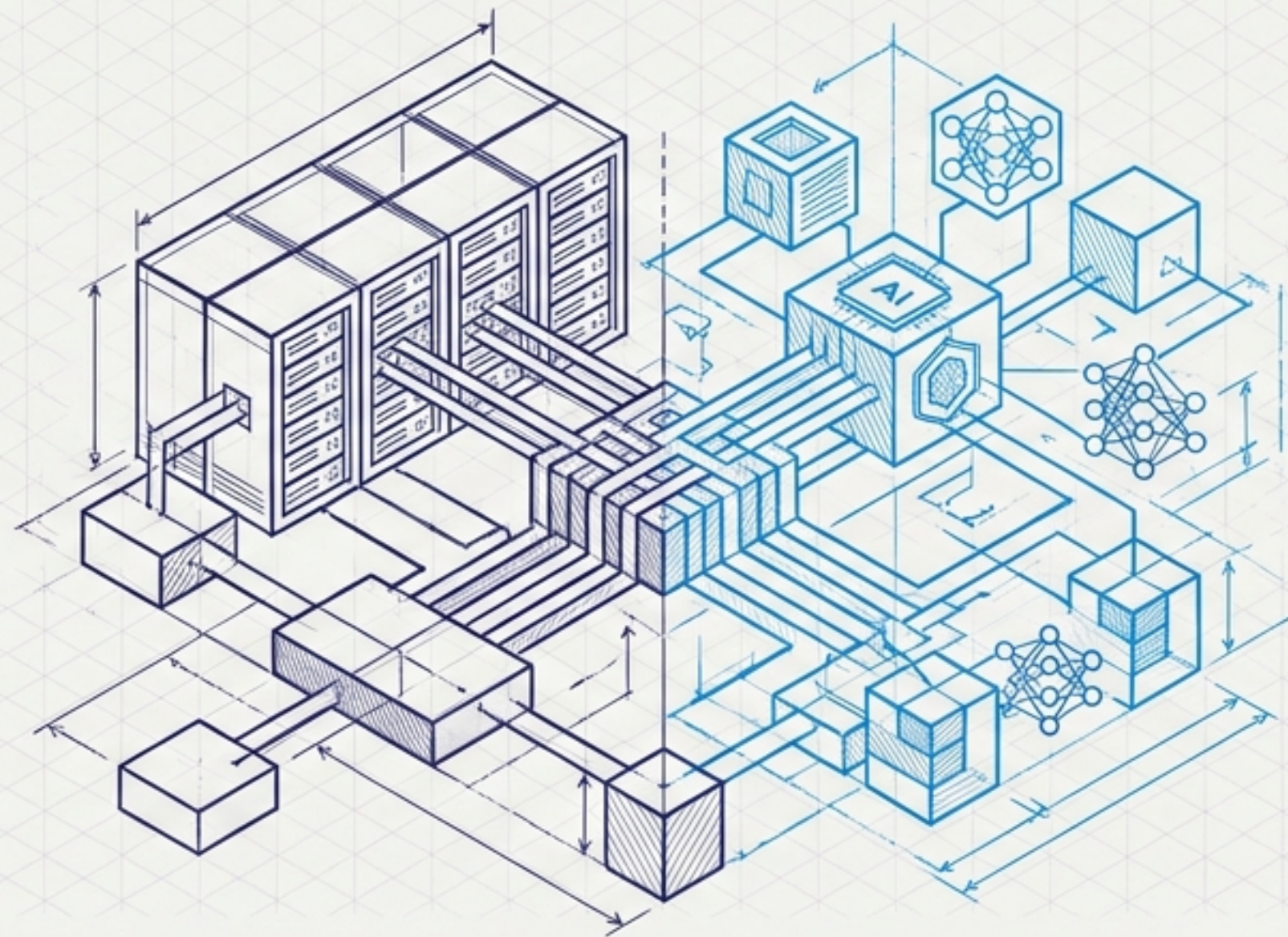




日本「ガバメントAI 源内」vs フランス「Albert API」

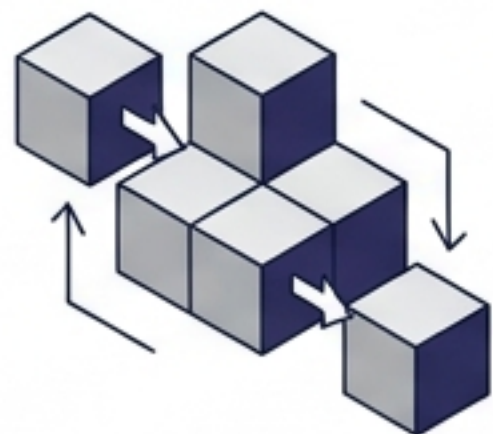
政府AI基盤における2つの設計思想と、次世代アーキテクチャへの示唆



Date: 2026年10月最新調査報告

Theme: 比較構造・ガバナンス・アーキテクチャ・運用実態

Executive Summary: 本レポートの4つの核心



前提の是正

「源内」と「Albert API」は同列の比較ではない。源内は「統合アプリ環境」、Albertは「推論API基盤」である。正しい比較構造を再定義する。



基本思想の対比

実用性とスピードを優先し米国商用モデルに依存する日本（アジリティ優先）と、主権確保のためインフラとモデルを自前で統制するフランス（主権優先）。



浮き彫りになった課題

単一の海外SaaSモデルに依存する日本のアーキテクチャは、他国の輸出規制などの地政学的リスクに対して脆弱性を持つ。



日本への5つの提言

2027年度の本格稼働に向け、API層層の分離、モデル切替先の確保、費用の共同負担ルールなど、フランスの事例から取り入れるべき具体策。

比較前提の再定義：なぜ「源内 vs Albert API」はアンフェアなのか

Visual Equation



源内

≠



Albert API

源内は全レイヤーを含むが、Albert APIは推論基盤のみ。



源内 (チャット+30種の業務アプリ+RAG)

=



L'Assistant等の
エンドユーザー向け製品

Albert API (DINUM運用のOpenAI互換API基盤)

フェアな比較は「源内」対「Albert API + L'Assistant」である。日本は「すべてが揃った場」を提供し、フランスは「再利用可能な部品 (API)」の提供に徹している。

