Information-technology
Promotion
Agency, Japan

第 14-01-307 号
2014 年 1 月 7 日
独立行政法人情報処理推進機構

今月の呼びかけ

「 おもいこみ　僕は安全　それ危険 」

第 9 回 IPA 情報セキュリティ標語・ポスター・4 コマ漫画コンクール 2013 標語部門
優秀賞　永瀬　孝樹 さん（福島県　いわき市立錦中学校）の作品

昨年発生した情報セキュリティに関する様々な事案の中で、金銭被害につながる可能性が高いという点で、特に一般利用者に影響が高いと考えられるものは以下の 4 つです。

1．インターネットバンキング利用者を狙った不正送金（☆）
2．過去の流行時の約 2 倍の件数に上るウェブ改ざん
3．偽の警告画面を表示させ有償版の購入を促し、クレジットカード番号を入力させる「偽セキュリティソフト」などの手口（☆）
4．従来の対策では見抜くことが難しい、スマートフォンのワンクリック請求アプリ（☆）

このうち 3 点が、1 年前の“呼びかけ“で紹介したもの（☆印）と重複していますが、着目すべきは 2012 年に既に存在していたこれら 3 つの手口が 2013 年に入り更に深化、巧妙化したことにあります。
被害に遭わないためには、以下の対策を漏れなく行うことが必須ですが、それに加えて「自分は大丈夫だ」という思い込みを捨て、日頃から用心するという心がけも重要です。

1．セキュリティソフトを導入し、ウイルス定義ファイルを常に最新に保つ。
2．パソコンやスマートフォンの OS（オペレーティングシステム）やアプリケーションソフトを最新版に更新する。
3．年に一度は、普段使用しているメーカー以外の無料ツールでウイルスチェックを行う。

2014 年最初の“呼びかけ”では 2013 年に顕著だった 4 点の事案を、更に巧妙になった手口を中心に説明します。

（1） 2013 年に発生した金銭的被害に繋がり易く、一般利用者に影響が高い新たな手口

【1】 インターネットバンキング利用者を狙った不正送金

2012 年から被害が続いている不正送金関連の相談は、2013 年上半期 20 件から、下半期半 96 件と約 4 倍に増加しています。従来の手口は、パソコンをウイルスに感染させて銀行のログイン情報を盗み取るものでしたが、2013 年 4 月ごろから、新たな手口が現れました。それは、ウェブメールサービスのログイン情報を盗み取る機能を有したウイルスを用いて、銀行から利用者宛にメールで送信されたワンタイムパスワードを盗み、本人に成りすまして不正に送金するというものです（図 1 参照）。

また、従来からある手口も引き続き用いられており、大手金融機関を装った偽のメールを送り、メール文中のリンクをクリックさせ偽サイトに誘導するフィッシングメールの相談が 2013 年 10 月以降 6 件寄せられており、今後も注意が必要です。

