Microsoft 365の
サイバー回復性を
実現する10のステップ

目次

Microsoft 365 サイバー攻撃の増加

数多くのビジネスやオペレーションの日常業務にMicrosoft 365スイートのアプリケーションが浸透している現代のサイバーセキュリティ戦略において、Microsoft 365のデータの保護は必須事項となっています。Microsoft 365には、Exchange、Teams、SharePoint、OneDriveなどの幅広い生産性ツールがあり、機密情報や重要なビジネスデータが豊富に格納されています。このため、保護のためにサードパーティのソリューションやマネージドバックアップサービスに投資する組織がこれまで以上に増えています。[1] 実際、ランサムウェアは、Microsoft 365やその他のSaaSアプリケーションに侵入するという特定の目的のために設計されているという証拠があります。Coalitionのレポートによると、2023年上半期には、ランサムウェアによるサイバー攻撃を受けたとする企業の割合は12%増加し、身代金要求額は平均で162万米ドルに上りました。[2] 広く使用されている結果、およびより多くの従業員が在宅勤務マシンにMicrosoft 365をインストールして使用するにつれて、このプラットフォームは、この多様なインフラストラクチャを利用する攻撃者に特に悪用されやすくなっています。

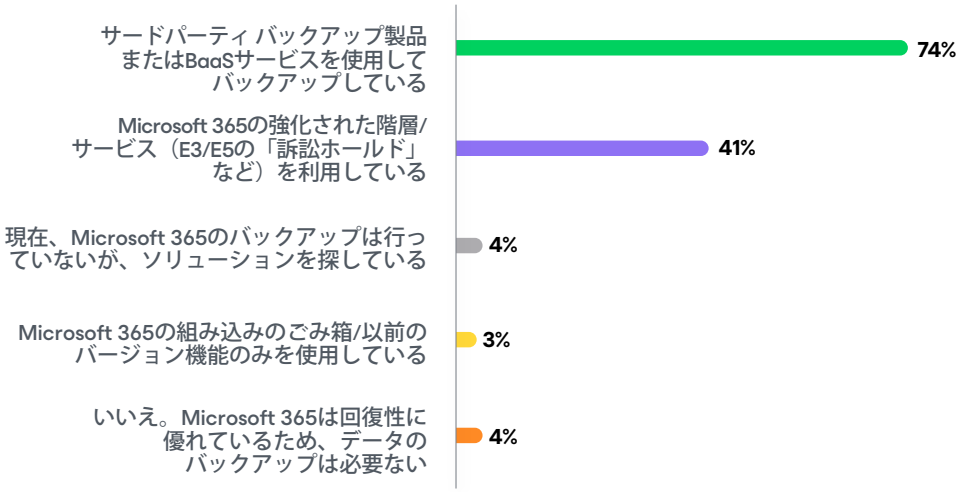
12%

2023年上半期 サイバー保険金請求の増加

162万ドル

要求される身代金（平均）

貴社は、Microsoft 365内のデータをバックアップしていますか？



[1] 2024データ保護トレンドレポート
[2] Microsoft 365ランサムウェア：理解、予防、および復元のための包括的ガイド

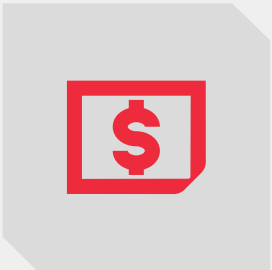
したがって、Microsoft 365データの消失に伴うリスクは、複雑であるだけでなく、非常に現実的です。データ消失は重大な運用中断をもたらし、ダウンタイムや生産性の損失により重大な経済的損害を与える可能性があります。あるレポートでは、ITリーダーはダウンタイムのコストを1分あたり1,467ドル（1時間あたり88,000ドル）[3] と見積もっています。この金額は、日々の業務でMicrosoft 365の使用に費やされる膨大な時間と作業量を踏まえれば、驚くにあたりません。さらに、機密データが漏洩すると、組織は多額のコンプライアンスペナルティや風評被害を受けることになり、GDPR侵害ともなれば、最高で2,100万ドルもの罰金が科せられます[4]。Microsoft 365のデータは組織とその従業員にとって非常に機密性が高いことを踏まえると、データ消失イベントが発生した場合、顧客の信頼だけでなく、従業員の信頼も失われ、社内外での業績悪化や長期的な評判の損失につながる可能性さえあります。

