

GROWTH RESEARCH

2025.06.26 (목)

[사이버 보안 산업보고서]

AI는 공격도, 방어도 한다.
보안의 판이 바뀐다!

Analyst. 한용희, 박재은

목차

- Part 1. AI 위협 시대, 사이버 보안의 판이 달라진다
- Part 2. 스테이블 코인 확산, 사이버 보안의 중요성 부각
- Part 3. 사이버 위협, 이제는 총과 미사일만큼 위협적
- Part 4. 강화되는 처벌과 제도, 민간 보안 시장도 커진다
- Part 5. 관련기업

기업분석

지니언스(263860)

드림시큐리티(203650)

Intro

사이버 보안은 디지털 환경에서 사이버 위협 및 공격에 대응하고 안전을 확보하기 위한 기술을 의미한다. 코로나 19 팬데믹 이후 급 성장한 가상 네트워크 환경과 ChatGPT, Deepseek 등과 같은 학습형 AI의 등장으로 사이버 공격은 현대 비즈니스 사회에서 기업의 지속 가능성을 위협하는 중대한 리스크 중 하나로 자리잡았다.

기존 공공 부문 중심의 사이버 보안 시장은 국방, 공공기관, 금융 등의 규제산업을 중심으로 투자가 이루어졌으며, 정부 보조금 기반의 국가 예산 주도 프로젝트가 대부분을 차지했다. 또한 보안의 목적이 정보 유출 방지에 국한되어 있어 사이버 보안 솔루션의 수요가 한정적인 구조로 진행되어 왔으나, 최근 발생한 두차례의 민간 기업 사이버 공격 사태를 거치면서 국내에서 비교적 미비했던 사이버 유출 처벌 제도가 강화되어 민간 부문 보안 시장의 확장을 이끌어낼 것으로 전망된다.

본 보고서에서는 AI 확산에 따른 사이버 보안의 중요성 및 공공에서 민간까지 영역이 확대되는 사이버 보안의 전망을 분석한다.

Part 1. AI 위협 시대, 사이버 보안의 판이 달라진다

디지털 환경의 성장은 디지털 공격을 부른다

사이버 보안은 디지털 환경에서 사이버 위협 및 공격에 대응하고 안전을 확보하기 위한 기술을 의미한다. 코로나 19 팬데믹 이후 급 성장한 가상 네트워크 환경과 ChatGPT, Deepseek 등과 같은 학습형 AI의 등장으로 사이버 공격은 현대 비즈니스 사회에서 기업의 지속 가능성을 위협하는 중대한 리스크 중 하나로 자리잡았다.

AI 발전의 양면성

특히 AI의 등장은 사이버 보안의 수요를 비약적으로 증가시키는 요인 중 하나이다. AI는 신경망 학습을 위한 데이터 수집, 활용 등으로 개인정보 보안 문제의 중요도를 더욱 높일 뿐만 아니라 AI 자체가 사이버 공격의 도구로써 사용되기도 한다.

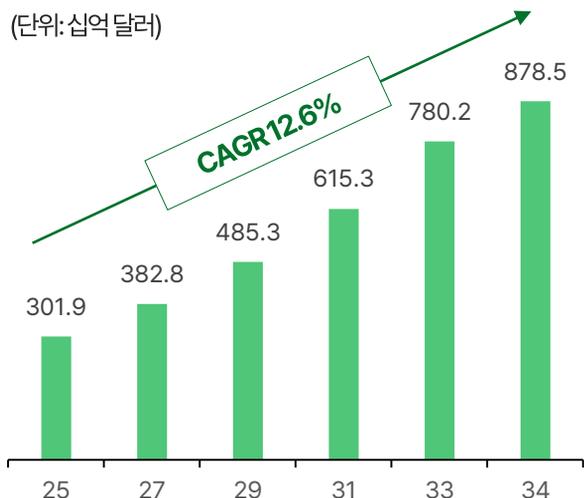
AI로 생성된 악성 코드의 수는 2024년에 전년 대비 125% 증가했으며, 일일 생성되는 악성 코드의 수는 45만개에 이른다. 또한 사이버 위협에 AI가 활용되면서 랜섬웨어 공격이 전년 대비 67% 증가했다. Palo Alto Networks Unit 42 연구에 의하면, LLM(AI 언어 모델)을 이용해 하나의 악성 스크립트를 10,000여 개의 변종으로 자동 생성할 수 있으며, 이 중 88%가 탐지 우회에 성공해 AI를 활용한 사이버 공격의 수준은 나날히 위협해지고 있다.

