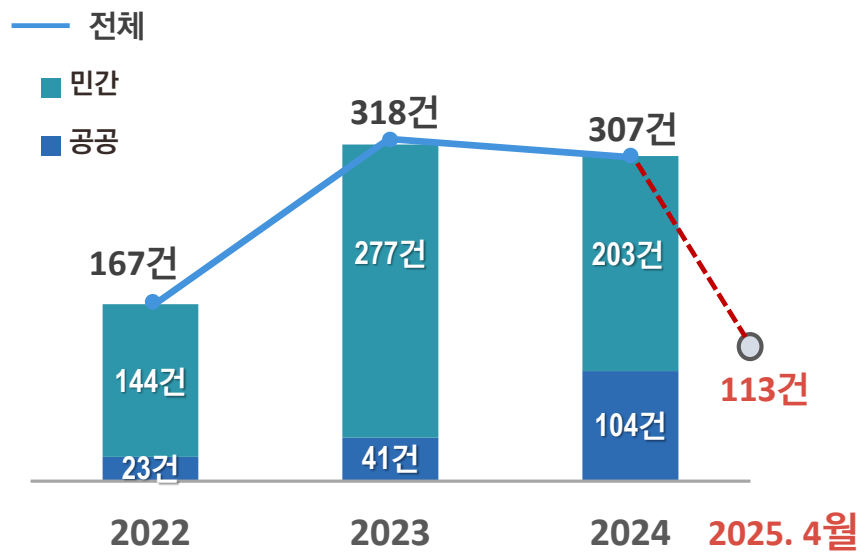
개인정보 유출사고 현황 및 대응방향

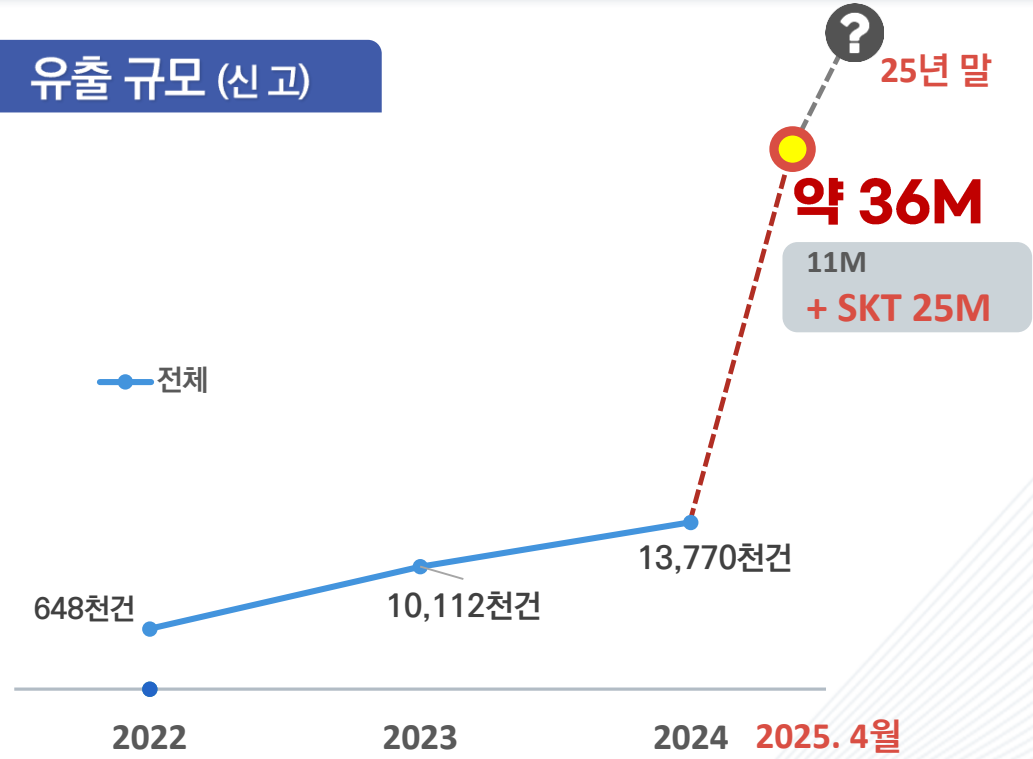
2025. 05. 21.

