

참고1

사이버보안 분야 정부 정책 · 전략 · 계획

○ 정보보호산업의 글로벌 경쟁력 확보 전략('23.9, 과학기술정보통신부)



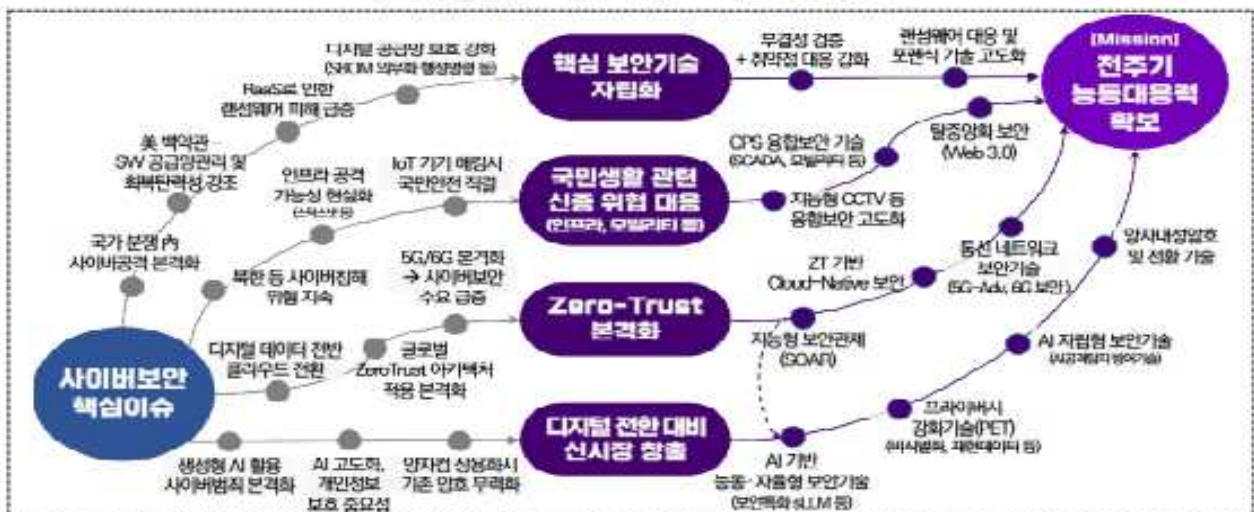
○ 국가전략기술 임무중심 전략로드맵('24.2, 관계부처합동)

3. 사이버보안 : 회복탄력성을 갖춘 전주기 능동대응력 확보

□ 핵심 이슈

- **(핵심 보안기술 자립화)** 고도화되는 사이버 침해사고 대응에는 단순 탐지로는 부족, **사전 취약점 식별 사고 후 복구 및 근원지 추적까지 전주기 회복탄력성(resilience) 필요**
 * (美 표준연) 위험 식별 → 접근 제어 등 보호 → 사고 탐지 → 대응 → 복구 등 5단계 프레임워크 요구
 - 특히 **주요국의 SW 보안 요건 강화**에 대비한 **SW공급망 안정성 확보 추진**
 * 美 국가사이버안보강화 행정명령(21.5.), EU '사이버 회복탄력성법' 추진 발표(22.9.)
- **(국민생활 안전망)** 국가기반산업시설, 모빌리티 등 **신종 안보 위협** 선제 대응하고, **생성형 AI 본격화**에 따른 **'AI 활용 보안(AI for Security) + AI 대상 보안(Security for AI)'** 중요
- **(ZeroTrust 대응)** ICT는 물론, **소산업 데이터의 클라우드 전환이 본격화** → 기존 접속제어 체계의 한계를 극복하는 **새로운 보안 패러다임 요구**

