「ソブリン AI」記事の深掘り検証

ベンダー各社の主張・政策の裏付けと知財戦略への示唆

対象記事：日経クロステック「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」（2026 年 11 月 5 日）[1]

作成日：2026 年 11 月 9 日（記載内容は同日までに確認した情報に基づく）

Claude Opus 5.5

凡例

【確認済み】一次ソース（企業・政府発表等）または複数の報道で裏付けた事実
【分析】筆者による評価・推論（事実と区別して記載）
【未確認】本書作成時点で裏付けを得られなかった事項
本文中の上付き番号［n］は巻末「参考文献」の番号に対応する。

エグゼクティブサマリー

1. **記事の骨格は正確。**Anthropic の最新モデル停止（2026 年 6 月 12 日〜7 月 1 日）、中国の AI 技術輸出管理案（10 月 16 日公表）、サイバー対処能力強化法の主要部分施行（10 月 1 日）、Noetra の計画、各社製品の発表内容は、一次ソースまたは複数の報道で確認できた。
2. **ただし時期と提供範囲の解像度が粗い。**富士通 MONAKA Server は「11 月販売開始」だが一般出荷は 2027 年 4 月以降、シャープは受注開始であって納入は 2027 年度から、Microsoft のナショナル パートナー クラウドは仏独向け、中国の規制は意見募集中の「案」、能動的サイバー防御の通信情報利用は未施行である。
3. **記事が触れていない論点が二つある。**第一に、米国企業の「ソブリンクラウド」でも米国法の管轄は消えないこと（仏上院での Microsoft France 幹部の証言）。第二に、最先端モデルは提供者側のデータ保持を利用条件にし得ること（Anthropic の 30 日保持義務と、その後の見直し）。主権の実体は、データの所在地ではなく、鍵・運用者・契約・出口の管理で決まる。
4. **知財部門の優先事項は三つ。**①外部 AI に入力する前のデータ分類、②学習利用・保持・削除証明・派生成果物の帰属を契約で確保すること、③主力モデル停止時の代替を用意すること。日立型の「暗黙知のオントロジー化」は営業秘密の特定を容易にする一方、流出時の損害も大きくする両刃の剣である。

1. 記事の要旨と構図

1-1. 要旨

記事は、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持つ AI システムを「ソブリン AI」と呼ぶ。そのうえで、国産 LLM（NEC・富士通）、オンプレミス AI サーバー（富士通・シャープ・レノボ）、データ主権とコンプライアンス管理（日立・IBM）、ソブリンクラウド（AWS・Microsoft・Oracle）の各社の取り組みを紹介する。「オンプレミス AI＝ソブリン AI」ではないと指摘し、海外の LLM・クラウドと国産技術を組み合わせた「日本で安心して利用できる AI 基盤」の構築支援が日本の IT ベンダーの勝ち筋だと結論づけている[1]。

1-2. 各社が解決する「主権」の層は異なる

【分析】記事は 10 社を同列に並べているが、各社が担う「主権」の層は異なる。ユーザー企業が必要とする層も業務ごとに違うため、次の三層に分けて読むと整理しやすい。

層	問われること	記事中の主な取り組み
技術主権	モデル・半導体・計算基盤を自国で作れるか	NEC「cotomi」、富士通「Takane」「FUJITSU-MONAKA」、Noetra
運用主権	誰が運用し鍵を持つか。遮断されても動かせるか	シャープ・レノボのオンプレミス向けサーバー、Oracle Alloy、AWS 専有ローカルゾーン
データ主権	データの所在・アクセス・準拠法・監査を証明できるか	日立「HMAX Data Fabric」、IBM「Sovereign Core」、AWS「Nitro Enclaves」

平将明衆院議員（元デジタル相）も、AI は半導体、データセンター、クラウド、基盤モデル、アプリケーションの各層で成り立つとし、何をもって「国産」とするかを冷静に見極め、他国にチョークポイントを握られないことに資源を割くべきだと述べている[2]。

