コンピュータウイルスとウイルス攻撃の種類

The type of computer virus attacks and computer viruses.

マルウェア【 malware 】

コンピュータウイルス、ワーム、スパイウェアなどの「悪意のこもった」ソフトウェア。
遠隔地のコンピュータに侵入し攻撃したりするソフトウェア、またコンピュータウイルスのようにコンピュータに侵入して他のコンピュータへの感染活動や破壊活動を行ったり、情報を外部に漏洩させたりする有害なソフトウェア。

広義のコンピュータウイルス【 computer virus 】

キーロガー【 key logger 】

情報収集専用の文字通りスパイを行う専用のスパイウエアソフト。キーボード入力を監視して記録する。
常駐型のソフトとして別のソフトの使用中に透過的に動作するようになっており、複数の人間が利用するパソコンにこっそり仕掛けてパスワードやクレジットカード番号などを収集する。
実際、インターネットカフェでパスワードが盗まれ、現金が引き出されるといった被害が発生。

アドウェア【 adware 】

画面に強制的に広告を表示させる代わりに、無料で利用できるソフトウェア。
コンピュータの環境や Web ブラウザのアクセス履歴などの情報を自社や顧客企業に通知し、その結果を元に表示させる広告内容設定などに用いる機能を持つものもある。こうしたソフトウェアは「スパイウェア」とも呼ばれる。

スパイウェア【 spyware 】

パソコンを使うユーザの行動や個人情報などを収集したり、マイクロプロセッサの空き時間を借用して計算を行ったりするアプリケーションソフト。
他のアプリケーションとセットで配布され、インストール時にはそのソフトと一括して利用条件の承諾などを求められる。また、ユーザに気づかれないよう、ウィンドウなどを出さずにバックグラウンドで動作するため、ユーザはインストールされていることに気づきにくい。

コンピュータウイルス【 computer virus 】

他人のコンピュータに入り込み悪さをするプログラム。画面表示をでたらめにしたり、無意味な単語を表示したり、ディスクに保存されているファイルを破壊する。
インターネットからダウンロードしたファイルや、他人から借りたフロッピーディスクなどを通じて感染。e-mail を介して感染するタイプのウイルス (ワーム) も存在。

発病機能　自己伝染機能

マクロウイルス【 macro virus 】

Microsoft Office などのアプリケーションソフトに埋め込まれて実行される「マクロ」と呼ばれる簡易プログラムを悪用したコンピュータウイルス。
ファイルに感染し、自己増殖や破壊活動を行う。
マクロウイルスは通常の文書ファイルに感染するため、企業活動などを通じて交換されやすい。電子メールに添付されて拡散することもある。

自己伝染機能　発病機能

ボット【 bot 】

ボット型ウィルス【bot-virus】

感染したマシンを乗っ取りボット化するタイプのコンピュータウィルスのこと。
ボット型ウィルスに侵入されると、自分のマシンは悪意の第三者によって操作されるボット（ゾンビマシン / 踏み台）となり、DDoS などの外部攻撃やスパムメールの送信などを行うためのマシンとして利用される。

発病機能

ワーム【 worm 】

ユーザに気づかれないようにコンピュータに侵入し、破壊活動や別のコンピュータへの侵入などを行う、マルウェアの一種。CD-ROM やフロッピーディスク、電子メール、Web サイトなどを介して増殖。
他のプログラムに寄生するわけではなく単独で活動する点や、スクリプト言語やマクロなどの簡易的な技術で作成される点など、(狭義の) コンピュータウイルスとは区別される。

発病機能

トロイの木馬【 Trojan Horse 】

正体を偽ってコンピュータへ侵入し、データ消去やファイルの外部流出、他のコンピュータの攻撃などの破壊活動を行うプログラム。ウイルスのように他のファイルに寄生したりはせず、**自分自身での増殖活動も行わない**。実行したとたん破壊活動を始めるものもあるが、システムの一部として潜伏し、時間が経ってから「発症」するものや、他のユーザがそのコンピュータを乗っ取るための「窓口」として機能するものなどもある。

潜伏機能　発病機能

デマウイルス【 hoax 】

騒動を起こすために人為的に流されたコンピュータウイルスのデマ情報。また、そうしたデマ情報の中で言及されている実在しないウイルス。
デマウイルス情報によりユーザはありもしないウイルスに対する対処に時間を割かれ、メーリングリスト等にこれらの情報が投稿された場合には無駄にトラフィックが増大するなどの悪影響が及ぶ。

ワンクリック詐欺【 a one click and charge claim 】

不当料金請求の一つで、アダルトサイトや出会い系サイトなどにパソコンや携帯電話からアクセスすると、いきなり料金請求の画面が表示されるという手口。
無差別に大量に送信される勧誘メールなどからサイトにアクセスすると、突然請求画面が表示される。また突然請求画面にならずに次のページへ一段階クリックさせる場合もある。

ソーシャルエンジニアリング【 social engineering 】

ネットワークの管理者や利用者などから、社会的な手段によって、パスワードなどのセキュリティ上重要な情報を入手すること。パスワード入力を盗見やメモごみ、利用者になりすましてパスワードを聞き出すなどの手法がある。ソーシャルエンジニアリングの手法は、メールや SNS などによる「フィッシング」、勧誘などの「電話」、なりすましなどによる「テールゲート」の 3 つに大別される

