2001-1-

コンピュータ・ヴィルスの研究

目次：

１）コンピュータヴィルスとは何か？

パソコンに触り始め、インターネットを楽しむようになると誰でもすぐにヴィルス問題にぶつかります.
しかし人は案外自分はかからないと楽観しているものですから、実態についてはよく解っていないし、ましてやその予防、治療、更にはそれに伴う諸問題の解決については意外なほど認識していません.（私自身がパソコンを始めてから５年間正しくそうでした！）

コンピュータ・ヴィルスとはプログラムの一種で、愉快犯とも言うべき人達が自分の力を誇示し、他人を困らせる目的で作り出すものです.
自然界に存在し、生命体に感染する「本物の」ヴィルスに似たような特徴を持っているので、「感染」「発病」「潜伏期間」「検疫」「駆除」というような言葉が通常使われているわけですが、自然界のヴィルスとの決定的な差異は、それが人為的に創り出されたものであり、且つ自然治癒はあり得ないという点です。
つまりパソコンには人間が持っているような自然治癒力はないので、一旦罹ってしまったら、放って置けば何時の間にか直っているということはありません. ユーザーは正しくワクチンを使ってこれを駆除するかハードディスクのフォーマットをせねばならないのです.

コンピュータウィルスは増殖しながら蔓延するように設計されたプログラムであり、一般にその犠牲者はその存在に気づかないのが普通です。コンピュータウィルスは他のプログラム（ワープロやスプレッドシートなどのアプリケーションファイル）やディスクのブートセクターに自分を付着させることで蔓延します。感染したファイルが起動されたり実行されるか、あるいは感染したディスクからコンピュータが起動されると、ウィルスも同時に起動されます。しばしばコンピュータのメモリーに潜んでいて、プログラムが起動されたり、ディスクがアクセスされるのを待ち受けて感染します。
世界で始めてコンピュータヴィルスという言葉を使ったのは、南カリフォルニア大学のフレデリック・コーエン氏で、１９８４年のこ

とでしたが、１９８６年にはパソコンをターゲットとした世界初のヴィルスである「パキスタンブレイン」が登場し、爾来その種類は加速度的に増加の一途を辿っています．
今までに発見されたヴィルスは６万種類以上と言われ、毎日数百個の新型ヴィルスが登場しているとも言われておりますが、ウィンドウ９５が世に出てからインターネットが爆発的に増えた為に、ヴィルスも又量、質両面で大幅な成長をしているわけです．
考えてみればパソコンユーザーの大多数は初心者であり、無防備な人達ですからヴィルスにとっては現在のインターネット社会はこの上ない繁殖の温床と言うわけでしょう．

コンピュータヴィルスの一番厄介な問題は、一度感染した人が自分では氣がつかない間にイノセントな加害者になってしまい、ネット或いはメディアを通じて他の人にヴィルスを撒き散らしてしまう事が多いという事にあります．特に昨今のヴィルスはそのような点が殊更強調されて作られているのです．

パソコンでインターネットを楽しみ、メールを送受信する以上は、最低の義務として自らがヴィルスについて正しい知識を持って自分を守ると同時に、他の人に知らない間に感染させてしまうという危険を防がなければなりません．他人のデータを喪失させてしまったら、それが自分の無知によるものである以上、御免なさいではすまないことを強く認識する必要があるのではないでしょうか？

２）ヴィルスの種類にはどのようなものがあるか

「コンピュータヴィルス」という言葉の生みの親であるコーエン氏の定義では、ヴィルスとは「第三者に危害を与える不正プログラムの中でも、感染・潜伏・発病というルーチンを持つもの」とされていました。

現在アンチヴィルスソフトを作っている各社は、コンピュータヴィルスについておよそ次の様に定義しているようです。

「コンピュータヴィルスとは、コンピュータで動作するプログラムで、他のプログラムや他のコンピュータへ自身の複製を作成して行き、病原体のように増殖してゆくプログラムである」としており、「自分自身の複製を作らないけれども」コンピュータに入り込んで様々な脅威を与える「不正プログラム」をヴィルスとは別のものとして、ワーム、トロイの木馬、理論爆弾等と呼んでいます。

