

2026年グローバルAI覇権のパラダイムシフト と日本の国家戦略：米中価格競争の深層と 「フィジカルAI」への戦略的ピボット

Gemini 3.1 pro

1. 序論：2026年7月、生成AI市場における歴史的地殻変動と 新たな競争原理

2026年7月現在、世界の人工知能(AI)産業は、その発展の軌跡においてかつてないほどの技術的、経済的、そして地政学的な転換点を迎えている。これまで生成AIおよびフロンティアAIモデルの市場は、OpenAIやAnthropicといった米国の少数の先端テクノロジー企業によって圧倒的な支配を受けてきた。しかし、ここ数週間の間に発生した二つの連動する重大事象により、この一極集中の構造は根底から揺るがされている。

第一の事象は、国家安全保障を理由とした米国政府による最先端AIモデルの輸出管理および提供停止措置である。米国の最高峰AIが「兵器」に準ずる扱いを受け、特定の外国籍市民や海外企業からのアクセスが突如として遮断された¹。第二の事象は、その政治的空白(間隙)を縫うようにして台頭した中国製AIモデルの驚異的な性能向上と、それに伴う劇的な価格破壊である³。日経新聞が「料金は20分の1」と報じたように、中国のオープンウェイトモデルは米国のクローズドモデルと同等の知能水準を達成しつつ、極限まで最適化されたアーキテクチャにより運用コストを劇的に引き下げた³。この結果、単なるコスト競争にとどまらない地殻変動が起きている。米国最大の暗号資産取引所であるCoinbaseをはじめ、LindyやSnowflakeといった米国の名立たる先端テクノロジー企業群が、自社のインフラストラクチャを支える基盤モデルとして、米国製モデルから中国のZhipu AI(GLM 5.2)やMoonshot AI(Kimi 2.7)、DeepSeek(V4)へと次々に乗り換えている事実である⁵。これは、イデオロギーや国家間の分断を超越した「資本の論理」と「トークンエコノミーの最適化」が、企業のAI選定基準の最上位に位置付けられたことを意味する。

本報告書は、「ミュトス(Mythos)いぬ間に」急成長を遂げた中国AI市場のメカニズムと、激化するソフトウェア領域でのLLM(大規模言語モデル)消耗戦を網羅的かつ多角的に分析する。その上で、米国製AIの供給不安定化リスクと中国製AIの価格攻勢に挟まれた日本が、国家主権と経済安全保障を維持しながらグローバル競争で優位に立つための戦略として、「フィジカルAI(物理的AI)」への注力と自律的データエコシステムの構築に向けた具体的な提言を行う。

2. 米国「ミュトス」規制の深層：国家安全保障とフロンティアAI のジレンマ

事の発端は、2026年6月9日に米Anthropic社が一般公開した最先端AIモデル「Claude Mythos 5」および「Claude Fable 5」に対する、米国政府からの異例の提供停止命令である¹。この一連の出来事は、AI技術がもはや単なるソフトウェア・サービスではなく、国家のサイバー防衛と安全保障の根幹を成す「戦略的インフラ」へと変貌したことを世界に強く印象付けた。

2.1. Project Glasswingと高度なサイバーセキュリティ能力

Claude Mythosは、元来ソフトウェアの脆弱性発見や高度な自律的推論において極めて高い能力を有するように設計されている。Anthropic社は「Project Glasswing」と称する大規模なイニシアチブを通じて、AWS、Apple、Microsoft、NVIDIA、Cisco、CrowdStrikeなど約50の重要パートナー企業とともに、世界で最もシステムの重要なソフトウェアにおける1万件以上の深刻な(High- or Critical-severity)脆弱性をMythosのプレビュー版を用いて発見してきた実績がある⁸。

この卓越したコード解析能力と自律的なエージェント推論能力は、サイバー防衛の観点からは極めて有用である一方、攻撃者に渡れば壊滅的なサイバーテロを引き起こす「諸刃の剣」であった。米国政府(特に商務省および国防総省)は、Mythos 5およびFable 5が敵対的外国勢力やサイバー犯罪者によって悪用され、米国の重要インフラが攻撃に晒されるリスクを極めて重く見た²。

2.2. 前例のない輸出管理と世界的な「ブラックアウト」

2026年6月中旬、米国政府は安全保障上の懸念からこれらのモデルを輸出管理の対象に指定し、外国人(日本企業を含む)によるアクセスを直ちに停止するようAnthropicに命じた¹。これにより、Anthropicは全世界での提供を一時停止するという前代未聞の事態に追い込まれた¹⁰。

この措置の衝撃は、単に特定のAIツールが使えなくなったという表面的な不便にとどまらない。グローバル企業にとっては、「自社の業務プロセスやプロダクトの中核に据えている米国のフロンティアAIモデルが、米国政府の一存で即日利用不可になる」という、極めて現実的かつ深刻なサプライチェーン・リスク(ベンダーロックインのリスク)が顕在化した瞬間であった。同社は数億人に提供されている商用モデルの回収判断に反発を示し、政府との対立が表面化した⁹が、最終的には政府の規制に従わざるを得なかった⁹。

2.3. 政府機関による特権的利用と供給不安の露呈

この規制措置の裏で展開されたもう一つの現実は、米国政府内の「ダブルスタンダード」である。一般社会や同盟国の企業への提供が厳格に制限された一方で、米国のサイバーセキュリティ・インフラセキュリティ庁(CISA)や国家安全保障局(NSA)といった中枢の政府機関は、Mythosを積極的に活用し続けていた。CISAのAttack Surface Evaluationチームは、外国の諜報機関に悪用される可能性のある脆弱性を特定するため、政府のコードリポジトリの監査にMythosをいち早く導入している¹¹。これは、AIスタートアップに対するホワイトハウスの厳しい姿勢とは裏腹に、実務レベルのサイバー防衛機関がこれらツールの導入を政治的に後押ししているという複雑な内部構図を示している。その後、約2週間の「ブラックアウト」を経た6月下旬から7月1日にかけて、Anthropicはハワード・ラトニック米商務長官らとの間で厳密なプロトコルの調整を行い、セキュリティリスクの事後的検出や悪意ある活動の政府への報告を条件に、一部の信頼された米国内組織や、安全対策(ガードレール)が施されたFable 5について段階的にアクセスを回復させた²。しかし、この2週間の供給不安が、後述する中国製AIの躍進に対する最大の「隙」を生むこととなったのである⁴。

