「ソブリンAI」は何を“主権化”するのか

富士通・日立・AWSの競争軸と、日本企業がとるべきAI主権戦略の青写真



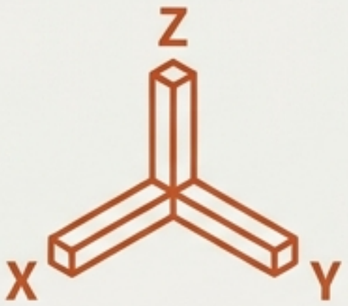
Gemini Notebook

ソブリンAIとは「国産製品の導入」ではなく、AIシステム全体における「支配権のポートフォリオ設計」である。



脱・オンプレミス信仰

サーバーが自社建屋にあっても、暗号鍵や運用権限を外部に依存していれば主権はない。物理的配置だけでなく、論理的・運用的な9つの「統制権」が問われている。



三者三様の競争軸

ベンダー戦略は排他的ではない。富士通（フルスタック所有）、日立（現場データと運用統制）、AWS（グローバル技術の境界内制御）は、全く異なる価値を提供する。



開かれたAI主権

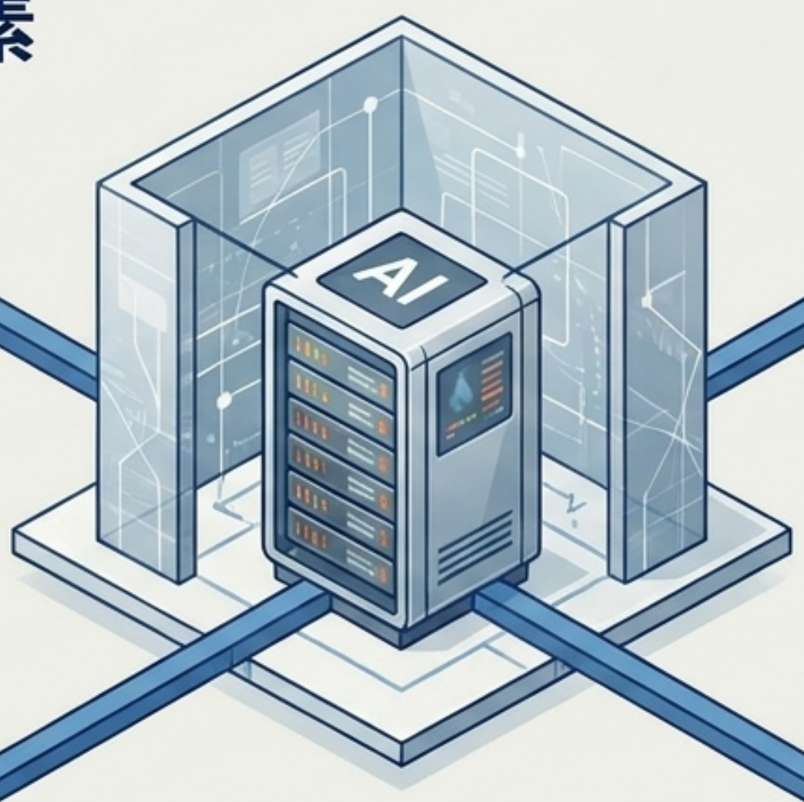
日本政府が目指すのは完全国産閉鎖系ではなく、複数選択肢による「戦略的自律性と耐遮断性」。企業も「AI版BCP」として主権要件を定義するフェーズにある。

