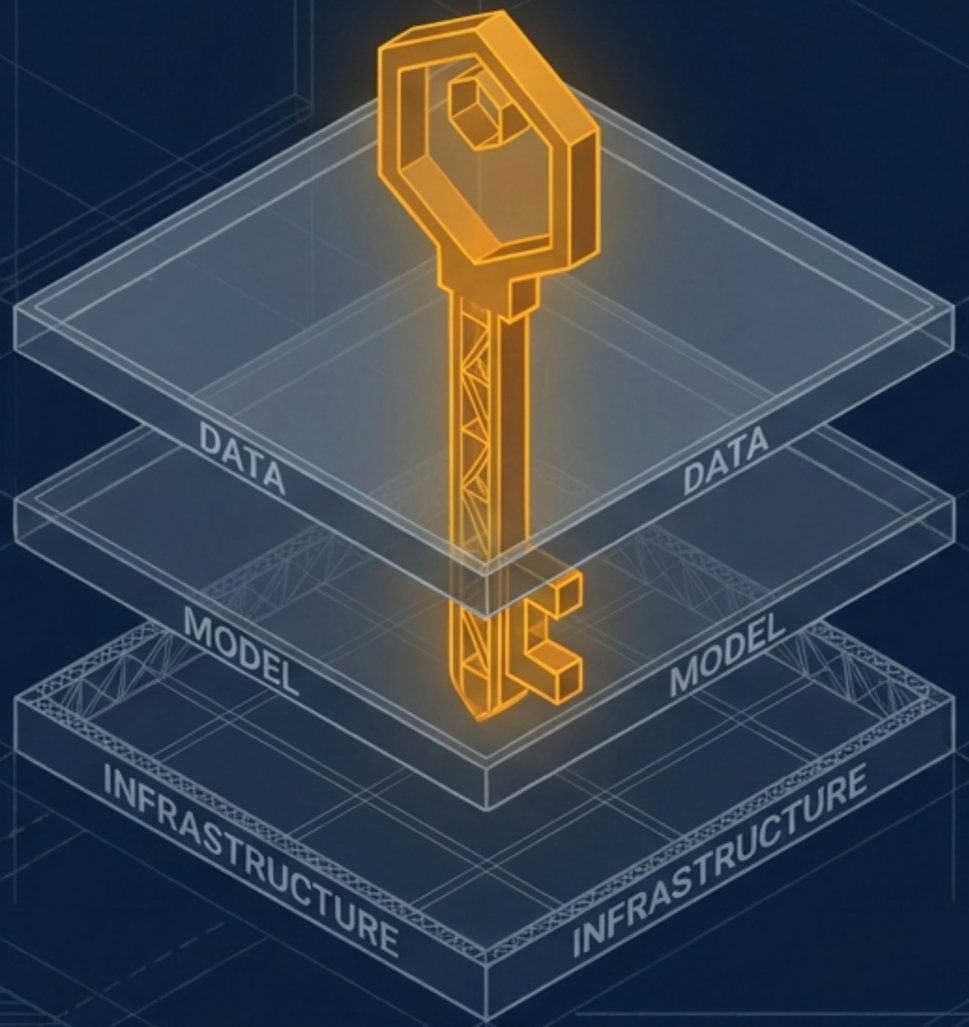


真のAI主権（Sovereign AI）を問う：メディアの過熱と、日本企業が直面する知財リスクの実態

2026年時点の最新動向検証と、経営層・知財部門向け実践プレイブック

Executive Strategic Briefing | November 2026

Gemini Notebook

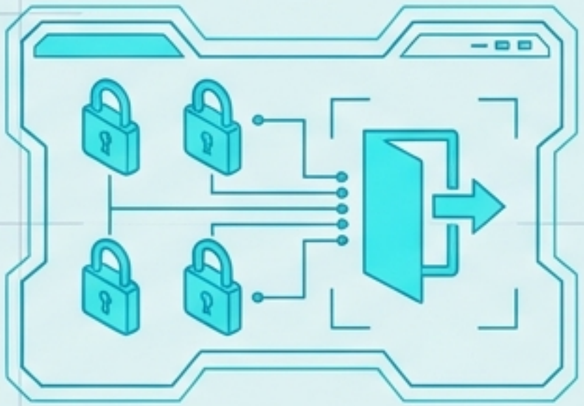
誤解の打破：「完全国産オンプレミス＝主権」ではない

世間の誤解



「データの所在地を日本国内にし、国産のオンプレミスサーバーと国産LLMですべてを構築すれば、完全なAI主権が手に入る」

冷徹な現実



「主権の実体は『物理的な場所』ではない。データ・モデル・インフラの各層において、『暗号鍵・契約の支配権・出口（エグジット）』を自社でコントロールできるかどうかに懸かっている」