設計思想の根本的対立：「実用優先」か「主権優先」か

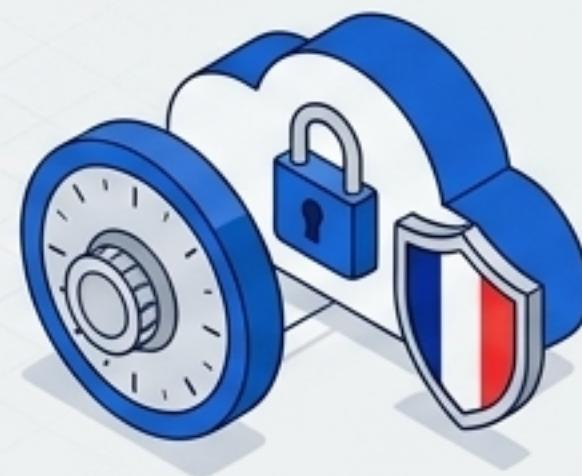
AI基盤設計の哲学

日本：実用優先 (Utility First)



- アプローチ：「隼より始めよ」。ガバメントクラウド（AWS中心）上で米国の高性能商用モデル（Claude等）を即座に利用可能にし、業務効率化を急ぐ。
- 国産育成：国産LLMは試用（さくらのクラウド上でA/Bテスト）から始め、2027年度から段階的に有償調達へ。

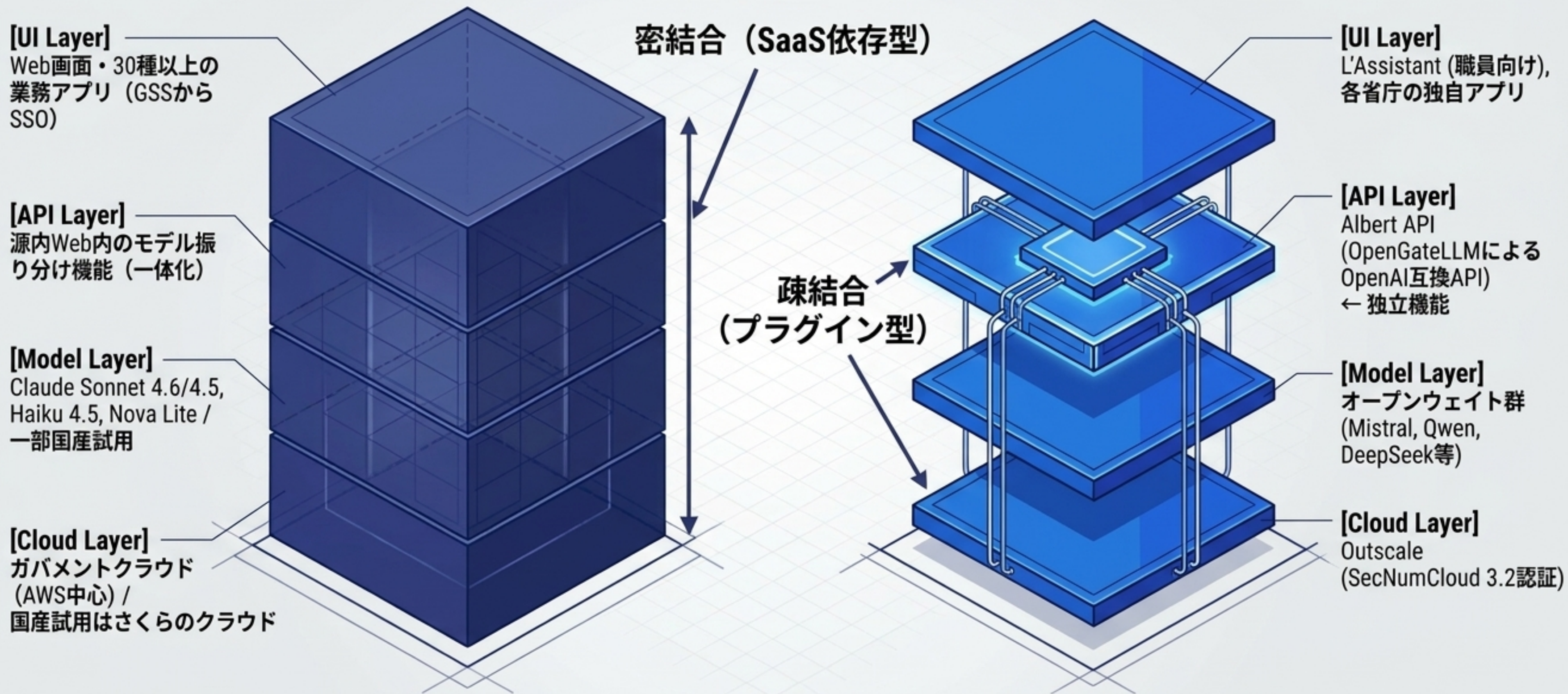
フランス：主権優先 (Sovereignty First)



- アプローチ：クラウド、ソフトウェア、モデルの全階層を国内または欧州で統制する。
- 主権の三本柱：
 1. **インフラ**: SecNumCloud認証（米国CLOUD Act等の域外適用を排除）
 2. **ソフトウェア**: 自社開発OSS（OpenGateLLM）
 3. **モデル**: オープンウェイト（Mistral等）の自前ホスティング

