nipa 글로벌 ICT 포털

ICT GLOBAL MARKET ANALYSIS

품목별 ICT 시장동향

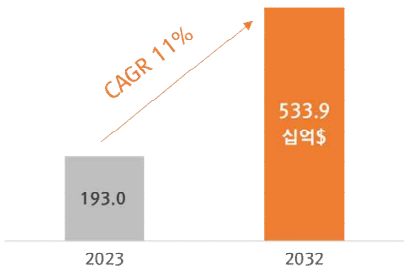
정보보호

CONTENTS

품목별 ICT 시장동향

(2023.07 ~ 2024.06) 정보보호 품목 동향

(2021~2024) 정보보호 발전 현황



Point ① 2024-2032년 정보보호 CAGR 11%

- 글로벌 정보보호 시장은 2023년 1,930억 달러를 기록하였으며, 이후 2032년까지 연평균 성장률 11%를 기록하며 5,339억 달러로 성장할 것으로 전망됨

Point ② 정보보호 발전 현황

- (2021~2022) 사이버보안 관련 논의 증가에도 불구하고, 보안 위협 증가
- (2023~2024) 인공지능을 활용한 사이버보안 솔루션 관심

(2024) 주요 정보보호 기업

Point ① AI 기술 활용해 네트워크 보안 기능 확대

- **Microsoft** : 오픈AI의 대형언어모델을 활용한 'Microsoft Copilot for Security' 출시
- **IBM**: IBM의 대표 보안 제품인 Guardium에 데이터 보안 상태 관리 기능 추가
- **Cisco**: 분산형 AI 네이티브 시스템 'Cisco Hypershield' 출시

(2023.7 ~ 2024.6) 주요 급성장 정보보호 기술

1위	데이터 마스킹
2위	하이브리드 메시 방화벽
3위	생성형 AI
4위	디지털 워터마킹
5위	API

- 데이터 마스킹, 시장 규모 2031년까지 22억 달러에 달할 전망
- 하이브리드 메시 방화벽, 여러 방화벽을 통합하여 관리 가능
- 생성형 AI, 주요 IT기업 보안 솔루션 출시
- 디지털 워터마킹, 콘텐츠 보호 필수 기술로 부상
- API, 보안 API로 디지털 서비스 보안 강화

(2023.7 ~ 2024.6) 주요 급성장 정보보호 수요처

1위	농업
2위	통신
3위	에너지
4위	정부
5위	은행

- 농업, 정밀 농업 및 자동화 증가로 사이버보안 문제 직면
- 통신, 네트워크 사이버보안 강화 활발
- 에너지, 국가별 에너지 사이버 안보 강화 활발
- 정부, 국가별 사이버보안 정책 및 제도 수립
- 은행, AI 및 생체 인식 기술로 정보 보안 강화

CONTENTS

품목별 ICT 시장동향

Ⅰ. 품목 개요

1. 정보보호 발전 현황

(2021~2022) 사이버보안 관련 논의 증가에도 불구하고, 보안 위협 증가

- 온라인 사용자가 급증하면서 각국에서는 개인정보 침해 및 사이버보안을 위한 노력을 지속함. EU는 정보보호 및 보안과 관련한 입법 조치를 추진함. 또한, 국가 간 사이버보안 전략 및 파트너십을 활발하게 추진하여, 호주·인도·미국, 아세안 국가들이 협력을 강화하였음. 2022년에는 우크라이나-러시아 전쟁이 발발하면서 악의적인 사이버 공격이 지속되었으며, 암호화폐 해킹 피해 사례가 증가하는 등 전세계적으로 보안 위협이 증가했음

(2023~2024) 인공지능을 활용한 사이버보안 솔루션 관심

- 2023년부터는 세계적으로 암호화폐 해킹 피해 사례 및 디지털 공급망에 대한 사이버보안 위협이 증가함에 따라 리스크 관리의 중요성이 대두되고 있음. 특히, IoT 기기의 활용이 증가하면서 데이터 보안의 중요성도 증가함. VPN을 대체하는 제로 트러스트의 채택이 확대되고 있으며, AI와 머신러닝을 활용한 위협 탐지 및 대응 솔루션, 전문인력을 통한 사이버보안을 강화하고 있음. 아울러 블록체인 역시 사이버보안을 강화할 수 있는 잠재력을 가진 기술로 인정받고 있음

[표 1] 2021~2024년 정보보호 산업 주요 이슈

구분	주요 이슈
2021	‣ 호주-인도-미국 사이버보안 파트너십 강화
	‣ 아세안, 사이버보안 협력 전략 추진
	‣ EU위원회, 새로운 사이버보안법 입법 추진
2022	‣ 러시아, 우크라이나에 악의적인 사이버 공격 지속
	‣ 암호화폐 해킹 피해 사례 증가
	‣ 디지털 공급망 위험 확대
2023	‣ VPN을 대체하여 제로 트러스트 채택 확대
	‣ AI 및 머신러닝을 사용하는 위협 탐지 및 대응 솔루션 주류화
	‣ 제3자 관리 및 아웃소싱을 통한 사이버보안 강화
2024	‣ 사이버보안 분야에서 AI와 머신러닝에 대한 관심 증가
	‣ 블록체인, 사이버보안 강화할 수 있는 잠재력 인정
	‣ IoT 데이터 보안의 중요성 증가

출처 : 주요 글로벌 ICT 매체 발표 기사 취합

Ⅰ. 품목 개요

2. 정보보호 시장 규모

■ 글로벌 정보보호 시장 규모, 2032년까지 연평균 성장률 11%

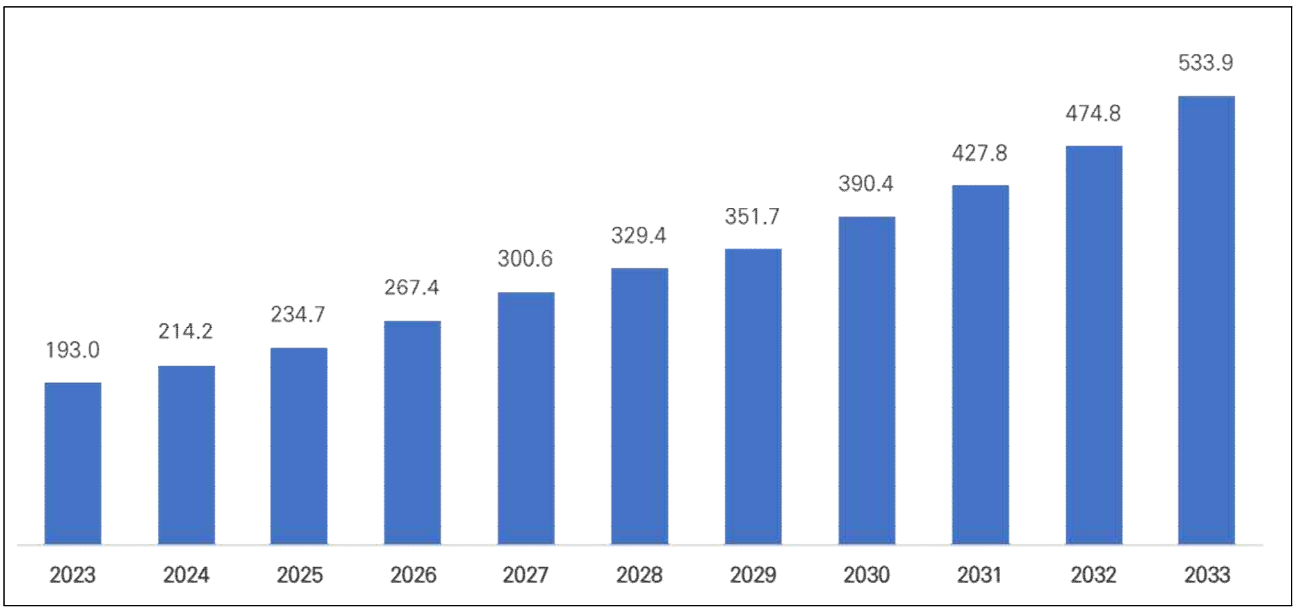
- 시장조사 기업 마켓어스(market.us)에 따르면, 글로벌 정보보호 시장은 2023년 1,930억 달러(약 266조 6,874억 원)를 기록하였으며, 이후 2032년까지 연평균 성장률 11%를 기록하며 5,339억 달러(약 737조 7,430억 원)로 성장할 것으로 전망됨
- 최근 기술과 인터넷에 대한 의존도가 높아짐에 따라 견고한 사이버보안 솔루션에 대한 필요성이 높아지고 있음. 조사에 따르면, 2025년까지 사이버범죄로 인한 지출 비용은 약 10조 5,000억 달러(약 1경 4,509억 원)에 이를 것으로 예상됨

