



제 428회 국회 (임시회)
제2차 과학기술정보방송통신위원회

정보통신망 이용촉진 및 정보보호 등에 관한 법률 일부개정법률안

검 토 보 고

〈정보기술부문 예산 중 정보보호 예산 비율 의무화〉

■ 구자근의원 대표발의(의안번호 제2211048호)

2025. 8.

과학기술정보방송통신위원회

수석전문위원 이복우

목 차

I . 제안경위	1
II . 제안이유 및 주요내용	1
III . 검토의견	2
1. 정보기술부문 예산 중 정보보호 예산 비율 의무화(안 제45조 제5항 신설)	2

I. 제안경위

가. 발 의 자 : 구자근의원 등 10인

나. 발 의 일 : 2025. 6. 24.

다. 회 부 일 : 2025. 6. 25.

II. 제안이유 및 주요내용

현행법은 정보통신망의 안전성 확보 및 개인정보 보호를 위해 주요 정보통신서비스 제공자 등에게 정보보호 관리체계 인증을 취득하도록 의무를 부과하고 있고, 이에 대한 사후관리를 받도록 규정하고 있음.

그러나 최근 SK텔레콤에서 발생한 침해사고의 경우 SK텔레콤이 정보보호 관리체계 인증을 받았음에도 불구하고 발생한 것으로, 2024년 기준 SK텔레콤의 정보기술 투자금액 대비 정보보호 투자금액 비율은 4.1%로 케이티 6.4%, LG유플러스 6.6%에 비해 낮은 수준이었는바, 정보보호 투자금액에 대한 일정 비율 이상의 확보가 필요한 것으로 보임.

이에 주요 정보통신서비스 제공자 등에게 정보기술부문 예산에 일정 비율 이상의 정보보호 예산을 반영하도록 규정을 마련함으로써 안전한 정보통신망 환경 조성에 기여하고자 함(안 제45조제5항 신설).

Ⅲ. 검토의견

1. 정보기술부문 예산 중 정보보호 예산 비율 의무화(안 제45조 제5항 신설)

가. 개정안 요지

- 다음의 어느 하나에 해당하는 자는 정보통신망 보호를 위해 정보기술부문 예산에 대통령령으로 정하는 비율 이상의 정보보호 예산을 반영하여야 함 (안 제45조 제5항 신설).
- 「전기통신사업법」 제6조 제1항에 따른 등록을 한 자(기간통신사업자)로서 대통령령으로 정하는 바에 따라 정보통신망서비스를 제공하는 자¹⁾
- 집적정보통신시설 사업자
- 전년도 매출액 또는 세입 등이 1,500억원 이상이거나 정보통신서비스 부문 전년도 매출액이 100억원 이상 또는 전년도 일일평균 이용자수 100만명 이상으로서, 대통령령으로 정하는 기준에 해당하는 자²⁾

-
- 1) 정보통신망법 시행령 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.
- 2) 정보통신망법 시행령 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.

나. 개정안 조문대비표

현행	개정안
제45조(정보통신망의 안정성 확보 등) ① ~ ④ (생략) <u><신설></u>	제45조(정보통신망의 안정성 확보 등) ① ~ ④ (현행과 같음) <u>⑤ 제47조제2항 각 호의 어느 하나에 해당하는 자는 정보통신망 보호를 위해 정보기술부문의 예산에 대통령령으로 정하는 비율 이상의 정보보호 예산을 반영하여야 한다.</u>

다. 검토사항

- 최근 SK텔레콤 해킹 사고와 관련하여, SK텔레콤의 정보보호 투자 비중이 다른 이동통신사에 비해 낮다는 점이 침해사고의 원인 중 하나로 지적되고 있음.
- 정보보호 공시에 따르면 2024년 SK텔레콤의 정보기술부문 투자금액 대비 정보보호 투자금액 비율은 4.2%로, 케이티(6.4%)·LG유플러스(6.6%) 및 전체 정보보호 공시 기업 평균(6.2%)에 비해 낮은 수준으로 나타남³⁾.
- 정보보호 투자와 관련된 현행법상 의무를 살펴보면, 「정보보호산업의 진흥에 관한 법률」에서 사업 분야, 매출액 및 서비스 이용자 수 등을 고려하여 일정 기준에 해당하는 자에 대하여 정보보호 투자 및 인력 현황,

3) 한국인터넷진흥원 정보보호 공시 종합 포털(<https://isds.kisa.or.kr/>) - 정보보호공시현황 한국인터넷진흥원, 「2024 정보보호 공시 현황 분석」, 2024.12., p.25

정보보호 관련 인증 등 정보보호 현황을 공시하도록 하고 있을 뿐⁴⁾,

정보보호 투자 금액 또는 비율을 일정 수준 이상으로 의무화하는 규정은 없음.