Gemini Notebook

ソブリンAI つの主権要素

モデル更新：
外部ベンダーに依存していないか？

暗号鍵：
海外の制御プレーンに送信されていていないか？



管理者アクセス：
外部ベンダーが特権IDを保持していないか？

サプライチェーン：
構成部品（メモリ・EDA）のトレーサビリティはあるか？

物理的なデータの所在（Data Residency）だけでは不十分。
これら9要素について「誰がどこまで支配できるか」が真の主権である。

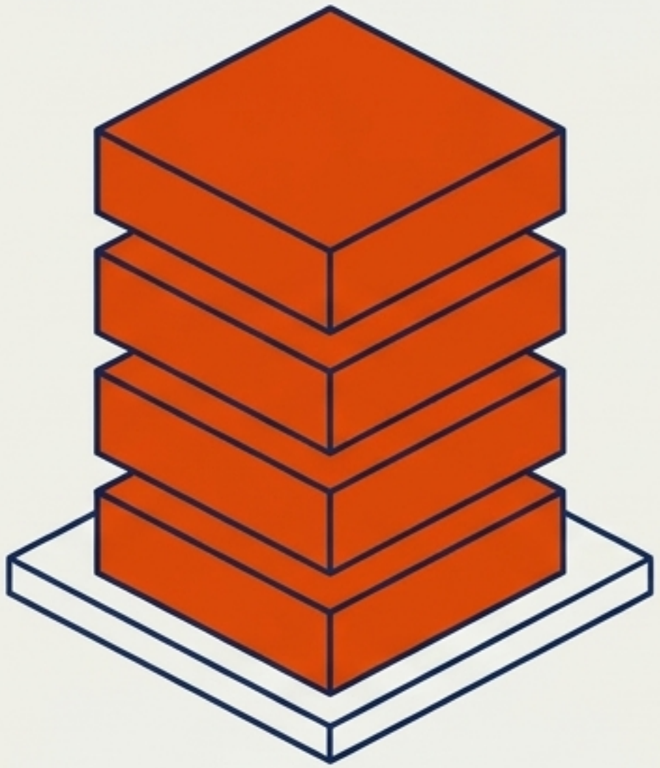
評価すべき9つの主権要素

データ	モデル	計算資源	暗号鍵	管理権限	運用者	監査ログ	サプライチェーン	切替可能性

Gemini Notebook

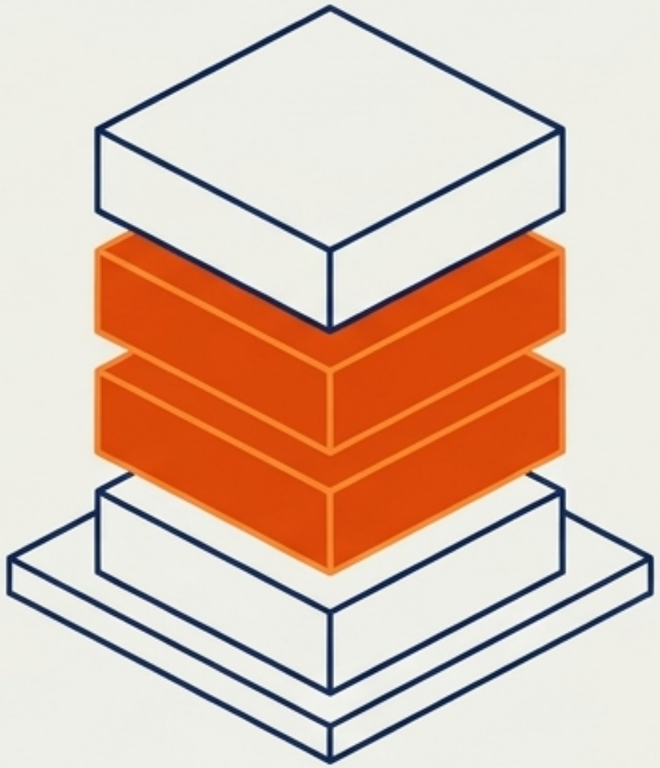
ソブリンAIアプローチの比較

【富士通】国産スタックの所有



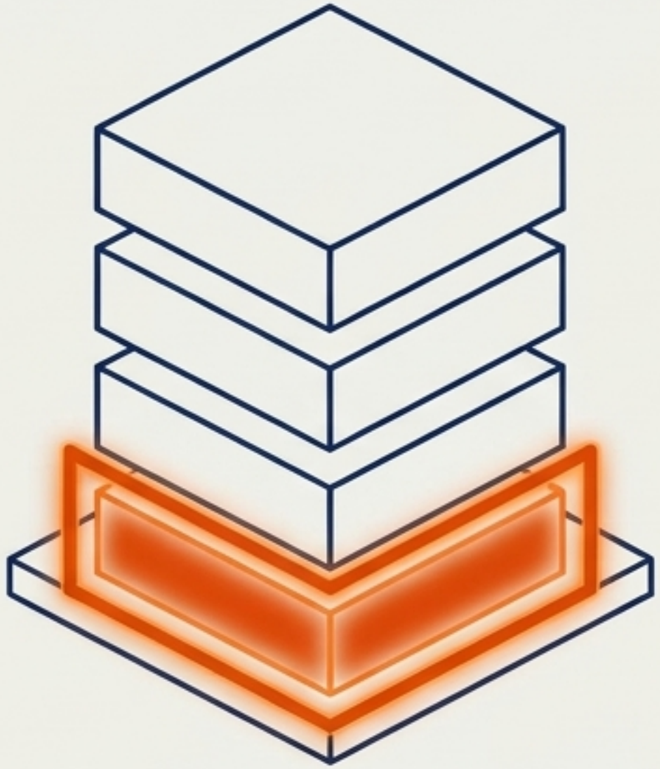
CPUからLLMまでを自社・国内製造で垂直統合し、サプライチェーンの透明性を担保するアプローチ。

