常時接続時代のネットワークセキュリティ

インターネットは高速低料金で常時接続が可能となり、動画配信などますます便利な環境となってきました。これからも色々な技術が開発され、ますます身近になってくると思います。しかし、この常時接続は便利という反面、大変恐ろしい「落とし穴」があることをしっかりと理解する必要があります。

今まで課金を気にしながら利用していたインターネットが高速常時接続となり、繋ぎっぱなしでも"まったく"気にしなくて良くなりました。
さて、ここでよく考えてみましょう。繋ぎっぱなしという事は"あなた"のコンピュータはその間、広大なインターネットの世界に接続され、どこからでも通信を行える状態になっているという事です。もし、あなたにセキュリティに関する知識が無ければ、既にあなたのコンピュータはクラッカー(*1)の標的になっているかも知れません。また、ウィルスに関する知識がなければ、既にウィルスに感染しているかもしれません。

(*1)クラッカーとは、悪意を持ってあなたのコンピュータのセキュリティ的に弱いところを攻撃し、あなたのコンピュータ内のデータを破壊したり、改竄したり、盗み見したり、乗っ取ったりする「盗人・悪人」のことです。

【Q】　どうすればいいの？　＜ウィルス編＞

まず、ウィルスに感染していないかチェックを行いましょう。
オンラインでウィルスチェックをしてくれるサイトがありますので、下記にご紹介します。

http://www.symantec.com/region/jp/securitycheck/index.html

http://www.trendmicro.co.jp/hcall/index.asp

上記サイトにて自分のコンピュータ内にウィルスがいないか検査してくれます。
もし感染していれば、上記サイトに「駆除ツール」もある程度ありますので、駆除しましょう。一番良い方法は、ウィルスチェックソフトを購入し、自分のコンピュータに入れておくことです。

【Q】　コンピューターウィルスって？

コンピューターウィルスは、ウィルスだからと言って人間に感染するものではありません。コンピューターウィルスという名前のとおり、コンピューターに感染します。

コンピューターウィルスは一般的に、

- 自己伝染機能（他のファイルに付着、もしくは自らをコピーする）
- 潜伏機能（一定の条件が揃うのを待つ）
- 発病機能（データの破壊などの実行）

という行動パターンを行うプログラム、と定義されています。

＊　参考資料：　通商産業省告示第４２９号
http://www.meti.go.jp/kohosys/topics/10000098/esecu07j.pdf

また、プログラムそのものに改竄を加えられたり、不正な動作を行うプログラムを送り込むといったものもあります。 現在ではこの様な手法をミックスした複合型がメジャーになってきています。
(例えばこんなウィルス　“Nimda”)
他にもマクロ機能（Excel 2000 などで、新規作成 -> 計算書 -> 納品書 と開くと「xxx はマクロを含んでいます」と出てきますよね？それです）を持つデータファイル、特にワードやエクセルをターゲットに「マクロ言語」で書かれた「マクロウィルス」といったものもあります。このウィルスは、マクロ機能を「有効」にしてファイルを開くと感染してしまいます。

要は、

「自分のパソコンや会社のパソコンに感染して悪さをするプログラムがいる。

これらに気をつけましょう！」

というお話です。

「悪さをする」とありますが、実際、具体的にはどんなことをするのでしょうか？
それは、ウィルスによって様々です。現実世界のウィルスも、種類によって「症状」が違うように、コンピュータウィルスも違うのです。

例えば...

ただ画面にメッセージを表示するだけのもの
音が鳴るもの
パソコンの動作を不安定にするもの
パソコンの中のデータを消してしまうもの

などなど。

「な〜んだ、それなら自分のパソコンには重要なデータは入ってないから大丈夫！」

「データのバックアップをちゃ〜んと取ってるから、消えてもいいや！」

と仰る方がいらっしゃいますが、それは違います！

近年流行っているウィルスには、パソコンの中からメールアドレスを収集して勝手にウィルスメールを送りつけたり、ウィルスを送りつけた上に、勝手にパソコンの中のファイルを添付して送信するものもあるのです！（例えばこんなウィルス　“KLEZ.E”　）

