과학기술정보통신부 보도자료 다시 대한민국! 새로운 국민의 나라

보도시점 2023. 9. 5.(화) 14:00 (2023. 9. 6.(수) 조간) 배포 2023. 9. 5.(화) 09:00

우리 정보보호산업의 경쟁력 강화를 통한 '튼튼한 사이버 안보' 실현

과기정통부, 「정보보호산업의 글로벌 경쟁력 확보 전략」 발표

△ '27년까지 **시장규모 30조원** 달성을 **목표**로 **관련 예산 총 1조 1천억 원 투입**

△ '27년까지 총 1,300억원 규모의 **「사이버보안 펀드」 조성을 통해 보안 유니콘 기업 본격 육성**

△ **제로트러스트 전환로드맵** 수립 및 제로트러스트 가이드라인 2.0 배포, 통신·금융·의료 등 **주요 기반 분야 보안 패러다임 전환 시범사업** 추진

△ **혁신 통합보안 모델 개발을 위한 「K-시큐리티 얼라이언스」** 추진을 통해 글로벌 수출지원 확대

과학기술정보통신부(장관 이종호, 이하 '과기정통부')는 9월 5일(화), 제30차 비상경제차관회의에서 **「정보보호산업의 글로벌 경쟁력 확보 전략」**을 발표하였다.

최근 글로벌 보안시장은 사이버위협 증가와 디지털화로 인한 보안영역의 확장, 각국의 보안규제 강화로 시장이 성장하고 있으며, '26년까지 연평균 8.5% 지속성장할 것이라는 전망이 나오고 있다.

※ 글로벌 정보보호 시장규모는 '23년 3,019억 달러(약 393.9조), '26년까지 연평균 8.5% 성장 전망(Markets&Markets, '22)

특히, 제로트러스트·통합보안 등 보안 패러다임 전환을 계기로, 고성장 중인 **글로벌 사이버 보안시장을 선점하려는 선도 기업들의 치열한 주도권 경쟁이 가속화**되고 있다.

또한, 러시아-우크라이나 전쟁에서 보듯이 사이버전이 확대되면서, 세계 주요국은 **자국의 정보보호산업 수준이 곧 안보와 직결된다는 인식**에 따라 **국제협력과 산업육성 정책을 경쟁적으로 추진**하고 있는 상황이다.

윤석열 대통령 또한 “사이버 안보 역량 강화가 국가 안보의 핵심”이라고 수차례 강조해왔으며, 최근 미국과 일본을 비롯해 중동과 동남아 등 **활발한 순방을 통해 사이버 분야 협력 행보를 확대**하고 있는 상황도 이와 맥락을 같이한다.

이에 따른 과기정통부의 이번 전략은, **우리의 힘으로 ‘튼튼한 사이버 안보’를 실현**하기 위해 글로벌 시장경쟁에서 뒤처지지 않는 정보보호 산업육성이 중요하고, **사이버 보안 패러다임 전환을 선점할 새롭고 발 빠른 대책이 필요**하다는 취지에서 마련된 것이다.

「정보보호산업의 글로벌 경쟁력 확보 전략」의 주요내용은 다음과 같다.

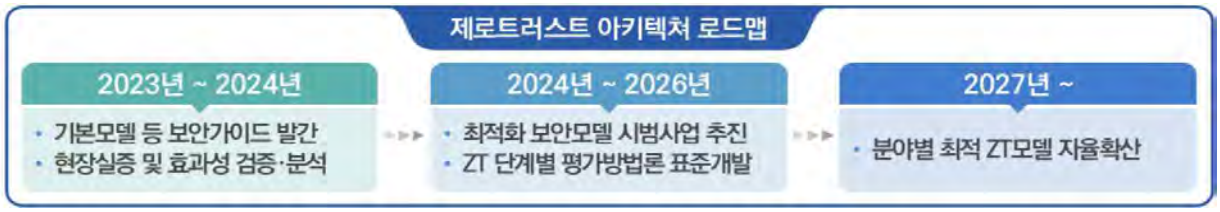
글로벌 정보보호산업 강국 도약이라는 비전 실현을 위해 ‘27년까지 정보보호산업 시장규모 30조원 달성, 보안유니콘 육성 등을 목표로 4대 전략과 13개 과제를 추진한다.

[전략 1] 보안패러다임 전환 주도권 확보 및 新시장 창출

첫 번째 전략으로, 보안 패러다임 전환에 따른 새로운 보안체계 적용과 스마트공장, 스마트헬스케어, 로봇, 우주·항공 등 미래산업의 보안내재화를 통해 보안 新시장을 창출하고, 융합보안 및 물리보안 산업을 집중 육성하여 글로벌 보안시장 진출 확대를 추진한다.

① 기존 경계보안의 한계를 해소하기 위한 **'제로트러스트* 전환 로드맵'**을 수립하고, 통신·금융·의료 등 기반 분야를 중심으로 기존 경계모델을 제로트러스트 보안 모델로 적용·확산하는 시범사업 추진 등을 통해 보안패러다임 전환을 강화해 나간다.

* 기존 경계기반 보안과 달리 제로트러스트는 정보시스템 등에 대한 접속 요구 시 네트워크가 이미 침해된 것으로 간주, 절대 믿지 말고, 계속 검증하라는 새로운 보안개념



아울러, SW 공급망 공격에 능동적으로 대응하고, 해외 무역장벽에 대비하기 위한 **'SBOM* 기반 SW 공급망보안 기술지원 체계'**를 구축하고, 보안SW 및 의료SW 등 파급력이 높은 분야 대상 공급망 보안관리를 지원한다.

