

Global Market Report

미국 사이버보안시장 동향과 우리기업 진출을 위한 시사점



CONTENTS

목 차

요 약 / 1

I. 조사배경 / 4

II. 글로벌 사이버보안 시장 개요 / 7

- | | |
|----|---------------------|
| 7 | 1. 산업의 정의 및 세부시장 분류 |
| 10 | 2. 사이버범죄 동향 |
| 13 | 3. 글로벌 시장 현황 |
| 18 | 4. 글로벌 투자 동향 |

III. 미국 사이버보안 시장 개요 / 21

- | | |
|----|---------------|
| 21 | 1. 시장 현황 및 전망 |
| 27 | 2. 정부정책 동향 |
| 29 | 3. 주목해야 할 트렌드 |

IV. 미국의 주요 사이버보안기업 현황 / 32

V. 미국의 사이버보안 유통 현황 / 48

- | | |
|----|------------|
| 48 | 1. 유통구조 |
| 49 | 2. 주요 유통기업 |

VI. 국내 사이버보안 산업 현황 및 문제점 / 52

- | | |
|----|-------------------|
| 52 | 1. 국내 사이버보안 산업 현황 |
| 54 | 2. 문제점 |

VII. 우리기업 진출을 위한 시사점 / 55

참 고 문 헌 / 60

요 약

I. 조사배경

- 모든 사물이 인터넷으로 연결되는 **초연결사회**로 진입이 급속하게 진행됨에 따라 **사이버보안산업** 시장은 어떤 산업보다 **가파르게 성장**하고 있는 중
- 사이버보안은 단순한 산업의 영역을 벗어나 **국가안보와 국민생명이 직결된 핵심기간 산업**으로서 **중요성이 부각**되고 있는 추세
- 주요 선진국들은 정부 주도하에 **사이버보안산업 경쟁력 확보**에 총력전을 펼치고 있으나, 우리의 경우 투자 부족, 내수위주 사업, 미래기술 확보 부진 등으로 **급성장**하고 있는 **글로벌 사이버보안시장 경쟁**에서 **뒤쳐지고** 있음.
- 이러한 배경에서, **본보고서는 미국 사이버보안시장 현황, 주요 기업의 사업전략, 유통구조 등을 분석**함으로써, **우리기업들이 세계 최대 미국 시장에 진출하는데 있어 시사점을 제공**하고자 함.

II. 글로벌 사이버보안 시장 개요

- (정의 및 분류) 사이버시장은 사이버 상의 범죄, 테러, 해킹 목적의 접근 및 스파이행위 등으로부터 정보, 시스템, 네트워크를 보호하는 IT솔루션으로,
 - ①네트워크보안, ②데이터보안, ③신원 및 접근관리, ④엔드포인트보안, ⑤어플리케이션보안, ⑥클라우드보안으로 세부 분류됨.
- (사이버범죄동향) 사이버범죄로 인한 경제손실은 연간 4천억 달러에 달하고 **초연결사회 도래에 따라 '19년까지 피해는 최대 2조 달러에 달할** 전망
 - 사이버범죄는 갈수록 **진화**하여 **중요기반시설(에너지, 금융, 교통)을 공격대상**으로 하는 등 **지능화·고도화·조직화**되는 추세
- (글로벌시장) 전 세계 사이버보안시장은 '15년 754억 달러에서 '21년에는 1,200억 달러 규모로 성장(연평균 8.1%)할 것으로 전망
 - ▲북미지역이 전체의 41%를 차지하는 최대시장으로 향후에도 7% 이상 성장이 기대됨. ▲분야로는 클라우드와 어플리케이션보안이 '21년까지 각각 14.2%, 10.7% 성장하여 전체 시장의 성장을 주도. ▲미국이 전체시장의 29%('15년, 221억 달러)를 차지, 향후에도 최대시장 지위 유지 전망

- (투자) '15년도 글로벌 사이버보안 관련 벤처투자는 총 360건, 37억 달러에 달하나, '16년도에는 전년대비 17.7%가 감소한 30억 달러에 그칠 것으로 전망
 - 최근 기업들은 자체 통합솔루션을 제공할 수 있는 대형화를 추구하고 있어, 지난 5년 동안 M&A 거래(금액)가 무려 235% 증가 ('15년 총 거래금액 38억 달러)

III. 미국 사이버보안시장 개요

- (시장전망) 미국 시장은 '15년 220억 달러에서 '21년에는 346억 달러로 연평균 7.8%의 성장세를 구가할 전망 (시장점유율도 29% 수준유지)
 - ▲미국 경제 호조세 ▲인터넷·스마트기기 이용증가 ▲연방정부의 적극적 투자 ▲중국·러시아와의 사이버군비경쟁 ▲IoT 등 신기술 시장 확대 등이 성장요인
- (정부시장) 美연방정부는 미국 사이버보안시장의 최대 투자가이자 소비자로 전체시장의 58%에 달하는 연간 140억 달러의 예산을 집행함.
 - 연방정부의 사이버보안 관련 예산은 '22년, 220억 달러까지 확대 전망
 - ▲부처별로는 국방부에 전체 관련 예산의 68% 이상을 배정. ▲지역별로는 워싱턴광역지역(버지니아, 메릴랜드州)에서 전체 정부지출의 64%가 집행됨.
- (트렌드) 주목해야할 시장 동향으로는 ▲국가안보전략으로서 사이버 억제력 개념 ▲미래 사이버산업의 중추인 블록체인 기술 ▲클라우드, 사이버보안의 대세 ▲정부수요가 견인하는 멀티팩터 인증기술 ▲암호화·복호화 기술 ▲머신러닝과 인공지능 기반 기술 등이 있음.

IV. 미국의 주요 사이버보안 기업

- 사이버보안 분야 상위 15개 기업의 매출 총합은 글로벌 전체 시장의 27% 수준에 그쳐, 특정기업이 시장에서 뚜렷한 우위를 점유하지 못하고 있는 완전경쟁 시장구조가 형성되어 있음.
 - 하지만, 빅데이터와 클라우드보안 시장에서 주도권을 확보하기 위해 기업들은 M&A를 통해 빠르게 대형화 경쟁에 뛰어들고 있음.

V. 미국의 사이버보안 유통 현황

- 사이버보안 유통구조는 벤더가 직접 온라인 등을 통해 소비자에게 판매하는 직접 판매방식과 전문유통업체를 통한 간접 판매방식으로 분류
 - 근래 들어, 사이버보안기업들은 독립소프트웨어 벤더 또는 서비스 관리기업 등과 『채널파트너십』을 통해 제품을 유통하는 방식을 적극 활용 중

VI. 국내 사이버보안 산업 현황 및 문제점

- (산업구조) 국내 사이버산업은 기업 규모의 영세성과 과도한 출혈경쟁으로 질(質)보다는 양(良)적 성장에 치우친 한계점을 보임.
- (수출부진) 국내기업들의 전체매출에서 수출이 차지하는 비중은 5%에도 미치지 못하는 등 글로벌 시장 진출 기반이 열악한 상황
- (기술확보) 제한적 대상(공공기관, 통신시설) 및 특정분야(개인정보보호 등) 중심으로 투자와 연구개발이 진행되어 新성장동력 확보 미진

VII. 우리기업 진출을 위한 시사점

- “사이버보안 생태계 조성을 위해서는 공공-민간 파트너십이 해답이다.”
 - 이스라엘은 정부주도 하에 유기적 공공-민간 협력시스템을 구축하여 전 세계 사이버보안 시장을 선도하는 국가로 거듭남.
- “기술은 실리콘밸리에서 돈은 워싱턴으로, 연방 정부시장에 주목해야”
 - 미국 연방정부의 사이버보안 공급을 주도하고 있는 해외국방기업들과의 협력 도모를 위해서는 무엇보다 『국방절충교역제도』 활용이 관건
- “신기술 트렌드에 주목해야, 미국기업들은 여전히 기술에 목마르다.”
 - 현실적으로 글로벌기업과의 기술격차가 엄존하는 상황에서 우리기업의 생존전략은 미래기술와 틈새시장에서의 경쟁력과 전문성을 확보하는 것
- “채널파트너십 전략, 완전경쟁시장 환경에서 돌파구”
 - 우리기업들도 미국시장 진출을 도모하기 위해서는 글로벌 기업들의 채널파트너 생태계에 적극 참여하고 적응하는 전략을 활용해야함.
- “사이버보안 전문인력 양산을 통한 해외 인력 수출 기회 모색 필요”
 - IoT, 클라우드 등 차세대 사이버보안산업의 국내 인재들이 해외기업에 취업하여 글로벌 전문가로 성장할 수 있는 기회 발굴 필요

- 모든 사물이 인터넷으로 연결되는 **초연결사회(Hyper-connected Society)**로 진입이 급속하게 진행되면서 사이버보안 시장은 빠르게 성장 중
 - 사물인터넷(IoT), 빅데이터 기술로 인한 유·무선 인프라의 고도화, 트래픽의 비약적 증가, 스마트기기 확산 및 제3차 산업혁명으로 일컬어지는 제조업의 디지털화 등으로 사이버공간은 무한확장 일로
 - 세계적 경영컨설팅사 맥킨지가 세계경제포럼에서 제출했던 보고서, 『초연결사회에서 위험과 책임』에 따르면 **매스데이터 분석, 클라우드 컴퓨팅, 빅데이터 등 첨단기술 도입으로 '20년까지 최소 9조6천억 달러에서 21조6천억 달러의 경제 효과가 발생할 것으로 전망**
 - 반면, 보안기술 발전 속도를 앞서는 사이버공격과 혁신을 저해하는 규제의 영향으로 3조 달러의 경제 손실이 발생할 것으로 예상
- 세계적으로 사이버보안은 단순히 산업의 영역을 벗어나 국가안보와 국민생명이 직결된 국가 기간산업으로서 가치가 강조되는 추세
 - 나날이 지능화·고도화되고 있는 사이버공격으로 인해 막대한 경제적 피해와 국가·사회적 혼란이 야기되는 등 그 위력이 사이버 공간을 넘어서 이미 현실적 위협으로 전이되고 있으며,
 - 전력, 통신, 교통 등 국가 핵심 인프라 시설을 대상으로 한 사이버 테러가 증가함과 동시에 국가 간 사이버 준비 경쟁이 가속화되고 있음.
 - * 미래부에 따르면, 사이버공격으로 인한 경제적 피해 규모는 연간 3.6조원으로 자연재해 피해액(1.7조원)의 2배를 상회함.
 - McAfee와 국제전략연구소(CSIS)는 공동연구¹⁾를 통해 **사이버공격으로 발생한 경제 피해액은 연간 3,720억~5,750억 달러*에 달할 것으로 추산함.**
 - * 연간 인터넷 산업으로부터 창출된 총 경제생산 2-3조 달러의 15-20%에 해당함.

1) McAfee, Net Losses: Estimating the Global Cost of Cybercrime

- 주요 국가들은 정부 주도하에 사이버보안 기술 확보에 주력하고, 급성장하고 있는 시장에서 우위 선점을 위해 막대한 투자를 진행 중
 - 4대 사이버보안 기술 선진국(미국, 이스라엘, 러시아, 중국)은 전 세계 시장의 58%를 차지하고 있으며, 비공식 통계에 따르면, 글로벌 투자의 72%를 담당하고 있는 것으로 추산됨.
 - * 세계시장점유율('15년) : 미국(29.2%), 이스라엘(10.0%), 중국(9.9%), 러시아(8.7%)
 - 특히, 이스라엘은 불과 5년 전까지만 해도 세계시장 점유율 1~2%에 불과하던 자국의 사이버보안 산업을 육성하여, '15년에는 연간 수출 65억 달러, 세계시장 점유율 2위의 선진국으로 도약함.
 - 이스라엘 정부는 '11년, 국가 사이버보안산업 육성 전략을 수립하고, 공공-민간협력 생태계를 구축, 명실상부 『Startup Nation』 으로 발돋움.
- 반면, 우리나라는 투자 부족, 내수위주 사업 등으로 新성장동력 확보가 미흡하여 급성장하고 있는 해외 사이버보안 시장에서 실기하고 있는 중
 - 『낮은 인식·투자 ▶ 보안솔루션·서비스 저평가 ▶ 기업수익 악화 ▶ 우수인력 기피 ▶ 기술·제품 경쟁력 저하 ▶ 신규시장 준비미흡 ▶ 국제 경쟁력 낙후』²⁾로 이어지는 악순환이 지속됨.
 - * 시장구조 악화에 따라 업계의 신규창업이 감소하는 추세 : 2000-2005년(224개), 2006-2010년(169개), 2011-2014년(60개)³⁾
 - 국내 사이버보안 기업 256개 중 35개(14%) 기업만이 해외 수출을 하고 있으며, 수출액은 전체 매출의 4.7%에 불과함.
 - 권역별 수출 비중도 일본(40.7%), 중국(17.1%)에 집중되고 있으며, 세계 최대 시장이자 기술 선진국인 미국으로의 수출은 2.0%에 불과
- 이러한 배경에서, 본보고서는 미국 사이버보안시장의 현황, 주요 기업의 사업전략, 현지 유통구조 등을 분석함으로써 우리기업들이 세계 최대 미국 시장에 진출하는 데 있어 시사점을 제공하고자 함.

2) 미래창조과학부, K-ICT 시큐리티 발전전략 (2015.4월)

3) 한국정보보호산업협회, 2015 국내정보보호산업 실태조사 결과보고서 (2015.12월)

[참고자료1] 모건스탠리, 사이버보안 : 패러다임 변화의 시기

- '16년도 기준 전 세계 사이버보안시장은 600억 달러에 육박하고, '20년까지 그 규모가 2배 이상 확대될 것으로 전망
 - '20년까지 사이버보안 시장은 전체 IT시장의 연평균 성장률보다 4배 이상 높은 성장*을 누릴 것으로 예상함.
 - * 사이버보안(18%), IT하드웨어 및 소프트웨어(4%), IT서비스(3%), 통신장비(3%)
- 모든 사물이 인터넷으로 연결되는 초연결사회로의 진입이 가속화됨에 따라 사이버범죄 노출 위험이 연평균 60% 이상 증가
 - 대기업들은 연간 수천만 달러의 직·간접 피해를 입을 뿐만 아니라, 특히 중소기업의 경우 사이버공격 피해 이후 6개월 이내 피해기업의 60%가 폐업하는 등 그 피해가 극심함.
 - 이에 미국정부는 민간기업과 기간 인프라 시설 보호를 위해 '17년까지 최소 200억 달러의 예산 투입 계획을 밝힘.
- 지속적 시장 확대 전망에도 불구하고, 현재의 사이버보안 기술은 지나치게 복잡하고 비효율적이라고 지적하며, 산업 패러다임의 변화는 이미 시작되고 있다고 보고함.
 - 자체 구축형 보안 프로그램(On-Premise)이 서서히 쇠퇴하고, 클라우드 기반 보안솔루션으로의 대체가 급격히 진행 중
 - '19년까지 클라우드 보안 분야의 연평균 성장률은 19%에 달하는 반면 One-Premise는 3% 성장에 그칠 전망
- 업계는 이러한 통합 클라우드 기반 솔루션 제공 환경에 적응하기 위해 인수합병 등을 통해 몸집 불리기 전략을 활용하고 있음.
 - 따라서, 5대 대형 보안업체의 시장점유율이 현재 26%에서 수년 내 40%로 확대되는 등 소수 대기업 위주로 산업 재편이 진행 중
- 이러한 전환의 시기에 생존을 위해서 중소기업들은 특수 목적 시장에 특화된 틈새 기술 개발에 집중하여야 할 것임.

II

글로벌 사이버보안 시장 개요

1

산업의 정의 및 상세 시장 분류

- **[정의]** 사이버보안은 사이버상의 범죄, 테러, 해킹 목적의 접근 및 스파이 행위 등으로부터 정보, 시스템, 네트워크를 보호하는 IT 솔루션을 일컬으며,
 - 암호, 인증, 인식, 감시 등의 정보보호 기술이 적용된 제품을 생산하거나, 해당 기술을 활용, 재난·재해·범죄 방지 서비스를 제공하는 산업으로,
 - 『네트워크·시스템기반의 정보보안』 과 『보안기술과 전통 산업간 융합으로 창출되는 융합보안』 을 포함함.
- **[분류]** 사이버보안 시장은 기술 운영의 목적과 적용범위 등을 기준으로 아래와 같이 6개의 상세시장으로 분류할 수 있음.

1) 네트워크 보안 (NetSec : Network Security)

- 네트워크에 비인가자의 접근, 오용, 교란 또는 인가된 사용자의 시스템 접근을 방해하는 시도 등을 감시하고 방지하는 솔루션으로,
- 침입감시시스템(IDS, Intrusion-detection-system), 게이트웨이/방화벽, 가상 사설망(VPN, Virtual Private Network), 콘텐츠 필터링 도구 등을 포함
 - * 대표 기업으로는 Cisco, Check Point, Juniper Networks, Fortinet, McAfee, Palo Alto Networks, MicroSoft, IBM 등이 있음.

2) 데이터 보안 (DataSec : Data Security)

- 비인가 외부 사용자의 침입과 데이터 오용·손상으로 부터 보호하는 솔루션으로, 본격적으로 BYOD⁴⁾ 시대가 도래 하면서 기업정보 유출 예방 기능에 대한 수요가 급격히 증가하고 있는 추세. 특히 전자의료기록 정보 보호가 최근 각광받고 있는 중
 - * Symantec, McAfee(Intel), Websense 등이 주요 플레이어로 꼽히며, 그 외에도 Check Point, Trend Micro, Fidelis 등이 활약 중

4) Bring Your Own Device : 개인이 소유한 스마트기기를 회사 업무에 활용하는 추세

3) 신원 및 접근관리 (IAM : Identity & Access Management)

- 시스템 운영자(기관)가 내부 시스템과 서비스에 대해 사용자의 접근을 허용 또는 차단하기 위한 솔루션으로, 암호화 알고리즘에서부터 신원인증 시스템까지 계정 및 비밀번호 관리와 관련된 일체의 기술
- 클라우드 컴퓨팅이 빠르게 도입되면서 사이버공격에 대한 안전 장치로서 신원인증 솔루션의 수요가 증가하고 있는 추세
- * EMC, IBM, Symantek, Oracle 등 주요기업들 뿐만 아니라 중소형 기업들도 적극적으로 가담하여 경쟁이 활발한 시장임.