保護されていないMicrosoft 365データに関して起こりうる結果は、いくら強調してもし過ぎることはありません。侵害により個人情報が漏洩すると、個人情報の盗難や詐欺につながるため、当初の侵害から長い時間が経過してから実害が発生する可能性があります。企業にとって、知的財産の損失は競争上の優位性を損なう可能性があり、費用のかかる法廷闘争や罰金につながる可能性があり、顧客のデータの保護を怠ったことが判明した場合、訴訟に直面する可能性もあります。

それを回避する方法はありません。Microsoft 365データを保護するためのプロアクティブな対策は、革新的なアイデアであるだけでなく、企業が継続性の維持、法的および規制上の責任の遵守、顧客の信頼の維持を実現する上で不可欠です。

[3] 2022年版 データ保護トレンドレポート
[4] GDPRの罰金額とは？

データ消失に関連するコスト



ダウンタイムのコストは1分あたり1,467ドル（1時間あたり88,000ドル）

GDPR違反の場合、最高で2,100万ドルの罰金が科せられます。

個人情報を公開する侵害は、個人情報の盗難や詐欺を引き起こす可能性があります。

攻撃に備えるための手順

1. マルチファクター認証

マルチファクター認証（MFA）は、メールアカウント、ビジネスアプリケーション、オンラインサービスなどのデジタルリソースにアクセスするために、ユーザーが2つ以上の検証要素を提供する必要がある重要なセキュリティ手段です。MFAは単なるパスワードにとどまらず、保護層を追加することでセキュリティを大幅に強化します。つまり、サイバー犯罪者がユーザーのパスワードを入手できたとしても、アカウントにアクセスするには、追加の認証要素による認証も受ける必要があります。これは、不正侵入に対する手ごわい障壁に他なりません。

MFAには数多くのメリットがありますが、機密性の高いデータや社内コミュニケーションが常に存在するMicrosoft 365環境において、その有効性は特に顕著です。MFAは、攻撃者がユーザーをだましてログイン情報を開示させるフィッシングなどの一般的なサイバー攻撃からユーザーを防御できます。この追加の認証手順では、ユーザーに既知の情報（PINや秘密の質問など）またはユーザーが所持しているもの（スマートフォンや会社のハードウェアなど）を用いることができます。

脆弱なパスワードや再利用されたパスワードが原因でパスワードが侵害された場合も、MFAの設定により、アカウントは不正アクセスから引き続き保護されます。このレベルのセキュリティは、リモートアクセスが日常的であり、ユーザーがセキュリティで保護されていないネットワークや個人用デバイスから接続している可能性があるMicrosoft 365環境では重要です。全体として、MFAは進化する脅威の状況に適応する、動的な防御メカニズムを生み出すというのは明確な事実であり、それがユーザーに安心感をもたらします。

MFAのメリット

一般的なサイバー攻撃を防御

不正アクセスからアカウントを継続的に保護

脅威の状況に適応する動的な防御メカニズムを構築

2. 最小権限アクセス

最小権限の原則は、効果的なサイバーセキュリティ実践の基礎であり、ゼロトラストアーキテクチャの概念と密接に関連しており、潜在的なサイバー攻撃から組織の防御を強化するのに役立ちます。ゼロトラストアーキテクチャは、ネットワークの内外に脅威が存在することを前提に運用され、ユーザーやシステムが自動的に信頼されることはありません[5] これは、ユーザーには職務を遂行するために必要な最低限のアクセス（または権限）を付与し、それ以上は付与しないという最小権限の原則に合致しています。Microsoft 365の場合、これらの原則を実装するということは、組織内のユーザーの役割に基づいて、特定のドキュメント、フォルダー、サイト、管理設定、およびアプリケーションへのアクセスを制限することを意味する場合があります。

