



제 439회 국회 (정기회)
제1차 과학기술정보방송통신위원회

정보통신망 이용촉진 및 정보보호 등에 관한 법률 일부개정법률안

검 토 보 고

〈침해사고정보 공유체계 구축·운영근거 마련 등〉
■ 이주희의원 대표발의(의안번호 제2218052호)

2026. 9.

과학기술정보방송통신위원회

수석전문위원 이지민

목 차

I. 제안경위	1
II. 제안이유 및 주요내용	1
III. 검토의견	2
1. 침해사고정보 공유체계 구축·운영근거 마련 등	2

I. 제안경위

가. 제 안 자 : 이주희의원 등 12인

나. 제 안 일 : 2026. 4. 2.

다. 회 부 일 : 2026. 4. 3.

II. 제안이유 및 주요내용

현행법은 정보통신시스템 등에 대한 보안 및 정보의 안전한 관리를 위하여 일정한 기준에 해당하는 정보통신서비스 제공자로 하여금 정보보호 최고책임자를 지정하도록 규정하고 있음.

그런데 최근 해킹 등 침해사고로 인한 개인정보 유출 사건이 빈번하게 발생하고 있으며 이에 대응하기 위하여 침해사고 관련 정보에 대한 기업과 정부 간의 정보 공유뿐만 아니라 기업 간 공유의 필요성이 지속적으로 제기되고 있음.

이에 침해사고정보 공유체계를 법률에 명시하고 정보보호 최고책임자를 지정하여 신고한 정보통신서비스 제공자는 해당 침해사고정보 공유체계에 의무적으로 가입하도록 하며 정보보호 최고책임자를 지정하지 아니한 정보통신서비스 제공자에 대하여도 자발적인 가입을 유도함으로써 정보통신망의 안전성과 신뢰성을 제고하려는 것임(안 제48조의2제10항부터 제13항까지 신설).

Ⅲ. 검토의견

1. 침해사고정보 공유체계 구축·운영 근거 마련 등

가. 개정안의 내용

- 과학기술정보통신부장관(이하 “과기부장관”)으로 하여금 침해사고에 대한 효과적인 예방 및 대응을 위하여 침해사고 관련 정보를 수집·분석·공유하는 침해사고정보 공유체계를 구축·운영하도록 함(안 제48조의2 제10항부터 제13항까지 신설).
- 정보보호 최고책임자를 지정하고 신고한 정보통신서비스 제공자는 공유체계에 의무적으로 가입하도록 함.
- 의무가입 대상자가 아닌 정보통신서비스 제공자가 공유체계에 가입하는 경우 기술적·재정적 지원 등을 할 수 있도록 함.

현 행	개 정 안
법률 제21500호 정보통신망 이용 촉진 및 정보보호 등에 관한 법률 일부개정법률 제48조의2(침해사고의 대응 등) ① ~ ⑨ (생략) <u><신설></u>	법률 제21500호 정보통신망 이용 촉진 및 정보보호 등에 관한 법률 일부개정법률 제48조의2(침해사고의 대응 등) ① ~ ⑨ (현행과 같음) <u>⑩ 과학기술정보통신부장관은 침해사고에 대한 효과적인 예방 및 대응을 위하여 제2항에</u>

현행	개정안
<u><신설></u>	4. 정보보호 전문인력 교육훈련 지원 5. 그 밖에 대통령령으로 정하는 지원 ⑬ 제10항에 따른 공유체계의 구축·운영, 제11항에 따른 공유체계 가입 및 제12항에 따른 지원에 관한 구체적인 내용, 방법 및 절차 등에 필요한 사항은 대통령령으로 정한다.
※ 부칙 이 법은 공포 후 6개월이 경과한 날부터 시행한다.	

나. 검토의견

- 최근 통신·금융·유통 등 국민생활과 밀접한 분야의 대규모 사업자를 대상으로 한 해킹 등 침해사고가 잇따라 발생하면서 침해사고 신고 건수는 2024년 1,887건에서 2025년 2,383건으로 전년 대비 26.3% 증가하는 등 개인정보 유출에 따른 피해발생과 함께, 정보통신 서비스의 안정성과 기업의 침해사고 대응체계에 대한 우려가 커지고 있음.

