バックアップを取得していますか？

はじめに

コンピュータやモバイルデバイスを一定期間使用していると、遅かれ早かれ誤ってファイルを削除してしまう、ハードウェア故障が起きる、デバイスを紛失するといった問題が起きます。ひどい時はランサムウェアのようなマルウェアによってファイルが全て削除されたり、デバイスがロックされたりします。このような場合、バックアップがあなたのデジタルライフを復旧させる唯一の方法となります。

何を、いつ、どの様に

バックアップとは、あなたのコンピュータやモバイルデバイス以外の場所に保存されたデータのコピーであり、重要なデータを失った時でも、バックアップからデータを復旧することができます。バックアップのはじめの一歩は、どのデータを取得するか決めることです。「(1)あなたにとって重要な特定のデータを対象とする」、あるいは「(2)OS全体を含む全てのデータを対象とする」という選択肢が示されるのが一般的ですが、多くのバックアップ技術は、デフォルトで最初の選択肢にあるデータを取得するように設定されており、最もよく使用されているフォルダのバックアップが取得されます。何のバックアップを取得すれば良いかわからない、より慎重にバックアップを管理したいとお考えの場合は、全てのバックアップを取得すると良いでしょう。

次に、バックアップ取得の頻度を決めましょう。Apple社のTime MachineやWindows Backup and Restoreなら、自動的に「設定してあとはそのままにしておく」ことができるスケジュールを作成することができます。一般的なオプションには、1時間ごと、日次、週次などがあります。その他の技術には、文書を保存する度に新しい、または変更が加えられたファイルのバックアップを取得する「継続的な保護」がありますが、重要なファイルのバックアップは最低でも毎日自動で取得することをお勧めします。

最後に、どの様にバックアップを取得するか決めましょう。ローカルへの保存とクラウドベースのストレージの利用という2つの方法があります。ローカルへのバックアップ保存では、USBドライブやWi-Fi経由でアクセス可能なネットワークデバイスといったあなたが制御できる機器を使用します。ローカルの長所は、大量のデータを素早くバックアップやリカバリできるということです。短所は、ランサムウェアなどのマルウェアに感染した場合、バックアップにも感染が広がる可能性があるという点です。また、火災や盗難などの災害が発生した場合、コンピュータだけでなくバックアップも紛失する可能性があります。外部機器をバックアップ用に使用する場合、コピーを離れたセキュアな場所に保存しバックアップが適切に分類されていることを確認しましょう。

クラウドベースの技術は、インターネット上であなたのファイルを保存するオンラインサービスです。通常、コンピュータにアプリケーションをインストールし、そのアプリケーションが自動でファイルをスケジュールに従って、もしくは変更を加える度に保存します。クラウド技術の長所は、その容易さです。バックアップの取得は大抵の場合自動で、どこからでもあなたのファイルにアクセスすることができます。また、データがクラウド上にあるため、火災や盗難といった災害が発生してもバックアップには影響が出ません。さらに、クラウド上のバックアップは、ランサムウェアなどのマルウェア感染時にあなたを助けてくれることでしょう。短所は、バックアップとリストアの能力が、どれほどの量のデータのバックアップを取得したかイメージしにくく、データの同期やリカバリーもネットワークのスピードに左右される点です。ローカルとクラウドのどちらを使うべきか判断できないときはどうすればいいかって？慎重を期して両方使ってみることをお勧めします。

モバイルデバイスを使用している場合、あなたのデータは既にクラウド上に保存されています。しかし、アプリの設定や最近撮った写真、システム設定などはクラウドに保存されていないかもしれません。モバイルデバイスのバックアップを取得することで、これらの情報を同期させるだけでなく、新しいデバイスにアップグレードする際のデータの転送が容易になります。

何を、いつ、どの様に

- **データのバックアップ取得はやるべきことの半分に過ぎません。データを復旧できることを確認する必要があります。ファイルをバックアップから復元したり開いたりすることで、バックアップが正常に取得できていることを確認するテストを定期的に実施しましょう。**
- **バックアップからシステムを再構築する場合、使用前に最新のセキュリティパッチやアップデートを適用し直しましょう。**
- **クラウド技術を使用する場合、使いやすいものを選び、セキュリティオプションについて調査しましょう。例えば、オンラインアカウントをセキュアな状態に保つための、二段階認証をサポートしているかといったものです。**

バックアップはあなたのデジタルライフを守るための、容易でコストのかからない方法です。

ゲストエディタ

マット・ブロマイリー氏は、サイバーセキュリティの専門家であり、大小さまざまな組織と仕事をした経験を持つインシデントレスポンダーです。さらに彼はSANSインストラクターとして、ホストやネットワークにおける高度なインシデント対応と脅威ハンティングを学ぶFOR508とFOR572を担当しています。ブロマイリー氏はTwitter（@mbromileyDFIR）でも情報を発信しています。

リソース

パスワードとその管理を容易なものにする: https://www.sans.org/u/TqR
マルウェアの侵入を阻止する: https://www.sans.org/u/TqW
自宅を安全なサイバー環境にするには: https://www.sans.org/u/Tr1

 Editorial Board: Walt Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley | Translated by: 小山 裕之, 時田　剛