< 핵심이슈 기반 임무·목표 도출 >



중점기술	목표 선정 배경
데이터·AI 보안	<ul style="list-style-type: none"> ▶ 양자컴퓨터 기술 발전에 의한 소인수분해 기반 기존 암호체계 무력화가 가시화 ▶ AI를 사용하는 고도화된 사이버·인지전 공격은 물론, AI 자체를 공격하는 새로운 유형의 사이버공격 본격화 전망 → 데이터 기반 신산업의 글로벌 경쟁력 확보는 물론, 신종 안보위협 대응 필수
디지털 취약점 분석·대응	<ul style="list-style-type: none"> ▶ 미국·EU 등의 공급망 보안 관련 법령 공표에 따라, 국내 SW기업은 물론, AI를 활용한 전분야에서 해외시장 진출 시 관련 기술 요건 충족 필요 → 공급망 보안이 新무역장벽화될 가능성이 높은 만큼, 대한 선제대응 필요
네트워크·클라우드 보안	<ul style="list-style-type: none"> ▶ 글로벌 거대기업 중심으로 클라우드 생태계가 고착화된 상황, 보안 패러다임마저 종속될 경우 우리 기업의 자체적 사이버보안 역량이 상실될 우려 → 국내 특성·환경에 최적화한 제로트러스트 보안 내재화 필요
산업·융합 보안	<ul style="list-style-type: none"> ▶ 우크라이나戰 사례, 美 송유관 해킹 등 국가기반시설 北의 가상자산 탈취 등 본격화 → 국민생활에 직결되는 신종 안보 위협 대응 필요

○ 범국가양자내성암호 전환마스터플랜('23.7, 관계부처합동)



○ 글로벌 전략 지도('24.12, 국가과학기술자문회의 글로벌 R&D 특별위원회)

- ④ 사이버보안 분야는 ①데이터·AI 보안 ②디지털 취약점 분석·대응 ③네트워크·클라우드 보안 ④산업·가상융합 보안 4가지 세부 기술로 나누어 수립하였다. '글로벌 기술수준 지도'에 따르면 우리나라는 데이터·AI 보안 3위, 디지털 취약점 분석·대응 6위, 네트워크·클라우드 보안 3위, 산업·가상융합 보안 6위 수준으로 파악되었다. '기술 유형별 협력전략 지도'에서 데이터·AI 보안은 시장 주도형 협력, 디지털 취약점 분석·대응 및 네트워크·클라우드 보안은 신기술 확보형 협력, 산업·가상융합 보안은 신기술 확산형 협력으로 분류하고, 미국·영국·일본·캐나다 등과 실시간 데이터 침해 탐지 및 분석 시스템 공동구축, 공급망 위협 실시간 탐지 AI 모델 공동 개발 등의 협력 전략을 제시하였다.

〈 사이버보안 분야 협력 유형 및 전략 〉

보급 양산 기술 주기 실증 원천	시장 추격형 협력	시장 주도형 협력
	—	① 데이터·AI 보안 협력기관 (英)캠브리지大, Deep Mind, (佛)INRIA 등 협력방식 실시간 데이터 침해 탐지 및 분석 시스템 공동 구축 등
원천	신기술 확보형 협력	신기술 확산형 협력
	② 디지털 취약점 분석·대응 협력기관 (美)MITRE, CMU, (이스라엘)Legit Security 등 협력방식 공급망 위협 실시간 탐지 AI 모델 공동 개발 등 ③ 네트워크·클라우드 보안 협력기관 (美)NIST, Microsoft, (日)NICT, NEC 등 협력방식 글로벌 위협 인텔리전스 통합 및 예측 성능 강화 등	④ 산업·가상융합 보안 협력기관 (獨)CISPA, Fraunhofer AISEC, Siemens 등 협력방식 산업 IoT 통신 보안 프로토콜 공동개발 등
	경쟁 열위 ←	우려 기술 경쟁력 → 경쟁 우위

