

의안번호	2218052
의 퇴 인	이주희의원
회 답 일	2026. 6. 18.
추 계 번호	26B1907

정보통신망 이용촉진 및 정보보호 등에 관한 법률 일부개정법률안

【비용추계서】

I. 비용추계 결과

- (일부 추계) 개정안에 따라 정보보호 최고책임자를 지정·신고한 정보통신 서비스 제공자에 대하여 침해사고정보 공유체계 가입을 의무화할 경우, 추가재정소요는 2027년부터 2031년까지 5년간 총 142억원(연평균 28억 4,000만원)으로 추계됨
- 개정안의 다른 재정수반요인에 대해서는 추계가 곤란하여 일부 재정수반요인에 대해서만 추계한 결과로, 개정안의 전체적인 추가재정소요액은 추계된 금액을 상회할 수 있음

[표 1] 개정안에 따른 추가재정소요: 2027~2031년

(단위: 백만원)

구분	2027	2028	2029	2030	2031	합계	연평균
정보보호 최고책임자 지정·신고 사업자의 공유체계 가입 의무화 (안 제48조의2제11항)	5,000	2,300	2,300	2,300	2,300	14,200	2,840

주: 과학기술정보통신부의 제출자료를 참고하여 재정소요를 추계한 것으로, 실제 시스템 개선의 시기, 내용 및 비용 등에 따라 추가재정소요는 증감할 수 있음
자료: 국회예산정책처

II. 재정수반요인

연번	조·항(조제목)	주요내용	비고
1	안 제48조의2(침해사고의 대응 등)	과학기술정보통신부장관은 침해사고에 대한 효과적인 예방 및 대응을 위하여 제2항에 따른 침해사고 관련 정보를 수집·분석·공유하는 침해사고정보 공유체계(이하 “공유체계”라 한다)를 구축·운영하여야 한다.(제10항 신설)	의무규정

연번	조·항(조제목)	주요내용	비고
		정보통신서비스 제공자는 침해사고에 대한 예방 및 대응을 위하여 공유체계에 가입할 수 있다. 다만, 제45조의3 제1항 본문에 따라 정보보호 최고책임자를 지정하고 신고한 정보통신서비스 제공자는 공유체계에 가입하여야 한다.(제11항 신설)	의무·재량 규정
		과학기술정보통신부장관은 제45조의3제1항 단서에 해당하는 정보통신서비스 제공자가 공유체계에 가입하는 경우 다음 각 호의 지원을 우선적으로 할 수 있다.(제12항 신설) 1. 침해사고 대응을 위한 기술지원 2. 정보보호시스템 구축 비용지원 3. 정보보호 관련 기술개발 자금 지원 4. 정보보호 전문인력 교육훈련 지원 5. 그 밖에 대통령령으로 정하는 지원	재량규정

Ⅲ. 비용추계의 전제와 상세내역

1. 재정수반요인별 추계 여부

연번	조·항(조제목)		추계 여부	비고(추계 미 실시 사유)
1	안 제48조의2(침해사고의 대응 등)	—침해사고정보 공유 체계 구축·운영(제10항)	—	•미대상 — 과학기술정보통신부에 따르면 현재 국내 침해사고 예방 및 대응을 위하여 침해사고 관련 정보를 수집·분석·공유하는 ‘사이버위협정보 분석·공유시스템(C-TAS)’을 구축·운영하고 있음
		—정보보호 최고책임자 지정·신고 정보통신서비스 제공자의 공유체계 가입 의무화(제11항)	○	•과학기술정보통신부의 제출자료를 참고하여 추계

