日本語版の提供について

本書は、Cloud Security Allianceより提供されている「CSA IoT Control Framework」の
日本語版で、原文をそのまま翻訳しています。
従いまして、日本独自の法令や基準に関する記述は含まれておりません。
原文と日本語版の内容に相違があった場合には、原文が優先されます。
また、この翻訳版は予告なく変更される場合があります。
以下の変更履歴（日付、バージョン、変更内容）をご確認ください。

変更履歴

日付	バージョン	変更内容
2019年11月28日	日本語バージョン1.0	

日本語版作成に際しての謝辞
以下に、翻訳に参加された方々の氏名および所属先（企業会員からの参加の場合のみ）を記します。（氏名あいうえお順・敬称略）
日本語版発刊に際して、謝意を表したいと思います。
有本　真由
甲斐　　賢（株式会社日立製作所）
勝見　　勉
二木　正明

日本クラウドセキュリティアライアンスに関する情報は、以下のURLより参照してください。
https://www.cloudsecurityalliance.jp

←左端列はフィルタ用です。セル値1"JP"を選択すると日本語のみ、セル値空白を選択すると英語のみが表示されます。

JP	cloud security alliance® iot CONTROLS FRAMEWORK	フレームワークの詳細を知るには、https://cloudsecurityalliance.org/artifacts/guide-to-the-iot-security-controls-framework/から、"Guide to the CSA IoT Controls Framework"（英文）をダウンロードしてください。			IoT システムリスクへの影響度			補足的なコントロールに関するガイダンス		実装ガイダンス			対象となるIoTシステムコンポーネント（エッジ、フォグ、クラウド）						
JP	コントロールの種別（ドメイン）	コントロールID	CCMとの対応	コントロールの内容	機密性	完全性	可用性	追加情報	参照/根拠	コントロールタイプ	実施方法	頻度	Simple Sensors	Simple Actuators	Complex Edge Devices	Fog / Network Compute Layer	Mobile Application	Local Gateway	Cloud Service Providers (CSPs)
JP													単純なセンサー	単純なアクチュエータ	複合的なエッジデバイス	フォグ / ネットワークレイヤ	モバイルアプリケーション	ローカルゲートウェイ	クラウドサービス事業者
JP	**リスクの低減** *リスクマネジメントアプローチ*	**RSM-01**	GRM-01	業界標準のリスクマネジメントアプローチを採用する。 適用される法的義務、法令、および規制を遵守するために、開発または取得したIoTコンポーネントに対してベースラインセキュリティ要件を設定する必要があります。 標準ベースライン構成からの逸脱は、展開、プロビジョニング、または使用の前に変更管理ポリシーおよび手順に従って承認される必要があります。 セキュリティベースライン要件への準拠は、ビジネスニーズに基づいて再評価されるべ	低	低	低	利用可能な多くのリスク管理フレームワークがあります。 重要インフラのサイバーセキュリティを向上させるためのNISTフレームワーク（バージョン1.1）は、リスクマネジメントプロセスにおいて組織を導くために使用することができます。 他のリスク評価プロセスには、ISO 31000：2018、ISO / IEC 27005：2001、およびNIST 800-39が含まれます。		予防型	手動型	四半期ごと	XX	XX	XX	XX	XX	XX	XX
JP	**リスクの低減** *リスク評価*	**RSM-02**	GRM-02	リスク評価を実行します。デバイス、ゲートウェイ、アプリケーション、データストア、モバイルアプリケーション、クラウドサービス、フォグコンピューティングサービス、およびネットワーク基盤全体にわたる機密データの発生源、保存先、および送信について分析します。機密データを不正使用、アクセス、損失、破壊、および改ざんから保護するため、データ分類メカニズムとデータセキュリティ機能を分析します。信頼された内部者がデータへの特権アクセスを悪用する可能性を分析します。データの保存期間とその終了に伴う廃棄処理の要件を分析します。安全上のリスクを特定します。影響と可能性に基づいてリスクに優先順位を付けます。リスクごとにリスクへの対応を決定する 。（ リスクの軽減、延期、または受け入れ） 以下のようにリスク評価を実行します。 •次の各コンポーネントのセキュリティが危険にさらされる可能性がある場合、潜在的なリスクを分析します。機密データの発生源、保存先、デバイス、ゲートウェイ、アプリケーション、データストア、モバイルアプリケーション、クラウドサービス、フォグコンピューティングサービス、ネットワーク基盤をまたいだ機密データの送信。 •機密データを不正使用、アクセス、紛失、破壊、改ざんから保護するために、データ分類メカニズムとデータセキュリティ機能を分析します。 •信頼された内部者がデータへの特権アクセスを悪用する可能性を分析します。 •データの保存期間とその終了に伴う廃棄処理の要件を分析します。 •これらの分析に基づいて、組織の安全上のリスクを特定します。	低	低	低	また、効果的にリスク評価を行うには、機密データを使用が利用できない場合やデータが改ざんされた場合、またはデータが許可されていない個人に漏れた場合に、それらが組織のビジネス目標に対して与える潜在的な影響も考慮する必要があります。	CSA CCM GRM-02から派生したもの：データガバナンス要件に関連するリスク評価は計画された間隔で行われなければならず、以下を考慮しなければならない： ・機密データがアプリケーション、データベース、サーバ、およびネットワークを越えて保存および転送される場所への留意 •定義された保存期間およびその終了に伴う廃棄処理の要件への準拠 •データの分類と不正使用、アクセス、紛失、破壊、および改ざんからの保護	予防型	手動型	四半期ごと	XX	XX	XX	XX	XX	XX	XX
JP	**技術的セキュリティポリシー** *ポリシーの遵守*	**TSP-01**	GRM-06	企業のIoTサイバーセキュリティポリシーを文書化します。 すべてのIoT実装にこのポリシーに準拠すること、または例外を申請することを要求します。 企業のIoTサイバーセキュリティポリシーには、最低限、暗号化、監視、監査、認証、およびアクセス制御と、同様にIoTシステム各コンポーネントに適用する必要がある物理的なセキュリティコントロールを含める必要があります。 コンプライアンスを遵守していない実装を特定するために頻繁に監視しま	中	中	中	適切性を確保し、新しい脅威やリスクに伴う変化を取り入れるために、ポリシーも定期的に見直す必要があります。	NIST SP 800-131A Revision 1 (Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths) @ http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar1.pdf	予防型	手動型	毎年	xx	xx	xx	xx	xx	xx	XX
JP	**技術的セキュリティポリシー** *更新とパッチ*	**TSP-02**	MOS-19 TVM-02	インベントリ内の各IoTデバイスのアップデート（パッチ/バージョン）ステータスを監視および検証します。 ポリシーに違反しているか、切断のためにアクセスできないデバイスを特定します。 IoTシステムで問題を解決（接続と更新）できない場合は、更新やデバイスの用途の重要性に応じて、電子メール、電話、または担当者による訪問が必要になることがあります。	中	中	中	検証の間隔は、アップデートの重要性とIoTデバイスに関連する脅威によって異なります		発見型	自動型	イベントごと			xx				XX
JP	**技術的セキュリティポリシー** *侵害された資格証明*	**TSP-03**	IAM-09 IAM-10 IAM-12	複製された、または侵害されたIoTデバイスを監視します。 セキュリティが侵害されている可能性がある同じID資格情報で認証されているデバイスを識別する規則を確立します。 検出時に問題を調査して修正します。	中	中	中	悪意ある攻撃者にとって、IoTデバイスによるボットネットを作りDoS（サービス妨害）攻撃を実行することは魅力的です。（不正なログインの発見はこうした行為を防止します。）		発見型	自動型	イベントごと	xx	xx	xx				XX
