

디지털 대전환시대 정보보호산업의 전략적 육성 방안

2022. 2. 10.

관 계 부 처 합 동

순 서

I. 추진 배경	1
II. 현황 및 평가	2
III. 목표 및 전략	5
IV. 주요 추진 과제	6
1. 성장 동력 확보를 위한 정보보호 新시장 창출	6
2. 글로벌 일류 정보보호기업 육성	9
3. 정보보호산업 기반 강화를 위한 생태계 확충	11
4. 차세대 정보보호 기술경쟁력 확보	15

I. 추진 배경

- 최근 사이버 위협이 국민생활 및 경제전반과 밀접한 분야에서 발생하면서, 디지털 경제 성장을 위해 정보보호 안전망 확충이 긴급
- 사이버 대응력 확보는 정부 정책만으로는 한계가 존재하고 민·관 협력이 필수적인 분야로, 정보보호산업의 고도화가 필요

- ▶ 사이버 공격으로 인한 **글로벌 경제피해** ('15)3조\$ → ('21)6조\$('20 Cybersecurity Ventures)
- ▶ 전세계 **최고경영자(CEO)**는 올해 회사의 성장을 위협할 **최대 글로벌 리스크** 1위로 **온라인 환경에서의 정보유출** 등 '사이버 리스크'를 꼽음(PwC 2022년 글로벌 CEO 설문조사)

- **코로나19 장기화로 인한 비대면 문화 확산** 속에서, 우리 정보보호 기술과 기업을 통해 디지털 자산을 보호해야 할 필요

※ 국가차원에서 반드시 확보해야 할 국가필수전략기술로 사이버보안 선정

- ▶ 「글로벌 기술패권 경쟁에 대응한 국가필수전략기술 선정 및 육성·보호전략」, 과기장관회의('21.12.22)



- 디지털 전환 가속화로 정보보호의 영역이 제조·유통·의료 등 **소산업** 영역으로 확장되면서 정보보호 제품·서비스 수요 증대

- 이에 따라 국내 정보보호산업이 **높은 성장률***을 보이면서, 새로운 경제 성장 기회를 창출하는 **국가 전략산업**으로 주목

* 국내 정보보호시장의 최근 3년간('18~'20년) 연평균 성장률은 8.4%로, 동기간 한국 경제 성장률('18년 2.9%, '19년 2.2%, '20년 -0.9%)을 상회

⇒ 국가 차원에서 정보보호산업을 **전략적으로 육성**하여 **사이버보안 대응력을 강화**하는 한편, **새로운 경제 성장 기회**로써 활용할 필요

Ⅱ. 현황 및 평가

□ 정보보호산업 시장 현황

- (개념) 정보보호 산업은 정보보호제품을 개발·생산·유통하거나, 보안 컨설팅, 보안관제 등 정보보호서비스를 수행하는 산업을 의미
 - 해킹, 데이터 유출로부터 PC·네트워크를 보호하기 위한 정보보안과, 재난·범죄 방지를 위한 CCTV, 출입통제 장비 등 물리보안으로 분류
 - 최근 전통산업과 디지털의 융합에 따른 디지털 융합 시장으로 보안의 범위가 확대되면서 융합보안 시장*의 성장이 예측
- * 스마트공장, 스마트카 등 디지털 융합산업의 정보보호 내재화를 위해 새롭게 창출된 시장
- * 디지털 전환 시장에서 정보보호가 차지하는 비율은 약 13.8~15%로 전망(markets&markets)

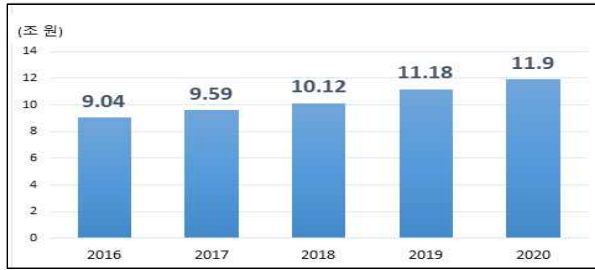
< 정보보호산업의 정의 >

“정보보호를 위한 기술 및 정보보호기술이 적용된 제품을 개발·생산 또는 유통하거나 이에 관련한 서비스를 제공하는 산업(정보보호산업법 제2조)”

