



제 439회 국회 (정기회)
제1차 과학기술정보방송통신위원회

정보통신망 이용촉진 및 정보보호 등에 관한 법률 일부개정법률안

검 토 보 고

〈공공기관 ISMS인증 의무화, 정보보호 취약점 신고포상금 상향 등〉
■ 박상혁의원 대표발의(의안번호 제2219917호)

2026. 9.

과학기술정보방송통신위원회

수석전문위원 이지민

목 차

I . 제안경위	1
II . 제안이유 및 주요내용	1
III . 검토의견	3
1. 공공기관에 대한 정보보호 관리체계 인증 의무화	3
2. 정보보호 취약점 신고포상금 상향	10
3. 정보통신서비스 제공자 등에 대한 자료보전의무 신설	16

I. 제안경위

가. 제 안 자 : 박상혁의원 등 15인

나. 제 안 일 : 2026. 7. 13.

다. 회 부 일 : 2026. 7. 14.

II. 제안이유 및 주요내용

현행법은 정보통신망의 안정성 확보를 위해 정보보호 취약점 신고 포상제, 정보보호 관리체계 인증, 침해사고 원인 분석 등에 관한 사항을 규정하고 있음.

최근들어 사이버상의 정보 침해사고가 빈번하게 발생하는 상황에서, 사고 이전 예방 체계 구축과 사후 대응 체계 정비 필요성이 대두되고 있음.

그러나 현행법 상 정보보호 취약점 신고 포상제의 포상 수준은 5만원 이상 1천만원 이하로, 취약점을 적극적으로 발굴하고 신고하기에 충분하지 않다는 의견이 있음. 또한, 최근 ISMS 제도 정비 및 강화를 내용으로 하는 정보통신망법 개정안이 발의된 바 있으나 정작 정보침해의 주요 대상이 되고 있는 공공기관은 ISMS 인증 대상에 포함되지 않아 제도의 실효성에 의문이 제기되고 있음.

이에 취약점 신고 포상제의 포상 기준 상한을 확대하고, ISMS 인증 대상에 공공기관도 포함하여 보안인증 제도의 실효성을 높이하고자 함. 뿐만 아니라, 침해사고 발생 시 원인 분석을 위한 자료 보존 의무를

강화하여 책임 귀속 주체를 명확히 하고, 사고의 재발 방지에 이바지하고자 함(안 제47조제2항, 제47조의6제1항 및 제48조의4제5항·제7항 등).

Ⅲ. 검토의견

1. 공공기관에 대한 정보보호 관리체계 인증 의무화

가. 개정안의 내용

- 정보보호 관리체계 인증 의무대상자에 「공공기관의 운영에 관한 법률」 제4조에 따른 공공기관으로서 정보통신망의 규모, 종류 등을 고려하여 대통령령으로 정하는 자를 추가함(안 제47조제2항제4호 신설).

현행	개정안
제47조(정보보호 관리체계의 인증) ① (생략)	제47조(정보보호 관리체계의 인증) ① (현행과 같음)
② 「전기통신사업법」 제2조 제8호에 따른 전기통신사업자와 전기통신사업자의 전기통신 역무를 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)
<u><신설></u>	4. 「공공기관의 운영에 관한 법률」 제4조에 따른 공공기관으로서 정보통신망의 규모, 종류 등을 고려하여 대통령령

현행	개정안
③ ~ ⑫ (생략)	으로 정하는 자 ③ ~ ⑫ (현행과 같음)
※ 부칙 이 법은 공포 후 6개월이 경과한 날부터 시행한다.	

나. 검토의견

- 정보보호 관리체계(ISMS; Information Security Management System) 인증제도는 정보통신망의 안정성·신뢰성 확보를 위하여 관리적·기술적·물리적 보호조치 등 종합적 관리체계를 수립·운영하는 자에 대하여 과학기술정보통신부장관(이하 “과기부장관”)이 고시한 기준에 따라 그 적합성을 인증하여 주는 제도임.
- ISMS 인증제도는 정부가 ISMS 모델을 개발·제공하고 기업이 스스로 ISMS를 구축·운영할 수 있도록 하며 기준에 적합한 경우 인증을 부여하여 기업 차원의 정보보호 환경 조성을 촉진하려는 취지로 2001년 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 개정을 통해 도입되었음.
- ISMS 인증을 받으려는 자는 관리체계 수립 및 운영에 대한 기준(16개)과 보호대책 요구사항(64개)을 충족하여야 함.
- 현행법 제47조제2항은 ISMS 인증을 받아야 하는 대상¹⁾으로

1) 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」

제47조(정보보호 관리체계의 인증) ① 과학기술정보통신부장관은 정보통신망의 안정성·신뢰

- ① 기간통신사업자로서 대통령령²⁾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 일일 평균 이용자수 100만명 이상으로서, 대통령령으로 정하는 기준³⁾에 해당하는 자(제3호)를 규정하고 있음.

성 확보를 위하여 관리적·기술적·물리적 보호조치를 포함한 종합적 관리체계(이하 "정보보호 관리체계"라 한다)를 수립·운영하고 있는 자에 대하여 제4항에 따른 기준에 적합한지에 관하여 인증을 할 수 있다.