3. 中国AIの飛躍的進化と価格破壊:アーキテクチャ革命のメカニズム

米国製の最高峰AIが政府の規制と安全保障の網の目に絡めとられ、停滞を余儀なくされている間、中国のAI開発企業は猛烈な勢いで技術的キャッチアップとアーキテクチャの革新を推し進めていた。特筆すべきは、これらのモデルが単に安価であるだけでなく、プログラミングや複雑なエージェントタ

スクにおいて、米国のクローズドモデルに肉薄、あるいは凌駕する性能を達成した点にある。

3.1. ソフトウェアエンジニアリングにおける中国モデルの台頭

中国企業のAIは、誰もが基盤のパラメーターにアクセスできる「オープンウェイト型」を中心にエコシステムを拡大している。このオープン性が、世界中の開発者コミュニティからのフィードバックループを加速させている。

Zhipu AIが開発した「GLM 5.2」は、プログラミング能力を測定する代表的なベンチマークである「SWE-bench Pro」において62.1という驚異的なスコアを記録し、業界標準と目されていたOpenAIの「GPT-5.5」(スコア58.6)を明確に打ち破った⁵。また、Moonshot AIが開発した「Kimi K2.7 Code」は、1兆パラメーターを持つMoE(Mixture-of-Experts: 専門家混合)アーキテクチャを採用し、複雑なプログラミングタスクや自律型エージェントのワークフローに特化している。Kimi K2.7 Codeは、実世界の5つの環境(Notion、GitHub、ファイルシステム、Postgres、Playwrightブラウザ自動化)を横断してエージェントの能力を評価するMCPMark Verifiedにおいて81.1を記録し、AnthropicのClaude Opus 4.8(76.4)を上回る結果を出している⁶。このKimi K2.7は、Cursorなどのグローバルなソフトウェア開発ツールにおいても基盤モデルとして採用されており、実務レベルでの普及が急速に進んでいる。

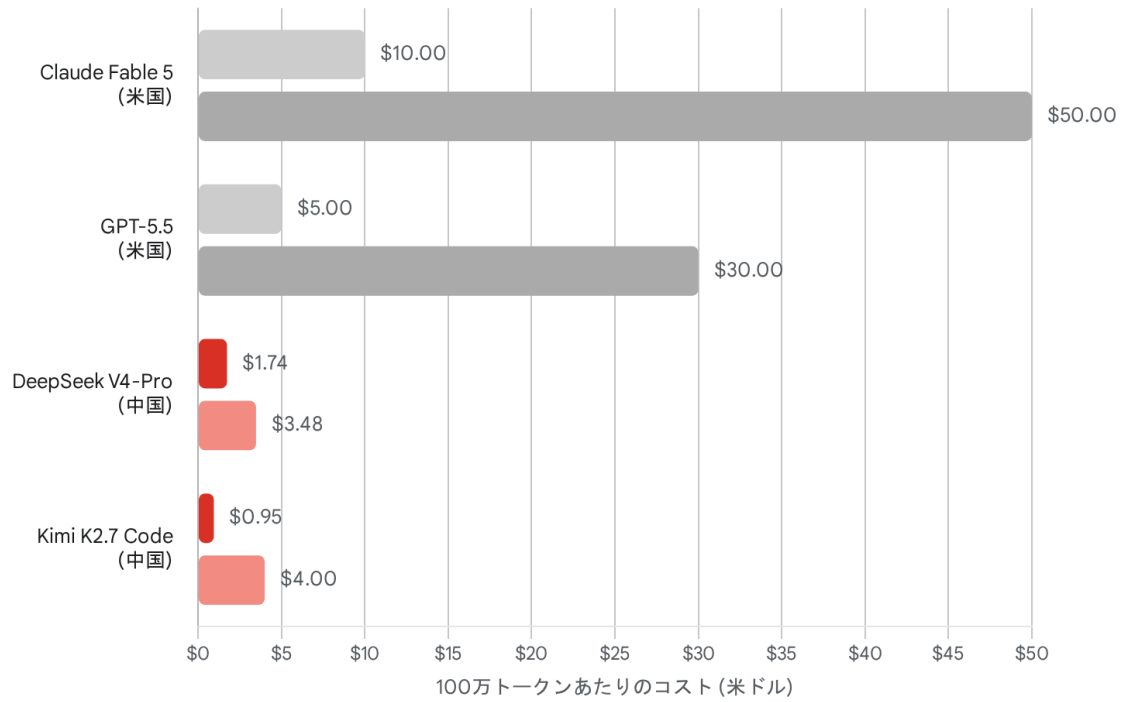
3.2. DeepSeek V4による計算効率の極限化と価格破壊

こうした性能向上以上に市場に衝撃を与えたのが、中国DeepSeekが公開した「DeepSeek V4」シリーズによるアーキテクチャの抜本的革新と、それに伴う「価格破壊」である。

DeepSeek V4-Proは、1兆6000億の総パラメーターを持ちながら、推論時にアクティブになるパラメーターを490億に抑えたMoEモデルである。このV4アーキテクチャの最大の技術的ブレイクスルーは、トークン圧縮技術と独自のスパースアテンション(疎な注意機構)を融合させた「ハイブリッドアテンション機構」の実装にある。これにより、100万トークンという長大なコンテキストを処理する際、前世代のV3.2と比較して計算量(FLOPs)をわずか27%、KVキャッシュ(コンテキストを保持するためのメモリ)を10%にまで劇的に削減することに成功した⁶。さらに、V4-Flashに至ってはFLOPsを10%、KVキャッシュを7%まで削減している。

