令和５年５月

医療情報システムの安全管理に関するガイドライン 第6.0版　**用語集**

用語		説明	概 O	経 G	企 M	シ C
あ	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。			○	○
あ	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（暗号化と復号とで別々の鍵を使用する方式）の二つに大別される。			○	
あ	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。			○	○
あ	安全管理措置	医療情報を安全に管理する（例えば、医療情報の漏えい、滅失又は毀損を防止する）ために必要かつ適切な内容で、講ずるべきこととされている措置。 個人情報の保護に関する法律（平成 15 年法律第 57 号。以下「個人情報保護法」という。）により、これを講ずることが法的な責務として求められている。	○	○	○	○
い	委託	医療機関等が外部の事業者との間で業務委託契約（契約の形態・種類は問わない）を締結し、外部の事業者に医療情報の取り扱いや、医療情報を取り扱う情報システム・サービスの管理・運用を行わせること。	○	○	○	○
い	医療情報	医療に関する患者情報（個人識別情報）を含む情報。 具体的には、	○	○	○	○

用語		説明	概 O	経 G	企 M	シ C
		①「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律等の施行等について」（平成 17 年 3 月 31 日付け医政発第 0331009 号・薬食発第 0331020 号・保発第 0331005 号厚生労働省医政局長・医薬食品局長・保険局長連名通知。平成 28 年 3 月 31 日最終改正。以下「施行通知」という。）に含まれている文書 ②施行通知には含まれていないものの、民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律（平成 16 年法律第 149 号。以下「e-文書法」という。）の対象範囲で、かつ、患者の医療情報が含まれている文書等（麻薬帳簿等） ③法定保存年限を経過した文書等 ④診療の都度、診療録等に記載するために参考にした超音波画像等の生理学的検査の記録や画像 ⑤診療報酬の算定上必要とされる各種文書（薬局における薬剤服用歴の記録等）等が対象となる。				
い	医療情報システム	医療に関する患者情報（個人識別情報）を含む情報を取り扱うシステム。 例えば、医療機関等のレセプト作成用コンピュータ（レセコン）、電子カルテ、オーダリングシステム等の医療事務や診療を支援するシステムだけでなく、何らかの形で患者の情報を保有するコンピュータ、遠隔で患者の情報を閲覧・取得するコンピュータや携帯端末等も、範ちゅうとして想定される。また、患者情報の通信が行われる院内・院外ネットワークも含む。	○	○	○	○
い	医療情報連携ネットワーク	情報通信技術（ICT）を活用して関係医療機関等の間で効率的に患者の医療情報を共有することを目的とした、患者の同意のもと、医療機関等の間で、診療上必要な医療情報（患者の基本情報、処方データ、検査データ、画像データ等）を電子的に共有・閲覧できることを可能とする仕組みのこと。	○	○	○	

用語		説明	概 O	経 G	企 M	シ C
い	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。				○
い	インフォームド・コンセント	医療の場合では、医療行為を受ける前に、医師および看護師から医療行為について、わかりやすく十分な説明を受け、それに対して患者さんは疑問があれば解消し、内容について十分納得した上で、その医療行為に同意すること。すべての医療行為について必要な手続き。もともとは米国で生まれた言葉で、「十分な説明と同意」と訳される場合もある。	○			
う	ウイルススキャン	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、ウイルススキャンを実行する必要がある。				○
う	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。				○
お	オンプレミス型	医療機関等自身が保有・管理する機材にソフトウェアを配備し、データを保管する形で情報システムを利用する形態のこと。 「クラウドサービス型」と対比されて用いられることが多い用語である。	○		○	○
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」を使うことが多い。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。				○
か	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。	○	○	○	○
か	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または常時監視する機器や				○

用語		説明	概 O	経 G	企 M	シ C
		システム。				
か	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。	○	○		
き	機微性	個人の生命・身体・健康等に関わる情報をはじめとした、漏えいすることによって深刻なプライバシー侵害につながる危険性がある情報の特性。	○	○		
き	基本４情報	氏名、生年月日、性別、住所を指す。			○	
き	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。	○	○	○	○
き	脅威	情報の盗難や不正利用など、情報セキュリティリスクを発生、または、顕在化させる要因のことを指す。 脅威は、人に起因するものと作業環境に起因するものの２つに大別され、人に起因するものは、意図的脅威と偶発的脅威に分類される。 意図的脅威としては、標的型攻撃やマルウェア感染、Web サイトの改ざんなど、外部の人間による悪意ある行為や機密データを持ち出し、悪用するといった内部不正などが該当します。	○			
き	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。				○
く	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。		○		○
く	クラウドサービス型	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	○	○		○

