2026年版購入者向けガイド

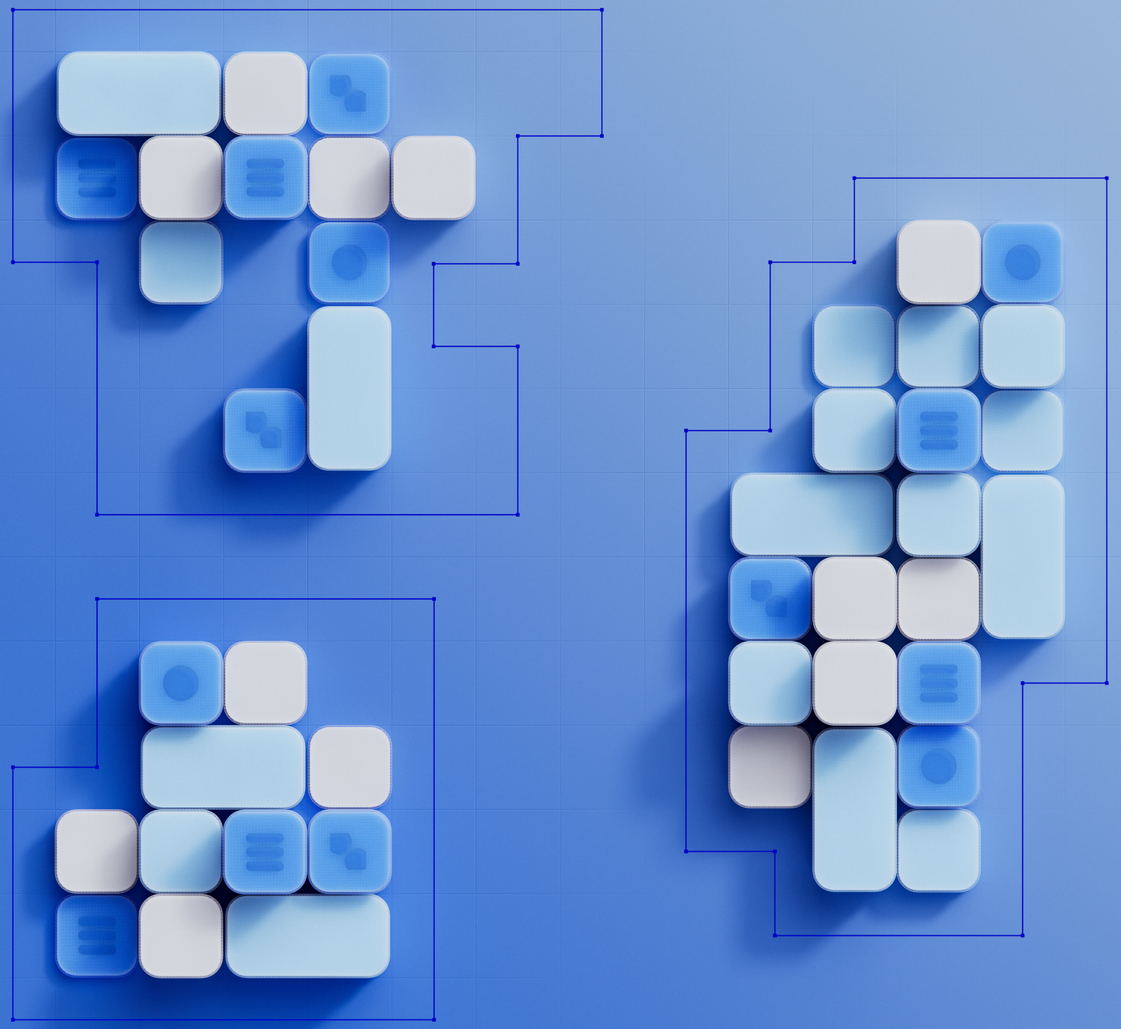
主権の運用化

ITリーダー向け、制御コンプライアンス、
独立性を維持しながらAIを拡張
するためのガイド

内容

第01章

主権の確保はもはや選択肢ではありません



長年にわたり、デジタル主権は企業戦略の周辺的な課題と見なされてきました。主にコンプライアンス・レビューや地域データ・ポリシー、契約条項の範囲内に限られていました。重要ではあるものの、緊急性はほとんどありませんでした。

