I 최근 사이버보안 기술·산업 동향 및 시사점[1)]

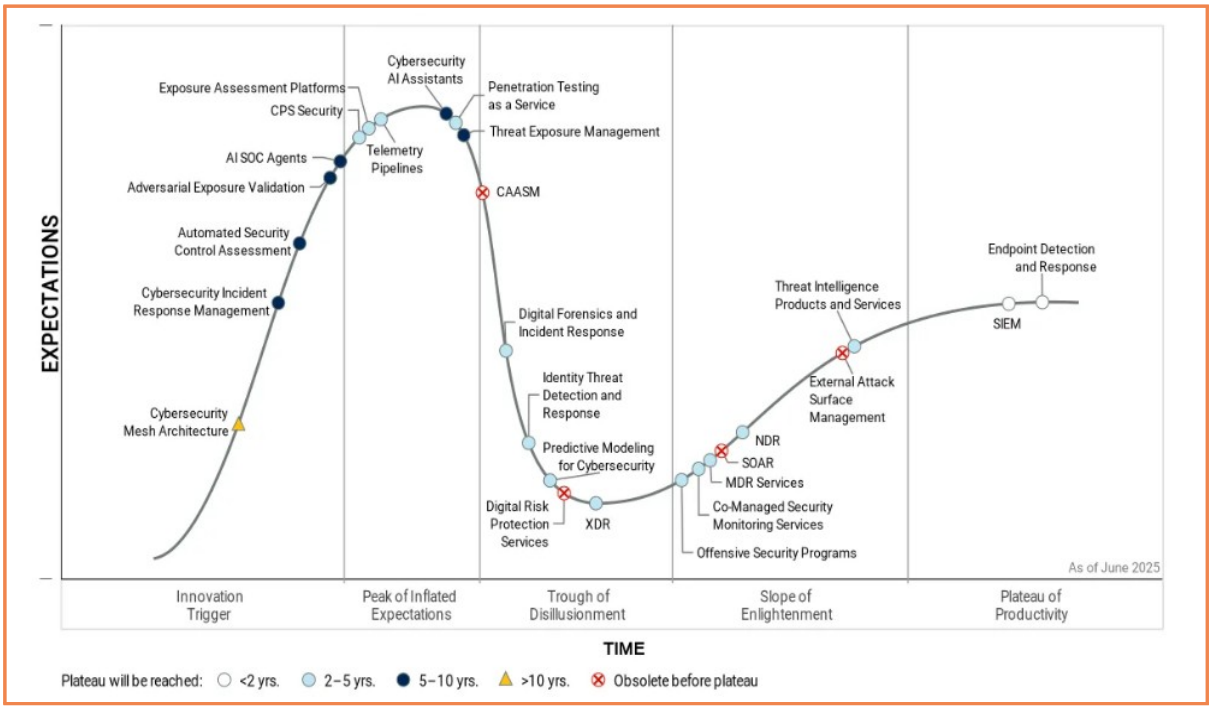
사이버보안은 ICT 및 전 산업의 초연결화, 디지털화와 인공지능(AI)·양자 등 기술 발전이 가속화됨에 따라 영역 확장 및 중요성, 복잡성이 점차 증가

- AI·데이터·인프라·융합 보안을 중심으로 세계시장은 '24년 3,843억 달러에서 연평균 13.1% 성장률로 '30년 8,233억 달러로 확대 전망
- 국내 시장은 '24년 35.9조 원에서 연평균 13.1% 성장을 통해 '30년 68.6조 원 규모의 시장을 형성할 전망

최근 AI 위협 대응 및 활용 기술 등이 관심의 최고점 단계에 진입

- 초지능형 공격 시대를 맞이하여 AI 기반 자율 보안 및 ICT와 산업 간 융·복합화에 효율적으로 대응을 위한 지능형 사이버보안 기술 주권 확보가 매우 중요

〈 사이버보안 기술 분야 관련 하이프 사이클 〉



출처 : Gartner(2025.8.), Hype Cycle for Security Operations, 2025

국가 안보·경제·사회를 지켜주는 사이버보안 분야의 전략적 기술 역량 확보 필요

- AI 자율 보호와 양자 내성 암호, 제로 트러스트 등 AI 강국 실현에 필수인 사이버보안 핵심기술의 글로벌 경쟁력 확보 및 사회 재난·안전 대응, 산업생태계 조성 요구

1) 정보통신기획평가원 AI반도체·SW단 조일구 수석연구원(cho19@iitp.kr)
본 고는 저자의 개인적인 견해이며 과학기술정보통신부와 KISTEP의 공식적인 의견이 아닙니다.

1 사이버보안 기술 개요

(개념 및 범위) 정보보호 및 전 산업의 초연결화, 디지털화로 야기되는 고도의 사이버 위협 대응 등 국민의 실생활에서 안전과 자산을 보호하는 신기술

- AI 등 기술 발전에 따라 사이버보안 영역이 확장 중이며, 산업과 ICT 융복합 현상이 가속화됨에 따라 사이버보안 대상도 점차 확대

〈 사이버보안 기술 범위 및 개념도 〉

출처 : 정보통신기획평가원(2025.11.13.), ICT 기술전망 컨퍼런스 사이버보안 분야

(기술 분류) 공통 보안, 디지털 취약점 분석·시스템 보안, 네트워크·클라우드 보안, 융합 보안, 물리보안 기술 등으로 크게 구분

- (공통보안) 암호, 인증·인가 및 데이터 라이프 사이클 전반에 대한 보호와 신뢰성 보장 기술, AI의 오남용 및 역기능 대응을 위한 AI 기술
- (디지털 취약점·시스템 보안) 하드웨어(HW)와 소프트웨어(SW)의 보안 취약점 분석 및 무결성 확보·검증, 악성코드 분석·탐지·차단, 디지털증거를 수집·분석하여 사실을 규명하는 디지털포렌식, 보안 위협 요소의 근원지 역추적 기술
- (네트워크·클라우드 보안) 유무선 네트워크에 연결된 데이터, 서비스, 네트워크 보호 및 클라우드 서비스 보호, ICT 인프라 환경에서 위협과 공격 탐지·분석·대응 기술
- (물리·융합보안) 휴먼·바이오 인식, 지능형 CCTV 보안 등 물리보안 및 가상/증강현실 등 가상 융합 보안, 모빌리티 보안, 항공·우주·의료 보안 기술 등 포함

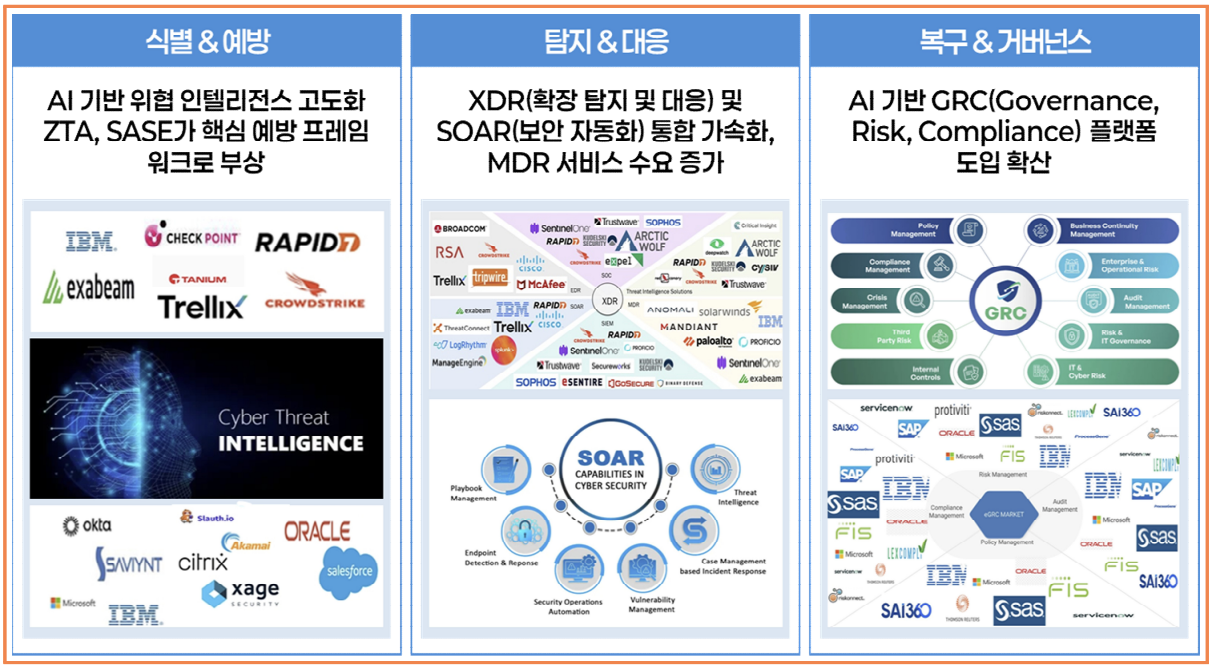
2 국내외 산업 및 시장, 정책 동향

(산업 동향) 사이버보안 산업의 가치사슬(Value Chain)은 AI, SW 공급망, 통합 플랫폼화, 인수합병(M&A), 자동화된 위협 대응 중심의 신생기업 탄생이 주요 이슈

