



2009年8月13日  
エフセキュア株式会社

## オンライン犯罪者が Facebook などの ソーシャルネットワーキングサービス (SNS) を狙い撃ちする理由とは？

エフセキュアは、E-mail と SNS のログインには同じパスワードを使用しないことが基本的な予防策になるとアドバイス。

2009年8月12日ヘルシンキ発(フィンランド)ー

オンライン犯罪者は、最も多くのユーザを引き付ける最新のインターネット上のトレンドを追いかけるといった特徴を持っています。そのため、Facebook や Twitter のように非常に人気のあるソーシャルネットワーキングサイトはフィッシングやオンライン詐欺といった詐欺攻撃の格好の標的となっています。

先日の金曜日にエフセキュアブログでも投稿がありましたが、Facebook や Twitter などのソーシャルネットワーキングサイト狙ったオンライン犯罪として昨今話題になっているのが、「Cyxymu」という名で呼ばれているグルジア在住のブロガーへの大規模攻撃です。この攻撃は、Facebook や Twitter などのソーシャルネットワーキングサイトのユーザを利用した DDos 攻撃で、金曜日に一時的に同サービスが使用不可になるなどの二次被害を引き起こしました。

エフセキュアの CRO(セキュリティ研究所首席研究員)のミッコ・ヒッポネンは「これは特定の個人を狙った攻撃ではありませんが、社会全体に多大な影響を与えることは間違いありません。「Cyxymu」の影の首謀者が誰なのかはわかりませんが、彼らが大規模な DDos 攻撃を実行できるインフラを持っていることは明らかです。」とコメントしています。

Facebook を介するコミュニケーションは、個人的なつながりや友人・知人のコミュニティがベースになっており、そこには高い信頼性があります。Facebook の友人から Wall(掲示板)にメッセージが送信されるということは、不特定多数の匿名送信者から E-mail やスパムメールを受け取るのとはまったく性質が異なり、こうした高い信頼性が、2億5千万人のユーザを抱えている Facebook が狙い撃ちされる理由です。フィッシング詐欺や金銭にからむオンライン詐欺は攻撃のターゲットが信頼に足るという錯覚を起こさせるからこそ、犯罪者は貴重な情報にアクセスし金銭を狙う詐欺を働くことができるのです。

エフセキュアのセキュリティ研究所のセキュリティアドバイザー、ショーン・サリバンは次のように述べています。

「脆弱性の高いパスワード、つまり安易なパスワードは、ソーシャルネットワーキングサイトに不正侵入する手口を犯罪者に教えるようなものです。彼らの狙いはコンタクトリスト(アドレス帳)、電話番号などの個人情報です。これらの情報を収集し、スパムメール業者に売りつけるなどして金銭を荒稼ぎすることにあります。」

Facebook アカウントへの不正侵入がもたらす被害は、そのユーザが同じパスワードを E-mail アカウントにも使用していればますます拡大します。つまり、犯罪者はいとも簡単にユーザのオンラインパスワードを全部リセットしてバンキング情報を盗み、セキュリティ対策の質問への正しい回答にもすぐにたどり着くことができます。たとえばミドルネーム、自宅の住所、ペットの名前だけでなく個人のセキュリティに関する対策ですら、Facebook 上で見つけられてしまうこともあるのです。

「Facebook のユーザネームは E-mail アドレスで構成されているので、個人の電子メールアカウントや Facebook などのソーシャルネットワーキングサイトへのログインには同じパスワードを使わないことがセキュリティを確保する上で、絶対不可欠です。E-mail アカウントをメインアドレス、ビジネス用、ソーシャルネットワーキング用とそれぞれ変えて設定するのも良い方法でしょう。」ともション・サリバンは述べています。

今年になって、いわゆる「友人」から送金を求める偽装メッセージの被害が続いていますが、Facebook ユーザがこのようなメッセージを受け取った場合は、たとえ家族や信頼できる人物からのメッセージであっても常に取り扱いに注意し、送金する前に徹底的な身元確認を行うべきです。

「とはいえ、ソーシャルネットワーキングサイトのセキュリティについてはポジティブな側面もあります。従来のチェーンレターのように何年も送り届けられるスキムメールと異なり、ネットワーク接続で Facebook に集うユーザの知恵を結集すれば、最新のセキュリティ驚異に迅速に対応できるという良い面もあります。有益なセキュリティ情報を友人・知人に知らせて、セキュリティの脆弱性に対して自己対策を取ることができる点で、コミュニティは役に立つでしょう。」とも同氏は付け加えています。

#### ◆ より安全なソーシャルネットワーキングを実現するための対策

- ✓ E-mail とソーシャルネットワーキングサイトのパスワードは常に個々に設定し、より高いセキュリティを確保する
- ✓ Facebook のセキュリティ上の問題に気付いた場合は、コミュニティが予防策をとれるように Wall に投稿する
- ✓ 友人は慎重に選び、仲間内でセキュリティリーダーを決めておく！
- ✓ Facebook を介してエフセキュアに問い合わせる（英語）

<http://www.facebook.com/FSecure.Labs>

## ◆ エフセキュア株式会社

エフセキュア社は、IT 先進国フィンランドで 1988 年に設立されて以来、20 年にわたりセキュリティ製品に取り組んでいる業界の老舗で、世界規模でセキュリティサービスを提供しています。1999 年に OMX ヘルシンキ証券取引所に上場し、以来、業界で最も急速に成長し続けている株式公開企業です。エフセキュア株式会社は、エフセキュア・コーポレーションの 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  
代表者 : 日本法人代表 桜田 仁隆  
所在地 : 〒220-0011 横浜市西区高島 2-19-12 スカイビル 23F  
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 担当:尾崎 risa.ozaki@f-secure.com

TEL: 045-440-6780、FAX: 045-440-6616

〒220-0011 横浜市西区高島 2-19-12 スカイビル 23F

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