わかりやすい コンピュータ ウイルス

ウイルス

Email

インターネット

携帯型デバイス

安全対策

リファレンス

わかりやすい
コンピュータ
ウイルス

目次

ウイルスが問題となる理由

コンピュータウイルス、ハッカー、クラッカー（侵入者）、データ犯罪などは、トップニュースとして扱われ、それによる損害額は何億円に上るとメディアは主張しています。しかし、ウイルスやその他サイバースペースの厄介なシロモノは、果たして問題にすべきなのでしょうか？本当に害があるのでしょうか？

不確かな場合は、職場や家庭で起こり得る以下の事柄を想像してみてください。

使用中のウイルス対策ソフトを数ヶ月アップデートしていなかったとします。そして、次にアップデートした際、ランダムに数値を変更する新種ウイルスに、簿記スプレッドシートが感染していることがわかりました。当然バックアップはあるでしょうが、感染したファイルを何ヶ月間に渡ってバックアップしていた可能性があります。どの数値が正しいのか、全く見当がつきません。

次に、新種の Email 送信型ウイルスが発見された場合を想像してみます。会社に多数のメールが送信されたため、メールゲートウェイを完全に封鎖することにしました。その結果、大手取引先からの緊急オーダを逃してしまいました。

また、自宅で MBA の勉強をしていたとします。論文完成間近の時、子供が PC に新しいゲームをインストールしたため、マシンが感染してしまいました。そしてウイルスは、ハードディスク上のファイルをすべて削除してしまいました。論文も含めて .....。

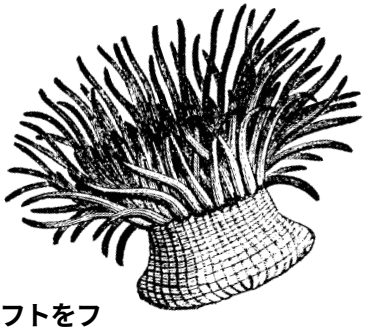
インターネットで見つけたというファイルを友達から受信しました。それを開くと、ウイルスが実行され、アドレス帳にある人全員に機密文書が送信されてしまいました。競合他社も含めて .....。

最後に、ウイルス感染したレポートを取引先に誤って送信してしまった場合を考えます。相手は、今後、取り引きを続けることは、セキュリティ上問題があると思うかもしれません。

このような出来事は、すべて実際起こったことですが、いずれの場合も、それほど費用のかからない簡単な予防措置によって、防ぐことができたかもしれません。

この文書では、どのようなリスクがあるかを説明し、その予防対策を説明して行きます。

ウイルス、トロイの木馬、ワーム



1980年代中頃、パキスタン、ラホーレのバスィット&アムジャット・アルビ兄弟は、自分達が作成したソフトウェアが不正にコピーされていることに気付き、これに対抗するため、ユーザーがそのソフトをフロッピーディスクにコピーすると、自らをコピーし、著作権に関するテキストを挿入するプログラムを作成しました。これは、コンピュータウイルス第1号となり、このような単純な始まりから、反体制的なウイルス文化が生まれました。今日、新種ウイルスは、数時間のうちに世界中に広がり、ウイルス感染事件は、大ニュースとなります。しかし、一般の人は、ウイルスに興味があっても、必ずしも正確な知識を持っているわけではありません。ウイルスの感染方法、予防対策の詳細についてはこの章をお読みください。

ウイルスとは？

コンピュータウイルスは、自己複製をして、通常、ユーザーが知らないうちに、マシンやネットワークに広がるコンピュータプログラムです。

ウイルスには、有害な副作用を持つものがあり、不愉快なメッセージを表示するものから、マシン上のファイルをすべて削除するものまで、色々あります。

ウイルスの感染方法

マシンが感染するためには、まずウイルスが実行される必要があります。

そこでウイルスは、別のプログラムに自らを貼り付けたり、特定の種類のファイルを開いた際、自動的に実行されるコードに身を隠したりして、悪性コードが必ず実行されるようにします。

ユーザーは、人からもらったディスク、Email の添付ファイル、またはインターネットからのダウンロード等を通じて感染ファイルを入手すると考えられます。ユーザーが感染ファイルを起動すると、直ちにウイルスコードが実行され、ウイルスは、他のファイルやディスクに自らをコピーし、ユーザーのマシンに変更を加えます。

詳細は、この章の「ブートセクタ感染型ウイルス」、「パラセティックウイルス」、「マクロウイルス」の項を参照してください。

トロイの木馬

トロイの木馬は、表向きの機能ではない機能を持つプログラムです。

ユーザーが、正規のプログラムだと思って実行すると、しばしば悪質な、隠れた機能を実行します。

例えば、*Troj/Zulu* 、は名目上、2000年問題を解決するためのプログラムですが、実際は、ハードディスクを上書きしてしまいます。

また、トロイの木馬は、ユーザーのマシンにウイルス感染する手段として、しばしば利用されます。

なお、バックドア・トロイの木馬は、インターネットを通じて、他人の PC を制御できるようにしてしまうものです。

ワーム

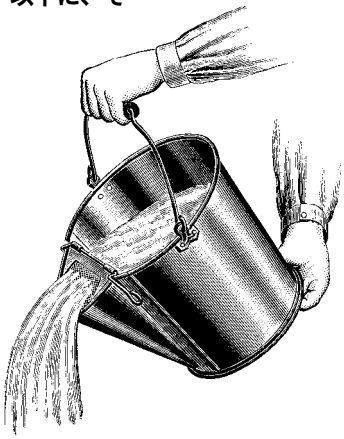
ワームはウイルスに似たプログラムですが、マクロやブートセクタのようなキャリアを必要としません。

そして、自らの完全なコピーを作成し、コンピュータ間のコミュニケーションを利用して広がります。

***Kakworm* (*VBS/Kakworm*) や「ラブレター」ウイルス (*VBS/LoveLet-A*) など、ワームのように動作して、メールを使って、自らを他のユーザーに転送するウイルスはたくさんあります。**

ウイルス副作用の例

「ペイロード」とも呼ばれるウイルス被害の副作用は、ユーザーの関心の的になります。以下に、その例をあげます。



メッセージ *WM97/Jerk* **は、「**I think **‘ユーザー名’**is a big stupid jerk!**」（‘ユーザー名’はバカだと思う！）というメッセージを表示します。**

いたずら *Yankee* **は、午後5時に『ヤンキー・ドゥードル・ダンディ』を演奏します。**

アクセス禁止 *WM97/NightShade* **は、13日の金曜日に、使用中の文書にパスワードをかけます。**

データ盗難 *Troj/LoveLet-A* **は、フィリピンのアドレスに、ユーザー情報とマシン情報を** Email **で送信します。**

データ改ざん *XM/Compatable* **は、**Excel **スプレッドシート内のデータに変更を加えます。**

データ削除 *Michelangelo* **は、ハードディスクの一部を3月6日に上書きします。**

ハードウェア不能 *CIH* **または チェルノブイリ** (*W95/CIH-10xx*) **は、4月26日に** BIOS **を上書きし、マシンを使用不能にしようとします。**

ウイルス感染対象

オフィスには、以下のようなウイルス侵入口があります。

インターネット

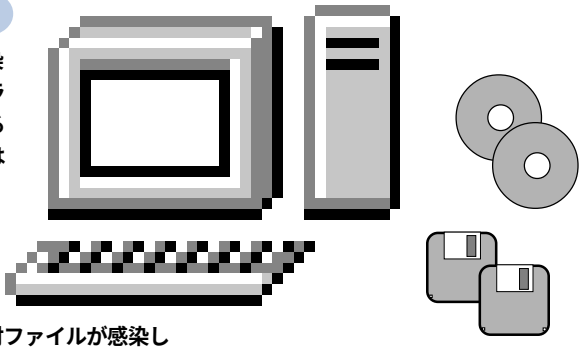
ダウンロードしたプログラムや文書が感染している場合があります。

文書ファイルとスプレッドシート

マクロウイルスが含まれている場合があります。これは、他の文書ファイルやスプレッドシートに感染して、変更を加えます。

プログラム

ウイルス感染したプログラムを実行すると、マシンは感染します。



Email

メールの添付ファイルが感染している場合、それをダブルクリックすると、マシンが感染することがあります。メールをプレビュー表示する、または本文を表示するだけで、悪質なスクリプトが実行されるメールもあります。

フロッピーディスクと CD

フロッピーディスクのブートセクタがウイルス感染している場合、または感染したプログラムや文書ファイルがディスクにある場合があります。また、CD に感染アイテムが含まれている場合もあります。

ウイルス感染を防ぐ

以下に、ウイルス感染を防ぐ方法、あるいは感染した際、対処するための簡単な方法をあげます。

ユーザーの認識を養成する

フロッピーディスクを交換、Web サイトからファイルをダウンロード、メールの添付ファイルを起動したりすると、ウイルスに感染する恐れがある、という認識を組織内に浸透させてください。

ウイルス対策ソフトを使って、定期的にアップデートする

ウイルス対策プログラムは、ウイルスの検出、そして駆除を行うことができます。オンアクセス検索は、感染アイテムへのアクセスを拒否して、ウイルス感染を防ぐので、この機能がある場合は使用することをお勧めします。この章の「ウイルス対策ソフト」の項を参照してください。

すべてのデータをバックアップする

すべてのデータ、OS、ソフトウェアをバックアップするようにしてください。ウイルス感染した場合、ファイルやプログラムを、未感染のものと置き換えることができます。

詳細は、「安全対策10ステップ」の章を参照してください。

ブートセクタ感染型ウイルス

最初に出現したウイルスは、ブートセクタ感染型ウイルスでした。これは、コンピュータを起動するプログラムが含まれるブートセクタに変更を加えて感染を広げるものです。

電源を入れるとマシンは、通常ハードディスクにあるブートセクタプログラムを探し、それを実行します。（フロッピーディスクや CD にある場合もあります。）その後、このプログラムは、残りの OS をメモリにロードします。