この計算効率の極限までの最適化は、そのままAPI提供価格の破壊的低下に直結している。

圧倒的なコスト優位性を示す中国製AIモデルのトークン単価比較



各AIモデルにおける100万トークンあたりのAPI利用料金（米ドル）。中国製モデル（赤系）は、計算効率の最適化により、同等クラスの米国製フロンティアモデル（青系）と比較して極めて安価な水準で提供されている。

データソース: The Decoder, Yahoo!リアルタイム検索, 日本経済新聞

以下の表は、主要な日米中のフロンティアモデルに関する100万トークンあたりのAPI提供価格の比較である。

モデル名	開発企業 (国籍)	100万入力トークン価格	100万出力トークン価格	備考・技術的特長
Claude Fable 5	Anthropic (米国)	\$10.00	\$50.00	Mythosベースの高度なサイ

				バーセキュリティ・生物学向け保護モデル ⁶
GPT-5.5	OpenAI (米国)	\$5.00	\$30.00	業界標準のフロンティアモデル ⁶
Claude Opus 4.8	Anthropic (米国)	\$5.00	\$25.00	前世代の強力な汎用推論モデル ⁶
DeepSeek V4-Pro	DeepSeek (中国)	\$1.74	\$3.48	1.6兆パラメーター、MoE、ハイブリッドアテンション ⁶
Kimi K2.7 Code	Moonshot AI (中国)	\$0.95	\$4.00	1兆パラメーター、キャッシュヒット時入力\$0.19 ⁶
DeepSeek V4-Flash	DeepSeek (中国)	\$0.14	\$0.28	2840億パラメーターの超軽量高速モデル ⁶

この表から明らかなように、AnthropicのClaude Fable 5（入力10ドル/出力50ドル）やOpenAIのGPT-5.5（入力5ドル/出力30ドル）と比較し、DeepSeek V4-Proは入力1.74ドル/出力3.48ドルと桁違いの低価格を実現している。さらにKimi K2.7 Codeに至っては入力0.95ドル/出力4.00ドルであり、後述するキャッシュ機能がヒットした場合には入力コストが0.19ドルまで圧縮される⁶。これが、日経新聞が報じた「料金はミツスの20分の1とコスパが高い」という表現の定量的な根拠である³。技術覇権を狙う米国勢にとって、このハードウェア制約をソフトウェアの最適化で乗り越えてきた中国モデルの進化は、最大級の警戒感をもたらしている。

4. トークンエコノミーの成熟と米企業の「静かなる反乱」： Coinbaseのインフラ最適化戦略

AIモデルの選択において、企業の関心事はもはや「モデルの出力精度」だけではなく、完全に「トークン・ユニットエコノミクス (Token Unit Economics)」、すなわち投下したコストに対してどれだけのROI（投資対効果）が得られるかという経営課題へとシフトしている。

4.1. Tokenmaxxing（トークン浪費）の終焉とコスト危機

2026年に入り、AIエージェントの普及と各社ツールの社内導入に伴い、企業におけるAIトークンの消費量は爆発的に増加した。AmazonやMetaといった一部の巨大テクノロジー企業では、このトークン

消費がモラルハザードを引き起こしていた。社内に設けられたAI利用量ランキング(リーダーボード)で上位に入るため、従業員がMeshClawのような内部ツールを用いて無意味なタスク(不要なコードデプロイメントのトリガーやメールのトリガー等)を自動化し、トークン消費を水増しする「

Tokenmaxxing(トークン最大化)」という現象が蔓延したのである⁶。

Meta社内では、「Claudeconomics」と名付けられたリーダーボードを巡って、従業員がわずか30日余りで73.7兆トークンを消費するという異常事態が発生した。このままでは内部利用のAIコストだけで2026年中に数十億ドル規模に達するとの見通しから、CTOのAndrew Bosworthは「目的のないAI利用」を厳格に禁じ、経営陣が厳格な予算管理とインハウスモデル(MetaCode)への誘導を図る「Token managing(トークン管理)」へと強硬に舵を切らざるを得なくなった⁶。

定額制のSaaSモデルから「従量課金制のトークンエコノミー」への移行は、あらゆる企業のIT予算に深刻な「価格のストレステスト(Pricing Stress Test)」をもたらしている。

4.2. Coinbaseによるスマート・アーキテクチャの構築

この激烈なコスト圧力の中、最も劇的かつ戦略的な対応を見せたのが、米国最大の暗号資産取引所であるCoinbaseである。CEOのBrian Armstrongは、自社開発チームへのAIトークン利用制限(キャップ)を設けて生産性を阻害するのではなく、インフラストラクチャの徹底的な知能化によってコストを制御する道を選んだ。具体的には、社内のAI基盤モデルをOpenAIやAnthropicから、中国製のGLM 5.2やKimi 2.7へと大胆に切り替えたのである⁵。

Armstrongは「AIへの支出が増えれば増えるほど、より高いインパクトを期待する」という説明責任(Accountability)の原則を敷きつつ、以下の3つの高度なシステムのアプローチを導入し、AI支出を50%削減(半減)させながらも、全体のトークン消費量を増加させるという離れ業を演じた⁵。

1. 動的モデルルーティング(**Dynamic Model Routing**)システム: 開発者がすべてのタスクを一律に高価なフロンティアモデル(GPT-5.5やClaude)に投げることを防ぐため、Coinbaseはアルゴリズムによる自動ルーティングシステムを構築した。リクエストが発生するたびに、システムは①タスクの複雑性(簡単な翻訳か、高度な推論か)、②現在のAPI価格、③キャッシュの可能性という3つの変数を瞬時に評価し、そのタスクに最も費用対効果の高いモデルを自動選択する。事実上、リクエストの91%は旧来の利用上限に達することなく、安価な中国製モデルで処理されている。
2. 徹底したキャッシュ戦略(**Caching**)による再利用: モデルへのリクエストにおいて、以前の計算結果を再利用するキャッシュシステムを徹底的に最適化し、キャッシュヒット率を従来のわずか5%から一気に60%にまで引き上げた。Kimi K2.7のように、キャッシュヒット時の入力コストが100万トークンあたり0.19ドルへと激減する仕組みにおいて、この60%というヒット率は莫大なコスト削減効果を生む。
3. コンテキスト・エンジニアリング(**Context Engineering**): プロンプト・エンジニアリングの次のフェーズとして、開発者に対し、プロンプトのコンテキストを極限まで無駄なく削ぎ落とす「コンテキスト・エンジニアリング」を徹底させた。新しいタスクを始める際は既存のセッションを引き継がず完全にリセットすることで、不要な過去の対話履歴(トークン)がAPIに乗って送信されるオーバーヘッドを排除している。

