# 添付C　対策要件に応じたセキュリティ対策例

・第Ⅲ部本編にて記載した対策要件を実装する場合の、対策の一例を High Advanced/Advanced/Basic のレベル別に記載している。High Advanced の対策例を実装する場合は、High Advanced だけでなく、Advanced 及び Basic に記載の内容も包含するよう対策を行う必要がある。
・対策のレベルは、既存の標準におけるレベル別に階層化された管理策をベースに、対策を導入・運用する際のコスト、対策の対象とするスコープ(例：自組織内のみの適用か、関連する他組織を巻き込んだ適用か)等により判断している。
・当該対策例の実装に際し、主体となる要素を、O「組織」、S「システム」、O/S「システム及び組織」の3つに分類して提示する。
・対策例の記載に当たっては、第Ⅲ部にて各要件に対して割り当てた「関連標準等」に記載の文書および該当項目の一部(本表「参照ガイドライン」という形に示している)を参照している。
・本項に記載の対策例はあくまで一例を示すものであって、他の実装方法を何ら否定するものではない。各組織の事業の特性やリスク分析の結果等に応じて、リスク対応を実施する際の参考として、本資料を参照されたい。

| 対策要件ID | 対策要件 | 対応する脆弱性 | 対策例 | 対策例を実行する主体 | 参照ガイドライン | | |
|---|---|---|---|---|---|---|---|
| | | | | | NIST SP 800-171 | NIST SP 800-53 rev.4 | ISO/IEC 27001:2013 付属書A |
| CPS.AM-1 | ・システムを構成するハードウェア及びソフトウェアおよびその管理情報の一覧を文書化し、保存する | L1_1_a_COM, L1_1_b_COM, L1_1_c_COM, L2_1_a_ORG, L2_3_b_ORG | <High Advanced><br>・組織は、自組織のシステムを構成する資産(IoT機器等を含むハードウェア、ソフトウェア、情報)を一意に特定し、各々の資産に管理責任者を割り当てた上で、資産の構成情報(例：名称、バージョン情報、ライセンス情報、場所等)を含めて、リアルタイムで状況を把握しながら目録を維持・管理する。<br>・システムは、認可されていない資産を自動的に検出するメカニズムを導入、運用している。<br>[参考] 重要度の算出方法には、"中小企業の情報セキュリティ対策ガイドライン ver.2.1"(IPA, 2018年)P.30～P.34に記載された情報の機密性、完全性、可用性に関する評価を用いる方法や、"制御システムのセキュリティスク分析ガイド"(IPA, 2018年)のP.21に記載された事業被害の大きさにおける評価を用いる方法等がある | O/S | ○<br>(3.4.2) | ○<br>(下記に加えて、CM-8(1), CM-8(2), CM-8(3), CM-8(5)) | ○<br>(下記に加えて、A.8.1.3) |
| | | | <Advanced><br>・資産の構成情報(例：名称、バージョン情報、ライセンス情報、場所等)を含めて、目録を定期的にレビュー、更新することで維持・管理する。<br>・組織は、システムコンポーネント上で利用可能な取り外し可能なメディア(例：USBメモリ)を一覧化し、使用を管理する。<br>・組織は、ポータブルストレージデバイスに識別可能な所有者がいないとき、このようなデバイスの使用を禁止する。<br>・組織は、機密性の高いデータを含むメディアへのアクセスを制御し、管理エリアの外部への持ち出し中のメディアの利用状況を適切に把握し、管理する。 | O/S | ○<br>(3.4.1, 3.8.5, 3.8.7, 3.8.8) | ○<br>(CM-8, PM-5) | |
| | | | <Basic><br>・組織は、自組織のシステムを構成する資産(ハードウェア、ソフトウェア、情報)を特定し、各々の資産に管理責任者を割り当てた上で、目録として一覧を文書化する。<br>・組織は、洗い出した資産を、自組織の事業運営における重要度に応じて優先順位づけする。<br>[参考] 資産目録(情報資産管理台帳)の作成に当たっては、「中小企業の情報セキュリティ対策ガイドライン」(IPA, 2018年)のP.33を参照することが可能である。 | O | | | ○<br>(A.8.1.1, A.8.1.2) |
| CPS.AM-2 | ・自組織が生産したモノのサプライチェーン上の重要性に応じて、特定方法を定める | L1_2_a_COM | <High Advanced><br>・組織は、トレーサビリティが要求事項となっている場合には、組織はアウトプット(製品)について一意の識別を管理し、トレーサビリティを可能とするために必要な文書化した情報を保持する。<br>・組織は、モノを一意に識別できるような方法を検討する際、異業種間でも通用するよう業種横断的な共通ナンバリングルール等に基づいていることが望ましい。<br>[参考] "ISO9001:2015" 8.5.2 識別及びトレーサビリティ | O | - | - | - |
| | | | <Advanced><Basic>共通<br>・自組織が生産したモノのサプライチェーン上の重要性に応じて、組織は、ナンバーを付与する等アウトプットを識別するために適切な特定方法(例：シリアルナンバーの付与)を定める。<br>・組織は、製造およびサービス提供の全過程において、監視および測定の要求事項に関連してアウトプットの状態を識別する。 | O | - | - | - |
| CPS.AM-3 | ・重要性に応じて、生産日時やその状態等について記録を作成し、一定期間保管するために生産活動の記録に関する内部規則を整備し、運用する | L1_2_a_COM, L1_3_a_COM | <High Advanced><br>・ 生産活動に関する内部規則を整備するとともに、生産したモノの記録については、その重要性に応じて、後日監査を受ける可能性があることを踏まえ、取引先との間であらかじめ重要性について認識を共有し、適切な記録管理レベルを確保する。 | O | - | - | - |
| | | | <Advanced><Basic>共通<br>・生産したモノのサプライチェーン上の重要性に応じて、生産日時やその状態等について記録を作成し、一定期間保管するための生産活動に内部規則を整備し、運用する。 | O | - | - | - |
| CPS.AM-4 | ・組織内の通信ネットワーク構成図及び、データフロー図を作成し、保管する | L1_3_a_ORG, L1_3_b_ORG | <High Advanced><br>・組織は、システム構成、通信ネットワーク構成、データフローをリアルタイムでモニタリングし、管理するための自動化されたメカニズムを導入・管理している。<br>・組織は、システムのベースライン構成のロールバックを可能にするために、旧バージョンのベースライン構成(例えば、ハードウェア・ソフトウェア・ファームウェア・構成ファイル・構成記録)を記録する。 | O | - | ○<br>(下記に加えて、CM-2(2), CM-2(3)) | ○<br>(A.13.2.1, A13.2.2) |
| | | | <Advanced><br>・組織は、作成する図に、ネットワーク接続におけるインターフェース特性、セキュリティ要求事項、伝達されるデータの性質を記載する。 | O | - | ○<br>(下記に加えて、CA-9) | |
| | | | <Basic><br>・組織は、企業内のシステム構成、通信ネットワーク構成、データフローを文書化し、保管する。<br>・組織は、定期的、あるいは、システム構成、ネットワーク構成、データフローに変更が生じた場合、関連する文書をレビューし、必要に応じて更新する。<br>[参考] システム構成、ネットワーク構成、データフローの文書化を行う際の手順については、「制御システムのセキュリティリスク分析ガイド 第2版」(IPA, 2018年)の3.2、3.3を参照することが可能である。 | O | - | ○<br>(CM-2, CM-2(1)) | |
| CPS.AM-5 | ・自組織の資産が接続している外部情報システムの一覧を作成し、保管する | L1_1_a_COM, L1_1_b_COM, L1_1_c_COM, L1_3_a_ORG, L1_3_b_ORG | <High Advanced><br>・システムは、自組織が利用している外部情報サービスを一覧化し、リアルタイムで利用しているサービスとともに利用者・機器等を管理している。<br>・システムは、利用を許可していない外部情報システムサービスを検知した場合、システム管理者へ通知するメカニズムを利用する。<br>・組織は、外部プロバイダによるサービスを使用する際に必要な機能、ポート、プロトコル、および他のサービスを明確にする。 | O/S | ○<br>(3.12.4) | ○<br>(下記に加えて、SA-9(2)) | ○<br>(下記に加えて、A.13.1.2) |
| | | | <Advanced><br>・組織は、外部の情報システムを所有、運用する他の組織に対して、下記を許可するうえでの条件を設定する。<br>a. 外部の情報システムから自組織の情報システムにアクセスすること<br>b. 外部の情報システムを使用して自組織の管理下にある情報を処理または保存もしくは伝送すること<br>・外部のシステム上での自組織のポータブルストレージの使用を制限する。 | O | ○<br>(3.1.20, 3.1.21, 3.12.4) | ○<br>(下記に加えて、AC-20) | |
| | | | <Basic><br>・組織は、自組織が利用している外部情報システムサービスを一覧化し、それぞれのサービスにおけるユーザーとしての役割と責任を定義する。<br>[参考] 特にクラウドサービス利用におけるユーザー側の役割と責任を、契約において規定する際のポイントについて、「クラウドセキュリティガイドライン活用ガイドブック」(経済産業省, 2013年) Appendix A 契約の具体的な内容例と解説 を参照することが可能である。 | O | - | ○<br>(SA-9) | ○<br>(A.6.1.1) |

| 対策要件ID | 対策要件 | 対応する脆弱性 | 対策例 | 対策例を実行する主体 | 参照ガイドライン | | |
|---|---|---|---|---|---|---|---|
| | | | | | NIST SP 800-171 | NIST SP 800-53 rev.4 | ISO/IEC 27001:2013 付属書A |
| CPS.AM-6 | ・リソース（例：ヒト、モノ、データ、システム）を、機能、重要度、ビジネス上の価値に基づいて分類、優先順位付けし、関係者に伝達する | L1_1_a_ORG, L1_1_b_ORG, L1_1_c_ORG | <High Advanced><br>・組織は、あらかじめ優先して継続・復旧すべき中核事業を特定しておき、事業継続の観点から重要なリソース(関係する他組織、ヒト、モノ、データ、システム等)と機能を特定し、優先順位付けする。<br>・組織は、特にフィジカル空間におけるモノの制御等を伴うモノ、システム等の分類、優先付けに当たっては、自組織の事業活動の適切でない運用によりHSE(Health, Safety and Environment)への悪影響が発生するかを考慮して実施する。<br>[参考] モノの制御等を伴うシステムにおける資産の重要度の判断基準については、「制御システムのセキュリティリスク分析ガイド 第2版」4.2.2および4.2.3を参照することができる。 | O | - | ○<br>(下記に加えて、SA-14) | - |
| | | | <Advanced><br>・組織は、リソース(データおよびデータを処理するモノ、システム等)を分類する際には，データを共有又は制限する業務上の要求，及び法的要求事項を考慮する。<br>・当該資産の管理責任者は，そのデータの分類に対して責任を負う。<br>・組織は、リソースの分類体系に，分類の規則及びその分類を時間が経ってからレビューするための基準を含める。 | O | - | ○<br>(RA-2) | ○<br>(A.6.1.1) |
| | | | <Basic><br>・組織は、洗い出した情報資産を、自組織にとっての重要度に応じて優先順位づけする。<br>・関係する法規制等により、自組織のリソース(例：システム、データ)について特定の分類に従うことが要求されている場合、該当する分類を資産に適用する。<br>[参考]重要度の算出方法には、「中小企業の情報セキュリティ対策ガイドライン」(IPA, 2018年) P.30-P.34に記載された情報の機密性、完全性、可用性に関する評価を用いる方法、「制御システムのセキュリティスク分析ガイド」(IPA, 2018年) P.21に記載された事業被害の大きさにおける評価を用いる方法等がある。 | O | - | - | |
| CPS.AM-7 | ・自組織および関係する他組織のサイバーセキュリティ上の役割と責任を定める | L1_3_a_ORG, L1_3_b_ORG | <High Advanced><Advanced>共通<br>・組織は、セキュリティインシデントにより損害が発生する場合に備えて、取引先等から指定されるセキュリティ対策の実装に加え、サイバー保険の利用等によるリスク移転を検討する。 | O | - | - | ○<br>(A.6.1.1, A.15.1.1) |
| | | | <Basic><br>・組織は、委託先あるいは委託元との契約において、業務においてセキュリティインシデントにより損害が発生した場合の自組織と取引先の責任範囲(免責事項の明記、損害賠償額の契約金額等での上限設定等)を規定する。<br>・組織は、契約において取引先に対応を求める/求められるセキュリティに関する要求事項の実効性を高めるため、要求事項への対応要否や過不足、具体的な対応方法や費用負担、対応できない場合の代替措置について契約時あるいは契約期間の初めに合意することが望ましい。 | O | - | ○<br>(SA-4) | |
| CPS.BE-1 | ・サプライチェーンにおいて、自組織が担う役割を特定し共有する | L1_3_a_ORG, L1_3_b_ORG | <High Advanced><br>・自組織において、事業への悪影響を及ぼすセキュリティインシデントが発生した際の、直接的な取引先およびサプライチェーン全体への影響の内容およびその規模を推定する。 | O | - | ○<br>(CP-2, SA-14) | - |
| | | | <Advanced><br>・組織間のモノの流れ、データの流れ等を考慮して、自組織の関係するサプライチェーンの概要を、自組織の全体における役割がわかるように図示する。<br>・上記の結果を関係する他組織(自組織からの発注先、自組織内の関係部門、自組織への発注元)と共有する。 | O | - | - | - |
| | | | <Basic><br>・組織間のモノの流れ、データの流れ等を考慮して、自組織からの発注先、自組織、自組織への発注元という取引関係の概要を、自組織の役割がわかるように図示する。<br>・上記の結果を関係する他組織(自組織からの発注先、自組織内の関係部門、自組織への発注元)と共有する。 | O | - | - | - |
| CPS.BE-2 | ・あらかじめ定められた自組織の優先事業、優先業務と整合したセキュリティポリシー・対策基準を明確化し、関係者(サプライヤー、第三者プロバイダ等を含む)に共有する | L1_1_a_ORG, L1_1_b_ORG, L1_1_c_ORG | <High Advanced><br>・組織は、あらかじめ優先して継続・復旧すべき中核事業および重要と考えられる業務を特定しておき、事業継続の観点から重要なリソース(関係する他組織、ヒト、モノ、データ、システム等)と機能を特定し、優先順位付けする。<br>・組織は、自組織の事業活動の適切でない運用によりHSE(Health, Safety and Environment)への悪影響が発生するかも考慮してリソースの分類、優先順位付けを行う。 | O | - | ○<br>(下記に加えて、SA-14) | - |
| | | | <Advanced><br>・組織は、組織の業務、組織の資産、個人、他の組織等にもたらされるリスクを考慮して、自組織のミッション／業務プロセスを定義し、活動に関する優先順付けを確立する。<br>・組織は、自組織のセキュリティポリシーにおいて規定されている自組織と関係する他組織のセキュリティに関する役割と責任について、関係する他組織に伝達する。 | O | - | ○<br>(PM-11) | ○<br>(A.5.1.1) |
| | | | <Basic><br>・該当なし | - | - | - | - |
| CPS.BE-3 | ・自組織が事業を継続する上での自組織および関係する他組織における依存関係と重要な機能を識別する | L1_3_a_ORG, L1_3_b_ORG | <High Advanced><br>・組織は、自らの事業を継続する上で、重要な依存関係にあるサプライヤーを識別する。<br>・組織は、自らの事業を継続する上で、自組織が有する下記のサポートユーティリティの果たす機能および依存関係を識別する。<br>- 通信サービス<br>- 電力設備(電力ケーブル等を含む)<br>・上記で識別されたユーティリティの内、事業継続という観点から重要な役割を果たすものについて、下記のような対策を講ずることを検討する。<br>- 代替通信サービスの確立<br>- システムの電力設備および電力ケーブルの物理的保護<br>- 短期無停電電源装置の準備<br>・特に、代替通信サービスの利用を検討する際、下記について考慮する<br>- 通信サービス事業者との契約事項を検討する際、組織の可用性に関する要求事項（目標復旧時間を含む）を明確にする<br>- 一次通信サービスとの間で単一障害点が共有される可能性を低減する | O | - | ○<br>(下記に加えて、CP-8, CP-8(1), CP-8(2), PE-9, PE-11) | ○<br>(下記に加えて、A.11.2.2) |
| | | | <Advanced><br>・CPS.AM-6で規定した当該システムの可用性に対する要求水準に応じて、その容量・能力に関する要求事項を特定する。<br>・要求されたシステム性能を満たすことを確実にするために，資源の利用を監視・調整し，また，将来必要とする容量・能力を予測する。 | O | - | ○<br>(SC-5(2)) | ○<br>(A.12.3.1) |
| | | | <Basic><br>・該当なし | - | - | - | - |

| 対策要件ID | 対策要件 | 対応する脆弱性 | 対策例 | 対策例を実行する主体 | 参照ガイドライン | | |
|---|---|---|---|---|---|---|---|
| | | | | | NIST SP 800-171 | NIST SP 800-53 rev.4 | ISO/IEC 27001:2013 付属書A |
| CPS.GV-1 | ・セキュリティポリシーを策定し、自組織および関係する他組織のセキュリティ上の役割と責任、情報の共有方法等を明確にする | L1_1_a_PRO,<br>L1_1_b_PRO,<br>L1_1_c_PRO | <High Advanced><br>・従来のIT環境において運用されているものと基本的な方針を共有しつつ、IoT機器が設置されるサイトの性質等を十分に考慮したセキュリティポリシー群、運用手順を策定する。<br>[参考] 例えば、産業用オートメーション及び制御システム(IACS)を対象としたセキュリティマネジメント規格であるIEC 62443-2-1では、IACS環境のための上位レベルのサイバーセキュリティポリシーの策定を求めている。特に産業分野におけるセキュリティポリシーおよび運用手順の策定にあたっては、"制御システムセキュリティ運用ガイドライン"(日本電気制御機器工業会, 2017年)等を参考とすることができる。 | O | - | ○<br>(controls from all security control families) | ○<br>(A.12.1.1) |
| | | | <Advanced><br>・組織は、上位の方針を支えるセキュリティポリシー群のより低いレベルとして、例えば下記のようなトピック個別の方針および実施手順を策定する。<br>a) アクセス制御および認証<br>b) 物理的セキュリティ対策<br>c) システムの開発および保守<br>d) 外部委託先管理<br>e) 情報分類および取扱い<br>・セキュリティポリシー群の策定に当たっては、自組織の a)事業戦略、b)関係する規制、法令および契約、c)セキュリティの脅威環境 を十分に考慮して、自組織の実情を十分に反映したものとなるよう策定を実施する。<br>・組織は、自組織の a)事業戦略、 b)関係する規制、法令および契約、c)セキュリティの脅威環境 の変化に応じて、セキュリティ方針をレビュー、更新する。<br>[参考] より詳細なレベルの方針策定の際には、ISO/IEC 27002等の関連する標準を参照して方針が必要となる分野を把握したうえで、"中小企業の情報セキュリティ対策ガイドライン ver.2.1"(IPA, 2018年) 付録3や"情報セキュリティポリシーサンプル改版（1.0版）"(JNSA, 2016年)等を参考にすることができる。 | O | - | | ○<br>(A.5.1.1, A12.1.1) |
| | | | <Basic><br>・組織は、自組織のセキュリティポリシー群の最も高いレベルに、セキュリティ基本方針を策定し、経営層の承認を得た後、適切に運用する。<br>・組織は、自組織のセキュリティ方針を定期的(例えば、1年に1度)にレビュー、更新する。<br>[参考] セキュリティポリシーの策定に当たっては、「中小企業の情報セキュリティ対策ガイドライン」付録3における「情報セキュリティ基本方針」や、日本ネットワークセキュリティ協会(JNSA)が公開する「情報セキュリティポリシーサンプル改版（1.0版）」における「01_情報セキュリティ基本方針」、「01_情報セキュリティ方針」等を参考とすることが可能である。 | O | - | | ○<br>(A.5.1.1) |
| CPS.GV-2 | ・個人情報保護法、不正競争防止法等の国内外の法令や、業界のガイドラインを考慮した社内ルールを策定し、法令や業界のガイドラインの更新に合わせて継続的かつ速やかにルールを見直す | L1_3_c_ORG,<br>L1_3_c_COM,<br>L1_3_c_SYS,<br>L1_3_c_PRO,<br>L1_3_c_DAT | <High Advanced><Advanced><Basic>共通<br>・自組織の事業活動において，セキュリティの文脈で関連するすべての法令，規制及び契約上の要求事項，並びにこれらの要求事項を満たすための組織の取組みを，明確に特定し，文書化し，また，最新に保つ。<br>・要求事項を満たすための具体的な管理策及び具体的な責任についても定め，文書化する。<br>・管理者は，その事業の種類に関連した要求事項を満たすために，各自の組織に適用される全ての法令を特定する。<br>・組織が他の国で事業を営む場合には，管理者は，関連する全ての国における遵守を考慮する。<br>[参考] 情報セキュリティ関連法令には例えば、不正競争防止法、電子署名認証法、e-文書法、個人情報保護法、不正アクセス禁止法等がある。 | O | - | ○<br>(controls from all security control families) | ○<br>(A.6.1.3, A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5) |
| CPS.GV-3 | ・各種法令や取決め等によって要求されるデータの保護の水準を的確に把握し、それぞれの要求を踏まえたデータの区分方法を整備し、ライフサイクル全体に渡って区分に応じた適切なデータの保護を行う | L1_1_a_DAT,<br>L1_1_b_SYS,<br>L3_1_a_SYS,<br>L3_1_a_DAT,<br>L3_4_a_ORG,<br>L3_4_a_PRO | <High Advanced><Advanced><Basic>共通<br>・組織は、各システム及び組織について、データ保護に関連する全ての法規制及び契約上の要求事項、並びにこれらの要求事項を満たすための組織の取組みを識別、文書化し、最新に保つ。<br>・組織は、識別したルールの分類に従い、自組織のデータを適切に分類する。<br>・組織は、識別したルールの要求事項に従い、該当するデータを扱うシステム、モノ等に対策を実施する。対策の実装が困難と考えられる場合は、当該データを自組織では非保持扱いとするような対策等の実施を検討することも考えられる。(例：割賦販売法におけるカード情報の非保持化) | O | ○<br>(3.1.22) | ○<br>(controls from all security control families) | ○<br>(A.8.2.1, A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5) |
| CPS.GV-4 | ・サイバーセキュリティに関するリスク管理を適切に行うために戦略策定、リソース確保を行う | L1_1_a_PRO,<br>L1_1_b_PRO,<br>L1_1_c_PRO | <High Advanced><Advanced>共通<br>・組織は、システムの運用と使用により生じる組織の業務と資産、個人、他の組織等に対するリスクを管理するための、包括的なリスクマネジメント戦略を策定する。<br>・組織は、リスクマネジメント戦略を定期的に、あるいは必要な場合にレビューし、更新する。<br>・組織は、すべての資本計画および投資管理プロセスに、セキュリティに関わるリスクマネジメントの実施に必要なリソースが含まれるようにして、この要件に対する例外を文書化する。 | O | - | ○<br>(下記に加えて、PM-3, PM-9) | ○<br>(Clause 6) |
| | | | <Basic><br>・組織は、システムまたはシステムサービスのセキュリティ要求事項を決定するとともに、システムまたはシステムサービスを保護するのに必要なリソースを決定・文書化のうえ割り当てる。<br>・組織は、セキュリティの個々の予算項目を、組織の計画および予算関連の資料に記載する。 | O | - | ○<br>(SA-2) | |
| CPS.RA-1 | ・自組織の資産の脆弱性を特定し、文書化する | L1_1_a_SYS,<br>L1_1_b_SYS,<br>L1_1_c_SYS | <High Advanced><br>・組織は、自組織の管理するシステムにおける既知の脆弱性を認識するため、定期的に侵入テストを実施する。<br>・組織は、ツールを用いて脆弱性診断を行う場合、診断すべきシステムの脆弱性をすぐに更新できる脆弱性診断ツールを使用する。<br>・組織は、脆弱性診断に際して、診断者に特権アクセスの権利を一時的に許可する制度を整備することで、より徹底した脆弱性の洗い出しを行う。 | O | - | ○<br>(下記に加えて、CA-8, RA-5(1), RA-5(5)) | ○<br>(A.12.6.1) |
| | | | <Advanced><br>・組織は、脆弱性診断を実施し、自組織の所有するシステムに存在する脆弱性を認識し、一覧化する。<br>・組織は、自組織の所有するシステムの運用段階において、各種ソースから収集した脆弱性の内、自組織に関連することが想定されるものに対して、脆弱性検査ツール等を用いて、定期的に自組織のシステムにおける脆弱性を特定し、当該脆弱性の影響度とともに一覧に追加する。<br>[参考]脆弱性情報の取得に際して、Japan Vulnerability Notes(https://jvn.jp/)等の情報源を参照することが可能である。また、脆弱性の影響の大きさを評価する指標として、CVSS(IPAによる解説：https://www.ipa.go.jp/security/vuln/CVSS.html)を参考とすることが可能である。 | O | - | ○<br>(RA-5, RA-5(2)) | |
| | | | <Basic><br>・「中小企業の情報セキュリティ対策ガイドライン」付録3における対策状況チェック等の、セキュリティ対策のベースラインとなる文書を活用して、自組織の管理策上の脆弱性を把握する。 | O | - | - | - |
| | ・セキュリティ対応組織(SOC/CSIRT)は、組織の内部及び外部の情報源(内部テスト、セキュリティ情報、セキュリティ研究者等)から脆弱性情報/脅威情報等を収集、分析し、対応および活用するプロセスを確立する | L1_2_a_ORG,<br>L2_1_a_ORG,<br>L2_1_c_SYS,<br>L3_1_a_SYS, | <High Advanced><br>・セキュリティに関わる研究会や会議等に出席したり、セキュリティの専門家による協会・団体との適切な連絡体制を維持することにより、セキュリティに関わる知識を最新のものとする。<br>・主に自社が提供している製品・サービスにおいて、新たな脆弱性が含まれていないかを分析し、発見した場合、IPAに関連情報を届け出る。 | O | - | ○<br>(下記に加えて、PM-15) | |