その状況は一変しました。

今日、主権は現代の企業がテクノロジーを設計、運用、管理する方法の中心に位置づけられています。もはやデータがどこに存在するかではなく、システムに対する運用権限を誰が握っているのかーそしてシステムやAIがリアルタイムで動作する中でその権限を実証できるかどうかが問われています。

CIO（最高情報責任者）やCTO（最高技術責任者）にとって、この変化は無視できないものとなっています。皆さんは、規制・セキュリティ・地政学的な複雑性が高まる中でも、迅速なイノベーションを実現しなければならないプラットフォームを担っています。現在、アーキテクチャに関する決定は、リスクへの露出、コンプライアンス体制、長期的な柔軟性にまで影響を及ぼすようになっています。

AIの台頭
→ 高まるリスク

モデルが本番環境に移行するにつれて、組織は結果だけでなく、その結果がどのように生み出されたのかによって評価されるようになります。規制当局、監査機関、取締役会、そして顧客は、後から数週間かけて説明を組み立てるのではなく、意思決定が行われたその時点での透明性と説明責任をますます求めるようになっています。AIが直接的な承認の及ばない形で動作すると、ランタイムでの挙動と、証明可能な制御との間に生じるギャップが深刻な弱点となります。

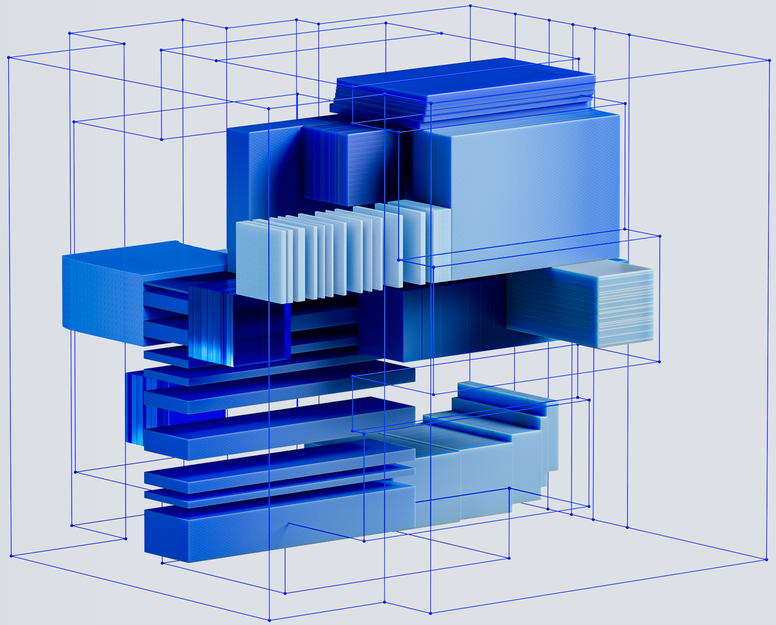
しかし、デジタル主権はもはや単なる法令遵守の問題ではなく、取締役会レベルの問題となっています。デジタル主権はテクノロジー戦略を形成し、AIのスケール方法、インフラストラクチャのモダナイズの進め方、絶えず変化する環境の中で独立して運用する自由をどう確保するかにまで影響を及ぼします。

