用語集（マネジメントコース）

BIOS パスワード

パソコンが起動する時に、OS（Operating System）の立ち上げ前に実行される BIOS（Basic Input/Output System）において、パスワード認証を行うこと。ログイン認証は、一般的には OS ログインのための利用者 ID とパスワードにより行われるが、OS ログインを行う前に、BIOS パスワードによる認証を行うこともある。（BIOS パスワードを設定する場合、事前に BIOS パスワードを忘れた場合の対策を考えておく必要がある。）

DoS（Denial of Service）

「サービス妨害攻撃」参照。

HDD パスワード

HDD（Hard Disk Drive）へのアクセスをパスワード認証により管理するもの。HDD パスワードを設定している場合、HDD を取り出して別のパソコンでその中のデータを読み出そうとしても、事前に設定されたパスワードが必要になる。なお、HDD パスワードを忘れた場合には、パソコンメーカーの修理・保守でも対応できず、HDD の交換が必要となるため注意が必要。

IM（Instant Messenger）

インターネットに接続したパソコン同士で、チャットやファイルのやりとりができるソフトウェア。同じソフトを利用している仲間がインターネットに接続しているかどうかがわかり、リアルタイムにメッセージを送ることができる。AOL Instant Messaging や MSN Messenger が有名。

PDA（Personal Digital Assistant または Personal Data Assistance）

情報携帯端末とも呼ばれる。スケジュール表、住所録、メモなどの管理を行う手のひらサイズの小型端末で、リアルタイム OS を搭載しているため、電子手帳と異なりアプリケーションの追加による機能追加が可能である。携帯電話機能、インターネット接続による web 閲覧やメールの送受信機能を備える場合もある。

P2P（Peer to Peer：ピアツーピア）

従来のクライアント・サーバ型のように、サーバにあるデータをクライアントにダウンロードして利用するのではなく、不特定多数の個人間で、サーバを介さずに、直接データのやり取りを行うインターネットの利用形態。

SQL インジェクション

データベースと連携した Web アプリケーションの多くは、利用者からの入力情報をもとにデータベースへの命令文を組み立てている。この命令文の組み立て方法に問題がある場合、

攻撃によってデータベースの不正利用を招く可能性がある。この問題を悪用した攻撃手法を一般に「SQL インジェクション」と呼ぶ。
SQL（Structured Query Language）は、リレーショナルデータベース（RDB)において、データベースの操作やデータの定義を行うための問い合わせ言語。

SSL（Secure Socket Layer）
インターネット上でやりとりする情報を暗号化して送受信するプロトコル(通信規約)。個人情報やクレジットカード番号などを安全に送受信することができ、オンラインバンキングなどのサイトで利用されている。

Web メール
専用の電子メールソフトを使うのではなく、Web ブラウザを使って、電子メールソフトと同様な操作を可能とする仕組みのこと。利用者は Web メールシステムで表示される Web サイトにアクセスし、電子メールを閲覧（あるいは送信）できる。Web ブラウザを使える環境であればどこからでも利用可能である。

Winny（ウイニー）
インターネットを利用してファイルを交換する P2P 型のファイル交換ソフトウェアの１つ。匿名性が高いという特徴を持っている。

アクセス権限
コンピュータシステムなどにおいて、ファイルやフォルダ、データベースなどを使用する権限のこと。どのシステム、フォルダ、情報などにアクセスできるか、また、アクセスした際に、何ができるか（読み、書き、実行など）という権限。

アクセス制御
正当な人、装置、プロセス、通信データ（「主体」と呼ぶ）にはネットワークや情報及び情報システムにアクセスすることを許し、不当な主体のアクセスは拒否するような制御のこと。

亜種
最初に発見された元のウイルス(原型)に対して機能の追加や動作を変更するなどの改変がなされ、作り出されたもの。パターンファイルを更新しないと新しい亜種に対応できず、検出することができないケースがあるため、ウイルス対策ソフトを常に最新の状態に保つことが重要。

