잇단 유출에 신뢰 잃은 ISMS-P… 사고 땐 즉시 인증 취소

〈정보보호·개인정보 보호 관리 체계〉

대형 기업유출 반복 무늬 인증 논란
정부, 실증심사 도입 형식 심사 축소
사고 땐 특별심사 착수 결함 시 취소
위험 기업엔 기술심사로 장벽 강화

송경희 개인정보보호위원장(왼쪽 세번째)이 6일 오후 서울 종로구 정부서울청사에서 열린 ISMS-P 인증 개선 회의에서 발언하고 있다. /뉴시스

'보안 최후 보루'로 여겨졌던 ISMS-P(정보보호 및 개인정보 보호 관리 체계) 인증이 대형 정보 유출 사고 앞에서 무력함을 드러내면서, 정부가 뒤늦게 제도 전면 수술에 나섰다.

쿠팡, SK텔레콤, KT, 롯데카드 등 까다로운 심사를 통과해 인증 마크를 획득한 기업들에서조차 대규모 개인정보 유출 사고가 반복되면서다. 결국 "돈만 내면 따는 면피용 간판 아니냐"는 비판에 직면하자, 정부가 뒤늦게 제도 전면 개편이라는 칼을 빼 들었다.

7일 〈메트로경제 신문〉 취재 결과, 정부는 지난 6일 송경희 개인정보위 부위원장과 류제명 과기정통부 제2차관 주재로 대책 회의를 열고 칼질을 시작했다. 이번 개정의 핵심은 '사후 처벌 강화'와 '진입 장벽 상향'이다.

ISMS-P는 과학기술정보통신부와 개인정보보호위원회가 공동 운영하는 제도로, 기업이 101개에 달하는 엄격한 보안 항목을 충족해야만 부여된다. 그러나 현실은 달랐다. 사회민주당 한창민 의원실 자료에 따르면 2020년 이후 ISMS-P 인증을 유지하고 있던 기업 27곳에서 총 34건의 개인정보 유출 사고가 터졌다.

권헌영 고려대학교 정보보호대학원 교수는 "현실에서는 실질 심사보다 형식적 심사에 그치는지 파악하기 어렵다"며 제도의 허점을 꼬집었다.

이에 따라 과학기술정보통신부와 개인정보보호위원회는 ISMS 및 ISMS-P 인증의 실효성 강화를 위해 관련 제도를 전면 개편하기로 했다. 정부 개편안의 목표는 '이름뿐인 인증'이 아니라 기업의 보안 능력을 확실하게 끌어올리는 제도로 기능을 정상화하는 데 있다. 그간 기업들이 인증을 마케팅 수단으로만 활용하고 실제 보안 투자에는 소홀했다는 '인증 무용론'을 불식시키겠다는 의지다.

우선 '무늬만 인증'인 기업의 자격을 박탈하는 고강도 처방이 내려진다. 기존에는 사고가 발생해도 인증이 유지되는 경우가 많았으나, 앞으로는 유출 사고 발생 시 즉각적인 '특별 사후 심사'가 진행된다. 심사 인력과 기간을 두 배로 늘려 진행하는 이 과정에서 중대 결함이 확인될 경우, 인증위원회 심의·의결을 거쳐 인증을 취소한다. 사실상 '원스트라이크 아웃' 제도가 도입되는 셈이다. 국회에서 '3370만 명의 개인정보를 유출한 쿠팡이 첫 인증 취소 사례가 되어야 한다'는 지적이 잇따르고 있어, 이번 제도 개선이 실제 기업 퇴출로 이어질지 주목된다.

심사 방식도 현장 중심으로 대폭 바뀐다. 그동안 서류와 샘플 점검 위주였던 본심사는 핵심 시스템에 대한 실증형 검사로 전환된다. 진입 장벽도 높아진다. 정부는 예비심사 단계에서부터 핵심 항목을 우선 검증하고, 기준 미충족 시 인증 신청 자체를 반려하기로 했다. 특히 과거 유출 사고 이력이 있거나 위험도가 높은 기업은 예비 심사 단계부터 취약점 진단과 모의 해킹(침투 훈련) 등 고강도 기술 심사를 거쳐야 한다.

아울러 정부는 대형 온라인 플랫폼이나 통신사, 주요 공공시스템 등 국민 생활과 밀접한 개인정보처리시스템에 대해 ISMS 및 ISMS-P 인증을 의무화하는 개인정보보호법·정보통신망법 개정도 추진한다. 자율에 맡겼던 영역을 법적 의무로 강제해 관리 사각지대를 없애겠다는 취지다.

양청삼 개인정보보호위원회 개인정보정책국장은 "ISMS, ISMS-P 인증을 받은 기업 중 유출 사고가 일어난 곳은 약 10%로 인증이 '아무 의미가 없다'고 볼 수는 없다"면서도 "제도의 순기능을 잘 살려 국민에게 신뢰받는 제도로 만들겠다"고 설명했다.

