Climb Inc.
Growing to Meet Your Needs

Office 365バックアップが重要な6つの理由

Office 365のデータ保護はなぜ必要なのか

2019年12月

株式会社 クライム

目　次

はじめに

Office 365 のデータは自分で管理できていますか？必要なときに必要なアクセスがありますか？

という質問には即答で、「もちろん！」か、「マイクロソフトが全部やってくれています」と応える人が大半です。

でも、即答せずに、よくよく考えてみたら、確信を持ってそう答えられるでしょうか。

たしかに、Microsoft は大部分をサポートし、顧客にすばらしいサービスを提供しています。しかし、Microsoft が主眼を置くのは、Office 365 のインフラストラクチャの管理と、ユーザーが実際に利用しているときのサポートです。データそのものに関しては、ユーザー側の制御に任せています。ところが、Microsoft がユーザーに代わって、データを完全にバックアップしてくれていると誤解している人が少なくありません。その考え方に捉われていると、気が付いたら誰もデータ管理の責任を取らず、大変な損害を被る危険性があります。

つまり、**ビジネスの重要なデータは、Exchange Online、SharePoint Online、OneDrive において、いつでもアクセスでき、制御できるようにしておかなければなりません。**

本稿では、セキュリティ対策に Office 365 のバックアップを加えておかないことの危険性と、単なる長期データ保存と真のデータ保護の溝を埋める Microsoft Office 365 のバックアップ ソリューションの重要性について解説します。

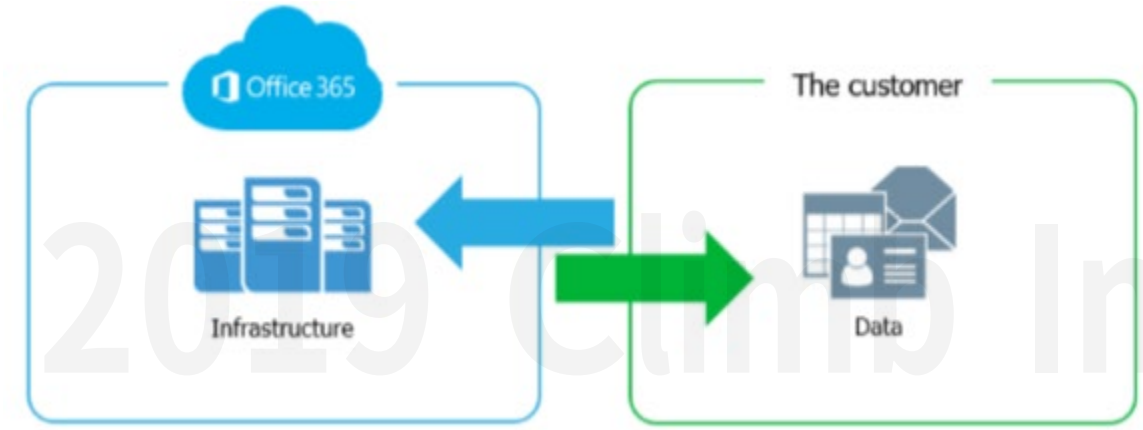
「Office 365 のバックアップとリテンションのポリシーについては懸念していました。Microsoft に我が社のデータを任せながらも、メールの履歴データを保護することが重要でした。それが、Office 365 内のデータに対する適切なバックアップ管理の施行を決めた理由です。」　— Columbia Power & Water Systems 社、IT 責任者カレン・セントクレア氏

Office 365 に関する大きな誤解

Office 365 に関する誤解は、Office 365 データの保護と長期保存に関して、Microsoft が考える責任とユーザーの実際の責任との間の差異に起因します。Microsoft が提供するバックアップとリカバリの機能と、ユーザーが提供を受けていると信じているものが、大きくかけ離れている場合も多々あります。Office 365 が喚起する標準的な注意事項とは別に、自分のデータをどのくらい制御できるのか、実際にどのくらいのアクセスがあるのか、調べ直す必要があります。