JP	**技術的セキュリティポリシー** *暗号に関するポリシー*	**TSP-04**	EKM-03	TLSやDTLSその他の暗号プロトコルについて、最低限の（事項の）文書化を行います。ポリシーには、許容されるアルゴリズム、鍵長、オペレーションモードなどが定義されるべきです。ポリシーはNIST SP800-131Aの最新バージョンに書かれたガイダンスに沿って策定します。	低	低	低	推奨される暗号スイートは、攻撃者の能力や、以前は安全であると考えられていたアルゴリズムで特定された脆弱性に基づいて頻繁に変更されます。 IoTシステムが確実にNIST SP 800-131Aで推奨されている暗号スイートを実装し、推奨されなくなったスイートを削除するようにしてください。 推奨されなくなったスイートを削除できなかった場合、IoTシステムは攻撃者はシステムコンポーネントを悪用して、より弱いアルゴリズムを使用して暗号接続をネゴシエートでき、IoTシステムに対し潜在的なダウングレード攻撃の可能性が生じます	NIST SP 800-131A Revision 1 (Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths) @ http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar1.pdf	予防型	手動型	毎年	xx	xx	xx	xx	xx	xx	XX
JP	**技術的セキュリティポリシー** *パスワードポリシー*	**TSP-05**	IAM-12 IVS-12 MOS-16	ITシステムユーザー、管理者、サービスアカウントについて、最小限の複雑性要求を定義したパスワードポリシーを文書化します。また、有効期限やロックアウトポリシーについても、すべてのIoTコンポーネントについて定義します。	低	低	低	デフォルトパスワードはリセットされなければいけません。		予防型	手動型	毎年	xx	xx	xx	xx	xx	xx	XX
JP	**技術的セキュリティポリシー** *データ分類*	**TSP-06**	DSI-01	IoTシステムについて、データセキュリティポリシーを文書化します。組織における（セキュリティ上の）データ分類（レベル）を定義し、それぞれの分類（レベル）について、最低限必要なセキュリティ要求を定義します。	中	中	中	データを適切に保護することで、データ侵害の可能性が減少し、組織が法的リスクを制限するのに役立ちます。		予防型	手動型	毎年	xx	xx	xx	xx	xx	xx	XX

JP	**技術的セキュリティポリシー** *ＩＤ管理ポリシー*	TSP-07	IAM-03 IAM-08	IoTシステムについて、ＩＤ管理ポリシーを文書化します。共有（対象）鍵やパスワード、電子証明書についての適切な取扱を定めます。異なるデバイスやユーザー、サービスに対して同一の資格情報（暗号鍵、電子証明書、パスワード）の発行を制限します。	中	中	中	このコントロールは、攻撃者に対しての難易度を上げることで、侵害されたデバイスからのリスクを低減します。		予防型	自動型	イベントごと			xx				XX
JP	**技術的セキュリティポリシー** *パッチとファームウエア更新*	TSP-08	IAM-06 MOS-19 TVM-02 TVM-03	IoTシステム用のデバイスセキュリティ管理ポリシーを文書化します。ファームウェアとソフトウェアの更新を実行するための最小頻度を定義します。IoTデバイスを危険にさらす可能性がある悪意のあるコードに対する最低限の保護策を定義します。サードパーティのライブラリにパッチを適用するための最小頻度を定義します。	低	低	低	パッチが適用されていないソフトウェアとファームウェアは、システムへの侵入経路を示します。 すべてのデバイスは、最新のソフトウェアの使用と、既知の脆弱性からの保護を確実とするために、定期的に更新される必要があります。		予防型	自動型	イベントごと	xx	xx	xx	xx	xx	xx	XX
JP	**ガバナンス** *ガバナンス・フレームワーク*	GVN-01	HRS-07 AAC-02 AAC-03	IoTシステムのためのガバナンス・フレームワークを作成します。分散システム及び、それらとクラウドや他のデータサービスとの間の接続に関するセキュリティについて、誰が責任を持つかを定義します。各システムを担当する管理責任者を特定し、それらのシステムを保護するための具体的な責任を定義します。IoTシステム内のデータと資産を保護するため、従業員とサードパーティの（データ）利用者について、その役割と責任を特定して文書化します。	中	中	中	ISO/IEC 27014 はIoTに適用可能な情報セキュリティガバナンスのフレームワークを定義しています。	ISO/IEC 27014 CSA CCM AAC-03：組織が確立された方針、基準、手順、およびコンプライアンス義務の不適合に対処することを確実にするために、独立したレビューと評価を少なくとも年1回実施しなければならない。	予防型	手動型	毎年	xx	xx	xx	xx	xx	xx	XX
JP	**ガバナンス** *規制及び法律上の要求事項*	GVN-02	AAC-03 GRM-01 GRM-11 SEF-04	IoTシステムに関連するすべての規格、ならびに規制、法律、および法定の要件を文書化します。 これらの要件の影響を個々のIoTシステムの所有者に伝えます。	低	低	低	安全に関する規制を無視してはいけません。（食品や医薬品に関するものや、運輸、航空などに関する規制など）		予防型	手動型	毎年	xx	xx	xx	xx	xx	xx	XX
JP	**ガバナンス** ***インベントリーの評価***	GVN-03	DCS-01 GRM-10 MOS-09	組織が、確立されたポリシー、標準、手順、およびコンプライアンス義務の不適合に対処することを保証するために、少なくとも年1回、IoTインベントリー（システム目録）の独立したセキュリティ評価を実行します。	低	低	低	独立した評価は、何がうまくいっていて、何を改善する必要があるかについてのフィードバックを提供します。 評価は、標準と手順に従う責任があるチームから独立した個人によって行われるべきです。		検知型	半自動型	毎年	xx	xx	xx				XX
JP	**ガバナンス** *アカウントの確認*	GVN-04	IAM-02 IAM-10 IAM-11	IoTシステム内のユーザー、管理者、サービス及びデバイスのアカウントについて、少なくとも毎年、監査を行います。不要な、または不正な、もしくは期限切れのアカウントと判断されたアカウントは、無効化します。	低	低	低	不十分なアカウント管理は、自動化された攻撃が組織内に拡散する手段を与えてしまいます。		検知型	手動型	毎年	xx	xx	xx	xx	xx	xx	XX
JP	**ガバナンス** *本番データの保護*	GVN-05	AIS-04 CCC-03 DSI-02 DSI-07	デバッグが必要になった際に機微な運用情報が、開発・テスト環境にコピーされるリスクを減らすために、本番環境から開発・テスト環境にデータを移動するときに機微なデータを消去する手順を確立します。	低	低	低	開発環境と本番環境の分離は、整合性を確保するための標準的なベストプラクティスです。		予防型	手動型	毎年							XX
JP	**プライバシー** *管理者への制限*	PRV-01	IAM-02 IAM-09	システム利用者の位置情報やその他の機微な属性情報の追跡に関する管理者の能力を制限するためのポリシーと技術的なメカニズムを実装し実行します。内部者がシステムによるイベントの記録を回避して、これらのコントロールを無効化できないよう、アクセス制御とログ取得を実装します。	中	対象外	対象外	匿名性の保護について考慮します。サービスは利用者が知らない間に追跡されることが無いようにすべきです。		予防型	自動型	常時	xx	xx	xx		xx		XX
JP	**プライバシー** 補助的なシステム	PRV-02		IoTデバイスとサービスに対して（認証のための）資格証明を発行するPKI（基盤）について、プライバシーアセスメントを実施します。発行されたPKI証明書との相関によって利用者の位置や活動が追跡される可能性について分析します。もし、プライバシー上の懸念が特定された場合は、PKIシステム内に位置情報を秘匿するためのプロキシー（サービス）や仮名証明書認証局のような匿名化メカ	中	中	中	ひとつの例として、コネクテッドカーの運用をサポートするためのセキュリティ資格情報管理システム（SCMS）が挙げられます。SCMSには位置情報秘匿プロキシー（LOP）や仮名証明書発行サービス、パタフライキー拡張アルゴリズムなどが組み込まれており、これらのプライバシー強化策により利用者の匿名性が保護されています。		予防型	自動型	常時				xx	xx		XX
