

## 가. 미국

'17년 GDP(십억달러)	19,390.60
'17년 인구수(천명)	325,719

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

· 미국은 법, 조직, 기술, 역량 강화 부문에서 최상위 수준이며 국제협력 부분은 상대적으로 낮은 수치를 나타냄

(● 상, ● 중, ● 하)

국가명	2017 GCI 지수 및 순위		5대 하위 항목 평가					종합
	지수	순위	법제	기술	조직	역량	협력	
미국	0.919	2	●	●	●	●	●	●
대한민국	0.782	13	●	●	●	●	●	●

### ■ ICT 관련 주요 지수

· 미국의 전반적인 ICT 발전 수준은 전 세계 상위 약 10% 이내에 속함

지표명	미국		한국	
	점수	순위	점수	순위
ITU ICT 발전지수(IDI 2017)	8.18	16	8.85	2
접근(Access) 부문	8.27	17	8.85	7
활용(Use) 부문	7.67	20	8.71	4
기술(Skills) 부문	9.05	3	9.15	2
ITU 글로벌 사이버보안 지수(GCI 2017)	0.919	2	0.782	13
UN 전자정부 지수(2018)	0.877	11	0.901	3

### ■ ICT 관련 주요 통계(ITU, 2017년 말 기준)

· 미국의 이동통신 보급률은 약 122% 수준이며 이 중 LTE 보급률은 70%대에 이룸

항목	미국		한국	
	가입자수(천 명)	보급률(%)	가입자수(천 명)	보급률(%)
유선전화	119,902	36.9	26,842	52.6
유선브로드밴드	109,838	33.8	21,195	41.5
이동통신	395,881	122.0	63,658	124.8
인터넷 이용률	76.18%		95.1%	

## 정보보호 산업 개요

### 1. 보안 환경

#### 정보보안 환경

- ▶ ITU 2017 'Global Cybersecurity Index(GCI)'에 따르면 미국의 사이버보안 지수는 0.919로 싱가포르에 이어 2위를 기록했으며, 미주 권역에서 압도적인 1위를 기록
  - 해당 지수는 법적·기술적·조직적 대응 및 역량 강화, 국제협력 등 5개 부문의 지수를 종합한 것으로, 미국은 법적·기술적 및 조직적 대응, 그리고 역량 강화 면에서 골고루 높은 점수를 기록
  - 특히 법적 대응과 역량 강화 측면에서는 만점을 나타내고 기술적 및 조직적 대응 지수도 1.0 만점에 0.9 이상을 기록하는 등 국제협력을 제외한 전 부분에서 고른 발전 수준을 과시
  
- ▶ 트럼프 행정부는 2018년 3월 러시아가 미국 전력시설을 목표로 지난 2년간 사이버 공격 캠페인을 지속해온 것에 대해 러시아 정부를 비판하고 처음으로 모스크바를 공개적으로 고발함(2018.3)
  - US-CERT는 미국 국토안보부(DHS)와 연방수사국(FBI)이 합동기술경보(joint Technical Alert)팀을 구성해 분석한 결과, 러시아 정부가 미국 정부시설뿐만 아니라 에너지·핵·수력·항공 시설과 핵심 제조업을 겨냥해 공격을 펼치고 있다고 경고함
  - DHS와 FBI는 다단계로 설계된 침투 캠페인이라는 사실이 이번 공격에서 특이할 만한 점으로 이른바 '사이버 킬 체인(Cyber Kill Chain)'이라고도 하며 러시아의 정부 지원 해커들은 소규모 상업시설의 네트워크에 멀웨어를 설치한 뒤 스피어 피싱을 수행하고 추후 에너지 부문 네트워크까지 원격 접근함
  
- ▶ 미국은 세계적으로 사이버 범죄의 피해가 가장 큰 지역 중 하나이며, 이에 따라 정보보안에 대한 수요가 지속될 것으로 기대
  - 2017년 4월, Symantec 사이버 보안 리포트에 따르면, 2016년에 미국은 멀웨어, 스팸, 피싱 공격 등의 사이버 공격 진원지에서 23.96%로 글로벌 1위 국가로 밝혀짐
  - 사이버 공격 진원지 2위는 중국으로 9.63%, 3위는 브라질로 5.84%를 기록
  - NexusGuard DDoS 동향보고서에 따르면, 2016년 전 세계 2분기 DDoS 공격이 전 분기 대비 83%

증가한 159,704건을 기록한 가운데 미국은 76,462건을 기록하며 러시아와 중국에 이어 DDoS 발생국가 3위를 기록

▶ 보안업체 시만텍이 조사한 2017년 노턴 사이버보안 인사이트 보고서에 따르면 미국 인터넷 인구 절반 이상인 1억4천300만 명은 지난해 악성코드나 바이러스, 스파이웨어, 피싱 등과 같은 공격을 받음

- 글로벌 피해 규모는 1천720억 달러로 '17년 미국 피해액만 174억 달러에 달함
- 이러한 피해는 대부분 사용자가 비밀번호와 같은 기초적인 데이터를 부주의하게 관리한 실수에서 비롯됐으며 미국인 60%는 비밀번호 하나로 여러 기기와 온라인 사이트 계정에서 동일하게 사용하고 있는 것으로 나타남

### 물리보안 환경

▶ 미국 내 테러와 총기 난사 등의 범죄에 대한 경각심 고취, 기존의 보안제품 발달 및 가격 인하에 따른 수요 증가 등으로 보안시장 성장 및 수요 급등

- 학교, 병원, 쇼핑몰, 오피스 등의 상업 시설에 첨단화된 보안 시스템이 설치되고 관련 포럼, 박람회 등의 국제 행사도 꾸준히 증가
- 미국 정부의 공공 안전 관련 정보통신기술 예산 편성 증가

▶ 건설 및 주택 경기의 활성화와 교체 수요에 힘입어 물리보안 시장의 성장세가 이어졌으며, 테러 대응과 관련한 물리보안 강화의 필요성도 적지 않은 상황

- 강력 범죄 발생, 주택 및 상업 빌딩의 신규 건설, 경기 안정화에 의한 구매력 증가 등이 물리보안 시장의 확대에 영향을 미치는 요소들
- 물리보안 장비 시장의 성장은 주거용 건물보다는 주로 상업용 빌딩이나 공항, 해안, 도로 등의 수송 관련 보안 분야의 비중이 큰 편
- 미국 물리보안 시장의 매출은 장비 판매, 설치, 서비스, 호스팅 및 모니터링 서비스 등에서 발생
- 시장의 수요는 정부기관, 기업과 상업시설, 개인 등으로 구분되며 상업용 빌딩에 대한 물리보안 수요 점유율이 개인 수요보다 2배 이상 큰 시장이지만 미국 내 가정의 보안 카메라 보유가구는 14%에 이르는 등 시장 성장은 지속될 전망

## 2. 인터넷 및 통신 환경

### ▶ 유선통신

- 2017년 기준 미국의 유선통신 가입회선 수는 2016년 대비 1.4% 감소한 1억 190만 회선(보급률 36.7%)을 기록했으며 점차 감소하는 추세임
- 주요 통신사들은 광케이블 네트워크로 초고속 유선 통신 서비스를 제공하고 있으나 모바일 인터넷 사용자의 수가 증가함에 따라 시장의 성장 동력이 크지 않은 상태
- 주요 유선통신 사업자로는 AT&T, Verizon, Century Link Inc.가 있으며, 인터넷 접속(44.1%)과 음성 서비스(29.9%) 관련 사업 비중이 높은 편

그림 \_ 미국 유선통신 가입자 수와 보급률

(단위: 천 명)



[출처] ITU Statistics DB(2018.10)

### ▶ 브로드밴드

- 2017년 기준 미국의 브로드밴드 가입회선 수는 2016년 대비 3.6% 증가한 1억 934만 회선을 기록, 보급률 33.9%를 기록했으며 가입자는 점차 증가하는 추세임

그림 \_미국 브로드밴드 가입자 수와 보급률

(단위: 천 명)



[출처] ITU Statistics DB(2018.10)

▶ 이동통신

- 2017년 기준 미국의 이동통신 가입회선 수는 2016년 다소 감소한 3억 9,588만 회선을 기록, 보급률 122.0%를 기록함
- 한편 시장조사업체 Buddecomm에 따르면, 미국의 이동통신 시장에서는 AT&T Mobility 및 Verizon Wireless가 가입자의 70% 점유하고 나머지 30%는 T-Mobile US, C Spire, US Cellular 및 MVNO TracFone 등임
- Buddecomm 보고서에 따르면, 미국의 Mobile-Only 가구는 2008년 18%에서 2017년 49%로 증가함
- 미국 통신사들은 최근 몇 년간 LTE 및 5G 기술로 이동하고 있으며 통신사 간 경쟁으로 몇몇 통신사에서 LTE 커버리지는 97%에 달함
- 미국 무선산업연합회는 2022년까지 미국 모바일 가입자의 25%가 5G 네트워크로 옮겨갈 것으로 전망

그림 \_미국 이동통신 가입자 수 및 보급률

(단위: 천 명)



[출처] ITU Statistics DB(2018.10)

## 정보보호 시장 현황

### 1. 시장 규모

#### 시장 개요

- ▶ 미국의 정보보호 산업 규모는 세계 최고 수준을 유지하고 있으며, 특히 미국 정부의 투자도 적극적으로 이루어짐
  - 글로벌 보안시장 전문 조사기관 Strategic Defence Intelligence(이하 SDI)에 따르면, 2024년까지 미국을 포함한 북미 정보보호 시장의 규모가 전 세계 시장의 50% 가량을 차지할 것으로 전망
- ▶ 미국의 정보보안 시장은 세계 최대 규모이며, 민간과 정부 부문에서 모두 활발한 투자를 진행하며 꾸준하게 성장
  - 미국 정보보안 시장은 전 세계 시장의 약 1/3 이상을 차지할 만큼 규모가 크고 IT 분야별 주요 사업자들이 대거 진입해 활약
  - 미국의 정보보안 시장에서 정부가 대규모 수요를 형성하고 있으며, 사이버 공격에 대한 정부 예산은 국방부(DoD), 국토안보부(DHS)를 중심으로 집행
- ▶ 미국 시장에서 보안 서비스 분야는 전체 보안 시장의 큰 부분을 차지하고 있으며, 실행, 평가 및 아키텍처 디자인을 포함한 애플리케이션 및 무선 보안 솔루션 등의 수요 증가가 시장을 강하게 견인
  - 미국 정보보안 장비 시장은 장비 출하량과 매출이 10% 가량의 성장세를 보이고 있는 것으로 추정되며, 미국을 겨냥한 보안 위협 증가로 방화벽, 가상사설망 (VPN) 등의 수요증가가 원인으로 분석
  - 보안 솔루션 가운데 안티바이러스, 이메일 보안 등에서 지속적인 신제품 출시가 이루어지고 있으며, 취약성 관리와 빅데이터 등 신기술을 적용한 정보 제공 및 이벤트 관리 (SIEM, Security Information & Event Management) 기반의 보안관제 서비스 등의 분야도 성장세
- ▶ 미국의 물리보안 시장은 보안 제품, 생산 및 유통 업체 등이 제품 및 서비스에 따라 혼재되어 시장이 여러 분야로 구분
  - 미국 내 보안장비 시스템 관련 업체는 경비, 알람 모니터링, 제품 설치 서비스 제공 업체까지 모두