* SW 개발 全 과정의 구성내역 상세명세서인 SBOM(SW Bill of Materials) 분석을 통해 취약점 발견 및 SW 보안성 확보가능

② 유기적 협력·선제적 보안내재화로 **미래형 융합보안 시장을 개척**하기 위한 작업도 본격 추진한다.

주요 新산업별 보안요구사항(정책·제도·인증)에 전략적으로 대응하기 위한 유관부처·기관 '융합보안 협력체계'를 구축하고, 융합보안 내재화를 위해 기존 **보안리빙랩을 핵심분야(스마트헬스케어, 자율주행차, 스마트공장 등)** 특화 개편하고, 이를 기반으로 보안인증 내재화 프로세스를 마련한다.

< 스마트헬스 분야 융합보안 내재화 프로세스 사례(예시) >

③ 국산 신기술 적용·확산을 통해 물리보안을 차세대 성장산업으로 육성한다.

정부 R&D로 국산화된 핵심부품인 **CCTV 반도체칩(SoC)의 보급을 확산**(10개社→40개社)하고, **2세대 반도체 칩을 조속히 양산**하여 국산 제품의 세계 시장 점유율을 확대할 계획이다.

또한 지문·안면 중심 **생체인식 성능평가 분야를 정맥 및 홍채 등으로 확대**하고, AI 등 신기술을 활용, 관련 데이터를 60만 건 이상 대량 구축하여 생체인식 물리보안 시장 확대를 견인할 계획이다.

국내 보안기술*을 집약시킨 **'한국형 무인점포'**를 구현하고, 실증을 통해 상용화를 추진하는 한편, 개발된 우수 무인기술·제품을 소상공인 무인점포에 지원하여 범죄 등 사회문제 해결과 무인보안 시장 확대를 도모한다.

* AI(객체인식, 모션인식)인지, 자동인증·결제, 성인인증 기술 등 기존 외산기술 대체

[전략 2] 협업 기반 조성을 통한 신흥시장 진출 강화

두 번째 전략으로, **기업 간 협력을 기반으로 혁신적인 통합보안 모델을 구현**하고, 신흥시장을 전략적으로 공략하여 글로벌 시장 內 우리기업의 경쟁력 확보를 추진한다.

① 혁신 통합솔루션·서비스 개발을 위한 '민간주도형 전략적 협업 추진연대 **「K-시큐리티 얼라이언스」**' 를 구성하고, 이를 통해 공동·협업형 통합보안 사업화모델, 표준화 및 상호운용성 확보 등을 민간이 주도할 수 있도록 적극 유도하되, 정부는 기업 애로해소와 판로·투자·해외진출을 전폭적으로 지원한다.

또한 '24년부터는 현장수요를 기반으로 우수 통합보안 모델을 공모를 통해 선정하여 협업 활성화의 마중물로 활용할 계획이며, 협업성과공유회, 성과사례집 및 협업가이드 발간, 우수 상호운용성 표준제정 등을 통해 글로벌 트렌드인 'Stronger Together' 조성을 적극 유도할 계획이다.

② 국제협력 기반의 신흥 보안시장 진출 관련 사업을 확대 추진한다.

정상외교를 통해 조성된 중동·동남아 지역 협력 분위기를 우리기업의 진출 기회로 활용하기 위한 노력의 일환으로, 중동 · 동남아 등 신흥시장 공략을 위해 중동 거점을 사우디로 재편하고('23.7~), 베트남 거점(하노이) 신설('23.12~)을 추진한다.

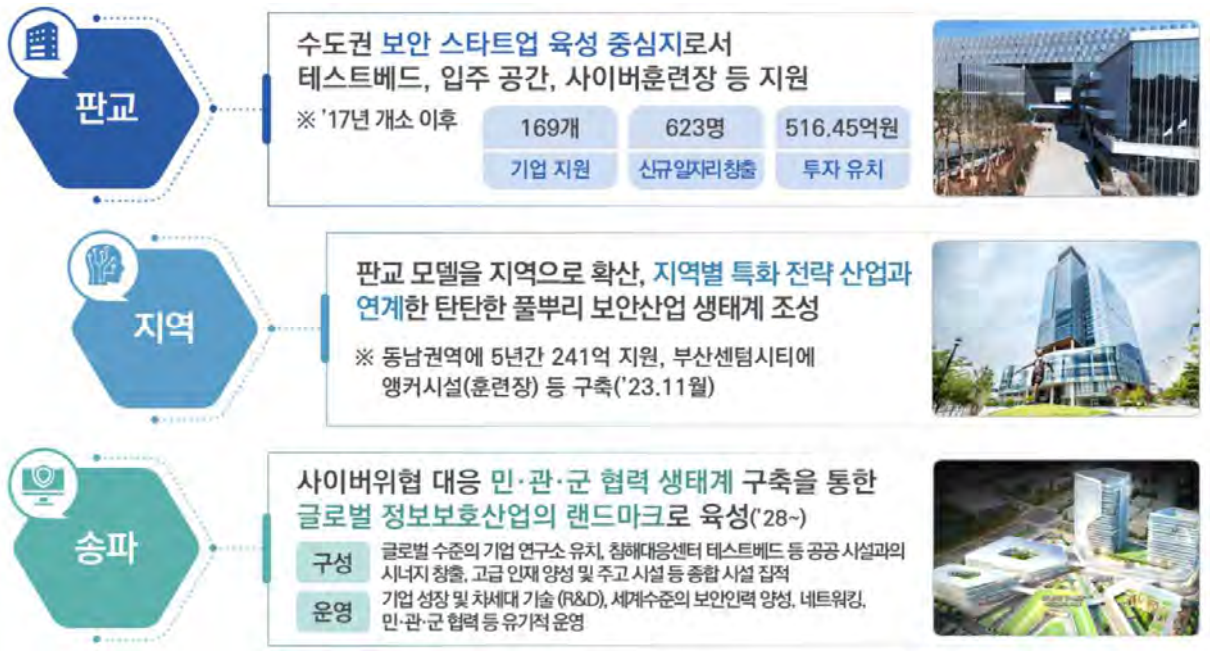
※ 정보보호 해외 전략거점: 미국(실리콘벨리), 동남아(인니), 중동(오만), 아프리카(탄자니아), 중남미(코스타리카)

또한 중동·동남아 기금·공공조달 사업 프로젝트 수주를 위한 민·관 협력형 **「시큐리티 팀 코리아」** 구성·지원을 통해 공공부문의 주도로 대형 해외사업 수주 가능성을 극대화하고, 수주 후 국내 사업자 참여를 통해 기업의 간접 수출 효과를 제고한다.