JP	**プライバシー** *メタデータ*	PRV-03		IoTシステムによって生成されるメタデータを文書化するための分析を実施します。これらのメタデータを、その機微度に基づいて格付けします。機微と判断されたメタデータの漏洩を監視し、漏洩が発見された場合の対処策を提議しておきます。	低	中	中	例えば、スマートメーターは（電力などの）使用パターンを暴露することで、在宅パターンを知るために悪用される可能性があります。		検知型	自動型	常時			xx	xx	xx		XX
JP	**プライバシー** *プライバシー影響評価*	PRV-04	GRM-01	新しいデバイス開発の開始時にプライバシー影響評価（PIA）を実行してください。 PIAの対象となる科目には、少なくとも以下が含まれます。デバイスからのデータの削除。 収集したデータをユーザーに知らせるために使用されるメカニズム。 ユーザーからデータの使用を承認する同意を得て保存すること。 個人データが転送される前にレビューおよび編集するためのアクセス権をユーザーに提供する手段。 データ収集のタイミングと頻度に関する通知。同様に、ユーザーがデータ共有をオプトインする機能も含まれます。	中	中	中	プライバシー影響評価は、データに関する法的要件および規制上の要件、対応するリスク、そしてどのような保護を講じるべきかを特定するのに役立ちます。 その結果、（法律の）管轄や業界によって要件が異なる場合があります。	PIAテンプレートの例： https://www.dhs.gov/sites/default/files/publications/privacy_pia_template%202017.pdf（DHS） https://iapp.org/media/pdf/knowledge_center/Generic_PIA_Report_-_The_Privacy_Professor_June_2012.pdf（IAPP） https://www.fedramp.gov/assets/resources/templates/SSP-A04-FedRAMP-PIA-Template.docx (FedRamp) European Union's Article 29 Working Party (WP29)	予防型	半自動型	イベントごと	xx	xx	xx	xx	xx	xx	XX
JP	**プライバシー** *プライバシー影響評価* *コンプライアンス*	PRV-05	GRM-09	プライバシー影響評価（PIA）を定期的に更新します。PIAで見つかった主要な問題について、すべてのシステム管理者に周知します。PIAの結果について、継続的にコンプライアンスの状況を追跡します。	中	中	中	管理者は（PIAの）結果に注意を払い、データについて適切に保護するとともに、リスクを増加させるような変更を行わないようにする必要があります。		予防型	手動型	イベントごと	xx	xx	xx	xx	xx	xx	XX
JP	**セキュアな接続** *証明書*	SCN-01		IoTシステムでパスワードが使われている場合は、その代わりに（電子）証明書を使用出来ないか検討します。可能な場合は認証においてパスワードの代わりに証明書を要求するようにシステムを更新します。	中	中	中	X.509証明書は一般的な選択肢です。1609.2証明書はX.509証明書に対しておよそ半分のサイズであり、楕円曲線暗号を使用しています。	パスワード及びその他の機微なデータをASP.NETやAzure App Serviceに導入する際のベストプラクティス https://docs.microsoft.com/en-us/aspnet/identity/overview/features-api/best-practices-for-deploying-passwords-and-other-	予防型	自動型	常時			xx	xx	xx	xx	XX
JP	**セキュアな接続** *アプリケーションの資格情報*	SCN-02		認証資格情報は、IoTデバイスにIEEE 1609.2証明書を使用するときにそれらの資格情報を使用することを承認された特定のアプリケーションにバインドできます。 IEEE 1609.2証明書を使用する場合は、アプリケーション固有の識別子を指定して、IEEE 1609.2 SSP / PSIDビット内で使用します。 承認を決定するときにSSP / PSIDフィールドを検証します。	中	中	中	SCMS（Security Credential Management System）は、複数のCA（認証局）を介した信頼チェーンに依存しています。	ISO 21177 Intelligent Transportation Systems https://tools.ietf.org/html/rfc5280	予防型	自動型	常時			xx		xx		XX
JP	**セキュアな接続** *コンフィグレーションの完全性*	SCN-03	BCR-04	IoTデバイスの設定ファイルすべてを文書化します。これらの設定ファイルについて電子署名を施し、安全なリポジトリに保管しておき、デバイスを復旧する際に使用します。その際に電子署名を使用し、改ざんされていないことを確認します。	中	中	中	たとえばロボットのように、いくつかの種類のIoTデバイスでは、ネットワークを経由してデバイスに送られた設定ファイルに含まれるパラメータに基づいて運用されます。これらのファイルは、悪意を持った者によって設定を変更、上書きされないよう、完全性に関して保護されなければいけません。		予防型	手動型	常時			xx				XX
JP	**セキュアな接続** *設定ファイルのアクセス制御*	SCN-04	IAM-05	IoTデバイスの設定ファイルに対するアクセスを制限します。IoTデバイスの設定変更に際して「疑似アクセス」を要求します。*訳注：「疑似アクセス」直接的に設定ファイルを変更させるのでは無く、なんらかのアプリケーション等を介して変更するなど、資格確認や記録が取れ、設定の整合性が確保できるような方法を意味していると思われます。	中	中	中	設定ファイルの変更を記録、監査することで、それらに不正がなかったかどうかを確認することができます。		予防型	自動型	イベントごと	xx	XX	xx				XX
JP	**セキュアな接続** *変更及びアクセスログ*	SCN-05	CCCp03 IVS-01 STA-03 TVM-02	設定ファイルについて、すべての変更を記録します。また、設定ファイルを変更するためのアクセスの試行すべてを記録します。そしてそれらを継続的に監視し、定期的に監査します。	中	中	中	バージョン管理は、変更の追跡と、セキュリティイベントのベースラインを確立するのに役立ちます。		発見型	自動型	四半期ごと			xx				XX
JP	**セキュアな接続** *Root （権限の制限）*	SCN-06		root（特権ユーザ）として実行される特権操作を最小化し、ネットワークサービスはrootで実行しないこと。	中	中	中			予防型	自動型	イベントごと	xx	xx	xx				XX

JP	**セキュアな接続** *ロールベースのアクセス制御*	**SCN-07**	IAM-05 IVS-09	ＩｏＴシステムにロールベースのアクセス制御（RBAC）を実装します。（これらのロールには）ユーザ、サービス、デバイスに関するロール（例えば、デバイス自身やローカルユーザ、システムオペレータ、監査者、個々のアプリケーション、ゲートウエイなどのロールを含めます）	中	中	中	たとえば、IBMでは、以下のロールや権限の組み合わせを使用しています。 ユーザ（管理者、オペレータ、開発者、アナリスト、参照者） アプリケーション（標準、運用、信頼されたバックエンド、データ処理、可視化、デバイス） ゲートウエイ（標準、特権）		予防型	手動型	イベントごと	xx	xx	xx	xx	xx	xx	XX
JP	**セキュアな接続** *特権操作*	**SCN-08**	IAM-05 IVS-09	IoTシステムに含まれる特権操作を特定します。そして、これらの特権操作に対応付けられて昇格されたロールを定めます。そうしたロールには、信頼済みのデバイス、特権ローカルユーザ、システム管理者、信頼済みのアプリケーション、信頼済みのゲートウエイなどが含まれることがあります。	中	中	中	特権操作は、その権限を承認されたグループのみが行われるようにすべきです。		予防型	自動型	常時	xx	xx	xx	xx	xx	xx	XX
