

コンピュータウイルスの歩み

伊藤和行

1. 序

昨年2001年の後半におけるコンピュータに関わる最大のニュースはインターネットを通じてのウイルスの大流行だったのではないだろうか。コンピュータウイルスはこれまでも何度か社会的問題になっていたが、7月に出現した"Code Red"はWindowsウェブ・サーバーを感染対象としたことで、また9月の"Nimda"は感染経路として電子メールのみならず、ウェブ・ページを利用したことで大きな大きな話題となった。さらに11月末に現れた"Badtrans.B"はメールを通じて瞬く間に世界中に広がったことが知られている。我が国においてウイルス発見時の届け出機関となっている情報処理振興事業協会セキュリティセンター(1)の発表によれば、2001年の年間ウイルス届け出件数は前年比2倍以上となる約2万4000件であり、12月には3900件という月間としては最悪を記録している(2)。コンピュータウイルスは、電子メールがコミュニケーションの手段として一般化し、WWWを中心としてインターネット・テクノロジーが急速に発展した状況に即応し、その感染方法を大きく変えてきた。以下では、コンピュータウイルスの歩みを、その誕生から辿ることにする。

1.1 コンピュータウイルスの定義

コンピュータウイルスとは、その名称が自然界に存在するウイルスにちなんだものであることから窺われるように、コンピュータに外部から侵入し、他のプログラムに伝染・寄生し、プログラムやデータなどの改竄や破壊といった動作を引き起こすプログラムである。経済産業省の「コンピュータウイルス対策基準」によれば、コンピュータウイルスは次のように定義されている(3)。

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

コンピュータのユーザに不利益を及ぼすプログラムとしては、ここで定義されているようなウイルスの他にも「ワーム」や「トロイの木馬」などが存在しており、これらは「不正プログラム」

(Malicious Program) と呼ばれている。「ワーム」(Worm=蠕虫ぜんちゅう)は、ウイルスが他のプログラムに寄生して増殖するに対して、単独で自己増殖可能なプログラムで、ネットワークを介して他のコンピュータに感染していくもので、ネットワーク内を這い回るように見えることから、このように名づけられた。「トロイの木馬」はその名前の通り、一見すると何も害のないプログラムに見せかけ、一度実行するとシステムを破壊したり、ユーザー情報を知らない間に他のコンピュータへ送信したりするものである。「ワーム」や「トロイの木馬」は他のプログラムにコピーされないの、厳密な意味では「ウイルス」とは異なるが、通常は不正プログラムの総称として「ウイルス」という名称が用いられ、これらも通常は「ウイルス」と呼ばれている。以下の記述でも、「ワーム」や「トロイの木馬」を「ウイルス」に含めることにする。

1.2 コンピュータウイルスの分類

現在までに知られているウイルスの数は膨大であるが、その感染する部所や方法によっていくつかに分類されている(4).

1. ブートセクタ (システム領域) 感染型ウイルス
フロッピーディスクやハードディスクにおいて、コンピュータが起動する際に参照するシステム情報が書き込まれた部分である「ブートセクタ (システム領域)」に感染する.
2. ファイル感染型ウイルス
プログラムファイルに感染する.
3. 複合感染型ウイルス
ブートセクタとファイルの両方に感染する.
4. マクロウイルス
Ms WordやExcelのマクロ言語で書かれたもの.
5. Javaウイルス
Java言語で書かれ、Javaアプレットやアプリケーションに感染する.
6. VBSウイルス
Visual Basic Scriptで書かれ、HTMLファイルに感染する.
7. ワーム
8. トロイの木馬

最初の三つはウイルスの誕生当時の分類で、感染する部所によって分類されている。残りはインターネットの発展とともに現れたもので、近年猛威を振るっているのはこれらである。

2. コンピュータウイルスの誕生

2.1 「コンピュータウイルス」の発明

「コンピュータウイルス」("Computer Virus")という言葉が公的な場で最初に用いられたのは、1984年、南カリフォルニア大学の電気工学科博士課程に在学していたFrederick B. Cohenによるコンピュータ・セキュリティ学会における発表だったといわれる。それに先立ち、すでに1983年にCohenは、大学で毎週行われていたコンピュータ・セキュリティに関するセミナーにおいて自己増殖プログラムの実験を行っていたことが知られている。Cohenは、「コンピュータウイルス」に関する最初の論文において、コンピュータウイルスについて次のように定義したが、この定義は現在でもウイルスを論じる際にはしばしば言及されている。

We define a computer 'virus' as a program that can 'infect' other program by modifying them to include a possibly evolved copy of itself. With the infection property, a virus can spread throughout a computer system or network using the authorizations of every user using it to infect their programs. Every program that gets infected may also act as a virus and thus the infection grows. (5)

Cohenが実験を行ったのはUNIXマシンだったが、実際に流布したウイルスはパソコン(すなわちPC = Personal Computer)を感染対象としていた。というのは、UNIXマシンはネットワーク上で複数のユーザーが用いることを前提としてOSが設計されており、ファイルのアクセスに対して制限が課せられているに対して、パソコンは単体で「善良な」ユーザーによって用いられることが前提とされており、システム・ファイルも含めてアクセス制限がまったくなされておらず、ファイルの改変が容易にできるからである。