- 최근 AI 기반 대응·탐지 기술은 위협 인텔리전스로부터 사고대응까지 통합하고, 공급망 보안은 가치사슬 전 단계의 근본적인 위험관리가 핵심 축으로 성장
  - (위협 인텔리전스) AI 기반 자동화 위협 및 에이전틱 AI 공격이 급증함에 따라 실시간 위협 탐지의 필요성 증가 및 다크웹/서드파티 위험의 감시 강화
  - (탐지) 행위 기반 사용자·기기·계정의 위험 탐지 기술 수요가 급증하고 있으며, AI 대규모언어모델(LLM)에 대한 위험 프롬프트 삽입에 대한 탐지 필요성이 부상
  - (대응) 위협 자동 분석 및 AI 기반 코파일럿(Copilot) 대응 체계가 필요하며, 평균 탐지·대응 시간 단축을 위한 업체 간 경쟁이 심화
  - (복구 및 회복) 랜섬웨어 및 클라우드의 설정 오류로 인한 대규모 피해가 증가함에 따라 무결한 백업체계와 복원 시스템 도입 중요도가 증가
  - (규정 준수 및 거버넌스) AI 사용의 법적 통제 및 감사 체계의 강화, ESG·NIS2· GDPR 등 다국적 컴플라이언스 참여 및 대응이 필수

* ESG : Environmental, Social, Governance, NIS2 : Network & Information Systems Directive 2, GDPR : General Data Protection Regulation

〈 사이버보안 분야의 주요 이슈 및 플레이어맵 〉

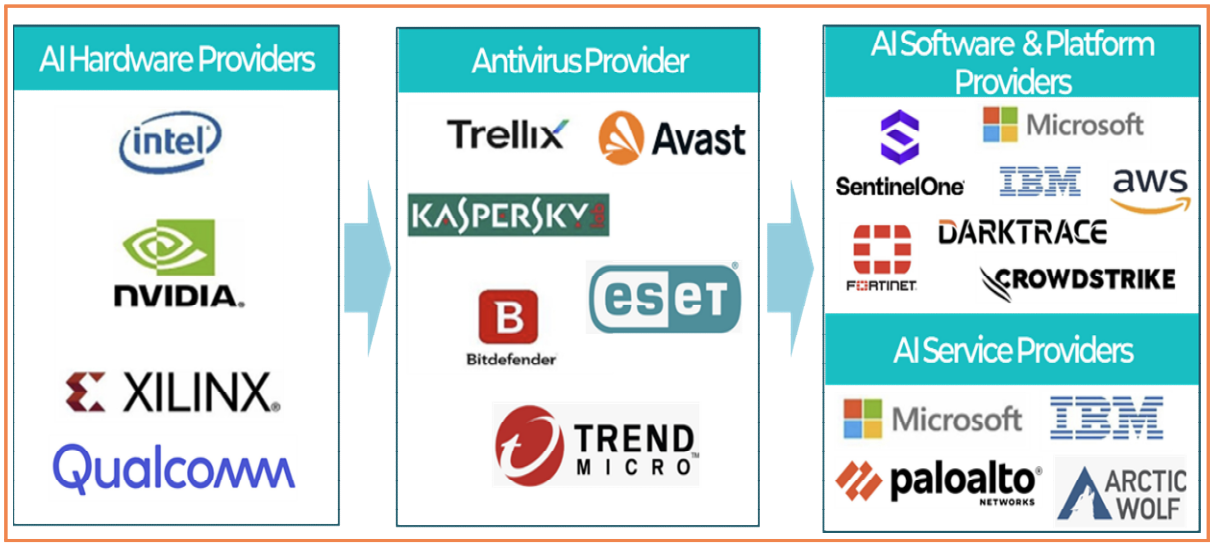


출처 : 정보통신기획평가원·윕스(2025.12.), 사이버보안 분야의 2025년 ICT 트렌드 분석 보고서

● AI 산업이 주류가 되면서 사이버보안 생태계도 AI HW 공급업체, AI SW 및 플랫폼 공급업체, AI 서비스 공급업체, 안티바이러스 공급업체 중심으로 재편

- (AI HW 공급업체) NVIDIA, Intel, AMD, Qualcomm 등이 핵심 플레이어
  * (NVIDIA) '24년 Trend Micro와 협업하여 데이터센터 보안용 AI 솔루션을 공동개발 및 NVIDIA의 NIM(Near In Memory) 및 Morpheus 플랫폼을 Trend Vision One에 통합하여 실시간 위협분석 및 대응을 강화, AI 성능을 대폭 강화한 GeForce RTX 50 시리즈와 함께, AI 슈퍼컴퓨팅용 GB10 'Blackwell' 시리즈를 공개
  * (Intel) '25년까지 Core Ultra 시리즈 및 NPU 통합 CPU 1억 대 이상 출하 목표로 자체 AI PC 생태계 구축 및 개발자 도구 생태계(oneAPI 등) 강화 중
- (안티바이러스 공급업체) Trellix, Avast, Ttren Micro 등이 핵심 플레이어
  * (Trellix) Trellix Security Platform에 AI 기반 탐지·응답 기능 강화, Trellix Wise GenAI 기능으로 엔드포인트, 이메일, 클라우드, 데이터 등 전 범위 위협 대응 지원
- (AI 소프트웨어 공급업체) SentinelOne, Darktrace, CrowdStrike, IBM, Fortinet, Microsoft, AWS 등이 핵심 플레이어
  * (SentinelOne) '25 RSAC에서 Athena Agentic 기능을 내장한 Purple AI Athena 발표, 이를 통해 보안 분석가의 사고·정책 결정을 모방하는 보안 자동화 에이전트 도입
  * (Darktrace) 클라우드 데이터 수집 전문기업 Cado Security를 인수해 AI 기반 보안 포렌식 역량을 강화하고, 강화된 머신러닝 기반 Cyber AI Analyst를 업데이트하여 경고 및 자동 조사, 사고 우선순위 지정 기능을 대폭 개선
- (AI 서비스 공급업체) IBM, Microsoft, Palo Alto Networks, Arctic Wolf, Secureworks 등이 핵심 플레이어
  * (IBM) Agentic AI 기반 보안 운영 자동화 시스템인 ATOM(Autonomous Threat Operations Machine) 출시로 위협 탐색·분석·대응을 최소 인력으로 수행, AI 보안과 거버넌스를 통합 관리하는 기업용 통합 AI 거버넌스 플랫폼을 업계 최초 출시

〈 사이버보안용 AI 주요 가치사슬 주요 플레이어맵 〉



출처 : MarketsandMarkets(2023.12.), Artificial Intelligence in Security Market

(시장 동향) 세계 사이버보안 시장은 '24년 3,843억 달러에서 연평균 13.1% 성장하여 '30년 8,223억 달러 규모의 시장 형성 전망

- '공통 보안'은 양자 내성 암호 전환 및 AI 확산에 따른 디지털 역기능 이슈, '디지털 취약점 분석·시스템 보안'은 공급망 보안 규제 요구 증가 및 오픈소스 사용 확대, 사이버 위협 고도화 및 다양화로 지속 확대
  - '네트워크·클라우드 보안'은 산업용 IoT(Internet of Things) 등과 융합되는 5G 고도화 및 클라우드 확산에 따른 위협 증가, '융합/물리 보안'은 산업과 ICT 융합, IoT 적용, 감시 및 보안 수요 확대, 가상 융합 보안 등이 지속 성장

〈 사이버보안 분야의 시장 전망 〉

(단위 : 세계시장 백만 달러, 국내시장 십억 원)