개인정보 유출사고 현황

신고 건수



유출 규모 (신 고)



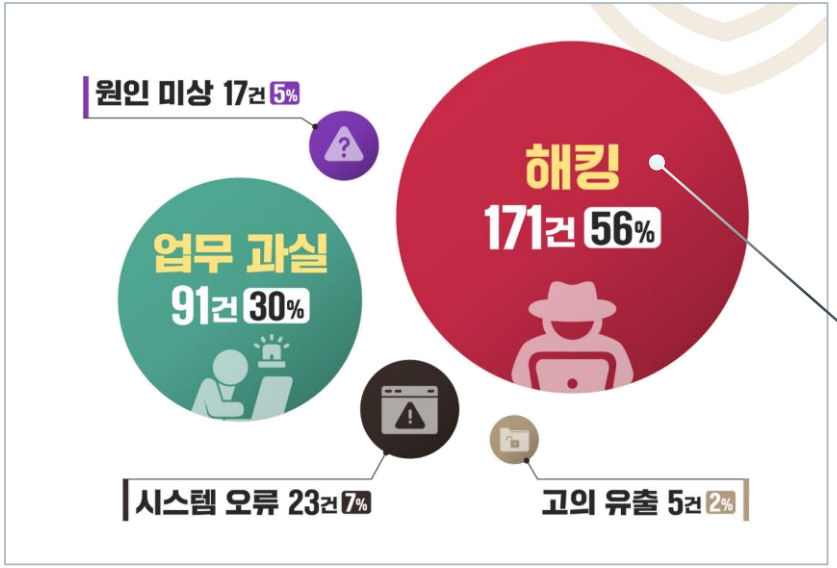
최근 3년간 유출신고 건수는 약 3백 건 내외이나,

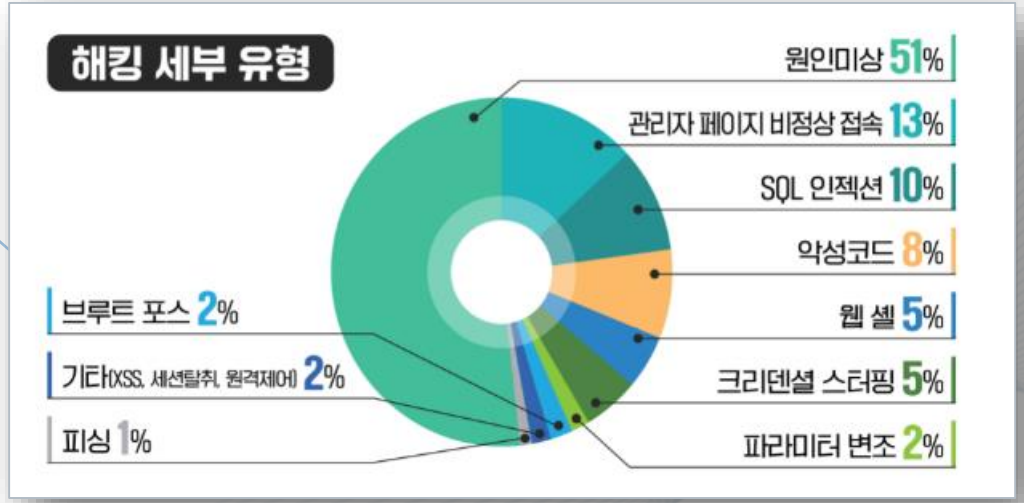
올해는 신고 건수 대비 개인정보 **유출 규모**가 SKT 사건 등으로 **위기상태** 규모로 급증
(전년도 유출 규모의 3배 가까이 증가)

개인정보 유출사고 현황

원인유형 (2024)

