4.2 マルウェア

マルウェアとは、制作者や配布者が悪意を込めたソフトウェアの総称です。ここでは、マルウェアの代表例とその対策について説明します。

4.2.1 ウイルス

■ ウイルスとは

コンピューターウイルスは、システムの正常な状態や運用に対し、何らかの悪影響を及ぼすことを目的として作成されたプログラムです。実際のウイルスが人間に感染して増殖するのと同じような行動をとるため、ウイルスと名付けられています。

平成 12 年 12 月 28 日（通商産業省告示 第 952 号）（最終改定）によって、以下のように定義されています。

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 1 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

ウイルスに感染し発病すると、パソコンが通常通りに動かなくなったり、パソコン内部のデータを勝手に送信したりします。しかし、たとえ発病機能のないウイルスであっても、被害は発生します。

たとえば、ウイルスがネットワークを介して増殖していくことで、ネットワークの負荷が高まってしまうことがあります。そして、ウイルスに感染すれば、ウイルスを駆除するために多くの

費用や人的負担が発生します。さらに、企業がウイルスの感染源となってしまうと、その企業の社会的信用が失われる可能性があります。

広い意味でのコンピューターウイルスは大きく3つに分類されますが、最近では、1つのウイルスが複数の特性を持つ複合型ウイルスが多く、単純に分類できない場合が増えています。

表 4-1 コンピューターウイルスの分類

分類	ファイルへの感染	自己増殖機能
（狭義の）ウイルス	あり	なし
ワーム	なし	あり
トロイの木馬	なし	なし

■ プログラム感染型ウイルス、ファイル感染型ウイルス

初期のウイルスは、他のプログラムに感染して活動を行うタイプでした。感染対象は、プログラムとして実行可能な形式のファイルに限られていました。そのため、プログラム感染型ウイルスやファイル感染型ウイルスと呼ばれていました。

日本で最初にウイルスが流行したのは、インターネットが普及する以前、1980年代後半です。当時はパソコン通信と呼ばれるネットワークサービスが広く使われていました。多くのフリーソフトやシェアウェアがダウンロードサービスで流通したため、ウイルスは、それらのフリーソフトやシェアウェアを介して流行しました。

■ ブートセクター感染型ウイルス

ブートセクターとは、ハードディスクやフロッピーディスクからOSを起動するときに使う特別な領域です。ブートセクター感染型ウイルスはこの領域に感染するタイプのウイルスです。このウイルスに感染すると、フロッピーディスクやハードディスクが使えなくなることがありました。

以前はフロッピーディスクを介して他のパソコンに感染が拡大していましたが、近年ではフロッピーディスクの利用が少なくなったため、ブートセクター感染型ウイルスは減少しています。

■ マクロウイルス

マクロとは、表計算ソフトやワープロソフトなどのアプリケーションソフトにおいて、処理を

NOTE

シェアウェア：無料の試用期間が設定されていて、試用期間を過ぎても継続して使う場合に代金を払う形態で配布されているソフトウェア。

自動化するための仕組みです。マクロはアプリケーションソフトのデータの一部として保存されるため、このタイプのウイルスはデータに感染していきます。マクロウイルスの出現により、ウイルスを監視しなくてはならない範囲が、プログラムファイルだけでなくデータファイルにまで拡大しました。

■ ワーム

他のファイルなどに寄生せずに、単独のプログラムとして活動するするものを、従来のウイルスと区別して「ワーム」と呼びます。2017 年には、感染したコンピューターのファイルを暗号化して利用を制限し、制限解除のための身代金を請求するランサムウェア「WannaCry」が話題になりました。

この「WannaCry」はワーム型ランサムウェアであり、ネットワーク経由で Microsoft Windows の脆弱性を利用して感染を広げていきます。

その他にも電子メールのアドレス帳に登録されているユーザーや、受信箱に入っているメールの送信者宛にワーム自身を添付した電子メールを送信し、拡散、増殖するものなど、様々な種類があります。

■ トロイの木馬

自らを有用なソフトウェアに見せかけて、実行したとたんに感染するタイプのウイルスもあります。これは「トロイの木馬」と呼ばれます。トロイの木馬には、感染してから時間をおいて活動を始めるものがあります。この様子が、ギリシャ神話のトロイア戦争に登場する木馬に似ているので、「トロイの木馬」と呼ばれます。

