第 12-30-265 号
2012 年 11 月 1 日
独立行政法人情報処理推進機構

今月の呼びかけ

「 濡れ衣を着せられないよう自己防衛を！」
～　踏み台として悪用されないために　～

便利なソフトウェアをダウンロードしたはずが、仕掛けられたウイルス感染し、自治体や掲示板サイトへの殺人予告や破壊予告などの投稿を勝手に実行された、という一連の事件が連日報道されています。この一連の事件は、自分のパソコンがウイルスに感染した場合、何かしらの犯罪に巻き込まれてしまう可能性があることを具体的に示すものでした。

IPA ではこれまで様々な呼びかけを行ってきましたが、今回の事件をうけて、ウイルス感染から身を守るための対策を、原点に立ち返って改めて呼びかけます。

（1）　IPA の届出制度により入手した遠隔操作ウイルスの概要

「一般利用者が遠隔操作ウイルスに感染するまで」と、ウイルス感染後の「攻撃者による遠隔操作」に分け、それぞれ図 1 と図 2 に示します。

▼一般利用者がウイルスに感染した仕組み（図 1 の解説）

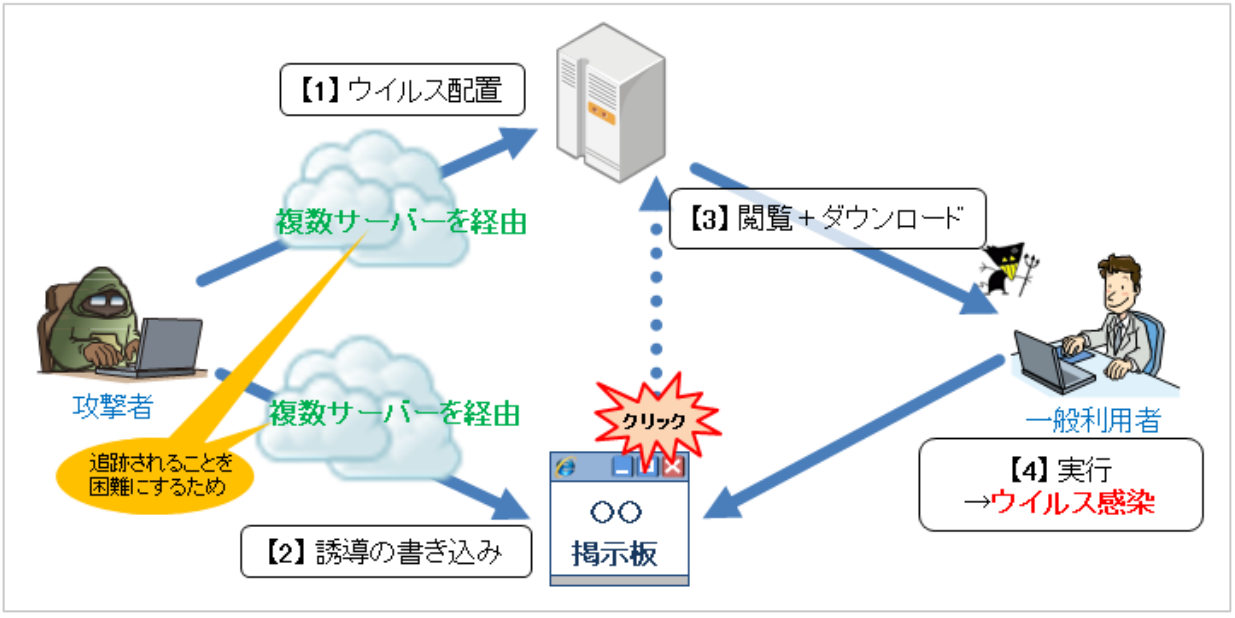

図 1：遠隔操作ウイルスに感染するまでのイメージ図

【1】ウイルス配置

攻撃者が、インターネット上のあるサーバーにウイルスを仕掛けたソフトウェアを配置します。この時攻撃者は、自身への追跡を困難にするために複数のサーバーを経由していると考えられます。

【2】誘導の書き込み

攻撃者が、誰でも閲覧が可能な掲示板に、【1】で配置したウイルスの場所（URL）を書き込みます。この時攻撃者は【1】と同様、自身への追跡を困難にするために複数のサーバーを経由していると考えられます。

【3】閲覧、ダウンロード

【2】の書き込みを読んだ一般利用者が、掲示板に書き込まれたリンク（URL）をクリックすると、ウイルスがパソコン内に保存されます。この時点ではまだパソコンはウイルスに感染していません。

