

調査報告書

中国 AI の躍進と「ミュトス空白」

日経報道の事実確認と、日本が採るべき国家・企業・知財ガバナンス戦略

2026 年 7 月 7 日 / Claude Fable 5

要旨

- 日経報道は事実として裏付けられる。2026 年 6 月、米政府の輸出規制命令で Anthropic が最先端モデル「Mythos 5/Fable 5」を全世界で一時的に停止した空白期に、中国製オープンウェイトモデル（GLM・Kimi・DeepSeek・Qwen 等）へ乗り換える米企業が続出した。料金は米フロンティアモデルの実質 10～100 分の 1 で、見出しの「20 分の 1」は複数の一次データと整合する。^{1,2}
- 躍進の本質は「性能逆転」ではなく「価格破壊×オープンウェイト×デファクト化」。OpenRouter での中国モデルのトークンシェアは 2024 年末の約 1.2%から 2026 年 6 月に約 61%へ急伸した。一方、汎用推論の性能は依然として米クローズド最先端が数ポイント上位で、収益シェアは米国勢が握る「二層市場」が形成されている。^{3,4}
- 日本の採るべき道は三層で明確。①国家戦略＝フィジカル AI・製造業データの主権確保に集中投資、②企業戦略＝マルチモデル＋用途別ルーティング（中国モデルはオンプレ自己ホスト前提）、③知財・データガバナンス＝中国データ三法・国家情報法の域外適用を前提とした調達チェックの徹底。^{5,6}

1 報道の特定と事実確認

問題の記事は、日本経済新聞 2026 年 7 月 6 日付「中国 AI がミュトスいぬ間に躍進 料金は 20 分の 1、米企業も乗り換え」である。「ミュトス」は Anthropic の最先端 AI「Claude Mythos 5」の日本語表記を指す。記事は、米 Anthropic が米政府の指示で先端 AI「ミュトス」の提供を停止していた間に、中国 AI へ乗り換える米企業が増えたと報じ、中国企業の AI は誰でも使える「オープン型」で料金はミュトスの 20 分の 1 だと記述する。冒頭事例として、暗号資産交換大手・米コインベースのブライアン・アームストロング CEO が 6 月末に AI 利用コストを半減できたと発言したことを挙げている。^{1,7}

結論として、報道の核心（「ミュトス停止」「20 分の 1」「米企業の乗り換え」）はいずれも一

次情報・複数の信頼できる二次情報で裏付けられる。ただし見出しの「20 分の 1」は最も高価な西側フラッグシップとの比較値であり、モデルや用途によって 10~100 倍と幅がある点に留意を要する。²

2 「ミュトス／フェーブル」停止事件の実像

- 2026 年 6 月 12 日、Anthropic は Mythos ベースの一般向け最先端モデル「Fable 5」と、より強力な「Mythos 5」を公開した。⁸
- 同日夕方、米商務長官が国家安全保障を根拠に、両モデルへの「あらゆる外国人（自社の外国籍従業員を含む）」のアクセス停止を指示。Anthropic は国籍確認が不可能なため、全世界の全ユーザーに対し両モデルを即時停止した。⁸
- 引き金は、Fable 5 の安全ガードレールを回避し Mythos の高度なサイバー能力を引き出す「ジェイルブレイク」手法の報告であった。Anthropic は「極めて限定的な脆弱性で、他社モデルでも同様に発見可能」と反論した。⁸
- 6 月 30 日に商務省が輸出規制を解除、7 月 1~2 日に Fable 5 が一般再開。停止は約 18 日間に及んだ。⁸

この事件は、中国勢に「キルスイッチのない安心」という強力なマーケティング材料を与えた。GLM 5.2 は Fable/Mythos 停止の翌日に MIT ライセンスで公開され、「輸出規制で突然使えなくなるクローズドモデル」との対比を鮮明にした。事業継続性を重視する組織にとって、オープンウェイトの魅力は価格を超えて高まっている。³

