

July 23, 2026

미국 정부의 Anthropic AI 모델 접근 통제와 해제: AI 수출통제 리스크의 새로운 국면

I. 배경

최근 미국 정부가 Anthropic의 최신 AI 모델인 Claude Fable 5 및 Mythos 5에 대하여 외국 국적자의 접근을 전면 중단하도록 지시하였다가, 약 3주 만에 이를 해제한 사례가 주목받고 있습니다. 이번 조치는 상용 배포된 AI 모델을 대상으로 미국의 수출통제 권한이 직접 발동된 최초의 사례로, 첨단 AI 모델의 출시-배포-접근권 부여를 미국 정부가 국가안보 관점에서 직접 통제할 수 있음을 보여주었습니다.

Anthropic은 2026년 6월 9일 Claude Fable 5 및 Mythos 5를 공개하였습니다. 두 모델은 동일한 기반 모델에 기초하되, Fable 5는 사이버보안 등 고위험 영역에 대한 안전장치를 적용하여 일반 이용자에게 제공되는 모델이고, Mythos 5는 해당 제한이 일부 완화된 형태로 사이버보안 및 생명과학 분야의 검증된 파트너에 한정하여 제공되는 모델입니다.¹

그러나 6월 12일 Anthropic은 미국 상무부 산업안보국(Bureau of Industry and Security, "BIS")으로부터 국가안보를 근거로 Anthropic의 외국 국적 임직원을 포함하여 미국 내외의 모든 외국 국적자(foreign national)에 대해 두 모델에 대한 접근을 중단하라는 서한을 받았다고 발표하였습니다. Anthropic은 이용자의 국적을 실시간으로 확인할 수단이 없다는 이유로 두 모델을 전 세계 모든 고객에 대하여 즉시 중단하였습니다(다른 Claude 모델의 이용에는 영향이 없었습니다).²

주목할 점은 이번 조치가 특정 우려국가가 아닌 모든 외국 국적자를 대상으로 하였다는 것입니다. 한국 국적자와 한국 기업 역시 예외 없이 차단 대상에 포함되어 미국 내에서 근무하는 한국 국적 임직원과 클라우드 플랫폼을 경유하여 해당 모델을 이용하던 한국 기업 모두 사전 통지 없이 접근이 중단되었습니다.

이후 미국 정부는 제한을 단계적으로 완화하여, 6월 26일 핵심 인프라 관련 일부 미국 기관·기업에 대한 Mythos 5 접근 복원을 승인하였고, 6월 30일 Fable 5 및 Mythos 5 양 모델에

¹ Anthropic(2026.6.9). "[Claude Fable 5 and Claude Mythos 5](#)".

² Anthropic(2026.6.12). "[Statement on the US government directive to suspend access to Fable 5 and Mythos 5](#)"; CNBC(2026.6.12). "[Anthropic disables access to Fable 5 and Mythos 5 to comply with government directive](#)".

대한 통제를 해제하였습니다.³ Fable 5는 7월 1일부터 일반 제공이 재개된 반면, Mythos 5는 정부의 통제 해제 이후에도 Anthropic 자체의 신뢰 기반 접근 프로그램(trusted access program)에 따라 승인된 기관 및 조직을 대상으로 제한적으로 제공되고 있습니다.⁴

이번 조치는 단기간 내 해제되었지만, 최첨단 AI 모델이 단순한 소프트웨어 서비스가 아니라 정부가 필요하다고 판단하는 경우 그 배포와 접근 자체를 통제할 수 있는 하나의 전략자산으로 취급되기 시작하였다고 볼 수 있습니다.