Microsoft Office 365 には地理的な冗長性がともないますが、それをバックアップと勘違いしている人が多くいます。バックアップとは、データの履歴コピーが作成され、別の場所に保管されることです。しかし、さらに重要なことは、それに直接アクセスでき、制御できることです。それにより、たとえば、データが失われたり、誤って削除してしまったり、悪意ある攻撃を受けたとき、すぐに復旧可能になります。それに対し、地理的な冗長性とは、データの所在地・施設やハードウェアの不備に対する保護を指します。たとえば、インフラストラクチャの障害や停電などによるサービスの停止が起きた際にユーザーが保護され、多くの場合、障害が起きていることにも気づかずに、そのまま利用し続けられるようにすることです。

Microsoft はインフラストラクチャを管理するが、データは個々の顧客の責任



Office 365 のアップタイム　　Office 365 データの保護と長期保存

「Office 365 で使用するデータはあなたのデータです。あなたが所有し、制御するものです」

— The Office 365 Trust Center

Office 365 バックアップが重要な 6 つの理由

耐性と機能性に優れた SaaS（Software as a Service）プラットフォームとして、Microsoft Office 365 は多くの企業や団体のニーズに合致します。Office 365 はアプリケーションの可用性と安定したアップタイムでユーザーの信頼を確固たるものとしています。しかし、Office 365 にバックアップ ソリューションを組み合わせれば、さまざまなセキュリティの脅威からユーザーをより安全に保護することができます。

社内の一般ユーザーも管理責任者も、「データは完全に消去する前にしばらくごみ箱に保存しておけば十分かな」と考えるかもしれません。そこが間違いの始まりです。データ侵害が生じてから、その事実が発見されるまでの平均期間は 140 日以上 [1]と言われています。驚くべき遅さです。ゴミ箱に放っておいたデータがいつの間にか無くなっていたと気づいたときには、手遅れの可能性が高いのです。

Office 365 へのマイグレーションに携わった世界中の IT 専門家数百名に話を聞いた結果、以下の項目がデータ保護の脆弱性の問題の上位 6 項目として挙げられました。

過失による削除

リテンション ポリシーとバックアップの矛盾

内部のセキュリティ侵害

外部からのセキュリティ侵害

法的／コンプライアンス要件

ハイブリッドのメール設定／Office 365 マイグレーション管理

#1 過失による削除

ユーザーを削除した場合、それが意図的なのか過失に因るのかにかかわらず、その削除はネットワーク全体に適用されます。そのユーザー個人の SharePoint サイトと OneDrive のデータもすべて削除されます。

Office 365 に元から備わっているごみ箱とバージョン履歴によるデータ保護には限界があり、データの紛失からユーザーを完全には守ってくれません。バックアップからの単純なリカバリも、Office 365 の地理的冗長性による保存データが完全消去された後や、リテンション期間を過ぎた後では深刻な問題になります。

Office 365 プラットフォームからのデータ削除には、ソフト削除とハード削除の 2 通りがあります。ソフト削除の例は、メールの「削除済みアイテム」フォルダを空（から）にすることです。これは「永久に削除する」と表現されることもありま

[1] https://discover.office.com/6-steps-to-holistic-security/chapter1/

す。この場合、「永久」とは完全な永久ではなく、削除されたアイテムは「回復可能なアイテム」フォルダ内に見つけることができます。これに対し、ハード削除とは、アイテムがメールボックスのデータベースから完全に削除された状態を指し、この場合、回復することは不可能になります。

#2 リテンション ポリシーとバックアップの矛盾

デジタル時代の目まぐるしいビジネス シーンでは、そのポリシーも継続的に進化していきます。たとえば、データの保持期間を規定するリテンション ポリシーも、その維持管理はもちろん、適正に準拠し続けるのも一筋縄ではいきません。前述のソフト／ハード削除と同様に、Office 365 のバックアップとリテンション ポリシーにも制限があり、特定の状態でのデータ損失のみが保護され、決して包括的なバックアップ ソリューションとは言えません。

たとえば、メールボックス アイテムに対するポイント イン タイムのリストアは Microsoft のサポート対象外です。重大な問題が発生した場合には、バックアップ ソリューションで対処することになります。それにより、問題が生じる前の特定時点（ポイント イン タイム）にロールバックで解決することができます。

Office 365 にバックアップ ソリューションを導入すれば、リテンション ポリシーとバックアップに矛盾が生じることもなく、柔軟なリストアが可能になります。短期間のデータのバックアップや長期間のアーカイブ、より緻密な、あるいはポイント イン タイムのリストアなど、すべて手軽にすばやくリカバリが可能になり、大きな安心が得られます。