[전략 3] 글로벌 공략을 위한 단단한 산업 생태계 확충

세 번째 전략은, 우리 기업의 글로벌 시장진출 가속화를 위해 시설확충, 펀드조성, 인재양성 등 지속성장 환경 조성에 집중 투자하는 것을 주요 골자로 한다.

① 보안 스타트업 육성(판교), 지역 보안산업 강화(부울경), 글로벌 시큐리티 클러스터(송파)로 구성된 **「K-시큐리티 클러스터 벨트」**를 조성하여 우리 기업의 해외진출 가속화를 위한 전진기지로 육성한다.



② **「사이버보안 펀드」**를 조성하여 민간투자의 마중물로 활용한다.

기업의 안정적 기술개발 및 민간투자 활성화를 위해 민관합동으로 「사이버보안 펀드」를 조성하고(~'27년, 총 1,300억 원 규모 예상),

제로트러스트 및 AI 등 유망 분야 스타트업 지원 및 기업 간 M&A를 통한 스케일업 지원에 펀드 결성액의 50% 이상 투자를 유도할 계획이다.

※ △ 스타트업 분야: 유망신기술(AI, ZT, 양자 등) 및 원천분야(네트워크, 5G, 암호 등) 제품·서비스 개발 및 사업화
△ M&A분야 중소·중견 사이버보안 기업의 인수합병을 통한 통합 제품·서비스 개발 및 사업화

「사이버보안 펀드」 기본구조(예시)

[전략 4] 차세대 정보보호 기술 경쟁력 확보

마지막으로, 미래 산업 성장에 필수적인 전략기술 개발에 집중하고, 선도국과의 공동연구를 통해 글로벌 기술패권 경쟁에서 우위를 점할 수 있는 기술력 확보에 주력한다.

① 미래 대응에 필요한 사이버보안 중점기술 확보를 추진한다.

국내·외 기술·시장 분석을 통해 **미래 도전, 기술·산업 선도, 안보투자** 등 주요 R&D 영역을 도출하고, 영역별 선택과 집중의 전략적 투자를 추진하여 성과를 극대화 한다.

차세대 정보보호 기술 R&D 추진방향

구분	주요내용 및 방향	주요 기술분야
미래도전 R&D	현재 국내 기술수준은 낮으나, 글로벌 시장 임팩트를 고려하여 미래 산업 경쟁력을 선제적으로 확보하기 위한 도전적 분야	AI·클라우드 보안, 제로트러스트, 위협인텔리전스, XDR, 신산업·융합보안
기술산업선도 R&D	국내 기술수준이 높은 기술을 대상으로 글로벌 기술 주도권 및 수출경쟁력 확보가 필요한 분야	양자내성암호, 프라이버시 강화 기술
안보 투자 R&D	해외시장 규모가 협소하고, 국내 기술수준도 낮으나 국가안보·국민안전과 연관된 핵심기술로 지속 투자가 필요한 분야	공격억지·선제면역·회복탄력

② 국제 공동연구를 통한 글로벌 보안기술 경쟁력 확보

미국·독일·핀란드 등 사이버보안 분야 강점을 지닌 선도국과 공동 연구를 통해 글로벌 수준의 기술 확보를 추진하고, 동남아·중동 등 주요 신흥시장을 전략적으로 공략하기 위한 신흥국 지원 연구도 신규 추진한다.

※ △ 선도국 협력연구(예시): 미국(가상자산 불법행위 추적, AI 영상보안 등 美DHS 협력), 독일(스마트공장·자율차 보안 등 獨 CISPA 협력), 핀란드(6G 등 이동통신 보안)

△ 신흥국 지원연구(예시) 협력연구(예시): 동남아(전문인력 양성체계, PKI 등 인증제도), 중동(스마트시티보안, 통합관제 등)

□ 과기정통부 이종호 장관은 “**최근 글로벌 보안시장**은 새로운 보안 패러다임 선점 경쟁이 가속화되는 가운데, **통합보안이라는 흐름에 뒤처지지 않기 위한 기업 간 협업과 공조가 활발하게 일어나는 등 격변의 시기**” 라며,

“**새로운 보안 패러다임 변화를 발 빠르게 준비**하고, **신흥시장을 공략할 탄탄한 산업 생태계를 조성하는 일은 단 하루도 늦출 수 없는 시급한 과제**로, 이번 전략을 통해 우리 정보보호 산업이 글로벌 경쟁력을 갖추고 시장 주도권을 확장함으로써, **우리의 힘으로 사이버 안보를 튼튼히 할 수 있도록 정부의 역량을 집중**하겠다”라고 밝혔다.

