사이버 보안 산업 동향 및 시사점

KDB미래전략연구소 산업기술리서치센터
조상진 전임연구원(kiltos@kdb.co.kr)

최근 국가·산업 보안을 위협하는 글로벌 해킹 조직의 증가와 개인정보 유출 등의 사이버 범죄로 인해 보안 산업의 중요성과 사회적 관심이 커지고 있다. 미국, 영국, 이스라엘 등의 주요국은 사이버 보안의 필요성을 국가안보 (안전, 경제, 사회 등) 차원으로 확대하고 있으며, 우리나라도 사이버 보안 기술을 12대 국가전략기술로 지정하고 민관 협동으로 산업 혁신전략을 추진하고 있다.

사이버 보안 산업은 '창과 방패'처럼 진화하는 보안 위협에 대응하여 지속적인 연구개발이 요구되는 산업으로 '21년 글로벌 사이버 보안 시장 규모는 1,321억 5,200만 달러(한화 약 167조 원)이며, 국내는 4조 5,497억원 규모를 형성하고 있다. 국내 사이버 보안 시장의 경우 해외 업체와 비교 시 시장 규모가 작고 자금 조달이 어려워 상대적으로 해외 시장에 대한 매출이 적으며, 국내외 상위 10개 기업을 대상으로 국내외 매출액을 비교할 때 해외 10개 기업(합산 매출액: 187조 3,774억원)은 국내 10개 기업(합산 매출액: 1조 2,497억원) 대비 약 150배 차이(2022년 결산 기준)를 보인다.

국내 사이버 보안 산업의 지속적인 성장과 경쟁력을 높이기 위한 전략으로 제로 트러스트(Zero Trust) 도입과 암호기술 및 AI 기반 기술과의 융합을 통해 사이버 보안 기술을 고도화하는 것이 필요하며, 국제 표준 사이버 보안 인증 취득과 오픈소스 역량 강화를 바탕으로 국내 시장에서 글로벌 시장으로 확대할 수 있는 산업 생태계 조성이 필요하다.

* 본고의 내용은 집필자 견해로 당행의 공식입장이 아님

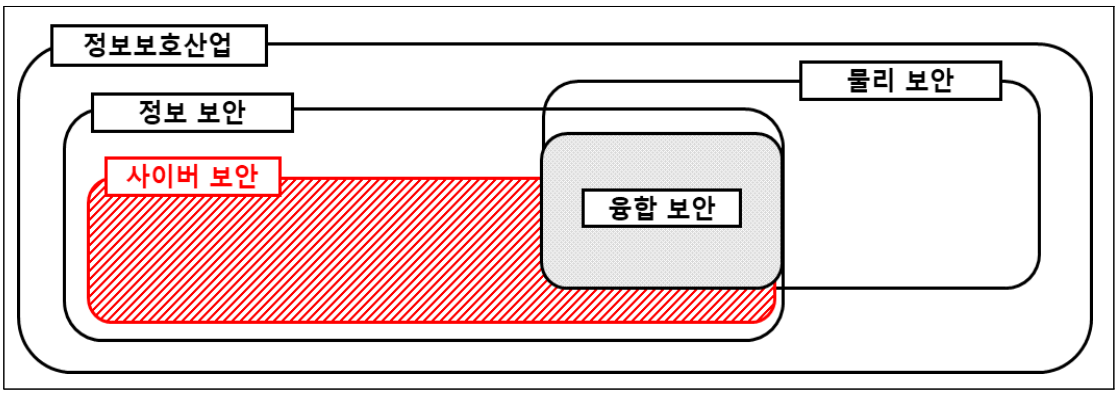
Ⅰ. 사이버 보안 정의 및 산업개요

1. 사이버 보안 정의 및 산업 동향

❑ 사이버 보안 산업은 모바일, 컴퓨터, 네트워크 등의 데이터를 사이버 공격으로부터 안전하게 보호하는 산업

○ **(사이버 보안)** 디지털 공격으로부터 중요한 시스템과 민감한 정보를 보호하는 활동이며, 사이버 공간에서의 위험을 최소화하는 보안기술
- 디지털 데이터를 안전하게 보호하는 것으로 사이버 보안이 정보보안의 하위집합임

〈그림 1〉 사이버 보안 산업 범위



자료 : 당행 작성

○ 사이버 보안 산업은 진화하는 보안 위협에 대응하는 산업이며, AI 기반 보안기술 확대와 융합을 통해 지속적으로 성장하는 산업
- 네트워크, 엔드포인트[1], 애플리케이션, 클라우드, 시스템, 데이터 등의 보안으로 분류
- 전방산업은 IT서비스 및 사용자 등이며, 후방산업은 개발 소프트웨어, 보안 관련 장치 및 인프라 하드웨어 등으로 구성
- 사이버 보안 산업은 '창과 방패'처럼 진화하는 보안 위협에 대응하여 지속적인 연구개발이 요구되는 산업

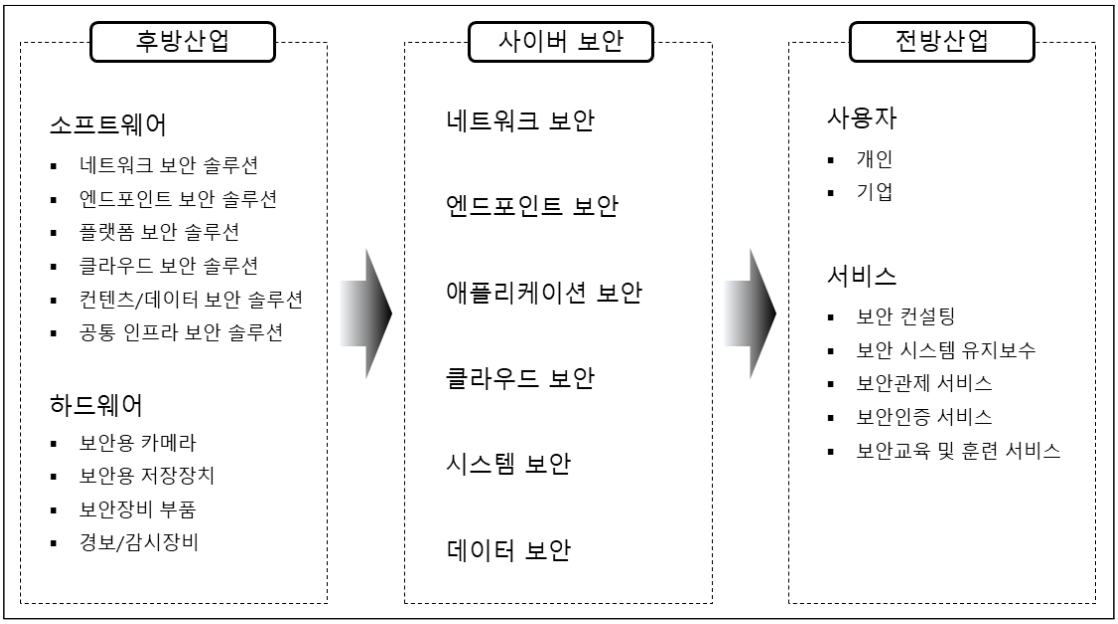
1) 엔드포인트(Endpoint): 네트워크와 최종적으로 연결된 IT 기기 및 단말을 말함

〈표 1〉 **사이버 보안 분류**

구 분	주요 내용
네트워크 보안 (Network security)	- 승인되지 않은 상태에서 기업 네트워크에 침입하는 것을 막거나 방지하는 활동
엔드포인트 보안 (Endpoint security)	- 악의적인 내부 및 외부 위협으로부터 데스크톱, 노트북, 서버 및 고정 기능기기를 보호하는 활동
애플리케이션 보안 (Application security)	- 애플리케이션 코드의 취약점을 찾아서 수정해 앱을 더 안전하게 만드는 보안 활동
클라우드 보안 (Cloud security)	- 클라우드 컴퓨팅 환경에서 데이터 및 서비스를 보호하는 활동
시스템 보안 (System security)	- 운영체계(OS), 데이터베이스(DB) 등 컴퓨터 시스템과 관련된 보안에 대한 것으로 악성코드 예방, 백신 소프트웨어 등을 포함
데이터 보안 (Data recovery)	- 데이터의 기밀성, 무결성, 가용성을 보호하는 활동

