Information-technology
Promotion
Agency, Japan

第 13-02-271 号
2013 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

**「 ウイルスの　ゴールをゆるすな　たよれるキーパー　セキュリティ※1 」**

※1 第8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2012 標語部門
最優秀賞　　酒井　七星さん（兵庫県　伊丹市立南小学校）の作品

2012 年は、ウイルス感染による個人情報や金銭の窃取被害が多い年でした。また、感染したウイルスが、インターネットを使って殺人予告などの投稿を勝手に行ったため、パソコンの持ち主の知らない所で事件に巻き込まれてしまう事案も起こりました。以下に、2012 年にウイルスや不正アプリが原因で起こった主な事案を示します。

●ウイルスが表示する偽の警告が原因で偽セキュリティソフトを購入してしまった（2 月）
●Android 搭載スマートフォンの電話帳情報が窃取されてしまった（4 月、8 月）
●パソコンを遠隔操作されて知らないうちに事件に巻き込まれてしまった（10 月）
●インターネットバンキングの口座から現金が窃取されてしまった（11 月）

上述事案は、いずれもウイルスや不正アプリが原因で引き起こされたものですが、原因がわかっているものについては**特に目新しい手口はなく、日頃から基本的なセキュリティ対策を十分に行っていれば防ぐことができた被害ばかり**でした。また、**手口が不明なものでも注意を怠らなければ被害に遭うことが避けられた**と考えられます。しかし、脆弱性（ぜいじゃくせい）が悪用されたほか、**利用者をだます手法が巧みになった**ため、多くの利用者が被害に遭ってしまったと考えられます。
今月の呼びかけでは、2012 年に起こったウイルスや不正アプリ被害の傾向を解説し、それを元に被害に遭わないための対策や心がけを示します。

## （1） ウイルスや不正アプリ被害の傾向

### 【1】日本語による偽の画面を使った巧みな犯行

これまで海外で流行していた既存のウイルスを、英語表示のまま流用したり、不自然な日本語を使って改造したウイルスが多かったため、感染前に利用者が気づくことも多かったのですが、最近では日本人が見ても違和感のない日本語表示を使うウイルスを用いるため、感染被害が増えました。

最近確認されたインターネットバンキングの情報を窃取するウイルスは、感染すると利用者は正規のサイトにアクセスしているつもりでも、実際は本物に似せた偽の画面が表示されてしまい、利用者は偽の画面と気づかずに情報を入力してしまいます。

海外ではこのようなインターネットバンキングを狙うウイルスが以前からありましたが、今回の事例からも日本が本格的に狙われてきたと言えます。

（ご参考）
「ネット銀行を狙った不正なポップアップに注意！」（IPA　2012 年 12 月「今月の呼びかけ」）
http://www.ipa.go.jp/security/txt/2012/12outline.html