■ 중소기업의 클라우드 기반 보안 솔루션 도입 증가

- 최근 몇 년 동안 표적형 사이버 공격이 증가함에 따라, 사이버보안 시장은 빠르게 성장하였음. 이전까지는 대기업을 중심으로 사이버보안 솔루션 도입이 증가했다면, 최근에는 중소기업에서도 클라우드 기반 사이버보안 솔루션을 도입하는 추세임
- 클라우드 기반 보안 솔루션은 서비스는 효율적인 비용으로 확장 가능하고 유연한 보안 서비스를 제공할 수 있다는 것이 가장 큰 장점임. 또한, 전문 지식 없이도 정교한 보안 기능에 접근할 수 있어 기업의 요구 사항에 충족하는 맞춤형 솔루션을 제공할 수도 있음

[그래프 1] 글로벌 정보보호 시장 규모

(단위 : 십억 달러)



출처 : market.us(market.us)

Ⅰ. 품목 개요

3. 정보보호 선진국가

■ 사이버보안 시장 규모를 기준으로 선진국가 선정

• 2023년 기준 사이버보안 시장 규모를 기준으로 상위 국가를 선진국가로 선정함. 시장조사 기관 스태티스타(Statista)의 조사에 따르면, 미국이 729억 2,000만 달러(약 100조 7,609억 원)로 1위를 기록하였으며, 중국과 영국이 그 뒤를 이었음

■ 미국 정부, DDoS 공격 등에 대응하기 위해 사이버보안 솔루션 적극 활용

• 미국의 정부 부문 정보보호 시장은 빠르게 성장하고 있음. 시장조사 기관 테크나비오(Tech Navio)의 조사에 따르면, 2022년부터 2027년까지 연평균 성장률 14.59%로 108억 2,000만 달러(약 14조 9,511억 원)까지 성장할 전망임. 특히, 미국 정부의 BYOB(Bring Your Own Device) 정책이 보안 우려를 불러일으키면서 사이버보안 솔루션에 대한 수요가 증가하고 있음

■ 중국, 정부 차원의 사이버보안 산업 지원 증가

• 중국 정부는 최근 개인정보 보호에 대한 요구가 증가하면서 데이터 보안에 대한 우려가 확대됨에 따라 사이버보안 부문 지원을 늘리는 정책을 시행하고 있음. 중국 공업정보화부(MIIT)는 사이버보안 정책의 일환으로, 2023년까지 IT 장비 업그레이드 예산의 10%를 사이버보안 부문에 할당하도록 규정했음

■ 영국, 글로벌 사이버 강국으로서의 입지를 공고히 하기 위한 사이버보안 전략 시행

• 영국은 최근 사이버 공격의 증가와 디지털화, 확장 가능한 IT 인프라, 클라우드 우선 전략의 시행 등으로 사이버보안 부문 시장 수요가 증가하고 있음. 정부는 이를 충족하기 위해 사이버 위협으로부터 보호하고, 글로벌 사이버 강국 입지를 공고히 하기 위한 새로운 국가 사이버보안 전략을 시작함. 또한, 상호 사이버 회복력을 강화하기 위해 인도와 협력한다고 발표했음

[표 2] 2023년 기준 사이버보안 시장 규모 상위 10개국 (단위 : 백만 달러)

순위	국가명	2023	2024	2025	2026	2027	2028	2029
1	미국	72,920	81,370	88,250	95,760	102,400	109,500	116,200
2	중국	13,040	14,750	16,710	18,820	20,680	22,710	24,590
3	영국	9,929	10,990	12,090	13,370	14,460	15,660	16,800
4	일본	9,027	9,374	10,270	11,170	11,860	12,660	13,250
5	독일	6,890	7,543	8,209	8,885	9,437	10,000	10,510
6	프랑스	5,281	5,785	6,229	6,718	7,129	7,563	7,948
7	호주	3,712	4,043	4,388	4,756	5,069	5,422	5,764
8	캐나다	3,442	3,834	4,228	4,626	4,968	5,335	5,682
9	러시아	3,242	3,551	3,783	4,007	4,206	4,415	4,599
10	한국	3,109	3,397	3,720	4,059	4,349	4,658	4,943

출처 : Statista(statista.com)

Ⅰ. 품목 개요

4. 정보보호 신흥국가

NCSI 점수보다 디지털 발전 수준 점수가 높은 국가를 신흥 국가로 선정

- 국가사이버보안지수(NCSI) 점수 50위 이내 국가 중, NCSI 점수보다 디지털 발전 수준 점수가 높은 국가(선진국가 제외)가 사이버보안 발전 잠재력이 높다고 판단하여 신흥 국가로 선정함

네덜란드 헤이그, 사이버보안 허브로 자리매김

- 네덜란드는 암스테르담에 유럽의 데이터센터 다수와 인터넷 거래소가 위치하고 있음. 이에 따라 사이버 범죄에 대한 우려가 증가하고 있는 실정임. 한편 헤이그는 사이버보안 허브로 자리 잡고 있는데, 유로폴의 사이버범죄 센터(EC3)와 NATO의 정보기관(NCI)가 위치하고 있음. 또한, 네덜란드 정부는 글로벌 사이버 전문성 포럼을 설립하며 그 입지를 공고히 하고 있음

뉴질랜드, 사이버보안 강화 위한 정부 기관 설립

- 뉴질랜드 정부는 2023년 7월, 사이버보안 준비 및 대응 강화를 위해 뉴질랜드 컴퓨터 비상 대응팀(CERT NZ)를 국가 사이버보안센터(NCSC)에 신설함. 정부는 2018년부터 사이버보안 역량 개선을 위해 9,400만 달러(약 1,299억 800만 원)를 투자해 왔음

사우디아라비아, 사이버보안 위한 다양한 정부 정책 시행

- 사우디아라비아는 국가 사이버보안기관(NCA)를 필두로, 다양한 정부 정책을 시행하고 있음. 2023년에는 새롭게 개정된 '개인정보보호법 2023'을 발표하였으며, 데이터 사이버보안 통제와 운영 기술 사이버보안 통제, 사이버보안 툴킷 2.0, 관련 가이드라인 등 여러 규정을 발표함. 또한, 유능한 사이버 인력을 구축하는 데 많은 노력을 기울이면서 ITU의 글로벌 사이버보안 지수에서 미국에 이어 2위를 차지하기도 했음

[표 3] 2023년 기준 사이버보안 시장 규모 상위 10개국 (단위 : 백만 달러)

순번	국가명	국가 사이버보안 지수(A)	디지털 발전 수준(B)	차이(A-B)
1	네덜란드	81.67	84.94	-3.27
2	호주	87.50	82.21	5.29
3	뉴질랜드	55.00	80.14	-25.14
4	에스토니아	85.83	80.02	5.81
5	캐나다	81.67	78.55	3.12
6	아일랜드	77.50	76.59	0.91
7	벨기에	77.50	76.59	0.91
8	리투아니아	76.67	73.93	2.74
9	키프로스	76.67	72.52	4.15
10	폴란드	92.50	72.29	20.21
11	체코	98.33	72.04	26.29
12	라트비아	79.17	71.88	7.29
13	사우디아라비아	59.17	70.77	-11.60

