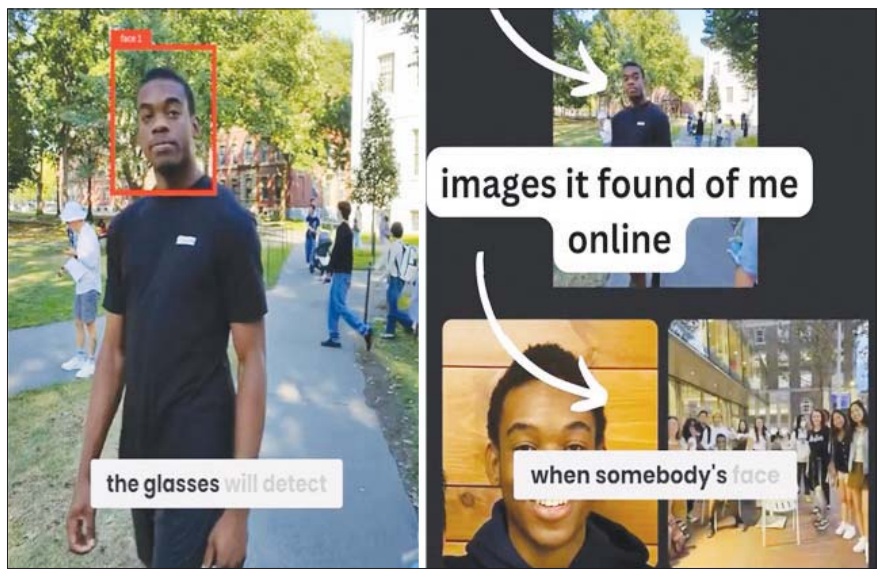
‘이름·전화번호 노출, 90초면 끝’ AI 스마트안경, 규제 논란 확산

하버드생, 개인정보 침해 가능성 입증
사회적 감시·범죄 악용 위험 부상
법적·윤리적 규제 마련 시급성 강조



미국 하버드 대학생 안푸 응우옌과 케인 아르다이피오가 X(구 트위터)와 인스타그램 등 사회관계망서비스(SNS)를 통해 공개한 ‘아이 엑스레이(I-Xray)’ 프로젝트 시연 장면. AI 스마트 안경으로 길거리에서 마주친 사람의 얼굴을 인식, 검색 엔진과 거대언어모델을 활용해 온라인 상에 퍼져있는 신원을 파악한다. /AnhPhu Nguyen X 계정. 이혜민 기자 재가공

메타와 애플 등 글로벌 정보통신기술(IT) 기업들이 인공지능(AI) 기반 스마트 안경을 잇달아 선보이며 기술 경쟁을 가속화하는 가운데, 미국 하버드대 학생들이 ‘AI스마트 안경’의 심각한 악용 가능성을 드러내며 논란이 일고 있다.

3일 업계에 따르면, 하버드대 학생 안푸 응우옌과 케인 아르다이피오는 아이 엑스레이(I-Xray) 프로젝트를 통해 ‘AI스마트안경’이 개인정보 침해의 도구로 악용될 수 있음을 입증했다.

이들은 메타의 AI 스마트안경 ‘레이밴 메타2’와 얼굴 검색 엔진 ‘핌아이즈’ 기술을 결합해 길거리에서 마주친 사람들의 이름, 주소, 전화번호 등 개인정보를 실시간으로 파악하는 데 성공했다. 이 과정에서 수집된 데이터는 거대언어모델(LLM)에 전송, 신원 정보로 가공된 뒤 아이 엑스레이 모바일 애플리케이션(앱)으로 전송됐다. 모든 과정은 불과 1분 30초 만에 완료됐으며, 3명 중 1명꼴로 신상 정보를 알아내는 데 성공했다.

응우옌은 “이번 프로젝트는 기술의 잠재적 위험성을 경고하기 위한 실험일 뿐”이라며 “학교 과제로 시도해 본 프로젝트라 상용화할 생각은 전혀 없다”고 밝혔다.

논란이 커지자 메타 측은 즉각 해명에 나섰다. 메타 대변인은 “현재 ‘레이밴 메타2’에는 얼굴 인식 기능이 포함되어 있지 않다”면서 “실험에 사용된 기술은 특정 기기에 국한되지 않고 다른 기기에서도 작동한다”고 해명했다. 또 “레이벤 메타 안경은 녹음 중임을 알려주는 LED 표시등과 음성 명령 기능을 탑재해 개인정보 보호를 위한 안전장치가 있다”고 강조했다.

애플 역시 AI스마트안경 개발 과정에서 개인정보 보호를 최우선으로 삼겠다는 입장을 밝혔지만, 안전장치에 대한 구체적인 계획은 공개하지 않았다.

전문가들은 이번 실험이 AI스마트안경 기술의 법적·윤리적 공백을 명확히 드러냈다고 평가했다. 우드로 하르초그 보스턴대 교수는 “미국 현행법상 공공장소에서 얼굴 인식 기술로 사람을 식별하는 것은 금지되지 않았다”면서 “법적 규제의 필요성을 언급했다.

