제2차 정보보호 종합 대책

기업 보안의 기준을 바꾸다

AhnLab

사후 대응에서 사전 예방 책임 체계로

2026년 1월 28일 정부가 발표한 「제2차 정보보호 종합대책」은 국내 정보보호 정책의 기준을 근본적으로 바꾸고 있습니다. '침해사고 이후 대응' 중심에서 벗어나 사고를 예방하고 책임을 입증해야 하는 '사전 예방 책임' 체계로의 전환이 핵심입니다. 기업의 법적 책임과 소비자 보호 의무는 확대되고, 보안 투자 수준과 운영 성숙도는 직접적인 평가 기준이 되고 있습니다. 이제 정보보호는 규제 준수를 넘어 기업의 법적·재무적 리스크를 좌우하는 핵심 경영 요소로 자리 잡았으며, 기업은 사전 예방 중심의 보안 운영 모델을 재정비해야 합니다.

반복되는 침해사고, 정책은 방향을 바꿨다

지난 한 해 동안 발생한 통신·금융·이커머스 분야에서 발생한 대형 침해사고는 고도화된 해킹 기술보다 기본 보안 관리와 운영 체계의 미비에서 비롯된 것으로 분석됐습니다. 암호 미적용, 보안 패치 방치, 권한 통제 부실 등 구조적 관리 실패가 누적되면서, 기업에 대한 사회적 요구도 함께 높아졌습니다.

	2025.04	2025.06	2025.09		2025.11
보안 사고	S통신사 유심 정보 유출	Y사 랜섬웨어 감염 및 회원정보 유출	K통신사 무단 소액 결제 피해	L카드사 고객카드 정보 유출	C사 고객정보 유출
원인	암호 미적용, 로그 관리 등 보안 규정 미준수	보안 패치 미적용, 보안 인력 체계 취약	통신 장비(펨토셀) 관리 소홀	알려진 취약점 방치, 내부 보안 관리 소홀	내부자(퇴직자) 통제 및 권한 관리 부실

정책 변화가 요구하는 3가지 전환

1. 소비자 피해 구제로의 기업 책임 범위 확대

침해사고 발생 시 기업 책임이 개인정보 유출을 넘어 소비자 피해 전반으로 확대됩니다.

기업 영향

- 분쟁 조정 제도 확대
- 조기 통지 의무 강화
- 사고 발생 후 법적·재무적 리스크 증가

요구 역량

기술적 복구를 넘어 소비자 보호 프로세스를 포함한 체계적 IR 운영 필요

2. 보안 투자 수준의 제재·평가 기준화

개인정보보호법상 안전조치 의무 수준을 넘어서는 인력·예산·설비 투자 수준이 제재와 감경의 기준이 됩니다.

기업 영향

- 과징금 경감 구조 도입
- 보안 투자 수준의 평가 요소화
- 컴플라이언스=경영 리스크 관리

요구 역량

보안 투자 수준을 증빙하고 관리할 수 있는
체계 마련

3. AI 기반 탐지·대응 체계 필수화

AI 기반 공격 확산에 대응하기 위해 민간·공공 위협 탐지·대응 체계의 AI 전환이 요구됩니다.

기업 영향

- AI 레드팀 운영을 통한 모의침투 테스트 본격화
- 모델 오염·업데이트 위조·중요 정보 유출 위협 대응
- 지능형 탐지·대응 체계 요구

요구 역량

AI 기반 SOC, XDR 등
상시적·자동화된 대응 체계 구축

컴플라이언스 대응, 기업은 무엇을 준비해야 하는가

「제2차 정보보호 종합대책」은 정보보호를 단순한 규제 준수 항목이 아닌, 법적·재무적 리스크를 최소화하기 위한 경영 체계로 내재화할 것을 요구하고 있습니다. 기업은 사고 이후 대응 중심의 운영 방식에서 벗어나, 사전 예방과 상시적 위험 관리를 중심으로 한 통합 보안 체계를 준비해야 합니다.

