내 삶을 지키는 정부 국민안전 플러스

개인정보보호위원회

보도자료

대체불가 대한민국

보도시점 2026.11.27.(금) 11:00 배포 2026.11.26.(목) 15:30

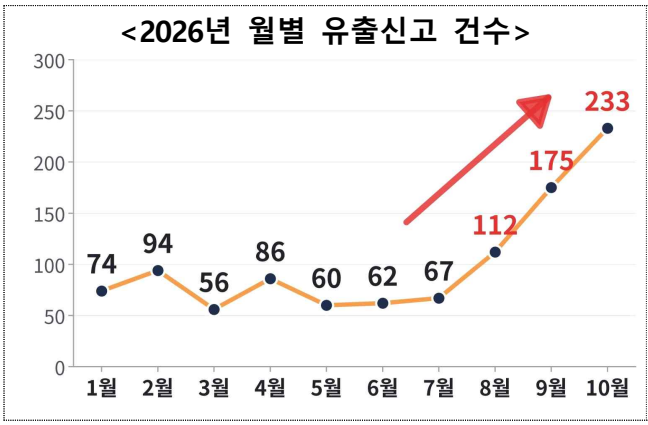
개인정보위, 유출 긴급대응 및 점검지원 체계 가동

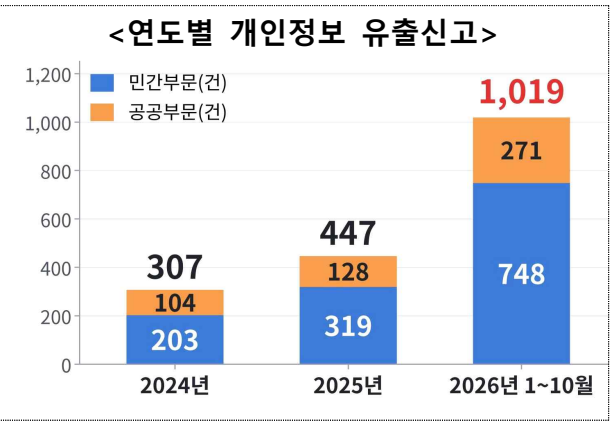
- 인공지능 기반 공격 확산, 유출 급증에 따른 보안 관계부처와 신속 정보 공유·협력 및 비상 대응
- 유출 유형·원인분석 기반 우선조치 필요사항 전파, 실태점검 추진 등

개인정보보호위원회(위원장 송경희, 이하 '개인정보위')는 **유출사고 급증**에 따른 **긴급 대응 체계를 가동**한다고 밝혔다. 최근 **인공지능 기반 해킹이 증가**하는 추세로, 사회 전반의 신속하고 긴급한 대응이 필요한 상황이다.

인공지능을 활용한 해킹은 공격 과정의 자동화·고도화를 통해 기존보다 **신속**하게 **대규모의 공격**이 가능하다. 해킹에 소요되는 **시간·비용이 적을** 뿐만 아니라 전문가가 아닐지라도 해킹을 시도할 수 있어 **진입장벽도 낮아졌다**. 이로 인해 **개인정보의 유출 양상도 달라질 우려**가 크다.

올해만 해도 개인정보 **유출신고 건수**가 **1월부터 10월까지 1,019건**으로, 이는 **작년 전체 유출신고 건수**(447건)와 비교하여 **이미 2배를 뛰어넘는 수준**이다.





1월부터 10월까지의 신고자료 분석 결과, **공공**부문에서 **271건**, **민간**부문은 **748건**의 신고가 접수되었다. 공공은 **중앙행정기관, 지방자치단체** 외 대학을 포함한 **각급학교**에서도 신고가 여럿 있었다. 민간의 경우 **중소기업 > 중견기업 > 소상공인·개인사업자 > 대기업** 순으로 신고가 많이 접수되었다. **업종·분야·규모 등**에 상관없이 **전방위적**으로 **유출사고가 발생하는 추세**임을 알 수 있다.