しかしながら、本稿は学術的論文ではないので、面倒な定義や分類に拘らず、これらを総称して「ヴィルス」と云って置きましょう。後はヴィルスをよりよく理解する為に、どのような種類があるのか

を調べますが、細かな点よりもその数の多さ、種類の多様さ、そして被害の深刻さを理解できればよいと思います。

３）ヴィルスの感染はどのように起こるか

パソコンはそれ自体で風邪をひくようなことはありません．つまり**なんらかの形で外からシステムファイルを受け取らなければ感染はしないのです．**

ヴィルスの感染経路は圧倒的にメールの受信によるものが多く、全体の６０％以上を占めています．
ヴィルスがプログラムなのですから、メールを受け取っただけでは通常は感染しません。**メールの添付書類をうっかり無防備に開いてしまったというのが大多数の感染経路となります．**

註：非常に稀な例ですが、メールを受け取って開いただけで感染するというヴィルスも報告されています．
それはメールが HTML 形式である場合で、テキスト形式であれば起こりえないのですが、HTML で通常メールの送受信しているというのは、このようなリスクもあるというわけです．

この他に他人から受け取ったフロッピーディスク、雑誌の付録などの CD などのメディアから感染する、或いはインターネットでデータをダウンロードした時に感染するという例もありますが、例えばインターネットで怪しげな画像をダウンロードしてもこれはシステムファイルではありませんからヴィルス感染はしません．

４）ヴィルス感染の兆候は？

感染の症状としては
＊ システムの動作不良
＊ 画面表示の異常
＊ データファイルの異常
などが表れることで、感染の疑いが先ず生じます。

更に具体的に挙げれば、
イ）　コンピュータが起動しなくなる
ロ）　コンピュータの動作が遅くなる
ハ）　プログラムの実行が出来なくなる
ニ）　プログラムの内容が変わってしまう
ホ）　不自然なディスクアクセスが生ずる
ヘ）　操作中にシステムが停止してしまう

ト）　意図しないメール発信が起きる
チ）　接続している機器を認識しなくなる
リ）　メモリーが不足して来る
ヌ）　メモリーやハードディスク容量の表示が減少して来る
ル）　画面上に異常なメッセージが表示される
ヲ）　おかしなグラフィックが画面に出て来る
ワ）　画面上のテキストや画面が崩れてしまう
カ）　データ破壊が起こる
ヨ）　モデムやプリンターの動作異常が起こる
タ）　キーボードからの入力が正しく行われなくなる
レ）　おかしな音や音楽が生じて来る
ソ）　保存したファイルに全く別の書き込みが現われる
ツ）　不審なダイアログボックスが生ずる
ネ）　ファイルの中身が勝手に変わってしまう
ナ）　正しい印刷が出来なくなる

これって案外今まで経験したような現象だとは思いませんか？
おかしいと思い出したらいろいろな兆候がヴィルス感染の恐怖へと繋がってしまいそうですね！？
最近はヴィルス作者も非常に巧妙になっており、感染しても暫くは発病しないものや、特定のコマンドや日付でのみ発病するものや、見つかり難いように自らを隠してしまうものやらが出ているので、もしも感染の発見が遅くなるとその間にどんどん感染が進み、自分のパソコンを食い荒らして修復不能に陥らせたり、知らない間にヴィルスを沢山ばら撒いてしまったりと言う事になってしまいます．
一寸変だなと思ったらすぐに感染の有無を調べる必要があるのです．

５）感染してしまったらどうするか？

メールの添付書類を開けてしまった、或いは開くというコマンドを打ってしまった．
「しまった！」と思ったらすぐにアプリケーションを閉じ、電源を切って「駆除」にかからねばなりません．
しかし感染したのを気付かずにいて、いろいろな異常が表れてしまったら、つまり「発病」してしまったら、逆に慌ててパソコンを閉じたりしないで、ヴィルスの炙り出しをするべきであると云われています．しかしこれは云うべくして無理で、我々素人はすぐにその時点で電源を切ってしまうというのが最低限の食い止め方でしょう．
勿論発病しているらしいと解ってから、更にパソコンを操作したり況やメールを発信したりすることは絶対に避けるべきです．

次にパソコンの検疫とヴィルスの駆除とが必要ですが、後で述べるワクチンソフトを常駐させていれば、そしてそれを常にアップデートさせている場合は、比較的簡単に出来るでしょうが、それが無い場合はとにかくパソコンには触らないで、必要なワクチンの入手に

努めねばなりません.
つまり絶対安静にして医者に行くという感覚です.

