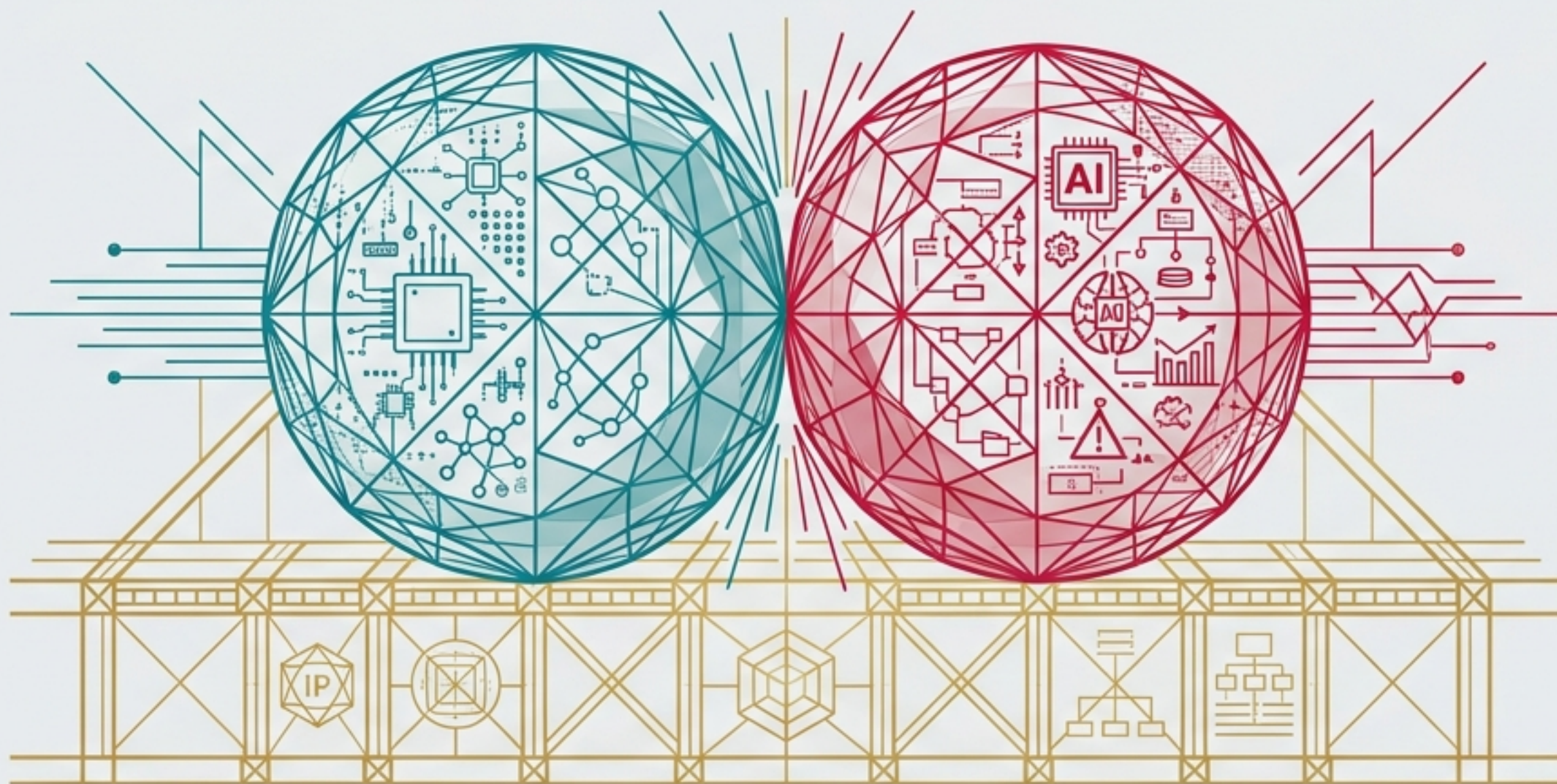


中国AIの躍進と「ミュトス空白」

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



Executive Summary: 構造的シフトと日本の防衛戦略



The Catalyst - 構造的シフト

米政府の輸出規制による「Fable 5 / Mythos 5」の一時停止（ミュート空白）が、米国企業における中国製オープンウェイトモデルへの歴史的な移行を引き起こした。



The Reality - 市場の現実

中国AIの躍進は単なる性能逆転ではなく、「10～100分の1の価格破壊」と「オープンウェイト」によるデファクト化である。汎用推論は米国がリードする「二層市場」が形成されている。



The Strategy - 三層の防衛戦略

日本は単純な排除も盲信もできない。①国家でのフィジカルAI集中投資、②企業でのオンプレ自己ホストを前提としたマルチモデル・ルーティング、③中国データ三法の域外適用を見据えた知財ガバナンスの三層構造が必須となる。