JP	**セキュアな接続** *監査のためのユーザグループ*	**SCN-09**	AAC-01	監査ログについて、そのレビューやローテーションによるデバイスからの取り出しなどを含む管理を担当するユーザグループを実装します。この監査グループに対してはログの読み出しのみを許可します。この監査グループのメンバーを作成し、ログの参照権限を与えますが、いかなる監査ログに対しても、書き込みの権限は与えないようにします。	中	中	中	セキュリティイベントを発見するために必要なデータを監査ログとして収集し、十分な期間、それを保持していることを確認してください。		予防型	手動型	四半期ごと	xx	xx	xx	xx	xx	xx	XX
JP	**セキュアな接続** *ジオフェンシング*	**SCN-10**		正当な理由があれば、ジオフェンシング（位置・地域的な制限）や時間帯による制限など、追加の承認プロセスを実装します。	高	高	高	何が不適切な振る舞いかを検討して実装します。		予防型	自動型	常時			xx				XX
JP	**セキュアな接続** *サービスディスカバリの制限*	**SCN-11**	DCS-03	認証付きのディスカバリーサービス（サービス情報を提供するためのサービス）を実装します。すべてのサービス情報要求を認証し、認証に失敗した要求を受け付けないようにします。	中	中	中	サービス情報を得られなくすることで、攻撃者にとってシステム侵害はより困難になります。		予防型	自動型	常時			xx	xx	xx	xx	XX
JP	**セキュアな開発** *ソフトウエア保証成熟度モデル（SAMM）*	**SDV-01**		開発されたすべてのIoTデバイスとコンポーネントについてセキュアな開発ライフサイクルを確立するために、ソフトウエア保証成熟度モデル（SAMM）を適用します。（例えばOpenSAMMなど）	低	低	低	IoT製品に使用できる脅威モデリングアプローチは多数あります。例としては、マイクロソフトの脅威モデリングアプローチおよびOWASPのアプリケーション脅威モデリングがあります。 言語固有のセキュリティガイダンスは、Javascript（https://www.owasp.org/index.php/AJAX_Security_Cheat_Sheet）、Python（http://www.pythonsecurity.org/）、およびその他の言語で利用できます。	Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) Version 3.1 @ https://cloudsecurityalliance.org/group/cloud-controls-matrix/#_overview AIS-01: アプリケーションおよびプログラミングインタフェース（API）は、業界の主要な標準に従って設計、開発、展開、およびテストされるものとします。 (e.g., OWASP for web applications) 適用される法的、法定、または規制順守の義務を遵守するものとします。 「つながる世界」を破綻させないためのセキュアなIoT製品開発　13のステップ @ https://cloudsecurityalliance.jp/WG_PUB/IoT_WG/future-proofing-the-connected-world_J_20170520.pdf	予防型	手動型	イベントごと	XX	xx	xx			xx	XX
JP	**セキュアな開発** *統合されたフレームワーク*	**SDV-02**	CCC-01	IoT統合フレームワークを選択して、新しく開発されたIoTデバイスにおけるセキュアな組み込み、構成管理、資産管理、ディスカバリー、およびセキュアな接続を標準化します。	中	中	中	様々なIoTプラットフォームの選択肢が市場にあります。これらの例には、シーメンス、GE、SAP、PTC、IBM、AWS、マイクロソフト（ Azure）なども含まれます。		予防型	手動型	イベントごと	xx	xx	xx			xx	XX
JP	**セキュアな開発** *最小特権の原則*	**SDV-03**	IAM-02 IAM-05	最小特権の考え方を実施します。rootとして実行されるアプリケーションとサービスを制限し、すべてのアクセスに認証を要求します。ネットワークサービス（ウェブサーバーなど）をrootとして実行しないでください。	中	中	中	これらのコントロールは不正な利用の防止に役立ちます。		予防型	手動型	イベントごと	XX	xx	xx	xx	xx	xx	XX
JP	**セキュアな開発** *パスワードの処理*	**SDV-04**		適切なパスワード処理を確立します。パスワードをデバイスに固定的に書き込んだり、同じIDとパスワードを複数のデバイスに割り当てたりしてはいけません。パスワードは定期的に変更を要求してください。	低	低	低	パスワードについてのコントロールは、承認された利用者の特定とその操作を追跡するために役立ちます。		予防型	手動型	イベントごと	xx	xx	xx			xx	XX
JP	**セキュアな開発** *（脆弱性の）開示ポリシーと手続き*	**SDV-05**	SEF-03	セキュリティ上の脆弱性が発見もしくは報告された場合の責任ある開示ポリシーと手続きを確立するとともに、製品の修正計画に反映するための手順を実装します。脆弱性を報告してくれた独立したテスターと協力して、確実に脆弱性の修正を完了させます。	中	中	中	脆弱性の開示の目標は、脆弱性の修正とユーザーへの通知、被害とコストの最小化によりリスクを軽減すること、ユーザーがリスクを理解できるように十分な情報を提供し、協力と調整に関する期待を醸成することです。	Revision - ISO/IEC 29147:2018 Information technology -- Security techniques -- Vulnerability disclosure https://www.iso.org/standard/72311.html Old - ISO/IEC 29147:2014 Information technology -- Security techniques -- Vulnerability disclosure https://www.iso.org/standard/45170.html	是正型	手動型	イベントごと	xx	xx	xx	xx	xx	xx	XX
JP	**セキュアな開発** *マイクロコントローラ（MCU）*	**SDV-06**		マイクロコントローラ（MCU）と共に事前にプロビジョニングされたクラウドトラストアンカーを活用して、IoTデバイスのより安全なブートストラップと自動（Zero-touch)プロビジョニングをサポートするChip-to-Cloudの機能を組み込みます。 セキュアMCUのハードウェア機能を使用して、機密データと暗号化プリミティブ（暗号鍵など）を保護し、起動前にソフトウェアを検証することで信頼できるブートローディングを実行します。	中	中	中	Chip-toCloudオプションは、AWS/MicrochipやAzule Sphereなどに含まれます。	「つながる世界」を破綻させないためのセキュアなIoT製品開発　13のステップ @ https://cloudsecurityalliance.jp/WG_PUB/IoT_WG/future-proofing-the-connected-world_J_20170520.pdf	予防型	手動型	常時			xx				XX
JP	**セキュアな開発** *暗号コプロセッサ*	**SDV-07**		暗号処理コプロセッサを使用して、暗号処理によるCPUの負担を軽減します。IoT製品においては、（将来的に）脆弱になった既存の暗号アルゴリズムや鍵長を更新出来るように暗号処理を柔軟に設計します。十分にテストされた暗号モジュール（理想的にはFIPS140-2（https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf）認証済み）を使用します。暗号鍵の生成に使用する乱数については、良好なエントロピーを提供できる発生源を使用します。暗号モジュールが、暗号アルゴリズムのテスト、ソフトウエアやファームウエアの完全性テスト、重要な機能のテストなどを含む起動時テストを確実に行うようにします。	中	中	中	効果的な暗号化（技術）により、機密性と同時に可用性も確保されます。		予防型	手動型	常時			xx			xx	XX
JP	**セキュアな開発** *不要なハードウエア機能*	**SDV-08**		IoTデバイスにおいては、（たとえば使用しない無線機能やUSBインターフェイスなどの）不要な機能をロックダウンします。また、（JTAGやUART, GPIOなどの）テスト用インターフェイスについても向こうにするか、またはパスワード等でロックします。	低	低	低	これらのテスト機能は、よく開発中に有効となっています。デバイスを本運用にかける前に、これらのテスト機能を削除もしくは無効化するためのプロセスを確立してください。		予防的	手動型	常時	xx	xx	xx				XX