자료 : ITWORLD(2019.12), '사이버 보안의 개념과 종류, 그리고 일자리' 및 당행 재구성

〈그림 2〉 **사이버 보안 전·후방 산업 생태계**



자료 : 당행 작성

○ **(사이버 공격)** 취약한 컴퓨터 시스템을 활용하여 기밀정보에 대한 무단 악용, 탈취, 손상 등을 시도하는 행위

- 단순 시스템 감염 및 파괴에서 시스템 장악을 통한 금전 요구로 사이버 공격 목적이 점차 변화

〈표 2〉 사이버 공격 유형

구 분	주요 내용
악성코드 (Malware)	- 악성 소프트웨어의 줄임말로 컴퓨터 네트워크에 손상을 입히기 위해 고안된 모든 종류의 소프트웨어
피싱 (Phishing)	- 공격자가 이메일을 조작해 목표 대상을 속여서 어떤 유해한 행동을 취하는 기술
스캠 (Scam)	- 공격자가 피해자를 속여 민감한 정보를 획득하거나 금전을 갈취하기 위해 신뢰할 수 있는 출처나 인물을 가장하는 공격 방법
랜섬웨어 (Ransomware)	- PC의 중요 파일(문서, 사진 등)을 암호화하고 금전을 요구하는 악성코드
서비스 거부 공격 (DDoS)	- 일부 온라인 서비스가 제대로 작동하지 않도록 시도하는 무작위 입력 공격 방법
중간자 (Man in the Middle)	- 사이버 범죄자가 사용자와 그들이 접근하려고 하는 웹서비스 사이에 은밀하게 끼어드는 방법
크립토재킹 (Cryptojacking)	- 다른 사람의 컴퓨터가 공격자를 위해 가상통화를 생성하는 일(가상 언어로 채굴(Mining)이라고 하는 과정)을 하도록 전문화된 공격 방법
SQL 인젝션 (Injection)	- 공격자가 취약점을 이용해 피해자의 데이터베이스를 제어할 수 있는 수단
제로데이 익스플로잇 (Zero-day exploits)	- 컴퓨터 소프트웨어의 취약점을 공격하는 공격 방법으로 패치가 나오지 않은 시점에서 이루어지는 공격

자료 : ITWORLD(2020.03), '사이버 공격이란 무엇인가 의미와 사례 동향 분석' 및 당행 재구성

〈참고 1〉 **정보보호산업**

❑ **보안은 외부의 위협으로부터 시스템, 자산, 정보 등을 보호하고 안전하게 유지하는 것이며, 기업·정부·개인·조직 등에 필수적인 요소**

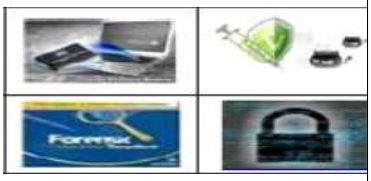
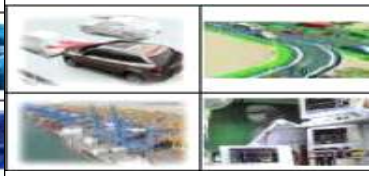
○ (정보보안산업) 정보보호 제품을 개발·생산 또는 유통하거나 정보보호에 관한 컨설팅, 보안관제 등 서비스를 제공하는 산업

- (정보보안) 컴퓨터 또는 네트워크상 정보의 훼손·변조·유출 등을 방지하기 위한 보안기술
  · 정보보안은 디지털 및 아날로그 형식에 관계없이 모든 데이터를 안전하게 보호하는 것이며, 사이버 보안은 디지털 데이터를 안전하게 보호하는 것으로 사이버 보안이 정보보안의 하위집합임
  · 방화벽, 안티바이러스, 디도스(DDoS) 대응장비 등

- (물리보안) 통제 수단(사람·물품·차량 등)을 적용하여 물리적인 위협 수단으로부터 정보·인명·시설을 보호하기 위한 보안기술
  · 출입 통제, 영상 감지 솔루션, 지능형 카메라, 바이오 인식 등

- (융합보안) 물리보안과 정보보안(사이버 보안 포함) 간의 융합 또는 IT 기술과 타(他) 산업 간 융·복합 시 발생하는 보안 위협을 해결하기 위한 보안기술
  · 차량 블랙박스, u-헬스케어 보안 장비 등

정보보안산업 범위

정보보안	물리보안	융합보안
"클린인터넷경제"	"안전안심생활"	"안전성강화"
		
네트워크 상의 정보 유출·훼손 방지	재난·재해, 범죄 등 방지	타 산업 분야의 보안 내재화

자료 : 과학기술정보통신부(2022.02), '디지털 대전환시대 정보보호산업의 전략적 육성 방안'

❑ 사이버 공격 기술의 고도화 및 증가로 사이버 보안 시장은 지속 성장

○ **(글로벌)** 사이버 공격 및 해킹의 증가로 전 세계 국가들은 사이버 안보에 집중하고 있어 사이버 보안 솔루션 및 서비스는 지속적으로 증가될 것으로 전망

- '21년 사이버 보안 시장 규모는 1,321억 5,200만 달러(한화 약 167조 원)로 '16년 이후 연평균 11.5%의 성장 추세
- 글로벌 사이버 보안 시장은 북미(44.2%) > 유럽(27.6%) > 아시아(22.0%) 순으로 시장 점유율을 형성
  · 미국 내 랜섬웨어 공격 건수는 7,840만 건으로 사상 최고치 기록('21.06)
  · 영국 기관에 대한 랜섬웨어 공격 건수 전년 대비 두 배 증가('21년)
  · 독일 사이버 보안 시장의 매출 중 약 78%는 컨설팅, 유지보수 등의 서비스 분야임
  · 일본 경시청에 보고된 기업·조직의 랜섬웨어 피해 건수는 61건으로 전년 하반기(21건) 대비 2.9배 증가하며 랜섬웨어 공격으로 인한 피해사례 급증('21.01~06)
  · 중국은 약 9억 명의 인터넷 사용자를 기반으로 네트워크 보안 시장이 지속적으로 성장

〈표 3〉 **글로벌 사이버 보안 시장 매출 현황**

(단위 : 백만 달러, %)

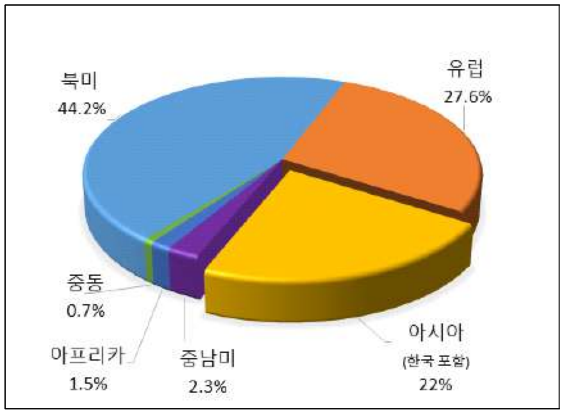
구 분	2016년	2017년	2018년	2019년	2020년	2021년	CAGR(%) ('16~'21)
북미	34,851	38,890	44,033	50,885	53,364	58,423	10.9
유럽	21,794	24,326	28,094	30,793	32,378	36,477	10.9
아시아	14,254	16,471	19,415	23,014	25,132	29,013	15.3
중남미	2,523	2,919	2,974	3,164	2,886	3,075	4.0
아프리카	1,413	1,524	1,652	1,797	1,841	1,984	7.0
중동	476	559	692	781	769	914	13.9
글로벌	**76,699**	**86,294**	**98,554**	**112,240**	**118,265**	**132,152**	**11.5**

자료 : 한국인터넷진흥원(2022.03), '2021 글로벌 정보보호 산업시장 동향조사' 및 당행 재구성

○ **(국내)** 정보통신기술(ICT)의 발전에 따른 사이버 위협과 보안 수요 증가로 물리보안 시장 대비 사이버 보안 시장이 더 빠르게 성장

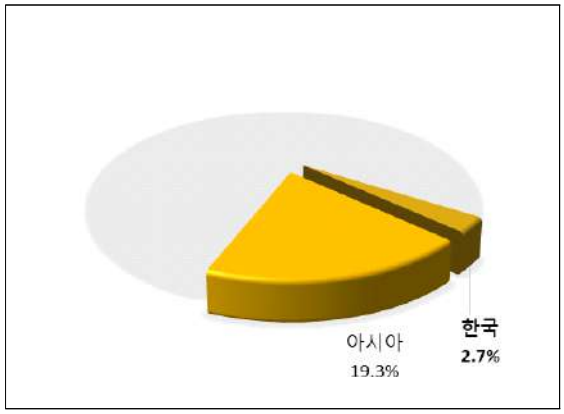
- 사이버 보안 시장을 포함하는 국내 정보보안 시장은 '15년 2조 1,087억원에서 '21년 4조 5,497억원으로 연평균 13.7% 증가(물리보안 연평균 7.3% 증가)
- 글로벌 사이버 보안 시장에서 한국은 2.7%를 차지하고 있으며, 약 40.9%를 차지하고 있는 미국(541억 달러)과 비교 시 약 15배 차이

〈그림 3〉 글로벌 사이버 보안 시장 비중



자료 : 한국인터넷진흥원(KISA), 2022

〈그림 4〉 사이버 보안 아시아 및 국내 시장 비중



자료 : 한국인터넷진흥원(KISA), 2022

○ 사이버 공격의 증가에 따라 사이버 보안 역량의 중요성 인식 필요

- 사이버 보안 사고는 검거건수(평균 증가율: 1.7%) 대비 발생건수(평균 증가율: 7.3%)가 더욱 빠르게 증가
  · '21년 유형별 사이버 공격 연평균 증가률(CAGR: 2016~2021)은 해킹 10.2%, 디도스(DDoS) -17.5%, 악성프로그램 -2.1%이며, 유형 중에서 해킹이 지속적으로 증가

〈표 4〉 글로벌 사이버 보안 시장 매출 현황

(단위 : 건, %)

구 분	2016년	2017년	2018년	2019년	2020년	2021년	CAGR(%) ('16~'21)
발생건수	153,075	131,734	149,604	180,499	234,098	217,807	7.3
검거건수	127,758	107,489	112,133	132,559	157,909	138,710	1.7