【4】実行（その結果ウイルスに感染）

【3】で保存したファイルを「実行」したことにより、遠隔操作ウイルスに感染してしまいました。

▼ウイルス感染後の遠隔操作の仕組み（図 2 の解説）

IPA の届出制度により入手した「遠隔操作ウイルス」は、攻撃者から直接操作されるものではなく、間接的に操作をされるタイプのものでした。

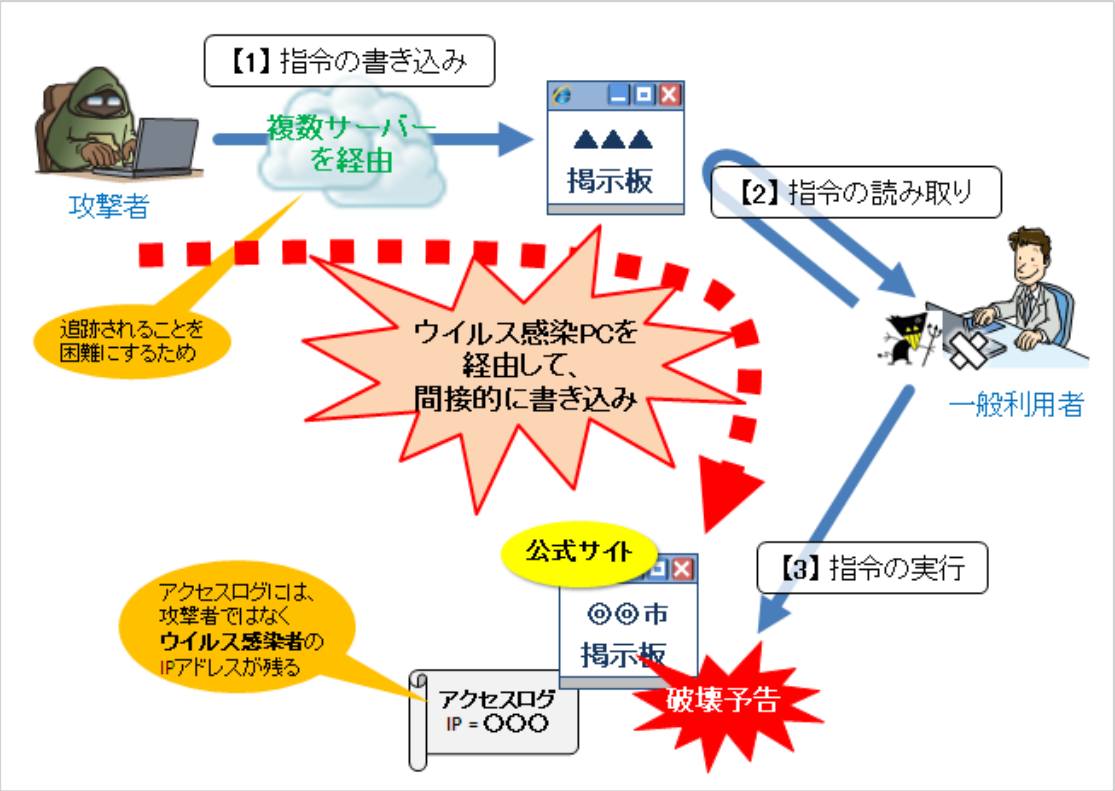

図 2：攻撃者が遠隔操作を行うイメージ図

【1】指令の書き込み

攻撃者が別の掲示板に、ウイルス感染パソコンへの指令に相当する文字列を書き込みます。この時攻撃者は、自身への追跡を困難にするために複数のサーバーを経由していると考えられます。

【2】【3】指令の読み取り、指令の実行

遠隔操作ウイルスが感染したパソコンから【1】の掲示板の特定のページを定期的にチェックします。そして自身への指令に相当する文字列を発見すると、その指令を実行します。

（2） IPA に届け出られたウイルスの簡易調査結果

IPA は、今回の一連の事件で使用されたものと同じと思われる遠隔操作ウイルス（chikan.zip）を入手しました。調査の結果、現時点で下記の動作をすることが判明しています。

1. パソコンの利用者が、「文字置換ソフト」という触れ込みで配布されていた chikan.zip をダウンロードして解凍すると、chikan.exe と data という 2 つのファイルが生成されます。