- 포함할 경우 약 총 5,000여 개를 상회
  - 최근 수 년 동안 이 분야에서 업체 간의 활발한 인수합병이 이루어졌음에도 불구하고, 전반적으로 미국 물리보안 산업은 매우 세분화 되어있는 편
  - 완성품 제조업체 기준으로 약 300개의 업체가 경쟁하고 있으나 기술 집약적인 보안 제품군에서는 소수 업체에 집약된 시장 구조를 보이는 것이 특징
  - 한편, 물리보안 장비 업체들의 매출 형태는 보안 장비 판매, 보안 장비 임대 및 모니터링 서비스에서 발생하는 가입자형 월별 서비스 매출 등으로 구성
- ▶ 미국의 물리보안 시장에서는 고객 대상 보안서비스를 제공하는 기업이 보안 장비에 대한 수요가 가장 많은 편이며, 물리보안 제품의 유통은 전문 도매업체들을 중심으로 하되 다양한 거래 유형이 혼재되어 있는 상황
- 생산된 제품은 시장에서 주로 전문 도매 유통업체나 유통 딜러에게 공급되며 일부는 OEM 생산자와 공급자간의 계약을 통해 판매
  - 전문 도매 유통업체는 수많은 로컬 딜러 및 시스템 통합업체와 거래하며, 다양한 제품을 취급하는 로컬 딜러들은 최종 소비자에게 제품을 공급
  - 제품생산 업체가 설치 업체나 최종 소비자에게 직접 제품을 공급하는 경우도 있으며, 특히 제품이 복잡하거나 기술 지원이 필요한 경우에는 생산 업체가 보안 제품을 직접적으로 설치 업체에 판매

표 \_ 미국의 물리보안 시장 구분 및 업체 구성

구분	업체
부품공급	제품 부품 및 소프트웨어 공급업체
생산	보안 시스템 생산자
유통총판	보안 시스템 전문 도매 유통업체
유통채널	딜러, 지역별 시스템 연동업체
사용자	가정, 산업, 정부 등의 실제 사용자
컨설팅	사용 그룹에 제품공급 방식 및 제품 컨설팅

[출처] Ken Research, 'The US Electronics Security Industry Outlook to 2017'(2013.6)

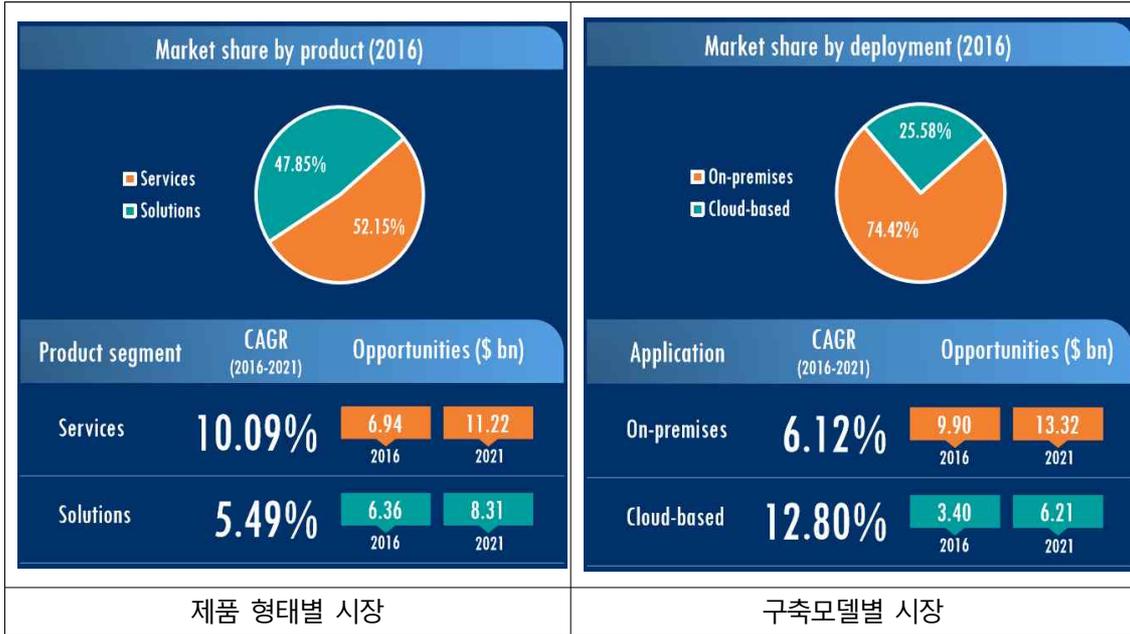
### 시장 규모 및 전망

- ▶ 글로벌 시장조사기관인 MarketsandMarket에 따르면, 2016년 세계 전체 보안시장의 규모는 2,475억 달러로, 2021년에 이르러 4,565억 달러까지 성장할 것으로 전망함

- 2017년 미국 보안시장은 317억 달러 규모로 예측되고, 전 세계 시장의 약 18% 이상을 차지하며 꾸준히 증가할 것으로 예상됨
  - 시장조사 전문기관 Frost & Sullivan에 따르면 2020년까지 북미지역 지방자치 기관의 공공안전 부문의 ICT 관련 예산 편성이 100억 달러를 초과할 것으로 분석
- ▶ 글로벌 마켓 리서치 전문기관 Market Research Media에 따르면, 미국 연방정부의 사이버보안 예산은 연평균 4.4% 성장해 2022년까지 220억 달러에 달할 것으로 전망함
- 미국 대통령 예산안에 따르면, 행정부가 연간 의회에 요청하는 사이버보안 관련 예산(2017년 기준)은 총 190억 달러로 매년 급증하고 있음
  - '17년 연방정부가 미국 전체 정보보호 시장의 약 60%인 143억 달러 시장을 차지하고 있으며, 이는 전 세계 정보보호 시장의 12.8%를 차지함
  - 또한 미국 연방정부 부처가 구매하는 사이버보안 제품/서비스 수요는 2015년 86억 달러에서 2020년까지 110억 달러로 성장(연평균 5.2%)할 것으로 예상(미국조달시장 조사기관 Deltek 보고서)되며 분야별로는 네트워크 보안 수요 비중이 40% 수준으로 가장 높고, 다음으로 데이터 보안(25%), IAM(19%), 클라우드 보안(15%) 등 순임
  - 또한, 연방정부 사이버보안 관련 지출의 64.4%인 총 6.9억 달러가 워싱턴 광역 지역(버지니아, 메릴랜드 주)에서 집행됨으로써, 이 지역이 사이버보안 분야 정부 지출의 특수를 누리고 있는 것으로 파악됨
  - 사이버보안 관련 벤처 투자가 캘리포니아 또는 보스턴 지역에 집중되고 있는 반면, 연방정부 기관을 배후에 두고 있는 워싱턴 광역지역이 공공 수요가 높은 사이버보안 산업의 새로운 메카로 각광 받고 있음
- ※ 미 주요 연방기관별 시장 점유율 : US Intelligence 기관 : 50.45% / DoD : 33.38% / DoD : 16.17%(16), AI 기반 금융 상품의 확산, 금융 시장의 새로운 성공 요건 제시



그림 \_미국 정부 기관의 보안제품 형태 및 서비스 현황



[출처] KISA 북미거점센터(2018.9)

- 보안솔루션 및 서비스를 연방정부 기관에 납품하기 위해서는 매우 엄격한 요건을 갖추어야 하며 영업을 위해서 인적 네트워크, 활용이 매우 중요
    - ※ 연방정부와 거래하는 대부분의 보안 솔루션 및 서비스 기업들은 연방정부 기관, 군출신자를 고용함
  - 하지만, 진출하게 되면 매우 안정적으로 영업 가능하며, 상당히 좋은 가격으로 공급 가능하므로 한국기업은 현지 사업자와 파트너십 맺어 OEM 형태로의 진출을 꼭 모색해야 함
- ▶ 글로벌 보안시장 전문 조사기관 SDI에 따르면, 2016년 미국 국토 보안 지출은 320억 달러 규모로 2025년 351억 달러에 이를 전망임
- 동 기간의 연평균 성장률은 1.01%로 현 수준을 유지하는 수준임

그림 \_ 미국의 국토보안 지출 규모 추이 및 전망

(단위: 백만 달러)



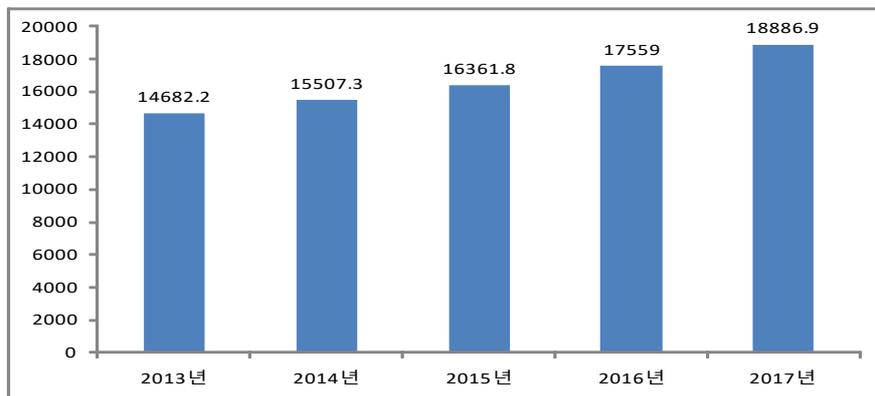
[출처] SDI, 'United States Defense Spends on Homeland Security(2016.8)