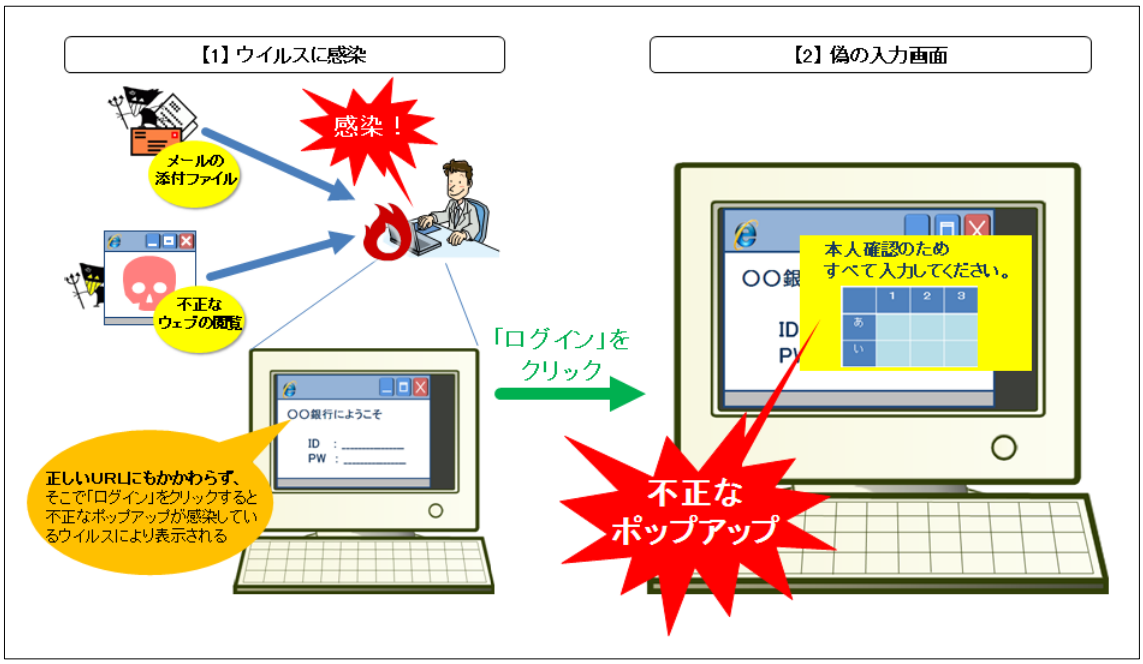


図 1：不正なポップアップ画面を出現させる手口のイメージ図

**【2】継続する「偽セキュリティ対策ソフト」型ウイルスの脅威**

「偽セキュリティ対策ソフト」型ウイルスは、"ウイルスに感染している"、"ハードディスク内にエラーが見つかりました"といった偽の警告画面を表示し、それらを解決するためとして、クレジットカード番号を入力させて有償版製品の購入を迫るウイルスです。

感染すると、二つのウイルスを感染させて、片方が駆除されても他方が同じ様に偽の警告画面を表示するものや、ウイルス自身が消されないように、スタートメニューの一部の機能を表示させなくするもの、デスクトップ上にあるアイコンを消したり、ファイルやフォルダを「隠しファイル」表示に設定し、あたかもパソコンに不具合が生じて保存していたはずのファイルが消えたように見せかけたりするものなど、さまざまな手法を使って有償版製品の購入を迫ってきます。

（ご参考）

「今なお続く、偽の警告を出すウイルスの被害！」（IPA　2012 年 3 月「今月の呼びかけ」）

http://www.ipa.go.jp/security/txt/2012/03outline.html

**【3】Android の情報を狙った不正アプリの増加**

2011 年に入ってから、増加の一途をたどっている Android に感染するウイルスや不正アプリですが、2012 年は Android 搭載スマートフォンなどの電話帳を狙った不正アプリが流行していたと言えます。

これは、人気のアプリ名や、実用性のあるアプリ、最新のアプリなどとかたってダウンロード・インストールさせようとするものでした。

インストールさせるまでの手口としては、便利なツールと偽った不正なアプリがあるサイトへ誘導する文章が書かれたメールの送信や、SNS（ソーシャルネットワーキングサービス）のコミュニティサイトに、興味を引く内容とともに不正なアプリがあるサイト URL を投稿することで、相手をうまくだましてインストールさせようとするものが目立ちました。

また、スマートフォン内の電話帳の情報を狙った不正アプリが公式のマーケットサイトからダウンロードが可能な状態だったこともありました。公式マーケットに置かれていたため、安心してダウンロードしてしまった多くの利用者が、情報窃取の被害に遭いました。

ウイルスや不正アプリではありませんが、SNS アプリをインストールし、電話帳利用を許可することで電話帳が窃取されるといった被害は、Android 搭載機に限らずスマートフォン全般で注意が必要です。

最近では、ダウンロード画面に「“利用規約”」を準備するような不正アプリもでてきているためより一層の注意が必要です。

（ご参考）
「スマートフォンでもワンクリック請求に注意！」（IPA　2012 年 2 月「今月の呼びかけ」）
http://www.ipa.go.jp/security/txt/2012/02outline.html
「あなたを狙うスマホアプリに要注意！」（IPA　2012 年 5 月「今月の呼びかけ」）
http://www.ipa.go.jp/security/txt/2012/05outline.html
「情報を抜き取るスマートフォンアプリに注意！」（IPA　2012 年 9 月「今月の呼びかけ」）
http://www.ipa.go.jp/security/txt/2012/09outline.html