【日立】現場と運用の掌握



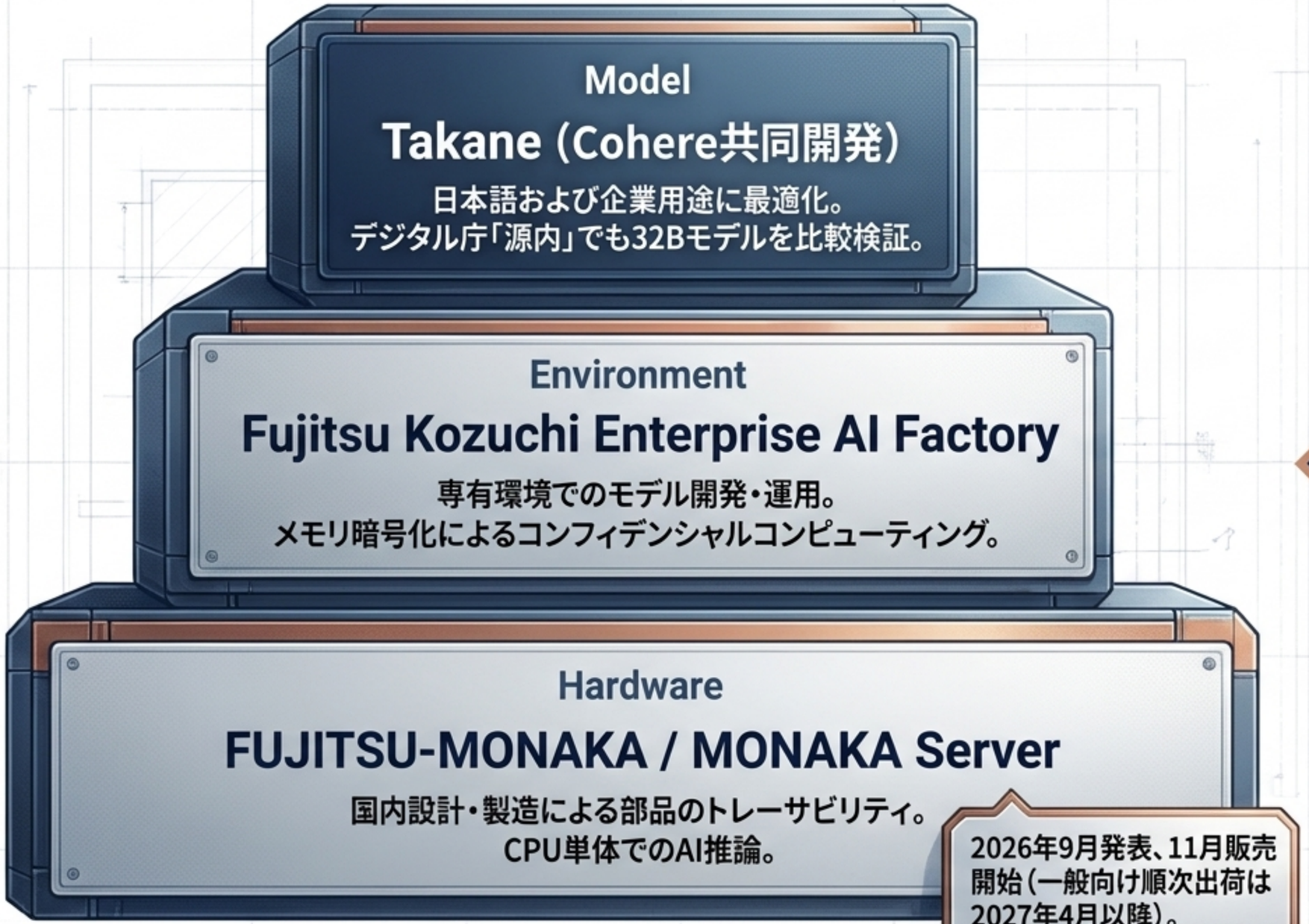
現場のOTデータや暗黙知を構造化し、AIのハルシネーションやガバナンスを継続監視する運用主権アプローチ。