3 中国製モデルへの乗り換え実例

- **コインベース**：CEO が 2026 年 6 月末、社内 LLM ゲートウェイの既定モデルを Zhipu (Z.ai) の GLM 5.2 と Moonshot AI の Kimi K2.7 Code に切替え、AI 支出を「ほぼ半減」しつつトークン使用量は増加と公表。キャッシュヒット率を 5%→60%（12 倍）に改善した。¹
- **Snowflake**：CEO が 103 のコーディングタスクで実地比較し、GLM 5.2 が 66%、Claude Opus 4.7 が 67%を解決という僅差の結果を示した。²
- **Lindy**（25 人の AI スタートアップ）：2026 年 6 月にトラフィックの 100%を Claude から DeepSeek へ移行。CEO は「コストカーブが地面に叩きつけられるように急落した」と語り、数ヶ月で数百万ドルの節約を見込むとした。²

[留意] 「米スタートアップの 80%が中国製モデルを使用」との一部報道は誇張である。a16z

の Martin Casado 本人が「オープンソース利用は 2～3 割、そのうち 8 割が中国製＝実質 16～24%」と訂正しており、実勢は 2 割前後と読むべきである。^{4}

4 トークンシェアと価格の一次データ

中国製オープンウェイトモデルの OpenRouter でのトークンシェアは、**2024 年末の約 1.2% → 2026 年 2 月に初めて米国モデルを逆転 → 2026 年 6 月に約 61% へと急伸した**。ただしこの「61%」はトップ 10 モデル内・特定週のスナップショットであり、全プラットフォーム総量では西側プロプライエタリが依然多数を占める。コーディング／エージェント用途に中国モデルが偏在していることがシェアを押し上げている。^{3,4}

■ 主要モデルの価格比較（2026 年 5～6 月、百万トークンあたり）

モデル	入力／出力	ライセンス	対フラッグシップ
DeepSeek V4-Flash	\$0.14 / \$0.28	MIT	約 35～100 倍安
GLM 5.2	約\$1.40 / \$4.40	MIT	約 5 倍安
Claude Opus 4.8	\$5 / \$25	クローズド	—（基準）
GPT-5.5	\$5 / \$30	クローズド	—（基準）

※定価ベース。プロモーション価格や西側ホスト経由では 2～10 倍の差が生じる。

見出しの「20 分の 1」は、高価格帯フラッグシップ（\$15/\$75 相当）や出力トークンとの比較では十分に成立する。OpenRouter の担当者は CNBC（2026 年 7 月 7 日）で「オープンソースの中国モデルは米最上位機より 60～90% 安い」と述べており、実用主力で約 5 倍安、最安モデルで数十倍安というのが実態に近い。²

5 性能ベンチマーク比較

Artificial Analysis Intelligence Index 等（2026 年 6 月）では、クローズド最先端は **Claude Opus 4.8=61.4**、**GPT-5.5=60.2**。オープンウェイト最強は **GLM 5.2=51** で、ダウンロード可能モデルとして史上初めてフロンティア圏内に入った。コーディング（SWE-bench Pro）では GLM 5.2 が GPT-5.5 を上回るなど特定タスクで逆転が見られる一方、SWE-bench Verified は Claude Opus 4.8 が優位を保つ。²

総括すれば、汎用推論では西側クローズドが 3～8 ポイントのリードを維持し、コーディング／エージェント用途では実質互角～一部逆転という構図である。「知能はコモディティ化し、フロンティアは機能になった」と言える。²

6 中国躍進の構造要因

- **オープンウェイト戦略**：DeepSeek R1（2025 年 1 月）以降、Qwen・Kimi・GLM 等が MIT／Apache 2.0 で相次ぎ公開。国务院の「AI+」行動計画（2025 年 7 月 31 日承認）がオープンソースモデルの階層別目標と資金メカニズムを規定し、政策と一致している。世界の新規派生オープンモデルの約 70%が Qwen ベースとされる。^{9,10}
- **価格破壊の技術的背景**：MoE（Mixture-of-Experts）による推論効率化（V4-Pro は 1.6 兆パラメータ中 49B のみ活性化）、蒸留、国家による API 利用・ライセンス購入補助。米国の半導体輸出規制がむしろ「少ない計算資源で多くを実現する」効率化を促した。³
- **蒸留疑惑**：Anthropic・OpenAI は 2026 年 2 月、中国勢が不正アカウントで Claude 等を蒸留したと主張。ただし係争中で独立には証明されていない。⁸
- **半導体**：Huawei Ascend が国産化の中核。ただし学習は依然 NVIDIA 依存で、Ascend は主に推論用途にとどまる。³

