1. 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[1]

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

1 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

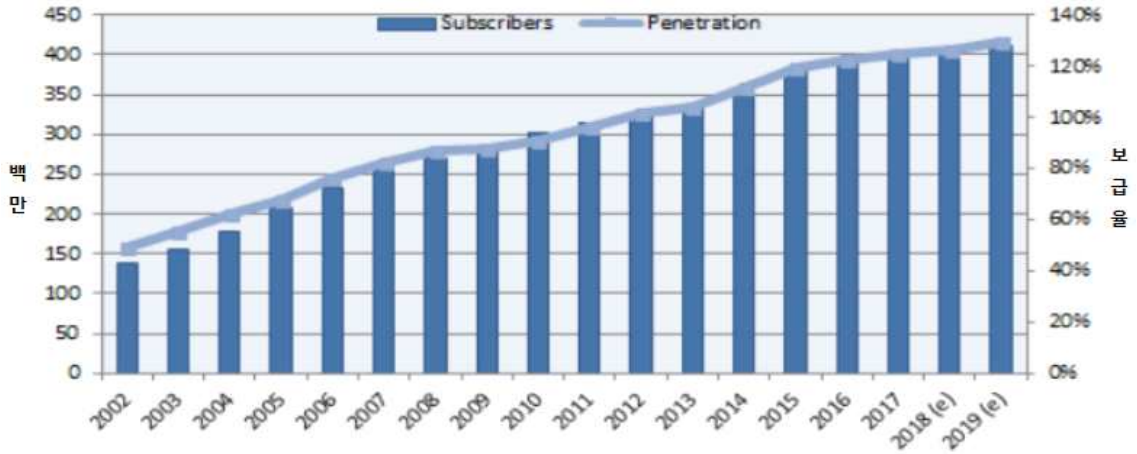
그림 _미국 브로드밴드 가입자 수와 보급률 (단위: 백만 명)

[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

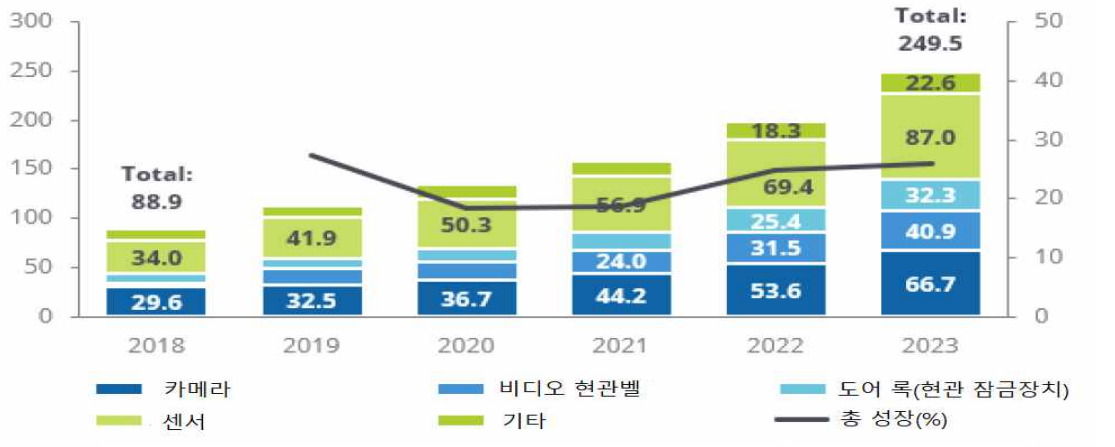
- 카메라 출하량은 2018년 2960만 대에서 2019년 3,250 만대로 증가하여 전년 대비 9.8% 성장할 것이며, CAGR 17.7%로 2023년에는 6670만대를 기록할 것으로 예측
- 카메라 시장은 ▲소비자 수요 증가 ▲가격 하락 ▲공급 업체 경쟁으로 인해 성장될 것이나, 개인 정보 보호에 대한 우려로 인해 시장의 성장이 제한될 것으로 예상
- 비디오 초인종 출하량은 2018년 470만 대에서 2019년 1,640만대로 전년 대비 245.4% 증가했으며,