【AWS】グローバル技術の境界内制御



ハイパースケーラーの利便性を維持しつつ、データプレーンと制御プレーンを技術的に切断するアプローチ。

Gemini Notebook



日本政府が求める「国内製造・完全国産スタック」に対する最強の受け皿。
課題はNVIDIA/CUDAエコシステムへの対抗。

Gemini Notebook

国産モデル開発ではなく、
組織固有の「現場データ」と
「設備制御ルール」の主権を
企業側に残す戦略。



鉄道・電力・製造などの
社会インフラ現場。

HMAX Data Fabric
（2026年9月提供）

IT/OTデータと熟練者の暗黙知を
オントロジー/ナレッジグラフとして構造化し、
特定のLLMに依存しない知識基盤を構築。

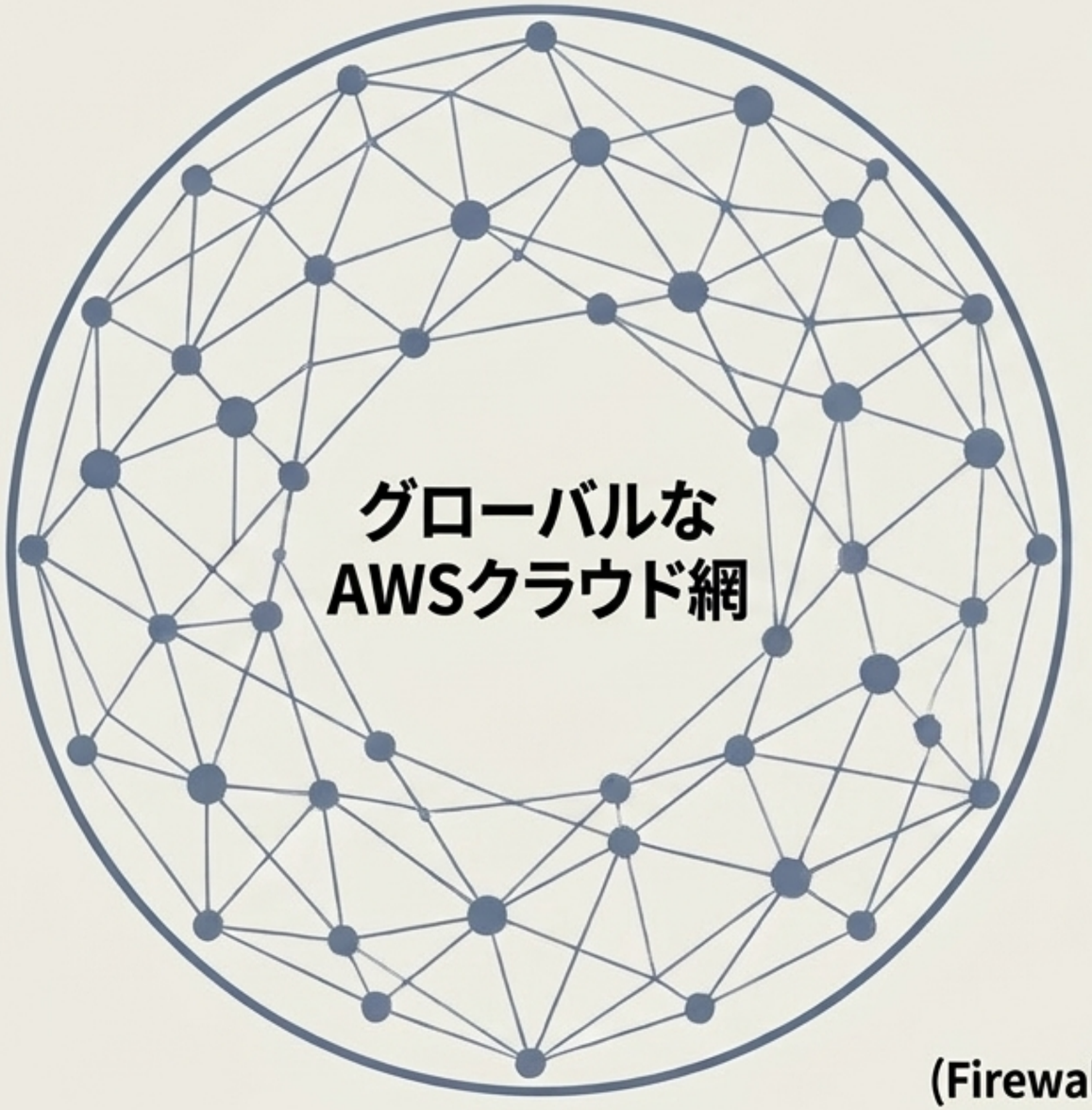
HMAX AI Operations / Physical AI FDE

AIの性能、セキュリティ、ハルシネーションを
継続監視し、物理世界を動かす
「フィジカルAI」のリスクを
運用面で抑制。

Hitachi EverFlex

プライベート/マルチテナント、暗号化、法規制対応を備えた透明性の高いクラウド基盤。

Gemini Notebook



境界
(Firewall / Boundary)

AWS European Sovereign Cloud
(2026年1月GA)

物理/論理分離。EU内データ・運用者居住要件・独立IAM。
(2026年10月に域外切断演習を実施)

AWS AI Factories
(2025年12月提供)
顧客の自社データセンター内にAWS専用AI基盤 (Trainium/NVIDIA GPU, Bedrock, SageMaker) を配置。

AWS Nitro System & 外部キーストア
制御プレーンを分離し、顧客自身が暗号鍵を管理。Bedrockは顧客データを学習に利用しないことを明記。

「国産か外資か」の二元論を破壊し、技術的に主権境界を引くアプローチ。

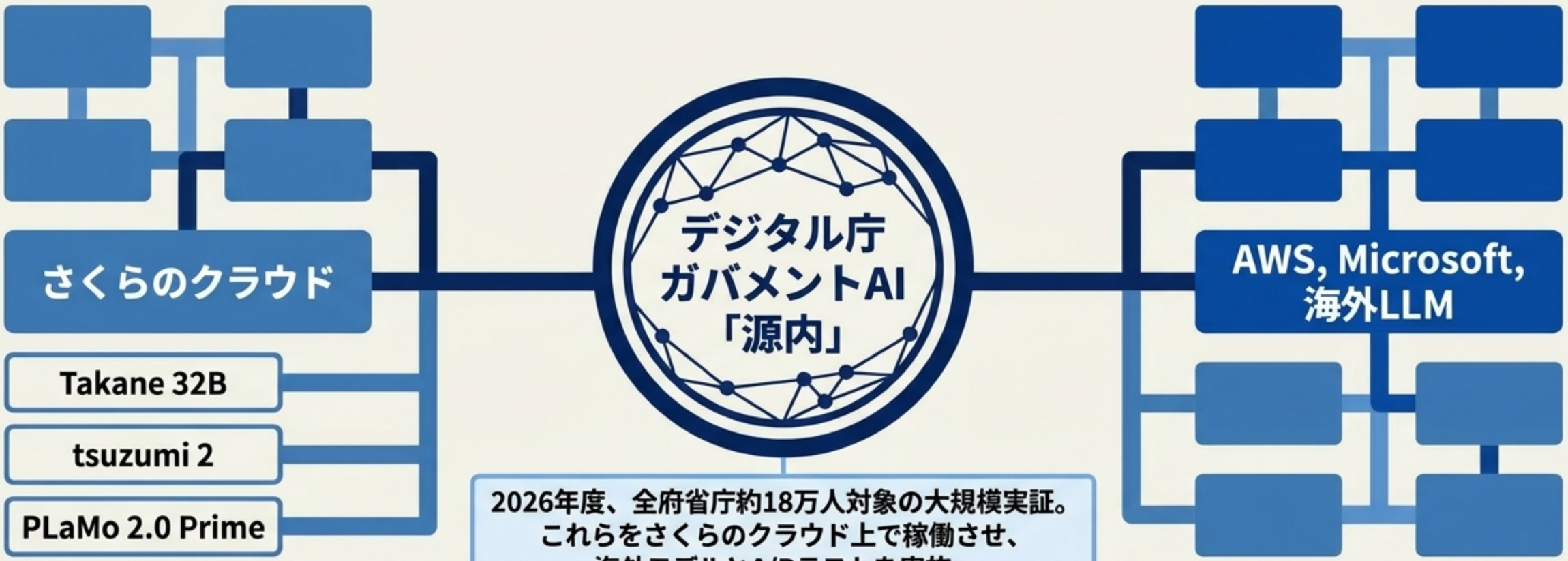
Gemini Notebook

	富士通	日立	AWS
戦略の核心	国産スタックの垂直統合と所有	IT/OT現場データと運用の統制	グローバル技術の境界内制御
主権の担保方式	国内製造・設計、コンフィデンシャルコンピューティング	オントロジーによる知識の独立、AI継続監視	Nitro、論理的/物理的分離、顧客管理鍵
収益・価格モデル	SI・専室環境・サーバー販売を含むTCO型	個別見積に基づく運用・データ基盤構築サービス	従量課金ベース（Sovereign構成により全体TCOは変動）
想定ユースケース	防衛・通信など完全国内要件が必須の領域	鉄道・電力・製造など物理制御（フィジカルAI）領域	政府・規制産業でのハイパースケールAI利用