2. 記事の事実主張の検証

2-1. 記事の記述と確認結果

記事の記述	確認結果	評価
Anthropic は 2026 年 6 月、国家安全保障上の懸念と米政府の輸出管理命令を受け、最新モデルの提供を停止（影響は限定的）	**【確認済み】**米政府は 6 月 12 日、Fable 5／Mythos 5 に輸出管理を適用し、米国内外の外国籍者へのアクセス制限を求めた。国籍をリアルタイムで確認できないため、同社は両モデルを全ユーザーに対して停止した[3,4]。6 月 30 日に規制が解除され、7 月 1 日に再展開された[5,6]。措置の契機は、研究者が安全対策の回避手法を報告したこととされる[7]。	正確。ただし停止は全世界・全ユーザーに及んだ。「限定的」は旧モデルが使えたという意味にとどまる
中国も 2026 年 10 月、LLM や AI エージェントなど AI 技術を輸出管理対象に追加する方針を発表	**【確認済み】**商務部・科学技術部公告 2026 年第 48 号（10 月 16 日）。AI・バイオ医薬・太陽光の計 40 項目を加える技術目録の改正案で、AI は大規模モデル、エージェント、計算クラスター等の 23 項目。公開済み（オープンソース化・論文発表済み）の技術は対象外。意見募集は 11 月 15 日まで。輸出前登録は公告日から暫定実施[8,9]。	正確。ただし目録改正は意見募集中の「案」で未確定
政府は 2026 年 10 月、能動的サイバー防御（ACD）始動へ根拠法「サイバー対処能力強化法」などを施行	**【確認済み】**2025 年 5 月 16 日成立、23 日公布。届出・報告義務などの主要規定は 2026 年 10 月 1 日施行[10]。同日、自衛隊によるアクセス・無害化措置も始まり、警察による同措置は 11 月までに施行予定とされた[11]。通信情報の利用は、公布から 2 年 6 カ月以内に政令で定める日に施行[12]。直接の対象は基幹インフラ 15 分野 258 事業者（2026 年 7 月 1 日時点）[13]。	概ね正確。ACD は段階的な始動で、通信情報の利用は未施行
Noetra：44 社出資、Rubin 約 2 万 7500 基、2027 年 4 月構築開始・2028 年 6 月稼働、政府は 5 年で 1 兆円規模（2026 年度約 3873 億円）	**【確認済み】**44 社出資、Rubin 約 2 万 7500 基、2027 年 4 月構築開始・2028 年 6 月稼働は 7 月 16 日の発表で確認[14]。Vera CPU 1 万 3750 基超、140MW 規模[15]。初年度に約 3873 億円の助成を受ける[16]。「5 年で約 1 兆円」は 2025 年 12 月の報道で、同報道は 2026 年度予算を約 3000 億円としていた[17,18]。	事実関係は確認。1 兆円は確定予算ではなく、報道された政府方針
富士通「Fujitsu MONAKA Server」を 2026 年 11 月から販売予定	**【確認済み】**9 月 14 日発表。CPU・サーバーとも 11 月に販売開始。サーバーは 2026 年度下期に金融・通信・製造の一部顧客へ先行提供し、日本・欧州向け出荷は 2027 年 4 月以降。CPU 単体の提供は 2026 年度第 4 四半期から[19,20]。	「販売」は正確。一般出荷は 2027 年 4 月以降で、調達計画上は要注意

記事の記述	確認結果	評価
シャープ：業務向け AI サーバーの受注を 2026 年 9 月に開始。大規模学習・推論向け（Rubin×8、液冷）は 2027 年度受注予定	**【確認済み】**9 月 15 日、業務向け（RTX PRO 6000 Blackwell 最大 8 基）の受注を開始。販売開始は 2027 年度[21]。大規模向けは「NVIDIA HGX Rubin NVL8」搭載の液冷機と報じられている[22]。2030 年度に AI サーバー売上高約 2500 億円が目標[21]。	正確。ただし受注開始であり、納入は 2027 年度から
レノボ「Lenovo AI Express」：3 つの検証済み構成、最短 15 営業日で出荷	**【確認済み】**10 月 15 日発表。Small（RTX PRO 6000×2、15 営業日）、Medium（同×8、20 営業日）、Large（HGX B300 NVL8、25 営業日）[23]。	正確
Microsoft「ソブリン パブリック クラウド」「ナショナル パートナー クラウド」など	**【確認済み】**2025 年 6 月 16 日に欧州向けに発表。ナショナル パートナー クラウドは仏 Bleu、独 Delos Cloud（SAP 子会社）が運営する形態[24]。 **【未確認】**日本での同等の提供	欧州向けの枠組み。日本でも同様に使えるかのような読み方は不正確
NEC cotomi：最大 12 万 8000 トークン（日本語で 20 万語）	**【確認済み】**NEC 公式ページに「128K（日本語で 20 万語）」と記載[25]。	正確

2-2. 補足（記事外・記事以降の動き）

- **富士通：**Takane は Cohere の「Command R+」をベースとし、富士通がグローバルで独占提供するモデルである[26]。FUJITSU-MONAKA は 2nm の 3D 積層 CPU で、Arm CCA（機密コンピューティング）に対応する。AI 推論で他社 CPU 比 2 倍、サーバー台数と消費電力の半減を掲げるが、いずれもメーカー公称値である[27]。サーバーは国内の笠島工場で製造し、部品の出所と製造履歴を追跡可能にするとしている[28]。
- **NEC：**記事と同日の 11 月 5 日、「cotomi Gateway」の提供開始を発表した。機密情報を自動で検知・マスキングして外部 AI モデルに渡し、マスキングでは処理しにくいタスクはオンプレミスのモデルに振り分ける[29]。ソフトウェア版は月額 100 万円（税別）から[30]。**【分析】**国産 LLM 一本から、外部モデルを安全に使うための仲介層へと戦略の軸が広がっている。
- **IBM：**Sovereign Core は 2026 年 1 月の発表時点で、2 月にテックプレビュー、2026 年半ばに一般提供の予定とされた[31]。5 月 5 日（Think 2026）に一般提供を開始した[32]。顧客が運用するコントロールプレーン、ID・暗号鍵・ログ・監査証跡の境界内保持、継続的なコンプライアンス監視と証跡の自動生成を備える[33]。