| 対策要件ID | 対策要件 | 対応する脆弱性 | 対策例 | 対策例を実行する主体 | 参照ガイドライン | | |
|---|---|---|---|---|---|---|---|
| | | | | | NIST SP 800-171 | NIST SP 800-53 rev.4 | ISO/IEC 27001:2013 付属書A |
| CPS.RA-2 | | L3_3_a_SYS,<br>L3_3_d_SYS, | <Advanced><br>・組織は、セキュリティ管理責任者を中心に、セキュリティ対応組織を立ち上げ、組織内でセキュリティ対策を取る体制を整える。<br>・組織は、情報処理推進機構(IPA)、JPCERT/CC、業界ISACのような組織や、取引関係のある機器ベンダー、ソフトウェアベンダーより、随時脆弱性情報、脅威情報等を収集し、自組織の資産目録と照らし合わせることで、対応要否を判断する。<br>[参考]セキュリティ対応組織の構想、構築、運用に当たっては、外部事業者からのサービスを利用するほかに、JPCERT/CCから公開されている「CSIRTマテリアル」、日本セキュリティオペレーション事業者協議会から公開されている「セキュリティ対応組織（SOC/CSIRT）の教科書 ～ 機能・役割・人材スキル・成熟度～」等の文書を利用することが可能である。 | O | - | ○<br>(下記に加えて、PM-16) | ○<br>(下記に加えて、A.6.1.4) |
| | | | <Basic><br>・組織は、セキュリティ管理責任者およびセキュリティ対策担当者を任命することで、組織内におけるセキュリティの役割と責任を明確化する。<br>・組織は、利用中の機器ベンダーやソフトウェアベンダーが提供するセキュリティに関わる注意喚起情報を確認し、自組織内の関係者に伝達する。 | O | - | ○<br>(SI-5) | ○<br>(A.6.1.1) |
| CPS.RA-3 | ・自組織の資産に対する脅威を特定し、文書化する | L1_1_a_SYS,<br>L1_1_b_SYS,<br>L1_1_c_SYS | <High Advanced><br>・組織は、セキュリティに関わる研究会や会議等に出席したり、セキュリティの専門家による協会・団体との適切な連絡体制を維持することにより、セキュリティ脅威に関わる知識を最新のものとする。 | O | - | ○<br>(下記に加え、PM-15) | ○<br>(下記に加え、A.6.1.4) |
| | | | <Advanced><br>・組織は、公開された新たな攻撃動向、マルウェア挙動情報や悪性IP アドレス/ドメイン情報などの情報（外部インテリジェンス）を収集する。<br>・組織は、得られた脅威情報の信頼度、自組織に与える影響などを評価し、対応すべき脆弱性を取捨選択し、対応する脅威について文書化する。 | O | - | ○<br>(下記に加え、PM-16) | - |
| | | | <Basic><br>・組織は、「中小企業の情報セキュリティ対策ガイドライン」付録3における脅威の状況等の、セキュリティ脅威洗い出しのベースラインとなる文書を活用して、自組織に関わるセキュリティ脅威およびその発生しやすさを把握する。 | O | - | - | ○<br>(Clause 6.1.2) |
| CPS.RA-4 | ・構成要素の管理におけるセキュリティルールが、実装方法を含めて有効かを確認するため、定期的にリスクアセスメントを実施する<br>・IoT機器およびIoT機器を含んだシステムの企画・設計の段階から、受容できない既知のセキュリティリスクの有無を、セーフティに関するハザードの観点も踏まえて確認する | L1_1_a_SYS,<br>L1_1_b_SYS,<br>L1_1_c_SYS,<br>L2_1_a_ORG<br>L2_1_a_PRO<br>L2_2_a_ORG | <High Advanced><br>・組織は、モノの制御等を伴うような、フィジカル空間に影響を及ぼす可能性のある新たな機器やシステムを開発する場合には、従来の製品や他の事故事例を収集・分析し、セーフティに関わるハザードを特定する。<br>・組織は、ハザードによって被害に至る状況を分析し、発生しやすさや被害の深刻度を明らかにすることで、生じるリスクを見積もる。その際、セキュリティの問題に起因するハザードの有無を確認することが望ましい。<br>[参考]セーフティ設計におけるハザードの特定と分析については、「つながる世界のセーフティ＆セキュリティ設計入門」(IPA, 2015年)の4.2にて具体的な手法が記載されており、参照することが可能である。 | O | - | - | ○<br>(A.12.6.1, A.18.2.2, A.18.2.3) |
| | | | <Advanced><br>・組織は、システム、またはシステムが稼働する環境に大きな変化があった場合(新たな脅威や脆弱性の特定を含む)、もしくはシステムのセキュリティ状態に影響を与える他の状況が発生した場合に、リスクアセスメントを更新する。<br>・組織は、新たにIoT機器を利用したシステムを企画・設計する場合、既存の資産や新たに導入するシステムにおける守るべき資産を特定し、システムの利用用途や構成に応じて、セキュリティ対策をまとめる。特に、ライフサイクルの長いモノ、システムや、高い可用性を求められるモノ、システムを扱う場合は、設計以前の段階におけるセキュリティ対策の考慮が特に重要である。<br>・組織は、調達する製品・サービスに対するセキュリティ対策を検討する際、当該製品・サービスの重要度に対策の水準が見合うものであることを確実にする。<br>[参考]システムおよびモノにおけるセキュリティの要求仕様を検討するにあたり、「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」(NISC, 2015年)、「非機能要求グレード」(IPA, 2018年)を参考にすることが可能である。 | O | ○<br>(3.11.1) | ○<br>(下記に加え、SA-12(2)) | |
| | | | <Basic><br>・組織は、セキュリティリスクアセスメントのプロセスを定め，定期的(例えば、年に1回)に適用する。<br>- セキュリティのリスク基準を確立し，維持する。<br>- 以下の方法によりセキュリティリスクを特定する。<br>1) 分析対象を明確化する<br>2) インシデント(周辺状況の変化を含む)並びにこれらの原因を特定する<br>- 以下の方法により、セキュリティリスクを分析する。<br>1) 上記で特定されたリスクが実際に生じた場合に起こり得る結果について評価する<br>2) 上記で特定されたリスクの現実的な起こりやすさについて評価する<br>- リスク基準を参照し、リスクのレベルを決定し、優先順位付けする<br>・組織は，情報セキュリティリスクアセスメントのプロセスを文書化し、保管する。<br>[参考] セキュリティリスクアセスメントの手法として、「資産ベース」の手法および「事業被害ベース」の手法があることが知られている。資産ベースの手法でアセスメントを実施する場合は、「中小企業の情報セキュリティガイドライン」(IPA, 2018年)や「制御システムのセキュリティリスク分析ガイド 第2版」(IPA, 2018年) 等を、事業被害ベースの手法を実施する場合は、「制御システムのセキュリティリスク分析ガイド 第2版」(IPA, 2018年)等を参照することができる。 | O | - | ○<br>(RA-3) | ○<br>(Clause 6.1.2, A.18.2.2, A.18.2.3) |
| | ・リスクを判断する際に、脅威、脆弱性、可能性、影響を考慮する | L1_1_a_SYS,<br>L1_1_b_SYS,<br>L1_1_c_SYS | <High Advanced><br>・該当なし | - | - | - | - |
| | | | <Advanced><br>・組織は、システム、またはシステムが稼働する環境に大きな変化があった場合(新たな脅威や脆弱性の特定を含む)、もしくはシステムのセキュリティ状態に影響を与える他の状況が発生した場合に、リスクアセスメントを更新する。その際、重要度の高いシステムを優先的に対応する。<br>※CPS.RA-4と共通の実施内容 | O | - | | ○<br>(A.12.6.1) |

| 対策要件ID | 対策要件 | 対応する脆弱性 | 対策例 | 対策例を実行する主体 | 参照ガイドライン | | |
|---|---|---|---|---|---|---|---|
| | | | | | NIST SP 800-171 | NIST SP 800-53 rev.4 | ISO/IEC 27001:2013 付属書A |
| CPS.RA-5 | | | <Basic><br>・組織は、セキュリティリスクアセスメントのプロセスを定め，定期的(例えば、年に1回)に適用する。<br>- セキュリティのリスク基準を確立し，維持する。<br>- 以下の方法によりセキュリティリスクを特定する。<br>1) 分析対象を明確化する<br>2) インシデント(周辺状況の変化を含む)並びにこれらの原因を特定する<br>- 以下の方法により、情報セキュリティリスクを分析する。<br>1) 上記で特定されたリスクが実際に生じた場合に起こり得る結果について評価する<br>2) 上記で特定されたリスクの現実的な起こりやすさについて評価する<br>- リスク基準を参照し、リスクのレベルを決定し、優先順位付けする<br>・組織は，情報セキュリティリスクアセスメントのプロセスを文書化し、保管する。<br>※CPS.RA-4と共通の実施内容<br>[参考]セキュリティリスクアセスメントの手法として、「資産ベース」の手法および「事業被害ベース」の手法があることが知られている。資産ベースの手法でアセスメントを実施する場合は、「中小企業の情報セキュリティガイドライン」や「制御システムのセキュリティリスク分析ガイド」等を、事業被害ベースの手法を実施する場合は、「制御システムのセキュリティリスク分析ガイド」等を参照することができる。 | O | - | ○<br>(RA-3) | ○<br>(Clause 6.1.2) |
| CPS.RA-6 | ・リスクアセスメントに基づき、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定め、対応の範囲や優先順位を整理した結果を文書化する<br>・IoT機器およびIoT機器を含んだシステムの企画・設計の段階におけるアセスメントにて判明したセキュリティおよび関連するセーフティのリスクに対して適宜対応する | L1_1_a_SYS,<br>L1_1_b_SYS,<br>L1_1_c_SYS,<br>L2_1_a_ORG,<br>L2_1_a_PRO | <High Advanced><br>・CPS.RA-4で実施したハザード分析の結果に基づき、必要な場合、重要なハザードにつながりうるセキュリティに係るリスク源に対して適切に対応する。<br>[参考] 特に安全制御系におけるセキュリティ面の統合については、近年国際標準化の場でも議論がなされており、IEC TR 63074, IEC TR 63069等を参照することが可能である。 | O | - | - | ○<br>(A.5.1.2) |
| | | | <Advanced><br>・組織は，セキュリティリスク対応のプロセスについての文書化した情報を安全に保管する。<br>・組織は、リスクアセスメントの結果に応じて対応策を選定する際、実施する対応策および当該対応策を採用する理由を文書化することが望ましい。<br>・組織は、対応策の適用等に関して、セキュリティリスク対応計画を策定し、リスク所有者の承認を得る。<br>・組織は、セキュリティリスク対応計画をレビューし、当該計画が、自組織全体のリスクマネジメント戦略における優先順位に適合しているかどうかを確認する。<br>・CPS.RA-4で抽出した、IoT機器を含む新しいシステムにおける必要なセキュリティ対策について、然るべき外部事業者に要求仕様として伝達する。<br>・組織は、IoT機器を含むシステムの導入時に、要求仕様や契約段階で定めたセキュリティ対策が実施されているかを受け入れ検査などで確認する。もし、不明な点があれば、外部事業者に確認する。 | O | ○<br>(3.12.4) | ○<br>(PM-4) | ○<br>(Clause 6.1.3, Clause 8.3, A.5.1.2) |
| | | | <Basic><br>・組織は，次の事項を行うために，リスクアセスメントの結果を考慮して，対応策を選定する。<br>・セキュリティリスクの受容について，リスク所有者の承認を得る。 | O | - | - | |
| CPS.RM-1 | ・自組織だけでなく、関係者と共同でセキュリティリスクの管理プロセスを確立、承認し、運用する | L1_1_a_PRO,<br>L1_1_b_PRO,<br>L1_1_c_PRO,<br>L1_3_a_ORG,<br>L1_3_b_ORG | <High Advanced><br>・組織は、リスクマネジメント戦略の策定時および改定時に、重要度の高い取引先との間で、リスクマネジメント戦略に関するインタビューを実施することで、セキュリティ上のリスクや必要な対策に関する認識を合致させる。その際、下記事項を扱うことが望ましい。<br>- 自組織の事業内容および事業の継続に関わる主なセキュリティリスク<br>- 上記リスクが顕在化した際の、取引先における影響の内容とその規模<br>- 上記セキュリティリスクへの対応方針<br>- (リスクマネジメント戦略改定時の場合)内外の情勢の変化および前回の版から変更すべきと考える主要なポイント | O | - | - | - |
| | | | <Advanced><br>・組織は、システムの運用と使用により生じる組織の業務と資産、個人、他の組織等に対するリスクを管理するための、包括的なリスクマネジメント戦略を策定する。<br>・組織は、リスクマネジメント戦略を組織全体にわたって一貫性が保たれるように実施する。<br>・組織は、リスクマネジメント戦略を定期的に、あるいは組織的変化に対処するために必要な場合にレビューし、更新する。<br>・組織の経営層は，組織の リスクマネジメント戦略を定期的にをレビューする。その際、下記を明確にする。<br>- 前回までの経営層によるレビューの結果とった処置の状況<br>- 関連する外部及び内部の課題の変化<br>- セキュリティパフォーマンスに関するフィードバック<br>- 利害関係者からのフィードバック<br>- リスクアセスメントの結果及びリスク対応計画の状況<br>- 継続的改善の機会<br>・組織は，経営層によるレビューの結果を文書化し、保管する。 | O | - | ○<br>(PM-9) | ○<br>(Clause 9.3) |
| | | | <Basic><br>・該当なし | - | - | - | - |
| CPS.RM-2 | ・リスクアセスメント結果およびサプライチェーンにおける自組織の役割から自組織におけるリスク許容度を決定する | L1_1_a_SYS,<br>L1_1_b_SYS,<br>L1_1_c_SYS | <High Advanced><br>・CPS.BE-1にて実施しているサプライチェーンに係るリスクの現状把握および、CPS.RA-4等で実施しているリスクアセスメントの結果を所与として、自組織におけるリスク許容度を決定する。<br>・自組織におけるセキュリティインシデントにより望ましくない影響を受ける可能性がある重要な取引先に対して、自組織のリスク許容度に関するインタビューを実施する。 | O | - | ○<br>(下記に加えて、SA-14) | - |
| | | | <Advanced><br>・CPS.BE-1にて実施しているサプライチェーンの現状把握および、CPS.RA-4等で実施しているリスクアセスメントの結果を所与として、自組織におけるリスク許容度を決定する。 | O | - | | ○<br>(Clause 6.1.3, Clause 8.3) |
| | | | <Basic><br>・組織は、CPS.RA-4等で実施しているリスクアセスメントの結果を所与として、自組織におけるリスク許容度を決定する。<br>・組織は、残存しているリスクの受容について，リスク所有者の承認を得る。<br>・組織は、リスク対応結果を文書化し、リスク許容度の基準および許容したリスクの一覧を安全に保持する。 | O | - | ○<br>(PM-8) | |

