docomo business

DX+

激増するランサムウェア被害に備えたMicrosoft 365の安全なデータ保護

Theme　Use Case　Reference Architecture

テーマ / Theme

ビジネスを加速させるための取り組みをご紹介

激増するランサムウェア被害に備えたMicrosoft 365の安全なデータ保護

コスト削減　セキュリティ強化　セキュリティ向上

課題 / Issue

ランサムウェア被害でMicrosoft 365のデータがロックされてしまった

月間アクティブユーザー数「3億」(※1)、Microsoft Teamsの日次利用者数「1.45億」(※1)など、まぎれもなくMicrosoft 365は世界的にポピュラーなビジネスツールだ。すでに利用している方も多いのでは。しかし、多くのビジネスパーソンが「クラウド上にデータを置いておけば安心」と思っているかもしれないが、これは大きな誤解だ。確かにMicrosoft 365のデータはSaaS/クラウド上に存在し、Microsoftの標準機能でもバックアップされている。一見、安全に感じるところに"落とし穴"がある。

※1:「Microsoft FY21 Third Quarter Earnings Conference Call, April 27, 2021」より

意外に知られてないことだが、Microsoft 365の最終的なデータ保護や管理責任はMicrosoft側ではなくユーザー側にある。Microsoft 365の約款には「お客様のコンテンツおよび本データは、定期的にバックアップするか、第三者のアプリおよびサービスを使用して保存することをお勧めします」「定期的なバックアップ計画を立てることをお勧めします」としっかり明記されている。つまり、何らかのトラブルでデータが"消えてしまった"際には、Microsoftは一切の責任を負わないと明言しているのである。

Microsoft 365でデータが損失される最大の原因は、悪意のある削除、うっかりミスといった人為的なもので、「25%」(※2)を占めている。退職者のデータが復旧できないなどのケースを含めると、その割合はさらに増えるだろう。ちなみにデータが損失した場合、100%完全に復旧できた割合は「15%」(※2)にとどまっているため、Microsoftではユーザー自身でのバックアップを推奨しているわけだ。しかし、実際にサードパーティのデータ保護ソリューションなどの保護対策を実施している企業は「22%」(※2)に過ぎない。

※2:ESG,「2021 Data Protections Cloud Strategies」より

データ損失のリスクは人為的なミスだけではない。たとえば、昨今、猛威を奮っているランサムウェアをご存じだろうか。これはマルウェアの一種で、感染したコンピュータはユーザーへのシステムへのアクセスをロックする。このロックを解除するためには、マルウェアの作者が要求する身代金を支払うしかない。実際にランサムウェア被害は医療機関にも広がるなど社会的な問題になっており、厚生労働省はサイバー攻撃対策のガイドラインを示している。ネットワークの境界対策やエンドポイントでの防御策を講じて感染を回避する入口対策の実施、感染の検知と対応の事後対策をする体制構築などである。

しかし、これらの対策を講じたとしても、ランサムウェア感染を完全に防ぐことは困難だ。そこで最近では「ランサムウェアに感染した場合でも速やかに復旧できるよう、データの上書きや改ざんを防止したバックアップを取得し、データ暗号化やデータ消失、金銭的な被害を抑える対策を実施する」という考え方が広まりつつある。もはやMicrosoft 365のデータ保護対策は、喫緊の課題といえるだろう。

概要 / Overview

バックアップ環境構築のポイントは安全性とコストの両立

コロナ禍によりテレワークが普及した現在、Microsoft 365を使うネットワーク環境はインターネットが一般的である。あるいはオフィスであっても、Microsoft 365を快適に利用するために社内WANを経由せずダイレクトにインターネットで接続するローカルブレイクアウトを採用するケースも増えている。業務効率で考えればユーザー側がオープンなインターネット接続を利用することは問題ない。しかし、データ保護やバックアップの観点で考える場合、まず重視すべきはセキュリティ対策などの安全性である。

第1のポイントはバックアップサイトまでの安全な通信経路の確保だ。インターネットを経由しないVPNなどのセキュアな閉域網に加え、Microsoft 365をはじめ各種クラウドサービスに安全に接続するインターコネクトサービスを利用すれば、いかなるときにも確実にバックアップサイトにデータを送れるようになる。

