관계부처합동 | 보도자료 | APEC 2025 KOREA

보도시점 2025.10. 22.(수) 14:00 (2025.10.23.(목) 조간) 배포 2025.10.22.(수) 10:00

범부처 정보보호 종합대책 발표

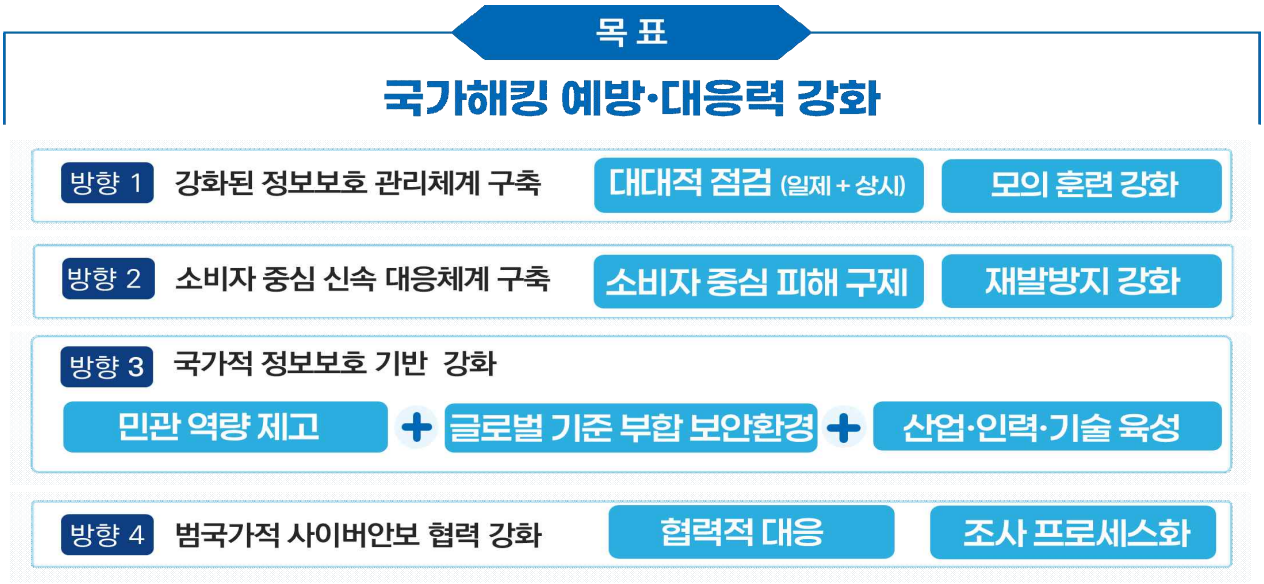
- **국가안보실 중심**으로 **관계부처 합동** 수립, **민·관**을 아우르는 **시급한 개선 과제 제시**
- **정보 기술 체계 전수점검, 정부 조사 권한 강화, 소비자 중심 피해구제** 등 **국민 불안 해소**
- **보안을 비용이 아닌 투자로 전환**하기 위한 **정보보호 등급제, 최고 경영책임자(CEO)·정보보호 최고책임자(CISO) 역할 강화** 등

과학기술정보통신부(부총리 겸 과기정통부장관 배경훈, 이하 '과기정통부')와 관계부처는 **전방위적인 해킹 사고**로 **국민 불안이 가속화**되는 현 상황을 **신속히 극복**하고 **국가 전반의 정보보호 역량을 강화**하기 위해 **「범부처 정보보호 종합대책」**을 수립하여 **10월 22일(수) 대국민 보고(브리핑)**를 통해 발표하였다.

정부는 분야를 막론하고 반복되는 **최근 일련의 해킹 사고**를 **심각한 위기 상황으로 인식**하고 있으며, **범정부 차원의 유기적인 대응체계를 즉시 가동**하고자 한다.

이를 위해 **국가안보실을 중심**으로 **과기정통부, 금융위원회, 개인정보보호위원회, 국가정보원, 행정안전부** 등 **관계부처 합동**으로 **민간과 공공을 아우르는 범부처 정보보호 종합대책을 수립**하였다. 동 대책은 현 사안의 시급성을 고려하여 즉시 실행할 수 있는 **단기과제 위주로 제시**하였으며, 이후 **중장기 과제를 망라**하는 **「국가 사이버안보 전략」을 연내 수립**할 계획이다.

「범부처 정보보호 종합대책」의 **주요 추진 방향**으로는 **❶국민 생활에 밀접한 핵심 정보기술 체계**의 **대대적인 보안 점검**을 추진하고, **❷소비자 중심의 사고 대응 체계 구축**과 **재발 방지 대책의 실효성을 강화**한다. 아울러 **❸민·관 전반의 정보보호 역량을 강화**하는 한편, 국제적 **기준에 부합하는 정보보호 환경 조성**과 **정보보호 산업·인력·기술을 육성**하고, 마지막으로 **❹범국가적 사이버안보 협력 체계를 강화**한다.



