국회입법조사처 | 2026. 03. 26. | 제401호

KOR 국회입법조사처
nars.go.kr

NARS 현안분석
NARS CURRENT ISSUES AND ANALYSIS

기본부터 다시 갖춰야 할 정보보호 체계

강은수
박소영

2025년 사이버 침해사고 유형 분석 및 제도 개선과제

- 2025년은 공공·민간 전반에서 대규모 사이버 침해사고가 잇따라 발생하며, 정보보호 체계의 구조적인 취약성이 집약적으로 드러난 해였음
- 반복적으로 발생한 사이버 침해사고와 개인정보 유출은 현행 정보보호 법·제도 전반에 구조적인 한계가 존재함을 드러내고 있음
- 본 보고서는 2025년 주요 침해사고를 유형화하고, 반복적으로 드러난 정보보호 체계의 구조적 문제점을 사전 예방 단계와 사후 대응 단계로 구분하여 종합적으로 분석하며, 이를 개선하기 위한 입법·정책적 개선 방안을 제시함
- 사전 예방 단계의 개선 과제로 제로트러스트 확산, 취약점 신고제도 활성화, 공급망 보안 강화 및 보안인증 제도 실효성 제고 방안을, 사후 대응 단계의 개선 과제로 자료 보전 의무 강화, 해커 처벌 및 범죄수익 환수 체계 정비, 피해자 보상 체계 확충을 제안함

국회입법조사처
NATIONAL ASSEMBLY RESEARCH SERVICE

Rebuilding the Information Security Framework from the Ground Up

국회입법조사처 nars.go.kr

Analysis of 2025 Cybersecurity Incident Types and Policy Improvement Measures

Ⅰ 반복된 2025년 사이버 침해사고: '기법' 아닌 '기본'의 문제

2025년은 정보보호 체계의 구조적인 취약성이 집약적으로 드러난 해였다.

2025년 한국인터넷진흥원에 접수된 사이버 침해사고는 2,383건으로 전년 대비 26.3% 증가하며 역대 최다를 기록했다('23년 1,277건, '24년 1,887건)[1]. 특히, 개별 시스템 침해를 넘어 통신, 금융, 플랫폼, 공공 행정망 등 국민 생활 밀접 인프라 전반으로 확산되는 양상을 보였다.[2]

표 1 2025년 분야별 사이버 침해사고 발생 현황

분야	해당 사고
통신	SKT 유심정보 유출(4월), LGU+ 침해사고(7월), KT 불법 팸토셀 침해사고(9월)
금융	SGI서울보증 랜섬웨어 감염(7월), 웰컴금융그룹 랜섬웨어 감염(8월), 롯데카드 고객카드정보 유출(9월), 가상자산거래소 업비트 침해사고(11월), 신한카드 가맹점주 정보 유출(12월)
플랫폼·유통·서비스	GS리테일 고객 개인정보 유출(1월), 결혼정보업체 듀오 회원 개인정보 유출(1월), 아디다스 고객정보 유출(5월), 예스24 랜섬웨어 감염(6월, 8월), 쿠팡 고객정보 유출(11월), 넷마블 고객정보 유출(11월), 신세계I&C 임직원 및 협력사 직원 정보 유출(12월)
명품브랜드사	디올 개인정보 유출(1월), 티파니 개인정보 유출(4월), 루이비통 개인정보 유출(6월)
운송 서비스	아시아나항공 임직원 및 협력사 직원 개인정보 유출(12월)
국가·공공분야	한국연구재단 개인정보 유출(6월), 정부행정망 침투(7월)

출처: 언론보도 등을 참고하여 작성

SK텔레콤(이하 "SKT") · 롯데카드 · 쿠팡의 고객정보 유출, KT의 불법 펨토셀 침해사고, 예스24 · SGI서울보증의 랜섬웨어 감염 등 민간 영역뿐 아니라 온나라시스템 등 정부 행정망 침투 사례까지 드러나면서 정보보호 문제는 개별 기업의 보안 실패를 넘어 국가 차원의 디지털 신뢰 기반을 위협하는 구조적 리스크로 확대되고 있다.

2025년 대규모 사이버 침해사고들은 발생 경로 및 공격 방식은 상이하나, 기본적인 정보보호 조치와 관리체계가 제대로 작동하지 않았다는 문제가 공통적으로 확인된다. 이는 다수의 침해사고가 AI · 디지털 전환에 따른 해킹 '기법의 고도화'에 기인했다기보다 기본적인 정보보호 '관리 실패'가 반복되면서 구조적 취약점이 누적된 결과임을 시사한다.

1) 과학기술정보통신부·한국인터넷진흥원, 『25년 사이버 위협 하반기 동향 및 26년 전망』, 2026, p.4
2) 박진형, 「작년 사이버침해사고 역대 최대…개인정보 유출發 2차 피해 우려」, 『전자신문』, 2026.1.27.

정보보호 법·제도 전반의 구조적 문제점을 종합적으로 분석하고, 개선방안을 제시한다.

또한 사고 대응 과정에서도 자료 보전 미흡과 실질적 피해보상의 한계가 반복적으로 드러났다. 이는 침해사고의 사전 예방뿐 아니라 사후 대응 및 책임 체계 역시 충분히 작동하지 않았음을 보여주는 것으로, 그 결과 현행 정보보호 관리 · 감독 체계 전반의 실효성에 대해 근본적인 의문이 제기되고 있다.

이에 본 보고서는 2025년에 발생한 침해사고 중 사회적 파급력과 피해 양상·규모 등을 종합적으로 고려하여 7개 주요 침해사고[3]를 선정하여 침해 원인과 문제점을 기준으로 유형화하고, 반복적으로 드러난 정보보호 체계의 구조적 문제점을 '사전 예방 단계'와 '사후 대응 단계'로 구분하여 분석한 뒤, 향후 대응 체계의 개선 방향을 제시하고자 한다.