最小権限アクセスモデルを採用することで、Microsoft 365環境のセキュリティ体制を大幅に強化できます。まず、Microsoft 365スイートにおける、サイバー犯罪者の潜在的な攻撃対象領域を最小限に抑えることができます。ユーザーのアカウントが侵害されると、攻撃者のアクセス権限はそのアカウントに制限されますが、このアクセス権限は、可能な限り抑制的であるのが理想的です。たとえば、ユーザーのログイン情報が盗まれた場合、それらの権限がユーザーのアカウントに関連付けられていない場合、攻撃者は機密情報にアクセスしたり、管理タスクを実行したりすることはできません。この被害の限定は、あらゆるセキュリティ侵害に対する隔離ゾーンを作成し、組織内での攻撃拡散を制御する中心的な役割を果たします。

[5] https://www.veeam.com/news/new-zero-trust-data-resilience-model-introduced-by-it-security-and-data-protection-experts.html

3. 定期的なバックアップ

サイバー犯罪者にとって主要なターゲットであるバックアップは、特にMicrosoftの責任共有モデル[6]を考慮した場合、Microsoft 365にとって極めて重要です。同モデルでは、組織が自身のデータの安全性について責任を追うことが言明されています。ランサムウェアは、攻撃者が組織のファイルを暗号化し、それらを解放するために支払いを要求することを目的としているため、データの整合性に重大な脅威をもたらします。とはいえ、データに対する脅威は悪意のある攻撃だけにとどまりません。データは、意図せぬ削除やその他のさまざまな事故によっても危険にさらされる可能性があります。バックアップを最新の状態に保つことで、消失の原因がランサムウェアや人的エラー、あるいはMicrosoft 365のバックアップを管理する、その他多くの重要な理由のいずれであっても、迅速にデータへのアクセスを取り戻すことができます[7]。このことは、ダウンタイムを最小限に抑えるだけでなく、組織が将来の攻撃の簡単な標的ではないという強いメッセージを送ることにもなります。

定期的なバックアップ・ルーチンを導入するということは、処理するデータの量と、バックアップ操作に利用可能なリソースとのバランスが取れたスケジュールを設定することを意味します。これには、メール、ドキュメント、連絡先、カレンダー、およびMicrosoft 365スイートに保存されているその他のデータのバックアップが含まれます。

保険のようなものだと考えてください。毎日必要ではないかもしれませんが、災害が発生すると、迅速な復元と致命的な大惨事の違いになる可能性があります。

[6] クラウドにおける責任共有
[7] Microsoft 365バックアップが重要である7つの理由

4. イミュータブルバックアップ

不変性は、サイバー脅威や人為的ミスによる改ざんや削除から組織のデジタル資産を保護する上で極めて重要な役割を果たします。大量のデータが日常的に生成、共有、保存されているMicrosoft 365の場合、バックアップのコピーを変更不可にすることは、堅牢な脅威軽減戦略の重要な要素です。イミュータビリティとは、一度バックアップされた情報が元の状態で維持され、一定期間変更できないことを保証します。

Microsoft 365を使用している組織にとって、書き換え不能なバックアップは、稼働中の運用データだけでなくバックアップ リポジトリも標的とするランサムウェア攻撃を防ぐ盾になります。事実、ある調査によると、ランサムウェア攻撃のほぼすべて（93%）はバックアップを標的としています。[8] さらなるセキュリティ対策として重要となるのが、データのイミュータブルバックアップコピーです。バックアップデータを上書きや改ざんから保護する保持ポリシーを作成し適用することで、企業は、データの不要な暗号化や破壊からビジネスの継続性を保護できます。イミュータビリティにより、現在のデータストアにセキュリティ違反が発生しても、クリーンな未変更のバックアップから運用をリストアできます。

93%

ランサムウェア攻撃は特にバックアップを標的としています。

[8] 2023ランサムウェアトレンドレポート

5. インシデント対応計画

インシデント対応計画では、適切に構造化された計画を策定します。さまざまなサイバーセキュリティインシデントに直面したときに組織が従う必要のあるプロセスを詳しく説明し、セキュリティの脅威を特定、封じ込め、根絶、および回復するためのプレイブックとして機能し、すべての利害関係者が情報を得て行動する準備が整っていることを確認します。