자료 : 경찰청(2022.11), '2021년 경찰통계연보' 및 당행 재구성

❑ 코로나19 장기화에 따른 원격근무 및 사회 전반에 걸친 비대면 서비스 증가로 사이버 보안에 대한 수요는 급격히 증가

❍ 재택근무, 비대면·비접촉, 출입 통제 강화 등으로 새로운 시장이 창출되었으며, 안전과 보안에 대한 수요 역시 증가

- 시장 내 주요 보안기업은 사이버 공격에 대응하기 위해 인터넷 보안 솔루션 개발에 주력하는 추세

❍ '21년 사이버 위협(데이터 침해, 피싱 등)이 증가하였고, 기업 조직 내 실수로 인한 사이버 보안 사고도 증가

- 데이터 유출 사고는 대부분 외부 해커에 의해 공격을 받는 형태로 이루어졌으나, 코로나19로 원격 및 재택근무가 증가하면서 데이터 유출 사고 발생 위험이 증가

❍ '21년 12월에 발생한 주간 사이버 공격은 조직당 925건에 달해 역대 최고치를 기록(CheckPoint Research 보고서)

- '21년 사이버 위협에 가장 취약한 부문은 교육 및 연구 분야로, 조직당 매주 1,605건의 공격이 발생하여 전년 대비 75% 증가

〈표 5〉 **산업 및 조직별 주간 평균 사이버 공격 건수**

(단위 : 건, %)

순위	구분	발생건수	전년비 (`20/`21)	순위	구분	발생건수	전년비 (`20/`21)
1	**교육 및 연구**	**1,605**	**+75%**	6	SI/VAR/Distributor	778	+18%
2	**정부 및 국방**	**1,136**	**+47%**	7	Utilities	736	+46%
3	통신	1,079	+51%	8	제조	704	+41%
4	ISP/MSP	1,068	+67%	9	금융 및 은행	703	+53%
5	헬스케어	830	+71%	10	보험	636	+58%

자료 : 한국인터넷진흥원(2022.03), '2021 글로벌 정보보호 산업시장 동향조사' 및 당행 재구성

2. 국내외 업계 현황

❑ (글로벌) 사이버 보안 시장의 약 40%를 차지하는 미국은 연방정부가 적극적인 투자 수요를 형성하여 글로벌 시장을 주도

○ 주요 기업으로는 NortonLifeLock(미) 15.9%, McAfee(미) 13%, CheckPoint(이) 3.9%이며, 기타 약 1만 730개의 기업이 존재

- 클라우드 기반의 보안 솔루션 도입이 증가하면서 해당 시장의 경쟁이 심화되고 있으며, Cisco Systems(미), NortonLifeLock(미), Fortinet(미), Palo Alto Networks(미) 등이 주도

〈표 6〉 글로벌 주요 사이버 보안 기업

기업명	주요 내용
Cisco Systems (미국)	- 차세대 네트워크, 데이터센터, 사이버 보안 등의 분야에서 활약하고 있으며, 전 세계 데이터 트래픽의 80% 이상이 해당 기업의 네트워크 인프라를 사용
Palo Alto Networks (미국)	- 네트워크 및 클라우드 보안, 엔드포인트 보호 업체로 2022년 11월에 애플리케이션 공급망 전문업체인 사이더시큐리티(Cider security)를 인수
Fortinet (미국)	- 네트워크, 클라우드 보안, AI 기반 보안관제, 사용자 보안, 클라우드 기반 애플리케이션 보안 제품 및 서비스 공급 기업
McAfee (미국)	- 엔드포인트, 에지 및 클라우드 보안을 포함한 광범위한 사이버 보안 플랫폼을 구축하였으며, CASB 공급업체인 스카이하이 넥스웍스를 인수
CheckPoint (이스라엘)	- 2021년 딜로이트(Deloitte)의 '고속성장 500대 기업(Technology Fast 500)'에 선정되며 북미지역 내 가장 빠르게 성장하는 사이버 보안 기업 중 하나로 인정
CrowdStrike (미국)	- 2011년에 설립하여 사이버 공격 전문 보안기업으로 2022년 09월 공격 통로를 관리해 주는 업체인 리포지파이(Reposify)를 인수
Okta (미국)	- IDaaS(IDentity-as-a-Service), 제로 트러스트 등 사이버 보안 사업을 영위하고 있으며, 워크플로우 자동화 스타트업인 아주쿠아(Azuqua)를 인수
NortonLifeLock (미국)	- 엔드포인트(데이터·이메일·인증서 등)에서 iOS, Android, Window OS 기반의 모바일 단말을 보안 위협으로부터 보호하는 앱 형태의 종합 솔루션 제공

자료 : 한국신용정보원(2019.02), '사이버 보안' 시장보고서, 업체 홈페이지 및 당행 재구성

○ 사이버 보안 기업은 '기존사업 강화' 또는 '신규사업 개척'에 집중
- 기존 보안 업체와 빅테크 기업들은 자사 보안 강화 및 보안업계로의 진출을 위해 신규 보안 업체를 인수

〈표 7〉 **2022년 글로벌 사이버 보안 업계 주요 M&A**

구분	1월	2월	3월	4월	5월	6월	7월	8월	9월	10월	11월	12월
M&A(수)	3	7	4	6	0	4	2	1	2	2	5	1
주요 내용	상반기						하반기					
	- (Google) 시엠플리파이 5억 달러에 인수						- (IBM) 란도리 인수					
	- (CheckPoint) 스펙트럴 인수						- (Microsoft) 미부로 인수					
	- (Akamai) 라이노드 인수						- (CrowdStrike) 리포지파이 인수					
	- (Google) 맨디언트 54억 달러에 인수						- (Intel 471) 스파이더풋 인수					
	- (Synopsys) 화이트햇시큐리티 인수						- (Palo Alto Networks) Cider security 인수					

자료 : 시큐리티월드(2023.01), '2022년 글로벌 사이버 보안 업체 주요 M&A' 및 당행 재구성

❑ (국내) 신규 온라인·모바일 서비스의 증가로 사이버 위협 및 보안의 중요성 증가

○ 비대면 환경의 확산으로 네트워크 보안(정보보안), 비대면 출입통제(물리보안) 등 보안 제품의 수요가 증가
- 실생활에 밀접한 IT서비스가 확산되면서 사이버 보안에 대한 관심이 높아지고 있어 지속적인 시장 확대가 전망됨

○ 국내 금융 및 제조 업종의 침해사고 증가
- 개인정보 침해, 랜섬웨어, 디도스(DDoS) 공격 등 불특정 다수 및 특정 목표를 대상으로 하는 해킹 범죄가 증가하면서 사이버 보안에 대한 수요가 확대되고 있음
- '22년 상반기 내 유형별 침해사고로 악성코드 39.2%, 중요 정보 유출 32.3%, 피싱·스캠 15.7%로 조사

〈표 8〉 국내 주요 사이버 보안 기업

기업명	주요 내용
SK쉴더스	- 2000년에 설립된 정보보안 전문업체로 사이버 보안 및 물리보안 사업역량을 보유하고 있으며, 보안 컨설팅, 관제, 솔루션/시스템통합(SI), 클라우드 보안, 모바일 케어 솔루션 등 보안 서비스를 제공하고 있음
안랩	- 1995년 안철수컴퓨터바이러스연구소로 설립하여 국내 최초의 백신 소프트웨어 V3를 개발한 이래, 대표적인 사이버 보안 업체로 성장해왔으며, 소프트웨어 및 하드웨어에 걸쳐 전반적인 보안 솔루션을 제공하고 있음
시큐아이	- 2000년에 설립 후 정보보안산업을 영위하고 있으며, 자체 클라우드 방화벽 솔루션 '블루맥스 NGF VE'와 멀티클라우드 인프라를 지원하는 클라우드 보안관제 서비스, 두 가지 방향으로 클라우드 보안 사업을 전개하고 있음
이글루시큐리티	- 1999년 설립한 네트워크 보안 솔루션 전문업체로, 국내 보안 정보 및 이벤트 관리(SIEM) 솔루션과 보안관제 서비스 시장을 견인하고 있음
윈스	- 1996년에 설립된 사이버 보안 기업으로 대표제품으로 '스나이퍼(SNIPER)'를 출시하였으며, 네트워크 보안 분야에서 침입방지시스템(IPS), 디도스(DDoS) 공격 대응 솔루션, 지능형공격(APT) 등을 개발·공급하고 있음
한국정보인증	- 1999년에 설립된 인증기관으로 공개키 기반구조(PKI) 솔루션 개발, 웹보안서버(SSL), 바이오인증서 서비스 등의 사업을 영위하고 있으며, 모바일 신분증 인증서 기술 보유를 바탕으로 카카오와 네이버에 독점계약을 추진 중에 있음
지란지교시큐리티	- 2014년 모기업 지란지교소프트 보안사업본부에서 분사하여 설립된 보안 소프트웨어 전문기업으로 메일·문서·모바일 보안 및 악성 위협 대응 솔루션을 제공하고 있으며, 이메일 보안 솔루션인 '스팸스나이퍼(SpamSniper)'를 개발·공급하고 있음
파이오링크	- 2000년에 설립된 클라우드 데이터센터 최적화 전문기업으로 애플리케이션 전송 컨트롤러, 웹 방화벽, 클라우드 매니지드 네트워킹, 하이퍼 컨버지드 인프라 등의 보안 제품(솔루션)을 개발·공급하고 있음
이니텍	- 1997년에 설립된 정보보안 전문업체로서 공개키 기반구조(PKI) 기반 정보보안 솔루션 및 금융IT 사업을 영위하고 있으며, 소프트웨어를 악용한 조직적 해킹 시도에 대비하여 'INISAFE CrossWeb EX V3'의 최신버전 보안 패치 개발을 완료함
라온시큐어	- 1998년에 설립된 IT보안 및 인증 전문기업으로 모바일 보안, PC 보안 솔루션 및 서비스를 제공하고 있으며, FIDO(Fast Identify Online) 생체인증 표준과 블록체인 기반 분산 ID 기술 및 관련 솔루션을 개발하고 있음

