

CISO、DPO、コンプライアンス責任者の皆様へ

データ主権はアーキテクチャであり、契約条項ではない

貴社のデータを、貴社の管轄で、貴社がコントロールする。

課題

日本は、米国のハイパースケーラーへの依存を維持しながらも、それと並行して「まず法域(ジュリスディクション)を重視する」データ主権戦略を進めており、日本の政策コミュニティ自身が「データが日本国内に留まる」という主張を真の主権の代替とすることを明確に否定し始めています。その典型例が2026年4月3日、マイクロソフトが日本国内に100億ドル(約1.6兆円)を投資すると発表し、これを「データを日本国内に保持するソブリンAIインフラ」と明確に位置づけたことです。しかし専門家や業界の分析はこの説明に真っ向から異を唱えました。マイクロソフトは米国法人であるため、物理的なインフラの所在地にかかわらず米国クラウド法(CLOUD Act)の適用対象であり続け、「データが日本国内にある」というのはデータの所在地(レジデンシー)を示すにすぎず、法域主権そのものを意味しないというのです。アナリストは、この発表の中で真に主権的と言える要素は、提携先のうち日本法域の当事者に限られると指摘しました。実際、その数日前の2026年3月27日には、日本のデジタル庁がさくらインターネットの「さくらのクラウド」について、政府共通クラウド(ガバメントクラウド)で全305項目の技術要件をすべて満たし、AWS、Azure、Google Cloud、Oracleと同等の本番運用が可能になったと発表しており、国内資本が管理する事業者がこの水準に達したのは史上初めてのことでした。

外国事業者と並行して法域を国内に置くドメスティックな選択肢を追加していく、全面的な移行を義務づけるのではなく、この現実的なモデルは、日本の業界ガイドスにも反映されています。すなわち、一般的な業務用途のAI利用はグローバルなクラウドサービスでも許容できる一方、政府・医療・金融など機密性の高いワークロードについては、データと処理が日本の法域から一切出ないソブリン基盤上で運用すべきだとする、リスクに応じた「セグメント化」導入戦略が支持を広げているのです。日本の経済安全保障ドクトリンは今や、クラウドとAIインフラを半導体や重要鉱物と並ぶ戦略分野と位置づけており、これを裏付ける形で国のAI基本計画には1兆円を超える予算が投じられ、約18万人の国家公務員を対象に、国産の基盤モデルを国内で管理するクラウド基盤上で稼働させる政府AI「GENAI」の実証も進んでいます。AI時代のデータ流通に対応するため2026年に改正された個人情報保護法(APPI)の下では、契約上の保証や「データは日本国内に保管されている」という主張だけでは、個人情報保護委員会(PPC)や日本の経済安全保障政策コミュニティが投げかける問いに答えられません。すなわち、お客様のデータとそれを処理するAIを実際に管理しているのは誰か、そしてその答えは日本の法域内にあるのか、という問いです。

ソリューション

Kiteworksは、データ主権を契約条項としてではなく、アーキテクチャとして提供します。これは、データのレジデンシー(所在地)と法域主権を明確に区別する、日本の政策コミュニティ自身の考え方や軌を一にするものです。オンプレミス、お客様自身のクラウド、またはKiteworksがホストするプライベートクラウドとして、日本国内を含むお客様が選択した法域に、シングルテナント(単一顧客専用)のインフラを展開でき、暗号化鍵はお客様だけが保持します。Kiteworksはお客様の暗号化鍵を一切保持せず、顧客間でインフラを共有することはありません。そのため「データは日本国内にある」という言葉は、インフラと鍵を誰が管理しているかを示す事実となり、米国クラウド法などの下でサーバーの所在地にかかわらず開示義務を負いかねない米国法人による、単なるレジデンシー上の主張とは一線を画します。

Data Policy Engineのジオフェンシング(地理的制御)ルールにより、あらゆる送信・共有・ダウンロードをリアルタイムで統制します。SIEMIにリアルタイムで連携される、完全かつ絞り込みのない監査証跡によってそれを証明できます。FedRAMPおよびIRAPの評価に対応したホスティングオプションにも対応しており、日本国内で広がりつつある「データの機微度に応じたリスクをセグメント化する」主権モデルにそのまま応えるものです。政府・金融・医療といったワークロードには最も厳格なアーキテクチャを適用しつつ、それ以外の一般的な業務利用を妨げることはありません。