ブートセクタ感染型ウイルスは、正規のブートセクタの内容を、ウイルスの持つ内容で置き換えます。（元のブートセクタの内容は、通常、ディスクの他の部分に隠します。）次にマシンを起動すると、感染したブートセクタの内容が実行され、ウイルスはアクティブになります。

マシンは、ブートセクタが感染しているフロッピーディスクなど、感染ディスクを使ってブートした場合にのみ感染します。

ブートセクタ感染型ウイルスの多くは、古くから存在するものです。DOS マシンを対象に作成されたものは、通常、Windows 95/98/Me/NT/2000 マシンには感染しませんが、正常に起動できなくしてしまうことがあります。

Form

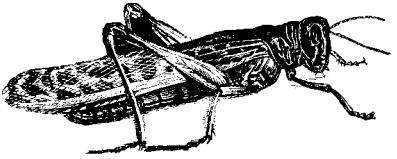
登場してから10年経った現在でも、広く感染しているウイルス。オリジナル版は、毎月18日に発病し、キーボードのキーを押すたびに、カチッという音を立てます。

Parity Boot

「Parity Check」（パリティチェック）とランダムに表示し、OS をハングさせるウイルス。これは、マシンのメモリに欠陥がある際に表示される、正規のエラーメッセージを模倣します。

パラセティックウイルス

パラセティックウイルス（実行ファイル感染型ウイルス）は、プログラム（実行ファイル）に自らを添付します。



パラセティックウイルスに感染したプログラムを実行すると、まずウイルスが先に実行され、その後ウイルスを隠すために、元のプログラムが実行されます。

ウイルスは、マシンの OS **によって、ユーザーが実行しようとしていたプログラムの一部とみなされ、それと同じ権限が与えられます。これによって、ウイルスは、自らを複製、メモリに常駐、副作用を起動したりできます。**

パラセティックウイルスは、ウイルス史初期に出現しましたが、未だに大きな被害を引き起こしています。インターネットによって、プログラムの配布は今までになく容易になったため、これらのウイルスは感染を広げる新たな機会を得ることになりました。

Jerusalem

13日の金曜日、実行されたプログラムすべてを削除します。

CIH（チェルノブイリ）

一定の月の26**日に、**BIOS **チップの一部を上書きし、マシンを使用不能にします。また、ハードディスクも上書きします。**

Remote Explorer

WNT/RemExp (*Remote Explorer*) **は、**Windows NT **実行ファイルに感染します。ユーザーがログインしていなくても、**NT **システムでサービスとして作動できる最初のウイルスとなりました。**

マクロウイルス

マクロウイルスは、マクロ（ファイル内に埋め込まれていて自動的に実行されるコマンド）を使用します。

ワープロ、スプレッドシートなど、多くのアプリケーションではマクロが使用されます。

マクロウイルスは、自らを一つのファイルから別のファイルにコピーして、感染を広げるマクロプログラムです。マクロウイルスを含むファイルを開くと、アプリケーションのスタートアップファイルにウイルスがコピーされ、これで、マシンは感染してしまいます。

そのマシンで同じアプリケーションを使って次回別のファイルを開くと、ウイルスはそれに感染します。感染マシンがネットワーク上にある場合、感染ファイルを他人に送ると、受信した人のマシンも感染して、感染が急速に広がります。

また、悪質なマクロは、文書ファイルや設定に変更を加えることもできます。

マクロウイルスは、たいていの企業で使用されている種類のファイルに感染し、Word と Excel など、複合的ファイルタイプに感染できるものもあります。また、そのアプリケーションを実行できるあらゆるプラットフォームに感染するものもあります。しかし、マクロウイルスが容易に広がる第一の理由は、文書ファイルが Email や Web サイトで頻繁に交換されることにあります。

WM/Wazzu

Word 文書に感染します。1 個から3 個の単語を別の場所に移動し、ランダムに‘ wazzu ’という単語を挿入します。

OF97/Crown-B

Word、Excel、PowerPoint ファイルに感染できます。Word 文書に感染すると、他の Office 97 アプリケーションのマクロ保護を解除し、感染を可能にします。

ウイルス対策ソフト

ウイルス対策ソフトは、ウイルスを検出し、感染ファイルへのアクセスを禁止します。また、駆除を実行することもあります。以下のような種類があります。

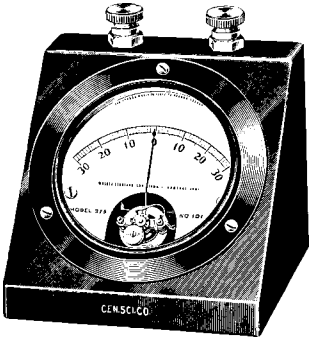
スキャナ

スキャナは、リリース時までに解析されたウイルスを検出、場合によっては駆除します。これは、最も一般に使用されているウイルス対策ソフトと言えますが、新種ウイルスを検出するためには、定期的にアップデートする必要があります。アップデートは、通常、毎月、あるいは３ヶ月ごとに行われます。

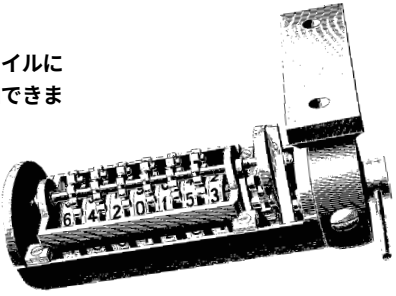
スキャナには、オンデマンドスキャナとオンアクセススキャナがあり、ウイルス対策ソフトの多くには両方の機能があります。

オンデマンドスキャナは、特定のファイルやドライブの検索をユーザーが開始、スケジュール設定します。

オンアクセススキャナは、マシンの使用中メモリに常駐し、ファイルを開く、または実行しようとする際に、ウイルス検索を実行します。



チェックサム方式



チェックサム方式ソフトは、ファイルに変更が加えられた際、それを検知できます。したがって、ウイルスがプログラムや文書ファイルに感染し、変更が加えられると、それを報告します。

チェックサム方式ソフトの主な利点は、ウイルス認識のために、各ウイルスについて何の情報を持たなくてもよいということです。よって、定期アップデートも必要ありません。

弱点は、ウイルス攻撃による変更と正規の変更を区別できないため、誤警告が頻繁に起こる可能性があるということです。文書ファイルの内容は頻繁に変わるため、これは、文書ファイルで特に問題となります。

また、ウイルス感染があった場合、それを報告するだけなので、ウイルスの種類を識別することもできなければ、駆除もできません。

ヒューリスティック

ヒューリスティック・ソフトは、ウイルスがどのようなコードで形成されているかという一般的なルールから、既知ウイルス、未知ウイルスの両方を認識しようとします。従来のスキャナと異なり、すべての既知ウイルスを認識するためのアップデートを行う必要もありません。

しかし、認識できない新種のウイルスが出現した場合、ソフトをアップデート、または入れ替えする必要があります。

なお、ヒューリスティック・ソフトでは、非常に多くの誤警告があることも問題です。

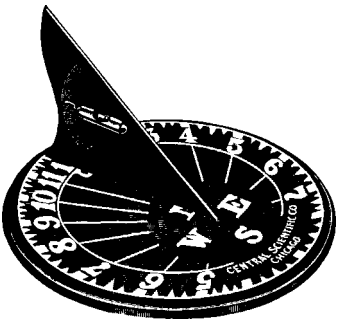
ウイルス略歴

1949年 **数学者** John von Neumann **が、コンピュータプログラムが自己複製できることを示唆。**

1950年代 **ベル研究所が、悪質なプログラムを使って、プレーヤーが互いのコンピュータを攻撃する試験的ゲームを開発。**

1975年 SF **作家** John Brunner **が、コンピュータ「ワーム」がネットワークを通じて広がることを想像。**

1984年 Fred Cohen **が、「コンピュータウイルス」という用語を、そのようなプログラムについての論文で使用。**



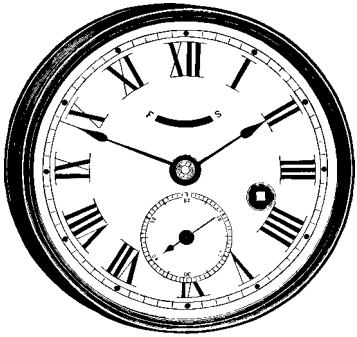
1986年 **初のコンピュータウイルス** *Brain* **が、パキスタンの**2**兄弟によって書かれたとされる。**

1987年 *Christmas tree* **ワームが、**IBM **ネットワークを世界規模で麻痺させる。**

1988年 *Internet* **ワーム が、米防衛高等研究企画庁（**DARPA**）のインターネットで広がる。**

1990年 Mark Washburn **が、感染するたびに自己修正する（自らの姿を変える）ポリモルフィック型ウイルス、***1260* **を作成。**

1992年　**実際に感染したコンピュータはわずかであるが、*Michelangelo* ウイルスが全世界にパニックを巻き起こす。**



1994年　**デマウイルス *Good Times* が出現。デマウイルスが初めて話題となる。**

1995年　**初のマクロウイルス *Concept* が出現。同年、オーストラリアのウイルス作成者が、初の** Windows 95 **対象ウイルスを作成。**

