ChatGPT

「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、日本のAI主権戦略を読み解く

エグゼクティブサマリ

日経クロステックの2026年11月5日付記事「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」は、ソブリンAIを「自国・自組織のデータやIT基盤を用い、外部への過度な依存を避けながらAIを主体的に管理・運用する仕組み」と捉え、AIが基幹業務へ浸透するにつれて、データ保存場所、管理者アクセス、モデル利用、クラウド依存、半導体調達まで含めた「AI主権」が企業ITの新しい競争軸になると論じている。記事は富士通、日立、AWSだけでなく、NEC、IBM、Oracle、Microsoft、Sharp、Lenovoなども含め、LLM、サーバー、データ基盤、クラウド、ガバナンスソフトの各層で「ソブリンAI」をめぐる市場形成が始まったと整理している。filecite turn0file0

記事の問題設定は概ね妥当である。2026年時点の日本政府は、単なる「国産化」ではなく、特定国・特定企業への過度な依存を避けつつ複数のモデルや基盤を選択可能にする「開かれたAI主権」を政策言語として明確化している。2026年7月に閣議決定された第 II 期「人工知能基本計画」や政府高官の説明では、戦略的自律性と戦略的不可欠性を確保することがAI政策の柱に置かれている。デジタル庁もガバメントAI「源内」で、AWS等のグローバルクラウドとさくらのクラウド、海外モデルと国産モデルを併用しながら比較評価する構成を採っており、日本の政策は「完全な国産閉鎖系」ではなく「選択肢と切替可能性を持つマルチソース型主権」に近い。 1

企業別にみると、**富士通の差別化はスタックの垂直統合**にある。日本語LLM「Takane」、生成AI基盤、国内設計・開発・製造をうたう「FUJITSU-MONAKA」と「Fujitsu MONAKA Server」、コンフィデンシャルコンピューティングを組み合わせ、モデルからCPU・サーバーまでを主権要件に結び付けている。2026年9月14日の公式発表では、MONAKA Serverを「ソブリンAI基盤」と明示し、国内製造による部品・製造履歴のトレーサビリティまで差別化要素としている。 2

日立の差別化はIT×OTと運用主権である。HMAX Data FabricはIT・OT・現場データや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、HMAX AI OperationsがAIの性能、ガバナンス、セキュリティ、コスト、ハルシネーション等を継続監視する。さらに、Hitachi EverFlexではクラウド基盤そのものの透明性、バックアップ、暗号化、法規制対応、仮想化基盤の選択肢を提供する。したがって日立の「主権」は、国産モデルそのものよりも、社会インフラの現場データと運用権限を企業側に残すことに重点がある。 3

AWSの差別化は「国産化」ではなく、ハイパースケールの機能を維持しながら主権境界を技術的に切ることにある。AWS Nitro System、顧客管理鍵、外部キーストア、専用環境、AWS AI Factories、AWS European Sovereign Cloudなどを使い、データ所在地、管理者アクセス、運用者所在地、メタデータ、制御プレーンを分離する。2026年1月14日に一般提供を開始したAWS European Sovereign Cloudは既存AWSリージョンから物理・論理的に独立し、EU域内運用を設計要件としている。2026年10月24日にはEU域外インフラに依存せず稼働できることを公開演習で実証した。 4

したがって、今後の市場で重要なのは「国産か外資か」という二分法ではない。調達側が評価すべきなのは、**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、切替可能性の九つについて、誰がどこまで支配できるか**である。EUのCloud and AI Development Act案も、主権を単一の要件ではなく複数の保証レベルとして制度化する方向にあり、日本でも今後、公共調達や重要インフラのRFPで

類似の「主権保証レベル」が実務上の評価軸になる可能性が高い。これは本稿の分析上の推論だが、日本政府の「自律性・代替性・耐遮断性」、EUの4段階ソブリン保証制度の方向性から合理的に導ける。 5

記事の要約と主要論点、事実検証

記事の中心的な主張は、「AIを業務システムの深部に組み込むほど、企業の設計図、製造ノウハウ、契約書、顧客情報、OTデータなどをAIが扱うため、従来のクラウド主権・データ主権だけでは不十分になり、モデル、推論環境、運用者、サプライチェーンまで統制するAI主権が必要になる」というものである。記事冒頭の三つのポイントも、①自国・自社のデータやIT基盤で主体的にAIを運用すること、②業務システムへのAI組込みが深まるほど重要性が高まること、③大手ITベンダーが構築・運用支援事業を強化していること、の三点に要約できる。filecite turn0file0

記事のp.3に掲載された一覧表は、ソブリンAI市場を単一製品カテゴリーではなく、AWS・Oracle・Microsoftのソブリンクラウド、IBMのSovereign Core、NEC・富士通の国産LLM、日立のHMAX Data Fabric、Sharp・LenovoのオンプレミスAIサーバーなどの集合として捉えている。この見方は重要で、実際にIBMもSovereign Coreを「顧客が制御プレーン、ID、鍵、ログ、AI推論を自ら統制するためのソフトウェア」と定義しており、AWSもAI sovereigntyをインフラ、モデル、データ、アクセス制御、運用レジリエンスを含むスタック全体の問題として位置付けている。filecite turn0file0 6