警告：「1トークン単価」での単純比較は無意味。初期構築からMLOps、セキュリティ監査、出口費用を含めた5〜7年のTCO評価が必須である。

Gemini Notebook

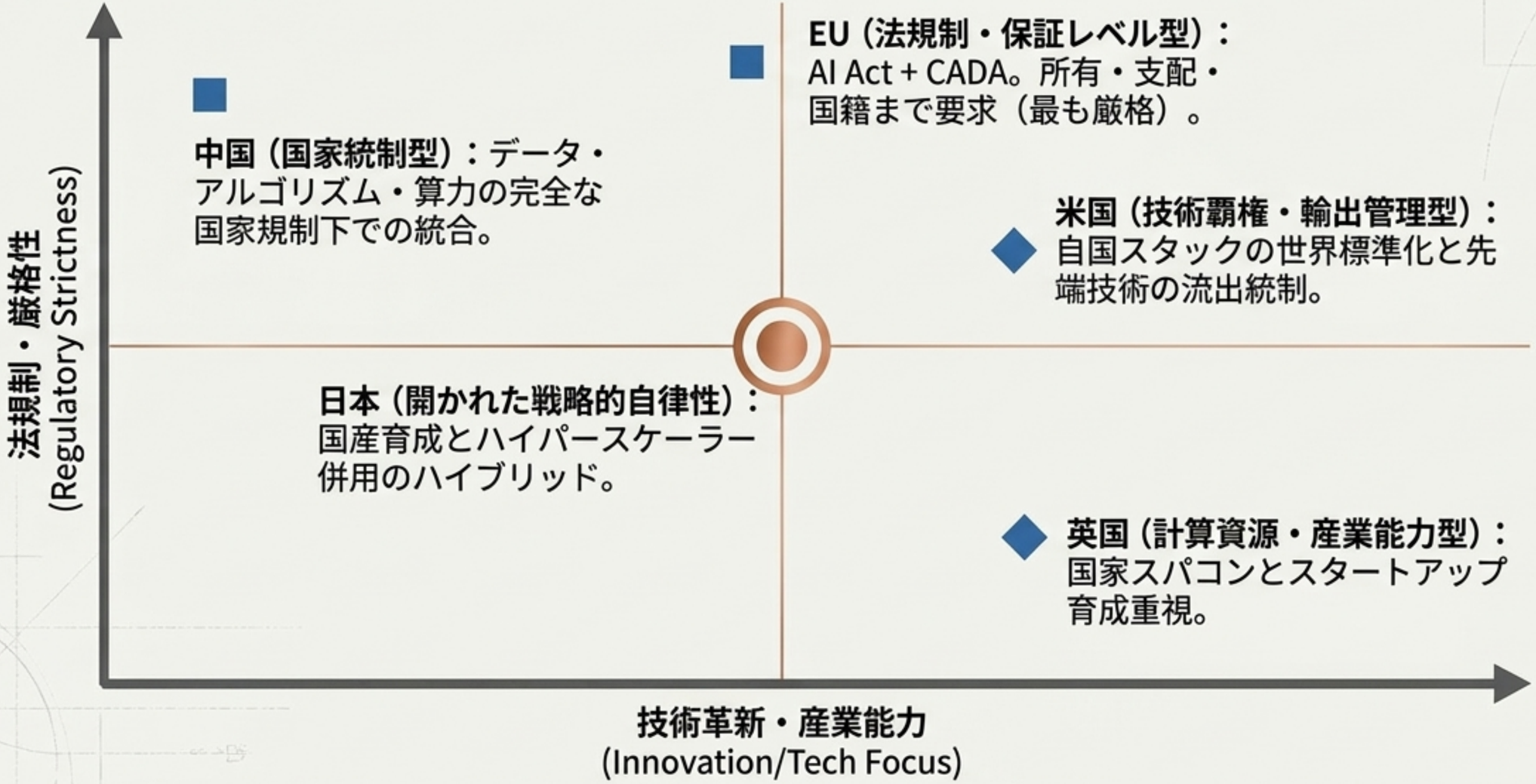
第II期人工知能基本計画（2026年7月閣議決定）：「戦略的自律性」と「戦略的不可欠性」の両立。



日本の政策は海外技術の排除ではない。依存先を複線化し、遮断や制裁が起きても代替できる「耐遮断性」と「切替可能性」を持つマルチソース構造こそが日本のAI主権である。