Gemini Notebook

ソブリンAIを解剖する「主権の3レイヤー」モデル



データ主権

データの所在・アクセス・準拠法・
監査証跡を証明できるか。
（関連領域：ガバナンス、機密保護）

運用主権

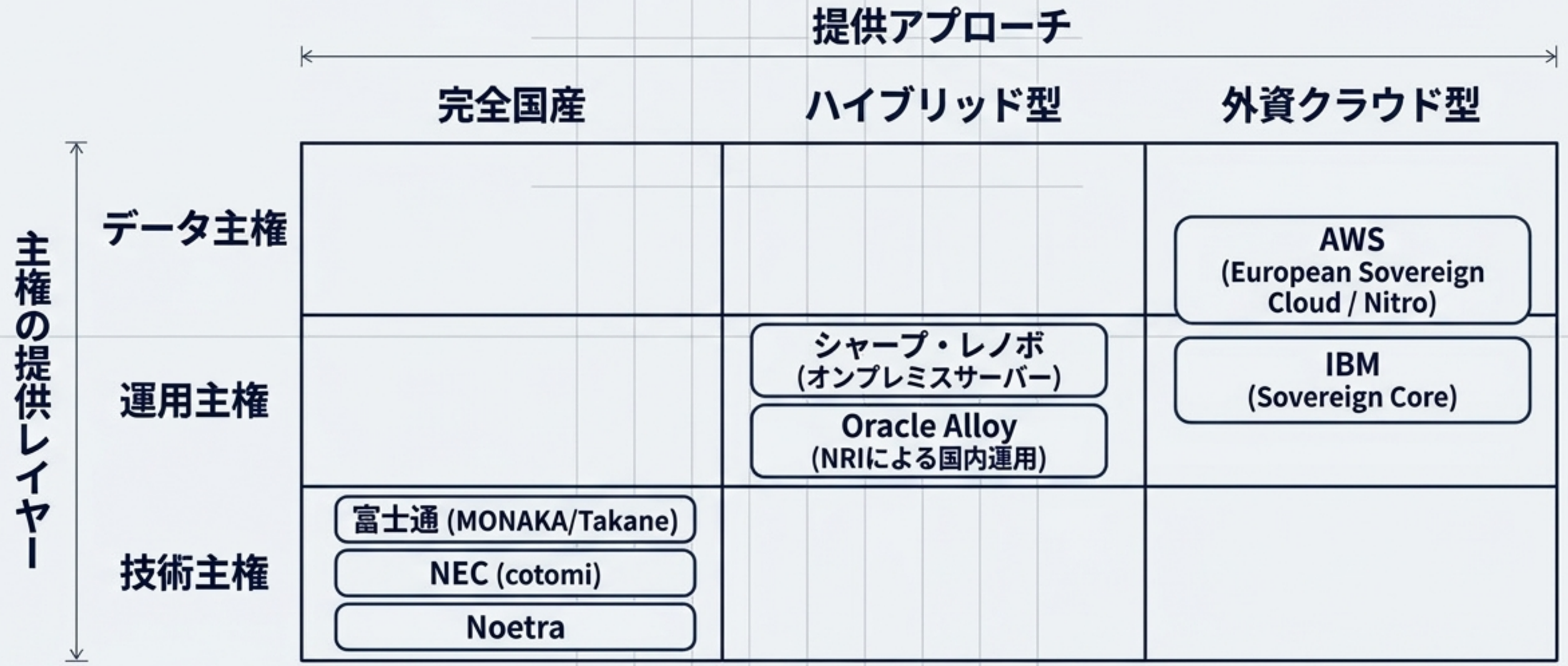
誰が運用し、誰が暗号鍵を持つか。
外部ネットワークが遮断されても稼働を
継続できるか。
（関連領域：耐遮断性、アクセス権）