② 「전기통신사업법」 제2조제8호에 따른 전기통신사업자와 전기통신사업자의 전기통신영무를 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

2) 「정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령」

제49조(정보보호 관리체계 인증 대상자의 범위) ① 법 제47조제2항제1호에서 "대통령령으로 정하는 바에 따라 정보통신망서비스를 제공하는 자"란 다음 각 호의 어느 하나에 해당하는 자를 말한다.

1. 「전기통신사업법」 제2조제3호에 따른 전기통신회선설비를 설치·보유하고 서울특별시 및 모든 광역시에서 정보통신망서비스를 제공하는 자
2. 「전기통신사업법」 제38조제1항에 따라 기간통신사업자로부터 이동통신서비스를 제공받아 재판매하는 전기통신사업자

3) 「정보통신망 이용촉진 및 정보보호 등에 관한 법률 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. 「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.

- 「공공기관의 운영에 관한 법률」 제4조에 따른 공공기관⁴⁾의 경우 현재 제3호의 사업규모 및 정보통신서비스 규모 기준에 따라 해당 기준을 충족하는 경우 ISMS 인증 의무대상으로 분류되고 있으며, 2026년 8월 기준 정보보호 관리체계 인증을 취득한 공공기관은 의무 대상 기관 21곳(병원 12곳 포함), 의무대상이 아닌 기관 24곳 등 총 45곳임.

4) 「공공기관의 운영에 관한 법률」 제4조(공공기관) ① 재정경제부장관은 국가·지방자치단체가 아닌 법인·단체 또는 기관(이하 “기관”이라 한다)으로서 다음 각 호의 어느 하나에 해당하는 기관을 공공기관으로 지정할 수 있다.

1. 다른 법률에 따라 직접 설립되고 정부가 출연한 기관
2. 정부지원액(법령에 따라 직접 정부의 업무를 위탁받거나 독점적 사업권을 부여받은 기관의 경우에는 그 위탁업무나 독점적 사업으로 인한 수입액을 포함한다. 이하 같다)이 총수입액의 2분의 1을 초과하는 기관
3. 정부가 100분의 50 이상의 지분을 가지고 있거나 100분의 30 이상의 지분을 가지고 임원 임명권한 행사 등을 통하여 해당기관의 정책 결정에 사실상 지배력을 확보하고 있는 기관
4. 정부와 제1호부터 제3호까지의 어느 하나에 해당하는 기관이 합하여 100분의 50 이상의 지분을 가지고 있거나 100분의 30 이상의 지분을 가지고 임원 임명권한 행사 등을 통하여 해당기관의 정책 결정에 사실상 지배력을 확보하고 있는 기관
5. 제1호부터 제4호까지의 어느 하나에 해당하는 기관이 단독으로 또는 두개 이상의 기관이 합하여 100분의 50 이상의 지분을 가지고 있거나 100분의 30 이상의 지분을 가지고 임원 임명권한 행사 등을 통하여 해당기관의 정책 결정에 사실상 지배력을 확보하고 있는 기관
6. 제1호부터 제4호까지의 어느 하나에 해당하는 기관이 설립하고, 정부 또는 설립 기관이 출연한 기관

② 제1항에도 불구하고 재정경제부장관은 다음 각 호의 어느 하나에 해당하는 기관을 공공기관으로 지정할 수 없다.

1. 구성원 상호 간의 상호부조·복리증진·권익향상 또는 영업질서 유지 등을 목적으로 설립된 기관
2. 지방자치단체가 설립하고, 그 운영에 관여하는 기관
3. 「방송법」에 따른 한국방송공사와 「한국교육방송공사법」에 따른 한국교육방송공사

<ISMS 인증 취득 공공기관 현황>

[ISMS 인증 의무대상으로서 인증 취득 공공기관 현황]

연번	기관명	연번	기관명	연번	기관명
1	칠곡경북대학교병원	8	양산부산대학교병원	15	한국마사회
2	분당서울대학교병원	9	경상국립대학교병원	16	공영홈쇼핑
3	부산대학교병원	10	서울대학교병원	17	한국조폐공사
4	전남대학교병원	11	화순전남대학교병원	18	한국문화진흥
5	경북대학교병원	12	충남대학교병원	19	강원랜드
6	충북대학교병원	13	서울올림픽기념국민체육진흥공단	20	한국철도공사
7	전북대학교병원	14	에스알	21	인천국제공항공사

[ISMS 인증 의무대상이 아님에도 인증 취득 공공기관 현황]

연번	기관명	연번	기관명	연번	기관명
1	서민금융진흥원	9	한국고용정보원	17	한국중부발전
2	한국서부발전	10	중소기업은행	18	한국전력거래소
3	부산항만공사	11	한국의약품안전관리원	19	예금보험공사
4	건강보험심사평가원	12	한국교육학술정보원	20	한국산업기술시험원
5	한국농업기술진흥원	13	한국재정정보원	21	농림수산물교육문화정보원
6	한국수력원자력	14	한국자산관리공사	22	한국산업안전보건공단
7	한국공항공사	15	국민건강보험공단	23	국립암센터
8	한국과학기술기획평가원	16	한국도로공사	24	공무원연금공단

자료: 과학기술정보통신부, 2026.8.

