「ソブリンAI」が切り拓くデジタル安全保障の新秩序：日経クロステック記事の徹底深掘りと戦略的インプリケーション

Gemini 4 Argon

2026年11月5日付の日経クロステック記事『富士通・日立・AWSも、「ソブリンAI」で競演 AI主権の機運に商機見いだす』（特集『AIが使えなくなる日 「デジタル安全保障」を確保せよ』第3回、中島募記者）は、生成AIおよび自律型AIが企業の基幹システムや社会インフラに深く組み込まれる中、「AI主権（Sovereign AI）」の確立が単なるIT導入の選択肢を超え、国家および企業の事業継続を左右するデジタル安全保障の中核課題へと浮上した現実を伝えている[1]。ソブリンAIとは、国や企業が外部の特定クラウドや海外AIベンダーに過度な依存をすることなく、自国・自社のデータ、AIモデル、技術基盤、運用ポリシー、ガバナンスの主導権を利用者側で主体的に統制・管理するAIシステムを指す[1]。本稿では、当該記事で報じられた日米中10社・団体の動向を起点に、その背後にある2026年特有の3つの地政学・法制ショック、ハードウエアからオントロジーに至る5層の技術アーキテクチャ、そして日本企業が直面するコストと主権のジレンマを体系的に深掘りする[1]。

当該記事が示す最大の戦略的転換点は、「海外の最新AIをAPI経由で呼び出すだけのアーキテクチャ」が、地政学リスクと国内法規制の双方から見直しを迫られているという点である[1]。2026年6月に米政府の輸出管理指令を受けて米Anthropicが最新モデル「Fable 5」および「Mythos 5」の提供を全ユーザー向けに突如停止した事案や、2026年10月に中国商務部等がAIモデルの重みやAIエージェントなど23技術を輸出管理対象に追加する草案を公表した措置は、「ある日突然、業務に組み込んだAIが利用制限を受ける」リスクが理論上の懸念ではなく実務上の脅威であることを浮き彫りにした[1]。さらに国内では、2026年10月1日に「サイバー対処能力強化法（能動的サイバー防御法）」の主要規定が施行され、15分野・258者の基幹インフラ事業者とそのサプライチェーンに対し、特定重要電子計算機の資産届出とインシデント報告、そして「誰がシステムにアクセスし何が起きたかを政府に証明できる監査体制」が法的に求められている[1]。

この機運を商機と捉え、ITベンダー各社は「モデル」「半導体・サーバー」「データ基盤」「ガバナンス」「ソブリンクラウド」の全レイヤーで主導権争いを展開している[1]。NECの軽量・長文対応LLM「cotomi」や富士通の「Takane」および2nmプロセス採用の国産設計CPU「FUJITSU-MONAKA」、ソフトバンク・ホンダ・NEC・ソニーグループなど44社が出資し政府が5年間で1兆円規模の支援を予定するフィジカルAI基盤「Noetra（FRONTia計画）」、日立製作所の暗黙知オントロジー基盤「HMAX Data Fabric」、シャープ（鴻海連携）やレノボの短納期オンプレミスAIサーバー、さらにはAWS・マイクロソフト・オラクル・IBMによる主権統制ソリューションまで、多様な選択肢が出揃いつつある[1]。一方で、記事が指摘する通り「オンプレミスAI＝ソブリンAI」という単純な図式は成り立たない[1]。以下では、各社の技術仕様と戦略的課題を解剖した上で、日本企業がコスト競争力（中国製AIによるモデル利用料20分の1の試算など）とデジタル主権を両立させるための意思決定フレームワークを提示する[1]。

1. なぜ今「ソブリンAI」なのか：地政学リスクの顕在化と「AIが使えなくなる日」の現実味

企業が経営戦略、製品の設計図面、製造ノウハウ、契約書、顧客情報といった機密データをAIに処理させる比重が高まるにつれ、「データの保存場所」「アクセス権限の所在」「外部AIによる学習流用の有無」「外部サービスへの過度な依存」という4つの課題が経営アジェンダとして浮上した[1]。日経クロステックの記事が2026年11月というタイミングでソブリンAIを特集した背景には、2026年半ばから秋にかけて相次いで発生した3つの外部環境ショックが存在する[1]。

2026年の地政学・法制ショックが企業のAI主権確立を不可逆的に加速させた

SHOCK 01 / 米国輸出管理
米政府指令による最新AIの即時停止
2026年6月、Anthropicが米輸出管理指令を受け「Fable 5 / Mythos 5」の提供を緊急停止。海外API依存の供給途絶リスクが顕在化。

SHOCK 02 / 中国技術規制
AI関連23項目の輸出規制と臨時登記
2026年10月、中国が2兆パラメータ以上や世界トップ10モデルの重み等を制限対象に追加。オープンモデルのライセンス調達に制約。

SHOCK 03 / 国内法制施行
能動的サイバー防御法の主要部施行
2026年10月、基幹インフラ15分野・258者に特定重要電子計算機の届出とインシデント報告を義務化。委託先やクラウド統制も対象に。

● 市場・ベンダー依存リスク ● 米中地政学・輸出管理ショック ● 国内法制・サイバー安全保障
● 国産ソブリンAI基盤（Noetra等）

2024年 — ベンダー依存リスク

海外クラウドAIの旧モデル提供終了（Deprecation）問題が顕在化 IMPACT: HIGH
プロプライエタリな海外製AIモデルの仕様変更や旧モデル提供終了に伴い、日本企業の間でシステム再構築コストや外部ベンダーロックインに対する警戒感が浮上。
旧モデル終了対応 / ベンダーロックイン懸念

2025年5月〜7月 — 国内法制整備

サイバー対処能力強化法（能動的サイバー防御法）成立・国家サイバー統括室発足 IMPACT: HIGH
2025年5月16日に同法および整備法が成立。同年7月には内閣サイバーセキュリティセンター（NISC）を改組した司令塔「国家サイバー統括室」が内閣官房に発足（2026年4月にはサイバー通信情報監理委員会を設置）。
2025年5月16日 成立 / 2025年7月 国家サイバー統括室

2026年6月12日 — 米国輸出管理

米Anthropicが米政府の輸出管理指令を受け「Fable 5 / Mythos 5」を緊急停止 IMPACT: CRITICAL
米政府による"セキュリティ脱獄"懸念と輸出管理指令を受け、Anthropicが最新LLMの提供を突如停止。Claude画面上で利用不可アラートが表示され、海外モデルへの直接依存が国家安全保障上の理由で即座に遮断されうる現実を露呈。
Fable 5 / Mythos 5 提供停止 / 米政府輸出管理指令

2026年10月1日 — 国内法制施行

能動的サイバー防御法の主要部分が施行、基幹インフラ258者に届出・報告義務 IMPACT: CRITICAL
電気・ガス・金融など15分野の基幹インフラ事業者（2026年7月1日時点で258者）に対し、特定重要電子計算機の導入届出（原則4カ月以内）とインシデント報告（速報3〜5日以内目安、詳報30日以内）を義務化。委託先やクラウド提供元の機器も対象となり、サプライチェーン全体の統制が必須に。
15分野・258事業者 / 速報3〜5日以内 / 詳報30日以内

2026年10月16日 — 中国輸出管理

中国商務部・科学技術部がAI関連23項目（禁止6・制限17）の輸出規制案を公表 IMPACT: CRITICAL
公告2026年第48号で「輸出禁止・制限技術目録」改正草案を公表し、同日より輸出前の「臨時登記」を即時実施。学習計算量10^26 FLOP以上、パラメータ数2兆以上、または世界トップ10水準の「モデルの重み」やソースコードのライセンス移転を制限（API利用は対象外、10月22日にはDeepSeek等の臨時登記完了報道）。
AI規制 23項目 (禁止6 / 制限17) / 2兆パラメータ以上 / 10^26 FLOP

2026年度 (10月時点) — 国産AI基盤戦略

国産AI基盤開発「Noetra」に44社が参画、経産省・NEDOが2026年度予算3,873億円で支援 IMPACT: CRITICAL
ソニーG・ソフトバンク・NEC・ホンダの中核4社や富士通、日立製作所など計44社が出資し、産総研・PFN等と研究開発事業「FRONTia」を推進。1兆パラメータ級マルチモーダル基盤モデルを開発し、学習済み重みを国内の条件適合事業者に限定提供するソブリンAI体制を本格化。
参画企業 44社 (中核4社) / 2026年度予算 3,873億円 / 1兆パラメータ級想定