日本は「今すぐ使える利便性」を買い、フランスは「自律的なコントロール権」を構築している。

アーキテクチャ・スタック解剖：密結合（日） vs 疎結合（仏）

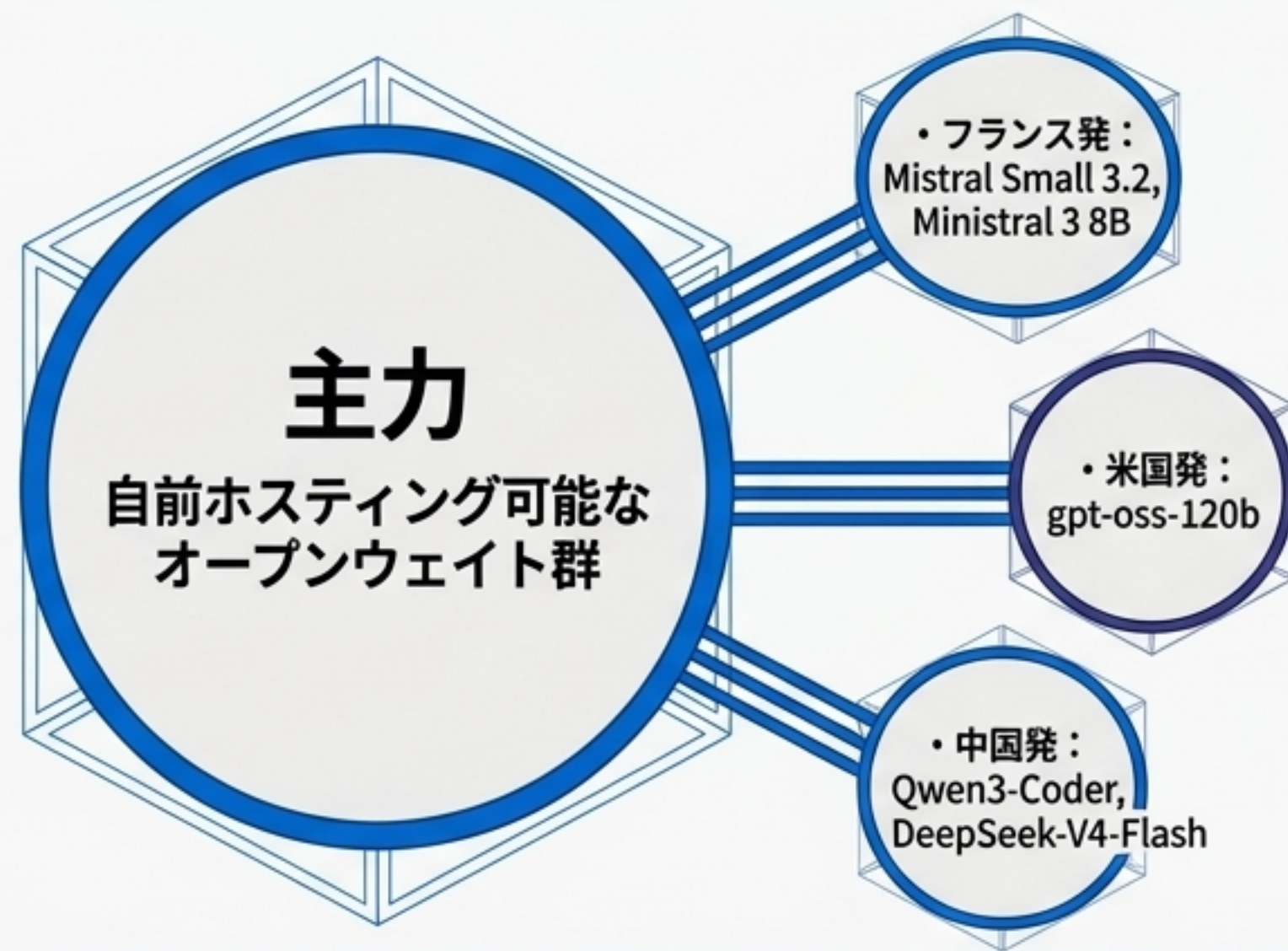


AIモデル選定戦略：商用SaaS依存とオープンウェイトの自前ホスティング

日本：米国商用SaaS + 国産LLM育成



フランス：オープンウェイトの自前ホスティング



主権の再定義：フランスの「主権」とは、モデルの開発国のことではない。「自国インフラ (SecNumCloud) で自律的にホスティングし、コントロールできるか」を重視している。

データ・セキュリティとガバナンス： 「運用ルール」vs「インフラレベルの遮断」



日本：ガイドライン主導 (Guideline-Driven)

- 運用体制: 各府省にCAIO（AI統括責任者）を設置。
- ルール: 「生成AI調達・利活用ガイドライン（第2.0版: 2026年6月12日）」による運用。
- データ保護: 機密性2情報まで入力可（デジタル庁基準）。

