



ソブリンAIの構築

基盤とアーキテクチャに関する技術的考察

David Girard

Director, Product Management

Numaan Huq

Senior Threat Researcher, Forward-
Looking Threat Research

目次

3

はじめに

5

ソブリンAIとは何か（そして何でないか）

8

ソブリンAIを必要とするのは誰か（そしてなぜか）

13

主権のスケール：評価のためのフレームワーク

20

管轄権、所有権、法的支配

23

導入アーキタイプ

26

ソフトウェア基盤とMLOps

28

実践的な提言と結論

1

はじめに

人工知能（AI）への政府投資が拡大するなか、ソブリンAIをめぐる問いはかつてないほど切実なものになっています。ソブリンAIとは正確には何を指すのか。主権はどの程度まで達成できるのか。そして、それを構築するには何が必要なのか。こうした問いは、2026年6月にAnthropicが最新AIモデルへのアクセス停止を余儀なくされた事例のような出来事を受けて、いっそう緊急性を増しています。この停止は、米国人以外の者（同社の米国オフィスに勤務する外国籍人材を含む）による利用を禁じる米国の輸出管理指令を受けたものでした。このような事例は、一国の政策がフロンティアAIシステムの世界的な利用に直接影響を及ぼしうることを浮き彫りにしています。



本リサーチでは、ソブリンAIをその実像どおりに理解するための実践的なフレームワークを提示します。すなわち、ソブリンAIとは到達すべき絶対的な状態ではなく、時間をかけて築き上げていく能力のスペクトラム（連続体）です。あわせて、基盤、インフラストラクチャ、データとモデル、運用、戦略的自律性という5つのレイヤーにわたる技術要件を検討します。

AIが世界を形づくり続けるなか、注目すべきは技術がどこまで進歩するかどうかではありません。相互接続された世界のなかで、各国がどのように自律性を維持しようとするのかについても考える必要があります。

2

ソブリンAIとは何か (そして何でないか)

ソブリンAIは、AIをめぐる法律や政策にとどまるものではありません。世界経済フォーラムによれば、それは自国の領域内でAIがどのように開発され、統治され、展開されるかについて、国家が実質的なコントロールを保持することを意味します¹。つまり、データの保存や処理からモデルの学習や推論に至るまで、AIスタック全体を自ら所有し運用するということです。各国がソブリンAIを追求する目的は、国内経済の強化、国家安全保障の保護、地政学的ショックの緩和、そしてAIシステムに自国の価値観と言語を反映させることにあります。

しかし、この概念はしばしば誤解されています。多くの組織が、国内でホスティングされていれば十分だという考えのもと、データレジデンシー（データが物理的に自国の国境内に置かれていること）を真の主権と混同しています。しかし、外国資本の企業に自国内でデータをホスティングさせても、それだけで主権が確保されるわけではありません。重要なのは、誰がプラットフォームを所有しているか、誰がソフトウェアを支配しているか、そしてどの法域が保存されたデータへのアクセスを強制できるかです。

ソブリンAIは、スペクトラムとして理解するのが最も適切です。今日、スタックの100%を自国で所有している国は存在せず、重要なのはどこに投資するかを意図的に選択することです。完全な主権に最も近いのは米国ですが、その米国でさえ、世界の最先端チップの約90%を製造するTaiwan Semiconductor Manufacturing Company（TSMC）に依存しています²。NvidiaのBlackwellチップですら、TSMCのChip-on-Wafer-on-Substrate（CoWoS）先端パッケージングに依存しています。そして台湾は、チップ製造に必要な極端紫外線（EUV）リソグラフィ装置をオランダのASMLに依存しています。したがってソブリンAIは、絶対の問題ではなく程度の問題です。本当に問うべきは、国や組織がどれだけの主権を、スタックのどのレイヤーで必要とするのかという点です。



見えにくい依存関係も、絶対的な主権の主張を揺るがします。技術人材の国籍、世界中のソースから収集された学習データ、少数の法域への基盤モデル開発の集中などがその例です。ほかにも、オープンソースコンポーネントにおける推移的依存関係や、名目上は国内企業であっても外国の法的影響力が及ぶケースが挙げられます。インフラに巨額を投じる国であっても、現実的な目標は、誰にも達成できない絶対的な主権ではなく、自国の要件を満たすのに十分な戦略的自律性の確保です。

2.1 ソブリンAIの経済的現実

ソブリンAIは戦略的投資であり、その経済性がコミットメントの規模を左右します。どのようなアプローチを取るにせよ、必要な資本は巨額です。Nvidia H100グラフィックスプロセッシングユニット（GPU）を1,000基備えた中規模のソブリンAI構想を考えてみましょう。意味のある学習と推論には十分な規模ですが、パリ近郊にあるフランスのMistralデータセンターの13,800基と比べればささやかなものです³。その財務プロファイルはおおよそ次のようになります。

資本的支出（CapEx）： GPU調達（2,500万～3,000万米ドル）、データセンターの新設または改修（適切な電力と冷却を備えたTier III施設で5,000万～1億米ドル）、ネットワークインフラ（1,000万～1,500万米ドル）、セキュリティシステム（500万～1,000万米ドル）。CapEx合計：9,000万～1億5,500万米ドル。

年間運用支出（OpEx）： 5メガワット（MW）持続の電力消費（年間300万～500万米ドル）、冷却インフラ（100万～200万米ドル）、機械学習（ML）エンジニア、プラットフォームエンジニア、セキュリティスペシャリスト、運用担当を含む25～30名の専門人材の人件費（500万～800万米ドル）、保守およびハードウェア更改（500万～700万米ドル）、ソフトウェアライセンス（200万～300万米ドル）。OpEx合計：年間1,600万～2,500万米ドル。

5年間の総所有コスト： 1億7,000万～2億8,000万米ドル。

これを、ハイパースケーラーから同等のコンピューティング容量を調達した場合と比較してみましょう。稼働率70%を維持した場合、同等のクラウドGPUリソースは現行価格で5年間に約1億2,000万～1億8,000万米ドルかかります。ソブリンアプローチは、稼働率が高く、かつコントロール、セキュリティ、法域からの独立性の価値を織り込めば、十分に採算が取れます。コンプライアンスと地政学的圧力が高まるにつれ、こうした懸念は大きくなっていきます。

経済性は規模が大きいほど改善し、固定費が支配的になる小規模では悪化します。フランスの1,090億ユーロのコミットメントは、国家規模では計算が変わることを示しています。ほとんどの組織にとって、ソブリンAIの根拠となるのはコントロール、レジリエンス、法域の確実性であり、クラウドハイパースケーラーと比較したコスト削減ではありません。規制対象ワークロードと地政学リスクが増大するにつれ、このトレードオフは自社構築に有利に傾きつつあります。

