제2차 정보보호산업 진흥계획

- 디지털 경제 전환을 정보보호산업 성장의 기회로 -

(2021 ~ 2025)

2020. 6.

관계부처 합동

목 차

Ⅰ. 추진배경

◇ 코로나19로 인한 비대면 서비스 확산으로 디지털 전환 가속화

○ 제조업 기반의 전통산업이 ICT와 만나 **디지털과 물리적 요소**를 **통합**하여 **빅블러(Big Blur) 현상***이 확대되는 **디지털 시대**로 전환

* AI・빅데이터・클라우드・IoT 등 첨단기술의 발달로 인해 산업 간 경계가 모호해지고, 오프라인과 온라인 경계가 허물어지면서 새로운 사업모델이 나타나는 현상

- 'Data・Netwok・AI' 기반 **디지털 전환**에 따라 **안전한 데이터 활용**이 중요해 지고, **ICT와 융합된 산업・서비스가 가속화**됨에 따라 **정보보호산업도** 환경변화에 따른 **기술혁신** 필요

※ 국내 데이터산업 시장규모는 약 16조 9천억원('19년)으로 최근 3년간 8.4% 성장하였고, '19년말 데이터 3법 개정에 따라 정부와 민간의 투자가 더욱 확대될 전망

○ **코로나19**로 인한 **비대면 서비스 확산**과 함께 **이용자에 대한 사이버 위협도 증가***하여 보안을 기본으로 한 **언택트**(Untact) **신산업 출현**

* 화상회의 솔루션 '줌' 보안 문제 대두, 정보시스템의 개인정보 유출 우려

※ 원격근무업체 분석에 따르면, 코로나 사태 이후 재택근무 기업 일주일만에 6배(200개→1200개) 증가, 화상회의 이용 건수 819% 증가('20.3월)

< 언택트 서비스 관련 비즈니스 모델(예시) >

원격근무	비대면 거래	원격교육
RemoteView	kakaobank	
화상회의 (실시간 쌍방향 소통)	간편 송금·결제 (카카오톡 연동)	EBS 콘텐츠로 강의 구성 (학습관리시스템)

☞ **全산업의 디지털 전환, 코로나19로 인한 비대면 서비스 확산 등 패러다임 변화는 정보보호산업을 재조명하는 위기이자 기회**

◇ 민간 **'사이버 복원력' 확보**를 위한 **정보보호산업 생태계 강화**

○ 세계 각국 정부의 **기존 PC·네트워크 중심의 사이버보안 대응 체계**로는 AI 등 신기술을 기반으로 국민 생활 및 사회 전반에서 새롭게 발생하는 **디지털안전 위협 대응에 한계** 발생

- 사이버 공격이 예측 불가능할 정도로 다양하고 복잡해지고 있어, 사전 예방보다는 사고가 발생하더라도 빠르게 회복할 수 있도록 **'사이버 복원력**(Cyber Resilience)*' **확보**가 중요

* 사이버 공격에 의한 시스템이나 서비스의 피해를 최소화하고 장애 또는 사고가 발생하기 이전 상태로 혹은 그에 준하는 상태로 신속하게 돌아가려는 역량

※ 사이버 공격으로 인한 글로벌 경제피해: ('15)3조$ → ('21)6조$('20 Cybersecurity Ventures)

○ 사이버 복원력 확보를 위해서는 정부 정책만으로는 한계가 있어 민·관 협력을 통한 정보보호 투자 확대, 신기술 확보 및 전문인력 양성, 규제 혁신을 통한 **정보보호산업 생태계 강화** 필요

- **해외도** 민·관이 협력하여 규제는 완화하면서도 책임을 강화하여 **민간기업이 스스로 정보보호에 투자**하도록 환경을 조성

※ 영국정부는 디지털 보안 내재화 계획으로 구글, MS와 약 1.9억 파운드(2,904억원)를 공동투자, 향후 5년간 사이버보안 솔루션 개발을 민·관이 함께 진행('19.8~)

☞ **디지털 안전 위협에 대한 민간 주도의 '사이버 복원력' 확보를 위해 정보보호산업 전반의 생태계 강화**

◈ 범정부 차원의 법정계획인 **제2차 「정보보호산업 진흥계획('21~'25년)」을 수립·시행**하여,

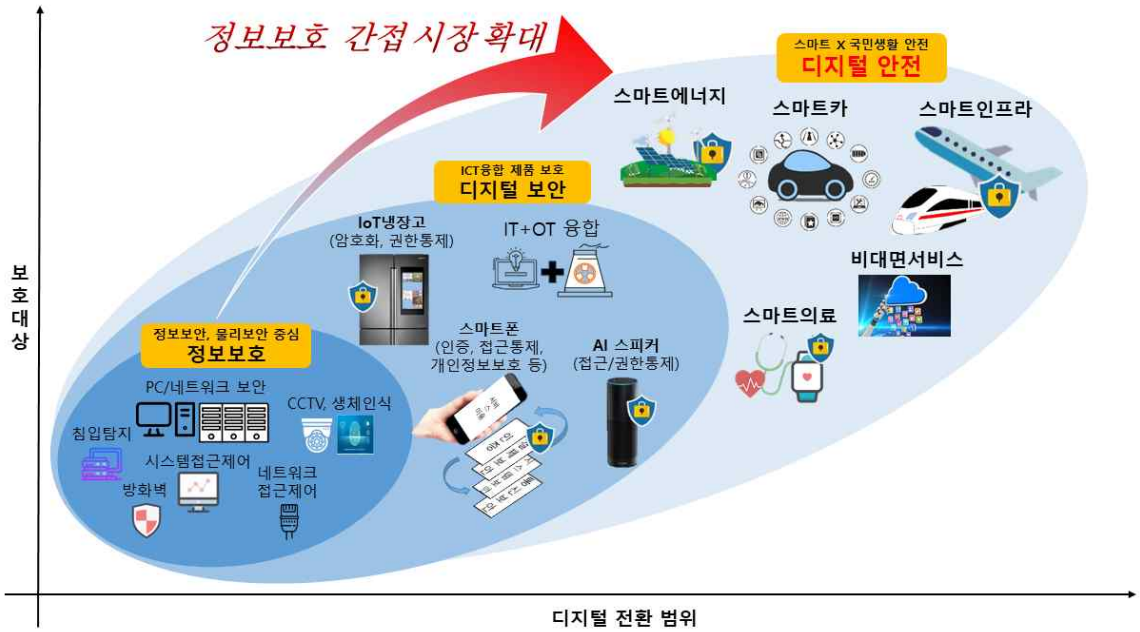
○ '디지털 전환(D·N·A) + 포스트 코로나'에 필수적인 **민간 사이버 복원력 확보**를 위한 정보보호산업 육성으로 **안전한 디지털 신뢰사회** 구현

1 정보보호산업 시장 환경변화

□ 국내 정보보호(정보보안*+물리보안**)시장은 '19년 약 **10.5조원** 규모, 이중 국내 **정보보안**시장(3.3조원)은 해외(1,212억불)의 **2.5%** 수준

* **(정보보안)** 네트워크·시스템 보안, 정보유출방지, 암호/인증, 보안관제, 컨설팅 등
** **(물리보안)** 카메라, 저장장치, 바이오인식, 알람/모니터링 및 출동보안 등

○ 정보보호는 **보안제품·서비스 중심 시장**에서 디지털 전환 확산으로 ICT와 융합된 **산업·서비스 내재화로 시장 구분 및 경계가 무의미**



기존 정보보호시장	향후 정보보호시장
▲ **(정보보안)** PC·네트워크 중심 **보안사고 예방·대응**을 위한 **보안제품·서비스**	▲ 가전, 모바일기기, 산업기계 등 유·무선 네트워크 연결에 따른 **디지털 보안** 중요
▲ **(물리보안)** 범죄·재해감시, 시설보호를 위한 **CCTV, 생체인식, 출입통제** 등 **설비**	▲ **'산업+ICT+안전'** 융합으로 **정보보호가 내재화된 간접시장** 성장 전망

□ **세계 주요국**들은 3~4년 전부터 **디지털 경제 전환 정책**을 추진해 왔으며, 코로나 19를 계기로 그 흐름이 **더욱 빨라질 것으로 전망**

※ '18년 세계 디지털경제 규모 12조 9천억달러(세계인터넷발전보고 2018)

○ 기존 정보보호시장에 머무르지 않고, 디지털 전환 확산에 따라 넓어지는 **정보보호 간접시장* 공략**을 위한 정책 필요

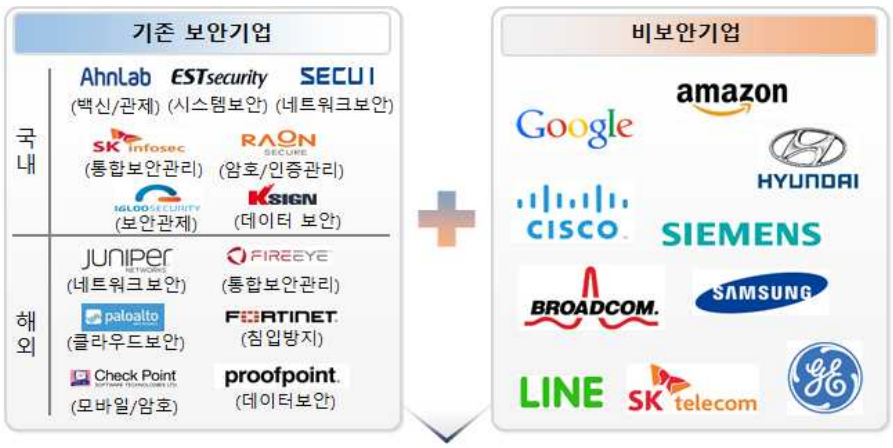
* 디지털 전환 시장에서 정보보호가 차지하는 비율은 약 **13.8~15%로 전망**

연 도	디지털전환 시장	정보보호 시장	비 율
'18년	2,900억$	401억$	**13.8%**
'23년	6,650억$	1,000억$	**15.0%**

(Markets&markets, '19.3월)

□ 국내 및 해외 **보안기업**들도 ICT, 통신, 제조업 등 **비보안기업**들과 **인수합병**(M&A)·**기술협력**·**투자** 등을 통해 시장 환경변화에 대응

< 국내·외 보안기업 변화 >



참고1 주요국 정보보호산업 관련 정책 요지

구분	주요 내용
미국 	• **안전한 5G 망 구축**을 위한 사이버보안 프로젝트에 **산업계의 지원**을 요청하여 사이버보안 분야의 **민관 협력을 주도** ☞ 제품 및 기술 지원으로 상용 및 오픈소스 제품을 통합하여 실질적이고 상호운용 가능한 솔루션 개발하여 **현실적인 사이버보안 이슈를 해결**하고 **산업을 발전을 도모**(5G Cybersecurity: Preparing a Secure Evolution to 5G, '20.5)
영국 	• **코로나-19**로 비즈니스 전반이 **디지털로 전환**됨에 따라 **사이버보안 지침**을 발표하고 **보안에 대한 새로운 개념** 및 **담당기관** 선정 ☞ 기존 공급자 중심의 사이버보안에서 **사용자 중심의 온라인 안전**(Safety Technology) **개념을 정의**, 산업 협회를 수립하여 새로운 산업을 지원 (Safer technology, safer users: The UK as a world-leader in Safety Tech, '20.5)
EU 	• 연합 내 **사이버보안 역량**을 **강화**하여 **수준 향상**의 관점의 법 개정 실시 ☞ **ENISA의 기능을 강화**하여 연합 내 사이버보안을 담당토록하고, 연합 차원의 **사이버보안 인증체계**를 **마련**하여 **고수준의 신뢰 구현** 도모 **(**사이버보안법, '19.3**)**
일본 	• **사이버보안**을 **경제사회의 활력 제고 요소**로 인식, **지속발전** 도모 ☞ 사이버보안에 대한 **경영진의 의식** 개혁, **투자 촉진**, 다양한 연결로 가치를 창출하는 **안전한 공급망** 실현 등 '20년 도쿄 올림픽 대응 태세 강화 **(**사이버보안'19, '19.5**)**
중국 	• 국가인터넷정보판공실 외 11개 부처 합동으로 **주요기반시설 내 ICT 제품 및 서비스 조달시 보안 심사를 의무화**(网络安全审查办法, '20.4)하고, **위반 시 제품 사용중지 및 벌금을 부과**하는 등 **높은 수준의 규제 마련** ☞ 사이버보안 업계를 대상으로 **사이버보안 산업 기금**(궈커자허, 중국인터넷 투자기금)을 통해 융자를 제공하고, **사이버보안 산업 단지**(우한, 베이징, 톈진, 톈커)를 **조성**하여 **산업 발전을 지원** (중국 사이버보안산업백서中国网络安全产业白皮书, '18.9)
캐나다 	• **사이버보안 강화**를 위한 주요 요소로 **정부** 및 **민간기업**, **학계**를 포함한 다양한 **이해관계자간 협업**을 **강조** ☞ ▲시스템 보안 및 복원력 ▲혁신성 및 적응력 있는 **사이버 생태계** ▲효과적 리더쉽·거버넌스·협업을 3대 목표로 설정**, 사이버보안 분야의 전략적 정책 역량 제고**(사이버보안 실행계획 '19~'24, '19.8)

2 우리의 상황

□ 제1차 산업진흥계획을 통해 지난 5년간 정보보호산업의 양적 성장을 달성하였으나, **디지털 전환과 비대면 서비스 확산**에 따른 새로운 보안 위협에 대응하는 정보보호산업의 **질적 성장**과 **체질개선** 필요

○ 그 간의 노력으로 '19년말 **국내 정보보호시장**은 **10.5조 돌파**('16년 9조, 16%↑), 정보보호 기업은 **230개 증가**('16년 864개→1,094개, 26.6%↑)

< 정보보호산업 매출액 >

< 정보보호기업 수 >

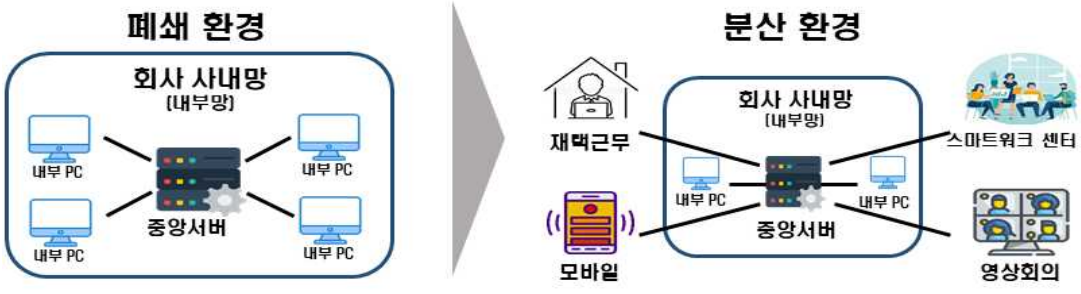
○ 디지털 전환 및 비대면 서비스 확산은 **보안점검 포인트를 증가**시켜 기존과는 다른 **분야별 특성에 따른 차별화된 보안을 요구**

