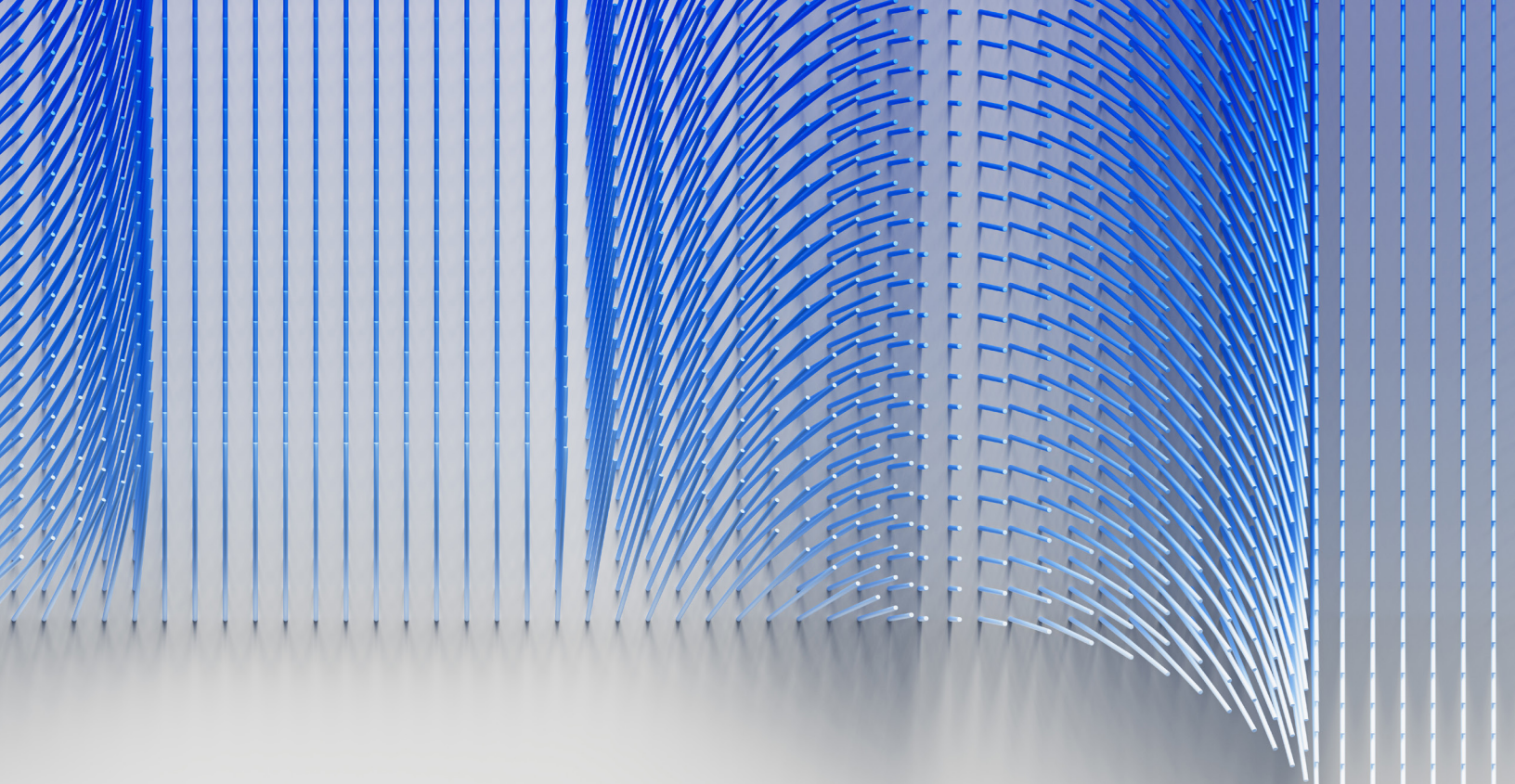




ハイブリッドクラウド とAIの時代における デジタル主権

統制、レジリエンス、
イノベーションに関する見解。



目次

03

エグゼクティブ
サマリー

09

エクスポージャー評価と
ストラテジー・
フレームワーク

04

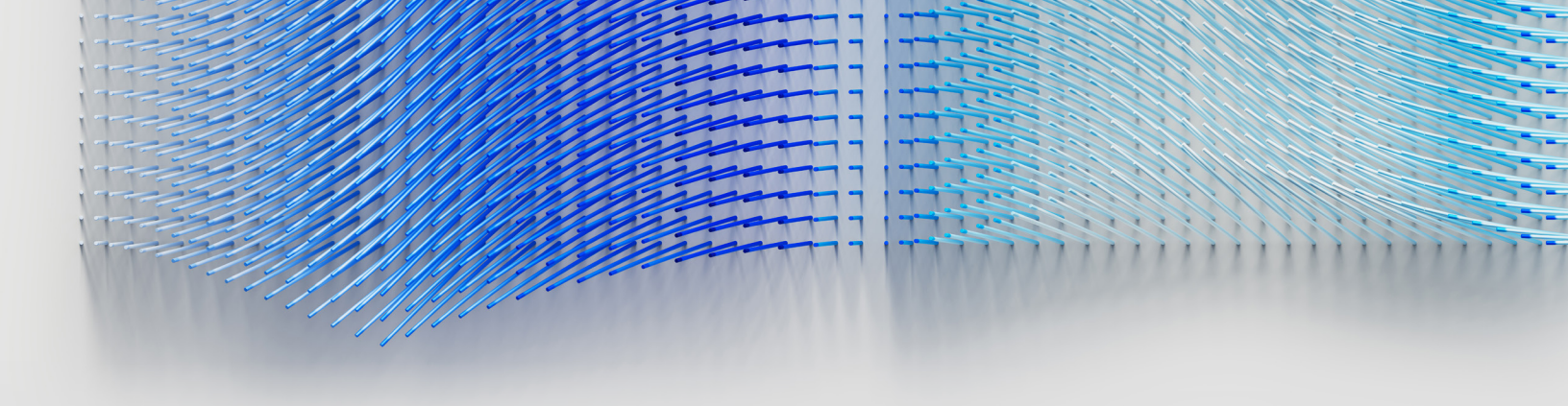
主権の重要性

12

重要ポイントと次のステップ

07

戦略的視点と基本原則



エグゼクティブ・ サマリー

デジタル主権は、いまや多くの企業で役員会議の議題に上がるようになっています。クラウド・アーキテクチャの採用からAIの導入に至るまで、あらゆる戦略的意思決定は、「組織のシステムやデータを最終的に誰が動かし、管理するのか」という問いと切り離せなくなっています。主権、すなわち「自らの条件に基づいてテクノロジーを活用する能力」は、組織がデジタル基盤をどのように設計し、拡張していくかを方向付けるグローバルな運用原則となっています。

組織がAIの効果的な拡張を進めようとする一方で、多くのリーダーは、こうした変革の可能性を持つソリューションの導入を遅らせる継続的な課題を指摘しています。代表的な障壁には、スキル不足、インフラストラクチャーの老朽化、そしてROI（投資収益率）の不確実性などがあります。こうした摩擦要因は多くの組織に共通しており、デジタル主権がもはやコンプライアンスの問題ではなく、モダナイゼーションの問題となっている理由でもあります。リーダーたちは、AIを迅速に導入しつつ、その運用方法に対する統制を維持できるという確信を必要としています。

主権は、組織が統制と柔軟性の基盤を確立するうえで役立ちます。これにより、プロバイダーの切り替えやワークロードの動き、AIの透明性のあるガバナンスの実現、さらに誰が何にアクセスできるのかを確認することが可能になります。