<유형별 침해사고 신고 현황>

(단위 : 건)

구분 연도		2023년			2024년			2025년		
		상반기	하반기	합계	상반기	하반기	합계	상반기	하반기	합계
침해 사고 신고	DDoS	124	89	213	153	132	285	238	350	588
	악성코드	156	144	300	106	123	229	115	239	354
	(랜섬웨어)	(134)	(124)	(258)	(92)	(103)	(195)	(82)	(192)	(274)
	서버해킹	320	263	583	504	553	1,057	531	522	1,053
	기타	64	117	181	136	180	316	150	238	388
합계		664	613	1,277	899	988	1,887	1,034	1,349	2,383

자료: 「25년 사이버 위협 하반기 동향 및 26년 전망」, 과학기술정보통신부·한국인터넷진흥원, 2026.1.

- 현행법은 주요정보통신서비스 제공자, 집적정보통신시설 사업자 및 대통령령으로 정하는 정보통신망 운영자에게 침해사고 유형별 통계, 접속경로별 이용 통계 등 침해사고 관련 정보를 과기부 장관 또는 한국인터넷진흥원에 제공하도록 하고, 한국인터넷진흥원은 이를 분석하여 과기부 장관에게 보고하도록 하고 있음¹⁾.
- 이를 근거로 한국인터넷진흥원은 여러 산업 분야에 걸쳐 광범위하게 발생하고 있는 침해사고에 대응하기 위해 2014년부터 C-TAS(Cyber Threat Analysis & Sharing, 사이버 위협정보 분석·공유 시스템)를 운영하고 있으며, 보안기업, 금융, 전자상거래 호스팅 등 다양한 분야의 기업이 참여하여 사이버 위협 및 보안 정보를 공유·전파하고 있음.

1) 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」

제48조의2(침해사고의 대응 등) ② 다음 각 호의 어느 하나에 해당하는 자는 대통령령으로 정하는 바에 따라 침해사고의 유형별 통계, 해당 정보통신망의 소통량 통계 및 접속경로별 이용 통계 등 침해사고 관련 정보를 과학기술정보통신부장관이나 한국인터넷진흥원에 제공하여야 한다.

1. 주요정보통신서비스 제공자
2. 집적정보통신시설 사업자
3. 그 밖에 정보통신망을 운영하는 자로서 대통령령으로 정하는 자

③ 한국인터넷진흥원은 제2항에 따른 정보를 분석하여 과학기술정보통신부장관에게 보고하여야 한다.

<C-TAS(사이버 위협정보 분석·공유시스템) 제도>

○ C-TAS 제도

- 여러 산업 분야에 걸쳐 광범위하게 발생하고 있는 침해사고에 대응하기 위해 2014년부터 운영하고 있는 시스템으로 보안기업, 금융, 전자상거래, 호스팅 등 다양한 분야의 기업이 참여하여 위협정보를 공유
- ※ 운영 근거 : 「정보통신망법」 제48조의2 제1항 제1호

○ 운영 방식

- 공유형 C-TAS : 양방향 상호 교환 방식으로 위협정보를 수집·공유
 - 회원사와 KISA 간 시스템 연동으로 위협IP, 악성코드 등 탐지 및 차단에 필요한 위협정보 실시간 자동 공유 운영('14.8월~)
- 개방형 C-TAS : 중소기업 등 모든 기업에서 위협정보를 제공받을 수 있는 홈페이지
 - 중소·영세기업 등 정보공유를 원하는 모든 기업에게 위협정보를 제공하는 홈페이지(PC/모바일) 운영('22.1월~)

자료: KISA 보호나라&KrCERT/CC, [정보보호서비스-주요사업소개-(C-TAS)]

- 한국인터넷진흥원 자료에 따르면 C-TAS는 2026년 7월 현재 약 5,700여 사를 대상으로 (누적)15억 건 규모의 위협정보를 공유하고 있는 것으로 나타나고 있으며, 시스템을 통한 사이버 위협에 대한 예방정보 공유건수는 2021년 약 6,097만 건에서 2025년 약 3억 5,187만 건으로 약 5.8배 증가한 것으로 나타나고 있음.

