# 医療情報システムの安全管理に関するガイドライン　別冊用語集

| 用語 | | 説明 |
|---|---|---|
| あ | アクセスポイント | 通常は、無線 LAN アクセスポイントを指す。ノートパソコンやスマートフォン等の無線 LAN 接続機能を備えた端末を、相互に接続したり、有線 LAN 等、他のネットワークに接続するための機器。 |
| | アプリケーション（アプリ） | コンピュータの OS 上で動作するソフトウェアのこと。ファイル管理やネットワーク管理、ハードウェア管理、ユーザー管理といった基本的な機能を持つ OS に対して、ワープロソフトや表計算ソフトといったソフトウェアのことをアプリケーションと呼ぶ。スマートフォンの場合は、ゲームを初め、辞書機能や動画再生、文書作成等、様々な目的に応じたアプリケーションがあり、「アプリ」と略されて使われる場合もある。 |
| | アプリケーションゲートウェイ | 院内 LAN（企業内 LAN）から直接外部ネットワーク（インターネット）にアクセスさせず、アプリケーションが代行して接続（通信制御）する関所のようなもの。このアプリケーションは通信されるデータやコマンドに不正がないかチェックしながら接続代行するため安全にネットワークアクセスが可能となる。 |
| | 暗号アルゴリズム | 暗号化の手順のこと。主な暗号アルゴリズムは、鍵の扱い方によって共通鍵暗号方式（暗号化と復号とで共通の鍵を使用する方式）と公開鍵暗号方式（暗号化と複号とで別々の鍵を使用する方式）の二つに大別される。 |
| | 暗号化 | データを見てもその内容が分からないように定められた処理手順でデータを変えること。また、暗号化されたデータは、復号という処理によって元のデータに戻すことができる。 |
| | 暗号鍵 | 暗号化（又は復号）する時に必要な鍵（情報）のこと。 |
| | インタフェース | コンピュータ等と他のコンピュータ・周辺機器等を接続するための規格や仕様。 |
| | インデックスデータベース | テーブル（データが記録された表）に格納されているデータを高速に取り出せるよう加工したデータベース。 |
| | ウェアラブル端末 | 腕や頭部等の身体に装着して利用する ICT 端末のこと。 |
| | オフライン攻撃 | パスワードを発見するために、事前に取得した当該システムの暗号化されたパスワードファイルを基に、オフラインでなされる攻撃。辞書に登録しておいた文字列をパスワードシステムと同じ暗号化を行い、その結果と照合し一致するものを探すことにより元のパスワードを知ることができる。 |
| | オンライン外部保存 | 医療情報を医療機関等外の事業者等の環境に、ネットワークを通じて保存を行うこと。 |
| | オンラインサービス | ネットワークを介して提供されるサービスの総称。 |
| か | 仮想デスクトップ | サーバやパソコン等で複数の OS を動かし、ネットワーク経由で個々のデスクトップ端末へ割り当てて通常のデスクトップパソコン同様の機能を実現する技術のこと。 端末側には、記憶装置を持たない「シンクライアント」を使うことが多く使われる。 ネットワークにさえ繋がっていれば、利用する環境の違いに関係なく同じ作業環境を提供できる。 |

| 用語 | | 説明 |
|---|---|---|
| | 可用性 | 情報に関して正当な権限を持った者が、必要時に中断することなく、情報にアクセスできること（Availability）。機密性、完全性、可用性は情報セキュリティの三大要素と呼ばれている。 |
| | 監視装置 | ネットワークの処理能力低下や障害の発生を定期的に若しくは常時監視する機器やシステム。 |
| | 完全性 | 情報に関して破壊、改ざん又は消去されていないこと（Integrity）。機密性、完全性、可用性は情報セキュリティの三大要素と呼ばれている。 |
| | 基本４情報 | 氏名、生年月日、性別、住所を指す。 |
| | 機密性 | 情報に関して正当な権限を持った者だけが、情報にアクセスできること（Confidentiality）。機密性、完全性、可用性は情報セキュリティの三大要素と呼ばれている。 |
| | 共通鍵 | 暗号化と復号に同じ暗号鍵を用いる暗号方式である共通鍵暗号方式において、暗号文の送信者と受信者の間で共有する暗号鍵。 |
| | クライアント | ネットワーク上で情報やサービスを利用するコンピュータのこと。 通常は、一般利用者が使用するコンピュータがクライアントになる。 なお、クライアントが要求した情報やサービスを提供するコンピュータは、サーバと呼ばれる。 |