IBMの立場は明確です。主権は意図的に設計され、テクノロジー・スタックのすべての層に組み込まれる必要があります。オープンなエコシステム、ハイブリッド・バイ・デザインの導入（クラウド、オンプレミス、エッジ、さらにはエアギャップ環境まで）、そして組み込み型のAIガバナンスにより、組織は運用に対する統制と柔軟性を確保できます。

主権の重要性

デジタル主権とは、組織、国家、または地域が、自らのデジタル・インフラストラクチャー、データ、標準、そして技術開発を多面的に統制する能力を指します。



データ主権：

データの保管場所を管理し、アクセス権限を持つ人物を制御すること。



AI主権：

組織の権限と管轄の下でAIを運用すること。



運用主権：

外部からの影響を最小限に抑えながら、戦略的意思決定に対する統制を維持すること。



テクノロジー主権：

基盤となるすべてのインフラストラクチャーやテクノロジーにおいて、選択肢と柔軟性を維持すること。

コンプライアンス要件が増え、サイバーリスクが高まる中、組織はAIツールのガバナンス、ホスティング、デプロイメント、運用設計を含むデジタル運用を、自らの権限のもとで統制していることを示すよう求められる場合があります。こうした統制ニーズの高まりを受けて、デジタル主権の重要性がさらに高まっています。

確かなデジタル主権を確立することで、組織はグローバル規模のテクノロジーがもたらすスピードやイノベーションを犠牲にすることなく、統制を維持できます。

なぜ今、デジタル主権が重要なのか

データは、現代経済における決定的な戦略的資産になりつつあります。テクノロジー・インフラストラクチャーはますますグローバル化し、国境をまたがるエコシステムの中で設計・導入・運用されるようになっていきます。そのため、デジタル・インフラストラクチャーやAIモデルに対する統制を維持することが不可欠です。中核となるデジタル統制を最新の状態にすることで、組織は現在の市場環境においてレジリエンスとコンプライアンスを保つことができます。

デジタル主権は、ベンダーへの依存度にかかわらず、組織が自らのデジタル・エコシステムに対して明確な主導権を持つことを可能にします。外部からの圧力が強まる中、こうした実証可能な統制力へのニーズは、経営層にとっての優先事項となっています。