- (사이버보안) 디지털 전환 및 AI 발전에 따른 신종 보안 위협 대응 및 개인정보 보호·활용 기술개발을 통해 ICT 안전 활용 기반 조성
 - 클라우드·생성형 AI 가속화 등 디지털 전환에 수반되는 위협 대응 및 양자암호통신 등 미래 보안기술을 확보하고, 사회적 발전에 대응한 융합형 사이버보안 분야 전문 인재 양성
 - AI 기술 발전에 따른 딥페이크 등 AI를 활용한 범죄 및 부작용을 조기 발견하고, 범죄 확산을 방지하기 위한 기술개발

참고3

사이버보안 분야 중장기 R&D 방향

미션	▶ 초거대AI, 클라우드 등 디지털 전환 가속화, SW공급망, 국가인프라 등 보안위협급증 → 클라우드, AI 등 디지털전환 관련 기술력과 능동 대응력을 확보 하고 공급망 보안 등 국가안보 직결 기술 자립화		
비전	▶ 사이버 회복탄력성을 갖춘 전주기 능동 대응력 확보		
미래상	As is (현재) ▶ 암호 및 개인정보보호 분야 기술 및 CCTV·휴먼인식 등 물리보안 기술확보 ▶ 세계최고 수준 네트워크 환경 기반으로 침입탐지 및 이벤트 대응 기술력 확보	⇒	To Be (미래) ▶ 클라우드·AI·양자 등 디지털전환관련 파괴적 신기술 확보 ▶ SW공급망·기반시설보안 등 국가안보 직결 분야의 자립기술 확보
중장기 R&D 추진방향	구분	R&D 중장기 목표	R&D 추진방향
	공통보안 (데이터·AI)	▶ 차세대 암호 및 AI보안기술 자립화	▶ AI, 양자 등 파괴적 신기술 위협 대응을 위한 보안기술 확보
	디지털취약점·시스템보안	▶ 디지털 공급망 안정성 등 디지털 밸류체인 보안프레임워크 구축	▶ 능동대응, 회복탄력성 등 핵심보안 기술 자립화
	네트워크·클라우드보안	▶ 제로트러스트 아키텍처 기반 초신뢰 보안 실현	▶ 제로트러스트기반 클라우드 통합 보안 기술력 확보
	물리·융합보안	▶ 국민생활에 직결되는 융합보안 솔루션확대	▶ 우주·항만, 기반시설 보안 등 국민생활 위협 선제 대응력 확보
기술확보 목표	공통보안 (데이터·AI)	데이터보호 및 초신뢰기술	▶ 양자 위협 대응 고신뢰 암호 전환 ▶ 동형암호, 다자연산 등 프라이버시 보호, 데이터 활용 기술
		AI통제 및 지속인증·인가	▶ 클라우드 네이티브 인증/인가 기술 ▶ 논리적 XAI 등 AI 신뢰성 자율 통제 및 대응 기술력 확보
	디지털 취약점·시스템보안	지능형·능동형 보안위협대응	▶ 능동형 보안위협 수집·분석 기술 ▶ 사이버범죄 인텔리전스 분석 및 역추적·대응 ▶ 범죄 억지를 위한 디지털포렌식 기술
		공급망보안 확보	▶ 클라우드 환경에서의 컨테이너 취약점 및 무결성 검증 기술 및 펌웨어 복원력 기술 확보
	네트워크·클라우드보안	제로트러스트 기반 클라우드 보안	▶ 클라우드 네이티브 환경, API 기반 연계 활성화 환경에서 적용 가능한 보안 기술개발
		차세대 통신 대비 지능형보안	▶ 6G 이동통신 및 저궤도 위성보안 기술개발
	물리·융합보안	고부가가치 물리보안기술	▶ AI 기반 지능형 CCTV 등 물리보안 기술 및 통합관제
		융합·모빌리티·우주보안기술	▶ 가상융합환경의 프라이버시 보존·보호 ▶ UAM보안 및 자율주행 보안위협 대응 등 모빌리티보안 ▶ 위성 SW 등 위성우주 보안기술확보

□ 기술발전 전망과 R&D 핵심이슈



□ 주요 사업 · 과제 기획 추진 로드맵

사이버보안 분야 사업·과제 기획 추진 로드맵(1075억원, '25)