トロイの木馬の中には、ランサムウェアと呼ばれる悪質なタイプがあります。ランサムウェアは、感染したパソコンを人質にとって身の代金を要求するウイルスです。

たとえば、ある特定のフォルダーを暗号化しパスワードをかけてしまいます。データを元に戻すためのパスワードを提供するための交換条件として、特定の商品の購入や特定サービスの契約を強要します。

コラム：CPU の脆弱性

2017 年末に、現在様々な機器で使用されている、ほぼ全ての CPU に影響を与え得る「メルトダウン」や「スペクター」と呼ばれる脆弱性が公表され激震が走りました。これは、OS やアプリケーションなどのソフトウェアを動かす際に使用されている CPU の保護機能に関する脆弱性です。この脆弱性が脅かされると OS やアプリケーションの間で働いていた保護機能が働かなくなり、OS やアプリケーション内の情報が改ざん、詐取されるという危険性があります。OS やアプリケーションのアップデートだけでは対応できない部分もあるため、各社が対応に追われることになりました。

■ Web サイトから感染

Web ブラウザーでアクセスするだけで、ランサムウェアなどのウイルスに感染する悪意を持つサイトもあります。また、エクスプロイトキット（exploit kit）と呼ばれる、脆弱性攻撃ツールキットを使用して感染させる攻撃もあります。見ただけで感染してしまう攻撃への対策としては、事前に攻撃される脆弱性を無くしておくことが重要です。OS や Web ブラウザー、Java など、インターネット接続に関わるソフトウェアを最新のものにアップデートしておく必要があります。

■ 検出を妨害するウイルス

ウイルス対策ソフトが普及すると、検出を妨害する機能を持つウイルスが登場しました。

検出を妨害するウイルスには、ウイルス自身を暗号化するタイプがあります。これは、ステルス型と呼ばれることがあります。また、ウイルス自身を自動的に変形させるタイプがあります。いずれも、ウイルス対策ソフトが持つウイルス情報との比較を妨げることにより、検出を妨害しています。

また、ウイルスが検出された後の対処を妨げるウイルスもあります。その機能の一例は、ウイルスに関する情報が豊富に掲載され、感染時の対処方法が掲載されている、ウイルス対策ソフト製造元の Web サイトへのアクセスを妨害するものです。

これらの Web サイトが閲覧できなくなると、対処方法に関する情報入手が難しくなります。

■ 暴露型ウイルス

ファイル交換ソフトの普及により登場したウイルスです。ファイル交換ソフトとは、不特定多数のコンピューターの間でファイルを共有するソフトウェアで Winny や Share などがあります。暴露型ウイルスは、これらのファイル交換ソフトを標的にします。暴露型ウイルスは、感染したパソコンのデータだけでなく、そのパソコンから利用できるデータすべてを送信の対象とするも

のもあります。たとえば、ファイルサーバーを利用している環境でパソコンが感染すると、ファイルサーバー内のデータまでもが送信されてしまいます。暴露型ウイルスによって、多くの個人情報漏えい事件が引き起こされ、企業や組織の信用を失墜させました。そのため、多くの企業や組織では、暴露型ウイルスによる被害を防ぐために、ファイル交換ソフトの利用が禁じられています。

4.2.2 スパイウェア

■ スパイウェアとは

スパイウェアとは、利用者が意図しないところでコンピューターに潜り込んでコンピューター内部の情報を収集し、外部に送信するソフトウェアの総称です。

■ キーロガー

キーロガーは、利用者のキー操作の履歴をすべて記録するソフトウェアです。

キーロガーの特徴は、キー操作そのものを記録するため、画面に表示されていない操作でも、すべて記録に残ってしまう点です。そのため、ブラウザーには「******」と表示されるパスワードも、キーロガーの記録を見ればすべて判明してしまいます。

2017 年 12 月にはあるメーカーのパソコン用のドライバーソフトウェアにキーロガーのコードが含まれていた事が発覚し、ドライバーアップデートで対応したという事件も発生しました。

■ アドウェア

アドウェアのアドとは、広告の意味です。アドウェアは、特定のサイトを閲覧した際にインストールされ、ブラウザーの利用時に広告を定期的に表示するものです。ただし、アドウェアは不正なものばかりとは限りません。それは、利用者の承諾の元に、特定のサービスや特定のソフトウェアを無料で利用するための交換条件として、アドウェアがインストールされる場合もあるためです。

