

1988 — 2026

한국 사이버보안의 역사

사고가 만든 제도, 제도가 남긴 과제

바이러스 대응에서 AI 거버넌스까지, 38년의 궤적



OVERVIEW

38년을 관통하는 세 가지 흐름

01

사고 대응형 입법

대형 침해사고가 터진 뒤에야 법과 기관이 만들어졌다.

1·25 대란 → 국가사이버안전센터,
카드 3사 유출 → 개인정보보호법 강화.

02

분산된 거버넌스

국정원(공공)·과기정통부/KISA(민간)·국방부(국방)·

개인정보위·금융위로 권한이 쪼개져 있다.

「사이버안보 기본법」은 20년째 미완.

03

규제와 실질의 괴리

ISMS 인증을 보유한 대기업에서 대형 사고가 반복.

인증 통과와 실제 보안 수준 사이의 간극이

2025년 사고들로 다시 드러났다.

TIMELINE

여섯 시기로 본 전체 흐름



※ 3기와 4기는 시기가 겹친다 — 금전 목적의 정보 유출과 국가배후 파괴형 공격이 동시에 진행됐다.

1기 · 1988~1998

태동기 — 백신과 전담기관의 등장

- 1986 ● 「전산망보급확장과이용촉진에관한법률」 제정, 국가기간전산망 사업 착수
- 1988 ● (C)Brain 바이러스 국내 확산, 안철수 V1 백신 개발 — 민간 보안의 출발점
- 1994 ● KORNET 인터넷 상용 서비스 개시 — 위협의 무대가 PC에서 네트워크로
- 1995 ● 「정보화촉진기본법」 제정 · 안철수연구소(현 안랩) 설립
- 1996 ● 한국정보보호센터(현 KISA) 설립 — 최초의 국가 보안 전담기관

이 시기 보안은 독립 기능이 아니라 「전산실 관리」의 부속물이었다.

2기 · 1999~2003

인프라 충격기 — 1·25 인터넷 대란

2003.1.25

전국 인터넷 마비

SQL Slammer 웜이 MS-SQL 취약점을 통해 확산되며
KT 혜화 DNS를 마비시켰고, 국내 인터넷이
수 시간 동안 사실상 정지했다.

사이버 침해가 「국가 재난」이라는 인식이
처음으로 자리 잡은 분기점.