技術主権

AIモデル、半導体、計算基盤そのものを
自国（自社）の技術で構築できるか。
（関連領域: サプライチェーン自律性）

Gemini Notebook

各社が解決する課題は全く異なる：ベンダー・マッピング



ベンダー10社を同列に比較するのは無意味である。自社の業務機密度に応じ、
必要な「レイヤー」を提供するパートナーを組み合わせ ることが真の最適解となる。

Gemini Notebook

調達タイムラインの現実：国産ハードウェアのリードタイム



「すぐ使える」クラウドサービスと、「2027年度以降」の国産インフラ本格稼働には明確な時間差が存在する。

Gemini Notebook

「データが国内にある」だけでは米国法を回避できない



2025年6月10日、仏上院調査委員会でのMicrosoft France幹部の証言：「仏市民のデータが米当局に渡らないことを保証できるか？」→

「Non, je ne peux pas le garantir（保証できない）」

Analysis

親会社が米国法人である限り、米CLOUD Act等による法的強制開示の可能性は原理的に消えない。「ソブリンクラウド」を標榜していても、運営資本が外資であれば法域リスクは残存する。

Solution Indicator

現実的対策は、国内資本（NRI型等）による運用か、自社のみが復号鍵を保持する機密コンピューティングの導入である。

Gemini Notebook

最先端モデルの代償：突然の「供給停止」と「データ保持義務」

Anthropic
2026年6月の実例



サプライチェーンの突然死



米政府の輸出管理により、2026年6月12日から約3週間、
Anthropicの最新モデル（Fable 5等）へのアクセス
が全世界・全ユーザーで突如停止された。



学習データの強制搾取

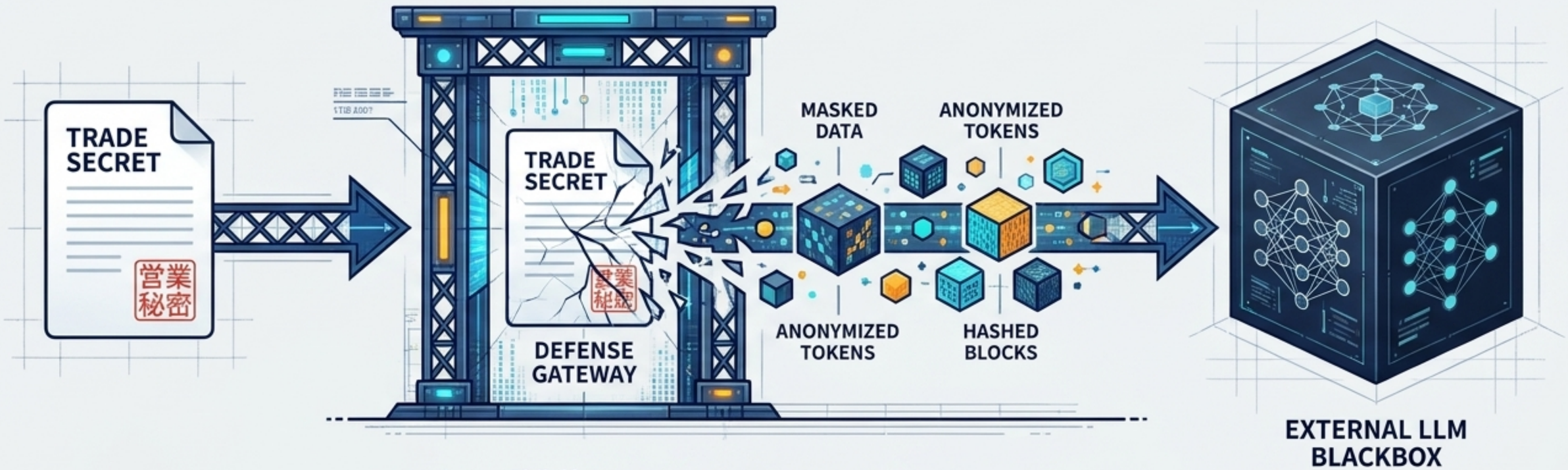
最先端モデルの利用条件として「プロンプトと出力の
30日間保持」が強制された。
これは既存の「ゼロデータ保持契約」を結んでいた
企業にも適用された。

