

2026. 7. 13 (월)

미중 AI 디커플링: 칩에서 코드로

- 알리바바, 7/10일부터 클로드 전면 사용금지, 미중 AI 디커플링은 칩에서 코드로
- 알리바바에 미칠 영향: 외부 AI 도구 사용료 절감, 자체 AI 생태계 풀스택으로의 전환
- 이번 사태는 궁극적으로 미중 AI 생태계 분리의 한 과정 → 중국산 AI 생태계 밸류체인 투자에 기회

글로벌 투자전략-신흥국
Analyst 최설화
xuehua.cui@meritz.co.kr

알리바바의 Claude 전면 사용금지

이번 사태는 미국 AI 기업인 엔트로픽과 중국 알리바바 사이의 갈등에서 시작됐다. 엔트로픽은 지난 2월부터 알리바바를 포함한 중국 AI 기업들이 자사 AI 모델 클로드의 답변을 대량으로 수집해, 훨씬 적은 비용으로 자체 AI 모델을 개발하는데 활용하고 있다고 주장해왔다. 이런 방식을 업계에서는 증류(Distillation)라고 부른다. 원본 모델의 코드나 가중치를 직접 복사하는 것이 아니라, 원본 모델이 만들어낸 대량의 답변을 학습 재료로 삼아 비슷한 성능의 모델을 값싸게 만들어 내는 기법이다.

엔트로픽은 6월 10일 미국 상원위원회에 보낸 서한에서 이 주장을 구체화했다. 알리바바가 4월 22일부터 6월 5일 사이 약 25,000개의 허위 계정을 이용해 클로드와 2,880만 회 이상 대화를 주고받았는데, 이는 자사 AI 기술을 대규모로 무단 추출하는 행위라는 것이다.

한편 엔트로픽은 이미 3월부터 이런 우회 접근을 걸러내기 위한 감지 기능을 자사 코딩 도구 'Claude Code'에 몰래 심어두고 있었다. 사용자의 접속 시간대, 프록시 경로, 중국 AI 연구소와의 연관성 등을 수집해 중국에서 접속하는 사용자를 식별했다. 이 기능은 4월 2일 배포된 버전(2.1.91)부터 6월 29일 배포된 버전(2.1.196)까지 포함되어 있었다. 이 사실이 6월 말 개발자 커뮤니티(레딧, 깃허브)를 통해 외부에 알려졌다. 개발자들은 이를 몰래 심어둔 추적 장치라고 비판했고, 엔트로픽은 “무단 재판매업자의 계정 남용과 증류를 막기 위한 실험이었으며, 이미 더 강한 대체 조치를 적용했고 다음 업데이트에서 완전히 제거하겠다”라고 해명했다. 즉 엔트로픽은 이 기능이 백도어라는 표현에는 동의하지 않고 있다.

이런 논란이 확산된 직후인 7월 3일 알리바바는 내부 소식통을 인용해 “클로드 코드를 고위험 소프트웨어로 지정하고, 7월 10일부터 사내에서 클로드 코드와 클로드의 모든 모델(Sonnet, Opus, Fable)의 사용을 전면 금지하며, 대체 도구로 자체 개발한 큐오더(Qorder)를 사용하도록 지시했다”라고 보도했다.

이어 7월 8일, 중국 공업정보화부 산하 국가취약점데이터베이스(NVDB)가 공식 성명을 내고 “클로드 코드 일부 버전에 사용자 동의 없이 위치, 신원 정보를 외부 서버로 전송할 수 있는 기능이 있으며, 이는 심각한 보안 위험을 초래한다”라고 발표하며 삭제 또는 업데이트를 권고했다.

알리바바의 Claude 전면 사용금지

단기적으로는 분명한 비용이 발생한다. 개발자 설문조사에 따르면 클로드 코드는 전 세계 개발자의 46%가 사용하는 사실상의 업계 표준 도구였고, 알리바바 개발자들도 회사 지원으로 상당한 비용을 들여 이를 활용해왔다. 복잡한 코드 수정이나 여러 파일에 걸친 작업에서 클로드 코드의 성능은 높은 평가를 받아왔기 때문에, 이를 자체 도구인 '큐오더'로 전면 교체하는 과정에서 한동안 개발 속도가 다소 떨어지는 것은 불가피할 것으로 보인다.

다만 이를 알리바바의 AI 경쟁력 자체에 대한 근본적 타격으로 해석하는 것은 성급하다. 몇 가지 이유가 있다.

첫째, 이번 조치로 막힌 것은 '외부 도구를 활용한 일상적인 코딩 보조 업무'이지, 알리바바가 자체 개발 중인 대형 언어모델(큐원 시리즈)의 핵심 연구개발 일정이 아니다. 애초에 엔트로픽은 지난해부터 중국 기업과 그 해외 법인에 대한 클로드의 정식 상업적 이용 자체를 금지해온 상태였고, 지금까지 이루어진 접근은 해외 법인 명이나 우회 경로를 통한 것이었다. 즉 알리바바 입장에서는 원래부터 공식적으로 보장된 권리를 잃은 것이 아니라, 회색지대에 있던 사용 방식이 이번에 정리된 것에 가깝다.

둘째, 이미 독자적인 AI 모델을 보유한 기업들은 외부 도구 없이도 자체적인 방식으로 코딩 도구를 고도화할 수 있다. AI가 스스로 문제를 만들고 다른 AI가 이를 검증하는 학습 방식(자가 피드백 루프)이 이미 여러 중국 기업에서 자리 잡고 있어, 외부 모델 의존을 끊는 것이 장기적으로 치명적이라 보기는 어렵다.