- 모바일 등 다양한 방법을 통해 **원격에서 이용하는 디지털 특성** 상 이용자 인증, 네트워크·접속단말 보안 등 **보안점검 포인트가 증가**

※ 전문가가 내부망을 집중 관리하던 방식 대신 **이용자 전반의 보안이 중요**

☞ 이용자가 **쉽고 편리하게 언제, 어디서나 안전하게 서비스를 이용**할 수 있도록 **기존 정보보호의 패러다임 변화** 필요

< 디지털 환경에서의 보안점검 포인트 변화 >



※ 악성 URL 클릭 횟수 전월대비 260% 증가, 스팸 위협 220배 증가(트랜드마이크로, '20.4월)

□ **영세 중소기업**은 대기업에 비하여 상대적으로 **정보보호 역량과 전담인력 부족**으로 **보안이 현저히 취약***한 **정보보호 양극화 심화**

* 중소기업 대상 사이버공격 지속 발생('14년 2,291건 → '19년 3,638건), 침해사고로 인한 기술유출 사건의 91%가 중소기업('18년 사이버공격 통계, 경찰청)

○ 보안문제에 대해 자체 해결이 어려운 **중소기업**이 전문가 컨설팅을 통해 실질적으로 필요한 **보안서비스·플랫폼이 도입** 될 수 있도록 **초기 정부가 마중물 역할**을 통한 **중소기업의 보안역량 강화** 유도

☞ **중소기업의** 자발적인 **정보보호 역량 강화** 유도를 통해, 민간 주도의 **사이버 복원력 확대·강화 기대**

□ **글로벌 기업**들은 **보안 토털솔루션** 공급과 활발한 **인수합병**으로 기술력과 규모를 키우고 있으나, **국내 기업**들은 단품 위주 **보안 제품 공급**과 더불어 **영세한 규모***로 **시장 확대에 한계**

* 국내 정보보호 기업의 70.1%가 자본금 10억 미만의 중소 규모로, 중견 보안기업(3년 평균 1,500억원 이상 매출)은 5개사에 불과

☞ 정보보호기업 간 **기술 제휴 및** 클라우드·AI 등 **차세대 기술 개발이** 활발히 이루어 질 수 있도록 **상생 협력체계** 강화를 통한 **국내 기업의 경쟁력 강화 지원**

□ **정보보호에 대한 인식**은 기업(87%)과 개인(95%)이 **모두 높은 수준**이나, 디지털 전환 등을 고려한 **정보보호 투자는 민간*·공공** 모두 미흡**

* 정보보호 예산 편성 기업은 32.3%, 정보보호 예산이 IT예산의 5% 이상인 기업은 2.9%에 불과('19년 정보보호실태조사)

** 공공부문 정보화 예산 중 정보보호 예산 비율 : 한국 **8.4%, 미국 19.9%**

☞ 디지털 경제에서 **정보보호**는 옵션이 아닌 **필수 인프라**로 인식, 중소기업에 대한 **안전한 사이버방역망 구축**, 공공분야 **대규모 사업**에 대한 **보안내재화**로 정보보호 투자를 연결

□ 사이버 위협이 국민 안전과 디지털 경제 발전의 걸림돌로 작용할 수 있으나, **정보보호산업 생태계**는 **기술, 인력이 부족**한 실정

○ **(기술력)** AI 등 차세대 보안의 핵심 기술은 소수 **글로벌 대기업 중심**으로 편중되고 **국내보안 기업의 경쟁력은 미약**

※ 국내 AI 기술수준(81.6%)은 성장하고 있으나 미국 중심의 기술발전 속도가 빨라 상대적 격차는 확대되고 있는 추세

• 미국(100%) 대비 AI 기술수준('18년) : 유럽(90.1%), 중국(88.1%), 일본(86.4%) <IITP, '19>

- 세계적 수준의 ICT 인프라 이용환경에도 불구하고 정보보호 **기술 격차*는 여전**, 단기간 내 중국이 한국을 추월할 것으로 예상

* 미국(100%) 대비 기술수준('18년) : 유럽(94.4%), 일본(90.4%), 한국(89.7%), 중국(88.9%)<IITP, '19>

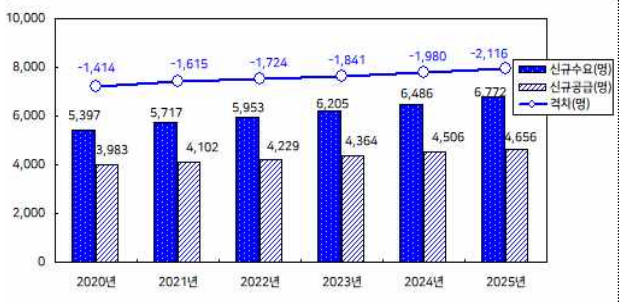
☞ 은밀화·고도화·지능화 되는 **사이버 위협에 선제적으로 대응하기 위해서는 차세대 보안기술 선점 및 기초·원천기술 개발 필요**

○ **(인력)** **ICT융합 확산, 신기술**을 활용한 **보안기술 필요성 증가**로 **인력수급차**가 **매년 상승**하고 있어 **정보보호 전문인력 지속 부족**

- **'사고 대응' 중심**의 **인력양성이 아니라**, 다양한 산업분야에 지식과 경험이 많고 **산업 현장에 즉시 활용 가능**한 **전문인력 요구**

☞ **정보보호 인력양성 전주기 관리체계 구축을 바탕으로 정보보호 잠재인력 및 산업 리더형 우수인재 양성 적극 추진 필요**

<국내 정보보호 인력 수급 전망('20~'25)>



<글로벌 정보보호 전문인력 수급 격차>

출처 : '19 정보보호 인력현황 보고서(과기정통부), Cybersecurity workforce study 2019, (ISC)²

참고2 그 간의 주요성과

□ (매출) 국내 정보보호산업 시장규모 16.2% 증가('16~'19)

< 국내 정보보호산업 매출액 >

- '19년 정보보호산업 매출액 : 10,5조원 (전년 10.1조원 대비 4.3%↑)
  - 정보보안(3.3조), 물리보안(7.2조)

☞ 국내 산업규모는 꾸준히 증가하고 있으나, 글로벌 기업과의 경쟁이 갈수록 치열

□ (규모) 국내 정보보호기업 수 26.6% 증가('16~'19)

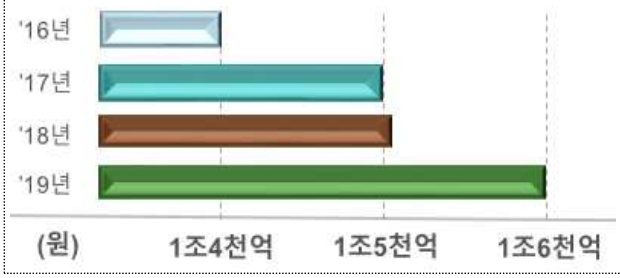
< 국내 정보보호 기업 수 >

- '19년 전체 정보보호기업 1,094개
  - 벤처기업 441개, 일반기업 653개

☞ 정보보호 스타트업 창업 및 성장 지원을 통해 양적 성장은 이루었으나, 300억 이상 기업은 37개에 불과

□ (수출) 국내 정보보호기업 수출액 14.3% 증가('16~'19)

< 국내 정보보호산업 수출액 >



- '19년 정보보호 수출액 1.6조원
  - 정보보안(1천억), 물리보안(1.5조)

☞ 제1차 진흥계획 수출 목표('20년 4.5조) 대비 부족한 성과를 만회하기 위한 보완책 필요

□ (인력) 국내 각 분야의 정보보호인력 11,451명 증가('16~'19)

< 국내 정보보호 인력 >

- '19년 정보보호 인력 135,194명
  - 공공분야 4,380명, 일반 84,539명, 보안기업 46,275명

☞ 산업계에서 필요로 하는 정보보호 전문 인력 양성 프로그램을 운영하고 있으나, 지속적으로 수급 미스매치 발생

3 나아갈 방향

□ 향후 5년은 D·N·A 기반 **디지털 전환**과 **비대면 서비스 확산**을 통한 혁신성장을 위해 **정보보호가 기본**이 되는 신뢰 기반의 **안전한 디지털 경제** 사회가 도래할 것으로 예측

○ 경쟁력 있는 정보보호기업 성장과 민간의 사이버 복원력 확보를 위해서 **정보보호산업을 차세대 핵심 산업**으로 육성할 전략 필요

< 주요 육성 전략 >

1 디지털 전환에 따른 정보보호 신시장 창출

○ **비대면 서비스** 관련 **보안시장 육성, AI 보안기술 고도화**를 위한 **데이터 활용**, 국민안전 및 ICT 기술융합에 따른 **신규보안 시장 선점**

2 민간 주도의 사이버 복원력 확보를 위한 투자 확대

○ 선진국 수준으로 **공공·민간분야 정보보호 투자 확대**, 정보보호 기업의 혁신성장을 통한 **경쟁력 있는 정보보호제품·서비스 공급**

3 지속성장 가능한 정보보호 생태계 조성

○ **차세대 핵심 보안기술** 확보, 정보보호 **규제와 법·제도 개선**, 현장에서 필요로 하는 전문인력 양성을 통해 **신규 일자리 마련**

◈ 全산업의 **디지털 전환**과 **비대면 사회 도래, D·N·A 기술 확산**

→ **신뢰(Trust) 기반의 디지털 사회**로 나아가기 위한 **산업진흥계획** 수립

Ⅱ. 비전 및 목표

비전	정보보호가 기본이 되는 신뢰 기반의 디지털 경제 확산

목표	<2019년>	<2025년>
전체매출액	10.5조원	➜ 20조원 (9.5조원, 연평균 11.3%↑)
300억이상 기업	37개	➜ 100개 (63개, 연평균 18%↑)
일자리	13.5만명	➜ 16.5만명 (3만명, 매년 6천명↑)

중점 추진 과제		
	디지털 전환에 따른 정보보호 신시장 창출	① 비대면 서비스 관련 보안시장 활성화
		② 정보보호 데이터 활용기반 조성
		③ AI기반 물리보안 산업 육성
		④ 5G⁺ ICT 융합보안 산업 저변확대
	민간 주도 사이버 복원력 확보를 위한 투자 확대	⑤ 공공·민간 분야 정보보호 투자 확대
		⑥ 중소 정보보호기업 성장지원
		⑦ 정보보호 해외진출 및 국제협력 강화
	지속성장 가능한 정보보호 생태계 조성	⑧ 차세대 보안 新기술 확보
		⑨ 정보보호산업 규제 및 법·제도 개선
		⑩ 정보보호 전문인력 양성

Ⅲ. 중점 추진과제

1. 디지털 전환에 따른 정보보호 신시장 창출

1-1 비대면 서비스 관련 보안시장 활성화

비대면 서비스 관련 **보안 新시장 창출 및 안전성 확보**

< 국내 클라우드 보안서비스 매출액 목표치>

□ 현황 및 문제점

o 코로나19 확산에 따라 경제 사회 전반에서 대면 접촉을 최소화하기 위해 **클라우드 기반 디지털 언택트**(Untact) 환경으로 전환

※ 재택근무, 온라인교육, 온라인 유통 등 디지털 기반의 비대면 산업 급부상

o 세계 **클라우드 보안 시장**은 기술력과 규모의 경제를 앞세운 **글로벌 기업의 선점**으로, 후발 주자인 **국내 기업의 경쟁력 확보에 애로**

※ 클라우드 기반 보안서비스 기술 격차 : 미국 대비 88.5%(약 1.1년)

o 국내 클라우드 보안 산업 육성을 위해 **공공부문의 우선 주도를 통해 경쟁력을 강화**하고 **민간 확산을 통한 시장 활성화** 필요

□ 추진 전략

o **안전한 비대면 환경 조성**을 위한 **시범사업 및 공공 선도**
o 비대면 **성장기반 마련**을 위한 **수요기업 지원**으로 이용 활성화
o **비대면 솔루션, 보안 공급기업** 지원을 통한 **경쟁력 확보**

□ 추진과제

◇ 비대면 서비스 보안 시범사업 및 공공분야 선도적 도입

○ **(보안내재화 시범사업)** 클라우드, 블록체인, 생체인식 등 신기술을 활용하여 차별화된 보안기능을 갖춘 **비대면 서비스 시범 적용**

* 무인점포의 경우 현장에 생체인식, 출동보안 등 기술을 적용해서 사업종료 후에도 실 서비스화 될 수 있도록 유도

< 비대면 서비스별 보안기능 예시 >

구분	원격교육	원격근무	상거래
특징	학생·교사 등이 **쉽게 적용** 가능	언제·어디서나 **동일한 보안수준**	**편리한 인증**기술
보안기능	토탈보안 솔루션 (한번 설치로 간편 이용)	클라우드 보안서비스	무인점포(**생체인식**+결제+출동보안 등)

- 보안 민감 분야에서 클라우드 도입 시 보안우려를 해소하기 위해 **클라우드 도입과 보안성 검증**을 **패키지***로 지원

* 클라우드 기반의 개인정보 관리시스템, 문서유출 방지가 가능한 클라우드 기반 콜센터 재택·원격근무시스템 등

○ **(신속 보안인증)** 공공분야 비대면 서비스 확산에 필요한 **클라우드 우선 도입**을 위해 **보안인증 신속처리*** 지원 및 **인증범위 확대**('21~)

* 클라우드 보안 인증에 필요한 소요기간 단축(3.3개월 → 2.5개월)

- 국가·공공기관에 개방형 OS 기반의 서비스형 데스크톱(DaaS)*이 원활하게 도입될 수 있도록 보안인증 기준 마련

* (Desktop as a Service) 개별 PC마다 윈도 등의 OS를 설치하여 작업 환경을 구축하는 대신, 접속단말을 통해 원격으로 작업 환경을 이용하는 클라우드 플랫폼

○ **(공공수요 창출) 보안성**을 **확보**한 **IoT 제품**(IP카메라, 공유기 등)이 **도입**되도록 **컨설팅·인증 등 지원***하여 보안강화 제품의 보급 확대

* 공공기관용 IP카메라 보안성능 인증(TTA), IoT 보안인증(KISA) 등

◇ (수요 확대) 중소기업의 비대면 서비스 보안 도입 확산 지원

○ 보안 지식이 부족한 영세·중소기업도 **쉽고 안전하게 비대면 서비스를 이용**할 수 있도록 **'클라우드 보안 서비스'** 비용 지원

- 정보보호에 **관심과 투자의향을 가진 기업**의 보안역량 강화를 위해 **종합컨설팅** 및 **보안솔루션 추가도입** 등 투자 지원

< 중소기업 맞춤형 정보보호 지원방안 >

구분	영세·중소기업	정보보호 관심·투자기업
대상 기업	351만개(PC 보유기업) **→ 9,000개 선정**	31만개(정보화 전담부서 보유) **→ 1,000개 선정**
지원 내용	보안 수준이 낮은 중소기업에 클라우드 보안 서비스 제공	종합컨설팅 결과를 기반으로 보안 고도화 지원
	원격 보안점검, 백신 및 웹·이메일 보안 등 필수 서비스 위주	APT*, UTM** 장비 등 보안제품 또는 데이터 변조방지 등 클라우드 보안 서비스

