

MCPC 情報セキュリティ読本「誰でもわかるセキュリティ入門」用語解説集

(1) キーワード（単語）とその解説

キーワード	解説
アクセス	ウェブサイトに接続する行為を指す
アドウェア (adware)	ユーザーの同意なしに広告を表示する目的で動作するマルウェア
アップグレード	ソフトウェアやハードウェアを新しいバージョンに更新すること
アプリ／アプリケーションソフトウェア	特定の機能を提供するためにデバイスにインストールされるソフトウェア
ウイルス (virus)	他のプログラムに感染し、自身をコピーして拡散するマルウェア
ウイルス対策ソフト	ウイルスを検出・削除し、システムを保護するためのソフトウェア 例： Windows Defender
インストール	ソフトウェアをデバイスに導入する過程
インターネット	世界中のコンピュータネットワークを接続するシステム
オペレーティングシステム (OS)	デバイスを制御する基本ソフトウェア
オフィススイート	文書作成、表計算、プレゼンなどを統合したソフトウェア群
感染	マルウェアなどがシステムに侵入して動作を始めること

キーワード	解説
更新	ソフトウェアのバージョンアップや修正を指す
公式サイト	企業や団体が運営する正規のウェブサイト
外部デバイス	パソコンに接続される USB メモリや外付け HDD/SDD、ネットワークアダプター、プリンタ、モニタ、ウェブカメラ、スキャナーなどの機器
終了日／サポート終了	ソフトウェアや OS の更新提供が終了する日 例：Windows 10 のサポートは 2025 年 10 月 14 日まで
設計ミス／セキュリティ欠陥	プログラムの設計段階での誤りやセキュリティ上の弱点（脆弱性）
設定	ソフトウェアや OS の各種項目をカスタマイズするための操作
新しいアプリ／新たな機能	新たに導入されるアプリやソフトの追加機能
スタート	Windows でメニューを開くためのボタン
スパイウェア（spyware）	ユーザーの情報を秘密裏に収集するマルウェア
セキュリティアップデート／パッチ	脆弱性を修正するための更新プログラム
セキュリティソフトウェア	マルウェアなどの脅威からシステムを保護するソフトウェア
ソフトウェアの最新化	ソフトウェアを最新の状態に保ち、新たな脅威に対する脆弱性を修正すること

キーワード	解説
トロイの木馬（Trojan horse）	正当なソフトに見せかけて侵入し、悪意のある操作を行うマルウェア
バックアップ	データ損失時またはデータ利用不可能な状態に陥った時に備えてコピーを保存しておくこと
バージョンアップグレード	ソフトウェアを新しいバージョンへ更新すること
バンキング	インターネット上で銀行取引を行う行為
ビジネスメール詐欺 （BEC : Business Email Compromise）	企業間の取引を装ってメールを送信し、不正な送金を促すサイバー犯罪の一種。犯罪者は、企業の経営者や取引先担当者になりすまして送金を指示したり、偽の請求書を送付したりします。 BEC の手口： CEO 詐欺：経営者や上司になりすまし、緊急の送金を指示する。 取引先詐欺：取引先担当者を装い、支払い口座の変更を通知する。 法人口座詐欺：実在する企業名義の口座への送金を指示する。 https://cybersecurity-jp.com/column/29527 https://codebook.machinarecord.com/info-security/31389/
PC 正常性チェック	PC が最新 OS へアップグレード可能か確認するツール
フィッシング詐欺 （phishing scam）	偽のメッセージやサイトで個人情報を盗む詐欺、悪意のある不正なプログラムをダウンロードさせるための偽のサイトへ接続させる手法

キーワード	解説
ブラウザ	Web ページを表示するためのソフトウェア
不具合／不具合改良／蓄積	ソフトウェアの誤動作、改良、および未修正の不具合が積み重なること
不審な Web サイト／偽メール／危険なウェブサイト	マルウェア配布や情報搾取を目的とした悪意ある Web サイトやメール
無料／有償ウイルス対策	無償版または有償で提供されるセキュリティ対策ソフト
メール	電子メールマルウェア感染経路やフィッシングの手段ともなる
マルウェア（malware）	悪意のあるソフトウェアの総称（例：ウイルス、ワーム、スパイウェアなど）
利用頻度	どの程度頻繁にシステムやソフトを利用しているか
ランサムウェア（ransomware）	ファイルを暗号化して金銭を要求するマルウェア
ワーム（worm）	ネットワークを介して自己複製し、感染を拡大するマルウェア
脆弱性（vulnerability）	システムやソフトウェアに存在するセキュリティの弱点

