

보도시점 2024. 7. 23.(화) 12:00
(2024. 7. 24.(수) 조간)

배포 2024. 7. 23.(화) 09:00

중소기업의 정보보호 인증부담 완화를 위한 「정보보호 및 개인정보보호관리체계 간편인증」 제도 시행

- (적용대상) △정보통신기술서비스 매출액 300억원 미만인 중소기업, △매출액 300억원 이상의 중기업 중 주요 정보통신설비 미보유 기업(웹호스팅·인터넷기반 자원공유(클라우드) 서비스 이용자)
- (인증기준) △ISMS: 80개 → 40개 또는 44개 / ISMS-P: 101개 → 62개 또는 65개
- (인증 수수료) △ISMS : 800 ~ 1,400만원 → 400 ~ 700만원 (약 50% 절감)
△ISMS-P : 1,000 ~ 1,800만원 → 600 ~ 1,100만원 (약 40% 절감)

과학기술정보통신부(장관 이종호, 이하 '과기정통부'), 개인정보보호위원회(위원장 고학수, 이하 '개인정보위') 및 한국인터넷진흥원(원장 이상중, 이하 'KISA')은 중소기업이 '정보보호 및 개인정보보호 관리체계'(이하 'ISMS 및 ISMS-P') 인증 취득 시 부담을 완화하기 위해 △인증기준, △인증비용 등을 간소화한 ISMS 및 ISMS-P 인증 특례(이하 'ISMS 및 ISMS-P 간편인증') 제도를 7월 24일(수)부터 시행한다고 밝혔다.

※ ISMS 및 ISMS-P(Personal Information Security Management System) 인증제

- (개요) 주요 정보자산 보호를 위해 기업이 구축·운영 중인 정보보호 및 개인정보보호 관리체계(예: 보안정책·인력·장비·시설 등)가 인증기준(관리적·기술적·물리적)에 적합한지를 인증(정보통신망법 제47조, 개인정보보호법 제32조의2)
- (종류) ISMS 인증을 기본으로, 개인정보보호 항목을 추가한 ISMS-P로 구분
 - ISMS 인증기준 : 80개(관리체계 수립 운영 16개 + 보호대책 요구사항 64개)
 - ISMS-P 인증기준 : 101개(ISMS 인증기준 80개 + 개인정보보호 요구사항 21개)
- (ISMS 의무대상) 주요 정보통신서비스 제공자, 집적 정보통신시설사업자, 정보통신서비스 매출액 100억원 이상의 자, 일평균 이용자수 100만명 이상의 자, 일부 상급종합병원·대학
- (인증현황) 911개 기업(의무대상 525개, 자율대상 388개) ISMS 인증 유지 중('23년말) 226개 기업(자율대상 282개) ISMS-P 인증 유지 중('23년말)

현행 ISMS 및 ISMS-P 인증제도는 중견기업 이상이 인증기준을 충족 가능하도록 설계되어, 중소기업들은 인증을 취득·유지함에 있어 많은 인증 항목과 높은 비용 등의 어려움을 호소*하여 왔다.

* 영세·중소기업 대상 평가요소, 비용 등을 경량화한 간편인증제 도입 건의(중기중앙회) 등

이에 정부는 중소기업의 규모 및 특성에 따라 **완화된 인증기준과 비용으로 인증을 취득할 수 있도록 특례제도를 도입하는 정보통신망법을 개정**(’24.1월 공포) 하고, 특례제도의 △적용대상, △인증기준, △수수료 등을 규정하기 위한 하위 법령을 정비하여 ISMS 및 ISMS-P 간편인증 도입의 제도적 기반을 마련하였다.

ISMS 및 ISMS-P 간편인증 적용대상은 △정보통신서비스 부문 매출액이 300억원 미만인 중소기업과 △정보통신서비스 부문 매출액이 300억원 이상인 중소기업 중 회사 내 주요 정보통신설비*를 보유하지 않은 기업이 신청할 수 있으며, 전체 의무대상 중 85개 기업(약 16%)이 적용받을 수 있다. 이에 관한 상세내용은 한국인터넷진흥원 누리집(<https://isms-p.kisa.or.kr>)에서 확인할 수 있다.