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

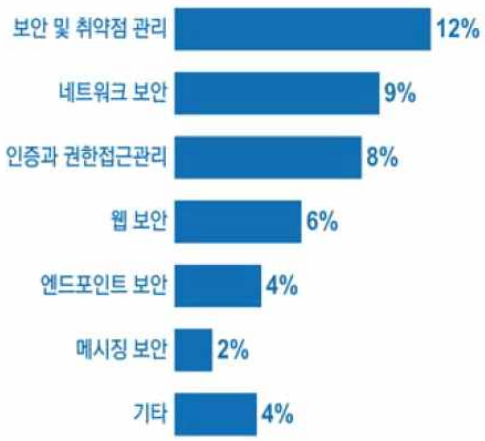
정보보안 제품 및 서비스 시장

▶ 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**

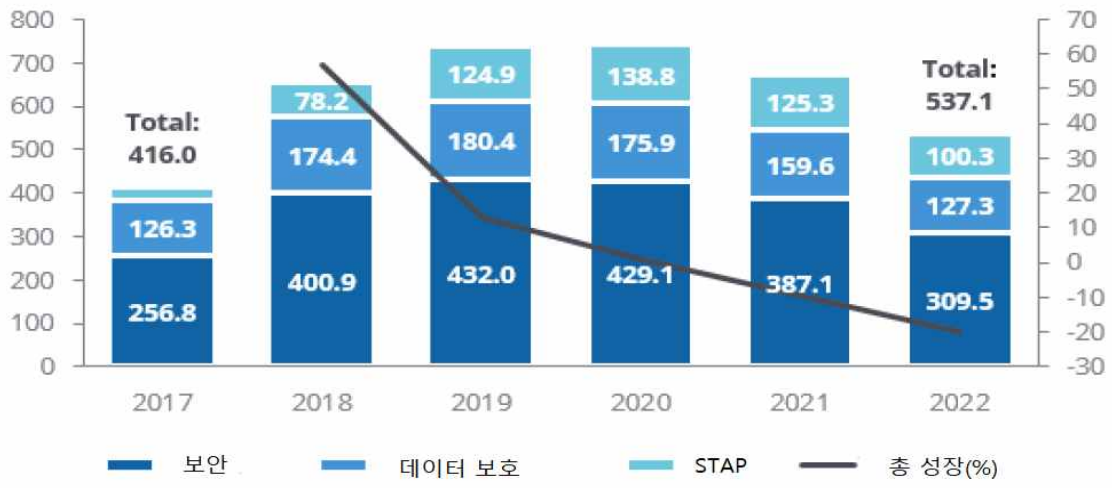
[출처] IDC, 2019.3

▶ 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

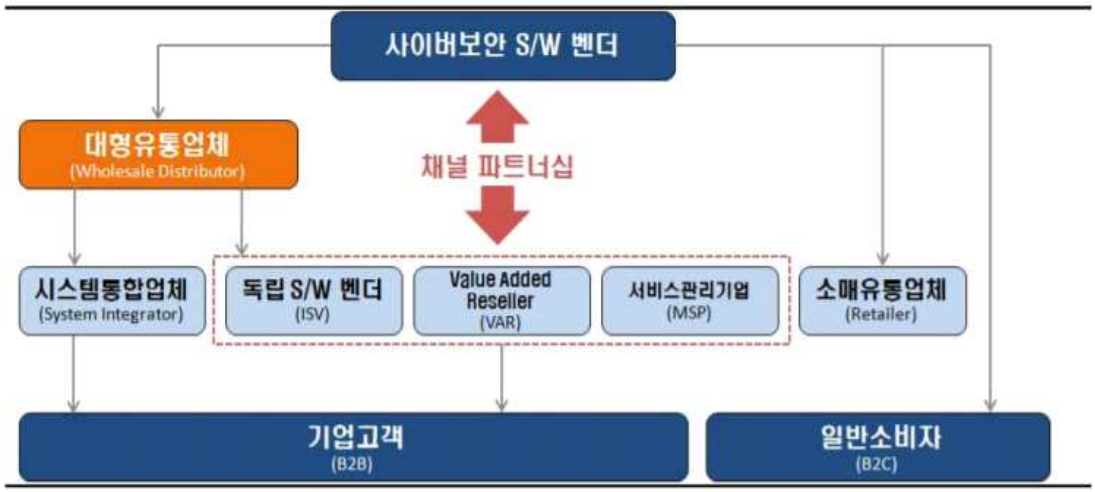
[출처] IDC, 2018

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

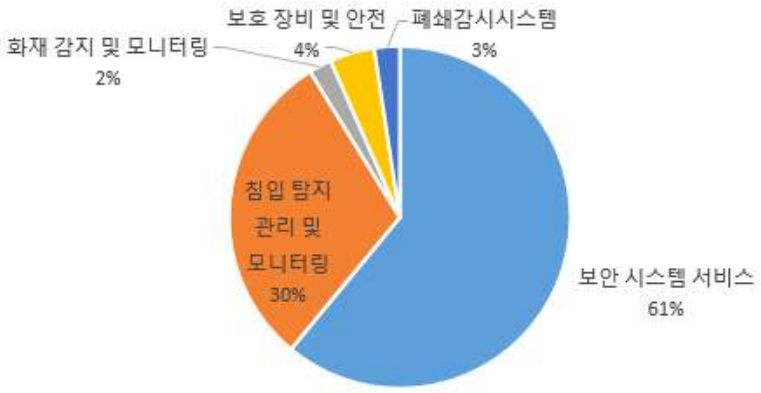
표 _ 미국 물리보안 시스템 서비스 시장

(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)