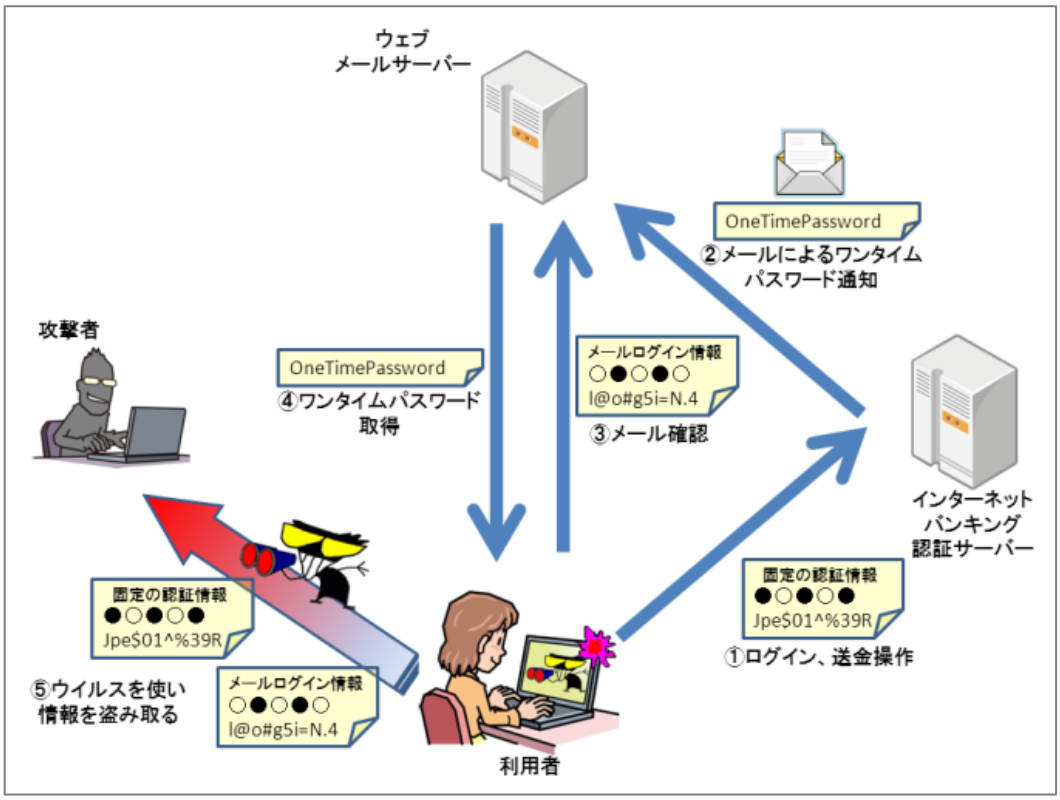

図 1：メールで受信するワンタイムパスワードを盗み取る手口のイメージ図

（ご参考）
IPA　2013 年 9 月「今月の呼びかけ」
「 インターネットバンキング利用時の勘所を理解しましょう！ 」
http://www.ipa.go.jp/security/txt/2013/09outline.html

【２】　過去の流行時の約 2 倍の件数に上るウェブ改ざん

2013 年 1 年間のウェブ改ざんに関する IPA への届出件数は 75 件でした。過去にウェブ改ざんが流行していた際の同様の届出件数は 2010 年 34 件、2012 年 38 件であり、それと比較すると 2013 年は約 2 倍に上っています。また、JPCERT コーディネーションセンター※1 から公表されているウェブ改ざん数も、2012 年第 3 四半期以降急増しています（表 1 参照）。こうしたことから、巷のウェブ改ざんの件数の増加が顕著であったと言えます。

その理由には、過去にウェブ改ざんが流行した際の手口と①ウェブサーバー上のソフトウェアなどの脆弱性を悪用する、②簡単な FTP パスワードなどを推測して改ざんを行う、といった複数の手口を組み合わせた手口の巧妙化があります。

改ざんされたサイトの多くは、セキュリティ対策の不十分なパソコンで閲覧するとウイルスに感染するよう細工されており、閲覧者に被害が及ぶ危険性があります。改ざんされてしまった正規のサイトは、なりすましサイトと違って閲覧者が一見しただけでは、判別することができない点が厄介です。

表 1：ウェブ改ざん数の推移（JPCERT/CC 公表のデータを基に作成）

期間	2012Q1	2012Q2	2012Q3	2012Q4	2013Q1	2013Q2	2013Q3
件数	142	139	769	737	1,184	1,847	2,774

（ご参考）
ウェブサイト改ざんの増加に関する一般利用者（ウェブ閲覧者）向け注意喚起（IPA）
http://www.ipa.go.jp/security/topics/alert20130626.html

※1：インターネットを介して発生する侵入やサービス妨害等のコンピュータセキュリティインシデント（人為的事象）について、日本国内のサイトに関する報告の受け付け、対応の支援、発生状況の把握、手口の分析、再発防止のための対策の検討や助言などを、技術的な立場から行なっている特定の政府機関や企業からは独立した中立の組織。

【３】　偽の警告画面を表示させ有償版の購入を促し、クレジットカード番号を入力させる「偽セキュリティソフト」などの手口

本手口に関する相談は 2012 年 354 件、2013 年 889 件と、昨年は一昨年の 2.5 倍の相談がありました。「偽セキュリティソフト」を用いた手口では、改ざんされたウェブサイトなどをセキュリティ対策が不十分なパソコンで閲覧した場合に、勝手にパソコンに「偽セキュリティソフト」がインストールされ、実際には感染していないのに“ウイルスに感染している”という脅しの画面を表示し、解決のためと偽って有償版の購入を促します。

また、新しい手口ではありませんが、パソコン内のデータを暗号化し、パソコン自体を使えない状態にし、環境を復元することを条件に金銭を要求するランサムウェアと呼ばれるウイルスに関する相談が、2013 年 8 月になって再び寄せられるようになり、2013 年 1 年間の件数は 22 件でした（図 2 参照）。

