



미-중 간 AI 모델의 수출 통제와 국내 시사점¹⁾

1 미국의 AI 모델 수출 통제²⁾

가. 수출 통제의 배경과 경과

→ '26년 6월 9일 미국의 앤트로픽(Anthropic)은 동일한 기반 모델을 공유하면서, 고위험 영역의 처리 제한 여부가 다른 두 개의 고성능 AI 모델을 출시

- '미토스5(Mythos5)'는 추론 성능이 뛰어날 뿐만 아니라 소프트웨어 취약점 탐지와 같은 사이버보안 영역에서도 탁월한 역량을 가진 모델로, 지난 4월에 제한적으로 사전 공개되었던 '미토스 프리뷰(Mythos Preview)'의 정식 버전
 - 이 모델을 일반 대중에게 공개할 경우 해킹 등에 악용될 우려가 있어, 앤트로픽은 미토스 프리뷰 때부터 신뢰할 수 있는 기업 및 기관을 선정해 '프로젝트 글래스윙(Project Glasswing)'이라는 연합을 구성하고 이들에게만 접근권을 부여
- '페이블5(Fable5)'는 미토스5에 안전장치를 걸어 고위험 영역의 처리를 제한한 일반 공개용 모델
 - 앤트로픽의 클로드(Claude) 이용자는 페이블5를 선택해 미토스5와 동일한 고성능 추론 기능을 이용할 수 있지만, 처리가 제한되는 요청이 감지되면 '오퍼스(Opus)' 등 성능이 낮은 모델로 전환되어 처리

→ 출시 3일 뒤인 '26년 6월 12일 미국 상무부 장관은 앤트로픽에 국가 안보를 이유로 미토스5와 페이블5의 해외수출 및 미국 내 외국인의 접속을 금지하는 비공개 서한을 발송

- 수출 통제의 직접적인 원인은 페이블5의 안전장치에 대한 탈옥(jailbreaking)* 우려
 - * 탈옥은 AI 모델에 내재된 안전장치를 우회하여, 원래는 차단되어야 할 위험한 정보나 기능을 모델로부터 끌어내는 행위를 의미
- 세계적으로 공개된 페이블5에 대한 탈옥이 이루어질 경우, 미토스5 수준의 사이버 공격과 생화학무기 제조 능력 등이 해커와 적대국의 손에 들어가 여러 국가의 안보를 위협할 수 있다는 판단이 작용

1) 국회입법조사처 과학방송통신과 정준화 입법조사관(joonhwa@assembly.go.kr),
본고는 저자의 개인적인 견해이며 과학기술정보통신부와 KISTEP의 공식적인 의견이 아닙니다.

2) 정준화, 「미국 정부의 미토스(Mythos) 수출 통제가 남긴 것 - 고성능 AI 모델 전략자산화와 한국 소버린 AI의 과제」, 『이슈와 논점』 제2510호, 국회입법조사처, 2026.7.14.

- AI 모델이 널리 배포된 뒤에는 이러한 위험을 사후적으로 통제하기 어렵기 때문에, 미국은 AI 모델이 외국으로 더 전파되기 전에 신속히 차단하는 방식을 선택
- ⇒ 직접적으로 언급되지는 않았지만, 폐쇄형 보안 컨소시엄인 프로젝트 글래스wing의 구성원이 확대되어 미토스5를 이용하는 외국의 기업·기관이 늘어난 것도 미국 정부의 안보 우려를 키운 요인으로 지목³⁾
- 앤트로픽이 지난 4월 선정한 프로젝트 글래스wing 파트너는 약 50개 규모로, 미토스 프리뷰 접근권을 통해 선제적으로 보안 취약점을 찾고 대응 방안을 마련하도록 했음
- 이후 외국 기업·기관의 추가 가입 요청이 늘어나자 앤트로픽은 파트너를 약 150개 추가하고 그 목록을 미국 정부에 제출
- 이는 자사 서비스에 대한 접근 대상을 넓히려는 사업자와 국가 안보를 이유로 공개 범위를 제한하려는 정부 사이에 긴장 관계를 형성했고, 여기에 페이블5의 탈옥 우려가 제기되면서 수출 통제로 이어진 것으로 평가
- ⇒ 상무부는 미토스5와 페이블5의 해외 수출 및 미국 내 외국인의 접속을 금지하였으나, 앤트로픽은 두 AI 모델에 대한 전 세계 모든 접속을 전면 차단하는 조치를 단행
- 앤트로픽은 미국 내 AI 이용자의 국적을 실시간으로 파악해 외국인만 접속을 차단하는 것이 현실적으로 불가능에 가깝다고 판단하여, 두 모델에 대한 전 세계 모든 이용자의 접속을 전면 중단
- 다만 앤트로픽은 상무부가 제시한 수출 통제 근거*가 페이블5만 해당되지는 않는다고 반박⁴⁾
 - * AI 모델의 안전장치를 광범위하게 무력화시켜 고위험 영역 처리를 활성화하는 '범용 탈옥'이 아니라 특정 상황에서만 작동하는 좁은 방식인 점, 문제가 된 탈옥 방법이 오픈AI의 공개 AI 모델에서도 통용된다는 점 등
- ⇒ 수출 통제는 '26년 6월 30일 상무부의 해제 서한으로 18일 만에 종료되었고, 앤트로픽은 7월 1일부터 모델별로 접근 권한을 복원
- 페이블5는 7월 1일부터 전 세계 서비스가 재개되었고, 미토스5는 6월 26일 미국 정부가 승인한 자국 기업·기관 100여 곳부터 접근이 먼저 복원된 뒤 미국 내 파트너를 중심으로 순차 확대되었음

3) Sebastian Herrera and Beatrice Nolan, 「The week that changed AI: Inside Trump's Anthropic crackdown, and how a phone call from Amazon CEO Andy Jassy triggered the chaos」, 『Fortune』, 2026.6.18.

4) Antropic, "Statement on the US government directive to suspend access to Fable 5 and Mythos 5", 2026.6.12., (<https://www.anthropic.com/news/fable-mythos-access>), (검색일: 2026.9.7.).