規制の自律性：

AI、データ・ガバナンス、デジタル・サービスに関するグローバルおよび各国・地域のルールを施行し、デジタル運用に対する強固な統制、透明性、独立性を確保する

セキュリティ・リスクの予測：

デジタル資産とテクノロジーを管理し、サイバー・リスクを低減するとともに、重要なインフラストラクチャーを保護する

デジタル・インフラストラクチャーの管理：

クラウド・サービス、ネットワーク、ソフトウェア・プラットフォームにおける自律性を維持し、オペレーショナル・レジリエンスを強化する

競争上の差別化：

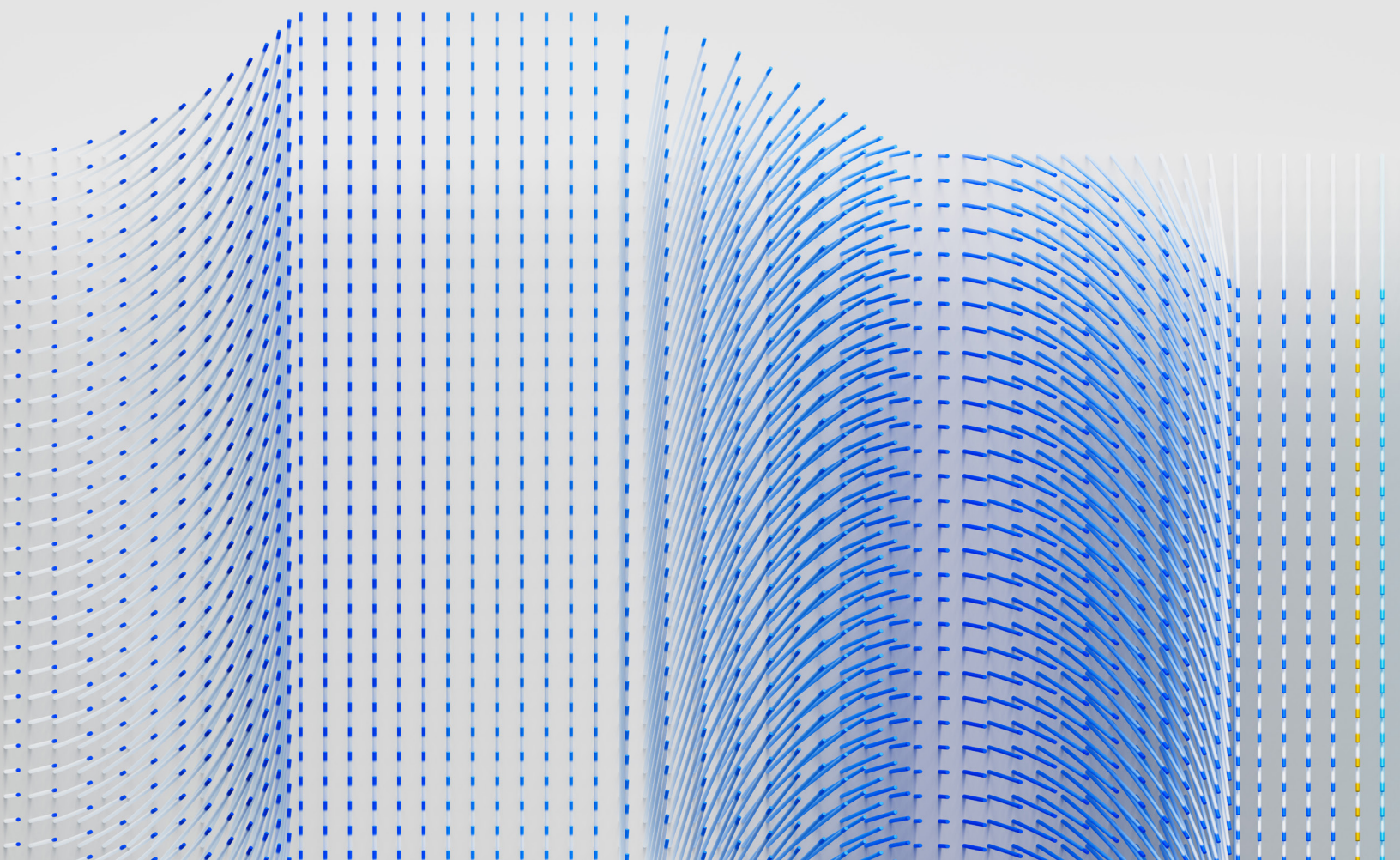
デジタル主権は、組織が明確なデジタルの主導権のもとで事業を進められることを示し、特に規制対象業界において、規制当局、パートナー、お客様からの信頼を高めます

デジタル主権は相互に依存する複数の領域にまたがっているため、組織は主権に関するあらゆる要件を満たすよう、自社の戦略を再評価する必要があるかもしれません。

デジタル主権の各要素は、互いに強化する関係にあります。オープン標準やポータブル・アーキテクチャに基づく**テクノロジー主権**は、プロバイダー間で運用を移行しやすくすることで運用主権を可能にします。そして**運用主権**は、組織が地域の要件に沿ってデータを管理できるようにすることで、**データ主権**を保護します。そして**AI主権**は、AIモデルの透明性を確保し、現地の統制下に配置するために不可欠なレイヤーを追加します。

これらの要素は連携し、より広範な**デジタル主権**フレームワークの中で機能します。このフレームワークは、そういった要素を一貫して適用するために必要なガバナンス、説明責任、透明性を包括的に提供します。

これらの要素が相互に依存していることから、組織はそれらを総合的に評価して、自社全体の体制における弱点を特定し、組織のニーズを優先した戦略的トレードオフを行う必要があります。



デジタル主権が業種・ 業務にもたらす影響

デジタル主権により、組織はシステムの運用者、データのガバナンス方法、そしてワークロードの実行場所を統制できるようになり、継続的なコンプライアンス管理の強化と運用リスクの低減を実現できます。これは、特に規制の厳しい業種・業務やクリティカルなインフラストラクチャーに関わるセクターにおいて特に重要です。こうした分野では、システム障害、データ漏洩、外部への依存がもたらす代償が、即時かつ深刻になり得るためです。



官公庁・自治体と公共部門：

多くの官公庁・自治体や公共機関は厳格な主権要件を遵守する必要があり、データ、AIシステム、運用プロセスに対する確実な統制が不可欠になります。ソブリン・プラットフォームは、部門間での安全かつコンプライアンスに準拠したデータ共有の基盤を提供し、AIの機能を政策や規則に整合させるとともに、規制や法制度のフレームワークを管理するための透明性の高い監査を可能にすることで、こうした要件を支援します。



