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。

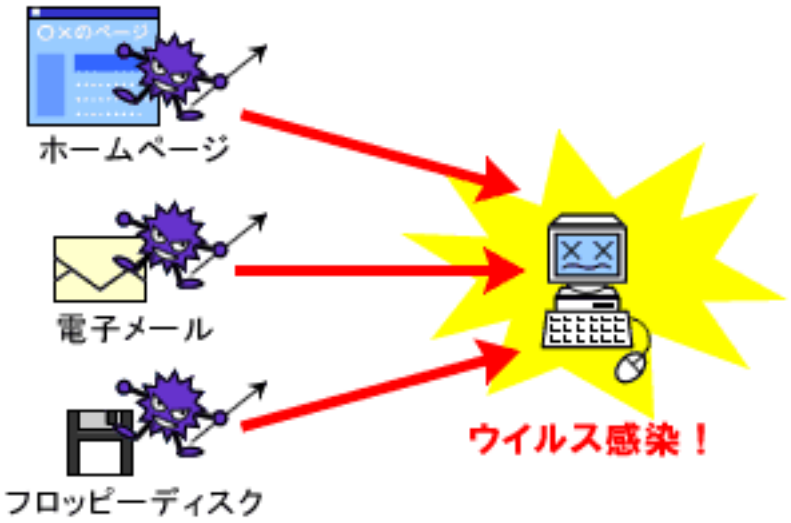
コンピュータウイルスとは

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。



＜＜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。

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

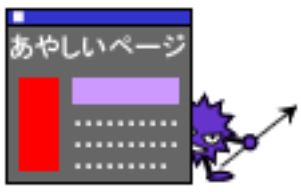
●電子メールの添付ファイル

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。

●電子メールの HTML スクリプト

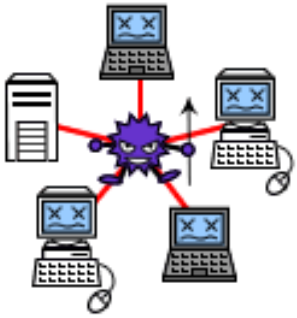
添付ファイルが付いていない電子メールであっても、HTML メールであればウイルスを送信することができます。HTML メールはホームページと同様に、メッセージの中にスクリプトと呼ばれるプログラムを挿入することが可能なため、スクリプトの形でウイルスを侵入させておくことができるのです。電子メールソフトによっては、HTML メールのスクリプトを自動的に実行する設定になっているものがあり、その場合には電子メールをプレビューしただけでウイルスに感染してしまいます。

●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。

●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。

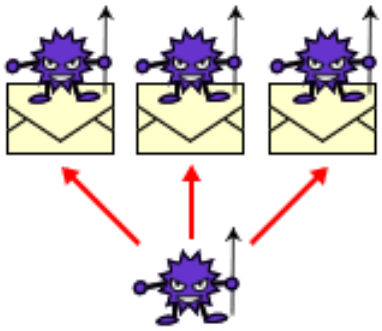
●マクロプログラムの実行

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。

■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。



●コンピュータシステムの破壊

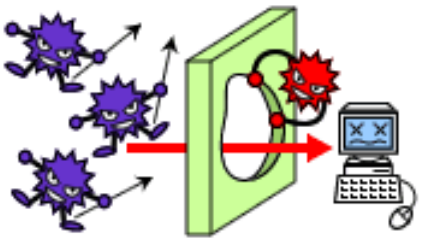
ウイルスによっては、コンピュータシステムを破壊してしまうものがあります。その動作はウイルスによって異なりますが、特定の拡張子を持つファイルを探し出して自動的に削除するものから、コンピュータの動作を停止してしまうものまでさまざまです。