4) 엔드포인트 보안 (EndSec : Endpoint Security)

- 중앙 네트워크에 연결된 단말기(데스크톱, 랩톱, 스마트폰, 테블릿, ATM 등) 단계에서의 보안 기술로 최근 말웨어(악성코드) 위협 증가 등으로 인해 꾸준히 증가하는 시장임.
- * Symantec이 전체 시장의 1/3 가량을 점유하고 있으며, McAfee(Intel), Trend Micro, Kaspersky Lab 등이 추격하고 있는 상황

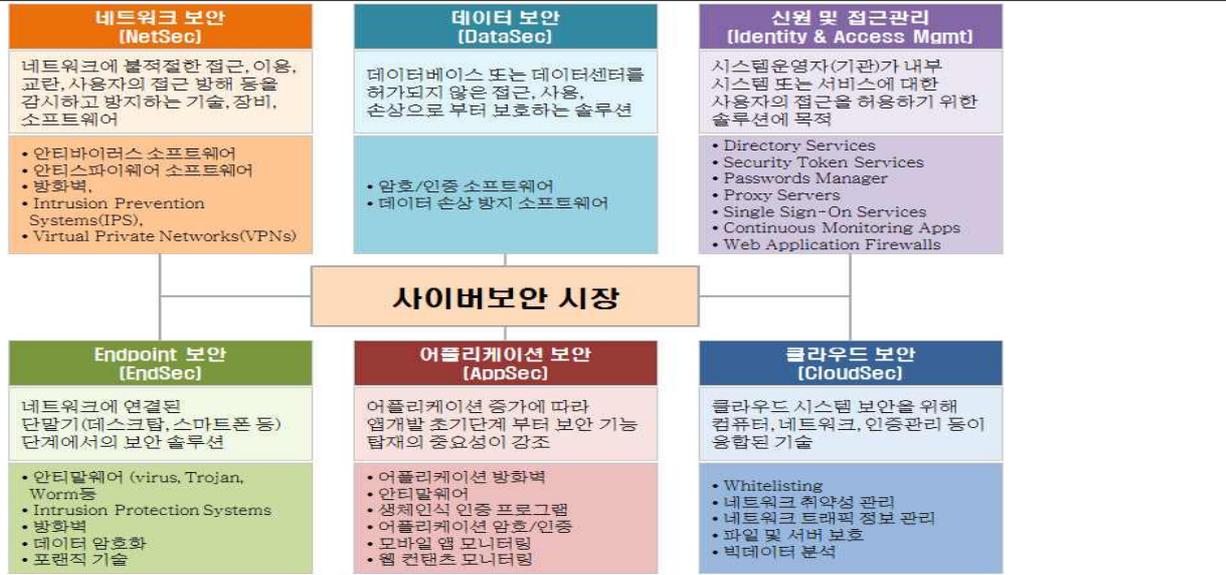
5) 어플리케이션보안 (AppSec : Application Security)

- 어플리케이션에 대한 외부로부터 부적절한 접근, 수정, 삭제, 오용을 예방하기 위한 기술로서 어플리케이션 증가에 따라 최근 앱 개발 초기단계 부터 보안 기능 탑재의 중요성이 강조되는 추세
- 급속한 모바일 스마트 기기 대중화와 BYOD 트렌드 확산으로 기업용 모바일 보안 솔루션 기술이 각광받고 있음.
- * 모바일 어플리케이션 보안기업으로는 Airwatch, Lookout, Good Technology 같은 신생기업들의 진출이 활발한 특징

6) 클라우드보안 (CloudSec : Cloud Security)

- 클라우드 기반 인터넷 데이터베이스 시스템의 보안을 위해 컴퓨터, 네트워크, 정보 및 인증관리 등이 융합된 솔루션으로 ID 접속관리, 엔드포인트, 웹 필터링, 네트워크 보안 분야에 빠르게 적용되고 있음.
- * 선도업체로 Cisco, Zscaler, Forcepoint, Symantec, McAfee 등이 활약 중

[그림1] 사이버보안 시장 세부시장 분류



[자료원] VisionGain / 워싱턴무역관 재배치

[표1] 사이버보안 세부시장 특징 및 규모

단위 : 십억 달러

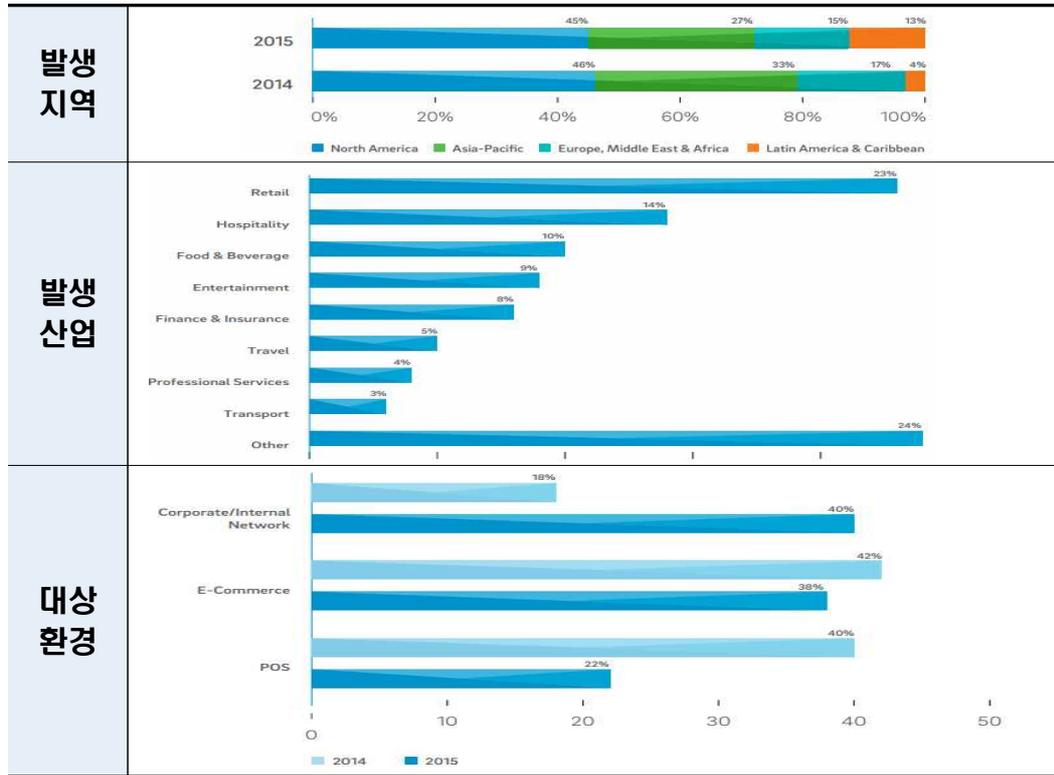
분류		내용	시장 규모('13년)	연평균 성장률
네트워크 보안	방화벽	비인가자 침입방지, 데이터암호화, 보안가상 접속 등	26	-1.6% (2012-2017)
	침입감시/예방	네트워크 접근 감시/방지 등	19	3.4% (2012-2017)
	콘텐츠 보안	말웨어로 부터 이메일 및 웹콘텐츠 보호 및 필터링 등	31	1.7% (2012-2017)
	데이터유실예방	데이터 접근제한, 조작방지, 디스크 암호화 등	7	14.6% (2011-2016)
	통합위협관리	단일보안솔루션을 통한 보안어플리케이션	32	14.1% (2012-2017)
	데이터센터	데이터베이스, 파일, 어플리케이션 공격 예방 솔루션	130	9.3% (2012-2017)
소프트웨어 보안	엔드포인트	바이러스, 스파이웨어 등 말웨어 감시/제거	94	7.6% (2011-2016)
	정보/사건관리	보안관련 로깅/사건 정보 및 패치 통합솔루션	17	11.3% (2011-2016)
	ID접속관리	비인가자 침입방지	49	9.4% (2012-2017)
	모바일보안	모바일 말웨어 감지 및 제거	12	22.3% (2012-2017)
	모바일기업관리	원격단말관리, 재고/자산관리, SW배급, 모니터링 등	12	22.4% (2012-2016)
보안 서비스	취약점/위기관리	OS취약점 등 파악을 통한 위기관리 솔루션	48	10.2% (2011-2016)
	클라우드기반서비스	클라우드 기반 보안솔루션, 이메일/웹 필터링 서비스 등	33	14.6% (2011-2016)

[자료원] William Blair (2013.07) / KISIA 글로벌정보보호산업동향조사(2013)

- **[사회비용]** 세계적 보험사 로이드(Lloyd)에 따르면, '15년 사이버범죄로 발생한 경제 손실은 연간 4천억 달러(전세계 GDP의 0.8%)에 육박하고, '19년까지 그 피해 규모는 최대 2조1천억 달러에 달할 것으로 전망함.
 - McAfee는 사이버범죄가 초래하는 경제적 손실은 상상을 초월하여 국제 마약 범죄 피해 또는 미국 내 교통사고 처리비용에 버금간다고 보고
 - * IP도용(사이버공격 외 포함)으로 인한 미국기업들의 손실만도 2,000~2,500억 달러에 육박
 - World Economic Forum은 “쉽게 적발되지 않는 사이버범죄의 특성상 산업 스파이 행위에 의해 유출된 기술·기업 비밀 정보를 포함한 유·무형 피해는 천문학적” 이라고 지적
 - '15년에 전 세계 252개 기관 대상 휴렛패커드의 설문조사⁵⁾에 따르면, 사이버범죄가 유발한 경제 비용은 미국 기업 1개당 평균 1,500만 달러로 세계 평균(7.7백만 달러)의 2배에 달함. (지난 5년 동안 192% 증가)
 - 특히, 금융과 에너지 산업이 피해 빈도가 높아 조사 기업 당 각각 연간 1,350만, 1,280만 달러의 피해가 발생한 것으로 조사됨.
- **[동향]** 사이버보안기업 TrustWave가 17개국의 사이버공격 피해 현황 ('15년)을 분석한 결과(2016 Trustwave Global Security Report)에 따르면,
 - (지역) 북미지역이 사이버공격의 최대 피해지역으로, 전체 사이버공격의 45%가 북미지역(특히 미국에 집중)에서 발생하였고, 다음으로 아시아(27%), 유럽·중동·아프리카(15%), 중남미(13%) 순임.
 - (업종) 소매(Retail)를 대상으로 한 공격이 23%로 가장 높고, 병원(14%), 식음료(10%), 연예·오락(9%), 금융(8%) 등의 공격 노출 빈도가 높음.
 - (대상) E-커머스 대상 범죄가 42%로 가장 높은 비중을 차지하나, 기업 및 인터넷 네트워크 기반 범죄가 '15년 40%로 전년(18%)에 비해 급속하게 증가하고 있는 추세

5) 2015 Cost of Cyber Crime Study: Global (<http://www8.hp.com/us/en/software-solutions/ponemon-cyber-security-report>)

[그림2] 사이버범죄 발생 동향



[자료원] 2016 Trustwave Global Security Report

- **[범죄의 진화]** 기존까지는 자기 과시 또는 금품 갈취 목적의 수동적이고 개별적인 공격이 주를 이뤘다면, 최근에는 중요 기반시설(에너지, 금융, 교통 등)을 타깃으로 하는 지능화·조직화된 범죄 양태로 진화 중
 - (환경) 유·무선 인프라의 고도화, 스마트기기 보급 확대, 모든 사물이 인터넷으로 연결되는 초연결사회가 도래함에 따라 향후 사이버 상의 공격과 범죄는 기하급수적으로 증가할 전망
 - '20년까지 스마트기기 공급은 현재 33억 대에서 59억 대로 늘어나고, 244억 개의 사물(기기)가 인터넷으로 연결됨으로써 월간 데이터 전송량이 현재 8.8 제타바이트*에서 44 제타바이트*로 급증할 전망

[그림3] 사이버공격의 환경변화



[자료원] McAfee, 2016 Threats Predictions / *exabyte : 10^18 bytes, **zettabyte : 10^21 bytes

- (유형) 사이버공격의 양태는 공격 목적, 대상의 단계, 침입 방법 등에 따라 크게 말웨어, DDos, SQL Injection, Skimming, Password Cracking 등으로 구분되는데, 해커들이 나날이 지능화·고도화하면서 그 공격 방법 및 루트가 복잡하고 예측 불가능하게 진화하고 있음.

[표2] 사이버공격의 유형

유형	설명	
Malware	Adware	특정 소프트웨어를 실행(설치) 후 자동적으로 광고가 표시
	Bot	컴퓨터를 좀비처럼 만들어 사용자도 모르는 사이에 스팸이나 바이러스 등을 전파하도록 하는 악성코드
	Dropper	바이러스 스캔을 우회하여 대상 시스템에 악성코드를 설치
	Logic Bomb	특정 조건이 충족되었을 때 악의적인 기능을 유발
	Ransomeware	불법으로 설치되어 해당 컴퓨터를 원격으로 잠그고 해제를 위해 금전을 요구하는 말웨어
	Rootkit	해커들이 컴퓨터나 또는 네트워크에 침입한 사실을 숨긴 채 관리자용 접근권한을 획득하는데 사용하는 도구
	Scareware	악성코드에 감염된 것처럼 위장, 가짜 보안 프로그램을 판매
	Spyware	사용자의 동의 없이 설치되어 컴퓨터의 정보를 수집하고 전송
	Trojan	겉보기에는 정상적인 프로그램으로 보이지만 실행하면 악성코드를 실행하여 범죄에 이용
	Virus	스스로를 복제하여 악의적 목적을 수행하는 악성 소프트웨어
	Wiper	데이터를 지우고, 복구가 불가능하게 만드는 악성코드
Worm	바이러스와 유사하나, 웜은 다른 프로그램에 기생하지 않고 독자적으로 실행이 가능함	
DDos (Distributed Denial-of-Service)	시스템을 악의적으로 공격해 해당 시스템의 자원을 부족하게 하여 원래 의도된 용도로 사용하지 못하게 하는 공격	
SQL Injection	응용 프로그램 보안상의 허점을 의도적으로 이용해, 데이터베이스를 비정상적으로 조작하는 코드 삽입 공격 방법	
Skimming	ATM 등에 장착되어 신용카드 정보를 불법 취득하는 공격방식	
Password Cracking	패스워드로 보안화한 리소스에 접근하기 위해 툴을 사용하여 네트워크, 시스템, 리소스로 침입하는 것	
Zero-Day	운영체제나 네트워크 장비의 보안 패치가 발표되기도 전에 그 취약점을 이용한 악성코드나 해킹공격을 감행하는 수법	
APT (Advanced Persistent Threat)	해커가 다양한 보안 위협들을 생성해 특정 기업이나 조직 네트워크에 지속적으로 가하는 공격 행위	

[자료원] VisionGain 2016

3 | 글로벌시장 현황

1] 글로벌 사이버보안 시장의 기회와 한계요인 (2016년)

기 회	한 계
<ul style="list-style-type: none"> ▶ 사이버 범죄에 대한 취약성 증가 스마트기기, 클라우드컴퓨팅 보급 확대 ▶ 초연결사회로 급속하게 진입 IoT, 인터넷 통신 급증으로 위험확대 ▶ 사이버범죄 유형의 진화 전문가가 아니라도 손쉽게 범죄 참여 가능 ▶ 국가 간 사이버 전쟁의 심화 핵전쟁에 버금가는 군비 경쟁 가속 ▶ 개인정보보호 수요 급증 온라인상에 신상, 금융, 의료 정보범람 ▶ 기간시설에 대한 사이버공격 증가 금융, 전력, 교통 마비에 대한 공포 	<ul style="list-style-type: none"> ▶ 개발도상국의 사이버보안 위축 글로벌 불황에 따른 수요 부진 ▶ 사이버보안 솔루션의 고비용 구조 기기 자체보다 높은 보안비용 ▶ 사이버보안 기술의 복잡성 중소기업/개인의 이용도 저조 ▶ 사이버보안 예산축소 정부/기업의 사이버보안 예산 긴축 ▶ 사이버보안 전문가 수급부족 수요 대비 전문가 양성이 부족한 실정 ▶ 국제 사이버보안 공조 확산 국제협력에 따른 사이버 군비 감축

2] 글로벌시장 전망

- 전 세계 사이버보안 시장 규모는 '15년도 기준, 754억 달러이며, '16년에는 814억 달러로 증가하여 전년 대비 8%의 성장을 구가할 것으로 전망됨. (자료원: ASD Research, Visiongain 2016)
- 또한, 향후 연평균(CAGR) 8.1%의 성장을 지속하여 '21년까지 1,200억 달러 규모 시장으로 성장할 것으로 예상

[표3] 글로벌 사이버보안 시장 전망 (2015-2021)

구 분	2015	2016	2017	2018	2019	2020	2021
규모 (\$백만)	75,429	81,439	88,093	95,283	102,923	111,143	119,986
전년대비성장률		8.0%	8.2%	8.2%	8.0%	8.0%	8.0%
연평균성장률(CAGR)		8.1%					

[자료원] ASD리서치, Visiongain 2016

3 지역별 시장전망

- '16년도 북미지역의 시장 규모는 332억 달러로 전체 글로벌 시장의 최대 비중 (40.8%)를 차지하고 있으며, 다음으로 유럽 24%, 아태지역 20%, 중동·아프리카 9%, 남미 6% 등의 순
- '21년까지 남미, 중동, 아태지역 시장 성장이 전 세계 평균을 상회할 것으로 전망되나, 여전히 전체 시장에서 북미지역이 차지하는 비중은 39%로 최대 시장의 지위를 유지할 것으로 보임.

* 연평균성장률(2015~2021) : 북미(7.1%), 유럽(6.8%), 아태(9.5%), 중동·아프리카(10.1%), 남미(11.4%)

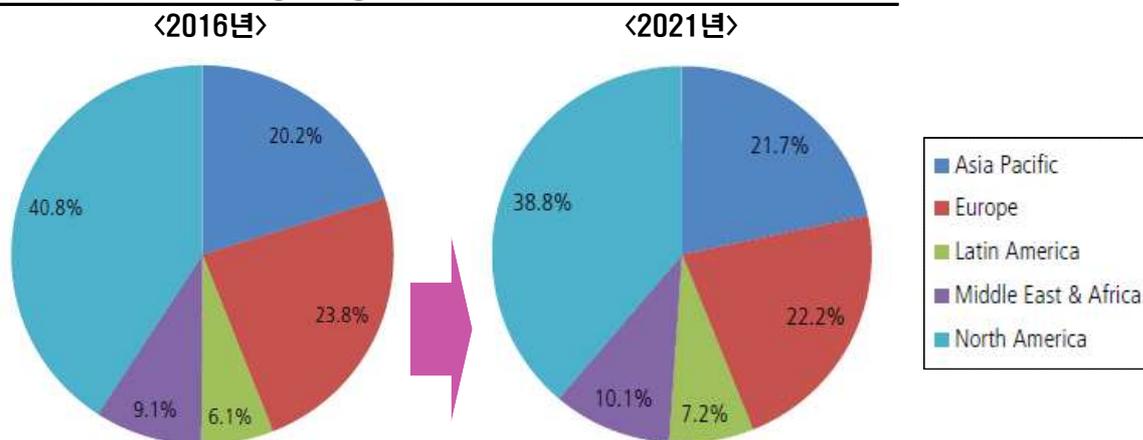
[표4] 지역별 사이버보안 시장 전망 (2015-2021)

단위: \$백만/%

구분	2015	2016	2017	2018	2019	2020	2021	연평균성장률
북미 (전년대비%)	30,926 -	33,227 (7.4)	35,413 (6.6)	37,732 (6.5)	40,346 (6.9)	43,346 (7.4)	46,554 (7.4)	7.1
유럽	18,103 -	19,382 (7.1)	20,702 (6.8)	22,201 (7.2)	23,569 (6.2)	25,007 (6.1)	26,637 (6.5)	6.8
아태지역	15,086 -	16,451 (9.0)	18,059 (9.8)	19,914 (10.3)	21,717 (9.1)	23,785 (9.5)	26,037 (9.5)	9.5
중동· 아프리카	6,788 -	7,411 (9.2)	8,193 (10.6)	8,957 (9.3)	10,086 (12.6)	11,114 (10.2)	12,119 (9.0)	10.1
남미	4,526 -	4,968 (9.8)	5,726 (15.3)	6,479 (13.2)	7,205 (11.2)	7,891 (9.5)	8,639 (9.5)	11.4
전체	75,429 -	81,439 (8.0)	88,093 (8.2)	95,283 (8.2)	102,923 (8.0)	111,143 (8.0)	119,986 (8.0)	8.0

[자료원] ASD리서치, Visiongain 2016

[그림4] 지역별 시장 비중 변화 (2016-2021)



[자료원] ASD리서치, Visiongain 2016

4 분야별 시장전망

- '16년 기준 네트워크보안 시장은 총 128억 달러로 전체의 16.9%의 비중을 차지하고, 다음으로 데이터보안(12.7%), Endpoint보안(12.3%), 어플리케이션 보안(12.2%), 신원 및 접근관리(10.1%), 클라우드보안(6.1%), 기타(29.7%) 순
- 클라우드보안과 어플리케이션보안 부문이 2015~2021년까지 각각 연평균 14.2%, 10.7%의 높은 성장세를 이어갈 것으로 전망됨.

