題　目　コンピュータウィルスとセキリュティー対策

発表者　田　中　雅　章

はじめに

情報処理の形態が汎用機を主体とするスタンドアロンから、ワークステーションやパソコンを主体としたインターネットを活用したネットワーク中心のシステムに変わってきた。それに伴い、コンピュータを利用した犯罪が急激に増加してきた。ネットワークを悪用した、ネット犯罪である。以前からコンピュータを利用した犯罪は存在した。しかし、罪を犯す人間はコンピュータの専門家に限られており、内部犯行が多いため警察による検挙率も高かった。ところが、インターネットなどのネットワークを利用した犯罪は、インターネットの匿名性を悪用したものである。そのため、犯人の特定が困難であり、犯人の検挙率もあまりよいとは言い難い。

コンピュータウィルス

コンピュータウィルスとは、コンピュータの基本ソフトに潜む悪質なプログラムの一種である。ネットワークを媒体として、コンピュータからコンピュータへソフトウェアがコピーされて続けていく様が、人間がインフルエンザウィルスなどに感染する様子に似ているため、ウイルスと呼ばれるようになったのである。コンピュータウィルスは、ハードディスク内のデータ破壊、システムを不安定にさせるなど、何らかのメッセージを送るために、心ない人間によって作成されたプログラムのことを指す。コンピュータウイルスは、生物ウイルスのように有機的なものではない。人間に感染したり、自らの意志で不規則に活動したりすることもない。コンピュータウィルスには、一般的なファイル感染型、マクロウィルス、トロイの木馬型、ワーム等がある。

ファイル感染型は、拡張子.COM、.EXE、.SYSなどの実行型ファイルに感染し、ファイルが実行される度にウイルスプログラムも実行される。ウイルス単体はプログラムを実行したり複製することは出来ないが、実行型ファイルに付着してその制御を奪い、プログラムを書き換えることによって感染増殖する。プログラムの処理を一時中断させ、ウイルスプログラムを実行した後に本来の処理に戻る。一般的には、ウイルスプログラムを実行した後に本来のプログラムを正常に実行されるため、その感染にほとんど気づくことはない。

マクロウイルスは、MicroSoft WordやExcelのマクロ機能を利用して感染するのである。機種・OSに依存ないため大抵のパソコンに感染する。マクロウイルスはWordやExcelがファイルをオープンした後に感染する。マクロ自体が、WordやExcelの正規な機能であるため、OSがその中の特異な活動を見分けるのは難しいといえよう。マクロウイルスはVisual Basicが書ける知識があれば簡単に作成出来てしまう。また、マクロ言語が判れば改造することも容易である。開発の容易さ、電子メールの普及などさまざまな条件が絡み合って、その被害件数を急激に増加させている。

トロイの木馬型は、ほかのファイルやシステムに感染活動を行わない、増殖を目的としないウィルスのことである。サーバー・クライアントに侵入するタイプが多い。ネットワークを介して被害者のマシンを自由に操ったり、またパスワードなど重要な情報を盗んだりすることを目的とする。いわゆるハッキング・ツールである。サーバーモジュールをクライアント・モジュールから遠隔操作する形式になっている。「便利なツール」などと称してサーバーモジュールがメールなどで送られてくることがあるが、うっかり解凍してインストールしてしまうと、そのマシンは他人から勝手に操作されてしまうことになるのである。

ワームは、ファイルやシステム領域に感染することはないが、ネットワークを通じてほかのマシンに拡散することを目的としたウィルスである。このタイプの特徴は、従来のウイルスにはないその強い増殖能力である。従来型のウイルスは、ネットワーク感染を志向したものではなかった。ウイルスが感染を広げるには、「感染したファイルを人がやり取りする」という偶発性に期待する必要があった。このため拡散スピードは比較的緩やかであり、被害が大規模なものになるには、数カ月から数年を要した。

これに対して、ワーム型はネットワークによる拡散することを追求している。ローカルネットワークを利用して拡散するワームは以前から存在した。このころのタイプは接続されているマシンの共有ドライブに自分自身をコピーすることでLAN内部で増殖することができた。インターネットが普及した現代のワームの特徴は、メールを最大限に利用することにある。ワームは、ワームプログラム自身を添付したメールを自動送信する機能を持っている。そのため、あっという間に世界中に広がってしまった。今なお続く被害報告は、ラブレターウイルスやMTXなど、メールを悪用するタイプのワームがほとんどである。

おわりに

筆者らグループは、90年より東海地区において各企業が、危機管理にどのような対策を講じているかを調査し続けている。97年頃からウィルス被害が目立つようになってきた。昨年では、３社に１社の事業所がコンピュータウィルス被害を被っている。

その対策として、各県警察本部は西暦2003年度の電子政府の実現や電子商取引の促進、教育の情報化をめざし、官民挙げて取り組みを始めた。県警察本部が主体となり、産・官・学による連絡協議会を発足させた。本年より、ネットワーク・セキリュティ・カンファレンスが開催される予定である。