●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。

●トロイの木馬

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。



代表的なウイルスの動作と被害内容

コンピュータウイルスには、数多くの種類があります。
ここでは、今までに大きな被害のあった代表的なコンピュータウイルスについて説明します。

■Nimda（ニムダ）

Nimda（ニムダ）は、その感染方法が多彩であったことにより、世界中で大流行したワーム型のウイルスです。ウイルス単体でも、トロイの木馬として活動します。

このウイルスは、感染すると、電子メール送信、ネットワークドライブへのファイルコピー、IIS を使用した Web サーバーへの侵入など、ネットワークを利用したさまざまな方法で増殖するため、広まるのがとても速いのが特徴です。また、電子メールの添付ファイルとして配布されることにより、Outlook Express や Outlook を利用者が適切な対策を施さずに利用している場合には、電子メールをプレビューしただけで、添付ファイルの“readme.exe”が実行されてしまい、ウイルスに感染してしまいます。なお、送信メールの宛先には、電子メールソフトの送信済みアイテムと受信トレイに保存されている電子メールから適当に選ばれたメールアドレスが使用されます。このウイルスによって電子メールが送信されても、送信の履歴は残されません。

さらに、システムの破壊活動も行うこともあります。コンピュータの設定を変更して、ファイルの拡張子を見えなくしたり、隠しファイル属性のファイルを表示しないようにして、感染状態を一目ではわかりづらくしてしまいます。また、Windows 9x/Me の場合には、設定ファイルを変更して、システムが起動するたびにウイルスも自動起動されるようにしてしまいます。

■Klez（クレズ）

Klez（クレズ）は、世界中で大流行したNimda（ニムダ）に類似した活動を行うワーム型のウイルスです。電子メールの自動送信とネットワークドライブへのファイルコピーで増殖し、プログラムファイルへの感染を行う別のプログラムも作成します。

自己増殖のための電子メールの自動送信時には、感染した端末の過去の受信電子メールの中から任意に選ばれた送信元のメールアドレスが、電子メールの送信者として使用されることがあるため、電子メールの送信者のコンピュータが必ずしも感染しているとは限りません。そのため、電子メールの送信元をウイルスの感染元として特定するという方法では感染元が判明しないため、ウイルスの駆除に時間がかかるということも大きな特徴です。

添付ファイルが実行されると、メモリに常駐して活動を開始するだけでなく、感染時にいくつかのファイルを作成することで、システム起動時にワームが自動実行されるように設定します。

■ Bugbear（バグベア）

Bugbear（バグベア）は、トロイの木馬型のワームです。Outlook Express のアドレス帳などからメールアドレスを取得して、170 件のアドレスに対して自身のコピーを添付した電子メールを送信します。このとき、送信者のメールアドレスも詐称します。さらに、ネットワークドライブなどを経由したネットワーク感染や、ハッキングツールとしてバックドアの作成や情報漏洩なども行います。

ハッキングツールとしての動作は、感染したコンピュータの特定のポートをオープンして、外部からの接続を待ち受けるというものです。このポートを利用して、外部からファイルの実行やプロセスの終了といったリモートコントロールを行ったり、そのコンピュータに関する情報を取得できるようになってしまいます。

さらに、収集したパスワードをコンピュータ名、ユーザー名とともに特定のメールアドレスに電子メールとして送信します。

また、このウイルスの特徴として、ウイルス対策ソフトやファイアウォールソフトなど、情報セキュリティ管理ソフトの正常な動作を妨害するということがあげられます。

■Badtrans（バッドトランス）

Badtrans（バッドトランス）は、トロイの木馬型のワームです。自身のコピーを電子メールに添付して送信することで、ネットワーク上で自己増殖するワーム活動を行います。また、感染したコンピュータ上のキー入力を記録して外部に送信するといったハッキングツールとしての活動も行います。

このワームは、Outlook Express や Outlook を利用者が適切な対策を施さずに使用している場合に、受信した電子メールをプレビューしただけでウイルスの活動を開始します。

特に感染の被害が大きかった Badtrans.B と呼ばれる亜種は、ウイルスのプログラムが直接電子メールを送信する機能を持っているため、電子メールソフトには依存せずに動作します。さらに、電子メールソフトの送信履歴にも残されません。送信者のメールアドレスは、受信トレイに保存されている電子メールから送信者のメールアドレスや特定のフォルダに格納されているファイルから取得できたメールアドレスが利用されます。

Badtrans（バッドトランス）に含まれているハッキングツールのプログラムである“kdll.dll”はメモリに常駐して、感染したコンピュータのすべてのキー入力をユーザー名や入力時刻などとともに記録して、電子メールで任意のメールアドレスに送信します。

