

OUCH!

月間セキュリティ啓発ニュースレター

春に向けてセキュリティしませんか？

はじめに

多くの人たちが春の到来を今かと待ち望んでいます。日々目に映る光景が少しずつ変わり、花が咲き始めるようになる頃、いろいろなことを綺麗にしたいと考えるでしょう。整理整頓の必要性は、ここで語るまでもなく容易に理解していただけるはずですが、デジタルな世界における整理整頓について考えたことはあるでしょうか。ここでは、デジタルライフを整理し、新しいデジタル習慣を作るための簡単なヒントをご紹介します。



バックアップ:このステップを最初に挙げたのは、長い目で見たときに最も重要で、ほかのステップに進む前に実行してほしいことだからです。現在の状態が安全であるかどうかは別にして、重要な情報をリカバリするにはバックアップが必要になります。リカバリが必要な状況としては、ハードディスクの故障やデバイスの紛失、ランサムウェアなどのマルウェア感染などがあるでしょう。自動でバックアップを作成するようにスケジュールすることで、最も重要な情報を確実にリカバリできるようになります。



削除:使用していないプログラムやアプリは、モバイルデバイスやコンピュータから削除しましょう。アプリの中には、大量のストレージ領域を消費していたり、動作が遅くなる原因になるほか、新しく脆弱性が発見される可能性があります。インストールされているアプリの数が少ないほど、あなたのシステムや情報のセキュリティが向上するでしょう。最近のデバイスは、アプリの使用時間などを記録してくれる機能があります。過去に実行して、数カ月経過しているようなアプリは、あなたにとって不要と考えていいと思います。



アップデート:お使いのデバイスとアプリをアップデートしましょう。また、可能な限り自動アップデート機能も有効にしておきましょう。自動アップデート機能によって、デバイスやアプリを最新の状態に保つことができるだけでなく、バグなどの修正も行われるため、安定動作が期待できます。



パスワード:まず、あなたのパスワードを確認してみましょう。複数のサービスやアカウントで同じパスワードを使用している時は、それぞれのサービスやアカウントで別々のパスワードを設定するようにしてください。バラバラのパスワードを覚えるのは大変だよ…そんなお悩みがありませんか？その場合は、パスワードマネージャーを使用しましょう。また、メールやオンラインバンキングといった、プライバシー・金銭が関連するようなアカウントの場合、可能な限り2要素認証(2FA)を有効に設定してください。



金融サービスアカウント: お使いのオンラインバンキングやクレジットカード会社のサービスで、大きな金額が動く決済が発生した場合に通知がされるように設定されているか確認してください。このような不正行為に対して、発見するのが早ければ早いほど、被害を小さくすることができるからです。居住している国や地域にもよりますが、最終的に個人と信を凍結することが、オンライン決済の世界において身を守る最も効果的な方法となることを覚えておいてください。



ブラウザ: はじめに、お使いのブラウザに導入されているすべてのアドオンやプラグインを確認してください。そのとき、プラグインに許可している権限を確認してみましょう。プラグインが、あなたの所在地やパスワード、連絡先リストにアクセスする必要があるでしょうか？特に重要ではないプラグインがインストールされていたり、プラグインに許可した権限によってプライバシーに懸念がある場合は、それらを削除してしまいましょう。



ソーシャルメディア: 自分でオンラインのプレゼンス情報を確認してみましょう。例えば、プライバシー設定の状態や、他者と共有する必要がない写真、動画などが見つかった場合は、削除してしまいましょう。また、検索エンジンを使って自分自身を調査し手確認することもできます。このチェックで大事なことは、公開している情報量の寡多ではなく、情報の公開範囲が適切かどうかを重要なることを誤解しないようにしてください。



デスク: 物理的に机もきれいにしましょう。古いハードディスクやUSBメモリなどがあったら、完全消去してしまいましょう。これらに貼付されたメモなども忘れずに破棄してください。紙で残されたメモなどが見つかった場合は、シュレッダなどを使用して破棄してください。



メール: メール本文だけではなく、メールの添付ファイルなども忘れずに削除してください。生年月日やマイナンバーなどが記載されたメールがないか慎重に内容を確認して整理しましょう。もし見つかった場合は、受信トレイから外してしまってもいいかもしれません。

ここまで挙げた作業を実施するのは大変と思うかもしれませんが、すべてを実施すると、デバイスや情報はこれまで以上に保護された状態になるでしょう。一気に実施しようとするのが大変に感じるので、1日や1週間といった短い期間に1つのテーマを決めて実施することを考えてみてください。最初は小さなことかもしれませんが、これらを積み重ねることによってあなたをきっと守ってくれるでしょう。

ゲストエディタ

Katie Nickels (@LiketheCoins) Red Canary社においてプリンシパルインテリジェンスアナリストを務めるとともに、SANSのインストラクターとしてFOR578: Cyber Threat Intelligenceを教え、彼女が持つネットワークディフェンスやインシデントレスポンス、およびスレットインテリジェンスにおける10年以上の経験が余すところなく活かされています。



リソース

バックアップを取得していますか？:	http://www.sans.org/u/Z2Q
パスワードをシンプルにする:	http://www.sans.org/u/Y63
インターネットで自分自身を検索する:	http://www.sans.org/u/ZVB
モバイル端末の処分方法:	http://www.sans.org/u/ZVG

OUCIはSANS Security Awareness プログラムによって発行され、Creative Commons BY-NC-ND 4.0 licenseに従って配布されます。このニュースレターを再配布し、もしくは啓発資料としてご利用いただけますが、コンテンツの改変は認められません。 翻訳その他に関しては、www.sans.org/security-awareness/ouch-newsletter までお問合せください Editorial Board: Walt Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley. Translated by: 時田 剛