구분		2024	2025	2026	2027	2028	2029	2030	CAGR
공통보안	세계	99,373	117,274	138,428	163,439	193,028	228,060	269,552	18.2%
	국내	2,294	2,628	3,015	3,457	3,968	4,555	5,233	13.9%
디지털 취약점 분석·시스템 보안	세계	59,910	66,210	73,490	81,480	90,610	100,540	111,623	11.0%
	국내	4,764	5,277	5,850	6,487	7,208	7,999	8,883	11.0%
네트워크·클라우드 보안	세계	38,470	44,028	50,508	58,000	66,668	76,736	88,393	14.7%
	국내	6,750	7,868	9,163	10,648	12,434	14,539	16,980	16.6%
융합보안	세계	59,314	67,461	77,487	88,775	100,465	118,921	141,115	14.4%
	국내	13,983	15,405	16,994	18,763	20,817	23,232	25,962	10.6%
물리보안	세계	127,293	138,240	150,267	163,491	178,041	193,887	211,670	8.7%
	국내	8,136	8,626	9,148	9,703	10,294	10,923	11,592	8.0%
합계	세계	384,360	433,213	490,180	555,185	628,812	718,144	822,353	13.1%
	국내	35,927	39,804	44,170	49,058	54,721	61,247	68,650	11.2%

출처 : 정보통신기획평가원(2025.1.), ICT R&D 기술로드맵(2025~2030) 사이버보안 분야

- 글로벌 시장은 클라우드 기반의 보안 솔루션 도입이 증가하면서 시장경쟁이 심화가 되고 있으며, Cisco, Palo Alto Networks, Fortinet 등 미국 기업이 주도
  - 사이버보안 시장 선점을 위한 ICT 기업들의 참여가 활발하며, 빅테크 기업도 사이버보안 기업에 대한 투자 및 펀딩으로 협업 확대 추세
    * 클라우드 확산 등으로 사이버 공격 빈도와 강도가 높아지고 있어 Google, IBM 등 빅테크 기업들의 보안 주도권 선점을 위한 전략적 M&A 및 투자 확대 중

〈 글로벌 사이버보안 기업 동향 〉

구분	주요 제품 및 서비스
Cisco Systems (미국)	• 차세대 네트워크, 데이터센터, 사이버 보안 등의 분야에서 활약하고 있으며, 전 세계 데이터 트래픽의 80% 이상이 해당 기업의 네트워크 인프라를 활용 • Cisco SecureX, Cisco Secure 솔루션 보유
Palo Alto Networks (미국)	• 네트워크 및 클라우드 보안, 엔드포인트 보호 업체로, '22년 11월에 애플리케이션 공급망 전문업체인 사이더시큐리티(Cider security)를 인수('22) • SASE 솔루션 '프리즈마 새시(Prisma SASE)' 보유

구분	주요 제품 및 서비스
Fortinet (미국)	• 네트워크 보안, 클라우드 보안, AI 기반 보안관제, 사용자 보안, 클라우드 기반 애플리케이션 보안 제품 및 서비스 제공 • 네트워크 방화벽 'NGFW' 솔루션 보유
McAFee (미국)	• 엔드포인트, 엣지 및 클라우드 보안을 포함한 광범위한 사이버보안 플랫폼을 구축하였으며, CASB 공급업체인 '스카이하이 넥스웍스'를 인수 • 맥아피 시큐어 웹 게이트웨이 맥아피(McAfee Secure Web Gateway), DLP(McAfee Data Loss Prevention) CASB M(MVISION Cloud) 및 솔루션인 맥아피 비전 클라우드 플랫폼을 발표
CheckPoint (이스라엘)	• '21년 딜로이트의 '고속성장 500대 기업(Technology Fast 500)'에 선정되었으며, 북미 지역 내 가장 빠르게 성장하는 사이버보안 기업 중 하나로 인정 • 지속적 통합/개발(CI/CD) 파이프라인 보호 기능을 향상시킨 클라우드 네이티브 애플리케이션 보호 플랫폼(CNAPP) '클라우드가드 CNAPP' 출시('23.2)
CrowdStrike (미국)	• '11년 설립하여 사이버 공격 전문 보안기업으로 '22년 9월 공격 통로를 관리해주는 업체인 '리포지파이(Reposify)'를 인수 • 새로운 관리형 확장 탐지 및 대응(MXDR) 서비스인 'CrowdStrike Falcon® Complete XDR' 출시('23)
Okta (미국)	• IDaaS(IDentity-as-a-Service), 제로 트러스트 등 사이버 보안 사업을 확장하고 있으며, 워크플로우 자동화 스타트업인 '아주쿠아(Azuqua)'를 인수
NortonLifeLock (미국)	• 엔드포인트(데이터·이메일·인증서 등)에서 iOS, Android, Window OS 기반의 모바일 단말을 사이버보안 위협으로부터 보호하는 앱 형태의 종합 솔루션 제공
GOOGLE (미국)	• 사이버보안 경쟁력 강화를 위해 시큐리티 스코어카드, 싱크에 투자('21)한데 이어 심플리파이, 멘디언트를 인수('22)하여 기업의 모든 보안 수명주기 단계를 보호하는 보안 운영 제품군을 제공 발표('22.9)
IBM (미국)	• 클라우드 보안 기업 '스파누고' 인수('20.6)에 이어 최근 '폴라시큐리티'을 인수('23.5)

출처 : 정보통신기획평가원(2025.1.), ICT R&D 기술로드맵(2025~2030) 사이버보안 분야

○ 국내 시장은 '24년 35.9조 원에서 연평균 11.2% 성장하여 '30년 68.6조 원 규모로 확대가 예상

- 국내 금융 및 제조 업종의 침해사고 증가에 따라 개인정보 침해, 랜섬웨어, 디도스(DDoS) 공격 등 불특정 다수와 특정 목표를 대상으로 하는 해킹 범죄가 증가하면서 사이버보안에 대한 수요가 확대
- '24년 기준 국내 관련 기업 수는 정보보안 876개(49.2%), 물리보안 904개(50.8%) 등 총 1,780개이며, 지속적 증가 추세(한국정보보호산업협회, '25.10)
- 통합형 차세대 보안 솔루션에 대한 수요가 증가하고 클라우드 기반 서비스의 채택이 증가함에 따라 응용 제품 개발 전문 중소기업의 시장경쟁이 치열해짐

* 국내 사이버보안 빅3 업체인 SK쉴더스, 안랩, 시큐아이가 '클라우드 보안'을 차기 성장동력으로 보고 역량 확보 집중

* 안랩은 AI 학습 기능을 적용하여 사용자와 자산 기반 리스크를 분석 및 대응해 조직의 보안 수준을 높이는 '안랩 XDR', 파수는 sLLM 서비스인 'ELLM' 출시 등 AI 활용 제품 출시 본격화

(정책 동향) 미국, 중국, 유럽 등 주요국들은 사이버보안 관련 국가 전략을 마련하여 국가 사이버 안보 강화 및 사이버보안 분야의 성장동력 확보에 주력

○ 제로 트러스트 네트워크로의 전환, 생성형 AI 출현, 대형 침해사고 발생 등 보안 이슈 대응을 위해 법제도 정비 및 핵심기술 개발에 지속적 투자 확대