II. 주요 내용

1. 이번 조치의 특징: 'Is-informed' 방식에 의한 통제

미국 정부는 조치의 내용과 근거를 공식 공표하지 않았으나, 이후 언론 보도를 통해 서한의 내용이 알려졌습니다.⁵ 보도에 따르면, 이번 조치는 수출관리규정(Export Administration Regulations, "EAR") Part 744에 따른 이른바 'is-informed' 방식, 즉 규칙 제정이나 품목 분류 개정 절차 없이 개별 기업에 서한으로 수출허가 요건을 부과하는 방식으로 이루어졌으며, 그 근거로 수출통제개혁법(Export Control Reform Act, "ECRA")상 신기술·기반기술에 대한 임시통제 조항(50 U.S.C. § 4817(b)(1)) 등이 인용된 것으로 알려져 있습니다.⁶

이번 조치는 ECRA의 신기술 통제 권한이 상용 AI 모델에 적용된 최초의 사례로서 이를 뒷받침하는 명시적인 이행 규정이 없는 상황에서 사전 예고, 의견 수렴, 관보 게재, 유예기간 등 통상적인 규정 제정과 관련한 절차적 요건을 충족함이 없이 개별 고지만으로 즉시 효력을 발생시켰다는 점이 가장 큰 특징입니다. 나아가 외국인에게 기술의 이전이 있었던 것이 아니라 외국인이 기술을 사용할 수 있었다는 점만으로 간주수출을 인정하고 수출통제 조치를 취한 것이라고 해석할 수도 있습니다. 요컨대 규정 입안 전 일정한 사전절차를 전제로 설계된 기존의 규제 대응 체계가 작동하지 않는 새로운 유형의 규제 리스크가 등장한 것으로, 기업들은 앞으로 규제의 '예측'에 더하여 예고 없는 통제조치에 대한 대비가 필요할 것으로 보입니다.

³ TechCrunch(2026.6.26). "[Trump administration releases Anthropic Mythos to be used by more than 100 US companies, agencies](#)".

⁴ AP News(2026.7.2). "[Trump administration lifts restrictions on Anthropic's Claude models after cybersecurity alarm](#)".

⁵ Bloomberg는 2026년 6월 16일 상무부가 Anthropic에 발송한 서한을 공개하였습니다. Bloomberg(2026.6.16). "[Read the Lutnick Letter That Led Anthropic to Disable Mythos](#)".

⁶ 서한의 법적 구조에 대한 분석으로는 Harvard Law Review(2026.6.26). "[Is Access to Fable an Export?](#)"를 참고 바랍니다.

2. 통제 완화의 경위: 전면 복원이 아닌 '차등적 접근'으로의 재편

이번 조치를 촉발한 것은 사이버보안 리스크였습니다. 보도에 따르면 Amazon 연구진이 Fable 5의 안전장치를 우회하는 기법을 발견하여 정부에 보고하였고, 해당 기법을 통해 모델이 소프트웨어 취약점을 식별하고 일부 사례에서는 이를 악용하는 코드까지 생성할 수 있다는 점이 문제되었습니다. 다만 Anthropic은 해당 기법이 특정한 경우에만 작동하는 좁은 우회이고, 유사한 능력은 통제 대상이 아닌 타사의 공개 모델에서도 확인된다고 반박하는 등 위험성 평가를 둘러싼 다툼이 있었습니다.⁷

복원의 구조도 눈여겨볼 필요가 있습니다. Fable 5는 일반 제공이 재개되었지만 클라우드 경유 이용은 순차 복원되었고, Mythos 5는 여전히 검증된 조직에 한정하여 제공됩니다. 요컨대 이번 통제 완화는 전면 공개로의 복귀가 아니라, 모델의 성능, 사용 목적, 이용자 유형, 보안조치 수준에 따라 접근 범위를 달리 설정하는 차등적 접근 구조로의 재편이며, 이러한 접근 통제가 향후 업계 표준 내지 제도의 형태로 정착될 가능성도 배제할 수 없습니다.⁸