主要な記事記述の検証結果は次の通りである。

記事の記述・主張	検証結果	原典・評価
富士通は日本語能力を強化したLLM「Takane」を展開	**確認済み**	富士通はCohereと共同開発し、2024年9月30日にTakaneを発表・提供。日本語企業用途、プライベート環境対応を強調している。 7
富士通はMONAKA搭載サーバーを2026年11月から販売	**確認済み。ただし販売開始と一般出荷開始は区別が必要**	2026年9月14日発表。販売開始は11月だが、公式には一般向けの順次出荷開始を2027年4月以降としている。記事の表現だけ読むと「11月から即時出荷」と誤解しやすい。 8
MONAKAにはメモリ上データを暗号化する機能がある	**確認済み**	富士通はVM単位のメモリ暗号化によるコンフィデンシャルコンピューティングを仕様として説明している。 9
日立はAI向けデータ基盤「HMAX Data Fabric」を提供	**確認済み**	2026年9月3日提供開始。IT/OTデータや暗黙知をオントロジーで体系化し、ナレッジグラフとしてAIに供給する。 10
IBMはデータ・AIの自律運用を支援する「IBM Sovereign Core」を提供	**確認済み**	2026年5月5日に一般提供開始。顧客運用型制御プレーン、境界内ID・鍵・ログ、ローカル推論、継続的コンプライアンスを特徴とする。 11
AWSなど米クラウド大手がソブリンクラウドを強化	**確認済み**	AWS European Sovereign Cloudは2026年1月14日GA。OracleもEU Sovereign Cloud、Dedicated Region、Alloy等を提供している。 12

記事の記述・主張	検証結果	原典・評価
米中間でAI半導体の輸出規制・囲い込みが激化	**概ね確認済み。ただし規制内容は動的**	米BISは先端AI半導体・製造装置への規制を継続している一方、2026年1月にはH200等について一定条件下で中国向け輸出を個別審査へ変更した。したがって「一律禁止」ではなく、品目・顧客・用途別の規制と表現すべき。 13
日本政府の能動的サイバー防御の導入がソブリンAI需要を押し上げる	**方向性は妥当。ただし直接の因果は政策文書で明記されていない**	サイバー対処能力強化法は2025年5月成立。重要インフラの説明責任・監査性・運用統制への要求は高まるが、「ソブリンAIを導入せよ」と直接規定しているわけではない。 14

記事の最も重要な洞察は、p.8以降で示される「オンプレミスAI＝ソブリンAIではない」という点である。サーバーが自社建屋にあっても、外部ベンダーが管理者権限を持ち、暗号鍵やログが海外の制御プレーンに送信され、モデル更新が外部依存なら、主権性は限定的である。IBMはまさにこの問題を、顧客運用制御プレーン、境界内の鍵・ID・ログという設計で解決しようとしており、AWSもNitro、外部キーストア、専用環境などで同じ課題に異なるアプローチを取っている。turn0file0 15

富士通・日立・AWSの製品・サービス比較

三社を同じ「ソブリンAI企業」として一括りにすると本質を見誤る。富士通は「国内技術＋垂直統合」、日立は「現場データ＋運用統制」、AWSは「ハイパースケール＋技術的分離」という異なる戦略で競争している。 16

企業	主な製品・サービス	発表・提供時期	主な機能・主権要素	導入・検証事例	公開価格
富士通	Takane	2024年9月30日	Cohere Command系をベースに日本語・企業用途へ最適化。プライベート／オンプレミス環境での利用を想定。RAG、特化学習、生成AIトラスト技術等と組合せ可能。 17	デジタル庁「源内」でTakane 32Bをさくらのクラウド上に載せ、2026年9〜11月に比較検証。 18	**未確認**。今回確認した公式ページでは一般向け単価を確認できず。
富士通	Fujitsu Kozuchi Enterprise AI Factory	少なくとも2026年2月時点で公式紹介	顧客専有環境でモデル開発、運用、継続学習を回し、機密データを外部へ出しにくい構成。 19	公開された固有顧客事例は今回の調査では確認できず。	**未確認／問い合わせ型**。公式問い合わせ窓口は存在するが公開料金表は確認できず。 20