ソブリンAIを必要とするのは誰か (そしてなぜか)

ソブリンAIのニーズは一樣ではありません。そのスペクトラムは、エアギャップ化された軍事級システムを必要とする各国政府から、規模とコストのためにインフラを共有する民間コンソーシアムまで多岐にわたります。どれだけ投資し、何を構築するかは、組織がこのスペクトラムのどこに位置するかによって決まります。

3.1 各国政府：国防、情報機関、公共サービス

政府には最も厳格な主権要件が課されますが、その内容は民生用途と国家安全保障用途とで異なります。軍や情報機関には、外部ネットワークへの接続を一切持たないエアギャップシステムが必要です。たとえばフランス軍事省は2026年1月、Mistral AIと枠組み契約を締結し⁴、防衛エコシステム全体に生成AIモデルを供給することとしました。ホスティングはフランス国内のインフラに限定することが確約されています。この契約は、原子力庁や国立航空宇宙研究局を含む関連公的機関にも適用されます。



民生分野の政府機関の要件はこれとは異なりますが、深刻さでは引けを取りません。患者データを扱う保健省、財務記録を管理する税務当局、学生情報を処理する教育省はいずれも強固なデータ保護を必要とします。ただし、国防用途のようなエアギャップの極端な措置までは通常求められません。デンマークのように、AIにとどまらない広範なデジタル主権を追求する国もあります。同国のデジタル化省は、デジタル主権の取り組みの一環として、Microsoft OfficeとMicrosoft 365をLibreOfficeに置き換えています⁵。

3.2 重要産業：金融、通信、公益、医療

重要インフラの事業者は、規制上の圧力と運用リスクに直面しており、それがソブリンまたはそれに近いAIへと向かわせています。金融取引を扱う銀行、通信インフラを管理する通信事業者、電力網を制御する公益事業者は、外国の主体が自社のAIシステムを妨害することを許容できません。その妨害は、技術的手段によっても法的強制によっても起こりえます。欧州では、Orange、Fastweb、Swisscom、Telefónica、Telenorをはじめとする通信事業者がNvidiaと連携し、ソブリンAIインフラの開発を進めています⁶。

同様の通信事業者主導モデルは東南アジアでも生まれつつあります。インドネシアのIndosat Ooredoo HutchisonとGoToは、Nvidia NeMoプラットフォームを用いてLlama 3 8Bをファインチューニングしたオープンソースのインドネシア語モデル「Sahabat-AI」を構築しました。同モデルは国内の「GPU Merdeka」ソブリンAIクラウドから提供され、同国の2億7,700万人の話者に届けられています⁷。

3.3 コンソーシアムモデル：競合しないナショナルチャンピオン

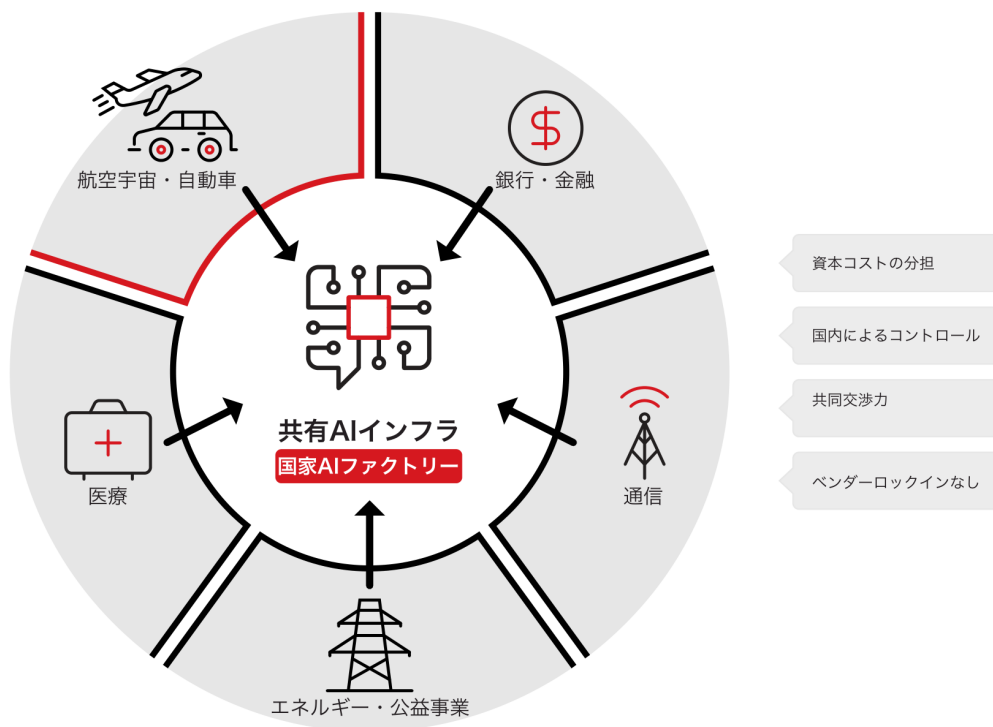


図1. コンソーシアムモデル：競合しない産業同士が共有AIインフラを構築する

競合関係にない国内組織がリソースを出し合い、共有AIインフラを構築するモデルが台頭しています。スウェーデンでは、異なるセクターの組織⁸が提携してAIファクトリーを建設しています。参加組織には、航空宇宙・防衛企業、国内最大手の銀行、主要通信事業者が含まれます。互いに競合しない異業種の大手企業が、共有のソブリンインフラで協力する形です。セクターとの相性には差があり、このモデルが最もうまく機能するのは、参加者が規制圧力と同程度のデータ機密性を共有している場合（金融、通信、防衛、医療）であり、事業のあり方が大きく異なるセクターをまたぐ場合ではありません。

このモデルの利点は明確です。資本コストの分担、規模の経済による運用負荷の低減、国内によるコントロール、そしてベンダーに対する共同交渉力です。コンソーシアムはハードウェアを共同で調達し、独自のソフトウェアスタックを展開し、何も国外に出さないことを保証します。

3.4 リソースに制約のある主体のためのソブリンAI

ここまで述べてきた取り組みは、豊かな国にしか手の届かない規模で行われていますが、同じ論理はより小さな国や中規模の組織にも当てはまります。そうした主体にとっての問いは、主権が望ましいかどうかではなく、予算の範囲内でどの程度の主権を達成できるかです。