- 해제 서한에서 상무부는 엔트로픽과의 전제조건* 합의 하에 두 모델의 수출과 외국인 접촉에 별도의 허가가 더 이상 필요하지 않다고 밝힘

* ①보안 위험의 선제적 탐지, ②향후 모델 출시 기준·절차의 정부 협의, ③악의적 활동의 정부 보고

나. 수출 통제와 출시 전 개입의 병행

⇒ 미국 정부는 「수출관리규정(EAR^{*})」과 「수출통제개혁법(ECRA^{**})」을 통해 전략자산 수출을 통제해 왔으며, 이번 미토스 수출 통제에도 해당 조항들이 직·간접적으로 활용

* Export Administration Regulations / ** Export Control Reform Act of 2018

- 일반적으로 수출 통제는 상무부 산하 산업안보국이 EAR에 따라 작성된 상무통제 목록(Commerce Control List, CCL)에 등재된 품목을 대상으로 하는데, 현재 AI 모델은 CCL에 등재되어 있지 않아 직접적 근거로 보기는 어려움

- 산업안보국은 2025년 1월 「인공지능 확산 프레임워크^{*}」를 통해 고성능 폐쇄형 모델의 가중치를 새로운 품목번호(ECCN 4E091)로 통제하고자 했음⁵⁾

* Framework for Artificial Intelligence Diffusion

- 다만 가중치가 이미 공개된 오픈웨이트 모델은 통제 대상에서 제외되었고, 동 프레임워크도 '25년 5월 철회 절차가 개시되면서 집행이 중단

- 한편, ECRA는 '이중용도(dual-use)^{*}' 물품 및 서비스에 대한 수출 규제 권한을 대통령에게 부여한 법으로, 상무부는 이를 반도체·장비 등의 대중국 수출 제한에 대한 비공개 서한을 발행하는 방식으로 활용해 왔음

* 전통적인 무기류는 아니지만 군사·민간 양면으로 활용되어 외국의 군사적 잠재력에 중대하게 기여할 수 있는 물품 또는 서비스

- 이번 수출 통제 조치가 공표된 규칙이 아니라 개별 기업에 대한 비공개 서한의 형식을 취한 것도 이러한 배경에서 이해할 수 있으며, 이는 통제의 대상과 시점을 사전에 예측하기 어렵게 만드는 요인이 됨

⇒ 미국 정부는 한발 더 나아가, 고성능 AI 모델이 출시되기 전에 사전 점검을 받도록 하는 제도를 마련

- 미국 상무부 산하 인공지능 표준·혁신센터(CAISI)는 이미 오픈AI·엔트로픽과 AI 모델의 사전 시험을 해왔고, 최근 구글·마이크로소프트 등과도 사전 평가와 공동 연구 수행에 대한 협약을 체결했음

5) Bureau of Industry and Security, 「Framework for Artificial Intelligence Diffusion」, 90 FR 4544, 2025.1.15., (<https://www.govinfo.gov/app/details/FR-2025-01-15/2025-00636>), (검색일: 2026.9.7.).

- 이 방식은 트럼프 대통령이 서명한 「첨단 인공지능 혁신 및 안보 증진」에 관한 행정명령*으로 제도적 틀을 갖추었음⁶⁾

* E.O.14409, Promoting Advanced Artificial Intelligence Innovation and Security, 2026.06.02.

- 동 행정명령의 핵심은 AI 기업이 미국의 안보에 영향을 미칠 우려가 있는 고성능 모델을 출시하기 전, 최대 30일간 미국 정부에 접근권을 제공해 보안 취약점을 사전 검토받도록 하는 자발적 체계를 마련한 것임

〈 미국 행정명령 제14409호의 고성능 모델 출시 전 사전 검토 조항 〉

제3조 안전한 프런티어 모델 확보

이 명령일로부터 60일 이내에, 재무부 장관, 국가안보국 국장을 통한 전쟁부 장관, 사이버보안 및 사회기반시설 보안국 국장을 통한 국토안보부 장관은 국가사이버국 국장을 통한 백악관 비서실장, 대통령 과학기술보좌관 (APST), 국립표준기술연구소(NIST) 소장을 통한 상무부 장관과 협의하고, 적절한 경우 타 기관과 협조하여 다음 사항을 이행해야 한다.

- (b) AI 개발자와 함께 개발자가 다음을 수행할 수 있도록 하는 자발적 프레임워크를 설계한다.
 - (ii) 해당 모델을 다른 신뢰할 수 있는 파트너에게 공개하기 전 최대 30일 동안, 적절한 기밀유지, 사이버보안 조치, 내부자 위험 관리 및 지식재산권 보호와 그 사용 및 비밀유지에 관한 요구사항을 준수하는 조건으로 연방 정부에 해당 프런티어 모델에 대한 접근권을 제공하는 것

Sec. 3. Secure Frontier Model Deployment.

Within 60 days of the date of this order, the Secretary of the Treasury, the Secretary of War, through the Director of NSA, and the Secretary of Homeland Security, through the Director of CISA, in consultation with the White House Chief of Staff, through the National Cyber Director, the Assistant to the President for Science and Technology (APST), and the Secretary of Commerce, through the Director of the National Institute of Standards and Technology, and in coordination with other agencies, as appropriate, shall:

- (b) design a voluntary framework with AI developers through which developers would be able to:
 - (ii) provide the Federal Government with access to covered frontier models, subject to appropriate confidentiality, cybersecurity, insider-risk, and intellectual-property protection, use, and nondisclosure requirements, for a period of up to 30 days before they plan to release such models to other trusted partners;

출처 : 국회도서관 입법자료포털, 외국법률번역DB, “첨단 인공지능 혁신 및 안보 증진에 관한 행정명령 제14409호”, (<https://law.nanet.go.kr/foreignlaw/foreignIndex/foreignIndexView.do?countPerPage=10&cn=TLAW1202600436>), (검색일: 2026.9.7.).

