



제 429회 국회 (정기회)
제16차 과학기술정보방송통신위원회

정보통신망 이용촉진 및 정보보호 등에 관한 법률 일부개정법률안

검 토 보 고

〈공공기관 정보보호 관리체계 인증 의무화〉

■ 김기현의원 대표발의(의안번호 제2212287호)

2025. 11.

과학기술정보방송통신위원회

수석전문위원 이복우

목 차

I . 제안경위	1
II . 제안이유 및 주요내용	1
III . 검토의견	3
1. 공공기관 정보보호 관리체계 인증 의무화(안 제47조 제2항 제4호 신설)	3

I. 제안경위

가. 발 의 자 : 김기현의원 등 14인

나. 발 의 일 : 2025. 8. 21.

다. 회 부 일 : 2025. 8. 22.

II. 제안이유 및 주요내용

현행법은 일정 규모 이상의 정보통신서비스 제공자에 대하여 정보 보호 관리체계(ISMS) 인증을 의무화하고 있어, 규모가 작은 공공기관은 의무 대상에서 제외되고 있음. 이로 인해 국가 주요 정보와 국민의 개인정보를 다루는 공공기관이 정보보호의 사각지대에 놓여 있음.

최근 공공기관을 대상으로 한 정보통신망 침해사고가 증가하고 있음. 공공기관이 보유한 정보는 유출 시 국민 전체에 미치는 파급효과가 크며, 디지털 전환이 가속화됨에 따라 정보통신망 침해사고의 위험이 높아지고 있어 공공기관의 정보보호 체계 강화가 시급한 실정임.

이에 「공공기관의 운영에 관한 법률」에 따른 공공기관으로서 보유한 정보의 종류, 중요도, 규모 등을 고려하여 대통령령으로 정하는 자에 대하여 정보보호 관리체계 인증을 의무화함으로써 공공부문의 정보보호 체계를 강화하고 국민의 권익을 보호하고자 함(안 제47조제2항제4호 신설).

Ⅲ. 검토의견

1. 공공기관 정보보호 관리체계 인증 의무화(안 제47조 제2항 제4호 신설)

가. 개정안 요지

- 「전기통신사업법」 제2조제8호에 따른 전기통신사업자와 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자로서 다음에 해당하는 자는 정보보호 관리체계 인증을 받아야 함(안 제47조 제2항).
 - 「공공기관의 운영에 관한 법률」 제4조에 따른 공공기관으로서 보유한 정보의 종류, 중요도, 규모 등을 고려하여 대통령령으로 정하는 자(제4호 신설)

나. 개정안 조문대비표

현 행	개 정 안
제47조(정보보호 관리체계의 인증) ① (생략)	제47조(정보보호 관리체계의 인증) ① (현행과 같음)
② 「전기통신사업법」 제2조제8호에 따른 전기통신사업자와 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자로서 다음 각 호의 어느 하나에 해당하는 자는 제1항에 따른 인증을 받아야 한다.	② ----- ----- ----- ----- ----- ----- -----.
1. ~ 3. (생략)	1. ~ 3. (현행과 같음)

현행	개정안
<신설> ③ ~ ⑫ (생략)	4. 「공공기관의 운영에 관한 법률」 제4조에 따른 공공기관으로서 보유한 정보의 종류, 중요도, 규모 등을 고려하여 대통령령으로 정하는 자 ③ ~ ⑫ (현행과 같음)

다. 검토사항

- 정보보호 관리체계(ISMS; Information Security Management System) 인증제도는 정보통신서비스 제공자가 정보통신망의 안정성·신뢰성 확보를 위하여 관리적·기술적·물리적 보호조치 등 종합적 관리체계를 수립하면 과학기술정보통신부장관이 그 적합성을 인증하여 주는 제도임.
- ISMS 인증제도는 정부가 ISMS 모델을 개발·제공함으로써 기업이 스스로 ISMS를 구축·운영할 수 있도록 하려는 취지로 2001년 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 “정보통신망법”) 개정을 통해 도입되었음.
- ISMS 인증을 받으려는 자는 관리체계 수립 및 운영에 대한 기준(16개)과 보호대책 요구사항(64개)을 충족하여야 함¹⁾.

1) ISMS 인증기준의 구체적인 내용은 참고자료 참조

○ 현행 정보통신망법 제47조제2항은 ISMS 인증을 받아야 하는 대상²⁾으로

① 기간통신사업자로서 대통령령³⁾으로 정하는 바에 따라 정보통신망서비스를 제공하는 자(이하 “주요정보통신서비스 제공자”)(제1호),

② 집적정보통신시설 사업자(제2호),

③ 전년도 매출액 또는 세입 등이 1,500억원 이상이거나 정보통신서비스 부문 전년도 매출액이 100억원 이상 또는 전년도 일일평균 이용자수 100만명 이상으로서, 대통령령으로 정하는 기준⁴⁾에 해당하는 자(제3호)를 규정함.