- **日立**：HMAX Data Fabric は 2026 年 9 月 3 日に提供を開始した[34,35]。現場データと熟練者の暗黙知をオントロジーで体系化し、AI が使える知識資産として蓄積する。IT・OT・プロダクトの専門家チーム「Physical AI FDE Team」が、現場知の抽出から運用まで伴走する[35]。
- **AWS**：2026 年 1 月 15 日、EU 域内にあり他リージョンから物理的・論理的に分離した「AWS European Sovereign Cloud」をドイツ・ブランデンブルクで一般提供開始した[36]。ドイツへの投資額は 78 億ユーロ超[37]。**【未確認】**記事にある Nitro Enclaves と専有ローカルゾーンの日本での提供条件。
- **Oracle**：野村総合研究所（NRI）は「OCI Dedicated Region」を世界で初めて採用し、「Oracle Alloy」を国内で初めて稼働させた。GPU も導入し、ソブリン AI の実現に向けた展開を表明している[38]。2025 年 2 月には大阪でも Alloy を稼働させ、AI 実行基盤サービスを打ち出した[39]。

3. 記事が十分に触れていない論点

3-1. 米国ハイパースケーラーの「ソブリンクラウド」の法的限界

【確認済み】2025 年 6 月 10 日、仏上院の公共調達に関する調査委員会で、Microsoft France の公共政策・法務担当ディレクター、アントン・カルニオー氏が宣誓のうえ証言した[40]。仏市民のデータが仏当局の同意なく米当局に渡らないことを保証できるかとの問いに対し、同氏は「Non, je ne peux pas le garantir（保証できない）」と答えた[40,41]。

【分析】運用者を EU 居住者に限り、物理的に分離しても、親会社が米国法人である限り、米 CLOUD Act 等による法的強制の可能性は原理的に残る。これを補うのが、現地資本が運営するパートナー型（仏 Bleu・独 Delos）や、顧客が鍵を保持する設計（外部鍵管理・機密コンピューティング）である。日本で現時点で最も近い実例は、国内事業者の NRI が自社データセンターで運営する Oracle Alloy である。

3-2. 「供給停止」と「データ保持条件」という新しいリスク

【確認済み】Anthropic は 2026 年 6 月、Fable 5 など Mythos 級モデルの利用条件として、悪用監視を目的にプロンプトと出力を 30 日間保持することを求めた。この条件はゼロデータ保持の契約を結んでいた企業顧客にも適用された[42]。同社は企業の反発を受け、9 月 1 日の Fable 5.1 発表と同時に方針を見直した。監視データを顧客自身のクラウド環境内に置く新方式（Enterprise Frontier Safeguards）を秋に向けて段階的に導入し、それまでは適格な顧客にゼロデータ保持での利用を認めるとしている[43,44]。

【分析】一連の経緯は二つのことを示した。一つは、米国の法的強制が「データ提出」ではなく「サービス停止」の形でも外国ユーザーに及び得ること。もう一つは、最先端モデルほど提供者側のデータ保持が利用条件になり得ることである。記事は前者を「影響は限定的」と評したが、知財の観点では後者の方が重い（4-1 参照）。条件は数カ月単位で変わるため、契約時点の条件を固定し、変更時の通知と解約権を確保しておくことが重要である。

3-3. 市場規模と各国の動き

【確認済み】Gartner は 2026 年 2 月 9 日、世界のソブリンクラウド IaaS 支出が 2026 年に 800 億ドル（前年比 35.6%増）に達すると予測した[45]。2026 年の地域別では中国 474 億ドル、北米 164 億ドル、欧州 126 億ドルで、2027 年には欧州（231 億ドル）が北米（211 億ドル）を上回る見込みである[46]。2026 年の成長率は中東・アフリカ 89%、成熟アジア太平洋 87%、欧州 83%と予測されている[47]。同社は、ソブリン化に伴って現行ワークロードの約 20%がグローバル事業者から地域事業者へ移ると見ている[45]。なお、この集計には AWS European Sovereign Cloud や Delos Cloud が含まれる一方、Microsoft Sovereign Cloud は含まれないと報じられている[48]。「ソブリン」の定義自体が調査機関によって異なる点に注意が要る。

【確認済み】欧州委員会は 2025 年 4 月 9 日に「AI Continent Action Plan」を公表した。InvestAI で 2000 億ユーロの投資動員を掲げ、うち 200 億ユーロを最大 5 カ所の AI ギガファクトリーに充てる。ただし、2000 億ユーロの大半（1500 億ユーロ）は民間企業連合による拠出表明である[49]。