金融サービス：

多くの銀行、保険会社、決済プロバイダーは、リアルタイム決済、重要なデータフロー、そしてリスク管理やコンプライアンス管理を支えるAIモデルに対する統制を維持するために、デジタル主権の原則を活用しようとしています。デジタル主権を最優先に据えたアプローチは、IDシステム、取引データ、モデル・ガバナンスに対する主導権を強化すると同時に、相互接続された金融エコシステム全体における透明性と説明責任を高めます。さらに、自動化されたコンプライアンス機能、継続的な証拠生成、統合されたレポート機能により、規制要件の管理を迅速かつ確実に行うことが可能になります。また、AIは不正防止におけるイノベーションの加速や、パーソナライズされた顧客体験創出の取り組みにも役立ちます。

デジタル主権は、長期的な安定と戦略的自律性への投資です。進化する規制要件への対応に今取り組む組織は、責任とレジリエンスが成功するための重要な要因となる市場において、自信を持ってイノベーションを推進し、より深い信頼を築き、リーダーシップを発揮する立場を確立できます。未来を切り拓くのは、自らのデジタル資産を管理・統制していることを、単に主張するだけでなく実証できる組織です。



医療：

医療組織は極めて機密性の高いデータ環境を運用しており、いかなる侵害や障害も、人的、運用上、そして経済的に即座に影響を及ぼす可能性があります。デジタル主権は、患者データ、ゲノム・データ、臨床データの厳格な所有権を支えると同時に、病院、研究機関、診断パートナー間での安全な情報共有を可能にします。



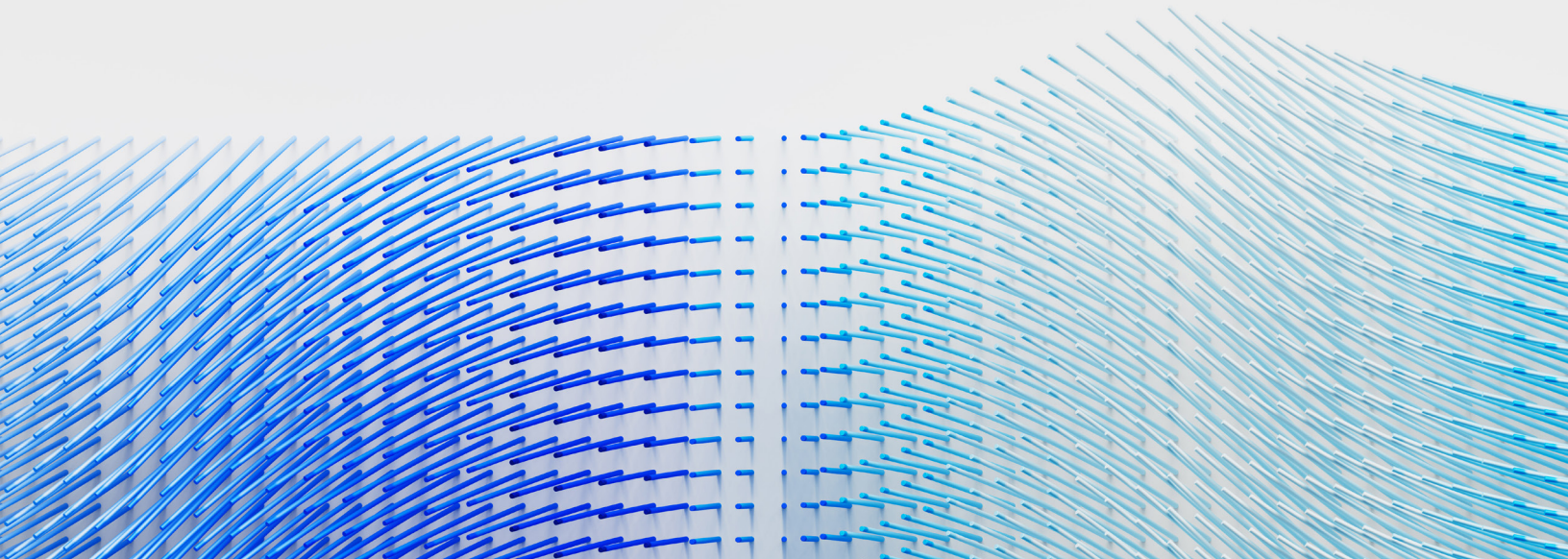
公益事業者と通信事業者：

公益事業や通信を担う組織において、デジタル主権は、オペレーションを認可された管理下に置くことで電力網管理や通信システムを保護し、外部からの脅威、サプライチェーンの問題、その他のリスクへの露出を低減します。ソブリン・インフラストラクチャーは、サービス継続性の強化、インシデント対応の迅速化、そして重要サービスの保護、コンプライアンス、信頼性の向上を支援します。

戦略的視点と基本原則

AIは、デジタル時代における主権の意味を再定義しています。意思決定、サービス提供、重要なインフラストラクチャーが、複雑でグローバルに分散したAIシステムにさらに依存していく中、データの所在地や領域的な管理に焦点を当てた従来の主権モデルでは、もはや十分ではありません。

IBMでは、「デジタル主権とは、変化が激しく規制の厳しい環境の中で、自らの条件に基づいて強力なテクノロジーを活用できる能力である」と考えています。それは、戦略的な柔軟性とレジリエンスを解き放つ鍵となり、データ、AIモデル、運用、テクノロジーに対する実証可能な統制を維持すると同時に、効率性、俊敏性、迅速なイノベーションを実現します。