정부는 내년 1분기 중 관련 고시를 개정해 시행할 방침이다. 하지만 전문가들은 인증 제도 강화만으로는 기업들의 '보안 불감증'을 뿌리 뽑기 어렵다고 입을 모은다.

미국의 경우 연방거래위원회(FTC)가 페이스북(현 메타)의 개인정보 위반에 대해 연 매출의 9%에 달하는 50억 달러(약 6조5000억 원)의 과징금을 부과한 바 있다. 반면 한국은 여전히 처벌 수위가 낮아 기업들이 보안 투자보다 과태료를 내는 편을 택한다는 비판이 제기된다. 인증 취소를 넘어, 징벌적 손해배상제도 강화 등 실질적인 금전적 타격을 줄 수 있는 구조가 마련되지 않는다면 이번 개정안 역시 '보여주기식 행정'에 그칠 수 있다는 우려가 나온다.

/김서현 기자 seoh@metroseoul.co.kr

정부, IP카메라 영상피해 방지 종합대책 마련

정부, 취약 비밀번호 해킹에 즉각 대응
피해자 지원 확대, 관련범죄 수사 강화
신체노출 시설 중심 보안인증 의무 추진

정부는 지속되는 IP카메라 해킹과 영상 유출로 인한 피해를 줄이기 위해 지난해 11월 발표한 'IP카메라 보안강화 방안'의 후속 대책을 마련해 추진한다고 7일 밝혔다. IP카메라는 가정과 사업장, 의료기관, 공공시설 등에서 안전관리용으로 활용되고 있으나, 해킹과 영상 유출 범죄가 계속 발생하며 국민 피해가 이어지고 있다.

최근 검거된 해킹 피의자들이 침입한 약 12만 대의 IP카메라는 단순하거나 이미 유출된 비밀번호를 사용해 추가 피해 우려가 큰 것으로 파악됐다. 정부는 통신사와 협력해 IP 정보를 바탕으로 이용자를 식별하고, 비밀번호 변경 등 보안조치 이행을 권고할 예정이다.

아울러 해킹 피해자 보호를 위해 성착취물 영상 삭제·차단, 법률·의료·상담 지원을 제공하고, 대규모 영상 유출 사업장에 대해서는 개인정보보호법 위반 여부를 우선 조사한다. IP카메라 해킹, 성착취물 판매·유통, 해당 영상의 구입·소지 등 관련 범죄에 대한 수사도 강화한다.

지난해 실시한 IP카메라 보안 실태조사 결과, 설치 대행업체와 이용자 모두 보안조치 필요성에 대한 인식이 낮은 것으로 확인됐다. 이에 다중이용시설 설치 대행업체를 대상으로 'IP카메라 설치·운영 보안 가이드'를 배포하고, 설명회를 통해 보안조치 이행을 유도한다.

범죄 위험이 큰 업종을 대상으로는 개인정보보호법상 안전성 확보 조치 의무를 고지하고 보안수칙을 지속 안내한다. 고령자와 농어민 등 디지털 취약계층을 대상으로는 디지털 교육 프로그램을 활용해 피해 사례와 보안수칙 교육을 진행한다.

또 기존 사후 점검 방식에서 벗어나 관계부처 합동 사전 점검과 개선조치를 실시하고, 주요 제품의 보안성 점검 결과도 공개할 계획이다.

병원, 수영장, 산후조리원 등 신체 노출 시설에서 사용하는 IP카메라는 보안인증 제품 사용을 의무화하는 법률 제정을 추진한다. 또한 제품 설계 단계부터 복잡한 비밀번호 설정 기능을 탑재하도록 관련 제도 개선도 병행한다. 기존 출시 제품에도 해당 기능이 적용될 수 있도록 제조사와 협의를 진행한다. /김서현 기자

엔씨소프트, '리밋 제로 브레이커스' 공개

AGF서 신작 시연하고 CBT 모집 진행

엔씨소프트가 6일 경기도 고양시 일산 킨텍스에서 개최한 애니메이션·게임 페스티벌인 'AGF 2025'에 서브컬처 애니메이션 액션 RPG '리밋 제로 브레이커스'로 참가했다고 7일 밝혔다.

브레이커스는 빅게임스튜디오가 개발하고 엔씨소프트가 퍼블리싱하는 애니메이션 수집형 액션 RPG다. 일본 엔터테인먼트 기업 카도가와와 협업하고 애니메이션 제작사 MAPPA도 참여했다.

행사 현장에서는 '위버랜드를 부탁해', '크리스티앙의 지원사격' 등 미니게임과 룰렛 이벤트를 운영했다. 코스어 '마이부'가 주요 캐릭터 '헬렌'으로 분장해 관람객들의 이목을 끌었고, 유튜버 '빙하유'와 '라디유'도 테마 카페 구역에 참여했다.