The Catalyst: 18日間の「ミュトス空白」が生んだ逆転劇

Chain Reaction Timeline

June 12, 2026

Anthropicが「Fable 5 / Mythos 5」を公開。同日夕方、ジェイルブレイクの懸念から米商務省がアクセス停止を指示。全世界のユーザーが突如アクセス不能に。

June 12, 2026

ミュトス空白 (The Mythos Blank) - 18日間

June 30 - July 2, 2026

米商務省が規制解除し、Fable 5が一般再開。

July 2, 2026

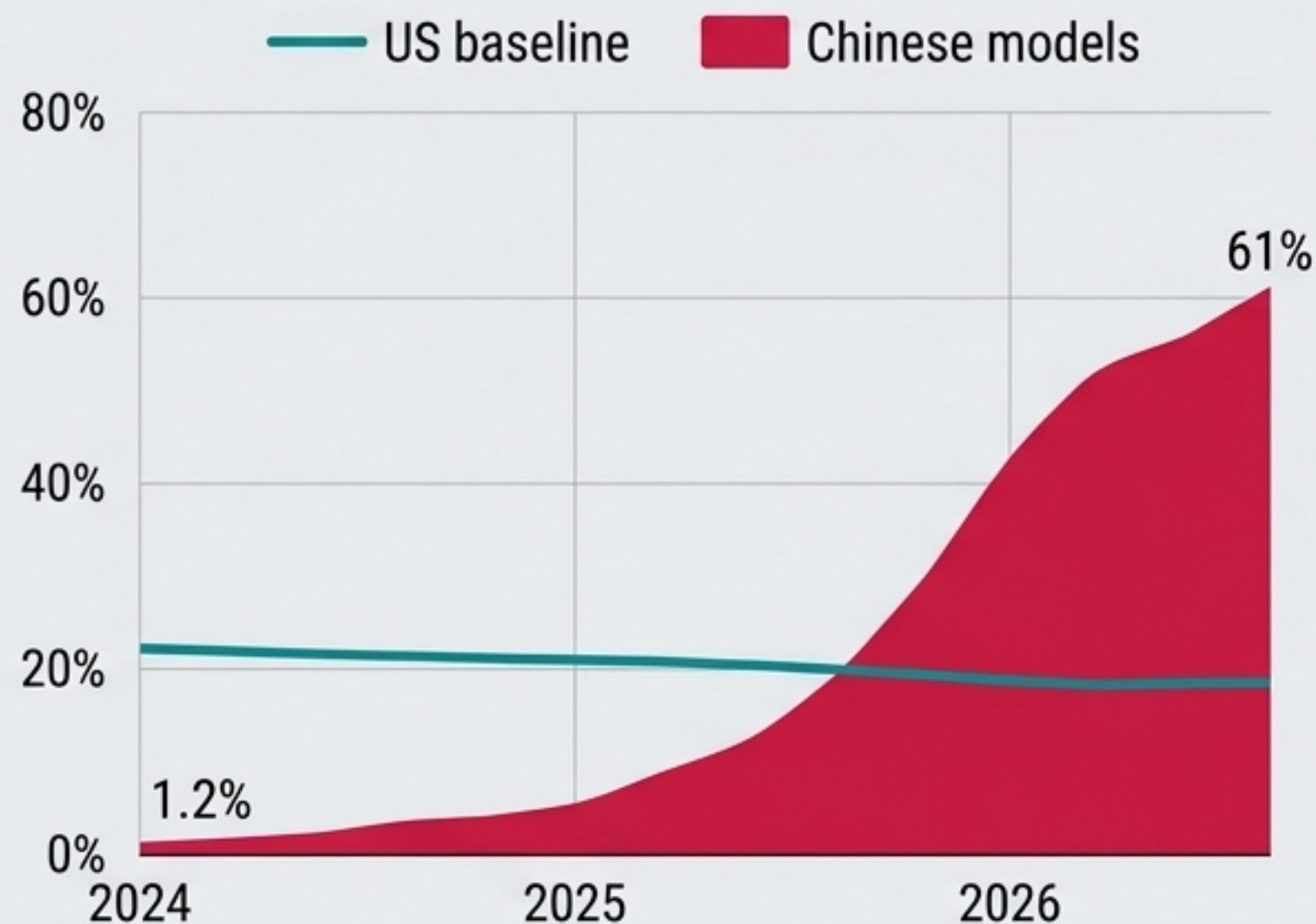
June 13, 2026

停止の翌日、中国Zhipuが「GLM 5.2」をMITライセンスで即時公開。

意図せぬマーケティング効果。この事件は中国勢に「キルスイッチのない安心」という強力な武器を与え、事業継続性を重視する組織のオープンウェイト移行を加速させた。

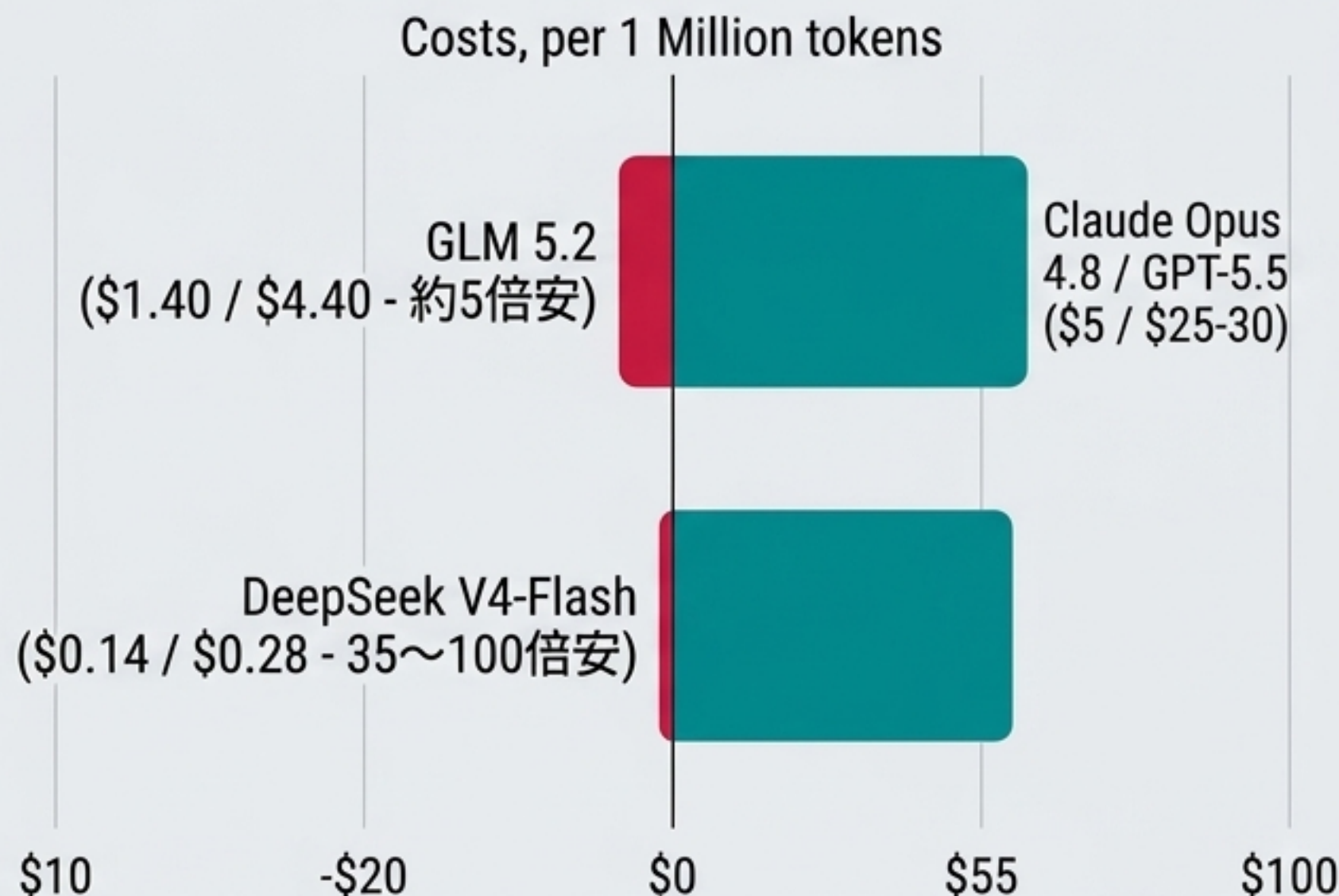
The Market Shock: トークンシェアの急伸と「20分の1」の価格破壊