1998年　***CIH*（別名 チェルノブイリ）が、コンピュータのハードウェアを麻痺させる最初のウイルスとなる。**

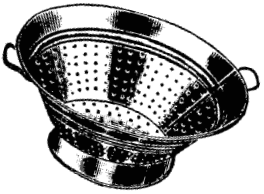
1999年　Email **によって自らを送信するウイルス、*Melissa* が全世界で広がる。メールを表示しただけでマシンに感染する最初のウイルス、*Bubbleboy* が出現。**

2000年　**「ラブレター」ウイルス が、史上、最も広く感染した** Email **送信型ウイルスとなる。感染したユーザーはいないが、パーム** OS **用の初のウイルスが出現。**

ウイルスによる隠れた被害

ウイルスは、データを破壊・削除するだけにとどまらず、隠れた被害を企業に与える場合があります。

ハードディスクを削除したり、文書ファイルを破損するウイルスのことは誰でも知っています。このような被害は深刻ですが、バックアップがきちんとあれば、復旧することは困難ではありません。より深刻なのは、一見しただけでは気づかない被害です。



例えば、 ウイルス感染によってマシンが作動しなくなったり、ネットワークをシャットダウンする必要が発生したりしますが、これは、作業時間、つまり生産性の低下を意味します。

また、企業が依存するコミュニケーションを妨げるウイルスもあります。Email によって送信される *Melissa* や *ExploreZip* は、非常に多くのメールを発信し、サーバーをクラッシュさせることがあります。このような事態にならなくても、ウイルス事件への対処方法として、メールサーバーをシャットダウンする企業もあります。

更に、企業機密が危険にさらされる場合もあります。例えば、*Melissa* は、機密情報を含んでいることもありうる文書を、アドレス帳内のユーザーに送信してしまいます。

ウイルスは、企業の信用に大きな打撃を与える場合もあります。客先に感染文書を送信してしまったら、取り引きを拒まれたり、賠償金を請求されるかもしれません。また、自社の信用に傷をつけるだけでなく、気まずい思いをさせるウイルスもあります。例えば、*WM/Polypost* は、ユーザー名を使用して、そのユーザーの文書を、alt.sex usenet ニュースグループに投函してしまいます。

ウイルス作成者？

コンピュータやネットワークがウイルスに感染した場合、まず最初に思うのは、「なぜ、ウイルスを書く人がいるのか？」ということでしょう。

一見すると、ウイルスを作成しても何もメリットはないように思われます。金銭的報酬を得たり、キャリアアップが図れるわけでもなく、有名になることもほとんどありません。また、ウイルスは無差別に感染してしまうので、ハッカーと異なり、特定の人を犠牲者に狙えるわけでもありません。

しかし、ウイルス作成は、落書き、公共物の破壊などの非行行為になぞらえると、理解しやすいと思われます。

ウイルス作成者の多くは、25才未満の独身男性で、仲間や小規模なｅ-コミュニティの称賛が自尊心につながっています。落書きアーティストと同様、ウイルス作成行為は、パフォーマーとしてのステータスを保証するのです。

また、ウイルス作成者は、ウイルスを書くことによって、現実の世界では決して持つことのできない力を、サイバースペースでものにすることができます。妄想の力量、権威を売り物にする、ヘビーメタルやファンタジー文学からインスピレーションを得た名前がペンネームとして使用されることからも、それがうかがえます。

ウイルス

Email

インターネット

携帯型デバイス

安全対策

リファレンス

ウイルス作成は絶対に悪か？

たいがいの人は、ウイルスは害のあるもの、と疑いを持っていませんが、実際のところは、どうなのでしょうか？

害のないウイルスやジョークウイルスは、たくさんありますし、ソフトウェアのセキュリティホールを指摘するものもあります。このため、バグ修正の配布など、ウイルスが役にたつこともあると主張する人がいます。しかし、よく吟味してみると、実際には、「無害」なウイルスがあるという主張は成り立たないことがわかります。

第一に、ウイルスは、ユーザーの許可なしに、時としては知らないうちに、マシンに変更を加えます。これは倫理に反するだけでなく、動機が何であろうとも、多くの国で違法となります。オイル交換するつもりでも、他人の車を無断で借りてはいけないのと同様に、他人のコンピュータに無断で触ってはいけないわけです。

第二に、ウイルスが常に作成者の意図に沿って動作するとは限りません。下手に書かれている場合、予期しない問題が起こることがあります。また、意図した OS 上では無害であっても、他のプラットフォームや将来開発されるシステム上で、非常に破壊的であることがありえます。

概念を証明する

時として、新しい種類のウイルスが存在可能なことを証明するためにウイルスを書く人もいます。このようなウイルスは「概念を証明する」ウイルスと呼ばれ、通常、副作用（ペイロード）はなく、ユーザー環境にリリースするべきではありません。

研究目的？

ウイルス作成者は、研究活動を行っていると好んで主張します。しかし、ウイルスのコーディングはしばしばお粗末で、予期していないユーザーを対象にランダムにリリースされ、その研究結果をまとめる手段は全くなく、研究活動と呼べるものではありません。

デマウイルス

Good Times、*Budweiser Frogs*、*How to give a cat a colonic* **といったウイルスについて警告するメッセージは、すべてデマウイルスの仕業でした。デマウイルス、特に** Email **デマウイルスは広く感染しており、それによって無駄になる時間とお金は、真のウイルスによる被害に匹敵します。**

ウイルス

Email

インターネット

携帯型デバイス

安全対策

リファレンス

デマウイルスとは？

デマウイルスは、偽りのウイルス報告で 、通常、Email で配布され、 以下のようなことを行います：

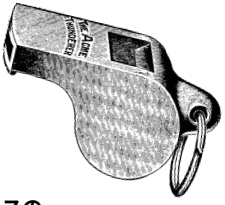
- **検出不能で、破壊的な新種ウイルスがあることを警告。**
- **「Join the Crew」、「Budweiser Frogs」など、特定の件名のメールを読まないよう促す。**
- **大手ソフトウェア会社、インターネットプロバイダ、政府機関（例：IBM、Microsoft、AOL、米連邦通信委員会 - FCC）によって警告が発せられたと主張する。**
- **新種ウイルスがありえないことをできる、と主張する。例えば、*A moment of silence* は、「マシンに新たに感染するためにプログラムが交換される必要はない」とする。**
- **ウイルスの影響を説明するために、技術的に意味のない言葉を使う。例：*Good Times* は、ウイルスが PC のプロセッサを n 段階、複合無限バイナリループに設定する、と主張する。**
- **他のユーザーに警告を転送することを強く促す。**

デマウイルスじゃなかった ……

2000年4月1日、件名が「*Rush-Killer virus alert*」という Email がユーザー間で交換されました。これはモデムを制御して 911（米国の緊急電話番号）をダイアルするウイルスについて警告するもので、このメールを転送することを促しました。メールはデマウイルスの特徴を持ち合わせていましたが、警告対象のウイルスは、真のウイルス *BAT/911* の一種で、Windows の共有ファイルを通じて感染し、911 をダイアルするものでした。デマウイルスと真のウイルスを見分けるのは難しいことです。この章の終わりの「デマウイルスの対処方法」にあるアドバイスに従ってください。

デマウイルスはなぜ問題となるか？

デマウイルスの中には、真のウイルスと同様、破壊的で、被害額がかさむものがあります。



各ユーザーが、友人や同僚全員にデマウイルスの警告を転送すると、大量のメールが流れることになります。メールサーバーには負荷がかかり、結果としてダウンしてしまいます。この現象は、「ラブレター」ウイルスの場合と同様ですが、デマウイルスの場合、コンピュータコードを書く必要もありません。

過剰反応するのはエンドユーザーだけではなく、デマウイルスを受信した企業も、メールサーバーやネットワークをシャットダウンするなど、しばしば大々的な処置を取ります。これによって、真のウイルスによる被害よりも、より確実にコミュニケーション網が麻痺し、重要なメールであっても、アクセスできなくなってしまいます。

また、偽りの警告は、真のウイルス脅威に対処するエネルギーをそらすことになります。

デマウイルスの中には、非常に執拗なものもあります。また、デマウイルスはウイルスでないため、ウイルス対策ソフトを使って、検出・無効にすることもできません。

どっちが先？

デマウイルス出現後、真のウイルスが作成されることもあり、またその逆もあります。デマウイルス *Good Times* がトップニュースになった時、それがデマであるということがあばかれるのを待って、それと同名の真のウイルス（ウイルス対策ベンダーは、*GT-Spoof* と呼ぶ）を書いたウイルス作成者がいました。

デマウイルスの対処方法

真のウイルスや幸福の手紙と同様、デマウイルスは、転送されて広がらない限り意味がありません。このため、デマウイルスを転送しないようユーザー教育できれば、それによる被害を最小限に抑えることができます。

ウイルス警告に関する方針を社内で設置する

ウイルス警告に関する方針を社内で立てることが必要かもしれません。以下にその例をあげます：

「ウイルス対策ベンダーが警告、大手コンピュータ会社、あるいは親友がそれを確認したとしても、ウイルス対策担当者以外には、いかなる種類のウイルス警告も転送しない。すべてのウイルス警告は、【*責任者名を記入*】にのみ転送する。そしてその担当者が責任を持って、全員に通知する。それ以外のウイルス警告は、すべて無視する。」

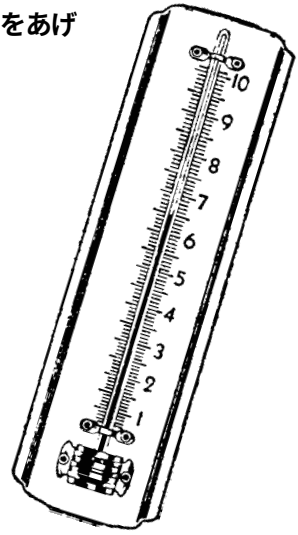
ユーザー全員がこの方針に従えば、メールが大量に送信されることもなく、担当者がその都度リスクを確認することができます。