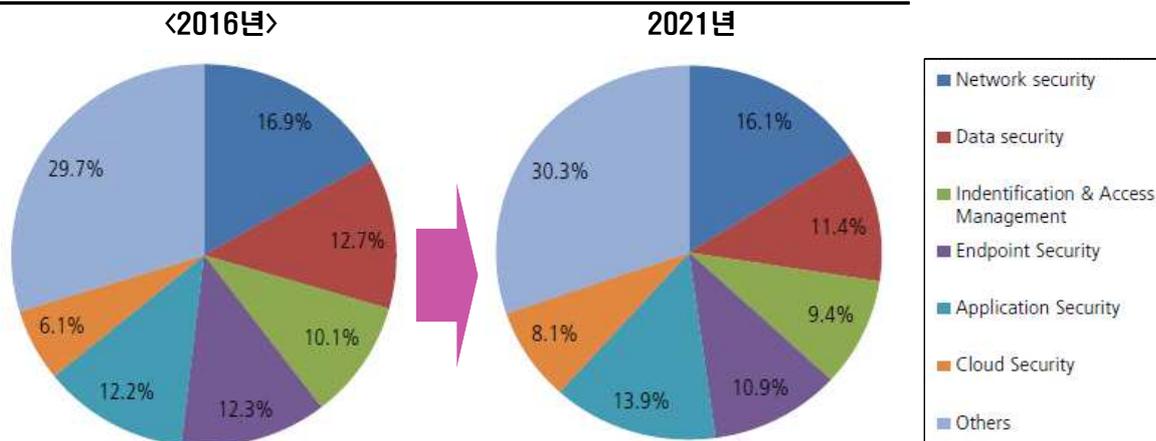
[표5] 분야별 사이버보안 시장 전망 (2015-2021)

단위: \$백만/%

	2015	2016	2017	2018	2019	2020	2021	연평균 성장률
NetSec (전년대비%)	12,819 -	13,729 (7.1)	14,718 (7.2)	15,807 (7.4)	16,929 (7.1)	18,080 (6.8)	19,274 (6.6)	7.0
DataSec	9,803 -	10,313 (5.2)	10,859 (5.3)	11,478 (5.7)	12,167 (6.0)	12,909 (6.1)	13,671 (5.9)	5.7
IAM	7,541 -	8,205 (8.8)	8,935 (8.9)	9,444 (5.7)	10,011 (6.0)	10,621 (6.1)	11,291 (6.3)	7.0
EndSec	9,528 -	10,014 (5.1)	10,555 (5.4)	11,177 (5.9)	11,848 (6.0)	12,476 (5.3)	13,125 (5.2)	5.5
AppSec	9,049 -	9,972 (10.2)	11,009 (10.4)	12,198 (10.8)	13,540 (11.0)	14,989 (10.7)	16,622 (10.9)	10.7
CloudSec	4,368 -	4,988 (14.2)	5,717 (14.6)	6,563 (14.8)	7,494 (14.2)	8,536 (13.9)	9,689 (13.5)	14.2
Other	22,321 -	24,218 (8.5)	26,301 (8.6)	28,616 (8.8)	30,933 (8.1)	33,532 (8.4)	36,315 (8.3)	8.4
전체	75,429 -	81,439 (8.0)	88,093 (8.2)	95,283 (8.2)	102,923 (8.0)	111,143 (8.0)	119,986 (8.0)	8.0%

[자료원] ASD리서치, Visiongain 2016

[그림5] 분야별 시장 비중 변화 (2016-2021)

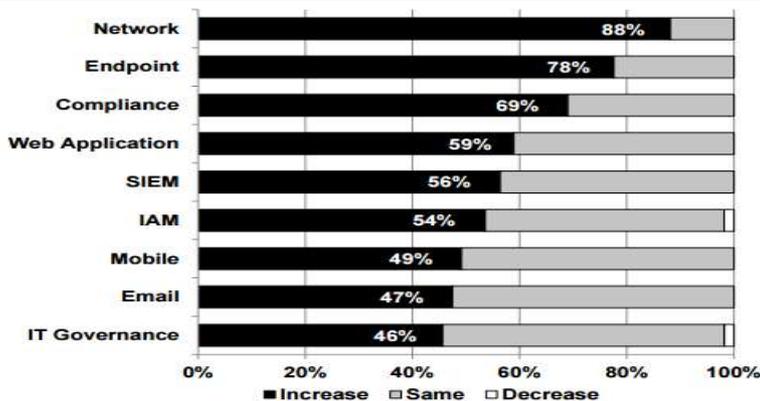


[자료원] ASD리서치, Visiongain 2016

[참고자료2] Piper Jaffray, 2015 CIO Survey

- 글로벌 투자은행 Piper Jaffray는 8개 산업분야, 112개 기업의 최고정보책임자들을 대상으로 한 기업의 IT 투자계획에 대한 설문조사를 실시함 ('15.1월)
 - 사이버보안 부문이 기업의 IT투자의 최우선 과제라고 한 응답자가 전년도(59%) 보다 월등히 증가한 75%로 조사됨.
 - * 사이버보안(75%), 모바일(62%), 클라우드(59%), 데이터저장(51%) 등
- 사이버보안 분야에서 네트워크 보안에 가장 많이 투자할 예정이라는 응답이 88%, 다음으로 Endpoint보안(78%), 컴플라이언스(69%) 등 순

[그림6] 분야별 시장 비중 변화 (2016-2021)



[자료원] Piper Jaffray 2015 CIO Survey

- 사이버보안 벤더 선호 조사에서 전체 응답자의 21%가 Symantec을 가장 선호한다고 응답했으며, 응답자의 25%가 향후('15년)에 거래할 계획이 있는 벤더로 FireEye를 꼽음.

[표6] 사이버보안 벤더 선호도 조사

선호 벤더		거래계획('15년)이 있는 벤더	
Symantec	21%	FireEye	25%
Cisco	10%	Palo Alto Networks	17%
Palo Alto Networks	10%	Cisco	8%
Intel/McAfee	10%	Barracuda	8%
Trend Micro	9%	Proofpoint	8%
FireEye	6%	EMC	8%

[자료원] Piper Jaffray 2015 CIO Survey

5 주요 국가별 시장전망

- 미국 시장은 '16년 238억 달러(전년 대비 7.6% 증가)에 달하여, 전체 글로벌 시장의 29%를 차지하는 최대 시장을 형성하고 있음.
- '21년까지 중국시장은 연평균 14.1%의 고속 성장을 통해 163억 달러 규모가 될 것으로 전망되나, 미국은 346억 달러 시장으로 성장(연평균 7.7%)하여 여전히 최대 시장의 지위를 유지할 것으로 보임.
- 한국의 사이버보안 시장은 '16년 기준 전 세계 시장의 8.5%를 차지하나, 점차 그 비중이 줄어 '21년에는 전체의 6.8%로 축소될 전망
- 상위 9개 국가가 전체시장의 85% 이상을 차지하고 있어, 소수국가가 전체시장을 주도하는 고기술 고부가가치 산업의 특징을 그대로 반영

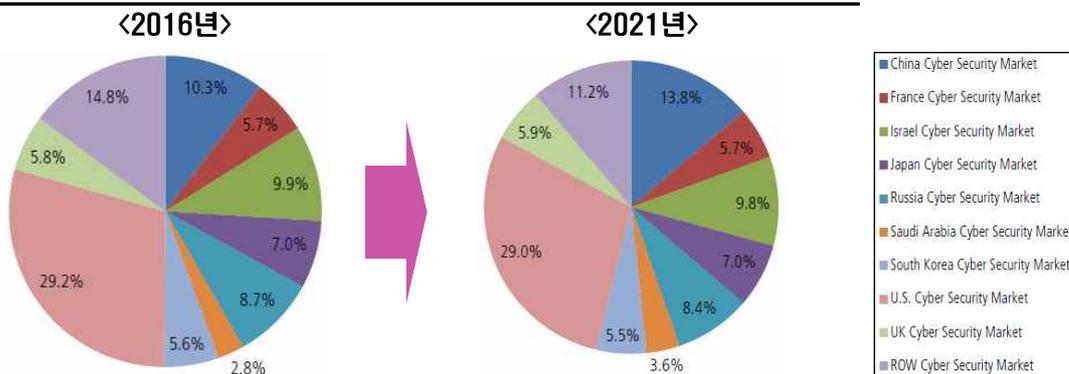
[표기] 분야별 사이버보안 시장 전망 (2015-2021)

단위: \$백만/%

	2015	2016	2017	2018	2019	2020	2021	연평균 성장률
미국 (전년대비%)	22,100 -	23,780 (7.6)	25,706 (8.1)	27,891 (8.5)	30,094 (7.9)	32,291 (7.3)	34,584 (7.1)	7.7
이스라엘	7,543 -	8,079 (7.1)	8,668 (7.3)	9,310 (7.4)	10,045 (7.9)	10,859 (8.1)	11,706 (7.8)	7.6
중국	7,430 -	8,403 (13.1)	9,546 (13.6)	10,873 (13.9)	12,428 (14.3)	14,255 (14.7)	16,393 (15.0)	14.1
러시아	6,600 -	7,082 (7.3)	7,606 (7.4)	8,169 (7.4)	8,781 (7.5)	9,405 (7.1)	10,035 (6.7)	7.2
일본	5,345 -	5,724 (7.1)	6,148 (7.4)	6,634 (7.9)	7,171 (8.1)	7,788 (8.6)	8,380 (7.6)	7.8
영국	4,409 -	4,731 (7.3)	5,100 (7.8)	5,503 (7.9)	5,959 (8.3)	6,466 (8.5)	7,022 (8.6)	8.1
프랑스	4,330 -	4,655 (7.5)	5,018 (7.8)	5,419 (8.0)	5,858 (8.1)	6,309 (7.7)	6,770 (7.3)	7.7
한국	4,220 -	4,578 (8.5)	4,977 (8.7)	5,370 (7.9)	5,773 (7.5)	6,183 (7.1)	6,603 (6.8)	7.7
사우디	1,976 -	2,243 (13.5)	2,550 (13.7)	2,912 (14.2)	3,334 (14.5)	3,805 (14.1)	4,333 (13.9)	14.0
기타	11,476 -	12,164 (4.9)	12,774 (4.0)	13,203 (2.3)	13,478 (1.0)	13,784 (1.2)	14,160 (1.9)	3.6
전체	75,429 -	81,439 (8.0)	88,093 (8.2)	95,283 (8.2)	102,923 (8.0)	111,143 (8.0)	119,986 (8.0)	8.0

[자료원] ASD리서치, Visiongain 2016

[그림기] 국가별 시장 비중 변화 (2016-2021)

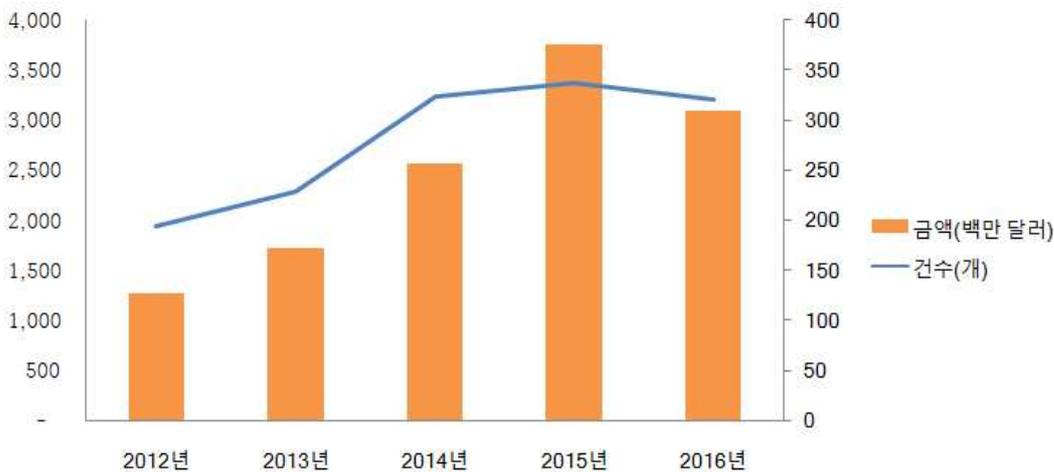


[자료원] ASD리서치, Visiongain 2016

4 | 글로벌 투자동향

- [벤처투자] '15년도 전 세계 사이버보안 관련 벤처투자는 총 360건, 37억 달러로 전년 대비(금액) 31.8% 증가 (자료원: CBInsights)
 - '16년에는 총 320건, 30억 달러로 전년대비(금액) 17.7% 감소할 전망
 - 기술과 시장이 급속히 통합되는 과정 속에 중소벤처기업들이 생존하기 어려운 환경으로 변화하고 있는 점이 벤처투자 감소의 원인으로 분석됨.

[그림8] 글로벌 사이버보안 관련 벤처투자 추이 (2012~2016)



[자료원] CBInsight / 워싱턴무역관 가공

- (사례) 최근 ('15~'16년 현재까지) 사이버보안 분야에서 1억 달러 이상의 대형 벤처투자 유치에 성공한 기업은 총 8개로, Tenable Network Security ('15년, 2.5억 달러), LogicMonitor ('16년, 1.3억 달러), Tanium ('15년, 1.17억 달러) 등이 대표적 사례로 꼽힘.

[표8] 최근 주요 사이버보안 관련 벤처투자 사례

(단위 : 백만 달러)

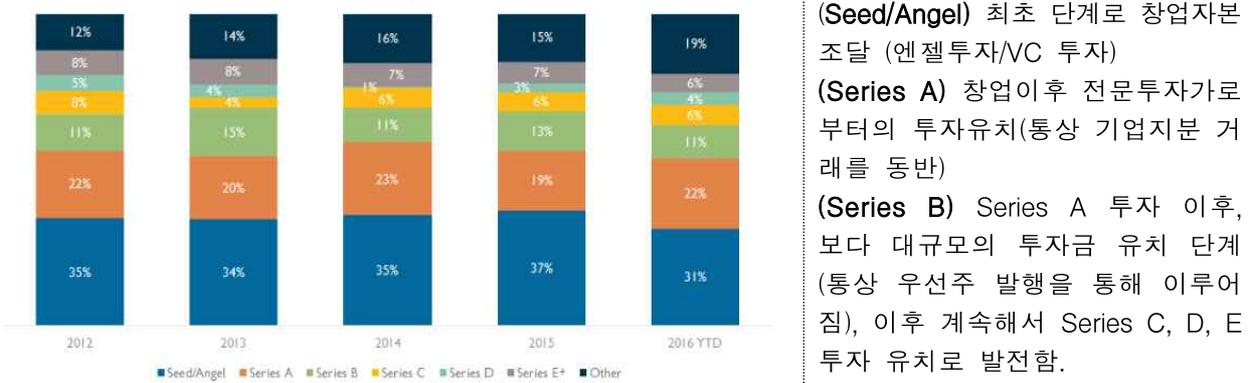
연도	유치 기업	유치금액	비고
2016	Cylance	100	인공지능을 통한 사이버범죄 감시
	Mobi Magic	100	안드로이드 앱 전문 보안솔루션
	LogicMonitor	130	기업용(인프라, IT서비스) 보안솔루션
2015	CrowdStrike	100	Software-as-a-Service (SaaS)기반 Endpoint 전문 보안솔루션
	Illumio	100	데이터센터, 클라우드서비스 보안
	CloudFlare	110	클라우드 기반 방화벽 기술
	Tanium	117.5	기업용 네트워크 복구 솔루션
	Tenable Network Security	250	네트워크 모니터링, 복구 솔루션

[자료원] 워싱턴무역관 언론보도 취합

○ (투자단계별) 투자 유형(단계별)으로는 '16년 기준, 초기 창업 투자 (Seed/Angel)가 여전히 전체의 31%로 가장 높은 비중을 차지하나, 예년에 비해 초기 창업 투자 비중은 감소하는 것으로 조사됨.

* 초기창업 투자 비중 감소 (37%('15년) → 31%('16년)) 원인은 벤처투자자들이 근래 보수적 투자로 전환한 이유뿐만 아니라, 대기업들의 직접 초기 개발단계 기술 사냥 경쟁에 뛰어들어 준 것도 중요 원인으로 꼽힘.

[그림9] 사이버보안 관련 스테이지별 글로벌 투자 (2012~2016)



[자료원] CBInsight

“급성장하는 사물인터넷 기술투자... 미국, 이스라엘이 최대 수혜”

IT전문 컨설팅사인 룩스리서치 (Lux Research)에 따르면, 사물인터넷 관련 보안 (S/W, H/W 포함) 투자가 '15년도 2.3억 달러(전년 대비 78% 증가)에서 '16년에는 4억 달러로 급성장할 것으로 전망함. 조사된 사물인터넷 보안 스타트업 중 절반 이상(77개 기업)이 미국을 기반 (이중 1/3은 이스라엘에 본사소재)으로 하고 있으며, 2000년 이래 총 8억 달러 이상의 투자를 유치함.