기존 (Before)

사고 발생 이후 대응 중심

〉

개편 (After)

사고 예방·상시 위험 관리 중심

거버넌스·기술·운영이 결합된
선제적 통합 대응 체계

사전 예방 중심의 운영 모델로 전환하기 위해서는, 정책 요구사항을 관리적·기술적 조치로 구체화한 실행 체계가 필요합니다. 아래 표에 제시된 보안 솔루션 및 서비스는 주요 정책 요구사항을 충족하기 위한 대표적인 적용 예시입니다.

구분	2차 주요 과제 목록	정책 유형	기업 대응 관련 이슈	개정 후
관리적 조치 중심 과제 (거버넌스·프로세스·제도 대응)	침해사고로 인한 개인정보 유출 이외의 소비자 피해에 대해서도 분쟁조정 제도 도입	제도 개선 (규제 강화)	침해사고 대응 및 사후 관리 체계 필요	
	개인정보 유출 가능성이 있는 경우 통지 의무화, 통지 항목(손해배상 청구 등) 추가	제도 개선 (규제 강화)	유출 대응 절차의 사전 정립 필요	ISMS-P인증 컨설팅
	개인정보 보호 투자에 따른 과징금 경감	제도 개선	정보보호 투자 수준의 체계적 관리 및 성과 가시화 필요	정보보호 마스터플랜 수립 컨설팅
	AI 분야별(인프라, 서비스, 에이전트) 보안 모델 개발	연구과제		
	AI-BOM 등 전주기(개발 → 배포) 평가 프레임워크 R&D 및 실증 추진('26~)	기반 지원 사업	AI 개발 운영 전 과정의 보안성 검토	ISO/IEC 42001:2023 컨설팅
	민·관 취약점 신고·공개 제도 자율 도입 확대를 위한 가이드라인 및 인센티브 강화	제도 개선	취약점 신고/공개 제도 구축	동적 취약점 진단(모의해킹) 컨설팅
	침해사고 조사 권한 강화(특별사법경찰권부여)	감독 기관 권한 강화		
	고위험 개인정보 처리기관 실태점검 강화	제도 개선 (규제 강화)	개인정보 관리 체계의 정기적 점검 및 개선 필요	개인정보관리체계 컨설팅 ISMS-P 인증 컨설팅 개인정보처리 수탁사 진단
	중소기업 보안 자율 점검 확대	기반 지원 사업	자율적인 보안 수준 점검 역량 강화 필요	보안 자가진단 체계 구축 컨설팅
	디지털·AI 융합 환경을 고려한 디지털 요소 포함 제품 보안 정책 마련	제도 개선	기획 단계부터 디지털·AI 보안 요소 반영 필요	
	국가 사업 기획·과제 선정 단계 보안 요소 필수 반영 체계 개선(ICT R&D 우선 적용)	제도 개선		
	SBOM 관리체계 구축 지원	기반 지원 사업	SW 자재명세 설계 및 공급망 절차 수립 필요	
기술적 조치 중심 과제 (보안 솔루션·서비스 대응)	사이버 공격 全 과정 AI 대응	신기술 적용	AI 기반 위협 탐지·대응 역량 고도화	AhnLab EDR/MDR/MDS AhnLab XDR/MXDR AhnLab ATIP
	국가·공공기관과 민간의 취약점 분석·관리 및 재발 방지 대책 수립 등을 AI로 효율화	신기술 적용	취약점 관리의 상시화·자동화 필요	AhnLab ESA(단말) AhnLab EDR/EPM(취약 S/W 모니터링 및 관리) AhnLab XDR 서버 및 네트워크 취약점 컨설팅/ASM 컨설팅