企業	主な製品・サービス	発表・提供時期	主な機能・主権要素	導入・検証事例	公開価格
富士通	FUJITSU-MONAKA / Fujitsu MONAKA Server	2026年9月14日発表、11月販売開始、順次出荷は2027年4月以降	国内設計・開発、国内工場製造、部品・製造履歴のトレーサビリティ、CPU単体AI推論、メモリ暗号化によるコンフィデンシャルコンピューティング。 2	2026年8月末から約45社へ先行検証サーバー貸出。金融、通信、製造の一部顧客へ先行提供予定。 21	**未確認**。公開定価を今回確認できず。
日立	HMAX Data Fabric	2026年9月3日提供開始	IT/OT/機器データ、熟練者の暗黙知をオントロジーで整理しナレッジグラフ化。AIモデルやAgentic AIと接続。 10	日立ハイテクの材料製造・計測データ統合など「カスタマーゼロ」の実践を基に製品化。 22	**個別見積**。 22
日立	HMAX AI Operations / Physical AI FDE	2026年9月3日提供開始	AI性能、ガバナンス、セキュリティ、コストを継続監視。ハルシネーションやデータ品質劣化を含むAI固有リスクを運用面から抑制。 22	日立社内での多数のAIエージェント運用ノウハウを活用。 22	個別見積を基本とするサービス群。 22
日立	Hitachi EverFlex クラウドサービス	2025年12月19日から順次	プライベート／マルチテナント、暗号化、バックアップ、監査、法規制対応、Hyper-V/KVM/OpenShiftの選択。HMAX基盤としても活用。 23	金融・電力・交通等で培った運用ノウハウを製品化。特定顧客名は当該発表では非開示。 24	**未確認**。公開定価を今回確認できず。
AWS	AWS AI Factories	2025年12月2日提供開始	顧客のデータセンター内にAWS専用AI基盤を配置。Trainium／NVIDIA GPU、Bedrock、SageMaker、Nitroを組み合わせ、データプレーンを主権境界内に保持可能。 25	政府・規制産業向けを対象。具体的な顧客名を伴うAI Factory本番事例は今回確認した公式資料では限定的。	**営業問い合わせ**。公式FAQはアカウントチームへの相談を案内。 26
AWS	AWS European Sovereign Cloud	2026年1月14日GA	既存AWSから物理・論理分離。EU内データ・メタデータ、独立IAM・課金、EU居住スタッフによる運用、Bedrock/SageMaker利用。 27	Dedalus、Mendix、BTC/Esriなどが利用。医療、GIS、規制産業向け事例あり。 28	EUR建て。一般AWS同様のサービス別課金。個別サービス料金は公開されるが、全体TCOは構成依存。 29

企業	主な製品・サービス	発表・提供時期	主な機能・主権要素	導入・検証事例	公開価格
AWS	Amazon Bedrock	継続提供	複数基盤モデル、IAM、Guardrails、ログ、暗号化。Bedrockは顧客データを基盤モデルの学習には使用しないとAWSが明記。 30	世界10万超の組織が利用とAWSが公表。 30	**公開従量課金**。例えば東京リージョンのGemma系は100万トークン単位で入力／出力課金。モデルごとに異なる。 31

価格の比較には注意が必要である。富士通・日立のソブリンAIはSI、専有環境、サーバー、運用支援を含むことが多く、AWS Bedrockのような「1トークン単価」と横並びにできない。実務上は、初期構築費、GPU/CPU設備、データセンター、電力、ライセンス、モデル利用、MLOps、監査、セキュリティ運用、DR、移行・出口費用まで含む5〜7年TCOで比較すべきである。これは各社の提供形態の違いから導く分析上の結論である。 32

三社の競争を一言でまとめると、**富士通＝「国産スタックを所有する主権」**、**日立＝「現場と運用を掌握する主権」**、**AWS＝「グローバル技術を境界内で制御する主権」**である。この三つは互いに排他的ではなく、日本企業の実システムではTakaneを国内クラウド上で動かしつつ、AWSを別ワークロードで併用し、日立がデータ統合・運用を担うといった複合構成も十分あり得る。実際、デジタル庁「源内」自体が国産クラウド・国産LLMとAWS等を併用する構成である。 18

日本政府のAI主権政策、ガイドライン、法制度

日本では「ソブリンAI法」という単独法が存在するわけではない。現行制度は、AI法、人工知能基本計画、AI事業者ガイドライン、ガバメントクラウド政策、ガバメントAI、経済安全保障、サイバー安全保障を組み合わせてAI主権を形成している。2025年6月4日に公布された「人工知能関連技術の研究開発及び活用の推進に関する法律（AI法）」は、同年9月1日に全面施行され、AI戦略本部、AI基本計画、研究開発・人材・国際規範・リスク調査等の政府施策を法的枠組みに置いた。 33

2026年7月14日に閣議決定された第 II 期人工知能基本計画では、AI開発・利用能力の強化が安全保障・競争力の問題として扱われている。政府は「開かれたAI主権」を、特定国・企業への過度な依存を避けて継続運用できる「戦略的自律性」と、日本の強みを世界に提供する「戦略的不可欠性」の両立として説明している。したがって、日本のAI主権政策は「海外技術排除」ではなく、複数のクラウド、モデル、計算資源を使いつつ、遮断や制裁、供給停止が起きても代替できる構造を作る考え方である。 34

AI事業者ガイドラインは2026年3月31日に第1.2版へ更新された。これは法的拘束力を中心とするEU型とは異なり、AI開発者、提供者、利用者に対して人間中心、安全性、公平性、プライバシー、セキュリティ、透明性、アカウンタビリティ等の実践指針を示すソフトロー型のガバナンスである。AI法の施行後も、このガイドラインが企業の実務的AIガバナンスの重要な基準となっている。 35

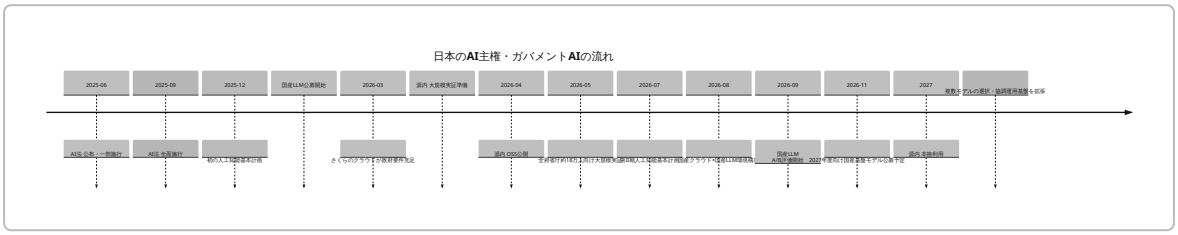
最もAI主権を具体化しているのがデジタル庁のガバメントAI「源内」である。2026年度には全府省庁約18万人を対象に大規模実証を行い、2027年度以降の本格導入を計画している。2026年夏には、NTTデータ「tsuzumi 2」、富士通「Takane 32B」、Preferred Networks「PLaMo 2.0 Prime」をさくらのクラウドで稼働させ、海外モデルとA/Bテストして有用性・信頼性・経済性を検証している。これは、政府調達そのものを国内AI産業育成と主権強化に用いる明確な産業政策でもある。 36