구분	기술분야	~ 현재	진행중·착수예정('24~'25 착수)	향후 기획 방향('26~'30)
능동 대응 (407억, '25)	AI보안 (111억, '25)	AI 프라이버시 보호 프라이버시 위험 분석 대응	AI 모델 안전성 검증 [AI 모델 취약성 분석 평가] [기밀상무결성 자동 평가] 보안 특화 LLM 조직원용 특화 LLM	28년 중기 [AI Shield] 1. AI 모델 내재화 2. AI 데이터 보호 3. AI해커 대응 4. AI 서비스 보안
	네트워크보안 (170억, '25)	5G-6G 보안 5G 코어망 공격 방지 6G 지능보안 기반 기술	5G 특화망·오르겐 보안 6G 트라스트 모델 분석 침해 대응 5G 특화망·무선 통신 환경 최적화 네트워크 슬라이싱 6G 개방형 NW 환경 지능형 침해 대응	과제수행연계
	능동보안 (126억, '25)	취약점 검증 [공격 탐지 대응] [표적 공격 예방]	취약점 탐지 자동화 [AI 기반 취약점 탐지 자동화] [인접한 코드 지능 생성] [하이퍼오메이선 디펜션] [VLM 관제]	과제수행연계
	제로트러스트 (33억, '25)	효율성 검증·실증 [인증성 점검 기술 도입] [사용 환경 실증]	제로트러스트 기반 접근 통제 적용 접속 보안 인증 강화 강화 정보 수직적 검증 강화 데이터 무결성 검증	과제수행연계
보안 역량 강화 (241억, '25)	공급망보안 (80억, '25)	SBOM 자동생성·무결성 검증 SBOM DB 구축 [SBOM 기반 취약점 확인]	SW 공급망 전주기 내재화 SBOM·PVX 연계 [마이크로 보안 패치 지능화] SW 공급망 위험 평가	과제수행연계
	클라우드보안 (28억, '25)		클라우드·심층 방어 보안 프레임워크 4C 계층 보안 취약점 분석 차단 [계층별 네트워크 트래픽 행위 분석]	과제수행연계
	데이터보안 (100억, '25)	임호 알고리즘 구현·고속화 원전 동행임호 알고리즘 개발 [GPU·ASIC 기반 암호알고리즘 고속화 설계]	실시간·편의성 동행 암호 분석 실시간 동행 통계 분석 처리 플랫폼 [SI 기반 암호 분석 분석]	과제수행연계
공공 안보 (107억, '25)	양자내성암호 (59억, '25)	효율성 PQC 성능 검증 저사양 디바이스 대상 PQC 안전성·성능 검증	PQC 인프라 전환 [양자안전 보안 인프라 전환] [대용량 복합 안전성 검증] [양자보안 기반 5G 특화망 기기 식별]	28년 중기 [양자내성암호 전환] 1. 암호화 민첩성 2. 하이브리드 암호체계 3. 암호모듈 인증
	사이버복원력 (10억, '25)		사이버 복원력 평가 [사이버 위기 정보 수집] [사이버 복원력 상황 평가] [복원력 강화 전략 생성]	29년 중기 [디지털 성과 연계 사이버전 대응] 1. 클라우드 다중 보안 체계(과거) 2. 군집 운용 통합 보안(국방) 2. 맞춤형 전술 보안망 (과거) 4. 전술 특화 양자 암호(국방) 3. 사이버 트랩 공세 대응 (국방)
	사이버전 (38억, '25)		국방무인기 제어권 보호 [제어권 상실 대비 침투위치 기술] 사이버 훈련장 구축 클라우드 기반 사이버 훈련장 구축	
신산업 융합 (320억, '25)	모빌리티 (54억, '25)	자율차 내·외부 아티팩트 분석 [운행기록 분석] [사고정보 추론]	자율주행 네트워크 전송 보안 V2X 무선통신 인프라 핵심 기술 [양자통신 보안 기반 인증 인프라]	과제수행연계
	위성 (34억, '25)		위성 데이터 보호 [인공위성 특화형 모니터링] [공격방위·취약점 분석] [시스템 실시간 이상 탐지]	과제수행연계
	지능형 영상 (82억, '25)	지능형 영상 기반 위험 예측 예측적 영상·인신 감지 기술 [지능형 CCTV 도입 시스템 개발]	지능형 영상보안 관계 기술 영상-언어 모델(VLM) 기반 [영상 내 객체간 관계성 분석·분석]	과제수행연계
	국제협력 (150억, '25)		선진 공동 연구 [AI·6G·신산업 분야 분야 공동연구] [식약처 및 박사후 연구원 육성] [해외 타겟형 국제 공동 기술개발]	과제수행연계

