添付Ｅ　用語集

(1) CC(Common Criteria)

セキュリティの観点から、情報技術に関連した製品及びシステムが適切に設計され、その設計が正しく実装されていることを評価するための仕組み。国際規格 ISO/IEC 15408 に規定されている。

(2) CSMS(Cyber Security Management System)

産業用オートメーション及び制御システムを対象としたサイバーセキュリティのマネジメントシステム。国際規格 IEC62443-2-1 に要求事項が定められている。

(3) EDSA(Embedded Device Security Assurance)認証

ISA/IEC 62443 に基づいて、米国 ISCI（ISA Security Compliance Institute）が開発し、運営する、制御機器のセキュリティ保証に関する認証制度。ソフトウェア開発の各フェーズにおけるセキュリティ評価、セキュリティ機能の実装評価、通信の堅牢性テストという3つの観点から評価を実施する。

(4) IDS(Intrusion Detection System)

サーバやネットワークの外部との通信を監視し、攻撃や侵入の試み等不正なアクセスを検知して管理者にメール等で通報するシステム。

(5) IoT(Internet of Things)

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。［ITU-T Y.2060(Y.4000)、 IoT 推進コンソーシアム/経済産業省/総務省 ”IoT セキュリティガイドライン ver.1.0”］

(6) IoT 機器

インターネットに接続して動作する機器。フィジカル空間とサイバー空間とをつなぐ。

(7) IPS(Intrusion Prevention System)

サーバやネットワークの外部との通信を監視し、侵入の試み等不正なアクセスを検知して攻撃を未然に防ぐシステム。

(8) ISMS(Information Security Management System)

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、資源を配分して、システムを運用するための仕組み。国際規格 ISO/IEC 27001 に要求事項が定められている。

(9) ITSMS(IT Service Management System)

IT サービス提供者が、提供する IT サービスを PDCA サイクルに基づいて管理することで、品質の維持管理及び改善を行っていくための仕組み。国際規格 ISO/IEC 20000-1 に満たすべき要求事項が定められている。

(10) アクチュエータ

機構又はシステムを動かし又は制御するためのデバイス。一般に電流、油圧、空気圧等のエネルギー源で作動し、そのエネルギーを運動に変える。アクチュエータは、制御システムが環境に働きかける機構である。制御システムは単純で(固定機構や電子システム)、ソフトウエアベース(プリンタドライバ、ロボット制御システム等)や人その他による。[NIST SP 800-82 rev.2]

(11) エンティティ

セキュリティの文脈においては、情報を使用する組織及び人、情報を扱う設備、ソフトウェア及び物理的媒体などを意味する。実体、主体などともいう。 [JIS Q 27000:2014]

(12) 可用性(availability)

認可されたエンティティが要求したときに、アクセス及び使用が可能である特性。[JIS Q 27000:2014]

(13) 監査

組織内においてサイバーセキュリティ対策が適切に実施されているかどうかを判定するために、監査証拠を収集し、それを客観的に評価するための、体系的で、独立し、文書化したプロセスのこと。監査は、内部監査(第一者)又は外部監査(第二者・第三者)のいずれでも、又は複合監査(複数の分野の組合せ)でもあり得る。[JIS Q 27000:2014]

(14) 完全性(integrity)

正確さ及び完全さの特性。[JIS Q 27000:2014]

(15) 機能安全

EUC(被制御機器)及び EUC 制御系の全体に関する安全のうち、E/E/PE (電気・電

子・プログラマブル電子の)安全関連系及び他リスク軽減措置の正常な機能に依存する部分。 [IEC 61508-4 Ed.2]

（16） **機密性(confidentiality)**

認可されていない個人、エンティティ又はプロセスに対して、情報を使用させず、また、開示しない特性。[JIS Q 27000:2014]

（17） **脅威**

システム又は組織に損害を与える可能性がある、望ましくないインシデントの潜在的な原因。 [JIS Q 27000:2014]

（18） **公開鍵**

暗号化と復号に異なる鍵を用いる公開鍵暗号方式で使用される一対の鍵の組のうち、一般に公開される側の鍵。

（19） **サービスプロバイダー**

一般的に、公的機関や、その他の営利組織に対するネットワーク運用に関する基本的なサービスまたは付加価値サービスのプロバイダー。 [NIST IR 4734]