* Advanced Persistent Threat(지능형지속공격) ** Unified Threat Management(통합위협관리)

◇ (공급 지원) 비대면 솔루션 & 정보보호 공급기업 지원

○ **(개발&고도화 지원)** 정보보호제품의 **클라우드 전환**을 유도하는 시범사업 추진 및 기능 고도화를 위한 보안수준 컨설팅 추진('21~)

- 유망한 클라우드 보안서비스* 중심으로 **서비스 전환 및 개발 지원**

* ID관리/접근제어, 이메일 보안, 웹방화벽 등 우리가 경쟁력 있는 클라우드 보안 서비스를 중심으로 서비스 전환 및 개발 지원

- 보안기업의 비대면 보안서비스 제공 내용·기간에 따른 적정한 대가를 받을 수 있는 **구독형 서비스**(월 사용료 지급)로 전환 유도

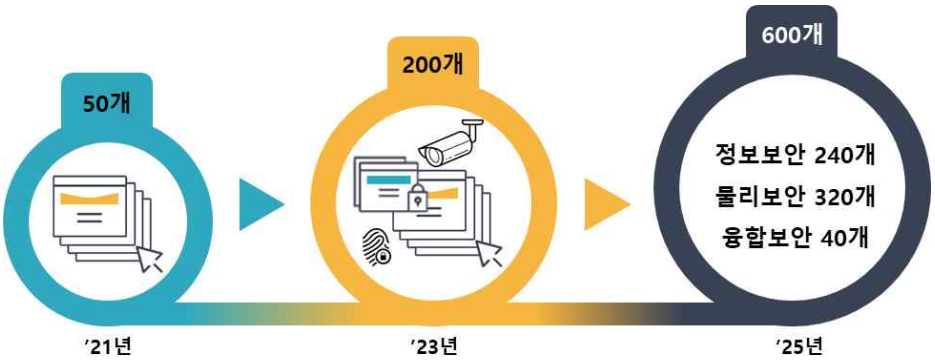
※ 정부·공공기관에서 예산계획 수립 및 편성, 집행 시 기존 보안제품 구입 및 유지보수 개념이 아닌 서비스 이용에 따른 대가지급 방식으로 변경 추진

○ **(보안 점검 지원)** 국민들의 사용 빈도가 높은 중소 SW개발업체 비대면 서비스*에 대한 **보안취약점 점검, 안전성 진단**('21~)

* 재택·원격근무 및 교육솔루션(156개 개발사 184개 솔루션, 한국SW산업협회)

1-2 정보보호 데이터 활용기반 조성

정보보호 데이터 활용을 통한 AI 기반 보안기술 확산



<정보보호 학습데이터 활용 기업 목표치>

□ 현황 및 문제점

o 글로벌 IT기업들은 **정보보호 빅데이터 축적**을 통해 AI기반의 **지능형 차세대 보안 기술개발**에 적극적인 투자 진행

※ **(구글)** AI를 활용해 일 1억개 이상의 스팸메일을 추가로 차단, **(IBM)** 사이버범죄를 원천봉쇄할 수 있는 보안위협 지능형 플랫폼 개발, **(아마존)** 머신러닝으로 자사 클라우드 계정을 완전히 보호하는 기술 개발

o 반면, **국내 AI 기술** 수준은 미국대비 78% 수준으로 미흡하고, 해킹·비정상 데이터 학습 등 **사이버 위협에 대한 대비도 부족**

※ 국내 데이터 시장은 수요, 공급이 모두 부족한 상황으로 거래량이 미국의 1/400 수준이며, 데이터 기술력은 미국(100)대비 79%, AI 기술력은 78% 수준으로 평가

o **데이터3법 개정**으로 AI와 데이터를 활용한 **보안산업 활성화**를 위해 정부차원의 **AI보안 기술·학습데이터 지원** 필요

□ 추진 전략

o 정보보호 관련 원천데이터를 AI보안 학습용으로 가공·지원하여 **'정보보호+AI'**에 활용할 수 있는 **데이터 지원체계 구축**

※ AI·데이터 바우처 사업을 통해 수집한 데이터를 최대한 활용

o AI 기반 보안제품 신규개발, 기존 제품의 AI 적용 및 테스트베드 환경 지원 등 **AI를 적용한 보안제품 개발** 활성화 유도

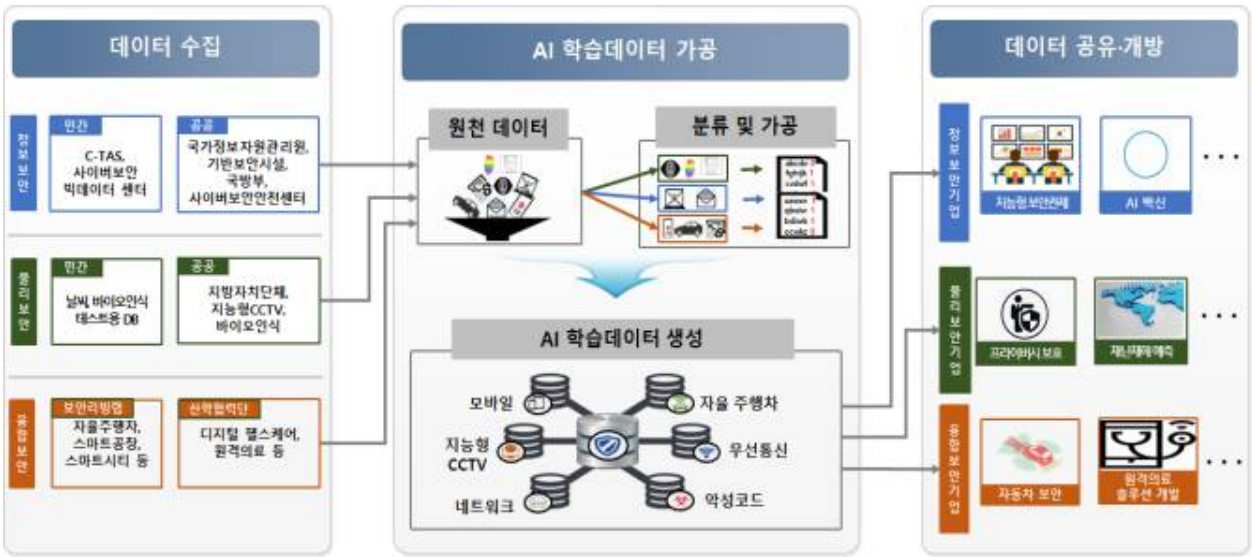
□ 추진과제

◇ AI 기반 보안제품 확산을 위한 학습데이터 가공·공유 체계 구축

○ **정보보호기업을 비롯한 산·학·연**의 AI 기반 정보보호 기술 및 제품·서비스 개발 지원을 위한 **학습데이터 가공·공유 체계 구축**('21~)

- 여러 곳에 분산되어 제공 중인 정보보호 원천 데이터를 종합적으로 수집·가공, **AI 학습데이터 공유**를 위한 이용 기반 강화

< AI보안 학습데이터 가공·공유 체계안 >



- 정보보호제품의 품질 향상을 위해 데이터의 규모, 다양성 등을 확대하여 **양질의 AI 보안 학습데이터를 단계적** 제공

구분	원천데이터 수집 확대
정보보안	KISA(6.9억건) 뿐 아니라 국가정보자원관리원, 기반시설 등 공공의 데이터를 추가로 수집·가공하여 학습데이터 정확도 제고 ※ 수집처 : (기존) C-TAS, 사이버보안빅데이터센터 → (확대) 국가정보자원관리원 등 공공기관
물리보안	업계가 확보하기 어려운 생체인식, 재난·재해 데이터를 가상데이터 생성 기술로 제작하여 학습데이터 규모 및 다양성 확대
융합보안	병원 등 산학협력단, 스마트시티, 스마트공장 등의 보안 리빙랩을 통해 OT(제어운영기술) 영역의 취약점 등을 수집·가공하여 학습데이터 확보

- **민간 클라우드 서비스 등**을 통해 **AI 보안 학습데이터를 개방**하여 시·공간 제약 없이 제품 개발이 이루어질 수 있도록 기업 지원

◇ 정보보호기업의 AI 학습데이터 이용 지원

○ 정보보호기업의 영상, 생체인식 등 데이터 기반 **지능형 보안제품·서비스 개발**을 위해 **학습 데이터 구매 및 가공 집중 지원**('22~)

※ 데이터 구매, 일반 가공, AI 가공 등을 데이터바우처 사업과 연계하여 지원

< 보안산업 데이터 사례 >

구분	주요 내용
물리보안	CCTV 영상, 바이오 이미지(지문, 얼굴, 홍채, 음성 등), 재난 재해 환경 영상(홍수, 산불, 산사태, 테러 등) 등
정보보안	악성코드 및 악성앱 데이터, 스팸 데이터, 보안관제 네트워크 데이터 등
융합보안	자율주행차, 스마트 공장 등 융합보안 선도 분야의 보안 관련 데이터

○ AI 보안 학습데이터의 안전한 활용을 위한 **비식별 처리**(기업정보, 피해자 정보 제거 등) **및 비식별 처리기술 개발*** 지원('22~)

* 데이터, 영상정보 등에 개인정보를 비식별처리, 영상합성 등

○ AI 보안 성능을 검증할 수 있는 **AI 보안 테스트 지원***을 통해 AI 보안 머신 학습의 정확도 개선과 제품 고도화('22~)

* AI 기반 보안제품 신규개발 또는 기존 제품에 AI 기능 적용을 위해 필요한 샘플 데이터셋 제공 및 AI 보안 성능개선 컨설팅

- 정보보호 AI 제품 신규개발 또는 기존 제품에 AI 기능 적용을 위해 필요한 샘플 데이터셋 제공 및 AI 보안 성능개선 컨설팅

○ AI보안 데이터를 활용하여 산·학·연 전문가가 기술개발·성능을 경쟁하는 **AI 보안 기술개발 챌린지 대회** 개최('22~)

- 개방형 문제해결 플랫폼인 **(가칭) 한국형 캐글**(Kaggle)*로 단계적인 확대 개편을 통해 **데이터 이용역량 강화 및 제품 개발 촉진**

* 기업이 해결하려는 문제에 데이터와 상금을 걸면, 전문가들이 해결책을 찾는 방식

※ AWS, 페이스북, 마이크로소프트가 캐글을 통해 총 상금 100만달러 상당의 '딥페이크 식별 알고리즘 개발 챌린지'를 개최하여 13개국 1,000개 이상의 팀이 참여('20.1)

1-3 AI 기반 물리보안 산업 육성

국민 삶의 질 제고를 위한 **물리보안 산업 육성** 및 **응용 확대**

□ 현황 및 문제점

o 급증하는 범죄, 테러, 재난·재해 **수요 증가** 및 **물리보안 의무화 인식** 제고에 따른 **수요**는 **꾸준히 증가**할 것으로 전망

※ 글로벌 물리보안 시장 규모는 840억 달러('18) → 1,190억 달러('23)로 연평균 7.3% 지속성장 예측(Markets and Markets, '19.1월)

o **국내 물리보안 시장 규모**는 7조원('18)→7.2조원('19)으로 연 3.5% **저성장 추세**이며, 외국기업의 **저가 공세**로 **성장 둔화**

※ 글로벌 CCTV 시장에서 중국 기업은 1, 2위를 차지하며 연평균 20%대 성장

o 국내 물리보안 기술 수준은 **주요국 대비 낮게 평가**(91.8%)되어, **기술 경쟁력 강화**를 통한 **신흥시장 개척** 필요

※ 기술수준: 미국(100%) > 유럽(96.9%) > 일본(94.4%) > 중국(92.0%) > 한국(91.8%)

□ 추진 전략

o 물리보안 산업 육성을 위한 **선도적 기술 개발** 및 **산업 기반 강화**

o **안전사회 구현**을 위한 **경쟁력**을 **갖춘** 물리보안 **제품·서비스 활용**

□ 추진과제

◇ 물리보안 선도적 기술 개발

○ ICT 환경 고도화에 따라 지능형 CCTV의 **무선화·이동성** 등 **활용성을 높이고,** 생체인식의 **원거리** 등 **정밀식별** 가능한 **선도 기술 개발**('22~)

* 기술개발 결과를 물리보안 기업에 기술이전하여 사업화할 수 있도록 지원

- **(Edge 기술)** 드론·차량 등 5G 모빌리티 연계 환경에서 **Edge 기반**(단말)으로 **실시간 객체식별** 및 **이상행위 분석·전송 기술 개발**

※ (객체) 사람, 동물, 식물, 사물 등 / (이상행위) 테러, 화재, 산불, 쓰러짐, 침입 등

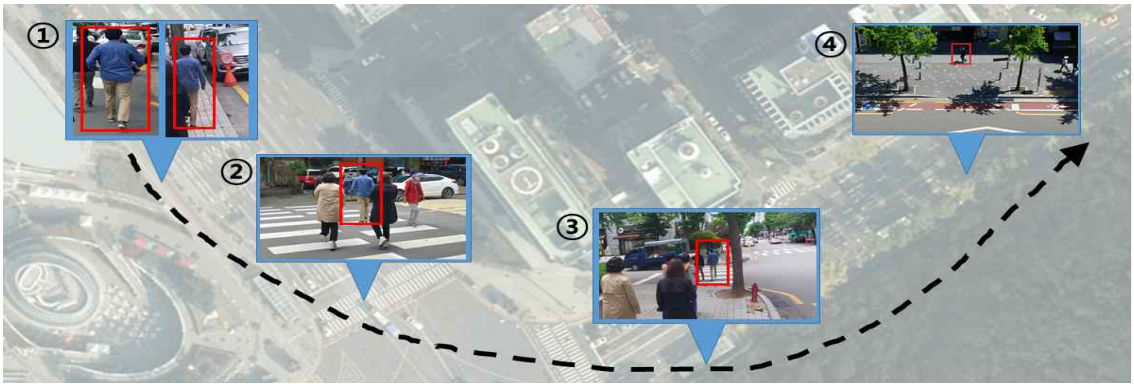
- **(이기종 센서간 객체인식 기술)** 야간(저조도), 원거리 등 **악조건 환경**의 이기종(열화성, 가시광) 센서간 지능형 **객체 인식기술 개발**

※ 열화상 기능으로 형태, 행동 탐지→가시광선으로 객체 정밀 인식(얼굴, 차량번호판 등)

< 열화상 + 가시광선 분석기술 활용 >

- **(다중카메라 객체 추적 기술)** 다수의 이기종 CCTV 영상(드론, 고정형 CCTV)간 사람, 사물 등 **이동객체 식별·추적 기술 개발**

< 다중 영상 카메라간 이동객체 추적 개념도 >



※ 객체 식별(옷색상, 얼굴 등)을 통한 CCTV, 드론 등과 연계로 이동 현황 파악 및 추적 가능

○ **(통합플랫폼 개발 및 확산)** CCTV 영상, 생체인식 정보, IoT 센서 정보를 **클라우드, AI 기술 기반**으로 **통합 분석**하여 **이상상황 관제, 경비출동** 등을 제공하는 **"물리보안 통합 플랫폼" 개발 및 확산**('22~)