4.3. 米国AI産業への波及効果とIPOへの暗雲

Coinbaseの事例は決して孤立したものではない。AIスタートアップであるLindyは、人員コストを超えるほどに膨れ上がったAnthropicへのAPI支払いを「ビジネスの死活問題」と捉え、自社システムを完全にDeepSeekへと移行させることで数百万ドルのコスト削減に成功した⁶。また、データクラウド大手

のSnowflakeも、より安価な代替手段として中国製モデルのテストを積極的に進めている⁶。

この「米国企業による中国AIへの静かなる乗り換え」は、OpenAIやAnthropicといった米国のAIリーディングカンパニーにとって深刻な脅威となっている。両社ともに巨額の資金調達を経て2027年頃のIPO(新規株式公開)を視野に入れているが、企業顧客がコスト感応度を高め、安価な代替モデルへの移行を進めることは、IPOの正当化に不可欠な「成長率」や「売上予測」という前提を根底から突き崩すリスク(レッドフラッグ)をはらんでいる。この価格圧力により、OpenAIがGPT-5.6-Solなどの効率化モデルを投入するなど、米国ラボ間でもAPIトークンを巡る消耗戦(価格競争)が勃発しつつある⁶。

5. 日本の地政学的・法務的優位性: ソブリンAIと著作権法第30条の4の戦略的活用

米国政府が安全保障上の理由でトップモデルへのアクセスを恣意的に遮断し、一方で米国のテクノロジー企業自身がコスト削減のために敵対国であるはずの中国製モデルへ経済合理性から乗り換えるという「大いなる矛盾」。このグローバルな混乱の中、日本は独自の立ち位置を確立し、世界的な競争力を確保するための基盤を着々と整えつつある。

5.1. 「ソブリンAI」と国内計算インフラの自律・強靱化

日本政府は、「人工知能基本計画」において「AI利活用の加速的推進」のみならず、「AI開発力の戦略的強化(AIを創る)」と「AIガバナンスの主導」を国家目標として明確に掲げている¹⁶。自民党の平井卓也元科学技術担当相が強調するように、特定の国や特定企業(米中のメガテック)への過度な依存を防ぎ、多様なモデルやクラウド基盤を組み合わせることで国家主権と経済安全保障を確保する「ソブリンAI」の概念が、政策の核として急速に浸透している¹⁷。

この政策的要請に応える形で、ハードウェア・インフラの国産化と強靱化が本格始動している。富士通は2026年2月12日、経済安全保障に対応するミッションクリティカルな「ソブリンAIサーバ」について、2026年3月より国内工場(笠島工場)における自社製造を開始すると発表した¹⁸。最新のNVIDIA HGX B300やNVIDIA RTX PRO 6000 Blackwell Server Editionを搭載したサーバ、さらには高い省電力性とコンフィデンシャルコンピューティングによる強固なセキュリティを備えた自社開発プロセッサ「FUJITSU-MONAKA」搭載サーバのプリント基板組み立てから実装までを国内で一貫生産する¹⁸。これにより、重要部品のトレーサビリティを厳格に管理し、海外での製造過程におけるハードウェアのブラックボックス化(スパイチップの混入等)を防ぎ、国内の重要インフラ事業者に対してデータ流出リスクを極限まで抑えた計算リソースを提供することが可能となる。

同時に、ソフトウェア(基盤モデル)の開発支援も佳境を迎えている。経済産業省とNEDOが主導する「GENIAC(Generative AI Accelerator Challenge)」プロジェクトは、総額約10億円の懸賞金と計算リソースを提供するAIコンテスト「GENIAC-PRIZE 2026」を始動させた¹⁹。この国家支援の効果は既に民間企業の業績に波及しており、例えばnote株式会社の2026年11月期第1四半期決算では、GENIACプロジェクトを通じたAI・IPの新規事業の推進や、主力事業でのAIによる全社的な生産性向上(限界利益率の高い事業構造への転換)により、営業利益が前年同期比で41倍の2億3,500万円へと爆発的に拡大する「利益爆発」のフェーズに突入している²⁰。

5.2. 著作権法第30条の4という世界的アドバンテージと「モデル蒸留」

日本のAI開発において、計算機リソースの不足を補い、世界に対して極めて強力な競争優位性をもたらしているのが、世界で最もイノベーション親和的と評される日本の著作権法「第30条の4(著作物に表現された思想又は感情の享受を目的としない利用)」の存在である。

この条文により、日本では「非享受目的（著作物を受け入れ、味わい、楽しむことを目的としない利用）」である限り、当該目的のために必要と認められる限度において、既存の著作物を機械学習のための学習データとして利用することが広く許容されている²¹。法学的な解釈においても、「機械学習への30条の4の適用が顕著に問題になるのは学習そのものより利用段階（出力）であることに照らせば、学習への同条の適用は広く認めるべきであり、権利者に不利益は生じない」との見解が主流を占めている²¹。特化型AIの開発によって特定の市場に競合製品が現れたとしても、それが直ちに「非享受目的市場から得られる著作権者の利益を不当に害する（但書）」とは解釈されない柔軟性を持っている²¹。