| | クラウドサービス | 事業者によって定義されたインタフェースを用いた、拡張性、柔軟性を持つ共用可能な物理的又は仮想的なリソースにネットワーク経由でアクセスするモデルを通じて提供され、利用者によって自由にリソースの設定・管理が可能なサービスであって、情報セキュリティに関する十分な条件設定の余地があるもの。提供形態から、IaaS（Infrastructure as a Service）、PaaS（Platform as a Service）及び SaaS（Software as a Service）に分かれる。また、実現形態から、プライベートクラウド、パブリッククラウド及びハイブリッドクラウドに分けることができる。 |
| | クラッカー | コンピュータネットワークに不正に侵入したり、破壊・改竄などの悪意を持った行為を行う者。 |
| | クリアスクリーン | 情報セキュリティに関する対策の一つで、自席のコンピュータを意図せず第三者に操作されたり画面を盗み見されたりしないことを求めるもの。 |
| | 検索エンジン | インターネット上に存在する Web ページや画像ファイルなどの情報を探すための仕組み。 |
| | 堅牢性 | ハードウェアやシステム等が頑丈で、壊れにくいこと。 |
| | 公衆無線 LAN | 駅や街中等、公共の場所で利用できるように設定された無線 LAN の施設やサービスのこと。 |
| | 互換性 | 部品や構成要素を置き換えても、従来通り使用できる性能を互換性という。IT 分野では、特に、特定の製品向けのハードウェアやソフトウェア等を他のものに置き換えても利用できることをいう。 |
| | コンピュータウィルス | 他のコンピュータに勝手に入り込んで、意図的に何らかの被害を及ぼすように作られたプログラムのこと。ディスクに保存されているファイルを破壊したり、個人情報等を盗むこともある。また、感染経路として、ウイルスは、インターネットからダウンロ |

| 用語 | | 説明 |
|---|---|---|
| | | ードしたファイルや、他人から借りたCDメディアや、USBメモリ、電子メールの添付ファイル、ホームページの閲覧等を媒介して感染する。<br>ウイルスにはウイルス対策ソフトでは検出・駆除できないものもあり、ウイルスに感染したことに気付かずにコンピュータを使用し続けるとウイルス自身が自分を複製する仕組みを持っていた場合には、他のコンピュータにウイルスを感染させてしまう危険性もある。 |
| さ | サーバ | ネットワーク上で情報やサービスを提供するコンピュータのこと。サーバに対して、情報やサービスを要求するコンピュータをクライアントという。 |
| | サービス不能（DoS）攻撃 | Denial of Service攻撃の略。サービス拒否攻撃のこと。攻撃者は、Webサーバやメールサーバ等に対して大量のサービス要求のパケットを送りつけ、過大な負荷をかけて相手のサーバやネットワークを使用不能にする。 |
| | サイバー攻撃 | コンピュータシステムやネットワークに、悪意を持った攻撃者が不正に侵入し、データの窃取・破壊や不正プログラムの実行等を行うこと。 |
| | 実在性 | 対象の個人・組織等が間違いなく実在していること。 |
| | 重要インフラ分野 | 情報通信、金融、航空、空港、鉄道、電力、ガス、政府・行政サービス（地方公共団体を含む）、医療、水道、物流、化学、クレジット、及び石油。重要インフラの情報セキュリティ対策に係る第4次行動計画において記載。 |
| | 証跡管理 | 不正アクセスや機密情報漏えい等、コンピュータ等に関する犯罪や法的紛争が生じた際に、原因究明や捜査に必要な機器やデータ、電子的記録を収集・分析し、その法的な証拠性を明らかにする手段や技術の総称。 |
| | 冗長化 | アイテム中に要求機能を遂行するための二つ以上の手段が存在し、手段の一部が故障しても故障とならない性質を冗長性という。冗長化は、システムの構成要素や機能の実現手段を複数用意した冗長性によって、一部に故障が発生しても上位系の障害に至らないよう配慮した設計を行うことをいう。 |
| | 情報処理関連事業者 | 情報処理（電子計算機（計数型のものに限る。）を使用して、情報につき計算、検索その他これらに類する処理を行うこと）を業とする事業者。 |
| | 情報セキュリティポリシー | 情報セキュリティに関する組織的取組についての基本的な方針及び情報セキュリティ対策における具体的な実施基準や手順等の総称。 |
| | 証明書ポリシー（CP：Certificate Policy） | 証明書発行（失効も含む）に関して「適用範囲」、「セキュリティ基準」、「審査基準」等の一連の規則を定めるもの。 |
| | シンクライアント | 団体・組織の情報システムで、従業者等が利用するコンピュータ（クライアント）に最低限の機能だけを持たせて、サーバ側でアプリケーションソフトやファイル等の管理を可能にするシステムの総称。また、そのようなシステムを実現するための、機能を絞ったクライアント用コンピュータのことをいう。 |

| 用語 | | 説明 |
|---|---|---|
