

AI, 해킹 10분 만에 취약점 7건 찾아... '국산 보안AI' 만들어야

과기부, 산학연 전문가 간담회
고성능 AI 모델 확장에 위기감
완벽 차단보다 '신속 대응' 핵심

정부, 실전 대응형 체계 전환부터
K-보안 체계·글로벌 협력 등 검토

정부가 생성형 인공지능(AI)을 활용한 차세대 사이버 공격 가능성에 대응하기 위해 독자적인 '보안 특화 AI 모델' 개발과 정보보호 체계 개편에 착수한다. 글로벌 빅테크 중심으로 재편되는 AI 보안 경쟁 속에서 'AI 보안 주권'을 확보하겠다는 전략이다.

10일 과학기술정보통신부에 따르면 배경훈 부총리 겸 과기정통부 장관은 지난 8일 산학연 전문가 간담회를 주재하면서 글로벌 AI 기업의 사이버보안 프로젝트 대응 방안을 논의했다.

이번 간담회는 최근 엔트로픽의 '미토스'와 오픈AI의 GPT-5.5 사이버 등 고성능 AI 모델이 취약점 탐지와 보안 분석 영역까지 빠르게 확장되면서 위기감이 커진 데 따라 마련됐다.

정부가 공개한 실험 결과는 AI 기반



배경훈 부총리 겸 과기정통부 장관이 8일 서울 종로구 광화문교보빌딩 국가과학기술자문회의 대회의실에서 열린 '빅테크 AI기업 사이버보안 프로젝트 관련 전문가 간담회'에서 발언하고 있다. /과기부

해킹 위협의 현실화를 보여준다. 과기정통부는 국내 기업과 협의해 엔트로픽의 최신 AI 모델을 활용한 모의해킹을 진행한 결과 약 10분 만에 7건의 취약점을 발견했다고 밝혔다. 인간 해커가 며칠 걸릴 작업을 AI가 단시간 내 수행한 셈이다.

최우혁 과기정통부 정보보호네트워크정책실장은 "AI 프롬프팅 수준에 따라 결과는 달라질 수 있지만, 해커의 작

업 속도를 획기적으로 높일 수 있다는 점을 확인했다"고 설명했다.

◆"완벽 방어보다 얼마나 빨리 막느냐가 핵심"

정부와 업계는 AI 시대 보안의 핵심이 '완벽한 차단'보다 '신속 대응'으로 이동한다고 본다. 공격 자체를 모두 막는 것은 사실상 불가능해진 만큼, 취약점을 얼마나 빨리 탐지하고 대응하느냐

가 중요해진다는 판단이다.

이에 정부는 화이트해커의 합법적 모의침투를 제도적으로 허용하는 방안을 검토한다. 실제 공격 환경을 기반으로 시스템 취약점을 선제 점검하는 방식이다. 업계에서는 기존 규제 중심 보안 체계에서 실전 대응형 체계로 전환되는 신호라는 평가가 나온다.

특히 정부는 장기적으로 국내 독자 '보안 특화 AI 모델' 개발도 추진한다. 글로벌 AI 모델 의존도가 높아질 경우 국가 핵심 보안 정보와 인프라가 해외 플랫폼에 종속될 수 있다는 우려 때문이다.

배경훈 부총리는 "정보보호 패러다임을 AI 기반 보안으로 전환해야 할 시점"이라며 "국내 AI 보안 특화 모델 개발과 제로트러스트 확산 등 대응 방안을 조속히 마련하겠다"고 밝혔다.

정부는 SK텔레콤과 엠펙스 등 독자 파운데이션 모델 개발 기업을 중심으로 'K-보안 AI' 체계를 검토하고 있다. 동시에 글로벌 AI 기업과의 협력도 확대한다. 정부는 엔트로픽 주도의 글로벌 보안 연합체 '프로젝트 글래스wing' 참여 가능성도 논의 중인 것으로 알려졌다.

◆"AI 위협 과장 경계해야" 신중론도

다만 업계에서는 AI 위협을 지나치게 과장해서는 안 된다는 의견도 나온다. 일부 전문가들은 현재 공개된 AI 모델이 전문 해커 수준 공격 역량까지 확보했다고 보기는 어렵다고 평가한다.

실제 이날 간담회에서도 AI 보안 모델의 과급력을 두고 의견이 엇갈렸다. AI가 보안 환경에 큰 변화를 가져올 것이라는 전망과 함께 기술 영향이 과대평가됐다는 신중론도 제기됐다.