7 各国政府・日本の対応

■ 米国

下院の関連委員会は 2026 年 4 月 29 日、DeepSeek・Alibaba・Moonshot・MiniMax を名指しした合同調査を開始した。NIST の AI 安全機関（CAISI）は、DeepSeek ベースのエージェントが米フロンティアモデルより平均 12 倍、悪意ある指示に従いやすいと計測している。米・台・韓・伊・豪では政府端末での DeepSeek 利用が禁止された。^{11,12}

■ 日本政府

個人情報保護委員会は 2025 年 2 月、「DeepSeek に関する情報提供」を公表し、取得データが中国国内サーバに保存され中国の法令（個人情報保護法・データセキュリティ法・国家情報法等）が適用されると明記した。デジタル社会推進会議幹事会も同月、業務利用に関する注意喚起を发出し、要機密情報の取扱い禁止を再確認した。^{13,14}

政府生成 AI 基盤「源内」は、2026 年 3 月に国産 7 モデル（NTT tsuzumi、NEC cotomi、富士通 Takane、PFN PLaMo、KDDI／ELYZA 等）を選定。ガバメントクラウド推論環境で機密性 2 情報を扱う要件により、中国製モデルは構造的に排除される設計である。⁵

■ 日本企業

日経の報道（2026 年 6 月）によれば、日本企業の主要独自モデルの約 6 割が DeepSeek または Qwen の二次開発である。みずほ FG は Qwen3 ベースの金融特化 LLM を発表（セキュアなオンプレ環境）。一方でソフトバンクグループは DeepSeek の社内利用を禁止するなど、対応は分かれている。⁶

[分析] この「二次開発 6 割」は諸刃の剣である。割安で高性能な基盤にアクセスできる一方、①中国モデルへ依存したエコシステム、②ライセンス変更・供給停止リスク、③知財・データの不透明性を抱え込む。オンプレ運用であれば当面のデータ流出リスクは遮断できるが、根本的な依存構造は残る。{6}

8 知財・データガバナンスの論点

- **中国データ三法の域外適用**：データセキュリティ法は中国国外の処理活動でも中国の国家安全・公共利益を害する場合に適用され、当局認可なしに外国司法機関へ国内データを提供することを禁止する。個人情報保護法も中国国内の自然人への商品・サービス提供等で域外適用され、違反時は最大 5,000 万元または前年売上 5% の罰金が科される。^{15,16}
- **オープンウェイトのライセンス論点**：GLM・DeepSeek は MIT、Kimi・Qwen は Apache 2.0。自己ホスト（オンプレ）であれば中国 API へのデータ送信リスクは遮断できるが、学習データの権利処理の不透明性、生成物の権利、悪意あるコード混入、重みに埋め込まれた検閲・バイアスは残る。¹³
- **AI 事業者ガイドライン**：学習データ・生成物に個人情報・知的財産権・機密情報が含まれる点、準拠法（モデル所在地・学習サーバ所在地）に応じた適合的取扱いが必要と明記されている。なお第 1.2 版は RAG を「学習」ではなく「推論」と整理した。¹⁷

9 提言：三層構造で日本はどうすべきか

■ 第 1 層 国家 AI 戦略

- **LLM 規模競争からフィジカル AI への選択と集中（即時）**。GENIAC とノエトラ（Noetra）を軸に、製造業データの AI-Ready 化・ロボット基盤モデルへ資源を集中する。2027 年までに国産フィジカル AI 基盤モデルを、日本企業で一般的なオープンモデルと同程度の基本性能に到達させる。¹⁸