2027年3月〜11月 — 国内法制期限

既存重要計算機の届出期限（3月末）と「通信情報の利用」施行（11月まで） IMPACT: HIGH
能動的サイバー防御法施行時点で導入済みの「特定重要電子計算機」の届出期限が2027年3月31日に到来（取引先へのIT資産棚卸し要請が加速）。さらに同年11月までに、攻撃サーバー検知のため政府が通信情報を取得・分析する「通信情報の利用」が施行予定。
2027年3月31日 既存機器届出期限 / 2027年11月迄 通信情報の利用施行

2028年6月 (〜2030年度) — 国産計算基盤稼働

NVIDIA Vera Rubin GPU 約2万7,500基の大規模計算基盤が稼働開始へ IMPACT: HIGH
Noetraと産総研が推進する「FRONTia」プロジェクト（2026・2028・2030年度の3段階ロードマップ）において、NVIDIA Vera Rubin GPU約2万7,500基で構成される国内大規模計算基盤が2028年6月に稼働開始する計画。
Vera Rubin 約27,500基 / 2026・2028・2030年度 3段階計画

2024年の旧モデル終了問題に端を発した外部依存リスクは、2026年6月の米Anthropicによる最新モデル提供停止と10月の中国AI輸出管理強化によって**国家安全保障レベルの供給途絶リスク**へと変質した。同時期に施行された日本の能動的サイバー防御法が、基幹インフラ企業にシステム統制の証明を迫っている。

Data sources: 日経クロステック / NTT西日本 Biz Clip（内閣官房・内閣府資料基） / IT Leaders (Impress) / ISSOH Tech / AI Revolution

1.1 米国の輸出管理指令と2026年6月「Anthropic最新モデル停止」の衝撃

特定の海外AIベンダーに業務システムを強く依存するリスクは、単なる「仕様変更」から「国家安全保障命令による即時遮断」へと先鋭化している[1]。2024年に米OpenAIが旧版のGPT-3.5系モデルの提供終了を発表した際にも、同モデルを業務に組み込んでいた国内企業の一部で混乱が生じたが、2026年6月に起きた米Anthropicの事案はより構造的なリスクを露呈させた[1]。

2026年6月9日に一般公開されたばかりのAnthropicの最上位モデル「Claude Fable 5」および「Mythos 5」は、わずか3日後の6月12日午後5時21分（米国東部時間）、米商務省からの国家安全保障上の輸出管理指令（外国人による最新AIモデルへのアクセスを禁止する措置）を受けて突如アクセス停止となった[3]。米政府が懸念したのは、特定のコードベースをモデルに読み込ませてソフトウエアの欠陥を探索・修正させる手法（「セキュリティ脱獄」や脆弱性発掘への悪用懸念）であったとされる[3]。Anthropic側は「発見されたのは既知の軽微な脆弱性が少数のみで、他社の一般公開モデルでも特別な回避策なしに再現できる水準に過ぎない」と反論したものの、外国籍ユーザーのみを技術的に即時切り分けて遮断することが困難であったため、コンプライアンス上の措置として全ユーザーに対してFable 5およびMythos 5のセッションを停止し、Opus 4.8やSonnetなどの既存モデルへ切り替える対応をとった[3]。

公開直後の最新モデルであったため業務利用していた企業は少なく直接的影響は限定的だったものの、この事案は「現在稼働しているクラウドAIモデルが、米国の国家安全保障判断一つで数時間後には利用できなくなる」という継続性リスクを日本の経営層に認識させた[1]。輸出管理の対象が従来の「貨物・技術」から「クラウド上のAIモデルへのアクセス」へと広がった象徴的事例といえる[6]。

1.2 中国のAI技術輸出規制（23項目）と「コスト20分の1」のジレンマ

米国の対中半導体輸出規制や対中AI投資制限に対抗する形で、中国政府もAI技術の管理強化に動いている[1]。2026年10月16日、中国商務部および科学技術部は「中国輸出禁止・制限技術目録」の第5次改正草案（2026年第48号公告）を公表し、AI・バイオ医薬・太陽光発電の3分野40項目（うちAI関連は禁止6項目・制限17項目の計23項目）を輸出管理対象に追加する案について11月15日までの意見公募を開始するとともに、同日より関連技術の海外移転に関する「臨時登記（事前届出制度）」を即日開始した[5]。

この規制案の核心は、中国の「核心データ」で学習した大規模モデルや国防・重要インフラ向けの高敏感AIエージェント等を「輸出禁止（6項目）」としたことに加え、中国の「重要データ」で学習したモデルや、以下の3基準のいずれかを満たす大規模モデルの「重み（ウエイト）パラメータ」「主要チェックポイント」「基盤ソースコード」「学習最適化・推論高速化技術」を輸出制限（ライセンス許可制、17項目のうち266504X）の対象とした点にある[5]。

1. 学習計算量：10^26 FLOP以上[5]
2. パラメータ数：2兆（20,000億）パラメータ以上[5]
3. 能力基準：輸出時点で国内外の主流評価機関や大規模産業プラットフォームの公開評価において「世界トップ10」に入るもの[5]

さらに、自然言語指示を20ステップ以上に分解（分解精度80%以上、サブタスク平均成功率90%以上）する自律型エージェント、60体以上が同時稼働するマルチエージェント協調、200個以上のツール統合、双方向800GB/s以上の計算クラスター技術、14nm以下プロセス等のAIチップ設計技術なども制限対象に含まれた[5]。草案では海外向けのAPI・アプリ・SaaS経由の利用は対象外とされ、2026年10月22日夜には中国CCTV系のSNSアカウント「玉淵譚天」などがDeepSeekとMiniMaxが臨時登記を完了してオープンソース公開や海外への使用許諾を継続していると伝えた（ただし10月23

日時点では商務部や両社からの公式発表は未確認）[5]。
一方で、日経クロステックが2026年10月7日に『みずほもライオンも選んだ中国AI、日本企業に浸透 コスト20分の1の衝撃』と報じた通り、日本の大手企業の間では定型業務や社内文書処理において低価格な中国製生成AIを採用する動きが出ている[1]。業界解説の試算によれば、TCO（総保有コスト）ではなくモデル利用料金のみが米国製AIの20分の1になると仮定した場合、月額1,000万円（年間1億2,000万円）の利用費が月額50万円（年間600万円）へと下がり、年間1億1,400万円の削減となる計算だ[4]。しかし、オープンモデルの重みを自社環境に取り込んで運用・更新する手法や共同開発・ライセンス取得には、今後の中国輸出管理の運用次第で制約が生じる可能性があるほか、米国土安全保障省（DHS）が2026年10月19日に連邦文民機関でのDeepSeek製品の調達・使用を禁じる命令を公表したように、日米双方に関わる企業にとってガバナンスとサプライチェーン構造の精査が不可欠となっている[4]。

1.3 国内「能動的サイバー防御法」の施行と監査証明義務

地政学リスクと並び、ソブリンAI需要を後押ししているのが国内の法規制強化である[1]。政府は2025年5月16日に成立（5月23日公布）した「サイバー対処能力強化法（正式名称：重要電子計算機に対する不正な行為による被害の防止に関する法律、令和7年法律第42号）」および同整備法（令和7年法律第43号）の主要規定を、2026年10月1日に施行した[1]。
警察庁資料に基づく政府発表では令和6年中に観測されたサイバー攻撃関連通信の99.4%が海外IPアドレスを発信元としており、また2026年10月にはGMOインターネットグループがFX取引向けVPSへのランサムウエア攻撃（身代金80億円要求）を受けて熊谷正寿社長が政府に能動的サイバー防御を要請した事案が大きく報じられた[1]。こうした脅威に対処する同法は、「官民連携の強化」「通信情報の利用」「アクセス・無害化措置」の3つの柱（組織・体制整備を含め4つの柱）で構成され、2025年7月1日の「国家サイバー統括室（NCO）」発足、2026年4月1日の独立機関「サイバー通信情報監理委員会」設置を経て段階的に施行されている[2]。