CIOとCTOには、制御を維持しながら成長を実現し、権限を犠牲にすることなくスピードを確保し、テクノロジーにとどまらない意思決定を支える役割が求められています。主権は、政策文書、契約書、各種保証などの書類上に記載されているだけの政策であってはならないのです。実際に機能させるためには、運用可能にする必要があります。主権は、プラットフォームの運用、AIのガバナンス、ーそしてシステムが稼働する中で、証拠を継続的かつ自動的に透明性をもってー生成する仕組みにまで組み込まれていなければなりません。

次の章では、主権がテクノロジー・リーダーにもたらす課題、彼らが日々直面するトレードオフ、イノベーションを遅らせることなく主権を実現するための実践的な方法について説明します。主権がいかにして信頼できる進歩の基盤となり、ーその足かせにはならないことを示します。

第02章

現代の要件が
レガシー設計を
上回る理由



多くのCIOやCTOにとって、デジタル主権は解決すべき単独の問題として扱われるものではありません。その代わりに、テクノロジー、オペレーション、チーム、期間全体を通じて相互に関連した一連の意思決定という形で現れますーこれらの意思決定は、概念的に説明するのは簡単ですが、既存のシステムや運用モデルの制約内で管理するのは困難です。

イノベーションが加速し、制御に対する期待も高まる中、こうしたトレードオフを乗り越えるのはますます困難になっています。ビジネスリーダーは、AI駆動型の洞察やオートメーションに期待しています。チームは、最新のクラウド・プラットフォームに関連する柔軟性を求めています。同時に、テクノロジー・リーダーは、システムがどのように動作するのか、誰がシステムを管理するのか、そしてどのような権限の下で意思決定が行われるのかについて説明することを、ますます求められています。

その結果、意図の問題というよりもアーキテクチャーの問題として微妙なバランス調整が必要になるのです。多くの環境は主権を第一原則として設計されていないため、制御メカニズムは後付けでプラットフォームに重ね合わされています。複数のプロバイダーが所有したり、運営したりするシステムから証拠が集約されます。疑問が生じると、チームは事態の展開に合わせて状況を制御していることを示すのではなくアクティビティの経緯を再構築することに追われます。ガバナンスは、継続的にレビューされるのではなく、定期的に見直すだけのものになってしまいます。

ベンダーへの依存は、この状況をさらに複雑にします。組織の管轄外にあるテクノロジーへの依存や集中型の制御プレーンは、説明責任が組織内にある場合でも、可視性を限定的なものにし、運用上の権限を制限する可能性があります。時間の経過とともに、これらの依存関係は、微妙ながらも重要な形でアーキテクチャー上の意思決定に影響を与え、柔軟性を低下させ、運用上の摩擦を増加させ、将来の選択肢を狭めることになりかねません。

柔軟性
→ 必要なときに

AIモデルが本番環境へ移行すると、ガバナンスはデプロイや設定の段階で終わるものではなくなります。リーダーは、推論がどこで行われるのか、アクセスがどのように制御されるのかそしてシステムが稼働している最中に、数週間後ではなく、どのように意思決定を検証できるのかについて確信を持つ必要があります。既存のプラットフォームの多くは、推論が行われる場所やアクセスを制御する能力を持たずまた、そのレベルのランタイムの透明性を提供するようには設計されていません。

これは、現代の要求とレガシー設計の前提との間の不一致を反映しています。第一世代の主権ソリューションは、データの場所と境界の制御を重視するものでした。これらは、ワークロードが静的で監視が定期的である場合には機能していました。意思決定が動的に行われ、システム稼働中に証拠が求められるようになるとこうした仕組みは十分に機能しなくなります。

主権が組み込み機能ではなくオーバーレイとして扱われると、運用やコンプライアンスからイノベーションのペースに至るまで、他のあらゆる場所に複雑さが現れます。その構造的なギャップこそが主権が繰り返し起こる制約を超えて動き自信、レジリエンス、前進の源となることを可能にするのです。