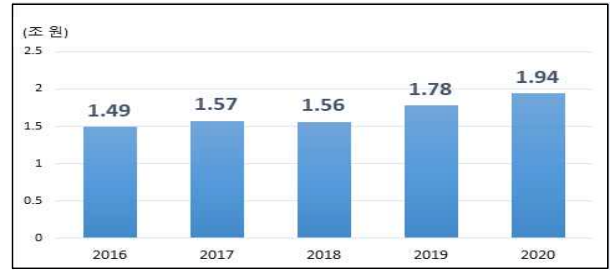
정보보안	물리보안	융합보안
“클린인터넷경제”	“안전안심생활”	“안전성강화”
		
네트워크 상의 정보 유출·훼손 방지	재난·재해, 범죄 등 방지	他 산업분야의 보안내재화

- (국내시장) 국내 정보보호시장 매출액은 최근 3년간 연평균 8.4%* 성장, 수출액은 연평균 11.5% 성장하는 등 고성장 중
 - * 소프트웨어(SW) 산업 매출액 성장률 '18년 4.6%, '19년 4.4%, '20년 2.8%(SPRI), 제조업 출하액 성장률 '18년 3.4%, '19년 -1.4%(KOSIS)를 상회
- 비대면·언택트 환경의 확산으로 네트워크 보안(정보보안), 비대면 출입통제(물리보안) 등 보안제품의 수요가 증가하면서 성장세 뚜렷

<정보보호산업 매출액('16~'20년)>



<정보보호산업 수출액('16~'20년)>



- (국외시장) 글로벌 사이버보안 시장규모는 '20년 1,319억 달러로 전년대비 약 4.8%성장하였으며, '24년까지 연평균 9.4%의 성장 전망
 - 미국, 유럽 등 주요 선진국이 시장의 90%이상을 차지하고 있으며, 이스라엘이 높은 기술력을 보유, 중국이 새로운 보안 시장으로 대두
 - 미국, 중국 등 주요국은 사이버보안을 경제 활력 제고 요소로 인식하고 국가 차원의 사이버보안 발전 전략 수립
- ※ 미국 Endless Frontier act에서 10대 핵심기술로 데이터관리·사이버보안을 선정
중국 사이버안보 산업발전 3개년(2021~2023) 행동계획안 발표 등

<글로벌 정보보호 산업 시장규모 및 성장률 전망 >

구분	2020	2021	2022	2023	2024
시장규모(억 달러)	1,319	1,432	1,570	1,722	1,887
성장률(%)	4.8	8.6	9.7	9.7	9.6

※ Gartner(2021), 'Forecast: Information Security and Risk Management

□ 정보보호 기술 현황

- 디지털 대전환에 따라 비대면 환경과 디지털 경제 인프라를 뒷받침하기 위한 제로트러스트, 데이터보호 등 기술 개발 증가
 - (제로 트러스트 보안) 비대면 환경 확산에 따라 경계망 보호(방화벽, VPN 등)에서 사용자 중심 비경제 보안기술* 연구가 진행 중
- * 2023년까지 전체 기업의 60%가 사설가설망(VPN)에서 벗어나 제로 트러스트(Zero Trust) 기반으로 보안 개념을 바꿀 전망('20, Gartner)
- (데이터 보호) 안전한 데이터 이용을 지원하기 위한 암호기술, 프라이버시 보호 기술 등 데이터 보호기술 활용 확산 전망

- AI를 폭넓게 활용한 보안기술 도입이 시도되고 있으며, 6G, 양자 등 미래 신기술에 대한 정보보호 원천기술 개발 진행 중
 - (AI 보안) 보안 프로세스(모니터링-분석-사고대응) 쏘과정에 AI를 접목하여 보안 위협 자율 대응*과 AI 역기능 해결을 위한 연구 진행 중
 - * SK인포섹, Palo alto 등 민간기업을 중심으로 AI 기반 보안 자동화 대응(Security Orchestration, Automation and Response)기술을 활용한 보안위협 대응 자동화 추진 중
 - (미래 기술 전략 대응) 글로벌 환경에서 사이버보안 주도권확보를 위해 국가 간 6G 보안*, 양자 보안**분야 기술 개발 국제 협력 확대
 - * 핀란드(오울루대) 주도로 세계최초의 '6G 플래그십 프로젝트' 추진 중('18년~)
 - ** 美 표준기술연구소(NIST)에서 차세대 암호화 알고리즘을 위한 표준을 공모 중

