SHIN&KIM
법무법인(유) 세종

정부, 유출사고 예방 위해 ISMSISMS-P 인증제도 전면 개편

2026.04.14

과학기술정보통신부(이하 '과기정통부')와 개인정보보호위원회(이하 '개인정보위')는 지난 4월 10일(금) 정부서울청사에서 열린 경제관계장관회의에서 「정보보호 및 개인정보보호 관리체계 인증제 실효성 강화방안」을 발표했습니다.

정보보호 및 개인정보보호 관리체계(ISMSISMS-P) 인증*은 국제표준(ISO2700127002)을 토대로 기업의 보안 수준을 높이고 침해사고를 사전에 예방하기 위해 정보보호 및 개인정보보호 관리체계를 점검 및 인증하는 제도입니다. ISMSISMS-P 인증의 긍정적 효과에도 불구하고, 최근 인증을 취득한 기업들에서 보안사고가 잇따르면서 제도의 실효성에 대한 의문이 커지고 있는 실정입니다. 이에 과기정통부개인정보위는 관계부처 대책회의, 현장 간담회 등을 통해 인증체계의 구조적 개편을 위한 정책방안을 적극 모색해 왔습니다. 이번 강화방안에는 ▲인증 의무대상 확대 및 기준 강화, ▲인증심사 방식 강화, ▲인증 사후관리 강화, ▲심사기관 및 심사원 전문성 강화 등 제도 전반에 걸친 개선과제를 종합적으로 담았습니다.

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

1. 인증 의무대상 확대 및 기준 강화

- **(개요)** 국민 파급력이 큰 대규모 개인정보처리자에게 개인정보보호 인증 의무를 부과하고, 통신사데이터센터 등 침해사고 발생 시 국민생활에 파급력이 큰 사업자들에 대한 인증기준을 강화함
- **(인증 의무대상 확대)** 종전에는 ISMS에 한하여 일부 기업에만 인증 의무가 부여되고 ISMS-P 취득은 기업기관의 자율에 맡겨져 왔으나, 선제적 예방 관리 강화를 위하여 공공민간의 중요 개인정보처리시스템을 중심으로 ISMS-P 인증을 의무화
- ▲주요 공공시스템운영기관, ▲본인확인기관, ▲매출액 및 개인정보 처리규모를 고려한 대규모 개인정보처리자 등을 대상으로 인증 의무를 부과하고, 향후 단계적으로 그 적용 범위를 확대할 계획
- **(인증 기준 강화)** 그간 기업 및 산업군의 사회 파급력과 무관하게 획일적인 인증기준이 적용되어 왔으나, 강화인증을 신설하여 인증체계를 '강화인증', '표준인증', '간편인증' 등 3단계로 재편하고, 국민생활에 파급력이 큰 강화인증군에 대하여는 기존보다 강화된 기준과 심사방식을 적용

2. 인증심사 방식 강화

- **(개요)** 서면 중심의 심사방식을 전면 개편하여 현장 중심의 심사체계를 구축하고, 미흡 기업에 대한 인증을 사전 차단하기 위해 인증심사 절차를 개선

- **(인증심사 절차 개선)** 본심사 전 예비심사 단계에서 핵심적으로 확인해야 할 인증기준*을 사전에 점검하고 본심사 진행 여부를 결정하여, 부실한 관리체계를 개선한 이후에 본격적인 인증절차에 돌입할 수 있도록 함

  * 핵심항목(안): ①CISOCPO의 정보보호 정책 관리 권한 여부, ②개인정보 처리외부 인터넷 접점 자산 식별, ③개인정보 처리시스템 비밀번호암호화 적용, ④취약점패치관리 등
- **(현장 중심 심사체계 구축)** 기존의 서면 확인 위주의 심사 방식에서 벗어나, 심사원이 실질적 보안관리 상태를 확인할 수 있도록 실시간 시연 확인 등 현장실증 심사방법을 적용하고, 취약점 진단모의침투와 같은 기술심사 방식을 적용

<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

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

3. 인증 사후관리 강화

- **(개요)** 심사 시 특정 시점만 확인하는 '스냅샷' 방식에서 벗어나, 인증심사 이후 상시 점검을 강화하고 중대 침해사고 발생 기업에 대한 사후관리 엄격 실시
- **(상시 점검체계 확립)** 인증의 취득부터 유지갱신에 이르는 전 과정에서 안전한 관리체계가 지속적으로 유지되고 있는지를 중점적으로 점검
- 주기별 점검양식을 표준화하고, 사후심사 시 이를 집중 점검하여 보안 수준이 유지되도록 함
- **(사후관리)** 정부와 인증기관 간 사고 이력을 상시 공유할 수 있는 체계 구축 및 사고기업에 대한 인증심사 재개 시 심사인력과 기간 투입을 확대하여 사고원인과 조치현황, 재발방지 대책 등을 철저히 심사
- **(인증취소)** 법령에 규정된 인증취소사유를 구체화하고 관련 법령에 따라 취소 진행
- 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 인증 취소 진행

4. 심사기관 및 심사원 전문성 강화

- **(심사기관 관리책임 강화)** 매 인증심사 종료 후 심사기관에 대한 신뢰도 조사를 실시하여 그 결과를 차년도 인증심사 배분 시 반영하고, 심사품질 관련 항목을 지정재지정 평가에 반영하여 부실심사를 방지
- **(심사원 실무교육 강화)** 기술심사 가이드를 제공하여 현장실증형 심사 수행능력 제고 및 심사 일관성 확보, AI클라우드 등 심사원별 전문분야 정보 관리, 심사원 인건비 등 심사원 처우 개선 등