IBMの主権に関する原則

IBMのデジタル主権へのアプローチは、規制要件を尊重しながら成長を促進するオープンでセキュアなハイブリッドクラウドおよびAIの機能を通じて、組織の力を引き出すことを重点に置いています。IBMは、国境を越えたデータ保護を支援しつつ、透明性を重視し、責任あるAIの導入を推進することで、データに対する統制を長期的な戦略的優位性へと転換できるよう支援します。

当社のデジタル主権への包括的なアプローチは、これらの基本原則に基づいています。

顧客による統制と選択

IBMは、ロックインに縛られることなく情報に基づいた意思決定を行えるよう、必要なツールと明確性を顧客に提供します。これにより、顧客はデータ、ワークロードの配置、テクノロジーの選択に対して高いレベルの統制を維持することができます。

透明性と信頼

IBMは、組織がデータ資産を発見し、キュレートし、管理することを可能にするテクノロジーを提供します。

柔軟な主権モデル

IBMは、ソフトウェア、インフラストラクチャー、コンサルティング・サービスにわたる幅広いソリューションを提供し、さまざまな組織、業種・業務、データの種類に応じたデジタル主権の要件に対応します。

妥協のないイノベーション

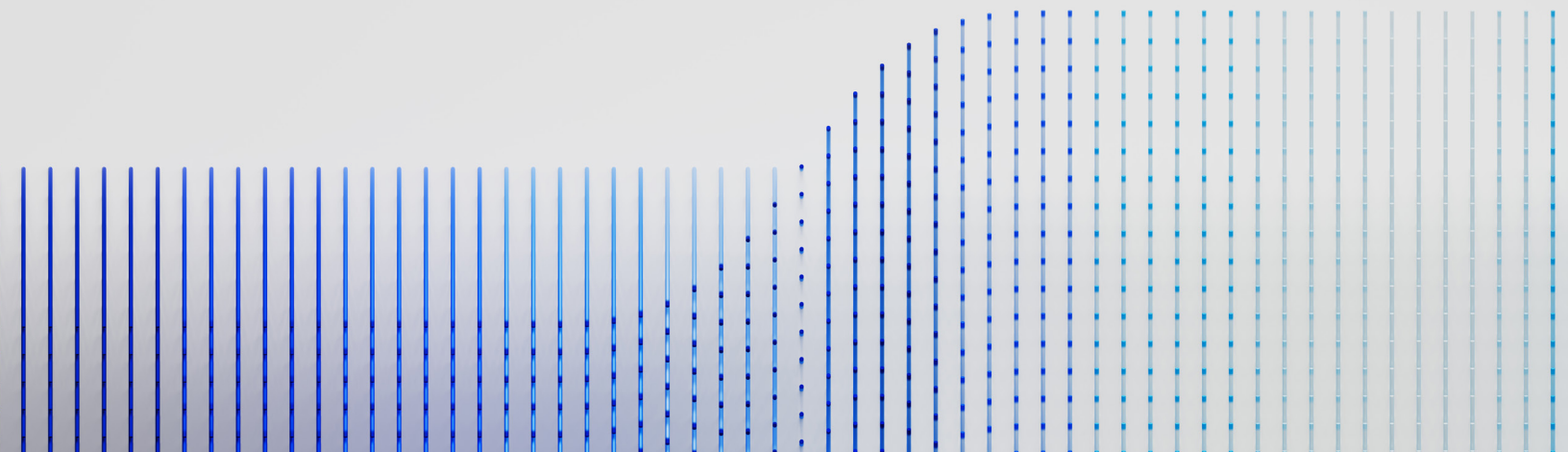
IBMのアーキテクチャへのアプローチは、データ、AIモデル、運用、テクノロジーといったデジタル主権のあらゆる側面において、選択の自由、統制、コンプライアンスを重視しながら、組織がイノベーション目標を達成できるよう支援します。

IBMは、ハイブリッドクラウドの公開性とAIの力が組み合わせることで、真の変革が実現すると考えています。この組み合わせは、増分アップグレードを超えた組織の動きを支援し、クライアントが制御できる柔軟性、セキュリティ、継続的なイノベーションを目的に設計されたアーキテクチャの構築に重点を置くことができます。

このアプローチにより、組織は次のことを実現できます。

- ベンダーの所在地や運用上の制約、意向に縛られることなく、使用するテクノロジー、モデル、実行環境を自由に選択し、それらをどこで利用するかを選ぶこと
- AI機能に対する統制を確保し、技術的な依存関係を把握すること

この基盤のもとで、IBMは顧客が自社の環境全体にわたってデータを活用し、確信を持って自動化を推進し、責任ある形でAIを拡張できるよう支援します。その成果は、技術的に高度であると同時に、組織が求める価値観、ガバナンス、パフォーマンスと戦略的に統合した変革を実現することが可能になります。