□ 그 간의 성과 및 평가

- '한국판 뉴딜('20.7)'의 일환으로 'K-사이버방역 추진전략('21.2.)'등 정책추진을 통해 국내 정보보호산업의 양적 성장*을 달성했지만, 분야별 전문화 및 기업 대형화 등 기업의 질적 성장 필요**
 - * 국내 정보보호기업 수 : '16년 864개 → '20년 1,283개, 48% ↑
 - ** 전세계 사이버 보안 유니콘 기업 42개 중 한국기업 전무(CB insights, '21.12.31.기준)
- | 국가 | 미국 | 이스라엘 | 캐나다 | 영국 | 스위스 | 중국 |
|----------|-----|------|-----|----|-----|----|
| 유니콘 기업 수 | 31개 | 6개 | 2개 | 1개 | 1개 | 1개 |
- 인공지능·비대면 보안 등 새로운 보안 시장에서 전문기업으로 성장하기 위해 선도제품 개발 및 차세대 보안기술 확보 필요
 - 글로벌 경쟁력을 갖춘 대형 보안기업 육성을 위해 해외 판로 개척, 국내 보안 기업 간 협업 활성화, 정보보호 투자 확대 요구
 - 지속적인 R&D 투자*와 우수한 ICT 인프라를 바탕으로 선도국(미국)과의 기술격차(88.4%, 1.0년)를 줄이는** 등 경쟁력 유지 중
 - * 정부 사이버보안 R&D 예산 : '17년 546억원 → '22년 928억원
 - ** '15년 81.7%(기술격차 1.5년) → '20년 88.4%(기술격차 1.0년)
 - 하지만, 미국과의 격차는 여전히 존재하며, 최근 중국(91.6%, 19년)에도 추월을 허용하는 등 글로벌 기술경쟁력 확보 시급

Ⅲ. 목표 및 추진전략

비전

튼튼한 정보보호산업 육성으로
안전한 디지털 전환 구현

목표

정보보호산업 시장규모 2025년 20조원 달성

※ '20년 11.9조원 → '25년 20조원

추진 전략

[전략1]

성장 동력 확보를 위한
정보보호 新시장 창출

① 인공지능(AI)기반 보안 산업 활성화

② 비대면 서비스 보안 시장 개척

③ 융합보안 산업 저변 확대

[전략2]

글로벌 일류
정보보호기업 육성

① 신성장 리딩 기술·제품 사업화

② 정보보호 초기기업 성장 지원

③ 정보보호기업 해외진출 가속화

[전략3]

정보보호산업 기반 강화를 위한
생태계 확충

① 정보보호공시제도 의무화

② 정보보호인증 고도화

③ 중소기업·지역 사이버보안 안전망 확충

[전략4]

차세대 정보보호
기술경쟁력 확보

① 정보보호 新기술 개발

② 디지털 인프라 보안기술 확보

IV. 주요 추진 과제

전략1. 성장 동력 확보를 위한 정보보호 新시장 창출

◇ 인공지능(AI)·비대면 서비스·융합보안 등 국가경제 및 국민 생활과 밀접한 분야의 신규 보안제품·서비스 개발 및 시장 선도

1 인공지능(AI) 기반 보안 산업 활성화

- (AI 보안기업 육성) 지능화되는 보안위협에 대응하여 제품·서비스 개발에 인공지능 기술을 활용하는 AI 보안 기업 단계별 집중 육성('21~'25년 60개社)
 - 차별화된 3개 분야별(①AI For Security, ② AI 융합보안, ③ AI 역기능방어) AI 보안제품 개발사를 발굴하여 시제품 개발 지원(1년차, '21년~)
 - 시제품 개발 완료 기업 중 우수 기업을 선별하여 수요 기반의 실증 및 테스트를 지원하고, 판로개척·해외진출까지 연계 지원(2년차, '22년~)



- (데이터셋 개방) 산·학·연 수요 기반의 사이버보안 AI 데이터셋을 구축·개방하여 AI 적용 보안제품·서비스의 성능 고도화 뒷받침
 - 가공·비식별·라벨링 등 AI 데이터 전주기(life cycle) 처리를 통해 악성코드, 침해사고 등 정보보안 데이터 8억여 건 개방('22년~)



- 싸움, 쓰러짐, 화재 등 재난·안전 물리보안 데이터(1,154GB)를 개방하고, Edge영상분석, 상황예측형 등 물리보안 영상데이터(5종) 신규 구축('22년~)