インシデント
情報セキュリティ分野において、情報セキュリティリスクが発現・現実化した事象のこと。

ウイルス（virus）

広義または狭義に定義される。

広義：「コンピュータウイルス対策基準」（経済産業省告示）においては、広義の定義を採用していて、自己伝染機能・潜伏機能・発病機能のいずれかをもつ加害プログラムをウイルスとしている。自己伝染機能については、他のファイルやシステムに寄生・感染するか、単体で存在するかを問わない定義になっているので「worm（ワーム）」や「ボット」も含むことになる。他のファイルやシステムへの寄生・感染機能を持たないがユーザが意図しない発病機能をもつ「Trojan（トロイの木馬）」や「スパイウエア」も、この広義の定義ではウイルスに含まれる。

狭義：PC 環境におけるコンピュータウイルスを念頭においた狭義の定義においては、他のファイルやシステムに寄生・感染（自己複製）する機能をもつプログラムをいう。この場合、システム中に単体として存在し、ネットワークを伝わって移動する「worm（ワーム）」や「ボット」は、ウイルスとは区別される。また、潜伏機能・発病機能しか持たない「Trojan（トロイの木馬）」や「スパイウエア」もウイルスと区別される。

サービス妨害攻撃（DoS attack: Denial of Service attack）

コンピュータ資源やネットワーク資源を提供できない状態に陥れる攻撃のこと。たとえば、一般に入手可能なツールを使用して、インターネットサーバーが提供する各種サービスを妨害する攻撃が行われている。このような DoS 攻撃には次の種類がある。

1) インターネットプロトコルの特性を悪用し、ネットワークに接続されたコンピュータに過剰な負荷をかけ、サービスを提供できない状態にする攻撃。

2) ネットワークの帯域を渋滞させる攻撃。

3) サーバーアプリケーションの脆弱性を攻略し、サービスに例外処理をさせてサービスを提供できない状態にする攻撃。

サービスレベル

提供されるサービスの内容とその品質のこと。サービス提供側とユーザ企業間でサービスレベルに関して取り決めた契約を SLA（Service Level Agreement：サービスレベル合意書）という。SLA に盛り込まれる内容には、たとえば、通信事業者と取り決めた回線の最低通信速度や、保守提供事業者と取り決めたサービス提供の時間帯や許容停止時間などがある。

修正プログラム（bugfix、patch）

セキュリティの脆弱性を除去するプログラムで、一般に「バグフィックス」または「パッチ」と呼ばれる。ベンダーは、脆弱性の発見に対応して修正プログラムファイルを提供する。ユーザは、これらのファイルをコンピュータシステムにインストールする必要がある。

情報セキュリティガバナンス

社会的責任にも配慮したコーポレート・ガバナンスと、それを支えるメカニズムである内部統制の仕組みを、情報セキュリティの観点から企業内に構築・運用すること。

シンクライアント

ユーザが使うクライアントには必要最小限の処理のみ行わせ、ほとんどの処理をサーバに集中させる構成のシステムのこと。

スパムメール（spam mail）

宣伝や勧誘目的で大量に送られてくる迷惑なメール。

脆弱性（vulnerability）

情報セキュリティ分野における脆弱性とは、通常、システム、ネットワーク、アプリケーション、または関連するプロトコルのセキュリティを損なうような、予定外の望まないイベントにつながる可能性がある弱点の存在や、設計もしくは実装のエラーのことをいう。オペレーティングシステムの脆弱性や、アプリケーションシステムの脆弱性がある。また、ソフトウェアの脆弱性以外に、セキュリティ上の設定が不備である状態も、脆弱性があるといわれる。

脆弱性は、一般に、セキュリティホール（security hole）と呼ばれることもある。

近年ソフトウェアの脆弱性について、広い語感を与える vulnerability を整理し、予定されたセキュリティ仕様を満たさないものを狭義の vulnerability とし、仕様上のセキュリティの欠如を Exposure（露出）として区別する動きがある。

このほかにも、広義には vulnerability もしくは security hole と呼ばれながらも、ソフトウェア自体の問題ではない論点には、弱いパスワード等の本人認証の回避問題、設定ミスによる問題がある。