Microsoft 365を使用している組織にとって、強力なインシデント対応計画の基盤には、Microsoft 365エコシステム内の重要な資産の特定が含まれます。これは、機密データが保存されている場所を、OneDrive、SharePoint、Exchange Online、またはその他の場所のいずれであっても特定することを意味します。これらの資産が特定されたら、計画では潜在的な脅威を定義し、リスクの優先順位付きリストとそれらを軽減するための戦略を作成する必要があります。これには、統合化 監視および検出ツールの使用、即時封じ込め戦略、脅威の根絶、当事者間の堅牢なコミュニケーション、損失または侵害されたデータの識別と復元が含まれます。

インシデント対応計画は、入念な準備によって、より確固としたものになります。このことは、テクニカルツール、トレーニング、ITチームとセキュリティチームのコラボレーションにとどまらず、すべての従業員に関連しています。Microsoft 365を使用している組織は、その複雑なエコシステムに合わせた定期的な教育セッションを実施する必要があります。OutlookやTeamsなど、Microsoft 365内のアプリケーションを使用する従業員は、疑わしい活動を識別し、対応するための知識を備えておく必要があります。そうした活動は、悪意を感じさせないメッセージ、同僚からの偽の会議招待状、または会社のリーダーが差出人になっている本物そっくりの電子メールの形態を取る可能性があります。人間はどの組織にとってもサイバーセキュリティの弱点になる可能性がありますが、よく訓練された従業員は、脅威に対して手ごわい障壁を形成する可能性があります。

インシデント対応計画を開始する

- 包括的なインシデント対応フレームワーク
- 重要な資産の特定
- 従業員の準備の重要性

6. 定期的な監査とペネトレーションテスト

定期的な監査とペネトレーションテストは、回復力のあるMicrosoft 365環境を維持するために不可欠なコンポーネントです。実際、Microsoft 365自体も、監査や脅威検知のための組み込みツールを多数提供しており[9]、さまざまなセキュリティ脅威に対する環境を強化するための基盤として機能しています。これらのプラクティスはプロアクティブな手段として機能し、攻撃者が悪用する前に、企業が問題を特定して修正できるようにします。

Microsoft 365エコシステムの監査では、ユーザー権限、データアクセス制御、セキュリティ設定など、さまざまな要素について体系的な審査が行われます。定期的な監査は、複雑な場合もありますが、システム構成がベストプラクティスおよび組織のセキュリティポリシーに沿った状態を維持するのに役立つため、監査の構築および維持を行うのは健全な習慣といえます。Microsoft 365にはさまざまなサービスが含まれているため、こうした監査は脆弱性の見落としを防ぐため、包括的であることと、各サービスをカバーしていることが必須となります。[10]

しばしば「倫理的ハッキング」と呼ばれる侵入テストは、組織がセキュリティ対策の有効性を評価できるようにすることで、定期的な監査を補完します。これには、Microsoft 365インフラストラクチャに対するサイバー攻撃をシミュレートして、実際の攻撃者が悪用できる弱点を特定することが含まれます。該当する組織の場合、侵入テストでは、従業員のフィッシング耐性から、ファイアウォール、脅威検出システム、インシデント対応計画などの技術ツールの回復力まで、Microsoft 365エコシステムのすべてのレイヤーを調査する必要があります。これらのテストから収集された洞察は、トレーニングプログラムとセキュリティ戦略を微調整する際に組織をガイドし、サイバー脅威が必然的に発生した場合により包括的で効果的な防御を開発できるようにします。

[9] Microsoft 365のセキュリティおよびコンプライアンスガイド

[10] Microsoft 365ネイティブセキュリティコンプライアンスおよび監視機能の活用

7. ソフトウェア制限ポリシー

ソフトウェア制限ポリシー（SRP） は、組織が特定のハードウェア上でソフトウェアの実行を識別および制御するために使用できるセキュリティ機能です。Microsoft 365を使用しているエンタープライズ組織にとって、こうした機能の実装は、自社が責任を追う多数のデバイスを保護する重要な防御メカニズムとして機能する可能性があります。Microsoft 365にはさまざまなツールが含まれているため、悪用可能な脅威ベクトルの要因もまたさまざまです。SRPは、システム上で実行可能なソフトウェアと実行できないソフトウェアを指示することで、悪意のある攻撃者の攻撃対象領域を効果的に縮小します。