② 비대면 서비스 보안 시장 개척

- (온라인) 디지털·비대면 4대 분야 서비스에 신 보안기술을 적용하여 안전과 신뢰의 비대면 서비스로 전환 가속화
- 원격의료지원 서비스(만성질환 등)와 메타버스 기반의 비대면 서비스(회의, 교육, 메타커머스)를 보안성이 확보된 온라인 안심서비스로 전환('22년~)
- ※ 비대면서비스 보안 기술 개발·상용·사업화, 해외진출 지원까지 One-stop으로 지원하여 新보안시장 창출 및 보안 산업 확대('22년 4개→'23년 7개→'24년 10개→'25년 15개)

비대면 진료	비대면 근무	비대면 교육	온라인 유통·결제
			
(예시) 만성질환 등 취약계층 건강모니터링 시스템 보안	(예시) MS'팀즈 회의에 메타버스 프라이버시 보안	(예시) 이투스의 초·중·고 개인화 학습플랫폼 보안	(예시) 제페트의 편의점, 백화점에 NFT 메타커머스

- (오프라인) 안심스마트점포 모델* 확산을 통해 무인점포 이용자의 안전을 제고하고, AI·융합보안 원천기술 확보 및 고도화

* 사용자 인증, 출입, 결제 등 일련의 과정이 무인자동화 시스템으로 처리되는 형태의 점포(예시: Amazon Go)에 물리보안 기술이 결합되어 보안성이 강화 모델



- 안심스마트점포 보안모델(2호점 등) 확산('22년~) 및 테스트베드* 구축·지원을 통해 지능형(AI) 물리보안 솔루션의 보안성능 제고

* 중소기업의 지능형(AI) 물리보안 솔루션을 고도화할 수 있도록 실운용 상황에서 학습

- 新스마트(물류, بانک 등) 분야*에 안심보안기술 발굴·적용확대('22년~)

* 비대면 전환으로 보안이 취약해 해킹, 화재, 침입 등 안전사고 발생 위험이 높은 분야

③ 융합보안 산업 저변 확대

- 5G+ 융합보안 거점 기능 강화로 안전한 5G 융합서비스* 환경조성

* (5G+ 전략 5대 서비스) 디지털헬스케어, 스마트공장, 자율주행차, 스마트시티, 실감콘텐츠

- (헬스케어) 의료기기 제조사 접근성 제고를 위해 의료기기 허가·심사용 보안성시험(IoT보안인증 연계)을 전국 보안리빙랩(5개소)으로 확대('22년~)
- (제조) 스마트공장(시화,창원 등) 생산공정 운영기술 보안 강화 확대
- (차량) 자동차융합기술원 기능안전 시험을 연계한 보안성시험 추진



- 융합·제조 산업 실수요자를 대상으로 원스톱(보안점검툴→컨설팅→솔루션제공 등 체계) 패키지 보안적용* 지원 확대('22년~)
 - * (원스톱 패키지 보안적용) '23년 30개社 → '24년 50개社 → '25년 70개社
- 융합산업 분야의 자발적인 보안내재화 유도를 위해 '보안적용 인증마크' 및 '융합보안 전문서비스 기업' 지정 제도 마련('23년~)
 - ※ 융합서비스 보안 인센티브 및 거버넌스 마련('23년), 보안적용 인증 기기와 범위 고시('24년), 보안적용 검증 및 인증마크 발급('24년~)
- 일상생활 주변에 쉽게 접하고 실제 보안위협이 발생한 스마트선박*, UAM(드론), 스마트팜 등 신규 융합서비스 보안 내재화 추진
 - * 국내 H선사('19) 및 미국 샌디에고 항만('18) 랜섬웨어 감염, 독일 선사 항해시스템 해킹('17) 등 선박과 항만 대상 보안위협 증가에 따라 국제기구, 협회에서 사이버보안 대응 필요성 강조