利用条件は米国政府とベンダーの都合で数カ月単位で一方的に覆る。
契約変更時の「解約権」と、停止時の「代替モデル（フォールバック）」の確保が必須である。

Gemini Notebook

外部AI利用による「営業秘密」喪失リスクと防衛ゲートウェイ

経済産業省の「営業秘密管理指針（2025年改訂）」に基づくリスク。AI提供事業者側でのデータ保持が条件となった場合、機密データの入力は「第三者への提供」とみなされ、法的保護（秘密管理性）が否定される恐れがある。



防衛策 (The Defensive Blueprint)

- マスキング層 (例: NEC cotomi Gateway):
  機密情報を自動検知して秘匿化し、外部AIへ渡す。
- 機密コンピューティング (例: 富士通 MONAKA Arm CCA, AWS Nitro Enclaves):
  処理中 (メモリ上) のデータも暗号化し、インフラ提供者すらアクセス不可にする。

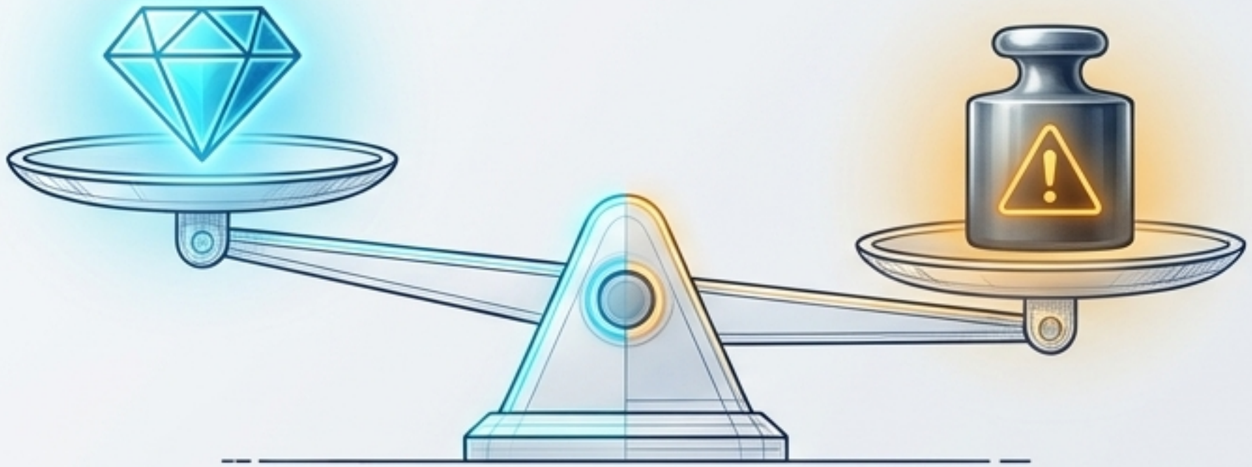
Gemini Notebook

日立型「暗黙知のオントロジー化」が孕む両刃の剣

熟練者のモヤモヤした「暗黙知」を、AIが読める知識グラフ（オントロジー）に変換し、企業の資産として固定する手法（例: 日立 HMAX Data Fabric）。

体系化された形式知 (Corporate Asset)
属人化を排除し資産価値を高める

一括コピー・流出のリスク (Hacker Target)
一度流出した際の事業ダメージが壊滅的になる



Strategic Rule

オープン領域（業界標準化する概念体系：スキーマ）と、クローズ領域（自社固有の閾値や故障パターン：インスタンス）を厳密に切り分け、後者へのアクセスログ監視を徹底せよ。