붙임. 정보보호산업의 글로벌 경쟁력 확보 전략(요약)

담당 부서	정보보호네트워크정책관 정보보호산업과	책임자	과 장	정은수 (044-202-6450)
		담당자	사무관	박세진 (044-202-6455)
			사무관	김성환 (044-202-6451)
			사무관	곽을경 (044-202-6453)
협조 부서	정보보호네트워크정책관 정보보호기획과	책임자	과 장	김경우 (044-202-6440)
		담당자	사무관	임수연 (044-202-6448)

[붙임] 정보보호산업의 글로벌 경쟁력 확보 전략(요약)

1 추진배경

○ 사이버위협의 양적 증가*와 디지털 심화로 인한 보안영역의 확장으로 **글로벌 보안시장**은 **지속가능한 고성장**** **산업**으로 발돋움

* 사이버공격으로 인한 글로벌 경제피해는 '15년 3조 달러에서 '22년 6조 달러로 2배 이상 증가('22, PwC)

** 글로벌 정보보호 시장규모는 '23년 3,019억 달러(약 393.9조), '26년까지 연평균 8.5% 성장 전망(Markets&Markets, '22)
시장의 성장세 속에 벤처캐피털의 집중 투자로 글로벌 사이버 보안 유니콘도 급증('19년 13개 → '23년 58개)

- 디지털심화 및 원격근무 확산 등을 계기로, 파트너십을 통해 **글로벌 시장을 선점**하려는 **기업들의 주도권 경쟁**이 본격화되는 시점

※ 구글, IBM등 미국 주요 보안기업은 M&A 및 파트너십 기반 통합보안 플랫폼 구축 등을 통해 급변하는 보안 시장의 주도권을 확보하려는 전략을 구사하고 있으며, 미국 M&A 규모는 '22년에만 60억 달러(7조 8천억 원) 이상 기록

○ 특히, 사이버공격이 전쟁수단화 되면서 각국은 **정보보호 산업육성을 자국 안보와 직결된** 문제로 인식하고, **경쟁력 확보에 주력**

※ 러시아는 우크라이나 침공 시 악성코드와 랜섬웨어를 활용한 사이버 전면전을 감행 (MS, '22)
미국(국가안보전략, '22.10), EU(사이버방어전략, '22.11), 영국(국가 사이버전략, '22.12)등 관련 정책을 경쟁적으로 발표

⇨ 정보보호산업을 **미래 전략산업**으로 **육성**하여, 우리 힘으로 **사이버 안보**를 **실현**하고, **고성장 중인 글로벌 보안시장 주도권 확보** 추진

2 그간의 성과와 우리의 기회

○ **성과** 정책·시장·기술 등 **적극적 정부 전략*** **추진**으로 국내 정보보호 시장은 최근 **3년간 평균 13.2% 이상 높은 성장세**** 유지

* 제2차 정보보호산업 진흥계획('20.6), 정보보호산업의 전략적 육성방안('22.2), 사이버 10만 인재 양성방안('22.7)

** '18년 시장규모 10조에서 '22년 16.2조로(정보보호산업협회,'23.8) **4년 만에 60% 이상 고성장** 달성

- **정보보호 10만 인재** 양성 노력*, 꾸준한 R&D 투자**로 선도국 **기술격차 단축**(미국, 1.5년→1.1년), **국제정보보호지수 4위**('21년) 등 성과

* 사이버보안 전문인재 양성 수 : '20년 8,141명 → '21년 9,377명 → '22년 10,670명(목표 대비 12% 초과 양성)

** 정부 정보보안 R&D 예산: '17년 546억 원 → '22년 928억 원(58%↑)

- **정보보호 공시제도 의무화**('21.12), **신속확인제 도입**('22.11)등 적극적 제도 시행으로 기업의 **경쟁적 보안투자 유도 및 시장진입 애로 해소**

※ △ 기존 정보보호 관련 인증 획득 시 6개월~1년 소요→신속확인제 도입으로 인증 발급까지 2개월 소요
△ 2년 연속 정보보호 공시를 이행한 기업(49개사)의 정보보호 투자액은 26.2%, 전담인력은 32.9% 증가

○ **위기** **내수 중심**의 경직된 시장구조, 기업 간 파트너십과 **공조문화 미흡**, 보안시장 **투자 부족**은 우리 산업의 **글로벌 경쟁력 약화 요인**

※ '22년 정보보안 매출액(5조 6,171억 원)중 수출은 2.76%(1,552억 원). 국내 보안 기업 기술개발 및 성장 애로사항 1위(40.8%)는 자금조달 (정보보호산업협회, '22.9)

[참고] 보안 유니콘 없는 우리, 원인과 정책방향은?

○ 글로벌 유니콘* 중 **사이버보안은 3번째**로 높은 증가세('19, 13개→'23, 58개, 4.8%↑), **한국은 여전히 보안 유니콘이 없는 상황으로, 원인 분석과 정책방향 설정 필요**

* **시장규모 및 점유율, 현금유동성, 기술혁신성**(창업 10년 이내, 비상장, 기업가치 1조) 등이 주요 선정 기준
** **글로벌 유니콘('23년 기준 1,209개)** 증가 업종 순위: 1위 핀테크, 2위 인터넷SW·서비스, **3위 사이버 보안**

글로벌 유니콘 판단 기준에 근거한 정책 추진방향

원인 분석		정책 추진방향
전통적 보안분야(관제 등)에 안주하는 시장문화 ('23, CTA 국가별 혁신순위에서 F학점(최하점))	기술혁신성	ZT, SW공급망, AI 및 융합보안 등 딥테크·신기술 시장 개척
단일제품 위주의 시장, 기업 파트너십 부재로 글로벌 시장점유율 정체	시장점유율	대·중·소 기업 간 전략적 파트너십을 통한 경쟁력 확보
내수·공공 중심 시장(年 약 5조)으로 단일기업 가치 1조원 이상 도달 어려움	시장규모	신흥국 등 해외시장 진출로 국내시장의 한계 돌파
경직된 시장으로 민간 투자매력도 하락 (국내 보안기업의 애로사항 1위는 자금조달)	투자기반	정부주도 정책펀드 조성을 통해 투자 활성화 기반마련

