OUCH! | 2017 年 08 月

コンピュータ利用者のためのマンスリー・セキュリティ・アウェアネス・ニュースレター

OUCH!

今月のトピック...

- バックアップとは：何か？いつ？どのようにして？
- 復旧
- 重要な点

バックアップと復旧について

はじめに

パソコンやモバイルデバイスを長い期間に渡って使用していれば、何かの手違いや事故が起こって、個人ファイルやドキュメント、画像などの重要なデータを失ってしまうことがあります。例えば、誤ってファイルを削除してしまったり、ハードウエアが故障したり、デバイスを紛失してしまったり、ランサムウエアに感染してしまったりするなどです。このような時、デジタルライフを短時間で再構築するために活用できるのは、バックアップしかありません。このニュースレターでは、バックアップとは何かを解説し、バックアップの取り方を説明すると同時に、自分自身に適切なバックアップ計画を検討する方法を説明しています。

ゲストエディタ

キース・パームグレン氏は、ITセキュリティ分野において30年以上の経験を持つサイバーセキュリティのプロフェッショナルです。SANSのシニア講師であり、SANS SEC301「Introduction to Information Security」の著者でもあります。彼は、セキュリティコンサルティング業で成果を出し続けており、ツイッター（@kpalmgren）でも情報発信をしています。

バックアップとは：何か？いつ？どのようにして？

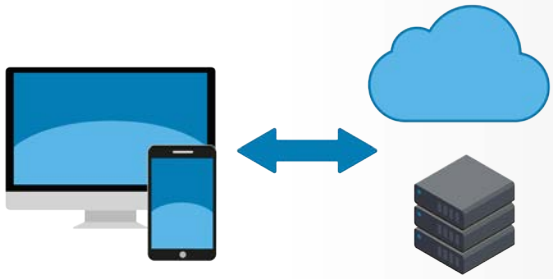
パソコンやモバイルデバイス以外の場所にもコピーが保存されていることをバックアップと呼びます。重要なデータを失った場合、バックアップからデータを復旧できますが、簡単でコストもあまりかからないのに関わらず、残念ながら定期的にバックアップを取っている人は極めて少数に留まっています。まず、最初のステップでは、何をバックアップするか決めなければなりません。ここでは二つのアプローチがあります：「（1）個人的に重要なデータ」、または「（2）オペレーティングシステムを含む、すべてのデータ」です。バックアップソリューションの大半は、デフォルトで（1）を行うよう設定されており、頻繁に利用されるフォルダに含まれているファイルのバックアップを取ります。多くの場合、これだけで十分です。しかし、何をバックアップしていいか分からない場合や、細心の注意を払いたい場合は、すべてのファイルをバックアップしてください。

次にどのくらいの頻度で自分のデータのバックアップを取るかを決めなければなりません。Apple の Time MachineやMicrosoft Windowsのバックアップと復旧のように、OSをインストールした直後に組み込まれている機能を使うと、一度設定を行うだけで、自動で定期的にバックアップを取るようにすることができます。バックアップのタイミングとしては、一般的に一時間、一日、一週間などのオプションから選択します。他のソリューションでは、「継続的な保護」を提供しているものがあり、新しいファイルや変更されたファイルが保存された際にバックアップが自動的に取られます。最低限、一日に一度バックアップを取ることを推奨します。

最後に、どのようにしてバックアップを取るか決めなければなりません。バックアップを取る方法は二つあります：物理的なメディアまたはクラウドストレージです。どちらのアプローチにも長所と短所があります。どちらのアプローチを利用すればいいか分からない場合は、両方同時に利用しても良いでしょう。物理的なメディアとは、自分自身で管理できる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を指します。自分自身で管理するメディアを使う

バックアップと復旧について

利点として、大量のデータをバックアップや復旧を素早く実行できることが挙げられます。このアプローチの端緒として、ランサムウエアなどのマルウエアに感染してしまった場合、バックアップを感染させてしまう可能性があります。また、火事や盗難などの災害に見舞われてしまった場合、パソコンだけでなくバックアップも失ってしまう可能性があります。そのため、外部接続デバイスにバックアップを保存している場合は、そのデバイスを別の安全な場所に保管することをお勧めします。そして、保管するバックアップに分かりやすいようにラベルを貼っておいてください。