図 2：不正なアプリが情報を流出させるイメージ図

**【4】便利なツールに見せかけてインストールさせるウイルスの脅威**

「便利なツールです。こちらからダウンロード」などと掲示板やメールなどで紹介されたツールをダウンロードすると、実際にはウイルスが中に仕込まれており、それをインストールすることで感染被害に遭ってしまうという、ウイルス感染の手口としてはかなり昔からあるものです。

しかし 2012 年 10 月には、こうした手口で感染したウイルスが「遠隔操作」を行うものだったため、いつのまにか感染被害の利用者が事件に巻き込まれてしまう事案が起こりました。

（ご参考）
「濡れ衣を着せられないよう自己防衛を！」（IPA　2012 年 11 月「今月の呼びかけ」）
http://www.ipa.go.jp/security/txt/2012/11outline.html


【1】から【4】の傾向としては次のようなことが言えます。
・被害に遭ったことで、機器等の初期化をせざるを得ないほどの重篤な症状をもつものがあった。
・重要な情報や金銭が窃取され、取り返しのつかない被害に遭うケースがあった。
・ウイルスを感染させたり、不正アプリをインストールさせたりするために、人間の心理を突いた「だましのテクニック」を駆使するケースがあった。
・利用者が少し注意していれば、感染を防ぐことが出来たかもしれないケースがあった。

このようなことにならないためには、基本的な対策を怠らないことと、普段からセキュリティに対する心がけを忘れないことが重要です。

## （2） ウイルスや不正アプリの被害に遭わないための対策

### 【1】日頃から心がけること

以下に掲げる項目は、日頃より持続的なセキュリティ対策として心がけることが重要です。

**○重要なデータのバックアップ**

ウイルス感染の被害や自然災害、操作ミスや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に備えて、**重要なデータを定期的にバックアップ**しておくことで速やかな修復が可能となります。ただし、バックアップデータから戻す場合は、事前に必ずウイルスチェックを行ってください。

**○出所の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。それと同様に**出所の不明なファイルをダウンロードして実行することは非常に危険**です。安易にダウンロードしたり、ファイルを開いたりすることは避けてください。

**○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 などの投稿文に書かれている URL リンクを安易に開くことは危険です。これらのリンクの中には**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に誘導されたり、場合によっては開いただけでウイルスに感染したり、不正アプリがインストールされることがあります**ので、安易に URL リンクを開くのは避けてください。

**○自分が管理していないパソコンやスマートフォンから ID／パスワードを入力しない**

インターネットカフェなどにあるパソコンや、自分の物ではないスマートフォンなどは、**ID／パスワードを窃取するウイルスに感染しているかも知れません。**そのようなパソコンやスマートフォンから、自分の ID／パスワードを入力して利用するウェブサイトやサービスにアクセスすることはできるだけ避けてください。

**○自分が管理していないパソコンに自分の USB メモリなどの外部媒体を接続しない**

自分の USB メモリを自分が管理していないパソコンなどに接続すると、**USB メモリがウイルスに感染したり、USB メモリの中にある情報をウイルスに窃取**されてしまうかもしれないので、接続はしないでください。同様に自分が管理していない USB メモリを自分のパソコンなどに接続しないでください。また、充電するつもりでスマートフォンなどをつなぐと、USB メモリのようにファイルシステムとして認識され、同じようなことが起きることもありますので、注意してください。

**○ファイルの拡張子を表示させる**

ファイルの拡張子（.exe や.txt など）やアイコンを偽装して、別のファイルに偽装してファイルを開かせることでウイルスに感染させようとする手口があります。こうした**偽装ファイルを見つけ出すため、ファイルの名前を拡張子まで全て表示させて、常にアイコンとそれに対応するファイルの拡張子に相違ないか意識し、ファイルのプロパティで本当のファイルの種類を確認すること**が大事です。

（ご参考）

「ファイル名に細工を施されたウイルスに注意！」（IPA　2011 年 11 月「今月の呼びかけ」）

http://www.ipa.go.jp/security/txt/2011/11outline.html

「ファイルを全て表示させる」（IPA）
http://www.ipa.go.jp/security/personal/base/mail/point3.html
「怪しいファイルを見分けよう」（IPA）
http://www.ipa.go.jp/security/personal/base/mail/point4.html