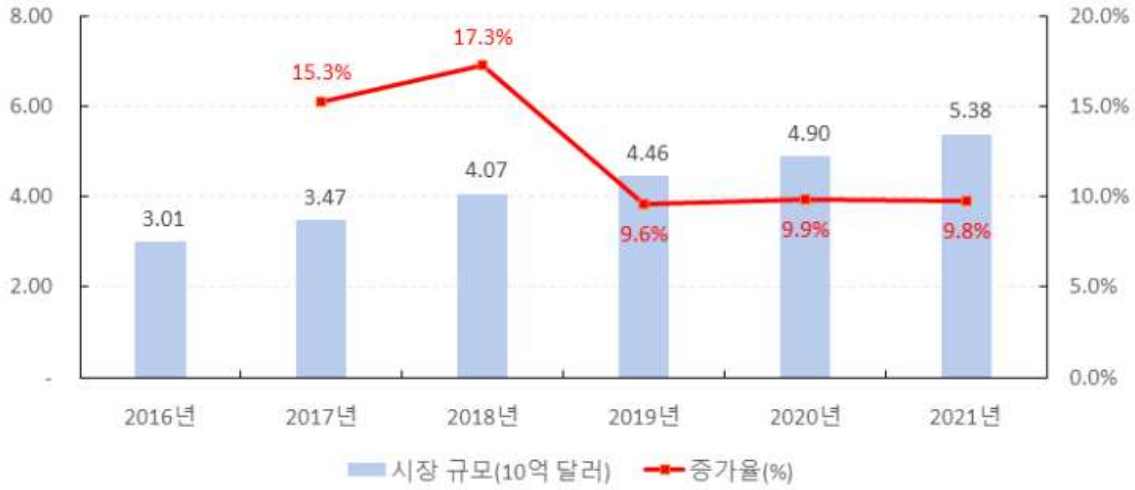


[출처] Barnes Report, 2019 U.S. Security Systems Services Industry-Industry & Market Report, 2019.1

▶ 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

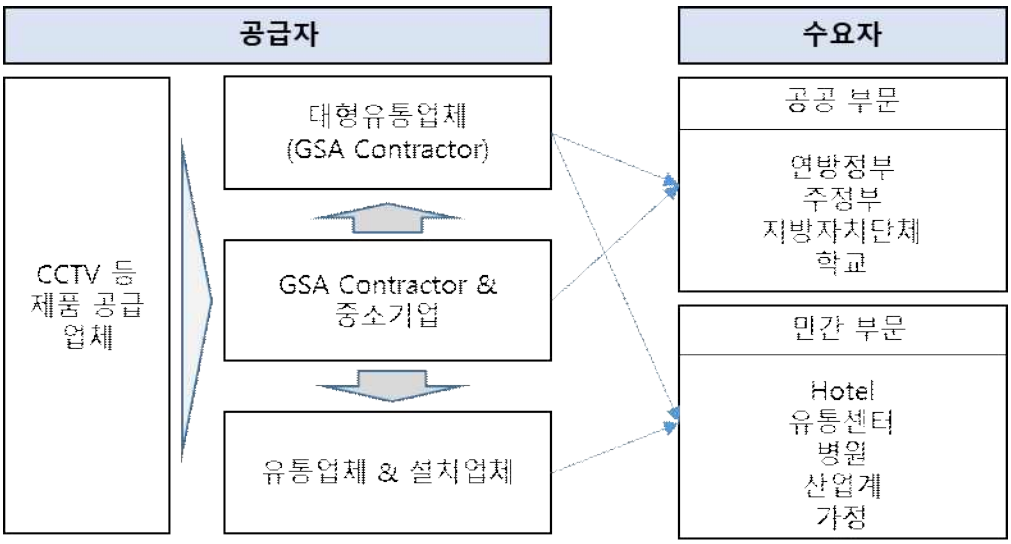
▶ 미국 물리보안 시장의 유통구조는 제품 및 서비스에 따라 시장이 여러 분야로 혼재되어 있어 복잡한 구조를 가지고 있음