〈 사이버보안 분야의 주요국 기술 정책 동향 〉

국가	주요 현황
한국	• 과기정통부를 중심으로 공공·민간의 보안 체계 강화 및 미래 기술 선도에 역점을 두고 추진 – 정보보호산업 육성방안('26.4) : 최근 빈번한 침해사고로 인한 사이버보안 강화 요구를 국내 산업의 성장과 경쟁력 강화의 기회로 삼기 위해 AI·양자 기반 정보보호 산업 육성 추진 – 범부처 정보보호 종합대책('25.10) : 공공·금융 등 1,600여개 IT 시스템의 보안 취약점 점검을 의무화하고, 물리적 망분리 제도를 데이터 보안 중심으로 개편하고, 다중 인증 도입, SW 공급망 보안(SBOM) 제도화, 양자 내성 암호화 기술 도입을 주요 과제로 추진
미국	• 국가 차원의 강력한 사이버 보안, 신기술(AI·양자암호 등)의 안전한 활용, 그리고 공급망 보안을 핵심 정책으로 추진 – 트럼프 행정부의 사이버 전략('26.3) : 미국 우선주의에 기반하여 공격적인 사이버 역량 강화를 명시하고, AI와 양자컴퓨팅 등 차세대 기술에서 패권을 유지하고, 민관 협력을 통해 인프라 및 공급망을 보호하는 포괄적인 사이버 안보 전략 – 사이버보안 강화 행정명령('25.6) : 국가 핵심 인프라를 보호하기 위해 국토안보부(DHS), 국방부(DOD), NIST 등 주요 연방기관에 AI 시스템의 보안 침해 탐지 및 대응 체계 통합 지시하여 SW 개발 프레임워크(SSDF) 기반 실무 가이드라인을 마련하여 기술 공급망 보안 강화
중국	• 정보보호 및 사이버보안 정책은 데이터 주권 확보와 국가 안보를 최우선으로 하며, 관련 핵심 기술(암호화, AI, 클라우드 등)의 개발 및 통제를 강화하는 방향으로 추진 – 국가 사이버보안 산업 발전계획('19.9) : 국가 사이버보안 전략지원, R&D, 첨단산업, 인재육성 등 인프라 구축을 지속적으로 추진 – 핵심기술 자립 : 사이버 위협에 대응하기 위한 자체 정보보호 기술(암호화, 네트워크 방어 등) 개발을 장려하면서도, 개발된 기술과 알고리즘을 국가 사이버 안보 체계 내에서 강력히 통제 – 데이터 및 AI 기술 감독 : 빅데이터 및 생성형 AI 기술 발전과 함께 강화된 보안 요구사항을 적용하여, 클라우드 아키텍처 및 AI 모델 운영 방식에 대한 보안성을 국가가 직접 감독
일본	• 국가 안보, 경제 산업 발전, 그리고 민간 공급망 보호를 통합하는 방향으로 추진 – 제5차 사이버시큐리티 기본계획('25.12) : 민간, 법 집행 기관, 국방 부문을 아우르는 새로운 통합 사이버보안 전략을 마련하여 핵심적으로 공급망 전체의 사이버 복원력 강화와 국가 안보를 위한 독자적 보안 기술·인재 생태계 구축 목표 – AI·양자암호 등 핵심기술 공동개발 지원('25.1) AI를 악용한 사이버 공격에 대응하기 위해 일본 정보통신연구기구(NICT)가 미국과 손잡고 관련 보안 기술 연구를 진행하고 있으며, 양자 컴퓨터에 대응할 수 있는 차세대 안전 암호화 기술 개발도 적극 추진 중
유럽	• 강력한 '사이버보안 주권(Cybersecurity Sovereignty)' 확보와 기술 회복력 강화에 초점을 맞추고 있으며, 이를 위해 대규모 재정 투입과 함께 엄격한 안전 표준을 의무화 – EU의 신규 사이버보안 전략('20.12) : 향후 유럽의 사이버 복원력 구축을 목표로, 기술 주권 확보, 핵심 인프라(에너지, 교통, 보건 등) 보호, 그리고 차세대 프로세서 및 6G 네트워크 공급망의 신뢰성 제고 추진 – 디지털 유럽 프로그램('21~'27) : 공공 행정, 기업 및 개인을 위해 사이버보안 인프라를 전면 배치하고, 차세대 디지털 기술과 사이버보안 역량 강화에 약 19억 유로를 투자하는 대규모 재정 지원

출처 : 정보통신기획평가원(2026.5.), 국가별 사이버보안 정책관련 보고서 정리

3 최근 논문 및 특허 창출 동향

(논문 동향) SCOPUS DB 기준으로 사이버보안 분야는 '14년부터 '24년까지 총 2,1467건의 논문이 게재되었으며 연평균 16.3%로 증가 추세

- (세부 기술별) 융합 보안 분야의 논문이 연평균 23.9%로 가장 높게 나타났으며, AI와 양자 기술 융합, 전 산업의 AI 전환 추세로 인해 상승세 지속 전망

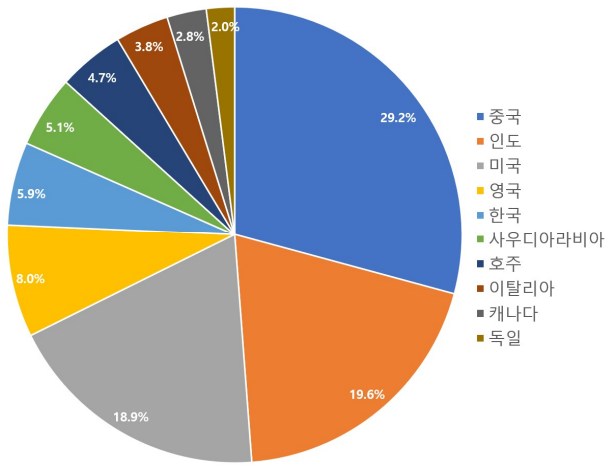
〈 사이버보안 분야의 연도별 논문게재 동향 ('14~'24) 〉

구분	'14	'15	'16	'17	'18	'19	'20	'21	'22	'23	'24	합계	CAGR
공통 보안	153	182	224	248	274	345	446	466	538	606	834	4,316	18.5%
디지털 취약점 분석·시스템 보안	407	393	454	421	485	604	599	658	810	828	1,051	6,710	10.0%
네트워크·클라우드 보안	93	134	155	150	178	309	271	311	432	410	564	3,007	19.8%
융합 보안	169	179	199	198	307	408	527	690	866	1,059	1,435	6,037	23.9%
물리 보안	73	90	124	121	112	134	136	125	161	147	174	1,397	9.1%
합계	**895**	**978**	**1,156**	**1,138**	**1,356**	**1,800**	**1,979**	**2,250**	**2,807**	**3,050**	**4,058**	**21,467**	**16.3%**

출처 : 정보통신기획평가원·윕스(2025.12.), 사이버보안 분야의 2025년 ICT 트렌드 분석 보고서

- (국가별) 중국 29.2%, 인도 19.6%, 미국 18.9%로 높은 비중으로 논문을 게재하고 있으며, 영국은 8.0%, 한국은 5.9%로 5위 수준

〈 사이버보안 분야의 국가별 논문 게재 현황(상위 10개국) ('14~'24) 〉



순위	국가	건수	비중
1	중국	5,256	29.2%
2	인도	3,522	19.6%
3	미국	3,399	18.9%
4	영국	1,443	8.0%
5	한국	1,052	5.9%
6	사우디아라비아	917	5.1%
7	호주	854	4.7%
8	이탈리아	678	3.8%
9	캐나다	507	2.8%
10	독일	353	2.0%
합계		**17,981**	**100.0%**

출처 : 정보통신기획평가원·윕스(2025.12.), 사이버보안 분야의 2025년 ICT 트렌드 분석 보고서

● (국제 협력) '21년~'24년간 중국은 3,244건의 게재 논문 중 861건(26.5%), 미국은 1,604건 게재 논문 중 680건(42.4%)의 국제 협력 연구 수행

- 한국은 9위권으로 547건의 게재 논문 중 233건(42.6%)으로 논문의 질적 수준 제고를 위해 논문 인용도가 높은 국가를 중심으로 연구 협력 강화 필요

〈 사이버보안 분야의 국가별 국제 협력 논문 게재 현황(상위 10개국) ('21~'24) 〉

순위	국가	국제협력 건수	국제협력 비중(%)	논문 건수	논문 인용도(평균)
1	중국	861	26.5	3,244	1.55
2	미국	680	42.4	1,604	1.58
3	사우디아라비아	611	73.7	829	2.18
4	인도	595	28.3	2,100	1.5
5	영국	494	66.8	739	2.17
6	파키스탄	320	88.9	360	2.39
7	호주	280	65.1	430	2.51
8	캐나다	273	63	433	2.58
9	한국	233	42.6	547	1.69
10	말레이시아	202	68.9	293	1.93