2.2 PCウイルス

PCウイルスの感染として文書が残っている最初のもは、1987年10月22日における、デアウェア大学のアカデミック・コンピュータ・センターにおける"Brain"によるものだった(6)。このウイルスは感染したフロッピーに"Brain"というVolume Labelを付けることからこの名称が与えられたが、ファイルの破壊などの被害を及ぼすことはなかった。"Brain"はブートセクタ感染型ウイルスであり、感染したフロッピーから起動するとメモリに常駐し、アクセスするフロッピーのブートセクタに感染する。

1987年には、さらにファイル感染型ウイルスが相次いで出現している(7)。その最初のもの一つである"Lehigh"は、"COMMAND.COM"にのみ感染するために感染力が弱かったが、感染した"COMMAND.COM"の数が4つになると、フロッピーのブートセクタとFATを上書きし、データを破壊する。イスラエルのヘブライ大学で発見されたところから、そう呼ばれる"Jerusalem"は"EXE"ファイルに感染し、"Lehigh"よりも大きな感染力を持っており、13日の金曜日になると、処理スピードを遅くし、実行したファイルを削除する。

初期のファイル感染型ウイルスとして最も強力であり、コンピュータ・ウイルスという言葉が知られるようになる契機となったのは"Cascade"である。このウイルスが発病するとディスプレイに表示されている文字が流れ落ちていくことからこの名称が付けられた。これは、感染すると、メモリに常駐し最初に実行される"COM"ファイルに感染する。また他の部分を復号化するために必要な非常にわずかな部分を残してほとんどの部分が暗号化されていたため、感染したファイルの修復が困難だった。"Cascade"はIBC PCおよび互換機のウイルスであるが、MS-DOS機であれば、国産機(NEC PC98シリーズ)でも感染し、日本では1990年末に発見が報告されている。

2.3 インターネットワーム

2001年に猛威を振るったウイルスのほとんどはインターネットを介して自己増殖するワームの性質をもったものだったが、ネットワークに最初にワームが放たれたのは1988年11月2日のことである(8)。このプログラムはSun 3システムと4 BSD UNIXが動作するVAXコンピュータに感染し、インターネットの先駆であるアルパネットに接続された全米のコンピュータ約3000台に侵入した。このワームの攻撃は、ユーザー情報を知るためのソフトfingerdとメール・サーバ・ソフトsendmailのセキュリティーホールにアクセスし、さらにpasswordの探索を行った。このワームを放った犯人は数日後に判明したが、それはコーネル大学コンピュータ・サイエンス学部在籍する大学院生Robert Morrisだった。彼の供述によれば、ネットワーク・セキュリティの不備を訴えるためにワームを放ったのだが、予想よりも増殖と感染の速度が速く、駆除方法を電子メールで送ろうとしても、ワームに阻まれて配信できなかったということである。

しかしながら、ある限定されたネットワーク内におけるワームの実験は、すでに1970年代後半にゼロックス社のパロアルト研究所(PARC = Palo Alto Research Center)においてJohn F. ShochとJon A. Huppによって行われていた(9)。彼らは、自己複製プログラムを、ネットワークの維持管理を助けるという有益な目的のために使うことを考えたのである。そのプログラムはネットワークに繋がれたコンピュータにおいて、ファイルのバックアップの作成や診断チェックを行いながら、次々と他のコンピュータへ移動していくものである。彼らの実験では、ワームは、指定されたコンピュータに移動し、自身のコピーを置いてくるようにプログラムしてあった。しかし実際にはワームがあまりに急速に増殖し、コンピュータのメモリ空間を占有してしまい、停止してしまう状態に陥った。ワームの安定した振舞いを維持しながら、増殖を制御することが極めて困難だったために彼らは実験を中止してしまった。彼らがこの自己増殖プログラムを「ワーム」と名づけたのは、1975年に発行されたJohn BrunnerのSF小説The Schockwave Riderの中に出てくる、ネットワークの中を自由に動く回る万能プログラム"tapeworm"に着想を得てだった(10)。

3. MS-DOSからWindowsへ

3.1 MS-DOSの時代

1990年代の前半まではまだインターネットが一般化しておらず、ほとんどの感染源はフロッピーディスクだったので、海外で発見されたウイルスが国内で発見されるまでにはかなりの時間が経過するのが通常だった。また当時日本国内で用いられていたパソコンの大部分はNEC PC98シリーズであり、海外の標準機であるIBC PCとは互換性がなかったため、海外では猛威を振るっても国内では流行しなかったウイルスが多かった。そのようなウイルスでもっとも有名なのが1992年の"Michelangelo"である。これはルネサンスの芸術家ミケランジェロの誕生日である3月6日に発病することからそう名づけられたが、発病するとハードディスクのデータを破壊するブートセクタ感染型ウイルスである。アメリカでは、多くの会社のオフィスで発見され、当時のFBI長官が対策を呼び掛ける声明を出す騒ぎとなり、マスコミが大きく取り上げたことで、コンピュータウイルスの存在が大きな社会的な問題となった(11)。そして"Michelangelo"のおかげで、ワクチンと呼ばれるコンピュータウイルス対策ソフトおよびその開発する会社が社会的に認知されるようになった。そして1993年にMicrosoft社がMS-DOS 6.0を出荷した際には、ワクチンソフト (Central Point Anti Virus) がバンドルされていた。