○**無線 LAN を適切な設定のもとに運用する**

**セキュリティ設定が不十分なまま無線 LAN 環境を使用していると、不正に悪用されてインターネット接続のただ乗りを許してしまう可能性**があります。暗号化方式など、適切なセキュリティ設定をするなどして、自宅の無線 LAN が犯罪のインフラとして利用されないようにしてください。

（ご参考）
「一般利用者が安心して無線 LAN を利用するために」（総務省）
http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000029.html
「一般家庭における無線 LAN のセキュリティに関する注意」（IPA）
http://www.ipa.go.jp/security/ciadr/wirelesslan.html
「犯罪インフラ対策プラン」（警察庁）
http://www.npa.go.jp/sosikihanzai/kikakubunseki/bunseki/taisakuplan.pdf

○**ニュースなどから情報収集をしておく**

最近では、コンピュータウイルスや不正アクセスによる事件が、ニュースでも大きく報道されるようになりました。そのような事件に、**もしかしたら自分自身もすでに巻き込まれているかもしれません。**そうしたニュースなどの**情報を日頃から収集しておくことは、万が一の際、適切な対処**をするために役立ちます。以下のサイトも参考にしていただき、日頃からニュースサイトなどを閲覧してセキュリティ意識を高めてください。

（ご参考）
「今月の呼びかけ」（IPA）
http://www.ipa.go.jp/security/personal/yobikake/index.html
「ここからセキュリティ！」（IPA）
http://www.ipa.go.jp/security/kokokara/

**【2】予防策**

○**基本的な対策**

基本的な対策は次の二つになります。**この二つは最低限実施**してください。

・**ウイルス対策ソフトを導入し、ウイルス定義ファイルを最新に保ちながら使用**します。
・**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、できる限り最新版に更新して脆弱性を解消**しておきます。

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

○**万が一の為の出口対策**

万が一、気づかないうちにウイルス感染や不正アプリをインストールされた場合、**自分の情報が外部に漏れていくことを防ぐための予防策として、パーソナルファイアウォール※の導入による出口対策をお勧めします。**パーソナルファイアウォールの設定より自分が許可したプログラムだけを外部との通信可能とし、ウイルスや不正アプリが行う通信を防ぐことで、感染したとしても情報が外部の第三者に窃取されるなど最悪の状態を防ぐようにします。

※パーソナルファイアウォール：
個々の端末（パソコンやモバイル機器など）に導入するもので、端末と外部ネットワークの間の通信を制御するソフトウェアです。通常、“事前に許可した通信以外を通過させない”、“許可するプログラムを事前に登録しておき、未許可のプログラムの通信を遮断する”といった機能を持ちます。OS の機能として組み込まれているほか、製品単体としても販売されていますが、「統合型セキュリティソフト」と呼ばれる製品の中にパーソナルファイアウォール機能を併せ持つものもあります。

**【3】パソコンも年に一度は他社のウイルス対策ソフトで定期健診を！**

**最新のウイルスや不正アプリは一種類のウイルス対策ソフトだけでは見つからない**こともあります。**最低一年に一度は、普段お使いのウイルス対策ソフトメーカ以外のウイルス対策ソフトを使い、パソコン内のウイルスチェック**をお勧めします。この場合、一例となりますが**複数社の無料オンラインスキャンツール**（※）を使うなどすると良いでしょう。

※ 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。既にウイルス対策ソフトがインストールされている環境に、他のセキュリティ対策製品をインストールすると、パソコンの動作が不安定になることがあります。なお、IPA では、個別製品の推奨は行っておりません。下記列挙した製品は、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の質問は、それぞれの提供元へお問い合わせください。

（ご参考）
「 Symantec Security Check」（シマンテック）
http://security.symantec.com/sscv6/home.asp?langid=jp&venid=sym&plfid=23
「トレンドマイクロ オンラインスキャン」（トレンドマイクロ）
http://safe.trendmicro.jp/products/onlinescan.aspx
「SpyRescue オンラインスキャナ」（ネクストウェッジテクノロジー）
http://www.shareedge.com/spywareguide/txt_onlinescan.php
「パンダ フリーオンラインスキャン（Active Scan2.0）」（パンダ）
http://www.ps-japan.co.jp/homeuser/content0001.html

**■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／青木
Tel:03-5978-7591 Fax:03-5978-7518
E-mail: isec-info@ipa.go.jp