자료 : 한국신용정보원(2019.02) '사이버 보안' 시장보고서, 업체 홈페이지 및 당행 재구성

〈참고 2〉 **국내 정보보호산업 업체 현황**

❑ **국내 정보보안 기업은 서울에 집중되어 있으며, 70% 이상이 정보보안 제품(솔루션) 사업을 영위**

○ 정보보안 관련 기업체의 소재지를 분석한 결과 669개 기업 중 487개 기업(72.8%)이 서울에 소재하고 있음

- 서울 487개(72.8%), 경기 89개(13.3%), 대전 19개(2.8%), 부산 16개(2.4%), 대구 12개(1.8%) 순으로 분포

국내 정보보안 및 물리보안 영위 기업 지역별 현황

(단위 : 개, %)

구분	정보보안		물리보안		합계	
	기업수	비율(%)	기업수	비율(%)	기업수	비율(%)
서울	487	72.8	305	36.0	792	52.2
서울 외	182	27.2	543	64.0	725	47.8
합계	**669**	**100.0**	**848**	**100.0**	**1,517**	**100.0**

자료 : 한국정보보호산업협회(2022.09), '2022년 국내 정보보호산업 실태조사'

○ 정보보안 기업체는 정보보안 제품(솔루션) 기업과 정보 보안 관련 서비스 기업으로 구분

- 정보보안 제품(솔루션)은 75.4%, 정보보안 관련 서비스는 24.6%로 조사

정보보안 기업의 품목별 취급 기업 현황

(단위 : 개, %)

대분류	중분류	기업 수	비율(%)
정보보안 제품 (솔루션)	네트워크 보안 솔루션	295	19.4
	엔드포인트 보안 솔루션	176	11.6
	플랫폼 보안/보안관리 솔루션	151	10.0
	클라우드 보안 솔루션	80	5.3
	컨텐츠/데이터 보안 솔루션	215	14.2
	공통 인프라 보안 솔루션	224	14.8
	소계	**1,141**	**75.2**
정보보안 관련 서비스	보안 컨설팅	147	9.7
	보안시스템 유지관리/보안성 지속 서비스	135	8.9
	보안관제 서비스	40	2.6
	보안인증 서비스	31	2.0
	보안교육 및 훈련 서비스	20	1.3
	소계	**373**	**24.6**
기타		3	0.2
합계		**1,517**	**100.0**

자료 : 한국정보보호산업협회(2022.09), '2022년 국내 정보보호산업 실태조사' 및 당행 재구성

Ⅱ. 사이버 보안 현황 및 주요 사례

1. 시대별 사이버 공격 및 보안

❑ 사이버 보안은 컴퓨터와 네트워크 등 정보통신기술의 발달이 진행되면서 다양하고 불규칙하게 진화를 거듭

○ 사이버 보안은 '창과 방패'라는 두 가지 보안전략의 요소를 가지고 있으며, 공격 이후 패턴을 업데이트하여 방어하는 방식으로 발전

- 창(Sword): 컴퓨터 또는 전산화된 정보시스템의 요소를 표적으로 삼아 데이터를 변경·파괴·유출하여 금품을 요구하는 공격
- 방패(Shield): 방화벽, 침입 탐지 시스템, 암호화 등의 보안전략으로 공격을 방어

〈표 9〉 시대별 사이버 공격 및 보안

구분		1세대 (1980년대)	2세대 (1990년대)	3세대 (2000년대)	4세대 (2010년대)	5세대 (현재)
주요기술	사이버 공격	- 바이러스 공격	- 악성코드	- 취약성 공격	- 공격의 전문화 - 타깃형 공격	- 공격의 진화 (디도스, 랜섬웨어 등)
	사이버 보안	- 안티 바이러스	- 방화벽	- IDS → IPS[2] - SIEM[3] 확대	- 안티봇 - 샌드박스	- SASE[4] - SECaaS[5] - XDR[6]
주요 기업		- McAfee - Symantec - 안랩	- CheckPoint - Cisco Systems	- Cisco Systems - Fortinet - Fireeye	- Fireeye - CheckPoint	- DarkTrace - Vectra

자료 : 한국인터넷진흥원(2021.12), 'AI 보안 관련 국내외 동향조사 및 기술수준 분석' 및 당행 재구성

2) IDS(Intrusion Detection System): 공격을 차단하지 않고 로그를 남기거나 경고를 보냄 → IPS(Intrusion Prevention System): 실시간으로 공격을 감지하고 대응

3) SIEM(Security Information and Event Management): 보안 관련 정보와 이벤트를 수집하고 분석하여 위협을 식별하고 대응하는 솔루션

4) SASE(Security Access Service Edge): 네트워킹 및 네트워크 보안 기능을 단일 클라우드 서비스로 결합하는 네트워크 보안 접근법

5) SECaaS(Security as a Service): 클라우드 서비스 모델로서 보안 솔루션을 제공

6) XDR(Extended Detection and Response): 보안 제품과 데이터를 간소화된 솔루션에 통합하여 최적화된 보안을 제공하는 서비스형 소프트웨어 도구

❍ 3세대 이후 사이버 공격이 본격화되었으며, 5세대부터 AI(인공지능) 기술을 도입한 새로운 유형의 사이버 공격 증가

- (3세대) 취약점을 겨냥한 공격은 방화벽·백신·IDS(침입탐지시스템) 등으로 쉽게 탐지 및 방어가 불가능하여 IPS(침입방지시스템)로 진보
- (4세대) 국제적인 스파이 활동이나 대규모 개인정보 유출 등을 노린 사이버 공격 등장으로, 이를 방지하기 위한 '안티봇'과 '샌드박스' 기술 등장
- (5세대) 사이버 공격이 진화함에 따라 이전 세대의 보안 솔루션들을 통합 보안시스템으로 발전시킴

〈표 10〉 **사이버 공격과 대응방안**

구분	사이버 공격(창)	사이버 보안(방패)
1990년대 ~ 2000년대 초반	- 컴퓨터 바이러스 - 웜(Worm) - 트로이 목마 - 서비스 거부(DoS/DDoS) 공격	- 안티바이러스 소프트웨어 설치 및 주기적인 업데이트 - 데이터 백업을 정기적으로 수행 - 이메일 첨부 파일 또는 링크 클릭하기 전에 확인 후 열기 - 서비스 공급자(ISP)와 협력 - 안티바이러스 및 방화벽 사용
2000년대 중반 ~ 2010년대 초반	- 스팸 - 스미싱(SMS 피싱) - 스파이웨어 - 봇넷	- 스팸 또는 광고 메일을 받기 전에 확인 - 문자 메시지나 메신저 등으로부터 수상한 링크를 열기 전에 확인 - 침입 탐지 시스템(IDS) 및 침입 방지 시스템(IPS)등의 보안 솔루션 사용 - 해킹이 의심되는 이메일, 링크, 파일 등은 확인 후 오픈
2010년대 중반 ~ 현재	- 랜섬웨어 - 디도스(DDoS) - APT(Advanced Persistent Threat) - 사이버 스파이 - 클라우드 서비스 공격	- 주기적인 백업 및 최신 보안 패치 적용 - 트래픽 임계값 설정 및 충분한 서버 용량 확보 - 데이터를 암호화하여 클라우드에 저장 - SASE, SECaaS 등 도입 - EDR, XDR 솔루션 적용

자료 : 당행 작성

2. 주요국의 사이버 보안 현황

❑ 사이버 보안을 강화하기 위한 제로 트러스트 적용과 잠재적 취약점을 보호하기 위해 소프트웨어 명세서(SBOM) 도입 필요

○ 미국이 사이버 보안 행정명령으로 제로 트러스트(Zero Trust)[7]를 의무화
- 미국뿐만 아니라 일본, 대만, 호주 등 다양한 국가에서 활발하게 도입과 발전 방향 논의

○ 국가 사이버 보안 안건으로 논의되는 소프트웨어 공급망 보안
- 미국을 포함한 주요 국가는 소프트웨어 공급망 보안 강화를 구체적으로 실현할 수 있는 방안으로 소프트웨어 명세서(SBOM)[8] 도입을 검토