▶ 시장조사기관 Barnes & Co.의 조사에 따르면, 미국의 물리보안 시장 규모는 업체들의 매출 기준으로, 2015년 163억 6,180만 달러 규모에서 2016년 175억 5,900만 달러와 2017년 188억 8,690만 달러 규모로 확대될 전망

- 미국의 물리보안 시장은 지금까지와 비슷하게 꾸준하게 성장할 것으로 예상
- 미국은 단독주택의 주거 비율이 높아 주택 보안서비스의 수요 또한 많은 편이며, 최근에는 카메라와 경보 알람 등을 직접 설치하고자 하는 소비자들의 관심도 많아짐에 따라 DIY 제품의 수요도 증가
- 미국 물리보안 시장은 새로운 기술의 발전에 힘입어 양방향 커뮤니케이션을 비롯해 좀 더 진화된 기능을 가진 제품으로 향상된 보안 서비스를 제공하는 방향으로 발전

그림 \_ 미국 물리보안 시장의 성장 추이 및 전망(2013년~2017년)

(단위: 백만 달러)



- ▶ 미국 보안카메라 시장은 2019년 45억 6,000만 달러 규모로 전망됨
  - 미국 보안카메라 시장은 2014년 30억 8,000만 달러였으며, 2019년까지 연평균 10.3% 성장해 45억 6,000만 달러 규모 전망
  - 품목별로는 돔(Dome) 형태, 외부용, HD 보안카메라가 가장 큰 비중을 차지하며, 가장 높은 성장률 전망
  - 사무실과 상점에서는 오랫동안 보안카메라를 사용해왔으나, 주택부문의 수요가 크게 많아지고 있으며 특히 직접 설치가 가능한 제품들이 시장을 주도하고 있음
  - 2017년 CTA가 실시한 설문 조사에 따르면 이미 보안카메라를 가진 가구는 14%이고, 2017년 내로 구매할 계획이 있는 가구는 13%로 시장 성장은 계속될 전망
  - Parks Associates에 따르면 2020년 Wi-Fi가 연결된 보안카메라 설치 가구 비율이 24%가 될 전망

## 2. 분야별 현황

### 정보보안 제품 및 서비스 시장

- ▶ 세부 정보보안 제품에서는 네트워크 보안 비중이 전체의 57%로 가장 높고, 데이터 보안이 31%로 2위, 클라우드 보안 16%, 신원확인 및 접근 통제가 14%를 기록
  - SDI에 따르면, 미국의 네트워크 보안 시장 규모는 2015년 35억 달러를 기록했으며 2015년부터 2025년까지 누적 시장 규모는 489억 달러에 이를 것으로 전망
  - 데이터 보안 시장 규모는 2015년 14억 달러에서 2025년에는 18억 달러로 증가 전망
  - 2015년의 경우 네트워크 보안 시장과 데이터 보안 시장의 규모가 전체 정보보안 시장의 70% 이상으로 절대적인 비중을 차지
  - 반면, 2015년 8억 8,600만 달러 규모였던 인증 및 접근 제어 시장은 시장 규모가 점점 줄어들어 2025년까지 연평균 3.27%의 하락세를 기록할 것으로 예상

표 \_ 미국의 정보보안 분야별 시장 규모와 전망(2015년~2025년)

(단위: 십억 달러)

분야	2015년	2025년	누적시장규모 (2015-2025)	연평균증감률 (2015-2025)
네트워크 보안	3.5	4.8	48.9	3.32%
데이터 보안	1.4	1.8	22.0	2.73%
클라우드 보안	0.925	1.4	14.9	4.55%
인증 및 접근 제어	0.886	0.636	9.2	-3.27%
<b>합계</b>	<b>6.7</b>	<b>8.7</b>	<b>94.9</b>	<b>2.70%</b>

[출처] SDI, 'The Cyber Security Market in the United States to 2025'(2016.3)

▶ IBIS World에 따르면, 정보보안 제품의 수요처로는 기업용 보안 소프트웨어가 시장의 61.6%를 점유, 기업 내의 데이터 서비스 구축, 클라우드 기반의 정보 저장 및 데이터 보안 비용 등으로 지난 5년간 지속적으로 성장

- 직접 소비자에게 공급되는 보안 소프트웨어의 점유율이 시장의 29.1%를 차지함
- 정부와 공공기업의 점유율이 시장의 9.3%를 차지하고 시민의 개인 정보 기록, 기밀 정책 및 관련 서류 보안 소프트웨어가 주로 사용됨

▶ Barclays가 미국 CIO(Chief Information Officer) 대상으로 실시한 설문조사에 따르면, 7개의 보안 분야 중 지난 12개월간 가장 우선순위가 높은 분야는 71점을 획득한 엔드포인트 솔루션으로 나타남

- 엔드포인트 보안, 인증 및 접근제어, 보안정보 및 이벤트 모니터링은 2015년 대비 우선순위 점수가 상승하고 있는 분야로 각각 1~3위를 기록함
- APT 대응 역시 2015년 13점에서 2016년 17점으로 다소 순위가 상승함
- 하지만, 보안 정보 및 이벤트 모니터링, DDoS 대응, 방화벽 등은 2015년 하반기에 비해 우선순위 점수가 다소 낮아지고 있는 것으로 나타남

▶ 미국에서 개최되는 RSA 2018과 Black Hat은 글로벌 정보보안 기업의 제품 트렌드 및 시장 동향을 파악할 수 있는 곳인데 Black Hat의 머신러닝 제품 출시를 주목할 만함

- 글로벌 보안기업의 전략, 제품 트렌드, 시장 동향을 파악에는 RSA 전시회 유용
- 보안위협 동향, 해커들의 관심분야, 세부 기술 트렌드를 파악하는데 있어서는 'Black Hat/Defcon'
- 특히 Black Hat은 RSA와 달리 상당히 많은 업체가 머신러닝(Machine Learning) 기술을 적용하고 있다고 홍보하여 전시장에서 '머신러닝'이라는 용어는 빈번하게 볼 수 있었던 반면, 'AI'용어를

사용하는 업체는 2018.1~2곳 정도로 매우 드물었음

- 파이어아이, 시만텍 등 Threat Intelligence를 운영하고 있는 대형 글로벌 보안 기업은 이미 위협분석에 머신러닝 기술을 적용하고 있었음

- ▶ 미국 전시회에서 파악된 머신러닝 기술은 위협 분석에 활용되며, 그 적용 포인트는 크게 3곳(로그관리시스템 연계, 네트워크 기반, 에이전트 기반)이며, 기대 이상으로 네트워크 기반 접근제어 시스템에 적용사례가 다수 있음

- SIEM과 같은 통합 로그관리시스템과 연동, 대량의 로그 기반으로 위협분석에 적용
- 네트워크 기반으로 In/Out bound 트래픽 흐름을 분석, 공격위협을 탐지하는데 적용
- 시스템에 설치되는 에이전트 기반으로 비정상적인 행위를 분석하여 공격 위협을 탐지하는데 적용

- ▶ 미국은 CLTC, IoT 전시회, APPA 포럼 등 행사에서 개인정보보호가 강조되고 있음

- CLTC의 경우, 유럽 기관/학생들과 많은 인터페이스가 있다고 하며, GDPR에 대응해야 한다는 것은 의식하나 대부분의 현지 기업이나 개인정보 담당자들은 개인정보보호에 초보 수준 임
- IoT 전시회에서 개인정보보호 관련하여 많은 주제발표가 이루어졌으나, 보안솔루션은 상당히 적음
- APPA 포럼(2018.6.25~27)에서 가장 많이 논의된 내용이 GDPR, 카펜터\* 등으로 현지에서의 개인정보보호 인식에 대한 변화를 느낄 수 있음
  - \* 미 대법원에서 항소결과를 뒤집고, 사용자의 전화 위치 데이터를 확보하기 위해서는 영장 청구가 필요하다고 판결
- 멀지 않은 시기에 개인정보보호 관련 미국 시장은 상당히 성장할 것으로 기대되는바 한국의 상당히 엄격한 개인 정보 규제에 대응해온 한국기업이 개인정보보호 측면에서 상당한 경쟁력을 확보하고 있다고 판단됨

- ▶ 하지만 IDC보고서(U.S. GDPR Security Products Forecast, 2018-2022)에 따르면 미국 보안시장에서 개인정보를 위한 예산 투입은 그다지 크지 않을 수도 있다고 전망

- 그 이유로 기업은 이미 GDPR을 준수할 수 있는 툴을 구입해서 활용하고 있어 성장이 제한적
- IDC는 미국 GDPR 시장 성장을 연복합성장률 5.2%로 2017년 4억 1600만 달러에서 2022년 5억 3700만 달러에 달할 것으로 전망

그림 \_ 미국 개인정보보호 시장 성장 전망(2017~2022)



\* STAP: Specialized Threat Analysis and Protection

[출처] SDI, 'The Cyber Security Market in the United States to 2025'(2016.3)

### 정보보안 제품 및 서비스 유통

▶ 미국의 정보보안 제품 및 서비스 유통은 일반 소비자를 대상으로 하는 B2C와 기업 및 정부 고객들을 대상으로 하는 B2B 방식에 차이가 존재

- 일반 소비자를 대상으로 하는 경우는 소매 유통업체를 통하거나 온라인 등을 통한 벤더의 직접 판매 방식이 활용되는 경우가 대부분을 차지
- 금융, 통신, 정부 분야 등 규모가 크거나 전략적으로 중요한 프로젝트의 경우 시스템 통합업체(SI)들과 제휴해 제품을 판매하는 경향이 보편적
- 일반 소비자 대상의 소매 시장의 경우 브랜드와 성능 이외에도 가격, 활용 용이성 및 소프트웨어의 업데이트 빈도 등이 경쟁력에 중요한 영향을 미치는 요소로 작용

▶ 미국 보안 소프트웨어 판매 채널은 직접 판매 방식과 간접 판매 형태인 유통업체(Distributor/Retailer) 경유 방식 등 두 가지로 구분

- 직접 판매는 현지에서 판매를 직접 수행하기 위해 지사 법인을 설립하거나 에이전트 계약을 맺는 방식으로, 2000년을 전후로 국내 주요 벤더들의 경우 장기적 현지 시장 개척 및 적극적 시장 진출 관점에서 현지 법인을 설립을 선호
- 간접 판매는 IT 및 SW 전문 도매(Wholesales) 유통 기업이나 PC 제조업체, 대형 소프트웨어

