'민간부문 정보보호 종합계획 2019' 주요내용

('19.1.8, 정보보호기획과)

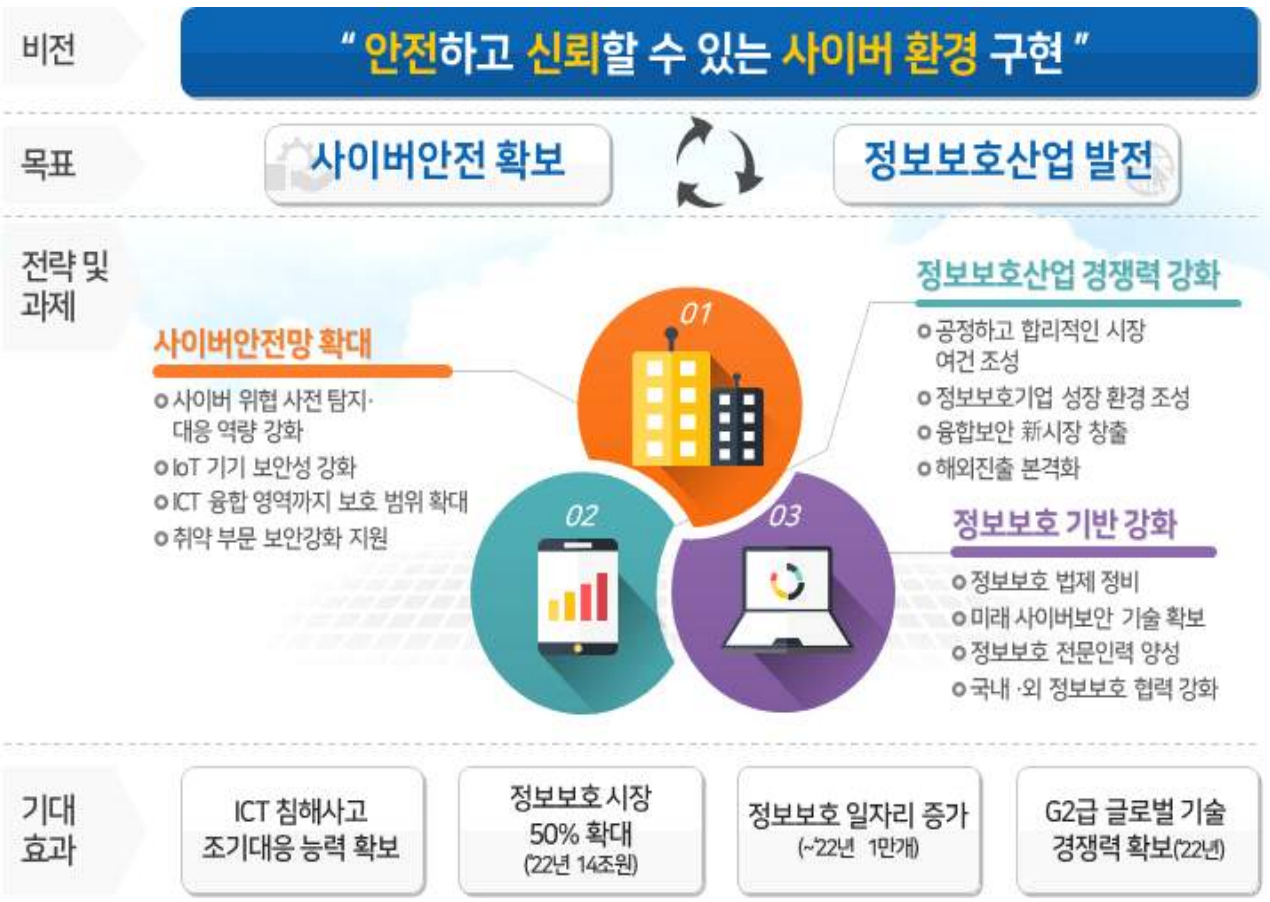
1 추진배경

○ 최근 랜섬웨어 공격, IP카메라 해킹 등 다양한 사이버사고가 발생하며 국민 불안감 확산, 해킹·안전 우려가 ICT 新기술 확산의 걸림돌로 작용

※ '17년 사이버사고에 의한 세계적 손실액 약 6천억 달러(676조원)로 추산 (맥아피,'18.2)

○ 사이버보안의 중요성 증대로 글로벌 보안 수요가 지속 확대(연 8% 성장)되고 있으나 국내 보안 산업 경쟁력이 미흡하여 대책 필요

2 비전 및 추진전략



3 주요추진과제

1 사이버안전 수준을 높이겠습니다.

◈ 사이버보안 빅데이터 센터 및 IoT 기기 상시 안전점검체계 구축, ICT 융합 산업 보안 강화 등을 통해 생활 주변 사이버보안 체감 수준 제고

① 사이버위협 탐지·대응 역량 강화

○ 사이버위협정보의 수집·공유는 물론 잠재 위협 및 사고 예측이 가능하도록 **사이버보안 빅데이터 센터 구축·고도화**(위협정보 現 3.5억건→6억건 이상)

○ **사이버보안 빅데이터**를 **활용**하여 사이버위협 패턴을 기계 학습·분석하고 위협을 사전 인지하여 **공격 조기 탐지·대응 역량 강화**

② IoT 기기 보안성 강화

○ **IP카메라 비밀번호 재설정 의무화** 제도 시행('19.2월), **IoT 기기 보안 인증서비스** 활성화 등을 통해 **안전한 IoT 이용환경 조성**

