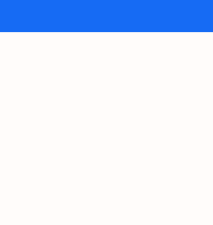


データ主権と Microsoft 365の レジリエンス要件を満たす 実践的なアプローチ

データの機密性が高まり、地政学的な不確実性が増し、デジタルビジネスにおける SaaS (Software as a Service) の定着が進む中で、データ主権を巡る競争が激化している。実現可能なアプローチを見極めることで、主権要件に対応できる。



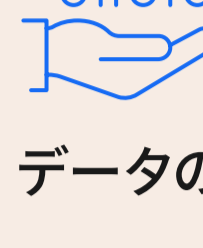
Archana Venkatraman
Senior Research Director,
Cloud Data Management, IDC Europe

必須要件となったデータレジリエンスとデータ主権

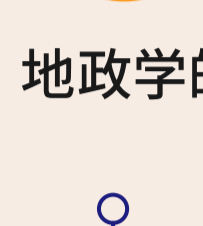
今やコンプライアンス対応におけるデータ主権は必須である。むしろ、デジタルトラストとリスク管理の中核となっている。

データ主権とクラウド環境の変化の可能性は、2026年における最大の懸念事項として挙げられた。

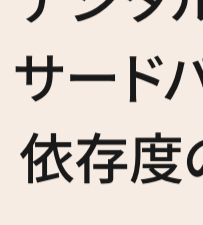
データ主権への関心が高まった理由



データの価値と機密性の高まり



地政学的な不確実性



デジタルビジネスの運営におけるサードパーティプラットフォームへの依存度の高さ

Source: IDC's Future Enterprise Resiliency and Spending Survey, Wave 5, June 2025

クラウド環境全体、特にSaaS環境に広がる主権とレジリエンスのリスクとエクスポージャー

デジタル環境においてSaaSアプリケーションが、IaaS (Infrastructure as a Service) やPaaS (Platform as a Service) を上回る形で主導的な役割を果たしている。その結果、機密性の高い重要なビジネスデータの主要なリポジトリとしての役割は、もはや軽視できないものとなっている。

47%

の企業において、SaaS環境が、ビジネスデータが最も急速に、または2番目に急速に増加している領域である。

53%

のITサポートチーム

42%

のサイバーセキュリティチーム

が、データ損失、誤削除、復旧手段の不足、監査不備が最も懸念されるのが、Microsoft 365環境であると認めている。

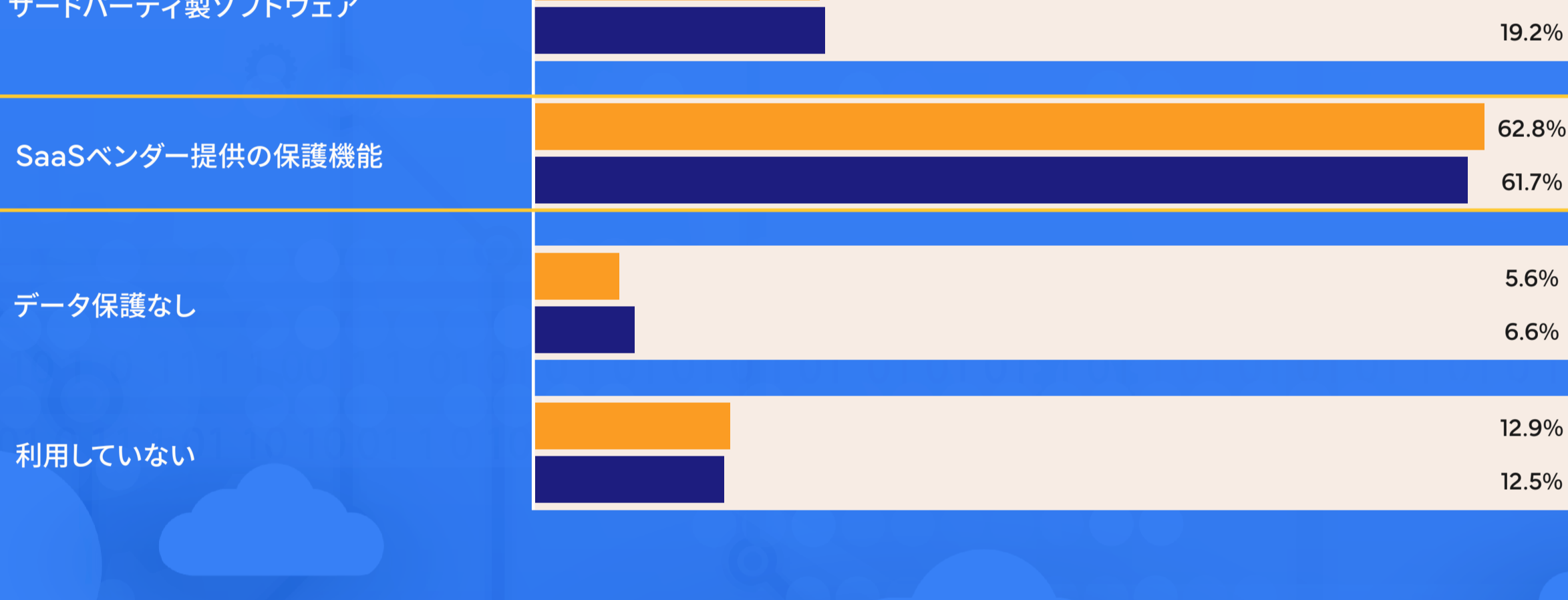
Source: IDC's EMEA Cloud Survey, 2024; IDC's 2024 CloudOps Survey