연번	조·항(조제목)		추계 여부	비고(추계 미 실시 사유)												
				- 제3호: 의안의 내용이 선언적·권고적인 형식으로 규정되는 등 기술적으로 추계가 어려운 경우 - 개정안에 따라 침해사고정보 공유체계에 가입하는 사업자에게 ‘침해사고 대응을 위한 기술 지원, 정보보호 시스템 구축비용 및 정보보호 관련 기술개발 자금 지원, 정보보호 전문인력 교육훈련 지원’을 할 경우, 국가의 추가재정소요가 발생할 수 있으나, 현 시점에서는 관련 사업의 내용 및 규모, 추진 방식 등에 대한 계획이 수립되지 않아 재정 소요 추계에 한계가 있음 - 참고로, 과학기술정보통신부는 침해사고 대응 기술 지원, 정보보호 기술개발, 정보보호 전문인력 양성 등의 사업을 다음과 같이 실시하고 있음 (단위: 백만원) <table><tr><th>사업</th><th>사업개요</th><th>2026</th></tr><tr><td>해킹·바이러스 대응 체계 고도화</td><td>-(사이버공격 탐지·대응체계 운영) 24시간 365일 인터넷 이용 환경 이상징후 상시모니터링·통합탐지대응 -(사이버위협 공유·협력체계 운영) 사이버 위협정보 공유 및 국내외 공동 대응 협력체계 확대 -(사이버공격 예방체계 운영) 사이버공격을 유발하는 보안 취약점을 사전 발굴·보완 등</td><td>63,252</td></tr><tr><td>정보보호 핵심원천 기술개발</td><td>국가 사이버 환경 조성 및 신규보안 위협 대응 기술개발을 위해 정보보호 원천기술 개발 지원 -데이터 및 네트워크 보호 기술, 취약점 대응 및 신산업 융합 보호기술 등 기술개발 지원</td><td>107,415</td></tr><tr><td>정보보호 전문인력 양성</td><td>산업계의 다양한 현장 수요를 반영한 다양한 정보보호 인력양성 -정보보호특성화대학, 사이버보안인력 융합보안인력·차세대보안리더 양성, 시큐리티아카데미 등 교육과정 운영</td><td>23,655</td></tr></table> 자료: 과학기술정보통신부	사업	사업개요	2026	해킹·바이러스 대응 체계 고도화	-(사이버공격 탐지·대응체계 운영) 24시간 365일 인터넷 이용 환경 이상징후 상시모니터링·통합탐지대응 -(사이버위협 공유·협력체계 운영) 사이버 위협정보 공유 및 국내외 공동 대응 협력체계 확대 -(사이버공격 예방체계 운영) 사이버공격을 유발하는 보안 취약점을 사전 발굴·보완 등	63,252	정보보호 핵심원천 기술개발	국가 사이버 환경 조성 및 신규보안 위협 대응 기술개발을 위해 정보보호 원천기술 개발 지원 -데이터 및 네트워크 보호 기술, 취약점 대응 및 신산업 융합 보호기술 등 기술개발 지원	107,415	정보보호 전문인력 양성	산업계의 다양한 현장 수요를 반영한 다양한 정보보호 인력양성 -정보보호특성화대학, 사이버보안인력 융합보안인력·차세대보안리더 양성, 시큐리티아카데미 등 교육과정 운영	23,655
사업	사업개요	2026														
해킹·바이러스 대응 체계 고도화	-(사이버공격 탐지·대응체계 운영) 24시간 365일 인터넷 이용 환경 이상징후 상시모니터링·통합탐지대응 -(사이버위협 공유·협력체계 운영) 사이버 위협정보 공유 및 국내외 공동 대응 협력체계 확대 -(사이버공격 예방체계 운영) 사이버공격을 유발하는 보안 취약점을 사전 발굴·보완 등	63,252														
정보보호 핵심원천 기술개발	국가 사이버 환경 조성 및 신규보안 위협 대응 기술개발을 위해 정보보호 원천기술 개발 지원 -데이터 및 네트워크 보호 기술, 취약점 대응 및 신산업 융합 보호기술 등 기술개발 지원	107,415														
정보보호 전문인력 양성	산업계의 다양한 현장 수요를 반영한 다양한 정보보호 인력양성 -정보보호특성화대학, 사이버보안인력 융합보안인력·차세대보안리더 양성, 시큐리티아카데미 등 교육과정 운영	23,655														
	-정보통신서비스 제공자의 공유체계 가입 지원(제 12항)	×														

2. 비용추계의 총괄적 전제

- 개정안 부칙은 공포 후 6개월이 경과한 날부터 시행하도록 규정하고 있으므로, 추계기간은 2027년부터 2031년까지 5년으로 함

3. 재정수반요인별 상세 추계내역

- 개정안은 정보통신서비스 제공자가 침해사고정보 공유체계에 가입할 수 있도록 하면서, 정보보호 최고책임자를 지정·신고¹⁾한 정보통신서비스 제공자의 경우에는 침해사고정보 공유체계에 의무적으로 가입하도록 하고 있음
 - 과학기술정보통신부는 현재 국내 침해사고 예방 및 대응을 위하여 침해사고 관련 정보를 수집·분석·공유하는 ‘사이버위협정보 분석·공유시스템(C-TAS)’을 구축·운영하고 있음

[표 2] 사이버위협정보 분석·공유시스템(C-TAS) 개요

○ (공유체계 명칭) 사이버 위협정보 분석·공유시스템(C-TAS: Cyber Threat Analysis & Sharing) ○ (목적) 기업·기관이 사이버 위협에 적시 대응할 수 있도록 실시간 상황전파 및 사이버 위협정보 공유 ○ (운용방식 및 기능) 홈페이지, API 등 온라인으로 위협정보*를 공유하여 기업 등에서 실시간으로 공격 차단에 활용 *악성코드 Hash, 공격시도 IP, 악성코드 경유지 및 유포지 IP 등 공격에 활용된 위협정보 ○ (구축 시기) 2013년 구축, 2014년부터 서비스 운영 중 ○ (가입 사업자 현황) 국내 기업·기관 5,561개사 참여 중('26.5월 기준) ○ (예산 현황)		
		(단위: 백만원)
사업명	사업 내용	예산('26)
해킹·바이러스 대응 체계 고도화 (사이버위협 공유협력체계 운영)	C-TAS 시스템 운영 및 C-TAS 시스템 기능 개선 등	1,400

자료: 과학기술정보통신부

1) 제45조의3(정보보호 최고책임자의 지정 등) ① 정보통신서비스 제공자는 정보통신시스템 등에 대한 보안 및 정보의 안전한 관리를 위하여 대통령령으로 정하는 기준에 해당하는 임직원을 정보보호 최고책임자로 지정하고 과학기술정보통신부장관에게 신고하여야 한다. 다만, 자산총액, 매출액 등이 대통령령으로 정하는 기준에 해당하는 정보통신서비스 제공자의 경우에는 정보보호 최고책임자를 신고하지 아니할 수 있다.