自動化された信頼できるバックアップは、自分のデータを保護するための最終防衛線です。

クラウドストレージは、インターネット上にファイルを保管するためのオンラインサービスです。多くの場合、パソコンにアプリケーションをインストールする必要がありますが、アプリケーションがパソコン上のファイルを自動的にバックアップしてくれます。バックアップは、定期的またはファイルに変更があった際に行われるのが大半です。クラウドストレージの長所は、簡単であることと、自動的にバックアップが行われることが多いこと、そしてどこからでもファイルにアクセスが可能であることが挙げられます。また、データがクラウド上にあるため、自宅での災害、例えば火事や盗難によってバックアップが影響を受けることはありません。また、最後の長所として、クラウドバックアップはランサムウエアなどのマルウエアの感染からの復旧に役立つことがあります。多くの場合、感染する前の状態のものから復旧してくれます。短所として、大量のデータをバックアップするために時間がかかることです。また、プライバシーとセキュリティが重要になります。利用するバックアップサービスは、強いセキュリティを提供しているでしょうか？例えば、データの暗号化や強い認証などを検証してください。

最後にモバイルデバイスを紛失しないようにしてください。モバイルデバイスの場合、多くのデータ、例えばメール、カレンダー、連絡先などの情報などが既にクラウド上に保存されています。しかし、モバイルアプリの設定や、画像、システムの設定などはクラウドに保存されていない可能性があります。モバイルデバイスのバックアップを取ることで、これらの情報を保存できるだけなく、新しいデバイスにアップグレードした際にデータの転送が楽になります。iPhone および iPad の場合、自動的に Appleの iCloud へバックアップします。Android や他のモバイルデバイスの場合は、製造元またはサービスプロバイダによって変わります。場合によっては、バックアップ用のモバイルアプリを購入する必要があるでしょう。

復旧

データのバックアップを取っただけでは不十分であり、半分しかやったことになりません。そのバックアップからデータを適切に復旧できる必要があります。定期的にバックアップからファイルを取得し、そのファイルを検証したり、バックアップからファイルを取得し、そのファイルを検証してください。また、メジャーアップグレード（新しいパソコンやモバイルデバイスへの移行）または大きな修理後（ハードディスクの交換）の前には、システム全体のバックアップを取り、そこから復旧できることも確認しておいてください。

バックアップと復旧について

重要な点

- バックアップを取るためのソリューションに関わらず、バックアップを自動で取るようにし、定期的にバックアップを確認してください
- バックアップからシステムを再構築する場合、最新のセキュリティパッチやアップデートを適用してから利用してください
- 古いバックアップは、必要の無いゴミデータになるおそれがあるため、外部から悪意のある人によってアクセスされないように削除または破壊してください
- クラウドソリューションを利用する場合、プロバイダのポリシーや評判を調査し、自分自身の要件を満たすか確認してください。例えば、データの暗号化をしているか？段階認証などの強い認証機構を提供しているか？ などがあります。

詳しくは

毎月発行のセキュリティアウェアネスニュースレター「OUCH!」をご活用ください。また、OUCH!のアーカイブで過去のトピックも参照できます。詳しくは、SANSセキュリティアウェアネスソリューションのサイトをご覧ください。
securingthehuman.sans.org/ouch/archives

日本語版翻訳チーム

日本語版翻訳－NRIセキュアテクノロジーズ株式会社

NRI セキュアテクノロジーズは、国内でも有数の情報セキュリティ専門企業です。マネージドセキュリティサービス、コンサルティング、ソフトウェアソリューションなどの提供を通じて、情報セキュリティのあらゆる視点からお客様をサポートします。http://www.nri-secure.co.jp

リソース

パスフレーズについて:	https://securingthehuman.sans.org/ouch/2017#april2017
2段階認証について:	https://securingthehuman.sans.org/ouch/2015#september2015
クラウドを安全に利用するには:	https://securingthehuman.sans.org/ouch/2016#november2016
暗号について:	https://securingthehuman.sans.org/ouch/2016#june2016
ランサムウエアについて:	https://securingthehuman.sans.org/ouch/2016#august2016