○ (투자가) 사이버보안 관련 주요 벤처투자가로는 New Enterprise Associates, Accel Partners, Intel Capital 등이 있으며, 특히 Andreessen Horowitz는 주로 초기 창업기업 투자에 주력하고 있는 것이 특징

[표9] 주요 벤처투자자

순 위	벤처투자자명	투자대상기업
1	New Enterprise Associates	CloudFlare 등
2	Accel Partners	Crowd Strike, AirWatch, Lookout 등
3	Intel Capital	Fortscale Security, Bromuim 등
4	Andreessen Horowitz	Tanium, Lookout, Illumio 등
5	Norwest Venture Partners	FireEye, Agari 등
6	Sequoia Capital	Palo Alto Networks, MobileIron 등
7	Kleiner Perkins Caufield & Byers	Good Technology, Synack 등

[자료원] 워싱턴무역관 언론보도 취합

- **[M&A]** '15년, 사이버보안 관련 M&A 거래는 전년 105건에서 133건으로 크게 증가하였고, 지난 5년 동안 무려 235%가 증가하여 전체 거래 금액은 38억 달러로 조사됨. (자료원: 451 Research, Tech M&A Outlook 2016)
- '14~15년도 글로벌 M&A 거래 현황을 분석했을 때, 전체 거래의 72%가 전략 목적의 인수(Strategic)이고 28%가 금융투자(Financial) 목적의 거래로 분류됨. (출처 : Willam Blair and Pitchbook, 2015)
- 대기업들은 In-house 기술개발 보다 우수한 기술을 보유한 스타트업을 인수하는 방식을 선호하고, 스타트업들도 수익 출구방식(Exit Plan)으로 자체 IPO 보다는 전략적 흡수합병 방식을 선호하는 추세

[표10] 최근 주요 사이버보안 관련 M&A 사례

(단위 : 백만 달러)

날 짜	피인수기업	인수기업	인수금액	비 고
'16.6월	Blue Coat	Symantec	4,650	기업용 통합 사이버 솔루션
'16.7월	AVG	Avast Software	1,300	모바일, PC 보안 어플리케이션
'16.6월	CloudLock	Cisco	300	클라우드 보안어플리케이션
'16.2월	Resilient	IBM Security	100+	사이버공격 사후관리 솔루션
'16.7월	Confer	Carbon Black	비공개	행동분석을 통한 사이버보안
'15.6월	OPenDNS	Cisco	635	클라우드기반 보안솔루션
'15.6월	Virtustream	EMC	1,200	기업용 클라우드 보안
'15.6월	Knowledge Consulting	ManTech International	비공개	사이버 리스크 관리, 운영
'15.5월	Resolution1 Security	General Dynamics	비공개	사이버 범죄 감지/해결
'15.5월	Creative Computing	Information innovators	비공개	사이버 의료정보 관련 솔루션
'15.4월	WatchBox	BlackBerry	비공개	기업용 데이터보안
'15.4월	Websense	Raytheon	2,300	말웨어, 데이터도난 방지
'15.4월	Trustwave	SingTel	827	데이터보안 방지 솔루션
'15.3월	Blue Coat	Bain Capital	2,400	웹보안 솔루션

[자료원] 워싱턴무역관 언론보도 취합

III 미국 사이버보안 시장 개요

1 시장 현황 및 전망

1 미국 사이버보안 시장의 기회와 한계요인 (2016년)

기 회	한 계
<ul style="list-style-type: none"> ▶ 미국 경제 호조세 지속 ▶ 인터넷 브로드밴드, 스마트폰 사용자의 광범위한 저변 확대 ▶ 연방정부의 사이버보안 적극적 투자 ▶ 국방부의 신규 사이버보안 전략 (18년까지 6,200명 증원 19억 달러 추가 예산) ▶ 사이버범죄 발생빈도 증가 ▶ 중국, 러시아 등과의 사이버공격 대응 ▶ 미국이 선도하는 IoT기술 및 시장 	<ul style="list-style-type: none"> ▶ 국내 사이버보안 시장 포화 ▶ 정부가 주도하는 적극적 사이버보안 정책에도 불구하고, 일부 업계의 무관심

2 시장전망

- 미국의 사이버보안시장 규모는 '15년 말 기준 220억 달러로 집계되며, '16년에는 7.6% 상승한 238억 달러에 달할 것으로 예상됨.
- 미국 사이버보안 시장은 '18년도를 정점으로 성장세가 다소 둔화될 것으로 보이나 '21년까지 연평균 7.8% 성장세를 유지하여 346억 달러 규모의 시장으로 성장할 것으로 전망되며,
 - 세계시장에서 미국시장이 차지하는 비중도 '21년까지 현재 수준인 29%를 유지함으로써 사이버보안의 최대 강국의 지위를 유지

[표11] 미국 사이버보안 시장 전망 (2015-2021)

단위: \$백만/%

	2015	2016	2017	2018	2019	2020	2021	누적 2016-2021
시장규모	22,100	23,780	25,706	27,891	30,094	32,291	34,584	174,345
전년대비 성장률(%)	-	7.6	8.1	8.5	7.9	7.3	7.1	-
세계시장 비중(%)	29.3	29.2	29.2	29.3	29.2	29.1	28.8	29.1

[자료원] ASD리서치, Visiongain 2016

[그림10] 미국 사이버보안 시장 전망 (2015-2021)



[자료원] ASD리서치, Visiongain 2016

③ 연방정부 시장

- **[현황]** 연방정부는 미국의 사이버보안시장의 최대 투자가이자 소비자로서 미국 전체시장의 58.8%에 해당하는 연간 140억 달러의 예산을 집행하여 관련 산업과 기술을 선도하는 역할을 담당함.
 - 미국 대통령예산(안)에 따르면, 행정부가 의회에 요청한 사이버보안 관련 예산('17년도)은 총 190억 달러로 전년 대비 무려 35.7% 증가

[표12] 사이버보안 관련 미국 연방정부 예산 추이

	2013	2014	2015	2016	2017*
금액(\$억)	103	130	130	140	190
전년대비 성장률(%)	-	26.2	0.0	7.7	35.7%

[자료원] ASD리서치, Visiongain 2016 / * 2017 대통령(행정부) 예산신청 기준

- **[전망]** 글로벌 마켓리서치 전문기관 Market Research Media에 따르면, 미국 연방정부의 사이버보안 예산은 연평균 4.4% 성장하여 '22년까지 220억 달러에 달할 것으로 전망함.
 - 미국 연방정부 부처가 구매하는 사이버보안 제품/서비스 수요는 '15년 86억 달러에서 '20년까지 110억 달러로 성장(연평균 5.2%)할 것으로 예상 (미국 정부조달시장 조사기관 Deltek 보고서 인용)
 - 분야별로는 네트워크보안 수요 비중이 40% 수준으로 가장 높고, 다음으로 데이터보안(25%), IAM(19%), 클라우드보안(15%) 등 순

- **[부처별]** '16년 전체 연방정부 사이버보안 관련 예산의 68%에 해당하는 95억 달러가 국방부에 배정되고 그 다음으로 국토안보부(10.1%), 법무부(4.6%), 에너지부(2.2%), 보건부(1.9%) 등 순
 - 국방부의 사이버보안 예산은 '16년에만 전년대비 12.3%가 증가하여 10억 달러 이상이 증액 편성됨
 - 조달청(GSA)와 국세청(IRS)의 관련예산이 전년대비 각각 549%, 256% 증가를 기록하여 연방부처 중 가장 높은 증가율을 보임.

[표13] 미국 연방부처별 사이버보안 예산 집행 (2015 / 2016)

단위 : \$백만%

부 처	2015	2016 (전체대비 비중%)	증가율(%)
국방부	8,460	9,500 (68.4)	12.3
국토안보부	1,300	1,400 (10.1)	7.7
법무부	547	636 (4.6)	16.3
에너지부	300	306 (2.2)	2.0
국무부	208	226 (1.6)	8.7
보건부	202	262 (1.9)	29.7
내무부	198	198 (1.4)	0.0
상무부	187	187 (1.3)	0.0
보훈부	152	180 (1.3)	18.4
항공우주청	108	117 (0.8)	8.3
국립 기술표준원(NIST)	102	109 (0.8)	6.9
국립 과학재단(NSF)	100	125 (0.9)	25.0
국세청(IRA)	68	242 (1.7)	255.9
조달청(GSA)	35	227 (1.6)	548.6
농무부	26	28 (0.2)	7.7
사회보장국	16	17 (0.1)	6.3
재무부	14	16 (0.1)	14.3
노동부	12	13 (0.1)	8.3
환경보호청	11	11 (0.1)	0.0
교통부	5	8 (0.1)	60.0
기타	45	73 (0.5)	62.2
합 계	12,096	13,881 (100.0)	14.8

[자료원] ASD리서치, Visiongain 2016

[표14] 미국 사이버보안 관련 주요 정부 계약 현황 (2015)

단위: \$백만

계약기간	발주처	수주기업	계약금액	내 용
'15.12월-'16.11월	공군	TASC,Inc	9.9	사이버보안 운영관리
'15.10월-'20.11월	공군	Alion 등	5	사이버공격 분석 처리
'15.9월-'18.9월	공군	Booze Allen Hamilton	17.6	사이버보안 통합 소프트웨어
'15.9월-'18.9월	Washington HQ Services	Booze Allen Hamilton	6.9	사이버보안 시스템 운영
'15.9월-'17.9월	공군	Sierra Nevada	9.5	사이버보안 소프트웨어
'15.9월-'18.12월	해군	ITGS,LLC	133.3	신분도용 방지 시스템 운영
'15.8월-'16.7월	육군	Notrhrop Grumman	13.6	사이버보안 통신시스템 관리
'15.7월-'16.8월	해군	Booze Allen Hamilton	13.2	해군 IT시스템 현대화
'15.7월-'16.7월	공군	Cyber Defense Information Assurance	7.9	사이버보안 네트워크 관리
'15.7월-'20.5월	공군	X-Technologies	7.6	사이버공격 대응시스템
'15.6월-'19.8월	공군	Kudu Dynamics	7.2	사이버공격 분석 대응
'15.6월	Defense Advanced Research Projects Agency	Vencore Lab	11.2	사이버보안 관련 연구개발
'15.5월-'18.6월	Defense Advanced Research Projects Agency	Raytheon	12.2	사이버보안 관련 연구개발
'15.6월	공군	TASC, Inc	6.9	사이버보안 관리 운영
'15.3월-'16.3월	Defense Logistics Agency	Isis Defense	7	데이터저장 보안 연구개발
'15.1월-'15.7월	해병대	Notrhrop Grumman	7.1	사이버네트워크 보안

[자료원] www.fedbizopps.gov

[참고자료3] 미국 국방부의 사이버보안 전략⁶⁾

- (배경) '12년도에 오바마대통령은 진화하는 사이버공격에 대응하기 위한 국방부의 사이버 대응 체계 구축을 명령함에 따라 국방부는 Cyber Mission Force(CMF)라는 조직을 출범시킴.
- (新전략) 미국 국방부는 '15.4월 新사이버전략(New Cyber Strategy)을 발표하여 5대 핵심 전략과제와 구체적 실행계획을 제시함.
 - 1) 사이버보안 상시 대응체계 구축
 - 2) 국방부의 데이터와 정보네트워크 보호를 통한 리스크 관리
 - 3) 미국 국토 내 위협적인 사이버 공격에 대한 차단
 - 4) 모든 단계에서의 사이버 공격에 대한 사전 대응 마련
 - 5) 국제 사이버범죄(테러) 방지를 위한 국제적 공조 체계 구축
- (대상) 중국과 러시아를 잠재적 사이버위협 대상국으로 지정하고 이들 국가로부터의 산업 스파이 및 사이버테러 행위 등에 대한 대응방안 천명
 - 이란, 북한 역시 잠재적 위협국으로 지정하고, IS와 같은 비국가 테러 단체에 대한 대응 조치도 포함함.
- (방안) '15년까지 예산 19억 달러를 배정하여 군인, 민간인 전문가 6,200명(133개 팀)으로 구성된 CMF을 출범시켜 일선에 배치 예정
 - 또한 국방부장관 산하에 사이버사령부를 운영하여 이를 통해 국방부 사이버 전략 극대화 추진
- (예산) 국방부의 사이버보안 관련 예산은 '16년 95억 달러로 전년 대비 12%이상 증액 배정
 - 악성 사이버코드 대응(30억 달러), 사이버보안 환경인프라 구축(50억 달러), CMF 활동(5억 달러), 연구개발 지원(10억 달러) 배정

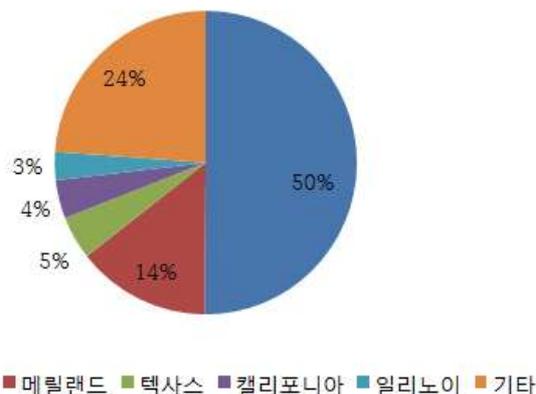
- **[지역별]** 미국 연방정부의 사이버보안 관련 지출 대부분을 워싱턴 광역지역이 흡수하고 있는 것으로 조사됨.
 - 연방정부 사이버보안 관련 지출의 64.4%인 총 6.9억 달러가 워싱턴 광역지역(버지니아, 메릴랜드州)에서 집행됨으로써 이 지역이 사이버보안 분야 정부 지출의 특수성을 누리고 있는 것으로 파악됨.
 - 사이버보안 관련 벤처 투자가 캘리포니아 또는 보스턴 지역에 집중되고 있는 반면, 연방정부 기관을 배후에 두고 있는 워싱턴 광역지역이 공공 수요가 높은 사이버산업의 새로운 메카로 각광받고 있음.
 - * '10년에서 '15년 상반기까지 글로벌 사이버보안 관련 벤처투자의 82%(금액기준)가 미국 내에서 발생, 미국 내 투자의 45%(건수기준)가 캘리포니아에서 이루어짐.
 - 지난 3년 간 연방정부 사이버보안 지출의 연평균 성장률도 버지니아(35.8%), 메릴랜드(67.9%)로 타 지역에 비해 빠르게 증가하고 있음.

[표15] 미국 연방정부 사이버보안 5대 집행 지역(주) 단위: \$백만/%

	2012	2013	2014	2015	연평균성장률(%)
버지니아	214.6	234.7	428.9	537.5	35.8
메릴랜드	32.5	47.2	128.0	153.8	67.9
텍사스	27.7	33.1	29.9	49.4	21.2
캘리포니아	72.4	36.5	46.6	43.5	-15.6
일리노이	3.2	16.0	7.6	32.1	115.6
전체	463.3	519.9	805.7	1,072.2	32.3

[자료원] ASD리서치, Visiongain 2016

[그림11] 5대 연방정부 사이버보안 지출 지역 (2015)



[자료원] ASD리서치, Visiongain 2016

6) http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

2 정부정책 동향

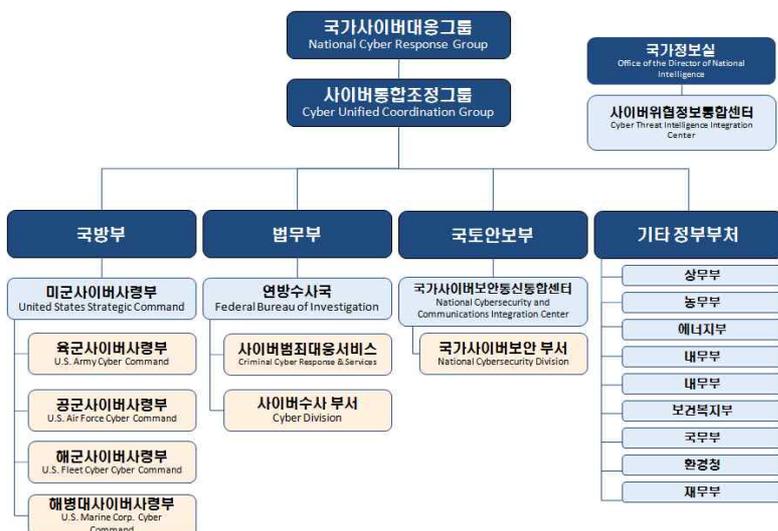
- **[정책]** 오바마 행정부는 사이버공격(테러)을 안보와 경제에 심각한 위협요인으로 인식하고 연방정부 차원의 대책마련에 주력함.
 - 정권출범과 동시에 미국의 사이버보안 정책에 대한 포괄적 검토를 지시하였고 그 결과물로 『Cyberspace Policy Review('09.5월)』를 발표함
 - 정부뿐만 아니라 중요 기간시설 및 민간부문의 사이버보안 시급성 공표
 - '13년 오바마대통령의 첫 사이버보안 관련 행정명령인 『중요 기간 시설에 대한 사이버보안 개선』을 발표
 - 국립기술표준원(NIST)로 하여금 국가적 사이버보안 표준 제정과 운영 체제를 구축하도록 지시함. (NIST framework 발표, '14.2월)
 - '15년 사이버위협정보통합센터(CTIIC : Cyber Threat Intelligence Integration Center)를 설립하여 해외로 부터 잠재적 사이버 위협에 대해 범부처간 공조 시스템을 갖추도록 함.
 - '16년 백악관은 『사이버보안관련 국가 행동계획(CNAP : Cybersecurity National Action Plan)』을 발표
 - 오바마 행정부의 지난 7년 동안의 사이버보안 관련 정책을 집대성하고 국가적 사이버보안 강화를 위한 실천적 행동계획 발표

Cybersecurity National Action Plan (CNAP) 주요내용

- ① 국가 사이버보안 증진위원회(Commission on Enhancing National Cybersecurity) 설립
 - 민·관·학계 전문가가 참여하는 국가 차원의 사이버보안 증진 대책 마련
- ② IT 현대화 기금으로 32억 달러 조성하고 연방최고정보보안관(Federal Chief Information Security Officer) 제도 신설 및 임명
- ③ 국가사이버보안협의체(National Cyber Security Alliance)를 구성하여 일반 시민의 온라인 사이버보안 강화
 - 구글, 페이스북, Visa 및 여타 금융기관과의 공동대응 체제 구축
- ④ '17년도 대통령예산안에 관련 예산을 전년대비 35% 증가한 190억 달러 신청

- [조직] 연방정부는 사이버위협에 대응한 범 정부부처 간 공동대처 능력 증진을 위해 다층적이며 통합적인 대응시스템 구축에 노력
 - 국가사이버대응그룹 (National Cyber Response Group)
 - 대통령 직속 국가안보위원회(NSC)와 국가안보테러보좌관이 주재하는 범정부 기관으로 사이버보안 정책과 전략을 수립하는 컨트롤타워 역할
 - 사이버통합조정그룹 (Cyber Unified Coordination Group)
 - 중대한 사이버위협에 대응하여 정부 부처 간, 민간부문과의 협력을 증진하고 업무와 역할을 조정 중재하는 역할
 - 미군사이버사령부 (United States Strategic Command)
 - 미군전략사령부 산하에 설치되어 미군 전체의 사이버보안 전략, 대응, 기관별 협력 계획을 수립하고 집행
 - 연방수사국 (FBI : Federal Bureau of Investigation)
 - '16.6월 대통령 지시명령에 따라, 기존까지 국토안보부가 주무부서로 담당해 오던 연방정부 사이버위협 대응 업무를 법무부 산하 FBI로 이관
 - 국가정보실 (Office of the Director of National Intelligence)
 - 사이버위협정보통합센터를 통해 국가차원의 사이버 위협 정보 수집
 - 국토안보부 (Department of Homeland Security)
 - 국가 기간 시설(자산)에 대한 사이버보안 감시 관리

[그림12] 미국 연방 사이버보안 관련 조직도



[자료원] 백악관 보도자료, Presidential Policy Directive, United States Cyber Incident Coordination

3 주목해야할 트렌드

① 지정학적 요구와 국가 안보전략으로서 사이버戰 억제력 개념 태동

- 국가 간 사이버전쟁이 현실화되면서 지정학적 요구에 따른 사이버 보안이 21세기 외교정책의 중요한 축으로 자리매김하기 시작함.
 - 20세기에는 핵 억제력 보유가 중요한 안보 현안이었으나, 현재는 사이버戰 억제력이 중요한 국가안보의 전략적 자산으로 인식되는 추세
- 기존의 산업스파이 행위에 그치지 않고, 사이버테러를 통한 국가 기간시설 무력화 시도, 최근 미국 대선국면에서 클린턴 캠프 및 민주당의 정보가 해킹되는 등 심각한 정치·사회적 리스크 상존
 - 미국, 중국, 러시아 등은 이미 사이버기술의 전략적 가치를 인정하고 자국의 인터넷 네트워크, 기간시설, 기업정보 등의 보호뿐만 아니라 유사시 보복용 사이버 기술 보유에도 노력 중

② 미래 사이버산업의 중추 기술 : 블록체인

- 블록체인은 디지털 가상화폐 ‘비트코인’에 사용됐던 핵심 기술로서 개인 간의 거래 정보를 여러 컴퓨터에 분산 저장해, 해킹이나 위변조를 방지할 수 있는 기술로 금융권과 IoT, 의료, 교통 등 광범위한 적용 가능
 - '15년 9월 세계경제포럼(다보스포럼)은 보고서를 통해 블록체인을 향후 사회를 뒤바꿀 기술로 보고 '27년이면 글로벌 GDP의 10%가 블록체인 기술로 저장될 것으로 전망함.
- Greenwich Associates의 조사에 따르면 '16년도에 블록체인 기술 관련 벤처투자는 10억 달러를 넘어설 것으로 예상
 - 40여 개의 금융기관의 컨소시엄은 R3CEV LLC라는 벤처기업을 설립하여 블록체인 기술을 실험 중에 있으며, 삼성전자도 최근 국내 블록체인 전문 업체에 투자결정 (조선 Biz, '16.7.14 기사 인용)

③ 클라우드 보안, 사이버 생태계의 대세로...