その構造的なギャップこそが
主権が繰り返し起こる制約を超えて
動き自信、レジリエンス、前進の源
となることを可能にするのです。

第03章

主権を経営判断として捉える

既存モデルの限界が明らかになると、問題は、いかに意図的にその限界にアプローチするかということになります。

CIOやCTOにとって、主権がテクノロジーの選択やコンプライアンス対応の一部として捉えられてしまうため、取り組みが前に進まなくなることがよくあります。実際には、これは、システム、データ、AIが稼働する際に―権限がどのように確立され、行使され、証明されるかという―制御に関するリーダーシップ上の決定です。

主権への取り組みは、権限の所在を明確にすることから始まります。その環境を運営しているのは誰でしょうか。アクセス許可と変更を管理するのは誰なのでしょうか。プラットフォームやAIシステムが稼働している間つまり―設定時だけでなく、実際に運用されている間も、コンプライアンスはどのように徹底されるのでしょうか。

これらの問いに対する共通の答えがなければ、主権を実装することは依然として難しいままです。

意思決定の構造化

IBM®は、CIOとCTOが主導しセキュリティ、コンプライアンス、リスク、オペレーションが早期に関与する部門横断的でリスクに沿ったプロセスとして主権に取り組むことを推奨しています。

このアプローチでは、主権を単一の調達イベントとして捉えるのではなく、イノベーション、制御、長期的な柔軟性のバランスを取る一連の意思決定として捉えます。実際には、このプロセスは3つの段階に分けることができます。

01

制御とリスク要件を定義する
この段階では、組織にとって主権が具体的に何を意味するのかを明確にします。リーダーたちは、管轄区域の境界、規制上の義務、運用権限、AIガバナンスに関する期待事項について合意しました。重要なのはツールではなく、結果です。つまり、何を自分の管理下に置くべきか、そしてなぜそうすべきかということです。

02

アーキテクチャーが証明可能な制御を提供できることを検証する。
要件が明確になった今、問題は、プラットフォームが設計段階から主権を強制するかどうかということになります。評価すべき最も重要な側面は、制御プレーンがどのように動作するか、データとAIワークロードがどこで実行されるか、ランタイムにガバナンスがどのように適用されるか証拠がどのように生成されるかです。目標は主権を後から証明するのではなく—継続的に行使し検証できるかを確認することです。

03

集中的なデプロイメントを通じてリスクを軽減する。
主権は、すべてを一度に再建することを要求するものではありません。対象を絞ったフェーズに進むことで、チームは想定を検証し、利害関係者と調整し、より広範囲に拡張する前に、自信を築くことができます。

リスクと監視が最も厳しい分野、つまり規制対象のワークロード、機密性の高いデータ領域、本番環境に移行するAIシステムから着手することで、大きな進歩を遂げることができます。

初期の取り組みは、明確な主権境界の確立ガバナンスと証拠生成の自動化日常業務のワークフローへの制御の組み込みに焦点を当てています。時間が経つにつれてこれらのパターンは再現可能になります。