制度の柱	施行時期	主な規制内容・ガバナンス要件
第1の柱：官民連携の強化（届出・報告・協議会）	2026年10月1日施行	電気・ガス・金融など15分野・258者（2026年7月1日時点、今後医療も追加予定）の「基幹インフラ事業者（特別社会基盤事業者）」に対し、①特定重要電子計算機の導入届出（原則4カ月以内、既存機器は2027年3月31日期限）と、②インシデントおよび原因となり得る事象の報告（ランサムウエア等の速報は認知から3〜5日以内、DDoSは可能な限り速やか、詳報は30

		日以内）を義務化[2]。報告怠慢・是正命令違反には200万円以下の罰金、資料提出拒否等に30万円以下の罰金[26]。約100組織による官民協議会も設置[27]。
第2の柱：通信情報の利用	2027年11月までに施行予定	攻撃サーバー等を検知するため、政府が通信情報を取得・分析し機械的情報（IPアドレス等）を自動選別する仕組み[2]。同意によらない外国関連通信の取得には、2026年4月1日に設置された独立機関「サイバー通信情報監理委員会」の事前承認が必要[21]。
第3の柱：アクセス・無害化措置	2026年10月1日施行	重大な危害を防止するため緊急の必要がある場合、警察（および国外からの特に高度な組織的・計画的攻撃には自衛隊が共同）が攻撃元サーバーへアクセスし、不正プログラム消去やシャットダウン等の無害化を実施[2]。

ここでソブリンAIと直結するのが、基幹インフラ事業者が事業に用いていれば「システムベンダーやクラウド事業者が所有する機器」も届出・報告対象の「特定重要電子計算機」に該当し得るという政府解説書の規定である[2]。PwC Japanリスク・アシュアランス部の平井彰シニアマネージャーが指摘する通り、基幹インフラ事業者は運営するシステムについて「誰がアクセスし、誰が運用して何が起きたかを政府に証明できなければならない」[1]。内部構造や運用アクセス履歴が不透明な外部AIサービスではこの資産可視化・監査証跡の提出義務に対応しきれないため、統制可能なソブリンAI基盤への関心が高まっているのである[1]。

2. ソブリンAIの5層アーキテクチャと主要10社の戦略マトリクス

日経クロステックの記事で取り上げられた主要プレイヤー10社・団体の取り組みを構造化すると、ソブリンAIは単一のソフトウエアではなく、①半導体・オンプレミスAIサーバー、②ソブリンクラウド・隔離実行環境、③データ主権・オントロジー基盤、④国産・特化型AIモデル、⑤自律ガバナンス・コンプライアンス監査という5つの技術レイヤーの組み合わせによって成立していることがわかる[1]。

ソブリンAIを構成する5つの技術レイヤーと主要10社のポジショニング

日本勢（国産・国内連合）：実線枠　米グローバル勢：破線枠　▲上位層：ガバナンス・知能／▼下位層：物理・計算基盤

LAYER 5
ガバナンス・主権監査 (Governance & Audit)

主権制御の要件 (CONTROL OBJECTIVE)
地域外ベンダーを介さない運用権限の保持、暗号鍵・認証の管轄領域内管理、監査証跡の自動生成

IBM — 米グローバル勢

IBM Sovereign Core（Red Hat基盤ソフトウェア一体型主権管理）

- 顧客自身が管理するセルフマネージド・コントロールプレーン
- 認証・暗号化キー・アクセス情報・システムテレメトリー・監査証跡を主権領域内で保持
- ローカルGPU推論・エージェント処理の監視と外部エクスポート防止

LAYER 4
基盤モデル・フィジカルAI (Foundation Models & Physical AI)

主権制御の要件 (CONTROL OBJECTIVE)
国産マルチモーダル基盤モデルの開発と学習済み重みの国内限定提供、モビリティ・ロボティクス実装

Noetra（ノエトラ） — 国内44社連合

研究開発事業「FRONTia」（1兆パラメーター級 国産マルチモーダル基盤モデル）

- 中核4社（ソニーG・ソフトバンク・NEC・ホンダ）＋PFN・産総研等で推進、44社が出資
- 政府支援（2026年度予算3,873億円・NEDO）とNVIDIA Vera Rubin GPU 約2万7,500基（2028年6月稼働）
- 学習済み重みは国内の所定条件を満たす事業者に限定提供

ソニーG / ソフトバンク / NEC / ホンダ — Noetra中核4社

国産基盤モデルの領域別・産業特化実装とAIインフラ供給

- ソフトバンク：大規模AI計算インフラの提供
- NEC：フルスクラッチ開発の知見投入と特化型AI開発
- ソニーG：エンタテインメント・半導体領域への活用 ／ ホンダ：モビリティ・ロボティクス実装

LAYER 3
データ主権・オントロジー (Data Sovereignty & Ontology)

主権制御の要件 (CONTROL OBJECTIVE)
現場の暗黙知やIT/OTデータの統合管理、オントロジーによる意味体系化とAIエージェント一元管理

日立製作所 — 日本勢

HMAX Data Fabric & 社会インフラ知能基盤モデル

- IT/OTデータを統合し、オントロジーによりデータの意味や関係性を体系化（2026年9月提供）
- FDE（Forward Deployed Engineer）のドメイン知識で現場の暗黙知や業務文脈をAI-Readyデータへ変換
- Physical AI開発・運用環境およびAIエージェント管理システムで安全性・可観測性を確保

LAYER 2
ソブリンクラウド隔離 (Sovereign Cloud Isolation)

主権制御の要件 (CONTROL OBJECTIVE)
法域内のデータ駐在、接続・非接続環境に応じた運用責任の分離、国内指定オペレーターによる独立運用

Microsoft — 米グローバル勢

3形態のソブリンクラウド（パブリック / プライベート / ナショナルパートナー）

- ソブリンパブリッククラウド：ソブリンランディングゾーンと暗号化キー管理・主権証跡の保持
- ソブリンプライベートクラウド：Azure Local（接続済み／Microsoft非依存の非接続デプロイ）
- ナショナルパートナークラウド：国内指定オペレーターがローカルガバナンス下で独立所有・運用

AWS（Amazon Web Services） — 米グローバル勢

ソブリンクラウド基盤・AI主権対応クラウドサービス

- AI主権（ソブリンAI）の機運に対応するクラウドインフラおよび隔離・制御環境の提供

LAYER 1
国産シリコン・オンプレミスサーバー (Silicon & On-Premises Servers)

主権制御の要件 (CONTROL OBJECTIVE)
コンフィデンシャルコンピューティング対応の国産設計CPU、自社サーバールーム設置と国内保守網の確保

富士通 — 日本勢

国産設計プロセッサ「FUJITSU-MONAKA」（2026年11月販売開始／2027年出荷）

- Armv9-A採用、1ソケット144コア（2nm Core Die×4＋5nm SRAM/I/Oの3D積層）、NEDO助成
- Arm CCA（Confidential Computing Architecture）搭載と超低電圧動作で高効率AI推論・DCを実現
- 2029年には1.4nm世代・200コア超の「MONAKA-X」を予定

シャープ（鴻海グループ連携） — 日本勢

業務向け空冷4U「AI-B43100」& 大規模学習・推論向け液冷HGXサーバー

- 空冷4U（RTX PRO 6000 Blackwell 8基・3TBメモリ）で既存サーバールームへのオンプレ導入に対応
- 液冷システム（HGX Rubin NVL8搭載）を2027年度受注開始、2030年度に売上高約2,500億円目標
- 鴻海（Foxconn）連携・亀山工場等の国内生産検討と、全国108か所のサービス網による迅速な保守

ソブリンAIの確立には、計算インフラの物理的・論理的隔離から、現場データの構造化、国産モデルの選択、さらには法規制順守を自動証明するガバナンス層まで、**垂直統合的な主権設計**が求められる。日本勢はモデル・データ・国産CPUで強みを発揮し、米勢はソブリンクラウドと監査ソフトで攻勢をかける。

Data sources: 日経クロステック, Microsoft Learn, 日立製作所, FUJITSU-MONAKA 技術解説 (note), 一創 (Noetra事業詳細), クラウド Watch (IBM Sovereign Core), イノベトピア (シャープ AIサーバー参入)

