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)

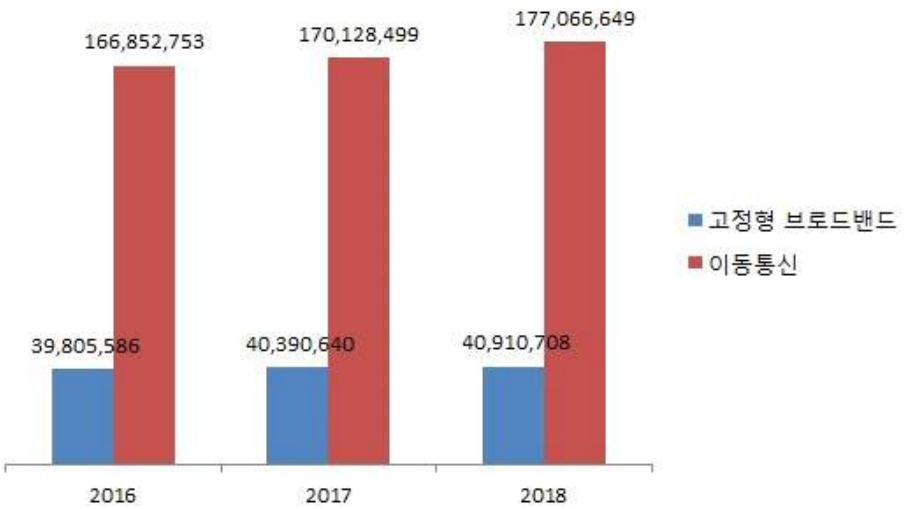
- 일본의 고정형 브로드밴드 가입 회선 수는 매년 미미한 증가세를 보이며 포화 상태에 근접 중
- ITU에 따르면, 2018년 말 일본 브로드밴드 인터넷 가입 회선 수는 4,091만 708회선으로 전년 대비 1.3% 증가
- 일본은 지진, 태풍 등 자연재해가 잦은 지리적·환경적 요인으로 인해 유선 대비 이동통신에 대한 기술 의존도가 높으며, 향후 이동통신 중심으로 투자가 확대될 것으로 예상

▶ 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[1]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

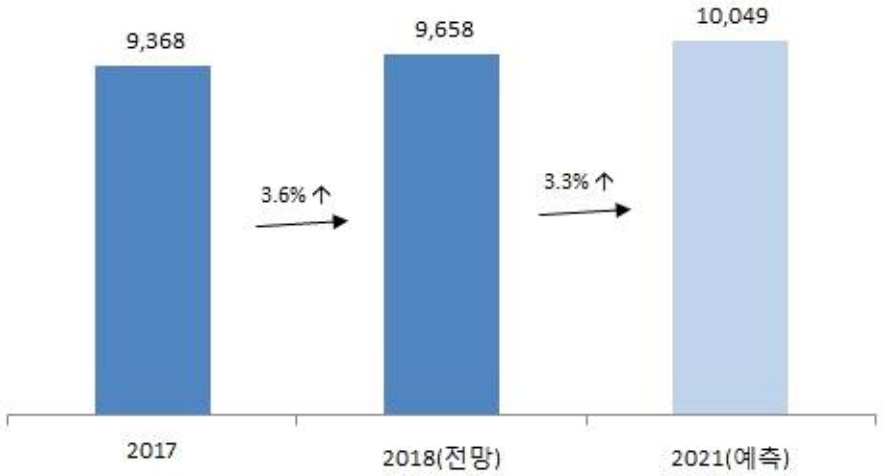
1 富士経済, 監視カメラ・アクセスコントロールシステム・緊急通報サービス・災害・防災関連機器/サービスなど国内のセキュリティ関連機器・システム・サービスの市場を調査, 2018.11