デマウイルスについての情報を集める

デマウイルスについての情報を、Web サイトなどから集めてください。（例：www.sophos.com/virusinfo/hoaxes）

ウイルストップ10

最も成功を収めたウイルスは何でしょうか？この章では、最も広く感染したもの、最も多くのマシンに感染したもの、最も長くユーザー環境にいたものをあげてみました。



ウイルス

Email

インターネット

携帯型デバイス

安全対策

リファレンス

ラブレター

(VBS/LoveLet-A)

恐らくラブレターウイルスが、最も名の知れたウイルスでしょう。ラブレターを装ってユーザーの興味をそそり、数時間のうちに全世界に広がりました。

発見年： 2000年5月

発生地： フィリピン

種類： Visual Basic スクリプトワーム

発病条件： 最初の感染時

ペイロード： オリジナル版は、件名が「I LOVE YOU」で、本文が「添付した私からのラブレターを読んでください。」というEmailを送信します。添付ファイルを起動すると、ウイルスが実行され、Microsoft Outlookがインストールされている場合、ウイルスは、Outlookアドレス帳内のアドレスすべてに自らを送信しようとします。他のニュースグループユーザーに自らを送信したり、ユーザー情報を盗んだり、ファイルを上書きしたりもできます。

Form

Formは、8年間ウイルストップ10内に位置し、現在でも広く感染しています。DOSや初期のWindows環境では存在が目立たず、広く感染しました。

発見年： 1991年

発生地： スイス

種類： ブートセクタ感染型

発病条件： 毎月18日

ペイロード： キーを押すたびに、カチッという音を立てます。NTマシンを作動不能にできます。

Kakworm

(VBS/Kakworm)

感染メールを表示するだけで、Kakworm **はマシンに感染することができます。**

発見年： 1999**年**

種類： Visual Basic **スクリプトワーム**

発病条件： **最初の感染時（副作用の大半）、毎月**1**日（**Windows **をシャットダウンする副作用）**

ペイロード： **このワームは、**Email **本文に埋め込まれて送信されます。**Outlook **を使用、あるいは**Internet Explorer 5 **と**Outlook Express **を併用している場合は、感染メールを開く、またはプレビュー表示した際にマシンが感染する場合があります。**Outlook Express **の設定を変更して、送信するメールすべてにウイルスコードが含まれるようにします。また、毎月**1**日午後**5**時以後、「**Kagou-Anti_Kro$oft says not today**」というメッセージを表示し、**Windows **をシャットダウンします。**

Anticmos

Anticmos **は、典型的なブートセクタ感染型ウイルスで、**1990**年代半ばに広く感染し、頻繁にウイルストップ**10**に含まれました。**

発見年： 1994**年**1**月**

発生地： **香港で発見されましたが、中国に源を発するものとされています。**

種類： **ブートセクタ感染型**

発病条件： **ランダム**

ペイロード： **インストールされているフロッピーディスクやハードディスクに関する情報を削除しようとします。**

Melissa

(WM97/Melissa)

Melissa **は、ユーザーの好奇心を利用して、急速に感染する** Email **送信型ウイルスです。一見、知っている人から送信されたメールに見え、読みたくなるような文書が含まれています。このため** Melissa **はわずか**1**日で世界中に広がりました。**

発見年： 1999**年**3**月**

発生地： **アメリカのプログラマ、**David L. Smith (31**才**) **が** alt.sex usenet **ニュースグループに感染文書を投函。**

種類： Word 97 **マクロウイルス、**Word 2000 **にも感染**

発病条件： **最初の感染時**

ペイロード： Microsoft Outlook **がアクセスできるすべてのアドレス帳にある最初の**50**個のアドレスに、件名にユーザー名を入れてメッセージを送ります。感染文書が添付されており、文書を開いた際、分と日付が同じ場合（例、**3**月**5**日の**10**時**5**分）、ウイルスはゲーム『スクラブル』に関するテキストを、文書に挿入します。**

New Zealand

New Zealand **は、**1990**年初頭、最も感染件数の多いウイルスでした。**

発見年： 1980**年代末**

発生地： **ニュージーランド**

別名： Stoned

種類： **ブートセクタ感染型**

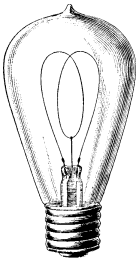
発病条件： **フロッピーディスクより起動した場合、**8**回につき**1**回。**

ペイロード： **「**Your PC is now Stoned!**」（**PC **は麻薬でハイになった！）というメッセージを表示。**360K **ディスクのルートディレクトリの最終セクタに元のブートセクタをコピーする。より容量の大きいディスクも破損可能。**

Concept

(WM/Concept)

Concept は Microsoft の公式ソフトに誤って含まれて発送されたため、一挙に広がりました。ユーザー環境で発見された最初のマクロウイルスで、1996年から1998年にかけて、最も一般的なウイルスの一つとなりました。このウイルスは、Word が自動的に実行する「AutoOpen」マクロを使用してファイルを制御し、Word が文書を保存する際に起動される「FileSaveAs」マクロも使って感染します。数多くの亜種があります。



発見年： 1995年8月

種類： マクロ

発病条件： なし

ペイロード： 感染文書ファイルを開くと、数字の1を含んだ、「Microsoft Word」というタイトルのダイアログボックスが表示されます。「That's enough to prove my point」（これで言いたいことは示せた）というテキストが含まれていますが、これは、決して表示されません。

CIH（チェルノブイリ）

(W95/CIH-10xx)

CIH は、コンピュータのハードウェアを破壊する初のウイルスです。BIOS を上書きすると、BIOS チップを交換するまで、マシンは使用不能となります。

発見年： 1998年6月

発生地： 台湾のチェン・イン-ハウが作成

種類： Windows 95 マシンに感染するパラセティックウイルス

発病条件： 4月26日。亜種は6月26日や毎月26日に発病します。

ペイロード： BIOS の上書きを試み、その後ハードディスクを上書きします。

Parity Boot

Parity Boot は、フロッピーディスクのブートセクタに感染します。このウイルスが現在でもまだ広く感染していることより、1980年代、1990年代に最も感染件数の多かったブートセクタ感染型ウイルスが、依然として勢力があることがわかります。1998年においてさえ、このウイルスは最も感染件数の多いウイルスの一つでした。特にドイツでは、1994年に雑誌の付録 CD-ROM によって配布されたため、広く感染しました。

発見年： 1993年3月

発生地： ドイツ？

種類： ブートセクタ感染型

発病条件： ランダム

ペイロード： 「Parity Check」（パリティチェック）と表示し、コンピュータをハングさせます。メモリエラーを模倣するため、ユーザーは、RAM（Random Access Memory）に原因があると勘違いしてしまいます。

Happy99

(W32/Ska-Happy99)

Email によって迅速に感染を広げるウイルスの中で、Happy99 は一番最初に知られたものです。

発見年： 1999年1月

発生地： フランスのウイルス作成者 ‘ Spanska ’ がニュースグループに投函。

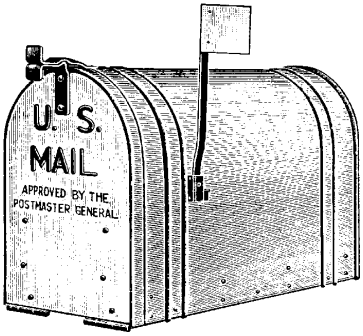
種類： Windows 95/98/Me/NT/2000 マシンで作動するファイル感染型ウイルス

発病条件： なし

ペイロード： 打ち上げ花火の模様を表示し、「Happy New Year 1999」というメッセージを表示します。このウイルスは、Windows システムディレクトリ内のファイル wsock32.dll を変更し、Email を送った際に、このウイルスを含む二通目のメッセージも送るようにします。

Email

ウイルス名を一つあげるとしたら、たいていの人は、「ラブレター」ウイルスか *Melissa* をあげるでしょう。大々的にニュースで取り上げられたこの二つのウイルスに共通していることは、Email によって全世界に広がったことです。



Email は、現在ウイルス感染の最も大きな原因です。これはなぜでしょうか？

フロッピーディスクによってウイルスが感染する限り、感染速度はゆっくりしたものでした。企業はフロッピーディスクの使用を禁止したり、ディスクのウイルス検索を徹底させるなどして対応できました。しかし、Email の発達によって、様子が一変してしまいました。ファイルの交換は、より敏速に行われ、ウイルスが PC に感染することは、アイコンにクリックする、またはそれ以上に簡単です。従来のウイルスは、より迅速に感染を広げられるようになり、新しいタイプのウイルスは、メールプログラムの機能をフルに活用しているのが現状です。

メールを読むだけで感染するか？

添付ファイルを開かない限り、メールを開くのは安全だと思っている人がいますが、これは必ずしも正しくありません。

Kakworm **や** *Bubbleboy* **などのウイルスは、メールを開いた段階で、ユーザーのマシンに感染します。そのメールはごく普通のメッセージを含んでいるように見えますが、メールを開く、あるいは（**Internet Explorer **の特定のバージョンと** Outlook **を使用している場合）、プレビュー表示しただけで実行されるスクリプトが隠されています。このスクリプトは、システム設定に変更を加え、メールを通じてウイルスを他のユーザーに送信します。**

Microsoft **より、このセキュリティホールに対応するパッチが発行されています。ダウンロード先は、**www.microsoft.com/technet/security/bulletin/ms99-032.asp **です。**