用語		説明	概 O	経 G	企 M	シ C
		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。 「オンプレミス型」と対比されて用いられることが多い用語である。				
く	クラッカー	コンピュータネットワークに不正に侵入するなど、破壊・改竄などの悪意を持った行為を行う者。				○
く	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。				○
こ	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。				○
こ	公的個人認証サービス（JPKI）	インターネット上での行政手続等に際して本人確認を行う場合に必要となる電子証明書を個人・法人が利用できるサービス。地方公共団体情報システム機構（J-LIS）が提供している。 作成・送信した電子文書が、利用者本人が作成した真正なものであり、利用者が送信したものであることを証明する署名用電子証明書と、インターネットサイト等にログインした者が利用者本人であることを証明する利用者証明用電子証明書の２種類の電子証明書をマイナンバーカードに搭載することでサービス提供がなされている。			○	
こ	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。			○	○
こ	コンピュータウイルス	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				○

用語		説明	概 O	経 G	企 M	シ C
		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。		○	○	○
さ	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。	○			
し	死活監視／死活管理	機器やシステム、ソフトウェアなどの対象が動作しているかどうか外部から定期的・継続的に調べること。特に、専用の装置やソフトウェアなどによって自動的に調べ続けること。				○
し	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。			○	
し	証跡	情報システムが行った処理内容や処理対象、処理過程のデータ、利用者が行った操作などを時系列にそのまま電子的に記録したデータのこと。 「証跡管理」とは、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の発生時における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を指す。		○	○	○
し	冗長化	システムの構成要素や機能の実現手段を複数用意することにより、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。			○	○

用語		説明	概 O	経 G	企 M	シ C
し	情報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。		○	○	○
し	情報セキュリティ監査	情報システムについて、セキュリティ対策を正しく実施し、機能させることができているかを実際に検証・評価することで、組織が保有する情報資産を守るために正しく対策がとれているかを第三者の目線で確認すること。 組織内で監査人を立てる内部監査、組織外から監査人を呼ぶ外部監査の二通りの実施方法がある。		○		
し	情報セキュリティマネジメントシステム	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。	○	○	○	
し	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。			○	
す	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。				○
せ	脆弱性	コンピュータの OS やソフトウェアにおいて、プログラムの不具合や設計上のミスが原因となって発生したサイバーセキュリティ上の欠陥のこと。セキュリティ・ホール（security hole）と呼ばれることもある。 セキュリティ上の設定に不備がある状態を指して、脆弱性があるといわれることもある。		○	○	○
せ	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			○	

用語		説明	概 O	経 G	企 M	シ C
		た制度。				
せ	責任分界	協働や提携、委託等する関係者間でそれぞれの責任の範囲を明確にして分けること。責任を分けて、責任の移行する点のことを責任分界点という。	○	○	○	○
せ	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。				○
せ	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。				○
せ	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。				○
せ	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。				○
そ	ソフトウェア	コンピュータを構成する電子回路や装置などの物理的実体を指す「ハードウェア」と対比して、それ自体は形を持たないプログラムや付随するデータなどを指す言葉。 ソフトウェアは、コンピュータの中で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 と、その OS の上で動作する、ワープロソフトや表計算ソフト等に代表されるアプリケーションの 2 種類に大別される。	○	○	○	○
た	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。		○	○	○
た	台帳管理	情報機器等（医療情報システムにおいて利用する物理的な資産、サービス、ライセンス等）や ID・パスワード、医療情報そのものといった、医療機関等におい			○	○

用語		説明	概 O	経 G	企 M	シ C
		て管理する情報資産を洗い出した上で、保存先や利用者範囲、保存期限等を台帳に記録して管理する方法のこと。				
た	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。			○	
た	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。				○
ち	チャネル・セキュリティ	ネットワーク回線を通って情報が伝送される途中で情報が盗み見られることのないよう、ネットワーク回線の経路を暗号化する等の措置をとること。				○
て	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。				○
て	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。			○	
て	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。				○
て	電子証明書	暗号化やデジタル署名に用いる公開鍵暗号の公開鍵が配送される際に添付され、受信者が鍵の所有者を確認するために利用する一連のデータセットのこと。信頼できる第三者（認証局）によって、間違いなく所有者本人であることを電子的に証明するために発行される。			○	○
て	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。	○	○	○	○
と	統制	一般的には、多くの物事を一つにまとめておさめることや国家などが一定の計画や方針に従って指導・制限することを指す。 情報セキュリティにおける統制としては、内部統制や情報セキュリティガバナンスとして用いられ、情報資産に係るリスクの管理を狙いとして、情報セキュリ	○	○	○	