| 対策要件ID | 対策要件 | 対応する脆弱性 | 対策例 | 対策例を実行する主体 | 参照ガイドライン | | |
|---|---|---|---|---|---|---|---|
| | | | | | NIST SP 800-171 | NIST SP 800-53 rev.4 | ISO/IEC 27001:2013 付属書A |
| CPS.SC-1 | ・サプライチェーンに係るセキュリティの対策基準を定め、責任範囲を明確化したうえで、その内容について関係者と合意する | L1_1_a_ORG,<br>L1_1_b_ORG,<br>L1_1_c_ORG | <High Advanced><br>・組織は、取引先(外部情報システムサービスのプロバイダ)に対して、サービスの使用に必要な機能、ポート、プロトコル、および他のサービスを明確にする。 | O | - | ○<br>(SA-9(2)) | |
| | | | <Advanced><br>・組織は、サプライチェーンに係るセキュリティ対策基準を参照して、ITT(Invitation To Tender)やRFP(Request For Proposal)などの入札書類を準備し、潜在的な取引先に提供する。特に、入札書類には以下が含まれることが望ましい。<br>1）調達する製品またはサービスの仕様<br>2）供給者が製品またはサービスを供給している間に従うセキュリティ要件<br>3）製品またはサービスの供給中に従うべきサービスレベルおよびその指標<br>4）セキュリティ要件に違反した場合に、委託元が課す可能性のある罰則<br>5）取引先の選定プロセス中に送信されるデータやシステムなどを保護するための秘密保持条項<br>・組織は、取引先によるセキュリティ管理策の遵守状況を継続的にモニタリングするための、プロシージャを整備する。<br>・取引先におけるセキュリティインシデントが自組織に影響した場合に備え、契約書にて外部事業者との責任分界点を明確にし、外部事業者の責任範囲において自組織に被害が発生した場合の損害賠償について記載する等の対応を行う。 | O | - | ○<br>(SA-9) | ○<br>(下記に加え、A.15.2.1) |
| | | | <Basic><br>・組織は、該当する法規制等を参照して、取引先(特に、自組織のデータを取り扱う可能性のある，またはデータを取り扱うための基盤を提供する可能性のあるもの)に対して適用するセキュリティ対策基準を策定し、内容について合意する。<br>[参考] 取引先に対して適用するセキュリティ対策基準の策定に当たり、IPAによりISO/IEC 27001 附属書Aの管理策をベースに作成された「情報セキュリティベンチマーク」や、JASA(日本セキュリティ監査協会)「サプライチェーン情報セキュリティ管理基準」等を参考とすることが可能である。 | O | - | | ○<br>(A.15.1.1, A.15.1.2) |
| CPS.SC-2 | ・自組織の事業を継続するに当たり重要なサプライヤーを特定、優先付けをし、評価する<br>・機器調達時に、適切なマネジメントシステムが構築・運用され、問い合わせ窓口やサポート体制等が確立されたIoT機器のサプライヤーを選定する<br>・サービスやシステムの運用において、サービスマネジメントを効率的、効果的に運営管理するサービスサプライヤーを選定する | L1_1_a_ORG,<br>L1_1_b_ORG,<br>L1_1_c_ORG,<br>L2_1_a_COM,<br>L2_1_a_PRO,<br>L2_1_a_DAT,<br>L2_3_a_ORG,<br>L2_3_c_ORG,<br>L3_1_b_ORG,<br>L3_3_d_ORG,<br>L3_1_c_ORG,<br>L3_3_a_ORG,<br>L3_3_b_ORG | <High Advanced><br>・組織は、あらかじめ優先して継続・復旧すべき中核事業を特定しておき、当該事業を運用するにあたり極めて重要なリソース(関係する他組織、ヒト、モノ、データ、システム等)と機能を特定し、優先順位付けする。<br>・取引先において、事業への悪影響を及ぼすセキュリティインシデントが発生した際の、自組織への影響の内容および、その起こりやすさ、規模を推定する。<br>※関連する対策要件に、CPS.AM-6, CPS.BE-2等がある。 | O | - | ○<br>(下記に加えて、SA-14) | ○<br>(A.15.1.1, A.15.1.2) |
| | | | <Advanced><br>・組織は、自組織のミッション/業務プロセスに重要な影響を及ぼしうるサプライチェーン上の取引先を特定し、当該組織が自組織のセキュリティポリシーに規定されているセキュリティ上の役割と責任を果たせるかどうかを確認する。 | O | - | | |
| | | | <Basic><br>・組織は、長期に渡ってIoT機器が使用されることが想定される場合、長期間のサポートが期待できる取引先(機器ベンダ)を選定する。<br>・組織は、機器のサポート終了時に機器を入れ替えることの要否についてシステムの導入前に取引先(機器ベンダ)に対して確認する。<br>・組織は、取引先(サービスプロバイダー)の選定に当たり、JIS Q 20000に基づくITSMS認証等を取得するか、あるいは自己適合確認により認証取得相当の対策の実装を確認しており、提供するITサービスのマネジメントを効率的、効果的に運営管理するサービスプロバイダーを選定することが望ましい。 | O | - | ○<br>(SA-4) | |
| CPS.SC-3 | ・外部の関係者との契約を行う場合、目的およびリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織のセキュリティマネジメントが適合していることを確認する | L1_1_a_ORG,<br>L1_1_a_PRO,<br>L1_1_a_DAT,<br>L1_1_b_PRO,<br>L1_1_c_PRO,<br>L1_1_d_ORG,<br>L2_3_c_ORG,<br>L3_1_b_ORG,<br>L3_1_b_DAT,<br>L3_3_d_ORG,<br>L3_1_c_ORG,<br>L3_1_c_DAT,<br>L3_3_a_ORG,.<br>L3_3_b_ORG,<br>L3_3_c_ORG,<br>L3_4_a_DAT | <High Advanced><br>・組織は、システム・モノ・サービスのいずれかを提供する取引先との契約において、当該組織に対して、下記の実施を要求する。<br>- セキュリティアセスメント計画の作成<br>- テスト／評価の適切な範囲での実施<br>- セキュリティアセスメント計画を実施したエビデンスの作成、セキュリティテスト／評価結果の提示<br>- 検証可能な欠陥修正プロセスの実施<br>- セキュリティテスト／評価時に特定された欠陥の修正<br>・組織は、直接の委託先に対して要求しているセキュリティ対策に関する要求事項およびそれに付随する要求事項の内で必要な事項を、サプライチェーンに由来するリスクの大きさ等を勘案し、再委託先以降の組織に対しても適用することが望ましい。<br>[参考] 関連情報の取得のためには、「ITサプライチェーンの業務委託におけるセキュリティインシデント及びマネジメントに関する調査報告書」(IPA, 2018年)等を参照することが可能である。 | O | - | ○<br>(下記に加え、SA-11) | ○<br>(A.13.2.4, A.15.1.2)- |
| | | | <Advanced><br>・組織のミッション／業務ニーズに応じて、システム、モノ、またはサービスの調達契約に以下の要求事項、記述、および基準を記載する。<br>- セキュリティ対策に関する要求事項<br>- セキュリティ関連のドキュメントに関する要求事項<br>- セキュリティ関連のドキュメントの保護に関する要求事項<br>- 秘密保持に関する条項<br>- インシデントが発生した際の報告先、報告内容、初動、調査、復旧等の各対応の実施主体、実施方法<br>- 自組織または認可された第三者によって監査され、定義されたセキュリティ要件への遵守を確認することを許可する条件<br>- 契約終了後の情報資産の扱い<br>・組織は、取引先に対して、該当する法規制等に準拠したセキュリティ要求事項を実施し、委託内容の特性等により必要と認められる場合、調達契約において、追加で対策を導入することを要求する。<br>・法規制等を参照してセキュリティ要件を決定し、取引先へ遵守を要求する際、下記を事前に考慮することが望ましい。<br>- 自組織と取引先の間の法令の相違によって生じる潜在的な法的規制リスクの特定<br>- 取引先に適用される法律および規制上の義務によるセキュリティの観点からの契約への悪影響 | O | - | ○<br>(下記に加え、SA-4) | |
| | | | <Basic><br>・組織は、取引先に対して、該当する法規制等に準拠したセキュリティ要求事項を実施することを要求する。 | O | - | ○<br>(SA-9) | |
| | ・外部の関係者との契約を行う場合、目的およびリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織の提供する製品・サービスが適合していることを確認する | L1_1_a_ORG,<br>L1_1_a_DAT,<br>L1_1_a_PRO,<br>L1_1_b_PRO, | <High Advanced><br>・調達する機器に対して、契約におけるセキュリティ要求事項が満たせているかを、自組織あるいは第三者がテストする。<br>・組織は、自組織のオペレーションにとって特に重要な機器について、再委託先以降の組織を含む関係するサプライチェーン全体に渡り、一定水準以上の品質管理能力、セキュリティマネジメント能力等を有した組織により、適切なプロシージャで製造されたものかを確認する。 | O | - | - | ○<br>(下記に加え、A.14.3.1) |

| 対策要件ID | 対策要件 | 対応する脆弱性 | 対策例 | 対策例を実行する主体 | 参照ガイドライン | | |
|---|---|---|---|---|---|---|---|
| | | | | | NIST SP 800-171 | NIST SP 800-53 rev.4 | ISO/IEC 27001:2013 付属書A |
| CPS.SC-4 | | L1_1_c_PRO,<br>L1_1_d_ORG,<br>L1_1_d_COM,<br>L2_1_a_ORG,<br>L2_1_a_COM,<br>L2_1_a_PRO,<br>L2_2_a_ORG,<br>L2_3_a_ORG,<br>L2_3_c_ORG,<br>L2_3_c_PRO,<br>L3_1_b_ORG,<br>L3_3_a_ORG,<br>L3_3_b_ORG,<br>L3_3_c_ORG,<br>L3_3_d_ORG | <Advanced><br>・組織は、契約において、例えば下記のように、取引先から調達する製品・サービスが具備すべきセキュリティ要求事項を明確化する。<br>- セキュリティに関わる特定の認証(例：ISMS認証、ISASecure EDSA認証、ITセキュリティ評価及び認証制度(JISEC))を有していること<br>- ベンダー自身により、セキュリティに関わる特定の認証の基準に適合する対策を実施していることが確認されていること<br>- リスク分析の結果等から導かれた必要なセキュリティ要件を設計時からの実装（セキュリティ・バイ・デザイン）し、検査していること<br>・組織は、調達計画時に、製品またはサービス自体、あるいは当該製品・サービスの調達・供給にて使用される資産の保護に係るセキュリティ要件の費用を確保しておくことが望ましい。<br>・下記を含む製品またはサービスの調達または供給を評価するためのセキュリティ測定ルールを策定し、運用および改善する。<br>- 測定対象の内容<br>- 措置の報告方法、報告の頻度<br>- 措置が実施されない場合に遂行される措置<br>・組織は、搬送中の改ざん・漏えいを検知(又は抑止)する手段とともに納品されるIoT機器やソフトウェアが、不正操作されていないかを確認する。<br>- 物品：セキュリティ便、プロテクトシール等<br>- 電送：暗号化、電送データ全体のハッシュ値等 | O | - | - | ○<br>(A.8.3.3, A.14.1.1, A.14.2.9, A.15.1.3) |
| | | | <Basic><br>・組織は、調達時に、自組織が所有するIoT機器が正規品であるかをラベルを確認する等して確かめる。<br>・組織は、IoT機器やソフトウェアに含まれるIDや秘密鍵、電子証明書等を用いて調達した機器が正規品であることを確認する。 | O | - | - | - |
| CPS.SC-5 | ・取引先等の関係する他組織が、契約上の義務を果たしていることを確認するために、監査、テスト結果、または他の形式の評価を使用して定期的に評価する | L1_1_a_SYS,<br>L2_3_c_ORG,<br>L3_1_b_ORG,<br>L3_1_e_ORG,<br>L3_1_e_DAT,<br>L3_3_e_ORG, | <High Advanced><br>・組織は、契約事項からの逸脱および、その兆候に対する調査・対応のためのプロシージャをサポートするレビュー・分析・レポートのそれぞれについて、一体的に扱う自動的なメカニズムを採用する。<br>・組織は、特に重要な取引先およびその再委託先以降の組織に対して、契約にて規定した組織のセキュリティマネジメント、納入する製品・サービスに実装されるセキュリティ機能等に関する義務事項が履行されているかどうかを一覧化して確認できるメカニズムを利用する。<br>・委託元による実地調査、外部監査等の手法により、外部サービスプロバイダによるセキュリティ管理策の遵守状況を定期的に確認する。 | O | ○<br>(下記に加えて、3.3.5) | ○<br>(下記に加えて、AU-6(1), AU-6(3)) | ○<br>(A.12.7.1, A.14.3.1, A.15.2.1) |
| | | L3_1_f_ORG,<br>L3_1_f_DAT,<br>L3_1_g_ORG ,<br>L3_3_f_ORG,<br>L3_1_g_ORG,<br>L3_3_a_ORG,<br>L3_3_c_ORG, | <Advanced><br>・組織は、自組織が取引先との契約において要求事項として規定した内容に関連して、システム上での監査が可能かどうか、確認する。<br>・上記で定義されているシステム上で監査可能なイベントのために、監査記録を生成する機能をシステムが提供する。<br>・組織は、監査に関連する情報が必要な他の組織との間で、セキュリティ監査の整合性を保つことができるようにする。<br>・組織は、手作業ないしはシステムにより自動で生成された監査記録を定期的にでレビュー・分析して、契約事項からの逸脱および、その兆候の有無を確認する。<br>・チェックリストを用いた取引先による内部監査により、外部サービスプロバイダによるセキュリティ管理策の遵守状況を定期的に確認する。 | O | ○<br>(3.3.1) | ○<br>(AU-2, AU-6, AU-12, SA-9) | |
| | | L3_3_d_ORG,<br>L3_4_a_DAT | <Basic><br>・各種認証・制度(ISMS認証、CSMS認証、Pマーク等)の取得証明書を確認することで、必要なセキュリティ対策実施確認の代替とする。 | O | - | - | - |
| CPS.SC-6 | ・取引先等の関係する他組織に対する監査、テストの結果、契約事項に対する不適合が発見された場合に実施すべきプロシージャを策定し、運用する。 | L1_1_a_PRO,<br>L1_1_b_PRO,<br>L1_1_c_PRO,<br>L1_1_d_ORG,<br>L2_2_a_ORG,<br>L2_3_c_ORG, | <High Advanced><br>・組織は、取引先の監査あるいはテストの不適合が発見された場合、下記を実施するプロシージャを策定し、運用する。<br>1）不適合から生じるセキュリティの影響を特定し評価する<br>2）契約で定義されているセキュリティに関わる規定を再検討すべきかどうかを判断する<br>3）調達された製品またはサービスの範囲内で許容可能なセキュリティレベルを取得するために、実施すべき是正措置を決定する。<br>4）上記を取引先と同意する | O | - | - | - |
| | | L2_3_c_PRO,<br>L3_1_b_ORG,<br>L3_1_c_ORG, | <Advanced><br>・組織は、取引先の監査あるいはテストの不適合が発見された場合、取引先に対して改善計画の策定を求め、計画の実施状況について必要に応じて確認するプロシージャを策定し、運用する。 | O | - | - | - |
| | | L3_3_a_ORG,<br>L3_3_b_ORG, | <Basic><br>・該当なし | - | - | - | - |
| CPS.SC-7 | ・自組織が関係する他組織との契約上の義務を果たしていることを証明するための情報(データ)を収集、安全に保管し、必要に応じて適当な範囲で開示できるようにする | L1_1_d_ORG,<br>L2_2_a_ORG,<br>L2_3_c_ORG,<br>L2_3_c_PRO,<br>L3_1_b_ORG,<br>L3_1_c_ORG, | <High Advanced><br>・組織は、取引先、第三者的な監査機関等の関係する他組織からのリアルタイムでのニーズに柔軟に応じるため、下記の特徴を有した証跡保管システムを利用する。<br>- 対象となる監査証跡の契約事項に対する適格性を高速で検証することができる<br>- 取引先や委託を受けた監査機関等の許可を受けたエンティティのみがアクセスできる<br>- 保管されているデータが、タイムスタンプや電子署名により証跡としての信頼性を有している | O | - | - | ○<br>(A.12.4.1, A.18.1.3) |
| | | L3_3_a_ORG,<br>L3_3_b_ORG,<br>L3_3_c_ORG | <Advanced><br>・組織は、システムによって生成された監査記録のうち長期にわたって取得する監査記録を確実に取得できるよう、対策を実施する。<br>・システムは、監査記録を次の脅威から保護するため、粒度の高いアクセス制御等を監査記録を保存するモノ、システムに適用することが望ましい。<br>- 記録されたメッセージ形式の変更<br>- ログファイルの変更又は削除<br>- ログファイル媒体の記録容量超過 | O/S | - | ○<br>(下記に加えて、AU-9, AU-11(1)) | |
| | | | <Basic><br>・組織は、法規制等により要求される事項を満たす事ができるよう、適切な期間の監査記録を保持する。 | O | - | ○<br>(AU-11) | |
| CPS.SC-8 | ・取引先等の関係する他組織の要員の内、自組織から委託する業務に関わる者に対するセキュリティ上の要求事項を策定し、運用する | L1_1_a_PEO,<br>L1_1_b_PEO,<br>L1_1_c_PEO, | ＜High Advanced＞<br>・組織は、委託先の要員により委託元が要求するセキュリティ要求事項が遵守されているかどうかを継続的にモニタリングし、通常とは異なる行動があった場合、自組織の担当者に通知できるようにプロシージャを整備する。 | O | - | ○<br>(PS-7) | ○<br>(A.16.1.2, A.16.1.5)- |
| | | L2_3_b_PEO,<br>L3_1_b_PEO,<br>L3_1_c_PEO | ＜Advanced＞<br>・サプライヤー関係のセキュリティ面について該当する要員を訓練し、機密情報の取り扱いが正しく理解されていることを特に確認する。<br>・委託業務の遂行に当たり、委託元が要求するセキュリティ要求事項が遵守されていることを定期的に確認する。 | O | | | |

| 対策要件ID | 対策要件 | 対応する脆弱性 | 対策例 | 対策例を実行する主体 | 参照ガイドライン | | |
|---|---|---|---|---|---|---|---|
| | | | | | NIST SP 800-171 | NIST SP 800-53 rev.4 | ISO/IEC 27001:2013 付属書A |
| | | | ＜Basic＞<br>・委託業務に係るデータの内、機密データや知的財産のように、公開または変更すべきではないものへのアクセスおよびデータの開示または変更に関わる要員を特定し、評価する。<br>・組織は、委託先との契約の終了後、速やかに委託先の要員に対する自組織施設へのアクセス権限等の、一時的に許可していた権限を停止する。 | O | | | |
| CPS.SC-9 | ・サプライチェーンにおけるインシデント対応活動を確実にするために、関係者間で対応プロセスの整備と訓練を行う | L1_3_a_PEO | <High Advanced><br>・組織は、サプライチェーンにおけるセキュリティインシデントの対処を想定し、自組織とサプライチェーンに関与する他の組織との間で、インシデント対応活動を調整するプロシージャを整備する。<br>・組織は、サプライチェーンにおけるセキュリティインシデントの対処を想定し、サプライチェーンに関与する他の組織との間で、インシデント対応活動を調整するテストを実施する。<br>[参考]サプライチェーンにおけるセキュリティインシデントには、たとえば、システムコンポーネント、IT 製品、開発プロセスまたは開発者、流通過程または倉庫施設に対する侵害等がある。 | O | ○<br>(3.6.1, 3.6.3) | ○<br>(下記に加えて、IR-4, IR-4(10)) | - |
| | | | <Advanced><br>・組織は、インシデント対応要件が満たされるよう、自組織のインシデント対応プロセスと、自組織の事業継続上、重要な機能を有する外部サービスプロバイダのインシデント対応プロセスを調整する。<br>・組織は、自組織と外部サービスプロバイダーとの間で連携を要するインシデント対応プロセスをテストする。 | O | ○<br>(3.6.1, 3.6.3) | (CP-2, CP-2(7)) | - |
| | | | <Basic><br>・該当なし | - | - | - | - |
| CPS.SC-10 | ・取引先等の関係する他組織との契約が終了する際(例：契約期間の満了、サポートの終了)に実施すべきプロシージャを策定し、運用する。 | L1_1_a_PRO,<br>L1_1_b_PRO,<br>L1_1_c_PRO | <High Advanced><br>・組織は、製品またはサービスの供給に必要な自組織のリソースにアクセスしそれを処理するために相手方に付与された論理的および物理的アクセス権が、契約終了後に適時に削除されることを保証する。 | O | - | - | - |
| | | | <Advanced><br>・組織は、製品またはサービスの供給が取り消されるか、または自組織または他の取引先に返還されるかどうかを現在の取引先と決定する。<br>・組織は、製品またはサービスの供給によって影響を受けるヒトにその終了に関する情報を提供するためのコミュニケーションを行う。<br>・組織は、終了計画に従い、製品またはサービス供給の終了を実行する。<br>・組織は、提供された製品またはサービスの終了の達成について、取引先と同意する。 | O | - | - | - |
| | | | <Basic><br>・該当なし | - | - | - | - |
| CPS.SC-11 | サプライチェーンに係るセキュリティ対策基準および関係するプロシージャ等を継続的に改善する。 | L1_1_a_PRO,<br>L1_1_b_PRO,<br>L1_1_c_PRO | <High Advanced><Advanced><Basic>共通<br>・取引先のセキュリティに関わるパフォーマンスを継続的にモニタリングし、最新の脅威動向、規制動向等を踏まえ、サプライチェーンに係るセキュリティ対策基準および、それに付随するプロシージャをレビューし、必要に応じて改定する。 | O | - | - | - |
| CPS.AC-1 | ・承認されたモノとヒトおよびプロシージャの識別情報と認証情報を発効、管理、確認、取消、監査する | L1_1_b_SYS,<br>L2_3_c_SYS,<br>L3_3_a_SYS,<br>L3_1_d_SYS | <High Advanced><br>・組織は、自組織のシステムアカウントの管理について自動化されたメカニズムを導入し、運用している。<br>・システムは、自組織のシステムの一時利用アカウントや緊急アカウント、用されていないアカウントについて、一定期間の経過後に自動的に無効にする。<br>・システムは、自組織が利用するシステムのアカウント作成・変更・削除に伴うアカウントの有効化および無効化について自動的に監査・報告する。 | O/S | - | ○<br>(下記に加え、AC-2 (1), AC-2 (2), AC-2 (3), AC-2(4)) | ○<br>(下記に加え、A.9.2.4, A.9.2.5) |
| | | | <Advanced><br>・組織は、システムアカウントの利用状況をモニタリングする。<br>・組織は、アカウントが不要にな-った場合や変更が必要となった場合には管理責任者に通知する。 | O | - | ○<br>(AC-2) | |
| | | | <Basic><br>・組織は、自組織のシステムのアカウントを管理する管理責任者を配置する。<br>・組織は、組織のミッションや業務機能を考慮して、必要なシステムアカウント種別(例：一般ユーザ/システム管理者)を識別・選択する。<br>・組織は、プロシージャに従ってシステムアカウントを作成、有効化し、必要に応じて変更・無効化・削除を実施する。<br>・組織は、システムアカウントの作成に当たっては、管理責任者による承認を必須とする。 | O | - | | ○<br>(A.9.1.1, A.9.2.1, A.9.2.2, A.9.2.6) |
| CPS.AC-2 | ・IoT機器、サーバ等の設置エリアの施錠、入退室管理、生体認証等の導入、監視カメラの設置、持ち物や体重検査等の物理的セキュリティ対策を実施する | L1_1_a_SYS,<br>L2_3_b_PEO,<br>L2_3_b_SYS,<br>L3_1_a_SYS | <High Advanced><br>・組織は、自組織のIoT機器、サーバ等に関わる配電線及び回線に対して物理アクセスによる制御を実施する。<br>・組織は、自組織のシステムの出力装置に対して物理アクセスによる制御を実施する。<br>・組織は、自組織の施設に対する物理的な侵入について警報と監視装置(例：監視カメラ)をモニタリングする。 | O | - | ○<br>(下記に加え、PE-4, PE-5, PE-6 (1)) | ○<br>(下記に加えて、A11.1.1.4, A11.2.3) |
| | | | <Advanced><br>・組織は、自組織のIoT機器、サーバ等が設置されているエリアに対する物理アクセスをモニタリングし、定期的に監査ログのレビューを実施する。<br>・組織は、自組織のIoT機器、サーバ等が設置されているエリアに対する来客のアクセス記録を、一定期間保管するとともに定期的にレビューを実施する。 | O | ○<br>(3.10.2, 3.10.4, 3.10.5) | ○<br>(下記に加え、PE-6, PE-8) | ○<br>(下記に加え、A.11.1.1, A.11.1.5) |
| | | | <Basic><br>・組織は、自組織のIoT機器、サーバ等が設置されているエリアに対するアクセスリストの維持管理及びアクセスに必要な許可証明書を発行する。<br>・組織は、自組織の施設内の一般の人がアクセスできるエリアを定め、必要に応じてアクセス制御を実施する。<br>・組織は、自組織のIoT機器、サーバ等が設置されているエリアに対する来客について、付き添う等して来客の行動をモニタリングする。 | O | ○<br>(3.10.1, 3.10.3) | ○<br>(PE-2, PE-3, PE-8) | ○<br>(A.9.2.6, A.11.1.2, A.11.1.3, A.11.1.6, A.11.2.8, A.11.2.9) |
| CPS.AC-3 | ・無線接続先(ユーザーやIoT機器、サーバ等)を正しく認証する | L2_3_c_SYS,<br>L3_3_a_SYS | <High Advanced><br>・システムが、自組織のシステムに関するリモートアクセスについて、自動モニタリングまたは自動制御を実施する。<br>・システムは、管理されたアクセスポイントによりルーティングされたリモートアクセスだけを許可する。<br>・システムは、定めた要求に基づく目的のみリモートアクセスによる特権コマンドの実行を認可する。<br>・システムは、機密性の高いデータを扱うシステムにアクセスしたユーザがリモートアクセスによって特権コマンドを実行した理由とともに、リモートアクセスによってセキュリティ関連情報にアクセスした理由を記録する。<br>・システムは、機密性の高いデータを扱うシステムへの無線アクセスは、ユーザおよび機器による認証を暗号化とともに用いることによって保護する。<br>・システムは、機密性の高いデータを扱う可能性のあるネットワークでつながっているホワイトボード、カメラ、マイク等の連携する機器をリモートから活性化することを禁止し、機器の利用者に利用中の機器の兆候を提供する。 | S | ○<br>(下記に加えて、3.1.12, 3.1,13, 3.1.14, 3.1.15, 3.1.17, 3.1.19, 3.10.6, 3.13.12, 3.13.15) | ○<br>(下記に加え、AC-17(1), AC-17(2), AC-17(3), AC-17(4), AC-18(1), AC-19(5)) | - |
| | | | <Advanced><br>・組織は、自組織で利用する携帯機器を制限し、携帯機器の設定要件、接続要件、実装ガイダンス等を定める。<br>・組織は、自組織で利用する携帯機器から自組織のシステムの接続に関する承認ルール等を定める。 | O | ○<br>(下記に加えて、3.1.18) | ○<br>(下記に加え、AC-19) | ○<br>(下記に加え、A.6.2.1) |