다. 소결: AI 모델의 전략자산화와 미국의 이중 우위

⇒ 이번 사태는 그동안 유형의 제품을 대상으로 이루어져 온 수출 통제가 고성능 AI 모델이라는 무형의 서비스로 확장되었음을 시사

- 최고 성능의 AI 모델은 일반에 바로 공개되지 않고 정부가 검증한 일부 기관에 우선 배포되는 양상이 자리 잡았으며, 초기 접근권은 더 이상 기업의 상업적 판단이나 시장 수요만으로 결정되지 않고 정부 승인이라는 새로운 층위가 얹어졌음

6) The White House, 「Promoting Advanced Artificial Intelligence Innovation and Security」, 2026.6.2., (<https://www.whitehouse.gov/presidential-actions/2026/06/promoting-advanced-artificial-intelligence-innovation-and-security/>), (검색일: 2026.9.7.).



- 미국 정부는 도입 주체의 신뢰도와 국적은 물론, 외국 주체일 경우 해당국이 미국의 신뢰를 받고 있는지와 미국 안보에 미칠 파급효과를 고려할 예정
- 따라서, 첨단 AI 모델의 초기 배포는 기업 간 비즈니스 검토를 넘어 국가 간의 정치·외교적 사안으로 확장됨
- ⇒ 미국 정부는 자국 기업이 보유한 기술 우위에 더해 그 기술을 먼저 들여다볼 수 있는 정책적·규제적 우위를 함께 갖게 되었지만, 수입국은 지금까지 경험하지 못한 새로운 차원의 공급망 불안정에 직면
- AI 모델이 시장에 공개되기 전 그 능력과 취약점을 가장 먼저 확인하는 주체가 미국 정부가 되면서, 신규 모델의 위험을 미리 파악해 대응 전략을 수립하는 보안 기술·정책의 우위를 확보함
 - 기업 입장에서는 출시 일정과 공개 범위가 정부 협회에 좌우되므로 정부와 협력할 수밖에 없는 관계가 됐으며, 미토스 사태의 해제 조건이 향후 출시 기준·절차의 협의와 악의적 활동의 보고였다는 점이 이를 단적으로 보여줌
- 반면 고성능 AI 모델은 소수 기업이 공급을 사실상 독점하고 있어, 수출국 정부의 통제로 특정 모델의 글로벌 공급이 중단될 경우 이를 즉각 대체할 모델을 찾기 어려워짐
 - 외산 AI 모델이 광범위하게 사용되고 있는 상황에서 서비스가 돌연 중단되면, 그 충격은 개별 기업이나 특정 산업에 그치지 않고 경제 전반은 물론 사회와 국방 영역에까지 동시에 파급되어 국가의 핵심 기능을 마비시킬 수도 있음

2 중국의 오픈웨이트 전략과 선별적 통제의 병행

가. 오픈웨이트 전략의 배경과 성과

- ⇒ 미국의 프론티어 AI 기업들이 모델을 API로만 제공하는 폐쇄형(closed-weight) 방식으로 운용하는 반면, 중국은 모델의 가중치를 공개하는 오픈웨이트(open-weight)* 방식을 활용

* 오픈웨이트는 학습된 파라미터 값(가중치)을 공개하는 방식으로, 소스코드와 학습 데이터·학습 과정까지 공개하는 오픈소스와는 구분됨

- 엔트로픽·오픈AI·구글 등 미국 주요 기업은 주력 AI 모델의 가중치를 공개하지 않고 자사 서버에서만 구동하며 API와 앱을 통해 접근권을 판매하고 있어, 이용자는 AI 모델을 내려받거나 자체 인프라에서 운영할 수 없음

- 반면 딥시크·문샷AI·알리바바 등 중국 AI 기업은 학습이 완료된 모델의 가중치를 허깅페이스(Hugging Face) 등에 공개해, 누구나 자체 서버에서 구동하고 용도에 맞게 수정할 수 있도록 하고 있음
- ⇒ 중국의 오픈웨이트 전략은 미국의 반도체 수출 통제라는 제약 아래에서 접근성과 가격을 앞세워 시장을 확보하려는 판단과 글로벌 AI 리더십 전략이 맞물린 결과
- 미국 정부의 첨단 GPU 수출 통제로 대규모 연산자원 확보가 어려워진 중국은 폐쇄형 구독 방식으로는 선발 주자를 추격하기 어렵다고 판단
 - 낮은 가격으로 글로벌 이용자와 데이터를 확보하고, 이를 다시 자국의 AI 기술 개선에 투입하는 순환 경로를 선택한 것으로 볼 수 있음
- 아울러 개방과 참여를 통해 AI 표준을 형성하는 중국 중심의 글로벌 AI 리더십을 확대하기 위해, 참여국에 중국의 AI 모델을 개방하는 정책을 추진하고 있음
 - '25년 7월 리창 총리가 세계인공지능대회(WAIC) 개막식에서 AI 핵심 자원이 소수 국가·기업에 집중되어 있다고 지적하며 '세계인공지능협력기구(WAICO)' 설립을 제안했고, '26년 7월 16일 WAICO가 29개국 참여로 출범⁷⁾
 - ※ WAICO는 유엔 헌장의 목적을 따르는 정부 간 국제기구로 본부는 상하이에 두며, 창립 회원국은 러시아·브라질·인도네시아 등 글로벌 사우스 중심으로 구성되고 미국·EU·일본·한국 등은 참여하지 않았음
 - 아울러 개발도상국에 5년간 5,000명 규모의 AI 연수를 제공하고 아세안·아프리카연합 등을 대상으로 국제 AI 응용 협력센터를 건설
 - 화웨이·알리바바가 일대일로 선상 국가에 데이터센터와 통신망을 공급하되 핵심 네트워크와 운영 솔루션은 자국 기업에 의존하게 하는 방식을 병행⁸⁾
- ⇒ 이 과정에서 중국 AI 기업은 정부의 지원 등에 힘입어 높은 성능의 오픈웨이트 모델을 잇따라 공개하고 있으며, 미국 AI 모델과 비교해서 성능과 비용의 균형 측면에서 경쟁력을 확보하고 있음
- '25년 딥시크 'R1' 이후 중국 AI 기업들은 높은 수준의 오픈웨이트 모델을 빠르게 시장에 공개
 - (딥시크) '25년 1월 공개된 추론 특화 모델 'R1'은 엔비디아의 저사양 GPU인 H800 칩 2천여 개로 학습해 AI 모델 개발비를 미국 빅테크의 10분에 1 수준인 약 80억 원 정도로 낮추었음

