가장 많은 10개 국가 중 하나로 선정했으며, 아일랜드, 호주, 뉴질랜드, 브라질, 노르웨이 및 영국에 이어 7위를 차지
- McAfee는 멕시코에서 사이버 범죄의 재정적 영향이 연간 30억 달러로 증가했다고 추정

▶ 미국 상무부는 멕시코 중소도시를 중심으로 하여 보안 시장 규모가 증가할 것으로 전망

- 멕시코 보안시장은 점차 융합보안의 방향으로 변화하고 있으며, 향후 GPS, 바이오인식, 인터넷 솔루션과 결합해 높은 성장이 있을 것으로 예측
- 민간보안회사협회(CNSP) 연구에 따르면, 2017년 민간부문에서 보안에 지출하는 총금액은 GDP의 약 1.2%를 차지
- 산업분야 중 특히, 물류 분야에서 큰 수요가 예상되며, 상품의 운송과정을 추적하고 도난을 방지할 수 있는 GPS 연계 시스템과 장비에 대한 수요는 지속해서 발생할 것으로 예측
- 전통적인 출입통제 시스템인 개인 ID카드를 이용한 방식보다는 홍채, 지문을 활용한 출입통제시스템의 수요가 증가할 것으로 전망

시장 규모 및 전망

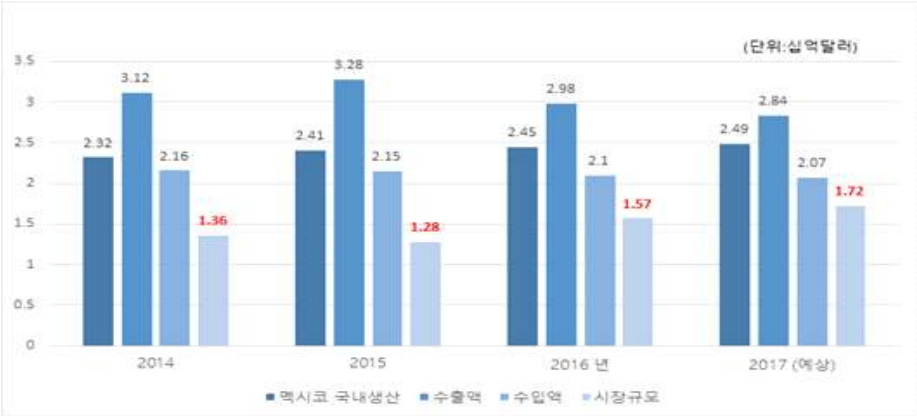
▶ 2019년 중남미 지역의 정보보호 시장규모는 119억 달러로 추산

- 시장조사기관 MicroMarket Monitor에 따르면, 중남미 지역의 IT보안 시장 규모는 2014년부터 2019년까지 연평균 17.6%의 성장률과 119억 달러 규모로 전망
- 소프트웨어연합(BSA)는 2015년 멕시코 내의 복제 소프트웨어의 규모는 약 9억 8,000만 달러 규모로 추정되고 있으며, 불법 복제를 통해 전파되는 소프트웨어가 멕시코 IT보안 분야의 주요한 위협이 되고 있다고 평가

▶ 멕시코의 전체 보안시장은 정부, 민간기업, 가정 등 다양한 분야에서 수요가 증가할 것으로 전망

- 최근 최신보안 기술이 멕시코 내에서 확대됨에 따라 프리미엄 보안 시장 규모가 확대되는 추세임
- 미국 상무부는 2017년 멕시코 보안시장 규모를 약 17억 달러로 추산하며 향후 시장규모가 더욱 확대될 것으로 예상

그림 _ 멕시코 정보보호 시장의 규모 (2014-2017)



[출처] Export.gov

2) 분야별 현황

정보보안 제품 및 서비스 시장

▶ 2018년 CNBV 은행 및 증권 규제 기관과 미국 정부 기관이 공동 연구를 수행한 사이버 보안 사고로 인한 대응 및 복구 노력과 관련된 멕시코의 비용이 1억 7,100만 달러에 이르는 것으로 조사

- 전국의 모든 은행이 연중 다양한 종류의 사이버 사건을 겪었으며, 주로 악성 코드와 피싱이 사이버 보안 사고를 이루고 있음
- 핀테크 회사조차도 사이버 범죄자들에 의해 타격을 입었으며, 지난 1년간 1,300만 달러의 손실이 발생

▶ 미국 Eport.gov에 따르면, 멕시코 시장에서의 보안 관련제품의 중요한 경쟁요소로는 ▲제품 내구성 ▲용이한 유지관리 ▲사후서비스 네트워크가 중요함을 언급

- 멕시코는 지역간 인프라 및 공공서비스 수준의 편차가 크며, 이로 인해 보안이 상대적으로 취약한 지역에서의 보안장비 및 솔루션에 대한 수요가 높은 것으로 파악
- 현지에서 사후서비스에 대한 접근이 용이하고 손쉬운 이용이 보장되는지 여부가 제품에 대한 가장 중요한 구매요소로 작용

▶ 2014년에 구현 된 Prosoft 3.0과 같은 민간 부문과 공공 부문 이니셔티브에 의해 ICT 시장은 2024 년에 580억 달러에 이를 것으로 추산

- 멕시코 기업은 데이터 분석 및 사이버 보안이 크게 성장할 것으로 예측되고 있으며, 제조업체는 소프트웨어 및 서비스에 대한 수요를 증가시켜 하드웨어 손실을 상쇄하려는 추세
- 2015년부터 2021년까지 소프트웨어 산업의 CAGR은 9.4%로 추정
- 공공 및 민간 부문의 정보에 대한 의존도가 높아짐에 따라 통합 보안 및 컨설팅에 대한 요구가 증가

그림 _ 멕시코에서 총 보안 소프트웨어 판매 현황 및 전망 (2015~2021) (단위: 십억 페소)



[출처] CYBERSECURITY MARKET ANALYSIS, PRO MEXICO, 2018

그림 _ 멕시코에서 총 보안 서비스 판매 현황 및 전망 (2015~2021) (단위: 십억 페소)



[출처] CYBERSECURITY MARKET ANALYSIS, PRO MEXICO, 2018

물리보안 제품 및 서비스 시장

▶ 2017년 멕시코 산업 수치에 따르면 보안 시스템 및 솔루션의 판매는 전체 경제에서 2% 성장을 훨씬 능가하여 10% 이상 증가함

- 최근 멕시코에서 폭력 범죄와 지속적인 공급망 위협으로 인해 안전과 보안은 거의 모든 가정 및 조직 예산의 일부가 됨
- 2018년 초에 진행되고 있는 안보 악화는 국가의 경제 발전을 제한할 수 있는 가장 중요한 요소로 강조됨

▶ 멕시코 민간 부문 회사는 물리보안 장비에 대한 총 지출의 10~12%를 소비하는 것으로 추정

- 이 비용은 주로 견고한 경보 시스템, 직원/계약 업체/방문객 식별 도구, CCTV 시스템 및 주변 보호 시설을 강화하고, 특히 물류 산업에 있어서 화물 도난 감시, GPS 모바일 추적 시스템 등에 사용
- 최근 비즈니스 조직인 COPARMEX는 회원의 40%가 안보 관련 범죄의 희생양이 되어 범죄와 불안에 대한 보다 강력한 정부의 조치를 요구
- 물리적 안전 및 보안 부문에는 공공 보안, 개인 보호, 주거 보안, 산업 안전, 기업 시설 및 인프라 보호 (액세스 제어, ID, 경계 보안) 및 다양한 솔루션 및 시스템에 사용되는 장비, 솔루션 및 서비스가 포함

표 _ 멕시코 안전 및 보안 제품 및 서비스 시장 규모 추정치

(단위: 억 달러)

	2015년	2016년	2017년	2018년(e)
총 현지 생산	2.41	2.45	2.49	2.53
총 수 출	3.03	3.07	3.14	2.92
총 수 입	2.06	1.98	1.98	2.02
총 시장 규모*	1.44	1.36	1.33	1.63

[출처] Global Trade Atlas 2018 / June

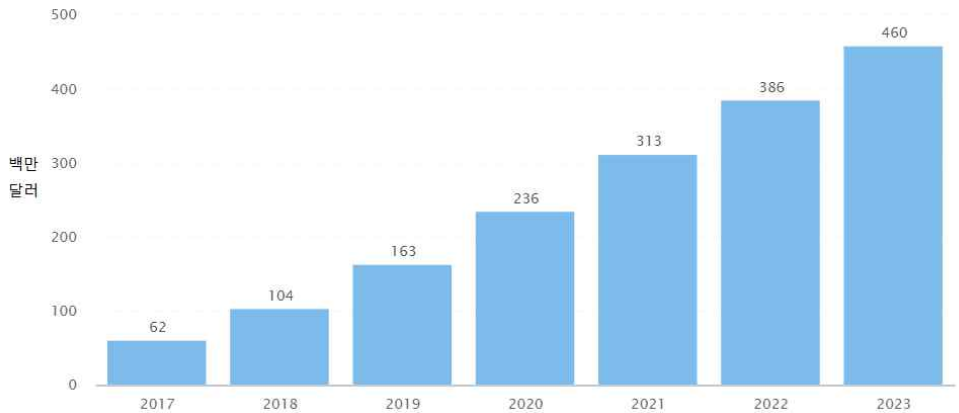
* 총 시장 규모 = = (총 현지 생산 + 수입)-수출

※ 참고: 안전 및 보안 장비 및 서비스 부문은 일부 국방 제품을 포함한 여러 부문으로 구성

▶ 스마트홈 보안 부문의 수익은 2019년 1억 6,300만 달러이며, 29.6%의 연간 성장률(CAGR 2019-2023)로 2023년까지 4억 6,000만 달러에 이를 것으로 예상

- 스마트홈 보안 부문은, 스마트홈과 관련된 감시 제품, 위험 모니터링 장비 및 건물 네트워크의 액세스 제어 장치/서비스가 포함
- 2019년 가계 보급률은 2.2%이며 2023년에는 8.3%에 도달할 것으로 전망
- 보안 부문의 스마트홈 당 평균 수익은 2019년 현재 256.28 달러임

그림 _ 스마트홈 보안 수입 전망 (2017~2023)



[출처] Statista, September 2019

▶ 모바일 동영상 감시 시스템은 안전 및 보안 목적으로 산업 분야에서 주로 사용되고 있으며, 특히 향후 정보보안과 융합하여 물류 산업에 활용도가 높을 것으로 전망

• MarektsandMarkets의 'Mobile Video Surveillance Market; Global Forecast to 2023'에서는, 2016년 멕시코 시장의 규모는 31억 4,000만 달러에서 2023년에는 62억 달러 규모로 성장할 것으로 전망

그림 _ 모바일 동영상 감시 시스템 시장 규모



[출처] MarketsandMarkets, Mobile Video Surveillance; Global Forecast to 2023

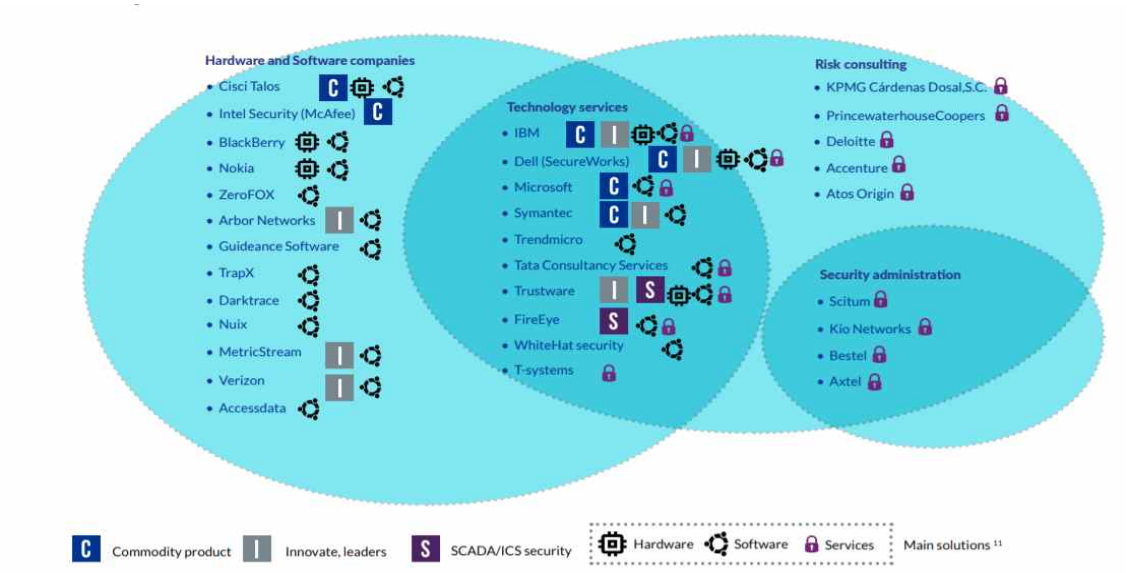
3) 주요 사업자 현황

시장 특성 및 경쟁 강도

▶ 멕시코의 사이버 보안 부문은 글로벌 대기업이 가장 큰 시장 점유율을 가지고 있으며 단편화되어 있음

- 사이버 보안 솔루션과 관련된 주요 하위 부문은 기술 서비스, 하드웨어 및 소프트웨어 제공 업체, 보안 관리 서비스 및 위험 컨설팅으로 구성
- 멕시코 시장의 주요 업체로는 IBM, Microsoft, Symantec, Nokia, BlackBerry, Trustwave, Dell (SecureWorks), ZeroFOX, Cisco Talos, Tata Consultancy Services, Accenture, PWC, Bestel, Axtel, Scitum, Kio Networks, Verizon 등이 시장을 형성
- 전반적으로 멕시코의 ICT 부문은 4,000개 이상의 현지 및 글로벌 기업으로 구성되어 있음
- Promexico에 따르면 멕시코의 사이버 보안 시장은 Cisco 및 Symantec이 주도하고, FireEye, ProofPoint, Fortinet 및 Palo Alto Networks 등의 업체가 SaaS의 하위 세그먼트를 계속 확장

그림 _ 멕시코 보안 시장 분류 및 주요 사업자

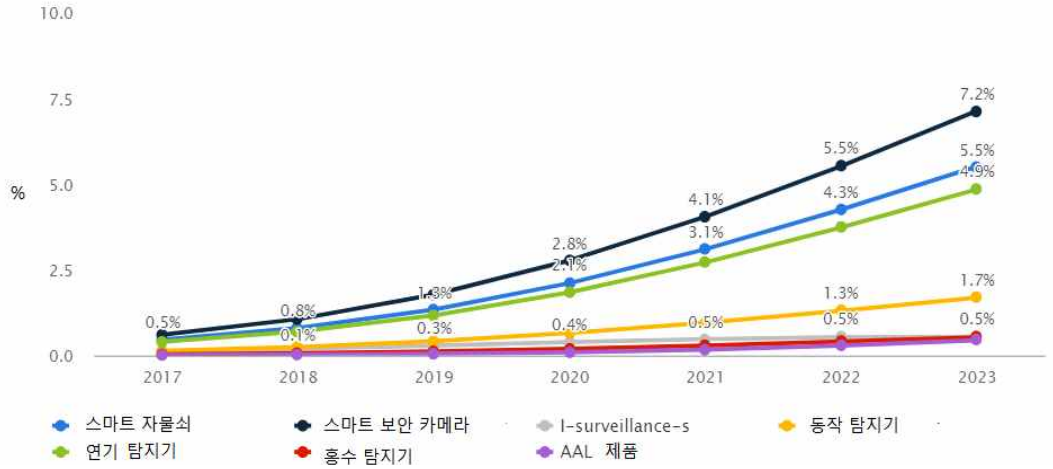


[출처] CYBERSECURITY MARKET ANALYSIS, PRO MEXICO, 2018

▶ 스마트홈 보안 부문은 도난 방지/감지, 화재 또는 누수, 비상 전화 및 액세스 제어와 같은 위험에 대한 경보을 대상으로 하는 시장임

- 주요 성장 제품은 스마트 잠금 장치 및 스마트 보안 카메라로서, 여러 산업의 업체들이 시장에서 경쟁 중임
- 기존 보안 회사(ADT 등) 및 기술 스타트 업(Canary, Alarm.com 등) 외에도 미디어 회사 및 연결 공급자(AT&T 또는 Comcast)는 전송해야하는 많은 양의 데이터로 인해 중요한 역할을 하는 사업자임

표 _ 스마트홈 제품 점유율



[출처] Statista, September 2019

주요 사업자 현황

▶ 정보보안 관련 사업자

- TrapX : 미국 캘리포니아 주에 본사가 있으며, 사이버 기만 기술의 선구자이자 글로벌 리더 업체. TrapX의 DeceptionGrid 솔루션은 지능형 사이버 공격과 사람이 진행하는 공격을 실시간으로 신속하게 탐지하여, 해당 공격을 속임으로써 실패하도록 유도. Quadrant Knowledge Solutions는 전세계 기만 기술 시장에서 TrapX Security를 '2018년 올해의 회사'로 인정했다고 발표
- Darktrace : 2013년 영국 캠브리지에서 설립된 정보보안 회사로서 캠브리지와 샌프란시스코에 본사를 두고 있으며, 영국 무역 및 투자가 주도하는 무역 업무에 참여하여 라틴 아메리카에서의 입지를 더욱 발전시키고 있으며, 멕시코 국가 사이버 방어력을 강화하기 위해 경찰, 군대, 정보 서비스
- Tata Consultancy Services(TCS) : 뭄바이에 본사를 둔 인도 업체로서 46개국 149곳에서 IT 서비스 및 컨설팅을 주로 제공하고 있으며, Tata Consultancy Services de México는, 2003년 멕시코 시티에서 사업을 시작했으며 고급 IT 서비스, 컨설팅, 테스트, 소프트웨어 개발, 비즈니스 프로세스 아웃소싱, 컨택트 센터, 인프라, 산업 및 엔지니어링 서비스를 위한 IT 솔루션 등을 제공
- Trustwave: 1995년 미국 시카고에서 설립된 정보 관리 보안 서비스 및 클라우드 컴퓨팅을 주로 제공하는 글로벌 업체로서, 2019년 8월 Trustwave와 대규모 정보 기술 통합 업체인 Grupo Tecno는 멕시코의 기업 및 기타 기관에 Trustwave 관리 보안 서비스 및 사이버 보안 기술을 제공하기 위해 제휴

▶ 물리보안서비스 및 장비제공 사업자

- ADT : 1874년에 설립된 플로리다에 본사를 두고 있는 세계 최대 규모의 물리보안 솔루션 공급 업체 중 하나로서, 주로 보안 모니터링 및 관련 서비스, 설치 및 기타 서비스를 제공
- Canary : 2012년 미국 뉴욕에서 설립된 스타트업으로서 스마트 폰으로 연결하는 홈 보안 장치를 제공하고 있으며, 민간 비디오 업계에서 2014년 Google이 인수한 Netgear and Nest에 이어 시장을 주도
- Alarm.com : 2000년 설립된 버지니아에 본사를 둔 미국 업체로서, 원격 제어, 홈 자동화 및 모니터링 서비스를위한 클라우드 기반 서비스를 제공하며, 2017년 현재 2억 3,360만 달러의 매출과 550만 명의 가입자 수를 기록

4) 주요 동향 및 이슈

▶ 멕시코 국가은행증권위원회는(National Banking and Securities Commission, CNBV)는 사이버보안을 위한 금융기관간 정보공유를 제안(2017년 10월)

- CNBV는 금융 기관에 대한 사이버 공격에 대응하기 위해 모든 관련 금융 기관이 해당 공격에 공동으로 대응할 수 있도록 정보를 공유할 것을 제안
- 사이버 범죄의 기술적 향상과 고도화에 따른 피해를 줄이기 위해 사이버 공격 관련 정보를 실시간으로 공유함으로써 동일한 위험 또는 취약성에 노출된 다른 금융기관이 대응에 필요한 정보가 제공되어 한다고 주장
- CNBV의 자료에 따르면, 멕시코 내에서 발생하는 금융기관의 정보보안 사고의 40% 가량이 전자금융 또는 신용카드 정보를 노린 피싱(phishing)시도로 집계

▶ Microsoft는 2017년 2월 멕시코시티에 새로운 사이버보안 센터를 개설한다고 발표

- 멕시코 지역의 Microsoft 제품 사용자에 대한 일반적인 서비스 제공을 목적으로 설립
- 또한 멕시코 연방경찰과의 특별 협약을 통해 멕시코 지역에서 발생하는 사이버범죄에 대한 조사 참여와 지원업무를 담당

5) 정보보호 스타트업 시장 현황

시장 규모

▶ 멕시코는 세계 핀테크 도입 7위 국가로서 남미에서 Fintech 스타트업에 대한 투자가 압도적으로 높음

- 2017년 기준 멕시코의 핀테크 기업은 개인간 대출(23%), 간편송금 및 결제(22%), 기업자산관리(15%), 개인자산관리(9%) 등의 서비스를 주로 제공
- 2018년 3월, 핀테크 법안이 통과되어 크라우드펀딩, 결제, 암호화폐 등의 분야에 대한 규제 안정성을 확보하여 스타트업이 법적 테두리 내에서 안정적으로 활동할 수 있는 기반을 마련
- 전통적인 금융기관과 스타트업 간 공동 응용 프로그램 인터페이스(API)를 통해 고객 금융정보의 공유를 허용하는 것이 가장 큰 특징

▶ 통신개혁에 따른 통신망 확충을 기반으로 2020년까지 멕시코인의 63%가 인터넷망(3G, 4G)에 접근성이 강화되며, 그 중 55%가 Fintech를 적극 활용할 전망

- 오프라인 ATM 기기 활용빈도 수가 급격히 낮아지는 반면 Fintech 활용 상품 및 서비스 다양화 추세
- 현재 멕시코 정부는 국가간 핀테크 서비스의 확대를 위한 협약 등에 참여하지는 않았으나, 중요성은 인식하고 있음

주요 사업자

▶ 멕시코시티는 남미의 스타트업 투자 허브로서, 실리콘 밸리의 대표적인 글로벌 벤처투자사인 500 Startups, Mountain Nazca 등의 기업이 진출

- Avalancha Ventures, Jaguar Ventures, Investo 등 멕시코시티에 기반을 둔 다양한 투자사가 남미 전체를 대상으로 스타트업 설립 초기 단계부터 활발히 투자
- 멕시코시티에서 시작된 자동차 공유 애플리케이션인 'Aventones'는 남미에서 가장 성공적인 차량공유 서비스로 성장했으며, Cornershop(식료품 배달 서비스), Clip (카드결재단말기) 등 성공사례를 창출

주요 동향 및 이슈

▶ 최근 멕시코 중앙은행이 발의한 'Fintech 규제법 'catch-22'가 시행됨에 따라 현지 핀테크 스타트업 201곳이 폐쇄 위기(2019년 8월)

- 멕시코의 핀테크 규제법 시행에 따라 현지 핀테크 스타트업 중 57% 이상이 당국의 사업 허가를 받기 위해 노력 중
- 규정 준수를 위해 요구되는 비용이 3만 5,000 달러에 육박한다는 것이 가장 큰 문제이며, 또한 해당 법안은 현지 핀테크 기업들에 연간 10만 달러 이상의 영업이익을 요구하고 있으며 이는 대다수 스타트업들이 달성하기 힘든 조건임
- 해당 규정에 따르면, 핀테크 기업은 암호화폐 보유, 거래 등이 금지

정보보호 정책 및 기관 현황

1) 관련 법령 및 정책

▶ 멕시코 법에는 "사이버 범죄" 및 "사이버 보안"이라는 용어에 대한 정의가 없으며, 현재 사이버 보안과 관련된 국제 표준을 채택하지 않음

- 이와 관련해서, 연방 형사법(Federal Criminal Code)은 전자 수단을 사용하여 사이버 범죄로 식별될 수 있는 전자 수단을 통해 저지른 불법 행위를 규제하며, 주로 금융 범죄, 정보 보안 및 테러와 같은 기타 범죄에서의 기술 사용에 관한 내용을 다루고 있음
- 기관(조직)이 사이버 위협으로부터 데이터 및 정보기술 시스템을 보호하기 위해 구현해야 하는 최소한의 보호조치는 규정되어 있지 않으나, 개인정보 보호법에 따라 데이터 컨트롤러는 정보의 손상, 손실, 변경, 파괴, 사용 또는 무단 액세스 혹은 처리로부터 정보를 보호하기 위해 다양한 기술적, 물리적 및 조직적 조치를 구현해야 함

▶ 특정 산업이 고객 데이터를 보호하기 위해 채택해야 하는 특정 필수 보안 조치가 존재

- 은행법 및 규정에 따르면 은행은 전자 은행 거래에서 특정 보안 조치를 구현해야 하며 거래의 규모와 성격에 따라 몇 가지 비밀번호를 사용해야 함
- 멕시코에는 직원 및 이사의 사이버 보안 책임 또는 부채와 관련된 특정 법률이 없음에도 불구하고, 데이터 보호법에 따라 개인정보를 처리하는 모든 개인 또는 조직은 조직의 대표자가 될 데이터 보호 책임자를 임명할 의무가 있음

▶ 개인정보보호법

- 2011년 7월 멕시코 최초로 개인정보보호 관련 법안이 마련되었으며 공공의견 수렴을 거쳐 같은 해 12월 최종안 승인 및 발효
- 개인정보보호에 관한 연방법은 '개인 당사자가 보유한 개인 정보의 보호에 관한 연방법'에 따라, 개인정보를 처리하는 모든 기관과 조직은 데이터 보호책임자를 임명하고 동 법률이 요구하는 규정의 준수를 요구하고 있음
- 동 법령은 국제 협약에 따라 멕시코 지역 내 또는 멕시코 이외의 지역이라 하더라도 실질적으로 멕시코 법률의 적용을 받는 기관이나 조직의 관할이라고 인정되는 경우에는 적용
- 개인정보보호법의 내용은 크게 ▲이용자의 동의 ▲고지 의무 ▲개인정보 유지 ▲제 3자와의 정보 공유 등으로 구분

▶ 연방 형사법

- 연방형사법은 정보보안과 물리보안 전 영역에서의 부적절한 위협과 위해를 초래하는 각각의 행동들과 관련하여 별도로 규정된 장들이 명문화되어 있으며, 악의적으로 이를 위반하는 경우에 대한 형사 처벌의 근거를 제공
- 정보보안과 관련한 항목으로서는, 온라인상에서 타인의 정보를 도용하는 경우 또는 해킹 등의 방법으로 데이터나 자산에 대해 손상을 가하는 경우에 오프라인상에서의 물리적인 공격과 마찬가지로 형사 처벌 근거를 제공

▶ 금융에 관한 법률

- 신용카드 또는 그 안에 포함된 정보를 도용하거나 영향을 끼치는 등의 금융상품과 관련한 불법행위를 제재하는 내용
- 타인의 신용카드 정보를 불법적으로 도용하는 경우, 정보보호에 관한 규칙을 위반한 것으로 보고 3년에서 9년 사이의 징역형을 부과하는 규정을 두고 있음

▶ 통신법

- 정보통신사업자에게 요구되는 개인정보, 위치정보 및 통신내역에 관한 정보에 관한 규칙과 위반사항에 대한 내용을 정의

2) 담당기관

▶ 멕시코 정보보안정책은 정보통신기술국 (Direccion General de Computo y de TIC) 산하의 정보보안과(Subdireccion de Seguridad de la Informacion)에 의해 주도되고 있으며, 정보보안과는 산하에 컴퓨터 전문가 그룹인 UNAM-CERT 정보보안사고 대응팀을 운영하고 있음

▶ 정보보안과(Subdireccion de Seguridad de la Informacion)

- 정보통신기술국(General Directorate of Computing and Information and Communication and Technology) 산하기관으로 ▲정보보안사고 대응조직 운영 ▲정보통신 보안전문 인력 양성 ▲정보통신 분야 보안정책 수립을 담당

▶ UNAM-CERT 정보보안사고 대응팀(UNAM-CERT Equipo de Respuesta a Incidentes de Seguridad Informática)

- 정보보안과 산하기관으로서 컴퓨터 보안전문가들로 구성되어 있으며 컴퓨터 보안사고 대응 업무를

담당

- 일반적인 컴퓨터 보안사고 대응 처리뿐만 아니라 피싱 사기와 같은 광범위한 사이버 범죄로 인한 피해에 대한 조치도 담당

기관명칭	관련 분야	상세 정보
Mexico Unido Contra la Delincuencia (MUCD)	보안	- 범죄 예방·치안 관련 프로그램 개발 등을 촉진하고 범죄 피해자에게 법적·심리적 서비스를 제공하는 비영리 민간단체
Consejo Nacional de Seguridad Privada (CNSP)	보안	- 보안 서비스와 제품을 제공하기 위한 민간보안회사들의 협회 - CCTV, 위치 정보 시스템, 개인 보호 장비, 안전 제품 관련 제품 제공

3) 규제 및 인증제도

▶ 멕시코 계측과 표준에 관한 연방법 (The Mexican Federal law on Metrology and Standardization)은 멕시코의 적합성 체계를 강제인증인 NOM (Normas Oficiales Mexicanas)과 자율 인증인 NMX (Normas Mexicanas)로 정의

- 강제인증인 NOM 품목에 해당하는 경우는 반드시 NOM 인증을 득해야 멕시코로 통관 및 판매가 가능
- NOM과 NMX에 적합함을 나타내는 인증은 인가된 기관에서 발급되어야만 함

표 _ NOM 인증과 NMX 인증

구분	주요 내용
NOM (Norma Oficial Mexicana)	- 멕시코 강제 규정 (Mexican Regulation) - 국가 자문위원회 (National Consultative Committees)에서 제정 - 관련 정부 부처에서 공표
NMX (Mexican standards)	- 품질 적합성을 보장하기 위한 자율 인증 - 국가표준 기구나 기술 위원회를 통해 자체적으로 제정하는 규격 - 관련 국가 표준 기구 혹은 SE (경제부)를 통해 공표됨

[출처] expertcenter.go.kr

▶ NOM의 인증 대상품목인지 여부를 정확히 판단하기 위해서는 제품의 HS code 정보와 함께 관련 기관으로 제품정보를 보내어 확인하는 것이 가장 정확

- 인증 대상 품목 중 전기전자 제품, 정보, 통신기기 등의 제품은 ANCE와 NYCE가 담당하고 있으며 각 기관에서 담당하는 관리 품목을 통해 대상 제품을 판단할 수 있음

▶ NOM의 관련 법규는 1992년 이전에는 연방정부가 표준제정, 인증, 인가 업무를 모두 관할하였으나, 1993년 10월부터 신규 멕시코 계측과 표준에 관한 연방법(The Mexican Federal law on Metrology and Standardization)에 의거하여 제 3자 표준 제정을 위한 규격 개발기구들(SDOs)과 인증기관(CBs)들이 관여하게 됨

- 과거에는 NOM 제도만을 시행하였으나 1992년부터 멕시코 계측과 표준에 관한 연방법(The Mexican Federal law on Metrology and Standardization)에 따라 멕시코의 적합성 체계를 강제인증인 NOM (Normas Oficiales Mexicanas)과 자율 인증인 NMX (Normas Mexicanas)로 정의하고 해당 제품의 수출, 통관에 적용

▶ NOM 인증 수행기관으로는 ANCE와 NYCE가 있음

- ANCE (Asociacion de Nomalizacion y Certificacion A.C.) : ECEE CB Scheme의 Member Body이며 CBTL로 지정받았으며, 세계 각국의 유사 기관과의 상호인정협력을 맺고 있으며, 전기전자 제품 및 가스제품에 대한 규격 개발 및 인증 수행
- NYCE (Normalizacion y Certificacion Electronica A.C.): 인증 및 국가 표준의 개발, 멕시코 내 표준(NOM, NMX) 및 국제 표준 (ISO, IEC) 간의 적합성 평가 등의 업무를 수행하며, 전자 제품 및 통신, IT 기기를 위한 규격 개발 및 인증을 담당

4) 최근 정책 동향 및 이슈

▶ 2018년 3월 금융 기술 규제법 (멕시코 Fintech 법)이 도입

- 해당 법 가운데에서도 '가상 자산'(암호 화폐)에 관한 운영을 규제하고 ▲Fintech 기관 (FTI) ▲집단 금융 기관 (군중 자금 지원 기관) ▲전자 지불 자금 기관에 대한 규제를 도입
- 동 법은 징역에 의해 처벌될 수 있는, ▲FTI 고객의 자산인 자원, 전자 지불 자금 또는 가상 자산을 사용, 입수, 양도 또는 기타 방식으로 처리하는 행위 ▲장비, 전자, 광학, 정보 또는 금융 기관의 기타 기술 수단에 대한 무단 액세스 등과 같은 사항을 규제

▶ 2018년 9월 멕시코는 지난 20년 이상 발효됐던 북미자유무역협정(NAFTA)을 대체하는 '미국-멕시코-캐나다 협정 (The United States-Mexico-Canada Agreement, USMCA)'을 맺음

- 규제 및 규정 준수 중심의 보안이 동작하지 않는다는 고객과 업계의 의견을 포함한 사이버 보안 관련 조항 신설
- 동 협정에서는 실제로 NIST 프레임 워크에서 식별, 보호, 탐지, 응답, 복구의 5가지 핵심 기능을 포함하는 위험 기반 사이버 메카니즘을 요구
- USMCA는 디지털 서비스와 관련된 비관세 무역 장벽에 대해 ▲거래 구역 내에서 데이터가 자유롭게 흐를 수 있도록 보장 ▲데이터 저장의 사용을 제한하거나 현지화 요구 사항을 처리 ▲상호 운용 가능한 데이터 보호 메커니즘의 개발을 촉진 ▲정부가 시장에서 기술을 판매하기 위한 전제 조건으로 소스 코드를 요구하는 능력을 제한하는 등의 일련의 중요한 보호 조치를 확립
- 이러한 새로운 디지털 거래 조항의 포함으로 사이버 보안 제품 및 서비스를 위한 통합 시장의 개발이 촉진될 것으로 전망

5) 정보보호 스타트업 관련 정책 동향

▶ 멕시코는 남미 주요국 중에서 스타트업 투자가 활발한 편이며 정부의 적극적인 지원책, 스타트업 투자허브 및 높은 서비스 접근성이 성장 기반으로 나타남

- 2013년 정부는 스타트업 인큐베이터인 INADEM를 경제부 산하에서 독립기관으로 편성, 기업가, 소기업 및 스타트업 등을 대상으로 3,400만 달러를 지원하여 6,000여개의 기업과 73,000여개의 일자리를 창출
- 2016년 9월, 'Ley General de Sociedades Mercantiles ' 개정을 통해 연매출 30만달러 이상의 기업은 24시간 온라인으로 무료 법인 설립 가능

융합보안 시장 및 정책 동향

1) 융합보안 시장 현황

스마트시티

▶ 멕시코시티와 과달라하라, 스마트시티 분야 협력을 위한 MOU 체결

- 2019년 8월초 Global Initiative for Inclusive ICTs(G3ict)가 멕시코 시티에서 개최된 전세계 도시의 디지털 포용성(inclusivity) 평가 행사에서 멕시코의 양대 대도시인 멕시코 시티와 과달라하라가 스마트시티와 포용성 증진 분야에서 협력하기 위한 MOU를 체결

자율주행차(양자암호통신, V2X 등 포함)

▶ 드론을 이용한 범죄 예방프로그램 가동

- 2016년 멕시코의 스타트업 Dronix는 자동차 서비스 및 보안·경비 업체인 LoJack과 함께 범죄 예방을 위한 파트너십을 형성
- 해당 파트너십을 통해 Dronix의 드론 무리가 LoJack의 장비를 갖춘 자동차의 도난을 방지하기 위해 멕시코시티를 순찰

사물인터넷(IoT)

▶ 2016년 멕시코 IoT 관련 시장규모는 33억 달러 도달

- 멕시코의 사물인터넷 시장은 아직 초기단계이나, 주요 이동통신 사업자들을 중심으로 시장 규모가 점차 확대되고 있음
- 2017년 5월, 미국의 정보통신 시장조사업체 IDC는 2016년 멕시코의 사물인터넷(IoT)관련 시장의 규모는 운송, 제조, 산업계의 여러 분야에 걸친 투자 증가세에 힘입어 33억 달러에 이르렀으며 2017년에는 26%의 성장률로 40억 달러에 달할 것으로 전망
- 2015년에는 멕시코 IoT 투자액의 70%가 산업 부문에 집중되었으며, 금액 기준 19억 달러 규모에 이르렀으나, 그러나 향후 3년 동안은 민간 분야의 비중이 증가할 것으로 전망

▶ IoT 기반 스마트 그리드 시장규모는 2023년까지 123억 달러로 성장할 전망

- 컨설팅 업체 Northeast Group에 따르면, 멕시코의 스마트 그리드 시장 규모는 2014년 2억 500만 달러를 넘어 2023년 123억 달러에 이를 것으로 예측
- 스마트 그리드 시장의 확대를 통해 멕시코의 낙후된 전기산업 환경으로 인한 정전 및 전기 도난 사고 가능성을 줄일 수 있을 것으로 기대

핀테크 등

▶ 멕시코는 중남미 권역 내에서 확고한 '핀테크 리더'로 부상

- Finnovista에 의하면, 2017년 6월을 기준으로 멕시코 내에는 238개의 핀테크 업체가 등록되어 있으며, 이는 직전 조사(2016년 5월)에 비해 약 50% 증가한 수치임
- Finnovista가 2016년 5월 발표한 자료에 따르면, 멕시코는 총 158개의 핀테크 기업을 보유함으로써 이미 브라질(130개), 콜롬비아(77개)와 칠레(56개)에 우위를 점하며 중남미 지역에서 핀테크 분야의 확고한 리더로 부상
- 멕시코의 핀테크 기업들은 향후 10년간 멕시코 금융 시장의 30%(약 300억 달러 규모) 에서 우위를 점하기 위해 치열하게 경쟁할 것으로 보일 것으로 예상되며, 이러한 경쟁은 기존 금융 서비스에서 소외되었던 인구에게까지 영향을 미침으로써 금융 서비스 시장을 넓힐 것으로 전망

▶ Fintech Mexico는 Fintech Iberoamerica 동맹에 참여

- 2017년 5월, 멕시코 Fintech 기업들의 협의체인 Fintech Mexico는 스페인, 콜롬비아, 우루과이, 페루, 중앙아메리카 및 카리브지역의 국가의 Fintech 협의체들과 중남미 지역의

2) 융합보안 정책 현황

스마트시티

▶ 멕시코 시티, 스마트시티 전환을 위한 매스터 플랜 발표 및 추진

- 멕시코 경제개발청(Secretary for Economic Development, SEDECO)과 World Bank, 멕시코 국립 자치대학교(National Autonomous University of Mexico)와 World Bank가 2016년 '멕시코 시티의 연결성(connectivity) 개선을 위한 마스터 플랜'을 수립과 실행 계획을 발표
- 해당 마스터 플랜은 ▲현재 멕시코 시티의 인프라 수요 추정, ▲최적의 네트워크 디자인을 제시, ▲새로운 방송 시스템의 제안, ▲정부 및 공공시스템 구조 및 니즈 분석 등이 주요 내용으로 포함

스마트의료

▶ 멕시코, 디지털 헬스와 의료 산업에 대한 외부 투자 확대 정책

- 멕시코 보건 당국은 2020년까지 병원 전체에 걸쳐 전가건강기록(electronic health record, EHR)시스템을 도입할 방침으로 알려짐
- 최근 유방암 재단인 'Fundacion de Cancer de Mama'는 클라우드 기반 EHR 시스템인 HarmoniMD을 도입하는 등 헬스 분야의 디지털화 전개
- 디지털 헬스 추진은 OECD 국가 중에서 1인당 숙련 간호사 수가 가장 적고, 헬스케어 서비스 업체들의 헬스 데이터와 리소스의 공유를 금지하고 있는 대신, 모바일 헬스케어 솔루션을 제공할 수 있는 이동통신 도매 네트워크 제도가 잘 되어 있다는 점도 특징

핀테크 등

▶ 2018년 3월 금융 기술 규제법 (멕시코 Fintech 법)이 도입

- 해당 법 가운데에서도 '가상 자산'(암호 화폐)에 관한 운영을 규제하고 ▲Fintech 기관 (FTI) ▲집단 금융 기관 (군중 자금 지원 기관) ▲전자 지불 자금 기관에 대한 규제를 도입
- 동 법은 징역에 의해 처벌될 수 있는, ▲FTI 고객의 자산인 자원, 전자 지불 자금 또는 가상 자산을

▶ 2018년 도입된 멕시코 Fintech 법은 브라질과 함께 중남미 시장에서 새로운 기술 개발을 견인

- 관련 분야의 기술 변화와 그 적용을 인정하는 다른 중남미 국가들에 대한 선행 모델로서의 역할
- 국가은행증권위원회(CNBV)에 따르면, 이는 아메리카 지역에서 이러한 종류의 첫 번째 법률이며, 특히 재무 통합 및 혁신의 원칙을 기초로 하고 있음

나. 코스타리카

'18년 GDP(십억달러)	60.126
'18년 인구수(천명)	4,999

■ ITU 글로벌 사이버보안 지수(Global Cybersecurity Index, GCI)

· 코스타리카의 사이버보안 지수 및 순위는 2017년에 비하여 큰 폭으로 하락

국가명	2018		2017		전년대비 증감	
	지수	순위	지수	순위	지수	순위
코스타리카	0.221	115	0.336	86	-0.115	-29
대한민국	0.873	15	0.782	13	+0.091	-2

■ ICT 관련 주요 지수

· 코스타리카의 전반적인 ICT 발전 수준은 ITU 조사국 175개국 중 중하위권에 속해 있음

지표명	코스타리카		한국	
	점수	순위	점수	순위
IMD 국가경쟁력지수(2019)	-	-	-	28
IMD 디지털경쟁력지수(2019)	-	-	-	10
UNCTAD 전자상거래지수(2019)	64.1	71	89.4	19
ITU 글로벌 사이버보안 지수(GCI 2018)	0.221	115	0.873	15
UN 전자정부 지수(2018)	0.700	56	0.901	3

■ ICT 관련 주요 통계(ITU, 2018년 말 기준)

· 코스타리카의 유선통신 보급률은 낮은 편이나 이동통신 보급률은 매우 높음

항목	코스타리카		한국	
	가입자수(천 명)	보급률(%)	가입자수(천 명)	보급률(%)
유선전화	774	15.48	25.906	50.63
유선브로드밴드	831	16.67	21,286	41.60
이동통신	8,496	169.93	66,356	129.67
인터넷 이용률	74.09%		95.90%	

정보보호 산업 개요

1) 보안 환경

▶ 코스타리카는 중미 지역에서는 드물게 정치적 안정성과 더불어 특히 2010년 이후 3%대의 안정적인 경제성장률을 보이고 있으며 코스타리카 중앙은행인 BCCR은 2019년 경제성장률은 3.4%에 이를 것으로 전망

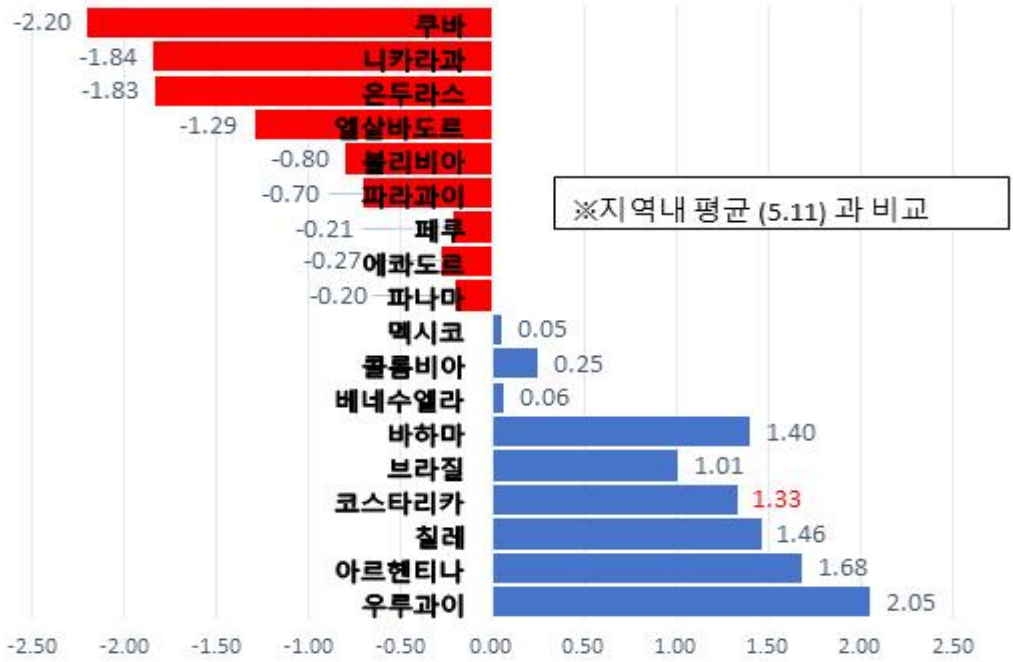
- 코스타리카의 인구는 2018년 기준으로 498만 7천여 명 수준이며, 2018년 기준 국내총생산(GDP)는 601.3억 달러로 코스타리카·엘살바도르·온두라스·니카라과·파나마 등 중미 5개국 중 가장 높아 중미 지역 경제를 이끄는 핵심 국가로 평가
- 그러나 코스타리카 경제는 사회간접자본의 부족과 높은 에너지 비용, 복잡한 행정 절차와 취약한 해외 투자자 보호 문제 등이 개선되지 못하고 있으며, 재정 적자 및 공공 부채의 확대와 20~25%에 달하는 높은 빈곤률에 따른 낮은 구매력이 문제로 지적되고 있음
- 특히 수도 산 호세를 중심으로 증가하고 있는 절도 등의 범죄에 대응하기 위하여, 코스타리카 정부는 치안개선을 주요 국정과제로 삼고 ▲국가 치안현황 진단(Polsepaz), ▲경찰 인력 증원을 통한 치안인프라 구축, ▲치안 분야 재원확충을 위해 주요 기업과 카지노에 대한 과세시행 ▲범죄신고 출동시스템의 전산화를 포함한 치안역량 강화 등을 위한 여러 가지 정책들을 추진

▶ 코스타리카는 중남미 국가 중 정보보호 관련 제도가 비교적 잘 정비되어 있다고 평가되고 있으나, 주로 물리적인 측면의 보안 분야가 주도하고 있는 양상

- 코스타리카는 다른 중남미지역 국가들에 비해, 상대적으로 잘 정비된 정보보안 관련 법률과 제도를 보유하고 있다고 평가되고 있으나, 디지털경제의 확장에 따른 공공 및 산업분야 전반에 걸친 보안사고 증가가 문제로 지적되고 있음
- 코스타리카에서 증가하는 사이버 범죄는 스팸메일을 통한 랜섬웨어나 멀웨어 전파 등의 피싱(Phishing)이나 가짜 웹페이지 접속을 유도하는 파밍(Pharming), 컴퓨터 시스템에 대한 무단 침입인 해킹 사고에 따른 경제적 손실발생에 따른 정보보안 역량 강화에 대한 요구에 국제협력과 투자확대를 확대해나가고 있는 추세이며, 콘텐츠 측면에서는 아동 포르노의 심각성이 주목되고 있음

▶ ITU가 평가하는 ICT발전지수(IDI)에서도 코스타리카는 전 세계에서 중위 그룹에 위치하고 있으나, 주변 중남미 국가들에 비해서는 양호한 평가를 받고 있음

그림 _ 중남미 주요국의 ICT 발전 지수 평균값과 비교(2017)



[출처] ITU, "Measuring the Information Society Report 2017"(2017.6)

▶ 코스타리카의 ICT 발전지수는 지역 내에서 선두권에 속하고 있음에도, 정보보안 수준은 전 세계 국가들 중에서 하위그룹에 속하고 있을 뿐만 아니라 중남미 국가들 중에서 가장 낮은 수준으로 조사

그림 _ 남미 주요국의 글로벌 사이버 보안 지수 비교



[출처] ITU Statistics DB 2017

▶ 최근 코스타리카의 물리보안 분야의 트렌드는 고급화와 시스템화로 대변되는 추세

- 코스타리카는 전통적으로 물리보안을 위해 경비인력을 업무시설과 주거용 시설에 배치해 왔으나, 최근 신축되는 사무실 및 주거용 시설에는 추가적인 도난방지 및 화재경보 시스템, 침입방지를 위한 CCTV 등 보안시스템을 설치하는 것이 하나의 트렌드로 형성

2) 인터넷 및 통신 환경

코스타리카의 일반 정보통신망 보급 현황

▶ 코스타리카 통신시장은 주변국에 비해 상대적으로 안정된 경제와 정치 환경을 바탕으로 모바일 통신시장을 중심으로 지속적인 성장세를 기록

- 코스타리카의 통신시장은 2008년부터 경쟁 체제에 돌입했으며, 시장 관련 제도가 완비된 이후 2011년부터 본격적인 시장 경쟁체제에 돌입
- 무선 통신시장의 경우, 전력산업과 통신산업을 겸하고 있던 국영기업인 Instituto Costarricense de Electricidad(ICE)에 의한 독점 체제가 붕괴되고 현재 ICE, Movistar, Claro의 3사 체제를 형성하는 한편, 2개의 MVNO가 시장에 참여하면서 모바일 통신 분야는 빠르게 글로벌 수준으로 성장
- 유선 통신시장은 무선 통신과 VoIP로 인해 성장세는 둔화되었으나, 시장 자유화의 영향으로 광-동축 하이브리드 기술(Hybrid fibre-coaxial) 기술이 확산되면서 대부분의 도시 지역은 물론 원격지에도 초고속 통신망을 구축

표 _ 코스타리카의 주요 지표 현황(2017년 기준)

정보통신 주요 지표	코스타리카	미주 평균	세계 평균
100명당 유선전화 가입자수	17.2	23.9	13
100명당 무선전화 가입자수	180.2	111.8	103.6
100명당 광대역 무선전화 실제 가입자수	116.6	89.5	61.9
3G 커버리지 비율(전체인구 대비, %)	97.3	93.9	87.9
LTE/WiMAX 커버리지 비율(전체인구 대비, %)	82.2	84.3	76.3
인터넷 사용자 비중(전체인구 대비, %)	71.6	67.5	48.6
컴퓨터 소유 가구 비율(%)	51	64.8	47.1
인터넷 접속 가구 비율(%)	68.6	68.3	54.7
인터넷 사용자당 국제 광대역망 사용 속도(kbit/s)	52.7	77.1	76.6
100명당 광대역 유선 인터넷 가입자수	15.2	19.9	13.6
인터넷 속도별 유선 광대역 가입자 비중(%)			
256 kbit/s ~ 2 Mbit/s	27.4	6.6	4.2
2 ~ 10 Mbit/s	63.8	23.1	13.2
10 Mbit/s 이상	8.8	70.3	82.6

[출처] ITU Measuring the Information Society Report (2018)

- 코스타리카 통신분야에 대한 전체 투자규모는 2012년 국내총생산의 2.2% 수준에서 2016년에는 0.7%로 감소한 것으로 나타났지만, 번호이동성 구현 등의 이슈로 향후 치열한 경쟁이 전개될 전망



[출처] We are Social (2018.01)

▶ 통신분야 성장률은 2014년에 24%를 기록한 이후 둔화되어 2016년에는 3% 수준으로 집계되었으나, 최근 통신업계의 전체 매출액은 꾸준히 증가하는 추세로 전망

- 통신부문은 코스타리카 GDP의 약 3%를 차지하면서 중남미 지역의 평균 수준을 보이고 있음
- 한편, VoIP 서비스와 관련한 매출은 최근 크게 증가했으나 여전히 전체 매출액의 1% 미만으로 조사

▶ 민간기업의 투자 참여에 힘입어 모바일 보급률은 이미 중남미 지역 내 최고 수준으로 집계

- ITU의 2017년 자료에 의하면, 2016년 말을 기준으로 코스타리카 내 유선통신 보급률은 16.0%를 기록
- 반면, 동기간 이동전화 가입 보급률은 159.2%로 조사
- 2010년 이후에는 유선전화 보급률은 감소하는 반면, 이동통신 보급률은 지속적으로 증가하고 있는 패턴을 보이고 있으며, 이와 같은 추세는 다른 중남미 국가에서도 유사한 흐름을 보이고 있음

표 _ 중남미 국가 유선전화 및 이동통신망 보급 현황

국가명	인구 100명당 유선전화 보급률			인구 100명당 이동전화 보급률		
	2010년	2014년	2016년	2010년	2014년	2016년
칠 레	20.2	19.2	19.2	115.8	133.3	127.1
파라과이	5.6	5.4	5.2	91.7	105.6	104.8
콜롬비아	15.5	14.7	14.2	95.8	113.1	117.1
페 루	10.8	9.9	9.7	99.5	105.8	117.1
코스타리카	**22.7**	**17.8**	**16.3**	**67.0**	**143.8**	**159.2**
니카라과	4.4	5.5	5.8	68.1	114.6	122.1
브 라 질	21.6	21.8	20.4	100.9	139.6	118.9

[출처] ITU Statistics DB (2017.6)

▶ UN의 전자정부 발전지수(E-Government Development Index) 조사에서 코스타리카는 56위를 기록

표 _ 미주지역 전자정부 발전지수 평가 (2018년 기준)

Country	Sub-region	OSI	HCI	TII	EGDI	EGDI Level	2018 Rank
United States of America	Northern America	0.9861	0.8883	0.7564	0.8769	Very High	11
Canada	Northern America	0.9306	0.8744	0.6724	0.8258	Very High	23
Uruguay	South America	0.8889	0.7719	0.6967	0.7858	Very High	34
Chile	South America	0.8333	0.8339	0.5377	0.7350	High	42
Argentina	South America	0.7500	0.8579	0.5927	0.7335	High	43
Brazil	South America	0.9236	0.7525	0.5220	0.7327	High	44
Barbados	Caribbean	0.6667	0.8301	0.6719	0.7229	High	46
Costa Rica	Central America	0.6736	0.7933	0.6343	0.7004	High	56
Colombia	South America	0.8819	0.7382	0.4412	0.6871	High	61
Mexico	Central America	0.9236	0.7044	0.4173	0.6818	High	64

[출처] UNITED NATIONS E-GOVERNMENT SURVEY 2018

코스타리카의 정보통신 정책 현황

▶ 코스타리카 정부는 2008년 시장 개방 이후, 통신 부문의 규제와 경쟁 정책을 전담하는 정보통신 감독국(Superintendence of Telecommunications)을 신설

- 코스타리카의 유선 및 무선 시장이 경쟁 체제에 돌입하면서 소매 부문의 통신시장은 물론 도매 시장 역시 2016년부터 경쟁체제에 돌입하였고, 무선 통신시장 역시 2017년 9월부터 경쟁이 본격화
- 전 국민의 보편적인 통신 접근 증진을 목표로 하는 일반 통신법(General Telecommunications Law No. 8642)을 제정하는 한편, 기간통신사업자들의 출연금을 기반으로 하는 국영 통신 펀드(National Telecommunications Fund, FONATEL)를 설립하여 학교나 원격지 등 취약 지역 주민들의 통신환경을 개선하는데 지출하고 있음
- 최근, 코스타리카 정부는 국영 통신 펀드(FONATEL)의 자금지원으로 국가 내 계층간 디지털 디바이드 현상을 완화하기 위한 CRDigital@I 라는 이름의 정부 전략 계획을 발표

▶ 코스타리카는 중남미 국가 중에서 통신 부문의 민영화 및 시장 개방이 가장 늦었던 국가

- 모바일 보급률도 2007년까지 매우 낮은 수준이었다가 2011년 시장 경쟁 제도 도입에 따라 국영 전기통신공사(ICE, Instituto Costarricense de Electricidad)가 서비스 개선 이후 증가하기 시작함
- 유선전화 시장은 여전히 국영 통신사업자 ICE에 의해 주도되고 있지만, 모바일 시장에서는 Claro와

Movistar의 비중은 지속적으로 증가하고 있는 것으로 평가

▶ 코스타리카 주요 통신분야는 국영기업인 ICE에 의해 주도

- ICE는 본래 에너지 분야를 발전시키기 위해 1949년에 설립된 자율적 국가기관으로서, 1963년 법률을 통해 통신서비스 분야도 산하에 통합
- 이후 ICE는 에너지 및 전기통신 분야의 지배적 사업자로서, 2010년 통신 자유화 전까지는 코스타리카 내에서 ICE와 RASCA만이 인터넷 서비스공급자 허가를 보유한 기업이었음

▶ 코스타리카는 지역별 통신인프라 접근성에 큰 편차가 존재한다는 문제가 지적되어 왔으며, 이를 해소하기 위하여 국가 정보통신 기금 (FONATEL, Fondo Nacional de Telecomunicaciones)을 운용해오고 있음

- 국가의 가장 가난한 지역과 가장 멀리 떨어진 지역의 정보격차를 줄이기 위해 전화 또는 인터넷 서비스에 액세스할 수 없는 시골, 해안 및 접경지역에 양질의 통신서비스를 제공하는 것을 목표로 하는 34개의 프로젝트로 구성
- 기금은 일반정보통신법(General Telecommunications Law, GTL)에 의거, 통신사업자가 매년 순이익의 1.5% 출연으로 조성되어, 통신감독국(SUTEL, Superintendencia de Telecomunicaciones)[164]에 의해 관리
- 동 기금은 코스타리카 전역에 공중전화와 130여 개 공공인터넷센터의 건립, 전국 모든 공공도서관에 인터넷망 보급 등을 목표로 운용

컴퓨터 및 인터넷 보급현황

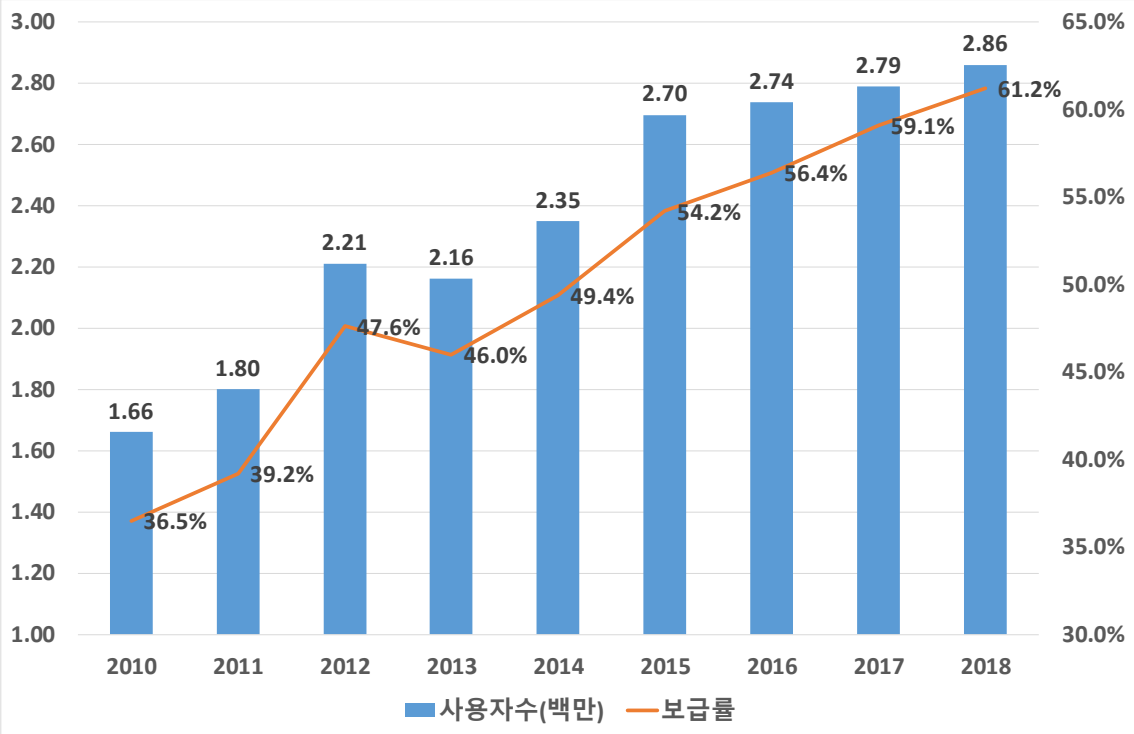
▶ 코스타리카 내 도시지역과 농촌지역 간의 통신 인프라 보급의 불평등에 따른 정보격차는 상당한 것으로 평가되고 있음

- 광섬유 케이블 매설 등 고정 통신 인프라 가설 부진 지방 및 농촌은 이동 통신망을 통한 무선 인터넷을 주로 사용
- 한편, 코스타리카 정부는 국가디지털전략의 일환으로 국가 정보통신 기금(Fonatel, Fondo Nacional de Telecomunicaciones)을 조성하고 지역별 정보통신격차를 줄이기 위한 34개의 프로젝트를 진행하고 있음

▶ 정부의 인터넷 보급정책으로 인터넷 보급률은 빠르게 증가하고 있음

164 2009년에 설립된 코스타리카의 전기통신 감독기관으로서 무선 주파수 규제, 통신사업면허 발급, 통신 분야의 공정한 경쟁을 조성하는 임무를 담당

그림 _ 코스타리카 인터넷 사용자 및 보급률 추이[165]



[출처] Buddecomm(2019.08)

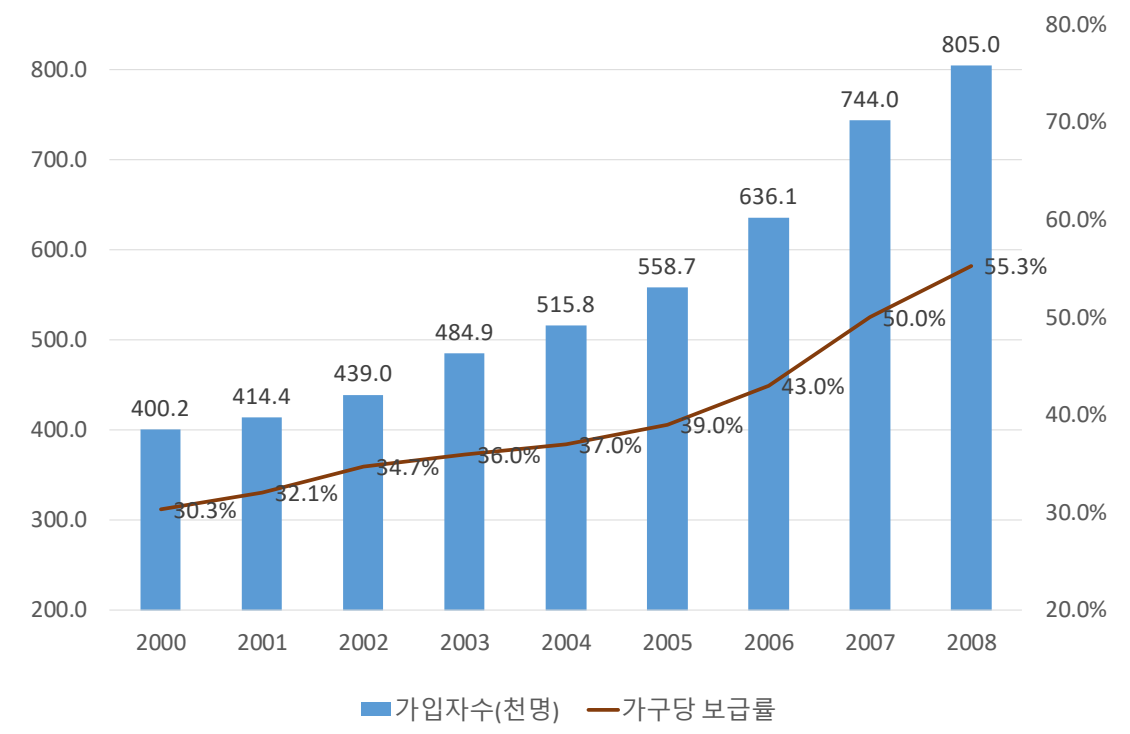
브로드밴드 보급현황

▶ 코스타리카의 브로드밴드 시장은 중앙아메리카 지역에서 활성화된 시장으로 평가

- 유선 브로드밴드 가입자수는 2000년 1,300명에 불과하였으나, 2010년 40만 명을 넘어섰으며, 2018년 기준으로 80만 5천 명으로 크게 증가하고 있음
- 가구당 유선 브로드밴드 보급률 역시 2000년 0.1%에 불과하였으나, 2010년 30%를 넘어섰으며, 2018년 기준으로 55.3%로 전체 가구의 절반 이상이 유선 브로드밴드 서비스를 사용하고 있음

165 2017, 2018년은 추정치

그림 _ 코스타리카 유선 브로드밴드 사용자 및 보급률 추이[166]



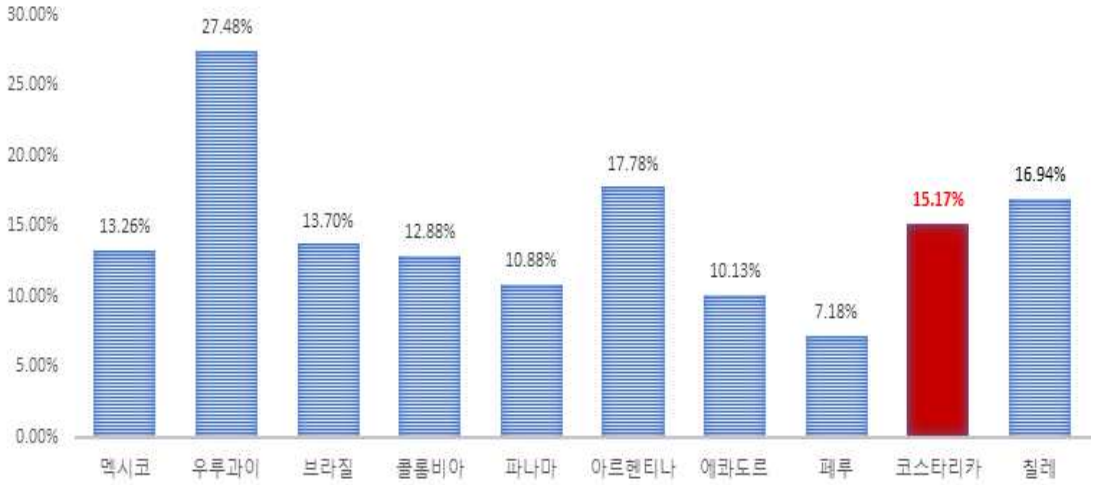
[출처] Buddecomm(2019.08)

표 _ 중남미 주요국 브로드밴드 인터넷 가입 현황 비교

(단위: 명, %)

국가명	2011년	2012년	2013년	2014년	2015년	2016년	2017년
칠레	2,011,244	2,166,330	2,295,169	2,489,717	2,719,439	2,887,000	3,058,979
콜롬비아	3,348,142	3,938,657	4,537,621	5,028,595	5,525,511	5,192,968	6,318,936
코스타리카	**419,782**	**448,594**	**484,883**	**515,859**	**558,656**	**587,000**	**744,059**
니카라과	85,092	101,312	131,687	111,409	116,308	177,024	210,124
파라과이	120,101	136,152	156,576	185,125	220,858	239,499	278,169
페루	1,211,767	1,442,784	1,612,812	1,767,057	1,999,459	2,120,762	2,310,217

166 2018년은 추정치



[출처] ITU Statistics DB (2017.6)

- 그러나 아직까지 지리적으로 브로드밴드 네트워크 보급률은 큰 불균형을 나타내고 있으며, 이러한 정보통신격차는 유선전화보다 브로드밴드 보급률에서 더 크게 나타남
- 2017년 말을 기준으로, DSL과 케이블모뎀을 통한 브로드밴드 접속이 전체 유선 브로드밴드 시장의 94.5%를 차지하고 있으며, 광케이블 등은 전체 시장의 약 2.5%를 차지하는 것으로 조사

표 _ 코스타리카 유선 브로드밴드 공급기술 현황(2015-2017)

년도	DSL	Cable modem	Fibre
2015	45.30%	53.50%	1.20%
2016	42.15%	56.10%	1.80%
2017	34.6%	59.9%	2.5%

[출처] Buddecomm(2019.08)

▶ 통신인프라 확대보급과 개선을 위한 중장기 국가개발계획 2015-2021 프로젝트[167]를 추진하고 있음

- 코스타리카 과학기술통신부(Micitt)는 2021년까지 자국민의 80%가 OECD 국가 평균 인터넷속도인 20MBps의 속도를 이용하게 되는 것이 목표임을 강조하면서, 브로드밴드 기술의 핵심은 광케이블이 될 것이라고 밝힌 바 있음
- 동 개발계획은 ▲디지털 보편화, ▲전자정부/투명한 정부, ▲디지털경제의 구현을 목표로 하고 있음
- 동 목표의 구현을 위한 세부목표로서 ▲(교통분야) 2018년까지 국민의 70%에 지능형 교통시스템과

167 MICITT, Plan Nacional de Ciencia, Tecnología e Innovación 2015-2021

디지털 교통카드의 보급, ▲(주파수) 2021년까지 890MHz의 주파수를 추가적으로 민간에 할당, ▲(디지털화) 2017년까지 전국 184 District에 인터넷을 보급(현재 약 125 District)을 제시

- 그와 같은 목표에 따라 ICE는 차세대 통신망 투자의 일환으로서 2016년 103,000개의 광케이블 허브건설을 위하여 3,300만 달러를 투자하고 2017년 연말까지 추가로 180,000개의 광케이블 허브를 건설하기 위해 9,100만 달러를 추가로 투자할 것이라고 발표
- 그러나 코스타리카 정부는 4년 단임제를 채택하고 있어, 중장기 대형 프로젝트를 추진하기 위한 정책의 지속성이 떨어지는 문제점을 노출해왔으며, 동 프로젝트 또한 구체적인 추진 로드맵이 결여되어 있다는 평가가 지배적인 상황

이동통신 보급 및 시장 현황

▶ 코스타리카의 이동통신 가입자는 2000년부터 유선통신 가입자수를 넘어선 라틴 아메리카의 다른 나라와 달리, 2006년에야 유선통신 가입자 수보다 많아짐

- 코스타리카의 이동통신 가입자 수는 여러 해 동안 라틴 아메리카의 다른 지역에 비해 낮은 수준에 머무르다 2010년대 중반 들어 선불폰 상품을 출시하면서 본격적으로 가입자 수가 확대되는 양상을 보임
- 코스타리카는 중미 지역에서는 최초로 1989년부터 다국적 기업 Millicom International과 코스타리카 기업인 Comcel의 합작으로 이동통신 서비스를 개시
- 그러나 1993년 이 합작 사업이 위헌이라는 법원의 판결로 ICE 독점으로 이동통신 사업을 전개

▶ 그러나 아직까지도 코스타리카 이동통신 분야는 국영기업 ICE에 의해 주도되고 있음

- 코스타리카 이동통신 시장은 국영기업체 ICE에 의해 독점상태에 있다가 2010년 중미자유무역협정 CAFTA을 계기로 2011년부터 멕시코 America Movil의 Claro와 스페인 Telefónica의 Movistar가 시장에 진입하면서 경쟁체제가 도입되었음
- 이동통신 서비스 이용시간은 사용자 수가 확대되면서 오히려 지속적으로 감소하는 양상을 보이고 있는데, 선불폰의 경우 2012년 103분/월이었던 사용시간이 2017년 41분/월으로 절반 이하로 줄어들었으며, 약정폰의 경우 선불폰보다는 사용 시간이 길지만 2012년 199분/월에서 2017년 143분/월로 줄어드는 양상을 공통적으로 보이고 있음
- Movistar와 Claro가 시장에 진입한 2011년 이후 코스타리카의 이동통신 보급률은 빠르게 증가하였으나, 2017년에도 여전히 ICE의 시장점유율은 50%를 상회하고 있으며, 상위 3개사의 시장점유율이 전체 시장의 98% 이상으로 집계

표 _ 2012~2017년 가입자 유형별 이동통신 서비스 이용 시간

년도	선불폰(분/월)	약정폰(분/월)	총계(분/월)
2012	103	199	302
2013	85	192	277
2014	86	190	276
2015	68	178	246
2016	54	153	207
2017	41	143	184

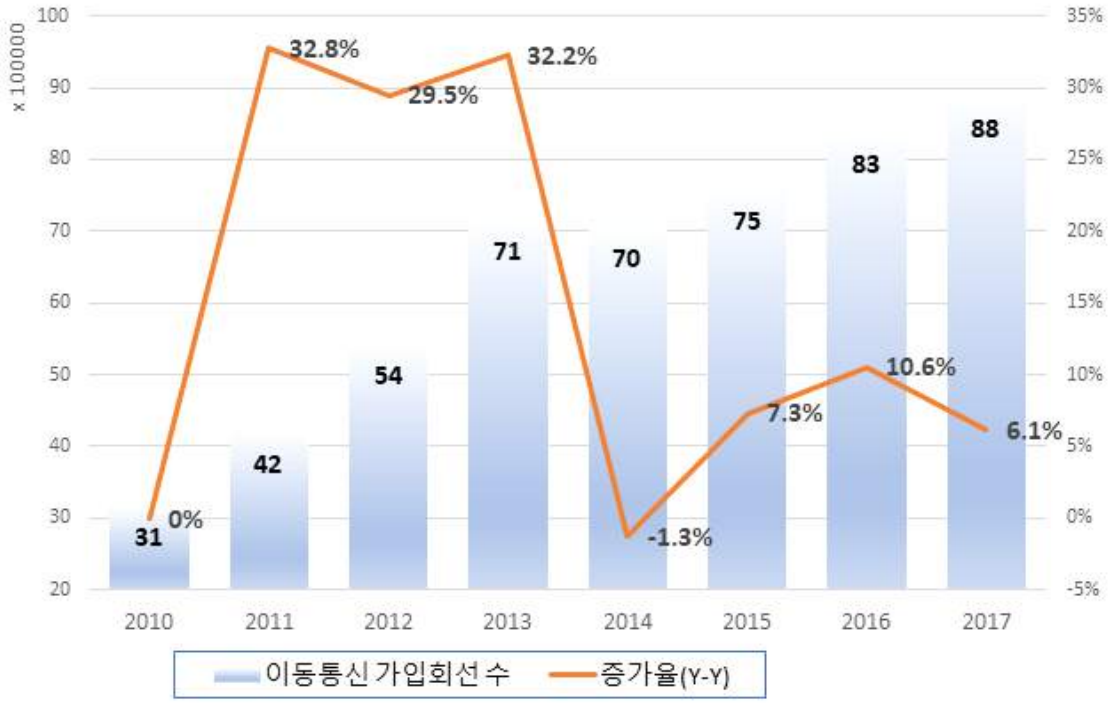
[출처] Buddecomm(2019.08)

표 _ 2011~2017년 이동통신 시장점유율 현황

년도	ICE	Claro	Movistar	Fullmóvil	Tuyo Móvil
2011	90.0%	3.0%	3.0%	2.0%	2.0%
2012	72.8%	15.0%	8.4%	2.3%	2.5%
2013	61.1%	19.0%	18.0%	0.8%	1.7%
2014	61.9%	16.3%	20.4%	0.5%	1.2%
2015	57.6%	19.0%	22.0%	1.0%	0.8%
2016	53.3%	19.7%	25.7%	1.6%	0.1%
2017	**51.8%**	**21.3%**	**26.3%**	**0.6%**	**0.0%**

[출처] Buddecomm(2019.08)

그림 _ 2010~2017년 이동통신 가입회선수와 증가율(Y-Y) 현황



▶ 코스타리카는 중미 국가 중 선불 모바일 서비스를 가장 늦게 도입했음에도 불구하고 현재 다른 국가들과 마찬가지로 후불제보다 선불제 가입자의 수가 압도적으로 많은 상황이 지속되고 있음

표 _ 2014~2017년 선불제 및 후불제 이동통신 가입자 수 비중 추이

연도	선불제	후불제
2010	49%	51%
2011	69%	31%
2012	79%	21%
2013	83%	17%
2014	80%	20%
2015	79%	21%
2016	78%	22%
2017	77%	23%

[출처] Buddecom(2019.08)

• 2011년 이후 음성통화와 문자를 포함한 이동통신 매출액은 꾸준히 증가하고 있으며, 2013년 이후 SMS/MMS 매출액은 꾸준히 줄어들고 있으며, 이에 반해 데이터 매출액은 지속적으로 증가

표 _ 2012~2017년 서비스별 매출액 추이

연도	음성 (10억 콜론)	SMS/MMS (10억 콜론)	데이터 (10억 콜론)	총계 (10억 콜론)
2012	273.34	38.77	41.16	314.5
2013	293.197	38.67	94.006	386.82
2014	366.143	23.562	127.198	493.217
2015	358.377	14.32	170.421	528.743
2016	347.713	10.583	194.502	542.202
2017	347.492	10.95	207.664	555.156

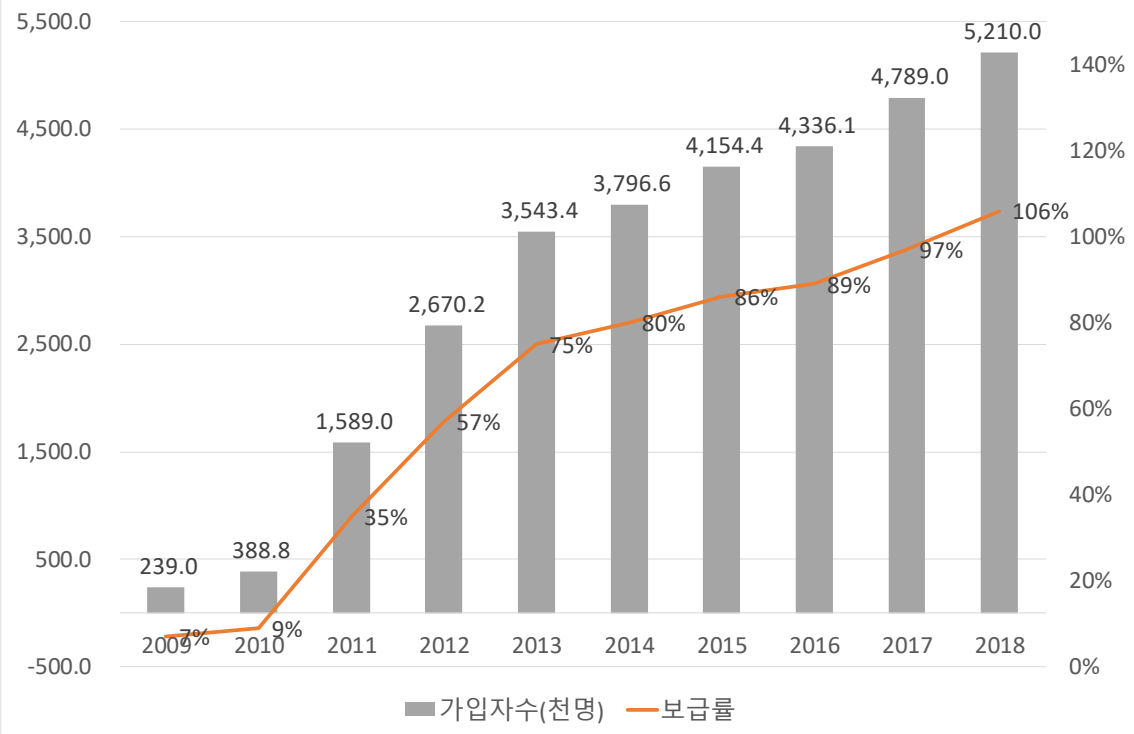
[출처] Buddecom(2019.08)

▶ 코스타리카의 모바일 광대역 인터넷 가입자 수는 지속적으로 증가 추세를 보이고 있음

• 모바일 인터넷 가입자 수는 2017년에 전년 대비 10.4% 증가하였으며, 이동통신 가입자 중 2.5%만 USB나 별도의 데이터 카드를 이용하여 모바일 인터넷에 접속하는 것으로 나타남

• 모바일 인터넷 서비스에 의한 매출액은 2017년에 전년 대비 7% 증가

그림 _ 2009~2018년 모바일 인터넷 가입자 및 보급률 추이



[출처] Buddecom(2019.08)

표 _ 2013~2017년 모바일 인터넷 매출액 추이

연도	매출액(10억 콜론)
2013	94,006
2014	127,198
2015	170,421
2016	194,502
2017	207,664

[출처] Buddecom(2019.08)

정보보호 시장 현황

1) 시장 규모

▶ 코스타리카의 정보보호 시장 규모는 공식적으로 집계된 통계가 없음

- 물리보안 부문의 경우 최근 강도, 살인 등의 강력범죄가 증가하면서 많은 상업시설 및 기업들이 사설경비업체 고용 및 경비시스템 확충에 많은 비용을 투자하고 있으며 정부 역시 GDP의 평균 3.5%에 해당하는 예산을 공안부에 책정하며 시민 및 시민의 재산 보호에 총력을 기울이고 있음[168]

2) 분야별 현황

▶ 코스타리카 정부는 공안부(Ministerio de Seguridad Pública) 내에 개인보안서비스부 (Dirección de Servicios de Seguridad Privados)를 두고 개인보안 서비스를 제공하는 자연인 및 법인의 활동을 규제하고 감독하고 있음[169]

- 공안부는 전자정부기술위원회와 공동으로 개발한 개인보안 사업자 등록 및 관리 플랫폼인 Control Pas, 개인보안요원 관리 플랫폼인 Segupriv를 통해 개인보안 서비스업자 등록 및 연장 업무, 무기 등록 및 요원들의 무기 소지 허가 등을 관리하고 있음

▶ 코스타리카의 공공 부문과 주요 국가 시설 조직은 ISO/IEC 27001과 같은 국제 보안 규격을 준수하고 보안 수준을 증진하기 위한 노력을 지속

- 그러나 민간 부문의 보안 수준은 상대적으로 낮은 수준이며, 인터넷 서비스 공급업자의 등록에 대한 명확한 규정이 제시되지 않은 상태임
- ICE와 같은 대형 통신업체는 소프트웨어 개발 기준을 제시하는 한편, 사이버 보안 시장에 대한 참여나 정보 기술 시스템에 대한 투자를 지속적으로 확대하고 있음
- 민간부문에서 피고용인의 프라이버시에 대한 인식이 제고되고 있으며, 프라이버시 관련 정책도 제도화 초기 단계에 진입하고 있음[170]

---

168 http://www.crhoy.com 및 2017.10.17, La Republica지, "Álvarez y Castro reducirían déficit fiscal eliminando el crimen"

169 http://www.seguridadpublica.go.cr

170 Organization of American States & Inter-America Development Bank(2016), 2016 Cybersecurity Report: Cybersecurity, Are We Ready in Latin America and the Caribbean?

▶ 컴퓨터 사이버 범죄 증가하는 반면 기업 및 개인의 보안 의식은 뒤떨어져 있음[171]

- 코스타리카 내에서 가장 흔히 일어나는 사이버 공격의 형태는 이메일이나 피싱 사이트를 통한 개인 및 기업 정보 유출로 나타남
- Eset사의 설문조사에 따르면 코스타리카 기업 중 42%가 피싱, 랜섬웨어를 비롯한 멀웨어로 고통받고 있다고 응답했으며 Microsoft사의 조사에 따르면 코스타리카 내 컴퓨터의 4~10%가 트로이의 목마, 웜 및 스파이웨어에 감염되어 있음
- 글로벌 조사기관인 IDC와 보안업체 Fortinet의 조사에 따르면 코스타리카 기업 80%의 IT보안 수준이 '중간(intermediate)'수준에 머무르고 있어 공격에 취약한 것으로 드러남

3) 주요 사업자 현황

시장 특성 및 사업자 수

▶ 코스타리카의 정보보호시장은 아직은 전통적인 인적 물리보안 사업이 주류를 이루고 있고 최근 들어 일부 다국적 기업 현지 법인 및 지사의 참여가 시작된 정보보안 부문 업체가 늘어나는 추세

- 2017년 6월 Control Pas에 등록된 사설보안업체 수는 737개이며 그 중 557개 업체가 실제 영업 중인 것으로 추정되며 2만 4천여 명의 사설 보안요원이 있는 것으로 추정됨

주요 사업자 현황

① 정보보호

- 코스타리카 현지 정보보호 업체는 없으며, 아카마이, IBM, HP 등 글로벌 기업이 진출하여 자체 SOC를 통해 고객사를 관제, 딜로이트는 정부기관을 대상으로 서비스를 제공하고 있음
- 중미지역 IT 전문기업 SPC International 코스타리카 지사에서는 딜로이트 코스타리카 지사 출신의 사이버보안 전문가를 영입(2015.6)하고 사이버보안 종합 서비스를 제공(니카라과, 엘살바도르, 과테말라, 온두라스에 지사 보유)
- Ciberlegal는 코스타리카 유일의 사이버 관련 전문 서비스 제공 로펌

② 물리보안

- CRISTHIAN FERNANDO CARBALLO SANCHEZ: 전자보안 장비 운영 기술 제공

171 2017년 4월 30일자 일간지 El Financiero지에 게재된 "Los ataques informáticos más frecuentes en Costa Rica"

- GRUPO MR DOS SEGURIDAD S.A: 경비, 모니터링 및 경호 서비스
- KRUMA CONSULTORES RD S.A: 화재, 침입, CCTV, 접근통제 등의 전자보안 솔루션
- PROARSA S.A : 모니터링 및 경보음 관리
- R.S SEGURIDAD DIGITAL INTERNACIONAL S.A : 전자 보안 솔루션
- SC SECURITY S.A : CCTV, 접근통제, 화재예방 시스템, 강절도 경보음 등 보안장비 판매, 설치 및 유지관리 서비스
- SEGURIDAD CONTINENTAL SECO S.A : 전자보안장비(CCTV, 폐쇄회로 카메라 및 TV 등), 접근통제 감시 및경보음 시스템, 각종 보안장비 판매 및 기술제공, 보안 프로젝트 컨설팅 등 종합 정보보안 사업 수행
- SEGURIDAD DELTA : 경비, 접근통제, CCTV, 경고음 및 감시 서비스
- SEKUNET S.A : 접근통제,CCTV, 화재 예방 및 경고음 장비 등이 유통 및 솔루션
- SENSORMATIC DE COSTA RICA S.A : 전자 및 물리보안 CCTV, 경고음 모니터링, 수사 및 사실증명활동 등
- TECNASA : 각종 솔루션, 보안관련 국제기업과 연계 보안장비 및 소프트웨어 등 서비스
- CEWTEC : 사이버 정보보안, 기술이전 등

4) 주요 동향 및 이슈

▶ 최근 코스타리카는 마약거래 관련 강력범죄의 발생이 증가 추세

- 특히, 과테말라, 온두라스 및 엘살바도르 3국에서 미국의 지원 아래 진행되고 있는 강력한 마약단속에 따른 풍선효과로 코스타리카의 수도지역과 일부 지방도시, 특히 카리브 연안 소재 리몬 등 지방도시에서 마약거래 관련 강력 범죄가 급증하는 추세
- 공안부 자료에 따르면 2017년 1월 30일부터 5월 30일까지 마약 판매, 소지 등 향정신성의약품관련법 위반으로 2만 9,000명이 구금되었으며 같은 기간에 마약통제경찰(PCD)이 압수한 마약의 양은 코카인 6,738,087kg, 마리화나 3,378,600kg을 포함하여 10톤에 달하는 것으로 알려짐

▶ 경기침체가 장기화되면서 민생범죄도 증가세

- 국내 경기침체 현상의 장기화에 따른 강절도 및 살인 등 범죄가 증가세 치안불안이 심화되고 있음
- 2016년 살인사건 발생건수는 577건이었으나 2017년 6월 30일 기준 살인사건 발생건수는 278건으로 집계되었으며, 코스타리카 정부는 2021년에는 706건의 살인이 발생할 것으로 예상

▶ 인근 니카라과인과 쿠바인들의 불법 체류자가 증가되고 있는 점도 치안유지상 부담되는 요인

- 코스타리카와 국경을 접하고 있는 니카라과의 경기침체와 실업증가 사태로 니카라과인들의 불법

월경이 증가되고 있는 추세

- 특히 미국과 쿠바의 외교관계 회복 시기 이전에 미국으로 이민하고자 탈출한 쿠바인들 상당수가 여전히 코스타리카와 니카라과 국경지대에 불법 체류 중이라는 점 등은 코스타리카 내 물리보안 장비 및 서비스에 대한 수요가 증가할 것이라는 방증으로 언급됨

정보보호 정책 및 기관 현황

1) 관련 법령 및 정책

관련 법령 및 규제

❑ 코스타리카 정보보호 범죄법(Ley de delitos Informaticos)

▶ 법령 번호 :Ley No. 8148(2012. 11. 26)

- 코스타리카는 정보보호 범죄에 대해 별도의 법을 정해 처벌 근거를 두지 않고 기존 형법(Ley No. 4573L 1970. 05.04)에 정보보호 범죄관련 조항을 유형별로 새로 추가하는 형태로 운영
- 이 법에서 규정하는 사이버 범죄의 유형은 전자적 형태의 통신에 대한 개입, 데이터의 변조와 컴퓨터 사보타지, 컴퓨터 사기, 청소년 대상 범죄 및 포르노 시뮬레이션, 청소년 이미지의 판매와 손괴 등임

▶ 주요 내용

- 167조: 미성년자와의 성관계를 위해 정보통신망을 악용한 자는 10년 징역형으로 처벌 근거
- 196조: 전자문서 관련 임의 조작, 편취, 절도, 매매 등 위반사항 6년 징역형 처벌 근거
- 217조: 컴퓨터 시스템을 이용한 정보사기 관련 처벌 근거
- 229조: 정보원 임의 접근, 삭제, 임의 수정 등 정보 스파이 및 정보조작 관련 범죄에 4년 징역형 근거
- 230조: 위키리크스(Wikileaks) 폭로사건과 같은 전자우편을 이용한 정보 보호법 위반 유형의 범죄에 대해 3년~8년 징역형에 처하는 처벌 근거 조항
- 231조: 정보 스파이행위에 대해서는 3년-6년 징역형 처벌 근거 등

❑ 코스타리카 개인정보보호법(Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales)

▶ 법령 번호 : Ley No. 8968(2011. 09. 05)

▶ 주요 내용

- 목적: 모든 사람이 국적, 거주국 및 주소에 관계없이 자신과 자신의 재화에 관한 모든 형태의 자료 취급 시 기본권과 자결권, 개인 인권에 관한 동등권과 자유를 보장하기 위한 법

- 보호대상 정보: 모든 데이터베이스, 개인보관 자료, 불법 접근금지 개인 자료, 접근제한 및 민감 개인정보, 기밀유지 대상 정보 등
- 보호대상 기본권: 정보의 자기판단권, 정보사용 동의 원칙, 사용내역 통보원칙, 정보의 사실성, 진실성, 정확성 유지 원칙, 정보사용 목적의 적합성 등

주요 전략 및 정책

▶ 코스타리카 정부는 2년이 넘는 기간 동안 준비한, 국가 사이버보안에 대한 지침인 국가사이버보안전략(Estrategia Nacional de Ciberseguridad de Costa Rica)을 발표(2017.11)

- 코스타리카 정부는 급증하는 사이버위협의 대처하기 위한 국제적인 협력을 통해 사이버보안 전략 수립 및 체계 강화 추진
- 코스타리카는 과학기술부(MCITT), 시민사회, 비정부기구뿐만 아니라, 캐나다, 영국대사관, 미국기관(OAS)의 과학기술자 등과 공동 작업으로 국가 차원의 사이버보안전략 개발 추진
- 코스타리카는 사이버보안전략에 관한 운영계획 수립을 위해 과학기술부, 사법부, 시민사회, 학계, 민간 등이 참여하는 보안위원회 구성 및 운영
- 최근에도 코스타리카는 지속적인 사이버공격으로 인한 위협 지속

※ Fortinet의 데이터에 따르면 코스타리카는 2019년 1분기에 1,900만 건의 사이버공격을 받음

▶ 국가사이버보안 전략의 목표와 주요 내용은 다음과 같음

- 국가사이버보안전략의 목표는 ICT 보안 분야에서 국가의 전략체계 개발, 참여자 조정협력 촉진, ICT 이용에 관한 위험에 대한 교육, 사이버위협 예방 및 완화 조치 촉진 등을 통한 국가사회의 안전하고 안정적인 환경 제공

표 _ 국가사이버보안전략의 8대 목표

목표	내용
1. 국가조정	• 사이버보안 사고 발생 시 완화와 관리, 복구 및 연속성 모두에서 관계자의 역할과 행동을 조정 및 협력
2. 인식제고	• 모든 디지털 기술 사용자의 기본적인 의무로서 디지털 보호의 책임을 장려하기 위한 사이버보안에 대한 인식 및 교육 캠페인 공동 개발 및 구현
3. 국가 사이버보안 역량 개발	• 사이버보안 개념 및 모범 사례 관련 최종사용자를 교육하고 사이버보안 기술 전문가(개발자, 관리자, 관리자)에 대한 교육 캠페인 제공
4, 사이버보안 및 ICT 법적체계 강화	• 기존 법적 체계를 검토하고 적절한 조사와 효과적인 기소를 보장하기 위한 법적 절차와 제도적 조치 강화

목표	내용
5. 주요정보통신 기반시설 보호	• 주요정보통신기반시설의 식별 및 보호를 위한 메커니즘을 촉진하고 공공 정책을 수립하며 중대한 사이버보안 사고 예방 및 완화
6. 위험관리	• 각 기관 또는 조직의 요구에 맞는 위험 관리 모델의 구현 촉진
7. 국제 협력과 참여	• 범죄, 기술, 교육 지원 및 협력과 관련 사이버보안 문제를 해결하기 위한 보안 조치 개발을 통해 국제 협력에 참여
8. 구현, 모니터링 및 평가	• 실행자들이 준수 여부를 평가하고 필요에 따라 조정할 수 있는 구현 및 후속 방법론을 설계 및 적용

• 국가사이버보안전략의 주요 내용은 국가조정, 인식제고, 국가 사이버보안 등 8대 목표가 제시되고 있으며, 8대 목표에 따른 세부목표 및 전략 내용은 다음과 같음

표 _ 국가사이버보안전략의 목표별 전략 내용

목표	세부목표	전략내용
1. 국가조정	국가조정관	• 사이버보안 조치를 담당할 책임이있는 국가조정관을 지정하고 전략 준수를 추적 - 국가조정관은 사이버보안과 관련된 모든 문제의 국내 및 국제 문제 관련 사항 수행
	민관 협업	• 사이버보안에 대한 국가의 관심을 유도하고 관련 당사자의 광범위한 대표가 참여하는 전략 개발을 위해 공공부문과 민간 부문의 긴밀한 협력 유지
2 인식제고	일반 대중	• 시민의 사이버보안 인식 캠페인을 개발하여 어린이와 청소년, 노인과 같은 취약계층을 보호하기 위한 행동 강화 - 원주민, 장애자 등 취약계층을 위해 민간 부문, 시민 사회 및 비정부 조직과 협력
	공공 부문	• 공무원 대상으로 인식 및 교육 캠페인을 개발 및 개인정보보호 모범 사례 공유
	중소기업	• 사이버보안 문제, 특히 중소기업을 위한 사이버보안 정보 교환 및 공유 등을 위한 포럼 신설
3. 국가 사이버보안 역량 개발	전문인력 교육	• 공공 부문 공무원의 사이버보안의 전문화 교육 및 교육 기회확대 장려 • 사이버보안 연구과정 개발 및 학부, 대학원 및 박사 과정에 사이버보안 교육과정 개설
	연구 개발	• 공립 및 사립대학과의 제휴를 통해 새로운 위협에 대한 연구 프로젝트와 사이버사고에 대한 혁신적인 솔루션 개발
4, 사이버보안 및 ICT 법적	사이버범죄의 규제 및 절차 적 체계 강화	• 사이버범죄에 대응을 위한 적절한 절차와 도구를 검토하기 위해 현재 규정을 검토하는 전문위원회 구성

목표	세부목표	전략내용
체계 강화	형사사법의 법 집행을 위해 사이버보안 역량 구축	• 사이버보안에 대한 기술과 지식을 강화해야하는 형사 사법 시스템의 핵심 영역 식별 • 식별된 주요 영역을 위한 역량 구축에 협력
	형사사법에 관심이있는 파트너 간 정보 교환 신뢰체계 촉진	• 사이버범죄와 관련된 관련 정보를 안전하게 교환할 수 있도록 법적 기밀 유지를 지원하는 신뢰할 수 있는 네트워크 구축 • 기밀 정보 교환을 위한 신속한 절차 설계
5. 주요정보통신기반시설 보호	주요정보통신기반시설의 식별 및 분류	• 보안조치 이행의 중요 단계로 국가의 주요정보통신기반시설 식별 • 국가의 주요정보통신기반시설 서비스의 지속적 운영과 안정성을 보장하기 위해 공공 정책 개발
	행정 정보 및 통신 시스템의 보안 조치 구현	• 각 기관의 성숙도와 공공 부문의 기존 요구에 따라 행정부 부처의 사이버보안 프로토콜 설계
6. 위험관리	정보 보안과 관련된 제품 및 서비스의 보안 향상	• NIST, ISO/IEC, COBIT와 같은 국제 표준, 경제협력 및 개발기구(OECD), ITU 등의 권고사항을 고려하여 공공 및 민간의 운영을 위한 보안 표준의 구현을 우선적으로 추진 • 관심이 있는 관계 기관 및 조직의 인증을 용이하게 하는 방식으로 인증기관과 협력
	금융 부문에서 모범 사례 구현 및 최소 보안요건 정의	• 각 섹터 조직의 다양한 성숙도와 규모를 고려하여 금융 부문 규제 기관과 협력하여 기업을 위한 특정 보안체계 개발 • 금융시스템을 구성하는 여러 기관과 지속적으로 의사소통하는 메커니즘을 구축하여 사이버보안 강화에 대한 개선방안 검토
	참조 보안 조치 채택	• 시민에게 제공되는 서비스에 대해 적절한 보안, 개인정보보호 및 데이터 소유권 보장, 디지털인증서 사용, 데이터 서비스의 보호에 대한 엄격한 표준 구현
	정부 기관을 위한 정보 교환 네트워크 구축	• 높은 수준의 기밀성과 전문성이 적용되는 신뢰 네트워크를 통해 정부의 정보보안 책임자 간의 정보교환 촉진 • 참가자의 범위와 조건을 설정할 수 있는 법률 도구 개발
	컴퓨터 보안사고대응 센터 강화	• 컴퓨터 장애 및 사고에 대한 복원력을 강화하고 향상 • 사이버침해사고대응센터(CSIRT)에 대한 자원 할당 • 국가 CSIRT와 협력하는 부문 별 CSIRT 생성을 장려하고 지원하여 각 부문에 대한 특정 솔루션을 제공하여 사고에 대한 보다 빠르고 효율적으로 복구
7. 국제 협력과 참여	국가 전략의 목표를 지원하기 위한 국제 사회 참여	• 다른 동맹국과 사이버보안 협력을 강화하기 위해 국내외의 전문포럼에 참여하도록 장려 • 인턴, 교육, 워크숍 등을 통해 국가의 필수 사이버보안 자원 및 시설을 강화하기 위해 국내외 협력 강화
8. 구현,	국가 사이버보안	• 국가 사이버보안 전략 시행에 대해 체계적으로 모니터링하기 위한 방법론 설계

목표	세부목표	전략내용
모니터링 및 평가	전략의 이행 평가	• 사이버보안전략에 제시된 목표의 진행과 효과를 모니터링하기 위한 점검 수단 정의
	국가사이버보안 전략 검토 및 개정	• 자문위원회는 국가사이버보안전략을 분석하고 필요한 수정을 위해 권장사항 등이 포함된 보고서 제출

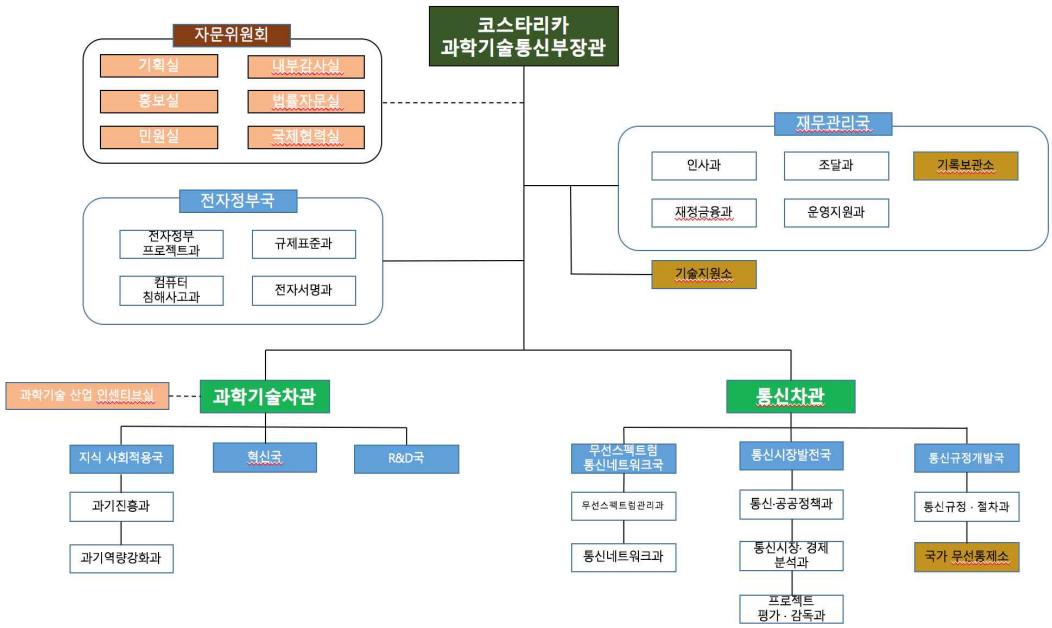
2) 담당기관

주무기관

▶ 과학기술통신부(MICITT : Ministerio de Ciencia y Tecnologia)[172]

• 2012년 과학기술통신부내부조직으로 국가침해 사고대응팀(CSIRT.CR)을 설치, 2013년 ICE 연구소에 대한 DDoS 공격을 비롯한 여러 위기 상황에서 미주기구(OAS) 및 기타 지역 및 국제 전문가의 기술 지원을 받아 사이버 보안 위협을 탐지·대응하였음

그림 _ 코스타리카 과학기술통신부 조직도



[출처] 코스타리카 과학기술통신부

172 www.micit.gob.cr

유관기관

❑ 코스타리카 국가침해사고대응팀(CSIRT.CR : Centro de Respuesta de Incidentes de Seguridad Informatica)

▶ 2012년 정보보안 대책의 하나로 창설되었으며 주요 활동은 다음과 같음

- 국가사이버보안대책 개발
- 사이버 범죄관련 국가 법률적 대응책 검토
- 정보통신과학부 부령(No 37052-MICIT) 검토 보완
- 신뢰할만한 통신망 육성 강화
- CSIRT.CR 활동 강화를 위한 기술기반 구축
- 웹사이트 및 사이버 정보사고 유형 분석
- 각종 개방 정보원 검증

▶ 민간기구로 코스타리카 정보보호조직협회(Asociacion de Organizaciones de Seguridad de Costa Rica) 산하에 정보보호사고특별대책팀(CR-CERT)을 가동하고 있으나 법적 근거가 없는 사조직 성격으로 정부와의 공식 관계는 전무하며, 활동도 미미한 수준

❑ 코스타리카 선거관리위원회(Tribunal Supremo de Elecciones Normativa:)[173]

▶ 법적으로 선거인 명부 작성 및 관리를 위해 개인정보를 수집, 데이터 베이스 작성 및 보관을 책임지고 있어 개인정보보호 기관의 하나로 지정되어 있음

❑ 시민 정보자료 보호기관(PRODHAB : Agencia de Proteccion de Datos de los Habitant)[174]

▶ 법령 근거 : Ley No. 8968(2011. 09. 05) 15조-20조

▶ 내용

- 법무부 산하에 독립된 사법 기구의 하나로 창설
- 자연인, 개인 및 법인관련 모든 정보자료의 보호 규정 수립 및 이해 당사자들의 이해여부 평가
- 개인정보보호법 침해관련 클레임 해결
- 개인정보 자료가 포함된 자료 및 데이터베이스의 유통에 대해 금지, 승인, 추가요건 요구 등 명령,

173 www.tse.go.cr
174 www.mjp.go.cr

공식화, 청원 등 필요한 조치

- 개인정보보호 위반 사범은 내무부 경찰청으로 이관 사법처리 절차처리 제재조치
- 개인정보보호 관련 법조항 검토 보완 조치 등

3) 인증제도

▶ 인증제도 현황

- 코스타리카에는 별도의 정보보호 관련 인증제도는 없음
- 공공부문은 ISO/IEC 27001과 같은 국제보안표준을 채택하여 준수하고 있으나 민간 부문은 명확한 규범이 없어 정보보안 수준이 높지 않음

4) 최근 정책 동향 및 이슈

▶ 미래보안 위협 등 사회적 인식 제고 노력 활성화(2019.9)

- 최근 코스타리카에서는 5G, IoT, AI 등 신기술 확산에 따른 사회적 문제점을 해결하기 위한 Simulator(사회적 논의체)에 정치, 교육, 기술 등 관련 종사자들 모임이 활성화 되고 있음
- 전 정보통신부 장관 등이 중심이 되어, 미래 신기술에 대한 사회적 위험 각성 및 대비를 위한 논의체 구성 등이 시작되었으며, 이러한 논의를 시작으로 신기술 도입에 대한 사회적 부작용 즉 실업, 사이버 범죄 등에 대한 인식이 제고되고 있음

▶ 코스타리카의 외무부장관을 겨냥한 대규모 해킹 공격이 발생, 관계 당국은 예의 주시 중(2019.3.10.)

- 인근 국가인 니카라과 출신으로 알려진 일단의 해커들이 730명에 달하는 공무원들의 신상을 온라인에 공개하면서 코스타리카의 외무부 장관을 표적으로 하는 해킹 공격을 시도
- 이 해커들은 니카라과 대통령 다니엘 오르테가의 실정을 고발하기 위한 해킹이라고 밝힘

▶ 최근 코스타리카에서 이메일 송장을 가장한 피싱 사건이 연달아 발생(2019.1.16.)

- "Hola. Este pago fue aprobado y enviado esta manana, por favor confirme los detalles del beneficiario y firme. Gracias",라는 메일 본문으로 수신되는 이메일이 피싱 메일 주의보가 발령됨
- 이 사기 이메일은 기업의 회계나 인사 담당자들을 대상으로 발송되는 것으로 알려졌으며, 첨부 파일을

클릭하는 순간 컴퓨터의 민감한 정보를 빼내거나 컴퓨터를 감염시켜 중요한 파일에 록(lock)을 걸고 이 파일에 대한 몸값을 요구하는 등의 피해가 발생

- 코스타리카 사법 기구의 통계에 따르면, 2017년에 1,042건의 사이버 공격 사건이 접수되었으나, 2018년에는 1,286건이 접수됨에 따라 코스타리카 내의 스캠 메일 발송 범죄는 증가 추세에 있는 것으로 나타남

▶ 코스타리카에서 가짜 뉴스를 유포할 경우, 1년~4년의 형을 받도록 법 개정이 추진되고 있음(2019.1.6.)

- 급증하는 코스타리카의 사이버 범죄에 대응하기 위해 기독사회통합당(Partido Unidad Social Cristiana)의 Erwen Masis 의원은 의안파일 21.187로 가짜 뉴스를 유포하는 사람에게 1~4년의 징역형을 구형하는 법안을 발의
- Masis의원의 설명에 따르면 이 법은 표현의 자유를 억압하는 것이 아니며, 가짜 뉴스가 유포되는 상황에 대한 법적 질서를 세우기 위한 것이며, 이 법을 지지하는 사이버 범죄 전문가인 Adalith Medrano 변호사는 이 법이 정치인 등을 조롱하거나 패러디하는 컨텐츠에는 적용되지 않을 것이라고 밝힘
- 이 법에서 정의한 사이버 범죄는 컴퓨터 사기(징역형 2~6년), 데이터 위조에 의한 잘못된 페이지로 유도하는 스푸핑(1~3년), 사이버 학대(6개월~3년), 아동 포르노의 제작과 유포(4~8년), 불법적인 신용카드나 현금카드의 구매와 사용(2~5년) 등임

▶ 미국 워싱턴에서 개최된 가상공간의 협력과 신뢰 구축 조치를 위한 워킹그룹(Working Group on Cooperation and Confidence Building Measures in Cyberspace)에 코스타리카 정부 대표 참여(2019.2.28.)

- 미주 대륙의 국가들로 구성된 이 워킹 그룹에 참여하는 국가들은 사이버 공간의 신뢰 구축을 위한 현재의 프레임 워크를 검토하고 신뢰를 제고하기 위한 다양한 조치를 논의
- 코스타리카 정부는 OAS/CICTE 사이버보안 프로그램의 일환으로 사이버 보안 훈련 프로그램을 조직하겠다는 계획과 함께, 이 프로그램에 참여하는 학생들은 주로 저소득층에서 선발하겠다고 발표

▶ 코스타리카 대표단이 국가 및 지역 수준에서 발생하는 사이버 범죄의 유형을 파악하고 관리하기 위한 CSIRT 지역 회의에 참여(2019.5.19.)

- 주요 사이버 범죄 사건의 유형이나 사이버 공간 속의 범죄 흔적 등에 대한 각국 사법기관의 의견을 교환하고 이에 대응하기 위한 미주 각국의 경험을 축적하기 위한 논의임

5) 정보보호 스타트업 관련 정책동향

▶ IBM, 2,100만 달러를 투자하여 코스타리카에 글로벌 IT보안서비스센터 설립 계획 발표(2019.2.11.)

- 130여개 국 고객사들의 보안사고 모니터링을 우선 수행하고, 향후 침해사고 대응, 포렌식 등의 업무로 확장할 계획으로, IBM은 2004년에 코스타리카 에레디아 지역에 소규모 고객 서비스 센터를 구축하여 운영 중에 있으며, 이를 확충해 코스타리카 센터를 중남미 지역에서 가장 큰 사이버보안 서비스센터로 만들 계획
- Microsoft가 지난 2018년에 사이버 보안 관련 주요 시설을 코스타리카에 확충하겠다는 계획을 발표한 이후, IBM도 이번 계획을 발표함에 따라, 코스타리카가 향후 중남미 사이버보안 허브로 성장할 계기가 마련됨

융합보안시장 및 정책 동향

1) 융합보안시장 동향

사물인터넷(IoT)

▶ 코스타리카 전력업체, IoT 기반 스마트그리드 사업 전개

- 2018년 11월 코스타리카의 전력 업체인 Conelectricas가 사물인터넷(IoT) 솔루션을 도입하여, 이를 활용한 스마트 그리드(Smart Grid) 사업에 나선다고 발표
- 해당 사업 계획에는 미국 유틸리티 솔루션 업체인 Itron이 제공하는 IoT 솔루션을 도입하고, 향후 5년간 2만 5,000개의 스마트 계량기(meters)를 보급하는 사업이 포함

스마트의료

▶ 코스타리카 의료 업계, 디지털 파일 형태의 건강 데이터 공유

- 코스타리카 종합병원인 Ebáis를 비롯해서 의료기관간 EDUS (Unique Digital Health File)가 가동되고 있는데, 헬스센터는 적절한 환자 치료에 필요한 정보를 공유받을 수도, 할 수도 있고, 환자 스스로 몇 시간 내에 검사 결과 확인 가능

블록체인(가상화폐 포함)

▶ 암호화폐가 합법적 임금 지급 수단으로 인정되며, 확산 여건 조성

- 2018년에 암호화폐가 정식으로 임금 지불수단으로 인정되면서, 코스타리카에서 암호화폐의 이용 기반이 급속하게 확산되고 있다는 현지 언론 보도가 제기
- 이는 코스타리카 중앙은행의 2017년 10월 지침에 따르면, 암호화폐는 기존의 공식적인 은행 시스템에서 벗어나 있다는 점에서 금융당국의 우려가 있는 것도 사실
- 다만, 급여의 일부가 현금이 아닌 다른 형태로 지급되는 것은 불법이 아니기 때문에, 여전히 임금 지불 수단으로 암호화폐가 활용되는데 문제가 없음
- 이미 다수의 비트코인 ATM 기계가 이미 코스타리카에 존재한다는 점도 암호화폐가 코스타리카에서 확산될 수 있는데 유리하게 작용할 것으로 예상

핀테크 등

▶ 핀테크 등 금융산업의 디지털 전환 분야 선도 국가로 부상할 잠재력 보유

- 코스타리카가 중남미 핀테크 산업을 선도할 국가로 잠재 받는 이유는 ▲풍부한 고등 교육 인력, ▲낮은 인건비, ▲안정적 거시 경제 구조를 갖추고 치안과 사회적으로 라틴아메리카에서 가장 안전한 국가 중 하나이기 때문임
- 현재 온라인 결제, 대출 및 상거래와 같은 실질적인 금융 서비스를 수행하는 핀테크 분야 메이저 전문 업체는 7개 정도에 불과
- 다만, 코스타리카 주요 금융기관들은 핀테크 전문 업체와 제휴를 기반으로 관련 기술 및 플랫폼 개발에 투자 할 의사가 있는 것으로 알려짐

2 융합보안정책 동향

스마트시티

▶ 카르타고시, 스마트시티로의 도약을 위한 5개년 계획 발표

- 지난 2016년 7월 카르타고주의 주도인 카르타고시가 2021년까지 스마트시티로의 도약을 위한 5개년 계획을 추진한다고 발표
- 이는 코스타리카에서 개별 도시 차원에서 최초로 추진하는 스마트시티 프로젝트로서, ▲IT인프라 현대화, ▲공공장소 무료 인터넷 제공 등이 주요 내용으로 포함

스마트의료

▶ 비도심 지역 시민들을 위한 원격 진료와 텔레메디슨 범위 방침

- 코스타리카에서는 농촌 또는 비도심 지역 트라우마 환자 치료를 위해서, 산호세 소재 Trauma Hospital와 실제 환자 거주지간 원격 및 텔레메디슨(Telemedicine) 서비스가 시도됨
- 코스타리카 의료보건 당국은 정형 외과, 안과 및 피부과 등 의료 서비스 수요가 많은 전문 분야에서도 원격 진료와 텔레메디슨을 허용할 것이라는 입장

다. 도미니카공화국

'18년 GDP(십억달러)	81.30
'18년 인구수(천명)	1,0630

■ ITU 글로벌 사이버보안 지수(Global Cybersecurity Index, GCI)

· 도미니카공화국의 사이버보안 지수는 0.430으로 세계 중위권 수준을 유지

국가명	2018		2017		전년대비 증감	
	지수	순위	지수	순위	지수	순위
도미니카공화국	0.430	92	0.162	122	+0.268	+30
대한민국	0.873	15	0.782	13	+0.091	-2

■ ICT 관련 주요 지수

· 도미니카공화국의 전반적인 ICT 발전 수준 역시 전 세계 중위권 수준에 해당

지표명	도미니카 공화국		한국	
	점수	순위	점수	순위
IMD 국가경쟁력지수(2019)	-	-	-	28
IMD 디지털경쟁력지수(2019)	-	-	-	10
UNCTAD 전자상거래지수(2019)	60.4	67	89.4	19
ITU 글로벌 사이버보안 지수(GCI 2018)	0.430	92	0.873	15
UN 전자정부 지수(2018)	0.4914	98	0.901	3

■ ICT 관련 주요 통계 (ITU, 2018년 말 기준)

· 도미니카공화국의 이동통신 보급률은 80%대로 다소 낮은 수준을 보이고 있음

항목	도미니카 공화국		한국	
	가입자수(천 명)	보급률(%)	가입자수(천 명)	보급률(%)
유선전화	1,345	12.49	25,907	50.63
유선브로드밴드	697	6.47	21,286	41.60
이동통신	8,708	80.83	66,356	129.67
인터넷 이용률	61.33%		95.90%	

정보보호 산업 개요

1) 보안 환경

정보보안 환경

▶ ITU가 2017년 4월 발표한 'Global Cybersecurity Index 2017'에 따르면 도미니카공화국의 사이버보안 지수는 0.162로 글로벌 순위는 165개국 중 하위권인 122위로 나타났으며, 아메리카지역에서는 중위권인 22위를 기록

- 도미니카공화국은 국가사이버 보안 체계 등이 갖추어져 있지 않으며 기술 수준은 매우 낮으며 국민의 전반적인 보안 의식도 낮은 편임

▶ Inter-American Development Bank가 발표한 라틴아메리카 및 캐리비언 사이버보안 고찰 보고서(Observatory of Cybersecurity in Latin America and the Caribbean, 2016)에 따르면, 도미니카공화국은 국가사이버 보안 전략이나 사이버 방어 정책은 가지고 있지 않음

- 도미니카공화국은 하이테크 사이버 범죄에 대항하여 정부의 많은 조직이 상호협력을 위해 노력하고 있으나 정부 내의 사이버 보안에 대한 의식은 아주 낮음
- 그럼에도 불구하고 국가 중요 시설의 운영자들은 사이버범죄를 발견하고, 방어하고 이에 대항하는 기초적인 능력은 보유
- 해당 보고서는 도미니카공화국의 보안수준을 정책 및 전략, 문화 및 사회, 교육, 법률 프레임워크 그리고 기술 등의 5개의 분야로 분류하여 각 분야에서 세부 항목별로 5등급으로 나누어 평가함
- 도미니카공화국의 사이버 분야별 수준을 보면 정책 및 전략 분야에서는 국가 사이버 정책, 사이버 방어 등의 능력에서 대부분 가장 낮은 수준인 레벨 1을 기록함
- 그 외 문화 및 사회, 교육, 기술은 대부분의 세부 항목에서 레벨1에서 레벨3까지 수준을 보였으나 법률 프레임 부분에는 여타 분야에 비해 상대적으로 점수가 높은 레벨 1에서 레벨5까지를 기록함

그림 _ 도미니카공화국 분야별 사이버 보안 준비 수준



[출처] Inter-American Development Bank, Observatory of Cybersecurity in Latin America and the Caribbean(2016)

▶ 미국 해외안보자문위원회(OSAC, Overseas Security Advisory Council)에 따르면 도미니카공화국의 사이버범죄는 신용카드 사기가 지속적으로 일어나고 있는데 ATM 카드 위조가 증가하고 있음
- 이러한 사건은 주로 은행 외부, 상점 및 호텔 등에 설치된 ATM 기기에서 보편적으로 발생하고 있음
- 이보다 복잡한 사이버범죄는 흔치 않으나 경찰 역시 이에 대응할 능력은 없는 것으로 평가

▶ 또한 미국 해외안보자문위원회가 주의를 요하는 가장 빈번한 사기 중의 하나는 "조부모 사기"라고 불리는 것으로 주로 도미니카공화국에 친척을 둔 미국인을 상대로 행해지고 있음
- 이러한 사기의 전형적인 유형은 미국대사관 또는 경찰을 사칭하는 사기범들이 미국인에게 전화해서 도미니카공화국에 거주하는 친척이 도움이 필요하다며 송금을 유도하는 경우가 대부분이며 일주일에 몇 건씩이나 미국 경찰에 피해 사례가 보고되고 있음

물리 보안 환경

▶ 물리 보안 영역의 경우, 글로벌 인증기업 UL이 발표한 'UL Safety Index(2017 업데이트)'에서 도미니카공화국은 59점을 기록하며 187개국 중 109위로 평가
- 해당 지표는 ▲각국의 안전 체계(Safety Framework) ▲장애나 사망 추정치 등 안전 관련 수치(safety Outcomes) ▲경제 및 사회적 자원 및 기관(Institutions & Resources) 등의 범주에 따라 각 국가의 안전 수준을 평가
- 도미니카공화국은 곳곳에 범죄가 증가하고 있고, 이로 인해 가정, 사업, 정부가 재산을 지키기 위해 CCTV를 설치하는 추세임
- 이에 따라 새로운 보안 회사들이 생겨나고 있으며, 100개 이상의 회사들이 CCTV 설치와 모니터링 서비스를 포함한 보안 서비스를 제공하고 있으며 정부는 산토도밍고와 산티아고에 911시스템의 일환으로 5,000대의 새 CCTV를 설치함
- 한편, 2013년 12월, 한국 정부는 200대의 첨단 CCTV를 도미니카공화국에 기증한 바 있음

▶ 미국 해외안보자문위원회(OSAC)에 따르면 범죄는 도미니카공화국의 사회 안전에서 해결해야 할 가장 큰 문제임
- 살인 등의 범죄는 Montecristi 및 Bahoruco에서 가장 많이 일어나며(25명/백만 명) 그다음 San Juan 및 Duarte 등의 순으로 발생하고 있음
- 강도 사건은 Santo Domingo City 및 Santo Domingo National District에서 가장 많이 발생하고 있음
- 또한, 성폭력 등의 범죄 역시 Santo Domingo, San Cristobal, Puerto Plata, La Altagracia 및 Montecristi 등의 순으로 발생 빈도가 높으며 데이트 상대에 의한 강간 등도 현저히 증가하고 있음을

보여 줌

- 그 외, 무기 및 약물 등의 보편적인 사용 또한 취약한 범죄 응징 시스템이 높은 범죄율을 불러오고 있음
- 가장 흔한 범죄는 모터사이클, 스쿠터 또는 자전거를 이용한 강도로써 손에 잡히는 대로 피해자의 아무 물건이나 잡아채 달아나는 것으로 심지어 범죄자들은 피해자에게 멈춰서 귀중품을 요구하기도 함
- 자문위원회는 이러한 범죄의 표적이 되지 않으려면 여행자는 귀중품을 지참하지 않으며 간혹 범죄를 피하더라도 범죄자가 재차 주변을 서성거리며 범행을 시도하는 것에 주의하도록 경고함

ICT 환경

▶ 도미니카공화국 정부는 5.3 전자정부 계획을 세우고 ICT를 이용한 공공 및 민간 부문의 구현과 발전을 포함시킴

- 5.3 전자정부 계획에는 ICT를 통한 ▲시민들의 민주적 참여 ▲저렴한 서비스 ▲ 정부용 기술 프로세스 및 관리 ▲ 투명한 서비스에 중점을 둠
- 전자서명, 새로운 회사의 디지털 등록, 사업체 및 대중교통 이용권 획득을 용이하게 하는 정책 추진

▶ 교육부는 2017년 1월 150개 학교에 55,000명 이상의 학생들에게 ICT 시범 운영을 진행

- 정보통신기술을 갖춘 175곳에 ICT기관 설치, 176개의 도서관, 283개의 사무실 등을 지원하고, 총 6,921대의 교육 지원 장치를 설치함
- 도미니카공화국 교육부의 목표 중 하나는, 효율적으로 서비스를 제공하는 것 외에 공립학교의 학생들에게 새로운 기술을 제공하는 것
- 이를 위해 ▲전문 교사의 수 확장 ▲중소 기업 지원 ▲디지털 시장 장려가 필요한 상황
- 한편 국민들의 인터넷 접근성을 위해 인터넷 서비스에 대한 세금 감면 법안 추진

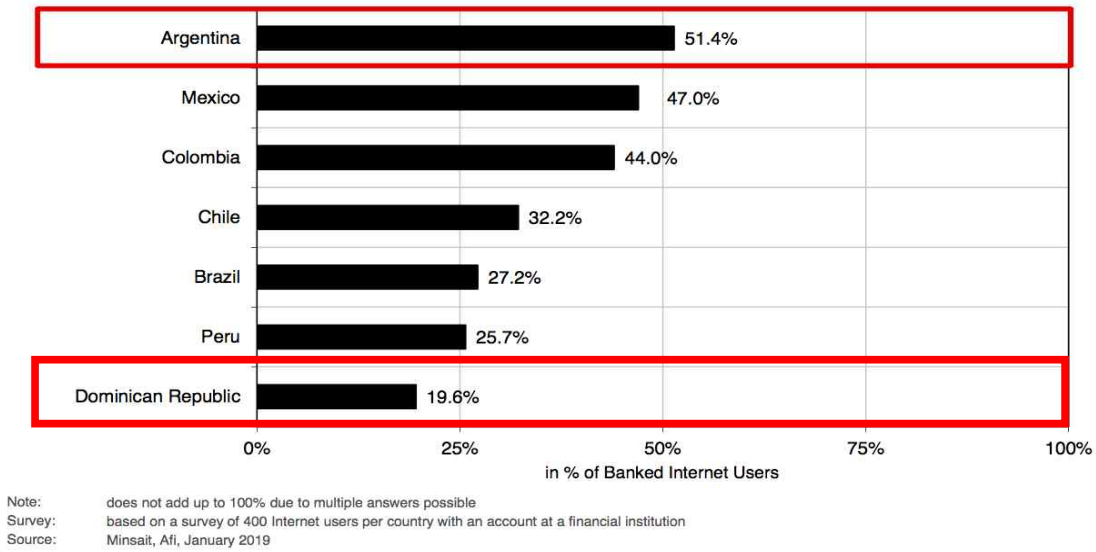
전자상거래 및 결제 환경

▶ 도미니카공화국 3대 통신사 중 하나인 Tricom, 1997년에 아미고 선불 카드를 출시함으로써 최초로 선불 서비스를 제공하였으며, 1999년 CDMA 기술을 사용하여 PCS 서비스를 시작

- 2002년, 은행 계좌 잔액 확인 및 자금 송금, 휴대폰이나 공공요금 등을 지불할 수 있는 모바일 뱅킹 서비스 시작

▶ 2018년 글로벌 전자상거래 조사업체인 yStats.com에 따르면, 도미니카공화국은 매장 내 모바일 결제 애플리케이션을 이용한 인터넷 은행 사용자 비율이 19.6%로 라틴 아메리카에서 가장 낮은 것으로 평가

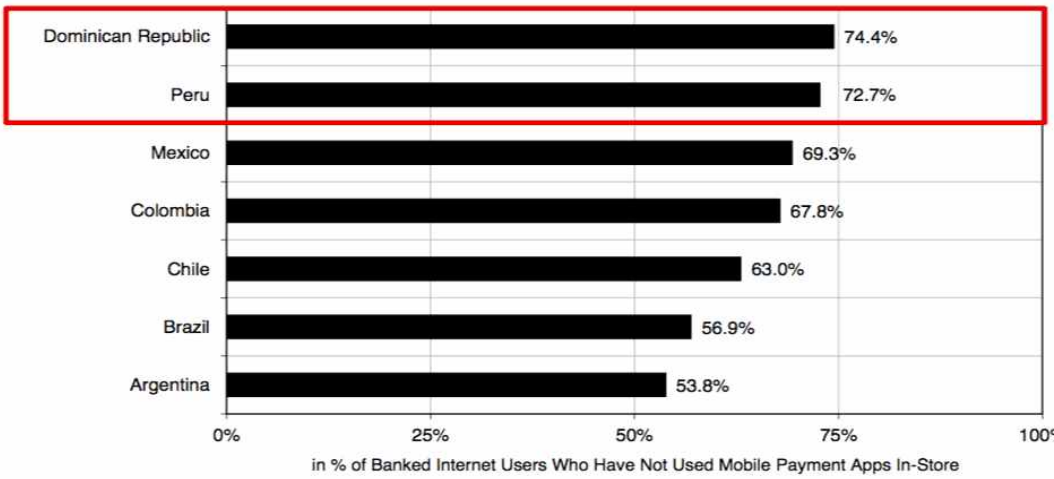
그림 _ 도미니카공화국 매장 내 모바일 결제 애플리케이션 사용자 비율



[출처] yStats.com, e-Commerce in the Caribbean 2018(2018.03)

▶ 2018년 스페인과 중남미의 디지털 및 정보 기술 컨설팅 조사업체인 Minsait가 실시한 설문에서, 도미니카공화국은 모바일 결제 애플리케이션 및 모바일 지갑을 사용하지 않았지만 내년에 사용하려는 은행 인터넷 사용자의 비율이 74%로 라틴 아메리카에서 가장 높은 것으로 평가

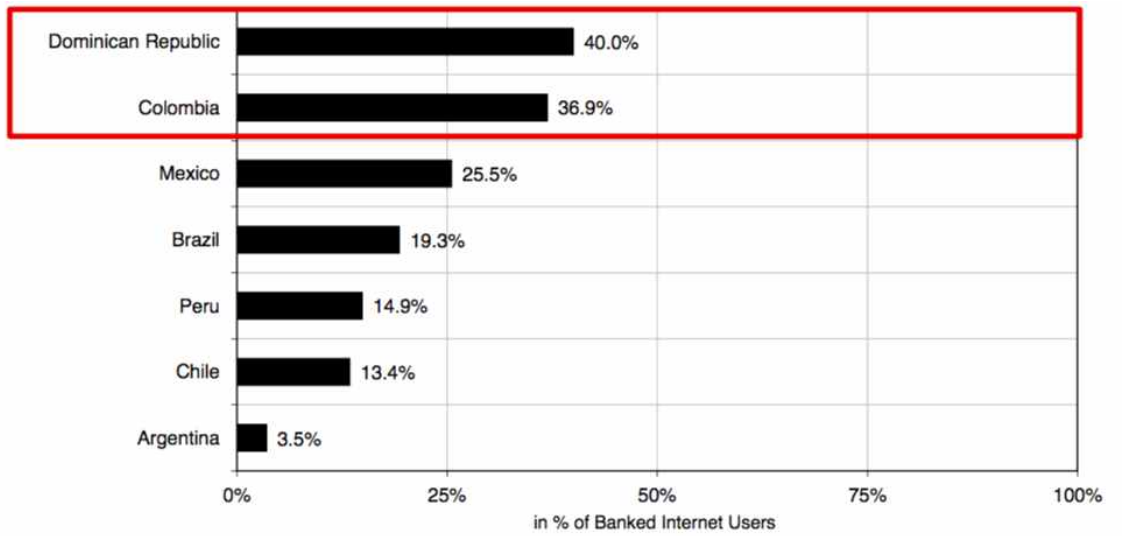
그림 _ 모바일 결제 및 모바일 지갑을 미사용자 중 내년에 사용하려는 은행 인터넷 사용자의 비율



[출처] Minsait, Afi, January(2019)

▶ 2018년 스페인과 중남미의 디지털 및 정보기술 컨설팅 조사업체인 Minsait가 실시한 설문에서, 도미니카공화국은 P2P 모바일 결제 사용자 비율이 40%로 라틴 아메리카에서 가장 높은 것으로 평가

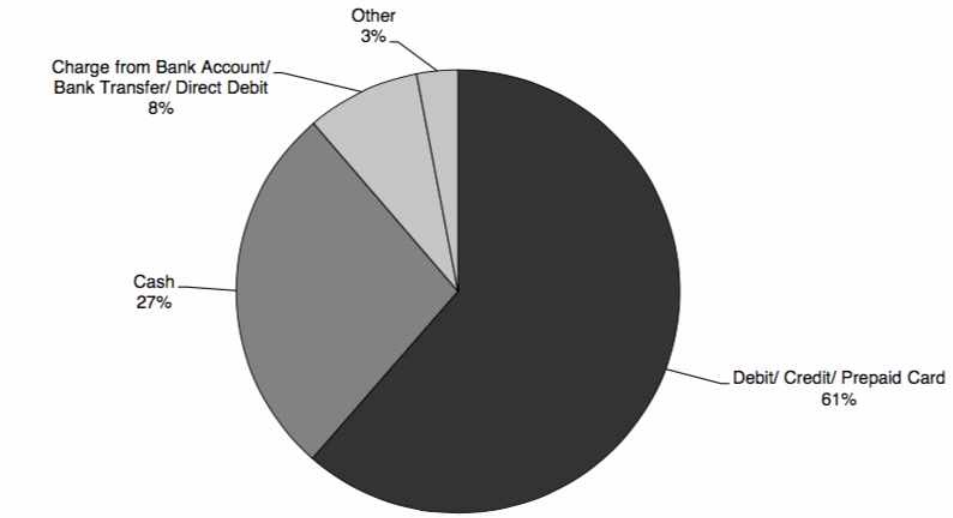
그림 _ 도미니카공화국 P2P 모바일 결제 보급률



[출처] Minsait, Afi, January(2019)

▶ 도미니카공화국은 중남미의 빠르게 성장하고 있는 전자상거래 결제 시장 중 하나로, 2018년 은행계좌를 가진 쇼핑객의 61%가 신용카드 혹은 직불 및 선불 카드로 결제

그림 _ 도미니카공화국 은행 계좌가 있는 온라인 쇼핑객의 비율



[출처] Minsait, Afi, January(2019)

2) 인터넷 및 통신 환경

▶ 국제 마케팅 조사업체 'We are Social'의 Digital in 2019: Dominica에 따르면 2018년 1월 기준 총 1,076만 명의 도미니카공화국 인구 중 실제로 인터넷을 사용하는 인구는 779만 명으로, 이는 전체 인구의 약 79.7%에 해당

- 모바일 가입자는 894만 명으로 보급률은 84.3%이며 모바일 사용자의 44% 정도가 소셜네트워크 서비스를 이용하고 있음
- 모바일을 통한 인터넷 사용인구는 점차 증가하고 있어 2018년 1월 지난해 같은 기간보다 37% 증가했으며 이는 모바일 가입자가 1.5% 증가한 것보다 높은 수치를 나타냄
- 도미니카공화국은 전체 인터넷 사용자의 84%가 소셜미디어 서비스로 페이스북을 사용하고 있으며 컴퓨터나 태블릿으로 인터넷에 접속하는 비율(10%)보다 스마트폰을 통해 인터넷을 접속하는 비율(90%)이 월등히 높음

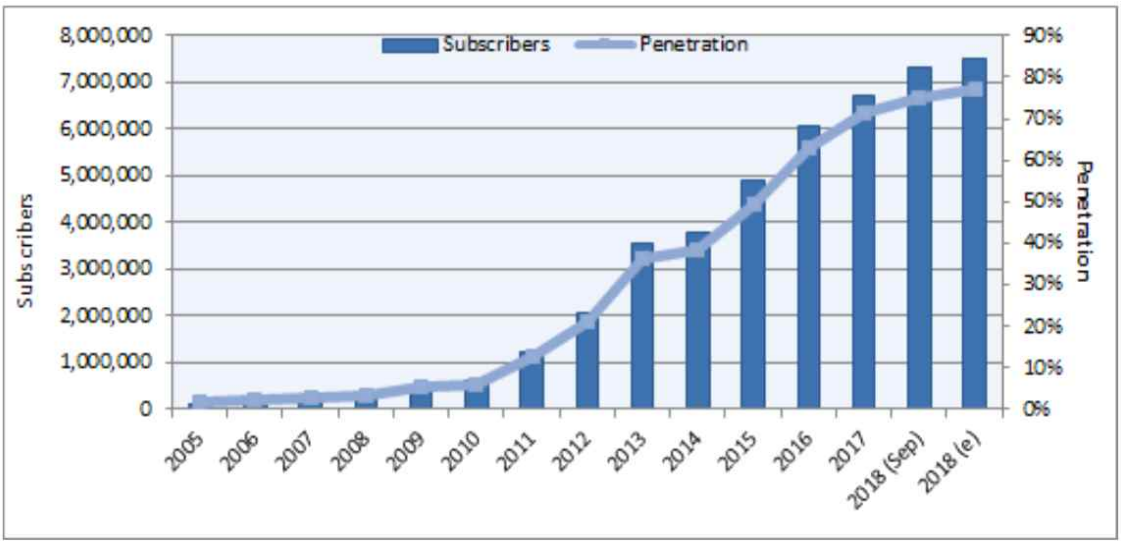
▶ 소셜미디어 통계사이트인 Social Media Stats Worldwide에 따르면 도미니카공화국의 소셜네트워크 서비스 이용은 Facebook 사용이 1위(73.9%)로 가장 많으며 이어서 Linkedin 2위(31%), Instagram 3위(20%), Twitter 4위(7.9%) 등이 그 뒤를 따름

▶ 글로벌 ICT 시장조사업체인 Buddecomm에 따르면, 도미니카공화국의 인터넷 이용률은 2011년 41.4%에서 2017년 73.2%로 증가함

그림 _ 도미니카공화국 인터넷 사용인구 추이

Year	Total users	Penetration
2010	3,851,280	39.5%
2011	4,120,000	41.4%
2012	4,550,000	46.3%
2013	5,220,000	49.4%
2014	5,450,000	54.3%
2015	6,054,000	59.8%
2016	6,266,000	66.3%
2017	6,993,670	73.2%
2018 (e)	7,790,000	79.7%

Source: BuddeComm based on Indotel data and BuddeComm estimates



[출처] BuddeComm based on Indotel data and BuddeComm estimates (2018.11.15.)