시장 규모는 가파르게 성장할 전망

글로벌 시장 조사 업계에 따르면, 전세계 사이버 보안 시장 규모는 '34년까지 연평균 12.6%씩 성장하여 약 8,784억 달러 규모로 매우 빠르게 큰 규모의 시장으로 성장할 것으로 전망된다.

전세계 사이버보안 시장 규모 전망

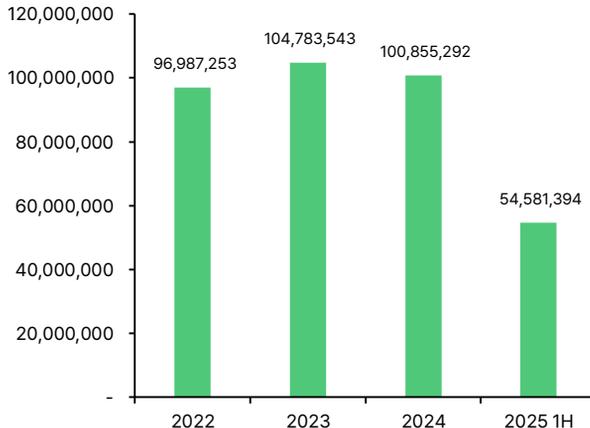
(단위: 십억 달러)



자료 : Precedence Research, 그로스리서치

매년 악성코드 감지 건수

(단위: 건)



자료 : AV-ATLAS, 그로스리서치

Part 2. 스테이블 코인 확산, 사이버 보안의 중요성 부각

공공에서 민간까지
영역 확장되는
사이버 보안

사이버 보안 시장은 공공 부문 뿐만 아니라 민간 부문에서도 빠르게 확장되고 있으며, 최근 발생한 두차례의 민간 기업 사이버 보안 위협 사태를 통해 사이버 유출 처벌 제도가 강화되는 방향으로 이어지며 민간 부문 보안 시장의 확장이 가속화될 것으로 보인다.
공공 부문에서의 사이버 보안 시장은 크게 금융과 국방에서의 중요성이 커지고 있다.

전세계적인 디지털
자산 도입 움직임

지난 6월 10일, 민병덕 더불어민주당 의원이 스테이블 코인 사전 인가제 도입 등을 골자로 한 디지털자산기본법 발의를 밝힌 바에 따라, 원화 기반 스테이블 코인 발행 허용 여부에 대한 관심이 높아지고 있다. 이미 미국에서 스테이블 코인 전용 법안인 '지니어스 액트'를 상원에서 통과시킨 것에 이어 EU, 일본 등의 주요국 또한 스테이블 코인을 비롯한 디지털 자산의 전방위 규제를 도입하는 등 제도화 움직임을 보이고 있는 추세이다.

스테이블 코인 등 디지털 자산이 제도권 안으로 편입될 시, 클라우드 기반의 금융 거래가 확산됨에 따라 해킹·피싱·계정 탈취 등 보안 위협을 방어하기 위한 보안 솔루션 수요가 폭발적으로 증가할 가능성이 높다. 스테이블 코인과 같은 디지털 자산 시장에서는 사이버 보안 문제가 안정성과 직결되는 중요한 이슈로, 디지털 자산 시장의 제도화가 본격적으로 이루어진다면 사이버 보안 시장도 세계적인 규모로 크게 성장할 것으로 보인다.

