「ソブリンAI」が切り拓くデジタル安全保障の新秩序

地政学ショック・5層アーキテクチャ・日本企業がとるべき実践フレームワーク

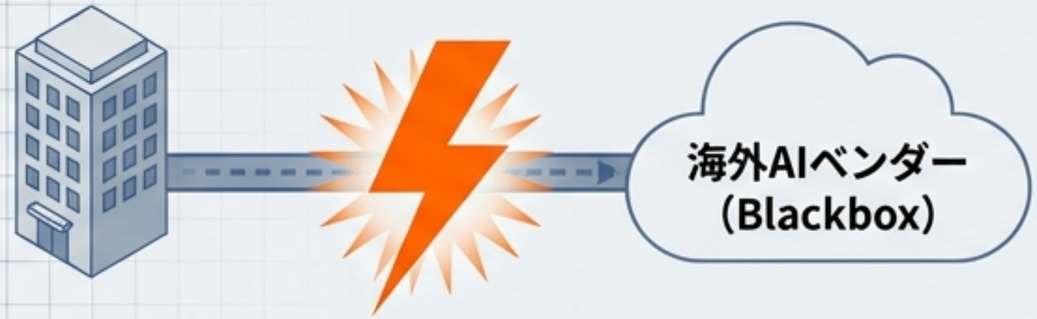




Gemini Notebook

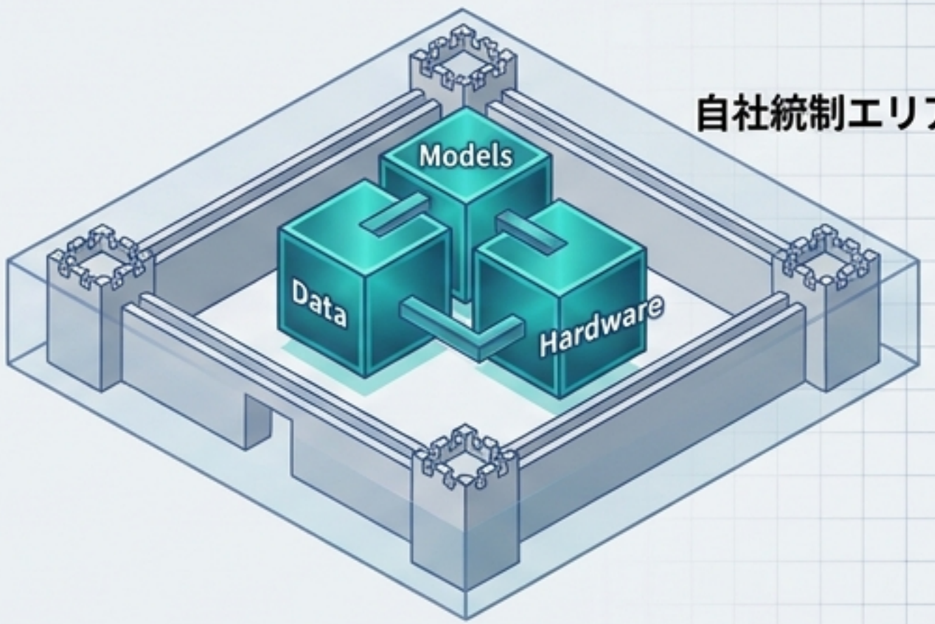
「海外API依存」の終焉。AI主権は事業継続の生命線へ。

従来型：盲目的依存



ある日突然、業務システムが停止するリスク

ソブリン型：自律的統制



自社のデータ、AIモデル、ガバナンスを主体的に管理・統制

生成AIを「API経由で呼び出すだけの導入」は、地政学・法制度の観点から限界を迎えた。
AIの統制力（主権）の確保が、企業の命運を握る。

Gemini Notebook

2026年を襲った3つのショック：不可逆的なルールチェンジ

米国

2026年6月

米政府の輸出管理指令。
海外ユーザーの最新AIモデルへのアクセスを制限。

日本

2026年10月1日

「サイバー対処能力強化法（能動的サイバー防御法）」
主要部分施行。基幹インフラへの法的監査義務化。

中国

2026年10月16日

中国商務部等がAI関連23項目の輸出規制案
（モデルの重み、AIエージェント等）を公表。

**米・中・日の同時多発的な規制強化により、
企業は猶予なく「AIインフラの再定義」を迫られている。**

Gemini Notebook

顕在化したリスク：「即時遮断」の実害と「1/20コスト」の誘惑

即時遮断の衝撃 (Kill Switch Shock)