- 이에 개정안은 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 “정보통신망법”) 제47조 제2항에 따른 정보보호 관리체계(ISMS)⁵⁾ 인증 의무대상자에 대하여 정보기술부문 투자금액의 일정 비율을 정보보호에 투자하도록 함으로써 기업의 침해사고 대응 역량을 제고하려는 것임.

- 현행 법령은 서비스 종류 및 규모 등이 일정 기준에 해당하는 사업자를 ISMS 인증 의무대상자로 하고 있으며⁶⁾, 2025년 5월 기준 총 553개 사(社)가 이에 해당함.

4) **제13조(정보보호 공시)** ① 정보통신망을 통하여 정보를 제공하거나 정보의 제공을 매개하는 자는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제2호에 따른 정보통신 서비스를 이용하는 자의 안전한 인터넷이용을 위하여 정보보호 투자 및 인력 현황, 정보보호 관련 인증 등 정보보호 현황을 대통령령으로 정하는 바에 따라 공개할 수 있다. (후단생략)

② 제1항에도 불구하고 정보통신서비스를 이용하는 자의 안전한 인터넷이용을 위하여 정보보호 공시를 도입할 필요성이 있는 자로서 사업 분야, 매출액 및 서비스 이용자 수 등을 고려하여 대통령령으로 정하는 기준에 해당하는 자는 제1항에 따른 정보보호 현황을 공시하여야 한다. (단서생략)

5) 정보보호 관리체계(ISMS; Information Security Management System) 인증제이란 정보통신서비스 제공자가 정보통신망의 안정성·신뢰성 확보를 위하여 관리적·기술적·물리적 보호조치 등 종합적 관리체계를 수립하면 과학기술정보통신부장관이 그 적합성을 인증하여 주는 제도임

6) **제47조(정보보호 관리체계의 인증)** 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.

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

정보통신망법 시행령 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.

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.

＜ ISMS 인증 의무대상자 ＞

구분	의무대상자 기준
정보통신망서비스 제공자(ISP)	「전기통신사업법」 제6조 제1항에 따른 등록을 한 자(기간통신사업자)로서 서울특별시 및 모든 광역시에서 정보통신망서비스를 제공하는 자
집적정보통신시설 사업자(IDC)	타인의 정보통신서비스 제공을 위하여 집적된 정보통신시설을 운영·관리하는 자
매출액 또는 이용자수 요건에 따른 대상자	정보통신서비스 부문 전년도 매출액이 100억원 이상인 자 (「전자금융거래법」 제2조 제3호에 따른 금융회사 제외)
	전년도 일일 평균 정보통신서비스 이용자 수가 100만명 이상인 자 (「전자금융거래법」 제2조 제3호에 따른 금융회사 제외)
	전년도 매출액 또는 세입이 1,500억원 이상이며 다음에 해당하는 자 - 「의료법」 제3조의4에 따른 상급종합병원 - 직전년도 12월 31일 기준으로 재학생 수가 1만명 이상인 「고등교육법」 제2조에 따른 학교

- 다만 개정안에 대해서는 다음의 사항을 고려할 필요가 있음.
- 첫째, 기업이 자신의 예산을 어떠한 영역에 투자할 것인지는 기본적으로 기업이 자율적으로 결정할 사항으로, 기업에게 특정 분야에 대한 투자 비율을 강제하는 것은 기업의 영업의 자유를 제한하는 측면이 있음.
 - 현행법은 정보보호 투자비율을 기업의 자율에 맡기는 대신 침해사고 예방 및 대응을 위한 다양한 조치의무를 두고, 이를 위반한 경우 벌칙 등 제재를 가함으로써 기업의 자유와 책임을 조화시키고 있다는 점을 고려할 필요가 있음.
 - 참고로, 사업자에게 특정 부문에 대한 투자비율을 의무화하는 입법례는

현재 에너지⁷⁾, 방송⁸⁾ 등 공공성이 강한 분야에 대해서만 예외적으로 도입되어 있음.