問題となるアドウェアは、利用者の承諾なしにインストールされるタイプです。これらの悪質なアドウェアはマルウェアの一種として分類されます。

4.2.3 ボット

■ ボットとは

ボットとは、ロボットの意味です。マルウェアのボットは、ウイルスとして対象のパソコンに

送り込まれます。ボットに感染したパソコンは、「ゾンビコンピューター」または「ゾンビ」と呼ばれます。ゾンビコンピューターは、悪意の者からの指令により、他のコンピューターへの攻撃を行ったり迷惑メールの送信を行ったりします。感染したパソコンが直接的な被害を受けることはほとんどありません。被害の発生が少ないので、利用者は感染に気づきにくいのが特徴です。

■ ボットネット

ボットに感染したゾンビコンピューターは、集団で活動することにより、悪意のある者がより悪質な活動を行えるようになります。この集団を「ボットネット」と呼びます。たとえば、他のコンピューターへの攻撃ならば、一度に多数のコンピューターから一斉に攻撃することにより、攻撃が防ぎにくくなります。迷惑メールの送信でも、送信できるコンピューターが多ければ、より大量のメールを送信しやすくなります。

インターネット上では、小規模のボットネットが多数存在していると考えられています。

4.2.4 マルウェア対策

■ 対策の考え方

マルウェア対策に限ったことではありませんが、被害を小さくするためには、事前の対策と事後の対策の２つが両輪となって、はじめて対策として機能します。ウイルスを例にすれば、ウイルスに感染する危険性を減らす対策は不可欠ですが、その可能性をゼロにすることは不可能です。したがって、ウイルス感染はあり得ることとして、被害を受けることを前提とした対策が必要となります。

これは、火の用心と消火の関係に似ています。どんなに火の用心をしても、火事を無くすことはできません。だから消火が必要です。しかし、どんなに優れた消火設備があっても、火事の被害をゼロにすることはできません。被害を減らすためには、火事を起こさないための用心が必須です。

■ セキュリティ対策ソフトの利用

パソコンにはセキュリティ対策ソフトは欠かせません。統合型のセキュリティ対策ソフトと呼ばれるものがあり、マルウェア対策、ファイアウォール機能、フィッシング対策機能など必要な機能を一通り実装しています。代表的なソフトに Symantec 社のノートンインターネットセキュリティーや、Trend Micro 社のウイルスバスターシリーズなどがあります。

セキュリティ対策ソフトには、「リアルタイム検索」や「リアルタイムスキャン」などと呼ばれる機能があり、ファイルの書き込みやメールの送受信、インスタントメッセンジャーなどによる通信を常に監視しています。ウイルスか否かは、パターンファイルと呼ばれるウイルス定義ファイルと比較することで判断しています。しかし、新しいウイルスはパターンファイルに載っていないので、ウイルスとして認識できません。したがってセキュリティ対策ソフトをアップデートし、パターンファイルを最新にしておくことが必須です。

パターンファイルを更新するタイミングより、新しいマルウェアの侵入が早い場合には検出することができません。

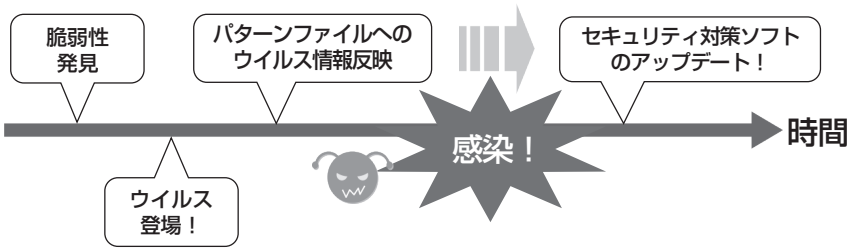


図 4-1 セキュリティ対策ソフトのアップデート前に感染する流れ

この場合、セキュリティ対策ソフトはマルウェアの侵入を検出できません。このような場合を想定して、定期的にパソコン全体をチェックする必要があります。これを「フルスキャン」などと呼びます。また、パターンファイルに載っていないウイルスを検出する方法には「ヒューリスティックスキャン」もあります。これは、プログラムの不審な挙動自体を監視することで、未知のウイルスを検出する方法です。