출처 : e-Governance Academy Foundation(ncsi.ega.ee)

CONTENTS

품목별 ICT 시장동향

Ⅱ. 선도 기업

1. 정보보호 선도 기업

■ AI 기술 활용해 네트워크 보안 기능 확대

- Microsoft : 'Microsoft Copilot for Security' 출시
  - 마이크로소프트(MS)가 보유한 78조 개 이상의 보안 신호를 포함한 대규모 데이터와 위협 인텔리전스를 활용해 정보를 처리하고, 오픈AI의 대형언어모델을 활용해 인사이트를 제공함
- IBM : Guardium에 데이터 보안 상태 관리 기능 추가
  - 대표 보안 제품인 Guardium에 IBM Security Guardium Insights SaaS DSPM(데이터 보안 상태 관리) 기능을 추가함
- Cisco : 분산형 AI 네이티브 시스템 'Cisco Hypershield' 출시
  - 네트워크에서 실행되는 애플리케이션의 소프트웨어 구성 요소와 서버, 퍼블릭 및 프라이빗 클라우드 배포에 보안을 적용하는 분산형 AI 네이티브 시스템 'Cisco Hypershield'를 출시함

[표 4] 글로벌 정보보호 선도 기업

순위	기업명	국적	연간수익	사업 분야
①	Microsoft	미국	$227.6B	엔드포인트 보안, 클라우드 보안 등
②	IBM	미국	$61.9B	통합 엔드포인트 관리, 암호화 등
③	Cisco	미국	$57.2B	네트워크 보안 제품 개발
④	Broadcom	미국	$35.8B	CASB, DLP, SASE, SD-WAN, 제로 트러스트 등
⑤	Fortinet	미국	$5.3B	방화벽, VPN 등
⑥	CrowdStrike	미국	$3.4B	엔드포인트 보호 제품 개발
⑦	Check Point	이스라엘	$2.4B	방화벽, 게이트웨이, 암호화 등
⑧	Okta	미국	$2.3B	ID 및 접속 관리, 제로 트러스트
⑨	Zscaler	미국	$1.9B	클라우드 보안 및 에지 보안
⑩	Trend Micro	일본	$1.3B	바이러스 백신, 디스크 암호화 등

출처 : eSecurity Planet(esecurityplanet.com)

2. 선도 기업 분석

① Microsoft

■ Microsoft : 엔드포인트 보안, 클라우드 보안 서비스 제공

• 생성형 AI 탑재한 'Microsoft Copilot for Security' 출시

- 2024년 4월 1일, 보다 빠르게 보안 업무를 처리하고 조직이 외부 위협을 신속하게 감지하고 대응할 수 있게 하는 'Microsoft Copilot for Security'를 출시함
- 마이크로소프트(MS)가 보유한 78조 개 이상의 보안 신호를 포함한 대규모 데이터와 위협 인텔리전스를 활용해 정보를 처리하고, 오픈AI의 대형언어모델을 활용해 인사이트를 제공함
- 사용량 기반 가격 책정 모델로, 하나의 보안 컴퓨팅 유닛으로 시작해 필요에 따라 확장할 수 있음

[표 5] Microsoft 기업 분석

구분		내용		
기업 정보	기업명 (국적)	Microsoft (미국) / microsoft.com		
	연간 수익	2,276억 달러	설립년도	1975
	기업 유형	엔드포인트 보안, 클라우드 보안 등		
발전 단계		▸ 애저 네트워크 보안에 생성형 AI 도입 - 코파일럿 환경에서 애저 WAF와 애저 방화벽 통합하여 생성형 AI 기능 도입을 위한 기반 구축 - MS의 보안 전문성과 생성형 AI를 결합하여 보안과 개인정보 보호, 규정 분수를 중심으로 구축된 솔루션의 보안성을 더욱 높일 수 있을 것으로 기대 ▸ Microsoft Copilot for Security 출시 - 2024년 4월 1일, 보다 빠르게 보안 업무를 처리할 수 있는 Microsoft Copilot for Security를 출시 - 사용량에 따라 요금을 지불하는 것이 특징으로, 산업별로 필요한 서비스를 필요한 만큼 이용할 수 있는 것이 장점		
개발 기술		▸ 대표 서비스: Microsoft Copilot for Security - 생성형 AI 보안 솔루션 - 조직이 외부의 위협을 신속하게 감지하고 대응할 수 있도록 지원 - MS가 보유한 78조 개 이상의 보안 신호를 포함한 대규모 데이터와 위협 인텔리전스를 활용해 정보 처리 - 오픈AI의 대형언어모델을 활용해 인사이트 제공		

출처 : Microsoft (microsoft.com)

2. 선도 기업 분석

② IBM

■ IBM : 통합 엔드포인트 관리, 암호화 등

• 보안 운영 및 위협 보호 부문에서 마이크로소프트와 협력

- 고객이 보안 운영을 간소화하고, 하이브리드 클라우드 ID를 관리하고 보호할 수 있도록 지원하기 위해 강화된 사이버보안 부문의 협력을 발표함

• Guardium 제품군에 데이터 보안 상태 관리 기능 추가

- IBM의 대표 보안 제품인 Guardium에 IBM Security Guardium Insights SaaS DSPM (데이터 보안 상태 관리) 기능을 추가함. 이를 통해 분산 클라우드 환경 모니터링의 사각지대를 줄이고, 클라우드 데이터 흐름을 이해하며 보안 취약성 발견 기능을 확대한다는 계획임

[표 6] IBM 기업 분석

구분		내용		
기업 정보	기업명 (국적)	IBM(미국) / ibm.com		
	연간 수익	619억 달러	설립년도	1911
	기업 유형	통합 엔드포인트 관리, 암호화 등		
발전 단계		▸ 보안 운영 및 위협 보호 부문에서 마이크로소프트와 협력 - 고객이 보안 운영을 간소화하고, 하이브리드 클라우드 ID를 관리하고 보호할 수 있도록 지원하기 위해 강화된 사이버보안 협업 발표 - IBM의 사이버보안 서비스와 MS의 보안 기술 포트폴리오를 결합하여 클라우드를 활용하고, 데이터를 보호하고, 비즈니스 성장을 추진하는 데 필요한 도구와 전문 지식 제공 ▸ 2023년 3월, AI 기반 위협 탐지 및 대응 서비스 발표 - AI 기술을 탑재하여 24시간 보안 모니터링, 조사 및 자동 수정 등의 서비스 제공 - 하이브리드 클라우드 환경 전반에서 활용 가능		
개발 기술		▸ 대표 서비스 1) IBM Guardium - 하이브리드 클라우드 환경에서 중요한 데이터를 찾고, 암호화하고, 모니터링할 수 있는 서비스로, 데이터가 클라우드와 데이터베이스, 애플리케이션 간 이동할 때 가시성과 데이터 보호 기능을 제공 2) IBM Verify - 실시간 위험 기반 인증을 통해 멀티클라우드 ID와 네트워크 접근을 보호 - 기존 도구로 효과적인 ID 패브릭을 구축하여 최신 인증 매커니즘을 기존 애플리케이션으로 확장		

출처 : IBM(ibm.com)

2. 선도 기업 분석

③ Cisco

■ Cisco : 네트워크 보안 제품 개발

• 2024년 4월, 분산형 AI 네이티브 시스템 'Cisco Hypershield' 출시

- 네트워크에서 실행되는 애플리케이션의 소프트웨어 구성 요소와 서버, 퍼블릭 및 프라이빗 클라우드 배포에 보안을 적용하는 분산형 AI 네이티브 시스템을 출시함
- 설계 단계부터 AI 기술이 고려돼 사람의 힘으로 달성하기 어려운 높은 수준의 보안 시스템을 구축할 수 있도록 지원함