【分析】EU は公的資金と域内事業者で計算基盤を作る路線、中国は今回の輸出管理案が示すとおり技術流出の防止を主権の中心に置く路線をとる。日本は Noetra（官民による計算基盤とモデル）、国産 LLM、海外クラウドの国内運用型を組み合わせるハイブリッド路線である。インド・韓国・中東の個別政策は、本書では検証していない。

3-4. 日本政府の方針：「全部国産」ではなく「耐遮断性＋複数モデル統御」

【確認済み】人工知能基本計画（第 II 期、2026 年 7 月 14 日閣議決定）は、戦略的自律性と戦略的不可欠性を確保し、開かれた「AI 主権」を確立するとした。行政・防衛・重要インフラ等の戦略領域では「耐遮断性と運用能力」を確保し、特定の国や企業への過度な依存を避けるため複数モデルを統御しながら利用するとしている。ガバメント AI「源内」による国内最大規模 18 万人の政府職員の AI 利用や、営業秘密等の機微情報の国外流出リスクへの対応も明記した[50]。

【分析】政府方針は、記事の結論（海外技術と国産技術の組み合わせ）と整合する。企業にとっての含意は「国産を選ぶか否か」ではない。「止まっても業務が回るか」「機微情報が国外に出ないか」を設計で担保することである。

3-5. 国産 LLM とオープンウエイトの主権上の論点

【分析】国産 LLM は日本語処理や軽量動作に強みがある一方、コーディングやエージェント用途の最先端性能では米国勢に差がある。現実的な役割は、機密・規制領域で常用するモデル兼、海外モデル停止時のフォールバックである。オープンウエイトのモデルをベースにする場合（Takane は Command R+ベース[26]）、主権上の論点は三つある。

- ベースモデルのライセンスが、派生モデルの商用利用や移転にどんな条件を課すか。
- 学習データの来歴が不透明だと、著作権・個人情報のリスクを引き継ぐ。
- 中国系モデルについて、今回の輸出管理案は公開済みの技術を対象外としている[9]。ただし、将来のバージョンは公開時の手続き次第で供給条件が変わり得る。関連記事にある中国 AI のコスト優位（20 分の 1）は、供給途絶と来歴のリスクを織り込んで評価すべきである。

3-6. オンプレミス回帰の経済性

【確認済み】シャープは、AI サーバーが世界的な部材不足や遅延で計画どおりに導入できない状況にあるとし、調達力のある鴻海との連携を強みに挙げる[51]。同社は国内 AI サーバー市場が 2025 年度の約 9000 億円から 2035 年度に約 7 兆円へ拡大すると予想し、需要の要因にソブリン AI、低遅延、都市部の電力制約を挙げた[52]。富士通は、MONAKA Server が空冷で周囲温度 40 度まで運用でき、冷却電力を最大 80%削減できるとしている（メーカー公称）[28]。

【分析】オンプレミスは、推論需要が恒常的に大きく、機密度が高い領域では投資を回収しやすい。一方、GPU の調達リードタイム、電力・冷却、運用人材、モデル更新への追随コストが重く、学習用途や需要変動の大きい用途ではクラウドが優位である。結論は記事と同じく「オンプレミス＝ソブリン」ではなく、機密度・継続性・規模で振り分けるハイブリッドである。

4. 知財・無形資産の観点からの示唆

4-1. 営業秘密を外部 AI で処理するリスク

【確認済み】経済産業省は 2025 年 3 月 31 日に営業秘密管理指針を改訂し、生成 AI の利活用を想定した記載を加えた[53,54]。改訂で修正された注記は、秘密管理された情報を生成 AI に利用し、その情報が AI 生成物として出力されても、それだけで秘密管理性は否定されないとの考え方を示す[55]。一方、経

団連タイムスが報じた改訂指針の解説では、生成 AI 提供事業者に情報が提供される場合には秘密管理性が否定される場合もあり得るとされている[56]。

【確認済み】経済産業省は 2025 年 2 月 18 日、「AI の利用・開発に関する契約チェックリスト」を公表した。保護すべきデータが予期せぬ目的に利用されたり第三者に提供されたりする懸念を踏まえ、ユーザーがアウトプットの権利を取得するか等の確認項目を整理している[57,58]。

【分析】提供者側のデータ保持が利用条件となる場合（3-2）、設計図面・製造ノウハウ・契約書を入力することは「第三者への提供」と評価され、秘密管理性の主張が弱まるおそれがある。NEC の cotomi Gateway のようなマスキング層、機密コンピューティング（MONAKA の Arm CCA、AWS の Nitro Enclaves）、国内運用型クラウドは、この法的リスクを技術的に下げる手段と位置づけられる。NEC と Acompany は、cotomi を機密コンピューティング環境で推論実行する技術実証にも成功している[59]。

4-2. 暗黙知のオントロジー化（日立型）の知財的意味

【分析】熟練者の暗黙知をオントロジー（知識グラフ）として形式知化すると、三つの効果が同時に生じる。

- 営業秘密として「特定・管理」しやすくなる。
- 人の退職とともに失われていたノウハウを、企業の資産として固定できる。
- 複製・持ち出しが容易な形に集約されるため、流出したときの損害が大きくなる。