〈표 11〉 주요국 사이버 보안 현황

국가	주요 내용
미국	- 제로 트러스트 아키텍처 구현 및 공급망 보안 강화에 집중 · 제로 트러스트 아키텍처를 美 연방정부에서 구현하도록 요구
EU	- 보안 취약점을 선별하고 관리하는 수단으로 SBOM을 제시 · 사이버 보안 관리가 필요한 업계를 중심으로 보안 가이드라인을 발표
영국	- 제로 트러스트 구조의 설계 원칙 제시 및 사이버파워[9]에 필수적인 기술 선도 · 영국 내 AI 기업을 지원하여 글로벌 우위 확보, 텔레콤 장비 공급망 다양화 추진
중국	- 제로 트러스트에 대한 관심 증대 및 비즈니스 역량 강화를 위한 데이터 개발 · '21년 IT 기업들이 데이터 개발 플랫폼의 개발 및 출시에 투자를 확대
이스라엘	- 제로 트러스트 솔루션 개발 및 출시 · 사이버 보안 기업들이 제로 트러스트 솔루션을 개발하고 시장에 출시(`21년)
한국	- '데이터보호 핵심기술 개발 전략'을 수립하고 발표(`21.11) · '가명정보 재식별 등 중요데이터를 안전하게 보호하기 위한 암호기술 개발

자료 : 한국인터넷진흥원(2023.02), '미국·EU·영국 등의 사이버 보안 전략 분석 및 시사점' 및 당행 재구성

7) 제로트러스트(Zero Trust): "아무것도 신뢰하지 않는다"를 전제로 한 사이버 보안 모델

8) SBOM(Software Bill of Materials): 소프트웨어의 구성요소를 식별하기 위한 명세서로 오픈소스의 이름과 버전, 외부 개발사와의 프로젝트명 등을 기록해 향후 취약점이나 장애, 업그레이드 시 애플리케이션 코드 구성을 파악하기 위한 것

9) 사이버파워: 5G/6G, AI, 블록체인, 반도체, 암호인증, IoT 등 기존 및 신흥기술

〈참고 3〉 **사이버 보안 정책 방향 및 단계**

❑ **주요국은 디지털 환경변화 및 패러다임 변화에 적시 대응할 수 있는 국가 차원의 사이버 보안 전략을 지속해서 발표**

○ 사이버 보안의 중요성이 국가안보(안전, 경제, 사회 등) 차원으로 확대
- 우크라이나-러시아 전쟁으로 촉발된 사이버전(戰), 주요 기반 시설에 대한 테러 등으로 사이버 보안 전략의 수립·개정, 거버넌스, 법·제도 개편

주요국 사이버 보안 전략 및 핵심 키워드

국가	주요 내용
미국	- 국가안보전략('22.10) · 국가 경쟁력 강화, 글로벌 협력, 사이버·기술·기후·에너지·경제·무역 보안 등 - CISA 전략계획 2023~2025('22.09) · 사이버 공간의 방어 및 복원력, 주요 기반 시설 및 네트워크 보호, 사고 대응 능력 향상, 정보 공유의 강화, 사이버안보·기간시설안보국(CISA) 조직 통합 등
EU	- 사이버방어정책('22.11) · 회원국 간 강력한 사이버 방어 공동 대응, 민간 커뮤니티 공조 강화, 사이버 복원력 강화, 사이버 방어 핵심 기술 개발, 사이버 보안 동맹 강화 등
영국	- 국가사이버전략 2022('22.12) · 사이버 생태계 강화, 사이버 복원력, 사이버 파워에 필수적인 기술, 사이버 보안 글로벌 리더십, 사이버 공간의 국가보안 강화
프랑스	- 국가전략 2022('22.11) · 강력하고 신뢰할 수 있는 핵 억지력, 단합 및 회복력, 프랑스 산업의 전쟁 지원 노력, 최고 수준의 사이버 복원력, 프랑스의 동맹 위상 등
독일	- 사이버 보안전략 2021('21.09) · 디지털 환경에서의 자기결정권, 국가와 기업의 사이버 보안 공동 대응, 지속 가능한 국가 사이버 보안 아키텍처, 국제 사이버 보안의 적극 역할
일본	- 新 사이버 보안전략 2021('21.09) · 디지털 대전환과 사이버 보안, 사이버 공간 전체의 안전 확보, 사이버 공격에 대한 안전 확보 및 동맹·우방국 협력 강화

자료 : 한국인터넷진흥원(2023.02), '미국·EU·영국 등의 사이버 보안 전략 분석 및 시사점' 및 당행 재구성

3. 사이버 보안 위협 및 사이버 공격 주요 사례

❑ 디지털 전환 가속화로 생활 밀접 온라인 서비스 확산, 금품요구 악성 프로그램 및 디도스 공격 증가

○ 사회적 이슈를 악용한 피싱, 스미싱(SMS 피싱), 해킹 메일 유포 및 지능형 지속 공격 등 사이버 위협 증가

- 2023년 사이버 공격 유형은 피싱·스캠(18%) > 디도스(12%) > 가상자산 탈취(5%) > 공급망 공격(4%) 순으로 조사

· 2023년 1분기 한국인터넷진흥원에 접수된 사이버 침해사고 신고 건수는 347건으로 전년 대비 58% 증가

- 2022년 사이버 공격 유형은 피싱(44%) > 스캠(33%) > 스파이웨어/멀웨어(22%) > 랜섬웨어(20%) 순으로 조사

· (국내) 공급망, 정보유출, 랜섬웨어, 디도스, 사회적 이슈 악용 지속 등

· (해외) 랩서스(LAPSUS$), 킬넷 등 글로벌 해킹 조직의 활동 증가

〈표 12〉 2022~2023년 국내외 사이버 보안 위협 사례

구분		국내	해외
2023	1분기	- LGU+ 개인정보 유출 - 지닥(GDAC) 가상자산 분실 - 인터파크 개인정보 유출	- 스위스 연방정부 디도스(DDoS) 공격 - 트위터 이메일 등 개인정보 유출 - 美 T모바일(이동통신사) 개인정보 유출
2022	1분기	- '심스와핑' 피해 - '삼성전자' 소스코드 유출 - 'LG전자' 임직원 계정 유출	- NVIDIA社 정보 유출 - MS社 소스코드 유출 ※ 러시아·우크라이나 무력 전쟁(2.24)
	2분기	- 방송사 유튜브 계정해킹 - '밀리의 서재' 고객정보 유출	- 美 T모바일 소스코드 유출 - 이탈리아 정부 디도스(DDoS) 공격
	3분기	- 콜택시 중계사 랜섬웨어 감염 - 기업 귀신 랜섬웨어 감염 - 정부 유튜브 계정 해킹	- 미국 의료기관 대상 랜섬웨어 공격 - 美 하원의장 대만 방문 중 디도스 공격 - '라자루스' 에너지 기업 공격
	4분기	- 카카오 장애 악용 - 이태원 사고 악용 해킹메일 ※ 카카오 서비스 장애(10.15)	- '킬넷' 美 재무부 공항 공격 - 호주 통신사 TPG 해킹 ※ 美 중간선거(11.08)

자료 : 과학기술정보통신부(2022.12), '2023년 사이버 보안위협 전망' 및 당행 재구성

❑ 스위스 연방정부 사이트 마비 및 교육부 개인정보 탈취(`23.06)

○ 디도스(DDoS) 공격으로 스위스 연방정부 사이트를 마비시키고, 교육부 서버에 침투하여 개인정보를 탈취하는 등 국가안보를 위협한 사건

- (사이버 공격) '노네임(NoName)'이라는 집단이 디도스(DDoS) 공격으로 연방정부가 관리하는 포털사이트를 비롯해 여러 행정부 웹사이트를 마비시키고 교육부 서버에서 개인정보를 탈취
  · 디도스 공격은 대량의 데이터를 전송해 시스템 장애를 발생하게 하는 사이버 공격으로 해킹 단체는 디도스 공격으로 스위스 연방정부 사이트를 접속불가 상태로 마비시킴
  · 해킹 단체는 교육부 서버에서 개인정보를 탈취해 금품을 요구

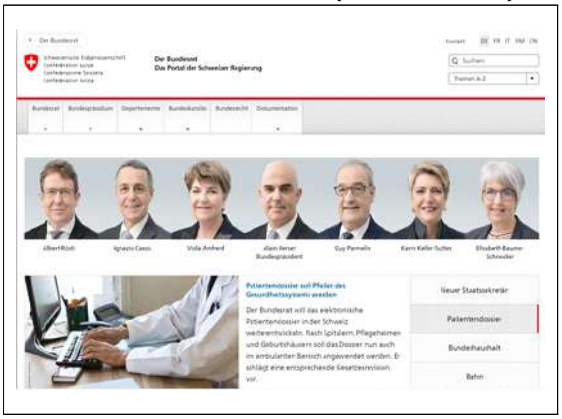
- (피해 규모) 연방정부 포탈사이트가 마비되고, 다크웹에 개인정보 유출 및 피해
  · 연방정부 포털사이트(www.admin.ch) 접속 불가
  · 교육부 서버 해킹 표적으로 학생 224명, 교사 195명, 교육부 공무원 342명 등의 개인정보가 다크웹에 게시

- (사이버 보안) 사이버 공격 피해 사실을 즉시 신고 및 공유하고 공격 방법 분석을 통한 예방책 마련
  · 국립사이버보안센터가 공격 내용을 분석하고 대응책 마련
  · 스위스 정보당국은 사이버 요원을 활용해 23년 말까지 사이버 테러를 방지하기 위한 해커 관련 정보 수집

〈그림 5〉 스위스 연방정부 청사

자료 : 언론사(KBS) 뉴스기사에서 발췌, 2023

〈그림 6〉 연방정부 사이트(www.admin.ch)