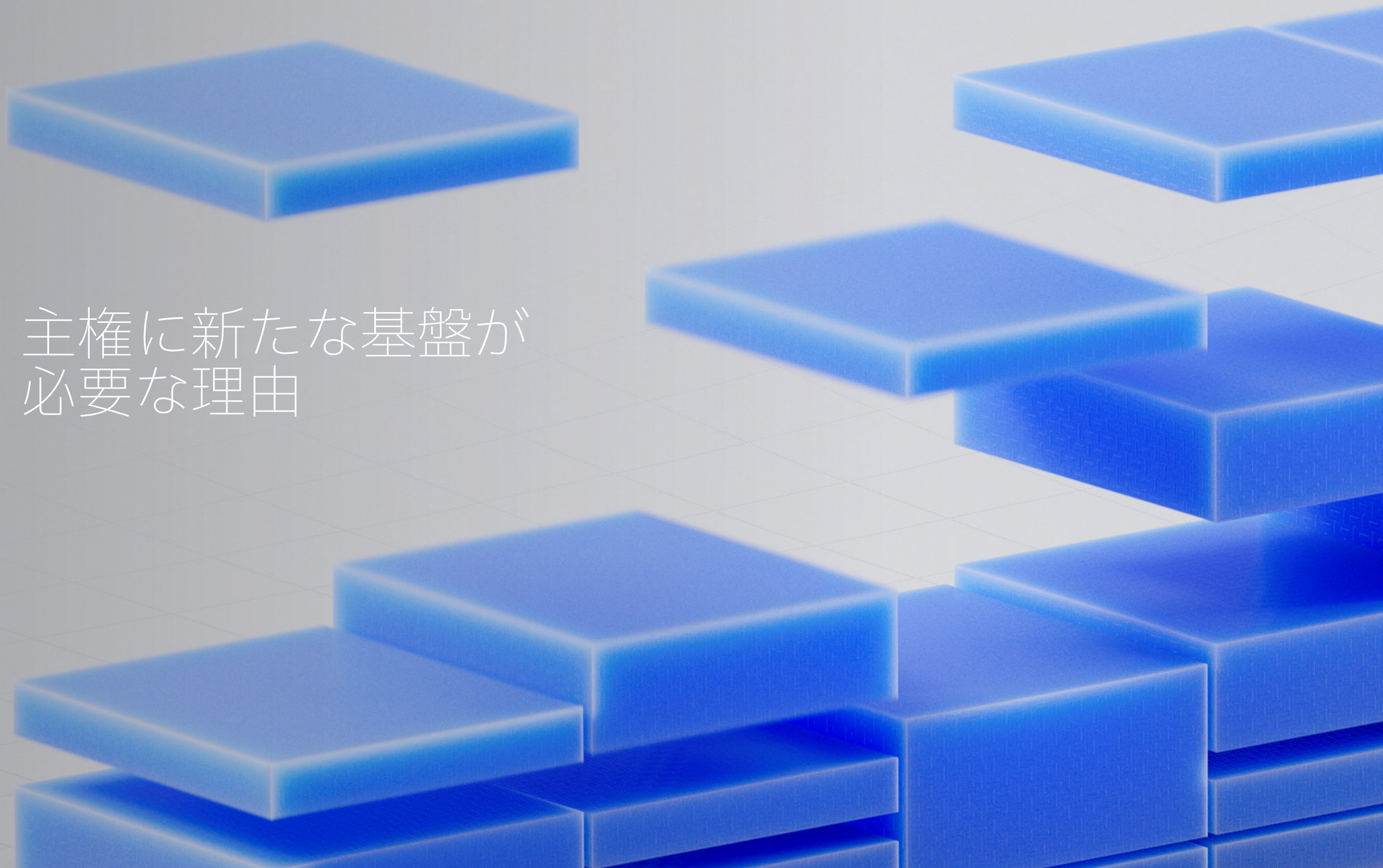
デジタル主権ソリューションにおいて評価すべき主要な機能：

主権を大規模に行使し、証明し、維持する必要があるとすれば、それを現実の環境で可能にする基盤とはどのようなものなのでしょうか。

- → **運用制御：**
  外部の制御プレーンやプロバイダーに依存することなく、環境全体を実行および管理できますか。
- → **境界内での保証：**
  データ、ID、鍵、ログAI推論は、あらゆる状況下で完全に管轄区域内に留まるのでしょうか。
- → **継続的なコンプライアンスと証拠：**
  手作業を必要とせずにリアルタイムで監査に対応するコンプライアンスの証拠を生成できますか。
- → **ランタイムのAIガバナンス：**
  AIモデルがどこで実行されるか誰がアクセスするか、決定がどのように記録され、監査されるかを制御できますか。

第04章

主権に新たな基盤が必要な理由



主権には、権限を明確にし、ガバナンスを強制力のあるものにし、遵守の証拠を継続的に示す運用モデルが必要です。多くの組織はその必要性を理解しているものの、依然として主権を本来の運用能力ではなく、単なる上乗せ機能として扱うプラットフォームに頼っているのが現状です。