JP	**セキュアな開発** *耐タンパ性*	**SDV-09**		脅威環境に応じて（ハードウエアへの物理的な介入の脅威が懸念される場合は）、単純なシールやロックされたカバーから圧電回路に至るまで、IoTデバイスのセキュリティ上重要なコンポーネントにタンパープロテクション（物理的な介入に対する保護）を適用します。	高	高	高	物理的なセキュリティは、デバイスコンポーネントへのアクセス、ポートへの接続、またはアクティビティの監視によって侵害される可能性があります。 これらの侵害は、攻撃で使用したり、追加のアクセスを取得したりするために使用できます。		予防的	手動型	常時			xx			xx	XX

JP	**セキュアな開発** *セキュアOS*	**SDV-10**	IVS-07 MOS-15	デバイスのリアルタイムOS（RTOS）として、アプリケーションのサンドボックス化、セキュアブート、アクセス制御、信頼出来る実行環境、カーネルの分離、（最小限の機能を持つ）マイクロカーネルといったセキュリティ機能を提供するものを選択します。	中	中	中	こうしたタイプのRTOSでは（ソフトウエアの）最下層にセキュリティを組み込むため、ネットワークか他の物理デバイスかを問わず、攻撃を入り口で阻止する助けとなります。このようなセキュアRTOSは、悪意ある攻撃に対し、それがどこを入り口にして行うかに関係なく、OS保護に役立つ数々の重要なセキュリティ機能を提供します。強化されたセキュリティ機能を備えたRTOSは、リアルタイム接続機能を提供し、必要なネットワーク機能をサポートし、通常はLinuxなどの汎用OSよりも小さいフットプリントを持っているため、組み込み接続デバイスの最適な保護対策です。また、ファイルシステムオブジェクトの任意アクセス制御、ロールと機能を使用したきめの細かいユーザーアクセス制御、ユーザーの識別と認証制御、分散型サービス拒否（DDoS）攻撃の防止に役立つデバイスおよびシステムクォータを含む高度なセキュリティ保護、保証された通信リンクの信頼できるパスメカニズム、使用済みメモリの再利用または悪意による攻撃を防止		予防型	手動型	常時			xx			xx	XX
JP	**セキュアな開発** *API（認証）鍵*	**SDV-11**	EKM-04	API（認証）鍵やその他の資格情報を公開されたソースコード管理システム（たとえば、gitlab/githubなど）に置かないでください。API鍵のセキュアな取扱に関する手順を公表します。API鍵をファームウエアやモバイルアプリケーション、その他、いかなるクライアント側のアプリケーションのコードにも直接組み込んではいけません。少なくとも四半期に一回はAPI鍵やその他の資格情報が公開されたソースコード管理システムに保存されていないかどうかモニタ	低	低	低	API監査（項目）にAPIインテグレーション標準への準拠確認 を追加します。API鍵が暴露されていないかや、安全なAPI鍵管理（生成、配布、アクセス制御、認証）が実装されているかを確認します。 弱い暗号化実装を使用しないでください。		予防型	手動型	常時			xx		xx		XX
JP	**セキュアな開発** *MCU インテグレーション*	**SDV-12**		より高い保証要求を満たすために、ハードウエアによる隔離アーキテクチャを持つMCUを組み込みます。セキュリティを必要とするアプリケーションをラベル付けして、ハードウエア上で（信頼できないアプリケーションと隔離された）信頼された側でのみ実行しま	中	中	中	（こうした）セキュアMCUはNXP, Atmel, microchip, STMicroelectronics, Freescale, Infineonなど、様々なメーカーから入手できます。	「つながる世界」を破綻させないためのセキュアなIoT製品開発　13のステップ @ https://cloudsecurityalliance.jp/WG_PUB/IoT_WG/future-proofing-the-connected-world_J_20170520.pdf	予防型	手動型	イベントごと			xx			xx	XX
JP	**セキュアな開発** *タンパ対応メカニズム*	**SDV-13**	EKM-03	脅威の状況から必要とされる場合は、暗号鍵やその他の機微なデータをゼロクリアするといったタンパリング対応メカニズムを実装します。	高	高	高			予防型	手動型	イベントごと			xx			xx	XX
JP	**セキュアな開発** *特定業種用オペレーティングシステム*	**SDV-14**	IVS-07	運輸・交通システム、工業用制御システム、医療用機器など特定の業種（業務）用に使用する場合、これらの目的で認証を受けているリアルタイムOS（RTOS）を選択します。	高	高	高	業種別の認証には、DO-178B（航空、アビオニクス）、IEC61508（工業用制御システム）、ISO62304（医療機器用ソフトウエア）、SIL33/SIL4（交通及び原子力システムの安全度水準）などが含まれます。		予防型	手動型	イベントごと			xx			xx	XX
JP	**セキュアな開発** *サプライチェーン*	**SDV-15**	BCR-09 DSI-02 IAM-02 IAM-07 STA-01 STA-02 STA-03 STA-04 STA-05 STA-06 STA-07	サプライチェーンのプラクティスを確立します。たとえば、すべてのサードパーティのコンポーネントおよびフレームワークについてのセキュリティアラート情報を購読します。（アラート情報で）提案された更新の導入について、ただちに確認します。	低	低	低		「つながる世界」を破綻させないためのセキュアなIoT製品開発　13のステップ @ https://cloudsecurityalliance.jp/WG_PUB/IoT_WG/future-proofing-the-connected-world_J_20170520.pdf	予防型	手動型	イベントごと			xx	xx	xx	xx	XX
JP	**セキュアな開発** *サードパーティー製のライブラリ*	**SDV-16**	STA-08 TVM-03	すべてのサードパーティー製ライブラリのセキュリティを評価するために、静的、動的解析ツールを使用します。	中	中	中			是正型	半自動型	イベントごと			xx	xx	xx	xx	XX
JP	**セキュアな開発** *サードパーティー製のコンポーネント*	**SDV-17**	STA-08 TVM-02	IoTシステム内のすべてのサードパーティライブラリとソフトウェアコンポーネントの真正性と完全性を検証します。（訳注：偽物や改ざんされたコンポーネントの混入を防ぐ必要があります）	低	低	低			予防型	半自動型	イベントごと			XX	XX	XX	XX	XX
JP	**セキュアな開発** *Web サービス*	**SDV-18**	AIS-01	WebサービスはOWASP (https://www.owasp.org/index.php/Main_Page) ガイダンスに沿って開発します。	低	低	低	優先順位を付ける必要がある場合は、OWASP Top 10リストを使用し、定期的に更新を確認しますが、トップ10で終わらせないでください。Webアプリケーションの全体的なセキュリティに影響する可能性のある問題は数百あります。 アプリケーションのコードを1行も変更しなくても、新しい欠陥が発見され、攻撃方法が洗練されるため、脆弱になる可能性があります。 セキュリティの脆弱性は非常に複雑で、コードに深く埋もれる可能性があります。 多くの場合、これらの弱点を見つけて解消するための最も費用対効果の高いアプローチは、高度なツールを備えた「人間の専門家」です。 ツールだけに依存することは、誤ったセキュリティ感覚をもたらすため推奨されません。開発組織全体でセキュリティを企業文化の不可欠な部分にすることに重点を置いてください	https://www.owasp.org/index.php/REST_Security_Cheat_Sheet https://www.owasp.org/index.php/Web_Service_Security_Cheat_Sheet V18 of ASVS 4.0 (not released yet) https://github.com/OWASP/ASVS/blob/master/4.0/en/0x23-V18-API.md https://www.owasp.org/index.php/Web_Application_Security_Guidance	予防型	自動型	常時				xx			XX