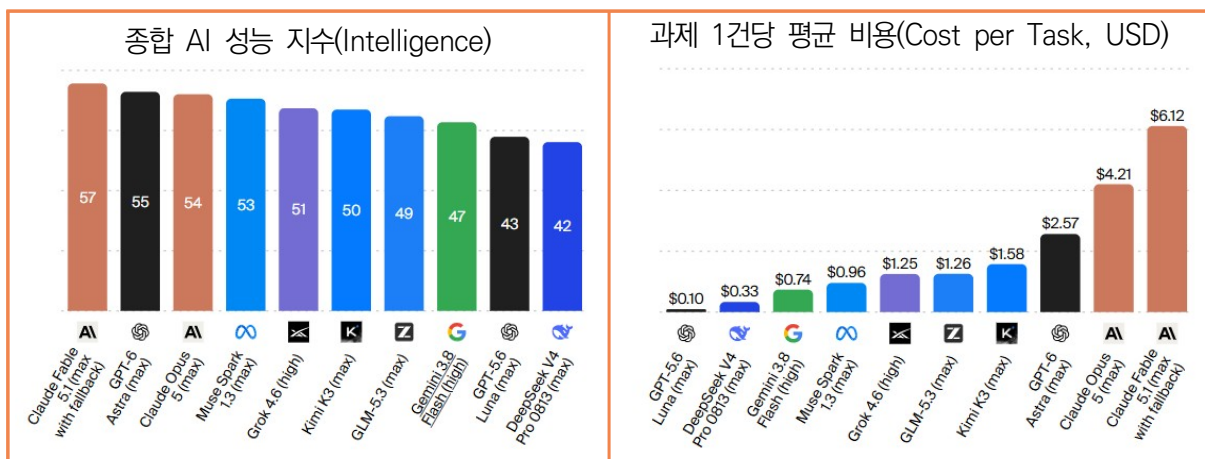
7) 뉴시스, 「中상하이에 세계AI협력기구 설립키로...29개국 참여」, 2026.7.17.

8) 아주경제, 「시진핑 첫 등판에 29개국 규합까지...中 WAIC서 'AI 국제질서' 새판 짰다」, 2026.7.19.



- (문샷AI) '26년 7월 공개된 '키미 K3'는 총 2조 8,000억 개의 파라미터를 사용하여 오픈웨이트 모델 사상 최대 규모를 보였으며, 전 세대 대비 스케일링 효율을 약 2.5배 개선하면서도 가격은 미국 모델의 3분에 1 수준으로 낮추었음
- 글로벌 AI 모델 평가에서 최상위 성능과 최저 비용은 여전히 미국 모델이 차지하고 있으나, 일부 중국 모델은 성능과 비용의 균형에서 미국 주요 모델을 앞서고 있음
- 아티피셜 애널리시스(Artificial Analysis)의 종합 AI 성능 지수 상위 3개는 모두 미국의 모델이며, 과제 1건당 비용이 가장 낮은 모델도 미국 모델임
 - ※ 종합 AI 성능 지수 상위 3개는 클로드 페이블5.1(57점), GPT-6 아스트라(55점), 클로드 오피스5(54점)이며, 과제 1건당 비용이 가장 낮은 모델은 GPT-5.6 루나(0.10달러)
- 딥시크 V4 프로(42점)는 성능은 낮으나 과제당 비용(0.33달러)이 두 번째로 저렴하여 일부 중국 모델은 미국 모델에 비해 높은 가성비를 보임
 - ※ 중국의 문샷AI의 키미 K3(50점)와 즈푸(Z.ai)의 GLM-5.3(49점)은 구글 제미니 3.8 플래시(47점)와 GPT-5.6 루나(43점)를 상회
- 특히, 성능 1위인 클로드 페이블5.1은 키미 K3보다 종합 AI 성능 점수가 7점 높은 대신 과제당 평균 비용은 6.12달러로 약 3.9배에 달해, 최고 성능을 요구하지 않는 업무에서는 중국 모델의 비용 효율이 두드러짐

〈 AI 모델 성능 지수 및 평균 비용 비교 〉



주: (좌) 여러 벤치마크를 가중 합산한 종합 지수, (우) 지수 산정 과제 1건을 수행하는 데 드는 가중평균 비용으로 실제 소비 토큰량이 반영된 값.

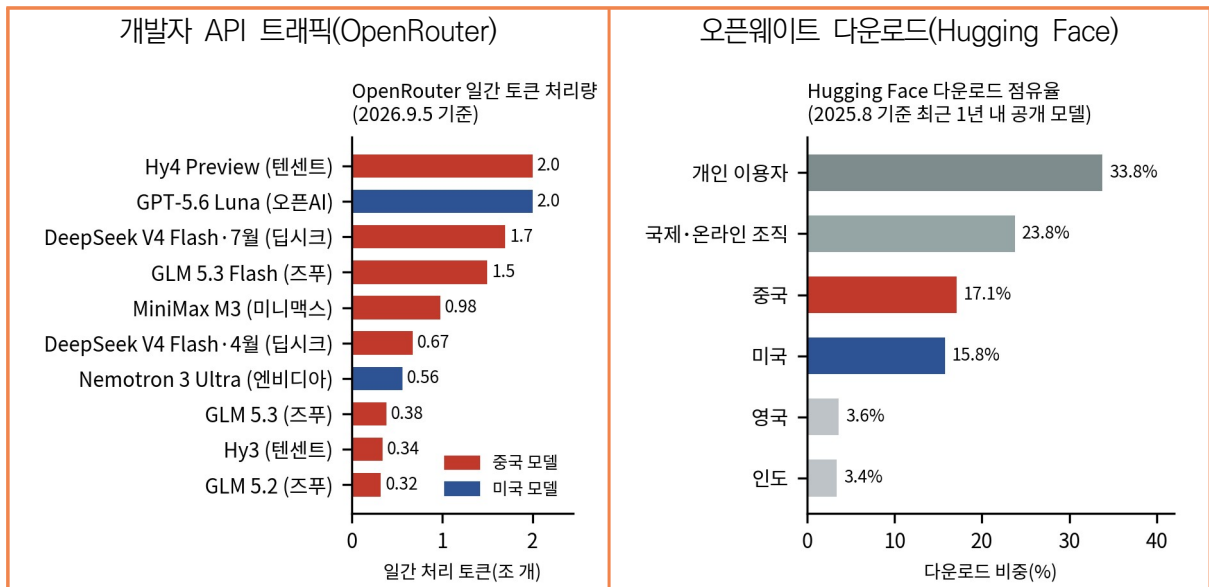
출처 : 아티피셜 애널리시스 홈페이지, (<https://artificialanalysis.ai/>), (검색일: 2026.9.7.).