▶ 도미니카공화국의 온라인상거래 이용자는 은행계좌를 가진 인터넷 이용자의 61%가 온라인 구매를 경험한 것으로 조사되었으며 이는 2017년 57%에서 4% 상승함

- 2017년 온라인상거래 이용자의 구매 건수는 매주 또는 한 달에 한 건 정도의 구매자가 21%, 3~6개월 한 건 구매자가 42%에 달해 6개월에 한 번 이상 이용하는 이용자가 63%에 달함
- 특히 매주 또는 한 달에 한 건 이상의 이용자는 2016년 15%에서 2017년 21%로 6% 정도 증가하여 빈번한 온라인상거래 사용자가 증가하고 있음을 보여줌

▶ 은행계좌를 보유한 온라인상거래 이용자의 온라인 결제 형태는 페이먼트 카드가 30%로 가장 높으며 계좌이체가 6% 정도인 것으로 조사됨

표 _ 도미니카공화국의 온라인 거래 결제 형태

결제 종류	비중
페이먼트 카드	30.0%
뱅크 트랜스퍼	6.0%
배달 시 현금 지불	1%~10%
직불 카드	1%~10%
여타 결제 수단	1%~10%

[출처] yStats.com, e-Commerce in the Caribbean 2018(2018.03)

▶ 온라인상거래 보안에 관한 설문에서 온라인상거래 이용자는 투팩터 인증에서 SMS 및 텍스트 메시지가 75.4%로 가장 높으며 68.1%는 이러한 이중 보안 체계가 온라인 구매 시 불편을 초래한다고 느낀다고 답함

표 _ 도미니카공화국의 결제 보조인증 방법 및 사용자의 태도

결제 방법/설문자의 두팩터 인증에 대한 태도		온라인상거래 비율
결제 방법	텍스트 메시지/문자	75.4%
	토큰	34.0%
	카드	28.8%
	바이오 인증	3.1%
설문 태도	이중 인증 시 불편하기 느낌	68.1%
	이중 인증 시 결제 지연을 초래	17.3%
	빠른 결제 진행을 위해 이중 인증을 회피 희망	6.8%
	이중 인증은 충분치 않음. 다른 인증 추가 희망	5.2%
	위의 어느 사항도 해당 없음	2.6%

[출처] yStats.com, e-Commerce in the Caribbean 2018(2018.03)

▶ 도미니카공화국의 온라인 트랜잭션은 2017년 결제 건수는 986만 7,000건으로 92억 도미니카 페소(DOP)[175](약 1억 9,440만 달러)에 달함

- 이는 2014년 591만 3700건, 31억 도미니카 페소에서 3배가량 증가한 규모임

그림 _ 도미니카공화국의 온라인 결제 규모 추이 (2014-2017)

(금액: 백만 DOP, 건수: 천 건)



[출처] yStats.com, e-Commerce in the Caribbean 2018(2018.03)

▶ 도미니카공화국 이동통신 사업자로는 Claro (Améerica Móovil), Tricom, VIVA (Trilogy Dominicana), 3개사가 대표적이며, 이들 3사가 전체 시장의 약 99%를 차지하고 있음

175 도미니카 페소, DOP(Dominican Peso)

- 2017년 기준 Claro (Améerica Móovil)이 475만 8,000명으로 54%의 시장 점유율을 보유한 1위 사업자이며, Tricom(39%)와 VIVA (6%)가 그 뒤를 잇고 있음
- 2018년 2월 제1 이동통신사 Claro는 2022년까지 569억 도미니카 페소(약 122억 달러)를 투자한다는 계획을 밝혔으며 자금은 주로 무선네트워크 및 FTTP 인프라 확장에 사용될 예정임
- 제2위 이동통신사 Altice Dominicana는 네트워크 업그레이드에 330억 도미니카 페소(약 6.9억 달러)를 2022년까지 투자한다는 계획을 밝혔으며 현재 GSM 네트워크로 인구 대비 95%를 커버하고 있음
- 제4위 이동통신사 Tricom은 1992년 도미니카공화국 최초로 선불카드 서비스를 시작했으며 2002년까지는 제2 통신사였으나 점유율이 2002년 22%에서 2016년 3.5%까지로 감소하여 지속적으로 시장 점유율을 잃고 있음. Tricom은 2012년 Altice 그룹에 의해 합병되었으며 여전히 모바일 서비스를 제공하고 있으나 Altice의 유선 서비스 제공을 위한 기반을 제공하고 있는 정도임

그림 _ 도미니카공화국 이동통신 가입자 추이



[출처] BuddeComm based on Indotel data (2018.11.15)

▶ 도미니카공화국 휴대전화 서비스 네트워크 회사는 Claro Dominicana(이전의 Verizon Dominicana)와 Orange Dominicana가 지배하고 있으며, 이들 2사가 전체 모바일 가입자의 약 90%를 관리하고 있음

- 1987년 도미니카공화국에 첫 번째 휴대전화 서비스 네트워크를 시작한 Codetel(Codetel)에 이어, 1988년 센테니얼 도미니카나(Centennial Dominicana)가 서비스를 시작, 1994년 트리콤(Tricom)이 그 뒤를 이음
- 2000년 말, 프랑스 텔레콤이 도미니카공화국에 Orange Dominicana로 진출 이후 2003년까지 거의 30%의 시장 점유율을 확보했는데, 이는 Codetel에 이어 두 번째로 큰 사업자로 자리매김
- 2006년 Orange Dominicana, Tricom, Codetel이 분당 요금과금에서 초당 과금으로 전환하면서

소비자단체들은 청구권 캠페인을 벌이기 시작

- 2008년 VIVA와 Tricom과 같은 소규모 모바일 사업자들의 경쟁력 강화로 가입자 급속하게 증가

▶ 2012년 Orange Dominicana가 1,900Hz 대역을 이용해 최초로 LTE를 구축한데 이어 Tricom도 사업 시작

- 2012년 중반 Tricom은 800MHz와 1,900MHz 대역의 CDMA 1x-EVDO와 LTE용 네트워크 업그레이드 계약을 체결, 2013년 5월 화웨이 싱글을 이용해 LTE 네트워크를 업그레이드함

그림 _ 도미니카공화국 이동통신 가입자 예상 추이 (2019-2023)

Year	Subscribers (million)
2019 (e)	9.21
2021 (f)	9.73
2023 (f)	10.06

[출처] BuddeComm based on Indotel data (2018.11.15)

3) ICT 및 산업 환경

▶ 코데텔(Codetel)이 1995년에 처음으로 인터넷 서비스 제공하기 시작했고, 유로나(Eurona)는 2018년 10월, 20년 동안 위성 광대역통신과 고정 음성 서비스 제공권을 확보

- 코데텔(Codetel)은 시골지역 광대역 프로젝트의 일환으로, 500개 이상의 시골지역 커뮤니티에 인터넷 카페와 기타 공공 와이파이 접속 지점을 배치하였고, 중소기업들이 인터넷 카페나 국제 전화 센터를 설립하기 위해 투자할 수 있도록 돕는 기업가 프로그램도 설립, 이로 인해 최근 몇 년 동안 라틴 아메리카의 나머지 지역에 비해 상대적으로 느리지만 인터넷 사용이 인상적으로 증가

▶ 도미니카공화국 정보통신위원회(Indotel)는 '2009-2011년 개발 프로젝트 비엔날레 계획'을 수립

- 이 프로젝트는 14개의 개별 추진기관에 약 3,200만 달러가 투자되었으며, 전국 100개 학교에 브로드밴드 설치, 비서비스 지역의 광섬유망 구축, 모든 자치단체에 걸쳐 무료 공공 접속을 위한 Wi-Fi 네트워크 개발, 커뮤니티 테크놀로지 구축 등 정보통신기술(ICT) 교육사업이 포함됨
- 위원회(Indotel)가 2007년에 시작한 시골지역 광대역 연결 프로젝트 2단계 핵심 계획 중 하나는 하드웨어, 소프트웨어, 백업 전기 공급 시스템을 포함한 기술 인프라를 제공하는 것뿐 아니라, 508개 非서비스 자치단체에 인터넷 카페를 통한 광대역 접속과 주거 및 공중 전화도 제공하는 것이었음

- 이 계획의 전략은 ICT에 대한 보편적 접근의 장기적 추진에 중점을 두었고, ICT의 발전과 장기적

경제성장과 인적 자본의 발전을 연계시키는 것으로써, 이 프로젝트로 인해 모든 가정에서 5km 이내에 인터넷 접속을 제공하는 것을 목표로 하는 e-도미니칸 전략의 일부가 구성됨

- 위원회(Indotel)가 2010년에 시작한 1억 1,900만 달러의 광섬유 네트워크 프로젝트는 기존에 구축된 파이버 네트워크와 상호 연결하여 시골지역에 광대역 및 전화 서비스를 제공하는 것으로써, 세계은행이 재정적인 지원을 함

▶ 2012년, 도미니카공화국 정보통신위원회(Indotel)는 광대역통신 서비스가 불가능한 나머지 시골 지역으로 확대하는 것을 목표로 하는 프로젝트에 다수의 지역 사업자들과 협력하기 시작

- 이 프로젝트는 지역에 광대역 접속을 제공하려는 인도텔의 이전 노력을 보완함으로써 인터넷 교환소(DANIX)설립이 최대 성과
- 이 교환소는 국제 경로를 거치지 않고도 한 ISP에서 출발한 인터넷 트래픽이 다른 지역 ISP의 네트워크에서 종료되도록 허용되는 것으로써, 3개의 ISP(LIME, Marpin 2K4, SAT Telecommunications)는 규제 기관 및 미국 기반의 패킷 클리어닝 하우스와 협력함

▶ 2002년 중반 네트워크트리콤의 자회사인 텔레케이블 드 트리콤(Telecable de Tricom)은 인터넷 토네이도라는 이름으로 케이블 모뎀 광대역통신 출시

- 2018년 6월 기준 케이블 가입의 88%를 차지하며 도미니카공화국에서 선도적인 케이블 광대역 공급업체로 자리매김
- 기업 고객을 위해 ADSL와 결합된 와이파이 서비스인 인터넷 터보 와이파이를 제공하기 시작

▶ 도미니카공화국, '바이엔에이 개발 프로젝트 2009- 2011' 착수

- 2010년 초, 규제기관은 전국 100개 이상의 지역에 무료 Wi-Fi 핫스팟을 설치하기 시작했으며, FDT의 자금 지원(약 35만 달러)과 '바이엔에이 개발 프로젝트 2009- 2011'의 일부를 구축
- 3,200만 달러를 투입해 공공 장소에서의 인터넷 접속을 위한 Wi-Fi 네트워크 개발

▶ 2016년 '도미니카공화국 디지털' 프로젝트 수립

- 시골지역과 가난한 지역의 통신을 향상시키는 것을 목표로 공공 지역에 무료 와이파이 핫스팟 5000개를 설치하는 것이 목표
- 산토도밍고에서 시작하여 Wi-Fi보다 더 먼 거리에서 더 빠른 속도로 사용할 수 있는 무선 네트워킹 기술인 와이맥스WiMAX(Worldwide Interoperability for Micraw Access)네트워크를 통해 VoIP 서비스를 개시하여 점차 그 외 지역으로 확산

▶ 2010년, 도미니카공화국 3번째 규모의 상용 와이맥스 제공업체 윈드 텔레콤은 2.5GHz 대역으로 LTE

테스트 시작

▶ 2013년 10월, 윈드 텔레콤은 모바일 네트워크를 LTE 기술로 업그레이드하기 위한 (2.5-2.7에서 주파수 사용) 2,700만 달러 투자 계획 발표

그림 _ 도미니카공화국 장치별 인터넷 가입자 추이

Year	Dial-up	DSL	Cable	WiMAX	Fibre
2011	11,450	388,230	13,310	20,710	-
2012	8,320	421,360	23,290	37,800	-
2013	5,795	449,960	32,510	43,270	-
2014	4,375	504,140	46,280	45,380	-
2015	3,880	488,090	72,700	56,590	-
2016	3,320	474,910	114,370	63,870	-
2017	3,230	474,140	145,050	62,010	132,610
2018 (Jun)	3,070	447,650	156,650	52,600	163,790

[출처] BuddeComm based on Indotel data (2018.11.15)

정보보호 시장 현황

1) 시장 규모

시장 개요

▶ 물리 보안 영역에서는 도미니카공화국 곳곳에 범죄가 증가하고 있어 앞으로 CCTV의 수요는 몇 년간 증가할 것으로 예상됨

- 치안 등의 사회적 문제를 해결하기 위해서는 오랜 기간이 필요한데다가, 도미니카공화국과 같은 개발도상국에서는 기술안보에 대한 수요가 지속될 여지가 많기 때문임
- 실제로 도미니카공화국에서는 산업용, 교육용, 의료용, 방재용 등 다양한 분야에서 CCTV의 수요가 증가하고 있음

▶ 글로벌 보안 기업인 Symantec이 발간한 LATIN AMERICAN+CARIBBEAN CYBER SECURITY 보고서에 따르면 도미니카공화국의 가장 빈번한 사이버범죄는 증가 추세임

- 신용카드복제, 이메일 및 소셜네트워크를 통한 명예훼손, 디지털 인증 도용, 피싱 및 전화를 이용한 사기 등임
- 또한 정부 웹사이트에 대해 해커 그룹에 의한 수많은 사이버 공격이 있었음

시장 규모 및 전망

▶ 미국 상무부 국제무역청(International Trade Administration)에 따르면, 도미니카공화국 안전 및 보안 산업은 1970년대 초 시작되었으며 현재 190여 개 기업이 경비보안. 모니터링 및 보디가드 등을 포함한 보안 서비스를 제공하고 있음

- 지난 10년간 도미니카공화국은 심각한 범죄 증가를 경험했으며 시민들은 국가 경찰력이 자신들의 자산과 생명을 지키기에는 부족함을 인식하고 있어 결과적으로 이는 도미니카공화국의 사설 보안 서비스의 성장을 가져옴
- 물리보안 회사는 지난 5년간 25% 정도 증가했으며 특히나 지난 1년 사이 많은 기업이 안전 및 보안 장비를 판매하고 있음은 주목할 만함

표 _ 도미니카공화국 안전 및 보안 시장 규모 추이

(단위: 백만 달러)

구분	2015	2016	2017	2018(추정)
총 시장 규모	29.7	34	39.2	40.5
총 로컬 제품	0.7	1	1.2	1.5
총 수출	0	0	0	0
총 수입	30	33	38.0	39.0
미국에서 수입	12.9	13.8	14.6	16.1

[출처] 미국 상무부, 국제무역청(International Trade Administration)[176]

▶ 도미니카공화국 치안 문제 및 최근 정부 주도 프로젝트 지속 추진으로 당분간 보안 카메라 수요 증가 전망임

- 치안 불안은 도미니카공화국 내 주요 이슈로 안전과 보안에 대한 수요가 지속 증가하고 있음
- 도미니카공화국에서는 치안 문제 해결을 위해 경비원 고용, 보안 카메라, 금고, 경보기, 전기 철조망과 차단기 등이 일반화돼 있음
- 도미니카공화국 내 치안 불안 때문에 학교, 기업, 정부 기관과 같은 대형 건물들도 시설보호를 위해 다양한 보안제품을 사용함
- 보안 및 치안 제품에 대한 수요는 범죄 증가, 인구 증가, 대규모 주거 프로젝트 시행 등에 따라 변동하나 당분간 지속적 성장 전망임

▶ 도미니카공화국 정부는 통합 공항 비디오 감시 시스템과 대만 정부가 지원하는 911 응급 및 보안 지원 시스템(우리나라의 119 서비스)과 같은 대규모 프로젝트를 진행함

- 도미니카공화국 국토교통연구소에 따르면 2018년 위와 같은 대규모 정부 프로젝트 확장 예정임
- 2014년 5월, 도미니카공화국은 911 긴급 시스템을 수도인 산토도밍고에 설치 개시했으며 동 시스템은 전자보안 카메라, 라디오 및 관련 장비를 포함했으며 향후 유사한 시스템이 여타 지역으로 확대될 것으로 예상됨
- 현재 도미니카공화국 내 약 2,492대의 카메라가 설치되었으며 911은 2018년 한해 600대의 카메라를 추가 설치한다는 계획임

▶ 도미니카공화국 아파트, 호텔, 병원 등 민간 건설 투자액은 2016년 6억 1,770만 달러에서 2017년 전년 대비 11% 증가했으며, 신축 건물 내 보안 시스템에 대한 투자 확대로 이어질 수 있음

176 https://www.export.gov/article?id=Dominican-Republic-Safety-and-Security-Equipment

2) 분야별 현황

물리 보안제품 및 서비스

▶ 도미니카공화국 관세청(Direccion General de Aduanas, DGA)에 따르면 도미니카공화국은 보안 카메라를 전량 수입 중으로 지난 5년간 도미니카공화국 보안 카메라 수입액은 4,960만 달러 규모에 이르며 2017년에는 전년 대비 37% 증가

- 최근 3년간 도미니카공화국 보안 카메라 수입 시장 점유율은 미국이 68.4%로 1위를 차지했고 중국(19.9%), 파나마(3.2%), 푸에르토리코(2.3%), 한국(1.6%) 순
- 도미니카공화국 보안 카메라 수입 규모는 2012년 큰 폭의 수요 증가 이후 2017년 다시 큰 폭의 증가세를 보임
- 보안 및 치안 제품은 주거, 상업시설 건설 시 생명과 안전에 직결된 투자로, 환율과 경기 변동에 비교적 민감하게 반응하지 않고 경제성장과 함께 지속 증가 경향을 보임
- 최대 수출국은 미국으로, 도미니카공화국과 자유무역협정을 맺고 있어 관세율 0%로 수출하고 있음
- 현재 도미니카공화국에서는 카메라 등의 물리 보안 장비에서 Fertec(미국), Dahua(중국), Vivotek(대만), Kocom(한국), AV Tech(대만), Hivision(중국), Samsung(한국) 등의 브랜드가 경쟁 중
- 도미니카공화국에서 보안 카메라 등의 수입에서 관세 외 특별한 수입규제는 없으며 자유무역협정을 체결하지 않은 국가는 20%의 관세 부과함

표 _ 도미니카공화국 보안 카메라 국가별 수입 동향

(단위: 달러)

국가명	2015	2016	2017	5년 누적 총액
미국	6,876,938.83	6,632,764.18	10,421,409.95	33,883,845.42
중국	2,579,536.96	2,701,004.78	2,886,509.34	8,864,156.34
파나마	259,835.53	141,573.97	190,569.53	1,563,702.08
푸에르토리코	47,390.00	545,250.03	140,857.24	1,129,571.25
한국	162,817.58	171,384.22	223,035.99	771,818.89
홍콩	199,454.00	198,897.00	154,415.71	649,951.29
대만	83,742.00	83,779.30	60,702.30	591,682.79
스페인	36,528.34	54,562.80	136,137.82	265,160.92
베네수엘라	36,091.70	50,800.24	18,297.81	130,174.14
기타	1,790,229.79	1,718,536.28	2,594,485.41	578,786.45
전체	12,072,564.72	12,298,552.79	16,826,421.09	49,559,249.57

[출처] 도미니카공화국 관세청(DGA)

▶ 저가의 중국산 및 기타 브랜드와 경쟁하기 위해 가격경쟁력과 함께 우수한 품질과 기술경쟁력을 갖춘 제품 공급이 매우 중요하며, 현지 소비자에게 어필 가능한 마케팅 및 최신 기술, 디자인 제품으로 현지 시장을 선도할 수 있는 전략 필요함

▶ 미국 상무부에 따르면, 또한 기술적인 진보는 보안 산업에 대한 접근 자체를 재구성하고 있는데 기존 인력을 이용한 서비스가 전자보안 장비, 알람, CCTV 등을 사용하는 방식으로 대체되고 있음

- 물리보안 시장에서 미국은 알람 시스템과 부품 시장에서 지난 3년간 전체 시장의 45%를 차지해 왔는데 도미니카공화국 업계 관련자에 따르면 제품의 품질 및 A/S 등을 들어 미국제품을 선호하며 가격에 매우 민감함
- 사이버 보안 역시 중요한 한 구성 요소가 되고 있는데 신용카드 관련 보안 소프트웨어 및 사이버 보안 트레이닝 등이 가장 전망을 보이는 분야임
- 시장 전망 측면에서는 신원 인증 및 접근제어 장비, 모니터링 및 제어 장비, 비디오 모니터링, 카메라 경고, 시그널링 단말, 개인보호 단말, 응급 대응 차량, 조사 장비 및 서비스, 그리고 이러한 시스템의 적절한 사용에 대한 관련 트레이닝에 대한 수요가 높을 전망임
- 알람 모니터링 서비스는 도미니카공화국 전역에 걸쳐 60여 개의 기업이 7만 개소에 서비스를 제공하고 있음. 대체로 동 기업의 20%는 자체적으로 무장한 순찰 대응을 하고 있으나 나머지 80%는 관할 경찰의 지원을 받으며 서비스를 제공하고 있음. 이러한 보안 서비스 기업은 규제대상은 아니라 도미니카공화국 무장병력 민간 보안 감독기관에 의해 관리되고 있음

정보보안 제품 및 서비스

▶ 도미니카공화국의 IT 및 정보보안 시장은 많이 공개되어 있지 않았으나 지리적으로 가까운 미국 기업들이 지원하는 것으로 보임

- 마이크로소프트는 도미니카공화국의 보안 프로그램을 운영하는 컴퓨터를 통해 멀웨어 등이 검출되는 보안보고서를 발간하고 있어 기본적으로 도미니카공화국에 보안 서비스를 제공하고 있는 것으로 보임

3) 주요 동향 및 이슈

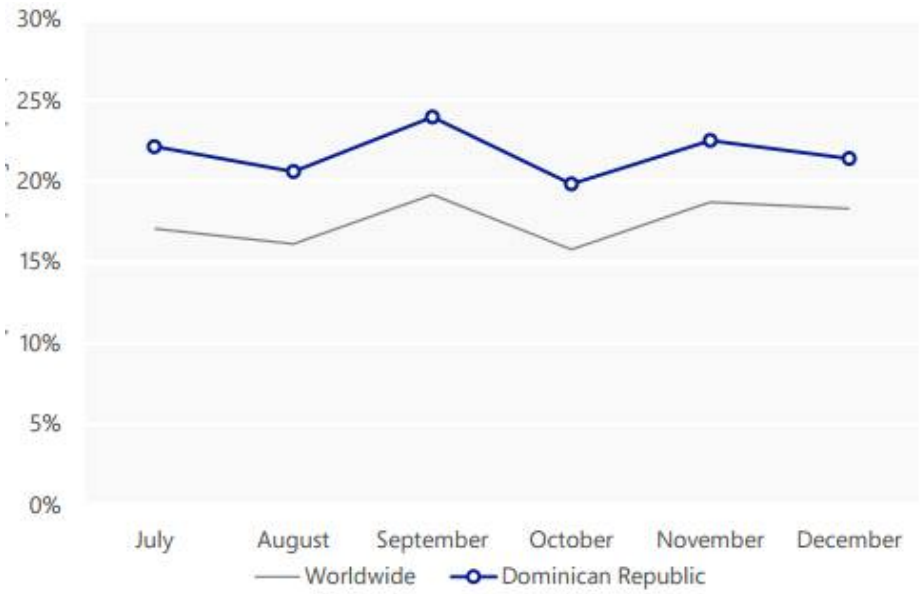
▶ 글로벌 보안 기업인 Symantec이 발간한 LATIN AMERICAN+CARIBBEAN CYBER SECURITY 보고서에 따르면 도미니카공화국의 가장 빈번한 사이버범죄는 신용카드복제, 이메일 및 소셜네트워크를 통한

명예훼손, 디지털 인증 도용, 피싱 및 전화를 이용한 사기 등임. 이 밖에 정부 웹사이트에 대해 해커 그룹들의 수많은 사이버 공격이 있었음

▶ 마이크로소프트 보안 인텔리전스 리포트에 따르면 2017년 12월 기간 도미니카공화국에서 사용되는 컴퓨터의 멀웨어 탐지는 전 세계 평균인 18.3%보다 높은 21.4%를 기록함

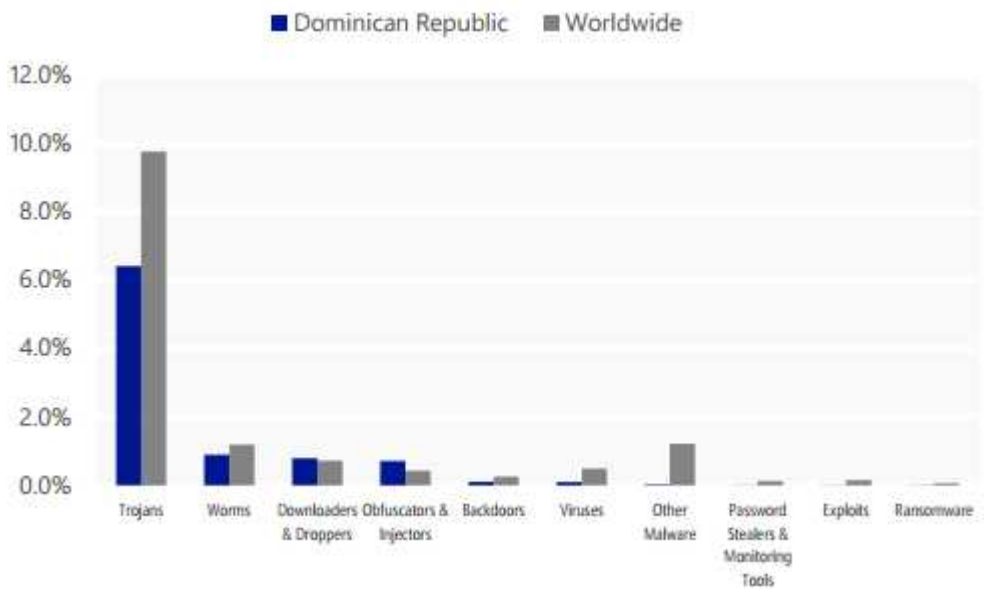
- 아래 그래프의 수치는 도미니카공화국의 컴퓨터에서 동작하는 마이크로소프트 보안 프로그램 및 서비스에 의해 수집되었으며 2017년 7~12월(3개월간)의 멀웨어 발생 추이를 보여줌

그림 _ 도미니카공화국 멀웨어 탐지 추이 (2017.7~12)



[출처] Microsoft Security Intelligent Report(volume 23), 2018.3

그림 _ 도미니카공화국에서 감지된 멀웨어 종류 (2017.7~12)

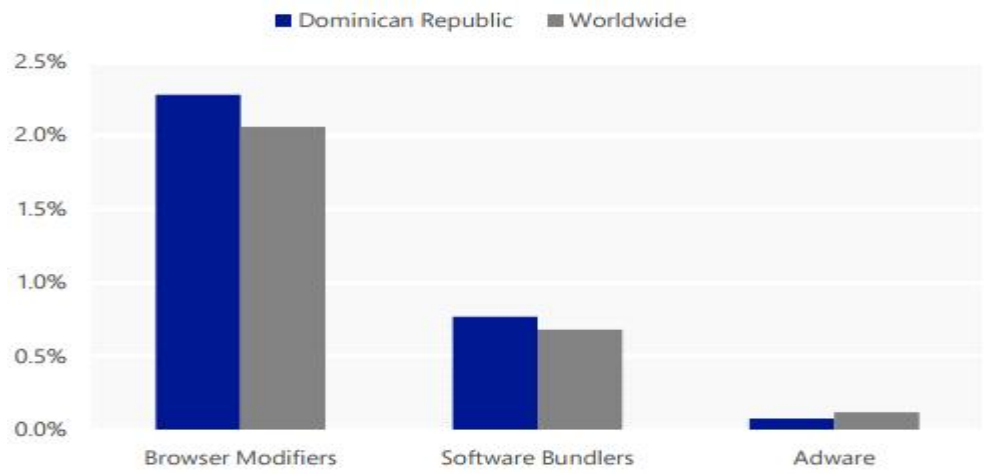


[출처] Microsoft Security Intelligent Report(volume 23), 2018.3

▶ 2017년 하반기 도미니카공화국에서 감지된 가장 공통된 멀웨어는 '트로잔'으로 월 평균 전체 컴퓨터 의 6.42%에서 검출됨

- 2번째로 검출 빈도가 높은 멀웨어는 '웜'으로 전체 컴퓨터의 0.9%3%에서 발견됨
- 3번째로 검출 빈도가 높은 멀웨어는 ' 다운로더 및 드롭퍼(Downloaders & Droppers)'로 전체 컴퓨터의 0.79%에서 발견됨

그림 _ 도미니카공화국에서 감지된 사용자 동의없이 설치된 소프트웨어 종류 (2017.7~12)



[출처] Microsoft Security Intelligent Report(volume 23), 2018.3

▶ 도미니카공화국에서 사용자 동의 없이 설치된(unwanted) 소프트웨어의 종류는 2017년 하반기 기준 웹 브라우저 설정을 변경하는 브라우저 모디파이어(browser modifier)로서 정보를 수집한 컴퓨터의 2.28%에서 발견됨

- 2번째로 사용자 동의 없이 설치된 소프트웨어는 '번들 소프트웨어'로 정보를 수집한 컴퓨터의 0.77%에서 발견되었음
- 3번째로 사용자 동의 없이 설치된 소프트웨어는 '애드웨어'로 정보를 수집한 컴퓨터의 0.08%에서 발견되었음

정보보호 정책 및 기관 현황

1) 관련 법령 및 정책

관련 법령 및 규제

▶ 사이버 보안 법령 Law 53-07, Law 310-13

- 도미니카공화국은 사이버 보안 법령 Law 53-07, Law 310-13을 통과시키면서 사이버범죄, 전자증거 처리, 스팸메일규제 및 국제 사이버 보안 협력 등을 규정하는 전반적인 입법 프레임을 갖추기 시작
- 법령 Law 53-07은 사이버범죄에 해당하는 활동 등을 규정하고 정부가 이러한 범죄를 예방하고 대응할 수 있는 프레임워크를 제공
- 이러한 법령에 근거하여 사이버범죄 조사를 위해 두 특별한 조직이 만들어졌으며, 그 중 한 부서는 법무부 소속 국가 경찰청 산하 첨단 기술 범죄 경찰국(Department for the Investigation of Cyber and High Technology Crimes: DICAT)이고 나머지 한 군데는 국가 수사국의 사이버범죄국(DIDI)임
- 그러나 도미니카공화국은 사이버 보안을 위한 국가 전체를 아우르는 공식적인 조직이나 정책은 없으며 또한 사이버 보안 사고에 대응하는 컴퓨터침해사고대응팀(CIRT, Computer Incident Response Team)과 유사한 조직도 구성되어 있지 않음

주요 전략 및 정책

▶ 2014년 일반법 A1:2014(General Rule A1:2014)을 통해 최초로 ICT의 이용 및 구현에 관한 일반규정을 제정하였으며, 2015년 Indotel과 미국 테러방지위원회(OAS) 간의 협력을 통해 ▲국가 사이버 보안 전략 수립 ▲국가 사이버 보안 구축 및 인식 향상 제고를 실시

▶ 국내 공식적인 사이버 보안 및 국가 대응 전략이 부족한 상태며 외부 정책의 도움을 받아옴

- 2013년에 최초로 사이버 범죄에 관한 부다페스트 협약에 서명
- 이 협약을 통해 범죄 및 첨단 기술 범죄에 대한 기관간 위원회와 첨단 기술 조사 부서 설립 및 주내 사이버 사건 조사 시작
- 사이버 범죄 협약위원회 및 유럽 평의회(T-CY)와 협력하여 국가 정보 보안 및 사이버 인식 캠페인을 조직

▶ 2018-2021 국가 사이버보안 전략 수립(Decreto 230-18, Establece y regula la Estrategia de Ciberseguridad 2018-2021)

• 도미니카공화국 대통령에 의해 대통령 정보 통신 기술국(La Oficina Presidencial de Tecnologías de la Información y Comunicación (OPTIC)) 하에 수립되었으며 주요 전략은 다음과 같음

▲ 법적 프레임워크 및 제도적 강화
▲ 국가 중요 인프라 및 주 IT 인프라 보호
▲ 사이버 보안의 국가 교육 및 문화
▲ 국가 및 국제 연합 강화

• 이는 정보통신 기술에 기반한 정보사회로의 이행에 관한 시책으로써 전략 시행을 위한 방안은 다음과 같음

▲ 인프라 및 접근권 강화
▲ 전자정부 및 디지털 서비스 강화
▲ 생산적 개발 및 혁신
▲ 정보통신 기술 환경 활성화

▶ 도미니카공화국 금융감독원은 2013년 말 선불 이동통신 가입자에게 세부사항 등록을 의무화하는 방안을 도입

• 이 같은 움직임은 모바일 가입자가 위조서류나 허위서류 등으로 대거 등록 가능한 범죄에 대응하기 위한 차원으로 실시

▶ 도미니카공화국은 정보통신 개발, 진흥, 및 규제를 위한 부분별 전략계획 2017-2020을 수립했으며 다양한 이해단체들이 참여해 도미니카공화국의 정보통신 분야 발전을 위한 전략 및 프로그램에 대한 가이드라인을 작성

• 가이드라인은 도미니카공화국의 정보통신 개발, 진흥, 및 규제를 위한 부분별 전략계획 2017-2020으로 최종 명명
• 정보통신 분야의 지속 가능한 개발 계획 및 가이드라인 수립을 목표로 하며, 정보통신 서비스의 지속적인 관리, 질적 향상, 재정 안정성 확보, 기관 간 협업 증대를 주된 목적으로 함
• 현재까지의 활동 내역은 ▲정보통신 분야의 제약(restriction) 및 추진 동력 정의 ▲향후 4년간 진행될 이행 목표 및 실행계획 수립을 위한 비전 제안 ▲부분별 테마 작성을 위한 태스크포스팀(TFT) 구성 ▲부분별 전략계획 2017-2020을 통해 수행된 작업의 연속성 보장을 위한 다자간 태스크포스팀(TFT)을 구성
• 기관 전략계획은 국제적인 기준에 맞춰 부분별 전략계획이 수립될 수 있도록 계획 작성 기관에 필요한

수단을 제공할 것이며 Agenda 2020이나 UN에서 발의한 지속성장발전목표(SDGs, Sustainable Development Goals) 관련 사항이 충실히 이행될 수 있도록 협력

▶ 디지털 공화국(República Digital) 이니셔티브

- 2016년 4월 다닐로 메디나(Danilo Medina) 도미니카공화국 대통령은 숏 국가적인 인터넷 접속과 ICT 기술 도입 확대를 위해 '디지털 공화국' 이니셔티브 추진을 선포했으며 동 이니셔티브는 도미니카공화국 정보통신위원회(Indotel)가 주도함
- 디지털 공화국은 2017년부터 약 95만 학생과 8만 교사들에게 PC 제공을 목표로 하며, 5,600개 학교와 개방형 대학에 소재한 18개 지역 센터에 무료 Wi-Fi 보급을 시행할 계획
- 2020년까지 "모두를 위한 브로드밴드 인터넷"이라는 기치 아래 전국의 70% 지역에 브로드밴드 환경을 구축하고, 국민들이 현재보다 30% 이상 저렴한 가격에 인터넷 서비스를 누릴 수 있도록 함
- 지역 중심 도시를 연결하는 국가 광섬유 네트워크를 배치를 추진

▶ 도미니카공화국 중앙은행은 금융 분야 국가 사이버 보안 정책을 Indotel(도미니카공화국 정보통신위원회)과 함께 협력하기로 함

- 동 협의체는 국가 내외부의 위협에 적절히 대응하기 위한 일련의 가이드라인을 도출할 계획*을 밝힘
  * 2017년 말 시행할 계획이라고 발표하였으나 실제 추진 여부는 미파악

2) 담당기관

▶ 대통령 비서실(Secretary Administrative of the Presidency)

- 대통령의 국정전략 수립.조정, 행정부처 간의 이견 조율, 대통령 비서실과 국무총리실의 역할 등을 담당하며 대통령을 대리하여 국가 정보화 관련 업무를 총괄함
- 대통령령 551-09에 의해 대통령 비서실이 국가 정보화 및 전자정부와 관련된 모든 업무의 총괄을 수행하도록 규정됨

▶ 도미니카공화국 정보통신위원회(Instituto Dominicano de las Telecomunicaciones, Indotel)

- 1998년 통신법 제153-98조에 의해 설립된 통신 규제기관으로 통신 서비스 규제와 촉진 정책으로 도미니카공화국의 통신 분야 발전을 도모
- 도미니카공화국 정보통신위원회(Indotel)는 호세 델 카스틸로 사비넌 위원장을 포함해 6인으로 구성되었으며 주요 기능은 다음과 같음
  ▲ 통신 사업자(유선, 케이블, 인터넷, 라디오) 등에 대한 통신 분야 규제

▲ 주파수 대역의 효율적인 재배치
▲ 통신 사업자들 간의 분쟁 해결
▲ 통신 서비스 사용자들의 정보 알림
▲ 통신 시장 경쟁 촉진
▲ 통신 요금 및 상호 접속 요금에 대한 법규 제정
▲ 통신망의 최소 품질, 기술, 운영 및 기능 호환성에 대한 표준 관리
▲ 통신 장비, 장치 및 통신 시스템에 대한 인증 및 기술 규격 개발
▲ 위성·통신 분야 국제기구 및 조직과의 협력

▶ 대통령 정보통신실(Oficina Presidencial de Tecnologí de Informació y Comunicació, OPTIC)
- 2004년 대통령령 1090-04에 의해 설립된 기관으로 전자정부 전략 수립 및 기반조성, 컨설팅 서비스 제공 등을 수행하는 전자정부 실행 기관
- 동 기관은 전자정부 사업을 위한 기술지원, 범정부 표준 제정 및 법제도 개선, 전자정부 프로젝트 개발, 전자정부 국제협력, 데이터센터가 없는 정부 기관을 위한 IDC 호스팅, 공무원 IT 교육 등을 담당함

▶ 국가정보지식사회위원회(National Commission of ICT)
- 정보지식사회 구현이라는 목표하에 도미니카공화국 국가 정보화 전략 수립과 정보화 분야 조정을 담당. 비상근위원회로 정보통신위원장이 의장직을 수행

▶ DICAT(la Dirección de Crímenes y Delitos de Alta Tecnología de la Policía, 첨단 기술 범죄 경찰국, 법무부 소속기관)
- DICAT는 설립된 후 교육기관에서 사이버 보안 교육을 시행하고 민간과 공공기관을 위한 사이버 범죄 예방 캠페인을 진행했으며 소셜네트워크 등을 통해 사이버 보안 의식을 높이는 캠페인 등도 실시함
- 또한 도미니카공화국 정보통신위원회(Indotel) 등의 여타 기관들과 함께 공공 조직들의 사이버범죄의 위험에 대한 인식을 높이기 위해 'Healthy Internet' 같은 캠페인을 실시함
- 또한 대학에서 사이버 보안 관련 강의 부족 등을 해결하기 위해 정부는 산토도밍고 기술 연구소와 파트너십을 맺고 관련 강의 및 인증 프로그램 개발을 위해 노력하고 있음

3) 규제 및 인증제도

▶ 도미니카공화국은 보안제품에 대한 특별한 규제 및 인증을 취하고 있지 않는 것으로 보임

4) 최근 정책 동향 및 이슈

▶ 도미니카공화국 정보통신위원회(Indotel), 사이버 보안 프로세스 정립 발표(2017.6)

- 2017년 6월, 도미니카공화국 Indotel 회장 조세 델 카스틸로는 2017년 9월 목표로 사이버범죄를 예방하기 위해 사이버범죄 규정, 신고 등의 프로세스에 관한 국가 사이버 시큐리티를 개시할 것으로 발표함
- 본 계획은 도미니카공화국의 영국 상공회의소가 주최한 "현대사회의 보안 위험" 포럼에서 공개됨
- 이를 위해 사이버 보안 사고 대응센터(Cyber Security Incident Response Center: CSIRT)가 수립되고 모든 웹 공격으로 영향을 받는 모든 민관기구는 본 센터와 협력할 것임을 언급함
- 또한 센터는 대중에게 사이버 보안 문화를 심어주고 한순간에 인터넷상에서 공격 대상이 될 수 있다는 인식전환이 필요함을 강조함

▶ 도미니카공화국, 미주기구(Organization of American States, OAS)와 사이버 보안 정책 개발 지원 합의(2017.5)

- OAS 사무총장 루이스 알메그로는 2015년 이후 스페인어를 사용하고 있는 카리브해 지역의 사이버 능력을 강화하기 위해 노력하고 있으며 이러한 MOU를 통해서 개방적이고, 접근할 수 있는 확고한 디지털 도미니카공화국을 만들기 위해 정부를 지원하는 것이 큰 의미가 있다고 언급함
- 정보통신위원회(Indotel) 회장 조세 델 카스틸로는 이러한 합의를 통해 도미니카공화국은 IT 정보기술에서 안전하고 방어적인 체계를 구출할 방법을 도출할 예정이라고 밝힘
- OAS는 테러리즘에 대항한 인터-아메리카 위원회의 사이버 시큐리티 프로그램을 통해 카리브해 지역의 국가 사이버사고 대응팀(CSIRT)의 구축을 지원하고 있음

융합보안시장 및 정책 동향

1) 융합보안시장 동향

스마트시티

▶ 도미니카공화국은 FITUR 2019박람회에서 동해안에 위치한 Bávaro-Punta Cana(바바로 푼타 카나)지역에 첫 스마트 시티를 조성할 것을 발표

- 여기에는 천연 가스 발전소의 85 메가 와트 및 138KW 전력선의 무효 전력 보상기가 포함
- The Consorcio Energético Punta Cana–Macao(CEPM)의 최고 경영진들은 Energy Consortium2019에서 이 지역을 스마트 시티로 성장시키기 위해 전기 그리드, 지능형 그리드, 지능형 플랫폼을 개발하고 있으며 스마트 네트워크와 미터기를 통해 24시간 동안 33,000 명 이상의 주거 고객과 72개 호텔에 전력을 공급 계획을 발표

▶ 2019년 2월 산티아고 전략 개발 협의회 (CDES)와 산토 도밍고 기술 연구소 (INTEC)는 산티아고를 스마트 시티로 만들 "Santiago, Smart City"를 발표

- 혁신적이고 지속 가능한 솔루션 구현을 위한 공공-민간 파트너십 추구가 핵심
- 이는 남미 개발 은행과 다자간 투자 기금 (IDB-MIF)의 후원으로 산티아고와 산토 도밍고에서 동시에 시행 될 "도미니카 도시 혁신 및 영토 정보 연구소"프로젝트의 일환

블록체인(가상화폐 포함)

▶ 도미니카공화국 중앙은행은 도미니카 법에 따라 가상통화는 법정 통화가 아니며 따라서 가상통화에 지원하지 않음을 명시

- 다만, 국가에서 영업을 허가받은 금융기관에 한해 가상통화 거래가 가능하며, 어떠한 위험에 대해서 국가는 책임을 지지 않음을 명시

▶ 비트코인 수요가 증가함에 따라 2016년에는 수도 Santo Domingo(산토 도밍고)에 Bitcoin ATM이 설치됨

- 해당 Bitcoin ATM으로는 비트코인과 현지 통화 교환은 불가하지만 비트코인 구매는 가능하며, 송금 시스템 추가를 고려 중
- 이후 암호화폐거래소 BitRD가 Santo Domingo에 2대의 Bitcoin ATM을 추가 설치했으며, 해당

기기에는 도미니카공화국 화폐 페소(Peso) 및 미국 달러 교환 기능이 추가됨

▶ 도미니카공화국 내 비트코인 이용률은 현저히 낮은 수준이며, 비트코인 결제 가능 소매 업체도 거의 없음

핀테크 등

▶ 전자상거래, 소셜 네트워크 및 전자 플래폼 개발에 대한 수요가 증가함에 따라 2018년 5월 도미니카 핀테크 기업 협회(ADOFINTECH)는 19개 기관과 통합 출범

▶ Fintech Latin America 2018: Growth and consolidation 보고서에 따르면 핀테크는 도미니카 공화국에서 백만 명의 사용자가 이용 중이며, 평균 1,200 만 건의 월간 거래를 발생시킴에 따라 빠르게 성장하는 산업이라 평가

- 도미니카공화국 중앙은행의 데이터에 따르면 2019년 1월~3월 분기 동안 1,745,372개의 현지 은행 거래가 온라인으로 이루어졌으며, 온라인을 통한 국제 상품 및 서비스가 같은 기간 동안 7,147,110건에 도달했다고 밝힘
- 도미니카공화국 현재 가장 큰 핀테크 사업 중 하나는 전자 지갑 및 은행 계좌 수집 애플리케이션인 Tpago로 10년 동안 80만 명 이상의 고객 보유

라. 페루

'18년 GDP(십억달러)	222.238
'18년 인구수(천명)	31,989

■ ITU 글로벌 사이버보안 지수(Global Cybersecurity Index, GCI)

· 페루의 사이버보안 지수는 소폭 상승했으나, 순위는 16계단 하락한 95위로 조사됨

국가명	2018		2017		전년대비 증감	
	지수	순위	지수	순위	지수	순위
페루	0.401	95	0.374	79	+0.027	-16
대한민국	0.873	15	0.782	13	+0.091	-2

■ ICT 관련 주요 지수

· 페루의 전반적인 ICT 발전 수준은 ITU 조사국 167개국 중 중위권에 속해 있음

지표명	페루		한국	
	점수	순위	점수	순위
IMD 국가경쟁력지수(2019)	-	55	-	28
IMD 디지털경쟁력지수(2019)	-	61	-	10
UNCTAD 전자상거래지수(2019)	47.8	94	89.4	19
ITU 글로벌 사이버보안 지수(GCI 2018)	0.401	95	0.873	15
UN 전자정부 지수(2018)	0.593	88	0.901	3

■ ICT 관련 주요 통계(ITU, 2017년 말 기준)

· 페루는 유선통신 보급률은 낮은 편이나 이동통신 보급률은 매우 높음

항목	페루		한국	
	가입자수(천 명)	보급률(%)	가입자수(천 명)	보급률(%)
유선전화	3,082	9.8	26,845	52.54
유선브로드밴드	2,310	7.35	21,196	41.48
이동통신	38,915	123.76	63,659	124.59
인터넷 이용률	52.54%(2018년 말 기준)		95.07%	

정보보호 산업 개요

1) 보안 환경

정보보안 환경

▶ 페루의 정보보호 산업 환경은 아직 후진적 구조
- 법적 제도적 정비는 타 중남미국에 비해 양호한 편
  - 정보보호 수요는 증가 추세이나, 자체 기술 수준, 조직적 체계, 역량구축 면에서는 열위 수준으로 제대로 정보보호 활동이 이루어지지 못하고 있는 상황
  - 타 국가와 협력의지도 상대적으로 강한 편이나 아직은 무상원조 성격의 비대칭적 지원을 원하는 입장으로 사업 추진이 원활치 못한 편

▶ ITU에서 평가한 글로버 사이버 보안 종합지수도 낮은 수준
- 중남미 역내 국가 중 9위 그룹에 머물고 있는 낮은 수준 기록[177]
- 쿠진스키 신정부가 국내 치안 및 정보보호 환경을 개선해 나갈 것으로 기대되고 있어 희망적 여건

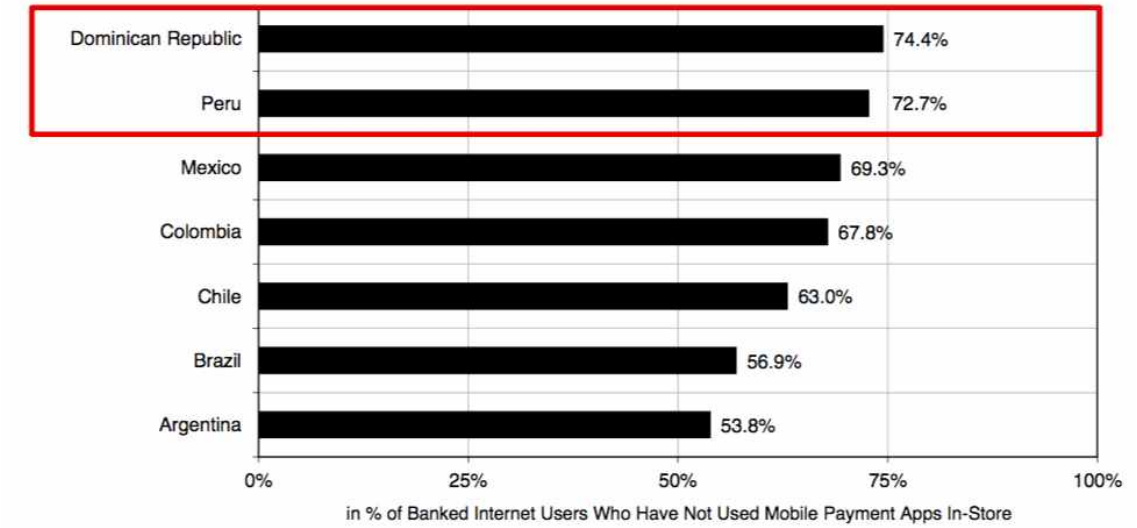
▶ 향후 정보보호 수요는 급격히 증가되어 나갈 것으로 전망
- 마약범죄, 빈부 격차에 의한 민생범죄 등 빈발과 원주민들의 대규모 광산개발 저항 세력화 등 범죄 및 정보보호 수요 저변 급격 확대 추세
- 공공기관 및 광공업 부문 등 대형 민간기업, 일부 부유층 주택 등 전통적인 중남미의 정보보호 수요층 확대 추세로 향후 정보보호 시장이 급격히 성장해 나갈 것으로 전망

전자상거래 및 결제 환경

▶ 2018년 스페인과 중남미의 디지털 및 정보 기술 컨설팅 조사업체인 Minsait가 실시한 설문에서, 페루는 모바일 결제 애플리케이션 및 모바일 지갑을 사용하지 않았지만 내년에 사용하려는 인터넷은행 사용자의 비율이 72%로 라틴 아메리카에서 높은 비율을 보임

177 ITU, Measuring the Information Society Report 2015

그림 _ 페루 모바일 결제 및 모바일 지갑을 미사용자 중 내년에 사용하려는 은행 인터넷 사용자의 비율



[출처] Minsait, Afi (2019.1)

▶ 인터넷은행 사용자 중 매장 직접 할인이 모바일 지갑 이용에 가장 큰 동기부여로, 라틴 아메리카의 인터넷 사용자들은 2018년부터 모바일 지갑을 사용하기 시작함

▶ 부정 행위 방지 조치, 보상 포인트 등은 그 다음으로 소비자들이 매장에서 모바일 결제 애플리케이션을 사용하는데 동기부여가 되는 것으로 나타남

▶ Minsait의 조사에 따르면, 2018년 모바일 지갑에 대한 신뢰 부족이 모바일 지갑 이용률 저조의 가장 큰 장벽(36%) 중 하나로 드러남

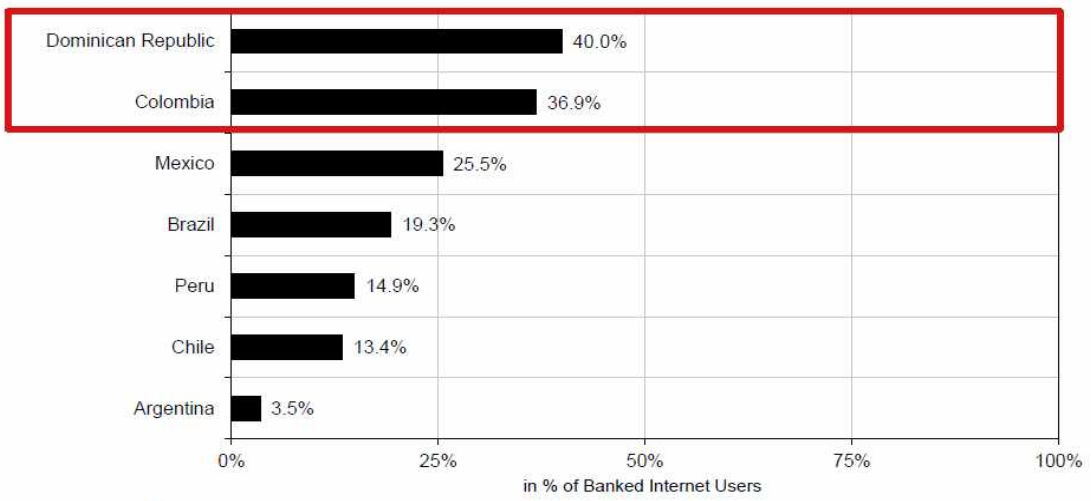
그림 _ 은행 인터넷 사용자 중 모바일 결제 애플리케이션 非사용 사유별 非사용자 비율

in % of Banked Internet Users Who Have Not Used Mobile Payment Apps to Pay In-Store	Colombia	Peru	Mexico	Argentina	Chile	Brazil	Dominican Republic
I do not trust this method	36.6%	36.0%	33.5%	31.0%	27.8%	20.7%	19.6%
I prefer to pay in cash	35.2%	29.7%	23.6%	26.4%	20.9%	22.7%	23.8%
I prefer to pay by card	24.7%	23.3%	21.2%	25.4%	30.8%	31.9%	28.0%
The establishments where I usually shop do not accept this mean of payment	21.6%	28.3%	26.4%	24.9%	23.1%	27.1%	34.6%

[출처] Minsait, Afi (2019.1)

▶ P2P 모바일 결제 사용자, 인터넷은행 사용자 비율은 14.9%로 라틴 아메리카에서 상대적으로 낮은 비율을 보임

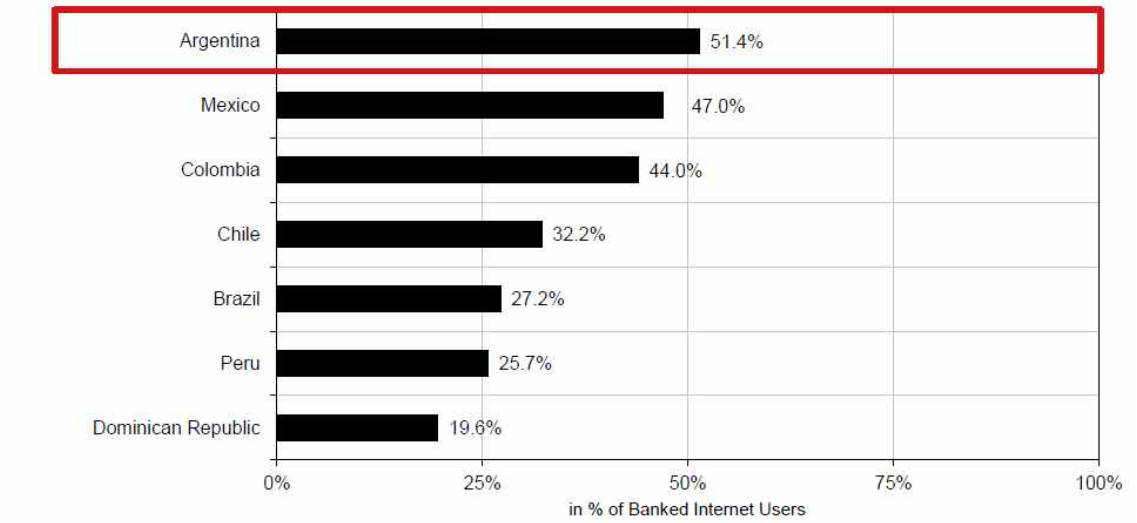
그림 _ P2P 모바일 결제 사용자, 인터넷은행 사용자 비율



[출처] Minsait, Afi (2019.1)

▶ Minsait의 조사에 따르면, 2018년 페루에서 매장 내 모바일 결제애플리케이션을 이용한 인터넷은행 이용자들 비율은 25.7%로 라틴 아메리카에서 상대적으로 하위권에 위치

그림 _ 매장 내 모바일 결제애플리케이션을 이용한 인터넷은행 이용자 비율



[출처] Minsait, Afi (2019.1)

▶ 매장 내 결제용 모바일 애플리케이션은 페루의 인터넷 사용자들에게 가장 많이 알려진 핀테크 서비스(48.5%) 중 하나

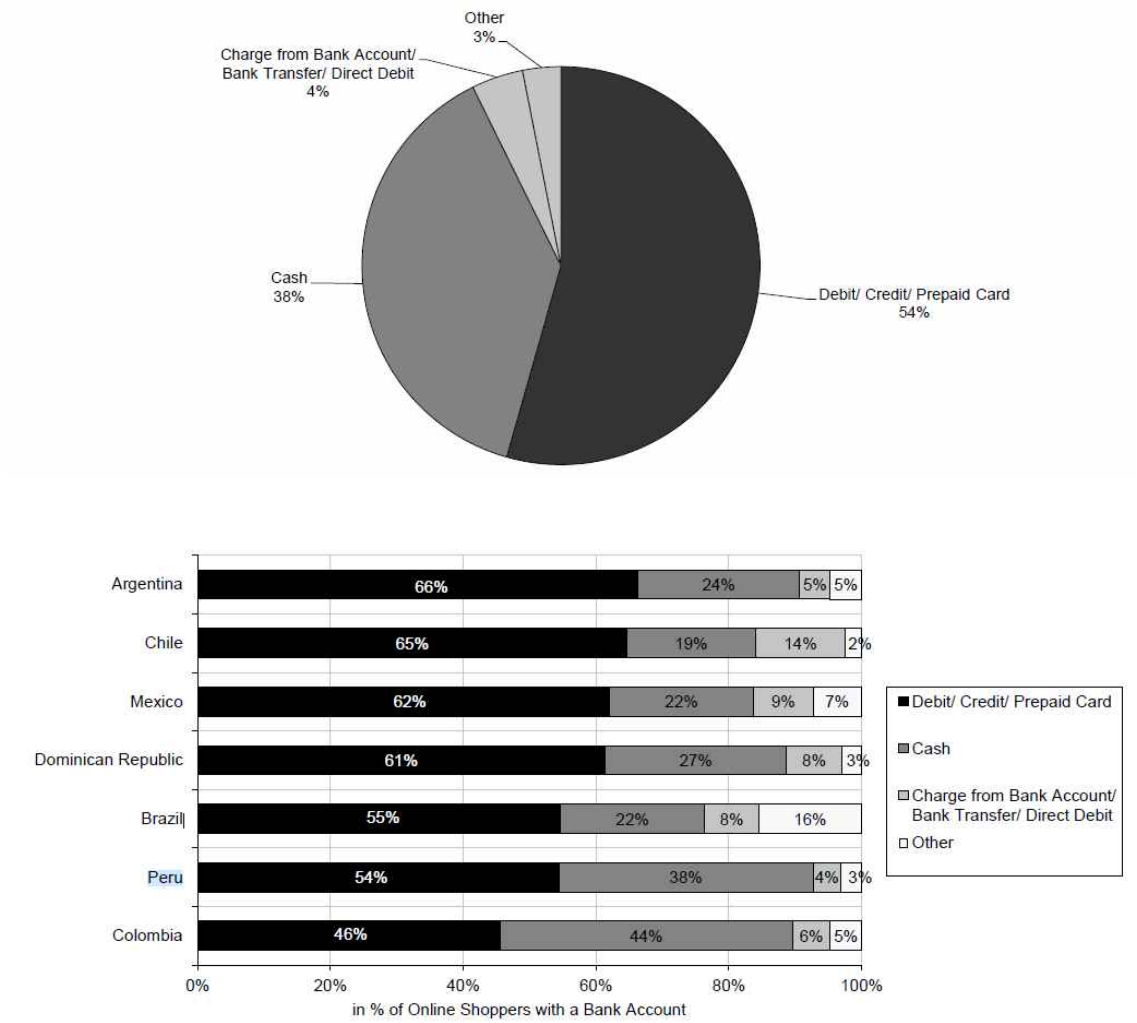
그림 _ 인터넷은행 사용자 중 유형별 핀테크 인식 비율

in % of Banked Internet Users	Argentina	Brazil	Chile	Colombia	Mexico	Peru	Dominican Republic
Mobile apps for in-store payments	70.1%	53.6%	48.1%	62.2%	63.8%	48.5%	44.8%
Cryptocurrencies	46.7%	46.4%	42.9%	53.6%	43.55	41.6%	51.1%
Crowdfunding	14.1%	11.4%	10.4%	10.6%	12.5%	7.2%	6.5%
Mobile P2P payment apps	10.1%	34.6%	24.8%	56.5%	40.0%	32.3%	66.6%
Companies that provide services of sending/ receiving payments in other currencies	5.4%	5.7%	5.7%	6.4%	4.5%	5.2%	17.2%
Financial aggregators	4.4%	7.2%	3.7%	4.9%	4.8%	3.7%	3.9%
Robo-advisors	2.5%	5.7%	1.2%	3.0%	1.5%	1.5%	1.9%

[출처] Minsait, Afi (2019.1)

▶ 2018년 페루에서 은행계좌를 가진 온라인 쇼핑객의 54%가 직불카드, 신용카드 또는 선불카드를 사용했으며, 현금은 38%로 2위를 차지

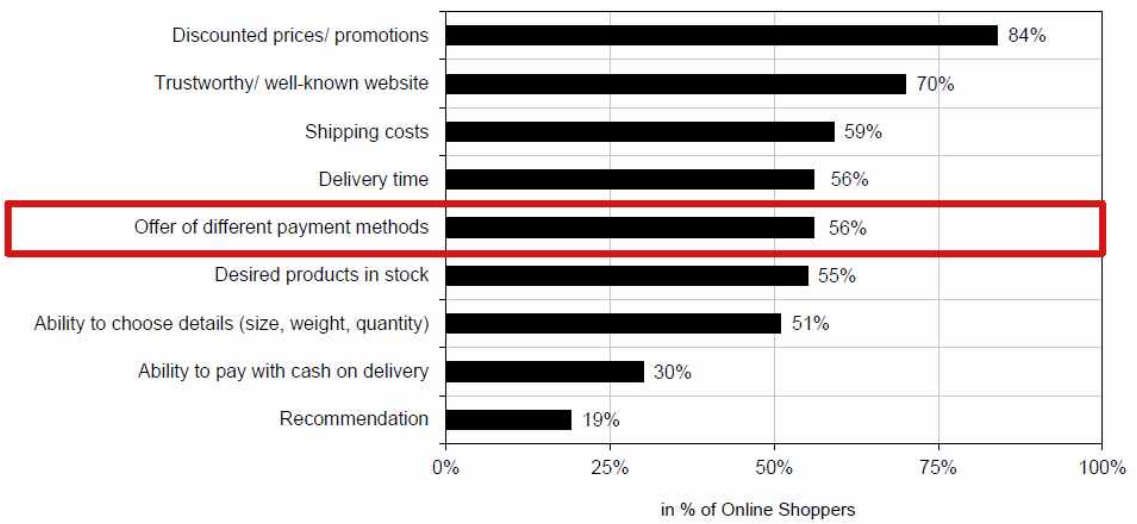
그림 _ 결제 수단에 따른 온라인 쇼핑객의 비율



[출처] Minsait, Afi (2019.1)

▶ 온라인 쇼핑객의 56%는 다양한 결제 옵션을 제공하는 것이 전자상거래의 중요한 측면이라고 생각하는 경향이 있음

그림 _ 페루 온라인 쇼핑객들의 결제 선호 옵션 비율



[출처] eMarketer, CCR International Research (2018.10)

2) 인터넷 및 통신 환경

▶ 페루는 방대한 국토 면적으로 인해 일반 정보통신망 보급이 부진한 상태

- 후진적 국가경제구조와 이에 따른 국가재정 능력의 취약으로 일반 국가 정보통신망 구축을 위한 사회간접자본 투자는 과거 1990년대 후지모리 정부 통치 시기 스페인 텔레포니카(Telefónica)사의 투자진출 이후 저조한 상태
- 전 우말라 정부부터 중기 국가정보통신망 확충계획을 추진 중이나 경기침체와 세수불안, 재정구조의 한계 등으로 계획대로 추진이 안 되고 지연되고 있는 상황
- 광범위한 빈곤, 고가의 전화 서비스, 안데스 산맥과 아마존 정글의 지리적 접근성 또한 발전 지연의 원인
- 쿠친스키 신정부의 국가개발전략이 공개 및 전기통신투자기금(FITEL)의 민간 사업자의 시골지역 및 기타 지역의 통신 서비스 제공에 보조금 지급 시작 등으로 발전방향 가늠이 가능할 전망

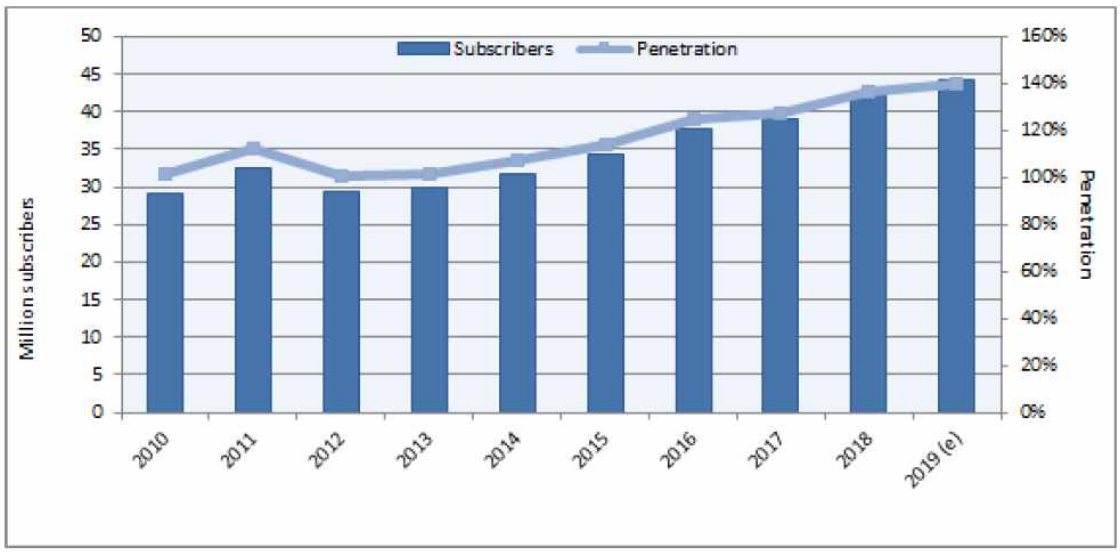
▶ 지리 및 자연적 환경으로 인해 유선통신 및 컴퓨터 보급률은 저조한 편으로, 라틴 아메리카 타 국가들과 비슷한 수준

▶ 이동통신 분야는 2019년 가입자 수 4,424만 명 규모가 예상되며, 보급률은 약 140%에 달할 전망

그림 _ 페루 이동통신 가입자 추이

Year	Subscribers (million)	Penetration
2010	29.115	101.7%
2011	32.461	112.1%
2012	29.388	100.9%
2013	29.793	101.9%
2014	31.666	107.4%
2015	34.235	114.2%
2016	37.719	124.5%
2017	38.915	127.2%
2018	42.154	136.5%
2019 (e)	44.240	139.9%

Source: BuddeComm based on regulator and company data



Source: BuddeComm based on regulator data

[출처] BuddaComm based on regulator and company data(2019.5)

▶ 페루의 이동통신 사업자로는 Teleficanica Peru, Claro Peru, Entel Peru 3개사가 대표적이며, 2014년 중반 페루에 진출한 베트남계의 Viettel이 2018년 6월까지 12.6%의 시장 점유율을 기록하면서 4위로 올라섬

- Viettel이 서비스를 시작하기 전까지 이동통신 시장은 침체되어 있었으나, Viettel의 시장 진입과 동시에 이동전화 번호 이동이 가능해지면서 시장이 가열되기 시작함
- Teleficanica Peru, Claro Peru가 시장의 약 3분의 1을 점유하고 있으며, 3위와 4위인 Entel Peru와 Viettel과의 경쟁이 치열해지고 있음

▶ 2014년 페루 교통통신부(MTC, De Transportes y Comunicaciones, MTC)는 통신망 구축 추진을 위해 지방 당국에 기지국 배치에 관한 이동통신사(MNO)와 협력할 것을 촉구

▶ 모바일 음성 서비스는 2016년 10월 Movistar Peru가 최초로 VoLTE(Voice-over-LTE) 서비스를 시작

▶ 공정위는 2018년 6월 칠레 통신 규제 기관(SUBTEL)과 MoU를 체결해 양국간 국제 이동전화 로밍 요금 삭제

그림 _ 페루 이동통신 가입자 예상 추이 (2019-2023)

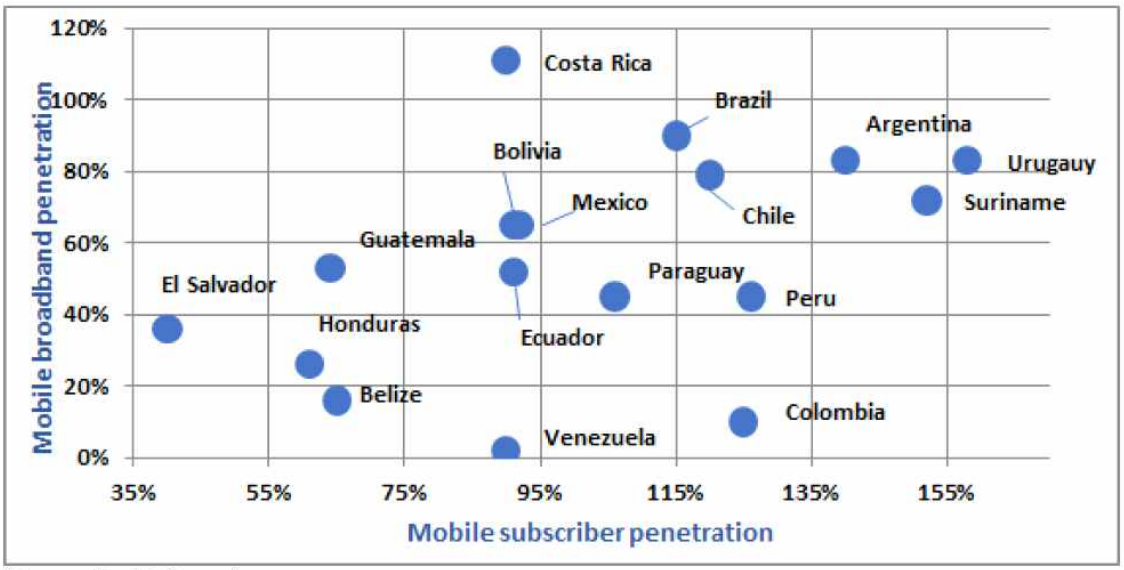
Year	Subscribers (million)
2019 (e)	44.24
2021 (f)	45.8
2023 (f)	47.5

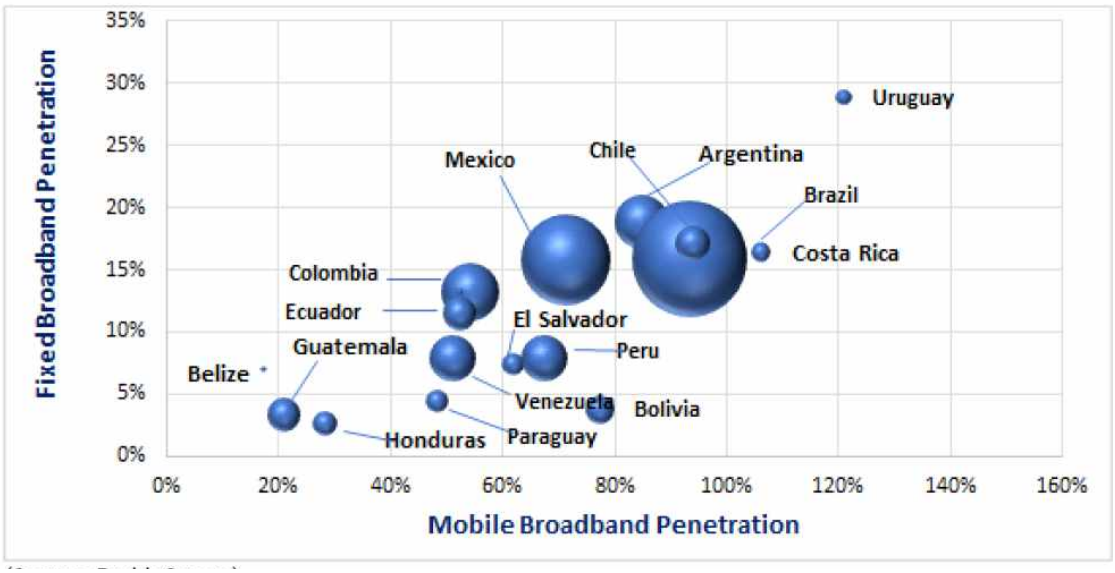
[출처] BuddaComm based on regulator and company data(2019.5)

▶ 광대역 브로드밴드 보급률 최근 들어 점차 개선되는 추세

- 2008년 3월 Claro 의 3G 서비스 개시를 계기로 2009년, 2014년에 Movistar와 Nextel이 각각 3G 서비스를 출시
- 2021년까지 전국에 광대역 브로드밴드 통신망 가설을 위한 국가 프로젝트를 추진 중이나 재정능력 열악과 관련 사회간접자본 투자 저조로 진행이 다소 지연되고 있는 상황
- 모바일 광대역 가입자 수는 유선 인프라의 상대적으로 열악한 조건과 스마트폰의 인기에 의해 강하게 성장함
- 2017년 말 Movistar는 모바일 광대역 시장의 41%를 점유하고 있으며, Claro 40%, Entel 11%, Viettel이 8% 차지하며 그 뒤를 이음
- 페루는 역대 정부의 여유가 없는 재정사정으로 브로드밴드 통신망 확장 프로젝트 투자가 미흡해 현재도 중남미에서 통신망 보급상황이 하위권에 속하는 국가

그림 _ 페루 광대역 브로드밴드 가입 현황





[출처] BuddaComm based on regulator and company data(2019.05)

3) ICT 및 산업 환경

▶ 3G

- 페루 교통통신부(MTC, De Transportes y Comunicaciones, MTC), 2008년 1,900MHz 대역의 25MHz 주파수 보급에 실패 후 2011년 1월로 연기했으나, 약 104만 달러의 투자금 우려에 보급 실패

- Viettel은 2012년 서비스가 미개통되었거나, 한 개 서비스 제공업체만 공급하고 있는 48개의 시골 지역에 2,800만 달러 투자로 모바일 서비스 제공 제안
- 한편 718개 정부기관(학교 438곳, 보건소 112곳, 시군구 168곳 포함)에 10년간 광대역통신을 무료 제공 및 인프라와 설치비용에 3억 2,400만 달러 투자 공약
- Claro는 2007년 7월 최초로 3G 사업을 시작했으며, MOVISTAR PERÚ는 2009년 5월 리마에서 UMTS 네트워크를 출시, Viettel은 2014년 중반에 3G 서비스 시작
- 3G 네트워크는 2015년 말 전국 약 85%, 2016년 말에는 90%를 커버

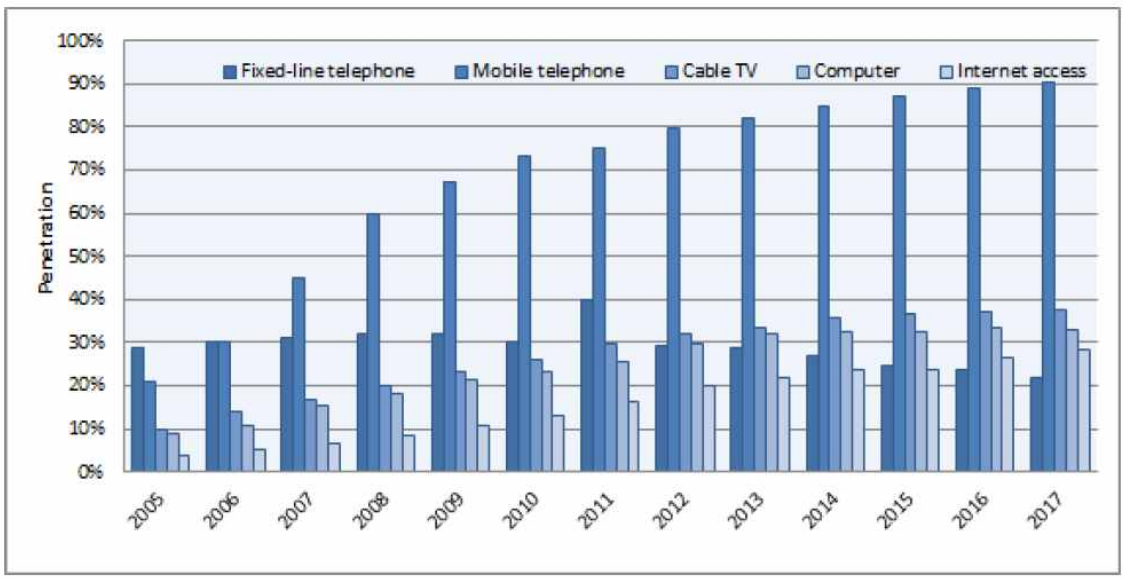
▶ 4G (LTE)

- ProInversió은 2013년 7월 LTE 서비스용 주파수 보급
- MOVISTAR PERÚ와 Entel Perú 역시 LTE 보급을 시작했으며 2019년까지 234개 구역에 LTE 서비스 보급을 공약
- MOVISTAR PERÚ는 2014년 1월 리마에서 LTE 서비스를 개시, 2017년 4분기에 3억 5,000만 달러 인프라에 추가 투자하였으며, 약 1,000개의 신규 기지국 건설
- 'Internet for All' 프로젝트 하에 2018년 7월 파스코, 산마틴, 안샤시, 아야쿠초, 후누코, 우카얄리 등 시골지역 약 600만 명의 사람들에게 모바일 광대역통신을 확장
- Entel Perú는 2013년 말, LTE 네트워크 200개 지역에 배치하기 위한 10년간 4억 달러의 투자 프로그램 시작
- 서비스는 2014년 10월 대부분의 해안 도시와 주요 도시에서 시작
- Claro Peru, 2014년 5월에 LTE 서비스 시작
- 고정 회선 서비스
- Telefónica와 Claro가 번호 이동이 가능한 시장을 지배하고 있으며, 고정 광대역통신망은 주로 DSL과 케이블 모뎀 기술(OSIPTEL, 2017)을 통해 제공되지만 보급률은 지역 및 글로벌 수준에 크게 못 미침

표 _ 페루 ICT 서비스 이용 가구의 비율

Year	Fixed-line telephone	Mobile telephone	Cable TV	Computer	Internet access
2005	29%	21%	10%	9%	4%
2006	30%	30%	14%	11%	5%
2007	31.0%	45.0%	17.0%	15.4%	6.6%
2008	31.9%	59.7%	20.0%	18.0%	8.6%
2009	32.1%	67.0%	23.1%	21.2%	11.0%
2010	30.4%	73.1%	26.0%	23.4%	13.0%
2011	39.8%	75.2%	29.8%	25.4%	16.4%
2012	29.4%	79.7%	31.9%	29.9%	20.2%
2013	28.6%	82.0%	33.6%	32.0%	22.1%
2014	26.9%	84.9%	35.9%	32.3%	23.5%
2015	24.5%	87.2%	36.7%	32.6%	23.5%
2016	23.5%	88.9%	37.1%	33.5%	26.4%
2017	21.9%	90.2%	37.4%	33.2%	28.2

Source: BuddeComm based on INEI and ITU data



Source: BuddeComm based on INEI and ITU data

[출처] BuddaComm based on regulator and company data(2019.05)

정보보호 시장 현황

1) 시장 규모

시장 개요

▶ 페루는 중남미 내에서 치안 수준 등급이 3등급

- 치안상태가 비교적 나쁜 편은 아니라고 평가되나 아직 해소되지 못하고 있는 빈부격차로 인한 민생범죄와 마약관련 범죄, 최근 들어 급증세인 해킹, 피싱 및 절도 등 다양화되고 있는 사이버 범죄 등이 정보보안 수요를 높이고 있는 국가

▶ 사이버범죄의 증가로 정보보안 시장이 점차 커질 것으로 전망

- 특히 최근 3년 전부터 사이버 범죄가 증가되면서 주요 표적이 되고 있는 공공기관 및 금융기관은 물론 심지어 중소기업까지 사이버 공격에 두려움을 가질 정도로 정보보안 수요가 빠르게 증가되고 있으나, 아직 큰 규모를 형성하지 못한 상황

▶ 페루 정보보호 시장 매출은 10% 이상 성장세

- 마약 관련 범죄, 사회계층간 충돌 및 민생범죄, 광산업계의 원주민과의 충돌 등 사회불안 요인 확대로 꾸준한 수요 증가세
- 관련 업체 수와 고용인원 측면에서는 2-3%대의 완만한 성장을 보이는 반면, 해당 기업의 매출액은 12-13%대의 고속 성장세를 기록

▶ 최근 들어서는 전자 장비를 통한 보안 산업이 점차 활성화 추세

- 종전의 전통적인 저임 인력을 활용한 보안 및 감시활동에서 벗어나 점차 첨단장비화되는 추세를 보이며 고용 인원당 매출액도 10% 이상의 고성장 기록 중

▶ 아직까지는 2,700개가 넘는 기업들이 전통적인 인적 물리보안 활동 중심 수행

- 최근 들어 대형 보안업체를 중심으로 ICT 기술을 활용한 고도의 정보보호 및 감시 활동을 강화해 나가는 추세

- 특히 전산망 해킹, 악성코드 침입 등 사이버 공격이 늘어나자 대형 은행, 유통업체 및 광산 업체 등 민간 기업들이 기존 단순 물리보안 중심 시설보안에서 첨단기기와 솔루션 등을 활용한 정보보호 활동으로 구조적 전환이 이루어지고 있음

▶ **보안 활동의 중심은 아직 수도권 및 일부 대도시에 집중**

- 일부 지역소재 대형 생산기업 및 광산기업들이 물리적 보안 및 정보보안 활동 및 시스템 강화 추세

시장 규모 및 전망

▶ 페루의 정보보호 시장은 물리보안 수요가 시장을 주도

- 정부소유 공공건물 및 대형 민간은행, 쇼핑몰, 백화점 슈퍼마켓 등 대형 유통기업 영업장, 대형 광산기업 등의 물리적 보안 수요가 주류 형성
- 최근 들어 ICT 산업 및 기술의 급성장으로 정보보안 기기 및 SW 수요도 지속 증가 추세

▶ 2014년을 기준으로 총 보안시장 규모는 1억 9,200만 달러 규모

- 물리보안 시장이 1억 2,300만 달러, 정보보안 시장이 약 6,900만 달러를 기록

▶ 아직까지는 물리보안 시장 중심으로 시장 활성화 전망

- 아직은 물리보안이 시장구조의 중심이나, 앞으로 정보보안 시장이 확장되어 나갈 유망시장
- 페루는 노상 소매치기를 비롯하여 강도, 절도, 사기 등 각종 민생범죄가 빈번하여 공공부문과 대형 민간기업 및 부유층 가정은 첨단장비를 이용한 물리보안을 중심으로 보안활동을 강화 중
- 최근 들어 주요 공공 사무실의 정보보안과 외부보안 강화를 위한 건물 물리보안을 강화하는 추세
- 따라서 전체 페루의 정보보호 산업시장은 당분간은 물리보안을 위한 중저가 보안장비 및 서비스 시장을 필두로 고가 첨단장비를 활용한 고도 사이버 보안 시장 수요가 급증하는 시장구조를 보일 전망

▶ 향후 정보보안 시장 역시 급성장 전망

- 최근 3년 전부터 페루 기업들 중 40% 정도가 바이러스, 악성 코드, 스팸 등 외부 사이버 공격에 대해 시달리고 있음
- 대부분의 기업들이 이에 대한 투자를 늘려 정보보안 라이선스 또는 솔루션 등 보안제품 구매를 증대하는 한편 정보보안업체와의 보안조치 계약 체결도 매년 60%씩 증가 추세

▶ 정부의 중기 브로드밴드 보급 인프라 투자계획의 성공적 추진이 향후 시장 환경의 중요 변수로 작용

- 계획대로 추진될 경우 브로드밴드 가입회선 수와 고속 인터넷 통신망이 획기적으로 개선되어 인터넷 사용과 고속통신망을 이용하는 서비스 사용이 급증 전망
- 아울러 이에 수반될 사이버 공격의 예방 또는 퇴치를 위한 정보보호 시장수요의 급증과 서비스 질의 고도화가 이루어질 전망

2) 분야별 현황

물리 보안제품 및 서비스

▶ 페루의 보안 장비 시장은 중국, 대만 등의 저가 브랜드 제품이 강세

- 보안기기 시장 주요 고객은 금융권과 공공기관, 대형 광산업체, 카지노 게임장 및 일부 부유층 주거시설 보안용 제품 등이며, 특히 점포망이 넓은 은행은 기기 및 솔루션 구매에 200만~300만 달러 정도를 투자하고 있고 중·소규모 은행도 50만 달러 이상을 투자하고 있는 것으로 분석
- 그러나 제조업부문은 첨단보안기기와 서비스체제로 전환하고 있는 일부 대기업을 제외하고 중소기업은 아직은 전자장비보다 저렴한 비용과 저 투자 장점 때문에 물리적 경비원 서비스를 선호하는 입장
- 미국, 영국, 한국, 대만 및 중국산이 주류를 이루어 왔으나 최근 가격경쟁력을 앞세운 중국, 대만 제품이 시장을 장악하는 강세 형성
- 특히 물리보안 시장은 제품의 질보다는 가격이 우선으로 수요는 증가세이나 고가제품 수입 기피성향으로 수입규모는 증가세가 저조한 이중구조 실현

▶ 주거용, 산업용, 사무용 보안장비에 대한 수요 강세

- 리마 및 다른 대도시에서 발생하는 강도나 가정 침입으로 인한 거주자들의 불만이 높은 상황
- 정부기관 및 개인들은 침입 방지와 경비원 지원, 감시카메라, 경보장치, 조명, 그물망, 철조망 등 광범위한 보안장비에 투자
- 1997년 2월 창설된 SARCC(Search and Rescue Coordination Center), 수색구조작업, 의료피난 등의 서비스를 통해 외딴 지역에서 근무하는 직원의 안전을 위협하는 비상상황에 대한 비상교육 자원 제공

표 _ 페루 안전 및 보안 장비시장 규모 추이

(단위: 백만 달러)

구분	2016년	2017년	2018년	2019(추정)
총 시장 규모	282.1	296.9	336.7	349.8
총 로컬 제품	0	0	0	0
총 수출	29.0	27.5	30.1	31.3
총 수입	311.1	324.4	366.8	381.1
미국에서 수입	73.5	60.9	68.4	71.1

[출처] 미국 상무부, International Trade Administration

▶ 중국과 미국이 시장을 장악하고 있으며 기업과 주택 소유자들은 경보, 감시 카메라, 조명 등 예방 장비에 대한 관심이 높아지는 추세

표 _ 페루의 안전 및 보안 장치 수입시장 점유율 (2018)

순위	국가	점유율
1	중국	41.2
2	미국	18.6
3	멕시코	5.0
4	스페인	3.7
5	대만	3.6
6	독일	3.4
7	이탈리아	2.8
8	콜롬비아	2.0
9	브라질	1.8
10	칠레	1.7
11	프랑스	1.6
12	캐나다	1.5

[출처] 미국 상무부, International Trade Administration

▶ 다양한 물리보안 제품 외에도 최근 들어 정보보안용 시스템, 단말기, 솔루션 등이 시장에 공급되고는 있으나 세관의 수입통계 분류 모호성으로 시장규모를 파악하기 어려운 시장

주요 사업자(경쟁/유통) 현황

표 _ 페루의 정보보호 기업 현황

구분	단위	2012	2013	2014	2015	2016
기업 수	개	2,387	2,418	2,465	2,636	2,707
매출액	$백만	192	214	240	271	307
매출액/기업	$백만	0.08	0.09	0.10	0.10	0.11
매출액/고용인원	$	15,246	16,805	18,492	20,449	22,589
고용인원	명	12,569	12,734	12,982	13,240	13,393
고용인원/기업	명	5.3	5.3	5.3	5.0	5.0

[출처] Barnes Reports, '2015 World Industry & Market Outlook_Security Systems'(2014.12)

▶ 페루의 정보보호 산업을 기능별로 분류해 보면 보안시스템 서비스 업체가 주류

- 아직 저임 노동력이 풍부한 국가로 고가 장비를 통한 정보보안 활동보다는 인력을 통한 감시 및 경비를 통한 전통적 물리보안 시스템에 의존하는 경향이 큰 국가
- 최근 들어 각종 ICT 정보보호 장비 공급 및 대여 업체의 역할이 점차 중요한 위치를 차지

표 _ 2015년도 정보보호 기업의 기능별 분류

구분	총 기업수(개)	총매출액(백만달러)	총 고용인원(명)
보안시스템 서비스	2,122	235	11,380
화재 경보 유지 및 감시	63	6	363
예방 및 보안 장비	272	11	1,239
억류 감시시스템	61	6	278

[출처] Barnes Reports, '2015 World Industry & Market Outlook_Security Systems'(2014.12)

▶ 페루 정보보호 산업을 기업 규모별 업체 수, 매출액 및 고용인원 별로 분석해 보면 영세기업 중심 구조

- 여타 중남미국들과 유사하게 9명 이하 고용 영세 기업들이 다수이고 250명 이상 고용 중견 및 대기업은 3개사 정도로 한정되어 있음

▶ 기업 매출 규모도 대·중소기업간 격차 극심 구조

- 50명 이상을 고용하고 있는 기업이 연간 100만 달러 이상을 기록하고 있고 250명 이상 고용하는 중견기업이 1,000만 달러 이상 매출을, 500명 이상 고용하고 있는 대기업이 4,000만 달러 이상 수입을 올리고 있음

• 반면 영세기업들인 1-4명 수준 고용 기업은 평균 4만 달러대, 5-9명 고용 기업은 평균 10만 달러대의 매출을 기록하며 저임 인건비를 활용한 인적정보보안 산업 양태를 실현

표 _ 페루의 정보보호 기업 분류

구분	기업 규모별 업체 수 (개)									
	1-4명 고용	5-9명 고용	10-19명 고용	20-49명 고용	50-99명 고용	100-249명 고용	250-499명 고용	500명 이상 고용	미분류	계
2014	368	128	104	71	24	13	2	1	1,754	2,465
2015	393	136	111	76	26	14	2	1	1,876	2,636
2016	404	140	114	78	26	15	2	1	1,926	2,707
구분	기업규모별 매출액 ($백만)									
2014	13	11	23	43	31	47	24	35	13	240
2015	14	13	27	48	35	53	27	39	14	271
2016	16	15	30	55	40	60	31	44	16	307
구분	기업 규모별 고용인원 (명)									
2014	1,022	823	1,574	2,383	1,580	1,856	656	1,136	1,951	12,982
2015	1,043	839	1,606	2,431	1,611	1,893	669	1,158	1,989	13,240
2016	1,071	862	1,648	2,496	1,654	1,944	687	1,189	2,042	13,592

[출처] Barnes Reports, '2015 World Industry & Market Outlook_Security Systems'(2014.12)

▶ **주요 사업자**

① ALGANGRUP SAC : 금융업 부문 경보 시스템, 비디오 감시, 접근통제 같은 전자보안 제품 설치 및 운영 서비스 제공

② BEST SECURITY DEL PERU S.A.C : 전자 보안장비 수입 및 공급

③ CIA DE SEGURIDAD POSEGUR S.A : 전자보안장비 솔루션 공급

④ DISTRIBUCION TECNOLOGICA S.A.C : 전자보안장비 솔루션 공급

⑤ DNT-DISTRIBUTION NETWORK TECNOLOGIES SAC : 전자보안장비 솔루션 수입 공급

⑥ ELECTRONIC INTERNATIONAL SECURITY S.A : 접근통제, 자동화, CCTV, 화재경보기기 업체 대리점 및 컨설팅

⑦ FRISAR S.AC : 전자보안장비 설치 및 유지관리

⑧ GRUPO DOSSIER S.A.C : CCTV, 화재예방, 경보 솔루션 공급 및 컨설팅

⑨ INVETSIONES INTERAMERICANAS S.A : 접근 통제, CCTV, 화재경보기기류 공급

⑩ INVFERCAT S.A.C : 전자 보안장비류, 경보감시시스템, 카메라, 가정용·상업용·차량용 장거리 GPS 시스템

⑪ NETCORE SOLUTIONS S.A.C : 전자보안 장비, 솔루션, 데이터 네트워크, 자동화 설비 등 종합적 정보

보안 장비 및 솔루션 등 공급업체

⑫ PROTEOUS SECURITY S.A.C : 개인 및 법인의 보안 장비와 솔루션

⑬ S3 PERU S.A.C : 접근통제 및 CCTV 기기공급, 솔루션 및 컨설팅

⑭ SAEG CONTROLS SAC : 산업자동화 솔루션, 화재예방시스템 기기류 공급 및 엔지니어링 서비스

⑮ SEGURITRON PERU S.A.C : 경보장치, CCTV, 접근통제 등 보안 및 감시 시스템 기기 및 감시 서비스

⑯ SEGO SEGURIDAD OPTIMA S.A : 접근통제, CCTV, 화재 경보 시스템 공급

3) 주요 동향 및 이슈

▶ 2016년 7월 쿠진스키 신정부 출범(2016-2021)

- 페드로 파블로 쿠진스키(Pedro, Pablo Kuczynski) 중도우파 정부가 직전 오얀타 우말라 중도좌파 정부를 대체하여 출범
- 신정부는 2021년도까지 인프라 확충을 위해 180억 달러를 투자하겠다는 정책제시 외에 악화되고 있는 민생범죄 및 마약관련 조직범죄 퇴치와 치안확보를 중요 정책목표로 제시
- 종전 우말라 정부와는 달리 코카재배지역 및 불법 마약 거래 단속을 강화하기 위해 군과 경찰의 효과적 협력 대응체제 구축을 공언
- 신정부는 직전 우말라 정부의 농촌 빈곤층의 생계형 코카인 재배 묵인형 자세에서 강경 단속자세 선회 가능성 시사
- 아울러 신정부 체제에 도전하려는 조직범죄와 테러 집단에 대한 대응체제를 강화하겠다는 입장 표명
- 이러한 정치 상황의 변화에 따라 페루 정부의 정보보안 정책이 종전보다 강화되어 나갈 것으로 전망

▶ 정보통신 방송투자기금을 조성, 정보통신산업 육성을 위한 투자기금으로 운영 중

- 페루 정부 교통통신부는 2006년에 제정된 방송통신법(법령번호 28900호에 의거 산간고립 지역 정보통신 및 방송 인프라 구축, 원활한 서비스 제공 목적의 정보통신방송투자기금을 조성 운영
- 2016년도까지 주요 도심지역 학교 병원 사무용 빌딩 등지에서 최소 2Mbps의 속도로 브로드밴드 접속이 가능하도록 5개년 국가브로드밴드발전계획(NBP)을 수립 추진

▶ 이베로 아메리카 사이버보안 경진대회에 페루팀 참가

- 스페인 외교부·국가사이버보안청·국제협력단은 2018년 12월 미주기구(OAS)와 함께 중남미 국가들을 대상으로 이베로 아메리카 사이버보안 경진대회(ICSC)를 콜롬비아에서 개최했으며, 페루 유소년팀이 참가
- 해당 대회에서 웹보안, 모바일 보안, 사물인터넷, 암호, 역공학, 포렌식 분야 문제가 출제됨

▶ 사이버보안 시장 2021년까지 2.2억 달러 규모로 성장 전망

- 소포스社 중남미 지역 부대표 Oscar에 따르면 페루는 사이버보안이 활성화되지 않은 얼마 남지 않은 국가라고 언급
- 2019년 현재 페루의 사이버보안 시장 규모는 소포스社 추산 1.8억 달러 규모이며, 2021년까지 2.2억 달러로 성장할 것이라고 전망
- 지난 2019년 8월 페루 은행이 해킹을 당했지만, 얼마나 많은 양의 고객정보 유출이 발생했는지 등을 밝히게 강제할 법이 존재하지 않음
- 또한, 페루는 고객 정보를 보관하는 조직들이 해당 정보를 중요하게 다루도록 해야만 하는 최소한의 규정도 없다고 언급
- 페루는 칠레나 아르헨티나보다 더 큰 보안시장이라고 강조

정보보호 정책 및 기관 현황

1) 관련 법령 및 정책

관련 법령 및 규제

▶ 개인정보보호법(Ley de Protección de Datos Personales, Ley No. 29733 : 2011. 06. 07)

• 2011년 6월 7일 의회 통과, 7월 3일 공식 공포

- 페루 정부는 2010년 7월 미국과 캐나다와의 FTA협정, EU와의 FTA협정 체결 협상을 위해 스페인의 정보보호법과 APEC의 개인정보보호 규범 (APEC Privacy Framework)을 기초로 동 법안을 입안, 의회에 회부 법제화

• 개인 정보보호법 주요 원칙

- 합법성 원칙 : 개인정보 수집의 합법성 준수 및 불법 및 사기성 복제 금지
- 개인동의 원칙 : 개인정보 수집은 대상 개인의 동의 필요
- 합법적 목적 원칙 : 개인정보 수집은 명확한 합법적 허용된 목적 아래 허용 및 타 목적 복제 금지
- 정보사용 적정성 원칙 : 수집된 개인정보 사용의 적정성 목적 외 사용 금지
- 개인정보의 성격 : 개인정보는 수집목적에 정확, 명료 및 적정 부합, 정보보안 및 필요기간 한정사용 보장 조건
- 보안유지 원칙 : 개인정보 보호 보안을 위해 필요 충분한 법적 조직적 기술적 조치 필요
- 개인정보원 보호조치 : 개인정보 보호 취약 시 필요한 행정적 법적 조치 의무
- 개인정보 적정보호 원칙 : 개인정보의 타 국가 유통 시 본법 및 국제법 기준에 부합하는 보호조치 보장 원칙

• 개인정보 보호 위반 유형 분류 및 제재

- 경미한 위반 : 개인정보의 동의 없이 사용, 해당 개인의 권리행사 방해, 개인정보 보호당국의 감독권행사 방해 등 의미
- 심각한 위반 : 본법에서 정한 보호원칙 및 규범의 위반, 비밀유지의무 미 준수, 법적으로 보장된 개인정보권 행사의 조직적 방해 및 제재, 국가개인정보등록청에 개인정보 미등록 처리 등
- 매우 심각한 위반 : 본법에서 정한 개인정보취급 원칙 및 규범 위반, 개인의 기본권 행사 방해, 본법을 준수하지 않고 개인정보 은행을 창설, 수정, 취소 및 유지 시, 국가개인정보보호 당국에 불완전 또는 허

위 자료 및 정보 제공 시, 정보보호 당국의 사전 요구에도 불구 불법 개인정보처리 중단 거부 시, 개인정보 보호당국의 개인정보은행 미등록 및 관련 등록요건 미 준수 시 등

• 개인정보 보호법 및 규정 위반 시 위반 사항이 경미한 경우에는 행정제재가, 심각하게 위반한 경우에는 사법당국 형사고발이 원칙

▶ 전자서명 및 전자증명법(Ley de Firmas y Certificados Digitales, Ley No. 27269)

• 2000년 5월 8일 국회통과, 5월 26일 후지모리 대통령 재임 시 공포

• 주요 내용

- 공공행정에 디지털 기기 사용이 확대됨에 따라 전자서명 및 증명의 법적 근거 및 보안 규정마련 목적 제정
- 전자서명은 신분증명, 신용보증기관이 확인한 신분 자료, 공적 확인 키워드, 전자서명자 서명증명, 인증번호 및 인증서인증기관의 전자서명, 등 제 서류 제출 필요
- 전자서명 출원자 정보 비밀유지
- 전자서명의 취소는 출원자 또는 인증기관의 요청, 인증 시효 종료, 인증기관의 기능 종료 등으로 취소 가능
- 외국기관에서 발행한 전자서명도 본법과 동일한 권한과 효력 유지(Ley N° 27310, 2000. 07. 17)

주요 전략 및 정책

▶ 페루 정보보안 정책

• 근거 법령 및 문서

- 내각명령(Resolución Ministerial) N° 129-2012-PCM, 2012.05.23)
- 전자정부 사무국 보고서 N° 44-2012-PCM/ONGEI
- 전자정부사무국 기술보고서 N° 028-2011-PCM/ONGEI-GPGF
- 페루 기술 규준 Norma Técnica Peruana "NTP-ISO.IEC 17799 : 2004/7"

• 주요 내용

- 2009년도에 수립한 경쟁력 및 지적재산권 보호청(INDECOPI)의 비관세장벽위원회가 검증한 국가 기술 규준 ISO/IEC 27001에 의거 국가정보보안 구축
- 내각에서 전자정부구축사무국(ONGEI)이 국가정보시스템관련 총괄기능 수행 위임
- 내각 명령 N° 066-2011-PCM을 통해 승인한 페루 정보사회 발전 플랜(La Agenda Digital Peruana 2.0)에 의거 정보통신망을 통해 발생하는 사이버공간의 범죄위험을 억제하고 국가정보원을 보호하기 위한 위험 최소화 전략을 기반으로 국가 사이버 보안전략 수행을 위한 공공행정 역량 강화

- 정책의 기본은 발전하고 있는 정보통신기술에 힘입어 국민들이 최단 시간 내 지리적 공간을 넘어 정부의 서비스와 정보에 접근할 수 있도록 국가정보통신 공간 인프라의 확장 발전 촉진
- 전자정부 사무국은 전자정부구축 인프라와 함께 국가정보시스템에 정보보안시스템과 보안기술, 정보통신기술을 종합한 정책으로 NTP-ISO/IEC 27001의 채택과 활용 페루기술규준 NTP-ISO/IEC 17799에 의거한 정보보안플랜의 수행시한을 설정하고 국가 정보보안활동의 현대화 추진
- 전자정부사무국은 국가 정보보안 기술과 국가 정보보안 활동시스템을 융합하여 포탈에 국가 정보보안 활동의 점진적 이행 일정을 수립 탑재 조치
- 핵심 정보보안 기술 규준으로 NTP-ISO.IEC 17799. Firewall 설치 등 공공부문 정보보안 전략과 이행 플랜 획정 전파
- 실무적인 국가정보보안은 전자정부 사무국에서 총괄, 정보보안 정책 수립, 정보보안 표준 및 절차 등 수립 제시
- 도메인 관리, 정보 및 소프트웨어 보호, 인터넷 해킹 방지 밑 퇴치, 인트라넷 보안관리, 개인 및 기관 정보통신망의 바이러스 침투 방지 및 치료 등 담당

2) 담당기관

▶ 페루 정보통신망긴급조정팀(PeCERT : Peru-Coordinación de Emergencias en Redes Teleinformáticas)[178]

- 내각 국무총리실 산하 정보통신 긴급상황대응팀 성격으로 2009년 총리령 RM 360-2009-PCM 호에 의거 설립
- 기관 주요 기능

- PeCERT는 페루 행정기관의 컴퓨터 보안업무를 수행하고 있으며 정부기관의 승인이 의거 각종 정보보호에 대한 긴급 상황 관리와 예방 임무 수행
- 공공 및 민간부문의 정보보안 위험도를 최소화시키기 위한 시스템 구축과 각종 학술전문기관 등 민간부문에 PeCERT가 개발한 기술 및 정보서비스 확산 업무 수행
- 국가 공공 행정 기관 간 정보보안의 예방, 탐지, 퇴치, 관리 및 법령화와 보안사고 해결 솔루션 개발 등 조정 업무 추진
- 공공행정상 정보기술 재원 및 시스템 상 보안수준 제고를 위한 규준수립, 제안 및 조정
- 공공기관의 정보시스템 상 보안 사고에 대한 자문 및 정보통신망에서 발생하는 정보보안 사고 보고서 종합
- 정보보안 사고 예방 및 방지 관련 정보 정리 및 공공 정보통신망의 정보보안 수준 제고를 위한 정보 전

178 www.pecrt.gob.pr

파 및 유관기관과의 협력활동

▶ 법무부(Ministerio de Justicia y Derecho Humanos)[179]
- 정보보호를 위한 사법적 보호정책 및 위반사범 사법처리 공권력 행사 역할
- 상기 역할의 관련 근거 법은 2011년 7월에 통과된 개인정보보호법

▶ 법무부 개인정보호국 (Dirección General de Protección de Datos Personales)
- 개인정보보호법에 의거 개인의 기본권리 보장관련 법적 일반 개인정보 보호업무를 담당하며 특히 개인의 보호권 및 보상권 보호에 중점
- 단, 개인 인신정보(Habeas Data) 침해관련 건은 사법부에서 관할

▶ 개인정보 침해 건에 대해서는 개인정보 침해에 책임이 있는 기관이 해당 개인에게 보상을 하도록 조치

관련 기관

▶ 페루 전자정부사무국(ONGEI : Oficina Nacional de Gobierno Electrónico e Informático)
- 국무총리실 산하 전자정부 추진 기술사무국 기능과 정부 포탈(PEP : Portal del Estado Peruano) 운영 담당
- 기관 주요 기능
- 전자정부 추진전략 및 국가정보보안시스템 운영
- 대민 및 기업 인터넷 서비스 (PSCE : Portal de Servicios al Ciudadano y Empresas) 및 정보사회 발전 위원회 (CODESI : Comisión de Desarrollo de la Sociedad de la Información) 포탈 운영
- 페루의 공공부문 정보보안관련 업무 및 보호기능 수행

▶ 교통통신부(MTC, De Transportes y Comunicaciones, MTC)
- 1992년에 창설되었으며 기반시설 개발 및 무선 스펙트럼 관리, 기술 표준 승인, 면허 발급 등을 담당
- 유선전화, 모바일, 공중전화 및 방송과 부가가치 서비스 운영
- 상호 접속료와 도매 가격 규제

▶ 민간투자감독기구(Organismo Supervisor de la Inversión Privada en Telecomunicaciones(Osiptel))
- 총리 국무조정실에 부속되어 있으며, 1991년 7월 입법령 702호에 의해 설치되어 1994년 1월에 운영

179 www.minjus.gob.pe

시작

- 페루 영토 최대 80%연결을 목표로 국가 광대역통신망 계획 수립
- 번호이동성 요건 및 관세 규제, 상호접속 표준, 서비스 품질, 민간 부문 투자 촉진 등 통신 서비스 시장 규제 및 감독
- 관세 공평성 보장 및 면허인 간의 분쟁 해결 담당
- 소매가 인하 및 네트워크 구축에 자금 투입으로 광대역 프로그램 추진 중

▶ 통신투자기금(Fondo de Inversión de Telecomunicaciones, FITEL)

- 보조금의 규정에 따라 시골지역 사업자를 위한 기금 수여
- 통신 사업자의 연간 총 수입에 대해 1%의 세금을 부과하여 자금 조달

▶ 민간투자진흥청(Proinversión)

- 공적 입찰자를 통해 통신 투자 기금(FITEL) 프로젝트 사업자를 찾는 업무 수행

기타 유관기관

▶ 국회

- 관련 입법 활동 지원

▶ 중앙은행

- 금융권 정보보안 관리 감독

▶ 주민보호위원회

- 대민 정보보호 조치

▶ 선거관리위원회

- 선거인 명부 작성 및 관리 과정에서 발생하는 개인정보에 대한 정보보안 책임

▶ 감사원

- 각 정부기관의 정보보안 관련 정책이행 감사 활동

▶ 내무부 및 검찰청

- 국가 정보보안 사범 단속

▶ 은행보험감독원
- 금융계의 정보보안 감독 활동

▶ 국가정보통계청, 민간 통신부문 투자 감독청, 페루 라디오 TV 감독청 등
- 소관업무에서 발생할 수 있는 공공 정보보안 및 개인정보 보호 활동 수행

3) 규제 및 인증제도

▶ 페루는 정보보호 관련 인증 업무를 전문으로 하는 기관이나 업체가 없고 일부 외국 정보서비스 업체가 관련 인증업무를 병행하는 수준으로 향후 관련부문도 확대 발전될 것으로 전망
- 예컨대 SGS Perú가 관련 업무를 취급하고 있으나 정보보안관련 인증업무를 전문으로 하는 업체는 아님

▶ 유사 공인인증 업무를 수행하는 공공기관은 다음과 같은 기관이 있음[180]
- 기관명: 대통령실 산하 국가대민서비스청 (La Autoridad Nacional del Servicio)
- 주요 업무: 공공활동 및 국가정보접근 활동에 대한 ISO 9001-2008의 국제공인인증 취득, SGS Peru 등 관련 민간부문 인증업무를 하는 업체에 대한 감사권 행사 등

4) 최근 정책 동향 및 이슈

▶ 쿠진스키 신정부는 치안 안정 및 공권력 확립을 보다 강력하게 추진 예상[181]
- 쿠진스키 신정부는 직전 우말라 대통령 정부 시기보다 공권력을 강력하게 행사하면서 치안관리를 강화해 나갈 것으로 시사
- 우말라 정부는 자신이 원주민 출신이었기 때문인지 아니면 정치적 소신인지는 불분명하나 원주민의 저항사태 및 저소득층의 소요사태나 민생범죄에 대해 비교적 관대하게 처리하는 경향 표출
- 그러나 신정부는 공권력 확립과 부정부패 척결을 내세우고 2021년까지 보다 엄정한 치안관리와 조직범죄나 민생범죄를 척결하여 국가 치안을 안정시켜 나가겠다는 취지의 정책 변화를 시사
- 이러한 변화 예상 중 하나는 페루 경제의 재건을 위해서 필요한 외국인투자 유치 활성화를 위한 특단

180 www.pcm.gob.pe
181 쿠진스키 대통령 취임사 정책방향 분석 및 대통령실 보도자료 분석

의 조치가 필요하다는 인식이 전제가 되는 변화

- 우말라 정부 초기에 약 40억 달러에 달하던 미국 기업의 페루 북부 까하마르까 지역 대규모 금광 개발 투자계획[182]이 현지 원주민의 식수오염 우려 등 환경보호를 이유로 내건 극렬한 저항으로 취소된 이후 외국인 투자자들이 페루의 지방 주민 및 원주민의 저항을 두려워해 대규모 광산개발이나 제조업 투자 진출을 주저하는 입장을 보이고 있다는 점을 인식하고 외국인 투자환경을 개선해 나가겠다는 의지를 제시하기 위한 정책 방향으로 해석

▶ 코카인 재배 및 불법거래 단속 강화 정책

- 2014년도부터 그간 사용하던 공중살포 제초제가 발암물질을 함유하고 있다는 비난으로 살포를 중단하자 중남미 콜롬비아, 페루 등지 밀림에서 코카인 재배면적이 증가되는 경향을 보여 왔음
- 직전 우말라 정부도 안데스 동부 열대우림지역 빈곤층의 생계형 코카인 재배를 묵인하는 듯한 인상을 주는 정책으로 미국과 마찰을 빚어 왔던 점을 들어 친미적인 쿠진스키 정부에서는 이를 대체작물 전환이나 생계보조 등을 통해 단속을 강화하고 국내 코카인 불법 거래를 강력하게 단속해 나갈 할 것이라 예상하는 내용

▶ 태평양 어업권을 두고 칠레와 페루 해커간의 사이버 전쟁 발발

- 인터넷 사용 자유 등에 대한 이슈에서 돈을 노린 범죄 등으로 사이버 공격 패턴이 다양화되기 시작
- 사이버 범죄에 대한 일반인의 인식이 높아지고 있고, 관련 컨설팅 기업들이 조금씩 늘어나고 있음

▶ 정부 부문 보안 관제 센터 구성 활성화

- 페루 정부(전자정부국 등)에서는 각 부처별 관제센터 구성에 노력하고 있음
  - 관련하여 페루 보안 기업들의 한국 보안 솔루션에 대한 관심 고조
  - 관제, 백신, 방화벽 등 보안 분야 한국기업 진출 가능성이 높아지고 있음
  - 전자정부국은 관련 페루기업과 한국 기업 간의 협력에 관심이 높음

▶ SIM 카드 등록 정책

- 페루는 2010년 범죄 행위를 위한 휴대 전화 사용 억제를 위해 모든 선불 모바일 사용자들에게 SIM 카드 등록을 명령
  - 모바일 가입자의 약 69%로부터 최소한의 소유자 식별 요건이 충족되지 않은 문제 발생이 요인
  - SIM 카드 등록 정책 시행 이후 모든 선불 모바일 사용자들은 지문 일치 시에만 가입 가능

182 주 페루 대사관 대본국 보고서 참조

융합보안시장 및 정책 동향

1) 융합보안시장 동향

스마트시티

▶ 한국 정부 주도, Telefónica del Perú와 Piura 지방자치단체의 스마트시티 프로젝트 개발 촉진 시작[183]

• 페루 상공 회의소와 Piura생산 지원으로 스마트시티 Piura 프로젝트 착수

- 한국 정부는 전자정부협력센터를 통해 이 프로젝트를 견인할 것을 협약했으며, Telefónica와 Piura 지자체 간의 합의는 4년 동안 지속될 예정
- 추진될 프로젝트는 지능형 교통, 디지털 정부, 지능형 보안 등에 중점을 둘 예정

블록체인

▶ 암호화폐는 페루의 인터넷 사용자들에게 가장 많이 알려진 핀테크 서비스(41.6%) 중 하나

▶ 2018년 Transparency.org에 따르면 국가부패지수(corruption perception index, CPI) 하위권 나라 중 하나인 페루는 GDP의 0.0136%를 차지하는 로컬 비트코인을 보유한 것으로 나타남

	Currency	Share of GDP	CPI 2018
1	Venezuela	0.2326%	18
2	Nigeria	0.0540%	27
3	Russia	0.0457%	28
4	Colombia	0.0254%	36
5	Ukraine	0.0227%	32
6	Kenya	0.0204%	27
7	Peru	0.0136%	35
8	South Africa	0.0116%	43
9	New Zealand	0.0113%	87
10	Malaysia	0.0111%	47

[출처] Transparency.org (2019)

▶ 라틴 아메리카 전 지역에서 암호 화폐 ATM 네트워크를 운영하는 ibitt는 HTC와 제휴 하여 암호화폐의

183 행정안정부, '전자정부협력센터 통해 한국 스마트시티 페루 본격 진출', 2019.7.10

하드웨어 지갑을 특징으로 하는 Exodus 1 Per La Cuarta을 2019년 10월부터 판매

- 2019년 초 ibitt는 페루에서 암호화 ATM 설치 확장 시작

▶ 블록체인 통해 범죄 및 노동 배경 증명서 발급 서비스 시작

- 현재 페루는 블록체인 기술을 통해 노동시장 진출을 희망하는 29세 미만에게 범죄, 경찰, 사법, 학술, 직업 체험 자격증을 발급하기 위해 블록체인 기술을 사용 중
- Cointelegraph를 통해 페루 정부의 국민 신뢰와 서비스 부족 개선 및 신뢰를 회복시키기 위한 혁신적 기술 프로젝트를 시작했으며, 이는 누구에게나 공개되어 진위 확인 가능

▶ 2019년 9월 공공 입찰 국영기관 페루 콤프라스, 한국 블록체인 대표단과 공개입찰 기술 협약

핀테크 등

▶ 페루 핀테크 협회 (Fintech Association of Peru)에 따르면, 2018년 평균 3,000번의 소비자 대출 및 100,000번의 소기업에 핀테크 재정 기반을 위한 서비스가 제공됨

- 이 핀테크 시스템은 3년 동안 개발되어 현재 약 70개 회사로 구성됐으며, 가장 활발한 활동은 대출(22개 회사), 전자 상거래 서비스(18개 회사) 및 디지털 거래소(casas de cambio digital, CCD)로 구성
- 특히 CCD는 페루에서 운영 3년 내 은행, 전통 환전소, 거리 환전소보다 좋은 서비스를 제공한 것으로 평가받음

▶ 페루 결제 핀테크 회사 Máximo, 2019년 디지털 뱅크 리마 대회서 우승

- Máximo는 중소기업을 위한 금융, 디지털화, 서비스 충성도에 초점을 두고 소비자를 위해 스마트폰 결제를 촉진해 저축과 편의성을 키우는 서비스 제공

▶ 글로벌 회계법인 회사 EY는 페루에 EY Peru의 새로운 법률 부서 서비스 라인을 추가하여 핀테크 법률 회사 Vodanovic Legal 설립

- 페루의 금융 시장과 핀테크 관행에 대한 규제를 목표로 기술 금융 서비스 (핀테크 및 인슈어테크), 금융 라이선스, 금융 규제 자문 및 규제 준수 등을 제공

▶ 가톨릭 경제 지불 솔루션 미국 회사 Cathio, 페루 최초의 핀테크 환전 플랫폼 Kambista S.A.C.와 MOU 체결

- Cathio는 가톨릭 공동체, 비영리 단체, 기관의 요구에 대응하여 사용하기 쉬운 지불 솔루션을 제공하기 위해 가톨릭 경제에서의 돈과 자원 이전을 개혁하기 위해 설립되었으며, Kambista S.A.C.는 이 기술을 활용하는 통합 프로젝트 추진 예정

- 해당 프로젝트는 송금 플랫폼 구축을 목표로 이용자들과 중소 기업들에게 온라인 거래를 통해 미국 달러화를 페루 솔즈로 환전할 수 있는 기회 제공
- 2016년에 설립된 Kambista는 페루에서 처음으로 모바일 교환 사업 모델을 구현했으며, 현재까지 총 2억 달러를 교환하고 10만 건 이상의 거래 이행
- 2019년 2억 달러 추가 교환 및 중남미 국가들로 사업 확장 예정

2) 융합보안정책 동향

사물인터넷(IoT)

▶ 마누국립공원(Manu National Park), 자연환경과 동물 모니터링에 IoT 도입

- LoRA 방식의 IoT 센서를 나무 혹은 모니터링이 필요한 지역에 설치한 기지국에 구축하고, 여기에서 발생한 데이터를 라우터에 모아 3G 이동통신망으로 클라우드 서버에 전송하는 방식

블록체인(가상화폐 포함)

▶ 페루, 미주개발은행이 추진하는 블록체인 프로젝트에 참여

- 2018년 10월 미주 개발 은행 (Inter-American Development Bank)이 라틴 아메리카 전역에 개방형 블록체인 생태계를 구축하기 위해 나선 이니셔니브에 코스타리카, 멕시코와 더불어 참가

▶ 페루 정부, 블록체인을 투명성 제고와 부정부패 철폐의 수단으로 인식

- 2019년 5월 페루 정부가 블록체인 스타트업인 Stamping.io와 협력하여 투명한 계약 조달 시스템을 구축했다고 발표
- 페루 정부는 이번 파트너십을 통해 데이터 조작 및 기타 부정부패 행위가 불가능한 정부 계약 검증 시스템을 구축하는 것에 초점을 맞출 계획

핀테크 등

▶페루개발은행, 핀테크 스타트업 지원 위한 씨드펀드 설립

- 핀테크 분야 스타트업 창업과 지속적인 성장을 지원하기 위해 페루 개발 은행인 'Cofide'가 2,000 억 달러의 시드펀드를 설립할 예정

마. 과테말라

'18년 예상GDP(십억달러)	78.46
'18년 인구수(천명)	17,247

■ ITU 글로벌 사이버보안 지수(Global Cybersecurity Index, GCI)

· 과테말라의 사이버보안 지수는 우리나라 대비 매우 낮으며 세계 중하위권 수준

국가명	2018		2017		전년대비 증감	
	지수	순위	지수	순위	지수	순위
과테말라	0.251	112	0.114	138	+0.137	+26
대한민국	0.873	15	0.782	13	+0.091	-2

■ ICT 관련 주요 지수

· 과테말라의 전반적인 ICT 발전 수준은 전 세계 167개국 가운데 중하위권에 속해 있음

지표명	과테말라		한국	
	점수	순위	점수	순위
IMD 국가경쟁력지수(2019)	-	-	-	28
IMD 디지털경쟁력지수(2019)	-	-	-	10
UNCTAD 전자상거래지수(2019)	37.5	119	89.4	19
ITU 글로벌 사이버보안 지수(GCI 2018)	0.251	112	0.873	15
UN 전자정부 지수(2018)	0.538	81	0.901	3

■ ICT 관련 주요 통계(ITU, 2017년 말 기준)

· 과테말라의 유선통신 보급률은 15% 미만으로 매우 낮으며 이동통신 보급률은 높은 편

항목	과테말라		한국	
	가입자수(천 명)	보급률(%)	가입자수(천 명)	보급률(%)
유선전화	2,461	14.55	26,845	52.54
유선브로드밴드	531	3.14	21,196	41.48
이동통신	19,986	118.16	63,659	124.59
인터넷 이용률	65%		95.07%	

정보보호 산업 개요

1) 보안 환경

정보보안 환경

▶ 과테말라의 정보보호 산업 환경은 후진적 구조
- 법적 및 제도적 정비가 제대로 갖춰지지 않음
- 정보보호 수요는 증가 추세이나, 자체 기술 수준, 조직적 체계, 역량구축 면에서는 열위 수준으로 제대로 정보보호 활동이 이루어지지 못하고 있는 상황
- 타 국가와 협력의지도 상대적으로 강한 편이나 아직은 무상원조 성격의 비대칭적 지원을 원하는 입장이라 원활치 못한 편

▶ ITU에서 평가한 글로버 사이버 보안 종합지수도 낮은 수준
- 중남미 역내 국가 중 9위 그룹에 머물고 있는 낮은 수준 기록[184]

▶ 향후 정보보호 수요는 급격히 증가되어 나갈 것으로 전망
- 부패, 부적절한 사법 제도, 폭력과 빈곤 등에 의한 잦은 민생범죄 발생으로 정보보호 수요 확대 추세
- 공공기관 및 광공업 부문 등 대형 민간기업, 일부 부유층 주택 등 전통적인 중남미의 정보보호 수요층 확대추세로 향후 정보보호 시장이 급격히 성장해 나갈 것으로 전망

전자상거래 및 결제 환경

▶ 2012년 중반 서비스를 시작한 선불업체 Movilway는 Banco Reformador 등 여러 은행과 제휴해 전자지갑 서비스 제공
- 이 서비스는 공공 요금과 같은 기본 서비스 비용을 지불하는데 사용될 수 있으며, 운송 및 소매 서비스에서도 이용 가능

▶ Tigo, 서유럽연합(Western Union)과 함께 국제 모바일 송금 서비스를 시작

---

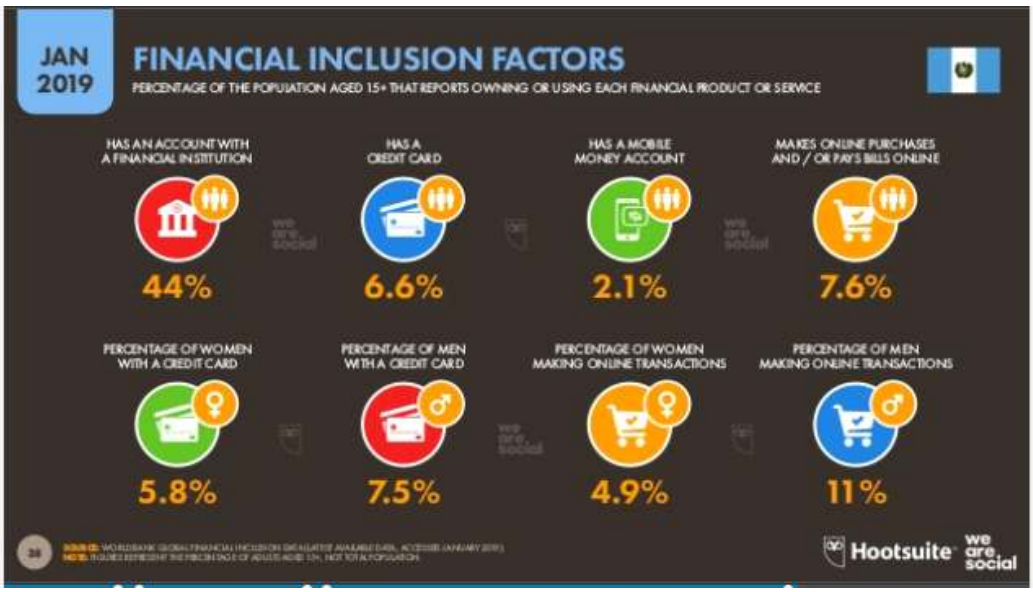
184 ITU, Measuring the Information Society Report 2015

- 이 서비스는 고객들이 해외에서 직접 돈을 모바일 지갑으로 받아 Tigo 판매점에서 현금으로 바꿀 수 있게 해 줌으로써 큰 호응을 얻음

▶ 국제 마케팅 조사업체 'We are Social'의 Digital in 2019: Guatemala에 따르면 2019년 1월 기준 과테말라 국민의 44%가 금융기관 계좌가 있으며, 신용카드 계좌는 국민의 6.6%가 소유하고 있는 것으로 나타남

- 국민의 2.1%가 모바일 지갑이 있으며, 7.6%가 온라인 거래 혹은 구매 경험이 있는 것으로 나타남

그림 _ 과테말라의 금융 서비스 및 전자상거래 이용률



[출처] We are Social, Digital in 2019: Guatemala

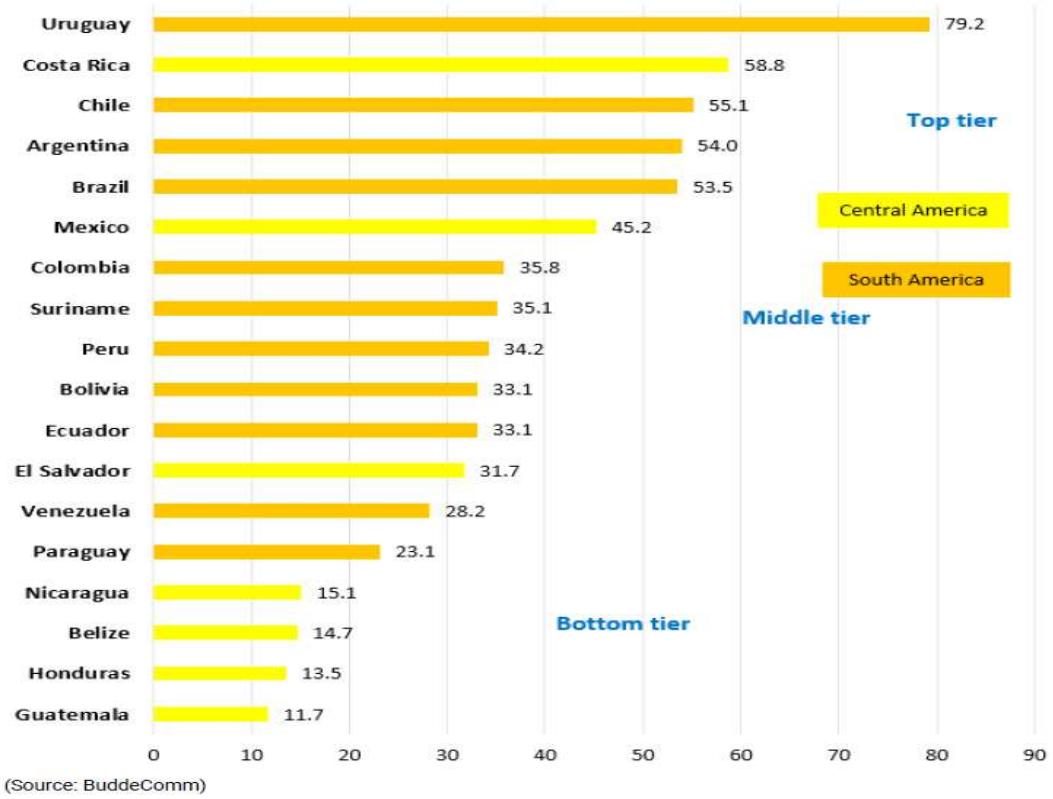
2) 인터넷 및 통신 환경

▶ 과테말라는 정부의 과소투자 등으로 인해 기반 시설이 열악한 상태

- 과테말라의 통신 기반시설은 주와 지방 정부의 수년간 과소투자 및 폭력과 빈곤, 부패 등으로 인해 어려움을 겪어왔으며 고정 회선은 열악한 상태
- 특히 대부분 시골 지역은 유선 접속이 불가하며 모바일 서비스는 필요에 의해 채택되어지는 상황

▶ 과테말라는 통신 서비스 지수(TELECOM MATURITY INDEX, TMI) 11.7%로 라틴 아메리카에서 최하위에 위치

그림 _ 과테말라 통신 서비스 지수(TELECOM MATURITY INDEX, TMI)



(Source: BuddeComm)

▶ 도시와 시골 간 통신 환경 격차가 상당히 큼

- 과테말라 도심과 시골 간 통신 시설이 각각 34%와 4%로, 도심에는 비교적 현대적인 네트워크가 있으나, 시골 지역은 매우 열악한 상태며 높은 비율의 인구가 시골 지역에 살고 있는 상황

▶ 모바일 서비스 보급률은 낮지만 꾸준히 성장 중

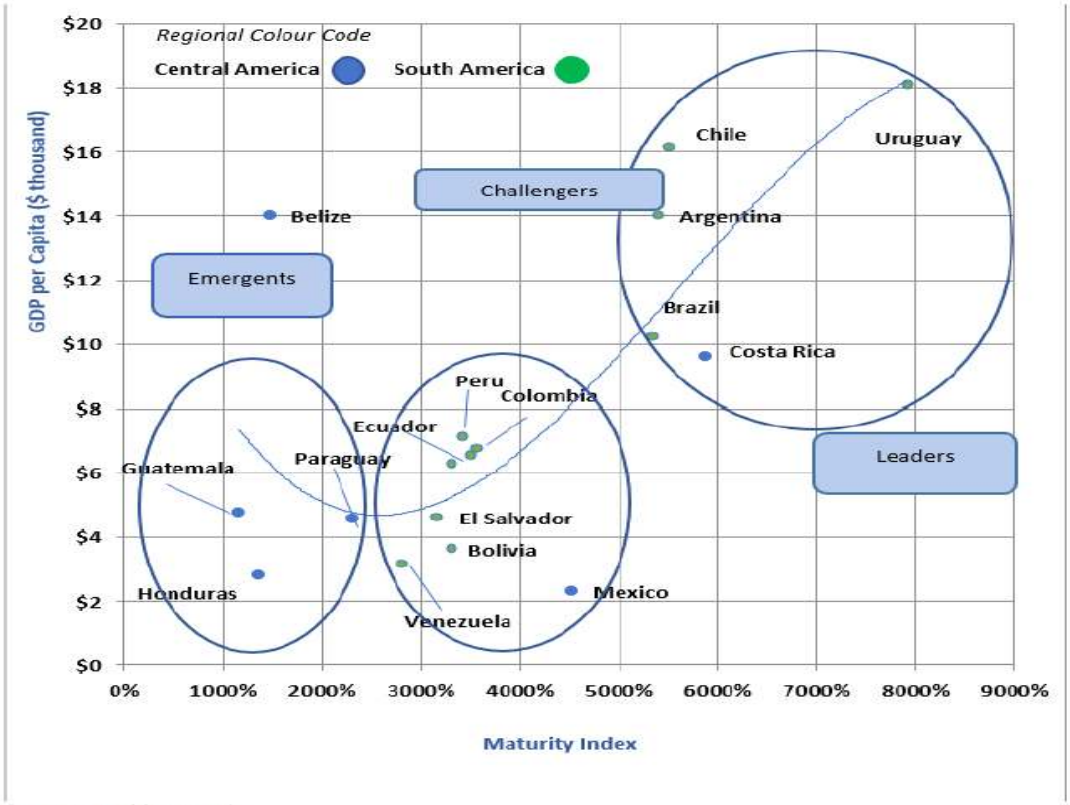
- 모바일 서비스 가격은 지역에 대한 기대치를 크게 상회하는 편
- 광대역 이동통신 개발은 느린 주파수 할당으로 지연되어 왔으며, 3G는 널리 이용 가능
- LTE는 현대화 3개년 계획에 따라 2014년 국내 첫 개통되었으며, LTE 기술 적용 범위는 상당히 좁은 편

▶ 유선전화와 모바일 서비스를 합친 수익률은 라틴 아메리카에서 가장 낮은 비율인 4.2%에 불과

- 1990년대 중반 시민들의 과테말라 정부의 비효율성에 대한 불만이 커지자 이 상황을 해결하기 위해 1996년 정부는 규제 당국인 통신 감독 기관 (Superintendencia de Telecomunicaciones, SIT) 창설 및 일반 통신법 제정

▶ 통신 서비스 성숙도 대 1인당 GDP는 라틴 아메리카에서 하위권에 위치

그림 _ 라틴 아메리카 통신 서비스 성숙도 대 1인당 GDP

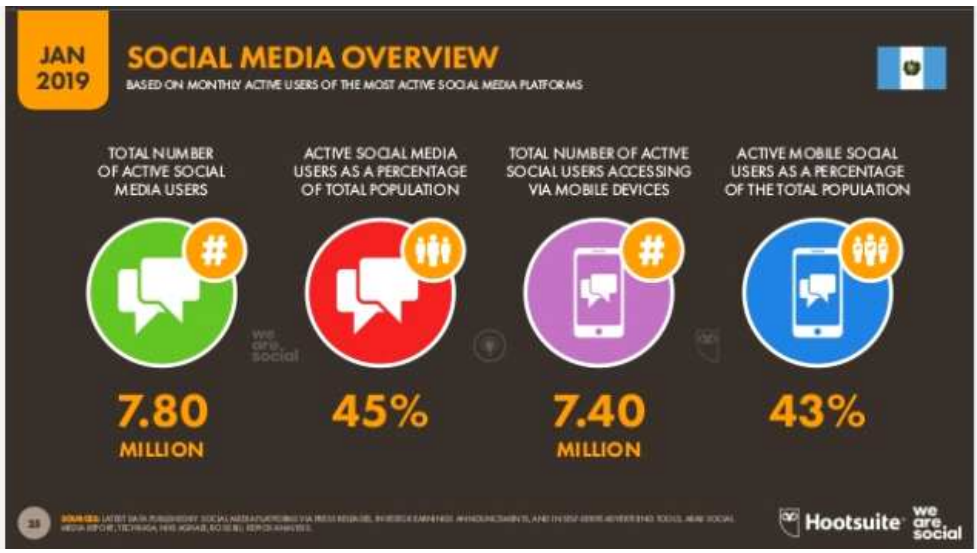


(Source: BuddeComm)

▶ 국제 마케팅 조사업체 'We are Social'의 Digital in 2019: Guatemala에 따르면 2019년 1월 기준 총 1,758만 명의 과테말라 인구 중 실제로 인터넷을 사용하는 인구는 780만 명으로, 이는 전체 인구의 약 45%에 해당

- 모바일 가입자는 2,043만 명으로 보급률은 117%이며 모바일 사용자의 740만 명인 43% 정도가 소셜 네트워크 서비스를 이용하고 있음
- 모바일을 통한 인터넷 사용인구는 점차 증가하고 있어 2018년 1월 지난해 같은 기간보다 8.3% 증가했으며 이는 모바일 가입자가 0.7% 증가한 것보다 높은 수치를 나타냄
- 과테말라는 전체 인터넷 사용자의 62%가 소셜미디어 서비스로 페이스북을 사용

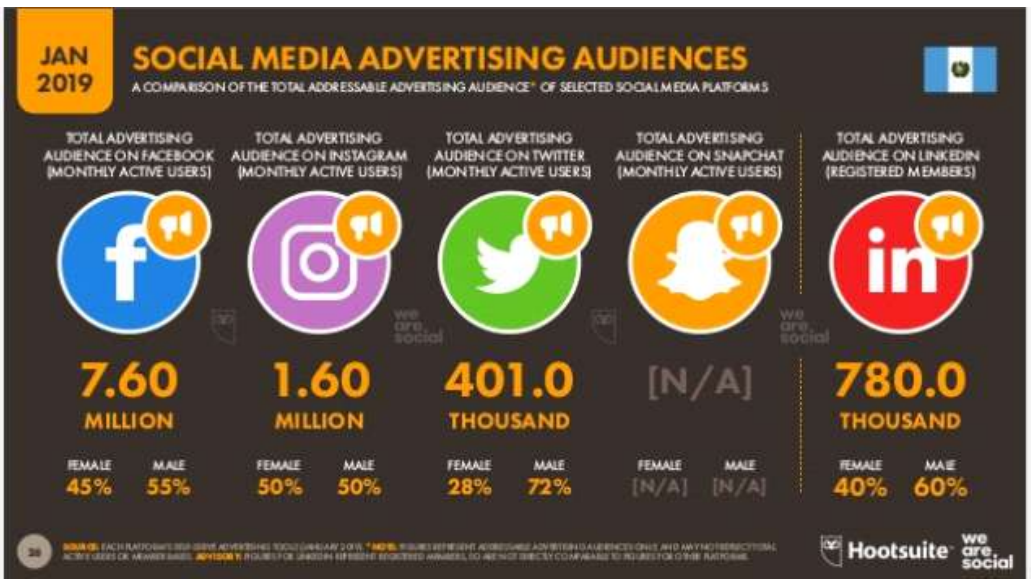
그림 _ 모바일 인터넷 서비스 이용자 비율



[출처] We are Social, Digital in 2019: Guatemala

▶ 소셜미디어 통계사이트인 Social Media Stats Worldwide에 따르면 과테말라의 소셜네트워크 서비스 이용은 Facebook 사용이 1위(62%)로 가장 많으며 이어서 Instagram 2위(13%), Linkedin 3위(7.5%), Twitter 4위(3.3%) 등이 그 뒤를 따름

그림 _ 소셜미디어 서비스 이용자 비율



[출처] We are Social, Digital in 2019: Guatemala

▶ 2008년 경기 침체의 영향으로 주택시장 및 기업시장에서 소비전력의 감소는 과테말라 통신부문의 경기 침체로 이어졌으며, 유선전화 시장은 2009년 이후 지속적으로 감소

▶ 과테말라의 이동통신 사업자로는 América Móvil'의 Claro, Telefónica의 Movistar, Millicom의 Tigo 3개사가 대표적이며, América Móvil은 자회사인 Claro를 통해 고정 회선의 약 83%를 지배

- Claro는 고정 전화 서비스에서는 우세하지만, A-Tel, Cablenet 등 소수의 지역 사업자들 또한 약 18%의 시장 점유
- 콜럼버스 통신 그룹의 콜럼버스 비즈니스 솔루션(Columbus Business Solution, CBS)은 파나마, 온두라스, 과테말라, 콜롬비아, 엘살바도르 등 여러 카리브해 시장에서 활동하고 있으며, 2015년부터 중앙아메리카 사업 전반에 4억 달러를 투자 시작

표 _ 인터넷 서비스 이용 가구의 비율

Year	Users	Penetration
2010	1,546,000	10.5%
2011	1,851,000	12.3%
2012	2,459,000	16.0%
2013	3,091,000	19.7%
2014	3,747,000	23.4%
2015	4,169,000	25.5%
2016 (e)	4,409,000	26.5%
2017 (e)	4,605,000	28.6%
2018 (e)	4,785,000	29.8%
2019 (e)	4,890,000	32.6%

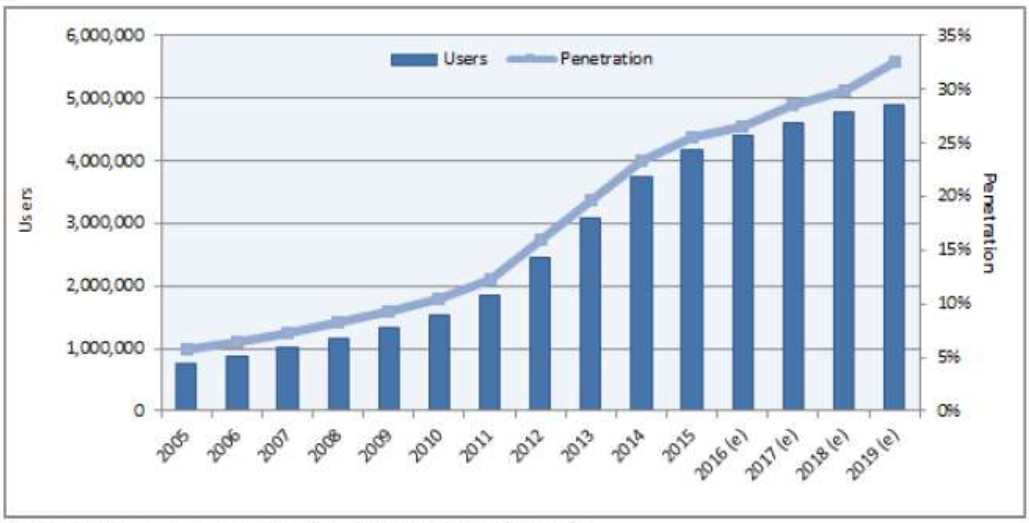
Source: BuddeComm based on ITU and internetlivestats data

3) ICT 및 산업 환경

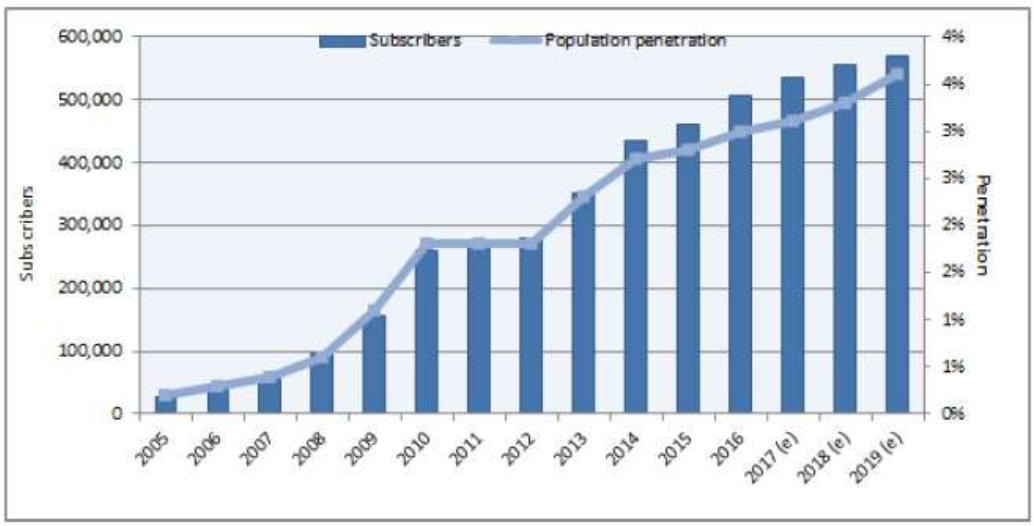
▶ 과테말라에서 사용되는 광대역 기술로는 DSL, 케이블 모뎀, 무선 등이며, 와이파이 서비스는 2004년 초에 등장

▶ 모바일 광대역 접속은 Tigo, Claro, Movistar 네트워크를 통해 제공

그림 _ 광대역 브로드밴드 가입 현황



Source: BuddeComm based on ITU and internetlivestats data



[출처] BuddeComm based on ITU ad industry data (2019.05)

▶ ICT 교육 등 정보통신 투자는 대부분 민간 기업에 의해서 자금 조달

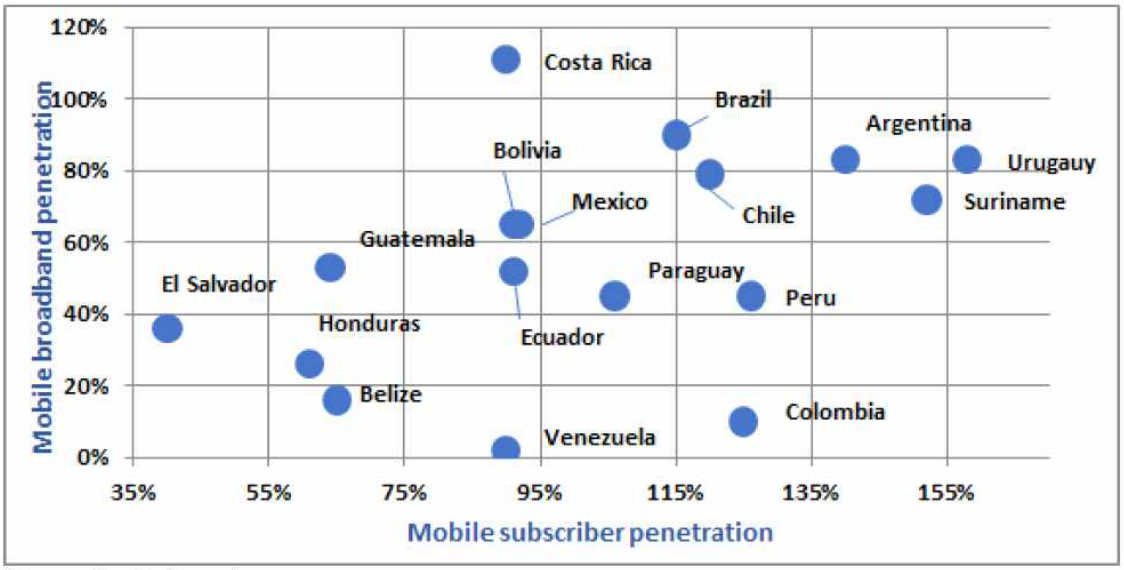
- 초기 아동 발달 센터 설립과 같은 디지털 포함 프로그램을 포함한 인구를 위한 개발 프로그램 등은 운영자 Tigo와 ALAS 재단의 협력을 통해 시행

▶ 광대역 브로드밴드 보급률 최근 들어 점차 개선되는 추세

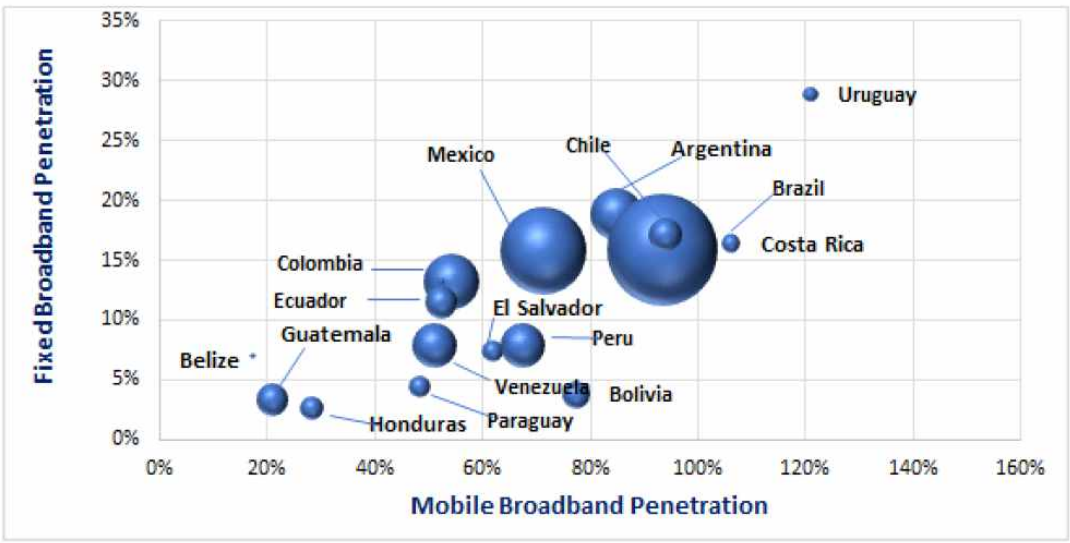
- 과테말라는 정부의 과소투자 등으로 브로드밴드 통신망 확장 프로젝트 투자가 미흡해 현재도 중남미