1990年代に入ると、ウイルスの数は急速に増大していき、様々な変種が登場している。その主要な理由の一つは、容易にウイルスの作成を可能にするウイルス作成ツールがコンピュータ通信を通じて配布されたことにある。その最初のもは1992年3月に米国で現れた"VCL" (= Virus Creation Laboratory) である。これを用いると、感染、潜伏、発病の方法を選択して作成者の好みのウイルスを作成することが可能になった。さらに7月には、"PS-MPC" (= The Phalcon/Skism Mass-Produced Code Generator) も現れている。これらによれば、1時間もかからずに、数十の異なるウイルスを作成することができた。

また同じ年には、ミューテーション型 (ポリモフィック型) ウイルスを作成するためのツール (Polymorphic Generator) も出現した。ミューテーション型ウイルスは、感染するたびに異なった暗号をランダムに生成し、その暗号を自分自身にかけることによって姿を変更する。そのためウイルスパターンとの比較によって暗号を検出するワクチンでは検出がきわめて困難になった。最初のPolymorphic Generatorは、ミューテーション型ウイルス"Mutation Dark Avenger"の作成者が配布した"Mutation Engine"であるが、以後多数のツールが現れた。その結果、プログラムの知識の余りない者がツールによって作成したウイルスが多数出現し、思いもよらない社会的被害を及ぼす事件も発生した。

3.2 Windows 時代 マクロウイルス(12)

1992年にWindows 3.1が現れた (日本では1993年) ことによって、ウイルスも変化を余儀なくされた。それまでブートセクタ感染型ウイルスとファイル感染型ウイルスが同じような割合で出現したのに対して、1992年ころから後者が劇的に減少していったのである。その理由は、Windows 3.1では、ファイル感染型ウイルスに感染するとシステム全体が強制終了されたため、ユーザーはウイルス駆除を行うことになったことにある。一方ブートセクタ感染型ウイルスでは、そのようなことがなく、発症するまでさらに感染を広めることが可能だったのである。

だが、このようなWindows 3.1におけるブートセクタ感染型ウイルスの繁栄も、Windows 95が1995年に (8月に発表、日本語版の発売は11月) 登場したことによって終焉を迎えることになる。というのは、Windows 95は、ブートセクタに対する変更を察知すると、ユーザーに対して警告を発するようになっていたからである。そしてこの年、実行形式ファイルではなく文書ファイルに感染するウイルスが登場した。それまでのウイルスはすべて"COM"や"EXE"という実行形式ファイルに感染するものであって、文書ファイルは感染することがないと考えられていたので、その出現は大きな衝

撃を与えた。それは、マイクロソフトのアプリケーション・ソフトWordやExcelのマクロ機能を利用して感染するマクロウイルスである。マクロウイルスは、90年代後半には、ブートセクタ感染型ウイルスに変わって流行の中心となった。

最初のマクロウイルスは、8月にWindows 95とともに現れた"Concept"である。このウイルスは、Microsoftのワープロ・ソフトMS Wordのマクロ言語で書かれており、電子メールの添付ファイルによって広まった。このウイルスに感染した文書を開くと、拡張子は文書ファイルの"DOC"のままであるが、マクロファイルの".DOT"ファイル形式に変換され、ウイルスマクロが標準テンプレートである"NORMAL.DOT"にコピーされる。日本語のWordの場合には、標準テンプレートが"標準.DOT"であるため、感染しなかった。

マクロウイルスが広範に流行した第一の理由は、実行形式ファイルとは違い、文書ファイルは、電子メールの添付ファイルとして頻繁にやり取りが行われていたことがある。またMS Wordが動作するものであればPCでなくアップルでも感染するというマルチプラットフォームという特質を持っていた。マクロは扱いやすい言語で書かれており、さらにウイルスがソースコードから構成されているため、従来のウイルスに比して作成が非常に容易であったので、以後多くのマクロウイルスが出現することになった。1995年10月には、感染した文書ファイルを開くと"Wazzu"（この名称はワシントン州立大学の愛称である）という単語を挿入する文字挿入型マクロウイルス"Wazzu"が出現し、以後様々な変種が現れている。