➔ 높은 가성비와 글로벌 사우스를 중심으로 한 이용자 확대에 힘입어, 실제 이용량 지표에서 중국 모델의 비중이 빠르게 증가

- 개발자 API 트래픽을 집계하는 오픈라우터(OpenRouter)에서는 '26년 9월 5일 기준 일간 처리 토큰 상위 10개 모델 중 8개가 중국 모델이었음

- 오픈웨이트 확산을 보여주는 허깅페이스 다운로드에서도 '25년 8월 기준 최근 1년 내 공개된 모델의 국가별 점유율은 중국(17.1%)이 미국(15.8%)을 처음 앞선 것으로 조사됨
- 다만 기업의 유료 LLM API 지출 기준으로는 앤트로픽(40%), 오픈AI(27%), 구글(21%)로 미국 폐쇄형 모델이 우위여서, '이용량은 중국, 매출은 미국'이라는 구조를 보이고 있음⁹⁾

〈 AI 모델 이용률 비교 〉



주 : (좌) 2026.9.5. 기준 일간 처리 토큰, (우) 2024.8 ~ 2025.8까지 1년간 공개된 AI 모델의 다운로드 점유율을 개발 주체의 소재 국가별로 집계한 값.

출처 : (좌) 오픈라우터 홈페이지, 「LLM Rankings」, (<https://openrouter.ai/rankings>), (검색일: 2026.9.7.), (우) Shayne Longpre et al., 「Economies of Open Intelligence: Tracing Power & Participation in the Model Ecosystem」, arXiv:2512.03073, 2025.

나. 개방에서 선별적 통제로의 전환

- ➔ 미국의 미토스 수출 통제 직후인 '26년 7월, 중국도 자국 첨단 AI 모델의 해외 접근을 제한하는 방안을 검토하기 시작¹⁰⁾
- 중국 상무부와 국가발전개혁위원회(NDRC)는 알리바바, 바이트댄스, 즈푸 관계자가 참석한 회의에서 해외 접근 제한 방안을 논의했으며, 아직 공개되지 않은 차세대 모델까지 대상에 포함되었음
- 그 배경에는 고성능 AI 모델을 안보 위협으로 보는 인식이 미국에 이어 중국에서도 확산된 점과, 키미 K3가 미국과의 격차를 크게 좁혔다는 기술적 자신감이 함께 작용하고 있음

9) Menlo Ventures, 「2025: The State of Generative AI in the Enterprise」, (<https://menlovc.com/perspective/2025-the-state-of-generative-ai-in-the-enterprise/>), (검색일: 2026.9.7.).

10) 한국일보, 「中도 첨단 AI 모델 해외 차단 검토… 美 미토스 등 통제에 맞불」, 2026.7.8.



- ➔ 검토안의 초점은 모델의 사용 통제가 아니라 AI 모델을 통째로 소유하는 것에 대한 통제에 있으며, 이를 위해 기존의 API 접근은 유지하되 가중치의 해외 반출을 차단하는 방식을 검토¹¹⁾
- 성능이 낮은 오픈소스 모델은 신고만 거치고, 더 강력한 시스템은 보안 심사를 받으며, 최상위 성능 모델은 공개 배포를 금지하거나 중국 내에서만 사용하도록 하는 단계별 규제가 검토되고 있음
- 이에 대해 중국 내 주요 AI 기업들은 과도한 통제가 해외 사업 확대와 글로벌 경쟁에서의 성장 속도를 떨어뜨릴 수 있다는 의견을 당국에 전달한 것으로 알려졌다

다. 소결: 미국의 수출 통제가 태동시킨 중국형 AI 생태계

- ➔ 미국의 대중국 첨단 GPU 수출 통제는 중국의 추격을 지연시키는 효과는 있었으나, 연산자원 효율화와 개방형 확산이라는 중국 특유의 AI 생태계를 태동시킴
- 딥시크는 낮은 비용 구조로 세계 개발자 시장에 진입했고, 키미 K3는 반도체 규제 속에서 스케일링 효율을 2.5배 끌어올린 점을 핵심 성과로 내세웠음
- 스탠퍼드대 「2026 AI 인덱스」에 따르면 2025년 주목할 만한 AI 모델은 미국 59개, 중국 35개였으나 양국 최상위 모델의 성능 격차는 사실상 해소
 - ※ 미국 국제전략문제연구소(CSIS)도 중국 모델이 미국 최첨단 시스템보다 불과 몇 달 뒤진 수준이라고 분석했음
- ➔ 앞으로 중국의 선택은 개방 기조의 철회가 아니라, 범용 모델은 오픈웨이트로 확산시키고 최첨단 모델만 통제하는 ‘이중 구조’로 수렴할 것으로 전망
- 이 경우 미국 모델과 중국 모델 어느 쪽도 안정적 공급이 보장되지 않으며, 가성비를 이유로 중국 오픈웨이트를 활용해 온 국내 기업에는 새로운 공급 리스크가 될 수 있음

11) AI타임스, 「중국, 오픈소스 AI ‘가중치’ 통제 검토…」해외 직접 다운로드 막는다, 2026.7.21.