Gemini Notebook

統合インサイト：機密度に応じた「ハイブリッド・AIアーキテクチャ」



極秘・重要インフラ

完全に隔離された国内オンプレミス、
または機密コンピューティング環境。
国産LLM（軽量・高セキュア）を常用。

社内業務・ノウハウ

マスキング機能を持つ「AIゲートウェイ」
を経由し、安全なデータのみを最先端の
外部海外モデル（Claude/GPT）へ渡す。

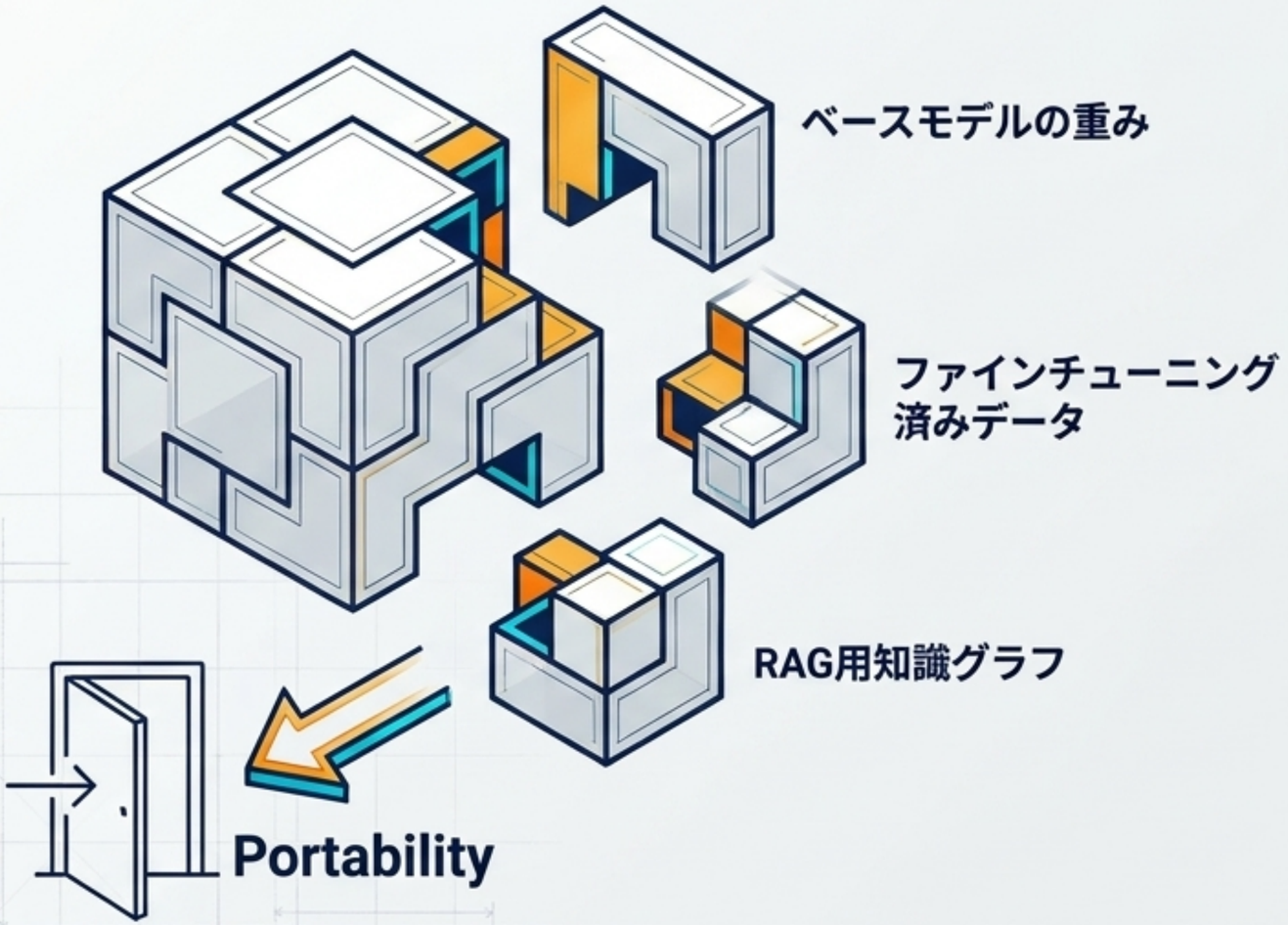
公開情報処理

スピードとコストを優先し、パブリックな
AIクラウドサービスを直接利用。

Gemini Notebook

ロックインを回避する「エグジット（出口）」の設計

ベンダー契約終了時に、蓄積した「AIの知恵」を取り出せなければ主権はない。
IBM Sovereign Core等がポータビリティを強調するのはこのためである。



Checklist for IP Exit

- **派生成果物の帰属**: ファインチューニングした重みやRAG用インデックスの所有権は自社にあるか？
- **ライセンスの制約**: ベースモデルの規約により、派生モデルを他社クラウドへ持ち出すことが禁じられていないか？
- **標準フォーマット**: 知識グラフはRDF/OWL等のオープン標準形式で抽出可能か？