전략2. 글로벌 일류 정보보호기업 육성

◇ 혁신기업 발굴·지정 및 사업화 지원, 기업간 협업 및 M&A 활성화, 해외 판로 개척 지원을 통해 글로벌 경쟁력을 갖춘 정보보호기업 육성

① 신성장 리딩 기술·제품 사업화

- 고도화된 사이버 보안 위협에 대응하기 위해 글로벌 기업 간의 기술 격차가 큰 제품을 과제로 선정하여 전문기업 육성 지원('22년 4개 과제)
 - ※ 차세대 보안 핵심 기술은 소수 글로벌 보안기업으로 편중되어, 국내 보안기업의 경쟁력은 미약한 수준 (미국 대비 국내 기술 수준은 89.7% 수준)
- 사업성을 인정받은 우수 정보보호 기술·제품* 기업 대상 정부정책 사업 집중 지원 등을 통해 판로개척 후속 지원('22년~)
 - * '18년 제도 시행 후 '21년까지 15개 기업을 선정했으며, 선정된 기업은 시장에서 기술의 우수성을 인정받아 약 35% 매출성장 실적을 보임
 - 공공기관 제품 도입 우대*, 정부정책사업 우선지원**, 혁신제품지정 등 지정 기업들의 지속성장 가능한 환경 조성('22년~)
 - * 공공발주협의회 회원사(정부부처 및 산하 공공기관) 대상 발주 시 가점 부여
 - ** 인증비용지원, 해외전시회 참여 및 맞춤형 수출지원 등 우선지원

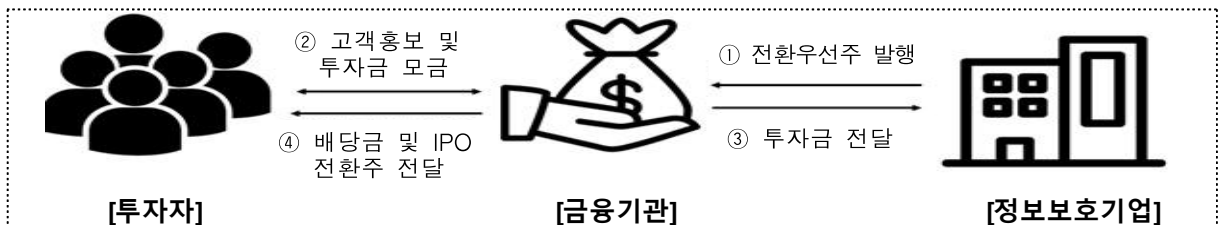
② 정보보호 초기기업 성장 지원

- 국내 육성 프로그램 + 해외 육성 프로그램 + 기술가치평가 3단계 원스톱 지원으로 맞춤형 기업 육성 프로그램 운영('22년~)
- 역량강화 및 기업가치평가 결과를 바탕으로 투자유치, M&A가 이뤄질 수 있도록 IR데이, M&A 수요연계 네트워킹 행사 연계



- 국내 보안기업의 제품·서비스 개발, 수출 관련 금융 애로사항 해소를 위해 안정적인 자금 운용 및 투자·융자 수혜 기회 확대
- 정보보안 분야 비상장 우수기업을 선발하여 금융기관과 협업을 통해 벤처기업 투자 상품 개발 및 정보보안 기업 IPO 상장 기반 마련

<참고> 금융상품 연계(안)



③ 정보보호기업 해외진출 가속화

- 효과적인 글로벌 판로개척을 위해 권역별 정보보호시장 현황에 따른 맞춤형 목표설정 및 5대 해외거점을 활용한 집중 공략

<권역별 맞춤형 지원(안)>

권역	유망분야	지원방안
미국	CCTV 등 물리보안	- 물리보안 분야 선점 기업 정보 및 수출 지원·규제 정책 분석을 통한 전략 수립 및 핵심 수요자 파트너 발굴
동남아	비대면 서비스 보안	- 현지 핵심 플레이어(은행, 보험사 등)와의 파트너십 구축 및 타당성조사, PoC 추진을 통해 현지 사업실력·업계 평판 축적 지원
중남미	국가안보 프로젝트	- 국제개발은행(CABEI 등) 및 협력기구의 공적기금을 활용, 대규모 치안 확보 보안 인프라 프로젝트 수요 제기 및 사업화 추진