■ CodeRed（コードレッド）

CodeRed（コードレッド）は、トロイの木馬型のワームです。このウイルスの大きな特徴は、セキュリティホールが存在するWebサーバーを狙ったウイルスであるという点です。情報セキュリティ対策がなされていないIISがこのウイルスからのHTTPリクエストを受信すると、ワームのプログラムコードがサーバーのメモリ上で実行されます。

このとき、感染したWebサーバーでは、ワームのプログラムがメモリ上で直接実行されますが、ディスクにはウイルスのファイルは作成されません。つまり、このウイルスはサーバー上に実体としてのワームのファイルが存在しないまま、メモリ上で活動してインターネットの中で繁殖し続けるというわけです。ただし、メモリ上のみで動作するプログラムであるために、コンピュータを再起動すればメモリ上のプログラムが消去されてしまいます。

このウイルスに感染したサーバーは、外部からのWebページの要求に対して、常に以下の内容のデータだけを送信するようになります。

```
Welcome to http://www.worm.com !
Hacked By Chinese!
```

感染してから10時間が経過すると、ワーム自身が改変したプログラムの機能を元に戻し、本来のWebページのコンテンツが表示されるようになります。

■Sircam（サーカム）

Sircam（サーカム）は、トロイの木馬型のワームです。ウイルス自身のコピーを電子メールに添付して送信します。このウイルスはウイルスプログラム自身で電子メール送信を行うため、ユーザーの電子メールソフトに送信履歴は残されません。このとき、送信メールの送信者のメールアドレスは、基本的に感染者とは異なるメールアドレスが使用されます。Nimda（ニムダ）と大きく異なる点は、電子メールの宛先として、コンピュータ内のアドレス帳やHTML ファイルなどからメールアドレスを探し出すところで、これがこのウイルスの大きな特徴となっています。

さらに、侵入したコンピュータにネットワークドライブが設定されている場合には、感染している状態を偽装するため、ウイルス（“SIRC32.EXE”）を隠しファイル属性でコピーします。また、ネットワークドライブに“Autoexec.bat”が存在する場合には、そのコンピュータの起動ディスクであると解釈して、このファイルを書き換えることで、そのコンピュータの起動時にこのウイルスが自動的に実行されるように設定します。

■ LOVELETTER（ラブレター）

LOVELETTER（ラブレター）は、VBScript で記述されたワームで、Windows Script Host がインストールされた Windows で動作します。Outlook と IRC クライアントプログラムの mIRC を利用して、自身を添付した電子メールやメッセージを自動的に送信します。

特徴としては、mIRC がコンピュータにインストールされている場合には、同じチャンネルに参加しているユーザーに対して、“LOVE-LETTER-FOR-YOU.HTM”というファイル名のワームプログラムのコピーを自動的に送信する点があげられます。

また、システム破壊行為として、特定の拡張子を持つファイルを探し出して、自分自身のコピーでファイルを書き換えることがあります。

■Happytime（ハッピータイム）

Happytime（ハッピータイム）は、トロイの木馬のワームです。HTML 形式の電子メールを送信して、Outlook や Outlook Express でプレビューした場合に、ネットワーク上で自己増殖するワーム活動を行います。VBScript で記述されたプログラムであるため、マイクロソフト社の IE（Internet Explorer）5.0 以降、もしくは Windows Script Host がインストールされている環境で動作します。

ワームのプログラムが実行されると Windows のシステムディレクトリ（通常は C：\Windows\System）に“HELP.HTM”というファイル名で自身のコピーを作成し、同時にこのファイルをデスクトップの壁紙に設定します。そのため、デスクトップが Acitve Desktop を使用するように設定されている場合には、Windows の起動時など、壁紙が表示されるタイミングでウイルスのスクリプトが実行されることになります。

このウイルスが実行されると、感染活動として、特定の拡張子のファイルを自身のコードで書き換えるか、末尾に自身のコードを追加します。

なお、このウイルスの特徴として、ウイルスの起動回数を記録している点があげられます。この起動回数が 366 で割り切れる数だった場合に、コンピュータの時刻の秒数によって異なる宛先に、ワームを添付した電子メールを送信します。秒数が奇数のときにはアドレス帳の宛先全員に、偶数のときには Outlook の受信トレイのすべての電子メールに対して、返信として電子メールを送信します。

