OUCH! | 2015 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...

- 何をいつバックアップするか
- バックアップの方法
- 復旧
- 要点

バックアップと復旧

はじめに

いつか何か悪いことが起こり、個人的なファイル、ドキュメントや画像を失うことがあるでしょう。例えば、誤って重要なファイルを削除してしまったり、ハードウェアが故障したり、ノートパソコンを紛失したり、マルウェアに感染してしまうことが挙げられます。このような事態が起きてしまった場合にデジタルライフを再構築するには、バックアップを利用するしかありません。このニュースレターでは、バックアップの説明、データのバックアップ方法、そしてご自身にあったバックアップ戦略のヒントをお教えします。

ゲストエディター

ヘザー・マカリク氏は、フォレンジック業界でも有名なエキスパートで、主にスマートフォンのフォレンジックを専門にしています。Practical Mobile Forensics の共著者で、Learning Android Forensics のテクニカルエディタも務め、さらに SANS Institute の FOR585 Advanced Smartphone Forensics とFOR518 Macintosh Forensics の共著者でもあります。ヘザーは、Smarterforensics.com およびツイッター（@heathermahalik）でも積極的に情報を発信しています。

何をいつバックアップするか

自分自身の情報が別場所に保管されているものをバックアップと呼びます。多くの人はバックアップを簡単に取ることができ、それほど高くないにもかかわらず、バックアップを取っていませんが、とても残念なことです。重要なデータを失ってしまった場合、これらのデータをバックアップから復旧できますが、何をバックアップするかを考慮するにあたり、二つのアプローチがあります：（1）自分自身にとって重要なデータをバックアップする、もしくは（2）オペレーティングシステムを含むすべてのデータをバックアップする　というものです。前者のアプローチは、バックアップのプロセスを簡素化し、ハードディスクの領域を節約できます。それに引き換え後者のアプローチは、簡単で包括的です。あなたが何をバックアップしていいのか悩んでいる場合は、すべてをバックアップすることをお勧めします。

次に考えなければならないのは、どのくらいの頻度でデータのバックアップを取るか、です。一般的な選択肢として、一時間ごと、一日ごと、一週間ごとなどがあります。自宅利用の場合、アップル社の Time Machine やマイクロソフト社のWindows Backup and Restore といった個人向けのソフトがあり、これらには、自動的にバックアップを行うための「設定して放置する（set it and forget it）」スケジュール作成機能があります。これらのソフトは、作業中もしくはパソコンから離れている間にバックグラウンドでデータのバックアップを取ります。ソフトによっては、「永続的な保護（continuous protection）」と呼ばれる機能を提供しているものがあり、新しいファイルや編集されたファイルを閉じたら、すぐさまバックアップを取ります。重要なファイルを扱うような方は、最低でも一日に一回バックアップを取ることをお勧めします。最終的に自分自身に問わなければならないのは、「バックアップから復旧することになった場合、どのくらいのデータを失う覚悟があるか？」となるでしょう。

バックアップの方法

データをバックアップする方法は二つあります：物理的なメディアに保存するか、クラウドベースのストレージを利用

バックアップと復旧

するか、です。物理的なメディアは、様々なハードウェアを指しており、DVD、USBドライブ、あるいは外付けのハードディスクなどがあります。どのメディアを選択するにしても、元のファイルがある機器と同じ機器にバックアップを取らないようにしてください。物理的なメディアの問題点として、メディアが保管されている場所に災害（例えば、火事や強盗など）があった場合、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、バックアップを別の安全な場所に保管することを考慮する必要があります。別の場所にバックアップを保管する場合、ラベルを貼り、いつ、何をバックアップしたのかを明記してください。追加のセキュリティ対策として、バックアップを暗号化するのも良いでしょう。

自動的に取られた信頼できるバックアップは、データを保護するための最終手段になることが多い。

クラウドベースのソリューションは、物理的なメディアと違い、ファイルはインターネット上のどこかにファイルを保管してくれるサービスですが、保存するデータのサイズによっては有料となる場合があります。いずれにしても、クラウドベースのバックアップでは、自動的にファイルをバックアップするためのプログラムをインストールすることで利用することができます。このソリューションの利点は、バックアップはクラウド上に存在するため、自宅が災害による被害を受けてもバックアップは安全なままです。また、出張先からでもバックアップ、もしくは個別のファイルにアクセスできるということもあります。クラウドベースのバックアップ（およびリカバリ）の不便なところは、特に大量のデータを扱う場合、遅くなる可能性があることです。どちらのバックアップ手法（物理的なメディア、クラウド）がご自身に適切であるか判断がつかない場合は、両方利用するという選択肢があることを忘れないでください。

最後に、モバイルデバイスのバックアップを忘れてはいけません。モバイルデバイスの利点として、多くのデータは既にクラウドに保存されているということがあります。例えば、メール、カレンダーに登録されているイベントや連絡先情報などが挙げられます。しかし、クラウドに保存していない情報、例えば、モバイルアプリの設定情報、最近撮影した写真やデバイスの設定などがあるでしょう。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するだけでなく、特に新しいデバイスにアップグレードした場合、デバイスの復旧が楽になります。たとえばiPhone/iPad は、アップルの iCloudを使って自動的にバックアップを取ることが可能です。また、Androidや他のモバイルデバイスも、自動バックアップを実現することができますが、バックアップを行うためのアプリを購入する必要があるなど、メーカーやサービスプロバイダによって変わってきますので注意してください。

復旧

データのバックアップを取るだけであった場合、必要事項の半分しかやっていないことになります。なぜなら、このバックアップから正常にリカバリできるかを確認する必要があるからです。一か月に一回は、ファイルを一つ削除し、バックアップからリカバリし、コンテンツが正常であるかを確認するようにしましょう。また、大きなアップグレード（新しいパソコンや

バックアップと復旧

モバイルデバイスを購入した場合）や大きな修理（ハードディスクのリプレースなど）を行う前には、システムそのもののバックアップを取るようにし、これも正常にリカバリできるか否かを確認しましょう。

要点

- バックアップを可能な限り自動化し、適度に確認すること
- システムをバックアップから復旧した場合、最新のセキュリティパッチや更新を適用してから使用すること
- あまりにも古い、または既にサポートされていない形式のバックアップは悪意ある第三者にアクセスされる可能性があるため、削除すること
- クラウドソリューションを利用している場合、プロバイダのポリシーや評判を事前に確認し、自分自身の要求を満たしているか確認すること。例えば、「保存されているデータを暗号化しているか？」「誰がバックアップにアクセス可能か？」「2段階認証のような強い認証機能があるか？」

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。
http://www.securingthehuman.org

日本語版翻訳チーム

日本語版翻訳ー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、国内最大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:	http://www.securingthehuman.org/ouch/2015#april2015
2段階認証:	http://www.securingthehuman.org/ouch/2013#august2013
クラウドを安全に利用するには:	http://www.securingthehuman.org/ouch/2014#september2014
暗号化機能について:	http://www.securingthehuman.org/ouch/2014#august2014
本日のワンポイントアドバイス:	http://www.sans.org/tip_of_the_day.php

Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Translated By: 内山　貴之, 時田　剛