3. 관련 소송의 제기: 호스팅 AI 모델에 대한 '접근'은 '수출'인가

이번 사건은 소송으로도 이어졌습니다. Anthropic의 고객사인 미국 기업 Legion LegalTech는 6월 23일 워싱턴 D.C. 연방지방법원에 대통령, 상무장관 및 BIS 담당 차관을 상대로 이번 조치의 취소(vacatur)와 접근 복원을 구하는 소를 제기하였습니다. Legion은 캐나다에서 근무하는 캐나다 국적 개발 인력을 두고 있어 이번 지시로 사업 운영에 회복하기 어려운 손해를 입었다고 주장하였는데, 규제 대상 기업이 아닌 고객 기업이 직접 정부를 상대로 제소한 첫 사례라는 점에서, AI 모델 접근에 대한 수출통제가 공급자뿐 아니라 해당 모델에 의존하는 이용 기업에도 상당한 법적·경제적 영향을 초래할 수 있음을 보여줍니다.⁹

Legion의 청구원인은 ① AI 모델 가중치를 직접 규율하였던 유일한 통제품목 분류(ECCN 4E091)는 BIS가 2025년 시행을 유예하여, 호스팅된 AI 모델 접근을 규율하는 유효한 통제품목이 현재 존재하지 않고, ② 호스팅 모델의 이용은 기술·소스코드·모델 가중치를 이전하지 않고 추론 결과인 텍스트 출력만을 제공하므로 EAR상 수출 내지 간주수출의 정의에 해당하지 않으며, ③ 국제비상경제권한법(International Emergency Economic Powers Act, "IEEPA")상 정보·정보자료에 대한 통제 배제 조항(Berman Amendment)에 저촉되고, ④ 유사한 능력의 타사 모델은 규제하지 않으면서 특정 모델만 차단한 것은 행정절차법(Administrative Procedure Act, "APA")상

7 Anthropic(2026.6.30). "[Redeploying Fable 5](#)"; Infosecurity Magazine(2026.7.1). "[Anthropic's Fable 5 and Mythos 5 Are Back with New Security Guardrails](#)".

8 CNBC(2026.6.30). "[Anthropic says Trump admin has lifted export controls on Claude Fable 5 and Mythos 5](#)".

9 Legion LegalTech Corp. v. United States, et al.([링크](#)); Bloomberg(2026.6.23). "[Anthropic Customer Sues US Over Loss of Fable AI Access](#)"; Export Compliance Daily(2026.6.25). "[Lawsuit: US Can't Block Anthropic Models With Export Controls That 'Don't Exist'](#)".

자의적·전단적 처분이라는 것입니다.

한편 본건 조치 이전부터 Anthropic은 국방부의 “국가안보상 공급망 리스크 공급자” 지정에 대해 별도의 취소소송을 진행하고 있었는데, 이는 최근 일련의 사건들이 첨단 AI 모델의 이용 범위와 국가안보 규제의 한계를 둘러싼 미국 정부와 AI 기업 간 갈등의 연장선상에 있음을 보여줍니다.¹⁰

6월 30일 통제가 해제됨에 따라 Legion 소송은 소의 이익이 다투어질 가능성이 있습니다. 그러나 이 사건이 제기한 근본 쟁점, 즉 호스팅된 AI 모델에 대한 접근 제공이 수출통제법상 ‘수출’에 해당하는가라는 문제는 사법적 판단 없이 남게 되었습니다. 법적 근거의 불확실성이 해소되지 않은 채 통제의 선례만 남았다는 점은 유사한 조치가 다른 모델·다른 기업을 대상으로 반복될 수 있음을 의미하며, 이 불확실성 자체가 기업이 관리하여야 할 리스크가 될 수 있습니다.¹¹

III. 시사점

이번 사건이 보여주는 것은 미국 정부가 첨단 AI 모델의 배포와 접근을 직접 통제할 수 있고 실제로 통제하였다는 사실입니다. 그 통제는 전면 금지라는 단일한 형태가 아니라 외국 국적자에 대한 접근 제한, 모델의 성능과 위험도에 따른 차등적 허용, 신뢰 기반 접근 프로그램을 통한 선별적 제공과 같은 정교한 방식으로 나타날 수 있습니다. 또한 이러한 통제는 정식 규칙 제정이 아닌 개별 서한에 의해 즉시 발효될 수 있으며, 그 영향은 공급자를 넘어 해당 모델에 의존하는 전 세계 이용 기업에까지 직접 미칠 수 있습니다.