想像してみて下さい。

＃もし、ウィルスの送信先が大事な取引先だったら... ？！

＃もし、勝手に添付されたファイルが機密文書だったら... ？！

現実世界でも人に病気をうつすのはよくないことですが、パソコンでも同じです。
また、メールアドレスを収集して勝手にウィルスメールを送りつける... ということは、自分のメールアドレスを登録している人間が感染していたら、ウィルスメールが自分のところへ届けられるかもしれません。

以前はフロッピーを使ってファイルのコピーを行った時などによく感染していました。しかし、現在はインターネットを使うようになって、インターネット上から感染する事が多くなりました。

例えば...

＃受信したメールに付いていた添付ファイルを実行した時に感染する

＃問題点を修正されていないメールソフトでメールを開いた時に感染する

＃ホームページなどから、ファイルをダウンロードして実行した時に感染する

など、感染する機会は多いのです。
というわけで、インターネットに接続している方は他人事じゃありませんよ！

【Q】　ワクチンソフト、入れてます？

「ウィルス、ウィルスって騒いでいるけれど、自分のパソコンは
普通に動いてるし、大丈夫、大丈夫...」

本当に大丈夫でしょうか？いいえ、大丈夫ではありません！もしかしたら、あなたのパソコンにも既にコンピューターウィルスが潜んでいるかもしれません。
実は人の病気と同じで、コンピュータウィルスにも「潜伏期間」があるのです。感染してもしばらくは普通にパソコンは動作している（潜伏中）が、「特定の日時」になるとパソコンを「破壊」するのです。 （ここで、またまた登場！ “KLEZ.E” このウィルスは、奇数月の 6 日にファイルを破壊します。何度も出てきますが、それだけ騒ぎになったウィルスなんです！） という風に、今、自分のパソコンで何もおきてないから「安心」ということはありません。

では、どうする？

パソコン自体を隔離してしまいましょうか？
インターネットやファイルのコピーなんかしないで、 金庫にしまってお祓いをする... ？！
確かにそれならばコンピューターウィルスに感染しないでしょうし、もし、感染していたとしても問題は起こらないでしょう。でも、それではパソコンが使えないですよね。
ということで、コンピューターウィルスを検出・除去するために ワクチンソフト と言われるものが色々なメーカーから発売されています。

＊参考ソフト

シマンテック　Norton AntiVirus	http://www.symantec.co.jp
トレンドマイクロ　ウィルスバスター	http://www.trendmicro.co.jp
McAfee　VirusScan	http://www.nai.com/japan/mcafee/

これらのソフトは、パソコンショップや少し大きな家電量販店に行けば手に入るかと思います。
まだワクチンソフトを入れてない方は、今すぐ買ってインストールする事をお勧めします。
今すぐ！ （あ、決してワクチンソフトメーカーの回し者じゃないです。。。）

さて、言われた通り(?)ワクチンソフトを買ってきてインストールしました。

「よし、これでウィルス対策は万全だ！」

でも、本当にそれで大丈夫？　いいえ、大丈夫ではありません。
インストールしただけの状態では、そのワクチンソフトが元々知っているウィルスの検出と除去しかできないのです。でも、新しいウィルスは次々と出てきます。

「えーーーっ！！！それじゃ、意味ないじゃん！」

そうなのです。インストールしただけの状態では意味がないのです。そこで、新しいウィルスに対応するために、ワクチンソフトメーカーより配布される「ウィルス定義ファイル」というものがあります。このファイルの最新版には、新しいウィルスの情報が入っており、これによって新しいウィルスの検出、除去ができるようになります。

例えば Norton AntiVirus であれば、”LiveUpdate”、ウィルスバスターであれば”最新版にアップデート”でウィルス定義ファイルを更新し、新しいウィルスに対応できるようになります。もちろん、他のメーカーの製品でも同じ機能があるはずです。

ワクチンソフトを使っている方で、ウィルス定義ファイルの更新をしてない方もいらっしゃると思います。でも、それでは新しいウィルスが出てきたときに検出する事が出来ず、ウィルスに感染してしまうかもしれません。現在では、毎日のように新種のコンピューターウィルスが発見されているので感染する確立が高くなります。