主権は二者択一ではなく、小規模なプレイヤーは段階的なアプローチを採るべきです。

- **ティア1：データレジデンシー（500万～2,000万米ドル）**： 外部モデルを利用しつつ国内ホスティングに依拠する段階です。モデル学習インフラを構築するコストをかけずに、基本的なデータ主権を確保できます。
- **ティア2：国内インフラ（2,000万～1億米ドル）**： 自社保有インフラと、ファインチューニングしたオープンソースモデルを組み合わせる段階です。コンピューティングとモデルのレイヤーに対する実質的なコントロールが可能になります。
- **ティア3：地域協力（1億～5億米ドル）**： コンソーシアム保有のインフラを同盟国間で共有する段階です。集団的な主権を維持しながら規模の経済を実現できます。
- **ティア4：完全なソブリンスタック（5億米ドル以上）**： 5つのレイヤーすべて（次章「主権のスケール」参照）にわたる完全な国内能力を実現する段階です。現実的に可能なのは主要経済大国に限られます。

中規模国家にとって最も有望な道は地域協力です。ベネルクス諸国であれば、1か国あたり約3分の1のコストでインフラを共有できます。北欧諸国は、スウェーデンのコンソーシアムモデルを近隣国に拡張できるでしょう。バルト三国は、エストニアのデジタルガバナンスの知見を土台に、地域全体で共有するAIインフラを構築できます。

3.5 民間のAIファクトリーと政府のソブリンクラウド

ほぼ同じインフラを指す2つのラベルが並行して使われています。Nvidiaの言う「AIファクトリー」（主に商用顧客向けの専用GPUキャパシティ）と、各国政府の言う「ソブリンクラウド」（公共部門のワークロード向けに構築されたキャパシティ）です。技術的な構成要素は重なりますが、優先事項

が異なります。民間のAIファクトリーは、商業的柔軟性、マルチテナンシー、収益化までの時間を優先します。政府のソブリンクラウドは、セキュリティ格付け、市民データの保護、調達の説明責任を優先します。両者は、サウジアラビアのHUMAIN⁹のように商用推論と政府ワークロードの両方を担う官民混合の展開において収斂します。ほとんどの意思決定者にとって重要なのは、ラベルではなく、設計を方向づける優先事項のほうです。

主権のスケール：評価のための フレームワーク

ソブリンAIフレームワーク

それぞれに意図的な投資が求められる5つのレイヤー



1つのレイヤーの欠落だけでも、システム全体の主権が損なわれかねません。
主権はスペクトラムです。どこに投資するかを選択しましょう。

図2. ソブリンAIフレームワーク：基盤ハードウェアから戦略的自律性まで、組織が評価すべき5つのレイヤー

主権を二者択一の状態として扱うのではなく、組織は5つのレイヤーにわたって自らの立ち位置を評価すべきです。各レイヤーには固有の技術的要求があり、1つのレイヤーの欠落だけでも、スタック全体の主権の主張が損なわれかねません。

4.1 レイヤー1：基盤（ハードウェアとサプライチェーン）

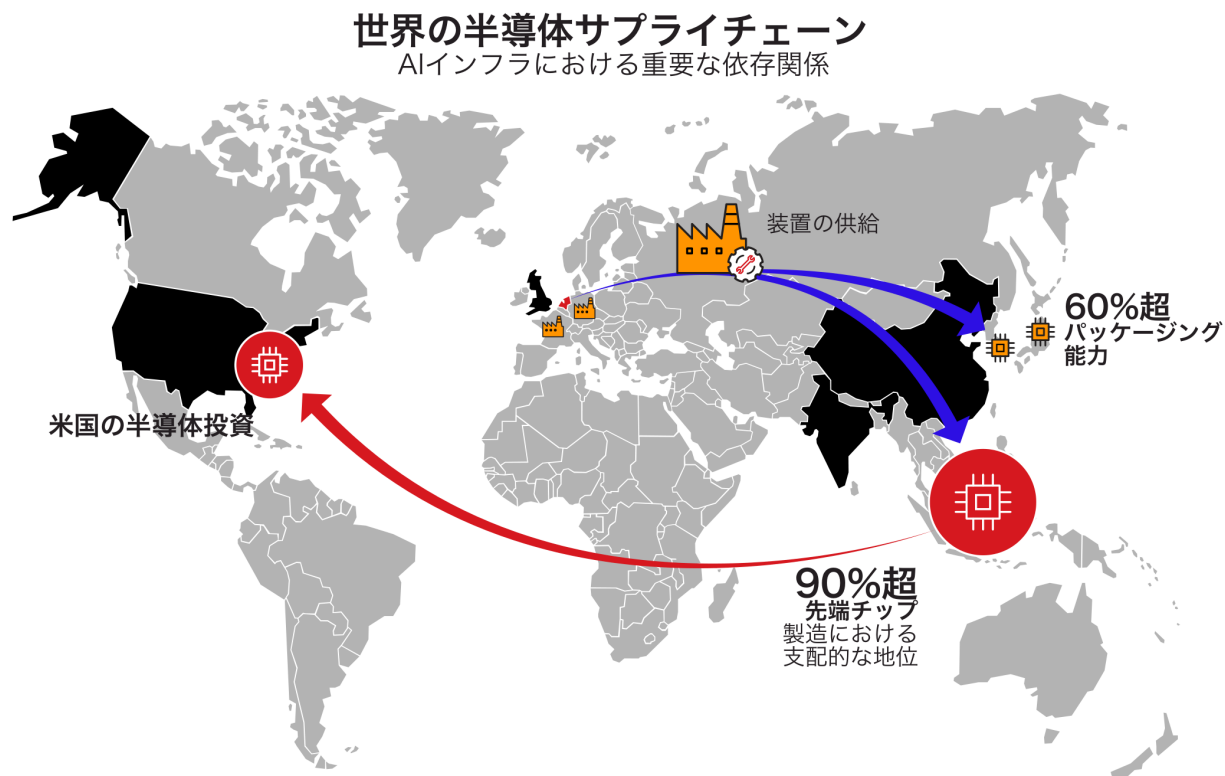


図3. 世界の半導体サプライチェーン：先端チップの製造、パッケージング、リソグラフィ装置が少数の地域に集中している

基盤レイヤーとは、物理的なハードウェア（GPU、サーバ、ネットワーク機器）と、その背後にあるサプライチェーンです。TSMCのCoWoS先端パッケージングは2026年分まで完売しており¹⁰、その6割超をNvidiaが押さえているため¹¹、GPUの供給はあらゆるソブリンAIプログラムのボトルネックとなっています。

米台間の二国間協定は半導体製造の分散を目指しており¹²、米国は2030年までに世界の最先端ロジックチップの20%を自国で生産する目標を掲げ¹³、TSMCはアリゾナ州の拠点を最大11のファブへと拡張しようとしています¹⁴。この目標が予定どおり達成されるかは不透明です。同様の分散化の取り組みは、これまでも遅延してきました。地理的な集中が実質的に変わらない限り、どれほど潤沢な資金を持つソブリンAIプログラムであっても、少数のサプライヤーに依存し続けることになります。台湾海峡でひとたび混乱が起これば、世界中のAI開発が後退するでしょう。