○ **기회** **新보안체계로의 전환**, 미래산업(자율차·로봇)의 **융합보안 강화**, 중동·동남아 등 **우호적인 신흥 시장**은 우리산업 혁신성장의 기회

※ △ (융합보안) 국내 시장규모는 '20년 7,721억 원→'25년 2조 5,317억 원으로 급성장 전망(매일경제, 22.11)
△ (신흥시장) 동남아(年 13.2%↑), 중동(年 10.1%↑)은 최근 보안시장 급성장 중으로, 우리기업과 협력 수요 多

3 주요 정책 방안

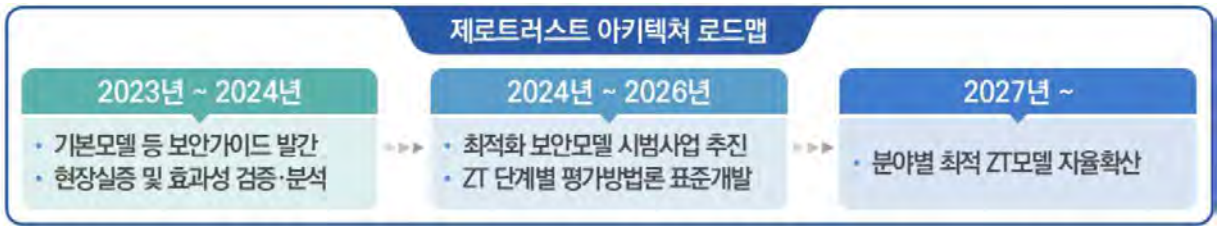
1. 보안패러다임 전환 주도권 확보 및 新시장 창출

새로운 보안체계 적용과 미래산업의 보안내재화를 통해 新시장을 창출하고, 융합보안 및 물리보안 산업 강화를 통해 글로벌 보안시장 진출 확대

① 사이버보안 패러다임 전환에 따른 新기술시장 주도권 확보

○ (**제로트러스트**) 기존 경계보안의 한계를 해소하기 위한 **'제로트러스트* 전환 로드맵'** 을 수립하고, **신속한 도입·확산 추진**('23~)

* 기존 경계기반 보안과 달리 제로트러스트는 정보시스템 등에 대한 접속 요구 시 네트워크가 이미 침해된 것으로 간주, 절대 믿지 말고, 계속 검증하라는 새로운 보안개념



- **통신·금융·의료 등 기반분야**를 중심으로 기존 경계모델을 ZT 보안모델로 적용·확산하는 **시범사업 추진**('24~'27, 24개 과제)

※ 산업 분야별 최적의 ZT 모델 구현 및 확산에 필요한 가이드라인 고도화('23. 가이드1.0→ '24. 가이드 2.0) 실증결과 기반 표준모델 정립('26년까지 6개 분야) 및 우수사례 전파로 '27년까지 新보안체계 전면 확산 유도

○ (**공급망 보안**) SW 공급망 공격에 능동적으로 대응하고, 해외 무역장벽에 대비하기 위한 **SW 공급망 보안점검·대응 인프라 구축**('23~)

- **'SBOM* 기반 SW 공급망보안 기술지원 체계'**을 구축하고 보안·의료SW 등 **파급력이 높은 분야** 대상 **공급망 보안관리**** 지원('25~'27, 年 25개社)

* SW 개발 全 과정의 구성내역 상세명세서인 SBOM(SW Bill of Materials) 분석을 통해 취약점 발견 및 SW 보안성 확보가능
** SW 자산식별, 보안취약점 점검 및 컨설팅, 실시간 모니터링 및 상황전파, 보안패치 등 공급망 전반의 보안대응 지원

② 유기적 협력·선제적 보안내재화로 미래형 융합보안 시장 개척

○ (**융합보안 협력체계 구축**) 자율차·스마트선박 등 산업별 보안요구사항*에 전략적으로 대응하기 위한 유관부처·기관 **'융합보안 협력체계'** 구축('24~)

* (자율차) EU의 자율차 사이버 보안관리체계 준수 규제, (선박) 국제해사기구의 스마트선박 사이버보안 요구사항 규제 등
※ 국제규제 대응을 위한 공동연구, 신규 인증제도 마련에 필요한 인증기준 수립, 법령 재정비 등 협력 추진

○ (**융합보안 내재화**) 융합보안 내재화를 위해 기존 보안리빙랩(5개소)을 핵심분야(헬스케어, 자율차, 스마트공장 등) 특화시설로 개편 운영('24~)

- 보안리빙랩을 활용한 **보안인증 내재화 프로세스를 마련**하고, 부처 협력을 기반으로 적용 분야를 점진적 확대(~'25, 3개 분야)

○ **(미래 융합보안 육성) 미래 전략산업**(스마트선박, 로봇, 우주 등) 특성을 반영한 선제적 보안모델 개발로 **융합보안 신분야 개척**('24~'27, 3개 분야 6개 과제)

※ 분야별 특화형 보안점검·컨설팅 제공으로 보안모델을 실증·고도화하고, 우수 적용사례를 산업계로 확산

③ **국산 신기술** 적용·확산을 통해 **물리보안을 차세대 성장산업으로 육성**

○ **(지능형 CCTV 수출확대)** 정부 R&D로 **국산화된 핵심부품**반도체칩(SoC)의 보급을 확산(10개社→40개社)하고, **해외수출 가속화**('24~)

※ 물리보안 분야 CCTV 관련 수출규모 '22년 1.6조에서 '27년 3조원까지 확대 추진

- **2세대 국산 지능형 SoC칩*** **개발·양산**을 추진하여(~'24년), 우리 제품의 **글로벌 시장점유율 확대로 연계**('22, 3%→'27, 10%)