유럽연합(EU) 데이터 보호 당국은 이미 2021년부터 이미 스마트안경의 개인정보 침해 가능성을 경고하며, LED 표시등만으로는 촬영 여부를 효과적으로 알릴 수 없다고 지적한 바 있다.

AI스마트안경의 딥페이크 기술 결합 가능성도 심각한 우려를 낳고 있다. 이를 활용해 타인의 얼굴을 조작하거나 위조된 영상을 생성하는 경우, 개인정보 침해를 넘어 사회적 혼란과 법적 문제를 초래할 수 있다.

전자 프런티어 재단(EFF)의 커트 옵살은 “스마트안경이 대중화될 경우 익명성을 파괴하고, 사회적 감시와 범죄 도구로 악용될 위험이 크다”며 강력한 규제를 촉구했다.

현재 AI스마트안경 시장은 급속히 성장하고 있다. 메타의 ‘레이밴 메타’는 연간 200만대 이상 판매가 예상되며, 중국 바이두와 샤오미 등도 관련 기술을 선보이며 시장에 진입했다.

이러한 성장세에 국내 전문가들도 법적 규제에 속도를 낼 것을 제언했다. 한 전문가는 “AI스마트안경은 혁신적 기술이지만, 강력한 법적·윤리적 프레임워크 없이 사용된다면 심각한 부작용을 초래할 수 있다”고 규제 마련의 시급성을 강조했다.

/이혜민 기자 hyem@metroseoul.co.kr

LGU+ “내비가 실시간 신호정보 안내”

인천시에 교통정보 통신망 구축

LG유플러스가 교통신호정보를 실시간으로 제공할 수 있는 무선통신망을 인천광역시에 구축한다고 3일 밝혔다. 해당 통신망은 내비게이션을 통해 교통신호의 잔여 시간을 실시간으로 확인할 수 있도록 도와 사고 위험성을 줄일 것으로 기대된다.

기존 통신망은 단일 회선으로 교통신호제어기에서 수집된 교통신호 정보가 인천교통정보센터에만 전달됐다. LG유플러스가 새롭게 구축하는 통신망은 다회선으로 경찰청 도시교통정보센터와 한국도로교통공단도 동시에 교통신호 정보를 받을 수 있다.

신규 통신망을 통해 경찰청, 한국도로교통공단이 신호 정보를 사용할 수 있게 되면서 미래 자율주행차 시대를 앞당길 수 있는 다양한 서비스들이 가능해질 전망이다.

한국도로교통공단은 교통신호제어기를 통해 받은 신호 정보를 내비게이션 회사들과 공유해 운전자들이 실시간으로 교통신호의 잔여 시간을 확인할 수 있도록 할 계획이다.

LG유플러스는 인천교통정보센터가 원격으로 무선 통신 상태를 확인할 수 있는 관제 시스템도 새롭게 구축할 예정이다. 문제가 발생할 경우 운전자의 신고 없이도 관제실에서 상태를 확인해 선제적인 조치가 가능하다.

LG유플러스는 이번 무선통신망 구축이 완전 자율주행 시대를 앞당기는 기반 기술이 될 것으로 기대하고 있다. 차량이 신호정보를 실시간으로 제공받으면 신호를 인식하지 않고도 안정적인 주행이 가능하기 때문이다.

LG유플러스는 내년 1분기까지 전체 2400여개소의 교통신호제어기에 자사 무선통신망을 구축하고, 사전 테스트를 거쳐 2025년 상반기에는 상용화할 예정이다.

/구남영 기자 koogija_tea@

LG CNS, 美서 스마트 빌딩 DX사업 본격화

소메라로드·마스턴아메리카와 협약

LG CNS가 미국 건물에 DX기술을 적용해 빌딩 자산 가치를 높이는 사업에 나선다.

LG CNS는 미국 부동산 전문 운용사인 소메라로드(SomeraRoad), 대체투자 운용사 마스턴투자운용 미국 법인 마스턴아메리카(Mastern America)와 업무협약(MOU)을 체결했다고 3일 밝혔다.

소메라로드는 부동산 투자 및 개발을 전문으로 하는 회사로 호텔, 물류센터, 산업단지 등의 부동산을 미국 전역에서 개발하고 운용하고 있다. 마스턴아메리카는 다양한 부동산 영역에 대한 투자, 개발, 운용 전문성을 보유하고 있는 회사다.

이번 MOU를 통해 3사는 미국 미주리주 캔자스시티, 테네시주 내슈빌 등에 있는 스마트 호텔, 리조트와 스마트 멀티패밀리(다세대 임대주택) △스마트 상업용 빌딩 등에 DX 기술을 접목하는 스마트 부동산 사업을 공동으로 추진할 계획이다.