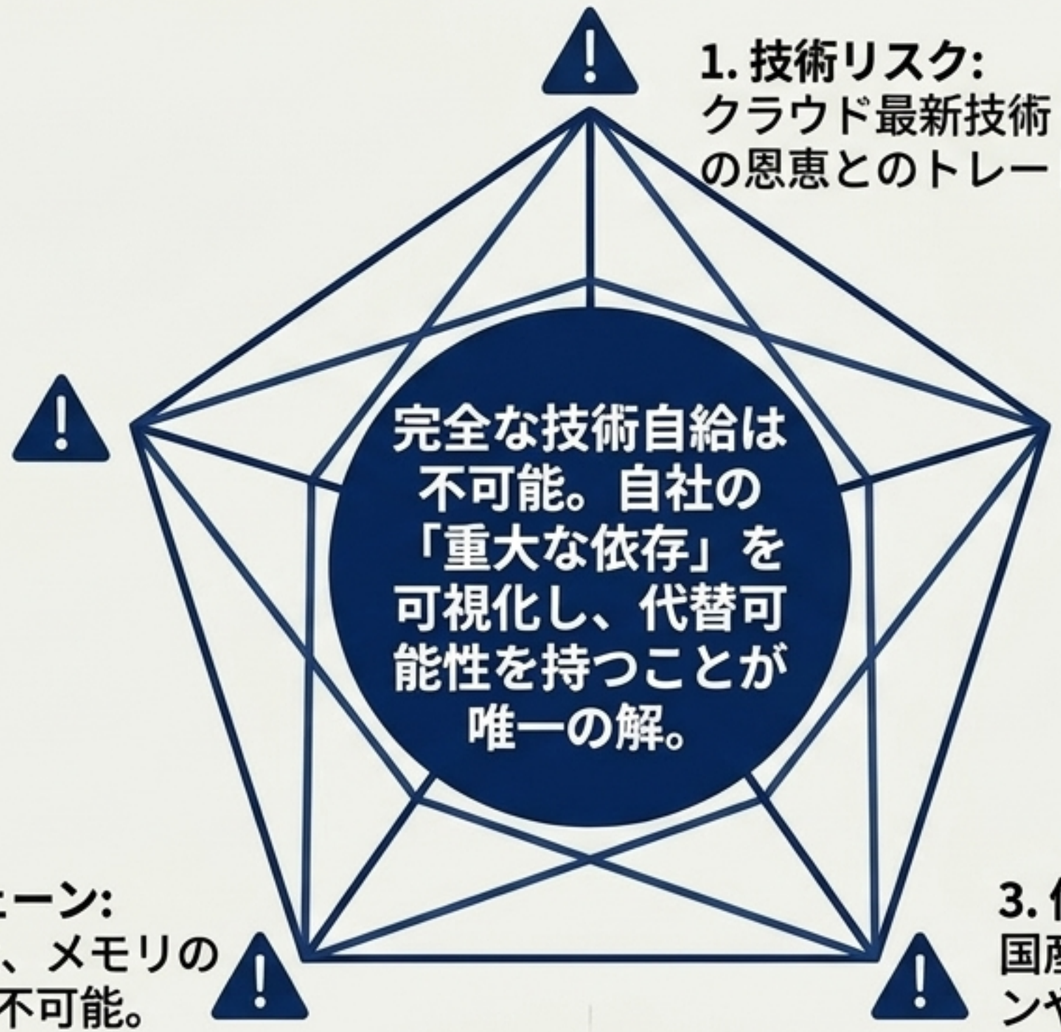
Gemini Notebook

世界各国・地域のAI主権戦略比較（2x2）



Gemini Notebook

リスク認識：完全な技術自給の不可能性と重大な依存



1. 技術リスク:
クラウド最新技術（GPU更新等）の恩恵とのトレードオフ。

2. 法務リスク:
個人情報、知財、越境移転、海外規制（EU AI Act等）の複雑化。

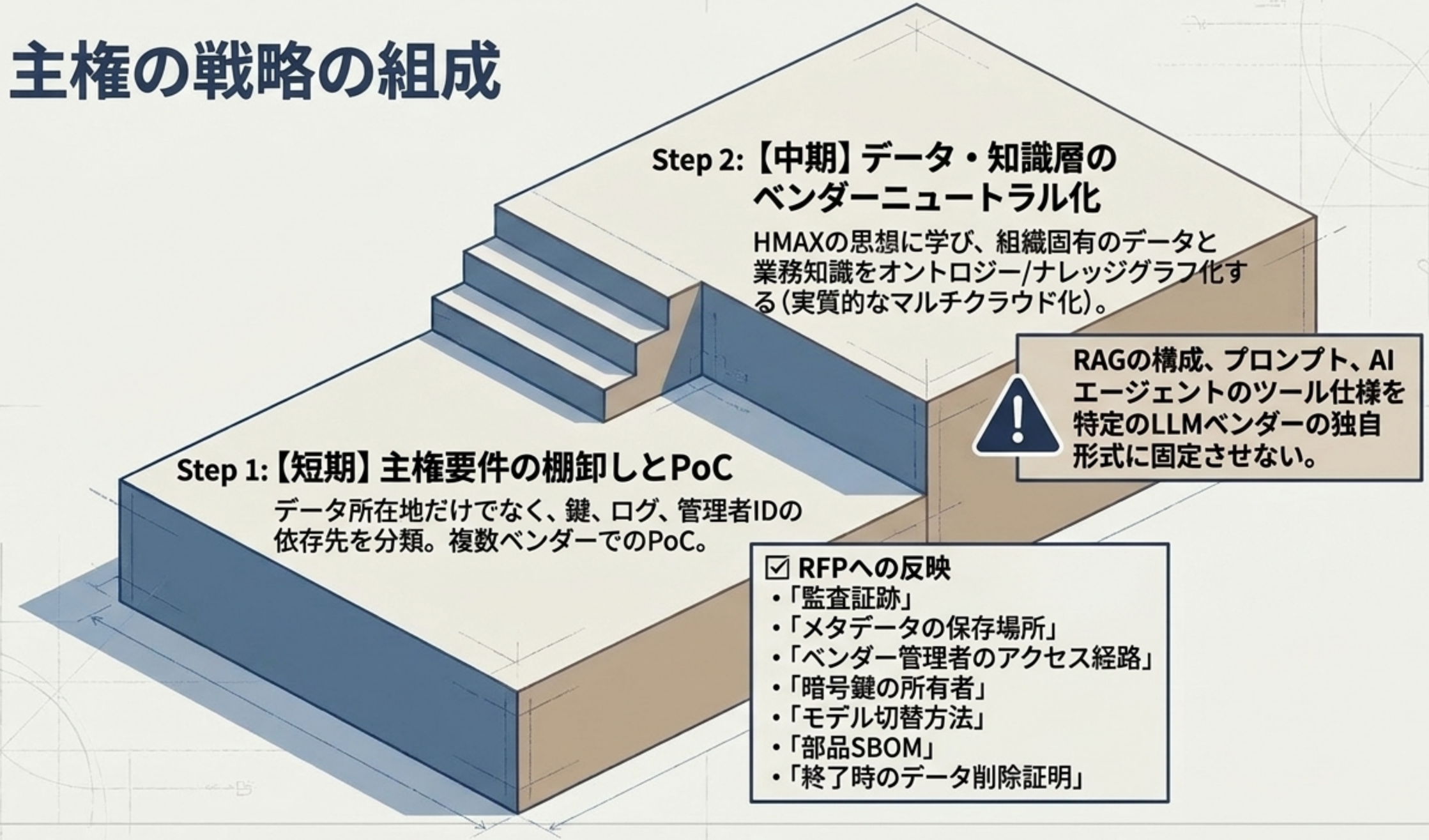
3. 倫理・ガバナンス:
国産モデルでもハルシネーションやバイアスは消滅しない。