Email **デマウイルス**

デマウイルスは、知っている人すべてに警告メッセージを転送するよう促す、偽りのウイルス報告で、Email **を利用したものが多数あります。**

Email **デマウイルスは、ウイルスのようにネットワークを通じて広がり、メールサーバーをダウンさせる場合があります。真のウイルスと違い、デマウイルスはウイルスコードを必要とせず、だまされやすいユーザーがいることを当てにして広がります。詳細は、「デマウイルス」の章を参照してください。**

メールによって自動的に感染するウイルス

今日最も勢力を振るっているウイルスは、自動的に Email で感染を広げるタイプです。

たいていの場合、これらのウイルスが効力を発するには、ユーザーが添付ファイルをクリックすることが必要です。これによって、メールプログラムを使用して感染ファイルを他のメールユーザーに送信するスクリプトが実行されます。例えば、*Melissa* は、Microsoft Outlook がアクセス可能なすべてのアドレス帳内の、最初の50のアドレスにメッセージを送ります。アドレス帳にあるすべてのアドレスに、自らを送信するウイルスもあります。

スパムとは？

スパムは、要求しないのに送られてくる Email で、しばしば、金儲け、自宅でする仕事の勧誘、ローン、わいせつサイトの宣伝などを扱っています。偽造した返信情報が含まれているものが数多くあるため、送信者の取り締まりは容易ではありません。スパムを受信したら、単に削除してください。

添付ファイルに伴うリスク

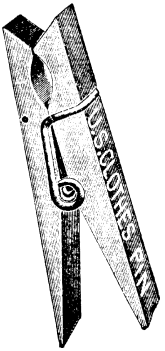
現在最大のセキュリティリスクは、Email ではなく、その添付ファイルです。

添付ファイルとして受信したプログラム、文書ファイル、スプレッドシートなどは、すべてウイルスを含んでいる可能性があり、それを起動すると、マシンが感染する恐れがあります。

添付ファイルによる情報交換は一般的で、スクリーンセーバー、グリーティング・カード、アニメーション、ジョークプログラムを交換するのは、たわいないことと思っているユーザーはたくさんいます。しかし、このようなファイルがウイルス感染している場合があるのです。

また、拡張子が .txt のファイルなど、安全なタイプのファイルと思われるものでも、危険な場合があります。つまり、テキストファイルと思っていたファイルが、.vbs の拡張子が隠された、悪質の VBS スクリプトファイルであったということがあります。

***VBS/Monopoly* ワームは、ゲームのように見せ掛けた悪質なプログラムの一つです。「Bill Gates ジョーク」 として振る舞い、これは（Microsoft の画像のある『モノポリー』のゲーム・ボードを表示する）ジョークですが、同時に、自分自身を他のユーザーに送信し、マシンのシステム情報を特定のメールアドレスに送信してしまいます。よって情報の機密性が侵される恐れがあります。**



Email 盗聴、改ざん

Email 盗聴は、メールの転送中に、他人がその内容を読むことです。これは、メールを暗号化して防ぐことができます。

Email 改ざんは、送信元アドレスを偽造してメールを送ったり、内容に手を加えることです。これは、デジタル署名を使用して防ぐことができます。

Email 送信型ウイルス対策

添付ファイルに関する厳重な方針を設置する

Email 送信型ウイルスは、ユーザーの行動パターンを変えることで、最も容易に対処できます。親友から添付ファイルを受信しても開かない、即座に報酬がある、無害な楽しみ、という謳い文句に乗せられない、ウイルス未感染か確かでない場合は、感染しているものとして扱うことなどが必要です。また、添付ファイルは**すべて**、ウイルス対策ソフトで検索し、認証してから開く、という社内方針を設けることが重要です。

Windows Scripting Host (WSH) を無効にする

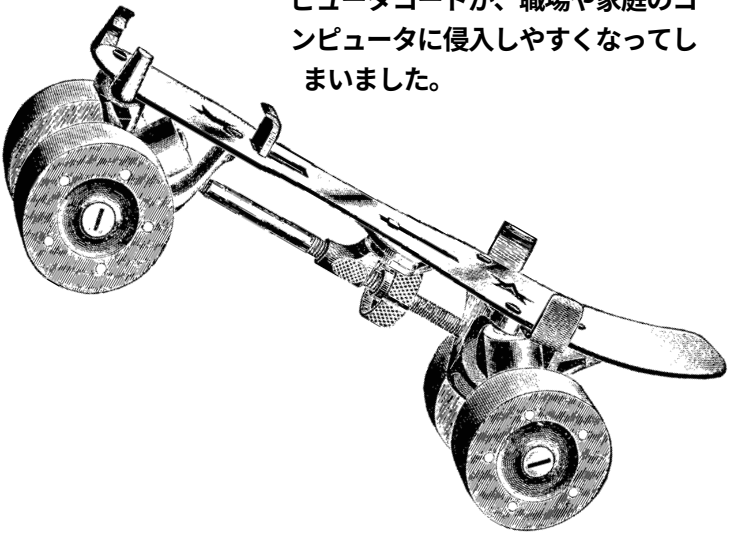
Windows Scripting Host (WSH) は、Windows マシンで、VBS や Java スクリプトを実行するといった操作を自動化します。しかし、これは、「ラブレター」ウイルスのようなウイルスの感染を広げる原因となります。WSH は通常必要ないと考えられますが、まずシステム管理者に相談してください。無効にする方法は、www.sophos.com/support/faqs/wsh.html を参照してください。なお、WSH は、Windows や Internet Explorer をアップデートするたびに有効になることにご注意ください。

ウイルス対策ソフトを使う

オンアクセス検索を実行するウイルス対策ソフトを、デスクトップマシンとメールゲートウェイで使用してください。これによって、メールによって送信されるウイルスより保護されます。

インターネット

インターネットによって、より多くの人に、より多くの情報を、より手早く伝えることが可能になりました。しかし、その結果、悪質なコンピュータコードが、職場や家庭のコンピュータに侵入しやすくなってしまいました。



クリック＆感染？

インターネットの登場によって、ウイルス感染のリスクは増加しました。

10年前、ほとんどのウイルスはフロッピーディスクを通じて感染しました。感染速度は遅く、感染するには、ユーザーがあえて未知のプログラムを実行することが必要でした。また、ウイルスの副作用があまりにも明らかであった場合は、感染を広げる見込みはありませんでした。しかし、インターネットが広く使用されるようになった現在、状況は一変しました。

インタネットでソフトを共有するのは容易なことで、マウスを一度クリックするだけで、プログラムをメールに添付でき、保存・起動も簡単です。Web ページにプログラムをアップロードすることも簡単で、だれでもそれをダウンロードできます。このため、プログラムに感染するパラセティックウイルス（実行ファイル感染型ウイルス）は、インターネットで大いに勢力を伸ばしています。

しかし、インターネットの恩恵を最も受けているのは、文書ファイルに感染するマクロウイルスです。ユーザーは、頻繁に文書ファイルやスプレッドシートをダウンロードしたり、メールで交換したりします。ダウンロードしたファイルや添付ファイルが感染している場合、それをクリックするだけで、ユーザーのマシンはマクロウイルスに感染してしまいます。

したがって、インターネットを使用する際は、マクロを無視するビューアで文書ファイルを開き、発信元が信頼できないプログラムは、実行しないことが重要となります。

Web サイトにアクセスしただけで感染するか？

Web サイトへのアクセスは、未知のプログラムや文書ファイルを開くことよりは安全ですが、リスクもあります。そのリスクは、各サイトで使用されているコードの種類、及びサービスプロバイダやユーザーが実施しているセキュリティ対策によって異なります。使用されている主なコードを以下にあげます。

HTML

Web ページは、HTML (Hypertext Markup Language) で書かれています。HTML は、テキストをフォーマットしたり、グラフィックや他のページにリンクを設定したりすることを可能にします。HTML コードにウイルスコードを含めることはできませんが、Web ページに、アプリケーションを起動したり、自動的に文書ファイルを開いたりするコードを含めることができるので、感染アイテムが実行される危険性が出てきます。

ActiveX

Windows マシン用、Web 開発者向け Microsoft 技術です。

Web ページでビジュアル効果を出すために使用される ActiveX アプレットは、マシンのリソースにフルアクセスできるため、危険をもたらす可能性があります。しかし、デジタル署名の使用によって、そのアプレットが信頼でき、変更が加えられていないことが証明されるので、ある程度セキュリティが保証されます。

続：Web サイトで使用されるコード

Java

Web ページで効果を出すための Java アプレットと、Java アプリケーションや Java スクリプトを混乱して、インターネットで Java ウイルスに感染することについて、必要以上に心配する人がいます。

アプレットは通常、安全で、ブラウザは、「サンドボックス」と呼ばれる安全な環境でアプレットを実行します。セキュリティ対策の手落ちで、悪質なアプレットが外部に流出したとしても、容易に広がることはできません。これは、アプレットが、ユーザー間でなく、通常サーバーからユーザーのマシンに流れるからです。（友達にはサイトのアドレスを教えるだけで、アプレットのコピーを送ることはありません。）更に、アプレットは、Web キャッシュ以外、ハードディスクには保存されません。

悪質なアプレットを見つけたら、それは通常、トロイの木馬（正規のソフトウェアになりすます悪質のプログラム）であると考えられます。

一方、**Java アプリケーション**は、Java 言語で書かれたプログラムで、通常のプログラムと同様、ウイルス感染するので、同様の注意を払う必要があります。

Java スクリプトは、Web ページにある HTML コードに埋め込まれているアクティブなスクリプトです。通常のスクリプトと同様、自動的にタスクを実行できるので、ウイルス感染のリスクが伴います。なお、Java スクリプトは無効にすることができます。（この章の終わりの、「インターネット安全対策」を参照してください。）