- 개정안은 「공공기관의 운영에 관한 법률」 제4조에 따른 공공기관으로서 정보통신망의 규모, 종류 등을 고려하여 대통령령으로 정하는 기관을 ISMS 인증 의무대상에 추가하려는 것으로, 정보통신망을 이용한 서비스를 제공하는 공공기관 또한 ISMS 인증을 받게 함으로써 정보보호 관리체계 인증의 실효성을 높이는 효과가 있을 것임.
- 현행법상 인증 의무대상도 주요정보통신서비스 제공자, 집적정보통신시설 사업자(데이터센터 사업자) 및 매출액·이용자 규모가

큰 사업자 등 처리하는 정보가 많거나 해당 서비스가 다른 정보통신서비스에 미치는 영향이 큰 사업자로 규정된 점을 감안하면, ISMS 인증 의무대상 공공기관을 규정하며 기관이 보유·처리하는 정보의 종류와 정보통신망의 규모 등을 고려하도록 한 것은 타당한 것으로 보임.

- 다만, 현재 ISMS 인증 및 심사 업무는 과학기술정보통신부가 직접 수행하지 않고 이를 수행할 정보보호 관리체계 인증기관과 정보보호 관리체계 심사기관을 지정⁵⁾하고 있는데, 현재 심사기관으로 지정된 기관은 모두 민간법인 또는 단체라는 점에서 공공기관의 보안상 민감한 정보나 정보보호 체계에 민간기관이 접근할 수 있게 되는 문제가 발생할 수 있음.
- 따라서, 공공기관의 ISMS 인증은 과학기술정보통신부가 인증업무를 직접 수행하거나 공공기관 대상 ISMS 인증·심사업무를 수행하는 별도의 공공기관을 지정하여 수행할 수 있도록 제한하는 방안 또는 심사기관에 대한 강화된 보안요건을 적용하여 관리·감독을 강화하고 심사기관의 독립성을 확보하기 위한 조치를 마련하는 등 방안을 고려할 필요가 있어 보임.
- 참고로, 공공기관에 대한 ISMS 인증 의무화와 관련한 내용으로 제22대 국회에서 발의된 3건의 유사한 개정안⁶⁾이 전체회의 상정

5) ·정보보호 관리체계 인증기관 : 한국인터넷진흥원(KISA), 금융보안원(FSI)

·정보보호 관리체계 심사기관 : 한국정보통신진흥협회(KAIT), 한국정보통신기술협회(TTA),
개인정보보호협회(OPA), 차세대정보보안인증원(NISC),
한국경영인증원(KMR), 한국생산성본부인증원(KPCQA)

(2025.11.17.) 후 소위원회에 회부되어 있고, 1건의 유사한 개정안⁷⁾이 위원회에 회부(2026.4.24.)되어 있는 상황이므로 동 개정안과 함께 논의할 필요가 있음.

다. 정부 및 관련 단체 의견

1) 과학기술정보통신부, 국가정보원

- 정보보호 관리체계 인증의 실효성을 높이기 위해 공공기관을 ISMS 인증 의무 대상에 편입하려는 취지에는 공감하나, 공공분야 사이버공격 및 위협에 대한 예방 및 대응 업무는 국정원 소관으로 공공기관은 ISMS 인증 제도와 유사한 ‘사이버 보안 실태 평가’를 받고 있으므로, 규제의 중복 적용 및 공공기관의 부담 가중 우려 등을 고려한 신중한 검토가 필요함.

6) 「정보통신망 이용촉진 및 정보보호 등에 관한 법률 일부개정법률안」 (김기현 의원, 2212287)

「정보통신망 이용촉진 및 정보보호 등에 관한 법률 일부개정법률안」 (차지호 의원, 2213021)

「정보통신망 이용촉진 및 정보보호 등에 관한 법률 일부개정법률안」 (김상훈 의원, 2213361)

7) 「정보통신망 이용촉진 및 정보보호 등에 관한 법률 일부개정법률안」 (김용만 의원, 2218584)

2. 정보보호 취약점 신고포상금 상향

가. 개정안의 내용

- 현재 대통령령에서 ‘5만원 이상 1천만원 이하’로 규정하고 있는 정보보호 취약점 신고포상금 지급 범위의 상한액을 2천만원으로 상향하고, 이를 법률에 직접 규정함(안 제47조의6제1항).

현행	개정안
제47조의6(정보보호 취약점 신고자에 대한 포상) ① 정부는 침해사고의 예방 및 피해 확산 방지를 위하여 정보통신서비스, 정보통신망연결기기등 또는 소프트웨어의 보안에 관한 취약점(이하 “정보보호 취약점”이라 한다)을 신고한 자에게 <u>예산의 범위에서</u> 포상금을 지급할 수 있다.	제47조의6(정보보호 취약점 신고자에 대한 포상) ① ----- ----- ----- ----- ----- ----- ----- ----- <u>2천만원의</u> ----- -----.
②·③ (생략)	②·③ (현행과 같음)

나. 검토의견

- 과학기술정보통신부는 현행법 제47조의6을 근거로 국내 민간 보안 전문가의 취약점 발굴을 활성화하고, 신규 취약점이 해킹

사고 등에 악용되는 것을 예방함으로써 국내 보안 취약점 발굴과 조치에 선도적 역할을 수행하기 위한 목적으로 정보보호 취약점 신고포상제도를 한국인터넷진흥원에 위탁하여 시행중임⁸⁾.