つまり、まめに「更新(Update)」することが必要になってくるという訳です。

他にも「デマウィルス」と呼ばれるものも流行っています。
これは、存在しないウィルスのデマ情報を送り、チェーンメールにする事を狙ったものです。
（＊チェーンメール・・・ 不幸の手紙みたいなものなので、絶対に転送しないで下さい。）
例えば、

jdbgmgr.exe に関するデマメール（IPA/ISEC より）
http://www.ipa.go.jp/security/topics/alert140515.html

デマかどうか分からないときは、定義ファイルを最新にしてウィルスチェックをし、ウィルス情報ページを見てみる事をお薦めします。

ウィルス対策について、よく言われることは、

＃ウィルス定義ファイルを常に「最新」のものに更新する

＃電子メールの添付ファイルを不用意に開かない

＃インターネット上からファイルをダウンロードしてきて不用意に実行しない

＃Windows の更新をする（Windows Update）

＃データのバックアップを行う

のようなことです。
これらに注意していれば、被害に遭う確率はかなり低くなります。
もちろん、ワクチンソフトをインストールしての事ですが...。

ウィルス情報は、IPA/ISEC セキュリティセンターや、ワクチンソフトのメーカーからも発信されていますので、興味のある方はこちらもご参照ください。

《参照》

IPA/ISEC セキュリティセンター：
http://www.ipa.go.jp/security/isg/virus.html
シマンテック：　http://www.symantec.co.jp/region/jp/sarcj/vinfodb.html
トレンドマイクロ：　http://www.trendmicro.co.jp/vinfo/
McAfee：　http://www.nai.com/japan/virusinfo/vinfo.asp

【Q】　どうすればいいの？　＜クラッカー編＞

ADSL などでブロードバンド接続されている方はブロードバンドルータを御存知ですよね？

「えっ？知らない...」

では、パーソナルファイヤーウォールは知ってますよね？

「えっ？知らない...」

上記二つに該当する方・・・「あなたは危険な環境でインターネットを楽しまれています。」

【Q】　どうして危険なの？

インターネットは世界中のパソコンが繋がって、お互いにアクセス可能になっています。だからこそ、日本からアメリカのホームページが見えたり、イギリスからメールが届いたりするわけです。
色々と外国のページを見にいかれる方も多いと思いますが、こちらから外国のホームページやパソコンにアクセスできると言うことは、逆を言うと、外国からもこちらのパソコンにアクセスできる... と言うことなのです。

インターネット上では、常に様々な国のクラッカー達がどこかに侵入可能なパソコンが無いか、日夜探しています。また、ワーム(上で説明したウィルスみたいなものです)と呼ばれるプログラムも、自動的に侵入可能なパソコンを探し回っています。もちろん、インターネットに繋がっているあなたのパソコンも狙われています。でも、勘違いしないで下さい。別にあなただから狙われる... と言う訳ではありません。クラッカー達は相手は誰でも良いのです。「自分だけは大丈夫！」なんて事はまったく無いですよ。

実は、常時接続環境では常に「攻撃」にさらされています。パーソナルファイアウォールソフトを入れられている方はログを見てみると、どれだけ攻撃が来ているかが分かると思います。そうじゃない人は・・・ただ、見えてないだけですよ。

インターネットに繋がっているパソコンを、家に例えて見ましょう。
扉がいくつかあります。チャットする為の扉、ファイル共有する為の扉、ホームページを見るための扉、メールを送信する為の扉。この中には、頑丈な扉、鉄格子の扉、鍵のかかっていない扉、すぐに壊れてしまう扉・・・色々ありますが、鍵の掛かってない扉だと直ぐに家に入られてしまいます。

「でも、うちの近所には勝手に家に入るような人はいないから大丈夫！」

そうですね。現実世界であれば、アメリカから飛行機に乗って 10～12 時間 かけて悪さをしに来ようって人は殆どいないでしょう。
でも、インターネットは・・・　例えば http://www.yahoo.com/ ここを開いてみましょう。アメリカにあるページですが、開くのに 5 秒とかからないでしょう。となると、アメリカも 5 秒で行き来できるご近所さんです。どこからどんな人が来るか分かりません。