Gemini Notebook

経営層・知財部門のための「5つの即時アクション」

1. データ分類の再設計

情報区分（営業秘密・限定提供・一般等）と、AI処理環境（国内/機密/パブリック）の紐付けルールを策定する。

2. 契約条項の標準化

「学習利用禁止」「削除証明の提出」「政府要請時の通知義務」「条件変更時の解約権」を必須要件とする。

3. 代替モデル（フォールバック）の確保

主力モデル（例：米国製最先端モデル）の突然のアクセス遮断に備え、業務を止めない代替国産モデルを待機させる。

4. 監査ログと証跡の自動化

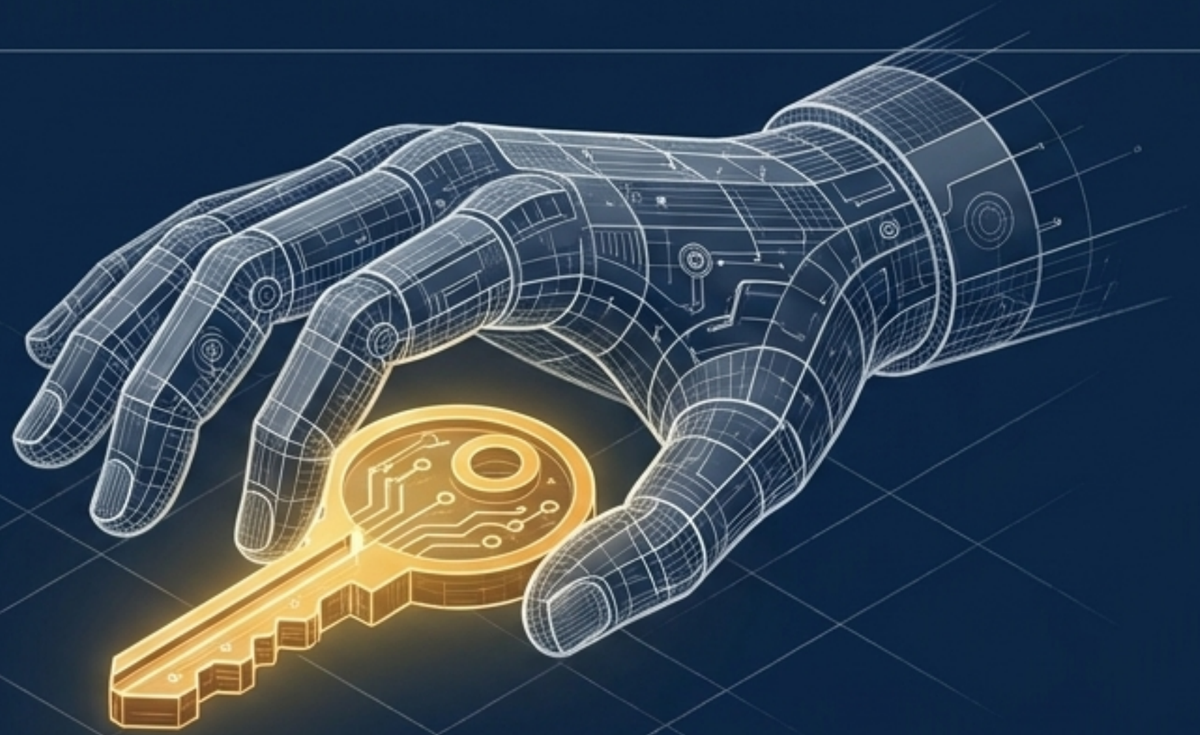
「誰が、どのデータを、どのモデルに入力したか」を証明できるシステムを構築する。

5. 暗黙知資産化のガバナンス

オントロジー（知識抽出）プロジェクト開始前に、ベンダーへのIP帰属を阻止する契約を締結する。

Gemini Notebook

結語



「AI主権とは、すべてを自国・自社でゼロから作ることではない。
他国や他社に『チョークポイント（急所）』を握られないよう、
技術・データ・契約の境界線を自らの手で統御することである。」

（日本政府「人工知能基本計画」が掲げる「耐遮断性」と「複数モデル統御」の哲学より）

End of Briefing. Action

Gemini Notebook