표 2 2025년 주요 사이버 침해사고 발생 현황

사고	시기	피해 규모	핵심 원인
SKT	4월	• 유심정보 25종 유출(9.82GB, IMSI[4] 기준 약 2,696만건)	• 핵심 계정정보 평문 저장 (암호화 조치 및 관리 부실)
예스24	6월	• 5일간 도서 검색·구매, 전자책 서비스, 공연 예매·취소 등 중단	• 기술지원 종료된 OS 사용
	8월	• 약 7시간 서비스 접속 장애	
SGI 서울보증	7월	• 전산망 마비(보증보험 가입 등 보증서 발급 업무 중단)	• SSL-VPN 장비의 SSH 포트[5]에 대한 무차별 대입 공격 통제 미흡(로그인 시도 횟수 제한 미설정 등)
정부 행정망	7월	• 온나라시스템(정부업무관리시스템) 무단 접속 및 자료 열람 • 일부 부처 자체 전용 시스템 접근	• VPN 및 내부망 접근통제 · 인증체계 미흡
롯데카드	9월	• 200GB 정보 유출(296.9만명의 개인신용정보 포함, 약 28.3만명(9.5%)은 카드비밀번호와 CVC도 유출)	• 보안패치 미적용 서버 장기 운영
KT	9월	• 22,227명의 IMSI, IMEI[6], 전화번호 유출, 무단 소액결제 피해 368명(777건/2.43억원), 감염서버 총 94대, 악성코드 총 103종	• 미사용 펨토셀 인증 · 관리 부실
쿠팡	11월	• 고객 계정 3,367만여 건 유출(내정보 수정 페이지 성명·이메일) • 배송지·주문 목록 페이지 등 조회	• 퇴사자 접근권한 미회수

출처: 민관합동조사단 발표, 보도자료, 언론보도 등을 참고하여 작성
※ 일부 사건은 현재 조사 진행 중인 관계로 향후 조사 결과에 따라 사실관계·피해 규모 및 원인 등이 변경될 수 있음

3) LGU+ 침해사고의 경우 사회적 관심이 컸던 사건이었으나, 서버 폐기 등으로 인해 구체적인 침해 경로와 원인에 대한 분석이 이루어지지 않아 본 보고서의 유형별 분석 대상에는 포함하지 않았다.

4) 가입자 식별번호(International Mobile Subscriber Identity) : 유심 내 저장되며, 통신사가 사용자 식별 시 사용

5) SSL VPN 장비는 원격 사용자가 인터넷을 통해 안전하게 기업 내부 네트워크에 접속할 수 있도록 암호화된 통신 터널을 제공하는 보안 솔루션이고, SSH는 원격 호스트에 접속하기 위해 사용되는 보안 프로토콜이다.

6) 단말기 식별번호(International Mobile Equipment Identity) : 휴대전화 기기 식별 시 사용

Ⅱ 2025년 주요 침해사고의 유형별 구조 분석

2025년 발생한 주요 침해사고는 직접적인 원인에는 차이가 있으나, 그 이면에는 '기본 보안 관리 부실'이라는 공통점이 확인된다. 핵심 정보의 보호 방식, 인증·접속통제 체계, 자산·계정 관리 등에 관한 기본적인 보안 수칙이 현장에서 제대로 작동하지 않았다는 점이다. 이는 개별 기업의 일회적 실수가 아니라, 형식에 치우친 현행 정보보호 관리·점검 체계의 구조적 한계를 보여준다.

이에 본 장에서는 2025년 주요 침해사고에서 반복적으로 나타난 관리 실패의 구조를 유형화함으로써, 향후 정보보호 관리·감독 체계 개선을 위한 분석적 근거를 마련하고자 한다. 주요 침해사고 7건을 침해 원인과 정보보호 체계상의 문제를 기준으로 살펴보면 ① 기본 보호조치 미흡형, ② 자산·계정 관리 실패형, ③ 보안 설계 취약형, ④ 공급망 위협형의 네 가지 유형으로 분류할 수 있다.

표 3 2025년 주요 사이버 침해사고 유형별 구분

유형	특징	해당 사고	원인 및 문제점
기본 보호조치 미흡형	암호화 · 점검 등 최소 보호조치 이행 실패	SKT	• 핵심 계정정보 평문 저장(암호화 조치 및 관리 부실)
		SGI서울보증	• SSL-VPN 장비의 SSH 포트에 대한 무차별 대입 공격 통제 미흡(로그인 시도 횟수 제한 미설정 등)
자산 · 계정 관리 실패형	장기 미사용 정보자산, 퇴사자 계정 등 방치	KT	• 미사용 펨토셀 인증 · 관리 부실
		예스24	• 기술지원 종료된 OS 사용
		롯데카드	• 보안패치 미적용 서버 장기 운영
		쿠팡	• 퇴사자 접근권한 미회수
보안 설계 취약형	인증 · 접속 구조의 설계 취약	정부 행정망	• VPN 및 내부망 접근통제 · 인증체계 미흡
공급망 위협형	외주 장비 · SW 구성요소에 대한 검증 · 관리 미흡	SKT	• 협력업체 공급 SW 보안점검 미흡
		KT	• 협력업체 공급 펨토셀 SBOM 관리체계 부재

출처: 민관합동조사단 발표, 보도자료, 언론보도 등을 참고하여 작성
※ 일부 사건은 현재 조사 진행 중인 관계로 향후 조사 결과에 따라 사실관계·피해 규모 및 원인 등이 변경될 수 있음

가. 기본 보호조치 미흡형

'기본 보호조치 미흡형'은 암호화 등 운영상 기본적으로 요구되는 보안 조치가 제대로 이행되지 않아 공격자의 내부 침투를 허용하는 것으로, SKT와 SGI서울보증 사고를 들 수 있다.

(SKT) 민관합동조사단(이하 "조사단")은 계정정보 관리 부실과 주요 정보 암호화 조치 미흡 등을 사고 원인으로 지적하였다. SKT는 핵심 인증 기반 시스템인 음성통화인증(HSS) 관리서버('21.12.24., 12.30. 감염)의 계정정보를 타 서버에 평문으로 저장하였고, 동 계정정보가 감염 경로에 활용된 것으로 확인되었다. 특히, 유심 인증키(Ki) 값은 유심 복제에 활용될 수 있어 세계 이동통신사업자협회(GSMA)가 암호화를 권고하는 중요 정보임에도 불구하고, 타 통신사들(KT, LGU+)이 암호화하여 저장한 것과 달리, SKT는 평문으로 저장하였다.[7)]

(SGI서울보증) 전세보증 등 국민 생활 밀착 업무에 차질을 초래한 SGI서울보증 사고는 SSL 가상사설망(VPN) 장비의 SSH(Secure Shell, 원격 접속 프로토콜) 서비스 포트를 통해 무작위 로그인을 시도한 것이 원인으로 지적되었다. SSH 무차별 대입 공격을 방어하기 위한 로그인 시도 횟수 제한, 속도 제한(지연 삽입), 다중 인증 등의 보안 조치를 충분히 마련하지 않은 것이 공격에 악용된 것으로 추정된다.[8)]

나. 자산·계정 관리 실패형

'자산·계정 관리 실패형'은 정보자산의 식별과 현황 관리가 제대로 이루어지지 않거나 퇴사자 계정 등이 방치되면서 침해가 발생한 것으로, KT, 예스24, 롯데카드 및 쿠팡 사고를 들 수 있다.