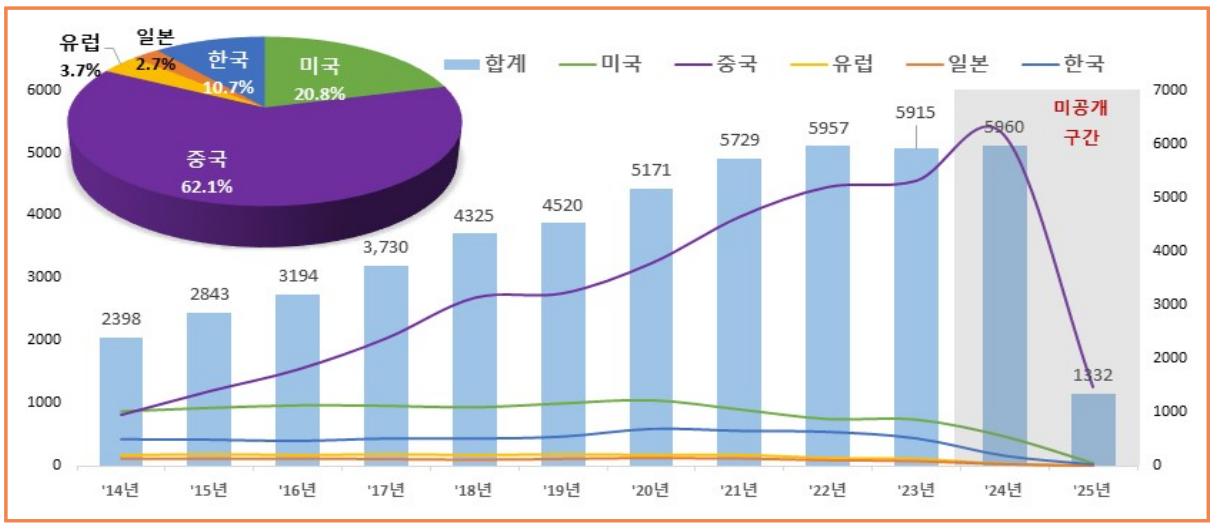
출처 : 정보통신기획평가원·윕스(2025.12.), 사이버보안 분야의 2025년 ICT 트렌드 분석 보고서

(특허 동향) '14년~'23년간 한국, 미국, 일본, 유럽, 중국 특허청에 특허 출원 건수는 '14년 2,398건에서 '23년 5,915건으로 연평균 11% 증가

● 최근 10년 전체 특허 출원 건수는 43,782건으로 중국이 62.1% 비중 차지

- 미국, 유럽, 일본, 한국은 연평균 증가율이 낮아지는 추세, 중국은 글로벌 기술경쟁력 확보를 위한 정부의 전방위 지원으로 지속적인 상승 추세

〈 사이버보안 분야의 국가별 특허 출원 건수 현황 ('14~'23) 〉

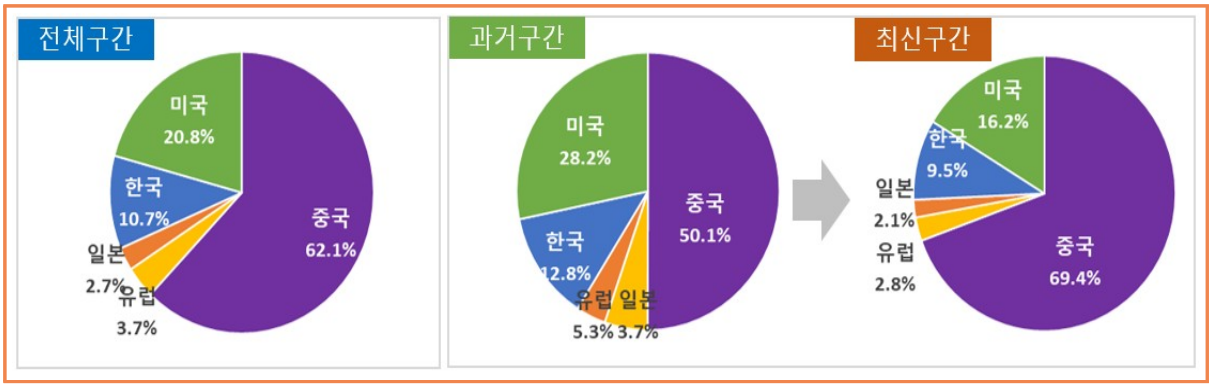


출처 : 정보통신기획평가원·윕스(2025.12.), 사이버보안 분야의 2025년 ICT 트렌드 분석 보고서

○ 과거 구간('14~'18)과 최신 구간('19~'23) 비교 결과, 중국은 과거 50.1%에서 69.4%로 특허출원 건수의 점유율이 크게 상승한 것으로 조사

- 중국과 달리 미국은 20.8%에서 16.2%, 일본 3.7%에서 2.1%, 유럽 5.3%에서 2.8% 각각 하락하였으며, 한국도 12.8%에서 9.5%로 하락 추세

〈 사이버보안 분야의 과거('14~'18)와 최신('19~'23) 구간의 국가별 특허 출원 건수 점유율 〉



출처 : 정보통신기획평가원·윕스(2025.12.), 사이버보안 분야의 2025년 ICT 트렌드 분석 보고서

○ 미국·일본을 제외한 국가에서 외국인 특허 출원 건수와 비중이 동시에 감소 추세

- 국내 출원인은 일부 대기업을 제외하고는 해외에 특허 출원 활동이 저조하여 글로벌 시장 진출을 위해서는 적극적인 해외권리 확보가 필요

〈 사이버보안 분야의 주요국 특허청별 외국인 특허 출원 비중 변화 ('14~'23) 〉

국가	주요 현황
미국	• 외국인 출원 비중 2.9% 증가, 출원 건수 증가율(-4.8%)에 비해 외국인 출원 증가율(-2.0%) 높음 • 대미 시장의 매력도가 높아 다수의 외국인들이 미국 내에 권리를 확보하기 위해 출원 • Bank of America(119건), Huawei(44건), 삼성전자(31건) 등이 최신구간에서 집중 출원
중국	• 외국인 출원 비중 -68.1% 감소, 5개 주요국 특허청 중 최저 증가율, 출원 건수 증가율(129.6%)에 비해 외국인 출원 증가율(-26.7%)이 낮음 • Alipay(225건), University of Xidian(166건), SGCC(132건) 등 최신구간에서 집중 출원하여 자국 시장에서 권리 확보 강화
유럽	• 외국인 출원 비중 -7.0% 감소, 출원 건수 증가율(-13.2%)에 비해 외국인 출원 증가율(-19.2%)이 낮음 • 자국 출원인 Erisson(12건), Siemens(10건), Philips(7건) 등 최신구간에서 집중적으로 출원하여 외국인 출원 비중 감소
일본	• 외국인 출원 비중 4.9% 증가, 출원 건수 증가율(-6.3%)에 비해 외국인 출원 증가율(-1.7%)이 높음 • 주요 외국출원인 IBM(16건), 한국수력원자력(11건), Huawei10건) 등이 최신구간에서 집중 출원이 이루어져 외국인 출원 비중 증가
한국	• 외국인 출원 비중 -36.4% 감소, 출원 건수 증가율(22.9%)에 비해 외국인 출원 증가율(-21.9%)이 낮음 • 자국 출원인 삼성전자(39건), 한국전력공사(31건), 현대자동차(25건) 한국과학기술원(20건) 등 최신구간에서 집중 출원이 이루어져 외국인 출원 비중 감소