소매판매업체(Retailer)를 경유해 유통하는 판매 방식으로, 2004년 이후 국내 기업들이 미국 및 해외 시장 진출 시 선호하는 유형

- 미국 내 IT 전문 유통기업(Distributor)으로는 Ingram Micro, Tech Data, Avnet, Arrow Electronics, SYNEX 등이 주요 플레이어로 활동
- 소매판매업체로는 주로 소비자용 전자 디바이스, 가전 및 소프트웨어를 취급 하는 대형매장들인 Best buy, Circuit City, OfficeDepot, Staples 등이 유명

▶ 정보보안 소프트웨어 유통은 Ingram Micro와 Avnet 같은 대형 IT 제품 전문 도매 유통업체들을 통하는 방식이 전체의 70%를 차지

표 \_ 미국의 대표적인 IT 및 소프트웨어 전문 도매 유통업체 현황

업체명	주요 취급 품목
Ingram Micro, Inc.	IT Peripherals, Systems, Software(15~20%), Networking
Avnet, Inc.	Electronics, Technology Solutions, Logistics, Managed Technologies
Tech Data Corp.	IT Peripherals, Systems, Software, Networking
Arrow Electronics, Inc.	Semiconductors, Computing Solutions, OEM Computing solutions, Passive, electromechanical and connectors
Tyco International	Hardware and software products, application development, asset and lifecycle management, product procurement, systems integration, and training
SYNNEX Corporation	PCs, servers, and software
IKON Office Solutions, Inc.	Scopiers, printers, fax machines, office supplies, document management outsourcing, electronic file conversions, facilities management
ScanSource, Inc.	Automatic identification and data capture (AIDC) products, point-of-sale(POS) products, voice and data communications products and electronic security equipment
Newegg Inc.	Cell phones, digital cameras, home appliances, networking devices, peripherals, DVDs, accessories, and software
MA Laboratories, Inc.	Memory modules, hard drives, motherboards, modems, power supplies, and graphics cards, monitors, software, GPS systems, network cards, digital cameras, notebook computers, wireless networking gear, digital music players, etc

[출처] Wikipedia, Google Finance 종합

- 대형 벤더들의 경우 독립소프트웨어 벤더(ISV), VAR(Value-added reseller), 서비스 관리기업(MSP)등과 채널 파트너십(channel partnership)을 체결해 제품을 유통하는 방식이 확대 추세
- 미국 정보보안 소프트웨어 부문의 주요 유통업체들은 다음 표와 같음

**물리보안 제품 및 서비스 시장**

▶ 미국 물리보안 시장은 주로 침입탐지, 비디오 감시 장비, 출입통제, 화재감지, 인터폰, 통합보안장비, 외부감지, 홈 자동화 및 그 외의 제품과 서비스로 구성

- 시장조사업체 Barnes & Co.의 조사에 따르면, 미국 보안 시스템 서비스 업체들의 2017년 총 매출 규모(추정)는 119억 200만 달러로 전체 시장에서 가장 높은 비중을 차지했으며, 업체 수는 총 2만 1,370개를 기록
- 침입 탐지 관리 및 모니터링 시장의 비중이 그 다음으로 높았으나 매출 규모는 보안 시스템 서비스의 절반 수준인 58억 900만 달러를 기록
- 보호 장비 및 안전 부문의 총 매출은 8억 2,600만 달러였으며, 업체 수는 3,780개를 기록해 업체당 사업 및 매출 규모가 상대적으로 소규모임을 반영
- 폐쇄감시시스템 시장의 매출이 4억 6,920만 달러였으며, 화재 감지 및 모니터링 부문의 매출은 4억 2,000만 달러를 기록

표 \_ 미국의 물리보안 분야별 시장 규모와 현황(2017년)

(단위: 백만 달러, 개, 명)

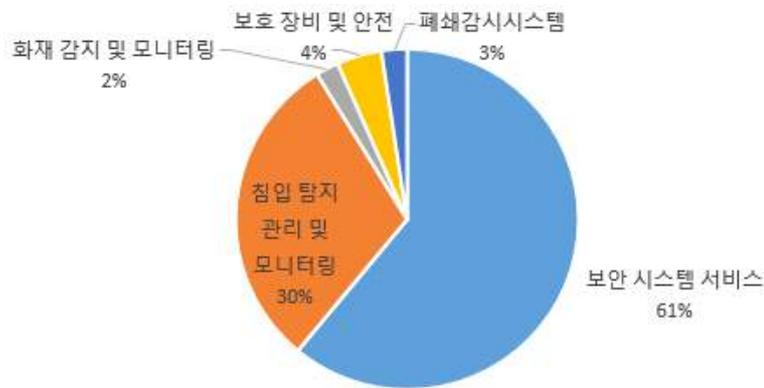
분야	총 매출 규모 (2014)	총 매출 규모 (2017)	업체 수 (2017)	종사자 수 (2017)
보안 시스템 서비스	10,713.0	11,902.5	21,370	98,103
침입 탐지 관리 및 모니터링	5,302.0	5,890.7	3,190	20,284
화재 감지 및 모니터링	378.2	420.2	730	3,780
보호 장비 및 안전	743.5	826.0	3,151	12,886
폐쇄감시시스템	422.3	469.2	706	2,897

[출처] Barnes Reports, '2016 U.S. Industry & Market Outlook: Security Systems Services Industry' (2016.5)

▶ 시장조사업체 Barnes & Co.(Barnes Reports)의 조사에 따르면, 2017년 보안시스템서비스 매출이 61%, 침입탐지 31%, 보호장비 및 안전 4%, 폐쇄감시시스템 3%, 화재감시 및 모니터링 2% 순이며, 이러한 시장 비중은 2014년과 거의 동일하며 각 분야의 매출 상승에도 불구하고 시장 판도에는 큰 변화가 없는 것을 나타냄

- 규제당국은 금융시장의 안정성 유지와 소비자 보호를 우선할 수밖에 없기 때문에 금융업체들과는 시각이 다를 수밖에 없음
- 이에 소비자, 규제당국, 금융업체간의 지속적인 협의를 통해 AI 금융상품에 대한 최적의 규제 방안을 도출하는 과정이 필요
- 국내 금융업계에서도 로보 어드바이저나 챗봇 같은 AI 기반 서비스가 잇따라 출시되고 있는 만큼, 소비자 보호와 시장 혁신 양쪽 모두에 부합하는 새로운 규제 시스템이 필요

그림 \_ 미국의 물리보안 분야별 시장 규모와 현황(2017년)



[출처] Barnes & Co.

- ▶ IBIS World에 따르면, 미국 보안 서비스 기업들의 시장점유율은 지난 5년간 크게 변화하지 않으며 기업(28.1%), 정부기관(22.4%), 주거 및 기타(16.6%), 소매상 및 레저(14.5%) 및 금융기관(18.4%) 등의 순으로 매출 차지
- ▶ 물리보안 시장은 경기의 부침에 따른 시장 수요의 변동이 있지만 안전과 테러 방지에 대한 요구 사항이 커지고 사용자 저변의 확대가 이어지면서 시장 규모를 유지
  - 보안 시스템 서비스, 침입 탐지 관리 및 모니터링, 화재 감지 및 모니터링, 보안 장비 부문 등 물리보안 전반적으로 건설 경기의 영향을 받는 편
  - 물리보안 산업 시장 비중은 주거용과 비주거용이 1:2 정도의 비율을 보이고 있으며, 이와 같은 매출 비율은 수 년 간 비슷한 수준을 유지
  - 미국 물리보안 시장은 ▲범죄 및 테러 방지에 대한 관심 증가 ▲기술 발전 및 신제품 개발에 따른 기존 제품 업그레이드 수요 증가 ▲가격인하에 따른 수요저변 확대 등에 힘입어 꾸준한 성장세를 이어나갈 것으로 기대

- ▶ 물리보안 시장의 전자출입통제 및 침입 탐지 시스템에 최신 정보기술 등이 적용되면서 보안 성능의 향상과 새로운 시장의 창출이 이어지고 있는 추세
  - 전자출입통제시스템(Electronic Access Control System)에 대한 수요는 사용자들 사이에서 모니터링 및 접근제어 통제를 통해 신뢰성 있는 범죄 예방 효과를 볼 수 있다는 인식이 확산되면서 점차 높아지는 추세
  - 바이오 인식 업계는 지문, 홍채, 망막 및 얼굴 인식 식별 시스템과 같은 바이오 인식 기술용 소프트웨어를 개발함으로 지난 5년간 많은 성장을 기록했음
  - 2013년 기존의 미국 방문자 및 이민 상태 표시 프로그램 대신 바이오 인식 신분증 관리소(Office of Biometric Identity Management)가 만들어지면서 기업의 민간 투자가 증가하고 이민 목적을 위한 바이오 인식 스캐닝이 더욱 강조되면서 업계 수익은 계속해서 증가할 것으로 예상됨
  - 보안 바이오 인식 시장은 2016년에만 14.0%의 성장률을 기록하며 전반적으로 업계 매출은 지난 5년간 연평균 7.8%, 총 54억 달러의 수익을 기록함
  - 도난 경보기 등을 포함한 침입탐지 시장은 주거용과 상업용 모두 스마트폰 및 태블릿으로 원격 모니터링, 제어 및 액세스가 가능한 통합형 솔루션으로 진화 중
  
- ▶ 영상 감시 부문은 디지털화, 네트워크화, 클라우드화 등을 통해 성능과 활용도가 크게 향상되고 있는 상황
  - 영상 감시 장비 산업은 미국에서 가장 빠르게 성장하는 물리보안 분야로서, 분석 기술 발달 및 클라우드 서비스를 접목한 VSaaS와 같은 새로운 서비스 영역이 확대되고 있으며 아날로그 시스템의 IP 기반 장비로 대체 확산
  - 보안카메라 시장은 디지털저장장치, 화질개선, 인터넷 기반의 모니터링 시스템 등 기능 개선 및 범죄자들의 행동패턴을 포착해낼 수 있는 '스마트 CCTV' 등과 같은 신기술 도입 등의 기술 진화가 주된 성장 요인이 될 것으로 전망
  - 최근의 지능형 CCTV 바이오인식 기술은 CCTV 시스템 가시거리 내의 객체 식별을 물체와 사람으로 구분해 식별하는 수준을 구현하고 있으며, 이동식 카메라에 의한 사람의 움직임 및 안면인식 기술을 결합해 휴먼 재식별 융합 기술로 발전하고 있는 추세
  - 딥러닝이 CCTV를 만나 AI CCTV로 발전하면서 감시만으로 활용하던 CCTV가 AI와 융합되면서 리테일, 제조, 오일 & 가스 등 스마트 팩토리 분야 등 활용 분야가 확대 중

