과학기술정보통신부
개인정보보호위원회

보도자료

보도시점 2026. 4. 10.(금) 08:00 (2026.4.10.(금) 석간) **배포** 2026.4.9.(목) 14:00

정부, 유출사고 예방 위해 인증제도 전면 개편

- 과기정통부·개인정보위 「정보보호 및 개인정보보호 관리체계 인증제 실효성 강화방안」 발표
- 서면 위주·스냅샷 방식의 한계를 벗어나 실제 운영을 추적·개선하는 체계로 전환

과학기술정보통신부(부총리 겸 과기정통부 장관 배경훈, 이하 '과기정통부')와 개인정보보호위원회(위원장 송경희, 이하 '개인정보위')는 4월 10일(금) 정부서울청사에서 열린 경제관계장관회의에서 「정보보호 및 개인정보보호 관리체계 인증제 실효성 강화방안」을 발표하였다.

정보보호 및 개인정보보호 관리체계(ISMS·ISMS-P) 인증*은 국제표준(ISO27001·27701) 기반으로 보안수준을 높이고 사고를 예방하기 위해 기업의 정보보호 및 개인정보보호 관리체계를 점검·인증하는 제도이다. ISMS·ISMS-P 인증의 긍정적 효과에도 불구하고, 최근 통신사·이커머스 해킹 등 인증기업의 연이은 사고로 인증제도의 실효성에 대한 우려가 커지는 실정이다. 이에 과기정통부·개인정보위는 관계부처 대책회의, 현장 간담회** 등을 통해 인증체계를 구조적으로 개편하기 위한 정책방안을 발굴해 왔으며, ▲인증 대상·기준, ▲심사방식, ▲사후관리, ▲심사품질확보 등 제도 전반의 개선과제를 이번 강화방안에 담았다.

* ISMS·ISMS-P(**P**ersonal Information & **I**nformation **S**ecurity **M**anagement **S**ystem): 주요 정보자산 유출 및 피해 예방을 위해 기업 또는 기관이 구축·운영 중인 개인정보 및 정보보호 체계가 적합한지 인증(정보통신망법 제47조, 개인정보보호법 제32조의2에 근거)

** 'ISMS·ISMS-P 인증제 개선 관계부처 대책회의'('25.12.6.), 'ISMS·ISMS-P 인증 취소 관계기관 대책회의'('25.12.26), 'ISMS·ISMS-P 인증제 실효성 강화를 위한 현장 간담회'('26.3.13.) 등 개최

〈 1. 인증 의무대상 확대 및 기준 강화 〉

먼저 국민 파급력이 큰 대규모 개인정보처리자에 개인정보보호 인증 의무를 부여하고, 통신사·데이터센터 등 침해사고 발생 시 국민생활에 파급력이 큰 사업자들에 대한 인증기준을 강화한다.

디지털 환경이 변화(DX·AX)하고 사이버위협이 커지는 상황에서 개인정보 관리가 중요함에도 그간 ISMS-P 취득은 기업·기관의 자율에 맡겨져 있었고, 기업 및 산업군의 사회 파급력과 무관하게 획일적인 인증기준을 적용했던 문제가 있었다.

이에 앞으로는 선제적인 예방 관리를 위하여 공공·민간의 중요 개인정보처리시스템을 중심으로 ISMS-P 인증을 의무화한다. ▲주요 공공시스템운영기관*, ▲이동통신사업자, ▲본인확인기관, ▲매출액 및 개인정보 처리규모를 고려한 대규모 개인정보처리자 등을 대상으로 의무화할 예정이며, 단계적으로 확대할 계획이다.

* 개인정보 보호법 시행령 제30조의2에 따라 개인정보의 처리 규모, 접근 권한을 부여받은 개인정보취급자의 수 등 개인정보위가 고시하는 기준에 해당하는 개인정보처리시스템

또한, 획일적인 인증체계에서 벗어나 위험 기반의 차등화된 관리체계를 구축한다. 강화인증을 신설하여 인증체계를 '강화인증', '표준인증', '간편인증' 등 3단계로 재편하고, 국민생활에 파급력이 큰 강화인증군은 기존보다 강화된 기준과 심사방식을 적용한다. 강화 인증기준은 주요 보안위협 사례와 주요국 보안 요구 사항을 참조하여 개발한다.