< 1. 핵심 정보기술 체계(IT 시스템)에 대한 대대적 점검과 상시 취약점 탐지 체계 구축 >

우선 해킹에 대한 국민들의 만연한 불안감 해소를 위해, **공공·금융·통신** 등 국민 대다수가 이용하는 **1,600여개*** **정보기술 체계(IT 시스템)**들에 대해 **대대적인 보안 취약점 점검**을 즉시 추진한다.

* 공공기관 기반시설 288개, 중앙·지방 행정기관 152개, 금융업 261개, 통신·온라인 이음터(플랫폼) 등 보안 인증 제도(ISMS) 인증기업 949개 등

특히 **통신사**의 경우에는 실제 해킹 방식의 **강도 높은 불시 점검을 추진**하고 **주요 정보기술 자산에 대한 식별·관리체계를 구축**하도록 한다. 아울러 **소형기지국(펨토셀)**은 안정성이 확보되지 않을 경우 즉시 폐기하는 등 **보다 엄격히 조치**할 계획이다.

아울러 **보안 인증 제도**(ISMS, ISMS-P)를 **현장 심사 중심으로 전환**하고 **중대한 결함이 발생**할 경우 **인증을 취소**하는 등 **실효성을 제고**하고 **사후관리를 강화**하는 한편, **모의해킹 훈련**과 **착한 해커(화이트해커)를 활용**한 **상시 취약점 점검 체계**도 구축한다.

< 2. 소비자 중심의 사고 대응체계 구축 및 재발 방지 대책 실효성 강화 >

기업의 보안 해태로 인한 해킹 발생 시 **소비자의 입증책임 부담을 완화**하고 통신·금융 등 주요 분야는 **이용자 보호 안내서(매뉴얼)를 마련**하는 등 **소비자 중심의 피해구제 체계**를 구축하는 한편, 개인정보 유출 사고로 인한 **과징금 수입**을 피해자 지원 등 **개인정보 보호에 활용**할 수 있도록 **기금 신설을 검토**한다.

이와 함께 **해킹 정황을 확보**한 경우에는 **기업의 신고 없이도 정부가 신속히 현장을 조사**할 수 있도록 **정부의 조사 권한을 확대**하고, 아울러 해킹 지연 신고, 재발 방지 대책 미이행, 개인·신용 정보 반복 유출 등 **보안 의무 위반**에 대해서는 과태료·과징금 상향, 이행강제금 및 징벌적 과징금 도입 등 **제재를 강화**한다.

그리고 **국가정보원의 조사·분석 도구**를 **민간과 공동 활용**하는 한편, **인공 지능 기반 지능형 디지털 증거복구실(포렌식실)을 구축**하여 **분석 시간을 대폭 단축**(건당 14일 → 5일)하는 등 **침해사고 탐지·대응 역량을 고도화**하고 영역별 **사고조사 전문인력을 확보·충원**하는데 박차를 가한다.

< 3-1. 정보보호 투자확대 유도 및 중소기업 지원 강화 >

공공부터 정보보호 역량 강화에 솔선수범하기 위해, **공공의 정보보호 예산***, **인력**을 **정보화 대비 일정 수준 이상으로 확보**('26년 1분기)하고 정부 **정보보호책임관 직급**을 기존 국장급에서 **실장급으로 상향**하는 한편, 위기 상황 대응 역량 강화 **훈련 고도화**, **공공기관 경영평가** 시 **사이버보안 배점 상향**(0.25→0.5점) 등을 추진한다.

* 현재는 정보화 예산 대비 15% 이상의 정보보호 투자를 권고하는 선언적 규정 수준

민간의 경우 보안에 대한 인식을 더 이상 비용이 아닌 기업의 성패를 가르는 필수 투자로 전환할 수 있게, **정보보호 공시 의무 기업**을 **상장사 전체로 확대**(현재 666개사 → 약 2,700여개사로 확대)하면서 동시에 공시 결과를 토대로 **보안 역량 수준을 등급화하여 공개**하는 제도를 도입한다.

아울러 최고 경영책임자(CEO)**의 보안 책임 원칙을 법령상 명문화**하고 **보안최고책임자(CISO·CPO)의 권한을 대폭 강화***하는 한편, 자체적인 보안 역량이 부족한 **중소·영세기업** 대상으로는 **정보보호 지원센터 확대**** 등을 통해 **밀착 보안 지원**을 강화한다.

* (예) 모든 정보기술 자산에 대한 통제권 부여, 이사회 정기 보고 의무화, 정보보호 인력예산 편성집행 등

** 지역 정보보호 지원센터 (현재) 10개소→16개

< 3-2. 국제 변화에 부합하는 제도 마련 및 환경 조성 >

기존 전통적인(레거시적인) 보안 고립(갈라파고스) 환경에서 과감히 탈피하여 국제적 변화에 부합하는 보안 환경을 조성하기 위해, **금융·공공기관 등이 소비자에게 설치를 강요**하는 **보안 소프트웨어를 단계적으로 제한**('26년~)하는 대신 **다중 인증***, **인공 지능 기반 이상 탐지 체계** 등의 활용을 통해 보안을 강화한다.