### 물리보안 제품 및 서비스 유통

- ▶ 미국의 민간 물리보안 부문에서는 주로 전문 도매(Wholesales) 업체나 대형 딜러 및 공급 업체를 중심으로 유통 시장이 형성
  - 대다수의 보안 장비 생산업체들은 주로 전문 도매 유통업체를 활용하고 있으며, 생산업체는 이들 총판에 전적으로 제품을 홍보하고 프로모션에 대해서도 높은 의존성을 보이는 것이 특징
  - 물리보안 제품 생산 업체가 직접 판매 및 제품의 설치와 서비스를 모두 담당하는 경우도 있으며, 이 경우 소비자에 대한 접근 권한이 커지는 것이 장점
  - 유통업체는 해외 브랜드를 그대로 유통하기도 하며, 브랜드 파워가 없는 해외 제품에 대해 일정 기간 OEM 방식으로 제품을 들여와서 미국 시장에 유통하는 경우도 드물지 않은 편
  
- ▶ 지문 인식은 바이오 인식 스캔 업계에서 매출의 약 55%를 차지함
  - 법 집행과 출입국 사무소나 개인 식별을 위해 지문을 사용하며 체육관이나 도서관과 같은 여러 공공기관에서 이제 카드키 대신 지문을 사용하고 있음
  - 안면 인식은 정부에서 주로 사용해 왔지만 서서히 다른 분야로 확대되고 있는 추세 보안 카메라 및 얼굴 샷을 통해 범인을 확인하는 기술로, 이 기술을 통해 확인된 범죄자 수는 더욱 증가할 것으로 예상됨
  - 3D 안면 인식과 같은 혁신기술은 정확도가 낮아 현재 점유율 상승에 한계 존재
  - 망막 및 홍채 인식은 업계 매출의 약 15.0%를 차지할 것으로 예상됨
  - 다른 바이오 인식으로는 손, 핏줄 및 음성 패턴을 통한 인식이 있으며, 업계 매출의 약 14.0%를 차지하고 있으나 오류로 인해 상대적으로 낮은 점유율을 보임
  
- ▶ 미국의 공공 물리보안 부문에서는 연방정부, 주정부, 학교 등에 대한 조달 시장이 형성되어 있으며 조달시장에 제품을 공급하기 위해서는 기본적으로 GSA 계약자(GSA contractor) 자격이 필요
  - GSA contractor 중에도 대형 유통/공급 업체들은 공공 부분의 제품 공급에 많은 영향력을 행사
  - GSA contractor 업체와의 관계를 형성하려면 공공 및 보안 전시회에서의 노출을 통해 이들 대형 유통업체에 국내 기업의 브랜드 인지도, 품질 및 기술력을 각인시키는 과정이 필수
  - 국내 기업 중 미국 조달 시장 진출에 성공한 업체 대부분이 GSA contractor 자격을 취득하여 제품 및 기술력에 대한 공인 받음은 물론, 전시회를 통해 대형 유통 업체와의 오랜 관계 형성으로 시장 진입에 성공

- ▶ 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 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
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 Buy, 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 운영하며 글로벌 기업의 보안 카메라 라인업 보유

[출처] Wikipedia, Google Finance 종합

### 3. 주요 사업자 현황

#### 시장 특성 및 경쟁 강도

##### □ 정보보안 시장

- ▶ 미국의 정보보안 시장은 특정 업체들이 시장에서 뚜렷한 우위를 점유하지 못한 상태에서, 다양한 기업들 간의 치열한 경쟁과 인수합병을 통한 시장 재편이 두드러진 상황
  - Check Point, Fortinet, McAfee, Cisco, Symantec, Trend Micro, Palo Alto Networks, Blue Coat Systems, Check Point Technology, Kaspersky Lab 등 다양한 업체들이 치열하게 경쟁 중

- Symantec, McAfee, Check Point가 시장을 이끄는데 3사 점유율은 2011년 35.4%에서 2016년 32.8%로 감소
- 최근에는 클라우드 보안 시장의 성장세가 두드러지고 신규시장이 확대 되면서 주도권 확보를 위한 기업 간의 인수합병(M&A) 사례가 급증

표 \_ 정보보안 시장의 최근 주요 인수합병 사례들

(단위: 백만 달러)

발표일	인수업체	피인수업체	피인수기업 가치 또는 매출규모	인수거래규모
2018.10.04	Palo Alto Networks	RedLock	N/A	173
2017.05.24	Microsoft	Hexadite	N/A	100
2016.09.20	Fortinet	AccelOps	N/A	28
2016.09.18	Oracle	Palerra	N/A	N/A
2016.09.07	TPG	Intel Security (지분51%)	N/A	3,100
2016.07.28	Oracle	Netsuite	N/A	9,300
2016.06.28	Cisco Systems	CloudLock	N/A	293
2016.06.12	Symantec	Blue Coat Systems	7.8	4,650
2016.06.01	Vista Equity Partners	Ping Identity Corp.	N/A	N/A

[출처] 451 Research, Oppenheimer Research, 기타 언론종합(2018.10)

- ▶ 미국 워싱턴 D.C.를 중심으로 보안 스타트업이 활발히 창업 중이며, 뉴욕 역시 경쟁이 심한 실리콘 벨리보다는 다양한 지원을 내세워 스타트업 유치에 앞장서고 있음
  - 맨해튼 중심의 '실리콘 엘라'는 2008년 금융위기 후 급속히 확장하고 있으며 스타트업 투자는 꾸준히 증가
    - ※ '17년 미 도시별 투자규모 : 샌프란시스코(196억 달러), 뉴욕(133억 달러), 산호세(69억 달러), 보스톤(60억 달러), LA(40억 달러), 워싱턴D.C.(17억 달러), 시카고(16억 달러), 시애틀(13억 달러), 샌디에고(13억 달러)
  - 뉴욕주 차원의 'Start-up NY' 정책, '코넬 테크' 조성 등 스타트업 생태계 육성 정책을 공격적으로 추진
    - ※ Start-up NY : 주세금 및 지방세 10년 감면, 판매 및 사용제 공제/환급, 부동산 양도세 면제 등
    - ※ 코넬 테크 : 뉴욕 루즈벨트 섬에 코넬대, 이스라엘 테크니온 공대가 컨소시엄으로 설립, 전 시장 블룸버그가 1억 달러 기부하였으며, 산학 협력 시너지를 통한 혁신 창업 생태계 조성
- ▶ Bardays가 미국 CIO 대상으로 실시한 서베이에 따르면, 지난 12개월간 미국 상위 보안 기업의 선호도에서 Palo Alto Networks의 상승이 두드러졌으며 2015년 상위인 Check Point와 Symantec은

선호도 조사에서 다소 점수가 낮아짐

- 특히 Palo Alto Networks는 2015년 하반기 25점에서 2016년 상반기 50점으로 가장 선호되는 벤더로 꼽혔기에, Firewall 분야 점유율과 연관이 있는 것으로 추정
- 그 뒤를 이어 FireEye, Cisco Systems, Trend Micro, Splunk 등이 2015년에 비해 2016년 상반기 선호도가 상승했으며 각각 2위에서 5위를 기록함
- 하지만, 2015년 선호도 1위였던 Check Point는 2016년 상반기 선호도 9위, Symantec은 2015년 2위에서 2016년 6위로 선호도에서 다소 하향세를 나타냄
- 또한, F5와 Juniper의 경우, 2016년 선호도에서 2015년에 비해 하향세를 보임

표 \_ 미국 CIO가 선호하는 보안기업 벤더 순위(2015 하반기~2016 하반기)

벤더	2016 하반기	2016 봄	2015 하반기
Palo Alto Networks	50	36	25
FireEye	47	48	39
Cisco Systems	41	47	16
Trend Micro	25	22	12
Splunk	24	24	14
Symantec	24	34	45
F5	19	21	38
Fortinet	18	6	5
Check Point	15	16	60
Juniper	11	15	24
Proofpoint	8	5	3
Imperva	5	5	3
Barracuda Networks	3	1	1
Sophos	3	6	6
Hewlett-Packard Enterprise	2	NA	NA
Rapid7	2	0	0
CyberArk	1	0	0
Qualys	1	1	0
Radware	1	0	0

[출처] Barclays, US Software Security, Design & VSS: Stock-Picker's Market in 2017

- ▶ Barclays 보고서에 따르면, 보안시장에서 기업 경쟁력을 엿볼 수 있는 분야는 방화벽(Firewall) 분야로 Palo Alto Networks와 Fortinet는 해당분야 시장 점유율이 상승하고 있으며 Cisco, Check Point 및 Juniper는 점유율이 감소하고 있음

- 특히 Palo Alto Networks는 2013년 5.3%에서 2015년 10.1%로 가장 성장이 두드러졌으며 Cisco 18.1%, Check Point 14.1%의 점유율을 보임

#### □ 물리보안 시장

- ▶ 미국 물리보안 시장에서 IT 등 새로운 기술 가치의 도입과 해외 기업들의 활약에 따른 경쟁이 치열해지고 있는 추세

- 미국의 물리보안 시장에서는 완성품 제조업체 기준으로 약 300~400개의 업체가 경쟁을 벌이고 있으며 보안장비 시스템 관련 업체는 경비, 알람 모니터링, 제품 설치 서비스 제공업체까지 모두 포함할 경우 약 총 5,000여 개를 상회할 것으로 추산
- 미국 보안 장비 판매시장에서는 United Technologies, Honeywell International, Tyco International 등이 시장점유율 상위 3개 업체로 우위를 차지
- 이 밖에 Assa Abloy(스웨덴), Checkpoint Systems, L-3 Communication, Robert Bosch(독일), Safran(프랑스) 등 해외 사업자들도 주요 시장 참여자로 활동 중