사용자 기업 입장에서 AI 서비스의 중단은 더 이상 단순한 IT 장애가 아니라 규제 리스크의 현실화입니다. 기업들은 AI 모델과 API에 대한 의존도, 접근 권한 구조, 대체 모델 전환 시나리오를 사전에 점검할 필요가 있습니다. AI 활용은 이제 기술 도입의 문제를 넘어 수출통제, 계약, 업무 연속성을 아우르는 사업 리스크 관리의 대상이 되고 있습니다.

특히 한국 기업들은 이번 사건을 미국 AI 기업에 대한 특수한 사례로만 볼 것이 아니라, 미국산 첨단 AI 모델에 대한 의존도와 글로벌 인력 운영 구조를 점검하는 계기로 삼을 필요가 있습니다. 한국에 본사를 두고 있더라도 해외 연구개발센터, 외국 국적 임직원, 글로벌 협력사 또는 해외 고객을 대상으로 미국 AI 모델을 활용하고 있는 경우에는 향후 유사한 접근 제한 조치의 영향을 직접 받을 수 있습니다. 반도체, 방산, 사이버보안, 바이오, 첨단제조 등 수출통제제도가

¹⁰ Anthropic PBC v. U.S. Department of War, et al. (링크); CNBC(2026.6.12). “Anthropic disables access to Fable 5 and Mythos 5 to comply with government directive”; Anthropic(2026.3.5). “Where things stand with the Department of War”; Lawfare(2026.3.9). “Anthropic Challenges the Pentagon’s Supply Chain Risk Determination”.

¹¹ Harvard Law Review(2026.6.26). “Is Access to Fable an Export?”

집중하고 있는 분야일수록 이러한 리스크는 더욱 커질 수 있습니다.

또한 기업들은 AI 모델의 성능이나 가격뿐 아니라 △특정 국가 또는 국적자에 대한 접근 제한 가능성, △서비스 중단 시 대체 모델 전환 가능성, △해외 계열사 및 외주인력의 사용 권한 구조, △공급계약상 책임 및 보상 조항, △수출통제 및 경제안보 규제 준수 의무 등을 함께 검토할 필요가 있습니다. 앞으로 AI 도입 전략은 정보보안이나 개인정보보호 차원을 넘어 수출통제, 경제안보, 공급망 관리 관점에서 함께 검토되어야 할 것으로 보입니다.

*

*

*

법무법인(유한) 태평양 수출입규제대응센터는 전략물자 및 해외수출통제(ITAR, EAR 등), 방산물자 및 국방과학기술(방위산업기술 포함) 수출통제, 국가핵심기술(NCT) 및 국가첨단전략기술(NHT), 국가안보심의 및 투자심사, 국내외 수출입규제 대응 컴플라이언스 시스템 구축 및 지원, 관세청 등 수사 및 조사 대응, 외환거래 및 대외투자 관리, 국제분쟁 및 조사대응 등 광범위한 영역을 아우르고 있습니다. 각 분야에서 풍부한 경험과 전문성을 갖춘 다수의 전문가들이 협업하여, 개별 고객의 상황과 필요에 최적화된 맞춤형 자문 서비스를 제공하고자 합니다.

관련 구성원

김지이나

변호사

T 02.3404.0698

E jeena.kim@bkl.co.kr

황호성

전문위원

T 02.3404.7488

E hosung.hwang@bkl.co.kr

유재규

변호사

T 02.3404.0842

E jaegyoo.yoo@bkl.co.kr

본 Legal Update는 본 법무법인의 이정민 통상전문 연구원이 함께 참여하였습니다.

법무법인(유한) 태평양의 뉴스레터에 게재된 내용 및 의견은 일반적인 정보제공만을 목적으로 발행된 것이며, 법무법인(유한) 태평양의 공식적인 견해나 어떤 구체적 사안에 대한 법률적 의견을 드리는 것이 아님을 알려드립니다. 뉴스레터와 관련된 문의사항이 있을 경우 위 연락처로 문의주시기 바랍니다.