□ 글로벌 기술 · 시장 동향

- (시장) 세계 사이버보안 시장은 '24년 384,360백만 달러에서 연평균 약 13.1% 성장률로 '30년 822,353백만 달러 규모의 시장 형성 전망
 - * (공통보안) ('24) 993억 달러 → ('30) 2,695억 달러(CAGR 18.2%)
 - * (디지털취약점분석·시스템보안) ('24) 599억 달러 → ('30) 1,116억 달러(CAGR 11%)
 - * (네트워크·클라우드보안) ('24) 384억 달러 → ('30) 883억 달러(CAGR 14.7%)
 - * (융합보안) ('24) 593억 달러 → ('30) 1,411억 달러(CAGR 14.4%)
 - * (물리보안) ('24) 1,272억 달러 → ('30) 2,116억 달러(CAGR 8.7%)
- (기술/R&D) 보안솔루션에 AI기술 기본 탑재 등 AI에 기반한 사이버 보안이 글로벌 메가트렌드로 자리매김(AI for Security)
 - 글로벌기업은 AI의 보안성 검증과 모델 개선을 위해 AI Copilot 활동 모니터링 및 이상행동 경고 등 관련 기술개발 진행 중
 - * DEFCON31, GRE(Generative Read Team) Challenge(구글, 메타, 오픈 AI 등 8개 벤더 모델 테스트), 세계 최대 AI 레드팀 프로젝트 Gandalf 등
 - 클라우드 복잡성 증가, 공격 증가에 따라 클라우드에 최적화된 보안 솔루션, API 통합보안, Zero Trust Security 기술개발 및 서비스 출시
 - * 클라우드 기반 위협 자동대응 솔루션(구글), API/APP 보안 솔루션(Salt Security), Zero Trust 솔루션(페리미터81(Perimeter 81))
- (주요기업) AI/클라우드 기반 보안 솔루션 도입이 증가하며 시장의 경쟁이 심화, M&A 및 투자 확대를 통해 미국 기업이 글로벌 시장 주도

<글로벌 사이버보안 기업 동향>

구 분	주요 서비스
Cisco Systems (미국)	<ul style="list-style-type: none"> 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)	<ul style="list-style-type: none"> 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

구 분	주요 서비스
Fortinet (미국)	<ul style="list-style-type: none"> • 네트워크, 클라우드 보안, AI 기반 보안관제, 사용자 보안, 클라우드 기반 애플리케이션 보안 제품 및 서비스 제공 • 네트워크 방화벽 "NGFW" 솔루션 보유
McAfee (미국)	<ul style="list-style-type: none"> • 엔드포인트, 엣지 및 클라우드 보안을 포함한 광범위한 사이버 보안 플랫폼을 구축하였으며, CASB 공급업체인 스카이하이 넥스웍스를 인수 • 맥아피 시큐어 웹 게이트웨이 맥아피 (McAfee Secure Web Gateway), DLP(McAfee Data Loss Prevention) CASB M (MMISION Cloud) 및 솔루션인 맥아피 비전 클라우드 플랫폼을 발표
CheckPoint (이스라엘)	<ul style="list-style-type: none"> • '21년 딜로이트의 '고속성장 500대 기업(Technology Fast 500)'에 선정되며 북미지역 내 가장 빠르게 성장하는 사이버보안 기업 중 하나로 인정 • CI/CD 파이프라인 보호 기능을 향상시킨 클라우드 네이티브 애플리케이션 보호 플랫폼(CNAPP) '클라우드가드 CNAPP' 출시('23.02)
CrowdStrike (미국)	<ul style="list-style-type: none"> • '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)