* 회사 내 자체서버, 네트워크 장비, 보안솔루션 등의 설비를 보유하지 않고, 웹호스팅 서비스(예: 쇼핑몰 임대 사용), 인터넷 기반 자원공유(클라우드) 서비스를 이용하는 경우

<ISMS 및 ISMS-P 간편인증 대상: ISMS 인증 의무기업 중 16%(525개 중 85개), 그외 자발적 신청기업 등>

정보통신서비스 규모	정보통신서비스 특성	간편인증 적용대상
매출액 100~300억원의 중소기업	-	74개 기업
매출액 300억원 이상의 대기업	주요 정보통신설비 미보유 기업 (웹호스팅서비스·인터넷기반 자원공유(클라우드) 서비스 이용자)	11개 기업

다만 상기 대상에 해당한다고 하더라도, 국민생활에 밀접한 영향을 미치는 △주요 정보통신서비스 제공자, △집적 정보통신시설 사업자, △일부 상급종합병원·대학교, △금융회사, △가상자산사업자는 ISMS 및 ISMS-P 간편인증 적용대상에서 제외된다.

인증기준은, 기업이 실질적인 정보보호 활동을 할 수 있도록 하는 핵심적인 필수항목은 유지*하되, 기업의 부담을 경감하기 위해 중소기업의 수준에서 불필요한 항목은 삭제 또는 완화하여 설계하였다. (⇒ 기존 인증기준 수 대비 36~40개 항목 감소)

* 사용자 식별·인증, 비밀번호 관리, 암호정책 적용, 악성코드 통제, 취약점 점검 및 조치 등

< ISMS 및 ISMS-P 간편인증 기준 >

현재 ISMS(-P)		구분	ISMS 간편인증	ISMS-P 간편인증
관리체계 수립·운영 (16개)	⇒	매출액 300억원 미만의 중소기업 인증기준 수	관리체계 수립·운영(7개)	관리체계 수립·운영(8개)
보호대책 요구사항 (64개)			보호대책 요구사항(33개)	보호대책 요구사항(33개)
			-	개인정보 요구사항(21개)
			40개	62개
개인정보 요구사항(21개) ※ ISMS-P 추가항목	⇒	매출 300억원 이상, 주요 정보통신설비 미보유 중기업 인증기준 수	관리체계 수립·운영(11개)	관리체계 수립·운영(11개)
			보호대책 요구사항(33개)	보호대책 요구사항(33개)
			-	개인정보 요구사항(21개)
인증기준 수* : 80개/101개			44개	65개

* ISMS 인증기준 : 80개(관리체계 수립 운영 16개 + 보호대책 요구사항 64개)

ISMS-P 인증기준 : 101개(ISMS 인증기준 80개 + 개인정보 요구사항 21개)

인증심사 수수료도, 인증기준 간소화에 따라 종전 대비 약 40~ 50% 수준으로 절감*된다. 또한 인증 준비에 필요한 기업의 제반 비용(예: 보안시스템 구축, 정보보호 조직 구성, 상담 등)도 감소할 것으로 기대된다.

* 인증 수수료 : (ISMS) 800~1,400만원 → 400~700만원 (약 50% 절감)

(ISMS-P) 1,000~1,800만원 → 600~1,100만원 (약 40% 절감)

한편, 한국인터넷진흥원은 새로 도입되는 ISMS 및 ISMS-P 간편인증 제도가 기업들에게 안착될 수 있도록 적용대상 기업 등을 대상으로 절차, 방법 등을 안내하는 온라인 설명회를 7월 24일에 진행할 계획이다.

※ (온라인 중계) 유튜브에서 "kisa_streaming" 검색 및 시청

과기정통부 정창립 정보네트워크정책관은 “이번 ISMS 간편인증제 시행으로, 영세한 기업들이 적은 부담으로도 사이버 위협을 선제적으로 예방·대응할 수 있게 되어 고무적”이라며, “향후에도 기업 혁신을 저해하는 불필요·불합리한 부담 경감 등 제도 개선에 더욱 힘쓰겠다”고 하였으며,

개인정보위 개인정보정책국 양청삼 국장은 “간편인증 도입을 통해 소규모 기업의 인증 취득 부담을 완화함으로써 개인정보보호 관리체계의 수준을 향상 시키고자 하는 기업의 자율적인 개인정보 보호 노력이 강화될 수 있는 계기가 되길 바란다”고 밝혔다.

담당 부서	과학기술정보통신부 사이버침해대응과	책임자	과 장	최광기 (044-202-6460)
		담당자	사무관	한지용 (044-202-6463)
	개인정보보호위원회 자율보호정책과	책임자	과 장	윤여진 (02-2100-3081)
		담당자	사무관	김현정 (02-2100-3050)
			주무관	이승연 (02-2100-3086)
	한국인터넷진흥원 ISMS팀	책임자	팀장	박창열 (061-820-1631)
		담당자	책임연구원	박영준 (02-405-5648)