GENIUSACT 주요내용

핵심 항목	주요 내용
발행자 자격 요건	정부 허가 받은 금융회사만 스테이블코인 발행 가능
준비금 및 투명성	달러나 국채 등으로 1:1로 준비금 보관, 매달 공개해야 함
규제 범위 및 법적 지위	주식이 아니라 금융상품으로 분류, 금융법 적용됨
외국 발행자 정부 권한	미국에서 팔려면 똑같이 규제 대상, 어기면 벌금·제재

자료 : 그로스리서치

스테이블코인 주요해킹방식

해킹 방식	설명
스마트 계약 취약점	스마트 계약의 버그(재진입, 잘못된 로직 등)를 이용해 담보 자산 탈취
준비금 인프라 침해	중앙화 발행사의 서버, 지갑 등을 해킹해 무단 발행 또는 자산 탈취
피싱 & 소셜 해킹	유저를 속여 개인 키 또는 서명을 유도해 지갑에서 자산 탈취
러그풀 & 가짜 토큰	위조된 토큰이나 프로젝트를 만든 뒤 투자금을 먹튀
플래시론 공격	대규모 단기 차입으로 가격을 인위적으로 조작하고 차익 실현

자료 : Chainalysis, 그로스리서치

Part 3. 사이버 위협, 이제는 총과 미사일만큼 위협적

최근 2-3년 내에 발발하여 현재 진행 중인 러시아-우크라이나 전쟁과 이란-이스라엘 전쟁의 사례를 통해 **국가 간 물리적 충돌 뿐만 아니라 사이버 공격(사이버전)이 병행이 확인되며 물리적 전쟁과 함께 사이버 인프라 보호가 국가안보의 핵심 요소로 부상**하고 있다.

물리적 분쟁 + 사이버 분쟁 대응의 필요성

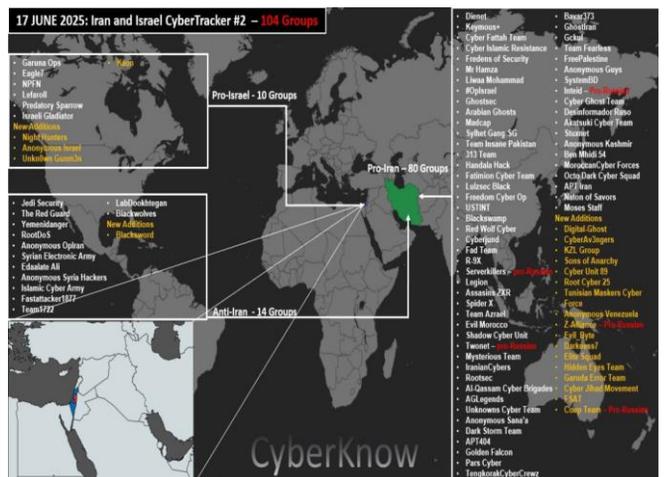
러-우 전쟁에서는 침공 전후로 러시아 해커 그룹에 의해 우크라이나의 군사 및 정부 시스템의 수백 차례의 사이버 공격이 가해졌으며, 최근에는 이란과 이스라엘 간 군사 충돌이 본격화됨에 따라 각국의 해커들에 의한 은행 서비스 마비 및 정보 유출 공격이 발생하고 있다. 또한 해커 그룹들의 공격 범위는 비단 이란과 이스라엘 뿐만 아니라 요르단, 사우디, 이집트 등 주변국은 물론 미국까지 확산 조짐을 보임에 따라 **주변국의 군사적 충돌 및 지정학적 리스크에 따른 사이버 보안 수요의 급증은 불가피한 것으로 보인다.**

4차 산업혁명 기술 지키는 것도 사이버 보안

물리적 충돌 외에도 미국과 중국 간의 경우 AI를 비롯한 산업 및 무역의 패권 경쟁이 이뤄지며 **양자, AI, 로봇 등 핵심 4차 산업혁명 기술 보호의 중요성 또한 국가안보 차원에서 중요성**이 커지고 있다. 이에 사이버 공격을 통해 원천 기술을 절취하려는 국가 차원의 시도가 늘어날 가능성도 무시할 수 없다. **미국은 사이버 공간 보호를 국가안보 최우선 분야의 하나로 표명**하고 있으며, 영국도 사이버안보를 제1의 국가안보 위기로 규정하고 있다.

러시아-우크라이나 사이버 공격

이스라엘-이란 사이버전 양상



자료 : MDPI, 그로스리서치

자료 : DarkReading, 그로스리서치

Part 4. 강화되는 처벌과 제도, 민간 보안 시장도 커진다

올해 상반기 들어 발생한 SK텔레콤 해킹 사태, 예스 24 랜섬웨어 사태 등 두 차례의 대규모 사이버 공격이 민간 기업의 보안 취약점을 드러내면서 **국내에서 비교적 미비했던 사이버유출 처벌 제도가 본격적으로 강화될 것**으로 보인다.

