

Microsoft 365の データ保護における 6つの問題と その解決方法

Microsoft 365を利用しているユーザーは、高可用性と信頼性の高いアプリケーションアクセスを期待しています。マイクロソフトは、自社のクラウドインフラストラクチャを絶え間なく稼働させていることで高い評価を得ていますが、Microsoft 365のデータ保護については責任を負っていません。実際、ユーザーが自社データを保護するためにサードパーティ製バックアップアプリやサービスを独自に導入することを、マイクロソフト自身が積極的に推奨しています。以下はMicrosoftサービス規約からの引用です。「マイクロソフトは、本サービスの稼働状態を維持するよう取り組んでいますが、すべてのオンラインサービスには中断および停止が時折発生します。マイクロソフトは、結果としてお客様に生じる可能性がある中断または損失について一切責任を負いません。停止が発生した場合、お客様は保存している**ご自身のコンテンツまたはデータの取得ができなくなることがあります**。本サービスに保存したお客様の**コンテンツやデータを定期的にバックアップするか、サードパーティのアプリケーションやサービスを使用して保存することをお勧めします。**」

しかし、多くの企業は、マイクロソフトがMicrosoft 365に対して堅牢なデータ保護と長期にわたるデータ保持機能を提供していると考えています。実際には、偶発的なデータ削除やマルウェア攻撃などの一般的で深刻なデータ損失の問題に対する保護はほとんど提供されていません。このような思い違いが、多くの企業でデータ保護の問題を生み出し、不本意な事態へ発展していきます。ITリーダーは、自社のMicrosoft 365データを保護する責任があることを自覚し、データ損失の一般的な原因から保護できる包括的なバックアップソリューションを実装する必要があります。

**すべての企業がMicrosoft 365データについて
考慮すべき6つの重要なデータ保護領域**

1. 偶発的なデータ削除

データリスク：従業員は、日常業務において、Microsoft 365のユーザープロフィール、Exchange Onlineのメールと添付ファイル、OneDrive for Businessのファイル、SharePoint Onlineのコンテンツを定期的に削除しています。このようなデータ削除は、偶発的なものと意図的なものがあり、後で後悔することにもなりますが、いずれの場合も重要なデータが失われる可能性があります。

Microsoft 365の課題：こうした日常的なリソースの削除はネットワーク全体で常に繰り返されています。時間が経過したリソースの場合は、問題がさらに大きくなります。つまり、古いデータは物理的に削除され、復元できなくなる可能性があります。一方、より新しいリソースを最近削除した場合は、削除済みアイテムフォルダへ移動したファイルとメールはゴミ箱や復元可能なアイテムフォルダから短期間で復元可能なため、問題は軽微で済みます。

2. 保持ポリシーの問題

データリスク：Microsoft 365のデータ保持ポリシーの変更や優先順位の不整合によって、データが完全に削除される可能性があります。このリスクは、定期的な見直しと保持ポリシーの更新によって部分的ではあるものの軽減することができます。

Microsoft 365の課題：Microsoft 365を利用する企業ユーザーは、保持ポリシーを管理する責任を負いますが、理由を問わず、既存の保持ポリシーの有効期限切れによって物理的な削除が発生した場合、マイクロソフトは削除されたリソースをリカバリできません。

3. 内部のセキュリティ脅威

データリスク：日常的な操作によって行われる正当な削除とは別に、Microsoft 365データとリソースは、不満を持つ従業員や解雇された従業員、請負業者またはパートナーによる、悪意のあるデータの改ざんや破壊から保護する必要があります。

Microsoft 365の課題：比較的新しいリソースの削除の場合を除いて、マイクロソフトは悪意のある社内関係者によるMicrosoft 365データの破壊や改ざんに対する保護を提供しません。

4. 外部のセキュリティ脅威

データリスク：Microsoft 365は、さまざまなマルウェア脅威、なかでも特にユーザーデータを暗号化し、オンラインで身代金を要求するランサムウェアによる破壊や犯行に対して脆弱です。

Microsoft 365の課題：マイクロソフトは、ランサムウェアのようなマルウェア攻撃に対して非常に限定的な保護しか提供せず、また、マルウェアによって暗号化されたり変更されたりしたファイルを攻撃前の状態に復旧する際にも限定的な機能しか提供しません。

5. オンプレミスのMicrosoft Officeからのマイグレーション

データリスク：従来のオンプレミス向けMicrosoft OfficeアプリケーションスイートからクラウドベースのMicrosoft 365サービスへの移行は、一般的にレガシーなデータ保護ソリューションから新しいクラウド対応のソリューションへの移行を含みます。2つのバックアップソリューションは互換性がない場合が多く、レガシーデータを新環境に復元することができません。

Microsoft 365の課題：マイクロソフトは、OfficeからMicrosoft 365への移行中に発生する可能性のあるデータ損失に対応するソリューションを提供しません。サードパーティのデータ保護ソリューションでも、OfficeとMicrosoft 365向けのバックアップ機能を統合して両方提

供しているものはほとんどありません。

6. 法的およびコンプライアンスの問題

データリスク：コンプライアンス要件および法的な問題は、上述した保護されていないデータの損失によって事業コストを悪化させる可能性があります。復元不可能なMicrosoft 365のデータ損失によって、企業が政府や業界特有の規制罰金、法的罰則、または収益や株価の下落、顧客からの信頼喪失、企業ブランドの失墜などに直面する可能性があります。

Microsoft 365の課題：上述したすべてのデータ損失リスクを考えると、コンプライアンスや法的問題からMicrosoft 365を使用する組織を保護するためにマイクロソフトができることはほとんどありません。例えば、ランサムウェア攻撃を受けた後、EUを本拠地とする顧客の個人データをSharePoint Onlineに保存している企業はそのデータのコピーを取ることができないため、GDPR要件に違反する可能性があります。

Microsoft 365のデータを保護する

Microsoft 365を使って業務を行う場合、信頼性が高く、使いやすいAcronis Cyber Protectでマイクロソフトの基本的なデータ保護を補完する必要があります。高速バックアップ、信頼性の高い復旧時点の選択リカバリ、柔軟性の高いリストアとクラウドストレージオプション、そして、クイック検索機能を備えるAcronis Cyber Protectは、常に進化する脅威ランandscapeにおいて、ビジネスにとって重要なMicrosoft 365データを保護するのに役立ちます。

マイクロソフトは、自社のクラウドインフラに対してはレジリエンスを確保していますが、ユーザーデータを保護するのはお客様自身の責任です。世界中のビジネスリーダーやテクノロジーリーダーは、Microsoft 365のデータを保護し、ビジネスを継続させるためにAcronis Cyber Protectを信頼してご利用頂いています。

**Acronis Cyber Protectを
詳しく知りたい方は、今すぐ30日間の
無償トライアルを始めてください。**

開始