* 2세대 SOC칩(EN677): CPU 등 성능개선 및 보안성 강화, 영상이미지·화질개선 및 보정기능 탑재 반도체 설계·제조 전 과정 국산화 통해 미·독·일 등 주요국에 수출 확대 기대('24년 1분기 출시 예정)

○ **(생체인식 기반강화)** 지문·안면 중심 **생체인식 성능평가 분야**를 확대(2종→ 6종, 지·장정맥, 홍채 등)하여 **생체인식 물리보안 시장확대**('24~)

- **AI 등 신기술***을 **활용하여 생체 데이터를 확대 구축**(~'24, 60만건)하고, **생체인식 기업의 제품화 성공률 대폭 향상**('22, 76%→'25, 85%)

* GAN(Generative Adversarial Network): 딥러닝을 통해 이미지를 생성 및 조합, 변형하는 기술로, 개인정보 이슈제거로 폭발적인 수량의 데이터 구축이 가능하고, 다수 데이터로 성능검증 정확도 향상

○ **(스마트 안심점포 확산)** 국내 보안기술*을 집약시킨 **'한국형 무인점포'**를 구현하고, 실증을 통해 상용화 추진(~'25)

* AI(객체인식, 모션인식)인지, 자동인증·결제, 성인인증 기술 등 기존 외산기술(클라우드픽(중국), AIFI(미국)) 대체

- (**무인기술 확산**) 개발된 우수 무인기술·제품을 **소상공인 무인점포에 지원하여 범죄 등 사회문제를 해결**하고, 무인보안 시장 확대 추진

※ 경찰청 및 지자체와 협력, 출입통제장치 및 지능형 CCTV 등 지원 후 범죄발생율 등 성과 추적('23, 총 120개소)

2. 협업 기반 조성을 통한 신흥시장 진출 강화

기업 간 협력을 기반으로 한국형 통합보안 모델을 구현하고, 신흥시장을 전략적으로 공략하여 글로벌 시장 경쟁력 확보

① 통합보안 모델 구축을 위한 「**K-시큐리티 얼라이언스**」 **추진**

○ (**통합보안 협업체계 강화**) 혁신적인 **통합솔루션·서비스 개발**을 위한 **민간주도형 전략적 협업 체계 강화** 추진('24년~)

- 민간주도 공동·협업 **통합보안 사업화모델, 표준화 및 상호운용성** 확보 등을 유도하고, **판로·투자·해외진출**시 우선지원

※ 전문기관, 출연연, 민간 전문가로 구성된 전문지원단을 통해 기술·법률·경영 등 분야별 애로해소 및 판로와 해외진출 지원

○ (**통합보안 시범사업**) 현장수요 기반 **우수 통합보안 모델***을 **우선 선정**하고, **시범사업**을 통해 개발하여 **협업 활성화 마중물**로 활용('24~, 年 5개)

* 통합보안 모델(예시): 이벤트 로그(SIEM) + 엔드포인트 보안(EDR) + 자동화된 통합관제(SOAR)가 결합된 단일 통합 솔루션 등

② 국제협력 기반의 신흥시장 진출 가속화

○ (신흥국 외교협력) 정상외교를 통해 조성된 중동·동남아 지역 협력 분위기를 우리기업의 진출 기회로 활용하기 위한 외교협력* 강화('23~)

* 사우디 사이버안보국(NCA), 아랍 ICT기구(AICTO), 인니 국가사이버암호원(BSSN), 베트남 정보보안청 등 주요국 사이버보안 유관기관과 고위급 면담 및 협정체결을 통해 기업 간 투자·공동사업 협력기반 마련

○ (전략거점 재편·확대) 신흥시장 집중공략을 위해 중동거점을 사우디로 재편하고('23.7~), 베트남 거점을 신설('23.12~), 6대 거점 중심 진출 지원 강화

※ 現 해외 5대 전략거점: 미국(실리콘벨리), 동남아(인니), 중동(오만), 아프리카(탄자니아), 중남미(코스타리카)

○ (민·관 협력 조달수주) 중동·동남아 기금 · 공공조달 사업 프로젝트 수주를 위한 민·관 협력형 '시큐리티 팀 코리아*' 구성·지원('24년~)

* 동남아(인력 양성, 전자서명인증), 사우디(드론·스마트시티) 등 현지 수요기반 사업화 타당성 조사 지원(~'27년 15건) 공공부문의 주도로 수주 가능성을 극대화하고, 수주 후 국내 사업자 참여를 통해 기업의 간접 수출 효과 제고

우수사례 ASEAN Cyber Shields Project

韓-ASEAN 경협기금 사업으로, KISA가 프로젝트 제안 및 대표 계약자로 사업수주 후 공개입찰로 국내 보안기업을 수행사업자로 선정(3년 간, 120억 원 규모)

