Marubeni Institute

2026年 6月 23日

AIは規制産業化するのか：曲がり角に差し掛かるAI開発競争

上席主任研究員　玉置 浩平

安全重視を標榜してきたアンソロピックに製品公開停止命令

米国政府は6月12日、輸出管理法令に基づき、米アンソロピックの最先端AI（人工知能）モデルへの外国人のアクセスを停止するよう命じた。対象は一部の企業や政府機関に限定的に提供されていた「Claude Mythos 5」とその一般公開版である「Claude Fable 5」であり、いずれも停止命令の3日前に公開されたばかりだった。アンソロピックは4月、ソフトウェアの脆弱性を発見する能力が極めて高い最先端モデル「Claude Mythos Preview」を限定的に提供するプログラムを開始しており、「Mythos 5」は「Mythos Preview」の後継とされていた。

アンソロピックはOpenAIの研究チームのメンバーらが、同社の方針やAIの安全性に関する懸念を抱いて独立・創業したとされる。それだけにアンソロピックは安全性の重視を経営理念として掲げ、性急な開発を戒めるメッセージを発信するなど、業界の「良心」として振る舞ってきた。そのアンソロピックが政府から製品の安全性に疑義を呈され、公開停止を命じられたのは皮肉とも言える。

最先端モデルが直面する規制リスクと政策的ジレンマ

今般、異例の措置が講じられたのは、「Fable 5」に一定のプロンプトを入力することでサイバー攻撃に悪用可能な出力が得られることが判明したためだという。このようにAIモデルに組み込まれた安全対策などを回避する手法は脱獄（ジェイルブレイク）と呼ばれる。これに対しアンソロピックは、完全な脱獄対策は不可能としつつ、当局が問題としている脱獄の影響は限定的だと説明している。同社は命令遵守のために米国人を含む全顧客のアクセスを停止したが、外国人を対象とする輸出管理法令が適用されたのは規制の不在による窮余の策という面もありそうだ。

もともとアンソロピックはトランプ政権とのトラブルを抱えていた。アンソロピックは昨年7月に米国防省と機密ネットワークにAIを導入する契約を交わしたが、国防省があらゆる合法的な目的のためにAIを使用する方針を示したのに対し、同社は大規模な国内監視と完全自律型兵器に自社製品を使わないよう求めた。不満を募らせた政府側は今年2月、連邦政府機関に対して同社の技術を使用しないよう命じるとともに、同社を「サプライチェーンリスク」に指定し、政府調達に関連した同社製品の使用を禁じた。こうした経緯が政府とのコミュニケーションを複雑化させた可能性もある。

それでも、AIの急速な性能向上により、安全性や悪用に対する懸念が高まっていることは事実だ。トランプ政権は親ビジネスの立場からAI規制には消極的な姿勢を見せてきたが、6月2日には企業の自主的な協力に基づき最先端モデルの安全性を事前審査する枠組みを創設する大統領令を発出している。既に欧州連合（EU）は包括的なAI規制を導入しているが、各国でも規制強化の議論が改めて活発化することは確実だろう。当局審査の長期化による開発プロセスの停滞や最先端モデルの安全対策の厳格化によるパフォーマンス低下は、各社にとって大きな負担となり得る。

一方、AIに対する懸念が開発競争を加速させる面もある。対立国に先んじて高性能モデルを開発し、自国のネットワークの脆弱性を特定して対策を講じなければ、深刻な安全保障上の脅威を抱えることになってしまうからだ。また、過度な規制がAI投資ブームを腰折れさせるリスクも意識されるだろう。各国はこうしたジレンマの中で開発と規制のバランスを模索していくことになろう。

折しもアンソロピックは6月1日、IPO（新規株式公開）申請資料を提出したばかりであり、8日にはOpenAIも続いた。巨額の資金調達を控える中で、各社が規制環境の複雑化をどのように戦略に織り込んでいくかが問われることになる。

AIの規制産業化がもたらす構造変化

米国が突如として最先端モデルへのアクセスを遮断したことで、AI技術の対外依存のリスクが改めて認識され、各国が独自にAIを開発・運用する「ソブリンAI」の動きは加速するだろう。ただ、米国との格差は大きく、当面は特定モデルへの依存を回避することに重点が置かれよう。

また、最先端のクローズドモデルに対する管理が強まることで、オープンモデルの活用がさらに進むことも考えられる。オープンモデルはAI導入コストの高騰が指摘される中で価格面でも優位性がある。非米国企業のプレゼンスが強いため、米国依存の緩和という意味でも好都合だ。

しかし、オープンモデルの性能向上に伴い、悪用リスクも高まることになる。開発者がアクセスを管理できるクローズドモデルに対し、オープンモデルは誰でも自由に入手できてしまう。モデルのパラメータが悪意をもって改変されることで、安全対策が無効化されるおそれもある。オープンモデルのエコシステムに規制の波が及ぶ可能性にも留意すべきだろう。

（執筆者プロフィール）

玉置 浩平（Kohei Tamaoki）
TAMAOKI-K@marubeni.com
上席主任研究員
研究分野：地政学リスク、経済安全保障、産業・通商政策
外務省入省後、朝鮮半島、宇宙・海洋安全保障などに関する外交政策の企画・立案に従事。2021年から丸紅経済研究所にて国際政治経済に関する調査分析を担当。企業の地政学リスク管理の在り方についても研究を行う。
東京大学法学部卒業、タフツ大学フレッチャースクールLL.M.修了（国際法学修士）。

株式会社丸紅経済研究所
〒100-8088　東京都千代田区大手町一丁目4番2号
https://www.marubeni.com/jp/research/