2027年度向けには、ガバメントAIで使用する国産基盤モデルの有償調達を予定しており、2026年11月に公募を行う計画が公表されている。政府は「国産モデルを使うこと」そのものを目的にするのではなく、性能評価を通じて実用可能なモデルを選定し、行政からの利用フィードバックと安定需要を国内AI開発へ還流させようとしている。 37

クラウドについても、2026年3月27日に「さくらのクラウド」が政府の全技術要件を満たし、ガバメントクラウドの本番環境として利用可能になった。これにより、日本政府はAWS等のグローバルクラウドだけでなく国産クラウドも実運用可能な選択肢として持つようになった。デジタル庁はガバメントクラウドに305項目の技術要件を課しており、この調達制度は実質的に「主権」「セキュリティ」「可搬性」を市場へ要求する政策手段になっている。 38

さらにサイバー安全保障では、2025年5月にサイバー対処能力強化法と関連整備法が成立した。重要インフラ等について、攻撃兆候の把握、政府・事業者間連携、運用状況の説明可能性を高める方向で制度が強化されている。AIが重要インフラの制御・判断に組み込まれるほど、アクセス権、ログ、モデル更新、外部接続を国内主体が検証できることの重要性が増すため、ソブリンAI市場への間接的な需要喚起要因となる。後半部分は政策文書を踏まえた分析上の推論である。 14

政策ロードマップは次のように整理できる。 39



海外のソブリンAIとの比較

EUは主要地域の中で最も「主権」を制度として明示的に定義する方向に進んでいる。既存のAI ActがAIのリスク・透明性・高リスク用途を規制する一方、2026年6月に欧州委員会が提案したCloud and AI Development Act（CADA）は、クラウドとAI計算基盤の「ソブリン保証」を4段階で評価する制度を導入しようとしている。Level 1はEU域内処理・保存、上位レベルでは第三国からの独立性、EU企業による所有・支配、人員要件、ソフトウェアサプライチェーンの完全な透明性まで要求する構想である。 40

EUは同時に、EuroHPCを用いたAI Factoriesを19拠点規模で整備し、AI Gigafactoryでは10万個超の先端AIプロセッサーを集約する構想を進めている。つまりEU型ソブリンAIは「規制だけ」でなく、計算資源、公共調達、研究開発、オープンソース、データセンターを一体化した産業政策である。 41

英国はEUより規制色が弱く、国家計算資源・半導体・企業育成に重点を置く。2025年のUK Compute Roadmapに続き、2026年6月には11億ポンド規模のAI Hardware Planを発表し、新しい国家AIスーパーコンピューター、次世代チップ購入、英国企業への投資を打ち出した。英国の「sovereign AI」は、自国計算能力とスタートアップを確保しつつ海外技術とも連携する産業・安全保障政策としての性格が強い。 42

米国は「ソブリンAI」という国内規制用語を中心に据えるより、AI技術・データセンター・半導体の世界的優位と輸出管理を国家戦略としている。2025年7月のAmerica’s AI Action Planは、国内AIインフラの急速な建設、米国AIフルスタックの同盟国輸出、先端半導体輸出管理の強化を柱とする。この意味で米国の主権戦略は「自国市場を外資から守る」より、「米国スタックを世界標準として維持し、戦略的競争相手への技術流出を制御する」外向きの主権政策である。 43

中国はデータ、アルゴリズム、生成AIサービス、コンテンツ、ネットワーク安全保障を一体的に国内規制する。生成AI暫行管理弁法は、合法な学習データ、個人情報・知的財産保護、生成内容管理、安全評価、国内法への準拠を要求し、安全で信頼できるチップ、ソフトウェア、算力、データ資源の利用を奨励している。中国型は「国内市場・データ・モデル・計算基盤を国家規制下に置く」度合いが最も強い。 44

比較すると次のようになる。

地域	技術面	運用面	規制・政策面	主権モデル
日本	国産LLM、国産クラウド、MONAKA等を育成しつつ海外クラウドも併用。 45	複数モデル・複数クラウドの選択、代替性、耐遮断性を重視。 46	AI法＋基本計画＋ガイドライン中心。	**開かれた戦略的自律性**
EU	AI Factories、Gigafactories、域内クラウドを拡充。 41	EU居住・国籍要件、域内制御プレーン等を段階的に要求。 47	AI Act＋CADAで法制化を強化。 48	**法規制型・保証レベル型主権**
英国	国家スーパーコンピューター、国内チップ企業支援。 49	国家的計算資源へのアクセスを強化。	比較的イノベーション重視。 50	**計算資源・産業能力型主権**
米国	GPU、クラウド、モデル、データセンターの世界優位を維持。 51	同盟国に米国AIスタックを輸出。	輸出規制と産業政策を組合せ。 52	**技術覇権・輸出管理型主権**
中国	国内クラウド、モデル、チップ、算力網を統合。	国内法・登録・安全評価下で運用。	データ・生成AI・ネット安全保障を強く規制。 44	**国家統制型主権**