※弱点: Claude利用時のデータ保存場所や学習除外の契約的担保は公開資料上では不透明。

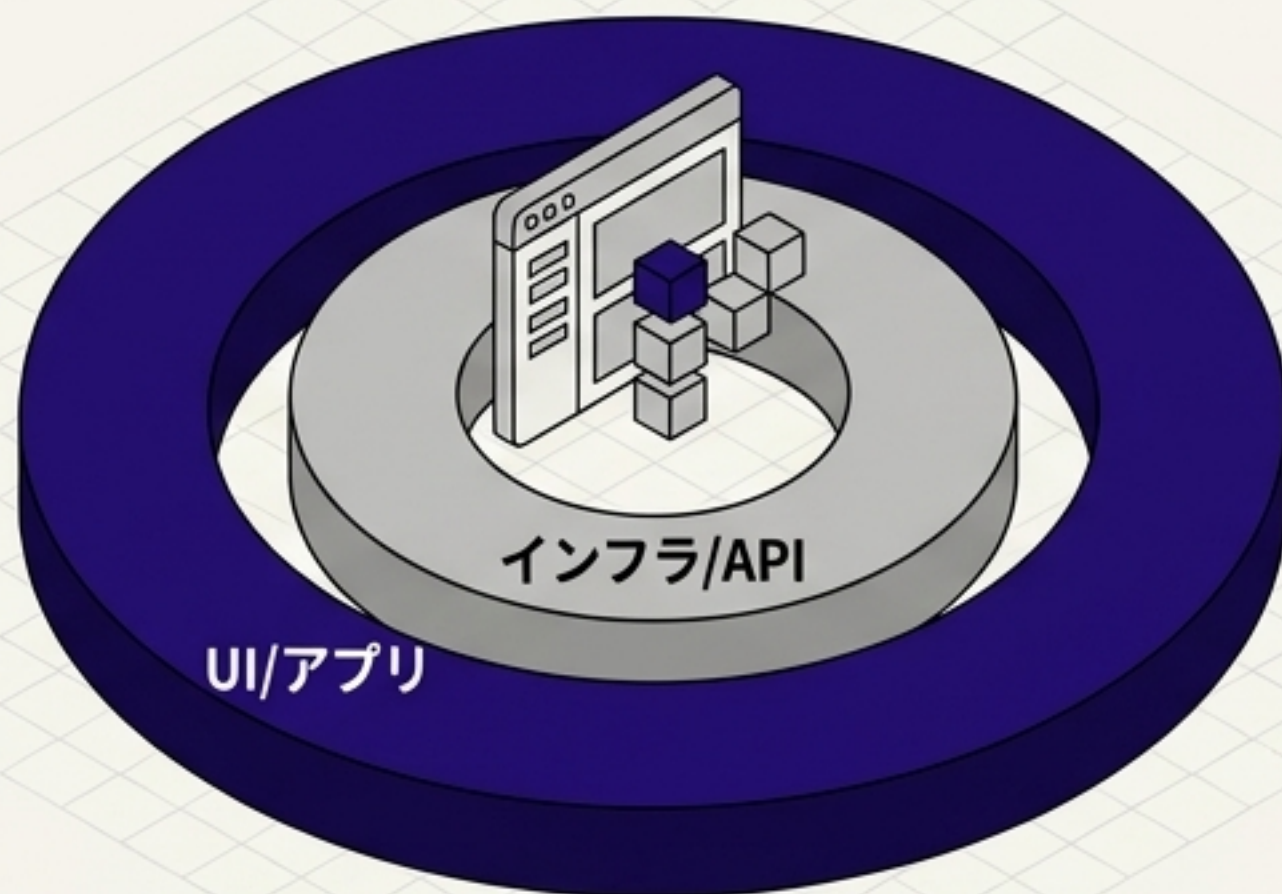


フランス：インフラ主導 (Infrastructure-Driven)

- インフラ認証: Outscaleによる「SecNumCloud 3.2」。外国法の域外適用（米CLOUD Act等）を物理的・法的に排除。
- システム仕様: 推論経路でデータを一切保存しない仕様を公表し、「ホモロゲーション（安全性の公式認定）」を2025年夏に取得済み。

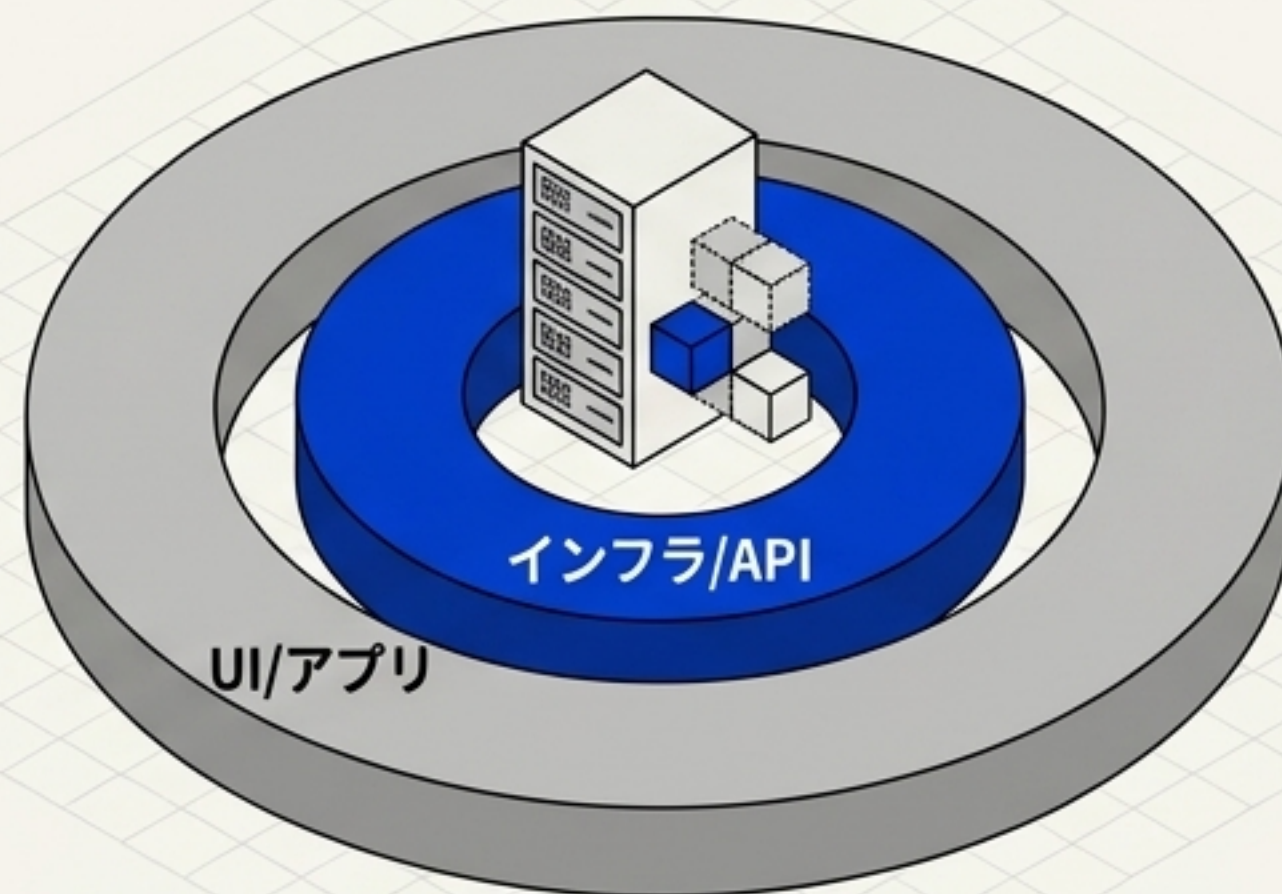
オープンソース（OSS）戦略：「UIの参照実装」vs「推論基盤の丸ごと公開」

日本：外層（UI/アプリ）に焦点



- **公開対象:** Web画面（genai-web）とAIアプリのテンプレート（2026年4月24日公開）。
- **目的:** 調達時の参照実装、自治体の重複開発防止。

フランス：中心核（インフラ）に焦点



- **公開対象:** 基盤ソフトウェア「OpenGateLLM」全体をGitHub等で公開。AgentPublicなどの追加学習モデルもHugging Faceで公開。
- **目的:** 他の行政機関が自前で独自のAIゲートウェイを構築できるようにする。