<최근 5년 연도별 C-TAS 사이버 위협 예방정보 공유건수>

(단위 : 건)

구분	2021년	2022년	2023년	2024년	2025년
예방정보 공유건수	60,969,451	96,193,927	153,494,722	247,860,831	351,867,410

자료: KISA 보호나라&KrCERT/CC, (정보보호서비스-주요사업소개-(C-TAS))

- 개정안은 이러한 침해사고와 관련한 정보 공유체계의 구축·운영 근거를 법률에 과기부장관의 업무로 명시함과 동시에, 사업자의 가입의무를 규정하여 제도의 안정성과 지속성을 확보하려는 것으로, 이를 통해 유사 사고의 확산을 방지하고 침해사고 초기 대응을 지원할 수 있다는 점에서 입법 취지는 타당한 것으로 보임.
- 다만, 개정안과 관련하여 다음의 사항을 고려할 필요가 있음.
- 첫째, 의무가입 대상자 기준을 정보보호 최고책임자(CISO)²⁾ 신고 여부로 정하는 것이 적절한지에 대한 검토가 필요함.
 - 정보보호 최고책임자 지정 제도는 현행법 제45조의3에 따라 민간 기업의 정보보호 투자확대 및 보안 역량 강화를 위하여 기업 내부의 정보보호 책임체계를 확보하기 위한 제도로, 그 신고의무자를 비교적 넓게 규정하여 자본금 1억원 이하 기업과 소기업 등만 제외되고 있으므로, 개정안의 침해사고 정보 공유 체계 가입 대상은 침해사고 발생 시 사회적 파급효과와 이용자 수, 정보처리 규모, 정보통신망의 중요성 등을 기준으로 정하는 것이 제도의 목적에 보다 부합할 것으로 보임.
 - 또한, 현행법은 정보보호 최고책임자 신고 의무를 규정하면서 신고 면제 대상 등 의무가입 대상의 범위에 영향을 미치는 사항이

2) 정보보호 최고책임자(CISO, Chief Information Security Officer)

- : 기업의 정보통신시스템 등에 대한 보안 및 정보의 안전한 관리 등 정보보호 업무를 총괄하는 최고책임자
- 정보보호 최고책임자는 정보통신망법 제45조의3제4항 각호에 따른 정보보호 관련 업무에 대한 최종 결정권 및 책임, 정보보호 업무 관련 예산·인사에 대한 직접적 권한을 가짐
[정보보호 최고책임자 지정·신고제도 안내서, 한국인터넷진흥원, 2024.9.]

하위법령에 위임³⁾되어 있는데, 개정안과 같이 공유체계 의무 가입자의 범위를 신고의무자와 연동하는 경우 공유체계 의무 가입자의 범위가 정보보호 최고책임자 지정 기준과 관련한 하위 법령이 변경될 경우 함께 달라지는 문제가 발생할 수 있으므로 이에 대한 명확한 기준을 설정할 필요가 있어 보임.

<정보보호 최고책임자(CISO) 지정·신고 기업 수>

(단위 : 건)

신고연도	~2020	2021	2022	2023	2024	2025	2026	합계
업체수	18,191	835	696	590	4,940	1,800	967	28,019

자료: 공공데이터포털, 정보보호 최고책임자 신고 업체현황(의무·자율신고 대상 기업 포함), 2026.4.

- 둘째, 개정안은 정보보호 최고책임자를 지정·신고한 사업자에게 공유체계 가입을 의무화하고 있음에도, 공유체계 가입으로 인해 사업자에게 부과되는 의무의 내용과 범위에 대해서는 별도로 규정하고 있지 않음.
- 가입 이후 사업자에게 추가적인 의무가 부여되지 않고 단순한 등록 절차에 그친다면 형식적 가입에 그쳐 제도의 실효성을 확보하기 어려울 수 있음. 반면, 가입자에게 실시간 정보제출, 시스템 연계 및 대응조치 의무까지 부과하는 경우에는 기업의 권리·의무에 직접적인 영향을 미칠 수 있으므로 핵심 사항은 대통령령에 포괄적

3) 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」

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, 자산 총액, 매출액 등이 대통령령으로 정하는 기준에 해당하는 정보통신서비스 제공자의 경우에는 정보보호 최고책임자를 신고하지 아니할 수 있다. (이하 생략)

으로 위임하기보다는 법률에 규정할 필요가 있어 보임.

