

主権設計図

「AI敗戦」の幻想と、主権の設計図

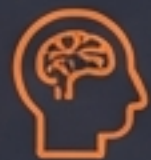
2026年秋、日本企業が直面する真の地政学リスクと実装戦略

対象 : 経営層・知財部門・政策担当者
調査基準日 : 2026年10月7日
主題 : 経済安全保障、マルチモデルBCP、
フィジカルAIへの転換

圧倒的な遅れ： 資本とフロンティアモデル



民間AI投資額（2025年）：
日本 11.1億ドル (14位) **vs**
米国 2,859億ドル (約250倍の格差)



注目すべきAIモデル数：
日本圏外 **vs**
米国59件 (韓国8件にも劣後)

静かなる逆転： 実装力と物理資産



企業の生成AI業務利用率：
86.4% (前年度55.2%から急拡大。
米国・ドイツを凌駕する組織的導入)

産業用ロボット設置数：
約4.5万台 (世界2位・高密度な現場データ)



AI特許の被引用シェア：
6.86% (世界3位・高品質な知財)

日本は「フロンティアAI」の資本戦で敗れたが、
「物理空間への実装戦」で独自の優位性を築きつつある。

決定的な転換点：2026年6月の「Anthropic Fable 5 ショック」

June 9: 【公開】
Anthropic社が最先端モデル「Fable 5」「Mythos 5」をリリース。

June 12: 【停止】米商務省の輸出管理指令が発動。Amazon研究者による安全装置迂回の報告を機に、米国籍以外の全世界のアクセスが一夜にして遮断。

June 26: 【一部再開】米国組織の一部のみアクセス再開。日本企業は依然ブラックアウト。

July 1: 【再提供・条件変更】全世界で再開されるも、従量課金への移行と政府への事前アクセス権限が課される。

同盟国のインフラであっても、米国内の安全保障判断により、提供停止・価格変更・輸出管理のトリガーが一方向的に引かれる事実が証明された。

「国産AI」の再定義：3つの主権レイヤー



「GPT-4oに勝てるか」は誤った問いである。
真の目的は、地政学リスクに対する「代替可能性の確保（BATNA）」にある。

懐疑論への回答：日本が戦うべき「真の土俵」

Skepticism

「巨額投資でも米国に勝てない。国費1兆円では米国の2,859億ドルに太刀打ちできない。」

「海外製のオープンウェイト（Llama, Qwen等）を社内で動かせば十分ではないか？」

「日本の課題はモデル開発ではなく『使う側（アプリ層）』の遅れにある。」

Strategic Reality

✓ 「汎用モデルでは戦わない。勝機は現場データと結びつく『フィジカルAI（Noetra）』に絞られている。」

✓ 「ライセンス変更リスク、学習データの不透明さ、特定国の安全保障リスク（輸出規制）は排除できない。」

✓ 「その通りである。しかし、活用が高度化・組織化（現在86.4%）するほど、基盤モデルへの依存リスク（単一障害点）が致命傷となる。」

国家主導の実装：需要側としての政府の動き

ガバメントAI「源内」プロジェクト

- **Scope:** 全府省庁の職員約18万人を対象とした大規模実証（2026年5月～2027年3月）。
- **Selection:** 15件の応募から、tsuzumi 2、ELYZA、Sarashina2、PLaMo等、国産7モデルを並列採用。
- **Constraint:** 国内完結のガバメントクラウド上での稼働を絶対条件化。

計算基盤とフィジカルAIへの集中投資

- **Infrastructure:** 産総研「ABCI 3.0」（H200×6,128基）の稼働と、クラウドプログラム認定事業者への支援。
- **Noetra Initiative:** ソフトバンク・NEC等44社会連合。5年で最大1兆円規模の国費を投入し、1兆パラメータ級マルチモーダル基盤モデルを開発。

政策の重心は「海外モデルの追従」から、「産業データ（製造・ロボティクス）のAI-Ready化と国内計算基盤の直結」へ完全にシフトした。

知財戦略の転換：AI時代の「防御可能な資産」とは何か

コモディティ化する基盤モデル (Commoditized)

汎用LLMそのもの。技術の陳腐化が早く、Sakana AI (Fugu) のようなオーケストレーション技術により特定の海外モデルへの依存は薄れつつある。

運用ノウハウと評価基盤 (Defensible)