結論：フランスのアプローチ（入口層のOSS化）は、モデルやクラウドに依存しないため、他機関からの再利用性が圧倒的に高い。

規模と効果測定：「利用回数」の日本 vs 「行動科学的評価」のフランス

規模とトラフィックの追及

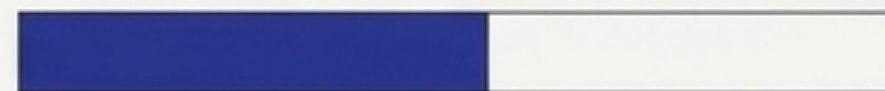


- 対象: 39機関・約18万人対象の大規模実証 (2026年5月開始時点約10万人が利用可能)。
- 初期実績: デジタル庁内試験で約8割利用、3ヶ月で延べ6.5万回。

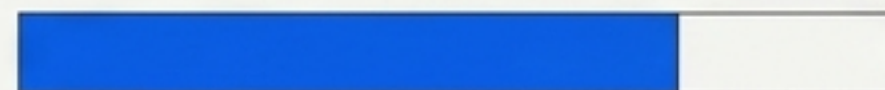
※課題: 管理職の利用率低迷 (二極化)。定量的な業務効率化データは未公表。

行動科学と業務品質の測定

メール作成: 21分 → **19分 (12%短縮)**



記事要約: 33分 → **28分 (16%短縮)**

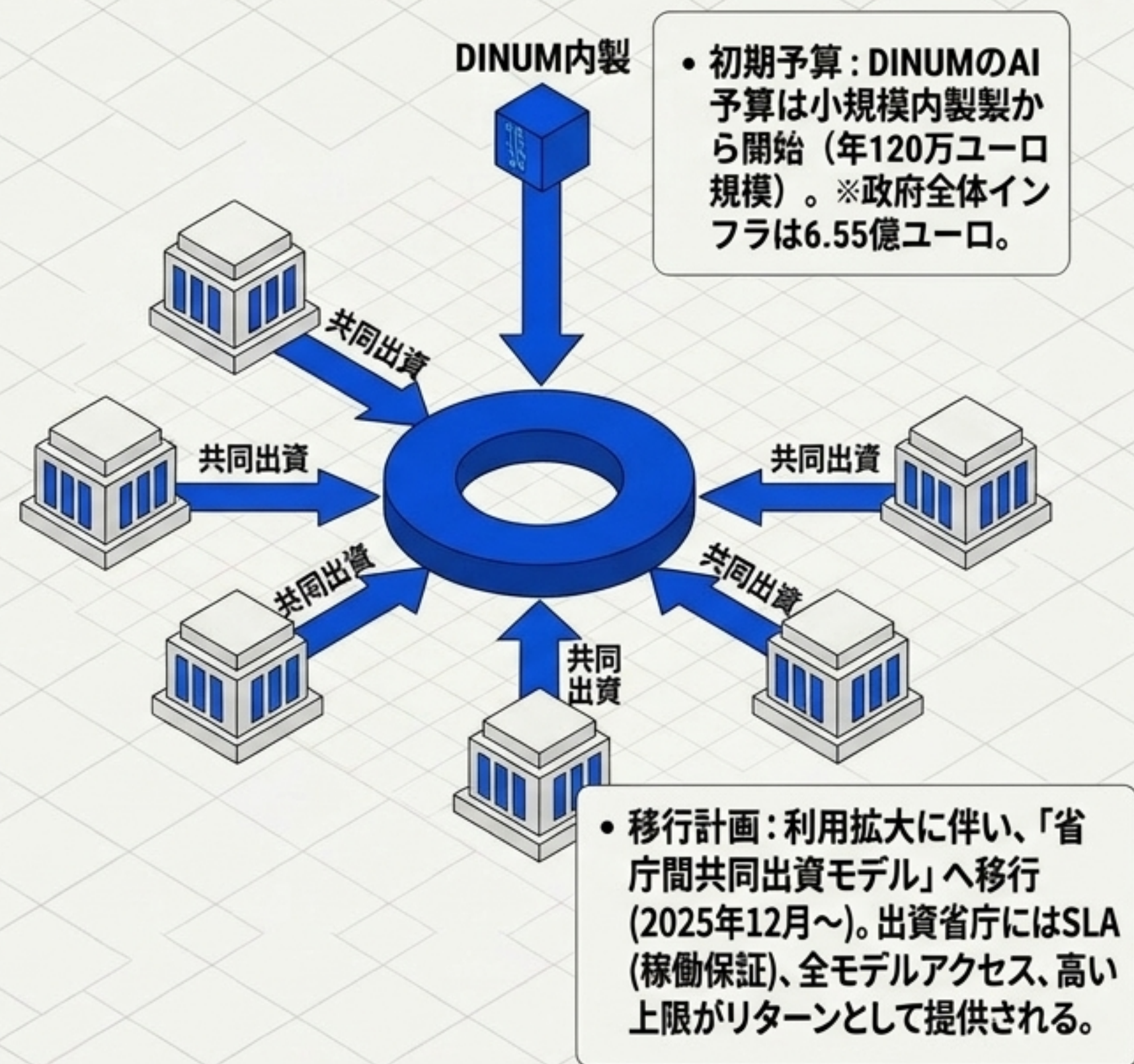
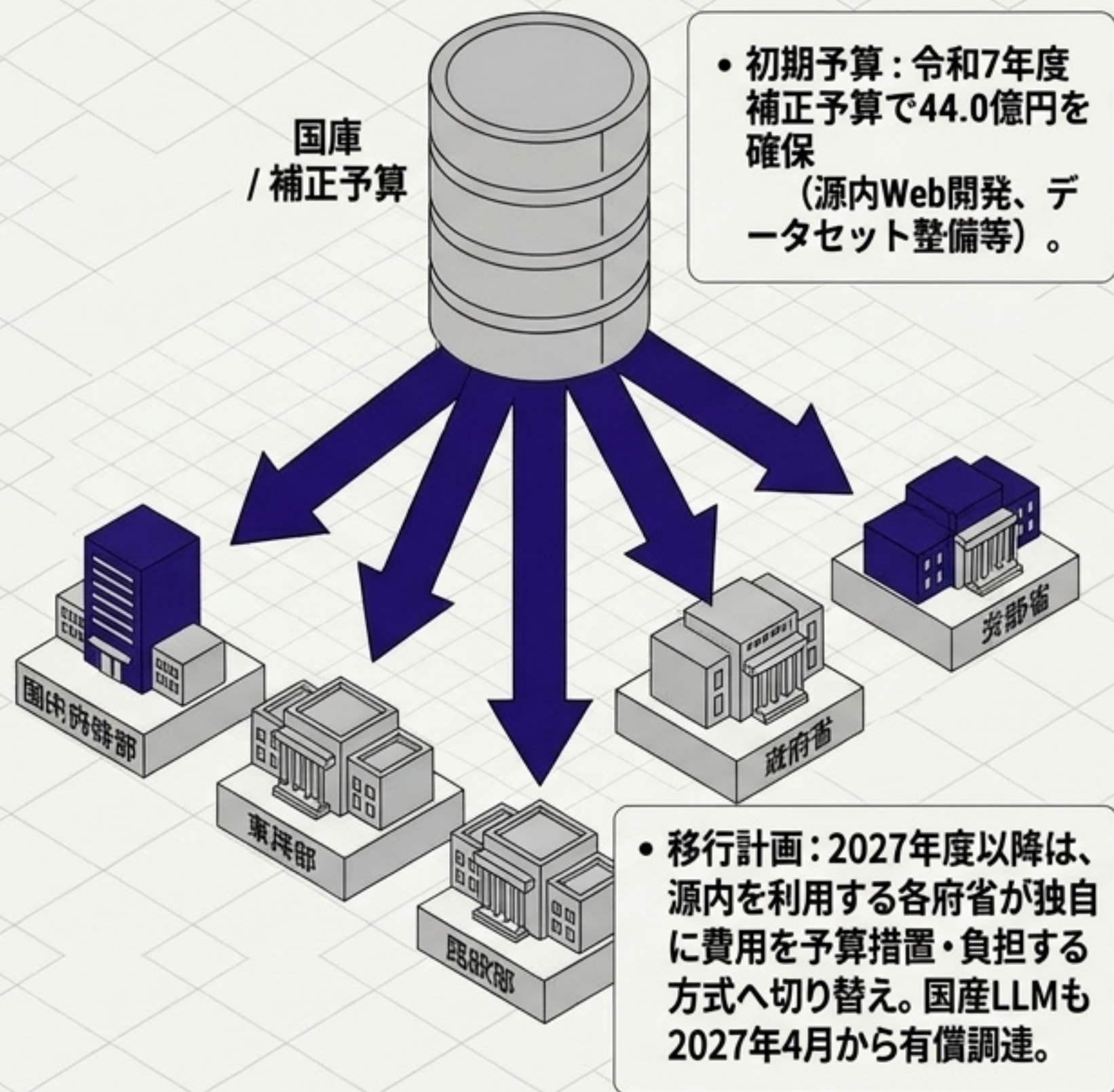