에서 통신망 보급상황이 하위권에 속하는 국가

그림 _ 라틴 아메리카 내 과테말라의 광대역 브로드밴드 현황



(Source: BuddeComm)



(Source: BuddeComm)

[출처] BuddaComm based on regulator and company data(2019.05)

▶ 3G

- 2008년 Claro와 Tigo, WCDMA 기술을 기반으로 3G 서비스 시작했으며 2009년 말 Movistar가 서비스 출시

- 3개 사업자는 모두 화상통화, 멀티미디어 다운로드, 모바일 광대역 서비스 제공
- 2012년 말 과테말라 정부는 추가 비용 없이 기존 면허 양허를 20년 더 연장하는 법안 통과

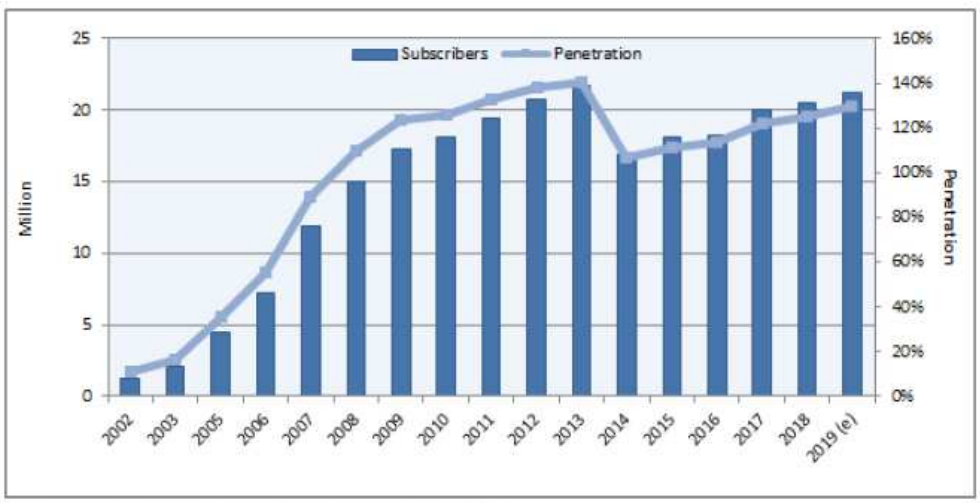
▶ 4G (LTE)

- Movistar는 2014년 10월 1900MHz 대역을 이용해 LTE 서비스 시작했으며, 2018년 후반에는 최대 300Mb/s의 데이터를 제공할 수 있는 LTEA 기반 서비스 개시
- Tigo는 2015년 중반 3년간의 인프라 현대화 프로젝트의 일환으로 과테말라 도심에 LTE 출시

표 _ 과테말라 이동통신 가입자 추이

Year	Subscribers (million)	Penetration
2010	18.067	125.9%
2011	19.479	132.4%
2012	20.787	137.8%
2013	21.716	140.4%
2014	16.911	106.6%
2015	18.121	111.5%
2016	18.264	113.9%
2017	19.986	122.3%
2018	20.467	125.2%
2019 (e)	21.260	129.7%

Source: BuddeComm based on ITU and regulator data



Source: BuddeComm based on ITU and regulator data

정보보호 시장 현황

1) 시장 규모

시장 개요

▶ 도미니카공화국-중앙미국자유무역협정(The Dominican Republic-Central American Free-Trade Agreement, DR-CAFTA)으로 과테말라와 미국과의 무역 시장 개방

- 미국으로부터의 수입품은 대부분 상업, 제조업, 전기, 은행 및 보험, 통신 등이며 정보 보호 시장의 규모는 상당히 작은 편
- 과테말라의 경제 지표는 대부분 비공식적이며, 경제의 핵심 요소는 대부분 미국에 정착한 이주민으로부터의 송금이 차지
- 치안상태가 최하위라고 평가되며 아직 해소되지 못하고 있는 빈부격차로 인한 민생범죄와 마약관련 범죄, 피싱 및 절도 등 다양화되고 있는 사이버 범죄 등으로 인한 정보 보안 수요가 점차 증가

2) 분야별 현황

물리 보안제품 및 서비스

▶ 중국과 미국이 시장을 장악하고 있으며 기업과 주택 소유자들은 경보, 감시 카메라, 조명 등 예방 장비에 대한 관심이 높아지는 추세

- 중국 정부는 과테말라 보안 프로젝트에 대해 세제 혜택, 면제 및 무제한 자금 지원을 통해 카메라, 비디오 레코더 및 기타 보안 장비 제조업체를 지원 중

▶ 주거용, 산업용, 사무용 보안장비에 대한 수요 증가

표 _ 과테말라 시장(안전 및 보안 포함) 규모 추이

(단위: 천 달러)

구분	2016년	2017년	2018년	2019(추정)
총 수출	22,857	23,744	25,243	25,674
총 수입	616,253	623,574	634,657	632,728
미국에서 수입	312,294	314,088	322,554	327,667

[출처] 미국 상무부, International Trade Administration

▶ 다양한 물리보안 제품 외에도 최근 들어 정보보안용 시스템, 단말기, 솔루션 등이 시장에 공급되고는 있으나 세관의 수입통계 분류 모호성으로 시장규모를 파악하기 어려운 시장

3) 주요 동향 및 이슈

▶ 마약 밀매, 조직범죄, 사회적 격차, 빈곤과 관련된 보안 문제 끊이지 않고 직면

- 대부분의 심각한 범죄는 지역 폭력조직에 의해 일어나며, 유죄판결 부족 및 기소 불충분 등 비효율적이고 불충분한 경찰력이 나라를 불안하게 만드는 형편
- 미국 상무부(The International Trade Administration)의 2019년 8월 26일 자료에 따르면, 지난 4분기 동안 과테말라에서 안보 이슈의 초점은 시민 갈등의 폭력에서 더 높은 수준의 범죄로 바뀌었으며, 과테말라의 약한 기관들, 주정부 기관이 없는 외딴 지역들 그리고 남미의 마약 생산국들과 미국의 소비자들 사이의 국가의 지리적 위치로 과테말라를 마약 밀매업자들과 다른 조직화된 범죄 집단의 주요 표적으로 삼았다고 발표
- 이로 인해 과테말라 시민들은 지방 사법 기관에 대한 신뢰가 거의 없으며, 이러한 전국적인 정서와 관련하여, 2007년 과테말라 정부는 과테말라에서 유엔 과테말라 임피던트 방지 위원회의 도움으로 부패한 불운함을 해결하고자 시도

▶ 경찰에 대한 불신이 커짐에 따라, 사적인 보안 수요 증가

- 기업과 시민들은 경찰이 사유재산권을 보호할 수 없다는 인식이 증가함에 따라 많은 사람들이 개인 보안을 선호하며 고용된 개인 보안과 보안 시스템에 대한 수요 증가 추세
- 13만 명의 사설 경비원이 있지만 현역 경찰관은 34,000 명 수준에 불과

▶ 심각한 살인율로 인한 민간 보안 부문이 빠르게 성장

- 과테말라는 2018년 10만 명당 22.4명의 살인 발생으로 살인율 현저하게 향상
- 2018년 3,881건의 살인 발생, 이는 2017년의 4,409건의 살인보다는 감소했으나, 여전히 높은 살인율을 보임
- 이로 인해 과테말라의 민간 보안 부문은 빠르게 성장하고 있으며, 일반 회사 예산의 약 10-12%가 민간 보안에 투자

▶ 과테말라는 시장 동향을 파악하기 위해 과테말라 보안실뿐 아니라 보안 및 안전장비 수입업체와 지속적으로 접촉하고 있으며, 수입업체들은 현재 대부분 미국산 제품에 의존하는 상황

정보보호 정책 및 기관 현황

1) 관련 법령 및 정책

관련 법령 및 규제

▶ 일반전기통신법(Ley General de Telecomunicaciones)

- 새로운 규제 체계 수립 및 기술 주체로서의 전기통신 교육 창설, 시장 메커니즘을 통해 농촌 및 도시 수준의 저소득 지역의 전화 서비스에 보조금을 지급하기 위한 기금 조성

2) 담당기관

▶ 통신위원회(Superintendencia de Telecomunicaciones, SIT)

- 1996년에 설립되었으며, 통신 분야 규제 및 시장 자유화 감독 및 규제 기관
- 국가통신기반주택부(Ministry of Communications, Infrastructure and Housing, CIV) 산하에 운영
- 무선 주파수 관리 및 감독, 전기통신 레지스트리 관리, 국가 번호 부여 계획 관리 및 제재
- 필수 자원에 대한 접근으로 인해 발생하는 사업자 사이의 분쟁 해결
- 타 기관과의 조정, 국제 전기 통신 기구의 회의 및 국제 통신 조약, 협정 및 협약 협상에 참가
- 일반 전기통신법의 제재 적용

3) 규제 및 인증제도

▶ 과테말라는 보안제품에 대한 특별한 규제 및 인증을 취하지 않고 있는 것으로 보임

4) 최근 정책 동향 및 이슈

▶ 도미니카공화국-중앙미국자유무역협정(The Dominican Republic-Central American Free-Trade

Agreement, DR-CAFTA)으로 인한 과테말라와 미국과의 시장 개방

- 미국과 중앙아메리카 사이의 자유무역지대를 만드는 것을 목표로 과테말라는 2003년 말에 서명
- 동 협정으로 인해 외국인 투자 장애물이 제거되었으며, DR-CAFTA 회원국 및 미국 사업자 사이의 완전하고 공정한 경쟁을 위한 통신 시장을 개방이 가능

융합보안시장 및 정책 동향

1) 융합보안시장 동향

스마트시티

▶ 과테말라는 Salcajá시에 과테말라 최초의 스마트 시티 프로젝트 착수

- 과테말라 수출업자협회(La Asociación Guatemalteca de Exportadores, AGEXPORT)는 2019년 9월 소프트웨어 수출업체와 함께 영토 내 수출을 촉진하는 투자 촉진을 목표로 프로젝트 착수 진행 시작
- 과테말라는 1년 동안 기술 파트너 회사인 SIGEL을 통해 현지 상품을 전자상거래화할 것을 약속
- 또한 중소기업과 장인들의 네트워크를 디지털로 전환 지원, 기술 개발 이용 및 관리 예정
- 이 프로젝트를 통해 과테말라는 현지 고용 창출 및 자국민 이주 중단 등의 효과도 기대

블록체인(가상화폐 포함)

▶ 가상화폐는 2019년 들어 수요가 서서히 증가하는 추세

- 미국에서 과테말라로 송금 시 추가 요금이나 세금이 부과되는 미국의 법에 따라, 과테말라에서는 암호화폐로 송금하려는 수요가 늘어나는 추세

▶ 일본 암호 화폐 거래소 과테말라에 서비스 제공

- 일본에 기반을 둔 암호 화폐 거래소 Bitpoint는 2019년 9월 과테말라에 암호 화폐 교환이 가능한 서비스 제공 시작

핀테크 등

▶ 2019년 들어 정부의 지원이 이루어지는 추세

- 과테말라 정부는 2019년 7월 18일 회사 설립 촉진을 위한 기업가 정신 강화에 관한 법률 통과
- 이 법에는 비록 벤처 기업 및 스타트업 등에 대한 지원은 미포함되어있으나, 젊은 기업가들의 크라우드 소싱 및 암호 화폐 지원 정책이 포함

▶ 온라인 결제 및 거래 애플리케이션 2019년 과테말라 시장 진출

- 과테말라 시장에 진출한 온라인 결제 및 거래 플랫폼 tPago는 2019년 9월 과테말라에 휴대전화를

통해 온라인 서비스 결제, 금융 문의, 금액 이전 및 잔액 보충 등의 서비스 제공 시작

▶ 과테말라 핀테크 회사들의 과테말라 정부에 생태계 조성 및 가능한 규제 요청에 대한 수요 증가

2) 융합보안정책 동향

사물인터넷(IoT)

▶ 지방자치단체(지자체)의 사물인터넷 등 디지털 기술을 활용한 대민 서비스 개선 시도
- 도시화로 인해 도시의 인구가 증가함에 따라 지자체 또는 공공 서비스기 기관이 대민 서비스를 제공해야 할 시민의 수와 서비스 수요가 증가
- 사물인터넷(IoT)은 일상적으로 대민 서비스를 제공해야 하는 지자체들이 도시 주민들을 대상으로 제공하는 대민 관련 응용 프로그램을 제공할 수 있게 해주는 중요한 기술적 기반으로 작용
- 즉, 사물인터넷을 활용한 공공 서비스의 디지털화를 통해서 도로 차단이나 수리 등과 같은 대민 공공 정보를 사전 혹은 실시간으로 제공 가능
- 또한 사물인터넷 기반의 디지털 대민 공공 서비스를 통해서 지방세 과금과 같은 세금 혹은 공공 서비스 요금 지불과 수금 메커니즘을 개선하는 것도 기대할 수 있음

핀테크 등

▶ 과테말라 핀테크 기업들이 증가하는 가운데, 과테말라 중앙은행이 핀테크 스타트업들의 동향과 기존 금융 시스템에 미칠 영향을 연구하기 시작
- 2017년 미주개발은행에 의하면, 2017년 12월 기준 과테말라 핀테크 기업 수는 4개에 불과했으나, 2019년 2분기 기준으로 16개로 증가한 것으로 파악되고 있음
- 과테말라 핀테크 기업의 증가로 인해서 과테말라 중앙은행(superintendency of banks guatemalan)은 핀테크 기업들의 전통적 금융 시스템에 미칠 영향과 관련 규제 정비에 나서고 하는 상황

바. 엘살바도르

'18년 GDP(십억달러)	26.057
'18년 인구수(천명)	6,420

■ ITU 글로벌 사이버보안 지수(Global Cybersecurity Index, GCI)

· 엘살바도르의 사이버보안 지수는 우리나라보다 매우 낮은 수준이며 순위도 2017년에 비해 최하위권으로 하락

국가명	2018		2017		전년대비 증감	
	지수	순위	지수	순위	지수	순위
엘살바도르	0.124	142	0.208	108	-0.084	-34
대한민국	0.873	15	0.782	13	+0.091	-2

■ ICT 관련 주요 지수

· 엘살바도르의 전반적인 ICT 발전 수준은 전 세계 167개국 가운데 최하위권에 속해 있음

지표명	엘살바도르		한국	
	점수	순위	점수	순위
IMD 국가경쟁력지수(2019)	-	-	-	28
IMD 디지털경쟁력지수(2019)	-	-	-	10
UNCTAD 전자상거래지수(2019)	37.2	96	89.4	19
ITU 글로벌 사이버보안 지수(GCI 2018)	0.124	142	0.873	15
UN 전자정부 지수(2018)	0.538	81	0.901	3

■ ICT 관련 주요 통계(ITU, 2017년 말 기준)

· 엘살바도르의 이동통신 보급률은 유선통신 보급률에 비해 매우 높은 편

항목	엘살바도르		한국	
	가입자수(천 명)	보급률(%)	가입자수(천 명)	보급률(%)
유선전화	915	14.33	26,845	52.54
유선브로드밴드	415	7.06	21,196	41.48
이동통신	9,478	148.37	63,659	124.59
인터넷 이용률	33.82%		95.07%	

정보보호 산업 개요

1) 보안 환경

정보보안 환경

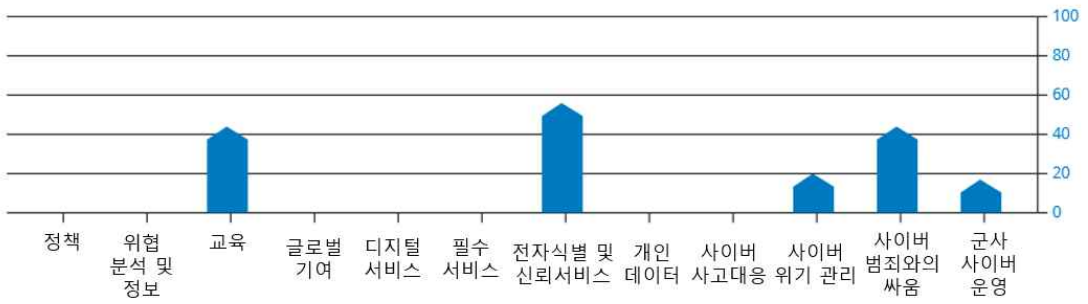
▶ 엘살바도르의 정보보호 산업 환경은 라틴 아메리카와 카리브해 평균보다 상당히 낮은 상태

- 정보보호에 대한 국가 수준의 정책이나 전략, 사이버 보안에 관련된 규제도 제대로 갖춰지지 않았음
- 최근 사이버 범죄 처벌을 위한 국가의 첫 번째 노력으로 사이버범죄 관련된 특별법이 시행 중이며, 전자 상거래 규제 체계는 아직 갖춰지지 않았으나 2015년 의결된 전자 서명법이 존재
- 사이버 공격에 대응하기 위하여 국가 CIRT에 해당하는 SalCERT를 유지하고 있으며, 경찰의 조사부서 내 사이버범죄단이 UNODC의 지원과 함께 설립되어 운영 중임
- 엘살바도르 군대는 보호할 인프라의 위험과 중요한 영역을 식별했지만 공식 사이버 방어 정책은 없음
- 그럼에도 불구하고 정부는 공식적으로 중요한 국가 산업(Critical National Industry, CNI)의 보안을 관리하고 역할과 책임을 설정하고 사이버 보안의 차이를 식별하기 위한 위험 관리 실습을 계획함

▶ ITU가 2019년 3월 발표한 'Global Cybersecurity Index 2018'에 따르면 엘살바도르의 사이버보안 지수는 0.124, 글로벌 순위는 142위, 아메리카권역에서는 27위를 기록하며 낮은 수준을 보임

그림 _ 엘살바도르 국가 사이버 보안 지수 이행률

(단위: %)



[출처] e-Governance Academy(2019)

▶ eGA(e-Governance Academy)의 국가 사이버 보안 지수(National Cyber Security Index, NCSI) 2019 자료에 의하면 엘살바도르는 전자 식별 및 신뢰 서비스 분야에 가장 높은 이행률을 보임

- 또한 사이버 교육, 사이버 범죄와의 싸움 분야에서도 많은 노력을 하고 있으며, 사이버 위기 관리 및 군사 사이버 운영 분야에도 노력을 보임
- 그러나, 사이버보안에 관련된 정책, 위협 분석 및 정보, 글로벌 기여, 디지털 서비스 방어 및 필수 서비스에 대한 방어, 개인 데이터 및 사이버 사고 대응 등 다수의 분야에 개선의 여지가 필요함
- 2002년 설립된 eGA는 에스토니아 정부, OSI(Open Society Institute) 및 UN 개발 프로그램의 공동 이니셔티브로서 비영리 씽크탱크 및 컨설팅 기관으로 전자 거버넌스, 전자 민주주의, 국가 사이버 보안과 같은 디지털 혁신 분야를 조사하고 분석
- eGA는 국가 사이버 보안 지수(NCSI)를 2019년에 134개국을 조사하여 웹사이트(ncsi.ega.ee)에 게시하고 있으며, 엘살바도르는 134개국 중 103번째 순위로 매우 낮음
- 좀 더 세부적인 항목을 보면, 전자 식별 및 신뢰서비스 분야에서 유능한 감독 기관, 고유한 영구 식별자, 전자 서명에서 이행률을 보이고, 교육 및 전문성 개발 분야에서 석사 수준의 사이버 보안 프로그램 및 사이버 보안 전문가 협회에서 이행률을 보임
- 또한 사이버 범죄와의 싸움 분야에서 사이버 범죄 단위, 사이버 범죄의 범죄 인식에서 이행률을 보이고, 사이버 위기 관리 분야에서 국제 사이버 위기 훈련 참가를 하였고, 군사 사이버 운영 분야에서는 국제 사이버 훈련에 참여하였음

▶ 엘살바도르는 인터넷 보급률이 약 34% 정도이므로 사이버 보안에 대한 인식도 낮음

- 2016년 3월 기준 국가 차원에서 사이버 보안 인식 제고 캠페인은 실시된 바 없으며, 정부는 대학이 사이버 보안 교육 기회를 제공할 능력은 없지만 해당 프로그램을 구축해야 한다고 필요성을 역설
- 반면, 민간 부문은 전자 상거래 서비스의 보안 필요성을 인식하고 강력한 사이버 보안 마인드를 개발하여 직원에게 사이버 보안 교육을 제공함

▶ 엘살바도르는 지속적인 치안 불안으로 2016년 미국 일간지 USA투데이는 '신(新) 세계 살인의 수도'라고 할 정도로 치안상황이 열악

- 엘살바도르는 중앙 아메리카에서 인구밀도가 가장 높은 국가로 높은 실업률, 낮은 임금, 비교적 높은 주택 비용 등과 같은 요인들로 인해 범죄 발생이 잦음
- 재산 범죄(강도, 도난 등)는 엘살바도르에서 가장 일반적인 범죄이며, 2018년 보고된 모든 사고의 약 47%를 차지, 개인에 대한 범죄(폭행, 살인, 강간, 성폭행 등)은 보고된 모든 사고의 38%를 차지함[185]
- 특히 엘살바도르는 라틴 아메리카에서 가장 높은 살인율을 차지하고 있으며, 연간 살인율은 인구 십 만명당 2016년 81명, 2017년 60명, 2018년 50명으로 줄어들고 있으나 살인 사건은 2018년 보고된 범죄 사건의 14%를 차지함
- 또한 유명 레스토랑, 호텔, 주유소 및 소매점을 포함한 ATM/ 신용 카드 범죄에 대한 우려도 존재

185 U.S. OSAC, El Salvador 2019 Crime & Safety Report, 2019.4.25.

2) 인터넷 및 통신 환경

▶ 엘살바도르는 경쟁을 장려하고 외국인 투자를 허용하는 라틴 아메리카 지역에서 상대적으로 한층 개방된 나라 중 하나에 속함

- 엘살바도르의 통신 분야는 1999년에 자유화되었고, 그 결과 유선통신뿐만 아니라 케이블 TV, 인터넷 및 기타 통신 서비스를 제공하는 많은 국내외 민간 기업들이 생겨남
- 통신시장은 소수의 지배적인 다국적 사업자들(Millicom의 Tigo, América Móvil의 Claro, Telefónica의 Movistar)이 주도하고 있으며, 이들은 거의 모든 통신 분야로 사업을 확장
- 도매 광대역통신을 촉진하는 규정이 없기 때문에 DSL 시장은 선두 주자인 Claro가 사실상 인터넷 서비스 제공(ISP) 시장에서 독점권 유지

▶ 통신산업은 엘살바도르 경제에서 가장 빠르게 성장하는 분야 중 하나에 해당함

- LTE 망 기반의 광대역 이동통신이 발전함에 따라, 모바일 인터넷 시장도 활발히 빠르게 성장 중
- 2019년까지 더 많은 신규 케이블에 대한 지속적인 투자로 인해 유선 통신 산업 역시 발전할 것으로 예측

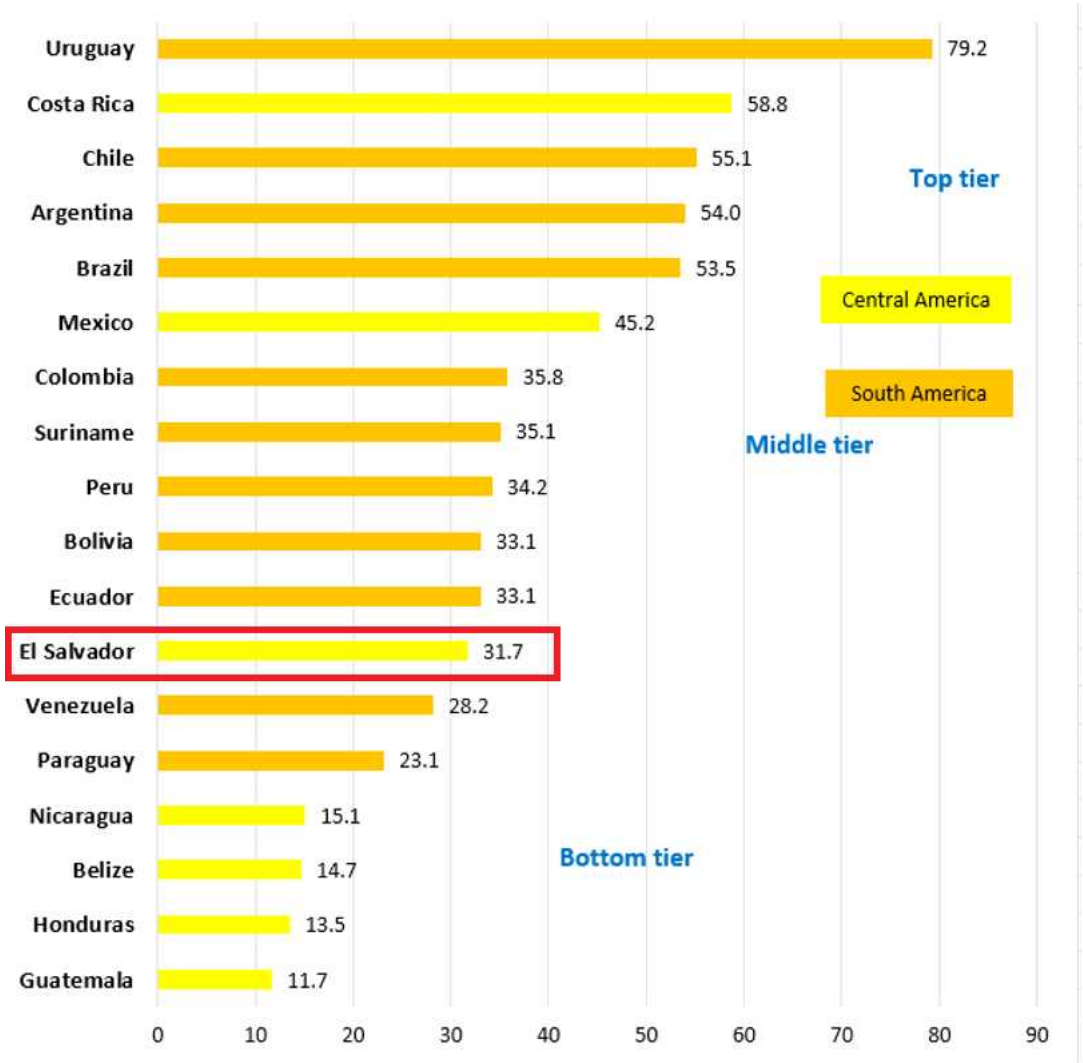
▶ 모바일 서비스 보급률은 낮지만 꾸준히 성장 중

- 광대역 이동통신 개발은 느린 주파수 할당으로 지연되어 왔으며, 3G는 널리 이용 가능
- LTE는 현대화 3개년 계획에 따라 2014년 첫 개통되었으며, LTE 기술 적용 커버리지는 상당히 좁은 편

▶ 유무선통신 시장, 통신규제환경, GDP 등을 고려한 BuddeComm의 분석에 따르면 엘살바도르는 통신서비스 지수(Telecoms Maturity Index)가 31.7%로 라틴 아메리카에서 통신 시장 특성에 따라 리더, 챌린저, 신생의 세 단계로 구분할 때 중간인 챌린저에 위치

- 엘살바도르의 유선전화 밀도는 모바일 전용으로 대체되어 중앙 아메리카 평균보다 약 5배 높고, 라틴 아메리카 및 카리브해 평균보다 5배 낮은 편임
- 엘살바도르 도심과 시골 간 통신 시설이 각각 34%와 4%로, 도심에는 비교적 현대적인 네트워크가 있으나, 시골 지역은 매우 열악한 상태
- 그러나 엘살바도르는 여전히 높은 비율의 인구가 시골 지역에 살고 있는 상황

그림 _ 라틴 아메리카의 통신서비스지수에서 엘살바도르의 위치



[출처] BuddeComm(2019.5.)

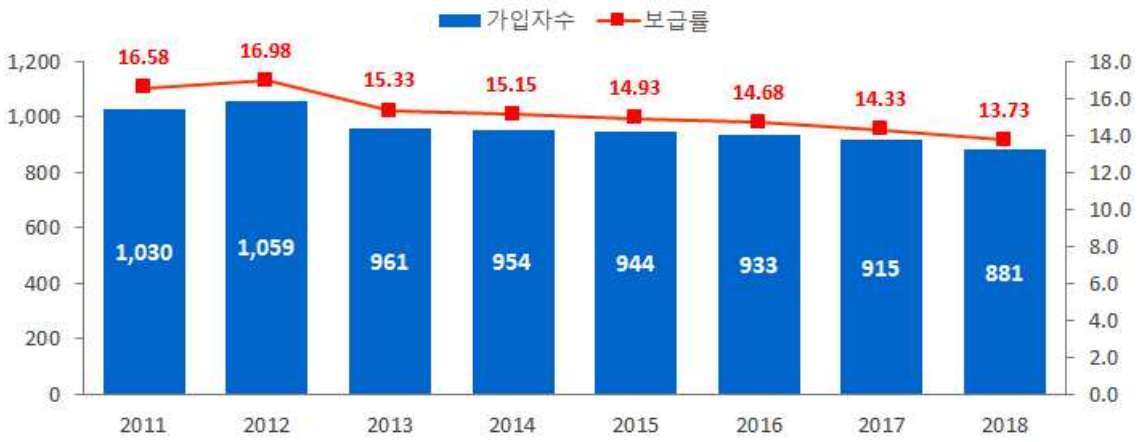
▶ 유선통신

- ITU의 자료에 의하면 2018년 말 기준, 유선통신 가입회선 수는 88만 1,334회선을 기록, 2017년 91만 5,303회선 대비 약 3.7% 감소하였음
- 유선통신 보급률은 2009년 17.85%로 최고치를 보인 후, 전체적으로 감소추세를 보이는데, 이는 2010년 이후, 특히 2017년 이동통신 서비스가 크게 확산되면서 유선 전화 회선 수가 크게 감소 중
- 주요 유선통신 사업자인 Claro 및 Telefónica 외에도 트리플 번들(TPS)의 일부로 유선 서비스를 제공하는 Tigo, VoIP 전화 통신 서비스를 제공하는 GCA Telecom, 지역 및 장거리 전화를 제공하는 Salnet이 있음

- Claro(América Móvil)는 엘살바도르의 주요 유선 사업자로 시장 점유율이 약 78%에 해당하며 América Móvil이 95.8%의 지분을 소유하고 있음
- MOVISTAR(Telefónica)는 유선 시장에서 약 18%의 시장점유율을 갖고 있어 Claro의 주요 유선 경쟁업체임

그림 _ 엘살바도르 유선통신 가입 회선 및 보급률 추이

(단위: 천회선, %)



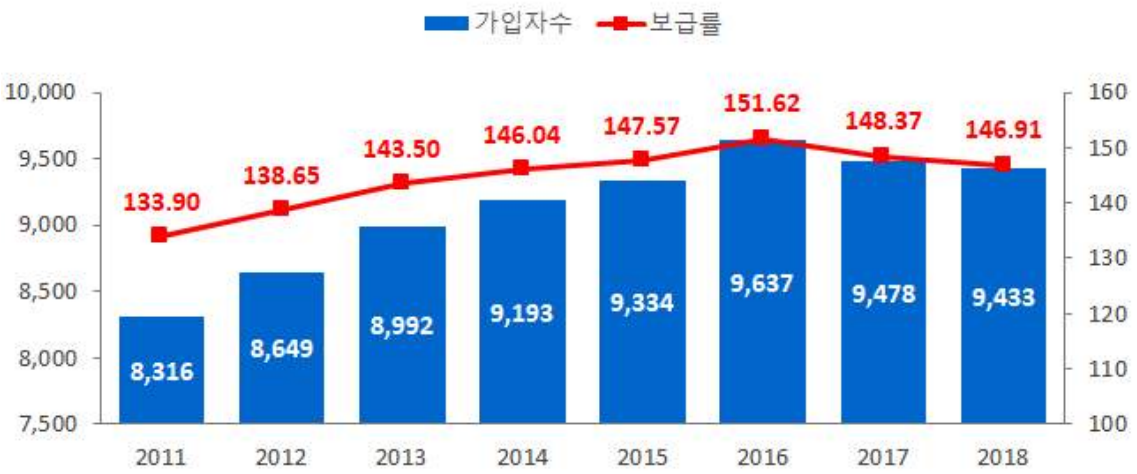
[출처] ITU Statistics DB(2019.6)

▶ 이동통신

- 2003년 이후 꾸준히 성장하고 있는 이동통신 부문은 가장 역동적인 통신 부문
- 사업자간의 치열한 경쟁과 유선 서비스 신청 후 이용에 대한 긴 대기 기간도 이동통신 성장에 기여하였음
- 또한 유선통신 연결이 빈약하거나 존재하지 않는 시골 지역에서는 성장이 빠르게 진행
- ITU의 자료에 의하면 2018년 기준 이동통신 가입자 수는 약 943만 2,925명을 기록하며 보급률이 146.91%로, 보급률은 2017년 대비 약 1.46% 감소하였고, 2011년부터 2018년까지 가입자 수의 연평균 성장률(CAGR)은 1.8%를 기록함

그림 _ 엘살바도르 이동통신 가입 및 보급률 추이

(단위: 천 명, %)



[출처] ITU Statistics DB(2019.6)

- 전국의 전화선 중 6%가 유선전화인 반면 약 94%가 이동전화 네트워크로, 이동전화 보급률이 유선전화 대비 월등히 높으며, 또한 라틴 아메리카 및 카리브해 지역의 평균보다도 약 3배 높음
- 엘살바도르의 이동통신 시장은 2018년 기준 5개 네트워크 사업자 Tigo, Movistar, Claro, Digicel, Intelfon가 서비스를 제공함
- 경쟁 당국이 2019년 5월 Telefónica 그룹이 현지 사업부를 Claro 브랜드 하에 운영되는 América Móvil에 판매하는 것을 평가하기 시작했으며, 승인되면 모바일 부문은 더 통합되어 2019년 후반에 4개의 사업자로 줄어들며 통합 서비스를 개발하기에는 더 좋은 지배적 환경이 만들어 질 것임
- 규제기관은 2016년 말 이동통신 네트워크는 85%의 인구 커버리지, 81.7%의 지리적 커버리지를 제공하며, 3G 네트워크는 인구 커버리지의 61%에 해당한다고 발표
- Claro는 2008년 초 엘살바도르에서 처음으로 3G 서비스를 제공한 이래 2017년 말 3G 가입자 수가 2G를 넘어 섰음
- 그러나 LTE 인프라의 범위와 기능을 확대하려는 이동통신사(MNO)의 투자에 따라 LTE 가입자 수가 빠르게 증가할 전망
- 단, 이동통신 서비스에 충분한 주파수 대역이 할당되지 않아 통신네트워크 사업자의 LTE 인프라 구축 속도가 느려, 엘살바도르는 주변 국가들에 비해 LTE 서비스 제공이 늦은 국가에 해당함
- Movistar는 2016년 11월 엘살바도르에서 LTE 서비스를 최초로 시작했으며, 공급업체로 Ericsson과 계약했음
- 2016년 연말 Tigo의 LTE 서비스가 이어졌으며, 2020년까지 LTE 서비스를 인구의 80%에 제공할 것으로 예상했으며, 이를 위해 최대 10억 달러를 투자할 것임

- Digicel은 2017년말 LTE 서비스를 시작했음
- LTE 지원 스마트폰의 광범위한 가용성으로 LTE 가입자는 2017년 중반 약 30만 명으로 성장하였으며, 2017년 4분기 기준 엘살바도르의 LTE 커버리지는 44.7%에 해당함[186]

▶ 인터넷 이용 환경

- ITU의 자료에 의하면 2017년 기준 인터넷 보급률은 33.82%로, 2016년 29% 대비 4.82% 증가함
- 엘살바도르는 도매 브로드밴드를 홍보하는 규제가 없어 DSL 시장의 선두주자인 Claro가 사실상 독점을 유지함
- 브로드밴드 시장에서 유일하게 효과적인 크로스 플랫폼 경쟁은 소수의 케이블 사업자이며, 최근 몇 년간 시장 통합이 이루어져서 Telemóvil은 지역 케이블 TV 제공업체인 Caribena Cable을 인수하였음
- BuddeComm의 자료에 의하면, 엘살바도르에서의 브로드밴드 인터넷 이용은 2018년 기준 모바일 브로드밴드 기반 이용자 수는 약 421만 명으로 보급률 61.9%에 해당하며 모바일 브로드밴드 가입 연평균성장은 17.7%로 높은 성장세를 보임
- 유선 브로드밴드 기반 이용자 수는 약 48만 1,000명으로 보급률 7.4%에 해당하며 유선 브로드밴드 가입자 연평균성장은 8.5%를 보임

표 _ 엘살바도르의 플랫폼별 브로드밴드 보급률(2018년 기준)

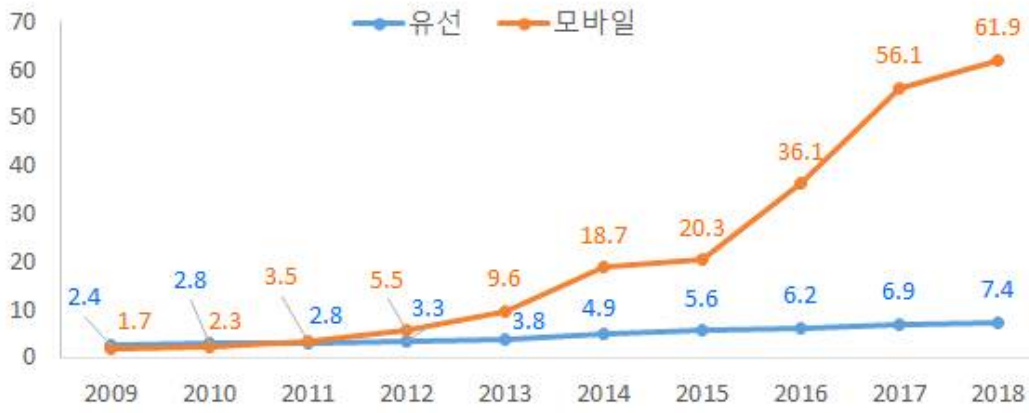
구분	이용자 수	점유율
모바일	4,210,000	61.9%
유선	481,000	7.4%
전체	4,691,000	100%

[출처] BuddeComm(2019.5.)

186 Alliance for Financial Inclusion, The Digital Financial Services Ecosystem in Latin America and The Caribbean, AFI Special Report, 2019.7.

표 _ 엘살바도르의 플랫폼별 브로드밴드 보급률 추세

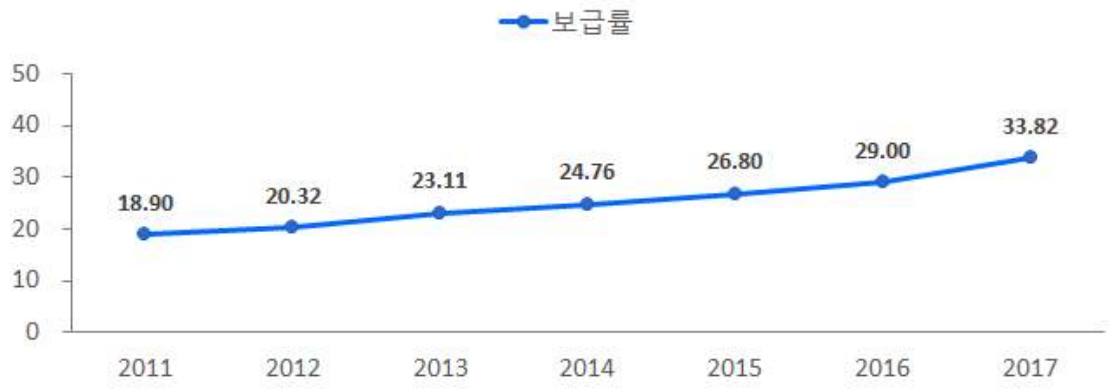
(단위: %)



[출처] BuddeComm(2019.5.)

- 주요 유선 브로드밴드 플랫폼은 DSL이며 그 외 케이블이 시장을 차지하고 있으며, 유선 브로드밴드 사업자로는 DSL 접속을 제공하는 Claro, 케이블 접속을 제공하는 Tigo, 케이블 접속 브랜드 Integra를 제공하는 Telefónica, 자체 광섬유 네트워크를 통한 DSL 접속을 제공하는 Salnet이 있음
- 모바일 네트워크 사업자는 거의 전국적인 모바일 브로드밴드 커버리지를 제공함
- 2019년까지 가장 빠르게 성장하는 통신 분야는 이동통신과 브로드밴드로 모바일 브로드밴드에 대한 전망이 특히 유망함
- 모바일 브로드밴드는 3G 인프라에 오랫동안 의존했지만 최근에는 LTE 인프라로 이동하고 있음
- Tigo의 3G 모바일 브로드밴드 서비스는 엘살바도르 전역의 주요 도시를 대상으로 하며, Claro의 서비스는 San Salvador 및 인근 도시로 제한됨
- ITU의 자료에 의하면 인터넷 보급률은 2017년 기준 33.82%에 해당하며 전년 대비 4.82% 증가함

그림 _ 엘살바도르 인터넷 보급률 추세



[출처] ITU Statistics DB(2019.6)

▶ 전자상거래

- 전자상거래 및 결제시장 전문 조사기관 yStats에 의하면, 엘살바도르의 전자상거래 시장은 2017년 1억 2,000만 달러에서 2020년 2억 2,000만 달러 규모로 성장할 것으로 예측하며, 연평균성장률(2017~2020)은 22% 이상으로 예상되어 라틴아메리카 지역에서 전자 상거래 시장이 빠르게 성장하는 국가 중 하나로 추정됨[187]
- 라틴아메리카 지역에서 전자상거래 시장의 연평균 성장률(2017년~2020년)이 가장 클 것으로 예상되는 국가는 아르헨티나(+32%)이며. 이후 콜롬비아(+27%), 멕시코(+25%) 순으로 나타나며, 이에 이어 엘살바도르는 과테말라(+22%)와 동일한 성장률로 예상됨
- AFI(Alliance for Financial Inclusion)의 2019년 7월 자료[188]에 의하면, 엘살바도르의 온라인 인증 및 식별 시스템은 전자 상거래 개발 초기 단계에 있기 때문에 개발이 미진한 수준
- 세계은행의 Global Findex Data 2017 자료에 의하면[189], 엘살바도르는 2017년 기준 인구의 30%가 은행 계좌를 갖고 있으며, 지난 1년 동안 인터넷을 통해 온라인으로 물품을 구매하거나 청구서를 지불한 경우는 인구의 4%에 해당하여, 이는 라틴아메리카 및 카리브해 지역 평균 11%에 비해 낮은 수준을 보임
- 2017년 기준 휴대전화 금융 서비스의 보급률은 4.6%로 라틴아메리카 지역의 평균 1.7%에 비해 전체 금융 서비스 사용률이 낮음에도 불구하고 빠르게 확산되고 있음
- 온라인 쇼핑 플랫폼을 갖춘 Aerocasillas는 2015년에 엘살바도르의 인터넷 판매가 전년 대비 25% 증가했으며, 고객의 90%가 온라인으로 서비스를 주문한 반면 10%만이 물건을 주문하러 실제 매장을

187 "Global E-Commerce Intelligence, Latin America B2C E-Commerce Market 2018", yStats, 2018.11.
188 The Digital Financial Services Ecosystem in Latin America and The Caribbean, AFI Special Report, Alliance for Financial Inclusion, 2019.7.
189 The Global Findex Database 2017, The World Bank: https://globalfindex.worldbank.org/

방문하였음

- 현지 신문인 El Diario de Hoy, 글로벌 소비자 조사회사인 Kantar Worldpanel의 데이터를 인용, 엘살바도르의 인터넷 사용자 중 7%만이 지역 평균과 같이 온라인 구매를 하는 것으로 나타났으며, 대부분의 구매는 영화표, 휴가 패티지와 같은 엔터테인먼트 또는 라이프 스타일 상품이라고 보도(2016년 6월)
- 엘살바도르 국민은 신용카드나 직불카드 정보 공개와 같은 온라인 상품 및 서비스 구매의 보안에 대해 여전히 우려를 보임
- 미국에 기반을 둔 물류회사인 Aerocasillas와 Trans Express에 따르면 엘살바도르의 전자 상거래 시장은 사람들이 점점 더 미국에서 상품을 구매하기 위해 온라인을 사용하게 되는 유망시장으로 평가

정보보호 시장 현황

1) 시장 규모

시장 개요

▶ 엘살바도르에서는 이동통신 시장의 강한 성장으로 인터넷 접속과 전자화폐, 모바일 결제 사용이 증가함에 따라 특히 금융, 통신 분야 정보보안 수요가 존재하는 것으로 예상됨

▶ 엘살바도르 전국 곳곳의 폭력조직이 벌이는 범죄는 현재 경찰 역량으로 통제가 어려운 상황이며,[190] 이에 대한 CCTV, 치안 시스템 등에 대한 수요가 존재함

- 한국의 KOICA는 지난 2010년, 2017년 치안역량 강화 1, 2차 사업을 통해 CCTV 치안 시스템을 엘살바도르에 최초 설치(제1차 사업)하고 자체운영체계 수립을 지원한 적 있음
- 제1차 사업에서 수도 산살바도르 센트로 지역 우범지역에 방범 카메라 50대 설치, 2차 사업에서는 시내 주요 차량 진출입로 17개 지점에 차량번호판 자동인식 카메라 66대 설치

시장 규모 및 성장률

▶ 엘살바도르의 정보보호 시장 규모 및 성장 전망에 대해 일반에 공개된 자료는 없는 것으로 보임

2) 분야별 현황

물리보안 제품 및 서비스

▶ 2019년 5월 엘살바도르 외교부와 한국의 KOICA는 수도 산살바도르에서 범죄예방 및 현지 경찰 범죄수사 역량을 강화하는 '엘살바도르 치안역량강화 3차사업' 협의의사록을 체결함[191]

- 해당 사업은 2019년부터 2024년까지 550만 달러를 지원해 수도 산살바도르를 포함 광역수도권을 대상으로 실시하는 프로젝트로 주요 내용은 CCTV 시스템 구축, 경찰청 911센터 내 CCTV 통합

190 KOICA, 코이카, 엘살바도르 주민 삶 개선 위한 치안 사업 추진, KOICA 보도자료, 2019.5.24.
191 KOICA, 코이카, 엘살바도르 주민 삶 개선 위한 치안 사업 추진, KOICA 보도자료, 2019.5.24.

관제센터 구축, 범죄예방 및 수사 교육과정 구축, 자체 교수요원 양성 등으로 관련된 물리보안 제품 및 관련 서비스에 대한 수요가 존재함

- 한국의 KOICA는 범죄 발생률이 높은 수도와 인근 23개 곳에 차량번호판 자동인식카메라 80대 설치, 범죄 예방 및 범인 검거율 향상에 기여하고자 함
- CCTV를 통한 치안 강화 효과를 높이고자 기존에 중복 설치된 CCTV 관제센터를 재정비하고 관제 인력을 통합시켜 실시간 범죄 추적 효율화에 힘을 쏟고자 함
- 또한 현지 우수 경찰인력을 교수요원으로 양성해 현지 상황에 맞는 자체 교육 확대, CCTV를 활용한 현지 경찰의 방범, 수사역량 강화를 계획함

3) 주요 사업자 현황

▶ Soluciones Seguras

- 중앙아메리카의 주요 사이버 보안회사로 파나마, 코스타리카, 과테말라외에 엘살바도르 San Salvador에 사무소를 운영하고 있으며, 라틴 아메리카 국가를 대상으로 사업 수행
- Soluciones Seguras는 사이버 보안 솔루션을 제공하며, 전문가들에게 업계에 대한 많은 경험과 전문 지식을 제공함
- 네트워크, 애플리케이션 및 통신 보안 관리 분야에서 15년 이상의 경험을 갖고 있음
- 2019년 4월에는 사이버보안 지역투어 행사를 운영하여 사이버보안 전문가를 모아 엘살바도르의 회사의 주요 취약성과 대응을 위해 수행할 수 있는 조치를 지적함
- 연락처 : Home Page : http://www.solucionesseguras.com/
  e-Mail : infosv@sseguras.com
  Tel. : +503 2206-6929

정보보호 정책 및 기관 현황

1) 관련 법령 및 정책

관련 법령 및 규제

▶ 사이버 범죄 관련

- 2017년 기준 엘살바도르에서 시행 중인 사이버범죄 및 관련 권리에 대한 특별법(Special Law against Cybercrimes and Related Rights)은 사이버 범죄를 저지른 사람을 처벌하기 위한 국가의 첫 번째 노력 중 하나에 해당함[192]
- 해당 법은 승인을 얻어 범죄 제제만을 시행한다고 밝혔으며, 법이 불법으로 표시하는 행동은 다음의 예와 같음
  - 피싱 사기
  - 공공 및 민간 레지스트리의 조작
  - 괴롭힘
  - 컴퓨터 시스템에 대한 부적절한 접근
  - 컴퓨터 시스템 등의 간섭 등

▶ 데이터 보호 및 공공 정보 접근에 관한 법률

- 엘살바도르 입법부는 해당 법률을 제정하여 정보의 투명성과 자유에 대한 규범을 확립하고 시민의 개인 정보를 보호함

▶ 시민 보안 및 공존법에 대한 특별 기금(Special Contribution for Citizen Security and Coexistence Law)

- 통신 서비스에 대한 부가가치세로 13%에서 18%로 인상
- 수입된 전자장비, 모바일 장치 구매, 데이터 전송 서비스에 대한 지불, 역 요금 통화 및 선불 서비스에 대해 5% 세금 부과

▶ 전자 서명법

- 엘살바도르는 전자 상거래에 대한 규제 체계가 없지만 전자 서명법(Decree 133/2015)을 2015년 10월 의결함

---

192 Garcia & Bodan News, Cybercrimes in El Salvador, 2017.9.7.

- 해당 법안을 통해 경제부((Ministerio de Economía – MINEC)는 전자 서명을 규제할 수 있으며, 사용자는 개인 키를 얻기 위해 등록해야 함
- 고객신원확인제도(KYC, Know-Your-Customer) 적용 대상 단체에는 은행, 농업 신용기관, 연금기관, 보험회사, 환전소, 감사인, 회계사, 공증인, 게임센터, 자동차 딜러 및 증권 딜러가 포함됨
- 전자서명법은 총 71개 조항으로 구성되어 있으며 다음의 내용 등을 포함함
  - 기술의 중립성
  - 개인의 데이터 처리방식
  - 전자서명의 법적 가치
  - 사용자들의 권리와 의무
  - 서비스 공급업체 허가 관련 내용

주요 전략 및 정책

▶ 사이버보안 관련 국가 전략 및 정책

- 2015년 ITU의 자료에 의하면[193] 사이버 보안에 대한 확립된 국가 전략 또는 정책은 없지만 개발 중인 것으로 조사됨

2) 담당기관

▶ 법무부(Ministry of Justice and Public Security)

- 엘살바도르의 사이버보안 정책의 국가 기관에 해당함
- 정보 도구 및 통신 전략을 만들고 유지하며 지속적으로 개선하는 것을 목표로 함
- 사이버 보안 정책을 정의하고 구현하는 것을 목표로 함
- 예방, 사건에 대한 관심, 인식 및 교육 워크숍을 관리하고 수행하기 위한 CSIRT의 생성을 강조하여 사이버 보안 집행 기관을 위한 제도적 전략 추진
- 2016년 기준 국가 사이버 보안 전략을 개발 중이지만 완성된 초안을 발표하지 않았음

▶ 엘살바도르 컴퓨터침해사고대응센터(SalCERT)

- 엘살바도르는 사이버 공격에 대응하고 다른 지역 대응팀과 협력하는 국가 CIRT인 SalCERT를 유지함
- SalCERT는 위협을 성공적으로 모니터링하고 해결하지만 예산 제약으로 인해 역량이 제한되었음

193 ITU, CYBERWELLNESS PROFILE REPUBLIC OF EL SALVADOR, 2015.4.

▶ 국가 경찰의 조사부서 사이버범죄단(Cybercrime Unit, Division of Investigation)

- 유엔 마약 및 범죄사무소(United Nations Office on Drugs and Crime, UNODC)와 엘살바도르 경찰에 의해 서명된 양해각서의 틀 안에서 설립되었으며 국가 경찰 소속임
- 사이버범죄단에는 디지털 법의학 연구소가 없지만 SalCERT의 기술 지원을 받아 성공적으로 임무를 수행하였음
- UNODC와 함께 사이버 범죄 부서의 미래를 형성하고자 컴퓨터 범죄 그룹, 검사 및 경찰 요원을 대상으로 사이버 범죄 조사 기업에 대한 교육도 실행되었음
- 사이버범죄단은 UNODC의 기술적 지원과 함께 어린이, 청년, 부모, 교사 등에게 정보통신 기술을 사용 시 직면하는 위협에 대한 예방 활동을 통해 사이버 범죄 발생과 관련된 건설적인 정보 교환을 통해 경찰과 시민의 관계를 강화하는 훈련을 이행함

3) 규제 및 인증제도

▶ 엘살바도르는 정보보호와 관련된 별도의 인증제도가 없는 것으로 조사됨

4) 최근 정책 동향 및 이슈

▶ 엘살바도르 공공안전부는 한국인터넷진흥원(KISA)이 운영하는 **글로벌 사이버보안 협력 네트워크**인 CAMP 회원으로 새로 가입(2019.4)[194]

- KISA는 중남미 권역의 사이버보안 협력 확대를 위해 코스타리카 과기부와 중미경제통합은행과 함께 글로벌정보보호센터(GCCD) 역량강화 세미나 및 글로벌 사이버보안 협력네트워크(CAMP)* 제 5차 지역포럼을 코스타리카 산호세에서 2019년 4월 25일~26일 개최했음

  * CAMP(Cybersecurity Alliance for Mutual Progress)는 한국 주도의 사이버보안 논의를 위해 KISA가 운영중인 국제협의체로 2019년 4월 기준 43개국, 57개 기관이 회원으로 활동 중

- 엘살바도르 공공안전부는 CAMP 제5차 지역포럼에서 CAMP 회원으로 새로 가입하여 자국의 사이버보안 현황을 공유했으며 역내 회원들과 더불어 중남미 지역 국가 사이버 보안 전략 과제와 협력 방안에 대해 논의하는 시간을 가짐

▶ 한국의 과학기술정보통신부와 한국정보화진흥원은 엘살바도르에 정보접근센터를 개소함(2018.12)[195]

194 인터넷진흥원, 중남미 권역 사이버보안 역량강화 세미나 개최, 한국인터넷진흥원보도자료, 2019.4.26.

- 엘살바도르 사카테콜루카에 위치한 한-엘살바도르 정보접근센터 개소식에는 현지 교육부 장관, 과학기술부 차관, 정보접근센터 운영을 담당하는 중미기술훈련원 원장 및 관계자 50여명이 참석
- 해당 정보접근센터는 개도국의 정보격차 해소 및 정보화교육 환경 개선을 위한 한국의 무상원조 사업의 일환이며, 기존에 구축하였던 정보화 교육장 세미나실, 사무실 뿐 아니라 장애인을 위한 전용 인터넷 라운지 구축, 콘텐츠 제작실을 구축함

▶ 엘살바도르 교육부는 UNODC 교육 자료를 사용하여 학교에서 사이버범죄 예방을 위한 전국 캠페인을 실행 (2018.10)[196]

- UNODC(United Nations Office on Drugs and Crime)는 엘살바도르의 학교에서 사이버 범죄 현상을 해결하기 위해 교육부와 협력하여 교사를 위한 전문교육, 학교를 위한 시청각 자료 및 인쇄물 개발 및 설치 등을 수행함
- 학교를 위한 시청각 자료 및 인쇄물은 사이버 괴롭힘, 인터넷 프라이버시, 사이버보안 등의 주제영역을 기반으로 인터넷에서 스스로를 즐기면서 돌볼 수 있도록 하는 캠페인의 부분으로 개발됨
- 해당 캠페인은 어린이에게 영향을 미치는 주요 사이버 범죄를 알리고 예방하며 인터넷에서 개인정보 보호 및 안전 유지의 중요성을 강조하는 것을 목표로 함'
- 해당 교육자료는 UNODC와 Telefónica El Salvador의 지원으로 카타르주의 재정 지원을 통해 개발되었음

5) 정보보호 스타트업 관련 정책동향

▶ 엘살바도르는 정보보호 스타트업 관련 정책 내용이 아직 없는 것으로 조사됨

195 과학기술정보통신부, 과기정통부, 중미 엘살바도르에 정보접근센터 개소 , 과학기술정보통신부보도자료, 2018.12.20.
196 인터넷진흥원, 중남미 권역 사이버보안 역량강화 세미나 개최, 한국인터넷진흥원보도자료, 2019.4.26.

융합보안시장 및 정책 동향

1) 융합보안 시장 현황

핀테크

▶ 엘살바도르 시장에서 기능적으로 운용되는 두 가지 주요 전자화폐(e-Money)는 Tigo Money와 MoMo이며, 이 두 회사의 고객들 간의 전자화폐 사용이 계속 증가하고 있음

- Tigo와 Momo는 3,000명 이상의 에이전트와 1백만명 이상의 사용자를 보유하고 있으며, 각 지방 자치단체와 성인 인구의 90%와 16%에 해당함
- 사용자는 현지 송금, 방송 구매. 국제 송금 및 기타 거래를 수행할 수 있음
- 이동통신 사업자 Tigo는 2011년 말 Western Union과 제휴하여 국제 모바일 송금 서비스인 Tigo Money를 시작했으며, 이 서비스를 통해 엘살바도르, 온두라스, 과테말라의 고객은 해외에서 직접 모바일 머니 지갑으로 돈을 받고 Tigo 매장에서 현금으로 환전할 수 있음
- Tigo Money는 2017년에 5억 달러의 거래를 보고 했으며, 이는 가족 송금 6억 4천5백만 달러를 포함하고, 전기 청구서의 25%를 포함하며, 또한 송금 중에서 90%는 미국에서 왔음
- Tigo Money의 거래 대부분은 전자 지갑(e-Wallet)과 마찬가지로 지불 및 송금을 포함하여 무료임

▶ Banco Agrícola은 셀카 찍어서 은행 계좌를 개설할 수 있는 디지털 제품을 출시[197]

- 엘살바도르의 주요 은행인 Banco Agrícola는 비은행 고객을 위해 Mobbeel의 신원확인 기술인 Mobbscan을 은행의 모바일 앱에 통합하여 수행
- MobbScan을 사용하면 DUI (Documento Único de Identidad)나 주민 카드와 같은 신분 증명서를 자동으로 스캔하여 은행 계좌를 개설하려는 고객의 신원을 확인 할 수 있으며, 이에 포함된 정보를 확인하고 안면 생체 인식을 통해 고객을 식별할 수 있음

2) 융합보안 정책 현황

핀테크

197 VIA News, Take a Selfie and Open a Bank Account in El Salvador, 2019.6.19.

▶ 2014년 1월 중앙 준비 은행(Central Reserve Bank, BCR)는 모바일 금융 서비스에 대한 규제 프레임워크를 마무리함

- 이동통신네트워크사업자(MNO)가 설립한 자회사를 통해 신용충전, 현금인출 및 예금, 청구서 지불 등 다양한 모바일 지불(m-payment) 서비스를 가능하게 함

▶ 금융포용법(Financial Inclusion Law)은 전자 화폐(e-money)를 엄격하게 규제함

- 법인이 제공하는 전자화폐는 법에 의해 100% 보증되며 중앙 준비 은행(BCR)에 예치금으로 보유됨
- 단일 거래는 300달러를 초과할 수 없으며, 월 거래는 1,200 달러로 제한됨

▶ Economist Intelligence Unit(EIU)의 2019년 자료에 의하면[198], 엘살바도르는 핀테크를 위한 감독 프레임워크를 개발하고 있음

- 엘살바도르 규제 당국은 금융거래에 대한 불균형 세금을 제거하고, 고객이 원격으로 개설할 수 있는 간단한 은행 계좌를 만들었음
- 2015년에 엘살바도르 정부는 금융 포용을 촉진하기 위해 법률을 통과시켰으며, 공공, 민간 및 국제 행위자와의 조정을 위해 수행된 후속 노력은 e-money 제공업체, 전자 임금 지불(electronic wage payments) 및 보다 큰 에이전트 네트워크의 도입을 통해 금융서비스에 대한 접근을 확대했음
- 2019년 11월, 엘살바도르 대법원은 1,000달러를 초과하는 금융거래에 대한 세금(이전에는 금융거래에 관한 세금법 No. 764/2016에 승인되었음)이 위헌이라고 선언하였음
- 전자 금융 서비스의 사용이 증가하고 있고, 2018년에 DaviPlata는 엘살바도르에서 최초의 온라인/모바일 저축예금 계좌를 사용자가 원격으로 개설하고 제어할 수 있게 했음
- EIU가 해당 보고서를 통해 5개 범주와 55개 국가에서 재정적 포용환경을 평가하였으며 엘살바도르의 경우 강점인 내용은 제품 및 판매점 영역의 금융 판매점으로 에이전트, 판매자 및 전자 채널이 포함됨
- 반면, 개선이 필요한 내용은 안정성 및 통합성 영역의 사이버 보안에 대한 책임, 소비자 보호 영역의 데이터 프라이버시 및 사이버 범죄 보호가 포함됨

198 Economist Intelligence Unit, Global Microscope 2019: The enabling environment for financial inclusion, 2019.

5. 중동·동유럽 시장

중동·동유럽 시장 개요

▶ 중동(Middle East)[199]은 동지중해부터 페르시아만까지 이르는 지역을 뜻하는데, 그 범주는 뚜렷하게 정해져 있지 않으나, 전통적으로 이집트에서부터 아라비아 반도 및 이란 등을 포함

- 걸프지역(The Persian Gulf): 아라비아반도와 이란사이의 만(gulf)인 페르시아만 일대를 말하며, UAE, 사우디아라비아, 카타르, 쿠웨이트, 이란, 이라크, 오만 등이 이 지역에 속함
- 마그레브지역(Maghreb): 아랍어로 '서쪽'이란 뜻으로 아라비아반도 기준 서쪽에 위치한 북서아프리카 지역의 이집트, 모로코, 알제리, 튀니지, 리비아, 모리타니 등을 포함
- 레반트지역(Levant): 역사적으로는 지중해 동쪽지역을 의미하며, 1920년 프랑스의 시리아, 레바논 점령 후부터 요르단, 레바논, 시리아, 이스라엘, 팔레스타인 등이 레반트 국가로 불림

▶ 동유럽의 경우에도 그 지역이 뚜렷하게 정해져 있지는 않으나, 흔히 독일과 오스트리아를 경계로 동쪽에 위치한 국가들을 통칭하는 표현으로서, 체코, 슬로바키아, 폴란드, 헝가리, 루마니아, 발칸반도 및 발트해 3국 국가들을 포함

표 _ 중동·동유럽 시장 주요국의 한국과의 관계(2017년 기준)

항목	수교일	우리나라 수출규모 (US$ 백만)	우리나라 수입규모 (US$ 백만)	우리나라의 주요수출품	우리나라의 주요수입품
오만	1974. 3	675	2,775	열연강판, 석유화학합성원료	천연가스, 기타석유화학제품
UAE	1980. 6	4,588	9,287	자동차부품, 휘발유, 연초류, 축전지	원유, 나프타, 알루미늄괴 및 스크랩, 중유
카타르	1974. 4	526	16,294	승용차, 건설중장비, 전선, 선박, 컬러TV	천연가스, 원유, 나프타, 알루미늄괴 및 스크랩
사우디 아라비아	1962.10	3,952	26,336	승용차, 타이어, 합성수지, 축전지	원유, 나프타, 기타석유화학제품
이란	1962.10	2,295	4,091	의료용기기, 합성수지, 공기조절기, 냉장고	원유, 동괴 및 스크랩, 판유리, 음료, 고령토
루마니아	1990. 3	483	404	자동차부품, 승용차, 합성수지, 아연도강판	자동차부품, 직물제의류, 펌프, 가방, 기타기계요소

199 중동(Middle East)이라는 용어는 1990년경 유럽을 중심으로 오리엔트(Orient)를 근동(Near East), 중동(Middle East), 극동(Far East) 등으로 구분한데서 유래한다.

[출처] Kotra-국가별 정보, stat.kita.net

▶ 주요 중동 국가별 IDI를 확인한 결과 아랍국가들 중에서도 GCC 주요국인 UAE, 카타르의 ICT 발전지수가 높게 나타남

• 특히 ICT 인프라에 투자 규모를 늘리고 있는 카타르와 UAE는 2017년 ICT발전지수(IDI) 종합 순위에서 각각 39, 40위를 차지하며 지속적으로 이 지역 ICT 발전의 중심 역할을 하고 있음

표 _ 중동·동유럽 시장 주요국 ICT 발전지수(IDI)

국가	IDI(2017년)		접근성(access)		이용성(use)		스킬(skill)	
	순위	지수	순위	지수	순위	지수	순위	지수
오만	62	6.43	48	7.32	55	5.71	90	6.07
UAE	40	7.21	24	8.11	31	7.09	108	5.63
카타르	39	7.21	33	7.90	32	7.07	89	6.09
사우디아라비아	54	6.67	52	7.21	59	5.68	48	7.57
이란	81	5.58	67	6.74	104	3.54	58	7.32
루마니아	58	6.48	60	6.98	61	5.59	60	7.25
한국	2	8.85	7	8.85	4	8.71	2	9.15

[출처] ITU, ICT Development Index 2017, https://www.itu.int/net4/ITU-D/idi/2017/index.html

▶ 국제전기통신연합(ITU)은 법적, 기술적, 조직적 대응 및 역량강화, 국제협력 등 5개 부문의 지수를 종합하여 글로벌 사이버보안지수(Global Cybersecurity Index, GCI)를 측정하여 국가 간 비교를 함

• 2018년 글로벌 사이버보안지수(GCI)에 따르면, 대부분의 아랍 지역 국가들의 글로벌 사이버보안지수는 세계 상위, 중위, 하위권에 넓게 분포하고 있으며, 아랍 지역에서 사우디아라비아의 GCI는 0,881점으로 세계 13위, 오만은 16위, 카타르는 17위를 기록함

표 _ 중동 지역 글로벌 사이버보안지수(GCI)

국가	GCI(2018년)		법적(Legal)	기술적 (Technical)	조직적 (Oranizational)	역량강화 (Capacity building)	국제협력 (Cooperation)
	순위	지수	지수	지수	지수	지수	지수
사우디아라비아	13	0.881	0.187	0.179	0.158	0.198	0.160
오만	16	0.868	0.133	0.184	0.197	0.195	0.160
카타르	17	0.860	0.193	0.154	0.192	0.171	0.151
한국	15	0.873	N/A	N/A	N/A	N/A	N/A

[출처] ITU, Global Cybersecurity Index(GCI) 2018,
https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

• 유럽국들의 글로벌 사이버보안지수는 세계 상중위권에 분포하고 있으며, 영국의 GCI는 0.931으로 세계 1위, 프랑스의 GCI는 0,918점으로 세계 3위, 리투아니아는 4위를 기록함

표 _ 유럽 지역 글로벌 사이버보안지수(GCI)

국가	GCI(2018년)		법적(Legal)	기술적 (Technical)	조직적 (Oranizational)	역량강화 (Capacity building)	국제협력 (Cooperation)
	순위	지수	지수	지수	지수	지수	지수
영국	1	0.931	0.200	0.191	0.200	0.189	0.151
프랑스	3	0.918	0.200	0.193	0.200	0.186	0.139
리투아니아	4	0.908	0.200	0.168	0.200	0.185	0.155
한국	15	0.873	N/A	N/A	N/A	N/A	N/A

[출처] ITU, Global Cybersecurity Index(GCI) 2018,
https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

▶ 유엔무역개발기구(UNCTAD)는 금융기관 또는 모바일 머니 서비스 제공업체의 계정 소유권, 인터넷을 사용하는 개인, 우편물 신뢰성 지수, 안전한 인터넷 서버 등 4개의 지수를 종합하여 B2C 전자상거래 지수(B2C e-Commerce Index)를 측정하여 국가 간 비교를 하고 있음

• 2019년 전자상거래 지수에 따르면, 대부분의 중동·동유럽 지역 국가들의 B2C 전자상거래 지수 순위는

세계 중상위권에 분포하고 있으며, UAE의 B2C 전자상거래지수는 83.8점으로 세계 28위, 이란은 42위, 카타르는 47위, 사우디아라비아는 49위, 오만은 59위, 동유럽의 루마니아는 46위를 기록함

표 _ 중동·동유럽시장 주요국 B2C 전자상거래 지수

국가	전자상거래지수 (2019)		인터넷 사용하는 개인	계정 소유권	안전한 인터넷 서버	우편물 신뢰성 점수
	순위	지수	지수	지수	지수	지수
오만	59	68.2	80	74	47	72
UAE	28	83.8	98	88	65	84
카타르	47	74.2	100	66	54	77
사우디 아라비아	49	73.3	93	72	47	81
이란	42	76.9	70	94	56	88
루마니아	46	74.5	71	58	84	86
한국	19	89.4	96	95	67	99

[출처] UNCTAD, B2C e-Commerce Index 2019, https://unctad.org/en/PublicationsLibrary/tn_unctad_ict4d14_en.pdf

▶ 글로벌 시장조사기관인 MarketsandMarkets이 발표한 물리보안시장에 대한 보고서는 물리적 보안 시장 영역을 시스템 분야와 서비스 분야에서 시장 규모를 발표함

- 시스템 분야에는 물리적 접근 제어 시스템, 비디오 감시 시스템, 경계 침입 탐지 및 예방, 물리적 보안 정보 관리, 물리적 신원 및 접근 관리, 보안 검색, 이미징 및 금속 탐지, 화재 및 생명 안전에 대한 시스템이 포함
- 서비스 분야에는 서비스 분야에서 서비스로서의 접근 제어, 서비스로서의 비디오 감시, 원격 모니터링 서비스, 보안 시스템 통합 서비스를 포함
- 중동 지역은 물리적 보안 분야의 새로운 시장 중 하나로 시장의 성장은 경제번영, 빠른 상업화, 테러 공격의 증가 및 이 지역의 인프라 개발 증가에 기인함
- 물리보안 시장규모는 2018년 UAE의 경우 27억 9,000만 달러 규모로 향후 연평균 성장률(2018-2023) 8.8%로 성장할 것으로 전망되고 있으며 사우디아라비아의 경우 16억 6,000만 달러 규모, 그 외 중동 국가들은 32억 9천만 달러 규모임

표 _ 중동 지역 주요국 물리보안 시장규모

(단위 : 십억 달러)

국가	2016	2017	2018e	2023p	연평균성장률 (2018-2023)
UAE	2.21	2.49	2.79	4.24	8.8%
사우디아라비아	1.26	1.52	1.66	2.69	10.1%
기타 중동 국가*	2.84	2.99	3.29	4.40	6.0%

주석: e: 추정, p: 예상

* 카타르, 쿠웨이트, 바레인, 오만, 기타 걸프 국가 등이 포함됨

[출처] MarketsandMarkets, Physical Security Market-Global Forecast To 2023, 2019

• 유럽 지역의 경우는 독일이 가장 큰 시장 규모를 보유할 것으로 전망되었으며 2018년 52억 4,000만 달러에서 2023년 69억 6,000만 달러 규모로 연평균 5.8%성장률을 기록할 것으로 예상되고, 영국은 2023년까지 52억 4,000만 달러 규모로 연평균 5.6% 성장률을 보일 것으로 전망됨

표 _ 유럽 지역 주요국 물리보안 시장규모

(단위: 십억 달러)

국가	2016	2017	2018e	2023p	연평균성장률 (2018-2023)
영국	3.50	3.74	4.00	5.24	5.6%
독일	4.55	4.89	5.24	6.96	5.8%
기타 유럽국가	9.45	10.20	10.96	14.73	6.1%

주석: e: 추정, p: 예상

*그외 유럽 국가에는 프랑스, 오스트리아, 스위스, 노르웨이, 네덜란드, 그리스, 스페인, 이탈리아, 러시아, 덴마크, 스웨덴이 포함

출처] MarketsandMarkets, Physical Security Market-Global Forecast To 2023, 2019

▶ MarketsandMarkets의 정보보안시장 보고서는 중동 지역의 정보보안 시장이 2018년 132억 2,500만 달러 규모에 달할 것으로 추산하였고, 2023년경 241억 5,000만 달러에 이를 것으로 전망

표 _ 중동 지역 정보보안 시장규모

(단위: 십억 달러)

2016	2017	2018e	2023p	연평균성장률 (2018-2023)
10.12	11.63	13.25	24.15	12.80%

[출처] MarketsandMarkets, Cybersecurity Market-Global Forecast To 2023, 2019

• 유럽 시장에서는 영국이 지배적인 규모를 보일 것으로 전망되었으며, 2018년 120억 2000만 달러 규모에서 2023년경 161억 7,000만 달러 규모로 성장할 것으로 예상됨

표 _ 유럽 지역 주요국 정보보안 시장규모

(단위: 십억 달러)

국가	2016	2017	2018e	2023p	연평균성장률 (2018-2023)
영국	10.39	11.23	12.02	16.17	6.1%
독일	6.69	7.40	8.11	12.31	8.7%
프랑스	5.21	5.81	6.42	10.12	9.5%
기타 유럽국가	7.83	8.59	9.33	13.56	7.8%

주석: e: 추정, p: 예상

[출처] MarketsandMarkets, Cybersecurity Market-Global Forecast To 2023, 2019

▶ MarketsandMarkets이 발표한 서비스형 보안시장에 대한 보고서에 따르면 서비스형 보안은 클라우드 기반 모델이며, 보안 공급 업체는 클라우드 및 사내 환경에서 엔터프라이즈 네트워크, 애플리케이션 및 데이터를 보호하고 유지 관리

• 중동 지역은 이스라엘, UAE 등을 포함하며, 서비스형 보안 시장규모는 2018년 5억 990만 달러 규모로 예상되었고, 향후 연평균 18.4%의 성장률(2018-2023)을 기록할 것으로 예상됨

표 _ 중동 지역 서비스형 보안 시장규모

(단위: 백만 달러)

국가	2016	2017	2018e	2023p	연평균성장률 (2018-2023)
중동 지역	332.1	414.3	509.9	1,187.5	18.4%

[출처] MarketsandMarkets, Security As a Service Market-Global Forecast To 2023, 2019

- 유럽 지역의 경우 영국이 정보보안 시장에서처럼 가장 큰 시장 규모를 보일 것이라 예상되었으며, 2018년 6억 3,200만 달러 규모를 기록한 뒤 2023년에는 12억 2,460만 달러에 이를 것이라 전망됨
- 독일과 프랑스도 같은 기간 영국의 연평균성장률(14.1%)을 상회하는 16.0%, 16.7%의 성장률을 각각 기록하며 영국의 서비스형 보안 시장 규모를 뒤쫓을 것으로 예상

표 _ 유럽 지역 서비스형 보안 시장규모

(단위: 백만 달러)

국가	2016	2017	2018e	2023p	연평균성장률 (2018-2023)
영국	451.1	537.5	632.0	1,224.6	14.1%
독일	289.0	351.0	420.7	883.6	16.0%
프랑스	225.2	275.8	333.2	722.2	16.7%
기타 유럽국가	336.5	402.8	475.7	939.5	14.6%

주석: e: 추정, p: 예상

*그외 유럽 국가에는 스페인 이탈리아, 러시아 등이 포함됨

[출처] MarketsandMarkets, Security As a Service Market-Global Forecast To 2023, 2019

▶ MarketsandMarkets의 IoT 보안시장에 대한 보고서에서는 IoT 보안 시장은 연결된 장치의 네트워크를 보호하고 연결된 장치의 위협 및 사이버 공격으로 인한 손실을 최소화하기 위해 제공되는 솔루션 및 서비스를 포함한다고 언급

- 중동의 경우 석유 및 가스 회사가 많아 지역 경제성장에 기여하고 있는데, 보안솔루션 제공업체인 Kaspersky에 따르면, UAE는 2016년 사이버 공격의 주요 대상 중 하나가 되었으며, 이러한 공격은 중동 지역의 전반적인 비즈니스 운영에 영향을 미치며 중동 지역 전역의 IoT 보안 공급업체에게 기회가 발생함

• IoT 보안 시장규모는 2018년 사우디아라비아의 경우 2억 9,980만 달러 규모로 연평균 성장률(2018-2023) 35.6%로 성장할 것으로 전망되며, UAE는 2억 6160만 달러 규모이며, 그 외 중동 및 아프리카 국가들은 3억 50만 달러 규모임

표 _ 중동 및 아프리카 지역 주요국 IoT 보안 시장규모

(단위: 백만 달러)

국가	2016	2017	2018e	2023p	연평균성장률 (2018-2023)
사우디 아라비아	185.6	235.1	299.8	1,375.3	35.6%
UAE	159.1	204.0	261.6	1,257.9	36.9%
기타 중동 및 아프리카	185.6	237.5	305.0	1,462.0	36.8%

주석: e: 추정, p: 예상

*그외 중동 및 아프리카 국가에는 아프리카, 이스라엘, 등이 포함됨

[출처] MarketsandMarkets, IoT Security Market-Global Forecast To 2023, 2019

• 유럽 지역에도 중동 지역과 비슷한 연평균성장률을 보일 것으로 전망되며, 영국이 유럽 내 가장 큰 IoT 보안 시장 규모를 보유한 국가로서 2018년 9억 7,000만 달러 규모를 기록한 뒤 2023년에는 38억 740만 달러 규모로서 연평균 성장률(2018-2023) 31.5%의 비율로 가파르게 성장할 것으로 예상

표 _ 유럽 지역 주요국 IoT 보안 시장규모

(단위: 백만 달러)

국가	2016	2017	2018e	2023p	연평균성장률 (2018-2023)
영국	639.7	786.0	970.0	3,807.4	31.5%
독일	399.8	497.7	622.2	2,604.0	33.2%
기타 유럽국가	559.8	691.2	857.3	3,452.3	32.1%

주석: e: 추정, p: 예상

*그외 유럽 국가에는 프랑스, 이탈리아, 네덜란드 등이 포함됨

[출처] MarketsandMarkets, IoT Security Market-Global Forecast To 2023, 2019

▶ 중동·동유럽 시장의 주요 진출 전략은 다음과 같음

- 오만 등 전략 거점국가를 활용한 SOC(Security Operating Centre), 디지털 포렌식 분야 등 한국형 정보보호 모델의 전파에 집중할 필요가 있으며, 국가별 총판 발굴 및 전략적 제휴를 통한 진출 전략이 필요

- 평창 동계올림픽 유치경험을 기반으로 진출전략 모색 : 카타르·UAE
  - 두바이 2020 EXPO, 2022 카타르 도하 올림픽 개최를 앞두고 사이버보안 관련 컨설팅, 인터넷침해대응센터 구축 및 운영 등 보안분야 수요 증가
- 기존 레퍼런스를 활용한 진출전략 추진 : 오만·사우디아라비아·UAE
  - 오만 디지털포렌식랩 구축 등 기존 수주 성공사례를 기반으로 자금력이 풍부한 주변국가에 한국형 정보보호 모델 전파

가. 오만

'18년 GDP(십억달러)	79.29
'18년 인구수(천명)	4,830

■ ITU 글로벌 사이버보안 지수(Global Cybersecurity Index, GCI)

· 오만의 사이버보안 지수는 한국과 거의 비슷한 수준이며, 선도 그룹에 속함

국가명	2018		2017		전년대비 증감	
	지수	순위	지수	순위	지수	순위
오만	0.868	16	0.871	4	-0.03	-12
대한민국	0.873	15	0.782	13	+0.091	-2

■ ICT 관련 주요 지수

· 오만의 전반적인 ICT 발전 수준은 중위권을 유지하고 있음

지표명	오만		한국	
	점수	순위	점수	순위
IMD 국가경쟁력지수(2019)	-	-	-	28
IMD 디지털경쟁력지수(2019)	-	-	-	10
UNCTAD 전자상거래지수(2019)	68.2	59	89.4	19
ITU 글로벌 사이버보안 지수(GCI 2018)	0.868	16	0.873	15
UN 전자정부 지수(2018)	0.684	63	0.901	3

■ ICT 관련 주요 통계 (ITU, 2018년 말 기준)

· 오만의 유선통신 보급률은 10%대로 낮은 편이며, 이동통신 보급률은 우리나라와 비슷한 수준

항목	오만		한국	
	가입자수(천 명)	보급률(%)	가입자수(천 명)	보급률(%)
유선전화	560	11.60	25,907	50.63
유선브로드밴드	422	8.74	21,286	41.60
이동통신	6,441	133.37	66,356	129.67
인터넷 이용률	-		95.90%	

정보보호 산업 개요

1) 보안 환경

▶ 오만 정부기관들은 보안 위협에 대응하기 위해 2015년을 기점으로 보안 솔루션 의무 설치를 시행함
- 2018 UN전자정부보고서에 따르면, 오만 전자정부 순위는 193개국 중 63위를 차지하여 아랍 국가 중 6위를 기록했으며 특히 보안 평가 지수는 글로벌 4위에 올라섬

▶ 2019년 9월 ITA는 전국 사이버 보안 훈련에서 오만이 2018년 432,978번의 사이버 공격을 당했다고 발표함
- 이중 OCERT는 2016년 1,744회, 2017년 1,838건의 사고를 처리함
- ITA (Information Technology Authority)에서 조직하고 오만 국립 CERT가 대표하는 이 훈련은 '맬웨어 및 다크 웹'이라는 주제로 진행되었으며 72개 이상의 정부 기관과 은행, 유틸리티, 운송, 물류 및 석유 및 가스와 같은 중요한 인프라 부문이 참여함
- 이 훈련은 참여 조직들의 사이버보안 대응팀의 준비 상태를 평가하고 이 분야의 국가 능력과 기술을 개발하는 것을 목표로 함

▶ 오만 ITA는 2019년 1월부터 지난 6월까지 607개의 블랙메일을 조사한 결과를 발표함
- 조사결과 사이버 블랙메일의 주요 희생자는 14세에서 45세 사이로 그 중 53%가 남자라고 언급함
- 사이버 범죄는 2017년 1,479건수에서 2018년 1,414건수로 다소 줄어든 모습을 보임
- ITA는 사이버 블랙메일을 처리하면서 이에 대한 인식을 제고하는 프로그램을 제공해 오고 있음

▶ 2015년 Information Technology Authority(ITA) 보고서에 따르면 오만 정부는 2015년 약 5백만 건 이상의 사이버공격을 받음
- 이중 정부 네트워크 부분의 480만 건의 공격, 정부 홈페이지에 대한 398,000건 이상의 공격을 막아냄

그림 _ 2011-2016년 블랙메일 증가 추이



- 랜섬웨어 및 블랙메일에 의한 공격 증가가 주목할 만한데 2016년에는 랜섬웨어-블랙메일를 활용한 공격 16,000건, 또한 블랙메일 단독 공격도 2011년 1건에서 161건으로 급격하게 증가하고 있음
- 사이버보안 범죄에서 블랙메일의 비중이 높아 2016년 355건의 사이버 범죄 가운데 블랙메일에 의한 사이버범죄는 161건임
- 오만 통계국에 따르면 외국인에 의한 범죄가 70%, 오만인 범죄가 30%로 외국인에 의한 범죄가 훨씬 높은 것으로 조사됨

▶ ITA 보고서에 따르면 오만 내 온라인 공격 및 범죄는 국가 기관 공격 및 개인에 대한 사기 등의 피해가 발생하고 있으며 범죄자들은 오만의 국가사이버보안법에 의해 처벌되고 있음

- 사례 1) 2017년 7월, Ministry of Education, www.traffic.gov.om, www.tra.gov.om, www.registry.om, www.omantel.om, www.ofa.om 등의 사이트가 자신을 Dr. DarknesS라 지칭한 14세 소년에 의해 공격당함
- 사례 2) 2013년 뱅크 무스카트가 4천만 달러를 인출하려는 터키 해커의 공격을 받음
- 사례 3) 14명으로 구성된 사기집단이 ATM 리더기에 부가적인 장치나 카메라 등을 설치하여 ATM 기기 이용자들의 자금 인출을 시도함
- 사례 4) 소셜미디어를 활용한 범죄는 데이팅앱을 활용한 성적 사기 및 금융사기 등의 두 종류가 있으며 이러한 범죄 유형도 증가 중

▶ 최근 중요 시설에 대하여 심각한 위협이 될 수 있는 사이버 공격이 증가하고 있으며, 범죄의 발생 가능성도 점차 증가하고 있음

- 2015년 초, 보안 솔루션 업체 Symantec은 세계적으로 에너지 관련 기업들에 대한 멀웨어 'Trojan.Laziok'를 발견해 발표했으며, 이들 멀웨어의 사이버 공격 주요 대상은 아랍에미레이트연합(UAE, 25%), 사우디아라비아(10%), 오만(5%) 및 카타르(5%)인 것으로 나타남

2) 인터넷 및 통신 환경

▶ 유선통신

- 2018년 7월 기준 유선전화 가입자 수는 54만 명이며 2017년 51만 명에서 11.9% 정도 증가함
- 2018년 7월 기준, 오만 유선 브로드밴드 가입자 수는 39만 2천명 수준으로 보급률은 8% 정도 수준이며, 모바일 브로드밴드 가입자는 410만 명으로 보급률은 86% 수준임
- 글로벌 리서치 기관 Buddecom에 따르면, 오만의 유선 브로드밴드 가입자의 절반 정도는 DSL을 이용하며, fTTB/fTTH 등 광통신 브로드밴드 사용자는 4천 명 정도에 불과해 전체 사용자의 97%가 2~10Mbps 인터넷 서비스를 이용 중임

표 _ 오만 유선 브로드밴드 가입자 현황

회선 종류	가입자 (명)
전체 유선 브로드밴드 가입자(2018.7)	392,000
DSL 가입자(2015)	161,000
FttB/FttH 가입자(2015)	4,000
고정형 무선가입자(2015)	66,000

[출처] Buddecom report(2018.3) OMAN TELECOMS

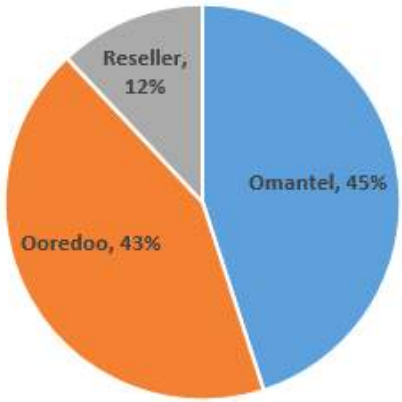
- 국가브로드밴드전략(National Broadband Strategy)의 일환으로 오만 브로드밴드社(Oman Broadband Company)는 무스카트 지역의 7만 주택과 사무실 등에 광 네트워크 접속을 가능하도록 하였으며, 2040년까지 모든 가정과 사무실에 광 네트워크를 제공한다는 목표를 수립함
  * 오만 국가브로드밴드전략은 2016.8월 승인되었으며 자국민의 인터넷 접근성을 도시인구의 50%(2020년), 95%(2030) 까지 달성한다는 목표로 추진 중
- 오만 인터넷 통신 서비스는 일반적으로 Omantel과 Ooredoo 양사에 의해 제공되며 2015년 기준 Omantel 80%, Ooredoo 20%의 시장 점유율을 보이고 있음. 네트워크 인프라 구축을 통해 FTTH(fibre-to-the-home) 기반 확산을 위한 정부의 정책에 적극 참여할 예정임
- Omantel은 51%가 오만 정부 지분인 국영 통신사로, 2015년 인터넷 브로드밴드 인프라 개선 프로젝트에 1억 2,000만 오만 리알(약 3억 1,170만 달러) 규모의 투자 실시
- Ooredoo는 5,500km 길이의 광케이블 인프라 구축에 1억 2,500만 오만 리알(약 3억 2,460만 달러)을 투자하고, 120개 학교에 브로드밴드 인프라를 구축했으며 일종의 월경지역인 Musandam(오만 국토이나 UAE 영토에 위치) 내 Madha 지역 800개 가구에 광케이블망을 구축했음. 이러한 인프라

확장으로 Ooredoo는 오만 60% 지역의 가정에서 홈 브로드밴드 인터넷 서비스를 제공할 수 있음

▶ 이동통신

- ITU 통계에 따르면 2018년 말 기준 오만 내 이동통신 가입자 수는 644만 명 규모로서 141%의 보급률을 보이고 있으며 이는 2017년 152% 대비 11% 감소함
- 오만은 Omantel과 Ooredoo Oman 2개의 이동통신사업자가 시장을 주도하고 있으며 그 외 리셀러가 12%를 점유함

그림 _ 오만 이동통신사 점유율 현황



[출처] Buddecom report(2019.5) OMAN TELECOMS

- 모바일 브로드밴드 가입자 수는 2017년 말 435만 명에서 2018년 말 411만 명으로 4% 감소, VoIP 가입자 수는 2018년 7월 기준 16만 4천명으로 2018년 말 대비 29만 명 증가함
- Oman Mobile은 오만 최초의 통신사업자인 Omantel이 99%의 지분을 소유하고 있으며, GSM-900MHz(GPRS, EDGE), 900/2,100MHz UMTS, HSPA+, 1,800MHz FD-LTE, 2,300MHz TD-LTE 서비스를 제공함
- Omantel과 Ooredoo는 각각 2012년 7월, 2013년 2월 LTE서비스를 개시했으며 2018년 1분기 기준 Ooredoo는 오만 내 LTE 커버리지 90%를 달성함
- Ooredoo는 LTE-A 서비스 제공을 위해 200Mbps 속도의 시연을 마친 바 있으며 2015년에 무스카트 주변에 LTE-A 핫스팟을 구축함
- 또한 Omantel은 2016년 LTE-A 시범서비스를 1Gbps 속도까지 성공적으로 완수했다고 밝힌 바 있음
- 오만 교통통신부(Ministry of Transport and Communications)는 2016년 내에 제 3 이동통신 사업자 선정 계획을 밝혔으나 2017년 10월 TRA는 이를 취소하고 지역 사업자에게 라이선스를 부여한다고 공표함

정보보호 시장 현황

1) 시장 규모

시장 개요

▶ 2017년 오만 IT시장규모는 2016년 4억 8,620만 달러 대비 1.6% 늘어난 4억 9,400만 달러를 기록할 것으로 예상되며 2021년까지 2017년 대비 2.9% 늘어난 5억 5,400만 달러까지 성장 예상

- 2017년 7월 기준 하드웨어 부분이 2억 3,900만 달러, IT서비스 부문이 1억 4,300만 달러, 소프트웨어 부문이 1억 1,200만 달러에 달할 전망

▶ 오만은 IT 보안제품에 대해 오만정보기술청(ITA)이 모니터링을 시행하는데, ITA는 산하 부서인 Centre of Information Security(CIS)와 오만 침해사고대응팀(OCERT)에 의해서 관련 업무 시행

- ITA는 2015년 한국인터넷진흥원(KISA)과 더존비즈온社와 디지털포렌식센터 건립 계약을 체결한 바 있음
- 오만은 CIS를 통해서 IT 보안 제품들의 기준, 관련 정책 등을 제시

▶ 석유가스, 은행, 항공, 유틸리티 등의 산업분야에 ICT와 보안에 대한 대규모 투자가 이루어지고 있음

- ICT 투자규모가 가장 큰 분야는 석유가스분야로, 오만석유개발공사(Petroleum Development Oman, PDO)에서는 원격감시, 보안, 모바일 데이터센터 등 ICT 인프라 구축에 투자하고 있음
- 또한 정부 관청, 공공기관, 신축의 경우 CCTV 등 보안장비 설치를 의무화하고 있어 이들 기관들도 높은 수요를 나타내고 있음

▶ 오만에서는 지문, 얼굴, 홍채 등을 인식하는 첨단 기술을 사용해 이용자를 식별하는 시스템 사용이 증가하고 있음

- 그 중에서 지문 인식 시스템이 많이 사용되고 있으며 공공 부문에서는 대표적으로 왕립 오만 경찰(Royal Oman Police)의 신분증 및 거주 관할(General of Passport and Residence) 부서가 국내 기업 Suprema 제품을 사용해 ID 카드에 지문을 등록하고 있음.
- 민간부문에서는 출입 관리, 외부인 접근 통제, 데이터 보안을 위해 Suprema 제품을 사용함.
- 오만에서 많이 사용되는 지문인식 시스템의 브랜드는 한국의 Suprema, 중국의 ZKTeco, 인도의 Matrix Security Solutions, 미국의 HID Secure 등임

시장 규모 및 성장률

▶ 오만 정보보호 시장 규모는 정보보안 분야가 2,550만 달러, 물리보안 분야가 4,830만 달러 규모로 총 7,380만 달러 규모를 형성하고 있음

- 오만의 경우 활발하게 정보보호 시장이 성장 중이지만, 인구수가 약 400만 명으로 작은 편이어서 GCC 주요국 중 소규모인 7,000만 달러 수준임

표 _ 오만 정보보호시장 규모(2014년 말 기준)

(단위: 백만 달러)

국가	정보보안	물리보안	합계
오만	25.5	48.3	73.8

[출처] KISA, '정보보호 산업 해외시장 진출방안 연구'(2015.9)

▶ 오만은 ITU가 발표한 2017 글로벌 사이버보안 지수(Global Cyber security Index, GCI)에서 글로벌 4위, 중동권에서는 1위를 기록했으며 이집트와 카타르가 그 뒤를 이음

- 조직, 법제도, 기술 및 측정 프로세스, 아랍 지역 및 국제 협력 등을 평가 항목으로 하고 있는 본 보고서에 의하면, 오만은 고수준의 사이버 보안 전략과 마스터플랜에 기반하여 조직적 실행이 우수한 국가로 평가
- 또한 IT 보안 교육 분야에서도 오만 침해사고대응팀(OCERT)이 교육부와 밀접한 관계를 가지고 정보보호교육과정 수립에 기여하고 있으며, 사이버보안 국제 인정 자격증 프로그램 하에 350개 공공분야에서 프로페셔널 인증을 보유하고 있음

▶ 오만은 에스토니아의 전자정부 아카데미에서 실시한 국가 사이버 안보지수 NCSI(National Cyber Security Index)에서 아랍 국가 중 3위를 기록

- 이 지수는 사이버 범죄 및 사이버 범죄를 대규모로 관리하고자 하는 국가의 준비 상태를 측정하는 것임
- 오만은 32.47점으로 전 세계 순위에서 61위로 카타르와 이집트 다음으로서 아랍국가 중에서는 세 번째이며 프랑스, 독일, 에스토니아, 슬로바키아, 핀란드, 리투아니아가 그 뒤를 이었음

▶ 2017년 오만정보기술청(ITA) 연례보고서에 따르면 OCERT는 정부 네트워크에 대한 880,843,349건의 공격을 방어함

- OCERT는 1,859가지 스파이웨어와 11,370가지 바이러스 및 멀웨어를 발견하였으며, 14개 웹 포털과 44개 정부 사이트 보안을 강화

- ITA는 컴퓨터, 휴대 전화, 하드 드라이브 및 USB와 같은 877개의 증거 장치를 사용하여 172건의 디지털 포렌식으로 사이버 범죄를 해결
- OCERT는 34개 정부 기관 및 국가 인프라 조직으로 17개 팀을 구성하여 국가사이버훈련(National Cyber Drill)을 운영
- 오만정부는 사이버 훈련을 운영하고 자국민의 사이버 보안 인식 제고를 위해 워크숍 및 세미나도 개최하는 등 사이버 보안 대처에 적극적임

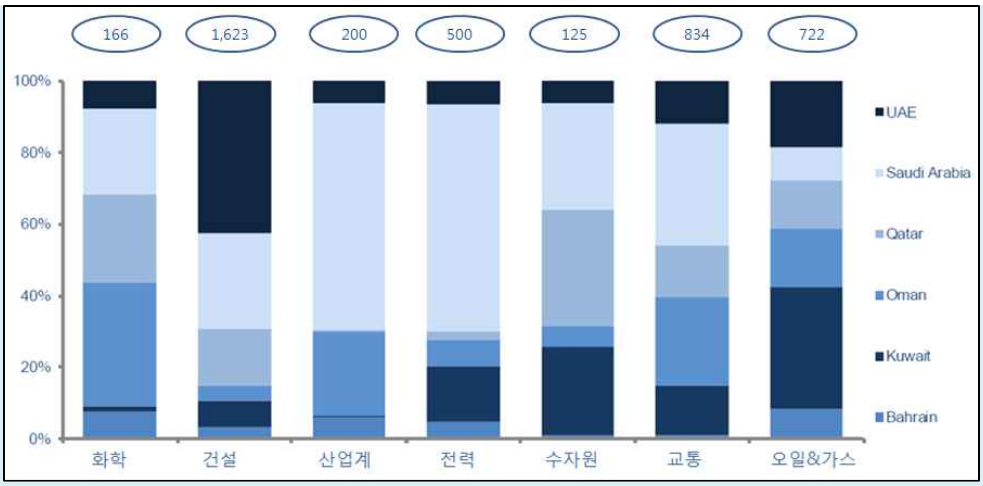
시장 전망

▶ 오만은 GCC 타 국가 대비 화학 분야 투자가 비중이 높으며 2014~2017년 GCC 국가 전체 화학 분야 보안 투자 중 약 40%를 차지할 것으로 예상됨

- 글로벌 리서치기관 MEED에 따르면 오만은 2014~2017년 보안 투자 중 교통 분야 투자가 가장 클 것으로 예측되며 GCC 전체 국가들의 교통 분야 투자액 8억 3,400만 달러 중 약 15%를 차지할 전망

그림 _ GCC 프로젝트별 보안 투자 규모 예측(2014~2017년)

(단위: 백만 달러)



[출처] MEED Insight(www.meed.com), 2014

▶ GCC 전체 보안 솔루션 시장 규모는 2014년~2017년 42억 달러 규모이며, 오만은 5.41억 달러로 가장 작은 규모임

표 _ GCC 국가별 보안 솔루션 분야 투자규모 예측(2014~2017년 합계)
(단위: 백만 달러)

사우디아라비아	UAE	쿠웨이트	카타르	오만
1,299 (31%)	994 (24%)	595 (14%)	569 (14%)	541 (13%)

[출처] MEED Insight(www.meed.com), 2014

2) 분야별 현황

물리보안 제품 및 서비스

▶ GCC 타 국가와 마찬가지로 CCTV에 대한 수요가 높으며, 최근 2~3년 사이 한국산 한화테크윈(舊 삼성테크윈), IPTEC, Pinetron, Camtron 등의 브랜드의 인지도가 높음

- 이 중 한화테크윈(舊 삼성테크윈) 제품이 다른 중소기업 경쟁사 제품에 비해 다소 높은 가격에도 불구하고 선호도가 높은 편임
- 또한, 시장 진출 역사가 오래된 유럽 및 일본 제품에 대한 선호도가 높음

▶ (바이오인식) 오만에서 가장 보편화된 바이오인식 시스템은 지문 인식 시스템으로 오만 경찰청에서 신분증 발급 시 사용하고 있는데, 국내 기업인 슈프리마 제품이 납품된 바 있음

- 민간 기업의 경우, 직원 출근 확인, 외부인 접근 제한 등을 위해 사용하고 있고 우리나라 슈프리마를 비롯하여 ZKTeco(중국), Matrix Security Solutions(인도), HID Secure(미국)가 시장 내에서 강세를 보이고 있음

정보보안 제품 및 서비스

▶ (방화벽) 오만에서 주로 사용되는 방화벽 소프트웨어는 러시아의 Kaspersky Lab과 미국 Symantec의 Norton으로 양분되어 있으며 소프트웨어 방화벽은 주로 가정이나 소규모 사무실에서 사용됨

- 하드웨어의 경우, Dell 및 Cisco를 중심으로 미국 회사 제품이 강세를 보이고 있으며 여기에 인도의 Cyberoam도 경합을 벌이고 있음
- 또한, 시장 진출 역사가 오래된 유럽 및 일본 제품에 대한 선호도가 높음

▶ (IT 보안 프로젝트) 오만 정부는 개인 정보 및 지적재산권 강화는 물론 새로운 유형의 범죄인 사이버테러 대비를 위하여 IT 보안 강화 노력 및 관련 프로젝트를 발주함

- 오만 정보기술청(ITA)은 2015년 한국인터넷진흥원(KISA) 및 더존비즈온과 디지털 포렌식 센터 건립을 위한 112억 원 규모의 계약을 체결했음
- 동 계약은 오만에 디지털 포렌식랩을 만들어 컨설팅, 시스템 구축, 운영까지 한국형 정보보호 모델을 수출한 건으로 단순 기술 판매가 아닌 지속적인 서비스 창출형 프로젝트 수주 모델임

▶ (클라우드 보안 서비스) 오만의 IT 및 클라우드 서비스 확대에 따라 사업자는 부가적으로 클라우드 보안 서비스 제공에 많은 기회 예상

- 그 예로, 통신사업자 Ooredoo는 2015년 5월 자사의 기업 인터넷 사용자를 위해 DDoS 공격을 방어하는 보안 시스템을 제공하기 시작함

3) 주요 사업자 현황

시장 특성 및 경쟁 강도

▶ 공항 건설, 공공기관들을 대상으로 하는 프로젝트에서의 물리적 보안 및 보안 시설 운영 분야는 다국적 기업들의 영향력이 큰 상황이며, 오만 국내 기업들의 정보보안 솔루션 제공이 증가하고 있음

- Thales와 Lockheed Martin과 같은 대형 글로벌 보안기업들이 전통적으로 오만 내 대형 인프라 구축 및 공공 프로젝트 등을 수행해오고 있음
- 중동 국가들의 경우 주변 국가들과 유사한 통신환경 및 기업 환경을 갖추고 있는 이유로 사업자가 특정 국가에만 한정된 형태를 띄기 보다는 UAE, 카타르, 오만 등 여러 국가에 두루 사무소를 두는 편

주요 사업자

❑ 정보보안 제품 유통사

▶ 오만 내에는 IT 보안 제품군을 생산하는 회사가 없어 수입에 의존하고 있으며, 통상적으로 에이전트 또는 바이어에 의해 수입되고 있음

- 에이전트의 경우 유명 다국적 기업의 IT 제품을 취급하고 있으며, 바이어(리셀러 등)의 경우 UAE를 통해 재수입하거나 다양한 제품군을 수입 및 조립하여 현지에 맞는 IT 솔루션을 제공하는 경우도 많음

· UAE 연방통계청에 따르면 UAE에서 오만으로 수출되는 비중은 전체 수출규모의 약 5%를 차지하는 것으로 나타남

표 _ 오만 주요 IT 보안 제품 바이어

회사명	내용
ITWork	· 오만 IT 제품 취급 회사로, 오만 경찰청 등 정부기관 및 주요 민간기업에 납품
Khimji Ramdas	· IBM 등 유명 다국적기업 제품딜러로 IT 분야 외 주요 소비재를 수입하는 기업임
OHI Electronics	· Hangzhou HikVision
Al Seeb Technical Establishment	· 삼성 등 IT 기업 주요 기업 제품 수입
SACTECH	· 슈프리마, 하니웰 등 주요 IT 보안 회사 관련 제품 수입

[출처] KOTRA 해외시장뉴스(2016.10)

- 오만 IT 보안시장에서 한국을 비롯한 미국, 중국 제품이 강세를 보이고 있는데, 미국의 경우 업계 내에서 2009년 오만과 FTA를 체결한 이후 ▲타경쟁국에 비하여 낮은 관세 ▲국가 브랜드 ▲기술력의 3가지 강점을 IT 분야에서 FTA 체결 효과를 보고 있는 것으로 평가받고 있음

❑ 정보보안 제품 제조사(외국계 수출 기업)

▶ First Information Security (First Info Sec)

- 모바일 음성 및 메시지 보안, 모바일 엔터프라이즈 데이터 보안, 정보보안 및 위기관리 서비스, 정보보안 교육 및 디지털 포렌식 분야 관련 솔루션 제공
- MENA 지역 고객사들에게 정보보안 솔루션을 제공, 2008년에 설립됨
- 오만, 사우디아라비아, 카타르, UAE, 이집트에 사무소가 있음

▶ Sachin Technologies LLC (SACTECH)

- 석유 및 가스, 정부, 통신, 금융, 유통, 공항, 교육기관, 헬스케어, 소매, 호텔 및 건설 산업 분야와 Fortune 500대 기업 등에 정보보안 솔루션 제공

▶ Vision Innovative Technologies LLC (VIT)

- 2007년 설립된 기업으로서, 정보보안 솔루션 및 CCTV 솔루션 등의 물리적 보안 제품을 공급하고 있음
- 정보기술, 정보보안 솔루션, 에너지 관련 솔루션, 웹 솔루션, CCTV 솔루션, 자동차 모니터링 솔루션

등이 주요 취급 품목임

▶ Gulf Business Machines (GBM) Oman

- 1990년 IBM 파트너사로 설립된 IT 솔루션 업체로서 현재 1,200여 명의 다양한 산업분야 (전자정부, 은행 및 금융, 통신, 소매, 석유 및 가스) 전문가를 보유하고 있음
- 현재 사무소는 UAE 아부다비(본사), UAE(두바이, 샤리아), 바레인, 쿠웨이트, 오만, 카타르, 파키스탄에 있음
- 사이버보안 솔루션제품 및 서비스로는 보안 위협 분석, 웹브라우저 기반 보안 애플리케이션, 데이터 보안, 네트워크 및 서버 등의 인프라 보안 등임
- GBM Oman은 대형 공공 및 민간 기업들을 고객사로 보유하고 있으며, 1990년에 설립되었음

▶ Thales

- 1970년 대 오만 최초의 통신 장비를 공급하면서 오만 사업을 시작하게 되었으며, 현재 135명의 직원이 근무하고 있음
- 교통통신부(Ministry of Transport and Communication, MOTC), 오만항공 (Oman Air), 오만 군대(Omani Armed Forces) 및 the Security Agencies of Oman과 지속적으로 사업을 진행해왔으며, 현재는 항공, 교통, 국방 및 보안 분야 관련 솔루션을 제공하고 있음

4) 주요 동향 및 이슈

▶ OCERT는 이슬람국가연합 침해사고대응팀(OIC-CERT)의 사이버 시큐리티 훈련을 조직하고 운영함 (2018.9)

- 동 훈련은 온라인에서 가상화폐 위험 및 떠오르는 위협을 해결할 목적을 가지고 실시됨

▶ OCERT가 미국 침해사고대응보안 포럼(Forum of Incident Response and Security Teams, FIRST)와 협력을 강화하기로 함(2017.6)

- FIRST는 국제기구로서 정부, 민간 및 교육 섹터에서 보안 공격을 다루는 사고 대응 및 보안팀을 보유
- 해당 협의는 사이버보안 공격 및 위험 교육 코스 및 정보 공유 등은 물론 사이버보안, 조직이벤트, 코스, 컨퍼런스에 대한 협력을 강화하는 것임

▶ OCERT는 NTRA(National Telecom Regulatory Authority) Egypt, Nispana와 사이버 보안 위협에 대한

대응을 위해 협력하기로 함 (2016. 8)

- 2016년 10월 30일 ~ 11월 1일까지 열릴 제 5차 Regional Cyber Security 연례회의를 기획, 개발 및 운영에 있어서 협력하기로 함
- 본 회의는 ITU-Arab Regional Cybersecurity Center (ITU-ARCC)가 주관하는 사이버 범죄와 안전한 인터넷 환경을 위하여 22개 아랍국가들과 북아프리카 국가들간 협력에 관한 내용이 중심임

▶ Oman Airports Management Company(OAMC)는 무스카트와 살랄라 공항 발전 계획 수립을 위하여 글로벌 산업 보안 및 군수 대기업인 Lockheed Martin의 BEONTRA Suite을 선정함(2016. 3)

- 무스카트와 살랄라 국제 공항 및 오만 국적 항공사인 Oman Air의 잠재적인 성장 계획을 위하여 OAMC는 BEONTRA 예측 솔루션을 공급하는 Lockheed Martin과 7개년 계약을 체결함
- 2015년 무스카트 국제 공항 이용 승객이 1,000만 명을 돌파한 가운데, OAMC는 2020년까지 연평균 18% 성장률을 전망하면서 세계 공항 TOP 20에 진입할 수 있을 것으로 예상

정보보호 정책 및 기관 현황

1) 관련 법령 및 정책

관련 법령 및 규제

▶ 전자거래법(Electronic Transactions Law)

- 전자거래법은 Royal Decree 69/2008에 의해 공표됨
- 전자 문자 및 전자적 전송에 따른 법적 효력, 전자적 전송 및 전자 계약 형태, 전자적 전송에 대한 보호 방법, 관할 기관, 관련 자격 및 인증 서비스, 개인정보 보호, 전자기록과 전자서명에 대한 정부의 이용, 처벌 등에 관한 법률임
- 본 법의 주요 목적은 ▲신뢰할 만한 전자 메시지 또는 기록을 이용한 전자적 전송 활성화 ▲전자적 전송 에 대한 일체의 방해 및 위협 제거 ▲전자문서의 전송 활성화 ▲전자 우편 및 전자 문서 수정에 대한 위조 최소화 ▲전자 우편 및 기록에 대한 인증 및 안전과 관련된 규칙, 규제, 제도를 위한 원칙 일원화 수립 ▲전자 거래, 전송 및 기록의 인증과 안전에 대한 신뢰도 확립 ▲전자서명을 이용하여 걸프 국가 및 아랍 국가들 간의 전자적 전송 분야 발전 등임

▶ 사이버 범죄법(Cyber Crime Law)

- 사이버 범죄법 (Royal Decree No 12/2011 issuing cyber crime law)은 오만의 새로운 디지털 사회 실현을 위하여 제정한 법률로서, 오만 ITA에 의해 추진되는 국가 IT 전략 실행을 위한 초석을 마련한 법으로 평가됨
- ▲안전의 위반, 데이터 & 전자정보 및 정보시스템에 대한 신뢰도 ▲정보기술 도구의 오용 ▲정보의 위조 및 사기 ▲콘텐츠 관련 범죄 ▲신용카드 무단 사용 등에 관하여 규정한 법률임

▶ 개인정보보호법(Personal Data Protection Law)

- 오만은 피고용인의 개인정보보호에 관해 명시적인 특별 법안은 없음
- 그러나 피고용인의 프라이버시를 보호하기 위해 고용인의 주의를 요하는 일반법은 제정되어 있으며 ▲기본법(Royal Decree No 101/1996) ▲형사소송법(Criminal Protection Law)은 제정되어 있음
- 오만 정보기술청(Oman Information Technology Authority, ITA)은 전문가와 커뮤니티를 중심으로 법률 초안을 논의하기 위해 3번의 세션을 개최한 바 있으며 2017년 11월 새로운 법률 초안이 의회 제출 전 법무부의 승인을 위해 제출된 상태이나 2018년 9월 현재 초안으로 남아있음

▶ 통신법(Telecom Act)

- 통신법은 2002년 제정된 Royal Decree No. 30/2002에 의해 입법화되어, 오만 통신 분야에 대한 일반 정책과 규제에 관한 법률로서 이전의 규칙과 법들이 본 법으로 대체됨
- 본 법은 통신 서비스 사업자가 제공하는 서비스 수준이 지속적이며 양질의 서비스를 제공함을 보장하며, 통신사업자들에게 부여한 라이선스의 조건 준수 여부, 통신 산업의 발전에 향상에 기여하는지 등에 대해서도 규제함

▶ 전자상거래(E-Commerce) 법안

- 오만 정보기술청(ITA)이 2006년부터 미국 상공부와 함께 오만 전자상거래 법안 관련 공동 연구 실시
- 2008년 오만은 E-Commerce 법을 처음으로 시행했으며 동 법에 의거하여 전자상거래를 실시하는 법적 근거 마련

주요 전략 및 정책

▶ 전자정부 계획(eGovernment Transformation Plan)

- 2018 UN전자정부보고서에 따르면 오만 전자정부 순위는 193개국 중 63위를 차지하여 아랍 국가 중 6위이며, 온라인 서비스 지수에서 오만 2016년 59%에서 81%을 확보함
- 또한 오만은 UN보고서에서 사이버 보안 추진 정책과 관련하여 상위 국가 중 하나로 평가됨
- 2012년 6월 12일, 전자정부 이행 전략(eGovernment Transformation Strategy)이 내각에 의해

승인되어 공공기관들이 양질의 전자정부 서비스(eService)를 제공할 수 있도록 명확한 지도체계와 목표들이 ITA를 포함한 모든 정부기관에 전달되었음

- eGovernment Transformation 계획은 6단계로 구성이 되며 ePresence Stage (2013년 6월) 이후 현재는 eParticipation Stage가 진행 중임

▶ 국가 인프라 개발(National Infrastructure Development); PKI 등

- ITA가 관련 업무를 담당하며, eVisa, Public Key Infrastructure(PKI), ePayment Gateway, National Data Center, Oman Government Network, National Contact Center 프로젝트가 있음
- 특히, PKI 분야는 국가디지털인증센터(National Digital Certification Center, NDCC)가 암호화, 인증 및 디지털 서명 기능을 이용하여 신뢰성 높은 공간 구축을 지원함
- 2015년까지 NDCC는 ITA를 포함한 13개 기관에 PKI 구축을 완료하고, ▲정부 포털과 전자 서비스를 위한 국가 ID/거주증 보안 인증 ▲정부 포털 및 전자 서비스를 위한 모바일 PKI 인증 ▲전자서명 기반 문서 및 전송 ▲서버 서명을 위한 시간인증(Time Stamping) ▲서버 서명을 위한 OCSP ▲서명 검증 등의 PKI 기반 서비스를 제공함
- NDCC는 이미 12개 정부 및 민간 기관(Ministry of Commerce and Industry, Ministry of Health, Ministry of Manpower, Bank Dhofar, Public Prosecution, Muscat Municipality, Al Raffd Fund, National Center for Statistics & Information, ROP DG of Customs, Public Authority for Social Insurance, ITA, Ministry of Environment and Climate Affairs)의 22개 시스템에 PKI를 적용하였음
- 현재까지 ▲ID/거주증(검증 및 전자 서명) 6백만 개 발급 ▲Omantel 및 Ooredoo를 통하여 PKI 내장 SIM 카드 기반 1,271개 MPKI(Mobile PKI) 발급 ▲포털 및 웹사이트용 SSL 91개 인증서 ▲공부원용 PKI 기반 통합 토큰 86개 등의 실적을 보임

2) 담당기관

▶ 오만 국가침해사고대응팀(OMAN National Computer Emergency Response Team, OCERT)

- 사이버 공간에서 발생할 수 있는 위험들과 보안 위협들을 분석하고 인터넷 서비스 이용자들에게 이러한 사이버 보안 관련 정보를 제공하기 위해 2010년 4월에 설립된 오만의 전문 IT 보안 기관임
- OCERT의 설립 목적은 ▲정부의 e-service에 대한 신뢰성 수립 ▲인터넷 공간에서의 사이버 보안 인지 수립 ▲보안 사고에 대처하기 위한 사이버 보안 역량 강화 ▲발생한 또는 발생이 예상되는 보안 위협 및 취약성에 대한 정확하고 신속한 정보 제공 – 보안 위협 가능성 및 영향에 대한 분석 ▲보안 사고를 최소화하기 위한 사전 측정 ▲보안 사고와 그 영향력의 최소화를 위한 대응 ▲정보 보안 R&D 향상

▲아랍 지역 및 국제 CERTs와 협력 등임

그림 _ Oman National CERT (OCERT) 홈페이지



- OCERT는 ▲Training & Awareness ▲Proactive Service ▲Reactive Service 등 3개 분야에서 30여 개 이상의 서비스를 제공함
- Proactive Service는 사이버 관련 범죄 및 사건이 발생하기 전에 보안서비스의 지속적인 향상 또는 탐지를 지원하기 위한 서비스이며, Reactive Service는 내부 시스템에 대한 어떠한 종류의 위협이나 공격으로부터 발생하는 사건에 대한 지원 및 보고 등에 대한 요청에 대응하는 서비스임
- OCERT는 이슬람 보안 협력체계인 OIC-CERT의 멤버로 상호협력을 강화하고 있으며 한국의 보안기업 더존비즈온도 OIC-CERT 멤버로 활동

▶ 정보보안부(ISD, Information Security Division)

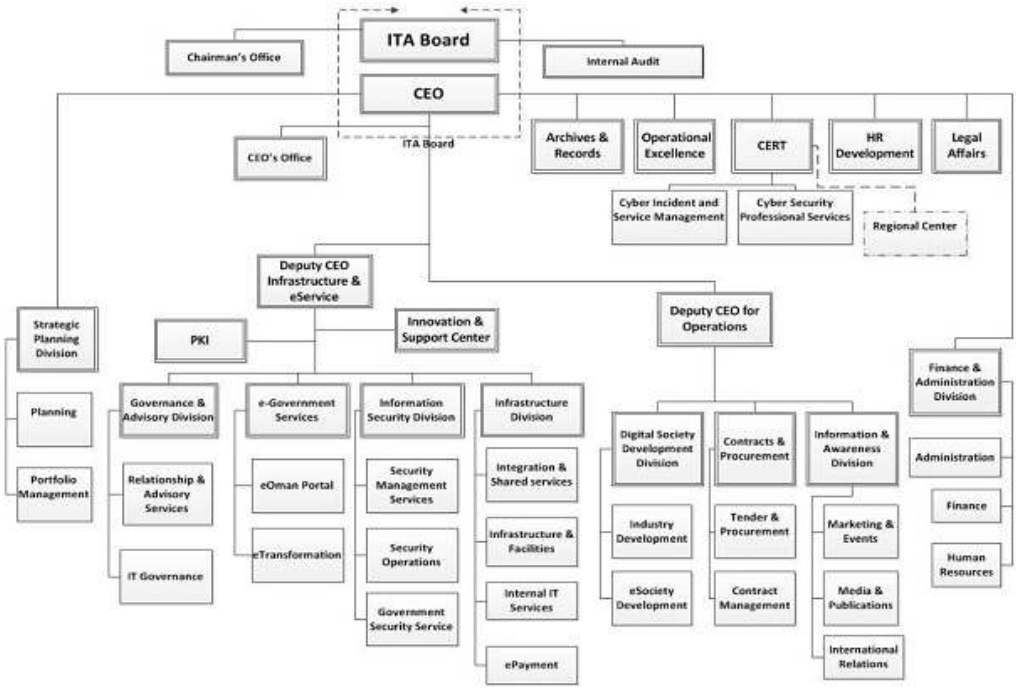
- 사이버 IT 관련 법률 및 사이버보안측면에서 정보보안부(ISD)는 e오만 사업의 핵심적인 역할을 수행하고 있음
- 해당 부서는 오만에서의 보안 위험을 해결하고 보안에 대한 인식을 향상시키는 것을 목적으로 설립되었으며 다양한 범위의 보안 서비스를 제공함
- ISD는 정보 기밀성, 무결성과 접근을 보장하는 모범사례에 따라 정부기관 및 산하기관에 보안 서비스를 제공하고 있으며, 다른 한편으로 정부 기관과 산하기관 직원들에게 정보보안에 대한 인식을 교육시키기 위해 정보보안 관리 시스템, 위험 관리, 사업 연속성 관리, 재해복구와 같은 주제의 세미나 및 워크숍 개최를 포함한 여러 가지 활동을 수행하고 있음

▶ 정보기술청(Information Technology Authority, ITA)

- 정보기술청은 오만 디지털 사회(Digital Society)[200] 목적을 달성하기 위해 2006년 국왕령 제42호(Royal Decree No: 42/2006)에 근거해 설립됨
- 정보기술청(ITA)은 국가경제청(Minister of National Economy, MoNE) 산하 기관으로서 eOman의 실현을 전담하고 정보통신 기술을 이용하여 오만을 지속성 있는 지식 사회로 변화시키기 위한 업무를 수행함
- eOman은 지식사회를 구축하기 위한 오만의 최고 통치자인 술탄 Gaboos bin Said의 비전을 기반으로 설립되었으며, 국민들에게 더 나은 공공서비스를 제공하기 위하여 정부-사회-시민을 연결하는 효율적인 인프라 구축을 주요 목적으로 함
- 이 기관은 ▲사이버 범죄 예방 전략, ▲사이버 범죄 수사를 위한 훈련, ▲오래되어 실효성이 떨어지는 법률에 대한 검토 등을 담당하며, 사이버 공간에서 테러 집단들이 소셜 미디어 등을 악용한 활동을 벌이지 못하도록 인도 및 미국의 정보기관들과도 공조하고 있음

200 2003년 3월, 오만 국왕은 오만 비전 2020(Oman Vision 2020)의 일환으로 디지털 사회와 전자정부 개발을 위해 '디지털 오만 전략'을 발표

그림 _ 정보기술청(Information Technology Authority, ITA) 조직도



[출처] Information Technology Authority 홈페이지

▶ 통신규제청(Telecommunications Regulatory Authority, TRA)

- 오만 통신 관련 정책들을 수행할 목적으로 국왕령 제30호(Royal Decree No: 30/2002) 하에서 공포된 통신법(Telecommunications Act)에 따라 오만 내 통신 서비스에 대한 규제 완화와 촉진을 위해 2002년에 설립됨
- TRA는 통신 분야의 성장을 촉진하기 위한 위원회로서, 확대되는 다양한 서비스들을 합당한 가격으로 고객들에게 공급하기 위한 최신의 기술이 적용될 수 있도록 보장함
- 신규 시장 상황에 맞는 규제와 규정들을 소개함으로써 오만 경제의 경쟁력을 향상시키고 지식 사회로의 발전 및 기술들의 향상을 위한 환경을 제공함

▶ 교통통신부(Ministry of Transport & Communications, MOTC)

- 교통통신부는 교통 및 통신 분야에서 2040년까지 세계 10대 국가로 진입하기 위한 업무를 수행함
- 통신 분야의 조직은 정책 제정, 규제 및 운영 등의 3개 주요 기구들 간의 분리를 기반으로 세계 표준에 의거하여 구성되는데, 교통통신부(MOTC)는 일반 정책 프레임워크 수립과 그에 따른 업무 수행을 담당하며, 통신규제청(TRA)은 통신규제법에 따라 통신 분야 서비스에 대한 규제를 담당하고, 통신사 및 서비스 제공사업자는 부여된 허가를 기반으로 통신서비스를 제공하는 공공기관 및 사기업을 지칭함

▶ 국가디지털인증센터(National Digital Certification Center, NDCC)
- 2013년 12월 24일에 개설된 ITA 산하 기관으로서 중동 지역에서는 최초임
- 스마트폰을 통하여 기업과 개인을 대상으로 발급되는 eSignature 공인 인증서에 대한 실제 운영 프로젝트의 두 번째 단계임
- 적용된 공개키 기반의 PKI 기술을 기반으로 온라인 서비스 사업자들은 디지털 인증서에 대한 신뢰성을 향상시킴

3) 규제 및 인증제도

▶ 오만은 자국 내에 별도 인증제도를 보유하고 있지 않기 때문에, 해외 주요 인증(UL, CE) 등으로 인증을 대체하거나 선적전 검사제도를 사용하기도 함

▶ 오만 ITA는 국제적으로 통용되는 사이버 보안 표준인 국가 사이버 보안 프레임워크인 ISO 27001 표준을 공식적으로 인정하고 있음
- 핵심 정보 인프라를 운영하는 모든 조직들이 인증받고 있는 ISO 27001 네트워크 보안 표준 (Network Security Standard ISO 27001)에 의거한 정보 보안 관리 실천방침을 공식적으로 인정하고 있음

▶ 사이버 보안 전문가 개발 서비스 기관인 OCERT는 다양한 정보보안 관련 교육을 제공하며, 인증서를 발급하고 있음
- OCERT는 정보보안 역량 강화를 위한 교육과정 및 인증 과정을 제공함으로써 다양한 보안 분야에 대한 프로페셔널 사이버 보안 교육을 실시함
- ISC, SANS 및 EC-council 등의 국제적 교육기관과의 협력을 통하여 정보보안 분야 교육 프로그램을 운영

4) 최근 정책 동향 및 이슈

▶ 오만 로컬기업 Thawani Pay는 핀테크 기술이 적용된 Thawani Pay 플랫폼 기반의 서비스를 오픈함(2018.3)
- Thawani Pay는 '07년부터 동 플랫폼(Apple Pay 대응, 자체솔루션)을 개발해 왔으며 모바일 애플리케이션을 통하여 전자 지불에서 비즈니스 분석까지 수행 가능함

- 사용자는 자신의 신용카드 또는 직불카드를 등록하고 모바일 지갑으로 사용할 수 있으며, 기업은 직원배치 및 작업내역 추적 등이 가능함

▶ 오만아랍뱅크(OAB)는 '17년 12월 디지털화로 변화 중인 금융서비스의 미래 비전을 위해 전자 지불 게이트웨이 서비스를 시행(2017.12)

- 고급 보안 및 사용 편의성으로 모든 고객에게 투명성과 편의성을 보장하는 전자 지불 솔루션 제공 추진
- 보안 관련, 데이터 무결성 및 안전한 암호화를 위한 국제 PCI DSS 및 PA-DSS 표준과 모든 CBO(오만중앙은행) 규정에 따라 플랫폼 구축

▶ 오만 국가 디지털포렌식랩 국제인증 획득 (2017.4)

- 더존비즈온은 '오만 국가 디지털포렌식랩'이 국제 공인 포렌식 시험 (Forensic Testing) 기관으로서 ISO/IEC 17025 인증을 획득했다고 밝힘
- 특히, ISO/IEC 17025 인증 획득은 오만 정보기술청(ITA)이 용역계약의 과업으로 제시한 주요 요구사항 중 하나로 인증 획득 분야는 컴퓨터, 모바일, 오디오, 비디오 등에 대한 포렌식 및 디지털 이미지 분석 등 총 5가지 분야임

융합보안시장 및 정책 동향

1) 융합보안시장 동향

스마트의료

▶ 오만 보건부(MOH)는 환자를 위한 스마트 서비스를 개시할 예정임(2019.8)

- 보건부는 2019년 모바일 애플리케이션을 통해 모든 환자들이 자신의 건강 기록과 상태를 온라인으로 볼 수 있는 서비스를 제공할 예정임
- 또한 모바일앱은 환자들이 스스로 진료 예약을 하고 다양한 검진기관으로부터 진료 기록을 받는 기능을 선보일 계획임

핀테크

▶ ITA는 오만 최초의 핀테크 포럼을 무스카트에서 개최(2019 6.)

- OiFF(Oman Islamic FinTech Forum 2019)는 이슬람국가의 핀테크 잠재력을 강조하고 경제발전 및 파이낸스 개선을 목적으로 하며 동 포럼은 글로벌 이슬람 기구를 위한 플랫폼을 마련하여 그들의 경험과 성공사례를 공유하는 기회를 제공할 예정임

블록체인(가상화폐 등 포함)

▶ Oman Oil and Orpic Group이 오만 최초로 블록체인 기반 무역 금융거래를 성사시킴 (2019.11)[201]

- Oman Oil and Orpic Group은 아부다비 국립 카펫공장에 폴리프로필렌 섬유를 판매하는 거래를 완료함
- 거래는 오픈소스 블록체인 플랫폼인 R3의 Corda 플랫폼을 이용하였고 HSBC Oman이 자문역할
- 블록체인을 통해 무역금융의 디지털화를 촉진시킨 사례로서 오만에서의 향후 블록체인 발전 및 활용의 기폭제가 되리라 전망

2) 융합보안정책 동향

201 https://www.orpic.com/news?newsId=1033

블록체인(가상화폐 포함)

▶ 오만은 디지털 혁신을 가속화하기 위해 국가적 블록체인 프로젝트를 개시함(2019.3)

- 해당 프로젝트는 오만통신사 Omantel, 블록체인 솔루션 및 서비스(BSS)와 ITA e-government 부서와의 협력의 결과로 이루어짐
- 블록체인 플랫폼으로는 하이퍼레저 패브릭이 선정되었는데 동 플랫폼은 리눅스 파운데이션과 함께 IBM에 의해 개발되었으며 이미 전 세계적으로 각국 정부 및 기업에 의해 사용되고 있음

스마트시티

▶ 오만은 2019년 4월 Duqm(두큼) 지역에 스마트 시티를 조성할 계획을 발표하고 2020년부터 단계적으로 착공에 들어갈 계획[202,203]

- 두큼 스마트 시티는 맞춤형 스마트 도시로 개발될 예정으로, 여러 단계로 나누어 추진될 예정
- 우선순위에 따라 공공 유틸리티 서비스, 관광, 보안 및 안전, 스마트 포트 솔루션, 캠퍼스 솔루션, 신호등, 도로 조명, 지능형 빌딩 관리 및 폐기물 관리와 같은 영역에서 우선 개발될 예정
- 교통 서비스, 트럭 무게, 스마트 버스 정류장, 주차, 비디오 감시 및 자동차 및 트럭 번호판 식별도 여기에 포함될 예정
- 이 프로젝트는 우리나라와 일본의 영향을 받은 것으로, 2018년 7월 우리나라와는 두큼 경제특구의 스마트시티 조성을 위한 MOU를 체결하기도 하였음[204]

202 https://timesofoman.com/article/1103777/Oman/Phase-I-of-Duqm-Smart-City-project-to-kick-off-next-year
203 https://www.omanobserver.om/duqm-to-be-developed-as-a-smart-city/
204 https://www.yna.co.kr/view/AKR20180725155100001

나. UAE

'18년 GDP(십억달러)	414.18
'18년 인구수(천명)	9,630

■ ITU 글로벌 사이버보안 지수(Global Cybersecurity Index, GCI)

· UAE의 사이버보안 지수 순위는 33위로 상위권에 속함

국가명	2018		2017		전년대비 증감	
	지수	순위	지수	순위	지수	순위
UAE	0.807	33	0.566	47	+0.241	+14
대한민국	0.873	15	0.782	13	+0.091	-2

■ ICT 관련 주요 지수

· UAE의 전반적인 ICT 발전 수준은 전 세계 20% 이내로 상위권을 유지하고 있음

지표명	UAE		한국	
	점수	순위	점수	순위
IMD 국가경쟁력지수(2019)	-	-	-	28
IMD 디지털경쟁력지수(2019)	-	-	-	10
UNCTAD 전자상거래지수(2019)	83.8	28	89.4	19
ITU 글로벌 사이버보안 지수(GCI 2018)	0.807	33	0.873	15
UN 전자정부 지수(2018)	0.829	21	0.901	3

■ ICT 관련 주요 통계 (ITU, 2018년 말 기준)

· UAE의 유선통신 보급률은 20~30%대이지만, 이동통신 보급률은 200%가 넘어 세계 최상위권에 속함

항목	UAE		한국	
	가입자수(천 명)	보급률(%)	가입자수(천 명)	보급률(%)
유선전화	2,341	24.31	25,907	50.63
유선브로드밴드	3,021	31.40	21,286	41.60
이동통신	20,081	208.50	66,356	129.67
인터넷 이용률	98.45%		95.90%	

정보보호 산업 개요

1) 보안 환경

▶ UAE는 풍부한 석유자원으로 인해 부유한 국가로 테러리즘의 역사나 종파 문제가 없는 걸프 지역에서 안정된 국가 중의 하나임

- 미국과 우호적인 유대관계로 인하여 미국으로부터 많은 지원을 받고 있음
- UAE는 민주주의와 투명성에서 다소 낮은 수준이지만, 풍부한 석유자원을 기반으로 한 자금을 보안 및 사회 보장에 투자하고 있으므로, 이러한 정치적 사항들에 대해 반론은 크게 없는 편임

▶ 2000년대 말부터 석유나 가스 산업의 의존도를 줄이기 위한 산업 다각화 정책을 추진 중으로 특히, 방송·통신·미디어 등 ICT 산업이 활성화 대상으로 선정

- UAE를 구성하는 7개 토후국 중에서 가장 큰 아부다비의 경우, 2008년 석유·가스 산업의 의존도를 줄이기 위한 2008년 아부다비 경제비전 2030을 수립
- 2010년 2월에 교육, 제조, 정부 서비스 등에 IT 솔루션을 도입하여, UAE 사회-경제 발전을 진행하겠다는 'UAE Vision 2021'을 발표
- 2014년 7월에는 Vision 2021의 일환으로 ICT 분야를 국가 경제 성장의 새로운 동력으로 추진하는 ICT 산업 발전 마스터플랜 'ICT Strategy 2021'을 발표
- Vision 2021은 UAE 다양한 분야에서 IT 투자가 확대되는 계기가 되었으며, 'ICT Strategy 2021'에는 2021년까지 안전이 보장된 서버를 20배 이상 확충하겠다는 내용이 포함되어 있어, 정부 차원의 보안 투자 확대 의지를 피력

▶ IT 도입과 보안에 대한 정부 투자 의지에도 불구하고, UAE가 외부의 보안 위협에 매우 취약한 상황이라는 분석과 사례가 등장

- Symantec의 2015년 Internet Security Threat Report에 의하면, UAE는 사이버 공격 발생 순위에서 2015년 중동지역 1위였으며, 세계 8위로 기록됨
- Kaspersky Security Bulletin 2016에 의하면, UAE는 뱅킹 트로이목마(Banking Trojans) 공격 비율이 높은 국가 TOP 10에 진입
- 안티바이러스 소프트웨어 업체인 노턴(Norton)에 의하면, 2016년 기준 UAE 소비자 중 253만 명이 사이버 범죄를 당했으며, 이 중 20%는 개인정보 유출을 경험
- 2013년 1,419건의 사이버 범죄가 발생하여, 2011년 588건에서 두 배 이상 증가했으며 사이버 범죄가 늘어감에 따라 관련 법률 개정이 이루어졌음

▶ UAE는 치안 및 시민 보호와 사이버 공격을 대응하는 과정에서 UAE 국토보안을 위한 지출이 증가하고, 이에 따른 보안 관련 장비와 시스템 수요도 증가할 것으로 전망

- 2016년 8월 발표된 시장조사기관 SDI 보고서[205]에 의하면, UAE의 주요 기반시설 정보보호 지출은 35억 달러에서 2025년 46억 달러 규모로 매년 지속 증가할 것으로 전망
- 이 중에서 사이버 보안과 관련된 네트워크 보안 지출은 2016년 2.4억 달러에서 2025년 3.3억 달러로 연평균 3.8% 증가할 것으로 예상됨
- 또한 2017년 3월 발표된 보고서[206]에 의하면, 중동 사이버 보안 시장 규모는 2017년 113.8억 달러에서 2022년 221.4억 달러로 연평균 14.2% 증가할 것으로 예상

2) 인터넷 및 통신 환경

▶ 유선통신

- 2018년 6월 기준 유선 전화 가입자는 232만 명, 전화 밀도는 26%

표 _ UAE 유선 전화 통계 및 주요 사업자(2017년 기준)

TELEPHONE NETWORK STATISTICS	
Fixed telephone lines in service	2.3 million
Fixed-line teledensity/households	24%
Major public telecom operators	• Emirates Telecommunications Corporation (Etisalat) • Emirates Integrated Telecommunications Company (EITC) – trading as 'du'

[출처] Buddecomm(2018.5)

- UAE의 인터넷 이용자 수는 2018년 897만 명으로 2016년 855만 명에서 42만 명 정도 증가한 수치
- 인터넷 보급률은 2018년 94%로 전년 대비 1% 증가

205 SDI(Strategic Defense Intelligence), United Arab Emirates Defense Spends on Homeland Security: 2016 to 2025, 2016.8
206 MarketsandMarkets, Middle East Cyber Security Market by Solution, Service, Security Type, Deployment Mode, Organization Size, Vertical, and Country - Forecast to 2022, 2017.3

표 _ UAE 인터넷 이용자 및 보급률(1995년~2016년)

Year	Users (million) (e)	Penetration
1995	.002	0%
1996	.009	0%
1997	.086	3%
1998	.190	7%
1999	.432	15%
2000	.715	24%
2001	.823	26%
2002	.913	28%
2003	.993	29%
2004	1.102	30%
2005	1.660	40%
2006	2.535	52%
2007	3.536	61%
2008	4.283	63%
2009	4.940	64%
2010	5.740	68%
2011	6.962	78%
2012	7.825	85%
2013	8.225	88%
2014	8.380	90%
2015	8.432	91%
2016	8.556	92%

[출처] Buddecomm(2018.5)

• 유선 브로드밴드 가입자는 2019년 전망치 135만 명, 보급률은 15%

표 _ UAE 유선브로드밴드 가입자 및 보급률(2010년~2017년)

Year	Subscribers (million)	Penetration
2010	.787	9.3%
2011	.867	9.7%
2012	.952	10.3%
2013	1.039	11.1%
2014	1.087	11.5%
2015	1.226	12.8%
2016	1.298	13.3%
2017 (e)	1.342	14.4%

[출처] Buddecomm(2018.5)

• UAE international internet bandwidth의 경우 2016년 최초로 100만Mb/s 돌파(118만 Mb/s) 2010년 10만 Mb/s에서 6년 새 급속성장

- 인터넷 카페가 활성화되어 있음
- 유동 인구인 국외 거주자, 임시 직원이 많아 인터넷 카페 발달
- 2010년부터는 신분이 증명되어야만 이용 가능
- 인터넷 전화(VoIP)는 두 사업체가 독점(Etisalat, Du)
- Skype는 UAE에서 사용 금지, 두바이에서 WhatsApp 인터넷 전화 기능은 사용 불가능
- FTTH 보급률의 경우 2016년 79.6%로 2012년 이래 세계적인 수준
- 유선통신 사업자는 Etisalat, Du, Yahsat가 있음

▶ 이동통신

- UAE 이동통신 가입자는 2019년 전망치 1,970만 명으로, 전체 인구 954만 명(2018년)을 기준으로 보급률은 204%
- 2016년 모바일 시장 점유율은 Etisalat가 54%, Du가 46%
- 모바일 브로드밴드 가입자는 2017년 기준 1,660만 명, 보급률 170%이며, 3G와 LTE 기술의 지속적인 투자로 유선 브로드밴드의 대체재가 되고 있음
- 2017년 Etisalat 가입자 수는 1,076만 명 (2016년 1,040만)
- 2017년 2위 업체 Du의 가입자 수는 810만 명 (2016년 864만)이나, 사업 구조 개편 및 경쟁으로 인하여 가입자 수 감소 추세

표 _ UAE 모바일 이용자 수 및 보급률 (2005년~2017년)

Year	Subscribers (million)	Penetration
2005	4.53	109%
2006	5.52	113%
2007	7.73	133%
2008	9.36	138%
2009	10.67	138%
2010	10.93	129%
2011	11.73	131%
2012	13.78	150%
2013	16.06	172%
2014	16.81	177%
2015	17.94	187%
2016	19.90	204%
2017 [1]	19.69	224%

[출처] Buddecomm(2018.5)

표 _ UAE 모바일 브로드밴드 이용자 수 및 보급률 (2010년~2017년)

Year	Subscribers (million)	Penetration
2010	1.13	13%
2011	1.71	19%
2012	4.13	45%
2013	8.32	89%
2014 (e)	8.50	90%
2015	12.53	131%
2016	15.28	157%
2017 (e)	16.60	170%

[출처] Buddecomm(2018.5)

▶ 5G 현황

- 2019년 5월 UAE 국영 통신사 Etisalat는 중국 스마트폰 제조사 ZTE와 협업하여 중동 및 북아프리카 지역 최초로 5G 기기 및 서비스를 제공
- ZTE의 Axon 10 Pro 스마트폰을 통해 사용자들은 초당 1기가바이트의 네트워크 속도와 지연시간 천분의 1초를 제공하는 5G 서비스를 이용할 수 있게 되며, 추가 비용은 납부하지 않음
- UAE는 5G를 AR/VR, IoT, 자율주행차량, 3D 프린팅, 웨어러블 기술 등으로 확대 적용해 나갈 계획

정보보호 시장 현황

1) 시장 규모

시장 개요

▶ SDI의 'United Arab Emirates Defense Spends on Homeland Security: 2016 to 2025' 보고서에 의하면 UAE의 국토(Homeland)보안 시장은 크게 ▲해양 보안 및 국경 보안 ▲치안 현대화 및 대테러 대응 ▲주요 기반시설 보안(critical Infrastructure security) 등 3개 분야로 구분

- 이 중에서 테러 대응 분야와 경찰의 치안 현대화가 CCTV, 카메라, 비디오 감시 장비, 포렌식(Forensic Science Laboratories) 및 기타 장비 수요 발생 부문
- 또한 주요 기반시설 보안은 ▲물리보안(Physical Security)과 ▲네트워크 보안(Network Security) ▲기타로 구분
- 물리 보안 분야는 사람이 직접 운영/개입하여 주요 기반시설의 보안과 보호를 위한 모든 요소에 투자하는 것을 의미
- 이 분야에 해당하는 장비의 예로는 바이오인식, ID 관리 시스템 등 접속을 제어하는 장비와 비디오 감시 장비, 선별 및 스캐닝 등이 포함
- 네트워크 보안 분야는 네트워크 보안, 데이터 보안, 클라우드 보안, 웹 기반 ID 및 액세스 관리, 보안 통신, SCADA 보안 등이 주로 포함
- 기타 분야에는 보안 컨설팅, 보안 아키텍처 설계, 리스크 관리, 빌딩 또는 시설 관리 등의 보안 관련 서비스가 포함

▶ UAE는 개인 및 민간 기업들의 정보보안에 대한 인식이 미흡하고, 정보보안 인프라가 취약하다는 점 때문에 사이버 공격이나 위협의 주요 타깃으로 노출

- UAE에서의 주요한 보안 침해 사례로는 2013년 라스알카이마 은행이 ATM기 현금 인출, 신용카드 도용 등 사이버 범죄로 4,500만 달러의 피해를 봄
- 2014년에 국영 통신사인 Etisalat도 서버 해킹으로 인한 웹사이트, 요금 납부시스템의 마비로 소비자들이 피해를 본 바 있음[207]
- 2016년 6월 조사에 의하면, UAE에서 온라인 카드 지불 과정에서, 카드 정보 유출, 가짜 거래 등 사기를

207 KOTRA 두바이 무역관, UAE 사이버보안시장(2015)

당한 이용자의 비중도 15%로 조사[208]

- Kaspersky Security Bulletin 2016에 의하면, Kaspersky Security 제품을 구매한 UAE 사용자 중 2.3%가 뱅킹 트로이목마의 공격을 당한 것으로 조사

표 _ 뱅킹 트로이목마 공격 비율 Top 10 국가

순위	국가	공격 비율	순위	국가	공격 비율
1	러시아	4.8%	6	오스트리아	2.6%
2	브라질	4.7%	7	베트남	2.4%
3	터키	4.5%	**8**	**UAE**	**2.3%**
4	스리랑카	4.5%	9	일본	2.2%
5	파키스탄	3.8%	10	모로코	2.2%

[출처] Kaspersky Security Bulletin 2016

▶ 스마트 시티 등 정부 주도 프로젝트와 핀테크 등 주로 스마트폰과 모바일 기반의 IT 시스템 보안을 위한 정부 차원의 사이버 보안 강화 노력과 투자가 강화됨

- 2017년 5월 31일 부통령이자 두바이 총리인 셰이크 모하메드 빈 라시드 알 막툼 (Sheikh Mohammed bin Rashid Al Maktoum)이 사이버 보안 전략을 발표
- 또한, 전자 보안 위협, 사이버 공격 및 모든 형태의 사이버 범죄를 다루는 두바이 전자보안센터(Dubai Electronic Security Center)를 개소
- 향후 스마트 시티 건설 등 IT 시스템을 활용하는 범위가 확대될수록 정부 차원의 사이버 보안 투자 및 공공부문 수요는 지속 증가할 전망

▶ UAE는 정부 차원의 투자뿐만 아니라, 향후 금융권 등을 중심으로 전자메일, 클라우드 보안 등 민간 분야의 보안 수요도 증가할 가능성이 큼

- 2017년 3월 49개 은행이 참여한 UAE 은행 연맹(UAE Banks Federation)이 사이버 보안 위협에 대한 정보를 공유하는 시스템을 구축
- 현지 보안업체 관계자는 UAE 기업에서 취약한 보안 영역 중 하나가 전자메일 보안이며 90% 이상의 사이버 공격이 전자메일에서 시작된다는 의견을 제시[209]
- 또한 현지 보안업체 조사에 의하면, 조사 대상 기업의 50% 이상이 최상위 보안 시스템 중 방화벽(60%)과 패스워드(63%)를 사용하는 것으로 조사
- 이는 향후 클라우드 상에 존재하는 데이터와 애플리케이션 보안이 부족함과 향후 해당 분야에서의 보안 수요가 증가할 것임을 방증

208 ystat.com, Fraud and Security in Global Online Payment, 2016.10
209 The National, 'WannaCry' online attacks a wake up call for cyber security, 2017.5.26

시장 규모 및 성장률

▶ SDI의 'United Arab Emirates Defense Spends on Homeland Security: 2016 to 2025' 보고서에 의하면 2016년 UAE 주요 기반시설 정보보호 시장 규모(Critical Infrastructure Protection Spends)는 16.6억 달러인 것으로 집계

- 이 중에서 물리 보안은 13.6억 달러, 네트워크 보안은 2.4억 달러, 기타 분야는 6천만 달러 규모로 물리 보안 분야 비중이 82%에 달할 정도로 높은 비중을 차지
- 2017년 시장은 물리 보안 13.8억 달러, 네트워크 보안 2.5억 달러, 기타 분야 6천만 달러로 총 16.9억 달러에 달할 것으로 전망
- 2016~2017년 시장 추세에 큰 변화는 없으나, 물리 보안 지출이 1.3% 증가하는 반면, 네트워크 보안 지출은 5.1% 증가해, 상대적으로 네트워크 보안 시장이 큰 폭으로 성장할 것으로 예상

▶ UAE가 2017년 정보보안 분야에 지출할 것으로 예상되는 비용은 GDP 대비 0.42%로서, 1%에 미치지 못하지만, 향후 지속되는 보안 위협에 대응하여, 정부와 민간의 지속적인 지출 증가세가 실현될 가능성이 큼

- UAE 정부는 전자정부 분야에서 급속한 성장을 보여 왔으며, ICT 수준 향상을 위하여 인프라에 투자해왔음
- 전문가들은 중동지역에서 사이버 공격이 더욱 심각해질 것으로 예상하며, 보안 전문업체 Kaspersky Lab에 의하면 UAE는 온라인 공격에 대한 위험성에서 세계 19위이며, 컨설팅 업체 KPMG는 2015년 UAE 기업과 기관들의 33%가 데이터 침해를 당하였다고 발표하였음
- UAE 정부는 사이버 보안 전략을 향상하기 위하여 지난 10년간 평가를 수행해 왔으며, 기술 및 규제를 통하여 UAE 국가 사이버 공간 및 ICT 인프라를 보호하고자 NESA(National Electronic Security Authority)를 설립함

▶ 물리 보안에 대한 주요 소비층은 테러 방지를 포함한 주요 시설 및 자산에 대한 보안 및 경비를 필요로 하는 건설 기업과 공공건물임

- 물리 보안 수요는 공공건물을 포함한 주요 시설, 군사시설, 외국 공관, 외국인 주거단지, 금융기관, 호텔 등 사무실과 주택까지 다양하며, 최근에 테러 방지를 포함한 주요 시설 및 자산에 대한 보안 및 경비를 위해 보안 장비 설치가 보편화되고 있음

시장 전망

▶ SDI에 의하면, UAE 주요 기반시설 정보보호 시장은 2025년까지 22억 달러 규모를 형성, 2016년부터

2015년까지 연평균 3.2%의 지속적인 성장세를 실현할 것으로 전망

- 세부적으로 2025년까지 물리 보안 시장은 18.1억 달러, 네트워크 보안 시장은 3.3억 달러, 기타 분야는 6천만 달러를 형성할 것으로 전망
- 특히 네트워크 보안 시장은 2025년까지 3.8% 성장하면서 전체 정보보호 시장 성장(3.2%)을 주도할 것으로 분석
- 이 같은 측면에서 향후 UAE 정보보호 관련 지출은 물리 보안 시장보다는 네트워크 보안 분야가 주도할 것으로 예상
- 특히 UAE 정보보안 지출은 스마트 시티 등 정부 주도의 대형 프로젝트의 IT 시스템이 본격 추진되고, 민간 수요가 증가하는 2018년이 가장 급격히 실현될 전망

표 _ UAE 주요 기반시설 정보보호 시장 현황 및 전망(2016~2025)

(단위: 백만 달러)

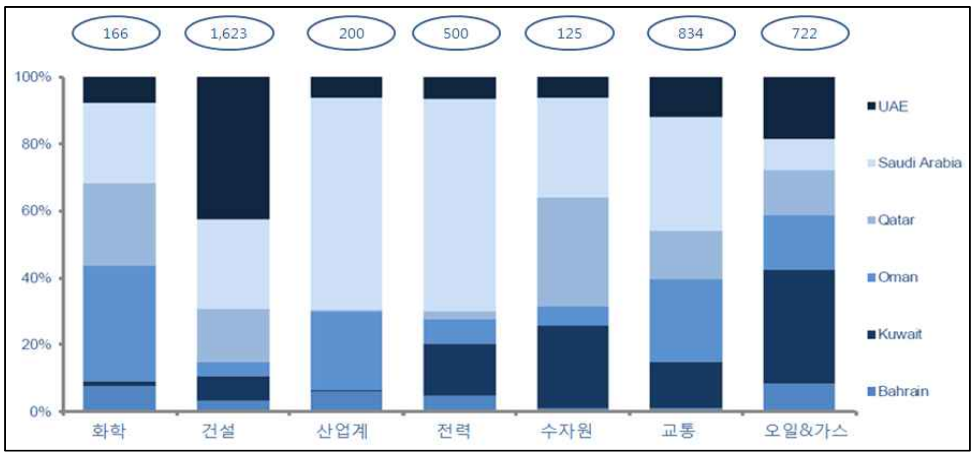
연도	물리 보안	네트워크 보안	기타	합계	성장률
2016	1,362.49	236.00	60	1,658.49	-
2017	1,380.49	248.00	60	1,688.49	1.81%
2018	1,552.59	261.00	64.00	1,877.59	11.20%
2019	1,597.59	281.00	68.00	1,946.59	3.67%
2020	1,636.69	303.00	71.00	2,010.69	3.29%
2021	1,687.69	318.00	74.00	2,079.69	3.43%
2022	1,736.79	316.00	60.00	2,112.79	1.59%
2023	1,734.99	319.00	64.00	2,117.99	0.25%
2024	1,781.19	336.20	68.00	2,185.39	3.18%
2025	1,814.69	330.00	60.00	2,204.69	0.88%
CAGR 2016~2025					3.21%

[출처] SDI,'United Arab Emirates Defense Spends on Homeland Security: 2016 to 2025

▶ UAE는 2017년까지 GCC 다른 국가들 대비 건설 분야에서의 보안 투자가 약 40% 이상을 차지하면서 가장 큰 규모를 차지할 것으로 예상함

그림 _ GCC 프로젝트별 보안 투자 규모 예측 (2014~2017년)

(단위: 백만 달러)



[출처] MEED Insight(www.meed.com)

▶ GCC 전체 보안 솔루션 시장의 규모는 2014년~2017년 42억 달러 규모이며, UAE는 9.9억 달러로 사우디아라비아 다음으로 큰 규모임

표 _ GCC 국가별 보안 솔루션 분야 투자 규모 예측(2014~2017년 합계)

(단위: 억 달러)

사우디아라비아	UAE	쿠웨이트	카타르	오만
12.99 (31%)	9.94 (24%)	5.95 (14%)	5.69 (14%)	5.41 (13%)

[출처] MEED Insight(www.meed.com)

▶ 은행, 금융, 서비스, 보험업 관련 기관을 중심으로 보안 시장이 확대되고 있음

- 현재 정부 영역이 상당 부분을 차지하고 있는 가운데, 보안관리서비스 시장 성장의 핵심고객이 은행, 금융, 서비스, 보험업 관련 기관들로 나타나고 있으며, 미래시장 성장은 오일, 가스, ICT, 헬스, 미디어, 제조영역에 의해 주도될 전망임[210]

▶ 방산 부문의 성장은 사이버보안시장 성장의 긍정적인 요소로 볼 수 있음

- UAE 정부는 2014년 약 256억 달러를 방산 부문에 지출한 것으로 추정되며, 2015년에는 전년 대비 7.3% 증가한 약 275억 달러를 지출한 것으로 추정됨[211]

---

210 Newswire Today, (http://www.newswiretoday.com/news/151154/)
211 BMI(2015)(www.bmiresearch.com)

표 _ UAE 정부의 연도별 방산 부문 지출액 현황 및 전망

(백만 달러, %)

구분	2012년	2013년*	2014년**	2015년**	2016년**	2017년**
지출액	22,527.2	24,182.3	25,655.7	27,530.0	29,455.4	31,346.7
증가율	2.9	7.3	6.0	7.3	7.0	6.5

[출처] BMI, UAE Defense & Security Report (Q1, 2015), KOTRA(2015)
주) * 추정치, ** 전망치

2) 분야별 현황

물리 보안제품 및 서비스

▶ 건설 경기 호조와 시민 안전 강화의 요구에 따른 CCTV 수요가 증가할 것으로 예상됨

- UAE 보안 시장은 금융위기 이후 되찾은 건설 경기 활기로 각종 인프라 시설 및 대규모 주택, 산업단지의 건설이 예정되어 CCTV 수요도 증가할 것으로 예상됨
- 2014년 기준 UAE에서 진행 중이거나 발주 예정인 프로젝트 규모는 부동산 건설 프로젝트가 409건으로 전체의 50%에 이름
- 두바이국제공항의 연간 6,000만 명 수준의 승객 처리능력을 2018년 9,000만 명 수준으로 확충하기 위해 78억 달러 규모의 확장공사 및 두바이 알 막툼, 아부다비, 알아인 등 UAE 대부분의 공항 및 항만 확장 계획을 발표하고 진행 중임
- 아부다비의 경우 치안 및 시민 보호를 위해 도시지역과 해안가, 발전소 주변에 최첨단 CCTV를 통한 감시를 강화하고 있으며, 인근 GCC 국가의 건설 경기 호조로 인해 재수출을 위한 CCTV에 대한 수요도 증가할 전망임

▶ UAE는 중동지역에서 비디오 감시 시스템 최대 수요국 중의 하나로서, 지능형 보안 및 정부의 이니셔티브의 증가로 인하여 향후 급속히 성장할 것으로 예상됨

- 비디오 감시 카메라의 판매가 하락으로 시장 경쟁이 더욱 치열해질 것으로 예상되며, 시장 규모는 더욱 확대될 것으로 전망됨
- 2021년 UAE의 비디오 감시 시장 규모는 2억 9,300만 달러에 이를 것으로 예상하며[212], IP 기반 비디오 감시 시스템이 시장 성장을 더욱 촉진시킬 것으로 보임

212 6Wresearch, Middle East Video Surveillance Market(2015-2021), 2015.10.