2. さらに 1.で生成された chikan.exe を実行すると、iesys.exe と cfg.dat という 2 つのファイルが生成されます（図 3－①）。これは、通常のソフトウェアの「インストール」に相当します。また、それと同時に chikan.exe が削除され（図 3－②）、1.で生成された data を chikan.exe にファイル名変更します（図 3－③）。

“cfg.dat”には、ウイルスが指令を読み取りに行く際、掲示板の中のどの「ページ」を参照するかが記述されていました（図 3－④）。当然ウイルス作成者である攻撃者は、当該ウイルスが参照する「ページ」がどこなのかを把握しているので、攻撃者がその「ページ」に指令を書き込んだことにより、実際に犯罪予告が書き込まれたものと考えられます。

また“cfg.dat”の内容を書き換えることで、ウイルスが指令を読み取りに行く「ページ」を容易に変更できます。「ページ」を変更したウイルスを別の利用者にダウンロードさせることで、攻撃者は対象者を特定した形で、用途と目的に応じて指令を出すことが可能です。

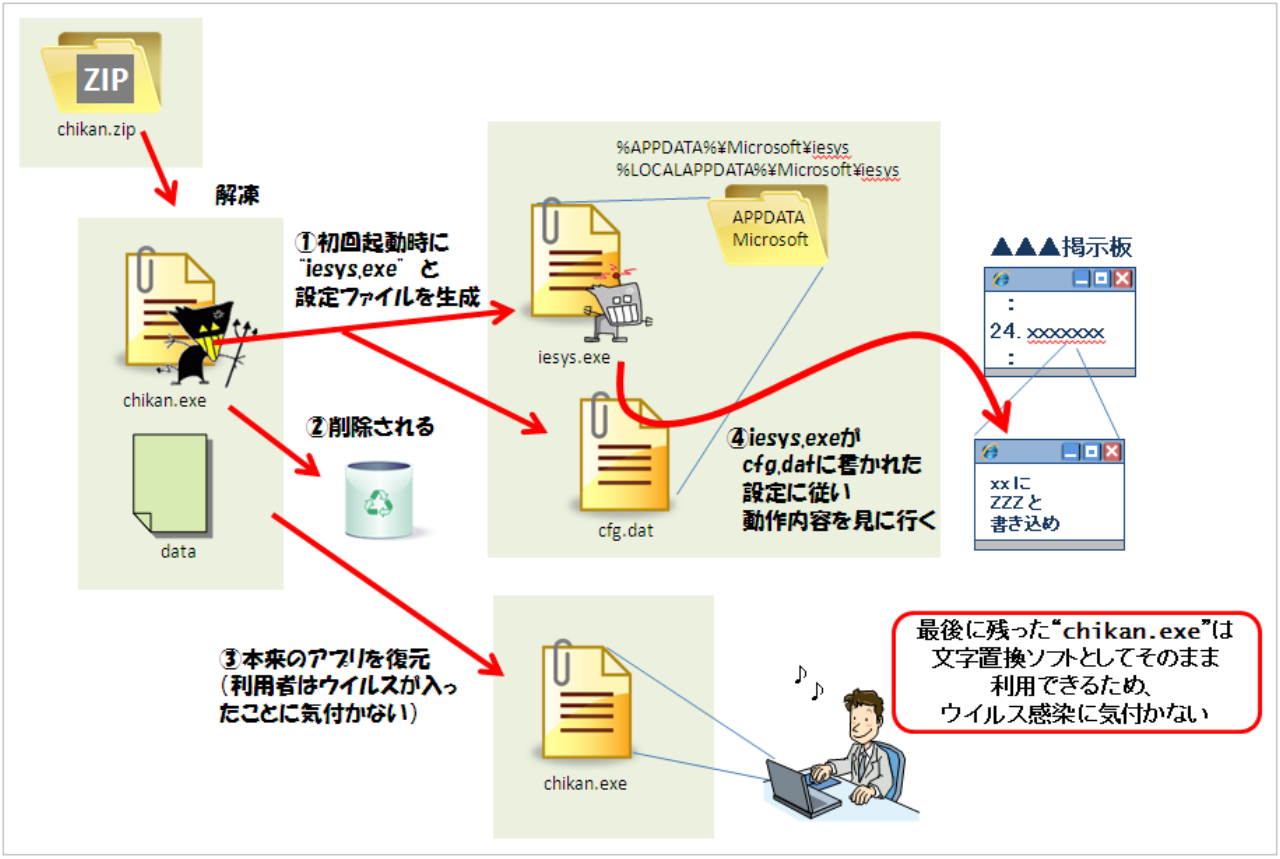

図 3：“chikan.zip”の挙動のイメージ図

（3）対策

このようなウイルスに感染しないためには、以下の基本的な「心掛け」と「対策」が重要です。

基本的なことではありますが、それゆえに少しでも疎かにすると非常に危険です。常に肝に銘じてください。

心掛け 1　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。それと同様に得体の知れない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。