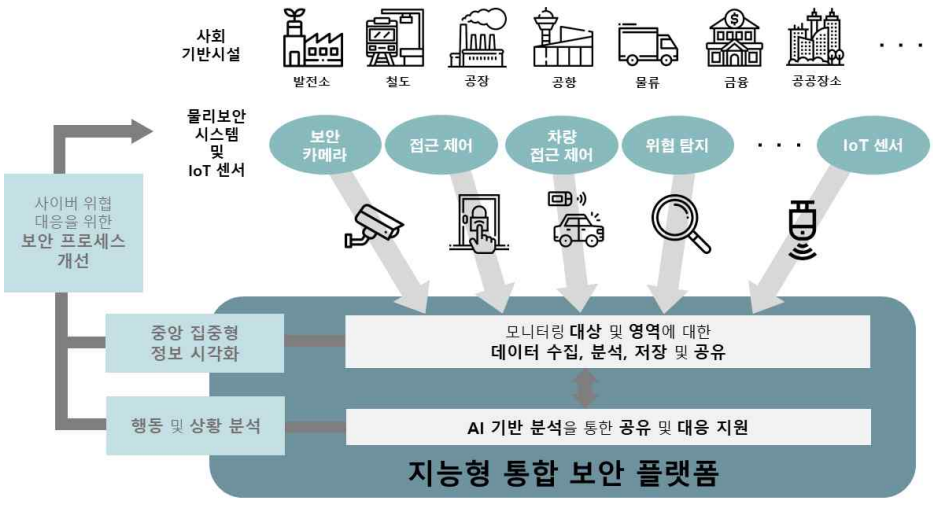
- AI, 클라우드 기반으로 표준 및 상호연동 데이터 **통합·분석·대응조치** 등 물리보안 통합서비스를 제공하는 **통합플랫폼 개발*** 및 보급**

* 데이터 표준화(전송프로토콜, 포맷 등), 이기종 제품간(예: 지능형 CCTV↔화재감지 센서, 생체인식↔출입통제 기기 등) 상호연동 및 관리 기능 구축

** 스마트 시티, 지자체 공모 등을 통해 시범사업 실증

- 건물·시설, 스마트팩토리, 농·어촌, 무인점포 등의 원격 안전관리, 마케팅 등의 **신규 영역으로 통합 플랫폼 확산**

< 물리보안 통합플랫폼 예시 >



◇ 물리보안 산업 기반 강화

○ **(인증 확대)** 5G 기반 **이동성 보장, 비접촉 인식기술** 등 시장**요구**에 맞춰 **성능인증 대상 확대**로 품질이 우수한 제품의 확산 지원('21~)

- **(CCTV 인증) 5G 기반 지능형 CCTV 장비**로 성능인증 대상 확대

※ 모바일 CCTV, 엣지 CCTV, 열화상 기반 CCTV, 다중 카메라 이동 객체 추적 기술 등에 대한 성능인증 추진

- **(생체인식 인증) 신체·행동적 특성***에 따른 **비접촉 방식** 성능인증

* (신체적 특성) 지문, 얼굴 등 / (행동적 특성) 음성, 걸음걸이 등

※ 코로나19 확산으로 지문, 홍채인식 등 접촉 방식보다 비접촉 인식 기술을 요구

○ **(실증단지 구축)** 물리보안을 **실제처럼 시험**할 수 있는 **실증단지 구축**('22~)

- 지자체 등 공모를 통해 실증단지를 선정하고, 공공, 소매, 가정, 교통, 금융 등의 분야별 물리보안 **혁신기술 제품·서비스* 도입·시험**

* 다중 CCTV 객체 추적, 드론 이상행위 탐지, 열화상 객체 탐지, 비대면 무인점포 운영 등

< 실증단지에서 물리보안 제품·서비스 운영 예시 >

○ **(경진대회 개최)** 물리보안 관련 기술개발, 품질제고, 신규 아이디어 공모 및 기술사업화 등을 위한 **물리보안 경진대회 개최**('22~)

◇ 물리보안 응용 서비스 확산

○ **(응용 서비스 확대)** AI, 클라우드 통합플랫폼 기반의 **보안서비스***를 공공, 소매, 가정, 금융, 건물관리 등 **영역별 응용 확대**('22~)

* CCTV영상, 생체인식 정보, IoT 센서 정보 등을 클라우드, AI 기술 기반으로 통합 분석하여 이상상황 관제, 경비 출동 핀테크 등을 제공하는 서비스

- **(생체인식 활용)** 생체인식 신기술 서비스 확대를 위해 **생체인증이 추가된 Multi-Factor 스마트통장, 스마트카드 시범사업 추진**

※ 기존 PIN 번호에 지문, 정맥 등 생체인식 정보가 추가된 스마트통장 및 스마트카드 기반의 서비스 개발, 기업이 제품개발 시 활용할 수 있도록 시범사업 결과 공유

- **(CCTV 사업화 지원)** 학교폭력, 미아찾기, 돌봄 서비스(아동, 노인) 등 **사회문제 해결 분야**에 지능형 CCTV **사업화 지원 확대**

※ 실시간 위급상황을 응급 의료·시설 등과 연계하여 사회 안전망 강화

○ **(무인서비스 기술고도화)** 유통, 금융분야 **무인화 서비스 확산**을 위해 범죄 예방, 안전 보장을 위한 **물리보안 서비스 결합**('22~)

- 무인화 서비스에 대한 정보보호 취약성 분석 및 보호 기술 검증을 통해 **안전성과 신뢰성이 확보된 서비스 개발**을 지원

※ 예) Just Walkout형 생체인식 스피드(아마존GO), 동선 추적형 머신비전 솔루션(알리바바 티몰)

<무인화 서비스 모니터링 보안 – 미래형 무인점포 사례>

1-4 5G+ ICT 융합보안 산업 저변확대

ICT 융합보안 강화를 위한 신규 보안서비스 시장 선점

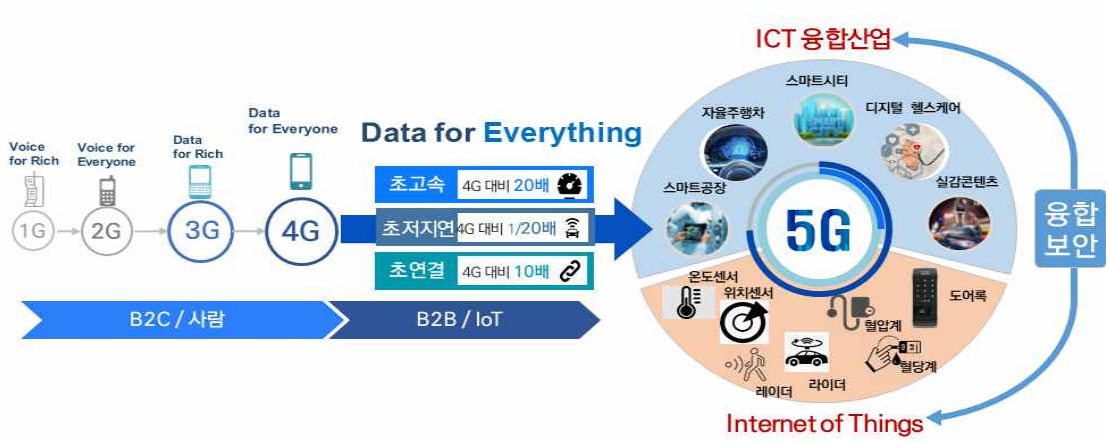
□ 현황 및 문제점

o ICT **융합산업 확산**에 따른 ICT와 제조·운영기기의 결합으로 기존 사이버보안 위협이 다양한 **전 산업의 안전 위협**으로 전이

o 5G 상용화로 ICT융합 서비스·기기가 확산됨에 따라 해킹사고 발생 시 **국민의 생명·안전 및 경제전반에 직접적 피해** 초래

※ 스마트시티, 헬스케어, 스마트공장, 자율주행차 등 융합서비스 분야별 세계 시장 확산 및 산업 중요도는 날로 증가

【 5G 상용화로 사물인터넷(IoT)·ICT 융합산업 가속화 】



□ 추진 전략

o ICT **융합산업 보안모델 개발** 및 **실증**을 통한 **보안 안정성 확보**

o **산업계 맞춤형 지원**을 통한 ICT 융합산업 **보안시장 창출**

o 융합보안 강화를 위한 **제도 정비**

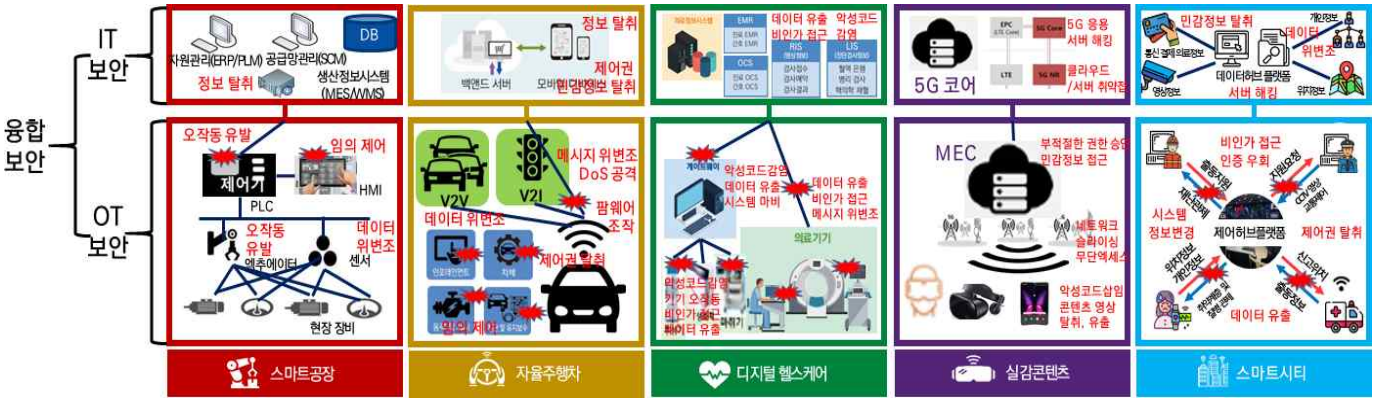
□ 추진과제

◇ ICT 융합산업 보안 강화

○ 5G 상용화로 초연결이 가속화되는 ICT 융합환경에서 보안위협에 선제적 대응으로 **안전하고 경쟁력 있는 5G 융합서비스** 환경조성('21~)

1차 산업진흥계획('16~'20) 성과		2차 산업진흥계획('21~) 방향
· ICT 융합산업별 **보안가이드**(7종) 발간·배포 및 IoT 인증제도 시행 · IoT기기, ICT 융합제품에 대해 공개된 보안위협 조치를 하는 대응 위주의 **초기 기반 조성**	⇒	· ICT 융합산업 **현장 실증**을 통한 보안모델 구축·확산 및 제도개선 병행 · **IT이용기업, 이용자로 확대**하여 ICT 융합산업 분야에 대한 보안사고 예방·대응·복구까지 **종합대응체계로 전환**

< 융합보안 개념도 >



○ **(보안모델 개발·실증) ICT 융합산업*** 서비스별 보안위협 진단을 통해 개선방안을 마련, **분야별 보안모델 개발**(융합산업분야 확대, '21~)

* '5G+ 전략(관계부처 합동 19.4월)'에서 선정한 5대 핵심서비스 분야(스마트공장, 자율주행차, 스마트시티. 디지털헬스케어, 실감콘텐츠)를 대상으로 추진

- **보안모델의 현장 적용**('21)을 통해 **미비점을 사전에 검토**하고, **우수 적용사례를 발굴**하여 산업계로 확산('22년~)

< ICT 융합산업 보안모델 개발·실증·확산 방향 >

보안모델 적용·검증 ('21)				보안모델 보완·확산 ('22~)
융합산업 핵심기기	**보안리빙랩 운영·고도화** 핵심 기기에 대한 신규 취약점 점검 도구 및 공간 제공	▶	**보안성 시험** 민간 참여형 보안시험을 통해 기기 보안위협 탐지·대응	
융합산업 서비스·플랫폼	**취약점 점검** 모의 침투, 취약점 점검 등을 통해 신규 보안위협 도출	▶	**컨설팅 지원** 융합보안 적용환경에 따라 특화된 보안 대응방안 지원	

- 기존 IT환경과 다른 융합서비스 기기·플랫폼의 **보안성을 테스트·검증** 할 수 있는 **환경*** **구축**

* 융합산업 관계부처, 유관기관과 협력하는 **융합산업 현장에 운영**하고 핵심기기 보안성 시험 도구와 절차를 제공(보안리빙랩)

< 보안리빙랩 구축(예) >

○ **(협력체계 구축)** 5G+ 핵심서비스별 **소관부처, 유관기관·단체 및 민간분야 전문가** 등이 참여하는 **민관협의체 구성·운영**('21~)

- 부처별 협력을 통한 핵심 서비스별 **보안강화** 및 **제도화*** 지원

* 개별법에 따른 시험·인증에 보안기준 반영을 위한 연구·실증사업 수행 시 지원

- 분야 간 협력을 통한 **융합보안 확산 및 시장·기술정보 공유**

< 민관합동 융합보안 협력체계 구축 방안(예) >

◇ 융합보안 강화를 위한 제도 정비

○ 융합서비스·제품의 보안위협에 대응하기 위한 **침해사고 예방·대응, 협력기반 조성, 보안강화**를 위해 **개별법령의 제도 정비** 추진

※ 5G, IoT 전반의 보안 강화를 위한 정보통신망법 개정안 공포('20.6월)

- 산업분야별 **보안 내재화**를 위해 **소관부처와 협력**하여 융합보안 강화를 위한 추진과제 발굴·시행

< 주요 제도 정비 추진과제 >

산업분야	추진과제	소관부처(기관)
홈네트워크	건설 설계기준(시방서)에 보안 기준 추가	과기정통부
스마트공장	스마트공장 수준확인제도 운영	중기부, 스마트제조혁신추진단
자율주행차	자율차 사이버보안 가이드라인(기술권고안) 개발 및 보안규정 제도화	국토부, 한국교통안전공단 자동차안전연구원
디지털헬스케어	의료기기 사이버보안 검증 방안 마련	식약처
드론	드론 기기 보안 인증제 도입	국토부, 항공안전기술원

◇ 융합보안 산업 신시장 창출

○ **(융합보안 B2B 네트워킹)** 융합보안 수요기업·기관과 보안업계간 정보교환, 수요 창출을 위한 **'융합보안 Tech-Day'** 개최('21~)

※ 융합산업계의 낮은 보안인식, 융합산업 보안 전문가 부재, 정부부처 소관 등의 이슈 해결을 위해 기업·기관 보안기술 현황 조사 및 매칭지원

○ **(보안강화 지원)** 사회적으로 파급력이 큰 공공분야를 중심으로 **보안기술 적용***, **융합산업 보안 컨설팅 바우처** 지원 검토

* 융합보안 기업의 레퍼런스 확보, 시장진출 지원을 위해 자율주행버스(세종), 스마트시티(부산), 디지털헬스케어(강원) 등 공공분야 적용 지원

○ **(융합보안 버그바운티)** 안전한 융합보안 제품의 확산과 보안성 강화를 위한 **융합보안 취약점 찾기 대회** 운영('21~)