セキュリティホール（security hole）

情報セキュリティ分野における「脆弱性」は、一般に「セキュリティホール」と呼ばれている。

トロイの木馬（trojan horse）

便利なソフトウェアに見せかけて、ユーザに被害を与える不正なプログラム。感染機能は持っていないので、感染増殖することはない。

トロイの木馬の内部に隠していたウイルスをパソコンに組み込む、パソコン内部の秘密のファイルをインターネット上に送信する、ファイルやディスク内容を破壊するなど、さまざまな被害をもたらす。

感染増殖はしないので、ワクチンソフトでは必ずしもトロイの木馬を検出できるとは限らない。信頼できないサイトに便利なツールとして掲載されていても、そのプログラムはむ

やみにダウンロードして実行しないようにする。「怪しいプログラムは実行しない」という原則を守れば、トロイの木馬の被害を防ぐことができる。

偽ウイルス対策ソフト

ウイルスを検出・削除する機能がないのに、その機能があるように装って導入を促すソフト。ウイルスに感染しているとのメッセージを表示して偽のウイルス対策ソフトの導入を促し、その後、ウイルスを駆除するためには購入が必要との案内をし、代金を詐取するケースがある。

バックドア（backdoor）

コンピュータシステムへの侵入者が侵入後、そのシステムに再侵入するために準備する仕掛け。

パッチ（patch）

「修正プログラム」参照。

フィルタリング（filtering）

特定のキーワード等の条件によりデータを分析し、選別すること。メールのフィルタリングの場合、件名や本文に特定の文字列があれば、自動的にごみ箱へ移動するなどの処理ができる。

分散サービス妨害攻撃（DDoS attack: Distributed Denial of Service attack）

サービス妨害攻撃（DoS 攻撃）には、インターネットプロトコルの特性を悪用して、ネットワークに接続されたコンピュータに過剰な負荷をかけ、サービスを提供できなくするような攻撃がある。このような DoS 攻撃の攻撃元が複数で、標的とされたコンピュータがひとつであった場合、その標的とされるコンピュータにかけられる負荷は、より大きなものになる。このような攻撃を DDoS（Distributed Denial of Service：分散サービス妨害）攻撃と呼ぶ。攻撃元は、攻撃者（人間）自身であるとは限らず、むしろ、攻撃者が事前に標的以外の複数サイトに攻撃プログラムを仕掛けておき、遠隔から一斉に DoS 攻撃をしかける手法が広く知られている。

ポートスキャン（port scan）

攻撃・侵入の前段階として、標的のコンピュータの各ポートにおけるサービスの状態を調査すること。

マルウェア

Malware（Malicious Software：悪意のプログラム）。ユーザの望まない悪さをするプログラムのこと。具体的には、ウイルスやスパイウエアなどの不正プログラムのことをいう。

迷惑メール（UBE： Unsolicited Bulk Email）

商用目的かどうかによらず、個人的、宗教的なものも含めて宣伝や嫌がらせなどの目的で不特定多数に大量に送信されるメールのこと。一般に、spam メール（スパムメール）とも呼ばれる。

誘導型攻撃（受動型攻撃）

利用者が攻撃者の仕掛けた罠に誘導される形（誘導型）の攻撃。このような攻撃は、専門的には受動的攻撃と呼ばれている。受動的攻撃は、利用者が罠のウェブページやメールを閲覧することで成立する。

レジストリ（registry）

Windows 系 OS で、システムやアプリケーションソフトウェアなどの各種動作に関する設定情報を記録したファイル。

Windows に付属しているレジストリエディタという専用のソフトウェアで編集できる。ただし、むやみに設定内容を変えるとシステムが動かなくなる可能性があるため、初心者は、レジストリの変更は避けた方がよい。

ワーム（worm）

通常のウイルスは感染対象のプログラムを必要とするが、ワームは、感染対象となるプログラムがなく、自分自身の複製をコピーして増殖する。

ネットワーク内を這い回る虫のように見えることから、この名称が付けられた。