- 사이버 공격에 취약한 자체 구축형(on-premise) 솔루션을 지양하고, 클라우드 기반 통합 보안 방식으로 급속한 전환이 진행 중
 - '16.4월, 워싱턴 DC 인근 최대 병원 체인인 MedStar의 최소 14개 병원의 자체 보안 시스템이 사이버공격에 의해 무력화됨. 온사이트 보안담당자가 빠른 해킹기술의 진화를 따라잡기에 역부족인 상황
- 클라우드 보안기술의 신뢰성이 제고되고 서비스 비용이 인하됨에 따라 회사내부 데이터를 클라우드 기반(오프사이트)으로 이전하는 것에 대한 기업들의 거부감이 점차 완화되고 있는 것으로 조사됨.
 - 글로벌 컨설팅사 PwC에서 전세계 1만명의 IT전문가들을 대상으로 수행한 설문조사⁷⁾에 따르면, 응답자의 69% 이상이 클라우드 기반 보안 서비스를 이용하고 있다고 답변함.
- 이런 추세 속에, 사이버보안 업계는 인수합병을 통해 몸집을 불리고, 솔루션 포트폴리오를 다각화하는 전략을 추진 중에 있음.
 - '16년도 Symantec은 Blue Coat를 인수하여 사이버보안 사업부문을 보강한 바 있으며, 시스코도 기업용 클라우드 보안 솔루션의 강자 CloudLock 인수를 공식 발표함(8월1일).

④ 멀티팩터 인증, 정부수요를 기반으로 급성장 중

- 연방정부는 정부기관 내 정보 시스템의 보안 강화를 위해 다층적(Multi-layer) 보안솔루션을 적극 도입 확산하고 있는 추세
 - 연방사회보장청(U.S. Social Security Administration)은 '16.7월, 사회보장 연금 시스템 접속을 위해서는 기존의 아이디, 비밀번호 외에 휴대 전화를 통한 멀티 인증을 의무화할 것이라고 발표함.
- 바이오메트릭 기술(지문, 안구인식, 보이스인식)이 기존의 멀티팩터 인증과 결합하여 빠르게 진화하여 새로운 시장을 형성 중
 - NICE Actimize社는 바이오메트릭을 이용한 멀티팩터 인증 프로그램을 개발하여 금융기관 등에 공급 중에 있음.

7) The Global State of Information Security® Survey 2016 (<http://www.pwc.com/gsis>)

5] 프라이버시 VS 시큐리티 : 암호화/복호화 기술

- '16년, 범죄자의 스마트폰을 Unlock하고자 하는 FBI와 이를 거부한 애플의 대결로 『사생활보호냐, 안보우선이나』 의 토론이 촉발됨.
 - FBI는 애플의 도움 없이 암호화된 스마트폰을 Unlock 하기 위해서 이스라엘 기업인 Cellebrite 복호화 기술을 이용한 것으로 알려짐.
- 전세계 십억 명 이상을 가입자로 보유하고 있는 온라인 메시지 서비스 기업인 WhatsApp은 자사의 앱을 통해 송수신된 모든 메시지, 사진, 전화통화 목록 등에 자동 암호화 서비스를 개시함.
- 시장조사기관 Markets and Markets은 전 세계의 암호화 소프트웨어 시장은 연평균 21% 이상 고성장을 구가하여 '19년까지 48억 달러 규모로 성장할 것이라고 전망함.
 - Credence Research('16.8월 조사)은 이메일 암호화 시장이 연평균 23% 이상 성장하여 '23년까지 27억 달러에 달할 것으로 전망

6] 머신러닝과 인공지능, 사이버범죄의 “마이너리티 리포트”

- 사이버범죄의 빈도가 증가하고 변종 공격이 일상화되면서 사이버 보안 전문가는 부족하고, 시스템 관리비용은 증가하는 이중고 발생
 - '19년까지 전 세계적으로 6백만 명의 사이버보안 전문가 수요가 예상되나, 150만 명의 공급이 부족한 인력 수급의 불균형이 발생할 전망
- 빅데이터를 기반으로 하는 머신러닝과 인공지능 기술을 활용하여 사이버공격의 유발환경, 유형, 빈도 등을 분석함으로써 실시간으로 범죄 발생을 예측, 예방하는 솔루션으로 진화
 - PwC 설문조사에서 59%의 IT전문가가 빅데이터 분석을 업무에 적용하고 있다고 답변하는 등 이미 기술의 상용화는 가시권에 접근함.
- 다크트레이스는 영국의 사이버보안 벤처기업으로 머신러닝을 보안에 접목, IT인프라 시스템의 정상적인 상태를 스스로 학습하고 자동으로 비정상적인 행위나 위협을 탐지해내는 차세대 기술을 보유. 최근 삼성SDS는 동사에 투자 결정을 발표함.

IV

미국의 주요 사이버보안 기업 현황

- [전체현황] 사이버보안 분야 상위 15개(매출기준) 기업들의 전체 매출은 전 세계 시장의 27.1%의 비중을 차지하고 있으며, 특정기업이 시장에서 아직 뚜렷한 우위를 점유하지 못하고 있는 비교적 완전경쟁 시장구조가 형성되어 있다고 평가됨.
- Symantec이 사이버보안 관련 연매출이 39억 달러로(전체대비 5.0%) 가장 높은 시장점유율을 보이고 있으며, Intel(2.9%), IBM(2.7%), Cisco(2.3%), Optiv(2.0%), Check Point(2.0%) 등이 다음을 차지
- 하지만, 최근 『Symantec의 Blue Coat 인수』, 『Cisco의 CloudLock 인수』, 『IBM Security의 Resilient Systems 인수』 등의 사례에서 보듯이 빅데이터와 클라우드 보안 시장의 주도권 확보를 위한 업계 재편이 빠르게 진행되고 있는 추세임.

[표16] 15대 사이버보안 기업 매출/시장점유율 현황

단위 : \$백만/%

회사명	전체매출 (2014/2015)	사이버보안 매출 (2014/2015)	사이버보안 시장 점유율(%)	사업 분야
Blue Coat Systems	613	613	0.8	IT보안
Check Point Technology	1,630	1,496	2.0	IT보안
Cisco	49,161	1,747	2.3	네트워크솔루션
EMC	24,440	1,035	1.4	IT
Fortinet	770	770	1.0	네트워크솔루션
Hewlett-Packard	110,616	1,035	1.4	IT
IBM	81,741	2,000	2.7	IT
Intel Corporation	55,355	2,167	2.9	Microprocessor
Kaspersky	711	711	0.9	IT보안
Lockheed Martin	45,600	779	1.0	항공/방위/보안
Northrop Grumman	25,969	622	0.8	항공/방위/보안
Optiv	1,513	1,513	2.0	사이버보안
Palo Alto Networks	928	928	1.2	네트워크보안
Symantec	3,600	3,600	5.2	IT보안/저장
Trend Micro	1,043	1,043	1.4	IT보안
기타	-	55,018	72.9	-
전체	-	75,429	100	-

[자료원] ASD리서치, Visiongain 2016

1 블루코트 시스템 [Blue Coat Systems, Inc]

	대표자	Greg Clark	종업원수	1,400명
	소재지	미국, 캘리포니아	사이버보안 매출	6.13억 달러 ('14년) 추정
	설립연도	1996년	시장점유율	0.8%
홈페이지	https://www.bluecoat.com/			
개요	<ul style="list-style-type: none"> - '96년도 CacheFlow라는 이름으로 설립된 이후, 웹 보안 및 WAN 최적화 솔루션 기업으로 발전했으며, 포천 500대 기업의 70%를 고객으로 두고, 전세계 15,000여개의 기업에게 서비스를 제공하고 있음. - '11년 Thoma Bravo에게 인수되어 나스닥 상장이 취소되고 개인회사로 전환되었고, '15년에 Bain Capital에 24억 달러에 재인수됨. 최근('15.6월) 사이버보안 최강자인 Symantec에게 46억 달러에 인수가 발표됨. 			
매출 현황	<ul style="list-style-type: none"> - '11년부터 개인 기업화됨으로써 정확한 매출규모는 공지하지 않고 있으나, Visingain보고서에 따르면 '14년도 전체 매출이 6.13억 달러에 달할 것으로 추정됨 - 매출에서 제품 판매와 서비스판매 비중이 6:4 정도의 비율이나, 서비스판매 성장률이 가파르게 성장하고 있는 추세임. - 지역별 매출 비중으로는 미국시장 45%, 유럽 35%, 아시아 20% 순이며, 미국에서의 매출은 정체하는 반면, 유럽, 아시아 시장이 지속적으로 확대되고 있음. 			
사업 분야	<ul style="list-style-type: none"> - 보안 강화와 모빌리티 지원, 네트워크 안정성 유지, 데이터 손실 방지 및 복구 등을 기업의 생산성 향상과 혁신을 지원하기 위해 5개 사업으로 세분화 			
주요제품 솔루션	<ul style="list-style-type: none"> - Proxy-based traffic inspection and policy enforcement - Encrypted traffic management - Advanced threat protection - Incident response, analytics & forensics - Web application protection - Network performance optimization 			
경쟁사	Intel Security, Raytheon, Cisco, Symantec, Trend Micro, Check Point			
M&A	<ul style="list-style-type: none"> - '11.12월, Thoma Bravo, LLC에 13억 달러에 피인수 - '15.05월, Bain Capital에 24억 달러에 피인수 - '15.08월, 기업클라우드 보안기업 Perspecsys 인수 - '15.11월, 클라우드 웹 보안기업 Elastics를 2.8억 달러에 인수 - '16.06월, Symantec에 46억 달러에 피인수 			

2

체크포인트 [Check Point Software Technologies Ltd]

	대표자	Gil Shwed	종업원수	3,400백명 (2015)
	본사 소재지	이스라엘, 텔아비브	사이버보안 매출	16.3억 달러 (2015)
	설립연도	1993년	시장점유율	2.0%
홈페이지	https://www.checkpoint.com			
개요	<ul style="list-style-type: none"> - 이스라엘에 본사를 둔 기업으로 미국에는 캘리포니아에 본사를 설립하여 운영 중임. 인터넷 정보보안에 전문성을 인정받아, 전 세계적으로 10만개 이상의 대기업, 중소기업을 대상으로 서비스를 제공하고 있음. 			
매출 현황	<ul style="list-style-type: none"> - '15년 매출은 16.3억 달러로 전년대비 9.4% 성장을 기록 중이며, 지역적으로는 미국이 전체 매출의 49%, 유럽 37%, 아시아 14%의 비중을 차지하고 있음. - Check Point Institute for Information Security (CPIIS)라는 연구소를 설립하여 연간 1.2억 달러 이상의 연구개발 투자 진행 중 			
사업 분야	<ul style="list-style-type: none"> - 차세대 위협방지 프로그램, 모바일보안, Endpoint보안, 방화벽, 사이버보안 시스템관리 기술에 집중하고 있으며, 현재 39건의 미국내 특허를 보유하고, 25건의 특허심사가 진행 중에 있음. - 특히, FireWall-1이라는 프로그램을 통해 방화벽 기술에 있어 독보적인 기술을 보유하고 있다고 알려짐. 			
주요제품/솔루션	<ul style="list-style-type: none"> - Next Generation Threat Prevention - Mobile Security - Endpoint Security - Next Generation Firewalls - Retail / Point of Sale (PoS) - Critical Infrastructure & ICS/SCADA - Public and Private Cloud Security 			
경쟁사	Dell, Cisco, Juniper Network, Fortinet, Palo Alto Networks, Intel Security 등			
M&A	<ul style="list-style-type: none"> - '11.11월, 사이버보안 리스크관리 전문업체 DynaSec 인수 - '15.02월, 사이버위협 감지기술 기업 Hyperwis, 8천만 달러에 인수 - '15.04월, 모바일보안기업 Lagoon Mobile Solution 인수 			
전략적 제휴	<ul style="list-style-type: none"> - '15.07월, VMware와 파트너십으로 데이터센터 통합보안 솔루션제공 - '15.07월, FireEye와 양사의 플랫폼간 정보공유 파트너십 제휴 			

3 | 시스코 시스템즈 [Cisco Systems]

	대표자	Chuck Robbins	종업원수	71,833명 (2015)
	본사 소재지	미국, 캘리포니아	사이버보안 매출	17.5억 달러 (2015)
	설립연도	1984년	시장점유율	2.3%
홈페이지	http://www.cisco.com/			
개요	<ul style="list-style-type: none"> - 시스코는 전 세계적으로 네트워크 장비의 디자인, 제조, 판매 공급하고 있는 S&P500 기업 중에 하나임. - 동사의 제품군은 크게 차세대네트워크, Service Provider Video, 데이터센터, 와이어리스, 사이버보안 등으로 나눌 수 있는데, 최근 타기업을 인수합병하는 방식으로 사이버보안 사업에 강자로 자리매김하고 있는 중임. 			
매출 현황	<ul style="list-style-type: none"> - 시스코의 기업 전체 매출은 2015년 490억 달러에 달하며, 사이버보안사업 분야 매출은 동년 17.5억 달러로 전체 매출대비 3.6%에 불과하나, 2015년 11.6% 성장하는 등 여타 사업부문의 성장률을 압도하고 있음. 			
사업 분야	<ul style="list-style-type: none"> - 사물인터넷, 가상현실, 클라우드를 세계의 큰 전략의 축으로 하여 기술개발뿐만 아니라, 타사와의 파트너십을 통한 성장을 추구. 특히 최근에 다수의 Endpoint, IoT, 클라우드 보안 기업을 인수하고 있는 추세임. 			
주요제품 솔루션	<ul style="list-style-type: none"> - Next-Generation Firewalls - Advanced Malware Protection - VPN Security Clients - Web Security - Router Security - Email Security - Next-Generation Intrusion Prevention Systems 			
경쟁사	Symantec, Alcatel-Lucent, Amazon Web Service, Check Point, FireEye, Dell 등			
M&A	<ul style="list-style-type: none"> - '15.09월, 클라우드 보안업체 Pawaa 인수 - '15.11월, 인프라 보안업체 Acano 인수 - '15.08월, 네트워크 보안업체 Lancope 4.5억 달러에 인수 - '16.08월, 클라우드 보안업체 CloudLock 2.9억 달러에 인수 			

4

이엠씨 [EMC Corporation]

	대표자	Joseph M. Tucci	종업원수	50,000명 (2016)
	본사 소재지	미국, 매사추세츠	사이버보안 매출	10.3억 달러 (2014)
	설립연도	1979년	시장점유율	1.4%
홈페이지	http://www.emc.com			
개요	<ul style="list-style-type: none"> - EMC는 데이터저장, 정보보안, 가상현실, 클라우드컴퓨팅 등의 제품과 서비스를 공급하는 S&P500기업임. 2006년 사이버보안 감시 전문업체인 RSA를 인수함으로써 본격적으로 사이버보안 사업에 뛰어든 바 있음. 			
매출 현황	<ul style="list-style-type: none"> - 2014년 동사의 전체 매출 244억 달러 중 사이버보안 관련 매출은 10.3억 달러(전체의 4.2%)로 지난 4년간 연평균 9.2% 성장을 기록. - 지역별로 전체매출에서 미국이 차지하는 비중이 53%, 유럽(29%), 아시아(13%), 중남미(6%) 등 순 			
사업 분야	<ul style="list-style-type: none"> - '15년 말 Dell은 EMC를 670억 달러에 인수 결정을 발표함. 이는 IT분야 최대의 블록버스터 M&A로 평가받고 있으며, Dell은 EMC를 인수함으로써, 사이버보안 분야에서 VMware, SecureWorks 기업을 계열사로 보유하는 강자로 부상하고 있음. 			
주요제품 솔루션	<ul style="list-style-type: none"> - 백업 및 보호 스토리지 : 중소기업 환경에 적합한 솔루션으로 백업, 아카이브 및 재해 복구 설계 - 백업 및 보호 소프트웨어 : 백업 및 복구 환경 전반에 통합되고 자동화된 모니터링, 분석, 보고 기능 - 데이터 보호 : 백업 및 복구, 스냅샷 기반 백업, 아카이브 등 포괄적인 데이터 보호 - 클라우드 백업 및 복구 : 클라우드 백업 및 복구로 데이터 보호 - 복제본 데이터 관리 : 셀프 서비스 데이터 관리 솔루션 			
경쟁사	IBM, HP, Western Digital Corp., Intel Security, Symantec, SanDisk Corp. 등			
M&A	<ul style="list-style-type: none"> - '13.07월, 신원접근관리 솔루션기업 Aveska 인수 - '14.05월, 빅데이터관련 보안업체 DSSD 인수 - '14.10월, 클라우드컴퓨팅 스타트업 Cloudscaling 인수 - '14.10월, 클라우드 기반 보안업체 Maginatics 인수 - '15.10월, Dell에 의해 670억 달러에 피인수 			

5 포티넷 [Fortinet Inc]

FORTINET	대표자	Ken Xie	종업원수	2,850명
	본사 소재지	미국, 캘리포니아	사이버보안 매출	7.7억 달러 (2014)
	설립연도	2000년	시장점유율	1.0%
홈페이지	https://www.fortinet.com			
개요	<ul style="list-style-type: none"> - 포티넷은 고성능 네트워크 보안 제품과 서비스 공급회사로 2000년에 중국계 미국인 Ken과 Michael Xie에 의해 설립되어 2014년 연매출 7.7억 달러의 글로벌 기업으로 성장함. - 대표 상품으로 FortiGate라는 통합네트워크 보안 방화벽이 있으며, 전세계 2만여개의 채널 파트너를 통해 서비스를 공급 중임. 			
매출 현황	<ul style="list-style-type: none"> - 포티넷은 2009년 매출 2.5억 달러에서 2014년 7.7억 달러로 지난 5년 동안 매출이 3배 이상 빠르게 성장하고 있음. - 제품과 서비스가 차지하는 매출 비중이 거의 유사하고 성장률도 2014년 각각 29%, 22%를 기록하는 등 매우 안정적 사업모델을 가지고 있는 것으로 평가됨. 			
사업 분야	<ul style="list-style-type: none"> - 포티넷은 통신업체, 데이터 센터, 엔터프라이즈, 분산 오피스 및 MSSP에게 네트워크 보안 어플라이언스 및 보안 구독 서비스를 제공 - 네트워크 보안 플랫폼, FortiGate는 방화벽, VPN, 말웨어 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 			
주요제품 솔루션	<ul style="list-style-type: none"> - 지능형 위협 보호(FortiSandbox) - 웹 애플리케이션 방화벽(FortiWeb) - 보안 이메일 게이트웨이(FortiMail) - DDoS 보호(FortiDDoS) - 애플리케이션 전송 컨트롤러(FortiADC) - 사용자 ID 관리(FortiAuthenticator, FortiToken) - 데스크탑, 노트북 및 모바일 기기용 엔드포인트 보안(FortiClient) 			
경쟁사	Cisco, Juniper Networks, Check Point, Palo Alto Networks, FireEye 등			
전략적 제휴	<ul style="list-style-type: none"> - '15.07월, 일본 NTT와 글로벌 사이버보안 파트너십 체결 - '15.05월, 미국 연방국토안보부와 R&D협력 파트너십 체결 			

6

휴렛패커드 [Hewlett Packard Enterprise]