- 민간 보안전문가의 집단지성을 활용하는 융합보안 보안취약점 **신고·포상제를 도입**하여 안전성 제고 및 관심 유도

◇ ICT 융합보안을 위한 사물인터넷(IoT) 보안인증 제도 개선

○ **IoT 보안인증** 제도에 대한 의무화 등 국제시장 변화(美 캘리포니아법(SB-327) 등)에 따라 **글로벌을 선도하는 인증체계로 개선**('21~)

- 융합 가속화에 따른 다양한 **산업분야**(의료, 스마트홈, 드론 등) **별로 인증기준**을 **마련**하여 산업 분야별 지원 확대

- IoT 보안인증제도의 **법적 근거**를 **마련**하고, 해외동향, 인증제도를 분석하여 인증 제품 공공분야 우선 도입 등 **활성화 방안 마련**

※ 산학연 전문가로 구성한 연구반을 운영하여 논의사항 반영

○ IoT 보안 인증의 **국제표준화**를 통한 국내 기업의 해외진출 지원('24~)

- 국제전기통신연합기구(ITU-T)를 통해 우리 IoT 보안인증 기준(X.iotsec-4)의 **국제표준화**(~'21) 및 **국가 간 상호인정 추진**(~'24)

※ (1단계) 국제표준화 → (2단계) 양국간 상호인정 → (3단계) 다국간 상호인정

◇ 안전한 ICT 융합보안 솔루션 개발 · 공급 지원

○ **(취약점 점검·보완)** 영세 ICT 중소기업을 위해 **소스코드 보안약점 점검도구**와 보안 취약점 점검 테스트베드 사용 지원

○ **(개발환경 점검) 중소 SW 개발·공급업체***를 대상으로 소스코드 백업시스템, 서버계정 관리 등 **개발환경 보안점검 및 컨설팅 지원**

* 원격근무, 재택근무 등 비대면 솔루션 및 민간에서 많이 사용하는 상용 정보보호 제품을 생산하는 사업자를 중심으로 실시

○ **(개발보안* 지원)** 설계-구현-테스트 등 단계별 SW 개발에서 지켜야 할 보안기능·안전한 구현 등의 **'개발보안 가이드라인' 제작·배포**('22~)

* 소프트웨어 개발 과정에서의 개발자 실수, 논리적 오류, 보안요소를 고려하지 않아 발생하는 보안 취약점을 최소화하기 위한 보안설계, 보안코딩, 보안테스트

2. 민간 주도 사이버 복원력 확보를 위한 투자 확대

2-1 공공 및 민간 분야 정보보호 투자 확대

선진국 수준으로 **공공·민간**분야 **정보보호 투자 확대**

□ 현황 및 문제점

o 글로벌 보안시장은 **미국(약 30% 비중)이 주도**하고 있으며, **정부의 대규모 수요**와 보안사고 시 징벌적 과징금 등이 **주요 투자 동인**

※ 美 정부는 보안시장의 약 60% 수준의 예산 집행 中('19, 워싱턴 포스트)

- **공공부문**의 정보화 예산 대비 정보보호 투자비율을 **선진국 수준**(美 19.9%)인 **20% 수준**까지 **확대하도록** 유인할 필요

o 중소기업의 정보보호 인프라가 열악해 **중소기업이 해킹의 주요 대상 혹은 악성코드 유포·경유지**로 악용

※ 중소기업 대상 사이버공격 지속 발생('14년 2,291건→'19년 3,638건), 침해사고로 인한 기술유출 사건의 91%가 중소기업('18년 사이버공격 통계, 경찰청)

□ 추진 전략

o 공공 정보보호 수요 확보를 위한 **국가주요시설의 보안내재화**

o **사이버 방역체계 구축**을 통한 정보보호 투자 확대 유도

□ 추진과제

◇ 공공부문 정보보호 투자 확대 기반 조성

○ **(사회)** 대규모 국가 투자사업(항만, 도로, 산업단지 등) 프로젝트에 **보안 내재화**(Security by Design)를 통해 정보보호 투자 활성화 촉진('23~)

- '사회기반시설사업' 및 '지역개발사업' 추진 시, 기존 정보화계획 수립 외에 **정보보호계획도 반영**할 수 있도록 의무화 확대 추진

※ (현행법) '사회기반시설사업' 및 '지역개발사업'은 국가정보화계획 수립·반영 中 → ('23~) 국가정보화 기본법 內 정보보호계획 수립·반영 조항 신설(안) 마련

○ **(공공분야 5G망 구축)** 유선 네트워크 기반의 행정업무 환경을 **5G 모바일 환경**으로 전환하기 위한 **시범사업의 보안성 실증** 추진

- 5G 기반 정부업무망 이용에 필수적인 **안전한 이용환경 조성**을 **정보보호 투자로 연계, '5G장비+단말+보안' 패키지化**로 **해외 진출**을 위한 레퍼런스 제공

○ **(양자암호통신) 국가 주요 통신망**에 **보안성**이 뛰어난 **양자암호통신망을 시범 적용**하여 차세대 기술 및 관련 시장을 육성

※ 세계 양자암호통신시장은 '30년까지 26조원 규모로 성장 전망('19년 IQT Report)

※ 미국, 중국은 양자암호통신을 국가 차원에서 지원이 필요한 5대 핵심기술(5G, AI, 양자암호, 반도체, 자율주행차)로 선정하고 적극 투자 중

○ **(적정대가 산정)** 원가분석 데이터 기반 정보보호 제품 및 서비스 **유형별 적정 대가 산정 가이드 개발** 추진('21~)

- H/W 일체형 보안제품, 보안 SW, 정보보안 서비스 등 유형별로 보안성 지속 서비스* 등의 **적정대가 세부 기준 제시**

* 정보보호제품은 일반 상용 SW와 달리 신규취약점 대응을 위한 수시 업데이트 필요

※ 시스템 구축 및 유지보수 시, 정보보호제품을 다른 제품들과 분리하여 계약 하도록 하는 근거 마련

◇ 민간분야 정보보호 투자 확대를 위한 제도 개선

○ **(사이버 방역망 강화) 전국적 사이버 안전망 구축·운영**을 통한 기업 정보보호 수준 제고 및 **신규 정보보호 투자 수요 도출**('22~)

- 現 지역정보보호지원센터를 확대·개편하여(10→17개소) 중소**기업 상시 보안컨설팅** 위한 **전국 단위 사이버방역망 구축**

- 사이버 방역팀* 구성 및 경제·사회적 관심 기업** 등 **보안 취약 기업군 정보보호 점검** 및 **집중지원**을 통한 **신규 수요 도출**

* 한국인터넷진흥원 침해사고대응본부 내 신설 + 민간 보안기업과 협업체계 구성
** 최근 코로나19로 진단키트 개발 등 바이오기업에 대한 관심 급부상

< 사이버 방역팀 구성 및 역할 >

구성	역 할
지역정보보호지원센터 + 보안기업	· **(평시)** 지역 중소기업에 대한 **기본적 보안사항 상시 점검** * 웹 취약점, 민감정보 보호조치, 비대면서비스 이용 시 보안 등 · **(대규모 사고) 사고 대응, 중소기업 복구 지원** 등 역할 전환

○ **(제도 개선) 민간기업 평가 기준 내 정보보호 투자 및 활동을 추가**하여 기업의 **자발적 정보보호 노력 및 투자 확대 유도**('22~)

< 민간기업 평가 기준 내 정보보호 지표 추가 방안>

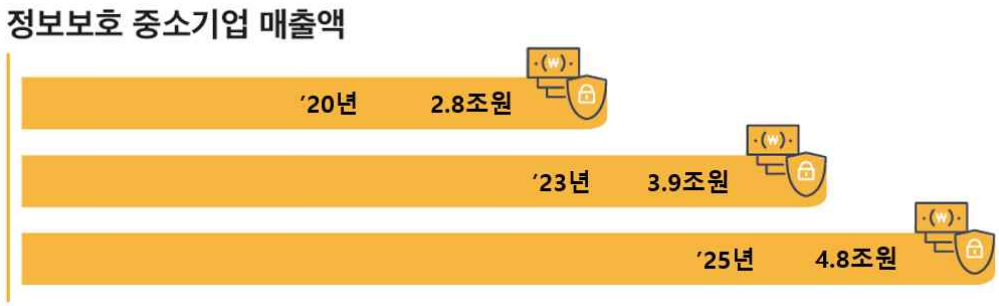
	기업신용평가	사업 보고서	정보보호 공시
추진 내용	**평가 기준** 중 '산업 위험'에 '**사이버 환경 변화' 항목 신설**	**사업보고서 內** 정보보호 투자액, 인력 등 기업 **'정보보호 투자 현황'** 항목 신설	ISMS인증 의무기업 및 CISO 등록 기업의 **'정보보호 공시' 유도**

○ **(지역 보안기업 육성)** 지역 우수 보안기업 육성을 통해 **양질의 지역 정보보호 기술 및 서비스 공급 기반 강화**('22~)

- 지역별 주요 기업·기관의 정보보호 서비스 수요, 참여요건 분석·공유 등 **정보보호 서비스 수요와 공급 매칭**

2-2 정보보호기업 성장 지원

정보보호기업의 **혁신 성장**을 위한 **선순환 생태계 구축**



□ 현황 및 문제점

o **국내 정보보호기업**의 **70.1%**가 **자본금 10억 미만**의 중소 규모로, **중견 보안기업**(3년 평균 1,500억원 이상 매출)은 **5개사**에 불과

- 또한 정보보호 **상장 기업의 비율도 9.4%**에 **불과**

※ 매년 정보보호 부분 주목해야 할 기업 150社 중 112개社가 미국, 18개社가 이스라엘, 7개社가 영국, 5개社가 캐나다(Cybersecurity Ventures)

o **글로벌 보안시장***은 급속히 성장 중이나, **국내 보안산업****은 대부분 **중소기업**으로 **영세성, 기술력 부족** 등으로 **시장 확대 한계**

* 연 12~15% 성장으로 '20~'25년간 누적 1조달러 시장('19 Cybersecurity Ventures)

** 국내 정보보안 매출은 3.3조원, 100인 미만 기업이 80.4%('19 정보보호산업 실태조사)

□ 추진 전략

o **혁신 스타트업** 및 **중소기업 고성장 지원체계** 강화

o **대·중·소 기업 상생협력 기반 구축**으로 지속 성장 환경 조성

o **혁신선도 보안 신기술 제품** 및 **서비스 창출 기반** 마련

□ 추진과제

◇ 정보보호기업 高성장 지원 클러스터 조성

◆ 정보보호 관련 **기업, 연구·교육기관, 지원 기관 및 시설 집적**을 통해 산·학·연 정보보호 **기술, 아이디어 공유와 新기술·제품 개발과 창업 유도**

○ **(정보보호 산업 고성장 기반 조성)** 우수 新기술 보유 정보보호 기업을 위한 시설·사업 등을 **송파 클러스터에 집적**하여 기업 고속 성장 기반 마련('23~)

< 정보보호 산업 고성장 지원 클러스터 구성(안) >

①기술 고도화	②기술 검증	③수요 확대	④사업 고도화	⑤해외 진출
· R&D기술공유이전 · 우수인력 연계 · 데이터 활용	· 제품성능평가 · 산학연 공동검증	· 사업화 실증 · 신규 수요창출 · 수요처 연계	·상생협력기반 제공 ·투자유치기반 제공	·해외진출 역량 강화 ·개도국 초청 비즈니스 연계

①정보보호 기술이전, 데이터셋 공유, AI 데이터학습센터, ②K-NBTC, K-ICTC 및 제품성능평가, K-CMVP 보안 인증 등, ③수요기반 실증센터, ④Secu-Tech 얼라이언스 등, ⑤해외진출 역량강화 프로그램

○ **(K-시큐리티 클러스터 벨트) 정보보호기업 단계별 성장 생태계 확립**('23~)

< K-시큐리티 클러스터 벨트 조성 계획(안)>

o 정보보호 클러스터(판교)를 통해 융합보안 등의 신규 분야 및 **초기창업 기업발굴, 정보보호 인재를 양성**하고 이를 통해 양성된 **우수 혁신 기술을 기반으로한 기업이 고성장할 수 있는 거점**(송파)을 신설, 국내 정보보호 기업의 단계별 성장 생태계 조성

	(판교) 정보보호 클러스터	(송파) 정보보호 산업 고성장 지원 클러스터
대상	• 정보보호 스타트업	• 고성장 정보보호 중소기업
목적	• 보안 新기술 발굴, 초기기업 육성	• 보안 新기술 고도화 및 사업화, 기회확대
주요 프로그램	• 스타트업 지원(창업), 인재양성(교육) • 사업화 모델 컨설팅, 네트워킹 등	• 신기술 도입을 위한 시험·인증·테스트 • 해외시장 진출 및 정착을 위한 지원

◇ 보안 리딩기업 주도 상생 생태계 구축 확대

○ **(성장 기반 마련)** 보안 리딩기업이 참여·투자하는 **정보보호 전문 엑셀러레이터 육성**을 통한 보안 시장 상생 생태계 구축('22~)

※ 중소기업창업지원법에 등록된 엑셀러레이터(230여개) 중, 보안은 안랩 1개社('19년)

※ (美) 사이버보안 스타트업 육성을 위한 전문 엑셀러레이터 FedTech('15년), SixThirty Cyber('16년), Sparklabs Cyber+Blockchain('18년)를 통해 보안기업 육성

- 스타트업 양성·투자 수요가 있는 **보안 리딩기업**과 보안 전문성이 부족한 **엑셀러레이터 대상**으로 정보보호 엑셀러레이터 양성

※ AI, 빅데이터, IoT 등 4차 산업분야 신서비스 모델에 부합하는 전문 엑셀러레이터 양성 프로그램인 'K-Global 엑셀러레이터 육성 사업('~23년)'에 보안부문 신설

< 정보보호 전문 엑셀러레이터 육성 방안 >

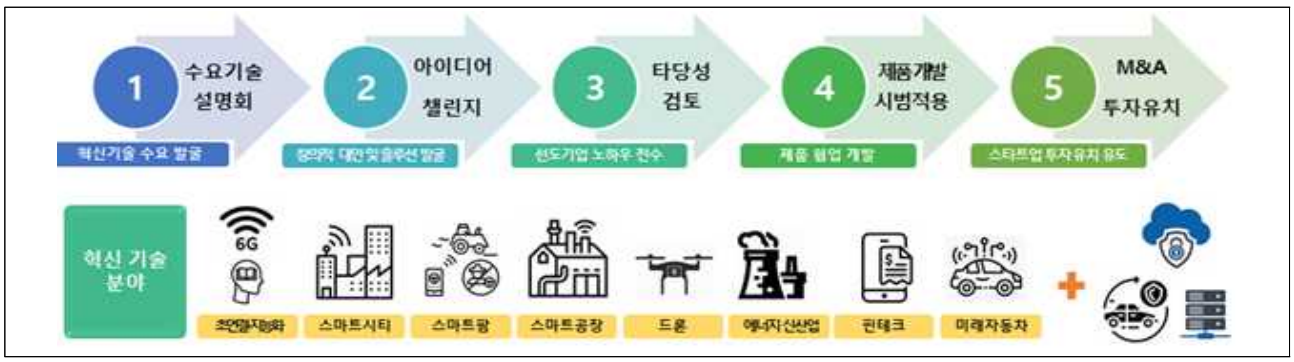
대상	설립지원	인프라지원	육성·성장지원	활동지원
정보보호 리딩기업	정보보호기업+ 엑셀러레이팅 역량강화	인큐베이팅 시설 입주를 통한 지원 정보보호 전문인력 직접 인건비 지원	엑셀러레이팅 역량강화, 정보보호 교육, 산업 트렌드 파악, 정보보호분야 네트워킹, 기업탐방	(보안기업 투자 시) 투자금액 매칭지원
엑셀러레이터	엑셀러레이터+ 정보보호전문가			