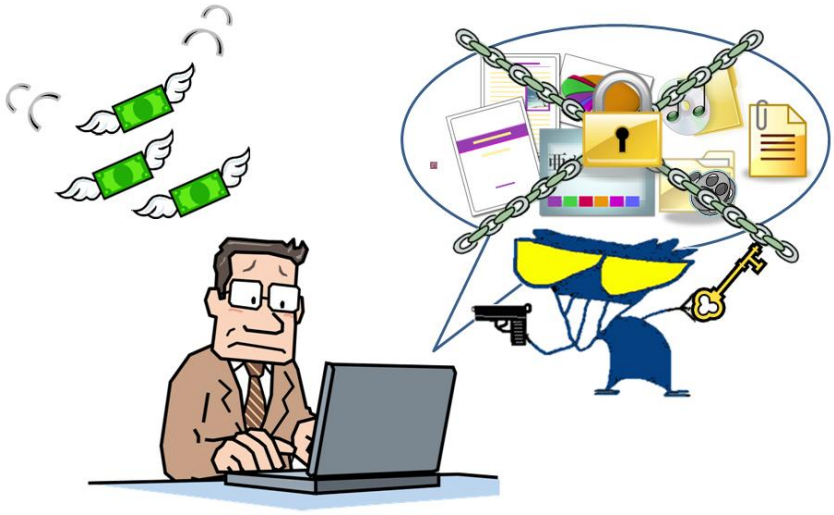

図 2：ランサムウェアによる被害のイメージ図

（ご参考）
IPA　2013 年 4 月「今月の呼びかけ」
「 どうして偽セキュリティ対策ソフトがインストールされるの？ 」
～基本的な対策を知って、慎重にネットサーフィンしよう～
http://www.ipa.go.jp/security/txt/2013/04outline.html

【４】　従来の対策では見抜くことが難しい、スマートフォンのワンクリック請求アプリ

スマートフォンのワンクリック請求でも 2013 年は新たな手口が出現しました。

新たな手口では、アプリのインストール時のアクセス権限確認では不審な権限許可を求めることはありませんが、アプリ内に設定されたアダルトサイトを表示し、画面に従って登録を完了すると請求画面を表示するというものでした（図 3 参照）。また、このアプリは公式マーケット上で公開されていました。

この手口は、不正なアプリをダウンロードしないための注意点である①正規のマーケットから入手する、②アクセス権限（パーミッション）を注意深く確認する、という従来の判断基準が通用しないのが特徴です。

もっともこの場合、アプリ自体が情報を盗み取るわけではなく、慌てずにアプリを削除するだけで復旧することができます。

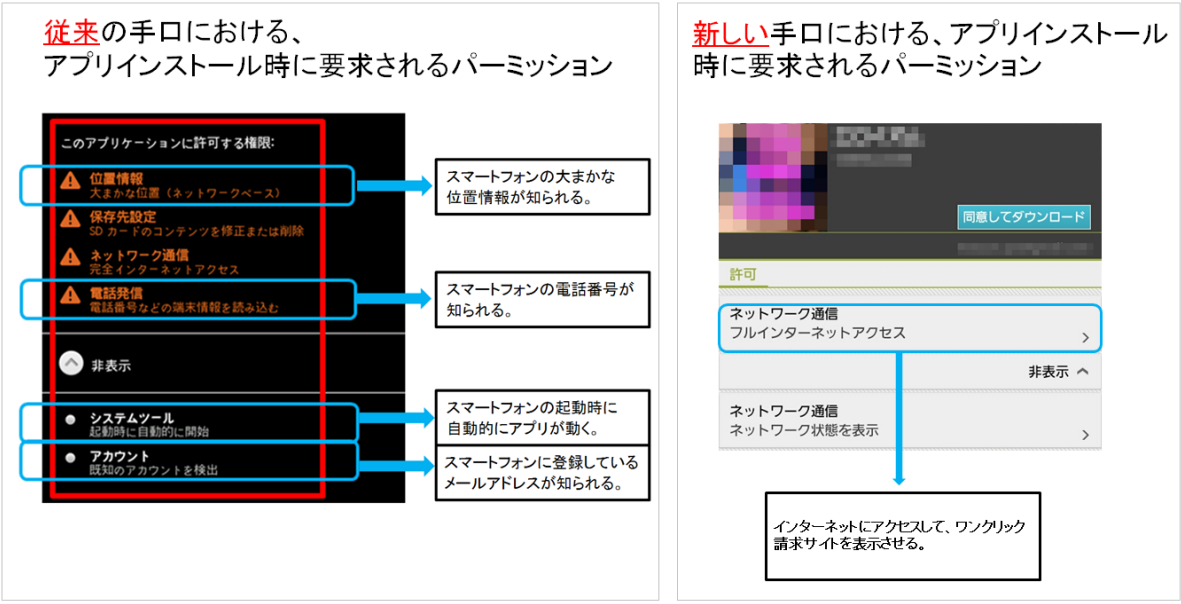

図 3：スマートフォンのワンクリック請求における新旧手口の比較

（ご参考）
IPA　2013 年 3 月「今月の呼びかけ」
「 公式マーケット上の不正なアプリに注意！ 」
～不正なアプリをインストールしないために～
http://www.ipa.go.jp/security/txt/2013/03outline.html

