参考資料3-8

別添2

# 用語の解説

（注）この「用語の解説」は、「医療情報システムの契約における当事者間の役割分担等に関する確認表」や、その別添資料で使用される用語について、利用者の理解のために、できるだけ分かりやすい表現で解説したものである。できるだけ分かりやすい表現としている関係上、各用語について、厳密に定義づけたもの等ではないこと、他の用語集等のものと若干表現が異なる場合があり得ること等に留意が必要である。

| 番号 | 用語 | 内容 | 記載場所（初出） | |
|---|---|---|---|---|
| ＊1 | サービス仕様適合開示書 | 医療機関等との契約等に基づいて医療情報システム等を提供する事業者が、自ら提供するサービスの仕様につき、「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」への適合状況を医療機関等へ開示するために作成するための資料のこと。 | Part1 | A.1 |
| ＊2 | MDS/SDS<br>(Manufacturer / Service Provider Disclosure Statement for Medical Information Security) | 「製造業者による医療情報セキュリティ開示書（MDS）」及び「サービス事業者による医療情報セキュリティ開示書（SDS）」の略称で、（一社）保健医療福祉情報システム工業会（JAHIS）及び（一社）日本画像医療システム工業会（JIRA）が定めた各製造業者/サービス事業者の医療情報システムのセキュリティ機能に関する説明の標準的記載方法（書式）のこと。これらの書式は製品/サービスの説明の一部として製造業者/サービス事業者が作成し、セキュリティマネジメントを実施する医療機関等を支援するために用いられることが想定されている。 | Part1 | A.1 |
| ＊3 | MDS2<br>(Manufacturer Disclosure Statement for Medical Device Security) | 「医療機器セキュリティのための製造業者開示説明書」の略称で、医療機器内に組み込まれたセキュリティおよびプライバシー対策機能に関する標準化された情報を提供することにより、医療提供組織内のセキュリティリスクマネジメントを支援することを目的としている。 | Part1 | A.1 |
| ＊4 | BCP<br>（Business Continuity Plan） | 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。<br>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。 | Part1 | C.3 |
| ＊5 | サービス・レベル合意書<br>(SLA：Service Level Agreement) | 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のこと(JIS Q 20000-1:2020)。 | Part2 | A.6 |
| ＊6 | クラウドサービス | 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。「オンプレミス」と対比されて用いられることが多い用語である。 | Part2 | A.9 |
| ＊7 | 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のことや、その量や密度のこと。 | Part2 | C.1 |
| （以下は、別添「推奨される対応例」の用語の解説である） | | | | |
| ＊8 | 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弱点のことを指し、「セキュリティホール」とも呼ばれる。 | Part1 | B.2 |
| ＊9 | プライバシーマーク | 日本産業規格「JIS Q 15001 個人情報保護マネジメントシステム―要求事項」に適合して、個人情報について適切な保護措置を講ずる体制を整備している事業者等を認定して、その旨を示すマークのこと。 | Part1 | 参考.1 |
| ＊10 | 情報処理安全確保支援士<br>（略称：登録セキスペ） | サイバーセキュリティ対策の重要性が社会的に高まる中で、サイバーセキュリティ対策の推進を担う人材の育成・確保を目的に作られた「国家資格」のこと。（独）情報処理推進機構（IPA）が実施する「情報処理安全確保支援士試験」の合格者が所定の手続きを経て当該資格を保有できる。当該資格の有資格者は、組織における安全な情報システムの確保支援や、サイバーセキュリティ対策の分析結果に基づき指導・助言を行うことが想定されている。 | Part1 | 参考.1 |
| ＊11 | 情報セキュリティマネジメント試験 | （独） 情報処理推進機構（IPA）が実施する国家試験である「情報処理技術者試験」の一つで、情報セキュリティマネジメントの計画・運用・評価・改善を通して組織の情報セキュリティ確保に貢献し、脅威から継続的に組織を守るための基本的なスキルを認定する試験のこと。 | Part1 | 参考.1 |
| ＊12 | リモートメンテナンス | 通信回線を通じて、遠隔地のネットワークやシステムの保守・点検等を行うこと。 | Part1 | 参考.3① |
| ＊13 | 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。 | Part1 | 参考.3③ |

| 番号 | 用語 | 内容 | 記載場所（初出） | |
|---|---|---|---|---|
| ＊14 | 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するまでの一連の作業のこと。 | Part2 | A.4 |
| ＊15 | 要配慮情報を含む個人情報 | 本人の人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実その他本人に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして政令で定める記述等が含まれる個人情報のこと。 | Part2 | A.8 |
| ＊16 | ISMS<br>(Information Security Management System) | 「情報セキュリティマネジメントシステム」の略称で、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。 | Part2 | A.9① |
| ＊17 | ISMAP<br>（Information system Security Management and Assessment Program） | 「政府情報システムのためのセキュリティ評価制度」の略称で、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のこと。 | Part2 | A.9① |
| ＊18 | 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。 | Part2 | B.3 |
| ＊19 | オープンソースソフトウェア | ソースコードが公開されているソフトウェアのこと。また、「オープンソース」であるプログラムの頒布条件は、再頒布の自由等一定の基準を満たしている必要がある。 | Part2 | B.6 |
| ＊20 | ソースコード | プログラミング言語などの人間が理解・記述しやすい言語やデータ形式を用いて書き記されたコンピュータプログラムのこと。 | Part2 | B.6 |
| ＊21 | ウイルス定義ファイル（パターンファイル） | セキュリティソフトがマルウェア（不正なプログラム）を検出するための定義情報が入ったファイル。実世界でいえば顔写真付きの手配書のようなもの。 | Part2 | 参考.4 |
| ＊22 | 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。 | Part2 | 参考.5 |
| ＊23 | ホットスタンバイ／コールドスタンバイ | システム障害発生時にあらかじめ用意した予備のシステムに切り替え方式である。ホットスタンバイとは、複数の系統を常時稼働状態に置き、一つに異常が生じると即座に他の系統に処理を引き継ぐ方式。これに対して、コールドスタンバイは、予備の機材などは用意しておくが普段は停止しており、障害時にシステムの起動や設定などから行う方式。なお、予備のシステムを用意することを冗長化という。 | Part2 | 参考.5 |
| ＊24 | 二重化 | 機器や部品、システムなどの信頼性や耐障害性を高める手法の一つで、同じ構成の機材を二系統用意すること。 | Part2 | 参考.5 |
| ＊25 | 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。 | Part2 | 参考.5 |
| ＊26 | ログ | その機器で行われた活動を記録したデータ。通信に関するものは「通信ログ」のこと。 | Part2 | 参考.8 |