○ 공공기관의 경우, 제1호에 따른 주요정보통신서비스 제공자나 제2호에 따른 집적정보통신시설 사업자에 해당하는 경우는 없고 제3호에 따라 사업규모가 큰 기관은 ISMS 인증을 받아야 함.

○ 개정안은 「공공기관의 운영에 관한 법률」 제4조에 따른 공공기관 중

2) 제47조(정보보호 관리체계 인증) ② 「전기통신사업법」 제2조제8호에 따른 전기통신사업자와 전기통신사업자의 전기통신업무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자로서 다음 각 호의 어느 하나에 해당하는 자는 제1항에 따른 인증을 받아야 한다.

1. 「전기통신사업법」 제6조제1항에 따른 등록을 한 자로서 대통령령으로 정하는 바에 따라 정보통신망서비스를 제공하는 자(이하 “주요정보통신서비스 제공자”라 한다)
2. 집적정보통신시설 사업자
3. 전년도 매출액 또는 세입 등이 1,500억원 이상이거나 정보통신서비스 부문 전년도 매출액이 100억원 이상 또는 전년도 일일평균 이용자수 100만명 이상으로서, 대통령령으로 정하는 기준에 해당하는 자

3) 제49조(정보보호 관리체계 인증 대상자의 범위) ① 법 제47조제2항제1호에서 “대통령령으로 정하는 바에 따라 정보통신망서비스를 제공하는 자”란 서울특별시 및 모든 광역시에서 정보통신망서비스를 제공하는 자를 말한다.

4) 제49조(정보보호 관리체계 인증 대상자의 범위) ② 법 제47조제2항제3호에서 “대통령령으로 정하는 기준에 해당하는 자”란 다음 각 호의 어느 하나에 해당하는 자를 말한다.

1. 전년도 매출액 또는 세입이 1,500억원 이상인 자로서 다음 각 목의 어느 하나에 해당하는 자.
가. 「의료법」 제3조의4에 따른 상급종합병원
나. 직전연도 12월 31일 기준으로 재학생 수가 1만명 이상인 「고등교육법」 제2조에 따른 학교
2. 정보통신서비스 부문 전년도(법인인 경우에는 전 사업연도를 말한다) 매출액이 100억원 이상인 자. 다만, 「전자금융거래법」 제2조제3호에 따른 금융회사는 제외한다.
3. 전년도 일일평균 이용자 수가 100만명 이상인 자. 다만, 「전자금융거래법」 제2조제3호에 따른 금융회사는 제외한다.

기관이 보유한 정보의 종류 및 중요도, 기관의 규모 등 대통령령으로 정하는 요건에 해당하는 공공기관을 ISMS 인증 의무 대상에 추가하려는 것임.

- 공공기관은 민간사업자와 달리 보유하고 있는 정보의 성격과 중요성이 사업규모와 반드시 비례하지 않을 수 있으므로 ISMS 인증 의무를 적용하는 공공기관을 규정할 때에는 단순히 매출액이나 이용자 수 등과 같은 사업규모 관련 기준뿐만 아니라, 보유한 정보의 종류 및 중요도, 업무의 특성에 따른 요구되는 정보보안 수준 등과 같은 다양한 요소를 고려할 필요성이 인정됨.
- 다만, 현행 정보통신망법에 따라 ISMS 인증 및 심사 업무는 과학기술정보통신부가 직접 수행하지 않고 이를 수행할 정보보호 관리체계 인증기관과 정보보호 관리체계 심사기관을 지정하고 있는데, 민간사업자도 지정대상에 포함된다는 점에서 공공기관 정보보호 체계에 민간사업자가 접근할 수 있게 되는 문제가 발생할 수 있음.
- 따라서, 공공기관의 ISMS 인증과 관련하여서는 과학기술정보통신부장관이 직접하거나 공공기관만 인증·심사기관으로 지정받아 수행할 수 있도록 제한하는 방안을 검토할 필요가 있음.
- 과학기술정보통신부는 공공기관들의 정보보호에 관한 사항은 국정원 소관으로 ISMS 인증과 유사한 ‘사이버보안 실태평가’를 이미 받고 있으며, 인증을 의무화하기보다 공공분야에 대해 일정규모 이상의 정보보호 예산, 인력 의무화 등 제도개선을 통해 보안역량을 강화하는 것이

적절하므로 신중한 검토가 필요하다는 입장임.

- 국가정보원은 공공기관에 대해 ‘사이버보안 실태평가’를 이미 운영 중으로 ISMS 인증 의무화 시 공공기관의 부담이 가중될 우려가 있어 신중한 검토가 필요하다는 입장임.

문 의 처
02)6788-5230