○ **지능형 IoT 기기 취약점 탐지·분석체계**를 **구축**하여 주요 시설 및 희망 기업·국민에게 점검·보완 서비스 제공

③ ICT 융합 영역까지 보호 범위 확대

○ 기존 ICT 보안성 검증 기준의 산업별 적용을 위해 **부처간 협력**을 통한 기준 개발 및 **산업별 안전성 관련 인증제도** 등에 **사이버보안 기준 추가**

○ 산업 분야별 정보공유·분석센터(ISAC)를 교통·제조분야 등으로 확대하고, **기반시설 지정 확대, 공급망 및 신규 장비 보안 등 관리책임 강화**

④ 취약부문 보안 강화 지원

○ **지역정보보호지원센터**를 **확대**(7개→'20년 10개)하고, 중소기업에 대한 컨설팅·보호조치 지원 확대 및 KISC연계 **지역안전망 구축 등 기능 강화**

○ **다중이용 ICT 서비스** 대상 **보안점검 강화**로 취약점 선제 대응

2 정보보호 산업을 육성하겠습니다.

◈ 기업하기 좋은 환경을 조성하고 융합보안 新시장 창출 및 해외 진출 지원을 통해 정보보호 산업 혁신성장 촉진

① 공정하고 합리적인 시장 여건 조성

○ **정보보호 인증제품**을 **공공구매 수의계약 대상**에 **포함**하고, 정보보호 관리등급제 및 준비도평가 등 **유사 인증 제도 정비방안 마련**

○ 공인인증서 제도를 폐지하고(서명법 개정안 국회제출, '18.9월), **신규 인증(authentication)서비스** 개발·확산 촉진을 위해 **상호운용성 검증**('20~) **등 지원**

○ SW사업 대가 산정 가이드에 **보안성지속서비스 요율 산정기준 개정 추진**

② 정보보호기업 성장환경 조성

○ 송파, 판교, 지역 정보보호 지원 인프라를 연계한 **권역별 '시큐리티 허브'**를 **조성**하고 보안 스타트업 등 **기업의 신제품 개발 원스톱 지원**

○ 제도 개선을 통한 정보보호 공시 활성화, **'Korea IT Fund' 등에 정보보호 분야 신설** 및 **정보보호 IR-프로그램 운영**('19) 등 **보안 투자 촉진**

③ 융합보안 新시장 창출

○ 의료·교통·공장 등 **분야별 보안 모델 개발·보급** 및 **실증사업 추진**

○ **정부의 8대 혁신성장 선도사업** 추진 시 **보안**을 **내재화**할 수 있도록 관계부처 협력 강화 및 **융합보안 모범사례집 발간·보급**

④ 해외진출 본격화

○ 전략국가를 고려해 거점 위치 조정 등 **해외거점 운영 확대·내실화**

○ VIP 순방 참여, 민·관 공동마케팅 강화 등 **해외진출 지원프로그램 개선** 및 스타트업 해외진출 보육프로그램 운영 등 **해외진출 역량 강화 지원**

3 정보보호 기반을 강화 하겠습니다.

◈ 기존 '네트워크 보호' 중심의 법제를 '융합'(IoT기기 등) 분야까지 확대하고, 기술·인력 육성 및 국내·외 정보보호 협력 강화

① 정보보호 법제 정비

○ 융합 분야 **정보보호 주체**를 **서비스 제공자에서 제품·운영·이용자까지 확대**하고 **주체별 보호책임 부여** 및 **위협 발생시 관계부처 대응 협력**

○ **사고통계 제공** 등 **사이버보험**을 **활성화**하고, 사이버사고 집단분쟁 조정제도 신설방안 연구 등 **사이버보안 정책연구 활성화**

② 미래 사이버보안 기술 확보

○ 데이터, 네트워크, AI 등 4차 산업혁명시대 핵심인프라 보호 기술 개발을 위한 **정부 R&D 투자 확대**(**5년간 3천7백억원 규모** 예타 추진)

◀ 4차 산업혁명 사이버보안핵심기술개발 사업 추진 방향 ▶

■ 데이터경제 신뢰성 보장 ■ 5G·IoT 융합서비스 안전성 강화 ■ 지능형 위협 대응 고도화

○ 현안 해결형 과제 및 미래 위협 대비 장기·도전적 과제를 구분 추진하고, 기술개발 시의성·효과성 제고 위한 **오픈 R&D 추진체계 정비**

③ 정보보호 전문인력 양성

○ 현장인력 교육·훈련 확대, 융합보안 대학원 석사과정 신설('19년 3개교) 등 **정보보호 전문인력 양성 확대**('22년까지 약 9,000명 규모)

④ 국내·외 정보보호 협력 강화

○ 정부, 기업, 해외 다자협의체 등 **국내·외 다양한 주체들과 협력 체계 강화** 및 **정보보호정책자문위, 사이버안전포럼** 운영 등 對**국민소통 활성화**

Ⅳ. 기대효과

○ '22년까지 **사이버 침해사고 조기 대응 능력**을 **강화**하고 기존 '네트워크' 중심에서 **ICT 융합 영역까지 보호 범위 확대**

○ **국내 정보보호 시장 규모 약 50% 확대**('17년 9.5조원→'22년 14조원), **일자리 1만개 창출** 및 정보보호 분야 **G2급 기술 경쟁력 확보**