Anthropicの最新モデル「Fable 5 / Mythos 5」が米商務省の命令により突如停止。
外国人ユーザーの即時遮断が困難だったため、全ユーザーが影響を受ける事態に。

1/20コストの誘惑 (The 1/20 Cost Temptation)



中国製AIモデル
（月額1000万円が50万円になる試算）

米国土安全保障省（DHS）による使用禁止令や、輸出規制・サプライチェーンの不透明性という「ガバナンス・リスク」

安価な代替手段への飛びつきは、次なるコンプライアンス違反の引き金となる。

Gemini Notebook

国内法制の壁：「能動的サイバー防御法」が迫る監査証明義務

「あなたのシステムのAIに対し、
誰がアクセスし、何が起きたか、
政府に証明できますか？」

官民連携（届出義務）

15分野・258者の基幹インフラ事業者（＋サプライチェーン）は「特定重要電子計算機」の導入届出が必須。

通信情報の利用

政府によるサイバー攻撃関連通信の取得・分析。

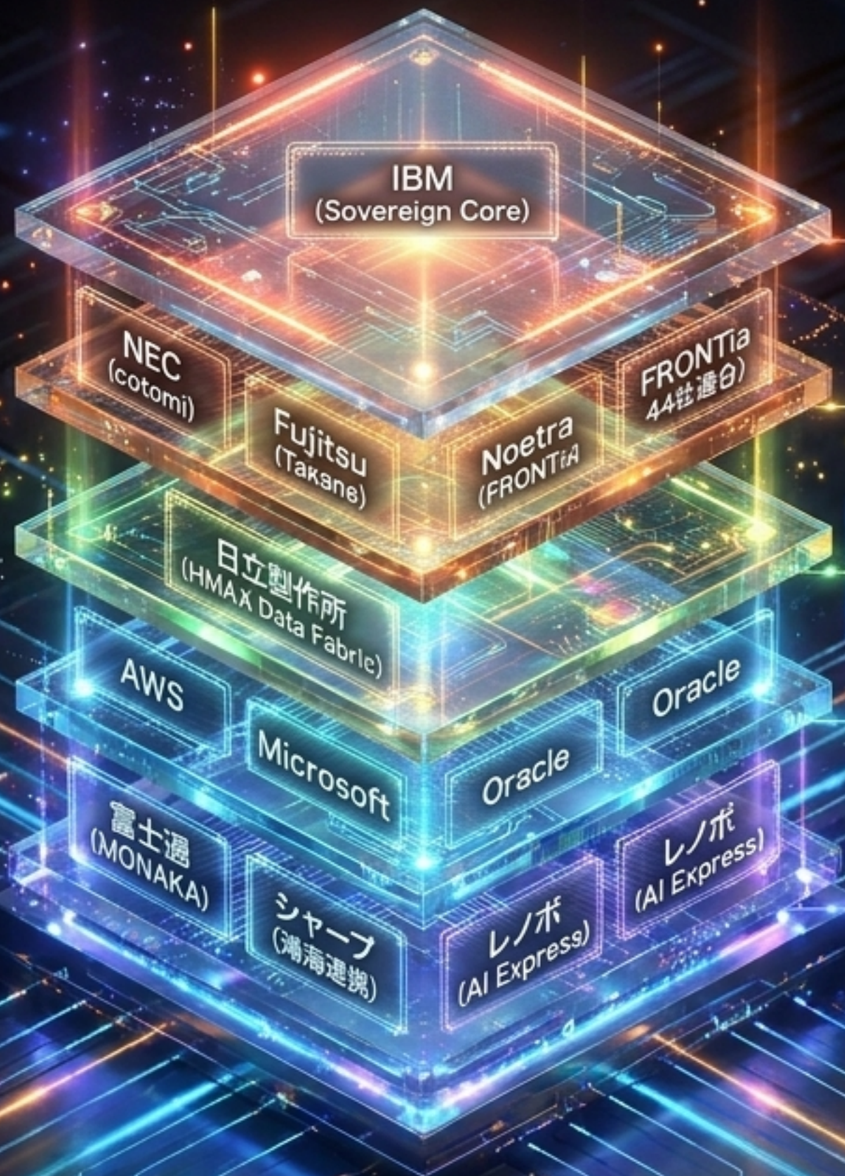
アクセス・無害化

重大被害防止のための警察・自衛隊によるサーバーへのアクセス。

**内部構造やアクセス履歴が不透明な外部AIサービスでは、
法的に求められる「監査証跡の提出義務」に対応しきれない。**

Gemini Notebook

ソブリンAIを構成する5層の技術アーキテクチャ



Layer 5: ガバナンス・主権監査

Layer 4: 基盤モデル・フィジカルAI

Layer 3: データ主権・オントロジー

Layer 2: ソブリンクラウド隔離

Layer 1: ハードウェア・サーバー