» 2024년 총 307건의 유출사고 발생, 해킹으로 인한 신고는 56%로, 전년 대비 13% 증가



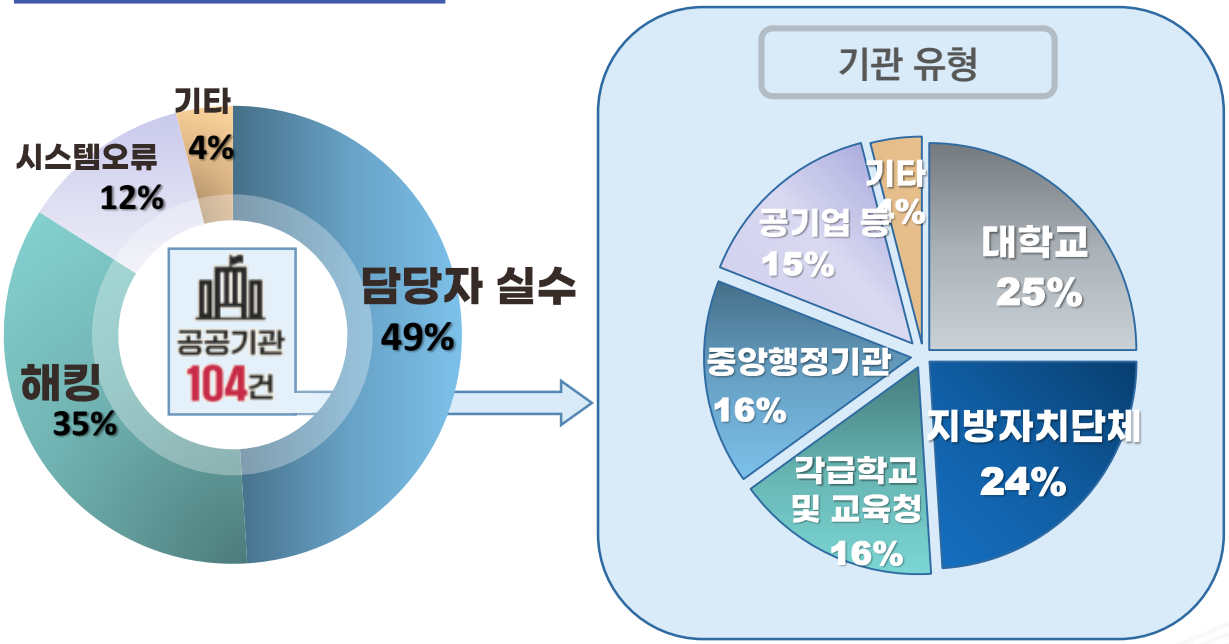


개인정보 유출사고 현황

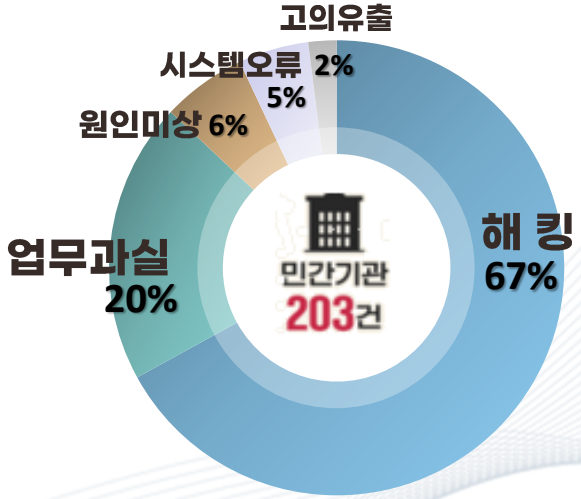
» 기관별로 보면 공공기관은 104건, 민간기관에서는 203건 유출

• 공공기관은 업무과실로 인한 개인정보 유출이 49%로 가장 많았고, 민간기관은 해킹이 67%로 가장 많았음

공공부문 유출원인



민간부문 유출원인



최근 주요 유출사고 경향

» 유출사고는 공공·민간, 처리자 규모를 불문하고 지속적·대규모로 발생 중

민간

'25.4月 2,564만 건(통지기준)

SK 텔레콤

'25. 1月 167만 건(추정)

GS

'25. 3月 780만 건(추정)

LG U+

'23.7月 30만 건

Incruit

'23. 12月 221만 건

GOLFZON

공공

'25.4月 57만 건(추정)

농촌진흥청 Rural Development Administration

SSN (사회복지협의회)

'23.2月 296만 건

'24.1月 135만 건

경기도교육청

최근 주요 유출사고 경향

(그림 생략)

›› 해킹 등 사이버 범죄는 전세계적으로 조직적 · 대규모화

- 조직적 대규모 공격이 증가하고 정교함 또한 빠르게 높아지고 있음
  (World Economic Forum, 「Global Cybersecurity Outlook 2025」)

- 사이버 범죄로 인한 피해 규모가 2015년 3조 달러에서
  2025년 연간 10.5조 달러에 이를 것으로 예측
  (Cybersecurity Ventures, 2024)

사고예방 및 대응방안

01 개인정보 관리 조치

» 취급 중인 개인정보 현황파악 및 관리체계 수립

- 처리자가 보유하고 있는 개인정보처리시스템, 개인정보취급자, 처리업무 위탁 시 수탁자에 대한 정확한 현황 파악
- 내부관리계획을 통해 구체적으로 점검 · 관리, 실제 운영 과정에서도 지속적 보완 · 강화

» 관리·감독 및 업무절차 개선

- 취급자 및 수탁자에 대한 주기적 관리, 실질적 점검이 될 수 있도록 항목과 절차를 구체적으로 설정
- 개인정보 탐지·암호화 솔루션 구매·적용, 이메일 '개별발송' 기본값 설정, 파일 첨부 전 개인정보 검사, 추가적 검증 절차 마련

02 개인정보 안전 조치

» 취약점 점검

- SKT 사건을 계기로 소관 개인정보처리시스템 전반에 대해 유·노출 사전 점검 분석 기능을 강화, 정기적 보호조치 및 취약점 점검

» 접근권한

- 처리시스템에 대한 접근 권한 차등 부여, 공유되지 않도록 조치
- 취급자 또는 정보주체의 인증수단을 안전하게 적용 관리
- 일정횟수 이상 인증 실패시 개인정보처리시스템에 대한 접근 제한