日本はEUほど「誰が所有するか」を法的に固定せず、米国ほど自国技術スタックに圧倒的優位があるわけでもない。このため、日本に最も合理的なのは「国産比率100%」ではなく、国産の最低限の代替能力を確保しつつ、AWS、Microsoft、Oracle等のグローバル技術を利用し、依存先を複線化することである。この方向性は政府が明示する「戦略的自律性」「開かれたAI主権」と整合する。 53

市場機会、競争構造、主要リスク

最も早く需要が立ち上がる顧客は、政府・自治体、防衛、金融、通信、電力、交通、医療、製造、研究機関である。これらは機密情報、個人情報、OTデータ、国家安全保障情報、知的財産を扱い、AI障害や外部サービス停止が事業継続に直接影響する。実際、AWS European Sovereign Cloudは公共部門・金融・医療などを主要対象とし、日立は金融・電力・交通の運用経験をソブリン型クラウドに転用し、富士通もMONAKA Serverの対象に防衛、金融、通信、製造を挙げている。 54

主なユースケースは、行政文書RAG、法令・規制検索、金融審査、不正取引検知、医療文書解析、製造設備保全、設計ノウハウ検索、AIエージェントによる運用自動化、ロボット・フィジカルAI、機密データを使うモデル微調整、サイバー防御である。日立がHMAX Data FabricをOT・フィジカルAIへ展開し、デジタル庁が行政文書RAGや政府共通データを源内へ投入していることからも、「汎用チャット」より「組織固有データと行動権限を持つAI」が主権需要の中心になるとみられる。 55

収益モデルは、①ハードウェア販売、②クラウド従量課金、③基盤モデルAPI、④専有環境の月額・年額利用料、⑤構築SI、⑥データ統合・オントロジー構築、⑦MLOps／AIOps、⑧セキュリティ監視、⑨法規制・監査対応、⑩マネージドサービスの十層に分解できる。特に継続収益性が高いのは運用・監査・AIモデル管理で

あり、日立のHMAX AI Operations、IBM Sovereign Core、AWSのマネージド主権環境はいずれも「導入後の継続的統制」を価値とする。[56]

競合は大きく四群に分かれる。国内フルスタックでは富士通、NEC、NTTデータ、Preferred Networks、さくらインターネット。国内SI・OT型では日立。グローバルクラウドではAWS、Microsoft、Oracle。ソブリン制御ソフトではIBMが強い。さらにSoftBankはOracle Alloyを用いて日本国内データセンターから主権型クラウド・AIサービスを提供する計画であり、クラウド事業者自身が「国内ブランドのハイパースケーラー互換環境」を構築するモデルも登場している。[57]

富士通にとって最大の機会は、日本政府が「国産クラウド×国産モデル×国産計算基盤」を一定比率で確保しようとする場合に、モデル、CPU、サーバー、SIを一括提供できる点である。一方の脅威は、GPUエコシステムとソフトウェア開発者基盤でNVIDIA／CUDA中心の世界に対抗する必要があること、また「国産」にプレミアム価格を支払う顧客がどこまで広がるかである。MONAKAのCPU単体AI推論性能は富士通が強く訴求しているが、実アプリケーション性能やAIソフトウェア生態系は今後の導入実績で評価される段階である。[58]

日立の機会は、生成AI単体ではなく、鉄道、電力、工場など「AIが物理世界を動かす」領域へ進むことである。この領域ではデータ所在地だけでなく、設備制御ルール、熟練者の判断、停止条件、監査ログまで含めて主権化する必要があり、IT×OTの蓄積は差別化しやすい。一方、基盤モデルやGPUそのものは外部エコシステムへの依存が残りやすく、主権価値を「完全国産」ではなく「運用統制」として説明できるかが重要になる。[59]

AWSの機会は、企業が「AWSの機能を失いたくないが、規制上は独立性が必要」という最大市場を取り込める点にある。European Sovereign CloudやAI Factoriesは、このトレードオフを解消しようとする商品である。一方の最大リスクは、米国企業であること自体が一部顧客の「法的主権」要件に抵触すると評価される可能性であり、EUがCADAで所有・支配・人員国籍まで主権保証レベルに組み込もうとしていることは、このリスクを端的に示す。[60]

横断的なリスクとして、第一に**技術リスク**がある。オンプレミス化・専有化するとクラウドの最新モデル、GPU更新、運用自動化の恩恵を受けにくくなり、主権性と技術鮮度がトレードオフになる。第二に**法務リスク**として、個人情報、知財、越境移転、AI Act等の海外規制、輸出管理が複雑化する。第三に**倫理・ガバナンスリスク**として、国内モデルであってもハルシネーション、バイアス、誤判断は消えない。第四に**サプライチェーンリスク**として、国産サーバーであってもEDA、製造装置、メモリ、先端製造プロセスなどを100%国内化することは現実的ではない。第五に**国際関係リスク**として、米中技術規制の変更がGPU・モデル・クラウド提供条件を突然変える可能性がある。[61]