□ 국내 기술 · 시장 동향

- (시장) 국내 사이버보안 시장은 '24년 35.9조 원에서 연평균 11.2% 성장을 통해 '30년 68조, 6,500억 원 규모의 시장*을 형성할 전망

- * (공통보안) ('24) 2.3조원 → ('30) 5.2조원(CAGR 13.9%)
- * (디지털취약점분석·시스템보안) ('24) 4.7조원 → ('30) 8.8조원(CAGR 11%)
- * (네트워크·클라우드보안) ('24) 6.7조원 → ('30) 16.9조원(CAGR 16.6%)
- * (융합보안) 세계/국내: ('24) 13.9조원 → ('30) 25.9조원(CAGR 10.6%)
- * (물리보안) 세계/국내: ('24) 8.1조원 → ('30) 11.5조원(CAGR 8%)

- (기술/R&D) 전통적 보안기술에서 벗어나, IT 환경변화를 반영하고 AI/클라우드 등 신기술을 도입한 혁신적인 보안 기술/제품 출시 위해 노력 중
 - (AI보안) AI 활용시 보안을 강화하는 AI보안 스타트업의 등장 및 AI기반 탐지 결과를 자연어 형태로 설명가능한 대화형 보안서비스 등장
 - (클라우드 보안) 클라우드 환경에서 제공하는 물리, 가상머신, 컨테이너의 런타임 보안 기술을 적용 중
 - (물리·융합보안) CCTV보안 분야 수출 및 시장 확장 중, 산업 제어시스템 보안 중심 융합보안 활발히 진행 중

- (주요기업) 국내에서는 통합형 차세대보안 솔루션에 대한 수요 증가 및 클라우드 기반 서비스의 채택이 증가함에 따라 응용제품 개발 전문 중소기업 중심의 시장 경쟁이 치열해질 전망

<국내 사이버보안 기업 동향>

구 분	주요 서비스
SK쉴더스	<ul style="list-style-type: none"> • 보안 컨설팅, 관제, 솔루션/시스템통합(SI), 클라우드 보안, 모바일 케어 솔루션 등 보안 서비스를 제공하고 있으며, 제로 트러스트 네트워크 아키텍처(Zero Trust Network Architecture), 정보보호 솔루션/SI 보유 • 한국정보인증과 함께 제1금융권에 양자암호 기술을 적용한 일회용 비밀번호 생성기(OTP)를 구축('22.04) • 기업 클라우드 전환과 운영에 필요한 정보보호 컨설팅, 시스템 구축, 위협 모니터링 등 토털 클라우드 보안 서비스를 제공('23.05)
안랩	<ul style="list-style-type: none"> • 안티바이러스 솔루션의 대명사인 V3 제품군을 비롯해 온라인 보안 서비스, 모바일 보안 솔루션, 네트워크 보안 장비 등 정보 네트워크 환경에 적합한 각종 보안 솔루션을 개발·공급 • 보안 특화 클라우드 관리 서비스 '안랩 클라우드'의 다양한 정보를 담은 안랩 클라우드 공식 홈페이지 정식 오픈('23.02)
(주)시큐레이어	<ul style="list-style-type: none"> • 보안관리 시스템eye Cloud SIM, eye Cloud AI 솔루션 보유 • 데이터를 정보보호의 관점에서 분석하고 대응하는 업무 프로세스 자동화 솔루션 '아이클라우드(eyeCloud) XOAR'을 출품 ('23.05)
드림시큐리티	<ul style="list-style-type: none"> • PKI(공개 키 기반 구조, Public Key Infrastructure) 기술 기반 보안·인증 솔루션을 공급하는 기업으로, 양자키관리장비인 MagicQKMI가 국가정보원(이하 '국정원')의 보안 검증을 국내 최초로 획득('23.11)
지니언스	<ul style="list-style-type: none"> • 기업 내부의 네트워크를 보호하는 NAC(네트워크 접근제어 솔루션)와 사이버 위협에 대응하는 EDR, PC 보안 진단 솔루션인 GPI 보유 • 국내 최초로 주력제품인 EDR(단말기반 지능형 위협탐지 대응 솔루션)에 인공지능(AI) 기술을 내재화
파수	<ul style="list-style-type: none"> • 보안솔루션 EDRM, 악성메일 훈련인 '마인드 셋(Mind-SAT)', 보안 모니터링 '파수 ARM(Anomaly Realtime Monitoring)', 암호화 및 백업 서비스 '랩소디 드라이브(Wrapsody Drive) 솔루션 보유 • 파수 매니지드 서비스 출시로 악성메일 훈련과 보안 모니터링, 암호화/백업 서비스를 포함하는 보안 운영 서비스로, 가장 효율적인 보안 관리 방안 제공('23.05) • 기업용 sLLM(small LLM, 경량 대형언어모델) '파수 ELLM(파수 엔터프라이즈 LLM, 이하 ELLM)'을 출시('24.03)