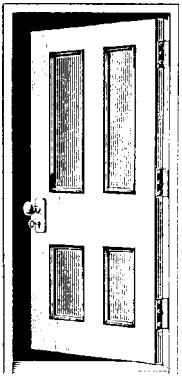
VBS スクリプト

使用しているブラウザの種類によって、VBS (Visual Basic Script) は、Web ページを表示した直後に、ユーザー介入なしで実行することができます。

VBS スクリプトは、*Kakworm* や *Bubbleboy* などの Email ワームで使用されていますが、Web ページで実行することもできます。

バックドア・トロイの木馬

バックドア・トロイの木馬は、インターネットを介して、他のユーザーの PC の管理権を与えるプログラムです。

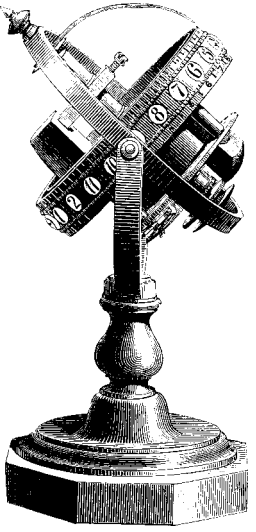


通常のトロイの木馬と同様、バックドア・トロイの木馬は、正規のソフトや望ましいソフトになりすまします。（通常 Windows 95/98 の PC で）実行されると、PC のスタートアップルーチンに自らをコピーし、インターネットへの接続が行われるまで PC を監視します。接続後、バックドア・トロイの木馬を送信したユーザーは、自分のマシンのソフトを使って、感染 PC のプログラムを開いたり、閉じたり、ファイルを変更したり、文書をプリンタに送ることさえできます。*Subseven*、*BackOrifice* などは、よく知られているバックドア・トロイの木馬です。

クッキーは安全か？

クッキーは、コンピュータや保存されているデータに直接脅威は与えませんが、Web サイトは、クッキーを使ってユーザー情報を記憶し、アクセス歴を記録するので、ユーザーの 機密性が侵されます。これを防ぐためには、ブラウザのセキュリティ設定で、クッキーを無効にしてください。

Web サーバーへの攻撃



インターネットで危険にさらされているのはエンドユーザーだけではありません。ハッカーの中には、Web サイトを運営する Web サーバーを攻撃の対象にする者もいます。

Web サーバーに大量のリクエストを送って、作動を遅くさせたり、ダウンさせるのは、よくある攻撃です。これが起きると、このサーバーがホストするサイトに、正規のユーザーはアクセスできなくなってしまいます。

CGI (Common Gateway Interface) スクリプトも弱点の一つです。CGI スクリプトは、Web サーバー上で作動し、検索エンジンやフォームに入力された内容などを処理しますが、正しく使用されていない 場合、ハッカーがサーバーを制御できるようになってしまいます。

インターネット安全対策

インターネットを安全に使用するためには、以下の事柄を実行してください：

インターネット用マシンのネットワークを別に設ける

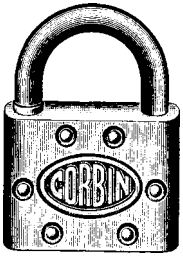
インターネットに接続しているマシンは、他のマシンとは別のネットワークに隔離してください。これによって、主要ネットワークに、ユーザーが感染ファイルをダウンロードしたり、ウイルス感染を広げる危険性が減ります。

ファイアウォールやルータを使用する

ファイアウォールは、認可されたトラフィックのみを組織内に流します。ルータは、インターネットからの、情報パケットの流れを管理します。

ブラウザのセキュリティレベルを正しく設定する

Java、ActiveX アプレット、クッキーなどを無効にする、あるいは、そのようなコードが作動していることを警告するようにしてください。Microsoft Internet Explorer **では、「表示」-「インターネット オプション」-「セキュリティ」-「このゾーンのセキュリティレベル」を選択し、適切なレベルを選択してください。**



携帯電話とパームトップ

1990年代には、インターネットを使って、デスクトップマシンから世界の情報をアクセスすることができるようになりました。今後10年の間には、携帯電話からそれが可能になるでしょう。既に、次世代携帯電話を使って、準インターネットサイトやサービスにアクセスすることが可能で、その技術は急速に発達しています。反面、移動中であっても容易にデータの転送ができる一方で、新たなセキュリティ脅威が出現する恐れがあります。

携帯電話にウイルスは存在するか？

メディアで騒がれ、デマウイルスこそ存在しますが、携帯電話に感染するウイルスは、現在ありません。

一方、電話にメッセージを送信するウイルスは存在します。例えば、Email で感染を広げるワーム *VBS/Timo-A* は、ユーザーのモデムを使って、特定の携帯電話番号にテキスト (SMS) メッセージを送信します。また、悪名高い「ラブレター」ウイルス も、FAX や携帯電話にテキストを送信することができます。しかし、これらのウイルスは携帯電話に感染したり、危害を加えることはできません。

しかし、より洗練された携帯電話が登場すれば、状況は変わると考えられます。

携帯型デバイスのデータは安全か？

携帯型デバイスは、PC と比較して、データを保存する場所としては安全ではありません：

- **紛失したり、盗まれやすい。**
- **電源が不意に切れた場合、データ損失の恐れがある。**
- **データがバックアップされない。**

携帯型デバイスがより複雑になるにつれて、ウイルスやハッカーによる攻撃の対象になる恐れがあります。

WAP 電話とウイルス

この分野で、最も話題になっている新技術は、
WAP (Wireless Application Protocol) **です。**

WAP **は、インターネットのような情報、サービスを、携帯電話やオーガナイザーに提供します。これは、**Web **と同様の方法で作動し、携帯電話にインストールされているブラウザが、中枢サーバーによって送信されたコードを実行します。したがって、現時点では、ウイルス感染の可能性は限られています。**

もちろんウイルスはサーバー自身に感染できますが、感染が広がったり、ユーザーに影響を与える可能性は限られています。

第一に、WAP **システムには、ウイルスが自らをコピーしたり、居残ったりするための場所がありません。**PC **と異なり、**WAP **電話は、使用するアプリケーションを保存しません。つまり、必要なコードをダウンロードして、一時的にブラウザのキャシュに保存するだけです。**

第二に、現在、クライアント電話間のコミュニケーションがないため、ウイルスが他の WAP **ユーザーに感染する方法がありません。**

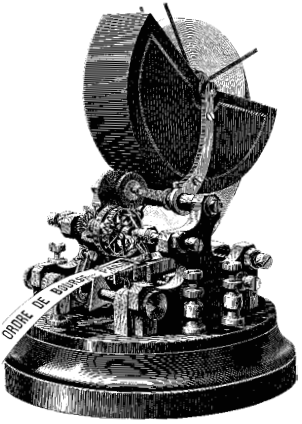
理論的には、悪質な WAP **サイトへの「リンク」をウイルスが配布し、ユーザーに有害なアプリケーションを使用することを促すことができますが、これにもコードをサーバーから実行する必要があります。**

用語ミニガイド

WAP	Wireless Application Protocol
WML	Wireless Markup Language
WML スクリプト	Java **スクリプトに似た、プログラミング言語**
カード	WML **でのページ**
デッキ	**それ以上ダウンロードせずに、**WAP **ブラウザで利用できる、互いに連結したページ。**

WAP：今後 のリスク

WAP は、Web ページのプロトコルである HTTP の一種を使用しているので、WAP ブラウザが現在処理している内容より、より複雑なものを送信することが可能です。したがって、次世代のブラウザによって、マクロウイルスを含んだ文書ファイルなど、より複雑なファイルがダウンロードできるようになるかもしれません。



近い将来 WAP 環境で、サーバーが、各携帯電話にコンテンツを「プッシュ型」で提供できるようになると考えられます。最新の情報（財務報告やスポーツの得点など）や、新しいメールがあることなどをユーザーに知らせる以外に、「プッシュ型」技術は、ユーザー未介入で、データをキャッシュにダウンロードしたりできます。したがって、悪質なコードは、この方法を使って、自らを配布することが可能になります。

これ以外に、例えば、悪質な WAP サイトが便利なサービスを模倣し、ユーザーのブラウザをクラッシュしたり、メモリを一杯にしたりするなどの問題が考えられます。

用語ミニガイド

XML	eXtensible Markup Language：Web での使用が推奨されている。
WTLS	Wireless Transport Layer Security：携帯電話ネットワークで使用される暗号化方法。

携帯型 OS

ウイルスは、非常に近い将来、パームトップや PDA に感染できるようになると考えられます。

パームトップや PDA では、EPOC、PalmOS、PocketPC（旧称 Windows CE） など、特別に書かれた、またはスケールダウンされた OS が実行されます。このような OSでは、いずれ、一般的なデスクトップアプリケーションを使用できるようになると考えられるので、デスクトップマシンと同様、悪質コードによる影響を受けることになります。2001年初め現在、パームシステムを攻撃するトロイの木馬が既に存在します。

パームトップは、アドレス帳やスケジュール帳など、マシン間のデータの同期をとるため、家庭や職場の PC に定期的に接続されるので、このようなデータの同期によって、ウイルス感染が容易に広がると考えられます。

将来的に、携帯型コンピュータか、「スマート」携帯電話のどちらが主流になるかは、現在のところ不明です。どちらにしても、携帯型デバイスを使ったハイレベルなコミュニケーションが可能になるにつれ、セキュリティリスクは増加すると言えます。

用語ミニガイド

EPOC	**パームトップ用** OS。
PDA	Personal Digital Assistant
PalmOS	**パームトップ用** OS。
PocketPC	Microsoft **のパームトップ用** OS。**（旧称** Windows CE**）**
UPNP	Universal Plug and Play**：携帯型デバイスと他のデバイスを接続する** Microsoft **のシステム。**