上記のリアルタイム検索やフルスキャン、ヒューリスティックスキャンは、マルウェア自体を検出するための監視ですが、セキュリティ対策ソフトの中には、マルウェアそのものを検出できなかった場合に備えて、マルウェアの活動を監視するものがあります。

たとえば、スパイウェアには、パソコンが起動されるたびに自分が起動されるように、スパイウェア自身をスタートアップメニューに登録するものや、他のソフトウェアの設定を書き換えるタイプがあります。セキュリティ対策ソフトは、これらの不正なシステム変更を常時監視し、変更を防止する手助けをするので、ウイルスやスパイウェアの侵入を許してしまっても被害の発生を抑えることができます。

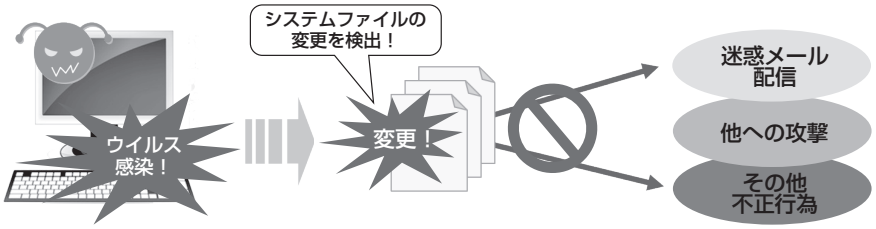


図 4-2 システムファイルの変更防止

ただし、この機能は、正常なシステム変更も検知してしまうことがあります。たとえば、アプリケーションソフトのインストールの際に、セキュリティ対策ソフトがシステム変更を拒否すると、インストールに失敗してしまいます。そのため、インストール作業を行う場合は、一時的にセキュリティ対策ソフトを終了させるなどして、システム変更を監視する機能を無効にする必要があります。ただし、セキュリティ対策ソフトを無効にしている間は、外部からの攻撃に対して無防備な状態です。ネットワークケーブルをはずして、インターネットに接続していない状態で作業するなどの注意が必要です。

■ パーソナルファイアウォールの利用

ファイアウォール（防火壁）とは、外部ネットワークと内部ネットワークの間でやり取りしているデータを監視し不正な通信を排除するハードウェアです。通常は、インターネットからLANへの不正アクセスを防ぐために設置します。

パーソナルファイアウォールとは、ファイアウォール機能をソフトウェアで実現するもので、パソコンにインストールして使います。パーソナルファイアウォールを用いると、外部に通信できるプログラムを利用者側で制限できます。たとえば、メールやブラウザーなど、普段インターネットを利用するソフトウェアの通信のみを許可する設定にして使用します。こうすることで、ウイルスなど利用者が許可していないプログラムが勝手に外部と通信しようとすると、パーソナルファイアウォールが通信を検出し、すぐさま通信を遮断します。ウイルスの伝染活動や、スパイウェアによる外部への情報漏えいなどが発生しないので、被害の拡大を食い止めることができます。

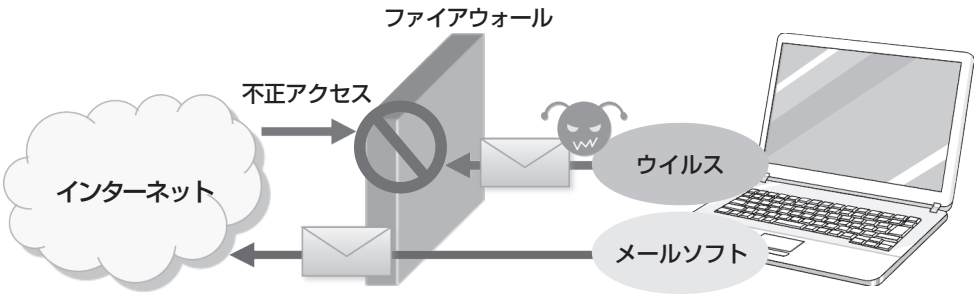


図 4-3 パーソナルファイアウォールの機能

■ OS やアプリケーションのアップデート

アップデートが必要なのは、セキュリティ対策ソフトだけではありません。OS や、ブラウザー、Adobe Reader などのアプリケーションソフトもアップデートが必要です。