６）アンチヴィルスソフトにはどのようなものがあるか？

沢山のソフトが市販されていますが、どれも機能的には似通っていると考えられますし、値段も大体横並びで大差はありません. ５～６千円と言う所です。
どのソフトを選ぶかの基準は、

１）ヴィルスの作成・繁殖がどちらかと言えば海外に多いので、コンピュータの本場である米国に本拠を置くものがよいと思われる.
２）比較的知名度が高く、沢山売れているものが何かとよいと思われる
３）使い易く、且つアフターサービスのよいもの、これは新しいヴィルスが後から後から生れている現状からすれば絶対の要件と思われる。

以上から下記３点が代表的な候補と考えられますが.MCC では識者の意見､経験などを伺って検討した結果Ⅰ)を選ぶことにしました。

Ⅰ） 株式会社シマンテック
Norton AntiVirus2001 ￥4,670.00

Ⅱ） トレンドマイクロ社
Virus Buster ￥5,780.00

Ⅲ） 日本ネットワークアソシエイツ株式会社(McAfee)
VirusScan ￥6,000.00

７）アンチヴィルスソフトはどのように働くのか？

アンチヴィルスソフトの機能を Norton AntiVirus 2003 の場合で簡単に取り纏めてみますとおよそ次の様なものです.

ｉ）ヴィルスの検出

AntiVirus 2003 が PC に常駐していると、その第一の機能としてヴィルスの検出（つまり発見）をします。
その方法としては Auto-Protect 機能をオンにしておけば､メールの受信、FD などリムーバブルメディアの実行などの度に自動的にその内容をスキャンしてヴィルスの有無を確認します。

またこれと同じ動作を手動で行うことも出来ます。

このような外部からのヴィルス侵入を検査する以外に、PC の各ドライブのスキャンを行い、自分のパソコンが現時点でヴィルスに感染していないかどうかを調べる事も出来ますが、これも予約により定期的且つ自動的に行うことも、手動で随時行うことも出来ます。

ii ） ヴィルスの駆除

ヴィルスを発見すると、Norton AntiVirus 2003 内のワクチンを施すことによりヴィルスを駆除してファイルを無害化することが出来ます。

iii ） 感染ファイルの隔離（検疫）

もしもワクチンが効かないような場合は、ファイルをパソコン内で隔離し、発病しない（つまりそのファイルが実行されない）ように保全することが出来ます。
この後で適切な措置（例えばレジストリの修復）の後にこの汚染されたファイルを削除するなり、シマンテック社に送って解析及び駆除処理を依頼することが出来ます。

iv ） 定期的・自動的アップデート

上記のタスクを実行出来るようにするには、そのソフトが常にアップデートされている必要があります.
つまり新型ヴィルスが世界の何れかの場所で報告されると、直ちにそのヴィルスのデータベース（シマンテック社ではヴィルス定義と呼ぶ）をダウンロードして置かなければならないわけです。
これは恰もヴィルスの指紋登録のようなもので、Norton AntiVirus2003 をインストールし、登録すればその後インターネットに接続すると、シマンテック社のサーバーが感知して自動的にヴィルス定義の更新とそれに対応するワクチンのダウンロードをやってくれるという便利なシステムです.
シマンテック社はこれを LiveUpdate と呼んでおり、１年間は無料です。

v ） 救済ディスクセット

AntiVirus2001 をインストールするプロセスの中で、ヴィルスが原因で PC が正常に起動しなくなた場合に備えて、5 枚の FD による救済ディスクセットの作成が指示されます。この FD を保存して置けばまさかの時にパソコンを立ち上げることが出来