インターネット上で URL リンクされているファイルは勿論のこと、知らない送り主からメールに添付されたファイル等も巧妙に偽装されたウイルスプログラムである可能性があります。**出所不明のファイルは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。**

心掛け 2　安易に URL リンクをクリックしない

インターネットの掲示板等に掲載された投稿には、「絶対に儲かります」など“美味しい話”と一緒に、URL リンクが貼り付けられているものがあります。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。この様なリンクをクリックした場合、**アダルトサイトやフィッシングサイトに誘導されたり、場合によってはクリックしただけでウイルスに感染することがありますので、安易に URL リンクをクリックするのは避けてください。**

基本的対策

確実に行うべき基本的な対策は次の 2 つです。

●使用しているパソコンの OS やアプリケーションなどの脆弱性を解消する

OS や、インストールされているアプリケーションソフトウェアには、最新の更新プログラムを適用して、脆弱性（セキュリティ上の弱点）を解消してください。定期、あるいは緊急に更新プログラムが発表されますので、発表された場合にはすぐに更新プログラムを適用してください。

IPA では、利用者のパソコンにインストールされている主なソフトウェア製品のバージョンが最新であるかを、簡単な操作で確認するツール「MyJVN バージョンチェッカ」を公開しています。是非ご利用ください。

・MyJVN バージョンチェッカ（IPA）
http://jvndb.jvn.jp/apis/myjvn/vccheck.html

●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する

ウイルス対策ソフトは万能ではありませんが、重要な対策の一つです。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つことで、ウイルスの侵入阻止や、侵入してしまったウイルスを駆除することができます。近年のウイルスは、パソコン画面の見た目からでは感染していることが分からないものも多いため、ウイルスの発見と駆除には、ウイルス対策ソフトが必須です。

一般利用者向けのウイルス対策ソフトとしては、ウイルスの発見と駆除だけでなく、危険なウェブサイトを閲覧しようとした時にブロックを行う機能などを備える、「統合型」と呼ばれるものを推奨します。

一歩進んだお勧めの対策

●パーソナルファイアウォール※1 を適切に設定して使用する

パーソナルファイアウォールを導入し、設定を厳しくして自分が許可したプログラムだけを通信可能とすることにより、**万が一ウイルスに感染してしまっても、そのウイルスが外部と通信することを防ぎ、さらにはウイルスの存在に気付くことができる可能性があります。**

※1 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。
製品単体としても販売されていますが、「統合型ウイルス対策ソフト」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合わせ持つものもあります。

●証拠を保全する試み

万が一遠隔操作ウイルスに感染して、外部への攻撃に利用されてしまった場合、その時の証拠が残っていないとパソコンの利用者が嫌疑をかけられる等の恐れがあります。特に真犯人が証拠隠滅を目論んで遠隔操作ウイルス自体を消去してしまうと、証拠が完全に失われる恐れがあります。

パソコン上のプログラムの動作記録や通信記録を残しておくことで、それが証拠になり得ることが考えられます。

パソコン上での全ての動作を記録することは困難ですが、Windows OS に標準に備わっている「Windows ファイアウォール」や、セキュリティ対策ソフトのログ機能※2などを用いることである程度の記録を取得することができます。

※2 セキュリティ対策ソフトのログ機能：
詳細につきましては、ご利用のセキュリティ対策ソフトの説明書をご覧いただくか、サポートセンターなどにお問い合わせの上ご確認ください。

（4）こんなときは…

遠隔操作ウイルスを検知してしまった、ウイルスに感染しているかもしれない、などがありましたら、IPA 安心相談窓口までご連絡ください。

まずは、ご相談ください。

	安心相談窓口の問合せ先
電話	03-5978-7509 （オペレータ対応は、平日の 10:00～12:00 および 13:30～17:00）
E-mail	anshin@ipa.go.jp ※このメールアドレスに特定電子メールを送信しないでください。
FAX	03-5978-7518
郵送	〒113-6591 東京都文京区本駒込 2-28-8 文京グリーンコート　センターオフィス 16 階 IPA セキュリティセンター「情報セキュリティ安心相談窓口」宛

■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