- 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

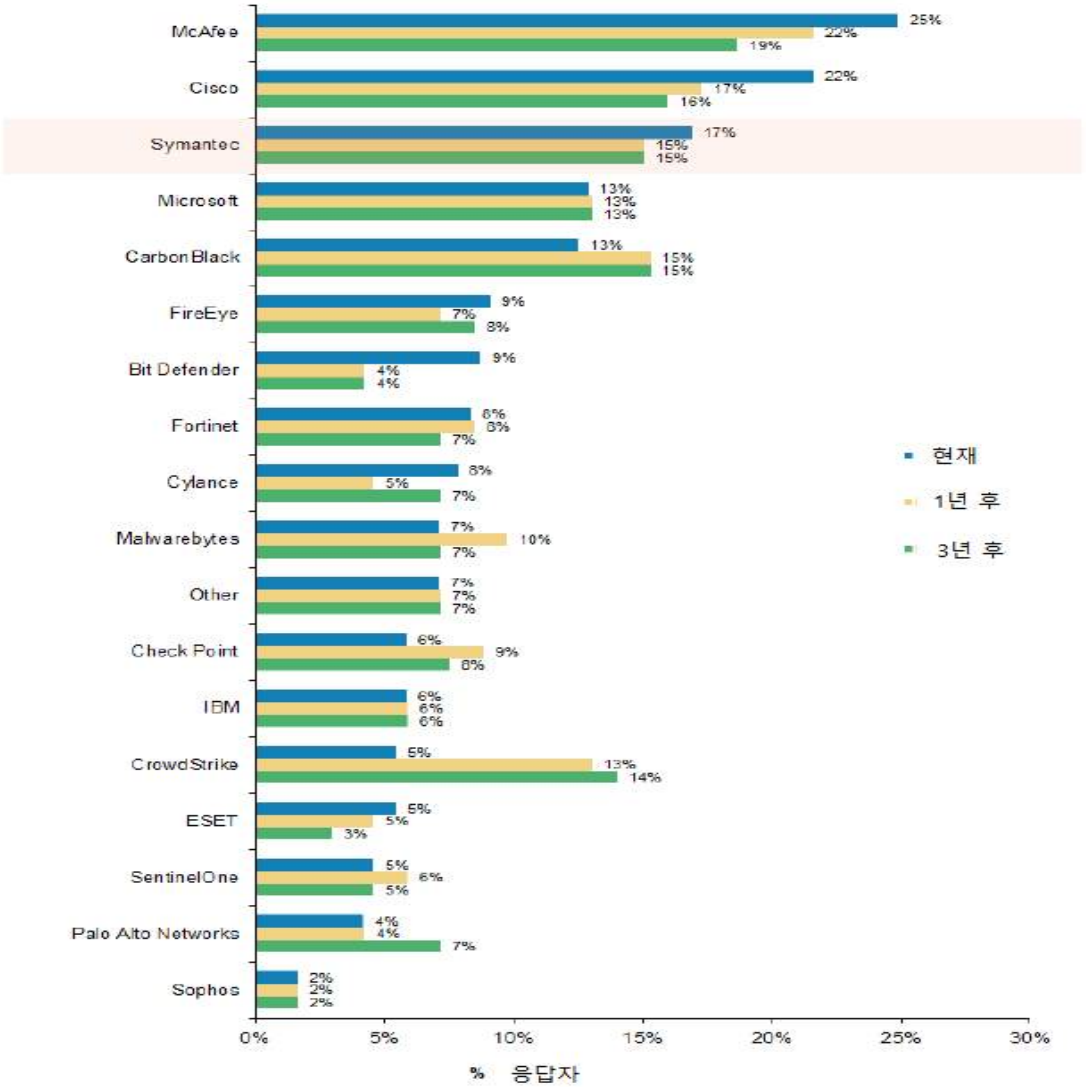
▶ 전 세계 시장의 40%를 차지하는 최대 시장인 미국은 연방정부가 적극적으로 투자 수요를 형성

- 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[2]

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

2 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[3]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

3 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[4]에서 개발한 의료기기 보안을 위한 생산자 공개문(MSD2) 최신 버전에 담긴 모든 기본적인 평가요인들에 관한 정보 ▲알려진 취약점을 해결하고 사이버보안을 개선하기 위한 보완통제[5] 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

4 Healthcare Information and Management Systems Society의 약자로 IT를 통한 건강 증진에 주력하는 세계 최대 규모의 비영리단체로, 의료기기의 사이버보안 수준을 평가하기 위한 측정도구로 MSD2를 제공
5 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[6]	• 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

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

융합보안 시장 및 정책 동향

1) 융합보안 시장 현황[7]

▶ 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[8]

자율주행차

7 미국 스타트업 동향과 시사점, 한국무역협회 뉴욕 지부, 2019.2
8 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[9], 구글의 웨이모(Waymo)의 경우 2018년 12월 애리조나 주에서 세계 최초로 자율주행 택시 서비스 시작[10]

▶ 자율주행차량은 차량 공유서비스보다 대형트럭에 먼저 적용되어 상용화될 가능성이 높음[11]

- 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[12]

2) 융합보안 정책 현황

▶ 미국 국립표준기술연구소(NIST)는 IoT의 사이버보안 및 개인정보보호 관리와 관련된 과제와 해결방안을 제시한 보고서인 'NISTIR 8228'[13]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[14](2019.4)

9 https://www.hankyung.com/economy/article/2019100935081
10 http://www.hani.co.kr/arti/economy/it/873694.html
11 https://www.cnbc.com/2019/11/22/self-driving-trucks-likely-to-hit-the-roads-before-passenger-cars.html
12 https://techcrunch.com/2019/05/29/waymo-is-bringing-its-self-driving-trucks-back-to-arizona/
13 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[15]

- 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[16]

14 https://www.nccoe.nist.gov/projects/building-blocks/mitigating-iot-based-ddos
15 https://news.joins.com/article/22858910
16 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[17]

- 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

17 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)

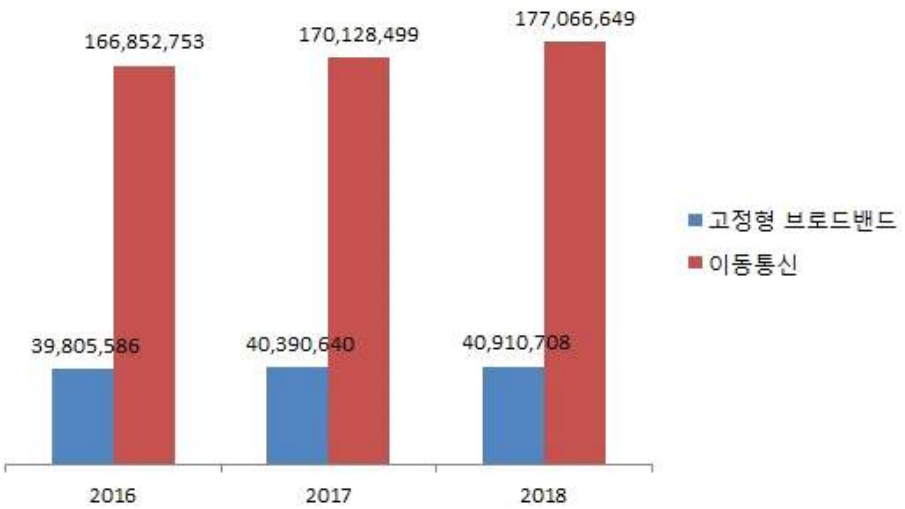
- 일본의 고정형 브로드밴드 가입 회선 수는 매년 미미한 증가세를 보이며 포화 상태에 근접 중
- ITU에 따르면, 2018년 말 일본 브로드밴드 인터넷 가입 회선 수는 4,091만 708회선으로 전년 대비 1.3% 증가
- 일본은 지진, 태풍 등 자연재해가 잦은 지리적·환경적 요인으로 인해 유선 대비 이동통신에 대한 기술 의존도가 높으며, 향후 이동통신 중심으로 투자가 확대될 것으로 예상