The Surge



OpenRouterにおける中国モデルのシェア推移（トップ10内スナップショット）。コーディングやエージェント用途での偏在がシェアを牽引。

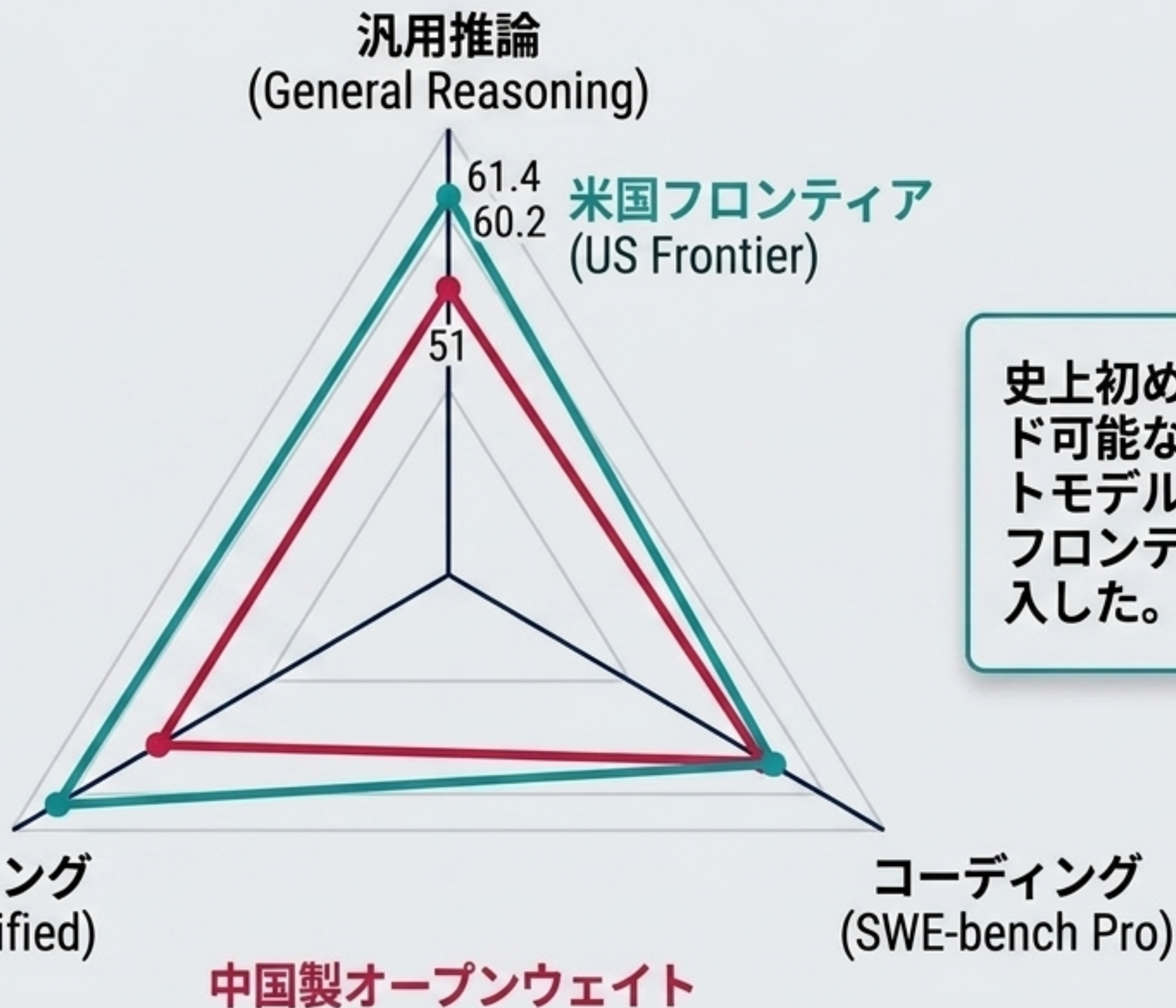
The Price Destruction



実用主力で約5倍安、最安モデルで数十倍安。高価格帯フラッグシップ（\$15/\$75相当）との比較において、日経の「20分の1」報道は十分に裏付けられる。

Performance Reality: 知能のコモディティ化と、機能としてのフロンティア

躍進の本質は「**全面的な性能逆転**」ではない。汎用推論では西側クロースドが3~8ポイントのリードを維持しているが、コーディングやエージェント用途では実質互角~一部逆転の「**二層市場**」が形成されている。



史上初めて、ダウンロード可能なオープンウェイトモデル (GLM 5.2) がフロンティア圏内に突入した。

Comparison Matrix: 二層化するグローバルAI市場

	米国フロンティアモデル	中国製オープンウェイト
提供形態	クローズド (API依存)	MIT / Apache 2.0 (オープンウェイト、自己ホスト可能)
性能の重心	汎用推論・多言語対応の頂点	高ボリュームなコーディング・要約 に特化した互角性能
コスト構造	プレミアム価格設定	徹底的な価格破壊 (フロンティアの10～100分の1)
潜在リスク	米政府の輸出規制による 「突発的なキルスイッチ」リスク	中国データ三法・国家情報法による データ流出・知財不透明性リスク

Structural Drivers: なぜ半導体規制下で躍進できたのか

国務院の「AI+」行動計画に基づく強力な政策支援。DeepSeek R1以降、Qwen・Kimi等が次々とMIT/Apacheで公開され、世界の新規派生モデルの約70%がQwenベースに。

オープン
ウェイト戦略

MoE (Mixture-of-Experts) 等による推論の推論の極限効率化（例：1.6兆パラメータ中、活性化はわずか49B）。

推論の
極限効率化

規制の
逆説

米国の半導体輸出規制（NVIDIA依存の制限とHuawei Ascendへの移行）が、逆に「少ない計算資源で多くを実現する」ためのアルゴリズムの最適化と効率化を強制した。