과기정통부와 개인정보위는 이번 실효성 강화방안의 추진과제를 차질 없이 이행하기 위해, 시행령고시안내서 등 관련 법령 및 규정을 정비하고 필요 예산을 확보하는 등 후속조치를 철저히 수행해 나갈 방침입니다. 구체적으로, 상시 점검 강화 및 인증 취소 등 인증 사후관리와 관련된 사항은 올해 하반기부터, ISMS-P 인증 의무화, 인증 차등 적용 및 강화된 인증기준 적용 등은 '27년부터 시행될 수 있도록 상반기에 관련 작업을 추진할 계획이라고 밝혔습니다.

시사점

- 그간 ISMS-P 인증 취득은 기업·기관의 자율에 맡겨져 왔으나 이번 강화방안은 주요 공공시스템 운영기관·본인확인기관·대규모 개인정보처리자 등을 ISMS-P 인증 의무 취득 대상으로 편입하고, 향후 단계적으로 그 범위를 확대한다는 점에서 인증제도의 패러다임이 '자율'에서 '의무'로 전환되는 중요한 전기로 평가됩니다.
- 이번 강화방안의 또 다른 핵심은 인증기준의 차등화입니다. 종전에는 기업 규모나 산업 파급력과 무관하게 획일적인 기준이 일률적으로 적용되어 왔으나, 앞으로는 '강화·표준·간편'의 3단계 인증체계로 재편됩니다. 특히 통신사·데이터센터 등 사회적 파급력이 큰 사업자에 대해서는 보다 엄격한 기준과 심사방식이 적용될 예정인 만큼, 각 기업은 자사가 어느 인증 단계에 해당하는지를 사전에 면밀히 검토할 필요가 있습니다.
- 심사 방식 측면에서도 실질적인 변화가 예정되어 있습니다. 기존의 서류 중심 심사에서 벗어나, 예비심사 단계에서의 핵심 항목 사전 점검, 실시간 시연 확인, 취약점 진단·모의침투 테스트 등 현장 실증형 기술심사가 본격 도입됩니다. 이는 형식적 서류 준비만으로는 인증 취득이 어려워진다는 것을 의미하며, 실제 보안 관리 수준을 뒷받침할 수 있는 기술적 역량과 내부 통제 체계의 정비가 선행되어야 함을 시사합니다.
- 사후관리 측면에서도 중요한 변화가 예상됩니다. 앞으로는 인증 취득 이후에도 취득-유지-갱신 전 과정에 걸친 상시 점검이 강화되고 인증 취소가 가능해지므로, 기업·기관으로서는 인증 취득 자체보다 이를 지속적으로 유지·관리할 수 있는 역량이 더욱 중요해질 것으로 보입니다.
- 이번 개편으로 ISMS-P 인증 의무 대상에 편입되는 기업은 2027년 시행에 앞서 선제적으로 준비에 착수할 필요가 있습니다. 인증 취득은 출발점에 불과하며, 강화된 심사 방식과 상시 사후관리 요건을 고려할 때 인증 심사 대응부터 사후관리·갱신에 이르는 전 주기를 포괄하는 통합적 관리 체계의 구축이 핵심 과제가 될 것입니다. 아울러 이번 강화방안은 시행령·고시 등 관련 법령 정비와 함께 단계적으로 구체화될 예정인 만큼, 과기정통부·개인정보위 등 유관 부처의 후속 정책 동향과 법령 개정 사항을 지속적으로 모니터링하고 선제적으로 대응 전략을 수립하는 것이 중요합니다. 법무법인(유) 세종은 개인정보·사이버보안 분야에서 축적된 전문성과 실무 경험을 바탕으로, 의무 편입 여부 검토 및 현황 진단 단계부터 인증 취득·사후관리 전반은 물론 정책·법령 변화에 대한 모니터링과 맞춤형 대응 전략 수립까지 폭넓은 조력을 제공해 드릴 수 있습니다.

About Shin & Kim’s ICT Group

법무법인(유) 세종 ICT그룹은 ICT 분야의 독보적인 전문성과 인적 네트워크를 보유하고 있으며, 고객들로부터 최근 수년간 가장 높은 평가를 받고 있습니다. 방송과 통신, 개인정보, 인터넷 IT 분야에서 축적된 역량을 바탕으로 방송·통신·ICT 규제 동향 파악 및 대관, 법제개선·입법컨설팅, 규제영향력 분석과 기업의 전략 수립 등에 대한 종합적인 법률자문을 제공하고 있습니다. AI Compliance, 침해사고 대응 등과 관련하여서도 다양한 업무경험과 전문성을 보유하고 있으므로, 보다 전문적인 내용이나 궁금하신 사항이 있으면 언제든지 연락 주시기 바랍니다.

관련구성원

강신욱
대표변호사

02-316-4059
sokang@shinkim.com

최광희
고문

02-316-4651
khchoi@shinkim.com

장준영
변호사

02-316-4985
jyojang@shinkim.com

노진홍
변호사

02-316-1639
jhnoh@shinkim.com

윤호상
변호사

02-316-2584
hsyoon@shinkim.com

박지윤
변호사

02-316-2898
jypark@shinkim.com