



제 432회 국회 (임시회)
제3차 과학기술정보방송통신위원회

정보통신망 이용촉진 및 정보보호 등에 관한 법률 일부개정법률안

검 토 보 고

〈정보보호 취약점 처리방침 수립 · 공개〉

■ 최형두의원 대표발의(의안번호 제2216276호)

2026. 2.

과학기술정보방송통신위원회

수석전문위원 이복우

목 차

I . 제안경 위	1
II . 제안이유 및 주요내용	1
III . 검토의견	3
1. 정보보호 취약점 처리방침의 수립 및 공개(안 제47조의8 신설)	3
2. 정보보호연구자의 책무(안 제47조의9 신설)	7
3. 정보보호 취약점의 신고 의무(안 제47조의10 신설)	12

I. 제안경위

가. 발 의 자 : 최형두의원 등 14인

나. 발 의 일 : 2026. 1. 23.

다. 회 부 일 : 2026. 1. 26.

II. 제안이유 및 주요내용

최근 디지털 전환의 가속화로 소프트웨어 및 정보통신망연결기기 등의 보안취약점을 악용한 사이버 침해사고가 급증하고 있음. 이에 따라 전세계적으로 민간 보안 전문가(화이트해커 등)와 협력하여 사전에 취약점을 발굴하고 보완하는 ‘보안취약점 협력대응제도(CVD)’가 확산되는 추세임.

그러나 현행법은 정당한 권한 없는 정보통신망 침입을 금지하고 있어, 선의의 목적으로 취약점을 연구·발굴하는 보안전문가들의 활동이 위축될 우려가 있고, 기업들 또한 별도의 신고 채널이나 처리 절차를 갖추지 않아 발견된 취약점이 방치되거나 음성적으로 거래되는 등의 문제가 제기되어 왔음.

이에 정보통신서비스 제공자 등으로 하여금 정보보호 취약점 처리 방침을 수립·공개할 수 있도록 하여 취약점 발굴 및 신고의 투명성을 확보하고, 해당 방침을 준수하여 활동하는 정보보호연구자에 대한 면책 근거를 마련하는 한편, 중대한 취약점에 대해서는 정부 신고 및 이용자 통지를 의무화함으로써 민간의 자발적인 보안 활동을 양성화

하고 사이버 침해사고를 선제적으로 예방하려는 것임(안 제47조의8부터 제47조의10까지 신설).

Ⅲ. 검토의견

1. 정보보호 취약점 처리방침의 수립 및 공개(안 제47조의8 신설)

가. 개정안 요지

- 정보통신서비스 제공자, 정보통신망연결기기등을 제조하거나 수입하는 자 및 소프트웨어사업자가 다음 각 호의 사항이 포함된 정보보호 취약점 처리방침을 수립·공개할 수 있도록 함(안 제47조의8제1항 신설).
 - 정보보호 취약점의 점검 허용 범위 및 준수 사항(제1호)
 - 정보보호 취약점의 신고 및 처리 절차(제2호)
 - 제47조의9에 따른 정보보호연구자의 접근권한 범위 및 면책에 관한 사항(제3호)
 - 그 밖에 정보보호 취약점의 점검을 위하여 필요한 사항(제4호)
- 과학기술정보통신부장관이 처리방침의 작성 및 공개지침을 정하여 처리방침수립자에게 그 준수를 권장할 수 있도록 함(안 제47조의8제2항 신설).

나. 개정안 조문대비표

현행	개정안
<신설>	제47조의8(정보보호 취약점 처리방침의 수립 및 공개) ① 정보통신서비스 제공자, 제45조제1

항제2호에 따른 정보통신망연
결기기등을 제조하거나 수입하
는 자 및 「소프트웨어 진흥
법」 제2조에 따른 소프트웨어
사업자(이하 “처리방침수립자”
라 한다)는 다음 각 호의 사항
이 포함된 정보보호 취약점 처
리방침(이하 “처리방침”이라 한
다)을 수립·공개할 수 있다.

1. 정보보호 취약점의 점검 허
용 범위 및 준수 사항

2. 정보보호 취약점의 신고 및
처리 절차

3. 제47조의9에 따른 정보보호
연구자의 접근권한 범위 및
면책에 관한 사항

4. 그 밖에 정보보호 취약점의
점검을 위하여 필요한 사항

② 과학기술정보통신부장관은
처리방침의 작성 및 공개지침
을 정하여 처리방침수립자에게
그 준수를 권장할 수 있다.