オープン＆クローズ戦略では、オントロジーの「スキーマ（概念体系）」は業界標準化や協調領域として開示を検討し得る。一方、「インスタンス（具体的な判断基準・閾値・故障パターン）」はクローズとし、アクセス権限・ログ・持ち出し制限を徹底するのが基本線である。特許化できる処理手法と、営業秘密として秘匿する知識内容を切り分ける判断も要る。

ベンダーの常駐支援（日立の「Physical AI FDE Team」等）を受ける場合は、抽出された知識の帰属、他の顧客への横展開の禁止、汎用化した部分の扱いを契約で定めておく。定めがなければ、自社の暗黙知がベンダーのバックグラウンド IP に吸収されるおそれがある。

4-3. 派生成果物の権利帰属と出口戦略

【分析】ファインチューニング済みの重み、自社データで構築した知識グラフ、RAG のインデックス、評価データセットについて、①所有権または排他的利用権、②契約終了時の引き渡し形式、③ベースモデルのライセンスが派生物の移転を許すか、の三点を確認すべきである。ベースモデルが他社のライセンスに依存する場合、重みを受け取っても他の基盤へ持ち出せない可能性がある。知識グラフは

RDF／OWL 等の標準形式で書き出せるかが、ロックイン回避の鍵になる。IBM が Sovereign Core の機能としてポータビリティとベンダーロックインの回避を掲げている点[33]も、出口設計がソブリン AI の評価軸になりつつあることを示している。

4-4. 特許動向

【未確認】機密コンピューティング、データファブリック、ソブリンクラウド管理を主題とする特許庁の技術動向調査や WIPO のランドスケープは、今回の調査では見つからなかった。

【分析】基盤技術（TEE、アテステーション等）は、Intel・AMD・Arm・クラウド大手が押さえている可能性が高い。日本企業が権利化を狙うなら、業種固有のデータ統制ワークフロー、監査証跡の自動生成、オントロジーの構築手法など、適用層での差別化が現実的である。具体的な出願動向は、特許データベースで母集団を抽出して確認することが次のステップとなる。

4-5. 知財部門・経営層の実務対応

【推奨】次の五点に、今すぐ着手することを勧める。

1. **データ分類の再設計：**営業秘密・限定提供データ・個人情報・一般情報の区分ごとに、外部 AI への入力可否と、許容する処理環境（国内運用／機密コンピューティング／オンプレミス）を紐づける。
2. **契約条項の標準化：**学習利用の禁止、保持期間、削除と削除証明、再委託先、準拠法・管轄、政府要請時の通知、派生成果物の帰属と引き渡し形式を標準条項にする。提供条件の変更時の通知と解約権も入れる。
3. **マルチベンダーとフォールバックの設計：**Anthropic の約 3 週間の停止を前提事象とし、主力モデルが止まった場合の代替（国産 LLM、オープンウエイトのオンプレミス版）を事前に検証しておく。人工知能基本計画の「複数モデル統御」とも整合する。
4. **監査ログと証跡：**誰が、どのデータを、どのモデルに入力したかを記録する。基幹インフラ事業者でなくても、取引先として「誰がアクセスし、誰が運用したか」の証明を求められる場面が増える。
5. **暗黙知資産化のガバナンス：**オントロジー化プロジェクトの開始時点で、営業秘密の指定、アクセス権限、ベンダーとの帰属条項を決めておく。

5. 今後の展望

- **【分析】ベンダーの勝ち筋：**記事の結論は妥当である。より具体的には、「切り替え可能性」と「証明可能性」を提供できる事業者が優位になる。NEC の cotomi Gateway（マスキングと振り分け）、IBM Sovereign Core（証跡の自動化）、NRI 型の Alloy 運営がその典型である。
- **【分析】ハードウエア勢の時間軸：**富士通 MONAKA Server とシャープの実機納入は 2027 年度以降、Noetra の計算基盤の稼働は 2028 年 6 月である。2026〜27 年の企業の意思決定には直接は間に合わない。価格、供給量、Arm 向け推論ソフトウエアの成熟度が普及の鍵になる。
- **【分析】ユーザー企業の現実的なアプローチ：**①機密度で業務を三層に分け、最上位だけを国内運用・機密コンピューティング環境に置く。②最先端モデルは中位層でゲートウエイ経由で使う。③停止時の代替モデルを用意する。④派生成果物の出口を契約で確保する。
- **【未確認】**連載第 4 回「正解なきデジタル主権論への『現実解』、日本企業へ 5 つの提言」は、記事中で 2026 年 11 月 6 日公開予定とされている[1]。提言の内容は本書では確認していない。