1999

CIH(체르노빌) 바이러스 대란

PC 보안의 대중화, 백신 산업 본격 형성

2001

「정보통신기반보호법」 제정

주요정보통신기반시설 지정·보호 체계 출범

2002

ISMS 인증제도 도입

정보통신망법 기반 관리체계 인증의 시작

2004

국가사이버안전센터(NCSC) 설립

이듬해 「국가사이버안전관리규정」 제정

3기 · 2008~2014

개인정보 유출기 — 규제의 방향을 바꾼 사고들

2008

1,081만 건

옥션

중국발 해킹, 국내 최초의 천만 단위 유출

2011

3,500만 건

네이트·싸이월드

사실상 전 국민 규모, 주민번호 포함

2011

전산망 마비

농협

내부 협력업체 노트북 경유 침해

2014

1억여 건

카드 3사

KB국민·롯데·NH농협, 외주 인력 반출

제도적 귀결

2011년 「개인정보보호법」 제정 · 주민등록번호 수집 원칙적 금지 · 암호화 의무화 · 징벌적 손해배상 도입

4기 · 2009~2016

국가배후 공격기 — 금전에서 파괴로

2009.7.7

DDoS 대란

청와대·국회·금융기관 등 국내외 주요
사이트 동시 마비

2011.3.4

DDoS 공격

2년 만의 재발, 좀비 PC 기반 공격의
고도화

2013.3.20

사이버테러

KBS·MBC·YTN 및 은행 전산망 파괴 —
데이터 삭제형 공격

2013.6.25

사이버공격

정부기관 홈페이지 변조 및 디도스 동
시 수행

2014.12

한국수력원자력 해킹

원전 도면 유출·공개, 국가 기반시설 위
협 현실화

2016

국방망 해킹

국방부 내부망 침투, 군사 기밀 유출
논란

단순 금전 목적을 넘어 사회 혼란과 시스템 파괴를 노린 공격이 등장 → 국정원·과기정통부·국방부로 나뉜 분산형 거버넌스가 고착

재편기 — 랜섬웨어와 제도 정비

위협의 변화

- 2017 WannaCry — 전 세계 동시 감염, 국내 확산
- 2017 인터넷나야나 — 호스팅 사업자 마비, 몸값 지급 논란
- 암호화폐 거래소 연쇄 해킹 (빗썸·유빗 등)
- 이중 갈취형 랜섬웨어와 공급망 공격의 본격화

제도의 정비

- 2018** ISMS와 PIMS 통합 → ISMS-P 출범
- 2020** 데이터 3법 · 개인정보보호위 중앙행정기관 격상
- 2020** 공인인증서 제도 폐지
- 2022** 정보보호 공시 의무화
- 2023** 개인정보보호법 2차 개정 — 과징금 산정 기준을 「전체 매출」로 전환
- 2024** 공공 망분리 개선, 다층보안체계(MLS) 전환 추진