MS Wordと並ビジネス・ツールである表計算ソフトExcelの代表的なマクロウイルスは1996年7月に現れた"Laroux"である。"Laroux"には、2つのマクロ("auto_open"と"check_files")が含まれており、感染したExcelブック（Excelのデータファイル）を開くと、自動的に"auto_open"マクロが実行され、さらに"check_files"マクロを実行し、"XLSTART"ディレクトリに"PERSONAL.XLS"というファイルが存在するかどうかをチェックする。そのファイルが存在する場合には感染しないが、存在しない場合にはそのファイルを作成し、自分のマクロをそれにコピーする。その後、作成および編集するExcelブックはすべてこのウイルスに感染する。"Laroux"はその出現以来、数年にわたって流行を続けており、この時期のウイルスとしてはもっとも寿命の長いものといえよう。

4. インターネット時代

4.1 Javaウイルス

1990年代後半はインターネットが急速に普及したが、その牽引車となったのはWWW (= World Wide Web) だった。1994年にグラフィック・ユーザー・インターフェイスを備えたウェブ・ページ閲覧ソフトNetscape Navigatorが登場したことによって、WWWはインターネットをまったく新たなメディアに変貌させてしまった。1995年には、Netscape Navigatorの一人舞台だったウェブ・ブラウザの世界に、Microsoft社がInternet Explorerを開発して参入し、以後3年に涉って、Netscape社とMicrosoft社の間では激しい闘いが繰り広げられた。この闘いは1998年の終わりにNetscape社がAOL (= America On Line) 社に買収されることによって、実質的にはMicrosoft社の勝利に終わった(13)。

この闘いの中でウェブ・ブラウザは様々な機能を備えていったが、その中でもっとも重要なのは、利用するOSに依存しないマルチプラットフォームと、画像、動画、音声を扱うマルチメディアである。両者の中心となったのが、1995年にSun Microsystemsが発表した言語Javaである。この言語はネットワークに接続されたマルチプラットフォームでの実行を目的として開発されており、実行形式のプログラムを必要に応じてサーバーからダウンロードして、メモリ上で実行するように作られている。WWWでは、ウェブ・ブラウザ上で、ウェブ・サーバーからダウンロードしたプログラム（Javaアプレット）を実行することができる。またJavaは非常に強力なマルチメディア機能を装備していたので、ウェブ・ページ上で動画や音声を再生したりするために広く用いられるようになった。

た。

Javaウイルスの特徴は、このJavaの特徴に他ならない。すなわち感染経路がメールの添付ファイルではなく、そのウイルスに感染したウェブ・ページを閲覧した際にウイルスプログラムをダウンロードすることによる点と、Windowsのみならず、Macintosh, UNIXにおいても感染する可能性がある点である。その最初のものである"Strange Brew" (1998年8月発見) は、JavaアプレットとJavaアプリケーションの両方に感染する能力を持ち、大きな話題となった。しかし多くのプログラム・ミスがあり、他への感染は感染したJavaアプリケーションを実行したときだけだった。次いで現れた"BeanHive" (1999年1月) は、9つのコンポーネントから構成され、感染したウェブページを閲覧すると、ウイルスのメインとなるコンポーネントがダウンロードされ、その後次々に必要なコンポーネントをダウンロードしていくように設計されていた。"BeanHive"も"Strange Brew"と同様にプログラム・ミスのために実際に設計通りに動作することはなかったが、以後に現れるJavaウイルスの出発点となった。

4.2 VBSとメール大量送信ウイルス

Microsoftが1998年に発表したWindows 98は、Netscape社とのウェブ・ブラウザを巡る闘いの中から誕生したものであり、インターネット接続機能がOSの重要な機能として含まれ、ウェブ・ブラウザInternet Explorerがシェルとして採用されている。またVBA (= Visual Basic for Applications) のサブセットであるVBS (= Visual Basic Script) が装備され、HTMLファイル内にScriptタグを埋め込むことによってInternet Explorer上でイベント処理が可能になった。VBSは、Windows上でのアプリケーション・ソフト間の提携作業を自動化するもので、MS OfficeにおけるVBAマクロをWindows全体に拡張したものと考えると理解しやすく、MS Word, Excel, Outlook, Internet Explorerといったソフトを連動して使用することができる。Windows 98では標準の電子メール・ソフトとしてOutlook, ウェブ・ブラウザとしてInternet Explorerが用いられるようになったことから、VBSとそれらのソフトとの連携を悪用し、大量のメールを自動送信するウイルスが現れることになる。

インターネットの普及とともに、ウイルスの感染手段はフロッピーから電子メールの添付ファイルに変化した。その場合でも、ユーザーがウイルスに感染していることに気づかずに感染ファイルを電子メールの添付ファイルとして送ることによっていた。それに対して、ウイルスが、ユーザーのアドレス帳をチェックし、自動的にウイルス添付メールを送信するメール大量送信ウイルスが1999年に出現し、以後急速に増加している。それらのウイルスは、VBSを利用し、Outlookのアドレス帳から得たアドレスに対してメールを自動送信する。

