AI 에이전트로 생산성 혁신… 보안문제는 여전

AI, '답변' 넘어 스스로 '행동'
오픈클로, 컴퓨터 작업 자동 처리
SKT·네이버 등 맞춤형 기능 적용
에이전트 간 위험행동 전파 확인
일부 中·韓 기업서 사용금지 지침

AI 기술이 발전하면서 '행동하는 AI' 에이전트 AI가 실제 현장에서 활발히 사용되고 있다. /챗GPT로 생성한 이미지

인공지능(AI)이 '답변'하던 시대를 넘어, 스스로 판단하고 실행하는 '행동하는 AI', AI 에이전트 시대가 본격화하고 있다. 주요 IT 기업들이 AI 에이전트를 업무 전반에 도입하며 생산성 혁신 경쟁에 나선 가운데, 기술 고도화 속도만큼 보안 리스크도 함께 커지고 있다는 우려도 제기된다.

19일 〈메트로경제 신문〉 취재를 종합해보면 주요 IT 기업들이 AI 에이전트를 속속 도입하며 업무 활용 범위를 빠르게 확대하고 있다.

AI 에이전트는 일종의 비서와 같은 역할을 한다. 사용자의 목표를 이해하고 스스로 판단해 작업을 수행하는 자율형 인공지능 시스템이다. 기존 생성형 AI가 질문에 답하는 수준에 머물렀다면, AI 에이전트는 일정 관리, 정보 탐색, 업무 실행 등 여러 단계를 연속적으로 수행할 수 있다는 점에서 차별화된다. 다양한 외부 도구와 데이터를 연동해 실제 업무를 대신 처리하는 '행동하는 AI'로 진화하고 있다는 평가다.

AI 에이전트는 지난해까지만 해도 단순 일정 관리 수준에 머물렀지만, 1년 사이 급격한 기술 발전을 거치며 실제 업무에 투입 가능한 단계로 진화했다.

최근 주목받는 AI 에이전트 가운데 하나는 '오픈클로(OpenClaw)'다. 오픈클로는 2025년 11월 오스트리아 개발자 피터 슈타인베르거가 공개한 오픈소스 기반 자율형 AI 에이전트 플랫폼으로, 젠슨 황이 "인류 역사상 가장 성공적인 오픈소스 프로젝트 중 하나"로 언급해 주목을 받았다.

이 플랫폼은 사용자 기기에 직접 설치돼 키보드 입력과 마우스 조작을 스스로 수행하며, 파일 관리와 웹 탐색, 업무용 메신저 연동 등 사람이 수행하는 대부분의 컴퓨터 작업을 자동으로 처리할 수 있다.

국내 기업들도 도입에 속도를 내고 있다. SK텔레콤은 '1인 1 AI 에이전트' 구축을 목표로 사내 플랫폼과 교육 체계를 마련했다. 구성원들은 자연어 명령이나 모듈 조합 방식으로 업무에 특화된 AI 에이전트를 직접 생성할 수 있다.

네이버는 쇼핑 앱 '네이버플러스 스토어'에 AI 에이전트를 적용했다. 사용자가 키워드를 입력하면 상품 특성과 쇼핑 가이드를 제시하는 방식으로, 실시간 트렌드 분석, 연관 상품 추천, 장바구니 기능 등도 단계적으로 고도화할 방침이다.

다만 보안 문제는 여전히 해결 과제로 남아 있다. AI 에이전트는 기기의 광범위한 권한을 활용해 작동하는 만큼 잠재적 위험이 크다.

MIT 등 10여 개 기관 연구진이 발표한 논문에 따르면 일부 AI 에이전트는 성과 최적화 과정에서 조작, 담합, 전략적 방해 행동으로까지 확장되는 경향을 보였다. 악의적 프롬프트 없이도 인센티브 구조만으로 이러한 문제가 발생한 것이다.

구체적으로는 권한 없는 외부 지시 수행, 민감 정보 노출, 시스템 파괴 명령 실행, 서비스 거부 유발, 자원 무단 사용, 신원 위장, 에이전트 간 위험 행동 전파 등이 확인됐다. 이같은 일들이 실제 상황에서 일어났을 경우 치명적인 피해를 입힐 수 있다.

이런 우려 속에 중국 정부는 최근 주요 은행과 공공기관, 국유기업을 대상으로 보안 문제를 이유로 PC에 오픈클로 설치를 금지하는 지침을 내린 것으로 전해졌다. 국내에서는 네이버,카카오, 당근 등이 사내에서 오픈클로 등을 사용금지 한 상태다.

/김서현 기자 seoh@metroseoul.co.kr

카카오, 역대최대 실적에도… 규제·미래 먹거리 '변수'

메신저 넘어 생활 플랫폼 안착
'성숙단계 진입 기업' 시선 늘어
AI로 수익모델 차별화 '관건'

카카오가 지난해 사상 최대 실적을 기록했음에도, 성장의 정점에 가까워졌다는 평가와 함께 다음 먹거리와 규제 대응이 동시에 시험대에 올랐다는 시장의 시선이 나온다.

