コンピュータウイルスの話

理工学部知能情報システム学科　渡辺 義明

1　はじめに

コンピュータウイルスの報道が頻繁になって来ています。そこで、コンピュータウイルスとは何か、またその対策はどうすれば良いかについてまとめてみました。

コンピュータウイルスは、悪意を持った処理を行うように意図的に作られたプログラムです。プログラムやデータの移動に伴って一緒に移動し、コンピュータの正常動作を阻害する様が、自然界のウイルスの行動と似ていることから、コンピュータウイルスと呼ばれます。最近になって騒がれるようになったのは、電子メールを始めとするネットワーク機能を利用して瞬く間に世界中に広がることと、PC (パーソナルコンピュータ) が基幹業務を担うようになっていることから、深刻な問題を引き起こす事例が出てきているためです。

発生する被害には、コンピュータシステムの停止、重要データの欠損や漏洩、回復作業による本来作業の停滞、さらに、それらによる社会的信用の失墜などがあります。また、はからずも他組織への感染を仲介した場合には、対外的問題を抱えることになります。

ではその対策は、どうすれば良いのでしょうか。基本は、ワクチンソフトによる予防措置とバックアップによる復旧措置、それに情報取得時における十分な注意です。

2　コンピュータウイルスとは

コンピュータウイルスは、例えば通産省のコンピュータウイルス対策基準[1] では、以下のように定義されています。

> 第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムであり、次の機能を一つ以上有するもの。
>
> 1. **自己伝染機能**：自らの機能によって他のプログラムに自らをコピーし、又はシステム機能を利用して自らを他のシステムにコピーすることにより、他のシステムに伝染する機能
> 2. **潜伏機能**：発病するための特定時刻、一定時間、処理回数等の条件を記憶させて、発病するまで症状を出さない機能
> 3. **発病機能**:プログラム、データ等のファイルの破壊を行ったり、設計者の意図しない動作をする等の機能

[1] http://www.ipa.go.jp/SECURITY/antivirus/kijun535.html

このように、自然界のウイルスと似た動作をしますが、あくまで単なるプログラムです。プログラムですので、ディスク上に存在するだけでは悪さができません。何らかの手段で実行の指示をもらわなければなりません。よって、例えば、システム領域に入り込み、システムの自動処理に伴って起動されるようにしたり、有用なソフトウェアに付随して一緒に起動されるのを待つ手段を取ります。

また、最近増加して来たのが「**マクロウイルス**」と呼ばれる種類です。ワープロや表計算などが持つマクロ機能は、データファイル中に書かれた命令に従って自動処理を行うものです。このマクロは、元来は簡易プログラム機能の提供でしたが、徐々に複雑な処理を記述することができるようになっています。例えば、文書ファイルの初期設定処理中にファイル削除命令や電子メール発信命令を書けば、その文書を開いた途端にデータの破壊や漏洩を起こすことができます。

コンピュータウイルスは、感染先や感染方法などにより、様々に分類されます。コンピュータウイルスのうちで、上記の全ての条件を満たしているものを「**真性ウイルス**」と呼びます。最近は、これらの

全ての条件に当てはまらないものも増加しています。場合によっては、そのようなものをコンピュータウイルスと呼ばないこともありますが、ここでは、上の定義に従います。

「**ネットワークワーム**」と呼ばれる種類は、他のプログラムに付随してコピーされるのを待つのではなく、ネットワークを介して自分自身をコピーする処理を行うプログラムです。ネットワークに開いた穴を通して移動するワーム (虫) の意味です。コピー先で即実行されるような仕掛けがあると、その感染は急速に広がります。過去には、ネットワーク機能の実装ミスを介して感染し、インターネットの多くのサイトを機能不全に陥れた歴史的事件がありました。最近ではファイル共有を通して広がる例が報告されています。