» 접근통제

- IP(Internet Protocol) 주소 등으로 인가 받지 않은 접근을 제한하고 접속한 IP주소 등을 분석하여 불법적인 유출 시도 탐지 및 대응
- 외부에서 접속시 안전한 인증수단 또는 안전한 접속수단을 적용

개인정보 전 주기 철저한 점검 및 관리 체계 전환이 필요한 시점

※ (예) 집중관리시스템 10대 안전조치 의무 도입 ('24.9월 시행)으로 특성에 맞는 맞춤형 안전조치 관리체계 마련

주요 유출사고 유형별 처분사례

민간부문 1 관리자 페이지 안전조치 미흡(A사)

개 념	관리자 페이지 2차 인증(MFA) 미적용, 접속 IP 미제한 → 회원정보 탈취
사 례	29만건 유출 / 관리자 페이지 750여회 접근 / 44만건 불법 문자 전송
위반사항	ID·PW만으로 로그인, 불법 접근 차단 미조치
처분결과	과징금 1억 517만 원, 과태료 720만원, 공표
예방법	로그인 시 2차 인증 도입, 접속 IP 제한

민간부문 2 SQL 인젝션 (B사)

개 념	웹사이트 취약점 이용, 악의적인 SQL문 실행하여 DB를 비정상적으로 조작 → 개인정보 탈취
사 례	53만건 유출 / 주민등록번호 포함
위반사항	불법 접근 탐지·차단 미조치(입력값 방어 조치 미흡, 웹방화벽 비활성화), 주민등록번호 미파기
처분결과	과징금 6,110만원, 과태료 960만원, 공표 명령
예방법	시큐어 코딩, 웹 취약점 점검, 보안 강화 조치 (웹방화벽 도입, DB접근권한 최소화 등)

주요 유출사고 유형별 처분사례

공공부문 1 크리덴셜 스터핑 (C기관)

개 념	확보한 ID/PW 무작위 대입 → 로그인 성공 시 개인정보 탈취
사 례	23만건 유출 / 분당 최대 1만회 / 1.25% (4,500만회 중 56만회 성공)
위반사항	불법 접근 탐지·차단 미조치, ID·PW만으로 로그인
처분결과	과태료 840만원(舊 보호법 적용, 주민등록번호 유출 없음)
예방법	개인정보 마스킹, 접속 IP 분석 및 차단 임계치 설정, 로그인 시 캡챠·추가인증 도입

* 최근 크리덴셜스터핑 방지 기능을 제공하는 침입탐지시스템도 존재

공공부문 2 웹셸 (D기관)

개 념	홈페이지 취약점 악용 내부공간에 악성코드 업로드·실행 → 개인정보 탈취
사 례	540건 유출 / 5.jsp 업로드 / 웹셸을 통한 데이터 통신(288MB) 발생
위반사항	불법 접근 탐지·제한 프로그램 미운영, OS 보안패치 미적용
처분결과	과징금 1억 9,300만원, 과태료 660만원, 시정조치명령, 개선권고
예방법	파일 업로드 제한, 파일 업로드 폴더 실행 제한

유출사고 신속 대응 및 피해구제 강화

» 다크웹 모니터링 및 조기탐지 강화

- 온라인 개인정보 유노출 탐지 범위를 다크웹으로 확대, 신속 공유 확인 및 유출경로 차단 + 정보주체 통지

» 대규모 유출사고 등 신속 대응체계 강화

- 포렌식 센터 설치('25. 말) 사고 초동대응 강화 / 증거자료 보전, 자료제출 지연 방지
- 정보주체 관점에서 민감도 높은 개인정보 유출에 대한 엄정 처분

» 정보주체 실질적 피해구제 지원 강화

- 정보주체 보상 등 구체적 피해보상과 과징금 부과 기준 연계 검토

➡ 정보주체 유출 통지부터 조사, 처분 등에 이르는 **개인정보 감독체계 전면 보완**

공공기관의 개인정보 유출·침해 책임성 강화

2023. 9월

- ▶ 유출신고 대상 확대
- ▶ 원칙적 과징금 부과 및 과징금 상한 확대
- ▶ 부정이용 시 형사처벌

2024. 9월

- ▶ 주요 공공시스템 추가적 안전조치 의무 부과

2025년

- ▶ 집중관리시스템 보호 2.0
- ▶ 공공기관 전면 공표제
- ▶ 대규모 유출 3년내 추가 실태점검

감사합니다