これらのソフトウェアには、セキュリティホールと呼ばれる脆弱性が発見されることがあります。ウイルスの中には、これらの脆弱性を悪用するものがあります。したがって、マルウェアの被害を受けないようにするには、OS やアプリケーションソフトのセキュリティホールを塞ぐためのアップデートが不可欠になります。

■ Web サイトの利用制限

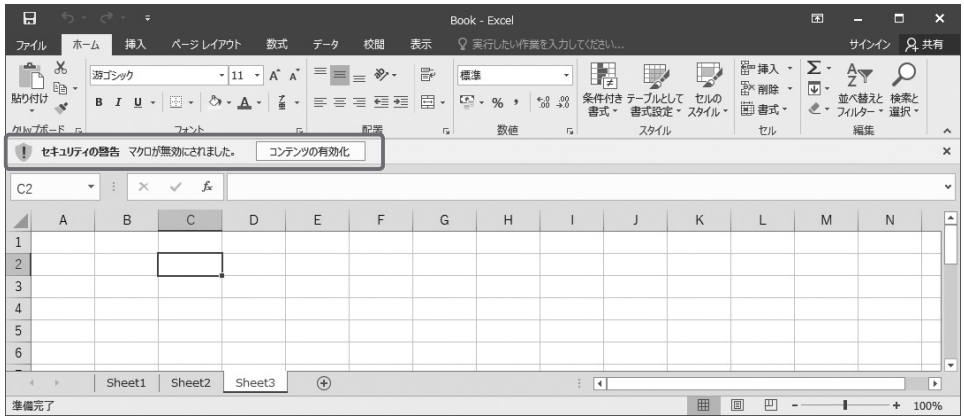
マルウェア対策のひとつは、信頼できない Web サイトにアクセスしたり、ファイルのダウンロードをしたりしないことです。

悪意のある者は、懸賞や無料のコンテンツなどさまざまな手段で自分のサイトに利用者を誘導します。そして、その Web サイトを閲覧するだけで、ウイルスに感染したり、スパイウェアを送り込まれたりします。信頼できないサイトは、見ないようにすることが肝要です。

また、セキュリティ対策ソフトの中には、ブラックリストに載っているサイトへのアクセスを遮断する機能を持つものもありますので、このような機能を利用することも有効です。

■ マクロの利用制限

マクロウイルス対策として、Excel や Word では、マクロを含むデータを開く場合は、マクロを有効にするか無効にするかの確認を行います。マクロ機能を無効にすることによりマクロウイルスの活動を制限できます。



画像 4-1 マクロ機能の有効 / 無効を設定する画面

自分の作ったマクロなど安全性が確認できるファイル以外でマクロを利用しなくてはならない場合は、ウイルス対策ソフトを最新の状態にアップデートした上でファイルのウイルス検査を行い、その後、マクロを有効にしてファイルを開きます。

4.2.5 マルウェアに感染した場合

今まで述べたようなセキュリティ対策は必須ですが、それでもマルウェアに感染してしまった場合は、まず被害の拡大を防ぐことを第一に考え、感染したパソコンを使用しないようにします。もし、マルウェアに感染したメールが送信されている痕跡があれば、電話やファックスなど、マルウェアに感染したパソコンを利用する以外の方法で、送信先にその旨を連絡し相手が感染しないようにします。

そして、感染したパソコンでセキュリティ対策ソフトのアップデートを行った上で、フルスキャンを行います。セキュリティ対策ソフトが対応していれば、駆除や隔離を行うことができます。

アップデートのタイミングが悪く、セキュリティ対策ソフトが対応していない場合は、マルウェアへの対処を個別に行わなければなりません。しかし、安易な対処は別のトラブルを引き起こします。たとえば、迂闊にファイルの削除を行うと、OS が起動しなくなることもあります。セキュリティ対策ソフトで対処できない場合は、専門家に対処を依頼します。

IPA（情報処理推進機構）では、情報セキュリティに関して相談窓口を設けています。

情報セキュリティ安心相談窓口（https://www.ipa.go.jp/security/anshin/）

・電話：03-5978-7509（2020 年 1 月現在）
受付時間：平日 10:00 ～ 12:00 13:30 ～ 17:00

・メール：anshin@ipa.go.jp

NOTE

IPA：独立行政法人 情報処理推進機構（Information-technology Promotion Agency, Japan）