<정보보호 취약점 신고포상제도>

- (제도개요) 소프트웨어(SW)의 신규 보안 취약점을 악용한 침해사고를 예방하고, 민간 보안 전문가들의 취약점 발굴을 장려하기 위해 포상금을 지급하는 제도('12.10월~)
- (법적근거) 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조의6(정보보호 취약점 신고자에 대한 포상)
- (신고대상) 국내외 제조사의 최신 버전 소프트웨어(프로그램)에 영향을 줄 수 있는 독창적인 신규 취약점
※ 홈페이지 등 현재 운영 중인 서비스에 대한 취약점은 평가 및 포상 대상에서 제외
- (신고접수) 보안취약점 정보포털 → [취약점 신고·조회] 메뉴를 통해 접수
- (평가기준) 취약점 공격 난이도, 영향도, 해당 SW의 국내외 보급률 등을 종합 평가
- (지급절차) 유효성 검증(과기정통부·KISA) → 1차 평가(과기정통부·KISA) → 2차 평가(외부 위원회)를 거쳐 평가 등급에 따라 포상금 차등 지급
(분기별, 최대 1000만원/건)

자료: 과학기술정보통신부

- 현행법은 시행령을 통해 포상금의 지급 대상 및 기준을 정하고 있으며, 포상금은 5만원 이상 1천만원 이하의 범위에서 해당 정보보호 취약점으로 발생할 수 있는 침해사고의 범위·정도, 해당 정보보호 취약점의 악용의 용이성 등을 고려하여 과기부 장관이 정하는 바에 따라 산정하고 있음.

8) · 2026년도 보안취약점 신고포상제도 관련 예산 편성 내역

- SW보안취약점 신고포상제도 운영(평가체계 5회×61백만원+포상금300백만원)=605백만원

<포상금 지급 관련 현행 법령>

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」

제47조의6(정보보호 취약점 신고자에 대한 포상)

- ① 정부는 침해사고의 예방 및 피해 확산 방지를 위하여 정보통신서비스, 정보통신망연결기기등 또는 소프트웨어의 보안에 관한 취약점(이하 “정보보호 취약점”이라 한다)을 신고한 자에게 예산의 범위에서 포상금을 지급할 수 있다.
- ② 제1항에 따른 포상금의 지급 대상·기준 및 절차 등은 대통령령으로 정한다.
- ③ 정부는 제1항에 따른 포상금 지급에 관한 업무를 한국인터넷진흥원에 위탁할 수 있다.

「정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령」

제55조의6(정보보호 취약점 신고자에 대한 포상) ① 법 제47조의6제1항에 따른 포상금의 지급 대상·기준 및 절차는 별표 4의2와 같다.

- ② 과학기술정보통신부장관은 법 제47조의6제3항에 따라 포상금 지급에 관한 업무를 인터넷진흥원에 위탁하는 경우에는 위탁업무의 내용을 고시해야 한다.

[별표 4의2] 정보보호 취약점 신고자에 대한 포상금의 지급 대상·기준 및 절차

1. 포상금의 지급 대상 및 기준

가. 지급 대상

포상금의 지급 대상은 침해사고의 원인이 될 수 있는 법 제47조의6제1항에 따른 정보보호 취약점(이하 “정보보호 취약점”이라 한다)으로서 아직 일반에게 알려지지 않은 취약점(이하 “신규정보보호취약점”이라 한다)을 신고한 대한민국 국민으로 한다.

나. 지급 기준

포상금은 5만원 이상 1천만원 이하의 범위에서 해당 정보보호 취약점으로 발생할 수 있는 침해사고의 범위·정도, 해당 정보보호 취약점의 악용의 용이성 등을 고려하여 과학기술정보통신부장관이 정하는 바에 따라 산정한다.

(이하 생략)

- 지속적으로 증가하는 해킹, 보안 취약점 발생 등 다양한 요인으로 인한 사이버보안 위협이 고도화되고 있는 가운데 개인정보 유출 사고 또한 증가하는 추세에 따라, 2025년의 보안 취약점 신고

건수 및 신고대상으로 인정되어 포상금이 지급된 건수는 전년 대비 크게 증가하였음.