エクスపోージャー評価 とストラテジー・ フレームワーク

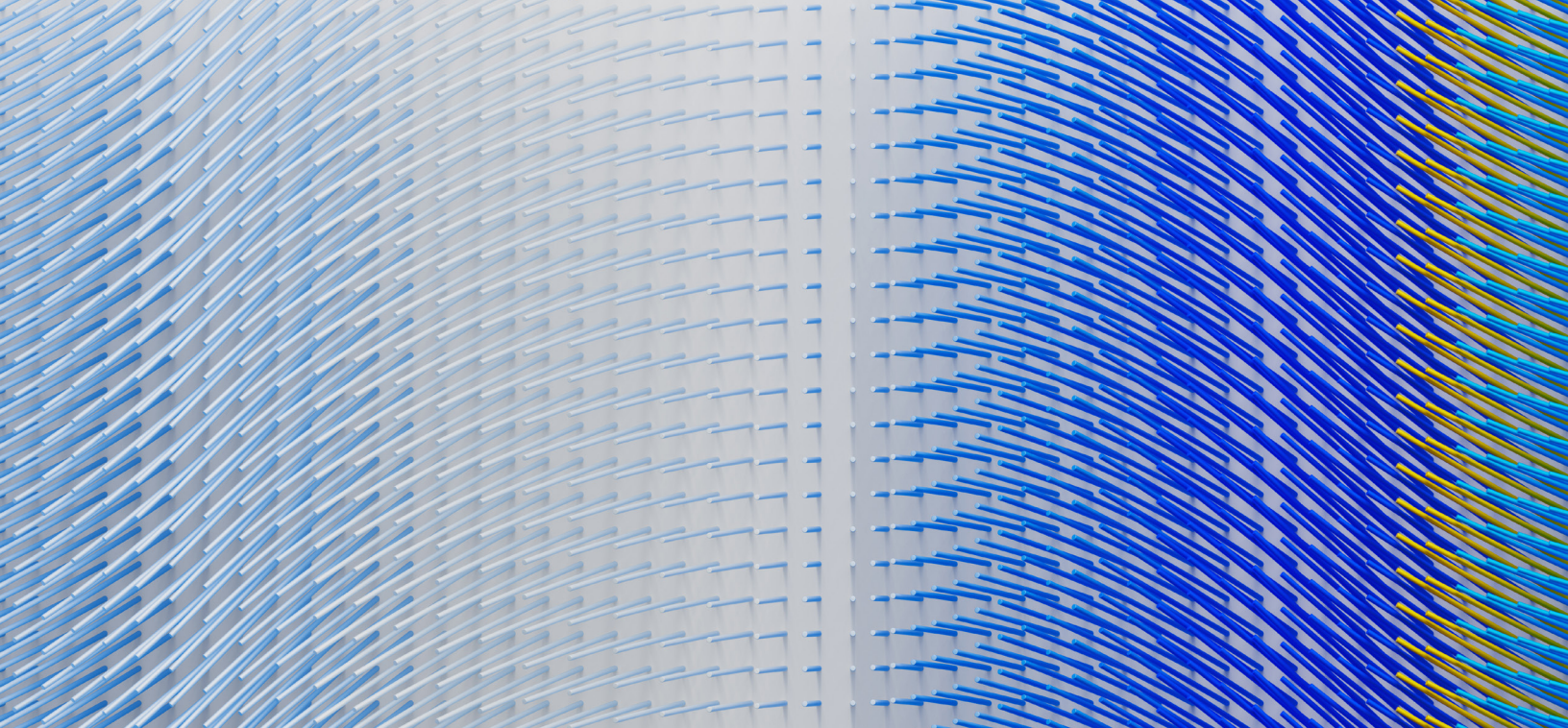
効果的なデジタル主権の実装は、まず組織のビジネス、データ、オペレーション、規制上の義務にわたって、主権が実際にどのような形で求められるのかを厳密に評価することから始まります。IBMの主権評価・フレームワークは、どこにリスクや脆弱性があるのか、そしてどの領域でより強固な統制が必要なのかを組織が特定できるよう、体系的なアプローチを提供します。

勤務地：	システムの設置場所を特定する
データの自律性：	データの保管場所と誰がアクセスできるのかを把握する
AIモデル：	使用されているAIモデルを特定する
プロセス：	ビジネス、運用、またはAIのプロセスを、誰が作成、調整、改善できるのかを定義する
ガバナンス：	AI成果物の精度、バイアス、ドリフト、説明可能性に関する要件を評価する
オープンネス：	標準、エコシステム、オープンソース・コンポーネントの公開性を評価する
運用：	システムの運用および保守を誰が行うのかを明確にする

包括的なストラテジー・フレームワーク

事後対応型の防御から事前対応型のガバナンスへの動きを支援することで、組織は国境やクラウド環境をまたいで重要なワークロードやデータを保護できるようになります。以下のステップは、長期的な運用の健全性とデジタル主権を確立するための基盤となるものです。

- リスクの特定：**
対応すべき課題やエクスపోージャーを明確に特定します。
- 統制の選択：**
特定されたリスクを軽減するための具体的な対策を選定します。
- 施行の実施：**
テクノロジー・スタックの5つのレイヤーすべてにわたって統制を適用します。
- 証拠収集：**
統制が効果的に、かつ意図した通りに機能していることを示す証拠を継続的に収集します。
- 監査と検証：**
規制当局、監査機関、利害関係者に対してコンプライアンスを実証します。



リスクの特定

主権に関する機能に投資する前に、組織は自社の状況においてなぜ主権が重要なのかを明確にする必要があります。このステップでは、規制要件を十分に理解することに加え、ビジネス目標、顧客の期待、競争環境を明確に把握することが求められます。

「なぜ主権が自組織にとって重要なのか」を明らかにすることで、以下の点を定義することができます。

- 具体的な規制要件とコンプライアンスの期限。
- 主権によって実現または保護されるビジネス目標。
- 主権によって軽減できるリスク・シナリオ。
- 利害関係者の期待と成功基準。
- 緊急性と影響度に基づく主権要件の優先順位付け。
- 組織の現在の成熟度レベルの特定。