6기 · 2025

국내 보안 역사상 최악의 해

2,324만

SK텔레콤 HSS 해킹

4월 · BPFDoor 계열 악성코드로
IMSI·유심 인증키 등 25종 유출

3,370만

쿠팡 회원정보 유출

하반기 · 퇴사자에 의한 내부 유출,
역대 최대 규모

297만

롯데카드 정보 유출

8월 · 카드번호·유효기간·
결제정보까지 포함

1,348억

개인정보위 과징금

SKT 대상 · 역대 최대 규모의
제재 부과

그 외 · 8월 KT 불법 소형 기지국을 통한 무단 소액결제 및 가입자 정보 유출 확인 · 9월 정부 「범정부 사이버보안 대책」 발표

ROOT CAUSE

고급 기법이 아니라 「기본」이 무너졌다

1 평문 저장

GSMA 권고와 달리 유심 인증키를
암호화하지 않고 보관

2 방치된 취약점

수년간 패치되지 않은 서버 취약점이
초기 침투 경로로 사용

3 계정·권한 관리 실패

퇴사자의 접근 권한이
장기간 회수되지 않음

4 기본 설정 미변경

초기 비밀번호를 그대로 둔
가정용 카메라 12만 대 노출

5 신고 의무 미이행

침해 인지 후에도 정보통신망법상
신고를 이행하지 않은 사례

6 협력업체 경유 침해

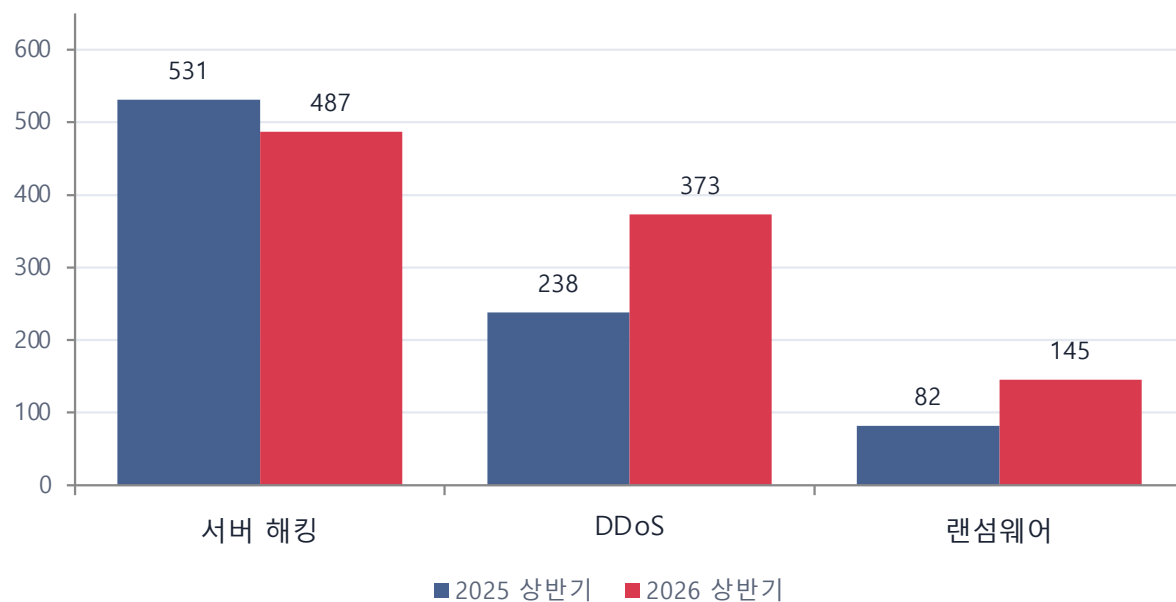
유지보수·외주 인력을 통한
공급망 우회 침투

시사점 — 문제는 탐지 기술의 부재가 아니라 자산·계정·권한에 대한 기본 통제의 운영 실패였다.

2026 상반기

침해사고 신고 1,236건 — 전년 동기 대비 19.5% 증가

KISA 침해사고 신고 유형별 건수



+56.7% DDoS 공격

해티비즘 성격의 가용성 공격 확산

+76.8% 랜섬웨어 신고

RaaS·초기 접근 브로커 분업 구조 정착

-8.3% 서버 해킹

여전히 최대 비중(39.4%)이나 소폭 감소

출처: 과학기술정보통신부·KISA 「2026년 상반기 국내 사이버위협 동향」

2026 · 규제 축의 이동

AI 기본법 — 세계 두 번째 포괄적 AI 규제

2024.12.26

국회 본회의 통과

19개 법안 병합, 여야 합의

2026.1.22

AI 기본법 시행

EU AI Act에 이어 세계 두 번째

2026.7.21

개정법·시행령 시행

고영향 AI 취약계층 범위 등 구체화

실무 쟁점

1

고영향 AI 판별

의료·금융·채용·자율주행 등 대상 여부 사전 진단

2

AI 영향평가

인공지능취약계층 특성 반영 의무 (시행령 제2조의2)

3

투명성·안전성 확보

생성형 AI 표시 의무, 학습연산량 기준 안전 조치

4

국내 대리인 지정

일정 규모 이상 해외 사업자 대상

분산된 거버넌스 — 20년째 미완의 통합

1

국가정보원

국가·공공 부문
국가사이버안전센터(NCSC)
운영

2

과학기술정보통신부 · KISA

민간 부문 침해사고 대응
ISMS-P 인증, 위협 동향 발
표

3

국방부

국방 부문
사이버작전사령부

4

개인정보보호위원회

개인정보 침해 조사·제재
중앙행정기관(2020~)

5

금융위원회 · 금융보안 원

금융권 전자금융감독규정
금융 ISAC 운영

미완의 과제

「사이버안보 기본법」은 2006년 첫 법안 발의 이후 20년 가까이 국회를 통과하지 못했다.
권한 배분과 민간 사찰 우려가 핵심 쟁점으로, 사고 발생 시 컨트롤타워 부재 문제가 반복된다.

CONCLUSION

역사가 남긴 세 가지 질문

Q1

왜 늘 사고 뒤에 법이 오는가

선제적 리스크 평가 체계 없이는
다음 사고도 같은 순서를 반복한다.

Q2

인증은 왜 사고를 막지 못했는가

ISMS-P 통과와 실질 보안 수준의 간극.
운영 검증 중심으로의 전환이 과제.

Q3

AI 시대의 컨트롤타워는 누구인가

AI 기본법·개인정보보호법·정보통신망법이
중첩되는 영역의 조율 주체가 불분명.