[표 7] Cisco 기업 분석

구분		내용		
기업 정보	기업명 (국적)	Cisco (미국) / cisco.com		
	수익('23)	572억 달러	설립년도	1984
	기업 유형	네트워크 보안 제품 개발		
발전 단계		▸ 2024년 4월, 분산형 AI 네이티브 시스템 'Cisco Hypershield' 출시 – 네트워크에서 실행되는 애플리케이션의 소프트웨어 구성 요소와 서버, 퍼블릭 및 프라이빗 클라우드 배포에 보안을 적용하는 분산형 AI 네이티브 시스템 – 설계 단계부터 AI 기술이 고려돼 사람의 힘으로 달성하기 어려운 높은 수준의 보안 시스템을 구축할 수 있도록 지원 – 하이퍼스케일 퍼블릭 클라우드를 위해 개발된 기술이 사용됐으며, 모든 IT 팀이 조직 규모에 따른 제약 없이 구축 가능 ▸ 2022년 개방형 플랫폼 '시스코 시큐리티 클라우드' 공개 – 업계에서 가장 개방된 플랫폼으로, 특정 업체의 솔루션 종속성 탈피 – 언제 어디서나 안전하게 디바이스를 애플리케이션과 연결할 수 있는 통합 경험 제공		
개발 기술		▸ 대표 서비스 : Cisco Security Cloud – 클라우드 기반의 글로벌 통합 보안 및 네트워킹 서비스 – 특정 퍼블릭 클라우드 업체의 서비스나 솔루션의 종속성을 탈피하고, IT 생태계 전반의 무결성 보존 – 통합 관리를 통해 위협 예방, 탐지, 대응 및 복구 기능 제공 – 하위 서비스 'Cisco XDR' 출시하여 네트워크와 엔드포인트 전반에 걸쳐 딥 텔레메트리 기능 제공 및 가시성 향상		

출처 : Cisco(cisco.com)

CONTENTS

품목별 ICT 시장동향

Ⅲ. 유망 기술

1. 유망 기술 선정

2023년 07월 ~ 2024년 06월 주요 급성장 정보보호 기술 키워드

- 데이터 마스킹(Data Masking): 시장 규모 2031년까지 22억 달러에 달할 전망
- 하이브리드 메시 방화벽(Hybrid Mesh Firewall): 여러 방화벽을 통합하여 관리 가능
- 생성형 AI(Generative AI): 주요 IT 기업 보안 솔루션 출시
- 디지털 워터마킹(Digital Watermarking): 콘텐츠 보호 필수 기술로 부상
- API: 보안 API로 디지털 서비스 보안 강화

[표 8] 2023년 7월 ~ 2024년 6월 급성장 정보보호 유망 기술

순위	키워드		발생률1)	성장률2)
	국문	영문		
①	데이터 마스킹	Data Masking	0.02%	400.00%
②	하이브리드 메시 방화벽	Hybrid Mesh Firewall	0.20%	126.67%
③	생성형 AI	Generative AI	0.14%	100.00%
④	디지털 워터마킹	Digital Watermarking	0.24%	36.00%
⑤	API	API	0.63%	18.57%
⑥	확장탐지 및 대응	XDR	1.05%	17.95%
⑦	바이러스 백신 소프트웨어	Antivirus Software	6.79%	15.76%
⑧	지문인식	Fingerprint	0.98%	14.41%
⑨	접근 제어	Access Control	0.48%	3.45%
⑩	가상사설망	VPN	3.46%	-2.58%

출처 : 2023년 7월 ~ 2024년 6월 IT 뉴스매체 분석 결과

1) 발생률 : 2023년 7월 ~ 2024년 6월 정보보호 기술 키워드 전체 발생량 24,394건 중 해당 키워드의 발생 비율을 뜻함
2) 성장률 : (후반 6개월 키워드 발생량) - (전반 6개월 키워드 발생량) / (전반 6개월 키워드 발생량)

2. 급성장 기술 키워드

① 데이터 마스킹(Data Masking)

(*) 데이터 마스킹(Data Masking)이란?
소프트웨어나 권한이 있는 직원이 계속 사용할 수 있는 상태에서 권한이 없는 침입자에게는 가치가 없거나 거의 없도록 민감한 데이터를 수정하는 프로세스임

■ 데이터 마스킹 시장, 2031년까지 2조 9,000억 원에 달할 전망

- KBV 리서치(KBV Research)의 신규 보고서에 따르면, 글로벌 데이터 마스킹 시장은 2031년까지 연간 복합성장률(CAGR) 11.8%로 성장하여 22억 달러(약 2조 9,000억 원)에 이를 것으로 전망됨. 특히 온프레미스 부문은 2023년 배포 모드별 글로벌 데이터 마스킹 시장을 주도하고 있으며 정부, 의료, 금융 등 규제 산업에서 엄격한 데이터 주권 요구사항에 의해 시장을 선도하고 있음
- 민감한 데이터를 실시간으로 보호하는 동적 데이터 마스킹도 주목받고 있으며, 2031년에는 시장 가치가 14억 달러(약 1조 8,000억 원)에 이를 것으로 예상됨. 특히, 의료 부문은 13.5%의 CAGR로 성장할 것으로 전망되며 데이터 마스킹으로 사이버 범죄로부터 민감한 환자 정보를 보호할 수 있음

■ 데이터 마스킹, 데이터 보안의 필수 기술

- 민감한 정보를 침해 및 사이버 공격으로부터 보호해야 할 필요성이 높아짐. 데이터 마스킹은 데이터 보안을 위한 필수 기술로 자리 잡았으며, 다양한 이점을 제공함
  - 데이터 개인 정보 보호 및 규정 준수 가능 : GDPR(General Data Protection Regulation) 및 HIPAA(Health Insurance Portability and Accountability Act)와 같은 다양한 데이터 보호 규정 준수에 중요한 역할을 하며 데이터 프라이버시를 강화하여 위험 없이 데이터 세트를 공유할 수 있음
  - 데이터 침해 위험 완화 : 도난당한 데이터를 악용할 수 없도록 만들어 데이터 유출 위험을 완화할 수 있음
  - 안전하고 실제 같은 테스트 환경 조성 : 개발자가 민감한 정보를 노출하지 않는 데이터를 사용하도록 하여 안전한 테스트 환경을 조성할 수 있음
  - 데이터 보존 유틸리티 : 분석 및 의사결정을 위한 데이터를 손상시키지 않으며 정확한 결과와 의미있는 통찰력 제공 가능
  - 직원 데이터 보호 : 조직 내 직원의 민감한 데이터를 보호할 수 있음
  - 클라우드 마이그레이션 지원 가능 : 데이터를 클라우드로 마이그레이션하기 전 민감한 정보를 보호할 수 있도록 함

2. 급성장 기술 키워드

② 하이브리드 메시 방화벽(Hybrid Mesh Firewall)

(*) 하이브리드 메시 방화벽(Hybrid Mesh Firewall)이란?
모든 방화벽을 서로 연결하여 IT 인프라 전체에 방화벽 기능을 배포할 수 있도록 지원하여 통합된 방화벽 보안을 구축할 수 있음

■ 하이브리드 메시 방화벽 플랫폼 이점

- 하이브리드 메시 방화벽이 다양한 네트워크 환경에서 여러 유형의 방화벽을 관리하는 복잡성을 해결하는 솔루션으로 부상하고 있음. 대표 제공업체로 포티넷(Fortinet), 팔로알토(Palo Alto), 시스코(Cisco)가 있음
- 하이브리드 메시 방화벽은 데이터센터, 클라우드 서비스에 배포된 방화벽을 중앙에서 관리할 수 있는 통합 인터페이스를 제공하여 배포, 모니터링을 용이하게 함

