

개인정보위, 2025년 개인정보 유출 신고 및 조사·처분 사례 분석결과 발표

- '25년 개인정보 유출 신고 447건으로 전년 대비 45.6% 증가
- '25년 총 227건 조사처분, 과징금 40건(1,677억원) 및 과태료 125건(약 5.9억원) 부과
- 랜섬웨어 등 해킹에 의한 유출 증가 추세, 사고 예방을 위한 보안 업데이트 적용, 안전한 백업 체계 운영, 접근통제 강화 및 개인정보 암호화 등 안전조치 당부

개인정보보호위원회(위원장 송경희, 이하 '개인정보위')와 한국인터넷진흥원(원장 이상중)은 2025년 동안 접수된 개인정보 유출 신고 및 처분 사례를 분석해 원인별 예방책 및 주요 사례를 담은 「2025년 개인정보 유출 신고 동향 및 조사·처분 사례」를 발간하였다.

주요 내용은 다음과 같다.

< 유출신고 분석 >

2025년 접수된 유출 신고 건은 총 447건으로 전년도 307건 대비 약 45.6% 증가했다. 전체 유출 원인 중에서는 해킹이 62%(276건)로 가장 높은 비중을 차지하였으며, 업무 과실 25%(110건), 시스템 오류 5%(24건) 순으로 나타났다.

해킹 사고의 유형으로는 랜섬웨어, 웹셸* 등 악성코드 35%(96건), 에스큐엘(SQL) 인젝션**, 파라미터 변조 등 웹 취약점 악용 12%(32건), 관리자 페이지 비정상 접속 8%(23건) 순으로 나타났으며, 전 세계적으로 급증하고 있는 랜섬웨어 유포와 대형 수탁사를 노린 공급망 공격 확대 등 외부 위협이 고도화됨에 따라 전년도에 비해 해킹(171건 → 276건)으로 인한 유출이 증가하였다.

* 웹셸 공격 : 특정 웹페이지의 파일 업로드 취약점(파일 업로드 기능을 이용해 비정상적인 스크립트 파일 등을 실행)을 통해 시스템에서 실행 가능한 악성코드를 삽입 및 실행하여 관리자 권한 획득, 개인정보 탈취 등을 행하는 공격 기법

** 에스큐엘(SQL, Structured Query Language) 인젝션 공격 : 악의적인 에스큐엘(SQL)문을 삽입해 데이터베이스가 비정상적인 동작을 하도록 조작하는 공격 기법

< 조사·처분 분석 >

2025년 개인정보위 조사·처분 건수는 총 227건이며, 과징금은 40건으로 총 1,677억원, 과태료는 125건으로 5억 8,720만원을 부과하였다. 전년도 비교 시 과징금·과태료 부과가 172%(1,083억원) 증가하였다.

기관별로 살펴보면, 공공 부문은 77건으로 공공기관 53%(41건), 중앙행정기관·헌법기관 등 29%(22건), 지방자치단체/학교 각 9%(각 7건) 순으로 확인되었다. 민간 부문은 150건으로 중소기업 50%(75건), 대기업·중견기업 20%(30건), 비영리 단체 등 기타 17%(25건) 순이었다.

총 227건 중 115건(과징금·과태료 1,583억원)이 개인정보 유출 관련 조사·처분으로 확인되며, 세부 유출 원인은 업무 과실 46%(53건), 해킹 45%(52건), 시스템 오류 7%(8건) 순이며, 유출 원인별 과징금·과태료 부과액은 해킹이 1,440억원(91%)으로 가장 큰 비중을 차지하였다.

< 예방·점검·대비 당부 >

개인정보위는 장기간 취약점 점검 및 개선을 하지 않아 개인정보 유출이 반복적으로 발생하는 것을 예방하기 위해 주요 개인정보 유출 사례를 기반으로 예방 방법을 안내했다.