4. サプライチェーン:
EDA、製造装置、メモリの100%国内化は不可能。

5. 国際関係:
米中規制変更によるGPU・クラウド提供条件の突然の変更。

Gemini Notebook

主権の戦略の組成



Step 2:【中期】データ・知識層のベンダーニュートラル化

HMAXの思想に学び、組織固有のデータと業務知識をオントロジー/ナレッジグラフ化する（実質的なマルチクラウド化）。

Step 1:【短期】主権要件の棚卸しとPoC

データ所在地だけでなく、鍵、ログ、管理者IDの依存先を分類。複数ベンダーでのPoC。

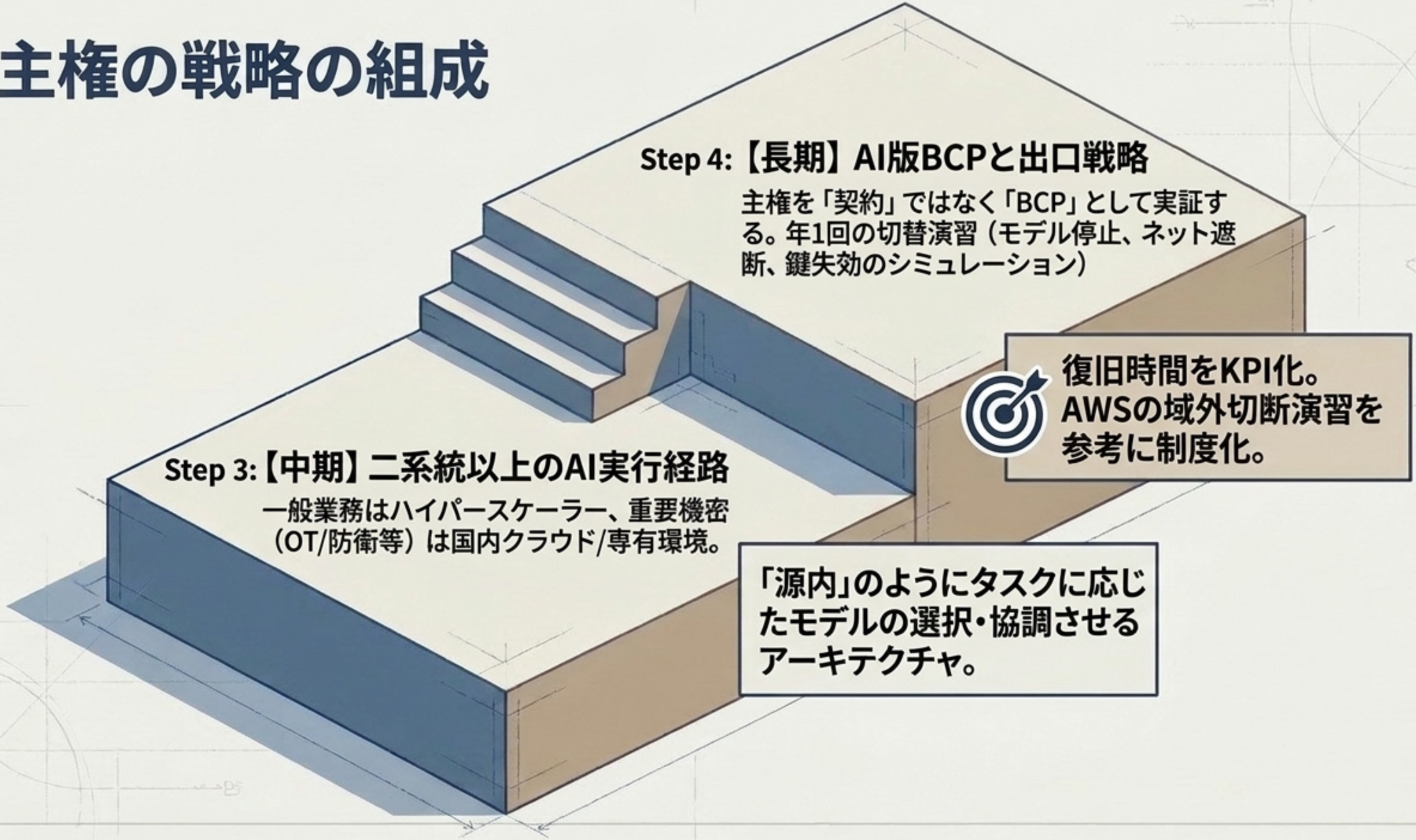
RAGの構成、プロンプト、AIエージェントのツール仕様を特定のLLMベンダーの独自形式に固定させない。