このため、企業が採用すべき考え方は「完全な技術自給」ではなく、**依存関係を可視化し、重大な依存について代替可能性を持つこと**である。これは日本政府が掲げる自律性・代替性・耐遮断性とも一致する。[46]

実務向け示唆、推奨アクション、利害関係者マップ

短期、すなわち今後6〜12カ月で企業が最初に行うべきことは、「ソブリンAI製品を買うこと」ではなく、自社のAI主権要件を定義することである。具体的には、データ、モデル、推論、学習、暗号鍵、IAM、ログ、管理者、ネットワーク、アップデート、半導体・サーバー、災害時運用の各項目について、「国内必須」「自社管理必須」「第三者運用可」「海外可」を分類する。EUやIBM、AWSの主権アーキテクチャが示す通り、データ所在地だけでは主権評価として不十分である。[62]

短期のRFPでは、少なくとも「顧客データの保存場所」「メタデータとテレメトリーの保存場所」「ベンダー管理者のアクセス経路」「暗号鍵の所有者」「モデル学習への二次利用」「モデル・クラウドの切替方法」「監査証跡」「ネット遮断時の継続運用」「部品・ソフトウェアSBOM」「終了時のデータ搬出と削除証

明」を質問項目に入れるべきである。AWS European Sovereign CloudやIBM Sovereign Coreがデータだけでなくメタデータ、鍵、管理者、制御プレーンを主権要件に含めていることは、この評価軸の妥当性を裏付ける。 63

中期、1〜3年では「二重化されたAI基盤」を構築するのが現実的である。一般機密度の業務はAWS等のハイパースケーラー、重要機密・OT・政府案件は国内クラウドまたは専有環境、さらにモデルは海外モデルとTakane、cotomi、PLaMo、tsuzumi等を切り替え可能にする。デジタル庁「源内」が複数モデルをA/B比較し、2027年度以降に複数モデルをタスクに応じて選択・協調させる方向を示していることは、民間企業にも有効な参照モデルである。 64

中期では同時に、モデルそのものより「データ層」を自社資産化すべきである。HMAX Data Fabricが示すように、AIに使える形でデータと業務知識をオントロジー化・ナレッジグラフ化できれば、LLMベンダーを変更しても企業固有の知識資産は保持できる。逆にRAG、評価データ、プロンプト、エージェントのツール定義が特定ベンダー独自形式に固定されると、形式上はマルチクラウドでも実質的なロックインになる。 10

長期、3〜5年以上では「AI版BCP」を経営課題として制度化する必要がある。想定すべき事象は、海外モデル提供停止、GPU輸出規制、クラウドリージョン障害、国際回線遮断、ベンダー撤退、法規制変更、AIモデルの重大脆弱性である。AWSがEuropean Sovereign Cloudについて2026年10月にEU域外との接続を切った独立運用演習を実施したのは、主権を単なる契約条件ではなくBCPとして検証する象徴的事例である。 65

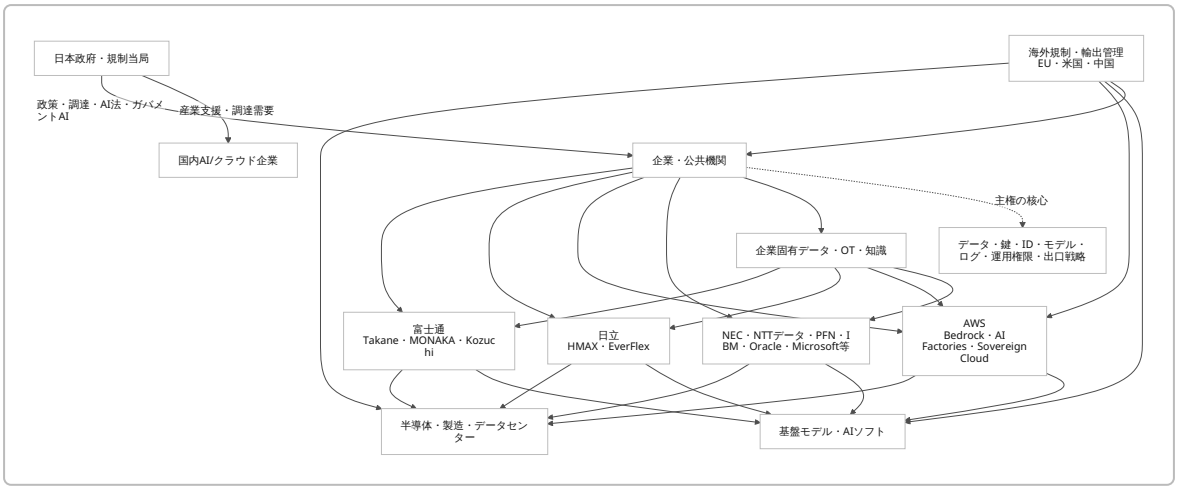
経営判断としては、「どのベンダーが最もソブリンか」を決めるのではなく、ワークロードごとに必要な主権強度を決めるべきである。一般的な社内FAQでは低い主権レベルで十分でも、防衛、制御系、医療、金融取引、政府機密では、専有インフラ、顧客保有鍵、国内運用者、ネットワーク隔離、監査可能性まで必要になる。EUが主権保証を4段階にしようとしているのも、この「用途別に必要強度が異なる」という発想に基づく。 66