| 対策要件ID | 対策要件 | 対応する脆弱性 | 対策例 | 対策例を実行する主体 | 参照ガイドライン | | |
|---|---|---|---|---|---|---|---|
| | | | | | NIST SP 800-171 | NIST SP 800-53 rev.4 | ISO/IEC 27001:2013 付属書A |
| | | | <Basic><br>・組織は、許可しているリモートアクセスのタイプごとに使用制限・構成要件・実装ガイダンス等を定める。<br>・組織は、自組織のシステムへのリモートアクセスの利用に関する承認ルール等を定める。<br>・組織は、自組織のシステムへの無線によるアクセスを許可するのに先立って、無線でシステムにアクセスする権限を与える。 | O | ○<br>(3.1.16) | ○<br>(AC-17, AC-18) | ○<br>(A.6.2.2) |
| CPS.AC-4 | ・一定回数以上のログイン認証失敗によるロックアウトや、安全性が確保できるまで再ログインの間隔をあける機能を実装する等により、IoT機器、サーバ等に対する不正ログインを防ぐ | L2_1_b_SYS,<br>L3_3_a_SYS | <High Advanced><br>・システムは、自組織のシステムに対してユーザが連続してログオンを失敗できる上限を設定し、上限以上失敗した場合には管理者が解除しなければ再ログインできない機能を実装する。 | S | ○<br>(3.1.8) | ○<br>(AC-7) | ○<br>(A.9.4.2) |
| | | | <Advanced><br>・システムは、自組織のシステムに対してユーザが連続してログオンを失敗できる上限を設定し、上限以上失敗した場合には一定期間再ログインできない機能を実装する。 | S | ○<br>(3.1.8) | | |
| | | | <Basic><br>・組織は、自組織のシステムに対するパスワードポリシーを定め、そのポリシーを満たすパスワードでなければ設定できない機能を実装する。 | O/S | - | - | - |
| CPS.AC-5 | ・ユーザーが利用する機能と、システム管理者が利用する機能を分離する | L1_1_b_SYS,<br>L2_1_c_SYS,<br>L3_1_a_SYS | <High Advanced><br>・組織は、アクセス権限設定等のセキュリティ機能を利用する管理者を明示し、自組織のシステムにおける特権アカウントを制限する。<br>・組織は、非セキュリティ機能を利用する場合には、非特権アカウントでの利用を要求する。<br>・システムは、特権的機能の使用をチェックするため、システムが監査するメカニズムを導入している。<br>・システムは、非特権ユーザによって変更されて実装されたセキュリティ対策を無効にするとともに回避・変更する等、システムが非特権ユーザによる特権的機能の実行を禁止する。 | O/S | ○<br>(下記に加えて、3.1.6, 3.1.7) | ○<br>(下記に加え、AC-6(1), AC-6(2), AC-6(5), AC-6(9), AC-6(10)) | ○<br>(A.6.1.2, A.9.2.3, A.9.4.1, A.9.4.4) |
| | | | <Advanced><br>・組織は、自組織のシステムにおいて職務分離(例：ユーザ/システム管理者)を踏まえたアクセス制御を実施する。<br>・組織は、特定の職務権限に対して最小権限の原則を採用する。<br>・組織は、担当者によって割り当てられた職務を分離し、明文化する。 | O | ○<br>(3.1.4, 3.1.5, 3.13.3) | ○<br>(下記に加え、AC-3, AC-5, AC-6, SC-2) | |
| | | | <Basic><br>・人的リソース等の関係で、職務の分離が困難な場合、あらかじめ指定された役職者以外が特定の職務を実行する際に、他の要員が職務の遂行をモニタリングする等の代替策を講ずることが望ましい。 | O | - | - | - |
| CPS.AC-6 | ・特権を持つユーザーのシステムへのへのネットワーク経由でのログインに対して、二つ以上の認証機能を組み合わせた多要素認証を採用する | L2_1_c_SYS,<br>L3_1_a_SYS | <High Advanced><br>・システムは、自組織のシステムについて非特権アカウントでのシステムやネットワーク等へのアクセスに対して多要素認証を実施する。<br>・機密性の高いデータを取り扱う自組織のシステムについて、特権アカウントまたは非特権アカウントでのシステムやネットワーク等へのアクセスに対して、リプレイ攻撃に対する耐性のある認証メカニズムを実施する。<br>[参考] 認証方式の強度および適切な利用ケースに関しては、NIST SP 800-63-3 を参照することが望ましい。 | S | ○<br>(下記に加えて、3.5.4) | ○<br>(下記に加え、IA-2(2), IA-2(8), IA-2(9)) | ○<br>(下記に加えて、A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4) |
| | | | <Advanced><br>・システムは、自組織のシステムについて特権アカウントでのシステムやネットワーク等へのアクセスに対して多要素認証を要求する。 | S | ○<br>(下記に加えて、3.5.3) | ○<br>(下記に加え、IA-2(1), IA-2(3)) | |
| | | | <Basic><br>・組織は、自組織のシステムについて特権アカウントまたは非特権アカウントでのシステムやネットワーク等へのアクセスに対して、一意に識別する認証を実施する。 | O/S | ○<br>(3.5.1) | ○<br>(IA-2) | ○<br>(A.9.2.1) |
| CPS.AC-7 | ・適宜ネットワークを分離する(例：開発・テスト環境と実運用環境、IoT機器を含む環境と組織内の他の環境)等してネットワークの完全性を保護する | L1_1_b_SYS,<br>L2_1_b_SYS,<br>L3_1_d_SYS | <High Advanced><br>・機密性の高いデータを取り扱う自組織のシステムの繋がるネットワークについては、ネットワーク通信をデフォルトで拒否するものとし、許可した通信トラフィックのみ接続可とする。<br>・機密性の高いデータを取り扱う自組織のシステムが遠隔地にある装置とコネクションを確立している場合、その装置がシステムとの間でローカル接続を複数同時に確立するのを阻止すると同時に、別の接続によって外部ネットワークのリソースにアクセスできないようにする。 | S | ○<br>(下記に加えて、3.1.3, 3.13.6, 3.13.7) | ○<br>(下記に加え、SC-7(5), SC-7(7)) | ○<br>(下記に加え、A.13.1.1, A.13.1.3, A.14.1.2, A.14.1.3) |
| | | | <Advanced><br>・システムは、自組織のシステムの繋がるネットワークにおける外部境界及び内部境界について通信をモニタリングし、制御する。<br>・組織は、自組織のシステムの有効なセキュリティを促進する設計として境界保護装置等を設置し、それ介して外部ネットワーク等に接続する。 | O/S | - | ○<br>(下記に加え、SC-7) | |
| | | | <Basic><br>・組織は、システム内でデータフローが許可される範囲やシステム間におけるデータフローが許可される範囲を定めたデータフロー制御ポリシーを定め、フローの制御を実施する。 | O/S | ○<br>(3.1.3) | ○<br>(AC-4) | ○<br>(A.12.1.4, A.13.2.1) |
| CPS.AC-8 | ・IoT機器、サーバ等がサイバー空間で得られた分析結果を受信する際、及びIoT機器、サーバ等が生成した情報(データ)をサイバー空間へ送信する際、双方がそれぞれ接続相手のID(識別子)を利用して、接続相手を識別し、認証する<br>・IoT機器での通信は、通信を拒否することをデフォルトとし、例外として利用するプロトコルを許可する | L2_1_b_SYS,<br>L3_3_a_SYS | <High Advanced><Advanced><Basic>共通<br>・組織は、自組織のIoT機器、サーバ等について識別子を割り当てるとともに、識別子が再利用することを防止、一定期間が経過した識別子を無効にすることで、識別を管理する。<br>・システムは、自組織のIoT機器、サーバ等について、ネットワークでの接続を確立する前に、それらのデバイスを一意に識別し、認証する仕組みを備える。<br>・IoT機器での通信は、通信を拒否することをデフォルトとし、例外として利用するプロトコルを許可する。 | O/S | ○<br>(3.5.5, 3.5.6, 3.8.2) | ○<br>(IA-4) | ○<br>(A.7.1.1, A.9.2.1) |
| | ・IoT機器やユーザーを、取引のリスク(個人のセキュリティ、プライバシーのリスク、及びその他の組織的なリスク)に見合う形で認証する | L1_1_b_SYS,<br>L2_1_b_SYS<br>L3_1_a_SYS | <High Advanced><br>・システムは、特に機密性の高いデータを取り扱う自組織のシステムへのログインについて、公開鍵基盤を利用した認証を要求する。<br>・システムは、自組織のシステムについて、セッションの切断が必要な条件を設定し、その条件に該当する場合にはユーザのセッションを自動的に終了させる機能を実装する。 | S | ○<br>(下記に加えて、3.1.11) | ○<br>(下記に加え、IA-2, IA-5(2), AC-12) | |

| 対策要件ID | 対策要件 | 対応する脆弱性 | 対策例 | 対策例を実行する主体 | 参照ガイドライン | | |
|---|---|---|---|---|---|---|---|
| | | | | | NIST SP 800-171 | NIST SP 800-53 rev.4 | ISO/IEC 27001:2013 付属書A |
| CPS.AC-9 | | | <Advanced><br>・組織は、ユーザの身元を確認し、取引のリスク(個人のセキュリティ、プライバシーのリスク等)に見合うメカニズムの強度を持った認証を実施する。<br>・システムは、ユーザが自組織のシステムにログインする際に、取引のリスク(個人のセキュリティ、プライバシーのリスク等)に関する通知メッセージ等を表示する。<br>・システムは、認証されたユーザに対して、実行可能なトランザクションおよび機能を制限する。<br>・組織は、パスワードによる認証を行う場合には、以下のことを満たすこととする。<br>- パスワードに最低限必要な複雑さを確保するため、パスワードに求める要求事項を定め、運用する。<br>- 新しいパスワードが作成される際には、少なくとも組織が定めた文字数に変更させる。<br>- 暗号によって保護されたパスワードのみを保存・伝送する。<br>- パスワードの有効期間を組織が設定する。<br>- 同じパスワードを組織が定めた世代にわたって再利用するのを禁止する。<br>- 強固なパスワードにすぐに変更するのを条件に、システムへのログオン時に、一時的なパスワードを使用することを許可する。<br>・システムは、自組織のシステムについて認証プロセス時に認証情報のフィードバックを見えないようにする。<br>・システムは、自組織のシステムについて、ユーザによる認証後に一定時間アクセスがない場合には、ユーザによる再アクセスがあるまで、スクリーンセーバー等に画面を切替えた上で、セッションをロックする。 | O/S | ○<br>(3.1.1, 3.1.2, 3.1.9, 3.1.10, 3.5.2, 3.5.7, 3.5.8, 3.5.9, 3.5.10, 3.5.11) | ○<br>(下記に加え、IA-5, IA-5(1), IA-6, AC-8, AC-11, AC-11(1)) | ○<br>(A.9.3.1, A.9.4.3, A.9.4.5) |
| | | | <Basic><br>・該当なし | - | - | - | - |
| CPS.AT-1 | ・自組織の全ての要員に対して、セキュリティインシデントの発生と影響を抑制するために割り当てられた役割と責任を遂行するための適切な訓練、教育を実施する | L1_1_a_PEO,<br>L1_1_b_PEO,<br>L1_1_c_PEO,<br>L1_1_d_PEO,<br>L1_2_a_PEO,<br>L1_3_b_PEO,<br>L3_4_a_PEO | <High Advanced><br>・組織は、内部不正の兆候を認識・報告するためのセキュリティ意識向上トレーニングを、全要員に対して実施する。 | O | ○<br>(下記に加えて、3.2.3) | ○<br>(下記に加え、AT-2(2)) | ○<br>(A.7.2.1, A.7.2.2) |
| | | | <Advanced><br>・組織は、基本的なセキュリティ意識向上トレーニングを定期的に全職員に対して実施する。<br>・組織は、情報セキュリティ要員の育成とレベル向上のための役割別(例：システム/ソフトウェア開発者、調達担当者、システム管理者、セキュリティ対策担当者)のプログラムを作成し、定期的に該当する要員に対して実施する。 | O | ○<br>(3.2.1) | ○<br>(下記に加え、AT-3) | |
| | | | <Basic><br>・組織は、自組織の利用するシステムに対する変更により必要になった場合や新規職員に対して基本的なセキュリティ意識向上トレーニングを実施する。 | O | - | ○<br>(AT-2) | |
| CPS.AT-2 | ・自組織におけるセキュリティインシデントに関係しうる関係組織の担当者に対して、割り当てられた役割を遂行するための適切な訓練(トレーニング)、セキュリティ教育を実施する | L1_3_c_PEO,<br>L3_3_a_PEO | <High Advanced><br>・組織は、自組織の要員及びセキュリティインシデントに関係しうる関係組織に対して、担当する要員へ割り当てられた役割の遂行状況をモニタリングを実施する。 | O | | - | - |
| | | | <Advanced><br>・組織は、自組織におけるセキュリティインシデントに関係しうる関係組織に対して、担当する要員へ割り当てられた役割を遂行するための適切な訓練、セキュリティ教育を実施を要求し、その実施状況を確認する。 | O | ○<br>(下記に加え、3.2.2) | - | - |
| | | | <Basic><br>・組織は、自組織の要員へ割り当てられた役割を遂行するための適切な訓練、セキュリティ教育を実施を要求し、その実施状況を確認する。 | O | ○<br>(3.2.1) | - | - |
| CPS.DS-1 | ・情報(データ)を適切な強度の方式で暗号化して保管する | L1_1_a_DAT,<br>L1_1_a_SYS,<br>L3_1_a_SYS,<br>L3_3_d_SYS | <High Advanced><br>・組織は、選択したアルゴリズムをソフトウェア及びハードウェアへ適切に実装し、暗号化された情報の復号又は電子署名の付与に用いる鍵、識別コード及び主体認証情報等を保護するため、暗号モジュール試験及び認証制度に基づく認証を取得している製品を選択する。<br>・自組織の保護すべきデータを組織外へ持ち出す場合、データを適切な強度で暗号化する。<br>[参考] 暗号技術検討会及び関連委員会（CRYPTREC）では、安全性及び実装性能が確認された暗号技術について、市場における利用実績が十分であるか今後の普及が見込まれると判断され、当該技術の利用を推奨するもののリストを「電子政府における調達のために参照すべき暗号のリスト」（CRYPTREC暗号リスト）として公開している。組織は、暗号機能を実装すべきシステム等を調達する場合、必要に応じて参照することが望ましい。 | O/S | ○<br>(下記に加え、3.8.6, 3.13.11, 3.13.8) | ○<br>(下記に加えSC-12(1)) | ○ (A.8.2.3) |
| | | | <Advanced><br>・組織は、必要とされる安全性及び信頼性について検討を行い、アルゴリズムを選択し、情報(データ)を適切な強度の方式で暗号化して保管する。CRYPTREC暗号リストに記載されたアルゴリズムが選択可能であれば、これを選択し、情報(データ)を適切な強度の方式で暗号化して保管する。 | O/S | ○<br>(下記に加え、3.13.16) | ○（下記に加えSC-28） | |
| | | | <Basic><br>・組織は、必要とされる安全性及び信頼性について検討を行い、アルゴリズムを選択し、情報(データ)を適切な強度の方式で暗号化して保管する。 | O/S | ○<br>(3.13.10) | ○（SC-12） | |
| CPS.DS-2 | ・IoT機器、サーバ等の間、サイバー空間で通信が行われる際、通信経路を暗号化する | L1_1_a_SYS,<br>L1_1_b_DAT,<br>L3_1_a_SYS,<br>L3_2_b_DAT,<br>L3_3_d_SYS, | <High Advanced><br>・組織は、重要なデータを扱う通信路について、通信経路の暗号化を実装するか、あるいは、代替の物理面での対策によって保護する。 | S | ○<br>(3.13.15) | ○(下記に加えてSC-12(1)) | ○<br>(A.10.1.1,A.13.2.1、A.13.2.3, A.14.1.2) |
| | | | <Advanced><br>・システムは、暗号メカニズムを導入し、通信経路を暗号化する。<br>[参考] 通信経路の暗号化には、IP-VPN、Ipsec-VPN、SSL-VPN等の方式が存在する。組織は、通信路を流れるデータの重要度や、かけられるコスト等を考慮しつつ、方式を選定することが望ましい。 | S | ○<br>(3.13.15) | ○(SC-8(1), SC-12) | |
| | | | <Basic><br>・該当なし | - | - | - | - |
| | ・情報(データ)を送受信する際に、情報(データ)そのものを暗号化して送受信する | L1_1_a_SYS,<br>L1_1_b_DAT,<br>L3_1_a_SYS, | ＜High Advanced＞<br>・システム/IoT機器は、少ないリソースでも可用性を損なわずに実装可能な暗号モジュールを導入し、重要度の高い機器からの通信データを適切な強度で暗号化することが望ましい。 | S | - | - | ○<br>(A.10.1.1, A.13.2.1, A.13.2.3 |

