

# 통신3사, 개인정보보호 강화 발 맞춘다... 체계 전반 점검

KT, CISO·CPO 각각 분리 선임  
보안분야에 연간 2000억 투자  
SKT, 정보보호 조직 독립성 강화  
앤스로픽 협력 대응체계 구축  
LG U+, 화이트 해커와 사전점검



국내 이동통신 3사가 개인정보 보호에 대한 정부의 규제 강화 기조에 따라 보안 체계를 대폭 강화하고 있다. /첫GPT 생성 이미지

국내 이동통신 3사가 정부의 개인정보 보호 규제 강화 기조에 따라 보안 체계를 대폭 강화하고 있다. 정부가 개인정보보호책임자(CPO)의 독립성을 높이고 개인정보 유출 사고에 대한 기업 책임을 강화하는 내용의 개인정보보호법 개정안을 시행하는 것에 대한 대응 차원이다.

4일 정부 및 업계에 따르면 개인정보보호법 개정안이 오는 9월 11일부터 시행된다. 개인정보보호책임자(CPO)의 독립성을 강화하고 정보보호 및 개인정보보호 관리체계(ISMS-P) 인증 대상을 확대하는 등 기업의 개인정보 보호 의무를 강화한 것이 핵심이다.

그동안 CPO는 기업 내 개인정보 보호를 총괄하면서도 인사나 예산 권한이 없어 제 역할을 하기 어렵다는 지적이 많았다. 이에 정부는 일정 규모 이상 기업의 CPO 인사를 이사회 의결과 개인정보위 신고 대상으로 못 박아 신분 보장을 강화하기로 했다.

이에 따라 앞으로 이사회 의사결정에

따라 개인 정보와 관련한 최고 책임자를 결정하게 되면서 거버넌스 체계 전반에 대한 점검이 불가피해졌다. 특히 개정법안에 따르면 CPO를 임명 또는 교체, 해임할 때에는 이사회 의결 절차를 거쳐 개인정보보호위원회에 신고해야 한다.

통신사들은 이미 관련 조직 개편에 나선 상태다. KT는 올해 박윤영 대표 체제

전환 이후 최고정보보호책임자(CISO)와 CPO를 각각 분리해 선임했다. SK텔레콤은 지난해 8월 해킹 사고 이후 재발 방지를 위한 후속 조치의 일환으로 CISO 겸직 체계를 개편하며 정보보호 조직의 독립성을 선제적으로 강화했다. LG유플러스는 정보보안센터장이 CISO와 CPO를 겸직하는 체계를 유지하고 있다.

정보보호 인증에 대한 관리도 한층 엄격해질 전망이다. 현재 통신 3사 모두 ISMS-P 인증을 보유하고 있어 정보통신서비스 인프라 운영과 이동전화 고객 관리 서비스에 대한 인증을 유효 기간에 맞춰 한국인터넷진흥원(KISA) 등을 통해 갱신해 왔다.

지난해 잇달아 발생한 해킹 사고로 인해 인증 취득 여부보다 실제 운영 체계와 사고 대응 역량이 중요하다는 지적이 제기됐다. 이에 따라 보안 체계 운영과 사고 대응 역량에 대한 점검이 더 엄격해질 것으로 보인다.

보안 모니터링 강도도 높아질 것으로 관측된다. 기존에는 개인정보가 분실되거나 유출됐을 경우에만 신고 의무가 있었지만 앞으로는 위조·훼손 사고가 발생한 경우에도 72시간 이내 신고해야 한다. 반복적인 법 위반에 대한 과태료 부과 기준도 부담이다. 과거 경로나 과태료 면제 처분을 받았더라도 유사한 위반 행위가 반복되면 더 높은 수준의 과태료가 부과될 수 있다.

통신 3사는 정보 유출 사전에 막기 위한 보안 투자를 확대하고 있다. KT는 보안 분야에 연간 2000억원의 투자를 대대적으로 진행한다. SK텔레콤은 글로벌 인공지능(AI) 기업 앤스로픽과 협력해 AI 기반 사이버 위협 대응 체계를 구축한다. LG유플러스는 정부가 승인한 화이트해커와 협력해 잠재적인 취약점을 사전에 점검해 선제 대응한다.

/조민선 기자

msjo@metroseoul.co.kr



## KT, 금융사 대상 최적화 AX 전략 공유

글로벌 6G 동향·기술 패러다임 담아서  
사이버 보안 강화 사례 등도 설명

KT가 금융사들을 위한 인공지능 전환(AI) 전략과 사이버 보안 강화 사례를 공개했다. KT는 KT 광화문빌딩에서 금융 고객을 대상으로 금융 최적화 AX 전략을 공유했다고 4일 밝혔다.