実務上の優先順位は以下の一つの流れにまとめられる。

1. **短期：主権要件を棚卸しする。** AI・データ・クラウド・鍵・ログ・管理者・サプライチェーンの依存先を可視化し、重要度を分類する。
2. **短期：複数ベンダーでPoCする。** 国産LLM、海外LLM、国内クラウド、ハイパースケーラーを同一評価データで比較し、精度だけでなくコスト、監査性、切替時間を測定する。
3. **中期：データ／知識層をベンダーニュートラル化する。** RAG、オントロジー、評価セット、AIエージェントのツール仕様を企業資産として管理する。
4. **中期：二系統以上のAI実行経路を持つ。** 一方のクラウドやモデルが停止しても重要業務を継続できる最小構成を設ける。
5. **長期：AI版BCP・出口戦略を監査対象にする。** 年1回程度、モデル停止、ネット遮断、鍵失効、クラウド移行を含む切替演習を行い、復旧時間をKPI化する。

これらの推奨は、日本政府が掲げる「自律性・代替性・耐遮断性」、IBMの顧客運用型制御プレーン、AWSの独立運用実証、EUの段階的主権保証という共通方向から導いたものである。 67

最後に、ソブリンAI市場の利害関係を図示すると次のようになる。政府は規制者であると同時に最大級の需要家であり、クラウド・モデル・半導体・SIの各社は競合しながら相互依存する。ユーザー企業にとって重要なのは、その相互依存の中心に自社の「制御権」を残すことである。 68



この記事を深掘りした結論は、**「ソブリンAI」は製品カテゴリーではなく、AIシステムにおける支配権の設計原則である**ということに尽きる。富士通、日立、AWSは同じ市場に見えて実際には異なる層を主戦場としており、勝者が一社に決まる市場ではない。むしろ企業・政府の調達は「国産か海外か」から、「どの層を誰に依存し、どこに代替経路を持つか」というポートフォリオ設計へ移る可能性が高い。日本政府が「開かれたAI主権」を掲げ、国産モデルを育成しながらAWS等も併用している現状は、その方向性を既に先取りしている。 69

---

1 53 69 小野田大臣記者会見（令和8年6月30日）｜政府広報オンライン
https://www.gov-online.go.jp/press_conferences/minister_of_state/202606/video-312153.html?utm_source=chatgpt.com

2 8 16 世界トップレベルのAI推論性能を実現する国産次世代CPU「FUJITSU-MONAKA」とソブリンAI基盤を実現する国産サーバ「Fujitsu MONAKA Server」販売開始について
https://global.fujitsu/ja-JP/pr/news/2026/09/14-02?utm_source=chatgpt.com

3 10 55 59 現場全体の自律的な最適化に向け、HMAX Data Fabricなど新たな基盤・運用管理ソリューションを提供開始：日立
https://www.hitachi.com/ja-jp/press/articles/2026/09/0903d/?utm_source=chatgpt.com

4 12 27 29 54 60 63 Opening the AWS European Sovereign Cloud | AWS News Blog
https://aws.amazon.com/jp/blogs/aws/opening-the-aws-european-sovereign-cloud/?utm_source=chatgpt.com

5 46 67 第12回デジタル社会構想会議｜デジタル庁
https://www.digital.go.jp/councils/social-concept/fd4f3007-18b2-4f88-a48a-1ba40c94a729?utm_source=chatgpt.com

6 15 Introducing IBM Sovereign Core: A new software foundation for sovereignty
https://www.ibm.com/new/announcements/introducing-ibm-sovereign-core-a-new-software-foundation-for-sovereignty?source=WEB_Search_INDIA&utm_source=chatgpt.com

7 FUJITSUファミリ会
https://jp.fujitsu.com/family/online/p415/pdf/415_settion1.pdf?utm_source=chatgpt.com

9 Next Arm Processor FUJITSU-MONAKA and Its Technologies
https://www.fujitsu.com/global/imagesgig5/FUJITSU-MONAKA.pdf?utm_source=chatgpt.com

11 IBM Japan Newsroom - ニュースリリース
https://jp.newsroom.ibm.com/2026-05-05-think-2026-ibm-makes-digital-sovereignty-operational-with-general-availability-of-ibm-sovereign-core?utm_source=chatgpt.com

13 52 61 産業安全保障局
https://www.bis.gov/press-release/department-commerce-revises-license-review-policy-semiconductors-exported-china?trk=article-ssr-frontend-pulse_little-text-block&utm_source=chatgpt.com

14 サイバー安全保障に関する取組（能動的サイバー防御の実現に向けた検討など）｜内閣官房ホームページ
https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo_torikumi/index.html?trk=article-ssr-frontend-pulse_little-text-block&utm_source=chatgpt.com

17 Fujitsu Uvance update
https://www.fujitsu.com/global/documents/about/ir/library/presentations/Uvance%20update%2020240716.pdf?utm_source=chatgpt.com

18 45 64 ガバメントAI 源内における国産クラウド上での国産基盤モデルの試用開始について｜デジタル庁
https://www.digital.go.jp/news/7eef939d-1c58-4229-b210-7b5adc9af590?utm_source=chatgpt.com

19 新たなAI活用の幕開け！専有環境で実現する自律型生成AIプラットフォーム：富士通
https://seminar.jp.fujitsu.com/public/seminar/view/130016?utm_source=chatgpt.com