• UAE 정부 주도 프로젝트에서 IP 기반 비디오 감시 시스템을 도입할 것으로 예상됨에 따라 관련 시장은 더욱 신속하게 성장할 것으로 예상됨

정보보안 제품 및 서비스

▶ 미 상무부에 따르면 정부 주도의 프로젝트를 중심으로 고급 보안 솔루션에 대한 투자가 이어질 전망으로, 특히 주요 인프라 프로젝트에 대한 보안 위협 관리 수요가 상당히 증가할 전망

• 테러 공격에 대비해 지휘권자의 의사결정을 도울 수 있는, 위기관리 및 사고관리 소프트웨어 솔루션 시장의 수요가 증가할 것으로 예측

• 이와 함께 리스크 관리의 가치가 갈수록 강조되면서 보안 컨설팅 서비스도 유망한 것으로 분석

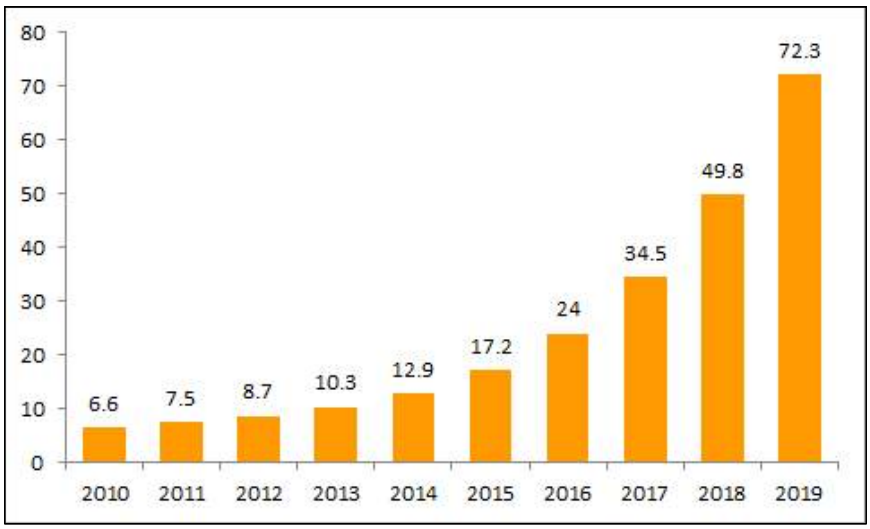
▶ UAE의 안티바이러스, 안티스파이웨어, 안티스팸 등 정보보안 소프트웨어 시장은 2012년 5,300만 달러에서 2015년 7,100만 달러로 성장했으며[213] 클라우드 보안 시장은 2019년 7,230만 달러 규모로 성장할 것으로 전망

• 클라우드 보안 시장은 2014년 1,290만 달러 규모에서 2019년까지 7,230만 달러의 시장을 형성할 것으로 전망되며[214] 2019년에는 네트워크 보안 시장의 12.7%까지 비중이 증가할 것으로 예측됨

• 또한 클라우드 보안 시장은 중소기업이 대기업에 비교해 높은 비중을 차지할 것으로 예상됨

그림 _ UAE 클라우드 보안 시장 전망

(단위: 백만 달러)



[출처] Frost & Sullivan(2013.05), KISA(2013)[215]

213 Kaspersky, 2012.01
214 Frost & Sullivan, 2013.05

3) 주요 사업자 현황

시장 특성 및 경쟁 강도

▶ UAE 시장은 글로벌 벤더들의 시장 점유율이 높은 편이며, 현지 법인설립을 통한 직접 판매방식과 현지 사업자들에 의한 간접 판매방식이 공존하고 있음

- Kaspersky Lab, Trend Micro 등 글로벌 벤더들은 현지법인을 설립하여 직접 판매도 하지만, 복수의 에이전트를 통한 다양한 유통채널을 활용해 도매업자/유통업체(1차), 리셀러(2차) 등으로 구성된 간접 판매에도 적극적임
- 글로벌 벤더들에게 기술 의존도가 높아 현지 사업자들은 에이전트, 유통업체, 리셀러 역할에 편중되어 있음
- UAE에서 한국 CCTV 제품의 성능은 이미 업계에 정평이 나 있으나, 최근 가격 문제로 시장 점유율이 하락하는 추세이며, 주로 선호하는 브랜드는 Honeywell, Pelco, Bosch, Siemens, Sony, Panasonic과 같은 글로벌 기업의 제품이며 중국산 제품 중에는 중국 CCTV 내수 시장 매출 1위의 Hikvision, Dahua 등의 업체가 비교적 높은 인지도를 가지고 있음

▶ UAE를 포함한 GCC 국가에는 글로벌 보안 기업이 대부분 진출해 있으며, Thales, IBM, UTC(전 GE Security), Honeywell, Schneider/Pelco, Siemens, Johnson Controls, Cisco, ARINC 및 Axis Communications 등이 시장을 주도하고 있음

- 특히 UAE는 인접 국가로의 수출을 하는 유통 지로 인근 GCC 국가로의 재수출 중심지가 되고 있으며 이들 글로벌 기업은 글로벌 및 현지 로컬 파트너를 통해 보안 솔루션을 구축하고 있음
- UAE 사이버 보안 시장은 공공과 민간부문으로 나뉘며, 공공부문은 정부 프로젝트가 대부분으로 Thales(프랑스), Narus(Boeing의 자회사) 등의 유럽, 미국 기업이 선점하여 경쟁이 치열함
- 주요 소프트웨어 사업자들은 아부다비와 두바이에 위치하며, 자유 무역지구를 중심으로 시장이 형성되어 있음
- 각 부문 관련 사업자 수는 컴퓨터 네트워크 시스템(96개), 컴퓨터 소프트웨어(206개), 컴퓨터 훈련 서비스 소프트웨어(103개) 등임

---

215 한국인터넷진흥원, 글로벌 정보보호 산업 동향조사, 2013년 제 4호 유럽・중동 편

그림 _ GCC 국가의 주요 보안 기업



[출처] http://www.sourcesecurity.com

표 _ 2015년 UAE 기능별 정보보호 기업 분류

산업	총 기업 수	총매출액(백만 달러)	총 고용인원
보안 시스템 서비스 (Major 1)	1,005	322	5,135
보안 시스템 서비스 (Minor 2)	150	159	1,062
화재 경보 관리 & 모니터링	34	11	198
보안 방법 기기	148	22	675
구류 감시 시스템	33	13	152

Major 1: 통상적이고 일반적인 보안 시스템 서비스, Minor 2: 특정 기업 또는 영역에 국한된 보다 세부적인 보안 시스템 서비스

[출처] Barnes Reports, '2015 World Industry & Market Outlook_Security Systems'(2014.12)

주요 사업자

▶ Techno World LLC

- 두바이를 기반으로 하는 컴퓨터 장비, 컴퓨터 소프트웨어, 시청각 기록 장비 등을 다룸

▶ Open Source Computer Solutions(OSCOMP)

- 주요 사업 분야는 IT Consultancy, Project Management, Information Security, IT Infrastructure Services, Wireless & Structured Cabling, Cloud Services, PABX, IP Telephony, Audio/Video Solutions, CCTV / IP Security, Managed Services 등임
- 2003년 설립되었으며, 중소기업이 주요 사업 대상임

▶ Pan Cyber Information Technology LLC

- 1997년 설립되었으며, UAE의 두바이와 인도의 첸나이에 사무소가 있음
- Pan Cyber는 다양한 IT 솔루션을 제공하고 있으며, 이 중에서 보안 관련 분야로는 VERINT이 Voice/Screen Recording, Quality Monitoring & Analysis, 모바일 뱅킹 관련 솔루션 등이 있음

▶ Thales

- 기업들에 중대한 인프라 사이버 보안 솔루션을 제공하기 위해, HP와 Mubadala Development Company의 조인트 벤처인 Injazat Data Systems와 파트너십을 체결
- 두바이와 아부다비 공항에 보안 및 통신 시스템 구축, ▲2013년 두바이국제공항 3터널에 초현대식 커뮤니케이션 및 보안 솔루션을 공급 ▲에미레이트 은행에 전자 결제 보안 솔루션 공급 ▲2013년 Injazat Data Systems와 협력하여 UAE 기업들에게 제공할 사이버 보안 시스템을 구축함

▶ Narus(Boeing의 자회사)

- 2013년 11월 Dubai Airshow에서 역량을 강조한 사이버 보안에 집중
- Narus는 정부와 민간 기업에 사이버 보안 솔루션을 제공하기 위해 Boeing, IBM, Maxtera, HP, NEC, Secure Tech, Giza Systems, Dell과 파트너임

▶ DarkMatter

- DarkMatter는 두바이에 본사를 두고 있는 보안 회사로서, 제공하는 서비스로는 ▲보안 컨설팅 및 전략 ▲침입 탐지 및 테스트 ▲턴키 수행 및 지속적인 운영 관리 ▲공격이 발생했을 때 복구 서비스 등을 제공함
- 주요 사업 분야는 ▲거버넌스, 위기 및 컴플라이언스 ▲사이버 네트워크 대응 ▲보안 서비스 관리 ▲커뮤니케이션 보안 ▲인프라 & SI ▲스마트 솔루션 등임

▶ Kaspersky Lab

- 러시아 모스크바에 본사가 있으며, 보안제품 Kaspersky를 개발한 보안업체
- 안티바이러스, 안티멀웨어 시장의 약 37%, 소비자 정보보안 시장의 약 30~40%를 차지하고 있음

4) 주요 동향 및 이슈

▶ 다크매터, UAE 사이버보안 연구상 발표 (2019.8)[216]

- 다크매터는 세계의 스마트 도시를 미래의 사이버보안 위협으로부터 보호하는 아이디어를 활성화하기 위한 UAE 사이버보안 연구상 이니셔티브를 발표
- 다크매터는 칼리파 대학교(Khalifa University)와 전략적인 협업을 맺고, 지역 및 국제기관의 대학생, 대학원 연구 조교, 연구원 및 교직원을 대상으로 스마트 도시 시대에 사이버보안 분야를 발전시키는 아이디어, 혁신적인 솔루션을 제시하는 사람에게 포상
- 아이디어 제안서 제출 기한은 2019년 8월 30일 종료되었으며, 후보군들이 2020년 2월에 발표 된 다음, 최종 우승자는 2020년 5월에 발표

▶ 구글, 다크매터 인증을 받은 웹사이트 차단 (2019.8)[217]

- 구글은 UAE 주도 해킹 작전을 벌인 것으로 드러난 다크매터가 인증한 웹사이트들을 블랙리스트에 등재
- 크롬, 안드로이드 브라우저는 UAE 보안 업체 다크매터가 인증한 모든 웹사이트를 안전하지 않을 것으로 표시하였으며, 이러한 조치를 취한 이유는 APT 활동을 했다는 신뢰할만한 증거를 수집했기 때문
- 로이터 통신은 2019년 1월, 보안 업체 다크매터가 UAE 정보기관을 대신하여 자/타국 국민들의 인터넷 활동을 해킹, 감시하는 사이버 작전 '프로젝트 레이븐(Project Raven)'을 수행하였다는 것을 폭로
- 인권 활동가, 언론인, 경쟁 정부 관료 등이 인터넷 계정 해킹 대상인 것으로 드러났으며, 다크매터는 사실무근이라고 반박

▶ 중동을 목표로 하는 사이버공격 증가 (2019.6)[218]

- 다크매터가 발표한 보고서에 따르면 지난 6개월간 중동, 특히 UAE를 목표로 하는 사이버공격이 급증
- UAE는 중동에서 가장 디지털화된 국가 중 하나이자 스마트폰 보급률이 높은 국가로, 사이버공격을 하기에 이상적인 목표
- 주 공격목표는 UAE의 중요 기반시설인 석유/가스 시설이며, 주요 동기는 사이버 첩보 및 사보타주, 주 공격수단은 이메일을 통한 스피어피싱(spear phishing)
- UAE는 2019년 첫 분기에만 총 2,340만 건의 멀웨어 공격을 받았는데, 이는 전년도 대비 12% 증가한 수치
- 모바일 멀웨어 공격의 경우 5만2천 건이 발생하였는데, 이는 전년도 대비 20% 증가한 수치이며, 피싱 공격의 경우 110만 건 이상이 발생

---

216 mystartupworld, "DarkMatter announces UAE Cybersecurity Research Award", 2019.8.27.
217 Reuters, "Google blocks websites certified by DarkMatter, after Reuters reports", 2019.8.2.
218 Khaleejtimes, "Cyberattacks increasing in UAE, study says", 2019.5.1.

▶ 미국 통신사 AT&T, 두바이 텔레콤 보안 얼라이언스 가입 (2019.3)[219]

- UAE에서 출범한 두바이 국제 텔레콤 보안 얼라이언스(Dubai: The Global Telco Security Alliance)에 미국 통신사 AT&T도 가입
- 얼라이언스는 2018년 4월, UAE 통신사 Etisalat, 싱가포르 통신사 싱텔(Singtel), 일본IT기업 소프트뱅크(SoftBank), Telefónica가 공동으로 구성
- 두바이 국제 텔레콤 보안 얼라이언스는 기업에 사이버보안에 대한 정보 및 자문 등을 제공하고 있으며, 최근 자라나는 사이버공격 및 기타 위협에 대응하기 위해 기업들을 지원
- AT&T의 가입으로 현재 두바이 국제 텔레콤 보안 얼라이언스는 4개 대륙, 60개국 12억 명의 인구를 담당
- AT&T는 최근 사이버보안 기업 에일리언볼트(AlienVault)를 인수하며 보안기술 및 역량을 강화한 바 있으며, 6천 명 이상의 보안전문가와 28개 국제 운영센터의 네트워크를 보유 중

▶ 다크매터, 보안 유지를 위한 군사용 스마트폰 개발 (2019.2)[220]

- UAE 보안 기업 다크매터는 군용 및 주요 기반시설 관리자용 스마트폰인 카팀R01(Katim R01)을 발표
- 카팀R01은 압력, 모래, 수중 등 극한상황 속에서도 작동이 가능하며, 다크매터의 최신 사이버보안 기술을 집약하여 해킹으로부터 안전
- 다크매터는 군용은 물론 걸프 지역의 근간산업인 건설, 광업, 교통 및 에너지 기업 관리자들을 위하여 카팀R01을 개발하였다고 밝혔으며, UAE, 핀란드, 캐나다 소프트웨어 엔지니어들이 서로 협업하여 안전한 소프트웨어를 개발
- 카팀R01은 실시간 모니터링 시스템으로 사용자의 데이터의 해킹, 유출 여부를 감시하며, 개인정보 보호를 강화할 수 있는 특별 통화 모드도 탑재

---

219 Gulf News, "American tech giant AT&T joins alliance formed by UAE's Etisalat, other telcos to boost cybersecurity", 2018.3.26.
220 The National, "Explainer: Cybersecurity firm DarkMatter's military smartphone", 2019.2.18.

정보보호 정책 및 기관 현황

1) 관련 법령 및 정책

관련 법령 및 규제

▶ 정보보호법(Law No.9 of 2004)

- 2004년 정보보호법 제정 이전 UAE에는 통합된 정보보호법은 없었으며, 1971년 개정된 헌법(UAE Constitution of 1971) 및 연방거래법(Federal Law No. 5 of 1985)의 일부 조항에 정보보호와 관련된 내용이 포함되어 있음
- 2004년 정보보호법을 제정, 2007년 4월 기존의 정보보호법을 더욱 강화한 새로운 정보보호법(DIFC Law No.1 of 2007)으로 개정함
- 2004년 정보보호법에 기반을 두어 정보보호위원실(Office of Commissioner of Data Protection)이 설립됨

▶ 전자상거래법(Federal Law No. (1) of 2006 on Electronic Commerce and Transactions)

- 총 37개 조항으로 구성되었으며, 온라인 계약, 전자서명, 정부의 전자서명 이용, 인증기관 및 인터넷상의 온라인 계약 증거력 등과 관련된 사항들을 규제함

▶ 개정 정보보호법(DIFC Law No.1 of 2018)

- 2007년 개정된 정보보호법(DIFC Law No.1 of 2007)은 개인의 정보 수집, 처리, 노출 및 이용에 관한 내용을 담고 있으며, EU 지침(EU Directives) 및 OECD 가이드라인을 수용하여 반영함
- 가장 큰 특징은 제11항 및 제12항에서 규정하고 있는 국제 전송 조항으로서, UAE의 정보보호법(DIFC Law No.1 of 2007)의 적용이 불가능한 지역에 UAE 국민의 개인정보가 제공되는 경우에도 UAE 국내에서와 같은 수준의 개인정보보호에 대한 법적 규제가 적용된다는 내용임
- 만약, UAE와 같은 수준의 개인정보보호 법적 보호 장치가 없는 국가에 정보를 전송할 때는 기본적으로 정보의 전송이 불가능하나 10가지 예외 사항을 두고 있음
- UAE의 개인정보보호와 유사하다고 인정되는 국가는 영국, 네덜란드, 이탈리아 등 유럽 국가를 포함한 37개 국가임

▶ 사이버 범죄법(Federal Law No. 5 of 2012 Combating Cyber Crimes)

- 2012년 제정된 법으로서, 개인의 사생활과 관련된 정보를 사진이나 데이터 형태로 복사하거나 저장 및 유포시킬 경우 최소 6개월, 최대 50만 디르함에 이르는 벌금형에 처할 수 있도록 하는 규정하고 있음
- 사이버 범죄법의 집행을 지원하기 위하여 2012년 국가전자보안청이 설립되었음
- 또한, 스마트폰 앱 등을 이용하여 타인에게 모욕을 주는 행위도 처벌 대상으로서, 2015년 6월 UAE에서 WhatsApp 상에서 동료에게 욕설한 남성에 대하여 연방 대법원은 25만 디르함의 벌금형에 처함
- 2018년 8월 13일 기존 조항 3개를 수정한 Emiri Decree No. 02 of 2018가 통과되었는데, 온라인 웹페이지를 운영하는 개인이나 단체가 테러리즘을 부추기거나 유발하는 글을 작성할 경우 최대 25년의 징역형이나 최대 400만 디르함에 이르는 벌금형에 처해질 수 있으며, 국가의 공공질서를 해치는 웹사이트를 운영하거나 온라인에 유포하는 경우도 일시적인 구금과 100만 디르함의 벌금형에 처함

▶ 사업장 내 CCTV 의무 설치법 발효

- 2011년부터 아부다비와 두바이 경찰청 연합은 병원, 호텔, 은행, 유통업체, 금융 등 산업 영역의 구별 없이 모든 사업장 내에 CCTV 설치를 의무화하는 법을 신규 제정함

주요 전략 및 정책

▶ 두바이, 사이버 보안 전략 발표(2017.5)

- 2017년 5월 31일 UAE 부통령이자 두바이 총리인 셰이크 모하메드 빈 라시드 알 막툼(Sheikh Mohammed bin Rashid Al Maktoum)이 두바이의 사이버 보안 전략을 발표
- 지적 재산을 국가의 핵심 자원으로 인식하고 포스트 석유 시대를 대비하기 위한 'UAE 비전 2021'의 일환으로 사이버 보안전략을 추진
- 모든 형태의 사이버 위협 및 공격과 사이버 범죄를 다루는 두바이 전자보안센터(Dubai Electronic Security Center) 개설을 통한 보안 수준의 향상이 목적
- 또한 금번 두바이의 사이버 보안 전략은 ▲사이버 스마트 국가(Cyber Smart Nation) ▲혁신(Innovation) ▲사이버 보안(Cyber Security) ▲사이버 대응력(Cyber resilience) ▲국제협력(National and International cooperation) 등 6개 세부 과제로 구성

표 _ 두바이 사이버 보안 전략 세부 과제

세부 과제	상세 내용
사이버 스마트 국가	• 사이버 보안의 중요성에 대한 대중의 인식을 높이고 두바이 정부, 기업, 개인 간 위험 관리에 필요한 기술과 역량을 개발
혁신	• 전자 보안 분야의 연구와 '자유롭고 공정하고 안전한' 사이버 공간의 설립
사이버 보안	• 데이터의 기밀성, 신뢰성, 가용성 및 개인정보를 보호 계획 수립
사이버 대응력	• 사이버 공격 발생 시 IT 시스템의 연속성과 가용성 보장 및 사이버 보안과 관련된 사건 관리 및 위협에 대처하기 위한 플랫폼도 구축
국가 및 국제협력	• 사이버 공간에서 위협에 대응하기 위해 글로벌 및 지역 차원에서 여러 분야의 협력을 위한 지역 및 글로벌 파트너십을 수립



[출처] Gulf business

▶ UAE Vision 2021

- 2010년에 UAE 정부가 발표한 'UAE Vision 2021'은 UAE의 사회-경제 발전을 주요 주제로 함
- 내각 미래부(Ministry of Cabinet Affairs and the Future)가 주관하며, 가능한 높은 수준의 복지 국가인 UAE로 나아가기 위한 다차원적인 프로그램으로서 이를 실현하기 위하여 교육, 제조, 정부 서비스 등에 IT 솔루션을 적극 도입 및 IT 투자 증가

▶ 정보보안규제 결의안(Cabinet Resolution No. 21 of 2013 On the Regulation of Information Security at the Federal Entities)

- 기업 내 직원들 간의 IT 보안 의식을 강화하고, 연방 정부 기구의 IT 부서에 의해 세워진 가이드라인을 준수하게 함을 목적으로 함
- 또한 IT 인프라와 업그레이드된 보안 대응 레벨을 통과한 데이터의 안전성을 보장하는 연방 정부 기구들을 위한 법적 프레임워크를 제공함
- 추가로, 연방 정부의 IT 담당 부서는 데이터와 IT 자산의 안전성을 보장하고 서비스의 지속성을 보장하기 위하여 모든 사전 주의를 수행하여야 함을 요구하고 있으며, 비밀 데이터를 다루는 경우는 고수준의 암호화 알고리즘을 사용해야 한다는 규정이 있음

▶ 스마트 시티의 사이버 보안을 위하여 e-Security Centre(Dubai Centre) 설립

- 두바이는 기술 혁신뿐만 아니라 인프라 설계 및 전략적 보안 분야에서 새롭게 부상하는 도시로서, 2020년까지 두바이를 '스마트 시티'로 조성하기 위하여 사이버 보안을 위하여 Dubai Centre를 설립함
- 2014년 UAE의 부통령이자 국방부 장관, 두바이 지도자인 Sheikh Mohammed bin Rashid Al Maktoum는 E-Security를 위하여 Dubai Centre를 설립하면서 Law No.11/2014을 공포함
- mGovernment Magazine에 의하면, Dubai Centre는 기업체이면서 법적 지위, 제정 및 행정 자율권을 가지고 있음
- Dubai Centre의 목적은 ▲두바이 내 정보, 네트워크 통신 및 정부의 정보 시스템 보호 ▲e-security에서 필요한 수단의 개발과 수정 ▲토후국 내의 모든 기관 사이에서의 정보를 교환하는 효율적인 방법에 대한 개발임

▶ UAE 통신규제청은 '사이버보안 국가 전략 2019'를 시행

- UAE 통신규제청은 2019년 6월, UAE 국가 사이버보안 전략(UAE National Cybersecurity Strategy)을 시행한다고 발표
- 시민들이 자신들의 목표를 달성하고 비즈니스가 번창할 수 있도록 UAE에 안전하고 탄력적인 사이버 인프라를 구축하는 것이 새로운 전략
- UAE 국가 사이버보안 전략은 사이버보안법 및 규정 강화, 기존 기술 및 신기술 보호, 중소기업 보호 지원 등 5개의 항목에 걸쳐 60개의 이니셔티브로 구성되어있음
- 학생들이 사이버보안 분야에 경력을 쌓는 것을 장려, 4만 명 이상의 전문가를 육성하는 것이 목표
- 국가 상 프로그램을 통해 우수한 사이버보안을 보상

2) 담당기관

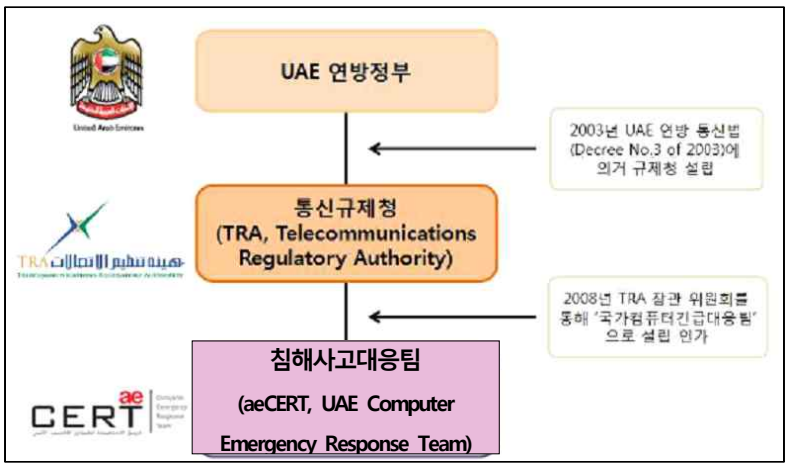
▶ 통신규제청(Telecommunications Regulatory Authority, TRA)

- TRA는 UAE Federal Law by Decree No. 3 of 2003 – Telecom Law에 기인하여 설립되었으며, 통신과 정부 기술 산업 모든 측면에 대한 관리를 책임 지고 있음
- TRA의 주요 역할은 ▲적합한 통신 서비스 보장 ▲서비스의 향상 달성 ▲양질의 서비스 보장 및 통신사업자들의 허가 조건 준수 보장 ▲통신사업과 IT 서비스의 향상 ▲통신사업자들 간의 분쟁 해결 ▲규제와 정책 프레임워크의 실행 ▲신기술의 프로모션 ▲UAE가 ICT 허브 역할을 하도록 함 ▲UAE의 인적 자원 개발 ▲R&D 장려 등임

▶ 침해사고대응팀(aeCERT)

- UAE 통신규제청(TRA)의 산하기관으로서 정보보호와 관련된 전반적인 업무를 수행
- aeCERT는 기관 목적에 따라 정보보안 품질서비스, 조사 분석, 사이버 공격 감시 및 대응 등 4개 영역에서 30여 개의 서비스를 제공함
- aeCERT의 주요 업무는 ▲네트워크 보안사고 처리 ▲사이버 보안 법률 강화 및 신규 법률 제정에 대한 조언 ▲정보보안 사고관리 및 디지털 포렌식에 대한 국립 전문 지식 체계 구축 ▲위협, 취약성 및 사이버 보안 사고에 대한 정보 제공 ▲국내 및 국제 CSIRITs 및 관련 기관과의 협조 요청 등임

그림 _ aeCERT 소속 계통 체계



[출처] aeCERT

▶ 국가전자보안청(National Electronic Security Authority, NESA)

- NESA는 사이버 보안에 대한 업무를 담당하는 UAE 연방 기관으로서, 국가 보안을 위하여 UAE 대법원 관할 하에서 운영됨
- NESA의 주요 목적은 UAE 내 사이버 보안의 진보 및 발전을 가능하도록 하는 국가 사이버 보안 전략을 정의하는 것으로서, UAE 내 사이버 보안에 대한 주의 및 협조적인 문화를 조성하고자 함
- NESA Compliance를 위한 주요 단계는 'UAE IA(Information Assurance) 표준'으로 알려진 UAE 사이버 보안 표준 프레임워크를 개발하는 것임
- NESA는 모든 중요한 국가 서비스들이 정부 조직에 의해 제공되는 정보 인프라 및 중요한 산업들을 보호하기 위하여 UAE IA 표준에 올라와 있는 사이버 보안 컨트롤을 실행하도록 함

▶ 두바이 전자보안센터(Dubai Electronic Security Center, DESC)

- 두바이 전자보안센터는 두바이 정부에 의해 2014년 6월 정부 정보 시스템과 통신 네트워크 보호를 위하여 설립됨(법령 No. 11 in 2014)
- DESC의 설립 목적은 사이버 보안 방법론을 개발하고, 두바이 내 모든 정부 기관들 사이에서 주고받는 정보들에 대한 보호 효율성을 높이기 위함
- DESC는 정부의 정보보안을 위한 두바이의 정책을 수립하고 실행하며, 사이버 보안을 보장하기 위한 기준을 수립하는 데 필요한 업무를 수행함
- DESC는 두바이 정부가 2017년 5월 발표한 '두바이 사이버 보안 전략'(Dubai Cyber Security Strategy) 추진 중추 기관 역할을 담당

3) 규제 및 인증제도

▶ UAE 자체적인 인증제도는 발달하지 않았으며, 선진국의 인증이 통용되고 있음

- UAE는 제조업 기반이 미미하여 인증제도가 발달하지 않았으며 대부분 제품을 수입에 의존하고 있어 선진국에서 발급해 주는 인증서를 취득했을 경우 UAE 수출에 도움이 될 수 있음
- CE(Confirmity European)는 유럽연합의 통합규격 강제인증제도로 유럽 내에서 유통되는 상품 중, 소비자의 건강, 안전, 위생 및 환경보호 차원에서 위험성이 내포되어 있다고 판단되는 제품에 적용하고 있음
- CE마킹은 해당 제품이 유럽연합과 유럽자유무역연합(EFTA)에 합법적으로 판매될 수 있음을 증명함

표 _ UAE 품목별 인증제도

품목	인증제도
전자 제품	CE(Confirmity European), US standards
전기, 기계류	UL, BS, TUV
의약품	USFDA, EU, GCC specs

[출처] 글로벌 전시 포털(www.sme-export.go.kr)

4) 최근 정책 동향 및 이슈

▶ UAE 통신규제청, 국가 사이버보안 전략 시행 (2019.6)[221]

- 2019년 6월 발표된 사이버보안 전략은 차후 3년간 60개의 이니셔티브를 실행하여 안전하고 탄력적인 사이버 인프라를 구축하는 것을 골자로 함
- 통신규제청은 50개가 넘는 국제 보고서와 사이버보안 시스템을 선도하는 10개의 국가를 참고하여 전략을 수립하였다고 밝혔으며, 사이버보안 강화 산업 분야로 통신산업, 건강 및 유틸리티, 에너지, 금융 등이 선정
- 통신규제청은 △사이버보안 프로그램을 진행, 장려하는 개인, 조직을 포상하며 △기업가들에게 사이버보안 혁신을 위한 영감을 주고 △학생들로 하여금 사이버보안 분야에 경력을 쌓도록 지원하고 동기를 부여하기 위하여 국가에서 수여하는 상 12개를 새로 신설, 연별로 수여할 예정
- 해당 전략의 성공적인 집행을 위하여, 통신규제청은 2개의 전략적 지표와 17개의 핵심 성과 지표를 통해 프로그램을 모니터링할 예정

표 _ UAE 국가사이버보안 5대 항목

UAE 국가사이버보안 전략 5대 항목
• 모든 종류의 사이버범죄에 대응, 기존 기술 및 신기술 보장, 중소기업을 사이버위협으로부터 보호하는 등의 모든 문제에 대응하는 법, 규제, 제도 마련
• 사이버보안 생태계 활성화
• UAE에서 사이버 사고가 발생할 경우 신속하게 대응할 수 있는 "국가 사이버 사고 대응 계획(National Cyber Incident Response Plan)" 수립
• 9개 부문의 UAE 중요 자산 보호(에너지, ICT, 정부, 전기 및 수도, 금융 및 보험, 긴급 서비스, 의료 서비스, 교통, 음식 및 농업)
• 지역 및 글로벌 협력(공공-민간-학계-국제 컨소시엄)을 통해 사이버 보안 목표 및 비전을 공동으로 달성

221 Gulf News, "UAE to roll out new laws to combat cybercrimes", 2019.6.24.

융합보안시장 및 정책 동향

1) 융합보안 시장 현황

핀테크

▶ 중동 및 북아프리카 지역의 핀테크 스타트업의 중심지에 해당[222]

- UAE에는 중동·북아프리카 지역(MENA지역)의 전체 핀테크 스타트업의 3분의 1이 몰려 있으며, 세계 10대 핀테크 허브에 해당
- 2015년 기준 559개사였던 이 지역 핀테크 스타트업은 2022년까지 1,845개에 달할 것으로 전망됨
- MENA지역에서는 2019년 10월 현재 총 354건에 517만 달러의 투자가 이루어졌고, 이 중 UAE는 62%의 비중을 차지하고 있음
- 대형 벤처 캐피탈의 투자가 이루어지는 곳이기도 하며, 총 시장 규모는 약 8조 달러에 이름
- Souq.com(중동지역 최초의 유니콘으로, 아마존에 인수), Careem(우버에 인수) 등이 큰 성공을 거두었으며, Fetchr, Property Finder 등도 이 지역에 기반을 둔 유망한 스타트업으로서 전망이 밝은 편[223]

블록체인

▶ 현재 UAE의 블록체인 시장 규모 및 발전 수준은 아직 낮은 단계이나 정부의 개방적 정책으로 인해 다양한 산업에서 빠르게 활용될 것으로 기대

- 제약 분야에 있어서, 세계적인 제약 회사인 화이자는 블록체인을 활용하여 대용량의 데이터를 보관·유지하고 있는데, 이러한 선진적인 해외 기술을 적극적으로 수용하여 자국의 산업에 적용[224]
- 블록체인 기술은 폐기물 처리 허가에도 사용될 전망으로, 함리야 자유무역지대(Hamriyah Free Zone Authority·HFZA)에서는 한 폐기물 처리사가 블록체인 플랫폼을 출시한 것을 활용할 예정
- 이 플랫폼을 통하여 폐기물 배출 승인 여부를 요청하게 되면 수일이 걸리던 기존의 시스템과 비교하여 획기적으로 프로세스를 줄이면서도 처리 결과 등을 효율적으로 저장할 수 있게 됨[225]

---

222 https://www.khaleejtimes.com/business/local/fintech-to-drive-uaes-growth-in-2020
223 https://www.zdnet.com/article/after-silicon-valley-snaps-up-souq-com-and-careem-four-tech-start-ups-in-the-middle-east-to-watch/
224 https://www.bioin.or.kr/InnoDS/data/upload/tech/6ff61026f4fe4a3799940d72cc8608c9.pdf p53 이하
225 https://news.v.daum.net/v/a5EN1AaM2w?f=p

2) 융합보안 정책 현황

▶ 두바이 자율주행 교통 전략(Dubai's Autonomous Transportation Strategy)(2016.4)[226]

- 두바이는 2030년까지 25%의 모든 교통수단을 자율주행화하여 연간 60억 달러의 경제적 비용을 절약한다는 내용이 담겨있는 '두바이 자율주행 교통 전략'을 발표
- '두바이 자율주행 교통 전략'의 일환으로 '두바이 세계 자율주행차량 도전'(Dubai World Autonomous Transportation Challenge)을 발표하였는데, 혁신적인 국제 기업, 교육 기관 및 연구소들의 최신 기술 개발을 독려하여 두바이에 현실적이고 적용 가능한 교통 솔루션을 제시하는 국제 제안요청서(RFP) 프로젝트
- '두바이 자율주행 교통 전략'은 △교통비용을 44% 절약 (연간 2억 달러를 절감) △환경오염을 12% 감소 (연간 4억 달러 절감) △운송수단의 효율성을 늘려 연간 49억 달러의 부가가치를 창출할 것으로 기대
- 그 외에도 △교통사고 사상자 수를 12% 감소 △개별 생산성 13% 증가 △교통 여행 시간을 연간 3.96억 시간 절약 △주차 할당 공간 감소 등을 전망
- '두바이 자율주행 교통 전략'의 주요 적용 분야는 자율주행 지하철, 버스, 택시이며, 4가지 주요 요소는 △개인(Individual) △기술(Technology) △입법 구조(Legislative Structure) △사회 기반시설(Infrastructure)
- (개인) '자율주행차량시스템 전문가 조직'(Centre of Excellence for Autonomous Transportation System)을 설립하여 자율주행 기술 분야의 전문가를 유치하고 국가 전문성을 구축
- 그 외, 지식 기반 컨텐츠(컨퍼런스·워크샵·출판물 등)를 보급하여 대중들에게 자율주행의 중요성에 대한 인식을 높이고 자율주행 이용을 장려하여 사고방식의 변화를 유도
- (기술) 현재와 미래의 교통수단에 자율 시스템을 적용하는 것뿐만 아니라 다양한 교통수단에 자율주행 기술 접목에 관해 연구
- UAE 내외부의 글로벌 기업, 연구개발센터 및 교육 기관과 협력하여 자율주행 시스템 분야의 연구개발 활동을 장려
- 자율주행과 직접적인 연관이 있는 기술 제공업체, 차량 제조업체, 운송 회사는 물론 간접적인 연관이 있는 보험 회사 및 기타 기관과의 글로벌 파트너십을 장려하는 것 또한 목표
- (입법 구조) 자율주행 기술 개발을 촉진하는 법률 도입 및 UAE에서 허용될 자율운송 수단 및 모델을 제시
- 자율주행 시스템에 관심이 있는 다른 글로벌 도시를 대상으로 국제 기준점 구현에 앞장서기 위한 자율주행 교통 정책 검토 및 강화
- (사회 기반시설) 미래의 표준이 될 자율주행 기술에 대비하여 인프라 구축 지원 및 기존 자율 주행 교통 시스템의 준비성 연구

---

226 Dubai Future Foundation, "Mohammed bin Rashid approves Dubai Autonomous Transportation Strategy", 2016.4.25

▶ UAE 정부, 블록체인 전략 2021 발표(2018.4)[227]

- UAE 정부는 블록체인 기술의 세계적인 리더가 되는 것을 비전으로 삼은 '블록체인 전략 2021'(Emirates Blockchain Strategy 2021)을 발표
- 2021년까지 연방 정부 상호작용의 50%를 블록체인 기술로 교체하는 것이 목표로, 전략이 성공할 경우 연간 △문서 작업 및 저장 비용 30억 달러 △7,700시간의 노동력 △16억 킬로미터의 주행거리 등을 절약할 수 있을 것으로 전망
- 블록체인 전략의 4가지 주요 요소는 △시민 및 거주민의 행복 △정부 효율성 △향상된 입법 △글로벌 기업가 정신이며, UAE 정부는 훈련 코스, 이벤트, 워크샵 및 보고서 등을 통해 블록체인에 대한 정부의 입장을 명확화하고 대학에 블록체인 연관 기술인 암호학 강의 등을 지원

▶ UAE 보건부, 블록체인 시스템 발표(2019.9)[228]

- UAE 보건부(Ministry of Health and Prevention, MoHAP)은 보건 데이터를 보관하고 공유하는 블록체인 시스템을 출시
- 보건부의 블록체인 솔루션은 2018년 4월 발표된 '에미리트 블록체인 전략 2021'의 일환
- UAE 보건부의 블록체인 플랫폼은 건강 전문가(의사, 약사, 기술자)들의 데이터 보관 및 공유를 용이하게 하며 기존 시스템에 비하여 데이터 무결성이 개선될 전망

스마트의료

▶ UAE 정부는 사물인터넷의 발달에 힘입어 원격 의료의 보급에 힘을 쏟고 있음

- 2015년 두바이 소재 하타(Hatta) 병원에 원격 진료로봇을 시범적으로 도입하여 의료 서비스를 제공
- 의사가 로봇에 달려 있는 장비를 이용해 환자를 진료할 수 있고, X-ray, 진단 결과 분석, 체온·맥박 등 환자의 상태를 파악 가능[229]

▶ 2017년 로봇이 처방약을 제조하는 스마트 약국 등장[230]

- 두바이 소재 라시드 병원(Rashid Hospital)에 생긴 로봇 약국으로, 바코드에 기반한 버튼을 클릭함으로써 로봇이 처방약을 제조하는 방식이며, 약사의 실수로 인한 처방약의 오제조를 대폭 줄이는 획기적인 발전
- 의사가 처방전을 발행하면 로봇이 바로 처리하는 시스템으로서, 전체적인 과정에 종이문서가 발생하지 않으며 제조 시간 단축이라는 부수적인 효과도 발생

227 Cointelegraph, "UAE Government Launches Blockchain Strategy 2021", 2018.4.13
228 Cointelegraph, "United Arab Emirates' Ministry of Health Launches Blockchain System", 2019.9.19
229 http://www.hkn24.com/news/articleView.html?idxno=148302
230 http://www.irobotnews.com/news/articleView.html?idxno=9664

- 보건당국(DHA)은 이 스마트 약국 시스템을 모든 병원으로 확대할 계획

▶ 2019년 두바이 소재 병원에 수술 로봇이 도입되어 성공적으로 수술에 이용[231]

- 두바이 소재 알 쿠웨이트 병원(Al-Kuwait Hospital)에서 첨단 수술 로봇을 이용하여 두 건의 수술을 성공적으로 마침
- 후두에 악성세포가 있는 환자와 혀 비대로 인한 수면무호흡증을 앓는 환자를 위한 수술로, 첨단 기술의 성공적인 활용으로 인해 의료진 및 병원의 경쟁력 향상 기대

231 https://dubaigazette.com/surgical-robot-employed-at-kuwait-hospital-in-dubai/

다. 카타르

'18년 GDP(십억달러)	192.01
'18년 인구수(천명)	2,780

■ ITU 글로벌 사이버보안 지수(Global Cybersecurity Index, GCI)

· 카타르의 사이버보안 지수는 전년 대비 순위가 8단계나 올랐으며, 한국과 비슷한 수준

국가명	2018		2017		전년대비 증감	
	지수	순위	지수	순위	지수	순위
카타르	0.860	17	0.676	25	+0.184	+8
대한민국	0.873	15	0.782	13	+0.091	-2

■ ICT 관련 주요 지수

· 카타르의 전반적인 ICT 발전 수준은 전 세계 중상위권을 유지

지표명	카타르		한국	
	점수	순위	점수	순위
IMD 국가경쟁력지수(2019)	-	10	-	28
IMD 디지털경쟁력지수(2019)	-	31	-	10
UNCTAD 전자상거래지수(2019)	74.2	47	89.4	19
ITU 글로벌 사이버보안 지수(GCI 2018)	0.860	17	0.873	15
UN 전자정부 지수(2018)	0.713	51	0.901	3

■ ICT 관련 주요 통계 (ITU, 2018년 말 기준)

· 카타르의 유선통신 보급률은 20% 미만이나, 이동통신은 140%가 넘는 상위권 수준

항목	카타르		한국	
	가입자수(천 명)	보급률(%)	가입자수(천 명)	보급률(%)
유선전화	452	16.25	25,907	50.63
유선브로드밴드	268	9.63	21,286	41.60
이동통신	3,946	141.86	66,356	129.67
인터넷 이용률	99.65%		95.90%	

정보보호 산업 개요

1) 보안 환경

▶ 2022년 카타르 도하 월드컵을 앞두고 사회전반에 걸친 인프라 개선이 진행 중이며 보안에 대한 요구와 위기의식도 고조

- 카타르 정부는 월드컵 개최를 위한 사회 인프라 개발에 박차를 가하고 있으며 이에 따른 투자는 최대 2,000억 달러에 이를 것으로 예상됨
- 이와 관련하여 CCTV 감시, 화재 패널, 통신 시스템과 같은 여러 기술이 현지 시장에 계속 제공되고 있으며, 물리, 통신보안 분야에 대한 수요가 증가하며 안전과 보안문제가 대두됨에 따라 관련 시설 및 서비스에 대한 수요 또한 증가할 것임
- 또한 최근 사이버 공격들로 인해 카타르 정부는 공격적이고 방어적인 사이버 역량을 강화하는데 중점을 두고 있으며, 2013년 국가 사이버 전략 수립 후 매년 국가 사이버 보안 훈련을 실시함[232]
- 이와 관련, 카타르 당국은 2006년에 설립된 '카타르 침해사고대응팀(Q-CERT)'운영을 통해 사이버 안전을 도모하며, 또한 내무부는 국가 안보 및 사이버 방위를 보장하기 위한 최선의 기술적·법적 접근 방식을 확인하고 시행하기 위해 사이버 보안위원회(Cyber Security Committee)를 설립함

▶ 높은 인터넷 이용률과 이동통신 보급률을 기록하고 디지털 전환이 진행되며, 사이버 보안이 중요한 사회 인프라 이슈로 대두

- ITU에 따르면 2018년 말 기준, 카타르 개인의 인터넷 이용률은 99.65%로, 인터넷 이용 기준으로는 세계 최고 수준을 기록
- 또한 2018년 이동통신 보급률은 141.86%로 완전한 보급을 넘어, 가입자당 1.4개의 회선을 이용할 정도로 ICT 인프라에서 이동통신의 비중이 높은 상황
- 2018년 모바일 브로드밴드 보급이 117%, 유선 브로드밴드 보급이 10%에 달하는 점을 감안할 때, 인터넷 접속의 상당 부분이 모바일로 이루어짐
- 중소기업 분야는 아직 IT 도입이 비교적 낮으나, 전자정부와 같은 일부 분야는 고도로 발달되어 있음
- 기업 부문에서는 클라우드 사용으로 전환하고 있으며, 창업 현장을 개발하려는 노력도 있음

▶ 2017년 6월 5일 사우디아라비아, UAE, 바레인, 이집트 정부는 카타르와 외교관계를 단절하고

232 Gulf International Forum, "The New Battlefront: Cyber Security Across the GCC", 2018.10.29. https://gulfif.org/the-new-battlefront-cyber-security-across-the-gcc/

사우디-카타르 국경을 폐쇄하고 카타르 등록 항공기의 공역을 폐쇄, 특정 해상 교통 제한 등을 포함한 일련의 경제 제한을 가했음[233]

- 이들 국가들은 카타르가 이슬람 급진 테러조직을 지원하며 안보를 불안하게 한다는 것을 단교 명분으로 내세움
- 이로 인해 육지와 바다 경계를 가로지르는 상품의 이동은 계속 영향을 받고 있고, 2019년 2월 초 Emirati 항만 당국은 카타르로 향하는 카타르 이외의 깃발이 있거나 소유된 선박이 상품을 운송할 수 있도록 허용했음
- 카타르는 이전 GCC 거래 파트너와의 손실을 상쇄하기 위해 터키, 오만, 쿠웨이트, 인도와 같은 지역 파트너와의 거래를 늘리며 새로운 공급업체에게 기회가 생김

▶ 인근 국가나 해외 국가의 사이버 공격 피해 사례가 증가하고, 이로 인한 국가적, 사회적 손실이 발생하면서 정보보안 수요가 증가할 가능성이 높음

- 이란, UAE 등 타 중동 국가들처럼 석유화학, 원전 등 주요 국가기반 산업인 에너지 분야가 해커들의 표적이 되고 있는 상황이며, 최근 몇 년 사이 에너지 외에 금융, 언론 등 기타 산업 분야에서도 사이버 공격이 가해지면서 정보보안의 위기 의식이 고조
- 실제 2017년 카타르 도하에 기반을 둔 Al Zazeera 미디어의 웹사이트와 디지털 플랫폼에 대한 체계적이고 지속적인 해킹시도, 2016년 카타르 국립은행(QNB)의 전산망이 해킹 당했고, 2013년에는 시리아의 사이버 군대가 카타르 재단의 소셜 미디어 계좌에 해킹을 시도하였고, 2012년에는 카타르 에너지 기업인 RasGas가 사이버 공격을 받았음
- 이에 따라 카타르는 에너지 및 금융 부문을 보호하고 사이버 안전과 관련된 인적 자원 및 사회 개발을 포함하는 'Qatar National Vision 2030'계획을 수립
- 또한 국가정보보안센터(National Information Security Center)를 통해 사이버 위협에 대한 모니터링 시스템을 개발하고 사이버 위협을 분석하고 탐지

▶ ITU가 2019년 3월 발표한 'Global Cybersecurity Index 2018'에 따르면 카타르의 사이버보안 지수는 0.86, 글로벌 순위는 17위로 성숙 상태에 해당하며, 아랍국가(Arab States)지역에서 사우디아라비아, 오만에 이어 3위를 기록

- 해당 지수는 법적·기술적·조직적 대응 및 역량강화, 국제협력 등 5개 부문의 지수를 종합한 것으로, 카타르는 법적 측면에서 0.193, 조직적 측면에서 0.192로 높은 점수를 기록하였으나, 국제협력 측면에서 0.151로 낮은 점수를 기록
- 카타르는 사이버보안문화 구축을 위한 캠페인을 실행하고, 언론 및 소셜 미디어를 통해 인터넷 사기와

233 U.S. Department of Commerce's International Trade Administration, Qatar - Market Overview, 2019.8.15. https://www.export.gov/article?id=Qatar-Market-Overview

같은 온라인 위협에 대한 경고를 확산하였음

- 또한 카타르 사이버 범죄수사센터 및 정보보안센터는 대중을 보호하고 사이버 범죄자들을 단속하기 위한 노력을 지원함

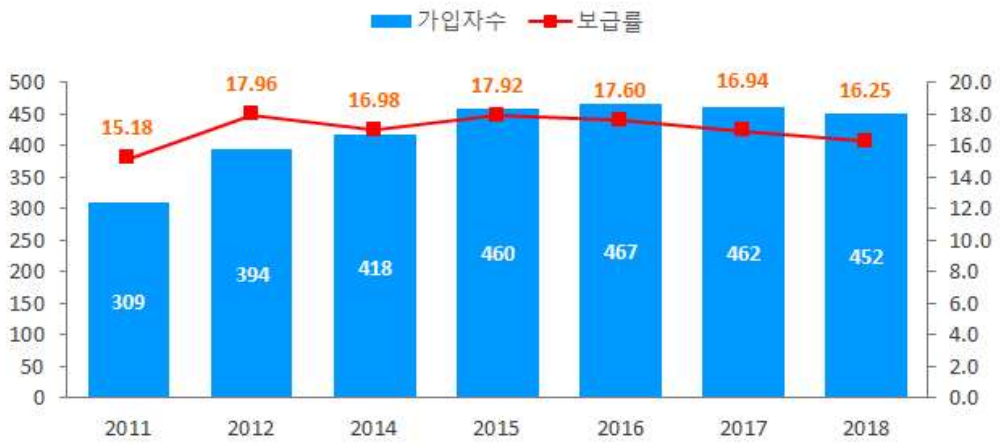
2) 인터넷 및 통신 환경

▶ 유선통신

- ITU에 의하면 2018년 말 기준, 유선통신 가입회선 수는 약 45만 회선을 기록, 보급률은 16.25%이며, 2017년 보급률 16.94% 대비 2.05% 감소함
- 카타르의 장기개발 계획 Qatar National Vision 2030에 따르면 QNBN(Qatar National Broadband Network)은 카타르 발전의 통로로서 지식 기반의 정보통신기술 경제 달성을 위해 최신 플랫폼 및 광통신 기반의 통신환경을 제공할 전망이며 성공적으로 진행 중임

그림 _ 카타르 유선통신 가입자 수 및 보급률 추이

(단위: 천 명, %)



[출처] ITU Statistics DB (2019.6)

- 1993년부터 유선 전화망은 디지털화가 완료되었으며 99%의 가정집은 유선 전화가 연결되어 있음
- 카타르에서의 유선시장은 경쟁 부족으로 Ooredoo가 지배적이며, 유선전화 가입 회선 수는 2016년 약 46만 7천 회선을 정점으로 이후 보급률과 함께 감소하는 추세임

▶ 이동통신

- ITU의 자료에 의하면 2018년 기준 이동통신 가입자 수는 2017년 대비 약 1% 감소한 394만 5천명으로 보급률은 141.38%였으며, 2015년 145.79%로 최고의 보급률을 기록하였고, 이후 140%~150% 사이의 보급률을 보이며 성숙된 시장의 상태를 보임
- 카타르의 이동통신 사업자는 Ooredoo와 Vodafone이며 MVNO사업자는 없으며, 이동통신 부문은 상당한 LTE 네트워크를 구축하면서 한동안 상당히 진행되었음
- Ooredoo는 2013년 4월에 상용 LTE 서비스를, 2015년 12월에는 상용 LTE-A 서비스를 시작하였고 2017년 말까지 약 15만명의 VoLTE 서비스 사용자가 있음
- Vodafone은 2014년에 LTE 4G 서비스를 시작했으며, 3G 네트워크를 계속 확장하고 있음
- BuddeComm 보고서에 의하면, 2017년 기준 3G 모바일 인프라 커버리지 인구비율은 99.7%, LTE의 경우는 99.5%에 해당하여 높은 수준의 4G LTE 인구범위로 5G로의 업그레이드 기회가 좋은 위치에 있는 것으로 전망[234]
- 카타르는 2019년 1월 Ooredoo와 Vodafone에게 3.5GHz 주파수로 5G 상용 라이선스를 발급했으며, 두 사업자 모두 5G 개발과 관련하여 상당히 적극적임
- Ooredoo는 에릭슨과 노키아와 같은 솔루션 제공업자와 파트너십을 맺어 특히 관심을 보였으며, 2018년 5월 3.5GHz 5G 네트워크를 켜고 수도 도하 주변에 50개 사이트를 배치하였다고 발표
- Vodafone은 5G 네트워크를 카타르 전역 약 50곳에 배치하기 시작했다고 발표했으며, 2018년 8월말까지 5G 네트워크를 개시하여 첫 번째 기업 고객을 연결했으며, 2019년 4월 GigaNet 5G 네트워크를 사용하여 5G 핸드셋으로 현지 및 국제 모바일 전화를 거는데 성공함
- 그러나 2019년 중반까지 5G 호환 장치를 사용할 수 있게 될 것으로 기대되지 않아, 두 사업자 모두 5G 대량 서비스를 제공할 수 없음
- BuddeComm 보고서에 의하면, 2018년 기준으로 Oredoo의 시장 점유율은 70%이며, 후발 통신사인 Vodafone은 30%를 차지하는 것으로 예측함[235]

234 BuddeComm, Qatar - Telecoms, Mobile and Broadband - Statistics and Analyses, 2019.4.22
235 BuddeComm, Qatar - Telecoms, Mobile and Broadband - Statistics and Analyses, 2019.4.22

그림 _ 카타르 이동통신 가입 및 보급률 추이

(단위: 천 명, %)



[출처] ITU Statistics DB (2018.6)

▶ 전자상거래 및 결제시장 전문 조사기관 yStats에 의하면 카타르는 중동지역에서 인터넷 사용률이 2017년 기준 쿠웨이트(98%)에 96%로 두 번째로 높으며 바레인(96%)과 같은 순위를 보임[236]

- 또한 카타르는 이 지역에서 모바일 인터넷 보급률이 2018년 6월 기준 UAE(84%)에 이어 83%로 두 번째로 높게 나타남
- 카타르에서 2019년 3월 기준 인터넷 트래픽 중 59.4%는 모바일 기기에서 발생했으며, 데스크톱은 38.7%이고, 태블릿이 1.9%로 나타남
- 카타르 개인 인터넷 사용률은 2011년 69%에서 2017년 96%로 성장했음
- 카타르에서 온라인 소매 판매는 2017년 13억 달러 규모에서 2020년 32억 달러에 달하여 연평균 성장률 19.7%로 성장할 것으로 예측
- 카타르에서 아마존 사이트(amazon.com)가 2019년 3월 기준 가장 많이 방문하는 쇼핑 웹사이트이자 10번째로 많이 방문한 웹사이트로 나타났으며, 2번째 순위 쇼핑 웹사이트는 Aliexpress.com이고, eBay.com가 뒤를 이으며, 카타르 국내 기업인 Mzadqatar.com이 4번째 순위로 나타남

▶ 금융 부문의 디지털 전환에 많은 투자[237]

- 카타르는 핀테크 혁명을 신속히 받아들이며, 디지털 기술이 금융부문 경쟁력과 보안을 동시에 높일 수 있다고 인식함
- 은행은 스마트 카타르 프로그램(Smart Qatar Program) 또는 TASMU와 같은 국가 핀테크

236 "Global E-Commerce Intelligence, MENA B2C E-Commerce Market 2019", yStats, 2019.6.
237 "The Report Qatar 2017", Oxford Business Group, 2018.10.2.

이니셔티브를 지지하며, 디지털 전환에 많은 투자를 함

- 예를 들어 카타르 전자지불시스템 공급업체인 QPAY는 2014년 출시 이후 2017년 11월까지 연간 300%의 성장률을 보였으며, 2017년 11월 기준 약 10,000개의 사업체와 28만 명의 소비자를 지원

▶ 인터넷 이용 환경

- ITU의 자료에 따르면 카타르의 인터넷 이용자 보급률은 2018년 99.65%로 전년의 97.39%에서 2.26% 증가하였으며, 2013년 직전년 대비 16% 크게 증가 후 꾸준히 증가 추세를 보임
- 브로드밴드는 대부분의 인터넷 연결을 나타내며, DSL, FTTH, 무선, 모바일을 통해서도 사용가능함
- 이동통신 사업자 Ooredoo와 Vodafone은 3G 또는 4G LTE 네트워크로 지원되는 모바일 브로드밴드 서비스를 제공하고 있으며, 모바일 브로드밴드는 브로드밴드 서비스를 제공하는 주요 플랫폼에 해당
- BuddeComm의 자료에 의하면 2017년 전체 인구에 대한 모바일 브로드밴드 보급률은 117%인 반면, 유선브로드밴드 보급률은 10%로 모바일 브로드밴드 사용이 월등히 많음을 알 수 있음
- MoTC에 의하면, 또한 스마트폰 보급률은 2015년 약 75%에서 2018년에는 약 95%로 추정됨

표 _ 카타르의 브로드밴드 보급률(2017년 기준)

구분	이용자 수	보급률
모바일 브로드밴드	3,090,000	117%
유선 브로드밴드	256,000	10%
전체	**3,346,000**	-

[출처] BuddeComm(2019.4.)

그림 _ 카타르의 인터넷 보급률



[출처] ITU Statistics DB(2019.6)

정보보호 시장 현황

1) 시장 규모

시장 개요

▶ MarketsandMarkets의 최근 중동 지역 사이버 보안시장 보고서[238]에 의하면, 카타르는 이 지역에서 가장 높은 비율로 성장할 것으로 전망

- 카타르에서 사이버 보안 솔루션으로 전환하고 있는 중소기업이 비즈니스의 엔드포인트, 네트워크, 애플리케이션, 클라우드 환경을 효율적으로 보호하고자 하기 때문에, 사이버 보안 시장 측면에서 잠재적 성장 기회를 보유한 것으로 평가

▶ 카타르 교통통신부는 2018년 9월 현지 언론에서 카타르의 ICT 부문이 2017년 약 39억 달러로 추정되며, 2021년에 약 44억 달러로 연평균 2.3% 성장할 것으로 전망한다고 발표[239]

- 또한 ICT 부문이 2017년 GDP의 2.7% 기여했다고 함

▶ 시장전문업체 IDC는 2021년까지 카타르의 소프트웨어 시장이 약 15억 5천만 QR(약 4억 2,560 USD)[240], IT 서비스 시장은 10억 QR(약 2억 7천만 USD) 이상, 인프라 시장은 8억 QR(약 2억 2천 USD)이상에 도달할 것으로 전망함[241]

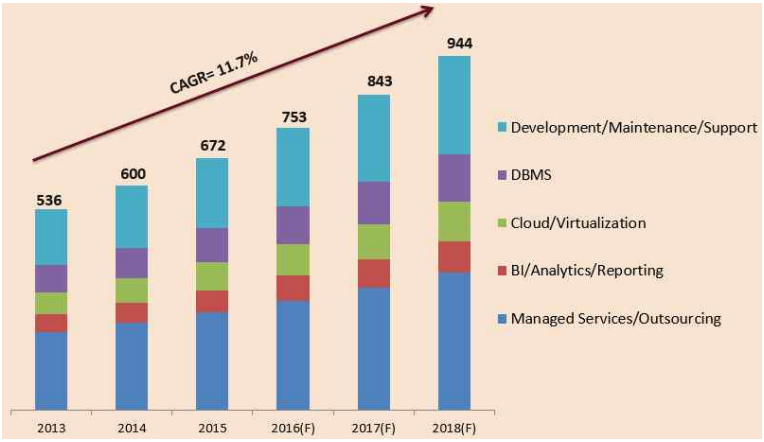
▶ Fujitsu의 중동 시장 보고서에 의하면, 카타르 IT 서비스 시장 규모는 2013년 5.36억 달러였으며, 2018년 9.44억 달러로 연평균 11.7%의 성장 전망치를 내 놓은 바 있음[242]

---

238 MarketsandMarkets, "Middle East Cyber Security Market worth 22.14 Billion USD by 2022", 2018.3.
239 The Peninsula, Qatar's ICT market likely to reach $4.4bn in 2021, 2018.9.5.
240 2019년 8월 30일 기준 1QR = 0.27 USD 로 계산
241 The Peninsula, Qatar's ICT market likely to reach $4.4bn in 2021, 2018.9.5.
242 Mukul Naskar, "IT Market in Qatar", 2015.9

그림 _ 2013~2018년 카타르 IT 서비스 시장 성장 추이 및 성장률

(단위 : 백만 달러)



[출처] Mukul Naskar,'IT Market in Qatar', 2015.9

▶ 카타르 IT 소프트웨어 및 하드웨어 시장 규모는 2014년 총 8.26억 달러 규모로 추정

- IT 하드웨어 시장 규모는 2014년 5.97억 달러에서 2019년 7.06억 달러로 연평균 3.4% 성장하고, 소프트웨어 시장은 2014년 2.29억 달러에서 2019년 3.43억 달러로 연평균 8.4% 성장할 것으로 예상
- 하드웨어 판매는 주로 태블릿PC 판매 증가가 원인이며, 소프트웨어 시장은 기업의 소프트웨어 도입에 따른 판매 증가가 시장 성장의 요인으로 분석

그림 _ 2014~2019년 카타르 IT 하드웨어/소프트웨어 시장 규모 추이

(단위 : 백만 달러)



[출처] Mukul Naskar,'IT Market in Qatar', 2015.9

정보보호 시장 규모 및 성장률

▶ 시장조사기관 Barnes Reports의 보고서에 의하면, 2017년 카타르의 보안 시스템 서비스 산업[243] 시장 규모는 약 2억 8,500만 달러에 달하며, 전년 2억 6,500만 달러 대비 7.5% 성장

- 보안 시스템의 세부 항목으로는 보안 시스템 서비스, 도둑 경보 관리 및 모니터링, 화재 경보 관리 및 모니터링 관련, 보호 장치와 보안, 감시 시스템 등이 포함됨
- 2018년에는 보안 시스템 서비스 산업 시장 규모가 전년 대비 17.7% 감소해 약 2억 3,400만 달러에 이를 것으로 전망
- 2017년 보안 시스템 서비스 산업 내 총 373개 기업이 설립되어 약 1,812명을 고용, 2018년에는 19.4% 증가하여 총 설립된 기업수가 445개에 이르고, 고용증가는 19.4% 증가하여 약 2,162명을 고용하는 것으로 전망
- 세부적으로 2018년에는 ▲보안 시스템 서비스 1억 9,090만 달러 ▲도둑 경보 관리 및 모니터링 관련 9,450만 달러 ▲보호 및 보안 장치 1,320만 달러 ▲감시 시스템 750만 달러 ▲화재 경보 및 감시 관련 670만 달러 규모로 시장이 형성될 것으로 전망

▶ 방위 및 보안 시장 전문 조사기관 SDI의 'Qatar Defense Spends on Homeland Security: 2016 to 2025' 보고서에 의하면 2016년 카타르의 물리보안과 네트워크 보안을 합친, 주요 기반시설 정보보호 시장(Critical Infrastructure Protection Market) 규모는 6.75억 달러인 것으로 집계

- 2017년 주요 기반시설 정보보호시장은 물리 보안 5.2억 달러, 네트워크 보안 1.2억 달러, 기타 분야 4천만 달러로 총 6.86억 달러에 달하면서 전체적으로 1.6%의 매우 완만한 성장이 예상
- 2016~2018년 시장 추세에서 물리보안 시장의 전년 대비 성장률은 2017년 1.55%, 2018년 2.29%에 그칠 전망
- 이에 반해 네트워크 보안 분야는 2017년 9.17%, 2018년 7.56% 성장하면서 물리 보안 대비 빠른 성장을 실현하고, 전체 정보보호 시장의 성장을 주도
- 이와 관련, 물리보안 분야는 사람이 직접 운영·개입하여 주요기반시설의 보안과 보호를 위한 모든 요소에 대한 투자를 의미
- 네트워크 보안 분야는 네트워크 보안, 데이터 보안, 클라우드 보안, 웹 기반 ID 및 액세스 관리, 보안 통신, SCADA 보안 등이 주로 포함

▶ 기술 분야 전문시장 조사기관 TechSci Research의 조사[244]에 의하면 카타르에서 CCTV 시장은

243 보안 시스템 서비스, 도둑 경보 관리 및 모니터링, 보호 및 보안 장치, 감시 시스템, 화재 경보 및 감시 등 보안 감시 서비스로 구성

2016년~2021년 동안 연평균 14%이상 성장할 것으로 전망

- 증가하는 건설 활동 및 소매점(retail malls) 및 호텔 체인의 확장과 함께 정부 지출의 증가가 카타르에서 CCTV 판매 추진의 동력으로 작용

시장 전망

▶ 시장조사기관 Research And Market의 보고서에 의하면[245], 카타르의 관리형 보안(Managed Security) 시장은 2018년~2024년 동안 연평균성장률 47.8% 이상으로 상당한 성장을 보일 것으로 전망

- 에너지, 은행, 금융 서비스 및 보험(BFSI)과 같은 여러 부문에서 사이버 공격이 증가함에 따라 카타르의 첨단 사이버 보안 시스템에 대한 수요가 증가함
- 또한 2017년 사우디아라비아, 바레인, UAE, 이집트에 의한 봉쇄 후 카타르는 국가의 디지털 인프라를 강화하려는 정부의 노력과 함께 사이버 보안의 필요성에 대한 인식이 높아짐에 따라 향후 몇 년간 카타르 관리 보안 서비스 시장의 성장은 활발해 질것으로 전망
- SAMM(Security Asset Monitoring Management) 서비스 유형은 카타르에서 관리형 보안 서비스의 성장에 가장 기여했으며, 카타르의 건설 시장이 빠르게 성장함에 따라 다양한 인프라 및 장치에 대한 관리 요구가 증가할 것이며 이는 SAMM 서비스의 점유율을 더욱 높일 것임

▶ 미국 국제무역국 자료에 의하면,[246] 2022년 월드컵에 대한 보안 요구사항과 최근 사이버 공격, 증가하는 네트워크 전쟁위협에 직면한 국가 사이버 방위 인프라 개선의지로 인해 다음과 같은 하위 부문에 높은 수요가 있을 것으로 전망함

- CCTV 감시 및 접근 제어, 사이버 보안, 통합 보안 시스템, 빌딩 관리 시스템, 침입 탐지 장비, 스포츠 안전 및 보안, 전자 안전 및 화재 감지, 통신 시스템 등

▶ SDI 보고서에 의하면, 카타르 기반시설 정보보호 시장은 2025년까지 연간 1.58%의 완만하지만 꾸준한 성장세를 나타낼 것으로 전망

---

244 TechSci Research, "Qatar cctv market forecast 2021 – brochure", 2016.7.7.
245 Research And Markets, Qatar Managed Security Services Market 2018-2024: Market Forecast by Service Types, Sectors, Regions, and Competitive Landscape, 2019.1.
246 U.S. Department of Commerce's International Trade Administration, Qatar - Safety and Security Equipment, 2019.8.15. https://www.export.gov/article?id=Qatar-Market-Overview

표 _ 카타르 주요 기반시설 정보보호 시장 현황 및 전망(2016~2025)

(단위: 백만 달러)

연도	물리보안	네트워크 보안	기타	합계	성장률
2016	516.04	109.00	40.00	675.04	-
2017	524.04	119.00	43.00	686.04	1.6%
2018	536.04	128.00	46.00	710.04	3.5%
2019	505.04	128.00	40.00	673.04	-5.2%
2020	515.04	138.00	41.00	694.04	3.1%
2021	505.44	135.00	37.00	677.44	-2.4%
2022	521.44	144.00	40.00	705.44	4.1%
2023	536.44	158.00	43.00	737.44	4.5%
2024	564.04	166.35	46.00	776.39	5.3%
2025	576.04	161.00	40.00	777.04	0.1%
CAGR 2016~2025					1.58%

[출처] SDI, 'Qatar Defense Spends on Homeland Security: 2016 to 2025', 2016.10

- 구체적으로는 2025년 물리보안 시장은 5.76억 달러, 네트워크 보안 시장은 1.6억 달러, 기타 분야는 4,000만 달러를 형성할 것으로 전망
- 특히 네트워크 보안 시장은 2025년까지 연평균 4.43% 성장하는 반면, 물리보안 시장은 1.23%로 성장하는데 그칠 전망
- 이 같은 측면에서 2025년까지 카타르의 주요 기반시설 정보보호 시장 성장률(연평균 1.28%)은 물리보안 시장보다는 네트워크 보안 분야가 주도할 것으로 예상
- 특히 도하 월드컵 개최연도인 2022년에는 물리보안 지출이 3.17%, 네트워크 보안 지출이 6.67% 성장하면서, 보안 분야의 대대적인 수요 확대가 전개될 것으로 관측

2) 분야별 현황

물리보안 제품 및 서비스

▶ CCTV 관련 수요가 증가하고 있음

- 카타르의 외국인 노동자 증가에 따라 범죄율이 증가하며 상업지구와 쇼핑몰 주변에 설치할 CCTV에

대한 수요가 증가하고 있음

- 카타르 정부는 도로 교통 제어를 위해 CCTV 설비를 강화했으며 33개 주요 교차로에 카메라를 설치함
- 이로 인해 교통량을 제어하고 교통법규 위반 단속이 가능하게 되었으며 추가로 15개 교차로에 시설 확충이 예정되어 있음
- 2022년 FIFA 월드컵 개최 예정으로, 2021년까지 11개의 경기장을 건설이 완료될 예정이며, 관련 CCTV 수요도 증가할 것으로 전망
- 2012년 카타르 정부는 정부 통관이 필요한 모든 프로젝트에서 IP카메라 사용지침을 발표하였는데, 이 지침은 보안 통제실, 은행, 환전소, 금 판매소, 위험물 및 귀중품의 창고 및 개인 상점, 병원 및 진료소, 호텔, 아파트 및 주거 단지, 쇼핑 및 엔터테인먼트 센터에 적용될 수 있으며, IP CCTV 채택의 증가가 예상됨

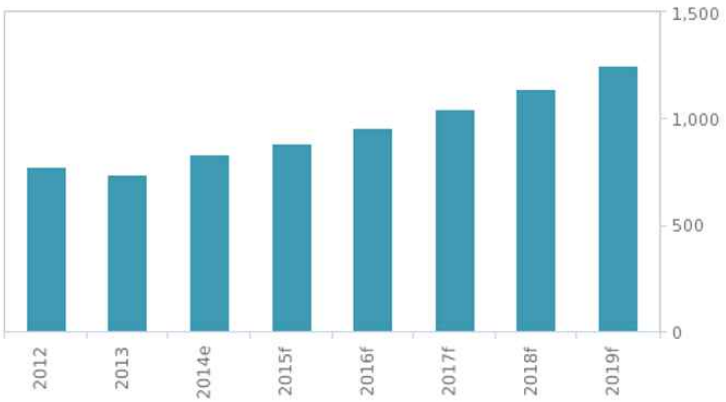
정보보안 제품 및 서비스

▶ 잇따른 해킹 공격으로 보안 소프트웨어에 대한 수요가 증가하며 소프트웨어 시장의 성장세가 예상됨

- 시장조사기관 BMI에 따르면 소프트웨어 시장은 2014년부터 2019년까지 연평균 14%의 성장률을 기록할 것으로 예상됨
- 정부의 IT 인프라 구축사업과 기업용 소프트웨어 판매가 성장세를 주도할 전망
- 특히, 카타르 정부는 2022년 월드컵을 대비해 비즈니스 인텔리전스, 대시보드, 금융 분야 관련 전망, 예산책정, 이벤트 관리 등 다양한 분야에서 최신 프로그램 도입을 추진함
- 카타르 정보통신부는 아랍어 소프트웨어 개발에 투자를 계획 중임
- 중소기업이 소프트웨어 시장의 34%를 점유하고 있으며 효율을 극대화하고 고객의 요구를 충족하기 위해 애플리케이션의 간소화를 진행 중임

그림 _ 2012~2019년 카타르 소프트웨어시장 판매 현황 및 전망

(단위: 백만 리얄)



[출처] BMI research(2015)

3) 주요 사업자 현황

시장 특성 및 경쟁 강도

▶ 카타르 보안 서비스 시장의 경쟁강도는 주변 GCC 국가들과 비교해 비교적 낮은 편

- 최근 보안 서비스 시장 성장세로 인해 주변국들과 국제 기업들의 진출이 늘어나고 있음
- 현재까지는 각 분야에 두각을 나타내는 기업이 없고 경쟁이 심하지 않은 상황임
- GCC 5개국 중 카타르의 경쟁강도는 중간 수준으로 평가받았으며 이는 오만과 함께 5개국 중 가장 낮은 경쟁강도를 보여줌
- GCC 5개국 중 시장규모는 작지만 성장률과 정치적 안정성이 높으며 낮은 경쟁강도를 고려하였을 때 시장매력도는 높은 편으로 평가됨

▶ 카타르 현지 보안업체들은 비디오 감시, 전자 제어 시스템, IT 보안 솔루션, 물리보안 등 다양한 영역에서 서비스를 제공하고 있으며, 해외 보안업체 중 가장 두각을 나타내는 업체는 세계 최대의 경비업체 G4S를 꼽을 수 있음

▶ 카타르 CCTV시장에서 활동하는 주요업체로는 Pelco, Hikvision Digital Technology, Axis

Communications AB, Dahua Technology Middle East FZE, Honeywell 등이 있음

- 카타르에서 전자보안제품을 제공하는데 관여하는 모든 주요 기업은 관련 딜러 및 유통네트워크를 통해 운영됨

주요 사업자

▶ Bin Arbaid Group

- 건설기술, 이송, 무역과 함께 카타르 내에서 물리보안 서비스를 제공 중인 업체임
- 접근제어로 출입제어 게이트, 차량 주차 및 확인, 화재감시등의 서비스를 휴대폰, 순찰 차량, 무선장비 등으로 정보 제공

▶ Ooredoo

- 대표적인 카타르 종합 통신 사업자로 카타르 정부가 지분의 일부(68%)를 가지고 있으며 본사는 도하에 위치함
- 유선, 무선, 이동통신 등 다방면에 서비스를 제공 중임
- 카타르, 쿠웨이트, 미얀마, 오만 등 중동국가와 아시아, 유럽 일부지역에서 서비스를 제공 중이며 2015년 9월 기준 약 1억 1,400만 명의 가입자를 보유한 글로벌 기업임
- 사이버 공격에 대비한 웹, 이메일, 모바일 등 전역에 걸친 클라우드 보안 서비스를 제공 중

▶ Informatica Qatar

- 인포매티카 카타르(iQTM)는 기술 솔루션, 장비 제공 업체이며 시스템 통합 솔루션을 제공하는 IT 컨설팅 제공 업체임
- 네트워크, 시각 및 청각 시스템, 기업 IT솔루션, 물리보안 등의 프로젝트를 진행 중임

▶ Teyseer Security Service

- 카타르 보안 산업의 선구자로 1994년 카타르에서 첫 서비스 제공을 시작함
- 시설 경비, 제어, 교통, 군중 제어, CCTV 시스템 관리 등 물리보안 서비스를 기업, 병원, 자원시설, 유통업체 등에 제공 중임

표 _ 카타르에 상주 중인 보안서비스 관련 해외 및 다국적 기업

기업명	활동분야	국적
Arecont Vision	IP네트워킹, CCTV	다국적
AxxonSoft	소프트웨어	다국적
LILIN	CCTV	다국적
MOBOTIX AG	CCTV	다국적
Sony Professional Solutions Europe	CCTV	다국적
TDSi	접근제어	영국
Vicon Industries	CCTV	다국적
Avigilon Corporation	CCTV	다국적
Bosch Security Systems	CCTV	다국적
Dallmeier electronic GmbH & Co.KG	CCTV	다국적
GEUTEBRUCK GmbH	CCTV	독일
HID Global	접근제어	다국적
Milestone Systems	소프트웨어 개발	다국적
Surveon Technology Inc	IP네트워킹	미국
Vanderbilt Industries	접근제어	다국적
VIVOTEK	IP네트워킹	다국적
G4S	경비업체	영국

[출처] www.sourcesecurity.com

4) 주요 동향 및 이슈

▶ 카타르 중앙은행은 전용 사이버 보안 기능을 설정(2019년 8월)[247]

- 금융기관에 대한 사이버 공격의 출현과 시스템의 재무 안정성에 대한 위협에 대해, 이 기능의 설정을 통해 금융기관을 안내하고 잠재적인 위협으로부터 기본 정보 인프라를 보호하는데 도움이 되고, 높은 수준의 사이버 복원력을 유지할 수 있음
- 카타르 중앙은행은 이 기능이 사이버 보안의 6가지 주요 영역인 거버넌스., 위협 정보, 보안 운영, 보안 아키텍처, 위험 관리, 사이버 보안 기능 개발 중에서 거버넌스 구성요소부터 시작하여 사이버 보안 프로그램의 기본 요소 개발에 중점을 두고 있다고 밝힘

247 Gulf Times, "QCB's cyber security program provides Qatar's financial sector with 'unique visibility' on cyber risks, threats'", 2019.8.3.

- 카타르 중앙은행에 따르면, 이 포괄적인 사이버 보안 프로그램은 사이버 위험과 위협 행위자에 대한 '고유한 가시성'을 제공할 것임

▶ 카타르의 민간 항공국은 '항공 사이버 보안 가이드라인' 발표(2019년 6월)[248]

- 카타르의 민간 항공국(Civil Aviation Authority, CAA)는 교통통신부의 사이버 보안 업무 부문과 협력하여 '항공 사이버 보안 가이드라인' 버전 1을 발표하였음
- 이 가이드라인에는 해당 분야의 전자 보안 모범 사례 외에도 중요 항공 시스템 보안과 관련된 표준 및 원칙이 포함
- 이 가이드라인을 통해 민간 항공 산업의 전자 위협 및 공격에 직면하고 완화하기 위해 표준의 배포에 초점을 맞춤

▶ 카타르 중앙은행은 사이버 위협에 대한 준비 강화(2018년 10월)[249]

- 카타르 중앙은행 총재는 카타르 중앙은행이 사이버 공격이나 해킹 문제를 해결하기 위해 IT부서에 필요한 보안 정책과 절차를 개발하고 구현하는 정보보안부서를 보유하고 있다고 설명함
- 또한 중앙은행의 네트워크를 보호하기 위한 보안기록을 모니터링하고, 정보 보안사건에 대응하여 사이버 공격에 대응하고 확인 하는 팀을 구성함
- 총재는 중앙은행의 보안 장비가 수많은 사이버 공격과 지속적인 해킹 시도를 처리했다고 언급함

5) 정보보호 스타트업 시장 현황

주요사업자

▶ QChain은 카타르에 기반을 둔 블록체인 기술 스타트업으로 규정준수 및 사이버 보안에 대한 새로운 솔루션을 구축함[250]

- Qchain은 카타르와 국제적으로 광범위한 사이버 보안 경험을 갖고 있으며, 사이버 보안 복원력을 높이고 포렌식 목적을 위해 무결성이 보장되는 사이버 보안 로그 세트를 제공함

주요 동향 및 이슈

▶ 2017년 주변국들과의 외교 단절은 스타트업과 중소기업에게 확장 기회 제공[251]

---

248 Gulf Times, "Qatar first in Middle East to launch 'Aviation Cyber Security Guidelines'", 2019.6.18.
249 Gulf Times, "Banking system in Qatar 'capable of facing risks'", 2018.10.21.
250 Qchain 홈페이지 https://qcha.in/
251 The Peninsula, SMEs seize expansion opportunities from blockade

- 사이버 보안 시장의 큰 업체들 사이에서 소규모 스타트업 회사를 운영하는 것은 유리한 환경은 아니지만, 블록체인, 인공지능, 클라우드 기술 등과 같은 혁신 기술을 활용하여 기회 모색
- 또한 주변국과의 외교 단절은 오히려 긍정적으로 작용하여, 자사 제품을 통하여 소비자의 신뢰가 구축되었으며 제품 및 서비스에 대한 수요가 지속 증가함
- 스타트업의 경우 한정적인 역량으로 인해 대규모 프로젝트를 수주하는 것은 어려운 일이나. 카타르의 다양한 부문에서의 움직임으로 새로운 기회가 열려 QChain과 같은 스타트업은 석유 부문과 같이 카타르의 대규모 프로젝트에 참여할 수 있게 됨

정보보호 정책 및 기관 현황

1) 관련 법령 및 정책

관련 법령 및 규제

▶ 사이버 범죄 예방법(Cybercrime Prevention Law)

- 카타르 국왕은 2014년 9월 사회적 가치나 보편적 질서를 해칠 수 있다고 생각되는 온라인 콘텐츠를 제작하거나 공유한 자를 처벌할 수 있는 법안을 승인함
- 국가의 안전과 질서를 해칠 목적으로 거짓정보를 퍼뜨리기 위한 웹사이트를 개설 및 운영, 방송, 출반을 할 경우 처벌할 수 있음

▶ 상업 등록법(Commercial Registry Law No.25/2005)

- 국내 및 외국회사 모두 법인설립을 위해서 당국 비즈니스 무역 및 사업부서(Ministry of Business and Trade 이하 MOBT)로부터 상업적 허가를 받아야함
- MOBT로부터 유지되는 허가를 받지 않은 모든 개인 및 단일 단체는 상업적 활동을 할 수 없음
- 등록 절차에 관한 모든 문의는 MOBT의 상업 담당 이사가 직접 담당함

▶ 전자상거래법(e-commerce law)

- 2010년 8월 제정된 전자상거래법은 법적으로 집행 가능한 온라인 커뮤니케이션 및 금융거래를 하며, 디지털 서명, 전자 문서, 지불 인증을 위한 프로토콜을 설정함

▶ 개인정보 보호 관련(Privacy concerns)[252]

- 카타르 법에 따르면 감시 카메라는 주거 시설, 병원, 쇼핑몰, 호텔을 포함한 대부분의 공공시설에 설치해야 함
- 내무부는 이 영상을 받아서 보안 및 조사 목적으로 저장하며, 결과적으로 내무부는 감시 카메라를 통해 대부분의 방문자와 주민을 모니터링함
- 카타르 정부는 또한 입국항에서 생체 데이터를 수집함

---

252 U.S. Overseas Security Advisory Council(OSAC), "Qatar 2019 Crime & Safety Report", 2019.2.26.

주요 전략 및 정책

▶ NCSS (Qatar National Cyber Security Strategy)

- 2014년 ictQATAR와 카타르 사이버보안위원회(NCSC)는 2018년까지 국가 사이버 보안의 발전을 위한 사이버 보안 전략을 발표함
- 국가사이버 보안전략(NCSS)은 4년마다 개정될 예정으로, 국내외의 법령, 기술, 운영 측면을 중심으로 전략 내용을 수정, 개선하게 될 것임
- 주요 목표는 5가지이며 다음과 같음
  - ·국가 주요기반시설 보호
  - ·사이버 공격에 대응하며 여러 기관과 정보를 공유·협업해 공격 복구
  - ·안전한 사이버 환경 조성을 위한 법제와 규제 구축
  - ·적절하고 안전한 사이버 공간을 위한 사이버 안전 문화를 육성
  - ·국가의 사이버 안전 역량의 개발과 강화

▶ Qatar National Vision 2030

- 2008년 발표된 카타르의 개발 프로젝트로 경제, 사회, 개인, 환경의 분야에서 각각의 발전을 도모하는 장기 개발 계획임
- Qatar National Vision 2030의 주된 계획은 카타르의 지속가능한 개발을 위한 사회의 역량 강화로 지식경제의 창출과 개발을 통한 목표 달성
- 이 계획을 뒷받침하는 프로젝트는 에너지, 재정 영역의 보안뿐 아니라 사이버 보안과 관련된 인구 사회적 발전을 포함함

▶ 카타르 전자정부 시스템 - eGovernment 포털 Hukoomi 도입 (www.hukoomi.qa)

- 카타르의 전자정부 시스템 Hukoomi의 주된 역할은 카타르의 거주자, 시민, 사업가등의 방문자들이 사회 정보에 쉽게 접근할 수 있게 하고 정보제공 서비스를 보다 효율적으로 제공하는 것
- 2003년 국왕의 감독 하에 전자정부 홈페이지가 개설된 이후 2008년 전자정부의 통합 프로그램과 동시에 Hukoomi(www.hukoomi.qa) 서비스가 시작
- 2017년 말 현재 약 20만 명의 사용자를 보유하고 있으며 232개의 기관에서 1,100여 가지의 서비스를 제공하고 있음

▶ 스마트 카타르 프로그램(Smart Qatar Program)

- 2017년 3월 시작된 스마트 카타르 프로그램(Smart Qatar Program)은 경제를 위한 수익을 창출하고

특히 스타트업 현장에서 일자리 창출을 촉진하는 것을 목표로 함

- ICT중소기업의 발전이 이 프로그램의 임무의 중요한 요소로, 카타르의 새로운 50개 기업에 대한 재정 지원을 통해 ICT분야의 일자리를 연간 10% 확대할 계획임
- 카타르 교통통신부(MoTC)는 개방형 데이터, 빅데이터 분석 및 스마트시티를 위한 사물인터넷에 대한 다양한 스타트업 개발 및 연구 프로젝트 분야에서 베이징의 국제 스마트 시티 연구센터, 화웨이, 에스토니아의 전자정부 아카데미와 일련의 양해각서에 서명함

2) 담당기관

▶ 교통통신부(Ministry of Transport and Communications, MoTC)

- 카타르 교통통신부는 교통 부문과 ICT 부문을 아우르는 주무부처로서 2016년 1월 27일, 국왕령에 의한 정부 부처 조직 개편으로 탄생
- 카타르의 기존 ICT 분야 주무부처는 2013년 개편 시 조직된 ictQATAR였으며, ictQATAR는 지식경제사회 구축을 위해 국가개발 계획으로 National ICT Plan 2015, National Vision 2030, National Development Strategy 2011-2016를 제시하고 실행함은 물론 국가 사이버보안 전략, 정책, 로드맵 이행에 대한 책임을 갖는 기관이었음
- 신설 교통통신부가 ictQARTAR를 완전하게 흡수함에 따라 국가 사이버보안 전략 수립 및 정책 로드맵 추진 역할도 교통통신부가 담당하게 됨

▶ 카타르 침해사고대응팀(Q-CERT)

- 2006년에 설립된 카타르 침해사고대응팀(Qatar Computer Emergency Response Team, Q-CERT)은 카타르의 인터넷 보안을 위해 전체 국가전략 수립에 중요한 역할을 하는 기관임
- Q-CERT의 주된 목표는 다음과 같음
  - ·대중과 공용 또는 개인기관에 사이버 안전에 대한 인식 제고
  - ·사회에 정보통신기술 보안에 발을 들이기 위한 가이드라인 제공
  - ·국가 정보 인프라의 취약성과 위험을 관리하는 민관 종사자 지원
  - ·다양한 온라인 서비스에 영향이 갈 수 있는 자료가 공개되기 전 자료의 정확성과 통합성을 재고하여 사이버범죄와 사생활에 대한 법을 도입하고 대중에 자신들의 권리 강화
- 카타르 침해사고대응팀은 ITU-아랍 지역 사이버보안(ITU-Arab Regional Cybersecurity, ARCC)에서 주관한 제5차 아랍국가 사이버 훈련을 주최하며, 아랍지역의 선도 센터 중 하나로 선정됨

▶ 통신규제국(CRA)

- 통신규제국(Communications Regulatory Authority, CRA)은 2014년 설립된 독립 규제 당국으로 모든 개인, 기업에게 합리적인 통신 서비스 제공을 목적으로 함
- 통신규제국(CRA)의 주요 역할은 다음과 같음
  - ·통신 부문 규제
  - ·주파수, 전화번호 및 도메인 관리 및 할당
  - ·통신 서비스 표준 설정 및 모니터링
  - ·불공정 행위로부터 소비자 보호
  - ·투명, 공정, 신속, 효과적인 분쟁 해결 시스템 관리
- 2018년 2월 법 개정안(law no.17/2017)이 시행되면서 통신규제국(CRA)의 모니터링에 더 강력한 권한이 부여되어 조사가 필요한 경우 해당 개인, 기업으로부터 모든 문서, 기록, 장비 및 데이터를 제공받을 수 있으며, 전기통신법을 위반하였다고 판명이 날 경우 금융 제재 위원회와 경찰관을 통하여 벌금을 부과할 수 있게 됨

▶ 카타르 보안청(Qatar State Security)

- 2004년 설립된 내무부 산하 기관으로 GIS(General Intelligence Service), 수사, 국가안전기관이 합쳐진 기관임
- 내부 보안 감사 수행 정보를 수집하고 안보 방해 행위와 간첩행위에 대한 수사와 저지에 일차적인 책임을 보유

3) 규제 및 인증제도

▶ National Information Assurance Framework (NIAF)

- NIAF를 통해 국제적으로 인정하는 사이버보안 표준을 수행하기 위한 사이버보안 프레임워크를 갖고 있음
- 모든 정부부처와 주요 기관들은 사이버 공격과 테러리즘에 대응하기 위해 위기관리계획(Crisis Management Plan)을 수행해야 함

▶ ISO 27001

- 카타르 고유의 보안 인증 표준은 없는 상황으로 카타르는 국제 표준인 ISO 27001을 따르고 있음

▶ National Information Assurance (NIA) Certification

- Q-CERT는 정부 기관의 광범위한 사이버 보안을 규정하며 데이터 보안을 위해 National Information Assurance (NIA) Certification 표준을 준수하도록 하는 새로운 프레임워크를 2019년 2월 발표
- NIA 인증은 정보보안에 대한 위험을 효과적으로 관리하며, ISO27001과 같이 다른 인증으로의 경로를 쉽게 함
- 은행, 금융, 건강, 공공, IT부문과 같은 정보보호가 중요한 경우 특히 적합, 또한 대량의 데이터 관리 조직이나, 카타르 정부에서 운영되는 데이터 센터, 다른 조직을 대신하여 정보를 관리하는 조직에도 적용됨

4) 최근 정책 동향 및 이슈

▶ 카타르 사이버 보안센터 등은 사이버 보안 분야 협력 및 훈련을 위해 Cisco와 계약 체결(2019년 7월)[253]

- 카타르 내무부의 사이버 보안센터, 최고 위원회와 보안위원회는 Cisco와 계약을 체결함
- 이를 통해 사이버 보안 분야에서 현대 기술을 다루는 자격을 갖춘 인력 확보, 다양한 전자 공격에 대응하기 위한 강력한 사이버 보안 시스템의 중요성 강화를 기대함

▶ 카타르 내무부 사이버 보안센터는 18개 정부 기관과 전자 링크를 구축(2019년 5월)[254]

- 내무부 사이버 보안센터는 사이버 공격으로부터 보호하기 위해 18개 정부 기관과 전자 링크(electric link)를 구축하였으며, 2019년 말까지 100개의 정부 및 준정부 기관과 연결하는 것을 목표로 함
- 사이버 위협이나 공격으로부터 보호하기 위해 알림을 보내어 연결된 기관을 탐지하고 경고하며, 연결된 기관이 준비 되지 않은 경우 센터가 도움을 주기 위함임
- 센터의 제어실은 초당 약 35,000건의 전자사고(e-incidents)를 받고 있으며, 사이버 보안센터의 역할은 사이버 범죄를 탐지하고 그것을 조사하여 범죄자를 법정에 세우는 것임

▶ 카타르 교통통신부, 사이버보안 프레임워크 개시(2019년 2월)[255]

- 2019년 2월 카타르 교통통신부(MoTC)는 국가 표준을 준수하기 위한 메커니즘을 수립하기 위해 국가 정보 보안 표준 프레임워크를 개시함
- 새로운 프레임워크는 법규제에 따라 디지털 정보와 데이터 보호를 위한 모범 사례와 ICT 프로그램, 시스템, 서비스를 조정하게 됨

---

253 The Peninsular, "Qatari organisations sign cyber security agreement with Cisco International", 2019.7.8.
254 The Peninsular, "MoI Cyber Security Center to link 100 govt entities by end of 2019", 2019.5.24.
255 CISOMAG, "Qatar MoTC launches new cybersecurity framework", 2019.2.12. https://www.cisomag.com/2784-2/

- 국가표준에 따라 라이선스 인증서, 문서, 공인을 발행하여 모든 부문의 기관이 정보시스템을 보호하고 정보 보호 정책을 구현할 때 성숙도를 향상시켜 보다 안전한 사이버 환경을 조성하도록 지원
- 규정준수 메커니즘은 기업이 공인 제어 서비스 제공업체를 통해 규정준수 인증을 받을 수 있도록 IT 감사 인증 프로그램을 시작하는 등 정부 시스템의 품질과 보안을 보장하는 새로운 보안 표준을 설정하게 될 것임

▶ 카타르 금융센터, 데이터 보호 이사회 설립 발표(2018년 5월)[256]

- 2018년 5월 시행된 유럽 GDPR에 대비하여 카타르 금융센터(Qatar Financial Center, QFC)는 데이터 보호 이사회 설립을 발표함
- 새로운 이사회는 마스트리흐트 대학교에 위치한 유럽 개인정보 보안센터(European Centre for Privacy and Cybersecurity, ECPC) 검증을 받은 데이터 보호 책임자(Data Protection Officer)가 주도할 것이며 카타르 금융센터(QFC)와 같이 유럽연합의 GDPR 표준을 적용하는데 주력할 예정
- 카타르는 2016년 12월 중동에서 개인정보보호법을 처음으로 제정한 나라로, 기존의 카타르 개인정보보호법을 GDPR 표준에 맞게 개정하거나 분쟁 요소를 완화하는 것이 주 업무
- 카타르 금융센터(QFC) 위원장은 GDPR의 엄중한 제재를 피할 수 있도록 카타르 기업들에게 필요한 정보, 도구 및 문서 등을 제공할 것이라 밝힘
- 또한 GDPR이 가져올 주요 변경 사항과 개인정보데이터를 다루는 카타르 회사들의 요구사항도 고려함

▶ 카타르, 2022년 월드컵에 대비하여 보안에 총력을 기울임(2018년 5월)[257]

- 2022년 월드컵 개최지인 카타르는 월드컵 준비에 2,200억 달러를 투자할 예정이며 보안에 총력을 기울이고 있음
- 카타르 월드컵준비위원회 산하 보안위원회는 월드컵에 대비하여 워크숍을 개최하여, 국제 표준, 현행 카타르법률 및 전자시스템에 적합한 국가 사이버 보안 체계를 만드는 것을 목표로 함
- 카타르는 2012년 인터폴과 협업하여 Project Stadia를 설립, 월드컵에 대비하여 산업 제어시스템, 국가 사이버 보안 능력, 사이버 위협 대응 능력 등을 키우는 10개년 계획을 실행 중

5) 정보보호 스타트업 관련 정책동향

건전한 정보보호 스타트업 생태계 조성을 위한 정부 정책 동향

256 The Peninsular, "Workshop on cybersecurity for 2022 World Cup", 2018.5.7.
257 The Peninsular, "QFC establishes Data Protection Directorate", 2018.5.24.

▶ 카타르 정부는 경제 수익 창출 및 일자리 성장 촉진을 위해 스타트업 생태계를 더욱 발전시키고자 노력하고 있으며, 이러한 노력의 중심에 2017년 3월에 시작된 TASMU(Smart Qatar Programme)가 있음[258]

- TASMU는 Qatar National Vision 2030 성취를 가속화하기 위해 설계되었으며, 향후 5년간 60억 QR(약 16억 4800 USD)을 지원할 계획임[259]
- TASMU를 통해 50개의 신규 기업에 재정 지원을 제공하여 ICT분야에서 일자리 수를 10% 늘리고자 함
- QSTP(Qatar Science and Technology Park)는 공공 기관, 민간 기업, 개인이 혁신적인 사업 아이디어를 개발하고 상용화 및 라이선스 할 수 있도록 지원함
- 1년에 두 번 운영되는 XLR8이라는 엑셀러레이터와 스타트업을 위한 3개월 투자, 훈련 및 멘토링 프로그램인 Doha Dojo를 포함하여 ICT분야의 다양한 이니셔티브가 있음

▶ 교통통신부의 디지털 인큐베이션 센터(Digital Incubation Center, DIC)는 카타르에서 기술 관련 비즈니스를 시작하거나 성장시키는 중요한 초기 단계에 있는 특히 젊은이들을 대상으로 ICT 혁신을 강화하기 위해 만들어짐[260]

- DIC는 모든 기술 아이디어에 대해 신청서를 접수하지만 특히, 사이버 보안, 전자상거래, 블록체인, IoT, 클라우드 컴퓨팅, 스마트 시티 솔루션 등 기술 분야의 아이디어 기업에 관심을 둠
- DIC는 스타트업에게 기술 및 비즈니스 가이드, 무료 사무실 공간, 교육 및 훈련, 멘터, 법적 조언, 홍보 등을 지원
- 성장 및 확장 능력을 갖춘 성공적인 스타트업은 Manateq Economic Zone의 카타르 디지털 클러스터에 입주할 수 있음
- DIC는 2019년 8월 기준 스타트업 트랙, 아이디어 캠프, 코워킹 스페이스의 세 가지 트랙을 제공하며 100개의 스타트업, 177개의 아이디어 팀이 입주해 있음

정부주도 정보보호 클러스터 조성 등 스타트업 관련 사례

▶ QF RDI(Qatar Foundation Research, Development and Innovation)*는 새로운 기금인 '혁신 쿠폰(Innovation Coupon)'을 카타르의 사이버보안 중소기업인 ADGS(Application Design for Global Solutions)에게 첫 번째로 수여함[261]

* QF RDI(Qatar Foundation Research, Development and Innovation)는 교육, 연구, 지역사회 개발에 일하는 50개 이상의 단체로 구성된 비영리 단체(qf.org.qa)로 왕족이 설립함

---

258 Oxford Business Group, 5G technology and Qatar's ICT sector
259 MoTC의 TASMU 웹사이트 http://www.motc.gov.qa/en/node/14067
260 Digital Incubation Center 홈페이지 https://dic.motc.gov.qa/
261 The Peninsular, QF-funded technology aims to enhance cybersecurity globally, 2019.6.26.

- QF RDI의 '혁신 쿠폰(Innovation Coupon)'은 카타르에 기반을 둔 모든 부문과 산업의 중소기업이나 스타트업을 대상으로 제품이나 서비스를 개발 할 수 있는 역량과 기술 지식이 있지만 특정 기술이나 비즈니스 과제를 해결하기 위해 보다 지원을 요구하는 기업에게 혜택을 주는 기금임
- ADGS는 행동학적 생체인식(behavioural biometrics)을 사용하여 사이버 위협에 대항하는 사이버 보안 수준을 높여주는 소프트웨어인 STROKK를 개발함
- ADGS의 STROKK는 컴퓨터 키보드로 사람이 입력하는 방식을 분석하는 사람 중심 기술과 같은 행동학적 생체인식을 기반으로 전 세계 스마트폰, 태블릿, 컴퓨터와 같은 디지털 도구 사용자에게 위협이 되는 데이터 유출에 대처하는 것을 목표로 함
- 이 기술은 금융 부문과 같이 사이버 위협의 위험과 영향이 높은 것으로 간주되는 부문에서 카타르 내에 이미 구축되었으며, 유럽과 남미의 일부 군사 방위 정보 서비스에 잠재적 사용을 위해 테스트됨

▶ 교통통신부는 '중소기업을 위한 디지털 전환 프로그램(Digital Transformation for SME's program)'을 2018년 시작하여 5천여 기업이 기술을 채택하고 생산 및 서비스를 개선하고 전자 상거래를 장려할 수 있도록 함

- 이 프로그램은 웹 서비스, 전자상거래, 클라우드 서비스 세 가지 영역에 중점을 두며, 이를 통해 올바른 서비스 제공업체와 중소기업을 연결하여 디지털 전환으로의 여정을 시작할 수 있도록 지원
- 이 프로그램은 독점적인 콘텐츠와 이벤트를 제공하고 승인된 공급업체에 우선적인 비용 및 제안에 접근 할 수 있도록 하여 ICT 개발의 최첨단을 지원하도록 설계됨

융합보안시장 및 정책 동향

스마트시티

▶ 카타르는 2022년 월드컵을 개최할 예정으로 Lusail 개발(lusail.com) 주도의 스마트 시티 개발을 도하로 연장하는 야심찬 도시 건설 프로젝트[262]

- Lusail 시의 크기는 38km^{2}이며, 4개의 섬과 19개의 다목적지구(주거, 상업)로 구성되며, 이 도시는 첨단기술 솔루션을 기반으로 스마트 시티 관리 및 모니터링을 수행할 Lusail 명령 제어 센터(Lusail Command and Control Centre, LCCC)에 의해 지원될 것임
- 카타르의 통신회사 Ooredoo와 Vodafone은 약 45만 명의 거주자가 거주할 것으로 예상되는 Lusail 시에 주택과 사무실에 광섬유 브로드밴드를 제공할 예정임[263]

사물인터넷(IoT)

▶ 2017년 2월 Vodafone과 QMIC(Qatar Mobility Innovations Centre)에서 차량 관리 서비스를 시작하였으며 Vodafone의 IoT 플랫폼을 사용하여 차량 추적 및 물류 관리가 가능

▶ Ooredoo의 차량 관리 서비스는 2018년 중반에 처음으로 선보였으며, 솔루션은 실시간 소프트웨어와 센서를 사용하여 글로벌 차량 관리 리더인 Geotab의 플랫폼을 기반으로 함

- Ooredoo는 2019년 초 IoT Builder라는 IoT 플랫폼을 개발하였으며, 하나의 애플리케이션은 기업이 장치를 원격으로 제어하고 관리할 수 있는 기능이 포함됨

블록체인

▶ 카타르는 금융기관이 암호화폐(cryptocurrency) 거래를 금지함

- 카타르중앙은행(QCB)는 국내 은행 시스템의 안전과 보장을 위해 2018년 2월 비트코인 거래를 금지[264]

▶ 커머셜 뱅크(Commercial Bank)는 블록체인 기반 엔터프라이즈 소프트웨어 기업인 R3와 제휴를 맺은 카타르에서 첫 번째 은행이 됨(2019년 3월)[265]

---

262 BuddeComm, Qatar - Telecoms, Mobile and Broadband - Statistics and Analyses, 2019.4.22. p.28.
263 Oxford Business Group, 5G technology and Qatar's ICT sector
264 GulfTimes, Qatar uses fintech as key tool for development goals: Sheikh Abdulla, 2019.4.11.

- 커머셜 은행은 1975년 설립된 개인은행으로 도하에서 매우 유명하고 신뢰할 수 있는 은행임
- R3는 뉴욕에서 2014년에 설립된 회사로 블록체인 플랫폼인 Corda에 혁신적인 앱, 소프트웨어/솔루션 개발을 촉진하기 위한 협력 벤처를 설립하고 있는 회사로 전 세계 Corda 블록체인 플랫폼으로 연결된 300개 이상의 벤처를 갖고 있음
- 커머셜 뱅크는 이번 제휴를 통해 고객에게 제공하는 서비스를 개선할 블록체인 기술을 사용하는 새로운 방법을 찾아 고객에게 빠르고 편리하며 원활한 서비스를 제공하고자 함

▶ 카타르 재단의 하마드 빈 칼리파 대학(Hamad Bin Khalifa University, HBKU)의 과학공학대학(College of Science and Engineering, CSE)은 카타르 국가 연구펀드(Qatar National Research Fund, QNRF)의 주요 자금 지원 프로그램인 국가 우선순위 연구프로그램(National Priorities Research Program, NPRP)프로젝트 7개를 받음[266]

- 그 중 2개는 핀테크를 다루고 있으며, 하나는 NPRP11 표준 프로젝트인 '확장 블록체인 기술-새로운 패러다임 및 사이버 보안 및 핀테크에 대한 응용 프로그램'으로 총 자금 백만 달러 이상을 지원 받음
- 다른 하나는 '사이버 탄력적인 핀테크'라는 NPRP11 클러스터 프로젝트로 블록체인 기반의 거래 금융을 조사하며, 이 프로젝트는 2019년 9월에 시작된 총 3백만 달러의 3년간의 프로젝트임
- CSE의 연구는 핀테크 혁신의 80% 핵심 기술인 블록체인과 밀접한 관련이 있으며 금융 거래의 보안 평가에도 도움이 됨

핀테크

▶ QFC(Qatar Financial Center)는 영국과 카타르의 금융 서비스 부문간 유대관계를 더욱 발전시키기 위하여 런던에서 개최된 '카타르 데이' 포럼에 참여(2019년 4월)[267]

- 영국의 국제무역부와 카타르 중앙은행의 파트너십과 함께 런던시가 주최한 행사에 영국의 약 120명의 C-레벨 임원들과 카타르의 주요 국가 및 금융 서비스 기관이 참여
- 프로그램은 자산관리, 자본 시장 뿐 아니라 핀테크, 금융서비스의 사이버보안 부문에 중점을 둠

▶ QDB(Qatar Development Bank)는 카타르의 핀테크 산업 발전을 지원하기 위한 글로벌 핀테크 허브인 '카타르 핀테크 허브'를 설립함(2018년 5월)[268]

- 이는 핀테크 생태계의 참가자와 이해관계자 간의 협력을 촉진하고 은행의 핀테크 비전을 향상시킬 지역 및 글로벌 관계를 개발하는 것을 목표로 함

---

265 CryptoNewsZ, Qatar's Commercial Bank is Joining Hands With Blockchain-based firm R3, 2019.3.18.
266 Qatar is on Course to Become a Regional Leader in FinTech, 2019.4.2.
267 The Peninsular, QFC puts fintech in spotlight at 'Qatar Day' in London, 2019.5.1.
268 Fintechnews Middle East, Qatar Works To Become A Fintech Hub, 2019.2.14.

라. 사우디아라비아

'18년 GDP(십억달러)	782.48
'18년 인구수(천명)	33,700

■ ITU 글로벌 사이버보안 지수(Global Cybersecurity Index, GCI)

· 사우디아라비아의 사이버보안 지수 순위는 한국보다 2단계 높은 13위이며 상위권에 속함

국가명	2018		2017		전년대비 증감	
	지수	순위	지수	순위	지수	순위
사우디아라비아	0.881	13	0.569	46	+0.312	+33
대한민국	0.873	15	0.782	13	+0.091	-2

■ ICT 관련 주요 지수

· 사우디아라비아의 전반적인 ICT 발전 수준은 전 세계 중상위권 수준을 유지

지표명	사우디아라비아		한국	
	점수	순위	점수	순위
IMD 국가경쟁력지수(2019)	-	26	-	28
IMD 디지털경쟁력지수(2019)	-	39	-	10
UNCTAD 전자상거래지수(2019)	73.3	49	89.4	19
ITU 글로벌 사이버보안 지수(GCI 2018)	0.881	13	0.873	15
UN 전자정부 지수(2018)	0.711	52	0.901	3

■ ICT 관련 주요 통계 (ITU, 2018년 말 기준)

· 사우디아라비아의 유선통신 보급률은 10% 미만으로 이동통신 중심으로 발전

항목	사우디아라비아		한국	
	가입자수(천 명)	보급률(%)	가입자수(천 명)	보급률(%)
유선전화	3,123	9.27	25,907	50.63
유선브로드밴드	1,901	5.64	21,286	41.60
이동통신	41,311	122.57	66,356	129.67
인터넷 이용률	93.31%		95.90%	

정보보호 산업 개요

1) 보안 환경

▶ ITU 2018 'Global Cybersecurity Index(GCI)'에 따르면 사우디아라비아의 사이버보안 지수는 0.881로 전세계적으로는 13위, 중동 국가에서는 1위를 기록

- 해당 지수는 법적·기술적·조직적 대응·역량 강화 및 국제협력 등 5개 부문의 지수를 종합한 것으로, 사우디아라비아는 특히 역량강화 및 국제 협력의 측면에서 중동국가 중 1위를 기록
- 사우디아라비아는 ▲BADIR (기술 인큐베이터 프로그램) ▲MAEEN (사우디 리서치 및 혁신 네트워크) ▲SAFCSP (사우디 사이버보안 및 프로그래밍 연맹) 등 많은 이니셔티브를 통해 역량 강화에 노력

▶ 사우디아라비아는 중동에서 가장 많은 사이버 공격의 대상으로, 매일 160,000건이 넘게 서버가 공격당하는데, 공공 및 민간 부문 조직의 온라인 시스템을 대상으로 국가 경제를 약화시키는 것이 목표

- ▲모든 부문에서 정부가 제공하는 서비스에 대한 디지털화 추세 ▲사우디아라비아가 위치한 지역의 지정학적 상황(리야드의 중추적 역할)으로 인해 사이버 공격의 대상이 됨
- 2012년 Saudi Aramco에 대한 공격이후 적극적인 사이버보안 조치를 시행하고 있으며, 2017년 8월 석유 화학 시설에 대한 또 다른 사이버공격은 악성 코드 코딩의 결함으로 실패함
- 전국의 고속 인터넷 액세스를 통해 안전한 디지털 인프라를 구상하는 Saudi Vision 2030 계획에 따른 사이버보안 강화 필요성 증대
- 카스퍼스키 시큐리티 네트워크 (Kaspersky Security Network)에 따르면, MENA 지역의 모든 사용자 중 평균 27.3%가 2019년 1분기 웹 위협 사건의 영향을 받았으며 사우디아라비아는 35.9%로 가장 높은 점유율을 기록

▶ 워싱턴 소재 사이버 연구 및 연구 재단 (Global Foundation and Research for Cyber Studies and Research)에서 실시한 최근의 정책 연구에 따르면, 사우디아라비아는 기술적으로 선진국 중 하나임에도 불구하고 지역별 교육 과정이 부족하고 사이버 공격 위험에 대한 일반적인 인식이 부재

- 지역 사우디 산업을 발전시키기 위한 교육 이니셔티브는 국가 사이버 보안국 (National Cybersecurity Authority) 하에서 시작해야 할 필요성 대두
- 소셜 미디어 테러와 핵티비즘(정보 도난이 아닌 서비스 중단)은 사우디 정부가 사이버 보안을

강화해야할 중요한 분야

▶ 중동의 사이버 위협은 급속도로 확대되고 있으며, 사이버 공격은 더 많아지고 정교해지고 있는 추세임

- 2018년 5월 설문 조사에 따르면 걸프 기반 기업의 약 41%가 지난 1년 사이버 공격을 경험했으며, 2016년보다 46% 증가
- 2017년 해커가 사우디아라비아의 석유화학 공장을 폭발 시도 사건도 발생
- Booz Allen Hamilton은 ▲공급 업체를 통한 공급망 공격 ▲산업 제어 시스템을 목표로 설정 ▲제3자 소프트웨어를 통한 공격 ▲cryptocurrency 환경 활용 ▲대규모 정부 및 산업 데이터베이스 침입 ▲ransomware 사용 ▲유명한 이벤트 활용 등 걸프 지역이 미래에 심각한 공격에 직면 할 수 있는 7가지 주요 영역을 발표

2) 인터넷 및 통신 환경

▶ 사우디아라비아의 ICT 시장은 자본 가치 및 지출 규모 측면에서 중동 최대 규모이며, 걸프만 협력위원회(GCC)의 모든 ICT 시장의 70% 이상을 차지

- 2017년 사우디아라비아 총 GDP 중 ICT 부문이 약 6%를 차지함으로써 GDP에서 중요한 기여를 하는 산업으로 자리매김
- 사우디 ICT 시장은 ▲높은 경쟁 ▲낮은 가격 ▲유선 및 모바일 광대역의 높은 사용량이 특징

▶ 유선통신

- 2019년에는 유선전화의 약 70%가 주거용, 30%는 기업용으로서, 유선전화 가입자(303만명) 및 전화 밀도(30%)는 지난 수년간 안정적으로 유지되고 있음
- 2019년 인터넷 점유율는 81%로서 중동 지역 평균 59%에 비해 상당히 높은 점유율을 보이고 있으며, 현재 인터넷 가입자는 2,740만명 임
- 유선 브로드밴드는 2016년 가입자수 329만명, 점유율 44%에서 2019년 가입자수 260만명, 점유율 35%로 지속적으로 줄어들고 있는 추세임

▶ 이동통신

• STC, Mobily, Zain 통신 사업자 모두 다양한 시장 세그먼트를 수용하기 위해 선불제 제품을 제공하고 있으며, 2016년 지문 등록 제도에 따라 선불 가입자 시장 점유율이 감소함

표 _ 2019 년 이동통신 사업자, 가입자 수, 시장점유율

(단위: 만, %)

이동통신 사업자	가입자 수	시장점유율
STC	2,320	54%
Mobily	1,200	28%
Zain	780	18%
합계	**4,300**	**100**

[출처] Buddcomm(2019.5)

• 모바일 부문은 사우디아라비아 전체 통신 수익의 약 75%를 점유함으로써, 통신 시장 성장의 대부분을 견인
• 2016년 초 시행된 내무부의 지문법(SIM카드 구입 시 소비자의 지문을 국가 정보 센터에 등록)으로 인해 2016년~2017년 모바일 보급률은 급격히 감소되었으나, 이후 반등 추세
• 2019년 예상 모바일 가입자 4,300만 명, 보급률 132%
• 모바일 브로드밴드도 내무부 규제로 인하여 2016년 급격한 감소(75%)를 보였으나, 이 후 성장세를 회복
• 2019년 예상 모바일 브로드밴드 가입자 3,440만 명 보급률 102%
• 3개 주요 사업자는 서비스 범위 확대 및 품질 개선에 중점을 두고 LTE 서비스를 개시하였으며, 2017년 말 인구의 약 90%에 LTE 네트워크 구축·제공
• 2017년~2018년 Mobily는 Ericsson, Nokia 및 Huawei와의 다양한 파트너십을 통해 5G에 대비하여 네트워크를 강화하였으며, STC와 Zain은 Nokia와의 MOU를 통해 5G 기술을 개발
• 사우디아라비아에는 이미 5G를 지원하는 약 1,000 개의 통신 타워가 있으며, 2019년 내에 초고속 모바일 서비스 제공을 계획

표 _ 사우디 IT 관련 서비스 가입자 현황

(단위: 십만 명, %)

구분(점유율)	2014	2015	2016	2017	2018
이동통신 가입자	527(171)	471(149)	437(138)	402(127)	413(127)
유선 브로드밴드 가입자	30(43.2)	36(50.7)	33(44.8)	25(33.6)	19(33.7)
인터넷 사용율 (%, 10~74세)	91.31	91.12	93.67	94.34	93.31

[출처] 통신정보기술위원회

▶ 5G

- 사우디아라비아에는 이미 5G를 지원하는 약 1,000개의 통신 타워가 있으며, 2019년 내에 초고속 모바일 서비스를 제공 계획 중임
- 현재 모바일 마켓 플레이어는 STC (Saudi Telecommunication Company), Etihad Etisalat Company (Mobily) 및 Mobile Telecommunication Company (Zain)이며, 모두 광범위한 모바일 서비스 (GSM, 3G 및 LTE) 및 사물 인터넷 (IoT) 솔루션을 제공 중임
- ▲5G 스펙트럼 가용성 ▲5G 인프라 및 시험 ▲5G 서비스 생태계의 개발을 촉진하는 모든 이해관계자들로 구성된 전국 5G 태스크 포스가 설립
- 사우디아라비아에서는 중동 지역에서 최초로 5G 라이브 시험을 시행하였으며(2018.5), 사우디 정부는 자국을 5G 서비스의 지역 리더로 만드는 것을 목표로 하고 있음

정보보호 시장 현황

1) 시장 규모

시장 규모 및 성장률

▶ GCC 지역의 사이버 보안 시장은 사우디아라비아, UAE, 오만에 의해서 주도되고 있으며, 여러 조사기관에 따르면 2022년까지의 약 20% 이상의 성장을 기록할 것으로 전망됨

- Market Research Engine에 따르면, 이 지역의 사이버 보안 시장은 2016년부터 2022년까지 CAGR 22%로 성장하고, 2022년까지 343억 7,000만 달러에 이를 것으로 전망
- Ken Research 연구에 따르면, 2017년부터 2022년까지 이 지역 사이버 보안 시장의 CAGR이 약 20%가 될 것이라고 예측
- 보안 서비스 산업은 2022년까지 3,373억 달러까지 성장 전망
- 사우디아라비아는 최근 중동에서 악성 사이버 위협의 주요 대상이 되었으며, 이로 인해 향후 가장 큰 사이버 보안 시장 점유율을 가질 것으로 예상
- GCC 지역은 전략적 경제적 중요성 때문에 사이버 공격의 중심지가 되었고, ▲사이버 위협 대응 ▲디지털화 계획 ▲국토 안보에 대한 투자가 시장을 주도

▶ 중동 사이버 보안 시장 규모는 CAGR 14.2%로, 2017년 110억 3,800만 달러에서 2022년 220억 1,400만 달러로 증가할 것으로 전망[269]

- 응용 프로그램 보안 분야는, 예측 기간 동안 가장 높은 CAGR로 성장할 것이며, 모바일 및 웹 기반 응용 프로그램 및 엔터프라이즈 이동성이 증가함에 따라 기업 응용 프로그램의 보안 솔루션 사용이 크게 증가할 것으로 예상
- 정부 및 방위 산업 부문은, 정부 부문 및 정부 규제 석유 업체에 대한 사이버 공격 사례가 증가함에 따라 중동 사이버 보안 시장에서 2017년부터 2022년까지 가장 높은 시장 점유율에 기여할 것으로 예상
- 가스 회사 및 의료 분야는, 의료 응용 프로그램의 기술 확산과 이 분야의 데이터 도난 사례 증가로

269 Middle East Cyber Security Market by Solution, Service, Security Type, Deployment Mode, Organization Size, Vertical, and Country - Forecast to 2022 보고서

인해 중동 사이버 보안 시장에서 2017년 부터 2022년 까지 두 번째로 높은 CAGR로 성장할 것으로 예측

- 사우디아라비아는 에너지 및 유틸리티, 정부 및 방위, IT 및 통신, 의료 등 다양한 산업 분야의 기업을 보호해야 하므로 2017년에서 2022년까지 중동 시장에서 가장 큰 시장 점유율을 차지하고 중동 사이버 보안 시장을 장악할 것으로 전망

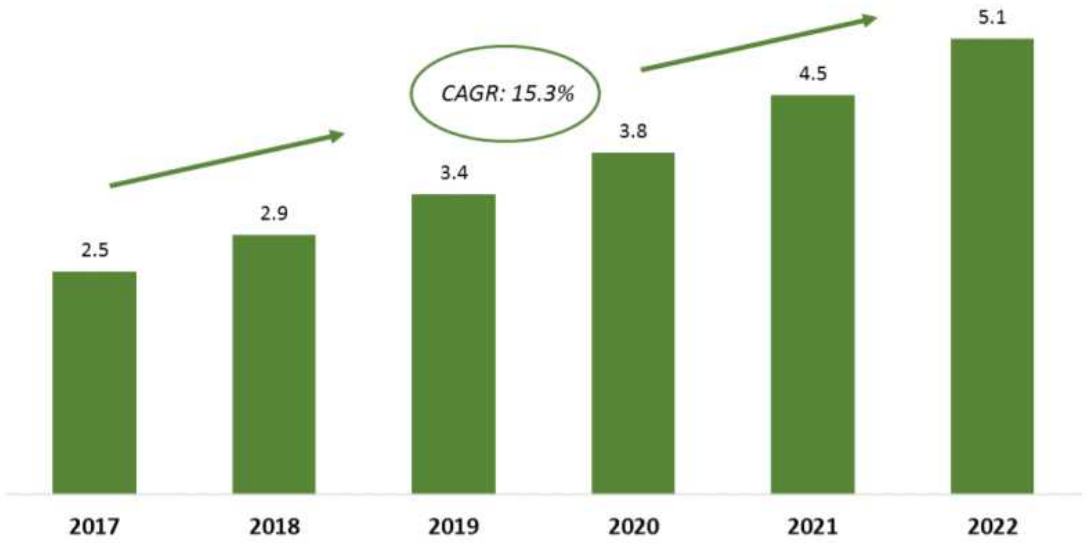
▶ 2018년에서 2022년까지 사우디아라비아의 전체 보안 지출은 CAGR 7.9%로 2019년 4억 5500만 달러에 도달할 것으로 전망

- 해당 지출의 절반 이상이 ▲보안 컨설팅 및 교육 ▲보안 구축 및 통합 ▲관리형 보안 서비스와 같은 보안 서비스에 사용
- 2019년 사우디아라비아의 통합 보안 서비스 지출은 약 9% 증가할 것으로 예상
- 보안 공급 업체와 서비스 제공 업체가 고객의 비즈니스 우선 순위에 능동적으로 대응하고, 보안 운영 센터(SOC) 관리, 위협 인텔리전스 및 고급 탐지 및 분석을 수행할 전망

▶ 사우디아라비아의 사이버 보안 시장은 2023년까지 55억 달러로 성장할 것으로 전망

- U.S.-Saudi Arabian Business Council에 따르면, 사이버 보안 시장이 2022년까지 CAGR 15.3 % 성장할 것으로 예상
- '2023년까지의 MEA 사이버보안 시장 예측 보고서'에서는, 2019년 보안 부문에 더 많은 투자가 이루어짐에 따라 사이버 보안 시장 가치가 30억 달러로 상승할 것으로 예상
- 사이버 보안 시장의 전문 서비스 부문이 가장 큰 비중을 차지할 것으로 예상되며, 2023년까지 CAGR 15.0%로 14억 달러로 성장할 것으로 전망
- 사우디아라비아는 최강의 사이버 보안 솔루션을 채택하고 있으며, 중소기업 및 대기업은 위협에 대한 인식이 증가하고 있어 컨설팅 및 자문 서비스에 대한 수요가 높아지고 있음
- 대기업 부문은 2023년까지 CAGR 14%로 34억 달러로 성장 예측
- 중소기업 부문의 채택률이 높아짐에 따라 2023년까지 CAGR 16.8%로 20억 달러로 성장 평가

그림 _ 사우디아라비아 사이버 보안 시장 전망 (2017-2022)



[출처] USSABC, 6Wresearch
[단위] 십억 달러

▶ 사우디아라비아의 물리 보안에 대한 시장 수요는 건설, 운송, 산업 플랜트, 석유 및 가스와 같은 인프라 관련 영역의 보안 문제 확대로 인해 증가 추세

- 2014년에서 2017년 사이의 GCC 영역에서의 보안 감시에 대한 모든 프로젝트 관련 투자의 1/3은 사우디아라비아에 의해서 수행
- 보안 감시 부문에 대한 자본 투자 프로젝트는 주로 건설, 전력 및 운송 부문으로서 이외 석유 및 가스, 석유 화학 등의 분야에서도 이루어짐
- 사우디 정부는 2017년 Hajj 순례를 위해 약 6,000 대의 디지털 카메라를 설치하는 등 보안 감시 부문에 많은 투자
- 사우디 정부는 국경을 지키기 위한 역량을 강화할 계획으로서, 보안 지출은 점차 국경과 석유 산업을 확보하는 데 집중할 것으로 전망

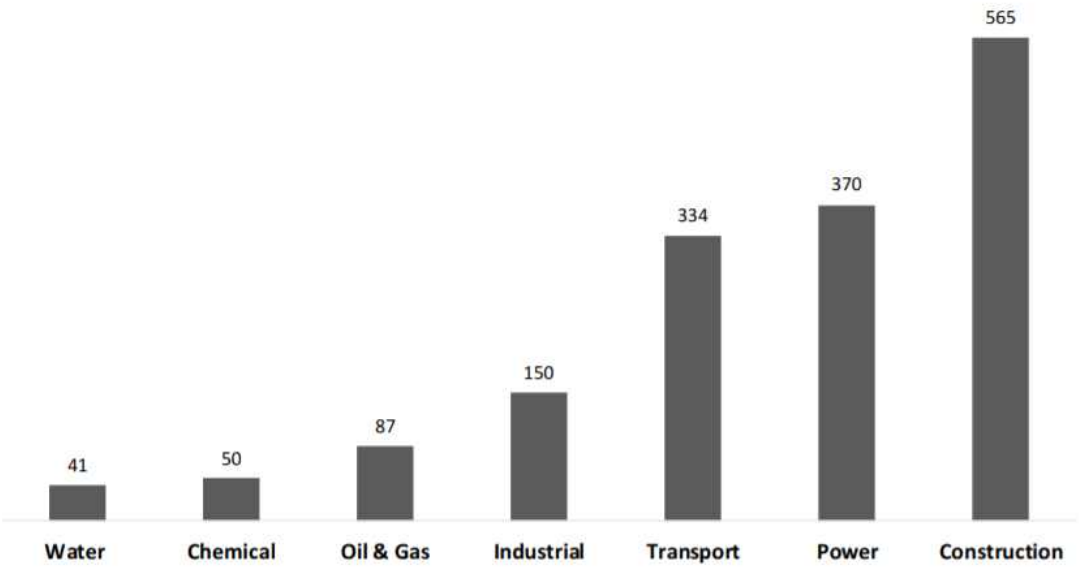
▶ 비디오 감시, 액세스 제어 및 침입 탐지를 포함한 물리 보안 시장은 2015년에서 2021년까지 연평균 14.4% 성장할 것으로 예측

- 공공 및 민간 인프라에 대한 잠재적 테러 공격 가능성에 대한 보안 우려가 증가함에 따라 관련된

보안솔루션의 수요 증가 추세

- 액세스 카드, 생체 인식 기반 시스템 및 컨트롤러로 구성되는 액세스 제어 시스템 시장은 2020년까지 약 12억 달러에 이를 것으로 전망되며, 정부 부문은 이 부문에서 가장 큰 수요를 견인할 것으로 예상
- 금융 서비스, 보험, 운송, 석유 및 가스 산업은 보안 시스템을 성장을 주도하는 또 다른 주요 산업임

그림 _ 사우디아라비아 보안 감시 부문 산업별 투자 프로젝트(2014-2017)



[출처] USSABC, MEED Insight Research
[참고] 프로젝트 수치는 추정치 임

2) 주요 사업자 현황

시장 특성 및 경쟁 강도

▶ 사우디아라비아 물리 보안 시스템 시장은 2024년까지 3억 1,300만 달러에 이를 것으로 예상

- 2014-2017년 동안 해당 시장은 주로 유가 하락에 따른 경제 상황의 악화로 인해 하락세를 기록했으며, 이 기간 동안 주요 정부 지출이 줄어 전국적으로 여러 정부 프로젝트가 중단
- 사우디아라비아의 안보 문제 및 범죄 지수 증가에 따라, 예측 기간 동안 물리 보안 시스템 시장의 성장이 가속화 될 것으로 전망

▶ 6wresearch에 따르면, 비디오 감시 부문은 주거 및 상업 부문의 정부 규제에 의해 IP 비디오 감시 시스템의 배치가 증가함에 따라 시장 점유율의 대부분을 차지

- 사우디 정부의 비전 2030에 따른 인프라 개발 프로젝트 투자 증가로 인해 향후 인프라가 크게 확장되어 비디오 감시 시스템 배치가 증가할 것으로 전망
- 사우디아라비아의 중앙 지역은 특히 상업 및 주거 분야의 인프라 개발 프로젝트가 증가함에 따라 물리적 보안 시스템 시장에서 차지하는 비중이 큰 것으로 나타남

▶ 국토 안보 및 치안은 현재 사우디의 시장 지출에서 2018년 46억 달러로 가장 큰 비중을 차지 (6WResearch 조사)

- 정보 보안 (26억 달러), 상업용 보안 (8억 8,800만 달러), 화재 방지 (2억 7,300만 달러) , 물리적 및 주변 보호 (1억 9,800만 달러)의 순으로 시장이 형성
- 이와 관련된 기술은, 세계 최대의 비디오 감시 제공 업체인 Hikvision이 인공 지능 및 기계 학습에 의해 구동되는 최신 기술을 보유하고 있으며, 해당 시장을 견인