第2のポイントはバックアップサイトにおけるストレージサービスの選定である。ここは信頼性に重きを置きつつも、なるべくランニングコストを抑制できる安価なサービスを選ぶべきだろう。さらにランサムウェア対策としてデータ上書き・改ざんを防止するオブジェクトロック機能が実装されていることが望ましい。

最後のポイントはデータ復元のしやすいバックアップツールの導入だ。なるべく、クラウド側の制限に縛られることなく、オンプレミス環境と同等のサービスレベルが実現できるツールを厳選すべきだろう。

ユースケース / Use Case

テーマを実現による業務の変化・メリットをご紹介

Use Case 01 データ保護に重きを置いた運用

自社のポリシーに即して指定した期間中、いかなるユーザーであっても上書き・削除等を不可能にするデータ保護、バックアップ体制を構築。安全に重きを置いた運用を開始した。

Use Case 02 オペレーションを重視した運用

情シス担当など特定の権限を持つユーザーのみ上書き・削除などができるデータ保護、バックアップ体制を構築。ストレージ容量の抑制を視野に入れた運用を開始した。

リファレンスアーキテクチャ / Reference Architecture

テーマを実現するシステム構成をご紹介

アーキテクチャ上のポイント

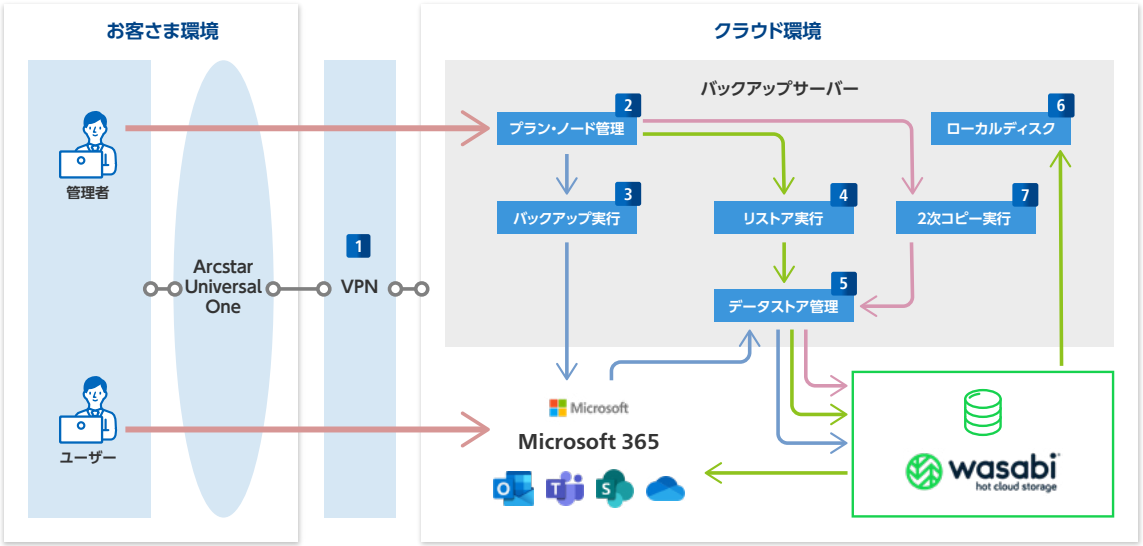
Point

本構成のポイント

- 閉域網から Microsoft 365 に接続するインターコネクトサービスを使ったセキュアな通信経路の確立
- 安価なストレージサービスを使用によるランニングコストの抑制
- データ上書き・改ざんを防止するオブジェクトロック機能を使ったランサムウェア対策の実施
- オンプレミス環境と同等のサービスレベルを実現するバックアップツールの利用

導入効果

- 人為的ミスなどによるデータ削除時に容易に復元が可能
- ランサムウェアによるデータ上書き・改ざんを防止
- バックアップ⇒保存⇒リストアまで一元的な障害対策を実現
- 膨大なデータバックアップコストの抑制



詳しくはこちら ›

docomo business

Smart Data Platform

本件の詳細につきましては、
お気軽にNTTコミュニケーションズにお問い合わせください。

お問い合わせはこちら