このレイヤーにおける実践的な推奨事項は次のとおりです。

- 複数のハードウェアベンダーとの関係を維持し、単一障害点のリスクを低減する。

- 信頼できるディストリビューターとの安全な調達チャネルを確立し、完全な管理履歴（チェーン・オブ・カストディ）文書を整備する。
- 数か月に及ぶ供給途絶を乗り切れるよう、予備部品とコンポーネントの備蓄を計画する。
- 完全なベンダーロックインを避けるため、Nvidiaに加えてセカンダリGPUベンダー（AMD、Intel）を検討する。
- 初期展開の段階から、ファームウェア検証とメジャーアップデートを要件とする。

4.2 レイヤー2：インフラストラクチャ（データセンターとネットワーク）

インフラの主権には、適切な物理セキュリティ、電力のレジリエンス、ネットワーク分離を備えた国内データセンターが必要です。Nvidiaは、VivaTech期間中のGTC Parisで、フランス、イタリア、スペイン、英国にわたって3,000エクサフロップス超のBlackwellシステムを展開すると発表しました¹⁵。ドイツでは、Deutsche Telekomが運用する10,000基のNvidia Blackwell GPUを擁する世界初の産業向けAIクラウドが立ち上がっています¹⁶。Nvidiaは欧州全体で20のAIファクトリーを設立中で、そのうち5つはギガファクトリー規模です¹⁷。

Hewlett Packard Enterprise（HPE）とNvidiaのAI Factory Labは、2026年ごろにフランスのグルノーブルで開設される計画ですが、この規模の建設は実際には遅延が常態化しています¹⁸。同ラボでは、顧客がソブリンな欧州連合（EU）インフラ上でAIワークロードをテスト・検証できるようになり、データ主権と規制遵守のためのオンプレミス環境も提供されます。

同様のAIファクトリー展開は欧州以外にも広がっています。NvidiaとサウジアラビアのHUMAINは2025年5月、5年間で数十万基のBlackwell GPUを擁する最大500MWのAIファクトリー群を建設することを確約し、まずは18,000基のGB300スーパーコンピュータから着手します¹⁹。アラブ首長国連邦（UAE）の「Stargate UAE」パートナーシップには、G42、OpenAI、Oracle、Nvidia、SoftBank、Ciscoが参画しています。計画中の5ギガワット（GW）規模の米国・UAE AIキャンパス内に1GWのアブダビクラスターを据えるもので、最初の200MWは2026年の稼働開始が見込まれています²⁰。10億米ドル超の公的資金に支えられたインドのIndiaAI Missionでは、YottaがShakti Cloud向けに20,000基超のNvidia Blackwell Ultra GPUを展開し、Larsen & ToubroがGW規模のAIファクトリーインフラを建設しています²¹。マレーシアのYTL Powerは、ジョホール州クライに同国初のNvidia Grace Blackwell施設を開設し、国内資本の大規模言語モデル（LLM）「Intelek Luhur Malaysia Untukmu（ILMU）」と組み合わせています²²。

インフラ面の主な考慮事項は次のとおりです。

- データセンター施設の物理的な立地と管轄権上のコントロール
- 適切なレジリエンスティアを備えた電力・冷却インフラ
- 同一施設内で機密ワークロードと非機密ワークロードを分離するセキュアゾーニング
- プライベートDNS、厳格なエグレス制御、データ分類に基づくセグメンテーションを備えたネットワークアーキテクチャ
- レイテンシに敏感なアプリケーションのための地域推論ノードと管理されたピアリング
- エアギャップ環境向けのオフライン更新メカニズムと管理されたパッチパイプライン

4.3 レイヤー3：データとモデル

データとモデルのレイヤーは、多くの主権確保の取り組みが集中する領域であると同時に、最も高くつく過ちが起こりがちな領域でもあります。Mistral AIの「Mistral Compute」はこのアプローチをよく示しています。フランスのエソンヌ県にある40MWのデータセンターに18,000基のNvidia Grace Blackwellシステムを設置し、インフラ全体をフランス領内でホスティングするというものです²³。EU一般データ保護規則（GDPR）の義務を負う銀行、医療機関、政府ユーザにとって、これは域外からのデータアクセス要求へのエクスポージャーを実質的に低減します。ただし、低減は排除ではありません。外国の法的影響力からの完全な免除には、運用主体、サポートチェーン、鍵管理を米国の管轄権が及ばない形に構成することも必要です。

組織は、オープンソースモデルを使うか、商用モデルをライセンスするか、モデルをゼロから学習するかを決める必要があります。いずれの選択にも主権上の含意があります。オープンソースモデル（MetaのLlamaファミリーやMistralのものなど）はより高いコントロールをもたらしますが、ファインチューニングと運用にはかなりの専門知識が必要です。商用モデルは性能面で優れる場合がありますが、外国の管轄権に服する外部ベンダーへの依存を生みます。

マルチモデル戦略は、単一ベンダーのリスクを低減します。あるプロバイダーが買収されたり、制裁を受けたり、契約条件を変更したりしても、複数のモデルを運用している組織であれば、アプリケーションを作り直すことなく移行できます。これに対しては、マルチモデルはマルチ管轄権を意味し、主権を損なうという反論が定番です。しかし、必ずしもそうはなりません。ソプリンプログラムは、国内で統治される異なるベンダーの2つのオープンウェイトモデルを運用することも、国産基盤モデルとファインチューニング済みオープンソースの代替モデルを同じソプリンインフラ上で組み合わせ

ることもできます。目標は、単一障害点（技術的、商業的、管轄権的のいずれであれ）からの独立であって、サプライヤーの国籍の多様さではありません。

アジアでは、地域の言語や文化への適合を目的として、国内で統治される基盤モデルへの投資が並行して進んでいます。インド政府は2025年4月、IndiaAI Missionを通じてSarvam AIを選定し、インド国内で構築・展開・最適化されるソブリンLLMファミリー（Sarvam-Large、-Small、-Edge）の開発を委ねました²⁴。シンガポールは国立研究財団（NRF）を通じて7,000万シンガポールドルを拠出し、東南アジアの言語と言語的文脈で学習されたオープンソースモデル「Southeast Asian Languages in One Network（SEA-LION）」を開発しています²⁵。この取り組みは、情報通信メディア開発庁（IMDA）、AI Singapore、A*STARが実施しています。韓国のNAVER Cloudは、GPT-3の6,500倍の規模を持つ韓国語コーパスでHyperCLOVA Xを構築しました。20年以上にわたるNAVERのユーザコンテンツを活用し、同国最大の国内AIデータセンターでホスティングされています²⁶。