既成概念からの脱却：データ管理の実践に不可欠なレジリエンス中心のアクション

データ主権は多面的かつ複雑であるため、実践的なレジリエンス中心のアプローチを取る必要があるが、最初の障壁は既成概念である。

10社のうち6社が、依然として、Microsoft 365のネイティブデータ保護のメカニズムに依存している。

回答率 (%) : EMEA 全体



この状況では、デフォルト設定された柔軟性に欠ける限定的なデータ保持機能によってデータ損失や、危機発生時の硬直的なデータ復旧能力といったリスクが生じる。

また、ネイティブ機能への依存度が高いということは、企業が自社データに柔軟にアクセスできないということであり、さらに重要なこととして、ビジネス継続性や主権、コンプライアンスに必要な情報を完全に統制できていないことを意味する。

Source: IDC's Cloud Data Logistics and Protection Survey, August, 2025

データ保護、セキュリティ、レジリエンス技術の価値と、デジタルネイティブと追従者の間で広がる格差

Microsoft 365などのSaaSにおけるデータの急激な増加によって、データ資産のコントロールと戦略的自律性の確保が極めて重要であることが明らかになっている。

87% のデジタルネイティブ企業 (全企業の77%) が、SaaSデータ保護への投資拡大を決定している。

企業は、データ分類とデータ保護を、近い将来に対処すべき「極めて重要」な2つの分野と位置づけている。



しかし、62%の企業が、依然としてMicrosoft 365のネイティブまたはデフォルトのデータ保護機能に依存しており、リスクを大幅に高めている。

セキュリティ、リスク、コンプライアンスは、マクロ経済の不確実性にもかかわらず予算削減の影響を受けずに、2025年以降は「大幅な予算増」が見込まれるテクノロジー領域である。

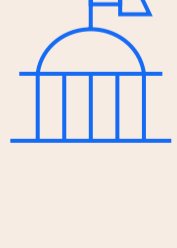
Source: IDC's 2024 CloudOps Survey; IDC's Future of Enterprise Resiliency and Spending Survey, December 2024

データ主権とMicrosoft 365のレジリエンス設計原則

主権的なMicrosoft 365環境は、アーキテクチャ選択と法的枠組みによって構成される。

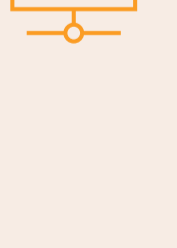
企業は規制上の監督を組み込んだレジリエントな (回復力のある) データ戦略を確立しなければならない。データ分類、役割と責任の文書化、リスクポリシーから始め、プロセスを変革すべきである。

技術的な管理戦略は、以下のデータ主権の3つの柱を網羅する必要がある。



法的管轄権:

バックアップデータのガバナンス、アクセス制御、暗号化に関する明確性を確保する。



データレジデンシー:

バックアップデータの保存場所について選択肢と柔軟性を確保し、データ移動とデータ監査を管理下に置く。メタデータも機密性に配慮して扱う。



運用自律性:

サイバーレジリエンスと規制コンプライアンスに必要な統制を、データの不変性、追跡可能な監査ログ、論理的分離などの機能で検証する。詳細レベルでの復旧、復旧時間の短縮、Microsoft 365環境全体を網羅する保護といったメカニズムを通じて復旧に重点を置くことは、運用上の完全性とビジネス継続性に不可欠である。

Source: IDC Research, 2025

スポンサーメッセージ



Veeamは、データレジリエンス分野における世界No.1のリーダーであり、妥協のないビジネス継続性を提供しています。

世界中に広がるパートナーネットワークを通じ、Veeamはビジネスが行われる場所を問わず、レジリエントなデータ保護とシームレスな復旧を保証します。Veeam Data Cloud for Microsoft 365およびEntra IDは、今日のサイバー脅威やデータ損失事故に立ち向かうべく、業界で最も包括的で最新のSaaSバックアップソリューションを提供します。Exchange、SharePoint、OneDrive、Teams、Entra IDをすべて1つのソリューションで保護しましょう。

詳細はこちら