| 対策要件ID | 対策要件 | 対応する脆弱性 | 対策例 | 対策例を実行する主体 | 参照ガイドライン | | |
|---|---|---|---|---|---|---|---|
| | | | | | NIST SP 800-171 | NIST SP 800-53 rev.4 | ISO/IEC 27001:2013 付属書A |
| CPS.DS-3 | | L3_2_b_DAT, L3_3_d_SYS | <Advanced><br>・システムは、情報の伝送中に、不正な 情報の開示を防ぎ、情報に対する変更を検出するために、暗号メカニズムを導入し、情報(データ)を暗号化して送受信する。 | S | - | ○ (SC-8(1)) | A.10.1.1, A.10.2.1, A.13.2.3, A.14.1.2) |
| | | | <Basic><br>・該当なし | - | - | - | - |
| CPS.DS-4 | ・送受信データ、保管データの暗号化等に用いる鍵を、ライフサイクルを通じて安全に管理する。 | L1_1_a_DAT, L3_1_a_SYS | ＜High Advanced＞<br>・組織は、ユーザが暗号鍵を紛失した場合に、情報の可用性を維持する。<br>・秘密鍵及びプライベート鍵をセキュリティを保って管理することに加え，公開鍵の真正性についても考慮することが望ましい。この認証プロセスは，認証局によって通常発行される公開鍵証明書を用いて実施される。この認証局は，要求された信頼度を提供するために適切な管理策及び手順を備えている，認知された組織であることが望ましい。 | O/S | - | ○ (下記に加え、SC-12(1)) | ○ (A10.1.2) |
| | | | <Advanced><br>・組織は、秘密鍵が危殆化した際に遅滞なく適切な対処を行うため、必要に応じて下記のような事項について方針及び手順を定めることが望ましい。<br>- 秘密鍵の危殆化に対応するための体制(関係者と役割、委託先との連携を含む)<br>- 秘密鍵が危殆化した、またはその恐れがあると判断するための基準<br>- 秘密鍵の危殆化の原因を調べること、及び、原因の解消を図ること<br>- 当該鍵を利用するサービスの利用停止<br>- 新しい鍵ペアを生成し、新しい鍵に対する証明書を発行すること<br>- 秘密鍵の危殆化についての情報の開示(通知先、通知の方法、公表の方針等)<br>[参考] 鍵管理に関するより詳細な内容については、ISO/IEC 11770規格群や、NIST SP 800-57 Part 1 Rev.4等を参照することが望ましい。 | O | ○ (3.13.10) | ○ (SC-12) | |
| | | | <Basic><br>・組織は、全ての暗号鍵を，改変及び紛失から保護することが望ましい。 | O | | | |
| CPS.DS-5 | ・サービス拒否攻撃等のサイバー攻撃を受けた場合でも、サービス活動を停止しないよう、モノ、システムに十分なリソース(処理能力、通信帯域、ストレージ容量)を確保する | L2_1_d_SYS, L1_1_c_SYS, L3_3_c_SYS | <High Advanced><Advanced>共通<br>・システムは、組織が定めたセキュリティ対策を実施することによって、組織が定めたタイプのサービス拒否攻撃、またはそうした情報の情報源への参照のサービス拒否攻撃による影響から保護する、あるいはそうした影響を最小限に抑える。<br>・システムは、予備の容量 / 帯域幅 / その他の予備を管理して、大量の情報を送りつけるタイプのサービス拒否攻撃による影響を最小限に抑える。<br>・要求されたシステム性能を満たすことを確実にするために，資源の利用を監視・調整しなければならず，また，将来必要とする容量・能力を予測しなければならない。<br>・組織は、<br>(a) 情報システムに対するサービス妨害攻撃の兆候を発見するための組織が定めた、モニタリングツールを使用する<br>(b) 組織が定めた情報システムリソースをモニタリングして、効果的なサービス妨害攻撃を阻止するための十分なリソースが確保されているかどうかを判断する。 | S | - | ○（下記に加えてSC-5(2)、SC-5(3)） | ○<br>（下記に加えて、A.12.1.3） |
| | | | <Basic><br>・システムは、組織が定めたセキュリティ対策を実施することによって、組織が定めたタイプのサービス拒否攻撃、またはそうした情報の情報源への参照のサービス拒否攻撃による影響から保護する、あるいはそうした影響を最小限に抑える。 | S | - | ○（SC-5） | ○<br>（A.17.2.1） |
| CPS.DS-6 | ・IoT機器、通信機器、回線等に対し、定期的な品質管理、予備機や無停電電源装置の確保、冗長化、故障の検知、交換作業、ソフトウェアの更新を行う | L2_1_d_SYS, L3_3_b_SYS, L3_3_d_SYS | <High Advanced><Advanced>共通<br>・要求されたシステム性能を満たすことを確実にするために，資源の利用を監視・調整しなければならず，また，将来必要とする容量・能力を予測する。<br>・装置は，サポートユーティリティの不具合による，停電，その他の故障から保護する。<br>・データを伝送する又は情報サービスをサポートする通信ケーブル及び電源ケーブルの配線は，傍受，妨害又は損傷から保護する。<br>・装置は，可用性及び完全性を継続的に維持することを確実にするために，正しく保守する。<br>・組織は、一次電源が失われた場合に、情報システムの長期間使用可能な代替電源への切り替えを支援する、短期無停電電源装置を用意する。 | O | - | ○（PE-11） | ○（A.11.2.2、A.11.2.3、A.11.2.4、A.12.1.3, A.17.2.1） |
| | | | <Basic><br>・要求されたシステム性能を満たすことを確実にするために，資源の利用を監視・調整しなければならず，また，将来必要とする容量・能力を予測する。<br>・装置は，サポートユーティリティの不具合による，停電，その他の故障から保護する。<br>・データを伝送する又は情報サービスをサポートする通信ケーブル及び電源ケーブルの配線は，傍受，妨害又は損傷から保護する。<br>・装置は，可用性及び完全性を継続的に維持することを確実にするために，正しく保守する。 | O | - | - | ○（A.11.2.2、A.11.2.3、A.11.2.4、A.12.1.3, A.17.2.1） |
| CPS.DS-7 | ・保護すべき情報を扱う、あるいは自組織にとって重要な機能を有する機器を調達する場合、耐タンパーデバイスを利用する | L1_1_d_COM, L2_3_b_COM | <High Advanced><br>・組織は、保護すべき情報を扱う、あるいは自組織にとって重要な機能を有する機器を調達する場合、耐タンパーデバイスを利用した機器を調達する。<br>：組織は、情報システム内で使用されている暗号技術向けの暗号鍵を保管するにあたり耐タンパーデバイスを用いて管理する。 | O | - | ○（SC-12） | ○（A.10.1.2） |
| | | | <Advanced><br>・該当なし | - | - | - | - |
| | | | <Basic><br>・該当なし | - | - | - | - |
| CPS.DS-8 | ・自組織の保護すべきデータが不適切なエンティティに渡ったことを検知した場合、ファイル閲覧停止等の適切な対応を実施する | L1_1_a_DAT, L3_1_a_SYS | <High Advanced><br>・組織は、自組織の保護すべきデータが不適切なエンティティに渡らないように、自動化されたメカニズムを利用して検知を実施する。<br>・共有システム資源を介した、不正な予期せぬ情報の転送を防止する。 | S | ○<br>(3.13.4) | ○<br>（下記に加えて、IR-4(1)） | ○<br>(A.16.1.5) |
| | | | <Advanced><br>・組織は、自組織の保護すべきデータが不適切なエンティティに渡ったことを検知した場合には、インシデントの把握・影響の拡大防止策を実施する。<br>・組織は、発生したインシデントに関して慣例責任者・関係部署・関係組織への連絡するとともに、証拠や記録等を保全する。 | O/S | - | ○<br>(IR-4) | |
| | | | <Basic><br>・該当なし | - | - | - | - |
| CPS.DS-9 | ・IoT機器、サーバ等の起動時に、起動するソフトウェアの完全性を検証し、不正なソフトウェアの起動を防止する | L2_3_b_SYS | <High Advanced><br>・組織は、完全性検証時に不一致が発見された場合にシステム管理者に通知する、自動化されたツールを使用する。<br>・組織は、設定の不正な変更や、システム権限の不正な昇格等の、セキュリティ関連の変更が不正に行われた場合の検知能力を、組織のインシデント対応能力に組み入れる。 | O/S | - | ○<br>（下記に加えて、SI-7(2), SI-7(7)） | ○<br>(A.12.2.1) |

| 対策要件ID | 対策要件 | 対応する脆弱性 | 対策例 | 対策例を実行する主体 | 参照ガイドライン | | |
|---|---|---|---|---|---|---|---|
| | | | | | NIST SP 800-171 | NIST SP 800-53 rev.4 | ISO/IEC 27001:2013 付属書A |
| CPS.DS-9 | | | <Advanced><br>・システムは、ソフトウェア・ファームウェアの完全性チェックを定期的に実施する。 | O/S | - | ○<br>(SI-7, SI-7(1)) | |
| | | | <Basic><br>・該当なし | - | - | - | |
| CPS.DS-10 | ・送受信・保管する情報(データ)に完全性チェックメカニズムを使用する | L1_1_b_DAT, L1_1_d_PRO, L3_2_a_DAT, L3_2_b_DAT | <High Advanced><br>・組織は、、設定の不正な変更や、システム権限の不正な昇格等の、セキュリティ関連の変更が不正に行われた場合の検知能力を、組織のインシデント対応能力に組み入れる。 | O | - | ○<br>(下記に加えて、SI-7(7)) | ○<br>(A.14.1.2, A.14.1.3) |
| | | | <Advanced><br>・組織は、完全性検証ツールを使用して、IoT機器、サーバ等からの通信データに対する不正な変更を検知する。<br>・システムは、保管データの完全性チェックを定期的に実施する。 | O/S | - | ○<br>(SI-7, SI-7(1)) | |
| | | | <Basic><br>・該当なし | - | - | - | - |
| CPS.DS-11 | ・ハードウェアの完全性を検証するために整合性チェックメカニズムを使用する | L1_1_d_PRO, L2_3_b_SYS | ＜High Advanced＞<br>・組織は、IC チップの純正品と不正品のサイドチャネル情報の違いからハードウェアの改ざん(ハードウェア・トロイの挿入)を検知する。<br>・組織は、PUF（Physically unclonable function）の技術を活用して物理的に読取り可能なチップの固有IDを生成し、テストを通じてハードウェアの改ざん(ハードウェア・トロイの挿入)を検知する。 | O | - | - | - |
| | | | <Advanced><br>・組織は、ハードウェアコンポーネントに対する不正な変更を検知するツール、複製しにくいラベルや、検証可能なシリアル番号等を用いて、完全性を確認できるようにする。<br>・組織は、自組織のオペレーションにとって重要なハードウェアについて、設置エリアに対して監視カメラ等によるモニタリングを行うことで、ハードウェアに対する物理的な改ざんを検知できるようにする。 | O | - | ○<br>(PE-6, SA-10(3)) | - |
| | | | <Basic><br>・該当なし | - | - | - | - |
| CPS.DS-12 | ・IoT機器やソフトウェアが正規品であることを定期的(起動時等)に確認する | L1_1_d_PRO, L2_3_c_ORG, L2_3_c_SYS | <High Advanced><Advanced>共通<br>・組織は、機器のシリアル番号やハッシュ値等を利用して、定期的にIoT機器および搭載されているソフトウェアが正規品であることを確認する。 | O | - | - | - |
| | | | <Basic><br>・組織は、調達時や資産の棚卸しを実施した際等に、自組織が所有するIoT機器が正規品であるかをラベルを確認する等して確かめる。 | O | - | - | - |
| CPS.DS-13 | ・データの取得元、加工履歴等をライフサイクルの全体に渡って維持・更新・管理する | L3_4_a_PRO | <High Advanced><br>・組織は、自組織が管理するデータの処理を実施するサイバー空間におけるサプライチェーンの中に、自組織が委託先等に要求している水準の対策を実装していないエンティティが介在していないかを確認する。 | O | - | - | - |
| | | | <Advanced><br>・組織は、他組織あるいは、自組織外の個人、IoT機器等から取得したデータの取得元を、当該データに紐づけて、取得から廃棄に至るまでのライフサイクル全体に渡り管理する。<br>・組織は、自組織が利活用するデータの取得元および、当該データを処理した組織、ヒト等を識別する。 | O | - | - | - |
| | | | <Basic><br>・組織は、他組織あるいは、自組織外の個人から取得したデータの取得元を、当該データに紐づけて、取得から廃棄に至るまでのライフサイクル全体に渡り管理する。 | O | - | - | - |
| CPS.DS-14 | ・計測の可用性、完全性保護によるセンシングデータの信頼性確保のために、計測セキュリティの観点が考慮されたIoT機器を利用する | L2_1_a_ORG, L2_1_a_COM, L2_1_a_PRO L2_3_a_ORG | <High Advanced><Advanced>共通<br>・ネットワーク接続性を持ち、フィジカル空間における動態をデジタル化しサイバー空間へ送信する機能を有する機器(センサー)を導入する際、当該機器の機能における下記の観点を考慮し、調達を実施することが望ましい。<br>- 完全性検証ツールを使用して、通信データに対する不正な変更を検知する機能を実装しているか<br>- 他のIoT機器、サーバ等から識別可能なユニークIDを有するか、あるいは証明書を搭載しており、通信先との相互認証等を通じて真正性を主張できるか<br>- 機器のリソースが、ある程度の規模のサービス拒否攻撃等を受けた際でも可用性を維持することが可能なレベルのものか<br>- 物理的な攻撃に対して耐性を有しているか | O | | ○<br>(SC-5, SC-6, SI-7) | - |
| | | | <Basic><br>・該当なし | - | - | - | - |
| CPS.DS-15 | ・組織間で保護すべきデータを交換する場合、当該データの保護に係るセキュリティ要件について、事前に組織間で取り決める | L1_1_a_DAT, L1_1_a_ORG, L3_1_a_SYS, L3_4_a_DAT | <High Advanced><Advanced>共通<br>・組織は、交換するデータの重要度、想定されるリスクを勘案して、具体的なセキュリティ対策要件を指定し、取引先に対して実装を求める。<br>・組織は、再委託先以降の事業者へのデータ取扱い業務の委託を、直接の取引先に求める水準のセキュリティ対策が実装されていることが確認される場合に限って、許可する。 | O | - | - | - |
| | | | <Basic><br>・組織は、取引先が取り扱う可能性のあるデータに関して、秘密保持契約を締結することで、取り扱いを規定する。<br>・組織は、直接の取引先に対して、データの管理に関わる業務の再委託を禁止する。<br>[参考]「中小企業の情報セキュリティ対策ガイドライン」(IPA, 2018年)で、委託契約時の機密保持契約条項のサンプルを提供している。 | O | - | - | - |
| CPS.IP-1 | ・IoT機器、サーバ等の初期設定手順(パスワード等)及び設定変更管理プロセスを導入し、運用する | L2_1_a_ORG, L2_1_a_DAT, L2_1_b_PRO, L2_3_b_ORG | <High Advanced><br>・組織は、構成管理の対象となるIoT機器、サーバ等に対して変更を実施する前に、それらの変更をテスト・承認・文書化する。<br>・組織は、IoT機器、サーバ等の設定を一つの場所から管理・適用・検証するための自動化されたメカニズムを使用する。 | O | - | ○<br>(下記に加え、CM-3(2)) | ○<br>(A.12.1.2, A.12.5.1) |
| | | | <Advanced><br>・組織は、構成管理の対象となるIoT機器、サーバ等に対する変更が生じた場合には変更に伴うセキュリティ影響分析を実施して変更の実施可否を判断し、実施手順等のを文書化する。<br>・組織は、許可されたIoT機器、サーバ等の変更に関して、実施できる要員（アクセス制限）を限定する。<br>・組織は、許可されたIoT機器、サーバ等の変更を実施するとともに、その変更の実施・記録・監査等を実施する。 | O | ○<br>(下記に加えて、3.4.3, 3.4.4, 3.4.5) | ○<br>(下記に加え、CM-3, CM-4, CM-5) | |

| 対策要件ID | 対策要件 | 対応する脆弱性 | 対策例 | 対策例を実行する主体 | 参照ガイドライン | | |
|---|---|---|---|---|---|---|---|
| | | | | | NIST SP 800-171 | NIST SP 800-53 rev.4 | ISO/IEC 27001:2013 付属書A |
| | | | <Basic><br>・組織は、自組織の運用に適合する最も制限された設定基準を定めた上で、導入されるIoT機器、サーバ等の初期設定手順及び設定内容を文書化するとともに、その文書に従って設定を実施する。<br>・組織は、IoT機器を設置する前にデフォルトの初期設定値を確認し、CPS.AC-4で定めたポリシーに準じていない場合に、適切なものへと変更する。<br>・組織は、IoT機器の導入前に、搭載されているソフトウェアを確認し、記録する | O | ○<br>(3.4.2) | ○<br>(CM-6) | |
| CPS.IP-2 | ・IoT機器、サーバ等の導入後に、追加するソフトウェアを制限する | L1_1_a_SYS,<br>L2_1_a_ORG,<br>L2_1_c_SYS,<br>L3_3_d_SYS,<br>L3_1_a_SYS,<br>L3_3_a_SYS | <High Advanced><br>・組織は、自組織のシステム上で実行を許可するソフトウェアの一覧(ホワイトリスト)、又は禁止するソフトウェアの一覧(ブラックリスト)を用いてソフトウェアの制限を実施するとともに、許可されていないソフトウェアのインストールを不可とする。 | O/S | ○<br>(下記に加えて、3.4.8) | ○<br>(下記に加え、CM-7(4), CM7-(5)) | ○<br>(下記に加えて、A.12.5.1) |
| | | | <Advanced><br>・組織は、自組織のシステム上でのユーザによるソフトウェアのインストールについて管理するメカニズムを導入し、モニタリングを実施する。 | O/S | ○<br>(3.4.9) | ○<br>(CM-11) | ○<br>(A.12.6.2) |
| | | | <Basic><br>・組織は、自組織のシステム上でのユーザによるソフトウェアのインストールに関するポリシーを確立し、ユーザに遵守させる。 | O | - | - | |
| CPS.IP-3 | ・システムを管理するためのシステム開発ライフサイクルを導入し、定めた各段階におけるセキュリティに関わる要求事項を明確化する | L1_1_a_ORG,<br>L1_1_b_ORG,<br>L1_1_c_ORG | <High Advanced><br>・組織は、システムの調達にあたり以下に示すような要求事項を明示的に提示する。<br>-セキュリティ機能に関する要求事項<br>-セキュリティ強度に関する要求事項<br>-セキュリティ保証に関する要求事項<br>-セキュリティ関連のドキュメントに関する要求事項<br>-セキュリティ関連のドキュメントの保護に関する要求事項<br>-そのシステムの開発環境と、そのシステムを稼働させる予定の環境についての記述<br>-受け入れ基準 | O | - | ○<br>(下記に加え、SA-4) | ○<br>(下記に加え、A.6.1.5, A.14.2.2, A.14.2.5) |
| | | | <Advanced><br>・組織は、 情報セキュリティ上の考慮事項を含むシステム開発ライフサイクルに従ってシステムを管理するとともに、システム開発ライフサイクル全体を通じた情報セキュリティリスクマネジメントプロセスを実施する。 | O | - | ○<br>(下記に加え、SA-3) | |
| | | | <Basic><br>・組織は、システムを構築するに当たり仕様書、設計、開発、導入、及び変更に、システムのセキュリティエンジニアリング原則を適用する。 | O | ○<br>(3.13.2) | ○<br>(SA-8) | ○<br>(A.14.1.1, A.14.2.1, A.14.2.6) |
| CPS.IP-4 | ・構成要素(IoT機器、通信機器、回線等)に対し、定期的なシステムバックアップを実施し、テストしている | L2_1_d_SYS,<br>L3_3_d_SYS | <High Advanced><br>・組織は、バックアップ情報を定期的にテストして、媒体の信頼性と情報の完全性を確認する。 | O | - | ○<br>(下記に加えて、CP-9(1)) | ○<br>(下記に加え、A.14.3.1) |
| | | | <Advanced><br>・組織は、自組織のシステムドキュメントのバックアップを定めたタイミングや頻度で実施する。<br>・組織は、保管拠点におけるバックアップ情報の機密性・完全性・可用性を保護する。 | O | ○<br>(3.8.9) | ○<br>(CP-9) | ○<br>(下記に加え、A.18.1.3) |
| | | | <Basic><br>・組織は、自組織のシステムに含まれるユーザレベル・システムレベルの情報のバックアップを定めたタイミングや頻度で実施する。 | O | | | ○<br>(A.12.3.1) |
| CPS.IP-5 | ・無停電電源装置、防火設備の確保、浸水からの保護等、自組織のIoT機器、サーバ等の物理的な動作環境に関するポリシーや規則を満たすよう物理的な対策を実施する | L1_1_a_SYS,<br>L2_1_d_SYS,<br>L3_3_c_SYS,<br>L2_3_b_SYS, | <High Advanced><br>・組織は、自組織の利用するシステムが設置されている施設に職員が常駐しない場合には、自動消火機能を導入する。 | O | - | ○<br>(下記に加え、PE-13, PE-15) | ○<br>(A.11.1.4, A.11.2.1, A.11.2.2) |
| | | | <Advanced><br>・組織は、無停電電源装置等により自組織のIoT機器、サーバ等が設置されているエリア内の機器の安定な稼働を維持する。<br>・組織は、独立した電源等により稼働する消火及び火災検知のための装置やシステムを導入し、維持する。<br>・組織は、閉止弁や遮断弁を用意し、自組織のIoT機器、サーバ等が設置されているエリアを水漏れ等の被害から保護する。 | O | | | |
| | | | <Basic><br>・組織は、自組織のIoT機器、サーバ等が設置されているエリアの温度と湿度を定めた許容レベルに保つ仕組みを導入する。<br>・組織は、自組織のIoT機器、サーバ等が設置されているエリアの温度と湿度を定期的にモニタリングする。 | O | - | ○<br>(PE-14) | |
| CPS.IP-6 | ・IoT機器、サーバ等の廃棄時には、内部に保存されているデータ及び、正規IoT機器、サーバ等を一意に識別するデータID(識別子)や重要情報(秘密鍵、電子証明書等)を削除又は読み取りできない状態にする | L2_3_b_DAT | <High Advanced><br>・組織は、廃棄対象のIoT機器やサーバ等の内部に保存されている情報のセキュリティカテゴリ等の分類を定義し、その定義に従い必要な強度と完全性を備えた情報の削除又は読み取りできない状態にする技法を使い分けるメカニズムを導入する。 | O | ○<br>(3.8.3) | ○<br>(MP-6) | ○<br>(下記に加え、A.8.2.3) |
| | | | <Advanced><br>・組織は、自組織のIoT機器やサーバ等を廃棄するプロシージャを定め、そのプロシージャに従って内部に保存されている情報を削除又は読み取りできない状態し、適切に実施できたことを確認する。 | O | | | ○<br>(A.8.3.1, A.8.3.2, A.11.2.7) |
| | | | <Basic><br>・組織は、自組織のIoT機器やサーバ等をを廃棄するに当たっては、内部に保存されている情報を削除又は読み取りできない状態する。 | O | | | |