국내에선 아직 미비한 사이버보안 움직임

실제로 스위스 국제경영개발대학원이 발표한 국가 경쟁력 평가 중 사이버 보안 부문에서 한국은 20위('24년)에서 40위('25년)까지 추락했다. 또한 이동통신 3사와 네이버, 카카오 등 주요 IT 기업의 매출 대비 정보보호 투자 비율이 0.5%가 채 되지 않음이 드러나며 사이버 보안의 핵심인 '사후 수습 보다 사전 예방'의 모토가 제대로 이루어지고 있지 않음을 여실히 보여준다.

두차례 사이버 공격, 민간기업 정보보안 규제 강화

SK텔레콤 해킹 사태 등 해킹 피해 사례가 이어지며 기업 정보보호 역량을 강화하기 위한 법안이 발의됐다. **지난 6월 11일에 발의된 정보통신망 이용촉진 및 정보보호 등에 관한 법률 개정안에는 정부가 부여하는 정보보호 및 개인정보보호 관리체계(ISMS-P) 인증 기준을 강화하여, 해당 법령을 중대하게 위반할 경우 인증을 취소하고 과징금을 부과하는 내용이 포함된다.**

또한 지난해 12월에는 '절대 신뢰하지 말고, 항상 검증하라'라는 보안 철학을 도입한 제로트러스트 아키텍처 도입 및 운용 가이드라인 2.0이 발간되며 민간 주도의 사이버 보안이 달성될 수 있도록 하는 정부차원에서의 노력이 드러난다.

개인정보보호법체계 변화

항목	변화 내용	핵심 포인트
유출 통지 기한 명문화	72시간 이내 정보주체 및 개인정보위에 유출 사실 통지 의무	GDPR 기준에 맞춘 글로벌 스탠다드 정비
책임자 처벌 방식 변경	CPO 등 실무자 형사처벌 폐지, 대신 기업에 과징금 부과 중심 전환	개인 → 법인 책임 전환으로 실제 책임소재 명확화
과징금 강화	과징금 = 해당 기업 매출의 최대 3%, 최대 20억 원까지 부과 가능	대기업 실질 부담을 반영한 구조
유출 사후 의무 신설 (개정안)	2년간 다크웹·텔레그램 등에서 불법 유통 모니터링 → 결과 보고 의무화+ 불법 확인 시 의무 고발 제도 도입 예정	'유출 → 통지'에서 끝나지 않고 '감시 → 추적 → 고발'로 이어지는 다층 구조로 강화 중

자료 : 청년의사, 그로스리서치

Part 5. 관련기업

사이버 보안 관련기업

(단위 : 억원)

기업명	기업개요	시가총액
지니언스 (263860)	<ul style="list-style-type: none"> '05년 설립. '17년 코스닥 상장 주요 사업: 정보 보안제품의 판매와 솔루션 도입 및 용역 제공 매출 비중:보안 솔루션 제품 81.6%, 용역 18.4% NAC 분야 국내 조달 시장 75% 점유율 차지하며 사실상 시장 독점 국내 IT 환경 맞춤형 솔루션 제공으로 외산 제품 대비 경쟁 우위 확보 	1,961
드림시큐리티 (203650)	<ul style="list-style-type: none"> '98년 설립. '17년 코스닥 상장 주요 사업: 공개키기반(PKI)의 보안 솔루션 공공-민간 부문 제공 매출 비중: 산업용기계 렌탈 및 보호솔루션 서비스 86.03%, 국방 보안 솔루션 6.55%, 개인정보 보호 서비스 3.51% 등 스테이블 코인 등 디지털자산 제도권 내 도입 본격화되며 디지털 아이디, 전자지갑 등 PKI 원천기술 보유한 동사 수혜 기대 	2,024
라운시큐어 (042510)	<ul style="list-style-type: none"> '98년 설립. '00년 코스닥 상장 주요 사업:FIDO 기반 생체 인증, 블록체인 디지털 ID, 모바일/PC 보안 솔루션 매출 비중: 솔루션 39.6%, 서비스 60.4% FIDO 인증(NFC/생체) 시장 선두주자, 최근 모바일 장애인등록증 구축 사업 수주 받으며 관련 사업 공공·민간 프로젝트 수주 기대 	1,470
파수 (150900)	<ul style="list-style-type: none"> '00년 설립. '13년 코스닥 상장 주요 사업: DRM(문서 보안), DLP, 데이터 보호 및 문서 관리 솔루션 제공 매출 비중: 데이터보안 45.1%, 애플리케이션보안 6.0%, 유지관리 47.4% 디지털 자산 보호 수요 증가에 따른 문서보안 수요 꾸준할 전망 글로벌 SaaS형 DRM, DLP 제품 출시로 해외시장 확대 기대 	629
슈프리마 (236200)	<ul style="list-style-type: none"> '00년 설립, '08년 코스닥 상장 주요 사업: 지문·얼굴 인식 기반 바이오 출입통제 시스템, 물리보안 솔루션 매출 비중:통합보안시스템 72.65%, 바이오인식 솔루션 15.78% 출입통제 및 AI 융합 솔루션으로 스마트 빌딩·공공시장 확대 및 글로벌 140개국 이상 수출 기반으로 시장 확장성 확보 	2,536