▶ 사우디아라비아는 중앙 집중기관을 통한 조달집행이 이루어지지 않으므로, 조달정책 결정 기관을 중심으로 각 조달집행에 대한 가이드를 제시하는 유관기관들이 존재함

- 재무부(Ministry of Finance)의 조달 및 입찰부서(Department of Procurement and Tenders)에서 조달법 제·개정을 담당하며, 해당 법률을 기반으로 각 정부기관에서 조달을 시행하는 분산조달형태를 나타냄
- 사우디아라비아 조달의 기본법은 2006년에 제정된 왕령인 '정부 입찰 및 조달법 (Government Tender and Procurement Law Royal Degree No,M/58)'임
- 동법은 2009년에 개정되었으며 입찰 준비, 입찰서 제출, 입찰 심사, 구매 방법, 계약 및 수행기간, 보증금 등에 관한 내용을 포함함
- 조달방법은 ▲공개입찰 ▲비공개입찰 ▲제한경쟁입찰 ▲수의계약(직접구매, Direct Purchase) ▲협상에 의한 계약 ▲매각(경매) 등이 있음

주요 사업자

▶ 중동에는 글로벌 보안기업이 대부분 진출하고 있으며, 중동 사이버 보안 시장의 주요 공급 업체인 Check Point(이스라엘), Cisco Systems, Intel Security, IBM, Computer Sciences, Forcepoint, Symantec, Hewlett

Packard (미국), Sophos(영국), Trend Micro(일본) 등이 시장을 주도하고 있음

▶ 사우디아라비아의 물리 보안 시장에서 활동하고 있는 업체는, GCC 대부분의 국가에서와 마찬가지로 글로벌 업체 및 국내 업체가 혼재되어 있음

- 물리적 보안 시스템 시장에서는 Avigilon, Axis Communications, Bosch Security, Hikvision, Siemens, Honeywell Security 및 Samsung Techwin 등의 주요 업체가 활동
- 국토 안보 및 치안 시장에서는 AI Alameya, Axis Communications, Bristol, Drager, Genetec, NAFFCO, Nedap 및 ZMR 등의 업체가 주로 활동

3) 주요 동향 및 이슈

▶ 사우디 외교 안보국에 따르면 최근 이란과 카타르와의 외교적 갈등과 관련하여 사우디 정부기관과 기업에 대한 사이버 공격이 지속

- 사우디 정부는 사이버 보안에 대한 경각심과 중요성을 느끼고 국민들의 인식 제고를 위해 사이버 위협 모니터링, 주요 사이버 보안 사고를 담당하는 비상 대응팀을 만드는 등의 노력을 경주
- 사우디 군에서는 사이버전 능력을 개발하고 있지만 이란의 사이버전 능력에 미치지 못하고 있어, 향후 사이버 보안 개발은 민간 부문보다는 사이버 전쟁 능력과 정부 네트워크 방어에 초점을 맞출 것으로 전망
- 사우디의 전자정부 프로젝트는 2016년 2단계에 접어들면서 규제와 안보에 중점을 두고 있어 사이버 보안과 관련된 IT서비스 수요 증가 전망

▶ 사우디 국영 석유기업 Aramco는 미 방산업체 Raytheon사와 IT 보안회사 설립 MOU 체결(2018.12)

- 합작 보안회사는 ▲통합 방어 사이버 보안 소프트웨어 및 하드웨어 기능 개발 ▲보안 서비스 개발 ▲마케팅 및 연구 개발 활동을 수행
- 기업들이 사물 인터넷 및 빅데이터와 같은 기술을 점차로 수용함에 따라 사이버 보안 서비스에 대한 수요가 증가할 것으로 예상되며, 합작 보안회사가 고도로 숙련된 일자리를 창출하고 장기적인 경제 비전을 지지할 것으로 기대

▶ UAE와 사우디아라비아 기관들은 여전히 사이버 보안 사고에 대응할 준비가 되어 있지 않으며, 약 30%는

사이버 보안 사고 대응 계획이 마련되어 있지 않음

- 계획을 수립한 조직 중 절반은 정기적으로 테스트를 수행하고 있지 않으며, 이로 인해 실제 공격에 대비한 준비가 부족한 것으로 파악됨
- 사이버 공격에 대한 30일 이내의 신속한 대응에 따라, 기업은 평균 데이터 유출 비용 대비 백만 달러 이상 절감 가능
- 개인 정보 보호와 사이버 보안 간의 협력이 사이버 복원력을 향상 시킨다는 것을 기관들이 인정하기 시작

▶ 클라우드, 빅데이터 및 분석, 엔터프라이즈 모빌리티 및 소셜 지원 비즈니스 기술과 같은 3차 플랫폼 기술의 확산으로 공격 영역이 크게 증가

- 공공 및 민간 부문에서 진행되는 대부분의 디지털 혁신 이니셔티브는 3차 플랫폼 기술 및 혁신 가속기(IoT, 인공지능 및 머신 러닝) 기반으로 구축되었으며, 이로 인해 발생 가능한 보안 취약점 증가
- IDC의 CIO 조사에 따르면 사우디 CIO의 46%가 1-2년 내 고급 보안 솔루션을 구현할 계획을 가지고 있으며, 약 71%는 보안 관리를 가장 큰 기술 관련 과제로 인식
- 또한, CIO의 75%는 특히 디지털 혁신 목표를 고려하여 사이버 보안 및 개인 정보 보호 기술에 대한 투자를 최고 전략적 비즈니스 목표로 설정

▶ 중동 및 KSA의 계약자인 이탈리아 SAIPEM사의 서버를 대상으로 공격(2018.12)

- 2012년 이전에 사우디 ARAMCO를 파괴한 Shamoon 멀웨어 변종이 업그레이드된 정교함과 접근 방식으로 재공격
- 원격 액세스를 통해 이탈리아의 산업 제어 시스템에 업로드 되었으며, 해당 멀웨어는 기존 버전과 달리 명령 및 제어 서버와 통신하지 않음
- 감염된 컴퓨터에 정치적 이미지를 표시하지 않고 감염된 컴퓨터의 모든 데이터를 복구 불가능한 방식으로 암호화

▶ 조직이 원격으로 제공되는 보안 서비스를 수용함에 따라 특히 관리형 보안 서비스(MSS) 시장이 확산될 것으로 전망

- 이에 따라 직원 보강을 통한 온-프레미스 보안 관리는 점차 완화될 것으로 예상
- 통신 사업자와 인터넷 서비스 제공 업체(ISP)는 이러한 보안 서비스 변화를 견인할 것으로

예상되며, SOC 및 글로벌 파트너십 등을 활용하여 MSS를 효과적으로 제공할 것으로 예측

4) 정보보호 스타트업 시장 현황[270]

시장 규모

▶ 최근 사우디아라비아 기업들의 투자가 증가하고 있으며, 정부가 주도적이고 전략적으로 이니셔티브를 진행함에 따라, 사우디아라비아 내 스타트업 환경이 개선되고 스타트업 생태계가 조성되고 있음

- 최근 외국 기업에 대한 개방적인 정책과 노선으로 전환하고 있으며, 이에 따라 기업의 진입 장벽과 규제를 줄이고 있음

▶ 사우디 정부에서는 걸프지역 테크 스타트업을 위해 총 450억 달러를 투자하기로 발표(2017년)

- 사우디아라비아 정부와 가장 긴밀히 협력하고 있는 기업 중 하나인 소프트뱅크는 데, 2017년 11월 향후 3~4년 간 사우디아라비아 내 약 250억 달러 규모의 투자를 발표
- 사우디아라비아는 세계은행(The World Bank)에서 조사한 '창업지수(Starting a Business)'[271]에서 135위를 기록할 만큼 아직 사업적 환경이 열악하며 소위 빌리언 달러(Billion-Dollar) 스타트업이라고 일컫는 성공적인 스타트업 사례는 현재 없는 상황임

주요 사업자

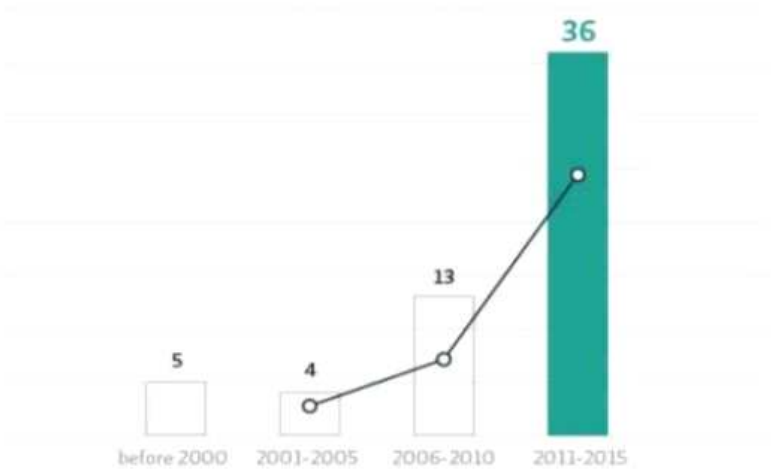
▶ 아람코(Aramco)를 비롯한 사우디 텔레콤(STC), 모빌리(Mobily) 등 사우디를 대표하는 기업들이 스타트업 인프라 구축 및 육성을 위해 막대한 비용을 투자

- 주요 대학교를 중심으로 사우디아라비아 청년들을 위한 교육 등 각종 프로그램들이 신설되고 있음
- 정부에서는 펀드-비(非)펀드 지원, 산학 협력, 디지털 기술 트레이닝 시스템 구축을 위한 테크노 파크 설립 등 주요 도시를 중심으로 스타트업 육성을 위한 다각적인 프로그램을 진행

270 UAE 컨텐츠 산업 동향, 한국 콘텐츠 진흥원, 2017.11 참조
271 http://www.doingbusiness.org/data/exploreeconomies/saudi-arabia

▶ 아랍에미리트(UAE) 스타트업 액셀러레이터 및 리서치 기업 Wamda가 발간한 'The Kingdom of Saudi Arabia: Status of the entrepreneurship ecosystem' 보고서에 따르면 2000년대 중반부터 관련 단체가 증가해 2011~2015년 사이에는 36개의 스타트업 지원기관이 설립된 것으로 조사되고 있음

그림 _ 연도별 사우디아라비아 내 스타트업 지원 단체(기업, 기관 등) 설립 횟수



[출처] The Kingdom of Saudi Arabia: Status of the enterpreneurship ecosystem

주요 동향 및 이슈

▶ 사우디 정부는 'Saudi Vision 2030'이라는 중장기 국가계획의 핵심사항 중 하나인 스타트업 육성을 강화하고 있음

- 국부펀드(PIF) 산하 Badir Program이라는 사우디 국내 및 해외 스타트업 지원 프로그램을 운영하며 다양한 IT 스타트업 창업기반 조성 노력
- Badir Program은 ▲SNS를 통한 마케팅 ▲조달 ▲부동산 거래 지원과 같은 IT 기반 플랫폼 분야의 스타트업 창업을 집중 지원하며, 최근에는 의료 서비스 정보제공 분야 등 다양한 분야로 지원 범위 확대
- 2015년부터 본격적으로 운영하고 있는 해외 스타트업의 사우디 진출을 위한 'Soft Landing Program'은, Healthcare, Pintech, Logistics을 주요 분야로 하고 있으며, 현지 법인설립 행정지원, 사무 공간 제공, 기술자문 및 마케팅, 현지 파트너사 발굴 등을 지원함

▶ 스타트업을 위한 맞춤형 라이선스 프로그램 운영

- 사우디아라비아투자청(Saudi Arabian General Investment Authority, SAGIA)은 2016년 4월부터 혁신적인 서비스와 제품을 개발하고자 하는 인재들의 창업을 독려하고 지원하기 위해 맞춤형 라이선스 프로그램을 운영
- 일명 '혁신기반 라이선스(Innovation-based Licence)'라 불리는 이 프로그램은 킹 압둘라 과학기술대학교(King Abdullah University for Sciences & Technology, KAUST)와 협력해 진행되고 있으며, 다양한 정부 지원 서비스, 투자기회 제공 등의 인센티브를 제공해 스타트업 활성화를 지원

정보보호 정책 및 기관 현황

1) 관련 법령 및 정책

관련 법령 및 규제

▶ 사우디아라비아는 2007년 왕실칙령 제70조에 의거하여 사이버 범죄법을 승인

- KSA에서 사이버 범죄를 저지른 사람에게 적용되며, 규정된 범죄는 형사 범죄로 간주되어 벌금 또는 징역에 의해 처벌될 수 있음
- 사이버 범죄자는 1년에서 최고 10년까지의 징역 또는 1만 리얄~최고 300만 리얄의 벌금형에 처해질 수 있음
- 사이버 범죄에는 해킹, 불법적 금융거래 혹은 신용 데이터 접근, 불법적 개인데이터 유포 및 삭제, 유출 등이 포함
- 사이버 범죄를 구성하는 행동 유형과 그러한 행동과 관련된 제재를 규정하지만, 사이버 범죄 법을 준수하기 위해 사람들이 취해야 할 특정 행동을 규정하지는 않음

▶ 사우디아라비아 통화 당국(Saudi Arabian Monetary Authority, SAMA)이 규제하는 모든 은행, 보험 회사, 금융 회사, 신용 관리국 및 모든 사우디 금융 시장은 SAMA 프레임 워크를 준수해야 함

- 사이버 보안 기능은 KSA에서 검증된 CISO (Chief Information Security Officer)가 주도해야 하며 해당 역할에 대한 자격을 충분히 갖추고 있어야 함
- SAMA 프레임 워크의 적용을 받는 금융 기관도 사이버 범죄 법의 적용을 받으며, 서비스 제공에 따라 통제 대상이 될 수 있음

▶ 정부 기관 및 해당 계열사는 사이버 범죄 법, 정부 명령 및 프레임 워크를 준수해야 하여, SAMA에 의해 규제되는 경우 SAMA 프레임 워크의 적용을 받음

- 정부 기관 및 해당 계열사를 포함한 KSA의 모든 인원은 사이버 범죄법의 적용을 받음
- 규정에 따라 정부 기관은 정보 보안 프로그램을 개발해야 하며, 해당 프로그램에는 /위험 평가 /자산 관리 /정보 액세스 및 보안 사고에 대한 정보 보안 정책 및 절차 문서가 포함되어야 함
- SAMA 프레임 워크는 정부 명령에 따라 정부 기관에 필요한 정보 보안 프로그램을 실제로 구현하는

방법의 구조를 제공

▶ 통신정보기술부(MCIT)가 발표한 국가정보보호전략(NISS) Draft 7에서는 ▲NISS ▲사이버 보안 ▲중요 인프라 보호(CIP)와의 관계를 정의함

- 세 가지 모두 공통되거나 고유한 요소가 있으나, NISS를 구현하면 사이버 보안 및 CIP의 핵심 요소는 그대로 유지됨
- 사이버 보안 및 CIP 전략은 NISS가 다루지 않는 영역을 다루기 위해 NISS와 함께 개발 및 구현되어야 함

그림 _ NISS, 사이버 보안 및 CIP 관계

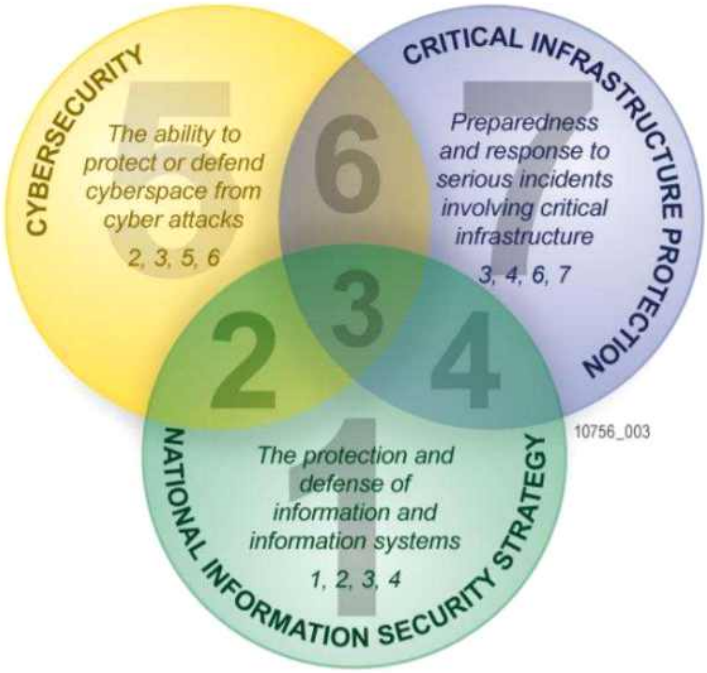


그림 _ 개별 도메인의 고유한 영역과 공통된 영역의 예

영역	도메인	예시
1	NISS 단독	정보 인프라 및 정보 시스템에 대한 컴퓨터 보안 및 암호화 정책, 지침 및 표준
2	NISS와 사이버 보안	사이버 위협 모니터링, 분석, 정보 공유, 위기 관리, 컴퓨터 비상 대응 팀 조정
3	NISS, 사이버 보안 및 CIP	정보 기술 인프라 및 운영 요원에 대한 물리적 및 정보 자산 보호, 전체 위협 스펙트럼 복원력 및 비즈니스 연속성
4	NISS와 CIP	위험 관리 평가 및 의존성 분석
5	사이버 보안 단독	국가 사이버 운영 센터 및 사이버 공격에 대한 대응 능력
6	사이버 보안 및 CIP	SCADA 제어 시스템 보안 및 광범위한 사이버 기반 공격에 대한 대응
7	CIP 단독	테러리스트의 주요 인프라 자산의 물리적 공격에 대한 보호 및 대응 기능

[출처] NISS, DRAFT 7

주요 전략 및 정책

▶ 사우디아라비아 정부는 사이버 및 물리 보안 강화를 위해 해외 기업들과의 협력을 증진하고 있음

- 사우디 사이버보안 및 프로그래밍 연합(The Saudi Federation for Cyber Security and Programming)은 구글과 자국 내 5개의 혁신 센터 구축에 합의하였으며(2019.4), 해당 센터를 통한 사우디 청년 교육 및 전문가 육성으로 인공지능 및 첨단 기술 산업 발전 도모 예정
- 사우디 사이버 안보위원회(The Saudi Cyber Security and Programming Federation, SFCSP)는 사이버 안보 협력 증진을 위한 미국 록히드마틴사와 양해각서를 체결하였으며(2019.3), 이를 통해 사우디 사이버 보안 및 프로그래밍 역량 강화 기여 전망

▶ 사우디 정부는 보안 본부 개발을 위한 King Abdullah 프로젝트 하에서 주요 보안 프로젝트에 대한 작업을 진행

- 이 프로젝트는 2020년 완료 예정으로, 총 1,296개의 보안 사이트를 설립할 계획이며 2018년 말까지 약 551개의 사이트 완성

2) 담당기관

▶ 컴퓨터 비상 대응팀 (Computer Emergency Response Team, CERT)

- CITC 하에서 2006년에 설립되었으며, 공공 및 민간 부문에 대한 사고 관리 컨설팅 서비스를 시작으로 사이버 공격의 영향에 대한 인식과 사건보고의 중요성에 대한 인식을 확산시킴
- CERT의 인식 이니셔티브는 시설에 교육 및 훈련 기능과 함께 사이버 사건 탐지 및 예방 기능을 갖추는 것을 주요 목표로 함
- ▲보안 위협 완화 기술 훈련 ▲교육 캠페인을 통한 사이버 보안 인식 확대 ▲대학과의 협업 ▲사이버 사고 정보, 취약성 및 발견된 공격에 대해 정부 기관을 위한 새로운 사이버 보안 커리큘럼 및 프로그램 개발 서비스 제공

▶ 정보 보증의 우수성 센터(Center of Excellence in Information Assurance, CoEIA)

- ▲사이버 보안 솔루션 개발 ▲사이버 보안 표준 적용 ▲산업, 학계 및 공공 부문의 상담 및 지원에 기여하는 비영리 센터로 2009년 설립
- 자문 서비스 외에도 사이버 보안 연구에 광범위하게 참여하고 있으며 혁신적이고 영향력 있는 사이버 보안 관련 정보 및 인식 캠페인 진행

▶ 사이버 보안 기술 센터(National Center for Cybersecurity Technology, C4C)

- King Abdulaziz City of Technology and Technology(KACST) 하에서 네트워크 보안, 애플리케이션 보안, 정보 보안 및 보안 거버넌스 영역에서의 연구를 위해 2014년 설립
- 국가 인적 자본의 잠재력을 활용하고 KSA 비전 2030의 성공을 위한 토대를 마련하는 역할
- 사이버 보안 연구 및 응용 능력에 유능한 전문가 제공

▶ 2016년에 설립된 국립 사이버 보안 센터(National Cyber Security Center, NCSC)

- 조직이 국제 사이버 보안 표준에 따라 보안 수준을 정의하고 보안 문제를 식별하는 데 도움이 되는 평가 패키지 개발
- 해당 평가를 통해 조직은 기술 취약성을 식별, 검증 및 평가할 수 있으며 IT 인프라의 보안 상태 개선에 대한 심층적인 이해 가능
- NCSC는 수행안 평가를 기반으로 기술 권장

▶ 국가 사이버 보안 기관 (National Cybersecurity Authority, NSA)

- NCA 혹은 NCSA라고도 지칭하며 국가 사이버 보안을 강화하고 국가 인프라를 방어하기 위한 왕령에 따라 2017년 설립
- 사이버 보안 정책, 프레임 워크, 기준 및 지침을 분석, 작성, 위임 및 규제를 주요 목표로 함
- KSA 비전 2030 및 기본 NTP (National Transformation Program)에 따라 국가별 사이버 기능을 구축 및 육성하고 기술 혁신 달성 기여를 목표

3) 규제 및 인증제도

▶ SASO(Saudi Standards, Metrology and Quality Organization)인증

- 사우디 표준청(Saudi Standards, Metrology and Quality Organization, SASO)는 사우디아라비아 표준인증기관으로서, Royal Decree No. M/10에 의거하여 설립됨
- 1985년 제 58회 이사회에서 품질마크제도 및 적합인증서 발행제도(SASO인증)의 도입을 결의하였고, 1986년부터 품질마크 제도 및 적합 인증서 발행제도를 실시함
- 품질마크제도는 사우디 표준청이 사우디 국내 기업 제품에 해당하는 SSA(Saudi Arabian Standards)규격의 적합성을 인증하는 제도로, SSA규격이 모든 제품에 적용되지 않기 때문에 SSA규격이 없는 제품은 ISO 및 IEC와 같은 국제규격 혹은 해당 품목 수출국의 규격을 적용함

▶ 사우디 표준청(SASO)의 신규 인증시스템 SABER

- SASO(Saudi Standards, Metrology and Quality Organization)는 2019년 1월 1일부터 SALEEM(Saudi Product Safety Program) 구현을 위해 온라인 인증 플랫폼 'SABER' 도입
- 기존의 사우디 CoC(Certificate of Conformity) 프로그램을 점진적으로 대처하기 위한 목적
- 현지 제조 또는 수입 여부와 상관없이 사우디 시장 진입을 위해서는 제품 적합성 증명서 및 제품의 출하 적합성 판단을 위한 선적 인증서가 필수적으로 요구
- SABER 전자 등록 의무는 수입업자가 지며, SABER를 통해 제품 적합성 증명서 및 선적 인증서 발급 가능

4) 최근 정책 동향 및 이슈

▶ 사이버 보안, 프로그래밍 및 드론을 위한 사우디아라비아 협회(Saudi Arabian Federation for Cybersecurity, Programming and Drones, SAFCSPD) 설립(2018년)

- 2018년 사우디아라비아 올림픽위원회 산하에 국가 기관으로 설립
- 국제적으로 인정된 관행 및 표준에 따라 사이버 보안, 프로그래밍 및 드론 기술 분야에서 국가 및 전문 역량을 구축을 목표
- 사우디아라비아가 기술 혁신 영역에서 선진국으로의 발돋움하는 촉매 역할 수행

▶ UAE와 사우디아라비아 기관들은 여전히 사이버 보안 사고에 대응할 준비가 되어 있지 않으며, 응답자 31%는 사이버 보안 사고 대응 계획이 마련되어 있지 않다고 밝힘(2019.5)

- 계획을 수립한 조직 중 절반은 정기적으로 계획을 테스트 하지 않기 때문에 공격에 대비한 준비 부족
- 사이버 공격에 30일 이내 신속하게 대응하면 기업의 평균 데이터 유출 비용 대비 백만 달러 이상 절감 가능
- 사이버 보안 사고에 계획적으로 대응하는 것은 복잡하고 전문 지식이 필요하지만 선택 사항이 아닌 필수 사항임
- 개인 정보 보호와 사이버 보안간의 협력이 사이버 복원력을 향상시킨다는 것을 기관들이 인정하기 시작
- 중동지역의 오일과 가스 시설은 해커의 주요 공격 대상이나 아직 사이버 공격에 준비가 안 된 곳이 많고 정기적으로 점검을 하지 않아 보안 준비 태세가 낮은 것으로 파악됨

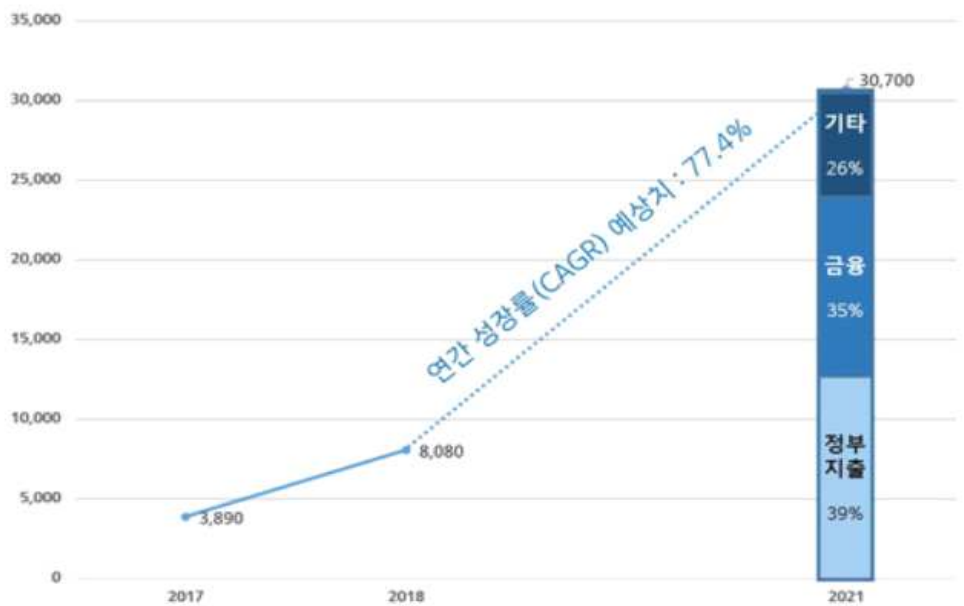
융합보안 시장 및 정책 동향

1) 융합보안 시장 현황

▶ IDC가 발표한 자료에 따르면, 2018년 MEA(Middle East and Africa) 지역의 블록체인 기술 관련 지출액은 2017년 대비 약 2.07배 성장하였으며(2017년 3,890만 달러 → 2018년 8,060만 달러), 2021년에는 CAGR 77.4%로 약 30,700만 달러에 이를 것으로 예상됨

- 2017년부터 UAE와의 협력을 통해 국가 수준의 암호화폐를 창설하기 위한 노력을 지속하고 있으며, 2018년부터 양국이 공동으로 추진하고 있는 '해결 전략(Strategy of Resolve)' 중 하나인 가상통화 발행의 일환으로, 2019년 1월 송금 서비스 비용 절감을 위한 공동 암호화폐 'Aber'의 발행을 위한 시범 테스트 실시에 최종 합의함
- 사우디아라비아 관세청은 머스크-IBM이 공동 개발한 TradeLens 플랫폼을 활용하여 블록체인 기반 물류 플랫폼을 도입하였으며, 해당 시스템을 적용한 첫 선박이 사우디 담맘항에서 출발함

그림 _ MEA 지역의 연간 블록체인 기술 관련 지출액 및 구성 예측치



[출처] Blockchain Spending in the Middle East & Africa to More than double in 2018, IDC, 2018.2

2) 융합보안 정책 현황

블록체인

▶ GCC 5개국 중 블록체인 기반의 암호화폐에 대한 제도적(법적) 기반을 마련한 국가는 아랍에미리트, 바레인 등 2개국이며, 쿠웨이트를 제외한 5개국 모두 블록체인 기술을 국가적 차원에서 도입하고 있음(Cointelegraph, 2018.9 기준 평가 기사)

- 사우디아라비아는 2018년 9월 현재 암호화폐의 제도적 기반은 마련되어 있지 않으며, 블록체인을 국가적 차원에서 도입하려는 의지를 가지고 있음
- 사우디아라비아는 'Vision 2030' 이니셔티브와 '국가개혁 프로그램(NPT) 2020'을 발표하여 다방면의 비석유 분야 육성을 추진하고 있으며, 블록체인 또한 미래 신성장 동력으로 주목하고 있는 기술임
- 사우디아라비아는 국가 암호화폐는 적극적으로 육성하나, 사설 암호화폐에 대한 보수적인 입장을 취하고 있으며, 2018년 8월 사우디아라비아 통화청(Saudi Arabia Monetary Authority)은 국내에서의 비트코인 거래는 불법이라며 외환 시장 관계자들에게 '인가받지 않은 거래'에 참여하지 않도록 경고

스마트시티

▶ 사우디아라비아 정부는 2025년까지 미국 뉴욕의 33배 크기에 달하는 초연결사회인 NEOM을 건설하는 프로젝트 발표[272]

- 석유산업 일변도의 국가산업 구성에 변혁을 일으키고 투자 허브로 거듭나기 위한 거대 프로젝트
- 로봇 집사, 플라잉 카, 인공 강우, 홀로그램 교사 등을 총망라한 첨단과학기술, 익스트림스포츠·게임을 즐길 수 있는 엔터테인먼트 및 휴양과 관광의 중심지 구축 목표
- 1만 평방 마일 크기의 홍해 연안에 총 5천억 달러를 투자해 홍해 연안의 사막에 조성될 예정으로, 1단계 완공은 2025년 예상

272 https://globetrender.com/2019/10/21/saudi-arabia-neom/

마. 이란

'18년 GDP(십억달러)	454.01
'18년 인구수(천명)	81,800

■ ITU 글로벌 사이버보안 지수(Global Cybersecurity Index, GCI)

· 이란의 글로벌 사이버보안 지수 순위는 60위로 전년과 같으며 중상위권에 위치

국가명	2018		2017		전년대비 증감	
	지수	순위	지수	순위	지수	순위
이란	0.641	60	0.494	60	+0.147	-
대한민국	0.873	15	0.782	13	+0.091	-2

■ ICT 관련 주요 지수

· 이란의 전반적인 ICT 발전 수준은 50위권 내외로 중상위권에 위치

지표명	이란		한국	
	점수	순위	점수	순위
IMD 국가경쟁력지수(2019)	-	-	-	28
IMD 디지털경쟁력지수(2019)	-	-	-	10
UNCTAD 전자상거래지수(2019)	76.9	42	89.4	19
ITU 글로벌 사이버보안 지수(GCI 2018)	0.641	60	0.873	15
UN 전자정부 지수(2018)			0.901	3

■ ICT 관련 주요 통계 (ITU, 2018년 말 기준)

· 이란의 의 유선통신 보급률은 약 40%로 타 주요 중동국가들에 비해 높은 반면, 이동통신 보급률은 110% 미만으로 상대적으로 낮은 편

항목	이란		한국	
	가입자수(천 명)	보급률(%)	가입자수(천 명)	보급률(%)
유선전화	30,494	37.28	25,907	50.63
유선브로드밴드	9,806	11.99	21,286	41.60
이동통신	88,722	108.46	66,356	129.67
인터넷 이용률	70.00%		95.90%	

정보보호 산업 개요

1) 보안 환경

▶ 이란 정보보호 시장은 매우 열악하며, 특히 개인정보에 대한 침해가 많이 발생하고 있음

- 이란은 개인정보 유출이 심한 국가로 개인정보 당 최소 1리얄(0.0001달러)에 판매되고 있으며, 이로 인해 스팸, 사기 및 신원도용 등이 빈번히 발생함
- 또한 이스라엘과의 정치적 대립으로 인한 분쟁이 지속되고 있어, 사이버 테러를 이용한 범죄 발생 건수도 지속적으로 증가하고 있음

▶ 2017년 5월부터 본격적으로 등장하기 시작한 전 세계적인 '워너크라이(WannaCry)' 랜섬웨어 사이버 공격의 피해를 입음

- 2017년 7월 현지 언론은 약 2개월간 워너크라이 공격에 대해 보안이 취약한 PC를 중심으로 사이버 공격을 당한 것으로 보도
- MAHER(이란 국가침해사고대응팀)에서 대응을 했음에도 불구하고, 병원과 의료 기관을 중심으로 공격을 받았고, 2,000대 가량의 PC가 감염된 것으로 파악[273]

▶ 2016년 8월에는 주요 산업 시설인 석유화학 공장에서 악성 소프트웨어에 사례가 보고되었음

- 이란 국립사이버공간위원회 (National Cyberspace Council)는 2016년 7~8월 발생한 석유화학 공장 화재들이 산업용 멀웨어와 관련이 있는지에 대한 조사를 진행
- 이란 시민안전국(civilian defense) 관계자는 석유화학 공장의 시스템이 산업용 멀웨어에 감염된 것을 확인, 제거했다고 발표
- 그러나 석유화학 공장 화재와 산업용 멀웨어 감염은 아무런 관련성이 없고, 멀웨어가 실제 활성화되지 못해서, 어떤 악영향도 미치지 못했다고 주장
- 2016년 8월 기준으로 이란 정부는 석유 화학 화재가 사이버 공격으로 인한 것인지 여부를 조사한 결과, 석유 화학 단지 두 곳에서 악성 소프트웨어를 탐지하고 제거하였다고 발표

273 Financial Tribune, "Second Malware Attack Hits Iran", 2017.7.15

2) 인터넷 및 통신 환경

유선 통신 및 인터넷

▶ 시장조사기관 BMI에 따르면 2016년 1월에 이루어진 이란에 대한 제재 해제조치는 향후 이란에 대한 직접투자(FDI)의 증가를 가져올 것으로 예상되며, 2016년 2.9% 수준의 GDP 성장률이 2020년에는 4.8%까지 증가할 전망

- 2014년 하반기, 3G와 4G 데이터 서비스의 등장과 함께 이란의 모바일 시장은 2020년까지 강한 성장세를 유지할 것으로 전망
- 유선 통신시장의 경우 모바일 서비스 시장의 성장을 통한 접근성 제고에 기인하여 성장이 둔화될 것으로 예상됨

표 _ 이란 ICT 시장 및 전망

구분		2013	2014	2016	2016	2017	2018	2019	2020
유선	회선 수 (천개)	28,462	29,316	30,049	30,650	31,120	31,587	32,050	32,509
	가입회선 비율(%)	36.9	37.5	38.0	38.3	38.4	38.6	38.8	39.0
모바일 폰	가입자 수 (천명)	100,966	114,410	129,055	137,701	143,209	147,506	150,456	151,960
	가입자 비율 (%)	130.9	146.4	163.1	172.0	176.9	180.3	182.1	182.2
3G & 4G	가입자 수 (천명)	1,600	9,920	23,213	33,659	41,737	47,997	53,037	57,916
	모바일 시장에서 차지하는 비중 (%)	1.6	8.7	18.0	24.4	29.1	32.5	35.3	38.1
브로드 밴드 인터넷	가입자 수 (천명)	3,695	4,531	5,417	6,403	7,482	8,642	9,865	11,127
	가입자 비율(%)	4.8	5.8	6.8	8.0	9.2	10.6	11.9	13.3

[출처] BMI research (2016)

▶ BMI 자료에 따르면 이란의 모바일 가입자 수는 신규 MVNO 사업자의 등장과 함께 2020년까지 지속적으로 증가하여 약 1억 5,200만 명(182.2%)에 이를 전망

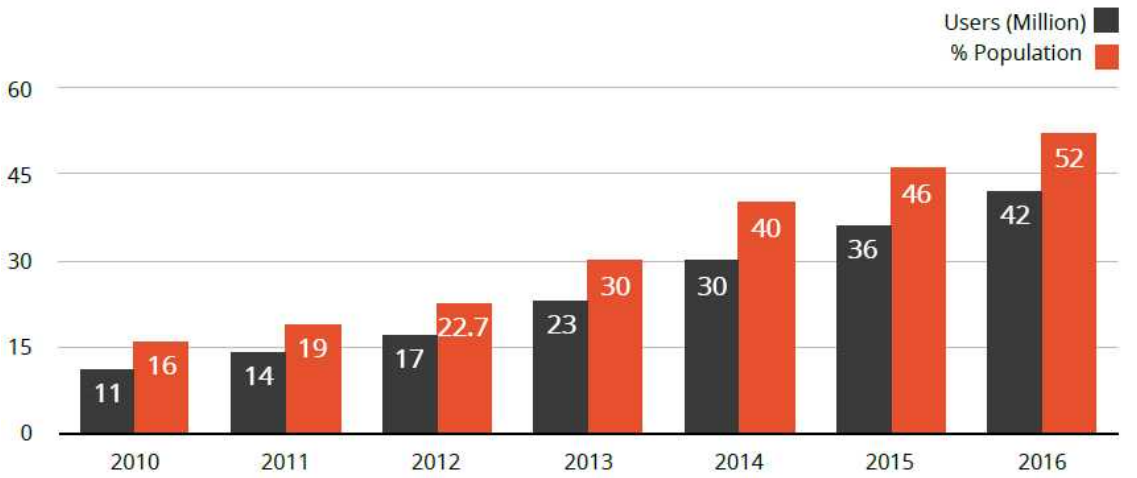
- 특히 2015년 2/4분기 TCI(Hamrahe Aval)가 3G 서비스를 시작하며 해당 분야에서 급속한 성장을 보였으며, 3G/4G 서비스의 경우 전체 모바일 시장에서 차지하는 비중이 2020년까지 계속해서 증가할 것으로 예측됨

- 브로드밴드 시장의 경우 꾸준한 성장세를 보일 것으로 분석되었는데, 2016년부터 2020년까지 연평균 15.5%의 성장률을 기록하여 2020년에는 약 1,110만 명(13.3%)의 브로드밴드 가입자 수를 나타낼 전망

▶ Techrasa 보고서에 의하면, 이란의 인터넷 인프라와 이용자수가 지속적으로 증가하면서, 2016년 말 기준 전체 인구의 52%가 인터넷을 이용하고 있는 상황임

- 이란의 인터넷 이용자수는 2010년 1,100만 명에서 2013년 2,300만 명, 2016년 4,200만 명으로 지속적으로 증가하는 추세
- 또한 인터넷 이용자수가 지속적으로 증가함에 따라, 인터넷 기반의 다양한 서비스들을 일상적으로 이용할 수 있는 환경이 조성 중이라고 분석

그림 _ 이란 인터넷 이용자수 및 보급률 추이



[출처] Techrasa (2016.11)

무선 통신

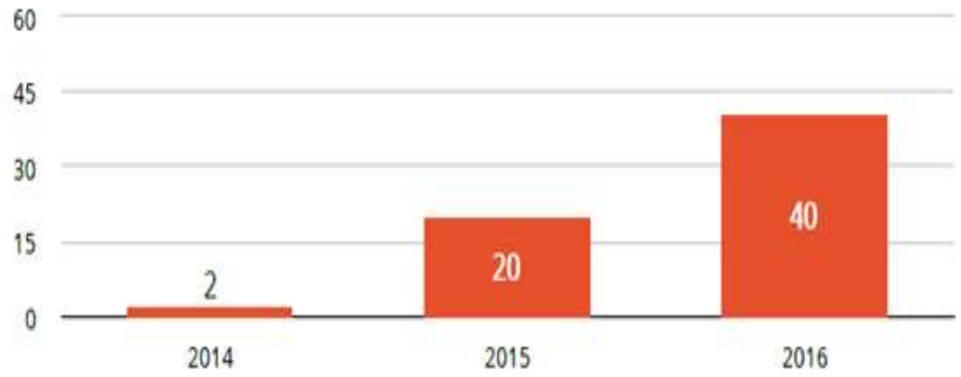
▶ Techrasa 보고서에 의하면, 이란은 스마트폰 이용자의 지속적인 증가와 3G 및 4G로의 모바일 네트워크 구축 전환이 진행되고 있는 만큼, 향후 모바일을 중심으로 하는 통신 및 인터넷 이용 환경이 갖춰질 것으로 전망[274]

- Techrasa는 2016년 이란에서 실제 사용되고 있는 스마트폰의 수가 2013년 대비 20배가 증가한 40만 명이라고 집계

274 Techrasa, "Iran ADtech Overview", 2016.11.11

그림 _ 이란 스마트폰 이용자수 추이

(단위: 백만 명)



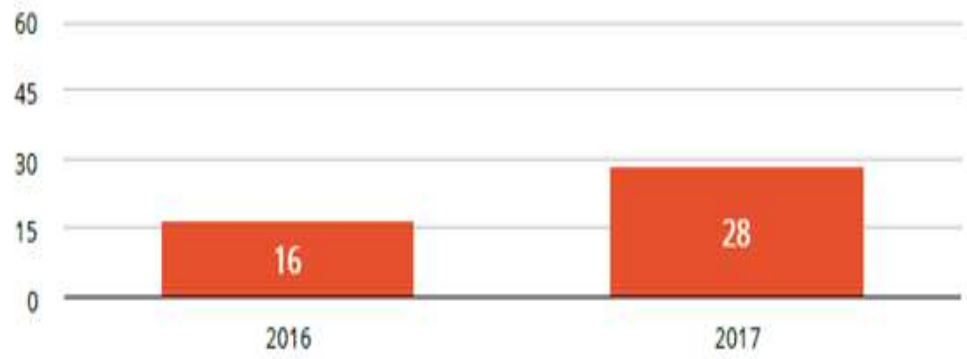
[출처] Techrasa (2016.11)

▶ 이란 이통사들이 2G → 3G → 4G로의 네트워크 전환 및 이용자들의 이동에 따라, 광대역 무선인터넷 시장이 확대될 전망

- 3G와 4G 등 속도와 용량(bandwidth)이 증가한 이동통신 네트워크가 확산되고, 이들 네트워크 가입자 비중이 커질수록 모바일 기반의 서비스 환경도 개선될 것으로 예상
- Techrasa 보고서는 이란의 무선인터넷 이용자수가 2016년 1,600만 명이며, 2017년 2,800만 명으로 증가할 것으로 전망

그림 _ 이란 모바일 브로드밴드 이용자수 추이

(단위: 백만 명)



[출처] Techrasa (2016.11)

표 _ 이란 ICT시장의 SWOT 분석

강점(Strengths)	약점(Weaknesses)
• 높은 모바일 보급률 및 증기하는 가입자 수 • 사업자들 간의 경쟁을 통한 성장과 혁신 • 3G와 4G의 도입으로 인한 모바일 데이터 활용 촉진	• 낮은 ARPU (가입자 당 낮은 수익) • 모바일 데이터 서비스에 대한 정부의 검열 • 한정된 국제 투자 (향후 개선 여지 있음)
기회(Opportunities)	**위협(Threats)**
• 2016년 1월, 제재 해지로 인한 외국인 직접투자 (FDI) 증대 예상 • 많은 미사용 선불 요금제 사용자들의 미래 고객 성장 잠재력 • 높은 스마트폰 전파율과 3G 서비스의 잠재 수요는 사용자의 증가와 이익 성장을 기대 • 발전된 데이터 서비스의 시행은 사업자와 제3자에게 고객과 기업을 위한 데이터 중심 서비스 개발 기회 제공 • 가상이동통신망사업(MVNO)의 등장과 대규모 무선 광대역 허가가 외국 투자자들에게 새로운 기회 제공 • 모바일과 데이터 네트워크의 지속적인 발전 기대	• 정부의 모바일 데이터 및 인터넷 서비스 통제가 수익성 하락을 초래할 수 있음 • 불안정한 정치 및 보안 환경이 장비 제조자들과 콘텐츠 제공자들의 투자를 방해할 수 있음

[출처] BMI research (2016)

▶ 이란의 주요 통신 산업자 현황을 살펴보면, 우선 유 . 무선통신 시장 전반에 걸쳐 서비스를 제공하고 있는 Telecommunications Company of Iran(TCI)이 있음

- TCI는 이란 유선통신 시장을 독점하고 있으며, 모바일 시장에 있어서도 Hamrahe Aval이라는 브랜드를 통해 서비스를 제공하고 있음
- 이란 전기발전회사(Iran Electronic Development Company)와 Mobile Telephone Networks(MTN)이 공동 소유하고 있는 MTN Irancell의 경우 모바일 시장에서 TCI와 함께 독점적 지위를 차지하고 있음

표 _ 이란 통신사업자 근황(2016년 기준)

사업자명	통신시장	지배(소유)구조
TCI (Telecommunications Company of Iran)	• 유선 • 모바일(브랜드명: Hamrahe Aval) • 데이터	• Etemad Mobin: 50% • Equity Shares Brokerage Companies: 20% • 정부: 19.9% • TCI 직원: 5.09% • 그 외: 5%
MTN Irancell	• 모바일	• Iran Electronic Development Company: 51% • MTN: 49%
Taliya	• 모바일	• RIC(Rafsanjani industrial Complex)
MTCE(Mobile Telecommunications Company of Esfahan)	• 모바일	• Telecommunications Company of Esfahan • Province

[출처] BMI resaerch(2016)

정보보호 시장 현황

1) 시장 규모

시장 개요

▶ 이란의 정보보호 시장은 이스라엘 등 주변 국가와의 정치적 대립이 지속됨에 따라, 개인정보보호보다는 정부의 국방 및 안보를 보호하기 위한 정책적인 지원에 주력할 가능성이 높고, 관련 정보보안 시스템 구축에 집중 투자할 전망

정보보호 시장 규모 및 성장률

▶ 시장조사기관 Barnes Reports는 2017년 이란의 정보보호 시장 규모를 아래와 같이 추산

표 _ 2015년 이란 기능별 정보보호 기업 분류

산업	카테고리	총 기업수	총 매출액(백만 달러)	총 고용인원
수사 및 무장 차량 서비스	Major1	1,326	95.3	25,906
가드 (guard)서비스	Minor1	3,086	271.9	19,825
무장 차량 서비스	Minor2	199	48.8	7,484
도난 방지 서비스	Minor2	13	1.1	188
보안견 렌탈 서비스	Minor2	15	1.0	209
보안 서비스, 가드	Minor2	389	331.5	13,552
보안 가드 서비스	Minor2	1,597	593.4	85,814
수색 서비스	Minor1	605	29.0	5,775
수색 요원	Minor2	419	22.8	5,477
지문인증 서비스	Minor2	49	1.4	369
거짓말 탐지 서비스	Minor2	86	2.0	404
사설(개인)수사	Minor2	2,794	82.4	14,945

Major 1: 통상적이고 일반적인 보안 시스템 서비스, Minor 2: 특정 기업 또는 영역에 국한된 보다 세부적인 보안 서비스

[출처] Barnes Report, '2017 World Industry & Market Outlook Security Systems', 2015.12

시장 전망

▶ 이란에 대한 경제 제재의 해제로 사이버 보안 위협이 보다 늘어날 것으로 예상되고 있으며, 이에 따라 해당 시장의 점진적인 성장이 기대되고 있음

▶ 전자상거래 전문 시장조사기관 yStats의 2016년 보고서(IRAN B2C E-Commerce Market)에 따르면, 이란의 전자상거래 관련 동향 및 성장 가능성은 아래와 같음

- 이란의 B2C 전자상거래 시장은 제재 완화 조치에 따라 외국 자본, 투자자, 기술, 기업 등의 광범위한 접근이 예상됨에 따라 많은 발전이 있을 것으로 예상됨
- 이란은 2016년 B2C 전자상거래 지수에서 다른 중동 국가들에 비해 낮은 77위를 기록하고 있으며, 특히 인터넷과 신용카드 부문에 있어서 낮은 수치를 기록
- 이란의 온라인 쇼핑 이용률은 10%로서, 다른 중동 국가들에 비해 역시 낮은 수치를 기록하고 있음 (요르단 27%, 사우디 25%)
- 2016년 말 기준으로 40%의 이란 국민들이 스마트폰을 소유하고 있으며, 3G와 4G 전환이 가속화됨에 따라, 향후 모바일 커머스 시장의 성장 잠재력이 매우 클 것으로 예상됨

표 _ 2016년 글로벌 B2C 전자상거래 지수

2016년 순위	국가	인터넷 보급률 (2014)	신용카드 보급률 (2014)	우편신뢰도 점수 Postal Reliability Score (2014)	B2C 전자상거래 지수(2015)
20	이스라엘	71	76	79	76.1
25	UAE	90	37	86	73.4
26	카타르	91	32	88	72.4
32	바레인	91	28	72	66.5
40	쿠웨이트	79	28	68	61.9
48	레바논	75	11	79	57.4
56	사우디아라비아	64	12	69	52.2
65	오만	70	27	30	48.8
77	이란	39	11	82	42.6
80	요르단	44	2	59	41.3
127	이라크	11	2	16	14.3

[출처] yStats Report, 2016 B2C E-Commerce Market, 2016.05

2) 분야별 현황

▶ 이란의 컴퓨터 하드웨어 시장은 2014년 51억 달러 규모였으나, 2019년에는 71억 달러 규모로 성장할 것으로 예상됨

- 향후 수년간 교육 프로젝트를 위한 정부조달과 전자정부 시스템 구축을 위해 정부의 컴퓨터 설비 수요가 증가할 것으로 전망
- 또한 이란 내 기업들의 경우에도 통신 시스템과 뱅킹 시스템의 현대화를 위해 컴퓨터 구매 수요가 증가할 것으로 예상됨

▶ 이란은 중동지역에서 PC 보급률이 낮은 수준이며 일부 고사양-고가 브랜드 컴퓨터를 제외하고는 이란 자국 내에서 조립 생산됨

- 컴퓨터 부품, 모니터, 프린터와 같은 컴퓨터 주변기기 수요도 함께 발생 (다양화 되어 가고 있는 다른 중동시장에서와 달리 이란에서는 LG와 삼성이 지배적)
- 아직은 판매의 1/3 이상이 데스크톱이지만, 향후 노트북, 넷북, 태블릿으로 수요가 이동할 것으로 예상

3) 주요 사업자 현황

주요 사업자

표 _ 이란에 상주 중인 보안서비스 관련 해외 및 다국적 기업

기업명	활동분야	국적
Arecont Vision	IP네트워킹, CCTV	다국적
BCD Video	CCTV	다국적
CLIQ – ASSA ABLOY	Locks	다국적
Dahua Technology Ltd	Digital video recording	다국적
Delta Scientific Corporation	Thermal imaging	다국적
FLIR Commercial Vision System	CCTV	영국
Hikivision	CCTV	다국적
MOBOTIX AG	CCTV	다국적
Pelco	Digital video recoding	다국적
Promise Technology	Digital video recoding	다국적
Seagate Technology	데이터/영상 스토리지	다국적
Vanderbilt Industries	접근 제어(Access control)	다국적
Vicon Industries	CCTV	다국적
Akuvox Networks	인터콤 시스템	중국
Anviz Global Inc.	바이오보안(Biometrics)	다국적
ASSA ABLOY	접근 제어(Access control)	다국적
Avigilon Corporation	CCTV	영국
Bosch Security Systems	CCTV	다국적
Dallmeier electronic GmbH & Co.KG	CCTV	다국적
DSX Access Systems, Inc.	접근 제어(Access control)	다국적
FUJIFILM Europe GmbH	CCTV	다국적
GEUTEBRUCK GmbH	CCTV	독일
HID Global	접근 제어(Access control)	다국적
Milestone Systems	소프트웨어	다국적
Mirasys Ltd	CCTV	핀란드
Nextchip	반도체	다국적
Optex	침임탐지	다국적
Surveon Technology, Inc.	IP 네트워킹	미국

[출처] www.sourcesecurity.com

정보보호 정책 및 기관 현황

1) 관련 법령 및 정책

관련 법령 및 규제

▶ 컴퓨터 오용 및 사이버 범죄법(Act No.22 of 2003)

- 이란은 2003년 7월에 제정된 "The Computer Misuse And Cybercrime Act 2003"에서 사이버 범죄에 관한 규정들을 명시
- 허가받지 않은 컴퓨터 데이터 접근, 컴퓨터 서비스 이용 및 차단, 불법 기기 및 데이터 소유 등에 대한 허용·처벌 범위를 설정
- 사이버범죄 수사 및 절차를 규정; 관련 데이터 보관 명령, 수사 목적을 위한 데이터 접근·수색·확보, 트래픽 데이터 실시간 수집 등

▶ 컴퓨터 범죄법(Law No.71063)

- 이란은 2009년 5월에 제정된 "Computer Crimes Act"에서 기밀 데이터·컴퓨터·통신을 대상으로 한 범죄 및 데이터 무결성을 해치는 범죄에 관한 규정을 명시
- 컴퓨터 범죄법에 의거하여, 이란은 불법 인터넷 콘텐츠에 대한 검열을 위한 기구인 '범죄 콘텐츠 결정 위원회(Commission to Determine the Instances of Criminal Content, CDICC)' 설립

주요 전략 및 정책

▶ 글로벌 인터넷 차단 정책(국가 정보네트워크)

- 이란은 포괄적인 사이버보안 전략을 수립하고 실행하고 있으며, 동 전략에는 전 세계 인터넷으로부터 이란 전 지역을 차단하는 정책이 포함됨
- 이란은 지난 20여 년간 서방 국가의 문화적 및 성적 콘텐츠로부터 이란 시민을 보호할 목적으로 인터넷에 대한 접근을 제한하고 통제
- 이란은 트위터, 페이스북 등 국제적인 소셜 네트워크 서비스를 포함하여 수십만 개의 인터넷 웹사이트 접속을 차단 중으로, 일부 이용자들은 가상사설망(VPN)을 통해 우회하여 서비스를 이용
- 2008년 12월, 이란 의회는 이란의 국가 정보네트워크(Iran's national information network, ININ)와 인트라넷에서, 글로벌 인터넷 네트워크 접속을 제한하는 법안을 발의[275]

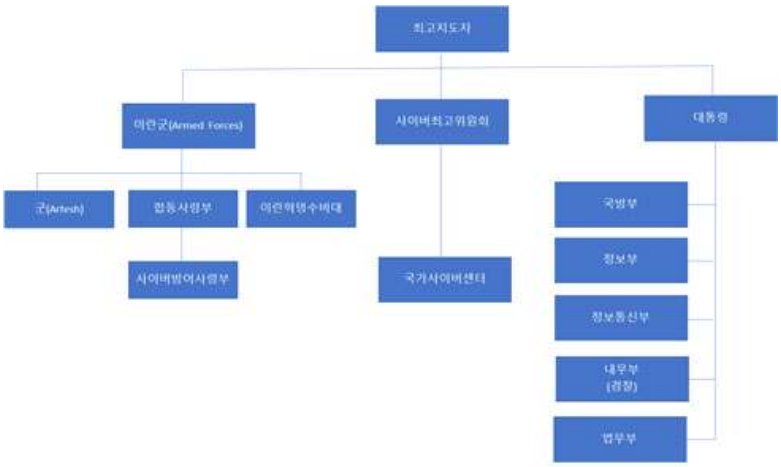
- 2019년 5월, 이란의 문화혁명최고위원회(Supreme Council of the Cultureal Revolution)는 국가정보네트워크가 80% 완료되었다고 발표[276]

2) 담당기관

▶ 개요

- 최고지도자 산하 사이버최고위원회가 사이버보안 관련 정책 방향을 결의
- 국가사이버센터는 사이버최고위원회가 설정한 정책 방향을 기반으로 사이버보안 정책을 개발·시행
- 군은 사이버사령부와 이란혁명수비대를 통해 사이버작전 수행
- 이란 행정부는 정보부, 정보통신부, 내무부(경찰) 등을 중심으로 사이버보안 업무 수행

그림 _ 이란의 사이버 보안 관련 정부 조직체계



▶ 사이버최고위원회(High Council of Cyberspace)

- 2012년 3월에 조직된 사이버최고위원회는 사이버보안 정책 수립 및 조정 역할을 수행하는 사이버보안 최상위 기관으로, 이란의 모든 사이버보안 관련 기관에 대한 감독 수행[277]
- 사이버최고위원회는 대통령, 사법권 수장, 국회의장, 정보부 장관, 정보통신부 장관, 이란혁명수비대 지휘관 등으로 구성
- 사이버최고위원회의 주된 역할은 다음과 같음

275 https://en.radiofarda.com/a/iran-planning-more-control-on-cyberspace-internet/29640710.html
276 https://en.radiofarda.com/a/iran-says-its-intranet-almost-ready-to-shield-country-from-harmful-internet/29952836.html
277 http://farsi.khamenei.ir/tag-content?id=8974

· 사이버공간에서 주요 기반시설을 사이버공격으로부터 보호
· 이란을 대상으로 하는 사이버위협에 대하여 체계적·지속적으로 모니터링

▶ 국가사이버센터(National Center for Cyberspace)
- 최고사이버위원회가 설립한 기관으로, 사이버공간의 위협에 대처하기 위한 종합 기능 수행
- 사이버최고위원회의 결의사항을 사이버보안 하드웨어, 소프트웨어, 콘텐츠 정책 등으로 이행
- 국가사이버센터의 주요 목표는 다음과 같음
  · 이란 자체 웹사이트·온라인 서비스·인프라 개발을 통해 타국에 대한 이란의 인터넷 의존도 최소화
  · 개인의 안전한 온라인 이용에 대해 교육

▶ 이란 통신규제청(Communications Regulatory Authority, CRA)
- 2004년, 정보부와 정보통신부가 설립
- 이란 통신규제청의 주요 목표는 다음과 같음
  ·국가 및 국제 표준에 따라 이란의 ICT 수요를 충족
  ·국가 및 국제 표준에 따라 ICT 국제 서비스 접근성 강화
  ·무선 주파수 스펙트럼 생산성을 극대화
  ·제한된 주소 및 번호 리소스를 활용하여 생산성을 극대화
  ·경쟁, 투명성, 공정성, 도덕성, 혁신을 준수하는 이해관계자들의 권리 보장
  ·이란 ICT의 발전 및 개선에 투자
  ·국제 및 지역 ICT 사회에서 이란의 국가적 이익을 대변

▶ 국가침해사고대응팀(Team Coordination Center Computer Emergency Response, MAHER)
- 이란의 MAHER는 이란 정보통신부(Ministry of ICT)가 설립했으며, 정부 및 민간 전 영역의 사이버침해 사고 대응을 담당
- MAHER의 구체적인 설립 목표는 다음과 같음
  ·이란 내 사이버침해 사고에 대응하는 이란 정보통신부의 전담 조직
  ·정보보안에 관한 정책 입안, 개발, 팀 발전 방법 최적화
  ·국가 사이버공간에서의 보안 역량 조사
  ·정보보안 관련 산하기관 및 민간 기업 지원
  ·유관 조직들과 정상적인 사이버 공간과 관련된 정보 공유 및 커뮤니케이션
  ·모든 팀들 간의 안전한 커뮤니케이션을 위한 메커니즘 개발
  ·아시아 및 전 세계 컴퓨터침해대응조직(CSIRT)에서 이란을 대표하는 회원으로 활동
- MAHER는 2017년 12월, 2개의 부문 아래 7개의 사무국으로 구성

표 _ MAHER의 조직체계

커뮤니케이션 및 운영 관리부문	침해사고 관리부문
· 기술지원 사무국 · MAHER 서비스 기획 및 개발 사무국 · 내부 커뮤니케이션 조정 사무국 · 개발 및 지식 관리 사무국	· 침해사고 조정 및 대응 사무국 · 구조 및 운영 사무국 · 침해사고 및 취약점 분석 사무국

- MAHER의 연락처는 아래와 같음
  - ·홈페이지: www.certox.ir/english
  - ·전화: +(98) 021-42650000
  - ·이메일: cert@certcc.ir

3) 규제 및 인증제도

▶ 표준

- 이란은 국제적으로 인정된 사이버 보안 표준 프레임워크를 보유하고 있지 않음

▶ 표준 개발

- 사이버 보안 표준 개발을 위한 프로그램이나 프로젝트 등이 없음

▶ 인증

- 이란은 국가기관이나 공공분야 전문가의 인증 또는 인가를 위한 사이버 보안 프레임워크를 보유하고 있지 않음
- 보안 제품 및 서비스 시장 진입을 위해서는 선진 시장 등에서 유용한 인증이나 납품 보유 실적 등이 유효할 것으로 예상

4) 최근 정책 동향 및 이슈

▶ 이란-미국 간 사이버공격 감행 정황 포착(2019년 6월)[278]

278 DW, "US hits Iran with cyberattack: reports", 2019.6.23.

- 2019년 5월 호르무즈 해협를 중심으로 한 유조선 공격 사건이 발생하고 이란이 배후로 지목되면서 미국-이란의 갈등이 첨예하게 대립하는 가운데, 이란과 미국은 서로 사이버공격을 감행하고 있다고 보도
- 미국은 이란의 무기 시스템을 대상으로 해킹을 감행하는 한편, 이란은 미국 재무부 직원들의 이메일을 스피어피싱을 통하여 공격하는 등 무력 갈등이 사이버전을 통해 격화되는 양상

융합보안시장 동향

블록체인(가상화폐 포함)

▶ 이란 중앙은행, 은행 및 금융 부문을 위한 국가 블록체인 플랫폼 프로젝트 착수[279]

- Borna 플랫폼으로 불리는 국가 블록체인 플랫폼 구축을 통하여 현재의 낙후된 시스템을 대체하고 디지털 금융경제로의 전환을 도모할 목적
- 미국의 경제 제재 조치 이후 이란 정부가 이를 타개할 방법 중 하나로 고안된 정책으로서 자국의 금융 거래 추적을 어렵게 만드는 시도로도 거론되며, 이와 동시에 금융 산업의 규모 확대 및 개선을 위한 프로젝트이기도 함

279 https://cointelegraph.com/news/iran-developing-national-blockchain-platform-on-ibm-hyperledger-fabric

바. 루마니아

'18년 GDP(십억달러)	239.55
'18년 인구수(천명)	19,470

■ ITU 글로벌 사이버보안 지수(Global Cybersecurity Index, GCI)

· 루마니아의 글로벌 사이버보안 순위는 72위로 전년 42위 대비 큰 폭으로 하락

국가명	2018		2017		전년대비 증감	
	지수	순위	지수	순위	지수	순위
루마니아	0.568	72	0.585	42	-0.017	-30
대한민국	0.873	15	0.782	13	+0.091	-2

■ ICT 관련 주요 지수

· 루마니아의 전반적인 ICT 발전 수준은 중위권 수준을 유지하고 있음

지표명	루마니아		한국	
	점수	순위	점수	순위
IMD 국가경쟁력지수(2019)	-	49	-	28
IMD 디지털경쟁력지수(2019)	-	46	-	10
UNCTAD 전자상거래지수(2019)	74.5	46	89.4	19
ITU 글로벌 사이버보안 지수(GCI 2018)	0.568	72	0.873	15
UN 전자정부 지수(2018)	0.667	67	0.901	3

■ ICT 관련 주요 통계 (ITU, 2018년 말 기준)

· 루마니아의 유선통신 보급률은 약 19%, 이동통신은 116%로 중위권 수준을 보이고 있음

항목	루마니아		한국	
	가입자수(천 명)	보급률(%)	가입자수(천 명)	보급률(%)
유선전화	3,660	18.76	25,907	50.63
유선브로드밴드	5,083	26.06	21,286	41.60
이동통신	22,675	116.25	66,356	129.67
인터넷 이용률	70.68%		95.90%	

정보보호 산업 개요

1) 보안 환경

정보보안 환경

▶ ITU가 발표한 글로벌 사이버보안(GCI) 2018에 따르면 루마니아의 사이버보안 지수는 0.568로 단계로 글로벌 순위는 175개국 중 72위로 나타났으며, 유럽국가 권역에서는 46개 국가 중 38위를 낮은 수준을 기록하고 있어 2017년 글로벌 순위 42위에서 많이 낮아짐을 알 수 있음

- 루마니아는 정보기술에서 보안 분야의 소프트웨어 제품 및 시스템에 대한 프로세스, 도구 및 기술에 관련된 국가 표준을 제정하기 위해 국가 표준화기구(National Standardization Organization)을 설립하였음
- 또한 허용된 국제 표준을 준수하며 기술서비스에 대한 암호화 알고리즘, 인증서비스 및 알고리즘의 표준화 무결성을 테스트함

▶ 루마니아 정보국(Romanian Intelligence Service, SRI)은 루마니아의 여러 금융 기관을 표적으로 하는 대량의 사이버 공격이 2018년 6월에서 8월 기간 동안에 기록되었다고 발표[280][281]

- 루마니아정보국((SRI)은 사이버공격자가 사용하는 방법 중 하나는 은행계좌의 인출한도 없이 돈을 인출하고 있으며, 매일 수 천 건의 사이버 공격이 기관, 단체, 고객을 대상으로 하고, 최근 금융기관에 대한 공격이 증가했다고 밝힘
- 사이버 공격자는 발전된 지속적인 위협(Advanced Persistent Threat, APT) 기술을 사용하여 정보시스템에 접속한 후 정보를 활용하는 방법을 찾음
- 이러한 복잡한 사이버 공격에 대해 루마니아정보국(RIS)은 일부 금융 기관에 공격을 평가하고 잠재적 효과에 대응하기 위한 지원을 제공함

▶ 루마니아 국가침해사고대응팀(CERT-RO)의 사이버 위협 평가 보고서[282]에 의하면, 2017년에 1억 3,820만 건 이상의 사이버 보안 경보(alert)가 수집되어 처리하였으며, 이는 2016년 대비 25% 증가함

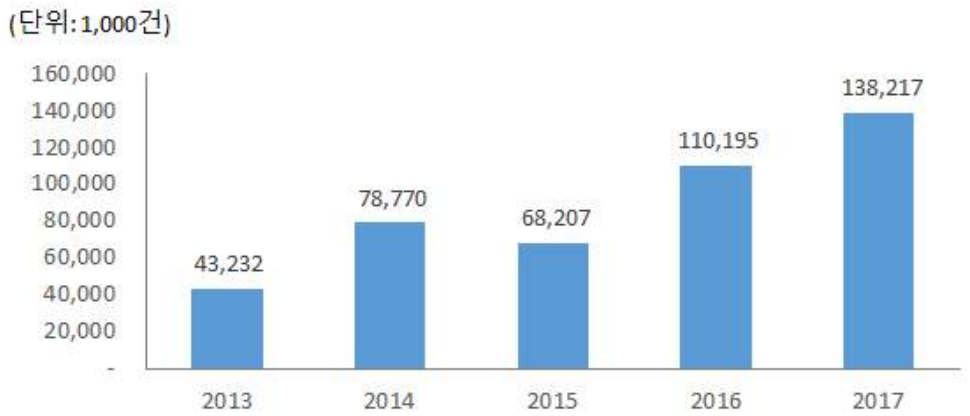
- 2017년 루마니아의 고유 IP 총 개수의 33.71%는 CERT-RO가 처리한 사이버 보안 경보에 적어도 하나

280 "SRI: Many Romanian banks under cyber attack this summer", Business Review, 2018.8.19.
281 "Romanian financial institutions targeted by big cyber-attacks", Romania Insider, 2018.8.20.
282 "Evolution of the Cyber Threat Landscape 2017", CERT-RO, 2018.4.9., p.14.

이상은 포함되었고, 이는 2016년 38.72%에 비해 약 5% 감소함

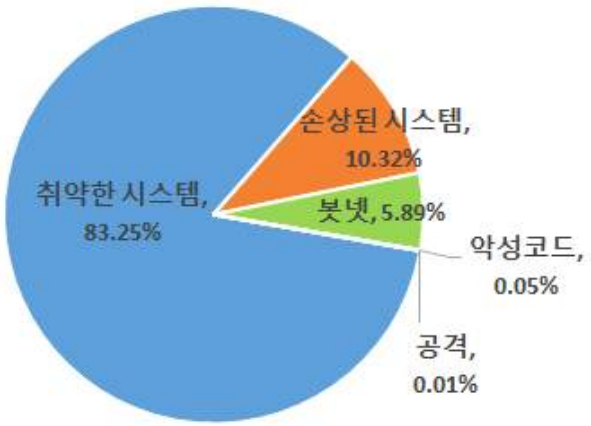
- 2017년 처리된 경보의 83.25%는 취약한 시스템에 의한 것으로, 이는 업데이트 되지 않았거나 보안되지 않거나 잘못 구성된 IT 시스템 등과 같은 취약점을 노리는 공격에 노출되었고, 이는 결과적으로 사용자의 사이버 보안 문화 수준이 상당히 낮음을 보여줌

그림 _ 루마니아 국가침해사고대응팀(CERT-RO)의 수집된 사이버 보안 경보 횟수 추이



[출처] CERT-RO, Evolution of the Cyber Threat Landscape 2017, 2018.4.9. p.14.

그림 _ 수집된 사이버 보안 경고 원인별 분포



[출처] CERT-RO, Evolution of the Cyber Threat Landscape 2017, 2018.4.9. p.14.

▶ 루마니아 사이버 보안 기업, Bitdefender에 따르면, 루마니아는 스크라노스라는 새로운 사이버 보안에서 전 세계에서 가장 취약한 국가임

- 스크라노스는 피해자의 비밀번호 및 은행 정보를 훔쳐내고 소셜네트워크를 통해 보상을 요구하는

랜섬웨어로 루마니아, 브라질, 프랑스, 이탈리아 등에서 위협이 되고 있음

▶ 루마니아는 사이버해커들이 기승을 부리고 있는데 수도 부쿠레슈티에서 2시간 거리에 위치한 름니쿠블체아(Râmnicu Vâlcea)가 사이버 범죄자들의 집결지로 유명함

- 2000년 초반 름니쿠블체아는 여러 사이버 사기꾼들이 가짜 이베이 광고나 경매 사이트를 게시해 순진한 다른 희생자들을 유혹하는 집단 사이버 범죄 마을로 전락함
- 이 마을이 해커빌로 유명해 진 것은 가짜 광고 및 판매사례가 늘어나면서 미연방수사국(FBI)까지 관심을 가진 것으로 알려지면서부터임

물리보안 환경

▶ 국가통신관리규제청(ANCOM)에 의하면, 2017년 루마니아의 통신 네트워크 보안에 영향을 미친 사건은 344건이며, 가장 큰 영향을 받은 분야는 모바일 인터넷과 전화통신에 해당함[283]

- 국가통신관리규제청(ANCOM)에 보고된 중요한 사건은 610만 건의 모바일 음성 연결, 3백만 건의 모바일 인터넷 연결, 1백만 건 이상의 유선 통신 회선, 약 1백만 건의 유선 인터넷 연결에 영향을 미쳤으며, TV 전송은 가장 영향을 받지 않음
- 보고된 사건 수는 작년에 20%까지 증가했으나, 각 사건별 영향을 받은 연결의 평균 수는 38%까지 급감하였으며, 보고된 중대 사건의 약 73%는 정전이나 케이블 고장 등과 같은 외부요인이며, 15%는 시스템 오류, 9%는 날씨에 의한 것임
- 국가통신관리규제청(ANCOM)은 네트워크 보안 사건으로 인해 Telekom Romania에게 총 11만 RON(23만 7,000 유로)의 벌금을 부과하였는데, 3월 5일 Telekom Romania의 모바일 네트워크가 수 시간 동안 고장나서 많은 사용자들에게 영향을 미쳤으며, 2018년 3월 말 기준 Telekom Romania의 모바일 고객은 약 470만 명임[284]
- 국가통신관리규제청(ANCOM)에 의하면 지역 이동통신사는 6개월 동안 등록된 네트워크 고장이 35분을 넘지 않아야 하고, 통신사는 네트워크 가용성 조건을 증명할 수 있도록 6개월 동안 네트워크 로그를 유지해야 하지만 Telekom Romania는 이를 구현하지 못함
- 통신 서비스 제공업체는 네트워크에 영향을 미치는 모든 중요한 보안 및 무결성 사건을 국가통신관리규제청(ANCOM)에게 보고해야 하며, 적어도 한 시간 동안 5,000건 이상의 연결에 영향을 미치는 경우 사건은 중요한 것으로 간주됨

283 "Mobile connections in Romania, most affected by security incidents in 2017", Romania insider, 2018.6.28.
284 "Telekom Romania to pay hefty fine for security incident in March", Rominia insider, 2018.5.24.

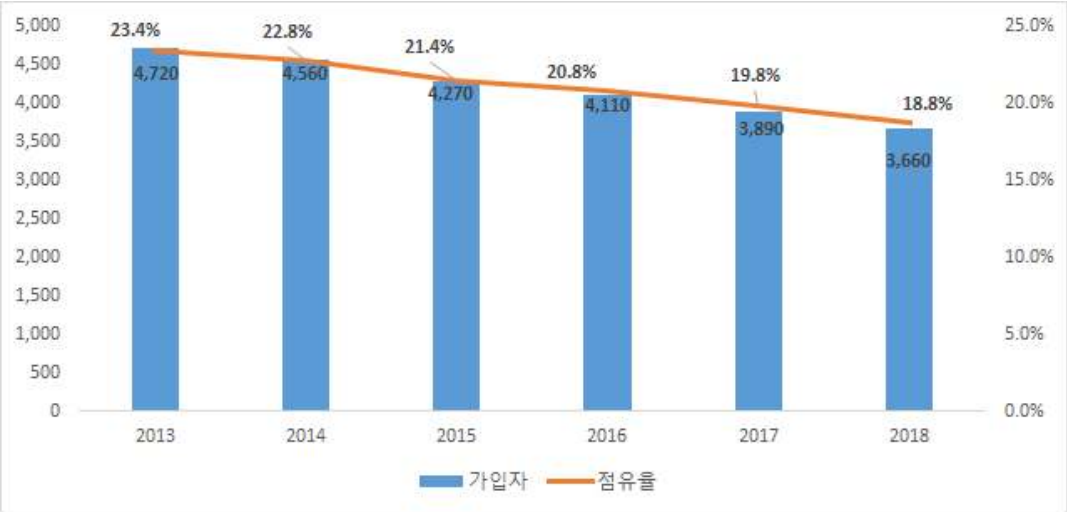
인터넷 및 통신 환경

▶ 유선통신

- ITU에 의하면 2018년 말 기준, 유선통신 가입회선 수는 366만 회선을 기록, 보급률은 18.8%이며, 2017년 366만 회선 대비 0.9% 감소하였으며, 유선통신은 2013년 23.4%에서 지속적으로 조금씩 감소 추세를 보임
- 루마니아의 유선통신 시장은 2003년 시장 개방 후 많은 경쟁업체들이 진출하였으나 기존 사업자인 Telekom Romania의 시장 지배력은 여전히 강하여 시장 점유율이 소매 수익의 약 70%에 달함
- 2017년 6월 기준 34개의 면허를 가진 유선 사업자들이 있으며 이들 중 큰 규모의 사업자로는 RCS&RDS, SN Radiocomunicatii(SNR), GTS Telecom 등이 있음
- 1990년에 설립된 기존 사업자 Telekom Romania은 2017년 6월 기준 가입자에 의한 시장 점유율은 43.7%에 해당하며, 이외 사업자들이 56.3%를 차지하고 있으며, Telekom Romania는 유선 통신, 이동통신, 위성, IPTV, 케이블 TV 서비스의 전체 포트폴리오를 제공함
- 네트워크의 디지털화는 2007년 완료되었으나, 수년간의 자금 부족으로 루마니아는 동유럽에서 가장 낮은 유선 보급률을 보이며 2017년 유선 통신 보급률은 약 20%에 해당함
- 지방에 새로운 유선 연결이 기대됨에도 불구하고 사람들이 업그레이드된 DSL, 케이블, 모바일 네트워크를 통해 모바일 전용 솔루션을 선택함에 따라 유선 보급률은 2013년 이후 조금씩 감소 추세를 보임
- 2014년 초 Telekom Romania는 RoNet 프로젝트를 착수하면서 783개 지역에 약 137,000개의 건물과 40만 주민에게 통신 서비스를 확장하며 2015년 말에 완료될 것으로 예상되었으나 많은 지연이 있었음
- RCS&RDS는 7,500km 이상 길이의 광섬유 백본과 대도시 네트워크를 소유하고 있으며, GTS Telecom은 전국 72.5Gb/s MPLS 네트워크를 구현하였고, Radiocom은 4,000km 길이의 전국 광섬유 네트워크를 운영함

그림 _ 루마니아 유선통신 가입자 수 및 보급률 추이

(단위: 천 명, %)



[출처] ITU Statistics DB (2019.6)

▶ 이동통신

- ITU의 자료에 의하면 2018년 기준 이동통신 가입자 수는 2016년 대비 약 2.3% 상승한 2,267만 명을 기록하며 보급률은 116.3%이며, 2009년 보급률 121.74%를 기록한 이후 최근 3년간 보급률은 약간의 감소 추세를 보이고 있으나 이는 복수 개의 SIM카드 소유권을 선호하는 고객이 줄어든 것으로 분석됨
- 루마니아 이동통신 시장은 네 개의 네트워크 사업자에 의해 제공되고 있으며, 그 중 세 개는 주요한 지역 사업자인 Vodafone Group, Orange Group, Deutsche Telekom의 자회사이며, 이외에 RCS&RDS(Digi) 등이 있음[285]
- Vodafone은 Huawei 장비와 5G SupernetTM 모바일 네트워크를 사용해 5G 서비스를 개시함. 따라서 루마니아는 유럽에서 가장 먼저 5G 서비스를 시작한 나라 중 하나가 되었으며 Vodafone 고객 중 5G 호환기기를 가진 고객이라면 누구든 추가비용 없이 5G를 이용 가능
- Digi Mobil은 2019년 6월 'Digi Mobile 5G Smart' 상용서비스를 개시함
- Orange Romania는 2018년 6월~7월 루마니아 제2도시인 클루지-나포카에서 5G 네트워크를 시험했으며 2020년 5G 상용서비스를 계획 중임

285 "Romania Telecoms Infrastructure, Operators, Regulations-statistics and analyses", BuddeComm, 2017.12.13.

- Orange Romania는 가정의 10% 정도가 5G 서비스를 유선 브로드밴드의 대체로 사용할 것으로 기대하며, 26GHz 대역의 스펙트럼을 사용하여 시행된 시험에서 제한된 수의 단말기에 최대 6Gb/s의 데이터 속도를 제공했음
- Orange는 2012년 말 LTE 서비스를 시작했고, 2016년 LTE-Advanced(LTE-A) 서비스가 뒤따랐으며, 이후 2018년 6월 최대 500Mb/s의 데이터 속력을 제공하도록 업그레이드함
- Vodafone은 2012년 말에 LTE 서비스를 시작했으며, 2016년 9월 약 3,500개 지역에서 LTE-A 서비스를 시작했고, 2017년 10월 최대 800Mbps/속력까지 데이터를 제공하기 위해 업그레이드 하였으며, 2010년~2015년 동안 약 5억 유로를 네트워크에 투자하여 LTE 네트워크 구축함
- Telekom Romania는 2013년 5월 LTE 서비스를 시작했으며, Orange Romania와 도매 네트워크 계약을 통해 2015년 12월부터는 LTE 도달 범위를 확장하였는데, 이 계약을 통해 Orange는 Telekom의 지방 접속 인프라를 통해 고정(fixed) 서비스를 제공할 수 있게 되었고, Telekom은 Orange의 LTE 네트워크에서 전국 로밍 액세스를 확보할 수 있게 됨
- RCS&RDS는 Digi Mobil 브랜드하에 2007년 말 3G 서비스를 개시하였고, 2015년 10월 LTE 서비스를 25개 도시에서 시작하였으며, 2017년 중반까지 Digi Mobil은 2100MHz 대역에 대한 1,100개의 기지국과 2600MHz 대역을 사용하는 1,000개의 기지국을 보유하고 있음

그림 _ 루마니아 이동통신 가입 및 보급률 추이

(단위: 천 명, %)



[출처] ITU Statistics DB(2019.6)

▶ Vodafone의 M-Pesa 서비스는 루마니아에서 2014년 4월 시작되었으며, M-Pesa는 GSM, 3G, LTE 기술에서 운영되는 텍스트 메시징 기술로, 고객은 하루 최대 30,000 레이(약 6,715 유로)까지 이체할 수 있음[286]

• M-Pesa 서비스를 이용하여 선불카드 상환, 공과금 요금 청구, 예금 입금 및 현금 인출, 상품 구매도 가능하며, 이 서비스는 기존 은행 시설에 대한 접근이 부족한 인구의 1/3에게 유용

▶ 인터넷 이용 환경

• ITU의 자료에 따르면 루마니아의 인터넷 이용자 보급률은 2018년 70.7%로 전년의 63.8%에서 6.9% 정도 증가하였으며, 꾸준한 증가 추세를 보임

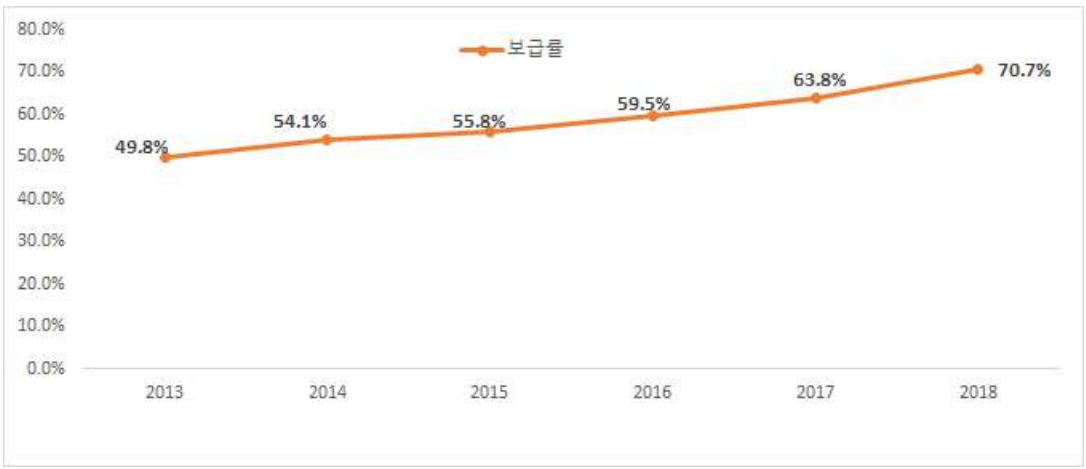
• BuddeComm의 자료에 의하면 2018년 전체 인구에 대한 모바일 브로드밴드 보급률 추정치는 89.2%인 반면, 유선브로드밴드 보급률은 25.1%로 모바일 브로드밴드 사용이 월등히 많게 나타남

그림 _ 루마니아의 플랫폼 별 인터넷 이용률(2018년 기준)

구분	이용자 수	보급률
모바일브로드밴드(e)	17,400,000	89.2%
유선브로드밴드(e)	4,615,000	25.1%
전체	**22,015,000**	-

[출처] BuddeComm(2018.10.)

그림 _ 루마니아의 인터넷 보급률



[출처] ITU Statistics DB(2019.6)

286 "Romania, Mobile Infrastructure Broadband, Operators – Statistics and Analyses", BuddeComm, 2018.7.6. p. 22.

정보보호 시장 현황

1) 시장 규모

시장 개요

▶ 사이버 보안은 루마니아 ICT부문의 핵심 요소에 해당하며, 루마니아의 IT 시장은 중동부 유럽에서 가장 빠르게 성장하는 시장 중 하나로 IT 시장은 2017~2021년에 3.1% 성장하여 2021년 99억 RON(24억 7,000만 달러)의 가치에 이를 것으로 전망[287]

- 루마니아의 IT서비스에서 소프트웨어 시장은 높은 속도로 크게 성장, 중장기적으로 GDP에 가장 중요한 기여를 할 것으로 보이며, 2000년 이후 소프트웨어 산업은 매년 15~20%씩 성장하고 있음
- 코딩과 사이버 보안 영역에서 훈련을 받은 약 2,500명의 학생들이 있으며, 그 수는 증가하고 있으며, 2017년 현재, 루마니아 교육부는 모든 공인된 학교의 모든 K5-K8 어린이들에게 필수적인 훈련으로 일부 사이버 보안 개념이 포함된 코딩을 도입하였고 현재 모든 K1-K12로 확대하고자 함
- 사이버 보안 보호 프로그램을 가장 필요로 하는 곳은 정부이며, 보건 부문은 특히 보건 시스템에 의해 관리되는 많은 양의 개인 데이터로 인해 사이버 보안 서비스의 가장 큰 구매자가 될 수 있음

시장 규모 및 전망

▶ 시장조사기관 Barnes Reports는 2017년 루마니아의 보안 시스템 서비스 산업 시장 규모가 약 2억 6,100만 달러에 달하며, 전년 2억 4,700만 달러 대비 5.7% 성장

- 보안 시스템의 세부 항목으로는 보안 시스템 서비스, 도둑 경보 관리 및 모니터링, 화재 경보 관리 및 모니터링 관련, 보호 장치와 보안, 감시 시스템 등이 포함됨
- 2018년에는 보안 시스템 서비스 산업 시장 규모가 전년 대비 4.5% 감소하여 약 2억 4,900만 달러에 그칠 것으로 전망
- 2017년 보안 시스템 서비스 산업 내 총 2,256개 기업이 설립되어 약 10,958명을 고용, 2018년에는 3.1% 증가하여 총 설립되는 기업수가 2,327개에 이르고, 고용은 3.1% 증가하여 약 11,301명을 고용할 것으로 전망
- 세부적으로 2018년에는 ▲보안 시스템 서비스 1억 7,470만 달러 ▲ 도둑 경보 관리 및 모니터링 관련 8,650만 달러 ▲보호 및 보안 장치 1,210만 달러 ▲감시 시스템 690만 달러 ▲화재 경보 및 감시

287 "Romania - Information Technology/Cybersecurity", U.S. export.gov, 2018.7.11.

관련 620만 달러 규모로 시장 배분될 것으로 전망

▶ 루마니아의 IT 부문은 지난 10년 동안 꾸준히 성장해 왔고 전문가들은 이러한 추세가 더 가속화될 것으로 예상함

- 현지의 여러 IT 회사들은 국제 기업용 소프트웨어를 만드는 것을 넘어 성공적으로 수출한 자체 브랜드를 개발하였고, 또한 해외기업을 인수하여 해외로 진출하기도 하는데, 루마니아의 첫 번째 기술 유니콘인 소프트웨어 플랫폼 UiPath 외에 TotalSoft, Tremend 및 Bitdefender 등이 있음
- 지속적인 혁신을 추구하는 지역 기업들의 등장 뿐만 아니라 Microsoft, HP, Oracle 등과 같은 글로벌 IT 기업들도 루마니아 지역의 스타트업들의 발전을 돕고 있으며, 지역의 통신 회사, 은행, 상공회의소 등도 스타트업을 후원하는 조력자 역할을 하면서 루마니아의 기술 스타트업은 지속 성장 중임
- 정부지원으로 루마니아 산업통상자원부에서는 2017년 6월 Start-Up Nation 프로그램을 실시하여 기준을 충족시키는 신규기업에게 43,900유로까지 지원하며, 해당 예산은 국가 예산 및 EU 기금을 통해 총 3억 7,300만 유로가 책정됨[288]

▶ Statista은 2018년 루마니아의 스마트 홈 보안 부문 매출을 1,100만 달러로 예상하고, 향후 2018년~2022년 사이에 연 평균 40.2%의 성장률을 보이며 2022년에는 시장 규모가 4,200만 달러에 이를 것으로 전망함[289]

- 현재 보안 부문의 스마트 홈 당 평균 매출은 237.16 달러에 해당하며, 2018년 가구 보급률은 0.7%, 2022년에는 3.1%에 이를 것으로 전망함

2) 주요 사업자 현황

시장 특성 및 경쟁 강도

▶ 루마니아에서 사이버보안 시장은 여전히 부상하고 있으며 루마니아는 유럽에서 가장 높은 기술노동자 비율을 자랑하고 있음

- 루마니아의 사이버 보안 시장은 미국 공급업체와 같은 외국 업체에게도 개방되어 있으며, 시장 진입자는 다양한 유럽연합 및 루마니아 시장 규제를 파악해야만 함
- 시장 진입은 현지 루마니아의 채널 파트너를 통해 판매하는 것이 해외 제조업체가 위험을 최소화하는 시장 진입 전략임

---

288 "2017년은 루마니아 스타트업 최고의 해", KOTRA 해외시장뉴스, 2017.11.14.
289 "Smart Home Report 2018 – Security- Romania", Statista, 2018.

- 그러나 루마니아 정부 부서에 판매할 경우, 특히 국가 안보 관련 프로젝트를 위해 타 업체와 경쟁할 때에는 루마니아에 직접 사업체를 설립해야 하는 것이 필수적일 수도 있음
- 루마니아 시장에 관심 있는 외국 기업에게는 사이버 보안에 가장 중요한 지역 협회인 ANSSI(www.anssi.ro)와 협력하여 파트너를 찾는 방식이 최상의 접근이며, ANSSI는 공공부문에 대한 시장 및 사업 기회에 대한 정보를 제공

주요 사업자

❑ 정보보안 시장

▶ Bitdefender

- Bitdefender는 2001년 설립되어 현재 세계 최고의 사이버 보안 및 안티-바이러스 소프트웨어 회사 중 하나에 속하며 본사는 루마니아 부쿠레슈티에 위치하며 미국, 유럽, 중동 등에 사무소를 둠
- 전 세계 150개 이상의 국가에서 정부 기관, 대기업, 중소기업, 개인과 협력하여 전 세계에서 약 5억 명의 사용자를 지원하며, 1,300명 이상의 직원과 600명 이상의 공학자 및 연구원으로 구성된 팀이 있으며, 2014~2016년 동안 매출액의 연평균 성장률은 약 30%에 달하며 72개의 특허를 갖고 있음
- 루마니아인 사업가 Florin Talpes가 Bitdefender를 지배하고, 런던 기반 사모 펀드 Vitruvian Partners가 30% 지분을 보유하며, 미국, 프랑스, 독일, 덴마크, 스페인, 이탈리아, 영국, UAE, 스웨덴, 캐나다 등과 같은 시장에서 직접 진출하였고, 최근에는 현지 파트너인 SMS eTech로부터 자산을 인수한 후 직접 호주로 진출함[290]
- 연락처 : Home Page : www.bitdefender.com, Tel. : +40 31 620 4235

▶ Safetech Innovations

- Safetech Innovations는 2011년에 설립되었으며, 루마니아에서 소프트웨어 보안, 정보 보안 관리, 정보 보안 거버넌스, 정보 보안 위험 평가 및 관리 등의 분야에서 서비스 및 제품을 공급하며, 사이버보안 'one stop shop' 솔루션을 제공하여 조직의 사이버 복원력을 증가시키고 사이버 보안 문제 해결을 지원함
- Safetech Innovations는 NATO 산업 사이버 파트너십(NICP)의 회원이며, Check Point社의 클라우드 보안 전문(Check Point Certified Cloud Security Professional, CCSP) 인증 취득
- 공공 행정, 은행 및 금융 서비스, 헬스케어, 교육, IT 서비스, 통신회사, 전자 상거래 등의 산업 부문에 보안 관련 제품 및 서비스를 공급하며, 루마니아 부쿠레슈티에 본사가 있고, 영국에도 사무소가 위치함

290 "Going global: Romanian IT companies that have grown into international brands", Romania Insider, 2018.10.3.

- 연락처 : Home Page : www.safetech.ro, e-Mail : office@safetech.ro, Tel. : +40 21 316 0565

▶ Bit Sentinel

- Bit Sentinel은 정보보안 회사로서 사이버 침투 테스팅, 악성코드 방지, 보안관리, 사이버 공격 복구, 사이버공격 시뮬레이션, 보안 감사 등 다양한 서비스를 제공하며, 또한 정보 보안에 대한 특별 훈련 코스를 제공
- 공공 부문, 은행 및 금융 서비스, 통신회사, 기업, 스타트업, 중소기업, 교육, 전자 상거래 등의 산업 부문에 보안 관련 제품 및 서비스를 공급하며, 루마니아 부쿠레슈티에 본사가 있음
- 연락처 : Home Page : bit-sentinel.com, e-Mail : contact@bit-sentinel.com

❑ 물리보안 시장

▶ UTI Group

- UTI Group는 정부, 공항 및 항구, 에너지, 석유 및 가스, 화학산업, 원자력 등 중요한 인프라를 위한 방위 및 보안 시스템의 통합 업체이며, 핀란드, 노르웨이, 폴란드, 불가리아, 우크라이나, 우즈베키스탄 등 여러 국가뿐 아니라 NATO 연합 지상 감시 프로그램 등의 프로젝트를 수행함
- UTI Group는 감시, 방어, 분석, 범죄 조사를 위한 특수 제품을 포함한 물리 보안 및 정보 보안 제품 및 서비스와 함께 보안 감사, 시스템 통합, 컨설팅 서비스, 유지관리 서비스도 제공함
- 1990년에 설립된 루마니아에 기반을 둔 회사로 루마니아 부쿠레슈티에 본사를 두고 있으며, 네덜란드, 폴란드, 불가리아, 몰도바 등에 사무실을 두고 있으며 1,800명 이상의 직원이 근무함
- 연락처 : Home Page : www.uti.eu.com, e-Mail : office@uti.eu.com, Tel. : +40 21 201 2300

▶ Mac Douglas Grup

- Mac Douglas Grup은 주로 카메라, 렌즈, 모니터, 디지털 비디오 기록기, 비디오 처리기, 전원 공급 장치 케이블 등과 같은 전체 범위를 갖춘 전문 CCTV 장비를 루마니아 시장에 유통
- 연락처 : Home Page : www.macdouglas.ro, e-Mail : oferte@macdouglas.ro, Tel. : +40 21 252 7570

3) 주요 동향 및 이슈

▶ 인도 대표 IT기업 Infosys는 루마니아 부쿠레슈티에 사이버보안센터 런칭을 발표함(2019.7)

- 센터는 24/7 사이버보안 모니터링 및 보호 서비스를 유럽 및 글로벌 비즈니스 고객 등에게 제공할

계획으로 해당 서비스에는 사이버 모니터링, 관리, 교정, 위협탐지, 보안분석 및 보안사고 복귀 수행 등 다양한 서비스를 제공할 계획임

- Infosys는 루마니아 현지 인력 채용을 늘리고 및 현재 인력에 대한 훈련 강화를 통해 루마니아 보안 사업을 확장하고 있음

▶ 사이버 보안 그룹 Bitdefender, 사이버 보안 중심 창업보육센터 투자 계획(2018.6)[291]

- 사이버 보안 그룹 Bitdefender의 창업자 Florin Talpes는 사이버 보안에 중점을 둔 창업보육센터(start-up incubator)에 투자할 계획
- Bitdefender가 스타트업에게 pre-seed 투자를 계획하고 있으며, 기술 검증, 시장에서 이러한 기술 배치에 대한 이해, 시장 진입 전략 초안 작성 및 계획과 관련된 조언을 제공할 계획
- Bitdefender는 창업 보육 센터에 지원하고자 하는 스타트업을 위한 안내서를 출시할 예정임

4) 정보보호 스타트업 시장 현황

▶ 루마니아 기업가 Clever Taxi 공동설립자 Mihai Totaru는 루마니아 사이버 보안 스타트업 Appsulate에 투자하기로 결정함(2108.7)

- Appsulate는 보스턴에 본사가 있으나 개발팀은 부쿠레슈티에 있으며 데이터 손실이나 데이터를 방지하기 위해 가상 방어체계를 사용하여 사이버 공격을 방어함

291 "Bitdefender launches start-up incubator", Romania Insider, 2018.6.13.

정보보호 정책 및 기관 현황

1) 관련 법령 및 정책

관련 법령 및 규제

▶ 컴퓨터 관련 범죄 조항(형법 개정)[292]

- 2014년 2월 1일부터 새로운 컴퓨터 관련 범죄내용을 포함하며, 컴퓨터 사기, 전자 지불 및 금융사기, 개인 인증 정보 도용 등의 내용을 포함
- 컴퓨터 사기와 관련하여 데이터 입력, 변경, 삭제, 접속 제한, 컴퓨터 시스템 작동 방해 등으로 손해를 초래한 경우 2~7년 징역형
- 전자 지불 수단 도용, 개인 인증 정보 도용의 경우 2~7년 징역형, 위조 전자 지불 및 전자 금융 사기의 경우 1년~5년 징역형
- 전자 지불 수단 위조, 컴퓨터 데이터 위조, 컴퓨터 시스템에 불법적인 접속, 컴퓨터 데이터 전속의 불법적인 차단이나 가로채기, 데이터 무결성 변경 등과 같은 내용도 포함
- 또한 아동 포르노의 컴퓨터 시스템에서 저장 및 유통, 전자 투표 사기 행위에 대한 내용도 규정

주요 전략 및 정책

▶ 루마니아 디지털 어젠다 2020[293]

- 루마니아는 유럽디지털어젠다 2020(Digital Agenda for Europe 2020)을 차용해 루마니아 디지털 어젠다 2020(Digital Agenda for Romania 2020) 국가 전략을 수립하여 2015년 2월에 승인
- 디지털 어젠다는 유럽 2020목표를 충족시키기 위해 ICT 사용의 주요 역할을 정의하고, 디지털 어젠다에 대한 국가전력을 다음과 같이 4개 실행영역으로 설정
  - 전자정부, 상호운영성, 사이버 보안, 클라우드 컴퓨팅 및 소셜 미디어 : 행정을 현대화하여 루마니아의 공공부문의 효율성을 높이고 비용을 절감하는 것을 목표로 하는 분야
  - 교육, 문화 및 보건에서의 ICT : 각 부문별 수준에서 기술을 지원하는 것을 목표로 하는 분야
  - 전자상거래, ICT에서의 연구, 개발 및 혁신 : 루마니아 지역의 비교 우위를 목표로 하며 민간 부문의 성장을 뒷받침하는 분야

292 "romanian cybercrime & computer crime legal blog", http://www.en.criminalitate.info, 2014.9.2.
293 "National Strategy on the Digital Agenda for Romania 2020", Romanian Government http://gov.ro/en/government/cabinet-meeting/national-strategy-on-the-digital-agenda-for-romania-2020

- 브로드밴드 및 디지털 인프라 서비스 : 사회적 포용 확보를 목표로 함

• 루마니아에서 ICT 부문의 전략적 비전의 완전한 이행을 위하여 약 24억 유로의 총 투자가 이루어질 것이며, 경제에 대한 직접 및 간접 영향은 2014년~2020년 동안 GDP 성장 13%, 일자리 수 증가 11%, 행정비용 절감 12%에 이를 것으로 봄

▶ 차세대네트워크(NGN) 인프라 개발 국가계획[294]

• 2015년 6월 정부는 브로드밴드 네트워크를 루마니아 전역의 커버리지와 더 빠른 접속을 위해 차세대네트워크(NGN) 인프라 개발에 대한 국가 계획을 승인하였으며, 2015년 4월에 승인된 루마니아 2020을 위한 디지털 어젠다에 대한 국가전략에 따라 진행됨

• 2020년까지 모든 건물에 최소 30Mb/p의 광대역 서비스를 목표로 하는 유럽연합(EU)의 목표에서 출발했으며, 모든 건물의 적어도 절반이 100Mb/s 서비스를 제공해야 하며, 이 목표는 2025년까지 진행되도록 갱신되었음

▶ 루마니아는 국가 사이버 보안 전략을 2013년 채택하였으며, 국가보안과 정부의 중요한 지원을 구성하는 국가 사이버 인프라를 기반으로 탄력성과 신뢰도가 높은 안전한 가상환경을 정의하고 유지하여, 시민, 기업, 루마니아 사회 전반에 걸쳐 이익을 최대화 하고자 함

• 루마니아의 사이버 보안을 보장하기 위해 목표를 다음과 같이 설정함

- 규제 및 제도적 프레임워크를 사이버 위협 역학에 적용
- 루마니아의 사이버 보안에 대한 취약성, 위험 및 위협에 대한 이해, 방지, 싸움을 통해 보안 확보
- 사이버공간에서 국가 이익, 가치, 목표를 증진할 수 있는 기회를 이용
- 사이버보안분야에서 국내 및 국제 수준에서 공공 및 민간 부문 간의 협력을 증진하고 발전시킴
- 사이버공간에서 유래된 취약성, 위험, 위협과 정보시스템의 보호를 보장할 필요성에 대한 국민의 인식을 고양시켜 보안 문화 개발
- 사이버공간 사용에 관한 일련의 국제적인 신뢰구축 조치를 정의하고 수립하는데 루마니아가 참여하는 국제기구의 새로운 계획에 적극적으로 참여

• 국가 사이버 보안 시스템(National cyber security system, NSCC)은 학계와 비즈니스, 전문 협회 및 NGO 단체들과 협력을 통하는 것을 포함하며, 사이버 보안을 위하여 국가적 차원에서 책임과 역량을 가진 공공 당국과 기관을 통합하는 일반적인 협력 프레임워크임

• NSCC의 임무는 국가 사이버 보안 인프라에 영향을 줄 수 있는 사이버 공간에 특정한 위협, 취약성, 위험에 대한 지식, 예방, 대응 요소를 제공하는 것임

294 "Romania Telecoms Infrastructure, Operators, Regulations-statistics and analyses", BuddeComm, 2017.12.13.

- NSCC의 주요 기능은 정보, 모니터링, 보급, 분석, 경고, 조정, 결정, 대응, 복구 및 인식, 사전 대책 및 대응 조치의 채택을 통해 달성됨
- 최고 국방위원회는 NSCC 활동의 전략적 수준을 조정하는 권한을 갖고 있으며, 루마니아의 사이버 보안 전략을 승인하고 사이버 보안에 관한 위원회 운영의 조직 및 기능의 규칙을 승인
- 사이버보안 운영위원회(Cyber security operative Council, COSC)는 NSCC의 단일 조정을 통한 조직임

2) 담당기관

▶ 루마니아 국가침해사고대응팀(Romanian National Computer Security Incident Response Team, CERT-RO)[295]

- CERT-RO 설립은 루마니아 정부 결정 H.G. 494/11 May 2011에 의해 위임되었으며, 사이버 보안 분야에서 연구, 개발, 전문지식을 보유한 루마니아 국가의 CERT로서 독립된 조직으로 설립
- 사이버 사건을 예방, 분석, 식별, 대응하는 책임을 지는 특화된 조직이며 CERT-RO는 유사한 조직들에 대해 국가 연락 조직에 해당함
- CERT-RO는 국가 사이버 공간에서 발생하는 사고를 예방하고 방지하기 위해 공공 정책을 정교하게 배포하는 책임을 짐
- CERT-RO가 제공하는 서비스는 사고 분류, 사고 조정, 사고 해결 등의 사고 대응과 정보 교육 행사, 처리된 보안 사고 기록 유지, 감사 서비스 등과 같은 예방적 활동을 함

▶ 정보사회통신부(MCIS)

- 정보사회통신부(Ministry for Communication and Information Society, MCIS)는 루마니아의 정보통신기술 산업을 총괄하는 정부 부처
- 2008년 12월 전신인 통신정보기술부(Ministry of Communication and Information Technology, MCIT)를 대체함
- 정보사회통신부(MCSI)는 전자통신, 정보기술, 정보사회 서비스 부문의 정책 입안, 전략 수립, 정책실현을 위한 규제 마련을 담당

▶ 국가통신관리규제청(ANCOM)[296]

- 국가통신관리규제청(National Authority for Management and Regulation in Communications,

295 CERT-Ro 웹사이트: https://cert.ro/
296 ANCOM 웹사이트: http://www.ancom.org.ro/en/ancom_106

ANCOM)은 루마니아 통신 사용자의 이익을 보호하고 통신 시장의 경쟁을 촉진하며, 부족한 자원을 관리하고 인프라에 대한 혁신과 효율적인 투자를 장려함

- ANCOM은 관련 관리 분야의 경험과 전문지식을 갖춘 두 기관인 통신정보기술검사국(Inspectorate General for Communications and Information Technology, IGCTI)과 국가통신정보기술사무국(National Regulatory Authority for Communications and Information Technology, ANRCTI)의 합병으로 2009년 초에 설립됨
- ANCOM은 2018년 실행계획(ANCOM's 2018 Action Plan)을 발행했으며, 실행계획에는 전자통신 인프라, 서비스에 관련된 규제, 주파수 관리, 전자통신 네트워크의 보안 및 무결성 등에 대한 내용을 포함함

▶ 루마니아정보국(SRI)[297]

- 루마니아정보국(Romanian Intelligence Service, SRI)은 국가 안보를 보장하기 위한 기관으로 사이버 보안은 루마니아정보국이 전문가의 전문성을 통해 유럽-대서양 수준에서 주목받았던 분야 중 하나이며, 디지털 시대에 필수적인 사이버 보안 분야에서 지역적 중추 역할을 강화
- 루마니아정보국(SRI)의 국가사이버정보센터(National Cyberint Center)는 국가방위최고이사회(Supreme Council of National Defense, CSAT)에 의해 사이버 정보 분야에서 국가 당국으로 지정되어, 루마니아의 사이버 보안에 대한 취약성, 위험, 위협을 식별하고, 방지하며 대응하기 위해 노력해 옴
- 2017년 5월 루마니아정보국은 CyDEx17이라는 최초의 국가 사이버 보안 훈련을 조직하였고, 이 훈련은 사이버 사고를 관리하는 방법, 운영단계에서 전술적 전략적 대응을 테스트 하고 평가하는 것을 목표로 함[298]

▶ 루마니아 사이버보안연구센터(CCSIR)[299]

- 루마니아 사이버보안연구센터(Cyber Security Research Center from Romania, CCSIR)은 단기, 중기, 장기적인 정보 보안 분야의 파트너십과 같은 국제 활동뿐 아니라 루마니아의 정보 보안 분야에서 보안 연구 촉진, 지원, 구현, 조정하는 목적을 가진 비정부 조직(NGO)임
- 2013년 설립된 CCSIR은 다음과 같은 다양한 활동에 참가함
  - 정보보안 분야의 전문기술에 참여, 새로운 기술 개발 및 새로운 정보 보안 시스템의 통합
  - 정보보안 범위 연구
  - 정보보안 분야의 위협을 완화하는 목적으로 핵심 국제 조직과의 파트너십 개발

297 Romanian Intelligence Service(SRI) 웹 사이트: www.sri.ro
298 https://cyberwiser.eu/romania-ro
299 Cyber Security Research Center from Romania(CCSIR) 웹사이트: http://ccsir.org/

- 정보보안의 품질을 향상시키기 위해 정보시스템의 취약 부분 조사
- 대중 매체 캠페인 및 보안 컨퍼런스 개최
- 지역의 IT 발전 프로젝트 참여 및 프로젝트 개발

3) 규제 및 인증제도

▶ 루마니아에는 정보보호와 관련된 별도의 인증제도가 없는 것으로 조사됨

4) 최근 정책 동향 및 이슈

▶ 루마니아와 이스라엘 양국은 사이버보안포럼 추진을 위한 MoU를 체결(2019.6)
- 루마니아-이스라엘 사이버 포럼은 양국 기업의 미팅을 주선하기 위한 목적으로 설립

▶ 루마니아 의회, GDPR 시행법 승인(2018.6)[300]
- 유럽연합에 의해 고안된 GDPR은 유럽연합 회원국민의 개인 데이터를 관리하는 모든 회사에서 준수되어야 하며, 늦어도 GDPR 시행일인 2018년 5월 25일까지 정책을 마련해야함
- 2018년 6월 27일 루마니아 의회는 EU의 GDPR의 위임조항을 다루는 루마니아의 GDPR 시행법(GDPR implementing Law)을 승인하였음
- GDPR 시행법은 제한된 영역을 다루고 있으며, ▲민감한 데이터(생체인식 데이터, 유전 데이터, 건강 관련 데이터) 처리와 관련된 특별 규칙을 규정 ▲다른 범주의 데이터(예: 개인 식별번호, 직원 데이터)와 관련한 규칙을 도입 ▲인증기관의 면허를 규제 ▲경과 과정을 승인 등의 내용을 포함

▶ 루마니아, 6개 EU국가의 사이버 신속 대응 선언 서명(2018.6)[301]
- 루마니아를 포함한 크로아티아, 에스토니아, 네덜란드, 스페인은 리투아니아 주도의 국방을 위한 영구적인 구조적 협력(Permanent Structured Cooperation of Defense, PESCO)하에 상호 지원 사이버 보안 프로젝트에 2018년 6월 25일에 서명함
- 사이버 신속 대응팀은 기존의 구조 및 형식에 얽매이지 않고 사이버 분야에서 국가, 유럽연합, 지역을

300 "EMPLOYEE MONITORING UNDER THE ROMANIAN LAW IMPLEMENTING GDPR", cloudprivacycheck.eu, 2018.7.5.
301 "Six EU states sign declaration on PESCO cyber rapid response", The Defense Post, 2018.6.25.

초월한 노력을 기울일 전망

- 사이버 신속 대응팀의 효과적인 배치 가능성을 조사하고 필요하다면 적응의 필요성을 모색하기 위해 법적 체계를 마련할 필요가 있으며, 유럽연합은 소프트웨어 및 기타 장비에 대한 자금을 할당할 것으로 예상하며, 법적 및 기술적 측면에 대해서는 유럽연합 기관들이 계속 논의 진행 중

융합보안시장 및 정책 동향

스마트의료

- 사이버 보안 프로그램의 도입이 가장 시급한 분야는 보건 부문임. 보건 부문은 건강 시스템에 의해 관리되어 수많은 개인 데이터들을 보유하고 있어 사이버 공격의 주요 타깃이 되고 있음.
- 루마니아 정보국((SRI)에 따르면, 2019년 6월 루마니아 5개 병원은 랜섬웨어 BadRabbit 4에 의해 감염된 것으로 보도되어 국가보안센터 팀이 상황을 해결하기 위해 부쿠레슈티 병원에 파견됨

스마트 시티

▶ 트란실바니아 지방 Alba Iulia시에 2018년까지 루마니아 최초의 스마트 시티 구축 계획 발표 ('16)

- 루마니아 건국 100주년을 맞아 2018년까지 진행되는 파일럿 프로젝트
- 스마트 조명, 디지털 교육, 공공 WiFi 설치, 의료 핫라인, 폐기물 관리, 불법 주차 모니터링 등 20개 이상의 개별 프로젝트가 진행[302][303]되었고, 2019년에도 프로젝트를 계속 이어갈 예정[304]

302 https://albaiuliasmartcity.ro/en/projects/
303 https://eu.smartcitiescouncil.com/article/will-alba-iulia-be-romanias-first-smart-city
304 https://hub.beesmart.city/city-portraits/alba-iulia-how-central-romania-quietly-created-a-smart-city-champion-in-europe#SOURCES

6. 아프리카 시장

아프리카 시장 개요

▶ 아프리카 지역은 총 면적 약 3,210만㎢, 지구 육지면적의 1/5을 차지하는 광활한 대륙으로, 약 11억의 인구가 54개의 독립국 구성

- 아프리카는 권역별, 국가별로 다양한 특성과 복잡성을 가지고 있는데, 북부아프리카, 서부아프리카, 동부아프리카, 중부아프리카, 남부아프리카로 5개 지역으로 구분
- 전 세계 최빈 개도국 49개국 중 34개국이 아프리카에 소재함에 따라 빈곤퇴치와 경제성장이 최대 당면 과제. 아프리카의 많은 국가에서 1인당 GNI는 1,000달러 미만으로 세계 최하위 수준
- 경제 집중도와 차이가 커서 6대 경제 강국(남아공, 알제리, 이집트, 나이지리아, 모로코, 리비아)들이 아프리카 전체 인구의 약 35%, 전체 GDP의 64%, 무역량의 약 60%를 차지하고 있음

표 _ 아프리카 시장 주요국의 한국과의 관계(2017년 기준)

항목	수교일	우리나라 수출규모 (US$ 백만)	우리나라 수입규모 (US$ 백만)	우리나라의 주요수출품	우리나라의 주요수입품
탄자니아	1992. 4.	194	33	의약품, 윤활유, 기타석유화학제품	연초류, 동괴및스크랩, 커피류, 채유종실
르완다	1963. 3.	72	1.9	컴퓨터, 기타산업기계, 서적	기호식품, 반도체, 휴대용품
케냐	1964. 2	240	50	기타석유화학제품, 합성수지, 곡류	커피류, 직물제의류, 동괴및스크랩
세네갈	1962.10	78	61	정제유, 계면활성제, 자동차, PVC, TV 등	냉동어류, 동웨이스트/스크랩 등
에티오피아	1963.12	105	54	기타석유화학제품, 합성수지	커피류, 화초류, 보석, 기타가죽, 편직제의류
지부티	1977.12	51	0.49	화학제품, 기계부품, 전자 등	동, 건설기계 등
베냉	1961.8. (1990.10 .재수교)	0.19	0.3	면화, 캐슈넛 등	식량 등

[출처] Kotra-국가별정보, KITA.net DB

▶ 대부분의 아프리카 국가들에서 ICT 발전지수는 정체를 보이고 있어, 현재까지 여전히 세계 최하위 순위를 기록하며 열악한 실정

- 2017년 글로벌 ICT 발전지수(ICT Development Index, IDI)에 따르면 조사 대상 대부분의 아프리카 지역 국가들의 순위는 세계 최하위를 기록하며 접근성, 이용성, 스킬 등 모든 지수에서 110위권 밖의 성적을 나타냄
- 주요 조사국 중 케냐와 세네갈은 이용성, 접근성, 스킬 측면에서 다른 조사 대상 국가에 비해 비교적 양호한 순위를 보이고 있음

표 _ 아프리카 시장 주요국 ICT발전지수(IDI)

국가	IDI(2017년)		접근성(access)		이용성(use)		스킬(skill)	
	순위	지수	순위	지수	순위	지수	순위	지수
탄자니아	165	1.81	162	2.52	164	0.75	164	0.75
르완다	153	2.18	155	2.67	148	1.58	148	1.58
케냐	138	2.91	135	3.63	139	1.76	139	1.76
세네갈	142	2.66	138	3.57	138	1.76	138	1.76
에티오피아	170	1.65	168	2.35	166	0.72	166	0.72
지부티	158	1.98	156	2.63	158	0.99	157	2.69
베냉	161	1.94	157	2.63	168	0.63	147	3.18
한국	2	8.85	7	8.85	4	8.71	2	9.15

[출처] ITU, ICT Development Index 2017, https://www.itu.int/net4/ITU-D/idi/2017/index.html

▶ 국제전기통신연합(ITU)은 법적, 기술적, 조직적 대응 및 역량강화, 국제협력 등 5개 부문의 지수를 종합하여 글로벌 사이버보안지수(Global Cybersecurity Index, GCI)를 측정하여 국가 간 비교를 함

- 2018년 글로벌 사이버보안지수(GCI)에 따르면, 대부분의 아프리카 지역 국가들의 글로벌 사이버보안지수 순위는 세계 중위권 및 하위권이지만 모리셔스의 GCI는 0.88점으로 세계 14위, 케냐는 44위, 르완다는 49위를 기록함

표 _ 아프리카 지역 글로벌 사이버보안지수(GCI)

국가	GCI(2018년)		법적(Legal)	기술적 (Technical)	조직적 (Oranization al)	역량강화 (Capacity building)	국제협력 (Cooperatio n)
	순위	지수	지수	지수	지수	지수	지수
모리셔스	14	0.880	0.182	0.168	0.200	0.186	0.144
케냐	44	0.748	0.195	0.110	0.147	0.147	0.149
르완다	49	0.697	0.157	0.117	0.178	0.137	0.108
한국	15	0.853	N/A	N/A	N/A	N/A	N/A

[출처] ITU, Global Cybersecurity Index(GCI) 2018

▶ 유엔무역개발기구(UNCTAD)는 금융기관 또는 모바일 머니 서비스 제공업체의 계정 소유권, 인터넷을 사용하는 개인, 우편물 신뢰성 지수, 안전한 인터넷 서버 등 4개의 지수를 종합하여 B2C 전자상거래 지수(B2C e-Commerce Index)를 측정하여 국가 간 비교를 함

- 2019년 B2C 전자상거래 지수에 따르면, 대부분의 아프리카 지역 국가들의 B2C 전자상거래 지수 순위는 세계 중위권 및 하위권에 분포하고 있으며, 케냐의 B2C 전자상거래지수는 49점으로 세계 88위, 탄자니아는 96위, 세네갈은 98위, 에티오피아는 120위를 기록함

표 _ 아프리카시장 주요국 B2C 전자상거래 지수

국가	전자상거래지수 (2019)		인터넷 사용하는 개인	계정 소유권	안전한 인터넷 서버	우편물 신뢰성 점수
	순위	지수	지수	지수	지수	지수
탄자니아	96	43.3	25	47	33	69
르완다	121	30.9	22	50	35	17
케냐	88	49	18	82	49	47
세네갈	98	42.7	46	42	29	53
에티오피아	120	31.1	19	35	9	61
지부티	124	28.6	56	12	35	11
베냉	138	21.0	20	38	22	3
한국	19	89.4	96	95	67	99

[출처] UNCTAD, B2C e-Commerce Index 2019, https://unctad.org/en/PublicationsLibrary/tn_unctad_ict4d14_en.pdf

▶ 글로벌 시장조사기관인 MarketsandMarkets이 발표한 정보보안 시장 보고서에서는 2018년 아프리카 의 정보보안 시장은 36억 3,000만 달러이며, 2023년에는 76억 7,000만 달러에 이를 것으로 전망

표 _ 아프리카 지역 정보보안 시장규모

(단위: 십억 달러)

국가	2016	2017	2018e	2023p	연평균성장률 (2018-2023)
아프리카 지역	2.61	3.09	3.63	7.67	16.10%

[출처] MarketsandMarkets, Security As a Service Market-Global Forecast To 2023, 2019

▶ 글로벌 시장조사기관인 MarketsandMarkets이 발표한 서비스형 보안시장에 대한 보고서에서는 서비스로서의 보안은 클라우드 기반 모델이며, 보안 공급 업체는 클라우드 및 사내 환경에서 엔터프라이즈 네트워크, 애플리케이션 및 데이터를 보호하고 유지 관리함

- 아프리카 지역은 이집트, 남아프리카공화국, 리비아 등을 포함하며 서비스형 보안 시장규모는 2018년 아프리카 지역의 경우 1억 3,960만 달러 규모로 연평균 성장률(2018-2023) 21.0%로 성장할 것으로 전망

표 _ 아프리카 지역 서비스형 보안 시장규모

(단위: 백만 달러)

국가	2016	2017	2018e	2023p	연평균성장률 (2018-2023)
아프리카 지역	85.6	110.1	139.6	362.3	21.0%

[출처] MarketsandMarkets, Security As a Service Market-Global Forecast To 2023, 2019

▶ 아프리카 시장의 주요 진출 전략은 다음과 같음

- 정보보호관련 ODA·PPP·KSP 협력사업 수요의 발굴 : 가봉·세네갈·탄자니아
  - 재원이 부족한 아프리카 국가의 특성을 고려하여, 무상원조(ODA) 및 민관합작투자사업(PPP)과 같은 협력수요 발굴 및 기획재정부를 통한 경제발전경험공유사업(KSP. Knowledge Sharing Program) 지원 추진

- 기존 레퍼런스를 활용한 주변국 진출 : 베냉·지부티·케냐·르완다
  - 기존 진출한 보안관제센터(SOC), 국가공인인증체계구축(PKI) 프로젝트를 기반으로 차세대 프로젝트로 발전 및 주변국으로 추가 수주 확대 전략 필요

가. 탄자니아

'18년 GDP(십억달러)	57.44
'18년 인구수(천명)	56,320

■ ITU 글로벌 사이버보안 지수(Global Cybersecurity Index, GCI)

· 탄자니아의 사이버보안 지수는 0.642(세계 59위)로 아프리카 국가 중 상위에 위치

국가명	2018		2017		전년대비 증감	
	지수	순위	지수	순위	지수	순위
탄자니아	0.642	59	0.317	88	+0.325	+29
대한민국	0.873	15	0.782	13	+0.091	-2

■ ICT 관련 주요 지수

· 탄자니아의 전반적인 ICT 발전 수준은 아프리카권에서는 상위권이나, 전 세계 중하위권에 위치

지표명	탄자니아		한국	
	점수	순위	점수	순위
IMD 국가경쟁력지수(2019)	-	-	-	28
IMD 디지털경쟁력지수(2019)	-	-	-	10
UNCTAD 전자상거래지수(2019)	43.3	96	89.4	19
ITU 글로벌 사이버보안 지수(GCI 2018)	0.642	59	0.873	15
UN 전자정부 지수(2018)	0.3929	139	0.901	3

■ ICT 관련 주요 통계 (ITU, 2018년 말 기준)

· 탄자니아의 유선통신 보급률은 0.22%로 인프라가 미비하며, 이동통신 역시 77% 수준으로 하위권

항목	탄자니아		한국	
	가입자수(천 명)	보급률(%)	가입자수(천 명)	보급률(%)
유선전화	124	0.22	25,907	50.63
유선브로드밴드	861	1.53	21,286	41.60
이동통신	43,497	77.24	66,356	129.67
인터넷 이용률	-		95.90%	

정보보호 산업 개요

1) 보안 환경

▶ 탄자니아 경제사회에서 ICT 활용 및 연결성이 증가함에 따라 사이버보안의 중요성이 더욱 강조됨

- 탄자니아는 ICT 사용증가와 함께 사이버 공격의 높은 목표가 되어 사이버위협이 함께 증가함
- 대부분 사이버범죄는 프라이버시 침입과 더불어 금융기관을 통한 금융 거래, 모바일머니 송금이 타깃팅 되며 심각한 문제로 인식됨[305]
- 또한 사이버범죄는 컴퓨터 사기, 해킹, IP범죄, ATM사기 등의 형태로 발생하고 있으며 주요 대상은 정부기관, 은행, 사업자 등이 포함[306]
- 탄자니아 정부는 사이버범죄 법률(Cybercrime Act)을 2015년 9월부로 시행하면서 사이버보안에 관한 대응활동을 본격적으로 추진
- 2017년에는 탄자니아 미디어에 가짜 뉴스들이 다양한 매체를 통해 유통됐으며, 가짜 계정과 거짓정보는 2017년 상반기에 3,340건이 경찰에 보고됨
- 온라인 콘텐츠에 대한 규제가 포함된 개정된 전자 및 우편 통신 규제 2018은 2018년 3월에 발효되어 인권, 미디어 등의 단체에서 반대가 있었으나 5월의 법원 명령은 정부를 지지하였으며, 이 규제하에 블로거를 포함한 온라인 라디오 방송국과 비디오 웹사이트를 운영하는 탄자니아인은 등록 라이선스 수수료, 연간 수수료 지불에 대한 내용이 포함됨

▶ 탄자니아는 2017년 사이버범죄로 9,950만 달러의 손실이 추정됨[307]

- 정부와 민간부문에서 ICT 기술과 자동화에는 많은 투자를 하는 반면, 사이버 위협 예방에 대한 투자에는 미비한 것으로 나타남
- 조사대상 조직의 51%는 사이버보안 관련 제품에 연간 5,000 달러 이하의 비용을 지출하는 것으로 나타났으며, 연간 10,000달러 이상 지출하는 조직은 은행 및 금융 부문인 것으로 나타남[308]

▶ 모바일 금융서비스 사용이 증가함에 따라 관련된 모바일 정보보호 위험이 증대됨

- 탄자니아는 모바일 머니(mobile money) 시장이 급성장하여 M-Pesa, Tigo-Pesa, Airtel-Money 등과

305 "Cyber criminals can be stopped", Dailynews, 2017.3.2.
306 Saidi M. Kalunde, "The status of Cybercrime in Tanzania", Octopus Conference on Cooperation Against Cybercrime, 2015.06.
307 "Tanzania Cyber Security Report 2017", SERIANU, p. 11.
308 "Tanzania Cyber Security Report 2017", SERIANU, p. 41

같은 모바일 뱅킹과 모바일 지급 솔루션이 이용되고 있으나, 이에 대한 보안 관리는 부족한 상황

- CitiGroup의 Digital Money Index 2018 보고서에 따르면 2018년 기준 탄자니아의 모바일 머니 보급률은 약 70%에 해당함[309]

▶ 인구가 밀집된 도시들은 범죄와 테러에 위협받고 있고, 공항, 호텔 등의 장소에서 납치도 발생하고 있어[310] 상응하는 대응 방안으로 물리보안 분야 수요가 증가할 것으로 예상됨

- 인구가 밀집된 Dar es Salaam은 특히 위협지역이며, 이외에도 Arusha, Mwanza, Stone Town 등의 도시들은 범죄와 테러에 위협받고 있으나 경찰의 규모가 작아 적절한 대응 및 예방에 어려움이 있음
- 대다수 범죄 사건들은 폭력이 없는 소유물 도난, 주거침입 도난, 거리 범죄 사건들에 해당하며, 폭력적인 범죄도 증가하고 있음
- 도시지역에서 만연한 거리범죄의 경우 가방, 컴퓨터, 카메라 등이 타깃인 날치기도 많이 발생하고 있으며, 특히 거리 차량에서 행인의 물건을 날치기하는 경우도 증가함
- 또한 최근에는 납치도 드문 것이 아니어서, 관광객이나 해외거주자들의 경우, 공항, 버스정류장, 호텔 등의 장소에서 납치되어 카드 비밀번호나 카드 최대 한도금액을 제공받고서야 풀어주곤 함
- 최근에는 탄자니아 당국이 광물 도난을 통제하기 위해 광산 주위에 CCTV 카메라를 설치함

▶ Kaspersky Lab의 모바일 악성코드 관련된 보고서에 의하면 2018년 한 해 동안 탄자니아는 모바일 악성코드에 의해 탄자니아 조사된 모바일 사용자의 약 31.34%가 공격당했음[311]

- 모바일 악성 코드에 가장 영향을 받은 국가 상위 10개 목록에 상위 10개 목록에 포함된 아프리카 국가로는 3순위의 나이지리아(37.72%), 5위의 알제리(35.06%), 8위의 탄자니아(31.34%), 9위의 케냐(29.72%)가 있음
- 사이버 범죄자들은 트로이 드랍퍼(Trojan-Droppers)를 점점 더 많이 사용하고 있으며, 이는 합법적으로 보이는 앱을 통해 악성 소프트웨어가 비밀리에 설치되는 일종의 공격이며, 이런 유형의 공격은 Android 장치에서 매우 일반적이며, 예방조치로는 스마트폰에 모바일 보안 솔루션을 설치하여야 함

▶ ITU가 2019년 3월 발표한 'Global Cybersecurity Index 2018'에 따르면 탄자니아의 사이버보안 지수는 0.642, 글로벌 순위는 59위이며, 아프리카 지역에서 6위를 기록

2) 인터넷 및 통신 환경

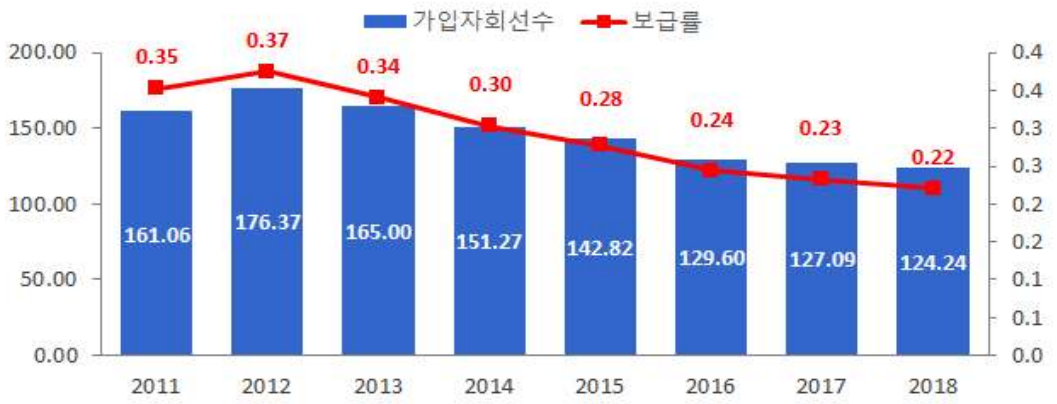
309 Tanzania drives Africa's e-money growth, The Citizen, 2018.10.16.
310 U.S. OSAC, "Tanzania 2017 Crime & Safety Report"
311 Victor Chebyshev, Mobile malware evolution 2018, Kaspersky Lab, 2019.3.5.

▶ 유선통신

- ITU에 의하면 2018년 말 기준, 유선통신 가입회선 수는 12만 4,238회선을 기록, 2017년 12만 7,094회선 대비 2.2% 감소함
- 유선통신은 인프라 부족으로 인해 시장 정체를 보이고 있으며, 모바일 이용자가 늘어남에 따라 유선 가입회선 수는 지속적으로 감소 추세를 보이고 있음
- 유선통신사업자는 소규모의 두 번째 운영자인 Zantel이 이동통신 서비스에 집중하면서 2019년 3월 기준 유선 서비스 제공을 중단 한 후, 기존 사업자인 TTC[312]만 유선서비스를 제공하고 있음
- 2019년 3월 기준 TTC 가입 회선 수는 7만 8,081회선, ZANTEL 가입 회선 수는 0회선에 해당하며, 2019년 2월 대비 TTC은 46,061회선 감소, ZANTEL은 17회선 감소하며 유선 가입자 수가 줄어듦[313]

그림 _ 탄자니아 유선통신 가입 회선 및 보급률 추이

(단위: 천 회선, %)



[출처] ITU Statistics DB (2019.6)

▶ 이동통신

- ITU의 자료에 의하면 2018년 기준 이동통신 가입자 수는 2016년 대비 약 8.9% 증가한 4,349만 7,261명을 기록하며 보급률이 77.24%이며, 2011년부터 2018년까지 연평균 성장률(CAGR)은 7.8%를 기록함
- 2019년 기준 이동통신 시장은 7개의 모바일 서비스 제공자가 있으며, 새로운 융합 규제 체제하에 네 개의 추가 사업자가 라이선스를 획득하였으며, BuddeComme의 자료에 의하면 2019년 3월까지 이동통신 보급률은 90% 달함[314]

---

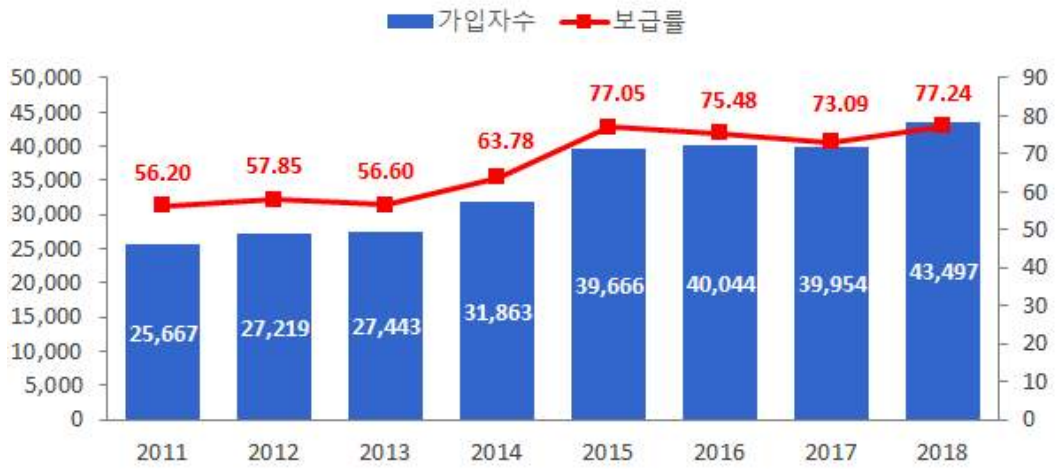
312 TTC는 탄자니아 정부가 2017년 9월 Bharti Airtel이 소유한 35% 지분을 인수하여 재획득하였으며 2018년 1월 TTCL(Tanzania Telecommunications Company Ltd)에서 TTC(Tanzania Telecommunications Corporation)로 개혁하여 통신서비스 개발, 인프라 관리를 함

313 TCRA, Quarterly Communications Statistics Report, 2019.3.

• 2019년 3월 기준, 이동통신 시장은 3대 업체인 Vodacom(32.3%), Tigo(28.4%), Airtel(26.0%)가 전체 이동통신 시장의 86% 이상을 차지하여 압도적으로 점유하고 있으며, 베트남계의 Halotel(8.4%)이 빠른 속도로 시장점유율을 넓히고 있는 가운데 그 뒤를 Zantel(2.8%), TTCL(1.8%), Smart(0.3%) 등의 군소 업체가 따르고 있음[315]

그림 _탄자니아 이동통신 가입 및 보급률 추이

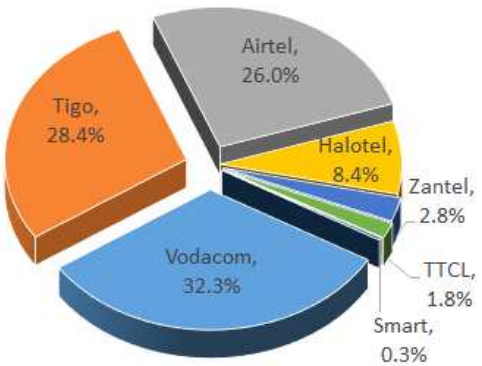
(단위: 천 명, %)



[출처] ITU Statistics DB(2019.6)

그림 _ 탄자니아 이동통신사별 시장 점유율(2019년 3월 기준)

통신사	가입자 수(명)	비율
Vodacom	14,206,120	32.3%
Tigo	12,474,091	28.4%
Airtel	11,452,120	26.0%
Halotel	3,709,678	8.4%
Zantel*	1,221,007	2.8%
TTCL*	801,163	1.8%
Smart	132,404	0.3%
전체	**43,996,583**	**100%**



* Zantel(탄자니아 잔지바르 국영 통신사), TTCL(탄자니아 국영 통신사)

[출처] Tanzania Communications Regulatory Authority(TCRA) (2019.3)

314 BuddeComme, Tanzania – Telecoms, Mobile and Broadband- Statistics and Anayses, 2019.7.4.
315 TCRA, Quarterly Communications Statistics Report, 2019.3.

- 탄자니아의 이동통신 시장은 매우 경쟁적이며, 모든 통신사 라이선스는 융합된 서비스가 허용되는 기술과 서비스 중립적임
- 2016년 기준 모든 이통통신 가입자 중 36%가 3G/4G 기반이며, 이는 2021년까지 67%까지 성장할 것으로 예측[316]
- 이통통신 보급에서의 성장률은 도시지역에서 모바일 금융서비스와 같은 고가치 서비스에 대한 증가하는 성장과 함께 지방에서 인프라 향상에 의해 활성화 될 것임
- 정부는 서비스가 제공되지 않는 지방에 3G서비스 확장을 위해 Ericsson과 파트너 관계를 맺어옴
- 이동통신사들은 최근 몇 년간 고객유치 확보를 위한 치열한 가격경쟁으로 인해 소기업은 어려움에 봉착함
- 이동통신 가입률의 증가로 인해 모바일 서비스도 활성화하여 모바일 소액결제뿐 아니라, 온라인 교육, 모바일 배달 서비스(Hello Food) 등 확장되고 있음
- 탄자니아 최대 시장점유율을 갖고 있는 Vodacom은 2G 및 3G 인프라 구축에 10억 달러 이상을 투자하여 3,300 개 이상의 사이트에서 95% 인구에게 제공하고 있다고 주장함
- Vodacom은 Nokia Networks의 장비를 사용하면서 LTE을 시험하였고, 2016년 5월에 상용 LTE를 수도에서만 시작함
- TTC는 농촌 지역 네트워크의 확장 및 업그레이드와 LTE 서비스를 개발하기 위해 2017년 3월 중국 정부로부터 6천만 TZS(약 2억 7,100만 달러)의 대출을 확보함[317]
- TTC는 2015년 말 LTE 서비스를 시작하였으며, LTE 기술 배포와 함께 2G, 3G 네트워크 인프라 업그레이드를 위해 Huaweo와 2015년 초에 계약하였으며, 2016년 말 LTE는 Zanzibar, Dodoma 등을 포함하여 10여개 지역에 확장되며 2018년 말까지 모든 지역으로 확장 될 예정임[318]
- TTC는 2016년 11월 장비공급업체인 Huawei와 함께 LTE-A 서비스를 시작함
- Tigo는 2015년 말 다르에스살람에서 LTE 서비스를 시작하였으며, 추가 5개 도시는 2016년 초에 포함되며, Tigo는 ISP UhuruOne과 파트너 관계를 맺음
- Zantel은 2016년 4월 Zanzibar에서 LTE 서비스를 시작하였으며, 2016년 10월에 다르에스살람에 상업용으로 출시함
- Smile 통신은 2018년 6월 4G 서비스를 Arusha에서 출시함

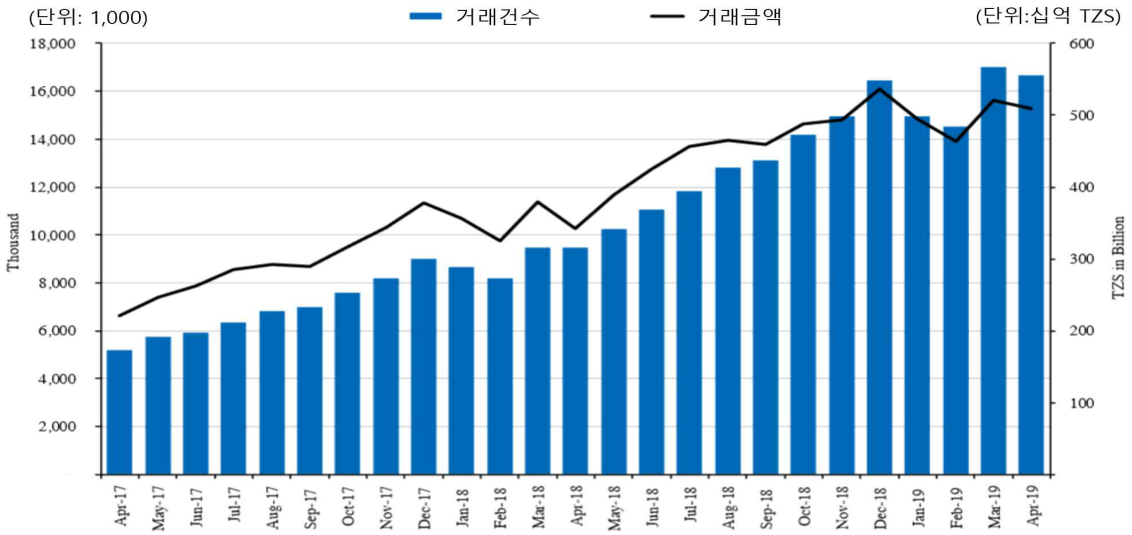
▶ 모바일 머니

- 탄자니아는 모바일 금융서비스에 대해 상호운용성을 제공하는 첫 번째 나라로서, 이는 낮은 은행 보급과 함께 증가하는 비즈니스 기회를 제공함

316 Business Sweden in Eastern Africa, "Opportunities in the ICT Sector in East Africa", 2017.4.26. p. 15.
317 BuddeComme, Tanzania – Telecoms, Mobile and Broadband- Statistics and Anayses, 2019.7.4. p. 37.
318 BuddeComme, Tanzania – Telecoms, Mobile and Broadband- Statistics and Anayses, 2019.7.4. p. 68.

- 모바일 송금은 2013년 송금 규정(Money Remittance Regulations) 제정에 의해 촉진되었으며, 이 국가 금융 프레임 워크는 공식적인 금융 서비스에 대한 접근을 확장하기 위해 지불 플랫폼, 인프라 및 소비자 보호에 중점을 둠[319]
- 2018년 7월~2019년 4월 10개월 동안 모바일 머니 거래금액은 약 4조 8,865억 TZS(약 21억 2600만 달러)[320]가치에 해당하며 약 1억 4,650만 건의 거래로 성장함[321]
- 이러한 성장은 2017/18년의 같은 기간 대비 거래건 수는 81.6%, 거래금액은 47.7% 증가한 것에 해당함

그림 _ 탄자니아 모바일 지급의 모바일 네트워크간의 거래량(2017.4~2019.4)



[출처] Governor Bank of Tanzania, "Monetary Policy Statement 2019/20", p.36. 2019.6.

- 모바일머니로 예금, 인출, 송금뿐 아니라 구매대금 지불, 항공권 구매, 세금납부, 전화/전기요금, TV요금, 수도세, 정부소유 집세 등 다양한 방면에서 편리하게 결제 가능하여 인기를 끌고 있음
- 2019년 5월 Haotel은 HaloPesa 플랫폼을 통해 국제 자금 거래를 처리할 수 있도록 Visa와 5년 계약을 체결했음
- Vodacom은 2014년 초 M-Pesa 서비스 파트너로 Umoja Switch와 계약을 맺고 가입자는 200개 이상의 ATM 네트워크에서 현금을 인출 할 수 있으며, 또한 Vodacom은 전국 24개 은행과 파트너관계를 체결하였음
- 2014년 중반 Vodacom와 CBA(Commercial Bank of Africa)는 MPawa 뱅킹 서비스를 시작했으며, 이

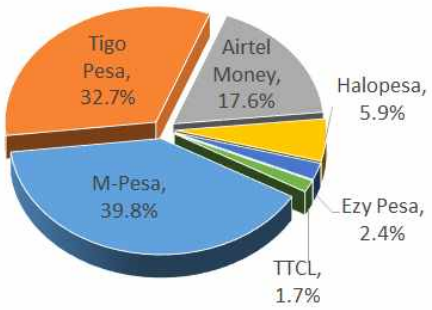
319 BuddeComme, Tanzania – Telecoms, Mobile and Broadband- Statistics and Anayses, 2019.7.4. p. 87.
320 2019년 9월 환율 기준: 1달러 = 약 2298 탄자니아실링
321 Governor Bank of Tanzania, "Monetary Policy Statement 2019/20", p.36. 2019.6.