LG CNS는 소메라로드와 마스턴아메리카의 부동산 개발 사업 내 DX기술 관련 전반을 맡는다. 먼저 LG CNS

LG CNS 최문근 전무(가운데)가 소메라로드 이안 로스(Ian Ross) CEO(오른쪽), 마스턴아메리카 오진석 대표이사(왼쪽)와 MOU 체결 후 기념사진을 촬영하고 있다. /LG CNS

는 호텔, 리조트, 멀티패밀리, 오피스 등에 ‘시티허브 빌딩(Cityhub Building)’ 플랫폼을 적용해 스마트빌딩을 구현한다.

시티허브 빌딩은 LG CNS가 자체 개발한 빌딩 통합운영 플랫폼으로 빌딩, 공장 같은 대형 건물의 데이터 수집, 설비 관리·제어, 에너지 관리 등을 한 번에 할 수 있는 다양한 기능을 제공한다.

3사는 스마트 항공 인프라에 DX기술을 도입하는 프로젝트도 논의하며 사업모델을 다각화해 나갈 예정이다.

/김서현 기자 seoh@

“사이버 공격 속도 빨라져 … 대응시간 부족”

SK쉴더스, ‘사이버 시큐리티’ 개최
AI 기술 활용 새 보안 체계 확장 필요

기업의 취약점을 발견해 사이버 공격을 감행하는 기간이 과거 2년 전 대비 30일 가량 단축된 것으로 드러났다.

SK쉴더스가 3일 서울 강남구 코엑스에서 열린 ‘2024 SK쉴더스 사이버 시큐리티’를 열었다. 이번 행사는 SK쉴더스의 전문가들이 올해의 보안 트렌드를 돌아보고 내년도 주요 위협과 대응 방안을 공유하기 위해 마련됐다.

홍원표 SK쉴더스 대표는 “최근 사이버 위협이 경영 리스크로 자리잡은 만큼 사이버 보안 확충이 산업·안보·사회 안정을 좌우하는 것은 물론 대비가 산업 생태계 전반으로 확장할 필요성이 커졌다”며 “AI가 만들어내는 산업 구조의 변화에 대비하기 위해 AI를 통제 가능한 모델로 사이버 보안 영역에 도입해야 할 것”이라고 말했다.


홍원표 SK쉴더스 부회장이 3일 삼성동 코엑스에서 열린 ‘2024 SK쉴더스 Cyber Security Media Day’에서 오프닝 연설을 하고 있는 모습. /SK쉴더스

SK쉴더스의 분석에 따르면 사이버 공격자가 제조사·개발자 보다 먼저 발견한 보안 문제인 ‘제로데이 취약점’이 악용되기까지 걸린 시간은 2022년 768시간(32일)이었다. 그러나 단 2년 만인 올해는 114시간(4.75일)로 나타났다. 제로데이 발견 시점과 이를 이용한 공격 시간의 간격이 줄어들며 대응 시간이 부족해지고 있다. 공격자가 감염 컴퓨터를 원격 제어하는 ‘원격 접근 트로이 목마’는 취약점 공개 5시간만에 악용되기도 했다

이날 SK쉴더스가 공개한 올해 업종별 사이버 보안 침해 사고 유형은 국내외 통틀어 공공 부문이 1위로 나타났다. 국내에서는 공공·제조 분야가 18%였고 국외에서는 공공 부문이 30%로 나타났다. 국내에서는 법무법인 등 서비스업 대상 기업을 향한 공격사례도 다수 나타났다.

올해 주요 사이버 위협으로는 랜섬웨어 그룹의 전략 고도화였다. 랜섬웨어는 가상환경인 하이퍼바이저 환경으로까지 공격이 확대됐으며 원격 모니터링·관리도구 취약점 악용 등 유포 방식도 더욱 정교해졌다.

알리스테어 닐 버라이즌 글로벌 정보보안 총괄은 “최근 랜섬웨어 침해 사고로 7천500만 달러를 요구한 사례가 있다”며 “해당 랜섬웨어 회복에 사용된 비용이 10억 달러로, 랜섬웨어 금액이 증가하고 방식이 고도화하는 게 트렌드”라고 말했다. /김서현 기자 seoh@

롯데케미칼, 여수 2공장 일부 라인가동 중단

“운영 효율화 조치”

롯데케미칼이 여수 2공장의 일부 라인을 가동 중단한다. 공장 수율화를 위한 조정 차원에서 이루어진 조치다.

3일 업계에 따르면 롯데케미칼은 여수 2공장내 에틸렌글리콜(EG), 산화에틸렌유도체(EOA) 등의 생산 라인을 가동 중단했다. 크래커 가동률이 전반적으로 낮아진 상태에서 원료 부족 등의 요인이 영향을 미친 것으로 분석된다.

앞서 롯데케미칼은 수익성을 고려해 여수PET 라인을 가동중단한 바 있다.

롯데케미칼 관계자는 “기초화학 생산부문의 원가 절감과 수익성 확보를 목표로 공장 단위의 운영 효율화를 지속적으로 추진 중”이라며 “현재 크래커 가동률 조정에 따라 다운스트림 일부 라인의 가동을 탄력적으로 운영하고 있으며, 최적의 가동 방안을 검토하고 있다”고 말했다. /차현정 기자 hyeon@