さらに、システム破壊活動として、システム日付の月と日の数字の合計が 13 になる日付（例：1 月 12 日、8 月 5 日など）の場合に、コンピュータのすべてのドライブに保存されている拡張子 DLL と拡張子 EXE のファイルを削除します。

■ MTX（マトリックス）

MTX（マトリックス）は、バックドア型のハッキングツールを持つワームです。感染すると、バックドア型ハッキングツールと電子メールを使用して自分のコピーを配布するワーム型プログラムとの 2 種類をコンピュータにインストールします。自分自身とは別のプログラムをインストールすることから、このタイプのウイルスは「ウイルスドロッパー」とも呼ばれています。MTX（マトリックス）は、ウイルスが作成するプログラムとウイルス自身が連携して動作するため、活動内容が非常に複雑で駆除が困難です。

ハッキングツールはシステムに常駐して、決められたホームページからプログラムをダウンロードしようとしますが、実際にはこの動作は成功しません。

■Melissa（メリッサ）

Melissa（メリッサ）は、マイクロソフト社のワープロソフトである Word97/98/2000 で動作するマクロウイルスです。Word 文書に“Melissa”という名前のマクロモジュールを作成して感染します。

このウイルスは、Outlook を利用して、アドレス帳に登録されているユーザーから 50 名を選択して、感染した文書ファイルを添付した電子メールを送信するという活動を行います。電子メールを内部的に起動して、大量の宛先にウイルス付きの電子メール送信を行うという大流行したワーム活動の原点となったウイルスです。

感染した文書ファイルを開くと、Word の標準テンプレートファイルである“NORMAL.DOT”に感染するため、次回からは Word を起動するたびにウイルスが動作するようになります。

なお、このウイルスでは感染したという動作を隠すために、［ツール］メニューの［マクロ］コマンドを使用不可にして、さらに以下の Word のオプション設定を無効にします。

- 標準設定を変更するかどうかを確認する
- 文書を開くときにファイル形式を確認する
- マクロウイルスの自動検出

このウイルスならではの動作として、感染した文書ファイルを開くときに、コンピュータの日付と時刻をチェックして、日付（日）と時刻（分）が同じ場合に、文書中の現在のカーソル位置に特定の文字列を挿入するという点もあげられます。

■ Laroux（ラルー）

Laroux（ラルー）は、マイクロソフト社の表計算ソフトである Excel で動作するマクロウイルスです。このウイルスに感染すると、他の Excel ファイルを開いたときに、そのファイルに自分自身をコピーして感染させます。このウイルス自体は感染するだけで、それ以上の破壊活動は行いませんが、その後に作り出されたさまざまな Excel 用のマクロウイルスの原種となりました。

感染したファイルを開くと、Excel のスタートアップフォルダ（通常は XLSTART フォルダ）に、ウイルスを含んだ“Personal.xls”という名前の Excel ファイルを作成します。このスタートアップフォルダに格納されているファイルは、Excel が起動したときに自動的に読み込まれるため、次回からは Excel を起動するたびにウイルスが動作するようになります。

■ MSBlaster（エムエスブラスター）

MSBlaster（エムエスブラスター）は、トロイの木馬型のワームです。Windows のセキュリティホールを利用して、ネットワーク上のコンピュータに“ MSBLAST.EXE ”というファイルを埋め込んで自動実行することで増殖します。感染したコンピュータは設定ファイルも同時に変更されてしまうため、システムを起動するたびに、埋め込まれた“ MSBLAST.EXE ”が実行されるようになり、別のコンピュータを攻撃するようになります。

さらに、決められた日時（2003年8月16日午前0時）に、マイクロソフト社のwindowsupdate.comに対する DoS 攻撃（サービス拒否攻撃）を実行します。

このワームには、以下のメッセージが埋め込まれており、このメッセージの内容から別名ラブサンと呼ばれています。

I just want to say LOVE YOU SAN!! billy gates why do you make this possible ?
Stop making money and fix your software!!