JP	**セキュアネットワーク** *許可のないブルートゥース*	**SNT-01**		許可のないブルートゥースによるペアリング処理（例：JustWorks: マウスのような認証なしデバイス）を無効にします。	中	中	中	Bluetooth接続標準3および4を使用するには、他のデバイスとペアリングする前に認証が必要です（標準4の方が安全です）。		予防型	手動型	イベント毎	XX	XX	XX				XX
JP	**セキュアネットワーク** *ブルートゥースのセキュリティ*	**SNT-02**	CCC-03 EKM-03 GRM-01 GRM-02 IVS-06 IVS-12 IVS-13 IPY-04	NIST SP.800-121r2（https://www.nist.gov/publications/guide-bluetooth-security-1）ドキュメントのセクション4.4にあるbluetoothセキュリティチェックリストを使用して、bluetooth実装のセキュリティを監査します。 欠陥を修正します。	中	中	中	他のワイヤレステクノロジーと同様に、BLE（Bluetooth Low Energy）もセキュリティの脅威から逃れることはできません。Bluetooth LEビーコンはIOT設計に多くの可能性をもたらしますが、デバイスの追跡、盗聴、中間者攻撃などのセキュリティ上の脅威は著しく増加しています。 BLEデバイスは、事前定義された間隔でMAC、UUID、およびサービス情報をブロードキャストするように設計されています。 継続的な情報発信により、ハッカーはデバイスを簡単に追跡し、スニファーやスマートフォンを使用してブロードキャストされた情報をデコードできます。 ペアリング、安全なキー生成、ボンディング、静的/プライベートデバイスアドレスの暗号化、近接認証、非表示のMACなどの技術を使用して、IoTデバイスでのBluetoothの実装をセキュアにします。	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-121r2.pdf	予防型	半自動型	イベント毎	XX	XX	XX				XX
JP	**セキュアネットワーク** *ボットネット*	**SNT-03**	TVM-02	ネットワークセキュリティツールを、新しいボットネットアクティビティを検索し、検出された感染したIoTデバイスをすぐに削除するよう設定します。 CSA IoTWGボットネットトラッカー（https://gitlab.com/brianr/CloudSA_IoT_WG/wikis/iot_botnets）を使用して、ボットネットの特性に関する最新の情報を得ます。	中	中	中	脅威管理を使用して、新しいボットネットベースの攻撃を識別し、侵害の兆候に基づいて監査システムを構成します（特定のポートでのアウトバウンド通信など）。 拡散を防ぐため、感染したデバイスはすぐにオフラインにします。		検知型	自動型	常時	XX	XX	XX			XX	XX
JP	**セキュアネットワーク** *セキュアな設定*	**SNT-04**	CCC-01	IoTシステムをサポートするすべてのサポートソフトウェアおよびインフラストラクチャ（Webサーバー、モバイルアプリケーション、クラウドサービスなど）をセキュアに設定します。 システムの実装については、そのためのセキュア設定ガイダンスを参照してください。	中	中	中	セキュア設定ガイダンスには以下が含まれます。 CIS Benchmarks DISA STIGs		予防型	手動型	年1回						XX	XX
JP	**セキュアネットワーク** *ホワイトリスト*	**SNT-05**	IAM-02 IAM-08 IVS-06	IoTデバイス、ゲートウェイ、サーバー間のホワイトリストを設定します。 証明書を用意して、バックエンドコンピューティングデバイスとのすべてのMQTTおよびHTTP通信に対してTLSまたはDTLSベースの認証を利用できるようにします。	中	中	中			予防型	自動型	常時	X	X	X	X		XX	XX

JP	**セキュアネットワーク モニタリングルール**	**SNT-06**		サーバー/ゲートウェイが侵害された疑いがある場合には、不正行為を監視し、資格情報を取り消す手順を確立します。	中	中	中	このコントロールは、タイムリーで効果的なインシデント対応に役立ちます。		検知型	自動型	常時						XX	XX
JP	**セキュアネットワーク** *モビリティ*	**SNT-07**		モバイルアプリケーションのセキュリティ対策を確立します。 モバイルデバイスが承認済み/信頼できるリポジトリから更新を受信するようにします。 IoTデバイスの管理には、承認されたモバイルデバイスのみを使用するように指定します。 モバイルデバイスがIDや鍵の素材（情報）をハードウェアで保護された安全な保管場所（Android KeyChain / KeyStoreおよびiOS KeyChainなど）に保管する	中	中	中	すべてのモバイルプラットフォームには、安全な保管場所が用意されています。 Androidの場合、それはKeyChainとKeystoreです。 iOSの場合、それはKeychainです。 開発者は、利用可能な場合は、Androidデバイス上のハードウェアで裏付けられた安全な保存場所を使用するようにしてください。		検知型	自動型	常時					XX		XX
JP	**セキュアネットワーク** *NFC*	**SNT-08**	IVS-06 IVS-12 IVS-13 IPY-04	込み合っていて、スニファーのインストールが無理な場所には、近接通信（NFC）デバイスをインストールします。 これらのデバイスへのアクセスを監視するために、物理的なセキュリティ保護対策（カメラ/ガードなど）を設置します。	中	中	中		CTA。 ホームシステムを保護するための推奨ベストプラクティス	予防型	手動型	常時							XX
JP	**セキュアネットワーク** *SDP*	**SNT-09**	IAM-08 IVS-06	Software-Defined Perimeter（SDP）を設定し、ネットワークに接続する前にIoTデバイスを認証し、事前に承認されたロールと特権に基づいてアクティビティを制限するようにします。	中	中	中	SDPの方式は、すべてのデバイス/ユーザーからネットワークを隠します。 ネットワークとアプリケーションは、許可されたデバイス/ユーザーからの接続要求を除くすべての接続要求を拒否するゲートウェイの背後に隠されています。 デバイス/ユーザーは、デバイス/ユーザーが「事前承認」されていることを判断するために必要な情報を保存しているコントローラーで最初に認証される必要があります。その後、コントローラーは特定のユーザー/デバイスからの接続を受け入れるようにサーバーまたはゲートウェイに通知します。 ネットワークへのアクセスに加えて、デバイス/ユーザーが対話できるアプリケーションも事前に決定されています。	"https://downloads.cloudsecurityalliance.org/initiatives/sdp/SDP_Specification_1.0.pdf https://downloads.cloudsecurityalliance.org/assets/research/sdp/SDP-glossary.pdf アーキテクチャドキュメント1.0が進行中であり、2018年に完成する見込みです。 仕様2.0は、2018年12月下旬から2019年1月上旬に開始されます。 Anti-DDOSペーパーも進行中であり、2019年第1四半期に完成します。 https://www.nist.gov/sites/default/files/documents/2016/09/16/sdwan-sdn-response.pdf "	予防型	自動型	常時			XX				XX
JP	***セキュアネットワーク 視覚化ツール***	**SNT-10**		ネットワーク視覚化ツールを使用して、IoTデバイス、ゲートウェイ、およびサービスの動作状態と正常かどうかを監視します。 シンプルなハートビートモニタリングを使用して、デバイスの接続可否またはSNMPv3トラップを監視し、CPU接続、メモリ、およびその他の異常な動作を検出します。	中	中	中	これらのツールは、ネットワーク通信とトラフィックの問題の発見に役立ち、DoS攻撃の発見にも役立ちます。		検知型	自動型	常時	XX	XX	XX			XX	XX
JP	**セキュアネットワーク** *ワイヤレスネットワークの接続境界*	**SNT-11**		WSNの物理的境界を設定し、ZigBeeおよびZWaveデバイスの電力定格を制限して、信号漏洩を最小限に抑えます。	高	高	高			予防型	自動型	常時	XX	XX	XX			XX	XX