ソブリンAIは単一の製品ではない。

これら5つのレイヤーを適材適所で組み合わせることで、初めて主権の要塞が完成する。

Gemini Notebook

Layer 1: ハードウェア覇権（国産シリコンと短納期オンプレミス）

富士通
（Fujitsu MONAKA）

- TSMC 2nm採用の独自設計CPU
- Arm CCA規格による「ハードウェアレベルのオンメモリ暗号化」
- 2026年11月受注開始

シャープ
（鴻海連携 AI-B43100）

- 台湾・鴻海（Foxconn）の調達力
- 液冷不要の「空冷4Uラック」で既存設備へ即時導入
- 全国108拠点の保守網

レノボ
（Lenovo AI Express）

- 検証済み構成により、工場出荷まで「最短15営業日」の圧倒的短納期

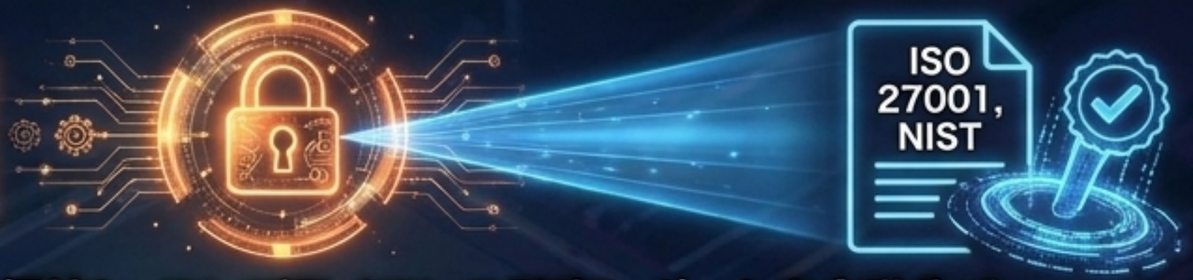
ARCHITECTURAL DIMENSION

【経済性の証明】オンプレミスAIは、稼働率「30%超」でクラウド利用を上回る経済合理性（ROI）を発揮する。

Gemini Notebook

Layer 2 & 5: クラウド隔離と自律的監査機構（Sovereign Cloud & Audit）

IBM (Sovereign Core)



暗号鍵を自国管轄内に保持し、コンプライアンス監査レポートを自動生成。

AWS (Nitro Enclaves)



CPU/メモリを物理的に切り出し、AWS運用者すら内部データを閲覧不能にする隔離機構。

Microsoft Azure



論理隔離のパブリックから、独立稼働可能な「Azure Local 非接続」モードまで3類型で提供。

Oracle (Alloy)