| 対策要件ID | 対策要件 | 対応する脆弱性 | 対策例 | 対策例を実行する主体 | 参照ガイドライン | | |
|---|---|---|---|---|---|---|---|
| | | | | | NIST SP 800-171 | NIST SP 800-53 rev.4 | ISO/IEC 27001:2013 付属書A |
| CPS.IP-7 | ・セキュリティインシデントへの対応、内部及び外部からの攻撃に関する監視/測定/評価結果から教訓を導き出し、資産を保護するプロセスを改善している | L1_1_a_PRO,<br>L1_1_b_PRO,<br>L1_1_c_PRO,<br>L2_1_a_COM | <High Advanced><br>・組織は、第三者によるセキュリティ評価を実施する。 | O | - | ○<br>(下記に加え、CA-2(1)) | ○<br>(A.16.1.6, A.18.2.1, Clause 9.1, Clause 9.2, Clause 10.1, Clause 10.2) |
| | | | <Advanced><br>・組織は、セキュリティ評価を適切に、かつ、計画的に実施するため、以下に示す事項を含めたセキュリティ評価計画を策定した上で、セキュリティ評価を実施する。<br>-セキュリティ評価の対象とするセキュリティ対策<br>-セキュリティ対策の有効性を図るために用いる評価手順<br>-セキュリティ評価を実施する環境や実施体制<br>-セキュリティ評価結果の取りまとめ方法とその活用方法 | O | ○<br>(3.12.1) | ○<br>(CA-2) | |
| | | | <Basic><br>・組織は、セキュリティ対策が正しく実装されているか及び運用されているかに加え、セキュリティ対策が期待された成果を上げているかに関する定期的に評価（セキュリティ評価）を実施し、管理責任者へ報告する。<br>・組織は、セキュリティ評価の結果に基づき、セキュリティ対策の改善を実施する。 | O | | | |
| CPS.IP-8 | ・保護技術の有効性について、適切なパートナーとの間で情報を共有する | L2_1_a_COM | <High Advanced><br>・組織は、保護技術に関する新たな情報や保護技術に関する有効性に関する情報を、自動化されたメカニズムを通じて適切なパートナーと適時双方向で共有をすることができる環境を整備する。 | O | ○<br>(3.14.4) | ○<br>(AC-21) | ○<br>(A.16.1.6) |
| | | | <Advanced><br>・組織は、保護技術に関する新たな情報や保護技術に関する有効性に関する情報を、パートナーに適時共有することができる環境を整備する。 | O | | | |
| | | | <Basic><br>・組織は、保護技術に関する新たな情報や保護技術に関する有効性に関する情報を、適切なパートナーから入手できる環境を整備する。 | O | - | - | |
| CPS.IP-9 | ・人の異動に伴い生じる役割の変更に対応した対策にサイバーセキュリティ（例：アクセス権限の無効化、従業員に対する審査）を含めている | L1_1_a_PEO,<br>L1_1_b_PEO,<br>L1_1_c_PEO, | <High Advanced><br>・組織は、自組織のシステムに対するアクセスの変更等の再審査が必要な条件を定め、要員の再審査を実施する。<br>・組織は、要員の退職時に、情報セキュリティをトピックとした退職者面接を実施する。 | O | ○<br>（下記に加えて、3.9.1 3.9.2） | ○<br>（下記に加え、PS-3, PS-4） | ○<br>（下記に加え、A.7.2.3, A.7.3.1） |
| | | | <Advanced><br>・組織は、要員が自組織内で配置転換／異動になった場合に、要員の配置転換／異動によりシステムや入退室管理等に関するアクセス権限の変更を実施する。<br>・要員が組織を離れるときの影響を最小限に抑えるために、運用と保守を含む供給者関係の重要な役割について、現担当者のバックアップ要員を指定する。 | O | ○<br>（下記に加えて、3.9.2） | ○<br>（下記に加え、PS-5） | ○<br>(A.7.1.1, A.7.1.2, A.7.2.1, A.8.1.4) |
| | | | <Basic><br>・組織は、自組織のシステムに対するアクセスを許可する前に、要員を審査する。<br>・組織は、要員の退職時に以下を実施する。<br>-自組織のシステムに対するアクセスを一定期間内に無効にする。<br>-職員に関連する認証及びクレデンシャルを無効にする。<br>-セキュリティに関連するシステム関連の所有物をすべて回収する。<br>-退職する個人が管理していた組織の情報と情報システムに対するアクセスを保持する。 | O | ○<br>(3.9.1 3.9.2) | ○<br>(PS-3, PS-4) | |
| CPS.IP-10 | ・脆弱性管理計画を作成し、計画に沿って構成要素の脆弱性を修正する | L1_1_a_SYS,<br>L2_1_a_COM,<br>L2_1_c_SYS,<br>L3_1_a_SYS,<br>L3_3_a_SYS | <High Advanced><br>・組織は、欠陥修正状況を管理するための自動化されたメカニズムを導入し、管理する。 | O | - | ○<br>（下記に加え、SI-2(2)） | ○<br>（下記に加え、A.14.2.3） |
| | | | <Advanced><br>・組織は、修正内容の有効性と副次的な悪影響の可能性についてテストを行った上で欠陥の修正を実施し、当該修正を構成管理として管理する。 | O | ○<br>(3.14.3) | ○<br>(SI-2) | |
| | | | <Basic><br>・組織は、自組織のシステムに関する欠陥の特定・報告・修正を計画的に実施する。<br>[参考] 特に、製造現場等に設置されるIoT機器には、可用性や機器自体の機能の関係で、タイムリーにパッチを適用すること、あるいはパッチの適用事態が困難な場合がある。その場合は、「制御システム利用者のための脆弱性対応ガイド 第2版」(IPA, 2016年)の P.23に記載されている通り、脅威への対策(機能の最小化、ネットワーク監視の強化等)を徹底し、セキュリティ被害の発生を回避することが望ましい。 | O | - | - | ○<br>(A.12.6.1) |
| | ・IoT 機器、サーバ等のセキュリティ上重要なアップデート等を必要なタイミングで適切に実施する方法を検討し、適用する<br>・可能であれば、遠隔地からの操作によってソフトウェア(OS、ドライバ、アプリケーション)を一括して更新するリモートアップデートの仕組みを備えたIoT機器を導入する | L1_1_a_SYS,<br>L2_1_a_COM,<br>L2_1_c_SYS,<br>L3_3_d_SYS,<br>L3_1_a_SYS,<br>L3_3_a_SYS | <High Advanced><br>・組織は、自組織のIoT機器、サーバ等のアップデート等でメンテナンスに必要な機器やツールを用いる際には、事前に承認するものとし、モニタリングを実施する。<br>・組織は、自組織のIoT機器、サーバ等のアップデート等を実施する要員が持ち込むメンテナンスに必要な機器やツールを検査し、不適切な変更または不正な変更がないか確認する。<br>・組織は、自組織のIoT機器、サーバ等のアップデート等でメンテナンスに用いる媒体を検査して、悪質コードが含まれていないことを確認した上で使用する。<br>・組織は、遠隔地からの操作によってソフトウェア(OS、ドライバ、アプリケーション)を一括して更新するリモートアップデートの仕組みを備えたIoT機器を導入する。 | O | ○<br>(3.7.1, 3.7.2, 3.7.4) | ○<br>（下記に加え、MA-3, MA-3(1), MA-3(2)） | ○ |

| 対策要件ID | 対策要件 | 対応する脆弱性 | 対策例 | 対策例を実行する主体 | 参照ガイドライン | | |
|---|---|---|---|---|---|---|---|
| | | | | | NIST SP 800-171 | NIST SP 800-53 rev.4 | ISO/IEC 27001:2013 付属書A |
| CPS.MA-1 | | | <Advanced><br>・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンスを実施するに当たり、メンテナンスの実施計画、実施、確認、文書化する。<br>・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンスを実施する際には、事前に承認するものとし、モニタリングを実施する。<br>・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンスを自組織の施設から離れた場所で実施する場合には、施設からの移動について事前に承認するものとともに、移動に先立って関連する保存されている情報の消去等の必要な処理を実施する。<br>・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンスの終了後、影響を受けた可能性のあるすべてのセキュリティ対策をチェックして、正しく機能しているかどうかを確認する。<br>・組織は、自組織のIoT機器、サーバ等のアップデート等のメンテナンス記録を保管する。<br>・組織は、メンテナンス要員の認可プロセスを確立し、認可されたメンテナンス組織または要員の一覧の最新化を図る。 | O | ○<br>（下記に加えて、3.7.1, 3.7.2, 3.7.4） | ○<br>（下記に加え、MA-2） | （下記に加え、A.11.2.4, A.11.2.5, A.11.2.6, A.14.2.4） |
| | | | <Basic><br>・組織は、メンテナンス要員が付添いなしでシステムのメンテナンスを行う場合に、その要員が必要なアクセス権限を有することを確認する。<br>・組織は、必要なアクセス権限を持たない要員によるメンテナンス活動を監督するのに必要なアクセス権限と技術的能力を有する組織の要員を指定する。 | O | ○<br>(3.7.6) | ○<br>(MA-5) | ○<br>(A.11.1.2) |
| CPS.MA-2 | ・自組織のIoT機器、サーバ等に対する遠隔保守は、承認を得て、ログを記録し、不正アクセスを防げる形で実施している | L1_1_a_SYS,<br>L2_1_a_COM,<br>L2_1_c_SYS,<br>L3_3_d_SYS,<br>L3_1_a_SYS,<br>L3_3_a_SYS | <High Advanced><br>・組織は、遠隔保守のための接続の確立と実施に関するポリシーとプロシージャを文書化し、その内容により実施する。 | O | - | ○<br>（下記に加え、MA-4(2)） | ○<br>（下記に加え、A.15.1.1） |
| | | | <Advanced><br>・組織は、実施した遠隔保守の実施記録を保管する。 | O/S | ○<br>(3.7.5) | ○<br>(MA-4) | ○<br>(A.11.2.4, A.15.2.1) |
| | | | <Basic><br>・組織は、遠隔保守を実施する際には組織の定めるネットワークアクセスに求める認証を実施するとともに、遠隔保守が完了したらセッションとネットワーク接続を確実に終了する。<br>・組織は、遠隔保守の実施に当たっては、実施計画を策定し・合意した上で実施し、実施結果を確認する。 | O/S | | | |
| CPS.PT-1 | ・セキュリティインシデントを適切に検知するため、監査記録／ログ記録の対象を決定、文書化し、そうした記録を実施して、レビューしている | L1_1_a_SYS,<br>L2_1_b_ORG,<br>L3_3_d_SYS,<br>L3_1_a_SYS,<br>L3_3_a_SYS | <High Advanced><br>・タイムスタンプが複数の監査ログで確実に一致する場合、組織が定めた対象についての監査ログをシステム全体にわたる監査証跡として、（論理的・物理的を問わず）管理される。<br>・監査記録のタイムスタンプを生成するための正式な情報源を用いて、内部システムクロックを比較し、同期するようなシステム機能を提供する。<br>・システムは、監査レビュー・分析・レポートのそれぞれについて、一体的に扱う自動的なメカニズムを採用する。<br>・組織が利用するIoT機器には、セキュリティに関わる監査ログの生成や既存のログ管理システムへの接続等が難しいものが含まれている可能性があるため、IoT機器からの監査ログの収集・分析に当たっては、主に利用しているものとは別のログ管理システムの利用や、システム側での対策による代替等、IoT機器のスペックを考慮した対応を行う必要がある。 | O/S | ○<br>（下記に加えて、3.3.7） | ○<br>（下記に加えて、AU-6(1), AU-11(1)） | ○<br>（下記に加えて、A.12.4.4） |
| | | | <Advanced><br>・システムは、監査ログおよび監査ツールのそれぞれの完全性を保護するために、暗号メカニズムを実装する。<br>・組織は、自組織におけるセキュリティ関係の責任に関する規定によって割り当てられたユーザに対してのみ、監査ログの管理権限を付与する。<br>・システムは、監査プロセスの失敗のインシデントにおいて、アラートを発する。 | O/S | ○<br>（下記に加えて、3.3.4, 3.3.8, 3.3.9） | ○<br>（下記に加えて、AU-9(3), AU-9(4)） | ○<br>（下記に加えて、A.12.4.2） |
| | | | <Basic><br>・組織は、自組織のリスクマネジメントの戦略や、リスクアセスメントの結果等に基づき、監査対象を設定し、対象において誰がいつ何を行ったかがわかるような監査ログの取得がシステムにより可能かを確認する。<br>・システムは、さまざまなシステムコンポーネントから規定された監査ログを生成する。<br>・システムの監査ログを定期的にレビュー・分析して、自組織に被害をもたらしうるセキュリティインシデントの兆候の有無を確認し、必要に応じてシステム管理者等へ報告する。 | O/S | ○<br>(3.3.1, 3.3.2, 3.3.3) | ○<br>(AU-2, AU-3, AU-6, AU-11) | ○<br>(A.12.4.1, A.12.4.3, A.12.7.1) |
| CPS.PT-2 | ・IoT機器、サーバ等の本体に対して、不要なネットワークポート、USB、シリアルポート等を物理的に閉塞する | L1_1_a_SYS,<br>L1_1_c_SYS,<br>L2_1_b_COM,<br>L2_3_b_SYS,<br>L3_1_a_SYS, | <High Advanced><br>・組織は、システム上での実行が許可されないソフトウェアプログラムを識別する。<br>・「ブラックリスト」あるいは「ホワイトリスト」管理により、そのシステム上で許可されていないソフトウェアプログラムを実行できないようにする。<br>・ブラックリストあるいはホワイトリストの一覧を定期的にレビューし、更新する。<br>・システムは、規定したルールに従って、プログラムの実行を阻止する。 | O/S | ○<br>（下記に加えて、3.4.7, 3.4.8） | ○<br>（下記に加えて、CM-7(2), CM-7(4)） | ○<br>(A.8.2.2, A.8.3.1) |
| | | | <Advanced><br>・組織は、システム、モノ等によって提供される機能とサービスをレビューし、削除の候補となる機能とサービスを特定する。<br>・組織は、禁止されている機能、ポート、プロトコル、サービスの使用を検知し防止するために、ネットワークスキャンツール、侵入検知防止システム、エンドポイントプロテクション（ファイアウォール、ホストベースの侵入検知システム等）を活用する | O | ○<br>（下記に加えて、3.4.6） | ○<br>（下記に加えて、CM-7） | |
| | | | <Basic><br>・使用するUSBメモリ等の周辺機器は、管理台帳を作成し、保管場所を施錠して管理する。<br>・IoT機器、サーバ等に接続するUSBメモリ等の外部記憶媒体に対して、ウイルス対策ソフトによるチェック、ウイルスチェックが可能なUSBメモリを用いる等の対策を行う。<br>・使用しないUSBポート、シリアルポートは栓をするなど物理的に閉塞する。 | O | ○<br>(3.8.1, 3.8.4) | ○<br>(MP-2, MP-3, MP-4) | |
| | ・ネットワークにつながることを踏まえた安全性を実装するIoT機器を導入する | L2_2_a_ORG | <High Advanced><br>・ハザードのエネルギー等を下げて事故が起きても影響を小さくするように設計する等、本質安全設計を通じて、影響度の高いハザードに対処することで、被害を極小化する。 | O | - | - | ○<br>(A.16.1.6) |

| 対策要件ID | 対策要件 | 対応する脆弱性 | 対策例 | 対策例を実行する主体 | 参照ガイドライン | | |
|---|---|---|---|---|---|---|---|
| | | | | | NIST SP 800-171 | NIST SP 800-53 rev.4 | ISO/IEC 27001:2013 付属書A |
| CPS.PT-3 | | | <Advanced><br>・セーフティの側面を考慮したセキュリティリスクアセスメント(CPS.RA-4)を実施し、対象システムにおける物理的な安全に関する対策の要否およびそのレベルを把握する。<br>・本質安全設計を通じてハザードの縮減を図る。当該プロセスを通じて、影響度の高いハザードが残存した場合、例えば、下記のような代替的対策を講ずることが望ましい。<br>- 安全装置等の付加装置による安全確保<br>- ハザードを有する機器に要員が近づかないような空間設計の実施 | O | - | - | - |
| | | | <Basic><br>・該当なし | - | - | - | - |
| CPS.AE-1 | ・ネットワーク運用のベースラインと、ヒト、モノ、システム間の予測されるデータの流れを特定し、管理するプロシージャを確立し、実施する | L1_1_a_COM,<br>L1_1_b_COM<br>L1_1_c_COM<br>L1_1_a_SYS,<br>L1_3_a_ORG,<br>L1_3_b_ORG,<br>L2_1_b_ORG,<br>L3_3_d_SYS,<br>L3_1_a_SYS,<br>L3_3_a_SYS | <High Advanced><br>・組織は、ネットワーク構成、機器のソフトウェア構成等の情報を自動的に収集するメカニズムを利用し、常時最新の状況をモニタリングする。<br>・システムは、システム内（および相互接続システム間）のデータフローを制御するために、ユーザに対して（管理者によって）承認されたアクセス権限を強制的に適用する。<br>・組織/システムは、定常的なシステムの通信状況やセキュリティアラートのパターンを分析し、典型的な通信パターンおよびセキュリティアラートを集約したプロファイルを作成、活用することで、未知の脅威や不審な振る舞い(通信)を検知できるようにする。 | O/S | ○<br>（下記に加えて、3.1.3, 3.14.1, 3.14.6, 3.14.7） | ○<br>（下記に加えて、AC-4, CM-2(2), SI-4, SI-4(13)） | |
| | | | <Advanced><br>・構成管理の一環として、組織がシステムの最新のベースラインとなる構成を把握し、文書化する。<br>・システムのベースライン構成に変更が生じる場合、速やかにベースライン構成を更新し、常に最新の状況を把握できるようにする。<br>・組織は、一方のシステムから他方のシステムへの接続に関して、一方のシステムが他方のシステムのセキュリティ対策状況が十分なものだと判断した上で、接続を許可する<br>・組織は、システム内(および相互接続システム間)のデータフローを制御するために、ユーザのアクセス権限に応じて任意アクセス制御を実施する。 | O | - | ○<br>（下記に加えて、CA-3） | |
| | | | <Basic><br>・組織は、システムのネットワーク構成、資産、機器の設定情報、構成情報等のベースラインとなる情報を文書化し、内容が適切かどうかを定期的に確認する。 | O | ○<br>(3.4.1) | ○<br>(CM-2) | |
| CPS.AE-2 | ・セキュリティ管理責任者を任命し、セキュリティ対策組織(SOC/CSIRT)を立ち上げ、組織内でセキュリティインシデントを検知・分析・対応する体制を整える | L1_2_a_ORG | <High Advanced><br>・組織は、セキュリティ専門の24時間365日モニタリングモニタリングにより収集した監査ログを、分析自動化ツール等を利用することで効率的に分析する。<br>・組織は、従来のIT環境だけでなく、制御システムやIoT機器も含めて、セキュリティ状況のモニタリングの範囲とすることが望ましい。<br>・組織は、セキュリティ対応組織の成熟度を定期的に評価し、セキュリティ状況のモニタリングやインシデントへの対応等のセキュリティ関連業務を継続的に改善することが望ましい。<br>[参考]セキュリティ対策組織(SOC/CSIRT)を評価するためのメトリクスには、"セキュリティ対応組織成熟度セルフチェックシート"(ISOG-J, 2018年)や、SIM3(Security Incident Management Maturity Model)等がある。 | O/S | - | ○<br>（上記に加えて、SI-4(2), SI-4(5)） | ○<br>（下記に加えて、A.12.4.1, A.16.1.5） |
| | | | <Advanced><br>・組織は、リスクアセスメントの結果等を参照して、下記の観点を考慮しながらモニタリング、相関分析の対象となる対象を確立する。<br>- モニタリングするシステムの範囲をどこまでとするか<br>- どのような機器のログを収集し、分析するか (CPS.AE-3を参照)<br>・組織は、モニタリングにより収集した監査ログを定期的にレビューする。<br>・組織は、資産情報、機器の構成情報、ネットワーク構成情報等を継続的に収集・管理し、自組織のセキュリティ対応状況を評価する。<br>・組織は、相関分析の結果等から対応が必要なセキュリティインシデントを適切に検知し、セキュリティ運用プロセスの記載内容に従い、対応を実施する。プロセスの内容については、CPS.RP-1等を参照。<br>・組織およびシステムのセキュリティ状態をセキュリティ管理責任者等の適切な要員に、定期的に報告する。報告内容には下記を含むことが望ましい。<br>- ログ分析の分析結果 (対処したインシデントの件数、対応済みの代表的なインシデントの概要、脅威動向、モニタリング上の課題等)<br>- モニタリングにおける今後の改善方針<br>[参考]セキュリティ対策組織(SOC/CSIRT)の業務、望まれる規模等については、"セキュリティ対応組織（SOC/CSIRT）の教科書 〜 機能・役割・人材スキル・成熟度 〜"(ISOG-J, 2018年)等を参照することが望ましい。 | O/S | ○<br>(3.6.1, 3.12.2, 3.14.6, 3.14.7) | ○<br>(CA-7, IR-4, SI-4) | |
| | | | <Basic><br>・組織は、セキュリティ管理責任者/担当者を明確化し、社内・社外向けのセキュリティ関係の窓口とする。 | O | - | - | ○<br>(A.6.1.1) |
| CPS.AE-3 | ・セキュリティインシデントの相関の分析、及び外部の脅威情報と比較した分析を行う手順を実装することで、セキュリティインシデントを正確に特定する | L1_2_a_SYS | <High Advanced><br>・最新の脅威情報、脆弱性情報、複数回にわたるセキュリティ管理策アセスメントの結果等から動向分析を実施し、継続的なモニタリングに用いられている活動の修正の必要性を判断する。<br>・組織は、自組織でIDS,IPS,SIEMと言ったセンサーのポリシーチューニング(適用シグネチャ管理)と維持管理を行う。<br>・組織は、自組織でセンサー機器でのカスタムシグネチャを脅威情報から作成する。 | O | ○<br>（下記に加えて、3.14.4） | ○<br>（下記に加え、CA-7(3)） | ○<br>(A.12.4.1) |
| | | | <Advanced><br>・"セキュリティ対応組織（SOC/CSIRT）の教科書 〜 機能・役割・人材スキル・成熟度 〜"(ISOG-J, 2018年)では、主に下記のような機器のログを監視し、リアルタイムに分析を行うよう記載されている。 多種多様なログの取り扱いが必要になるため、ログを正規化し、同一のデータベースに格納したり、SIEMを利用したりして、効率的な分析を実現する必要がある。取得可能な場合はネットフローの情報も扱うことが望ましい。<br>- ファイアウォールなどのネットワーク装置からのログやネットフロー<br>- IPS/IDSなどのセキュリティ装置からのログ<br>- Web サーバなどのアクセスログ<br>- ActiveDirectoryやDNSなどの各種システムからのログ<br>- ユーザ利用端末に関するログ | S | ○<br>(3.12.3) | ○<br>(CA-7) | |
| | | | <Basic><br>・ファイアウォールやエンドポイントセキュリティ製品等の通知を個別に確認することで、影響を及ぼすようなセキュリティインシデントを特定する。 | O | | | |