서비스를 통해 사용자는 휴대폰으로 돈을 저축하고 빌릴 수 있게 됨

- Vodacom은 2016년 중반에 M-Pesa 서비스를 위해 업데이트된 플랫폼인 G2를 설치하여 더 빠르고 강력하며 추가 제품 및 서비스를 제공할 수 있었음
- 2019년 3월 기준, 탄자니아 모바일 머니 계좌 건수는 2,279만개를 넘어섰으며, 모바일머니 시장은 M-Pesa(39.8%)가 1위를 차지하고 있으며, Tigo Pesa(32.7%), Airtel Money(17.6%), Halopesa(5.9%), Ezy Pesa(2.4%), TTCL(1.7%) 순임[322]

그림 _ 탄자니아 통신사 및 모바일 머니별 시장 점유율(2019년 3월 기준)

통신사	모바일 머니	가입자 수(명)	비율
Vodacom	M-Pesa	9,077,341	39.8%
Tigo	Tigo Pesa	7,445,395	32.7%
Airtel	Airtel Money	4,009,347	17.6%
Halotel	Halopesa	1,341,630	5.9%
Zantel	Ezy Pesa	538,064	2.4%
TTCL	TTCL	385,053	1.7%
전체		**22,796,830**	**100%**



[출처] Tanzania Communications Regulatory Authority(TCRA) (2019.3)

▶ 탄자니아는 2017년 스마트폰 보급률이 13%로 남아프리카공화국 51%, 케냐 30% 등에 비해 상대적으로 낮은 보급률을 보임[323]

▶ 인터넷 이용 환경

- TCRA의 자료[324]에 따르면 탄자니아의 인터넷 이용자 규모는 약 2,314만 명이며, 주로 이용하는 환경은 모바일이 96.3%인 반면, 고정 무선과 유선 환경에서는 각각 0.6%와 3.1%로 나타남
- 융합 라이선스 체제로 인해 새로운 사업자들이 시장에 들어오게 되었으며, VoIP 전화통신의 자유화, 3G와 LTE 이동통신 서비스, 무선 브로드밴드 네트워크의 도입으로 인해 유선 네트워크 개발의 낮은 수준으로 방해받던 인터넷 부문이 향상됨
- 특히 모바일 네트워크 사업자들은 인터넷 서비스 제공을 주도하며, 모바일 데이터 서비스에 의한 매출 성장을 기대하며 네트워크 업그레이드에 투자를 하였으며, 빠르게 발전하는 수입원은 모바일 송금 및 모바일 뱅킹 서비스임

322 TCRA, Quarterly Communications Statistics Report, 2019.3
323 "Global E-Commerce Intelligence, Africa B2C E-Commerce and Online Payment Market 2019", yStats, 2019.6.
324 TCRA, Quarterly Communications Statistics Report, 2019.3

• 2009년과 2010년에 탄자니아 최초의 광섬유 국제 해저 케이블의 착륙 덕분에 값비싼 위성 연결에만 의존하던 시장에서 벗어날 수 있게 되었으며, 또한 정부는 전국 인구 중심지를 연결하는 것을 목표로 국가 광섬유 백본 네트워크의 후기 단계를 진행

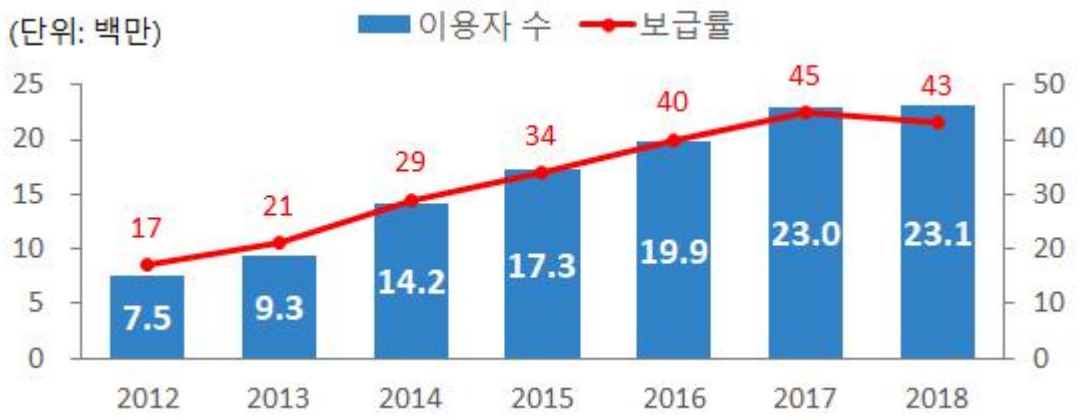
그림 _ 탄자니아의 플랫폼별 인터넷 이용률(2018년 12월 기준)

구분	이용자 수	점유율
모바일	22,281,727	96.3%
고정무선	135,954	0.6%
유선	725,279	3.1%
전체	**23,142,960**	**100.0%**

[출처] TCRA(2019.3)

• TCRA의 자료[325]에 따르면 2018년 인터넷 보급률이 43%, 사용자수는 2,314만 명에 이르는 반면, ITU의 자료에 의하면 2017년 인터넷 보급률이 25%로 상당히 적게 나타남

그림 _ 탄자니아의 인터넷 보급률 및 이용자 수(2018년 12월 기준)



[출처] TCRA(2019.3)

325 TCRA, Quarterly Communications Statistics Report, 2019.3

정보보호 시장 현황

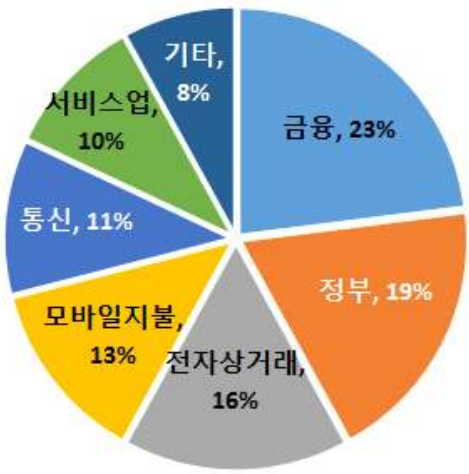
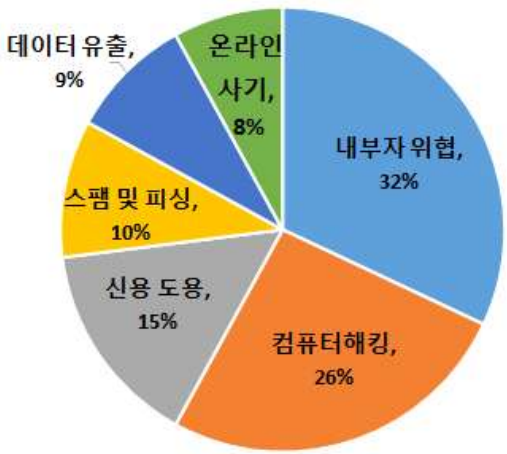
1) 시장 규모

시장 개요

▶ 탄자니아에서 사이버 범죄의 신고 건은 2014년 380건, 2015년 1,823건 등 최근 들어 급증하고 있음[326]

- 실제 발생한 사이버 범죄 중 9%만이 경찰청에 신고되고, 그 중에서 1%만이 법적으로 기소 처리되는 상황을 고려할 때, 사실상 사이버 범죄가 무방비 상태에 놓여 있는 실정임
- 글로벌 보안컨설팅 기관은 사이버 범죄로 인한 탄자니아의 2016년 금전적 손실 규모가 8,500만 달러에 달한다고 발표
- 특히, 금융 분야에서 23%로 가장 높은 손실이 발생했으며, 손실을 야기하는 범죄 유형으로는 내부자가 32%로 가장 높았고, 그 다음으로는 컴퓨터 해킹이 26%로 뒤를 이음

표 _ 탄자니아 사이버범죄 손실 및 유형

탄자니아 산업별 사이버범죄 손실	탄자니아 사이버범죄 유형
	

[출처] www.serianu.com의 자료를 인용한 이태승, "[전문가 기고] 탄자니아 정보보호시장 현황 및 진출 팁", 2017.10.16.에서 인용

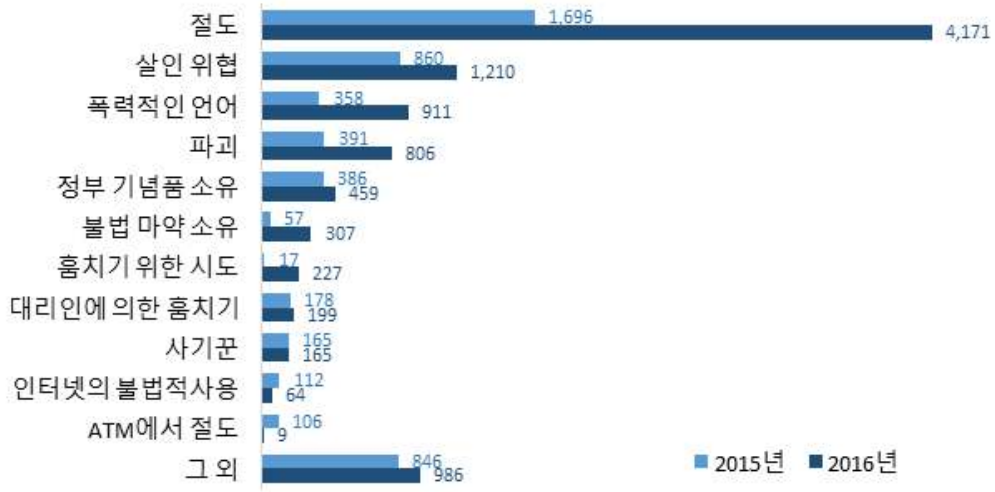
▶ 2016년 사이버 범죄 사건은 9,441건으로 증가함

326 이태승, "[전문가 기고] 탄자니아 정보보호시장 현황 및 진출 팁", 2017.10.16

- 2017년 1월에 발행된 탄자니아 경찰청의 보고[327]에 의하면, 사이버범죄 사건은 2016년 9,441건으로 2015년의 5,172건에 비해 4,269건(82.5%) 증가함
- 2016년 사이버 범죄 사건의 주된 유형은 절도, 살인 위협, 폭력적인 언어, 고장 등의 순으로 나타남

그림 _ 탄자니아 사이버범죄유형별 사고건수

(단위: 건)



[출처] The United Republic of Tanzania, 'Crime and Traffic Incidents Statistics Report'(2017.1), p33. 자료 기반 재구성

▶ 케냐 기반의 IT 비즈니스 컨설팅 기업 SERIANU社의 사이버 보안에 관련된 보고서에 의하면[328] 2017년 한 해 동안 사이버 범죄로 인한 탄자니아의 손실 비용은 9,950만 달러로 추정되며, 이외 2017년 주요 사이버 보안 이슈는 다음과 같음

- 2017년 사이버범죄로 인한 손실 비용은 아프리카 전체 35억 달러, 나이지리아 6억 4900만 달러, 케냐 2억 1000만 달러, 탄자니아는 9,950만 달러로 아프리카에서 세 번째로 높게 나타났으며 이는 탄자니아의 GDP 47억 달러의 0.2%에 해당함
- 사이버 범죄의 손실비용 9,950만 달러 중 가장 큰 손실 비용 항목은 내부자 위협이 2,990만 달러(30%)이며, 이후 컴퓨터 시스템 공격이 1,990만 달러(20%), 이메일 스팸 및 피싱이 1,490만 달러(15%) 순으로 나타남

구분	비용(백만 달러)	비중(%)
내부자 위협	29.9	30
컴퓨터 시스템 공격	19.9	20

327 "Crime and Traffic Incidents Statistics Report 2016", The United Republic of Tanzania, 2017.1., p33.
328 "Tanzania Cyber Security Report 2017", SERIANU, p. 11

구분	비용(백만 달러)	비중(%)
이메일 스팸 및 피싱	14.9	15
사회공학 및 신원도용	11.9	12
온라인 사기	9.9	10
데이터 유출	8	8
랜섬웨어	5	5
합계	99.5	100

- 탄자니아 조직의 90% 이상이 사이버 보안 위험에 크게 노출되어 있으며, 조직 내에서 많은 프로세스가 여전히 오래된 수동적인 프로세스의 사고방식으로 수행되고 있으며, 사이버 위험을 처리하기 위한 충분한 제어가 부족함
- CISA, CISM, GIAC, 등과 같은 정보 보안 자격증을 가진 공인된 전문가는 300명으로 추정되며, 조직들은 IT, 컴퓨터 과학 등과 같은 전통적인 기술 인증을 가진 사람들을 찾고 있어 정보 보호에 대한 역량에 차이를 보이고 있고, 젊은 대학 졸업생들도 보안 인증의 이해가 여전히 낮아 관련된 보안 인증을 받기 위한 기술 능력을 향상 시키는데 충분한 관심을 보이지 않음
- 가짜 뉴스들이 탄자니아 미디어에서 나타나며 사람들이 점점 더 검증되지 않은 가짜 뉴스를 보게 되고, 가짜 뉴스들은 다양한 매체들을 통해 유통되고 있으며, 가짜 계정과 거짓 정보들은 TCRA에 의하면 2015/16년에 7,000건 이상, 2017년 상반기에는 3,340건이 경찰에 보고되었음
- 탄자니아의 산업에서 가장 타깃이 되는 부문은 여전히 은행 부문에 해당하며, 온라인 뱅킹, 모바일 뱅킹 사용이 증가함에 따라 공격자들은 이러한 플랫폼을 사용하고 있으며, 보고된 여러 공격들에서는 해커들이 휴면계정을 이용하여 엄청난 액수의 은행 송금을 처리한 것으로 나타남
- 내부자의 위협은 여전하며, 보고된 많은 경우들로부터 악의적인 침해를 수행하는데 최적의 위치인 관리자 계정과 특권의 사용자 계정을 가진 그룹들이 가장 연루되기 쉬운 것으로 나타났으며, 이들의 실수나 과실은 조직에 가장 심각한 영향을 가져오게 됨
- 90% 이상의 부모들이 자녀를 사이버 괴롭힘으로부터 보호하기 위해 어떤 조치를 취해야하는지 이해하지 못함
- 대다수 조직의 사이버 보안 프로그램은 툴에 의존하고 있으며, 사이버 보안 사고의 94.4%는 보고되지 않거나 해결되지 않음

▶ 또한 SERIANU의 보고서에 의하면[329] 사이버 위험이 큰 산업 부문은 은행부문, 통신부문, 금융서비스 및 모바일 머니 부문, Sacco의 협동 조합 및 소액 금융 부문, 전자상거래 부문, 서비스 및 소매 부문으로

329 "Tanzania Cyber Security Report 2017", SERIANU, pp. 56-57.

분석됨

- 은행부문: 은행과 금융기관들은 특히 악의적인 내부자들로부터 사이버 범죄의 큰 타깃이 되고 있으며, 일년 내내 발생한 사이버 공격에는 직접적인 DB 조작, 전자메일 피싱 및 가동 중지시간을 초래하는 중요한 시스템의 손상이 포함됨
- 통신부문: 전화번호, 신원 번호, PIN 번호 등과 같이 개인데이터를 소유하고 있는 통신회사들은 결과적으로 사이버 공격의 매력적인 목표가 되므로, 통신회사들은 사이버 공격에 견딜 수 있는 고급 보안 솔루션을 채택하는 것이 중요하며, 대다수의 통신회사가 자체적인 사이버 보안 관리를 하는 것은 주목할 만 함
- 금융서비스 및 모바일 머니 부문: 탄자니아에서 휴대전화를 통한 연간 송금액은 GDP의 47%에 해당하는 43조 탄자니아 실링에 해당하며, 현재 대다수의 은행, 교통, 통신, 전자상거래, 서비스 산업 회사들은 모바일머니 서비스를 대안 채널의 하나로써 도입함
- 이와 같이 여러 부문과 모바일 머니와의 통합은 사이버 공격자에게 많은 기회를 제공하게 되므로, 회사들은 모바일 머니와의 통합 부분을 안전하게 하고, 또한 사용자들에게 휴대 전화를 안전하게 보호하는 방법, 금전적 손실로 이어지는 사회공학을 피하는 방법에 대한 교육을 하는 것이 중요함
- Sacco 신용 조합 및 소규모 금융 부문: 고객 만족과 비용절감에 중점을 두어 상대적으로 사이버범죄 예방을 위한 투자에 소홀하여, 사이버범죄에 목표가 되기 쉬움
- 전자상거래 부문: Jumia, E-Bay, OLX 등과 같은 온라인 쇼핑 몰을 포함한 전자유통업체의 확산은 크게 증가하고 있으며, 이러한 전자상거래 업체들은 시스템 취약성으로 인해 온라인 사기, 거래사기, 고객 개인정보 침해의 증가가 알려지고 있으며, 판매자는 전자 거래의 위험을 인식하고 시스템을 최소수준으로 유지하기 위한 노력을 해야 할 필요가 있음
- 서비스 및 소매부문: 주로 민감한 고객 정보를 다루는 서비스 및 소매부문의 경우, 예약 정보, 지불, 개인 정보 등의 처리가 자동화되고 있으나 정보보호 측면은 무시되는 경향이 있어, 신용카드 도용, 정보 도용, 데이터 유출 등의 수많은 위험이 초래됨
- 이러한 산업을 타깃으로 하는 악성코드는 신용카드 데이터를 훔치려는 POS(point-of-sale) 단말기에서 나타나고 있고, 개인 데이터를 훔치고자 호텔시스템을 공격하는 것으로 나타나고 있으며, 이로 인해 금전적인 측면 및 명성에도 영향을 주어 고객들로부터 신뢰를 쉽게 잃게 됨

시장 규모 및 성장률

▶ 물리보안 시장규모는 상대적으로 적은 규모의 경찰력으로 인해 점차 확대 전망

- 탄자니아는 경찰 1명이 약 1,049명에게 서비스하고 있어[330] 국제적 표준에 따른 경찰 1명당 약 450명에게 서비스하는 것과 비교하여 상당수가 부족하며, 결과적으로 탄자니아의 경찰들이 권고되는

330 "Crime and Traffic Incidents Statistics Report", The United Republic of Tanzania, 2017.1., p. 57.

국제기준에 비해 두 배 이상의 부담을 가짐

- 또한 경찰은 낮은 임금, 불충분한 수의 경찰 인력, 제한된 차량, 불충분한 가솔린, 소수의 무선, 훈련 부족 등 자원 부족으로 어려움을 겪음[331]

▶ 2017년 기준 탄자니아 정보보안 시장 규모는 750만 달러 수준으로 추정

- 시장조사기관 Technavio의 2015년 자료에 따르면[332], 2014년 기준 탄자니아의 정보보안 시장 규모는 678만 달러였으며, 이를 활용해 2017년 시장 규모를 추계하는 회귀식을 구하고, 이를 2017년 변수에 적용하는 방법을 취했을 때 750만 달러 규모가 도출됨[333]

2) 분야별 현황

물리보안 제품 및 서비스

- CCTV 장비, 접속제어, 원격 비디오 카메라 시스템, 네트워크 보안 기기와 서비스, 등의 제품 및 서비스뿐만 아니라 Bio-Lock, Bio-Metric 등 최신 바이오기술도 시장에서 제공됨

▶ 탄자니아의 CCTV시장은 유럽제품과 중국제품이 경쟁하는 가운데 중국제품이 점유율을 크게 확대하고 있는 추세임

표 _탄자니아 CCTV 주요 수입국 (2010-2016)

(단위: 천 달러)

국가명	2010	2011	2012	2013	2014	2015	2016
중국	483	139	225	498	602	1,002	1,220
미국	138	197	290	201	286	317	513
한국	30	5	8	20	2	20	220

주) HS 852580 Television cameras, digital cameras and video camera recorders

[출처] UN Comtrade DB

331 U.S. OSAC, "Tanzania 2019 Crime & Safety Report"
332 Technavio, Global Information Security Products and Services Market 2015-2019(2015)
333 GDP와 인구규모를 독립변수로 다중회귀분석을 실시. 계수의 p값이 낮은 GDP 데이터를 활용했으며, 국가별 GDP 편차가 크게 나타나 LOG값을 취하여 다중회귀분석을 재실시하여 추정의 정확도를 제고함. 데이터가 있는 22개 국가의 시장규모와 GDP에 기울기인 1.09544492562193를 곱해서 산출

정보보안 제품 및 서비스

- 보안 거버넌스, 보안 평가와 리뷰, 사고 대응 등의 컨설팅 및 자문, 보안 기술 교육 제공, 데이터 보안 등을 포함한 사이버보안 서비스가 제공됨

3) 주요 사업자 현황

▶ Tera Technologies and Engineering Ltd.

- Tera Technologies and Engineering Limited은 2011년 9월에 설립되어 다르에르 살람에 위치하며, 통신, ICT, 전력, 보안 시스템 솔루션을 제공
- 주된 보안 솔루션에는 접속 제어, CCTV, 침입자 알람, Bio lock, Bio-metric 시스템, 출입 접속 제어 등을 포함함
- CRDB Bank에 서버룸 환경모니터링시스템, CCTV 접속 제어 및 침입 알람 등을 공급 및 설치하였고, EXIM Bank에 Cisco Access 포인트, 라우터, 스위치를 공급 및 설치, 보안시스템을 설치 프로젝트를 수행하였음
- 연락처 : Home Page : http://www.teratech.co.tz
  e-Mail : info@teratech.co.tz
  Tel. : + 255 22 2701612, Mobile: +255 713 899 309, +255 754 912281.

▶ CATS Tanzania Ltd.

- CATS Tanzania Ltd.는 1986년부터 탄자니아 지역에서 컴퓨터와 통신 시스템을 담당하며, 서아프리카의 몇 국가들에서도 사업을 하고 있으며, 정부 부처 및 에이전시, 공공 조직, 민간기업 등에 인프라, 앱, IT솔루션, 보안 등의 토탈 솔루션을 제공
- 주로 제공하는 보안 서비스는 앱 서버, 메일 서버, 컴퓨터 및 랩탑 등을 위한 보안 시스템이 설계되도록 제공
- 연락처 : Home Page : http://www.catsgroup.co.tz/
  e-Mail : sales@catsgroup.co.tz Tel. : T. +255 22 213 7915

▶ NRD East Africa Ltd.

- NRD(Norway Registers Development) East Africa Ltd.는 2013년 3월에 설립되어 탄자니아 다르에스살람에 위치하며, 디지털 보안 영역에서 탄자니아를 포함한 동아프리카 지역에서의

프로젝트를 수행함

- 주요 서비스는 정보시스템 감사 및 IT 거버넌스, ICT 인프라 아키텍처 수행 및 관리, 사이버 보안제품과 컨설팅, 교육 등 제공
- ISACA Tanzania Chapter와 함께 탄자니아 사이버 보안 프레임워크 자문을 수행함
- 주로 경찰, 정부 사이버 보안센터와 CERT, 법원과 정보보안 부서 등과 같은 특수한 조직에 사이버보안 기술 컨설팅, 사고 대응, 응용 연구를 제공함
- 사이버 보안기술을 제공하기 위해 Lumension, IBM Security, AccessData, Qualys, FireEye, Fortinet and Vasco 등과 파트너 관계를 맺고 있음
- 연락처 : Home Page : http://www.nrd.co.tz/
  e-Mail : info@nrd.no Tel. : T. +255 222 110 895

▶ Cyberoam

- 네트워크 보안기기 및 보안 솔루션 제공 업체인 Cyberoam은 탄자니아 시장 파트너인 Mart Networks Tanzania Limited을 통해 네트워크 보안기기를 유통
- 케냐에서 1996년에 설립된 Mart Networks는 동아프리카, 서아프리카 등에서 물리적 보안과 인터넷 보안 서비스를 제공[334]
- 연락처 : Home Page : https://www.cyberoam.com/emeatz.html
  e-Mail : poonam.bhatti@mart-networks.com
  Tel. : + 255 683 901 203, Mobile: +255 784 444 490, +255 658 344 490

▶ SCI

- SCI는 50년 전에 탄자니아에서 설립된 회사로 기술 컨설팅 및 솔루션에서 주도하는 회사로, 특히 탄자니아 전 지역의 은행지점에 1,500개 이상의 ATM을 공급, 구축, 관리하고 있음
- 현재 은행, 금융뿐만 아니라 통신, 정부와 NGO, 에너지, 제조, 미디어, 출판 등 다양한 산업부문에 솔루션과 서비스를 제공하고 있으며, 케냐, 콩고 등 아프리카 대륙으로 사업을 확장함
- 연락처 : Home Page : http://www.sciafrica.net
  e-Mail : sales@scitz.com Tel. : +255 22 2198600

▶ Softnet Technologies Limited

- Softnet은 네트워킹, 데이터센터, 서비스 관리 등의 일을 하며 서비스와 제품을 제공하는 기업으로 2002년에 설립되었으며 2014년에는 70명 이상의 직원이 IT 자격증을 갖고 전문적인 팀을 구성하며 빠른 성장을 보임

334 http://www.mart-networks.com/products-solutions

- 탄자니아의 대기업과 수많은 중소기업고객에게 비즈니스 중심의 기술솔루션을 제공하며 확장하여 탄자니아와 케냐에 2개 사무소 11개 지사를 갖고 있음
- 연락처 : Home Page : http://softnet.co.tz
  e-Mail : info@softnet.co.tz Tel. : +255 222 515 100

▶ ComSec Security Systems Ltd.

- ComSec은 선도적인 보안업체가 설계하고 제작한 보안 시스템과 솔루션을 제공하며, CCTV 감시, 접속 제어, 보안 검색, 침입자 경보기 등의 보안 제품과 스마트 뱅킹 솔루션을 제공하는 기업임
- 탄자니아의 계약자 등록 위원회(Contractors Registration Board)에 1등급 보안 전문업체로 등록되어 있으며, 금융기관, 공항 및 항만, 쇼핑몰, 호텔, 정부기관, 경찰 등 의 고객들에게 솔루션과 제품을 제공하며 본사는 탄자니아 다르에르살람에 위치하고, Mbeya, Mwanza, Arusha에 지사를 두고 있음
- 연락처 : Home Page : comsec.co.tz/
  e-Mail : comsec@comsec.co.tz Tel. : +255 22 2865137/8

4) 주요 동향 및 이슈

▶ 탄자니아, 탄자나이트 광물의 도난 방지를 위해 CCTV 카메라 설치(2019년 2월)[335]

- 탄자니아 당국자들은 탄자나이트 광물 도난을 통제하기 위해 Manyara 지역의 Mirerani 광산 주위 벽에 CCTV 카메라를 설치하기 시작함
- 광산을 벽으로 막는 것만으로는 충분하지 않으며, 상인, 광부, 판매 당국 모두에게 안전이 보장되도록 광산 내 및 주변의 모든 지역을 24시간 모니터링 하고자 감시 CCTV 카메라를 설치함
- Starfix Enterprises라는 회사가 정부의 위임을 받아 감시 카메라, 스캐너, 기타 안전 전자 장치를 설치함

▶ 탄자니아 정부는 통신사가 모바일 머니 사기 희생자에게 환불하는 방안을 고려(2018년 7월)[336][337]

- 탄자니아 당국은 만연한 모바일 머니 절도를 제어하기 위해 새로운 법을 제정하거나 현행법을 구현할 필요가 있는지를 고려 중
- 모바일 머니 가입자를 겨냥한 모바일 머니 절도를 통제하기 위해 적절한 조치를 취하는 정부의 노력에도 불구하고 상황이 너무 만연해 정부의 긴급 개입이 요청됐음
- 정부측에서는 모바일 가입자로부터 돈을 훔칠 수 있는 방법의 가능성에 회사의 직원이거나 일했던 직원일 가능성도 있으므로 정부는 고객이 관련된 범죄자를 추적하는 동안 이동통신 회사가

335 "Tanzania installs CCTV cameras to control theft of Tanzanite minerals", Xinhua, 2019.2.27.
336 "Tanzania considers pushing telcos to refund mobile money fraud victims", Business Daily, 2018.7.25.
337 "Vodacom has 30 days to give answers on cyber crime", The Citizen, 2018.7 24

고객들에게 환급해 줄 책임이 있는 솔루션을 찾고 있음을 언급함

- 노동교통통신부 장관은 Vodacom Tanzania Plc.에 회사의 사이버 범죄 관련 문제에 대한 답변을 제공하도록 30일을 주었음
- 장관은 만약 회사의 경영진이 문제 해결 방법에 대한 상세한 답변을 제공하지 않으면 네트워크상에 일어나는 어떤 온라인 범죄에 대해 상환 책임이 있다고 밝혔음

▶ 한국의 KT는 탄자니아에 전자주민등록 데이터센터 구축을 완료함(2018년 7월)[338]

- KT는 탄자니아 주민등록청이 발주한 사업을 지난 2015년 4월에 착수해 3년 3개월에 걸쳐 추진하여, 탄자니아 전자주민등록 사업을 위한 메인 데이터센터와 백업센터, 13개 지역 주민등록소의 건축과 지문인식 관리시스템, 네트워크 관제시스템, 주민등록 웹 사이트 등 IT 시스템 구축까지 모두 담당하였음
- KT-삼성물산 컨소시엄이 주도한 이번 사업은 526억 원 규모이며, IT, 네트워크 분야의 국내 우수 중소기업 15개사가 참여해 해외에서 사업실적을 쌓았음
- KT는 완료한 데이터센터 구축에 이어 2020년 6월까지 유지보수를 맡게 되었고, 탄자니아 정부는 KT가 데이터센터 구축을 완료함에 따라 전자주민등록 사업을 본격화 할 계획임

5) 정보보호 스타트업 시장 현황

▶ 다양한 기술 관련 기관들이 합류하여 다르에스살람은 '실리콘 다르'를 형성 중(2019년 7월)[339]

- 다르에스살람의 Moroco Road 교차점에 Ali Hassan Mwinyi Road에 Vodacom, TTC, Zantel과 같은 주요 통신 본사가 위치하고, 탄자니아 과학기술위원회, Buni 허브, 다르에스살람 대학교 등이 위치하면서 다양한 기술 기관들이 합류하며 이 일대가 탄자니아의 새로운 기술 허브로 혁신생태계를 반영하며 이곳의 기술 전문가들은 '실리콘 다르(Silicon Dar)'라 부름[340]
- 통신사들은 인터넷 연결을 보장하며, 인프라와 전기, 국영 기관들은 청년 기업가에게 소규모 보조금을 통해 데이터 주도 혁신을 촉진함
- 다르에스살람 대학 컴퓨팅 센터의 데이터 센터 및 데이터 주도 혁신인 탄자니아 데이터 랩, Seedspace, KiotaHub, Hub255도 이 지역에서 위치하고 있으며, 현재 이 일대에는 약 12개의 혁신 허브가 위치하며, 이러한 혁신 허브들은 수백명의 청년 기업가에게 기회와 자원을 제공함
- 예를 들어 건강 및 의료 지원 정보도 DLIIC(Data for Local Impact Innovation Challenge)를 통해

338 "KT, 탄자니아에 '전자주민등록 데이터센터' 구축 완료", KT 보도자료, 2018.7.24.
339 "Tanzania's self-formed 'Silicon Dar' turning city into smart hub", TheEastAfrican, 2019.7.23.
340 silicondar.org/

제공되며, 헬스케어 서비스 관련 정보를 제공하는 모바일 앱인 AfyaBox는 2017년 3월 DLIIC로부터 2만 달러 보조금과 더불어 훈련 및 멘토십을 받음

- 통신사들은 자체 프로그램을 통해 혁신 시스템에 포함되어 있는데, 예를 들어 Vodacom은 14세~18세 사이의 젊은 여성을 대상으로 '여자 같은 코드(Code like a girl)' 프로그램으로 기본적인 IT지식을 갖고 있는 사용자를 지원하는 클라우드 스토리지 앱 Tigo Backup과 Tigo Twende와 같은 코딩 앱 프로그램을 통해 생태계에 포함됨
- DTBi(Dar Teknohama Business Incubator)는 탄자니아의 디지털 혁신 청년 강화 프로그램(Tanzania Digital Innovation Youth Empowerment Programme)을 운영하여 청년 기업가에게 기업가정신과 디지털 문맹 퇴치 기술을 가르침
- DTBi는 모바일 기반 학습 플랫폼인 Business Entrepreneurship Skills Platform을 통해 비즈니스와 기업가 정신 지식 및 기술을 확산하고 있으며, 또한 Vodacom과 dLab과 협력하여 'Code like a girl' 운영도 지원하여 젊은 여성에게 기술 혁신에 관한 기술 및 기업가 정신을 불어 넣고 있음
- 이 지역은 또한 여러 주요 은행 및 소액금융 기관이 위치하고 있어 스타트업과 중소기업(SME)을 위한 대체 금융을 제공할 수 있음

▶ LAD 컨설팅은 다르에스살람에서 이스라엘의 새로운 사이버 보안 기술을 아프리카의 사이버 보안 전문가에게 소개하고자 관련된 다양한 meet up 행사를 주최함[341]

- LAD 컨설팅은 아프리카에서 활동하는 이스라엘의 혁신적인 사이버 보안 기술회사로 사이버 보안 부문에서 200개 이상의 스타트업 회사가 활동하고 있으며, 혁신 솔루션을 아프리카에 소개하고 인지도를 높여 시장에 비용 효율적인 솔루션을 제공하고자 함
- LAD 컨설팅사는 새로운 사이버 보안 과정 및 인증 소개 행사, 이스라엘의 사이버 보안 기술의 혁신과 최신 동향에 관련된 행사 등을 개최함

341 LAD consulting의 meet up 웹사이트 https://www.meetup.com/ko-KR/Cyberafrica/

정보보호 정책 및 기관 현황

1) 관련 법령 및 정책

관련 법령 및 규제

▶ 사이버 범죄에 관한 법(Cybercrimes Act 2015)

- 2015년 2월 20일 사이버 범죄에 대한 법률(Cybercrimes Act, 2015)이 제정되어[342] 2015년 9월 1일부터 발효[343]
- 컴퓨터 시스템 및 정보통신 기술과 관련된 범죄 관련 조항들이 포함 되며, 전자적 증거의 조사, 수집, 사용 등의 내용들이 포함
- 또한 해킹, 불법기기, 온라인 사기, 거짓정보, 유해 콘텐츠, 데이터 보호, 사이버 공격 등의 불법성과 사업자의 책임에 대해 다루고 있음

▶ 전자거래법(The Electronic Transactions Act 2015)

- 2015년 5월 전자거래에 대한 법률(The Electronic Transactions Act 2015) 제정[344]
- 전자거래법은 전자거래, 전자정부서비스, 증거수집에서 ICT의 사용, 전자증거의 허용, 안전한 전자서명의 사용의 촉진, 그리고 다른 관련된 문제들을 다루고 있음

▶ 컴퓨터긴급대응팀 규제(CERT Regulations)

- 2011년 탄자니아 정부는 CERT에 대한 규제 내용을 전자우편통신법을 통해 공표[345]
- CERT는 관련된 보안 사고로부터 컴퓨터를 보호하고 해결책을 지원 및 해결하기 위해 필요한 서비스를 제공함으로써 컴퓨터 보안 사고에 대응하는 팀을 정의하며, 또한 이들의 권한과 설립, 국가CERT의 구성, 책임, 등의 내용을 포함
- 또한, 사이버 보안에 대한 서비스 제공자들의 의무를 포함

▶ 전자 및 우편 통신 규제 2018(Electronic and Postal Communications Regulations 2018)

---

342 "The Cybercrimes ACT, 2015", The United Republic of Tanzania, 2015
343 "Recognising significance of cyber security awareness", DailyNews, 2015.10.1.
344 "The Electronic Transactions Act, 2015", The United Republic of Tanzania, 2015
345 "The Electronics and Postal Communications(Computer Emergency Response Team) Regulations, 2011", The United Republic of Tanzania,

- 개정된 해당 규제는 블로거, 인터넷 카페, 온라인 콘텐츠 호스트, 소셜 미디어, 라이선스가 부여된 온라인 콘텐츠 사용자에 대해 요구사항 요구사항이 있음
- 예를 들어 온라인 콘텐츠 게시자 및 스트리밍 콘텐츠에 대한 신청 및 라이선스/갱신 요금이 도입됨
- 수정된 전자 및 우편 통신 규제는 2018년 3월에 발효되었으며, 법률 및 인권 센터, 탄자니아 미디어 협의회 등은 이에 반대했으나 5월에 법원 명령은 정부를 지지함
- 해당 규제는 외설적, 증오심의 표현, 극단적인 폭력이나 타인을 불쾌하게 하거나 선통하거나 범죄를 유발하거나 위협하거나 장려하거나 선동하거나 공공 무질서에 이르게 하는 내용으로 간주되는 콘텐츠를 게시하는 경우 허가를 취소 할 수 있는 권리를 정부에게 부여함[346]

주요 전략 및 정책

▶ 국가발전계획(Vision 2025)

- 국가발전계획인 비전 2025(Vision 2025)는 원조 의존 및 1차 산업위주의 경제구조를 다변화하여 2025년 중소득국으로 발전하고자 주요 발전계획 및 이행사항을 명시
- 국가발전계획 비전 2025에서 ICT의 역할은 ICT활용과 교육을 통한 지식중심사회, 지속가능한 발전 및 혜택 공유, 이를 위한 국가 경쟁력 확보에 해당

▶ 탄자니아 5개년 개발 계획(2016/2017 – 2020/2021)[347]

- 거시경제 지표

지표	2015/2016	2020/2021
실제 경제성장률 (%)	7.0	10.0
일인당 국민총생산 (USD)	1,005	1,500
환율 (TZS/USD 1)	1,985.39	2,185.62
회계 예산 (TZS, billion)	14,604	32,663

- ICT 거버넌스 부문

구분	도전과제	요구되는 추진방안	기대결과
주민증 발급	. 탄자니아 국민들이 주민증 미보유	. 18세 이상 모든 국민에게 주민증 발급	. 2021년 6월까지 모든 국민들이 주민증 사용

346 "Tanzania cyber law introduces $900 fees for bloggers, compulsory passwords", Euronews, 2018.4.12.
347 NATIONAL FIVE YEAR DEVELOPMENT PLAN 2016/2017 – 2020/2021(2016.6)

	소요예산 (TSH, Billion)	2016/17	2017/18	2018/19	2019/20	2020/21
	327.41	65.48	65.48	65.48	65.48	65.48

• ICT 및 전자정부(E-Gov) 부문 : 전체 소요예산 37,322.36(TSHS, Billion)

구분	도전과제		요구되는 추진전략		기대결과	
ICT 장비, 제조, e-폐기물 재활용 및 소프트개발센터 구축(설립)	. ICT분야 숙련 기술자 . 사업 재원마련 . 사업수립을 위한 적절한 제안		. 내실있는 사업제안		. 컴퓨터 및 라디오 제고/조립 공장 설립;ICT 및 전자 하드웨어를 위한 재활용 센터 . ICT 인큐베이터	
	소요예산 (TSH, Billion)	2016/17	2017/18	2018/19	2019/20	2020/21
	N/A	N/A	N/A	N/A	N/A	N/A
ICT 파크, 수출처리구역(EPZA) – 바가모요 도시	. 기반시설 부족 . 재원 부족		. 국토.지형.지질 조사 . 마스터 플랜 수립 . 상세 공학 설계 및 기반시설 BOQ 준비		. 고품질 직업 진흥	
	소요예산 (TSH, Billion)	2016/17	2017/18	2018/19	2019/20	2020/21
	3.51	1.00	0.63	0.63	0.63	0.63
국가 ICT 브로드밴드 백본 (3단계 – 2단계 일부) – 도도마 수도	. 네트워크 연결 부족		. 네트워크 확장 . 지역 전송 네트워크 . 도도마 인터넷 데이터 센터(IDC) 구축		. ICT 네트워크 백본 확장 . 2020.6월까지 동남 아프리카 통신 허브국가로 자리 매김	
	소요예산 (TSH, Billion)	2016/17	2017/18	2018/19	2019/20	2020/21
	794.73	158.95	158.95	158.95	158.95	158.95
우편 통신: 92개 구역 국가 주소 체계	. 우편서비스 열악		-		. 정보 산업화를 위해 우편통신서비스 개선	
	소요예산 (TSH, Billion)	2016/17	2017/18	2018/19	2019/20	2020/21
	57.88	14.40	14.40	14.40	14.40	N/A
산업 환경	. 제조업의 오염가스		. 센서 기술에 기반한		. 산업 안전성 증가	

<table>
<tr><th>구분</th><th colspan="2">도전과제</th><th colspan="2">요구되는 추진전략</th><th colspan="2">기대결과</th></tr>
<tr><td rowspan="3">모니터링을 위한 무선 센서 네트워크 개발</td><td colspan="2">. 대량 방출 초보적인 기술을 활용하고 있어 제대로 모니터링이 되지 않고 있음</td><td colspan="2">산업 환경 오염 가스 모니터링</td><td colspan="2">. 환경 오염 감소</td></tr>
<tr><td>소요예산 (TSH, Billion)</td><td>2016/17</td><td>2017/18</td><td>2018/19</td><td>2019/20</td><td>2020/21</td></tr>
<tr><td>1.50</td><td>N/A</td><td>0.70</td><td>0.80</td><td>N/A</td><td>N/A</td></tr>
<tr><td rowspan="3">첨단 사이버보안 교육훈련(TIRDO)
※ TIRDO : 탄자니아 산업 연구개발 기관</td><td colspan="2">. 주요시설 기반보호 불충분
. 은행거래 매체가 안전하지 않음
. 사이버보안 위협에 대한 인식 부족</td><td colspan="2">. 인식제고를 위한 사이버보안 교육
. 정보보호 수단 수립
. 산업 응용 소프트웨어 개발</td><td colspan="2">. 정보보호 수준 및 인식 제고</td></tr>
<tr><td>소요예산 (TSH, Billion)</td><td>2016/17</td><td>2017/18</td><td>2018/19</td><td>2019/20</td><td>2020/21</td></tr>
<tr><td>0.50</td><td>0.20</td><td>0.30</td><td>N/A</td><td>N/A</td><td>N/A</td></tr>
<tr><td rowspan="3">개방형(Open) 정부 및 데이터</td><td colspan="2">. 국민에게 데이터를 전달하고 계획수립, 의사결정, 개발을 위한 혁신 및 연구 등 다목적 이용을 위한 최신 메커니즘 부족</td><td colspan="2">. 데이터 품질 관리를 위한 표준 및 가이드라인 개발
. 개방형 정부 및 데이터를 위한 공통 인프라 및 응용프로그램 개발</td><td colspan="2">. ICT 인큐베이터</td></tr>
<tr><td>소요예산 (TSH, Billion)</td><td>2016/17</td><td>2017/18</td><td>2018/19</td><td>2019/20</td><td>2020/21</td></tr>
<tr><td>2.50</td><td>0.50</td><td>1.00</td><td>1.00</td><td>N/A</td><td>N/A</td></tr>
</table>

<table>
<tr><th>구분</th><th colspan="2">도전과제</th><th colspan="2">요구되는 추진전략</th><th colspan="2">기대결과</th></tr>
<tr><td rowspan="2">전자정부 - 거버넌스 및 조직 프레임워크</td><td colspan="2">. 전자정부 구현을 조율, 감독, 촉진을 책임지는 기관과 ICT부서간 효과적인 조율 부족</td><td colspan="2">. 전자정부 구현의 감독 및 조율을 맡는 기관 강화</td><td colspan="2">. 정부 기관의 데이터 및 정보의 품질 및 신뢰성 강화</td></tr>
<tr><td>소요예산 (TSH, Billion)</td><td>2016/17</td><td>2017/18</td><td>2018/19</td><td>2019/20</td><td>2020/21</td></tr>
</table>

<table>
<tr><td></td><td>5.00</td><td>1.00</td><td>3.00</td><td>1.00</td><td>N/A</td><td>N/A</td></tr>
<tr><td rowspan="3">전자정부 - 기반시설</td><td colspan="2">. 대부분의 정부기관이 기존의 정부 네트워크에 연결되어 있지 않아 능률적인 의사결정과 서비스 제공이 어려움</td><td colspan="2">. 모든 정부기관을 안전한 정부 네트워크에 연결</td><td colspan="2">. 정부간 네트워크 연결을 통해 효율적인 의사결정 및 서비스 제공</td></tr>
<tr><td>소요예산 (TSH, Billion)</td><td>2016/17</td><td>2017/18</td><td>2018/19</td><td>2019/20</td><td>2020/21</td></tr>
<tr><td>11.00</td><td>N/A</td><td>4.00</td><td>3.00</td><td>2.00</td><td>2.00</td></tr>
<tr><td rowspan="3">전자정부 - 연구개발</td><td colspan="2">. 전자정부 연구결과의 부적절한 활용
. 전자정부 연구개발 부족</td><td colspan="2">. 전자정부 연구, 혁신, 개발센터 구축</td><td colspan="2">. 지속가능한 전자정부 응용
. 국민에게 서비스 제공에 있어 정부 이슈를 취급하는 다양한 프로그램 혁신개발</td></tr>
<tr><td>소요예산 (TSH, Billion)</td><td>2016/17</td><td>2017/18</td><td>2018/19</td><td>2019/20</td><td>2020/21</td></tr>
<tr><td>26.00</td><td>10.00</td><td>16.00</td><td>N/A</td><td>N/A</td><td>N/A</td></tr>
<tr><td rowspan="3">전자정부 - 정보보호</td><td colspan="2">. 정부 정보보호를 위한 불충분한 자원(인력, 예산, 기술 등)</td><td colspan="2">. 전자정부 사이버보안 센터 구축</td><td colspan="2">. 보안사고 위험 감소</td></tr>
<tr><td>소요예산 (TSH, Billion)</td><td>2016/17</td><td>2017/18</td><td>2018/19</td><td>2019/20</td><td>2020/21</td></tr>
<tr><td>5.00</td><td>2.00</td><td>1.00</td><td>1.00</td><td>1.00</td><td>N/A</td></tr>
</table>

구분	도전과제	요구되는 추진전략	기대결과
전자정부 - 전송채널	. 국민에게 정부서비스를 제공하기 위한 채널	. 정부 모바일 서비스 제공 플랫폼 구축 . 전자정부 키오스크	. 정부서비스 제공 및 접근 관련 편리한 환경

	부족		개발		. 정부서비스 제공 및 접근 관련 비용 및 시간 절약	
	소요예산 (TSH, Billion)	2016/17	2017/18	2018/19	2019/20	2020/21
	25.00	N/A	8.00	7.00	10.00	N/A
전자정부 – 응용플랫폼	. 데이터를 주고 받지 않는 체계		. 정부 데이터 교환 플랫폼 구축		. 의사결정을 위해 데이터 및 정보를 교환하는 시스템 및 응용프로그램	
	소요예산 (TSH, Billion)	2016/17	2017/18	2018/19	2019/20	2020/21
	944.62	188.05	215.98	191.78	186.98	161.58

▶ 경찰청의 사이버 범죄 대응 전략[348]

- 탄자니아 경찰청(Tanzania Police Force)은 "Crime and Traffic Incident Statistics Report 2016"를 2017년 1월 발행하였으며, 보고서 내용에는 사이버범죄에 대응하기 위한 전략을 포함함
- 경찰청에서는 사이버범죄 위반이 발생하는 가능한 원인들로는 1) 경제적인 어려움, 2) 도덕성의 결핍, 3) 가난한 사람들이 잘 사는 사람들로부터 훔치고 싶은 유혹의 원인이 되는 도시화, 4) 사람들이 적절히 불법을 획득하는 방법에 관한 새로운 범죄행위들에 노출시키는 세계화, 5) 가난, 6) 빈부의 큰 격차, 7) 청년층 실업, 8) 부를 축적하고자 하는 욕구 등이 있음
- 경찰청은 사이버범죄에 대응하기 위한 전략으로 1) 사이버 범죄를 다루는 금융 기관과 협력, 2) 청년들이 적절한 문화 및 사회 활동에 참여하도록 격려하기 위해 대중 및 기타 이해관계자들을 공감하게 함, 3) 자영업, 특히 청년 그룹에 대한 교육을 포함함

2) 담당기관

▶ 탄자니아 침해사고대응팀(Tanzania Computer Emergency Response Team, TZ-CERT)[349]

- 2015년 5월에 출범한 탄자니아 침해사고대응팀(TZ-CERT)은 국가차원에서 사이버 보안 사고에 대한

348 The United Republic of Tanzania, 'Crime and Traffic Incidents Statistics Report', 2017.1. p. 65.
349 https://www.tzcert.go.tz/

대응을 조정하고, 사이버 보안 사고의 관리에 관련된 지역적, 국제적인 주체들과 협력

- TZ-CERT는 사고 대응, 포털과 등록된 회원을 통해 커뮤니티에게 보안 경고 및 알림, 취약성과 보안 위협에 대한 자문, 정보보안 인식, 기술 역량 강화 등을 제공함
- TZ-CERT의 서비스는 악성코드 분석, 침입 탐지, 현장 사고 대응 등을 포함
- 사이버범죄 사건에 대한 대응을 조정하는 것을 지원하는 CERT 설립에 대한 가이드라인을 제공하는 법률인 전자우편통신법(Electronic and Postal Communications Act, EPOCA)은 2010년에 통과되었으며[350] TZ-CERT는 통신규제청(TCRA)에 설립됨

▶ 노동교통통신부(Ministry of Works, Transport and Communication), MWTC)

- 노동교통통신부(MWTC)의 통신부문은 2008년 ICT에 대한 투자와 환경 장려, 국가 발전에 도모하기 위해 설립
- 통신부문의 역할은 정책 형성, 모니터링과 평가, 통신, ICT, 과학기술과 혁신에 속하는 법규제 문제를 다룸
- 국가 ICT정책 2016(NICTP2016)을 실행, 모니터링, 평가, 주기적인 리뷰 등 전체적인 조정에 대한 책임을 맡음

▶ 탄자니아 통신규제청(Tanzania Communications Regulatory Authority, TCRA)

- 통신규제청(TCRA)는 통신과 방송부문 규제를 책임지는 준(quasi) 독립 정부기관, 전기통신과 우편서비스, 주파수 관리 등을 규제하기 위한 탄자니아 통신신규제법(Tanzania Communications Regulatory Act No.12 of 2003)하에 설립되었음
- ICT 보안에 관련된 정책 및 규제를 담당
- TCRA는 2003년 11월 1일에 운영을 시작하여 이전의 탄자니아 통신위원회(TTC)와 탄자니아 방송위원회(TBC)의 기능을 인계받음

▶ 탄자니아 국가 경찰청

- 탄자니아 정부는 사이버범죄 위험을 인식하여 국가 경찰청 산하에 사이버범죄 단속 조직(Cybercrime Unit)을 2012년에 설립하였으며, 사이버범죄 조사와 대응센터에서 훈련된 수사관들의 특별팀으로 구성[351]
- 탄자니아 경찰청은 다음과 같이 정보통신기술과 관련된 4개의 부문에서 사이버 보안, 사이버공간, 사이버 범죄에서 활동을 함[352]

350 Amos Nungu, "Cyber firm to boost network security in Tanzania", 2012.6.26.
351 UNIDIR, "The Cyber Index, International Security Trends and Realities", 2013. p88
352 Semboja, Haji H. et al., Cyber Security Institutional Framework in Tanzania: a policy analysis, Global Scientific Journals, Vol. 5, Issue 6, June 2017., p. 16.

부문	주요 기능
ICT 부문	내부적인 사용과 통신을 위해 ICT 기술 개발을 취급
사기 부문	인터넷 사기 및 자금 세탁을 취급
포렌식 부문	지문 서비스를 포함한 모든 범죄 현장의 포렌식 검사를 취급하며, 범죄를 저지르는데 사용된 컴퓨터를 검사, 범죄 수행에 사용된 소프트웨어 및 프로그램을 평가
지능 부문	사람과 재산의 안전을 평가

3) 규제 및 인증제도

- 정보보호 제품 및 서비스와 관련해 별도의 규제와 인증제도가 없는 것으로 조사됨

4) 최근 정책 동향 및 이슈

▶ 탄자니아는 보안 강화 및 사이버 범죄 방지를 위해 개인이 보유할 수 있는 휴대 전화 번호 수를 네트워크 당 한 개의 SIM카드로 제한할 계획(2019년 4월)[353]

- 이번 계획에는 5월 1일부터 9월까지 모든 SIM 카드 소지자의 새로운 생체 등록이 포함될 것이며, 가입자는 신원카드나 등록 번호를 제시해야 함
- 통신규제청(TCRA)에 따르면, 현재 시스템은 충분히 안전하지 않으며 2년 전에 시작된 국가 신원 카드 등록에 필수적인 중요한 가입자 세부정보가 부족한 반면, 등록된 SIM 카드에서 얻은 정보는 가입자의 국가 신원 카드에 직접 연결되어 문서에 대한 잘못된 정보나 위조가 없도록 하고자 함
- 해당계획을 통해 생체인식 등록으로 인해 개인이 동일한 네트워크의 여러 회선을 보유하지 못하게 될 것이지만, TCRA에 서면으로 적용하여 다른 네트워크의 전화 번호를 보유하거나 동일한 운영자의 추가 SIM 카드를 소유하는 경우도 허용되지만 권한을 알 수 있음

353 The East African, Tanzania to limit SIM cards to one per network, 2019.4.27.

▶ 탄자니아 통신규제청(TCRA)은 남 아프리카 통신 규제 협회의 연례 총회를 주최하여 사이버 범죄에 대해 논의(2019년 3월)[354]

- 탄자니아 통신규제청이 주최한 8차 남아프리카 통신 규제 협회(CRASA)의 연례 총회를 위해 다르에스살람에 모인 남아프리카 통신 규제 당국자는 사이버 범죄와 싸우는 방법을 논의하며 이틀간 회의를 하였음
- 이번 모임의 의제는 사이버 범죄와의 싸움 넘어서 비공개 회의의 주제는 '스마트 사회를 현실로 만들기'였으며, 탄자니아, 말라위, 모잠비크, 나미비아, 남아프리카공화국 등의 정보통신기술 및 우편 규제 기관이 참석
- 지역 통신규제 기관의 운영에 적용되는 정책과 지침을 검토하며, 지역의 연결성을 촉진할 포괄적인 방법론을 제시함
- 협회(CRASA) 회장은 높은 모바일 데이터 요금이 회원국이 직면한 과제 중 하나이며, 이동통신 사업자가 해당지역이 데이터 가격을 낮추도록 권장하기 위한 지침을 발표하기로 결정했음

▶ 탄자니아 통신규제청(TCRA)은 사기성 트래픽 추적 시스템 도입(2019년 1월)[355]

- 탄자니아 통신규제청은 사기성 트래픽을 추적하기 위한 목적으로 통신 트래픽 모니터링 시스템(telecommunication traffic monitoring system, TTMS)을 고쳤다고 밝힘
- 이 시스템은 사기성 트래픽과 모바일 머니 거래, 시스템 없이 정확하게 접근하기 어려운 데이터를 식별하는데 유용하며, TCRA는 이 시스템은 John Magufuli 대통령에게 공식적으로 양도할 것임
- 이 기술로 인해 통신규제청은 휴대전화 사업자가 고객에게 제공하는 서비스 품질을 확인 할 수 있었음

▶ 탄자니아 통신규제청(TCRA)은 탄자니아 침해사고대응팀(TZ-CERT)가 만든 인터넷 서비스 제공자들에 대한 최소 보안 가이드라인을 승인함(2018년 6월)[356]

- 동 가이드라인의 목적은 인터넷 서비스 사용자들이 적절히 보호되고, 보고된 사건이 인터넷 서비스 제공업체로부터 충분한 증거를 제공하는 효과적이고 효율적인 방식으로 대응할 수 있도록 보장하는 것임
- 동 가이드라인은 인터넷 서비스 제공자(ISP)가 고객에게 서비스를 제공하는 네트워크에 관련된 인프라에 대해 다음과 같은 운영적인 보안 요구사항에 대한 내용을 실행하도록 요구함

354 Xinhuanet, Southern Africa communication regulators meet in Tanzania to discuss cybercrime, 2019.3.28.
355 Xinhuanet, Tanzania's communications regulator introduces system to trace fraudulent traffic, 2019.1.18.
356 Tanzania Communications Regulatory Authority, Internet Service Providers Minimum Society Guidelines, 2018.6.

구분	내용
정보 보안 거버넌스, 위험 및 준수	인터넷 서비스 제공업체(ISP)는 조직 내에 다음을 실행하여 정보보안관리를 위한 기초를 제공 - 정보보안정책 - 정보보안 거버넌스, 위험 관리 및 규정 준수 프레임워크 - 조직의 정보보호 역할 및 책임 - 제 3자 서비스 관리
시스템과 시설의 보안	ISP는 다음을 보장함으로써 보안 환경을 유지하도록 요구됨 - 물리적 보안 - 접속 제어 - 감사 및 책임 - 시스템 및 네트워크 인프라의 보안
사고 관리 및 대응	ISP는 다음을 수행하여 보고된 정보보안사고가 효과적이고 효율적으로 대응되도록 함 - 사고 대응 절차 - 사고 감지 역량
정보 보안 테스트 및 감사	ISP는 다음을 보장하여 고객에게 서비스를 제공하기 위한 보안 환경을 유지하도록 요청됨 - 사고 비상 계획 테스트 - 보안 평가 - 규정 준수 모니터링 및 감사
비즈니스 연속성 관리	고객이 겪을 위험을 최소화하고 비즈니스 연속성을 보장하기 위해 ISP는 다음을 수행해야 함 - 비즈니스 연속성 전략 및 비상 계획 - 재해 복구 역량

• 탄자니아 통신규제청(TCRA)은 이러한 가이드라인을 준수하는 것을 보장하기 위해 규제 확인을 수행할 수 있음

▶ 탄자니아와 이스라엘은 주요 방위 및 안보 문제에 대한 협력 강화하기로 합의(2018년 3월)[357]

357 "Tanzania: Dar, Tel Aviv Ties Under Revival", allAfrica, 2018.3.22.

- 탄자니아와 이스라엘의 국방부 장관은 모든 형태의 안보 위협을 제거하기 위한 중요 정보를 공유하기 위해 양해각서에 서명하였고, 사이버 및 영토 보안, 개선된 군사 기술, 군대 훈련 등 주요 방위 및 안보 문제에 관한 협력을 강화하기로 합의함
- 이 서명식에는 탄자니아 정보 및 보안 서비스(Tanzania Intelligence and Security Service, TISS)의 장관(Director General) 및 국방부와 내각부의 고위 관리를 포함한 최고 보안 요원들이 참석함
- 이스라엘 장관은 서명한 합의를 통해 양국이 기술 기반 보안 분야의 보안 및 전문 분야에 관한 정보를 공유하는데 도움이 될 것이라고 언급함

5) 정보보호 스타트업 관련 정책동향

▶ 탄자니아는 사이버 보안 실무교육의 주요 임무를 포함한 ICT 센터 건설을 위해 세계은행(WB)로부터 1,600만 달러를 받음(2019년 9월)[358]

- 탄자니아의 다르에스살람 기술대학(Dar es Salaam Institute of Technology, DIT)은 지역 대표 ICT 센터 구축하며, 이 시설의 주요 임무는 동아프리카 공동체(East African Community, EAC) 의제 중 하나인 사이버 보안에 대한 실무 교육을 포함
- 이 센터는 매년 2,000명의 학생과 2,500명의 단기 과정을 수용할 수 있게 되며, 사이버 보안 관련 커리큘럼은 아프리카 각 국의 EAC 회원국 및 기타 국가의 이해 관계자가 준비하고 승인하여 아프리카 대륙 전체에서 더 많은 학생을 유치하고 혁신을 장려 할 것임
- 센터는 2021학년도에 완료되어 운영될 예정이며, 이 센터는 모든 산업화 이슈에 많은 노력을 기울이게 될 것이며, 미국 MIT의 ICT전문가들은 이미 센터의 학생 및 트레이너와 전문 지식을 공유할 것을 약속함
- ICT 관련 연구에서 여학생의 채용 증가 및 여성 졸업생의 고용 가능성은 세계은행이 고려해야 할 기준 중 하나에 속함

358 constructionreviewonline, Tanzania receives US $16m for construction of ICT centre, 2019.9.6

융합보안시장 및 정책 동향

사물인터넷(IoT)

▶ 2018년 7월 규제기관은 M2M/IoT 서비스의 사용 증가와 관련된 다양한 범위의 필요성에 대한 대응으로 번호 계획(numbering plan)에 대해 의논을 함[359]

- 규제기관은 ITU의 권고에 따라 15개의 숫자 범위를 사용하도록 제안하였고, M2M 장치의 활성화는 2018년 SIM 카드 등록 규제에 따라 적용됨

▶ Vodafone은 영양 실조를 해결하기 위해 설계된 탄자니아의 IoT 기반 밀가루 공장에 사물 인터넷 기술 사용하여 아프리카 전역의 농업 프로젝트를 지원[360]

- 네트워크 제공업체의 IoT 진영인 Vodafone IoT는 IoT 작물을 면밀히 모니터링함으로써 IoT 기술이 수확에 부정적인 영향을 완화하는데 도움을 줄 수 있을 것으로 기대함
- 또한, IoT 기술을 통해 직원의 효율성을 개선하고 기업의 공급망 및 운영에 대한 가시성을 제공하기 위해 구축됨
- Vodafone은 아프리카 지역에 밀가루를 제공하는 비영리 단체인 Sanku에게 밀가루 생산 기술의 효율성을 향상시키고자 관리되는 IoT 연결 플랫폼을 제공함으로써 연결성을 추가하여 데이터를 수집하고 클라우드 기반 데이터베이스로 전송하도록 통합함
- Sanku 작업자는 Vodafone의 IoT 연결 플랫폼을 사용하여 밀가루가 부족하거나 유지 보수가 필요한 경우 직원에게 알려주는 실시간 경고와 함께 100개의 밀가루 공장에 연결 할 수 있게 됨
- 이 IoT 프로젝트는 현재 탄자니아에서만 진행되고 있지만 향후 몇 년 내에 다른 아프리카 국가로 확장할 계획

블록체인(가상화폐 포함)

▶ Belfrics 그룹은 다르에스살람 기술대학(DIT)과 제휴하여 블록체인을 위한 기술 전문가 풀을 도메인으로 개발하기 위해 공동 이니셔티브를 발표[361]

- Belfrics 그룹은 전 세계 블록 체인 움직임을 주도하는 주요 대기업 중 하나로, 아시아, 아프리카, 중동, 남미 등 전 세계에 진출하여 정부 기관, 금융 규제 기관 및 대기업과 협력하여 블록체인 인프라를 구축하는 글로벌 기업 중 하나임

---

359 BuddeComme, Tanzania – Telecoms, Mobile and Broadband- Statistics and Anayses, 2019.7.4. p. 73.
360 Computerworld, How IoT is helping fight malnutrition in Tanzania with next-gen flour mills, 2019.6.26.
361 IT News Africa, Blockchain skill-drive initiative to address knowledge-gap in Tanzania, 2019.4.15.

- 이번 제휴를 통해 DIT는 블록체인 기술의 허브가 될 것이며, 직원의 역량 강화 뿐만 아니라 정부 서비스 제공을 개선하기 위한 블록체인 시스템의 실험 및 개발이 이루어질 허브가 될 것을 기대함
- DIT는 Belfrics와의 협력을 통해 학생 및 직원의 역량 구축과 디지털 기술을 갖춘 인력 생성에 중요한 것으로 인식함

▶ 2018년 탄자니아 정부는 블록체인 기술의 구현을 통해 공공 부문에서 수천 명의 '유령노동자'를 퇴치하였으며, 이 감사 업무는 정부가 상당한 비용 절감을 달성할 수 있도록 하여 주정부에 유익했음[362]

- 실제로 탄자니아는 종이에만 존재하는 유령노동자의 임금을 지불하는데 매달 4,300억 탄자니아실링(1억 9,540만 달러) 규모의 손실이 있었으며, 이제 이러한 자금이 제대로 분배될 수 있을 것으로 기대함

▶ 아일랜드의 의료 프로젝트는 탄자니아에서 세계 최초로 '블록체인 아기(blockchain baby)'를 등록함[363,364]

- 아프리카 전역에 의료 서비스를 제공하는 아일랜드 기반의 의료 프로젝트인 Aid:Tech는 디지털 신원 및 블록체인 기술을 사용하여 정부, 기업, NGO가 임산부를 식별하고 필요한 치료를 제공할 수 있는 새로운 투명한 방식임
- 2018년 7월 세계 최초 탄자니아에서 태어난 아기의 디지털 신원이 이 디지털 원장에 추가되었으며, 이와 같이 아기는 디지털 원장의 기록을 통해 의료 치료 및 자금에 쉽게 접근될 수 있음
- 해당 블록체인 프로젝트는 산모와 신생아의 의료 서비스에 대한 접근성을 높여 탄자니아에서 10만명당 556명이 사망하는 사망률을 줄이면서 투명성 및 후원자 지원 및 약품이 의도한 수혜자에게 전달되도록 함

핀테크

▶ 탄자니아의 핀테크 시장[365]

- 탄자니아는 6개의 MNO(Mobile Network Operators)들이 전자머니 송금 플랫폼 서비스를 제공하고 있는데, Vodacom의 M-PESA, Tigo의 TIGOPESA, Aritel의 Aritel Money, Zantel의 EZYPESA, Halotel의 HALOPESA, TTCL의 TTCL PESA 모바일 머니 송금 플랫폼이 있음
- MNO들의 경우, Vodacom과 CBA은행의 M-PAWA, Aritel와 Jumo의 Timiza, Tigo와 AFB금융서비스의 Nivushe services 등과 같이 고객이 저축하고 또한 소액대출을 할 수 있도록 하는 많은 금융 상품을

362 infomineo, The Upsurge of Blockchain Market in Africa 2018, 2019.6.
363 The Citizen, World's first 'blockchain baby' is Tanzanian, 2019.2.26.
364 Fairplanet, TANZANIA'S FIRST BLOCKCHAIN BABY RUBBERSTAMPS POWER OF TECH IN MEDICAL CARE, 2019.6.25.
365 global legal group, The International Comparative Legal Guide to: Fintech 2018, 2018.6.

내 놓음

- MNO을 제외하고, 탄자니아아는 핀테크 영역에서 혁신하는 많은 새로운 기업들이 있는데, 예를 들어 Jumo는 데이터 기반으로 모바일 고객에게 금융서비스를 제공하고 있으며, Mastercard에 의해 제공되고 있는 Masterpass QR은 온오프라인에서 새로운 스마트한 현금없는 지불방식이며, Tigo Pesa에 의해 제공되는 Ecobank Tanzania는 Mastercard가 Tigo와 Selcom과 협력하고 있음
- 또한, 런던기반 핀테크 회사인 Humaniq는 은행이 없는 인구를 대상으로 P2P경제가 가능한 애플리케이션을 출시하였는데 탄자니아를 포함한 5개의 아프리카 국가에서 사용가능함
- 또한, 카드를 긁거나 탭핑(tapping)을 통해 모든 형태의 비자카드, 마스터카드, Umoja, 모바일 머니 지불을 허용하는 Clickpesa와 같은 결제 게이트웨이가 등장하였음
- 이와 같은 모든 혁신은 중요한 금융 포용을 포함하며 다른 핀테크 사업을 구축하는데 자극이 됨
- 탄자니아에서 핀테크 사업은 모바일 뱅킹, 모바일 대출 및 저축, 소액 대출, 송금, 모바일 결제 시스템 등이 포함되며, 이외에 개발된 기타 주목할 만한 핀테크 사업은 결제 플랫폼, 온라인 결제 시스템, 스캔 및 탭핑(tapping) 카드 결제, 온라인 거래, 집계 및 국제 송금 사업이 있음
- 활동적인 모바일 지갑의 성장은 2,100만개 이상(탄자니아 성인인구의 75%)에 도달하였으며, 모바일 금융서비스를 활동적으로 사용하는 지갑은 1,660만개에 해당함

▶ 관련 법규제

- BoT(Bank of Tanzania)는 탄자니아은행법(Bank of Tanzania Act 20016), 국가결제시스템법(National Payment System Act 2015, NPS Act), 은행및금융기관법(Banking and Financial Institutions Act 2006)하에 권한이 확정됨에 따라 핀테크 사업까지 확장하여 탄자니아의 금융 부문 규제기관임
- 특히 BoT의 부서인 국가결제시스템은 모든 핀테크 사업을 취급하며, 시장에서 출시되는 새로운 금융 기술 제품을 검토함
- MNO에 대한 의무상장요건으로 인해 일부 핀테크 사업은 또한 자본시장 및 증권법(Capital Market and Securities Act 1994)에 의해 규제될 수 있으며, 다르에르 살람 증권거래소규칙(Dar es Salaam Stock Exchange Rules 216)을 준수해야함
- 핀테크 사업은 기술 및 통신에 의존하므로 혁신을 구현하기 위해 핀테크 사업이 자체 통신인프라를 구축하거나 인프라 공유를 수행해야 하는 경우 전자우편통신법(Electronic and Postal Communications Act 2010, EPOCA 2010)하의 라이선스나 승인이 적용될 수 있음
- 이 경우, 라이선스는 통신규제기관인 TCRA가 발행한 라이선스는 다른 라이선스가 있는 실체가 소유한 시설을 이용하기 위한 동의 서한으로 적용할 수 있음
- 탄자니아의 정책입안자, 금융 및 통신 규제기관은 핀테크 혁신을 잘 수용하고 있으며, BoT는 적절한 법적 체계가 확립되기 전에도 전자 머니 이체 플랫폼(electronic money transfer platforms)을 운영할 수 있게 했음

- 또한 TCRA는 "National Switch" 상호운용성 계약에 서명함으로써 고객이 서로 다른 모바일 머니 지갑에 이체 할 수 있음
- BoT는 탄자니아에서 암호화화폐(cryptocurrency)에 대해 회의적이지만, 이를 금지하지는 않았으며, 시스템 붕괴 시 사용할 수 있는 보호 기능이 없기 때문에 암호화화폐 처리에 대해 대중에게 경고하는 공개 통지를 발표하였음
- 그러나 BoT는 가상 통화 규제를 포함하거나 금지하는 추가 조치를 고려하기 전에 탄자니아에서 암호화화폐의 사용을 계속 모니터링 할 것이라고 밝힘

▶ BoT(Bank of Tanzania)는 즉시 지불 시스템(instant payment system)인 TIPS(Tanzania Instant Payment System)을 개발하는 프로젝트를 2019년 2월에 시작하였음[366]

- TIPS는 2020년 6월에는 운영할 것으로 예상되며, 단일 즉시 지불시스템으로 비용이 효과적이고 안전한 시스템으로 다른 지불 시스템 제공업자와 연결 될 것임
- TIPS는 디지털 금융 서비스 제공업체의 상호운용성을 통해 금융 포용을 촉진할 것으로 기대됨

366 Governor Bank of Tanzania, "Monetary Policy Statement 2019/20", p.36. 2019.6.

나. 르완다

'18년 GDP(십억달러)	9.51
'18년 인구수(천명)	12,300

■ ITU 글로벌 사이버보안 지수(Global Cybersecurity Index, GCI)

· 르완다의 글로벌 사이버보안 지수순위는 49위이며, 아프리카 국가 중 3위에 위치

국가명	2018		2017		2016		전년대비 증감	
	지수	순위	지수	순위	지수	순위	지수	순위
르완다	0.697	49	0.602	36	-	-	+0.095	-13
대한민국	0.873	15	0.782	13	-	-	+0.091	-2

■ ICT 관련 주요 지수

· 르완다의 전반적인 ICT 발전 수준은 100위권 밖으로 중하위권에 속함

지표명	르완다		한국	
	점수	순위	점수	순위
IMD 국가경쟁력지수(2019)	-	-	-	28
IMD 디지털경쟁력지수(2019)	-	-	-	10
UNCTAD 전자상거래지수(2019)	30.9	121	89.4	19
ITU 글로벌 사이버보안 지수(GCI 2018)	0.697	49	0.873	15
UN 전자정부 지수(2018)	0.459	120	0.901	3

■ ICT 관련 주요 통계 (ITU, 2018년 말 기준)

· 르완다의 유선통신 보급률은 0.11%로 거의 이용하지 않으며, 대신 이동통신을 활용

항목	르완다		한국	
	가입자수(천 명)	보급률(%)	가입자수(천 명)	보급률(%)
유선전화	13	0.11	25,907	50.63
유선브로드밴드	8	0.06	21,286	41.60
이동통신	9,701	78.85	66,356	129.67
인터넷 이용률	-		95.90%	

정보보호 산업 개요

1) 보안 환경

▶ ICT 발전과 함께 사이버 보안 위협과 범죄가 증가, 특히 온라인 금융사기와 관련됨

- 르완다는 증가하는 ICT 연결성, 인터넷 접속의 증가 및 발전으로 인해 사이버 보안 위협과 사이버 범죄의 증가로, 관련 법제도 및 담당 기관 설립 뿐 아니라 국민들의 사이버 보안에 대한 인식이 필요
- 르완다는 정책적으로 ICT를 통해 경제사회발전을 이루고자 하여, 전자정부, 전자상거래, e-Banking, 다른 ICT 기반 서비스 뿐 아니라 르완다 사회는 점점 비즈니스, 건강, 교육, 농업, 등 다른 부문에서도 ICT의 의존성이 점점 증가함
- 르완다 중앙은행은 르완다의 전자 금융 시스템이 성장함에 따라 금융부문은 사이버 보안 위협 및 사기에 취약하다고 경고하였으며,[367] 특히, 사이버 범죄는 모바일 머니 송금과 같은 특정 부문이 타깃이 되고 있으며, 이러한 사이버 범죄로 인해 국가 경제에도 피해를 줌

▶ ITU가 2019년 3월 발표한 'Global Cybersecurity Index 2018'에 따르면 르완다의 사이버보안 지수는 0.697, 글로벌 순위는 49위, 아프리카권역에서는 모리셔스(Mauritius), 케냐(Kenya)에 이어 3위를 기록

- 해당 지수는 법적·기술적·조직적 대응 및 역량강화, 국제협력 등 5개 부문의 지수를 종합한 것으로, 르완다는 조직 측면에서 0.178로 높은 점수를 기록하고, 국제협력 측면에서 0.108로 낮은 점수를 기록
- 르완다는 핵심 정보 인프라 보호를 감독하기 위해 국가 사이버보안 기관(National Cybersecurity Agency, NCSA)이 설립되었으며, 정부 인프라의 관리를 감독하기 위해 르완다정보사회국(Rwanda Information Society Authority)이 설립되어 있고, 또한 공익사업규제기관(Rwanda Utilities Regulatory Authority)는 민간 부문 사업자 및 서비스 제공업체를 모니터링 함
- 르완다는 사이버공간을 보호하기 위해 노력해 오고 있으며, 또한 사이버 범죄 상황을 모니터하고 위험을 평가하기 위해 국립컴퓨터침해사고대응센터(National Computer Security Incident Response Centre)를 2014년에 설립함[368]
- 르완다 정부는 2015년에 국가 사이버보안정책(National Cyber Security Policy, NCSP) 및 국가 사이버보안전략을 승인하고, 국가 정보보안 거버넌스 프레임워크 내용을 포함함
- 르완다의 국가 사이버 보안 정책은 국가의 위험, 우선순위 및 목표를 다루며 대중의 인식 제고, 사이버 범죄의 완화, 사고 대응 능력 및 국가의 핵심 인프라 보호와 관련된 문제를 해결하는 조치를 설명함

---

367 "e-Banking and cyber security", New Times, 2018.8.28.
368 The NewTimes, "Public urged to be vigilant against cyber attacks", 2015.08.30.

- NCSA의 설립은 규정된 국가 사이버 보안 정책(National Cyber Security Policy, NCSP)의 구현 지침을 제공하는 국가 사이버보안 전략 계획(National Cybersecurity Strategic Plan, NCSSP) 2015-2020을 구현하는 일을 맡고 있음
- NCSP와 NCSSP는 또한 사이버보안에 대한 역량 구축 및 투자를 촉진하며, 사이버보안 관련 지표 및 측정 프로세스가 확립되어 의사결정에 정보를 제공하기 위해 구현 및 사용됨

▶ 르완다에서 사이버 보안 문제의 주요 원인과 정부대책[369]

- 르완다에서 사이버 보안 문제는 사이버보안 영역에서 충분한 전문성과 기술 부족뿐 아니라 사이버 보안과 정보 보안 인식의 부족이 포함됨
- 이에 대해 Rw-CSIRT를 통해 국가적 차원에서 사이버 보안 의식을 고취하는 캠페인 실행함
- 정부 또한 국가 사이버 보안 인식 프로그램을 수립하였고, 주요 대상자는 공공 및 민간 부문의 모든 직급에 직원들과 ICT서비스를 사용하는 일반 대중임
- 또한 매년 '사이버 보안 인식 위크'라 불리는 프로그램을 진행하여 인식 고취시키고자 함
- 르완다는 2015년 국가 사이버 보안 정책을 채택한 후 온라인 범죄로부터 공공 기관 및 민간 기관을 보호하기 위해 300만 달러 규모의 사이버 보안 시스템을 시작함[370]
- 르완다 경찰은 사이버 범죄 부서를 구성하였고, 국방부는 정부가 '사이버 대대(Cyber Battalion)'라는 사이버 보안 부서를 시행할 것을 고려함에 따라 여성 군인들이 사이버범죄에 대응하여 주도적 역할을 수행하도록 지시함

▶ 르완다 정부 관점에서 사이버 보안 관련 현재 상태

- 사이버 보안은 ICT 정책과 규제 기능, 고객 보호, 국가적 관심과 데이터 보안의 중요성, 전자 인증 서비스 제공자에 관한 규제, 인증당국의 의무, 컴퓨터 오용, 사이버 범죄, 개인 정보 보호 등의 범위를 포함[371]
- 포괄적인 ICT 법은 전자 메시지, 전자 서명, 전자 거래에 관련된 법을 포함하는 여러 ICT 관련 법의 대체를 위한 제정됨
- 사이버 보안에 실행되고 있는 여러 인프라와 이니셔티브로는 인터넷 보안의 상태를 모니터 하기 위한 인터넷 보안센터(Internet Security Center)의 설립, 안전한 전자거래를 제공하기 위한 국가 공공키 인프라(National Public Key Infrastructure, PKI), 공공 및 개인 사이버 공간에서의 사이버 보안 사고를 예방하고 대응하기 위한 국가 컴퓨터 보안 및 사건대응팀(National Computer Security and Incident Response Team, CSIRT)의 설립을 포함함

---

369 Symantec, "Cyber Crime & Cyber Security Trends in Africa", 2016.11. p84
370 "How Rwanda Stopped Eight Million Cyber Attackers", KTPRESS, 2018.1.19.
371 Republic of Rwanda, "National Cyber Security Policy", 2015.3.

- 무엇보다도 국가 백본(National Backbone, NBB), 국가 데이터 센터(National Data Center, NDC), 4G LTE last mile 네트워크, 전자정부 시스템, 에너지 인프라, 은행 및 금융 시스템 등과 같은 중요한 인프라는 보호되어야 함
- 사이버 및 정보 보안에서 교육 및 훈련 프로그램의 개발과 실행, 지식 및 기술 이전을 위해 국제 사이버 보안 기관과의 협력 및 파트너십, 훈련 프로그램 등을 포함하여 르완다인의 사이버 보안 역량을 향상시키기 위해 여러 번의 사이버 보안 역량 강화 이니셔티브를 진행해 옴

▶ 르완다 경찰은 사이버 범죄와의 싸움에서 직면한 문제로는 공항, 정부기관 같은 주요 정부 인프라를 보호하는 책임뿐만 아니라 국가 사이버 인프라를 보호하는 것으로 발전되었음[372]

- 르완다 경찰은 사이버 보안 센터를 보유하고 있으며, 르완다 국립 경찰 아카데미(Rwandan National Police academy)는 이러한 사이버 범죄와 싸우는 방법에 대해 경찰관을 교육하고 있으며, ICT 부문의 중등 및 대학 졸업생들도 훈련을 받음
- 르완다 경찰관은 사이버 범죄에 대해 2015년 르완다는 하루에 1,000번 이상의 공격을 겪었으나, 2019년에는 하루에 15~20번으로 줄었다고 함
- 르완다 경찰은 르완다 대학(University of Rwanda)과 같은 다른 기관들과 협력하여 교과 과정, 역량 강화, 또는 르완다 정보보안국(RISA)과의 협력을 통해 침투 행위를 예방함

2) 인터넷 및 통신 환경

▶ 유선통신

- ITU의 자료에 의하면 2018년 말 기준, 유선통신 가입회선 수는 1만 2,960회선을 기록, 2017년 1만 2,333회선 대비 약 5% 증가하였음
- 2015년 이후 유선 회선수의 감소는 다수의 유선 전화 가입자들이 이동전화로 대체하면서 Liquid Telecom의 비활성 유선 회선 연결해제로 인한 것임[373]

372 "Rwanda Is Becoming Testing Ground For New Technologies", Taarifa, 2019.8.14.
373 BuddeComm, Rwanda - Telecoms, Mobile and Broadband - Statistics and Analyses, 2019.5.1. p. 32.

그림 _ 르완다 유선통신 가입 회선 및 보급률 추이

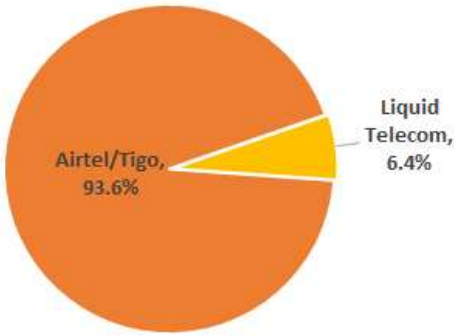
(단위: 회선, %)



[출처] ITU Statistics DB(2019.6)

그림 _ 르완다 유선통신사별 시장 점유율('19년 6월 기준)

통신사	가입자 수(명)	비율
Airtel/TIGO	9,521	93.6%
Liquid Telecom	654	6.4%
전체	10,175	100%



[출처] RURA[374](2019.6)

- 2019년 6월 기준 Airtel/TIGO 가입자 회선 수는 9,521회선, Liquid Telecom 가입자 회선 수는 654회선에 해당하며, 유선통신 시장점유율은 Airtel/Tigo(93.6%), Liquid Telecom(6.4%) 순으로 나타남[375]
- 유선가입자수는 2018년 12월 12,960회선에서 2019년 6월에는 10,175회선으로 2,785회선 정도 감소하였으며, 2019년 6월 기준 유선통신 가입률은 0.1%인 반면, 이동통신 가입률은 74.8%로 르완다 국민의 대다수는 이동통신을 사용함
- 이와 같은 유선통신의 낮은 보급 상황은 신뢰할 만한 전기의 부족, 인프라에 대한 높은 운영 및

374 Rwanda Utilities Regulatory Authority(르완다유틸리티규제청): 통신, 에너지, 상하수 등 공공산업 규제기관
375 RURA, Statistics Reoirt for Telecom, Media and Postal Sector as of the Second Quarter of the year 2019, 2019.6.

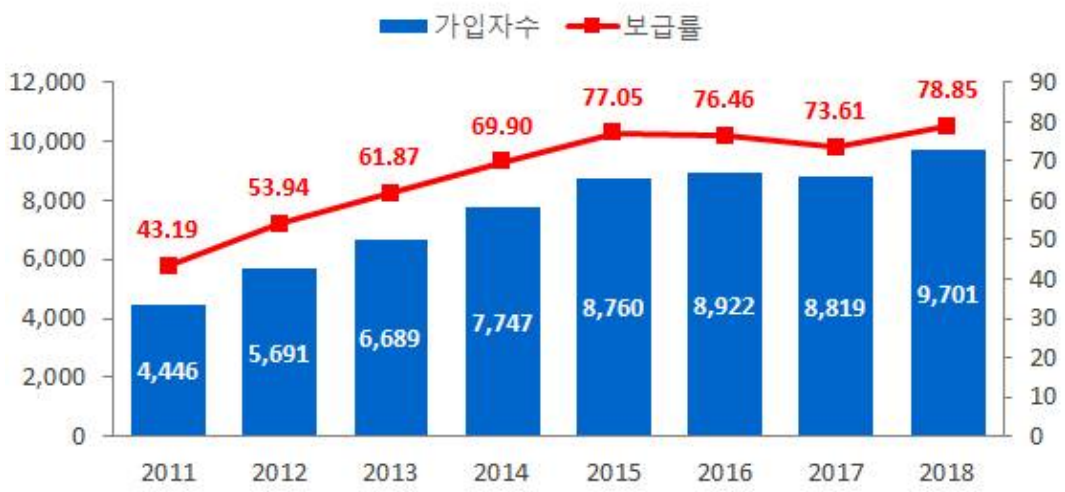
유지보수 비용, 시설파괴에 대한 낮은 보안 등 여러 부문에서의 방해요소들로 인한 것임

▶ 이동통신

- 이동통신 시장은 최근 몇 년 동안 빠른 성장을 보였지만, 2016년과 2017년에 성장이 둔화 되었고, 2018년에 다소 회복을 보여줌
- ITU의 자료에 의하면 2018년 기준 이동통신 가입자 수는 약 970만 609명을 기록하며 보급률이 78.85%로, 보급률은 2017년 대비 약 10% 증가하였고, 2011년부터 2018년까지 가입자 수의 연평균 성장률(CAGR)은 11.8%를 기록함

그림 _ 르완다 이동통신 가입 및 보급률 추이

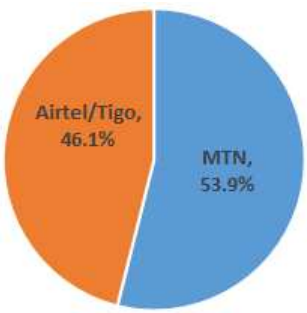
(단위: 천 명, %)



[출처] ITU Statistics DB(2019.6)

그림 _ 르완다 이동통신사별 시장 점유율('19년 6월 기준)

통신사	가입자 수(명)	비율
MTN	4,874,797	53.9%
Airtel/Tigo	4,165,530	46.1%
전체	9,040,327	100%



[출처] RURA(2019.6)

- 르완다의 이동통신 시장은 MTN Rwanda, Airtel/Tigo 2개사가 주요 경쟁을 하고 있으며, 2019년 6월 기준 시장점유율은 MTN Rwanda(53.9%), Airtel/Tigo(46.1%)순이며, MTN Rwanda의 시장 점유율이 1순위에 해당[376]
- 2009년 서비스를 시작한 Tigo는 이동통신 가입자 기반의 성장에 중요한 역할을 했지만, 2018년 초 Airtel이 Tigo 인수하는 것을 규제 승인받아, 2년 프로그램으로 인수 과정이 진행되며 이로 인해 시장에서는 상당한 통합이 이루어짐[377]
- 2018년 초 MTN Rwanda는 Airtel과 Tigo의 합병으로 예상되는 경쟁에 대응하여 3G 인프라 업그레이드에 220 Rwf(2,470만 달러)를 투자하여 구형장비를 이중 네트워크 용량으로 교체하는 것을 포함한 네트워크 변환 계획의 일부를 구성하였음[378]
- 2019년 6월 기준 2G 및 2.5G 기술은 지리적으로 99.13%, 인구의 99.92%를 커버하고, 3G 및 3.5G 기술은 지리적으로 82.52%, 인구의 93.38%를 커버함[379]
- 또한 4G LTE 기술도 지리적으로 95.1%, 인구의 97.0%를 커버하고 있어 LTE 기반 가입자 수가 상당히 증가하였으며, 이는 KTRN*의 네트워크로써, 르완다 내 전국 LTE 네트워크의 개발, 건설, 운영뿐 아니라 LTE 인프라 및 도매 서비스 제공까지 전담하고 있으며 2015년 5월 4G LTE를 개시하였음
  * KTRN은 2013년 3월 르완다개발청(RDB)와 한국의 KT간 민관합작 투자회사(KT Rwanda Networks, KTRN)임
- Tigo는 2015년 말 르완다에서 4G LTE를 개시한 첫 번째 서비스 공급자로 대중버스에 Wi-Fi 서비스를 제공하기 위해 정부와 파트너 관계를 맺었음[380]
- MTN Rwanda는 2016년 말 스마트폰 사용자를 위한 LTE 서비스를 시작하였음[381]

376 RURA, Statistics Reoirt for Telecom, Media and Postal Sector as of the Second Quarter of the year 2019, 2019.6.
377 BuddeComm, Rwanda - Telecoms, Mobile and Broadband - Statistics and Analyses, 2019.5.1.
378 BuddeComm, Rwanda - Telecoms, Mobile and Broadband - Statistics and Analyses, 2019.5.1.
379 RURA, Statistics Report for Telecom, Media and Postal Sector as of the First Quarter of the year 2019, 2019.3. p. 9.
380 Business Sweden in Eastern Africa, "Opportunities in the ICT Sector in East Africa", 2017.4.26. p13.
381 BuddeComm, Rwanda - Telecoms, Mobile and Broadband - Statistics and Analyses, 2019.5.1.

▶ 모바일 머니

그림 _ 르완다 모바일 지불 거래금액 및 거래건수 추이



[출처] RURA, (2017.12, 2018.9)자료를 기반으로 재구성

- 전통적으로 이동통신사업자들은 음성전화로부터 수익을 창출하였으나 현재는 데이터, 모바일 머니 송금 등 수익 채널을 다중화함
- 2017년 1월~2018년 9월 동안 분기별 모바일 머니 거래금액과 거래건 수 추세를 보면 2017년 2분기에 약간 감소 후 점차 증가하고 있음
- 2018년 3Q 거래금액은 약 8,267억 Rwf(약 89억 6백만 달러)[382]이며, 거래 건수는 약 9,717만 건에 해당하며, 2018년 2Q 대비 거래금액은 11.7% 증가, 거래 건수는 10.4% 증가함

그림 _ 르완다 모바일 가입자 추세



[출처] RURA, (2017.12, 2018.9)

382 2019년 9월 기준 환율: 1달러 = 923.99Rwf

- 2018년 3분기 기준 르완다의 모바일 머니 가입자 수는 약 1,071만 명으로 2018년 2분기 대비 0.3% 감소함[383]
- 르완다 인구의 약 1/3이 모바일 머니 서비스에 등록되어 있으며, 모바일 머니 서비스의 활동적인 사용자의 약 2/3이 농촌 지역에 있으며, 이들에게는 모바일 뱅킹 및 지불 시스템이 실행 가능한 대안에 해당됨
- 모바일머니 서비스 주요 사업자인 MTN, Airtel, Tigo는 2018년 중반 모바일머니 서비스에서 교차 네트워크 전송을 허용하기로 합의하였음
- 정부는 또한 민원 서비스(출생증명서, 운전면허 갱신 등)에서 지불 할 수 있는 전자 지불 플랫폼인 Irembo e-Goverment 서비스를 통해 모바일머니로 지불 할 수 있게 함

▶ 전자상거래 및 결제시장 전문 조사기관 yStats에 의하면 르완다는 아프리카지역에서 인터넷 사용률이 2019년 5월 기준 인터넷 트래픽 중 67.2%는 모바일 기기에서 발생했으며, 데스크톱은 31.5%이고, 태블릿이 1.3%로 나타남[384]

- 2017년 기준 르완다의 경우 금융기관에 계정을 소유한 비율이 37%이며, 직불카드를 소유한 비율은 5%, 신용카드의 경우 1%이며, 모바일 머니 계정을 소유한 비율은 31%에 해당함

▶ 인터넷 이용 환경

- RURA의 자료[385]에 따르면 2019년 6월 기준 르완다의 인터넷 이용자 규모는 약 623만 이상으로 이는 주민 100명당 51.6%의 보급률에 해당하고, 주로 이용하는 환경은 모바일이 99.87%를 보이고 있는 반면, 유선 환경에서는 0.13%를 보이며 대다수 인터넷 사용자는 모바일 환경을 사용하고 있음
- 또한 2019년 6월 기준 모바일 인터넷 사용자 중 4G 이용자가 76,274명으로 전체 모바일 인터넷 이용자의 1.22%에 해당함

표 _ 르완다의 플랫폼별 인터넷 이용률(2019년 6월 기준)

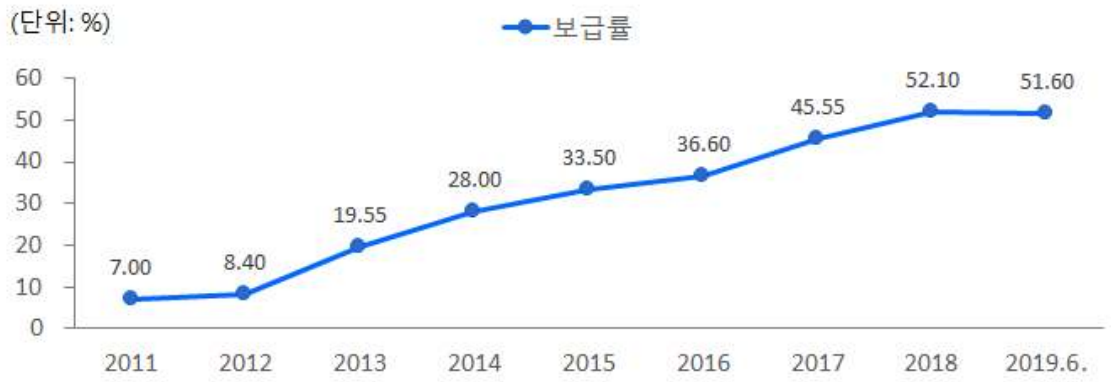
구분	이용자 수	점유율
모바일	6,226525	99.87%
유선	7,995	0.13%
전체	6,234,520	100.00%

[출처] RURA(2019.6)

383 RURA, Statistics and Tariff Information in Telecom, Media and Postal Service as of the Third Quarter 2018, 2018.9.
384 "Global E-Commerce Intelligence, Africa B2C E-Commerce & Online Payment Market 2019", yStats, 2019.6.
385 RURA, Statistics Reoirt for Telecom, Media and Postal Sector as of the Second Quarter of the year 2019, 2019.6. pp. 8-9.

- 인터넷 보급률을 살펴보면 2019년 6월 기준, 2018년 말 대비 0.5% 정도 감소하였는데, 이는 2019년 1월말부터 한 개의 ID하에 SIM카드가 6개 초과 또는 한 개의 여권하에 SIM카드 2개 초과하지 못하도록 SIM 카드 소유 수를 제한하고 있기 때문임
- 르완다의 모바일 인터넷의 전반적인 성장은 통신사의 유연한 가격 책정 모델로 인터넷 소매 가격이 하락했으며, 고객은 구매력에 따라 데이터 요금제를 선택할 수 있음[386]
- 르완다의 인터넷 및 브로드밴드 부문은 제한된 유선 인프라와 높은 가격으로 어려움을 겪고 있음에도 불구하고 사업자들은 국가의 광섬유 백본 네트워크를 출시하여 2009년 중반 이후 아프리카 동해안의 국제 해저 광섬유 케이블에 연결할 수 있게 되며, 위성에 대한 종속성을 끝낼 수 있게 됨[387]
- Liquid Telecom은 Kigali와 여러 다른 도시에 FTTP 서비스를 계속하여 확장함
- 2011년 9월 한국 통신(KT Corporation)과 계약을 체결하여 국가 광섬유 백본을 구축했으며, 2013년 9월 한국 통신과 PPP(Public-Private Partnership)에 서명하여 국가의 광섬유 인프라 위에 국가 LTE 네트워크를 구축하여 2017년 말까지 인구의 95%에게 서비스를 제공할 수 있게 됨
- 2019년 초 기준 모바일 네트워크 사업자를 제외한 27개의 라이선스 소매 인터넷 서비스 제공업체가 있음

그림 _ 르완다 인터넷 보급률 추세



[출처] RURA(2015~2019.6. 자료 종합하여 재구성)

386 "The five milestones that shaped Rwanda's ICT sector in 2018", MINICT Latest news, 2018.12.31.
387 BuddeComm, Rwanda - Telecoms, Mobile and Broadband - Statistics and Analyses, 2019.5.1.

정보보호 시장 현황

1) 시장 규모

시장 개요

▶ 르완다에서는 정부차원에서 ICT분야와 정보보안 분야 발전을 위한 종합계획을 발표하고 추진함에 따라 정보보안 수요가 증가할 것으로 예상

- 스마트 르완다 마스터 플랜(SMART Rwanda Master Plan 2015~2020)은 ICT분야 전략 계획(ICT Sector Strategic Plan 2013-2018)의 후속 정책으로 정보보안, 브로드밴드 구축, 오픈데이터를 비롯한 국가 ICT 개발의 정책 방향을 제시하고 있음
- 2017년에는 법안 통과로 국가사이버보안당국(NCSA)이 설립되어 사이버 보안에 대한 전문적인 기관운영의 제도적인 기반이 마련되어 정부의 ICT정책에서 관련된 사이버 보안 부문에 민간의 활발한 참여가 요구됨

▶ 지난 5년간 르완다의 금융부문은 57억 RwF에 해당하는 705건의 사기 사건을 기록했으며[388], 2018년 22건의 개별 사건에서 사이버 범죄자들이 2억 8,950만 르완다 프랑을 훔쳤음[389]

- 클라우드 및 보안 정상회의(Cloud and Security Summit)에 참석한 ICT 혁신부 장관은 환자 데이터 및 재무 데이터 도난을 포함한 사이버 범죄 사례는 평판 손상 및 재정 손실과 같은 피해자에게 광범위한 영향을 미치며, 특히 사이버 범죄로 인한 평판 손상은 고객관계를 구축하려는 회사에 불신을 유발 하게 된다고 강조함
- 2018년 초부터 사립 기관으로부터 74억 르완다 프랑을 훔친 사이버 범죄자의 주요 타깃은 금융기관과 통신회사이며,[390] 이것은 송금, 전자결제 및 ATM 운영을 위한 프로세스 중에 이루어졌으며, 회사와 개인도 해킹, 협박 및 기타 범죄 중에서 신원 도용을 통해 대상이 되고 있음
- 중앙은행 통계에 따르면, 2017년 한해 동안 약 15만 건의 네트워크 공격과 최소 8백만 건의 사이버공간 공격자가 르완다의 금융기관에 해킹을 시도했으며 여러 경우에 시스템 중 하나에 침입했지만 도난당한 돈은 항상 추적되고 복구되었다고 발표함[391]
- 2017년에는 80건의 해킹 사건이 등록되었으며, 이와 관련된 금액은 26억 Rwf(60만 달러) 이상으로 6개 기관이 영향을 받았음[392]

388 "Cybersecurity efforts mobilise local innovative solutions", TheNewTimes, 2018.12.21.
389 "Rwanda intensifies war on cybercrime", The New Times, 2019.4.2.
390 "Cybersecurity efforts mobilise local innovative solutions", TheNewTimes, 2018.12.21.
391 "Rwanda To Host First Ever Cybertech Conference In Africa", KTPress, 2019.8.14.
392 KTPRESS, "How Rwanda Stopped Eight Million Cyber Attackers", 2018.1.19.

- 대부분의 금융사기 사건은 경찰과 중앙은행의 공동 노력에 의해 성공적으로 회복되었으며, 여러 차례에 걸쳐 시스템 중 하나에 침투하였지만 도난당한 돈은 항상 추적되고 회수되었으며, 회수된 돈의 한 경우는 9억 르완다 프랑 금액이 도난당한 기관 중 한 곳으로 경찰의 도움으로 성공적으로 완료됨
- 그러나 2017년의 수치는 2016년 금액인 13억 르완다 프랑의 두 배로 증가하였으며 취약성 및 위협이 높아짐
- 전문가들은 사기꾼의 접근 방식 중에는 은행시스템에 접근하고 해킹하는 것, 전자자금이체, 은행직원과 공모하는 것이 있으며, 다른 일반적인 사기활동에는 POS(Point of Sale) 기계 및 신분도용이 포함됨[393]

표 _ 르완다의 등록된 금융분야 사이버 범죄 현황(2016-2017)

연도	등록된 사이버 범죄 건수	관련 피해 금액
2016	74건	1,325,050,620 르완다 프랑[394] 340,000 유로
2017	80건	2,612,101,816 르완다 프랑 605,028 달러

[출처] "How Rwanda Stopped Eight Million Cyber Attackers", KTPRESS, 2018.1.19.

▶ 국가보안국(National Security Services)의 수장에 따르면, 르와다는 사이버 위협이 사이버 테러 도구로 무기화되었으며, 사이버 지식에 대한 투자 부족, 적절한 법률, 지도자 및 사법부의 기술 부족으로 인해 급진화와 같이 그러한 범죄를 저지하는 데 방해가 됨[395]

- 2018년 체포되어 기소된 40명의 테러 용의자들의 경우, 지방법원은 그들 중 18명만 석방했으며, 22명은 소셜미디어 급진화와 테러 공격 계획에 큰 사건에 해당하였음

▶ 르완다 국립 통계 연구소의 보고서에 따르면 2017년 전체 범죄 건수는 24,179건이며, 그 중 사이버 범죄는 78건에 해당됨[396]

표 _ 르완다의 사이버 범죄(2015-2017)

393 "Cybersecurity efforts mobilise local innovative solutions", TheNewTimes, 2018.12.21.
394 Rwf(Rwanda franc): 르완다 프랑. 르완다의 통화 단위. 1Rwf=1.28원(2018년 10월 23일 기준)
395 "Kaspersky Tips Security Symposium On Cyber Security", KTPRESS, 2019.5.15.
396 "New Bill Allows Rwanda to Launch Cyber Attacks at Any Threat", KTPRESS, 2017.3.27.

범죄	2015년	2016년	2017년
사이버 범죄	66	73	78
전체 범죄	16,702	17,006	24,179

[출처] National Institute of Statistics of Rwanda, "Rwanda Statistical Yearbook 2018", 2018.12. p.153

시장 규모 및 성장률

▶ 2017년 기준 르완다 정보보안 시장 규모는 280만 달러 수준으로 추정

- 시장조사기관 Technavio의 2015년 자료에 따르면[397], 2014년 기준 르완다의 정보보안 시장 규모는 192만 달러였으며, 이를 활용해 2017년 시장 규모를 추계하는 회귀식을 구하고, 이를 2017년 변수에 적용하는 방법을 취했을 때 280만 달러 규모가 도출됨[398]

2) 분야별 현황

물리보안 제품 및 서비스

▶ 2019년 6월 르완다 정부가 결정한 2019-2020 회계 연도의 예산 2조 8천억 르완다 프랑(약30억 3,100만 USD)[399] 중에서 르완다 경찰이 공공 CCTV를 출시 할 수 있도록 최소 50억 르완다 프랑를 할당하여 경찰의 역량과 운영을 향상 시키고자 함[400]

- 또한 15억 르완다 프랑(약160만 USD)는 테스트 운영을 위한 디지털 센터 구축, 사이버 보안을 위해 19억 르완다 프랑(약 210만 USD)가 따로 할당되어 CCTV 구축 및 관련 물리보안 제품 및 서비스에 대한 수요가 증가할 것으로 기대

3) 주요 사업자 현황

397 Technavio, Global Information Security Products and Services Market 2015-2019(2015)
398 GDP와 인구규모를 독립변수로 다중회귀분석을 실시. 계수의 p값이 낮은 GDP 데이터를 활용했으며, 국가별 GDP 편차가 크게 나타나 LOG값을 취하여 다중회귀분석을 재실시하여 추정의 정확도를 제고함. 데이터가 있는 22개 국가의 시장규모와 GDP에 기울기인 1.09544492562193를 곱해서 산출
399 2019년 9월 기준 환율: 1달러 = 923.99Rwf
400 "2019/2020 Budget: Winners and losers", TheNewTimes, 2019.6.14.

▶ Pergamon Group Ltd.

- 2004년 케냐에서 설립되어 컴퓨터 악세사리 등을 제공하면서 시작하여 현재는 IT 솔루션 제공업체로 성장하며 르완다, 케냐, 탄자니아에 제품을 공급하고 있으며, 2011년부터 르완다에 사무소를 운영하고 있음
- 보안 장비로는 CCTV 카메라, IP카메라, 모바일 카메라, 보모 카메라 등 다양한 카메라 제품들, 홈 시큐리티 보안 시스템, 접근 제어 시스템, 금속 탐지기 등을 공급
- 연락처 : Home Page : rwanda.pergamongroup.com
  e-Mail : info.rwanda@pergamongroup.com
  Tel. : 0786654151, 0786654154

▶ Fodey Security & Alarm System (FOSES) LTD.

- 2000년 설립되어 르완다 키갈리에 위치하며 현재 다양한 보안 제품을 제공하며 르완다를 포함한 탄자니아, 우간다, 케냐 등에 지사를 두고 동아프리카 지역에 서비스와 제품 제공
- 알람시스템, 접속제어 장치 등의 보안 제품과 함께 알람 모니터링, CCTV 감시 등의 보안서비스도 제공
- 고객으로는 통신사 MTN, Agaseke bank, Fina Bank, East African Business Council 등 다양한 고객에게 서비스 및 제품을 제공
- 연락처 : Home Page : www.fodeysecurity.com
  e-Mail : salesfodeysecuritykigali@live.com
  Tel. : 55106062, Fax : 55106063

▶ ISCO

- ISCO는 1995년에 설립되어 현재 르완다 키갈리에 위치하며, Intersec Security 회사로부터 전통적인 보안 회사에서 혁신적인 서비스 제공자로 회사명을 다시 바꿈
- 주요 보안 제품은 보안 시스템, 비디오 감시 카메라 시스템, 알람 시스템 및 접속제어, 4G 인터넷 연결을 제공하는 4G 가능한 보안 서비스 등이 있음
- 주요 고객으로는 GTBank, EQUITY Bank, TiGo, MTN 등 은행, 통신사를 포함한 다수의 고객에게 서비스를 제공
- 연락처 : Home Page : www.isco.co.rw/
  e-Mail : info@isco.co.rw

▶ Cyberteq[401]

- Cyberteq은 르완다에 설립된 ICT 컨설팅회사로서, 비즈니스와 연결성에 안전을 위한 사이버 보안회사회사이며, 싱가포르의 Cybercom의 자회사로 2017년 설립되었으며 키갈리에 위치함
- 보안 서비스로 보안감사, IT 보안, 정보보안 등 컨설팅 서비스를 제공하며, 또한 제조, 스마트 시티, 교통, 농업 등의 부문에서 센서, 연결성, 클라우드 등을 적용한 사물인터넷을 포함한 서비스를 제공
- 정부, 은행, 금융기관, 통신사, 서비스 제공자, 산업계 등 다양한 고객들에게 정보 보안 서비스를 제공
- 연락처 : Home Page : www.cyber-teq.com
  e-Mail : info@cyber-teq.com
  Tel. : +250 788 647 718

▶ KK Security Ltd.

- KK Security Ltd.의 본사는 케냐 나이로비에 위치, 르완다, 탄자니아, 우간다 등 동아프리카 지역에 지사를 두어 보안 솔루션 제공, 르완다지사는 키갈리에 위치함
- 주요 보안 솔루션으로는 CCTV 및 모니터링 시스템, 침입 알람 시스템, 알람 모니터링 및 대응, 접속 제어, 바이오인식 시스템(biometrics system) 등과 함께 시스템 설계에 대한 보안 컨설팅 등을 제공
- 연락처 : Home Page : www.kksecurity.com
  e-Mail : kkkigali@kksecurity.com
  Tel. : +250(0) 788 907 867, +250(0) 725 404 601

▶ Sekanyolya Systems Ltd.

- 1993년 설립, 우간다에 본사를 두고 르완다 키갈리에 지사를 두어 사업을 수행함
- 보안 및 접속 제어 시스템에 대한 턴키방식의 기술 솔루션 설계 및 실행에 전문성을 지니며, 보안시스템 공급과 설치뿐 아니라 고객에게 컨설팅도 제공
- 주요 제품으로 CCTV, 접속제어시스템, 알람 등 제공
- 연락처 : Home Page : www.sekanyolya.com
  e-Mail : infor@sekanyolya.com
  Tel. : +250 788 699 000, +250 456 000 035

▶ Highsec Ltd.

- 2009년 설립되어, 르완다 키갈리에 위치하며, Airtel, gulf energy, university of Rwanda, WorldWide e-learning campus 등 공공부문 및 민간부문에 보안 서비스 및 제품을 제공함
- 주요 제품으로는 CCTV 카메라, 알람 시스템, 지문 및 홍채 등 바이오인식 시스템 등과 보안 컨설턴트 서비스 제공

401 https://www.linkedin.com/company/cyberteq

• 연락처 : Home Page : highsecltd.com
e-Mail : info@highsecltd.com, highsecltd@yahoo.com
Tel. : +250 788 309 751, +250 788 308 216

4) 주요 동향 및 이슈

▶ 보안업체 Kaspersky Lab은 르완다에 사무실을 열어 동아프리카에서 사이버보안을 강화하며 사업을 확장함(2019.5.)[402]

• Kaspersky Lab은 새로운 Kigali사무소를 통해, 지역 전체의 파트너와 고객 수를 증가시키는 것을 목표로 함
• 르완다는 Kaspersky Lab을 위한 보다 큰 공간을 제공하여 IT 및 사이버 보안 관련 문제를 다루는 르완다 회사들이 유명한 안티바이러스 솔루션 제공업체와 긴밀히 협력할 수 있는 기회를 갖게 됨
• Kaspersky Lab의 CEO는 Transform Africa Summit에서 르완다 대통령을 만나 르완다 정부와의 협력 및 사이버 위협으로부터 국가를 보호하는 방법에 대해 논의 하였으며, 새로운 지역사무소에 대한 계획과 다른 이웃 국가로 사업을 확장할 계획도 논의하였음

▶ 보안 분야 기술회사인 Secure Services Mauritius는 르완다에서 보험 회사 및 금융기관의 사이버 보안 위협을 줄이기 위해 르완다 지사를 설립(2019.3.)[403]

• Secure Services Mauritius는 2018년 9월 르완다 시장에 진출한 후, 5만 달러(약 4억 5천만 Rwf)를 초기 투자할 것이며, 인적 자원 및 기술 개발에 보다 집중할 것이며, 르완다 지사는 아프리카 대륙에 대한 투자에 필수적일 것으로 간주함
• Secure Services (Mauritius) Ltd는 2004년에 모리셔스에서 설립되었으며, 인도양 지역의 기업에게도 정보기술 서비스를 제공하고 있음
• Kigali사무소는 Citrix 및 ForcePoint와 같은 글로벌 사이버 보안업체와 비즈니스 파트너를 맺고 있음

▶ ESET East Africa는 올해의 Cyber Security Company 수상 (2018.9.)[404]

• ESET East Africa사는 2018 Digital Inclusion Awards(DIA)에서 올해의 사이버 보안 회사로 선정됨
• ESET은 기업과 일반 사용자에게 보안 솔루션을 제공하는 업체로 슬로바키아에 본사가 있고, 2015년에 나이로비에 지역 사무소를 연후 케냐에서도 운영을 하고 있으며, ESET East Africa는 르완다를

402 "Kaspersky Lab opens its office in Rwanda to boost cybersecurity in East Africa", RegionWeek, 2019.5.17.
403 "Mauritius Cyber Security Firm Opens Rwanda Subsidiary", KTPress, 2019.3.18.
404 "ESET East Africa awarded Cyber Security Company Of The Year", tech-ish.com, 2018.9.17.

포함하여 케냐, 우간다, 탄자니아를 책임짐

- 이번 수상은 동아프리카 지역에서 ESET East Africa의 전문적인 사이버 보안 제품과 서비스의 채택과 사용이 증가함에 따라 회사의 전략이 올바르게 추진되고 있음을 보여 주는 것을 의미함
- ESET이 제공하는 고객 중심 서비스에는 기업 및 직원을 대상으로 한 무료 사이버 보안 인식 교육이 포함됨
- 90분 온라인 과정을 통해 제공되는 교육은 사이버 공격 및 관련 데이터 유출의 영향 및 잠재성을 줄이는 동시에 조직이 보안 준수 요구사항을 충족하도록 돕는 것을 목표로 하며, 교육모듈에는 웹 및 전자 메일보호, 피싱 전자 메일, 암호 모범 사례, 사회공학, 2단계 인증 및 IoT 보안 방법이 포함됨

▶ Andela사는 르완다 Kigali에 범 아프리카 기술 허브를 설립 (2018.8.)[405]

- 르완다 정부는 르완다 Kigali에 Andela사의 범 아프리카 기술 허브 설립에 대한 파트너십 협약을 체결
- 향후 5년간 소프트웨어 개발 전문지식을 갖춘 500명의 르완다인을 모집하여 6개월간 유급 훈련을 제공할 계획이며 연수생들은 세계적인 경쟁력을 갖게 될 것임
- Andela사는 전 세계 45개 도시에 150개 이상의 회사가 있으며, 소프트웨어 개발자들은 미국 내 대부분의 회사와 전 세계 기업에서 원격으로 작업할 수 있을 것임
- 정보기술통신부(MITEC) 장관은 지역 기술 생태계의 경쟁력을 향상 시킬 수 있을 것으로 기대하며, 르완다가 역량 구축 요소를 갖춰 기회를 최대한 활용할 수 있을 것으로 기대함

5) 정보보호 스타트업 시장 현황

주요 동향 및 이슈

▶ 비정부 조직인 르완다 사이버 컨소시엄 구성 및 활동[406]

- 르완다 사이버 컨소시엄(Rwanda Cybersecurity Consortium, RCSC)은 비정부조직(NGO)으로 회원사 및 파트너십을 기반 협회로 활동함
- RCSC는 사이버보안 동향 및 관련 영향에 대한 최신 지식 및 기술을 습득하여 사이버보안의 다양한 관련 문제에 대해 국내외 모든 사람, 기업, 기관 및 조직이 협력 할 수 있는 올바른 환경을 제공하며, 회비, 교육비, 연구 지원비, 컨설팅 등을 통해 수익을 창출함
- RCSC는 2019년부터 시작하는 사이버보안에 16억 6천 4백만 르완다 프랑(190만 달러)이상을 투자하여 르완다의 사이버 범죄, 사이버 공격 및 위협을 줄이기 위해, 충분한 지역인력, 지식 공유,

405 "Andela to open Pan-African technology hub in Kigali", MITEC News, 2018.8.20.
406 Rwanda Cybersecurity Consortium 홈페이지: rwandacybersec.org

공공 및 민간 기관이 적정한 가격에 글로벌 최고의 사이버 보안 제품 및 서비스 제공자에 대한 접근을 제공하고자 함

- 기타 활동 및 관심분야는 지역 및 국제 파트너십, 연구, 교육 및 인증, 멘토십 및 코칭, 강의 및 세미나, 경쟁, 사이버 보안 자금 지원 기회, 고용 및 인턴십, 컨설팅 서비스, 감사, 준수 평가 등의 활동이 포함됨
- RCSC의 전략은 역량강화, 연구 및 개발, 파트너십 및 회원제, 인증, 정책 및 규제 자문 및 지원, 기금 조성 및 투자에 중점을 둠

정보보호 정책 및 기관 현황

1) 관련 법령 및 정책

관련 법령 및 규제

▶ 사이버 범죄에 관한 법(Cyber crime Law)[407,408]

- 르완다 국회는 사이버 범죄에 관한 법(Cyber crime Law)을 2018년 5월에 통과시켜 온라인 범죄와 사이버공격에 대한 민간 및 정부의 ICT 인프라를 보호하고자 함
- 기존 형법과 ICT법에 포함되어 있던 사이버범죄의 처벌 규정을 사이버 범죄에 관한 법(Cyber crime Law)으로 통합
- 정부의 보안 기관이 민간 및 공공 기관에서 모든 위협을 조사하고 사이버 범죄를 기소하고 사이버 공격으로부터 국가를 보호 할 수 있게 함
- 사이버 보안 업무가 RISA로 이관 및 전담하도록 하는 등 사이버 보안과 관련된 정책을 강력히 추진

주요 전략 및 정책

▶ 국가 ICT 전략계획(NICI Plan)

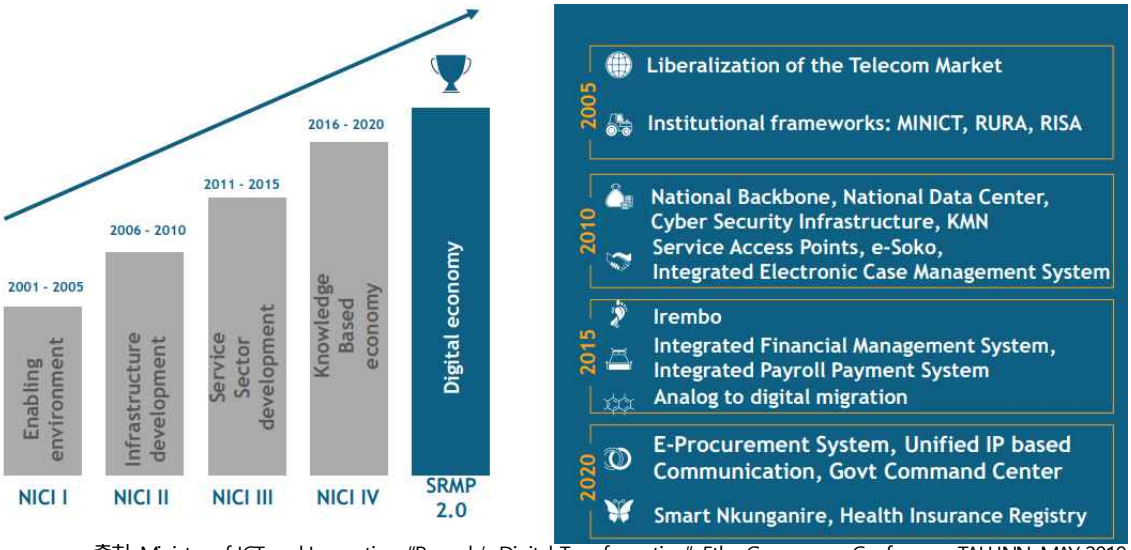
- 르완다의 ICT 전략계획은 'NICI(National Information and Communication Infrastructure) Plan'으로 1998년 UNECA(Economy Committee for Africa) AISI(African Information Society Initiative)의 지원을 통해 수립
- 르완다 국가개발전략 Vision 2020의 성취를 위해 ICT를 통해 접근하며 총 4단계 계획으로 구성
- NICI-Phase I (NICI-2005): 2000년~2005년 계획
  - 지식기반 경제를 조성하기 위해 ICT 조직 및 법 규제 프레임워크, 통신 정책 마련 추진
  - 교육, 공공행정 혁신, ICT 인프라 개발, 대외 직접투자 유치, 법 제도 기반 마련, ICT 사용 활성화, 민간 부문 발전촉진, 인적자원 개발 등 8개 분야 정책 제시
- NICI-Phase II (NICI-2010): 2006년~2010년 계획
  - 통신 네트워크, 국가 광섬유 백본 네트워크 등 ICT 인프라 기반 강화 및 접근성 강화 추진
  - 교육, 인적자원 개발, ICT 인프라 개발, 경제 개발, 사회 개발, 전자정부, 민간분야, 개발, 정보격차 해소, 법제도 기반 마련, 정보보호 등 10개 분야 정책 제시

---

407 "Rwanda passes anti-cybercrime law", africa.cgtn.com, 2018.5.31.
408 "MPs adopt cyber Crime law", MITEC News, 2018.5.31.

- NICI-Phase III (NICI-2015): 2011년~2015년 계획
  - ICT 인프라를 바탕으로 한 경쟁력 있는 ICT 산업 개발 목표
  - 역량강화, 민간분야 개발, 지역 개발, 전자정부, 사이버 보안의 5개 분야의 정책 제시
- NICI-Phase IV(NICI-2020): 2016년~2020년 계획
  - 지식기반 경제 진입 및 ICT 개발 지속 목표

그림 _ 르완다의 20년간 국가 ICT 정책 및 전략



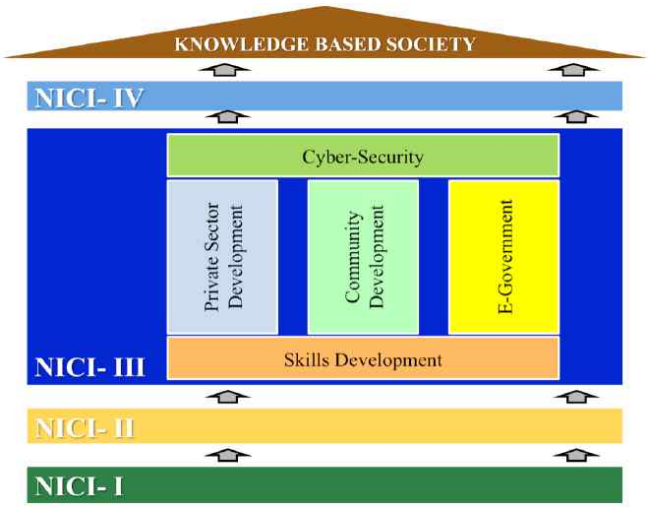
출처: Ministry of ICT and Innovation, "Rwanda's Digital Transformation", 5th eGovernance Conference, TALLINN, MAY 2019

▶ NICI-Phase III (NICI-2015)의 사이버 보안 분야 내용[409]

- NICI III 프레임워크는 5개 부문(역량 개발, 민간부문 개발, 지역사회 개발, 전자정부, 사이버 보안)에 중점을 두고 있으며, 사이버 보안 부문은 르완다의 사이버공간과 정보자산을 보호하는 것을 미션으로 함

그림 _ 국가 ICT 전략계획 NICI-Phase III 프레임워크

409 National ICT Strategy and Plan NICI - 2015 pp. 15, 21, 25~26

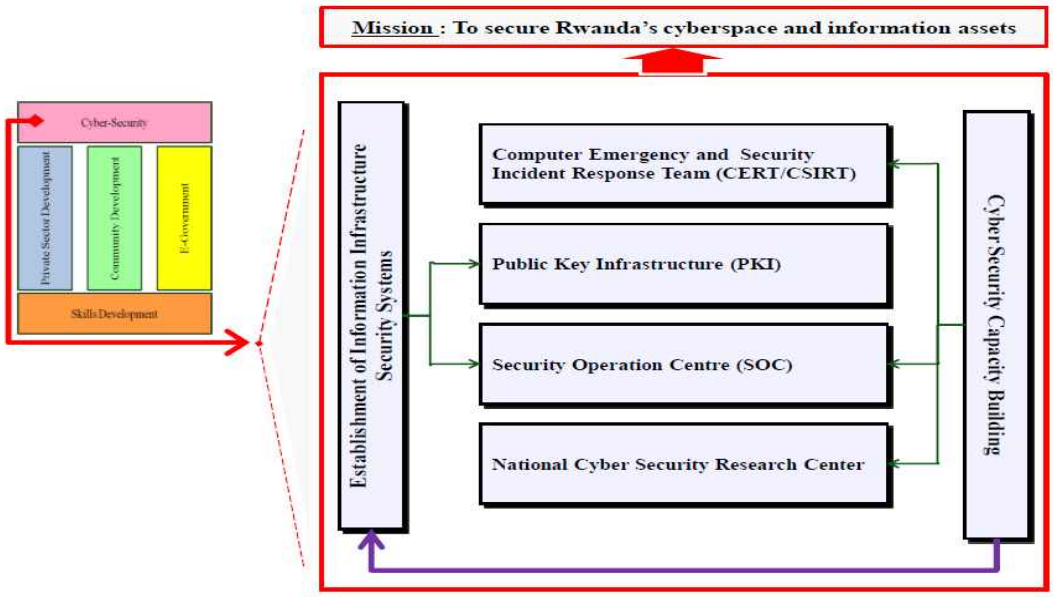


[출처] National ICT Strategy and Plan NICI - 2015

- 지식기반 사회의 핵심인 사이버보안은 국가의 우선순위에 놓이며, 사이버 보안은 르완다의 ICT 목표의 모든 양상들을 지원하기 위해 확산된 ICT 자산의 안전한 관리의 확신을 의미함
- 인터넷은 글로벌 네트워크에 노출되어 있어 반복적이며 진화되는 사이버 공격을 받기 쉬우므로, 르완다는 국가 정보와 ICT 자산의 보호와 완전함을 확신하기 위해 IT와 정보보안에 지속적인 투자가 필요함
- 사이버 보안의 범위는 첫째 사이버 보안 의식 수준을 높이고 사이버 공격으로부터 핵심 ICT 자산을 보호하는 것, 둘째 사이버 보안에서 국제협력을 조성할 뿐 아니라 공격에 대응할 수 있는 국지적인 역량을 강화하는 것, 셋째 법, 규제 환경을 생성하고 사이버 취약성을 완화하는 것임
- 제시하고 있는 5가지 목표는 ① 사이버 보안 의식 고취, ② 사이버 보안 역량 강화, ③ 사이버 공격으로부터 르완다의 중요 인프라와 시스템 보호 확신, ④ 사이버 범죄와 위협을 제어하기 위해 국가적, 국제적 협력 조성, ⑤ 사이버 보안을 확신하고 지원하기 위한 법, 규제 환경 개선하는 것임
- 사이버 보안 관련 선택된 프로젝트는 다음과 같음
  - 컴퓨터 침해사고대응팀(Rw-CERT/CSIRT[410]): 사이버 위협에 즉각적인 대응을 제공하기 위함
  - 공공키 인프라(Public Key Infrastructure, PKI) 구축: 정보 보안을 향상시키기 위함
  - 보안 운영 센터: 모든 국가 사이버 보안 활동을 중앙 집중화하기 위함
  - 정보 인프라 보안 시스템 구축: 르완다의 중요한 ICT 인프라를 방어하고 보호하기 위함
  - 사이버 보안 역량 강화: 르완다인의 사이버 보안 역량을 높이기 위함
  - 국가 사이버 보안 연구 센터 구축: 사이버 보안 준비성을 향상시키기 위함

410 Rw-CERT/CSIRT: Computer Emergency and Security Incident Response Team

그림 _ 국가 ICT 전략계획 NICI-Phase III 프레임워크 내의 사이버 보안 프로젝트



[출처] National ICT Strategy and Plan NICI 2015. p56

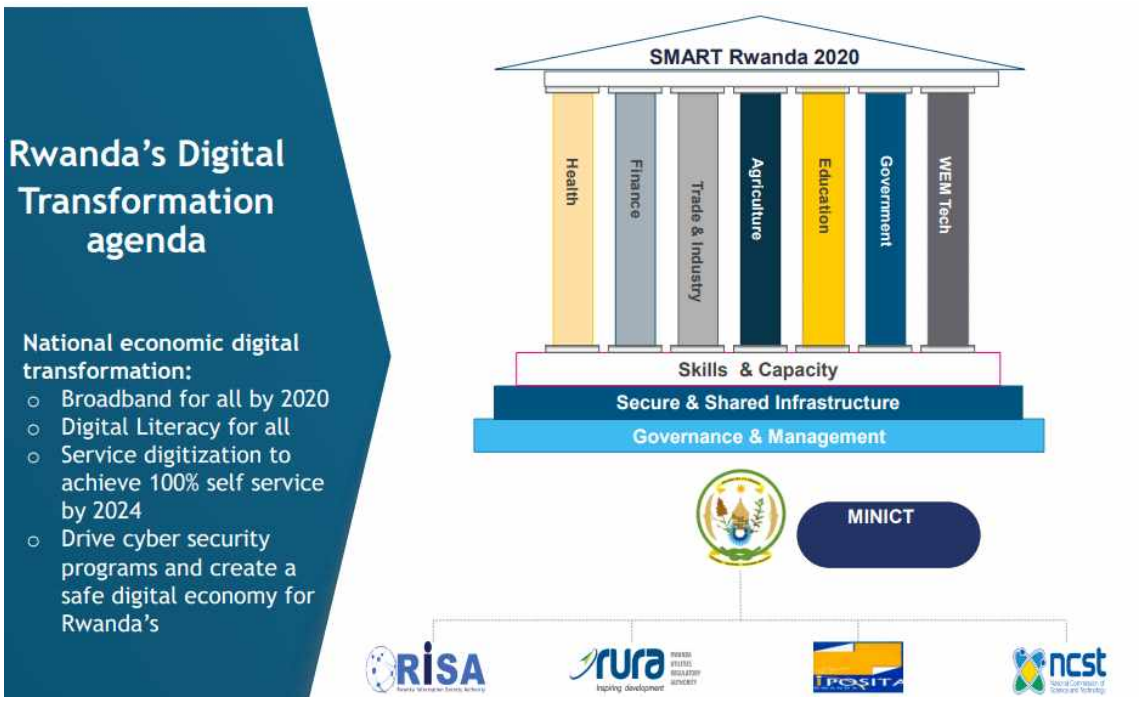
▶ 스마트 르완다 종합계획(SRMP 2015~2020)

- 청년 ICT부는 스마트 르완다 종합계획(SMART Rwanda Master Plan 2015~2020, SRMP) 초안을 2014년 발간[411]
- SRMP는 정부가 ICT를 사용하여 더 나은 서비스를 전달하고, 일자리를 창출하며, 끊임없이 변화하는 환경에서 르완다의 사회경제를 전환하고자 하며, 계획된 5년내에 모든 새로운 정부 서비스는 온라인으로 제공하고자 함
- SRMP는 ICT 개발, 확산, 이용뿐 아니라 현재 국가 사회경제 개발 정책, 전략, 조항들을 검토 및 분석함
- SRMP 목표는 정보지식기반 사회를 이루기 위해서 가속화된 성장을 하고자 경제적 환경을 개선하고 르완다의 경제적 기반을 강화하기 위해 과거 국가 ICT 전략계획(NICI) 위에 수립됨
- SRMP 비전은 지식경제로 향하기 위해 르완다의 사회경제적 전환을 강화하는 것이며, 다음과 같은 원칙을 갖고 있음
  - 르완다의 글로벌 경쟁력과 일자리 창출을 이끄는 서비스 지향적 (Service- oriented), 현대적(Modern), 책임있는(Accountable), 실시간(Real-Time) 스마트 (SMART) 정부 구축
  - 대규모 투자를 유인하고, 기업가정신에 보상하며, 빠른 성장과 수출이 가능한 비즈니스 친화적인 환경을 갖는 높은 경쟁력, 신속함, 개방과 혁신적인 스마트 경제가 되는 것
  - 오픈 데이터, 빅데이터 분석, 클라우드 컴퓨팅, 모바일 앱 등과 같은 강력한 ICT 혁신을 통해

411 SMART Rwanda Master Plan(2015~2020)

스마트한 사회로 전환하고자 함

그림 _ SMART Rwanda 2020



출처: Ministry of ICT and Innovation, "Rwanda's Digital Transformation", 5th eGovernance Conference, TALLINN, MAY 2019

- SRMP하에 기대되는 프로젝트 투자 비용은 약 5억 달러이며, ROI 142.3%에 해당하는 경제적 효과는 17억 2,200만 달러로 GDP 대비 21%이며 7만 개 이상의 일자리가 생성될 것으로 기대함
- IT 정보 자원과 서비스의 성장을 고려하면, 사이버 보안은 매우 중요하게 인식되고 있으며, 사이버 사건은 극적으로 증가할 것이며 모든 영역으로 확산될 것으로 예상됨
- 르완다의 국가적 사이버 보안 정책과 보안기술 수준의 향상은 경제, 사회 안정성과 번영에 큰 영향을 미칠 것임
- 모든 사회조직과 구성원은 지속적인 노력과 관심을 가질 뿐 아니라 사이버 사건을 인식해야만 함
- 이에 대해 SRMP의 핵심이니셔티브에는 국가적 안정성을 보장하기 위해 보안 및 안전 관리 시스템 향상, 사이버 위협에 대한 방어시스템 향상 등의 사이버 보안 관련 내용이 포함됨
  - 관련 프로젝트로는 국가 사이버 안전성 및 정보 보호 센터 구축, 사이버 위협 공유 시스템 구축, 공공 CCTV, 검사 지원 시스템, 긴급대응 시스템, 국가 경찰 관리 정보시스템, 정부 클라우드 데이터복구 센터 등을 포함
- 스마트 르완다 종합계획(SRMP)는 10가지의 실행과제로 구성되어 있으며, 이 중 보안과 관련된 과제는 8번째로서 'ICT에 기반한 안정적 성장을 위한 안전한 국가 정보보안 구축'임

- 동 과제는 7가지의 세부 실행과제로 구성되며 로드맵을 통해 실행계획 수립

그림 _ SRMP 중 'ICT 기반의 안정적 성장을 위한 안전한 국가 정보보안 구축' 실행로드맵



[출처] Smart Rwanda Master Plan v2.1, Annex 3.(2015) 8p.

▶ 르완다개발위원회(RDB)는 사이버 범죄 담당인력의 역량강화 및 사이버 범죄를 보고할 수 있는 공공 핫라인 구축 등 정보보호를 위한 각종 방안들을 실행함[412]

- RDB는 인터넷을 통해 이루어지는 금융 범죄 비율을 조사하며, 기업들을 대상으로 사이버 범죄 노출 사례를 수집
- RDB는 전자뱅킹, 전자정부, 전자교육, 전자상거래 등의 분야에서 사이버 범죄가 발생할 확률이 높다고 판단하여, 이들 분야에 대한 사이버 범죄 예방에 주력함
- RDB는 통신업체와 은행 등 기업 인력에게 어떻게 사이버 범죄가 발생하고 또한 어떻게 대처해야 하는지 교육함

▶ 국가 사이버보안정책(National Cyber Security Policy)[413]

- 르완다 정부는 2015년 3월 국가 사이버보안정책과 전략을 승인하였고, 이는 증가하는 사이버 위협에 대응하고 개인, 사업, 중요한 국가 인프라와 정부를 위해 사이버 보안을 향상시키기 위함
- 르완다 정부는 르완다가 지역적 ICT 허브가 되는 목적과 함께, 현재 ICT 산업 성장의 동향을 고려하면 사이버 보안은 ICT 전략계획의 3단계(NICI-Phase III)를 위한 핵심 우선순위에 놓임
- 사이버보안정책은 사이버공간의 보호와 관련된 실행을 정의하고 가이드하는 프레임 워크 역할을 함
- 사이버보안정책은 국가개발정책(Rwanda Vision 2020), 국가 ICT전략계획(NICI Plan)에 비추어

412 ITU Manaho, 2014,
413 Republic of Rwanda, "National Cyber Security Policy", 2015.3.

르완다를 위한 중요한 정보 자산으로 고려되어지는 ICT 인프라와 애플리케이션에 대해 투자되어 왔으며, 그 결과로서 모든 부문에서 ICT 인프라의 기능과 운영에 대한 의존성이 증가

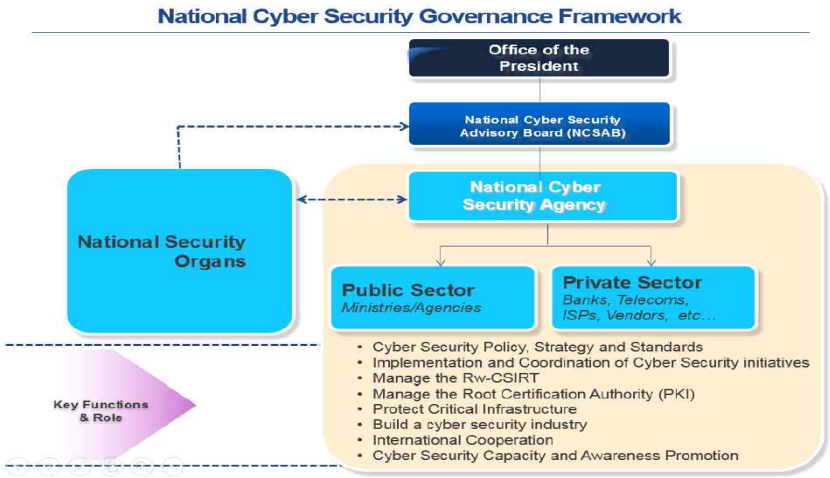
- 이에 따라 사이버 보안을 향상 시키고 중요한 정보 인프라를 보호하는 것은 국가 보안과 경제적 복지에 필수적임
- 현재 정부의 노력과 국제 커뮤니티와의 전략적 목표의 선상에서 르완다의 국가 사이버보안정책 개발의 기본 원칙은 다음과 같음
  - 국가적인 리더십: 사이버 보안의 규모와 복잡성은 강한 국가적 리더십을 요구함
  - 역할과 책임: 정부, 비즈니스, 시민을 포함한 모든 ICT 사용자들은 자신의 정보와 정보시스템을 안전하도록 하기 위한 합리적인 조치들을 취하고, 다른 사용자의 정보와 시스템을 존중하는 의무를 가짐
  - 공공-민간 협력: 정부와 민간 부문의 사이버 보안에의 협력적인 접근은 필수적이고 중요함
  - 위험 기반 관리: 절대적인 사이버 보안은 없으므로 르완다는 위험기반 접근을 적용함
  - 르완다인의 가치: 르완다는 사회, 경제, 국가비전을 보호하는 사이버 보안 정책을 추구함
  - 국제 협력: 사이버위협의 성격상 국제 협력을 증진하는 것은 필수적이며, 르완다는 국제 사이버 보안 활동에 공헌하며 지원함
- 국가 사이버보안 정책의 목적(goal)과 목표(objective)는 다음과 같음
  - 사이버 보안 사고와 위협에 대해 감지, 예방, 대응하기 위한 사이버 보안 역량 강화
  - 사이버 보안 거버넌스와 협력을 조성하기 위한 제도의 프레임워크를 수립
  - 적절한 기술적 운영적 보안 표준 준수를 증진할 뿐 아니라 법, 규제 프레임 워크의 강화
  - 사이버보안영역에서 연구 개발 증진
  - 국가 내에서 보안 문화 구축을 위해 모든 부문과 수준에서 사이버 보안 인식 증진
  - 사이버 보안 영역에서 국가적, 지역적, 국제적 협력 증진

▶ 국가 사이버보안전략(National Cyber Security Strategic Plan)[414]

- 르완다 정부는 2015년 3월 국가 사이버보안정책과 함께 국가 사이버보안전략을 승인하였고, 전략에서는 정책의 실행 가이드를 제공하며 특히 국가 사이버 보안 제도 프레임워크에 대한 내용을 포함

414 Republic of Rwanda, "National Security Strategic Plan", 2015.3.

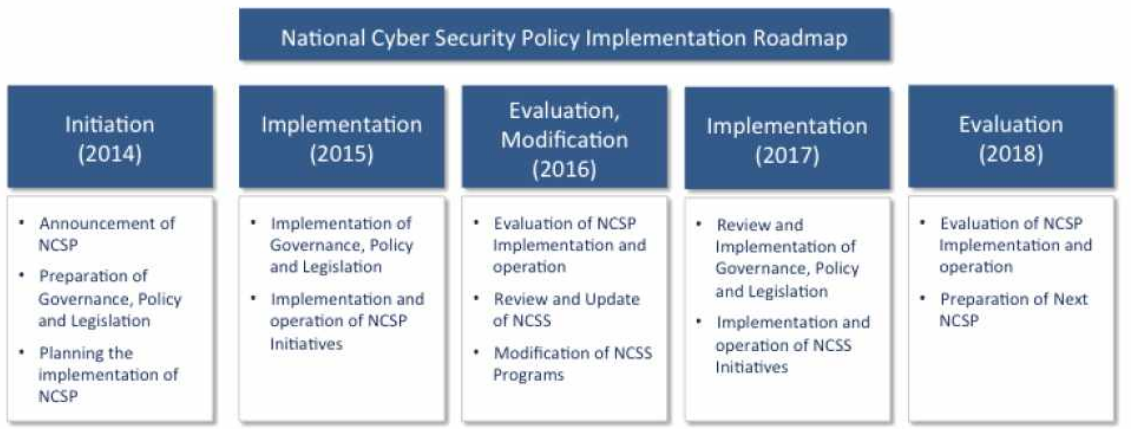
그림 _ 르완다 국가 정보보안 거버넌스 프레임워크



[출처] Republic of Rwanda, 'National Security Strategic Plan'(2015.3)

• 국가 사이버 보안 정책 실행 로드맵은 다음과 같으며, 전략계획 2015-2020 기간 동안 168억 5,500만 르완다 프랑(Rwf)의 예산을 투입할 계획임

그림 _ 르완다 국가 사이버 보안 정책 실행 로드맵



[출처] Republic of Rwanda, 'National Security Strategic Plan'(2015.3)

▶ 스마트 아프리카 스마트시티 청사진(The Smart Africa Smart Cities Blueprint)[415]

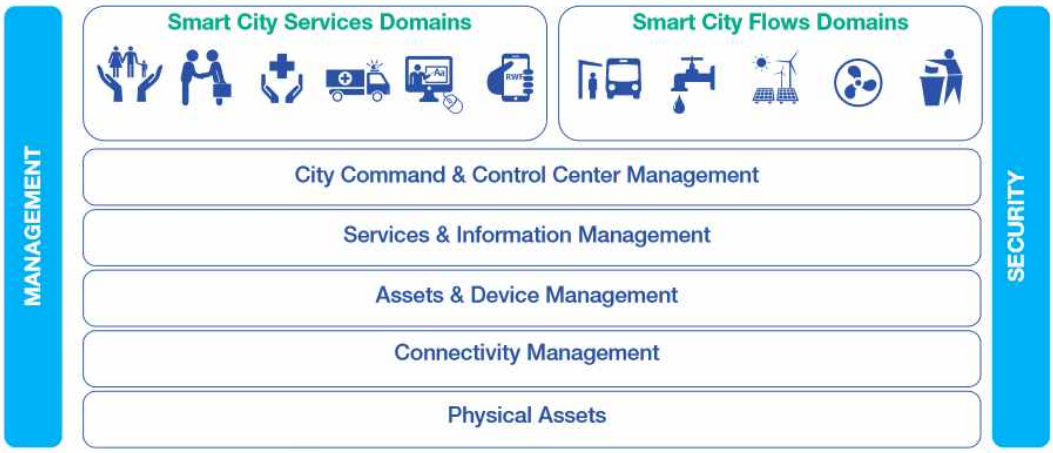
• 동 보고서는 2017년 5월에 개최된 'Transform Africa Summit 2017' 행사에서 발표되었으며, 동

415 Republic of Rwanda, "The Smart Africa Smart Cities Blueprint", 2017.5.

보고서에 포함된 정보보호에 관련된 내용은 다음과 같음

- 스마트 지속가능한 도시의 ICT 설계 부문에서 정보 보안 층(layer)
  - 정보 보안 층은 데이터와 민감한 정보를 보호하는 인프라를 제공하며, 이는 모든 IT 네트워크, 앱, 서버들이 보안 구성요소를 가져야 함
  - 이러한 보안 구성요소들은 불법적인 접속, 침입, 비윤리적인 위반행위 등을 막을 수 있기 위해 최신기술로 이루어짐
  - 암호화 프로토콜은 데이터의 안전한 저장, 처리, 전달을 확신해야 하며, 또한 인증과 개인 권한은 민감한 시스템과 데이터의 접속을 제어해야 함

그림 _ 지속가능한 스마트 도시를 위한 수평적인 스택



[출처] Republic of Rwanda, "The Smart Africa Smart Cities Blueprint"(2017.5.) p.29

- 정책과 거버넌스 부문에서 IT 보안과 프라이버시
  - 사용자의 프라이버시를 보호하기 위해 도시는 프라이버시 정책을 가져야 함
  - 어떤 해로움으로부터 시민을 보호하기 위해 모든 데이터는 보안되고 엄폐 되어야 함
  - 또한 도시는 안전과 데이터 프라이버시에서 타협 없이 개방형 데이터 프레임워크와 협력적인 혁신을 포용해야 함

2) 담당기관

▶ 르완다 개발위원회(Rwanda Development Board, RDB)

- 르완다의 정보보호 정책을 담당하는 기관은 청년 ICT부(Ministry of Youth and ICT)와 르완다개발위원회(Rwanda Development Board, RDB)임
- RDB는 르완다 정부의 모든 ICT 이니셔티브를 조정하고 실행하는 기관으로 국가 ICT 개발전략인 NICI Plan의 실행을 주도하였음
- RDB 내 IT부는 ICT4D의 실질적인 실행 기구에 해당하며 르완다 경제개발을 위한 동인으로서 ICT 산업의 활성화를 추진하였으며, 사이버 범죄를 추적할 수 있는 소프트웨어 설치와 기술팀 운영을 맡았음
- 2016년 정부는 RDB에 국립 디지털 인증 센터(National Digital Certification, NDCC)라 불리는 정부 인증 당국(Certification Authority, CA)을 설립[416]
- RDB는 2017년에 설립된 르완다 정보사회당국(RISA)에게 ICT부문의 많은 기능을 넘긴 후, RDB내에는 경제클러스터의 ICT 비즈니스개발 기능이 존재함[417]

▶ ICT 혁신부(MINICT)[418]

- ICT 혁신부(Ministry of ICT and Innovation, MINICT)는 이전의 정보기술통신부(Ministry of Information Technology & Communications, MITEC)에서 2018년 10월 18일 개각으로 인해 바뀌며 기존의 르완다 개발위원회의 ICT 책임자였던 Paula Ingabire이 장관으로 새로 임명됨[419]
- 기존의 정보기술통신부(Ministry of Information Technology & Communications, MITEC)는 2017년에 전신인 청년ICT부(Ministry of Youth and ICT, MYICT)로부터 각각 교육부와 정보기술통신부로 분리되었으며,[420] 르완다 대통령 Paul Kagame는 2017년 12월 새로운 정보기술통신부 장관(Jean de Dieu Rurangirwa)을 임명하였음[421]
- ICT 혁신부의 미션은 국가 정보기술, 통신 및 혁신 정책과 프로그램의 개발 및 조정, 시민의 권한 부여를 통해 경제 성장 및 빈곤 감소를 위한 국가 우선순위를 해결하는 것임
- ICT 혁신부는 혁신 및 비즈니스 개발, 디지털 전환, 우편서비스, 규제 부문에서 업무를 수행함

▶ 르완다 컴퓨터침해사고대응센터(National Computer Security Incident Response Centre, Rw-CSIRT)

- 국가적인 차원에서 사이버 보안 상황을 모니터하고, 위험을 평가하며, 그에 따라 적절한 대응을 위해 2014년에 설립되었고[422] 내각에서 2015년 4월에 승인됨

---

416 Rw-CSIRT사이트: http://www.rw-csirt.rw/eng/about-us/history.php
417 RDB 조직 사이트: http://rdb.rw/about-rdb/#organization-structure
418 Ministry of ICT & Innovation 웹사이트: https://minict.gov.rw/home/
419 "Kagame reshuffles Cabinet, women take up more slots", TheNewTimes, 2018.10.19.
420 "Rwanda gets new Cabinet, who is in?", NewTimes, 2017.8.31.
421 "Who are the new Cabinet ministers?", NewTimes, 2017.12.7.
422 Rwanda Development Board news, "The Rwanda Development Board Meets Applicaion Developers over Cyber Security", 2015.4.28.