現地パートナー企業のデータセンター内でフルサービスを提供するアプローチ。

ARCHITECTURAL DIMENSION

「オンプレミス＝ソブリン」ではない。高度に隔離・暗号化されたクラウド領域も、主権ポートフォリオの強力な選択肢となる。

Gemini Notebook

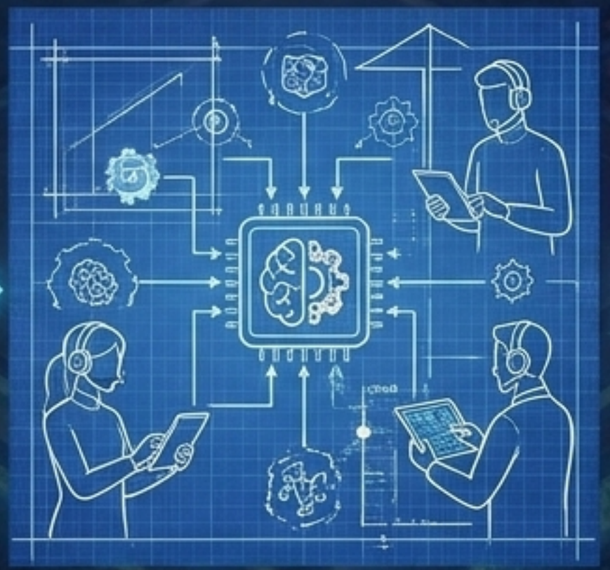
Layer 3: データ主権と現場の暗黙知（オントロジー）

散在するデータ



ITデータ、OT（制御）データ、
熟練技術者の「暗黙知」

Physical AI FDE Team



日立の専門チーム（Forward Deployed Engineer）が現場に入り込み、文脈を抽出。

HMAX Data Fabric / オントロジー



自社統制下の知識グラフ（Ontology）
として美しく構造化されたデータ資産。

ARCHITECTURAL DIMENSION

ハードやモデルを揃えても、データが未整理・未統制では主権は機能しない。
データの作成から廃棄までを自社統制下に置く「データファブリック」が不可欠。

Gemini Notebook

Layer 4: 企業向け軽量LLMと、1兆円規模の国家フィジカルAI基盤

企業内即時実装 (Enterprise LLM)



NEC cotomi: 13B/30Bの軽量設計(GPU1枚で動作)、最大12万8000トークンの長文マルチモーダル対応。

富士通 Takane: Cohere「Command R+」をベースに日本語特化させたオープンモデル活用。

国家規模の将来基盤 (Noetra / FRONTia計画)



2万7,500基のNVIDIA Rubin GPU
(1.4ゼタフロップス級)

政府1兆円規模の支援。ソフトバンク、ホンダ、NEC、ソニーGなど44社連合による「フィジカルAI」基盤モデル開発(2028年稼働予定)。

Gemini Notebook

統合戦略：3階層ハイブリッド主権ポートフォリオ



Tier 1（中核）

Need: 極秘データ・基幹インフラ・OT制御
Strategy: オンプレミスAI（MONAKA / Lenovo）
＋国産モデル（cotomi / Takane）
＋自動監査（IBM）。完全な自社統制。

Tier 2（内部）

Need: 一般社内業務・顧客情報
Strategy: ソブリンクラウド
（AWS Nitro / Azure）
＋日米モデルの適材適所併用。

Tier 3（外部）

Need: 大量定型処理・非機密データ
Strategy: コスト最適化されたオープンモデル
（厳密な監視下での運用）。

全てを国産・オンプレミスにする必要はない。
データの機密性に応じた「ポートフォリオ設計」こそが真の主権確保である。

Gemini Notebook

アーキテクチャの絶対条件：「モデル・ポータビリティ」

⚠ 密結合（危険）



特定のモデルに直接固く結びついているため、
モデルが停止すると業務全体が即時停止する。

疎結合（安全）



アプリケーションとモデルの間に抽象化層が存在。
有事の際、数分で別モデルへ切り替え
（フェイルオーバー）が可能。

**「どのSDKでシステムを作るか」と「背後でどのAIを回すか」を完全に切り離す。
特定モデルの停止が業務停止に直結するリスクを排除せよ。**

Gemini Notebook

タイムリミットは2027年3月末。サプライチェーン対応「4つのステップ」



ITベンダーの「勝ち筋」：マルチベンダー・オーケストレーション

海外ハイパースケーラー

AWS / Microsoft / Oracleの先端機能

国産特化型LLM&国家基盤

cotomi / Takane / Noetra



データ主権・監査基盤

HMAX / IBM Sovereign Core

独自ハードウェア

MONAKA / シャープ / Lenovo

単体製品の販売ではなく、これら全てを顧客のTier要件に合わせて統合し、「日本で安心して利用できるAI基盤」として提供（インテグレーション）することに最大の商機がある。

Gemini Notebook

AI主権の確立は、次世代の企業競争力の根源である

[1] リスクは現実である

海外APIへの盲目的依存は、地政学リスクにより「事業停止」に直結する。

[2] ポートフォリオを設計せよ

「オンプレ vs クラウド」の二元論を脱し、3階層の主権ハイブリッド環境を構築する。

[3] 法定期限は2027年3月

基幹インフラとサプライチェーンは、
直ちに監査対応とポータビリティ確保に動くべきである。



Gemini Notebook