不正なプログラムも仕組みを理解すれば怖くない　IT推進コラム②

IT推進委員会
副委員長　前田　守（沼津柿田川RC）

今年IT推進委員会の副委員長を務めさせていただいている前田です。

いよいよ地区でもインターネットを利用した事務の効率化が7月から始まり4ヶ月が経過しました。この4ヶ月の間で、ウイルスやワーム感染、迷惑メール等いくつかの問題で困っている事務局の方が多いとの声を多く耳にしました。私も仕事柄、不正プログラムの感染による駆除や予防方法についての相談を日常的に受けます。

確かにインターネットは注意を怠れば被害を受けることがあります。

その被害を回避するためには、企業での運用と同じように重要なファイルは外部のハードディスク（移動後ケーブルを切り離す）やCD等の別媒体に移動させる、重要なファイルには暗号化するなどの方法が考えられます。

不正なプログラムはどのような仕組みになっているのでしょうか？

ここで不正なプログラムの仕組みについて少しお話しします。

（現在はWindowsユーザーが主流なので、ここではWindowsに限定させて頂きます）

不正プログラムの代表的なものには、「ウイルス」「ワーム」「スパイウェア」があります。

「ウイルス」は、ブートファイルやプログラム、データファイルなどに寄生するもので、それ自体ではパソコン上に存在できないものです。

「ワーム」は、それ自身が独立して存在でき、増殖することができます。

「スパイウェア」（迷惑メール含む）は、悪意をもって他人のパソコン内の情報を持ち出す行為を実行し、パソコンの所有者に気付かれないように活動を開始します。

「なんだかパソコンの起動が極端に遅くなった・・・」「ソフトを使用中に突然パソコンの処理が遅くなる・・・」そんな現象が現れた時には、皆さんの知らない間に情報は外部へ送信されている可能性があります。

では、スパイウェアの手口についてもう少しふれてみましょう。その手口はさまざまです。Windowsに潜り込む為に、不正プログラムが利用する技術の多くが「Cookie」、「ActiveXコントロール」、「レジストリ」等から実行されています。

[Cookie]　WebサーバがWebブラウザとの間で情報を受け渡しするために接続した
Webブラウザに読み込ませるテキストデータです。

[ActiveXコントロール]
Windows用のソフトウエアの一部で、Webサーバから接続したWebブラウザに対しActiveX命令が実行されます。

[レジストリ]
Windowsのシステムやアプリケーションの設定情報等が保存しているデータベースです。

これらは何れも、Windowsやインターネットを便利にするために開発された技術です。

一つの例ですが、レジストリ情報を持ち出すものにはWebサイトに仕掛けられていることも多くあります。Webサイト内のあるボタンをクリックするとプログラムが実行され、レジストリの特定の場所にあるメールアドレスの情報を盗み出し外部へ送信します。サイト内の「確認」ボタンなどに悪意あるプログラムが埋めこまれているケースです。（悪意をもったサイト以外に、セキュリティ管理の甘いWebサイトが侵略されているケースも多いです）ボタンをクリックさせパソコンに実行ファイルを送り込みます。（アダルトサイトは「年齢認証」「18歳以上」とボタンに埋め込まれている場合も多いです）このファイルが実行されてしまうとプログラムが起動して、メールソフトに登録してあるコンピュータ名、ユーザー名、メールアドレス等を収集すると同時にレジストリの情報を自分で書き換えWindows起動時に自動実行させる情報を書き込み、Windowsを起動する度に実行されてしまうのです。その後は、取得したメールアドレスを特定なサイトに送信します。これらのスパイウェアは、

ホームページの見るためのシステムであるHTTPやメール送信システムのSMTPのポート（通り道のようなもの）を利用しており、ルータやファイアウォール設定でポートの制限をしていてもほとんどが通過してしまいます。

どのようなことに注意すればよいのでしょうか。

まず、最低限の備えとして最新のWindowsシステムアップデートとセキュリティ対策ソフトを導入して下さい。最新のWindowsセキュリティ対策ソフトには「ウイルス」「スパイウェア（迷惑メール）」「ファイアウォール」「フィッシング」「広告ブロック」対策等多くのセキュリティ機能が一つのパッケージになっています。但し、セキュリティ対策ソフトがインストールされているからといって安心してはいけません。
セキュリティ対策ソフト導入後であっても、下記の点に心がけてください。

1．Windowsアップデート、Microsoftアップデートはできるだけ速やかに行なう
※「スタートメニュー」の「すべてのプログラム」より「WindowsUpdate」を実行すればアップデートが開始します。自動アップデートの設定が可能です。
2．セキュリティ対策ソフトのアップデートはできるだけ速やかに行なう
※自動アップデートの設定が可能です。
3．WebブラウザへのCookieの受入れは信頼できるサイトのみを受け入れる
※信頼するサイトは自分自身で追加します。受け入れた場合でも終了する都度削除をお薦めします。
4．パスワードはブラウザやWindowsに記憶させない
5．Webブラウザのキャッシュは常にクリアする
6．JAVA 、JAVAScript、ActiveXコントロールには警告するように設定し、疑問に思ったらそのサイトではこれらを実行させない

これらを心がけることによって更に被害にあう可能性を下げることができます。

「WebブラウザはInternetExplorerでなくてもかまわない」という方には、ActiveXコントロールが標準では実行できないフリーのWebブラウザを使われることをお奨めします。下記のブラウザはCookieやキャッシュも終了時に自動削除が可能です。

Webブラウザ（フリーウエア）「Mozilla Firefox」ダウンロードサイト
http://www.mozilla-japan.org/
直接ダウンロード
http://www.mozilla-japan.org/products/download.html?product=firefox-2.0&os=win&lang=ja

もうひとつ、迷惑メールで悩んでいる事務局の方も多いかと思います。こちらも、セキュリティ対策ソフトを導入していただければ極端に少なくなります。しかし、迷惑メール対策機能が実装されているといっても全ての迷惑メールを排除できるわけではありません。フィルターをすり抜けて入ってくるメールも数多くあります。そこで、ワンクリックで迷惑メールフィルターに登録できるメールソフトウエアを利用してみるのも一つの方法です。下記のメールソフトには、迷惑メールフォルダへの移動や自動削除のできる機能が実装されています。

メールソフト（フリーウエア）「Mozilla Thunderbird」のダウンロードサイト
http://www.mozilla-japan.org/products/thunderbird/
直接ダウンロード
http://www.mozilla-japan.org/products/download.html?product=thunderbird-1.5.0.8&os=win&lang=ja

※各ソフトウエアの設定方法についてはサイト内の説明を良くお読み下さい。

インターネットはこれからもビジネスや生活に無くてはならないものです。
不正なプログラムも注意をはらえば怖くありません。インターネット環境を皆さんで便利に使いこなしていきましょう。