米国や欧州のAI企業が、The New York Timesなどのメディア企業やクリエイターからの巨額の著作権侵害訴訟に直面し、学習データの収集に膨大なライセンスコストと法務リスクを抱え、結果としてモデルの性能進化が鈍化しているのに対し、日本はこの法環境において圧倒的なフリーハンドを持っている。

この法的優位性が最大の威力を発揮するのが、「合成データ（Synthetic Data）」の生成と「モデル蒸留（Model Distillation）」のプロセスである。中国DeepSeek V4の技術論文にも見られるように、最新の高性能モデルは、膨大なWebデータをそのまま学習するのではなく、内部で特化型の教師モデル（Teacher Model）を複数育成し、それらの推論プロセスから生成された高品質な合成データを用いて、軽量の学生モデル（Student Model）へ知識を圧縮・移植する「On-policy distillation（方策内蒸留）」という手法によって性能とコスト効率を両立している⁶。

日本の著作権法下では、海外の最高峰フロンティアモデルが出力した推論プロセス（Chain-of-Thought）や、クローラーで網羅的に収集した国内の専門文献・データを、AIに「認識」させ解析する行為が合法的に担保されやすい。つまり日本は、他国が莫大なパラメーター競争と訴訟リスクで疲弊する中、世界最高品質のデータを合法的に抽出し、国内のソブリンインフラ上で「軽量・高速・低コスト」な国産特化型モデル（SLM: Small Language Models）を量産する最適なエコシステムを構築できる環境にあるのである。

6. 国家戦略としての「フィジカルAI」：製造業の暗黙知とVLAモデルの融合

米中がデジタルの世界における純粋なソフトウェアLLMで、血みどろの価格競争（1/20の価格破壊）と巨大パラメーターの拡大競争を繰り広げている現在、日本が彼らと全く同じ土俵（純粋な汎用言語モデル単体）で勝負を挑むのは戦略的に得策ではない。LLMの知能はコモディティ化し、API価格は底辺への競争（Race to the bottom）に突入している。

日本が国家の命運を懸けて戦略的にピボット（旋回）し、世界覇権を握るべき絶対的な領域。それこそが、自国の圧倒的な強みである製造業の物理的基盤・ロボティクス技術と、デジタルAI空間をシームレスに融合させる「フィジカルAI（Physical AI / 物理的AI）」の領域である。

6.1. 2026年「フィジカルAI元年」の到来と資金の大転換

2026年は、世界のベンチャーキャピタル市場や産業界においても明確に「フィジカルAI元年」と位置付けられている。米国のベンチャーキャピタル大手Andreessen Horowitz（a16z）の分析によれば、2026年第1四半期のロボティクスなどフィジカルAI分野への投資額は約160億ドル（約500件）に達し、四半期ベースで過去最高を記録した。未上場企業の企業価値（トップ100）のカテゴリー別で見ると、フィジカルAIは10年前には存在感すら皆無であったにもかかわらず、現在では2,630億ドルに達し、フィンテック・決済（2,450億ドル）を抜いて、純粋なAI・ソフトウェアに次ぐ第2位のセクターに躍り

出た²²。

a16zはこの現象を「デジタル(ソフトウェア)からリアル(物理世界)への資金の大転換」と定義している。投資家の審査基準も「技術的な実証実験」から「量産可能か、実用化して金を払う顧客がいるか」というフェーズへと移行しており、基盤モデルからシミュレーション訓練基盤、部品供給網までが一気に成熟しつつある²²。

自民党デジタル社会推進本部の平井氏が「人口減少や高齢化が進む日本において、AIは社会課題を解決する重要な鍵になる」と述べているように、人手不足が世界で最も深刻に進行している日本にとって、製造業、介護、物流、防災の現場で物理的作業を代替するフィジカルAIは、単なる成長産業ではなく国家生存の必須インフラである¹⁷。

6.2. VLAモデルへの進化と「暗黙知」のデータ化エコシステム

従来のロボティクスは、工場などの固定された環境下において、人間が記述した厳密なルールベースのプログラミングに従って反復動作を行うもの(ティーチング・プレイバック方式)であった²³。しかし、フィジカルAIの時代においては、「プログラミング」から「学習」へと根本的なパラダイムシフトが起きる。

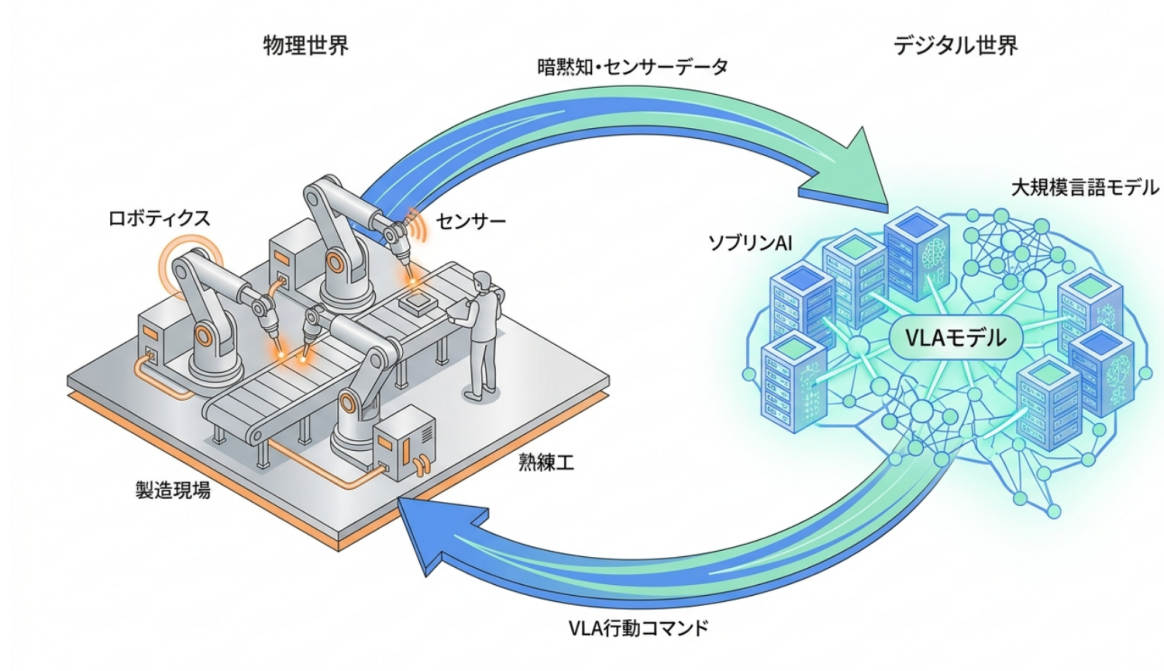
その中核を担うのが、VLA(Vision-Language-Action)モデルと呼ばれるマルチモーダル基盤モデルである²³。これは、カメラからの視覚情報(Vision)と言語による指示(Language)を入力として直接理解し、ロボットの関節やモーターに対する物理的な制御コマンド(Action)を自律的に出力するAIモデルである。これにより、現場ごとに環境や対象物の形状が異なる複雑な作業(組み立て、ピッキング、検査など)にも柔軟に対応できるAIロボットが実現する²⁵。

