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）　CSIRT（Computer Security Incident Response Team）

コンピューターセキュリティに関連するインシデントへの対応を支援する目的で確立される機能 ; CIRT(Computer Incident Response Team)や、CIRC(Computer Incident Response Center, Computer Incident Response Capability)とも呼称されることがある。[NIST SP 800-61 Rev.2]

（3）　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 IEC 62443-2-1 に要求事項が定められている。

（4）　EDSA（Embedded Device Security Assurance）認証

IEC 62443-4-2 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。

（5）　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。

（6）　IoT（Internet of Things）

フィジカル空間とサイバー空間からの情報を処理し、反応するサービスと相互接続されたエンティティ、ヒト、システムおよび情報資源のインフラストラクチャ。
[ISO/IEC 20924:2018 を本フレームワークの用語に合うよう一部改変]

（7）　IoT 機器

センシング、あるいはアクチュエーティングを通じてフィジカル空間と相互作用し、通信する IoT システムのエンティティ。
注記　IoT 機器とはセンサまたはアクチュエータを指す。

（8） 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。

（9） 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。

（10） 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。

（11） SOC（Security Operation Center）

セキュリティインシデントの検出、分析、対応、報告、防止を目的とした主にセキュリティアナリストから構成されるチーム。[RFC 2350, CNSS Instruction No. 4009]

（12） **アクチュエータ**

IoT の文脈においては、正当な入力に応答して物理的なエンティティの 1 つ以上の特性を変更する IoT 機器を指す。[ISO/IEC 20924:2018]

（13） **エンティティ**

物理的あるいは非物理的に、明確な存在を持つもの。[ISO/IEC 15459-3:2014]

（14） **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]

（15） **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]

（16） **完全性（Integrity）**

正確さ及び完全さの特性。[JIS Q 27000:2014]

（17） **危害（harm）**

人への傷害若しくは健康障害，又は財産及び環境への損害。[JIS Z 8051:2015]

（18） **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]

（19） **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]

（20） **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]

（21） **公開鍵**

エンティティが所有する非対称鍵ペアの鍵で、公開できるもの。

注記　非対称署名システムの場合、公開鍵は検証変換を定義する。非対称暗号化システムの場合、公開鍵は暗号化変換を定義する。“公知”の鍵は、全世界的に利用可能である必要はない。鍵は、既定のグループの全メンバーに利用可能であるだけでもよい。[JIS X 19790:2007]

（22） **サービス**

組織と顧客との間で必ず実行される，少なくとも一つの活動を伴う組織のアウトプット。[JIS Q 9000:2006]

（23） **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]

（24） 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。

（25） 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]

（26） 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。

（27） 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]

（28） 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]

（29） 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（PLC）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]

（30） 識別子

アイデンティティに関わる特定の文脈において、あるエンティティを他のエンティティと明確に区別する情報。[ISO/IEC 20924:2018]

（31） 冗長化

機能単位が要求された機能を遂行するために十分な手段、又はデータが情報を表すのに十分な手段のほかに、別の手段を用意すること。[JIS X 0014:1999]

（32） **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]

（33） **信頼（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。[JIS X 25010:2013]

（34） **信頼性（Trustworthiness）**

信頼又は信用に値する特性。IoT の文脈では、IoT 実装のライフサイクル全体の中でセキュリティ、プライバシー、セーフティ、リライアビリティ及びレジリエンスを保証するための、信頼または信用に値する特性を指す。[ISO/IEC 20924:2018]

（35） **信頼性の基点（Basis of trustworthiness）**

信頼性を確保するための観点。

（36） **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]

（37） **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]

（38） **脆弱性修正措置計画**

組織のシステムが直面する 1 つ以上の脅威または脆弱性を対象に、修正措置を実施するための計画。この計画には、通常、脅威や脆弱性を取り除くためのオプションと、修正措置を実施する優先順位が含まれる。[NIST SP 800-40 Ver.2.0]

（39） **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。

（40） **セーフティ（安全性）**

危害を引き起こすおそれがあると思われるハザードから守られている状態。[JIS Z 8501:2015]

(41) 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。

(42) 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。

(43) 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。

(44) 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。

(45) セキュリティ対応組織

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。セキュリティ対応組織は、SOC, CSIRT といった組織や機能を包含する。[セキュリティ対応組織(SOC,CSIRT)強化に向けたサイバーセキュリティ情報共有の「5W1H」 v1.0（日本セキュリティオペレーション事業者協議会(ISOG-J), 2017 年)、セキュリティ対応組織の教科書 v2.1（ISOG-J, 2018 年)、セキュリティ対応組織の教科書 ハンドブック v1.0 (ISOG-J, 2018 年)、セキュリティ対応組織の教科書 成熟度セルフチェックシート v2.2（ISOG-J, 2019 年）]

(46) 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（例 : 脅威分析、セキュリティアーキテクチャ、外部仕様分析、プライバシー影響評価)を組み込むこと。

(47) 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セキュリティに係る意図や方向付け及び、そのような意図や方向付けに基づいてセキュリティ対策を行うために組織が定めた規定。

（48） セキュリティリスク

セキュリティに関連した不具合が生じ、それによって自組織や取引先等の関係する他組織の目的、あるいは社会全体に何らかの影響が及ぶ可能性。

（49） 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。

（50） センサ

IoT の文脈では、1 つ以上の物理的なエンティティの 1 つ以上の特性を測定し、ネットワーク経由で送信可能なデジタルデータを出力する IoT 機器を指す。[ISO/IEC 20924:2018]

（51） 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。

（52） 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。

（53） タイムスタンプ

共通の時刻基準に関して、ある時点を表す時変パラメータ。[ISO/IEC 18014-1:2008]

（54） 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]

（55） 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。

（56） 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]

252 （57） **ハザード**
253 危害の潜在的な源。[JIS Z 8051:2015]
254
255 （58） **ハッシュ関数**
256 任意のビット列（通常は上限が存在）を固定長のビット列に写像する関数であって、
257 以下の 2 つの性質を満たすもの：
258 - 与えられた出力値について、出力値に対応する入力値を見つけることが計算
259 上不可能であること
260 - 与えられた入力値について、同じ出力値に対応する 2 つ目の入力値を見つけ
261 ることが計算上不可能であること [ISO/IEC 10118-1:2016]
262
263 （59） **ハッシュ値**
264 ハッシュ関数の出力であるビット列。 [ISO/IEC 27037:2012]
265
266 （60） **秘密鍵**
267 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
268 ち、他者に対して公開しない鍵。
269
270 （61） **ファイアウォール**
271 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
272 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、
273 システム等のこと。
274
275 （62） **フィジカル空間**
276 現実の世界。サイバー空間と物質から構成される世界とを区別するための表現。
277
278 （63） **プロセス**
279 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、論
280 理的又は物理的な一連の活動。
281
282 （64） **プロトコル**
283 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
284 められた約束事や手順の集合のこと。
285
286
287

（65） **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。

（66） **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]

（67） **目的**

達成する結果。[JIS Q 27000:2014]

（68） **リスク**

目的に対する不確かさの影響。[JIS Q 27000:2014]

（69） **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]

（70） **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]

（71） **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]