- **製造業データの主権確保**（1 年以内）。海外プラットフォームに依存しない国内データ精製・組織横断連携基盤を整備し、営業秘密流出リスク対応を組み込む。日本の真の勝ち筋は、匠の知恵を海外勢に奪われる前にデータ精製技術を確立することにある。¹⁹
- **計算資源の持続的確保**（継続）。GPU 支援終了後に自力で計算基盤を維持できるスタートアップがほぼ皆無という現実を直視し、国家計算基盤を継続提供する。¹⁸
- **経済安保との整合**（継続）。経済安全保障推進法の見直しで重要データの保存・処理先規律を明確化し、政府調達では源内方式（国産モデル+ガバメントクラウド+機密性 2 要件）を維持・拡大する。²⁰

■ 第 2 層 企業の AI 調達・活用戦略

- **マルチモデル+用途別ルーティングを標準化**（即時）。既定は安価モデル、複雑タスクのみフロンティアにエスカレーション、積極キャッシュというコインベース方式を範とする（キャッシュヒット率 60%以上を目標）。¹
- **中国モデルは「オンプレ自己ホスト」を絶対条件に**（即時）。中国 API へのデータ送信は原則禁止。MIT/Apache 2.0 のオープンウェイトを国内ホスティング/オンプレで運用すればデータ流出リスクは遮断できる。機密情報・行政情報は国産 LLM を国内完結で運用する。¹³
- **タスク別の適材適所**（即時）。汎用推論・多言語は Claude/GPT/Gemini、高ボリュームのコーディング・要約はオンプレの中国製オープンウェイト、日本語業務文書・契約文言は国産 LLM、と使い分ける。²

■ 第 3 層 知財・データガバナンス

- **AI 調達チェックリストの整備**（即時）。①提供元の国・準拠法、②データ保存先と再学習利用の有無、③ライセンス条項、④学習データの権利処理の開示、⑤生成物の権利帰属、⑥重みへの悪意あるコード・バイアス検証、を確認項目とする。¹⁷
- **中国データ三法・国家情報法の域外適用を前提とした社内規程**（3 ヶ月以内）。中国 API 利用時は機密情報・営業秘密・技術情報の入力を禁止し、個人情報保護委員会の「情報提供」を社内リスク評価の基準に採用する。^{13,15}
- **契約・調達実務**（継続）。ベンダー契約でデータの所在・送信先・保存期間・再学習利用・準拠法・紛争解決を明記。CAIO（AI 統括責任者）を設置しサプライチェーンリスクを一元管理する。¹⁷

- **リスク評価フレームワーク（継続）**。NIST AI RMF・AI 事業者ガイドライン第 1.2 版に基づき、モデルの出自・データフロー・準拠法・事業継続性（キルスイッチリスク）を定期評価する。^{12,17}

10 留意事項（Caveats）

- **「61%」シェアの解釈**：トップ 10 内・特定週のスナップショットであり、全世界 API 総量では西側プロプライエタリが依然多数。直近 12 ヶ月平均は約 11%との報道もあり、瞬間最大風速と平均を区別すべきである。³
- **ベンチマークの限界**：SWE-bench 等はスキャフォールド依存で、自己申告値と独立検証値が混在する。学習データ汚染の懸念も指摘されている。²
- **企業事例の出所**：一部の DeepSeek 禁止事例は二次情報が主で、一次の企業発表は未確認のものがある。みずほの性能同値は「推論なし+コンテキスト付与あり」の条件限定値である。⁶
- **将来予測の扱い**：米ラボの価格戦争、IPO 動向、中国半導体の学習用途拡大、蒸留疑惑の帰趨などは進行中の動向であり、確定した結果ではない。⁸