JP	**セキュアネットワーク** *ネットワーク分離*	**SNT-12**	IVS-09	ZigBee、ZWave、Bluetoothなどのワイヤレスセンサーネットワーク（WSN）をセットアップして、インターネットとの接続を承認済みゲートウェイのみとし、一般のインターネットからは遮断します。	中	中	中		CTA。 ホームシステムを保護するための推奨ベストプラクティス IoTのゼロからの保護　Microsoft Azureホワイトペーパー。	予防型	手動型	イベント毎	XX	XX	XX			XX	XX
JP	**セキュアネットワーク** *環境のスキャン*	**SNT-13**	IVS TVM	少なくとも四半期ごとに、物理環境をスキャンして、無線周波数（RF）攻撃や不正なデバイスの挿入などの異常を探します。	高	高	高			検知型	自動型	常時	XX	XX	XX				XX
JP	**セキュアネットワーク** *デバイスとの通信*	**SNT-14**	IVS TVM MOS	IoTデバイスとのすべての通信は、デバイスによって開始される必要があります。 不正な接続要求にはアラートを上げ、ログを取ります。	中	中	中			検知型	自動型	常時	XX	XX	XX				XX
JP	**セキュアネットワーク** *ZigBee のデフォルトの鍵*	**SNT-15**		デフォルトのZigBee Trust Center（TC）鍵を無効にし、搬送中の鍵の機密性を保護するためにデフォルト以外の鍵を生成/使用します。	中	中	中		https://www.blackhat.com/docs/us-15/materials/us-15-Zillner-ZigBee-Exploited-The-Good-The-Bad-And-The-Ugly-wp.pdf	予防型	半自動型	イベント毎	XX	XX	XX			XX	XX
JP	**セキュアネットワーク** *ZigBee のマスター鍵*	**SNT-16**		ZigBeeのマスター鍵をネットワークの外側で配布します。 マスター鍵をネットワーク経由で決して渡さないでください。 マスター鍵は、追加の鍵生成素材を生成するために使用されます。	中	中	中			予防型	自動型	常時	XX	XX	XX			XX	XX
JP	**セキュアネットワーク** *ZigBee のネットワーク鍵*	**SNT-17**		ZigBeeのネットワーク鍵を少なくとも年に1回更新し、新しいネットワーク鍵の配布/設定を行ったら以前の鍵を無効にします。	中	中	中			予防型	自動型	年に1回	XX	XX	XX			XX	XX
JP	**セキュアなネットワーク** *Zwave*	**SNT-18**	IVS-06 IVS-12 IVS-13 IPY-04	認証用に、AES 128暗号鍵でZ-Waveネットワークを補完します。 Z-Waveネットワークにアクセスするには、標準の4バイトのホームIDに加えてこれらの鍵を使用します。	中	中	中		CTA。 ホームシステムを保護するための推奨ベストプラクティス	予防型	自動型	常時	XX	XX	XX			XX	XX
JP	**運用における可用性** *メンテナンス計画*	**OPA-01**	BCR-07	保守計画を作成し、IoTハードウェアを定期的に検査および保守します。 部品在庫を持ち、 問題が検出されたらすぐにIoTデバイスの修理と交換ができるようにします。	中	中	中	IoTデバイスは機械的デバイスで、多くの場合可動部分を伴います。 運用上の可用性を維持するには、I.T.チームと機器の保守を担当する人々の間の関係を構築する必要があります。 IoTデバイスの具体的な種類に応じて、メンテナンスデポの作成、機器仕様の作成/管理、および運用メンテナンス計画の検討が必要になります。 可能であれば、予測モデリングを使用して起こりうるハードウェア障害の可能性を把握し対処します。	CSA CCM BCR-07から派生したもの。機器の保守のための方針と手順を確立し、支援する業務プロセスと技術的措置を実装し、運用とそれをサポート要員要員の継続性と可用性を確保しなければならない。	是正型	手動型	イベント毎	XX	XX	XX	XX		XX	XX
JP	**運用における可用性** *予防保全的分析*	**OPA-02**		予防保全分析を使用して、IoTシステムで予想されるパフォーマンスの問題または故障を想定します。 この分析に基づいて予防策を講じます。	高	高	高	予防保全では、機械学習モデルを使用して、障害が発生する可能性がある場所を予測します。 主に産業分野および製造業で使用されます。	https://www.ibm.com/blogs/internet-of-things/improving-operations-iot-predictive-maintenance/ https://aws.amazon.com/blogs/iot/using-aws-iot-for-predictive-maintenance/	是正型	自動型	常時			XX			XX	XX
JP	**運用における可用性** *Failover のサポート*	**OPA-03**	BCR-01 BCR-07	ノードやゲートウェイの地域間のフェールオーバーをサポートするようにクラウドサービスを設定します。 ある一つの地域がオフラインになった場合にフェールオーバーが自動的に行われることの確認のために、年1回テストします。	中	中	中	セカンダリIoTハフの設定とデバイスルーティングロジックの設定が含まれます。 クラウドサービスプロバイダは、デバイス設定のオンラインストレージ（twin, shadowなど）を提供しており、デバイスがオフラインのときでも設定の更新を確実に行えるようにするために使用できます。		予防型	手動型	年に1回							XX
JP	**運用における可用性** ***ネットワークトラフィック***	**OPA-04**	IVS-06 TVM-02	IoTデバイスから送信される異常に大量のトラフィックを識別して警告するように監視手順を設定します。それはセキュリティの侵害を示す可能性があります。そのようなトラフィックを検出したら、クライアントからの接続を自動的にレート制限するようにクラウドサービスを設定し、 DDoS攻撃の可能性から保護します。	中	中	中			予防型	自動型	常時				XX			XX
JP	**運用における可用性** ***サービスレベル条項 (SLA)***	**OPA-05**	STA-03 STA-05 STA-07	クラウドサービスプロバイダ（CSP）と交渉して、稼働率と対処のタイミング（インシデント/パッチ）に関するサービスレベル保証（SLA）を設定します。 SLAの違反に対して常にCSPに責任を負わせるようにします。	低	低	低	ISO / IEC 19086-1は、クラウドSLAに共通の要素を規定しています。		予防型	手動型	毎日							XX
JP	**運用における可用性** ***クラウドの設定***	**OPA-06**		IoTデバイスの設定をクラウドに保存します。 物理デバイスが切断されている場合でもデバイスロジックへのインタフェースをサポートするために、デジタルツイン、デバイスシャドウなどを構成します。 少なくとも年1回は、デバイスをオフラインにし、設定変更コマンドを送信してからデバイスをオンラインに戻すことによって、IoTハードウェアがオフラインの間にデバイス設定を更新できるこ						予防型	自動的	年に1回							XX

JP	**運用における可用性** ***無線によるセンサネットワーク（WSN）***	**OPA-07**	IVS-12	1つのゲートウェイがオフラインになった場合のフェイルオーバーのサポートと、高負荷にうまく対応するために、無線によるセンサネットワーク（WSN）のゲートウェイをクラスタ構成で設定します。 プライマリゲートウェイで障害が発生したときにバックアップゲートウェイと通信するようにIoTノードを設定します。 少なくとも年1回、フェイルオーバー機能と負荷の分散・分散機能をテスト	中	中	中	一部のIoTシステムはほぼリアルタイムの通信を必要であり、過度の待ち時間はシステムが侵害されていることを示している可能性があります。	Trusted and Secure Wireless Sensor Network Designs and Deployments. Bravo, Palomar, Gardel et al. 4 August 2017. MDPI Sensors	予防型	自動的	イベント毎						XX	