| 対策要件ID | 対策要件 | 対応する脆弱性 | 対策例 | 対策例を実行する主体 | 参照ガイドライン | | |
|---|---|---|---|---|---|---|---|
| | | | | | NIST SP 800-171 | NIST SP 800-53 rev.4 | ISO/IEC 27001:2013 付属書A |
| CPS.AE-4 | ・関係する他組織への影響を含めてセキュリティインシデントがもたらす影響を特定している | L1_3_a_PRO | <High Advanced><br>・組織は、発生したセキュリティインシデントの形態，規模及び費用を定量化及び監視できるようにする自動的なメカニズムを備える。<br>・組織は、セキュリティインシデント発生時において、マルウェアや攻撃者が配置したプログラムやスクリプトが発見された場合、それらの機能の解析を自組織のセキュリティ対応組織(SOC/CSIRT)にて実施する。<br>・組織は、攻撃者のプロファイル（所属組織、組織の活動目的など）に関する仮設を構築する。<br>[参考]複数のシステムが連携する"System of Systems"が構築されている環境においては、セキュリティインシデントの影響評価はより困難なものになることが想定される。当該領域における先行的な試みである"Internet of Things(IoT)インシデントの影響評価に関する考察"(一般社団法人日本クラウドセキュリティアライアンス, 2016年)では、デバイスの特性、サービスの特性、デバイス数により影響度を評価する試みがなされている。 | O/S | - | - | ○<br>（下記に加えて、A.16.1.6） |
| | | | <Advanced><br>・組織は、IPA、JPCERT/CC、業界ISAC、セキュリティベンダー等と連携して情報収集し、脅威情報、脆弱性情報等を相互に関連付けて、共有することによって、当該セキュリティインシデントの全容を把握する。<br>・セキュリティインシデント発生時において、マルウェアや攻撃者が配置したプログラムやスクリプトが発見された場合、それらの機能の解析を外部のセキュリティベンダー等に依頼する。 | O | ○<br>(3.6.1) | ○<br>(IR-4, IR-4(8)) | ○<br>(A.6.1.4) |
| | | | <Basic><br>・該当なし | - | - | - | - |
| CPS.AE-5 | ・セキュリティインシデントの危険度の判定基準を定める | L1_2_a_PRO | <High Advanced><br>・組織は、あらかじめ優先して継続・復旧すべき中核事業を特定しておき、当該事業を運用するにあたり極めて重要なリソース(関係する他組織、ヒト、モノ、データ、システム等)と機能を特定し、優先順位付けする。　※CPS.AM-6, CPS.BE-2に同様の対策例を記載<br>・組織は、セキュリティインシデントの追跡と、インシデントに関係する脅威収集・脆弱性等の情報の収集および分析を支援する自動化されたメカニズムを使用して、セキュリティインシデントの分類(トリアージ)等に活用する。 | O | - | ○<br>（下記に加え、CP-2(8), IR-5(1)） | ○<br>(A.16.1.4) |
| | | | <Advanced><br>・組織は、自組織のセキュリティ運用プロセスにおいて、対象となるシステムの復旧目標、復旧の優先順位、およびメトリクスを考慮してインシデントを分類する。 | O | - | ○<br>（下記に加え、CP-2） | |
| | | | <Basic><br>・当該セキュリティインシデントのもたらす影響の大きさを考慮し、報告義務のあるインシデントを定める。<br>[参考]セキュリティインシデントの影響の大きさを測るための尺度を検討する場合、下記文書等を参照することができる。<br>・"SP 800-61 rev.1"(NIST, 2008年) 3.2.6 事件の優先順位付け<br>・"サイバー攻撃による重要インフラサービス障害等の深刻度評価基準"(NISC, 2018年) | O | - | ○<br>(IR-8) | |
| CPS.CM-1 | ・組織内のネットワークと広域ネットワークの接点において、ネットワーク監視・アクセス監視を実施する | L1_1_a_SYS,<br>L1_1_c_SYS,<br>L1_2_a_SYS,<br>L2_1_b_ORG,<br>L3_3_d_SYS,<br>L3_1_a_SYS,<br>L3_3_a_SYS | <High Advanced><br>・システムは、管理されたインターフェース上で認証されたプロキシサーバー経由で、通信を宛て先IPアドレスの属するネットワークにルーティングする<br>・システムは、モバイルコードの使用を管理し、監視する。<br>・システムは、VoIPの使用を管理し、監視する。 | S | ○<br>（下記に加えて、3.13.13, 3.13.14） | ○<br>（下記に加えて、SC-7(8)） | - |
| | | | <Advanced><br>・組織は、インターネットなどの外部ネットワークと社内ネットワークの中間に内部ネットワークへのアクセスを隔離されたネットワーク上のセグメント(DMZ: 非武装地帯)を構築する。<br>・組織のセキュリティアーキテクチャに従って配備された境界保護装置によって構成される管理されたインターフェースを介してのみ、外部ネットワークまたはシステムに接続する。<br>・システムは、個々の外部通信サービスに対して、管理されたインターフェース(ゲートウェイ、ルーター、ファイアウォール等)を必ず経由させる<br>・組織は、個々の管理されたインターフェース(ゲートウェイ、ルーター、ファイアウォール等)に対して、通信制御ポリシーを定める<br>・管理されたインターフェースにおけるシステムは、ネットワーク通信をデフォルトで拒否し、例外的に許可する | O/S | ○<br>（下記に加えて、3.13.6） | ○<br>（下記に加えて、SC-7(4), SC-7(5), ） | - |
| | | | <Basic><br>・組織は、システムの外部境界、およびシステム内の主要な内部境界において通信をモニタリングし、制御する。 | S | ○<br>(3.13.1, 3.13.5) | ○<br>(SC-7) | - |
| CPS.CM-2 | ・IoT機器、サーバ等の重要性を考慮し、適切な物理的アクセスの設定および記録、監視を実施する | L1_1_a_SYS,<br>L2_3_b_SYS<br>L3_1_a_SYS | <High Advanced><br>・組織は、特に重要な資産を管理している範囲内での重要資産の位置や移動を追跡し、モニタリングする。 | O | - | ○<br>（下記に加えて、PE-20） | - |
| | | | <Advanced><br>・施設内の、一般の人がアクセスできる指定エリアに対するアクセスを制御するための、入退室管理対策を実施する。<br>・組織は、個人の物理的なアクセスを許可する前に、当該要員のアクセス権限を確認し、入退室時のログを保持する。<br>・監視カメラ等による常時モニタリングは実施していないが、入退室管理等により物理アクセスログを取得している場合、定期的に、また、インシデントあるいはその兆候が顕在化した際に監査ログをレビューする。<br>・自組織の保護すべき資産に直接アクセス可能なエリア(執務室等)において、自組織の担当者が来客に付き添って、来客の行動をモニタリングする。<br>・組織は、IoT機器、サーバ等が設置されている自組織の業務上重要な施設に対する物理アクセスを監視カメラ等によりモニタリングすることによって、物理的なセキュリティインシデントを早期に検出し、対応できるようにする。<br>・自組織のオペレーションにとって重要度が高いと考えられるIoT機器、サーバ等のモノであるが、遠隔地に存在している等の理由により上記の物理的セキュリティ対策の実装が難しいと考えられる場合、耐タンパー性の高い機器を利用する(CPS.DS-6)等して、機器自体の物理セキュリティ特性を高めることで対策することを検討する。 | O | ○<br>(3.10.4, 3.10.5) | ○<br>(PE-3, PE-6) | ○<br>[A.11.1.1, A.11.1.2, A.11.1.3] |
| | | | <Basic><br>・コスト等の問題により、物理的アクセスを制御すべきエリアに入退室管理、映像監視等の対策が実施できない場合、自組織の担当者が来客に付き添うなどして人手による代替的な対策を実施する。 | O | | | |

| 対策要件ID | 対策要件 | 対応する脆弱性 | 対策例 | 対策例を実行する主体 | 参照ガイドライン | | |
|---|---|---|---|---|---|---|---|
| | | | | | NIST SP 800-171 | NIST SP 800-53 rev.4 | ISO/IEC 27001:2013 付属書A |
| CPS.CM-3 | [第2層]<br>・指示された動作内容と実際の動作結果を比較して、異常の検知や動作の停止を行うIoT機器を導入する<br>[第3層]<br>・サイバー空間から受ける情報(データ)が許容範囲内であることを動作前に検証する | L2_2_a_COM,<br>L3_3_a_DAT,<br>L3_3_d_SYS | <High Advanced><br>・IoT機器あるいはそうした機器を含んだシステムが、通常期待される結果とは異なる結果をもたらすような特定の攻撃(例：コマンドインジェクション)に備え、ソフトウェアプログラムまたはアプリケーションからの出力情報を検証して、期待される内容と一致しているかを確認する。<br>・システムは、インプットとなるデータが指定されたフォーマットや内容に適合しているかどうかを確認することで、有効性をチェックする。<br>・システムは、IDS/IPSによる悪質コードの検知ロジックを自動的に更新する。<br>・エンドポイント(IoT機器、サーバ等)において、マルウェアに対する振舞い検知型の検出・修復ソフトウェアを導入することで、未知の脆弱性を突く攻撃コードの検知を実施する。<br>・組織のシステムの定期的スキャン、及びファイルがダウンロードされ、開かれ、または実行されるような、外部情報源からのファイルのリアルタイムスキャンを実行する。 | S | ○<br>(下記に加えて、3.14.4, 3.14.5) | ○<br>(下記に加え、SI-10, SI-15) | ○<br>(A.12.2.1) |
| | | | <Advanced><br>・システムは、IDS/IPSを通じて自身に対する悪質なコードが検出した場合、当該コードを遮断、隔離するか、管理者に通知する。<br>・エンドポイント(IoT機器、サーバ等)において、マルウェアに対するパターンファイル型の検出・修復ソフトウェアを導入することで、攻撃コードの検知を実施する。<br>※ 特にIoT機器においては、マルウェア対策ソフトが利用可能なOSが使用されているとは限らないケースがある。組織は、調達時等に導入する機器がマルウェア対策ソフトに対応できるものかを確認し、対応可能なものを選定することが望ましい。マルウェア対策ソフトに対応する機器を調達することが困難な場合、ネットワーク上でマルウェアを検知する仕組みを導入・強化する等、代替的な対策を実施することが望ましい。 | S | ○<br>(3.14.2, 3.14.3) | ○<br>(SI-3) | |
| | | | <Basic><br>・該当なし | - | - | - | - |
| CPS.CM-4 | IoT機器、サーバ等において、送受信する情報(データ)の完全性および真正性を動作前に確認する | L3_3_a_DAT,<br>L3_3_d_SYS | <High Advanced><br>・組織は、データ入力に対する「ホワイトリスト」の概念を導入することで、インプットデータの出所を既知の信頼できるモノ、システム等と、そうしたインプットデータの許容できるフォーマットを指定する。<br>・IoT機器、サーバ等は、他のIoT機器と通信する際、機器間の相互認証が成功した後にはじめて通信を開始することで、データの出所の把握を確実なものとする。<br>・システムは、通信セッションの真正性を保護する。 | S | ○<br>(下記に加えて、3.14.5) | ○<br>(下記に加えて、SI-10(5)) | ○<br>(A.13.2.1, A13.2.3) |
| | | | <Advanced><br>・システムは、完全性検証ツールを使用して、IoT機器、サーバ等からの通信データに対する不正な変更を検知する。<br>・IoT機器、サーバ等は、他のIoT機器と通信する際、当該IoT機器が自組織の業務において重要なものと認められる場合、機器間の相互認証が成功した後にはじめて通信を開始することで、データの出所の把握を確実なものとする。 | S | ○<br>(3.14.5) | ○<br>(下記に加えて、SI-7) | |
| | | | <Basic><br>・該当なし | - | - | - | - |
| CPS.CM-5 | ・発生する可能性のあるセキュリティインシデントを検知できるよう、外部サービスプロバイダとの通信内容をモニタリングする | L1_1_a_COM,<br>L1_1_b_COM<br>L1_1_c_COM<br>L1_1_a_SYS,<br>L1_3_a_ORG,<br>L1_3_b_ORG,<br>L3_3_d_SYS,<br>L3_1_a_SYS,<br>L3_3_a_SYS | <High Advanced><br>・組織は、外部情報システムサービスのプロバイダに対して、サービスの使用に必要な機能、ポート、プロトコル、および他のサービスを明確にするよう要求する。<br>・組織は、上記で明確化した事項が遵守されているかどうかモニタリングする。 | O/S | - | ○<br>(下記に加えて、SA-9(2)) | ○<br>(下記に加えて、A.13.1.2,<br>A.15.2.2) |
| | | | <Advanced><br>・組織は、外部サービスプロバイダおよびシステム開発の委託先の要員に対してのセキュリティ上の要求事項を文書化し、契約等に記載する。<br>・組織は、外部サービスプロバイダおよびシステム開発の委託先に対して、自組織のシステムに対する権限を有する要員が異動、または雇用が終了する場合に、自組織へ通知することを要求する。<br>・組織は、関連する業務情報，業務システム及び業務プロセスの重要性，並びにリスクの再評価を考慮して，外部サービスプロバイダーによるサービス提供の変更を管理することが望ましい。<br>・組織は、外部サービスプロバイダおよびシステム開発の委託先による要求事項の遵守状況をモニタリングする。<br>・組織は、外部サービスプロバイダーおよびシステム開発の委託先による作為あるいは不作為による不正アクセスを検知するため、当該外部事業者による自組織のシステムへのアクセスををモニタリングする。<br>・組織は、外部サービスプロバイダーおよびシステム開発の委託先の活動のモニタリング結果を、適切なシステム管理者に報告する。 | O/S | ○<br>(3.14.6, 3.14.7) | ○<br>(下記に加えて、PS-7, SI-4) | |
| | | | <Basic><br>・組織は、外部情報システムサービスのプロバイダおよびシステム開発の委託先に対して、自組織が対象となっている、あるいは当該プロバイダーが対象として該当するルールに従って、例えば下記に関連するようなセキュリティ要求事項を設定し、導入することを要求する。<br>- (例えば、ISMS認証取得相当の)セキュリティ対策が十分に行われていること<br>- 運用中のデータが適切に管理されること<br>- サービス利用終了時にデータが適切に削除されること | O | - | ○<br>(SA-9) | ○<br>(A.14.2.7) |
| CPS.CM-6 | ・機器等の構成管理では、ソフトウェア構成情報、ネットワーク接続状況(ネットワーク接続の有無、アクセス先等)および他の組織、ヒト、モノ、システムとのデータの送受信状況について、継続的に把握する | L1_1_a_COM,<br>L1_1_a_SYS,<br>L1_1_b_COM<br>L1_1_c_COM<br>L1_3_a_ORG,<br>L1_3_b_ORG,<br>L2_1_a_ORG,<br>L2_3_b_ORG,<br>L2_1_c_ORG,<br>L2_1_c_SYS,<br>L3_1_a_SYS,<br>L3_3_a_SYS | <High Advanced><br>・組織は、システム内に許可されてないハードウェア、ソフトウェア、ファームウェアが存在する場合に、それを自動で検知するメカニズムを使用する。<br>・システムは、許可されてないコンポーネントのネットワークアクセスが検知された場合に、そうしたコンポーネントによるネットワークアクセスを無効にする、それらのコンポーネントをネットワークから切り離す等の一次対処を実施し、システム管理者に通知する。<br>・IoT機器には、既存の資産管理システムと必ずしも接続できないものも存在することが想定されるため、組織が管理できる範囲で複数の資産管理システムを運用することも視野に入れて資産管理・構成管理を実施する。 | O/S | - | ○<br>(下記に加えて、CM-8(3)) | |
| | | | <Advanced><br>・組織は、新たな資産のインストールや削除の際に、または、システムのアップデートの際に、資産、構成情報の一覧を更新することが望ましい。<br>・システムは、個々の外部通信サービスに対して、管理されたインターフェース(ゲートウェイ、ルーター、ファイアウォール等)を必ず経由させる<br>・個々の管理されたインターフェース(ゲートウェイ、ルーター、ファイアウォール等)に対して、通信制御ポリシーを定める<br>・管理されたインターフェースにおけるシステムは、ネットワーク通信をデフォルトで拒否し、例外的に許可する。<br>・システムは、セッション終了後、あるいは一定以上の間非アクティブな状態が持続しているセッションのネットワークコネクションを終了する。<br>・組織は、承認されていないモノ、システム等への通信、あるいは適切でない内容を含んだ通信を検知するため、管理されたインターフェースにおいて通信をモニタリングする。 | O/S | ○<br>(下記に加えて、3.4.1, 3.4.3,<br>3.13.9, 3.14.6, 3.14.7) | ○<br>(下記に加えて、CM-3,<br>CM-8(1), SC-7(4),<br>SC-7(5), SI-4) | |

| 対策要件ID | 対策要件 | 対応する脆弱性 | 対策例 | 対策例を実行する主体 | 参照ガイドライン | | |
|---|---|---|---|---|---|---|---|
| | | | | | NIST SP 800-171 | NIST SP 800-53 rev.4 | ISO/IEC 27001:2013 付属書A |
| | | | <Basic><br>・IoT機器、サーバ等を含む資産の型番やソフトウェアのバージョン、サポート期限等を管理する台帳を作成し、定期的に棚卸する。<br>・組織は、運用時に実施すべき対策（IoTデバイスの不正利用や盗難、パッチの適用、ログのチェック等）、IoT機器の状況を定期的に確認する。 | O | ○<br>(3.4.1) | ○<br>(CM-8) | |
| CPS.CM-7 | ・自組織の管理しているIoT機器、サーバ等に対して、定期的に対処が必要な脆弱性の有無を確認する | L1_1_a_SYS,<br>L3_3_d_SYS,<br>L3_1_a_SYS,<br>L3_3_a_SYS | <High Advanced><br>・組織は、スキャンすべきシステムの脆弱性をすぐに更新できる脆弱性スキャンツールを使用する。<br>・組織は、スキャンされたシステムの脆弱性を定期的に、あるいは新たな脆弱性が特定され、報告された場合に更新する。<br>・組織は、指定された脆弱性スキャン活動に関して、対象システムのコンポーネントに対する特権的アクセスの許可制度を実施する。 | O | ○<br>(下記に加えて、3.11.2) | ○<br>(下記に加えて、RA-5(1), RA-5(2), RA-5(5)) | ○<br>(A.12.6.1) |
| | | | <Advanced><br>・組織は、システムおよびアプリケーションの脆弱性のスキャンを定期的に、あるいは、それらのシステム／アプリケーションに影響を及ぼす新たな脆弱性が確認され、報告された場合に実施する<br>・組織は、脆弱性スキャンにツールを用いる。以下を満たす標準的な手法を使用することによって、脆弱性管理プロセスの一部を自動化できることが求められる<br>- プラットフォーム、ソフトウェアの欠陥、および誤った設定を列挙する<br>- チェックリストとテスト手順をフォーマットする<br>- 脆弱性による影響を評価する<br>・組織は、リスクアセスメントを通じて、特定された脆弱性を適切な期間中に修正する<br>・上記のプロセスから得た情報を組織内の他のシステムの管理者と共有することによって、他の情報システム内の同様の脆弱性を把握し、必要に応じて修正する。<br>[参考]脆弱性情報の取得に際して、Japan Vulnerability Notes(https://jvn.jp/)等の情報源を参照することが可能である。また、脆弱性の影響の大きさを評価する指標として、CVSS(IPAによる解説：https://www.ipa.go.jp/security/vuln/CVSS.html)を参考とすることが可能である。 | O | ○<br>(3.11.2, 3.11.3) | ○<br>(RA-5) | |
| | | | <Basic><br>・組織は、システムおよびアプリケーションの脆弱性のスキャンを定期的に実施する | O | | | |
| CPS.DP-1 | ・セキュリティインシデントの説明責任を果たせるよう、セキュリティインシデント検知における自組織とサービスプロバイダーが担う役割と負う責任を明確にする | L1_2_a_ORG | <High Advanced><Advanced><Basic>共通<br>・組織は、リスクマネジメントに係る戦略やアセスメントの結果等から、セキュリティインシデントを検知するために収集することが望ましいログ情報を決定する。<br>・組織は、取引先(サービスプロバイダー)に対して、取得されるサービス利用者の活動，例外処理及びセキュリティインシデントを記録した監査ログの存在を確認する。<br>・組織は，サービスプロバイダーにより取得される監査ログが，サービスの利用者の活動，例外処理及びセキュリティインシデントを記録できており、適切な方式で保護されていることを確認する。 | O | ○<br>(3.12.3) | ○<br>(CA-7, PM-14) | ○<br>(A.6.1.1, A.12.4.1) |
| CPS.DP-2 | ・監視業務では、地域毎に適用される法令、通達や業界標準等に準拠して、セキュリティインシデントを検知する | L1_2_a_ORG,<br>L1_3_c_ORG | <High Advanced><Advanced><Basic>共通<br>・組織は、モニタリング業務に関係する法制度、業界標準、顧客との契約事項等が存在するか、存在するならばどのような制約があるかを認識する。<br>・組織は、上記で認識したルールに準拠してモニタリングを実施し、セキュリティインシデントを検知する。<br>・組織は、自組織のモニタリング活動がルールに準拠したものかどうかを定期的にレビューし、確認する。 | O | ○<br>(3.12.3) | ○<br>(CA-7, PM-14) | ○<br>(A.18.2.2) |
| CPS.DP-3 | ・監視業務として、セキュリティインシデントを検知する機能が意図したとおりに動作するかどうかを定期的にテストし、妥当性を検証する | L1_2_a_ORG | <High Advanced><br>・最新の脅威情報、脆弱性情報、複数回にわたるセキュリティ管理策アセスメントの結果等から動向分析を実施し、継続的なモニタリングに用いられている活動の修正の必要性を判断する。<br>・システムに、既知で害のないテストケースを導入して、マルウェア検知メカニズムをテストする。<br>・組織は、侵入検知モニタリングに用いているメカニズムを定期的にテストする。テストの頻度は、組織が使用するツールの種類と、ツールの設置方法により変わる。 | O/S | - | ○<br>(下記に加えて、CA-7(3), SI-3(6), SI-4(9)) | ○<br>(下記に加えて、A.14.3.1) |
| | | | <Advanced><br>・組織は、自組織のシステムのモニタリング活動が、組織のリスクマネジメント戦略と、リスク対応のためのアクションの優先順位に適合しているかどうかを定期的に確認するプロシージャを定め、運用する。<br>・ネットワーク機器やエンドポイントからのセキュリティに係る情報の相関分析を行うのに合わせて、誤検出や検出漏れの割合を算出し。定期的に検知メカニズムの妥当性を確認する。 | O | - | ○<br>(CA-7, PM-14) | ○<br>(A.14.2.8) |
| | | | <Basic><br>・該当なし | - | - | - | - |
| | ・セキュリティインシデントの検知プロセスを継続的に改善する | L1_2_a_ORG | <High Advanced><br>・組織は、検知能力向上のため、様々な情報ソースをもとに、検知ルールの作成とチューニングを行う<br>- 相関分析ルールの開発<br>- IPS/IDSの独自シグネチャの開発<br>- 独自ブラックリストの開発<br>・組織/システムは、システムの通信やセキュリティアラートのパターンを分析し、典型的な通信パターンおよびセキュリティアラートを集約したプロファイルを作成、活用することで、誤検出の数や、検出漏れの数を減らすためのチューニングを行う。 | O/S | - | ○<br>(下記に加えて、SI-4(13)) | |