参考文献

1. **日本経済新聞** 「中国 AI がミュトスいぬ間に躍進 料金は 20 分の 1、米企業も乗り換え」 2026 年 7 月 6 日。コインベース (B. Armstrong CEO) の AI 費用半減・既定モデル切替に関する記述を含む。
2. **CNBC** 中国製オープンソースモデルの価格優位 (米最上位機比 60~90% 安、OpenRouter J. Summerville 発言) および Lindy (F. Crivello CEO) の DeepSeek 全面移行に関する報道、2026 年 7 月。
3. **Bloomberg/Exponential View/Crypto Briefing** OpenRouter における中国製オープンウェイトモデルのトークンシェア推移 (2024 年末約 1.2%→2026 年 2 月に米国モデルを逆転→2026 年 6 月約 61%) に関する分析。
4. **a16z/OpenRouter** 100 兆トークン規模の利用調査、および M. Casado による「オープンソース利用は 2~3 割、うち 8 割が中国製=実質 16~24%」との訂正 (X, 2025 年 11 月)。
5. **デジタルレクラーメ株式会社** 「デジタル庁がガバメント AI『源内』で国産 LLM7 件を選定——全府省庁 18 万人へ展開」 2026 年。 <https://www.digital-reclame.co.jp/blog/digital-agency-gennai-llm-7-2026/>
6. **日経デジタルガバナンス** 日本企業の主要独自モデルの約 6 割が DeepSeek/Qwen の二次開発である旨の報道、およびみずほ FG・ソフトバンクグループ等の対応、2026 年 6 月 3 日。
7. **Anthropic 公式声明ほか** Claude Mythos 5/Fable 5 の公開 (2026 年 6 月) と米商務省の輸出規制に基づく一時停止・再開 (6 月 12 日~7 月 2 日) の経緯に関する一次情報。
8. **Anthropic 公式声明ほか (前掲)** ジェイルブレイク報告を引き金とする停止判断、および蒸留疑惑 (Anthropic・OpenAI の主張、2026 年 2 月) に関する記述。
9. **中華人民共和国国務院** 「AI+」行動計画 (人工知能+行動計画、2025 年 7 月 31 日承認)。オープンソースモデルの階層別目標と資金メカニズムを規定。
10. **Artificial Analysis/ATOM プロジェクト** Intelligence Index (2026 年 6 月: Claude Opus 4.8=61.4、GPT-5.5=60.2、GLM 5.2=51)、および世界の新規派生オープンモデルの約 70% が Qwen ベースとの調査。
11. **米下院国土安全保障委員会・対中特別委員会** DeepSeek・Alibaba・Moonshot・MiniMax を対象とする合同調査の開始 (2026 年 4 月 29 日)。
12. **NIST CAISI/CNAS** DeepSeek ベースのエージェントが米フロンティアモデルより平均 12 倍悪意ある指示に従いやすいとする評価 (2025 年 9 月 30 日)、および CNAS 「Red Lines」報告。
13. **個人情報保護委員会** 「DeepSeek に関する情報提供」 (2025 年 2 月 3 日公表、3 月 5 日更新)。取得データの中国国内サーバ保存と中国法令 (個人情報保護法・データセキュリティ法・国家情報法等) の適用を明記。 https://www.ppc.go.jp/enforcement/infoprovision/laws/offshore_report_china/
14. **デジタル社会推進会議幹事会** 「DeepSeek 等の生成 AI の業務利用に関する注意喚起」 (2025 年 2 月 6 日)。要機密情報の取扱い禁止、NISC・デジタル庁への事前相談を規定。
15. **中華人民共和国** データセキュリティ法 (第 2 条・第 36 条: 域外適用および外国司法機関へのデータ提供制限)。

16. **中華人民共和国** 個人情報保護法（第 3 条：域外適用。違反時は最大 5,000 万元または前年売上 5% の罰金）。
17. **経済産業省・総務省** AI 事業者ガイドライン（第 1.2 版、2026 年 3 月 31 日）。準拠法に応じた適合的取扱 い 、 RAG を 推 論 と 整 理 。
https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20260331_1.pdf
18. **経済産業省ほか** GENIAC（第 4 期採択）、AI ロボティクス戦略、および国家計算基盤・国産フィジカル AI 基盤モデルの整備方針（2026 年）。
19. **日本経済新聞** 「国産 AI、カギ握るデータ精製技術 守れるか現場データ」。製造業の現場データ精製・主権確保に関する報道。<https://www.nikkei.com/nkd/company/article/>
20. **内閣官房・経済安全保障法制** 経済安全保障推進法（令和 4 年法律第 43 号）および重要経済安保情報保護活用法（令和 6 年法律第 27 号、2025 年 5 月全面施行）。重要データの保存・処理先規律の検討。