20 Fujitsu Kozuchi Enterprise AI Factoryに関するお問い合わせフォーム : 富士通
https://contactline.jp.fujitsu.com/contactform/csque34803/7105394/?utm_source=chatgpt.com

21 2026年度2Q決算概要
https://www2.jpx.co.jp/disc/67020/140120261029559004.pdf?utm_source=chatgpt.com

22 32 56 現場全体の自律的な最適化に向け、HMAX Data Fabricなど新たな基盤・運用管理ソリューションを提供開始：日立
https://www.hitachi.com/ja-jp/press/articles/2026/09/0903d/?phai=260903&utm_source=chatgpt.com

23 日立、企業システムにおけるソブリン性の確保やモダナイズを促進する、新クラウドサービスを提供開始 - Digital Evolution Headline:日立
https://deh.hitachi.co.jp/_ct/17812787?ct=rel&fr=wg&utm_source=chatgpt.com

24 日立、企業システムにおけるソブリン性の確保やモダナイズを促進する、新クラウドサービスを提供開始 - Digital Highlights:デジタル:日立
https://digital-highlights.hitachi.co.jp/_ct/17812098?tg=%E3%82%AF%E3%83%A9%E3%82%A6%E3%83%89&utm_source=chatgpt.com

25 Introducing AWS AI Factories - AWS
https://aws.amazon.com/about-aws/whats-new/2025/12/aws-ai-factories/?utm_source=chatgpt.com

26 Amazon Web Services | AI Factories FAQs
https://aws.amazon.com/about-aws/global-infrastructure/ai-factories/faqs/?utm_source=chatgpt.com

28 BTC & Esri Success Story
https://aws.amazon.com/partners/success/btc-esri/?utm_source=chatgpt.com

30 Amazon Bedrock – Build genAI applications and agents at production scale – AWS
https://aws.amazon.com/bedrock/?utm_source=chatgpt.com

31 Amazon Bedrock の料金
https://aws.amazon.com/jp/bedrock/pricing/?utm_source=chatgpt.com

33 39 人工知能関連技術の研究開発及び活用の推進に関する法律（ＡＩ法） - 科学技術・イノベーション - 内閣府
https://www8.cao.go.jp/cstp/ai/ai_act/ai_act.html?utm_source=chatgpt.com

34 人工知能基本計画 - 科学技術・イノベーション - 内閣府
https://www8.cao.go.jp/cstp/ai/ai_plan/ai_plan.html?utm_source=chatgpt.com

35 AI事業者ガイドライン（METI/経済産業省）
https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/20260331_report.html?utm_source=chatgpt.com

36 68 ガバメントAI「源内」｜デジタル庁
https://www.digital.go.jp/policies/genai?utm_source=chatgpt.com

37 ガバメントAIで使用する国産基盤モデルの公募について（予告）｜デジタル庁
https://www.digital.go.jp/news/207cadc2-c218-42f6-92ec-c0eda476b49c?utm_source=chatgpt.com

38 ガバメントクラウド｜デジタル庁
https://www.digital.go.jp/policies/gov_cloud?utm_source=chatgpt.com

40 47 62 66 Cloud and AI Development Act | Shaping Europe’s digital future
https://digital-strategy.ec.europa.eu/en/policies/cloud-and-ai-development-act?utm_source=chatgpt.com

41 AI Factories | Shaping Europe’s digital future
https://digital-strategy.ec.europa.eu/en/policies/ai-factories?utm_source=chatgpt.com

42 50 UK Compute Roadmap - GOV.UK
https://www.gov.uk/government/publications/uk-compute-roadmap?utm_source=chatgpt.com

43 51 White House Unveils America's AI Action Plan – The White House
https://www.whitehouse.gov/releases/2025/07/white-house-unveils-americas-ai-action-plan/?utm_source=chatgpt.com

44 生成式人工智能服务管理暂行办法
https://cqca.miit.gov.cn/zwgk/zcwj/flfg/art/2026/art_27b7613aa2b8419384caa6c31fbdd7f0.html?utm_source=chatgpt.com

48 AI Act | Shaping Europe’s digital future
https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai?utm_source=chatgpt.com

49 A decisive shift to power British AI: new £1.1 billion plan to back chip firms, boost computing power and skills for the AI revolution - GOV.UK
https://www.gov.uk/government/news/a-decisive-shift-to-power-british-ai-new-11-billion-plan-to-back-chip-firms-boost-computing-power-and-skills-for-the-ai-revolution?utm_source=chatgpt.com

57 SoftBank Corp. Accelerates Japan's AI and Sovereign Cloud Future with Oracle Alloy | About Us | SoftBank
https://www.softbank.jp/en/corp/news/press/sbkk/2025/20251008_01/?utm_source=chatgpt.com

58 Fujitsu launches made-in-Japan next-generation CPU FUJITSU-MONAKA and Fujitsu MONAKA Server for sovereign AI infrastructure | Fujitsu Global
https://global.fujitsu/en-global/pr/news/2026/09/14-02?utm_source=chatgpt.com

65 Inside a successful AWS European Sovereign Cloud exercise to demonstrate independent operation | AWS Security Blog
https://aws.amazon.com/blogs/security/inside-a-successful-aws-european-sovereign-cloud-exercise-to-demonstrate-independent-operation/?utm_source=chatgpt.com