19일 IT 업계에 따르면 지난해 사상 최대 실적을 기록한 카카오를 향한 시장의 평가는 엇갈린다. 카카오는 2025년 연결 기준 매출 8조원대, 영업이익 7000억원대를 기록하며 역대 최대 실적을 냈다. 메신저 트래픽을 수익으로 전환하는 모델을 완성했다는 평가가 나오는 배경이다.

금융 확장은 카카오 성장의 또 다른 축이다. 카카오뱅크와 카카오페이는 간편한 사용자 경험을 앞세워 이용자를 빠르게 확보하며 금융 서비스 이용 방식을 바꿨다. 기존 금융권 대비 낮은 진입 장벽과 직관적인 인터페이스를 기반으로 금융을 일상 서비스로 끌어들였다는 분석이다. 콘텐츠 영역에서도 웹툰과 웹소설, 음악, 영상까지 사업을 넓히며 글로벌 시장 진출 기반을 마련했다. 일본을 중심으로 한 웹툰 사업은 카카오의 대표적인 해외 성과로 꼽힌다.

모빌리티를 포함한 생활 서비스 확장도 카카오 모델의 특징이다. 카카오 T를 중심으로 이동, 결제, 예약 등 일상 동선을 플랫폼 안으로 통합하면서 카카오는 단순 IT 기업을 넘어 생활형 플랫폼으로 진화했다.

이 같은 성장 속에서 최근 시장의 시선이 점차 바뀌고 있다. 플랫폼 영향력 확대 과정에서 골목상권 침해 논란과 수수료 구조에 대한 비판, 정부 규제 이슈가 반복되면서 성장의 속도와 방향에 대한 의문이 제기되고 있기 때문이다. 실제로 카카오는 최근 몇 년간 계열사 정리와 사업 구조 재편 등 '선택과 집중' 전략에 나서며 체질 개선을 진행해왔다.

증권가에서는 카카오를 '성숙 단계에 진입한 플랫폼 기업'으로 보는 시각이 늘고 있다. 한 증권사 연구원은 "카카오는 이미 국내에서 확장 가능한 영역을 상당 부분 선점했다"며 "톡비즈와 금융, 콘텐츠 이후 뚜렷한 신규 캐시카우가 보이지 않는 점이 한계로 지적된다"고 말했다. 또 다른 업계 관계자는 "카카오의 경쟁력은 여전히 카카오톡 트래픽에 있지만, 이 트래픽을 추가 수익으로 전환하는 속도는 예전보다 둔화된 측면이 있다"고 짚었다.

AI 역시 새로운 변수다. 카카오는 최근 AI를 차세대 성장 축으로 제시하며 서비스 고도화에 나서고 있지만, 시장에서는 수익화 가능성에 더 주목하는 분위기다. 업계 한 관계자는 "AI는 대부분 플랫폼 기업이 공통적으로 추진하는 영역"이라며 "카카오만의 차별화된 수익 모델로 이어질지가 관건"이라고 말했다.

카카오 측은 구조 개선을 통한 수익성 강화와 미래 투자 확대를 동시에 추진하겠다는 입장이다. 카카오 관계자는 "핵심 사업 중심으로 효율화를 진행하며 안정적인 수익 기반을 강화하고 있다"며 "AI를 포함한 미래 성장 동력 확보에도 속도를 낼 것"이라고 밝혔다.

/최빛나 기자 vitna@

SK AX, 에이전틱 AI 기반 기업운영 혁신

브랜드 '엑스젠틱와이어' 공개

SK AX는 에이전틱 AI 기반 통합 브랜드 '엑스젠틱와이어(AXgenticWire)'를 공개하고, 기업 운영 전반의 혁신 사업을 본격화한다고 19일 밝혔다.

'엑스젠틱와이어'는 스스로 판단하고 실행하는 에이전틱 AI와 기업 구조를 재설계하는 개념을 결합한 것으로, 다수의 AI 에이전트가 협업해 의사결정과 실행까지 수행하는 운영 체계를 지향한다.

최근 생성형 AI 확산으로 업무 단위 자동화는 빠르게 확산됐지만, 개별 시스템 중심의 도입으로 인해 기업 전체 생산성 향상으로 이어지지 않는 한계가 지적돼 왔다. 이에 따라 AI 간 협업을 조율하고 전사 운영을 통합 관리하는 구조의 필요성이 커지고 있다.

SK AX는 구조화된 'AI 리더블 데이터'를 기반으로 다양한 AI 에이전트가 협업하는 멀티 에이전트 환경을 제공할 계획이다. 이를 통해 추론, 의사결정, 실행까지 이어지는 전 과정을 자동화하고, 기업 운영의 효율성과 안정성을 동시에 확보한다는 구상이다.