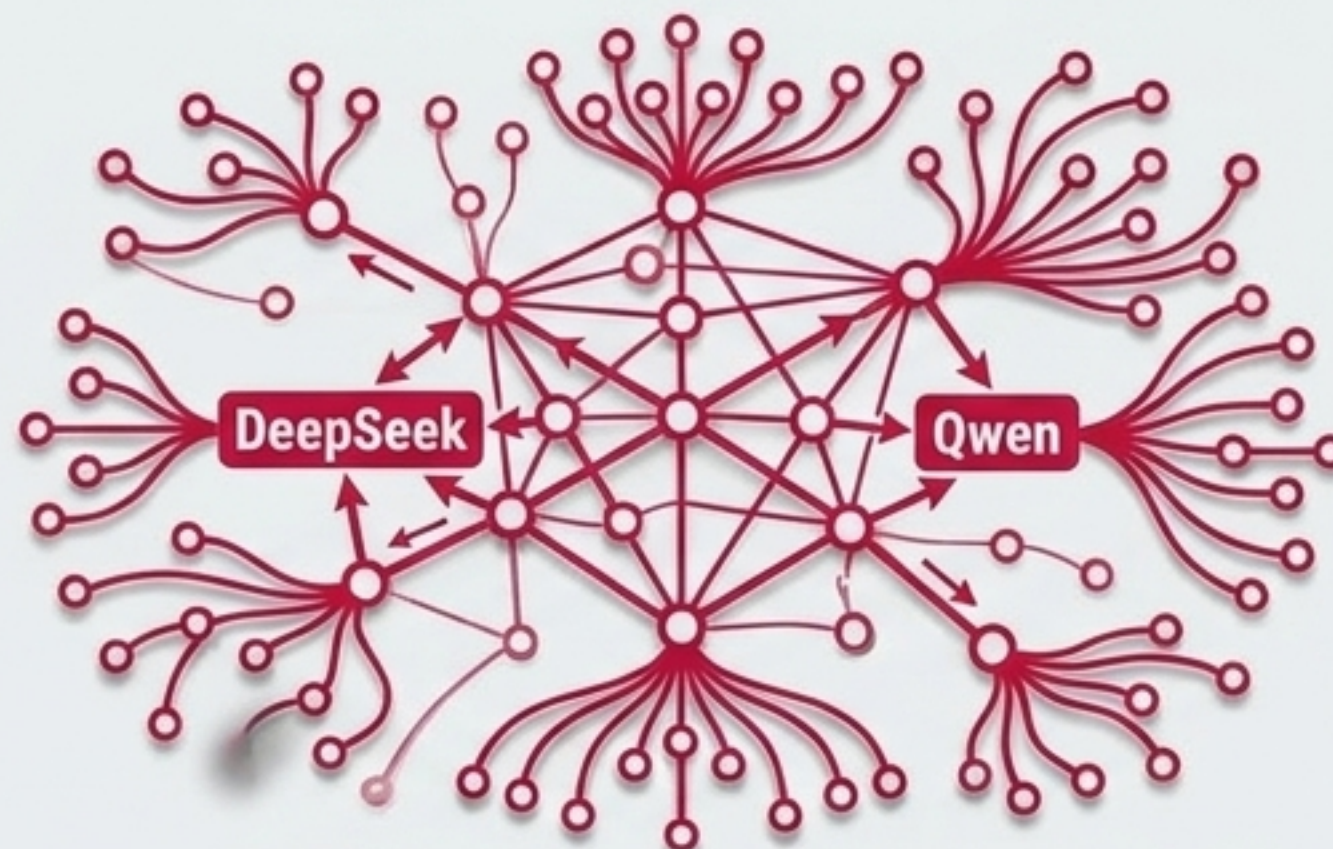
The Japanese Dilemma: 理想の政府クラウドと、依存を深める企業エコシステム