<최근 5년간 보안 취약점 신고 및 인정 건수>

(단위: 건)

구분	2021년	2022년	2023년	2024년	2025년
신고 건수	1,727	1,963	1,877	1,786	2,525
인정 건수	667	671	566	611	781
인정률	38.6%	34.2%	30.2%	34.2%	30.9%

자료: 과학기술정보통신부

- 개정안은 시행령에 1천만원으로 규정되어 있는 신고포상금의 상한액을 2천만원으로 상향하여 법률에 규정함으로써, 최고등급의 중대한 취약점에 대해 더 큰 포상금을 지급할 수 있게 함으로써 취약점 신고를 활성화하고 취약점 발굴에 투입되는 전문성과 노력에 상응하는 보상을 제공하려는 것으로 그 입법 취지는 타당한 것으로 보임.
- 다만, 개정안과 관련하여 다음의 사항을 고려할 필요가 있음.
- 첫째, 최근 5년 동안의 연도별 건당 포상금 최대지급액은 2022년 510만원, 2021년 670만원으로 상한액인 1천만원의 51%~67%에 머물러 있어, 현행 상한액이 실제 포상금 지급을 제약하고 있었다고 보기에는 어려운 측면이 있음.

<최근 5년간 건별 포상금 최대지급액>

구분	2021년	2022년	2023년	2024년	2025년
건별 포상금 최대지급액	670만원	510만원	525만원	525만원	630만원

자료: 과학기술정보통신부

- 국가적·사회적 파급력이 매우 큰 취약점이 신고되어 현행 상한액인 1천만원을 초과하는 수준의 보상이 필요한 경우에는 개정안의 의의가 있을 수 있겠으나, 최근 포상금 지급 실적과 지급 경향을 고려할 때 상한액 상향만으로 취약점 신고가 실질적으로 활성화될 수 있을지는 추가적인 검토가 필요함.
- 둘째, 포상금 상한액만을 상향하여 규정하고, 포상금 예산이나 지급기준이 바뀌지 않는다면 실제로는 종전과 같은 금액이 지급될 수 있으므로, 개정안 취지를 달성하기 위해서는 충분한 예산의 확보와 함께 지급기준의 변경이 수반되어야 할 것으로 보임.
- 최근 5년간 330만원 이상의 고액 포상금을 지급한 경우는 연평균 12.8건에 불과하여 그 비중이 2% 미만으로 낮아, 상한액 상향을 통하여 취약점 신고를 활성화하기 위해서는 전체적인 포상금 지급 수준의 상향이 뒤따라야 할 것으로 보이고, 그러려면 포상금 심사·지급 기준의 완화와 관련한 논의와 포상금 예산의 확대가 필요함.

<최근 5년간 연도별 포상금 지급구간별 지급현황>

(단위: 건)

구분	2021년	2022년	2023년	2024년	2025년	평균
5만원 이상 ~ 10만원 미만	113	215	232	345	35	188
10만원 이상 ~ 30만원 미만	276	149	112	59	122	143.6
30만원 이상 ~ 70만원 미만	116	118	103	55	64	91.2
70만원 이상 ~ 120만원 미만	62	126	71	75	253	117.4
120만원 이상 ~ 180만원 미만	48	38	11	40	125	52.4
180만원 이상 ~ 330만원 미만	45	22	31	33	138	53.8
330만원 이상 ~ 690만원 미만	7	3	6	4	44	12.8
690만원 이상 ~ 1,000만원 이하	0	0	0	0	0	0
합계	667	671	566	611	781	659.2

자료: 과학기술정보통신부

- 셋째, 개정안은 이 법 시행 전 신고되었으나 시행 후 포상 여부가 결정되거나 포상금이 지급되는 경우에 대한 적용 여부가 모호한 측면이 있으므로, 법 적용 시점을 명확히 하기 위하여 개정규정은 법 시행 이후 정보보호 취약점을 신고한 경우부터 적용하도록 적용례를 두는 방안을 검토할 필요가 있음.
- 참고로, 신고포상금의 하한액을 5만원에서 20만원으로 상향하여 법률에 규정하는 내용의 개정안⁹⁾이 위원회에 회부(2026.7.1.)되어 있으므로 동 개정안과 함께 논의할 필요가 있음.

다. 정부 및 관련 단체 의견

1) 과학기술정보통신부

- 취약점 신고포상제의 포상 수준을 상향하여 취약점을 적극적으로 발굴하고 신고할 수 있는 유인을 제공하려는 취지에 공감하나, 포상금 액수는 취약점의 중요도나 시급성, 예산 여건에 따라 조정할 필요가 있어 법률에 상한액을 직접 규정하면 향후 탄력적 조정을 제약할 우려가 있으므로, 법률 개정보다는 시행령 개정을 통해 반영할 필요가 있음.

9) 「정보통신망 이용촉진 및 정보보호 등에 관한 법률 일부개정법률안」(이상희 의원, 2219649)

3. 정보통신서비스 제공자 등에 대한 자료보전의무 신설

가. 개정안의 내용

- 과학기술정보통신부장관의 정보통신서비스 제공자에 대한 자료보전 명령 권한을 삭제하고, 정보통신서비스 제공자 등 정보통신망을 운영하는 자에게 침해사고의 징후를 발견하거나 발생 사실을 인지한 시점부터 정보통신망의 접속기록 등 대통령령으로 정하는 관련 자료를 즉시 보존하도록 의무를 부여함(안 제48조의4제5항).
- 정보통신서비스 제공자 등 정보통신망을 운영하는 자가 보존해야 할 자료에 영향을 미치는 조치를 취할 경우 이사회 및 정보보호 최고책임자에 보고 후 승인을 받도록 하고, 의사결정 과정을 기록해 3년간 보관하도록 함(안 제48조의4제7항 신설).