- ▶ 2017년 미국의 보안카메라 관련 수입액은 67억 달러로 전년 대비 16.27% 증가

- 미국의 주요 수입국은 중국, 일본, 태국 등으로 중국으로부터의 수입액은 30억 달러로 전년 대비 32.88% 증가하였으며 전체 수입금액의 약 45%를 점유. 베트남, 독일도 각각 전년 대비 152.63%, 50.86% 수입금액이 증가했음
- HIS Markit의 애널리스트인 Kim Dearing은 와이파이가 연결된 초인종 카메라의 수요는 폭발적이며, 앞으로 더욱 대중화될 전망이라고 밝힘
- 비교적 진입 장벽이 낮아 여러 스타트업이 경쟁하고 있으며 보안제품 진입의 중요한 요소는 기술적 측면보다는 소비자가 직접 설치가 쉬운 제품 개발이 중요
- 또한 적정수준의 가격이 중요한 요소로 설문조사에 따르면 500달러 이상의 보안카메라를 구매한 소비자의 비율이 28%로 가장 많은 비중을 차지했으며, 그 뒤로 27%는 250달러에서 500달러 사이의 제품을 구매
- Motorola, Axis, Netgear, Nest Cam, Icontrol Networks, Canary, Amcrest Technologies, Unide 등 다양한 브랜드의 제품이 시장에 나와 있으며 중국제품은 비교적 저렴한 가격을 강점으로 온라인 마켓에서 쉽게 구매가 가능함

## 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 주목
- 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 탐지함으로써 AI 기반 보안제품 경쟁에 선두로 나섬

#### ▶ Trend Micro

- Trend Micro는 모바일 단말, 엔드포인트, 게이트웨이, 서버, 클라우드 보안 솔루션에 주력하고 있으며 개인과 기업, 정부 기관의 데이터센터, 클라우드, 네트워크 및 엔드포인트에 다층 보안 솔루션을 제공
- 엔드포인트 보안과 멀웨어 감지기술 분야의 선두 업체이지만, Symantec, McAfee 등과의 경쟁이 심화됨에 따라, 차세대 유망 기술 분야인 클라우드보안, 가상화(Virtualization), 모바일보안, 지능형지속위협(APT), 사물인터넷(IoT) 기술 시장에 주목
- Amazon의 AWS와 Microsoft의 Azure 등 유력 클라우드 서비스 플랫폼에서 Trend Micro를 보안 벤더로 추천한 것을 계기로 2014년 이후 Trend Micro의 클라우드 관련 총 매출은 큰 폭의 성장세를 이어가는 중
- 독립형(stand-alone) 솔루션으로 이용하는 것은 물론, 'Trend Micro Control Manager' 콘솔을 통해 다른 Trend Micro 엔드포인트 보안 솔루션도 일원화해 관리 가능

## ▶ Palo Alto Networks

- 2007년에 설립된 보안 업체로서 차세대 방화벽 전문 기업 외에 지능적 지속 위협(APT) 보안 솔루션 업체로 유명
- 차세대 방화벽 기능 이외에 침입방지 시스템(IPS), 안티바이러스, URL 필터링 기능 등을 지원하는 네트워크 통합 플랫폼과 Wildfire와 Traps를 연동해 위협 정보를 다루고 있음
- 2016년에는 클라우드 컴퓨팅 시스템 환경을 검할 수 있는 시스템을 공개했으며, 이 같은 검용 시스템을 통해 최근 기술 업그레이드에 속도를 높이고 있는 상황
- 클라우드 기반의 지능적 지속 위협(APT) 솔루션인 Wildfire는 지능형 공격에 대한 탐지와 대응, 사전 방어를 종합적으로 지원하는 전략을 구현하고 있으며, SecaaS형 클라우드 접근 보안 브로커(CASB) 솔루션도 제공
- 또한 Palo Alto는 지난 2017년 10월 주로 기업 고객들이 원하는 보안 서비스를 클라우드 환경(SaaS)에서 골라 쓰도록 하는 보안 앱스토어 생태계를 구축 발표

## ▶ 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

## ▶ 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 버추얼 시스템과 함께 방화벽, 가상사설망(VPN), 인터넷침입방지시스템(IPS), 애플리케이션 컨트롤, URL 필터링, 안티봇, 안티바이러스, ID인식 등 체크포인트 소프트웨어 블레이드를 선택해 가상화 보안을 강화할 수 있음
- 2016년 출시된 차세대 보안관리 플랫폼 'CheckPoint R80'은 전체 인프라스트럭처를 포괄하는 단일 콘솔로서 메인 게이트웨이, 데이터센터 지점, 클라우드 구현을 두루 관리하는 것이 특징

▶ Fortinet

- Fortinet은 고성능 네트워크 보안 제품과 서비스 공급회사로서 Unified Threat Management(UMT) 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

▶ McAfee(구 Intel Security Group)

- 미국 산타클라라 소재 보안 전문기업으로 7,500명의 전문인력과 1,200여 개의 보안 기술 특허를 보유
- 네트워크보안, 서버보안, 보안분석, 웹보안 등 네트워크에서 엔드포인트까지 다양한 보안 솔루션 제공
- 주요 제품으로는 시간 가시성과 분석 제공, 위험 감소, 컴플라이언스 보장, 인터넷 보안 개선을 목적으로 기업을 지원하는 보안 관리 기능과 악성 프로그램 방지, 안티스파이웨어, 안티바이러스 소프트웨어 등을 제공

□ 물리보안 시장

▶ Tyco Integrated Security

- 스위스계 Tyco International Ltd.의 북미 지역 자회사로서, 미국 물리보안 산업의 주요 사업자 중 하나

- 상업용 보안장비들의 연동을 통해 다양한 산업계에 종합 솔루션을 공급하고 있으며, 상업 보안 비즈니스를 화재 방지 비즈니스와 결합하여 시너지를 내는 전략으로 시장에서 경쟁
- 주요 취급 품목은 출입 통제, 자산 트래킹, 화재 및 안전, 장비 설치 및 유지보수 서비스 부문

▶ Stanley Convergent Security Solutions

- Stanley Black & Decker 그룹의 계열사로서 알람 모니터링을 포함하여 보안 시스템의 설계, 공급, 설치 및 전자 보안 서비스를 제공.
- 미국 시장 내에서만 30만 명의 고객을 보유하고 있으며 직접 세일즈 방식으로 사업을 전개
- 주택, 상업빌딩, 산업계, 정부 등의 다양한 고객군을 보유하고 있으며, 연방 정부 및 주정부 보안 솔루션 공급업체로도 활동
- 주요 취급 품목으로는 출입제어, CCTV/비디오 감시, 자동 화재감지, 침입탐지 모니터링, 종합 보안 솔루션 공급 등이 대표적

▶ 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

▶ Monitronics International

- 주택 및 기업 고객에게 보안 모니터링 서비스를 제공하고 있으며, 450여 개 독점 딜러 네트워크를 형성
- 2010년에 Ascent Capital Group에 피인수 된 후에도 사업을 지속
- 주요 취급 품목으로 일반가정, 한부모 가정, 시니어를 위한 맞춤형 시스템 공급, 강도, 화재 및 침입 감지 등의 모니터링 서비스 등을 제공

▶ Dieblod Security

- 전자 및 물리보안 시스템을 개발, 생산, 판매 및 서비스하는 전문 업체로서 뉴욕을 위시한 미국 동부지역을 중심으로 활동
- 자사 솔루션은 물론 금융 및 상업 시장 분야에서 다수의 서드파티 솔루션을 제공
- 주요 취급 품목으로는 ATM 보안, 전자 보안 서비스 등을 제공

▶ Vector Security Incorporation

- 미국 내 전자 보안 솔루션 제공 업체로서 미국 10여개 이상의 지역 거점 오피스를 보유하고 있으며, 캐나다 및 캐리비안 지역에도 서비스 제공
- 북미 지역에서 26만여 개의 일반 가정과 비즈니스에 전자 보안 솔루션을 제공하고 있으며 주택 시장 확대에 집중
- 주요 취급 품목으로는 전자보안, 화재 경보, 비디오 감시, 접근 제어, 강도 및 침입 탐지 등의 솔루션이 대표적

▶ Guardian Protection Services

- 1950년에 설립된 보안 시스템 기업으로서 보안 시스템을 설계, 설치 및 모니터링하고, 25만 여의 주택 및 상업빌딩 고객에게 서비스를 제공
- 원격 홈 제어, 모니터링 서비스, 무선 가정보안, 침입 탐지, 비디오 감시, 화재 감지, 응급 의료 상황 처리 등의 서비스를 제공

▶ Raytheon

- 미국 4대 방산 업체로서, 방공 미사일뿐 아니라 정보 수집, 소방, 기상, 항공관제 등의 레이더 장비, 커뮤니케이션 장비, 전자무기 등을 생산하고 있으며 전자 데이터 처리 시스템 및 소형 컴퓨터 시스템도 개발
- 주요 취급 품목인 전자 제품 및 항공 우주와 방위 분야의 주 고객은 미국 정부이며 공급자 등록(supply registration)을 한 업체에 한해 공급 계약 논의가 가능

#### 4. 주요 동향 및 이슈

- ▶ MS는 2014년 설립된 이스라엘 사이버보안 스타트업 Hexadite를 1억 달러(약 1,119억 원)에 인수함(2017.5)

- Hexadite는 2014년 텔아비브에서 설립된 신생업체로, 현재는 미국 보스턴에서 직원 35명을 두고 있음
  - 사이버보안 가운데서도 머신러닝을 통해 사이버 공격을 감지하고 이에 따른 시스템 피해를 최소화하는 기술에 특화됨
- ▶ 미국 샌프란시스코에서 열린 RSA 2017에서 보안 업체들인Fortinet, McAfee, Palo Alto Networks, Symantec이 설립한 사이버 위협 얼라이언스(Cyber Threat Alliance, CTA)가 공식 비영리 단체로 출범함(2017.2)
- CTA의 첫 번째 최고 관리자로 이전 미국 대통령인 버락 오바마의 정권 당시 사이버 안보 조정관(cybersecurity coordinator)이었던 마이클 다니엘(Michael Daniel)이 임명됨
  - 또한, 보안 전문업체인 Check Point와 Cisco Systems가 새로운 CTA 멤버로 합류함
  - CTA의 처음 과제는 동으로 위협 첩보를 공유하는 분석 플랫폼을 런칭하는 것으로서, 이는 멤버들이 이미 갖고 있는 위협 첩보 공유 시스템을 통합하여 사이버 위협 정보 표현 규격(STIX/TAXII)을 활용하는 것으로 알려짐
- ▶ IBM은 인공지능(AI) 보안 기술인 '왓슨 포 사이버 시큐리티(Watson for Cyber Security)'를 발표함(2017.2)
- '왓슨 포 사이버 시큐리티'는 IBM의 새로운 코그니티브 보안관제센터에서 제공되는 서비스로 엔드포인트, 네트워크, 사용자, 그리고 클라우드 전반에서 발생하는 보안 위협에 대응할 수 있도록 코그니티브 기술 기반으로 보안 운영서비스를 제공
  - 이러한 보안 운영 서비스에서 가장 중심에 있는 제품은 'IBM 큐레이터 왓슨 어드바이저'로 IBM 왓슨의 사이버 보안 통찰력 전체를 활용하는 최초의 제품임
  - IBM은 그간 자사의 클라우드 기반 인공지능 컴퓨터 시스템인 Watson을 정보보안 비즈니스에 활용하기 위해 IBM의 X-Force 보안팀이 제공하는 데이터를 통해 8백만여 건의 스팸 및 피싱 공격, 십만 건 이상의 취약점에 대한 학습을 진행 함
- ▶ 미국 DNS 서비스 업체, IoT 봇넷에 의한 대규모 디도스 공격 피해 (2016.10)
- 인터넷 도메인 서비스 업체인 Dyn이 대규모 디도스 공격을 받아 미국 동부지역의 근거지를 두고 있는 메이저 웹 사이트에 장애가 발생
  - 감시 카메라가 하이재킹 되어 미라이(Mirai)라는 봇넷 구성에 이용된 것으로 확인됐으며, 감시 카메라의 복잡한 유통구조로 인해 최종 사용자와 현재 보안 현황을 파악 및 대처하는 것이 어려운