다. 검토사항

- 최근 디지털 전환의 가속화에 따라 소프트웨어 및 정보통신망 연결기기등의 보안취약점을 악용한 사이버 침해사고가 급증하고 있으며, 특히 IP카메라 해킹 및 개인정보 유출 등 피해가 급증하고 있어, 사후적 대응을 넘어서 선제적으로 보안취약점을 발굴하고 보완할 필요성이 높아지고 있는 상황임.
- 개정안은 정보통신서비스 제공자 등으로 하여금 정보보호 취약점 처리방침을 수립·공개할 수 있도록 재량을 부여함으로써 보안 취약점을 발굴하고 신고하도록 자율적인 가이드라인을 세우도록 장려하고자 하는 것으로 보이며, 그러한 취지에 대해 공감함.
- 다만, 현행법상 이뤄지는 각종 지침들과의 정합성, 중복 여부에 대한 검토가 필요함.
 - 현행 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 “정보통신망법”) 제45조는 정보통신서비스 제공자 및 정보통신망연결기기등 제조·수입업자에게 보호조치 의무를 부여하고, 과학기술정보통신부장관에게는 정보보호지침을 고시하도록 함¹⁾.

1) 제45조(정보통신망의 안정성 확보 등) ① 다음 각 호의 어느 하나에 해당하는 자는 정보통신서비스의 제공에 사용되는 정보통신망의 안정성 및 정보의 신뢰성을 확보하기 위한 보호조치를 하여야 한다.

1. 정보통신서비스 제공자
2. 정보통신망에 연결되어 정보를 송·수신할 수 있는 기기·설비·장비 중 대통령령으로 정하는 기기·설비·장비(이하 “정보통신망연결기기등”이라 한다)를 제조하거나 수입하는 자

② 과학기술정보통신부장관은 제1항에 따른 보호조치의 구체적 내용을 정한 정보보호조치에 관한 지침(이하 “정보보호지침”이라 한다)을 정하여 고시하고 제1항 각 호의 어느 하나에 해당하는 자에게 이를 지키도록 권고할 수 있다.

③ 정보보호지침에는 다음 각 호의 사항이 포함되어야 한다.

1. 정당한 권한이 없는 자가 정보통신망에 접근·침입하는 것을 방지하거나 대응하기 위한

- 현행법 제45조의2는 정보통신서비스 제공자에게 정보보호 사전점검 의무를 부여하고, 과학기술정보통신부장관에게는 대통령령으로 정하는 **사전점검기준**에 따른 보호조치를 권고할 수 있도록 규정함²⁾.
- 현행법 제45조의3은 정보통신서비스 제공자에게 정보보호 최고책임자를 지정하도록 하면서 그 업무로 정보보호를 위한 각종 **계획, 대책** 마련을 규정함³⁾.
- 현행법 제47조의4는 이용자의 정보보호를 위해 정부가 **정보보호에 필요한 기준**을 정하여 이용자에게 권고하고 취약점 점검, 기술 지원 등 필요한 조치를 할 수 있도록 규정함⁴⁾.

정보보호시스템의 설치·운영 등 기술적·물리적 보호조치

2. 정보의 불법 유출·위조·변조·삭제 등을 방지하기 위한 기술적 보호조치

3. 정보통신망의 지속적인 이용이 가능한 상태를 확보하기 위한 기술적·물리적 보호조치

4. 정보통신망의 안정 및 정보보호를 위한 인력·조직·경비의 확보 및 관련 계획수립 등 관리적 보호조치

5. 정보통신망연결기기등의 정보보호를 위한 기술적 보호조치

- 2) **제45조의2(정보보호 사전점검)** ① 정보통신서비스 제공자는 새로이 정보통신망을 구축하거나 정보통신서비스를 제공하고자 하는 때에는 그 계획 또는 설계에 정보보호에 관한 사항을 고려하여야 한다.
② 과학기술정보통신부장관은 다음 각 호의 어느 하나에 해당하는 정보통신서비스 또는 전기통신사업을 시행하고자 하는 자에게 대통령령으로 정하는 정보보호 사전점검기준에 따라 보호조치를 하도록 권고할 수 있다
- 3) **45조의3(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.
④ 정보보호 최고책임자의 업무는 다음 각 호와 같다.
 1. 정보보호 최고책임자는 다음 각 목의 업무를 총괄한다.
 - 가. 정보보호 계획의 수립·시행 및 개선
 - 나. 정보보호 실태와 관행의 정기적인 감사 및 개선
 - 다. 정보보호 위험의 식별 평가 및 정보보호 대책 마련
 - 라. 정보보호 교육과 모의 훈련 계획의 수립 및 시행
- 4) **제47조의4(이용자의 정보보호)** ① 정부는 이용자의 정보보호에 필요한 기준을 정하여 이용자에게 권고하고, 침해사고의 예방 및 확산 방지를 위하여 취약점 점검, 기술 지원 등 필요한 조치를 할 수 있다.