<기관 유형별 유출건수(건)>



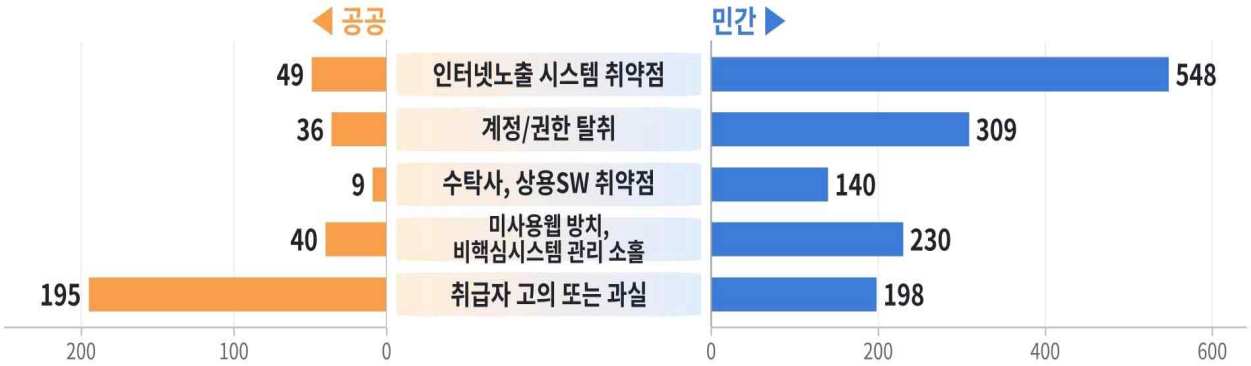
※ '26.1~10월 유출신고 초기분석 결과 (출처 : 개인정보위)

유출 원인은 공공·민간별로 **상이**하게 나타났다. **공공**은 **인적과실이나 시스템 오류**가 차지하는 비중이 높지만 **최근 해킹사고**가 **늘고 있는 추세**이고, **민간**은 상대적으로 **해킹으로 인한 유출이 다수**였다. 세부적으로 **공공부문**은 이메일·공문 등을 통한 **문서 오발송**이나 게시판 등 **공개된 장소에 개인정보를 게시**하는 **'취급자 고의 또는 과실'**이 전체 유출원인 중 가장 높은 비중을 차지하였다. 반면, 민간의 경우 **접근통제·공개설정 미흡**이 가장 큰 비중을 차지하였고, **API·파라미터 변조·인증 우회 등으로 인한 유출**이 다음으로 높은 비중을 차지하는 등 **'인터넷노출 시스템 취약점'**이 가장 큰 원인이었다.

특히, **계정·접근키 탈취**와 같은 **정상적 권한을 악용하는 유출 사례**가 크게 증가하여 **전통적인 웹 취약점**(SQL 인젝션*, 파일업로드 취약점 등)과 **비슷한 수준**인 것으로 확인되었다. 그 외에도 **수탁사 서버를 침해**하거나, 미사용 API·테스트 서버 방치 등 **관리되지 않은 자산**으로 인한 유출, **업무지원 시스템이나 부가 서비스** 등 **비핵심 서비스 해킹**이 **다수 발견**되었다.

* 악의적인 입력값을 넣어, 웹사이트가 데이터베이스에 보내는 명령을 조작하는 공격

<주요 원인별 유출건수(건)>



※ '26.1~10월 유출신고 초기분석 결과 (출처 : 개인정보위)

앞으로 금융·교육·유통·통신 등 **일상생활 전 영역에 걸친 유출 사고**가 **더욱 심화**될 것으로 예상된다. 이에 대응하기 위해서는 **신속한 탐지**와 상황 **전파체계**를 갖추는 한편, 악용 우려가 높은 **취약 자산이 제대로 식별되어 관리**되고 있는지, **기본적 보안조치**에 부족한 점이 없는지 **시급한 점검·보완**이 필요하다. 중장기적으로는 현 보호체계를 제로베이스에서 검토하여 **인공지능 위협 상시화에 대응**한 **전사적 차원의 개인정보 보호 체계 강화**가 요구되는 상황이다.

이러한 상황 인식에 따라 개인정보위도 **긴급대응 및 점검지원 체계로 전환**하여, **보안 관계부처**(과기정통부, 금융위, 국정원 등)와 **더욱 신속하게 정보를 공유**하고 **긴밀하게 협력**할 예정이다. 또한, **유출사고 유형 및 원인분석**을 바탕으로 인터넷 노출 시스템 점검, 접근권한 관리 등 구체적인 **우선조치 필요사항을 전파***한다.

* [붙임] 공통적 우선조치 필요사항

아울러, **12월부터 3개월 간 각 기관**이 **대응체계를 갖추고 조치사항을 점검**할 수 있도록 **집중 관리**할 계획이다. 우선, **각 부처와 광역 지방자치단체**들이 **긴급점검·대응 체계(팀장: 부기관장 원칙)**를 **가동**하도록 하고, **본부외 소속·산하기관** 등도 **우선조치 필요사항**을 신속히 **이행**할 수 있도록 **지도·감독을 요청**할 예정이다. 그간 **전문인력 부족**으로 인해 각 부처가 소관 공공기관을 **서면·용역의 방식**으로 **점검**하고 있는 현실을 감안하여 **개인정보위가 부처의 현장점검도 적극 지원**한다.