3 미·중 간 AI 모델 수출 통제의 구조와 쟁점

가. 통제 단위의 이동: 재화의 이전에서 접근권의 관리로

⇒ 미국 정부가 취한 미토스 수출 통제의 본질은 통제의 대상이 물리적 재화에서 디지털 서비스에 대한 접근권으로 옮겨간 데 있음

- 기존의 전략 물자 통제는 해당 품목이 국경을 넘는 행위를 전제로 하나, AI 모델은 물리적 반출 없이 원격 접속만으로 그 능력이 이전되므로 품목 지정 방식으로는 관리되기 어려움
- 또한, 고성능 AI 모델은 민간 업무와 사이버 공격, 연구와 국방에 동시에 활용되는 이중·다중 용도 자산이어서 용도를 기준으로 통제를 하는 것도 어려움
- 그 결과 통제의 실효적 수단이 '무엇을 반출하지 못하게 할 것인가'에서 '누구에게 접속을 허용할 것인가'로 이동한 것으로 볼 수 있음

⇒ 이러한 변화는 고성능 AI 모델을 국가전략자산의 지위로 끌어올림

- 전략자산은 통상 대체가 어려운 공급의 집중, 경제와 안보 전반에 미치는 파급력, 확보 여부가 곧 국력의 격차로 이어지는 성질을 요건으로 하는데, 고성능 AI 모델은 이 세 가지를 모두 충족함
- 특히 AI 모델은 산업·연구·국방 전반에 공통으로 투입되는 범용 기반 기술이면서 소수 기업이 공급을 독점하고 있어, 그 가용성이 곧 국가 기능의 수월성과 연속성을 좌우함
- 에이전트 AI와 피지컬 AI로 활용이 확장될수록 AI 모델은 개별 서비스를 넘어 산업 공정과 행정, 국방 체계가 그 위에서 작동하는 기반 설비가 되므로, 공급의 중단은 곧 그 위에서 수행되던 업무 전체의 중단을 의미하게 됨
- 나아가 AI 역량의 격차는 생산성과 군사적 능력의 격차로 직결되므로, 누구에게 어떤 순서로 접근을 허용할 것인지를 정하는 권한 자체가 국가 간 경쟁의 수단이 됨
- 미국이 자국 기업의 모델 출시 시점과 공개 범위까지 관리하기 시작한 것도 이러한 자산의 초기 배분을 국가가 직접 통제하겠다는 판단으로 이해할 수 있음

나. 접근권의 계층화와 통제에 대한 낮은 예측 가능성

⇒ 고성능 AI 모델에 대해서 '정부 → 정부가 검증한 기관 → 신뢰 파트너 → 일반 이용자' 순의 계층적 접근 구조가 형성되어, 수입국의 지위가 수출국의 판단에 따라 결정됨



- 엔트로픽의 미토스 프리뷰와 미토스5는 프로젝트 글래스윙 파트너 선정에 미국 정부가 관여했고, 오픈AI의 GPT-5.6도 정부와 공유된 신뢰 파트너에게 우선 제공되었음
- 행정명령 제14409호의 ‘신뢰할 수 있는 파트너’ 선정 메커니즘은 이러한 계층 구조를 일회성 조치가 아니라 상시 제도로 고정할 가능성이 있음
- ⇒ AI 모델 수출 통제의 기준과 절차가 명확하지 않고 수출국 정부의 재량권이 크기 때문에, 수입국이 통제의 대상과 시점을 사전에 가늠하기 어려움
- 미토스 수출 통제는 법령 개정이나 통제목록 등재가 아니라 개별 기업에 대한 비공개 서한으로 이루어져, 통제의 대상과 시점·기간이 사전에 공표되지 않았음
- 해제 역시 기업의 이행 약속을 전제로 한 비공개 서한으로 이루어져, 유사한 조치가 언제 어떤 요건에서 반복될지 예측하기 어려움
- ⇒ 그 결과 수입국의 기업과 정부는 만일의 사태에도 서비스와 국가 기능을 안정적으로 지속하기 위해 상시적인 대체 수단 확보와 외교적 교섭이라는 가외적인 비용을 부담하게 됨
- 통제가 실제로 발동되지 않더라도 그 가능성만으로 대체 모델의 확보와 전환 체계의 유지에 비용이 지속적으로 투입됨
- 아울러 상위 계층에 편입되기 위한 협의와 설득에도 외교적 자원이 소요되므로, 접근권의 확보 자체가 국가 차원의 정책 과제가 됨

다. 폐쇄와 개방의 수렴: 공통 목표로서의 통제력

- ⇒ 미국과 중국 모두 고성능 AI의 수출 통제를 직·간접적으로 고려하고 있다는 점에서, 미-중 경쟁을 폐쇄와 개방의 대립으로 보는 것은 충분하지 않으며, 양국 전략의 공통된 본질을 ‘AI 생태계의 연결을 누가 관리하는가’로 보는 것이 적절함¹²⁾
- 미국은 접근권 통제로 최고 성능과 안전성 검증, 고신뢰 기업 시장을 확보하는 쪽에, 중국은 오픈웨이트와 낮은 이용료로 확산과 표준 영향력을 넓히는 쪽에 무게를 두고 있음
- 어느 한쪽이 우월한 전략이라기보다 서로 다른 자산을 축적하는 방식이며, 양국 모두 상대를 완전히 배제하기보다 자신에게 유리한 방식으로 연결 구조를 재편하려 함
- ⇒ 실제 정책에서도 미국과 중국은 서로의 방식을 부분적으로 흡수하면서 수렴하고 있음
- 미국은 오픈소스·오픈웨이트 지원과 풀스택 수출을 장려하면서도, 프론티어 모델에는 사전 검토와 접근 계층화를 적용하고 있음

12) 최중현학술원·서울대학교 미래전략연구센터, 「보유에서 운용으로: 에이전트 AI 시대의 국가안보와 소버린 AI 2.0」, 2026.8.

- 중국은 오픈웨이트 확산을 유지하면서도 최상위 모델의 가중치 반출은 제한하는 방안을 검토하고 있음
- 결국 개방과 폐쇄는 목적이 아니라 수단이며, 양국 모두 자국이 관리할 수 있는 범위 안에서 생태계를 넓히려 한다는 점에서 동일한 구조를 공유함
- ⇒ 결국 제3국은 어느 진영에서도 고성능 AI 모델 공급을 보장받지 못하는 위치에 놓이게 됨
- 미국 모델은 접근권이, 중국 모델은 가중치의 소유가 통제의 분기점이 되어 두 경로 모두 외부의 정책 결정에 종속되는 구조를 보임
- 따라서 한국의 과제는 어느 쪽을 선택할 것인가가 아니라, 어느 쪽이 제한되더라도 핵심 기능을 지속할 수 있는 구조를 갖추는 데 있음