- 또한, 의무가입 대상자가 가입하지 않은 경우의 의무이행 확보 수단에 관한 사항도 규정되어 있지 않으므로, 관련 내용을 명확히 규정하여 제도의 실효성을 확보할 필요가 있음.

- 셋째, 개정안 제48조의2제10항은 ‘제2항에 따른 침해사고 관련 정보를 공유체계를 통해 공유’하도록 규정하고 있으나, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률 일부개정법률」(법률 제21500호) 제48조의2제5항은 ‘제2항에 따라 제공받은 정보를 목적 범위를 벗어나 제3자에게 제공하거나 일반에게 공개하여서는 아니 된다’라고 명시하고 있어, 양 규정 간 법적 정합성 문제가 발생할 소지가 있음.⁴⁾.

- 공유체계 가입 사업자에게 제2항에 따른 침해사고 관련 정보를 제공하는 것이 개정법 제5항에서 규정한 제3자 제공에 해당한다면, 개정안 제10항과 개정법 제5항 사이에 해석상 충돌이 발생할 수 있으므로, 공유체계를 통한 정보공유에 대한 예외 규정을 두거나 제공 범위·목적·대상 등을 법률에 명확히 규정하는 것이 필요해 보임.

4) 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 [시행 2026. 10. 1.][법률 제21500호, 2026. 3. 31., 일부개정 제48조의2(침해사고의 대응 등) ⑤ 과학기술정보통신부장관이나 한국인터넷진흥원은 제2항에 따라 제공받은 정보를 침해사고의 대응을 위하여 필요한 범위에서만 정당하게 사용하여야 하며, 그 목적 범위를 벗어나 제3자에게 제공하거나 일반에게 공개하여서는 아니 된다.

다. 정부 및 관련 단체 의견

1) 과학기술정보통신부

- 침해사고 예방 및 대응을 위해 정보공유 체계 구축·운영이 필요하다는 법안 취지에는 공감하나, 침해사고 정보공유 체계의 실효성 제고를 위해 자발적인 참여 기반 조성이 필요하다는 점과 공유체계 가입 의무화에 따른 기업 부담 가중이 우려된다는 점 등을 고려하여 신중하게 접근할 필요가 있음.

2) 국가정보원

- 모든 중앙행정기관·공공기관·지방자치단체는 「사이버안보 업무 규정」 제14조에 따라 정보공유 기능을 포함한 실시간 탐지체계(통합보안관제체계)에 의무적으로 연계되어 있으므로, 정보 공유 체계 가입의무 대상에서 ‘공공기관등’을 제외할 필요가 있음.
- 동일 취지로 현행법 제48조의4제2항 또한 침해사고 발생 시 과기부장관이 해당 정보통신서비스 제공자에게 필요한 조치를 명할 수 있도록 하면서, ‘공공기관등’을 그 대상에서 제외하고 있음⁵⁾.

5) 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」

제48조의4(침해사고의 원인 분석 등) ② 과학기술정보통신부장관은 정보통신서비스 제공자의 정보통신망에 침해사고가 발생하면 그 침해사고의 원인을 분석하고 피해 확산 방지, 사고대응, 복구 및 재발 방지를 위한 대책을 마련하여 해당 정보통신서비스 제공자(공공기관등은 제외한다)에게 필요한 조치를 이행하도록 명령할 수 있다.

3) 한국인터넷기업협회

- 침해사고정보 공유체계 공유 대상 정보의 내용 및 범위, 주기, 공유정보에 대한 접근 권한 보유자의 범위 등 핵심적인 사항은 법률에서 구체적으로 규정할 필요가 있음.

문 의 처

02)6788-5235
