脆弱性
コンピュータやソフトウェア、ネットワークなどが抱える保安上の弱点。正規の管理者や利用者など以外の第三者が保安上の脅威となる行為（システムの乗っ取りや機密情報の漏洩など）に利用できる可能性のある欠陥や仕様上の問題点のこと。

セキュリティホール
ソフトウェアの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。

不正アクセス
そのコンピュータに対してアクセス権を持たない人が不正に権限を取得し、アクセスを試みること。実際にアクセスすることも含みます。代表的な不正アクセスに、盗聴やホームページ改変、パスワードを奪い取るなどの行為があります。

乗っ取り
サーバーと、そのサーバーと接続していて認証されている正当なユーザー間の既存の通信セッションを、侵入者が支配するという攻撃の種類。侵入者は、セッションを監視して、パスワードやコードなどの機密情報の転送を受動的に記録することができます。

ファイアウォール
インターネットなどの信頼できないネットワークからの攻撃や、不正アクセスから組織内部のネットワークを保護するためのシステム。

暗号化
暗号化とは、通信の内容が当事者以外には解読できないように、文字や記号を“一定の約束”でほかの記号に置き換えることをいい、暗号化されたデータを元に戻し、読める状態に戻すことを復号（復号化）という。

IPアドレス
ネットワーク上のノードが自分あてのデータを受け取るために持つ、TCP/IPプロトコルのアドレス。

ログ(アクセスログ・エラーログなど)
あるコンピュータシステムについて、それに対するアクセスの日時や相手先ドメインやIPアドレス、そのほかIDなどについての記録のことをいう。

マルウエア
malicious software (悪質なソフトウェア) の略。システムまたはデータの破損、プライバシーの侵害、情報の盗難、パソコンへの不正侵入といった被害を与えるために設計されたソフトウェアの総称。代表的なマルウェアとして、ウイルス、ワーム、トロイの木馬、キーロガー、スパイウェア、アドウェア、ボットなどがあります。

ウイルス
コンピュータメモリまたはディスク上にあるプログラムに自身を付着して、次々にプログラム間で繁殖するソフトウェアプログラム。ウイルスには、データに被害を加えたり、コンピュータをクラッシュさせたり、メッセージを表示したりするものがある。

スパイウェア
スパイウェアとは、パソコンを使うユーザーに関する情報を収集し、それを情報収集者に送信するソフトウェアの総称。最初にユーザーの同意を適切に得ることなく、広告の表示や、ユーザーの行動履歴等の個人情報の収集、コンピューターの設定の変更などの動作をすることがある。

ワーム
主に自己増殖を目的とした不正プログラムをワームと呼ぶ。最近ではネットワークの普及に伴って、電子メールに自己の分身を添付して自己増殖の手段を得るケースがほとんどとなっている。ほかのプログラムに依存せず、独立して機能を実現する。

トロイの木馬
自らを有益なプログラムであるかのように見せかけ、ユーザーに不利益をもたらすための機能を提供するウィルスのこと。単独のプログラムとして動作し、感染すると、裏でこっそりと犯罪者がコンピューターに侵入するためのバックドアと呼ばれる侵入口を設けたり、ユーザーの個人情報を詐取したりといった被害をもたらす可能性がある。

ランサムウェア
「ランサム(ransom)」とは、身代金の意味の英単語で、感染するとユーザーに身代金を支払うように要求するクライムウエアのことを、「ランサムウエア」という。一見すると有益なソフトウエアであるように信じ込ませ、ユーザーに開かせる傾向がある。

スパム

同じ内容を複数の人に送る意味のないメールをスパムメールと呼んでいる。ハッカーやクラッカーが行うメール爆弾は、スパムメールとして第三者のサーバを中継して発信されることが多く、メールサーバのセキュリティをしっかり行っていないと気が付かないうちに中継者になってしまう場合も多い。

踏み台

あるサーバのセキュリティ・ホールを悪用して、不特定多数の第三者に攻撃を行うこと。踏み台にされたサーバがもともとの被害者であるにもかかわらず、実際に攻撃を受けた側からは、踏み台にされたサーバからの攻撃のように見えてしまう。

ゼロデイ攻撃

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、開発者側が脆弱性に対する対策（パッチなど）を提供する以前から、当該脆弱性を突いた攻撃をしかけるというもの。対策と攻撃の「時間差」がゼロ以下であることからこう呼ばれている。

ブルートフォースアタック

「ブルートフォース攻撃」または「総当たり攻撃」とも言われる。「brute force」とは「力ずくで、強引に」という意で、考えられる全ての鍵をリストアップし、片っ端から解読を試みる暗号解読手法のこと。

SQLインジェクション

Webアプリケーションに対する攻撃手法の一つ。または、その攻撃を可能とする脆弱性のこと。SQL文の中に、不適切な文字列を含めることで、不正な動作をさせることが可能となる。データベース内のすべての情報が外部から盗まれるなど非常に深刻な影響を受ける可能性がある。

XSS(クロスサイトスクリプティング)

Webアプリケーションの脆弱性を悪用し、Webサイトを閲覧しているユーザーのネットワーク上にあるプリンタに、ユーザーが意図しない印刷ジョブを送り込むことができてしまう手法のこと。直接PCに接続されたローカルプリンタには影響がない。