- 국내 정보보호기업의 해외진출을 위해 선결적으로 해소되어야 할
성능인증, 인지도 제고, 코로나19 장벽 등 극복 지원
- (해외인증) 정보보안·물리보안 제품의 미국, 유럽 등 해외 선진시장
진출을 위한 필수요건인 정보보호 해외인증 획득지원
- (글로벌 경진대회 참가) 국제적 보안 경진대회*에 국내기업이
참가하고 입상할 수 있도록 집중적 지원체계** 마련('22년~)
 - * 글로벌 최대 보안 행사인 RSA에서 개최되는 Innovation Sandbox Contest 등
 - ** 지원사항 : 대회별 트렌드 및 평가 주안점 분석, IR 전문가 코칭, 피칭 영상 제작 등
- (클라우드마켓) 글로벌 클라우드 마켓플레이스 등록 지원*을 통해
코로나19로 인한 해외영업 제한 등 한계 극복 및 판로 확대('22년~)
 - * MS Azure, AWS등 글로벌 CSP(Cloud Service Provider) 등록을 위해 MSP(Managed Service Provider) 사업자 활용 컨설팅, 구축서비스, 운영 등 클라우드 전환지원
- 한국형 비대면 서비스 보안모델(비대면 서비스+보안솔루션) 해외전파를
위해 수요처 기반 현지·초청 쇼케이스 개최 및 해외실증 지원('22년~)

전략3. 정보보호산업 기반 강화를 위한 생태계 확충

◇ 정보보호공시제도 의무화, 정보보호인증 고도화, 중소기업·지역
사이버보안 역량 강화 등 지속성장을 위한 산업 생태계 조성

① 정보보호공시제도 의무화

- 이용자의 알권리를 보호하고, 기업의 정보보호 관련 투자를 촉진
하기 위하여 정보보호 공시 의무화 시행('22년~)

< 정보보호공시제도 의무화 >

- (개념) 정보보호산업법 제13조(정보보호공시)를 근거로 정보보호 투자 및 인력 현황,
정보보호 관련 인증 등 정보보호 현황을 공개하는 제도
- (목적) 국내 기업·기관의 정보보호 수준 제고 및 이용자의 안전한 인터넷 이용환경 조성
- (의무화) 정보보호산업법 시행령 개정('21.12.9(목) 시행)을 통해 ▲사업분야, ▲매출액,
▲이용자 수에 따른 의무대상 기준 및 예외 규정 신설



- 전자공시시스템 도입으로 분야별 현황 및 투자 증감 추이를 공개하고, 정보보호 투자 현황 보고서 발간하여 경쟁적 투자 유도
 - ※ 6월까지 정보보호공시 이행을 완료하고, 9월 정보보호공시 결과 공개 및 보고서 발간
- 의무화 제도의 안정적 시행을 위해 사전 컨설팅 및 정보보호 공시 가이드라인을 제공하고, 사후 검증 확대를 통해 신뢰도 제고
 - ※ 사전 컨설팅 '21년 50개사 → '22년 120개사, 사후 검증 '21년 2개사 → '22년 24개사

② 정보보호인증 고도화

- (IoT 인증고도화) 열화상카메라, 홈IoT(도어락, 월패드) 등 다양한 분야로 인증 확대하여 해킹을 대비한 정보보호 내재화 기반 마련
 - IoT 보안인증* 증가 및 신규 수요 충족을 위해 시험자동화 도구** 및 신규 인증대상(드론, 의료 X-ray 등)*** 개발 등 효율적 보안인증 추진
 - * 보안인증(수) : '20년 41건 → '21년 73건 → (목표확대) '22년 90건 → '23년 100건
 - ** 제조사 자체 보안성을 시험하도록 일부 시험항목의 '자동화 툴' 개발('22~'25년, R&D)
 - *** 드론, 의료 등 다양한 분야의 대상제품 발굴과 시험지원 및 인증기준개발 추진
 - 홈 네트워크 보안 강화(망분리, 보안충족, 인증제품 등 고시)를 반영한 홈·가전 IoT보안을 신축 주택에 적용('22.7~) 및 조기 안착 지원
 - ※ 월패드 등 해킹 예방을 위해 신축 건설사를 대상으로 홈 IoT 보안점검 및 컨설팅 추진