■ SQLSlammer（エスキューエルスラマー）

SQLSlammer（エスキューエルスラマー）は、マイクロソフト社のサーバー向けデータベースソフトである SQL Server 2000 の脆弱性を利用して、コンピュータのメモリ内に侵入するワームです。このワームに感染すると、ネットワーク上のコンピュータの UDP ポート 1434 番を攻撃して増殖を試みます。

このワームはメモリに常駐するだけで、ファイルとしては存在しません。また、INI ファイルやレジストリなどの設定ファイルも改変しないため、コンピュータを再起動したときには、メモリがクリアされて、ワームが駆除されます。ただし、SQL Server 2000 の脆弱性が残されたまま使用しているコンピュータには、再度侵入される可能性があります。

SQLSlammer（エスキューエルスラマー）は、感染活動を繰り返すだけで特別な破壊活動は行いませんが、UDP ポート 1434 番のトラフィックの急激な増大をもたらします。そのため、ネットワーク内のシステム全体のパフォーマンスに悪影響を受けることがあります。

実際に、韓国ではこのワームの影響で、2 日間に渡り、DNS サーバーがダウンしてしまいました。

■ Mydoom（マイドゥーム）

Mydoom（マイドゥーム）は、電子メールの添付ファイルを通じて感染するワーム型のウイルスです。このウイルスは、送信エラーなどに見せかけた電子メールを送信することがあるというのも特徴のひとつです。

このウイルスに感染したコンピュータは、そのコンピュータのアドレス帳やファイルから収集したメールアドレスの他に、特定のファイルの情報を元に作成したすべてのメールアドレスに対して、ウイルス自身のコピーを添付した電子メールを送信します。このとき、送信者のメールアドレスも詐称します。また、設定ファイルを変更することによって、システムを起動するたびにウイルスも自動起動されるように設定してしまいます。さらに、sco.com という Web サイトに対する DoS 攻撃（サービス拒否攻撃）やハッキングツールとしてのバックドアの作成なども行います。

生成するハッキングツールの動作は、感染したコンピュータの特定のポートをオープンして、外部からの接続を待ち受けるというものです。このハッキングツールによって、外部の不正ユーザーがファイルの実行やプロセスの終了などのリモートコントロールを行ったり、そのコンピュータに保存されている情報をダウンロードしたりすることを可能にされてしまいます。

なお、このウイルスによって攻撃された sco.com では、Web サイトの運用ができなくなったため、Web サイトを一時移転するといった被害も発生しました。

さらに、Mydoom（マイドゥーム）に感染しているコンピュータだけに感染する Doomjuice（ドゥームジュース）というウイルスも発見されています。Doomjuice（ドゥームジュース）は、ネットワークを通じて感染して、Microsoft.com への DoS 攻撃（サービス拒否攻撃）を行います。

■ Netsky（ネットスカイ）

Netsky（ネットスカイ）は、トロイの木馬型のワームで、非常に多くの亜種を持つウイルスです。電子メールまたはネットワークの P2P ファイル共有ソフトを経由して感染を広げますが、亜種の中には、Nimda のようにネットワークドライブへのファイルコピーによって増殖するものもあります。

電子メールの送信時には、電子メールの宛先として、コンピュータ内のアドレス帳や HTML ファイルなどからメールアドレスを探し出します。送信者のメールアドレスも同様にして詐称します。

電子メールの添付ファイルが実行されたときには、ワームのプログラム自身を services.exe という名前でシステムのフォルダにコピーして、コンピュータ内の設定ファイルを変更します。このとき、偽のエラーメッセージを表示して、ユーザーにウイルスに感染したことに気付かせないようにする機能も持っています。

このウイルスに感染すると、設定ファイルが変更されることによって、システムが起動するたびにウイルスも自動起動するように設定されてしまいます。

■ Bagle（バグル）

Bagle（バグル）は、システムに常駐するトロイの木馬型ワームで、自身の複製を電子メールの添付ファイルとして送信することで広まります。電子メールの送信時には、電子メールの宛先として、コンピュータ内のアドレス帳やHTMLファイルなどからメールアドレスを探し出します。送信者のメールアドレスも同様にして詐称します。