政府基盤「源内」



ガバメントクラウド推論環境（機密性2要件）。
国産7モデル（NTT, NEC, 富士通, PFN等）を選定し、
中国製モデルを構造的に排除。

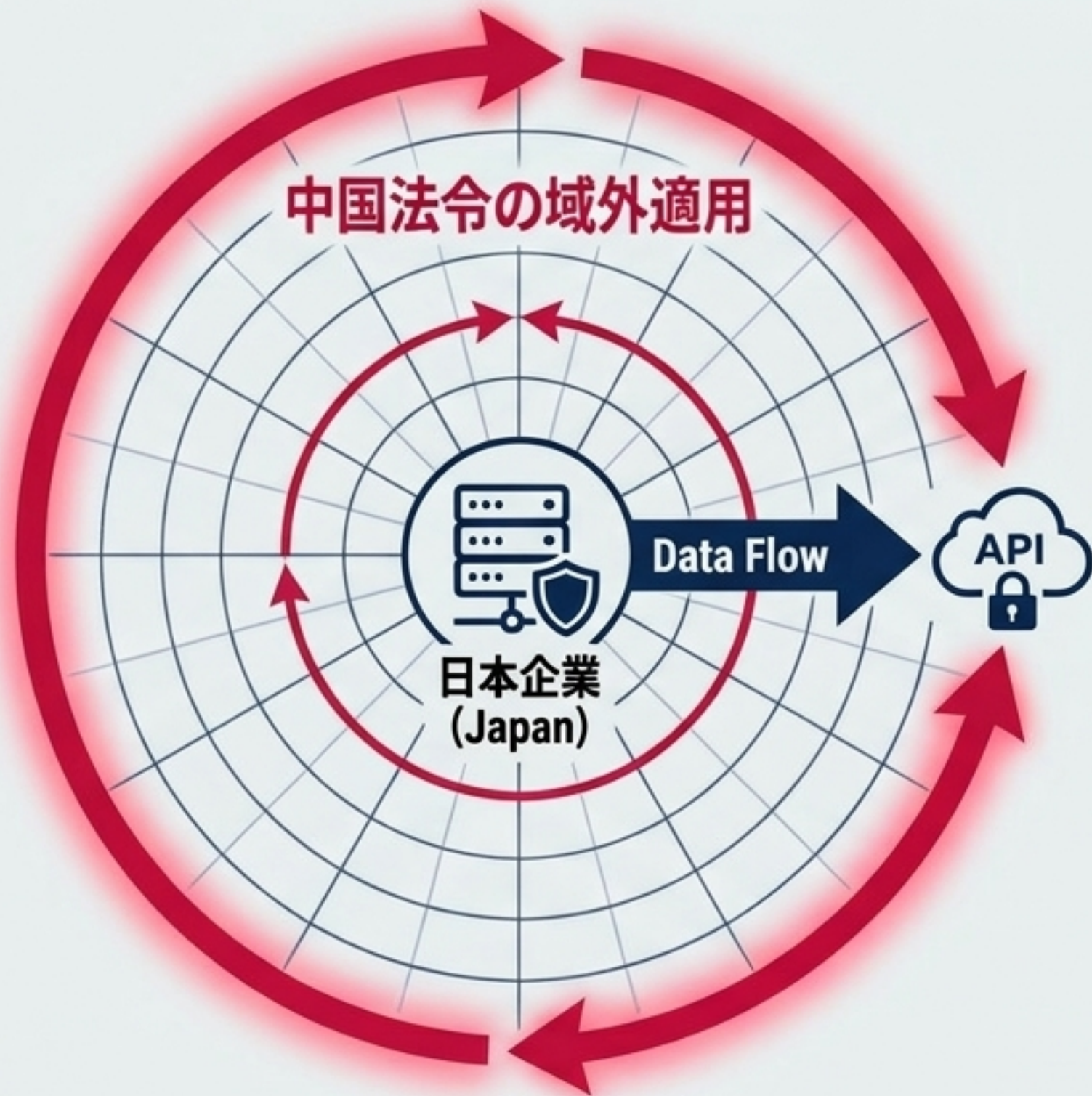
日本企業の現実



日系企業の主要独自モデルの「約6割」が
DeepSeekまたはQwenの二次開発に依存。

「二次開発6割」は諸刃の剣。安価で高性能な基盤を得る一方で、ライセンス変更
リスク、供給停止リスク、知財の不透明性をエコシステム深部に抱え込んでいる。

The Core Threat: 「オープン型」の錯覚と中国データ三法の網

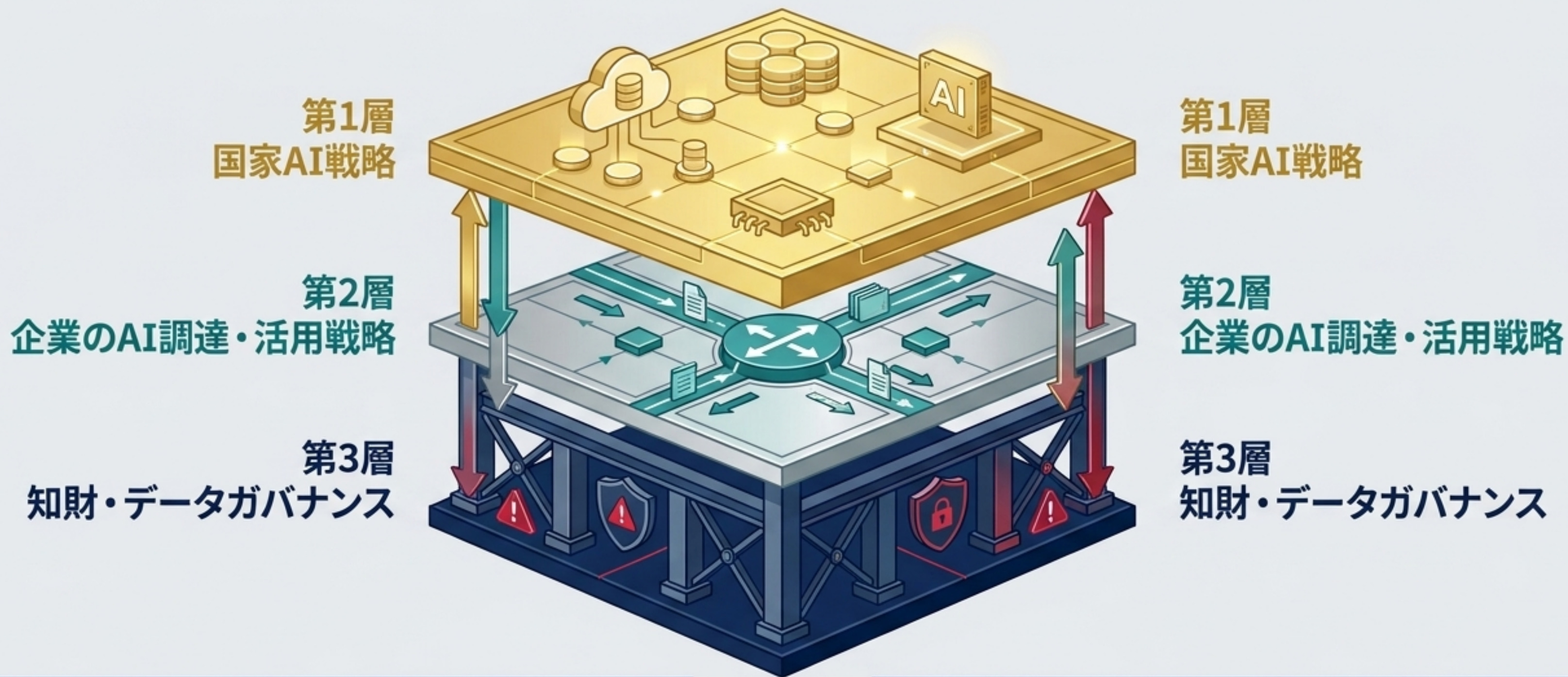


データセキュリティ法: 中国国外の処理活動であっても、中国の国家安全・公共利益を害する場合に適用。当局認可なしでの外国司法機関へのデータ提供を禁止。

個人情報保護法: 中国国内の自然人へ商品・サービスを提供する等の場合、日本国内での処理にも域外適用される。違反時の罰金は最大5,000万元または前年売上5%。

⚠
MIT/Apacheライセンスであっても、API経由での利用は致命的リスクを伴う。オンプレミス（自己ホスト）運用によりデータ流出リスクは遮断可能が、学習データの権利処理や埋め込まれた検閲・バイアスの懸念は残留する。

Synthesis Arc: 求められる三層の防衛・活用戦略



圧倒的なコスト競争力を持つ中国AIを「完全排除」することはグローバルでの企業競争力を失う。一方で「無条件の導入」は国家安全保障と企業知財を致命的な危険に晒す。日本は、国家・企業・ガバナンスの三層が連動したアーキテクチャを構築しなければならない。

Layer 1 (National): フィジカルAIへの選択と集中・データ主権の確保



製造業データ
(Raw Factory Data)