▶ 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[18]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

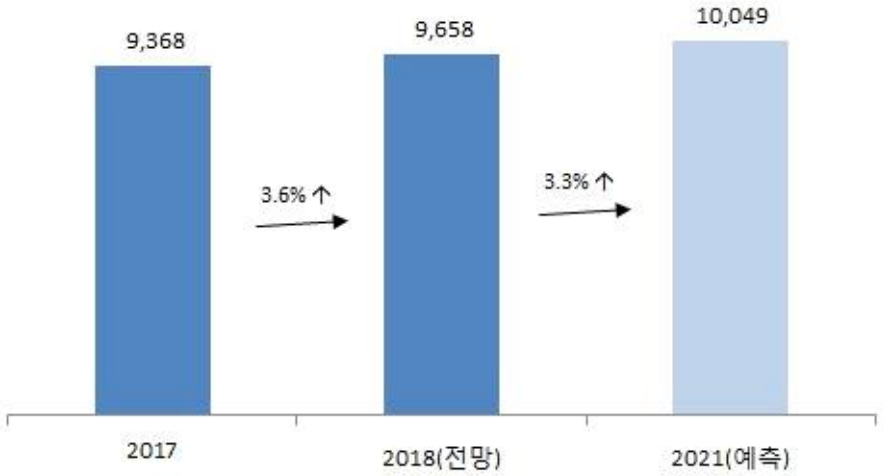
18 富士経済, 監視カメラ・アクセスコントロールシステム・緊急通報サービス・災害・防災関連機器/サービスなど国内のセキュリティ関連機器・システム・サービスの市場を調査, 2018.11

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

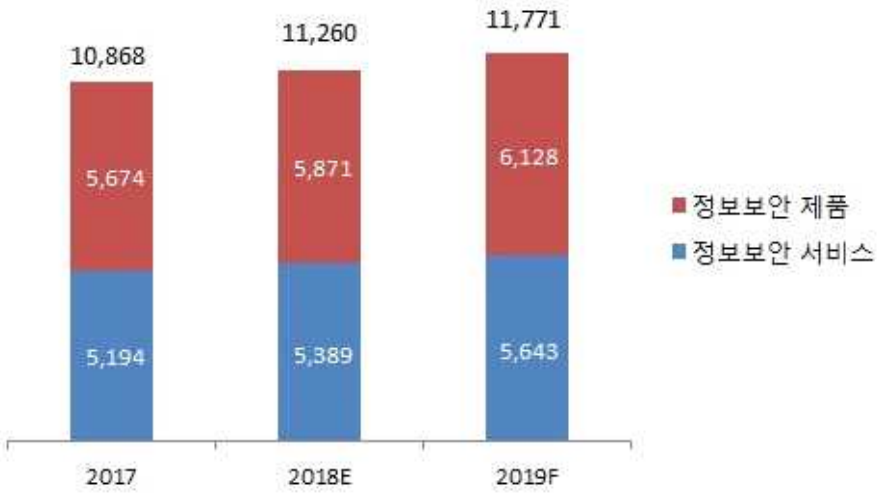
특수는 예상을 밑돌고 있는 상황으로, 향후 동영상 해석, AI, IoT 등의 기술혁신을 통한 새로운 분야에서의 수요 개척을 기대

▶ 일본네트워크보안협회(JNSA)가 일본 내 정보보안 제품과 서비스를 제공하는 사업자를 대상으로 한 조사[19]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

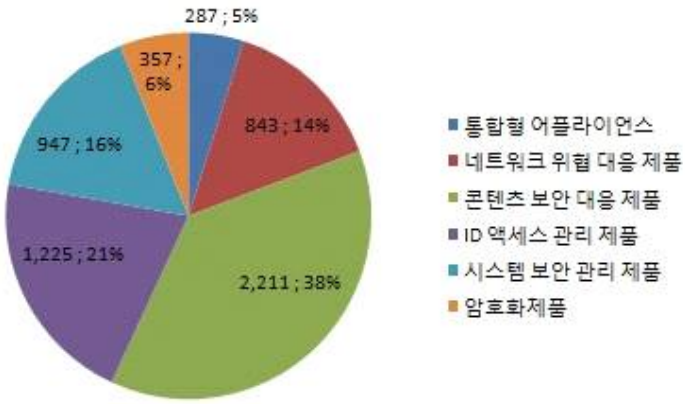
19 日本ネットワークセキュリティ協会(JNSA), 2018年度 国内情報セキュリティ市場調査, 2019.6