電子メールの添付ファイルが実行されたときには、ワームのプログラム自身をbbeagle.exeという名前でシステムのフォルダにコピーして、コンピュータ内の設定ファイルを変更します。このとき、Windowsに装備されている電卓のアプリケーションを起動して、ユーザーに感染したことを気付かせないようにしています。

このウイルスに感染すると、設定ファイルが変更されることによって、システムが起動するたびにウイルスも自動起動するように設定されます。また、ハッキングツールとしてのバックドアの作成なども行います。

ハッキングツールとしての動作は、感染したコンピュータのTCPのポート6777をオープンして、外部からの接続を待ち受けるというものです。このことにより、外部の不正ユーザーがコンピュータ上でコマンドを実行することができるようにされてしまいます。

■ Sobig（ソービッグ）

Sobig（ソービッグ）は、電子メールの添付ファイルを通じて感染するトロイの木馬型のワームです。

2003 年 5 月に発見された亜種では、電子メールの送信者アドレスを「support@microsoft.com」とすることによって、マイクロソフト社のサポート部門からの電子メールであるかのように偽っていました。

このウイルスに感染すると、コンピュータのアドレス帳やファイルから収集したメールアドレスに、自身のコピーを添付した電子メールを送信します。亜種の中には、送信者のメールアドレスを詐称するものもあります。また、コンピュータ内の設定ファイルを変更することによって、システムを起動するたびにウイルスも自動起動するように設定されてしまいます。

■Mimail（ミメイル）

Mimail（ミメイル）は、電子メールの添付ファイルを通じて感染するトロイの木馬型のワームです。このウイルスは、コンピュータ内の設定ファイルを変更することによって、システムが起動するたびにウイルスが自動起動されるようにします。

また、このワームは、Outlook Express や Outlook を適切な対策を施さずに使用している場合に、受信した電子メールをプレビューしただけでウイルスの活動が開始されます。

Mimail（ミメイル）の大きな特徴のひとつは、コンピュータから収集したメールアドレスへ電子メールを送信する際に、送信者名を「admin@(受信者のメールアドレスのドメイン名)」と詐称することです。また、本文に、メールアドレスがまもなく有効期限切れになるといった内容を記載することによって、受信者が添付ファイルを実行してしまうように仕組まれています。

本文：

```
Hello there,

I would like to inform you about important information regarding your
email address. This email address will be expiring.
Please read attachment for details.

---
Best regards, Administrator
```

■Antinny（アンティニー）

Antinny（アンティニー）は、日本向けのトロイの木馬型のワームです。日本で開発されたファイル共有ソフト「Winny」を利用して自身のコピーを頒布することで増殖します。

このウイルスに感染すると、システムの設定を変更することで、ワームが指定したフォルダを「Winny」のアップロード用フォルダに設定し、その中に複数の自分自身のコピーを異なる名前で作成して感染を拡大させようとします。

いくつかの亜種の中には、非常に危険性の高いものもあります。たとえば、ログオン中のユーザーのデスクトップのイメージを jpeg ファイルでキャプチャして、「Winny」の共有フォルダに保存するため、そのときに使用しているソフトウェアによっては機密情報が漏洩することがあります。また、システム情報やメールアドレスなどをテキストファイルに保存して「Winny」上で共有させることによっても、情報が漏洩します。

さらに、コンピュータ内の特定のフォルダに保存されているファイルを削除したり、ウイルス対策ソフトの実行を停止させたり、任意の Web ページにユーザー情報を送信したりするものもあります。

■ Swen（スウェン）

Swen（スウェン）は、トロイの木馬型のワームで、多くの感染経路を持つ非常に感染力の強いウイルスです。

このワームは、Outlook Express や Outlook を適切な対策を施さずに使用している場合に、受信した電子メールをプレビューしただけでウイルスの活動を開始されます。

感染経路のひとつは電子メールですが、このウイルスはメールアドレスをコンピュータから収集するだけでなく、インターネット上のニュースグループを検索して収集します。また、電子メールの件名や本文、送信者のメールアドレスは複数確認されていますが、マイクロソフト社からの電子メールを装ったり、メールサーバーからの送信エラーを装ったりするものもあります。