しかし、VLAモデルを賢くするためには、LLMIにおけるインターネット上のテキストデータのように、大量の「現実世界の物理データ」が必要となる。日本が直面していた最大の課題は、この実環境データが企業や工場ごとに分散・サイロ化して管理されており、AIモデルの学習に十分な質と量を持ったデータが蓄積・共有されていないことであった²⁶。

このデータ・ボトルネックを打破するための国家的エコシステム構築が、現在急ピッチで進められている。愛知県名古屋市に立地する日本最大級のオープンイノベーション拠点「STATION Ai」は、経済産業省とNEDOのGENIAC事業(データエコシステム構築)の支援を受け、2026年12月の稼働を目指して本社内にフィジカルAIのデータ収集センター「STATION Ai Data Foundry」を設立した。トロン株式会社などのスタートアップと連携し、製造業の現場から作業者のマルチモーダルデータ(音声、画像、動画、センサーデータ)を横断的に収集・加工し、ロボットデータと連携させるハブ機能を担っている²⁶。

さらに、同じくGENIACに採択された株式会社ELEMENTSは、「製造業の熟練工の暗黙知(Tacit Knowledge)」にスコープを定め、匠の技術や直感的な動作をデジタルデータセットとして構築し、日本の製造現場に眠る知見を国産AIの基盤資産へと変換する取り組みを進めている²⁷。また、一般社団法人AIロボット協会(AIRoA)は、工場だけでなく「実家庭におけるロボット動作データ」の収集・活用を継続的に拡大し、多様な家庭環境でロボットを継続的に運用することでデータの蓄積とモデル改善が循環するエコシステム(テレオペレーションの仕組み等)の確立を目指している²⁴。

日本の競争優位性を確立する「フィジカルAI」データエコシステム



日本の製造現場に蓄積された熟練工の「暗黙知」やマルチモーダルデータ（視覚・触覚・センサー）が、ソブリンAIインフラ上でVLA（Vision-Language-Action）モデルとして学習され、再び物理世界（ロボット）の制御へと還元される好循環サイクル。

日本が世界に勝てる唯一にして最大のシナリオは、この「現場のリアルな物理データ（ロボティクスのハードウェア資産）」の圧倒的な質と量をいち早く独占確保し、それを富士通などが構築する国内の安全なソブリン計算インフラ上で処理し、世界最高のフィジカルAI基盤（VLAモデル）を創り上げることである。サイバースペースの言語モデル競争を制したのが膨大なWebデータを持つ米国であるならば、フィジカルスペースのAI競争を制するのは、精緻な物理データと高度なメカトロニクスを擁する日本でなければならない。

7. 日本が直ちに実行すべき包括的アクションプラン（4つの提言）

「米国製AIへのアクセス遮断リスク（安全保障上の制約）」と「中国製AIの急速な台頭と価格破壊」というマクロ環境の急激な変化を踏まえ、日本企業および日本政府は、以下の具体的な行動（アクション）を国を挙げて早急に実行に移すべきである。

提言1: インフラのハイブリッド化と「スマート・ルーティング」の全社的導入

Coinbaseが実証した「トークン・ユニットエコノミクス」の最適化モデル⁶に倣い、日本の大企業および行政機関は、単一の米国製フロンティアモデル（OpenAIやAnthropic等）への過度な依存状態から

直ちに脱却しなければならない。社内のAI利用を統合管理する「AIゲートウェイ」を構築し、以下の基準に基づく「動的モデルルーティング」を実装すべきである。

タスクの性質	推奨ルーティング先モデル	期待される効果・目的
機密データ処理・重要インフラ・高度推論	国産LLM(GENIAC発モデル等)、自社内VPCに構築したソブリンAIサーバ	情報漏洩の完全防止、地政学的な供給遮断リスク(ベンダーロックイン)の排除
中規模の要約・社内文書作成・一般支援	費用対効果の高い中規模・軽量モデル(Llama等オープンモデルのファインチューニング)	運用コストの適正化、レイテンシ(応答速度)の向上
定型タスク、単純なコード生成、多言語翻訳	最安値のオープンウェイトモデル(DeepSeek V4-Flash等、利用規約とデータ保護要件を満たした上でのAPI利用または自己ホスト)	トークン消費の極小化によるコスト半減、経済合理性の追求

このスマート・ルーティングと並行して、キャッシュヒット率を引き上げるアーキテクチャや、プロンプトのオーバーヘッドを削ぎ落とす「コンテキスト・エンジニアリング」を従業員教育として徹底することで、増大し続けるAIインフラコストを劇的に圧縮することが可能となる。

提言2: 著作権法第30条の4を最大限活用した「モデル蒸留」の国家的大規模実施

日本の著作権法第30条の4が提供する「非享受目的の利用における柔軟性」は、世界のAI開発競争において日本に与えられた最大の「チートコード(特権)」である²¹。日本政府(経済産業省・文部科学省等)および研究機関は、この法環境に対する萎縮効果を排除し、合法的な範囲内での「合成データ」生成と「モデル蒸留」を国家プロジェクトとして大規模に推進すべきである。