4.4 レイヤー4：運用

運用面の主権は、AIシステムを日々動かし維持するのが誰かという問題です。実際には、原則よりも規制が、こうした統制への投資を組織に促す主要因となっています。ここには、人材（データサイエンティスト、MLエンジニア、セキュリティスペシャリスト、オペレーター）だけでなく、それらを統括する組織構造も含まれます。人員配置は、技術だけでは解決できない主権上の問題を提起します。

本社が国内にある企業でも、労働力がグローバルに分散していることは珍しくありません。Mistral AIはフランス企業でありながら、人材が世界中に分散しているため、米国、シンガポール、フランスの各拠点で英語を使って事業を運営しています。このことは、インサイダーリスクや、機密性の高いシステムと学習データにアクセスできる人員の国籍をめぐる問題を提起します。

組織面の考慮事項は次のとおりです。

- データ分類に応じた適切なセキュリティクリアランスを持つ、プラットフォームエンジニアリングおよび機械学習運用（MLOps）チーム
- AI脅威検知の訓練を受けたセキュリティオペレーションセンター（SOC）要員
- 職務分掌や特権アクセス管理を含む、要員リスクの統制
- 机上演習で検証されたAI固有のプレイブックを備えたインシデント対応体制

- 重要な能力が特定の個人に依存しないようにするナレッジ移転プログラム

4.5 レイヤー5：戦略的自律性

主権の最高段階は、地政学的な混乱のさなかでも運用を継続し、外部からの支配から独立を保つ能力です²⁷²⁸。これは、予備のコンピューティング容量、全面的なリプラットフォームなしにベンダーを入れ替えられる能力、そしてすべての重要な依存関係について文書化された撤退計画を持つことを意味します。試金石はこうです。買収、制裁、政策変更によって重要な関係が明日終わったとしても、運用を継続できるか。

戦略的自律性には、あらゆるレベルの依存関係を率直に評価することが求められます。カナダが Sovereign AI Compute Strategyの下で行ったCohereへの投資²⁹³⁰は、そのトレードオフをよく示しています。この資金拠出は国内AI能力の構築と位置づけられましたが、関連インフラは米国の管轄権に服する米国企業CoreWeaveとの提携により建設されています³¹。この判断は商業的には合理的かもしれませんが、実質的な運用上の権限をカナダの外に置くことになります。さらに、Cohere自体が米国の大手テクノロジー企業の出資を受けており、投資家が外国の巨大テクノロジー企業から買収提案を受けた場合に何が起こるのかという疑問も残ります。

5

管轄権、所有権、法的支配

データレジデンシーと法的主権

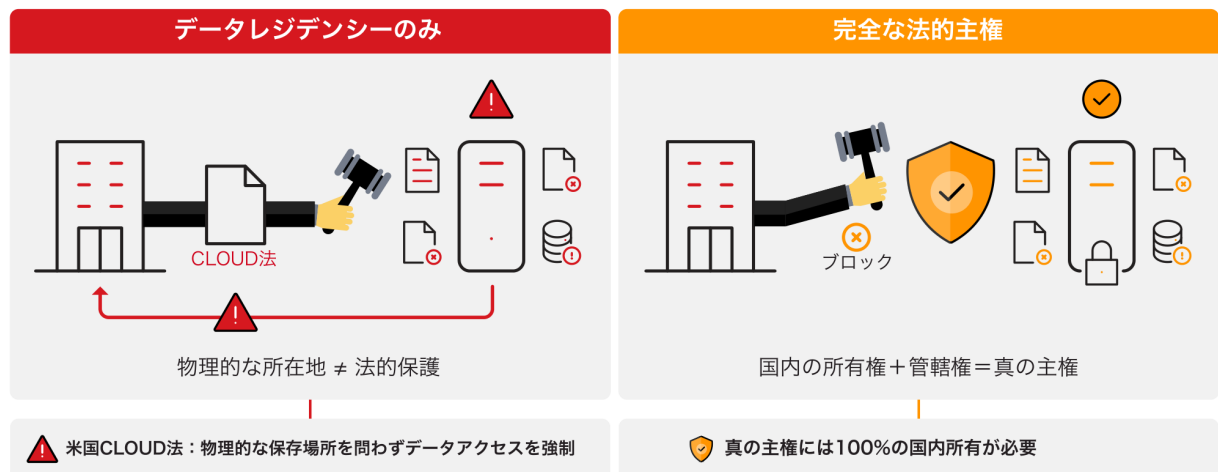


図4. データレジデンシーと法的主権の対比：CLOUD法により、米国当局は物理的な保存場所にかかわらずデータにアクセスできる

データレジデンシーと法的支配の区別は、ソブリンAIをめぐって最も誤解されている論点の1つです。データが物理的に国内にあっても、運用企業の本社が国外にあれば、そのデータは外国の管轄権に服したままになりえます。これを「見せかけのソブリンクラウド」と呼ぶ論者もいます。法的な裏付けを欠いた、主権の外観だけの状態という意味です。実際には、多くの企業は規制当局に迫られて初めてこの区別に向き合います。この問題を顕在化させるのが、以下で説明する法制度です。

米国のCLOUD法（Clarifying Lawful Overseas Use of Data Act）により、米国当局は、データが物理的にどこに保存されていようと、米国企業に対してデータの提出を強制できます³²³³。つまり、ドイツ、フランス、カナダに置かれたAmazon Web Services（AWS）、Azure、Google Cloudのデータセンターも、依然として米国の法的影響下にあるということです。米国政権がMicrosoftに特定の法域でのMicrosoft 365へのアクセス制限を命じた際、同社はこれに従いました³⁴。データレジデンシーは、米国ベンダーに対する外国の法的権限からデータを守ってはくれないのです。

フランスはこの問題に、SecNumCloud認証³⁵で対応しています。同認証は、ソブリンクラウドプロバイダーに対して欧州資本の過半数維持を義務づけるものです（非EU資本の上限は資本および議決権の39%）³⁶。S3NSやOVHcloudなどがこの要件を満たしており³⁷³⁸、S3NSはGoogle Cloud Platform（GCP）のコードをライセンスし³⁹、展開前に独立したセキュリティレビューを実施し、認証されたフランス管理下のインフラを運用しています。米国のハイパースケーラーは、サーバをどこに置こうとも、この資本要件を満たすことができません。フランスのアプローチではさらに、政府

