ウイルスって何？

ウイルスは、人が病気になるときの病原体のひとつですが、コンピュータの世界のウイルスとはどのようなものなのでしょうか。

ここでは、情報セキュリティの対策を立てる上で避けては通れないコンピュータウイルスについて、その動作、過去に発生したウイルスの解説、その対策について説明します。

Copyright 2003 - 2009 総務省

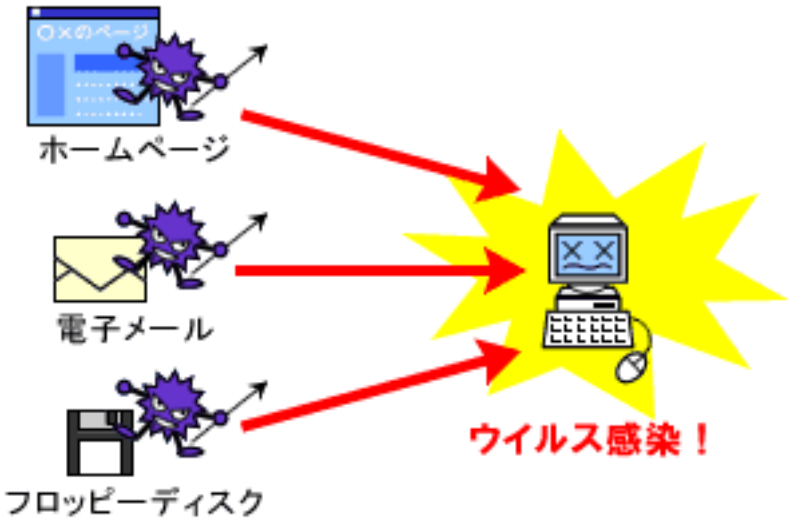
コンピュータウイルスとは

コンピュータウイルスは、電子メールやホームページ閲覧などによってコンピュータに侵入する特殊なプログラムです。数年前まではフロッピーディスクを介して感染するタイプのウイルスがほとんどでしたが、最近はインターネットの普及に伴い、電子メールをプレビューしただけで感染するものや、ホームページを閲覧しただけで感染するものが増えてきています。また、利用者の増加や常時接続回線が普及してきたことで、ウイルスの増殖する速度が速くなってきています。

ウイルスの中には、何らかのメッセージや画像を表示するだけのものもありますが、危険度が高いものの中には、ハードディスクに格納されているファイルを消去したり、コンピュータが起動できないようにしたり、パスワードなどのデータを外部に自動的に送信したりするタイプのウイルスもあります。

そして、何よりも大きな特徴としては、「ウイルス」という名前からも分かるように、多くのコンピュータウイルスは増殖するための仕組みを持っています。たとえば、コンピュータ内のファイルに自動的に感染したり、ネットワークに接続している他のコンピュータのファイルに自動的に感染したりするなどの方法で自己増殖します。最近はコンピュータに登録されている電子メールのアドレス帳や過去の電子メールの送受信の履歴を利用して、自動的にウイルス付きの電子メールを送信するものも多く、世界中にウイルスが蔓延する大きな原因となっています。

ウイルスに感染しないようにするためには、ウイルス対策ソフトを導入する必要があります。また、常に最新のウイルスに対応できるように、インターネットなどでウイルス検知用データを更新しておかなければなりません。



Copyright 2003 - 2009 総務省

＜＜参考＞＞

1990 年 4 月 10 日に通商産業省が制定した「コンピュータウイルス対策基準」では、コンピュータウイルスを次のように定義しています。

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、条件が満たされるまで症状を出さない機能

（3）発病機能
プログラムやデータ等のファイルの破壊を行ったり、コンピュータに異常な動作をさせる等の機能

※ 2001 年 1 月 6 日より通商産業省は経済産業省に移行しました。

Copyright 2003 - 2009 総務省

ウイルスの変遷

ウイルスの感染経路や活動内容は、その目的とともに変化し続けています。1990 年代前半、コンピュータの多くはスタンドアロンで利用されており、フロッピーディスクなどの外部記憶媒体から感染するシステム領域感染型ウイルスやファイル感染型ウイルスが横行しました。