(KT) 주요 문제점으로 펨토셀 보안 관리 부실로 인한 불법 펨토셀 접속 등이 지적되었다. 모든 펨토셀 제품이 동일 제조사의 인증서를 사용하고, 인증 유효기간도 장기(10년)로 설정되어 있었다. 또한 펨토셀 접속 인증과정에서 비정상 IP를 차단하지 않고, 펨토셀 고유번호·설치 지역정보 등이 KT망에 등록된 정보인지에 대한 검증도 이루어지지 않았다.[9)]

(예스24) 기술지원이 종료된 윈도우 운영체제(OS)를 사용한 것이 주요 원인으로 지적되었다. 해당 OS는 공식적인 보안 패치 업데이트 지원을 받을 수 없음에도 불구하고 교체 또는 업그레이드가 이루어지지 않았고, 그 결과 랜섬웨어 감염에 취약한 환경이 유지된 것으로 분석된다.[10)]

(롯데카드) 해커가 오라클 웹로직(Oracle WebLogic) 서버의 원격코드 실행 취약점(인증 없이 원격 실행 가능)을 이용해 "온라인 결제서버(WAS)"에 침입한 뒤 악성 프로그램(웹쉘)[11)]을

7) 과학기술정보통신부 보도자료, 「SK텔레콤 침해사고 최종 조사결과 발표」, 2025.7.4.
8) 강현주·여이레, 「[단독] SGI서울보증 랜섬웨어, 최초 침투 경로는 'SSL-VPN'…로그인 횟수 제동 장치 없었다」, 『보안뉴스』, 2025.7.17.
9) 과학기술정보통신부 보도자료, 「KT, LGU+ 침해사고 최종 조사결과 발표」, 2025.12.29.
10) 조재학·권혜미, 「예스24 '닷새간 먹통 사태' 원인은?…기술지원 끝난 윈도 서버 OS 썼다」, 『전자신문』, 2025.6.17.
11) 웹쉘(Web Shell) : 해커가 웹 서버를 원격으로 제어하기 위해 설치하는 악성 코드

설치해 정보를 유출한 사건이다. 해당 취약점은 2017년 이미 패치가 제공되었음에도,[12] 사용량이 거의 없었던 해외 소규모 페이 서비스를 처리하던 웹로직 서버 1개가 보안 패치 과정에서 누락되면서 취약점이 장기간 방치된 것으로 분석된다.[13] 이는 사용 빈도가 낮은 서버가 관리 범위에서 제외되는 등 자산 식별 및 패치 관리 체계가 제대로 작동하지 않은 데서 비롯된 것으로 볼 수 있다.

(쿠팡) 퇴사자 계정 관리 부실이 대규모 정보 유출로 이어졌다. 공격자(퇴사자)는 재직 당시 관리하던 이용자 인증 시스템의 서명키를 탈취한 후, 이를 활용해 '전자 출입증'을 위·변조하여 정상적인 로그인 절차 없이 쿠팡 인증 체계를 통과하였다. 쿠팡이 관리하는 서명키는 '전자 출입증' 발급에 사용되는 도구인 만큼 퇴사할 경우 해당 서명키를 더 이상 사용하지 못하도록 갱신되어야 하나, 관련 체계 및 절차가 미비하였다.[14]

다. 보안 설계 취약형

'보안 설계 취약형'은 인증 · 접속 구조 등의 설계 단계에서 보안 고려가 충분히 반영되지 않아 구조적 취약점이 내재된 것으로, 정부 행정망 사고를 들 수 있다.

(정부 행정망) 국가정보원 발표(2025.10.)에 따르면, 해커는 다양한 경로로 공무원 행정업무용 인증서(GPKI) · 패스워드 등을 확보하여 합법적 사용자로 위장해 행정망에 접근한 것으로 밝혀졌다. 해커는 인증서(6개) 및 국내외 IP(6개)를 이용해 2022년 9월부터 2025년 7월까지 행정안전부가 재택근무를 위해 사용하는 원격접속시스템(G-VPN)을 통과해 온나라시스템에 접속해 자료를 열람했다. 또한 국가정보원은 해커가 일부 부처가 자체 운영 중인 전용 시스템에도 접근한 사실을 확인했다고 밝혔다.[15]

해당 사고는 정부 원격접속시스템에 본인확인 등 인증체계가 미흡하고 온나라시스템의 인증 로직이 노출되면서 복수기관에 접속이 가능하였으며 각 부처 전용 서버에 대한 접근통제가 미비한 것이 사고 원인으로 드러났다.[16]

이는 원격접속시스템과 내부 행정망 간의 신뢰 구조 및 권한 분리 체계가 구조적으로 취약한 상태였음을 의미하며, 보안 설계 단계에서 기관 간 경계 설정과 접근 권한 통제가 충분히 강화되지 못한 측면이 있었음을 시사한다.

12) 김민석, 「CVC 번호 유출 롯데카드 해킹…'원격취약점·웹쉘 복합공격' 추정」, 『뉴스1』, 2025.9.18.
13) 유진호, 「2025년 주요 사이버 침해사고 및 시사점」, 2025년 주요 침해사고 진단과 개선과제 간담회 자료, 국회입법조사처, 2026, p.15.
14) 과학기술정보통신부 보도자료, 「쿠팡 전 직원에 의한 정보통신망 침해사고 조사 결과 발표」, 2026.2.10.
15) 국가정보원 보도자료, 「국정원, 온나라시스템 등에 대한 정교한 위장침투에 대응」, 2025.10.17.
16) 국가정보원 보도자료, 위의 글.

라. 공급망 위협형

'공급망 위협형'은 협력업체로부터 공급받은 소프트웨어·장비에 대한 보안 검증과 관리가 미흡해 외부 위험이 내부 시스템으로 유입된 것으로, SKT와 KT 사고를 들 수 있다.

(SKT) 조사단은 SKT가 협력업체로부터 공급받은 소프트웨어를 면밀히 점검하지 않고 내부 서버 88대에 설치하여 해당 소프트웨어에 탑재되어 있었던 악성코드가 유입되었음을 지적하였다. 다만, 유입된 악성코드가 SKT 시스템에서 실행된 흔적은 확인되지 않았다.[17)]

(KT) 조사단은 KT 사고와 관련해서도 KT가 협력업체로부터 공급받는 펨토셀 장비에 대한 표준 보안 규격서 및 소프트웨어 패키지에 대한 SBOM(Software Bill of Materials : 소프트웨어의 구성 컴포넌트에 관한 메타정보)[18)] 관리체계가 부재함을 확인하였다.[19)]

이러한 사례들은 협력업체를 통한 공급망 관리의 취약성이 잠재적인 위협 요인으로 작동할 수 있음을 보여주며, 공급망 전반에 대한 체계적인 보안 관리 강화의 필요성을 시사한다.