2025년 이후 증가 추세인 랜섬웨어를 통한 개인정보 유출 방지를 위해 운영체제, 보안 장비 등의 보안 업데이트 적용 및 정기적인 악성 이메일 모의 해킹 훈련, 랜섬웨어 감염 시 즉시 복원할 수 있도록 안전한 백업 체계 운영, 접근통제 강화 및 데이터베이스(DB) 개인정보 암호화 등의 방법을 강조했다.

또한, 기관 및 기업별 특성을 고려한 구조적 대비책도 주문했다. 공공기관은 개인정보 보호 업무에 관한 전담 인력 지정 및 타 업무 겸직 금지 등을 통해 실무 전문성을 제고하고, 기관 차원의 개인정보 보호 관리 체계를 전면 재정비할 것을 촉구했다.

민간기업은 새로운 보안 위협에 대응하기 위해 개인정보보호책임자(CPO)를 중심으로 개인정보 관리 및 대응 체계를 상시 점검·강화하는 한편, 수탁사를 통한 연쇄적인 유출이 개인정보 관리 사각지대로 대두됨에 따라 수탁사에 대한 관리·감독 의무를 철저히 이행할 것을 요구했다.

아울러 '26. 9. 11. 부터는 고의·중과실로 인한 대규모 유출 시 전체 매출액의 최대 10%에 달하는 과징금을 부과하는 등 제재가 대폭 강화된 만큼 경영진 차원의 선제적인 보안 예산 확보와 인력 투자가 필수적이라고 덧붙였다.

앞으로 개인정보위와 한국인터넷진흥원은 반복되는 대규모 유출 사고 등에 대해서는 엄정히 제재하는 한편, 자발적 보호투자 확대 유도과 민간·공공 기관에 대한 위험기반 관리체계 구축 등 사고 예방 조치를 강화하여 실질적인 보호 수준을 높일 수 있도록 지원해 나갈 방침이다.