1990 年代後半から 2000 年代初めにかけては、コンピュータの利用形態がスタンドアロンからインターネットへ移行していく過程であり、Melissa（メリッサ）やLOVELETTER（ラブレター）などの電子メールの添付ファイルで感染するウイルスが増えてきました。さらには、CodeRed（コードレッド）、MSBlaster（エムエスブラスター）などのセキュリティホールを狙う大規模感染型のウイルスも現れました。これらのウイルスは、攻撃者の興味本位や自己技術の誇示、愉快犯的な発想により作成されたものと考えられています。

これに対して、2002 年ごろから、Agobot（アゴボット）をはじめとするボットが台頭してきました。ボットはそれまでの愉快犯的な発想によるウイルスとは異なり、金銭的な利益の追求という明確な目的をもって作られています。

ボットは、ボットネットワークという巨大なネットワークを構成し、ボットネットワークをコントロールする犯罪組織によって、DoS 攻撃やDDoS 攻撃、迷惑メール配信、情報漏洩などに利用されています。

最近の傾向としては、旧来の愉快犯的な発想によるウイルスと比べると、感染したことや活動していることに気付かれないように密かに動作するようになり、ウイルスの脅威が見えにくくなっているのが特徴と言えます。

	1980年代後半	1990年代後半 ～2000年代初め	最近の傾向
感染経路	FD、CD-ROM等の 外部記憶媒体を経由	ネットワーク経由 (メール、ダウンロード、ワーム型)	ネットワーク経由 Web感染、メール感染
脅威の対象	パソコン、ミニコン	パソコン、サーバー 特定の個人・組織の情報	パソコン、携帯電話、 PDA、情報家電 特定の個人・組織の情報
活動形態	パソコン等の不具合	パソコンの不具合、情報漏えい ネットワークの脅威 (DDoS攻撃、スパムメール)	ネットワークを用いた脅威 情報漏えい 詐欺行為(フィッシング詐欺等)
目的	能力の誇示	能力の誇示、経済目的	経済目的 犯罪、スパイ行為

Copyright 2003 - 2009 総務省

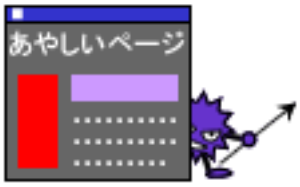
基本的なウイルスの動作

コンピュータウイルスは、フロッピーディスクや電子メール、ホームページの閲覧など、そのウイルスのタイプによってさまざまな方法で感染します。また、ウイルスに感染すると、コンピュータシステムを破壊したり、他のコンピュータに感染したり、そのままコンピュータに残ってバックドアと呼ばれる不正な侵入口を用意したりするなど、さまざまな活動を行います。

ここでは、主なウイルスを感染経路と活動方法によって分類してみましょう。

■ウイルスの感染経路

●ホームページの閲覧



現在のWebブラウザは、ホームページ上でさまざまな処理を実現できるように、JavaScriptやVBScript、ActiveXコントロール、Javaなどのプログラムを実行できるようになっています。そのため、これらのプログラムでウイルスが埋め込まれたホームページを閲覧した場合は、コンピュータがウイルスに感染してしまいます。

最近では、Webブラウザや Webブラウザへのプラグインソフトの脆弱性を利用した感染方法が増加してきており、ホームページを閲覧するだけでウイルスに感染させる手口はますます巧妙化してきています。

かつては怪しいWebサイトを訪問しなければ大丈夫と思われていましたが、近年ではSQLインジェクションという手口が横行し、正規のWebサイトがウイルス付きの内容に書き換えられてしまうケースが急増しています。この場合には、正規のWebサイトを訪問した場合であっても、ウイルスに感染してしまうことになります。