独自のファインチューニング手法、RAG構築ノウハウ、自社専用のベンチマークデータセット。

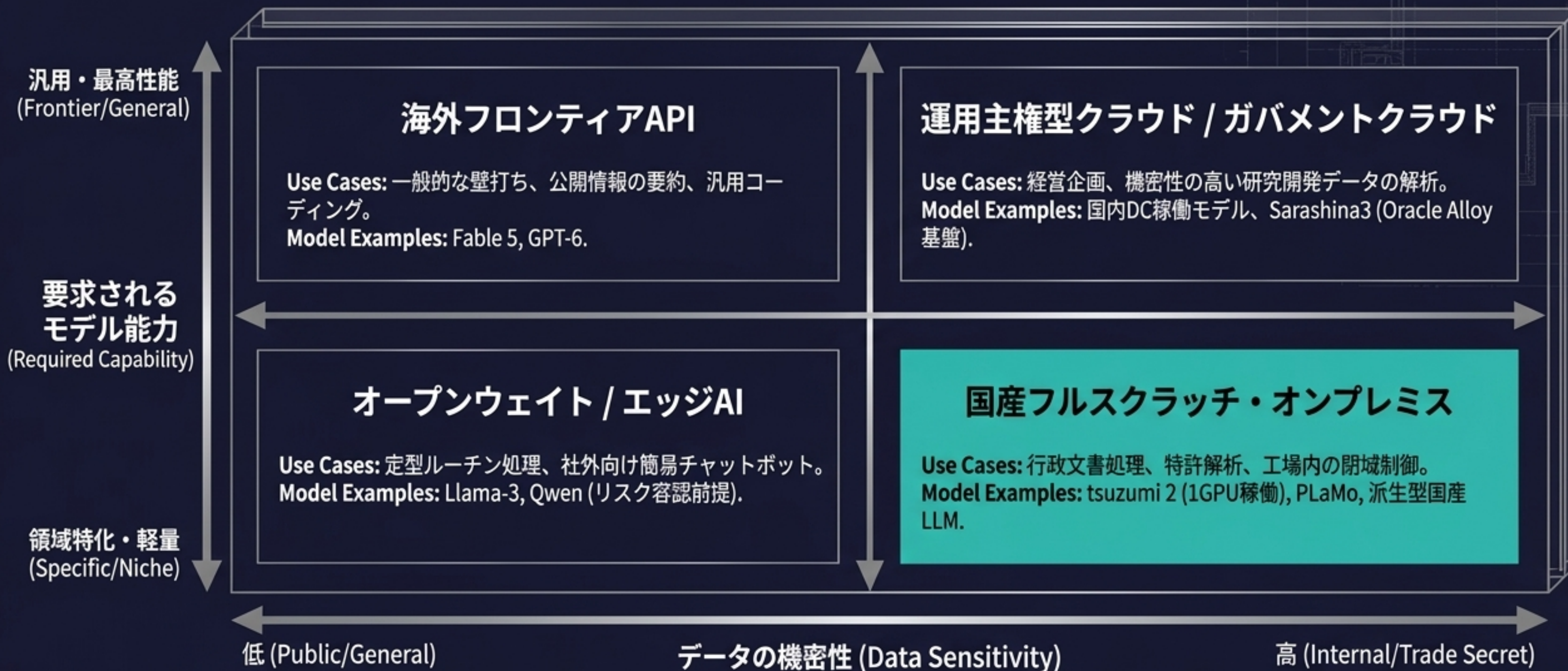
産業データと業務プロセス (Core IP / Trade Secret)

不正競争防止法で保護された独自の現場データ（製造、医療、行政）。



【警告】モデル内部の特許取得よりも、ロボット制御や製造プロセスなど「適用側の業務フロー」での特許網構築が、侵害立証と価値保全において極めて重要。

マルチモデル配置の最適解：機密度と能力によるマトリクス



自社のデータを「どのモデルにも差し替えられる資産」として管理するマルチモデルBCPが必須。

経営・知財部門が直ちに講じるべき3つの実務対応

1



著作権法第30条の4の戦略的活用

情報解析目的での柔軟な権利制限規定（30条の4）を活かし、国内環境での自社特化型モデルの事前学習・継続学習を加速させる。

「プリンシプル・コード（仮称）」制定を見据えた透明性の確保が先行優位となる。

2



ベンダーロックインの排除（契約担保）

プロンプト、評価セット、RAG用データを特定ベンダーに縛られない形式で保有する。契約書には「自社データの学習利用禁止」「データの所在国」「提供終了時の猶予期間（通知期間）」を明記する。

