

# 取扱説明書：インターネット

## はじめに

最近、どこそこがハッキングされたとか、なにになにと言うコンピュータウイルスが広まっているという話をよく耳にします。そういう時代の流れに便乗してここでは個人がすべき防御について書きたいと思います。ちなみに、”具体的に”のところでは想定するOSはWindows、ブラウザはInternet Explorer(略してIE)、メーラーはOutlook Express(略してOE)です。理由は、単に使っている人が多いだろうから・・・と言うだけで僕はMicrosoft社(略してMS)の回し者ではありません。

本文中で”コンピュータウイルス”という用語をワーム・トロイの木馬と区別しないで使ったり、脆弱性、不具合等々をまとめてバグと呼んでいたりします。区別するのが面倒だったので……

まず、被害の受け方を3つに分けたいと思います。

1. 自分の使っているパソコンのデータを破壊・改竄(かいざん)される。又は盗まれる。
2. 自分の使っているパソコンがフリーズする。
3. その他

これらについて、典型的な攻撃の使っている方法と防御について解説します。

## ほんぶん

### 1. 自分の使っているパソコンのデータを破壊・改竄される。又は盗まれる。

やられると一番辛いのがこのタイプです。例えば、パソコンのコントロールを奪われるというのがこのタイプに入ります。

このとき、攻撃者側が使う手段が

- 1) ソフトウェアのバグ
- 2) ユーザーを騙す
- 3) 気合いと根性
- 4) 物理力

等々です。

#### 1) ソフトウェアのバグについて

まず最もよく使われる手段が「ソフトウェアのバグ」を使う方法です。メジャーなところではコンピュータウイルスである Badtrans が使っている、MS01-20 という O E ・ I E についてのバグがあります。これはちょっと工夫したメールを送ると添付ファイルを自動で実行してしまうと言う恐ろしいモノで、その添付ファイルを悪意のあるモノにすることで 1 . のようなことが出来ます。

1 . のようなことを可能にするバグは非常に多くのソフトウェアで見つかり注意が必要です。

#### **対策方法：**

ソフトウェアのアップデートをする・設定を見直す、この二つが重要です。ソフトウェアのバグが見つかったら、まともな会社はすぐにそのバグを修正するソフトウェアを公開します。まずはその修正を行うことが重要です。特に、ブラウザやメーラーなど外から来るデータ（信頼の置けないデータ）に直接触れるプログラムは常に最新の状態に保っておくべきです。

設定を見直すというのは、よくバグが見つかる項目を使用不可にする、例えば I E の ActiveX の実行をすべて止める。などのことです。これによって、修正パッチがない状況でも安全にソフトウェアを使うことが出来ます。

#### **具体的に：**

まずは、Windows Update に行きましょう。そこで公開されているすべてのパッチを適用してください。これでブラウザとメーラーは最新の状態となります。次に、そのまま MS Office のアップデートにしてください。（MSOffice が入ってない方は別にいいです）そしてすべてのパッチを適用してください。「MS Office めったに使わないし別にいいのでは？」とか思っただけです。I E は MSWord のファイルをダウンロード扱いにはしないので・・・。（I E は W E B ページにある MSWord のファイルを開く）

その後、I E に入っている Plug-in のアップデートになります。Plug-in とは例えば、Flash ムービーを見たりするのに必要なソフトウェアで I E の機能を強化するためのモノです。これも、外から来るデータに直接触れるプログラムですのでアップデートするべきです。ちなみに、2002 年に入ってから少なくとも Real Player と QuickTime にはバグが発見されているので注意した方がいいです。

さらに安全にしたければ、「インターネットのプロパティ」の「セキュリティ」の設定を高にする、等の方法があります。

## **2) ユーザーを騙すについて**

ユーザーを騙して、悪意のあるプログラムを実行させ、1 . のようなことを起こすというの

は昔から定番の方法です。最近では myparty というコンピュータウイルスが www.myparty.yahoo.com という、一見URLに見せかけた添付ファイルを使い非常に多くの人を騙すことに成功しています。

#### **対策方法：**

怪しいプログラムを実行しない。の一言です。ただし怪しいファイルを見分けるのはかなり難しくなかなか大変です。しかも、友達からもらった怪しくないファイルが実はコンピュータウイルスに感染していた（この場合その友達も自分がコンピュータウイルスに感染していることを知りません）ということもよく起こります。