6. 留保事項

- 中国の輸出管理は意見募集段階の案であり、最終内容は変わり得る。API・SaaS 経由の海外提供の扱いは、本書では原文で確認していない。
- サイバー対処能力強化法のうち通信情報の利用に関する規定の具体的な施行日は、本書作成時点で確認していない。
- 「5 年で 1 兆円」は報道された政府方針であり、確定した予算ではない。
- MONAKA の性能・省電力の数値はメーカー公称値であり、第三者による検証はない。
- AWS の Nitro Enclaves・専有ローカルゾーン、Microsoft のソブリンクラウドについて、日本での提供条件は確認していない。
- 営業秘密管理指針の該当箇所は、経済産業省のパブリックコメント回答資料と経団連タイムスの記事で確認した。改訂指針の本文は、本書作成時に直接参照していない。
- Anthropic のデータ保持方針は 2026 年 9 月以降に段階的に変更されている。利用時点の条件を確認する必要がある。
- 法的評価は一般論であり、個別案件では弁護士の確認を要する。

参考文献

※URL は 2026 年 11 月 9 日に閲覧または検索結果で所在を確認した。「URL 未再確認」と付したものは、本書作成時に本文を直接参照できなかった文献である。

[1] 中島募「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（連載「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）, 2026 年 11 月 5 日. https://xtech.nikkei.com/atcl/nxt/column/18/03795/102700004/（有料会員限定記事。本書はユーザー提供の PDF で内容を確認）

[2] nippon.com「AI が変える日本の安全保障：パランティア活用と同時に、独自システム開発を―自民党の平将明氏に聞く」（掲載日は未確認）. https://www.nippon.com/ja/in-depth/d01261/

[3] The Free Press Journal, “Anthropic redeploys Claude Fable 5, Mythos 5 after US lifts export curbs,” 2026 年 7 月. https://www.freepressjournal.in/tech/anthropic-redeploys-claude-fable-5-mythos-5-after-us-lifts-export-curbs

[4] Anthropic, Claude Fable 5／Mythos 5 へのアクセス停止に関する声明, 2026 年 6 月 12 日. https://www.anthropic.com/news/fable-mythos-access（URL 未再確認（本書作成時に本文を直接参照できず））

[5] Anthropic, “Redeploying Claude Fable 5,” 2026 年 6 月 30 日. https://www.anthropic.com/news/redeploying-fable-5（URL 未再確認（表題・日付は文献[6]等の報道で確認））

[6] The Next Web, “US lifts export controls on Anthropic’s Fable 5, clearing the model’s return,” 2026 年 6 月 30 日. https://thenextweb.com/news/anthropic-fable-5-export-controls-lifted

[7] Cointelegraph, “Anthropic to bring back Fable 5 as US lifts export controls,” 2026 年 7 月 1 日. https://cointelegraph.com/news/anthropic-reactivates-newest-ai-models-after-us-govt-lifts-restrictions

[8] 新華網「两部门就修订中国禁止出口限制出口技术目录公开征求意见」（商務部・科学技術部公告 2026 年第 48 号）, 2026 年 10 月 16 日. https://www.news.cn/20261016/c15d168f570a48838178ca74e12ca9e7/c.html

[9] 安全内参「商务部 科技部公告 2026 年第 48 号」（公告全文の転載）, 2026 年 10 月 16 日. https://www.secrss.com/articles/94759

[10] 「デジタル・ガバナンス／サイバーセキュリティニュース No.10　2026 年 10 月 1 日施行 サイバー対処能力強化法」（法律事務所ニュースレター、miyake.gr.jp 掲載 PDF）, 2026 年 8 月. https://www.miyake.gr.jp/wp-content/uploads/2026/08/デジタル・ガバナンス_サイバーセキュリティニュース_No10_サイバー対処能力強化法.pdf

[11] @IT「政府が『攻撃元サーバ』に踏み込む 10 月始動『能動的サイバー防御』で何が変わる?」, 2026 年 10 月 5 日. https://atmarkit.itmedia.co.jp/ait/articles/2610/03/news001.html

[12] 契約ウォッチ, サイバー対処能力強化法の解説記事（公布日・施行日）, 2026 年. https://keiyaku-watch.jp/media/hourei/2026-cyber-response-capability/

[13] トレンドマイクロ「『能動的サイバー防御』で組織は何に備えるべきか～2026 年 10 月 1 日施行～」, 2026 年 8 月 14 日. https://www.trendmicro.com/ja_jp/jp-security/26/h/securitytrend-20260814-01.html

[14] 電波新聞デジタル「ノエトラ、国産 AI 開発を本格化 44 社が出資、GPU2 万 7500 基 30 年度に実世界対応へ」, 2026 年 7 月 17 日. https://dempa-digital.com/?p=720634

[15] Real Sound テック「NVIDIA と Noetra、国家規模の『AI ファクトリー』構築へ Rubin GPU を 2 万 7500 基超導入」, 2026 年 7 月. https://realsound.jp/tech/2026/07/post-2463096.html

[16] ビジネス+IT「【日本総力戦】国産 AI 開発企業『Noetra』が NVIDIA と大規模 AI 計算基盤構築へ」, 2026 年 7 月 16 日. https://www.sbbit.jp/article/cont1/186136