これらの点を定義することは、目標とする成熟度レベルや戦略的アプローチの選定など、その後のすべての意思決定の指針となります。

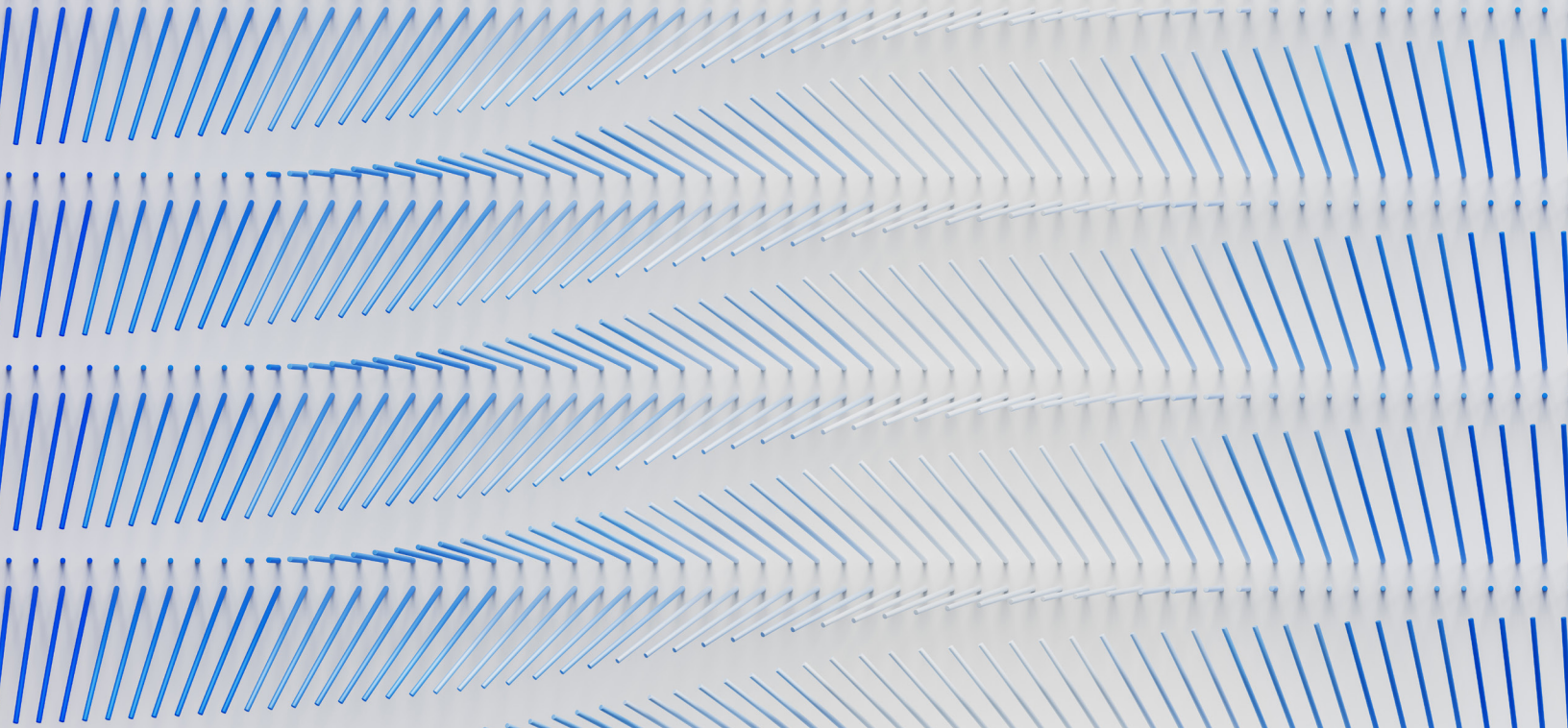
統制の特定

主権に関する要件が明確になったら、組織はそれを満たすために必要となる技術的、運用的、組織的な統制を特定しなければなりません。

すべての統制が、すべての組織に必要というわけではありません。適切な統制は、次の要素に基づいて選定する必要があります。

- 適用される規制要件
- 組織のリスク・プロファイルおよび具体的なリスク・シナリオ
- 組織の現在の成熟度レベルと目標とする成熟度レベル
- 組織全体にわたる戦略的なアプローチ
- コストと比較して最良のリスク削減を提供するコストメリット分析
- 利用可能な参考情報と専門知識による実装の実現可能性

このプロセスでは、組織全体の戦略的方向性を踏まえ、統制が現在の能力と長期的なビジョンの双方に整合するよう選定することが重要です。



レイヤー全体への実装

適切な統制を特定することは最初のステップに過ぎません。組織は統制をテクノロジー・スタック全体にわたって適用し、維持する必要があります。このステップでは、主権に関する統制がアーキテクチャーの各レイヤーでどのように機能するのかを理解し、環境の変化に応じてそれらを一貫して適用していく方法を把握します。IBMは、それぞれに固有の技術要件および運用要件を持つ5つの重要なレイヤーにわたる実装を可能にします。

- インフラストラクチャー：あらゆる主権統制の基盤。
- プラットフォーム：コンテナ・オーケストレーションなどの中核機能に加え、プラットフォームおよびミドルウェア・サービス、IDおよびアクセス管理、オブザーバビリティを備えたアプリケーションのランタイム環境
- アプリケーションとワークロード：ビジネス・ロジックが実行され、データ処理が行われるレイヤー
- データとAI：組織にとって価値が高く機密性の高い資産の管理
- オペレーション：規制要件を満たすために環境を管理する人、プロセス、ツール