아울러 인증대상 서비스와 관련된 장비, 시설 등은 빠짐없이 포함되도록 인증범위를 단계적으로 확대한다. 특히, 외부 인터넷과 연결되어 공격 경로로 활용될 가능성이 있는 디지털 자산은 인증범위 내에 반드시 포함되도록 한다.

〈 2. 인증심사 방식 강화 〉

다음으로 기존 서면 중심의 심사방식을 전면 개편하여 현장중심의 심사체계를 구축하고, 미흡 기업에 대한 인증을 사전에 차단하기 위해

인증심사 절차를 개선한다.

구체적으로, 본심사 전 예비심사 단계에서 핵심적으로 확인해야 할 인증기준*을 사전에 점검하고 본심사 진행 여부를 결정하여, 부실한 관리체계를 개선한 이후에 본격적인 인증절차에 돌입할 수 있도록 한다. 또한 취약점진단·모의침투와 같은 기술심사 방식을 적용한다. 취약점 점검 전문인력이 점검도구(취약점 스캐너, 스크립트, 소스코드 진단툴 등)를 활용하여 취약점 진단과 모의침투를 수행하게 된다. 기존에 서면 확인 위주의 심사방식에서 벗어나, 심사원이 실질적 보안관리 상태를 확인할 수 있도록 실시간 시연 확인 등 현장실증 심사방법을 적용한다.

* 핵심항목(안) : ①CISO·CPO의 정보보호 정책 관리 권한 여부, ②개인정보 처리·외부 인터넷 접점 자산 식별, ③개인정보 처리시스템 비밀번호·암호화 적용, ④취약점·패치관리 등

〈 기술심사(취약점 점검) 수행 절차(안) 〉

정보자산 식별	점검범위 설정	취약점 점검	취약점 결과 검토
인증범위 내 모든 정보자산을 목록화	중요정보, 가용성 등을 고려한 범위 설정	①CVE, ②CCE, ③소스코드 점검, ④모의침투테스트	발굴된 취약점에 대해 종합적으로 검토 실시

* ①**CVE**(Common Vulnerabilities and Exposures) : 표준화된 방식으로 식별·관리되는 공개된 보안 취약점 목록을 참고하여 점검, ②**CCE**(Common Configuration Enumeration) : 비밀번호 길이/복잡성, 기본 계정 삭제 등 시스템 구성 및 설정에 대한 취약점 점검

아울러, 심사투입 인력과 기간을 확대하는 등 심사팀 구성 체계도 개편한다. 표준인증군은 인증심사원을 추가 투입해 현장실증을 강화하고, 강화인증군은 취약점점검원을 전담 투입하여 중요도가 높은 정보자산을 기술심사를 통해 정밀하게 점검하고, 점검 자산 수도 대폭 늘린다.

〈 3. 인증 사후관리 강화 〉

심사 시 특정 시점만 확인하는 '스냅샷' 방식에서 벗어나, 인증심사 이후에도 보안관리가 유지될 수 있도록 상시 점검을 강화한다. 아울러, 중대 침해사고 발생 기업에 대한 사후관리도 엄격히 실시한다.

먼저, 상시 점검체계를 확립하여 인증의 취득부터 유지·갱신에 이르는 전 과정에서 안전한 관리체계가 지속 유지되고 있는지를 중점적으로 점검한다. 이를 위해 주기별 점검양식을 표준화하고, 사후심사 시 이를 집중 점검하여 보안 수준이 유지되도록 한다.

정부와 인증기관 간 사고 이력을 상시 공유할 수 있는 체계를 구축하고, 중대 사고 발생시 기업이 사고복구 및 재발방지에 집중할 수 있도록 인증심사를 잠정 중단한다. 정부조사·처분 등이 종료된 이후 사고기업에 대한 인증심사 재개시 심사인력과 기간 투입을 확대하여 사고원인과 조치현황, 재발방지 대책 등을 철저히 심사한다.