- 둘째, 정보기술부문 투자금액 중에는 정보보호 투자금액 외에 기업의 운영 및 성장을 위한 다양한 투자비용과 인건비 등의 고정지출도 포함되어 있음을 고려할 때,

한정된 예산의 일정 비율을 정보보호에 투자하도록 강제하는 경우 다른 정보기술 분야 투자 축소에 따른 기업의 성장 정체, 고용 감축 등의 부작용은 없는지 종합적으로 검토할 필요가 있음.

- 「정보보호 공시 가이드라인」에 따르면, ‘정보기술부문 투자액’이란 정보기술부문에 소요된 모든 비용의 합계로서, 인건비, 정보처리시스템 구입비 및 임차료, 정보처리시스템 유지보수비,

7) 「신에너지 및 재생에너지 개발·이용·보급 촉진법」 제12조의5(신·재생에너지 공급의무화 등) ① 산업통상자원부장관은 신·재생에너지의 이용·보급을 촉진하고 신·재생에너지산업의 활성화를 위하여 필요하다고 인정하면 다음 각 호의 어느 하나에 해당하는 자 중 대통령령으로 정하는 자(이하 “공급의무자”라 한다)에게 발전량의 일정량 이상을 의무적으로 신·재생에너지를 이용하여 공급하게 할 수 있다.

1. 「전기사업법」 제2조에 따른 발전사업자
2. 「집단에너지사업법」 제9조 및 제48조에 따라 「전기사업법」 제7조제1항에 따른 발전사업의 허가를 받은 것으로 보는 자
3. 공공기관

8) 「방송법」 제71조(국내 방송프로그램의 편성) ①방송사업자는 해당 채널의 전체 프로그램중 국내에서 제작된 방송프로그램을 대통령령으로 정하는 바에 따라 일정한 비율 이상 편성하여야 한다. ②방송사업자는 연간 방송되는 영화·애니메이션 및 대중음악중 국내에서 제작된 영화·애니메이션 및 대중음악을 대통령령으로 정하는 바에 따라 일정한 비율 이상 편성하여야 한다.

③ 지상파방송사업자·종합편성을 행하는 방송채널사용사업자 및 연간 전체 방송시간 중 대통령령으로 정하는 비율 이상 애니메이션을 편성하는 방송채널사용사업자는 해당 채널에서 연간 방송되는 전체 프로그램 중 국내에서 제작된 애니메이션을 시청률, 매출액 등을 고려하여 대통령령으로 정하는 바에 따라 일정한 비율 이상 신규로 편성하여야 한다. 다만, 대통령령으로 정하는 지역을 방송구역으로 하는 지상파방송사업자는 제외한다.

제72조(순수외주제작 방송프로그램의 편성) ①방송사업자는 해당 채널의 전체 방송프로그램중 국내에서 해당 방송사업자나 그 특수관계자가 아닌 자가 제작한 방송프로그램(이하 “순수외주제작 방송프로그램”이라 한다)을 대통령령으로 정하는 바에 따라 일정한 비율 이상 편성하여야 한다.

정보기술 서비스 이용료, 정보기술 외주용역비, 정보기술 교육·훈련비, 통신회선 이용료 등이 포함됨⁹⁾.

- 특히 개정안에 따른 의무대상자 중에는 이용자 수 요건에는 해당하나 매출액이 적은 영세사업자도 포함될 수 있는바, 정보보호 투자비율 의무화가 영세사업자에게 특히 과도한 부담이 될 우려는 없는지에 대해서도 검토가 필요해 보임.

- 과학기술정보통신부는 안전한 정보통신망 이용 환경을 구현하려는 취지에는 공감하나, ISMS 인증 의무대상자 중에는 재정여건 등이 열악한 중소기업, 대학 등도 다수 포함되어 예산투자 의무화는 과도한 부담을 줄 우려가 있으므로¹⁰⁾, 정보보호 공시제도 활성화 등을 통해 자율적으로 투자를 확대하도록 유도하는 것이 바람직하다는 입장임¹¹⁾.

문 의 처
02)6788-5230

9) 과학기술정보통신부·한국인터넷진흥원, 「정보보호 공시 가이드라인」, 2025.2., p.12

10) 2025년 5월 기준 의무대상자 553개 중 중소기업(156개), 대학(34개), 병원(39개)이 다수 포함

11) 금융위원회에서도 2025년 2월 「전자금융감독규정」(금융위원회고시)을 개정하여, 금융회사 등이 정보보호 예산을 정보기술부문 예산의 일정 비중 이상으로 하도록 노력하여야 한다는 규정을 폐지한 바 있음