品質スコア向上
+0.95~1.28点 / 20点満点

- L'Assistant効果測定 (DITP・研究機関合同評価): 70件以上の公共PJ、週10万件以上のリクエスト。

※課題: 76%が「誤り」を懸念。

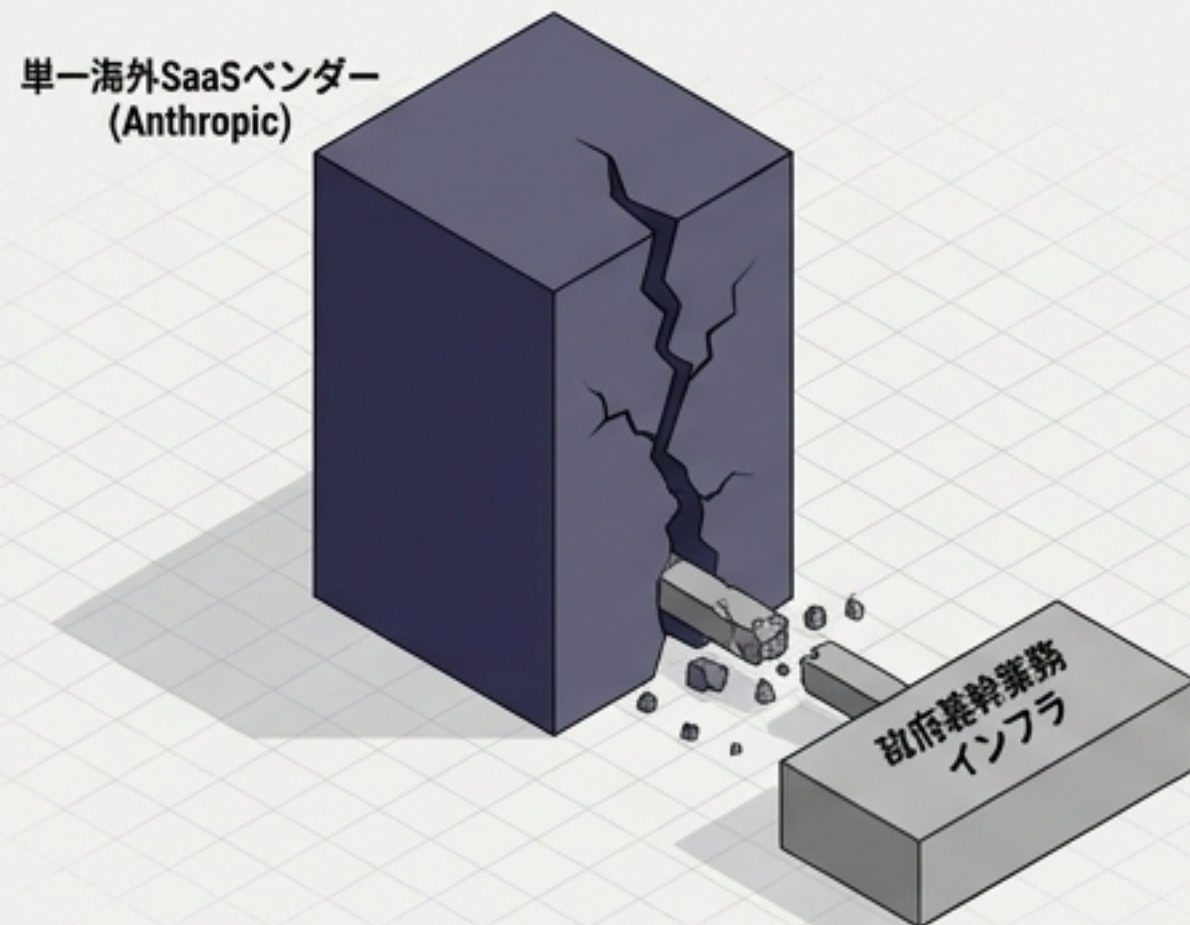
予算と調達構造：トップダウンの大型予算 vs 省庁間共同出資モデル



【インサイト】 浮き彫りになったリスク：「単一海外SaaS依存」の脆弱性

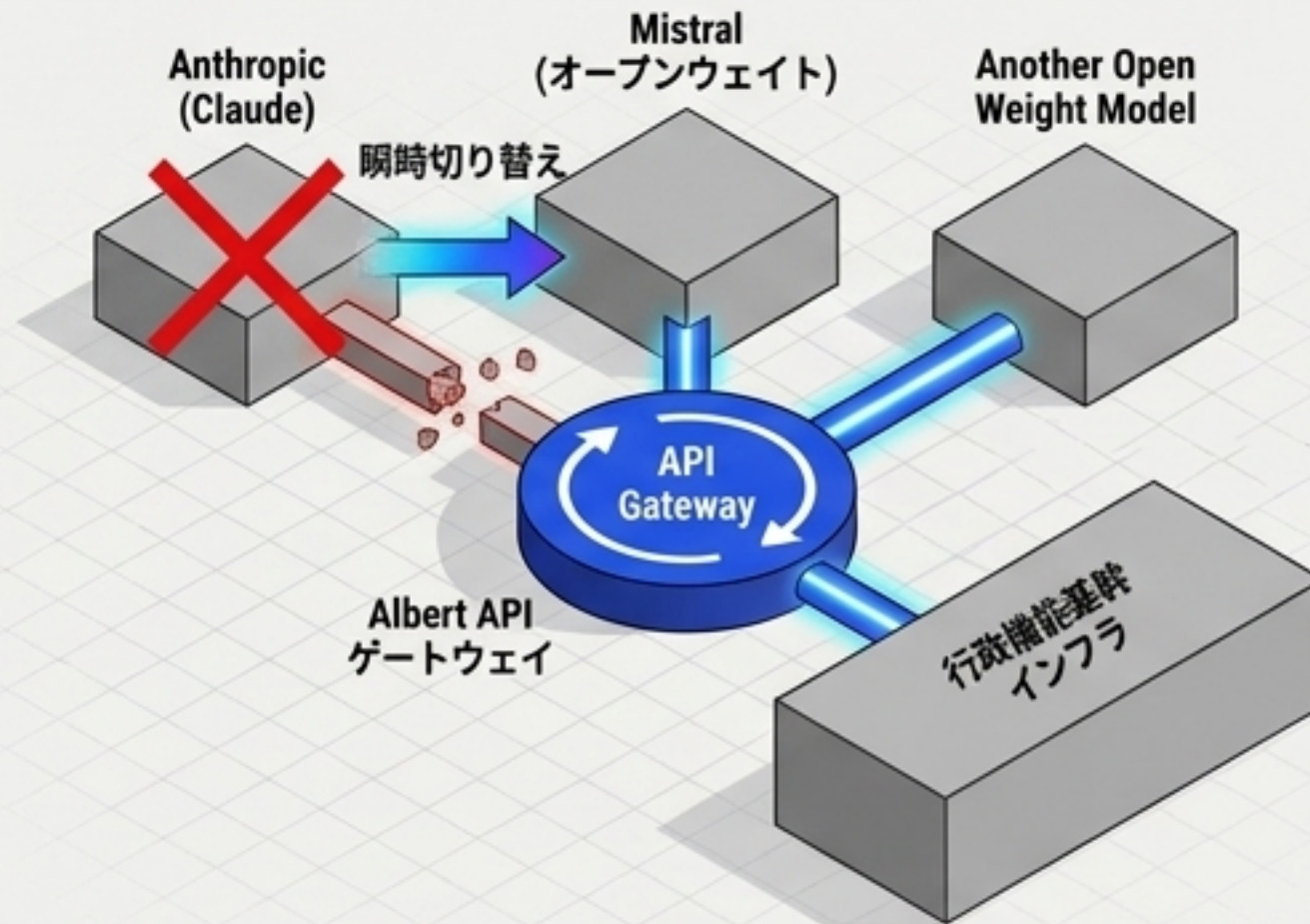
事象（2026年6月12日）：米国政府の輸出管理指令により、Anthropic社が「Claude Fable 5」「Mythos 5」へのアクセスを突如停止（7月1日解除）。