具体的には、グローバルなオープンモデルやAPI経由で取得可能な高度な推論プロセスをデータセット化し、それを用いて国内の計算リソースに最適化された軽量かつ高性能な「特化型SLM」を次々と派生させるエコシステムを構築する。欧米が法的制約と巨額のライセンス費用で身動きが取れなくなる中、日本は知財法のグレーゾーンを恐れることなく、明文法(30条の4)の射程を最大限に活かせるアグレッシブなデータ戦略を展開しなければならない。

提言3: 製造現場の「暗黙知」を資産化するデータトラストの形成

フィジカルAIの勝敗は、「どれだけ高品質な現実世界の物理データ(接触、摩擦、視覚、力覚、失敗時のリカバリー動作等)をモデルに食わせることができるか」という一点にかかっている。しかし現状、日本の強みである製造業の実環境データは企業ごとに厳重に秘匿され、サイロ化している。政府および業界団体(AIRoA等²⁴)は、競合する企業間であっても安全にデータを持ち寄り、共有・連

携できる「データトラスト(信託機関)」の仕組みを法整備とともに急ぎ設立すべきである。STATION AI Data Foundry²⁶のようなオープンイノベーション拠点を、中京工業地帯のみならず全国の主要な産業集積地に水平展開し、熟練工のモーションデータやロボットの稼働データを標準フォーマットで継続的に収集・匿名化し、それを国内のVLAモデル開発者に無償または低コストで提供する「データエコシステム」を、道路や港湾に次ぐ国家の重要インフラとして整備・運用しなければならない。

提言4: 高リスク領域における「ヒューマン・イン・ザ・ループ」の法制化

米国政府がAnthropicのMythosに対して輸出を一時停止し、自国のNSAやCISAのみがそのサイバー防御能力を活用したという事実は、高度なAIがすでに一企業のプロダクトの枠を超え、国家のインフラと兵器の二面性(デュアルユース)を明確に帯びていることを証明している¹。

日本においても、AIへの過度な依存がもたらすシステム障害や倫理的破綻を防ぐため、自民党の平井氏が提唱する「ヒューマン・イン・ザ・ループ」の原則¹⁷をより強固なものとするべきである。具体的には、医療診断、金融システム、重要インフラ(電力・交通)、そして安全保障・防衛といった高リスク領域におけるAIの自律的な意思決定を制限し、最終的な判断、承認、および法的責任の主体を必ず人間の専門家(Human-in-the-loop)に帰属させる国内法を整備する。これにより、ブラックボックス化したAIの暴走を防ぐと同時に、AIによる意思決定プロセスに透明性と監査可能性を持たせる国内独自のガバナンス基準を確立し、欧州の過剰規制(AI Act)とも米国の放任主義とも異なる、実利と安全を両立したアジャイルな日本型AI規制モデルを国際社会に向けて発信・主導すべきである。

8. 結論: 次世代AI競争における日本の「勝ち筋」

2026年7月、「ミトゥスいぬ間に」起きた中国AIの爆発的躍進と、米国テクノロジー企業による大規模な乗り換え劇は、言語モデルを中核とする「知能のコモディティ化」と「ソフトウェア価値の価格破壊」が限界点に達した決定的な証左である。純粋なデジタル空間(クラウド上)での汎用LLM基盤の開発において、膨大な資本力と計算リソースを持つ米国メガテックや中国の国家支援企業に対し、日本が正面から物量戦を挑むことは、もはや現実的ではない。

しかし、AIがコンピュータの画面の中から現実空間へと飛び出し、物理世界で直接的に作用する「フィジカルAI」のフェーズへと戦場が移行した現在、前提条件は完全に覆る。日本が有する世界最高峰のメカトロニクスと精密なロボティクスハードウェア、全国の製造現場に蓄積された幾百万の精緻な暗黙知、そして機械学習データの生成に極めて寛容な著作権法(第30条の4)の存在は、米中がいくら資本を投下しても短期間では模倣・構築できない強固な「経済的な堀(Economic Moat)」となる。

日本がなすべき戦略的決断は明確である。安価な中国製モデルや米国のオープンソースモデルを「コモディティ化された知能のAPI」として冷徹かつスマートに使い倒し、企業のデジタルトランスフォーメーションにかかるコストを徹底的に最適化する。そして、それによって浮いた自国のリソース、国家予算、エンジニアの才能をすべて、現実世界の物理データの収集とフィジカルAI基盤モデル(VLA)の構築、ならびにそれを支える強靱な国内サブリン計算インフラの拡充へと集中投下することである。

デジタルサイバースペースの消耗戦から、リアルな物理空間の高付加価値競争へ。この国家的かつ戦略的ピボットこそが、激動のグローバルAI覇権競争において、日本が確固たる国家主権を維持し、次代の圧倒的な経済成長を牽引するための唯一にして絶対の道筋である。