- 복잡성 감소 : 기업 내 다양한 방화벽 관리를 간소화함. 방화벽의 복잡성은 보안 성능을 저하할 수 있음
- 가시성 향상 : 모든 유형, 기능, 위치에 관계없이 방화벽을 한눈에 볼 수 있는 단일 대시보드를 제공하여 관리 능력을 향상시키고 문제를 조기에 감지하고 해결할 수 있음
- 일관된 보안 정책 적용 가능 : 모든 환경에서 보안 정책을 일관되게 적용할 수 있도록 하여 데이터 보호 및 개인정보 보호 규정 준수에 중요한 역할을 함
- 제로 트러스트 보안 모델 구현 : 제로 트러스트 보안 접근 방식을 지원하여 기업이 관리하는 모든 방화벽에 엄격한 보안 조치를 적용할 수 있음
- AI 및 기계 학습 통합 : AI와 기계 학습을 활용해 효율적이고 신속하여 위협을 감지함. 방화벽 배포의 보안 능력을 자동화하여 강화할 수 있음

■ 다양한 차세대 방화벽 솔루션 출시

- 대표 방화벽 솔루션 제공업체인 포티넷(Fortinet)은 초대규모 및 중견 데이터센터를 위한 새로운 차세대 방화벽(NGFW)을 선보임. 이는 다양한 규모의 데이터센터에 맞춘 보안 솔루션을 제공하며 하이브리드 메시 방화벽을 위한 통합 관리 기능을 갖추고 있음
- 소닉월(SonicWall)은 현대 하이브리드 워크포스와 멀티 클라우드 환경을 보호하기 위해 기존 방화벽 기능과 고급 보안 기능을 결합한 하이브리드 메시 방화벽 플랫폼을 공개함. 이 플랫폼은 유연한 배포 옵션, 통합 클라우드 기반 관리, 고급 보안 서비스를 제공하여 다양한 사이버 위협으로부터 조직을 보호하고 보안 인프라를 효율적이고 종합적으로 관리할 수 있도록 도움

2. 급성장 기술 키워드

③ 생성형 AI(Generative AI)

(*) 생성형 AI(Generative AI)란?
텍스트, 오디오, 이미지 등의 기존 콘텐츠를 활용하여 새로운 콘텐츠를 만들어 내는 AI 기술임

■ 생성형 AI로 사이버보안 강화

- 생성형 AI가 적응형 위협 탐지, 예측 분석, 멀웨어 생성 및 분석 등을 통해 사이버보안에 혁신을 일으키고 있음. 생성형 AI는 과거 데이터를 분석하여 이상 패턴을 감지해 새로운 위협과 진화하는 위협을 실시간으로 인식할 수 있음
- 생성형 AI는 합성 생체 데이터를 생성하여 생체 인식 보안 시스템을 강화할 수 있음. 생체 인증의 정확성을 개선하여 안전한 신원 확인을 할 수 있도록 함. 또한, 보안 패치를 자동으로 생성해 소프트웨어 취약점을 식별하고 맞춤형 패치를 생성해 신속하고 효과적인 대응을 보장함. 다양한 사이버 위협과 공격 시나리오를 시뮬레이션하여 사이버보안 전문가와 대응팀을 훈련시키고, 실제 사이버 위협에 대비할 수 있음

■ MS, 사이버보안 전문가를 위한 생성형 AI 챗봇 출시

- 마이크로소프트(Microsoft)가 사이버보안 전문가를 지원하기 위해 설계된 생성형 AI 챗봇 '코파일럿 포 시큐리티(Copilot for Security)'를 출시함. 코파일럿 포 시큐리티는 다른 구독 모델과 달리 종량제 요금제로 운영되며, 시간당 4달러(약 5,300원)가 부과됨
- 이 챗봇은 협업을 위한 핀보드, 보고를 위한 이벤트 요약, 코드 및 파일 분석 기능 등을 포함하고 있음. 기업은 초기 비용 없이 AI 기반 사이버보안 능력을 강화할 수 있음

■ 구글 클라우드, 위협 감지 강화 위한 보안 AI 워크벤치 출시

- 구글 클라우드가 위협 탐지 및 분석을 개선하기 위해 고안된 AI 기반 사이버보안 툴 제품군인 '보안 AI 워크벤치(Security AI Workbench)'를 선보임. 이 제품군은 보안 사용 사례에 맞게 조정된 대형 언어 모델인 'Sec-PaLM'을 기반으로 함
- 보안 AI 워크벤치는 생성형 AI 모델을 활용해 잠재적인 악성 스크립트를 분석하고 사용자에게 침해를 경고하여 더 빠르고 정확한 위협 탐지를 제공함. 구글 클라우드의 Vertex AI 인프라에 구축되어 있으며 기업의 데이터 보호 및 규정 준수를 지원함

2. 급성장 기술 키워드

④ 디지털 워터마킹(Digital Watermarking)

(*) 디지털 워터마킹(Digital Watermarking)란?
사진이나 동영상 같은 각종 디지털 데이터에 저작권 정보와 같은 정보를 삽입하여 관리하는 기술

■ 디지털 워터마킹으로 민감한 데이터 보호

- 빅테크 기업들의 관심 속에 디지털 워터마킹이 정보보호에 필수적인 기술로 부상함. 인터넷을 통해 디지털 미디어를 빠르게 공유하고 복제가 가능하기에 지속적인 콘텐츠 보호 메커니즘을 구축하는 것이 필수적임. 디지털 워터마킹은 콘텐츠의 품질을 손상하지 않으면서 지속적으로 저작권 보호를 할 수 있고, 승인되지 않은 유통 소스를 식별할 수 있음. 또한, 타임스탬프 및 GPS 위치와 같은 포렌식 정보를 인코딩할 수 있음. 디지털 워터마킹은 디지털 권리 관리, 불법 복제 억제, 민감한 문서의 무결성 보장을 위한 다목적이고 효과적인 도구임

■ 에코마크, 내부 위협 보호 위한 AI 구동 워터마킹 출시

- 정보보호 소프트웨어 전문 기업 에코마크(EchoMark)가 개인정보을 보호하기 위해 설계된 AI 기발 워터마킹 솔루션을 발표함. 이 소프트웨어는 주요 이메일 시스템과 통합되어 이메일과 문서에 포렌식 워터마킹을 자동으로 삽입하여 위협을 즉시 식별할 수 있음. 최근 2년간 데이터 침해 및 유출이 44% 증가함에 따라, 워터마킹 기술로 해결하고 있음
- AI가 탑재된 이 기술은 문서가 변경되어도 위협을 식별하는 데 100%에 가까운 정확도를 보이며, 기업이 유출된 정보를 출처로 빠르게 추적할 수 있도록 함. 에코마크의 솔루션은 기존 워크플로우를 방해하지 않고 5분 이내에 배치할 수 있으며, 다양한 분야에서 증가하는 내부 위협 문제를 신속하게 해결함

■ 디지마크와 데이터트레일, 디지털 콘텐츠 보호 강화 위한 파트너십 체결

- 디지마크 코퍼레이션(Digimarc Corporation)과 데이터트레일즈(DataTrails Inc.)가 업계 최초로 완전 통합 콘텐츠 보호 솔루션을 선보이기 위한 파트너십을 발표함. 솔루션은 디지털 콘텐츠의 진위성을 보장하며, 생성형 AI의 콘텐츠 메타데이터 제거 문제를 해결함
- 해당 솔루션은 디지마크의 디지털 워터마킹 기술과 데이터트레일즈의 암호화 증명을 활용해 콘텐츠 인증을 위한 다층 툴셋을 제공함. 이를 통해 가짜 데이터와 잘못된 정보로부터 콘텐츠 제작자, 기업, 소비자를 보호할 수 있음

2. 급성장 기술 키워드

⑤ API

(*) API(Application Programming Interface)란?
응용 프로그램 프로그래밍 인터페이스로 불리며, 컴퓨터나 소프트웨어를 서로 연결하여 서비스를 제공하는 기술