Ⅲ 사전 예방 단계의 개선과제

사이버 침해사고는 일단 발생한 이후에는 피해 확산을 완전히 차단하거나 원상회복하기가 어렵다는 점에서, 사고 이전 단계에서의 예방 체계 구축이 무엇보다 중요하다. 그러나 2025년 주요 침해사고는 앞서 살펴본 바와 같이 사전 예방 체계가 충분히 작동하지 못했음을 드러냈다. 특히 기본 보호조치의 부재, 정보자산·계정에 대한 관리 미흡, 침해를 전제로 하지 않은 보안 설계, 외부 공급망에 대한 통제 미흡은 개별 사고의 직접적 원인으로 작용하거나, 침해 발생 가능성을 구조적으로 증대시키는 요인으로 확인되었다.

이에 앞서 유형화한 분석 결과를 바탕으로, 사전 예방 역량을 실질적으로 강화하기 위한 개선과제로 제로트러스트의 확산, 취약점 신고제도의 활성화, 공급망 보안 강화, 보안인증 제도의 실효성 제고 방안을 제안한다.

17) 과학기술정보통신부 보도자료, 『SK텔레콤 침해사고 최종 조사결과 발표』, 2025.7.4.
18) SBOM은 SW 개발 全 과정의 구성내역 상세명세서로서, 분석을 통해 취약점 발견 및 SW 보안성 확보가 가능하다.(과학기술정보통신부, 「정보보호산업의 글로벌 경쟁력 확보 전략」, 2023.).
19) 과학기술정보통신부 보도자료, 「KT, LGU+ 침해사고 최종 조사결과 발표」, 2025.12.29.

가. 제로트러스트 확산

2025년 주요 침해사고들은 신뢰를 전제로 한 기존 보안 체계가 침해 상황에서 효과적으로 작동하지 못했음을 보여준다. 특히 정상 사용자·계정·장비로 인식된 접근이 반복적으로 악용되면서, 사고 초기 단계에서의 침투 차단과 이상 징후 탐지에 한계가 드러났다. 이에 대한 해법으로 '제로트러스트 보안 모델'의 확산 필요성이 지속적으로 제기되고 있다. 제로트러스트는 정보 시스템 등에 대한 접속요구가 있을 때 네트워크가 이미 침해된 것으로 간주하고, "절대 믿지 말고, 계속 검증하라"는 보안개념이다.

실제로 조사단은 SKT와 KT 사고 조사 결과 발표에서 보안관리 미흡에 대한 개선 방안으로 제로트러스트 도입을 제시하였으며, 쿠팡 사고 관련 국회 현안질의(2025.12.2.)에서도 정부가 대형 플랫폼 기업을 중심으로 제로트러스트 원칙이 이행되도록 노력할 필요가 있다는 의견이 제시되었다.[20]

이처럼 제로트러스트 도입 필요성이 지속적으로 강조되고 있음에도 불구하고 현재 제로트러스트 보안에 관해서는 가이드라인 중심으로 규정되어 있어 법적 구속력이 부족하며, 이로 인해 현장 적용과 확산에 한계가 있는 상황이다.[21]

> 제로트러스트 보안 관련 법적 근거 마련을 고려할 필요가 있다.

대규모 사이버 침해사고의 예방과 재발 방지를 위하여 제로트러스트 보안 모델의 도입을 제도적으로 뒷받침할 수 있도록 일정 범위에 대한 의무화와 함께 재정적 지원 근거를 마련하는 법제화를 검토할 필요가 있다. 예컨대, 공공분야나 주요정보통신기반시설 등에 대해서는 「전자정부법」이나 「정보통신기반 보호법」을 개정하여 제로트러스트 보안 도입을 의무화하고, 민간 영역에 대해서는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 "정보통신망법")을 개정하여 재정적 지원 근거 등을 마련하는 방안을 고려할 수 있다.[22]

나. 취약점 신고제도 활성화

2025년 대규모 침해사고는 보안 취약점이 적시에 발견·조치되지 못하거나 기존의 취약한 보안 관리 상태가 누적된 상황에서 발생하였다는 공통점을 보이고 있다. 이에 보안 취약점을 조기에 발굴하고 신속한 시정을 유도하기 위하여 취약점 신고제도를 활성화할 필요가 있다.

정보통신망법 제47조의6 및 동법 시행령 제55조의6에 따라 보안 취약점을 신고한 자에게 정부가 포상금을 지급하는 '정보보호 취약점 신고포상제'가 운영되고 있다.[23] 그러나 현행

20) 국회사무처, 「제429회국회(정기회) 과학기술정보방송통신위원회회의록」, p.119.

21) 미국 보안 기업 옥타에 따르면 제로트러스트 보안을 진행 중인 한국 기업은 4%에 불과한 것으로 나타났다(김기찬, 「"제로트러스트 보안 진행중 한국기업 4% 불과"」, 『ZDNET Korea』, 2025.10.30.).

22) 제22대 국회에는 정보통신서비스 제공자가 제로트러스트 보안체계를 구축 · 운영하도록 노력할 의무와 정부의 제로트러스트 시책 수립·추진 근거, 중소기업에 대한 지원 근거 등을 규정하는 정보통신망법 개정안이 과학기술정보방송통신위원회에 계류되어 있다(최민희의원 대표발의, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률 일부개정법률안」(의안번호 2215639), 2025.12.26.).

정보보호 취약점 신고 포상금 상한을 인상하고, 기업의 자발적 취약점 발견·개선 등에 대한 인센티브 제도 도입을 고려할 필요가 있다.

포상 수준(5만원 이상 1천만원 이하)은 신규 취약점 발굴·신고를 적극적으로 유인하기에 충분하지 않다는 지적이 제기되고 있으므로, 제도의 실효성 제고를 위해 포상금 상한을 인상하는 방안을 검토할 수 있다.[24)]

아울러, 기업의 자발적 취약점 발견 및 개선 참여를 실질적으로 유도하기 위하여 인센티브 제도 도입이 필요하다는 의견도 있다.[25)] 기업의 취약점 신고포상제 운영 및 개선 실적을 「개인정보 보호법」 상 과징금 감경과 연계하는 방안 등을 고려할 필요가 있다.[26)]

다. 공급망 보안 강화

SKT 및 KT 사고와 관련하여서는 공통적으로 소프트웨어(SW) 공급망 보안 문제가 지적되었으며, 이에 따라 SW 공급망 보안을 구조적으로 강화할 필요성이 제기된다.

유럽 등 주요국은 SW 공급망 공격에 체계적으로 대응하기 위해 SBOM 제도 도입을 추진하고 있다. 유럽연합(EU)은 「사이버 복원력법(Cyber Resilience Act, CRA)」에 시장에 유통되는 소프트웨어, 하드웨어 제품에 대해 개발·유지보수·보안 업데이트 의무를 부과하고, 기술문서에 SBOM 또는 이와 동등한 수준의 구성요소 투명성 입증 자료를 포함하도록 규정했다.[27)] 이러한 주요국의 입법 동향과 비교할 때, 국내에서는 SBOM의 도입과 확산이 아직 제한적인 수준에 머물러 있는 상황이다.[28)]

우선 공공부문에 SBOM 도입을 추진하고, 민간부문에서는 단계적 적용을 검토할 필요가 있다.