また、「**トロイの木馬**」と呼ばれる種類もあります。外見上は有用なプログラムやデータのように見せかけて、実は悪意のある処理を内在するものです。最近では、2000 年問題対応ソフトウェアを偽称したものやフリーのセキュリティソフトに付加されたものがありました。

また、これらの機能を併せ持つことも多くなっています。例えば、以下のようなコンピュータウイルスが報告されています。電子メールの添付ファイルとして、有用を装った誘い文句を付けてやってくる。添付ファイルを開くと、電子メールシステムの設定を変え、登録メールアドレスに向けて自分を添付したメールを自動配布する。また、利用者が送付するメールにも自動的に添付する。さらにファイル共有を介してファイルのコピーや削除を行う。

なお、このコンピュータウイルスは添付ファイルを開かなければ安全ですが、最近では、HTML 形式のメール本文中に記述されたものも見つかっています。この場合は、本文を開いただけで行動を開始しますので、メール本文は単純なテキスト形式にしておくことを勧めます。

3　感染したらどうなるか

感染したときの動きはコンピュータウイルスによって千差万別です。派手な画面を見せて感染を誇示する陽性のものがありますが、全く変化無いように見せてデータを盗んだり、消してしまったりする陰湿なものもあります。単に感染を繰り返すだけで、何も積極的なことをしないものもあります。また、特定の条件が揃うまでは全く動きを見せないものもあります。

コンピュータウイルス感染時には例えば以下のようなことがあります。

- 変なメッセージや画像が表示される。
- プログラムの動作がおかしい。
- 速度が遅い。
- 突然に停止する。
- 変なディスク/ネットワークアクセスがある。

しかし、これらの現象は、コンピュータウイルス以外でも発生します。正常動作中でも有り得ますし、操作や設定の誤り、機器の不具合などでも起こります。後述のワクチンソフトで確認できて始めて他の原因では無いと言えます。一般には、誇示行動以外の変な動作は、コンピュータウイルスではない他の原因で発生していることの方が多いと思います。

4　対策

コンピュータウイルスに対する対策は基本的には次の 3 つです。

1. ワクチンソフトによる予防措置
2. バックアップによる復旧措置
3. 情報取得時における十分な注意

4.1　ワクチンソフトによる予防措置

ワクチンソフトは、自然界のウイルスに対するワクチンと同様に、コンピュータウイルスの発見と駆除を行うソフトウェアです。ワクチンソフトには多くの製品がありますが、製品の性能差は少なくなっているようです。

ワクチンソフトが、あるプログラムをコンピュータウイルスと認識するには、そのプログラムがコンピュータウイルスの様な挙動をするかチェックすること、または、前もって知っているコンピュータウイルスと同じパタンを含むかチェックすることの二つの手段が基本です。よって、監視のために常にワクチンソフトを動かして置く必要があります。さら

表 1: Web 上の情報

IPA(情報処理振興事業協会)	http://www.ipa.go.jp/SECURITY/index-j.html
アンチウイルス（電通大小菅研運営）	http://www.iosnet.ne.jp/anti-virus/
JCSA(日本コンピュータ・セキュリティ協会)	http://www.jcsa.or.jp/
ウイルスコンサルティングセンター	www.vcon.dekyo.or.jp/
ワクチンバンクセントラルウェブ	http://www.vaccinebank.or.jp/
JCVA(日本コンピュータ・ウイルス協会)	http://www.systemsite.com/jcva.html
トレンドマイクロ	http://www.trendmicro.co.jp/
シマンテック	http://www.symantec.co.jp/
ネットワーク アソシエイツ	http://www.nai.com/japan/

に、常に新しいコンピュータウイルスのパタンを入手して置く必要があります。即ち、ワクチンソフトの効果を生かすには、データ更新と常駐使用が必要です。

最近では、PC を購入すると最初からワクチンソフトが付いてくることも多くなっています。しかし、それらはデータ更新が制限されているものがほとんどだと思います。製品版では、購入後半年から１年程度の更新サポートがありますし、その後も安価な費用で更新サポートの継続ができます。