各社が提供するソブリンAI関連製品・サービスの全体像と、それぞれの主権担保メカニズムおよび主な特徴を整理すると以下の通りとなる[1]。

企業・団体名	主な事業・提供領域	中核製品・サービス名	ソブリン**AI**における技術的特徴と主権担保メカニズム
NEC	国産AIモデル（LLM・自律型AI）	**cotomi**（コトミ）	13B/30Bパラメータの軽量設計（30BでGPU 1枚動作可能）と高速推論を強みとする[31]。最大12万8000トークン（日本語約20万語）の長文処理と図表・画像を含むマルチモーダルに対応し、海外AIへの依存を低減[1]。
富士通	国産AIモデル・国産設計AI向けCPU・サーバー	**Takane**（タカネ） **FUJITSU-MONAKA** **Fujitsu MONAKA Server**	Cohereの「Command R+」を基に日本語強化したLLM「Takane」を提供[1]。さらにTSMC 2nm/5nm採用・144コアの独自設計CPU「MONAKA」でArm CCAによるオンメモリー暗号化を実装し、2026年11月よりサーバー販売開始予定[1]。
Noetra（ノエトラ）	フィジカルAI向け国産マルチモーダル基盤モデル	**FRONTia**（フロンティア）計画	ソフトバンク・ホンダ・NEC・ソニーGの中核4社やPFNなど44社が出資[10]。政府が5年間で1兆円規模（2026年度予算は事業全体で3,873億円）の支援を予定し、

			NVIDIA Rubin約2万7,500基の計算基盤（2028年6月稼働予定）で基盤モデルを開発[1]。
日立製作所	データ主権基盤・オントロジー構築	**HMAX Data Fabric** **Physical AI FDE**	製造・物流現場のIT/OTデータや熟練者の暗黙知を「オントロジー（知識グラフ）」として体系化[1]。専門のFDEチームが現場に入り、データの作成から廃棄まで自社統制下に置く「データ主権」の環境整備を支援[1]。
シャープ	オンプレミス向けAIサーバー	業務向け**AI**サーバー（**AI-B43100**） 大規模学習・推論向け**AI**サーバー	親会社の台湾・鴻海科技集団製サーバーを自社ブランドで展開[1]。空冷4U（RTX PRO 6000 Blackwell×最大8基、2026年9月受注開始）と液冷2U予定（Rubin×8基、2027年度受注予定）を用意し、全国108拠点の保守網と亀山工場等での国内生産検討で差別化[1]。
レノボグループ	短納期オンプレミスAI導入プログラム	**Lenovo AI Express**	GPUサーバー、ネットワーク、ストレージ、ソフトを3つの検証済み構成（Small/Medium/Large）に標準化し、EUC等の手続き完了後最短**15**〜**25**営業日で工場出荷[1]。稼働

			率30%超でクラウドよりコスト優位性を発揮と試算[38]。
IBM	データ・AIの自律統制・監査ソフト	**IBM Sovereign Core**	Red Hat基盤上にセルフマネージド・コントロールプレーンを構築[30]。認証・暗号鍵・テレメトリーを主権領域内に保持し、ISO 27001、NIST、SOC 2、GDPRや各地域要件への順守を自動検証・監査レポート出力[1]。
AWS	ソブリンクラウド・隔離実行環境	**AWS専有ローカルゾーン** **AWS Nitro Enclaves**	顧客ごとに物理分離した「専有ローカルゾーン」に加え、EC2からCPU/メモリーを切り出し別ハードウエアで機密処理する「Nitro Enclaves」を提供[1]。親インスタンス管理者やAWS運用担当者でも内部データ・コードの直接閲覧や変更が不可能[1]。
マイクロソフト	ソブリンクラウド（3類型）	ソブリンパブリッククラウド ソブリンプライベートクラウド ナショナルパートナークラウド	論理独立のパブリック環境、顧客オンプレミス環境でAzure Localを動かすプライベート環境（非接続の独立動作モードも選択可）、国内パートナーのデータセンターで現地管轄下にて運用するナショナルパートナー環境を展開[1]。

オラクル	ソブリンクラウド	**OCI Dedicated Region** **Oracle Alloy**	顧客のオンプレミスや現地パートナー企業のデータセンター内でOCIのフルサービスを提供[1]。国内でも金融・製造・流通大手を中心に導入企業が拡大[1]。

3. レイヤー別技術深掘り：国産LLM・フィジカルAIから2nm国産CPU・データ主権まで

記事中で言及された各社のソリューションについて、技術仕様や事業構造の深層を掘り下げると、それぞれのプレイヤーが狙う市場ポジションと課題が浮かび上がる[1]。

3.1 モデル層：NEC「cotomi」・富士通「Takane」と1兆円規模の国家プロジェクト「Noetra（FRONTia）」

海外の巨大モデルに対する「国産LLM」の戦略は、大きく①企業システム組み込み向けの軽量・高効率モデルと、②日本の製造業・ロボティクスの競争力を賭けた国家規模のフィジカル**AI**基盤モデルの2方向に分かれている[1]。

第1の領域を推進するNECの「cotomi（コトミ）」は、企業のオンプレミス環境やプライベート環境で実用的に運用できる「軽量動作と日本語処理性能の両立」に焦点を絞っている[1]。公開資料によれば、130億（13B）パラメータモデル（GPT-4o比で2.2倍の推論速度）や、2025年10月に提供開始された30Bパラメータモデル（GPU 1枚から動作可能）を展開している[31]。コンテキスト長は最大12万8000トークン（日本語で約20万語）に対応し、2026年5月19日のアップデートでは企業文書に多用される図表や画像を含むマルチモーダル読解能力を強化した[1]。NECは2026年1月より自律型AI領域へもcotomiを展開し、生成AI関連事業で売上高500億円を目標に掲げている[31]。一方、富士通の「Takane（タカネ）」は、カナダのAIスタートアップCohereのオープンウエイトLLM「Command R+」をベースに採用し、日本語能力を強化する追加学習とファインチューニングを施すことで、海外のオープン技術を活用しつつ国内企業の主権要件を満たすアプローチを採っている[1]。

第2の領域として2026年7月16日に本格始動が発表されたのが、国産マルチモーダル基盤モデル開発会社「Noetra（ノエトラ、旧社名：日本AI基盤モデル開発）」と産業技術総合研究所（産総研）が推進する経済産業省・NEDOのプロジェクト「**FRONTia**（フロンティア）」である[10]。FRONTiaは「*Foundation for Real-world Omni-Native Trustworthy Intelligence and Alignment*（実世界を自然と理解する、信頼性の高いAI基盤）」の頭文字であり、AIが人間の意図や価値観から逸脱しない制御・安全技術（Alignment）と、ロボットや自動運転など現実の物理空間で動作する「フィジカルAI」の実現を掲げている[1]。

Noetraの出資・開発体制は、AIを作る企業と現場で使う企業を結集した44社連合（うち公式サイトで42社公表）となっている[10]。中核企業（コア4社）として、AIインフラ提供で後押しするソフトバンク、フルスクラッチの基盤モデル開発経験を持ち込み特化型AIを作る**NEC**、得た知見をエンタテインメントと半導体領域に活用するソニーグループ、モビリティとロボティクスへの社会実装を担う本田技研工業（ホンダ）が中心に位置付けられている[10]。さらに開発の中枢にはPreferred Networks（PFN）と産総

研が参画し、Sakana AIや松尾研究所、製造業からファナック、安川電機、DMG森精機、オークマ、ヤマザキマザック、川崎重工業、日立製作所、富士通、三菱電機、日本製鉄、JFEスチール、金融から3メガバンク（みずほ・三井住友・三菱UFJ）などが名を連ねる[10]。なお、独自に超軽量モデル「tsuzumi」（30B/7B/0.6B、グループAI受注額約1,478億円・引き合い2,000件）を展開するNTTグループはこの44社連合には含まれておらず、国内でも戦略が分かれている[10]。

計算インフラと予算規模も大規模である[1]。Noetraは2027年4月に構築を開始し、2028年6月に稼働させる計画で、米NVIDIAの次世代GPU「Rubin（Vera Rubin）」を約**2万7,500**基搭載したAI計算基盤を整備する[1]。技術解説記事の分析によれば、この基盤はVera Rubin NVL72構成で約382ラック相当（Vera CPU約1万3,750基、GPUメモリー物理容量合計約7.9ペタバイト、全体メモリー約28.6ペタバイト、NVFP4推論性能で理論値約1.4ゼタフロップス級、電力容量140MW級）に達し、計算ラックの市場推計価格は3,100億～5,600億円とされる[33]。政府支援は5年間で総額1兆円規模（報道ベースおよび参画企業公表の総事業規模。財務省資料における2026年度予算は事業全体で3,873億円であり、Noetraと産総研への個別配分額は非公表）が見込まれている[1]。NEDOとの契約はまず2026・2027年度分として結ばれ、毎年度のステージゲート審査を経て2026年度・2028年度・2030年度の3段階ロードマップで1兆パラメータ級などを想定した国産マルチモーダル基盤モデルを開発し、「2040年に世界市場の30%獲得」を目指す計画だ[10]。開発されたモデルの学習済み重みは、所定の条件を満たす国内事業者に限定して提供される方針であり、ソフトバンク傘下のSB Intuitions代表を務めてきたNoetraの丹波廣寅社長が「一度失敗したら、もう後がない」と語る通り、米中に次ぐ「第3の選択肢」を確立できるかの試金石となる[1]。