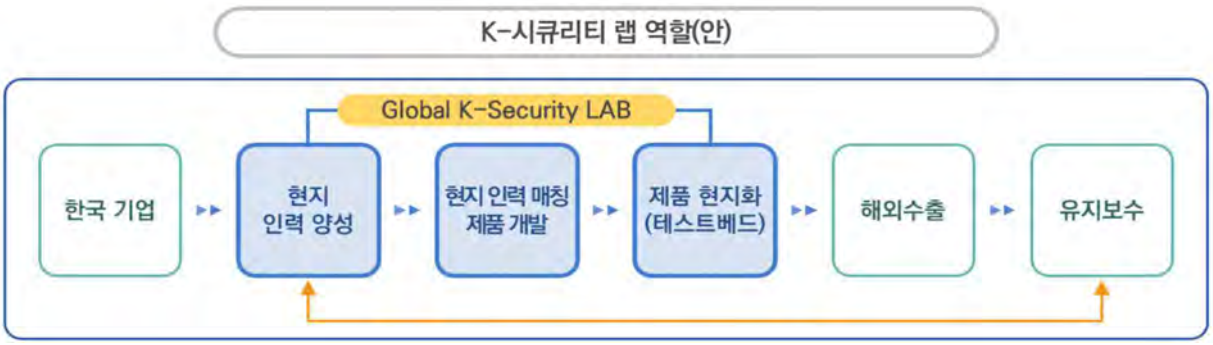
③ 우리 기업의 현지 애로해소 등 수요 중심의 해외진출 지원 확대

현장 의견

- 보안 분야만의 현지 애로사항을 잘 해결해 줄 수 있는 조력자가 없음
- 현지 문화와 시장을 잘 아는 숙련된 보안 분야 인력 수급이 어려움
- 해외 사업수주를 위해 국제인증 취득은 필수적인데, 고비용와 긴 시간으로 고통
- 스타트업은 기술력 좋아도 글로벌 진출을 위해 어디부터 준비할지 막막

○ (현지 인력양성 플랫폼 구축) 해외거점과 연계하여 양질의 현지 인력을 확보하고, 제품개발 및 현지화까지 연결하는 'K-시큐리티 랩' 구축('24~'27)

※ [1단계] 우리기업의 베타버전 개발과제 제출 → [2단계] 과제별 현지 인력 선발 및 프로젝트형 교육 → [3단계] 인턴십 혹은 정규 직원 채용 후 개발제품의 실증 및 현지화 수행



○ **(해외인증) 주요 해외 보안인증**(국제CC, Mitre Att&ck, CE 등) **취득 비용**(상한액 0.75억→1.5억) **및 지원 기간 확대**(1년→2년) ('24~'27)

※ 해외거점 등 국제협력을 통해 국내 보안인증(IoT보안인증 등)과 해외인증 간 상호인정, 동등성 평가 확대 추진('24~)

○ **(마케팅 및 판로개척) 수출 경쟁력이 있는 스타트업**의 유망 기술 발굴, 레퍼런스 확보 및 **해외진출까지 전주기 지원 강화**('23~'27)

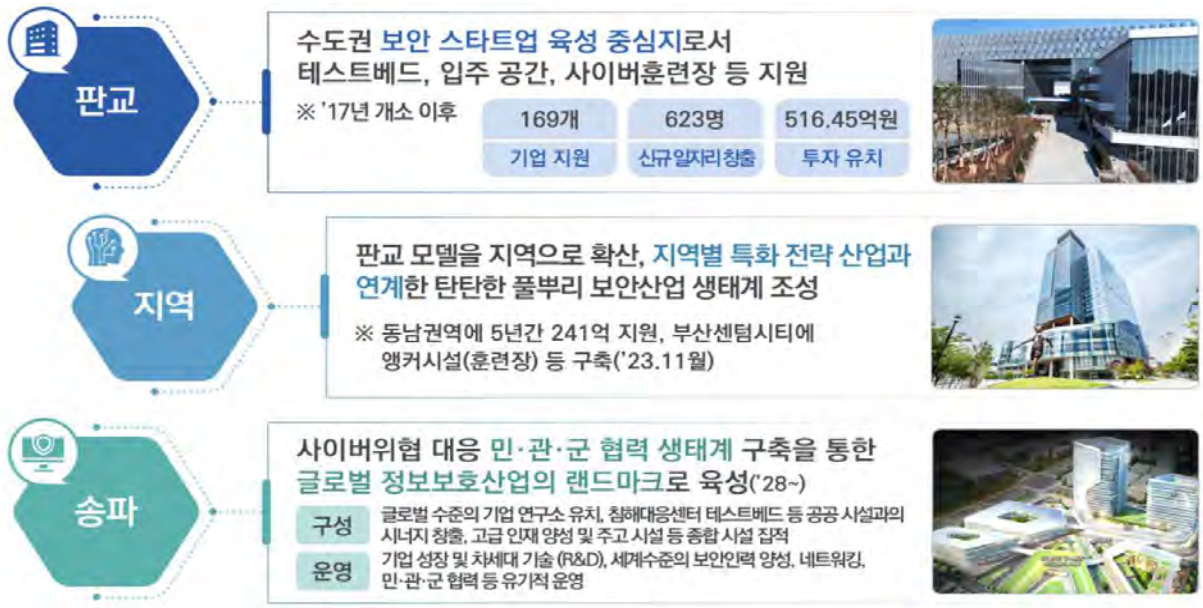
※ 글로벌 시장 內 인지도 부족 해소를 위해 글로벌 시장조사기관(IDC, 가트너 등) 마켓가이드에 국내 기업의 솔루션 등재 지원(가이드배포, 전문애널리스트 코칭·컨설팅 등) 추진('24~'27)

3. 글로벌 공략을 위한 단단한 산업 생태계 확충

우리 보안기업의 글로벌 시장진출 가속화를 위해 시설확충·펀드조성·인재양성 등 지속성장 환경 조성에 집중 투자

① 우리 기업의 **해외진출 가속화를 위한 전진기지 구축**

○ **보안 스타트업 육성**판교 **및 지역 보안산업 강화**부울경**, 글로벌 시큐리티 클러스터**송파로 구성된 「**K-시큐리티 클러스터 벨트**」조성 추진('23~)



② **사이버보안 펀드를 조성하여** 민간투자의 마중물로 활용

○ **(펀드조성)** 기업의 안정적 기술개발 및 민간투자 활성화를 위해 민관 합동으로 「**사이버보안 펀드**」 **조성**(~'27, 총 1,300억 원 규모)

※ 연간 300억 원 규모 투자시, '30년에 일본 사이버보안 시장규모 추월전망(사이버보안 펀드 조성방안 연구, '22, KISA)