メール大量送信ウイルスの存在が社会的に知られるようになったのは、1999年3月に発見された"Melissa"によってである。このウイルスはMS Wordのマクロウイルスであるが、VBSの機能を利用して多数のメールを自動発信する機能を持っていた。すなわち感染したMS Wordの文書ファイルを開くと、ウイルスはMS Wordのマクロウイルス保護機能を無効にし、セキュリティ・レベルを「低」に変更した上で、バックグラウンドでOutlookを起動し、アドレス帳に登録されている最初の50のメール・アドレスに対してウイルス添付メールを送付する。ユーザーの知らないうちに自動的にメールが発信され、感染が広まる点で、このマクロウイルスはワームの性格を持っていると言える。このウイルスのために大量のメールが一斉に送られ、メール・サーバーのトラフィックが急激に増大し、マイクロソフト社やインテル社といった会社のメール・サーバーが一時閉鎖せざるを得なくなった。米国では、FBIが捜査に乗り出し、ウイルスの作成者が逮捕される数少ない事件の一つとなった。

VBSを利用したウイルスは1998年には出現しているが、電子メールにVBSファイルを添付する形のVBSウイルスとしてもっとも流行したのは、2000年5月に出現した"Loveletter"である。このウイ

ルスは、"ILOVEYOU"というタイトルのメールに添付されたファイル"LOVE-LETTER-FOR-YOU.TXT.vbs"を実行すると発病し、Outlookをバックグラウンドで起動してExchangeサーバーにアクセスした後、アドレス帳に登録されているすべてのアドレスに送信されてきたのと同じウイルス添付メールを送信する。さらに発病した際には、既存のファイルへの感染がなされ、jpgなどの特定の拡張子のファイルが破壊されることもある。アドレス帳に登録されたアドレスに"ILOVEYOU"というタイトルのメールを送ることからこのような名前が付けられた。

"Melissa"がメールを送付するのが最大50箇所だったのに対し、"Loveletter"はすべての登録アドレスにメールを送付し、さらにメールアドレスがメールグループになっている場合があるため、非常に多くの数のメールが発信されることにより、メールサーバーに異常に大きな負担が掛かり、ダウンするなどのトラブルが生じるという被害が起こった。"Loveletter"の流行の要因の一つは、その送信メールのタイトルが"ILOVEYOU"という関心を引くものだったことにあった。メールの添付ファイルによって感染するウイルスの存在が知られるにつれ、一般ユーザーは、メール添付ファイルを安易に実行しなくなってきたのに対して、ウイルス製作者は受信者が添付ファイルを実行するようにし向けるため、"Loveletter"のように送付の仕方を工夫するようになってきている。

電子メールを介して感染するウイルスはすべて添付ファイルを用いていたが、メールの本文自体に埋め込まれるウイルスが1999年に現れている。11月に発見された"Bubbleboy"は<=[ルの本文にHTMLを記述するHTMLメールを利用し、本文の中にVBSウイルスを埋め込んでいる。このウイルスは、Internet Explorer 5のセキュリティ・ホールを利用し、メールをマイクロソフトのメールソフトOutlookやOutlook Expressによって開く、あるいはプレビューウィンドウによって表示することによって感染し、再起動後、アドレス帳に登録されているアドレスすべてに感染メールを送付する。このウイルスによって、ウイルスはメールを開いても添付ファイルを実行しなければ感染しないという、従来の常識が覆されてしまった。

4.3 インターネットワーム

"Melissa"や"Loveletter"はマクロウイルスであったが、インターネットを介して単独で増殖する点においてワームの性格を持っていた。1999年より、マクロファイルではなく、実行形式ファイルで書かれた大きなプログラムからなるインターネットワームと、その性格を持つファイル感染型ウイルスが流行し始め、2000年に入り、マクロウイルスよりも大きな被害を及ぼすようになった。

この種のウイルスで最初に大きく流行したのは、"TROJ_SK" (1999年1月)である。このウイルスは、"Happy99.exe"という実行形式ファイルからなることから"Happy99"という通称で知られている。感染すると、ユーザーが電子メールを送信するたびに、自分自身のコピーを添付することによって感染を広めていく。この添付ファイルを受信者が実行すると、モニターの画面上に花火のアニメーションが表示されるが、バックグラウンドではシステムファイルやレジストリが書き換えられている。このアニメーションのためもあり、"Happy99"は1999年から2000年年前半にかけてもっとも感染数の多いウイルスだった。

2000年後半期から2001年前半にかけて流行したのは、インターネットワームの性格をもったファイル感染型ウイルスである"MTX" (2000年9月)と"Hybris" (2000年11月)である。両者とも"Melissa"や"Loveletter"のように多くのアドレスに対して一斉にメールを送信するのではなく、1通ずつ送信するというようにより巧妙にメールを送信するようになっている。"MTX"はインターネットの通信を監視し、ユーザーがメールを送信したすぐ後に、同じアドレスに対して自分のコピーを添付したメールを一通送信する。添付ファイルの拡張子は"PIF", "EXE", "SCR"のどれかであるが、"PIF"ファイルはWindowsでは"PIF"が表示されないために、他の無害なファイルと見誤らせる可能性がある。こうして"MTX"は、その感染の発覚を遅くするように作られていた。また感染時に、バックドアを作るハッキングツールをインストールするという「トロイの木馬」活動も行う。

