

보도시점 2025. 12. 6.(토) 17:00
(2025.12.8.(월) 조간)

배포 2025. 12. 6.(토) 16:00

과기정통부·개인정보위, 정보보호 및 개인 정보보호 관리체계 인증 실효성 전면 강화

- 핵심항목 중심 점검 강화, 사후관리 강화 등 제도 전면 개선
- 유출사고 발생 인증기업 대상 특별 현장점검 등 사후관리 강화

과학기술정보통신부(부총리 겸 과기정통부 장관 배경훈), 개인정보보호위원회(위원장 송경희)는 최근 정보보호관리체계 인증 및 정보보호 및 개인 정보보호 관리체계(ISMS · ISMS-P)¹⁾ 인증기업의 해킹, 대규모 개인정보 유출사고가 반복 발생함에 따라, 개인정보위 위원장 주재로 과기정통부 제2차관, 한국인터넷진흥원장 등이 참여하여 동 인증제 개선 관계부처 대책 회의를 6일 16시에 개최하고 인증 실효성 강화를 위한 제도의 전면적 개편 방안을 추진한다고 밝혔다.

※ 참석자 : 개인정보위 위원장, 과기정통부 제2차관, 한국인터넷진흥원장 등

먼저 기존 자율적으로 운영되던 ISMS-P 인증²⁾을 ①공공·민간 주요 개인정보처리시스템(주요 공공시스템, 통신사, 온라인 플랫폼 등)에 대해 의무화하여 상시적 개인정보 안전관리체계를 구축하도록 하고, ②통신사, 대규모 플랫폼 등 국민 파급력이 큰 기업에 대해 강화된 인증기준을 마련하여 적용한다. 양 기관은 이를 위한 개인정보 보호법 및 정보통신망법 개정을 조속히 추진할 예정이다.

1) (Personal Information & Information Security Management System) 주요 정보자산 유출 및 피해 예방을 위해 일정수준 이상의 기업 또는 기관이 구축·운영 중인 개인정보 및 정보보호 체계가 적합한지 인증(정보통신망법 제47조, 개인정보보호법 제32조의2에 근거)

2) ISMS : 법상 의무대상자 규정(정보통신망서비스제공자(ISP), 집적정보통신시설사업자(IDC) 등)
ISMS-P : 자율적으로 임의 신청하여 인증 취득

또한 ③심사방식을 전면 강화하여 예비심사 단계에서 핵심항목을 先검증하고, 기술심사 및 현장실증 심사를 강화하도록 개선한다. ④분야별 인증위원회 운영 및 심사원 대상 AI 등 신기술 교육을 통해 인증의 전문성을 높인다.

< 심사방식 강화방안 주요내용(안) >

구 분	기 존	개 선
인증신청	• 관리체계 운영명세서	• 관리체계 운영명세서 + <u>인증범위 자산현황 추가</u>
예비심사	• 심사팀장 1인 방문(1일)	• ① <u>핵심항목 先 검증,</u> ② <u>(ISMS(고위험, 사고기업), ISMS-P) 기술심사 방식 적용(취약점진단, 모의침투)</u>
	핵심항목 미충족 → 본심사 불가 → (최초인증) 신청 반려, (사후심사) 인증효력 취소	
본심사	• 서면위주, 샘플링 점검(5일)	• 서면점검 + ③ <u>코어시스템 중심 현장실증형 심사</u>
사후심사	• 심사팀장 1인 방문(1일)	• 심사팀장 1인 + <u>결함발생 수준별 심사인력 추가 투입</u>

아울러, ⑤사후관리를 대폭 강화한다. 인증기업의 유출사고 발생 시 적시에 특별 사후심사를 실시하여 인증기준 충족 여부를 확인할 수 있도록 하고, 사후심사 과정에서 인증기준의 중대 결함이 발견되는 경우 인증위원회 심의·의결을 거쳐 인증을 취소한다. 또한 사고기업에 대해서는 사후심사 투입 인력·기간을 2배로 확대하고, 사고원인 및 재발방지 조치를 집중 점검한다.

한편, 개인정보위는 유출사고가 발생한 인증기업에 대해 이달부터 현장 점검을 실시한다. 특히 쿠팡 등 현재 조사가 진행 중인 기업의 경우, 과기정통부 민관합동조사단·개인정보위 조사와 연계하여 인증기관³⁾ 주관으로 인증기준 적합성 등에 대해 점검한다.

3) 인증심사 및 인증서 발급 등 인증 관련 업무를 수행하는 KISA(법정 인증기관), 금융보안원(금융분야 인증·심사기관)

또한 과기정통부도 「정보보호 종합대책」(10.22., 관계부처 합동) 후속으로 통신, 온라인쇼핑몰 등 900여개 ISMS 인증기업들을 대상으로 모든 인터넷 점점에 대한 보안 취약점 점검 등 긴급 자체 점검을 실시하도록 요청하였으며, 기업들의 점검 결과에 대해 내년 초부터 현장 검증을 실시할 예정이다.

양 기관은 지난달부터 운영 중인 과기정통부·개인정보위·인증기관 합동 제도개선 TF를 통해 개선방안을 최종 확정하고, 특별 사후점검 결과 등을 반영하여 '26년도 1분기 중 관련 고시를 개정하여 단계적으로 시행할 예정이다.

담당 부서	과학기술정보통신부 사이버침해대응과	책임자	과 장	최광기	044-202-6460
		담당자	사무관	한지용	044-202-6463
담당 부서	개인정보보호위원회 자율보호정책과	책임자	과 장	윤여진	02-2100-3141
		담당자	사무관	공윤정	02-2100-3084
담당 부서	한국인터넷진흥원 보안인증단	책임자	단 장	김선미	061-820-3800
		담당자	팀 장	양선주	061-820-3810
담당 부서	금융보안원 금융보안부	책임자	부 장	이수미	02-3495-9800
		담당자	팀 장	김정덕	02-3495-9830