자료 : 연방정부 사이트(www.admin.ch)에서 발췌, 2023

❑ 가상자산거래소 G사 해킹(`23.04)

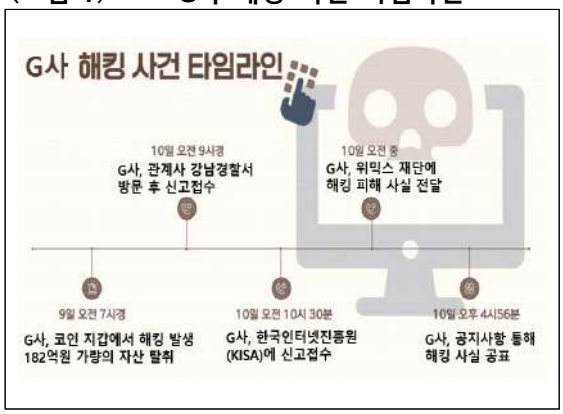
○ G사가 해킹 공격으로 보관 중인 가상자산의 23%를 분실한 사건

- (사이버 공격) 내부 인프라 시스템 침투로 인한 가상자산 해킹
  · 가상자산 트랜잭션 내역을 분석한 결과 해킹 방식이 거래소 코인 지갑의 비밀키 유출보다는 내부 인프라 시스템 침투로 추정
  · 국내 정보보안 기업 티오리에 분석 의뢰한 결과 스윕[10] 트랜잭션을 이용해 이용자 → 거래소 → 해커 경로로 코인 탈취

- (피해 규모) 전체 자산의 약 23%(현재 시세 약 180억원)에 해당하는 가상자산 분실
  · 비트코인(BTC) 60여개, 이더리움(ETH) 350여개, 위믹스(WEMIX) 1,000만개, 테더(USDT) 22만개 등 분실

- (사이버 보안) 시스템 보안성 검토 및 자산 충당을 완료하여 입출금 재개와 서비스 정상화
  · 경찰과 한국인터넷진흥원(KISA), 금융정보분석원(FIU) 등에 신고 및 공유
  · 해킹된 물량 전액 충당 및 보전하였으며, 입출금 재개는 페이코인, 스텔라루멘, 코스모스, 이더리움클래식을 제외한 나머지 코인을 먼저 입출금 재개
  · OTP(1회용 비밀번호) 및 비밀번호를 일괄 초기화하여 재설정 요청

〈그림 7〉 G사 해킹 사건 타임라인



자료 : 언론사(Daum) 뉴스기사에서 발췌, 2023

〈표 13〉 G사 피해자산

(단위 : 개)

피해자산	피해수량(합계, 개)
비트코인	60.81
이더리움	350.50
위믹스	10,000,000
테더	220,000

자료 : 언론사(지디넷코리아) 뉴스기사에서 발췌, 2023

10) 스윕(Sweep): 거래소 회원들이 가상자산을 입금함으로써 '사용자 입금용 지갑'에 자산이 쌓이면 이를 모아서 거래소 핫월렛(온라인 지갑)으로 보내는 것

❑ L사 개인정보 유출(`23.01) 및 서비스 장애(`23.02)

○ L사에 가입한 고객 29만 명의 개인정보가 해킹되었고, 일주일 동안 5차례 디도스(DDoS) 공격으로 전국 인터넷망 장애가 발생

- (사이버 공격) 29만 명의 개인정보(전화번호, 이름, 주소 등이 포함) 해킹
  · 해커는 원격으로 웹 서버에 공격 명령을 실행하는 '웹셸'[11] 방식으로 정보를 탈취 및 '포트 스캔'[12]을 통해 디도스 공격

- (피해 규모) 29만 명의 개인정보 유출 및 피해 지원센터에 접수된 인터넷 접속 오류 2,284건
  · 유심(USIM) 무상교체와 'L사 스팸전화알림' 서비스 무료 제공이 요구
  · 디도스 공격으로 피해입은 개인고객 약 427만 명에게 장애시간 대비 10배에 달하는 요금을 감면

- (사이버 보안) IT 자산 통합관리시스템 개선으로 개인정보 유출 대비 및 정보보안 투자 규모 확대, 트래픽 우회 등을 통해 디도스 공격 대응
  · 홈페이지를 통해 개인정보 유출 여부 조회할 수 있는 서비스 지원
  · 연간 정보보호 투자액 1,000억원으로 3배 증액

〈그림 8〉 L사 개인정보 유출 공지사항

자료 : 언론사(전자신문) 뉴스기사에서 발췌, 2023

〈표 14〉 L사 서비스 장애 현황

날짜	인터넷 장애 발생 시점	총 장애 시간
1/29	- 새벽 2시 - 오후 5시 - 오후 11시 등	- 63분
2/4	- 오후 4:57~5:30 - 오후 6:07~6:23	- 59분

자료 : 언론사(Chosun Biz) 뉴스기사에서 발췌, 2023

11) 웹셸(Web Shell): 공격자가 원격에서 웹서버에 명령을 수행하도록 올린 스크립트 파일이며, 웹서버의 피해 공격 중 약 90%에서 웹셸이 발견

12) 포트 스캔(Port Scan): 운영 중인 서버에서 열려있는 포트를 검색하는 것

❑ 美 송유관 랜섬웨어 사건(`21.05)

❍ 미국 최대 송유관 업체가 랜섬웨어 공격으로 모든 시설 운영이 중단되어 미국 유가에 영향을 준 사건

- (사이버 공격) '다크사이드'라는 랜섬웨어 공격으로 송유관 8,850km 구간 폐쇄 후 금품을 요구
  · 피싱 공격 수행 및 인터넷에 노출된 시스템 계정정보 탈취
  · 민감 데이터를 유출하고 파일을 암호화하여 금품을 요구

- (피해 규모) 美 남·동부 일대 석유의 45% 이상을 점유하는 파이프라인 시스템이 6일간 가동 중단
  · 미국 유가에 영향(연료값이 2~3%상승)
  · 해커들에게 500만 달러(약 56억 5,000억원)의 비트코인을 지불

- (사이버 보안) 랜섬웨어 예방과 대응 체계 구축 및 정부 지원
  · 美 바이든 대통령의 사이버 보안 강화에 초점을 둔 행정명령 발표('21.05)
  · 송유관 시설의 사고 신고 의무화 등 제도 개선 추진

〈그림 9〉 송유관 랜섬웨어 사건 구간

자료 : 언론사(조선일보) 뉴스기사에서 발췌, 2021

〈그림 10〉 송유관 사건 개요

자료 : 언론사(조선일보) 뉴스기사에서 발췌, 2021

❑ U사 이더리움(ETH) 탈취(`19.11)

❍ U사 해킹 공격으로 이더리움 34만 2,000개 유출 사고

- (사이버 공격) U사에서 이더리움 34만 2,000개(약 580억원)가 알 수 없는 지갑으로 전송
  · 탈취된 가상화폐는 하나의 지갑으로 옮겨진 뒤, 1일 후 다른 지갑으로 분산되었으며, 여러 개의 분산된 지갑으로 출금

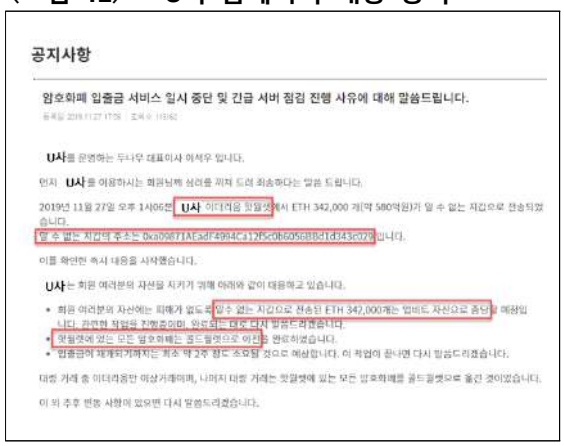
- (피해 규모) 이더리움 34만 2,000개(약 580억원) 비정상 출금
  · 100% U사 자산으로 충당

- (사이버 보안) 핫월렛(Hot Wallet)[13] → 콜드월렛(Cold Wallet)[14] 이전하여 인터넷과 단절된 상태 유지 및 즉각적인 대응으로 추가 피해 예방
  · 해킹 피해가 발생한지 5시간도 안되서 해킹 피해 공지
  · 입·출금 서비스 일시 중단(2주간)
  · 분실된 이더리움(ETH)을 U사 자산으로 충당
  · 이상거래감지시스템(FDS)를 고도화

〈그림 11〉 U사 이더리움 사건경위

자료 : 언론사(Daum) 뉴스기사에서 발췌, 2019

〈그림 12〉 U사 홈페이지 대응 공지



자료 : U사 홈페이지 공지사항에서 발췌, 2019

13) 핫월렛(Hot Wallet): 온라인 상태의 지갑
14) 콜드월렛(Cold Wallet): 오프라인 상태의 지갑

❑ 워너크라이(WannaCry) 또는 워너크립트(WannaCrypt)(`17.05)

❍ 랜섬웨어 공격이 순식간에 전 세계 100여 개국으로 확산되는 등 역사상 전례가 없는 최악의 해킹으로 간주되고 있는 워너크라이 사태

- (사이버 공격) 영국, 러시아 등 150여 개국에 대규모 피해를 발생시킨 랜섬웨어(Ransomware)의 일종
  · 랜섬웨어에 감염되면 컴퓨터 내의 파일들이 암호화되며, 파일 몸값으로 비트코인 $300(한화 68만원)을 요구하는 메시지 창이 화면에 출력
  · 감염 시점에서 비트코인 $300(처음) → $600(3일 후) → 파일 삭제(7일 후)