■ 보안 API로 디지털 보안 강화 시 이점

• API는 개발자가 온라인 서비스에서 데이터를 통합, 개선 및 공유하는 방식에 혁신을 가져옴. 사이버보안 분야에서 API는 아래와 같은 이점을 지님

- 악성 소프트웨어 및 바이러스 감지 : API는 파일과 코드에서 악성 콘텐츠를 스캔하여 감염이 감지되면 사용자에게 신속히 경고함
- 웹사이트 평판 확인 : 보안 API는 피싱 도메인과 위험한 웹사이트를 감지함
- 공격 표면 분석 : DNS 기록, IP 주소, 도메인 이름을 감사하여 도메인 하이재킹을 방지하고, 오래된 DNS 기록을 찾을 수 있음
- 사기 조사 : 보안 API로 사기 행위을 조사하고 가해자를 추적할 수 있음
- 브랜드 모니터링 : 브랜드 이름이나 상표를 불법 사용을 감지함
- 저작권 침해 조사 : 저작권이 있는 자료를 불법으로 사용하는 웹사이트를 찾을 수 있음

[표 9] 보안 API 종류

API명	주요 특징
Google Safe Browsing API	• 사용자를 피싱 도메인, 사기성 사이트, 멀웨어 감염 웹 페이지로부터 보호할 수 있음 • 조회 API, 업데이트 API, 캐싱, 압축, 로컬 데이터베이스, 위협 유형에 대한 메타데이터와 같은 기능 제공
PhishTank API	• 피싱 캠페인으로부터 보호하며, 다운로드 가능한 데이터베이스와 실시간 API 요청을 제공 • HTTP POST 요청을 통한 URL 상태 확인, DNS 기반 기술과 결합 가능
VirusTotal API	• 파일 및 URL 스캔, 스캔 결과 확인가능한 온라인 바이러스/멀웨어 스캐너임 • 공용 API (제한된 요청, 비상업적 사용), 개인 API (프리미엄 접근) 기능 제공, VirusTotal 커뮤니티 계정과 API 키 필요함
Quttera API	• 웹사이트가 바이러스나 멀웨어에 감염되었는지 확인가능한 온라인 멀웨어 스캐너임 • 사전 모니터링, Quttera 데이터베이스에서 URL 확인, 심층 스캔 결과, 멀티스레딩, REST API (JSON, XML, YAML) 등 기능 제공

출처 : SecurityTrails(securitytrails.com)

CONTENTS

품목별 ICT 시장동향

Ⅳ. 유망 수요처

1. 유망 수요처 선정

2023년 07월 ~ 2024년 06월, 주요 급성장 정보보호 수요처 키워드

- 농업(Agriculture): 정밀 농업 및 자동화 증가로 사이버보안 문제 직면
- 통신(Telecommunication): 네트워크 사이버보안 강화 활발
- 에너지(Energy): 국가별 에너지 사이버 안보 강화 활발
- 정부(Government): 국가별 사이버보안 정책 및 제도 수립
- 은행(Banking): AI 및 생체 인식 기술로 정보 보안 강화

[표 10] 2023년 7월~2024년 6월 급성장 정보보호 유망 수요처

순위	키워드		발생률[3]	성장률[4]
	국문	영문		
①	농업	Agriculture	0.74%	375.76%
②	통신	Telecommunication	1.00%	186.36%
③	에너지	Energy	3.92%	77.62%
④	정부	Government	11.83%	48.24%
⑤	은행	Banking	2.15%	36.05%
⑥	국방	Defense	3.38%	34.32%
⑦	미디어	Media	15.69%	24.83%
⑧	공공	Public	14.92%	24.22%
⑨	엔터테인먼트	Entertainment	1.69%	11.71%
⑩	소매	Retail	3.99%	2.57%

출처 : 2023년 7월 ~ 2024년 6월, IT 뉴스매체 분석 결과

3) 발생률 : 2023년 7월~2024년 6월 정보보호 수요처 키워드 전체 발생량 25,616건 중 해당 키워드의 발생 비율을 뜻함
4) 성장률 : (후반 6개월 키워드 발생량) - (전반 6개월 키워드 발생량) / (전반 6개월 키워드 발생량)

2. 급성장 수요처 키워드

① 농업(Agriculture)

■ 농업 분야의 사이버보안 필요성

- 농업이 정밀 농업 및 자동화 농업의 발전으로 디지털 전환을 겪으면서 새로운 사이버보안 문제에 직면하고 있음. AI, 로봇공학, 스마트 센서의 통합은 효율성과 생산성을 높였지만, 동시에 랜섬웨어, 피싱, 데이터 조작, 공급망 중단, 기밀 정보 도난 등 사이버 위협 취약성이 드러남
- 농업에 대한 사이버 공격은 세계 식량 안보 위협, 재정적 손실, 공급망 중단, 식품 안전 저하 등 심각한 결과를 초래할 수 있음. 이러한 문제를 해결하기 위해서는 사전 예방적 사이버보안 교육, 자동화 시스템을 위한 포괄적인 보안 전략, 농촌 지역의 인프라 개선, 현대 농업 시스템의 상호 연결된 특성에 대한 인식이 필요함. 농업 분야의 사이버보안을 강화하는 것은 전 세계적으로 탄력적이고 안전한 식량 공급망을 보장하는 데 필수적임

■ 스마트 농업을 위한 사이버보안 전략

- 농업 부문이 적극적으로 디지털 기술을 통합함에 따라 증가하는 사이버보안 위협에 직면해 있음. 따라서, 농업 기업은 다양한 사이버보안 전략을 채택해야 함
  - 정기적인 위험 평가를 시행하여 위험 수준에 따라 보안의 우선순위를 정해야 함
  - 직원들에게 정보 보안 우수 사례를 교육하고, 농장 내 IoT 장치 보안 펌웨어 도입
  - 악성 소프트웨어 및 무단 침입의 확산을 제어하기 위해 네트워크를 세그먼트로 분할
  - 종합적인 사고 대응 계획을 개발하여 무단 침입 시 신속하게 해결함
  - 블록체인 기술로 투명성과 추적 가능성을 보장하여 공급망 보안을 강화함

■ 식품 및 농업 부문 사이버보안 강화 법안 도입

- 미국 양당 합동 그룹이 식량 및 농업 산업의 사이버보안 강화를 위한 '농장 및 식품 사이버보안법(Farm and Food Cybersecurity Act)'을 제출함. 이 법안은 브래드 핀스타드(Brad Finstad) 하원의원, 엘리사 슬로트킨(Elissa Slotkin) 하원의원 등 양당이 공동 제안함. 이 법안은 2021년 랜섬웨어 공격으로 인해 육류 공급이 중단된 사건을 계기로 비상 상황을 처리하는 연례 훈련과 정기적인 위협 평가를 통해 취약점을 식별하는 것을 목표로 함
- 법안에 따르면 농업 장관은 2년마다 사이버보안 위협을 조사하고 그 결과를 의회에 보고해야 함. 또한, 다른 기관과 매년 교차 훈련을 실시하여 사이버 위협에 대한 조정 및 대응 능력을 향상하도록 요구함

Ⅳ. 유망 수요처

2. 급성장 수요처 키워드

② 통신(Telecommunication)

Du, 시스코와 협력하여 사이버보안 혁신

- UAE 통신사 Du(Emirates Integrated Telecommunications company)가 시스코(Cisco)와 협력하여 보안운영센터를 첨단사이버 방어 및 인텔리전스센터로 전환함. 해당 이니셔티브는 모바일 월드 콩그레스 2024에서 공개되었으며, AI와 자동화를 활용해 듀텔레콤의 보안 및 운영 효율성을 강화할 예정임
- 이번 협력을 통해 Du는 UAE의 디지털 전환 전략을 지원하고 국가의 디지털 인프라를 보호할 수 있음. 또한, 시스코의 첨단 보안 운영 및 AI 역량을 통합함으로써 사이버 위협으로부터 시스템을 강화하여 사이버보안 분야의 선도적 역할을 수행하게 됨