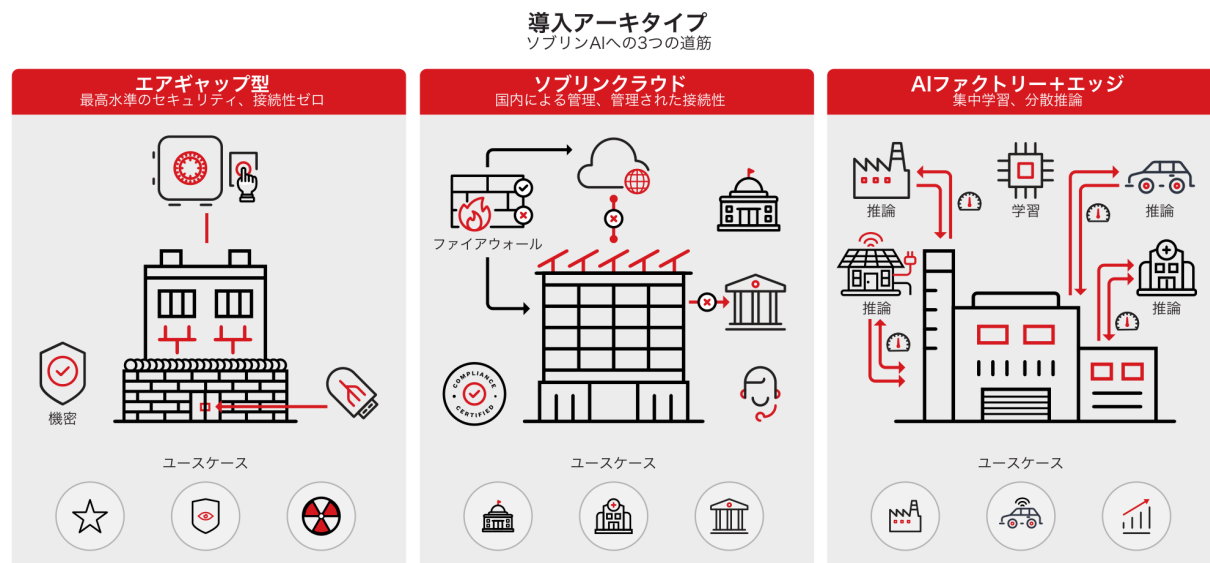
システムへの展開に先立ち、セキュリティレビューのためにソースコードへアクセスできること、そして外国のバックドアが存在しないことの認証が求められます。

契約面の主な考慮事項は次のとおりです。

- ベンダーが外国企業に買収された場合の対応を定める支配権変更（チェンジ・オブ・コントロール）条項
- ベンダーのシステムと業務慣行に対する定期的なセキュリティ評価を可能にする監査権
- 外国の再委託先に対する承認権を付与する再委託先開示要件
- 現地規制に準拠したデータ取り扱いおよび侵害通知の規定
- 関係終了時のデータポータビリティと事業継続を保証する撤退・移行条項

6

導入アーキタイプ



アーキタイプ	セキュリティ	接続性	複雑さ	コスト
エアギャップ型	最高	なし	非常に高い	非常に高い
ソブリンクラウド	高	管理された接続	中	中
AIファクトリー+エッジ	中～高	分散	中	変動

図5. 導入アーキタイプ：セキュリティと接続性のトレードオフが異なる、ソブリンAIへの3つの道筋

組織には複数の導入オプションがあり、それぞれ主権、コスト、運用面のトレードオフが異なります。適切な選択は、データ分類、予算、運用の成熟度によって決まります。

6.1 エアギャップ型ソブリンAI

最も高い保証を提供する選択肢は、完全なネットワーク分離であり、軍や情報機関の機密ワークロードには必須です。エアギャップシステムには、管理されたパッチパイプラインや物理メディアによる搬送を含むオフライン更新メカニズムが必要です。運用負荷は相当なものですが、国家安全保障の用途において、これに匹敵する選択肢は他にありません。

6.2 ソブリンクラウド

ソブリンクラウド型の導入では、現地事業者による国内ホスティングを維持しつつ、更新のために管理された外部接続を残す場合があります。これは企業で最も一般的な導入モデルです。鍵となる要件は、データセンターの所在地だけでなく、運用主体そのものが国内の支配下になければならないという点です。

6.3 AIファクトリーとエッジ推論

AIファクトリーは、AIワークロード向けのローカルプラットフォームスタックを備えた専用GPUインフラです。レイテンシに敏感なアプリケーションでは、エッジ展開によりデータ生成の現場で推論を実行し、機密データをオンサイトに保持したまま、中央で学習したモデルを動かします。

7

ソフトウェア基盤とMLOps

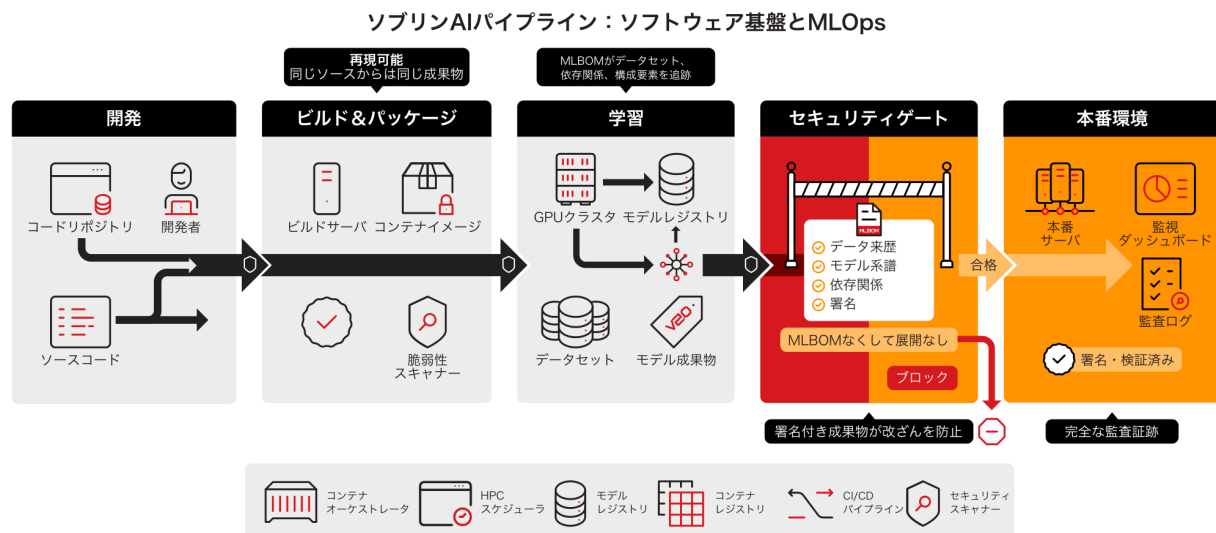


図6. ソブリンAIパイプライン：MLBOMセキュリティゲートを備えた、開発から本番までの流れ

ソブリンAIのソフトウェアスタックは、外国のSaaS（Software as a Service）に依存することなく、セキュアかつ運用効率の高いものでなければなりません。