- 현행법은 정부에게 각종 지침을 수립할 수 있고 취약점 점검을 위한 조치를 할 수 있도록 규정하고 있으며, 정보통신서비스 제공자에게는 보호조치 및 사전점검, 대책 마련 의무를 부과하고 있으므로, 기존 제도들과 개정안이 도입하고자 하는 정보보호 취약점 처리방침 사이의 관계나 기능 중복에 대한 충분한 논의가 필요해 보임.

2. 정보보호연구자의 책무(안 제47조의9 신설)

가. 개정안 요지

- 정보보호 취약점의 발견을 목적으로 정보통신서비스, 정보통신망연결기기등 또는 소프트웨어에 접근하려는 자가 정보보호 취약점 점검 시 다음 각 호의 사항을 준수하도록 함(안 제47조의9제1항).
 - 제47조의8에 따라 수립·공개된 처리방침 준수
 - 정보보호 취약점 발견의 목적으로만 점검 대상 접근
 - 처리방침수립자 및 이용자 피해 방지
 - 관계 법령 준수
- 정보보호연구자는 정보보호 취약점 발견 시 처리방침수립자에게 신고하여야 하고(안 제47조의9제2항),

정보보호연구자는 제1항의 사항을 준수했음을 대통령령으로 정하는

바에 따라 과학기술정보통신부장관에게 신고하여야 하며 장관은 그 준수 여부를 조사할 수 있도록 하며(안 제47조의9제3항),

정보보호연구자가 준수사항을 지키고 신고의무를 다한 경우 취약점 점검 수행 결과에 대하여 고의·중대한 과실이 없는 한 민·형사상 책임을 면제함(안 제47조의9제4항).

나. 개정안 조문대비표

현행	개정안
<u><신 설></u>	제47조의9(정보보호연구자의 책무) ① 정보보호 취약점의 발견을 목적으로 정보통신서비스, 정보통신망연결기기등 또는 소프트웨어에 접근하려는 자(이하 “정보보호연구자”라 한다)는 정보보호 취약점의 점검을 수행하는 과정에서 다음 각 호의 사항을 준수하여야 한다. 1. 제47조의8에 따라 수립·공개된 처리방침을 준수할 것 2. 정보보호 취약점 발견의 목적으로만 점검 대상에 접근할 것 3. 처리방침수립자 및 이용자에

게 부당한 피해를 주지 아니
할 것

4. 발견한 정보보호 취약점 및
관련 정보를 목적 외의 용도
로 사용하지 아니할 것

5. 이 법, 「개인정보 보호법」
및 「저작권법」 등 관계 법령
을 준수할 것

② 정보보호연구자는 정보보호
취약점의 점검 수행 결과 정보
보호 취약점을 발견한 경우에
는 처리방침수립자에게 처리방
침에 따라 그 내용을 신고하여
야 한다.

③ 정보보호연구자는 정보보호
취약점의 점검을 수행하는 과
정에서 제1항에 따른 사항을
준수하였음을 대통령령으로 정
하는 바에 따라 과학기술정보
통신부장관에게 신고하여야 한
다. 이 경우 과학기술정보통신
부장관은 처리방침수립자로부터
이의 제기가 있거나 제1항
에 따른 사항을 준수하지 아니
하였다고 의심할만한 상당한
사유가 있는 경우에는 정보보

	<u>호연구자가 제1항에 따른 사항을 준수하였는지를 조사할 수 있다.</u> <u>④ 정보보호연구자가 제1항에 따른 사항을 준수하였으며 제3항에 따른 신고를 한 경우에는 정보보호 취약점의 점검을 수행한 결과에 대하여 그의 행위에 고의나 중대한 과실이 없는 경우에는 민사상·형사상의 책임을 면제한다.</u> <u>⑤ 제3항에 따른 신고의 방법 및 그 밖에 필요한 사항은 대통령령으로 정한다.</u>
--	--