なぜ今、日本において主権が経営会議レベルの課題なのか

33%	過去1年間に主権関連のインシデントに見舞われた組織の割合。
1兆円超	日本の国家AI基本計画のもと、ソブリンなコンピューティングおよびAI基盤に投じられた予算規模。
1,700以上	中央省庁とあわせて、日本の標準化されたガバメントクラウドへの移行対象となっている地方自治体の数。
2025年12月	PPCのガイドラインにおいて、Global CBPR認証がAPPIの越境移転における「同等の保護」要件を満たすものとして認められた時期。

Kiteworksが提供する、証明できる主権

■ 設計段階からのシングルテナント

データベース、ファイルシステム、アプリケーション実行環境、OSを他社と一切共有しない専用インフラ。オンプレミス、お客様自身のクラウド、またはKiteworksがホストするプライベートなシングルテナントクラウドとして、日本国内を含むお客様が選択した法域に展開できます。これは、さくらインターネットが日本のガバメントクラウドの資格を得るために満たした法域管理の水準と同じものです。

■ 顧客保有の暗号化鍵

HSM連携により、Kiteworksはもちろん、Kiteworksに開示を強制しようとするいかなる第三者もお客様のデータを復号できません。これは、事業者の物理的なインフラの所在地にかかわらず、米国クラウド法の下で米国人法人に開示を強制しようとする外国当局に対しても同様です。

■ ジオフェンシングによる送信制御

Data Policy Engineは、ユーザーの位置情報、ブロック対象国、IPレンジに基づいて、送信・共有をブロックまたは承認制にし、ダウンロードそのものを完全にブロックすることも可能です。APPIの越境移転に関する安全管理措置を直接的に支える機能です。

■ あらゆるチャネルをのコントロールプレーンで統制

電子メール、ファイル共有、SFTP、MFT、API、AIエージェントはすべて同じ送信ポリシーで統制されるため、政府・金融・医療といった機密性の高いワークロードにも最も厳格な基準を適用しつつ、それ以外の一般的な業務利用を妨げることはありません。

■ 完全かつ絞り込みのない監査証跡

すべてのユーザー、管理者、システムの操作がリアルタイムで記録され、サンプリングや負荷時の制限なくSIEMへリアルタイムに連携されます。PPCや日本の経済安全保障に関する審査がますます求めるようになっている証跡です。

■ 政府水準の評価基準をクリア

FedRAMP High(申請中)、2017年からのFedRAMP Moderate認証、IRAP評価対応のホスティングは、このアーキテクチャが政府レベルの主権要件を満たしていることを示しています。日本のデジタル庁が国内事業者をガバメントクラウドに迎え入れる前に適用したのと同種の、厳格な技術基準です。

日本において主権が譲れない領域

政府・公共部門

日本のガバメントクラウド移行に関わる国民のデータ。中央省庁に加え、デジタル庁のもとで標準化されたクラウド基盤への移行対象となっている1,700以上の地方自治体を含みます。

重要インフラ・経済安全保障

経済安全保障推進法のもとで指定される、クラウド・AI・重要インフラといった戦略分野のデータおよび技術。これらは純粋な市場競争ではなく、産業政策の対象として扱われています。

金融サービス

APPIおよび金融分野の監督指針の下にある顧客データ。

医療・ライフサイエンス

APPIにおける要配慮個人情報の規定のもとにある患者データ、および所在地に関する条件が付される研究データ。

出典

Yeandel & Co: “A Flag on the Data Centre: Microsoft’s \$10bn ‘Sovereign AI’ Investment in Japan,” 2026.

Yeandel & Co: “Japan Lets a Domestic Provider In: Sakura Internet and the Government Cloud,” 2026.

Baker McKenzie / IPTech client alert on Global CBPR System addition to APPI guidelines, Jan. 2026.

デジタル庁 (digital.go.jp): Government Cloud および Government AI GENAI に関する公開情報。

内閣府: AI基本計画(案), 2026年6月。

「Data Sovereignty in Japan: Legal Framework, Policy, and Practice」にまとめた調査資料。

Copyright © 2026 Kiteworks. Kiteworksのミッションは、あらゆる送信・共有・受信、そしてプライベートデータの利用におけるリスクを、組織が効果的に管理できるようにすることです。Kiteworksプラットフォームは、統合されたコントロールプレーンにおいて、データガバナンス・コンプライアンス・保護を実現する安全なデータ交換基盤をお客様に提供します。Kiteworksは、組織内外へ移動する機密データを一元的に把握・追跡・制御・保護することで、リスク管理を大幅に向上させ、あらゆるプライベートデータ交換における規制遵守を確実にします。シリコンバレーに本社を置くKiteworksは、世界中で1億人を超えるエンドユーザーと、数千に及ぶグローバル企業・政府機関を保護しています。