（20） **サイバー空間**

コンピュータシステムやネットワークの中に広がる仮想空間。デジタル化されたデータを活用して価値を生み出す。

（21） **サイバー攻撃(Cyber Attack)**

資産の破壊、暴露、改ざん、無効化、盗用、又は認可されていないアクセス若しくは使用の試み。[JIS Q 27000:2014]

（22） **サイバーセキュリティ**

電子データの漏えい・改ざん等や、期待されていたITシステムや制御システム等の機能が果たされないといった不具合が生じないようにすること。

（23） **サイバーフィジカルシステム(CPS:Cyber Physical System)**

現実社会に新たな価値を生み出すデータシェアのメカニズムのこと。現実社会をサイバー空間に写し取り、モデル化されたノウハウや経験・知識を活用し、誰でも自由に情報(データ)を組み合わせることで、新たな気付きや発見を得ることができる。

（24） サプライチェーン

複数の開発者間でリンクされたリソース・プロセスで、製品とサービスについて、調達に始まり設計・開発・製造・加工・販売および購入者への配送に至る一連の流れ。［ISO 28001：2007、 NIST SP 800-53 rev.4］

（25） 産業用制御システム

製造、製品の出荷、生産、および販売などの産業プロセスを制御するのに使用される情報システム。産業用制御システムには、地理的に分散している資産を管理するのに使用される監視制御データ収集システム（SCADA）、分散制御システム（DCS）、および前二者より小規模ながらローカルなプロセスをプログラマブル論理制御装置の利用を通じて制御するシステムなどがある。［NIST SP 800-53 rev.4］

（26） サプライヤー

製品またはサービスの供給のために買い手と合意した組織あるいは個人。［ISO/IEC 27036-1：2014］

（27） 識別子

様々な対象から特定の 1 つを識別するのに用いられる名前や符号、数字等のこと。

（28） 冗長化

コンピュータやシステムに何らかの障害が発生した場合に備え、予備装置を配置すること。

（29） 真正性（authenticity）

エンティティは、それが主張するとおりのものであるという特性。［JIS Q 27000：2014］

（30） 信頼性(trust)

利用者又は他の利害関係者がもつ、製品又はシステムが意図したとおりに動作するという確信の度合い。［X 25010：2013］

（31） 信頼性の基点

エンティティが認可されたプロセスまたは認可されたパッケージの検証を開始するための確立された信頼点（通常、一部のヒト、オフィス、または組織の権限に基づく）。［CNSSI 4009-2015］

（32） ステークホルダー

意思決定若しくは活動に影響を与え、影響されることがある又は影響されると認知している、あらゆる人又は組織。［JIS Q 27000:2014］

（33） 脆弱性

一つ以上の脅威によって付け込まれる可能性のある、資産又は管理策の弱点。［JIS Q 27000:2014］

（34） 生体認証

指紋や静脈、眼球の虹彩、声紋等の身体的特徴によって本人確認を行う認証方式のこと。

（35） セーフティ(安全性)

許容できないリスクから免れている状態。［IEC 61508-4 Ed.2］

（36） 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セキュリティ事象、又は予期しない単独若しくは一連の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セキュリティを脅かす確率が高いもの。

（37） セキュリティ管理責任者

組織のセキュリティマネジメントシステムの運用及び管理に係る最終責任者。

（38） セキュリティ事象

セキュリティポリシーへの違反若しくは管理策の不具合の可能性、又はセキュリティに関係し得る未知の状況を示す、システム、サービス又はネットワークの状態に関連する事象。