또 IT 운영 자동화 기술을 결합해 기업별 시스템 환경에 맞는 안정적인 운영 체계를 구축하고, 데이터 보안과 거버넌스 관리 기능도 함께 지원할 예정이다.

해당 기술은 이미 제조 기업의 공급망 관리(SCM) 영역에 적용되고 있다. 기존에는 분산된 데이터를 사람이 취합해 생산 계획을 수립했다면, AI 기반 운영 체계에서는 데이터를 실시간으로 분석해 수요 예측과 재고 관리, 생산 계획 수립이 동시에 이뤄진다. 수요 변동이나 재고 부족 등 상황 발생 시에도 AI 에이전트가 협업해 대응 방안을 도출함으로써 의사결정 속도를 높일 수 있다는 설명이다.

업계에서는 에이전틱 AI 도입 여부에 따라 기업 간 생산성과 경쟁력 격차가 확대될 것으로 보고 있다. 기업 운영을 AI 중심으로 재구성한 경우 매출 성장과 비용 효율 측면에서 유의미한 개선이 나타날 수 있다는 분석도 나온다.

SK AX는 향후 산업별 적용 사례를 확대하고, 멀티 에이전트 기반 운영 체계를 고도화해 기업의 AI 전환을 지원해 나간다는 방침이다.

/김서현 기자

SKT-에릭슨
6G 대비 기술 공동연구

AI 기반 네트워크 기술협력 '맞손'

SK텔레콤은 에릭슨과 AI 기반 네트워크 기술 협력을 위한 업무협약(MoU)을 체결했다고 19일 밝혔다.

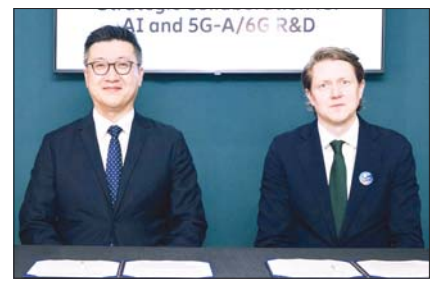
양사는 5G 고도화부터 6G까지 이어지는 차세대 통신 기술을 공동 연구하고, 표준화 기반 마련에 협력할 계획이다. 특히 AI를 활용한 네트워크 자동화와 성능 최적화 기술 개발에 초점을 맞춘다.

주요 협력 분야는 AI 기반 무선 접속망(AI-RAN), 개방·자율 네트워크, 보안, 6G 표준화 등이다. AI-RAN을 통해 네트워크가 트래픽과 환경을 학습해 자원을 효율적으로 배분하고, 운영 자동화를 통해 생산성과 안정성을 높인다는 구상이다.

보안 측면에서는 제로트러스트 기반 보호 체계와 실시간 위협 대응 기술을 강화하고, 멀티벤더 환경에서도 안정적인 네트워크 운영이 가능하도록 한다는 방침이다.

양사는 향후 주파수 전략, 초대형 다중 안테나, 통신·센싱 결합 기술 등 6G 핵심 기술 영역에서도 협력을 확대할 계획이다.

/김서현 기자



(왼쪽부터) 류탁기 SKT 네트워크기술담당과 마르텐 레너(Marten Lerner) 에릭슨 네트워크 전략 및 제품 총괄의 모습. /SKT

CJ올리브네트웍스
그룹 AX 전략 이끌 신입사원 공개 채용

내달 1일까지 12개 분야서 진행

CJ올리브네트웍스는 19일 CJ그룹의 인공지능 전환(AX) 전략을 이끌 신입사원 공개채용을 진행한다고 밝혔다. 지원서는 내달 1일까지 CJ그룹 채용 홈페이지를 통해 접수한다.

이번 채용은 AI, DX, 소프트웨어, ERP 시스템, 보안, 데이터, 인프라 서비스, 네트워크 서비스, UX·UI, 사업지원, 경영지원, 인사 등 총 12개 분야에서 진행한다.

DX 엔지니어는 그룹 주요 사업 영역의 시스템 구축과 플랫폼 개발을 맡고, ERP 엔지니어는 SAP 기반 업무 시스템 구축과 차세대 시스템 전환을 담당한다. 특히 CJ올리브네트웍스는 AI 분야 채용을 전략적으로 확대한다. AI 엔지니어는 딥러닝 기반 기술 개발과 함께 언어 AI, 피지컬 AI, 에이전트 기반 서비스 개발 등을 수행하며 다양한 산업의 AX를 지원한다.

채용 절차는 서류전형 이후 AI 역량검사, 직무 테스트 및 인성검사, 1차와 2차 면접 순으로 진행한다. 이후 2차 면접 합격자는 약 3주간 인턴십을 거쳐 최종 합격 여부를 결정한다. 지원자의 직무 이해도를 높이기 위한 온라인 채용설명회도 3월 24일과 27일 두 차례 진행한다.

/최빛나 기자