셋째, 이번 조치는 알리바바에 두 가지 실질적 이익을 준다. 하나는 그동안 지원해온 외부 AI 도구 사용료를 절감할 수 있다는 점이고, 다른 하나는 자사 엔지니어 조직을 자체 AI 생태계 안으로 완전히 편입시킬 수 있다는 점이다. 또한 미국 정부의 대중국 AI 규제가 강화되는 흐름 속에서, 알리바바가 먼저 미국 도구 사용을 중단했다는 점은 향후 미국 의회나 정부발 제재 가능성에 대한 선제적 방어도 작용할 수 있다.

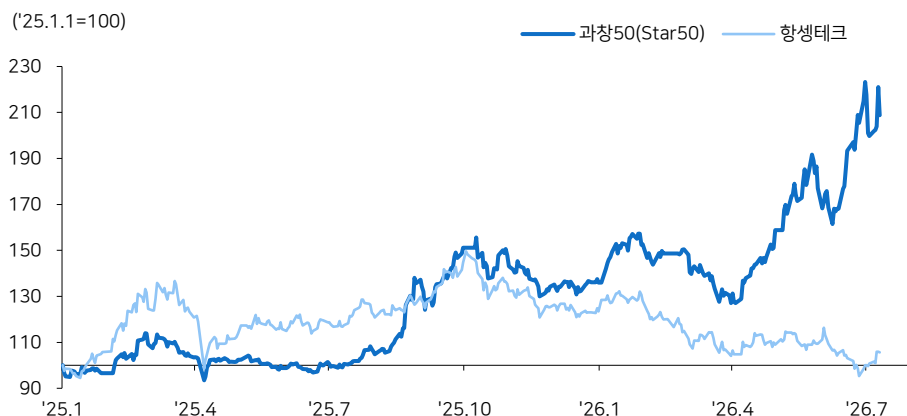
투자 관점에서의 시사점: 평가 기준의 전환, 국산 AI 생태계 가속화

이번 사태에서 투자자가 주목해야 할 핵심은 알리바바와 엔트로픽 중 누가 옳은가가 아니라, 중국 AI 기업을 평가하는 기준 자체가 바뀌고 있다는 점이다.

지금까지 시장은 중국 AI 모델을 평가할 때 ‘미국 모델과 비교해 벤치마크 점수가 얼마나 따라왔는가’를 주된 기준으로 삼아왔다. 그러나 미국의 대중국 기술 통제(수출 규제, 접근 차단, 기능 추적 논란 등)와 중국의 대응이 반복되는 지금 국면에서는 미국의 부품과 소프트웨어 없이 자체 기술만으로 얼마나 효율적인 AI 서비스를 만들어 낼 수 있는가가 더 중요한 평가 기준으로 떠오르고 있다. 특히 물류, 제조, 전자상거래 등 방대한 산업 데이터와 알리바바·텐센트가 보유한 폭넓은 서비스 생태계가 결합될 경우, 기초 모델 성능에서는 다소 뒤처지더라도 실제 업무에 AI를 적용하는 능력에서는 중국이 앞설 가능성도 배제할 수 없다.

이런 맥락에서 이번 사태는 하나의 우발적 사건이라기보다, 미국의 기술 통제와 중국의 기술적 대응이 맞물려 양국의 AI 생태계가 점차 분리되는 더 큰 흐름의 한 장면으로 보는 것이 타당하다. 따라서 방향성은 비교적 분명하다. 소프트웨어의 자립이 진행될수록, 그 아래 하드웨어에서의 반도체 및 장비와 소재의 국산화 압력도 함께 커질 수밖에 없다. 중장기적인 관점에서 중국의 AI 생태계에 포함된 LLM 모델, AI 칩, 반도체 장비 및 소재 등 전반 밸류체인에 대한 투자에 계속 관심을 가져야 하는 이유이다.

그림1 과창50 지수와 항생테크 지수 추이



자료: Bloomberg, 메리츠증권 리서치센터

Compliance Notice

- 본 조사분석자료는 제3자에게 사전 제공된 사실이 없습니다.
- 당사는 자료작성일 현재 본 조사분석자료에 언급된 종목의 지분을 1% 이상 보유하고 있지 않습니다.
- 본 자료를 작성한 애널리스트는 자료작성일 현재 추천 종목과 재산적 이해관계가 없습니다.
- 본 자료에 게재된 내용은 본인의 의견을 정확하게 반영하고 있으며, 외부의 부당한 압력이나 간섭 없이 신의 성실하게 작성되었음을 확인합니다.

본 자료는 투자자들의 투자판단에 참고가 되는 정보제공을 목적으로 배포되는 자료입니다. 본 자료에 수록된 내용은 당사 리서치센터의 추정치로서 오차가 발생할 수 있으며 정확성이나 완벽성은 보장하지 않습니다. 본 자료를 이용하시는 분은 본 자료와 관련한 투자의 최종 결정은 자신의 판단으로 하시기 바랍니다. 따라서 어떠한 경우에도 본 자료는 투자 결과와 관련한 법적 책임소재의 증빙자료로 사용될 수 없습니다. 본 조사분석자료는 당사 고객에 한하여 배포되는 자료로 당사의 허락 없이 복사, 대여, 배포 될 수 없습니다.