### 상황

- 가정용 라우터, 웹캠, 스마트 냉장고 등 사물인터넷(IoT) 기기들의 보안 취약점에 대한 여론이 환기되면서 이 분야 보안에 대한 수요와 관심이 커질 것으로 전망

#### ▶ 미 중소기업 보안 수준 열악, 정보보안 투자 확대방안 필요 (2016.10)

- 미국의 보험 회사인 Nationwide는 미 중소기업의 80%가 정보보안 사건 사고 발생 시 대응할 만한 계획을 가지고 있지 않다고 지적
- 미국 중소기업 절반 이상이 2015년 한 해 동안 적어도 한 번 이상의 사이버 공격을 받았으며, 사이버 공격을 받은 경험이 있다는 기업들 중 60%가 복구에 1달 이상 소요된 것으로 확인
- 미 하원의 소기업위원회는 2,800만 개에 달하는 미국 소기업들의 정보보안을 강화하기 위한 노력을 기울이고 있으며 2016년 9월에는 소기업사이버보안강화법(Improving Small Business Cyber Security Act)이 하원을 통과하는 등 관련 분야의 투자 확대를 위한 노력이 진행

#### ▶ Intel, 사모펀드 TPG에 Intel Security 지분 매각 (2016.09)

- Intel이 정보보안 사업부 Intel Security의 지분 51%를 사모펀드 TPG에 31억 달러에 매각했으며 이에 따라 2017년부터는 McAfee 브랜드로 영업 개시
- Intel은 2011년 McAfee를 77억 달러에 인수한 이후 2014년 Intel Security로 개명
- Intel은 PC 보안 위협 분야가 성장세를 지속할 수 없다는 판단에 따라 지분을 매각했으며, 사모펀드 TPG는 사이버 공격 우려 증가에 따른 보안업계의 수익성에 주목해 지분을 인수한 것으로 평가

## 정보보호 정책 및 기관 현황

### 1. 관련 법령 및 정책

#### 관련 법령 및 규제

- ▶ 트럼프 정부, 2003년 이후 15년 만에 연방차원의 '국가 사이버보안 전략' 공개 (2018.9)
  - 전략 보고서에서는 ▲미국 내 네트워크, 시스템, 데이터 안보 강화 ▲강화된 사이버보안 환경에서 디지털 경제와 기술혁신 증진 ▲미국의 국제 평화와 국가안보 증진 ▲국제 인터넷 환경과 기술 분야에서 미국의 리더십 확대 등을 핵심 목표로 제시함
  - 사이버 범죄에 대응하기 위해 연방정부는 범정부부처 간 통합적인 대응 시스템 구축을 하기 위해 노력해옴
  - 대통령 직속 국가안보위원회(NSC)와 국가안보테러보좌관이 주재하는 범정부 기관으로 사이버보안 정책과 전략을 수립하는 컨트롤 타워 역할을 하고, 국방부 산하 사이버사령부, 연방수사국, 국토안보부 등이 분야별 대응책을 마련하고 있음
  
- ▶ 트럼프 정부, 오바마 정부에서 신설한 국가 사이버 보안 조정관 제도 폐지(2018.5)
  - 미국 국토안보부가 사이버보안 위협을 식별하고 관리하기 위한 새로운 전략을 발표했음에도 불구하고 백악관은 국가 안보위원회 역할이 더 이상 필요하지 않다고 판단하고 사이버보안 조정관 직책을 폐지함
    - \* 오바마 대통령은 2009년 12월 미국 정부의 사이버 정책을 총괄하는 사이버 보안 조정관 제도를 신설한 바 있으나 트럼프 정부는 해당 제도를 2018년 5월 폐지함
  - 사이버보안조정관은 대규모 침해사고 발생 시 국방부, 국가안보국, 국토안보부 등과 협력을 총괄하는 총 지휘관 역할을 담당하였음
  
- ▶ 2015년 민·관 사이버보안 위협정보 공유를 주요 내용으로 하는 「사이버 보안법(Cyber Security Act 2015)」제정
  - 2002년 제정된 「사이버보안강화법(Cyber Security Enhancement Act)」을 수정하여 2015년 사이버 보안법(Cybersecurity Act of 2015)이 제정

- 민간기관이 사이버보안 목적으로 정보시스템 및 정보를 ① 모니터링 및 ② 방어조치를 취하고, ③ 정보를 공유할 수 있는 법적 근거를 마련
- 국가정보국장, 국토안보부장관, 국방부장관 및 법무부장관은 연방기관과 비연방 기관(민간기관, 주지방정부 등 포함) 간 사이버위협지표 및 방어조치에 관한 정보 공유 절차 구축 및 가이드라인을 마련하도록 규정
- 민간 기관이 이 법에 따라 사이버위협지표와 방어조치를 모니터링, 공유 제공받는 행위는 소송의 원인(cause of action)이 되지 못하도록 규정하고, 반독점법에 따른 책임 면제 등 보호규정을 마련
- 국토안보부 장관 및 법무부 장관은 연방정부 내에서의 정보공유체계를 구축하고, 대통령은 민간기관과의 정보공유 역량 절차를 개발·실시하는 연방기관(국방부 제외)을 지정하는 것이 가능
- 국토안보부 산하 국가사이버보안정보통합센터(National Cybersecurity and Communications Integration Center, NCCIC)에 사이버보안위협지표 및 방어조치 정보, 사이버보안 위협과 사고 관련 정보 공유 기능을 부여

▶ 2016년 미 국방부의 사이버 침해사고 보고의무에 관한 규칙 개정안 발표

- 국방부와 계약을 체결하고 있는 계약 당사자 및 하도급업자들에게 사이버 침해사고 (cyber incidents)가 발생한 경우 이를 의무적으로 국방부에 보고하도록 하는 국방부 방위산업기지 사이버보안행위(Defense Industrial Base Cybersecurity Activities)에 관한 규칙의 개정안을 11월 3일부터 시행
- 이 규칙은 국방부와 방위산업기지 관련 기업 간 체결된 모든 형태의 계약의 당사자에게 적용되므로, 계약, 보조금, 협력협정, 그 밖의 거래계약, 기술투자협정 및 그 밖의 모든 종류의 법적 계약 등의 당사자를 모두 대상으로 포괄
- 계약당사자 및 하도급업자로 하여금 대상계약당사자 정보시스템 또는 그 안에 존재하는 대상 국방정보(covered defense information)에 관한 사이버 침해사고를 72시간 내에 보고할 것을 의무로 규정
- ※ 대상국방정보란 기밀이 아닌 통제된 기술정보나 법령 및 범정부적 정책에 따라 보호 또는 전파에 대한 통제가 요구되는 그 밖의 정보를 의미하며 대상국방정보임이 표시되어 있거나 계약의 이행을 위하여 국방부 또는 국방부 대리에 의하여 표시되어 계약자에게 제공된 정보, 또는 계약의 이행을 위하여 계약당사자 또는 계약당사자 대리가 수집, 개발, 수취, 전송, 이용 또는 보관하는 정보

## 2. 담당기관

- ▶ 국토안보부(Department of Homeland Security, DHS)

- 미국은 2003년 3월 「국토안보법(Homeland Security Act)」에 의거하여 국가 기반시설 보호를 담당하는 기존 부서들을 통합하여 국토 안전 및 사이버보안 주무부처로 국토안보부(DHS)를 신설
- 국토안보부는 국가기반보호 계획 수립, 주요기반시설과 자산 식별, 정보보호 활동의 우선순위 설정 및 프레임워크 구성 등을 담당
- 국토안보부는 2009년 10월 30일 국가를 상대로 한 각종 사이버 테러 대응 및 IT 기반시설 보호를 위해 미국 정부기관들의 사이버 안보 기능을 통합한 '국가사이버보안 및 통신통합센터'(NCCIC: The National Cybersecurity and Communications Integration Center)를 개소
- 미국의회는 트럼프정부의 사이버보안조정관 제도 폐지함에 따라 국토안보부에 미국 사이버보안 관리 총책의 권한을 부여하는 의결 진행함(2018.9)

▶ 국방부(Department of Defense, DOD)

- 국방부는 2010년 10월 전략사령부(U.S. Strategic Command)내에 육군, 해군, 공군, 해병대가 개별적으로 운영하던 사이버부대를 통합하여 사이버사령부(U.S. Cyber Command, US CYBERCOM)를 창설
- 2009년 1월 국방보고서에서 '네트워크 중심의 전투(Network-Centric Warfare, NCW)'를 미국의 핵심 역량으로 규정하였으며, 군 컴퓨터 네트워크 통합과 보안, 공격형 사이버무기 개발 등 사이버안전과 사이버테러에 대응하는 사이버사령부를 표방
- 국방부(DOD)는 국토안보부(DHS)와 국가 사이버보안에 관한 협력체계를 구축하여 인력, 기기, 설비 등을 상호 지원하는 것을 내용으로 협약을 교환했으며, 2011년 7월에는 국방부(DOD)가 사이버 사령부의 역할을 포함해 국가 사이버 공간에 관한 방어 전략을 발표
- 2016년에는 사이버 침해사고 보고의무에 관한 규칙 개정안을 발표하여 외부 협력 업체들과의 보안 침해 정보 공유 체계를 강화

