蔓延するネットワークウィルスとその対策

The spreading network virus and measures against it

～進化するウィルスとセキュリティの階層化～

米澤基，中村康昭

Motoi YONEZAWA，Yasuaki NAKAMURA

Abstract: This paper shows the network virus and mesures against it.The network serves as a infrastructure now. In such network society, the number of damages by the computer virus is increasing. As for the route of infection, it accounts for 90 percent from networks. As mesures against such network virus, Division by class of security is introduced.

1　はじめに

我が国の情報化は，コンピュータネットワークやパソコン等の普及により，着実に進展しており，セキュリティ確保の問題が非常に重要となっている．コンピュータウィルスの感染経路は数年前まではフロッピーディスクなど外部からの媒体によるものが多くの割合を占めていたが，現在ではメールなど，ネットワークからの感染が 9 割を占める．

本稿では，このようなネットワーク環境を利用して感染を広げるコンピュータウィルス，つまりネットワークウィルスに注目し，なぜここまで驚異的に広まるのか，また，実際にどのようなものがあるのかを述べた後，その対策を示す．

2　ウィルス感染経路の推移

1996 年以降のコンピュータウィルスの感染経路の推移を Fig. 1 に示す．

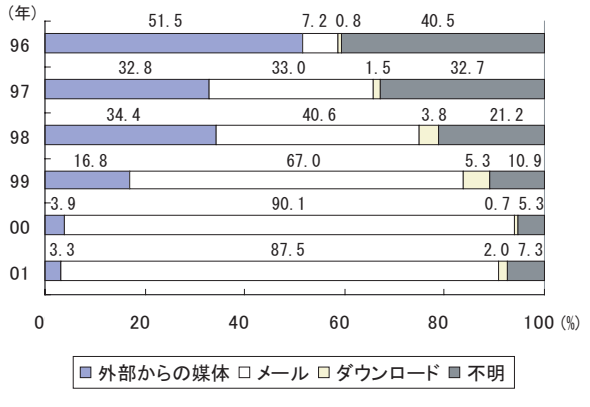

Fig. 1　感染経路の推移 [1)]

Fig. 1 を見ると，1997 年からメールによる感染の割合が急増しているが，これはマクロウィルスの出現に起因している．マクロウィルスとは Microsoft Office などが持つマクロ機能を悪用して自己増殖や破壊活動を行なうコンピュータウィルスである．それらの中には自動的に自らをメールに添付し送信する機能を持つものも存在し，爆発的に拡散する．1999 年からはメール機能を悪用したウィルスが増え，その傾向は現在も続いている．

次章で，昨年メールから爆発的に感染が広まったネットワークウィルスの例として「Badtrans.B」を取り上げる．

3　Badtrans.B

3.1　Budtrans.B の概要

Badtrans.B とは Badtrans.A の亜種であり，2001 年 11 月に作成され放たれたワーム[1]に分類されるコンピュータウィルスである．感染するとワーム活動のほかに，キー入力を盗むというトロイの木馬[2]の特徴も持ち合わせている．昨年最も被害を及ぼしたネットワークウィルスである．

3.2　Budtarns.B の感染方法

Badtrans.B が爆発的に広まったのには理由がある．Badtrans.A と Badtrans.B はともに自身をメールに添付して送信するが，Badtrans.A がその添付ファイルを実行しない限り感染しないのに対し，Badtrans.B は Outlook や Outlook Express といったメーラーでそのメールをプレビューしただけで添付ファイルが実行され感染してしまう．これは Microsoft の web ブラウザ Internet Explorer(IE) のセキュリティホールをついたものだ．

ここで，このセキュリティホールについて説明する．Badtrans.B の本文は HTML 形式である．Outlook は HTML メールを受信すると IE にその処理をゆだねる．IE は HTML メールを表示し，メールにバイナリ形式[3]の添付ファイルが存在する場合，その MIME[4]タイプに合った方法で開くことができる．この時，ある種の不適切な MIME タイプが指定されている場合，添付ファイルが

[1]単独のプログラムとして活動し，ファイル感染はしない．ネットワーク環境で増殖する．

[2]ワーム同様単独のプログラムで活動し，データの破壊，改ざん，または盗聴を行う．

[3]テキスト形式以外のデータ形式全般のこと．

[4]メールで，各国語や画像，音声，動画などを扱うための規格．

自動的に実行されることがある．

Badtrans.Bはこのセキュリティホールをついて感染を広げた．このセキュリティホールについては，Badtrans.B登場以前からMicrosoftから警告されており，修正パッチも公開されていた．しかし，それらのアップデートを実行していなかったり，存在を知らないユーザが大勢いた．このことがBadtrans.Bが蔓延した大きな要因といえる．