日本の教訓：源内が使用するSonnet/Haikuは対象外だったものの、「他国政府の判断で、政府の基幹業務インフラが突然停止するリスク」が露呈した。



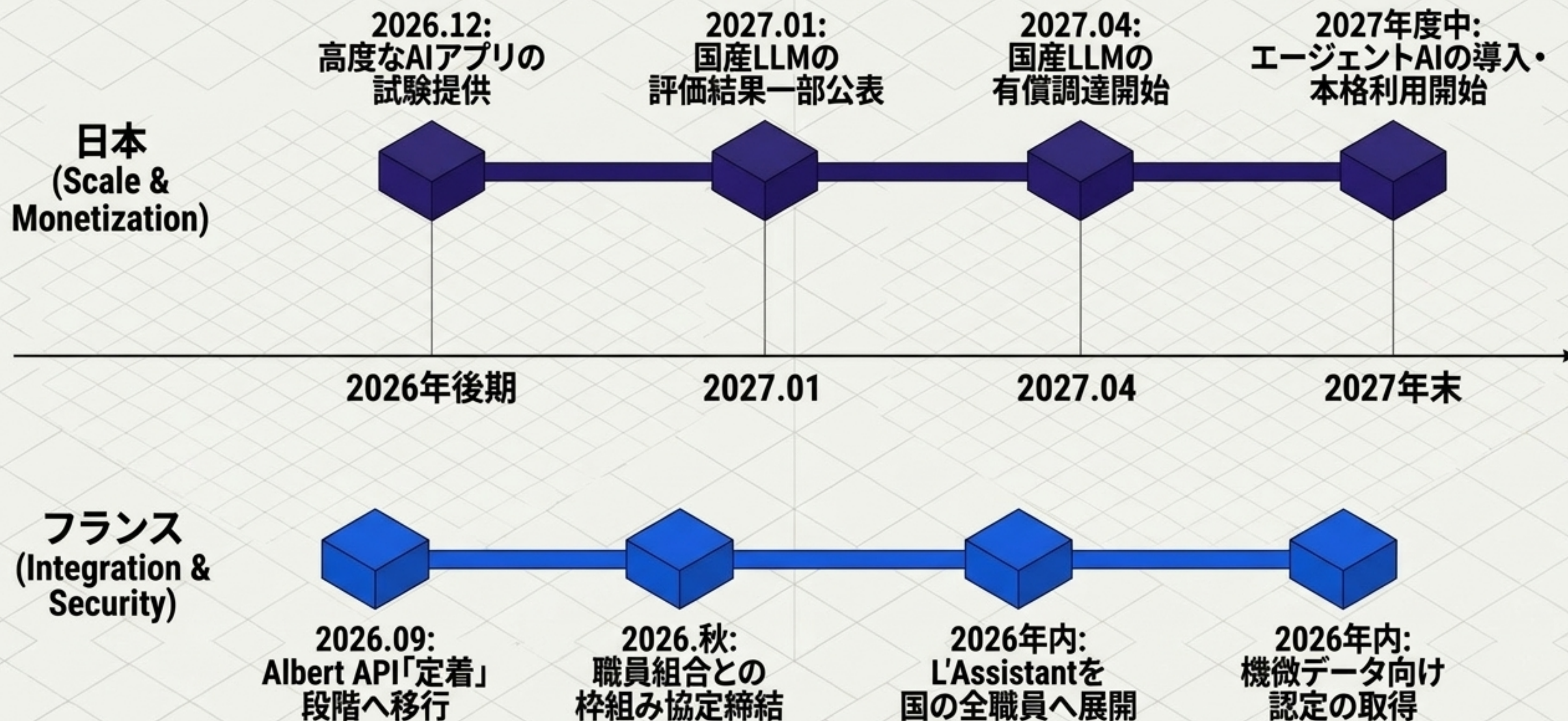
日本の教訓：源内が使用するSonnet/Haikuは対象外だったものの、「他国政府の判断で、政府の基幹業務インフラが突然停止するリスク」が露呈した。

フランスの回避策：Albert APIのような「APIゲートウェイ」を自前で握っていれば、に瞬時に切り替えることで、行政機能の停止を防ぐことができる。



フランスの回避策：Albert APIのような「APIゲートウェイ」を自前で握っていれば、特定モデルへのアクセスが遮断されても、裏側で別のオープンウェイトモデル (Mistral等) に瞬時に切り替えることで、行政機能の停止を防ぐことができる。

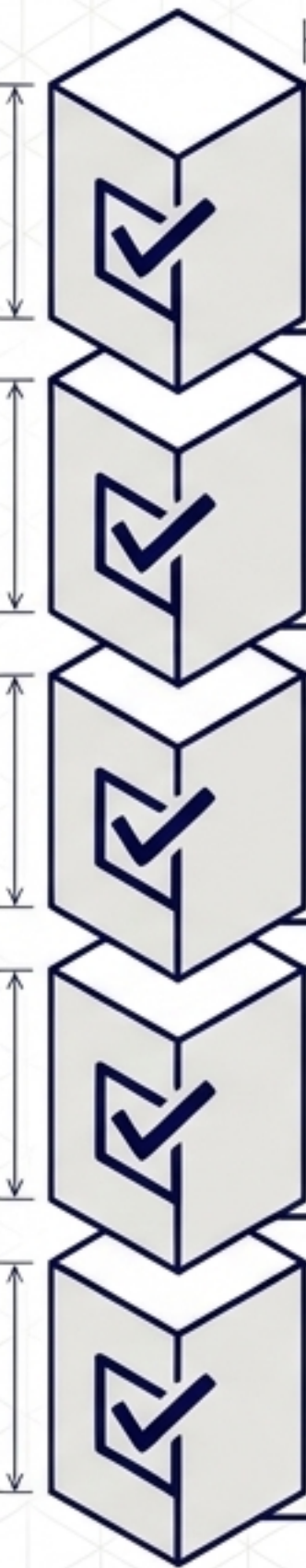
2026-2027 ロードマップ：本格利用への移行と定着



総合比較マトリクス：日仏アーキテクチャの構造的差異

観点	日本（源内）	フランス（Albert API + 関連製品）
設計思想と対象	統合環境による利便性・ 18万人規模展開	推論APIとしての汎用性・ 主権確保
アーキテクチャ・ スタック	SaaS密結合 (UI～Cloudの一体提供)	疎結合 (API層の独立分離、モジュール型)
モデルと主権	米国商用モデル依存 + 国産育成	自前ホスティング+オープンウェイト (国籍不問)
ガバナンスと評価	ガイドライン運用・ 利用回数重視	SecNumCloud認証（インフラ統制）・ 行動科学的評価

戦略的提言：2027年度本格稼働へ向けた5つのアクション



1. モデル切替先の確実な担保

輸出規制等の地政学リスクに備え、2027年度の調達要件に「代替モデルへの切り替えやすさ」を明記する。

2. 府省共通 API層の分離・提供

源内のモデル振り分け機能を独立させ、OpenGateLLMのような共通APIとして公開し、自治体の重複投資を防ぐ。

3. 費用負担ルールの早期提示

フランスのSLA連動型の共同出資方式を参考に、各府省が納得する2027年度の算定方法を2026年度中に策定する。

4. 独立機関による定量的効果測定

利用回数だけでなく、DITPにならい研究機関を交えた業務時間短縮・品質向上の数値化を行う。

5. 「AI主権」の定義のアップデート

国産モデルに固執するのではなく、「機密区分に応じたインフラの国内管理」へと方針を精緻化する。

結論：真の「AI主権」とは何か？

**「AI主権」とは、自国製のモデルを生み出すことだけを意味しない。
どの国のモデルであれ、自国のインフラ上でホスティングし、
APIゲートウェイを通じて『制御権』を完全に掌握することである。**

2027年度の本格稼働に向けて、**日本**は「**実用性の追求** (アプリ層)」を維持しつつ、**フランス**の「**統制力** (API/インフラ層)」の思想をアーキテクチャに組み込むハイブリッド戦略への転換が求められている。