	대표자	Meg Whitman	종업원수	287,000명
	본사 소재지	미국, 캘리포니아	사이버보안 매출	10.3억 달러 (2015)
	설립연도	1939년	시장점유율	1.4%
홈페이지	https://www.hp.com			
개요	<ul style="list-style-type: none"> - 휴렛패커드는 '15년 프린터 및 PC 사업부 위주의 HP Inc.와 기업 하드웨어 및 서비스 부문인 휴렛팩커드 엔터프라이즈(HPE)로 분사 - HPE는 IT 인프라스트럭처, 빅데이터, 보안, 업무환경 생산성 향상 솔루션 등 4개의 핵심 영역에 중점 - HP는 '10년에 ArcSight를 인수하여 본격적으로 사이버보안 사업에 뛰어들어, 정보보안 및 이벤트 관리(SIEM) 분야의 최강자로 자리매김. - '15년에 자사의 네트워크 보안 부문인 TippingPoint를 Trend Micro에 매각하고, 네트워크 보안 부문의 기술 라인업을 위해서 제3자로부터 기술을 아웃소싱하는 전략을 구사할 계획 			
매출 현황	<ul style="list-style-type: none"> - 기업 전체 매출은 1,030억 달러('15년)에 달하며, 이중 사이버보안 부문 매출은 10억 달러 수준임. - '14년 HP는 미국 국토안보부로부터 3,200백만 달러의 네트워크 및 시스템 보안 솔루션 계약을 체결하여 33개 연방정부 기관에 제공 - '15년 국방부와 향후 3년 동안 4.7억 달러의 차세대 네트워크 보안 솔루션 제공 계약을 체결하는 등 對정부 사업에서 실력을 입증 			
사업 분야	<ul style="list-style-type: none"> - 엔터프라이즈 보안 소프트웨어 및 솔루션은 정보 연관성을 포함 애플리케이션 분석 및 네트워크 수준 방어를 통합하고 보안에 대한 사전 대응적 접근 방식을 제공 			
주요제품 솔루션	<ul style="list-style-type: none"> - Fortify 애플리케이션 보안 : 모바일, 타사 및 웹 사이트 보안을 위한 전체 SDLC(소프트웨어 개발 라이프 사이클)에 적용 - ArcSight SIEM : 솔루션 포괄적 위협 탐지 및 컴플라이언스 관리 - HPE Security 클라우드, 사내, 모바일 데이터 중심 보안 솔루션 - HPE Security Research : 취약성 조사 및 보안 인텔리전스 제공 			
경쟁사	Cisco, Symantec, Juniper Networks. Checkpoint, IBM등			
M&A	<ul style="list-style-type: none"> - '10.9월, SIEM 솔루션기업 ArcSight를 15억 달러에 인수 - '15.2월, 모바일 네트워크 기술기업 Aruba Networks 인수 - '15.5월, 클라우드 보안업체 Voltage Security 인수 - '15.10월, 네트워크보안 부문 TippingPoint를 Trend Micro에 매각 			

7 | 인텔 [Intel Corporation]

	대표자	Brian Krzanich	종업원수	107,300명
	본사 소재지	미국, 캘리포니아	사이버보안 매출	21.7억 달러
	설립연도	1968년	시장점유율	2.9%
홈페이지	https://www.intel.com			
개요	<ul style="list-style-type: none"> - 세계적인 마이크로프로세서 제조업체인 인텔은 '11년에 전격적으로 McAfee를 인수함으로써 사이버보안 분야의 최강기업으로 거듭남. - '15년, McAfee를 제품 브랜드로는 사용 중이나, 회사명은 Intel Security Group 개명하고 인텔본사와 화학적 통합을 추구 - '16.6월, 파이낸셜타임즈는 인텔이 사이버보안 부문 사업을 사모펀드에 매각을 고려하고 있다고 보도함. - 당초 인텔은 McAfee의 사이버보안 기능을 반도체칩에 내장해 해킹위협 감지 수준을 더 높이겠다는 계획이었으나, 개발이 지연되면서 사이버보안 부문 보다는 지능형 반도체칩 제조에 보다 집중할 계획인 것으로 알려짐. 			
매출 현황	- McAfee가 포함된 소프트웨어 및 서비스부문(Software and Service Operating Segment) 매출은 21.7억 달러로 인텔의 전 세계 매출의 4% 비중을 차지함.			
사업 분야	- 시간 가시성과 분석 제공, 위험 감소, 컴플라이언스 보장, 인터넷 보안 개선 목적으로 기업을 지원하는 보안 관리 기능과 악성 프로그램 방지, 안티스파이웨어, 안티바이러스 소프트웨어 등 제공			
주요제품 솔루션	<ul style="list-style-type: none"> - 일반소비자용 : 개인용 기기 바이러스, 인터넷, 방화벽 제품 등 - 기업용 : 중소기업, 대기업용 보안 솔루션, 엔드포인트 안티말웨어, 안티 스파이웨어, 관리자용 보안 스캔 기능 - Security as a Service(SaaS) : 웹 및 이메일 보안, 필터링, 암호화 등 - 데이터센터용 : 클라우드 및 데이터 보안 솔루션 			
경쟁사	Kaspersky Lab, Symantec, HP, EMC, Trend Micro 등			
M&A	<ul style="list-style-type: none"> - '11.2월, 대표적 사이버보안기업 McAfee를 78억 달러에 인수 - '11.4월, 데이터베이스 보안기업 Sentrigo 인수 - '11.4월, 정보보안업체 NitroSecurity 인수 			

IBM	대표자	Ginni Rometty	종업원수	379,592명
	본사 소재지	미국, 뉴욕	사이버보안 매출	20억 달러
	설립연도	1911년	시장점유율	2.7%
홈페이지	https://www.ibm.com			
개요	<ul style="list-style-type: none"> - 1970년대 후반 보안 사업을 시작한 이래, 현재까지 지속적인 기업 인수 및 R&D를 통해 성장하여 전세계 보안시장 3위의 위상을 정립 - '15년 1월부터 보안 서비스 영역과 소프트웨어 영역이 하나의 보안 사업부로 통합되어, 보안 컨설팅 서비스에서 세부 분야 보안까지 종합 솔루션을 제공 			
매출 현황	<ul style="list-style-type: none"> - '15년 IBM 보안사업 분야의 총 매출은 20억 달러로 전년 대비 12%이상의 고성장. 			
사업 분야	<ul style="list-style-type: none"> - 기업의 보안 전략 및 리스크 관리, 컴플라이언스 관리를 포함하는 보안 거버넌스 컨설팅을 비롯하여, 보안 인텔리전스를 기반으로 엔드포인트 보안에서부터 네트워크, 데이터, 애플리케이션, 모바일 보안 등 전영역의 보안 컨설팅 서비스 및 솔루션을 제공 - 사이버보안 분야에 총 20억 달러에 달하는 연구개발 투자를 통해 3,700개 이상의 기술특허를 보유하고 있음 - 보안 위협 및 관련 데이터를 스스로 이해하고, 학습 및 추론도 가능한 코그니티브 시스템에 있어 최강자 			
주요제품 솔루션	<ul style="list-style-type: none"> - 사이버 위협 분석 인텔리전스 플랫폼 QRadar, 클라우드 환경에서 사이버 위협 없는 업무를 지원하는 클라우드 시큐리티 인포서(Cloud Security Enforcer), 보안 위협을 감지해 위협 요소를 신속히 차단하고 파트너 생태계를 활용한 협업 기반 보안 플랫폼 X-Force Exchange 등이 대표적 - 일종의 온라인 보안 앱스토어인 App Exchange를 통해 IBM뿐 아니라 보안 관련 파트너 솔루션을 다운로드 할 수 있는 서비스 제공 - 그 외에도 통합 로그 수집 및 보안 분석/관제솔루션, 온라인뱅킹 PC/맥/모바일 보안솔루션, 통합계정 및 접근권한 관리 솔루션, 실시간 데이터보호 및 암호화 솔루션 등 			
경쟁사	인텔, 오라클, HP, 아마존 웹서비스, 델, 체크포인트 등			
M&A	<ul style="list-style-type: none"> - '13.8월, 사이버보안업체 Trusteer 인수 - '14.7월, 클라우드보안업체 CrossIdeas 인수 - '14.8월, 클라우드보안업체 Lighthouse Security Group 인수 - '16.2월, 사이버보안업체 Resilient Systems 인수 			

9 | 캐스퍼스키 랩 (Kaspersky Lab)

	대표자	Eugene Kaspersky	종업원수	3,000명
	본사 소재지	러시아, 모스크바	사이버보안 매출	7.1억 달러
	설립연도	1997년	시장점유율	0.9%
홈페이지	https://www.kaspersky.com			
개요	<ul style="list-style-type: none"> - 캐스퍼스키는 러시아 모스크바에 본사를 두고 있는 국제적 사이버보안기업으로 전세계 30여개 국에 영업사무소를 설치하여 25만개 이상의 기업고객 및 3억 명에 달하는 소비자 고객을 대상으로 서비스를 제공하고 있음. - IDC와 카트너 등은 기업용 엔드포인트보안 기업들 중 캐스퍼스키를 글로벌 리더 기업으로 선정함 			
매출 현황	<ul style="list-style-type: none"> - '15년도 전세계 매출은 7.1억 달러로 전년대비 6.2% 성장세 구가하여 전체 시장점유율은 0.9% 수준 - '07년 매출 1억 달러에서 '15년에는 매출이 무려 7배가 성장하는 등 사이버보안 분야에서 가장 빠르게 성장하는 기업 중 하나로 꼽힘. 			
사업 분야	<ul style="list-style-type: none"> - 캐스퍼스키는 안티말웨어 및 엔드포인트보안 분야에 특화되어 두각을 나타내고 있음. - 동사는 인터폴(INTERPOL)과의 협력을 통한 다수의 글로벌 금융 사이버범죄 방지 및 대응에 성공함으로써 명성을 얻음. - 특히 동사는 리셀러들과의 채널 파트너십을 통해 신규 시장을 확대하는 마케팅 전략을 성공적으로 활용한 대표적 케이스임. - 야심차게 미국 정부시장 진출에 뛰어들었으나, 러시아기업인 관계로 미국 정부시장으로부터 신뢰를 얻지 못하고 있는 것으로 알려짐. '15년 블룸버그통신은 동사가 러시아정부와 유착관계가 있다고 보도하기도 함. 			
주요제품 솔루션	<ul style="list-style-type: none"> - 일반소비자용 인터넷 보안솔루션 - 중소기업용 보안 : 통합 관리 콘솔, 워크스테이션용 안티 말웨어, 파일 서버용 안티 말웨어, MDM(모바일 기기 관리) 등 - 기업용 엔드포인트 보안 : 모바일 보안, 제어(애플리케이션, 매체, 웹), 암호화, 인터넷 게이트웨이 보안 등 			
경쟁사	트렌드마이크로, 인텔, 소포스, 세멘텍, EMC 등			
M&A	<ul style="list-style-type: none"> - 동사는 외부기업 인수보다는 자체 기술개발(In-house)을 통한 기업의 혁신문화를 유지하는 전략을 채택함. 			

10

락히드마틴 [Lockheed Martin Corp.]

	대표자	Marillyn A. Hewson	종업원수	126,000명
	본사 소재지	미국, 메릴랜드	사이버보안 매출	7.8억 달러
	설립연도	1995년	시장점유율	1.0%
홈페이지	https://www.lockheedmartin.com			
개요	<ul style="list-style-type: none"> - 락히드마틴은 미국 최대의 항공방산업체이자 정부조달사업자로서 '15년도 전체 기업 매출이 460억 달러에 달하는 글로벌 기업임. - 미국 연방정부와의 네트워크를 기반으로 국방부, 국토안보부 및 정보기관들의 사이버보안 계약을 체결하는 등 정부시장에 역량보유 - 사이버보안은 정보서비스 및 글로벌 솔루션(IS&GS) 부서에서 담당 - '16.8월, 동사는 IT서비스 부문을 Lidos에 46억 달러에 매각함으로써 기업 전략차원에서 상업용 사이버보안 사업을 청산하기로 결정함. - 이로서 Leidos는 미국 정부조달 IT서비스 및 사이버보안 분야의 최대 사업자로 부각되게 됨. 			
매출 현황	<ul style="list-style-type: none"> - 동사의 사이버보안관련 연간 매출은 7.8억 달러('14년)로 IT서비스 관련 사업 분야 매출에서 사이버보안 사업이 차지하는 비중은 10% 정도에 해당함. 			
사업 분야	<주요 정부조달 계약 현황> <ul style="list-style-type: none"> - '15년, 영국 경찰청 사이버사령부 제어시스템 공급(90백만 달러) - '15년, 미국 육군 사이버연구소 건설(1.4백만 달러) - '14년, 미국 연방정부 사이버공격대응시스템 공급(6,000백만 달러) - '13~18년, 미국 국방부 사이버보안시스템 (217백만 달러) - '12~17년, 미국 육군 사이버보안사령부 시스템구축(80백만 달러) - '12년, 미국 국방부 글로벌 데이터 네트워크 구축(4,600백만 달러) 			
주요제품 솔루션	<ul style="list-style-type: none"> - 첨단 사이버정보 분석과 공격대응을 위한 Cyber Kill Chain 솔루션 - 전력망, 석유·가스 시설 등 주요 인프라에 대한 사이버 공격 방어 - ATP공격 감시시스템 등 			
경쟁사	BAE 시스템즈, 노스롭그룸맨, 레이스온, 인텔, Booz Allen Hamilton 등			
M&A	<ul style="list-style-type: none"> - '14.4월, 오일·가스·화학시설 등에 대한 사이버보안업체 Industrial Defender 인수 - '14.12월, 의료관련 사이버보안기업 System Made Simple 인수 			

11 | 노스럽그룸맨 [Northrop Grumman Corporation]

	대표자	Wes Bush	종업원수	65,000명
	본사 소재지	미국, 버지니아	사이버보안 매출	6.2억 달러
	설립연도	1994년	시장점유율	0.8%
홈페이지	https://www.northropgrumman.com			
개요	<ul style="list-style-type: none"> - 노스럽그룸맨은 미국의 항공방위기업으로 연간 매출 235억 달러에 달하는 세계5위의 방위산업체임. - 락히드마틴 다음으로 미국 정부(국방부 포함) IT솔루션을 제공하는 최대기업으로 '09년에 자체 사이버보안운영센터를 설립하여 정부 및 민간기업의 사이버보안 관련 서비스를 제공하고 있음. - 미국, 영국, 호주에 4개의 사이버보안협력센터를 설립하고 이를 통해 공동기술개발, 스타트업 진흥, 글로벌 전략적 파트너 생태계를 조성하고 있음. 			
매출 현황	<ul style="list-style-type: none"> - '14년 사이버보안 관련 매출은 6.2억 달러로 전체 IT매출의 10%를 차지함. 연방정부의 국방예산 감축으로 IT서비스 매출이 다소 감소하는 추세 속에서는 사이버보안 관련 매출은 지속적으로 증가하고 있는 중. 			
사업 분야	<p><주요 정부조달 계약 현황></p> <ul style="list-style-type: none"> - '15년, 국토안보국 생체인식 인증솔루션 제공(1.7백만 달러) - '15년, 영국 사이버보안 관제소 시스템 공급(비공개) - '14~20년, 해군기지 네트워크 보안 솔루션(2,500백만 달러) - '14년, 국토안보국 사이버비상대책팀 운영서비스(350백만 달러) - '14년, 국토안보국 엔드포인트 자산관리 소프트웨어(60백만 달러) - '12년, 나토 본부내 사이버보안 센터 설립(64백만 달러) 			
주요제품 솔루션	<ul style="list-style-type: none"> - 사이버정보분석 위협정보 수집 및 분석을 통한 예방책 마련 - 바이오메트릭을 통한 신분도용 방지를 위한 인증·암호화 - 국가 인프라 보안 및 국방관련 솔루션 등 			
경쟁사	Raytheon, BAE Systems, Lockheed Martin, General Dynamics, L-3 Communications 등			
M&A	<ul style="list-style-type: none"> - '12.9월, 호주 사이버보안기업 M5 Network Security 인수 - '16.5월, 사이버정보분석기업 Code Dx 인수 			

	대표자	Dan Burns	종업원수	1,200명
	본사 소재지	미국, 덴버	사이버보안 매출	15억 달러
	설립연도	2015년	시장점유율	2.0%
홈페이지	https://www.optive.com			
개요	<ul style="list-style-type: none"> - Optiv는 '15년 Accuvant와 FishNet Security가 합병하여 설립된 사이버보안 솔루션제공 기업임. - 300여개의 사이버보안 개발기업과의 기술협력을 통해 전문분야에 걸친 사이버보안 서비스 및 기술을 제공함. - 제품, 서비스, 솔루션이 결합된 프로그램을 통해 정부기관, 교육기관, 기업 고객을 대상으로 사이버 리스크 관리, 공격 대응 및 후속처리, 신분확인 및 도용방지 등의 기능 제공\ 			
매출 현황	- '15년 기준, 동사의 매출은 15억 달러 이상을 전체 시장의 2.0%를 차지하고 있는 것으로 조사됨.			
사업 분야	<ul style="list-style-type: none"> - 서비스 : 보안프로그램전략, 기업 리스크 및 컴플라이언스, 위협방지 및 관리, Managed Security Services, 신원접근관리 등 - 기술 : Monitoring and Operations, Defenses and Controls 등 - 솔루션 : Cloud Security, Enterprise Security Architecture, Advanced Threat, IoT, Security Intelligence 등 			
주요 파트너사	A10 Networks, Arbor Networks, BeyondTrust, BitSight, Blue Coat, Check Point, Cisco, CyberArk, Digital Guardian, F5 Networks, FireEye, Forcepoint, ForeScout, Fortinet 등 300여개			
경쟁사	Dell, IBM, HP, BT Group 등			
M&A	- '15.7월, Accuvant와 FishNet Security 합병, Optiv 출범			

13 | 팔로알토 네트워크 [Palo Alto Networks]

	대표자	Mark D. McLaughlin	종업원수	1,722명
	본사 소재지	미국, 캘리포니아	사이버보안 매출	9.3억 달러
	설립연도	2005년	시장점유율	1.2%
홈페이지	https://www.paloaltonetworks.com			
개요	<ul style="list-style-type: none"> - 캘리포니아에 소재한 네트워크, 기업보안 전문기업으로 핵심제품은 네트워크 보안을 위한 첨단 방화벽, 클라우드 기반 방화벽 솔루션 - '15년 현재 전 세계 140개 국에 31,000개의 고객을 확보하고 있음. - 동사는 빠른 매출 성장에도 불구하고, 기업용 사이버보안 시장의 경쟁이 심화됨에 따라 신시장 및 제품 개발을 위해 막대한 R&D 투자를 진행하고 있어 장래가 가장 촉망받는 사이버보안 기업으로 여겨짐. 			
매출 현황	<ul style="list-style-type: none"> - 동사의 '15년도 매출은 9.3억 달러로 전년대비 55%가 넘는 성장세를 보이고 있음. - 연간 1.8억 달러가 넘는 막대한 R&D 투자를 진행하고, 매년 R&D 투자 증가율이 60~70%대를 유지하고 있음. 			
사업 분야	<ul style="list-style-type: none"> - 기업용(전력, 금융, 병원, 소매 등) / 서비스제공자(Service Providers, Cloud Providers, MSSPs) / 정부 / 교육기관 등을 대상으로 한 종합 보안 솔루션 제공 - Internet Gateway, Mobility, Ransomware, Threat Prevention 분야 등에서 Accenture, Amazon Web Services, Microsoft, Proofpoint, PwC, Splunk, Tanium, VMware와 같은 글로벌 리더기업과 협력을 통해 발전하고 있음. 			
주요제품 솔루션	<ul style="list-style-type: none"> - 차세대 방화벽 - 금융 서비스 사이버 보안 - 차세대 데이터 센터 보안 - 중요 인프라를 위한 차세대 보안 플랫폼 			
경쟁사	Cisco, Juniper Networks, Intel, IBM, HP, Check Point, Fortinet 등			
M&A	<ul style="list-style-type: none"> - '14.1월, 사이버보안 기업 Morta Security 인수 - '14.5월, 엔드포인트 보안전문기업 Cyvera 인수(200백만 달러) - '15.5월, SaaS 어플리케이션 개발 전문기업 CirroSecure 인수 			

