

5 CSIS, 미국의 앤트로픽 AI 수출 통제 조치의 쟁점과 정책 대안 검토

➔ 미국 전략국제연구센터(CSIS)는 전문가 견해를 바탕으로 미국의 앤트로픽 AI 모델 수출 통제 조치의 법적 쟁점, 산업계의 영향, 정책적 대안 등을 검토해 제시^{*}(‘26.6)

* The Department of Commerce Restricted Access to Anthropic’s Latest Models. What Comes Next?

※ 본 고는 CSIS 내부 연구부서에 소속된 케이트 코렌(Kate Koren)과 케빈 커랜드(Kevin Kurland), 그리고 CSII 내에 자리한 와드와니 AI 센터(Wadhvani AI Center) 소장인 알록 메타(Aalok Mehta)의 견해를 CSIS가 인터뷰 형식으로 정리해 공개한 자료를 정리

● (수출 통제) ‘26년 6월 12일 미국 상무부는 앤트로픽의 첨단 AI 모델인 미토스5(Mythos 5)^{*} 및 페이블5(Fable 5)^{**}에 수출 통제를 부과

* 사이버보안 전문가 수준으로 매우 뛰어난 취약점 탐지 능력을 갖춘 고성능 AI 모델로, 사이버 공격에 악용될 경우에는 치명적인 위험을 초래

** 미토스5를 기반으로 하면서, 해킹이나 무기 제작 등 민감한 분야의 질문에 대해서는 응답을 제한하는 안전장치를 적용해 일반에 공개된 모델

- 수출 통제란 테러 지원국이나 적대국으로 군사적·전략적 가치가 있는 품목이 유입되는 것을 막기 위해 해당 기술이나 제품 수출 시 정부 허가를 받도록 한 규제로, 수출통제개혁법(ECRA)^{*}을 근거로 시행

* Export Control Reform Act: 국가안보와 외교 정책을 위해 첨단기술 및 이중용도 품목의 해외 이전을 통제하는 법률로, 상무부 산업안보국(BIS)이 수출관리규정(EAR)을 통해 집행

- 상무부는 앤트로픽의 고성능 AI 모델이 사이버 공격에 악용될 가능성을 우려해 수출 통제를 결정하고, 앤트로픽에 서한을 보내 이들 모델에 해외 이용자는 물론 내부 외국인 직원까지 접근을 제한하도록 명령

- 수출 통제를 통해 AI 모델에 외국인의 접근을 전면 제한한 것은 사상 최초이며, 물리적인 품목이 아닌 AI 모델 자체에 수출 통제가 적용된 것도 매우 이례적

- 이후 상무부는 앤트로픽으로부터 보안 강화에 대한 약속^{*}을 받고 18일 만에 수출 통제를 해제

* 앤트로픽은 모델의 보안 위험을 선제적으로 탐지해 대응하고, 정부와 배포 프로토콜·표준을 함께 마련하는 한편, 악성 활동(malicious activity)을 정부에 보고하기로 약속

● (권고사항) CSIS는 미토스5·페이블5 수출 통제 조치의 법적 근거가 불명확하다고 지적하고, 산업계의 영향과 정부에 대한 권고사항을 제시



1. BIS의 AI 모델 수출 통제 권한

- ECRA는 상무부에 EAR을 통해 군사용·이중용도·상업용인 물품·소프트웨어·기술의 수출, 재수출 및 간주수출*을 통제할 수 있는 권한을 부여
- * Deemed Export: 통제 대상 기술·소프트웨어를 자국 내에 있는 외국인에게 공개하거나 제공하는 것을 그 외국인의 모국으로 수출한 것으로 간주(Deemed)하는 제도
- 특정 기술·품목이 통제 대상에 포함되는 경우, 상무부가 관련 업체에 사전에 수출 허가가 필요하다는 사실을 통지할 수 있는 권한을 명시
- 다만 현재 사전 수출 허가 조치를 전 세계적으로 부과할 수 있는 권한은 대량 살상무기(WMD) 관련 활동이나 미국의 국가안보나 외교정책의 이익에 반하는 활동에 관여하는 당사자에 대한 수출 등으로 제한
- ※ 상무부는 '25년 1월 'AI 확산 규칙(AI diffusion rule)'을 발표하고 고성능 AI 모델 가중치를 수출 통제 대상에 포함시켰으나 현재는 미시행 상태