라. 에이전트 AI와 피지컬 AI 시대, 독자 모델의 중요성 심화

- ⇒ AI의 활용 방식이 대화형·생성형 AI에서 에이전트 AI와 피지컬 AI로 급격히 확장되면서, 외산 모델에 대한 의존은 비용 부담과 통제력 상실의 문제를 초래할 우려가 있음
- 에이전트 AI는 하나의 요청을 수십 단계로 나누어 반복 수행하므로, 기존 생성형 AI의 단순 질의응답 대비 10~50배의 토큰을 소모
- 업무 난이도에 따라 국내·외 모델을 나누어 배치하는 ‘모델 믹스’로 비용을 관리할 수 있으나, 최상위 모델에 대한 접근이 제한되면 작업 흐름 전체가 중단되므로 주권적으로 운용 가능한 AI 모델의 중요성이 높아짐
- 피지컬 AI는 기계·장치에 탑재되어 인식·판단·행동을 반복하는 폐루프 구조(closed loop)이므로, 탑재된 모델의 접근권이 제한되면 물리적 작동 자체에 대한 통제력을 상실
- 피지컬 AI의 활용 영역이 산업·신체·생명과 직결된다는 측면에서 주권적으로 통제 할 수 있는 AI 모델이 더욱 필요한 영역임
- ⇒ 보안 측면에서도 AI 모델의 성능보다 통제권의 소재가 더 중요한 문제가 됨
- 에이전트 AI는 권한을 위임받아 스스로 실행하므로, 작업 과정에서 남기는 판단과 접근의 기록이 어느 관할권의 서버를 지나느냐가 새로운 안보 변수로 부상
- 피지컬 AI는 제조 공정과 물류, 전력 설비 등 기간 인프라의 운영에 직접 결합되므로, 접근 중단의 영향이 서비스 장애를 넘어 현장 운영의 정지로 이어지지 않도록 관리하는 것이 중요
- ⇒ 따라서 독자 AI 모델의 확보는 기술 자립을 상징하는 목표가 아니라, 비용을 통제하고 운영의 연속성을 지키기 위한 실무적 수단으로 이해할 필요가 있음

4 한국의 대응 과제

⇒ 소버린 AI 전략을 ‘한국산 AI 모델·인프라의 확보’에서 ‘AI 생태계에 대한 주권적 통제력의 강화’로 재정의할 필요가 있음

- 핵심은 독자 모델의 보유 여부가 아니라 외부의 결정에도 불구하고 필요한 AI 기능을 지속적으로 운용할 수 있는가에 있음
 - 이는 핵심 모델과 인프라에 대한 접근권을 안정적으로 확보하는 능력과, 특정 모델이나 서비스가 중단되더라도 즉시 다른 체계로 전환해 핵심 업무를 지속하는 능력으로 구체화됨
- 이하에서는 AI 모델·시장·보안·외교의 네 층위와 이를 뒷받침할 거버넌스로 나누어 과제를 제시함

⇒ AI 모델: 독자 모델과 개방형 생태계의 병행

- AI 생태계에 대한 주권적 통제력의 출발점은 독자적인 AI 모델을 확보하는 것이며, 정부는 핵심 업무를 지속할 수 있는 수준의 성능과 운용 능력을 갖추는 방향으로 독자 AI 파운데이션 모델 사업을 추진하는 것이 중요
- 이 과정에서 소수 정예팀을 단계적으로 탈락시키는 현재의 선발 방식은 기술적 다양성을 좁힐 수 있으므로, 탈락 팀의 접근과 방법론이 생태계에 남도록 설계하고 분야별 소형 전문 모델을 육성하는 상향식 접근을 병행할 필요
- 개발된 AI 모델이 산업과 현실 공간에서 외산 모델을 대체하지 못하면 독자 모델의 전략적 의미는 제한적이므로, 정예팀 평가의 기준도 벤치마크 점수에서 운용 능력과 대체 전환 가능성으로 옮겨야 함
- 우수 오픈웨이트 모델 확보를 병행하여 특정 공급자에 대한 의존을 분산해야 함
 - 해외의 우수 오픈웨이트 모델을 국내에서 지속적으로 운영할 수 있다면 독자 모델의 성능 한계를 보완하면서 특정 기업·국가에 대한 의존도 함께 낮출 수 있음
 - 다만 중국의 가중치 통제 논의에서 보듯 개방형 모델의 이용도 영속적으로 보장되지 않으므로, 복수의 모델을 확보하고 규제 저촉과 보안 검증을 사전에 점검하는 체계를 갖추어야 함

⇒ AI 시장: 대체 불가능한 수요국으로의 도약

- 한국 시장을 미국·중국 등 주요 AI 모델 수출국이 놓칠 수 없는 핵심 수요국으로 자리매김하도록 만드는 것이 AI 접근권을 지키는 현실적인 수단임

- 수출 통제는 자국 기업의 매출 손실을 감수해야 하는 조치인 만큼, 수요자로서의 비중이 클수록 통제의 대상에서 제외되거나 우선적으로 복원될 가능성이 높아짐
- 아울러 신규 모델의 우선 배포나 공동 검증 파트너로 참여할 기회가 늘어나고, AI 보안 취약점이나 사전 위험평가 결과를 신속하게 공유받을 수 있는 협력 기반도 확대됨
- 반대로 시장 규모가 작으면 상대국이 통제로 부담하는 비용도 작아 고려의 우선순위에서 밀리게 되므로, 수요 기반의 확대는 그 자체로 안보적 의미를 가짐
- 이때 수요 기반의 크기는 결국 국가 전반의 AI 전환(AX) 수준에 좌우되므로, AX의 속도와 범위를 함께 끌어올려야 함
- AI에 대한 수요는 개인의 이용이 아니라 기업과 공공의 업무가 AI 위에서 처리되는 정도에서 발생하며, 에이전트 AI의 확산으로 업무 단위의 소비량이 커질수록 국가 간 수요 격차도 함께 벌어짐
- 또한 AX 과정에서 축적되는 산업별 데이터와 활용 사례는 국내 모델의 학습 기반인 동시에 해외 사업자와의 협상 자산이 되므로, AX는 시장의 확대와 독자 역량의 강화를 동시에 뒷받침함
- 다만 도입률을 높이는 것만으로는 부족하고 업무 방식 자체가 바뀌어야 실질적인 수요로 이어지는바, 그 출발점은 조직의 의사결정권자와 중간관리자가 AX의 본질을 인식하고 성과에 대한 보상과 실패에 대한 용인을 제도화하는 것임