主要コンポーネントは次のとおりです。

- コンテナ化ワークロード向けのKubernetesや、ハイパフォーマンスコンピューティング（HPC）における学習ジョブ向けのSlurmといったオーケストレーションプラットフォーム
- 完全なバージョン管理とアクセスログを備えたモデルレジストリおよびアーティファクトストア
- 未承認のアーティファクトが本番環境に到達するのを防ぐセキュリティゲートを備えた、継続的インテグレーション／継続的デリバリー（CI/CD）パイプライン
- 脆弱性スキャンと署名検証を備えたプライベートコンテナレジストリ

再現可能ビルド、すなわち任意のアーティファクトをソースから決定論的に再作成できる能力は、基本要件です。機械学習部品表（MLBOM）は、CycloneDX（Open Worldwide Application Security Project、OWASPのプロジェクト）などの標準がサポートする文書形式で⁴⁰、サプライチェーン監査のためにモデルのコンポーネント、データセット、依存関係を構造化して文書化します。CycloneDXは、組織がデータの出所を追跡し、MLBOMの生成をゲートにすることを明確に推奨しています。つまり、MLBOMがなければ本番展開もない、ということです。署名付きアーティファクトと検証済みの来歴（プロベナンス）が、展開パイプライン全体を通じてモデルの改ざんを防ぎます。

実践的な提言と結論

ソブリンAIの取り組みを評価するリーダーに向けて、次の点を推奨します。

- **主権は絶対ではなくスペクトラムであると受け入れる。** 最先端の国々でさえグローバルなサプライチェーンの中で活動しています。重要なのは、要となるレイヤーに対する実質的なコントロールを、肝心なところで確実に効かせることです。
- **データレジデンシーと主権を明確に区別する。** 物理的な所在地は、主権を主張するための必要条件ではあっても十分条件ではありません。
- **5つのレイヤーすべてを体系的に評価する。** 1つのレイヤーの欠落だけでも、システム全体が損なわれかねません。
- **複数ベンダーを活用する。** ハードウェア、モデル、運用パートナーの各面で複数のベンダーを使い、単一障害点のリスクを回避します。
- **支配権変更イベントに備える。** ベンダー買収に対する契約上および技術上の防御策を組み込みます。
- **人材もサプライチェーンの一部として扱う。**
これらのシステムを構築・運用する専門知識には、それ自体に主権上の含意があります。



ソブリンAIは、正しい条件の下でなら追求する価値があります。データ、モデル、運用に対する実質的なコントロールは、規制対象セクターにおいて、また国家のレジリエンスの観点からも、基本要件になりつつあります。同時に、本リサーチを通じて述べてきた依存関係は、願望で消し去るのではなく、設計で織り込むべきものです。成功する国や組織は、どのレイヤーを支配し、どの依存関係を受け入れるかという意図的な選択の積み重ねとして主権を扱うでしょう。100%の自給自足（アウトルキー）を追い求めることが目標ではありません。ここで述べた技術的基盤は、その出発点です。

本テーマに関する次回の記事では、ソブリンAIをどう守るかを検討します。組織が国内でのコントロールを引き受けるとき、物理、ソフトウェア、モデルのサプライチェーンリスクは重要性を増すことはあっても減ることはありません。インフラの構築は最初の一步にすぎません。それを守るには、攻撃者がシステムだけでなくモデルと学習データをも標的とする、新たなアタックサーフェスを理解する必要があります。

参考文献

1. Muath Alduhishy. (April 25, 2024). World Economic Forum. "Sovereign AI: What it is, and 6 strategic pillars for achieving it." Accessed June 1, 2026, at: [Link](#).
2. David Sacks and Adam Segal. (March 4, 2025). Council on Foreign Relations. "Unpacking TSMC's \$100 Billion Investment in the United States." Accessed June 1, 2026, at: [Link](#).
3. Matthew Gooding. (March 30, 2026). Data Center Dynamics. "Mistral AI raises \$830m in debt financing for data center in Paris, France." Accessed June 1, 2026, at: [Link](#).
4. Mistral. (Jan. 9, 2026). Generation Digital. "Mistral AI wins French defence AI framework agreement." Accessed June 1, 2026, at: [Link](#).
5. Mike Saunders. (July 8, 2025). The Document Foundation. "Danish Ministry switching from Microsoft Office/365 to LibreOffice." Accessed June 1, 2026, at: [Link](#).
6. Chris Penrose. (June 11, 2025). NVIDIA Blog. "Leading European Telcos Build AI Infrastructure With NVIDIA for Regional Enterprises." Accessed June 1, 2026, at: [Link](#).
7. Joao Gomes. (Nov. 13, 2024). NVIDIA Blog. "Indonesia Tech Leaders Team With NVIDIA and Partners to Launch Nation's AI." Accessed June 1, 2026, at: [Link](#).
8. SEB Group. (May 24, 2025). SEB Group. "SEB joins Swedish consortium building AI factory with Nvidia." Accessed June 1, 2026, at: [Link](#).
9. Qualcomm. (Oct. 28, 2025). Qualcomm. "HUMAIN and QUALCOMM to deploy AI Infrastructure in Saudi Arabia for Global Inferencing." Accessed June 1, 2026, at: [Link](#).
10. Silicon Analysts. (March 13, 2026). Silicon Analysts. "Foundry Allocation Status 2026: Where Capacity Is and Isn't." Accessed June 1, 2026, at: [Link](#).
11. Monica Chen. (Nov. 22, 2024). DigiTimes. "Nvidia secures 60% of TSMC's doubled CoWoS capacity for 2025." Accessed June 1, 2026, at: [Link](#).
12. U.S. Department of Commerce. (Jan. 15, 2026). U.S. Department of Commerce. "Fact Sheet: Restoring American Semiconductor Manufacturing Leadership Through an Agreement on Trade & Investment with Taiwan." Accessed June 1, 2026, at: [Link](#).
13. Gina M. Raimondo. (Feb. 26, 2024). U.S. Department of Commerce. "Remarks by U.S. Secretary of Commerce Gina Raimondo: Investing in Leading-Edge Technology." Accessed June 1, 2026, at: [Link](#).
14. Brian Tristram Williams. (Jan. 14, 2026). EE News Europe. "TSMC Arizona expansion plan jumps to \$465bn under proposed US-Taiwan tariff deal." Accessed June 1, 2026, at: [Link](#).