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

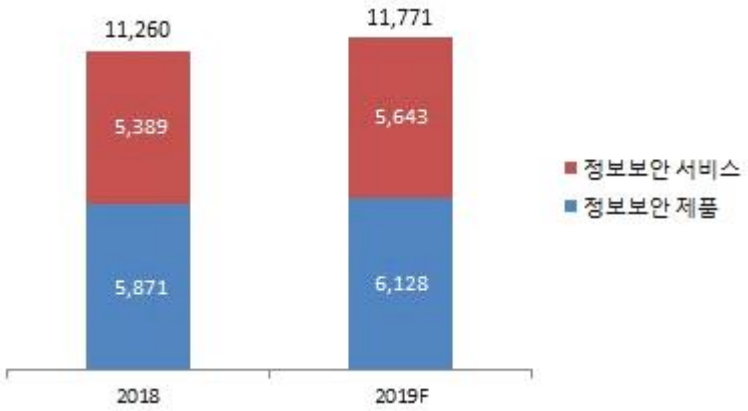
그림 _ 2019년 일본 정보보안 서비스 시장 구성 추산치

(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[20]

20 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

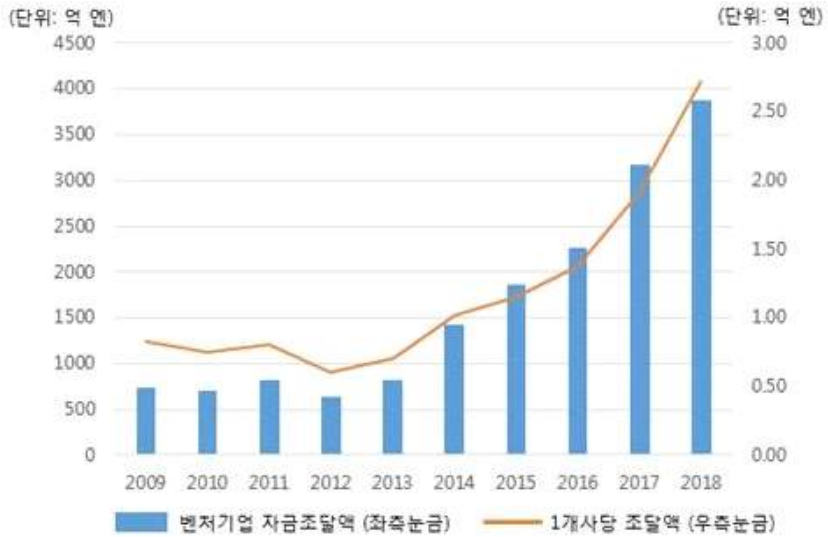
5) 정보보호 스타트업 주요 동향 및 이슈

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[21]

21 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[22]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)