また"Hybris" (2000年12月) も、インターネット上でのアクセスを監視し、送信および受信メールや閲覧したウェブ・サイトから得たアドレスすべてに対してメールを送付するウイルスである。さらにインターネット接続中にプラグインをダウンロードして組み込もうとする。このプラグインの一つとして、モニターの画面の最前面に白黒の渦巻のアニメーションが表示されるものが知られている。

2001年7月に登場した"Sircam"は、それまでのメール大量送信ウイルスと同様にアドレス帳およびウェブ・ブラウザのキャッシュから見つけたアドレスに対してメールを自動送信するものだったが、それまでで最大の被害を引き起こした。感染方法はそれまでのものと大きく異なっていないにもかかわらず、被害が拡大したのは、用いる添付ファイル名によるところが大きい。従来のウイルスは、いくつかの特定のファイル名から選んで添付ファイル名にしていたので、受信者も用心して実行しないようになってきていた。それに対し、"Sircam"は「マイドキュメント」フォルダ中の任意のファイルを選び、それに自分のコピーを加えて、実行可能ファイルにして添付ファイルとするのである。送信されるメールおよび添付ファイルのタイトルとしては、選ばれたファイルのタイトルが用いられるため、受信者も添付ファイルを開きやすくなり、感染力が増大することになった。さらにユーザの重要なデータが送信され閲覧されてしまうことが起こるといって従来にはなかった被害も生じた。

5. 2001 セキュリティホール悪用ウイルス

5.1 "Code Red"

2001年の夏には、感染経路として電子メールのみならず、ウェブ・サイトも用い、ウェブ・サーバを攻撃する複合型のウイルスが出現し、以後この種のウイルスが猛威を振るっている。その第一歩は2001年7月13日に現れたワーム"Code Red"だった。

このウイルスは、Windows NT/2000用のウェブ・サーバーソフトであるIIS (Internet Information Server) に感染するものであり、その意味ではクライアントが感染する通常のウイルスとは異なっているが、2か月後に現れる"Nimda"によって通常のウイルスと統合されることになる。"Code Red"はIISの"remote buffer overflow vulnerability"というセキュリティホールを利用し、短期間に数十万のウェブ・サーバーが感染したと言われる。その感染方法は、対象となるウェブ・サイトに特殊なURLリクエストを行い、サーバーにバッファのオーバーフローを起こらせ、アプリケーションの支配権を奪って進入する。この際、プログラムはメモリ上で実行され、ファイルとしてセーブされることはないので、感染したサーバーのドライブにファイルとしてワームのプログラムが残ることはない。感染したサーバーは、1日~19日の間は、ランダムにIPアドレスを作成して、他のサーバーに対して感染活動すなわちアクセスを試みる。20~28日は合衆国大統領官邸ホワイトハウスのアドレスに対しDDoS攻撃 (Distributed Denial of Service attack = 分散サービス妨害攻撃) を行い、29日から月末までは何も行わない。

さらに8月4日には、その亜種である"Code Red II"が現れた。これWindows2000にのみ感染するが、感染したウェブ・サーバーのローカルドライブに、外部からアクセスできるように設定するためのハッキングツール (バックドア) "EXPLORER.EXE"をインストールするという悪質な活動を行う。感染したサーバーがランダムに生成したIPアドレスに対してアクセスを試みるため、インターネット上のトラフィックが膨大になり、またしばしばWindows NT/2000のユーザーが事態を理解できず、十分な対策を取らなかったため、各サーバーは非常に多くのアクセスを受けることになり、大きな社会的問題ともなった。

5.2 複合感染ウイルス "Nimda"

9月18日にはそれまでのウイルスの機能を統合した"Nimda"が現われ、短時間のうちに大きな被害を引き起こした。このワームは複数の感染方法を持ち、IISサーバーとWindowsクライアントの両方

に感染するために、他のウイルスに比べて非常に大きな感染力を持っていた。感染方法は以下のような4つからなっている。

- (1) メール ウイルス自身のコピー ("readme.exe") が添付されたHTMLメールをOutlook Expressのアドレス帳に登録されているアドレスに自動的に送付する。Outlook Expressでは、プレビューしただけで活動を始める。
- (2) ウェブの閲覧 ウイルスに感染したサーバーでは、ウェブ・ページに不正なJavaスクリプトが組み込まれ、そのページを閲覧すると、Internet Explorerのセキュリティホールにより、ウイルスに感染する。
- (3) IISサーバーへの侵入 IISサーバーへアクセスを試み、セキュリティホールを利用して自身のコピーを転送し実行する。また侵入のためにCode Red IIとsadmin/IISによって作られるバックドアを利用する。
- (4) 共有ファイル すべてのディレクトリに自らをコピーすることによって、ネットワーク上の共有ファイルを介して他のマシンに自身のコピーを拡散する。

