

개인정보위·과기정통부, 정보보호 및 개인정보보호 관리체계 인증 취소 관계기관 대책회의 개최

- ‘ISMS·ISMS-P 인증제 개선 관계부처 대책회의(12.6.)’ 후속조치
- 사이버침해, 개인정보 유출사고 기업 인증취소 기준·절차 구체화 논의
- 사고 연관 핵심항목의 중대 결함 시 인증취소 엄격 적용

개인정보보호위원회(위원장 송경희, 이하 ‘개인정보위’), 과학기술정보통신부(부총리 겸 과기정통부 장관 배경훈, 이하 ‘과기정통부’)는 12월 29일 한국인터넷진흥원, 금융보안원 등 인증기관* 및 민간 전문가들로 구성된 인증위원회와 함께 ‘정보보호 및 개인정보보호 관리체계(ISMS·ISMS-P)** 인증 취소 관계기관 대책회의’를 개최했다.

* 인증심사 및 인증서 발급 등 인증 관련 업무를 수행하는 KISA(법정 인증기관), 금융 보안원(금융 분야 인증심사기관)

** ISMS-ISMS-P(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)

이번 대책회의는 지난 12월 6일 개최된 ‘정보보호 및 개인정보보호 관리체계(ISMS·ISMS-P) 인증제 개선 관계기관 대책회의’의 후속 조치이다. 최근 ISMS-P 인증기업의 사이버침해, 유출사고 빈발로 사후관리의 엄격성을 높여야 한다는 목소리를 반영하여 관계기관은 긴밀한 협력체계를 구축해 왔으며, 이번 대책회의를 통해 그간 논의해 온 인증취소 기준 구체화 방안을 최종 심의·확정하고 즉각 시행할 계획이다.

개인정보위와 과기정통부는 지난 11월부터 운영 중인 관계기관 합동 제도 개선 TF를 통해 최근 사이버침해 및 개인정보 유출사고의 주요 원인을 면밀히 분석하고 핵심항목이 되는 인증기준을 도출해 왔다. 이번 대책회의에서는 이를 취소기준에 반영하는 방안을 논의하고, 향후 인증취소를 엄격히 적용할 계획이다.

주요 논의 사항은 다음과 같다.

먼저, 그간 TF에서 논의된 외부 인터넷 접속 자산 식별, 접근권한 관리, 패치관리 등 실제 사고와 밀접하게 연관된 핵심항목을 인증기업이 연 1회 받는 사후심사에서 집중 점검한다. 사후관리를 미이행하는 등 거부하는 경우, 자료를 미제출 또는 허위제출 시 인증을 취소한다. 또한, 점검 결과 중대 결함이 발견된 경우, 인증위원회의 심의를 거쳐 인증을 취소한다.

또한 인증기업이 개인정보 보호법 위반으로 과징금 등의 처분을 받은 경우 위반행위의 중대성을 따져 인증을 취소한다. 특히 1천만명 이상의 피해 발생, 반복적 법 위반, 고의·중과실 위반행위로 사회적 영향이 큰 경우에는 원칙적으로 인증을 취소한다는 방침이다. 정보통신망법에서도 망법 등을 위반하고, 그 행위가 중대한 경우 인증취소할 수 있도록 법이 개정 중이며, 개정이 완료될 경우 관련 세부기준을 수립할 예정이다.

인증 취소 이후의 관리 방안도 마련한다. 의무대상 기업*에 대해서는 취소 이후 1년간 재신청 유예기간을 두어 실질적인 보안 개선이 이루어지도록 유도하고, 해당 기간에는 인증의무 미이행 과태료를 면제하여 기업의 불필요한 부담을 방지한다. 또한, 의무대상이 아닌 기업의 경우에도 지속적 관리체계를 구축하기 위해 인증 재취득을 권고하기로 했다.

* ISMS : 법상 의무대상자 규정(정보통신망서비스제공자(ISP), 집적정보통신시설사업자(IDC) 등)
ISMS-P : 현행 자율 인증 ⇒ 주요 공공·민간 개인정보처리자 대상 의무화 개인정보 보호법 개정안이 정무위 전체회의 통과(25.12.17.)

개인정보위 관계자는 “이번 회의는 지난 10월 범부처 정보보호 종합대책부터 이어 온 관계기관의 제도 개선 의지를 결집하는 자리”라며, “앞으로도 지속적인 협력을 통해 인증기준에 미달하거나 중대한 위반이 있는 기업은 인증을 유지할 수 없도록 엄격히 관리하여 인증제도의 신뢰성을 회복해 나가겠다”고 밝혔다.

과기정통부 관계자는 “인증 사후심사시 기준을 미달하는 등 인증받은 기업이 정보보호관리체계의 수준을 지속 유지하지 않는 경우 인증취소를 적극 실시하여 정부 인증제의 제도의 실효성을 높ی겠다.”고 밝혔다.

담당 부서	개인정보보호위원회 자율보호정책과	책임자	과 장	윤여진	02-2100-3081
		담당자	사무관	공윤정	02-2100-3084
		담당자	주무관	최화평	02-2100-3048
담당 부서	과학기술정보통신부 사이버침해대응과	책임자	과 장	최광기	044-202-6460
		담당자	사무관	한지용	044-202-6463
담당 부서	한국인터넷진흥원 보안인증단	책임자	단 장	김선미	061-820-3800
		담당자	팀 장	양선주	061-820-3810
담당 부서	금융보안원 ISMS-P인증센터	책임자	센터장	이수미	02-3495-9800
		담당자	팀 장	김정덕	02-3495-9830