- Rw-CSIRT의 목표는 다음과 같음[423]
  - 컴퓨터 보안 사고 조정과 대응에 대해 국가적 차원에서 연락지점으로 서비스를 제공
  - 현재 정보 및 새로 나타나는 사이버 보안 위협 및 취약성을 정확하고 적시에 제공
  - 사이버 보안 사건과 위협을 다루기 위해 르완다의 사이버 보안 역량을 함양
  - 르완다에서 인터넷사용자에 대한 사이버 보안 문화를 세우는 목표와 함께 정보보안 인식을 증진
  - 사이버 보안 영역에서 연구개발을 증진
  - 사이버 보안 영역에서 지역적, 국제적 협력을 증진
- RDB는 Rw-CSIRT의 활동과 운영을 위한 재정적 지원을 제공하여 Rw-CSIRT에 대한 주요한 이해관계자에 해당함[424]
- 르완다는 사이버범죄 조사를 하는 업무를 하는 부서를 운영하고 있는데, Rw-CSIRT 하에 '사이버 사건 분석'이라는 조직이 컴퓨터 보안 사건들을 조사하고 분석하는 책임을 맡고 있음

▶ 르완다 정보사회당국(Rwanda Information Society Authority, RISA)[425]

- 2017년 1월 내각에서 RISA 설립과 조직 및 기능에 관한 제정된 법(law No 02/2017 of 18/02/2017) 하에 2017년 상반기에 설립되었으며, 르완다의 경제 발전을 위해 필요한 현대 기술에 더 나은 접근성과 활용성을 가속화하기 위함
- 르완다 정보사회당국(RISA)는 RDB 이전의 IT 부서에서 파생되었으며, 현재 기술부(Ministry of Technology) 산하에 있으며, 르완다의 디지털 서비스를 목표로 하는 정부 프로젝트를 구현함
- RISA는 모든 ICT 프로젝트 구현의 최전선에 서고, ICT부문 내의 연구, 인프라, 혁신을 간소화하며, 또한 스마트 르완다 마스터 플랜(SRMP) 초기계획의 구현을 지원함
- RISA의 미션은 다른 부문의 개발을 위한 ICT의 증가된 사용을 통해 르완다 사회의 디지털화화는 것임
  - 빠른 추격형(fast-track) 사회경제적 성장을 위해 국가 ICT 정책 및 프로그램 실행
  - ICT의 접근성 및 적정성 확대를 위한 전략 실행
  - 국가 사회경제적 부문에서 ICT를 주류화하여 지역 발전을 가속화
  - 지식기반 경제를 성취하기 위해서 ICT 영역에서 필요로 하는 기술 증가 프로그램을 준비하여 조정
  - ICT 혁신에 대한 프로그램을 강화
  - ICT 서비스를 제공하기 위한 프로젝트 실행을 조정
  - 유사한 미션을 가진 다른 지역적 국제적 기관들과 협력 및 협조
- RISA는 CEO와 함께 정부최고혁신관 (Government Chief Innovation Officer) 및 정부최고정보관 (Government Chief Information Officer)의 두 부대표가 이끔

---

423 http://www.rw-csirt.rw/eng/
424 Symantec, "Cyber Crime & Cyber Security Trends in Africa", 2016.11. p83
425 RISA 웹사이트: http://risa.rw/

▶ 공익사업규제기관(Rwanda Utilities Regulatory Agency, RURA)[426]

- RURA는 2001년 말에 법률 No. 39/2001에 의해 설립되어 2003년부터 운영됨
- 다양한 공공 시설에 대한 전반적인 다중 부문 규제기관으로 통신 네트워크 및 통신 서비스, 방송 분야 외에도 전력, 수자원, 가스, 교통 분야에 대한 규제를 담당하며, 공공서비스 향상을 위한 법적 기반을 마련
- RURA는 ICT 부문 규제기관으로서, 다음과 같은 전략적 목표를 추구함
  - 통신분야에서 라이선스 할당, 주파수 등의 운영, 서비스 사업자 모니터링, 공정한 경쟁환경 조성, 기술표준 선정, 상호접속 및 번호배정, 소비자 보호, 분쟁 해결 등 담당
  - 투명성을 바탕으로 르완다 국민들의 통신 등의 분야 수요를 충족시키며 소비자들의 권익을 증진시키고, 민간사업자들이 공공사업 부문에 투자하고 참여하도록 독려하는 것 등을 주요 임무로 함

▶ 르완다 국립 경찰조직 하에 사이버 범죄 부서

- 르완다 경찰조직 하에 정보기술 및 사이버 범죄 조사 부서가 설치되어 있고[427], 또한 디지털 포렌식에 대한 책임을 지는 특수 부서를 설립하여 컴퓨터 침해 사건이 발생하는 경우 Rw-CSIRT와 긴밀하게 업무를 진행함[428]

▶ 르완다 국가사이버보안청(National Cyber Security Authority, NCSA)

- 르완다 의회는 2017년 5월 국가사이버보안청(NCSA) 설립에 관련된 법안(National Cyber Security bill)을 채택하였으며, 법안에는 NCSA의 미션, 조직, 기능을 포함
- 2017년 8월, 정부는 NCSA 조직 설립을 위한 예산배정을 마쳤으며, ICT부서에서 38억 Rwf를 삭감하여 NCSA 건설자금을 지원하였으며,[429] 2017년 11월 정보기술통신부(MITEC) 자료에 의하면[430] 설립되었으며 운영이 진행 중
- NCSA 설립 관련된 법안[431]에서 제시하고 있는 NCSA의 미션은 경제사회 발전을 이루기 위해 국가 통합 및 안보의 보호를 보장하는 관점으로 사이버 보안 역량과 스킬을 구축하는 것임
- 또한 법안에서 제시하고 있는 NCSA의 책임은 다음과 같음
  - 사이버공간에서 국익을 방어하기 위한 전략에 대해 대통령, 공공, 민간 기관에게 자문을 줌

426 RURA 홈페이지: rura.rw
427 Rwanda Polic 웹사이트: https://www.police.gov.rw/about-rnp/organisational-structure/
428 Symantec, "Cyber Crime & Cyber Security", 2016.11. p83
429 "Rwanda To Host First Ever Cybertech Conference In Africa", KTPress, 2019.8.14.
430 "ICT Sector Strategic Plan 2018-2024", MITEC, 2017.11. p. 41.
431 No 26/2017 of 31/05/2017, Law establishing the National Cyber Security Authority and determining its mission, organisation and functioning, Official Gazette nº 27 of 03 July 2017

- 관련 조직에게 사이버 국가보안위협에 대한 사이버 정보를 수행하고 그러한 정보로부터 관련 기관에게 정보를 제공
- 국가적, 지역적, 국제적 ICT 보안 원칙의 기초에 관한 가이드라인을 수립
- 국가 ICT 보안 정책과 전략을 조정하고 이행
- 모든 전자적 운영을 보장하기 위한 전략을 개발
- 모든 국가적 ICT 보안 프로그램을 모니터함
- 일반적인 ICT 인프라와 특히 중요한 정보 인프라를 보호하기 위해 사이버 공격을 방어
- 국가 사이버 보안 교육 프로그램을 수립하고 증진하며, ICT분야에서 연구와 산업을 육성
- 사이버 보안에 대한 사회인식을 창출
- 국가 ICT 보안을 보장하기 위해 다른 공공 및 민간 기관과 다른 정보기술관련 조직들과 협력
- 사이버 보안에 책임을 지는 다른 지역적 및 국제적 조직들과 조정하고 협력

3) 규제 및 인증제도

▶ 르완다에는 정보보호와 관련된 별도의 인증제도가 없는 것으로 조사됨

4) 최근 정책 동향 및 이슈

▶ 르완다 정부는 사이버 보안 및 개인정보보호에 관한 말라보 협약을 비준(2019.7.)[432]

- 르완다는 사이버 보안 및 개인정보보호에 관한 아프리카 연합의 말라보 협약(Malabo Convention)을 비준하여 정부가 사이버 범죄와 싸우는데 있어 다른 국가와 협력할 수 있게 할 것임
- 사이버보안 및 개인정보보호에 관한 아프리카연합(African Union, AU) 협약은 2014년 6월 27일 적도 Guinea에서 서명되었으며, 현재까지 르완다를 포함한 아프리카의 12개국만이 협약을 비준했음
- 2019년 7월 25일 ICT 혁신부장관은 의회에 합의를 발표하면서 르완다가 사이버범죄와 싸우고 정부가 전략을 추진하는데 큰 도움이 될 것이라고 함
- 해당 비준으로 인해 향후 사이버 범죄를 막기 위해 다른 국가와 협력할 수 있어, 누가 우리의 정보에 접근하고 어떻게 사용했는지 추적할 수 있게 됨

---

432 "Rwanda Ratifies Malabo Convention On Personal Data Protection", KTPRESS, 2019.7.25.

- 해당 비준은 ICT법에 포함되지 않지만 일반적으로 부문이나 기술에 관계없이 적용됨

▶ 르완다, 최초의 스마트 폰 공장 설립 계획(2019.2.)[433]

- 스마트폰을 생산하는 공장이 르완다에 열 예정이며, 디지털 서비스에 대한 접근성이 향상 될 것으로 관리들은 기대함
- ICT 혁신부 장관은 범-아프리카 기술 회사인 Mara Corporation과 공장 설립을 위한 협상을 진행 중이며, 세부사항을 밝히지는 않았지만 2019년 4월까지 관련된 국내 활동을 시작할 수 있다고 의회의 교육, 과학, 문화 및 청년에 관한 상임 위원회(Standing Committee on Education, Technology, Culture and Youth)에게 이 계획을 밝힘
- ICT 혁신부 장관은 디지털 서비스에 접근하기 위해 스마트폰은 중요한 ICT도구임에도 불구하고 높은 비용으로 시민들이 다양한 디지털 서비스로부터 혜택을 받지 못하므로 스마트폰의 경제성을 확보할 필요가 있다고 강조함
- 공장에서 스마트폰을 생산하면 24개월 동안 사람들이 할부로 지불하며, 인터넷 사용 가격을 낮추기 위해 통신사와 협력하여 ICT 보급률과 디지털 서비스가 향상될 것으로 기대함

▶ 르완다 중앙은행, '현금 없는 르완다'를 2024년까지 80% GDP로 목표함(2017.11.)[434]

- 디지털 방식으로 거래할수록 경제 활동의 전환이 더 빨라지므로 중앙은행은 현재 진행 중인 현금 없는 르완다(Cashless Rwanda) 캠페인을 통해 르완다 전역에서 디지털 머니 거래를 증가시키고자 함
- 중앙은행은 모든 르완다인의 '현금 없는 르완다'를 현재 21% GDP 수준에서 2024년까지 80% GDP수준까지 끌어들이는 것을 목표로 함
- PoS와 ATM 수는 2010년 99개에서 2017년 2,031개로 증가하였고, 같은 기간 동안 ATM은 84개에서 405개로 증가함
- 그러나 금융서비스 이용은 2016년 1,736,203건에서 2017년 1,871,858건으로 예금계정 형태로 증가함

5) 정보보호 스타트업 관련 정책동향

건전한 정보보호 스타트업 생태계 조성을 위한 정부 정책 동향

▶ RISA와 MINICT는 '사이버스타 르완다(Cyber Star of Rwanda)'를 통해 르완다의 디지털 혁신을 도모함[435]

- 사이버 스타 행사는 2019년 현재 아프리카 지역에서는 우간다, 탄자니아, 르완다가 참여하고 있으며, RISA와 MINICT는 이 경쟁에서 사이버스타 행사의 조정뿐 아니라 대학 및 기타 중요한 곳과

433 "Rwanda set to get first smartphone factory", MINICT Latest news, 2019.2.9.
434 "Rwangombwa Outlines Safety And Security In Going Cashless", KTPress, 2017.11.29.
435 "Cybersecurity efforts mobilise local innovative solutions", TheNewTimes, 2018.12.21.

커뮤니케이션 활동을 조정하며 행사를 주관함[436]

- 르완다에서는 사이버스타 행사를 통해 사이버 공간 보호부문에 전국 경쟁을 진행하여 전국의 대학 참가자들이 참여하여 2018년 12월에 12개 혁신적인 솔루션에 상을 수여함
- 해당 경쟁에 참여한 참가자들은 윤리적인 해킹(공격자), 침입 탐지 및 보안 모니터링(수비자), 컴퓨터 포렌식(응답자) 영역에서 소프트웨어 솔루션을 개발하고 피칭하여 르완다가 사이버 공간을 보호하는데 도움이 되는 ICT솔루션을 개발하였음
- 2018년 3월에 시작된 이 대회는 ICT 혁신부에서 RISA, Silencec, MTN Rwanda와 협력하여 10개 지역 대학의 대학생을 유치하였으며, 다양한 대학의 400명 이상의 ICT 학생들이 초기 애플리케이션을 만들었으며 그들 중 52명이 그랜드 피날레에 진출했었음
- 해당 행사는 국가 사이버 보안 역량, 구축 프로그램의 구현의 프레임워크의 일부로 시작되었고 식별된 기술격차에 대응하였음
- 2019년 Cyber Star 행사의 주요 일정은 다음과 같음

표 _ 르완다의 사이버 스타 주요 일정(2019년)

단계	일정	내용
등록 및 사전 선택	~2019.9.6	등록 오픈
멘토십 프로그램	2019.9.11.~10.11.	멘토십 프로그램
워크숍/커리어 데이	2019.10.16.	워크숍/커리어 데이
전국 준결승	2019.10.31.	각 대학의 학생들은 그들 사이에서 경쟁 할 것이며, 최고의 3명으로 구성된 팀은 전국 수준에서 대학을 대표할 것임
전국 결승	2019.11.21.	여러 대학에서 선택된 팀은 최고 팀/대학을 결정하는 생방송 전국 행사에서 경쟁할 것임
지역 결승	발표예정	전국 경쟁에서 승리한 팀/대학은 지역 경쟁에 르완다를 대표할 것임

[출처] cyberstars.pro/rwanda/

▶ 르완다 정부는 아프리카의 사이버 보안 위협이 증가함에 따라 아프리카 최초의 사이버테크(Cybertech) 컨퍼런스를 개최 예정(2019.8.)[437]

- 르완다는 사이버 아프리카 컨퍼런스 및 전시(Cybertech Africa Conference and Exibition)을 2020년 3월에 개최할 예정으로 아프리카에서 개최되는 첫 번째 컨퍼런스에 해당하며, 사이버테크(Cybertech)

436 Cyber Star 홈페이지: https://cyberstars.pro/rwanda/
437 "Rwanda To Host First Ever Cybertech Conference In Africa", KTPress, 2019.8.14.

및 이스라엘 국방의 창립자이자 편집장인 Amir Rapaport와 협력함

- Amir Rapaport는 이스라엘의 사이버, 첨단기술 및 방위 산업의 최고 전문가 중 한명이며, 이스라엘 및 전 세계의 사이버 컨퍼런스 및 전시회는 이스라엘 및 국제 혁신과 기술에 대한 최고의 전시뿐만 아니라 현장 및 산업 분야에 리더를 위한 국제적인 대화 역할을 함
- 이 행사를 주최하기로 한 결정은 금융, 보건, 교육, 커뮤니케이션 및 항공 등 사이버 분야의 전문가들이 모이는 회사에서 발표되었으며, 이 행사를 통해 참가자들은 사이버 기술 분야의 위협에 대처하기 위한 최신 기술 혁신, 위협 및 솔루션에 대해 배울 수 있는 기회가 될 것으로 기대함

정부주도 정보보호 클러스터 조성 등 스타트업 관련 사례

▶ ICT 혁신부는 지속가능한 개발 프로그램을 위한 GIZ 디지털 솔루션과 제휴하여 창의적인 장소인 테크 스타트업을 지원할 디지털 전환 센터(Digital Transformation Center)를 시작함(2019.5.)[438]

- 디지털 전환 센터는 임팩트 중심 디지털 솔루션 개발, 지역 생태계 역량 개발, 지역 및 대륙 수준에서 디지털 솔루션 복제 및 확장을 목표로 하는 르완다-독일의 이니셔티브 임
- 이 프로젝트는 르완다와 아프리카를 위한 디지털 솔루션의 개발, 구현, 보급을 위한 구조와 역량을 확립하는 것을 목표로 함
- 디지털 전환 센터는 초기 아이디어 및 솔루션 개념에서 디지털 프로세스 체인 및 비즈니스 모델의 구현 및 도입에 이르기까지 모든 단계에서 디지털 전환 프로세스를 지원하고자 함
- 또한 이 센터는 블록체인, 사물인터넷, 인공지능 등과 같은 특정 전문 분야에 대한 혁신, 연구, 기업가 정신 및 훈련을 함께 함

438 "MINICT and GIZ officially launch the Digital Transformation Center", MINICT Latest news, 2019.5.14.

융합보안시장 및 정책 동향

1) 융합보안 시장 현황

블록체인

▶ WISeKey는 Microsoft와 파트너십을 통해 블록체인 기술 채택하여 르완다 정부의 토지등록 디지털화 사업 진행(2018.1)[439]

- 2017년 10월 WISeKey 및 Microsoft와 파트너 관계를 맺고 르완다 정부가 블록체인 기반 이니셔티브를 개발 할 수 있도록 지원하며, 이러한 파트너십은 르완다를 블록체인/IoT 우수센터로 전환하기 위한 지속적인 협업의 일부임
- 이 이니셔티브의 첫 번째 단계는 르완다의 토지 등록(land registry)을 디지털화는 사업으로, WISeKey는 Microsoft의 Azure 블록체인 기술을 기반으로 ID관리를 위한 기술 도구를 제공하며, 이를 통해 소유권 및 거짓 문서 등 기존 부동산 시장에서 발생하던 문제를 제거하고자 함

▶ 사이버 보안회사인 WISeKey는 르완다에서 블록체인/IoT 우수 센터를 설립 후 활동(2017.3.)[440]

- 스위스에 본사를 둔 사이버 보안회사인 WISeKey는 르완다와 협력하여 블록체인/IoT 우수센터를 Kigali에 2017년 설립
- 이 센터는 블록체인 생태계 구축을 촉신하기 위해 신뢰할 수 있는 블록체인 서비스 플랫폼을 구축하고자함
- WISeKey는 센터에 참여하는 현지 회사와 협력하여 산업 관점 및 도메인 전문화를 통해 다양한 블록체인 체계(공공, 컨소시엄 및 개인)에 걸쳐 분산원장기능, 개념 증명, 정책, 교육 자료를 구축하고자 함

핀테크

▶ Visa는 르완다를 핀테크 관련 변화를 일으키려는 솔루션을 개발하는 많은 스타트업이 있어 스타트업 커뮤니티에 참여하고자 함(2019.7.)[441]

---

439 "Rwanda to adopt blockchain technology for its land registry", The Express News Rwanda, 2018.1.3.
440 "WISeKey to launch blockchain/IoT centre of excellence in Rwanda", SmartCitiesWorld, 2017.3.2.
441 "Visa makes case for Fintech players in Africa", TheNewTimes, 2019.7.21.

- Visa는 르완다에서 디지털 또는 물리적 형태 또는 두 가지 형태로 비자 신용 신용증명 배포를 가능하게 하기 위해 고유의 사업을 계속 추진할 것이지만, 르완다에서의 많은 스타트업으로 인해 스타트업의 인큐베이터로 간주하여 스타트업에게 Visa의 기능을 제공하고, 스타트업이 접근 할 수 있도록 API를 공개하여 글로벌 경험을 주도하길 원함
- 이러한 스타트업과의 활동을 통해 추가적인 Visa 시장에 훌륭한 솔루션을 제공할 수 있다고 간주함
- Visa는 아프리카의 금융 기술이 디지털 방식으로 추진될 것이며, 소비자는 디지털, QR, 메시지, 모바일 장치 등을 사용하여 거래 및 결제를 할 수 있기를 원함

▶ 르완다 민간부문 협회와 통신사 MTN은 파트너십을 맺어 현금 없는 결제 확대(2019.5.)[442]

- 민간부문 협회(Private Sector Federation, PSF)와 MTN Rwanda는 모바일 머니 결제 및 티켓팅 솔루션인 Momo Pay and Ticketing을 시작으로 디지털 사용자 친화적인 솔루션 향상을 목표로 파트너관계를 맺음
- 이를 통해 고객이 현금을 사용하지 않고 모바일 머니 지갑을 사용하여 쉽게 거래할 수 있도록 현금 없는 결제를 촉진하는 것을 목표로 하며, 모바일 머니를 사용하여 시장에 있는 모든 제품을 구매할 수 있도록 함
- 예를 들어 Momo Pay and Ticketing 솔루션은 2019년 7월 22일에 시작되는 르완다 국제무역박람회에서 방문객, 구매자 및 판매자는 모바일 머니를 사용하여 입장권 지불, 엑스포에서 제품 및 서비스를 지불할 수 있음

▶ 르완다의 핀테크 스타트업체 Exuus는 저축 그룹을 디지털 방식으로 취함(2019.5.)[443]

- 2016년 설립된 핀테크 스타트업체 Exuus는 집단적이고 분산된 원장을 통해 지속가능한 VSLA(Village Savings and Load Associations)으로 알려진 저축 그룹에 재정적으로 강화할 수 있는 디지털 플랫폼인 SAVE를 구축함
- 이 플랫폼을 통해 프로세스를 원활하게 하고 저소득층 커뮤니티의 재정적 탄력성을 높이기 위해 기존 저축 그룹을 온라인으로 전환하고 있음
- 2019년 2월에 Kigali에서 아프리카 스타트업 서밋에서 선발된 10개 스타트업 업체 중 하나인 Exuus는 서비스에 가입한 저축 그룹의 구성원이 USSD를 통해 현금 없이 거래할 수 있으며, 개인 지갑에서 그룹의 디지털 지갑을 인출하고 신용할 수 있음
- 2018년 사전 시드(pre-seed) 자금으로 75,000 USD를 모으고, 현재 500,000 USD의 시드(seed)를 모으고 있는 Exuss는 작년에 두 개의 국제 NGO와 함께 파일럿을 수행하여 800명 이상의 회원이 합쳐짐

---

442 "PSF, MTN Rwanda forge partnership to scale up adoption of cashless payments", TheNewTimes, 2019.5.22.
443 "How Rwandan fintech startup Exuus is taking savings groups digital", TheNewTimes, 2019.5.22.

- Exuss는 현재 규모가 커지고 있으며, 2019년 12월까지 백만명의 사용자를 확보할 목표를 갖고 있으며, 현재 르완다에서만 서비스를 제공하고 있지만, 향후 5년 내에 다른 동아프리카 국가에 입지를 구축하기를 기대함

▶ 르완다에서 디지털 보험 혁신은 아직 초기 단계이지만 일부 보험사는 통신사와 제휴하여 새로운 디지털 보험 상품을 시작함[444]

- 예를 들어 3일 연속으로 병원에 입원했을 때 의료 서비스가 필요한 경우, 통신사의 모바일 머니 고객을 위해 개발된 디지털 보험 상품인 'Ingoboka Cash'가 출시됨
- 이 새로운 디지털 제품은 의료보험 서비스의 흡수를 높이고 국가의 보험 보급 수준을 향상시킬 것으로 기대됨

2) 융합보안 정책 현황

스마트시티

▶ 르완다 정부는 비전 2020개발 프로그램 및 2017-2024년 국가 전략의 일환으로 르완다를 세계적으로 경쟁력 있는 지식 기반 경제로 되기 위해 시작한 주요 프로젝트로 Kigali 혁신도시 구축[445]

- Kigali 혁신도시(Kigali Innovation City)는 약 20억 달러 규모로 Kigali 특별 경제 구역에 위치하며 70헥타르 면적에 세계적 수준의 대학, 기술 회사, 생명공학 회사, 상업용 및 소매용 부동산을 수용할 계획임[446]
- Kigali 혁신도시는 금융기술, 스마트 에너지, 생물의학, 사이버 보안, 데이터 및 분석, 농업 등 7개 부문에서 기술 및 R&D, 기존 기술 서비스의 대규모 배포 및 지원 서비스를 통해 혁신에 초점을 둔 여러 유형의 기업을 유치하는 것을 목표로 함
- 특히 디지털 혁신지구(Digital Innovation Precinct)는 Kigali 혁신도시의 모든 기술회사를 수용할 시설이며, 또 다른 부문은 생태계 내의 회사에서 일하는 직원을 수용할 주거시설의 혼합임
- Kigali 혁신도시는 현재 세계적 수준의 학습 기관과 기술 회사로 구성된 혁신 및 지식 허브를 갖추고 있으며, 추가 회사를 위한 공간도 있음[447]
- 아프리카 개발 은행(African Development Bank) 및 다른 아프리카 정부들이 설립한 아프리카의

444 Eulade Rugambwa, "The Insur-Techs, the next game changer in Rwanda's insurance sector ", Rwandan Banker Magazine April 2019, Issue No. 32 ISSN 2410-6844, 2019.4.17. pp. 21-22.
445 "After Africa's Silicon Valley, Rwanda to start building $5 billion Green City in 2020", FaceFaceAfrica, 2019.5.20.
446 "Africa50 to spend $400m on Kigali Innovation City", TheNewTimes, 2018.12.12.
447 "Government, Africa50 to establish firm to develop Kigali Innovation City project", TheNewTimes, 2019.8.27.

인프라 프로젝트 자금조달을 위한 특수목적의 범-아프리카 인프라 투자회사인 Africa 50은 이 혁신 도시에 4억 달러를 투자하여 르완다의 기술 허브 개발 노력을 강화할 것임[448]

- 르완다 정부는 Africa50이 3억 1,500만 달러의 소매 및 상업 단지 건설을 포함하여 프로젝트의 부동산 부분에 집중할 것이라고 밝혔으며, 또한 Kigali 혁신도시의 모든 기술회사와 생태계 내 회사에서 근무하는 직원을 위한 주거시설을 수용한 디지털 혁신지구(Digital Innovation Precinct)에 대한 작업을 할 것임[449]
- 르완다 정부를 대표하는 RDB(Rwanda Development Board)와 Africa 50은 Kigali 혁신도시 프로젝트를 개발하기 위해 회사를 설립하기로 2019년 8월 27일 협약을 체결함[450]
- 르완다 정부와 Africa 50이 합작 투자회사를 설립하여 Kigali 혁신도시의 상업 구성요소를 개발, 자금조달, 건설, 운영할 예정
- 이 협약에 따르면 르완다 정부는 도로, 조명, 전원 공급, 기타 수평적인 '플러그 앤 플레이'와 같은 토지 및 금융 보조 인프라에 기여하게 될 것이며, RDB는 또한 효과적인 민간부문의 참여가 가능하도록 정책 주도형 세금 인센티브를 포함한 거액 및 소액 지원자의 촉진을 보장할 것임
- 이 프로젝트는 민간부분이 참여하도록 초청된 세계적 수준의 기술개발을 위해 1억 달러 규모의 펀드인 르완다 혁신 펀드(Rwanda Innovation Fund)의 구성 요소를 갖고 있음[451]
- 르완다 정부의 투자가 혁신 주도 기업을 유치하는 목적은 포괄적인 성장을 육성하고 수천명의 사람들의 삶에 영향을 미침으로써 혁신 주도 기업을 유치하고 전략적 파트너십을 자극하여 기술 분야를 더욱 발전시키고자 함

▶ 르완다 정부는 2017년 5월 Nokia와 지역 개발 기관인 SRG의 도움을 받아 스마트 시티 인프라에 투자할 계획을 발표했음[452]

스마트 의료

▶ 르완다 내각의회는 르완다 정부와 드론업체 Zipline의 드론을 통한 의료 제품 배달에 대한 계약을 승인함[453]

- 르완다 정부와의 3년 계약 연장을 통해 긴급 의약품을 위한 세계 드론 전달 시스템을 운영하는 미국에 본사를 둔 기술 회사인 Zipline은 르완다 병원에 혈액뿐 만 아니라 다른 필수 의약품도 배달하게 됨
- Zipline 측은 긴급 의약품 목록에 기본 의약품을 포함할 계획을 진행 중이며, Zipline은 약 2년 전

448 "Government, Africa50 to establish firm to develop Kigali Innovation City project", TheNewTimes, 2019.8.27.
449 "After Africa's Silicon Valley, Rwanda to start building $5 billion Green City in 2020", FaceFaceAfrica, 2019.5.20.
450 "Government, Africa50 to establish firm to develop Kigali Innovation City project", TheNewTimes, 2019.8.27.
451 "Government, Africa50 to establish firm to develop Kigali Innovation City project", TheNewTimes, 2019.8.27.
452 BuddeComm, Rwanda - Telecoms, Mobile and Broadband - Statistics and Analyses, 2019.5.1. p. 38.
453 "The five milestones that shaped Rwanda's ICT sector in 2018", MINICT Latest news, 2018.12.31.

미얀마 보건부(Ministry of Health)에 의해 지불 합의에 따라 르완다 남부 Muhanga 지역에서 운영을 시작하였음

- 이후 르완다 남부 및 서부 지역에 있는 19개 병원에 드론을 통해 혈액을 공급한 후 지리적 범위를 확대하고 모든 공공 병원 및 보건소에 서비스를 제공할 계획이 진행 중임
- 향후 Zipline은 르완다 내에 드론 조립 및 유지 보수 공장을 설립하고 동부 지방의 Kayonza 지역에 두 번째 드론 항구를 열 예정임

블록체인

▶ 르완다 중앙은행인 르완다 국립 은행(National Bank of Rwanda)은 자체 디지털 화폐 발행하는 방법을 모색 중(2019.8.)[454]

- 르완다 국립 은행은 디지털 화폐(digital currency)를 사용해 거래 처리를 개선하고 경제 성장을 촉진할 계획
- 르완다 국립 은행의 재무 안전국장(Financial Stability Director-General)에 따르면, 싱가포르, 네델란드, 캐나다와 같은 다른 국가의 중앙은행의 경험을 통해 블록체인 기술의 사용 사례를 연구할 계획임

▶ 르완다 국립 은행은 암호 화폐인 Get-Rich-Quick의 사기 혐의에 대해 공공 서비스 발표(2019.5.)[455]

- 르완다 국립 은행은 초기 코인 제공(ICO) 사기 및 암호화 기반 폰지(Ponzi) 체계에 대해 대중에게 경고하여 초기 투자자에게 신속하게 투자에 대해 빠르고 상당한 회수를 할 수 있게 함
- 르완다 국립 은행은 투자자에게 잠재적인 프로젝트를 조사할 것을 경고하고, 사기 피해자들에게 보상을 제공하지 않는다는 사실을 대중에게 상기시킴

핀테크

▶ 르완다 정부는 금융 서비스에 ICT를 사용하여 르완다를 현금없는 경제로 전환할 계획을 갖고 있음[456]

- 르완다는 전자결제 도입을 장려하는 이니셔티브인 Better Than Cash Alliance에 가입하였으며, 이 얼라이언스는 또한 금융서비스를 이용할 수 없고 일반적으로 현금 전용 경제에 사는 사람들을 지원함
- 이 얼라이언스는 UN Capital Development Fund와 Bill & Melinda Gates 재단, Citi, Ford 재단, MasterCard, Omidyar Network, USAID(United States Agency for International Development), Visa가 자금을 지원함[457]

---

454 "Rwandan Central Bank Studying Ways of Issuing Digital Currency", Bloomberg, 2019.8.22.
455 "Rwanda's Central Bank Issues PSA on Alleged Cryptocurrency Get-Rich-Quick Scams", cointelegraph, 2019.5.30.
456 "Visa makes case for Fintech players in Africa", TheNewTimes, 2019.7.21.
457 BuddeComm, Rwanda - Telecoms, Mobile and Broadband - Statistics and Analyses, 2019.5.1. pp. 52~53.

다. 케냐

'18년 GDP(십억달러)	87.908
'18년 인구수(천명)	51,393

■ ITU 글로벌 사이버보안 지수(Global Cybersecurity Index, GCI)

· 케냐의 글로벌 사이버보안 지수 순위는 44위이며, 아프리카 국가 중에는 2위를 차지

국가명	2018		2017		전년대비 증감	
	지수	순위	지수	순위	지수	순위
케냐	0.748	44	0.574	45	+0.174	+1
대한민국	0.873	15	0.782	13	+0.091	-2

■ ICT 관련 주요 지수

· 케냐의 전반적인 ICT 발전 수준은 ITU 조사국 167개국 중 하위권에 속해 있음

지표명	케냐		한국	
	점수	순위	점수	순위
IMD 국가경쟁력지수(2019)	-	-	-	28
IMD 디지털경쟁력지수(2019)	-	-	-	10
UNCTAD 전자상거래지수(2019)	49.0	89	89.4	19
ITU 글로벌 사이버보안 지수(GCI 2018)	0.931	1	0.873	15
UN 전자정부 지수(2018)	0.454	122	0.901	3

■ ICT 관련 주요 통계(ITU, 2018년 말 기준)

· 케냐는 각종 통신 서비스 보급률은 최하위권이나 이동통신 보급률은 상대적으로 높음

항목	케냐		한국	
	가입자수(천 명)	보급률(%)	가입자수(천 명)	보급률(%)
유선전화	65	0.13	25.906	50.63
유선브로드밴드	371	0.72	21,286	41.60
이동통신	49,501	96.32	66,356	129.67
인터넷 이용률	17.83%(2017년 말 기준)		95.90%	

정보보호 산업 개요

1) 보안 환경

▶ World Economic Forum의 The Global Information Technology Report 2016에 따르면 케냐의 네트워크 준비지수(NRI)는 3.8로 전 세계 143개국 중 86위임

- 미국 CIA(Central Intelligence Agency)에 따르면, 2018년 기준으로 케냐 인구는 4,839만 명, 0-14세 인구는 39.03%, 유선 인터넷 사용자는 26%에 불과한 반면, 모바일 가입자는 4,281만 명으로 거주자 100명당 90명의 높은 가입률을 보이고 있음

▶ 케냐는 2017년 4월 6일, '컴퓨터 및 사이버범죄 법안 2017(Computer and cybercrime Bill)'을 통과시킴으로써 사이버 보안 범죄에 대한 본격적인 규제가 가능해짐(Article 19(2018.4), Kenya: Computer and Cybercrimes Bill 2017)

- 이 법안은 컴퓨터 데이터 저장 매체, 컴퓨터 시스템, 데이터, 가입자 정보, 데이터 트래픽 등과 같은 컴퓨터 보안과 관련된 주요 내용을 정의하고 법률 위반의 유형을 컴퓨터 시스템과 데이터에 대한 잘못된 취급과 정보의 유해성 정도에 관련된 내용으로 구분
- 법률 위반에 대한 처벌 역시 위반에 따른 처벌의 수준이나 범죄 협력이나 사주 등에 대한 범죄의 범위 등에 따라 세분함으로써 사이버 보안 범죄에 대한 체계적 대응이 가능

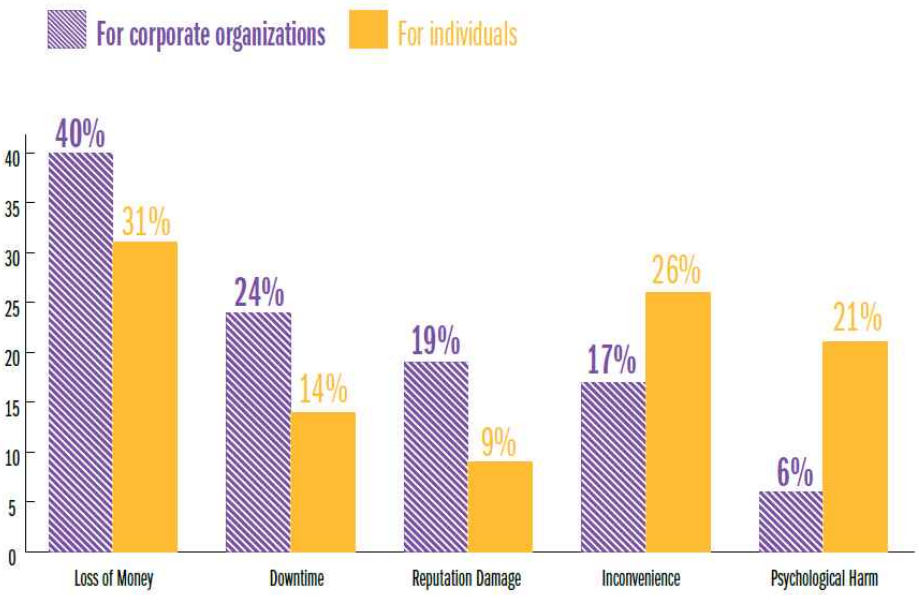
▶ African Cyber Security Report 2018 보고서에 의하면, 케냐의 멀웨어에 의한 피해는 지속적으로 증가하는 양상

- Emotot, Trickbot 등과 같은 멀웨어들에 의한 공격이 지속적으로 증가하는 것으로 나타남
- 특히 Bitcoin이나 Etherium과 같은 가상화폐와 관련된 금융 멀웨어의 증가가 주목되는 가운데 케냐의 제조업체나 교육기관, 금융기관 등이 사이버 범죄의 주요 타겟이 되는 것으로 나타남

▶ 케냐의 사이버 범죄에 대한 노출 정도 역시 매우 높고, 금전적 피해도 심각한 것으로 나타남

- Cyber Security Report 2018의 조사 결과에 따르면, 응답자의 58%가 최근 5년간 사이버 범죄에 노출된 경험이 있는 것으로 나타났으며, 주로 회사 등의 공간에서 업무 시간 중에 사이버 범죄에 노출된 경우는 54%, 개인적 활동의 경우에 사이버 범죄에 노출된 경우도 39% 달하는 것으로 나타남

그림 _ 2018년 케냐의 사이버 범죄 노출에 의한 피해 양상

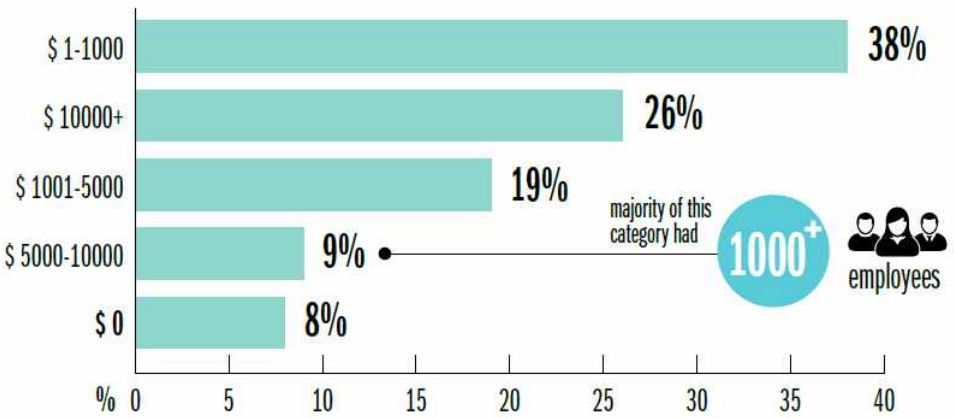


[출처] Cyber Security Report 2018

▶ 이러한 사이버 범죄에 대한 노출에 대비해서 케냐의 기업과 공공기관들의 사이버 보안에 대한 투자도 확대되고 있음

- 2016년 조사의 경우 응답자의 95%가 연간 5,000달러 이하의 사이버 보안 투자를 한다는 것으로 나타났으나, 2017년의 경우 이 수치가 7% 줄어든 88%로 나타났으며, 2018년 조사에서는 연간 1만 달러 이상의 투자를 한다는 비중이 26%로 나타났음

그림 _ 2018년 케냐의 사이버 보안 투자 분포

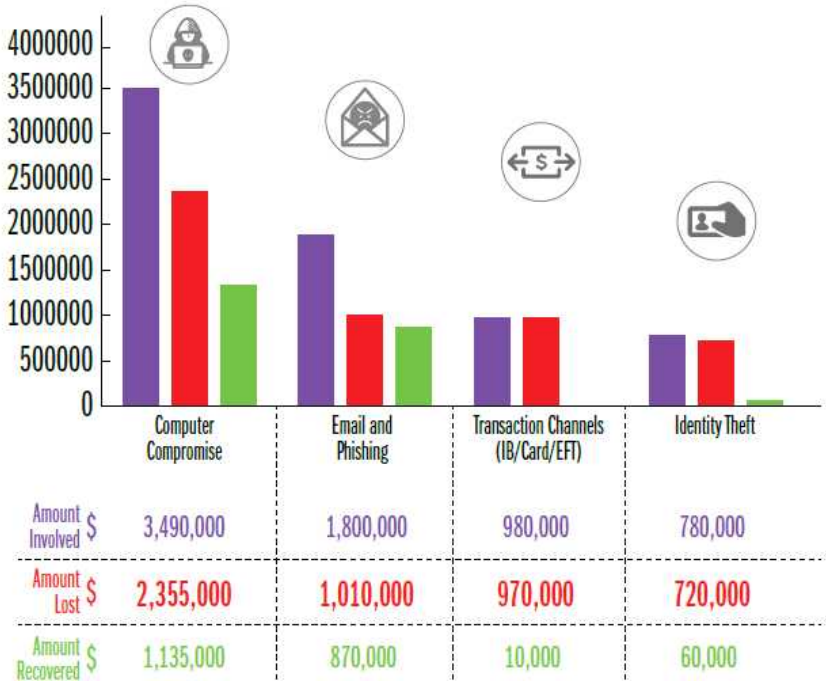


[출처] Cyber Security Report 2018

▶ 케냐의 사이버 범죄에 의한 피해 규모는 2018년 2억 9천만 달러에 이르는 것으로 추산되고 있음

- 케냐 소재 정보보안 컨설팅 기업인 SERIANU의 추정에 의하면, 2018년 사이버 범죄에 의한 경제적 비용은 직접적 비용 8, 850만 달러, 간접적 비용 2.6억 달러에 달하는 것으로 나타났으며, 이를 합쳐 2억 9천만 달러에 달하는 사회적 비용이 발생

그림 _ 2018년 케냐의 사이버 범죄의 유형별 피해 규모



[출처] Cyber Security Report 2018

- 비용 측면에서 피해 규모의 순위를 보면, 컴퓨터 침입(Computer compromise)에 의한 피해가 가장 많은 235.5만 달러에 달했으며, 다음으로 이메일과 피싱에 의한 피해가 101만 달러, 카드나 인터넷 뱅킹 등 거래 채널에 의한 피해가 97만 달러, 신원 도용이 78만 달러에 이르는 것으로 나타남

▶ 이러한 피해에도 불구하고 케냐의 사이버 범죄는 거의 신고 되지 않는 것으로 나타남

- 케냐에서 발생하는 사이버 범죄의 90% 이상은 사법 당국에 신고 되지 않는 것으로 나타남
- 사이버 범죄에 의한 직접적인 피해는 금전이나 대외적 신뢰도 등에 의해 발생하는 비용과 사이버 범죄에 대응하는 과정에서 발생하거나 관계 기관이 부과하는 벌금 등에 의해 발생하는 비용으로 나뉨
- 사이버 범죄에 의한 간접적인 피해 역시 백신 소프트웨어나 대응을 위한 보험 가입 등에 의한 비용과 기업의 대외 이미지 추락 등에 의한 비용 등으로 나누어 볼 수 있음

그림 _ 2018년 케냐에서 발생한 사이버 범죄에 의한 직/간접적인 피해 규모

유형	분야	추정 피해 규모(1,000USD)
직접적 비용	금융 서비스(은행, 보험 등)	28,000
	정부 및 공공 부문	25,500
	서비스 업체(통신, 핀테크, 금융 앱 업체 등)	20,000
	보건 의료 및 소매업	3,000
	기타	12,000
	합계	88,500
간접적 비용	금융 서비스(은행, 보험 등)	64,350
	정부 및 공공 부문	59,650
	서비스 업체(통신, 핀테크, 금융 앱 업체 등)	48,000
	보건 의료 및 소매업	7,000
	기타	27,500
	합계	206,500

[출처] Cyber Security Report 2018

▶ 케냐의 사이버 범죄에 대한 대응에서 가장 큰 문제는 전문인력의 부족임

- 케냐의 사이버 전문 인력은 1,700명에 불과하며, 영역별로는 감사 및 리스크 관리, 사고 발생에 대한 대응 등의 영역에서 숙련 수준이 크게 부족한 것으로 나타남

그림 _ 2018년 케냐의 사이버보안 영역별 숙련 Gap



[출처] Cyber Security Report 2018

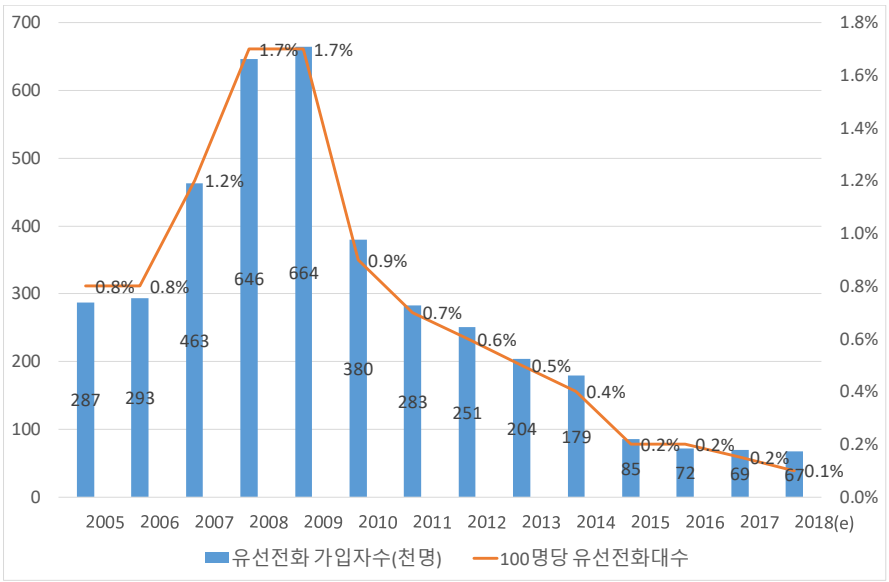
- 케냐의 경우 인구 수를 5천만 명으로 할 때 약 1만 명의 보안전문 인력이 필요한 것으로 파악되며, 케냐 소재 기업의 2/3가 사이버 보안 전문가 인력 부족에 직면할 것으로 예상[458]

2) 인터넷 및 통신 환경

▶ 유선통신

- 케냐의 전국 유선 통신 네트워크는 1999년 41.1만 라인에서 2005년 53.2만 라인으로 꾸준하게 증가하는 양상을 보이는 반면, 무선 통신 회선의 숫자가 같은 기간 3.5만에서 6백만개로 늘어나고, 무선 통신 서비스가입자 역시 같은 기간 1만 5천명에서 500만명 가까이 급증
- 유선 전화 라인수는 2018년까지 연평균 14% 감소하는 추세를 보이고 있음

그림 _ 케냐의 유선전화 라인수와 인구 100명당 전화 대수

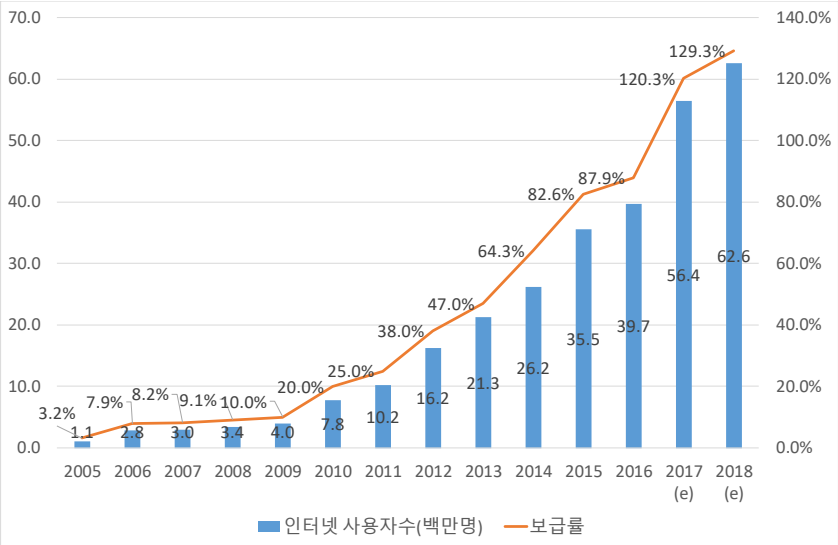


[출처] Buddecomm(2018.)

- 유선전화 설치는 대부분 도시 지역에 집중되어 있으며 전체 회선 중 55%는 수도인 나이로비에 설치되어 있음
- 농촌 지역의 유선전화 라인 점유율은 10%에 지나지 않는 것으로 나타남

458 KISA 정보보호 해외진출 전략거점 주요동향 각 월호

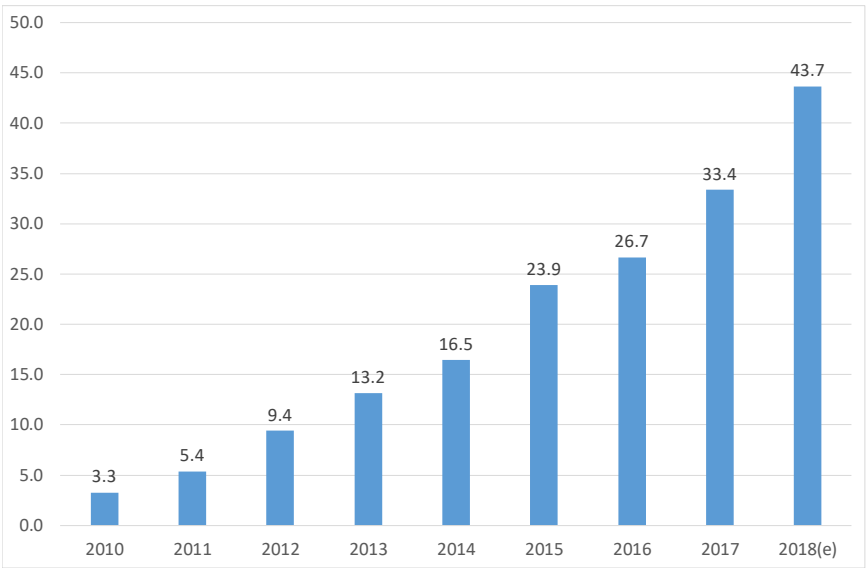
그림 _ 인터넷 사용자 및 보급률 추이



[출처] Buddecomm(2018)

- 인터넷 이용자와 보급률은 2015년 이후의 급증세가 지속되고 있으며, 마을별로 사이버 카페(cyber cafe)가 활성화되어있음
- 2018년 현재 인터넷 가입자수는 유선과 무선을 합쳐 4,370만명으로 5,100만 전체 인구의 대다수가 인터넷에 가입한 것으로 나타남

그림 _ 인터넷 가입자수 추이(백만명)



[출처] Buddecomm(2018.)

• 유선 인터넷 유형별로는 2018년 추정치 기준으로 광통신망 가입자가 16.3만 명으로 가장 많으며, 다음으로 케이블 가입자가 12만명, DSL 가입자수가 1천명 순으로 나타남

표 _ 유선 인터넷 유형별 가입자수(천명)

연도	광통신	DSL	케이블	합계
2010	8.6	12.4	0.03	21
2011	22.5	11	0.03	33.5
2012	54.4	10.8	0.03	65.4
2013	67.5	12	0.03	79.5
2014	81.24	14.51	0.03	95.74
2015	111.35	3.73	0.025	115.08
2016	39.255	2.483	86.139	127.877
2017	99.643	1.953	96.876	198.472
2018(e)	163.45	1.07	125	289,520

[출처] Buddecomm(2018.)

• 인터넷 사업자별 가입자수를 보면, Wahachi Group의 가입자수가 10.5만명, 시장점유율 36.7%로 가장 많은 것으로 나타났으며, 다음으로 Safaricom 가입자수 4.8만명, 시장 점유율 16.7%, Mawingu Networks가 4.6만명, 시장 점유율 16.1% 순으로 나타남

표 _ 유선 인터넷 주요 사업자 및 점유율(2018년 9월 기준)

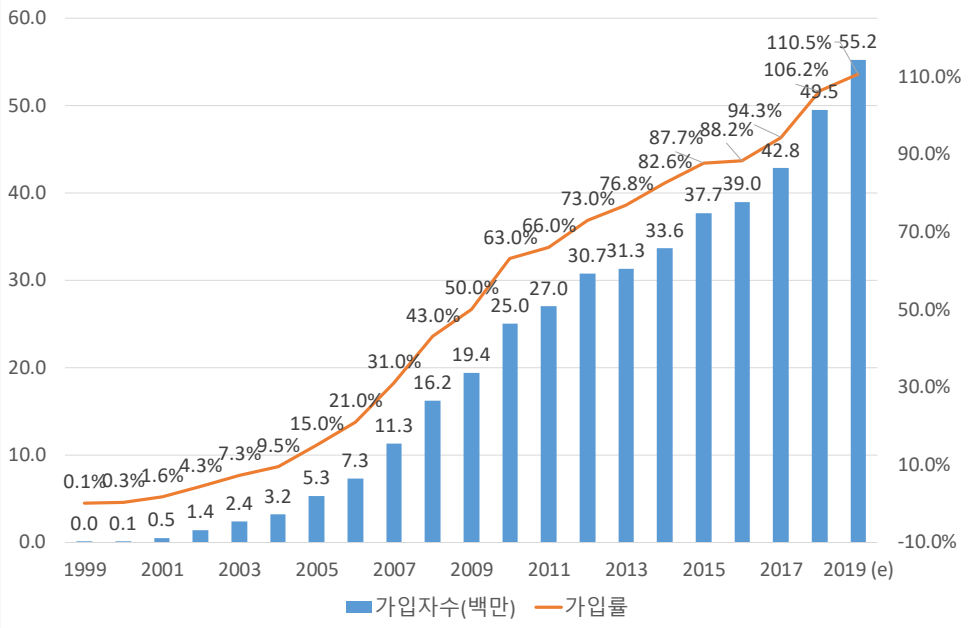
인터넷 사업자(ISP)	가입자(명)	시장점유율
Wanachi Group	105,710	36.70%
Safaricom	48,270	16.70%
Mawingu Networks	46,530	16.10%
Jamii	36,180	12.50%
Argon Telecom	22,460	7.80%
Access Kenya	13,620	4.70%
Liquid Telecom	8,750	3.00%
Telkom Kenya	3,770	1.30%
Iway Africa	900	0.30%
Mobile Telephone Networks	600	0.20%
Other	1,500	0.50%

[출처] Buddecomm(2018.)

▶ 이동통신

- 케냐의 이동통신 시장은 지속적인 성장을 지속하고 있으며, 2019년 추정치 기준으로 모바일 서비스 가입자 수는 5,500만명 수준으로 보급률이 인구보다 많은 것으로 나타나고 있으며, 보급률인 110%에 달하고 있음
- 시장 경쟁이 치열해지면서 기업 간 인수합병이 활발해지고 있는데, Safaricom의 YuMobile 인수와 2019년 2월 Airtel Kenya와 Telekom Kenya의 합병 발표가 대표적이라 할 수 있음

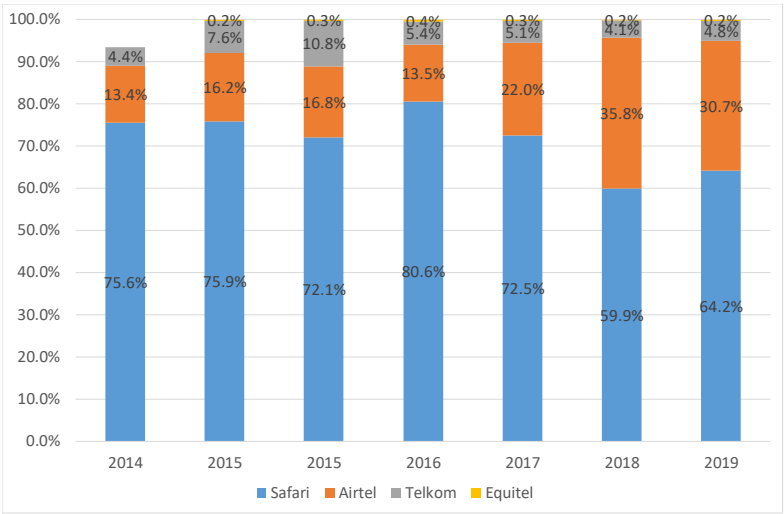
그림 _ 모바일 가입자와 보급률 추이



[출처] Buddecomm(2018.)

- 기업별 이동통신 사용량 추이를 보면, Safaricom이 2014년 75.6%에서 2016년 80.6%까지 증가하다 이후 다시 감소하여 2019년 현재 64.2%로 감소한 반면, 2위 업체인 Airtel은 2017년 22%를 기록하였으며, 이후 2019년 30%대로 점유율을 늘려가고 있음

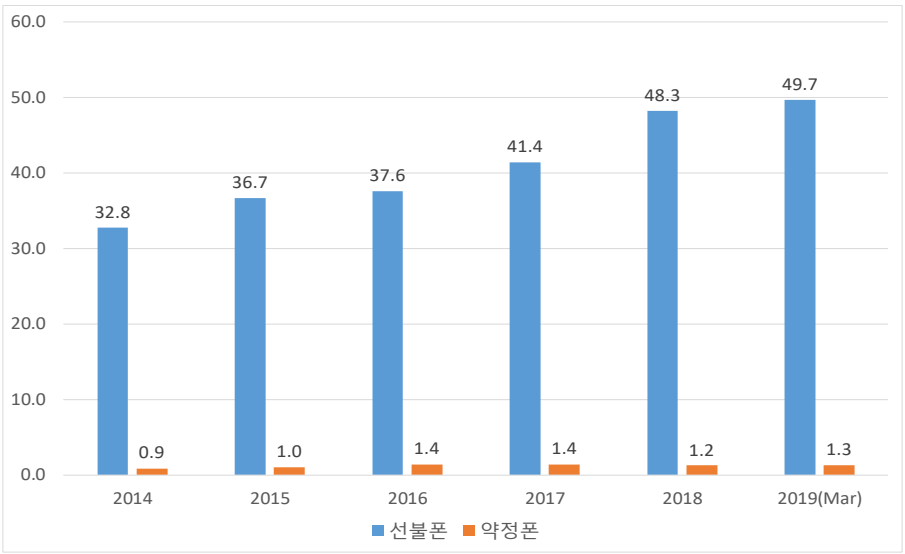
그림 _ 이동통신 기업별 통신 사용량 점유율 추이



[출처] Buddecomm(2018.)

- 이동통신의 가입형태별 가입자 수 추이를 보면, 케냐의 이동통신 가입자 대부분 약 4,970만명이 선불폰을 사용하는 것을 나타났음

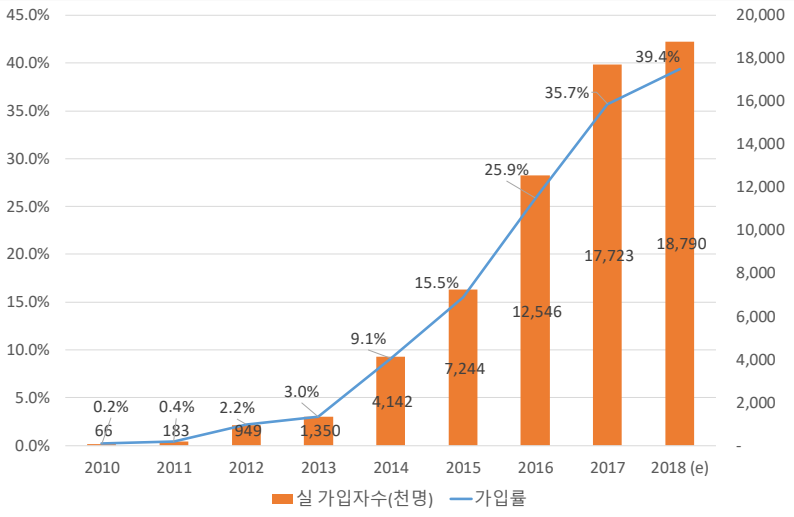
그림 _ 이동통신 가입형태별 가입자수 추이(백만명)



[출처] Buddecomm(2018.)

- 이동통신 실가입자(Active Subscriber)는 2018년 추정치 기준으로 1,870만여명으로, 가입률은 39.4%에 달하고 있음

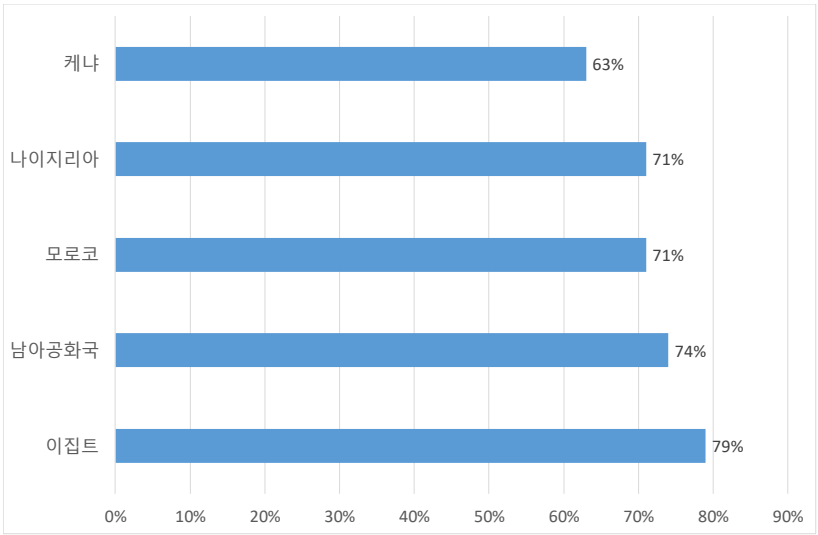
그림 _ 이동통신 실가입자 및 가입률 추이



[출처] Buddecomm(2018.)

- 케냐의 모바일 사업자들은 모바일 데이터 서비스를 위해 최신 모바일 기술과 인프라 구축을 위해 지속적인 투자를 단행하고 있지만, 시장 경쟁의 격화로 인해 수익성에 문제가 있는 것으로 나타남
- 케냐 정부는 모바일 사업자에게 LTE 서비스를 독려하고 있으나, 특허를 둘러싼 기업 간 분쟁으로 인해 LTE 서비스의 공급이 지연되고 있음

그림 _ 2017년 2/4분기 기준 아프리카 지역 스마트폰 인터넷 사용자 보급률



[출처] yStat.com

• 케냐는 아프리카 주요국 중에서 스마트폰을 이용한 인터넷 접속 비중이 63%에 달할 정도로 이동통신 인터넷 사용 비중이 높은 나라이나, 이집트나 남아공화국, 모로코 등에 비해서는 상대적으로 낮은 비중을 보이고 있음

• 케냐의 모바일 인터넷 사용자들은 SNS 사용 등의 활동이 56%로 가장 많은 것으로 나타났으며, 다음으로 검색엔진 사용 43%, 온라인 비디오 시청 31% 순으로 나타났는데, 국가별로 다소 차이는 있으나 대체로 유사한 경향을 보이고 있음

표 _ 아프리카 주요국의 모바일 인터넷 사용 영역

주요국	온라인 비디오 시청	SNS 사용	검색엔진 사용	제품정보 확인	온라인 구매	게임
모로코	62%	60%	44%	34%	22%	19%
나이지리아	22%	58%	43%	7%	7%	4%
남아공화국	13%	56%	32%	8%	7%	5%
케냐	31%	56%	43%	11%	5%	6%

[출처] yStats.com

정보보호 시장 현황

1) 시장 규모

시장 규모 및 성장률

▶ 2014년 전 세계 보안 시장 성장률은 7.9%이며 중동/북아프리카는 8.4%, 남아프리카는 3.8%의 성장률을 기록함

- 아프리카 시장의 성장률에도 불구하고 글로벌 시장에서 아프리카가 차지하는 비중은 중동과 아프리카 전역을 합하여 2% 정도에 그치고 있음

▶ 2017년 기준 케냐 정보보안 시장 규모는 2,330만 달러 수준으로 추정

- 시장조사기관 Technavio의 2015년 자료[459]를 활용해, 2017년 시장 규모를 추계하는 회귀식을 구했으며, 이를 2017년 변수에 적용하는 방법을 취해 2,330만 달러 규모를 도출[460]

▶ 케냐 보안 시장은 IT서비스의 시장 성장과 더불어 성장할 것으로 예상되나 현재 케냐 IT서비스 시장 자체는 여전히 작은 규모임

그림 _ 케냐 IT서비스 시장 : 2014-2020



[출처] BMI Research(2016)

459 Technavio, Global Information Security Products and Services Market 2015-2019(2015)

460 GDP와 인구 규모를 독립변수로 다중회귀분석을 시행. 계수의 p 값이 낮은 GDP 데이터를 활용했으며, 국가별 GDP 편차가 크게 나타나 LOG 값을 취하여 다중회귀분석을 재시행하여 추정의 정확도를 높임. 데이터가 있는 22개 국가의 시장 규모와 GDP에 기울기인 1.095444925621930을 곱해서 산출했으며, Y 절편인 -0.668571234를 계산하여 세네갈 등 데이터가 없는 8개 국가의 GDP에 곱해서 추정

- 케냐 2016년 IT서비스 시장 규모는 IT 전체 시장 중 21.5%로, 이집트의 28.4%, 남아프리카공화국의 40%와 비교됨
- 정부가 추진하는 프로젝트가 동 기간 동안 가장 큰 IT 시장의 재원
- 향후 클라우드 컴퓨팅과 비용 대비 효율적인 솔루션이 케냐 IT시장의 긍정적인 전망을 가져올 것으로 예상됨

▶ 정보보안 시장에서는 각종 제품과 서비스에 대한 수요가 지속적으로 증가하고 있는 것으로 보이나, 신뢰할만한 시장 정보를 확보하기는 쉽지 않은 상황임

- 글로벌 기업들의 움직임을 보면 Cyberoam 등의 네트워크 장비 기업이 현지 여러 기업과 파트너십을 체결하고 자사 제품을 현지에 마케팅하고 있는 것을 파악할 수 있음
- 또한, 클라우드 서비스의 증가로 MSS(Managed Security Service) 등과 같이 아웃 소싱 및 서비스 형태로 기업에게 통합적인 보안 서비스를 제공하는 사업자도 증가하고 있음
- 케냐 침해사고대응팀 사이트인 KE-CIRT 홈페이지에서는 보안 사고에 대한 신고를 받고 있으나, 케냐 자체적으로 사이버 범죄에 대한 신뢰성 있는 자료를 구하기 힘든 상황이며 이러한 통계는 글로벌 기업의 통계에 의지할 수밖에 없는 상황임

▶ 시장조사기관 SDI는 2015년 국토 보안(Homeland Security) 부문에 대한 케냐 정부의 예산을 10억 달러 규모로 분석했으며, 이집트, 앙골라, 모로코 등과 비교할 때 낮은 것으로 평가함

- 정부의 국토 보안을 향상시키기 위한 현대화 계획 및 국력 증강에 힘입어 케냐 예산 지출 증가율은 2016년~2020년까지 연평균 3.94%의 성장률을 기록할 전망임

표 _ 아프리카 주요국 국토 보안 예산 : 2011-2015 vs. 2016-2020

국가	CAGR 2011-2015	CAGR 2016-2020	2015년 예산 (십억 달러)
앙골라	22.54%	10.74%	8.2
이집트	8.42%	9.82%	5.9
남아공	-2.87%	2.85%	4.0
모로코	4.70%	4.44%	4.0
케냐	2.60%	3.94%	1.0

[출처] SDI, 'Homeland Security Expenditure in Kenya to 2020: Market Review(2015.6)

그림 _ 2016~2020년 케냐 국토 보안 부문에 대한 정부 지출 규모 및 성장률 전망



[출처] SDI, 'Homeland Security Expenditure in Kenya to 2020: Market Review(2015.6)

2) 주요 사업자 현황

시장 특성 및 경쟁 강도

▶ 케냐 사이버 보안 시장은 Symantec 및 Cyberoam 등 다국적 기업들이 현지 통신사 및 ISP 등과 협력하여 시장을 공략하고 있는 형국임

- 케냐는 여타 국가와 같이 다국적 보안솔루션 기업의 영향력이 큰 상황이며, 최근에는 네트워크 장비 위주의 보안에서 통합적으로 제공되는 보안 서비스 시장으로의 전환 및 보완도 이루어지고 있는 것으로 판단됨
- 현지 IT 솔루션 기업인 Naisoft가 현지에서 판매하는 제품을 보면 다음과 같으며 주로 네트워크 보안 장비에 치중하고 있는 것으로 분석됨

·Antivirus
·Content/Spam Filtering
·Network Management
·Change and Configuration Audit
·Data Leakage Protection
·Intrusion Detection & Prevention IDS/IPS.
·Firewalls
·Virtual Private Network (VPN)
·Integrated Security Appliance (UTMs)

주요 사업자

▶ Safricom

- 케냐 통신사업자 Safricom은 케냐 정부와 149억 케냐 실링(KES)(1억 6,220만 달러) 규모의 시스템을 구축하는 계약을 체결하였으며 18개월에 걸쳐 완료될 예정임
- 국회 행정 및 보안 협의회는 해당 프로젝트를 2014년 6월 승인했으며 이러한 조치는 2013년 9월 나이로비 웨스트게이트 쇼핑몰의 보안 사고 후에 일어난 조치임
- 해당 계약 하에 사업자는 통신 및 보안경계 시스템을 설치 및 운영할 것이며, 우선 나이로비 및 몸바사 지역 경찰서를 연계할 예정임

▶ Cyberoam

- 인도의 네트워크 보안솔루션 공급자인 Cyberoam은 케냐에 본거지를 둔 민간 및 공공 IT서비스 제공사업자 BusinessIT Africa와 파트너십을 체결하고 보안 분야에서 협력하기로 함 (2014.10)
- BusinessIT는 Cyberoam 보안제품, 즉 UTM(Unified Threat Management Appliances) 및 관련 보안제품을 케냐에서 마케팅하기로 함
- Cyberoam 케냐 채널 매니저에 따르면, 케냐의 인터넷 및 스마트폰 사용 증가로 네트워크 보안은 비즈니스의 필수불가결한 부분이 되고 있음
- 케냐에서 판매되는 Cyberoam 제품은 다음과 같음
  - ·Cyberoam NetGenie
  - ·Cyberoam Network Security Appliances–Next-Generation Firewalls(NGFW), Unified Threat Management Appliance(UTM)
  - ·Cyberoam iView
  - ·Cyberoam Central Console

그림 _ 케냐에서 판매되는 Cyberoam 제품



▶ Symantec

- Symantec은 SEACOM의 클라우드 컴퓨팅 계열사 Pamoja와의 파트너십을 발표함
- Symantec은 사하라 이남 지역(Sub-Sahara) Pamoja의 네트워크에서 전 계층을 포괄하는 통합 솔루션을 제공할 예정임
- 케냐 및 남부 아프리카에 데이터센터를 가지고 있는 Pamoja는 중소기업을 타깃으로 함

▶ AccessKenya

- 인터넷 서비스 제공자 AccessKenya는 보안기업 Security Risks Solution 및 Internet Solutions Kenya와 협력하여 보안 관리 서비스(Managed Security Service, MSS)를 출시함(2014.3)
- 동 서비스는 주 7일 네트워크 모니터링이 가능하고, 실시간으로 로그를 캡처링할 수 있으며, 전자파일 조작을 사전에 고지하는 등의 기능을 제공함

▶ NetGuardians

- 스위스 소프트웨어 기업인 NetGuarians는 금융 IT 기업 Sofgen과 파트너십을 체결하고 케냐에 사기방지 SW를 출시하기로 함
- NetGuarians는 Price Waterhouse Coopers(PwC) 현지 조직이 수행한 컨설팅 및 리서치에 의하면 케냐 내 기술적 금융 사기가 큰 위협으로 나타나고 있어 동 서비스를 시작하게 됨

3) 주요 동향 및 이슈

▶ 케냐 SafariCom, 중국 Huawei와 400G 백본 네트워크 제공을 위한 파트너십 체결(2018.2.28.)[461]

- 400G 백본 네트워크는 나이로비와 몸바사 지역에서 처음 시행될 예정으로 2단계에 나누어서 구축 예정
- Huawei의 시스템이 적용됨에 따라, 보안장비도 Huawei의 제품으로 적용될 것으로 예상되며, 최근 미국, 유럽 등에서 발생되는 백도어에 대한 불안은 증가할 것으로 사료
- 이에 따른 보안제품에 대한 인증 등과 관련해 한국과의 사이버보안 관련 협력 필요할 것으로 전망되고 있음

▶ 케냐의 새로운 프라이버시 보호법이 오히려 경제에 부정적 영향을 미칠 가능성(2018.11.8.)[462]

- 시장 전반의 개인정보 보호를 위한 세이프 가드를 마련하고 국가의 디지털화를 촉진하기 위한

461 KISA 정보보호 해외진출 전략거점 주요동향 각 월호
462 Sabina Frizell, How Kenya's New Data Privacy Bill Could Hurt Its Economy, Council on Foreign Relations

목적으로 케냐 정부가 추진 중인 새로운 데이터 보호 법안이 현재 케냐 의회의 검토 중에 있으나 과도한 규제 때문에 오히려 케냐 경제의 활성화를 저해할 가능성이 지적되고 있음

- 이런 의구심은 케냐 정부의 선거부정 관련 스캔들을 덮기 위한 것이 아니냐는 의혹과 함께, 법안의 주요 내용이 개인 데이터에 대한 통제에 초점이 맞춰져있는 한편, 규제 기준의 대부분이 대형 다국적 기업이 아니면 쉽게 충족하기 어려울 정도로 높기 때문에, 케냐의 중소기업으로써는 커다른 부담이 되고 있기 때문임
- 이번에 의회에 계류되어 있는 케냐의 프라이버시 보호 법은 유럽의 개인정보보호 규정(General Data Protection Regulation, GDPR)과 사이버 보안과 개인 정보 보호에 대한 아프리카 연합 조약(African Union Convention on Cyber Security and Personal Data Protection)에 부응하기 위해 도입을 준비하고 있음

▶ 사이버보안 내재화 교육 강화(2019.3.26)[463]

- 케냐는 고등학교에서부터 사이버시큐리티, 개인정보보호, 안전한 데이터 관리 교육 추진 예정
- 케냐에서는 2018년 기준으로 약 300억 실링(한화 3,000억원)이 사이버범죄에 따른 손실이 발생하였고, 이를 완화시키기 위한 중장기전략 수립 필요
- 케냐는 아프리카 국가 중 IT가 발달되어 있고, 그에 따라 아프리카 국가 중 5대 사이버침해 피해 국가임
- 특히, 관련 기술은 대부분 수입에 의존하고 있어 자체 개발과 운영능력 향상을 위한 전문교육 필요

▶ 보안 강화를 이유로 도입하는 케냐의 바이오메트릭 계획이 오히려 논란을 불러일으키고 있음(2019.5.3.)[464]

- 대국민 서비스를 증진하기 위해 6천만 달러를 들여 도입하는 정부의 바이오메트릭 데이터 수집 계획이 오히려 비효율과 잘못된 관행을 낳을 것이라는 비판에 직면하고 있음
- 케냐 정부는 이번 바이오메트릭 정보 수집 계획이 시장의 보안을 공고히 할 뿐 아니라 사회에 만연한 부정부패를 제거하고, 사회적 자원을 보다 효율적으로 사용하고 정부의 서비스 전달을 효율적으로 하기 위한 것이라고 주장
- 그러나 이러한 바이오메트릭 정보를 수집하는 기관들이 대부분 심각한 교통체증을 겪고 있는 도심지에 위치하고 있어 등록 절차가 매우 어려운데다, 개인 정보 등록을 거부하는 개인에게는 정부의 서비스 제공을 중단하겠다는 위협적인 내용도 들어 있어 케냐의 인권 단체에서 이에 대한 반감이 높아지고 있으며, 이 계획을 주도하는 기업이 프랑스의 다국적 기업이라는 점 역시 국민들의 반감을 사는 요인으로 작용하고 있음

463 KISA 정보보호 해외진출 전략거점 주요동향 각 월호
464 Keren Weitzberg, Kenya's Controversial Biometric Project Is Shrouded in Secrecy, .Coda Story

▶ 케냐에서 사이버 보안 위험 증가 추세로 나타나(2019.5.15)[465]

- 케냐통신위원회에 따르면 2018년 4분기에 케냐 사이버공간을 목표로 한 사이버 위협이 1,020만 건으로 전년 동기간 380만 건보다 2배정도 증가한 것으로 조사됨
- 발견된 사이버 위협으로는 서비스 거부 공격 (DoS), 온라인 사기, 혐오 발언, 폭력 및 가짜 뉴스 선동, 소셜 미디어 계정 및 도메인 이름을 통한 온라인 사칭, 앱 불법 액세스 등의 웹 애플리케이션 공격 등임
- Emotet 이라는 악성코드가 11개 케냐 기관을 공격하여 온라인 뱅킹 및 지불 시스템을 통해 케냐 시민들의 기밀 정보에 접근한 것으로 보고되었으며, 2017년에도 이런 사이버 공격으로 케냐 금융기관들이 210억 KES의 손실을 본 것으로 집계되었음

▶ 아프리카 지역의 데이터 보호와 프라이버시를 주제로 하는 대규모 토론회에서 케냐의 데이터 보호 법안의 내용이 주목을 받음(2019.6.26)[466]

- 2019년 6월 24~27일 동안 가나에서 열린 아프리카 국제 데이터 보호 및 프라이버시 컨퍼런스(Africa International Data Protection and Privacy Conference)에서 케냐 정부가 추진 중인 데이터 보호 법안에 관심이 집중되었음
- 아프리카 지역에서 모바일에 기초한 경제규모가 2020년경에 아프리카 전체 지역 GDP의 7.6%를 차지할 것으로 예견됨에 따라 금융과 헬스 케어, 교육과 농업 등의 분야에서 보다 품질 높은 서비스 제공의 필요성이 높아지고 있음
- 2018년부터 케냐 정부에 의해 도입이 추진되고 있는 데이터보호법안은 디지털 전환에 따른 경제적 이해를 선제적으로 포착하기 위한 주목할 만한 움직임으로 주목받았음

▶ 케냐 주요 정부기관 해커 공격으로 웹사이트 한때 마비(2019.7.8)[467]

- 인도네시아 해커 그룹 Kurd Electronic은 케냐 주요 정부기관 홈페이지를 공격하여 2019년 6월 3일 오전에 이들 기관의 웹사이트가 마비되는 상황이 발생
- 주요공격 웹사이트는 케냐 국가청소년서비스사업위원회, 이민국, 육류위원회, 석유부, 난민청, 국가환경신탁기금, 기획처, 국가개발실행기술위원회, 정부 중앙 결제 시스템(IFMIS), 통신청 등
- 케냐 CERT는 관문국에 대한 모니터링, 특정 IP차단, DDoS 공격 우회 등의 대응시스템이 부재하며, CERT를 운영중인 통신청(CA)과의 협력을 통한 국가 사이버 테러 대응 시스템이 필요한 것으로 나타남

465 KISA 정보보호 해외진출 전략거점 주요동향 각 월호
466 CIO East Africa, Kenya's progress on data privacy comes under the spotlight
467 KISA 정보보호 해외진출 전략거점 주요동향 각 월호

▶ 케냐 2019년 1/4분기 사이버 위협, 전분기 대비 10.1% 증가한 것으로 나타나(2019.8.2)[468]

- 케냐 통신청(CA)에 따르면 케냐의 2019년 1분기 사이버 위협은 1120만 건으로 전분기 대비 10.1% 상승, 악성프로그램, 웹애플리케이션 공격, 시스템 구성 오류 및 온라인 남용의 사례가 증가
- CA 사이버정보팀은 1만 4078건의 사이버위협 경보를 내렸는데 이는 전분기 1만 2138건보다 증가. 기술 컨설팅회사인 Serianu가 최근 발표한 보고서에는 사이버 보안 위협이 케냐의 경제에 약 295억 달러의 손실을 입힌 것으로 추정

▶ 케냐중앙은행, 고객정보관리를 위한 새 시스템 도입 추진(2019.8.2)[469]

- 케냐중앙은행은 은행 및 모바일머니, 결제서비스 회사 등이 고객정보를 단일 전자 플랫폼에 저장하고 액세스 할 수 있도록 변경할 예정
- 새로운 플랫폼 공동개발을 위해 싱가포르 통화청 양해각서를 체결, 동 시스템은 사기 및 돈세탁을 억제하며 고객정보를 효율적이고 안전하게 관리 할 수 있을 것으로 기대

▶ 2019년 8월 19일에 개최된 AfricaHackOn 사이버보안 컨퍼런스에서, 케냐에서 점증하는 사이버 범죄에 대응하기 위한 전문인력의 양성과 숙련 확대를 주장(2019.8.16)[470]

- 케냐의 통신업체인 Safaricom의 사이버 보안 담당 이사인 James Yogo는 케냐의 사이버 보안 인력 양성의 중요성을 강력하게 언급
- 최근 케냐의 IT 컨설팅 업체 Serianu는 케냐에서 발생한 사이버 범죄에 따른 피해액이 2016년 기준으로 1억 7,500만 달러에 이르렀으며 이는 2015년 1억 5천만 달러에 비해 급증한 것이라고 발표했으며, 케냐의 통신 감독당국은 2019년 1/4분기에 발생한 사이버 범죄 건수는 1,120만건으로 전년에 비해 10.1% 증가했다고 발표

468 KISA 정보보호 해외진출 전략거점 주요동향 각 월호
469 KISA 정보보호 해외진출 전략거점 주요동향 각 월호
470 Julie Owing, Companies urged to implement new strategies of dealing with cyber security threats, Capital Business

정보보호 정책 및 기관 현황

1) 관련 법령 및 정책

관련 법령 및 규제

▶ 케냐 정보통신 보안법령(Kenya Information and Communication Act CAP411A)

- 케냐 정보통신 보안법령은 1998년 제정되었으며, 2013년과 2014년에 개정됨
- 동 법령은 Communications Commission of Kenya(CCK)가 국가보안대응팀인 CIRT(National Computer Incident Response Team)를 설립하고 이를 통해 국가 사이버 보안 프레임워크를 개발하도록 규정함
- CCK는 KE-CIRT/CC 설립을 통해 국가 사이버 보안 사고에 대응·관리하고 자국 내 이해관계자, 지역 및 해외와의 협력을 주도하도록 역할을 부여함

▶ 컴퓨터 오용 및 사이버 범죄법(Computer Misuse and Cybercrimes Act)

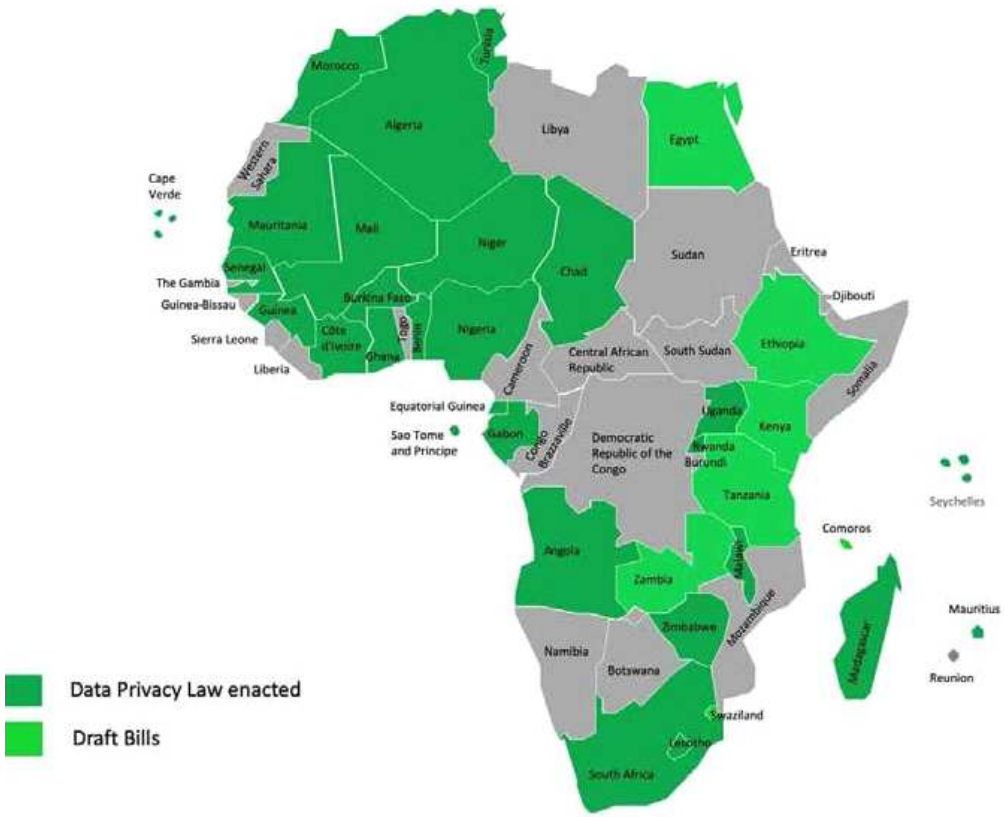
- 8년 동안 케냐 정보통신 부문의 논의를 거쳐, 2018년 5월 14일 케냐 국가 안보 위원회 의장이자 대통령인 우후루 케냐타(Uhuru Kenyatta)가 서명하면서 컴퓨터 오용 및 사이버 범죄법 발효
- 이 법은 케냐에서 발생하는 사이버 범죄에 대한 처벌의 프레임워크를 제공하는 것을 목표로 하며, 허위 정보 유포, 사이버 공격, 사이버 침해, 아동 포르노그래피 및 컴퓨터 시스템 무단 침입 등을 사이버 범죄로 규정 및 처벌하는 것을 주된 내용으로 하고 있음
- 보안 시스템이 설치된 컴퓨터에 대한 무단 침입에 대해서는 2,500만 KES나 20년 징역형, 아동 포르노그래피는 2,000만 KES나 25년 징역형이 부과됨
- 모바일 금융 사기에 대한 범죄의 정의와 형벌 역시 규정되어 있음
- 이 법에서 규정하는 사이버 범죄의 모호성과 시민의 프라이버시의 침해 가능성 등에 대해 케냐 시민사회의 지속적인 문제제기가 있으며, 케냐 고등 법원 역시 이에 대해 유사한 우려를 표명하고 있음
- 이 법의 발효에도 불구하고, 실제로 이 법이 작동하기 위해서는 다양한 장애물이 존재하는데, 가장 큰 문제점은 정보통신 기술 분야 전문 인력의 부족이 지적되고 있음

▶ 데이터 보호법(Data Protection Bill)

- 2018년 7월 3일 데이터 보호법이 도입됨에 따라 케냐에서 개인정보보호체계가 본격적으로 수립되었음

- 이 법의 주된 내용은 기업과 공공기관들이 수집하고 보관하는 개인정보를 보호하는 것을 목적으로 하고 있으며, 개인의 프라이버시에 대한 권리의 법적 기초를 확보하는데 주안점을 두고 있음
- 이 법의 발효에 의해 케냐 2010년 수정 헌법 제31조(c)와 (d) 항에 규정된 개인과 가족과 관련된 정보가 불필요하게 공개되지 않을 권리와 통신 비밀의 보호가 가능해졌음
- EU가 2018년 5월에 공표한 일반 데이터 보호 규정(General Data Protection Regulation, GDPR)의 골격을 준수하는 한편, 동아프리카 지역에서 르완다에 이어 두 번째로 데이터 보호와 관련된 법체계를 가진 나라가 되었음

그림 _ 아프리카 지역 보안 법률 제정 현황



[출처] Cyber Security Report 2018

▶ 산업별 사이버 보안 관련 주요 규정

- 케냐는 금융부문에 다양한 보안 관련 규정을 두고 있는데, 저축신용협동조합(Sacc0)은 물론, 이 Sacco의 감독당국인 SASRA, 케냐 중앙은행, 지급결제 서비스 제공자의 위험관리 시스템을 구체적으로 규정하는 가이드라인을 수립

구분	발효 일자	규제 범위
SASRA(Sacco Societies Regulatory Authority) 사이버 보안 위험 관리 가이드라인	2018	사이버보안과 위험 관리 프레임워크를 효과적으로 발전시키기 위해 예금 저축 조합(Deposit Taking Savings)이 채택해야 하는 최소한의 기준
케냐 중앙은행(Central Bank of Kenya) 사이버보안 가이드 노트	2017.8	· 거버넌스-이사회, 중견 관리자 및 CISO의 역할 · 내부 감사의 역할 · 리스크 관리 기능의 역할 · 외부 감사의 역할 · 아웃소싱 · 사이버보안 관련 훈련/경각심 부여 · 사이버 보안 침입에 대한 보고
지급결제 서비스 제공자의 사이버 보안 가이드라인	2018.8 초안 수립	· 지급결제 서비스 공급업체(Payment Service Provider, PSP)의 분류 · PSP의 거버넌스 구조 · PSP의 일반적인 리스크 관리 요건 · 리스크 관리 전략의 종속성과 사이버 복구 능력 · 독립적인 규제 평가와 테스트 · 아웃소싱 · 사이버보안 관련 훈련/경각심 부여 · 사이버 보안 침입에 대한 보고
수신 기능이 있는 저축신용협동조합 (Sacco)의 위험관리 관행에 대한 가이드라인	2015.6	· 전반적인 리스크 관리 프레임워크 요구사항 · 전략적 위험 관리 · 신용위험 관리 · 운영위험 관리 · 정보 및 통신기술 위험 관리 · 유동성 위험 관리 · 시장 위험 관리 · 규정 준수 위험 관리

[출처] Cyber Security Report 2018

주요 전략 및 정책

▶ 케냐는 ITU와 미국 무역개발부의 도움으로 CIRT를 설립함

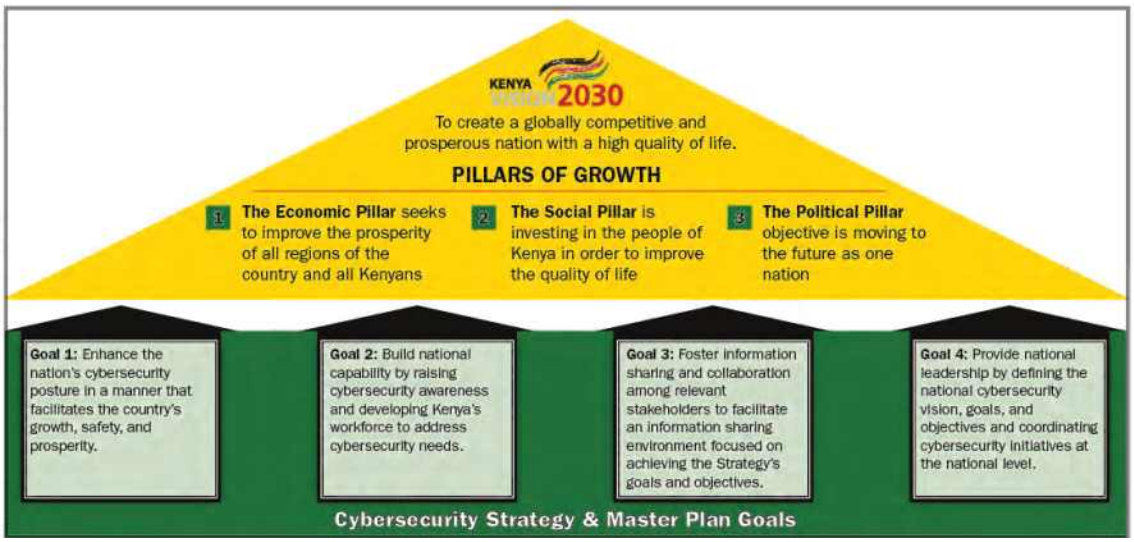
- 케냐 통신위원회는 국가 사이버 보안 사고 중재 및 관리에 책임 기관인 CIRT를 운영함
- 2012년 2월, 정부는 ITU와 국가 컴퓨터 사고 대응 센터를 설립하기로 계약을 체결함

- 또한 정부는 법률 및 사이버 공간의 표현 자유를 해결하기 위한 지역 사이버 보안 수련회에 참가함
- 케냐는 동아프리카 커뮤니티(East African Community)에 포함되어 있으며, Common Market Protocol을 뒷받침하기 위한 사이버 법률을 개발하는 것에 관심을 표명했음
- 미국 무역개발청은 58만 달러를 케냐 정보통신부에 기부하여 케냐가 국가 사이버 보안 마스터 플랜, 즉 국가 정보 네트워크를 위한 사이버 보안 표준, 보안 프레임워크를 개발하도록 지원함

▶ 케냐 정부의 국가 사이버 보안 전략(National Cyber security Strategy)

- 케냐 정부의 보안 전략은 Vision 2030의 3가지 원칙을 중심으로 움직이면서 국가 ICT 마스터 플랜도 지원하는 개념으로 진행
- 전략의 목적은 케냐 사이버 보안 비전, 성취목표 및 목적을 확고히 하여 케냐 사이버 공간의 안전을 확보함으로 케냐의 지속적 경제성장에 필수적인 ICT 성장을 장려하기 위함임
- 케냐 정부는 사이버 보안 인식수준을 향상 시킬 필요성을 인식하고 다음과 같은 몇 가지 조치를 취함: Kenya Information and Communications (Amendment) ACT, 2014 개정안, National Kenya computer incident response Team coordination Center(KE-CIRT), Nation Certification Authority Framework 제정
- 공공 주요 인프라 구현 및 케냐 현지 및 국제 사이버 보안 협력기구 및 포럼과의 협력을 위한 프레임워크를 설립함

그림 _ 케냐 사이버 보안 전략 및 마스터플랜의 목표

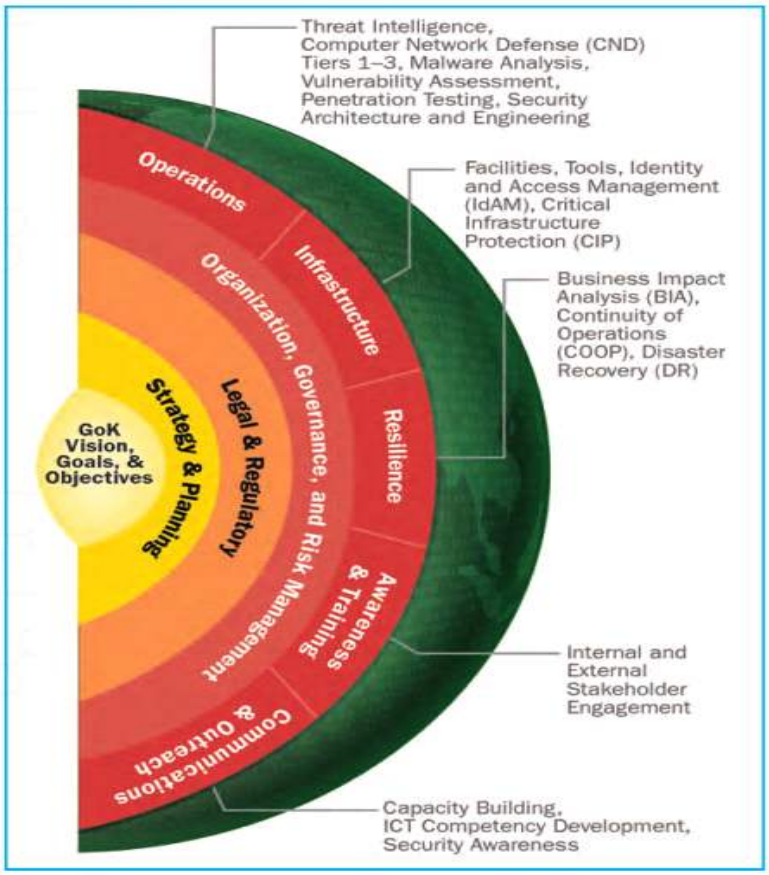


[출처] Kenya Cybersecurity Report 2015

▶ 케냐 정부는 사이버 보안에 관한 정부 차원의 확고한 실천을 위해서 다음과 같은 4가지 목표를 설정함

- 목표1) 정부는 사이버 보안이 국가 성장, 안전 및 번영을 가속한다는 자세로 정부 차원의 사이버 보안 의식을 강화함
- 목표2) 정부는 사이버 보안 의식을 높이고 사이버 보안 필요에 따른 인력 등의 개발함으로써 국가적 사이버 보안 능력을 구축함
- 목표3) 정부는 사이버 보안 정책 및 정보 등을 업계 이해관계자와 공유, 이를 통한 협력 체계를 강화함
- 목표4) 정부는 국가 사이버 보안 비전, 목적, 목표 등을 정의하여 사이버 보안의 국가적 리더십을 확립하고 국가 차원의 사이버 보안 동기 부여를 고취함

그림 _ 케냐 사이버 보안 목적 및 목표



[출처] Kenya Cybersecurity Report 2015

2) 담당기관

▶ 케냐 통신규제국(Communications Authority of Kenya; CA)

- 2013년 정보통신법이 개정되면서 기존 통신 규제 기관이었던 케냐 통신위원회(CCK)가 해산되고 정부로부터 독립되고 상업적 영향을 받지 않는 케냐 통신규제국(CA)이 설립됨
- CA의 기능
  - ·통신, 우편, 택배, 방송 등 통신 업계의 모든 시스템과 서비스에 면허 부여
  - ·국가 주파수 스펙트럼 및 전화번호 자원 관리
  - ·전자상거래 발전 촉진
  - ·케냐에서 사용되는 통신 장비의 승인 및 도입
  - ·통신 환경에서의 소비자 권리 보호
  - ·면허 사용자 활동 모니터링 및 계약 조건 준수 확인

▶ 케냐 컴퓨터침해사고대응팀(Kenya Computer Emergency Response Team, KE-CERT)

- KE-CIRT의 기능은 다음과 같음
  - ·로컬 CIRT, 지역 CIRT, 타국의 CIRT 및 다른 조직과의 연계를 담당
  - ·정보 보안 사고에 관한 기술 정보 수집, 취약점, 보안 수정사항 및 여타 보안 사항 등의 공표 및 알림
  - ·컴퓨터 보안 및 관련 기술 리서치 및 분석 수행, 또한 새로운 트렌드에 대한 정보 제공 및 가이드
  - ·국가 공공 보안 인프라스트럭처(PKI)의 개발 독려
  - ·정보보안에 대한 능력 확립 및 사이버 보안 관련 활동에 대한 인식 제고
- KE-CIRT/CC의 이해관계는 다음과 같음
  - ·Ministry of Information and Communication(MOIC)
  - ·Communications Authority of Kenya(CAK)
  - ·Kenya ICT Board(KICTB)
  - ·International Telecommunications Union(ITU)

그림 _ 케냐 사이버 보안 거버넌스 조직



[출처] www.privacyinternational.org

4) 최근 정책 동향 및 이슈

▶ 사이버 보안법의 기초를 닦는 케냐 (2018.5)[471]

- 케냐의 새로운 사이버 보안법(Computer Misuse and Cybercrimes Bill)이 5월 30일 자로 발효됨
- 케냐 국가 안보 위원회(National Security Council)가 작성한 사이버 보안법은 의장이자 대통령인 우후루 케냐타(Uhuru Kenyatta)의 주도로 이루어짐
- 컴퓨터를 이용한 위조, 사기, 허위 정보 게시, 신분 도용 등의 사이버 범죄를 강력하게 처벌하는 것을 골자로 함
- 허위 정보 게시 및 유포의 경우 최대 5백만 케냐 실링의 벌금 혹은 2년의 징역형을 선고받게 됨
- 사이버 폭력 및 스토킹의 경우 10년 이하의 징역, 2천만 케냐 실링의 벌금 혹은 두 가지 형벌을 모두 받을 수 있음
- 그러나 대법원 판사 차차 위타(Chacha Mwita)는 법안 중 단어의 정의가 모호하여 개인의 권리와 기본권 침해 소지가 있는 26개 항목은 7월 16일까지 발효를 중지시킴
- GDPR을 대비한 개인정보 보호법 제도 완비 및 사이버 보안법 보완을 위하여 7월 3일, 데이터

471 Citizen, "Ksh.5M fine or 2 years in jail for fake news as Uhuru signs Cyber-Crimes Bill", 2018.5.16.
VOA, "Kenyan Court Suspends Key Parts of New Cyber Law", 2018.5.30.
Hunton, "Kenya Considers Data Protection Bill", 2018.7.6.
Business Daily Africa, "Why EU's data privacy rules matter for Kenyan businesses ", 2018.5.24.

보호법(Data Protection Bill)의 초안이 작성됨

- 데이터 보호법은 은행, 통신사업자, 공공시설, 회사와 개인이 개인 데이터를 수집하고 처리하기 전에 데이터 주체의 동의를 얻도록 요구하는 내용을 담고 있는 법안
- 데이터 보호 법안을 위반할 경우 벌금 50만 케냐 실링 혹은 최대 5년 이하의 징역형을 선고받게 됨

융합보안시장 및 정책 동향

1) 융합보안시장 동향

스마트의료

▶GE Healthcare와 케냐의 의료 엔지니어링 협회가 주관하는 회의가 개최(2019.8.8.)[472]

- 케냐의 민간과 공공 부문에서 종사하는 의료 관련 엔지니어 100여명이 GE Healthcare가 주관하는 의료 분야의 숙련 향상을 주된 내용으로 하는 회의와 행사에 참여
- 이 회의는 바이오 메디칼 분야의 최신 정보와 지식, ksfus 의료 장비의 사용 방법 등에 대한 훈련을 주제로 진행되었음
- GE Healthcare는 케냐 정부와 함께 지난 2016년에 1300만 달러를 들여 케냐에 헬스케어 훈련 센터를 건립하여 케냐의 의료 및 헬스케어의 질을 제고하기 위한 다각도의 노력을 펼치고 있음

스마트공장

▶ 케냐, 인공지능에 대한 대비 순위 아프리카에서 중 1위로 나타나(2019.7.8.)[473]

- Government Artificial Intelligence Readiness Index 2019에 따르면 인공지능에 대한 정부의 대비가 케냐는 아프리카에서 1위, 세계에서 52위에 링크되었음
- 케냐 제조업 분야 디지털화 구축에 있어 중소기업이 가장 준비가 취약한 것으로 나타났으며, IT정책을 시행 중인 기업을 규모별로 보면, 대기업은 78%인데 반해 중소기업은 20~40%만이 IT정책을 시행하는 것으로 조사 됨
- 케냐의 제조업의 디지털화에 따른 물리·정보보호에 대한 장비 수요가 증대할 것으로 전망

블록체인(가상화폐 등 포함)

▶ 케냐 중앙은행의 경고에도 불구하고, 케냐에서 가상화폐에 대한 인기가 점증하는 것으로 나타남(2019.2.22.)[474]

---

472 African News, GE Healthcare and the Association of Medical Engineering of Kenya host more than 100 biomedical engineers for Biomedical Excellence Day
473 KISA 정보보호 해외진출 전략거점 주요동향 각 월호
474 Mary-Ann Russon, Crypto-currencies gaining popularity in Kenya, BBC News

- 케냐 블록체인 협회의 발표에 따르면, 케냐에서 가상화폐인 Bitcoin의 거래 금액이 150만 달러를 상회하는 것으로 나타남
- 현재 가상화폐는 높은 보안성에도 불구하고 케냐의 정부나 중앙은행의 감시가 없는 상황이며, 케냐의 중앙은행은 현재 가상화폐를 은행에서 취급하는 것을 금지하고 있음
- 케냐에서 현재 통용되는 가상화폐는 Bitcoin 외에도 Dash, Lisk 등이 통용되고 있음

핀테크 등

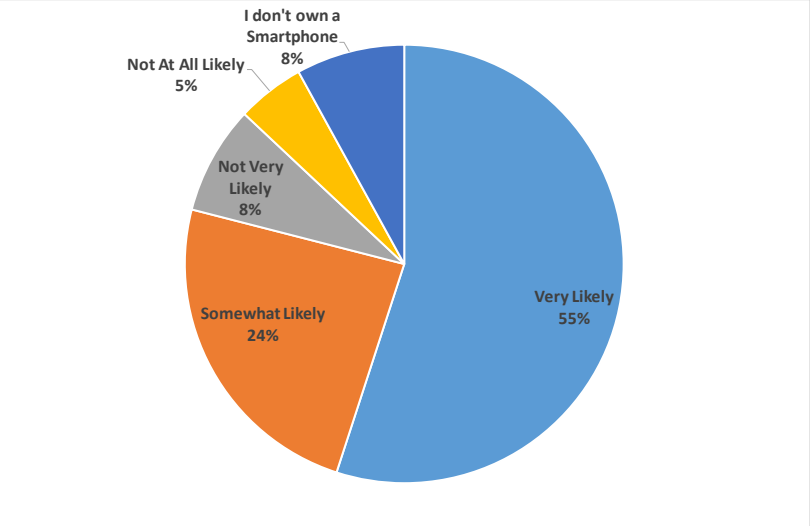
▶ 케냐의 모바일 지급결제 시장은 2018년 기준으로 3조 9,844억 KES의 시장을 형성하고 있음

- 2018년 기준으로 모바일 지급 결제 건수는 연간 17억 4천만여 건이며, 모바일 계좌는 4천 7백만개에 달함
- 모바일 금융 중개인의 숫자는 20만개에 달하고 있음

표_ 케냐 모바일 지급결제 시장 현황

년도	거래건수 (백만건)	거래금액 (10억 KES)	모바일 계좌수 (백만개)	중개인수 (천명)
2008	62.7	166.6	5.1	6.1
2009	193.5	473.4	8.9	23
2010	311	732.2	16.4	39.5
2011	433	1,169.20	19.2	50.5
2012	577.4	1,544.80	21.1	76.9
2013	732.6	1,901.60	25.4	113.1
2014	911.3	2,371.80	25.3	123.7
2015	1,114.20	2,816.10	31.6	143.9
2016	1,526.20	3,355.80	35	165.9
2017	1,543.20	3,638.50	37.4	182.5
2018	1,739.60	3,984.40	47.7	205.7

[출처] yStats.com



[출처] yStats.com

- 모바일 금융 사용 의향에 대한 설문조사 결과를 보면, 차년도에도 매우 적극적으로 모바일 금융을 이용하겠다는 응답이 55%, 다소 그럴 것 같다는 응답이 24%에 이르는 등, 미래 모바일 금융의 사용에 대한 긍정적 응답이 79%에 달하는 것으로 나타남

▶ 케냐의 모바일 금융 서비스 이용자수 지속적 증가 양상(2019.5.15.)[475]

- 2019 Financial Access Household survey에 따르면, 케냐의 금융서비스 이용률이 2016년 75%에서 2018년 82.9%로 증가, 이는 M-Pesa, Airtel money 등의 모바일 머니 서비스에 기인하고 있으며, 지역별로는 나이로비 96%, 몸바사 94%, 리프트밸리 지역은 88%, 중앙지역은 85% 북부 리프트밸리 지역은 57%로 집계
- 통신사 중심의 모바일머니 활용이 급증함에 따른 사이버해킹 사고도 급증하고 있으며, FIDO와 같은 한국의 앞선 모바일 보안기술 등에 대한 시장 진출이 필요

▶ 케냐인들 모바일 머니 활용 증가 및 온라인 도박금지법 발의(2019.7.8.)[476]

- Consumer Insight Africa가 '19년 1-3월간 16개 주요 카운티의 3703명을 상대로 실시한 조사에 따르면, 모바일 대출은 2017년 33%, 2018년 38%, 2019년 49%로 증가세
- 케냐 도박금지법(Gaming Bill 2019), 휴대폰으로 온라인 게임 사용 시 벌금 부과(BD) 및 온라인 게임을 할 경우, 최대 200만 실링 또는 최대 2년 징역형에 처하는 법안 도입 추진

475 KISA 정보보호 해외진출 전략거점 주요동향 각 월호
476 KISA 정보보호 해외진출 전략거점 주요동향 각 월호

▶ 케냐에서 대중적으로 사용되는 모바일 지급결제수단인 M-Pesa가 지난 50년간 가장 영향력 있는 50대 프로젝트 중의 하나로 선정(2019.8.8.)[477]

- 프로젝트 관리 연구소(Project Management Institute)가 발표한, 지난 50년간 가장 영향력 있는 50대 프로젝트 중의 하나로 케냐에서 인기 있는 모바일 지급결제 수단인 M-pesa가 선정됨
- 선정된 프로젝트로는 인터넷 형성에 큰 역할을 수행한 World Wide Web이 1위, 아폴로 11호가 2위로 선정되었으며, 이외에도 사회적 프로젝트로는 르완다의 국가 통합과 화해 위원회, 문학작품으로 해리포터 시리즈 등이 선정되었음
- 2007년부터 Safaricom과 Vodafone이 공동개발한 핸드폰 문자를 기반으로 하는 모바일 지급결제 플랫폼인 M-Pesa는 케냐의 금융 및 은행산업의 지형을 완전히 바꾸었으며, 2019년 기준으로 케냐에서만 3,180만명의 사용자를 확보한 것으로 알려지고 있음

2 융합보안정책 동향

스마트시티

▶ 케냐 정부에서 개발 중에 있는 스마트시티인 콘자 지역에 소재한 케냐 테크노폴리스에 한국과학기술연구원(KAIST)dl 분교 설립을 추진 중(2018.2.28.)[478]

- 한국은 100억 KES(한화 약 1,000억원)을 투자하여 2021년 완공을 목표로 케냐 테크노폴리스에 정보기술 대학 설립
- 사이버보안 관련 학과 개설 지원 등을 위해 한국형 사이버 보안 정책, 기술 노하우 등의 교육을 통해 전문인력 양성 방안을 강구

▶ 케냐의 스마트 시티 계획이 진행되고 있는 콘자 지역의 개발을 중국 선전의 화웨이 캠퍼스 모델을 따라하겠다고 발표(2019.9.29.)

- 케냐의 콘자 테크노폴리스 개발청은 앞으로 40년 동안 이 지역의 인구를 30만에서 1600만명으로 늘리고 이 인구의 90%를 젊은 창업가로 채우겠다는 계획과 함께, 중국 선전에서 성공적인 케이스로 평가되는 화웨이의 본사 지역 개발 모델을 따라하겠다는 계획을 발표
- 케냐 정부는 직장과 주거지역을 근접하게 함으로써 2만명이 넘는 엔지니어를 확보하고 세계적인

477 KISA 정보보호 해외진출 전략거점 주요동향 각 월호
478 KISA 정보보호 해외진출 전략거점 주요동향 각 월호

경쟁력을 확보한 화웨이의 성공 모델을 따라 함으로써 100억 KES가 투자되는 콘자 지역의 개발을 촉진하려 하고 있으나, 자금 조달과 관료주의로 인해 추진 속도는 매우 저하되어 있는 상태임

블록체인(가상화폐 포함)

▶ 케냐 정부, 음식의 안전성을 제고하기 위해 블록체인 기술을 적용하기로 결정(2019.7.28.)[479]

- 케냐의 정보통신기술부 장관 Joe Mucheru는 농산물의 유통과정을 추적하기 위해 블록체인과 같은 첨단기술을 사용하기로 했다고 발표
- Mucheru 장관은 음식료 제품의 수확부터 유통과정은 물론, 섭취하기에 위험한 불량 식음료 제품의 유통과정을 추적하기 위해 분산원장 기술에 기초한 블록체인 기술과 인공지능 추적 기술을 적용하는 것을 추천하는 것을 주된 내용으로 하는 4차 산업혁명에 대비하기 위한 태스크포스의 보고서를 수령했다고 밝힘
- 이 태스크포스의 의장인 Bitange Ndemo는 블록체인 기술은 농산물과 식료품의 안전성 제고 외에도 헬스케어, 농업, 교육 및 정부 서비스의 질 제고에도 기여하게 될 것이라고 언급함

479 Ronald Njoroge, Kenya to use blockchain to boost food security, Business Report

라. 세네갈

'18년 GDP(십억달러)	24.14
'18년 인구수(천명)	15,854

■ ITU 글로벌 사이버보안 지수(Global Cybersecurity Index, GCI)

· 세네갈의 사이버보안 지수 순위는 2017년에 비해 소폭 하락하여 우리나라와의 격차 심화

국가명	2018		2017		전년대비 증감	
	지수	순위	지수	순위	지수	순위
세네갈	0.305	102	0.314	89	-0.009	-13
대한민국	0.873	15	0.782	13	+0.091	-2

■ ICT 관련 주요 지수

· 세네갈의 전반적인 ICT 발전 수준은 ITU 조사국 175개국 중 하위권에 속해 있음

지표명	세네갈		한국	
	점수	순위	점수	순위
IMD 국가경쟁력지수(2019)	-	-	-	28
IMD 디지털경쟁력지수(2019)	-	-	-	10
UNCTAD 전자상거래지수(2019)	42.7	108	89.4	19
ITU 글로벌 사이버보안 지수(GCI 2018)	0.305	102	0.873	15
UN 전자정부 지수(2018)	0.349	150	0.901	3

■ ICT 관련 주요 통계(ITU, 2018년 말 기준)

· 세네갈은 유선통신 및 이동통신 보급률, 인터넷 이용률 등에서 낮은 활용성을 보임

항목	세네갈		한국	
	가입자수(천 명)	보급률(%)	가입자수(천 명)	보급률(%)
유선전화	302	1.91	25.906	50.63
유선브로드밴드	130	0.82	21,286	41.60
이동통신	16,560	104.45	66,356	129.67
인터넷 이용률	46%(2017년 말 기준)		95.90%	

정보보호 산업 개요

1) 보안 환경

▶ 2018년 ITU 발표에 따르면, 세네갈은 GCI(Global Cybersecurity Index) 0.305를 기록함으로써 아프리카 국가 내에서 16위, 전 세계에서 106위를 차지함

▶ 세네갈의 국가적 사이버 보안 환경은, ▲사이버 보안 관리 체계적 구조 부재 ▲국가 사이버 보안 전략에 대한 공식 문서의 부재 ▲사이버 보안 사건을 관리하는 기관의 부족 등의 취약한 환경을 가지고 있음

▶ 타 아프리카 국가와 마찬가지로 세네갈 내 사이버 공격 및 사이버 범죄도 날로 증가하는 추세

- 다크웹을 통한 조직범죄, 멀웨어 및 고도의 사이버 공격으로 인해 정부 기관, 민간 기업, 개인의 정보 시스템 및 네트워크가 심각한 피해를 입고 있으며, 디도스 공격 및 랜섬웨어의 공격도 심화되는 추세
- 이러한 조직적인 사이버 범죄 외에도 모바일 사칭 및 사기 범죄에 많은 개인과 기관들이 노출되어 있음
- 또한 세계적으로 IoT기술의 발전에 따른 보안 위협은 경제, 사회적 디지털화를 국가적 목표로 삼은 세네갈에게도 취약점으로 작용할 수 있음

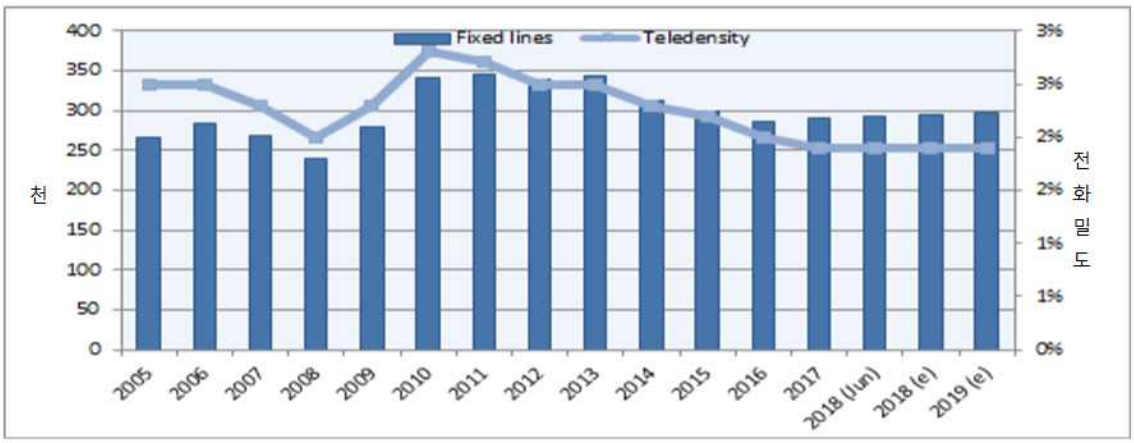
2) 인터넷 및 통신 환경

▶ 유선통신

- 2018년 기준 세네갈의 유선전화 가입회선 수는 2017년 대비 1.2% 증가한 294,100 회선(전화 밀도 1.9%)을 기록함

그림 _ 세네갈 유선전화 가입회선 수 및 전화 밀도 추이 (2005~2019)

(단위: 천, %)



[출처] BuddeComm based on ITU, ARTP, company and industry data, 2019.3

▶ 브로드밴드

- 2018년 기준 세네갈의 브로드밴드 가입회선 수는 2017년 대비 5.4% 증가한 117,807 회선(보급률 0.8%)을 기록함

그림 _ 세네갈 유선 브로드밴드 가입자 및 보급률 추이 (2014~2018)

(단위: 명, %)

연도	가입자	보급률
2014	103,360	0.7%
2015	100,610	0.7%
2016	98,353	0.6%
2017	111,795	0.7%
2018(e)	117,807	0.8%

[출처] BuddeComm based on ARTP data, 2019.3

▶ 이동통신

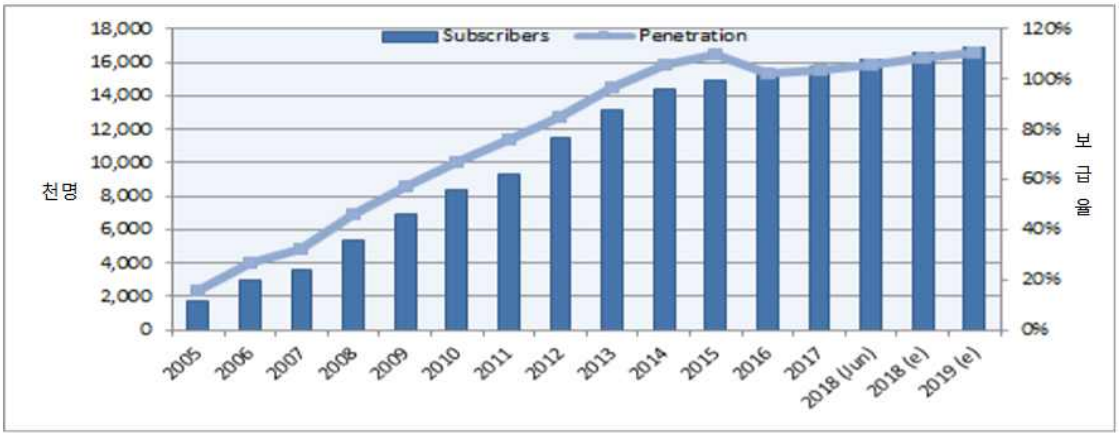
- 2018년 기준 세네갈의 이동통신 가입자 수는 2017년 대비 4.88% 증가해 약 1,635만 명(보급률 108.3%)를 기록
- 이동통신 보급률은 2017년 103.3%에서 2018년 108.3%로 증가하는 등 연평균 성장률 4.9%로 모바일 시장은 꾸준히 성장하고 있음
- 사업자별 2018년 모바일 가입자 수에 따른 점유율은, Orange Group의 로컬 법인인 Sonatel이 53.8%로 지속적으로 시장을 독점하고 있으며, Tigo Senegal과 Sudatel의 로컬 법인인 Express가 각각 23.

8%와 22.4%의 시장 점유율을 차지하고 있음

- Sonatel은 2016년 6월 LTE 라이센스를 획득함으로써 2018년까지 50%의 인구, 5년 후에는 70%, 10년 후에는 90%의 인구에 LTE를 제공해야 하며, 5G 시장은 아직 열리지 않고 있음

그림 _ 세네갈 이동통신 가입자 수 및 보급률 추이 (2005~2019)

(단위: 천명,%)



[출처] BuddeComm based on ITU, ARTP and industry data, 2019.3

정보보호 시장 현황

1) 정보보호 시장 규모

시장 개요

▶ 2018년 4월 IT 서비스 및 컨설팅 회사인 Serianu가 발표한 보고서에 따르면, 아프리카의 사이버 범죄로 인한 손실이 전년도 20억 달러에서 35억 달러로 증가
- 아프리카 전체의 공공 및 민간 조직의 95% 이상이 사이버 보안 조치에 연간 1,500 달러 미만을 지출했으며 특히 중소기업은 보안 투자에 실패함

▶ 세네갈 기업들은 자신들과 관련된 사이버 보안 문제를 거의 공유하지 않음
- 일반 대중에게 법적 조치를 취했거나 매체가 알고 있는 경우에는 정보를 공유하는 사례도 있음
- 2017년 랜섬웨어인 WannaCry 공격으로 인해, 세네갈은 첫 번째 사례가 탐지된 후 4시간 동안 영향을 받았으며, 이는 정보 공유 속도가 느린 이유로 인해 피해가 컸음

▶ 세네갈은 공공 치안 문제로 인해 사설보안이 차지하는 비중이 매우 높은 국가로서, 물리보안 시장의 경우 정확한 통계를 통한 분석이 어려움
- 세네갈 내 치안불안으로 인해 경비, 재화 이동시 에스코트, 근접경호, 원격 감시, 접근 통제 및 화재 보안 경보 등의 서비스를 제공하는 사설보안업체가 늘어나고 있는 추세이며, 2016년 현재 약 400여개 정도 있는 것으로 파악됨

▶ 세네갈 정부는 지속적으로 ICT 분야의 발전을 위한 다양한 정책을 추진하고 있으며, 이로 인해 사이버 보안 시장의 성장도 기대됨
- 2016년 세네갈 정부는 2025년까지 디지털 분야의 GDP 기여율을 10%로 끌어올린다는 목표로 ICT산업 진흥, 국토 디지털 정비 사업 확대, 법제 개선, 기업, 관공서, 개인의 디지털 네트워크 및 서비스 접근 개선 등을 골자로 하는 '디지털 세네갈 2025 (Sénégal Numérique 2025)'전략을 수립해 25개 개혁(세부 사업 69개)을 단행할 예정
- 이 밖에도 모바일 교육, 서아프리카 최초의 co-working space, 여성의 정보기술 교육프로그램 도입 등 역내 ICT 분야의 선두주자로 자리매김 하고 있음

▶ 세네갈 IT시장은 Microsoft, Cisco, IBM 등의 글로벌 IT 네트워크, 서버 및 솔루션 기업이 진출해 있으며, 현지에서 보안 제품을 생산하는 기업이 부재

- 세네갈은 전문보안 기업이 대리점을 통한 단독 마케팅을 추진하기보다는 기존 진출한 IBM과 같은 글로벌 IT기업과의 제품 협력을 통해 간접 진출하는 방법을 고려

시장 규모 및 성장률

▶ 2017년 기준 세네갈 정보보안 시장 규모는 430만 달러 수준으로 추정

- 시장조사기관 Technavio의 2015년 자료[480]를 활용해, 2017년 시장 규모를 추계 하는 회귀식을 구했으며, 이를 2017년 변수에 적용하는 방법을 취해 430만 달러 규모를 도출[481]

▶ 세네갈의 CCTV 수입 시장규모는 뚜렷한 성장이나 감소세가 나타나지 않고 있으며, 2016년 기준 57.8만 달러 규모로 나타남[482]

- 프랑스 식민 국가였던 세네갈에서는 한국의 물리보안 제품 수출은 거의 미미한 수준
- 물리보안 제품은 중국이나 프랑스 제품이 주종을 이룸

표 _ 세네갈 CCTV 수입현황 및 한국의 점유율 (2015 vs 2016)

(단위: 천 달러)

구분	2015	2016	증가율
수입액	900	578	-35.8%
한국의 점유율	0.03%	0.00%	-

주) HS 852580 Television cameras, digital cameras and video camera recorders

[출처] UN Comtrade DB

2) 주요 사업자 현황

480 Technavio, Global Information Security Products and Services Market 2015-2019(2015)

481 GDP와 인구규모를 독립변수로 다중회귀분석을 실시. 계수의 p값이 낮은 GDP 데이터를 활용했으며, 국가별 GDP 편차가 크게 나타나 LOG값을 취하여 다중회귀분석을 재실시하여 추정의 정확도를 제고함. 데이터가 있는 22개 국가의 시장규모와 GDP에 기울기인 1.09544492562193를 곱해서 산출했으며, Y절편인 -0.668571234를 계산하여 세네갈 등 데이터가 없는 8개 국가의 GDP에 곱해서 추정

482 UN Comtrade DB (2017)

시장 특성 및 경쟁 강도

▶ 사이버 보안 문제에 대한 일반적인 인식이 여전히 낮으므로, 사이버 보안 시장은 아직 완전히 개발되지 않고 있음
- 세네갈은 국내에서 생산되는 사이버 보안 제품이 없으며, 글로벌 기업의 보안 제품을 사용하는 실정
- 세네갈에서 사용되는 바이러스 백신에는 Kaspersky Lab, McAfee, Panda, Trend Micro 등의 글로벌 기업의 제품이 주를 이루고 있음

▶ 이 밖에도 Abus, SPB securite privee, Axis 등의 유럽 기업뿐 아니라 ZKTeco, Hikvision, Dahua Technology(중국), Nec Xon(일본) 등의 아시아 기업 다수 진출하고 있는 상황임

주요 사업자

▶ Sagam securite Senegal
- 세네갈 및 서아프리카에서 활동하는 Sagam International 그룹사의 보안 부문 법인으로 화재 경보, 원격 경보 시스템 등 전자 보안 제품이나 현금 수송 등의 서비스를 제공
- 홈페이지 :http://sagam-intl.com/le-groupe-sagam/filiales/sagam-securite/sagam-securite-senegal/
- 전화번호 : (+221) 33-859-74-00
- 이메일 :sagam@sagam.sn

▶ Sentrust
- 2013년에 설립된 세네갈 기업으로 행정기관, 공식 기관 및 기업 대상 전자서명, 디지털 인증서, 데이터 인증 등의 서비스 제공
- 홈페이지 : https://sentrust.sn/
- 전화번호 :(+221)-33-865-24-04
- 이메일 : sentrust@sentrust.sn

▶ Visiocontact
- 영상 감시, 보안 장치 공급업체로 Polycom의 우수협력업체로 지정됨
- 홈페이지 : http://www.visiocontact.sn/
- 전화번호 :(+221) 33-867-43-42

▶ Comtel Ingenierie

- 출입 제어, IP 및 아날로그 비디오 감시, 화재 및 보안 경보, 보안 신원 확인 등
- 홈페이지 : https://www.comtelingenierie.com/
- 전화번호 : (+221) 33- 867-15-15
- 이메일 : contact@comtelingenierie.com

▶ La Colombe Groupe

- 데이터 센터, 사이버 보안, 원격 감시 서비스 제공
- 홈페이지 : https://colombegroup.com/
- 전화번호 : (+221) 33-821-81-81
- 이메일 : contact@colombegroup.com

정보보호 정책 및 기관 현황

1) 관련 법령 및 정책

관련 법령 및 규제

▶ 세네갈의 법률 및 규제 프레임 워크는 초기 단계와 확립된 성숙 단계 사이에 있는 것으로 확인
- 세네갈은 2008년 사이버 보안을 다루는 광범위한 법률을 채택했으나, 이 후 사이버 보안 환경의 변화를 반영하여 법률이 개정된 것은 없음
- ▲정보 사회에 관한 오리엔테이션 법에 관한 법률 No. 2008-10 ▲전자 거래에 관한 법률 No. 2008-08 ▲암호에 관한 법률 No. 2008-41은 국가 ICT 보안을 위한 틀을 구축하며, 이는 안전한 e-commerce, 전자 거래 및 암호 서비스 제공에 대한 법률적 근거가 됨
- 개인 정보 보호위원회(CDP)를 통해 시행되는 개인 데이터 보호에 관한 법률 No. 2008-12에 의해 데이터 보호 및 온라인 개인 정보 보호 제공
- 사이버 범죄의 실질적이고 절차적인 측면은 사이버 범죄에 관한 법률 No. 2008-11에 의해 보호되나 이 법적 체계는 충분한 다양성을 갖추고 있지 않음

▶ 세네갈은 2008년 정보보안 법률(Data protection Act)을 제정
- 동 법과 시행령은 데이터 처리, 데이터 관련 개인의 권리, 데이터 보유자의 의무, 세네갈 정보 보호 당국(Data Protection Authority)의 설립 등을 주요 내용으로 함

▶ 법 집행 기관은 특히 사이버 범죄에 대한 특수 여단을 통해 컴퓨터 관련 범죄를 조사할 수 있는 능력이 있음
- 그러나 모든 법 집행관이 적절한 전문 교육을 받을 수 있는 것은 아니며, 조사 기능이 제한적임
- 검찰과 판사는 일반적으로 적절한 훈련을 받지 않았으며, 컴퓨터 관련 범죄를 기소하고 감리할 능력이 떨어짐

주요 전략 및 정책

▶ 국가 정보보호정책에 관한 대통령 지시(Politique de Securite des Systemes d'Information de l'Etat du

Senegal, PSSI-ES) [483]

- 국가의 ICT기술 활용 증가에 따라 정보 시스템의 보호 문제가 대두되면서 국가의 정보 시스템을 최적의 보안 상태로 유지하기 위해 적용할 원칙과 규칙을 규정하기 위해 2017년 1월 동 지시가 공포됨
- 동 정책은 국가기관 직원의 정보 보안 인식 제고, 교육, 모든 정보시스템의 인수 및 개발에 필요한 보안 관련 필수 사항, 정보 단말기 재고 파악 의무 및 도난 및 파손 방지를 비롯한 관리 강화, 데이터센터, 서버실, 장비실 등의 보안 강화, 보안 구역 출입 제한 등을 골자로 함

▶ 디지털 세네갈 전략 2016-2025(Senegal Numerique 2016-2025)[484]

- '디지털 세네갈 2025 전략'은 잠재적 사이버 테러 대비를 위한 필수국가기간시설(Infrastructures Nationales Critiques, INC) 지정, 인터넷침해사고 대응팀(CERT) 구축, 전문조직을 갖춘 군경과 연계한 사이버보안 및 사이버국방 전략 수립 등 사이버 보안 관련 현안들을 국가적 우선순위로 삼고 있음

▶ 세네갈 사이버 보안 국가 전략 2022(Strategie nationale de cybersecurite du senegal, SNC 2022)[485]

: 디지털 인프라를 제어하기 위한 사이버 보안의 거버넌스 및 운영 필요성에 대해 전 세계적으로 조정된 대응의 관점에서 SNC2022를 정의함

- 실제로 세네갈 정부는 동 전략에 설명된 다양한 국가 이니셔티브를 통해 시민의 일상생활에서 ICT의 광범위한 사용을 적극적으로 개발
- 동 전략 개발을 통해 위험을 식별하는 동시에 국가 차원에서 사이버 위험에 사용되는 모든 수단도 식별
- 세네갈 정부는 동 전략을 통해, ▲사이버 보안에 대한 법적 및 제도적 프레임 워크 강화 ▲지역 및 국제 사이버 보안 노력에 대한 적극적 협력 ▲세네갈의 중요한 정보 인프라(ICT)와 정보 시스템 보호 ▲모든 경제 부문에서 사이버 보안 역량과 기술 지식 구축 ▲사이버 보안 문화 홍보의 5가지 전략적 목표를 달성

483 ARTP, Instruction presidentielle relative a la politique de securite des systems d'information de l'Etat du Senegal(PSSI-ES), 2017.01.03
484 Strategie Senegal Numerique 2016-2025, 2016.10
485 Cybersécurité au Sénégal, Enjeux et perspectives 2019

표 _ 세네갈 사이버 보안 국가 전략 2022의 5대 목표 및 주요 계획

목표	내용	주요 계획
사이버 보안 관련 법제 강화	사이버 위협과 사이버범죄에 효과적으로 대응하면서 디지털 전환으로 생긴 새로운 기회가 세네갈 경제의 강점이 되도록 현행법과 규제를 개선	- ICT 분야 현행법 및 규제의 결함 분석 및 사이버 환경 개선 및 사이버 범죄 퇴치에 적합한 법제 마련 - 정보보호 법 및 규제 개선을 통한 국제 표준 준수 - 동 전략 수행을 책임질 사이버보안 전담 국가조직 설치 - 상기 조직 내 국가 CERT/CSIRT 설치 - 사이버 국방 컨트롤 타워 구성 - 국방 및 치안 당국의 권한 증대 및 조사나 증거 수집에 필요한 도구의 효율적 사용 - 사이버보안 관련 표준 제정 및 민간 및 공공부문, 특히 중소기업에서의 표준 도입 촉진
필수정보인프라(IIC) 및 국가정보 시스템 보안	모든 국가 정보시스템 및 네트워크, 필수정보인프라(IIC)는 모든 사이버 사고가 발생하는 동안이나 사후에 정상 작동해야 함	- IIC들의 보안수준 및 취약점에 대한 총체적 현황 조사 - IIC 및 국가 정보시스템 운영 및 소유 주체들이 지켜야 할 절차, 과정 정립 - IIC 및 국가 정보 시스템의 테스트 및 감독 실시 - 모든 위협, 사고, 리스크의 감시, 분석 및 목록 작성과 업데이트 - 사이버 사고 대응 훈련에 사용할 시나리오 및 시뮬레이션 프로그램 고안
사이버보안 문화 촉진	온라인 서비스에 대한 기관 및 개인의 신뢰를 바탕으로 하는 디지털 세네갈을 건설하기 위해 민간 및 공공부문의 사이버 위협에 대한 이해도와 지식 함양	- 경제, 산업 부문 전반에 걸친 사이버 보안 인식 수준 연구 및 수준별 그룹을 위한 인식 제고 프로그램 마련 - 사이버 보안 모범 사례 홍보 - 고위급 공무원 및 민간 부문 이사회 임원 대상 사이버 보안 필수 교육 실시 - 디지털 환경 개선을 통한 디지털 신뢰도 제고를 위해 IPv4에서 IPv6로의 전환 완료
경제 부문 전반에 걸친 사이버 보안 관련 기술 지식 및 역량 강화	혁신적이고 활동적인 ICT 생태계 조성을 위해서는 경쟁력 있는 사이버보안 인적 자원이 필요하므로 관련 교육과정, 경력 개발 장려	- CERT/CSIRT 팀, 법 집행 및 규제 시행 당국의 사이버 보안 역량 및 지식 평가 및 정기 교육 - 민간 및 공공부문 사이버 보안 교육 관련 기본 필수 사항 정립 - 국가 차원의 사이버 보안 정규 교육(중,고등교육) 및 직업 훈련 과정 신설 - 사이버 보안 관련 진로 장려 - 각급 학교의 사이버 보안 교육 과정과 자료의 평가 및 업데이트
사이버 보안을 위한 지역 및 국제적 노력 동참	사이버스페이스의 탈국가적 성격을 감안하여 지역 및 국제 차원의 협력에 적극 동참	- 세네갈의 지역 및 국제 사이버 범죄 퇴치 활동 참여 조직화 - 지역 및 국제 파트너들과 사이버범죄 퇴치를 비롯한 사이버 보안 노력에 대한 협력 강화

[출처] 세네갈 통신우정디지털경제부 홈페이지, 2018.05

2) 담당기관

▶ Information Systems Security and Digits Central Technic Service (STCC-SSI)

- 국가의 모든 주체에 속하는 정보 시스템, 정보 및 인프라에 대한 국가 규제 기관
- ▲긴급하고 중대한 상황에 연루된 대통령, 고위 정부 당국, 공공 기관 및 유기체의 커뮤니케이션 확보 ▲정보 시스템 보안과 관련된 전략적 방향 제안 및 이행 ▲정보 시스템의 보호 수준을 제어하고 평가하여 요구 사항을 분석하고 적절한 보안 솔루션 제안 역할 담당

▶ 세네갈 CIRT

- ITU-IMPACT는 세네갈 CIRT 설립을 위한 평가를 완료했으나 공식적인 CIRT가 설립되지는 않았음. 우정통신부가 국가 CIRT 구축 프로젝트를 진행 중이나 수년째 지연되고 있으며 사이버보안 전략 2022에서 CERT 구축을 2018년 12월까지 완료할 계획

▶ 사이버범죄 대응 특수여단(BSLC, Brigade Spéciale de Lutte contre la Cybercriminalité)

- 2013년 설립된 세네갈의 사이버보안 및 범죄 관련 대응조직으로, 디지털 증거분석 및 테스트, 대외협력 등의 업무 수행
- 주요 임무는 디지털 범죄 수사, 사법기관 기술지원, 국방 및 보안기관의 훈련 참여, 사이버범죄 대응 조직과 협업 등임

▶ 개인정보보호위원회(Commission de protection des données personnelles, CDP)

- 2008년 1월 25일 제정된 개인정보보호법에 의거해 설립된 독립행정기관으로서 개인 정보의 수집, 사용, 전송 및 파일의 적법성 검토를 담당

▶ 국가정보기술국(Agence de l'information de l'Etat, ADIE)

- 2004년 행정절차 디지털화, 전자정부 전략, 네트워크 인프라 건설, 통신 및 정보기술 발전을 위한 법제 및 규제 실시 연계 등 담당

3) 규제 및 인증제도

▶ 세네갈 정부 차원의 인증 시스템 부재

- 세네갈 정부는 공식 승인된 인증을 위한 국가(특화된 분야 포함) 사이버 보안 프레임과 국가차원의 에이전시 또는 공적부분의 전문가 시스템을 보유하고 있지 않음
- 다만, ICT와 관련하여 ARTP라는 모든 유무선 통신기기 및 네트워크기기(Radio and Tele-communcations Terminal Equipment)에 대한 강제 통신 인증 제도를 운영

▶ 세네갈 정부 차원의 보안 표준 부재
- 세네갈 정부는 보안 표준을 위한 공식적으로 승인된 인증을 위한 국가(특화된 분야 포함) 사이버 보안 프레임을 보유하고 있지 않음

4) 최근 정책 동향 및 이슈

▶ 2018년 11월 아프리카 사이버 보안 학교 개설
- 세네갈 수도 다카르에 설립된 아프리카 최초의 사이버 보안 국립 학교로서, 사이버 보안 전문가 양성 등을 통한 아프리카에서의 허브 역할 수행
- 아프리카 국가의 보안 전문가에게 사이버 범죄에 대응하고, 프랑스와 아프리카 간의 보안 및 방어에 대한 협력을 향상시킬 수 있는 향상된 기능을 제공
- 법률 및 거버넌스 문제는 물론 정보 시스템 보안 및 위협 인텔리전스 전략에 중점을 둔 교육 프로그램 진행

▶ 세네갈의 IOT 준비 및 개발 우선순위에 관한 논의를 위한 이해 관계자 워크숍 개최(2018.11)
- 세네갈 IoT 보안 프로젝트를 구성하는 데 사용할 수 있는 주요 문제 및 활동에 대한 다양한 이해 관계자의 의견을 수집
- 논의된 내용은, ▲세네갈의 IoT 보안 ▲우선 순위의 IoT 개발 ▲잠재적 위협 및 과제 ▲연구 초점 문제를 다룸

▶ 2019년 4월 세네갈 정부의 ICT 정책 역량 및 관리·실행 능력 강화 지원을 위한 한국정보화진흥원(NIA)과의 협업 진행
- 세네갈 정부의 의견을 반영해 국가정보보안, 스마트시티, 전자정부, ICT 인력 양성 등 맞춤형 주제를 기반으로 한국의 ICT/전자정부 발전 경험을 세네갈에 전수
- 빅데이터·공공데이터 분석 실습에서 세네갈의 공공데이터를 분석하는 과정을 통해 세네갈 공무원의 정보화 실무 능력 및 전문성 향상을 지원

▶ 세네갈은 금융 서비스 이용자를 위해 사하라 이남 아프리카 최초의 사이버 보안 센터 개소

- 세네갈 정부는 룩셈부르크, 유럽투자은행, 프랑스 사이버 보안 업체인 'Sécurité Suricate'의 투자를 받아 2018년 6월 수도 다카르에 사하라 이남 아프리카 지역 최초의 금융 사이버 보안 센터를 개소함
- 마이크로 파이낸스를 세네갈 경제의 핵심 분야로 삼고 이를 통해 '금융포용(Financial Inclusion)'을 실현하고자 소비자들이 개인 및 금융 정보 유출의 피해를 입지 않도록 예방 및 감시하는 것이 동 센터 설립의 목적임

▶ 세네갈 은행 업무 아웃소싱, 사이버 보안, 원격 감시 기업인 La Colombe Groupe은 일본 정보시스템 통합 및 보안 솔루션 기업인 NEC XON과 합작으로 다카르에 사이버 보안 센터를 설립(2018.09.11.)