14

시멘텍 [Symantec Corporation]

	대표자	Daniel Schulman	종업원수	11,000명
	본사 소재지	미국, 캘리포니아	사이버보안 매출	36억 달러('16년)
	설립연도	1982년	시장점유율	5.2%
홈페이지	https://www.symantec.com			
개요	<ul style="list-style-type: none"> - Symantec은 1982년 설립되어 '15년 현재 50여 개국, 18,500명 이상의 직원들이 근무하는 세계 최대 소프트웨어 기업으로 성장 - Symantec의 보안, 스토리지 및 시스템 관리 솔루션은 기업 및 개인이 정보를 보호하고 관리할 수 있도록 지원하고, 다양한 사이버 위협으로부터 효율적인 보호를 제공 - 동사는 '15년 사이버보안 부문 Symantec과 정보관리 부문 Veritas Technologies로 분사하였고, Veritas는 사모펀드 Carlyle Group에게 매각됨. 			
매출 현황	<ul style="list-style-type: none"> - '15년 사이버보안과 정보관리 부문 분할 이전 매출은 총 65억 달러로 이중 사이버보안부문 매출(39억 달러)은 전체의 60%에 달함. - 분할 이후, 사이버보안 부문 Symantec의 매출('16년)은 36억 달러로 전년 대비 소폭 축소 			
사업 전략	<ul style="list-style-type: none"> - 기업용보안 제품과 노턴 엔드포인트에서 수집된 위협정보를 기반으로 인텔리전스와 원격정보를 제공 - 보안관제, 사고대응, 보안 인텔리전스 및 보안전문가 대상 시뮬레이션 기반 교육 등 사이버보안 서비스 역량을 강화 - 주력상품인 Norton 제품군을 통합해 보안제품 포트폴리오 간소화 			
주요제품 솔루션	<ul style="list-style-type: none"> - 주력제품 : Endpoint Protection, Encryption(PGP), Data Loss Prevention, Mobile Security and Management, SSL Certificates 등 - 신규제품 : Advanced Threat Protection, Endpoint Suite, IT Management Suite, Code Signing for Android 등 - 산업별 솔루션 : 금융, 보건, 공공부문, 통신 분야 등 			
경쟁사	Intel Security, Trend Micro, EMC, Dell, IBM, HP 등			
M&A	<ul style="list-style-type: none"> - '13.7월, 스페인 사이버보안 스타트업 PasswordBank 인수 - '14.5월, 데이터보안 기업 NitroDesk 인수 - '15.8월, 사이버보안 교육기업 Blackfin Security 인수 - '16.6월, 사이버보안 기업 Blue Coat 인수(46억 달러) 			

15 | 트렌드 마이크로 [Trend Micro]

	대표자	Eva Chen	종업원수	5,258명
	본사 소재지	일본, 도쿄	사이버보안 매출	10억 달러
	설립연도	1988년	시장점유율	1.4%
홈페이지	https://www.trendmicro.com			
개요	<ul style="list-style-type: none"> - 트렌드마이크로는 대만계 미국인인 Steve Chang에 의해 미국 캘리포니아에서 설립된 후, 현재는 본사를 일본에 두고 있는 사이버보안솔루션 분야 글로벌 기업으로서, 개인과 기업, 그리고 정부 기관의 데이터센터, 클라우드 환경, 네트워크 및 엔드포인트에 다층 보안 솔루션을 제공함 - 상호 연결된 제품은 위협 인텔리전스 공유 및 중앙집중식 보안관리를 구현함으로써, 글로벌 위협 인텔리전스인 '클라우드 보안센터(SPN)'의 데이터베이스를 통해 안전한 클라우드 전환을 지원 중 			
매출 현황	<ul style="list-style-type: none"> - '15년 매출이 10억 달러 규모로 전세계 시장의 1.4% 비중을 차지함. - 일본시장에서 매출이 4.8억 달러에 달해 전체 매출의 48%를 차지하고, 미국 24%, 유럽 23% 등의 글로벌 실적을 올리고 있음. 			
사업 분야	<ul style="list-style-type: none"> - 엔드포인트보안과 멀웨어 감지기술의 최강자이나, 근래 Symantec, McAfee 등과의 경쟁이 심화됨에 따라, 차세대 유망기술분야인 클라우드보안, Virtualization, 모바일보안, APT, IoT 기술 시장 진출이 박차를 가하고 있음. 			
주요제품 솔루션	<ul style="list-style-type: none"> - 가상화 및 클라우드 & 서버 통합 보안 - 엔드포인트 보안 - 메시징 및 그룹웨어 보안 - APT 대응 및 네트워크 보안 - 폐쇄환경 보안 - USB 스토리지 보안 등 			
경쟁사	EMC, IBM, HP, Kaspersky, Intel 등			
M&A	<ul style="list-style-type: none"> - '10.11월, 엔드포인트 보안기업 Mobile Armor 인수 - '12.6월, 사이버보안기업 Affirm Trust 인수 - '13.10월, 첨단네트워크 보안기업 Broadweb 인수 - '15.10월, HP의 네트워크보안 부문 TippingPoint 인수(300백만 달러) 			

V

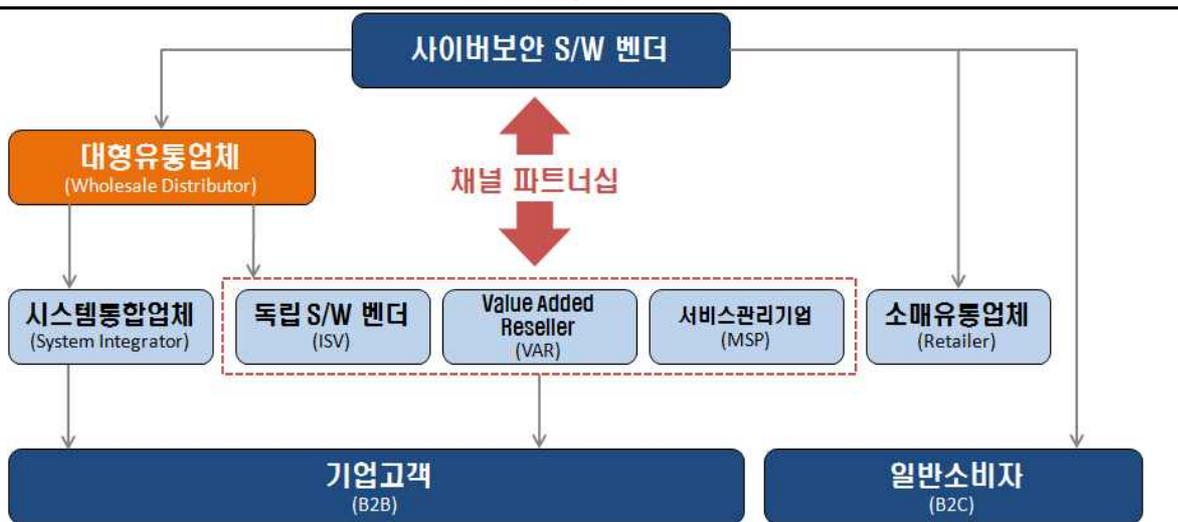
미국의 사이버보안 유통 현황

1

유통구조

- **[개황]** 미국 내 사이버보안 유통구조는 크게 벤더가 직접 온라인 등을 통해 소비자에게 판매하는 직접방식과 전문유통업체를 통한 간접방식으로 구분할 수 있음.
 - Ingram Micro와 같은 대형유통업체를 경유하는 방식이 전체 유통의 70%를 차지하나, 일반적으로 정부, 금융, 통신, 국방 분야의 대규모 프로젝트 경우는 시스템통합업체(SI)를 통한 방식이 보편적
 - 근래 들어 대형벤더들의 경우 독립소프트웨어 벤더(ISV⁸), VAR⁹), 또는 서비스 관리기업(MSP¹⁰)등과 이른바 『채널 파트너십』을 체결 하여 제품을 유통하는 방식이 급격히 증가하고 있음.
 - Kaspersky Lab은 마케팅을 채널파트너에 의존하는 전략으로 '05년 5개에 불과하던 채널 파트너 네트워크가 '15년에는 3,500개로 증가함.

[그림13] 미국 사이버보안 소프트웨어 유통 구조



[자료원] STRABASE / 워싱턴무역관 분석 재구성

8) Independent Software Vender
 9) Value Added Reseller
 10) Managed Service Provider

2 주요 유통기업¹¹⁾

1 Ingram Micro, Inc

주소	1600 E. St. Andrew Place, Santa Ana, Calif.		
전화	(800) 456-8000	홈페이지	www.ingrammicro.com
매출(달러)	426억('14년)	직원수(명)	21,800
개요	세계 1위의 IT 컴퓨터 제품/서비스 공급자이자 시스템통합 솔루션, 마케팅, 유통 전문기업		
주력품목	IT주변기기, 시스템, 소프트웨어, 네트워크 기기 등		
거래벤더	Compaq Computer, Hewlett-Packard, IBM, Microsoft, 3Com 등		

2 Avnet, Inc

주소	2211 South 47th Street, Phoenix AZ 85034		
전화	(480) 643-2000	홈페이지	www.avnet.com
매출(달러)	279억('15)	직원수(명)	19,000
개요	미국을 본사로 둔 다국적기업으로 전세계의 전자기기, 부품, 데이터저장 장치 등 광범위한 IT생태계를 구축하고 있음		
주력품목	기업용 IT장비/솔루션 (servers, storage, software, networking)		
거래벤더	IBM, HP/Compaq, Oracle, EMC 등		

3 Tech Data Corp

주소	15350 Tech Data Drive, Clearwater, Fla		
전화	(800) 237-8931	홈페이지	www.techdata.com
매출(달러)	277억('15)	직원수(명)	9,100
개요	수백개 이상의 IT제품/솔루션을 전세계 십만개 이상의 IT 소매기업에게 공급		
주력품목	IT전자, 기술솔루션, 시스템 관리, 소프트웨어 등		
거래벤더	Compaq Computer, Hewlett-Packard, Microsoft, IBM, 3Com 등		

4 SYNEX Information Technologies

주소	3797 Spinnaker Court, Fremont CA 94538		
전화	(864) 289-4000	홈페이지	www.synnex.com
매출(달러)	133억('15)	직원수(명)	7,500
개요	세계수준의 IT전문유통업체로 VAR, SI, OEM 업체 등에 IT 하드웨어, 소프트웨어를 공급		
주력품목	IT주변기기, 서버, 소프트웨어, 시스템통합, 네트워크 솔루션		
거래벤더	HP, IBM, Intel, Microsoft, Seagate 등		

11) [자료원] <http://www.inetstart.com/>, 위키피디아, 야후파이낸스

5 Arrow Electronics, Inc

주소	2211 South 47th Street, Phoenix AZ 85034		
전화	(303) 824-4000	홈페이지	www.arrow.com
매출(달러)	227억('14)	직원수(명)	17,000
개요	전세계 13,000개 이상의 리셀러와 협력을 통해 IT전자기기, 부품, 보안솔루션 등 제공		
주력품목	기업용 IT장비/솔루션 (servers, storage, software, networking)		
거래벤더	IBM, HP, Sun, Veritas, Hitachi Data Systems		

6 ScanSource, Inc

주소	6 Logue Court, Greenville SC 29615		
전화	(864) 288-2432	홈페이지	www.scansource.com
매출(달러)	32억('15)	직원수(명)	15,000
개요	Identification and data capture (AIDC) and point-of-sale (POS) 기술에 주력하여 전세계 리셀러에 공급		
주력품목	AIDC, POS, converged communications 등		
거래벤더	Intermec, IBM Retail Solutions, Avaya, Intel 등		

7 MA Labs

주소	2075 N. Capitol Ave. San Jose CA 95132		
전화	(408) 941-1088	홈페이지	www.malabs.com
매출(달러)	20억('13)	직원수(명)	1,200
개요	모델, 발전장비, 디지털장비, 보안장비, 네트워크 솔루션 등 전문 유통업체		
주력품목	CPUs, Storage Devices, Motherboards, Graphics Cards, Displays, Wireless Networking, Consumer Electronics, Software 등		
거래벤더	Samsung, Micron, AMD, Intel, Microsoft 등		

8 D&H DISTRIBUTING

주소	2525 N 7th St, Harrisburg, PA		
전화	717-236-8001	홈페이지	www.dandh.com
매출(달러)	4.5억('15)	직원수(명)	950
개요	미국과 캐나다에 IT, 전자기기, 전자부품관련 도매유통업체로 주로 중소규모의 리셀러에 유통을 담당		
주력품목	가전, 사무 IT기기, 사이버보안 S/W 및 솔루션 등		
거래벤더	Microsoft, Intel, Creative Labs, Palm, Linsys, Toshiba 등		

9 기타업체

회사명	소재지	업종	거래벤더
Azerty (www.azerty.com)	캘리포니아	wholesale distributor of computers, hardware, computer supplies	HP, Canon, Brother, Lexmark, Imation
Infotel Distributing (www.infotelistributors.com)	오하이오	Full-line distributor	Intel, Microsoft, HP, AMD
ASI Corp (www.asipartner.com)	캘리포니아	Full-line distributor	Microsoft, Intel, Asus, Western Digital, Viewsonic
SED International (www.sedonline.com)	조지아	Full-line distributor	Maxtor, Intel, Microsoft, Acer, Creative Labs, AOC
WYNIT, Inc. (www.wynit.com)	뉴욕	consumer electronics, digital photography, print and presentation, video editing, security and photo ID market	-
Evertex Computer (www.evertex.com)	캘리포니아	excess computer and consumer electronics equipment	-
Arbitech (www.arbitech.com)	캘리포니아	Full-line distributor	3Com, Acer, APC, Cisco, D-Link, HP, IBM, Kingston, Lenovo, Lexmark, Microsoft, Netgear, Sun, Toshiba, Xerox
Westcon Group (www.westcongroup.com)	뉴욕	Networking solution	Cisco, Avaya, Nortel, Check Point, Noki
Interwork Tech (www.interwork.com)	뉴욕	information security, voice, cloud computing & storage, and IT management solutions	-
Agilysys (www.agilysys.com)	오하이오	proprietary enterprise software, services and solutions to the hospitality and retail industries	-
AMAX Engineering (www.amax.com)	캘리포니아	innovative HPC and GPGPU servers and clusters, and storage solutions	-

VI

국내 사이버보안 산업 현황 및 문제점

1 국내 사이버보안 산업 현황

□ 국내기업 현황

- (기업수) 한국정보보안협회의 조사('15년)에 따르면, 국내 소재 사이버보안 기업의 전체 숫자는 299개로 전년보다 43개가 증가함.
 - 서울, 경기, 인천 등 수도권에 사이버보안 기업의 87%가 집중
- (형태) 기업 형태별로는 일반기업이 139개이고, 벤처기업은 160개로 벤처기업 비중이 전체의 53.5%로 높은 편이며, 자본금 50억원 미만인 기업이 전체의 92%에 달하는 등 초기단계 기업이 대다수를 차지함
 - * 자본금 10억원 미만(204개) / 10억~50억(70개) / 50~100억(9개) / 100억 이상(16개)

□ 매출 현황

- (매출) '15년도 사이버보안 기업들의 전체 매출은 전년 대비 11.1% 증가한 1조9천2백억 원에 달할 것으로 추산됨.
 - 네트워크 보안(4,814억 원), 콘텐츠/정보유출 방지보안(3,037억 원) 분야의 매출 비중이 높으며, 보안관리(20.4%), 유지관리(14.6%) 분야의 증가율이 높은 것으로 조사됨.

[표17] 국내 사이버보안 분야별 매출 (2013-2015)

(단위: 백만원, %)

구분		2013년	2014년	2015년(추산)	증가률 (2014-2015)
제품	네트워크 보안	448,224	411,272	481,489	17.1
	시스템(단말) 보안	212,982	181,477	183,615	1.2
	콘텐츠/정보유출	257,716	263,784	303,676	15.1
	암호/인증	126,761	82,672	90,607	9.6
	보안관리	97,542	161,621	194,559	20.4
	기타 제품	133,316	234,308	236,020	0.7
	소계	1,276,541	1,335,134	1,489,966	11.6
서비스	보안컨설팅	76,061	108,978	113,244	3.9
	유지관리	85,212	98,305	112,638	14.6
	보안관제	150,310	144,973	163,053	12.5
	교육/훈련	16	1,251	1,255	0.3
	인증 서비스	42,973	47,224	48,252	2.2
	소계	354,572	400,731	438,442	9.4
합계	1,631,113	1,735,865	1,928,408	11.1	

[자료원] KISIA, 2015 국내 정보보호산업 실태조사

- (전망) 사이버보안 산업은 '15년도 매출 1조9천2백억 원에서 연평균 14.8% 성장을 구가하여 '20년까지 3조8천5억 원으로 증가할 전망
 - '20년까지 제품 부문은 연평균 15.2% 증가하여 3조178억 원, 서비스 부문은 13.6% 성장하여 8,290억 원에 달할 것으로 예상

[표18] 국내 사이버보안 매출 전망

(단위: 백만원, %)

구분	2015	2016	2017	2018	2019	2020	CAGR (2015-2020)
제품	1,489,966	1,688,287	1,940,903	2,246,520	2,605,425	3,017,847	15.2
서비스	438,442	489,350	553,719	631,980	723,844	829,084	13.6
합계	1,928,408	2,177,637	2,494,622	2,878,500	3,329,269	3,846,931	14.8

[자료원] KISIA, 2015 국내 정보보호산업 실태조사

□ 수출 현황

- (전체) 사이버보안 수출은 '11년 450억 원에서 '15년 907억 원으로 연평균 19.2%의 높은 성장세를 보였음에도 불구하고,
 - 전체 매출에서 수출이 차지하는 비중은 4.7%로 미미한 수준

[표19] 국내 사이버보안 수출현황 (2011-2015)

(단위: 백만원, %)

구분	2011	2012	2013	2014	2015(추정)	CAGR (2015-2020)
수출액(A)	45,000	58,688	70,422	72,989	90,700	19.2
전체매출(B)	1,457,900	1,577,587	1,631,113	1,735,865	1,928,408	7.2
전체매출대비 수출비중(A/B)	3.1	3.7	4.3	4.2	4.7	

[자료원] KISIA, 2015 국내 정보보호산업 실태조사

- (국가별) 권역별 수출비중을 살펴봤을 때, 전체의 40.7%를 차지하는 일본이 우리나라의 사이버보안 관련 최대 수출대상국으로 조사되었으며, 다음으로 중국(17.1%), 유럽(5.7%), 미국(2%), 기타(34.6%) 순
 - 전체 수출에서 대미수출 비중이 '13년, 5.1%에서 '14년, 8.3%, '15년에는 2.0%까지 감소하고 있는 추세

[표20] 국내 사이버보안 권역별 수출 비중 (2013-2015)

(단위: %)

국가	2013	2014	2015
일본	70.4	52	40.7
중국	7.0	11.2	17.1
유럽	2.3	4.6	5.7
미국	5.1	8.3	2.0
기타	15.2	23.9	34.6

[자료원] KISIA, 2015 국내 정보보호산업 실태조사

2 문제점

- **[산업구조]** 국내 사이버보안 산업은 기업규모의 영세성과 과도한 출혈 경쟁으로 질(質)보다는 양(良)적 성장에 치우친 한계점 노출
 - 매출 300억 미만의 기업이 전체의 92%를 차지(상장사 18개에 불과)하고 자체 OS, 네트워크 등 기반기술 부재로 주로 응용제품을 만드는 전문 중소기업 위주로 발전
 - 또한, 보안 소프트웨어를 탑재한 하드웨어 솔루션 위주(전체 시장의 73% 이상) 시장으로 발전하여 서비스 위주로 발전한 선진 시장*에 비해 후진적 구조를 가짐. * 세계시장의 경우 서비스시장 60% 이상 비중을 차지
- **[수출부진]** 국내기업들의 전체매출에서 수출시장이 차지하는 비중은 5%에도 미치지 못하는 등 글로벌 진출 기반이 열악한 상황
 - 국내 사이버보안업체 256개('14년) 중 약 14%인 35개 기업만이 해외 수출을 하고 있으며, 이나마도 수출이 일본(40.7%), 중국(17.1%)에 집중됨.
 - 특히, 세계 최대 미국시장으로의 수출비중은 '14년도 8.3%에서 '15년에는 2.0%로 감소하는 등 고전하고 있는 것으로 조사됨.
 - 해외현지지사 비용 부담, 원천기술 부족, 신뢰성 및 해외진출 레퍼런스 부족 등이 주요 원인으로 꼽힘¹²⁾.
- **[기술확보]** 제한적 대상(공공기관, 통신기반시설 등) 및 특정분야(개인정보 보호 등) 중심으로 투자와 연구개발이 진행되어 新성장동력 발굴 미흡
 - 국내기업들의 매출대비 연구개발비*(기술도입 및 각종 인증획득 비용 포함) 비중은 계속하여 감소하는 추세
 - * 매출대비 연구개발비(%) : '14년(14.6) → '15년(15.4) → '16년(11)
 - 신규 ICBM(IoT, 클라우드, 빅데이터, 모바일) 환경에 대처하고 지능화되는 신종 사이버보안위협에 대응할 수 있는 기술개발 미흡
 - 선진국과의 기술격차 해소는 답보 상태이며, 중국은 빠르게 한국과의 기술격차를 좁혀오고 있는 것으로 조사됨.
 - * 對美 기술격차 ('11년 79.8% → '13년 79.9%) / 對中 기술격차 ('11년 70.6% → '13년 72.7%)

12) 한국정보보호산업협회, 2015 국내 정보보호산업 실태조사

VII

우리기업 진출을 위한 시사점

① 사이버보안 생태계 조성, 공공-민간 파트너십이 해답이다.