#### **具体的に：**

まず拡張子を表示する設定にし、害を与える可能性のあるファイルを見分けるべきです。拡張子とはファイル名の後に.XXXと言う形で書かれているモノのことで、ファイルの種類を表しています。しかしこれは、デフォルトでは表示されなくなっています。そこで、フォルダオプションから表示を選び”拡張子を表示しない”のチェックをはずしてください。

害を与える可能性のある主な拡張子は .exe .com .scr .pif .vbs .vbe .doc .xls .ppt .js .jse .bat .wsf .msi です。このほかにも、多くありますし、拡張子を隠すテクニックもありますので、この拡張子以外なら安全と言うことではありません。少なくとも、変なメールにこれらのファイルが添付されていたら怪しいと思った方がいいということです。このときは送信者にそのファイルを送ったかどうか確認してみましょう。

逆に、.txt .jpg .gif は安全であるといえる拡張子です。ただし、この場合もダブルクリックで開くのではなく、テキストエディタやイメージビューワから開くほうが安全であるといえます。

また、ワクチンソフトを使って防ぐというのもおすすめです。こういったソフトの多くは開こうとする前に”これは不正なプログラムである”と警告してくれます。ただし、ワクチンソフトだけで完全に安全であるというわけではありません。（これについては後述します）

### **3) 気合いと根性について**

ドライブ丸ごとを共有フォルダとしてフルアクセスで公開し、しかもパスワードをかけていなかったためにデータを改竄された。と言う事例や、総当たり攻撃を掛けられ内部に侵入された、と言う事例もあります。こういった総当たり攻撃を”気合いと根性”に分類します。

#### **対策方法：**

弱いパスワードをつかわない。不必要なサービスは止める。

### 具体的に：

基本的にアルファベット大文字小文字+数字+記号の8文字のパスワードならばまず安全だと言われています。ということで出来るだけその長さのパスワードを使うようにしてください。ネットワーク経由での総当たり攻撃ではそれほど速い速度で試行できないのでこれでほぼ安全と言えます。ただし、nekoneko とか nyannyan とか明らかに辞書に載っているようなのは駄目です。

また、共有はある特定のフォルダのみとするべきです。ドライブ丸ごとを共有する必要はないはずですので。そのほか、共有フォルダの設定を読み取り専用にしておけば改竄は防げます。ただし、この場合も特定のフォルダのみ許可としておくべきです。見られるだけでも危ないファイルはかなり多いです。(例えば、暗号化されたパスワードファイルなど)

外部から内部を守るという観点で、ファイアウォールやルーターを使うという手もあります。

## 4) 物理力について

友達にパソコン使わせてたらいろいろ漁られた、弱みを握られた、という私の実体験がありません・・・。

### 対策方法：

友達といえども自分のパソコンを触らせないことが一番です。トイレに行くとき等には、ノートパソコンなら携帯する、デスクトップならばブレーカーを切る等の対策が有効です。

### 具体的に：

Windows のログオン時や、スクリーンセーバーにパスワードをかけるという手段もありますが、詳しい友人への対策としては不十分です。というか、それでも漁ってくるヤツとはとっとと別れましょう。

## 2 . 自分の使っているパソコンがフリーズする。

いわゆるD o S 攻撃というヤツです。サーバーなどを運営し、かつ、恨みを買っているとかでない限り攻撃されることはまずありません。また、たとえ攻撃されても、パソコン自体が壊れることは無く、多くは再起動すれば直りますので個人はたいして気にする必要がないかもしれません。しかし、無差別にD o S 攻撃をする人がいないわけではなく、知識として知っておくのはよいことなので簡単に解説したいと思います。

このとき攻撃者側が使う手段は

- 1) ソフトウェアのバグ
- 2) 集団リンチ

等が有名です。

### 1) ソフトウェアのバグ

Windows95 が現役だった頃、Winnuke という Tool がはやったことがありました。この Tool は Port139(NetBIOS)に大量の文字列を送信し、修正プログラムを当てていない場合、攻撃を受けたマシンは止まってしまいました。