ますが、このディスクもいつもアップデートして置かないと、ディスクに入っているヴィルス定義が古いものである場合は新種のヴィルスを認知出来ないので除去出来ないというのは当然ですが､またシステムの復元も出来ない場合があるようです。しかしこれを常にやっておくというのは結構大変な手間なのでそこまで神経質にならなくても１年後にソフトのヴァージョンアップの時までは大丈夫と考えてもよいのではないかと思います？）

８）結論としてのヴィルス予防措置

結論的に如何にコンピュータヴィルスを防ぐかを纏めてみると次の様になると思われる。

１）　ヴィルスについての基礎知識を充分に持つこと

先ずは敵を知らねばならない．徒に怯えていることはないが、甘く見て無防備でいるのは愚の骨頂と言うべきである。
2000年に話題を呼んだI love you,Pretty Park,W32xmt何れもかなり報道されていたので、もしこれを予め勉強していれば、おかしなメールのファイル名を見ただけでピンと来た筈である．この意味では新種のヴィルスが現われると、すぐに報道されているので、ユーザーが強い関心を持っていれば、充分な予備知識を常に持ち得る環境はあるのである．

２）　アンチヴィルスソフトをパソコンに常駐・機能させること

リアルタイムでヴィルスを補足し、特定・駆除出来るように自分のパソコンを武装して置くべきである。
更にこれが重要な事であるが、このソフトのメンテナンスが重要で、常にアップデートして、新種のヴィルスのデータベース（シマンテックではヴィルス定義）を入手しておくと共に、ワクチンをダウンロードしておくことが絶対に不可欠である。

３）　定期的にパソコンの全ドライブのヴィルス検索をすること

２）が水際作戦とすれば、これはその上で更にパソコン内部をよく掃除して置こうという意味で、定期的に全ドライブのスキャニングをすることが必要である．これには２０分程度の時間がかかるので、月一回位のタスクでよいと思う。

４）　それでも尚外からのヴィルス侵入に対し充分警戒すること

つまりはメールの添付書類を開くには、それがたとえ信頼出来

ると思う人からのメールでも、充分気をつけて不用意に扱わないこと。
雑誌の付録の CD や、他人のデータを FD で受け取ったら時は一応感染の危険が無いか確かめる心掛けが必要であろう。
AntiVirus　ソフトが常駐していれば、必ず自動的にチェックされる仕組みになってはいるし、手動でもチェック出来るのであるが、新種のヴィルスで検出不能ということもあり得ることなのだ。

５）　このような予防体制を敷いていても尚感染・発病したという疑念が生じたら、直ちに適切な駆除或いは検疫に努め、徒に蔓延させないことに心掛けること．

６）　データファイルのバックアップを常に講じて置くこと。

ヴィルスに感染し発病しても、パソコンが壊れてしまうわけではない．いざとなればハードディスクのフォーマットで根こそぎヴィルスは退治出来るのであるが、その際システムファイルは再現出来ても、データファイルは永遠に戻らないことが起こり得るのであるから、常にこれに備えてバックアップを怠らないように心がけねばならない．

要するに「備えあれば憂いなし」なのである．

９）バックアップについて

さてヴィルスの予防及び駆除については既に述べた通りですが、それでもまだ万全とは云い難いのです。例えば新型ヴィルスに襲われ、データベースが無い為その検出が出来なかった時にはどうしようもありません．　感染は免れないのです．

そこで考えられるのが「バックアップ」です．
これまでどちらかと言えばハードディスククラッシュに備えてのバックアップを屡々論じて来ましたが、ヴィルスの被害に遭って究極の選択はハードディスクのフォーマットということになれば、これまで長い間蓄えて来たデータは根こそぎ失われてしまい、二度と回復する事は出来ないのです．
この被害は金銭には替えられないほど大きいかも知れません。
この機会に是非定期的なバックアップを取って置く事をお奨めする次第です。