○ **(협업 기반 마련)** 정보보호 리딩기업과 유망 정보보호 중소기업간 자발적 상생·협력을 위한 Secu-Tech 얼라이언스* 구성·운영('22~)

* 정부·산하기관, ICT·정보보호 리딩기업 ,스타트업, 창업투자사 등 50여개로 구성하여 민간 주도의 M&A 활성화를 유도할 수 있는 기반으로 역할

- **오픈 이노베이션 챌린지** 및 **수요와 협업기회 발굴**을 위한 정기 네트워킹 활성화, 기술설명 데모데이 및 투자 상담회 등 운영

< 오픈 이노베이션 챌린지 운영(안) >



◇ AI 기반 등 혁신 보안 기업 고성장 지원 체계 강화

○ **(AI 보안기업 육성) AI 보안기술 고도화 및 글로벌 경쟁력 확보**를 위해 우수 AI 보안 기술을 가진 유망 기업을 선정·육성

※ 유망기업 발굴부터 해외진출까지 우수 아이디어 사업화 지원(5년간 20개社)

- 창업·육성 지원 플랫폼인 정보보호 클러스터(판교)를 활용하여 AI 기반의 혁신보안 기술 **유망 보안기업 단계별 집중 지원**

< 단계별 지원체계 >

(1단계) 유망기업 발굴	(2단계) 시뮬레이션	(3단계) 시제품 개발
AI 보안기술 보유 유망 보안기업 발굴 (10개社)	모델링/시뮬레이션, 타당성 결정 (10개社)	프로토타입을 통한 성능검증, 개선 (5개社)
(4단계) 제품 제작	**(5단계) 제품 상용 및 사업화**	**(6단계) 해외진출 지원**
수요기반*의 제품/서비스 제작 (5개社)	제품/서비스 고도화 후 상용·사업화 지원 (5개社)	KISA 해외거점 활용한 글로벌化 추진 (5개社)

※ 국내 공공 및 민간기업 등 연계를 통한 수요처 발굴 및 매칭 프로젝트 추진

○ **(고성장 지원) 기업 경쟁력 제고**를 위해 **고성장 보안기업 확산 중심의 맞춤형 3SS**(3-Stage-ScaleUp) **성장 프로그램 도입**('21~)

※ 高성장 기업 매출상승→고급인력 유입→제품 경쟁력 제고→성장의 선순환 지속

- ①스타트업→②유망 스타트업(내수)→③고성장 중소기업(수출)으로 Scale-up 할 수 있는 성장 주기별 **seamless 지원체계** 강화

< 연도별 배출기업 수(총 150개社) >

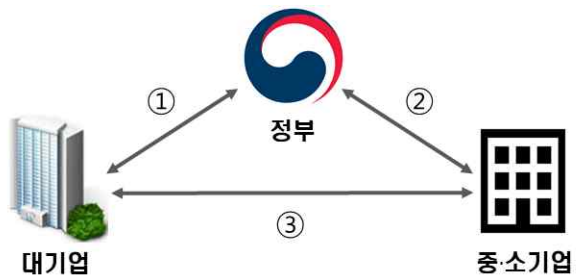
○ **(투자기반 확충)** 중기부 **스케일업 펀드***를 활용하여 고성장 보안 중소기업의 후속성장에 필요한 **대규모 투자금 공급** 촉진

* '20년 출자사업에서 2개, 3,250억원 규모 벤처펀드 선정

◇ 대기업과 정보보호기업 매칭형 기술개발 지원 사업

○ **(수요 중심 DNA 新기술 확산)** 신뢰기반의 디지털 전환 촉진을 위해 데이터, 네트워크, 인공지능(AI) 관련 보안 新기술 개발('23~)

- **대기업**의 **新기술 수요**와 **중소 정보보호기업**의 **유연한 기술 경쟁력을 매칭**하여 상생·협력 기반의 성장 환경 조성



구분	역할
①	**(정부)** 기술개발 지원사업 기회 제공 **(대기업)** 新기술 과제 지원
②	**(정부)** 기술개발 지원금 지급 **(정보보호기업)** 新기술 연구개발 수행
③	**(대기업)** 완제품 1년간 구매 유도 **(정보보호기업)** 수요맞춤형 제품 개발

◇ 매칭을 통한 **대기업**과 **중소 정보보호기업**이 가지고 있는 **한계**를 **해소**

- **(대기업)** 정보보호 新기술에 대한 수요는 있으나, 해당 분야의 투자 대비 낮은 사업성으로 인하여 기술개발 투자에 소극적
- **(정보보호기업)** 수요가 확실하지 않은 보안 신기술에 대한 연구·투자가 쉽지 않고, 수요처(대기업)의 요구사항에 대한 접근이 어려움

○ 신규투자가 쉽지 않은 **정보보안 신기술 분야 투자환경을 활성화**하고 **시장↔공급자를 매칭**하여 지속가능한 성장 환경 조성('23~)

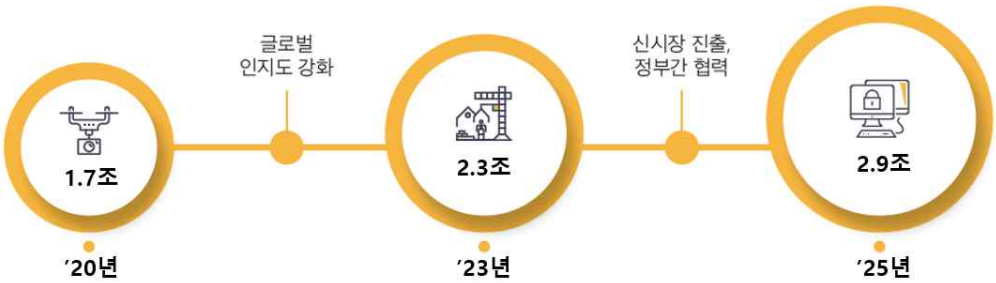
- **보안 신기술**에 대한 **레퍼런스**를 쌓기 힘든 중소기업에게 해당 분야에 대한 진출 기회 마련

- 적극적인 **보안 신기술 연구** 및 도입에 대한 **진입장벽 완화**

구분	1단계(`23~`24)	2단계(`25~)
집중지원 분야	4개 분야	7개 분야로 확대
	AI보안, 5G보안, 클라우드보안, 데이터 보안	
	-	반도체 보안, 퀀텀통신보안, 6G보안
과제개수	8개	10개

2-3 정보보호기업 해외진출 및 국제협력 강화

해외 정보보호 신시장 발굴을 통한 기업 성장구조 완성



< 국내 정보보호산업 수출액 목표치>

□ 현황 및 문제점

o 국내 보안기업 수출액(1.6조원, '19년)은 **대부분 물리보안제품 수출**(1.5조원)이며, **정보보안은 약 1천억원 수준**에 그침

< 최근 정보보호산업 수출액 현황 (단위 : 백만원, %) **>**

구분	정보보안		물리보안		합계	
	수출액	증가율	수출액	증가율	수출액	증가율
2015	78,133	+7.1	1,545,540	+6.3	1,623,673	+6.3
2016	88,978	+13.9	1,400,102	-9.4	1,489,080	-8.3
2017	94,398	+6.1	1,475,755	+5.4	1,570,153	+5.4
2018	82,363	-12.7	1,473,769	-0.1	1,556,132	-0.9
2019e	108,528	+31.7	1,537,785	+4.3	1,646,313	+5.8

※ 정보보호 수출은 두드러진 급성장보다는 매년 비슷한 수준으로 유지

o **'19년** 기준 글로벌 정보보안시장 규모는 **1,212억불**이며, **'23년**(1,679억불)**까지 연평균 8.3% 성장**할 전망(Gartner)

- 세계적으로 스마트시티, 스마트공장 등 **물리·정보보안 연계** 및 코로나19로 인한 **언택트(비대면) 보안시장**이 급성장 예상

□ 추진 전략

o 한국형 **'물리보안·정보보안 연계 보안모델'** 및 **'비대면 서비스 + 보안 패키지 모델'**을 활용하여 **해외 보안시장 개척**

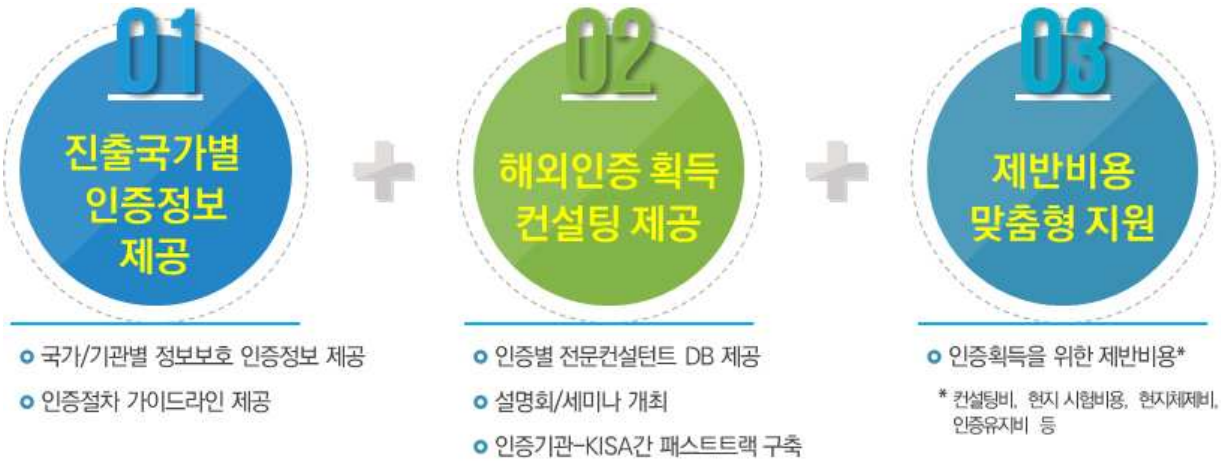
o 정부 간 **국제협력 활용** 및 **보안 선진시장**(미국 등) **진입 지원**을 통해 국내 보안기업의 해외사업 참여기회 확대

□ 추진과제

◇ 정보보호 선진시장 진출지원

○ **(해외인증 획득지원)** 국내 정보보호기업의 **해외진출을 위해 선결**되어야 하는 **해외인증 획득 가이드라인 및 컨설팅 제공**('21~)

- 물리보안 및 정보보안 해외인증 획득을 위해 **▲ 국가별 인증정보 제공, ▲ 컨설팅 제공, ▲ 인증획득 제반비용** 맞춤형 지원



○ **(글로벌 경진대회 진출)** 기술 혁신 **보안기업의 글로벌 경진대회 진출**을 통한 국내 정보보호기업 위상제고·해외 투자유치 확대('21~)

- 사이버보안 시장전망 및 분석을 통해 향후 보안트렌드를 반영한 **집중지원 분야 선정** 및 **관련 기업 발굴·지원**

※ RSA(세계최대보안엑스포) 內 Innovation Sandbox Contest(혁신 스타트업 투자유치 경진대회) 참가 및 우승을 목표로 기업 발굴

○ **(조인트벤처)** 해외 **현지기업-국내기업 간 조인트 벤처 지원을 통한** 현지화 강화 및 공공시장 진입지원 등 **선진시장 진출**('22~)

- 현지 조인트벤처를 통해 **▲** 현지 운영인력 및 마케팅, 기술지원 등 **현지 활동비 절감**, **▲** 현지 진출의 **시행착오를 최소화**

※ **(조인트벤처)** 국내기업을 대신하여 현지에서 입찰지원, 영업활동, 기술지원 역량을 보유한 현지기업과 국내기업 간 파트너십 기업

◇ 한국형 보안모델을 활용한 해외 보안시장 개척

○ **(보안 수출모델 개발) 물리보안·정보보안 연계모델**을 발굴하여 전자정부 협력사절단, 한국형 스마트시티 수출 등 동반 해외진출('22~)

- 보안서비스 맞춤형 컨소시엄 구성, 물리·정보보안 해외진출협의회 구축, 정보보호해외수주지원센터 운영 등 **해외진출 네트워크 구축**

※ 세계시장 규모 : (스마트시티) '25년 1.56조$, (스마트공장) '24년 3,912억$, 연평균 9.22%↑(Frost&Sullivan, Smart Cities/Marketwatch, Smart Factory Market Overview, '18년)

< 물리보안·정보보안 연계보안모델 >

○ **(비대면 서비스+보안 패키지사업)** 언텍트 서비스 모델과 **보안 서비스를 결합하여** 국내 정보보호기업의 해외 수출시장 확대('21~)

- **한국형 '비대면 서비스+보안 패키지 모델'**을 KOTRA 등 유관기관의 언택트 수출사업과 연계하여 **K-사이버 방역 확산** 추진

◇ 정부間 협력을 활용한 해외진출 수요 발굴

○ **(해외협력 네트워크 구축)** 글로벌 사이버보안 협력 네트워크(CAMP*) 회원국 대상 **정보보호 역량강화 세미나** 활동 수행('21~)

* Cybersecurity Alliance for Mutual Progress : 45개국 59개 기관('19년 기준)이 사이버보안 국제협력 활성화를 위한 정보공유 및 침해사고에 대한 공동 대응

- **국내·현지 정보보호 전문 자문단을 활용한** 수요국 대상 정책자문, 연구조사 활동을 통해 **현지 보안 시장의 親한국 환경조성 지원**

< 컨설팅 수행 프로세스 >

○ **(국제기구 협력)** WB, IDB, CABEI 등 **다자개발은행(MDB) 개발협력기금** 활용을 위한 보안 타당성조사·지식공유프로그램 기획('21~)

- 유관기관(NIPA, KIND, NIA 등)의 해외 타당성조사 활동 공동수행을 통해 개도국 보안인프라 구축사업 등 **국제기구 협력사업 수행**

○ **(유관기관 공동진출)** 국내 **유관기관과 공동 해외진출**을 통해 **정보보호산업 진흥** 및 **국가 이미지 제고**('21~)

- **전자정부 협력사절단**과 정보보호컨설팅 공동수행, 원조사업을 통한 **개도국 정보보호 역량강화 과제**수행, **유관기관과 연계** 추진

전자정부 컨설팅	유상원조	무상원조	유관기관 연계사업
행정안전부(NIA)	수출입은행 대외경제협력기금(EDCF) 경협증진자금(EDPF)	한국국제협력단 공적개발원조(ODA)	NIPA (타당성조사) KIND (타당성조사)