キーワード	解説
DMARC (Domain-based Message Authentication, Reporting, and Conformance)	メールのなりすましやフィッシング詐欺を防ぐために、SPF や DKIM の認証結果に基づいてメールの処理方法を定義する。 <機能> 認証ポリシーの設定: SPF や DKIM の認証に失敗したメールをどのように処理するか（受信、隔離 拒否）を指定する。レポート: 認証結果をレポートとして受け取り、ドメインの使用状況を監視する。
DKIM (DomainKeys Identified Mail)	メールの送信者が正当であり、メールの内容が改ざんされていないことを確認する。<機能> デジタル署名: メールにデジタル署名を付与し、受信者がその署名を検証することで、送信者の正当性とメールの改ざんがないことを確認する。公開鍵と秘密鍵の使用: 送信者が秘密鍵で署名し、受信者が公開鍵でその署名を検証する。

キーワード	解説
SPF (Sender Policy Framework)	メールの送信元 IP アドレスを検証し、正規の送信者であることを確認する。 <機能> IP アドレスの検証: 送信者のドメインに関連付けられた IP アドレスを DNS レコードに登録し、受信者がその IP アドレスを検証する。 なりすまし防止: 不正な IP アドレスからのメールをブロックすることで、なりすましメールを防ぐ。

(2) キーワード（単語）とその解説

キーワード	解説
マルウェア（ウイルス等）対策	ウイルス対策ソフトのインストールや定期スキャンなどの総合的な対策手法
標的型攻撃	特定の個人や組織を狙った攻撃フィッシングやマルウェアが使用される
ソーシャルエンジニアリング攻撃	人間の心理的隙について情報を引き出す手法
電子メール添付	マルウェアが添付ファイルを通じて感染する経路
不正なウェブサイト	マルウェア感染や情報搾取の目的で設計されたサイト
身代金要求	ランサムウェアにより暗号化されたファイルの復号と引き換えに金銭を要求する行為
定期的なチェック	ソフトウェアの更新や脆弱性診断を定期的に行うセキュリティ対策
ユーザー教育	セキュリティ意識を高め、攻撃を未然に防ぐための教育活動
サポート期間内に行うべきこと	アップデート、バックアップ、正常性チェックなど
終了後の影響	ソフトウェアのサポート終了により更新が停止し、脆弱性が残る
アップグレードの導線	安全なアップグレードのために公式サイトなど信頼できる手段を用いること
現行の機能改善	既存機能の不具合や欠陥の修正サポート終了後は提供されない

キーワード	解説
SNS／ショートメッセージ	フィッシングリンクや詐欺情報が拡散されやすいメディア
偽情報（Disinformation）	意図的に広められる虚偽の情報
誤情報（Misinformation）	誤って広められる不正確な情報
プロパガンダ	政治的・思想的目的で誇張された情報
フェイクニュース	事実に基づかない偽のニュース形式の情報
ディープステート	陰謀論で語られる、政府とは別の非公開支配構造の存在
XSS（クロスサイトスクリプティング）	Web ページ上に悪意あるスクリプトを実行させる攻撃
XSRF／CSRF（クロスサイトリクエストフォージェリ）	ユーザーの意図しないリクエストを送信させる攻撃
ゼロデイ攻撃	脆弱性が発見されても修正前に行われる攻撃
セッションハイジャック攻撃	正規ユーザーのセッションを乗っ取って不正操作を行う攻撃
SQL インジェクション攻撃	Web フォームなどから不正な SQL 文を送信し、データベース操作を乗っ取る攻撃
ブルートフォース攻撃／辞書攻撃	パスワードを総当たりや辞書から推測する攻撃手法
MITM 攻撃（中間者攻撃）	通信の間に介入して内容を盗聴・改ざんする攻撃
DDoS 攻撃／DoS 攻撃／UDP フラッド攻撃／SYN フラッド攻撃／HTTP フラッド攻撃／ICMP フラッド攻撃	サービスの停止を狙った攻撃手法の総称

キーワード	解説
ドライブバイダウンロード攻撃	Web ページ閲覧時にマルウェアを自動ダウンロード・実行する攻撃
リバースブルートフォース攻撃	特定のパスワードを固定し、それに対して多数のユーザーID で不正ログインを試行する攻撃手法
DNS スプーフィング攻撃	偽の DNS 応答でユーザーを不正な Web サイトへ誘導する手法
PhaaS／RaaS（as a Service 系攻撃）	フィッシングやランサムウェアをサービスとして提供する犯罪ビジネスモデル