4 コンピュータウィルスへの対策

ネットワークウィルスへの対策としてはワクチンソフトの導入がもっとも有効である．しかし，IPA(Information-technology Promotion Agency)[5]の調査によると，国内の企業のほぼ9割がウィルス対策を導入しているという結果が出ているにもかかわらず，感染被害報告は増える一方である．これは，ネットワーク上にウィルス対策が行われていないコンピュータが1台でも存在すると，その1台の感染によりネットワーク全体にウィルスが蔓延するためである．このような事態を防ぐには，クライアントPCでのセキュリティレベルの統一が重要となる．またそれ以外に，ゲートウェイ，グループウェア[6]サーバやファイルサーバなどの各層でウィルス対策を行う必要がある．

4.1 ワクチンソフトの分類

現在，次のようなワクチンソフトが提供されている．

1. **クライアントPC用ソフト**
   ウィルスの大半はクライアントPCに感染するものである．そこでクライアントにワクチンソフトをインストールし，メールやファイルに対してウィルスの検出および駆除を行う．現在ではシステム管理者が一括管理可能なワクチンソフトも開発されており，それを導入することによりシステム全体のセキュリティレベルを統一することが可能となる．
2. **グループウェアサーバ，ファイルサーバ用ソフト**
   これらのサーバではアプリケーションやファイルを共有するため，感染による被害は急速に拡大する．ファイルサーバでは外部からアクセス可能なものもあり，加害者となることもある．グループウェアサーバやファイルサーバを運用している組織では，それぞれにワクチンソフトをインストールすることにより，共有アプリケーションや共有フォルダを守る．ただし，サーバを介さない記憶媒体によるクライアントの感染には対処できない．
3. **ゲートウェイ用ソフト**
   SMTP，HTTP，FTPによるインターネットアクセス時に，そのアクセスを中継するゲートウェイ上でウィルスを監視および除去する．ただし，サーバ用ソフトと同じく，記憶媒体からの感染は防ぐことができない．

以上のように，それぞれ守るべき対象が異なるため，ウィルス対策に万全を期すにはどれか一つでは不十分である．しかし，導入費用や初期設定，運用のためのコストを考えるとすべての導入は難しい．そこでもっとも効果的な対策としてゲートウェイ用ソフトの導入があげられる．集中管理ができ，また，大半のウィルスの感染経路であるメールを一括して監視および駆除できるためである．

4.2 ウィルス検知技術

ワクチンソフトのウィルス検知技術には代表的なものとして次の二つがあげられる．

- **パターンマッチング方式**
  ウイルスプログラム内の特徴的な部分を「パターン」として取り出してデータベース化しておき，それを検索対象のファイルの内容と照合する方法．
- **ルールベース方式**
  ウイルスの活動を分析して「ルール化」しておき，プログラムの動作を監視し，「ルール」と合致する動作をするプログラムをウイルスとして判定する方法．解析が済んでいないウイルスに対しても有効だが，ウィルスだという確証を得にくい．

5 今後の展望

ワクチンソフトの発達により，一部でのウィルス対策はより強固になると考えられるが，社会全体的なセキュリティに対する意識はまだまだ低い．ネットワークがインフラとなっていくこれからは，ウィルスによる被害は増え続けると考えられる．

また，これまでは端末と言えばPCが中心であったが，PDAや携帯電話などからはもちろん，今後はカーナビ，テレビ，およびゲーム機等からの接続も増えることになる．これらの端末はすべてネットワークウィルスの脅威と対面することになる．すでに，携帯電話のOSに感染するウィルスは登場ている．近い将来，テレビやゲーム機に感染するウィルスも出現するかもしれない．

参考文献

1) IPAセキュリティーセンター．
   http://www.ipa.go.jp/security/index.html.
2) コンピュータウィルスの被害の現状と対策管理．
   http://www.ipa.go.jp/security/awareness/administrator/virus.pdf.

[5]情報処理進行事業協会．1970年10月に設立された政府関係機関．

[6]業務を効率的に処理するためにネットワークを利用してグループで作業するためのソフトウェア．電子メール，電子会議，進行管理などのシステムがある．