用語		説明	概 O	経 G	企 M	シ C
		ティに関わる意識、取組及びそれらに基づく業務活動を組織内に徹底させるための仕組みを構築・運用することを指す。 （参照）経済産業省「情報セキュリティガバナンスの概念・定義」 https://www.meti.go.jp/policy/netsecurity/secgov-concept.html				
と	トラフィック	通信回線やネットワーク上で送受信される信号やデータ、およびその量や密度のこと。				○
に	二要素認証	情報システムの利用者を認証する方式のうち、IC カード等のセキュリティ・デバイス＋パスワードやバイオメトリクス＋IC カード、ID・パスワード＋バイオメトリクスのように、認証の 3 要素である「記憶」、「生体情報」、「物理媒体」のうち、2 つの独立した要素を組み合わせて認証を行う方式のこと。				○
ね	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。				○
は	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。				○
は	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。 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。				○
は	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、またはそれを実現するプログラムのこと。このプログラムが実行されると、攻撃者によってインターネットを通じてコンピュータを遠隔操作されてしまう可能性がある。 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。				○
は	パブリッククラウド	情報システムのインフラをサービスとして遠隔から利用できるようにしたクラウドコンピューティング環境のうち、インターネットを通じて事業者から一般				○

用語		説明	概 O	経 G	企 M	シ C
		の法人や個人に広く提供されているもの。Web サービス運営などによく用いられる。 限られた環境からのみアクセス可能なクラウドコンピューティング環境である「プライベートクラウド」と対をなす言葉である。				
ひ	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。			○	
ひ	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。				○
ふ	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。				○
ふ	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。			○	○
ふ	フェイルセーフ	システムが故障した場合において、安全性が確保された状態で機能を停止させることで、被害を最小限に留めることを目指す考え方のこと。			○	
ふ	不可逆変換	ある文字列を他の文字列に変換する方法の一つで、変換後の文字列を使って変換前の文字列を特定することができないように変換する方法のこと。				○
ふ	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	○		○	○

用語		説明	概 O	経 G	企 M	シ C
		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。				
ふ	不正ソフトウェア	利用者の予期していない不利益をもたらす不正な活動を実行する、悪意を持ったソフトウェアのこと。マルウェアとも呼ばれる。 コンピュータウイルス、ワーム等、様々な形態がある。		○	○	○
ふ	振る舞い検知	ウイルス対策の方法の一つで、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たりするなどして、不審な挙動が行われていないかを確認し、それによってウイルスかどうか判断する方法。				○
ふ	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。				○
ほ	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。				○
ほ	保健医療福祉分野 PKI（HPKI）	「保健医療福祉分野の公開鍵基盤（Healthcare Public Key Infrastructure）」の略。医療現場において、本人確認だけでなく、公的資格の確認機能を有する電子署名や電子認証を行うための基盤。基盤の設置要件等は厚生労働省において策定されている。 現在は日本医師会、日本薬剤師会、医療情報システム開発センターにおいて、医師等の資格確認を行うための HPKI カードを発行している。			○	
ほ	本人性	申請等が行われる場面において、当該申請等の内容が、間違いなく当該申請等の対象者本人が作成した真正なものであること。			○	
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			○	

用語		説明	概 O	経 G	企 M	シ C
		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。				
ま	マクロ	アプリケーションソフトの操作を自動化する機能の一つで、利用者が関連する複数の操作や手順、命令を一連の手続きとして記録し、必要に応じて簡単な操作で繰り返し呼び出して実行することができる機能。表計算ソフトでよく利用される。				○
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。				○
ま	マルウェア	「不正ソフトウェア」参照				○
む	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。				○
む	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。				○
り	リスク	医療の場合でのリスクとは、健康や生命に被害や悪影響、危険を与える可能性のことを指す。 情報セキュリティにおけるリスクは、情報セキュリティを損ねる要因のことを指し、脅威と脆弱性の要素で構成される。 （参照）日本ネットワークセキュリティ協会（JNSA） https://www.jnsa.org/ikusei/01/02-03.html	○	○	○	○