3.2 ハードウエア・オンプレミス層：富士通「MONAKA」、シャープ（鴻海連携）、レノボ「AI Express」の覇権争い

ソブリンAIを自社の管理下で動かすための物理インフラである「オンプレミスAIサーバー」および「半導体」領域でも、2026年秋に具体的な製品投入が相次いだ[1]。

オンプレミスAI基盤の経済合理性と導入スピード：主要ハードウエアの仕様比較

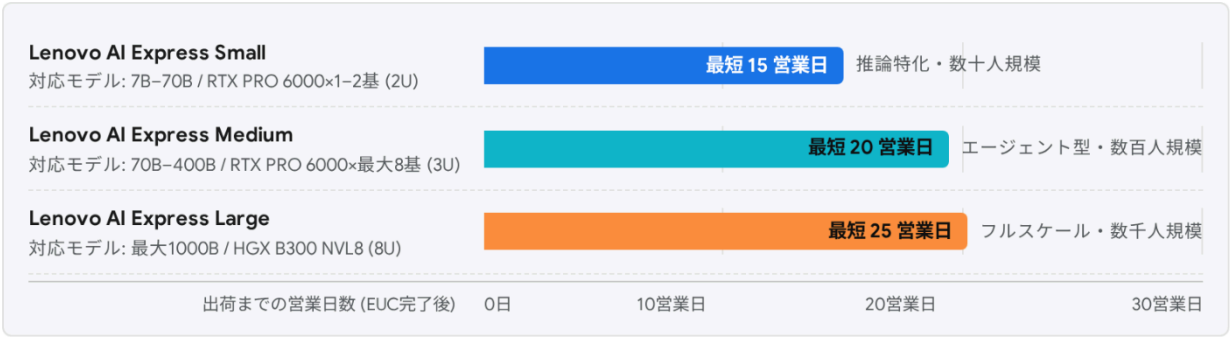
1. マクロ投資規模とオンプレミス回帰の経済指標

国家規模の投資と並行し、コスト損益分岐点から自社保有への移行が進行

Noetra政府支援規模	国内AIサーバー市場予測	オンプレミス損益分岐稼働率	中国製AIのモデル利用料衝撃
約1兆円	**4兆円**	**>30%**	**1/20**
2026年度予算 3,873億円	2030年度 (2025年度0.9兆円)	クラウドに対する経済優位点	米国製最上位モデル比の試算

2. 検証済み構成による迅速出荷リードタイム（Lenovo AI Express）

※EUC（エンドユーザー証明）および輸出承認手続き完了時点からの所要営業日数



3. 国内主要ソブリンAIハードウエア基盤の仕様比較マトリクス

独自シリコン・既存設備向け空冷・国家級液冷ファクトリーのアプローチ比較

システム / 提供主体	プロセッサー / 演算構成	冷却方式・筐体規模	主権・導入上の主要特徴	提供・稼働時期
富士通 **Fujitsu MONAKA Server**	**FUJITSU-MONAKA** TSMC 2nm (N2P) 採用 / Armv9-A / 144コア×2ソケット (最大288コア)	**1U / 2U ラック** 空冷（周囲40℃動作対応）および水冷モデルを展開	**Arm CCA 準拠暗号化** ハードウエアレベルのメモリー保護 / 石川県・笠島工場で国内製造	**2026年11月〜** 受注開始（出荷は2027年4月以降）
シャープ **AI-B43100 (業務向け)**	**RTX PRO 6000 × 8基** Blackwell Server Edition / メモリー3TB搭載	**空冷・4Uラック** 3200W電源×4基（3+1冗長構成）	**液冷配管工事が不要** 既存サーバールームへ即時設置可 / 全国108拠点の保守網	**2026年9月受注** 2027年度に販売開始予定
シャープ **NVIDIA HGX システム (大規模向け)**	**HGX Rubin NVL8** 8基のGPUをNVLinkで高速結合	**液冷方式** 大規模学習・データセンター中核向け高密度構成	**鴻海連携・国内生産検討** 亀山工場等の活用を視野 / 2030年度に事業売上2,500億円目標	**2027年度** 受注開始予定
Noetra / 産総研 **FRONTia AIファクトリー**	**NVIDIA Rubin 27,500基** Vera CPU 約13,750基 / 総物理メモリー約28.6PB / 約1.4 ZFLOPS	**液冷・約382ラック** Vera Rubin NVL72構成 / 設備電力容量 140MW級	**国家規模フィジカルAI基盤** 国内主要44社が参画し製造現場の「匠・暗黙知」をAI継承	**2028年6月** 稼働予定（2027年4月建設開始）

オンプレミスAIは安全保障だけでなく、**稼働率30%超でクラウドを上回る経済合理性**からも導入が加速している。レノボは検証済み構成で最短15営業日出荷を実現し、シャープは空冷4Uサーバーで既存サーバルームへの即時導入を狙う。一方、富士通は2nm採用の独自CPUでハードウエアレベルのメモリー暗号化を提供する。

Data sources: Business Wire (Lenovo), クラウド Watch, note (生成AIコスト試算分析), note (FUJITSU-MONAKA仕様解説), イノベトピア, note (FRONTia計画・Noetra計算基盤解説)

① 富士通「**FUJITSU-MONAKA**」：**2nm/5nm 3D**チップレットと**Arm CCA**によるメモリー暗号化

富士通がスーパーコンピューター「富岳」の技術を基にNEDO助成を受けて独自設計し、2026年11月より販売開始（2027年3月TSMC量産、2027年4月以降順次サーバー出荷予定）するAI向けプロセッサー「FUJITSU-MONAKA」は、省電力なAI推論とハードウエアレベルの機密保護を両立させる国産設計CPUである[1]。

Hot Chips 2026等の技術報告に基づく解説によれば、MONAKAは3Dチップレット積層構造（Broadcom 3.5D XDSiP技術、F2Fハイブリッドボンディング＋シリコンインターポーザ）を採用している[9]。1ソケットあたり144コア（36コア×4ダイ、2ソケット構成で288コア）のArmv9-A（Armv9.3-A）演算コアダイにのみTSMCの2nmプロセス（N2P）を採用して総シリコン面積の**30%**未満に抑え、その下に接合する**SRAM**ダイ（**LLC**全量搭載）および中央の**I/O**ダイにはTSMC 5nmプロセス（N5）を用いることで、製造コストと性能・消費電力をバランスさせ、最大動作周波数3.8GHz（ベース周波数は空冷2.1GHz／水冷2.9GHz）、TDP 350W（高効率版）／500W（高性能版）を実現している[9]。また、1コアあたり256ビットのSVE2演算ユニットを2基搭載し、行列演算の専用命令によるハードウエア支援やPCI Express 6.0 / CXL 3.0（計96レーン）、DDR5 12チャネルを備えることで、AI推論処理を効率的に実行する[9]。

ソブリンAIの観点で注目されるのが、Arm CCA（Confidential Compute Architecture）規格に準拠したコンフィデンシャルコンピューティング機能である[9]。1ソケット144コアを1/4/8ノードで使えるNUMA構成と連動し、オンメモリーで実行中のデータやアプリケーションを隔離・暗号化して保護する[1]。これにより、クラウドなどのマルチテナント環境でもデータの機密性を確保できる[1]。搭載サーバー「Fujitsu MONAKA Server」（ソブリン向け1U/2U、HPC向け2Uマルチノード水冷の3種類）は石川県の富士通・笠島工場で国内製造される一方、半導体ダイの製造自体は台湾TSMC（N2P/N5）で行われるため、「設計とサーバー製造は国内だが、ウエハー製造は海外ファウンドリーに依存する」という構造は正確に押さえておく必要がある[9]。なお富士通は2029年にコアダイを1.4nm世代へ微細化し200コア超へ拡張した次期「MONAKA-X」の投入も予定している[9]。