引用文献

1. アンソロピック ミュトス級AIの提供停止 米政府の輸出管理対象指定で 安保懸念か, 7月 7, 2026にアクセス、<https://www.youtube.com/watch?v=LUH7v-mOKrY>
2. Anthropic says US has lifted export controls on Fable and Mythos AI models after security fears, 7月 7, 2026にアクセス、
<https://www.theguardian.com/technology/2026/jul/01/anthropic-fable-mythos-ai-models-us-export-controls-lifted>
3. [B! AI] 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 ..., 7月 7, 2026にアクセス、
<https://b.hatena.ne.jp/entry/s/www.nikkei.com/article/DGXZQOGN242Z50U6A620C2000000/>
4. 中国AIがミュトスいぬ間に躍進料金は20分の1, 7月 7, 2026にアクセス、
<https://www.trueplookpanya.com/knowledge/content/67205/-blog-blo-?live-blog-15784310-2026-07-06-zhong-guoaiamyutosuinu-jianni-yue-jin-liao-jinha20fenno1-mi-qi-yemo-chengri-hua>
5. Coinbase Switches to Chinese AI Models GLM and Kimi, Cuts AI Spending by 50% - MLQ.ai, 7月 7, 2026にアクセス、
<https://mlq.ai/news/coinbase-switches-to-chinese-ai-models-glm-and-kimi-cuts-ai-spending-by-50/>
6. Coinbase joins the rush to Chinese AI models as Western labs face ..., 7月 7, 2026にアクセス、
<https://the-decoder.com/coinbase-joins-the-rush-to-chinese-ai-models-as-western-labs-face-a-pricing-stress-test/>
7. Coinbase、中国製AIモデルに切り替え、コストを半分に削減, 7月 7, 2026にアクセス、
<https://www.kucoin.com/ja/news/flash/coinbase-switches-to-chinese-ai-models-cuts-costs-by-half>
8. Claude Mythos - Anthropic, 7月 7, 2026にアクセス、
<https://www.anthropic.com/claude/mythos>
9. 【米・アンソロピック】高性能AI「ミュトス」など提供停止へ “米政府から国家安全保障上の懸念と命令” 日本も制限対象か - YouTube, 7月 7, 2026にアクセス、
<https://www.youtube.com/watch?v=AV2BsJYHGau>
10. 「ミュトス級」提供を再開 アンソロピック、規制解除, 7月 7, 2026にアクセス、
<https://www.47news.jp/14555268.html>
11. Anthropic's Mythos AI Reportedly Helping Find Weaknesses in US Government Software After Surviving Trump, 7月 7, 2026にアクセス、
<https://www.benzinga.com/markets/tech/26/07/60296255/anthropics-mythos-ai-reportedly-helping-find-weaknesses-in-us-government-software-after-surviving-trump-admin-clash>
12. Why the US cyber agency is using Anthropic's Mythos to audit government code, 7月 7, 2026にアクセス、
<https://www.thenews.com.pk/latest/1408332-why-the-us-cyber-agency-is-using-anthropics-mythos-to-audit-government-code>
13. US Government Turns To Anthropic's Mythos AI For Cybersecurity Audits: Report, 7月 7, 2026にアクセス、
<https://www.ndtvprofit.com/business/us-government-turns-to-anthropics-mythos-ai-for-cybersecurity-audits-report-11736607>

14. アンソロピック、米政府の規制解除で提供再開...AIモデル「ミトス5」と一般向け「フェイブル5」, 7月 7, 2026にアクセス、
<https://www.yomiuri.co.jp/economy/20260701-GYT1T00138/>
15. 人気ポスト - X(旧Twitter)で話題のおもしろ画像や動画 - Yahoo!リアルタイム検索, 7月 7, 2026にアクセス、
https://search.yahoo.co.jp/realtime/search/tweet/2074257454624628844?detail=1&ifr=tl_twdtl&rkf=1
16. 初の「人工知能基本計画」を閣議決定しました - 内閣府, 7月 7, 2026にアクセス、
https://www.cao.go.jp/press/new_wave/20260206.html
17. 日本はAI時代にどう生き残るのか 自民・平井卓也氏が語る「人間主導」と現場AI | 黄信維(コウ・シンイ) | ニュース, 7月 7, 2026にアクセス、
<https://japan.storm.mg/articles/1147092>
18. 富士通、経済安全保障に対応する「ソブリンAIサーバ」の国内製造を開始 - IoTNEWS AI+, 7月 7, 2026にアクセス、
<https://iotnews.jp/ai/272483/>
19. 総額約10億円の懸賞金・計算リソースを提供するAIコンテスト「GENIAC-PRIZE 2026」が始動します - 経済産業省, 7月 7, 2026にアクセス、
<https://www.meti.go.jp/press/2026/05/20260529003/20260529003.html>
20. 【5243.T FY2026 Q1 決算説明会】営業利益が前年同期比41倍の2.35億円に急拡大、AI活用と高収益構造で「利益爆発」の巡航へ, 7月 7, 2026にアクセス、
https://finance.biggo.jp/news/JF_5243.T_2026-04-14
21. 7月 7, 2026にアクセス、
https://www.publication.law.nihon-u.ac.jp/pdf/property/property_18/each/08.pdf
22. 米のフィジカルAI投資、過去最高に＝未上場企業の第2勢力に, 7月 7, 2026にアクセス、
<https://exawizards.com/column/ai-trend/news-07-06-2026-3/>
23. 2026年、日本は「フィジカルAI」で再起する。――国家生存をかけた三つの潮流と、その戦略の全貌(第1部) - Qiita, 7月 7, 2026にアクセス、
<https://qiita.com/mhamadajp/items/45fac1827abab63b369d>
24. AIRoA、経済産業省およびNEDOが実施する国家プロジェクト「GENIAC(*1)」の採択事業者に決定 ―実家庭におけるロボット動作データの収集・活用を継続的に拡大するデータエコシステムの構築へー - PR TIMES, 7月 7, 2026にアクセス、
<https://prt看mes.jp/main/html/rd/p/000000013.000158322.html>
25. 「AIロボット・フィジカルAIを見据えたマルチモーダル基盤モデル開発事業」を開始します, 7月 7, 2026にアクセス、
<https://www.meti.go.jp/press/2026/06/20260630005/20260630005.html>
26. 製造業向けフィジカルAIのデータ収集センター「STATION Ai Data Foundry」2026年12月稼働予定 NEDO補助事業へ採択, 7月 7, 2026にアクセス、
<https://robotstart.info/article/2026/07/06/382115.html>
27. 経済産業省および国立研究開発法人新エネルギー・産業技術総合開発機構(NEDO)が推進する「データエコシステムの構築等に関する研究開発(GENIAC)」にELEMENTSが採択, 7月 7, 2026にアクセス、
<https://prt看mes.jp/main/html/rd/p/000000149.000061051.html>