これらの感染方法はすべてすでに他のウイルスによって用いられていたものである

が、"Nimda"は、それらを組み合わせて用いることによって大きな感染実害率をもたらした。ウイルスに感染したウェブ・ページからの感染は、メールによらない新たな感染方法として注目された。不正なJavaスクリプトによるウイルスとしては、2001年8月に発見されたOffensiveがすでにあつた。このウイルスに感染したウェブ・ページを、Windows 95/98/Me/NT/2000上のInternet Explorer 4/5で閲覧すると、アプリケーションの起動、システムの終了ができなくなり、強制終了後に再起動するとまったく使用できなくなる。

さらに"Nimda"では、Internet Explorerのセキュリティホールを悪用し、添付ファイルを実行しなくともOutlook Expressではプレビューしただけで自動実行するようになっていて、感染を大きくした。その仕組みは以下の通りである。OutlookおよびOutlook ExpressはHTML形式のメールを表示する際にInternet Explorerの表示機能を用いており、HTML形式からなる本文を持つメールに含まれる画像ファイルなどを表示するために、MIME (= Multipurpose Internet Mail Expression) に従ってバイナリの添付ファイルを起動するが、MIMEヘッダー情報によってはInternet Explorerが電子メールを表示する際に添付ファイルを自動的に起動してしまうという問題があつた。"Nimda"は本文をHTML形式にして、ウイルス本体は添付ファイルとなっており、このセキュリティホールを利用してウイルスを自動実行させるのである。この問題を含んでいるInternet Explorerを用いていると、Outlookではメールを開くことによって、またOutlook Expressではプレビューしただけで、自動的にメールに添付されているウイルス・ファイルを実行してしまうのである。このような自動実行型のウイルスは"Nimda"が最初ではなく、"Bubbleboy"らがすでに存在していたが、それらはあまり流布せず、一般にはウイルスは添付ファイルを開かねば大丈夫と思われていたために大流行となり、インターネット渋滞まで引き起こした。

5.3 "Badtrans.B"

このように2001年はセキュリティホールを利用したインターネットワームの年と言えるだろうが、その最後を飾ったのが、11月24日に発見され、"Nimda"を上回る史上最大の流行を引き起こした"Badtrans.B"である。このウイルスの元となった"Badtrans" (2001年4月) は、自分のコピーを添付したメールを大量に自動発送することによって増殖する。感染すると、未読メールの送信者に対し返信の形でメールを送信するが、そのメールの件名と本文は元のメールと同じものを用いる。またキーボード操作を記録するためのプログラムをインストールし、定期的にキーボード操作をチェックして、その内容を暗号化して記録し、データをいくつかのメールアドレスに送信するという「トロイ

の木馬」機能を持っている。これは、パスワードなどを取得することを目的としたものである。

"Badtrans.B"はさらに、"Nimda"と同様に、Internet Explorerのセキュリティホールを利用して、添付ファイルを実行しなくともOutlook Expressでプレビューするだけで自動実行されるようになっており、感染力を増している。またメールの宛先としてアドレスブックの他、さらに「マイドキュメント」フォルダーおよび"temporary Internet files"フォルダー内にある".HT"および".ASP"という名前のファイルをチェックし、そこから得られたアドレスを利用している。少し前に"Nimda"が流行していたにもかかわらず、多くのユーザーが、Internet Explorerの問題を解決しておらず、Outlook Expressでプレビューしてしまったために、"Badtrans.B"は"Nimda"を上回る速さで全世界に流布した。

6. 終わりに

情報処理振興事業協会セキュリティセンター (IPA/ISEC) に届けられたウイルス発見届出数を見ると、ここ数年急激に増加している。1996年までは1千件前後だったものが、1997年に2千件を超え、1999年には3千件、2000年には1万件、2001年には2万件を超えた(14)。次々と新しいウイルスが現れ、流行するウイルスも大きく変わってきた。1997年にはマクロウイルス、1999年にはメール大量発信ウイルス、そして2001年にはセキュリティホール悪用ウイルスが登場した。

昨年2001年夏以降は、"Sircam"、"Nimda"、"Badtrans.B"といった、それまでの感染記録を更新するウイルスが次々と現れている。この現象はウイルスがますます進化していることもあるが、その感染方法がほとんど電子メールによることからわかるように、インターネットの家庭への急速な普及によって電子メールが日常的なコミュニケーション手段となったことがあるだろう。

またWindows 98の登場以降、WindowsがOSとしてPCを支配し、OutlookとInternet Explorerが標準的なメーラーとウェブ・ブラウザになったことによって、大流行するウイルスのプラットフォームはほぼこの三点セットに確定している。メール大量送信ウイルスやインターネットワームは、これらのセキュリティ・ホールを悪用することによって大きな感染力を獲得している。さらにブロードバンド・サービス、定額接続サービスが普及していくにつれて、「トロイの木馬」をインストールするウイルスが多くなり、他のサーバーを攻撃する足場として利用される危険がさらに増すものと予想されている。