[17] 時事通信（nippon.com 転載）, “Japan Eyes 1-T.-Yen Aid for Domestic AI Development,” 2025 年 12 月 21 日. https://www.nippon.com/en/news/yjj2025122100305

[18] 共同通信（秋田魁新報電子版）「国産 AI、政府が 1 兆円支援 ソフトバンクなど新会社」, 2025 年 12 月 21 日. https://www.sakigake.jp/news/article/20251221CO0065/

[19] ビジネス+IT「富士通が世界トップレベルの AI 推論性能の次世代 CPU『FUJITSU-MONAKA』発売」, 2026 年 9 月 14 日. https://www.sbbit.jp/article/st/186958

[20] IT Leaders, 富士通「FUJITSU-MONAKA」「Fujitsu MONAKA Server」販売開始に関する記事, 2026 年 9 月. https://it.impress.co.jp/articles/-/29791

[21] MONOist「目標は 2030 年度に売上高 2500 億円 シャープが日本国内向けに AI サーバの受注を開始」, 2026 年 9 月 16 日. https://monoist.itmedia.co.jp/mn/articles/2609/16/news029.html

[22] EE Times Japan「シャープが国内向けに AI サーバ展開 NVIDIA 製 GPU 搭載」, 2026 年 9 月 16 日. https://eetimes.itmedia.co.jp/ee/spv/2609/16/news091.html

[23] EnterpriseZine「レノボが『Lenovo AI Express』を発表 AI インフラの本番導入を最短 15 営業日に短縮へ」, 2026 年 10 月. https://enterprisezine.jp/news/detail/25290

[24] Microsoft, “Announcing comprehensive sovereign solutions empowering European organizations,” 2025 年 6 月 16 日. https://blogs.microsoft.com/blog/2025/06/16/announcing-comprehensive-sovereign-solutions-empowering-european-organizations/

[25] NEC「NEC 開発の AI コア技術『cotomi』」（製品ページ）. https://jpn.nec.com/LLM/cotomi.html

[26] クラウド Watch「富士通、プライベート環境で使用可能な企業向け大規模言語モデル『Takane』を提供」, 2024 年 9 月 30 日. https://cloud.watch.impress.co.jp/docs/news/1627569.html

[27] DX Magazine, 富士通「FUJITSU-MONAKA」「Fujitsu MONAKA Server」販売開始に関する記事, 2026 年 9 月. https://dxmagazine.jp/news/2651ko13/

[28] DX Magazine「AI の電力問題を『半分』に? 富士通が国産 CPU を発表、何が変わる」, 2026 年 9 月. https://dxmagazine.jp/?p=222381

[29] NEC「NEC、機密情報を保護しながら AI のトークンコスト最適化を実現する『cotomi Gateway』を提供開始」, 2026 年 11 月 5 日. https://jpn.nec.com/press/202611/20261105_01.html

[30] クラウド Watch「NEC、AI モデルの自動選定によりトークンコストを最適化する『cotomi Gateway』」, 2026 年 11 月 5 日. https://cloud.watch.impress.co.jp/docs/news/2153948.html

[31] TelecomTV, “AWS activates sovereign cloud in Europe,” 2026 年 1 月 15 日. https://www.telecomtv.com/content/digital-platforms-services/aws-activates-sovereign-cloud-in-europe-54659/amp/

[32] IBM Newsroom, “Think 2026: IBM Makes Digital Sovereignty Operational with General Availability of IBM Sovereign Core,” 2026 年 5 月 5 日. https://newsroom.ibm.com/campaign?item=2756

[33] 同上プレスリリース全文（PR Newswire 配信、bolsamania.com 転載）, 2026 年 5 月 5 日. https://www.bolsamania.com/nota-de-prensa/mercados/think-2026-ibm-makes-digital-sovereignty-operational-with-general-availability-of-ibm-sovereign-core--22413167.html

[34] 日立製作所「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」, 2026 年 9 月 3 日. https://www.hitachi.com/ja-jp/press/articles/2026/09/0903d/

[35] MONOist「日立が HMAX の新ソリューション群を発表 データセンター向け事業などを展開」, 2026 年 9 月 7 日. https://monoist.itmedia.co.jp/mn/articles/2609/07/news035_2.html

[36] Amazon, “AWS Launches AWS European Sovereign Cloud and Announces Expansion Across Europe,” 2026 年 1 月 15 日. https://press.aboutamazon.com/aws/2026/1/aws-launches-aws-european-sovereign-cloud-and-announces-expansion-across-europe

[37] Intelligent CIO Europe, “AWS launches European sovereign cloud, expands footprint across EU,” 2026 年 1 月 15 日. https://www.intelligentcio.com/eu/2026/01/15/aws-launches-european-sovereign-cloud-expands-footprint-across-eu/

[38] 日本オラクル「『Oracle Alloy』が野村総合研究所のデータセンターで稼働開始」, 2024 年 4 月 16 日. https://www.oracle.com/jp/news/announcement/oracle-alloy-goes-live-in-nomura-research-institute-data-center-2024-04-16/