* (예) 비밀번호, 일회용 비밀번호(OTP), 생체인식 등 조합(모바일 신분증 등)

그리고 인터넷 기반 자원공유(클라우드), 인공 지능 확산 등 국제 변화에 부합하지 않은 **획일적인 물리적 망분리**를 **데이터 보안 중심으로 본격 전환**('26년~)하고, **인터넷 기반 자원공유(클라우드) 보안 요건 개선** 등 민간 사업자의 공공 진출 요건 완화를 추진한다.

아울러 **공공분야에 사용되는 정보기술 체계(IT 시스템)·제품**에 대해 소프트웨어 **구성요소(SBOM)의 제출을** '27년까지 **제도화**하고 **보안 문제가 발견**된 정보기술 제품은 **공공 조달 도입 제한**을 추진하며. **산업용·생활용 정보기술 제품군**(사물인터넷 가전 등)에 대한 보안 평가 공개 등을 추진한다.

< 3-3. 보안산업을 국가전략 산업화하고 사이버안보 인력·기술 육성 >

인공 지능 3대 강국을 뒷받침할 보안산업 육성을 위해 인공 지능 대리인(AI 에이전트) 보안 이음터(플랫폼) 등 **차세대 보안 기업을 집중 육성**(연 30개사)하고, 보안 산업의 저변 확대를 위해 **정보보호 서비스***의 **범위를 확대**한다.

* 정보보호산업법에 따라 안전하고 신뢰할 수 있는 정보보호서비스 기업을 지정하는 제도
(현행) 보안 자문(보안컨설팅)·관제 전문기업 → (확대) 인공 지능 보안·소프트웨어 공급망보안 등 관련 전문기업

아울러 보안 최고 전문가인 착한 해커(**화이트해커**)(연 500여명) **양성 체계를 기업 수요로 재설계**하고, **정보보호특성화대학**(학부, 7개교), **융합보안대학원**(석박사, 9개교)을 **5극3특*** **권역별 성장엔진 산업에 특화**된 **보안 인재 양성 거점**으로 기능을 강화('26년~)하는 등 전주기 보안 인력 양성을 체계화·고도화한다.

* 동남권(지능형 조선<스마트조선> 등), 대경권(미래차부품 등), 호남권(인공 지능 등), 중부권(생명과학<바이오> 등)

그리고 다가오는 양자 시대를 대비하기 위해 **양자내성암호 기술 개발** 등 **국가적 암호체계 전환을 착수**하고, **공공부문**에서 자율주행차, 지능형 로봇, 드론 등 **신기술 이동수단(모빌리티)의 안전한 활용**을 위한 **보안 점검표(체크리스트)** 및 **방침(가이드라인)을 수립**('26년)한다.

< 4. 범국가적 사이버안보 협력 강화 >

국가 핵심 기반시설(인프라)인 **주요정보통신기반시설**을 범부처 위원회인 **정보통신기반시설보호위원회**(위원장 : 국조실장)를 통해 **지정을 확대**해 나가고, **기반시설의 사고 원인 조사** 단계에서는 **침해사고대책본부**(국가사이버위기관리단으로 지정)를 활성화한다.

아울러 **부처별로 파편화된 해킹 사고조사 과정을 체계화***하여 현장의 혼선을 최소화하고, **민관군 합동 조직**인 국가정보원 산하 **국가사이버위기관리단**과 **정부 부처 간의 사이버 위협 예방·대응 협력을 강화**한다.

* 일괄(One-Stop) 신고체계 도입, 조사단별 투입시기 최적화, 상호 정보공유 강화 등

배경훈 부총리는 대국민 보고(브리핑)에서 "과기정통부 등 관계부처는 이번 **종합대책이 현장에서 제대로 작동**될 때까지 **실행 과정을 면밀히 살펴볼 것**이며 **부족한 부분을 지속적으로 보완**해 나가겠다"라고 하면서, "앞으로도 정부는 **인공 지능 강국을 뒷받침**하는 **견고한 정보보호 체계 구축**을 취해 총력을 기울이겠다"고 하였다.

과기정통부	정보보호네트워크정책관 정보보호기획과	책임자	과 장	김연진 (044-202-6440)
		담당자	사무관	심재환 (044-202-6441)
기획재정부	경제예산심의관 정보통신예산과	책임자	과 장	김건민 (044-215-7230)
		담당자	사무관	김기홍 (044-215-7394)
금융위원회	디지털금융정책관 금융안전과	책임자	과 장	김태훈 (02-2100-2970)
		담당자	서기관	김영민 (02-2100-2573)
		담당자	사무관	이혜인 (02-2100-2979)
개인정보보호위원회	개인정보정책국 신기술개인정보과	책임자	과 장	고낙준 (02-2100-3061)
		담당자	서기관	정종일 (02-2100-3066)
행정안전부	디지털정부정책국 디지털보안정책과	책임자	과 장	주경애 (044-205-2741)
		담당자	사무관	박병호 (044-205-2747)

내일을 만드는 과학기술 내삶을 채우는 디지털·AI
대한민국 정책브리핑
APEC 2025 KOREA 10.27.~11.1. 경주
OPEN 출처표시 공공누리 공공저작물 자유이용허락