では、クラッカーはあなたのパソコンにイタズラをして何をするのか？
ここでも、

「自分のパソコンには重要なデータが入ってないから大丈夫！」

と、仰る方もいらっしゃるかと思いますが、重要なデータを改竄、破壊したり、盗み見したりするだけではなく、乗っ取ったあなたのパソコンを使って別のパソコンへの攻撃を始めるかもしれません。もし、攻撃先が某 5 角形な所だったら、気が付いたらサングラスの黒服の人たちに囲まれてた... ！なんて事も有るかもしれないですよ・・・とまぁ、これは冗談ですが。

例えばファイルの共有。会社ではよく Windows 同士のファイルの共有が行われていますが、ADSL や CATV インターネットで、別のパソコンから、自分のパソコンのファイルが見えていた！などと言う話をよく耳にします。もし、自分の知らない間に、自分のパソコンの中身を見られていたら気持ち悪いですよね？見られるだけなら良いですけど、ファイルが見えたりコピーできたりしたら、違法なデータの交換場所になってしまうかもしれません。

では、現在、他のパソコンからあなたのパソコンがどのように見えているか、インターネット上でチェックすることができます。下のページの ”セキュリティリスクのスキャン” で見てみましょう。

http://www.symantec.com/region/jp/securitycheck/index.html

結果はどうでしたか？
「他のパソコンから丸見え状態... !」　こういった問題からパソコンを守ってくれるものが、ブロードバンドルーターやパーソナルファイアーウォールです。
自分のパソコンのセキュリティを守るためには技術的な知識が要求されます。しかし、パーソナルファイヤーウォールは、その専門的な知識が無くともあなたをこのような脅威から守ってくれます。（ブロードバンドルーターは・・・ちょっと知識が必要かもしれませんが。）

【Q】　ブロードバンドルーターって？

ブロードバンドルーターは、例えるなら家の門のようなものです。パソコンと ADSL モデムの間につなぎます。一本の回線に、複数のパソコンをつないで同時に使うためにも使いますが、予め「こんなデータとこんなデータは怪しいから通しちゃ駄目！」と設定しておくと、あなたのパソコンの前で入ってくるデータをチェックして、パソコンにたどり着く前に止めてくれます（パケットフィルタリング）。また、IP マスカレード（NAT）という機能を使えば、外から見ると “ ブロードバンドルーターが見えるだけ ” と、パソコン自体を隠してしまう事ができます。
もちろん、隠されてもちゃんとインターネットはできます。また、隠れてても分かる人には分かるので、ちゃんとソフトのアップデートも、ウィルスチェックもして下さいね。

【Q】　パーソナルファイアウォールって？

パーソナルファイアウォールは、パソコン自体にインストールして使います。もし、外部から怪しい攻撃があった時はその攻撃を防ぎ、画面に表示したり、記録（ログ）を残したりしてあなたのパソコンを守ってくれます。

例えば、

- Norton Internet Security 2003
  http://www.symantec.com/region/jp/products/nis/

- ウィルスバスター2003 リアルセキュリティ
  http://www.trendmicro.co.jp/product/vb2003/index.asp

上記の製品はパーソナルファイヤーウォールとウィルススキャンが一つになっている優れものです。

「インターネットって恐いものなんだぁ。。。」っとここで思わないで下さいね。
ちゃんとした知識を身に付けた上で気を付けていれば、そこまで怖いものではありません。

でも、自分が何かの被害を受けるだけなら良いです
が、それが原因で、他の人にまで迷惑がかかること
もあるかもしれません。

インターネット中には色々なものがありますし、
使っている人の中にも色々な人が居ます。
全ての人が悪い人ばかりではありませんが、みんな
がみんないい人だって事もないですよね？

こういったことを踏まえた上で、自分自身を守るようにしましょう。

愛媛県ネットワーク防犯連絡協議会
http://www.iyo.ne.jp/ensa/