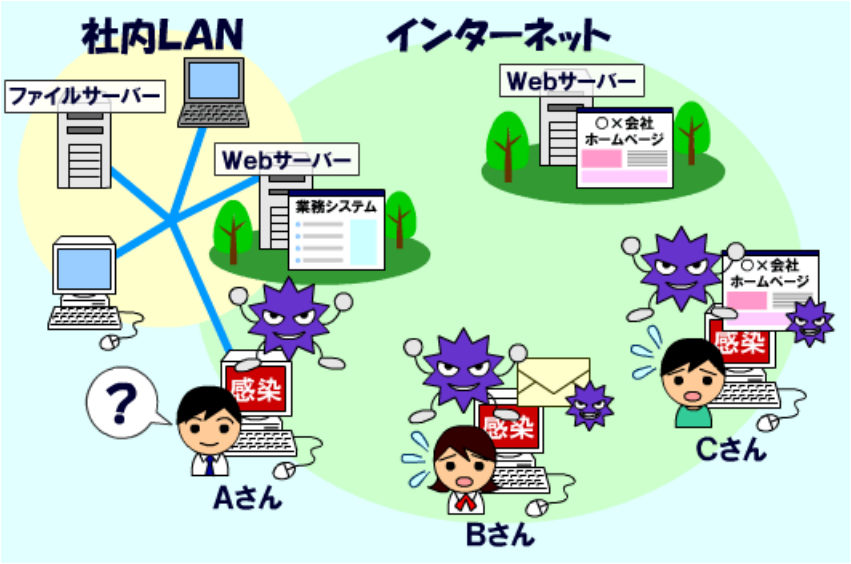
電子メール以外には、ネットワーク上の共有フォルダ、インターネット上の IRC（インターネット・リレー・チャット）、ファイル共有ソフト（KaZaA）を利用して感染活動を行います。

このウイルスに感染すると、自分自身をシステムにインストールし、コンピュータ内の設定ファイルを変更することによって、システムが起動するたびにウイルスが自動起動するように設定されてしまいます。また、感染活動以外にも、ウイルス対策ソフトやファイアウォールソフトの動作を終了したり、レジストリエディタを使用できなくしたり、外部のハッカーサイトに接続して感染したコンピュータ台数の統計を更新したりする機能も持ちます。

Nimda(ニムダ)の感染経路

現在のウイルス（ワーム）の多くは、数多くの感染経路を持っています。クライアントやサーバー、ネットワーク機器などのいずれかに情報セキュリティ上の弱点が残されている場合に、その弱点を突くことで、ウイルスが侵入するようになります。

このような数多くの感染経路を持つウイルスとしては、2001 年に大流行した Nimda（ニムダ）というウイルスがとても有名です。



■ネットワークドライブによる感染

Nimda は、LAN に接続されているネットワークコンピュータを介した感染活動も行います。

Nimda に感染したコンピュータは、自分のコンピュータのドライブにウイルスのファイルをコピーしますが、このとき、ネットワークドライブに接続している場合には、それらのドライブにもウイルスのファイルがコピーされるため、LAN 上の他のコンピュータもウイルスに感染してしまいます。

■Web サーバーによる感染

Nimda は、Web サーバーを利用した感染活動も行います。Nimda は、セキュリティホールが残されたままのマイクロソフト社の IIS という Web サーバーに感染して、ホームページにウイルスを埋め込みます。

そして、Nimda に感染したホームページを閲覧しようとしたコンピュータが、ホームページと一緒に Nimda のファイルをダウンロードしてしまうと、このウイルスに感染します。

■電子メールによる感染

Nimda でもっとも強力な感染方法は、電子メールの添付ファイルです。コンピュータに適切な情報セキュリティ対策を施していない場合には、Nimda ウイルス付きの電子メールをプレビューしただけで感染してしまいます。

そして、Nimda に感染したコンピュータは、新たにウイルス付きの電子メールを外部に送信します。その際に、送信メールの宛先には、電子メールソフトの送信済みアイテムと受信トレイに保存されている電子メールから適当に選ばれたメールアドレスが使用されます。

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。