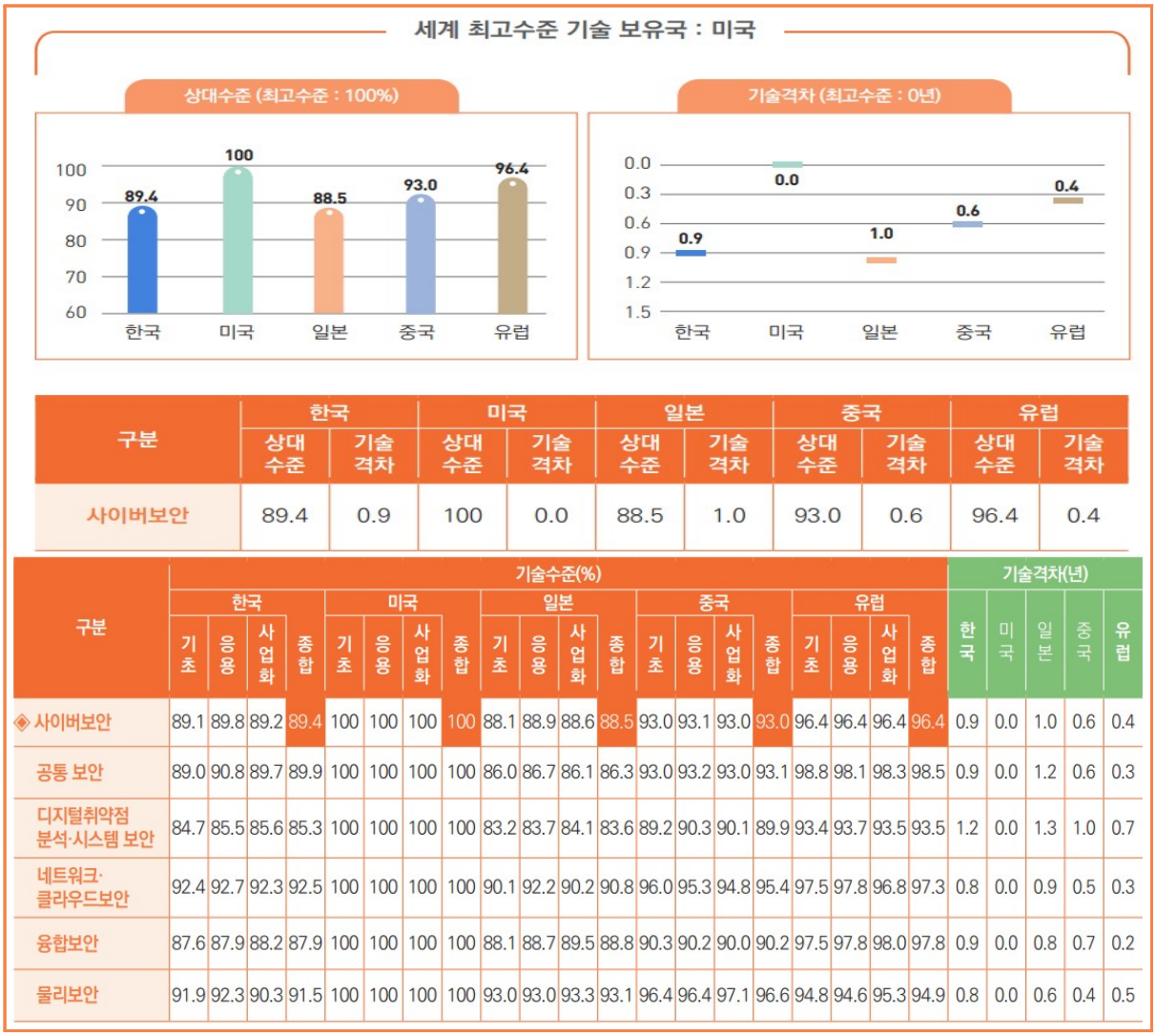
출처 : 정보통신기획평가원·윕스(2025.12.), 사이버보안 분야의 2025년 ICT 트렌드 분석 보고서

4 기술경쟁력 현황 및 기술발전 전망

(기술경쟁력) 사이버보안 분야의 '24년 기준 세계 최고 기술 보유국은 미국으로 한국의 기술 수준은 미국 대비 89.4%, 기술격차는 0.9년 차이가 나는 것으로 조사

- (미국) 사이버안보국(CISA)과 국립표준기술연구소(NIST) 등 국가기관이 표준화를 주도하고 있으며, 국가 사이버보안 개선에 대한 행정명령(EO14028) 및 정부 주요 기반 시설의 사이버 플랫폼 전장화 대응 체계 구축 등으로 최고 기술국 유지
- (한국) 국가 지원 정책과 기업, 금융, 국방 등 모든 시장이 클라우드 네이티브로 전환 중이며, 출연연구소(ETRI)는 암호 양자 안전성 검증 플랫폼 등 핵심 역량 발전 중
  * 한국의 펌웨어 분석 등은 미국, 유럽 대비 기술격차가 상대적으로 크게 나타나고 있으며, 융합 보안 영역은 사업화 기술이 일부 미흡한 수준으로 평가

〈 사이버보안 분야의 기술수준 및 기술격차 〉



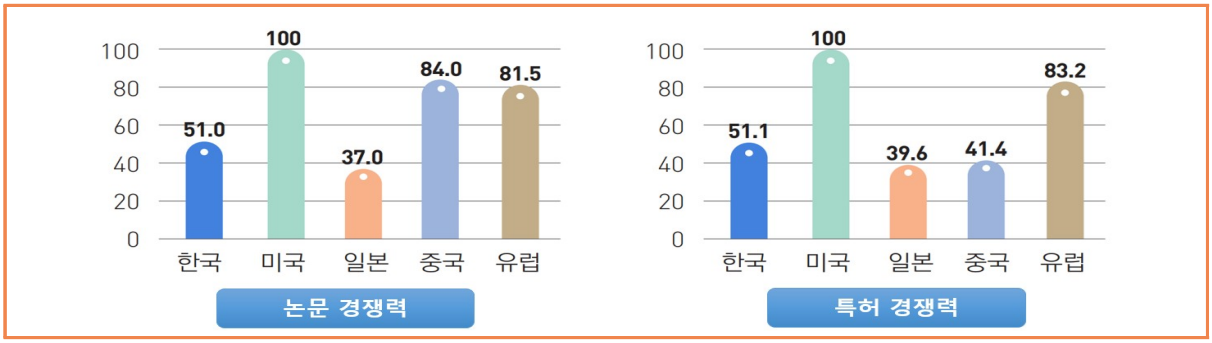
구분	한국		미국		일본		중국		유럽	
	상대수준	기술격차	상대수준	기술격차	상대수준	기술격차	상대수준	기술격차	상대수준	기술격차
사이버보안	89.4	0.9	100	0.0	88.5	1.0	93.0	0.6	96.4	0.4

구분	기술수준(%)																기술격차(년)				
	한국				미국				일본				중국				유럽				
	기초	응용	사업화	종합	기초	응용	사업화	종합	기초	응용	사업화	종합	기초	응용	사업화	종합	기초	응용	사업화	종합	한국	미국	일본	중국	유럽
◈ 사이버보안	89.1	89.8	89.2	89.4	100	100	100	100	88.1	88.9	88.6	88.5	93.0	93.1	93.0	93.0	96.4	96.4	96.4	96.4	0.9	0.0	1.0	0.6	0.4
공통 보안	89.0	90.8	89.7	89.9	100	100	100	100	86.0	86.7	86.1	86.3	93.0	93.2	93.0	93.1	98.8	98.1	98.3	98.5	0.9	0.0	1.2	0.6	0.3
디지털취약점 분석·시스템 보안	84.7	85.5	85.6	85.3	100	100	100	100	83.2	83.7	84.1	83.6	89.2	90.3	90.1	89.9	93.4	93.7	93.5	93.5	1.2	0.0	1.3	1.0	0.7
네트워크·클라우드보안	92.4	92.7	92.3	92.5	100	100	100	100	90.1	92.2	90.2	90.8	96.0	95.3	94.8	95.4	97.5	97.8	96.8	97.3	0.8	0.0	0.9	0.5	0.3
융합보안	87.6	87.9	88.2	87.9	100	100	100	100	88.1	88.7	89.5	88.8	90.3	90.2	90.0	90.2	97.5	97.8	98.0	97.8	0.9	0.0	0.8	0.7	0.2
물리보안	91.9	92.3	90.3	91.5	100	100	100	100	93.0	93.0	93.3	93.1	96.4	96.4	97.1	96.6	94.8	94.6	95.3	94.9	0.8	0.0	0.6	0.4	0.5

출처 : 정보통신기획평가원(2025.2.), ICT 기술수준조사 및 기술경쟁력 분석 보고서

(논문/특허 기술경쟁력) 사이버보안 분야의 논문/특허 기반 기술 경쟁력은 미국이 1위이고, 한국은 미국의 51% 수준으로 평가(논문 경쟁력 4위, 특허 경쟁력 3위)

〈 사이버보안 분야의 논문 및 특허 기술경쟁력 〉



출처 : 정보통신기획평가원(2025.2.), ICT 기술수준조사 및 기술경쟁력 분석 보고서

(SWOT 분석) 한국의 사이버보안 분야의 강점은 제로 트러스트 기술 본격화 및 우수한 암호기술력을 보유하고 있으나, 금융과 융합 보안의 핵심기술이 부족한 상황

