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。
	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、可能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、可能性は情報セキュリティの三大要素と呼ばれている。
	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、可能性は情報セキュリティの三大要素と呼ばれている。
	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。
	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。 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 の略。提供するサービスを妨害したり停止させる攻撃。
	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。
	重要インフラ分野	情報通信、金融、航空、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 3 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。
	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、機能を絞った低価格のクライアント用コンピュータのことをいう。
	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。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。
	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・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。
	セキュリティインシデント	望まない単独若しくは一連の情報セキュリティ事象、又は予期しない単独若しく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。（JIS Q 27000:2014）
	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。
	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。
	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。
	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。
	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を変調し、通信を行う。
	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。
	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。
	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。
	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。
	ブロードバンド	ネットワークにおける広帯域幅を表す言葉。大容量のデータを高速に流すことができるADSLや光回線等のネットワークやそこで提供されるサービスを指すこともある。
	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	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。
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。
	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。
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	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。
H	HL7	Health Level Seven の略。医療情報交換のための国際標準規格。
	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、SSL/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	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。
	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。
	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。 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。
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。 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	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。
S	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。
	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。
	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。 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/TLS	それぞれSecure Sockets Layer、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。現在は、SSL3.0を基に改良が加えられたTLS1.2が標準的なプロトコルとして利用される。
	SSL-VPN	SSL-Virtual Private Networkの略。リモートアクセスでの通信経路上をSSL/TLS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。
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。 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。