| | シングルサインオン | ユーザーが一度認証を受けるだけで、許可されているすべての機能を利用できるようになるシステム。 |
| | スキャン（ウィルススキャン） | コンピュータがウイルスに感染していないかどうかを検査すること。 一般のウイルス対策ソフトは、通常の動作では、電子メールやファイルのコピー等で送受信されるデータについて、ウイルス感染を調査するようになっている。そのため、既にコンピュータに感染してしまったウイルスを検出するには、ウィルススキャンを実行する必要がある。 |
| | スタンドアロン | ネットワークに接続されていない状態のこと。 |
| | ステートフルインスペクション | 通信内容を検査して、動的にポートの閉鎖・開放を制御すること。 |
| | ステルスモード | 無線 LAN のアクセスポイントで、SSID を外部に見えなくする機能のこと。 アクセスポイントの存在を隠すことができるため、無線 LAN を利用する場合の情報セキュリティ対策の一つとして利用できる。 なお、メーカーによっては、SSID 隠蔽機能等の呼び名になっていることもある。 |
| | スマートフォン | 従来の携帯電話に比べてパソコンに近い性質を持った情報機器。大きな画面でパソコン向けの Web サイトや動画を閲覧できたり、アプリケーションを追加することによって機能を自由に追加したりすることができる。また、タッチパネルを使い、画面の拡大やスクロールなど直感的な操作が可能。 |
| | スループット | 一定時間内に処理できるデータ量のこと。CPU の処理性能の指標となる。 |
| | 脆弱性 | 情報セキュリティ分野において、通常、脆弱性とは、システム、ネットワーク、アプリケーション、又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、設計若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である場合もあれば、アプリケーションシステムの脆弱性である可能性もある。<br>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な状態においても、脆弱性があるといわれることがあるセキュリティ・ホール（security hole）と呼ばれることもある。 |
| | 政府情報システムのためのセキュリティ評価制度（ISMAP） | 政府が求めるセキュリティ要求を満たしているクラウドサービスを予め評価・登録することにより、政府のクラウドサービス調達におけるセキュリティ水準の確保を図り、もってクラウドサービスの円滑な導入に資することを目的とした制度。 |
| | 責任分界点 | 情報システムに係る関係者間の責任の移行点。 |
| | セキュリティインシデント | 望まない又は予期しない、単独又は一連の情報セキュリティ事象であって、事業運営を危うくする確率及び情報セキュリティを脅かす確率が高いもの。 |
| | セキュリティターゲット | 情報処理製品や情報処理システムの、セキュリティ対策方針・セキュリティ機能等を記載した文書。情報処理製品や情報処理システムの開発や改善に際して利用されるものであり、評価対象を評価する際に必要なドキュメントでもある。 |

| 用語 | | 説明 |
|---|---|---|
| | セキュリティ・デバイス | IC カード、USB キー等の認証用の個人識別情報を格納するデバイス。 |
| | セキュリティ・パッチ | セキュリティ上の脆弱性・機能的不適合等を解消するためのプログラム。単に「パッチ」ともいう。 |
| | セキュリティ・ホール | 脆弱性の項を参照されたい。 |
| | セッション | コンピュータシステムやネットワーク通信において、接続/ログインしてから、切断/ログオフするまでの、一連の操作や通信のこと。 |
| | セッション乗っ取り | ホームページの閲覧等、パソコンと Web サーバとの間で通信を行っている際に、その通信を利用者以外の者が乗っ取る攻撃のこと。通信が乗っ取られると、本来の利用者になり代わって通信が行われてしまう。「セッションハイジャック」と呼ばれることもある。 |
| | 選任監督義務 | 情報処理を第三者に委託する場合に、適切な者に委託し、かつ当該第三者に対して必要かつ適切な監督を行う義務。 |
| た | ダイアルアップ接続 | 電話回線や ISDN 回線等を通じてインターネットや社内 LAN に接続するサービス又はその方式のこと。 |
| | タイムスタンプ | 電子文書がタイムスタンプが付与された時点で存在することを証明する技術。作成された電子文書がその時点で存在したことだけではなく、その時点からいかなる人にも改ざんされていないことを証明するもの。 |
| | 立会人型電子署名 | 利用者の指示に基づきサービス提供者自身の署名鍵による暗号化等を行う電子契約サービス。 |