●電子メールの添付ファイル

ウイルスの感染経路として一般的なのは、電子メールの添付ファイルです。電子メールの添付ファイルとして送信されたウイルスを誤って実行すると、そのウイルスに感染してしまいます。

●USBメモリからの感染

多くのコンピュータでは、USBメモリをコンピュータに差し込んだだけで自動的にプログラムが実行される仕組みが用意されています。この仕組みを悪用して、コンピュータに感染するウイルスがあります。このようなウイルスの中には、感染したコンピュータに後から差し込まれた別のUSBメモリに感染するなどの方法で、被害が拡大されていくこともあります。

Copyright 2003 - 2009 総務省

●ファイル共有ソフトによる感染

ファイル共有ソフトとは、インターネットを利用してファイルをやり取りするソフトウェアのことです。ファイル共有ソフトでは不特定多数のユーザーが自由にファイルを公開することができるため、別のファイルに偽装するなどの方法でいつの間にかウイルスを実行させられてしまうことがあります。

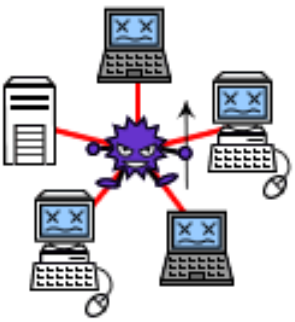
●偽のウイルス対策ソフト

あたかも無料のウイルス対策ソフトのように見せかけて、ウイルスがインストールされてしまう被害が増えています。その代表的な手口は、ホームページなどで「あなたのコンピュータはウイルスに感染しています」のようなメッセージを表示し、偽のウイルス対策ソフトのダウンロード用 Web サイトに誘導する方法です。

●電子メールの HTML スクリプト

添付ファイルが付いていない電子メールであっても、HTML メールであればウイルスを送信することができます。HTML メールはホームページと同様に、メッセージの中にスクリプトと呼ばれるプログラムを挿入することが可能なため、スクリプトの形でウイルスを侵入させておくことができるのです。電子メールソフトによっては、HTML メールのスクリプトを自動的に実行する設定になっているものがあり、その場合には電子メールをプレビューしただけでウイルスに感染してしまいます。

●ネットワークのファイル共有



ウイルスによっては、感染したコンピュータに接続されているファイル共有用のネットワークドライブを探し出して、特定の拡張子を持つなど、ある条件で探し出したファイルに感染していくタイプのものがあります。このようなウイルスは社内のネットワークを通じて、他のコンピュータやサーバーにも侵入する可能性があります。とても危険度が高く、完全に駆除することが難しいのが特徴です。

Copyright 2003 - 2009 総務省

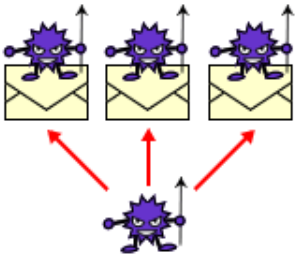
●マクロプログラムの実行

マイクロソフト社のOfficeアプリケーション（Word、Excel、PowerPoint、Access）のマクロ機能を利用して感染するタイプのウイルスがあります。これらは、マクロウイルスと呼ばれています。Officeアプリケーションのマクロ機能では、高度なプログラム開発言語であるVBA（Visual Basic for Applications）を使用することができるため、ファイルの書き換えや削除など、コンピュータを自在に操ることが可能になります。そのため、マクロウイルスに感染したドキュメントは、ファイルを開いただけでVBAで記述されたウイルスが実行されて、自己増殖などの活動が開始されます。

Copyright 2003 - 2009 総務省

■ウイルスの活動内容

●自己増殖



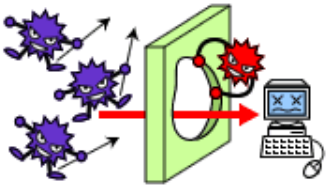
ウイルスのほとんどは、インターネットやＬＡＮを使用して、他の多くのコンピュータに感染することを目的としています。特にワーム型と呼ばれるウイルスは、自分自身の複製を電子メールの添付ファイルにして送信したり、ネットワークドライブに保存されているファイルに感染したりするなど、ユーザーの操作を介さずに自動的に増殖していきます。