3. 지속성장 가능한 정보보호 생태계 조성

3-1 차세대 보안 新기술 확보

4차 산업혁명 시대를 앞당길 미래 선도 보안기술 육성

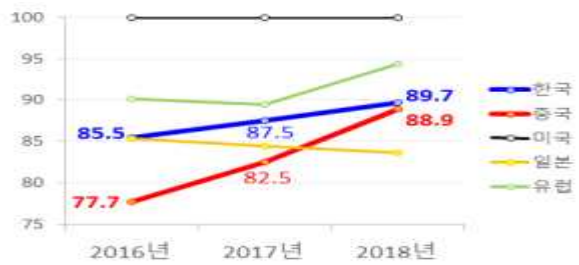
□ 현황 및 문제점

o 사이버공격이 대규모 테라급 공격으로 **규모가 확대**되고, 초연결·지능화 시대 AI 등 **신기술**로 무장한 **5세대 사이버공격으로 진화**

o 국내 정보보호 기술수준은 미국의 기술수준 대비 점진적으로 상승 추세이나 최근 중국의 기술력이 급상승하고 있어 한국 추월 우려

- 민간부문 정보보호 R&D 예산 규모는 증가세가 둔화하고 있으며, 정보보호 R&D 투자 비중*도 해외에 비해 낮아 투자 확대 필요

* 한국 6.5%, 미국 16.7%, 일본 20.7% (2018, 전체 R&D 대비 정보보호 R&D 비중)



< 정보보호 기술수준(%) >

< 정보보호 R&D 예산 규모(백만원) >

□ 추진 전략

o 디지털 전환과정에서의 새로운 사이버 위협에 대비할 수 있는 **정보보호 R&D 투자 확대**('25년 정보보호 R&D 예산규모 1,000억원)

o **차세대 정보보호 원천기술 확보** 및 R&D 지원체계 고도화

□ 추진과제

o 비대면 시대로의 디지털 환경 변화와 데이터 3법 통과로 인한 디지털 경제 활성화 촉진을 위해 데이터·AI **보안新기술의 신속한 개발** 필요

o 5G/6G 네트워크 환경, 양자컴퓨팅 시대 도래에 따른 새로운 보안 위협*의 대두로 미래를 선점할 수 있는 **미래 전략기술 확보** 필요

* 테라급 DDoS 공격, AI기반 사이버 공격, 기존 암호체계 붕괴 등

◇ 디지털 경제 활성화를 위한 新기술 집중 투자('21~'25, 250억/년)

○ **(비대면 서비스 보안강화)** 포스트 코로나 시대를 대비하는 **비대면 서비스 보안 강화 및 신뢰성 보장** 기술개발 중점 지원

< 유사 망분리 >

내·외부망 분산환경을 고려하여 망분리와 유사한 보안 수준 제공

< 비정상 행위 탐지 >

지속적인 모니터링을 통해 비정상 행위를 탐지·차단하는 보안 체계 제공

< 사용자 편의성 제공 >

사용자 불편없이 지속적 보안 솔루션 제공이 가능한 보안 내재 환경

○ **(데이터 보호)** 개인·가명정보 활용을 위해 안전한 저장·관리·유통을 가능하도록 하는 **데이터 보호 新기술 개발** 추진

- AI 학습 데이터 보호를 위해 대용량의 정형·비정형 정보를 암호화한 상태로 안전하게 이용 가능한 **동형암호* 기술** 개발 및 확산

* 동형암호 : 민감한 데이터를 암호화된 상태에서 복호화 없이 가공·활용

- 개인정보 노출을 최소화함과 동시에 데이터의 활용성을 높여주는 **차분프라이버시 기술** 활성화

* 차분프라이버시 : 데이터의 삽입·삭제, 변형에 의한 변화량을 일정수준 이하로 유지하여 정보노출 최소화

< 데이터 보호를 위한 기술 >

- **활용성 강화 암호화** : 암호화 상태를 유지하면서 원본 데이터의 정렬, 범위검색이 가능한 암호화 기술
- **위험기반 비식별화** : 데이터(개인정보) 특성과 환경에 따른 위험도를 기반으로 적용할 비식별화 수준을 자동 결정하는 기술
- **재식별 검증 및 추적** : 개인정보를 가명·익명처리하는 과정에서 발생할 수 있는 재식별화 위험성 분석·검증, 개인·가명정보 이용내역 추적 등 대응 기술

○ **(AI 기반 지능형 보안)** 국내 AI 기술 도입 지연에 따라 기술력이 하락한 영역*에 대해 **AI 기반 보안기술** 및 AI 자체 보안 **집중**

* 통합보안관리, 엔드포인트 보안, 네트워크 방화벽 분야에 AI 기술 적용

- AI가 기술·산업·사회 전반에 활용됨에 따라 **AI 자체에 대한 취약점 조치 및 보안 강화*** 연구

* AI 데이터의 조작, 학습데이터 추출 공격 등 AI 유형별 공격에 대응하는 방어 기술

◇ 미래 정보보호 전략기술 · 체계 마련

[1] 차세대 정보보호 R&D 기술 육성(~'25년, 500억 원)

○ **(양자내성암호)** 양자컴퓨팅 시대에 **기존 암호 인프라 무력화에 대비**하기 위한 선도 투자 및 저변 확대

- 다양한 환경에서 사용 가능한 응용기술 개발* 및 국내·외 표준화, 양자내성암호 성능·안전성 테스트 및 유관제품 개발 지원

* 스마트시티, 헬스케어 등 5G, ICT 융합 인프라에 양자내성암호 기술을 적용하여 성능검증 및 상용화 기반 마련

○ **(6G 보안)** 6G 보안위협 분석 및 대응기술, 6G 환경에서의 보안 내재화를 위한 기반기술 등에 대한 선행 연구 추진

※ 6G 기술의 본격적인 표준화 단계 이전에 6G 보안 기술연구를 통해 6G 보안기술, 장비 및 운영 보안 시장 선점 노력

[2] 정보보호 R&D가 성장할 수 있는 체계 정비

○ **(플래그십 R&D)** 해외 시장을 선도할 수 있는 **특화된 R&D 추진**

- **산·학·연 협업**을 통해 기술과 자원을 결집시켜 **시너지 효과**
- 국내·외 시장규모에 비해 기술수준이 정체된 분야를 **신기술과 접목**
- 국제적으로 통용되는 국제산업표준을 준수하여 해외 시장 선도

○ **(혁신적 R&D 지원)** 창의적인 **정보보호 신기술 개발을 유도**하고, **우수 연구자 선별 및 집중지원**을 위한 혁신적 R&D 지원

- 정부는 문제만 제시하고 대회를 통해 우수 연구자 선발 및 후속 연구를 지원하는 **챌린지형 R&D 지원**
- 복수의 연구기관 선정 후 단계별로 연구결과 경쟁을 통해 우수 연구기관을 선정하여 연구비 집중 지원하는 **경쟁형 R&D 지원**
- 파급력 높은 고난이도 신기술, 국가·사회 측면 미래 위협에 선제 대비할 수 있는 분야로 **역할 중심 전문연구실 확대**

◇ 사회문제 해결 및 안보강화를 위한 R&D 지속 투자('21~'25, 300억/년)

○ **(부처협력)** 정보보호 관련 R&D 수요는 있으나 독자적인 R&D가 부재하여 **기술개발이 불가한 부처들의 기술 수요** 반영 확대

- 「관계기관 R&D 협의체」 등을 통해 각 부처의 자체 보안 수준 향상 등 기술 수요 기반 R&D 추진 및 결과물의 현장 적용 지원

○ **(사회문제해결)** 국가 치안 및 재난상황 대응, 사생활 침해 해결 등 **대국민 사회 안전**을 위한 **사회문제 해결형 R&D*** **확대**

* 언택트 환경에서의 딥페이크 사기 방지, N번방 등 유해컨텐츠 추적/감시, 클라우드 기반의 신개념 서비스 등장에 따른 안전한 보안환경 구축 등

○ **(안보강화)** 시장 규모가 적고 국내 기술 수준도 낮으나, 침해사고 원인분석 및 안전성 검증 등 **안보 관점**의 **핵심기술 지속 투자**

※ 취약점분석/보안 테스트를 해외에 의존(해외기관 시험 의뢰 등)할 경우, 소스코드 등 국내 기술·데이터 유출 우려

참고2 국내외 정보보호 기술수준

○ **(기술) 국내 정보보호 기술수준***은 '16년 대비 점진적으로 **상승 추세**
('16년 85.5% [기술격차 : 1.1년] → '18년 89.7% [기술격차 0.8년] 4.2%↑)
* IITP ICT 기술수준조사, 5개국(미국, EU, 한국, 일본, 중국) 상대수준(미국 100%) 비교 결과

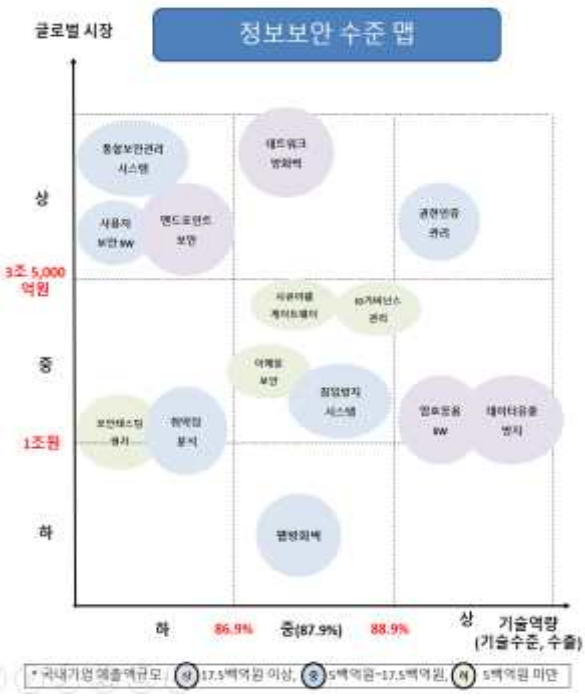
- 최근 중국의 기술력이 급상승(한국 2.7배)하여 **한국 추월 예상**
('16년 77.7%→'18년 88.9%, 11.2%↑)

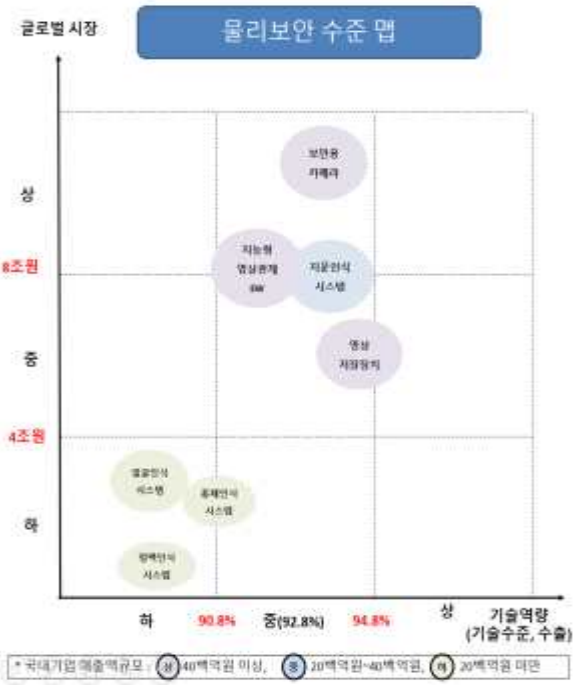
	유럽			일본			한국			중국		
구분	2016	2018	증가률	2016	2018	증가률	2016	2018	증가률	2016	2018	증가률
정보보호	90.2%	94.4%	4.2%	85.4%	90.4%	5.0%	85.5%	89.7%	4.2%	77.7%	88.9%	11.2%
정보보안	88.9%	91.9%	3.0%	83.8%	86.4%	2.6%	82.7%	87.5%	4.8%	77.0%	85.8%	8.9%
물리보안	91.6%	96.9%	5.3%	87.1%	94.4%	7.3%	88.2%	91.8%	3.6%	78.5%	92%	13.5%

○ **(R&D) 최근 5년간 민간부문 정보보호 R&D 정부 투자**는 '16년 411억원 → '20년 605억원 규모로 **연평균 10% 증가**
(투자비중 :정보보안 75%, 물리보안 12%, 융합보안 13%)

구분	2016	2017	2018	2019	2020	합계
R&D 투자 (단위: 백만원)	41,157	53,917	61,750	61,905	60,527	279,256 (연평균 10% 증가)

※ 정보보호 R&D 정부 투자금액으로 민간 기업 등의 R&D 투자금액은 제외





<출처 : 정보보호 제품 및 기술 수준 진단맵, 2019, 과기정통부>

3-2 정보보호산업 규제 및 법·제도 개선

국가 정보보호 인증제도 개선 및
정보보호산업 법령 정비를 통한 **제도적 기반 강화**

□ 현황 및 문제점

o 정보보호기업들은 **인증제도의 중복**과 인증 획득을 위한 **시간·비용 부담**으로 기업 활동의 어려움을 호소하고 있고, **한국 대표 정보보호 브랜드 부재**로 해외인지도 부족

o **디지털 전환 및 비대면 서비스** 전반에서 **신기술 활용과 정보보호 데이터 이용 확대**를 위한 **법적 근거** 마련 필요

o 전자서명법 전면개정으로 **블록체인, 생체인증 등 신기술 기반의 다양한 전자서명의 개발·이용**이 활성화되고 국민의 전자서명 이용 편리성도 높아질 것으로 기대

□ 추진 전략

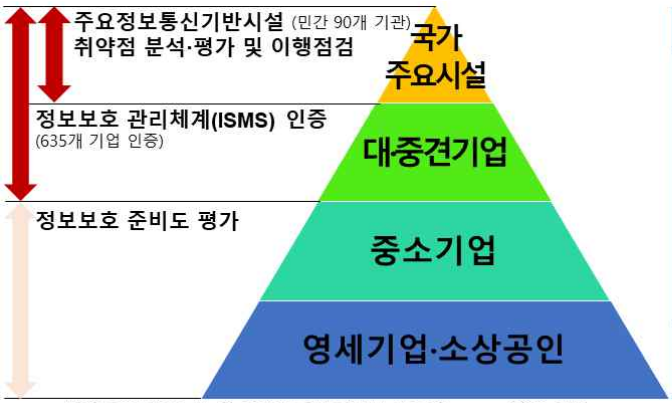
o **기업 부담경감과 보안 사각지대 해소**를 위한 **보안인증 체계화**

o ICT융합 환경에서 **정보보호산업의 지속 성장을 위한** 제도적 개선과제 발굴 및 법령 정비

□ 추진과제

◇ 수요자 관점에서 SMART한 보안인증 체계 마련

< 기업규모별, 제품·서비스별 주요 정보보호 인증제도 현황 >



※ 법적요건 충족 시 주요정보통신기반시설 지정, ISMS 인증 의무

구분	제도	비고
제품	정보보호제품 평가·인증 (Common Criteria; CC)	침입차단·방지시스템 스팸메일 차단시스템 무선랜 인증제품 등 23종
	정보보호제품 성능평가	DDoS 대응장비 안티바이러스 제품 소스코드 보안분석 도구
	IoT 보안인증	IoT제품, 연동 모바일앱 등
	IP 카메라 보안성능 인증	IP 카메라
	바이오인식제품 시험인증	바이오인식제품(S/W)
서비스	클라우드 서비스 보안 인증	클라우드 환경의 서버·장비 등 인프라, S/W 등