이에 우리나라에서도 우선 공공부문을 중심으로 SBOM 도입을 의무화하고, 민간부문에서는 금융·의료 등 민감한 개인정보를 취급하는 분야를 대상으로 단계적 적용을 검토할 필요가 있다는 의견이 제기된다.[29)]

다만, SBOM 도입이 의무화되면 SW의 취약점 감소 등 긍정적 효과가 기대되는 반면, 안전한 SW 공급망 구축을 위해 추가적인 시간과 비용 투자가 요구되어 SW 개발 비용이 증대되는 등 SW 산업에 부담으로 작용할 가능성도 제기되므로[30)], 의무화의 범위 등에 대해서는 산업계와의 충분한 논의 및 의견수렴이 필요할 것으로 보인다.

23) 2012년 10월부터 운영되고 있으며, 2022년 6월 시행령에 있는 포상금 지급 근거 규정을 보다 구체화하여 법률에 규정하였다. 포상금 수준은 도입 당시와 동일하게 현재까지 유지되고 있다.

24) 유진호, 앞의 글, p.22.

25) 박광하, 「보안 전문가들 "기업·기관 자발적 보안 활동 '버그바운티' 활성화 필요"」, 『뉴스윅스』, 2025.9.24.

26) 최근 국가 인공지능전략위원회는 보안 취약점 신고·조치·공개 제도 도입 단계별 이행안(로드맵)을 발표하였는데(2026.2.25.), 민간의 경우 보안인증 가점, 공공 조달, 「개인정보 보호법」에 따른 사고시 과징금 감경 요소에 반영 등을 통해 참여를 유도한다는 내용이 포함되었다.

27) 한국정보보호산업협회, 『국·내외 SW공급망보안 현황 및 SBOM 도구 실증 결과보고서』, 2025, p.12.

28) 정부는 2025년 10월 '범부처 정보보호 종합대책 발표'에서 공공분야에 사용되는 IT 시스템·제품에 대해 SW 구성요소(SBOM)의 제출을 2027년까지 제도화하겠다는 계획을 밝혔다.

29) 유진호, 앞의 글, p.28.

30) 이만희, 「열린 SW 생태계를 위한 과제: 소프트웨어 공급망 보안 강화 필요성과 의의」, 『TTA저널』 206호, 2023, p.34.

라. 보안인증 제도 실효성 제고

SGI서울보증과 정부 행정망 사고를 제외한 5건의 침해사고에서 해당 기업들은 ISMS 또는 ISMS-P 인증[31]을 취득한 상태였음에도 중대한 침해사고를 예방하지 못하였다. 이는 인증 보유 여부와 실제 보안 역량 간에 상당한 괴리가 존재함을 보여주는 것으로, 현행 인증제도가 형식적·절차적 요건 충족에 치중된 나머지 실질적인 위험 관리와 사고 예방 기능을 충분히 수행하지 못하고 있다는 근본적인 한계를 드러낸다.

이러한 문제 인식을 바탕으로, 국회는 2026년 3월 12일 고위험 사업자에 대한 인증 기준 강화, 현장심사 확대, 중대한 위반 사항 발생 시 인증 취소 등을 주요 내용으로 하는 정보통신망법 개정안(대안)을[32] 의결하였다. 이번 개정으로 인증의 형식화를 방지하고 사후 관리와 책임성을 강화함으로써 인증제도가 실질적인 보안 수준 제고 수단으로 기능할 것으로 기대된다.

> 보안 인증 기준 및 심사 강화와 더불어 의무 대상 확대를 검토할 필요가 있다.

한편, 인증 기준 및 심사 강화 등과는 별도로 의무대상자 선정 기준 자체에 대한 재검토도 필요하다. 정보통신망법 시행령 제49조제2항제2호에 따라 금융회사는 ISMS 인증 의무 대상에서 제외되어 있으나,[33] SGI서울보증 사고와 관련하여 민감한 개인정보 취급 및 국민 생활과 직결된 서비스를 제공하는 분야임에도 불구하고 인증 취득이 의무화되지 않은 제도적 사각지대가 존재한다는 비판이 제기된 만큼,[34] 금융회사를 인증 의무 대상에 포함하는 방안을 검토할 필요가 있다. 아울러, 현재 대다수 공공기관도 인증 의무 대상에서 제외되어 있으므로 고위험 정보를 처리하는 공공기관 역시 ISMS 인증 의무 대상에 포함할 필요가 있다.[35]

31) ISMS-P 인증 제도는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조 및 「개인정보 보호법」 제32조의2에 따라 정보통신망의 안정성 확보 및 개인정보 보호를 위해 조직이 수립한 일련의 조치와 활동이 인증기준에 적합함을 인증기관이 평가하여 인증을 부여하는 제도이다. ISMS-P 인증에는 정보보호 중심의 'ISMS 인증'(과학기술정보통신부 소관)과 개인정보의 흐름과 정보보호 영역을 모두 인증하는 'ISMS-P 인증'(개인정보보호위원회 소관) 두 가지 유형이 있다.

32) 과학기술정보방송통신위원장 제안, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률 일부개정법률안(대안)」(의안번호 2214896), 2025.12.4.

33) 2016년 규제개혁위원회 단계에서 금융회사는 타법과의 중복·과잉규제 등으로 판단하여 의무대상에서 제외하는 것으로 의결되었다(과학기술정보통신부 제출자료, 2026.2.12.).

34) 이승엽, 「"터질 게 터졌다" 랜섬웨어 타깃 된 SGI서울보증… 정보보호 인증도 안 받아」, 『한국일보』, 2025.7.15.

35) 황현희·강은수, 「한국연구재단 해킹 사건을 계기로 본 공공기관 정보보호 강화방안」, 『이슈와 논점』 제2387호, 국회입법조사처, 2025.

IV 사후 대응 단계의 개선과제

사이버 침해사고는 보호조치를 지속적으로 강화하더라도 기술적 복잡성과 외부 위협의 진화 속도를 고려할 때 완전히 배제하기 어려운 측면이 있다. 따라서 사고 발생 이후의 사후 대응 체계는 피해 확산을 최소화하고, 침해 원인을 정확히 규명하며, 책임을 귀속하는 데 있어 중요한 의미를 가진다. 자료가 적시에 완전하게 보전되지 않을 경우 유출 경위와 범위를 정확히 평가하기 어렵고, 이는 이후 행정제재·형사처벌·손해배상 등 후속 법집행 전반의 실효성을 저해한다. 또한 공격자에 대한 실효적 제재의 한계와 피해자 구제의 구조적 한계는 침해행위로 인한 이득을 높여 반복적 공격을 유인하는 요인으로 작용한다.