●情報漏洩

ウイルスによる情報漏洩は、大きく分類すると、インターネットの特定のＷｅｂサイトやメールアドレスにデータを送信するケースと、インターネット上に情報を公開するケースがあります。ウイルスによって漏洩する情報は、ユーザーアカウントやパスワード、コンピュータ内のファイル、メール、デスクトップの画像などさまざまです。そして、情報漏洩を目的としたウイルスでは、感染していることに気づかせないようにするため、コンピュータの画面上には何も変化が起こらないことが一般的です。

なお、ファイル共有ソフトを介して感染するタイプのウイルスによって情報が漏洩した場合には、その情報をネットワークから完全に消去することは非常に困難です。

●バックドアの作成



感染したコンピュータの内部に潜伏するタイプのウイルスをトロイの木馬と呼びます。この中でもバックドアを作成するタイプのウイルスは極めて悪質なもので、インターネットを通じて、感染したコンピュータを外部から自由に操作されてしまうこともあります。

●コンピュータシステムの破壊

ウイルスによっては、コンピュータシステムを破壊してしまうものがあります。その動作はウイルスによって異なりますが、特定の拡張子を持つファイルを探し出して自動的に削除するものから、コンピュータの動作を停止してしまうものまでさまざまです。

Copyright 2003 - 2009 総務省

●メッセージや画像の表示

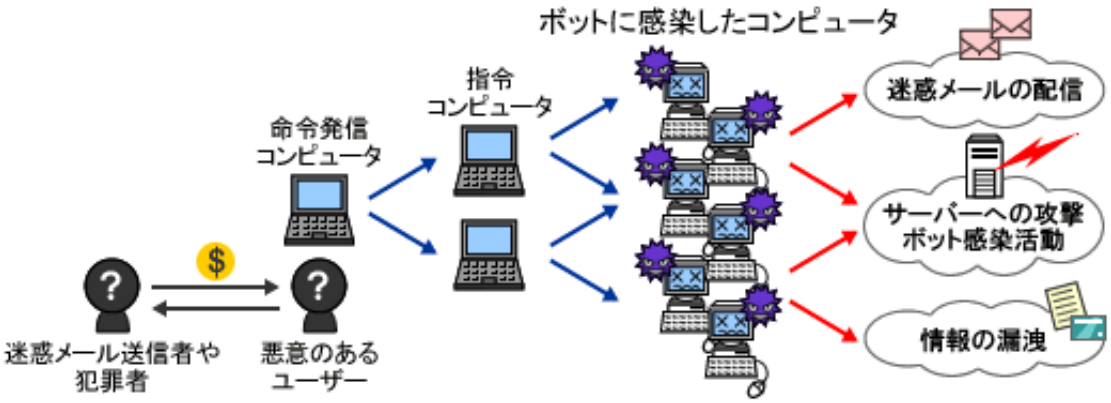
いたずらを目的としたウイルスは、一定期間潜伏して、ある日時に特定のメッセージや画像を表示することがあります。ただし、最近はこのようないたずらを目的としたウイルスは減ってきてます。

Copyright 2003 - 2009 総務省

ボットとは？

ボット（BOT）とは、コンピュータを外部から遠隔操作するためのコンピュータウイルスです。ボットに感染したコンピュータは、ボットネットワークの一部として動作するようになります。そして、インターネットを通じて、悪意のあるハッカーが、常駐しているボットにより感染したコンピュータを遠隔操作します。外部から自由に操るという動作から、このような常駐型の遠隔操作ソフトウェアのことをロボット（Robot）をもじってボット（BOT）と呼んでいます。