〈 사이버보안 분야의 SWOT 매트릭스 〉

강점

- **개인정보보호법 제정에 따른 데이터 보안기술에 대한 연구 및 제품 개발 관심 증가**
  - 제로트러스트 기술을 위한 민간기업 기술 솔루션 출시 및 정부의 제로트러스트 공급망 보안 포럼 발족
- **개인정보보호를 위한 우수한 암호기술력**
  - 경량암호, 동형암호 등 일부 분야에서 세계적 수준의 기술을 확보하고 있으며, 양자내성암호에 대한 국가적 투자 확대 중
  - PKI 기반의 응용기술은 세계적인 수준인 가운데 차세대 인증 분야인 DID, 디지털 신분증 등으로 글로벌 진출 도모 가능

약점

- **금융과 융합보안 영역을 중심으로 빠르게 기술적용이 이루어지고 있으나 원천기술 부족**
  - 인공지능을 활용한 악성코드, 침입탐지, 보안관제 적용 시도는 활발하나 원천기술력 부족
  - 랜섬웨어에 대응한 해외 솔루션(Armis, Medigate, Paloalto networks, CyberMDX 등) 다수
- **글로벌 리더 기업의 부재와 중소기업이 다수인 산업 생태계 현황**
  - 클라우드 중심으로 IT환경이 변화되고 있는 가운데 Amazon, Microsoft, Google 등 미국 빅테크들은 사이버 보안 기업과의 인수합병이 이루어지고 있어, 국내 보안 기업들과의 격차 심화 예상
  - Google Kubernetes Engine, Azure Kubernetes Service, Kubernetes용 Amazon Elastic Container Service 등 해외 관리형 서비스에 의존성 증대
- **제로트러스트 및 클라우드를 위한 관련 보안 장비 및 국제 표준에 대한 활성화 부족**

기회

- **개방형 영상보안시스템 등 산업생태계 변화 시점 도래**
  - 공공용 CCTV에 대한 보안 성능 인증이 강력히 요구됨에 따라, TTA를 중심으로 해당 인증에 대한 지원 강화 및 기업들의 보안성능 확보
  - CCTV 카메라 중심의 영상보안시스템에서 지능형 엣지 카메라/단말, 딥러닝 기반 영상분석/상황인지, AI기반 통합보안솔루션 등 소프트웨어 중심으로 제품/기술 트랜드가 급격히 변화 (SECON, '23)
- **사이버 공격의 국제적 규범 논의 단계**
  - 타 국가와의 사이버보안 협력 강화 가능성 증대
- **융합보안 분야별 글로벌 리딩 기업이 존재**
  - 자율주행차, 선박·해양, 스마트공장 등 기업과 연계하여 보안 기술 개발 및 적용을 통해 해당 산업분야의 보안 기술수준 향상 기회

위협

- **챗GPT 등 생성AI 관련 보안 위협 대두**
  - 원천기술 및 서비스가 글로벌 기업에 의해 독과점 되고 있어, 한국의 대응 기술 개발이 용이하지 않음
- **선도국 및 글로벌 기업의 독점성 우려**
  - Google, Microsoft 등 OS 공급자의 인증 기술을 내재화에 대한 우려
  - 미국, 이스라엘 중심으로 보안 기업의 대형화를 통해 세계 보안 시장 리드('22년 사이버보안 유니콘 기업 58개중 미국 44개, 이스라엘 7개)
  - 중국 등 주변국은 투자가 확장되는 반면, 국내 R&D 투자 감소에 따른 보안기술 R&D역량 저하 우려
  - 생성형 AI, 클라우드 네이티브 등 원천기술 및 서비스는 글로벌 기업이 독과점하고 있어, 한국의 대응 기술 개발이 용이하지 않음
- **산업별 표준과 관련 보안 표준 제정 주도권 상실**
  - 산업별 리딩 기업들과 글로벌 보안업체들이 전략적으로 표준 제정에 참여
  - 국내 보안 기업들은 규모가 작아 기회가 제한적

출처 : 정보통신기획평가원(2025.2.), ICT 기술수준조사 및 기술경쟁력 분석 보고서

(기술 발전 전망) '25~'30년간 AI 기반 자율 대응 보안 강화와 ICT와 산업 융·복합 심화가 가속화되고 있으며, 물리 및 융합 보안 기술도 혁신적으로 발전 중

- 사이버 공간상 고신뢰 암호 및 데이터 보호, 클라우드 네이티브 IAM(Identity & Access Management), AI 통제 기술 등이 필수적인 기술 발전의 핵심축에 위치

〈 사이버보안 분야의 기술발전 방향 전망 〉

출처 : 정보통신기획평가원(2025.1.), ICT R&D 기술로드맵(2025~2030) 사이버보안 분야

- 특히, AI 기술 발전에 따른 사이버 위협 지능화 및 고도화에 대응하기 위한 보안 기술(Security for AI), AI를 활용한 보안 기술(AI for Security)이 급진전

〈 사이버보안 분야의 AI 연계발전 방향 전망 〉

출처 : 정보통신기획평가원(2025.1.), ICT R&D 기술로드맵(2025~2030) 사이버보안 분야

5 산업 경쟁력 제고를 위한 시사점 및 제언

(AI 대응) 초지능 AI 공격 대응에 대응한 AI 자율 보호와 방어 기술 고도화 추진 시급

- 생성형 AI 확산으로 악의적 프롬프트 삽입, 데이터 중독, 모델 탈취 등의 사이버보안 위협이 현실화가 되고 있어 AI 모델 보호 및 활용 보안에 정책 지원 강화
  * 국내는 AI 자체 보호 기술 시장은 아직 초기 단계로 평가되며, 주요 대학과 출연연 중심으로 AI 취약점 분석 연구 등 진행 중이나, 기업의 시장 창출은 미미한 수준

(신산업 대응) 6G, 위성통신 등 미래 네트워크 신산업 출현에 대응한 보안 솔루션 내재화 및 시장 선점을 위한 국가 차원의 선제적 투자 필요

- 5G/6G, IoT, 운영 기술(Operational Technology) 네트워크 등이 출현함에 따라 관련 보안 시장은 지속적인 성장을 거듭하고 있는 상황에 지속 대응
  * 국내는 방화벽, 가상사설망 등 전통적인 솔루션은 보편화되어 있으나, 차세대 기술인 SASE(Secure Access Service Edge)와 NDR(Network Detection & Response)은 낮은 수준
- SpaceX의 스타링크(Starlink) 등 민간위성 인터넷 서비스, 위성항법 시스템 등 상용·공용 위성 활용이 급격한 증가에 대응
  * 국내는 최근에 KPS(Korean Positioning System) 추진, 차세대 다목적 실용 위성 개발 등 우주 프로젝트가 초기 단계로 사이버보안 분야도 초기 연구 단계에 그침
- 전통적인 ICT 인프라의 클라우드 이전 가속화, 멀티·하이브리드 클라우드 운영의 일반화로 시장 성장이 가속화됨에 따른 클라우드 보안 수요에 적기 대응
  * 국내 주요 기업들은 클라우드 VM(Virtual Machine)에 대한 기본적 보안체계는 적용했으나, 멀티 클라우드 통합 관리, 네이티브 환경 보안 등은 미흡한 상황

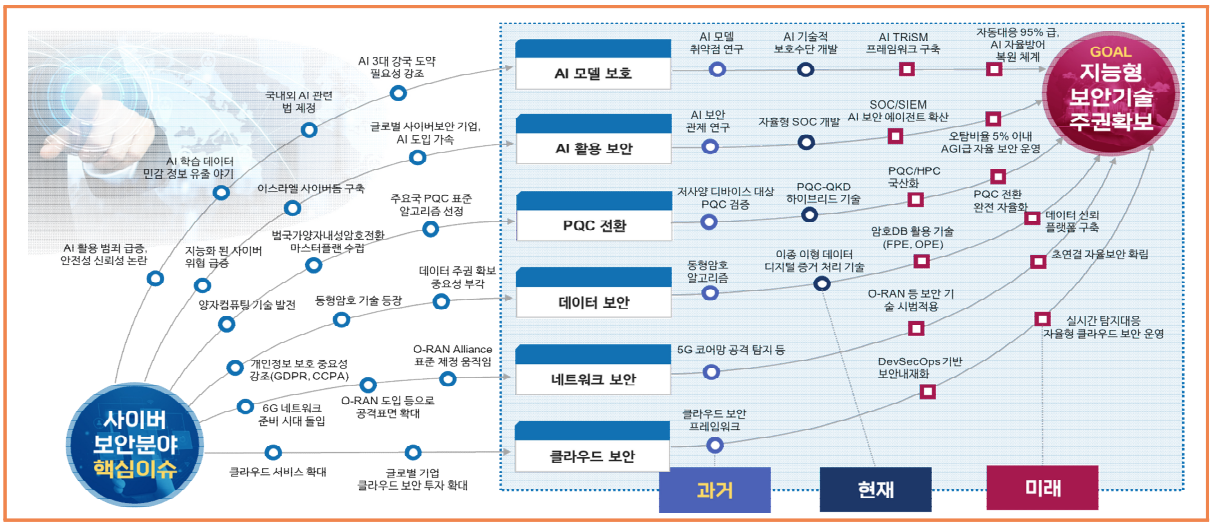
(데이터 보안) 데이터 보안 및 디지털 생태계 전반에 제로 트러스트 패러다임을 정착시키고, 양자 내성 암호 적용 등을 위한 점진적 시장 확대 정책 필요