기술적 조치 중심 과제 (보안 솔루션·서비스 대응)	AI 레드팀 운영을 통한 AI 취약점 점검 수행	신기술 적용	AI 서비스 선제적 보안 점검 필요	AI 대상 모의해킹/AI 서비스 침투 테스트(Pentest)
	암호화 기술 개발·상용화 촉진	연구과제	중요 데이터 보호 기술 적용 확대	데이터 암호화 솔루션
	민·관이 중요 데이터를 암호화하도록 인증기준(ISMS) 등 개정	제도 개선	데이터 보호 수준의 체계적 강화 필요	보안 컨설팅 서비스
	개인정보 불법 유통 처벌 강화	제도 개선 (규제 강화)		
	다크웹 모니터링 확대	정부 감시 수준 제고	외부 유출 정보 사후 탐지 필요	AhnLab TIP 연계 다크웹 모니터링(정보 수집·분석 중심)
	온라인플랫폼 인증 강화	제도화/권고	인증 체계 고도화 필요	다중요소인증(MFA)
	중소기업 개인정보 유출 예방	기반 지원 사업	기본 보안 역량 강화 필요	중소기업용 엔드포인트·네트워크 보안 통합 패키지
	공급망·SW 구성 요소 관리	기반 지원 사업	소프트웨어 구성 요소 가시성 확보 필요	SBOM 관리 솔루션 공급망 보안 진단

[표] 주요 정책 변화에 따른 기업 대응 과제: 관리적 조치 vs 기술적 조치 예시

※ 본 표는 정책 과제의 성격에 따라 관리적·기술적 조치를 구분해 정리했으며, 하나의 정책 과제가 두 영역을 동시에 요구하는 경우에는 이를 각각 제시했습니다.

※ 본 표는 정책 요구사항을 기준으로 한 대표적 대응 솔루션의 예시이며, 산업별 환경에 따라 적용 솔루션은 달라질 수 있습니다.

정책 변화 대응을 위한 안랩 보안 적용 모델

정책 전환은 보안을 기술 영역의 문제가 아닌, 기업 책임과 리스크 관리의 문제로 재정의하고 있습니다. 기업은 개별 솔루션이 아닌, 거버넌스·운영·기술 통제를 통합한 상시 위험 관리 체계를 갖춰야 합니다. 안랩은 정책 요구사항을 기능 중심의 보안 운영 모델로 구조화해 실행 가능한 대응 체계를 제시합니다.

거버넌스·컨설팅

정책 대응 및 관리 체계 수립

ISMS-P 인증 컨설팅
개인정보보호 컨설팅

위협 인텔리전스

선제적 위협 분석·정보 공유 체계

AhnLab TIP

취약점·공격 표면 관리

사전 위협 식별·공격 표면 관리

기술진단 컨설팅
AhnLab ASM 컨설팅

위협 탐지·대응

상시 위협 탐지·사고 대응 체계

AhnLab EDR/MDR
AhnLab XDR/MXDR
AhnLab MDS
AhnLab A-FIRST

엔드포인트·네트워크 보호

핵심 자산 보호 및 통제 체계

AhnLab EPP
AhnLab EDC
AhnLab ESA
AhnLab EPrM
AhnLab XTG

정보보호는 '규제 대응'이 아니라 '경영 리스크 관리' 입니다. 제2차 종합 대책은 기업 보안 수준을 사후 책임이 아닌 사전 예방 역량으로 평가하겠다는 선언입니다. 이제 기업은 ▲보안 투자 수준 증명 ▲상시 위협 대응 체계 마련 ▲거버넌스·운영·기술 통제 통합 구조로 전환해야 합니다. 안랩은 이런 정책 변화에 맞춰 기업이 실행 가능한 통합 보안 운영 모델을 단계적으로 구축할 수 있도록 지원합니다.

AhnLab

경기도 성남시 분당구 판교역로 220 (우)13493
홈페이지: www.ahnlab.com
대표전화: 031-722-8000 팩스: 031-722-8901