현 행	개 정 안
법률 제21500호 정보통신망 이용 촉진 및 정보보호 등에 관한 법률 제48조의4(침해사고의 원인 분석 등) ① ~ ④ (생략) ⑤ <u>과학기술정보통신부장관은 제2항에 따른 침해사고의 발생 여부, 원인 분석 및 대책 마련을 위하여 필요하면 정보통신서비스 제공자에게 정보통신망</u>	법률 제21500호 정보통신망 이용 촉진 및 정보보호 등에 관한 법률 제48조의4(침해사고의 원인 분석 등) ① ~ ④ (현행과 같음) ⑤ <u>정보통신서비스 제공자 등 정보통신망을 운영하는 자는 제2항에 따른 침해사고의 발생 여부, 원인 분석 및 대책 마련을 위하여 침해사고의 징후를</u>

현행	개정안
<u>의 접속기록 등 관련 자료의 보존을 명할 수 있다.</u> ⑥ (생략) <u><신설></u> ⑦·⑧ (생략) 법률 제21500호 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제71조(벌칙) ① 다음 각 호의 어느 하나에 해당하는 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다.	<u>발견하거나 발생 사실을 인지한 시점부터 정보통신망의 접속기록 등 대통령령으로 정하는 관련 자료를 즉시 보존하여야 한다.</u> ⑥ (현행과 같음) ⑦ <u>정보통신서비스 제공자 등 정보통신망을 운영하는 자가 서버의 재설치·폐기 등 제5항에 따라 보존해야할 자료에 영향을 미치는 조치를 취할 경우 이사회 및 정보보호 최고책임자(CISO)에 보고 후 승인을 받아야 하며, 의사결정 과정을 기록해 3년간 보관하여야 한다.</u> ⑧·⑨ (현행 제7항 및 제8항과 같음) 법률 제21500호 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제71조(벌칙) ① ----- ----- ----- ----- -.

현행	개정안
1. ~ 13. (생략) 13의2. 제48조의4제5항에 따른 명령을 위반하여 관련 자료를 <u>보전하지</u> 아니한 자	1. ~ 13. (현행과 같음) 13의2. 제48조의4제5항을----- ----- <u>보전 의무를 이행하지</u> ----- -----
14. (생략) ② (생략)	14. (현행과 같음) ② (현행과 같음)

나. 검토의견

- 현행법은 정보통신서비스 제공자로 하여금 침해사고가 발생하는 경우 즉시 과기부장관이나 한국인터넷진흥원에 신고하도록 하고¹⁰⁾, 침해사고의 원인 조사, 피해 확산 방지, 사고 대응, 복구 및 재발 방지에 필요한 조치 등을 수행하도록 규정하고 있음¹¹⁾.
- 이처럼 현행법은 정보통신서비스 제공자에게 침해사고 대응을 위한 여러 의무를 부과하고 있음에도, 침해사고가 발생한 경우 정보통신망 접속기록 등 관련 자료의 보전은 과기부장관의 보전

10) 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」

제48조의3(침해사고의 신고 등) ① 정보통신서비스 제공자는 침해사고가 발생하면 즉시 그 사실을 과학기술정보통신부장관이나 한국인터넷진흥원에 신고하여야 한다. 이 경우 정보통신서비스 제공자가 이미 다른 법률에 따른 침해사고 통지 또는 신고를 했으면 전단에 따른 신고를 한 것으로 본다.

11) 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」

제48조의4(침해사고의 원인 분석 등) ① 정보통신서비스 제공자 등 정보통신망을 운영하는 자는 침해사고가 발생하면 침해사고의 원인을 분석하고 그 결과에 따라 피해의 확산 방지를 위하여 사고대응, 복구 및 재발 방지에 필요한 조치를 하여야 한다.

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 과학기술정보통신부장관은 제2항에 따른 조치의 이행 여부를 점검하고, 보완이 필요한 사항에 대하여 해당 정보통신서비스 제공자에게 시정을 명할 수 있다.

명령이 있을 때에만 하도록 되어 있어 관련 자료의 훼손·멸실로 조사를 위한 관련 기록의 확보에 어려움이 있는 사례가 발생하고 있음.

- 이에 개정안은 정보통신서비스 제공자 등 정보통신망을 운영하는 자에게 침해사고의 징후를 발견하거나 발생 사실을 인지한 시점부터 정보통신망의 접속기록 등 대통령령으로 정하는 관련 자료를 즉시 보존하도록 하여, 침해사고의 원인 규명과 피해 확산 방지도모하고 정보통신망 운영자의 책임성을 강화한다는 측면에서 그 입법 취지에 공감할 수 있음.
- 다만, 개정안과 관련하여 다음의 사항을 고려할 필요가 있음.
- 첫째, 안 제48조의4제5항의 자료보전 의무 신설은 시행 예정인 정보통신망법 개정법¹²⁾에 따라 강화되는 자료 보존명령 제도의 시행 효과를 확인한 후 추가적인 제도 변경의 필요성을 판단할 필요가 있음.
- 현행법은 과학기술정보통신부장관이 침해사고의 원인 분석 및 대책 마련을 위하여 필요 시 정보통신서비스 제공자에게 정보통신망의 접속기록 등 관련 자료의 보존을 명할 수 있도록 규정하고 있는데, 2026년 10월 1일부터 시행되는 개정법은 이러한 자료보전명령을 이행하지 아니한 자에 대한 법정형을 현행 2년 이하의 징역 또는 2천만원 이하의 벌금에서 5년 이하의 징역 또는 5천만원 이하의 벌금으로 상향하고 있음.