22 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

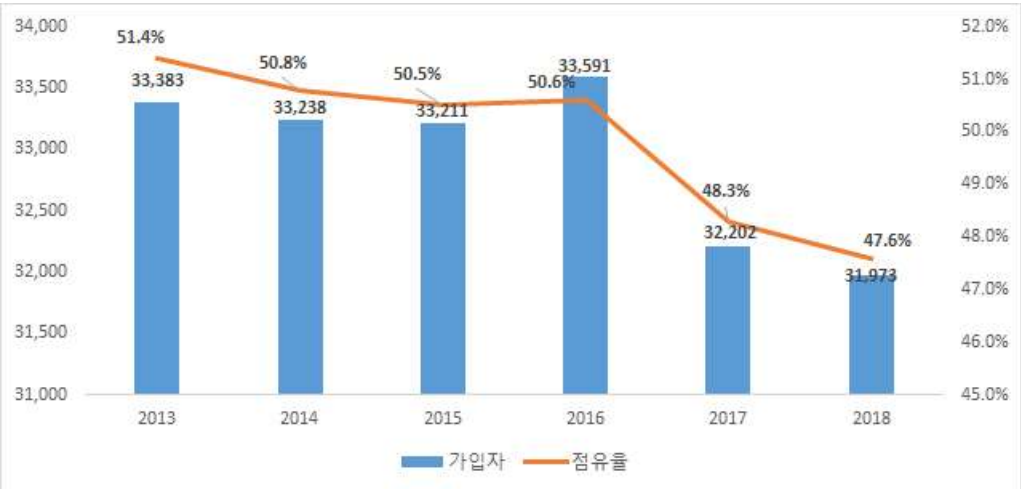
❑ 유선 통신

▶ 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

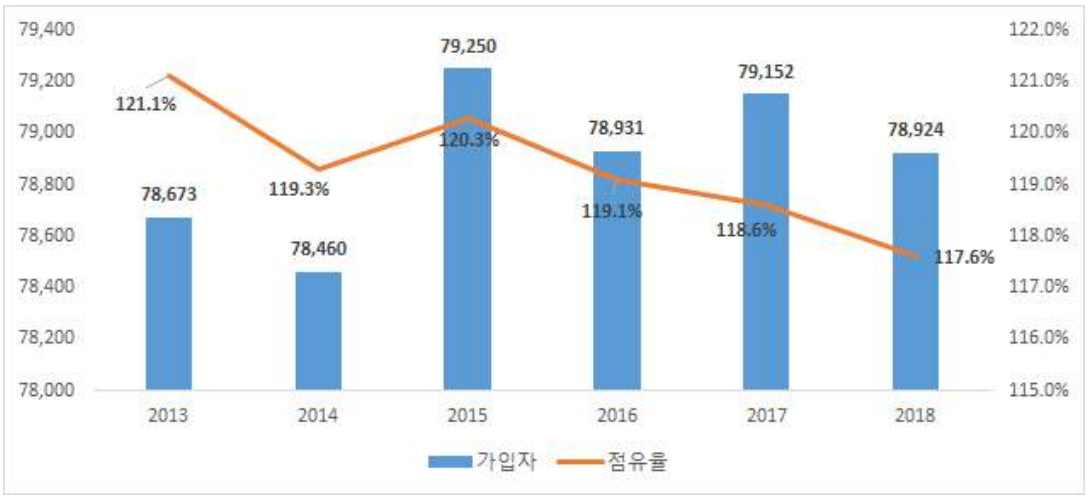
❑ 이동통신

▶ 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)

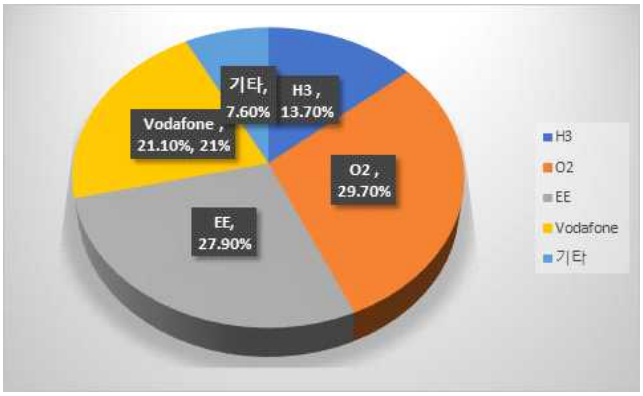
- 영국 4개 이통사(EE, Vodafone, Three, O2)의 LTE 커버리지는 서비스 제공지역의 64%, 실내 76%에

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[23]
- 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[24]
- 2018년 3월 e-borders[25]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[26]

- 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)

23 Guidance launched for in-house monitoring centres, 2018.10.24
24 Surveillance camera guidance, tools and templates, 2018.10.3
25 경찰, 보안, 출입국 관리 목록에 대해 개개인 승객의 세부사항들을 전자적으로 수집하고 체크하는 시스템
26 "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

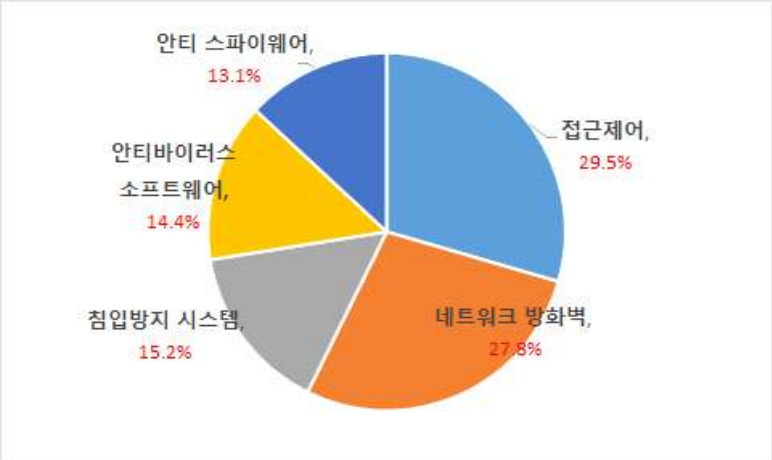
- 2017년 워너크라이(WannaCry*) 공격 등으로 영국 기업은 침입 방지 시스템에 대한 투자를 가속화하고 있으며, 영국 내 보안 소프트웨어를 개발하는 스타트업 수도 증가하고 있음

* 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[27]

▶ 영국 디지털문화미디어스포츠부의 자료에 따르면 영국 사이버 보안 시장은 846개 회사가 활동하고 그 매출 규모는 56억 파운드로 추정[28]

- 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[29]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

27 https://news.kotra.or.kr/user/globalBbs/kotranews/782/globalBbsDataView.do?setIdx=243&dataIdx=171291
28 DMCS UK Cyber Sector Report, 2018.6
29 '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[30]

- 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

30 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

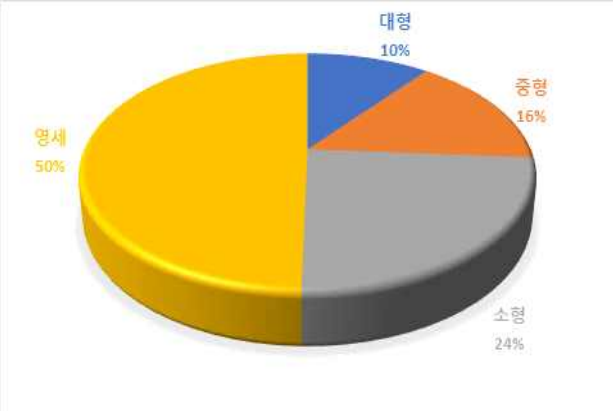
▶ 영국의 물리보안 서비스 업체는 4,800개 내외가 되는 것으로 집계되고 있고 연간 매출 규모는 26억 달러 수준이 되는 것으로 추산