#3 内部のセキュリティ侵害

セキュリティの脅威と言えば、すぐにハッカーやウイルスが頭に浮かびます。しかし、企業内部にもセキュリティに対する脅威は存在し、それも意外に頻繁に起こり得る脅威です。意図的か過失に因るものかにかかわらず、会社がその社員によってセキュリティの脅威に晒されることは珍しくありません。

ファイルや連絡リストなどへの社員のアクセス権はしばしば変更されるので、企業がその信用にもとづいて設定した権限に目を光らせ続けることは困難です。たとえば、通常のユーザーと、解雇された直後に会社を去る前に機密データを削除しようとするユーザーの違いなど、Microsoft には知る由もありません。それに加え、悪意がなくても、誤ってウイルス感染したファイルをダウンロードする社員もいれば、信用できると思っていたサイトに大事なユーザー名やパスワードを入力して、フィッシング被害を受ける社員もいるでしょう。

そのほか、社員による証拠隠滅という状況も考えられます。何らかの不正を働き、その証拠となるメールやファイルを計画的に削除して、人事や法務、コンプライアンス担当者の目をごまかし、会社に損害を与える可能性もあります。

#4 外部からのセキュリティ侵害

ランサムウェアをはじめ、マルウェアやウイルスは世界中で企業に深刻な被害を及ぼしています。会社の名誉が傷つけられるばかりか、会社内部および顧客データのセキュリティとプライバシーが脅かされています。

外部からの脅威はメールや添付ファイルを通じて社内に侵入します。どんなに社内ユーザーに注意を喚起しても、感染メッセージの巧みさもあって、社内への侵入を完全にブロックするのが非常に難しくなっています。Exchange Online の限られたバックアップ／リカバリ機能では、外部からの攻撃に対処するのに不十分です。定期的なバックアップにより、感染していないデータのコピーを隔離して保管し、いつでもリカバリ可能にしておくことが大切です。

#5 法的／コンプライアンス要件

法的な措置においては、メールやファイル、その他のタイプのデータを予定外に突然、取り出さなければならないときがあります。世の中には、絶対に起きないと思っていたことが起こることもあります。Microsoft は、訴訟ホールドなど、ある程度のセーフティーネットを用意していますが、これもまた、会社を法的なトラブルから完全に守り切るほどの十分なバックアップ ソリューションではありません。たとえば、ユーザーを誤って削除すると、訴訟ホールドされるべきメールボックスや SharePoint サイト、OneDrive アカウントもすべて削除されてしまいます。

法的要件、コンプライアンス要件、データアクセスに関する規制は業種や国によって異なりますが、罰金、罰則、訴訟の 3 項目を予定に入れたくないことに違いはないはずです。

#6 ハイブリッドのメール設定／マイグレーション管理

Office 365 を導入する企業は通常、オンプレミスの Exchange から Office 365 の Exchange Online への移行を完了するための時間的な幅を設けているはずです。オンプレミスにおける従来のシステムを一部だけ残すことによって、柔軟性とより直接的な管理を保持しようする企業もあります。このようなハイブリッドのメール デプロイメントは決して珍しくなく、セキュリティ管理を複雑化させています。

Office 365 の適切なバックアップ ソリューションを用いれば、ハイブリッドのメール デプロイメントにも対処でき、オンプレミスかクラウドかにかかわらず、Exchange のデータを同じように扱うことができます。

まとめ

上記の内容を踏まえ、自社環境の Office 365 を見直してみてください。今まで気づかなかったセキュリティの盲点が潜んでいないでしょうか。

Microsoft Office 365 を取り入れただけでも、ビジネス上の賢い決定を下したと言えますが、せっかくなら適切なバックアップで、Office 365 をより安全に運用しましょう。バックアップ ソリューションにより、Office 365 のデータへのアクセスとその制御が完全掌握でき、データを失うリスクが回避できます。

©株式会社クライム

〒103-0014 東京都中央区日本橋蛎殻町 1-36-7 蛎殻町千葉ビル 4F

www.climb.co.jp Email: soft@climb.co.jp TEL:03-3660-9336 / 06-6147-8201