② シャープ：鴻海（**Foxconn**）の調達力×全国**108**拠点の保守網と「亀山工場」生産構想

シャープは2026年9月15日、親会社である台湾・鴻海科技集団（Foxconn）が製造したAIサーバーを自社ブランドで提供し、2030年度に売上高約2,500億円を目指すAIサーバー事業参入を発表した[1]。同社は国内AIサーバー市場が2025年度の0.9兆円から2030年度に4兆円、2035年度に7兆円へ拡大し、用途構成比も「学習中心」から「推論中心（2030年度に約65%）」へ移行すると予測している[12]。

第1弾として2026年9月に受注を開始（2027年度販売開始予定）した「業務向けAIサーバー（AI-B43100）」は、4Uラックマウントの「空冷方式」を採用し、「NVIDIA RTX PRO 6000 Blackwell Server Edition」を最大8基、メモリー3TB、3200W電源4基（3+1冗長構成）を搭載する[1]。液冷配管を新設せずに既存の企業データセンターや自社のサーバルームにそのまま設置できるため、企業や自治体、研究機関がオンプレミスで生成AIの推論処理やシミュレーションを導入する需要を狙う[1]。さらに2027年度には、次世代GPU「NVIDIA Rubin（HGX Rubin NVL8）」を8基搭載する液冷方式・2Uサイズ予定の「大規模学習・推論向けAIサーバー（NVIDIA HGXシステム）」の受注も開始する計画だ[1]。

シャープが掲げる強みは、複合機事業やコンビニ向け事業等で45年以上にわたり培ってきた全国**108**カ所のサービス網による迅速なフィールド保守体制（運用・保守でトゥモロー・ネット、販売でダイワボウ情報システムやリョーサン菱洋と連携）にある[1]。また、2028年度頃に構築・導入支援へ拡大するとともに、Dynabookとの連携や鴻海による国内生産（三重県の亀山工場等の活用・候補化）も

検討しており、「日本企業としての信頼性と全国サポート体制」を軸にオンプレミス市場を開拓する方針を示している[1]。

③ レノボ「**Lenovo AI Express**」：最短**15**営業日出荷と「稼働率**30%**超」の経済合理性

従来、オンプレミスAIの導入には数カ月から半年以上のリードタイムを要することが課題であった[46]。これを短縮するため、レノボ・エンタープライズ・ソリューションズは2026年10月15日、検証済みのAIシステム構成を最短15営業日で工場から出荷する「Lenovo AI Express」を日本で開始した[1]。世界30以上の製造拠点（本サービス向けNVIDIA GPU搭載機はメキシコや欧州拠点で生産）の調達力を活用し、規模や用途に応じた以下の3つの検証済み標準構成を提供している[1]。

1. **Small**構成（最短**15**営業日納品）：2U筐体「Lenovo ThinkSystem SR650a V4」にNVIDIA RTX PRO 6000を1〜2基、Intel Xeon 6530P×2基を搭載。7B〜70BモデルのAI推論にフォーカスし、30 TPSの処理速度で数十人のユーザーをサポート[11]。
2. **Medium**構成（最短**20**営業日納品）：3U筐体「Lenovo ThinkSystem SR675 V3」にNVIDIA RTX PRO 6000を最大8基、AMD EPYC 9535×2基を搭載。70B〜400Bモデルの高スループット推論やエージェント型AIに向け、30 TPSで数百人のユーザーをサポート[11]。
3. **Large**構成（最短**25**営業日納品）：8U筐体「Lenovo ThinkSystem SR680a V4」（重量約130kg）にNVIDIA HGX B300 NVL8、Intel Xeon 6776P×2基を搭載。最大1000Bまでのフルスケール生成AIモデルに対応し、数千人規模をサポート[11]。

実務上の条件として、15〜25営業日のカウントはエンドユーザー証明（**EUC**）および該当するデューデリジェンス／輸出承認手続きのすべてが完了した時点から起算される[11]。これに90日以内でのパイロット導入を支援する「AI Fast Start」や「保護・設置・最適化・稼働」の4つの包括的導入支援サービスを組み合わせることで、立ち上げの壁を下げている[11]。レノボの早川哲郎Japan ISG CTOは、安全保障や業務継続性に加え「データが発生する場所（オンプレミスやエッジ）でAI処理を実行するのが最も効率が良い」と指摘しており、同社の試算ではオンプレミス構成は稼働率が**30%**をわずかに上回る水準でクラウド利用に対する経済合理性を発揮するとされる[1]。

3.3 データ主権・ガバナンス層：日立「HMAX Data Fabric」のオントロジー戦略と「IBM Sovereign Core」の自動監査

ハードウエアとモデルを揃えても、そこに投入するデータが未整理であったり、コンプライアンス証跡が欠落していればソブリンAIは機能しない[1]。この「データ層」と「ガバナンス層」に注力するのが日立製作所とIBMである[1]。

日立製作所が2026年9月3日に販売開始した「**HMAX Data Fabric**」は、機密性の高いデータや基幹業務データの作成から活用、修正、廃棄までを完全に自社の統制下に置く「データ主権」の環境整備を支援するデータ基盤サービスである[1]。製造や鉄道、電力、物流などの現場では、ITデータとOT（制御・運用技術）データ、さらには熟練技術者の「暗黙知」が散在している[1]。日立は、IT・OT・プロダクトの専門知識を持つ「**Physical AI FDE**（**Forward Deployed Engineer**）**Team**」が顧客の現場に入り、現場の暗黙知や業務文脈を抽出して「オントロジー（特定領域の概念と概念間の関係性を体系的に定義した知識グラフ）」として構造化・蓄積する[1]。さらに、AIエージェントを一元管理して信頼性・安全性・オブザーバビリティ・コスト可視化を確保する「HMAX AI Operations」や、電力・IT・冷却設備を統合管理する「HMAX Data Center」、サイバー攻撃に備える「HMAX Cyber」と組み合わせることで、社会インフラ領域における高信頼なAI運用を支える[35]。

一方、グローバルで事業を展開する企業や政府機関が直面する「法規制順守の証明」を支援するの

が、IBMが2026年1月に発表したAI対応主権管理ソフトウエア「**IBM Sovereign Core**」である[1]。Red Hatのオープンソース基盤上に構築された同ソフトは、既存アーキテクチャの上に管理レイヤーを重ねるのではなく、主権管理機能そのものをソフトウエア自体に組み込み、顧客自身が管理する「セルフマネージド・コントロールプレーン」を提供する[30]。これにより、地域外のベンダーを介することなく、すべての認証、承認、暗号化キー、システムテレメトリー、および自動化IDを含む監査証跡を組織の管轄領域（主権領域）内で生成・保持できる[30]。その上で、ワークロードがISO 27001、NIST、SOC 2、GDPR、および各地域の主権要件に適合しているかを継続的に自動監視・検証し、監査人や規制当局向けの監査レポートを出力する機能を備えており、オンプレミスや地域内クラウドに数日以内で隔離されたマルチテナント環境を構築できる[1]。

3.4 ソブリンクラウド層：「オンプレミスAI＝ソブリンAIではない」の真意と米ハイパースケーラー3社のアプローチ

日経クロステックの記事が強調する重要な視点の一つが、「オンプレミス**AI**＝ソブリン**AI**ではない」という点である[1]。クラウドサービスを利用する場合でも、データの保存先やアクセス権限、モデルの選択、運用ポリシー、法令への準拠度合いなどを利用者側で適切に把握し選択できるようにしておけば、組織が求める主権を確保できる[1]。この「ソブリンクラウド」需要の開拓に向けて、米クラウド大手3社（AWS、マイクロソフト、オラクル）はそれぞれ異なる隔離・統制アプローチを展開している[1]。

AWSは、自社のデータセンター内で顧客ごとに物理的に分離したクラウド環境を提供する「**AWS**専有ローカルゾーン」を用意するほか、主力IaaSである「Amazon EC2」において機密データを安全に処理する隔離実行環境「**Nitro Enclaves**（ナイトロエンクレーブ）」を提供している[1]。Nitro Enclavesは、親となるEC2インスタンスから仮想CPUとメモリーの一部を切り出し、親インスタンスとは別のハードウエアを使って独立した仮想マシンを作成する仕組みである[1]。この構造により、親インスタンスの管理者やAWS自身の運用担当者（オペレーター）であっても、内部で処理されるデータやコードを直接閲覧したり変更したりできない技術的統制を担保している[1]。