スパム【 SPAM 】

入手したメールアドレスに、無差別に本人に許諾を得ず、一方的に営利目的の広告メールを配信すること。
受信者に選別・削除作業の負担を強いる一方、送信側は低コストで実行可能なため根強く行われている。
多くはアダルトサイトへの誘導や架空請求、フィッシング詐欺目的であり、金銭トラブルはもちろん、ネットワーク上のトラフィックを食い尽くすとして社会問題化している。

フィッシング【 phishing 】

金融機関などからの正規メールや Web サイトを装い、暗証番号やクレジットカード番号などを詐取する詐欺。メールの送信者名を金融機関の窓口などのアドレスにしたメールを無差別に送りつけ、掲載の URL をクリックさせる。一部、正規の Web サイトを表示させることにより、ユーザを安心させ暗証番号やパスワード、クレジットカード番号などの秘密を入力・送信させ、だまし取る。

ボットネット【 bot net 】

ウイルスなどにより多くのパソコンやサーバに遠隔操作できる攻撃用プログラム (ボット) を送り込み、外部からの指令で一斉に攻撃を行わせるネットワーク。
感染したコンピュータは、他のコンピュータをウイルス感染させたり、キーロガーを仕込んだり、フィッシングサイトを開設したり、迷惑メールを送信したり、DoS 攻撃を行ったりする。感染したコンピュータは、以前通りに利用できるため、感染に気づかない。

DoS 攻撃【 Denlal of Service attack 】

ネットワークを通じた攻撃の一つ。相手のコンピュータやルータなどに不正なデータを送信して使用不能に陥らせたり、トラフィックを増大させて相手のネットワークを麻痺させる攻撃。
IT 資源に対するアクセスができないように妨害したり、遅延させたりするための攻撃のことである。
ネットワークケーブルを切断する、コンピュータを物理的に破壊することもこの攻撃の一種である。

バッファオーバーフロー【 buffer over-flow 】

アプリケーションソフトに共通する代表的なセキュリティホールの一つ。また、それを悪用して遠隔地からコンピュータを乗っ取ること。プログラムでは、確保したメモリサイズを越えて文字列が入力されると領域があふれて (オーバーフロー) しまい、予期しない動作が起きる。成功するとプログラムが持っているアクセス権の範囲で任意の動作を行うことが可能となる。

セキュリティホール【 security hole 】

設計ミスなどによって生じた、システムのセキュリティ上の弱点。放置しておくと不正にコンピュータを操作されてしまう可能性がある。また攻撃を受けると、Web サーバで公開されている情報が改ざんされたり、機密データが漏洩したり、他のコンピュータへ不正アクセスするための踏み台に利用されたりする。
ワームがコンピュータに感染する糸口としてセキュリティホールを使うケースが急増している。

ドライブ・バイ・ダウンロード【 drive-by download attack 】

スパイウェアやマルウェア、コンピュータウィルスなどの悪意のあるツールや悪意のあるアプリケーションを秘密裏にダウンロードさせるために用いられる。
ユーザが Web サイトを閲覧しただけで自動的にダウンロードされてしまうため、ユーザは気づくことができない。主にウェブブラウザ、OS やその他のサードパーティー製のソフトウェアの脆弱性やセキュリティーホールを突くようにして行われる。

ゼロデイ攻撃【 zero-day attack 】

ソフトウェアにセキュリティ上の脆弱性 (セキュリティホール) が発見されたときに、問題の存在自体が広く公表される前にその脆弱性を悪用して行われる攻撃。コンピュータシステムを外部からの攻撃から守るには、メーカーや開発者が公開するパッチを、公開後即座に適用するのが基本だが、ゼロデイアタックの場合は対応策が公表される前に攻撃が行われるため、このような対策では防ぎきれない。

バックドア【 backdoor 】

コンピュータへの侵入に成功すると、次回も侵入できるようにこっそりと侵入経路を確保 (設置) すること。設置されると、管理者が不正侵入に気づいて侵入路をふさいでも、前回侵入時に設置したバックドアから再び不正侵入が可能。他のコンピュータへの攻撃の踏み台として利用されてしまうことも多い。
トロイの木馬やコンピュータワームの中には、感染するとバックドアの設置を行うタイプのものがある。

ランサムウェア【 ransomware 】

マルウェアの一種で、ユーザーのデータを「人質」にとり、データの回復のために「身代金」（ransom）を要求するソフトウェア。トロイの木馬として PC 内に侵入し、正常にデータにアクセスできないようにし、正常にアクセスできるよう復元するための対価として、ユーザーに金銭を支払うように要求する。要求に応じなければ、一定時間が過ぎるごとにファイルを削除していくと脅迫するものもある。

DDoS【 Distributed Denlal of Service 】

複数のネットワークに分散する大量のコンピュータが一斉に特定のサーバへパケットを送出し、通信路をあふれさせて機能を停止させてしまう攻撃。
悪意ある第三者が、無関係な多数のコンピュータに侵入し、気づかれないようにプログラム (トロイの木馬) をしかけ、コンピュータを操るため「踏み台攻撃」ともいう。攻撃された側は真の攻撃元であるコンピュータを割り出すことは難しい。