따라서 사후 대응 단계는 단순한 사고 처리를 넘어, 침해사고 경험이 예방으로 이어지는 선순환 구조를 형성해야 한다. 이를 위해서는 기업의 리스크 인식을 제고하고 침해행위에 따른 대가를 엄중히 하는 방향으로 제도를 정비할 필요가 있다. 구체적인 개선과제로 자료 보전 의무 강화, 해커 처벌 및 범죄수익 환수 체계 정비, 피해자 보상 체계 확충 방안을 제안한다.

가. 자료 보전 의무 강화

2025년 침해사고들의 사후 대응 과정에서 피해 기업들이 디지털 증거를 체계적으로 보전하지 않아 조사·수사에 난항을 겪는 일이 반복되었다. SKT는 과학기술정보통신부가 침해사고 원인 분석을 위해 자료 보전 명령을 하였음에도 불구하고 관련 서버를 임의로 조치하여 디지털 포렌식이 불가능한 상태로 조사단에 제출하였다.[36] KT는 문제가 된 서버를 폐기하였다고 답변하면서 폐기 시점을 허위 제출하고 폐기 서버의 백업 로그가 있음에도 불구하고 이를 한동안 조사단에 보고하지 않았다.[37] LGU+는 한국인터넷진흥원(KISA)으로부터 침해사고 정황을 안내받은 이후 침해 경로로 의심되는 네트워크 경로상의 주요 서버 전부에 대해 OS 재설치 또는 폐기를 단행하여 조사 자체가 불가능하게 만들었으며,[38] 쿠팡은 조사단 및 수사기관과 사전 협의 없이 독자적으로 유출자를 특정하고 증거를 수집한 뒤 자신이 선정한 외부업체에 이를 전달하여 자체적으로 포렌식을 수행하였다.[39]

이러한 사례들은 제재, 손해배상, 경영진 책임규명 등 침해사고의 법적·정책적 사후대응의 전제가 되는 사실인정 기반 자체를 약화시키는 문제를 유발한다. 디지털 증거는 특성상 변경·멸실이 용이

36) 과학기술정보통신부 보도자료, 「SK텔레콤 침해사고 최종 조사결과 발표」, 2025.7.4.
37) 과학기술정보통신부 보도자료, 「KT, LGU+ 침해사고 최종 조사결과 발표」, 2025.12.29.
38) 과학기술정보통신부 보도자료, 「KT, LGU+ 침해사고 최종 조사결과 발표」, 2025.12.29.
39) 과학기술정보통신부 보도 설명자료, 「쿠팡의 개인정보 유출 조사 관련 배포 자료는 민관합동조사단의 확인이 필요한 사항입니다」, 2025.12.25.; 개인정보보호위원회 보도자료, 「개인정보위, 쿠팡의 자체조사 결과 홈페이지 공지 중단 등 촉구」, 2026.1.14.

하고 수집 시점부터 종결까지 동일성을 유지하는 것이 핵심이므로, 자료 보전은 조사·수사 및 이후 법집행의 필수적인 전제조건이다.

그러나 현행 법체계는 자료보전 의무의 실효성이 미흡하다. 현재는 침해사고 발생 시 과학기술정보통신부장관이 명한 자료 보전 의무를 위반한 경우 2년 이하의 징역 또는 2천만 원 이하의 벌금에 처할 수 있고(정보통신망법 제48조의4제5항 및 제73조) 경우에 따라 위계에 의한 공무집행방해로 형사처벌을 적용할 수 있다(「형법」 제137조). 그러나 현행 규정은 과학기술정보통신부장관의 명령이 있어야 자료보전 의무가 발생하므로 그 전에 이루어지는 자료 훼손 행위에 적용하기 어렵다는 점, 징역과 같은 자유형은 기업에게 부과할 수 없고 벌금은 그 액수가 미미하여 실질적인 억지력이 부족하다는 점의 문제가 있다.

> 침해 인지 즉시 자료 보전을 의무화하고, 관련 의사결정의 책임을 명확히 하며, 보전 위반으로 조사 불능 시 기업 귀책을 추정하는 방안을 검토할 수 있다.

이러한 문제를 해소하기 위해서는 다음과 같은 개선이 필요하다. 첫째, 침해 정황을 인지한 시점부터 자료 보전 의무가 즉시 발동되도록 해야 한다. 둘째, 서버 재설치·폐기 등 자료에 영향을 미치는 조치를 취하는 경우 이사회 및 정보보호 최고책임자(CISO)에 대한 보고와 의사결정 기록을 의무화하여 해당 결정에 대한 책임이 상위 의사결정자에게 귀속되도록 해야 한다. 셋째, 자료보전 의무 위반으로 인해 조사 불능이라는 결과가 발생한다면 기업의 귀책사유로 인해 침해사고가 발생한 것으로 법률상 추정하는 규정을 두어 자료를 충분히 보전하도록 유인하는 방안을 검토할 수 있다.

나. 해커 처벌 및 범죄수익 환수 체계 정비

기업의 침해사고 예방 의무 강화와 병행하여, 공격 주체인 해커에 대한 실질적인 억지력을 확보하는 것 역시 중요하다. 최근에는 다크웹을 통한 공격 도구의 상업화(Ransomware as a Service)와 가상자산을 활용한 자금 세탁의 용이성으로 인해 해킹 범죄의 진입 장벽이 현저히 낮아졌고, 이에 따라 침해사고의 빈도와 규모도 확대되는 경향을 보이고 있다.

현행 법체계상 정보통신망 침입·악성프로그램 유포(정보통신망법 제48조·제70조의2·제71조제1항제11호), 데이터 손괴·은닉(「형법」 제366조), 국가기반시설 공격(「정보통신기반 보호법」 제12조·제28조) 등에 대하여 형사처벌 규정이 존재한다. 그러나 사이버범죄의 초국가적·분산적 특성으로 인해 행위자 특정과 검거가 쉽지 않고, 부과되는 벌금 역시 실제 범죄 수익 규모에 비해 낮은 수준에 머물러 있어[40] 체감 가능한 억지력을 확보하기에는 한계가 있다.

따라서 해커의 침해 활동을 효과적으로 억제하기 위해서는 국제 공조를 통한 검거 가능성 제고와 범죄수익 환수 체계의 정비를 병행할 필요가 있다. 우선 국제 공조 수사의 실효성을 확보하기 위하여, 「형사소송법」 등에 해외 서버에 저장된 전자증거에 대한 보전 요청 제도의 도입, 외국 수사기관이 적법하게 수집한 증거의 국내 형사절차상 증거능력 판단 기준의 명문화, 외국 수사

40) 징역형을 제외하고 벌금형만을 보면, 정보통신망 침입·악성프로그램 유포는 5천만원 또는 7천만원 이하의 벌금, 데이터 손괴·은닉은 700만원 이하의 벌금, 국가기반시설 공격은 1억원 이하의 벌금에 해당한다. 한편 IBM의 「데이터 침해 비용 보고서(Cost of a Data Breach Report)」에 따르면, 16개국 553건 이상의 침해 사례를 분석하면 2025년 기준 대규모 조직의 데이터 침해 1건당 평균 피해액은 444만 달러(약 66억 원)에 달한다.