□ 2026년 중점 기획방향

- (AI생태계 보안 내재화) AI 시스템(모델, 데이터, 애플리케이션 등)의 모든 공격 예상 지점에서 보안을 강화하기 위한 기술 기획
 - AI 모델 복제 공격 대응, 학습 데이터에 포함된 민감한 개인정보 유출 방지 및 AI 응용시스템 보안 기술
 - AI 공급망 전주기 무결성 검증, 보안성 자동 평가 등 최종 AI 생태계 전반의 보안을 검증·평가·대응하는 프레임워크 마련
- (양자내성암호 전환 기술) 기존 ICT 인프라 암호체계를 양자컴퓨터의 위협을 막는 '양자내성암호(PQC)' 체계로 전환하기 위한 기술기획
 - 취약암호 탐지 후 영향력을 분석하고, 기존 암호와 PQC 상호운용성을 보장하는 하이브리드 암호모듈 및 PQC 전환 민첩성 기술
 - 전자서명, 블록체인 등 무결성 확보가 필수적이고 다수의 타 시스템과 연계된 주요플랫폼·도메인에서의 선도 전환 기술
- (사이버보안국제협력기반기술) 제로트러스트, 공급망 보안 등 보안 新시장 관련 기술력 확보를 위한 선진공동연구 기술기획
 - (선진공동연구) 해외 협업이 중요한 제로트러스트 등의 분야에 해외 우수 기업·기관들과 공동연구 협력
 - (해외 수출연계) 동남아, 중동 등 우리 보안산업 수출이 유망한 국가 내 기술 현지화 R&D를 통한 해외시장 진출 확대 지원
 - (인력파견) 사이버보안 분야 글로벌 대학 등에 박사후 연구원 및 석·박사생 파견을 지원하여 연구역량 증진, 해외 네트워킹 지원

□ 2026년 투자계획(안)

(단위:백만원)

구분		'25년 예산	'26년 예산	비고
세부사업	내역사업			
AI생태계보안내재화핵심 기술개발	AI생태계보안내재화핵심 기술개발	-	3,600	'26년 신규
범국가양자내성암호전환 핵심기술개발	범국가양자내성암호전환 핵심기술개발	-	3,600	'26년 신규
사이버보안국제협력기반 기술개발	사이버보안국제협력기반 기술개발	-	15,906	'26년 신규 1개 과제, 500백만원
합계			23,106	

* '26년 예산은 신청금액으로, 추후 변경 가능