冷蔵庫に感染するウイルス？

近い将来、赤外線リンクや低電波を使って、多様なデバイスが交信し合うようになると考えられますが、それによって、新たなセキュリティリスクが生まれると予想されます。

Bluetooth は、10メートルなどの非常に短い距離で、データ通信を行う際に使用する低電波の標準です。コンピュータ、携帯電話、FAX、また、ビデオ、冷蔵庫などの家電製品でさえも、Bluetooth を使って、近くにあるデバイスが提供するサービスを調べ、自動的にリンクすることができます。

Bluetooth を使用するソフトウェアは既に登場しており、Sun の Jini 技術は、デバイスが互いに接続し、自動的に Java コードを交換して、サービスをリモートコントロールすることを可能にします。ここでのリスクは、未許可のユーザーや悪質なコードが、Bluetooth を使用してサービスを妨害することです。

Bluetooth や Jini は、既知の発信元からの信頼できるコードのみが、セキュリティに関する操作を実行できるように作成されています。このため、大規模なウイルス感染が起こることはないと思われますが、万一ウイルスがセキュリティを回避した場合、阻止されることなく感染を広げて行くと考えられます。

用語ミニガイド

3G	第3世代移動体テクノロジー。
Bluetooth	短域無線データ通信。
Jini	デバイス間で、Java コードの自動交換を可能にする技術。
MExE	Mobile station application Execution Environment：WAP の後を継ぐと予想されるもので、サービスプロバイダは、ユーザーの携帯電話に Java コードをダウンロードできる。

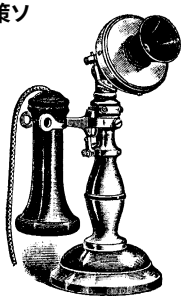
携帯型デバイスの保護方法

携帯電話や PDA の技術が発達するにつれ、セキュリティ対策も変更を迫られることになります。主な問題は、どの地点において、ウイルス対策ソフトを使用するかということです。

ゲートウェイ、またはデータ交換時のウイルス検索

将来的には、携帯型デバイスのデータは、発信・受信する際にチェックすることが最も良い方法であると考えられます。例えば携帯電話の場合、すべての情報は、解読された形で WAP ゲートウェイを通過するので、ここにウイルス対策ソフトをインストールするのは理想的です。

パームトップの場合、従来型 PC とデータの同期を図る際に、ウイルス対策ソフトを使用することがふさわしいと考えられます。PC が、ウイルス対策ソフトの主部分を実行すれば、パームトップが高速でないことや、メモリが少ないことは問題になりません。

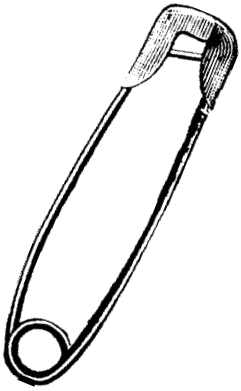


携帯型デバイスでのウイルス検索

携帯電話が互いに連結されるにつれ、中枢点において、データ交換を取り締まるのは困難になって行きます。解決策として、将来、携帯電話の処理能力が向上し、メモリ容量が増えた時点で、ウイルス対策ソフトを各デバイスにインストールすることが考えられます。

安全対策10ステップ

ウイルス対策ソフトを使用する以外にも、家庭や職場の PC をウイルスから保護する簡単な方法は多数あります。ここでは、安全対策のトップ10をあげてみました。



安全対策

.doc、.xls 形式の文書ファイルを使用しない

Word 文書をリッチテキスト形式 (RTF) で保存し、Excel スプレッドシートをカンマ区切り (CSV) ファイルとして保存してください。これらのファイル形式は、マクロをサポートしないので、最も一般的なウイルスであるマクロウイルス感染の恐れがなくなります。まわりの人にも、RTF や CSV でファイルを送信するよう頼みましょう。マクロウイルスの中には、「FileSaveAs RTF」に割り込んで、ファイルを、拡張子が RTF の DOC ファイルとして保存するものがあるので注意が必要です。なお、テキストファイルを使用すれば、安全が保証されます。

要求なしで送信されたプログラムや文書を起動しない

アイテムが、ウイルス未感染か確かでない場合は、感染しているものとして扱いましょう。スクリーンセーバーやジョークプログラムなどの、未許可のプログラムや文書ファイルを、インターネットからダウンロードしないということを社内で徹底させてください。また、すべてのプログラムは、使用前に、IT 責任者が認可し、ウイルス対策ソフトで検索しなければならないという方針を立ててください。

ウイルス警告は担当者1人にのみ転送する

デマウイルスはウイルスと同様、大きな問題を引き起こします。各ユーザーが、友達や同僚、アドレス帳内のすべての人にウイルス警告を転送しないよう徹底し、警告は、担当者1 人、または担当部門1 ヵ所に転送するという方針を社内で立ててください。

安全対策

必要ない場合は WSH を無効にする

Windows Scripting Host (WSH) は、Windows マシンで一部のタスクを自動化しますが、「ラブレター」ウイルスや *Kakworm* のような Email 送信型ウイルスに感染する危険を招きます。必要ない場合は、無効にしてください。詳細は、www.sophos.com/support/faqs/wsh.html を参照してください。

各ソフトウェア会社のセキュリティサイトを参照する

セキュリティに関する情報を入手し、新種ウイルスに対抗するためのパッチをダウンロードしてください。「知っておきたいリンク先」を参照してください。

望ましくないファイルをメールゲートウェイで阻止する

現在、VBS (Visual Basic Script) や Windows スクラップオブジェクトファイル（.SHS ファイル）を使って感染を広げるウイルスは多数あります。外部からこの種のファイルを入手する必要があることは稀なので、ゲートウェイで阻止するようにしてください。

マシンのブートシークェンスを変える

たいていのコンピュータは、まずフロッピーディスクドライブ（A：ドライブ）からブートしようとするので、IT スタッフに相談して、デフォルトでハードディスクからブートするように CMOS 設定を変えてください。これによって、感染したフロッピーディスクがマシンにあっても、ブートセクタ感染型ウイルスに感染することはありません。フロッピーディスクを使ってマシンをブートする必要がある場合は、後日この設定を元に戻すことができます。

安全対策

フロッピーディスクを書き込み禁止にして他人に渡す

書き込み禁止にしたフロッピーディスクにウイルスは感染できません。

Email 警告サービスに登録する

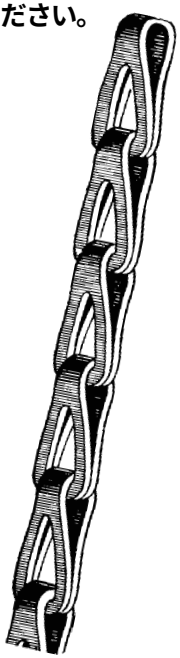
警告サービスに登録すれば、新種ウイルスに関する警告や、それをウイルス対策ソフトで検出するためのウイルス ID を受信することができます。Sophos の無料警告サービスに関しては、www.sophos.com/virusinfo/notifications を参照してください。

すべてのプログラム、データを定期的にバックアップする

これで、ウイルス感染しても、プログラムやデータを回復することができます。

知っておきたいリンク先

詳しい情報は、以下のサイトを参照してください。



ウイルスに関する情報

www.sophos.com/virusinfo/analyses
www.ipa.go.jp/security/virus/search
www.jcsa.or.jp/viruinfo.html

デマウイルスに関する情報

www.sophos.com/virusinfo/hoaxes
www.vmyths.com
www.jcsa.or.jp/hoax2.html

新種ウイルスのメール通知

www.sophos.com/virusinfo/notifications

Microsoft **セキュリティ情報**

www.microsoft.com/japan/technet/security

Netscape **セキュリティノート**

home.netscape.com/ja/security

Java **セキュリティ情報**

java.sun.com/security

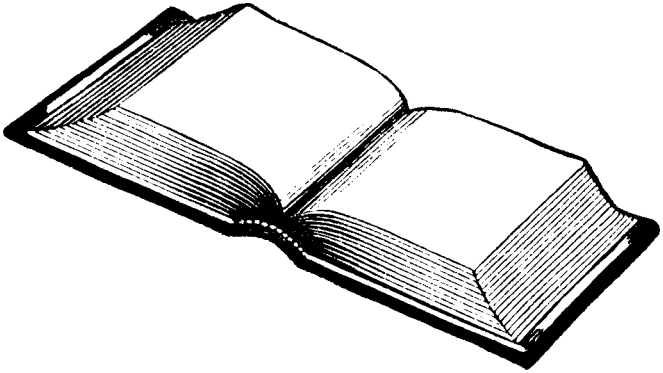
ワイルドリスト

www.wildlist.org

コンピュータウイルス対策技術専門誌『Virus Bulletin』

www.virusbtn.com

用語集



ウイルス

Email

インターネット

携帯型デバイス

安全対策

リファレンス

ActiveX	Microsoft の技術で、Web ブラウザの機能拡張を可能にするもの。
ASCII	American Standard Code for Information Interchange（米国情報交換標準コード）： 文字や記号を表記するための標準システム。
BIOS	Basic Input/Output System：ソフトウェアの最も低いレベルで、ハードウェアに直接接する部分。
CGI	Common Gateway Interface：Web サーバーが、プログラムやスクリプトを実行し、ユーザーの Web ブラウザに出力結果を送るようにするメカニズム。
CSV	Comma Separated Values：Excel スプレッドシートなどからの値が、カンマによって区切られているファイル形式。この形式は、マクロをサポートしないので、マクロウイルスに感染することはない。
DOS ブートセクタ	DOS を PC の RAM にロードするブートセクタ。ブートセクタ感染型ウイルスの感染対象となる。
FTP	File Transfer Protocol：インターネットユーザーがリモートサイトに接続して、ファイルをアップロード、ダウンロードすることを可能にするシステム。
HTML	Hyper-Text Markup Language：WWW 上の大概の文書が持つ形式。
HTTP	Hyper-Text Transfer Protocol：Web サーバーが Web ブラウザに文書を提供するために使用するプロトコル。
Java	Sun Microsystems が開発した、プラットフォームに依存しない Web 用のプログラミング言語。Java で書かれたプログラムは、アプリケーション、あるいはアプレット（小規模のアプリケーション）と呼ばれる。