第一世代の主権ソリューションは、プロバイダーによる中央集権的な制御プレーン、契約上の保証、手作業のプロセスに依存してコンプライアンスを示しています。彼らはデータの所在に重点を置いてはいるものの、運用制御は別の場所に残されたままです。この種のソリューションは初期の期待には応えられても、AIが本番運用へ移行し、システムのリアルタイム動作に注目が集まる段階になると、対応しきれなくなっていきます。

IBMは、主権はプラットフォームそのものに組み込まれるべきだと考えています。後からオーバーレイや契約で追加するのではなく、アーキテクチャーに組み込むことでシステムの稼働中に制御、ガバナンス、コンプライアンスが自動的に発揮されるようにする必要があります。これが、IBM Sovereign Coreの基盤となるものです。

Sovereign Coreは、シンプルながらも厳しい基準に基づいて設計されています。それは、組織が自らの権限の下でクラウドおよびAI環境を運用し、その権限を継続的に証明できなければならないというものです。制御は境界の外には存在しません。ガバナンスはデプロイメント後も継続します。疑問が生じたからといって、証拠が再構築されるわけではありません。これは、通常の操作の一部として自動的に生成されます。


前進
→ 制御と共に

このアプローチが重要なのは、AIがリスクの本質そのものを変えるからです。モデルがランタイムにトレーニング、推論、意思決定を行う場合、主権もその場面まで拡張されている必要があります。リーダーは、データがどこに保存されているかだけでなく、AIの振る舞いを誰が管理しているのか、アクセス権限がどのように執行されているのか、そして決定事項を即座に確実に監査できるのかどうかについても、確信を持つ必要があります。IBM Sovereign Coreは、AIガバナンスを後付けの考えではなく、ファーストクラスのランタイム機能にします。