このような問題は、非常に多くのソフトウェアで発見されています。

#### 対策方法：

ソフトウェアのバグを修正するのが一番です。1. の 1) を参考にしてください。また、ファイアウォール・ルーターなども効果があります。

### 2) 集団リンチ

いわゆる DDoS というヤツで有名企業に対し、よく行われるのがこの攻撃です。非常に多くのコンピュータからの一斉攻撃によって相手のマシンに障害を与えるのを目標としています。多数のコンピュータというのがポイントで、その台数を確保するために、コンピュータウイルスを用いる、工夫したパケットを用いる、等様々な手法があります。

最近ではコンピュータウイルスである Codered がホワイトハウスへの攻撃を目標し、感染を広げました。このときは Codered の設計上の甘さからホワイトハウスのサイトは被害を受けませんでした。数十万台のコンピュータから一斉に攻撃を食らってはどんな環境のサーバーであろうと止まってしまうと思われま

#### 対策方法：

基本的にありません。ちなみに狙われることも多分ありません。ただし、攻撃をするための台数として確保されないように対策しましょう。対策方法は 1. と同じです。

### 3. その他

その他、よく耳にするであろう話題を 3 つほど取り上げます。

- 1) ブラウザクラッシャー
- 2) cookie を盗まれる
- 3) クロスサイトスクリプティング

#### 1) ブラウザクラッシャー

WEB サイト閲覧中、いきなりうじゃうじゃウィンドウが開いた、ウィンドウが移動した、IE が止まった、等の経験をした人は多いのではないのでしょうか？このような、ブラウザを止める攻撃（というか罠）をブラウザクラッシャーといいます。

・ JavaScript によりウィンドウをうじゃうじゃ開く、ループをたくさんさせる

- ・ などのタグでメーラーをうじゃうじゃ開く
- ・ 不正な画像を読み込ませる
- ・ タグを閉じていない、容量の大きな文章を読み込ませる

などなど、ブラウザクラッシャーが使う手法は非常に多くあります。

#### 対策方法：

JavaScript を切る、怪しいサイトに行かない等である程度対策できます。

また、proxy によるフィルタリングも有効です。

#### 具体的に：

proxy によるフィルタリングについては、proxomitron というソフトを使う方法が一般的です。使い方は google などで検索してください。

## 2) cookie を盗まれる

cookie とはWEB サイトごとの一時的なデータの保管方法と考えればそう外してはいません。yahoo など多くのサイトで使われ、パソコンを再起動してもログインした状態が維持されるのは cookie があるおかげです。

しかし、WEB サイトによっては cookie にメールアドレスを保存していたり、ID やパスワードを簡単な暗号処理をした後（酷いときはそのまま）保存していたりします。cookie はWEB サイトごとに管理され、あるサイトへの cookie はその他のサイトからアクセスは出来ないと言っていることになっていますが、その抜け道はたくさんあります。実際、多くのブラウザで cookie を盗めるバグが見つかっていますし、後述のクロスサイトスクリプティングを使うことでも cookie を盗むことが出来ます。

#### 対策方法：

ブラウザのアップデートをする。信

頼の置けそうなWEB サイト以外では cookie を使わない。

#### 具体的に：

「インターネットのプロパティ」の「セキュリティ」の設定で cookie に対する設定を変更する。

## 3) クロスサイトスクリプティングの問題

この問題があるページをあたかも改竄したように見せることが出来る手法のことです。って、意味不明ですので、例を挙げます。

例えば検索エンジンなどで "XXX" と検索すると、その結果のところ "XXX の検索結

果 xxx 件 ” 等という記述があると思います。このとき検索する文字列を ” <script>cookie ぬすむ  
ぜー 内容をかきかえるぜー</script> ” のようにすると、結果のところで ” <script>cookie ぬすむ  
ぜー 内容をかきかえるぜー</script>の検索結果 x 件 ” となる場合があります。このとき  
<script></script>はタグとしてブラウザに認識され内部の Script が実行されます。検索エンジ  
ンの URL でこれらの Script が実行されるため、cookie を盗むことができますし、その URL で変  
な内容のページを見せることができます。

ただし、まともなところであれば<を&lt;にするなど、対策がしてありますので普通は心配あ  
りませんが、大きめの会社のサイトでもこの問題があるところがまだ結構あります。

#### 対策方法：

基本的に無し。(サーバー側の問題なのでこちらでは対処のしようがありません)