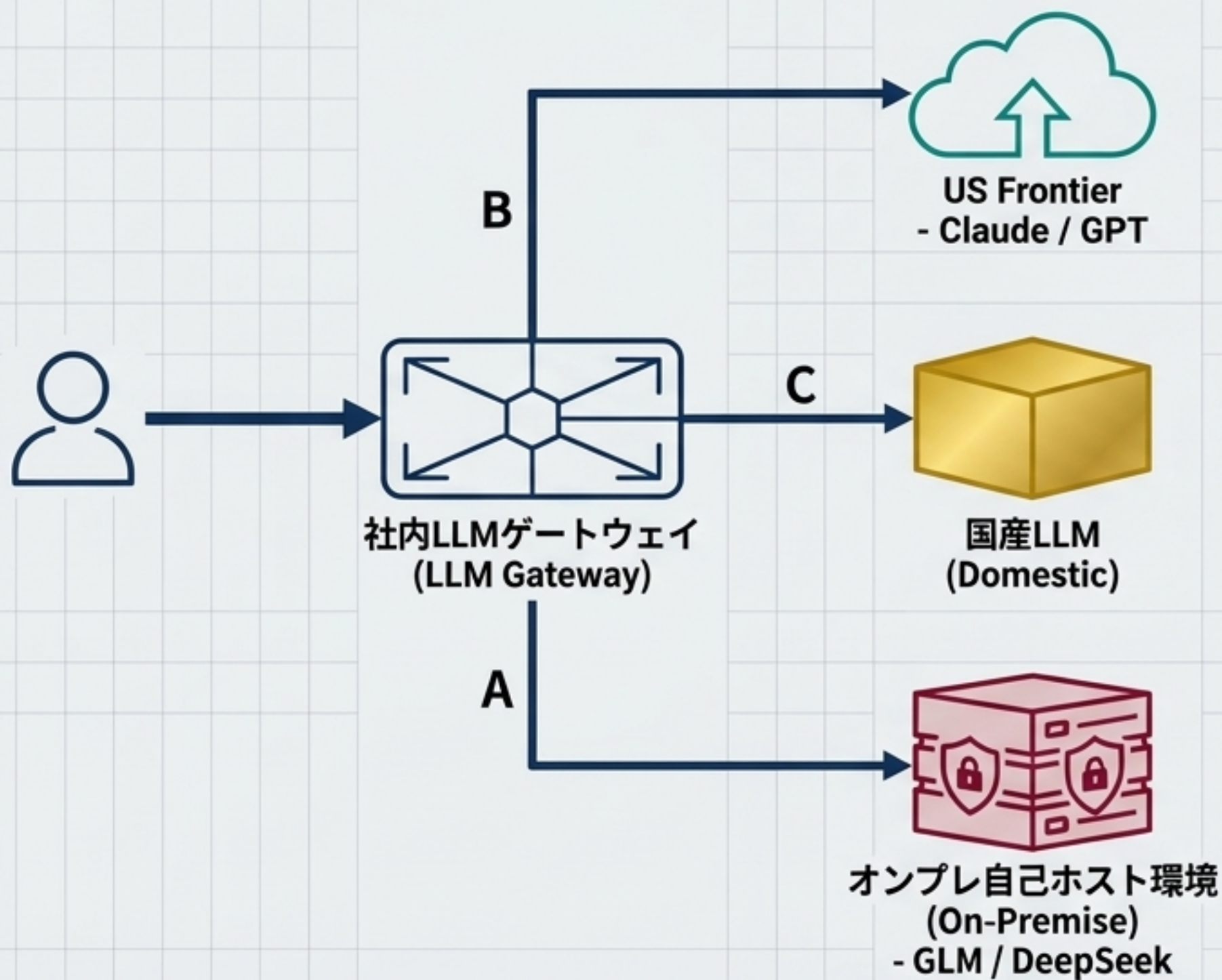
データ精製・主権確保
(Sovereign Data Refinement)

フィジカルAI基盤モデル
(Physical AI Foundations)

1. LLM規模競争からの転換: GENIACと「ノエトラ (Noetra)」を軸に、製造業データのAI-Ready化およびロボット基盤モデルへ国家資源を集中。2027年までに国産フィジカルAI基盤を世界水準へ引き上げる。
2. 製造業データの主権確保: 匠の知恵を海外プラットフォームに奪われる前に、国内でのデータ精製技術・組織横断連携基盤を1年以内に確立する。
3. 経済安保と計算資源: GPU支援終了後を見据えた国家計算基盤の継続提供。政府調達における「源内方式」の維持・拡大。

Layer 2 (Corporate): マルチモデル・ルーティングと自己ホストの徹底

Idealized Multi-Model Enterprise Routing Diagram



アーキテクチャの要諦:

コインベース方式を範とし、社内LLMゲートウェイによる用途別ルーティングを標準化する（キャッシュヒット率60%以上を目標とし、コストを最適化）。

適材適所の絶対原則:

- ・ 高ボリュームのコーディング・要約
→ **【オンプレ限定】中国製オープンウェイト**
- ・ 高度な汎用推論・多言語
→ **米国フロンティアモデル (API)**
- ・ 機密情報・日本語業務文書・行政情報
→ **国産LLM (国内完結)**

絶対ルール

中国モデルの利用は「**オンプレミスでの自己ホスト**」を絶対条件とし、中国APIへのデータ送信は**原則禁止**とする。

Layer 3 & Caveats: 調達ガバナンスの徹底と市場データの冷静な解釈

AI調達・必須チェックリスト（即時導入）

- ☐ 1. 提供元の国と適用される準拠法
- ☐ 2. データの保存先と再学習利用の有無
- ☐ 3. ライセンス条項と学習データの権利開示
- ☐ 4. 重み（ウェイト）への悪意あるコード・バイアス検証

留意事項（Caveats / Reality Check）

- ・「シェア61%」の解釈: オープンルーターのトップ10内・特定週のスナップショットに過ぎず、全世界のAPI総量では依然として西側プロプライエタリが圧倒的多数を占める。
- ・ベンチマークの限界: SWE-bench等はスキャフォールド（周辺プログラム）に依存しており、学習データ汚染の懸念も残る。
- ・過剰な報道への警戒: 「米スタートアップの80%が中国モデル使用」との報道は誇張であり、実勢は2割前後である(a16z調査)。瞬間最大風速と構造的トレンドを厳密に区別せよ。