자료 : 그로스리서치

지니언스(263860)

20년 흑자·보안시장 독점... 민간 시장도 확장 중

투자포인트

NAC, EDR, ZTNA 보안 소프트웨어 판매 기업

동사는 '05년에 설립되어 '17년 6월 코스닥 시장에 상장한 기업이다. 동사는 정보 보안 소프트웨어 기업으로, 정보 보안제품의 판매와 솔루션 도입 고객에 대한 유지관리 및 용역을 제공하고 있다. 현재 상용화 및 개발 중인 대표 솔루션은 NAC, EDR, ZTNA로 구분되며 매출 비중은 제품이 81.6%, 용역 18.4%로 구성된다.

20년간 실적 연평균 성장률 24%, 지니언스

동사는 보안 소프트웨어 기업 중에서도 흔히 않은, **설립 후 20년 동안 흑자 경영을 달성한 기업**이다. '05년 매출액 8.4억원에서 '24년 매출 496.1억원으로 설립 이후 **연평균 23.9%의 꾸준한 실적 성장세**를 보여주고 있다. 이러한 실적 성장의 배경에는 국내 NAC 시장에서 압도적인 점유율(조달 시장 기준 75%)을 차지한 동사의 NAC 제품이 있다. NAC는 내부 네트워크에 접속하려는 장비 및 사용자를 식별하고 인증 후 통제하는 네트워크 접근 제어 솔루션으로, 내부 정보의 유출 가능성을 막는 보안 역할을 담당한다. **B2G에서 B2B/B2C로 제품 판매 대상이 확장되고 있으며, 1Q25에는 비수기임에도 불구하고 영업이익의 흑자 전환에 성공**하며 규모가 커진 산업 내에서 안정적인 수익창출을 이룩하고 있음을 확인할 수 있다.

AI 위협의 핵심 보안 솔루션, EDR 해외시장 개척 완료

NAC 외의 주력제품인 EDR은 사용자의 PC, 서버 등 단말기에서 발생하는 행위를 감시하고, 이상 행위 탐지하는 보안 솔루션으로, 동사는 **구축형(On-Premise) EDR을 자체 개발해 국내 EDR 시장에서 점유율 1위를 차지**하고 있다. **전세계적으로도 구축형태의 EDR을 납품할 수 있는 업체는 전세계적으로 적은 편**이며, 이러한 강점을 바탕으로 중동 고객사로 부터 직접 도입 요청을 받아 납품을 하게 되었다. **해당 레퍼런스를 바탕으로 해외시장 진출을 통한 침투 시장 확대도 기대**된다.

국내 NAC 시장 1위

민간 중심 확장되는 사이버 보안에 발맞춰 동사 EDR도 기대

20년간 매출 추이



자료 : 지니언스, 그로스리서치
그로스리서치 GROWTH RESEARCH

글로벌 고객분포도



자료 : 지니언스, 그로스리서치

드림시큐리티(203650)

스태이블 코인 시대의 보안 파트너

투자포인트

PKI 보안 알고리즘 기반 보안 솔루션 판매 기업

동사는 '98년 8월에 설립되어 '17년 1월 코스닥 시장에 특례상장한 기업이다. 동사는 정보보안 기술 제품 및 서비스를 판매하는 기업으로, 공개키기반(PKI)의 보안 알고리즘을 기반으로 공공-민간 부문 보안 솔루션을 제공한다. 매출 비중은 산업용기계 렌탈 및 보호솔루션 서비스 86.03%, 국방 보안솔루션 6.55%, 개인정보 보호 서비스 3.51% 등으로 구성된다.