ワクチンソフトは、コンピュータウイルスを発見する機能とともに、それらを駆除する機能も持ちます。ただし、コンピュータウイルスがファイルを書き換えてしまっていた場合には消された情報は戻せません。よって、重要なデータなどはバックアップが必要です。

4.2 バックアップによる復旧措置

ワクチンソフトは万能ではありません。また、コンピュータウイルス以外にも、ハードウェアの故障、ソフトウェアのバグ、誤った操作、ネットワークを介した破壊工作などによっても、データの破壊が引き起こされます。

よって重要なデータはバックアップを取って下さい。ただし計画性を持ったバックアップでないと、いざと言うときに役立ちません。例えば、破壊されたファイルをバックアップして正常ファイルを上書きしてしまうことがありますので、複数のバックアップを持っておくことが必要です。

バックアップはフロッピーディスクや MO 等のリムーバブル媒体への退避が基本ですが、手間を考えるとネットワーク経由でのバックアップやハードディスクの二重化も考えて良いでしょう。

また、データのバックアップだけでなく、システムが動かなくなった時に対する対策も考える必要があります。このためには、例えばハードディスクをまるごとバックアップするソフトもあります。

4.3 情報取得時における十分な注意

他人からファイルをもらったときは、利用する前にウイルスチェックをして下さい。また、必要性の薄いファイルをむやみとダウンロードしたり、貸し借りしたりしないで下さい。入手先が信用できるところでも、感染の危険はゼロではありません。省庁や有名企業等の Web 上のファイルに感染していた例があります。また、大学内回覧のフロッピーディスクが感染していた例があります。

文書ファイルを開くときに、「ウイルスに感染している可能性があります。マクロを有効にしますか。」等のメッセージが出る事があります。これは「マクロ (自動化処理) がファイル中で設定されているが、本当にマクロを実行して良いのか。危険性はゼロではないよ」と言っているだけで、ウイルスに感染していることを意味しません。ただし、マクロ機能が必要でない場合は無効にした方が賢明です。また、警告表示無しに設定にするコンピュータウイルスもあるので、警告が無いから安全だとは言えません。

電子メールは、コンピュータウイルス感染の格好の手段となっています。単純なテキスト形式のメールでは、開いただけで感染することはありませんが、添付ファイルは感染の危険性があります。不用

意に開かないでウイルスチェックをして下さい。受信時に自動的に検査する機能を持つワクチンソフトも出ています。また、電子メール本文に HTML 等を使って複雑な表示や動きを入れることが可能なソフトがありますが、このような自動化処理にコンピュータウイルスが仕掛けられた例が出ています。メールソフトは基本的な機能に限るようにした方が良いでしょう。

自分にとって便利な機能は、コンピュータウイルス作者にとっても便利な機能になる可能性があります。必要性の薄い機能は無効にしておいて下さい。

5　おわりに

以上、簡単にまとめましたが、より詳しくまた新しい情報は、表 1 に示す URL などを見て下さい。攻撃側も防御側も次々に新手を投入して来ます。変な情報に惑わされず、信頼できる所の情報を参照するようにして下さい。

例えば、緊急ウイルス情報などと称する電子メールが回ってくる事がありますが、これはデマです。鼠算的な電子メール数の拡大を狙った愉快犯罪です。親切心で他へ転送しないで下さい。もう一つ杞憂でしょうが、コンピュータウイルスを興味本位に作成・改造しないで下さい。誤って伝染させると根絶は困難です。また作成ファイルには作者を特定できる情報が様々な形で含まれます。

最後に、快適なコンピュータ環境を維持するためには、コンピュータウイルスにのみ神経質になるのではなく、コンピュータは故意・過失・故障を含めた様々な原因によって誤りを起こすものだと言うことを認識して、総合的な対策を取っていただくようお願いして終わりにします。