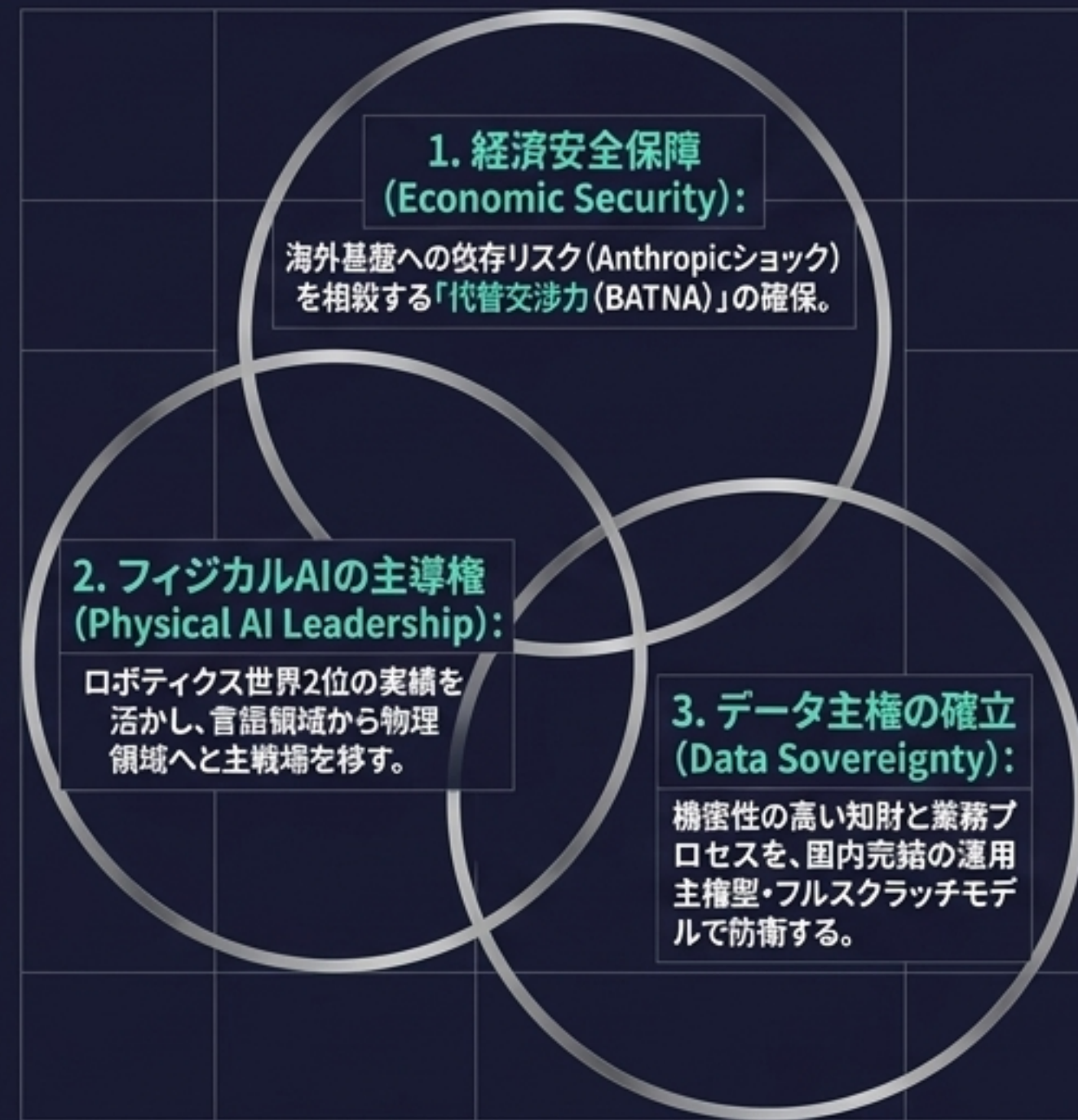
3



現場データの「AI-Ready化」と営業秘密管理

GENIACの支援対象でもある「製造業データのAI-Ready化」を推進。同時に、これらのデータセットが学習用素材として流出しないよう、アクセス制限や秘密表示など営業秘密（不正競争防止法）としての管理体制を再構築する。

国産AIは、米国モデルに
勝つための「剣」ではない。
予測不能な地政学リスクから
企業を守る「盾」であり、
日本の産業データを次世代の
価値へ変換する「基盤」である。



主権の設計図は完成した。あとは、実装するのみである。