엔씨소프트는 이번 행사에서 브레이커스의 비공개 테스트(CBT) 참가자 모집도 함께 진행했다. 신청은 AGF 현장과 공식 홈페이지를 통해 가능하며, CBT는 구글 플레이와 스팀에서 진행된다. 참가자 중 일부는 추첨을 통해 경품도 제공된다.

브레이커스는 원소의 힘을 다루는 능력자 '브레이커'들이 자신의 소원을 이루기 위해 '신들의 서고'로 향하는 모험을 그린 작품이다. 모두를 위한 영웅이 아니라 각자의 삶을 세우기 위해 떠나는 이야기를 전면에 내세운 점이 특징이다.

/김보민 기자 kbm@

LGU+, AI 비서 '익시오' 개인정보 유출

캐시설정 오류로 타인 통화정보 노출
즉시 차단 조치 후 피해자 안내 완료

LG유플러스가 야심 차게 내놓은 인공지능(AI) 통화 비서 '익시오(ixi-O)'에서 개인정보 유출 사고가 발생했다. 특히 이번 사고는 LG유플러스가 '온디바이스 AI' 기술을 앞세워 강력한 보안과 프라이버시 보호를 핵심 마케팅 포인트로 삼아온 직후 발생해 타격이 불가피할 전망이다. LG유플러스는 지난 6일 개인정보보호위원회에 익시오 통화정보 유출 사실을 자진 신고했다고 7일 밝혔다.

사측에 따르면 사고는 지난 2일 오후 8시부터 3일 오전 10시 59분 사이에 발생했다. 최근 진행된 익시오 서비스 운영 개선 작업 중 개발진의 '캐시(임시 저장 공간)' 설정 오류가 원인이었다. 이로 인해 해당 시간 동안 익시오 앱을 새로 설치하거나 재설치한 이용자 101명의 화면에, 엉뚱하게도 다른 고객 36명의 개인정보가 일시적으로 노출됐다.

노출된 정보는 ▲통화 상대방 전화번호 ▲통화 시각 ▲통화 내용 요약 등이다. 주민등록번호나 금융 정보는 포함되지 않았지만, 사적인 대화가 AI로 요약된 텍스트 정보가 생면부지의 타인에게 그대로 보여진 셈이다. 피해 고객 1명의 정보가 최소 1명에서 최대 6명에게까지 노출된 것으로 확인됐다.

LG유플러스는 지난 10월 개인 맞춤형 기능을 강화한 '익시오 2.0'을 공개하고, 이어 11월에는 구글 클라우드와 협력해 '익시오 AI 비서'를 선보이며 공격적인 행보를 보여왔다. 데이터가 서버로 전송되지 않고 기기 자체에서 처리되는 '온디바이스 환경'을 구축해, 보이스피싱 탐지와 통화 요약 기능을 안심하고 쓸 수 있다는 점을 최대 강점으로 내세웠다. LG유플러스는 3일 오전 10시경 문제를 인지한 즉시 원인 파악과 복구 작업에 착수해 노출을 차단했다고 설명했다. 피해 고객 전원에게는 유선과 문자 등으로 개별 안내를 마친 상태다. /김서현 기자

공공 행정 혁신 이끄는 AI 서비스 공개

네이버클라우드 정부혁신 박람회 참여

네이버클라우드는 '2025 대한민국 정부혁신 박람회'에서 공공 업무와 행정 전반의 효율성을 높일 수 있는 인공지능(AI) 기반 서비스를 소개했다.

이번 행사에서는 실제 공공 현장에서 활용 중인 AI 서비스를 중심으로 행정 분야의 AI 전환 사례가 공유됐다.

행사 현장에서는 범정부 지능형 업무관리 플랫폼으로 시범 운영 중인 네이버웍스를 비롯해 AI 안부 전화 서비스 클로바 케어콜, 공공망에서 AI를 개발·운영할 수 있는 'CLOVA Studio for Gov' 등 행정·민원 업무의 생산성을 높이는 서비스가 시연됐다.

특히 네이버웍스는 행정안전부, 과학기술정보통신부, 식품의약품안전처 등 주요 중앙 부처에서 시범 운영 중인 업무 협업 플랫폼으로, 회의록 자동 요약, 메일 요약 및 답장 초안 생성, 미열람 메시지 요약, 기관별 맞춤형 AI 어시스턴트 생성 등 공공 행정에 특화된 기능을 제공한다.

현장에서 열린 '웍스 워크숍' 세션에서는 제주도청, 부산광역시 등 주요 공공기관이 네이버웍스를 도입해 업무 방식을 개선한 사례가 소개됐으며, AI 기반 행정 업무 전환이 실제 현장으로 확산되고 있음을 보여줬다.

/김서현 기자