2. 외국인 접근 통제에 대한 BIS의 권한

- 상무부는 ECRA 상 신흥기술 및 기반기술에 대해 '잠정적으로 통제를 수립할 수 있는 권한'과 '특정인에게 수출 허가가 필요하다고 통지할 수 있는 권한'을 근거로 외국인이 엔트로픽의 AI 모델에 접근하는 것을 통제
- 다만, 잠정적 통제 수립 권한을 규정한 조항은 이전까지 수출 통제 부과 근거로 사용된 전례가 없으며, 이에 대응하는 구체적인 EAR 규제 체계 미비
- 또한 수출 통제의 근거로 EAR 제744.22조*도 언급했으나, 해당 조항은 소수 적대국을 대상으로 한 허가 요건만 허용하고 있을 뿐 전 세계적인 수출 통제는 비허용
- * 군사정보 최종 용도 및 최종 사용자(Military-intelligence end uses/users)에 대한 수출·재수출을 통제하는 조항
- 더욱이 외국인이 해외에서 원격으로 AI 모델에 접근하는 것이 EAR 적용 대상인 '수출'에 해당하는지 불명확

3. AI 모델 접근 통제에 대한 상무부 권한의 불확실성

- 일반 사용자들의 엔트로픽 AI 모델 접근을 EAR 상 소프트웨어·기술의 공개·이전으로 간주할 수 있는지 불분명
- 모델·가중치가 해외로 이전되는 것이 아니라, 외국인이 엔트로픽 서버에 원격으로 접속해 결과를 얻는 서비스 구조는 기존의 수출 개념으로 포섭이 불가
- 때문에 미국 의회에서는 원격접근보안법(RASA)*이라는 별개의 입법이 추진되어 '26년 1월 하원을 통과한 상황
- * Remote Access Security Act: 클라우드 컴퓨팅을 통해 해외 국가(우려 국가)의 사용자가 미국의 민감한 기술에 원격으로 접속하는 것을 통제하기 위한 법안

4. 미국인 통제 관련 상무부 권한의 불확실성

- 상무부는 미국인(개인·법인)이 관할권 밖에서 특정 첨단 기술이나 통제 대상 품목을 개발·생산하는 것을 금지할 수 있는 권한을 보유
- 엔트로픽이 미토스5·페이블5에 대한 접근을 허용하는 행위가 WMD·군사·정보 목적의 지원에 해당한다면 상무부의 통제 대상에 해당
- 그러나 EAR은 전 세계적으로 허가 요건을 부과할 수 있는 경우를 화학·생물 무기 관련 지원으로 한정하고 있으므로, 사이버 공격 우려를 이유로 모델 접근을 제한하는 것은 전 세계가 아닌 소수의 적대국에만 가능

5. 엔트로픽의 수출 통제 대응 방법

- 엔트로픽은 수출 통제를 해제하기 위해 상무부와 협의하거나, 조치의 적법성에 대한 소송을 제기하거나, 또는 모델에 접근하는 모든 사용자의 신원과 국적 확인을 수행하는 방식 등을 고려 가능

※ 엔트로픽과 상무부간 합의를 통해 '26년 6월 30일을 기준으로 수출 통제는 해제된 상태

6. AI 모델 수출 통제가 업계에 던지는 함의

- 이번 조치로 향후 BIS가 어떠한 법적 근거로, 어느 범위까지 모델 접근을 통제할 수 있는지에 대한 불확실성이 고조
- 이는 미국 AI 기업들의 글로벌 전략에 구조적 리스크를 더하고, 유럽이나 중국의 AI 모델 등 대체 옵션을 부각시키는 결과를 초래할 위험이 존재

7. AI 모델의 안보 우려를 해결하기 위한 대안적 경로(권고사항)

- 수출 통제는 AI 공급망의 특정 물리적 구성 요소, 특히 첨단 모델에 필요한 연산 능력에 대한 접근을 통제하는데 일정 효력을 발휘하지만, 국가안보 우려를 해결하는 데에는 부적합
- AI 모델 보안 우려를 해소하는 방안으로 첨단 AI 모델을 감독할 새로운 전담 기관 설립, AI 모델 개발에 대한 허가를 발급·거부·취소할 수 있는 허가제 운영 등을 제안
- 또한 AI 개발자들에게 중대 안전사고 보고 의무를 부여한 주(캘리포니아주, 뉴욕주 등)의 주(州)법들을 참고해 연방 차원의 입법을 추진 검토 필요

출처 : 미국 전략문제연구소(CSIS) (2026.6.16.)

<https://www.csis.org/analysis/departments-restricted-access-anthropics-latest-models-what-comes-next>