- (피해 규모) 150여 개국 20만대 이상의 컴퓨터에서 감염
  · 국내 4,000건이 넘는 워너크라이 계열 랜섬웨어 탐지
  · CGV를 포함한 정식으로 피해 신고된 기업은 9곳이며, 감염 의심 건수는 13건

- (사이버 보안) 네트워크 단절, 감염경로 차단, 보안 업데이트 등을 수행
  · 네트워크 단절: 랜선 단절, 와이파이 끄기
  · 감염경로 차단: 방화벽 설정 변경
  · 보안 업데이트: 윈도우 보안 패치 실행, 백신 프로그램 업데이트

〈그림 13〉 워너크라이 윈도우즈 배경화면 변경

자료 : 소프트캠프, 2017

〈그림 14〉 워너크라이 금전 요구 창 생성

자료 : 소프트캠프, 2017

Ⅲ. 시사점

❑ 국내 사이버 보안 산업의 경쟁력을 높이기 위해 1) 사이버 보안 기술 고도화 및 2) 사이버 보안 산업 생태계 활성화 필요

○ (사이버 보안 기술 고도화) 차세대 기술(인공지능, 머신러닝 등)을 접목한 실시간 탐지·대응 기술 등을 통해 사이버 보안 기술 고도화
- 제로 트러스트 모델 도입, 암호기술 및 AI 기반 기술과 융합하여 사이버 보안 기술을 고도화

○ (사이버 보안 산업 생태계 활성화) 국제 표준 사이버 보안 인증 취득과 오픈소스 역량 강화를 통해 국내 시장에서 글로벌 시장으로 확대할 수 있는 산업 생태계 조성
- 사이버 보안 관련 인증을 취득하여 글로벌 시장 공략 체계 마련, 오픈 체인 프로젝트(Open Chain Project)[15] 참여를 통해 글로벌 오픈소스 역량 확보 필요

〈표 15〉 사이버 보안 기술 확보 전략

사이버 보안 기술 고도화	사이버 보안 산업 생태계 활성화
- 제로 트러스트(Zero Trust) 보안 도입 · 개인정보 보호와 데이터 보안을 강화하기 위해 제로 트러스트 모델 적용이 필요	- 글로벌 시장 공략 · 사이버 보안 관련 국제 표준 사이버 보안 인증 취득 및 관리 필요
- 암호기술 및 AI 보안기술 고도화 · 데이터 보호를 위한 암호기술(동형암호, 양자내성암호 등) 고도화 · AI를 활용한 데이터 보호 기술(연합기술, 재현데이터 등)을 통해 사이버 보안기술 강화	- 글로벌 오픈소스 역량 확보 필요 · 오픈 체인 프로젝트 지속적 참여

자료 : 당행 작성

15) 오픈체인 프로젝트(Open Chain Project): 기업의 오픈소스 소프트웨어 체계 및 컴플라이언스 역량을 평가해 국제 인증을 부여하는 제도

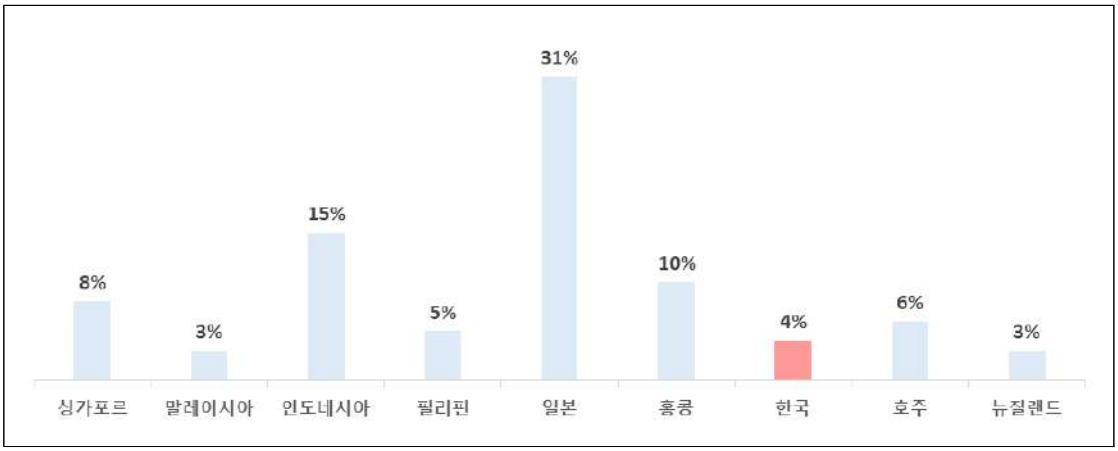
1. 사이버 보안 기술 고도화

❑ 제로 트러스트 모델 도입에 대한 필요성을 높이고, 국내 상황에 맞는 사이버 보안 강화 정책을 마련

○ 전반적인 통합 모니터링 강화, 데이터 암호화, 화이트리스트 기반의 접근제어 등 복합적인 방법으로 제로 트러스트 구현 필요

- 재택·원격근무, 클라우드 도입 등으로 변화하는 업무 환경과 진화하는 사이버 위협 등에 대응하기 위해 최소 권한 접근, 보안 가시성 확보 등에 기반한 제로 트러스트로 보안 패러다임 전환 필요
- 사이버 범죄로부터 기업의 중요 정보자산을 지키기 위해 다른 국가들은 제로 트러스트 모델을 주목하고 있음
  · 제로 트러스트 보안을 진행 중인 한국 기업은 4%에 불과('21년 결산 기준)

〈그림 15〉 APAC 지역 Zero Trust 보안 현황 리포트



자료 : Okta(2022.08), '2021년 APAC 지역 Zero Trust 보안 현황'

○ 국가안보와 국민 보호 및 경쟁력 강화를 위한 사이버 보안 강화 정책 요구

- 클라우드, 비대면 환경 등 새로운 보안 패러다임에 대응하기 위하여 국가 주요 정보통신기반시설, 공공기관 등에 제로 트러스트 아키텍처를 우선적으로 도입할 예정
- 국내 상황에 맞는 기술을 연구·개발하여 가이드라인 발간 및 국내 사이버 보안 관련 정책과 체계 등에 대한 세밀한 검토가 필요

❑ 암호기술 및 AI 기반 기술의 융합과 기존 단점 개선 등을 통해 사이버 보안 기술을 고도화

❍ (암호기술) 동형암호[16], 양자내성암호[17] 등의 단점 보강과 기술 관련 투자를 확대하여 기술 고도화 필요

- 동형암호 기술의 단점인 암호화 후 데이터 크기 증가로 평문 대비 데이터 처리 속도가 느려지는 문제를 해결하는 기술 필요
- 양자내성암호 알고리즘의 이론적 취약점 또는 구현 과정에서 발생 가능한 취약점 검증 및 지속적인 연구개발 필요
  · 일반적으로 양자내성암호는 계산이 복잡하여 암호화 및 복호화(암호화 해제) 작업에 많은 리소스와 시간이 필요
  · 양자내성암호 기술을 적용하기 위해서는 알고리즘 표준화가 선행되어야 함

〈표 16〉 암호기술 동작 방법 예시

동형암호	양자내성암호
	
[내용] 암호화된 상태에서 연산할 수 있는 기술로 데이터를 복호화(암호화 해제)하지 않아도 연산이 가능해 정보 유출 방지가 가능 - 기존 암호화 기술 1→A, 2→B일 때, A + B=? (연산불가) - 동형암호 기술 1→A, 2→B일 때, A + B=3 (연산가능)	[내용] 양자컴퓨터를 이용한 공격에도 해킹이 불가능한 차세대 암호기술 - 기존 암호기술은 양자컴퓨터로부터의 공격에 정보보호가 불가능하나, 양자내성암호 기술은 양자컴퓨터를 이용한 공격에도 정보보호가 가능

자료 : 과학기술정보통신부(2021.11), '데이터보호 핵심기술 개발 전략' 및 당행 재구성

16) 동형암호(Homomorphic Encryption): 평문과 암호문의 동형 성질로 인해 암호문 상태에서도 연산이 가능한 차세대 암호기술

17) 양자내성암호(Post-Quantum Cryptography): 양자컴퓨팅 환경에서 안전하게 암호기술을 이용할 수 있도록 하는 새로운 공개키 암호

○ (AI 보안) AI 기반 연합학습[18] 및 재현데이터[19] 등 단점 보완 기술을 확보하고, 지속적인 연구개발을 통해 기술 우위 확보

- AI 연합학습에서는 통합 모델의 안정성이 저하되는 단점 개선
- 재현데이터 기술에서는 실제 데이터와의 불일치로 인해 예측 정확도가 감소하는 단점 개선

〈표 17〉 AI 보안 기술 동작 방법 예시

AI 연합학습	재현데이터
	
[내용] 스마트폰에서 학습된 여러 AI 모델을 중앙 서버에서 취합하여 정교하게 만든 후 재배포하여 향상된 AI 모델을 만드는 학습 방식	[내용] 실제로 측정된 데이터를 바탕으로 유사한 통계적 성질을 보이는 가상의 데이터를 만들어 민감정보를 외부에 노출하지 않아 데이터 유출을 방지