15. NVIDIA Newsroom. (June 11, 2025). NVIDIA Newsroom. "Europe Builds AI Infrastructure With NVIDIA to Fuel Region's Next Industrial Transformation." Accessed June 1, 2026, at: [Link](#).
16. NVIDIA Newsroom. (June 11, 2025). NVIDIA Newsroom. "Europe Builds AI Infrastructure With NVIDIA to Fuel Region's Next Industrial Transformation." Accessed June 1, 2026, at: [Link](#).
17. Nick Patience. (June 23, 2025). Futurum. "NVIDIA's European AI Sovereignty Push: Infrastructure, Partnerships, and Policy — Report Summary." Accessed June 1, 2026, at: [Link](#).
18. HPE Newsroom. (Dec. 1, 2025). HPE Newsroom. "HPE simplifies and accelerates development of AI-ready data centers with secure AI factories powered by NVIDIA." Accessed June 1, 2026, at: [Link](#).
19. NVIDIA Newsroom. (May 13, 2025). NVIDIA Newsroom. "Saudi Arabia and NVIDIA to Build AI Factories to Power Next Wave of Intelligence for the Age of Reasoning." Accessed June 1, 2026, at: [Link](#).
20. SoftBank Group. (May 22, 2025). SoftBank Group. "Global Tech Alliance Launches Stargate UAE." Accessed June 1, 2026, at: [Link](#).
21. Jay Puri. (Feb. 17, 2026). NVIDIA Blog. "India Fuels Its AI Mission With NVIDIA." Accessed June 1, 2026, at: [Link](#).
22. TechNode Global Staff. (Nov. 3, 2025). TNGlobal. "YTL Power completes NVIDIA-powered AI data center facility in Johor." Accessed June 1, 2026, at: [Link](#).
23. Blake Crosley. (March 19, 2026). Introl. "France's AI Sovereignty Push: Infrastructure Behind the European AI Champion." Accessed June 1, 2026, at: [Link](#).
24. Sarvam AI. (April 26, 2025). Sarvam AI. "The government of India selects Sarvam to build India's sovereign large language model." Accessed June 1, 2026, at: [Link](#).
25. IMDA Singapore. (Dec. 4, 2023). IMDA Singapore. "Singapore pioneers S\$70m flagship AI initiative to develop Southeast Asia's first large language model ecosystem catering to the region's diverse culture and languages." Accessed June 1, 2026, at: [Link](#).
26. Jimin Lee. (Jan. 10, 2024). Futurum. "HyperCLOVA X: Leading AI Sovereignty in South Korea." Accessed June 1, 2026, at: [Link](#).
27. Virpratap Vikram Singh. (Aug. 28, 2025). IISS. "Sovereign AI: pathways to strategic autonomy." Accessed June 1, 2026, at: [Link](#).
28. Pablo Chavez. (Nov. 7, 2024). Lawfare. "Sovereign AI in a Hybrid World: National Strategies and Policy Responses." Accessed June 1, 2026, at: [Link](#).
29. Julie Sobowale. (Nov. 17, 2025). The Walrus. "Cohere Is Canada's Biggest AI Hope. Why Is It So American?" Accessed June 1, 2026, at: [Link](#).

30. Josh Scott. (Dec. 6, 2024). BetaKit. "Cohere secures federal backing to build multibillion-dollar Canadian AI data centre." Accessed June 1, 2026, at: [Link](#).
31. Joe Castaldo. (July 2, 2025). The Globe and Mail. "CoreWeave to operate AI data centre in Cambridge, Ont., with Cohere as customer." Accessed June 1, 2026, at: [Link](#).
32. Bill Whyman. (Dec. 4, 2025). CSIS. "Sovereign Cloud-Sovereign AI Conundrum." Accessed June 1, 2026, at: [Link](#).
33. U.S. Department of Justice. (April 2019). U.S. Department of Justice. "Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act." Accessed June 1, 2026, at: [Link](#).
34. Brad Smith. (March 4, 2022). Microsoft. "Microsoft suspends new sales in Russia." Microsoft On the Issues. Accessed June 1, 2026, at: [Link](#).
35. S3NS. (Dec. 17, 2025). S3NS. "S3NS Announces SecNumCloud Qualification for PREMI3NS." Accessed June 1, 2026, at: [Link](#).
36. Stéphane Vanrechem. (May 13, 2025). Forrester. "S3NS Summit Highlights Sovereignty And Trusted Cloud Progress." Accessed June 1, 2026, at: [Link](#).
37. OVHcloud. (n.d.) OVHcloud. "SNC Cloud Platform." Accessed June 1, 2026, at: [Link](#).
38. Nick Patience. (March 5, 2026). Futurum. "S3NS & Sovereignty: Can Thales-Google Venture Make AI Sovereignty Work at Scale?" Accessed June 1, 2026, at: [Link](#).
39. Google Cloud. (n.d.) Google Cloud. "France Data Boundary by S3NS." Accessed June 1, 2026, at: [Link](#).
40. CycloneDX. (n.d.) CycloneDX. "Machine Learning Bill of Materials (ML-BOM)." Accessed June 1, 2026, at: [Link](#).

TREND MICRO

本書に関する著作権は、トレンドマイクロ株式会社へ独占的に帰属します。

トレンドマイクロ株式会社が書面により事前に承諾している場合を除き、形態および手段を問わず本書またはその一部を複製することは禁じられています。本書の作成にあたっては細心の注意を払っていますが、本書の記述に誤りや欠落があってもトレンドマイクロ株式会社はいかなる責任も負わないものとします。本書およびその記述内容は予告なしに変更される場合があります。

本書に記載されている各社の社名、製品名、およびサービス名は、各社の商標または登録商標です。

〒160-0022

東京都新宿区新宿 4-1-6 JR新宿ミライナタワー

<https://www.trendmicro.com>

トレンドマイクロはサイバーセキュリティのグローバルリーダとしてデジタル情報を安全に交換できる世界の実現に貢献します。私たちの革新的なソリューションはデータセンター、クラウド、ネットワーク、エンドポイントにおける多層的なセキュリティをお客様に提供します。

当社のリーダーシップの根幹であるトレンドマイクロリサーチは、多くのエキスパートに支えられています。それは最新の脅威を発見し、重要なインサイトを公に共有し、サイバー犯罪の防止を支援することに情熱を注ぐ人材です。当社のグローバルチームは、日に数百万もの脅威を特定し、脆弱性の開示を先導し、標的型攻撃・AI・IoT・サイバー犯罪等における革新的な研究結果を公表しています。私たちは次に来る脅威を予測し、セキュリティ業界が進むべき方向を示しうる示唆に富んだ研究成果を提供するため、継続的に取り組んでまいります。

© 2026 Trend Micro Incorporated. All Rights Reserved.



さらに詳しい情報をお求めの方へ

TrendAI | Resources and Insights



TrendAI™は、AIセキュリティのグローバルリーダーであり、Trend Microのエンタープライズ事業部門として、AIの完全な可視化と統合されたセキュリティを提供します。それにより、組織に確かな信頼をもたらし、イノベーションを促進し、リスクを排除します。

TrendAI™は、185の国と地域にわたる大手企業や政府機関から信頼を得ており、アイデンティティからインフラストラクチャ、データに至るまで、組織全体を保護します。

AI Fearlessly.

詳細はこちら：trendaisecurity.com

Copyright © 2026. Trend Micro Incorporated. All rights reserved. [REP00_Building_Sovereign_AI_200726US]