4 중국, 첨단 AI 모델 해외 접근 제한 검토 착수

오픈웨이트 확산 전략 뒤집는 中, 해외 접근 제한 전격 검토

○ 中 상무부·NDRC, 6월 알리바바 등과 회의 열고 논의 착수

- 중국 상무부와 국가발전개혁위(NDRC)가 지난 6월 한달간 알리바바·바이트댄스·지푸AI 등 주요 AI 기업과 회의를 열고, 자국 첨단 AI 모델의 해외 접근을 제한하는 방안을 논의
- 규제 대상에는 외부 공개를 처음부터 막는 폐쇄형 모델뿐 아니라 누구나 내려받아 쓸 수 있는 오픈웨이트 모델까지 포함, 이미 공개된 모델이 아닌 미출시 차세대 모델에 우선 적용될 가능성
- 무료 개방을 앞세워 세계 시장을 파고들던 중국이 스스로 빗장을 걸려는 움직임으로, AI를 반도체에 준하는 국가 전략 자산으로 관리하려는 방향 전환의 신호로 해석

○ 딥시크 R1이 불붙인 中 AI의 세계 확산, 이제는 통제 대상으로 부상

- 지난해 딥시크의 R1 모델이 저비용·고성능을 앞세워 세계 시장에서 주목받은 이후, 큐원·더우바오·GLM-5.2 등 중국 AI 모델의 해외 영향력이 빠르게 확대
- 특히 지푸AI의 GLM-5.2는 美 선도 모델에 근접한 성능을 낮은 비용으로 구현해 실리콘밸리서도 주목, 일부 美 기업은 비싼 자국 모델 대신 중국 모델을 채택해 비용을 절감
- 중국 AI가 美 최고 모델에 평균 7개월 뒤진 후발주자임에도 개방으로 세계에 침투한 성과가 클수록, 이를 지키려는 통제 요구도 함께 커지는 '성장의 역설'이 이번 논의의 배경

○ 美의 접근 제한 직후 나온, 中 보호 조치의 정점

- 이번 검토는 美 정부가 앤트로픽의 최상위 모델 접근을 국가안보를 이유로 막은 직후 나온 대응이자, 올해 中이 이어온 자국 AI 보호 조치의 연장선에서 나온 흐름으로 파악
- 美는 6월 외국인의 미소스·페이블 접근을 금지해 앤트로픽이 전 세계 서비스를 일시 중단했고, 中은 4월 메타의 마누스 인수 철회 요구, 6월 해외 거래 심사 강화 등으로 유출 차단에 집중
- 첨단 AI를 안보 자산으로 다루는 규범이 미·중 양쪽에서 동시에 굳어지는 국면으로, 개별 조치가 '해외 유출 차단'으로 수렴하며 이번 논의가 그 흐름의 정점에 해당한다는 평가

해외 접근 제한을 둘러싼 3대 쟁점

(1) 국가안보와 글로벌 시장 접근성의 정면 충돌

- 무료 개방, 中 AI를 세계로 밀어 올린 핵심 지렛대
  - 중국이 자국 AI 모델을 대부분 무료로 개방해 온 것은 후발주자가 짧은 시간에 세계 시장을 파고들 수 있게 한 가장 강력한 성장 지렛대로 작동
  - 무료·저비용을 앞세운 덕에 일부 美 기업까지 중국 모델을 실제 업무 환경에 도입, 美 최고 모델과의 성능 격차를 가격 경쟁력으로 상쇄
  - 따라서 해외 접근을 막는 것은 세계 확산의 원동력을 스스로 내려놓는 선택으로, 시장 기회를 포기해야 하는 큰 기회비용을 감수해야 한다는 점이 이번 검토의 근본적인 딜레마
- 강점을 스스로 포기하려는 결정, 안보 우려가 이익을 넘어섰다는 신호
  - 후발주자가 자신의 최대 무기를 스스로 내려놓으려는 것은 매우 이례적인 일로, 시장 이익보다 국가안보 우려가 더 크다는 판단이 그 배경에 깔려 있다는 해석
  - 카네기국제평화재단의 스콧 싱어 연구원은 中도 백악관과 같은 고민, 즉 글로벌 시장 접근의 편익과 안보를 위한 통제 사이에서 균형을 찾아야 하는 처지에 놓였다고 진단
  - 시장 이익보다 안보 논리를 앞세우는 판단이 미·중 양쪽에서 나타나는 것으로, 첨단 AI 통제의 명분이 후발국에서도 자리 잡는 전환점에 이르렀다는 의미