☑ RFPへの反映

- 「監査証跡」
- 「メタデータの保存場所」
- 「ベンダー管理者のアクセス経路」
- 「暗号鍵の所有者」
- 「モデル切替方法」
- 「部品SBOM」
- 「終了時のデータ削除証明」

Gemini Notebook

主権の戦略の組成



Step 4:【長期】AI版BCPと出口戦略

主権を「契約」ではなく「BCP」として実証する。年1回の切替演習（モデル停止、ネット遮断、鍵失効のシミュレーション）

復旧時間をKPI化。
AWSの域外切断演習を
参考に制度化。

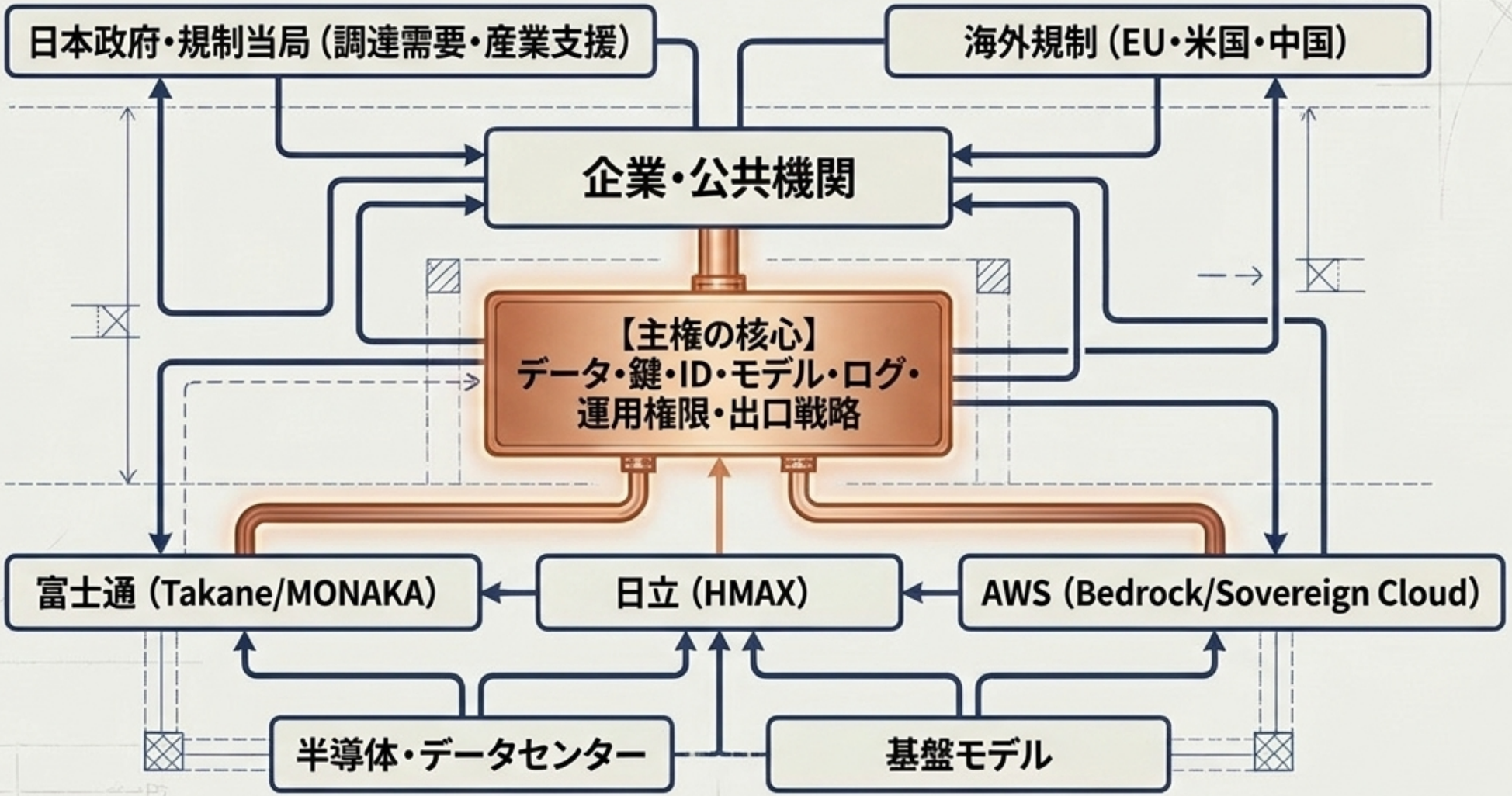
Step 3:【中期】二系統以上のAI実行経路

一般業務はハイパースケーラー、重要機密（OT/防衛等）は国内クラウド/専有環境。

「源内」のようにタスクに応じたモデルの選択・協調させるアーキテクチャ。

Gemini Notebook

AI主権のエコシステム構想図



Gemini Notebook

結論：「二分法」から「ポートフォリオ設計」へ



- ✓ 「どのベンダーが最もソブリンか」ではなく、「ワークロードごとに必要な主権強度（保証レベル）は何か」を問う。
- ✓ 経営が下すべき判断は、国産か海外かの二元論ではない。自社の事業継続における「重大な依存」を可視化し、いざという時の代替経路（切替可能性）をアーキテクチャとして担保すること。
- ✓ その設計図を描き切ることこそが、真の「AI主権戦略」である。

Gemini Notebook