▶ 국가 리스크 매니지먼트 센터(NRMC: National Risk Management Center)

- 미국 국토안보부는 새로운 국가 리스크 매니지먼트 센터(NRMC: National Risk Management Center)를 설립한다고 발표함(2018.9)
- 동 센터는 미국의 주요 인프라를 보호하기 위한 국가적 미션을 수행할 예정으로 민·관 합동 리스크 관리를 하며 국가사이버보안 허브인 NCCIC(Cybersecurity and Communications Integration center)와 밀접하게 협력할 계획임
- NRMC는 사이버보안 위기 상황에서 지역, 주정부, 연방 및 민간조직을 위한 911 같은 기동대의 역할을 수행할 것임

## ▶ 법무부(Department of Justice, DOJ)

- 법무부 산하 연방수사국(FBI)에 사이버범죄를 전담하는 사이버범죄수사부(Cyber Division)소속의 운영지원과, 사이버범죄과, 컴퓨터침입범죄과, 특수기술응용과, 능력개발 및 대외협력과 등 5개과를 설치
- 컴퓨터침입범죄과는 해킹수사를 전담하는 '컴퓨터침입범죄수사계'와 사이버 테러를 전담하는 '대테러/방첩 컴퓨터침입수사계', 공격정보 분석을 전담하는 '사이버정보계' 로 구성
- 이와 함께 FBI는 주요 22개 도시에 사이버 태스크 포스 조직을 별도로 운영

## ▶ 국립표준기술연구소(National Institute of Standards and Technology, NIST)

- 상무부 산하 국립표준기술연구소는 연방정보보안관리법(Federal Information Security Management Act, FISMA)에 근거해 정보보안 정책, 절차 그리고 실무뿐만 아니라 정보시스템을 보호하기 위한 표준과 가이드라인 대응에 관해 정부 기관들에게 기술적인 지원을 제공하는 임무를 부여받음
- 2015년 6월에는 취약점 및 위협, 리스크 관리, 보안의 아키텍처, 실천사항, 보안 능력 및 톨에 대한 내용이 보강된 '산업 제어 시스템에 대한 사이버 보안 가이드' 개정판을 발표
- 2016년 7월 '디지털 인증 가이드라인(NIST SP 800-63B 초안)' 개정판을 통해 SMS 메시지를 통한 2단계 인증을 사용 중단할 것을 권고

## 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<sup>1</sup>에서 개발한 의료기기 보안을 위한 생산자 공개문(MSD<sup>2</sup>) 최신

1 Healthcare Information and Management Systems Society의 약자로 IT를 통한 건강 증진에 주력하는 세계 최대 규모의 비영리단체로, 의료기기의 사이버보안 수준을 평가하기 위한 측정도구로 MSD<sup>2</sup>를 제공

버전에 담긴 모든 기본적인 평가요인들에 관한 정보 ▲알려진 취약점을 해결하고 사이버보안을 개선하기 위한 보완통제<sup>2</sup> 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 의무화 하여 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 최고 정보관리자협의회(CIO)가 작성한 보안항목에 대한 승인작업을 수행
  - 국립표준기술연구소(NIST)는 보안기술을 개발하는 연구소로 환경에 따라 보안 설정을 적용/시험 할 수 있는 프로그램을 개발하고, 표준과 가이드라인을 개발하는 업무를 담당
  - 최고정보관리자협의회(CIO)는 보안제도를 실행하는 기관으로서, 예산관리국(OMB)의 지시사항을 이행하기 위해 관련 업무에 대한 계획과 요구사항을 NIST와 함께 처리 및 진행

---

<sup>2</sup> 기존 보안 조치를 보완할 수 있는 추가적인 통제

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
- 전파발생장치에 대한 전파발생기준을 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 방해가 줄 수 있는 전파 장애의 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 47 CFR(The Code of Federal Regulations: 연방법규집)이며, FCC 인증이 필요한 관련규정은 CFR(Code of Federal Register) 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 조치를 했는지 인증하는 제도로서 클라우드의 도입과 이용을 확산시키는 목적과도 연관

- 미 연방정부에 도입되는 클라우드 제품 및 서비스에 대한 보안성 평가&#8228;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&#8228;인증을 수행
- FedRAMP는 전문 평가 대행기관으로 연방정부 1곳과 민간 기업 8곳을 선정하고, 프로그램 운영을 시작

- ▶ 각 정부기관 및 민간분야와 학계가 협력해 개발한 FedRAMP서비스는 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)제도, FISMA(Federal Information Security Management) 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 연방거래위원회(Federal Trade Commission, FTC)는 중소기업이 사이버보안을 강화하여 중요한 데이터를 보호할 수 있도록 국가 교육 캠페인을 시작함 (2018.4)
  - 미국 내 중소기업은 약 3천만 개가 존재하고, 이들은 미국 경제를 이끄는 중요한 요소임에도 불구하고 사이버 공격을 받아서 기술유출과 같은 피해가 발생하고 있으며, 피해는 증가 추세임
  - FTC는 중소기업에서 필요로 하는 사이버보안에 대한 정보를 제공하고 있으며, 교육 자료를 개발하여 배포 할 예정임
- ▶ 미국 상원 의원들이 미국 정부기관<sup>3</sup>에 납품되는 IoT기기의 보안 취약점을 관리하기 위한 가이드라인을 수립하도록 하고, 보안 연구자에게 IoT 보안 취약점을 조사하고 공표할 수 있는 권한을 부여하는 내용의 법안 발의(2017.8)
  - 2020년까지 IoT 기기가 200억 개를 넘어설 것으로 예상되며 IoT 기기를 이용한 DDoS 공 등의 보안위협이 증가하고 있어, 연방정부에 납품되는 IoT 기기에 최소한의 보안 가이드라인을 수립할 필요가 있다는 것이 법안 발의의 취지
  - 법안은 연방 정부기관에 납품하는 IoT기기에 알려진 보안 취약점이 없어야 하며, 변경 불가능한 초기 비밀번호를 설정해서는 안 된다고 규정
  - 법안 발표 후 180일 이내에 예산관리국장은 각 행정기관이 IoT기기를 납품할 도급업체와 계약을 체결할 때 포함해야 할 요구사항을 담은 가이드라인을 발표해야 함
- ▶ 미국 오리건주에서 주 행정기관들의 사이버보안 업무를 최고정보관리책임자(CIO)로 이전하고 사이버보안 강화를 위한 자문위원회 및 전문가 조직을 설치하는 내용을 골자로 한 《SB 90》법안이 발효됨(2017.7)

3 executive agency. 중앙 행정부처와 육해공군, 독립관청, 정부공사 등을 포함

- 새 법안은 사이버보안과 관련된 CIO의 권한을 강화하여 각 행정기관에서 사이버보안 관련 인력을 CIO 산하로 이전하고, 각 행정기관이 사이버보안 분야에서 CIO에 협력할 것을 강제함
  - 주의 모든 행정기관은 리스크 기반의 IT 보안 평가와 개선 프로그램 시행을 위해 CIO에 협력하고, 행정기관의 IT 보안업무 통합과 관련해 CIO가 채택한 계획과 규정, 정책, 표준을 준수해야 함
- ▶ 미국 하원의 양당 의원들이 화이트해커를 활용해 국토안보부(DHS) 시스템의 보안 취약점을 찾아내기 위한 버그 바운티<sup>4</sup> 프로그램을 도입하는 《사이버보안 강화 법안》(Hack the DHS Act)을 발의(2017.6)
- 동 프로그램은 보안 취약점의 발견에 미국 최고의 보안 전문가들의 도움을 받기위한 방안으로 법안 발효일로부터 180일 이내에 국토안보부 장관은 국토안보부 정보시스템의 보안 취약점을 최소화하기 위한 버그 바운티 프로그램을 수립해야 함
- ▶ 미국 메릴랜드주에서 랜섬웨어(Ransomware) 범주에 대한 민사상 손해배상과 강화된 형사처벌을 가능하게 하는 법안<sup>5</sup>이 의회에 제출됨(2017.2)
- 2016년 3월 메릴랜드주 워싱턴 카운티에 위치한 메드스타 헬스(MedStar Health) 종합병원이 랜섬웨어의 공격을 받아 일주일간 컴퓨터 운영 시스템을 폐쇄하는 사건이 발생하는 등 최근 랜섬웨어로 인한 피해가 급증하는 추세
  - 현행 메릴랜드 주법 하에서 랜섬웨어 관련 범주는 공갈죄(extortion)에 해당되어 피해액이 1,000달러 미만일 경우 경범죄로 처벌되어 왔으나 법안이 통과될 경우 랜섬웨어 관련 범죄를 따로 처벌하는 규정이 신설되어 피해액이 1,000달러 미만이라도 중범죄로 기소될 수 있음
- ▶ 미국 연방통신위원회(FCC)는 '광대역통신망 개인정보보호 규정' 마련에 대하여 '보고 및 명령(Report and Order)'을 발표(2016.11)
- 동 규정은 광대역통신망 인터넷접속 서비스 제공자 및 그 밖의 전기통신사업자를 대상으로 개인정보보호 관련 각종 의무를 정하고 있음
  - 보호대상은 전기통신사업자가 수집한 고객통신망정보(Customer Proprietary Network Information, CPNI), 개인식별정보, 통신 내용 등임

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

5 House Bill 340. Criminal Law - Extortion -Unauthorized Software

- ▶ 미국방부(Department of Defense)는 국방부와 계약을 체결하고 있는 계약 당사자 및 하도급업자들에게 사이버 침해사고(cyber incidents)가 발생한 경우 이를 의무적으로 국방부에 보고하도록 하는 국방부 방위산업기지 사이버보안 행위(Defense Industrial Base Cybersecurity Activities)에 관한 규칙의 개정안을 발표함(2016.10)
  - 동 규칙은 국방부와 국방부의 계약상대방 간 공유되는 정보에 보호가 필요한 극도로 민감한 정보가 포함되어 있다는 점에 대한 인식을 바탕으로, 사이버 침해사고에 대한 정보를 공유함으로써 국가의 방위산업기지를 목표로 하는 악의적인 행위를 이해하고 올바르게 대처하고자 하는 움직임으로 보임
  - 동 규칙은 국방부와 방위산업기지 관련 기업 간 체결된 계약의 당사자에게 적용됨