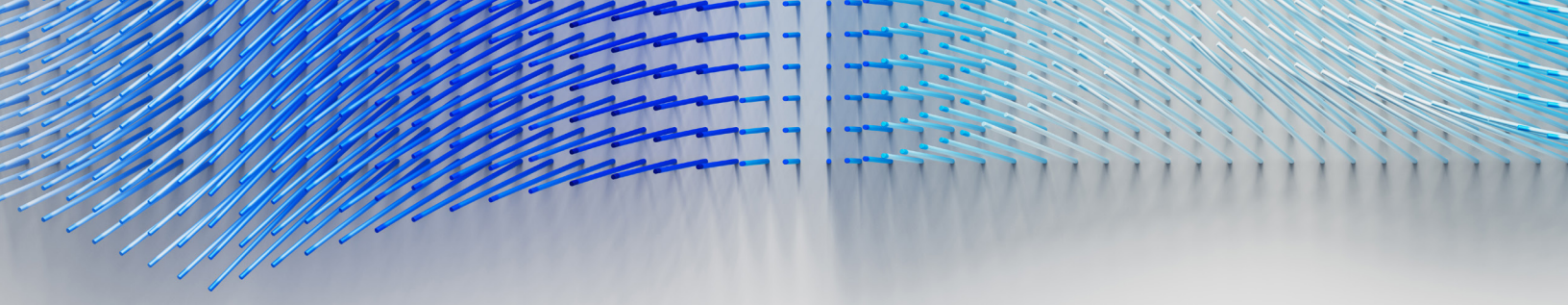
証拠収集と監査対応

統制の実装は、デジタル主権を示すうえで重要なステップです。組織は、統制が実際に機能していることを確認する必要もあり、そのためには包括的な証拠の収集、継続的なモニタリング、そして監査機関、規制当局、顧客に対する明確な報告が求められます。

この検証フェーズには、次の取り組みが含まれます。

- 主権レベルを示すイベントを記録するための証拠収集システムの自動化
- 主権に関する体制の評価
- 対応手順および証拠パッケージの監査
- 適用される規制要件を満たすためのコンプライアンス・レポートの作成
- 調査結果に基づく継続的な改善プロセスの支援

規制要件の変化やテクノロジーの進歩に伴い、組織には継続的な適応を可能にするフレームワークが求められます。IBMは、戦略的な評価とモジュール型のソリューション・ブロックを組み合わせることで、顧客のデジタル主権の実現を支援します。まずクリティカルな要件から着手し、ニーズの変化に応じて拡張していくことで、時間をかけてデジタル主権の体制を構築していきます。



重要ポイントと 次のステップ

デジタル主権は、オープン標準、オープンなエコシステム、そして透明性の高いテクノロジーといったオープンネスに基づいています。これらは、組織に持続的な統制と柔軟性をもたらします。規制が厳格化し、サイバー脅威が加速する中、組織は主権を回避すべき負担として捉えるのか、それとも構築すべき戦略的能力として捉えるのかを判断する必要があります。今投資を決断する組織は、イノベーションと長期的なレジリエンスの強化を促進するデジタル主権の実践により、自信を持ってモダナイゼーションを推進できる立場を確立できます。

IBMは、コンプライアンス対応とイノベーション加速を両立する、明確なデジタル主権戦略の策定を支援します。IBMのハイブリッドとマルチクラウドのアプローチは、ワークロードのモビリティを支援し、規制基準に対応し、エンタープライズ・セキュリティを強化できるよう設計されています。これにより、貴社は将来を見据えた基盤を整え、デジタル主権の確立と強化を図れます。

データ、運用、AI全体に統制を組み込むことで、貴社はコンプライアンス対応に伴う負荷を競争優位性へと変えられます。安心して事業を進め、信頼を維持しながら拡張し、事業を展開するあらゆる市場で効率性、俊敏性、イノベーションを加速できます。詳細はこちら：ibm.com/jp-ja/sovereignty

専門家への相談予約 →

© Copyright IBM Corporation 2026

IBMとIBMのロゴは、米国およびその他の国または地域におけるInternational Business Machines Corporationの商標または登録商標です。その他の製品名およびサービス名は、IBMまたは他社の商標である場合があります。IBMの商標の最新リストはibm.com/jp-ja/trademarkで確認できます。

本資料は最初の発行日時点における最新情報を記載するもので、IBMにより予告なしに変更される場合があります。

IBM製品およびプログラムを使って他社製品またはプログラムの動作を検証する場合は、お客様の責任で行ってください。IBMは、他社の製品やプログラムに責任を負いません。

IBMが事業を展開している国または地域であっても、特定の製品を利用できない場合があります。

本書の情報は「現状のまま」で提供されるものとし、明示または暗示を問わず、商品性、特定目的への適合性、および非侵害の保証または条件を含むいかなる保証もしないものとし、IBM製品は、IBM所定の契約書の条項に基づき保証されます。

完全に安全と見なすことができるITシステムまたはIT製品は存在せず、またいかなる単一の製品、サービスまたはセキュリティ対策も、不正な使用やアクセスの防止において、完全に有効ではありません。IBMは、いかなるシステム、製品、またはサービスも第三者の悪意のある行為や違法行為の影響を受けないこと、またはお客様の企業が影響を受けないことを保証するものではありません。

お客様は、自己の責任ですべての関連法規および規則を順守しなければならないものとします。IBMは法律上の助言を提供せず、IBMのサービスまたは製品を使用することでお客様による法律または規則の遵守が確約されると表明することも保証することはありません。

