ウィルスの現状と対策

総合情報基盤センター　技官　山田　純一
j_yamada@cns.toyama-u.ac.jp

1. はじめに

年々、大容量化、高速化していくインターネット社会に企業や個人などが参加する割合はかなり多くなった。その反面、コンピュータウィルス（以下、ウィルスと呼ぶ）は後を絶たなくなり、更には年々、増加し、進化し続けている。ここでは、2003 年におけるウィルスの現状と今後のウィルス動向、その対策について説明する。

2. ウィルスとは

ウィルスとは悪意のあるプログラムの事を指し、狭義にウィルスを定義した場合、ウィルスは一般的に

① 表計算やワープロソフトのマクロを利用したマクロウィルス
② 増殖はせず、コンピュータに潜み、クラッキングするために利用するトロイの木馬
③ 自己繁殖して次々と感染を広めていくワーム

の約 3 種類に分けることができる。また、トロイの木馬とワームが連携したウィルスなども存在する。これらのウィルスに感染すると、様々な被害が発生する。どのような被害が起こるかはウィルスによって違うが、主に

① 勝手にプログラムが実行される。
② パソコン内部の重要な情報が外部に漏れる。
③ パソコンやネットワークに負荷がかかり、動作が遅くなる。
④ パソコンやデータが破壊される。
⑤ 特定のサイトの攻撃やスパムメールの踏み台にされる

などの被害が発生する。

3. 従来のウィルスとの比較

現在、大半のウィルスは受信したメールの添付ファイルを開くなど、ユーザーの操作で感染し、更に感染を拡大した。また、従来はウィルスメールが届いた時、送信元メールアドレスから、感染源が分かったが、最近のウィルスメールは送信元を偽装するため感染源の特定が難しくなっている。Microsoft やウィルス対策ソフト各社などの企業名に偽装したもの、感染したパソコン内にあるアドレス帳やWebのキャッシュから送信元を偽装するなど、手口は巧妙化している。それに加え、添付されるウィルスファイルにしても同様な傾向が見られる。例えば、登録されている拡張子を表示しない場合、ウィルス「test.exe」を「test.jpg.exe」といったファイル名にすると、「test. jpg」に偽装され、初心者には画像ファイルのように見えるのである。送信元を偽装するウィルスには SWEN や SOBIG などがある。ウィルス対策ソフト各社の被害件数を見ても、2003 年は SWEN や SOBIG の被害も多かったことが分かる。

富山大学においてもこれらのウィルスの攻撃があったが、VirusWall により遮断されている。なお、昨年 8 月から 12 月までの主要なウィルスの攻撃回数は以下の図 1 の

通りである。なお、各ウィルスは亜種も全て含んで集計してある。

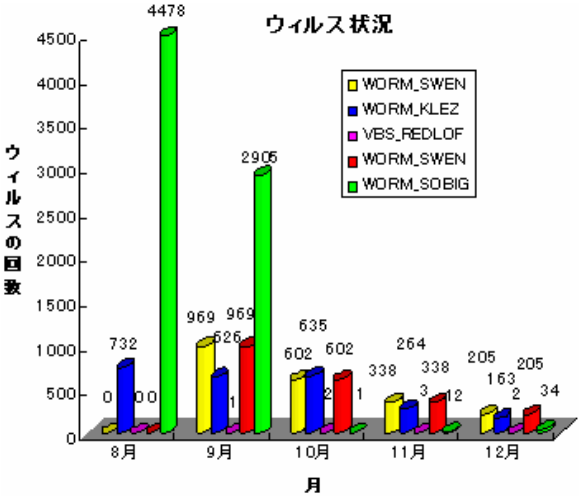

図 1　主要なウィルスの攻撃回数

さらに、最近の新しいウィルスは OS やソフトのセキュリティーホールを狙ったものが増えてきている。

4.　新しい形のウィルス

2003 年 8 月には、インターネットを経由して、Windows パソコンに感染し、勝手にパソコンの動作を終了させてしまう、新種のウィルス「WORM_MSBLAST.A / 別名：W32.Blaster.Worm / W32/Lovsan.Worm（以下、Blaster と呼ぶ)」の被害が世界的に拡大した。このウィルスが今までのウィルスと違う点は、ウィルス対策ソフト及び Windows の修正プログラムがインストールされてないマシンは、ネットワークに接続しただけで感染した点にある。