「사이버보안 펀드」 기본구조(예시)

○ (**투자활용**) AI 및 제로트러스트 등 유망 분야 **스타트업 지원** 및 기업 간 M&A를 통한 **스케일업 지원**에 **집중 투자** 유도(펀드결성액의 50%이상)

※ △ 스타트업 분야: 유망신기술(AI, ZT, 양자 등) 및 원천분야(네트워크, 5G, 암호 등) 제품·서비스 개발 및 사업화
△ M&A분야 중소·중견 사이버보안 기업의 인수합병을 통한 통합 제품·서비스 개발 및 사업화

③ 글로벌 보안시장의 주인공, **정보보호 전문 인력양성**

○ (**산업수요형 인재**) 정보·물리보안 분야 **현장 연계를 강화**하는 **수요기반형 실무 인재**양성 프로그램 확대·강화('23~'27)

※ △ **(K-Shield·주니어**, '23~'27, 3,800명) 모의해킹, 보안컨설팅, 침해사고 대응 등 직무중심 기술교육 및 취업지원
△ **(시큐리티아카데미**, '23~'27' 1,000명) 기업이 선발→교육→취업을 주도하고 정부가 지원(직무/기업 중심)
△ **(S-개발자**, '23~'27, 250명) IT개발 인력을 선발하여 보안제품 개발 및 취·창업을 지원

○ (**민·관·군 인재**) 대학·군·공공부문 보안인력의 전문성 강화를 통해 **국가 사이버위협 대응 및 사이버범죄 대응역량** 제고('23~'27)

※ △ **(民, 분야별특화)** 정보·물리보안 관련 대학(원) 지원사업을 통해 新보안체계 환경에 적합한 분야별 특화인력 양성
△ **(官, 실무강화)** 전자정부 보안, 정보시스템 위험진단 기술 등 실무형 보안역량 교육 강화
△ **(軍, 사이버탈피오트 지원강화)** 우수 인력 선발→軍 사이버분야 근무→취업과 연계하는 '사이버 탈피오트'의 재직역량과 취·창업 강화를 위한 지원프로그램 확대 등 고도화 추진

○ (**인프라 확충**) 우크라이나 발전소 해킹과 같은 **실제사례** 및 자율차 등 **미래 핵심서비스의 취약점 활용 훈련 인프라*** 확충('23~'27)

* 실제 사고기업/조직 인프라, 공격방법 등을 가상자원(VM)화하여, 교육·훈련에 활용

- (**훈련장 확대·고도화**) 다양한 침해사고 인프라 환경 구축으로 실전과 동일한 교육훈련이 가능한 **'사이버훈련장**(Security-Gym)' **확대**(1개 → '23, 2개)

※ 실전형 공방훈련 시나리오 확대('23, 7종→'26, 10종) 및 실습 보안제품도입 확대('22, 2종→'23, 12종)

4. 차세대 정보보호 기술 경쟁력 확보

미래 산업 성장에 필수적인 전략기술 개발에 집중하고, 선도국과의 공동연구 추진으로 글로벌 기술 패권 경쟁에서 우위를 점할 수 있는 기술력 확보

① 미래 대응에 필요한 **사이버보안 중점기술 확보**

○ 국내·외 기술·시장 분석 통해 **①미래 도전, ②기술·산업 선도, ③안보 투자** 등 주요 R&D 영역을 도출하고, 영역별 전략적 투자 추진('23~)

차세대 정보보호 기술 R&D 추진방향

구분	주요내용 및 방향	주요 기술분야
미래도전 R&D	현재 국내 기술수준은 낮으나, 글로벌 시장 임팩트를 고려하여 미래 산업 경쟁력을 선제적으로 확보하기 위한 도전적 분야	AI·클라우드 보안, 제로트러스트, 위협인텔리전스, XDR, 신산업·융합보안
기술산업선도 R&D	국내 기술수준이 높은 기술을 대상으로 글로벌 기술 주도권 및 수출경쟁력 확보가 필요한 분야	양자내성암호, 프라이버시 강화 기술
안보 투자 R&D	해외시장 규모가 협소하고, 국내 기술수준도 낮으나 국가안보·국민안전과 연관된 핵심기술로 지속 투자가 필요한 분야	공격억지·선제면역·회복탄력

② **국제 공동연구**를 통한 글로벌 **보안기술 경쟁력 확보**

○ **(선도국 협력연구) 미국·독일·핀란드 등** 사이버보안 분야 강점을 지닌 선도국과 **공동 연구**를 통해 **글로벌수준 기술 확보**(~'27)

글로벌 선도국별 강점분야 및 공동연구 추진 방안

	강점 분야	추진 방안
미국	• CISCO, IBM, 구글 등 글로벌 기업이 클라우드, 사이버위협 추적 등 세계 최고 기술력을 보유, 스타트업도 활발	• 클라우드 보안·가상자산 불법 행위 추적기술, 인공지능 활용 보안 기술 등 공동 연구 * 韓과기정통부-美국토안보부(DHS) 공동연구 논의
독일	• Platform Industries 4.0 등 스마트공장 기술력 보유 • 스마트카, 모빌리티 기술력을 바탕으로 보안 연구 활발	• AI기반 스마트 공장 보안 기술 고도화 등 연구 * 독일 CISPA(독일 최대 연구 기관 헬름홀츠 연구협회 연구센터) 등과 공동연구 논의

○ **(신흥국 지원연구)** 동남아·중동 등 주요 **신흥시장을 전략적으로 공략**하기 위한 **현지 시장 수요기반 보안기술** 공동개발(~'27)

※ 협력연구(예시): △ 동남아(전문인력 양성체계, PKI 등 인증제도), △ 중동(스마트시티보안, 통합관제 등)