다. 검토사항

- 최근에 화이트해커, ICT사업자, 조정기관간의 소통·협력·조정에 기반하여 ICT제품·서비스에 존재하는 보안취약점을 발견하고 신고, 조치, 공개하는 보안취약점 대응 프로세스가 대두되는 바, 이러한 보안취약점 협력대응제도 (Coordinated Vulnerability Disclosure: CVD)가 미국, EU, OECD국가들 사이에서 도입·확산되고 있음⁵⁾.
- 정보보호 취약점에 대한 점검 및 조치에 있어서 민간의 화이트

5) 이태승. (2024). 보안취약점 협력대응제도(CVD) 도입을 위한 법제화 방안 연구: 정보통신망법 중심으로. 정보보호학회논문지 제34권 제4호. pp. 782.

해커와 같은 전문가의 도움을 요청하는 것이 필요한데, 현행법은 정당한 권한 없는 정보통신망 침입을 금지하고 있으므로⁶⁾, 보안취약점 발굴을 위한 보안전문가·연구자들의 활동이 위축될 우려가 있다는 지적이 제기되고 있음.

- 따라서 개정안은 CVD를 국내에 도입하고 선의의 보안전문가들의 활동을 가능하도록 하기 위한 법적 근거를 마련하고자 일정한 기준을 충족한 정보보호연구자에 대한 민사상·형사상 책임을 면제하고자 하는 것임.
- 선의의 연구자들에게 접근권한을 설정하여 주고자하는 입법 취지에 대해 공감하나, 다음의 사항을 고려할 필요가 있음.
- 먼저, 법조문 간에 일부 상충·모순되는 측면이 있어, 검토가 필요함.
 - 정보보호연구자는 처리방침수립자 및 이용자에게 부당한 피해를 주지 아니하여야만 안 제47조의9제4항에 따라 민사상·형사상 책임이 면제되는데, 정보보호연구자로 하여금 면책조건으로서 피해를 주지 않을 것을 요구하면서 그러한 의무를 다할 경우 면책이 되도록 함으로써 사실상 “효과를 요건으로 요구”하여 면책 규정을 두는 실익이 없어짐.
 - 따라서 의도치 않은 경미한 피해가 발생하더라도 정보보호연구자가

6) 제48조(정보통신망 침해행위 등의 금지) ① 누구든지 정당한 접근권한 없이 또는 허용된 접근권한을 넘어 정보통신망에 침입하여서는 아니 된다.

제71조(벌칙) ①다음 각 호의 어느 하나에 해당하는 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다.

11. 제48조제1항을 위반하여 정보통신망에 침입한 자

안 제47조의9제1항에 따른 의무를 준수한 것이 되도록 규정을 수정하는 것을 논의할 필요가 있음.

- 또한, 민사상·형사상의 책임을 면한다는 규정이 있으나, 여전히 현행법 제48조제1항에 따라 금지되는 행위를 하는 것이 될 수 있어, 정보보호연구자는 여전히 행정처분에 처할 위험이 존재하는 등 그 법적 지위가 불안정하므로, 정보보호연구자는 정당한 접근권한을 획득한다는 점을 규정하는 등의 보완을 검토할 필요가 있음.
- 추가적으로 법제적인 관점에서, 안 제47조의9제1항은 ‘다음 각 호의 사항을 준수하여야 한다.’고 규정하면서 제1호는 ‘처리방침을 준수할 것’이라 규정하고, 제5호 또한 ‘관계 법령을 준수할 것’이라고 규정하고 있는데, 이는 곧 ‘준수할 것’을 ‘준수하여야 한다’고 규정하는 것이 되어 입법기술적 측면에서 서술어가 중복되는 바, 문구를 일부 수정하여야 할 것으로 보임⁷⁾.

3. 정보보호 취약점의 신고 의무(안 제47조의10 신설)

가. 개정안 요지

- 처리방침수립자에게 정보보호 취약점을 알게 된 때에는 지체없이 당국에 신고하고 이용자에게는 관련 정보와 보호조치 방법을 통지하도록 함(안 제47조의10제1항)

7) 안 제47조의9제1항의 서술어를 ‘지켜야 한다’, ‘따라야 한다’ 등으로 바꾸는 것을 고려할 수 있음.