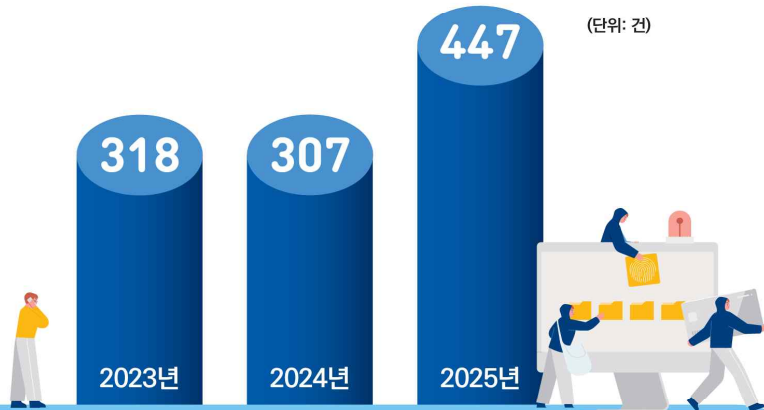
[붙임1] '25년 개인정보 유출 신고 동향 주요 인포그래픽

[붙임2] '25년 개인정보 조사·처분 동향 인포그래픽

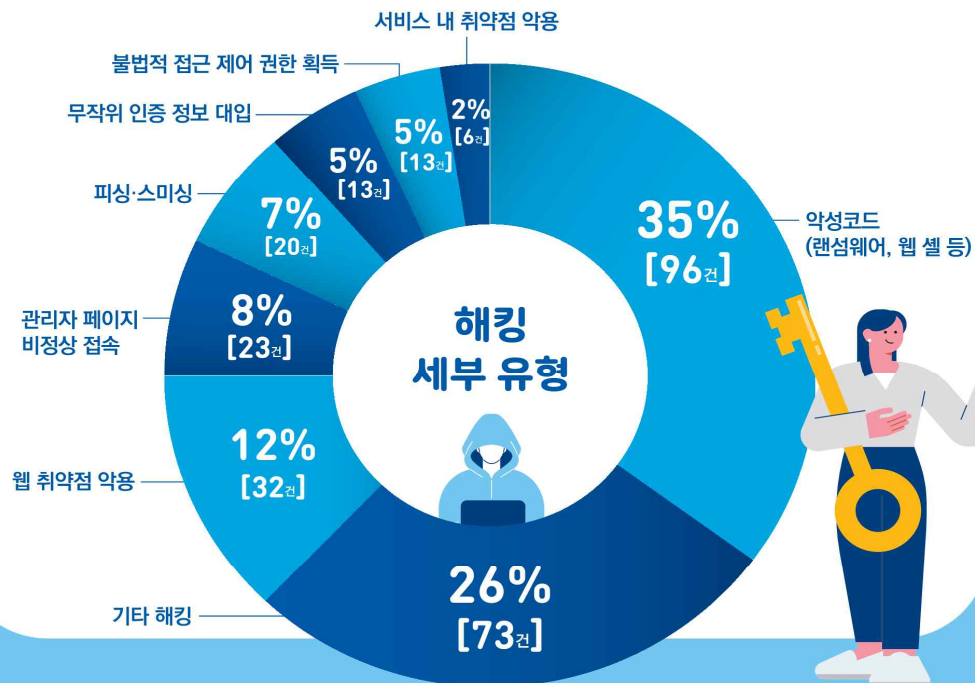
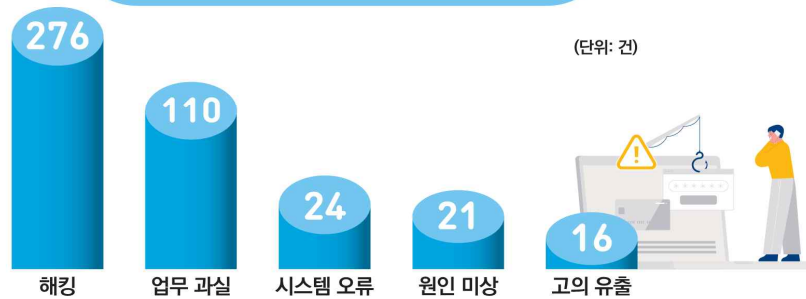
담당 부서 <총괄>	개인정보보호위원회 조사총괄과	책임자	과 장	강대현 (02-2100-3101)
		담당자	사무관 주무관 주무관	장수용 (02-2100-3102) 지한구 (02-2100-3093) 이혜원 (02-2100-3189)
<공동>	한국인터넷진흥원 유출조사팀	책임자	팀 장	손기종 (061-820-2850)
		담당자	선 임 주 임	이광재 (061-820-2854) 한승주 (061-820-2861)



최근 3년간 개인정보 유출 신고 현황



2025년 개인정보 유출 사고 원인





2025년 조사·처분 현황

개인정보 보호법 위반행위
조사·처분 현황

총 **227건**

※ 경고, 의견제시 등을 모두 포함한 의견은 425건

과징금 **40건, 1677억원**

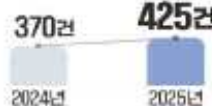
과대료 **125건, 5.9억원**

개선권고 **51건**, 시정명령 권고 **85건**, 공표 명령 **45건**

전년 대비 처분 건수



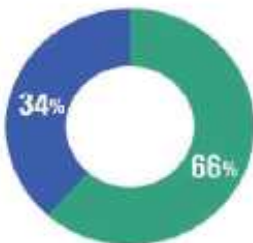
전년 대비 조사 의견 건수



전년 대비 과징금 부과액



처리자유형



■ 공공분야 77건
■ 민간분야 150건

공공분야 (총 77건 처분)



※ 과징금 기준: 학교(대학 등) 9.6억(71%), 국가 2.2억(66%), 산하 공공기관 1.0억(14%) 배

민간분야 (총 150건 처분)



※ 과징금 기준: 대기업 1,550억(94%), 해외사업자 42.2억(3%), 중견기업 38.4억(2%) 배

사고 유형 원인



위반행위



유출원인