（39） セキュリティ・バイ・デザイン

機器やシステムの企画・設計段階からセキュリティ確保するための方策を組み込むこと。

（40） セキュリティポリシー

トップマネジメントによって正式に表明された組織の意図及び方向付け。［JIS Q 27000:2014］

（41） セキュリティリスク

セキュリティリスクとは、セキュリティに関連して不具合が生じ、それによって企業の経営に何らかの影響が及ぶ可能性のこと。

（42） セキュリティルール

発生しうるセキュリティリスクに対する対応策の内容を明確にし、対応の範囲や優先順位を定めたもの。

（43） セキュリティ運用プロセス

検知したセキュリティインシデントに即座に対応できるよう、あらかじめ対応手順を明確に文書化したもの。

（44） セキュリティ対策組織

組織の内部及び外部の情報源から脆弱性情報を継続的に収集・分析し、監視対象とするセキュリティインシデントへの適切な対処方法(優先順位、範囲等)を判断する体制のこと。

（45） センサ

計測中の物理特性（速度、温度、流量等）を表した電圧又は電流出力を発生させるデバイス。［NIST SP 800-82 rev.2］

（46） 相互認証

認証方式の 1 つで、双方の当事者が互いに相手の正当性を認証する方式。

（47） 耐タンパーデバイス

内部構造や記憶しているデータ等の改ざん・読み出しの困難さを備えるデバイス。

（48） タイムスタンプ

時間の整合性を保証するために使用される情報のトークンであり、時刻を含むタイムスタンプ付きデータと、信頼できるタイムスタンプ局（TTA）によって生成された署名が含まれる。［NIST SP 800-89］

（49） 電子証明書

認証局(CA)が発行する、デジタル署名解析用の公開鍵が真正であることを証明するデータ。

（50） 多要素認証(Multifactor Authentication)

2 つ以上の異なる要素を使用する認証。要素には、以下をのものが含まれる:①被認証者が知っていること(例:パスワード・暗証番号)②被認証者が持っているもの(例:暗号認証デバイス・トークン)③被認証者であること(例:生体認証情報)。[NIST SP 800-53 rev.4]

（51） 認証(authentication)

エンティティの主張する特性が正しいという保証の提供。[JIS Q 27000:2014]

（52） ハザード

危害(身体への傷害、人の健康逸失、所有物の毀損又は環境破壊)の潜在的な源。[IEC 61508-4:2010]

（53） ハッシュ値

元になるデータから一定の計算手順により求められた、規則性のない固定長の値。

（54） 秘密鍵

暗号化と復号に異なる鍵を用いる公開鍵暗号方式で使用される一対の鍵の組のうち、他者に対して公開しない鍵。

（55） ファイアウォール

あるコンピュータやネットワークと外部ネットワークの境界に設置され、内外の通信を中継・監視し、外部の攻撃から内部を保護するためのソフトウェアや機器、システム等のこと。

（56） フィジカル空間

現実の世界。

（57） プロセス

インプットをアウトプットに変換する、相互に関連する又は相互に作用する一連の活動。[JIS Q 27000:2014]

（58） プロトコル

複数の主体が滞りなく信号やデータ、情報を相互に伝送できるよう、あらかじめ決められた約束事や手順の集合のこと。

（59） マルウェア(Malware)

許可されていないプロセスの実施を試みることによって、情報システムの機密性・完全性・可用性に悪影響をもたらすソフトウェアまたはファームウェア。[NIST SP 800-53 rev.4]
セキュリティ上の被害を及ぼすウイルス、スパイウエア、ボット等の悪意を持ったプログラムを指す総称。

（60） マルチステークホルダー・プロセス

3 者以上のステークホルダーが、対等な立場で参加・議論できる会議を通し、単体もしくは 2 者間では解決の難しい課題解決のために、合意形成などの意思疎通を図るプロセス。［内閣府］

（61） リスク

目的に対する不確かさの影響。 [JIS Q 27000:2014]

（62） リスク源

それ自体又はほかとの組合せによって、リスクを生じさせる力を本来潜在的にもっている要素。［JIS Q 31000:2010］

（63） リスクマネジメント

リスクについて、組織を指揮統制するための調整された活動。［JIS Q 31000:2010］

（64） レジリエンス

システムが以下の状態を維持できること:①悪条件下にあっても、あるいは負荷が掛かった状態であっても、(顕著に低下した状態または無力化したような状態に陥ったとしても)稼働して、基礎的な運用能力を維持すること②ミッションニーズと平仄が合う時間内に、有効的に運用されている状態に復旧すること。［NIST SP 800-53 rev.4］