（イ）バックアップ先のメディア
ハードディスクに入っているデータファイルを何らかのリムーバブ

ルメディアにコピーすることが、バックアップです.
メディアは FD、PD、ZIP、MO、CD 更には外付け HD など色々あり、容量もまちまちなのでバックアップするべきデータの量によって選べばよいのですが、FD 以外は書き込み用のドライブが標準品としてパソコンに付いていないので先ずこれらの周辺機器の整備が必要です。
またこれらの機器のインターフェースとして、スカジーボードが必要になることもあり、それなりの設備投資を必要とします。

取り敢えずはミニマムの措置として FD に取れるだけでもバックアップしておけば、かなりの文書データは保存出来ると思います。

リムーバブルディスクの種類	容量	ドライブの接続	ドライブの値段	メディアの値段
FD	1．4MB	PC標準品	0	¥50.00
ZIP	100MB	パラレルポート	¥15,000.00	¥2,000.00
MO	230-500MB	SCSI	¥30,000.00	¥1,000.00
CD-R	630MB	SCSI,USB	¥30,000.00	¥100
CD-RW	630MB	SCSI,USB	¥30,000.00	¥1,500.00
HD(外付け)	2～20GB	SCSI,USB	¥15,000以上	－

（ロ）バックアップの方法

①エクスプローラでコピーを作っておく方法

簡単な方法としては、エクスプローラ画面でハードディスクの中にあるファイルを FD などのメディアにコピーすればよい.
データファイルの数がそれほど多くない人にとってはこれが一番簡単な方法です。
またエクスプロら画面を呼び出さなくても、「ファイル」→「送る」で３．５インチＡドライブへ送ってしまえば、それだけでフロッピーディスクにコピーされてしまいます。(この場合の「送る」は移動でなくコピーですから、元のハードディスク中のファイルはそのまま残っています。
Word, Excel などで作ったデータファイルはこれでかなり賄えるし、筆まめの住所録なども１枚の FD で殆ど充分であると考えてよいでしょう. 一度保存したデータはそれを何度でも上書き出来ますから、定期的に修正バックアップするのも簡単です。
但しこの方法はアプリケーションソフトのコピーを同時に取っているわけではないので、そのデータは当該ソフトの無いパソコンでは読み取る事は出来ません。

②ウィンドウ・システムとしての「バックアップ」を使う方法

もっと正式にバックアップしたければ、Windows の中にあるバックアップのシステムを使ってやれます。
「スタート」→「プログラム」→「アクセサリー」→「システムツール」で「バックアップ」というアプリケーションがありますのでこれを実行すればよいのです。
このスタートアップアイコンをデスクトップに取って置くとその後の定期的バックアップが簡単に出来るでしょう。

もしも上の方法でバックアップが見つからない時は、ウィンドウの設定段階でこれを入れていないと言う事なので、下記の方法で設定をします。
「マイコンピュータ」→「コントロールパネル」→「アプリケーションの追加と削除」で、「Window ファイル」タブをクリックし、ファイルの種類から「システムツール」を選んで下さい。
「説明」→「詳細」の中から「Microsoft バックアップ」のチェックを入れてやればこのアプリケーションが入って来ます。

このバックアップは意外に簡単でウィザードの画面に従って進んで行けばよいだけですし、ドライブの中の任意のフォルダーのみのバックアップも出来るので直ぐに馴れて使えるようになります。
また一度バックアップを取ったファイルをその後の変更に応じてバックアップのし直しをして保存するのもこの方法で簡単にやることが出来ます。

③究極のバックアップ

一番完全な形でバックアップを取る方法はと言われれば、現段階では外付けのハードディスクに自分の PC 内のハードディスクをそっくりそのままバックアップする事でしょう。
この外付け HDD は最近容量も８GB 以上でも SCSI が認知するようになったし、値段的にも革命的に安くなったので前に述べたような様々なメディアを沢山使ってバックアップを取るよりよほど簡単です。
このハードディスクは外付けですから、PC のヴィルス感染やクラッシュによる HDD フォーマットの危険からは完全に圏外となります。
しかしこのハードディスクもまたクラッシュの運命からは免れないので、この中の重要なデータを定期的に CD で取って置くと言うパソコンの達人が居られましたが、茲まで来ればそれこそ究極のバックアップと言ってよいでしょう。

以上/