디지털자산 시장에 필요한 보안 솔루션 모두 준비 완료

PKI는 데이터를 주고 받을 때 지정한 사람들만 데이터를 열 수 있도록 포장해주는 보안 기술로, 전자서명/인증서/생체 인식 등 본인 확인 기술과 온라인 정보보호에 적용된다는 특징을 가진다. 드림시큐리티는 이러한 **PKI 보안 알고리즘을 기반으로 전자서명 원천기술을 보유해 다수의 공공기관과 금융권에 전자서명, 인증, 암호화 기반 솔루션을 공급한 바 있다.** 최근 삼성전자와 카카오가 블록체인 기반 결제 시스템 및 디지털 자산 지갑 개발을 가속화하며, 그 핵심 인프라 중 하나인 보안 시스템 구축을 위한 협력사로 동사가 떠오르고 있다.

동사는 블록체인, 디지털 아이디(DID, 분산 신원 관리), 지갑형 인증 솔루션 등 인증 및 암호화 기반 보안 솔루션 라인업을 보유 중이며, 사용자의 단말과 서버간 보안을 모두 제공할 수 있는 엔드-투-엔드 보안 기술 보유 기업으로서 디지털 자산 시장의 개화가 가속화될 수록 수혜를 입을 것으로 기대된다.

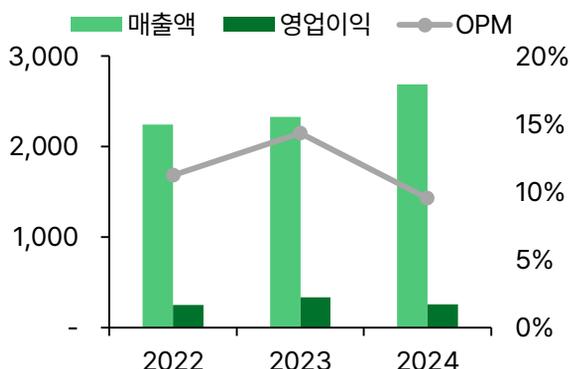
보안·인증 솔루션 관련 매출, 이젠 날아오를 때

동사의 외형 성장의 직접적인 요인은 자회사 한국렌탈의 산업용기계 렌탈 매출의 성장이나, 지난 수년간 보안·인증 부문에서 DID 및 전자지갑 연구 개발 등을 통해 꾸준한 실적치를 유지하고 있다. 또한 **전세계적인 디지털자산 시장 제도권 도입 움직임이 활발해지면서 동사의 보안 솔루션 매출의 성장이 기대된다.**

스태이블 코인 등 디지털자산 도입 수혜 기업

꾸준한 실적 유지, 이젠 날아오를 때

실적 추이



자료 : DART, 그로스리서치

PKI 설명



자료 : 드림시큐리티, 그로스리서치

Compliance Notice

- 동 자료에 게재된 내용은 조사분석담당자 본인의 의견을 정확히 반영하고 있으며, 외부의 부당한 압력이나 간섭 없이 작성되었음을 확인합니다.
- 동 자료는 투자 판단을 위한 정보제공 및 교육용일 뿐 해당 주식에 대한 가치를 보장하지 않습니다.
- 투자판단은 본인 스스로 하며, 투자행위와 관련하여 어떠한 책임도 지지 않습니다.
- 동 자료는 고객의 주식투자의 결과에 대한 법적 책임소재에 대한 증빙 자료로 사용될 수 없습니다.
- 당사는 해당 자료를 전문투자자 또는 제 3자에게 사전 제공한 사실이 없습니다.
- 동 자료의 작성자는 해당 기업의 유가증권을 발간 전에 보유하고 있지 않으며, 발간 후에 매수·매도할 수 있습니다.
- 동 자료에 대한 저작권은 그로스리서치에 있습니다. 당사의 허락 없이 무단 복사 및 복제, 대여를 할 수 없습니다.