최근 디지털 전환에 따라 금융 산업 현장에서 네트워크 기반 인프라의 안정성과 업무 혁신을 위한 AX 전략의 중요성이 커지고 있다. 이에 따라 KT는 금융업계 IT 실무 고객 50여명을 초대해 금융 환경에 최적화된 AX 인프라 전략과 운영 혁신 방향을 제시했다.

특히 KT는 글로벌 6G 동향과 기술 패러다임 변화를 담은 'KT 2026 네트워크 전략'과 국내 금융사의 AX 트렌드 및 협력 사례 등을 폭넓게 소개했다. KT 커뮤니케이션 서비스를 도입한 고객사의 실제 활용 사례를 발표해 참석자들의 공감을 이끌어냈다.

KT 엔터프라이즈서비스부에서 주도한 인프라 트랜스포메이션 세션에서는 안정성과 보안성이 강화된 플랫폼 전략을 중심으로 구체적인 서비스 적용 사례를 공유하기도 했다. 주제는 'KT 스마트메시



4일 김원태 KT 공공·금융사업본부장(전무)이 서울 광화문 KT 웨스트 사옥에서 금융 고객을 대상으로 KT의 금융 산업 최적화 AX 전략을 공유하고 있다. /KT

지가 제공하는 고객 커뮤니케이션 가치 혁신'으로, 변화하는 소비자 행태와 커뮤니케이션 트렌드에 대응하는 기업메시징 전략을 설명했다. 주요 상품 라인업인 ▲스마트메시지 RCS ▲커뮤니즈 ▲모바일 고지 등도 공개했다.

KT 기업메시징의 안정성과 빅데이터 기반 분석 리포트, 아이폰 RCS 자동전환 등 플랫폼의 차별화된 경쟁력을 강조하고, 실제 적용 고객 사례를 통해 서비스 도입 효과를 구체적으로 설명했다.

보안 플랫폼 '클린존'을 통한 디도스 대응 전략도 공유했다. 클린존은 디도스 공격 발생 시 유해 트래픽을 차단하고 정상 트래픽만을 서버로 전달해 서비스 중단

없이 안정적인 운영을 지원하는 클라우드 기반 보안 솔루션이다. 현장에서는 실제 공격 대응 사례와 함께 운영 방식, 관제 경험, 기술 노하우 등이 함께 소개됐다.

AI 기반 금융서비스 안정성과 생산성 혁신 방안으로 'KT 매니지드 AIGPU 서비스'를 통한 AI 인프라 운영 방안도 제안했다. 해당 서비스는 AI 솔루션과 GPU 인프라를 통합 제공하는 구독형 모델로, 인프라 구축 부담 없이 AI 개발에 집중하려는 기업과 연구기관의 수요를 반영한 것이 특징이다.

향후 다양한 산업 분야 고객으로 대상을 확대해 AX 전략 설명 자리를 지속적으로 마련할 계획이다. /조민선 기자

## NC AI, 조선업 자율용접 로봇 'AI 두뇌' 개발

한화오션 과제 최종 수주

NC AI가 조선업계의 숙원 과제인 용접 자동화·자율화를 위한 로봇 인공지능(AI) 두뇌 개발에 나선다.

NC AI는 한화오션의 비전 인식 기반 용접 전용 모델 및 협동로봇 기반 자율용접 모델 개발 과제를 최종 수주했다고 4일 밝혔다. 이에 따라 NC AI는 한화오션과 본격적인 협업 체계를 가동할 예정이다.

이번 과제는 그동안 숙련공의 노하우에 의존해 온 선박 건조의 핵심 공정인 용접 작업에 AI 비전 인식과 정밀 로봇 제어 기술을 융합하는 프로젝트다. 정해진 궤적을 반복하는 기존 자동화의 한계를 넘어, 로봇이 용접 부위를 스스로 인식·판단해 실시간으로 최적의 용접을 수행하는 '자율용접 솔루션' 구현이 목표다.

NC AI는 이번 수주로 산업 특화 AI 분야에서의 기술 경쟁력을 다시 입증했다고 자평했다. 앞서 현대로템과 다중·다중 로봇을 통제하는 국방 AX 분야 국책과제를 수행하고 포스코DX와 로봇 AI 기술협력을 진행해 온 NC AI는 난도가 높은 '조선·해양' 도메인까지 사업 영역을 넓히게 됐다는 설명이다.