| 対策要件ID | 対策要件 | 対応する脆弱性 | 対策例 | 対策例を実行する主体 | 参照ガイドライン | | |
|---|---|---|---|---|---|---|---|
| | | | | | NIST SP 800-171 | NIST SP 800-53 rev.4 | ISO/IEC 27001:2013 付属書A |
| CPS.DP-4 | | | <Advanced><br>・組織は、経営層等の組織内の然るべき要員に、定期的に組織およびシステムのセキュリティの状態を報告するプロシージャを整備し、運用する。組織は、報告の場を最新の脅威や残存するリスクに対する脅威を認識し、セキュリティを向上するための場とすることが望ましい。<br>・例えば下記のような注意喚起情報の発信があった際等に、セキュリティに係るリスク増加の兆候がある場合、信頼できる情報源からの情報に基づいて、システムのモニタリング活動のレベルを上げる。　※下記のリストは、"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 "(ISOG-J, 2017年)より引用している。<br>・ 攻撃の特徴 攻撃の特徴<br>➢ 攻撃形態、関連する通信の内容<br>➢ 核心となる攻撃コード<br>・ 攻撃によって残る痕跡<br>➢ 被害を受けた後の通信内容<br>➢ サーバやクライアントに残るログ<br>➢ サーバやクライアントに残るその他特徴<br>・ 各セキュリティ製品における検知名 | O | ○<br>(3.14.6, 3.14.7) | ○<br>(CA-7, SI-4) | ○<br>(A.16.1.6) |
| | | | <Basic><br>・該当なし | - | - | - | - |
| CPS.RP-1 | ・対応が必要なセキュリティインシデント発生時の対応の内容や優先順位、対策範囲を明確にするため、セキュリティ運用プロセスを定め、運用する<br>・不適切なセキュリティインシデント(例：アクセス元/先が不正なエンティティである、送受信情報が許容範囲外である)を検知した後のIoT機器、サーバ等による振る舞いをあらかじめ定義し、実装する | L1_1_a_SYS,<br>L1_2_a_PEO,<br>L2_2_a_PRO,<br>L3_3_d_SYS,<br>L3_1_a_SYS,<br>L3_3_a_SYS | <High Advanced><br>・システムは、IoT機器、サーバ等に異常(誤動作等)が発生した場合に、緊急停止、管理者へのアラート通知等のフェールセーフのための対応を実施する。<br>・システムは、有効でないインプットデータを受け取った場合に、組織の目的とシステムの目的に沿って、予想できる形で、かつ記載どおりに動作する。 | S | - | (下記に加えて、SI-10(3), SI-17) | ○<br>(A.16.1.5) |
| | | | <Advanced><br>・組織は、セキュリティ運用マニュアルにおいてインシデントの検知および分析、封じ込め、低減、復旧を含む内容を規定する。<br>- インシデントの報告を受けた者が、どのような判断で対応をするのか、あるいはより上位に報告するのか、の判断基準を明確にしておく<br>- すべてのインシデントの取り扱いに関する記録をとる<br>- 外部組織等に対して、インシデント発生の事実と対応状況に関する報告をする必要があるかどうかを判断する | O | - | ○<br>(下記に加えて、IR-8) | |
| | | | <Basic><br>・組織は、対処が必要と判断されたセキュリティインシデントの発生時に利用するセキュリティ運用プロセスを策定し、運用する。当該プロセスには、下記を例とする内容を含むことが望ましい。<br>- 緊急時の指揮命令と対応の優先順位の決定<br>- インシデントへの対応（インシデントレスポンス）<br>- インシデントの影響と被害の分析<br>- 情報収集と自社に必要な情報の選別<br>- 社内関係者への連絡と周知<br>- 外部関係機関との連絡<br>[参考]セキュリティインシデント発生時の対応手順の検討において、"インシデントハンドリングマニュアル"(JPCERT/CC, 2015年)、"SP 800-61 rev.1"(NIST, 2008年)、"インシデント対応マニュアルの作成について"(JPCERT/CC, 2015年)を参照することが可能である。 | O | ○<br>(3.6.1) | ○<br>(IR-4) | |
| CPS.RP-2 | ・セキュリティ運用マニュアルにおいて、取引先等の関係する他組織との連携について手順と役割分担を定め、運用する | L1_3_a_PEO,<br>L1_3_a_PRO,<br>L1_3_b_PEO,<br>L1_3_b_PRO | <High Advanced><br>・組織は、サプライチェーンにおけるセキュリティインシデントの対処を想定し、自組織とサプライチェーンに関与する他の組織との間で、インシデント対応活動を調整するプロシージャを整備する。<br>・組織は、インシデント対応要件が満たされるよう、自組織のインシデント対応プロセスと、自組織の事業継続上、重要な機能を有する外部サービスプロバイダのインシデント対応プロセスを調整する。<br>・組織は、脅威情報、脆弱性情報等と、個々のセキュリティインシデントへの対応を相互に関連付けることによって、状況認識を改善する。<br>[参考]サプライチェーンにおけるセキュリティインシデントには、たとえば、システムコンポーネント、IT 製品、開発プロセスまたは開発者、流通過程または倉庫施設に対する侵害等がある。 | O | - | ○<br>(下記に加えて、CP-2(7), IR-4(4), IR-4(10)) | ○<br>(下記に加えて、A.17.1.2) |
| | | | <Advanced><br>・組織は、セキュリティインシデントにより第1の処理拠点の可用性が低下した場合に利用する代替処理拠点を定める。<br>・組織は、自組織の一次処理機能が利用できない場合に、自組織が定める目標復旧時間内に、代替処理拠点により所定のオペレーションを移転・再開して、重要なミッション／業務機能を遂行できるようにするようサービス契約で規定する。<br>・組織は、同じ脅威に対する脆弱さを減らすために、一次処理拠点から離れた代替処理拠点を指定する。<br>・組織は、システムのユーザにセキュリティインシデントの対応と報告に関する助言と支援を提供する、組織のインシデント対応能力に不可欠な、インシデント対応支援リソース(ヘルプデスク、CSIRT等)を自組織に用意する。 | O | - | ○<br>(下記に加えて、CP-7, CP-7(1), CP-7(2), CP-7(3), IR-7) | |
| | | | <Basic><br>・対処の必要なセキュリティインシデントを発見した場合、速やかにIPA、JPCERT/CC等の関係機関に報告し、対応の支援、発生状況の把握、手口の分析、再発防止のための助言等を受ける。 | O | - | ○<br>(IR-6) | ○<br>(A.16.1.1, A.16.1.2) |
| CPS.RP-3 | ・自然災害時における対応方針および対応手順を定めている事業継続計画又はコンティンジェンシープランの中にセキュリティインシデントを位置づける | L1_2_a_PRO | <High Advanced><Advanced>共通<br>・組織は、災害等と比較して被害状況が見えづらく事業継続計画の発動タイミングが不明確、インシデントの原因究明の重要性が高い等の特徴を有するセキュリティインシデントに特化した事業継続計画又はコンティンジェンシープランを策定し、運用する。<br>・組織は、セキュリティインシデントに特化した事業継続計画又はコンティンジェンシープランを策定する際、組織全体の事業継続に係る方針と合致するような内容とすることを確実にする。 | O | - | ○<br>(CP-2) | ○<br>(A.17.1.1) |
| | | | <Basic><br>・該当なし | - | - | - | - |
| CPS.RP-4 | ・セキュリティインシデント発生時に被害を受けた設備にて生産される等して、何らかの品質上の欠落が生じていることが予想されるモノ(製品)に対して適切な対応を行う | L1_3_a_COM | <High Advanced><Advanced>共通　※CPS.CO-3と関連<br>・組織は、社外の取引関係組織、エンドユーザー等の外部関係者にセキュリティインシデントの概要を説明し、具体的な被害状況の情報収集を行う。<br>・組織は、サプライチェーンに関与する外部関係者との間で、復旧活動およびインシデントの事後処理に関わる活動を調整する。その際、CPS.AM-2, CPS.AM-3にて記載している方法により、対応の対象となるモノを特定していることが望ましい。 | O | ○<br>(3.6.2) | ○<br>(下記に加えて、IR-4, IR-4(10)) | ○<br>(A.17.1.1) |

| 対策要件ID | 対策要件 | 対応する脆弱性 | 対策例 | 対策例を実行する主体 | 参照ガイドライン | | |
|---|---|---|---|---|---|---|---|
| | | | | | NIST SP 800-171 | NIST SP 800-53 rev.4 | ISO/IEC 27001:2013 付属書A |
| | | | <Basic><br>・自組織の業種等を考慮して、事業継続計画又はコンティンジェンシープランの中に、インシデント発生後の生産したモノへの対応について記載するかを検討する。その際、事業継続計画又はコンティンジェンシープランは、必ずしもセキュリティインシデントを想定したものでない場合も許容されるものとする。 | O | - | ○<br>(CP-2) | |
| CPS.CO-1 | ・セキュリティインシデント発生後の情報公表時のルールを策定し、運用する | L1_2_a_PRO | <High Advanced><Advanced><Basic>共通<br>・組織は、下記の内容を含むセキュリティインシデント発生後の情報公表時のルールを策定し、運用する。<br>- 公表する内容<br>- 情報公表の実施時期<br>- 情報公表の実施者<br>- 情報公表までの実施プロセス | O | - | - | ○<br>(Clause 7.4) |
| CPS.CO-2 | ・事業継続計画又はコンティンジェンシープランの中に、セキュリティインシデントの発生後、組織に対する社会的評価の回復に取り組む点を位置づける | L1_2_a_PRO | <High Advanced><Advanced><Basic>共通<br>・マスコミや取引先に対する情報のやり取りの窓口を一本化し、対応方針が一貫したものとなるようにする。<br>・セキュリティインシデントによる被害に関する重要な情報について、情報の機密性に配慮しつつ丁寧に説明することの肯定的な側面を認識する。 | O | - | - | - |
| CPS.CO-3 | ・復旧活動について内部および外部の利害関係者と役員、そして経営陣に伝達する点を、事業継続計画又はコンティンジェンシープランの中に位置づける | L1_2_a_PRO | <High Advanced><Advanced>共通<br>・組織は、監督官庁、社外の取引関係組織、エンドユーザー等の外部関係者にセキュリティインシデントの概要を説明し、具体的な被害状況の情報収集を行う。<br>・組織は、サプライチェーンに関与する外部関係者との間で、復旧活動およびインシデントの事後処理に関わる活動を調整する。ここで該当する活動の例として、生産システムにおけるセキュリティインシデント発生時に生産されたモノの回収等が挙げられる。 | O | ○<br>(3.6.1) | ○<br>(下記に加えて、IR-4, IR-4(10)) | ○<br>(A.17.1.2) |
| | | | <Basic><br>・組織は、自組織に影響を及ぼすようなセキュリティインシデント発生時における役割、責任、そうした役割と責任を割り当てられたヒトと連絡先情報を示す。<br>・組織は、事業継続に関わる意思決定の責任が割り当てられたヒトに対して、意思決定をより適切なものとするため、セキュリティインシデントの概要や被害状況に関する説明を実施する。 | O | - | ○<br>(CP-2) | |
| CPS.AN-1 | ・セキュリティインシデントの全容と、推測される攻撃者の意図から、組織全体への影響を把握する | L1_2_a_PRO | <High Advanced><br>・システムは、発生したセキュリティインシデントの形態，規模及び費用を定量化及び監視できるようにする自動的なメカニズムを備える。<br>・組織は、セキュリティインシデント発生時において、マルウェアや攻撃者が配置したプログラムやスクリプトが発見された場合、それらの機能の解析を自組織のセキュリティ対応組織(SOC/CSIRT)にて実施する。<br>・組織は、攻撃者のプロファイル（所属組織、組織の活動目的など）に関する仮説を構築する。<br>[参考]複数のシステムが連携する"System of Systems"が構築されている環境においては、セキュリティインシデントの影響評価はより困難なものになることが想定される。当該領域における先行的な試みである"Internet of Things(IoT)インシデントの影響評価に関する考察"(一般社団法人日本クラウドセキュリティアライアンス, 2016年)では、デバイスの特性、サービスの特性、デバイス数により影響度を評価する試みがなされている。 | O/S | - | - | ○<br>(下記に加えて、A.16.1.6) |
| | | | <Advanced><br>・組織は、IPA、JPCERT/CC、業界ISAC、セキュリティベンダー等と連携して情報収集し、脅威情報、脆弱性情報等を相互に関連付けて、共有することによって、当該セキュリティインシデントの全容を把握する。<br>・セキュリティインシデント発生時において、マルウェアや攻撃者が配置したプログラムやスクリプトが発見された場合、それらの機能の解析を外部のセキュリティベンダー等に依頼する。 | O | ○<br>(3.6.1) | ○<br>(IR-4, IR-4(8)) | ○<br>(A.6.1.4) |
| | | | <Basic><br>・該当なし | - | - | - | - |
| CPS.AN-2 | ・セキュリティインシデント発生後に、デジタルフォレンジックを実施する | L1_2_a_PRO | <High Advanced><br>・システムが、重要なセキュリティインシデントに関する監査記録について処理するプロシージャを提供する。 | S | ○<br>(3.3.6) | ○<br>(AU-7, AU-7(1)) | ○<br>(A.16.1.7) |
| | | | <Advanced><br>・組織は、媒体，装置及び装置の状態(例えば，電源が入っているか，切れているか)に従って，証拠の特定，収集，取得及び保存のプロシージャを規定する<br>・組織は、重要なセキュリティインシデントについて、発生後に下記の証跡を保全することが望ましい。<br>- 識別情報(インシデントの発生場所/発生日時/対象となるモノのシリアル番号/ホスト名/MACアドレス/IPアドレス等)<br>- 証跡を収集・処理したヒトの役職、名前、連絡先<br>- 証跡保全処理の日時(タイムゾーンを含む) | O | | | |
| | | | <Basic><br>・組織は，証拠となり得るデータを特定，収集，取得及び保存するためのプロシージャを定め，運用する。 | O | | | |
| CPS.AN-3 | ・検知されたセキュリティインシデントの情報は、セキュリティに関する影響度の大小や侵入経路等で分類し、保管する | L1_2_a_PRO | <High Advanced><br>・組織は、あらかじめ優先して継続・復旧すべき中核事業を特定しておき、当該事業を運用するにあたり極めて重要なリソース(関係する他組織、ヒト、モノ、データ、システム等)と機能を特定し、優先順位付けする。　※CPS.AM-6, CPS.BE-2に同様の対策例を記載<br>・組織は、セキュリティインシデントの追跡と、インシデントに関係する脅威収集・脆弱性等の情報の収集および分析を支援する自動化されたメカニズムを使用して、セキュリティインシデントの分類(トリアージ)等に活用する。 | O | - | ○<br>(下記に加え、CP-2(8), IR-5(1)) | |
| | | | <Advanced><br>・組織は、自組織のセキュリティ運用プロセスにおいて、対象となるシステムの復旧目標、復旧の優先順位、およびメトリクスを考慮してインシデントを分類する。<br>・組織は、自組織に影響を及ぼすセキュリティインシデントを追跡し、文書化する。<br>"SP 800-61 rev.1" では、セキュリティインシデントを文書化する際の記載の観点として、下記を例示している。<br>- インシデントの現在の状況<br>- インシデントの概要<br>- 当該インシデントに対して自組織のとった行動の内容<br>- ほかの関係者(システム所有者、システム管理者等)の連絡先情報<br>- 調査の際に収集した証拠の一覧<br>- インシデントの処理担当者からのコメント<br>- 次にとるべきステップ | O | ○<br>(3.6.1) | ○<br>(下記に加え、CP-2, IR-5) | ○<br>(A.16.1.3, A.16.1.4) |

| 対策要件ID | 対策要件 | 対応する脆弱性 | 対策例 | 対策例を実行する主体 | 参照ガイドライン | | |
|---|---|---|---|---|---|---|---|
| | | | | | NIST SP 800-171 | NIST SP 800-53 rev.4 | ISO/IEC 27001:2013 付属書A |
| | | | <Basic><br>・当該セキュリティインシデントのもたらす影響の大きさを考慮し、報告義務のあるインシデントを定める。<br>[参考]セキュリティインシデントの影響の大きさを測るための尺度を検討する場合、下記文書等を参照することができる。<br>・"SP 800-61 rev.1"(NIST, 2008年) 3.2.6 事件の優先順位付け<br>・"サイバー攻撃による重要インフラサービス障害等の深刻度評価基準"(NISC, 2018年) | O | - | ○<br>(IR-8) | |
| CPS.MI-1 | ・セキュリティインシデントによる被害の拡大を最小限に抑え、影響を低減する対応を行う | L1_2_a_PRO | <High Advanced><br>・組織は、セキュリティインシデントの対応プロセスを支援する自動化されたメカニズムを使用する。<br>・組織は、脅威情報、脆弱性情報等と、個々のセキュリティインシデントへの対応を相互に関連付けることによって、状況認識を改善する。<br>[参考]対応段階におけるインシデントの影響低減、復旧段階において有用に機能すると考えられる情報の例として、"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 "(ISOG-J, 2017年)では、下記が挙げられる。<br>・攻撃行為をセキュリティ製品や関連するシステムで遮断するための設定要件<br>・攻撃を無効化する方法(パッチの適用、設定変更等)<br>・被害を受けたシステム復旧方法 | O/S | - | ○<br>(下記に加えて、IR-4(1), IR-4(4)) | ○<br>(A.16.1.5) |
| | | | <Advanced><Basic>共通<br>・組織(あるいはその構成員)は、あらかじめ定められたプロシージャに従って、セキュリティインシデントを低減するためのアクション(たとえば、システムのシャットダウン、有線/無線ネットワークからの切断、モデムケーブルの切断、特定の機能の無効化など)を実行する。<br>[参考]セキュリティインシデントの影響低減のための活動は、インシデントの性質(例えば、サービス拒否攻撃、マルウェア感染、不正アクセスのような顕在化する脅威の差異)により内容が異なる場合がある。より詳細な影響低減活動の情報については、「インシデントハンドリングマニュアル」(JPCERT/CC, 2015年)、"SP 800-61 rev.1"(NIST, 2008年)等を参照することが望ましい。 | O | ○<br>(3.6.1) | ○<br>(IR-4) | |
| CPS.IM-1 | ・セキュリティインシデントへの対応から教訓を導き出し、セキュリティ運用プロセスを継続的に改善する | L1_2_a_ORG | <High Advanced><br>・システムが、発生したセキュリティインシデントの形態，規模及び費用を定量化及び監視できるようにする自動的なメカニズムを備えることが望ましい。 | S | - | - | |
| | | | <Advanced><Basic>共通<br>・セキュリティインシデントの評価から得た脅威情報、脆弱性情報等は，再発する又は影響の大きいインシデントを特定するために利用することが望ましい。<br>・セキュリティインシデントへの対応活動から学んだ教訓を事業継続計画又はコンティンジェンシープラン、教育／訓練に取り入れて、結果として必要となる変更を実施する。NIST SP 800-61には、教訓を抽出する際の観点として下記が例として示されている。<br>- 正確に何がいつ起きたか。<br>- スタッフとマネジメント層がどの程度うまく事件に対処したか。文書化された手順に従ったか。それは適切だったか。<br>- すぐに必要になった情報は何か。<br>- 復旧を妨げたかもしれないステップや行動があったか。<br>- 次に同様の事件が起きた場合、スタッフやマネジメント層は、どのような違った行動をとるか。<br>- どのような是正措置があれば、将来にわたって同じ様な事件が起きるのを防げるか。<br>- 将来事件を検出、分析、軽減するために、どのようなツールやリソースが追加で必要となるか。 | O | ○<br>(3.6.2) | ○<br>(IR-4) | ○<br>(A.16.1.6) |
| CPS.IM-2 | ・セキュリティインシデントへの対応から教訓を導き出し、事業継続計画又はコンティンジェンシープランを継続的に改善する | L1_2_a_ORG | <High Advanced><Advanced><Basic>共通<br>・組織は、セキュリティインシデントへの対応から、事業継続のためのプロシージャおよび関連する対策の機能が、事業継続のより上位の方針と合致しているかを確認する。<br>・セキュリティインシデントへの対応活動から学んだ教訓を事業継続計画又はコンティンジェンシープラン、教育／訓練に取り入れて、結果として必要となる変更を実施する。 | O | ○<br>(3.6.2) | ○<br>(IR-4) | ○<br>(A.17.1.3) |