그럼에도 AI 기반 공격 속도가 빠르게 고도화되는 만큼 기존 정보보호 체계만으로는 대응이 어렵다는 데에는 공감대가 형성됐다. 특히 국내 기업들은 망 분리 환경과 레거시 시스템 비중이 높아 취약점 패치와 대응 속도가 상대적으로 느린 구조라는 지적도 나왔다.

정부는 이달 말에서 내달 초 사이 AI 기반 사이버 위협 대응 종합 대책을 발표할 예정이다. 내년도 예산과 제도 개선안도 상반기 안에 확정해 AI 보안 대응 체계를 본격 구축한다는 방침이다. /최빛나 기자

vitna@metroseoul.co.kr



metro

NC AI, 분사 첫해 흑자... "IPO·외부투자 모두 검토"

매출 298억, 영업이익 50억 기록
게임산업서 축적한 AI 기술 '경쟁력'
'배키 커머스'로 커머스·콘텐츠 확장

NC AI가 분사 첫해 흑자를 기록하며 존재감을 키우고 있다. 생성형 인공지능(AI) 시장 경쟁이 과열되는 가운데, 수익성 확보에 어려움을 겪는 국내 AI 업계에서 안정적인 실적을 냈다는 평가가 나온다.

10일 업계에 따르면 NC AI는 지난해 매출 약 298억원, 영업이익 약 50억원, 당기순이익 약 42억원을 기록했다. 영업이익률은 약 16.9% 수준이다.

㈜엔씨 AI 연구 조직 'NC 리서치'가 지난해 2월 물적분할 방식으로 독립한 이후 약 11개월 만에 거둔 성과다.

AI 업계에서는 아직까지 뚜렷한 수익 모델을 확보하지 못한 기업이 많다. 거



NC AI가 게임산업서 축적한 AI 기술을 기반으로 분사 첫해 흑자를 기록했다. /따스이에 의해 생성된 이미지

대언어모델(LLM) 개발과 GPU 인프라 투자 부담이 커지면서 상당수 기업이 적자를 감수하는 구조다. 이런 상황에서 NC AI는 게임 산업에서 축적한 AI 기술을 기반으로 빠르게 상용화 모델을 구축

했다는 분석이 나온다.

◆"게임 AI에서 시작된 수익화... '실전형 AI 경쟁력'"

NC AI 경쟁력의 핵심은 실제 서비스 운영 과정에서 축적한 데이터와 AI 기술이다. 엔씨는 오래전부터 음성합성(TTS), 번역, 모션 생성, NPC 대화, 콘텐츠 제작 자동화 등에 AI를 활용해왔다.

NC AI는 이런 기술 자산을 기반으로 게임 산업 밖 기업 시장까지 사업 영역을 확대하고 있다. 최근 공개한 AI 기반 커머스 콘텐츠 제작 솔루션 '배키 커머스'가 대표 사례다. 상품 이미지를 기반으로 상세페이지와 마케팅 콘텐츠를 자동 생성하는 형태로 제작 비용과 시간을 줄이는 것이 핵심이다.

업계에서는 게임 산업에서 축적된 생형 AI 기술이 커머스와 콘텐츠 산업으로 확장되는 흐름이 본격화하고 있다는

분석도 나온다.

임수진 NC AI 최고사업책임자(CBO)는 최근 인터뷰에서 "게임 개발 과정에서 축적한 기술들이 다양한 산업에서도 활용 가능하다는 점을 확인하고 있다"며 "올해는 지난해보다 더 큰 폭의 매출 성장을 기대하고 있다"고 말했다.

◆"AI는 결국 수익화"... IPO·외부 투자 가능성도 열어둬

시장 관심은 자연스럽게 외부 투자와 기업공개(IPO) 가능성으로 이어진다. NC AI 역시 가능성을 열어둔 상태다.

임수진 CBO는 "외부 투자와 IPO 가능성은 모두 열어놓고 있다"면서도 "지금 은 우리만의 사업 구조와 성장 스토리를 정교하게 만드는 단계"라고 설명했다.

업계에서는 NC AI가 당장 상장 절차에 돌입하기보다는 실적 안정성과 독자 사업 구조 강화에 집중할 가능성이 크다

고 본다. 다만 분사 첫해 흑자 달성 자체가 시장에서는 의미 있는 신호로 받아들여진다.

최근 AI 시장 분위기가 단순 기술 경쟁에서 실제 수익성과 서비스 확장성 중심으로 재편되는 점도 긍정적 요소다. 글로벌 시장에서도 AI 스타트업 투자 기준이 기술력보다 '실제 수익 구조' 중심으로 이동하는 흐름이 뚜렷해지고 있다.

