マルウェアの種類

マルウェアとは、不正かつ有害な動作を行う意図で作成された悪意のあるソフトウェアや悪質なコードの総称です。

悪意のあるソフトウェアはコンピュータウイルスと呼ばれていたことがありますが、その挙動がウイルスのように感染し、有害な動作をすることだけではないため、「悪意のある」という意味の英語「malicious（マリシャス)」と「software（ソフトウェア)」を組み合わせて創られた造語「Malwear（マルウェア)」が使われるようになりました。

マルウェアはその挙動などで分類されますが、共有された標準的な分類方法がないため、人により異なります。以下は一つの分類方法で、その特徴、挙動を合わせて表にしてあります。

	マルウェア分類名	特徴・挙動など
1	ウイルス	他のプログラムに寄生して、そのプログラムの動作を妨げたり、ユーザの意図に反する、有害な作用を及ぼすためのプログラムで、感染機能や自己拡散機能を持っています。 現在はマルウェアの中で純粋のウイルスは１０％程度になっています。 ウイルス単体の駆除は難しいため、多くの対策ソフトは感染したファイルを隔離・削除することで対応しています。
2	ワーム	独立のファイルで、誰かが操作することなく他のプログラムの動作を妨げたり、ユーザの意図に反する、有害な作用を及ぼすためのプログラムで、自己感染能力や自己拡散能力を持っています。 その歴史はウイルスより古いです。
3	トロイの木馬	攻撃者の意図する動作をリモートから侵入先のコンピュータで秘密裏に行うプログラムです。 ギリシア神話におけるトロイア戦争のストーリーにあるトロイの木馬になぞらえて名前を付けられています。 トロイの木馬は、メール添付を開いたり感染したWebサイトを閲覧したりウイルス対策ソフトに見せかけた偽プログラムをインストールしたりしたときに入り込みます。 これもその歴史はウイルスより古いです。 さまざまなキットや既製のツールを闇市場で手に入れて使うことができるため他のマルウェアを送り込むために広く使われています。

4	ハイブリッド型	いくつかの種類の不正プログラムの性質を併せ持つものをいいます。現在のマルウェアはほとんどがハイブリット型です。
5	ランサムウエア	感染先のパソコンのデータを暗号化して「人質」にとり、暗号資産（仮想通貨）で「身代金」を支払うよう要求するマルウエアです。企業、病院、警察、自治体で被害が発生していることが報道されています。
6	スパイウェア	他のマルウェアと同じように、ユーザーが明白に気付くことなくバッチを適用していないソフトウェアなどで侵入される。標的となったデバイスのあらゆる通信をモニタリングすることができ個人情報や、インターネットの閲覧データ、その他の詳細情報を取得し、犯罪者に送ります。
7	ファイルレスマルウエア	実行や常駐の方法で見た区分の１つ。ファイルやファイルシステムを直接的には使わず、メモリー上のみの処理で攻撃や拡散を行ったり、レジストリーキー、API、スケジュールタスクなど、OS が備えるファイル以外の部分を利用したりしています。ファイルを使用せず、痕跡も残さないため、検知や除去が難しくなっています。
8	スケアウェア	典型的な例では、インターネットを閲覧中に、「警告: コンピューターがウイルスに感染しました！」や「ウイルスを検知しました！」などの警告メッセージを表示します。犯罪者は、これらのプログラムや不適切な広告手段でユーザーを脅し、偽装アプリケーションを購入させます。
9	アドウェア	多くの場合、無料でプログラムを使用できる権利など、別のサービスと引き換えに、点滅広告やポップアップウィンドウを表示させます。
１０	ボット	「ロボット」の略で、人の代わりに自動実行するプログラムの総称。マルウェアの一種として悪意ある攻撃者による指令を、外部から自由に実行できるようにするプログラムです。グーグルなどのサーチエンジンのデータベースを作成する専用ソフトウエアであるサーチボットもあります。

マルウェアに感染したときの症状

パソコンがマルウェアに感染した場合の一般的な症状です。

１．パフォーマンスの低下（遅くなった）

2．ブラウザーが意図していないサイトに移動する（偽サイトが多い）
3．ウイルス感染に関する警告が、たいていは問題解決のため何かを購入するよう促すメッセージを伴って表示される
4．コンピューターが勝手にシャットダウンまたは起動する
5．ポップアップ広告が大量に表示される

マルウェアの対策方法

パソコンを守る

1．オペレーティングシステムとアプリのアップデートが入手可能になったら、すぐにインストールし最新状態に保ちます。
2．ポップアップのリンクを絶対にクリックしない。右上の［X］をクリックしてメッセージを閉じ、そのメッセージを出したサイトを閉じましょう。
3．パソコンにインストールするアプリの数を絞りましょう。必要なアプリや定期的に使用するアプリのみにしてください。不要になったアプリは、すぐにアンインストールしてください。アプリの入手先は信頼できるところだけにしましょう。
4．できるだけパソコンを他人に貸さない。
5．できれば設定やアプリを定期的に確認しましょう。自ら変更した設定以外が変更されている場合、あるいは、知らぬ間に新たなアプリが表示されている場合は、スパイウェアがインストールされているかもしれません。

オンライン上では警戒を怠らない

1．不明なリンクをクリックしないようにしましょう。メール、SNS、テキストメッセージを問わず、見知らぬリンクをクリックしないようにしましょう。
2．できる限り、既知の信頼できるサイトのみ使用しましょう。
3．個人情報をやパスワードを要求するメールには気を付けましょう。銀行から送信されたらしきメールが来て、リンクをクリックしてパスワードのリセットやアカウントへの接続などをするよう指示されたとしても、絶対にクリックしないでください。直接その銀行のサイトに移動し、そこでログインしてください。

ダウンロード版などソフトウェアの購入には注意する

1．セキュリティソフトは有名な企業のもののみに使用しましょう。
現在の Windows10 では標準の Windows セキュリティで十分です。
2．友人や知人から届いた場合でも、中身の分からないメールに添付されたファイルを開かない。

定期的にチェックする

1．パソコンが侵害されたかもしれないと思った時は、パソコンにインストールされたセキュリティソフトを使ってスキャンしてください。
2．定期的に銀行口座やクレジットカードの明細を確認しましょう。