Microsoft 365環境のSRPの策定においては、必要に応じて脅威ベクトルをホワイトリストおよびブラックリストに登録するなど、信頼できるアプリケーション、スクリプト、およびプロセスのみの実行を許可することが目的となります。SRPは、その効果が最大限に発揮されるよう、最小権限アクセスを念頭に置いて構成すること、そして組織で使用されるソフトウェアの変更を反映するため、定期的に更新することが必要となります。これには、Microsoft 365ツールの更新、新しいソフトウェアの追加、または従来のアプリケーションの廃止が含まれます。

SRPは、マルウェアが一般的なエクスプロイト手法を利用するのを阻止することで、感染の連鎖を断ち切り、隔離ゾーンを維持するのに非常に効果的です。SRPのサイバーセキュリティ戦略への統合は、組織のインフラストラクチャを信頼できないソフトウェアの実行から保護するのに役立つ先進的なアプローチであり、企業が成長し、新しい従業員を採用するに従い、その可能性はますます高まります。

8. 監視とロギング

監視とログ記録は、Microsoft 365環境のセキュリティと整合性を確保するための重要なステップです。システムアクティビティを警戒し、イベントの包括的な記録を維持することで、組織は潜在的なセキュリティインシデントをリアルタイムで検出し、システムの問題を診断し、侵害の範囲を理解し、全体的なセキュリティ態勢を改善できます。

Microsoft 365管理者の場合、対応可能なセキュリティ情報およびイベント管理（SIEM）システムにログをインポートすると、このプロセスが大幅に簡素化されます。たとえば、Azure SentinelはMicrosoftネイティブのSIEMであり、事前に構築されたさまざまなデータコネクタを使用して、組織のログデータをSIEMアプリケーションに直接転送します。次に、このデータを正規化して一貫性のあるデータセットを実現し、組み込みの分析ツールを介して監視します。

効果的な監視は、（ブルートフォース攻撃を示唆する）ログイン試行の失敗から、（望ましくないデータ流出を示唆する）異常なダウンロードパターンまで、セキュリティ脅威を示す可能性のあるさまざまな異常を検出すべく、広範囲にわたって行う必要があります。包括的なロギングも同様に重要であり、監視対象のすべてのアクティビティのドキュメントとして機能します。このようなログは、インシデントの発生前、発生中、発生後など、インシデント全体のイベントを再構築するのに十分な詳細情報をキャプチャする必要があります。このことは、インシデント後のフォレンジック分析で極めて重要となりますが、コンプライアンス監査と時間の経過に伴うセキュリティ対策の改善にも役立ちます。ロギングは、収集されたデータが実用的であり、明確で適切な情報を提供するよう慎重に構成されていて、過剰なデータ収集によって生じる可能性のあるノイズを含まないことが求められます。

時間が経つにつれて、監視とログから収集された洞察は、組織にプロアクティブなポリシー変更とセキュリティ更新の合理化に必要なデータを提供します。

9. データの分離

権限の分離は、組織がセキュリティ インフラストラクチャを強化するために使用する、広く適用可能で効果的な戦略であり、Microsoft 365のようなデータ駆動型サービスを統合する場合に大いに適用可能です。マルチテナント アーキテクチャ、管理境界、条件付きアカウント制限などの戦略は、データとその権限を構造化して、不正アクセスを減らし、セキュリティ侵害による潜在的な損害を制限することに重点を置いています。異なるデータセットを分離し、ネットワークを個別のセグメントに分割することで、組織はセキュリティ侵害の初期リスクを大幅に軽減し、アウトブレイクが発生した場合に効果的に隔離します。

Microsoft 365内で権限分離ポリシーを使用すると、組織は厳格なアクセス規則を維持できます。前のセクションで説明したように、これらのルールで最も理想的なのは、ユーザー、管理者、サービスに、必要なタスクの実行に必要なアクセス許可のみを付与し、それ以上は付与しないことです（たとえば、最小権限とロールベースのアクセス制御（RBAC）など）。