또한, 법령에 규정된 인증취소 사유를 구체화하고 관련 법령에 따라 취소를 추진한다. 특히, 주요 사고 원인 분석 등을 토대로 인증기준 미달 여부를 판단하기 위한 중대 결함 기준을 마련하고, 중대 결함에 대한 보완을 기한 내 조치하지 않을 경우 인증취소를 진행하게 된다.

〈 4. 심사기관 및 심사원 전문성 강화 〉

부실심사를 방지하고 심사품질을 제고하기 위해 심사기관의 관리책임을 강화하고, 심사원의 전문역량 개발에 집중한다.

이를 위해, 매 인증심사 종료 후 심사기관에 대한 신뢰도 조사를 실시하고 그 결과를 차년도 인증심사 배분 시 반영하여, 심사기관이 스스로 품질을 관리하는 체계를 마련한다. 심사품질 관련 항목을 지정·재지정 평가에 반영하여 부실심사를 방지하고, 심사기관의 지정 기준 준수 여부를 매년 사후점검을 통해 철저히 확인한다.

취약점 점검 등 심사원의 기술심사 검증 능력 제고를 위해 실무교육을 강화한다. 특히 기술심사 가이드를 제공하여 현장실증형 심사 수행능력을 제고하고 심사의 일관성을 확보한다. 또한 AI·클라우드 등 전문분야별 특화 심사가 가능하도록 심사원별 전문분야 정보를 관리하여 심사에 활용한다. 심사원 인건비를 현실에 맞게 높여 심사원 처우도 개선한다.

과기정통부와 개인정보위는 이번 실효성 강화방안의 추진과제를 빈틈없이 실현하기 위하여 시행령, 고시 및 안내서 등을 개정하고 관련 예산을 확보하는 등 후속조치도 철저히 수행할 예정이다.

구체적으로, 상시 점검 강화·인증취소 등 인증 사후관리와 관련된 사항은 올해 하반기부터, ISMS-P 의무화·인증 차등 적용 및 강화 인증기준 적용 등은 '27년부터 시행될 수 있도록 상반기에 관련 작업을 추진할 계획이다.

송경희 개인정보위 위원장은 "사이버 공격이 고도화되는 상황에서 ISMS·ISMS-P 인증제를 통해 국민 피해를 사전에 예방할 수 있도록 제도 전반에 대한 근본적 개편이 필요한 시점"이라며, "오늘 발표된 실효성 강화방안을 시작으로 인증제도를 개인정보 보호의 사전예방 핵심수단으로 개선하여 국민이 안심할 수 있는 디지털 환경을 구현하겠다"라고 밝혔다.

류제명 과기정통부 제2차관은 "정보보호 관리체계 인증제도는 국민이 안심하고 디지털 서비스를 이용할 수 있도록 하는 핵심 안전장치"라며, "급변하는 사이버 보안 환경에 대응하여 정보보호 관리체계를 보다 엄격하고 내실 있게 운영하여 인증제도의 실효성을 높이고, 국민이 신뢰할 수 있는 인증체계로 발전시켜 나가겠다"고 밝혔다.

[붙임] 정보보호 및 개인정보보호 관리체계 인증제 실효성 강화방안

담당 부서	과학기술정보통신부 사이버침해대응과	책임자	과 장	백대현	044-202-6460
		담당자	사무관	사공석	044-202-6468
담당 부서	개인정보보호위원회 자율보호정책과	책임자	과 장	황지은	02-2100-3081
		담당자	사무관	배혜진	02-2100-3086
담당 부서	한국인터넷진흥원 보안인증단	책임자	단 장	김선미	061-820-3800
		담당자	팀 장	장승재	061-820-3810

내일을 만드는 과학기술
내삶을 채우는 디지털·AI
대한민국 정책브리핑
OPEN