⇒ AI 보안: 독자적 보안 역량의 내재화

- 미토스 사태는 AI 모델 경쟁의 무게중심을 추론 성능에서 ‘보안 통제권의 확보’로 옮겨놓았으며, 이러한 변화에 대응하기 위해서는 AI 보안을 독립적인 정책 영역으로 격상할 필요가 있음
- AI는 공격과 방어 양쪽에 동시에 활용되는 수단이므로, 상대의 공격 역량이 고도화되는 속도에 맞추어 자국의 방어 역량을 함께 높이지 않으면 그 격차가 누적됨
- 하지만 국내 보안 체계가 외산 모델에 의존하는 한, 해당 모델의 접근이 제한되면 방어 역량도 함께 중단될 수 있음
- ※ 미토스 차단 당시 국내 기업의 AI 사이버위협 공동 대응에 차질이 빚어진 것이 그 사례
- 이에 정부는 국내 정보보호 체계를 독자 AI 기술 기반으로 전환할 계획인바, 이를 뒷받침할 세 가지 기반을 함께 갖추어야 함
- **(독자 역량)** 특정 모델의 접근이 끊기더라도 취약점 탐지와 패치가 지속되도록, 국내 보안 환경에 맞는 보안 특화 모델과 그 성능을 검증할 능력을 확보하는 것이 우선임

- (평가 체계) AI안전연구소 등 전문기관의 기술적 전문성과 독립성을 보장하고, 평가의 단위에 어떤 판단이 어느 관할권의 통제 아래 위임되었고 그 결과를 되돌릴 수 있는가를 포함해야 함
- (국제 협력) 단일 국가나 개별 기업이 고도화된 위협을 완벽히 방어하는 것은 불가능하므로, 신뢰 관계에 기반한 글로벌 보안 협력망 참여가 병행되어야 함

➔ AI 외교: 전략적 상호보완성에 기반한 협력 관계의 관리

- AI 접근권이 통상·안보 의제로 확장된 만큼, 주요국의 정책 동향을 상시 파악해 국내 정책에 반영하는 체계가 필요함
 - 각국의 조치는 공표된 규칙보다 앞서 진행되는 경우가 많아 사후에 인지해서는 대응 시점을 놓치게 되므로, 주요국의 규제 논의와 기술 동향을 지속적으로 분석하고 그 결과를 산업계와 공유할 필요가 있음
- 아울러 핵심 국가와의 협력 관계를 평시에 면밀하게 관리해 나가야 함
 - AI 공급망은 모델·반도체·데이터센터·전력이 국경을 넘어 결합되어 있어, 어느 국가도 단독으로 완결하기 어려운바, 협력의 지속성 자체가 정책 목표가 됨
 - 특히 한국은 메모리 반도체와 첨단 제조, 데이터센터 입지 등 상대국이 필요로 하는 역량을 보유하고 있으므로, 서로에게 이익이 되는 전략적 상호보완 관계임을 지속적으로 설명할 필요가 있음
 - 이러한 관계가 축적될 때 통제가 논의되는 단계에서 한국의 사정이 고려될 수 있고, 사전 통보와 협의 같은 실무적 관행도 자리 잡을 수 있음
- 국제규범 논의에는 초기 단계부터 참여하고, 이를 관통하는 국가 차원의 원칙을 정립해야 함
 - 규범은 완성된 뒤 가입하는 것과 초안 단계에서 참여하는 것의 의미가 다르므로, 유사 입장국 간 협의가 본격화되기 전에 핵심 원칙과 기술 기준을 준비할 필요가 있음
 - AI 모델의 안전성 검증과 접근 조건에 관한 기준은 주요국이 선제적으로 설계할 경우 사실상의 국제 표준으로 작동할 수 있으므로, 논의 초기부터 우리의 산업 여건과 기술 기준이 반영되도록 해야 함
 - 이를 위해 각 부처와 국제기구별로 이루어지는 대외 활동이 하나의 원칙 아래 조율될 수 있도록, 국가 차원의 AI 대외 정책 기조를 사전에 정립해 둘 필요가 있음

➔ AI 거버넌스: 정부의 실행력 제고와 국회의 역할 강화

- 모델·시장·보안·외교 과제는 여러 부처와 정책 영역에 걸쳐 있어 조정 난이도가 높은 만큼, 정책의 내용 못지않게 AI 정책 거버넌스의 실행력이 중요함
- AI 기본법과 시행령이 '26년 1월 22일 시행되어 거버넌스 체계와 고영향 AI, 투명성·안전성 의무 등 기본 틀은 마련되었으나, 현 국면을 돌파할 구체적인 단기 대응 체계는 약한 상황임
 - 특히 접근 제한과 같은 상황은 예고 없이 발생하므로, 사안이 생길 때마다 부처 간 협의를 새로 구성하는 방식으로 대응 시점을 맞추기 어려움
- 따라서 정부는 부처를 가로지르는 조정 기능을 상시화하고, 정책의 순환 주기를 짧게 설정해야 함
 - 국가인공지능전략위원회와 AI미래기획수석, 과학기술·AI 부총리의 삼각편대가 원활하게 협력할 수 있도록 해야 함
 - 아울러 정책 시행의 결과를 빠르게 평가해 다음 정책과 입법에 신속히 반영하는 체계와, 이를 뒷받침할 행정부의 전문 인력 확대가 함께 요구됨
- 국회 역시 AI 입법·정책 역량을 높여 여러 과제가 적기에 실현되도록 지속적으로 점검하고 지원해야 함
 - AI 기본법의 시행 성과와 미비점을 정기적으로 점검하고, 접근 제한과 같은 상황에서 공공·핵심 인프라의 대체 전환을 뒷받침할 제도적 근거가 필요한지 검토할 필요가 있음
 - 아울러 소버린 AI 관련 예산이 개별 사업으로 분산되지 않고 모델·시장·보안·외교의 과제와 연결되어 집행되는지 살펴야 함