- 과학기술정보통신부장관이 취약점이 발견된 경우에 해당 처리방침수립자에게 예방 조치를 권고할 수 있도록 함(안 제47조의 10제2항)

나. 개정안 조문대비표

현행	개정안
<u><신 설></u>	<u>제47조의10(정보보호 취약점의 신고 등) ① 처리방침수립자는 침해행위에 이용되었거나 이용될 가능성이 높은 정보보호 취약점을 알게 된 때에는 지체 없이 과학기술정보통신부장관 또는 한국인터넷진흥원에 신고하여야 한다. 이 경우 처리방침수립자는 이용자에게 정보보호 취약점에 관한 정보와 보호조치 방법을 통지하여야 한다.</u> <u>② 과학기술정보통신부장관은 제1항에 따른 정보보호 취약점이 발견된 경우에는 해당 처리방침수립자에게 정보보호 취약점의 개선 등 침해사고의 발생을 예방하기 위한 조치를 할 것을 권고할 수 있다.</u>

	③ 제1항에 따른 신고의 시기, 방법 및 절차 등에 관하여 필요한 사항은 대통령령으로 정한다.
--	---

다. 검토사항

- 정보보호 취약점에 대해서 정부에 신고하게 하고, 동시에 이용자에게는 그 취약점에 관한 정보 및 보호조치 방법을 통지토록 하는 것은 정부 당국으로 하여금 정보보호 취약점에 대해서 파악토록 하고 이용자에게는 취약점에 대해 사전에 대응하도록 하려는 것으로, 그러한 입법취지에 대해 공감함.
- 다만, 안 제47조의8제1항에서 처리방침수립자에게 처리방침의 수립을 재량으로 규정하는 것을 고려할 때, 처리방침수립자에게 신고 및 통지의무를 부여하는 것은 재량 사항인 방침 수립을 기피하도록 유도해 입법취지를 달성하기 어려울 것으로 보임.
 - 개정안에 따르면 정보보호 취약점 처리방침의 수립 및 공개는 정보통신서비스 제공자의 재량 사항이며, 정보보호연구자는 스스로 정보통신망법 제48조 및 제71조에 따른 형사상 책임에서 면하기 위해서 처리방침수립자의 처리방침을 준수하여야 함.
 - 사실상, 개정안에서 처리방침수립자, 정보보호연구자는 각각 자발적으로 처리방침을 수립하거나 정보보호 취약점의 점검을

수행할 유인이 미미하며, 정부 또한 CVD의 조정기관으로서의 역할 및 권한이 부여되어 있지 않음.

- 입법취지를 달성하고 CVD를 성공적으로 도입하기 위해서는 처리방침 수립자 및 정보보호연구자에 대한 유인책을 마련하는 한편, 조정기관으로서 과학기술정보통신부 또는 그 업무를 위탁받아 수행하는 한국인터넷진흥원⁸⁾이 정보보호연구자(화이트해커), 처리방침수립자(ICT사업자), 조정기관으로서 정부의 소통·협력·조정 기능을 수행할 수 있도록 역할 및 권한을 규정하는 등 보완이 필요해 보임.

- 정보통신망법 제47조의6에 따른 취약점 신고자에 대한 포상제도를 신설하는 조문들과 연계시키는 방안, 예산의 한계 또는 포상제도 악용 가능성 등을 고려하여 비금전적인 유인책을 추가적으로 고안하는 방안 등을 논의할 필요가 있음.

○ 과학기술정보통신부는 선제적인 침해사고 예방 및 민간의 자발적 보안 활동 양성화를 위한 CVD 도입의 필요성에 공감하나 다음을 이유로 신중한 검토가 필요하다는 입장임.

- 연내 시범사업 운영⁹⁾ 이후 그 결과를 고려하여 정보통신망법과 개인정보보호법 등 타부처 소관 법률까지 포함한 종합적인 법률 개정 검토가 필요함.

8) 제47조의4(이용자의 정보보호) ① 정부는 이용자의 정보보호에 필요한 기준을 정하여 이용자에게 권고하고, 침해사고의 예방 및 확산 방지를 위하여 취약점 점검, 기술 지원 등 필요한 조치를 할 수 있다.

② 정부는 제1항에 따른 조치에 관한 업무를 한국인터넷진흥원 또는 대통령령으로 정하는 전문기관에 위탁할 수 있다.

9) 대한민국 인공지능행동계획에 따라 올해 시범사업을 거칠 예정('26.2.10. AI전략위)

- 취약점 공개에 관한 사항 및 조정기관으로서 과기정통부나 한국인터넷진흥원의 역할에 관한 규정 추가도 고려할 필요가 있다는 의견임.

문 의 처
02)6788-5228