자료 : 과학기술정보통신부(2021.11), '데이터보호 핵심기술 개발 전략' 및 당행 재구성

❑ 글로벌 환경에서 사이버 보안 주도권확보를 위해 선제적으로 미래 기술(6G 보안, 양자 보안기술 등)에 대해 전략 대응방안 마련

○ 6G 서비스에는 가상자산의 거래가 확대될 것으로 예상됨에 따라 양자 암호기술 등의 선제적 투자를 바탕으로 원천기술 확보 필요

- 양자 암호기술 특허출원 관련하여 한국은 미국과 비교 시 약 1/3에 불가하므로 적극적인 투자를 통한 기술 추격 필요
  · 양자기술 특허출원 비율: 미국(31.6%) > 일본(16.2%) > 중국(13.2%) > 한국(10.2%)(자료: '23년 특허청 융복합기술심사국 보도자료 발췌)

18) AI 연합학습(Federated Learning): 자신의 데이터는 안전하게 보관하고, AI를 학습하는 방법만 공유하기 때문에 프라이버시와 보안 문제 해결이 가능

19) 재현데이터(Synthetic Data): 민감정보를 외부에 노출하지 않고 AI 기반의 가공된 데이터 사용 가능

2. 사이버 보안 산업 생태계 활성화

❑ 국내 사이버 보안 기업은 국제 표준 인증 취득과 오픈소스 역량 강화를 통해 글로벌 비즈니스의 발판 마련 필요

○ 국내 사이버 보안 시장의 경우 해외 업체와 비교 시 시장 규모가 작고 자금 조달이 어려워 국내 시장에만 집중하고 해외 시장을 공략하지 못하고 있음

- 국내 사이버 보안 시장은 PC 백신 등 솔루션을 저가에 판매하고, 유지보수로 수익을 확보하는 영세적 구조
- 국내외 상위 10개 기업을 대상으로 매출액 비교 시 해외 10개 기업의 합산 매출액은 187조 3,774억원이며, 국내 10개 기업의 합산 매출액은 1조 2,497억원으로 약 150배 차이('22년 결산 기준)

〈표 18〉 국내외 사이버 보안 기업(2022년 매출액 기준 상위 10개)

(단위 : 억원)

순위	국내 기업명	매출액	순위	해외 기업명	매출액
1	㈜에스케이쉴더스(사이버 보안)	3,887	1	Cisco(미국)	670,360
2	㈜안랩	2,164	2	Accenture(아일랜드)	592,081
3	㈜시큐아이	1,376	3	Deloitte(영국)	352,273
4	㈜이글루코퍼레이션	1,030	4	Palo Alto Networks(미국)	77,623
5	㈜윈스	1,014	5	Fortinet(미국)	55,703
6	한국정보인증㈜	876	6	McAfee(미국)	29,785
7	㈜지란지교시큐리티	654	7	CheckPoint(이스라엘)	29,380
8	㈜파이오링크	616	8	CrowdStrike(미국)	28,262
9	이니텍㈜	538	9	Okta(미국)	23,429
10	라온시큐어㈜	468	10	Rapid7(미국)	8,639

자료 : 각 사 IR자료 및 당행 재구성(환율은 2022.12.30. 매매기준율 적용)

❍ 국내 사이버 보안 기업은 해외 시장으로 진출하기 위해 국제 표준 사이버 보안 인증을 취득하여 글로벌 시장 공략 체계 마련

- 사이버 보안 관련 인증인 'UNECE R-155'[20], 'ISO/IEO 27001:2022'[21], 'IEC 62443'[22] 등을 취득하여 글로벌 시장을 공략 필요
  · '22년 07월 이후 개발에 들어가는 모든 자동차는 사이버 보안 관리체계 인증(UNECE R-155) 취득이 요구되며, 유럽 경제위원회 협약국에 출시가 가능
  · 정보통신기획평가원(IITP)은 ISO/IEC 27001:2022를 취득하여 정보보호와 개인정보보호 분야에 대한 관리체계를 강화하고 있음

❍ 오픈 체인 프로젝트 참여를 통해 글로벌 오픈소스 역량 확보 필요

- 오픈체인 프로젝트에 참여하고 있는 국내 사이버 보안 기업은 전무하며, 현재 주요 대기업(삼성, 현대, 엘지 등) 및 테크기업(네이버, 카카오 등)이 참여 중
  · 국내 사이버 보안 기업은 오픈체인 프로젝트의 국제 표준인증(ISO/IEC 5230)[23]을 취득하여 기술 역량 확보 필요

〈그림 16〉 국내 오픈체인 프로젝트 참여 기업

자료 : OPENCHAIN 홈페이지 및 당행 재구성

20) 유럽경제위원회(UNECE): 산하 차량 기준 국제조화 회의(WP.29)에서 차량 사이버 보안에 관한 법규 2개를 채택(R-155: 차량 사이버 보안 관리체계, R-156: 차량 소프트웨어 업데이트 관리체계)

21) ISO/IEC 27001: 국제표준화기구/국제전기기술위원회에서 제정한 정보보호 관리체계에 대한 국제 인증

22) IEC 62443: 산업 보안 국제 표준으로 산업 통신망의 위험 완화를 목적으로 고안되었으며, 사이버 보안에 대한 전체적인 접근방식을 제공

23) ISO/IEC 5230: 리눅스 파운데이션의 오픈체인 프로젝트에서 만든 규격으로 소프트웨어 공급망 내 신뢰할 수 있는 오픈소스 컴플라이언스를 보장하기 위한 최소한의 핵심 요구 사항

참고문헌

[국문자료]

경찰청(2022), “2021년 경찰통계연보”
과학기술정보통신부(2021), “데이터보호 핵심기술 개발 전략“
_____(2022), “과학기술&ICT 정책·기술 동향”
_____(2022), ”디지털 대전환시대 정보보호산업의 전략적 육성 방안“
_____(2022), ”2023년 사이버 보안위협 전망“
_____(2023), “LGU+ 침해사고 관련 재발방지 대책 마련 및 시정조치 요구”
금융보안원(2022), ”2023 디지털금융 및 사이버보안 이슈 전망”
국가정보원(2022), “2022 국가정보보호백서“
김기문(2023), ”양자시대 안전한 차세대 암호기술 개발 및 대응 방안“, 한국인터넷진흥원
김도원, 하병욱, 김성훈(2023), “미국·EU·영국 등의 사이버 보안 전략 분석 및 시사점”, 한국인터넷진흥원
김소정(2023), “2023 미국 사이버안보 전략 주요내용과 한국에의 시사점”, 국가안보전략연구원
김수진(2022), “글로벌 사이버 보안, 보안의 새 원칙: 아무도 믿지 마라(Zero Trust)!”, 미래에셋증권
김태은(2022), “사이버 보안 오케스트레이션 및 자동 대응 기술”, 정보통신기획평가원
문가용(2023), “2022년 글로벌 사이버 보안 업체 주요 M&A“, 시큐리티월드
박경민(2021), ”다크웹의 현황 및 시사점”, KDB산업은행
박창현, 임현(2023), "데이터 보안 시대의 10대 미래유망기술", 한국과학기술기획평가원
소프트캠프(2017), ”워너크라이 랜섬웨어 리서치 리포트“
송왕철(2022), ”2022 Zero Trust Architecture“, 한국지능정보사회진흥원
송태은(2023), ”최근 사이버 위협의 추세와 향후 전망 및 국제사회의 대응“, 외교안보연구소
쉬만스카 알리나(2019), ”이스라엘 사이버 안보전략” 국제문체연구소
에스케이쉴더스(2022), ”EQST 2022 상반기 보안 트렌드“
_____(2023), ”EQST 2023 상반기 보안 트렌드“
오일석, 조은정(2022), “미국 사이버전략의 평가와 전망“, 국가안보전략연구원
옥타(OKTA)(2022), ”2021년 APAC 지역 Zero Trust 보안 현황“
이글루코퍼레이션(2022), ”2023년 보안 위협·기술 전망 보고서”
이후기(2022), “제로 트러스트 보안기술 동향과 적용방안”, 한국문화정보원

조은정(2022), “영국「국가사이버전략 2022」의 특징과 시사점”, 국가안보전략연구원
최성호(2020), “4차 산업혁명의 숨은 원동력, 오픈소스 현황과 시사점“, KDB산업은행
한국신용정보원(2019), “사이버 보안 시장보고서”
한국인터넷진흥원(2021), “AI 보안 관련 국내외 동향조사 및 기술수준 분석”
_____(2022), “2021 글로벌 정보보호 산업시장 동향조사“
한국정보보호산업협회(2022), ”2022년 국내 정보보호산업 실태조사”
황원섭(2021), “보안 운영 끝판왕, SOAR! 이것만은 알고가자“, SPLUNK

[영문자료]

Chainalysis(2023), ”The 2023 Crypto Crime Report“
Gatner(2022), ”Market Share Analysis: Consulting Services, Worldwide, 2021“
_____(2023), ”Top Trends in Cybersecurity 2023“
IDC(2023), ”Cybersecurity Macro Trends and the Implications for Security Professionals“

[인터넷 자료]

ITWORLD, itworld.co.kr