NC AI는 현재 엔씨와 협력을 유지하며 AI 연구개발과 콘텐츠 제작 자동화 영역도 계속 확대하고 있다. 게임 개발 생산성을 높이는 동시에 외부 기업 대상 AX 사업도 강화하는 구조다.

업계에서는 NC AI가 향후 엔씨의 AI 전략 전초기지 역할을 맡을 가능성에도 주목한다. 단순 게임 지원 조직을 넘어 독립 AI 기업으로 성장 기반을 만들고 있다는 분석이다.

임 CBO는 "엔씨는 첫 번째 고객이자 중요한 파트너"라며 "재무적 지원과 기술 협업 측면에서도 긴밀한 관계를 유지하고 있다"고 말했다. /최빛나 기자

SOOP-S27M, 스트리머·아티스트 음악 콘텐츠 협업 확대

음악 생태계 활성화·공동 콘텐츠 협력

SOOP(쑤)이 종합엔터테인먼트사 S27M 엔터테인먼트와 음악 콘텐츠 생태계 확대를 위한 협력에 나선다.

SOOP은 10일 S27M 엔터테인먼트와 음악 생태계 활성화 및 공동 콘텐츠 사업 추진을 위한 업무협약 MOU를 체결했다고 밝혔다.

S27M 엔터테인먼트에는 보컬 그룹 노을을 비롯해 나윤권, 정우석, 진호, 켄 등이 소속돼 있다. 회사는 아티스트 중심 음악 제작과 공연, 콘텐츠 사업을 기반으로 음악 지식재산권 IP 확장에 주력하고 있다.



S27M 엔터테인먼트 김재덕 대표(왼쪽)와 SOOP 이세민 소셜콘텐츠사업본부장이 엔터테인먼트와 음악 콘텐츠 생태계 확대를 위한 업무협약을 체결한 뒤 기념촬영을 하고 있다. /SOOP

이번 협약은 SOOP의 스트리머 기반 콘텐츠 제작 역량과 S27M의 아티스트·

음악 IP를 결합해 협업형 음악 콘텐츠를 확대하고 신규 수익모델을 발굴하기 위해 추진됐다. 양사는 라이브 스트리밍과 음악 산업을 연결해 스트리머와 아티스트가 함께 참여하는 새로운 음악 콘텐츠 생태계 구축에 나선다는 계획이다.

협약에 따라 양사는 ▲라이브·오디션·공연·음원 공동 콘텐츠 기획 및 운영 ▲스트리머·아티스트 협업 콘텐츠 제작 ▲S27M 소속 아티스트 홍보 및 콘텐츠 제작 지원 ▲신규 음악 IP 공동 개발 ▲음원·라이브 콘텐츠 기반 수익모델 발굴 ▲온·오프라인 이벤트·캠페인 운영 ▲글로벌 콘텐츠 협력 등 다양한 분야에서 협력을 이어간다. /최빛나 기자

LG U+, 비대면 고객 서비스 비중 확대

회수방식 변경·셀프 개통 등 늘려

LG유플러스가 비대면 고객 서비스 비중을 확대하고 있다.

10일 LG유플러스에 따르면, 최근 1인 가구 증가 등으로 홈네저의 방문을 기피하는 고객이 늘어나고 있다. 이에 인터넷 단말기 회수 방식을 변경하고 셀프 개통을 확대하는 등 비대면 전환에 나섰다.

먼저 단말기 포장 전용 박스를 제공해 회수지를 직장까지 확대했다. 여기에 편의점 택배 서비스까지 넓힌 결과 단말기 비대면 회수 건수는 지난해 3만6000여건에서 올해 4만3000여건까지 늘었다.

셀프 개통 서비스 범위도 공유기, 셋

톱박스, AI 스피커 등으로 늘리고, 공식 홈페이지를 통해 설치 안내 리플렛을 제공했다. 이에 월 평균 3000여건 수준에서 지난해 1만3000여건으로 급증하고, 올해에는 2만 건을 넘어섰다.

올해부터 AS 영역까지 비대면 서비스를 늘리기도 했다. 현재 전체 단말기 회수, 상품변경 개통의 비대면 서비스를 월 평균 6만건 이상 처리하고 있다. 이는 전체의 약 54% 수준이다.

고객 반응도 긍정적인 것으로 나타났다. 내부 조사 결과, 택배 개통 서비스를 추천하는 이유는 '홈네저를 기다릴 필요 없는 빠른 설치(52%)', '방문 없는 비대면 진행(17%)' 순이었다. /조민선 기자 msjo@