マイクロソフトは、制御の範囲と導入スピードに応じた3つのソブリンクラウド形態を用意している[1]。第1の「ソブリンパブリッククラウド」は、Microsoftがインフラを運用しつつ顧客ごとに論理的に独立したAzure環境と主権コントロール・暗号化キー管理を提供し、ハードウエア調達不要で最速の導入パスを実現する[1]。第2の「ソブリンプライベートクラウド」は、顧客のオンプレミス環境で検証済みハードウエアを用いて「Azure Local」を運用する形態であり、Azureパブリッククラウドと接続を維持する「Azure Local 接続済み」構成だけでなく、デプロイ後はMicrosoftクラウドサービスに依存せず独立して動作する「**Azure Local** 非接続」構成も選択できる[1]。第3の「ナショナルパートナークラウド」は、国または地域内に本社を置く指定されたソブリンクラウドオペレーター（現地パートナー企業）がローカルガバナンスと管轄下でクラウドを所有・運用し、Microsoftの操作とは別に環境を管理する形態である[1]。オラクルも同様に、顧客のオンプレミス環境でOCI（オラクル・クラウド・インフラストラクチャー）のフルサービスを提供する「**OCI Dedicated Region**」や、現地のパートナー企業のデータセンター内でOCIのフルサービスを提供する「**Oracle Alloy**」を展開しており、国内の金融・製造・流通大手を中心に導入企業を増やしている[1]。

ただし、ソブリンクラウドの選定においては「データの機密保護（オペレーターによる閲覧防止）」と「サービスの継続可用性（外国法による輸出規制・提供停止リスク）」を分けて評価する必要がある[1]。AWSのNitro Enclavesやパブリッククラウド上の論理隔離によってデータの覗き見や域外移転を防げたとしても、クラウドの制御プレーンやAIモデルの提供元が米国企業の管轄下にある場合、2026年6月のAnthropic事案のように米国政府の輸出管理指令等によって特定モデルやサービスへのア

クセスが突如制限されるリスクを完全に排除することは難しい[1]。したがって、高度な業務継続性が求められる領域では、マイクロソフトの「Azure Local 非接続」のような独立稼働オプションや、国産LLM・オープンウエイトモデルへ迅速に切り替えられる設計を併用することが重要となる[1]。

4. 日本企業およびITベンダーへの戦略的提言：AI主権確立に向けた実践フレームワーク

ソブリンAIは単なる一過性のAI導入案件ではなく、経済安全保障や国家のアイデンティティー（教育や子ども向けサービスにおいて自国の文化・価値観・法規制に沿ったAI利用環境を選択肢として持つことを含む）を支える基幹インフラ市場である[1]。本記事および関連動向の分析から導き出される、ユーザー企業および国内ITベンダーが採るべき実践的アクションは以下の4点に集約される[1]。

4.1 業務データの機密性と事業継続性に応じた「3階層ハイブリッド主権ポートフォリオ」の設計

すべての業務を単一の国産AIやオンプレミス環境に統一することは、コスト面でもAIの性能進化への追随面でも現実的ではない[1]。企業は自社のAIワークロードを以下の3階層に分類し、業務特性に応じた主権レベルを設計することが有効である[1]。

1. **Tier 1**（基幹インフラ・極秘データ・OT制御領域）：経営戦略、製品の設計図面、製造ノウハウ（熟練者の暗黙知）、および「サイバー対処能力強化法」の特定重要電子計算機に関わる領域[1]。ここは外部サービスの停止に左右されないよう、オンプレミスAIサーバー（Fujitsu MONAKA Server、シャープ製AIサーバー、Lenovo AI Express等）や独立運用可能なソブリンプライベートクラウド上に、NEC「cotomi」や富士通「Takane」、将来の「Noetra」モデル等の国産・オープンウエイトモデルを配置し、日立「HMAX Data Fabric」によるデータ統制と「IBM Sovereign Core」等の自動監査機構を組み合わせる[1]。
2. **Tier 2**（一般社内業務・顧客情報処理領域）：社内文書の検索・要約、コード生成、業務自動化など[4]。AWS（専有ローカルゾーン / Nitro Enclaves）、Microsoft Azure（ソブリンパブリッククラウド）、Oracle（Dedicated Region / Alloy）などのソブリンクラウド環境上で、データの保存先・アクセス管理・学習非利用を統制しつつ、海外の主要モデル（Claude Opus / SonnetやGPT系など）と国産LLMを適材適所で併用する[1]。
3. **Tier 3**（定型大量処理・非機密データ領域）：定型帳票の作成や一般的な問い合わせ整理など、最高水準の推論性能よりも費用対効果が重視される領域[4]。ここでは低価格なオープンモデル等を日本国内の管理された環境で運用しコストを圧縮する選択肢が成り立つが、「入力データの保存先」「適用される国の法規制」「外部からの更新管理と脆弱性対応」「処理履歴の監査可能性」の6項目を厳格に検証し、海外クラウドAPIへの無防備な依存や中国の輸出制限対象技術への単一依存を避けることが前提となる[4]。

4.2 「モデル・ポータビリティ（代替可能性）」を前提としたシステム疎結合設計

2026年6月のAnthropicによるFable 5 / Mythos 5の緊急停止や、2024年のOpenAIによるGPT-3.5系モデル終了が示した教訓は、「今そのモデルが動いていること」と「数時間後も同じモデルが使える保証があること」は別問題であるという点だ[1]。日経クロステックの関連報道でも指摘されている通り、「どのSDKでシステムを作るか」と「背後でどのAIモデルを回すか」を別の意思決定として切り離す設計が不可欠である[51]。特定のAIベンダーや単一モデルが止まった際に業務全体が停止する状態を作らないよう、抽象化されたモデル切り替え層を設け、規制やトラブルの発生時には即座に別ベン

ダーのモデルやオンプレミスの国産LLMへエンジンを載せ替えられる体制を整えておく必要がある[1]。

4.3 2027年3月末の「特定重要電子計算機」届出期限に向けたサプライチェーン対応の4ステップ

2026年10月1日に施行されたサイバー対処能力強化法により、基幹インフラ15分野・258事業者は、施行時点で導入済みの特定重要電子計算機について**2027年3月31日**までに事業所管大臣へ届け出る義務を負っている[2]。委託先やクラウド提供元が管理する機器も報告対象になり得るため、基幹インフラ事業者およびそのサプライチェーン（開発・納入元、運用保守委託先、中小企業を含む取引先）は以下の4つの備えを速やかに進める必要がある[2]。

1. 取引先と該当業務の確認：自社の取引先（直接取引だけでなく孫請け等の間接関与を含む）に、内閣府が公表する15分野・258者の基幹インフラ事業者（および今後追加予定の医療分野）が含まれるかを確認する[2]。
2. **IT・OT・クラウド資産の棚卸しと可視化**：基幹インフラ事業者が届け出る「特定重要電子計算機」のうち、自社が納入・運用・保守しているハードウエア、ソフトウエア、クラウドアカウント等を洗い出し、製品名・製造者名・機能・設置場所の台帳を最新化する[2]。
3. セキュリティ・**AI**運用記録の保持：取引先や規制当局から対策状況を確認された際に「誰がアクセスし、誰が運用して何が起きたか」を証明できるよう、OSやアプリの更新、定義ファイル更新、アクセス履歴、バックアップ復旧テストの実施日時などを監査可能な記録として残す[1]。
4. インシデント発生時の早期連絡・報告フローの整備：不正アクセスやマルウエア実行だけでなく「その原因となり得る事象（兆候）」を認知した際、基幹インフラ事業者が目安となる3〜5日以内の速報（詳報30日以内）を国へ提出できるよう、サプライチェーン間の連絡手順とログ保存期間を定める[2]。

4.4 日本のITベンダーにとっての「勝ち筋」：マルチベンダー統合インテグレーション

最後に、日本のITベンダー（富士通、日立製作所、NEC、シャープ、国内SIer各社）にとっての真の商機は、国産モデルや国産ハードウエアの単独販売にとどまらない[1]。記事が結論づけている通り、行政や社会インフラ企業、製造業などの大手企業に向けて、海外の優れたLLMやクラウドサービスも柔軟に活用しつつ、産官連携の国産モデル（Noetra）や自社の強みである独自LLM（cotomi、Takane）、機密保護ハードウエア（FUJITSU-MONAKAや国内保守網付きAIサーバー）、そして現場の暗黙知を構造化するデータ基盤（HMAX Data Fabric）を組み合わせて、「日本で安心して利用できる**AI**基盤」の構築・運用を統合的に支援することこそが、日本のITベンダーにとって最も有力な「勝ち筋」となる[1]。