Java アプリケーション	Java ベースのプログラムで、ディスクにファイルを保存するなど、従来の機能をフルに持ち合わせたもの。
Java アプレット	一般に、Web ページで効果を出すために使用される小規模のアプリケーション。アプレットは、安全な環境（「サンドボックス」を参照）でブラウザによって実行され、ユーザーのシステムに変更を加えることはできない。
OS	ハードウェアリソースの使用を管理し、ファイルの管理、プログラムの実行といった、基本的な管理作業を実行するプログラム。
PC	Personal Computer：デスクトップやポータブルな個人ユーザー用コンピュータ。
PDA	Personal Digital Assistant：アドレス帳やスケジュールなどのデータを管理するために使用される小型のモバイル型コンピュータデバイス。
RAM	Random Access Memory：コンピュータの非持久型メモリ。RAM は、コンピュータのワークスペースとして作動するが、そこに保存されるデータは、マシンの電源を切ると失われる。
ROM	Read Only Memory：コンピュータの持久型メモリの一種。ROM は通常、起動ソフトウェアを保存するために使用される。
RTF	Rich Text Format：マクロをサポートしない文書ファイル形式。マクロウイルス感染の恐れはない。
SHS	Windows スクラップオブジェクトファイルの拡張子。SHS ファイルにはたいていのコードを含めることができ、クリックすると自動的に実行される。拡張子は、隠されている場合がある。

ウイルス

Email

インターネット

携帯型デバイス

安全対策

リファレンス

SMTP	Simple Mail Transport Protocol：**インターネットメール用の転送システム。**
TCP/IP	Transmission Control Protocol/Internet Protocol：**標準的なインターネットプロトコルの総称。**
URL	Uniform Resource Locator：Web **のアドレス。**
VBS	Visual Basic Script：**アプリケーション、文書ファイル、**Web **ページに埋め込まれていて、ページを表示すると即座に実行されるコード。**
WAP	Wireless Application Protocol：**インターネット用のプロトコルで、携帯電話やオーガナイザーに情報を提供するもの。**
Web	**「**WWW**」を参照。**
Web **サーバー**	**インターネットに接続し、一般に、**HTTP **を使用して** Web **コンテンツを提供するコンピュータ。**
Web **ブラウザ**	Web **のクライアント側で、**Web **上の情報にアクセスするために使用されるプログラム。**
WSH	Windows Scripting Host：Windows **マシンで、**VBS **や** Java **スクリプトの実行などのタスクを自動化するユーティリティ。**
WWW	**インターネット上で文書を読むためのハイパーテキストシステム。**
アプレット	**小型のアプリケーション。通常 「**Java **アプレット」を意味する。**
インターネット	**多数のコンピュータネットワークのつながったネットワーク。「インターネット」が群を抜いて規模の大きなものである。**
ウイルス	**他のプログラムに貼り付き、自らのコピーを作成することによって、コンピュータやネットワークを介して広がるプログラム。**

ウイルス ID	**ウイルスの特徴を表現したもので、ウイルス認識のために使用される。**
ウイルススキャナ	**ウイルスを検出するプログラム。たいてい、既知ウイルスを認識する。「ヒューリスティック・スキャナ」を参照。**
クッキー	**ユーザーのマシンに情報を保存する、データの小型パケット。通常、Web サイトがアクセス歴を記録したり、訪問者情報を保存するために使用される。**
クライアントマシン	**しばしば、ネットワークに接続される、シングルユーザー用コンピュータ。**
ゲートウェイ	**データの転送のために使用されるコンピュータ（例：組織内に入ってくる Email の処理するメールゲートウェイ）、あるいは一つのプロトコルから別のプロトコルにデータを変換するコンピュータ。**
コンパニオンウイルス	**同じ名前のプログラムが二つ存在する場合、どちらを先に実行するかを OS は、ファイルの拡張子より決定するという属性を利用するウイルス。例えば、DOS マシンは、.exe ファイルより .com ファイルを先に実行する。コンパニオンウイルスは、.exe ファイルと同じ名前の .com ファイルを作成して、その中にウイルスコードを挿入する。**
サンドボックス	**管理された環境でプログラムを実行するためのメカニズム。特に Java アプレットと共に使用される。**
実行ファイル感染型ウイルス	**「パラセティックウイルス」を参照。**
ステルス型ウイルス	**割り込みサービスを操作することによって、その存在を PC ユーザーやウイルス対策プログラムから隠すウイルス。**
スパム	**要求しないのに送られてくる Email。**

ウイルス

Email

インターネット

携帯型デバイス

安全対策

リファレンス

ダウンロード	コンピュータ、通常サーバーから、別のコンピュータにデータを送信すること。
チェックサム	データに変更が加わっていないことを確認するために、アイテムのデータより算出される値。
デジタル署名	メッセージが変更されておらず、送信元に偽りがないかを保証するための方法。
デマウイルス	存在しないウイルスについての警告。
添付ファイル	文書ファイル、スプレッドシート、グラフィック、プログラムなど、Email メッセージに添付されるファイル。
トロイの木馬	実行されると、仕様にはない、（好ましくない）副作用を起こすコンピュータプログラム。
なりすまし	他人、他のものであるかのように見せかけること。（例：Email の送信元アドレスを偽造。）
ハードディスク	密閉磁気ディスクで、通常コンピュータ内にあり、データの保存に使用される。
パームトップ	手のひら（palm）に収まるぐらい小型のコンピュータ。
ハイパーテキスト	ファイルを広範囲にリンクすることを可能にする、コンピュータが読めるテキスト。
パスワード	システムへのアクセスをユーザーに許可するための文字列。
ハッカー	他人のコンピュータシステムに不正侵入しようとするユーザー。
バックアップ	損失、置き忘れ、破損、削除されたデータを回復するために利用されるコンピュータのデータのコピー。
バックドア	コンピュータシステムの通常のアクセス管理手順を迂回する裏の方法。「バックドア・トロイの木馬」を参照。

バックドア・トロイの木馬	**「トロイの木馬」プログラムで、リモートユーザーに他のマシンへの未許可のアクセス、及び制御を与えるもの。**
パラセティックウイルス	**他のコンピュータプログラムに自らをコピーして感染し、そのプログラムが実行されるとアクティブになるコンピュータウイルス。**
ヒューリスティックスキャナ	**ウイルスの性質や動作に関する一般的ルールからウイルスを検出するプログラム。**
ブート	**初めてコンピュータの電源を入れる際に起こるプロセス。OS のソフトがディスクからロードされる。**
ブートセクタ	**PC の電源を入れた際、ディスクからメモリに最初に読み込まれる OS の部分。その後ブートセクタに保存されているプログラムが実行され、今度はそれが、残りの OS をロードする。**
ブートセクタ感染型ウイルス	**ブート過程を変更するウイルス。**
ファイアウォール	**インターネットと組織のネットワークの間、あるいはネットワーク上に位置し、認可したネットワークトラフィックのみを通過させるセキュリティシステム。**
ファイルサーバー	**中枢データ格納機能を提供するコンピュータで、ネットワーク上のクライアントマシンに他のサービスを提供する場合もある。**
複合感染型ウイルス	**ブートセクタとプログラムファイルの双方に感染するウイルス。**
プロキシ・サーバー	**マシンの代わりにインターネットにリクエストを送るサーバー。企業とインターネットの間に位置し、セキュリティ対策の一環として使用できる。**
プログラム	**コンピュータの動作を特定する、一連の命令文。**

ウイルス

Email

インターネット

携帯型デバイス

安全対策

リファレンス

フロッピーディスク	**データを保存するために使用される入れ替え可能な磁気ディスク。**
ポリモルフィック型ウイルス	**自己修正するウイルス。ウイルスコードを変更することによって、検出が困難になる。**
マクロ	**データファイル内にあって、ファイルを開く、閉じるなどの、プログラムコマンドを自動的に実行する一連の命令。**
マクロウイルス	**データファイル内にあるマクロを使用してアクティブになり、他のデータファイルに自らを貼り付けるウイルス。**
マスターブートレコード	**バーティションセクタとも言われる。**PC **がブートされる際にロード、実行されるハードディスクの第一物理セクタ。起動コードの中で最も重要な部分。**
モデム	MOdulator/DEModulator **は、コンピュータデータを、電話線、無線チャンネル、衛星リンクなどを使った送信にふさわしい形に置き換える。**
モバイル PC	**ラップトップよりも小型のコンピュータ。**
ラップトップ	**ひざ（lap）の上に乗せて使えるほど小型の携帯型** PC**。**
リンクウイルス	**ディレクトリエントリを破壊してウイルスコードを指定し、それを実行するウイルス。**
ワーム	**自分自身のコピーをいくつも配布するプログラム。ウイルスと異なり、ワームは、「ホスト」プログラムを必要としない。**

索引

ウ

オ

ク

ケ

コ

サ

シ

ス

タ

チ

テ

ト

ナ

ハ

ヒ

フ

ホ

マ

モ

ラ

リ

ワ

ウイルスの一覧

デザイン・編集 Paul Oldfield
訳 **マギル香子**

ご連絡先 sales@sophos.co.jp
Web www.sophos.co.jp