用語		説明	概 O	経 G	企 M	シ C
り	リスクアセスメント	現実に自組織が持つ情報資産（経営情報や預かり情報と、それを扱う情報システムや、紙を含む記録媒体）について、どのようなリスクが存在するのか、調査して洗い出し、そのインパクトを評価して、対応を決める必要があり、この一連の作業をリスクアセスメントという。 （参照）日本ネットワークセキュリティ協会（JNSA） https://www.jnsa.org/ikusei/01/02-04.html				○
り	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。			○	
り	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施設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。				○
る	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。				○
ろ	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	ネットワークを通じてほかのコンピュータに拡散することを目的としたマルウェアのこと。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。				○
わ	ワンタイムパスワード	接続する度に入力するパスワードが毎回変わり、一度使用されたパスワードは次回からは使用できないような方式のこと。実装にあたっては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	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。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。				○
A	ASP	「Application Service Provider」の略。ネットワークを通じて、アプリケーショ				○

用語		説明	概 O	経 G	企 M	シ C
		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	「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。		○		
B	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。施設や組織における情報セキュリティを統括する責任者を指す。			○	
C	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。		○	○	
E	EDR	「Endpoint Detection and Response」の略。情報システムのネットワーク末端（エンドポイント）の端末に導入し、そこに存在する脅威を監視・検知することで、インシデント対応等を支援するセキュリティ対策システム・対策手法のこと。				○
H	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				○

用語		説明	概 O	経 G	企 M	シ C
		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インターネット経由で利用できるサービスとして提供するクラウドサービス。			○	○
I	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。				○
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。				○
I	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。				○
I	IoT 機器	IoT は「Internet of Things」の略。物理的または仮想的なモノに通信機能を持たせ、インターネットに接続したり相互に通信したりすることにより、自動認識や自動制御、遠隔計測等の高度なサービスを実現するために配置する機器。				○
I	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。				○
I	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。				○
I	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				○

用語		説明	概 O	経 G	企 M	シ C
		ワーク同士を LAN 同様に運用することが可能になる。				
I	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。				○
I	ISMS	「Information Security Management System」の略。「情報セキュリティマネジメントシステム」参照	○	○	○	
K	Kerberos	利用者のコンピュータ（クライアント）からネットワークを通じてサーバにアクセスする際に利用者の認証を行う方式の一つで、パスワードから一定の手順により生成した暗号鍵により、クライアントとサーバ間の通信経路を暗号化することで、認証情報を安全に送受信する仕組み。 複数のサーバにアクセスする際、共通に認証情報を利用することができる利点もある。				○
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 アドレス」の略。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。				○
M	MDM	「Mobile Device Management」の略。組織内の従業者に支給する携帯情報端末のシステム設定等を統合的・効率的に管理する手法、あるいはそれを実現するシステム。 利用できる機能、導入できるソフトウェアやデータに制限を加えたり、端末の紛失時に遠隔制御によってデータの消去や操作のロックを行ったりすることが可				○

用語		説明	概 O	経 G	企 M	シ C
		能となるものもある。				
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。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。				○
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）をインターネット経由で利用できるサービスとして提供するクラウドサービス。			○	○
P	PKI	「Public Key Infrastructure」の略。信用の起点となる最上位の認証局（ルート認証局）が自らの秘密鍵で署名した電子証明書に基づいて、他の認証局が提供する公開鍵を利用する形で、インターネットによる通信のみによって公開鍵暗号とデジタル署名サービスが運用される仕組みのこと。			○	○
R	REST-API	「Representational State Transfer Application Programming Interface」の略。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。				○
S	SaaS	「Software as a Service」の略。ソフトウェアをインターネット経由で利用できるサービスとして提供するクラウドサービス。			○	○
S	SLA	「Service Level Agreement」の略。書面にしたサービス提供者と顧客との合意であって、サービス及びサービス目標を特定した、サービス提供者と顧客との間の合意文書（JIS Q 20000-1:2020）。	○		○	○

用語		説明	概 O	経 G	企 M	シ C
S	SSL-VPN	「Secure Socket Layer-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」の略。公衆回線網等の上に仮想的に構築された閉域網（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。				○
W	WPA2-AES、WPA2-TKIP	WPA2 は、無線 LAN 上で通信を暗号化して保護するための技術規格である WPA（Wi-Fi Protected Access）のセキュリティを向上させた技術規格であり、そのうち WPA2-AES は、共通鍵暗号方式として AES と呼ばれるアルゴリズムを用いた CCMP と呼ばれる暗号化方式を、WPA2-TKIP は、共通鍵暗号方式として RC4 と呼ばれるアルゴリズムを用いた TKIP と呼ばれる暗号化方式を、それぞれ採用している。				○