Blaster は、Windows2000/XP で標準機能として備えている、RPC DCOM の欠陥を狙ったウィルスである。RPC DCOM は、ネットワーク上の異なるマシンで通信を行うものであり、データの交換や処理依頼のやり取りなどをする。また、Windows の起動と共に必ず動き、TCP の 135 番ポートを開いている。以下は Blaster に感染するときの動作である。

① Blaster に感染したパソコンはランダムな IP アドレスの TCP135 番ポートに向かって、大量のパケットを送信する。

② Windows の修正プログラムがあたっていないパソコンはこのパケットによって、RPC DCOM のバッファ・オーバーフローが起こり、送り込まれた不正プログラムを実行する。

③ 不正プログラムによって、TCP4444 番のポートを開き、Blaster 本体を攻撃側のパソコンからダウンロードして実行する。

④ その結果、Blaster に感染し、今度は他のパソコンへ攻撃を始める。

⑤ また、感染したパソコンは RPC DCOM がバッファ・オーバーフローを起こしているので、システムが不安定になり、頻繁にパソコンが再起動したりする。

富山大学では総合情報基盤センター（以下、センターと呼ぶ）において、早急にこのウィルスが用いる TCP135 番ポート等を閉鎖するなどの対策を取ったが、学外から感染したノートパソコンを持ち込まれたことにより、被害が発生し、拡大した。これまでの富山大学の Blaster 感染状況をまとめると図 2 の通りになる。

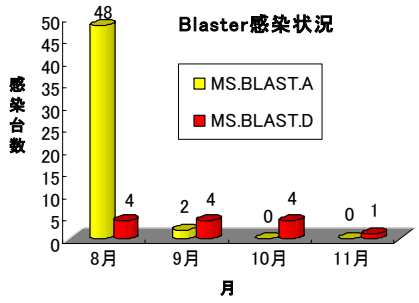

図 2　富山大学の Blaster 感染状況

最も被害の大きかったのは 8 月で、Blaster の発生後、学外から持ち込まれたノートパソコンによって、対策のないマシンが一気に感染したのが分かる。しかし、図 2 はセンターにおいて確認し、対処したパソコンのみなので、実際の被害はこれよりも大きくなる。現在は各セグメントにおいてのポート閉鎖に加え、センターから各教員方への対策を行った結果、このウィルスの被害は沈静化したものと思われる。

しかし、今後もこのようなウィルスが出てくる可能性は非常に高く、それに対して、各ユーザーがセキュリティ対策をしっかりしなければならない状況である。

5.　ウィルスへの対策

ウィルス対策にまず効果があるのはウィルス対策ソフトの導入である。富山大学内においても、感染したパソコンにウィルス対策ソフトのないものが幾つかあった。それに加えて、ウィルス対策ソフトを導入していても、ウィルス定義ファイルが古い状態のままになっているものがあった。Blaster に感染したパソコンの大半がこのいずれかの状態であった。

ウィルス対策ソフトは主に

① アクセスするファイルにウィルスがないか常にチェックするリアルタイム監視。

② 設定した時間にパソコン内にウィルスがいないかチェックする定期スキャン。

③ ウィルスを発見した場合、ウィルスを取り除くウィルス駆除。

の役目を持っている。

ウィルス感染からパソコンを守るためにはウィルス定義ファイルを常に最新のものにし、かつリアルタイム監視を有効にし、定期スキャンを実行することで大抵のウィルス感染は防げる。この中でも、特にウィルス定義ファイルの更新は重要であるが、例えばウィルス定義ファイルの更新時間を設定しても、連休等で長い間、パソコンを使用しない場合や設定した時間にパソコンの電源が入っていなければ更新は行われない。その場合、今回の Blaster のように、連休の間に発生したウィルスに感染する可能性はとても大きくなる。そのため、ウィルス定義ファイルを常に最新のものにすることは重要である。