複数の管轄区域で運営している組織や、異なる事業部門を持つ組織の場合、マルチテナント アーキテクチャを介してMicrosoft 365テナントを分離することで、データを分離し、アクセスを制御できます。これは、テナントごとに個別の管理境界を作成することを指します。これにより、環境が独自のデータ、ユーザーアカウント、およびアクセス制御に分離され、セキュリティおよびコンプライアンス要件が個別に満たされ、1つのテナント内で問題があっても、他のテナントの完全性が損なわれなくなります。

これらの管理境界内では、条件付きアクセス ポリシーとアカウント制限によって防御層が追加され、Microsoft 365に直接実装できます。これらのポリシーにより、組織は特定のアカウントに対してコンテキストベースのルールを定義および実装できるため、組織セキュリティルールをアカウントのリスクレベル、地理的な場所、または疑わしいログインやダウンロードなどの動的な不規則性に合わせて最適化できます。

そのため、方法的な分離は、組織階層のすべてのレベルに適用でき、Microsoft 365データやその他のデジタル資産を保護するための堅牢な基盤を提供します。戦略的な区分化は、不正アクセスのリスクを軽減するだけでなく、セキュリティ侵害に対する多層的な保護手段とフォールバックを提供するため、データと権限の分離は、組織がサイバー防御を強化し、事業継続性 / ビジネス継続性を維持して、最終的には自社のMicrosoft 365環境内でサイバー回復性を達成する大きな一歩としての地位を獲得しています。

10. 暗号化

暗号化は、機密情報の保護における主要な防衛線として機能する基本的なセキュリティ手段であり、正しい復号化キーを持つ、許可された当事者のみが元の情報にアクセスできます。また暗号化は、データの使用、移動、または場所に関係なく適用されます。Microsoft 365に関して言えば、暗号化は、企業が通信、ドキュメント、その他のデータを保護するのに役立つセキュリティレイヤーを提供し、それらがクラウドインフラストラクチャ内のどこに存在していても適用されます。

フィッシングメールや感染したWebサイトは、多くの場合、深刻なランサムウェア攻撃の微妙な前兆です。近年、RobbinHoodランサムウェアが、組織に壊滅的打撃を与えることでその悪名を轟かせています。誤ってダウンロードされた感染メールにより、このマルウェアがシステムに取り込まれると、身代金、ダウンタイム、および復元のコストは数百万ドルにも上ります。

Microsoft 365の秘密度ラベルなどの組み込みツールは、ドキュメントや電子メールを自動的に暗号化できる厳格なプロトコルを順守することでこれを防ぐのに役立ち、疑わしい電子メールを信用せず、潜在的に危険な送信者をユーザーに警告することで最初の感染を防ぎます。こうしたラベルは、権限管理ポリシーを使用して構成でき、管理者は、誰がデータにアクセスでき、どのように使用できるかを決定できます。ここで決定されるのは、組織が一元管理するコンテンツの分類および保護レベルであり、IT管理者はデータの取り扱い、共有、および操作を調整できます。こうすることで、善意のあるユーザーは、マルウェアの感染または拡散を（プロセスのワークフローを妨げずに）防止する複数の保護手段を講じることができます。

効果的な暗号化は、最終的にプライバシーと規制コンプライアンスを構築する基盤を形成します。既存のセキュリティポリシーと並行してMicrosoft 365の暗号化 機能を効果的に活用している組織は、そうでない組織よりもはるかに高いサイバー回復性を備えています。強固な暗号化プラクティスは、ランサムウェアやサイバー脅威から貴重なデータを保護する上で極めて重要であり、それによってプライバシーを支え、規制コンプライアンスを確保し、安全なコラボレーションワークスペースをサポートします。

Microsoft 365のサイバー回復性はバックアップから始まる

データマネジメントとセキュリティの将来的な展望を考えると、Microsoft 365のようなSaaSアプリを保護するための好ましい方法として、バックアップas a Service（BaaS）が浮上してきました。BaaSは、組織にデータのバックアップと保存のためのリモートのオンラインシステムを提供する、クラウドベースのアプローチです。BaaSをMicrosoft 365戦略と統合することは、組織の回復性を確保するうえで欠かせない要素である、堅牢でスケーラブルなかつ柔軟なデータ保護ソリューションの必要性に合致します。