- 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[31]

- 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[32]

31 WaveStone, 2018 UK Cybersecurity Start-Up Radar, 2018.11.9.
32 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[33]
- 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)

33 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[34]

▶ 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[35]

❑ 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

34 http://www.legislation.gov.uk/ukpga/2016/25/contents/enacted
35 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)[36]

- 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[37][38]

36 National Cyber Security Strategy 2016-2021, 2016.11.1.
37 Department for Business, Energy & Industrial Strategy, Civil Nuclear Cyber Security Strategy, 2017.2.14.
38 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

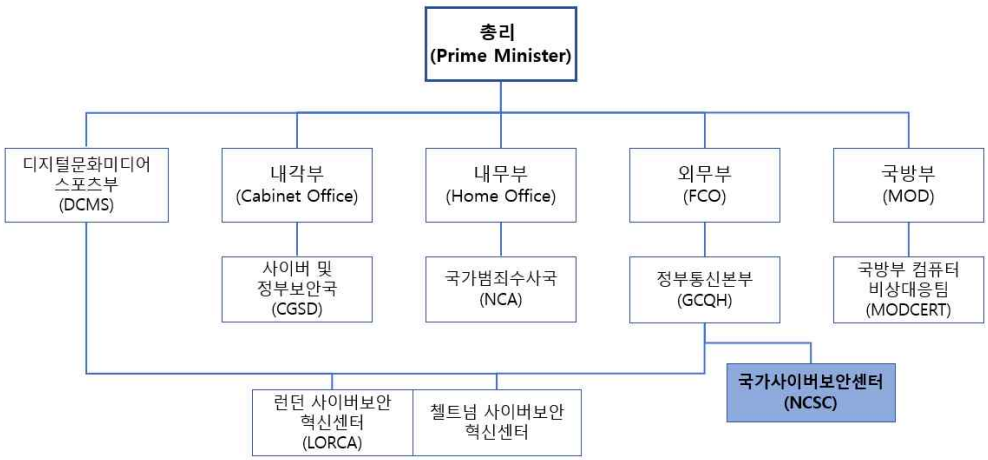
- 영국기술전략위원회(Innovate UK)SMS 2018년까지 디지털 혁신전략을 추진 중
- 동 전략은 2020년까지 영국 경제의 교통, 에너지, 헬스 분야의 혁신을 위해 이용자 편의 중심 디지털 솔루션 개발, 개인정보보호 및 데이터 보안 시스템 설계 지원 등 디지털 생태계 진입을 지원할 계획
- 4년간 매년 3,000만 파운드씩 총 1억 2,000만 파운드를 지원해 나가는 한편 관련한 혁신적인 비즈니스 프로젝트에 매년 1,500만 파운드씩 지원 계획

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)[39]

- 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)[40]

- 영국의 공공이익 관련 정보접근권, 공공기관의 개방성 제고 및 개인정보보호 등을 담당하는 독립기관

39 https://www.gov.uk/government/groups/office-of-cyber-security-and-information-assurance

40 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[41] ▲사이버보안 제품 및 서비스 인증[42] ▲사이버보안 기술 컨설팅 등 사이버보안 관련 폭넓은 영역을 담당
- 영국 산업계, 영국 정부 각 부처, 중요한 국가 인프라 및 민간중소기업 등을 대상으로 사이버 위협관련

41 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

42 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[43] : 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

43 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)[44]

- 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)[45]

- 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)[46]

- 영국은 필수 네트워크와 인프라를 미래 사이버 공격의 위험에 대해 안전하고 복원력 있도록 만들려는

44 국가사이버보안센터(NCSC), 'Increased Cyber Threats: Security steps to take', 2018.5.16
45 DCMS, 'Secure by Design: Improving the cyber security of consumer Internet of Things Report', 2018.3.7.
46 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)[47]

- 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

47 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[48]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

48 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)[49]

- 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[50]

- 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

49 Department for Transport, "The key principles of vehicle cyber security for connected and automated vehicles", 2017.8.6.
50 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.[51] 구체적으로 개인 데이터 안전 저장, 정기적 소프트웨어 업데이트, 데이터 삭제 용이, 디폴트

51 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[52]

- 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[53]

- 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[54]

▶ 2018년 Smarter London Together 계획을 통해 런던 스마트 시티 로드맵 발표[55]

- 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

52 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
53 http://magazine.hankyung.com/business/apps/news?popup=0&nid=01&c1=1011&nkey=2018052101173000071&mode=sub_view
54 https://www.connectingbristol.org/strategy/
55 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)[56]

- 매년 전 세계 스마트 시티 순위를 발표하는 스페인 바르셀로나 IESE 비즈니스 스쿨의 2019년 발표에서 런던이 1위를 차지

56 https://www.london.gov.uk/what-we-do/business-and-economy/supporting-londons-sectors/smart-london/smarter-london-together