- 개정안에 따라 정보보호 최고책임자를 지정·신고한 정보통신서비스 제공자에 대하여 침해사고정보 공유체계 가입을 의무화할 경우, 가입자 확대에 따른 C-TAS 시스템 개선 등의 추가재정소요가 발생할 것으로 예상됨
- 과학기술정보통신부는 개정안 통과 시 C-TAS 가입자 확대가 예상되므로 시스템 개선(인프라 증설, 운영비용 확대 등)이 필요하다는 의견임
 - '26.5월 기준 C-TAS 가입 사업자는 5,561개사이며, 정보보호 최고책임자 지정·신고 사업자는 약 28,000개사로 가입 대상자가 약 5배 증가할 것으로 예상됨
- 개정안에 따른 시스템 개선 비용은 과학기술정보통신부가 제출한 'C-TAS 시스템 개선 계획(안)'에 따라 '운영 인프라 증설, 인텔리전스 서비스 구매, 시스템 운영비용 증가, 가입 홍보 사업'의 비용을 추계함

[표 3] 과학기술정보통신부의 C-TAS 시스템 개선 계획(안)

(단위: 백만원)

구 분	연도별 구축비				
	1차년	2차년	3차년	4차년	5차년
운영 인프라 증설	3,000	300	300	300	300
	•서버(3.7Ghz CPU 16Core 급) 12식×75백만원 •스토리지(400TB급) 10식×50백만원 •네트워크(10Gbps) 2식×50백만원 •GPU(엔비디아 DGX B300 이상) 1,200백만원(1식) •전용회선 2회선×150백만원	•전용회선 2회선×150백만원(연간)			
인텔리전스 서비스 구매	1,500	1,500	1,500	1,500	1,500
	•국내·외 위협 인텔리전스 라이선스 1,000백만원×1년 *국내·외 위협 인텔리전스 라이선스 3종 •공격표면관리(ASM) 라이선스 500백만원×1년 *공격표면관리(ASM) 라이선스 비용				
시스템 운영비용 증가	300	300	300	300	300
	•증설 인프라에 따른 시스템 운영 및 유지보수 비용(증설 인프라의 약 10%요율 적용)				
가입 홍보 등	200	200	200	200	200
	•C-TAS 가입 및 이용 활성화를 위한 홍보 사업(가입 안내 홍보, 컨퍼런스 행사 홍보부스 운영, C-TAS 소개 발표 등): 200백만원				
합 계	5,000	2,300	2,300	2,300	2,300

주: 소요비용의 단가는 현행 시스템 구축 비용 및 조달청 나라장터 종합쇼핑몰 등을 참고하여 산정
자료: 과학기술정보통신부, 한국인터넷진흥원

- (추계 결과) 개정안에 따라 정보보호 최고책임자를 지정·신고한 정보통신 서비스 제공자에 대하여 침해사고정보 공유체계 가입을 의무화할 경우, 추가재정소요는 2027년부터 2031년까지 5년간 총 142억원(연평균 28억 4,000만원)으로 추계됨

[표 4] 개정안에 따른 추가재정소요: 2027~2031년

(단위: 백만원)

구분	2027	2028	2029	2030	2031	합계	연평균
운영 인프라 증설	3,000	300	300	300	300	—	—
인텔리전스 서비스 구매	1,500	1,500	1,500	1,500	1,500	—	—
시스템 운영비용 증가	300	300	300	300	300	—	—
가입 홍보 등	200	200	200	200	200	—	—
합 계	5,000	2,300	2,300	2,300	2,300	14,200	2,840

주: 과학기술정보통신부의 제출자료를 참고하여 재정소요를 추계한 것으로, 실제 시스템 개선의 시기, 내용 및 비용 등에 따라 추가재정소요는 증감할 수 있음

자료: 국회예산정책처

IV. 부대의견

- 개정안의 다른 재정수반요인에 대해서는 추계가 곤란하여 일부 재정수반요인에 대해서만 추계한 결과로, 개정안의 전체적인 추가재정소요액은 추계된 금액을 상회할 수 있음
- 과학기술정보통신부의 제출자료를 참고하여 재정소요를 추계한 것으로, 실제 시스템 개선의 시기, 내용 및 비용 등에 따라 추가재정소요는 증감할 수 있음

V. 작성자

□ 성명

국회예산정책처	분석관	과장
경제비용추계과	최동완	예승우

□ 대표연락처

성명	전화번호	이메일 주소
최동완	02-6788-3746	dongwaniii@nabo.go.kr