| | タブレット PC | 薄い板状（タブレット）の本体に、タッチして操作が可能な液晶画面が組み込まれたパソコン。 |
| | データ形式 | プログラム上でデータを保存する形式をいう。また、補助記憶にデータを保存する形式、転送でデータを送る形式等を指す場合を含む。ファイルとして保存する場合はファイル形式という。代表的なものとして CSV 等が挙げられる。 |
| | データセット | コンピュータで処理が行われるデータのまとまり。通常は、属性によって分類され、若しくは何らかの目的で収集されたデータが記録されたファイル群を指すもの。 |
| | データセンタ | サーバやネットワーク機器などの IT 機器を設置、運用する施設・建物の総称。 |
| | データベース | 複数の主体で情報を共有若しくは利用し、又は用途に応じ加工、再利用ができるように、一定の法則に基づき、作成、管理されたデータの集合をいう。 |
| | デジタル署名 | 数学的なコンピュータ プログラムによって生成される。手書きの署名ではなく、それをコンピュータに取り込んだものでもない。公開鍵暗号技術を利用して、電子メール メッセージ、又はファイルに添付される。メッセージ又はファイルの出所は、専用のツールを使って、このデジタル署名によって検証される。 |
| | 電子証明書 | 信頼できる第三者（認証局）が間違いなく本人であることを電子的に証明するために発行されたデータセットをいう。 |

| 用語 | | 説明 |
|---|---|---|
| | 電子署名 | 電子文書に付加される電子的な署名情報。電子文書の作成者の本人性確認や、改ざんが行われていないことを確認できるもの。 |
| | 電子認証 | 電子認証とは、電子認証局から発行される「電子証明書」を用いて、なりすましの防止や情報の改ざんを防止する技術。 |
| | 電力線搬送通信（PLC） | 電力を供給する電力線を伝送路として通信を行うもの。既設の電力線を利用することにより容易にネットワークを構築することが可能。 |
| な | ネットワーク機器 | ルータ、スイッチ、HUB 等の情報通信ネットワークを構築する際に用いられる機器。 |
| | 熱暴走 | 機器の発熱を適切に制御できないこと等により、中央演算装置等のコンピュータチップ等が高熱により誤動作、停止等の状態になること。 |
| は | バグ | ソフトウェアで設計者の認識の有無に関わらず、全ての成果物において、要件定義の誤り、仕様設計の誤り、プログラミングの誤り、システム構築の誤り等により、期待される結果」と乖離があるために、何かしらの対策・対応が必要と考えられる現象、又はその原因。 |
| | パケットフィルタリング | フィルタリングとは、一般的な意味ではろ過することであるが、コンピュータや Web 等、インターネットの世界では「情報ろ過」を指す。パケットフィルタリングは、ネットワークを行き交うパケット（ネットワークを通して送信されるデータを分割する際に使われる単位）をポリシーに応じて制御する手法。 |
| | バージョン不整合 | プログラムの不備の修正や機能の追加等のため、バージョンの更新を行った際に、何らかの理由で特定のファイルやプログラムの更新が行われず、更新された他のシステムとの整合性が取れなくなること。その結果として、間違ったデータを参照したり、システムエラーにより停止したりする場合がある。バージョンは元々「版」を意味する。 |
| | パーソナルファイアウォール | 個人向けファイアウォール製品。 |
| | パターンファイル | ウイルス対策ソフトがウイルスを発見するために使用するデータのこと。ウイルスは日々新しいものが出現しているため、最新のウイルスに対応するためには、パターンファイルを常に最新のものに更新しておく必要がある。パターンファイルは、ウイルス対策ソフトによっては「ウイルス定義ファイル」や「ウイルス検知用データ」、「シグネチャ」等と呼び名が異なる。 |
| | バックドア | 外部からコンピュータに侵入しやすいように、“裏口”を開ける行為、または裏口を開けるプログラムのこと。このプログラムが実行されると、インターネットからコンピュータを操作されてしまう可能性がある。なお、一部のウイルスでは、感染時にバックドアを埋め込むことがある。 |
| | 搬送波 | 音声や映像、データ等の情報を伝送する信号。信号は電波（無線通信）や光（光ファイバーケーブル）等によって伝達される。送信する信号に応じて搬送波に対して変調を加え、通信を行う。 |

| 用語 | | 説明 |
|---|---|---|
| | 秘密鍵 | 公開鍵暗号で使用される一対の暗号鍵の組のうち、相手方に渡したり、一般に公開したりせず、所有者が管理下に置いて秘匿する必要がある鍵。公開鍵暗号では一対の対応関係にある暗号鍵のペアを用い、公開鍵で暗号化した暗号文は秘密鍵でしか復号できないという仕組みになっている。 |