注

- (1) IPA/ISEC = Information-technology Promoiton Agency / Information-technology Security Center (<http://www.ipa.go.jp/security/index.html>)
- (2) 「2001年ウイルス発見届出状況」 (http://www.ipa.go.jp/security/txt/attach/2002_01-1.html) 参照.
- (3) 通商産業省告示第535号 (<http://www.meti.go.jp/policy/netsecurity/CvirusCMG.htm>)
 情報処理振興事業協会セキュリティセンターのホームページにある説明では次のようになっている (http://www.ipa.go.jp/security/y2k/virus/cdrom/basic/basic_f.html) .
 コンピュータウイルスとは、プログラムに寄生する極めて小さなプログラムであり、自分自身を勝手に他のプログラムファイルにコピーする事により増殖し、コンピュータウイルス自身にあらかじめ用意されていた内容により予期されない動作を起こす事を目的とした特異なプログラムです.
- (4) コンピュータウイルスの分類および基本的な説明は、益田岳人『コンピュータ・ウイルス』, エスシーシー, 2000; アトミックドロップ『最新コンピュータウイルスがわかる』, 技術評論社, 2000などを参照.
- (5) F. Cohen, "Computer Viruses - Theory and Experiments," in DOS/NBS 7th Conference on Computer Security, originally appearing in IFIP-Sec. 84, also appearing in IFIP-TC11 Computers and Security, 6 (1987), pp. 22-35.
 彼は、1986年にコンピュータ・ウイルスに関する博士論文"Computer Viruses"を南カリフォルニア大学に提出している,
 好ましくないコンピュータ・コードを表すものとしてvirusという言葉が用いられたのは、David GerroldのSF小説When Harley Was One, 1972においてであるが、そこでの意味は現在のコンピュータ・ウイルスのものとは異なっていた.
- (6) "Brain"に関しては、H. J. Highland, The BRAIN Virus: Fact and Fantasy, Computer & Security, 7 (1988), pp. 367-370, reprinted in Denning (1990), pp. 293-298.
- (7) 1980年代のウイルスに関しては、H. J. Highland, Computer Viruses - A Post Mortem, Computer & Security, 7 (1988), pp. 117-125, reprinted in Denning (1990), pp. 299-315. また渡辺章『コンピュータウイルス事典』, オーム社, 1993; クラフ&マンゴー『コンピュータ・ウイルスの恐怖』, 日暮雅通・久志本克己訳, 早川書房, 1994.
- (8) この事件に関しては、Denning (1990), Part III Worms, pp.191-263 の諸論文を参照.
- (9) Schoch, J. F. and Hupp, J. A., The Worm Programs -- Early Experience with a Distributed Computation, Communications of the ACM, 25 (1982), pp. 172-180, reprinted in Denning (1990), pp. 264-281.
- (10) 邦訳はジョン・ブラナー『衝撃波を乗り切れ』, 安田均訳, 集英社, 1983.
- (11) 米国のワクチンソフトメーカー"McAfee Association"の社長John McAfeeが世界中で500万台以上のパソコンが破壊されると警告したことによって大騒動となったが、実際に感染したパソコンは約1万台だった. コンピュータウイルスとワクチンソフトの歴史については、Eugene Kaspersky, "The History of Computer Viruses - From the Ancient Days to Present Time" (<http://www.avp.ch/avpve/entry/entry2.htm#1-4>)が詳しい.
- (12) コンピュータウイルスに関する様々な情報は、情報処理振興事業協会 (IPA) セキュリティセンター (<http://www.jpa.go.jp/security>) , ウイルスコンサルティングセンター (<http://www.vcon.dekyo.or.jp>) などのウェブページから得られる. また個々のウイルスに関しては、ウイルス対策ソフトを販売している各社のウェブページに詳しい情報がある. トレンドマイクロ (<http://www.trendmicro.co.jp>) , シマンテック (<http://www.symantec.com/region/jp/>) ,

ネットワークアソシエイツ (<http://www.nai.com/japan/>) などを参照.

近年のウイルスの流布状況については、情報処理振興事業協会 (IPA) セキュリティセンターが公表している「ウイルスの被害届出状況について」 (<http://www.ipa.go.jp/security/txt/list.html>) を参照. またそれに基づいて作成された、橋本晋之介「月刊分析レポート Part2 コンピュータウイルスの被害」, Cyber Security Management連載, およびウイルスコンサルティングセンターのウェブ・ページにある「発生ウイルスストップ10」 (<http://www.vcon.dekyo.or.jp/damage/ranklist/index.html>) などから情報が得られる.

以下の本文の記述は以上のウェブページおよび文献の情報に基づいている.

- (13) WWWを中心としたインターネットの歴史に関しては、Moschovitis, Ch. et al., Hisoty of the Internet : A Chronology, 1843 to the Present, Santa Barbara, Cal., 1999 およびリード『インターネット激動の1000日』, 山岡洋一訳, 日経B P社, 1997.
- (14) 「2001年ウイルス発見届出状況」 (http://www.ipa.go.jp/security/txt/attach/2002_01-1.html) 参照.