기관과의 합동수사 및 공동조사에 대한 법적 근거 마련 등을 검토할 필요가 있다.[41)]

국제공조 수사 및 범죄수익 환수 제도를 정비하여 해커의 침해활동을 억제하여야 한다.

아울러 범죄수익 환수 제도의 보완도 중요한 과제이다. 현행 「범죄수익은닉의 규제 및 처벌 등에 관한 법률」상 몰수·추징 대상 범죄의 범위에 정보통신망 침입 등으로 인한 수익은 포섭되지 않으므로,[42)] 경제적 동기를 차단하기 위해서는 해킹으로 인한 범죄수익을 몰수·추징할 수 있는 방안을 검토할 필요가 있다.

다. 피해자 보상 체계 확충

사이버 침해사고 대부분은 개인정보 유출을 수반한다. 개인정보 유출로 인한 개인적 피해는 통상 소액에 그치는 경우가 많아, 피해자 개인이 소송을 제기하거나 입증을 다투는 데 필요한 비용·시간 대비 기대회수가 낮다. 그 결과 권리행사가 위축되고, 침해가 발생하더라도 실질적인 구제로 이어지지 못하는 구조가 반복된다. 이렇게 보상받지 못하는 침해가 누적되면 사회 전반의 개인정보 보호 감수성은 낮아지고 이는 개인정보처리자의 예방 투자 유인을 약화시키는 방향으로 작용한다. 책임이 충분히 귀속되지 않는 환경은 기업 내부의 리스크 관리 체계 개선을 지연시키는 요인이 될 수 있다. 따라서 피해자 보상 강화는 개별 피해의 회복에 그치는 문제가 아니라 개인정보처리자의 책임성을 제고하고 재발 방지를 유도하는 선순환 구조를 형성하기 위해 필요하다.

피해자 보상 강화는 기업 내부의 리스크 관리 체계 개선을 촉진한다. 집단소송제 등을 종합적으로 검토하여야 한다.

개인정보 침해로 인한 소액·다수 피해는 개별소송에 소요되는 시간·부담 대비 얻을 수 있는 실익이 한정적이어서 구제가 제대로 이루어지지 않는 문제가 반복되고 있다. 「개인정보 보호법」에서 다수의 소액 피해자를 구제하기 위해 집단분쟁조정과 단체소송을 두고 있으나, 집단분쟁조정제도는 당사자 일방인 개인정보처리자의 불응으로 절차가 무력화될 수 있고[43)] 단체소송은 역시 금지·중지 청구에 한정되고 손해배상 청구는 허용되지 않아[44)] 실질적 권리 구제에 한계가 있다고 평가된다. 또한 과징금 제도는 제재적 성격이 강하여 피해자에게 보상으로 환원되지 않는다는 점에서 한계를 가진다.

41) 진우경·권헌영, 「UN 사이버범죄협약의 초안과 국내법의 비교에 관한 연구」. 『치안정책연구』 제37권 제4호, 경찰대학 치안정책연구소, 2023.

42) 「범죄수익은닉의 규제 및 처벌 등에 관한 법률」은 범죄수익, 범죄수익에서 유래한 재산 등을 몰수하도록 규정한다(제8조제1항). '동법 제2조제2호는 "범죄수익"을 ①중대범죄에 해당하는 범죄행위에 의하여 생긴 재산 또는 그 범죄행위의 보수(報酬)로 얻은 재산, ②「성매매알선 등 행위의 처벌에 관한 법률」 제19조제2항제1호의 죄와 관련된 자금 또는 재산, ③「폭력행위 등 처벌에 관한 법률」 제5조제2항 및 제6조(제5조제2항의 미수범만 해당한다)의 죄와 관련된 자금 또는 재산 등으로 나열하여 규정하고 있는데(제2조제2호) 사이버 범죄로 인한 수익은 이에 포함되지 않는다.

43) 고형석, 「집단적 피해와 집단분쟁조정제도에 관한 연구」, 『비교사법』 제25권 제2호, 한국사법학회, 2018, 476면.

44) 황창근, 「개인정보 보호 관련 분쟁해결방안 고찰 – 개인정보단체소송을 중심으로」, 『공법연구』 제41집 제4호, 한국공법학회, 2013, 253면.

이에 피해자 보상을 강화하기 위해 집단소송제[45], 공중피해보상조치[46], 동의의결[47]등을 종합적으로 검토할 필요가 있다.[48] 손해배상·집단구제의 현실적 가능성이 높아질수록 경영진의 리스크 인식은 강화되고, 이는 정보보호 체계 고도화와 보안 투자 확대라는 예방적 효과로 이어질 것이다.

V 정부와 국회의 역할: 사후조사를 넘어서는 선제적 대응

앞서 살펴본 유형별 구조 분석 결과에 따르면, 2025년 주요 침해사고에서 공통적으로 드러난 취약점은 기본적인 정보보호 관리가 제대로 이행되지 않았다는 점이다. 이는 기업의 보안 관리 미흡과 동시에 정보보호 관리·점검 체계가 현장에서 제대로 작동하도록 관리·감독해야 할 정부의 역할 역시 충분히 이루어지지 못했음을 시사한다. 향후 이러한 문제가 개선되지 않는다면 2026년에도 전년도와 같은 대규모 사이버 침해사고가 반복될 가능성을 배제하기 어렵다.

반복되는 침해사고를 근본적으로 방지하기 위해서는 정부가 단순한 심판자나 사후 조사기관의 역할에 머무르기보다 예방 단계에서의 관리·감독 기능을 보다 적극적으로 수행할 필요가 있다. 정부는 작년 대규모 침해사고와 관련하여 다양한 대응 대책을 발표해 왔으나, 이러한 대책이 일회성에 그치지 않고 정보보호 관리체계의 실질적인 제도 개선으로 이어질 수 있도록 노력하여야 할 것이다.

국회 역시 정부가 정보보호 관리·점검 기능을 제대로 수행하고 있는지 지속적으로 감독할 필요가 있다. 아울러 앞서 제기한 입법 과제와 관련된 법안(정보통신망법, 「개인정보 보호법」, 「형사소송법」 개정안 등)이 과학기술정보방송통신위원회, 정무위원회, 법제사법위원회 등 여러 상임위원회에 계류되어 있는 만큼, 각 상임위원회가 관련 입법을 신속히 추진할 필요가 있다. 이를 통해 국가 차원의 사이버 안전과 디지털 신뢰 기반을 강화해 나갈 수 있을 것으로 기대된다.