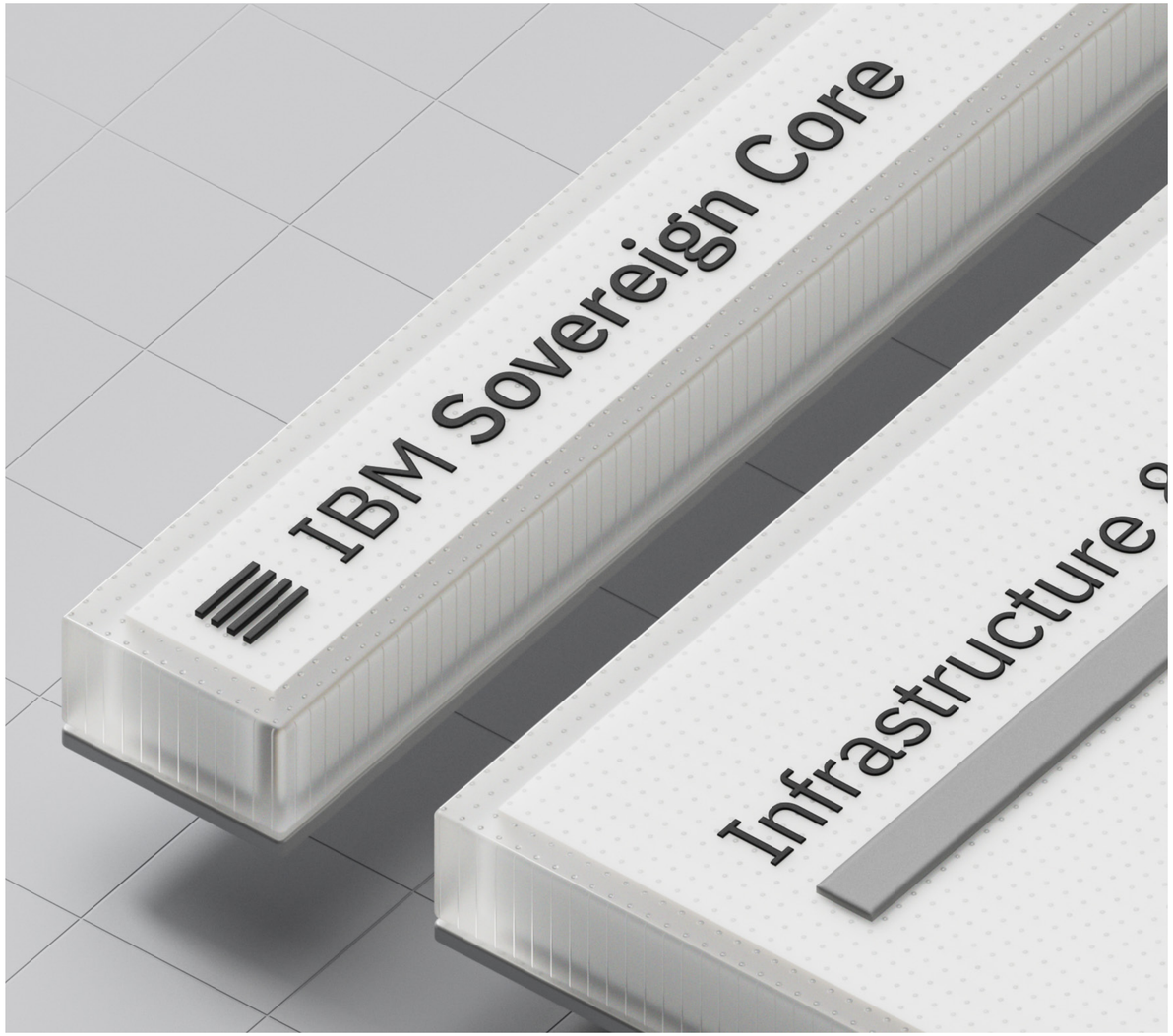
同様に重要なのは、独立性です。単一のプロバイダーの制御プレーンやインフラストラクチャー、または独自のアーキテクチャーに依存する主権は、長期的に選択肢を狭めてしまいます。IBM Sovereign Coreは、環境を問わず柔軟性を維持できる、オープンで移植性の高い基盤の上に構築されています。このオープン性により、組織は制御を手放したり容易に覆せない決定に縛られたりすることなく、モダナイズし、拡張し、適応できます。

その成果として、異なる運用体制が生まれます。ITチームは、面倒な保守作業に費やす時間を減らし、戦略的な目標により多くの時間を費やすことができます。コンプライアンスは、断続的なものではなく継続的なものへ事後対応型ではなくリアルタイム型へと変わります。イノベーションは隠れた制約が減ることで、前進しやすくなります。権限、責任証拠が一致することで、リーダーシップはより明になります。

行動を起こす必要性が高まっているのは、AIの導入が加速しているという、技術融合の進展によるものです。規制当局の期待が高まっています。地政学的リスクやベンダーリスクは、無視することがますます難しくなっています。これらの要因が複合的に作用することで、何もしないことのリスクは、変化を起こすリスクよりも高くなります。

主権が適切に機能すればリスクを軽減する以上の効果を発揮します。それにより、信頼されるイノベーションを拡張するための条件が整えられます。IBM Sovereign Coreは、組織が最も重要な局面で、自信、制御と確かな根拠を持って前進できるよう支援します。

IBM Sovereign Coreは、組織が最も重要な局面で、自信、制御と確かな根拠を持って前進できるよう支援します。



次のステップ

証跡を伴う主権を手に入れる。
IBM Sovereign Coreの実際の動作をご覧ください。
AIはリアルタイムで動作します。
その証明もリアルタイムで行えるべきです。
IBM Sovereign Coreによって主権がランタイムに、常に運用可能になる様子をご覧ください。

デモの予約 →