メールの添付ファイルによるウィルスの対策としては、従来の通り怪しげなメールの添付ファイルは開かないで削除する。また、添付ファイルだけのメール、特にファイルの拡張子が exe や com などの実行ファイルである場合は、ウィルスである可能性が高い。逆に、ファイルを添付したメールを送るときには、メールの本文に添付ファイルの個数や名前などを記述することも 1 つの対策である。

次に、ウィルス対策ソフトによるウィルスの対策方法については説明したが、OS の欠陥を狙ったウィルスが発生した場合、ウィルス対策ソフトではウィルスを防げない場合がある。Blaster の場合も攻撃パケット

で RPC DCOM がバッファ・オーバーフローを起こすのは防げない。要するに、ウィルス対策ソフトを導入してもセキュリティーホールがある限り、ウィルスは侵入し続ける。しかし、これに対する Windows の修正プログラムがウィルスの発生するかなり前から公開されており、各ユーザーがそれを適用していれば、今回のような被害はかなり少なかったと考えられる。

このような事態を防ぐためには、緊急の OS の修正プログラムが出た時に、それを常に適用することが必要である。Windows 系には「Windows Update」があり、設定によっては重要な Windows の修正プログラムをパソコンが自動的に適用する。Microsoft にはプログラムの欠陥が多く報告されており、11 月の終わりには Internet Explorer に 7 つの欠陥と複数の脆弱性が報道された。また、研究者によって複数の新たな欠陥が発表されていることもあり、Microsoft は修正プログラムを毎月第 2 火曜日に公開することも報道された。

更に Word や Excel などの Microsoft Office にも欠陥が存在し、それを狙ったウィルスがいつ発生してもおかしくない状態である。そのために、Microsoft Office の Update も行っておく必要がある。

6. まとめ

インターネットがある限り、ウィルスは決してなくなることはない。今後もウィルスは進化し続ける。そして、ウィルスの感染は他人事ではなく、感染した時点で他のコンピュータへの不正攻撃を行っている場合がほとんどである。その原因はユーザーのセキュリティー対策及びウィルス対策の欠如である。ほとんどのウィルスは、以上のようなウィルス対策ソフトの導入と OS の修正プログラムのインストールで防ぐことができる。

しかし、これからウィルスの感染経路は更に多様化すると考えられる。また、ウィルス対策ソフトで検出できないウィルスやセキュリティーホールの発覚と同時にウィルスが発生し、感染を拡大することも考えられる。今後、このようなウィルスの情報をいかに早く集めるか、学外から持ち込まれたパソコンへの対策をどうするか、ウィルスの対策についてどれだけ周知徹底できるかが課題である。

参考文献

1) Trendmicro 社 : http://www.trendmicro.com/jp
2) Symantec 社 : http://www.symantec.co.jp
3) Network Associates 社 : http://www.nai.com/japan/
4) 日経 NETWORK 2003 年 11 月号、日経 BP 社、2003 年
5) Trendmicro 社　2003 年度ウイルス感染被害年間レポート（最終版）: http://www.trendmicro.com/jp/security/report/report/archive/2003/mvr2003-12.htm
6) NETWORK MAGAZINE 2004 年 1 月号、ASCII、2004 年
7) NETWORK MAGAZINE 2003 年 2 月号、ASCII、2003 年
8) CNET Japan NEWS : http://japan.cnet.com/news/ent/story/0,2000047623,20062630,00.htm