※ 국가·공공기관 도입 시 필수(음영)

○ (Standardization(표준화)) 현행 인증·평가제도와 국제기준, 비대면 보안 등 ICT 환경변화를 고려해 **'정보보호 표준인증항목'** 마련('21~)

- 각 정보보호 인증제도에 대해서 표준인증항목을 토대로 제도별 특성을 고려한 세부항목을 추가

○ (Modification(조정)) 분야별 유사한 인증은 **중복 부분을 제거**하고 **하나로 묶어서 심사·인증**하고, **인증 간 상호호환성 확대**('21~)

< 정보보호 인증제도 간 상호 호환성 확대(안) >

(1) 보안관리 관련 인증을 **정보보호 및 개인정보보호 관리체계**(ISMS-P) **인증 중심으로 통합**하고, 기업 규모별 **맞춤형 운영**

(2) 금융·의료·교육 등 분야별 관계기관과 정보보호 인증체계 협업을 통해 분야별 정보보호 인증제도와 ISMS 인증 간 **상호인정 등 부담경감 방안 마련**

(3) **ISMS 인증 획득 기업**이 **클라우드 보안인증** 신청 시 **평가항목 일부항목 면제**

○ (Application(신청)) **'정보보호 인증 통합 신청포탈'** 구축 및 홍보('22~)

- 정보보호 인증 신청을 한 곳에서 한 번에 처리하고, 인증 정보 현황 및 인증 민원 처리현황 등 실시간 모니터링 지원

○ (Redesign (범위 재설계)) **클라우드서비스, 가상자산사업자** 등 ICT 신산업에 대한 사각지대를 해소하여 **촘촘한 사이버안전망** 구축('21~)

- 가상자산 거래의 투명성 제고와 보안강화를 위해 **가상자산 사업자 맞춤형 정보보호 관리체계(ISMS)** 인증 마련
- 기업 보안정책수립에 활용토록 **비대면 서비스, 정보자산 폐기, 융합보안, IoT 보안** 등 IT환경 변화를 반영한 **정보보호지침** 마련

○ (Total Service(종합지원)) 기업의 **정보보호 인증 혜택을 확대**하고, 기업이 **직접 인증을 준비**할 수 있는 환경 조성('21~)

- 인증별 증빙서류의 **표준양식화,** 알기 쉬운 **준비 가이드라인 제작** 및 영세기업 대상 **정보보호인증 컨설팅 지원 확대**

< (예) SMART하게 개선된 정보보호 관리체계(ISMS) 인증제도 >

(1) **(표준화)** 증빙서류 축소 및 제출양식 50% 이상 표준화, 표준 기업보안정책 등을 제공하여 컨설팅 없이 기업 스스로 인증을 준비할 수 있는 환경 조성

(2) **(상호인정)** ISMS 인증 획득 기업이 클라우드 보안인증 신청 시 평가항목 약 40% 면제

◇ 국가 정보보호 인증 프레임워크 구축 및 브랜드化

○ **국가인증(K-Trust) 프레임워크 구축 및 브랜드화**('22~)

- 성능, 보안성, 안전 관리체계 등 기존의 개별인증을 복합적으로 획득한 제품·서비스에 **K-Trust 인증을 부여**하는 인증체계 개발

< K-Trust 인증 개념(안) >

[K-Trust Level 1 인증]

□ 성능 + 보안성, 성능 + 관리체계, 보안성 + 관리체계 등 2개의 인증을 획득한 비대면, 정보보호 제품·서비스 대상 부여

[K-Trust Level 2 인증]

□ 3개의 인증(성능 + 보안성 + 관리체계)을 획득한 비대면, 정보보호제품·서비스 대상 부여

< 브랜드 구성안 >

K-Trust	구분코드
	K - Security - OO - OOO OO: 보안성, 성능 / 제품, 서비스

□ 추진과제

◇ 정보보호산업 관련 법·제도 개선

○ **(D·N·A기반 법제 신설) 디지털 전환 및 비대면 서비스** 전반에서의 **신기술 활용 및 데이터 이용 활성화**의 근거 마련('21~)

- 비대면 서비스의 핵심 기술인 클라우드, AI, 생체인식 등 **신기술 보안성 검증 및 이용 확대**를 위한 법적 근거 마련

※ 클라우드 보안 인증제도 법적 근거 마련, 원격 생체인식의 이용근거 마련 등

- 데이터 이용 활성화를 위해 기업의 정보보호기술·제품 및 서비스 연구개발 지원을 위한 **정보보호 데이터 수집·활용 체계 법제화**

※ 정보보호 데이터 수집·가공 체계 구축·운영 등 법적 근거 마련

○ **(전자서명법 전면개정 후속조치)** 공인인증서 제도 폐지에 따른 블록체인, 생체인증 등 **신기술 정보보호기업의 시장진출** 지원('21~)

- 전자서명 수단의 신뢰성 제고, 이용자의 합리적 선택에 필요한 정보제공을 위해 **'전자서명인증업무 운영기준 등 고시'** 마련

※ 생체인증·블록체인 기술 기반 전자서명인증업무 세부 평가기준('20~'21)→다양한 신기술 도입에 따라 평가·인정대상 확대(~'23)

○ **(정보보호산업 법제 개선)** AI, IoT, SW 등의 **보안 강화**를 위한 관련 법 개정 및 개별법의 **정보보호 기능 강화·연계**를 위한 **정보보호기본법 제정** 등 정보보호 신산업 육성을 위한 법제 개선('21~)

- 지능정보서비스 보안(지능정보화기본법), 5G+ 융합서비스 보안(정보통신망법), SW 개발보안(소프트웨어진흥법) 등에 따라 정보보호 기술개발 및 사업화 지원을 위한 법제 개선 연구

- ICT융합 환경변화에 대응하여 현행 정보통신망법 등 정보보호 법제를 **정보보호 기본법**을 **중심**으로 **체계화**하는 개편방안 마련

3-3 정보보호 전문인력 양성

정보보호 인력체계 혁신을 통한 **정보보호산업 성장 주도**

□ 현황 및 문제점

o **전통산업의 ICT융합 확산**에 따라 다양한 융합제품·서비스 및 산업분야별 보안위협에 대응할 **보안 전문인력 수요 증대**

※ ICT융합 등 4차산업 육성 강조추세에도 현장은 인력난('19.4월, 한국경제)

o 정보보호는 전세계적으로 **인력공급이 크게 부족***한 분야로서, 성공적인 디지털 경제 전환을 위해 **인력수급 개선 필요**

* 국내 정보보호 전문인력은 매년 1.4~2천명 부족('19.12월, 한국인터넷진흥원)
- '21년까지 세계적으로 350만 명에 달하는 IT 보안 인력 부족('20.4월, Cybersecurity Venture)

o 정보보호산업 혁신성장을 위한 임금, 근로여건 등 **처우개선** 및 경력모델 개발, 인력지원체계 구축 등 **정보보호인력 성장지원 요구**

□ 추진 전략

o 정보보호산업 혁신성장을 선도할 **정보보호 전문인력 양성**

⇒ '25년까지 **정보보호 전문인력 일자리 3만개 마련**

o **사람 중심**의 **全 주기적 정보보호인력 지원체계** 구축

◇ 정보보호산업 일자리 창출을 위한 정보보호 전문인력 양성

○ **(신규인력) 산업계 수요** 기반의 **맞춤형 정보보호 신규 인력 양성**('21~)

- 산업계 수요를 반영한 교육과정 설계 및 프로젝트 수행을 통해 **산업 맞춤형 실무인력** 및 **차세대 보안리더** 양성

- 5G · 클라우드 환경 기반의 신산업 및 비대면 서비스 등 **분야별 특화된 정보보호 특성화대학 · 융합보안 대학원** 확대

※ 특성화대학('20년 4개 → '25년 8개), 융합보안대학원('20년 8개 → '25년 12개)

○ **(재직자) 실무역량** 및 **신기술 분야 보안 역량** 강화 지원('21~)

- 재직자 대상 보안기술 습득·강화를 위한 실습과정 및 위협사례 기반의 **사이버훈련장** 운영 등 **보안인력의 실무역량 제고**

- 자율주행차·스마트시티 등 **ICT융합보안 산업 분야**에 대한 **재교육**을 통해 재직 인력의 **신기술 분야 보안 역량 강화** 지원

○ **(기반 강화) 우수인재 발굴 · 육성**을 위한 **인력양성 기반 강화**('22~)

- **(저변확장)** 중·고등학생 대상 초급 정보보호 교육, 대학 정보보호 동아리 지원 및 국제해킹방어대회 개최 등 **정보보호 인재 활동 확장**

- **(교육연계)** SW·AI분야 인재양성 프로그램과 연계*(학점교류 등)하여 다양한 영역에 정보보호가 내재화 될 수 있도록 **정보보호 교육 확대**

* 융합보안대학원에서 학점을 취득하면, SW・AI분야 대학원에서도 그 학점을 인정

- **(협력체계 구축)** 유관부처 간 정보보호 인력양성 정책실무협의회 구성 및 정보보호 교육기관, **인력 수요기업·기관 등과 협력 강화**

< 정보보호인력양성 기반 강화 >

정보보호 인재 저변 확대	정보보호 교육 확대	협력체계 구축
		

◇ 全 주기적 정보보호 일자리 관리체계 구축

○ **(생애주기 경력 관리)** 정보보호 신입→경력→전문가 성장을 위한 **全주기 경력관리** 및 **지역별 인력유입·순환을 위한 일자리 공유**('22~)

- 주요 직무별 경력경로, 커리큘럼 안내 등 **경력관리*** 및 지역별 구직정보(채용규모·임금·직무·필요역량 등) 제공 가능한 **일자리 맵 구축**

* 정보보호 직무별로 필요한 교육수준·교육과정 등을 표준화하고, 이에 필요한 커리큘럼·자격·기술 등을 제공하여 정보보호 전문가로 성장할 수 있게 지원

○ **(신규 및 전환지원)** 공공기관·기업의 **신입 및 경력직 구직 정보 제공, 구직자**가 **쉽게 정보보호 산업계**로 **진출**할 수 있게 지원('22~)

- 정보보호 관련 분야 학위·자격·경력 등을 등록한 **보안전문가**와 지자체·지역기업 등 **일자리 수요를 연결**하는 **지원시스템 구축·운영**

- **포스트 코로나 환경**에서 온라인을 활용한 구직자가 입사를 희망하는 기업 등의 **현직자 멘토 매칭 및 취업지원** 강화

< 정보보호 일자리 관리체계 '경력활용 시스템(안)' >

○ **(처우개선 및 위상강화)** 정보보호 업계 **우수인력 확보 · 유지**를 위한 **정보보호 전문인력 처우개선 및 위상강화**('22~)

- **적정 임금기준* 마련**, 파견업무 등 **근로환경 개선** 및 분쟁조정위원회 확대를 통한 **인력별 법률자문, 고충처리 등 지원**

* 정보보호 전문가에 대한 직무 표준화 및 구체적 임금정의 추진(SW노임단가)

- 임원·고위직 대상 **인식제고**와 **전문인력 처우 및 제도** 개선방안 연구 및 개선으로 근로자부심, 평생근무의욕 제고

※ 정보보호 기업 대상 직원 경력관리 지원제도(직원대상 교육비 지원, 대체임금 지원 등) 마련

붙임 과제별 추진일정

추진과제	소관부처	추진일정 '21	'22	'23	'24	'25
1 디지털 전환에 따른 정보보호 신시장 창출						
1-1 비대면 서비스 관련 보안시장 활성화						
• 비대면 서비스 보안 시범사업 및 공공분야 선도적 도입	과기정통부, 행안부					
• 중소기업의 비대면 보안 서비스 도입 확산 지원	과기정통부, 기재부					
• 비대면 관련 솔루션&정보보호 공급기업 지원	과기정통부					
1-2 정보보호 데이터 활용기반 조성						
• AI 기반 정보보호제품 확산을 위한 학습데이터 가공공유 체계 구축	과기정통부					
• 정보보호기업의 AI 학습데이터 이용 지원	과기정통부					
1-3 AI 기반 물리보안 산업 육성						
• 물리보안 선도적 기술	과기정통부					
• 물리보안 산업 기반 강화	과기정통부					
• 물리보안 응용 서비스 확산	과기정통부					
1-4 5G⁺ ICT 융합보안 산업 저변확대						
• ICT 융합산업 보안 강화	과기정통부, 국토부, 중기부, 식약처					
• 융합보안 강화를 위한 제도 정비						
• 융합보안 산업 신시장 창출	과기정통부					
• ICT 융합보안을 위한 사물인터넷(IoT) 보안인증 제도 개선	과기정통부					
• 안전한 ICT 융합보안 솔루션 개발·공급 지원	과기정통부					
2 민간 주도 사이버 복원력 확보를 위한 투자 확대						
2-1 공공·민간분야 정보보호 투자 확대						
• 공공부문 정보보호 투자 확대 기반 조성	과기정통부, 행안부					
• 민간분야 정보보호 투자 확대를 위한 제도 개선	과기정통부·금융위					
2-2 정보보호기업 성장지원						
• 정보보호 기업 高성장 지원 클러스터 조성	과기정통부					
• 보안 리딩기업 주도 상생 생태계 구축 확대	과기정통부					

추진과제	소관부처	추진일정				
		'21	'22	'23	'24	'25
• AI 기반 등 혁신 보안 기업 고성장 지원 체계 강화	과기정통부, 중기부					
• 대기업과 중소 정보보호기업 매칭형 기술개발 지원 사업	과기정통부					
2-3 정보보호 해외진출 및 국제협력 강화						
• 정보보호 선진시장 진출지원	과기정통부					
• 한국형 보안모델을 활용한 해외 보안시장 개척	과기정통부, 행안부·국토부					
• 정부間 협력을 활용한 해외진출 수요 발굴	과기정통부, 행안부·기재부, 외교부, 국토부					
3 지속성장 가능한 정보보호 생태계 조성						
3-1 차세대 보안 新기술 확보						
• 디지털 경제 활성화를 위한 新기술 집중 투자	과기정통부					
• 미래 정보보호 전략기술·체계 마련	과기정통부					
• 사회문제 해결 및 안보강화를 위한 정보보호 R&D 지속 투자	과기정통부					
3-2 정보보호산업 규제 및 법·제도 개선						
• 수요자 관점에서 SMART한 보안인증 체계化 추진	과기정통부					
• 국가 정보보호 인증 프레임워크 구축 및 브랜드化	과기정통부					
• 지속성장 가능한 정보보호 생태계 조성을 위한 법제 개선	과기정통부					
3-3 정보보호 전문인력 양성						
• 정보보호산업 혁신성장을 선도할 정보보호 전문인력 양성	과기정통부					
• 全 주기적 정보보호인력 관리체계 구축	과기정통부					