JavaScript・cookie を使わない設定にする、URL でやたら長い文字列が入っている場合は内  
容を疑う、ソースを見るなどである程度対応は出来ませんが、根本的な解決ではありません。

## なんとなく

### セキュリティはワクチンソフト&ファイアウォールで完璧か？

結論から言えば、完璧ではない、と思います。ワクチンソフトの限界について、簡単な実験を紹介  
します。

実験用のワクチンソフトとしてトレンドマイクロ社のウイルスバスターを使います。これを選ん  
だ理由はオンラインウイルススキャンを使って無料でウイルスチェックが出来るからです。また、  
実験用のウイルスとしてVBS\_Loveletterを使います。これを選んだ理由は、VBS で書かれているた  
め改造しやすいためです。多分、ソース自体は検索すればいくらでも手にはいると思います。

まずVBS\_Loveletter をテキストエディタで開き、ファイルの一番上と一番下にコメントを多めに  
書きます(40文字を5行くらい)その後、変数を2,3個追加してください。これでウイルスバ  
スターでは発見できない亜種の誕生です。

ワクチンソフトは処理時間を短くしないといけないため、ファイル一つを丁寧にチェックす  
ることが出来ません。そのため、このように簡単な改造でそのソフトのチェックを抜ける亜種が作  
れてしまいます。

ファイアウォールも同様にパケットをいちいち細かくチェックすることは出来ないという限界が

あります。

もちろん、これらが無いよりはるかにマシですが、「ワクチンソフト&ファイアウォールで完璧」と言う考えは捨てた方が賢明です。

## IE・OEは駄目!?

IE・OEにはバグが多いと言われていて、見つかった数は確かに他のブラウザよりも多いと言えます。よってIE・OEの使用を中止し、他のブラウザ・メーラーに乗り換えるべきだという意見があります。私はある程度この意見に賛成ですが、「バグの数」を主眼においた理由付けには反対です。どちらかというところ「IE・OEのようにメジャーなソフトウェアは攻撃対象になる可能性が高く、被害に遭いやすい」ことを理由にするべきだと思います。(もしくはバグに対する修正の速度)

どんなブラウザを使おうとアップデートは必須です。よく、「IE・OE以外のモノにはバグがない」というように文章を書くページを見かけますが、それは間違いであり完全な嘘です。IE・OEのバグを使用したコンピュータウイルスが広がった理由はそのバグが非常に使用しやすかったためだけであり、IE・OE以外のブラウザやメーラーに対しても有効な自動実行型のコンピュータウイルスを作ることは可能です。誤解しないでください。

ちなみに、アップデートが必須というのはWindowsであろうがMacOSであろうがLinuxであろうが変わりません。バグが存在しないソフトウェアは無いと思った方がいいです。

## おわりに

長い長い文章を最後まで読んでくれてありがとうございます。突っ込み歓迎です。セキュリティに必要なのは多分、情報です。情報を早く仕入れ、バグの修正・設定変更をすればまず安全だと思います。情報収集の方法は「メーリングリストにはいる」「セキュリティに関するWEBサイトのチェックをする」のがいいと思います。メーリングリストであればBugtraqが有名で、非常に情報量が多いです。しかし、専門的な話題が多く、また英語で話が進むため読むのが大変です。WEBサイトであれば

<http://www.st.ryukoku.ac.jp/~kjm/security/memo/> セキュリティホール memo

がお勧めです。また、最近のポータルサイト(Yahooなど)のコンピュータニュースにはセキュリティ関連の話題がある場合が多いので、そちらを参考にしてもいいと思います。

紙面と私の腕の関係上、パスワードに関する記述や暗号化といった話題がありません。これは、

他人に迷惑をかけないための防御方法を中心に書いたためです。自衛策として必要なパスワードの常識は、"文字数は8文字以上"、"使う場所ごとに変える"です。暗号化についてはそれについて扱ったサイトを調べてみてください。

WEBの散策やメールの交換、ネットワークゲームは非常に楽しいですが、たまにはセキュリティについて考えるのもいいかと思います。友達にコンピュータウイルスを送ってしまったり、他人にパソコンを乗っ取られたりというのは腹が立ちますし、いろいろと問題を起こします。

文責 高橋 怜士@Vole