[39] 日本オラクル, 野村総合研究所の大阪データセンターでの「Oracle Alloy」稼働と AI 実行基盤サービスに関するプレスリリース, 2025 年 2 月 13 日. https://www.oracle.com/jp/news/announcement/oracle-helps-nomura-research-institute-2025-02-13/

[40] Sénat, Commission d’enquête sur la commande publique, compte rendu de l’audition de MM. Anton Carniaux et Pierre Lagarde (Microsoft France), 2025 年 6 月 10 日. https://senat.fr/compte-rendu-commissions/20250609/ce_commande_publique.html

[41] heise online, “Not sovereign: Microsoft cannot guarantee the security of EU data,” 2025 年. https://heise.de/-10494789

[42] PYMNTS, “Microsoft Balks at Anthropic’s Claude Fable 5 Data Retention Policy,” 2026 年 6 月. https://www.pymnts.com/?p=3833997

[43] CX Today, “Anthropic Drops Data Retention Requirement for Mythos and Fable 5.1 After Enterprise Pushback,” 2026 年 9 月 2 日. https://www.cxtoday.com/security-privacy-compliance/anthropic-zero-data-retention-enterprise-ai/

[44] implicator.ai, Anthropic による監視データの顧客クラウド内保持（Enterprise Frontier Safeguards）に関する記事, 2026 年 9 月 2 日. https://www.implicator.ai/anthropic-moves-claude-monitoring-data-into-customer-clouds-after-enterprise-pushback.md

[45] Gartner, “Gartner Says Worldwide Sovereign Cloud IaaS Spending Will Total $80 Billion in 2026,” 2026 年 2 月 9 日. https://www.gartner.com/en/newsroom/press-releases/2026-02-09-gartner-says-worldwide-sovereign-cloud-iaas-spending-will-total-us-dollars-80-billion-in-2026

[46] ITdaily, “Global sovereign cloud market grows, Europe on track for second place,” 2026 年 2 月. https://itdaily.com/news/cloud/global-sovereign-cloud-market-grows

[47] DIGIT, “Sovereign Cloud Infrastructure Spend to Reach $80BN in 2026,” 2026 年 2 月. https://www.digit.fyi/sovereign-cloud-infrastructure-spend-to-reach-80bn-in-2026/

[48] Computerwoche, „Ausgaben für Sovereign-Cloud-Angebote schießen durch die Decke“, 2026 年 2 月. https://www.computerwoche.de/article/4129404/ausgaben-fur-sovereign-cloud-angebote-schiesen-durch-die-decke.html

[49] CSIS, “The EU AI Continent Action Plan,” 2025 年 4 月. https://www.csis.org/analysis/eu-ai-continent-action-plan

[50] 内閣府「人工知能基本計画～日本ＡＸ、より強く、より豊かに～」（令和 8 年 7 月 14 日閣議決定）. https://www8.cao.go.jp/cstp/ai/ai_plan/aiplan_20260714.pdf

[51] Impress Watch, シャープの AI サーバー事業参入に関する記事, 2026 年 9 月. https://www.watch.impress.co.jp/docs/news/2141109.html

[52] 電波新聞デジタル「シャープ、AI サーバー事業参入 30 年度で売上高 2500 億円へ」, 2026 年 9 月 15 日. https://dempa-digital.com/?p=725522

[53] 経済産業省「営業秘密管理指針」（2025 年 3 月 31 日改訂）. https://www.meti.go.jp/policy/economy/chizai/chiteki/guideline/r7ts.pdf（URL 未再確認（本書作成時に本文を直接参照できず））

[54] 経済産業省 産業構造審議会 不正競争防止小委員会 配布資料（生成 AI の利活用を想定した営業秘密管理指針への追記の報告を含む）, 2025 年. https://www.meti.go.jp/shingikai/sankoshin/chiteki_zaisan/fusei_kyoso/pdf/028_04_00.pdf

[55] 経済産業省「『営業秘密管理指針（改訂案）』に対する主な御意見及びそれに対する考え方」（資料 3-1）, 2025 年 3 月. https://www.meti.go.jp/shingikai/sankoshin/chiteki_zaisan/fusei_kyoso/pdf/028_03_01.pdf

[56] 経団連タイムス, 営業秘密管理指針の改訂に関する記事, 2025 年 10 月 23 日. https://www.keidanren.or.jp/journal/times/2025/1023_08.html

[57] IT Leaders, 経済産業省「AI の利用・開発に関する契約チェックリスト」公開に関する記事, 2025 年 2 月. https://it.impress.co.jp/articles/-/27490

[58] @IT「AI サービスの契約時には何を見るべき? 経済産業省が『AI 初心者向け契約チェックリスト』を公開」, 2025 年 2 月 20 日. https://atmarkit.itmedia.co.jp/ait/articles/2502/20/news093.html

[59] EnterpriseZine「NEC の国産 LLM『cotomi』、Acompany との実証で秘匿環境下での推論実行に成功」（掲載日は未確認）. https://enterprisezine.jp/news/detail/24555