- (정보보호제품 성능평가) 성능이 검증된 우수 제품의 확산을 통해 정보보호 산업 경쟁력을 제고하기 위한 정보보호제품 성능평가 제도개선 추진
 - 기존 제품군 기준 업데이트 및 수요기관·개발업체 의견수렴을 통해 도출된 시장요구형 신규제품군(EDR, 단말 이상행위 탐지 및 대응제품) 기준 개발('22년~)
 - AI 기반 제품의 상용화와 서비스 확산 및 안전·신뢰성을 검증할 수 있도록 「정보보호산업지원센터*」 內 시험·개발환경 확대
 - * 정보보호시스템/네트워크 제품 및 바이오인식 제품 테스트랩실 구성
- (지능형CCTV) 국민안전 분야 신기술* 도입에 쓰이는 이상상황(이동중 쓰러짐, 원거리 범죄(폭력,스토킹)상황포착 등)을 평가항목 추가·개발
 - * 마스크 착용자 얼굴인식 기술, 3D 영상 영상보안 시스템, 스마트시티 전용 안전플랫폼
 - 비대면 확산으로 이용이 큰 스마트빌딩(점포 등)에서 운영하는 물리보안 통합플랫폼 연동·분석·검증 기술('22~'25년)과 평가 연계
 - 소기업(점포)의 안전을 위해 검증된 물리보안 솔루션* 확산·고도화
 - * 일반 CCTV 영상을 저사양 PC(AI 박스)로 분석하여 이상행위(절도 등)를 인식하는 솔루션
- (CC인증) 정보보호업계를 위한 보안적합성* 사전인증 요건 확대, 제도 이해력 제고를 위한 국가용 보호프로파일** 개정 등 시장 친화형 방안 마련
 - * 보안적합성: 국가·공공기관이 도입하는 정보보호제품의 안전성 검증 제도(국정원 운영)
 - ** 국가용 보호프로파일: CC인증 시 적용하는 사전인증 대상 제품군별 보안규격
 - 공공기관이 다양한 보안기능을 가진 새로운 정보보호 제품을 제때 도입할 수 있도록 사전인증 요건을 확대*하여 업계 부담 완화
 - * 기존: CC인증만 가능 → 확대: CC인증, 정보보호제품 성능평가, 보안기능 확인서

③ 중소기업·지역 사이버 보안 안전망 확충

- 보안 투자여력이 부족한 중소기업 8,300개사('22년)를 대상으로 보안제품 도입과 데이터 백업을 지원하여 민간영역 보안투자 마중물 마련
 - 민·관 합동으로 백신, 탐지·차단SW 등 보안솔루션을 지원하고, 소규모 중소기업을 대상으로 클라우드 기반 보안서비스(SECaaS) 지원
 - ※ 정보보호 컨설팅 및 보안제품 도입 지원('22년 600개社) + 랜섬웨어 대응 보안솔루션 무상지원('22년 2,000개社)+클라우드 기반 보안서비스 지원('22년 700개社)

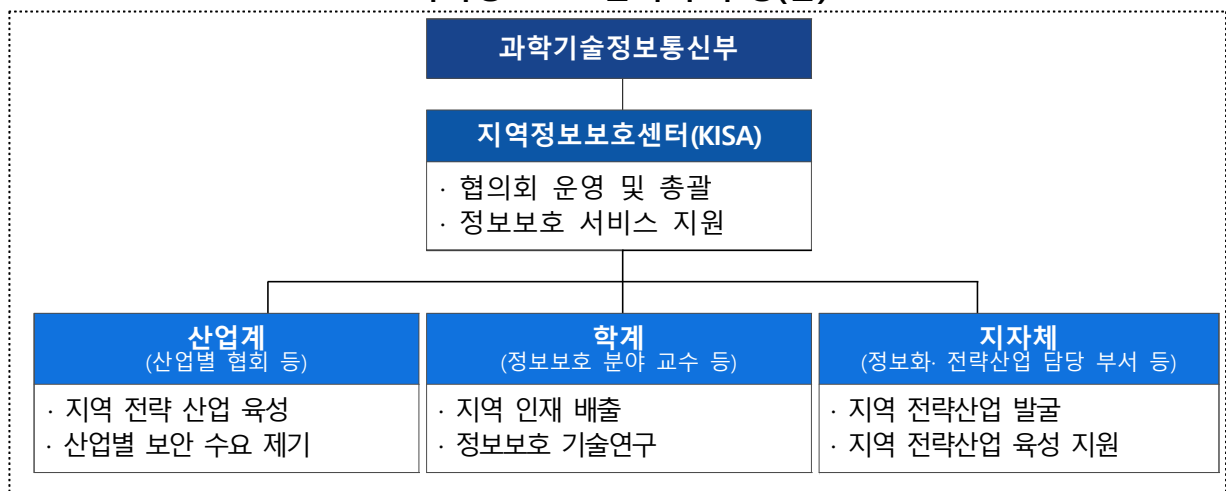
- 랜섬웨어로 인한 업무중단, 데이터 유실 예방 강화를 위해 **데이터 금고*** 구축을 통한 중요데이터 백업 지원('22년 5,000개사) 및 확대