싱텔과 포티넷, 파라곤 플랫폼에서 5G 보안 강화 협력

- 싱가포르 통신사 싱텔(Singtel)과 포티넷(Fortinet)은 싱텔의 파라곤 플랫폼 마켓플레이스(Paragon Platform Marketplace)에 첨단 사이버보안 솔루션을 도입하기 위한 협력을 발표함. 포티넷의 'FortiGate VM 차세대 방화벽'을 활용하여 기업에 플러그 앤 플레이(Plug-and-Play) 보안 솔루션을 제공함
- 포티넷의 보안 기술을 싱텔의 파라곤 플랫폼에 통합하면 기업들은 5G 애플리케이션을 안전하게 배포할 수 있으며, 증가하는 사이버 공격의 위협에 대응할 수 있음. 이번 협력을 통해 점점 더 정교해지는 사이버 위협을 방어할 수 있으며, 기업들이 5G 기술을 적극적으로 도입할 수 있도록 효과적인 사이버보안 솔루션을 지원함

텔레포니카 테크, MS와 협력해 글로벌 사이버보안 서비스 강화

- 스페인 통신사 텔레포니카 테크(Telefónica Tech)가 마이크로소프트(Microsoft)와의 글로벌 협력을 통해 전 세계 기업을 위한 사이버보안 서비스를 강화한다고 발표함. 이번 협력은 샌프란시스코에서 열린 RSA 콘퍼런스에서 공개되었으며, MS의 고급 보안 및 AI 솔루션을 텔레포니카 테크의 운영 사이버보안 솔루션과 통합하여 능동적이고 자동화된 실시간 보안 관리를 제공할 예정임
- 이번 협력으로 텔레포니카 테크의 사이버 위협 탐지 및 대응, 신원 접근 관리 등의 서비스가 추가됨. 스페인 마드리드(Madrid)와 콜롬비아 보고타(Bogota)의 디지털 운영 센터에서 전문팀이 관리하며, 이번 파트너십으로 사건 대응 능력을 향상시키고 보안 프로세스를 최적화하여 온라인 위협에 대한 정보 보안을 제공할 예정임

2. 급성장 수요처 키워드

③ 에너지(Energy)

■ 에너지 부문에 필수적인 사이버보안 조치

- 에너지 부문에서 사이버보안 대책을 시행하기 위해서는 기술, 프로세스, 종사자 인식을 통합한 종합적인 접근이 필요함. AI, 머신러닝, 블록체인 등 신흥 기술이 에너지 분야 사이버보안을 강화하는 데 중요한 도구가 되고 있음. 이러한 기술은 이상 징후를 감지하고 거래를 확보하며 중요한 인프라를 보호하는 데 도움을 줌. 또한, 정부 규제와 산업 표준이 중요한 역할을 함. 규제 기관은 에너지 인프라의 보안과 복원력을 보장하는 데 집중하고 있으며, 에너지 기업은 표준 규정을 준수해야 함

■ 미국, 에너지 사이버보안 투자 증가

- 미국 에너지부(Department of Energy)는 에너지 분야 전반에 걸쳐 사이버보안을 강화하기 위한 16개 프로젝트에 4,500만 달러(약 600억 원)를 투자한다고 발표함. 이 프로젝트는 사이버보안, 에너지보안 및 비상대응국(Office of Cybersecurity, Energy Security, and Emergency Response)에서 관리하며, 전력망, 유틸리티, 파이프라인 및 재생 에너지원을 포함한 에너지 시스템의 사이버 위험을 완화하고 복원력을 향상하는 도구 개발에 중점을 둠
- 에너지부는 오번대학교(Auburn University)의 맥크레이 연구소(McCrary Institute)에 1,000만 달러(약 135억 원)의 보조금을 지급하여 동남권 사이버보안 협력 센터(SERC3)를 설립함. 이 센터는 오크리지국립연구소(ORNL)와 협력하여 전력망과 기타 주요 부문을 사이버 공격으로부터 보호하는 솔루션을 모색할 예정임. 총 프로젝트 비용은 1,250만 달러(약 169억 원)로, 오번대학교와 기타 파트너들이 추가로 250만 달러(약 34억 원)를 지원함

■ EU, 에너지 분야 사이버보안 강화 위한 훈련 실시 및 규칙 채택

- EU 집행위원회는 에너지 분야 사이버 안보 강화를 위한 '사이버 유럽' 훈련을 실시함. 이는 대규모 사이버 공격에 대비해 EU 에너지 부문의 준비 상태를 시험하기 위한 것으로, EU 에너지 인프라의 사이버 위협 회복력에 대한 조정, 협력 역량 및 위기 관리 기술을 중심으로 평가함
- 위원회는 전력 부문의 사이버보안을 위한 최초의 EU 네트워크 코드를 채택함. 이 법안은 EU 전력규정(EU) 2019/943(제59조) 및 2022년 에너지 시스템 디지털화를 위한 EU 행동 계획에 따라 진행된 것임. 유럽 내 주요 에너지 인프라와 서비스의 사이버 복원력을 강화하고, 유럽 내 국경을 넘는 전력 흐름에 대한 높은 수준의 사이버보안을 보장하는 것을 목표로 함

2. 급성장 수요처 키워드

④ 정부(Government)

■ 미 NIST, 사이버보안 프레임워크 2.0 공개

- 2024년 2월 미국 국립표준기술원(National Institute of Standards and Technology)은 사이버보안 프레임워크(CSF, Cybersecurity Framework) 2.0 버전을 공개함. 새로운 버전에서는 기존의 다섯 가지 기능인 식별, 보호, 탐지, 대응, 복구에 '거버넌스'라는 여섯 번째 핵심 기능을 추가하여, 사이버 리스크 관리가 기업의 거버넌스 구조에 통합되는 중요성을 강조함
- 업데이트된 프레임워크는 또한 사이버보안 위협의 상호 연결된 특성을 인식하여 공급망 위험 관리도 중점을 둠. NIST는 기업이 지침을 보다 쉽게 채택하고 적용할 수 있도록 구현 예시와 참조 매핑 도구를 포함한 리소스 모음을 함께 제공하고 있음. 이번 업데이트를 통해 다양한 부문에서 사이버보안 회복력을 강화하는 데 기여할 수 있음

■ 영국 정부, 사이버보안 거버넌스 실천 강령 제안

- 2024년 1월 영국 정부는 국가 사이버보안 센터(National Cyber Security Centre)와 협력하여 기업 지도자를 대상으로 한 '사이버 거버넌스 실천 강령(Cyber Governance Code of Practice)' 초안을 공개함. 제안된 내용은 기업이 사이버 리스크를 재무나 법적 문제처럼 중요시 여기도록 하며, 강력한 사건 대응 계획과 향상된 직원 보안 교육의 필요성을 강조하고 있음
- 이번 이니셔티브는 영국 기업의 사이버 위협에 대한 회복력을 강화하여 신흥 기술을 안전하게 활용할 수 있도록 하는 것을 목표로 함. 정부는 제안에 대한 의견 수렴을 진행하며, 효과적인 사이버보안 관행을 형성하는 데 있어 산업계의 의견이 중요하다고 강조함

■ 영국-일본, 사이버보안 파트너십 강화

- 2024년 1월 영국과 일본이 사이버보안 협력을 강화하기 위한 협력각서(MOU)를 체결함. 이번 협약은 일본 경제단체연합회(Keidanren) 사이버보안위원회의 영국 방문 중에 이루어짐. 이번 협약은 공공-민간 파트너십을 심화하여 사이버 방어를 강화하는 것을 목표로 함
- 이번 파트너십은 글로벌 사이버보안 협력의 중요성을 강조하며, 양국은 디지털 공급망 보안, 기업의 사이버 회복력 강화, 사이버 기술 향상에 중점을 두고 있음. 이번 협약은 2023년 5월에 체결된 히로시마 협정(Hiroshima Accord)을 기반으로 하여 기술 및 보안 파트너십에 대한 내용을 포함하고 있음