(2) 오픈웨이트라는 배포 방식 자체의 구조적 한계

- 오픈웨이트 회수 불가 문제, 이번 규제 논의의 근본적 한계로 지적
  - 오픈웨이트 모델은 핵심 설정값인 가중치를 인터넷에 공개하는 방식이어서, 한 번 배포되면 개발사조차 이를 회수하거나 삭제할 수 없다는 근본적 특성 보유
  - 이용자가 시스템을 통째로 내려받아 자체 실행하므로, 폐쇄형과 달리 공개 후에는 위험 기능을 막는 안전장치를 사후에 덧붙이는 것도 불가능해 별도의 보안 과제가 발생
  - 이 때문에 규제를 새로 도입하더라도 이미 풀린 모델에는 효력이 없고 앞으로 나올 미래 모델에만 적용 가능, 통제에 태생적 한계가 존재한다는 점이 이번 쟁점의 핵심
- 사후 규제 무력화, 中의 사전 차단 정책 설계 유인으로 작용
  - 공개 이후 통제가 불가능한 구조이기 때문에, 규제의 초점은 모델을 세상에 내놓기 전 단계의 사전 심사에 맞춰질 수밖에 없는 상황

- 5월 최고인민법원 회의에서는 기본 오픈소스는 신고만, 고성능 모델은 보안 심사, 가장 민감한 프론티어 모델은 공개 금지·국내 한정으로 나누는 단계별 관리안이 제시
- 여기에 기술 유출·도용을 국가안보법 위반으로 처벌하는 방안까지 더해지며, 공개 전 심사와 유출 후 처벌을 아우르는 이중 통제망 구축으로 이어질 전망

(3) 증류 기술을 둘러싼 미중 기술 유출 공방 심화

● '증류'를 둘러싼 앤트로픽-알리바바 충돌 및 유출의 안보 위협화

- 성능이 앞선 AI의 답을 베껴 뒤처진 모델을 끌어올리는 '증류' 문제가 中의 추격 수단으로 지목되며 미·중 AI 갈등의 새 뇌관으로 부상
- 앤트로픽은 2월 보고서에서 딥시크·문샷·미니맥스 등 중국 AI 기업들이 약 2만 4천개 부정 계정으로 클로드와 1,600만 건 대화를 주고받으며 증류를 시도했다고 주장, 6월엔 알리바바를 직접 지목
- 앤트로픽이 클로드 코드에 中 이용자 여부를 판별하는 코드를 넣은 사실이 드러나자, 알리바바는 클로드 코드의 사내 사용을 금지하고 직원 PC에서 삭제하도록 요청하며 맞불

● 유출을 '안보 위협'으로 보는 시각, 미·중 양쪽서 확산

- 앤트로픽은 증류를 기업 간 도용 다툼을 넘어선 국가안보 위협으로 규정하며, 미·중 AI 경쟁을 안보 문제의 틀로 끌어올리는 프레임을 앞세우는 상황으로 파악
- 해외 연구소가 빼낸 능력을 군사·감시 시스템에 흘리거나 권위주의 정부가 공격적 사이버· 감시에 악용할 수 있다는 경고이자, 오픈소스 공개 시 사업 모델이 잠식된다는 상업적 우려도 병존
- 반대로 중국은 美 앤트로픽의 미소스가 자국 소프트웨어 취약점을 공격할 수 있다고 우려, 中 360의 저우훙이가 이를 '사이버 무기'로 부르며 양방향 불신이 서로의 통제로 번지는 구조로 귀결

출처 : TIME 외(2026.7.)
https://time.com/article/2026/07/07/china-ai-models-alibaba-bytedance/
https://www.reuters.com/world/beijing-is-looking-curbing-overseas-access-chinas-top-ai-models-sources-say-2026-07-07/
https://www.aitimes.com/news/articleView.html?idxno=212524
https://www.joongang.co.kr/article/25443378