45) 공통의 피해자들을 대표하는 자가 소를 제기하여 판결을 받으면 그 판결의 효력이 모든 피해자들에게 미치게 하는 제도를 말한다. 한편 판결의 효력을 신청한 자에게만 미치게 하는 방식도 있다.

46) 정부가 다수의 국민이나 소비자에게 발생한 피해를 복구하기 위하여 행정적·사법적 절차를 통해 위법행위로 취득한 부당이익을 환수하고 이를 피해자에게 환급 또는 보상하는 제도를 말한다(설민수, 「다수 피해자 구제를 위한 집단소송의 대안으로서 미국의 독립규제행정기관의 공중피해보상조치의 현황과 한국에의 도입가능성 – 연방증권거래위원회의 경우를 중심으로 –」, 『법조』 통권 720호, 사단법인 법조협회, 2016, pp.185-194.).

47) 규제당국의 조사나 심의를 받고 있는 사업자가 스스로 소비자 피해구제, 원상회복 등 자진 시정방안을 제안하면, 이해관계인 등의 의견수렴을 거쳐 사업자가 제안한 시정방안이 타당하다고 인정되는 경우 위법 여부를 확정하지 않고 사건을 종결하는 절차를 말한다(공정거래위원회 누리집 정책/제도 「동의의결」 참고. 〈https://www.ftc.go.kr/www/contents.do?key=5217〉).

48) 박소영, 「통신사 해킹 등 개인정보 침해 피해자 구제 : 집단소송제와 공중피해보상조치·동의의결제 방안」, 『NARS 현안분석』 제372호, 국회입법조사처, 2025.

참고문헌

- 강현주·여이레, 「[단독] SGI서울보증 랜섬웨어, 최초 침투 경로는 'SSL-VPN'…로그인 횟수 제동 장치 없었다」, 『보안뉴스』, 2025.7.17.
- 개인정보보호위원회 보도자료, 「개인정보위, 쿠팡의 자체조사 결과 홈페이지 공지 중단 등 촉구」, 2026.1.14.
- 고형석, 「집단적 피해와 집단분쟁조정제도에 관한 연구」, 『비교사법』 제25권 제2호, 한국사법학회, 2018.
- 과학기술정보통신부 보도 설명자료, 「쿠팡의 개인정보 유출 조사 관련 배포 자료는 민관합동조사단의 확인이 필요한 사항입니다」, 2025.12.25.
- 과학기술정보통신부·한국인터넷진흥원, 『25년 사이버 위협 하반기 동향 및 26년 전망』, 2026.
- 과학기술정보통신부 보도자료, 「KT, LGU+ 침해사고 최종 조사결과 발표」, 2025.12.29.
- 과학기술정보통신부 보도자료, 「SK텔레콤 침해사고 최종 조사결과 발표」, 2025.7.4.
- 과학기술정보통신부 보도자료, 「쿠팡 전 직원에 의한 정보통신망 침해사고 조사 결과 발표」, 2026.2.10.
- 과학기술정보통신부 제출자료, 2026.2.12.
- 과학기술정보통신부, 「정보보호산업의 글로벌 경쟁력 확보 전략」, 2023.
- 국가정보원 보도자료, 「국정원, 온나라시스템 등에 대한 정교한 위장침투에 대응」, 2025.10.17.
- 국회사무처, 「제429회국회(정기회) 과학기술정보방송통신위원회회의록」.
- 김기찬, 「"제로트러스트 보안 진행중 한국기업 4% 불과"」, 『ZDNET Korea』, 2025.10.30.
- 김민석, 「CVC 번호 유출 롯데카드 해킹…'원격취약점·웹쉘 복합공격' 추정」, 『뉴스1』, 2025.9.18.
- 박광하, 「보안 전문가들 "기업·기관 자발적 보안 활동 '버그바운티' 활성화 필요"」, 『뉴스웍스』, 2025.9.24.
- 박소영, 「통신사 해킹 등 개인정보 침해 피해자 구제 : 집단소송제와 공중피해보상조치·동의의결제 방안」, 『NARS 현안분석』 제372호, 국회입법조사처, 2025.
- 박진형, 「작년 사이버침해사고 역대 최대…개인정보 유출發 2차 피해 우려」, 『전자신문』, 2026.1.27.
- 설민수, 「다수 피해자 구제를 위한 집단소송의 대안으로서 미국의 독립규제행정기관의 공중피해 보상조치의 현황과 한국에의 도입가능성 - 연방증권거래위원회의 경우를 중심으로 -」, 『법조』 통권 720호, 사단법인 법조협회, 2016.
- 유진호, 「2025년 주요 사이버 침해사고 및 시사점」, 2025년 주요 침해사고 진단과 개선과제 간담회 자료, 국회입법조사처, 2026.
- 이만희, 「열린 SW 생태계를 위한 과제; 소프트웨어 공급망 보안 강화 필요성과 의의」, 『TTA저널』 206호, 2023.
- 조재학·권혜미, 「예스24 '닷새간 먹통 사태' 원인은?...기술지원 끝난 윈도 서버 OS 썼다」, 『전자신문』, 2025.6.17.
- 진우경·권헌영, 「UN 사이버범죄협약의 초안과 국내법의 비교에 관한 연구」. 『치안정책연구』 제37권 제4호, 경찰대학 치안정책연구소, 2023.
- 한국정보보호산업협회, 『국·내외 SW공급망보안 현황 및 SBOM 도구 실증 결과보고서』, 2025.
- 황창근, 「개인정보 보호 관련 분쟁해결방안 고찰 - 개인정보단체소송을 중심으로」, 『공법연구』 제41집 제4호, 한국공법학회, 2013.
- 황현희·강은수, 「한국연구재단 해킹 사건을 계기로 본 공공기관 정보보호 강화방안」, 『이슈와 논점』 제2387호, 국회입법조사처, 2025.
- 공정거래위원회뉴리집정책/제도「동의의결」참고〈https://www.ftc.go.kr/www/contents.do?key=5217〉.

국민을 지키는 미래로 나아가는 국회

국회입법조사처
nars.go.kr

기본부터 다시 갖춰야 할 정보보호 체계

2025년 사이버 침해사고 유형 분석 및 제도 개선과제

국회입법조사처
NATIONAL ASSEMBLY RESEARCH SERVICE

07233 서울시 영등포구 의사당대로 1 국회입법조사처 02-6788-4510
발행처 | 국회입법조사처 **발행인** | **이관후** 국회입법조사처장
저 자 | **강은수** 사회문화조사실 과학방송통신팀 입법조사관
02-6788-4712 eunsu@assembly.go.kr
박소영 사회문화조사실 과학방송통신팀 입법조사관, 변호사
02-6788-4713 sypark@assembly.go.kr

발간등록번호 31-9735044-001621-14
ISSN 2586-565X