ボットに感染させたハッカーは、その感染したコンピュータを遠隔操作することで、インターネットに対して、「迷惑メールの配信」、「インターネット上のサーバーへの攻撃」、「感染活動」などの迷惑行為や犯罪行為を行ないます。また、感染したコンピュータに含まれる情報やコンピュータを操作した情報を盗み出す「スパイ活動」も行なうことがあります。ボットは旧来のウイルスのように愉快犯的な行為で作られたものではなく、迷惑メールの送信者や個人情報を不正に利用しようとする犯罪者と取引するために作られているという点が手口の巧妙化の要因のひとつとなっています。このような目的から、旧来のウイルスと比べると、感染しているということに気付きにくくしているというのも特徴のひとつです。



ボットに感染したコンピュータとそのコンピュータの持ち主はもちろん被害者なのですが、感染したコンピュータが迷惑メールを送信したり、別のサイトを攻撃したりするため、迷惑メールを受け取ったり、攻撃されたりしたコンピュータから見ると、ボットに操られたコンピュータは加害者になってしまいます。あなた自身が加害者にならないようにするためにも、ボットへの対策はとても大切なことです。

ボットへの対策として、日常的に適切な情報セキュリティ対策を心がける必要があります。まず、ボットはウイルスとして侵入してくることが多いため、基本的にはウイルス対策がもっとも重要と言えます。しかし、最近ではさまざまな手口の侵入方法が考えられているため、以下のような対策を心がけるようにしてください。

- ウイルス対策ソフトの導入とウイルス検知用データの更新
- セキュリティホールを塞ぐためのＯＳ やソフトウェアのパッチの適用
- パーソナルファイアウォール・ブロードバンドルーターの導入

Copyright 2003 - 2009 総務省

ウイルスを駆除するためには

ウイルスを駆除するためには、コンピュータにウイルス対策ソフトを導入する必要があります。ウイルス対策ソフトは、ワクチンソフト、アンチウイルスソフトと呼ばれることもあります。一般的に、ウイルス対策ソフトはコンピュータの電源がオンであるときには常に起動した状態になり、外部から受け取るデータを常時監視することで、インターネットやLAN、フロッピーディスクなどからコンピュータがウイルスに感染することを防ぎます。また、逆に電子メールなどで外部に送信するデータにウイルスが含まれていないこともチェックしてくれます。コンピュータがウイルスに感染してしまった場合には、コンピュータからウイルスを除去する機能も持っています。

ただし、ウイルス対策ソフトは、今までのウイルスに対応するウイルス検知用データからウイルスを見つけ出す仕組みになっているため、新しいウイルスは検知できないことがあります。そのため、ウイルス検知用データはいつでも最新のものに更新しておかなければなりません。最新のウイルス検知用データはインターネットやCD-ROMなどで配布されているので、ウイルス対策ソフトのマニュアルやヘルプ、メーカーのホームページなどで確認してみましょう。

また、ウイルス対策ソフトを導入する以外にも、プロバイダが自社の接続サービスの利用者向けに提供しているウイルス対策サービスを利用する方法もあります。ウイルス対策サービスの提供の有無や提供内容などについては、プロバイダのホームページで確認するか、加入しているプロバイダに問い合わせてください。なお、プロバイダのウイルス対策サービスを利用する場合には、プロバイダがウイルス検知用データを自動的に更新するため、ユーザーによる更新作業は不要になります。

Copyright 2003 - 2009 総務省

注意

最近、無料のウイルス対策ソフトのように見せかけて、ウイルスをインストールさせる手口による被害が増えているため、注意してください。その代表的な手口は、ホームページなどで「あなたのコンピュータはウイルスに感染しています」のようなメッセージを表示し、偽のウイルス対策ソフトのダウンロード用Web サイトに誘導して、ウイルスをインストールさせる方法です。

ホームページを見ているだけでウイルス対策ソフトのインストールを促された場合には、不用意にリンク先のホームページに接続したり、ソフトウェアをダウンロード / インストールしたりしないようにしてください。

Copyright 2003 - 2009 総務省