- 이스라엘, 전 세계 사이버보안 시장을 선도하는 산업 생태계 구축
 - 이스라엘 내 무려 430개 사이버보안 기업이 소재하고, 이들의 연간 매출은 전 세계 시장의 10%에 해당하는 65억 달러에 달함.
 - 또한, 전 세계 사이버보안 투자의 12%가 이스라엘에 집중되고, 40개의 글로벌 R&D센터*가 진출해 있음. (Financial Times 인용)
 - * Cisco, Microsoft, Google, Apple, IBM, Oracle, SAP, EMC, HP, Facebook 등
- 성공배경에는 유기적 공공-민간 협력 시스템이 핵심적 역할
 - 이스라엘은 '11년 국가사이버보안정책(National Cyber Initiative)을 통해 '15년까지 자국을 사이버보안의 메카로 키우겠다는 목표를 천명하고,
 - 국가 사이버국(Israel National Cyber Bureau)을 신설하여 정부, 학계, 민간기업, 투자자본이 협력하는 유기적 시스템을 구축함.
 - 대학에서 개발된 원천기술이 자연스럽게 기업에서 상용화될 수 있는 매개체로 BGN Technologies와 같은 비영리단체가 활약
 - * BGN은 엑손, 지멘스, GM과 같은 150개 글로벌기업과 협약을 체결하여 자국기업과의 파트너십 제휴, 기술판매를 주선해 옴.
- 정부(軍)과 기업의 긴밀한 정보협력이 사이버보안산업 육성의 성공비결
 - 사이버안보 역량과 경험이 풍부한 국방부 산하 사이버사령부(일명 8200부대)가 기술개발과 전문 인력의 산실로서 역할
 - * 이스라엘의 대표 사이버보안기업 Check Point의 창업자도 8200부대 출신임.
 - 이스라엘의 독특한 안보상황* 속에서, 군에서 축적된 사이버 공격 정보와 대응경험이 제대군인 들을 통해 원활하게 민간 기업에 이전되어 타국에서 모방하기 어려운 산업발전의 자양분으로 작용.
 - * 이스라엘은 이슬람세계와의 오랜 전쟁을 거쳐 오면서 90년대 초부터 높아진 사이버안보 수요에 따라 軍이 보유한 사이버보안 기술(정보)이 월등한 수준

② 기술은 실리콘밸리에서 돈은 워싱턴으로... 정부시장에 주목해야

- 미국 연방정부, 사이버보안산업 발전의 핵심 동력으로 역할
 - 연방정부는 연간 미국 전체 사이버보안 시장의 60%에 육박하는 140억 달러의 예산을 집행하고, 연방부처의 사이버관련 지출의 64%가 워싱턴 광역지역(버지니아, 메릴랜드)에 집중됨.
 - 실리콘밸리에는 상용(민간) 기술개발 위주의 기업들이 편재한 반면, 워싱턴을 중심으로 정부 및 군 수요의 시스템통합, 리셀러, 서비스/솔루션 기업 또는 인프라 보안 기업들의 클러스터가 형성됨.
 - * 워싱턴인근 주요업체 : Lockheed Martin, L-3, Leidos, Northrop Grumman, General Dynamics, SAIC, Tenable Network, Novetta, Arxan, Cyren, ZeroFox, CyFIR, Haystax, LookingGlass, Protenus, Paraben, CACI 등 다수
 - 국내 사이버보안 기업들은 연방정부와 거래하는 시스템통합사업자, 리셀러, 서비스업체와 협력을 통해 조달시장 진출을 모색할 필요
 - * Lockheed Martin, L-3, Leidos, Northrop Grumman 등 주요 방산업체들은 시스템 통합업자로서 국방부 및 정부기관의 대형 계약을 수주 공급 중
- 미국 사이버보안 시장 진출, 국방절충교역제도¹³⁾ 활용이 관건
 - 우리나라가 해외 방산업체로부터 무기류 등 구매를 통해 발생한 절충교역 가치는 지난 30년('83~'13년) 동안 174억 달러, '17년까지 63억 달러 규모에 달할 것으로 전망
 - * 우리나라와 절충교역 의무를 가지고 있는 해외방산기업들은 Lockheed Martin, Raytheon 등과 같은 연방정부 대상 사이버보안 솔루션 제공기업임.
 - '09년 방위사업법 시행령 개정을 통해 방산물자 이외에 중소기업의 일반물자(최근 소프트웨어도 포함)도 절충교역을 활용한 수출도 가능
 - 그러나, 중소기업청 『민수분야 절충교역 운영지침』 개정('16.4월)에 따르면, 절충교역 추천대상기업 자격이 전년도 수출실적이 있는 기업의 경우 기존의 생산품목과 다른 신규 품목을 절충교역으로 수출하고자 하는 경우로 제한하고 있는 바, 이에 대한 보다 완화된 제도 마련이 필요함.

13) 해외에서 무기 또는 장비 등을 구입할 때 계약 상대방으로부터 관련 제식 또는 기술 등을 이전 받거나, 국산무기·장비 또는 부품 등을 수출하는 등 일정한 반대급부를 제공받는 조건부 교역을 의미

③ 신기술 트렌드, 미국기업들은 여전히 기술에 목마르다.

- 급변하는 시장 환경에 적응하기 위해 현재 사이버보안 업계는 기업의 사이즈를 불문하고 『통합의 열풍(Consolidation Wave)』 속에 있음.
 - 사이버보안전문 벤처투자기업 Trident Capital의 셀 커닝햄에 따르면, “지난 5년 동안 사이버보안 벤처투자는 무려 235%나 증가하였으나, 향후(’16년 이후)에는 사정이 달라질 것”으로 예측
- 중소기업 대상 벤처투자는 줄어드는 반면, 대기업들은 클라우드 시장 선점을 위한 M&A 경쟁뿐만 아니라, 차별화된 기술력 확보를 위해 기술 구매에 앞 다투어 뛰어 들고 있는 상황임.
- 현실적으로 선진기업과의 기술격차*가 엄존하는 상황에서 우리 중소기업들의 유일한 생존전략은 미래기술과 틈새시장에서의 경쟁력과 전문성을 확보하는 것임.
 - * 미국(100%) 대비기술수준(’13년) : 유럽(88.2), 일본(84.6), 한국(79.9), 중국(72.7) (정보통신기술진흥센터, ’13)
- McAfee, Fortinet, IBM 등 주요 글로벌 기업은 매년 자체 보고서를 발간하여 사이버보안 동향과 주목해야 할 기술에 관한 전망을 제시하고 있는 바, 신기술 수요 파악을 위해 우리기업들의 관심이 요망됨.

[표21] McAfee, Fortinet 선정 차세대 사이버보안 유망 분야

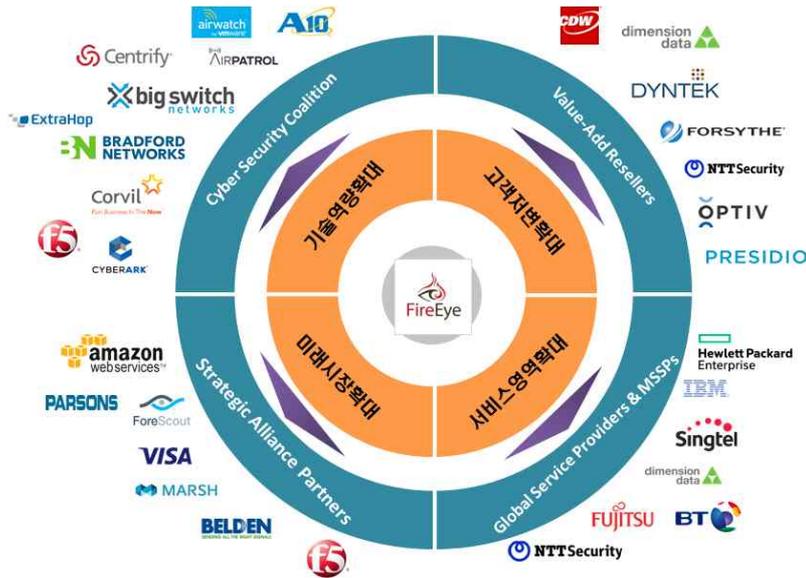
키워드	기 회
웨어러블	스마트 시계, 운동량 추적기, 홀로그램 헤드셋 등 IoT 기기를 사용하는 소비자가 증가함에 따라 IoT 기기의 보안 강화 필요성
클라우드	하이브리드 클라우드 및 가상화에 대한 기업들의 의존성이 커지면서 사이버 범죄에 악용될 것으로 예측
커넥티드카	운행 중인 커넥티드카 대상의 해킹 공격이 현실화 될 것으로 전망됨에 따라 완성차 업체를 중심으로 커넥티드카 보안성 강화 움직임 활발
인공지능	빅데이터를 학습하고 추론하여 사이버보안 관련 방대한 정보량, 복잡성, 비예측성 등을 해결
프라이버시	개인 생체 정보를 활용한 기기, 서비스의 보급이 확대되면서 시장 혼란, 개인 프라이버시 침해 방지를 위한 표준화 및 제도적 보완 시급
모바일	사용자의 문서나 이미지 등을 암호화시키고 돈을 요구하는 악성코드인 랜섬웨어가 스마트폰 이용 확대에 따라 모바일로 확대될 전망
핀테크	금융, 의료 등 비ICT 분야에서도 보안 중요성이 부각됨에 따라 주요 정보 자산을 효율적으로 보호·관리하기 위한 정보보호 시스템 수요증가
인프라	주요 기반시설에 대한 해킹 위협이 증가함에 따라 사전 방지 대책과 함께 신속한 사고처리, 복구 등 체계적인 사후 대응 시스템 구축시급

[자료원] McAfee Labs, Fortinet, 한국인터넷진흥원 등 자료 종합

4] 완전경쟁 시장환경에서 돌파구로서 채널파트너십 전략

- 사실상 완전경쟁구도가 형성된 미국시장에서 기업들은 각자 도생하여 출혈 경쟁하는 길보다 채널파트너십 전략을 통해 시장의 파이를 지속적으로 확대하는 방식을 선택함.
 - 개별 기업이 개인·중소기업·대기업에 이르는 넓은 고객층과 전 산업 분야에 걸친 수요를 아우르는 솔루션을 제공하는 것이 불가능한바 기업들은 시장수요 충족을 위해 다양한 협력 모델을 강구 중
 - 클라우드 기반 서비스형 소프트웨어(SaaS) 확산에 따라 독립 서비스 제공자*가 빠르게 증가하는 속에서 기존 대형유통업체를 통한 마케팅보다 채널 파트너를 활용하는 전략이 빠르게 확산되고 있음.
- * VAR(Value-Added Reseller), 시스템통합자(System Integrator), 서비스제공자(MSSP : Managed Security Service Providers), 시장특화 유통기업 등
- 서비스형 소프트웨어(SaaS) 기업들은 아마존웹서비스(AWS), MS, IBM 등 글로벌 클라우드 플랫폼을 대상으로 애플리케이션을 개발·공급하는 방식으로 활발하게 글로벌 시장에 진출하고 있음.
- 우리기업들도 미국시장 진출을 도모하기 위해서는 글로벌 기업들의 파트너 생태계에 적극 참여하고 적응하는 전략을 활용해야 할 것임.
 - 이를 위해서 기술력과 시장 격차로 인한 글로벌 기업 대비 경쟁력 열위를 어떻게 극복할 수 있는지가 최대 과제임.
- '04년에 설립하여 매출 6억 달러로 성장한 미국의 FireEye는 ① 사이버 보안 기술연합, ② VAR 및 유통업체, ③ 글로벌 서비스제공자 및 MSSP, ④ 전략제휴를 통해 채널파트너 생태계를 구축
 - 사이버보안 기술연합(Cyber Security Coalition)으로 50여 개 기업과 기술제휴, 공동연구개발을 통해 통합솔루션 제공 역량 확보
 - VAR 및 유통기업을 통해 고객저변을 확대하고, 서비스제공자(시스템 통합)와 연대를 통해 서비스 영역 확대, 클라우드 플랫폼 제공사와 함께 미래 첨단기술 시장을 확대하는 전략 구사

[그림14] FireEye의 채널파트너 전략



[자료원] FireEye 홈페이지 참조 재구성

5 사이버보안 전문인력 양산을 통한 해외 인력수출 기회 모색 필요

- 급격히 증가하는 사이버보안 수요에 따라 업계는 전 세계적으로 사이버보안 전문가 수급에 심각한 어려움을 겪고 있음.
 - IT전문 취업전문기업 Experis 조사에 따르면, '19년까지 사이버보안 전문가 수요는 전 세계적으로 6백만 명에 달하나, 150만 명 이상의 인력 부족이 발생할 것으로 전망함.
 - Symantec 前CEO, 마이클 브라운은 인재확보가 기업의 최우선 과제라고 밝히는 등, 미국 내 글로벌 기업들은 앞 다투어 사이버보안 분야 인재 확보 경쟁에 뛰어들고 있는 상황임.
 - * 미국 내 사이버보안 소프트웨어 엔지니어의 평균 연봉은 23만 달러로 업계최고 수준
 - 미국 내 글로벌 기업들은 H-1B 비자(전문 인력을 채용을 위한 비이민 비자) 스폰서를 통해 이스라엘, 인도 등으로부터 IT전문가 영입에 노력 중
- IoT, 클라우드 등 차세대 사이버보안산업 분야 국내 인재들이 해외 기업에 취업할 수 있는 기회를 도모함으로써 글로벌 전문가로 양성하는 방안을 모색할 필요

참고문헌

<해외문헌>

1. Cybersecurity Market Report 2016–2021, ASD Research, Visiongain(2016.6)
2. Risk and Responsibility in a Hyperconnected World, McKinsey & Company(2014.1)
3. Net Losses: Estimating the Global Cost of Cybercrime, McAfee–CSIS(2014.6)
4. Cybersecurity: Time for a Paradigm Shift, Morgan Stanley(2016.6)
5. Lloyd's CEO: Cyber attacks cost companies \$400 billion every year, Fortune(2015.1)
6. 2016 Trustwave Global Security Report, Trustwave(2016.4)
7. 2015 Piper Jaffray CIO Survey, Piper Jaffray(2015.1)
8. The 2015 Cybersecurity Report, CB Insight(2016.7)
9. Global Technology M&A Trends and Analysis, Woodside Capital Partners(2015.7)
10. Cybersecurity Venture Investment in Pervasive Computing and the IoT, Lux Research(2016.4)
11. Tech M&A Outlook 2016, 451 Research(2016.2)
12. Overview of Market Activity in the IT Sector(Q2 2015 Update), William Blair(2015.5)
13. Cybersecurity: The Battle for Vigilance, William Blair(2016.3)
14. U.S. Federal Cybersecurity Market Forecast 2017–2022, Market Research Media(2016.6)
15. An American Strategy for Cyberspace, AEI(2016.6)
16. Federal Cybersecurity Market Drivers and Impacts, Deltek(2013.10)
17. The Global State of Information Security Survey 2016 (<http://www.pwc.com/gsis>)
18. Email Encryption Market, Credence Research(2016.7)
19. 2016 Threats Predictions, McAfee Labs(2016.8)
20. Protecting Your Organization in a Talent–Scarce Market, Experis(2016.3)
21. As technology evolves, new risks drive innovation in cybersecurity, svb Analytics(2015)
22. Bitcoin and the Blockchain, Bloomberg (2016.6.20.)
23. Top Cyber Trends to Watch, PWC(2016)
24. Why Israel Dominates in Cyber Security, Fortune(2015.9.1.)
25. Fact Sheet: Cybersecurity National Action Plan, White House(2016.2.9.)
26. Under Pressure, Cybersecurity Market is Ripe for M&A in 2016, Wall Street Journal(2016.2.29.)
27. Cyber Security, the UK's approach to export, UK Trade & Investment (2012)

<국내문헌>

1. 2015 국내 정보보호산업 실태조사, 한국정보보호산업협회(2015.12)
2. 글로벌정보보호산업동향조사, 한국인터넷진흥원(2013)
3. K–ICT 시큐리티 발전전략, 미래부(2015.4)
4. 사이버보안 경쟁력과 발전방향, 서울여대 박춘식교수
5. 사이버전쟁의 침범, 보안산업의 미래와 과제, KT경제경영연구소(2015) /끝/



작성자

◆ 워싱턴 무역관	이정민 과장
◆ 구미팀	강환국 과장



Global Market Report 16-045

**미국 사이버보안시장 동향과
우리기업 진출을 위한 시사점**

발행인 | 김재홍
발행처 | KOTRA
발행일 | 2016년 9월 1일
주소 | 서울시 서초구 현릉로 13
(06792)
전화 | 02) 1600-7119(대표)
홈페이지 | www.kotra.or.kr

ISBN : 979-11-87617-08-2(95320)

Copyright © 2016 by KOTRA. All rights reserved.
이 책의 저작권은 KOTRA에 있습니다.
저작권법에 의해 한국 내에서 보호를 받는
저작물이므로 무단전재와 무단복제를 금합니다.

Global Market Report

미국 사이버보안시장 동향과 우리기업 진출을 위한 시사점