Ⅳ. 유망 수요처

2. 급성장 수요처 키워드

⑤ 은행(Banking)

■ 은행에서 사이버 공격에 대응하는 전략

- 모니터링 : 모든 디지털 은행 서비스에 보안 테스트 및 패치 설치를 수행하는 추적 소프트웨어를 구현하여 침해 발생 시 실시간 알림이 오도록 함
- 위험 평가 : 정기적인 위험 평가를 통해 새로운 위협을 방어하고 효과적인 대응 계획을 수립함
- 암호화 : 모든 고객 정보는 암호화되어야 하며, SSL 및 TLS 프로토콜과 같은 보안 표준 사용
- 접근 관리 : 시스템, 애플리케이션, 데이터에 적절한 접근 방법을 설정함. 고객에게는 이중 인증 또는 생체 인식을, 직원에게는 역할 기반 액세스 제어(RBAC)를 적용함
- 네트워크 보안 : 방화벽, 침입 탐지 소프트웨어 등 사전 예방 네트워크 보안 솔루션을 탑재함
- 엔드포인트 보안 : 엔드포인트 탐지 및 대응 솔루션(EDR) 및 모바일 장치 관리(MDM) 도구를 사용하여 장치 보안을 강화하고, 손상된 장치가 있는 경우 데이터를 제거함
- 데이터 손실 방지 : 데이터 손실을 방지하기 위해 탐지 시스템, 백신 소프트웨어 등을 사용하여 악성코드나 랜섬웨어에 대해 시스템을 보호함

■ 금융 보안의 주요 트렌드, AI 및 생체 인식 기술 사용

- 금융권은 고객 인증과 사기 방지에 초점을 맞춘 보안 대책을 강화하는 추세임. 사이버 공격에 대처하고 보안을 강화하는데 가장 주목할 만한 트렌드 중 하나는 암호 없는 인증으로의 전환임. 이는 전통적인 암호의 필요성을 제거하여 보안을 강화하고 사용자 경험을 개선할 수 있으며, 생체 인식과 일회용 코드 등으로 수행할 수 있음
- AI를 활용한 사기 탐지 및 방지 기술도 증가하고 있음. AI 산업은 지불, 대출 및 고객 온보딩 프로세스에서 의심스러운 활동을 즉시 식별할 수 있는 알고리즘을 개발하고 있음. 또한 AI 솔루션으로 개인에게 최적화된 프로필을 만들 수 있으며 이를 바탕으로 실시간 행동을 분석하여 사기 및 위험을 예방함
- 또한, 생체 인식 인증을 주로 채택하는 추세로 민감한 정보를 보호하고 거래 승인을 간소화함. 이는 특히 온라인 뱅킹 사기에 효과적인 대책으로 입증되었으며 안전하고 사용자 친화적인 인증 방법임

[참고문헌]

■ 참고 사이트

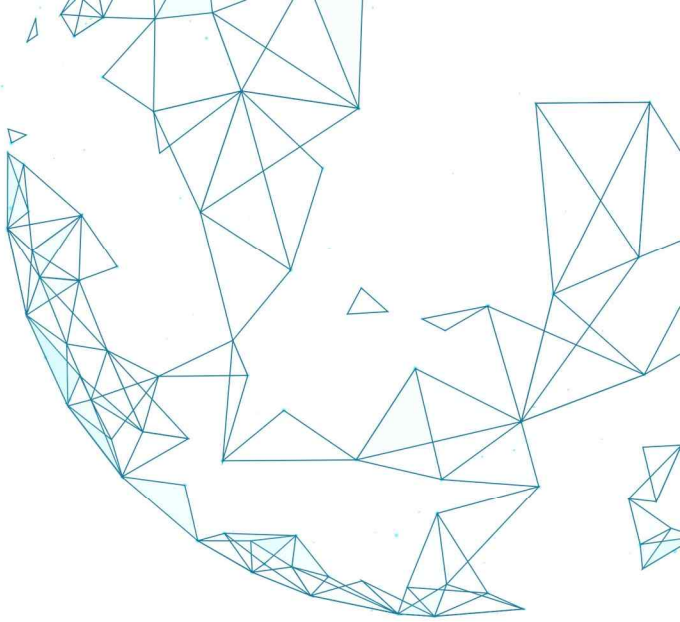
1. European Parliamnet(europarl.europa.eu)
2. CNBC(cnbc.com)
3. Gartner(gartner.com)
4. Forbes(forbes.com)
5 Splashtop(splashtop.com)
6. market.us(market.us)
7. Statista(statista.com)
8. e-Governance Academy Foundation(ncsi.ega.ee)
9. Tech Navio(technavio.com)
10. Mordor Intelligence(mordorintelligence.com)
11. Internatoinal Trade Administration(trade.gov)
12. Beehive.govt.nz(beehive.govt.nz)
13. NCSC(ncsc.govt.nz)
14. PWC(pwc.com)
15. eSecurity Planet(esecurityplanet.com)
16. Microsoft(microsoft.com)
17. IBM(ibm.com)
18. Cisco(cisco.com)
19. Info.Pivitglobal(info.pivitglobal.com)
20. Blog.Sonicwall(blog.sonicwall.com)
21. Avfirewalls(www.avfirewalls.com)
22. Sdxcentral(www.sdxcentral.com)
23. Kbvresearch(www.kbvresearch.com)
24. Techtarget(www.techtarget.com)
25. Linkedin(www.linkedin.com)
26. Icariatechnology(icariatechnology.com)
27. Freepressjournal(www.freepressjournal.in)
28. Turing(www.turing.com)
29. Bigid(bigid.com)
30. Theverge(www.theverge.com)
31. Thehackernews(thehackernews.com)
32. Datapatrol(datapatrol.com)
33. Networksimulationtools(networksimulationtools.com)
34. Csoonline(www.csoonline.com)
35. Businesswire(www.businesswire.com)
36. Instasafe(instasafe.com)
37. Securitytrails(securitytrails.com)
38. Cybersecurityguide(cybersecurityguide.org)
39. Cyberscoop(cyberscoop.com)
40. Tripwire(www.tripwire.com)

[참고문헌]

■ 참고 사이트

41. Gmanetwork(www.gmanetwork.com)
42. Telefonica(www.telefonica.com)
43. Singtel(www.singtel.com)
44. Newsroom(newsroom.cisco.com)
45. Smart-Energy(www.smart-energy.com)
46. Hackernoon(hackernoon.com)
47. Institutedata(www.institutedata.com)
48. Securityweek(www.securityweek.com)
49. Energy(energy.ec.europa.eu)
50. Helpnetsecurity(www.helpnetsecurity.com)
51. Managedservicesjournal(managedservicesjournal.com)
52. Techmonitor(techmonitor.ai)
53. Cybersecuritydive(www.cybersecuritydive.com)
54. Techuk(www.techuk.org)
55. Verdict(www.verdict.co.uk)
56. Startups.Epam(startups.epam.com)
57. Cybersecurity.Asee(cybersecurity.asee.io)

nipa 글로벌 ICT 포털



품목별 ICT 시장동향

· 발행·편집 : 정보통신산업진흥원
· 발행일자 : 2024.07.19

해당 원고에 대해 사전 동의 없이 상업 상 또는 다른 목적으로
무단 전재·변경·제 3자 배포 등을 금합니다.
또한 본 원고를 인용하시거나 활용하실 경우
△출처 표기 △원본 변경 불가 등의 이용 규칙을 지키셔야 합니다.

Copyright 2024 NIPA 정보통신산업진흥원 All Rights Reserved.
Printed in Korea