조선소 용접 공정은 선박 제조 원가와



품질을 좌우하는 핵심 작업이지만, 강력한 이크 광과 불꽃, 용접 분진, 야외 환경에 따른 카메라 렌즈 오염 등 비전 인식 AI가 작동하기에 열악한 조건을 갖고 있다.

NC AI는 이를 극복하기 위해 한화오션의 실제 작업 현장 데이터와 엔지니어 피드백을 반영하는 현장 밀착형 연구를 진행 중이다. 노이즈와 오염 속에서도 용접선을 정밀하게 추출하고 결함을 실시간으로 잡아내는 조선 특화 비전 인식 기술을 완성하겠다는 방침이다. 개발된 자율용접 모델과 로봇 시스템은 한화오션이 건조할 차세대 상선과 특수선 공정에 실제 적용될 예정이다.

NC AI는 용접 자율화의 핵심 동력으로 멀티모달 기술력을 내세웠다. 지난해 공개한 비전언어모델 '바르코비전 2.0'의 성능을 업그레이드한 차세대 산업 특화 VLM '배키 비전'을 올해 발표하고 이번 과제에 핵심 엔진으로 적용한다는 계획이다.

/최빛나 기자 vitna@

## SKT, 앤스로픽 '프로젝트 글래스wing' 합류

사이버 보안 국제 협력 프로그램  
'클로드 미토스' 프리뷰 접근권 확보

SK텔레콤이 글로벌 기업들과 디지털 보안 강화에 나선다.

SK텔레콤은 해킹 대응 체계를 공동 구축하는 앤스로픽의 '프로젝트 글래스wing'에 합류했다고 4일 밝혔다.

프로젝트 글래스wing이란 앤스로픽의 고성능 AI 모델 '클로드 미토스'를 활용해서 사이버 보안 취약점을 검증하고 대응 체계를 공동으로 구축하는 국제 협력 프로그램이다. 참여 기업은 클로드 미토스 프

리뷰 접근권을 확보하게 된다. 이는 고성능 AI 모델로 수준 높은 공격 시나리오를 생성할 수 있어 일반 고객에 공개되지 않고 한정적으로 부여한다.

최근 앤스로픽은 해당 프로젝트 대상을 전세계 15개국 150개 기업·기관으로 확대했다. 기존에는 미국 정부 및 영국 AI 보안 연구소 등 50여곳에 제한적으로 개방했었다. 국내에서는 이번 프로젝트 대상 확대로 SK텔레콤을 비롯해 한국인터넷진흥원(KISA)과 삼성전자, SK하이닉스 등이 참여하는 것으로 알려졌다.

SK텔레콤 관계자는 "이번 프로젝트를



미국 인공지능(AI) 기업 앤스로픽의 웹사이트 페이지와 기업 로고가 띄워져 있는 모습. /뉴스시스

통해 위협 요소를 선제 방어함으로써 핵심 인프라와 서비스 보안을 강화해 나갈 계획"이라며 "수 천만 국민의 일상을 함께하는 통신·AI 인프라 운영 기업으로서 이번 협력을 기반으로 대한민국 디지털 안보 강화에 기여하겠다"고 말했다. /조민선 기자

## 개보위, 티빙 개인정보 유출사고 조사 착수

유출 경위 등 법령 준수 여부 조사

개인정보보호위원회가 온라인 동영상 서비스(OTT) '티빙'에서 발생한 개인정보 유출 사고를 집중적으로 들여다본다.

개인정보위는 티빙의 개인정보 유출 신고를 접수하고 조사에 착수했다고 4일 밝혔다.

지난 2일 외부에서 티빙 가입자들의 개인정보가 저장된 데이터베이스(DB)에 비인가 접근으로 접속이 이뤄졌으며 개인정보 파일이 외부로 전송된 정황이 확인됐다. 이에 회사 측은 사고 인지 후 공격자 IP 접근 차단, 클라우드 접근통제 정책 변

경, DB 접속 모니터링 강화 등의 조치를 취했다고 설명했다.

유출 항목은 아이디, 이름, 생년월일, 성별, 연계정보(CI), 중복가입 확인정보(DI), 휴대전화번호, 이메일, 환불 계좌번호, 비밀번호 등이다.

과학기술정보통신부는 이번 사고에 대해 대규모 정보 유출과 추가 피해 발생 가능성이 있는 중대한 침해사고라고 보고, 민관합동조사단을 꾸리기로 했다. 개보위는 자료 제출 요구, 현장 조사 등을 통해 구체적인 유출 경위와 피해 규모, 안전조치 의무 및 유출 통지·신고 의무 등 관련 법령 준수 여부를 조사한다. /조민선 기자