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

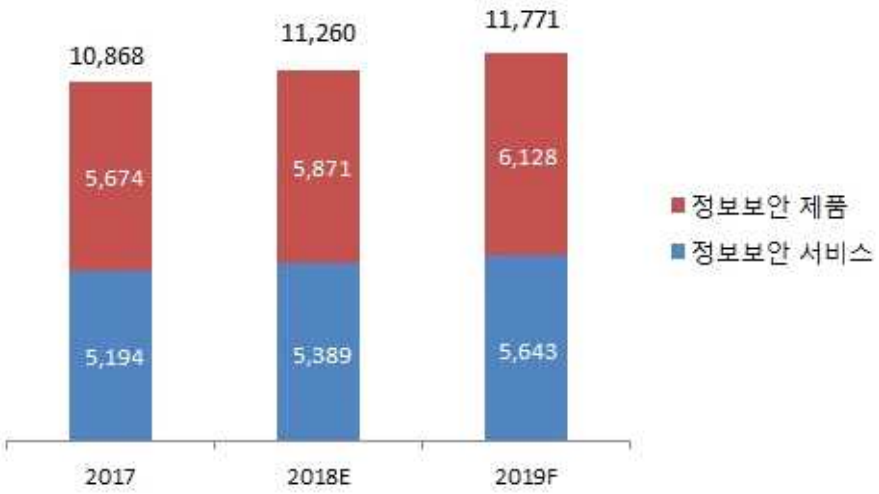
특수는 예상을 밑돌고 있는 상황으로, 향후 동영상 해석, AI, IoT 등의 기술혁신을 통한 새로운 분야에서의 수요 개척을 기대

▶ 일본네트워크보안협회(JNSA)가 일본 내 정보보안 제품과 서비스를 제공하는 사업자를 대상으로 한 조사[2]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

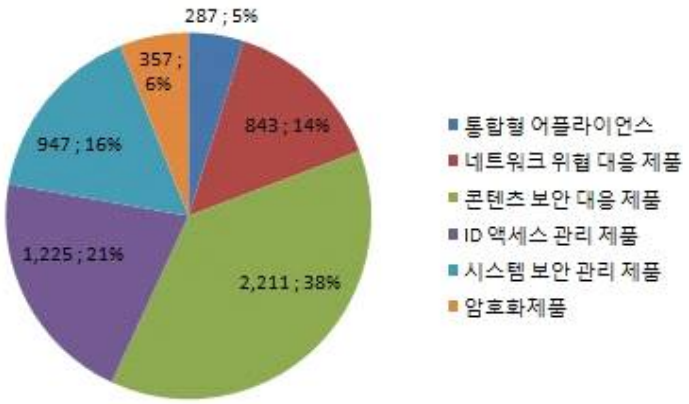
2 日本ネットワークセキュリティ協会(JNSA), 2018年度 国内情報セキュリティ市場調査, 2019.6

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

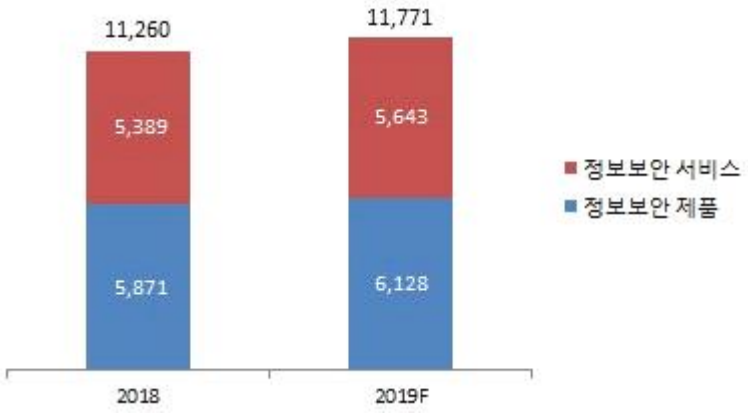
그림 _ 2019년 일본 정보보안 서비스 시장 구성 추산치

(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[3]

3 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[4]

4 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[5]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)

5 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