| | 標準時刻 | 国立研究開発法人情報通信研究機構の原子時計で生成・供給される協定世界時（UTC）をベースに定められた時刻。日本国内では、英国の標準時であるグリニッジ標準時（GMT）に対して 9 時間を加えた日本標準時（JST）が用いられる。 |
| | 標的型メール | 情報システムへの攻撃や機密情報の漏洩等を目的に、特定の企業や個人を対象に送りつけられる電子メールのこと。その電子メールの添付ファイルやリンクを開かせ、マルウェア等を利用して攻撃する。 |
| | ファイアウォール | 外部のネットワークと内部のネットワークを結ぶ箇所に導入することで、外部からの不正な侵入を防ぐことができるシステム、又はシステムが導入された機器。 ファイアウォールには防火壁の意味があり、火災のときに被害を最小限に食い止めるための防火壁から、このように命名されている。 |
| | ファイル交換ソフト（ファイル共有ソフト） | 複数の利用者によるネットワークでのファイルのやり取りを可能にしたソフトウェア。 |
| | ファームウェア | ハードウェアの基本的な制御を行うために機器に組み込まれたソフトウェア。パソコンや周辺機器、家電製品等に搭載されており、機器に内蔵された ROM やフラッシュメモリに記憶されている。 |
| | 不正アクセス | 利用する権限を与えられていないコンピュータに対して、不正に接続しようとすること。実際にそのコンピュータに侵入したり、利用したりすることを不正アクセスに含むこともある。 |
| | 不正コマンド | プログラムに対して、本来期待される機能が損なわれるような処理の実行を求める命令 |
| | 不正侵入 | 利用する権限を与えられていないネットワークやコンピュータに侵入して、不正にネットワークやコンピュータを操作する行為のこと。 |
| | 不正ソフトウェア | コンピュータウイルス、マルウェア、ワーム等様々な形態・呼称があるが、端末に悪影響を与えることを目的とするソフトウェアを指す。 |
| | ブラウザ | Web サイトを閲覧するためのアプリケーションソフト。 |
| | 振る舞い検知 | アンチウイルスの一種で、検査対象のプログラムを仮想環境で実行したり、実際の環境で監視し、その振る舞いによってウイルスかどうか判断する方法。 |
| | ブレークグラス | ICT システムにおいて非常時専用の ID パスワードを準備し、使った痕跡が残る運用を「ブレークグラス」という。火災を発見時、消火栓が使用できるように、消火栓設置の非常押しボタンを覆うガラスを割ってから、ボタンを押してポンプを起動し、警報を鳴らす。このとき、割れたガラスが痕跡として残ることから、このように呼ばれる。 |

| 用語 | | 説明 |
|---|---|---|
| | プロセスアプローチ | 同じ性質の活動の集まりをプロセスとみなし（例：設計プロセス、購買プロセス、製造プロセス など）、品質マネジメントシステム（QMS）を構成するプロセス間の前後を効果的に繋げ、さらに個々のプロセスの管理を徹底することで、個々のプロセス及びプロセス全体の効率とパフォーマンス（意図した結果の達成）、を高めようとする品質管理活動手法のこと。 |
| | プロトコル | ネットワークを介してコンピュータ同士がデータをやり取りするために定められた、データ形式や送受信の手順等の国際標準規則のこと。通信プロトコルとも呼ばれる。 |
| | ポート | 外部とデータを入出力するための、ソフトウェアやハードウェアの末端部分（インタフェース）のこと。多くのパソコンは、周辺機器を接続するインタフェースとしてのUSBポート、LANポート等を備えている。 |
| ま | マイナンバーカード | マイナンバー制度導入により、平成28年1月から交付が開始されたICカードで、基本4情報と顔写真、電子証明書機能等が付されている。本人の申請により交付され、個人番号を証明する書類や本人確認の際の公的な本人確認書類として利用できる。 |
| | マスターデータベース | 情報システムにおいて、複数のデータベースで共通で用いられる情報群。医療分野では、医薬品や病名等に関するマスターが厚生労働省標準規格として、広く用いられている。 |
| | マッピング | AとBを関連付けること。例えば、地図上に住所を関連付けること等をいう。 |
| | マルウェア | malicious softwareの短縮された語。不正かつ有害な動作を行う、悪意を持ったソフトウェアのこと。 |
| | 無害化 | 無害化とは、攻撃者からの悪意のあるファイルの送付やファイル・データ等の利用に対して、利用者のPC等の利用環境にマルウェア等が混入しないように行われる対策。これにより送付された悪意のあるマクロやコード等を削除し、送付先のシステム等の障害や情報漏えいを防止することが期待される。 |
| | 無線LAN | ケーブル線の代わりに無線通信を利用してデータ送受信を行うLANシステム。 |