バックアップサービスにより、企業はバックアップのニーズを、バックアッププロセスを自動化し、必要なオンプレミスインフラストラクチャの規模を削減して、一流のセキュリティ対策を提供するエンドツーエンドソリューションを提供する、専門のプロバイダーにアウトソーシングしながら、こうしたプロバイダーにデータへの直接的なアクセスと制御を提供します。Microsoft 365ユーザーにとって、BaaSはデータの安全性、運用効率、安心の向上を意味します。

Microsoft 365エコシステムの保護は多面的な取り組みであり、組織は戦略的な予防策と効果的なインシデント対応計画の両方に取り組む必要があります。Microsoft 365サイバー回復性への道のりは継続的な取り組みであり、先進技術の効果的な活用へのコミットメントが求められます。幸いにも、Microsoft 365データに特化して、カスタムソリューションを構築しているバックアップベンダーが存在します。

Veeam Data Cloud *for Microsoft 365*

Veeam Data Cloud *for Microsoft 365*は、モダンなアプローチでMicrosoft 365データの根源的な回復力を実現します。業界をリードするMicrosoft 365バックアップソリューション、Veeam Backup *for Microsoft 365*が、サービスとして提供されるようになりました。

ソフトウェア、バックアップインフラストラクチャ、無制限のストレージをオールインワンのクラウドサービスで利用することで、バックアップ戦略を簡素化し、シンプルでシームレスなエクスペリエンスの中でパワフルな データ保護とセキュリティテクノロジーを活用できます。

Veeam Data Cloud *for Microsoft 365*は、**Microsoft Exchange、SharePoint、OneDrive for Business、Teams**のための包括的データ保護およびデータ復元機能を提供するバックアップサービスであり、Microsoft 365環境を完全に制御できます。

→ Veeam Data Cloud *for Microsoft 365*のデモをリクエストする

With **Veeam Data Cloud *for Microsoft 365***では、次のことが可能です。

- **業界を牽引する信頼性の高いテクノロジー：**拡張可能性を念頭に置いて構築された、10年以上にわたる継続的なイノベーションに基づく最も包括的なデータ保護ソリューションです。
- **先進的でセキュアかつ直感的なプラットフォーム：**最新のWeb UIから、バックアップジョブの作成やリストアの完了、Microsoft 365の分析情報の取得も簡単に行えます。
- **オールインクルーシブサービス：**ソフトウェア、バックアップインフラストラクチャ、無制限のストレージがバンドルされており、継続的な保守もエキスパートが対応します。

あらゆる事態に備え、常に最新の情報を得る

Microsoft 365のサイバー回復性に向けた道のりはここで終わりではありません。まだ始まったばかりです。2024年に理解を深め、戦略を練り上げ、時代を先取りできます。Veeamの広範なリソースコレクションをチェックして、貴社の課題を機会に転換しましょう。

- Microsoft 365のバックアップサービスがもたらす8つのメリット
- 初心者向けのMicrosoft 365バックアップ
- Microsoft 365復元 ベストプラクティス

Veeam Softwareについて

Veeam®は、データ保護およびランサムウェア 復元における#1のグローバルマーケットリーダーであり、あらゆる組織がデータの停止または損失からただ回復するだけでなく、前進するよう支援することを使命としています。Veeamは、データセキュリティ、データ復元、ハイブリッドクラウドのデータの自由を通じて、組織が根源的な回復力を実現します。Veeam Data Platformは単一のソリューションで、クラウド、仮想、物理、SaaS、Kubernetesの各環境に対応し、アプリケーションとデータが常に保護され、利用可能であるという安心感をITリーダーやセキュリティリーダーに提供します。シアトルに本社を置き、30ヶ国以上に事業拠点を構えるVeeamは、世界中で45万社を超える顧客を保護しており、その中にはGlobal 2000の74%の企業も含まれており、事業継続性の確保にVeeamを利用しています。根源的な回復力はVeeamから始まります。詳しくはwww.veeam.com/jpをご覧いただくか、LinkedIn@veeam-softwareおよびX@veeamでVeeamをフォローしてください。