* 중소기업의 데이터 이중화 지원을 위해 클라우드(또는 하드웨어) 기반 백업 지원



- 지역 정보보호지원센터('22년 10개소)를 중심으로 지역전략산업별로 특화된 민간 사이버보안 구심점을 확립하여 지역의 보안내재화 가속화
- 지역 산·학·연·관 정보보호 담당자로 구성된 **지역정보보호협의회***를 운영하여 지역 전략산업 맞춤형 보안내재화 기반 마련('22년~)

<지역정보보호협의회 구성(안)>



- 지역센터 교육프로그램을 통해 지역 중소기업에 랜섬웨어 등 보안 이슈를 전파하고, 지역대학과 연계한 정보보호 인재양성* 지원

* 지역대학의 정보보호 유관학과 학생들을 대상으로 특강 및 온라인 교육 제공, 지역 내 정보보호 관련 인재교류를 위한 사이버보안 경진대회(가칭) 개최 등

- 중기부(기술보호지원반) 협업을 통한 지역 정보보호지원센터 역할 확대('22년~)

※ 13개 지방중기청 기술보호지원반 + 10개 지역 정보보호지원센터 연계

※ 중소기업 침해사고 발생 시 법률 상담·자문(기술보호지원반), 웹취약점 점검(지역정보보호지원센터) 등 합동 피해구제 지원, 중소기업 대상 유사사업 공동 홍보 등

전략4. 차세대 정보보호 기술경쟁력 확보

◇ 정보보호산업 성장을 뒷받침하고, 안전한 디지털 전환을 위한 정보보호핵심원천기술 확보('21년 747억원 → '22년 928억원, 24% ↑)

① 정보보호산업 성장을 위한 정보보호 新기술 개발

- (사이버공격 대응) 사이버공격에 효과적·효율적 대응을 위해 4대 방어 체계(억제→보호→탐지→대응) 중심의 기술개발 추진('22년 416억원)

※ 美 정부는 “사이버보안 R&D 전략계획”(19.12월, 백악관 과학기술정책실)을 통해 사이버 보안 목표 실현을 위한 4대(억제·보호·탐지·대응) 방어요소 프레임워크를 제시

- (억제) 근원지 추적 등으로 공격자의 위험 부담을 증가시켜 사이버위협을 억제
- (보호) 사이버공격에 저항하여 시스템의 기밀성·무결성·가용성을 보장
- (탐지) 공격자의 의도나 행위를 탐지·예측하는 기술
- (대응) 사이버공격에 의한 파괴에 효과적으로 대응하고 복원력을 확보

- (공급망 보안) 글로벌 공급망 위협에 대응하여 SW/HW 제품 취약점을 탐지하고 무결성을 검증하는 공급망 보안 기술 개발('22년 40억원)

- (미래 인프라 보호) 글로벌 기술패권 경쟁에 대응하여 6G, 양자 등 미래 기술 도입에 대비한 보안기술*의 선제적 확보 추진('22년 119억원)

* (6G) 설계단계에서부터 필수적 보안품질을 보장하는 6G 보안내재화 기술 (양자) 양자컴퓨터의 암호 인프라 해독 위협에 대응하는 양자내성암호 기술

② 안전한 디지털 전환을 뒷받침하는 디지털 인프라 보안기술 확보

- (비대면 보안) 중요 기업 및 기반시설 보안을 개선하기 위해 제로트러스트 보안정책 도입을 위한 기반 기술 확보 추진('22년 76억원)

- (데이터 보호) 기업비밀, 개인정보 등 민감정보 유출없이 안전한 데이터 활용을 지원하기 위해 동형암호* 등 기술 개발('22년 159억원)

* 데이터가 암호화된 상태에서 연산·분석이 가능한 암호기술

- (IoT 보안) 국민의 안심할 수 있는 생활을 위해 홈네트워크 등에 인한 개인정보 노출을 방지하는 IoT 보안 위협 대응 기술 개발('22년 81억원)

⇒ 사이버보안의 10대 국가필수전략기술 선정에 따라 공급망 보안, 제로트러스트 등에 대한 “사이버보안 新기술 개발 로드맵” 수립 추진('22년 하반기)