| ら | ランサムウェア | 感染することによりPCをロックしたり、ファイルを暗号化したりすることによって使用不能にしたのち、元に戻すことと引き換えに「身代金」を要求する不正ソフトウェアをいう。 |
| | リモート署名 | クラウド上のサーバに利用者自身の署名鍵を格納し、利用者が当該サーバにリモートでログインした上で行う電子署名。 |
| | リモートログイン | 遠隔地から公衆回線網やインターネット等を利用して社内のネットワークシステム（LAN）に接続し、ネットワーク上の情報資源を活用すること。 |
| | ルータ | ネットワーク上を流れるデータを他のネットワークに中継する機器。 |
| | ローカル署名 | ICカードやパソコン等の媒体に格納された、本人が管理する鍵で署名するもの。 |
| わ | ワーム | 他のファイルに寄生して増殖するのではなく、自分自身がファイルやメモリを使って自己増殖を行うタイプのウイルスのこと。 |

| 用語 | | 説明 |
|---|---|---|
| | ワンタイムパスワード | 接続する毎に入力するパスワードが毎回変わる方式で、一度使用されたパスワードは次回からは使用できない。専用プログラムやハードウェアを利用するため、パスワードの盗み見等に対するリスクも軽減できる。 |
| A | ACL（アクセス制御リスト） | 情報等へのアクセスの制御を行う際に利用する、誰からのどのような操作を許可するかのリスト。 |
| | ANY 接続拒否 | 無線 LAN アクセスポイントの設定において ESSID が「ANY」や空欄の設定になっている無線 LAN クライアントを拒否する対策のことをいう。この対策により、不特定多数の無線 LAN 端末からの接続を防ぐことが可能となる。 |
| | ASP・SaaS | ASP（Application Service Provider）は、ネットワークを通じて、アプリケーション・ソフトウェア及びそれに付随するサービスを利用させることを指す。SaaS（Software as a Service）もほとんど同様であるため、「ASP・SaaS」と連ねて呼称する。 |
| B | BCP | BCP：Business Continuity Plan の略。災害時、中でも大規模災害時には医療情報システムだけでなく、医療機関等の様々な機能や人的能力に変化が生じる。その一方で、そのような事態では医療の需要が高まり、平常時以上の対応が求められることもある。このような事態に可能な限り対応するためには、普段からあらゆるレベルの異常時を想定し、対策を立て、文書化し、訓練を繰り返すことが有用である。このような対策を事業継続計画（Business Continuity Plan）と呼ぶ。 |
| | BYOD | Bring Your Own Device の略。個人の所有する、あるいは個人の管理下にある端末の業務利用。 |
| C | CISO | Chief Information Security Officer の略。最高情報セキュリティ責任者。企業における情報セキュリティを統括する責任者を指す。 |
| | CSIRT | Computer Security Incident Response Team の略。コンピュータセキュリティにかかるインシデントに対処するための組織の総称。インシデント関連情報、脆弱性情報、攻撃予兆情報を常に収集、分析し、対応方針や手順の策定などの活動をする。 |
| D | DICOM | Digital Imaging and Communications in Medicine の略。医用画像情報やそれらの通信に関する国際標準規格。 |
| | DoS | サービス不能（DoS）攻撃の項を参照されたい。 |
| F | FIPS140-2 | コンピュータシステム及び電気通信システム(音声システムを含む)内の、米国の”the Information Technology Management Reform Act of 1996, Public Law 104-106”の 5131 節に定義された重要情報を保護するセキュリティシステムで利用される暗号モジュールに対するセキュリティ要求事項を規定する標準（FIPS140-1 の改定版）。 |
| E | EDR（Endpoint Detection and Response） | 端末での脅威を検知してインシデント対応等を支援する手法。 |
| H | HL7 | Health Level Seven の略。医療情報交換のための国際標準規格。 |
| | HL7 FHIR | HL7 International によって作成された医療情報交換の次世代標準フレームワーク。HL7 International の一連の標準規格、HL7 |

| 用語 | | 説明 |
|---|---|---|