12) 「정보통신망 이용촉진 및 정보보호 등에 관한 법률 일부개정법률」 [시행 2026. 10. 1.][법률 제21500호, 2026. 3. 31., 일부개정]

<자료보전명령 미이행 시 벌칙 개정사항 비교>

법률	현행법	개정법(2026.10.01.시행)
벌칙	2년 이하의 징역 또는 2천만원 이하의 벌금	<u>5년 이하의 징역 또는 5천만원 이하의 벌금</u>
관련 조문	제73조(벌칙) 다음 각 호의 어느 하나에 해당하는 자는 2년 이하의 징역 또는 2천만원 이하의 벌금에 처한다. 6. 제48조의4제5항에 따른 명령을 위반하여 관련 자료를 보전하지 아니한 자	제71조(벌칙) ① 다음 각 호의 어느 하나에 해당하는 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다. 13의2. 제48조의4제5항에 따른 명령을 위반하여 관련 자료를 보전하지 아니한 자

- 그런데 동 개정법이 아직 시행되지 않아 벌칙 강화의 효과가 확인되지 않은 상황에서 자료보전 의무와 형사처벌 체계를 다시 변경하는 것은, 수범자의 예측 가능성을 저해하고 법적 안정성을 약화시킬 우려가 있음.
- 따라서 우선 시행 예정인 개정법에 따른 벌칙 강화가 자료보전 명령의 실효성을 충분히 확보하는지를 살펴본 후, 현행 명령 방식 만으로는 침해사고 관련 자료를 적시에 확보하기 어렵다는 점이 객관적으로 확인되는 경우 개정안에 따른 직접적인 자료보전 의무의 도입 여부를 검토할 필요가 있을 것으로 보임.
- 둘째, 안 제48조제5항의 자료보전 의무 부과 대상의 확대 필요성, 관련 법체계와의 정합성 등을 고려하여 의무 주체의 범위를 정하고, 형벌의 구성요건이 되는 보전 의무의 발생 시점을 수범자가 쉽게 예측할 수 있도록 설정하는 등 규정의 명확성을 제고할 필요가 있음.

- 개정안은 자료보전 의무의 주체를 정보통신서비스 제공자가 아닌 “정보통신서비스 제공자 등 정보통신망을 운영하는 자”로 규정하고 있는데, 정보통신서비스 제공자는 영리 목적으로 정보를 제공하거나 정보의 제공을 매개하는 자¹³⁾로 한정되나, 개정안에 따르면 행정기관이나 비영리법인·단체 등으로서 정보통신망을 운영하는 자까지 범위가 확대될 수 있음.
- 특히, 공공부문의 경우 「국가정보원법」에 따라 공공부문의 사이버 공격 및 위협에 대한 대응 업무는 국가정보원이 담당하고 있고¹⁴⁾, 그에 따라 현행법에서도 과기부 장관이 침해사고가 발생한 정보통신망에 대하여 원인 분석 및 대책 마련에 필요한 조치를 이행하도록 명할 수 있도록 하면서 그 대상에서 공공기관등을 제외하고 있으므로¹⁵⁾, 개정안의 내용은 현재 침해사고 대응체계와 다소 부합하지 않는 측면이 있음.

13) 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조(정의) ① 이 법에서 사용하는 용어의 뜻은 다음과 같다.

3. “정보통신서비스 제공자”란 「전기통신사업법」 제2조제8호에 따른 전기통신사업자와 영리를 목적으로 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자를 말한다.

14) 「국가정보원법」 제4조(직무) ① 국정원은 다음 각 호의 직무를 수행한다.

4. 다음 각 목의 기관 대상 사이버공격 및 위협에 대한 예방 및 대응

가. 중앙행정기관(대통령 소속기관과 국무총리 소속기관을 포함한다) 및 그 소속기관과 국가인권위원회, 고위공직자범죄수사처 및 「행정기관 소속 위원회의 설치·운영에 관한 법률」에 따른 위원회

나. 지방자치단체와 그 소속기관

다. 그 밖에 대통령령으로 정하는 공공기관

15) 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」

제48조의4(침해사고의 원인 분석 등) ② 과기기술정보통신부 장관은 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.