5) 정보보호 스타트업 현황

▶ Weego 및 CoinAfrique와 같은 ICT 스타트업은 Microsoft와의 협력을 통해 기술 및 비즈니스를 확장하고 있는 반면, 정보보안에 특화된 스타트업은 없는 것으로 파악

- Weego는 대중교통으로 쉽게 여행 할 수 있도록 설계된 SunuBus라는 공동 대중교통 앱 제공
- CoinAfrique는 신규 및 중고 제품을 위한 무료 분류 플랫폼 제공

융합보안시장 동향

▶ 세네갈의 IoT 준비 및 개발 우선순위에 관한 논의를 위한 이해 관계자 워크숍 개최(2018.11)

- 세네갈 IoT 보안 프로젝트를 구성하는 데 사용할 수 있는 주요 문제 및 활동에 대한 다양한 이해 관계자의 의견을 수집
- 논의된 내용은, ▲세네갈의 IoT 보안 ▲우선 순위의 IoT 개발 ▲잠재적 위협 및 과제 ▲연구 초점 문제를 다룸

▶ 세네갈 통신 업체인 Tigo Senegal은 디지털 시장을 가속화하기 위해 Ericsson과 함께 클라우드를 포함한 전국 네트워크의 현대화 프로젝트 진행(2018.12)

- Ericsson의 클라우드 패킷 코어, 클라우드 데이터 관리 및 정책 솔루션 제공을 통해 새로운 사용자 서비스 도입 추진

▶ 세네갈은 세계에서 블록 체인 기술을 기반으로 한 디지털 통화를 도입한 두 번째 국가로, 2016년 11월 eCFA라는 이름의 디지털 통화 발행

- eCFA는 Banque Régionale de Marchés (BRM)와 eCurrency Mint Limited 의 파트너십에서 비롯되었으며, BRM은 Banque Centrale des Etats de l' Afrique의 전자 화폐 규제에 따라 eCFA를 발행
- eCFA는 블록 체인을 사용하여 거래를 추적하지만 디지털 통화는 중앙 은행 시스템에 의해 규제된다는 점에서 비트 코인과 다르며, 위조 및 허위 거래를 방지하기 위해 투명성 및 암호화 제공

마. 에티오피아

■ ITU 글로벌 사이버보안 지수(Global Cybersecurity Index, GCI)

· 에티오피아 사이버보안 지수는 0.267로 글로벌 99위이며 우리나라보다 매우 뒤처짐

국가명	2018		2017		전년대비 증감	
	지수	순위	지수	순위	지수	순위
에티오피아	0.278	105	0.267	99	+0.011	-6
대한민국	0.873	15	0.782	13	+0.091	-2

■ ICT 관련 주요 지수

· 에티오피아의 전반적인 ICT 발전 수준은 ITU 조사국 175개국 중 하위권에 속해 있음

지표명	에티오피아		한국	
	점수	순위	점수	순위
IMD 국가경쟁력지수(2019)	-	-	-	28
IMD 디지털경쟁력지수(2019)	-	-	-	10
UNCTAD 전자상거래지수(2019)	31.1	140	89.4	19
ITU 글로벌 사이버보안 지수(GCI 2018)	0.278	105	0.873	15
UN 전자정부 지수(2018)	0.346	151	0.901	3

■ ICT 관련 주요 통계(ITU, 2017년 말 기준)

· 에티오피아 유선통신 보급률은 최하위권이나 이동통신 보급률은 상대적으로 높은 편

항목	에티오피아		한국	
	가입자수(천 명)	보급률(%)	가입자수(천 명)	보급률(%)
유선전화	1,181	1.11	26,845	52.54
유선브로드밴드	62	0.06	21,196	41.48
이동통신	39,600	37.22	63,659	124.59
인터넷 이용률	18.62%		95.07%	

정보보호 산업 개요

1) 보안 환경

▶ World Economic Forum의 The Global Information Technology Report 2016에 따르면, 아프리카 국가인 에티오피아의 네트워크 준비지수(NRI, Network readiness index)는 3.1로 전 세계 139개국 중 120위임

- BuddeComm에 따르면, 2018년 기준 에티오피아의 유선 브로드밴드 인터넷 가입회선 수는 2017년 대비 다소 증가한 605,000회선을 기록, 인구 당 보급률 0.5%임
- ITU 자료에 의하면, 2017년 유선전화 가입회선 수는 118만 1천 회선으로 인구 당 보급률 1.11%이고, 이동전화 가입은 2,960만 회선을 기록, 인구 당 보급률 37.22%임

▶ 에티오피아는 아직까지 유선전화 및 브로드밴드 인터넷의 보급률은 미약하나 지난 10년간 10%대의 지속적인 경제성장률에 힘입어 꾸준한 성장이 이루어졌으며, 특히 이동통신 분야는 비약적으로 발전함

- 휴대폰 사용자 수는 2007년 120만 명에서 2017년 6,261만 7천만 명으로 증가함
- 중국 기업 ZTE와 Huawei는 에티오피아 내 4G 네트워크 공사를 완료하였으며 그 결과 2015년부터는 4G 서비스를 아디스아바바에서 개통, 주요 도시(9개주)에서는 3G 서비스 이용 가능

▶ ITU가 2019년 3월 발표한 'Global Cybersecurity Index 2018'에 따르면 에티오피아의 사이버보안 지수는 0.278, 글로벌 순위는 105위, 아프리카권역에서는 18위를 기록하였으며, 2017년 사이버보안지수는 0.267로 글로벌 순위는 98위였음

▶ 에티오피아의 INSA는 에티오피아 회계연도 2018/19의 마지막 9개월 동안 488건의 사이버 공격을 기록했다고 밝힘[486]

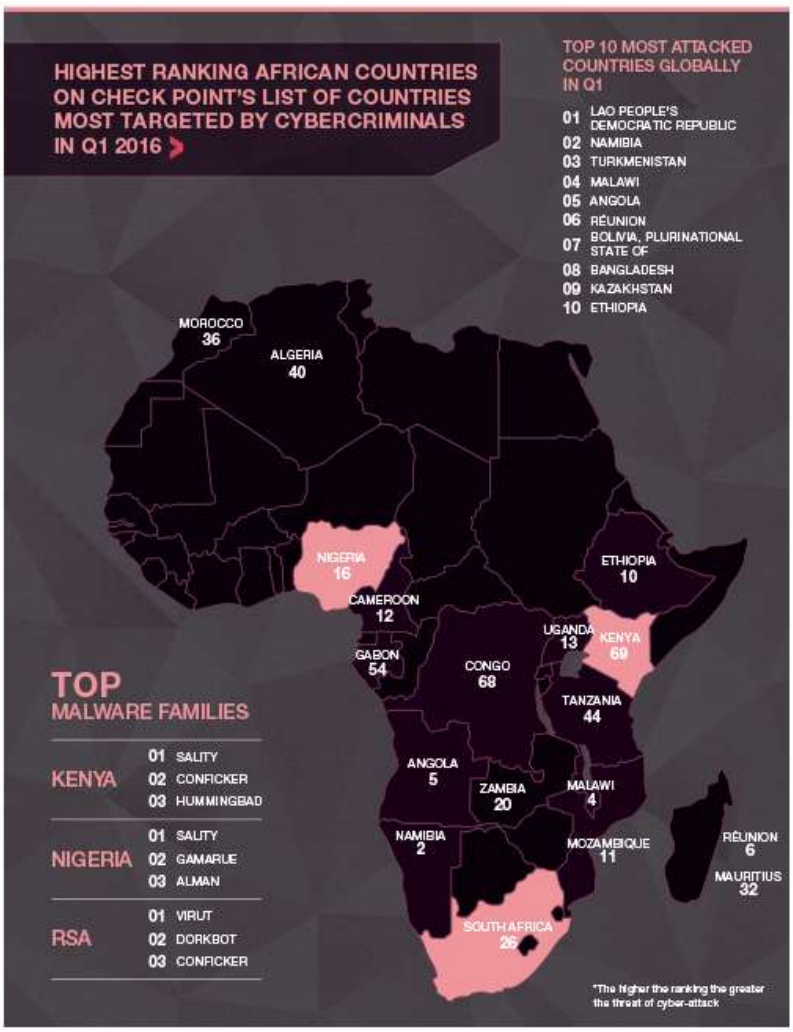
- INSA는 에티오피아에서 가장 많은 수의 사이버 공격은 웹사이트를 겨냥한 것이며 전체 사이버 공격의 약 40%를 차지했으며, 두 번째로 많은 사이버 공격은 주요 인프라 시설을 겨냥한 것이라고 하였으며, 또한 2018/19년 마지막 9개월 동안 사이버 공격의 약 15%가 사이버 해킹 시도라고 밝혔음
- 그러나 INSA는 에티오피아를 겨냥한 대부분의 사이버 공격이 심각한 피해를 입기 전에 막아냈다고 함
- 에티오피아는 현재 사이버 기술을 핵심 구성요서로 사용하여 기존의 기본 서비스 인프라와 정부 행정을 크게 업그레이드 하려고 하고 있으며, 2018년 4월 취임한 현 총리는 INSA의 이전 이사였으며, 모든 공공 및 민간 부문에 사이버 기술을 도입하기 위해 노력을 기울임

---

486 Ethiopia records 488 cyber attacks in 9 months, Xinhua, 2019.5.24.

▶ 이스라엘계 글로벌 보안 기업 Check Point에 따르면, 에티오피아는 아프리카에서 멀웨어 및 보안 위협에 노출된 상위 10개국에 속할 정도로 보안이 취약함

그림 _ 아프리카 멀웨어 및 보안 취약국 (2016. 1분기)



[출처] Check Point, 'Top Malware & Threat Index Q1 2016' (2016.6)

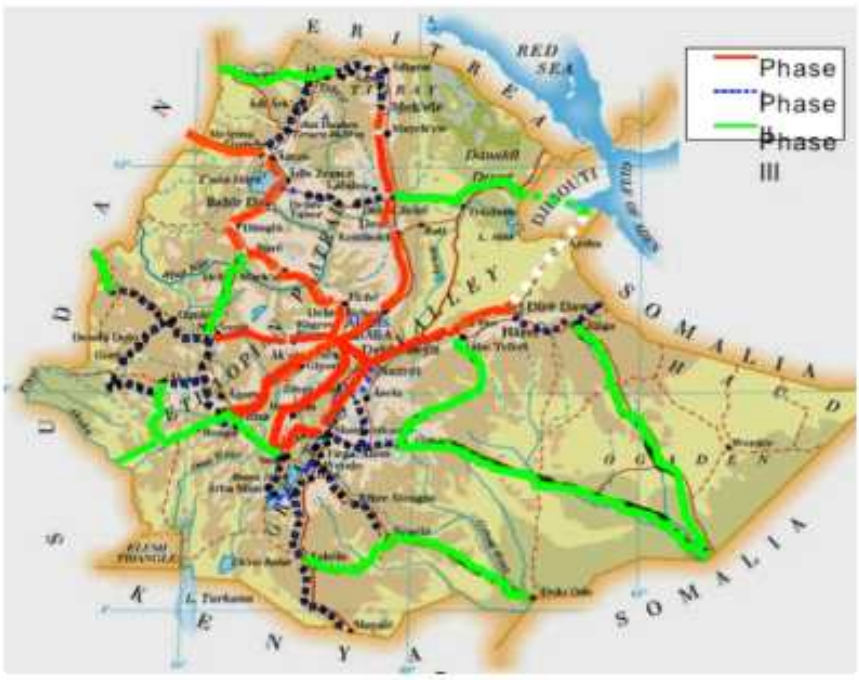
▶ 에티오피아는 1997년 국가 통신정책을 수립, 지속적인 정책 개발에 노력해 2007년 인터넷 정책인 Proclamation No.533 수립, 에티오피아는 ICT분야 발전이 농업중심 사회에서 지식 기반 사회로 나아가기 위한 중요 산업으로 인식, 인프라 구축에 집중함

- ICT 인프라 구축 및 인터넷 접근 향상

▶ 에티오피아는 對아프리카 중국 원조의 최대 수혜국으로 ICT분야에서 다양한 투자를 받음

- Huawei, ZTE가 에티오피아 ICT 산업에 투자했으며 2003년 중국 ZTE사가 GSM 네트워크를 확장(2900만 달러)하면서 중국 기업의 투자가 많아짐
- 이후 2006년 핸드폰 라인 확장과 3G기술 확장(약 24억 달러)이 중국 3개사 합작(ZTE, Huawei, CITCC)으로 이뤄지고, 이는 2007년 이후에도 계속됨
- 2013년 중국 수출입 은행의 자금으로 약 1900만 달러 투자
- ZTE는 약 1만 ㎞의 통신망 건설

그림 _ 에티오피아 통신망 현황



[출처] 에티오피아 정보통신부(Ministry of Communication and Information Technology

2) 인터넷 및 통신 환경

▶ 유선통신

- ITU에 의하면 2017년 기준, 유선통신 가입회선 수는 약 118만 1천 회선을 기록, 보급률은 1.11%이며, 전년도 보급률과 같음
- 에티오피아의 유선시장 보급률은 2013년 이후 지속적으로 증가하는 추세를 보이다가 2016년 2017년 보급률이 동일함

그림 _ 에티오피아 유선통신 가입회선 수와 보급률

(단위: 천 회선, %)



[출처] ITU Statistics DB (2019.6)

- 국영통신사인 Ethio Telecom은 유선, 모바일, 인터넷 및 데이터 통신을 포함한 모든 통신 서비스에서 무기한 독점이 허용됨
- 에티오피아 통신 규제 당국(ETA, Ethiopian Telecommunications Authority)은 오랫동안 Ethio Telecom을 부분적으로 민영화 할 계획을 개발하였음
- 2019년 2월 정부는 시장 경쟁을 발전시키고 부문을 개혁하기 위해 새로운 통신 규제 기관 설립 계획을 발표하였으며, 새로운 규제기관 설립은 6월에 승인 되었으며, 통신부문에 대한 수정안은 국제 사업자가 시장에 진입하여 Ethio Telecom과 경쟁하는 능력이 포함됨
- Ethio Telecom은 유선 및 인터넷 서비스를 전국 18,000개 농촌지역의 대부분으로 확장 중임

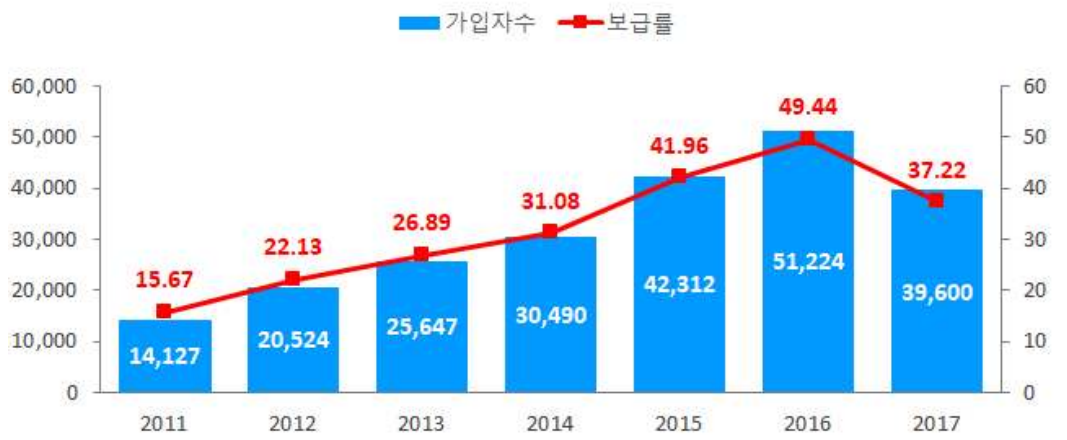
▶ 이동통신

- ITU의 자료에 의하면 2017년 기준 이동통신 가입자 수는 2016년 대비 약 22.7% 감소한 약 3,960만 명으로 보급률은 37.22%임
- 이동통신 보급률은 지속적으로 성장해 왔으나 2017년에는 전년대비 12%이상 감소한 것으로 나타났는데, 이는 2017년 9월 SIM카드 등록으로 Ethio Telecom이 1,800만개의 휴면 모바일 서비스

번호를 되찾았기 때문임

그림 _ 에티오피아 이동통신 가입자수 및 보급률

(단위: 천 명, %)



[출처] ITU Statistics DB (2019.6)

- GSM 서비스는 2009년 3G 서비스에 의해 보완되었으며, LTE 서비스는 2015년 3월에 Addis Ababa에서 제한적으로 출시되었음
- Ethio Telecom은 2013년 말에 종료된 Orange Group과 2011년 관리 계약 이후, France Telecom은 통신확장 프로그램을 지원하였고, 브로드밴드 연결 가격이 수년 동안 과도하게 감소하여 결과적으로 모바일 보급률이 빠르게 증가하여 시장 부문이 개선되기 시작하였음
- Ethio Telecom은 모바일 인프라 개발을 위해 2013년 중반에 Huawei 및 ZTE와 약 16억 달러 규모의 계약을 체결하였으며, 이러한 계약을 통해 2G 및 3G 네트워크를 정밀 점검하고, LTE 서비스는 최근 Addis Ababa에서 시작됨
- 2014년 12월 Ericsson은 ZTE와 계약한 6개 영역 중 4개 영역에 계약을 하여 Ethio Telecom의 CDMA 네트워크는 기본 인터넷 서비스를 지원하는 3G 기술인 EV-DO로 업그레이드 되었음
- Huawei는 중국 철도 그룹이 2015년 1월 완공한 Addis Ababa 경전철 프로젝트에 LTE 인프라를 제공하기 위해 계약을 체결하여 에티오피아 정부는 4억 7,500만 달러를 투자함
- 정보통신정책연구원 자료[487]에 따르면, 2018년 4월 기준 Ethio Telecom은 6,200만 이통통신 회선 용량을 보유하고 있으며, 3G 가입자의 비중은 약 35%이며, 4G LTE는 수도 Addis Ababa에만 40만 회선 용량 보유하고 있으며, 5G는 장기 계획으로 2018년 4월 기준 구체적인 전략이 없으며, 3G와

487 이종화 외, 2018 개도국 정보통신방송 정책자문, 정보통신정책연구원, 정책자료 18-16-01, 2018.12.

4G 확장 계획을 하고 있음

▶ 인터넷 이용 환경

- ITU의 자료에 따르면 에티오피아의 인터넷을 이용하는 개인의 비율은 2017년 18.62%로 전년의 15.37%에서 3.25% 증가하였음

그림 _ 에티오피아 인터넷을 이용하는 개인의 비율



[출처] ITU Statistics DB(2019.6)

- BuddeComm의 자료에 의하면 전체 인구에 대한 모바일 브로드밴드 보급률은 2018년 추정치는 9.7%이며, 전체 인구에 대한 유선 브로드밴드 보급률은 2018년 추청치는 0.5%에 해당함[488]

표 _ 에티오피아 브로드밴드 보급률(2018년 기준)

구분	이용자 수	보급률
모바일 브로드밴드	9,900,000	9.7%
유선 브로드밴드	605,000	0.5%
전체	**10,505,000**	-

주석: 데이터는 2018년 추정치에 해당함

[출처] BuddeComm(2019.6.)

- 3G 모바일 브로드밴드 기술 및 국가 광섬유 백본을 포함한 고정무선 및 모바일 네트워크 인프라에 대한 거대한 투자에도 불구하고, 매우 낮은 유선 연결은 인터넷 부문의 개발에도 영향을 미침
- 인터넷 서비스 제공업체(ISP) 시장에도 경쟁이 도입되어 2018년 중반 Ethio Telecom은 현지 회사가

488 BuddeComm, Ethiopia – Telecoms, Mobile and Broadband - Statistics and Analyses, 2019.6.18

네트워크를 통해 가상 ISP로서 인터넷 서비스를 제공할 수 있게 하여 전국 인터넷 사용자 수는 더욱 증가할 것으로 기대

- 그러나 외국 통신사는 부가서비스(VAS, Value Added Services) 제공업체로서 에티오피아 시장에 진입할 수 있어 이러한 독점적 통제는 혁신을 저해하고, 인프라 확장을 지연시킴
- Vodacom과 같은 통신사는 에티오피아 통신 시장이 자유화 되면 시장을 활용하고자 수도에 사무소를 개설하고 VAS 라이선스를 갖고 있으며, 남아프리카 공화국의 MTN도 VAS 라이선스를 갖고 있음
- 인터넷 접속 요금이 높음에도 불구하고 도시의 인터넷 카페에 대한 수요가 매우 높으며, 수도에는 약 200개의 인터넷 카페가 있으며, Ethio Telecom은 다른 도시에도 최소 8개의 자체 인터넷 카페를 오픈했음

▶ 전자상거래 및 결제시장 전문 조사기관 yStats에 의하면[489] 에티오피아는 2017년 기준 금융 기관의 계정 소유 보급률은 35%, 직불 카드 소유 보급률은 4%로 나타남

▶ 에티오피아는 신용카드사용이 높지 않고 국민 대다수가 은행계좌를 보유하지 않아 상거래 시 현금이 필수적이나 2015년 이후 모바일 계좌 및 모바일 머니 활성화가 진행 중

- 아일랜드 기업인 MOSS ICT는 2015년 M-Birr의 런칭 이후 M-Birr를 이용할 수 있는 7천개소를 통해 120만 명의 사용자를 확보하며 국가적인 네트워크를 구성함
- MOSS ICT는 2천 260만 명의 가입자를 확보한 Kenya M-Pesa와 같이 M-Birr (Birr는 에티오피아 통화)를 확대하기 위한 노력 중
- 에티오피아는 단지 10%의 국민만이 은행 계좌를 보유하고 있으며 1,500 ATM 기기와 2,200개의 은행 지점이 존재함

489 "Africa B2C E-Commerce & Online Payment Market 2019", yStats, 2019.6.24.

정보보호 시장 현황

1) 시장 규모

시장 개요

▶ 2017년 기준 에티오피아 정보보안 시장 규모는 2,410만 달러 수준으로 추정

- 시장조사기관 Technavio의 2015년 자료[490]를 활용해, 2017년 시장 규모를 추계 하는 회귀식을 구했으며, 이를 2017년 변수에 적용하는 방법을 취해 2,410만 달러 규모를 도출[491]

▶ 에티오피아의 CCTV 카메라 수입 시장규모는 2016년 기준 436만 달러 규모였으며, 영상 전화기 수입 시장규모는 1억 4,031만 달러였음

- 주요 물리보안 제품은 거의 대부분 수입에 의존하고 있는 가운데 우리나라의 비중은 그리 높지 않은 상황

표 _ 에티오피아의 주요 물리보안 제품 수입현황 및 한국의 점유율 (2016)

(단위: 천 달러)

구분	CCTV 카메라 (HS852580)	DVR (HS847150)	디지털 도어록 (HS830140)	영상 전화기 (HS851769)
수입액	4,364	6,327	8,227	140,305
한국의 점유율	1.67%	0.08%	0.36%	0.08%

[출처] UN Comtrade DB (2017)

▶ 시장조사기관 6Wresearch에 따르면,[492] 에티오피아의 비디오 감시 시스템 시장이 2019년~2025년에 증가할 것으로 예상하며, 이는 외국인 투자 급증으로 산업, 제조, 운송 및 전략 유틸리티 분야의 건설 프로젝트가 증가함에 따라 이루어짐

- 에티오피아 수도인 Addis Ababa의 건설 프로젝트 증가로 인해 안전 및 보안 목적으로 상업 및 사무실

490 Technavio, Global Information Security Products and Services Market 2015-2019(2015)
491 GDP와 인구규모를 독립변수로 다중회귀분석을 실시. 계수의 p값이 낮은 GDP 데이터를 활용했으며, 국가별 GDP 편차가 크게 나타나 LOG값을 취하여 다중회귀분석을 재실시하여 추정의 정확도를 제고함. 데이터가 있는 22개 국가의 시장규모와 GDP에 기울기인 1.09544492562193를 곱해서 산출했으며, Y절편인 -0.668571234를 계산하여 세네갈 등 데이터가 없는 8개 국가의 GDP에 곱해서 추정
492 Ethiopia Video Surveillance System Market (2019-2025), 6Wresearch, 2019. 9.

공간에 감시카메라의 설치가 증가할 것임

- 예를 들어 중국의 건설 대기업인 CSCEC(China State Construction Engineering Corporation)이 Addis Ababa의 최고층 빌딩(52층 건물)으로 건설 중인 Commercial Bank of Ethiopia은 2015년 시작되어 2020년 11월에 완공될 예정이며, 2019년 완공 예정인 해상 해운 엔터프라이즈 본부(Martitime Transit Shipping Enterprise Headquarters) 건설 등이 있음
- 또한 제조 및 산업부문에서도 에티오피아의 비디오 감시 시스템 시장에서 상당한 점유율을 차지할 것으로 예상함
- 구성요소를 기반으로 카메라, 레코더, 비디오 관리 소프트웨어는 향후 몇 년 동안 에티오피아의 비디오 감시 시스템 시장에서 시장을 지배할 것으로 예상함

▶ 에티오피아는 ICT발전지수가 매우 낮지만, 시급성이 높은 분야의 기본적 수요는 존재하는 것으로 파악됨

- 아프리카 정보보호 시장은 시장규모가 작아, 현재까지는 매력적인 시장으로 보기 어려우나, 경쟁강도가 매우 낮아, 시장규모가 빠르게 성장하고 있다는 점을 고려한다면 장기적 관점에서 접근할 수 있는 시장으로 판단됨
- 정보보안 시장은 현재까지는 시장규모가 매우 협소하나, 경쟁이 저조하여, 장기적 관점에서 시장진출의 기회는 풍부할 것으로 판단됨
- 물리보안 시장도 비교적 시장규모가 작으나, 수요가 급증하고 있으며, 중국저가제품과 유럽제품이 경쟁하고 있는 상황임
- 그러나, 최근 에티오피아 건설프로젝트와 금융권에서 보안설비에 대한 수요가 파악되고 있고, 정부의 전략적 투자도 증가하고 있어 한국 기업의 해외진출 기회가 있는 것으로 파악됨

2) 주요 사업자 현황

시장 특성 및 경쟁 강도

▶ 정보보안 시장에서는 IBM, CISCO, Fortinet, Check Point 등 글로벌 보안기업이 활동하고 있는 것으로 보이나 경쟁이 거의 없는 것으로 파악되며, 물리보안시장은 중국 제품이 유럽 제품을 크게 제치고 시장을 잠식 중

주요 사업자

▶ 에티오피아 정보보안 시장에 진출한 정보보안 기업은 명확하지 않으나 정보보안 및 IT분야 글로벌 기업 2~3개사가 활동하고 있는 것으로 짐작할 수 있음

- 일례로, 정보네트워크보안청(INSA) 사이트에는 글로벌 보안 기업인 Kaspersky가 링크되어 있어 해당 사이트를 통해 보안 관련 정보를 제공하고 있는 것으로 보임

▶ Kaspersky는 아프리카에 매니지드 서비스 프로바이더(Managed Service Providers, MSP)를 대상으로 하는 새로운 파트너 프로그램을 개시함

- 동 프로그램은 MSP가 IT보안 서비스에 대한 증가 수요를 해결하기 위한 것으로 중소기업 시장에 새로운 가입자를 유인하기 위한 전략임

▶ 에티오피아 네트워크 및 보안제품 대리점 MKTY는 SOPHOS 및 Cyberoam의 제품을 취급하고 있으며, 중소기업을 위한 UTM(Unified Threat Management)에서 Firewall, CCTV 등 물리보안 및 정보보안에 관한 다양한 제품을 현지에 공급하고 있음을 알 수 있음

그림 _ 에티오피아의 보안제품 대리점이 취급하는 SOPHOS의 제품



[출처] http://www.mktyethiopia.com/mkty/index.php/pages/network_and_security

3) 주요 동향 및 이슈

▶ 에티오피아 정보네트워크보안청(Information Network Security Agency, INSA)은 은행을 위한 통합 사이버 보안 솔루션을 개시했다고 발표함(2016.7)[493]

- 동 시스템은 사이버 공격으로부터 은행을 보호하는데 활용되며, National Bank of Ethiopia(NBE)에 의해 도입됨

4) 정보보호 스타트업 시장 현황

▶ 에티오피아는 디지털 기업가를 모으고, 엔젤 투자자 네트워크를 구축하며, 정부 정책을 개선하고자 하며 아프리카의 스타트업 허브가 되기 위한 야심을 기울임[494]

- 에티오피아는 현재 나이지리아, 케냐, 남아프리카 등에 비해 스타트업 형성, 벤처 캐피털, 엑시트(Exit)의 초점이 된 아프리카 대륙의 기술 우위에 뒤쳐져 있으나 이러한 기술 순위에 합류하기 위해 다양한 노력이 나타남
- Addis Ababa에서 2019년 6월 8일~9일에 열렸던 첫 번째 Startup Ethiopia 행사에 에티오피아의 대부분 스타트업이 참여하였으며, 스타트업체외에도 VC, 인큐베이터 등 다양한 활동이 나타남
- 모빌리티 분야 벤처인 Ride와 ZayRide는 성장 동력을 얻기 시작했으며, ZayRide는 2019년 8월에 Liberia로 사업을 확장
- 결제 분야의 YenePay(www.yenepay.com)는 에티오피아의 현금기반 경제에서 디지털 결제를 구축하기 위해 노력하고 있으며 ZayRide를 포함하여 500개 이상이 이미 등록하였음
- Deamat은 전자 상거래와 농산품 기술을 혼합하여 소비자는 농산물 생산자인 소규모 농민들과 휴대전화를 통해 연결하여 농산물을 구입하기 위해 지불할 수 있음
- 기술 인재 및 스타트업 마켓플레이스인 Gebeya는 전 세계에 지사를 갖고 Addis Ababa에 위치하며, 개발자가 기술을 습득하고 디지털 비즈니스를 확장 할 수 있는 프로그램과 서비스를 벤처 및 기술 전문가에게 제공함
- BlueMoon은 에티오피아의 에그테크(agtech)분야 인큐베이터이며 시드(seed) 펀드를 제공함
- 개발자 및 코워킹 유형의 공간 측면에서 AI 및 로봇 연구회사인 iCog Labs과 에티오피아 최초의 기술 허브 중 하나인 IceAddis가 있음

493 2Merkato.com, "Ethiopia: Integrated Cyber-Security Solution for Banks Started", 2016.7.21
494 Ethiopia's bid to become an African startup hub hinges on connectivity, TechCrunch, 2019.6.21.

- 2011년에 설립된 IceAddis의 미션은 에티오피아의 IT 생태계를 개발하는 것으로, 이 허브는 40개의 벤처들이 졸업한 6개월간의 스타트업 엑셀러레이터 부트캠프인 Ice180과 같은 프로그램을 운영하며, 또한 24시간 코워킹 공간을 제공함
- 아프리카 비즈니스 엔젤 네트워크(African Business Angels Network)가 지원하는 최초의 Addis Ababa Angel Network도 발표되었으며 2019년 스타트업을 받아들일 것임
- Startup Ethiopia 행사에는 또한 실리콘밸리에서 현지 스타트업을 만나기 위해 방문한 Ethiopians in Tech[495]가 있으며, 이는 실리콘밸리 기반을 둔 에티오피아의 기술 및 스타트업 생태계 성장을 지원하는 기업가 지원 그룹임
- 그러나 Startup Ethiopia에서 이틀 동안 테크 이벤트의 Wi-Fi가 제대로 작동하지 않은 것을 배경으로 에티오피아의 스타트업 커뮤니티의 가장 큰 장애물 중 하나는 현지 인터넷 상황임
- 이에 대해 에티오피아의 혁신기술 국무장관과 같이 몇몇 관리들은 내년 안에 인터넷 품질, 접속, 및 선택을 개선하기 위한 구체적인 약속을 하였으며, 정부도 국영 통신사인 Ethio Telecom을 민영화하기로 하며, 2019년 말까지 새로운 통신사에게 라이선스를 발급하는 정책 단계를 발표했음

▶ 작은 규모로 민간에서 스타트업을 육성하고자 하는 움직임이 감지되고 있으며, 비영리 조직인 blueMoon Ethiopia는 스타트업 인큐베이션을 통해 에티오피아의 현실에 부합하는 실질적인 아이디어의 사업화를 지원하고자 노력함[496]

- blueMoon Ethiopia는 1년에 2번 전국 대회를 운영하고, 5~10개 팀 정도의 2~3인으로 구성된 스타트업팀을 Addis Ababa에 기반을 둔 4개월 프로그램에 수용하여, 2월~5월, 8월~11월동안 인큐베이터 프로그램을 수행하며, 스타트업 팀에게 아이디어를 사업화하기 위한 시드 머니(Seed Money)를 투자함[497]
- blueMoon Ethiopia는 에티오피아 선물거래소 CEO 출신인 Eleni Garbre-medhin 박사에 의해 설립되었으며, 매년마다 경쟁을 통해 스타트업 팀을 선정하는데, 입주할 수 있는 팀은 전체 응모팀의 1%에 해당할 정도로 경쟁이 치열함
- 선정된 스타트업 팀의 사업 아이디어는 예를 들면 농업, 낙농업 등 현존하는 산업 바탕으로 시스템 구축을 통한 공정거래 및 생산성 향상을 목표로 함
- 2019년 기준 blueMoon Ethiopia은 MasterCard 재단으로부터 재정적 지원을 받고 있으며, 또한 스타트업에게 기술 교육을 제공하기 위해 기업가정신 개발 센터(Entrepreneurship Development Centre), R&D 그룹, iceAddis, xHub Addis, DOT Ethiopia, UNIDO 등과 같은 프로그램 제공 파트너와 협력하며, 12개월의 집중적인 1:1 멘토링 지원 프로그램을 위해 영국의 Mowgli 재단 및 나이로비와

495 Ethiopians in Tech 홈페이지: www.ethiopiansintech.org
496 김종현, 에티오피아의 우수 스타트업 사례와 시사점, KOTRA 해외시장 뉴스, 2018.9.21
497 Bluemoon Ethiopia 홈페이지: https://www.bluemoonethiopia.com/

제휴함

정보보호 정책 및 기관 현황

1) 관련 법령 및 정책

관련 법령 및 규제

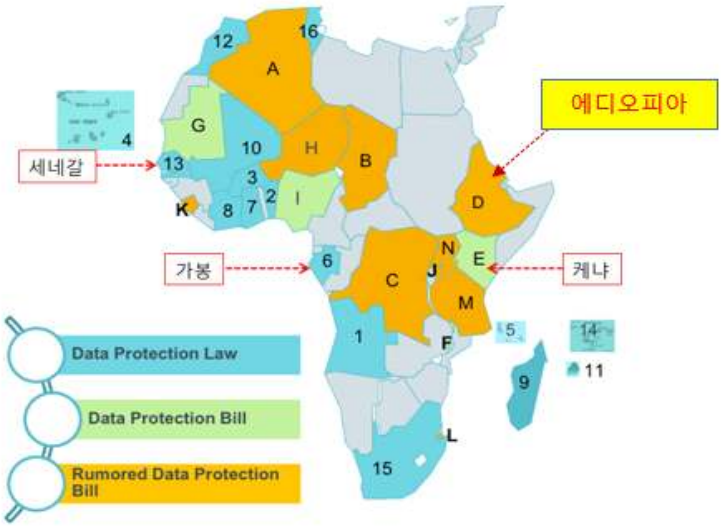
▶ 에티오피아는 1997년 국가 통신정책을 수립, 지속적인 정책 개발에 노력해 2007년 인터넷 정책인 Proclamation No.533 수립하여 에티오피아는 ICT분야 발전이 농업중심 사회에서 지식 기반 사회로 나아가기 위한 중요 산업으로 인식, 인프라 구축에 집중함

- ICT 인프라 구축 및 인터넷 접근 향상
- 인적개발과 ICT 문서 보유
- ICT 법률 시스템 및 보안 시스템 마련
- ICT 산업과 민간부분의 발전
- 데이터베이스 구축 및 자료생산에 ICT 이용

▶ 에티오피아에서는 국가 사이버보안을 위해 다음의 법률을 제정하고 운영하고 있음

- 국가전자거래법 (National Electronic Transaction Law)
- 국가데이터보호법 (National Data Protection Law)
- 전자상거래법 (E-Commerce Law)
- 전자서명법 (E-Signature Law)
- 컴퓨터 오용 및 사이버 범죄관리법(Computer Misuse and Cyber Crime Law)

그림 _ 아프리카 지역 보안 법률 제정 현황



[출처] simmons & simmons(2015.6)

주요 전략 및 정책

▶ 2017년 2월 22일~23일, 에티오피아 INSA가 "Critical Security Requirement Standard"를 발표[498]

- 정부 및 민간의 주요 인프라에 대한 경각심을 고취하기 위한 2일 간의 워크숍에서 INSA는 '사이버 보안 능력을 강화하고 일반 문서 보안 및 IT정보 시스템의 보안 리스크를 관리하기 위해 요구되는 프로세스를 정립해야 한다.'고 강조함
- 또한, INSA는 정부가 사이버 보안 시스템이 작동하기 위해 최소한으로 요구하는 표준을 구현하는 기준도 공개했으며 이를 위해 관련 기업들은 각자의 리더십을 발휘해야 한다고 강조함

▶ 성장 전환 계획(Growth and Transformation Plan II)[499]

- 에티오피아 정부는 5년 단위의 국가 계획인 성장 전환 계획(Growth and Transformation Plan, GTP)을 통해 중소득국으로 진입, 산업별 발전 방향과 목표를 제시하고 각 부처에서는 해당 계획을 바탕으로 세부 추진 계획을 수립해 시행하고 있음
- 정부는 2011년~2015년 동안 수행된 1차 GTP에 따라 통신 부문에서 통신 인프라에 대한 상당한 투자를 통해 접근성을 높이고 통신 서비스의 품질을 향상 시켰음
- 1차 계획 동안 통신 서비스 가입자 수는 2010년 6월 770만 명에서 2015년 6월 3,980만 명으로 증가하였으며, 5km 이내 통신 서비스에 접근 할 수 있는 농촌지역의 비율은 62%에서 97%로 증가했음

498 AllAfrica.com, "Ethiopia: INSA Issues Cybersecurity Standards", 2017.2.23
499 BuddeComm, Ethiopia – Telecoms, Mobile and Broadband - Statistics and Analyses, 2019.6.18

- 2차 계획(2016년~2020년까지)에는 ICT 사용을 가속화하고 산업 및 민간 부문 개발을 위한 통신 서비스를 홍보하기 위한 법적 프레임워크를 개발하며, 정부 행정을 위한 ICT 사용을 확대하기 위한 조치가 포함됨
- 또한 3G 및 LTE 서비스 개발에 중점을 두고 GSM 기술 시장 점유율을 2015년 93%에서 2020년 47%로 줄이는 것을 목표로 함
- 그리고, ICT 부문에서 컴퓨터 사용을 늘리고 ICT 제조 산업을 확장하는 것을 목표로 하며, 모바일, 브로드밴드 및 데이터 서비스의 가입자 수를 늘리는 것을 목표로 함

2) 담당기관

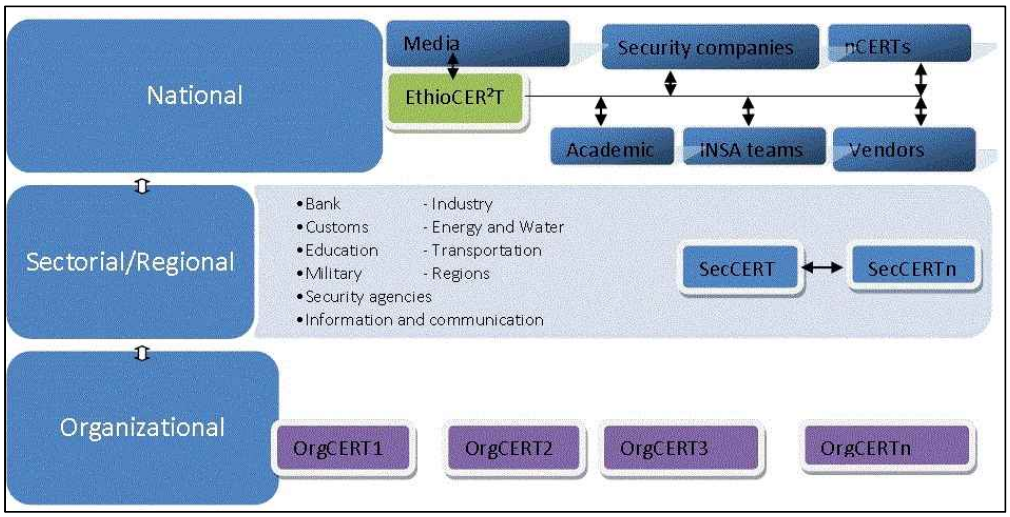
▶ 혁신기술부(Ministry of Innovation Technology, MIT)

- 기존 정보통신부(Ministry of Communication and Information Technology, MCIT)와 과학기술부(Ministry of Science & Technology, MoST)가 2018년 조직 개편을 통해 혁신기술부(Ministry of Innovation Technology, MIT)로 통합됨
- 기존의 정보통신부(MCIT)는 에티오피아의 정보통신 정책을 주관하는 부처로 2010년 설립되었으며, 다음과 같은 주요 이슈들을 위한 정책을 추진함
- 정보통신기술 및 우편서비스에 대한 표준개발 및 승인
- 정보통신분야 표준 구현 모니터링 및 평가
- 정보통신 및 우편서비스분야 지식센터 역할 담당
- ICT분야 국제 행사 참가

▶ 정보네트워크보안청(Information Network Security Agency, INSA)

- 에티오피아 정보통신기술부 산하에 2006년 설립된 정보네트워크보안청이 있으며 동 기관 내부에 에티오피아 침해사고대응팀(Ethiopian Cyber Emergency Readiness and Response Team)이 운영됨

그림 _ 에티오피아 침해사고대응팀(Ethio-CERT) 운영체계



▶ 에티오피아 침해사고대응팀(Ethiopian Cyber Emergency Readiness and Response Team)에서는 기관의 업무를 다음과 같이 규정하고 있음

- 정보통신기술 및 우편서비스에 대한 표준개발 및 승인

표 _ 에티오피아 침해사고대응팀(Ethio-CERT) 기관 업무

구분	세부 내용
국가 사이버보안 모니터링	• 시스템을 활용한 사이버 범죄 파악 • 사이버 공격 제보 수집 / 사이버 공격 데이터 수집 • 위험 기관 정보 제공
사이버보안 연구 분석	• 멀웨어, 해킹 연구분석 주관 • 사이버 공격 조사 지휘 • 사이버 범죄 트렌드 파악 및 예측 • 사이버 보안 준비 • 국가 통계 조사
사이버범죄 사전대비	• 리스크 및 취약성 평가 주관 • 정보보안 제품 품질 검증 • 정보보안 전문인력 역량 검증 • 정보보안 정책 및 수행 검증 • 기술 동향 모니터링 및 인력 교육
사고 대응	• 취약성 보완 / 복구 지휘 • 사이버 공격 시 사업 연속성 확인
역량강화 및 인증	• 국가차원의 사이버 보안 인지도 강화 • 사이버 공격 관련 교육 제공 • 정보보안 전문인력 교육 • 국제적 수준에 맞춘 조직 역량 강화 • 필요 인프라 배치 • 정책 및 표준 준비
협력	• 팀의식 배양 및 협력 • 미션달성을 위한 충분한 협력 • 국제 협력 관계 구축

3) 규제 및 인증제도

▶ 정부 차원의 인증 시스템 부재

• 에티오피아 정부는 공식적으로 승인된 인증을 위한 국가(특화된 분야 포함) 사이버 보안 프레임과 국가차원의 에이전시 또는 공적부분의 전문가 시스템을 보유하고 있지 않음

4) 최근 정책 동향 및 이슈

▶ 에티오피아 대통령은 2020년 7월말 이전에 2개의 민간 회사가 통신 산업 부문에서 영업허가를 받을 것이라고 함(2019.10)[500]

- 현재 국영 통신사인 Ethio Telecom은 통신 시장에서 독점권을 갖고 있으며, 1억 이상의 인구 중 4,100만 이상의 고객에게 음성, SMS, 데이터 서비스를 제공하는 유일한 회사임
- Safaricom, MTN 그룹, Orange, Vodafone을 포함한 다국적 회사들이 라이선스 입찰에 관심을 보임

▶ 에티오피아의 인터넷이 암살이후 10일만에 복원됨(2019.7)[501]

- 2019년 6월 22일 정부의 고위 공무원이 포함된 6명의 암살로 인해 에티오피아 전국적으로 인터넷 셧다운이 있었으며, 이후 10일만에 인터넷이 Addis Ababa에서부터 복원되며 단계적으로 다른 지역에도 복원됨
- Ethio Telecom은 인터넷이 중단된 동안 사용자가 구매했지만 사용할 수 없는 모든 인터넷 패키지는 상환될 것이라고 함
- 국영 통신사인 Ethio Telecom은 2주 전 전국 학교 시험동안에도 인터넷 접속을 차단했음
- 인터넷 모니터링 그룹인 NetBlocks는 인터넷 차단 동안 에티오피아가 하루에 최소 450만 달러의 손실이 있는 것으로 추정함

▶ Finnovation Ethiopia 2018이 아디스아바바에서 2018년 11월에 개최(2018.10)

- 본 행사에는 정부정책담당, 은행 및 금융권 기업, 통신사, 투자자 및 테크 스타트업 커뮤니티 등이 참석하여 디지털 트랜스포메이션, 모바일 머니, 페이먼트 및 블록체인 등 다양한 ICT 및 관련 금융 기술 및 비즈니스가 논의될 예정

▶ 사이버 시큐리티 아프리카는 에티오피아 아디스아바바에서 '제5회 에티오피아 뱅킹 및 ICT 서밋 2018'을 개최함(2018.4)

- 본 행사에는 에티오피아 여러 은행의 ICT 분야 및 관련 비즈니스 전문가들이 참석했으며, 아프리카 20개국에서 뱅킹솔루션을 운영하고 있는 Fintech는 은행권 ICT솔루션을 소개함
- 또한 ATM 기기 사기로 인해 발생하는 분쟁을 해결하기 위한 방안이 Fintech Kenya의 세일즈 및 마케팅 책임자 Polycup Osero에 의해 발표됨

---

500 Ethiopia to give telecoms licences to two firms, BBC News, 2019.10.8.
501 Internet restored in Ethiopia 10 days after assassinations, Federal News Network, 2019.7.2.

5) 정보보호 스타트업 관련 정책동향

▶ 에티오피아 정부는 5년 단위의 GTP(Growth and Transformation Plan)에 산업별 목표 외에 제조업과 중소 규모 기업체 육성 및 경쟁력 강화, 스타트업 지원 등도 포함되어 있어 원대한 목표에도 불구하고 이를 실현할 실질적인 예산지원 및 구체적인 정부의 실행방안 찾아보기 어려운 상황임[502]

▶ UAE는 혁신, 기술을 향상시키기 위해 에티오피아에 1억 달러의 보조금을 제공

- 에티오피아 혁신 기술부(Ministry of Innovation and Technology) 장관은 UAE 정부와 1억 달러 보조금 계약을 2019년 7월 15일 체결하였으며, 칼리파 기업 개발 기금(Khalifa Fund for Enterprise Development)을 통해 제공됨
- 이 기금은 주로 소(micro)기업 및 중소기업 역량을 강화할 것으로 기대되며, 특히 혁신과 기술 분야의 기업에게 강조되어 농기업 및 농가공업, 정보 및 기술 서비스, 에너지 및 제조 부문의 기업이 주로 참여할 것임
- 에티오피아 정부가 개발 야심의 중심에서 혁신을 촉진하기 위해 노력을 감화함에 따라 이번 재정 계약이 체결되었음

502 김종현, 에티오피아의 우수 스타트업 사례와 시사점, KOTRA 해외시장 뉴스, 2018.9.21

융합보안시장 및 정책 동향

1) 융합보안 시장 현황

사물인터넷(IoT)

▶ 2014년 9월 Metal & Engineering Corporation (MetEC)은 에티오피아 전기 유틸리티(Ethiopian Electric Utility, EUU)에 현지에서 제조한 스마트 전기 계량기를 공급하였음

- 중앙에서 제어되는 It-Plus 미터는 전력 소비에 대한 데이터를 제공하며 원격으로 전원을 끌 수 있음

블록체인

▶ 스마트 계약을 위한 블록체인 기반 생태계인 Cardano는 대륙에서 이니셔티브를 주도하기 위해 IOHK의 아프리카 운영 이사인 John O'Connor로 하여금 에티오피아 Addis Abba에 본사를 설립하여 우간다, 케냐 및 남아프리카 공화국으로 확장하고자 함

- 2015년 설립된 IOHK는 블록체인과 암호화폐를 정부 기관, 기업 등을 위해 구축하고자 하며 Cardano, 이더리움 클래식 프로젝트에서 작업하며, 에티오피아의 경우 레거시 시스템과 레거시 인프라가 부족한 국가로 새로운 기술에 더 많은 혜택을 가질 수 있을 것으로 간주함
- IOHK는 에티오피아 정부와 MoU를 2018년 5월 3일에 서명하여 파트너십을 맺고, 주니어 소프트웨어 개발자를 훈련, 채용하고, Cardano를 에티오피아의 농업 분야 산업에 적용하기로 하였음
- IOHK는 에티오피아 농업 기술을 블록체인에 연결하며, 예를 들어 아프리카 최대 커피 생산국인 에티오피아에서 블록체인 기술을 통해 시골 농장에서의 커피 생산부터 도매 구매자에 이르기까지 커피를 추적하는 방법을 탐색하고자 함

핀테크

▶ 전자 지불 솔루션 제공업체 iVeri는 전자 상거래 및 모바일 뱅킹 서비스를 제공하는 최초의 에티오피아 은행인 Dashen Bank에 지불 게이트 및 MiCard 전자 지불 처리 솔루션을 제공함

- Dashen Banks는 에티오피아에서 Visa 및 MasterCard의 주요 회원으로 임명된 최초의 은행 중 하나임
- 계정 소유자는 MiCard를 사용하여 모바일 방송 시간을 늘리고 계정 잔액을 확보하여 SMS를 통해 다른 카드로 송금 할 수 있음

▶ 모바일 뱅킹 서비스 제공업체인 Monitise는 Monitise East Africa 서비스를 2009년 우간다에서 처음 시작하여 에티오피아를 포함한 주변국가로 확장했음

▶ 2015년 초 네델란드에 본사를 둔 BelCash Technology Solution은 2개의 Lion International Bank와 Somali Micro Finance와 제휴하여 에티오피아에서 HelloCash 모바일 머니 서비스를 시작하였음
- 이 서비스를 통해 은행 고객은 모바일 장치를 통해 예금, 인출, 송금 및 지불을 할 수 있으며, HelloCash 시스템은 상호 운용 가능하며 여러 은행과 상호 연결할 수 있음

▶ MOSS ICT도 M-Birr 모바일 머니 서비스를 시작하였으며, 2014년 12월 중앙은행에 의해 라이선스를 받았으며, M-Birr은 처음에 여러 소액 금융 회사에 제공했음

▶ 2018년 7월에 Safaricom과 정부는 현지 은행과 연계하여 Safaricom의 MPesa 모바일 머니 서비스 고려
- M-Pesa 이름은 은행에 라이선스가 부여되지만 서비스는 나이로비의 서버에서 Safaricom에 의해 호스팅되고, Ethio Telecom은 현지 서비스 제공업체가 됨

▶ Finserve Africa는 해외에 사는 약 3백만 명의 에티오피아인의 송금에 중점을 맞추어 여러 에티오피아 은행들과 국경 간 모바일 지급 및 전자상거래 서비스를 구축하는 방안을 모색함
- Finserve Africa는 에티오피아안들이 2017년 약 46억 달러를 송금했다고 밝힘

▶ 모바일 플랫폼 대출업체 Equity Bank는 2019년 에티오피아 시장에 주목하며 시장 진출을 준비함[503]
- 케냐 나이로비에 본부를 둔 Equity Bank는 서비스와 제품을 완전히 디지털화하기 위해 지속적으로 노력하며, 케냐의 이동통신사 Safaricom과 협력을 체결하여 모바일 머니 서비스, 사이버 보안에 대한 기술 등 협업을 추구하기로 함
- 주요 업무로 대출을 주요 업무로 하는 Equity Bank는 모바일 플랫폼(Eazzy App, Equitel)에서 93%의 대출을 처리했으며, 남수단, 콩고민주공화국(DRC)와 같은 동부 중앙 아프리카 국가에 이미 진출하였지만, 에티오피아에는 아직 진출하지 않은 상태인데, 2019년 5월 기준 이미 에티오피아 정부에게 연락하여 에티오피아 시장으로 확장을 준비하고 있음

2) 융합보안 정책 현황

503 Equity Bank Eyes Ethiopia Market, Reports KES 6.2 Billion Pre-tax Profit in Q1, techweez, 2019, 2019.5.9.

스마트시티

▶ 에티오피아 정부는 10년간 프로젝트 비용 최대 30억 달러 규모로 Amhara주의 Bahir Dar에 실제의 와칸다(Wakanda)라는 기술 도시를 건설하기 위해 2018년 8월 Hub City Live와 파트너십을 체결하였으며, ICT 개발에 중점을 두며 8~10후 완공될 것임

- Addis Ababa에서 열린 워크숍에서 Hub City Live는 에티오피아 정부 및 주 정부의 프로젝트 이해관계자들에게 발표하였으며, 이러한 기술 도시는 사람들의 삶을 개선 할 뿐 아니라 청년들의 일자리 창출에도 도움이 될 것으로 기대하며, 또한 다양한 ICT 혁신을 모아 과학기술 분야에 관련된 다양한 기관 및 사람들을 수용할 것임
- 새로운 기술 도시 건설 계획은 2015년 6월 오픈한 에티오피아의 최초의 ICT 파크(ICT Park) 개발에 이어진 계획으로, ICT 파크는 약 200헥타르의 부지에 2년이 걸렸으며, 많은 기술 회사를 수용함

▶ 에티오피아는 볼레 국제공항 근교에 약 200ha의 면적 및 약 2500만 달러 투자로 EthioICT – Village 건설 2015년 6월 완공

- 에티오피아를 아프리카 ICT산업의 허브로 육성시키기 위한 정부의 정책 중 하나
- Business zone, Assembly warehouse zone, commercial zone, Administrative zone, Knowledge part zone의 총 5개 구획으로 구성
- 5년간 세금 면제, ICT 관련 자본재 수입 시 면세, 재정지원 등의 인센티브 제공
- 완공 당시 중국의 ZTE(Zhongxing Telecom Corporation), CNET(Techno Mobile and Security Innovation Network), Smadle, Techno 등 20개 기업 입주 예정
- 기술 발전을 통해 약 30만 개 일자리 창출 예측

바. 지부티

'18년 GDP(십억달러)	1.97
'18년 인구수(천명)	960

■ ITU 글로벌 사이버보안 지수(Global Cybersecurity Index, GCI)

· 지부티의 사이버보안 지수순위는 159위로 전년 대비 하락했으며 최하위권에 속함

국가명	2018		2017		전년대비 증감	
	지수	순위	지수	순위	지수	순위
지부티	0.063	159	0.099	140	-0.036	-19
대한민국	0.873	15	0.782	13	+0.091	-2

■ ICT 관련 주요 지수

· 지부티의 전반적인 ICT 발전 수준은 전 세계 최하위권에 머물고 있음

지표명	지부티		한국	
	점수	순위	점수	순위
IMD 국가경쟁력지수(2019)	-	-	-	28
IMD 디지털경쟁력지수(2019)	-	-	-	10
UNCTAD 전자상거래지수(2019)	28.6	124	89.4	19
ITU 글로벌 사이버보안 지수(GCI 2018)	0.063	159	0.873	15
UN 전자정부 지수(2018)			0.901	3

■ ICT 관련 주요 통계 (ITU, 2018년 말 기준)

· 지부티의 유선통신과 이동통신 보급률 모두 전 세계 최하위권 수준을 보임

항목	지부티		한국	
	가입자수(천 명)	보급률(%)	가입자수(천 명)	보급률(%)
유선전화	37	3.84	25,907	50.63
유선브로드밴드	26	2.66	21,286	41.60
이동통신	395	41.20	66,356	129.67
인터넷 이용률	-		95.90%	

정보보호 산업 개요

1) 보안 환경

▶ 지부티는 1977년 프랑스로부터 독립해 2001년까지 10년간 지속된 두 주요 민족 간 내전, 수도인 지부티에 인구의 2/3이 집중되어 있고 나머지 지역에는 유목민들이 거주하는 등 천연자원, 산업, 인프라가 낙후된 지역[504]

- 이에 지부티 정부는 디지털 경제 발전 촉진을 위한 국가 목표에 맞춰 2014년 ICT 개발을 위한 국가전략(National Strategy for ICT Development)을 포함한 ICT 육성 10개년 계획을 채택해 추진 중
- 지부티는 유럽, 동아프리카, 중동, 동지중해, 남아시아를 잇는 해저 케이블 8개에 연결되어 동아프리카에서 가장 많은 국제 연결 케이블을 가진 국가로, 'Vision 2035'라는 계획에 따라 지역 내 디지털 강국으로 거듭나기 위한 목표를 세움

▶ 2014년 수도 지부티의 한 레스토랑에서 폭탄테러가 발생하는 등, 인근 예멘과 소말리아에서 이슬람 테러조직, 소말리아 해적들의 활동 방지를 위해 미국, 프랑스, EU, 일본 등의 군 병력 7,000여명이 주둔하고 있는 데다 정부의 강력한 경찰력으로 치안상황이 비교적 안정적[505]

- 그러나 높은 실업률과 소말리아, 에티오피아, 예멘 피난민들에 의한 범죄 발생 가능성이 높아 지부티 거주 외국인들은 주거지역내 절도 방지를 위해 사설 경비를 고용하고 있는 실정

▶ 지부티의 2017 ITU 글로벌 사이버보안 지수(GCI)는 0.99로 140위를 차지했으나 2018년 0.063으로 아랍지역국가[506] 중 20위, 글로벌 순위는 159위를 기록하면서 큰 폭으로 하락

- ITU의 2019년 자료에 의하면 전체 인구 대비 인터넷 사용자의 비율이 56%로 모로코(62%), 세이셸(59%), 카보베르데(57%), 남아프리카공화국(56%)과 함께 아프리카 지역 상위 10개국 내에 오르며 인터넷 사용이 증가 추세[507]
- 국가정보보호국(ANSIE)가 현재 국가 차원의 사이버보안전략을 마련하기 위한 초기 논의 단계에 있으며, 사이버보안 관련 법제를 개선할 방침

▶ UN무역개발회의(UNCTAD)에서 발표한 2017 B2C 전자상거래 지수(B2C E-commerce Index)는 18로

504 Telecoms, Mobile and Broadband – Statistics and Analyses Buddecom, 2019.03.05
505 http://www.0404.go.kr/dev/country_view.mofa?idx=191
506 지부티는 ITU의 GCI 보고서에서 지역적으로 아랍권(Arab States region)으로 분류되어 있음
507 https://www.lanation.dj/internet-djibouti-au-top-10-des-pays-les-plus-connectes-dafrique/

2016년에 비해 다소 하락했으며 144개국 중 126위를 차지[508]

표 _ UNCTAD B2C 전자상거래 지수 및 순위 비교(2017)

구분	인터넷 사용률 (2016)	15세 이상 인구 결제계좌 보유율 (2014 또는 최신)	인구 100만 명당 암호화 인터넷 서버 개수(2016)	만국우편연합(UPU) 우체국 신뢰도 (2016)	B2C 전자상거래 지수 (2016)	B2C 전자상거래 지수 (2015)	세계 순위 (2015)
한국	93	94	96	99	95.5	95	4
지부티	13	12	39	8	18	20	126
에티오피아	15	22	5	23	16	27	113

[출처] UNCTAD B2C e-commerce index(2017)

▶ 세계은행의 전자상거래 지표에 따르면 지부티에서 사용한 결제 수단 중 신용카드(15세 이상 인구) 보유율은 3.96%, 체크카드는 7.60%이며 휴대폰을 통한 계좌 결제에 대한 정보는 없음[509]

▶ 지부티텔레콤(Djibouti telecom)은 지부티 항구에서의 배송 추적과 모바일 머니 세그먼트를 포함하여 M2M (machine-to-Machine) 분야로 사업을 확대[510]

- 2016 년 3 월 eServGlobal과 계약을 맺어 전자 지갑(e-wallet) 플랫폼을 제공하여 가입자에게 휴대폰을 통한 현금 관리 및 전자 결제 서비스를 제공

2) 인터넷 및 통신 환경

▶ 유선통신

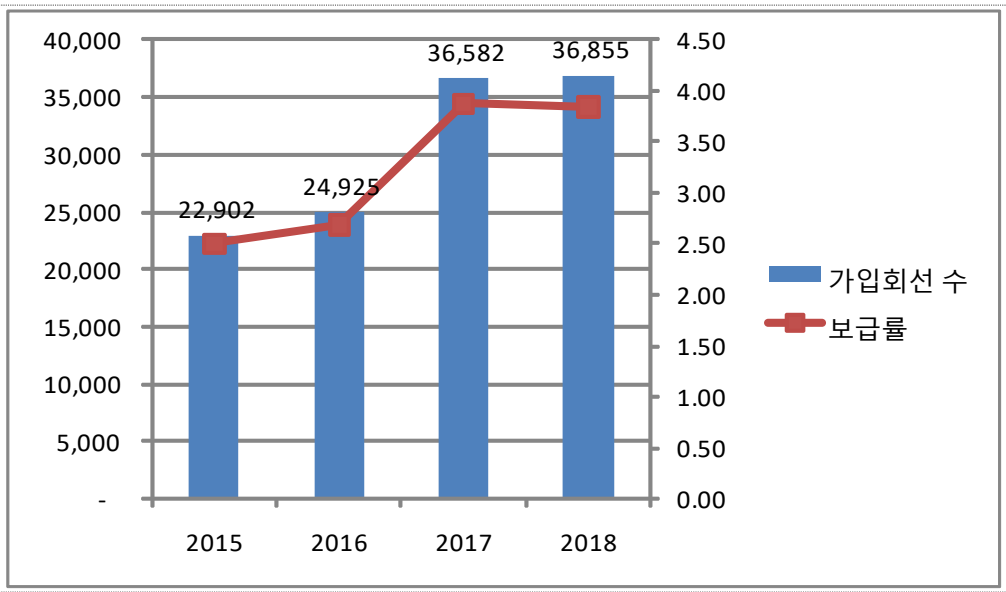
- 2018년 지부티의 유선통신 가입회선 수는 2017년 대비 0.7% 증가한 36,855회선을, 인구 당 보급률은 3.84%를 기록해 아프리카 지역 평균에 해당
- 지부티는 국영통신사인 지부티 텔레콤에 유선, 이동, 인터넷, 데이터 통신을 포함한 모든 통신

508 https://unctad.org/en/PublicationsLibrary/tn_unctad_ict4d09_en.pdf
509 https://wits.worldbank.org/analyticaldata/e-trade/country/DJI
510 Telecoms, Mobile and Broadband – Statistics and Analyses Buddecom, 2019.03.05

서비스의 독점권을 부여한 마지막 아프리카 국가들 중 하나로, 이러한 독점이 GDP가 더 낮은 아프리카 국가들보다도 시장 성장이 더딘 원인이 됨

그림 _ 지부티 유선통신 가입회선 수 및 보급률

(단위: 회선, %)



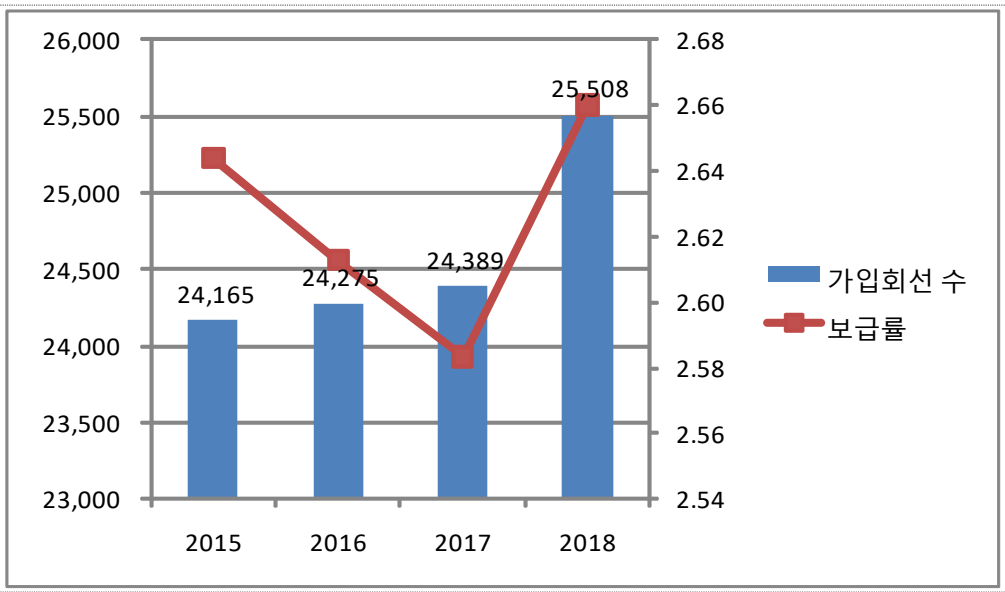
[출처] ITU Statistics DB(2019)

▶ 브로드밴드

- 2018년 지부티의 브로드밴드 인터넷 가입회선 수는 2017년 대비 4.6% 감소한 25,508선을, 인구 당 보급률은 2.66%를 기록
- 유선 브로드밴드 보급률은 최근 몇 년 동안 크게 증가했지만 국제적 기준보다 낮으며 서비스도 비교적 비싼 수준

그림 _ 지부티 브로드밴드 가입회선 수 및 보급률

(단위: 회선 ,%)



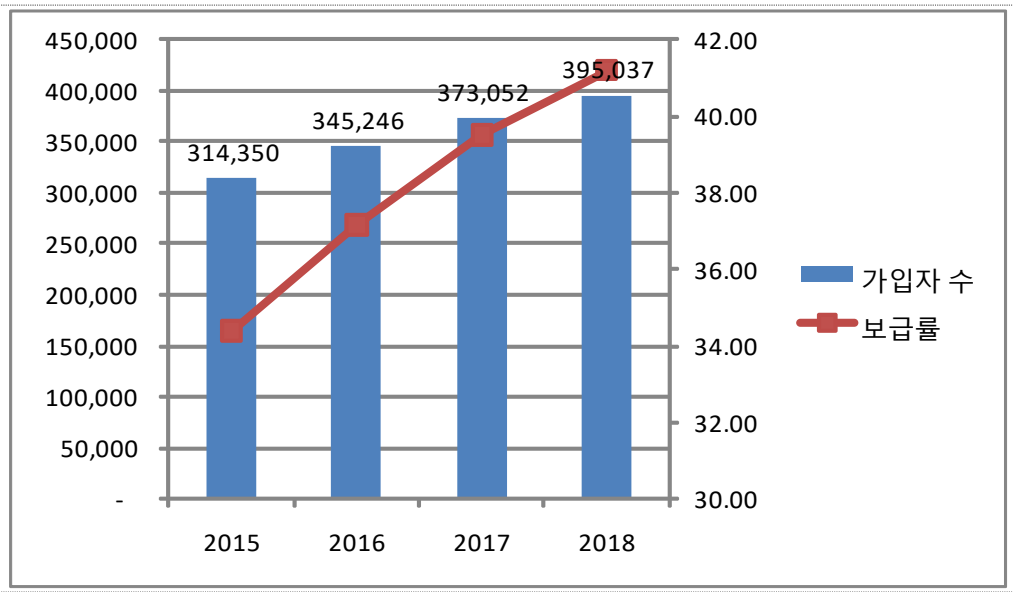
[출처] ITU Statistics DB(2019)

▶ 이동통신

- 2018년 지부티의 이동통신 가입자 수는 2017년 대비 5.9% 증가한 395,037 명을 기록, 인구 당 보급률 41.20%를 기록함
- 지부티 텔레콤은 2001년 Evatis라는 브랜드 이름으로 GSM 900 네트워크를 출시했지만, 모바일 보급률은 현재 아프리카 평균의 절반에 불과
- 그러나 가입자 기반은 꾸준히 성장하고 있으며 아프리카에서 가장 빠르게 발전하는 시장 중 하나로 평가받음
- 2007 년부터 EDGE 기술을 사용하여 제한된 모바일 브로드밴드 서비스가 제공되었지만 높은 비용으로 인해 대부분의 모바일 사용자들에게 서비스를 제공하지 못함
- 선불 서비스는 더 저렴하지만 시간 기준으로 청구되어 상대적으로 비싼 수준임
- 지부티 텔레콤은 2011 년 말 3.5G (HSPA+) 서비스를 시작했으며 2016년 중반부터 LTE 서비스를 시험하고 있음
- 모바일 데이터의 잠재력에도 불구하고 대부분의 사업자 가입자는 음성 서비스만 사용하며, 인구의 약 60 %가 3G 인프라를 사용할 수 있음

그림 _ 지부티 이동통신 가입자 수 및 보급률

(단위: 명, %)



[출처] ITU Statistics DB(2019)

정보보호 시장 현황

1) 시장 규모

시장 개요

▶ 지부티 정보보호 시장 현황에 대한 정보 부재

▶ 지부티 물리보안 시장에서 큰 비중을 차지했던 유럽 및 일본 전자보안기기보다 중국제품의 사용이 더욱 많아지고 있는 추세인 것으로 파악됨

- 겔레 (Ismail Omar Guelleh) 지부티 대통령은 2015년 중-아프리카 협력포럼의 일환으로 열린 시진핑 주석과의 정상회담에서 지부티 필수 인프라 시설에 대한 중국의 비디오 감시 카메라 시스템 도입을 논의한 바 있으며 한 매체에 의하면 2019년 현재 중국이 안면 인식 감시 카메라 600대를 지부티 정부에 무상으로 제공[511]

2) 주요 사업자 현황

시장 특성 및 경쟁 강도

▶ 지부티에 자체적인 사이버 보안 및 물리 보안 제조사가 없어 글로벌 IT 솔루션 기업들의 제품이 시중에 판매되고 있는 것으로 파악됨

- 네트워크 및 기본적인 글로벌 IT 솔루션 기업은 현지에 진출하거나 대리점을 통해 제품을 판매하고 있으며 Cisco는 네트워킹 보안 및 장비 교육 과정을 개설해 운영 중

주요 사업자

▶ 정보보안

- SDSI(Société de Développement de Systèmes d'Information)
  - 2007년 설립된 로컬회사로 소프트웨어 통합, 아카이빙, 보안 컨설팅 등을 서비스함

511 https://human-village.org/spip.php?article553

- 전화번호 : +253 21 35 11 12
- 홈페이지 : http://www.sdsi.dj/
- 주소 : Bâtiment Boulevar ㅇ Venise 1ère étage
  Appartements 3 et 4
  BP 2929 Djibouti

• Tech in Djib
- 가정, 기업을 위한 IT장비 설치, 홈페이지 개설, 사이버보안 서비스
- 전화번호 : +253 21 34 21 72, 77 71 36 98, 77 87 52 02
- 홈페이지 : http://techindjib.com/
- 주소 : Cité poudrière lot 82 , Djibouti Ville

• Dis-pro Informatique
- IBM 공식 판매점이자 보안 및 경보 장치, IT장비 및 Microsoft Windows 설치, 유지 및 교육, 각종 바이러스백신 소프트웨어 솔루션 제공
- 전화번호 : +253 21 35 88 22
- 홈페이지 : http://www.groupe-marill.com/fr/activite/informatique-0
- 주소 : Dis-pro Informatique
  Rue Clochette
  BP 57 - DJIBOUTI

▶ 물리보안

• AGS Sécurité
- 경비, 순찰, 비디오 감시, 화재 및 침입 경보, 출입제어 등
- 전화번호 : +253 21 35 40 91, 92
- 홈페이지 : http://www.agssecurite.com/
- 주소 : BP 2060 - Impasse des Acacias-Héron-DJIBOUTI

• Somelec
- 출입제어, 화재 경보, 침입 방지, CCTV, 차량 출입 시스템 등 전자보안시스템 설치 및 유지
- 전화번호 : +253 21 34 17 78
- 홈페이지 : http://www.somelecdjib.com/
- 주소 : Somelec Avenue Nelson Mandela
  BP6097 Djibouti Ville RDD

• Alfa Mep
- CCTV 보안, 야간투시카메라. 하이브리드 &IP 리코더, 경보관리시스템, 차량 모니터링 시스템, 주요

인프라, 금융시설 보안 등 전자보안시스템 공급, 설치, 유지

- 전화번호 : + 253 77 81 25 15, 25
- 홈페이지 : https://alfamep.com/alfa-security/
- 주소 : ALFA MEP s.a.r.l
  Nelson Mandela Street , Djibouti

3) 주요 동향 및 이슈

▶ 2019년 2월 지부티 중앙은행(BCD)은 세계은행의 지원을 받아 개선된 자동이체시스템(système de transfert automatique amélioré, ATS+)라는 국가결제시스템을 사용해 실시간으로 안전하게 은행간 결제 및 대량 송금이 가능하게 될 전망

• 미국의 전자결제시스템 구축기업인 Montran과 로컬 파트너인 Hypercube, 국가정보보호국(ANSIE), 국가투자진흥청(ANPI)이 협력하여 개발한 동 시스템을 시작으로 차후 광섬유케이블이나 와이파이를 통한 중앙은행과 시중은행 간 연계를 목표로 하는 2단계 사업도 추진할 방침

정보보호 정책 및 기관 현황

1) 관련 법령 및 정책

관련 법령 및 규제

▶ 지부티는 사이버 범죄에 대한 법령이 정비되어 있으나, 전자상거래, 개인정보보호 관련법은 부재

- 사이버보안 및 사이버범죄 방지법(Loi N° 66/AN/14/7ème Loi relative au cyber sécurité et à la lutte contre la cybercriminalité) : 2014.7.20 제정

주요 전략 및 정책

▶ 지부티는 국가차원의 사이버 보안에 대한 정부 로드맵을 마련하는 초기 과정에 있음

- 국가정보보호국(Agence nationale des systèmes d'information de l'Etat, ANSIE)은 2019년 7월 모든 국가기관 대표들을 소집해 사이버보안 인식 제고, 사이버범죄 감소, 사고대응능력 제고, 주요 인프라 보호, 사이버 공간에서의 신뢰 구축을 목표로 국가사이버보안전략 수립을 위한 토론회를 개최

▶ 현재 마련된 표준 및 인증제도는 없으며 2019년 2월 표준화 및 품질 증진 제도 채택 관련법이 통과되어 관련 법제를 정립하고 구상 및 승인 절차를 마련할 방침[512]

- 그러나 대상 분야에 정보 보호나 물리보안이 해당되는지는 확실하지 않음

▶ 대내외 협력 체계 부재

- 지부티는 사이버 보안 대응 시스템을 활용할 수 있는 대내외 협력 시스템 및 파트너십을 구축하고 있지 않음

▶ 자국 내 공공 분야 간 협력

- 2015년 설립된 국가정보보호국(ANSIE)은 모든 국가행정기관을 고속인터넷으로 연결하고 범용 컴퓨터 애플리케이션을 개발해 하나의 데이터센터에 호스팅 함으로써 행정의 효율성과 생산성을 높이고 온라인 교육, 보건, 상거래 분야의 사업과 시민을 위한 온라인 서비스 개발을 궁극적 목표로 함

512 https://www.presidence.dj/texte.php?ID=33&ID2=2019-02-14&ID3=Loi&ID4=3&ID5=2019-02-14&ID6=n

▶ 국제 협력

- 지부티는 2018년 5월 세계은행그룹, 우간다 국가정보기술청(NITA-U), 동아프리카공동체(EAC), 이스라엘 정부가 공동 주최한 '동 아프리카 사이버 보안 클리닉'에 참가, 전 세계적으로 확대되는 사이버 위험과 위협에 지역적으로 대응하기 위한 사이버 보안 인식 제고, 공공부문의 사이버 보안 프레임 워크 및 이니셔티브 구상 및 개발과 해당 지역의 지역 협력 및 시너지 효과 창출에 참여[513]

2) 담당기관

▶ 국가정보보호청(Agence nationale des systèmes d'information de l'Etat,ANSIE)

- 지부티 정부는 ICT기술을 활용한 행정 기능 현대화를 가속화하기 위해 2015년 7월 동 기관을 설립, 전자정부 구축을 통해 시민 및 기업과 행정기관 간에 보다 신속하게 정보 공유가 이뤄질 수 있도록 하는 것을 목표로 함

표 _ 지부티 국가정보보호청(ANSIE) 주요 역할

ANSIE의 주요 역할
국가행정 정보시스템 개발을 위한 공동전략프레임 구상 및 제안
신뢰할 수 있고 정확하며 안전한 네트워크 및 시스템 국가 인프라 구축
국가행정기관의 IT 프로젝트를 규격화하고 조화하고 합리화하는 모든 사업에 대한 기술 협조
온라인 발급 서비스의 기능적 모델 개발
공공기관 및 전략적 사업자의 정보시스템 보안에 영향을 미치거나 위협하는 위기대응책 마련
정부에 정보시스템 보호 방안을 제언하고 채택된 방안의 시행 감독
인프라 업그레이드 및 확장을 위한 기술 및 규제 감독
정보시스템 보안 장치 및 기술의 연구개발 방향 제시에 참여

[출처] ANSIE 홈페이지

3) 규제 및 인증제도

▶ 정부 차원의 인증 시스템 부재

513 https://africabusinesscommunities.com/tech/tech-news/east-africa-cybersecurity-clinic-launched/

- 지부티에는 정보보호를 위한 인증제도가 마련되어 있지 않음

▶ 정부 보안 표준 프레임워크 부재

- 지부티에는 보안 표준을 위한 국가 프레임워크가 없음

4) 최근 정책 동향 및 이슈

▶ 2019년 8월 지부티 내무부는 세계적으로 증가하는 사이버범죄를 방지하기 위해 법제를 강화할 방침이라고 발표함과 동시에 법무부, 국제법전문가, 국가정보보호국(ANSIE), 변호사 등이 참여하는 협의회를 처음으로 개최

- 모든 국가정보시스템, 국가의 사회경제활동에 필수적인 인프라뿐 아니라 온라인상에서 기업 및 개인의 정보시스템을 보호하는 것을 목적으로 함

▶ ICT 기술을 사용한 범법행위를 예방하고 퇴치하기 위해 2018년 1월 지부티 국가안보국(Direction Générale de la Sécurité Nationale) 내에 디지털정보국(Direction de l'Intelligence numérique)을 신설

- 국영통신사업자 네트워크 관련 정보 수집 및 보호, 국가의 안전을 위협하는 테러행위 또는 반체제적 행위로 간주되는 범법행위 예방을 위한 인터넷 통신수단 감독 및 네트워크 감시 등을 담당

사. 베냉

'18년 GDP(십억달러)	10.36
'18년 인구수(천명)	11.49

■ ITU 글로벌 사이버보안 지수(Global Cybersecurity Index, GCI)

· 베냉의 글로벌 사이버보안 지수는 80위로 아프리카권에서는 상위권에 속함

국가명	2018		2017		전년대비 증감	
	지수	순위	지수	순위	지수	순위
베냉	0.485	80	0.069	149	+0.416	+69
대한민국	0.873	15	0.782	13	+0.091	-2

■ ICT 관련 주요 지수

· 베냉의 전반적인 ICT 발전 수준은 전 세계 중하위 수준을 보이고 있음

지표명	베냉		한국	
	점수	순위	점수	순위
IMD 국가경쟁력지수(2019)	-	-	-	28
IMD 디지털경쟁력지수(2019)	-	-	-	10
UNCTAD 전자상거래지수(2019)	21.0	138	89.4	19
ITU 글로벌 사이버보안 지수(GCI 2018)	0.485	80	0.873	15
UN 전자정부 지수(2018)			0.901	3

■ ICT 관련 주요 통계 (ITU, 2018년 말 기준)

· 베냉의 유선통신 보급률은 0.4%, 이동통신 보급률은 82%로 주로 이동통신에 의존

항목	베냉		한국	
	가입자수(천 명)	보급률(%)	가입자수(천 명)	보급률(%)
유선전화	49	0.42	25,907	50.63
유선브로드밴드	279	0.24	21,286	41.60
이동통신	9,462	82.38	66,356	129.67
인터넷 이용률	-		95.90%	

정보보호 산업 개요

1) 보안 환경

▶ ITU의 글로벌 사이버보안 지수(Global Cybersecurity Index, GCI)에 따르면 베냉은 2017년 164개국 중 148위(0.069)에서 2018년 175개국 중 80위(0.485)로 상승, 아프리카지역 국가 중에서는 8위를 차지

- 2017년 사이버범죄방지 및 사이버보안법인 디지털법(Code du Numérique)을 도입함으로써 GCI 지수의 법 부문에서 에스토니아, 폴란드와 함께 좋은 평가를 받음
- 2017년 컴퓨터비상대응팀(bjCSIRT) 구성 등 사이버 보안 관련 정책, 법제, 조직이 상대적으로 잘 마련된 아프리카국가 중 하나

▶ 서아프리카에서 나이지리아, 코트디부아르에 이어 가장 많은 사이버범죄행위가 일어나는 국가[514]

- 사이버범죄진압 중앙국(Office central de répression de la cybercriminalité, OCRC)의 발표에 따르면 2017년 상반기에 개인에 대한 98건의 사이버공격이 있었으며 피해액은 4억1,000만 세파 프랑으로 추정, 총 73명이 체포되었으며 기관에 대한 사이버공격의 피해액은 2억 세파 프랑에 달함

▶ 베냉 정부는 2017년 10월 통신 인프라 및 ICT발전계획(Projet de Développement des Infrastructures de Télécommunications et des TIC, PDI2T)을 통해 통신과 ICT분야의 발전을 촉진할 방침으로 이에 따라 보안 환경도 개선될 전망

2) 인터넷 및 통신 환경

▶ 유선통신[515]

- 베냉은 유선통신 인프라 환경이 좋지 않아 유선 음성 및 인터넷 서비스 사용률이 낮아 매출액도 낮은 상황
- 유선통신 사업자로는 국영기업 BE.TELECOMS SERVICES가 있는데, 1992년 국가경제에서 통신 부문의 전략적 역할을 규정한 법률 도입에 따라 독점권을 가짐(당시 회사명은 OPT)
- 유선통신망은 국토의 3/4에 보급되어 있지만 전화선의 1/3이 일부 주요 도시에 집중되어 있어

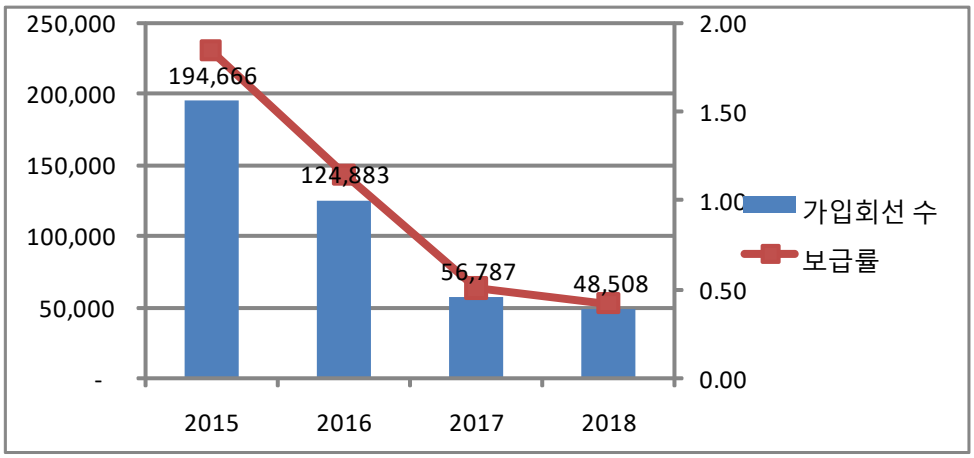
514 http://ortb.bj/index.php/tech/6156-cybercriminalite-au-Bénin -necessite-de-reagir-face-a-un-fleau-qui-perdure
515 'Telecoms, Mobile and Broadband Statistics and Analyses',Buddecom(2019.03.29)

전화밀도가 전국 평균의 2배에 달함

- 베냉은 저개발된 유선 인프라로 인해 유선통신 이용률이 2015년부터 감소세로 돌아선 후 급격히 하락하는 추세로, ITU의 자료에 따르면 2018년 베냉의 유선전화 가입회선 수가 2017년 56,787회선에서 48,508회선으로 14.6% 감소하면서 보급률은 0.42%에 그침

그림 _ 베냉 유선전화 가입회선 수 및 보급률 추이 (2015~2018)

(단위: 회선, %)



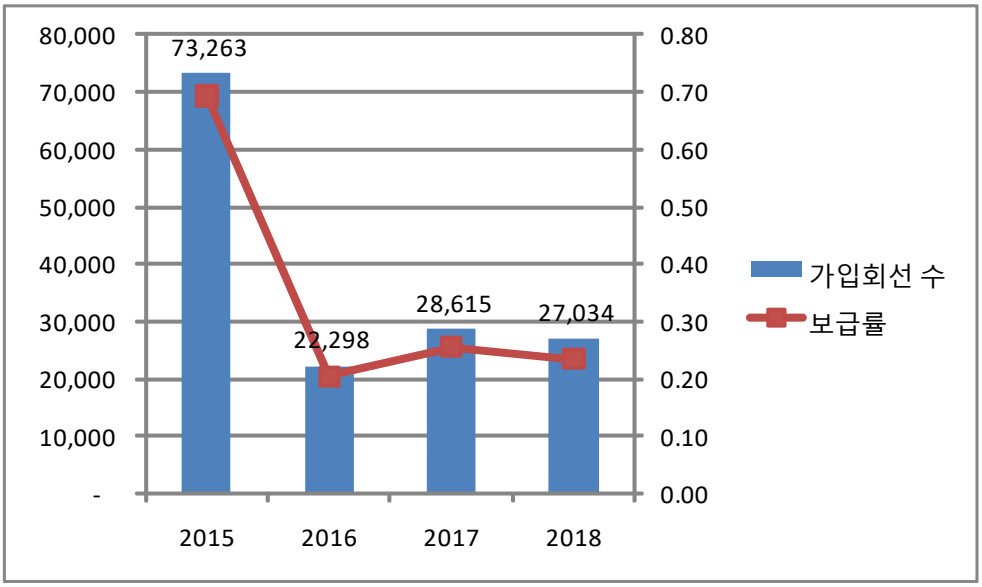
[출처] ITU Statistics DB(2019.6)

▶ 브로드밴드

- 베냉은 2017년 통신인프라 및 ICT발전계획(Projet de Développement des Infrastructures de Télécommunications et des TIC, PDI2T)을 통해 브로드밴드 인프라를 확충, 2021년까지 인구의 80%에 브로드밴드 인프라를 제공할 수 있도록 할 방침(유선 브로드밴드 40%, 모바일 브로드밴드 60%)
- 2018년 베냉의 브로드밴드 가입회선 수는 2017년 28,615에서 5.5% 감소한 27,034회선으로 보급률 0.24%를 기록, 2016년 전년도 대비 62.7% 하락한 후 3년 연속 비슷한 수준을 보이고 있음

그림 _ 베냉 유선 브로드밴드 가입회선 수 및 보급률 추이 (2015~2018)

(단위: 회선, %)



[출처] ITU Statistics DB(2019.6)

▶ 이동통신

- 베냉의 낙후된 유선통신 인프라로 인해 대부분의 음성 서비스 및 인터넷 연결이 MTN Bénin 과 Moov가 운영하는 모바일 네트워크를 통해 이뤄지고 있음
- 이동통신 시장은 베냉 정부가 2000년 GSM 라이센스를 Telecel Bénin (현 Moov), Spacetel-Bénin (현 MTN), Libercom 3개사에 부여하면서 민영화되었으며 2003년, 2007년에도 각각 Bell Bénin 과 Globacom에 라이센스를 부여함
- 현재 베냉 최대 이동통신사는 Moov로 52.4%의 시장점유율을 보이고 있으며 그 뒤를 2018년 라이센스가 취소된 Glo Mobile 가입자를 인수한 MTN이 바짝 뒤쫓고 있음.
- 2017년 정부가 승인한 구조조정계획으로 국영기업 Bénin Telecoms에서 분리된 Libercom은 MTN 및 Moov와의 경쟁에서 실패해 2018년 9월 서비스를 중단한 상태이며 2017년 규제당국의 통신품질규제 관리 후 두 기업(Bell Bénin , Globacom)의 라이센스가 취소되었음
- 가까운 시일 내에 다른 사업자에 대한 라이센스 발급이 발표될 것으로 예상됨
- MTN은 2012년 3월에 라이센스를 획득하여 3G 및 4G 모바일 서비스와 공용 Wi-Fi 및 VoIP서비스를 운영하고 있으며 Moov는 2014년 초 수도인 Cotonou에서 3G 서비스를 시작함
- 2015년 3월 베냉 정부는 be.Telecoms에 브로드밴드 연결성을 개선하기 위해 LTE 서비스 사업을 전개할 수 있도록 승인, 1800MHz대역의 스펙트럼을 사용하도록 함
- LTE서비스는 2015년 초부터 제공되기 시작해 2016년 12월 Porto Novo, Cotonou, Ouidah, Abomey-Calavi, Alladah에서 상용화되었으며 통신망 확장 1단계 종료 시 20개 도시에 상용화하는 것을 목표로 함

표 _ 베냉 이동통신가입자수에 따른 통신사별 시장점유율(2012~2018)

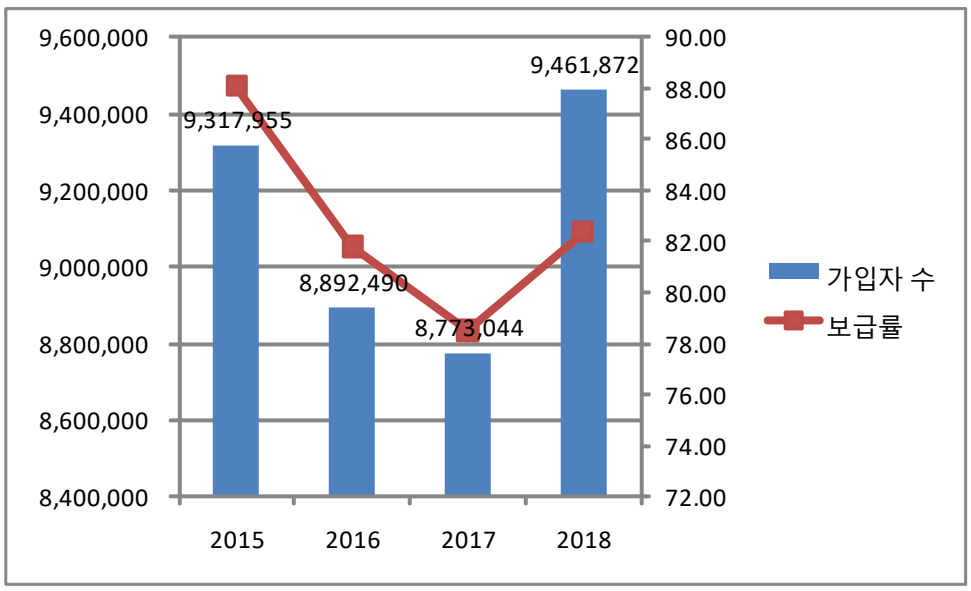
(단위: %)

연도	MTN	Moov	BBCom (Bell Bénin)	Glo Mobile (Globacom)	Libercom
2012	32.5	33.2	12.8	18.0	3.5
2013	36.0	34.4	11.5	15.3	2.9
2014	44.1	33.1	3.0	15.0	0.8
2015	46.0	35.0	2.0	18.0	1.0
2016	46.6	42.0	-	11.7	0.7
2017	48.7	45.1	-	5.4	0.7
2018(6월)	47.2	52.4	-	-	0.3

• 2018년 기준 베냉의 이동통신 가입자 수는 2017년 8,773,044명에서 7.9% 증가한 9,461,872명으로 가입률 82.38%를 기록

그림 _ 베냉 이동통신 가입자 수 및 보급률 추이 (2015~2018)

(단위: 명, %)



[출처] ITU Statistics DB(2019.6)

▶ 전자상거래 및 결제시장 전문 조사기관 yStats에 의하면 베냉은 모바일 인터넷 사용률에 있어 서아프리카에서 6위(24%)를 차지했으며 15세 이상 인구 중 모바일 머니 계좌 보유율은 18%로 나타남[516]

▶ Buddecom의 보고서에 따르면 베냉의 모바일 머니 서비스 가입자 수가 2016년 906,000명에서 2017년 1,722,930명으로 무려 90.2%나 증가

- MTN은 베냉에서 대리점 네트워크를 통해 사용자들이 현금을 입금하고 인출할 수 있어 휴대폰 유무에 관계없이 송금이 가능한 모바일 머니 서비스를 운영
- Moov는 2013년 후반에 m-commerce 서비스인 'Flous'를 출시해 고객이 휴대폰을 디지털 지갑처럼 사용해 상품 및 서비스 구매에 따른 결제, 계좌 이체, 현금 인출 및 입금, 휴대폰 충전, 은행계좌 관리를 할 수 있도록 했으며 'Moov Money'라는 브랜드명으로 m-banking 서비스를 제공 중
- 2017년 프랑스에서 Orange Bank를 출시한 Orange group은 공통중앙은행 및 통화(세파프랑, CFA)를 공유하는 베냉, 부르키나 파소, 코트디부아르, 말리, 나이지리아, 니제르, 세네갈 및 토고 등을 포함한 서아프리카경제통화연맹(WAEMU)에 은행업 라이선스를 신청했으며 현지 은행과의 제휴를 통해 Orange Money 플랫폼을 통해 서아프리카 지역에서 서비스를 제공할 계획

표 _ 베냉 모바일 머니 서비스 사업자별 가입자 현황 (2016~2017)

(단위: 명)

연도	MTN	Moov	총계
2016	751,130	155,870	906,000
2017	1,364,030	358,900	1,722,930

[출처] "Telecoms, Mobile and Broadband-Statistics and Analyses",Buddecom(2019.3)

516 "Global E-Commerce Intelligence, Africa B2C E-Commerce & Online Payment Market 2019", yStats, 2019.6.

정보보호 시장 현황

1) 정보보호 시장 규모

시장 개요

▶ 베냉의 정보보호 시장 규모는 파악하기 어려움

시장 규모 및 성장률

▶ 베냉은 ICT 분야가 발전함에 따라 ICT기술을 사용한 범죄가 증가하면서 정부 및 민간 주도로 많은 토론회, 포럼 등이 개최되고 관련 법제, 조직 등이 정비되는 등 사이버보안에 대한 의식이 제고되고 있는 상황이나 보안 시장 자체는 여전히 작은 규모이며 파악이 어려움

2) 주요 사업자 현황

시장 특성 및 경쟁 강도

▶ 베냉은 자체 정보 보호 상품이 없고 글로벌 기업 상품을 사용하는 실정
- 많은 나이지리아의 CCTV, 출입 제어, 화재 및 도난 경보 시스템 설치기업들이 베냉에 진출해 판매, 설치 및 유지·보수 서비스를 제공

주요 사업자

▶ ExperTIC
- 사이버보안 및 IT솔루션 컨설팅 기업
- 홈페이지 : http://www.expertic.bj/
- 전화번호 : (+229) 66 55 95 95
- 이메일 : info@expertic.bj

▶ Sagam Sécurité Bénin

- 글로벌 기업인 Sagam international의 베냉 법인
- 현금 이송, 전자보안시스템 공급, 설치 및 유지 보수 서비스 제공
- 홈페이지 :http://sagam-intl.com/le-groupe-sagam/filiales/sagam-securite/sagam-securite-Bénin /
- 전화번호 : (+229) 21 31 56 01 / 21 31 56 03
- 이메일 : sagam@leland.bj

▶ e-telecom

- CCTV(아날로그&IP), 출입제어, 출입문 원격제어 시스템 등의 물리보안 제품 설치 및 유지 보수
- 홈페이지 : http://e-telecom.net/Systeme-surveillance.php
- 전화번호 : (+229) 21 32 41 51 / 67 01 80 80
- 이메일 : info@e-telecom.net

▶ Sobitech

- 해킹, 사이버공격, Shadow IT, 침입, 범죄 등 정보시스템 및 장비 관련 위협에 대한 솔루션 (CCTV, 소프트웨어, 알람시스템 등) 제공
- 홈페이지 :http://www.sobitech-Bénin .net/index.php?giwu=accueil
- 전화번호 : (+229) 21 32 51 53 / 97 42 73 37
- 이메일 : info@sobitech-Bénin .net

4) 주요 동향 및 이슈

▶ 미국의 사이버보안기업 컨소시엄인 'ATR Cyber Security Agency'가 베냉의 수도인 Cotonou에 2017년 진출함으로써 베냉 정부 및 민간 기업에 관련 전문역량을 공유[517]

- 기업들에게 정보시스템의 데이터를 평가함으로써 사이버 공격으로부터 보호하기 위한 가이던스 제공

517 https://www.digitalbusiness.africa/cybersecurite-le-Bénin -va-beneficier-de-lexperience-du-consortium-atr-cyber/

정보보호 정책 및 기관 현황

1) 관련 법령 및 정책

관련 법령 및 규제

▶ 디지털법(Loi n° 2017-20 portant code du numérique)[518]

- 2014년 아프리카 연합(AU)이 채택한 사이버보안 및 개인정보보호협약과 서아프리카경제공동체를 비롯한 지역공동체에서 채택한 표준에 부합하기 위해 동 법을 마련함
- 동 법은 7권에 걸쳐 총 647개의 조항으로 구성되어 (1)용어의 정의, (2)전자통신 네트워크 및 서비스, 전자도구 및 문서, (3)신뢰서비스업자, (4)전자상거래, (5)개인정보보호, (6)사이버범죄 및 사이버보안, (7)과도기 및 최종 조치를 총망라함
- 동 법의 제5권은 정보의 수집, 처리, 이전, 저장에 따른 개인정보 및 직업정보 보호를 통해 개인의 자유와 기본권리를 보장
- 동 법의 제6권은 사이버범죄 방지 규칙과 방법을 규정함과 동시에 암호화 기술의 사용방식과 규칙, 제도적 틀을 규정함

주요 전략 및 정책

▶ 베냉은 현재 국가 차원의 사이버보안 전략을 갖고 있지 않으나 관련 전략을 구상 중

▶ 통합 정보시스템 보안 계획(Plan Global de Sécurité du Système d'Information, PGSSI)[519]

- 2014년 경제재정부 산하 정보시스템국(Direction des systèmes d'information)은 정보시스템의 일상적 사용에 있어 준수해야 할 방침 및 절차, 정보시스템 보안 거버넌스 등을 편집해 동 계획을 마련함
- DSI는 동 계획을 통해 IPS/IDS를 비롯한 정보시스템 보안 감시, 보안 관련 공지 및 이상 보고, 여러 분야에서 실행해야 할 패치 및 업데이트 추천, PGSSI의 절차 및 방침의 적용에 대한 인식 제고, 기존 시스템들에 대한 침입 테스트, 모든 IT프로젝트에 대한 보안서류 취합

518 https://cio-mag.com/decryptage-de-la-loi-portant-code-du-numerique-du-Bénin /
519 https://www.finances.bj/dsi/domaines-dintervention/#sec

▶ 스마트 정부 계획(Smart Gouv)

- 베냉 디지털부가 추진하는 Smart Gouv 계획은 사용자 중심의 공공서비스 제공을 통한 행정의 효율성과 개방성 개선, 굿 거버넌스 및 부패 방지 촉진을 목적으로 함
- 행정 효율성 증대를 통한 경제 성장 가속화, 국가예산 및 지출 운영 개선, 비즈니스 환경의 투명성 증대 등으로 인한 경제·사회적 파급효과가 매우 클 것으로 기대됨
- 동 계획은 여러 국가 및 산업 정보시스템을 통해 베냉 시민이 사회보장제도, 디지털 신분증, 직업 교육의 혜택을 받을 수 있도록 하는 'e-identité', 가족관계등록부, 국가공무원 급여 지급 및 인력 관리시스템, 국가예산관리시스템, 단일창구 도입을 통한 행정 간소화 등을 골자로 함
- 상기 이니셔티브들은 공공서비스의 디지털화, 행정기관 간 상호연결성 및 정보 공개를 가능하게 하는 기술적, 법적, 조직적 토대가 마련된 후 추진될 방침

▶ Revealing Benin 프로젝트

- 2016년 12월 베냉 정부는 베냉 역사상 전례 없는 규모의 개발 및 투자프로그램인 'Revealing Benin ' 프로젝트를 통해, 5년 간 9조 390억 세파 프랑(약 137억8천 유로)을 투자하여 디지털 경제를 비롯한 45 개 주요 프로젝트와 9 개의 주요 부문(관광, 농업, 인프라, 전기, 생활 환경 및 지속 가능한 개발, 식수 보호, 국제 지식 및 혁신도시)에 걸친 대규모 개발을 추진할 예정

2) 담당기관

▶ 디지털부(Ministère du Numérique et de la digitalisation)

- 동 부처는 디지털 부문에 대한 투자 촉진, 산업 성장, 거버넌스 개혁, 기업의 성장과 경쟁력 제고에 필요한 통신 및 디지털 인프라 개발을 담당
- 산하에 디지털국(Agence du Numérique)을 신설, 고속인터넷 및 초고속인터넷망 개발, 디지털지상파방송(TNT), Smart Gouv, 전자 상거래 대중화, 교육부문에서의 디지털기술 활용 촉진, 디지털 컨텐츠 개발 촉진 등 디지털부가 추진하는 모든 사업의 포컬 포인트로서 사업의 추진, 이행, 인력 및 기술 동원, 사업 평가 등을 수행[520]

▶ 베냉 국가정보보호국(Agence nationale de la sécurité des systèmes d'infromation, ANSSI Bénin)[521]

- 2017년 디지털법 제604조에 의거해 출범한 대통령 직속 기관으로, 베냉 영토 내 정보시스템 및 네트워크의 보안을 총괄

520 http://revealingBénin .com/agencies/numerique/
521 https://www.afapdp.org/wp-content/uploads/2018/06/Benin-Loi-2017-20-Portant-code-du-numerique-en-Republique-du-Benin.pdf

- 국가 차원의 정보보안전략의 마련 및 방향 제시, 정보시스템 보안과 관련된 모든 계획 및 프로그램 추진과 관련 공공 및 민간 주체들과의 협력, 감독, 보안 사고에 대한 지원 요청의 중앙집권화 등을 담당

▶ 사이버범죄진압 중앙국(Office central de représsion de la cybercriminalité, OCRC)

- 베냉 경찰 산하의 사이버범죄 방지를 담당하는 부서이지만 진화하는 사이버범죄에 대응하기 위한 첨단 장비가 부족한 상황[522]

▶ 정보시스템관리국(Direction des systèmes d'information, DSI)[523]

- 경제재정부의 서비스 조직 및 정보화 관련 정책의 시행을 담당하는 기관으로 동 부처에 IT정책 제언 및 시행, IT사업계획 추진, 부처의 IT 시스템 및 장비 유지보수, 동 부처의 통신네트워크 설치 및 운영 등이 주요 임무

▶ 베냉 컴퓨터비상대응팀(bjCSIRT)[524]

- 2017년 9월 구성된 컴퓨터비상대응팀은 컴퓨터 보안 침해 사고 발생 시 정부기관들이 처음으로 연락을 취해야 하는 조직으로, 베냉의 사이버보안 및 디지털 촉진 협회(ABCPN)와 사이버범죄진압 중앙국(OCRC)를 비롯한 여러 인터넷 보안 주체 및 경찰과 적극적인 협조 아래 사이버범죄를 퇴치
- 2019년 bjCSIRT는 아프리카 컴퓨터침해대응팀(AfricaCERT)의 일원으로 받아들여짐으로써 해당 분야에서 국제적으로 인정받을 수 있는 대열에 오름

▶ 개인정보보호국(Autorité de protection des données à caractère personnel, APDP)[525]

- APDP는 개인정보보호를 감독하는 독립행정기관으로, 감독 및 처벌 권한을 가지고 있으며 경고 및 컨설팅의 기능도 수행함

3) 규제 및 인증제도

▶ 베냉 정부 차원의 인증 및 표준 시스템 부재

- 베냉은 사이버 보안 및 물리 보안을 위한 공식 인증 및 표준 시스템을 보유하고 있지 않음

---

522 http://ortb.bj/index.php/tech/6156-cybercriminalite-au-Bénin -necessite-de-reagir-face-a-un-fleau-qui-perdure
523 https://www.finances.bj/dsi/la-dsi/
524 https://csirt.gouv.bj/
525 https://apdp.bj/presentation/

4) 최근 정책 동향 및 이슈

▶ 베냉의 ANSSI는 2017년 출범 이후 글로벌사이버전문역량포럼(Global Forum for Cyber Expertise) 가입, 아프리카연합 사이버보안 협약 및 부다페스트 협약 회원국 인준절차 개시 등 사이버보안 관련 이니셔티브를 적극적으로 추진 중[526]

▶ 베냉 정부는 2017년 각종 조직 강도 행위 예방을 위해 범죄조직들의 주요 표적인 공공기관, 기업 및 공공장소에 CCTV를 설치하기로 결정함[527]

▶ ANSSI-Bénin은 사이버보안 관련 경쟁력을 강화하고자 2019년 9월 제2회 해커랩2019(Hacker lab 2019)를 개최[528]

- 예선을 통해 100명을 선발한 후 본선에서 3명을 최종 선발하는데, 참가자들은 웹, 포렌식, 암호화 기술, 스테가노그래피(Steganography), 리버스 엔지니어링(reverse engineering) 등의 분야에서 사이버범죄 방지를 위한 테크닉을 선보여야 함

▶ ANSSI-Bénin은 2019년 4월 디지털 보안 국가 전략 마련을 위한 토론회를 개최, 주요 공공 및 민간 주체들이 모여 주요 사이버 보안 이슈, 사이버 위협의 정의 및 종류, 국가보안전략의 필요성 및 목표, 주요 이슈 등에 대한 의견을 교환[529]

526 https://www.gouv.bj/actualite/250/le-Bénin -classe-8eme-au-plan-continental-en-matiere-de-cybersecurite-par-le-global-cybersecurity-index-2018/
527 https://www.bbc.com/afrique/region-38930409
528 https://cio-mag.com/lanssi-benin-sorganise-pour-la-deuxieme-edition-du-hackerlab/
529 https://isoc.bj/atelier-dechange-autour-de-la-strategie-nationale-de-securite-du-numerique-du-benin-compte-rendu-de-la-participation-disoc-benin/#.XZb3SkYzaUk

융합보안시장 및 정책 동향

1) 융합보안시장 동향

▶ 베냉에는 아직 융합보안시장이 형성되지 않은 상태이지만, 핀테크, 스마트시티, 사물인터넷에 대한 관심 및 인식이 높아지는 상황

2) 융합보안 정책 현황

▶ 2016년 2월 Cotonou에 스마트 시티 착공

- Buddecomm의 자료에 따르면 1억2천만 달러가 투자되는 베냉 스마트 시티는 베냉 최초의 디지털 구역으로서, 육양국(ACE cable landing station) 주변의 12헥타르에 해당하는 면적에 건설될 예정이며 디지털 경제 개발 계획의 중심을 이룰 계획

참고문헌

1. 689Cloud, "689Cloud – Vietnam-based Cybersecurity Startup receive funding from Singapore's ICE71", 2019.5.10.
2. ABC, "Indonesia picks Jakarta capital replacement in East Kalimantan province on Borneo", 2019.8.27.
3. AllAfrica.com, "Kenya: Cybersecurity Framework Set for Launch", 2014.6.24.
4. Alliance for Financial Inclusion, The Digital Financial Services Ecosystem in Latin America and The Caribbean, AFI Special Report, 2019.7.
5. Article 19, "Kenya: Cybercrime and Computer Related Crimes Bill", 2014.7.
6. Asia Blockchain review, "Cambodia National Bank Tests Blockchain for Cross-border Payments", 2019.11.1.
7. ASMAG, "Smart IoT Indonesia 2019 ready to unveil latest IoT trends", 2018.12.19.
8. Barclays, "Technology - 2H19 CIO Survey Shows Slowing IT Spending Growth", 2019.10.22.
9. Barnes & Co., "2019 Global High Tech & Emerging Markets", 2019.5.26.
10. Barnes Reports, "2018 Worldwide Security Systems Services Industry-Industry & Market Report", 2018.8.8.
11. Barnes Reports, "2019 U.S. Security Guards & Patrol Services Industry-Industry & Market Report", 2018.10.
12. Barnes Reports, "2019 U.S. Security Systems Services Industry-Industry & Market Report", 2019.1.9
13. Barnes Reports, "2019 Worldwide Security Guards & Patrol Services Industry & market Report", 2019.1.18
14. Barnes Reports, "2019 Global Forecast for Network Design And Development Services (2020-2015 Outlook)-Services & Markets Report", 2019.5.17
15. Barnes Reports, "2019 Global Forecast for Automotive Cyber Security (2020-2025 Outlook)-High Tech & Emerging Markets Report", 2019.5.26
16. Barnes Reports, "Barnes Reports-2019 Global Forecast for Cognitive Security (2020-2015 Outlook)-High Tech & Emerging Markets Report", 2019.5.26.
17. Bernama, "ICT industry sees bright prospects in 2018-2019", 2018.12.24.

18. Bitcoin, "Malaysia Starts Regulating Cryptocurrencies Today", 2019.1.15.
19. BMI Research, "Qatar security software", 2015.6.26
20. Buddecomm Telecoms Research, "Benin - Telecoms, Mobile and Broadband - Statistics and Analyses", 2019.3.29.
21. Buddecomm Telecoms Research, "Cambodia - Telecoms, Mobile and Broadband - Statistics and Analyses.", 2019.5.21
22. Buddecomm Telecoms Research, "China – Fixed Broadband Market - Statistics and Analyses", 2019.4.29
23. Buddecomm Telecoms Research, "China - Mobile Infrastructure, Broadband, Operators - Statistics and Analyses", 2016.11.29.
24. Buddecomm Telecoms Research, "China - Telecoms Infrastructure, Operators, Regulations - Statistics and Analyses", 2019.4.29
25. Buddecomm Telecoms Research, "Costa Rica - Telecoms, Mobile and Broadband - Statistics and Analyses", 2019.5.15.
26. Buddecomm Telecoms Research, "Djibouti - Telecoms, Mobile and Broadband - Statistics and Analyses", 2019.3.5.
27. Buddecomm Telecoms Research, "Dominican Republic - Telecoms, Mobile and Broadband - Statistics and Analyses", 2018.11.15.
28. Buddecomm Telecoms Research, "El Salvador - Telecoms, Mobile and Broadband - Statistics and Analyses", 2019.5.17
29. Buddecomm Telecoms Research, "Ethiopia - Telecoms, Mobile and Broadband - Statistics and Analyses", 2019.6.18.
30. Buddecomm Telecoms Research, "Guatemala - Telecoms, Mobile and Broadband - Statistics and Analyses", 2019.5.17.
31. Buddecomm Telecoms Research, "India – Fixed Broadband Market - Statistics and Analyses", 2019.3.2
32. Buddecomm Telecoms Research, "India - Mobile Infrastructure, Broadband, Operators - Statistics and Analyses", 2019.3.2.
33. Buddecomm Telecoms Research, "India - Telecoms Infrastructure, Operators, Regulations - Statistics and Analyses", 2019.3.2.
34. Buddecomm Telecoms Research, "Indonesia– Fixed Broadband Market - Statistics and

Analyses", 2019.6.3
35. Buddecomm Telecoms Research, "Indonesia - Mobile Infrastructure, Broadband, Operators - Statistics and Analyses", 2019.6.3.
36. Buddecomm Telecoms Research, "Indonesia - Telecoms Infrastructure, Operators, Regulations - Statistics and Analyses", 2019.6.3.
37. Buddecomm Telecoms Research, "Iran - Telecoms, Mobile and Broadband - Statistics and Analyses", 2019.2.20.
38. Buddecomm Telecoms Research, "Japan– Fixed Broadband Market - Statistics and Analyses", 2019.4.30
39. Buddecomm Telecoms Research, "Japan - Mobile Infrastructure, Broadband, Operators - Statistics and Analyses", 2019.4.30.
40. Buddecomm Telecoms Research, "Japan - Telecoms Infrastructure, Operators, Regulations - Statistics and Analyses", 2019.4.30.
41. Buddecomm Telecoms Research, "Kenya– Fixed Broadband Market - Statistics and Analyses", 2019.7.3
42. Buddecomm Telecoms Research, "Kenya - Mobile Infrastructure, Broadband, Operators - Statistics and Analyses", 2019.7.3.
43. Buddecomm Telecoms Research, "Kenya - Telecoms Infrastructure, Operators, Regulations - Statistics and Analyses", 2019.7.3.
44. Buddecomm Telecoms Research, "Laos - Telecoms, Mobile and Broadband - Statistics and Analyses", 2019.3.13.
45. Buddecomm Telecoms Research, "Malaysia – Fixed Broadband Market - Statistics and Analyses", 2019.3.2.
46. Buddecomm Telecoms Research, "Malaysia - Mobile Infrastructure, Broadband, Operators - Statistics and Analyses", 2019.3.2.
47. Buddecomm Telecoms Research, "Malaysia - Telecoms Infrastructure, Operators, Regulations - Statistics and Analyses", 2019.3.2.
48. Buddecomm Telecoms Research, "Mexico – Fixed Broadband Market - Statistics and Analyses", 2019.5.21.
49. Buddecomm Telecoms Research, "Mexico - Mobile Infrastructure, Broadband, Operators - Statistics and Analyses", 2019.5.21.

50. Buddecomm Telecoms Research, "Mexico - Telecoms Infrastructure, Operators, Regulations - Statistics and Analyses", 2019.5.21.
51. Buddecomm Telecoms Research, "Oman - Telecoms, Mobile and Broadband - Statistics and Analyses", 2019.5.6.
52. Buddecomm Telecoms Research, "Peru – Fixed Broadband Market - Statistics and Analyses", 2019.5.23.
53. Buddecomm Telecoms Research, "Peru - Mobile Infrastructure, Broadband, Operators - Statistics and Analyses", 2019.5.23.
54. Buddecomm Telecoms Research, "Peru - Telecoms Infrastructure, Operators, Regulations - Statistics and Analyses", 2019.5.23.
55. Buddecomm Telecoms Research, "Qatar - Telecoms, Mobile and Broadband - Statistics and Analyses", 2019.4.22.
56. Buddecomm Telecoms Research, "Romania – Fixed Broadband Market - Statistics and Analyses", 2019.3.13.
57. Buddecomm Telecoms Research, "Romania - Mobile Infrastructure, Broadband, Operators - Statistics and Analyses", 2019.3.13.
58. Buddecomm Telecoms Research, "Romania - Telecoms Infrastructure, Operators, Regulations - Statistics and Analyses", 2019.3.13.
59. Buddecomm Telecoms Research, "Rwanda - Telecoms, Mobile and Broadband - Statistics and Analyses", 2019.5.1.
60. Buddecomm Telecoms Research, "Saudi Arabia - Telecoms, Mobile and Broadband - Statistics and Analyses", 2019.5.6.
61. Buddecomm Telecoms Research, "Senegal - Telecoms, Mobile and Broadband - Statistics and Analyses", 2019.3.29.
62. Buddecomm Telecoms Research, "Thailand – Fixed Broadband Market - Statistics and Analyses", 2019.3.2.
63. Buddecomm Telecoms Research, "Thailand - Mobile Infrastructure, Broadband, Operators - Statistics and Analyses", 2019.3.2.
64. Buddecomm Telecoms Research, "Thailand - Telecoms Infrastructure, Operators, Regulations - Statistics and Analyses", 2019.3.2.
65. Buddecomm Telecoms Research, "United Arab Emirates - Telecoms, Mobile, Broadband

and Digital Media - Statistics and Analyses", 2018.10.10.
66. Buddecomm Telecoms Research, "United Kingdom – Fixed Broadband Market - Statistics and Analyses", 2019.3.18.
67. Buddecomm Telecoms Research, "United Kingdom - Mobile Infrastructure, Broadband, Operators - Statistics and Analyses", 2019.3.18.
68. Buddecomm Telecoms Research, "United Kingdom - Telecoms Infrastructure, Operators, Regulations - Statistics and Analyses", 2019.3.18.
69. Buddecomm Telecoms Research, "USA – Fixed Broadband Market - Statistics and Analyses", 2019.4.14.
70. Buddecomm Telecoms Research, "USA - Mobile Infrastructure, Broadband, Operators - Statistics and Analyses", 2019.4.14.
71. Buddecomm Telecoms Research, "USA - Telecoms Infrastructure, Operators, Regulations - Statistics and Analyses", 2019.4.14.
72. Buddecomm Telecoms Research, "Vietnam – Fixed Broadband Market - Statistics and Analyses", 2019.5.29.
73. Buddecomm Telecoms Research, "Vietnam - Mobile Infrastructure, Broadband, Operators - Statistics and Analyses", 2019.5.29.
74. Buddecomm Telecoms Research, "Vietnam - Telecoms Infrastructure, Operators, Regulations - Statistics and Analyses", 2019.5.29.
75. Channel News Asia, "Almost 20,000 medical records of Malaysian patients found to be freely available online", 2019.9,18.
76. CISION PR News, "Vietnam Cyber Security Market is Expected to Reach about USD 215 Million in Terms of Revenue by the Year Ending 2023: Ken Research," 2019.9.2.
77. CNBC, "How Cambodia is using blockchain for payments", 2019.10.22.
78. CNBC, "Self-driving trucks likely to hit the roads before passenger cars", 2019.11.22.
79. Connecting Bristol, "Bristol launches new Smart City Strategy", 2019.9.12.
80. CyberSecurity Malaysia, "Staying ahead of emerging security challenges in digital industrial revolution - Malaysia's perspective", 2019.5.16.
81. DCMS, "Secure by Design: Improving the cyber security of consumer Internet of Things Report", 2018.3.7.
82. DCMS, "UK Cyber Sector Report", 2018.6.

83. Digital News Asia, CYBERSECURITY MALAYSIA WINS INTERNATIONAL COMPETITION, 2019.7.4.
84. Digital News Asia, "FUTURE OF CYBERSECURITY CONFERENCE TO ADDRESS INDUSTRY CHALLENGES", 2019.6.12.
85. Digital News Asia, KASPERSKY SET TO OPEN FIRST TRANSPARENCY CENTRE IN ASIAPAC IN CYBERJAYA, 2019.8.19.
86. Digital News Asia, "KPMG CYBER CHALLENGE 2019 TESTS UNDERGRADS IN REAL BUSINESS CASE SCENARIOS", 2019.9.27.
87. EC, "Communication on a Cybersecurity Strategy of European Union – An Open, Safe and Secure Cyberspace", 2013.2.7.
88. Economist Intelligence Unit, "Global Microscope 2019: The enabling environment for financial inclusion", 2019.
89. El Financiero, "Los ataques informáticos más frecuentes en Costa Rica", 2017.4.30.
90. ENISA, "ENISA threat landscape for 5G Networks", 2019.11.21.
91. export.gov, "Dominican Republic - Safety and Security Equipment", 2019.11.21.
92. export.gov, "United Kingdom - Cyber-Security", 2019.8.1.
93. FedScoop, "Trump's cybersecurity budget emphasizes DOD while spreading cuts elsewhere", 2019.3.18.
94. Focus Malaysia, "ASIACYBERX offers RM 200M to local talent", 2019.4.19.
95. Frost & Sullivan, "Digital Market Overview; Indonesia", 2018.5.25.
96. Garcia & Bodan News, "Cybercrimes in El Salvador", 2017.9.7.
97. Gov.UK, "Civil Nuclear Cyber Security Strategy", 2017.2.14.
98. Gov.UK, "Guidance launched for in-house monitoring centres", 2018.10.24.
99. Gov.UK, "National Cyber Security Strategy 2016 to 2021", 2016.11.1.
100. Gov.UK, "New fines for essential service operators with poor cyber security", 2017.8.8.
101. Gov.UK, "Surveillance camera guidance, tools and templates", 2018.10.3.
102. Governor Bank of Tanzania, "Monetary Policy Statement 2017/18", 2017.6
103. HM Treasury, "Chancellor speech: launching the National Cyber Security Strategy", 2016.11
104. Homeland security research, "UK Homeland Security & Public Safety Market – 2017-2022", 2017.5.

105. I-Scoop, “IoT 2019: spending, trends and hindrances across industries”, 2019.6.
106. International ICT Policy in East and Southern Africa and Privacy International, "The Right to Privacy in the United Republic of Tanzania", 2015.9
107. IDC, “Market Analysis Perspective: India Security Software Market 1H18 Update”, 2019.3.
108. IDC China, “IDC：多因驱动， 2018年中国IT安全软件市场持续高增长”, 2019.5.29.
109. IDC China, “IDC：突破瓶颈， 2018年中国IT安全硬件市场规模再创历史新高”, 2019.4.2.
110. ITSP Magazine, “Accelerating Cyber Security For A Safer Indonesia | ISS 2019”, 2019.9.4.
111. ITU, "Global Cybersecurity Index (GCI) 2018", 2019.3.
112. ITU, “Measuring the Information Society Report 2015”, 2015.12.
113. ITU, "Measuring the Information Society Report 2018", 2018.12
114. Journal of ASEAN Studies, "Cybersecurity Policy and Its Implementation in Indonesia", 2016.8.9
115. J.P. Morgan, "J.P. Morgan CIO Survey 2019 - Shifting Center of Gravity", 2019.6.
116. Jusfoun, "China IT Security Services Industry on Market Segment", 2017.2.10
117. Kable, "Indonesia's ICT Spends - Future Perspective to 2019", 2016.8
118. Kable, "United States's ICT Spends - Future Perspective to 2019", 2016.8
119. Ken Research, "China Electronic Security Market Outlook to 2019", 2015.7
120. Ken Research, "India Cyber Security Market Outlook to 2020", 2016.5
121. Ken Research, "India Electronic Security Industry Potential to 2020", 2016.6
122. Khmer Times, “Singaporean company plans to build smart city in Cambodia”, 2019.8.19.
123. La Republica, “Álvarez y Castro reducirían déficit fiscal eliminando el crimen”, 2017.10.17.
124. legislation.gov.uk, “Automated and Electric Vehicles Act 2018”, 2018.7.19.
125. legislation.gov.uk, “Data Protection Act 1998(Revised)”, 2018.12.17.
126. legislation.gov.uk, “The Network and Information Systems Regulations 2018”, 2018.4.19.
127. legislation.gov.uk, “Investigatory Powers Act 2016”, 2016.11.29.
128. LifeWire, “Are Self-Driving Cars Legal in Your State?”, 2019.11.17.
129. london.gov.uk, “Smarter London Together”, 2018.6.
130. Marcomm, “UNV Targetkan Pangsa Pasar CCTV 20% di 2019”, 2019.5.10.
131. MarketsandMarkets, "Artificial Intelligence in Cybersecurity Market – Global Forecast to 2026", 2019.5.
132. MarketsandMarkets, "Cybersecurity Market – Global Forecast to 2022", 2018.9.

133. MarketsandMarkets, "IoT Security Market – Global Forecast to 2023", 2019.4.
134. MarketsandMarkets, "Physical Security Market – Global Forecast to 2023", 2019.8.
135. MarketsandMarkets, "Security as a service Market – Global Forecast to 2023 – Global Forecast to 2023", 2019.2.
136. MarketLine, "Security Services in the United Kingdom", 2015.11.25
137. MarketLine, "Software in Indonesia", 2017.6
138. MICITT, "Plan Nacional de Ciencia, Tecnología e Innovación 2015-2021", 2015.2.
139. Microsoft, "Microsoft Security Intelligence Report, Volume 24: July through December, 2018", 2019.2
140. Ministry of International Trade and Industry(MITI), "Industry4WRD, National Policy on Industry 4.0", 2018.
141. Morgan Stanley, "2Q19 CIO Survey: Still Solid Growth, But Cracks May Be Starting to Show", 2019.7.11
142. Morgan Stanley, "Software Finding Pockets of Opportunities Across 4Q18 Security Earnings", 2019.1.23.
143. NIST, "Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks", 2019.6.
144. NCCoE, "Mitigating IoT-Based DDoS", 2019.4.
145. NCSC, "Increased Cyber Threats: Security steps to take" 2018.5.16.
146. NST Business, Malaysia IT spending to reach RM65b in 2019, 2018.11.13.
147. Organization of American States & Inter-America Development Bank, "2016 Cybersecurity Report: Cybersecurity, Are We Ready in Latin America and the Caribbean?", 2016.
148. Oxford Business Group, "Country Profile - Colombia", 2016.2.24
149. Oxford Business Group, "Country Profile - Ethiopia", 2017.5.15
150. Oxford Business Group, "Kenya Economy", 2016.1
151. Oxford Business Group, "Oman ICT", 2017.2
152. Oxford Business Group, "Qatar Trade & Investment", 2016.7
153. Oxford Business Group, "UAE Security, Aerospace & Defence", 2017.5.14
154. Piper Jaffray, "2019 CIO Survey IT Budgets Growing; Priorities", 2019.1.3.
155. PrWeb, "Dropsuite and Mat Bao Join Forces in Southeast Asia to Partner On Data Protection", 2018.6.25.

156. PwC, "Creating cyber secure smart cities", 2018.9.
157. Red Piranha, "Red Piranha signs US$5 Million Cyber Security capability partnership at Indonesia-Australia Free Trade Agreement Signing ceremony", 2019.3.4.
158. Reuters, "Indonesia looks to blockchain to fix its dodgy data challenges", 2018.5.4.
159. Saigoneer, "베트남 최초의 자율주행 자동차 프로젝트, 파일럿 단계 시작", 2018.7.9.
160. Serianu, "Kenya Cyber Security Report 2015", 2016.3
161. Statista, "Frost & Sullivan Indonesia Market Tracker", 2018
162. Statista, "Smart Home Report 2019 – Security", 2019.4.
163. Strategic Defence Intelligence, "Homeland Security Expenditure in Oman to 2020: Market Review", 2016.3
164. Strategic Defence Intelligence, "Indonesia Defense Spends on Homeland Security: 2016 to 2025", 2016.8
165. Strategic Defence Intelligence, "Qatar Defense Spends on Homeland Security: 2016 to 2025", 2016.8
166. Strategic Defence Intelligence, "Saudi Arabia Defense Spends on Homeland Security: 2016 to 2025", 2016.8
167. Strategic Defence Intelligence, "Thailand Defense Spends on Homeland Security: 2016 to 2025", 2016.8
168. Strategic Defence Intelligence, "The Cyber Security Market in the China to 2025: Market Profile", 2016.3
169. Strategic Defence Intelligence, "The Cyber Security Market in the India to 2025: Market Brief", 2016.3
170. Strategic Defence Intelligence, "The Cyber Security Market in the Saudi Arabia to 2025: Market Profile", 2016.3
171. Strategic Defence Intelligence, "The Cyber Security Market in the United Kingdom to 2025: Market Brief", 2016.3
172. Strategic Defence Intelligence, "The Cyber Security Market in the United States to 2025: Market Profile", 2016.3
173. Strategic Defence Intelligence, "The Oman Defense Industry - Competitive Landscape and Strategic Insights to 2020: Market Profile", 2016.3
174. Strategic Defence Intelligence, "The Oman Defense Industry - Industry Dynamics to 2020:

Market Profile", 2016.3
175. Strategic Defence Intelligence, "The Oman Defense Industry - Market Attractiveness and Emerging Opportunities to 2020: Market Profile", 2016.3
176. Strategic Defence Intelligence, "United States Defense Spends on Homeland Security 2016 to 2025", 2016.8
177. TechCrunch, "Waymo is bringing its self driving trucks back to Arizona", 2019.5.30.
178. TechWorld, "The UK's 13 most promising cybersecurity startups", 2017.7.11.
179. Tempo.com, "Kominfo Preps Draft Bill on Personal Data Protection, 2019.5.17.
180. The Asian Post, "Hoax busters: Fighting fake news in Indonesia", 2019.4.9.
181. The Conversation, "Indonesia needs to fix 'authoritarian' clauses in bill on cyber security before passing it into law". 2019.9.4.
182. The Phnom Penh Post, "VN e-commerce booming but hard to control", 2019.9.22.
183. The Star Online, "MDEC launches comeback career programme for more women to join cybersecurity sector", 2019.6.20.
184. The Sundaily, "CSM-ACE the right platform to address cyber security issues: Gobind", 2019.9.23.
185. The White House, "24. CYBERSECURITY FUNDING", 2019.3.18.
186. Tribunn News, "Empat Rekomendasi Teknologi Keamanan Canggih untuk Ibu Kota Baru dari ATISI", 2019.8.8.
187. UBS, "China Software and Service - How will software companies evolve in the age of SMAC", 2017.1.10.
188. U.S. OSAC, El Salvador 2019 Crime & Safety Report, 2019.4.25.
189. UK Cabinet Office, "The UK Cyber Security Strategy 2011-2016: Annual Report", 2016.4
190. UK Department for Culture, Media & Sport, "Cyber Essentials scheme research", 2016.12
191. UK Department for Culture, Media & Sport, "Cyber Security Regulation and Incentives Review", 2016.12
192. UK Department for Transport, "The key principles of vehicle cyber security for connected and automated vehicles", 2017.8.6.
193. UNCTAD, "B2C e-Commerce Index 2018 Focus on Africa", 2018.12.
194. VIA News, "Take a Selfie and Open a Bank Account in El Salvador", 2019.6.19.
195. Viet Nam News, "e-Gov't focuses on cyber security", 2018.8.17.

196. Viet Nam News, "Việt Nam ready to embrace Industry 4.0", 2019.10.4.
197. Vietnam e-Commerce Association, "Vietnam E-Business Index 2019 Report", 2019.
198. Vnexpress, "Spyware attacks half a million plus computers in Vietnam", 2018.7.27.
199. Vnexpress, "Vietnam loses $542 million to cyber viruses in 2017", 2018.1.2.
200. Vnexpress, "Virus alert: 80 percent of USBs in Vietnam are infected", 2018.6.14.
201. VNISA, "HCM City becomes first locality in Vietnam to get 5G service", 2019.9.23.
202. VNISA, "Over 10,000 cyber-security vulnerabilities found in government agencies", 2019.9.30.
203. VOV,"Vietnam hosts 2018 ASEAN-Japan cyber security", 2018.5.24.
204. WaveStone, "2018 UK Cybersecurity Start-Up Radar", 2018.11.5.
205. yStats.com, "Africa B2C E-Commerce Online Payment Market 2019", 2019.6.24.
206. yStats.com, "Global B2C E-Commerce Delivery 2018", 2018.12.14.
207. yStats.com, "Global Alternative Online Payment Methods 2019", 2019.3.5.
208. yStats.com, "Fraud and Security in Global Online Payments 2019", 2019.7.5.
209. yStats.com, "Global Digital Payment Forecast 2019-2022", 2019.5.31.
210. yStats.com, "Global M-Commerce 2018", 2018.12.6.
211. yStats.com, "Global Mobile Payment Forecast 2019-2022", 2019.5.16.
212. yStats.com, "Global Mobile Payment Methods 2019", 2019.3.8.
213. yStats.com, "Global Mobile Wallet 2019", 2019.3.29.
214. yStats.com, "Global Online Payment Methods 2019", 2019.3.1.
215. yStats.com, "Indonesia B2C E-Commerce Online Payment Market 2019", 2019.8.1.
216. yStats.com, "Latin America B2C E-Commerce Market 2018", 2018.11.2
217. yStats.com-, "Saudi Arabia B2C E-Commerce Market 2019", 2019.4.16.
218. yStats.com, "Thailand B2C E-Commerce Online Payment Market 2019", 2019.8.5.
219. yStats.com, "UAE B2C E-Commerce Market 2019", 2019.4.9.
220. yStats.com, "USA Online Payment Methods 2019", 2019.4.12.
221. 中国互联网络信息中心(CNNIC), "中国互联网络发展状况统计报告", 2019.8.
222. 中国网(중국망신문중심), "베이징 대형병원, 3년 내 진찰까지 대기 시간 30분 이내로 줄일 것", 2018.5.7.
223. 富士経済, "監視カメラ、アクセスコントロールシステム、緊急通報サービス、災害・防災関連機器/サービスなど国内のセキュリティ関連機器 ・システム 、サービスの市場を調査",

2018.11
224. 日本ネットワークセキュリティ協会(JNSA), "2018年度 国内情報セキュリティ市場調査", 2019.6.12.
225. サイバーセキュリティ戦略本部, "重要インフラにおける情報セキュリティ確保に係る安全基準等 策定指針", 2018.4.4.
226. 内閣官房, "未来投資戦略 2017", 2017.6.9.
227. 건축도시공간연구소 스마트·녹색연구단, "스마트도시 해외사례 및 주요기관: 런던 스마트도시 관련 정책·제도(2019)", 2019.9.17.
228. 과학기술정보통신부, "2018 국내 정보보호산업 실태조사", 2019.1.
229. 과학기술정보통신부, "과기정통부, 중미 엘살바도르에 정보접근센터 개소", 2018.12.20.
230. 대한무역투자진흥공사, "라오스 핀테크 산업동향", 2019.11.11.
231. 대한무역투자진흥공사, "美, 대중교통 시스템에 자율주행차 도입 속도 낸다", 2019.11.28.
232. 대한무역투자진흥공사, "베트남, 현금없는 미래를 꿈꾸다", 2019.6.25
233. 대한무역투자진흥공사, "베트남 스타트업 화두는 "Tech"", 2019.8.22.
234. 대한무역투자진흥공사, "사이버 공격을 막아라! 영국 사이버 보안시장 동향", 2018.11.28.
235. 대한무역투자진흥공사, "英, 국가안보 관련 산업 보호 움직임", 2018.10.11.
236. 대한무역투자진흥공사, "지금 주목할 만한 일본 스타트업은?", 2019.9.5.
237. 대한무역투자진흥공사, "캄보디아 모바일 결제시장, 치열한 경쟁 속 무서운 성장세", 2018.9.18.
238. 세계도시정보 UBIN, "런던시의 스마트시티 계획 2018", 2018.12.
239. 보안뉴스, "올해 中 IT보안 지출 약 70억 달러...연평균 25% 이상 전망", 2019.4.17.
240. 보안뉴스, "한국 전자정부, 베트남 시작으로 신남방지역 본격 진출", 2018.5.25.
241. 삼성SDS, 동남아 진출 박차...베트남 IT기업에 500억 투자, RayThe, 2019.5.27.
242. 아시아경제, "[신남방을가다⑪] "말레이 스타트업 최고 관심은 소비자"", 2018.6.15.
243. IT조선, "KB국민은행, 캄보디아 핀테크 업체와 MOU 체결", 2019.3.17.
244. 연합뉴스, "DGB금융, 캄보디아 핀테크 업체와 MOU...금융서비스 현지화", 2019.8.1.
245. 유안타증권, "중국 IT보안시장 분석", 2016.10.4
246. 유안타증권, "중국, 사이버보안 강국으로 성장 기대", 2016.4.5.
247. 잇츠데일리, "인도네시아, 공공 및 민간 부문에서 블록체인 용도 연구", 2018.5.7.
248. 조선일보, "블록체인은 어떻게 인니 빈농의 삶을 바꿨을까", 2019.8.13.
249. 중앙Sunday, "원격의료 46조원 시장, 미·일·중은 족쇄 풀고 육성 한창", 2018.8.4.

250. 로봇신문, "베트남 FPT, 일본 야마하와 제휴해 자율주행차 개발한다", 2019.4.12.
251. 한겨레, "자율주행차 상용화 세계 첫 '시동', 어디까지 달릴까", 2018.12.9.
252. 한국경제, "美 구글 자율車 지구 400바퀴 돌때...韓은 규제·기득권 막혀 '공회전'", 2019.10.9.
253. 한국경제매거진, "'낡은 도시'를 똑똑하고 안전하게...영국의 스마트 시티 실험", 2018.5.23.
254. 한국국제협력단, "코이카, 엘살바도르 주민 삶 개선 위한 치안 사업 추진", 2019.5.24.
255. 한국무역협회, "미국 스타트업 동향과 시사점", 2019.2.
256. 한국인터넷진흥원, "2013 글로벌 정보보호산업 동향조사 보고서", 2013.12.
257. 한국인터넷진흥원, "2018 글로벌 정보보호 산업시장 동향 조사", 2019.2.
258. 한국인터넷진흥원, "영국, 민간 원자력 사이버보안 전략 발표", 2017.3.20.
259. 한국인터넷진흥원, "정보보호 해외진출 전략거점 1월 주요동향", 2019.2.12.
260. 한국인터넷진흥원, "중남미 권역 사이버보안 역량강화 세미나 개최", 2019.4.26.
261. 한인포스트, "자카르타 교통국 인공지능 CCTV 카메라 설치", 2019.7.3.

참고DB

1. CIA, The World Fact Book(www.cia.gov)
2. Google Finance(www.google.com/finance)
3. IMF Data(www.imf.org/external/data.htm)
4. ITU Statistics(www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx)
5. Statista(www.statista.com)
6. UN Comtrade(https//comtrade.un.org)
7. Wikipedia(www.wikipedia.org)
8. 대한무역투자진흥공사(KOTRA) 해외시장 뉴스(http://news.kotra.or.kr)
9. 한국무역협회 무역통계(www.kita.net)