4 중국, 오픈클로 확산 속 정부 통제 본격화

에이전틱 AI 오픈클로의 등장과 중국 내 기업-정부 간 엇갈린 대응

○ 오픈클로, 중국이 세계 최대 이용국으로 부상

- 사용자 시스템에 직접 접근해 업무를 자율 수행하는 오픈소스 AI 에이전트 '오픈클로'의 중국 내 도입·활용이 급증하면서, 사용량 기준 미국을 넘어 세계 최대 이용국으로 부상
- 중국 내에서는 빅테크와 지방정부가 오픈클로 생태계 확산을 주도하는 한편, 중앙정부는 국가 데이터 보안 기조에 따라 공공부문 사용을 제한하는 등 확산과 통제가 동시에 진행

○ 에이전틱 AI 확산에 중국 정부, 공공부문 사용 제한으로 대응

- 에이전틱 AI는 이메일·캘린더·파일·인증 정보 등에 직접 접근·조작하는 구조로, 기술 확산 속도에 비해 보안·프라이버시 리스크 관리가 뒤따르지 못한다는 우려가 산업계·정부 양쪽에서 제기
- 중국 공업정보화부(MIIT)와 국가인터넷응급센터(CNCERT)가 두 차례에 걸쳐 보안 취약성을 경고, 2026년 3월에는 정부기관을 중심으로 업무용 기기에서 오픈클로 설치·사용을 금지하는 조치로 확대
- 이러한 긴장은 오픈클로 전에도 존재, 2025년 12월 바이트댄스의 Doubao AI 폰 출시 당시 위챗·알리페이 등 슈퍼앱이 접근을 차단한 바 있어 에이전틱 AI를 둘러싼 플랫폼 간 갈등이 이미 표면화

(현황① 오픈클로 확산) 중국 빅테크 경쟁과 지방정부 지원 속 생태계 확대

○ 중국 빅테크 주도 오픈클로 생태계 확장

- 오픈클로 마켓플레이스 상위 3개 모델이 모두 중국 기업이며, 상위 10개 모델 중 중국 모델이 토큰 소비량의 61%를 차지하여 구글 제미나이·앤트로픽 클로드 합산 사용량의 약 2배를 기록
- 텐센트·알리바바·바이트댄스는 자사 클라우드 서버에서 오픈클로를 즉시 실행할 수 있는 사전 구성 환경을 경쟁적으로 제공하며, 중국 내 기업·개발자 중심 활용 기반을 빠르게 구축
- 일례로 텐센트는 2026년 3월, 10억 이상 사용자를 보유한 위챗·QQ에 오픈클로를 통합하는 원클릭 설치 도구 QClaw를 출시, 텐센트 클라우드 기반 오픈클로 설치 사용자가 10만 명을 돌파

- 타오바오에서는 원격 설치 대행 서비스 거래가 확대되어 일부 판매자가 1,000건 이상의 주문을 처리하고, 샤오홍슈에서는 오픈클로 튜토리얼 콘텐츠가 확산되는 등 일반 사용자층으로도 관심 확대

○ 지방정부, 오픈클로 기반 산업 생태계 조성에 대규모 재정·인프라 지원 착수

- 선전 룽강구는 2026년 3월 오픈클로 중심 AI 생태계 조성과 1인 기업 육성을 위한 초안 정책을 발표, 최대 1,000만 위안(약 22억 원)의 보조금과 무료 컴퓨팅 자원·사무공간을 지원
- 우시는 오픈클로 기반 제조업 응용 프로젝트에 최대 500만 위안(약 11억 원) 지분 투자를 제안하는 등 지방정부 간 오픈클로 생태계 유치 양상 본격화
- 지방정부의 대규모 재정·인프라 지원은 오픈클로를 활용한 업무 자동화 기반의 1인 기업 육성과 지역 산업 생태계 조성을 목표로, 중앙정부의 보안 우려와는 상반된 정책 기조를 형성

(현황② 보안 리스크 대응) 에이전틱 AI 보안 위험과 중국 정부의 통제 대응

○ 에이전틱 AI의 구조적 보안 취약점

- 오픈클로는 악성 웹페이지를 방문하는 것만으로 관리 권한이 하이재킹될 수 있는 구조적 결함이 있으며, 공격자가 사용자 확인 절차를 우회해 PC에서 임의 명령을 실행할 수 있는 것으로 확인
- 기본 설치 상태에서 비밀번호가 설정되지 않고 입력 시도 횟수 제한도 없어 외부 접근 및 무차별 대입 공격에 노출되는 등 설계 단계의 기본 보안 요건을 충족하지 못한 것으로 지적
- AI 에이전트가 외부 웹페이지·문서 등 비신뢰 콘텐츠도 자동으로 처리하는 구조로 인해 악성 지시문에 의해 모델 행동이 조작되는 프롬프트 인젝션 공격에도 취약
- 오픈클로 공식 플러그인 마켓 ClawHub에서는 비밀번호·금융정보·암호화폐 지갑 등을 탈취하는 악성 플러그인이 1,184개 이상 발견되는 등 빠른 확산에 비해 보안 관리 체계가 미흡한 상황

○ 중앙정부, 국유기업·공공기관 대상 오픈클로 사용 제한 조치 본격화

- 이러한 취약점과 함께, 자율적 데이터 처리로 인한 기존 프라이버시 보호 체계 실효성 약화 우려와 분산된 개인정보의 단일 시스템 집중 구조 등이 정부 차원의 규제 논의 배경으로 작용

- MIIT·CNCERT는 2~3월 두 차례에 걸쳐 오픈클로 관련 보안 경고 발령, 주요 클라우드 기업의 간편 배포 확산 속에서 부적절한 설치·운용이 심각한 보안 위험을 초래할 수 있다고 공식 지적
- CNCERT는 2차 경고에서 프롬프트 인젝션 및 운영 오류로 인한 이메일·파일 등 중요 데이터 삭제 가능성, 시스템 키 유출 위험 등 에이전틱 AI 고유의 보안 위협 유형을 구체적으로 제시
- 3월 MIIT는 국유기업 및 정부기관에 업무용 기기에서 오픈클로 설치를 금지하는 보안 지침을 전달했으며, 일부 기관은 이미 설치한 직원에게 상급자 보고와 보안 점검·삭제 조치를 지시

출처 : Bloomberg 외(2026.3.)

https://www.bloomberg.com/news/articles/2026-03-11/china-moves-to-limit-use-of-openclaw-ai-at-banks-government-agencies
https://www.yahoo.com/news/articles/chinas-shenzhen-backs-openclaw-ai-122205994.html
https://theedgemalaysia.com/node/795664
https://www.lawfaremedia.org/article/china-s-agentic-ai-controversy
https://beam.ai/agentic-insights/tencent-launches-qclaw-what-the-ai-agent-mainstream-moment-means-for-enterprise
https://www.businessinsider.com/openclaw-moltbot-china-internet-alibaba-bytedance-tencent-rednote-ai-agent-2026-2
https://www.giskard.ai/knowledge/openclaw-security-vulnerabilities-include-data-leakage-and-prompt-injection-risks
https://www.adminbyrequest.com/en/blogs/openclaw-went-from-viral-ai-agent-to-security-crisis-in-just-three-weeks
https://www.koreatimes.co.kr/business/tech-science/20260208/top-tech-firms-ban-openclaw-over-security-breach-fears