

2014年8月26日

## オンライン攻撃のたびに すべてのパスワードを変更しないで済ませるには

(2014年8月19日ヘルシンキ発 - フィンランド本社発表資料抄訳)

**セキュリティの専門家の秘訣：彼らはパスワードを頻繁には変更しません。その必要がないからです。皆様にも役立つ秘訣をご紹介します。**

12億ものパスワードがロシアのハッカーに盗まれたとの報告がありました。Heartbleedが発見される以前のことで、広範囲に及び特定できないデータ漏洩が発生した場合、すべてのパスワードを変更すべきだというのが一般的な見解です。しかしエフセキュア セキュリティラボによれば、さらに優れた方法があります。パスワードを適切に管理する習慣があれば、オンライン攻撃の情報を聞いたときにすべてのパスワードを変更する必要はなくなります。

「すべてのパスワードを変更すれば被害はないでしょうが、手間がかかってしまいます。それだけではなく、より強固な長期的対策とは言えず応急処置に過ぎません」とエフセキュア セキュリティラボのセキュリティ・アドバイザー、ショーン・サリバンは述べています。データ漏洩は新たな現実であり、もし起きたらという問題ではなく、いつ起こるかという問題になっています。サリバンは次のように述べています。「ユーザには、すべてのパスワードを変更するように指示するのではなく、従う価値のある役立つアドバイスが必要です。次に漏洩が報告された際には、被害に遭ったパスワードは管理下に置かれ、そのパスワードのみ変更すれば良いのです」

サリバンはまたこのように述べています。「専門家の秘訣、それはデータ漏洩によってすべてのパスワード変更を推奨されても、そのアドバイスに従っていないということです。なぜなら、その必要がないからです。特定のアカウントについて漏洩されていないのであれば、私はパスワードについて心配しません。それは、私がパスワード記録用のツールや、アカウント管理に役立つシンプルな各種のテクニックを利用して、リスクを最小限に抑えているからです」

それでは、パスワードを絶えず変更する手間をなくす有効な手段とは何でしょうか。サリバンは重要な点をいくつか指摘しています。

**リスクを低減するためにアカウントを分散。** 個人関連、業務関連、金融関連など、目的ごとに E メールアドレスを作成することによって、アカウントを分けます。そうすれば、1つの E メールが侵害されても、その他のすべての情報が危険にさらされることはありません。サリバンは次のように述べています。「金融口座用の E メールアドレスを別に作成してみたいかがですか。そして、そのアドレスを金融機関以外の誰にも教えないことです」さらにもし、個人アカウントに銀行関連の E メールが届いたら、それは不法なものであるとすぐにわかります。

**可能であれば、E メールアドレスの他に、ユーザ名も異なるものを使用。** Eメールの他に固有のユーザ名を取得できるサービスもあります。ハッカーははるかに多くの情報を得ることが必要になるため、可能であればこのオプションを利用すると良いでしょう。また、利用可能であれば二要素認証を使用します。

各オンラインアカウントに対し、個別のパスワードを使用。異なるアカウントに対して同じパスワードを使用することは、ハッカーのためにレッドカーペットを広げているようなものです。Facebook アカウント用のパスワードが盗まれたら、犯罪者は E メールや他のアカウントに飛び移り、そこで同じパスワードを試すでしょう。

必須ではないデータをオンラインアカウントに提供しない。危険にさらされるものが少ないほど、安全性は高まります。

ある特定のアカウントについて漏洩が通知されたら、そのパスワードを変更。これは言うまでもありません。アカウントのパスワードを変更することは、少々骨が折れるかもしれませんが。しかし、長い目で見れば、漏洩のたびにすべてのパスワードを変更するよりは、簡単でストレスも少なく済みます。また、個人情報やオンラインの身元識別情報の安全を守るためには価値のあることです。サリバンは、最初は 1 つのアカウントにて変更するところから開始し、すべてのパスワードについて完了するまで、対応を強化していくことを提案しています。

サリバンは次のように述べています。「これは PC の憂慮すべき次なる課題です。すべてのアカウントはクラウドにあるからです。世の中には 2 種類の人々がいます。アカウントをうまく管理する人々と、トラブルの世界に入りこむ人々です。どちらのグループに入りたいですか?」

### 適切なツールを使用すれば簡単です

ではどうすれば、多くの個別のパスワードとログイン名を覚え、効率的に管理できるでしょうか。エフセキュアのパスワードマネージャ、F-Secure KEY なら、適切なパスワード管理ができるだけ簡単に苦もなく行えます。F-Secure KEY では覚える必要があるのは、たった一つのマスターパスワードだけです。各アカウントに対して個別のパスワードを設定することが簡単になります。ユーザ名、パスワード、PIN コード、その他重要なデータが、1 つの安全なアプリケーションに保存されています。

F-Secure KEY には現在、全面的にアップデートしリフレッシュしたモバイルバージョンがあります。新しいモバイルユーザインターフェースには「お気に入り」機能があり、頻繁に使用するアカウント情報へのアクセスを、簡単に素早くできるようにします。F-Secure KEY のすべてのバージョンは、独自の強固なパスワードを生成するのに役立ちます。また、エフセキュア セキュリティラボからのニュースフィードが導入されており、主要なハッキングに対しては最新の状態を保つことができます。強力な暗号化により、すべてのデータが守られます。

F-Secure KEY は無料でダウンロードでき、Android、iOS、Windows、Mac など、あらゆるデバイスで使用できます。複数デバイス(何台でも可)上で同じマスターパスワードを用いて F-Secure KEY を使用したり、安全な欧州のクラウド経由で複数デバイスのパスワードを同期するには、プレミアムバージョンにアップグレードしてください。プレミアムバージョンは有償になります。F-Secure KEY は Apple App Store、Google Play、[f-secure.com/key](https://f-secure.com/key) で取得できます。

\*エフセキュアの社名、ロゴ、製品名は F-Secure Corporation の登録商標です。

\*本文中に記載された会社名、製品名は各社の商標または登録商標です。

---



<http://www.f-secure.co.jp/>

## F-Secure – Switch on freedom

エフセキュアは、オンラインセキュリティおよびプライバシー保護を提供するフィンランドの企業です。弊社は、世界中の何百万人もの人々が、監視されることなくインターネットを楽しみ、さまざまなデータを保存や共有する力と、オンラインの脅威からの安全性を提供します。弊社の存在意義は「デジタルフリーダム」のために闘うことです。この動きに参加し、自由のために闘いましょう。1988年創業のエフセキュアは、NASDAQ OMX Helsinki Ltd に上場しています。

エフセキュア株式会社は、エフセキュア社 100%出資の現地法人として設立され、以降、増収を続けながら順調に企業規模を拡大しており、2009年5月に日本法人設立満10周年を迎えました。

会社名: エフセキュア株式会社  
カントリーマネージャ: アリエン・ヴァン・ブロックランド  
所在地: 〒107-0052 東京都港区赤坂 2-11-7 ATT 新館 6F  
設立: 1999年5月  
事業内容: セキュリティ関連製品・サービスの販売およびサポート

---

### 本件に関するお問合せ先

エフセキュア株式会社

マーケティング部

Tel: 03-5545-8942 Fax: 03-5545-8945

Email: [japan@f-secure.co.jp](mailto:japan@f-secure.co.jp)

〒107-0052 東京都港区赤坂 2-11-7 ATT 新館 6F

URL: <http://www.f-secure.co.jp/>

Blog: <http://blog.f-secure.jp/>