IPA　2013 年 5 月「今月の呼びかけ」
「 スマホにおける新たなワンクリック請求の手口に気をつけよう！ 」
http://www.ipa.go.jp/security/txt/2013/05outline.html

（２） 被害に遭わないための対策

【１】 日頃から用心するべきこと

以下に掲げる項目を、日頃から常に行い、用心する必要があります。

○出所が不明なファイルをダウンロードしたり、ファイルを開いたりしない

得体の知れないファイルを実行してウイルスに感染することは、道端に落ちている食べ物を拾い食いしてお腹を壊すことに似ています。非常に危険ですので出所の不明なファイルをダウンロードして実行するのはやめましょう。

○安易に URL リンクを開かない

メールやインターネットの掲示板、SNS や見知らぬブログなどの投稿文に書かれている URL リンクの中には悪意のあるサイトに誘導するリンクも存在します。このようなリンクを開いた場合、ワンクリック請求サイトやフィッシングサイトへの誘導、ウイルス感染、不正アプリのインストールなどの被害に遭う可能性があります。

○重要なデータのバックアップ

ウイルス感染の被害に備えるという目的のためだけでなく、自然災害、操作ミス、コンピュータの物理的破損など、予測不可能なトラブルが起こった場合への備えとして、重要なデー

タを定期的にバックアップしておくことが重要です。これにより速やかな修復が可能となります。

【２】 基本的な予防策

次の**二点は必ず実施**してください。

◯セキュリティソフトを導入し、ウイルス定義ファイルを常に最新に保つ。

◯パソコンやスマートフォンの OS やアプリケーションソフト（特に Adobe Flash Player、Adobe Reader、Java）を最新版に更新して脆弱性を解消する。

（ご参考）

「Windows Update 利用の手順」（日本マイクロソフト）
http://www.microsoft.com/ja-jp/security/pc-security/j_musteps.aspx

「サポート – ダウンロード」（アップル）
http://support.apple.com/ja_JP/downloads/

「iOS：iPhone、iPad、iPod touch をアップデートするには」（アップル）
http://support.apple.com/kb/ht4623?viewlocale=ja_JP

「MyJVN バージョンチェッカ」（IPA）
http://jvndb.jvn.jp/apis/myjvn/#VCCHECK

※ Android OS のバージョンアップの詳細については、各端末メーカーにご確認ください。

【３】 年に一度は普段使用しているメーカー以外の無料ツールでウイルスチェックを行う。

主なセキュリティベンダは有償版製品の他、無料オンラインスキャンツールも提供しています。普段使用しているメーカー以外のツールを選び、年に一度は、パソコン内のウイルスチェックを行うことで、ウイルスが検知されることがあります。

※ ご利用にあたっては、商用利用の可否など利用条件や、使用するための前提条件、要件をご確認ください。

（ご参考：各社の無料オンラインスキャンツール）

「エフセキュア オンライン スキャナ」（エフセキュア）
http://www.f-secure.com/ja/web/home_jp/online-scanner

「オンラインウイルススキャン」（カスペルスキー）
http://www.kaspersky.co.jp/security-scan

「SpyRescue オンラインスキャナ」（ネクステッジテクノロジー）
http://www.shareedge.com/spywareguide/txt_onlinescan.php

「パンダ フリーオンラインスキャン」（PS Japan）
http://www.ps-japan.co.jp/homeuser/content0001.html

「Virus Removal Tool」（ソフォス）
http://www.sophos.com/ja-jp/products/free-tools/virus-removal-tool.aspx

「オンラインスキャン」（トレンドマイクロ）
http://safe.trendmicro.jp/products/onlinescan.aspx

※ IPA では、個別製品の推奨は行っておりません。上に列挙した製品は、参考として示したものであり、これらのみを推奨しているわけではありません。また、各製品やサービスについては、それぞれの提供元へお問い合わせください。

■お問い合わせ先
IPA 技術本部セキュリティセンター 加賀谷／田中
Tel:03-5978-7591 Fax:03-5978-7518
E-mail: isec-info@ipa.go.jp