- 또한, 개정안은 침해사고의 징후를 발견한 경우에도 자료 보존 의무를 규정하고 있는데, 보존의무 위반은 5년 이하의 징역 또는 5천만원 이하의 벌금의 대상이 된다는 점에서 위반행위의 구성 요건이 명확하게 규정될 필요가 있으나, 징후 발견의 판단기준이 명확하지 않은 측면이 있음. 따라서 2026년 10월 1일 시행 예정인 정보통신망법 개정법도 사업자의 침해사고 대응 조치를 확대하면서 침해사고가 발생하였다고 의심할 만한 정황이 있어 침해사고조사심의위원회가 조사가 필요하다고 인정하는 경우에 침해사고의 발생 여부 및 원인 분석 등에 필요한 조치를 하도록 규정¹⁶⁾하였음을 고려하여, 이를 준용하여 조문을 구성하는 등 명확성을 보완할 필요가 있어 보임.
- 셋째, 개정안에서 신설되는 자료 보존의무는 그 대상의 경우 대통령령으로 위임하여 구체적으로 정할 수 있도록 하고 있으나, 그 외 세부내용이 규정될 필요가 있는 사항에 대한 위임 범위가 불명확한 측면이 있음.
- 안 제48조의4제5항은 침해사고 발생 시 과기부장관이 정보통신 서비스 제공자에게 자료 보존을 명하는 대신 당사자 스스로 자료를 보존하도록 의무를 부과하고 있는데, 명령이 있을 때 비로소 발생

16) 「정보통신망 이용촉진 및 정보보호 등에 관한 법률 일부개정법률」 [시행 2026. 10. 1.][법률 제21500호, 2026. 3. 31., 일부개정] 제48조의4(침해사고의 원인 분석 등) ① 정보통신서비스 제공자 등 정보통신망을 운영하는 자는 침해사고가 발생하였거나 내부 정보 유출 등 침해사고가 발생하였다고 의심할 만한 정황이 있어 제48조의2제7항에 따른 침해사고조사심의위원회가 침해사고 발생 여부에 대한 조사가 필요하다고 인정하는 경우에는 침해사고의 발생 여부 및 원인을 분석하고 그 결과에 따라 피해의 확산 방지를 위하여 사고대응, 복구 및 재발 방지에 필요한 조치를 하여야 한다.

하던 의무가 상시적 의무로 바뀐다는 점에서 자료 보존의 기간이나 방법 등이 구체적으로 규정될 필요가 있음에도 명확한 하위법령 위임 근거가 없으므로 이에 대한 보완이 필요함.

- 또한, 자료 보존 의무 부과는 사업자에게 상당한 부담이 될 수 있다는 점을 감안하여, 보존 요건이 되는 침해사고를 사고의 중대성, 영향을 받는 이용자의 수 등을 고려하여 하위 법령으로 정하는 기준을 충족하는 사고로 한정하는 것을 검토할 필요가 있음.
- 넷째, 안 제48조의4제7항은 서버의 재설치·폐기 등 보존자료에 영향을 미치는 조치를 취할 경우 이사회·정보보호 최고책임자(CISO)에 보고 후 승인을 받고 의사결정 과정을 기록해 3년간 보관하도록 의무화하고 있지만, 이를 위반한 경우의 제재는 별도로 규정하지 않고 있음.
- 따라서 제7항을 법적 의무사항으로 둔다면 위반 시 적용되는 벌칙 규정 등 의무이행 확보수단을 함께 마련하여 실효성을 제고할 필요가 있어 보이며, 이 경우 보존자료에 영향을 미치는 조치의 세부 판단기준, 관련 절차, 보관 방법 등에 대한 명시적인 하위 법령 위임 근거를 두어 의무의 실질을 구체화할 필요가 있음.
- 마지막으로, 안 제48조의4제5항에 따른 자료 보존의무의 적용 시점을 명확히 하기 위하여 부칙에 자료 보존의무 부과에 관한 적용례를 둘 필요가 있음.

- 개정안 시행 전에 발생 사실을 인지한 사고에 대한 자료가 이미 삭제된 경우에도 개정안을 적용하게 되면, 소급적용에 따른 벌칙 부과 문제가 발생할 수 있으므로 자료 보존의무에 대하여는 개정안 시행 이후 침해사고가 발생하거나 그 정황을 인지한 경우 부터 적용하도록 명확히 규정할 필요가 있음.
- 참고로, 평상시에는 일정한 기준에 해당하는 정보통신서비스 제공자에게 로그기록을 보관하도록 의무화하고, 침해사고 발생 시에는 모든 정보통신서비스 제공자에게 로그기록 보존의무를 부과하는 내용으로 침해사고 관련 자료보전 의무를 신설하는 내용의 개정안¹⁷⁾이 위원회에 회부(2026.3.30.)되어 있으므로 동 개정안과 함께 논의할 필요가 있음.

다. 정부 및 관련 단체 의견

1) 과학기술정보통신부

- 침해사고 발생 시 원인 분석을 위한 자료 보존 의무를 강화함으로써 책임 귀속 주체를 명확히 하려는 취지에 공감하며, 아울러 자료 보존과 관련하여 서버 재설치·폐기 시 이사회 및 CISO의 승인과 의사결정 기록 보관을 의무화하는 것은 투명한 사고대응 체계를 확립하는 차원에서 필요성이 있다고 판단됨.

17) 「정보통신망 이용촉진 및 정보보호 등에 관한 법률 일부개정법률안」(조인철 의원, 2217815)

문 의 처
02)6788-5235