민간기업·기관을 대상으로는 개인정보보호책임자(CPO) 협의회, 자율규제 단체 등을 통해 **우선조치 필요사항을 안내하고 당부**할 계획이다. 또한, **유출 시 파급력이 높은 고위험군** 중심 **긴급점검**을 실시한다. **산·학·연** 협력으로 **기술현안**에 **신속 대응**할 수 있도록 **기술지원 체계**도 구축·운영한다.

개인정보위는 **충분한 개인정보 보호 투자 및 노력**에 대해서는 과징금을 감경하는 반면, **예방 가능했던 유출사고**에 대해서는 **엄정하게 조사·처분**한다는 원칙을 분명히 하였다. 동시에 **사고 조사**가 **완료**된 **이후** 시정·개선하는 기존 **체계를 보완**하여 **초기 위협정보를 공유**하고 **선제적으로 대응**할 수 있는 체계도 갖춰나갈 방침이다.

담당 부서 <공동>	기획조정관 혁신기획담당관	책임자	과 장	정혜원 (02-2100-2451)
		담당자	서기관	김푸르나 (02-2100-2453)
	조사조정국 조사총괄과	책임자	과 장	강대현 (02-2100-3101)
		담당자	사무관	이승철 (02-2100-3118)
	예방조정심의관 사전실태점검과	책임자	과 장	김해숙 (02-2100-3060)
		담당자	사무관	정진아 (02-2100-2424)
	예방조정심의관 자율보호정책과	책임자	과 장	황지은 (02-2100-3081)
		담당자	사무관	공수진 (02-2100-3082)
	예방조정심의관 공공실태점검단	책임자	과 장	임종철 (02-2100-3200)
		담당자	사무관	임용현 (02-2100-3201)
	개인정보정책국 신기술개인정보과	책임자	과 장	신용우 (02-2100-3061)
		담당자	사무관	서민호 (02-2100-3062)

대한민국 정책브리핑
대체불가 대한민국
OPEN 출처표시 공공누리 공공저작물 자유이용허락

붙임 공통적 우선조치 필요사항

◇ 인터넷 노출 시스템 점검	
①	SQL 인젝션, 파일업로드 등 웹 취약점 점검
②	API 인증절차 확인 및 인증 없는 개인정보 호출차단
③	관리자페이지, DB, 클라우드 스토리지의 외부 접속 IP 제한
④	접근통제·설정 미흡(관리자페이지·DB 노출) 여부 점검
◇ 계정 등 접근권한 관리	
⑤	관리자·VPN·메일·클라우드 등 계정 MFA 적용
⑥	액세스 키·토큰을 소스코드, 서버 등에 저장 여부 점검 및 저장 금지, 주기적 교체
⑦	퇴사자·미사용·공용 계정, 테스트계정 점검 및 삭제
⑧	장기(예. 180일 이상) 미사용 계정·권한 말소·회수
◇ 수탁사 · 상용SW 관리	
⑨	수탁사·협력업체 계정은 최소 권한, 공용계정 금지
⑩	시스템 운영 수탁사의 접근통제 등 안전조치 점검
⑪	사고 발생 시 수탁→위탁사 즉시 통지 절차 마련
⑫	종료된 위탁 업무 관련 개인정보 반환·파기 확인
⑬	상용SW 현황 파악 및 보안패치 즉시 적용 ※ 인증 없이 임의 코드 실행 가능한 PHP2Shell, Java4Shell 등의 치명적인(Critical) 취약점 우선 조치
◇ 자산 관리 및 정비	
⑭	구버전 API·앱·관리자 기능 삭제·차단
⑮	운영 종료 서비스·미사용 페이지 제거
⑯	업무지원 시스템(그룹웨어·파일서버·메일 등) 포함 ·운영 중인 모든 시스템 현황 파악(자산관리)
◇ 취급자 관리 등 기타	
⑰	개발·테스트용 데이터·DB에 방치된 개인정보 파기
⑱	기간 경과, 목적달성한 임시파일, 로그, 백업 등 파기
⑲	메일 발송, 문서 교부 전 수신자·첨부 확인
⑳	문서게시, 정보공개 전 개인정보 검출·마스킹