| | | version 2 、 HL7 version 3 と CDA(Clinical Document Architecture)の優れた機能等を踏まえ、最新の Web 技術を活用し、実装性に重点を置いて策定された。 |
| | HTTPS | HTTP Security の略。インターネット接続における情報通信プロトコル（HTTP：Hyper Text Transfer Protocol）に、TLS 技術による暗号化プロトコルを付加した通信プロトコル。 |
| I | IaaS | Infrastructure as a Service の略。 CPU、メモリ、ストレージ、ネットワーク等のハードウェア資産をサービスとして提供するクラウドサービス。 |
| | IDS | Intrusion Detection System の略。不正な攻撃を検知するシステム。ネットワークやサーバーを監視し、不正なアクセスを検知する役割を担う。ファイアウォールで防ぐことのできない不正プログラムの侵入や行為を発見する仕組みであり、不正な通信を検知した場合、管理者に通知する機能を提供する。 |
| | IKE | Internet Key Exchange の略ネットワーク上の機器や端末間で暗号鍵の交換及び管理を行うためのプロトコル。 |
| | Internet-VPN | Internet-Virtual Private Network の略。各事業所の LAN をインターネット経由で接続しながら、VPN 技術を使うことで盗聴や改ざんを未然に防止し、インターネット経由でも安全に情報を伝送することができる技術。インターネット VPN を提供するための選択肢としては、IPsec、SSL-VPN が代表的である。 |
| | IoT | Internet of Things の略。情報社会のために、既存もしくは開発中の相互運用可能な情報通信技術により、物理的もしくは仮想的なモノを接続し、高度なサービスを実現するグローバルインフラのこと。 |
| | IPS | Intrusion Prevention System の略。不正な攻撃を遮断するシステム。不正な通信を検知した場合,管理者への通知に加え、その通信を遮断する機能を提供する。 |
| | IPsec | IP レイヤー（ネットワーク層）において暗号に基づくセキュリティサービスを提供する機能。インターネット規格の RFC 4301 で規定されている。 |
| | IP-VPN | IP-Virtual Private Network の略。電気通信事業者の閉域 IP 通信網を経由して構築された仮想私設通信網。IP-VPN を利用することにより、遠隔地のネットワーク同士を LAN 同様に運用することが可能になる。 |
| | IP アドレス | インターネット等の TCP/IP 環境に接続されているネットワーク関連機器の識別番号。 |
| | ISDN | Integrated Services Digital Network の略。電話やファクシミリ、データ通信等を統合して扱うデジタル通信網のこと。 |
| | ISMS | Information Security Management System の略。個別の問題毎の技術対策の他に、組織のマネジメントとして、自らのリスクアセスメントにより必要なセキュリティレベルを決め、プランを持ち、資源配分して、システムを運用すること。 |

| 用語 | | 説明 |
|---|---|---|
| | ISP | Internet Service Provider の略。インターネットに接続できるサービスを提供する事業者のこと。通常、電子メールを送ったり、ホームページを閲覧するためには、プロバイダと契約する必要がある。 |
| K | Kerberos | オープンネットワークシステムのための認証システム。 |
| L | LAN | Local Area Network の略。企業内、ビル内、事業所内等の狭い空間においてコンピュータやプリンタ等の機器を接続するネットワーク。 |
| M | MAC アドレス | Media Access Control（メディア・アクセス・コントロール）アドレス。LAN カードの中で、イーサネット（特に普及している LAN 規格）を使って通信を行うカードに割り振られた一意の番号のこと。<br>インターネットでは、IP アドレス以外にも、この MAC アドレスを使用して通信を行っている。LAN カードは、製造会社が出荷製品に対して厳密に MAC アドレスを管理しているため、全く同一の MAC アドレスを持つ LAN カードが 2 つ以上存在することはない。 |
| | MO | MO（Magneto-Optical）ディスク。光磁気ディスクのこと。 |
| N | Nonrepudiation（否認防止） | 送信元（あるいは受信者）が、あとになってその送信事実（受信事実）またはその内容を否定する主張をすることができないように証拠を残すこと。 |