引用文献

1. 富士通・日立・AWSも、「ソブリンAI」で競演　AI主権の機運に商機見いだす _ 日経クロステック（xTECH）.pdf
2. 2026年10月施行「サイバー対処能力強化法」で何が変わる？ 基幹, https://business.ntt-west.co.jp/bizclip/articles/bcl00163-065.html
3. AnthropicがLLM「Fable 5/Mythos 5」の提供を停止 - IT Leaders, https://it.impress.co.jp/articles/-/29459
4. 日本企業はなぜ中国製AIを選び始めたのか？ | IT-daytrading - note,

https://note.com/it_daytrading/n/nfec376311bb0
5. 中国のAI輸出規制案とは？モデルの重み・23技術の中身と日本企業, https://ai-revolution.co.jp/media/china-ai-export-control-draft/
6. 使っているAIが、ある日突然止まる「アクセスの該非判定」が問, https://timewell.jp/columns/ai-access-export-control-2026
7. 【2026年6月13日】Fable 5とMythos 5が突然使えなくなった理由, https://note.com/kazu_t/n/n8138e02885b9
8. 能動的サイバー防御へ本格始動、基幹インフラ 15 分野 258 事業者に, https://s.netsecurity.ne.jp/article/2026/11/06/56684.html
9. 富士通「FUJITSU-MONAKA」からMONAKA-X、富岳NEXTへ - note, https://note.com/kagawatomo/n/n0e6b4892ebad
10. Noetra（ノエトラ）とは｜出資44社の一覧、NTT・富士通の参画, https://www.issoh.co.jp/tech/details/11749/
11. レノボ、AIサーバーを最短15営業日で納品する「Lenovo AI Express, https://cloud.watch.impress.co.jp/docs/news/2148576.html
12. シャープのAIサーバ参入、なぜ空冷4Uからか｜強みは全国の保守網, https://innovatopia.jp/ai/ai-news/117897/
13. 米Anthropicが最新AI「Mythos 5」の提供を全面停止 米政府の輸出, https://www.sbbit.jp/article/cont1/185751
14. Claude Fable 5が利用停止｜理由と今後の動向, https://www.sei-san-sei.com/blog/blog-0419.html
15. AIモデルの輸出規制（Export Controls on AI Models）とは・意味, https://harch.jp/ai/glossary/export-controls-on-ai-models
16. AI規制と企業リスク管理 Anthropicモデル強制停止が示す統治の, https://crystal-method.com/blog/amazon-warning-white-house-anthropic-mythos-shutdown-implications/
17. Anthropic、Claude Fable 5／Mythos 5へのアクセスを停止 - gihyo.jp, https://gihyo.jp/article/2026/06/suspend-access-to-fable-5-and-mythos-5
18. 大規模言語モデル・太陽光シリコンウエハーなど40技術を輸出管理, https://finance.biggo.jp/news/00109a7c-e877-4c3f-b098-ed3841de8f90
19. 中国商務部など、輸出を制限・禁止する技術目録の第 5次改正草案を, https://www.jetro.go.jp/biznews/2026/10/7ff8e9cb1624ef81.html
20. 中国、AI技術23項目の輸出管理へ――ドイツはNVIDIAと産業AI協業, https://note.com/china_case/n/nec3f6b950dc2
21. 能動的サイバー防御とは？2026年施行のサイバー対処能力強化法で, https://cyseek.jp/column/proactive-cyber-defense/
22. 攻撃者から80億円要求 GMO熊谷社長「応じず」“きょう正午”利用客, https://www.fnn.jp/articles/-/1140414
23. GMO、2年前の脆弱性指摘を「生かせず」熊谷会長が初会見で陳謝, https://finance.biggo.jp/news/0032bc55-70d5-49e8-8fdb-c37603e2f92c
24. 社内のホワイトハッカー「誰より悔しい」不正アクセス受けたGMO, https://www.sankei.com/article/20261026-FPM5XMZGCZP4RDOXILAKMEOOFE/?outputType=asynd
25. Contents「能動的サイバー防御法」の施行と企業実務, https://mypage.tokyo-cci.or.jp/mypage/contents/column/11872.php

26. 能動的サイバー防御とは？関連法の概要と企業の対応義務を解説, https://www.ntt.com/business/lp/acd.html
27. 「能動的サイバー防御」とは：サイバー攻撃を未然に防ぎ、被害, https://internet.watch.impress.co.jp/docs/column/keyword/2148826.html
28. 能動的サイバー防御の導入による基幹インフラ事業者への影響, https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/active-cyber-defense-impact2.html
29. デジタル主権の導入 - Cloud Adoption Framework - Microsoft Learn, https://learn.microsoft.com/ja-jp/azure/cloud-adoption-framework/sovereignty/executive-strategy
30. IBM、AIを活用したデジタル主権管理環境を構築・管理するための, https://cloud.watch.impress.co.jp/docs/news/2079929.html
31. 2026年 日本の国産LLM採用, https://yorozuipsc.com/uploads/1/3/2/5/132566344/japan_domestic_llm_2026.pdf
32. 国産LLMを徹底比較！各モデルの特徴と選び方【2026年最新版】, https://spikestudio.jp/blog/japan-llm-companies
33. 日本政府の国家AIインフラ、Rubin GPU 2万7500基・約382ラック, https://note.com/kagawatomo/n/n1074c341fd24
34. PFN岡野原大輔氏の見立てと国産AI「Noetra」の実像, https://yorozuipsc.com/uploads/1/3/2/5/132566344/3e35972a4fc5767805c4.pdf
35. 日立「HMAX」を拡充 データセンター／セキュリティ, https://enterprisezine.jp/news/detail/25011
36. AIエージェントは現場で動くのか？ - 日立がHMAXで挑む社会, https://news.mynavi.jp/techplus/article/20260904-4915796/
37. 現場全体の自律的な最適化に向け、HMAX Data Fabricなど新たな, https://www.hitachi.com/ja-jp/press/articles/2026/09/0903d/
38. レノボ、実証済み・検証済みのユース・ケースでAI Libraryを拡充し, https://home.kingsoft.jp/news/pr/businesswire/20261022201085.html
39. IBM Sovereign Core, https://www.ibm.com/jp-ja/products/sovereign-core
40. ソニー・ソフトバンク・NEC・ホンダらの「国産マルチモーダル, https://businessnetwork.jp/article/35932/
41. Noetra（ノエトラ）とは？国産AIの狙い・参加企業・開発計画, https://visioncon-global.com/ai-plus/ai-plus-vol-19
42. 一度失敗したら後はない」――Noetra丹波社長の危機感が伝わった, https://hashout.jp/ai/8256/
43. Fujitsu MONAKA Server | 富士通, https://global.fujitsu/ja-JP/offering/fujitsu-monaka-server
44. ISC High Performance 2026に参加・展示しました #3 ～次世代Arm, https://blog.fltech.dev/entry/2026/08/06/isc2026-monaka-ja
45. GPU不足に新たな選択肢、エクストリーム-Dらが循環型GPUサーバ, https://news.mynavi.jp/techplus/article/20261020-5162230/
46. オンプレミスAIインフラの構造：短納期化が拓く社内実装の現実解, https://www.pheedo.jp/physical-ai/7699/
47. レノボが「Lenovo AI Express」を発表 AIインフラの本番導入を最短, https://enterprisezine.jp/news/detail/25290

48. HMAX Data Fabric・HMAX AI Operations・Physical AI FDE Team, https://www.hitachi.com/ja-jp/products/digital/data-fabric-operations/
49. 継続的なコンプライアンス - IBM Sovereign Core, https://www.ibm.com/jp-ja/products/sovereign-core/continuous-compliance
50. ソブリンクラウドとガバメントクラウドの違い｜データ主権・法域, https://www.issoh.co.jp/tech/details/16789/
51. 特筆すべきAI関連ニュース(10月4日～10月10日)｜HIROE - note, https://note.com/hiroe28/n/n98db0c841a93