- GDPR(General Data Protection Regulation) 등 개인정보 보호 규제 강화와 데이터 활용 증가가 맞물려 데이터 암호화, 데이터 거버넌스 등 솔루션 개발 지원
  * 국내는 파수의 데이터 손실 방지 솔루션과 안랩, 시큐아이 등이 DB 암호화 솔루션 등 보유
- 전통적인 VPN 기반 접근제어에서 신원·단말 단위로 세분화된 접근 통제 등 제로 트러스트 시장 변화 패러다임에 적기 대응
- 양자컴퓨팅 출현으로 현행 암호체계 붕괴 가능성에 따라 양자 내성 암호 전환도 글로벌 화두로 급부상하고 있어 정부 차원의 선제적 대응이 중요
  * 범국가 양자 내성 암호 전환 로드맵 마련에 따라 단계적으로 국가 주요망에 PQC(Post-Quantum Cryptography) 도입을 추진

(정책 대응 체제) '지능형 보안 기술 주권 확보'라는 정책목표 달성을 위해 기술 궤적맵을 상시 모니터링하여 정책에 반영하는 선진화된 기술 정책 모델 구축도 필요

* 기술 궤적맵(Technology Trajectory Map) : 특정 기술이 과거부터 현재까지 어떻게 발전해 왔는지, 그리고 미래에는 어떤 방향으로 나아갈지 시각적으로 도식화한 전략 지도

〈 사이버보안 분야의 핵심 이슈 및 기술궤적맵 (예시) 〉



출처 : 정보통신기획평가원(2025.11.13.), ICT 기술전망 컨퍼런스 사이버보안 분야

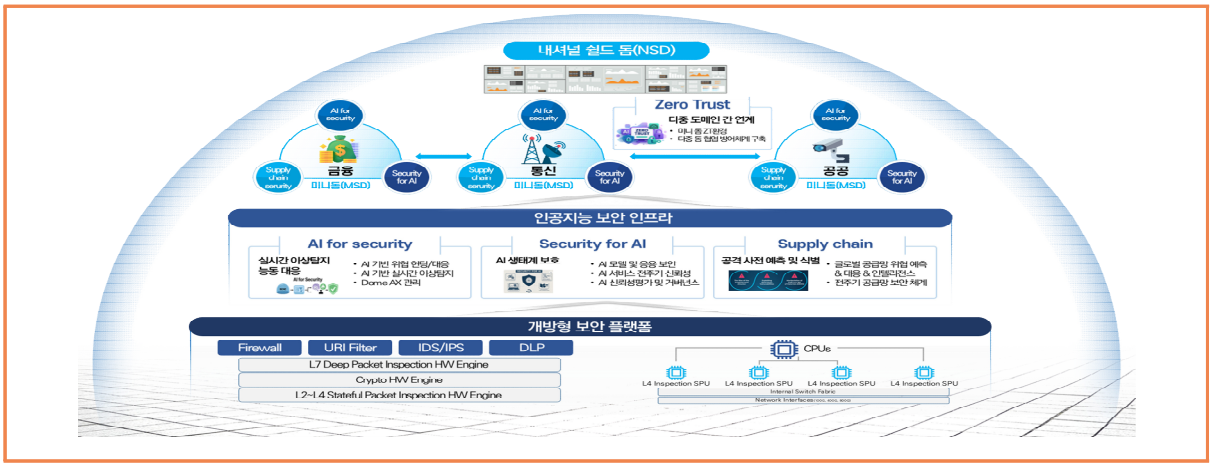
(선단형 국가 프로젝트) 미사일 방어체계와 같이 초지능 AI 위협에 대응하기 위한 사이버보안 위협을 사전에 예측·탐지·방어하는 'AI 사이버 쉴드 돔' 사업을 신속하게 추진

- 산·학·연 역량을 총결집하여 사이버보안 전용 칩(SPU*)을 기반으로 국내 유입 트래픽을 분석하고, 해킹 위협을 사전에 예보·대응하는 사이버 방어체계 구축

  * SPU(Security Processing Unit) : 보안 기능·연산을 전담 지원하는 HW 프로세서

  - 급증하는 사이버 공격으로부터 방어가 절실한 국가 핵심 인프라인 공공, 통신, 에너지 등 국가기관, 사이버보안 관제 기업의 수요를 적기에 반영하여 추진

〈 AI 사이버 쉴드 돔 개념도 (예시) 〉



출처 : 정보통신기획평가원(2025.11.13.), ICT 기술전망 컨퍼런스 사이버보안 분야

(기반 정책) 산업 수요를 반영한 지원체계 개선, 표준화 대응력 강화 필요

- IT-OT/IoT 등 사이버-물리시스템(CPS, Cyber Physical System)의 각 도메인을 통합할 수 있는 보안 프레임워크 및 솔루션 마련 지원
  - 융합 산업 보안 강화를 위해 CPS 보안 협의체 등을 발족, 산업계 협력 체계를 구축하여 대응하고, 통합적인 보안 아키텍처 및 솔루션 등은 현재 부족한 상황이므로 공동 테스트베드 구축 및 시장 확산 실증 기반 조성으로 지원
- 핵심 기술 중심의 정부 R&D 사업 구조를 실용·상용화 중심 R&D 체계 강화
  - 그간 R&D는 기초·원천기술 중심의 성과를 추구하여 상용화로 이어지지 않는 구조적 문제의 고착화 탈피를 위해 개발·사업화 중심 과제에는 성능·표준·인증·매출 기반의 평가 체계 강화
  - 사이버보안 R&D 예산이 국가 전체 R&D 규모 대비 상당히 낮은 수준에 그치고 있어 실증·상용화 중심으로 R&D 예산 확대 추진
- 기업·기관의 사이버보안 투자가 낮아 보안규정 집행 및 산업 수요 기반 조성 확대
  - 국내 기업·기관은 보안을 비용으로 인식해 최소 수준만 대응 중으로 보안기업 시장 규모가 협소하고 투자·인재 수급도 힘든 상황 개선에 대한 정부 지원
  - 잘 마련된 사이버보안 법·규정의 실제 집행 강화하고, 사이버보안 투자 확대 및 의무화를 통해 산업·인재 수요 창출을 위한 정책적 지원도 병행
- 국가망 보안 체계(N2SF*)·위협 정보·국제 협력으로 국가 보안 인프라 강화

  * N2SF : National Next-generation Security Framework(국가정보원의 국가망 보안 체계)
  - N2SF는 국가 보안망을 근본적으로 전환할 핵심 인프라이므로 실증 규모를 확대하고 국산 보안 솔루션이 유기적으로 연동되는 통합 플랫폼 구축
  - 현재 분산된 위협 정보(한국인터넷진흥원·국가정보원·민간업체)를 통합 분석·공유하는 국가 CTI 허브(Cyber Threat Intelligence) 구축이 국가 차원의 대응력 확보
  - 미국, 이스라엘, 아세안 등과 분업형 국제 협력(AI 보안·위협 인텔리전스·SW 자재 명세서·제로 트러스트 실증)이 국내 약점을 보완하여 시장 확대 추진
- Web3·블록체인 및 물리보안·재난 안전 분야의 구조적 규제·데이터 제약 개선 필요
  - Web3·디지털자산·분산 신원 증명은 법·거버넌스 부재 및 국제 표준 불일치로 글로벌 호환성·수출 경쟁력 약화를 개선해 줄 수 있는 정책 개발 및 지원
  - 전 세계적으로 안전, 보호를 위해 CCTV 등 물리보안에 AI 기술 접목이 본격적으로 가속화됨에 따라 영상·음성 등 데이터 개방성 및 활용성 확대 추진