| O | OS | Operating System の略。コンピュータを動作させるための基本的な機能を提供するシステム全般のこと。<br>例えば、メモリやディスク等のハードウェアの制御、キーボードやマウスといったユーザーインタフェースの処理、画面への表示とウィンドウの制御等、コンピュータが動作するための数多くの基本処理を行う。さらに、コンピュータシステムを管理するための数多くのツールが用意されている。 |
| | OSI 階層モデル | ISO（国際標準化機構）が提唱した、異機種間通信を実現するためのネットワーク設計方針である OSI（開放型システム間相互接続）において、プロトコルを機能により 7 つの 階層に分割した概念モデル。 |
| P | PaaS | Platform as a Service の略。オペレーティングシステムや、アプリケーションの実行環境（開発環境を含む）をサービスとして提供するクラウドサービス。 |
| | PKI | Public Key Infrastructure の略。公開鍵をベースに秘匿性、アクセスコントロール、データの完全性、認証、否認防止を確実にするための公開鍵暗号とデジタル署名サービスを提供する包括的なシステム。 |
| R | RAID | Redundant Arrays of Inexpensive Disks 若しくは Redundant Arrays of Independent Disks の略。複数のハードディスクを組み合わせ、仮想的な 1 つのハードディスクとして運用する技術。これにより冗長性の向上が期待できる。 |
| | REST API<br>（Representational State | Web システムを外部から利用するためのプログラムの呼び出し規約（API）の種類の一つで、「REST」（レスト）と呼ばれる設計原則に従って策定されたもの。 |

| 用語 | | 説明 |
|---|---|---|
| | Transfer Application Programming Interface) | |
| S | S/MIME | 電子メールに送信内容の電子署名や暗号化の機能を付加するための規格。 |
| | SNS | Social Networking Service（ソーシャル・ネットワーキング・サービス）の略。登録したユーザーだけが参加できるインターネットの Web サイトのこと。 |
| | SSID | Service Set Identifier の略。無線 LAN で特定のコンピュータや通信機器で構成されるネットワークを指定して、接続するための一意の識別コードのこと。ESS ID とも呼ばれている。<br>無線 LAN で送信するパケットのヘッダ（先頭部）に含まれ、受信側は、SSID が一致しない場合は、そのパケットを無視するため通信ができない。 |
| | SSL-VPN | SSL-Virtual Private Network の略。リモートアクセスでの通信経路上を TLS（SSL の後継技術）で保護する技術。IPsec を用いた VPN のような特定端末間だけで VPN を構成する、いわゆる拠点間 VPN とは異なる。 |
| T | TLS | Transport Layer Security の略。インターネットにおいてデータを暗号化したり、なりすましを防いだりするためのプロトコルのこと。利用者は、認証機関により発行されたサーバ証明書によって、サーバの真正性を確認する。 |
| V | VPN | Virtual Private Network（バーチャル・プライベート・ネットワーク）の略。インターネット上を利用しながら、仮想的にプライベート・ネットワーク（イントラネットのように外部に対して非公開であるネットワーク）を構築する技術。 |
| W | Winny | 日本で開発されたファイル共有ソフト。 インターネット上でクライアント同士が互いの保有するファイルをやり取りすることができる P2P 方式のソフトウェア。 |
| | WPA2/AES | WPA2 は、Wi-Fi Protected Access 2 の略。無線 LAN の暗号化方式である WPA（Wi-Fi Protected Access）のセキュリティを向上させ、AES 暗号に対応した方式。AES は上記の暗号技術のこと。 |
| | 802.1x | LAN におけるユーザー認証の方式の規格。IEEE802.1x は、無線 LAN だけでなく、有線も含んだユーザー認証の方式である。クライアントが接続を要求した場合には、認証サーバである Radius サーバが認証処理を行う。クライアントが認証された場合には、セッションごとに暗号鍵が与えられる。<br>なお、IEEE802.1x では通常暗号化を行わないため、無線 LAN を利用する場合には暗号化する。 |