JP	**運用における可用性** ***無線センサーネットワーク***	**OPA-08**		大都市規模のファイバレスセンサーネットワーク配置を行う場合は、相互接続点を最小限に抑え、長距離トラフィックを減らすために、地理的区域毎に配置されたノードのクラスタを使用して設定します	中	中	中			予防型	手動的	常時	XX	XX	XX			XX	
JP	**運用における可用性** ***ネットワークのモニタリング***	**OPA-09**	IVS-06	ネットワーク監視ツールを展開し、輻輳についてIoTネットワークを監視します。 優先トラフィックフロー（例えば、差別化されたサービス）を確立し、輻輳した通信の検出時に動的再ルーティング（例えば、ＷＳＮ／ＳＤＮ）を実行します。	中	中	中			是正型	自動的	常時				XX		XX	
JP	**運用における可用性** ***ネットワーク遅延***	**OPA-10**		IoTノードがオフラインになってもメッセージングが利用できるように、少なくとも1日間（または環境によってはそれ以上）ゲートウェイでメッセージングをキャッシュします。	中	中	中			予防型	自動的	毎日						XX	XX
JP	**運用における可用性** ***通信の阻害***	**OPA-11**		無線（RF）通信を阻害しようとする妨害者の発見のために（地理的な）周辺領域をスキャンします。 そのような事象を検出したら、インシデント対応計画を実行します。	高	高	高			検知型	自動的	常時				XX			
JP	**運用における可用性** ***電池に関する警報***	**OPA-12**		バッテリの消耗を警告するようにノードを設定して、IoTノードの電力レベルを監視します。 これは、WSNアーキテクチャの重要なルーティングノードからエネルギーを浪費することを目的とした攻撃の防止に役立つ可能性があります。 バッテリーの過剰な消耗を伴う全てのインシデントを調査するようにします。	高	高	高		Trusted and Secure Wireless Sensor Network Designs and Deployments. Bravo, Palomar, Gardel et al. 4 August 2017. MDPI Sensors	予防型	自動的	常時	XX	XX	XX			XX	
JP	**資産と設定のトラッキング** ***インベントリ管理***	**ACT-01**	DCS-01 MOS-09	在庫管理システムを導入し、各IoTデバイスに関する詳細をインベントリ台帳に記録します。 このインベントリシステムを使用して、各IoTデバイスのバージョンを追跡します。併せて、ファームウェアやパッチのステータス、 RTOSのバージョン/イメージのバージョン、アプリケーション/ライブラリのバージョン、失われたまたは停止したステータス、デバイスが割り当てられている人、そして装置の位置を追跡します。	中	中	中	これはすべてのIoTデバイスに適用することが大事で、それにより、ボットネット活動で使用するためにデバイスが乗っ取られる脅威を減らします。		検知型	自動的	常時	XX	XX	XX			XX	
JP	**資産と設定のトラッキング** ***コンプライアンスの維持***	**ACT-02**		デバイスを監視して組織のポリシーに準拠していないデバイスを特定し、アップデートやパッチを指示します。	中	中	中	脆弱性またはベースラインセキュリティのスキャンにより、対処が必要なデバイスを特定できます。		検知型	自動的	常時	XX	XX	XX	XX	XX	XX	XX
JP	**資産と設定のトラッキング** ***更新スケジュール***	**ACT-03**		可能であれば、オンラインデータベースを実装して、IoT資産/インベントリデータベースへの変更を自動的に更新します。 このプロセスの自動化が不可能な場合は、最低四半期に1回、作業の実施をスケジュールします。	中	中	中	セキュリティリスクを管理するには、完全で正確な資産インベントリ管理が重要です。	https://www.cisecurity.org/controls/	予防型	自動的	常時	XX	XX	XX			XX	
JP	**資産と設定のトラッキング** ***名前付けの規則***	**ACT-04**	CCC-01	IoTデバイスの命名規則を確立し、各デバイスに一意の識別子を設定します。 識別子は、企業全体で一意であり、後日（たとえば合併や買収の際に）、大量の追加デバイスを命名の競合を起こさずに組み込めるように設計されている必要があります。	低	低	低	正確な識別子は、資産管理と脆弱性/パッチ管理に役立ちます。		予防型	自動的	イベント毎	XX	XX	XX			XX	
JP	**資産と設定のトラッキング** ***デバイスの識別子***	**ACT-05**		ライフサイクル全体にわたって、デバイスを追跡するために一意の識別子を使用します。それはまた、暗号化されたID /証明書をプロビジョニングするための基礎となります。	低	低	低	さらに、個々の識別子は、メンテナンス、トラブルシューティング、フォレンジック、および品質/パフォーマンスレビューに対するトレーサビリティを実現するのに役立ちます。		予防型	自動的	常時	XX	XX	XX			XX	
JP	**セキュアコンポーネント** ***デバイスおよびゲートウェイ***	**CMP-01**		ハードウェアによるセキュリティ機構を組み入れ、暗号化鍵の格納にハードウェア型のトラストアンカー用いて暗号動作、セキュアブート、ファームウェアのシグネチャ検証を行えるIoTデバイスを調達します。	中	中	中	一部のCSPは現在、「チップツークラウド」ソリューションを提供するためにチップメーカーと提携しています。 暗号化ライブラリを備えた低コストのマイクロコントローラ（MCU）がIoT製品に組み込まれており、デバイスとCSPの間でTransport Layer Security（TLS）およびその他の暗号化プロトコルトランザクションを実行します。 暗号化操作はハードウェアで行われるため、セキュリティがさらに強化されます。 チップツークラウドソリューションは、IoTデバイスに保存されているすべての暗号化プリミティブのハードウェアベースの処理と保存をサポートします。	NIST IR Report on Lightweight Cryptography @ http://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8114.pdf Microsoft IoT Security Best Practices @ https://docs.microsoft.com/en-us/azure/iot-suite/iot-security-best-practices Wireless: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-8.pdf Automotive: https://www.gsma.com/iot/wp-content/uploads/2018/03/Automotive-IoT-Security-digital-Mar-18.pdf Medical: https://downloads.cloudsecurityalliance.org/assets/research/owasp/OWASP_Secure_Medical_Devices_Deplo	予防型	自動型	イベント毎				XX		XX	
JP	**セキュアコンポーネント** ***ソフトウェアセキュリティメカニズム***	**CMP-02**		ハードウェアベースのセキュリティを実装できないデバイスの場合は、ソフトウェアセキュリティメカニズムを使用して重要な構成要素と暗号化機能を保護します。	中	中	中			予防型	自動型	イベント毎	XX	XX					
JP	**セキュアコンポーネント** ***セキュリティ評価***	**CMP-03**	GRM-10	レガシーIoTデバイスを毎年評価して技術の更新がないか確認します。 ハードウェアセキュリティのトラストアンカーをサポートしていない旧式のデバイスは、できるだけ早く交換する必要があります。 その間、ゲートウェイのセキュリティメカニズムを使用してセキュリティ境界を拡張し、これらの旧式のデバイスによってもたらされるリスクを軽減します。	低	低	低			予防型	手動型	年に1回	XX	XX					
JP	**セキュアコンポーネント** ***ハードウェアセキュリティメカニズム***			すべてのゲートウェイがFIPS 140-2に基づいて検証済み（https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf）のトラストアンカーを使用することを要求します。	中	中	中			予防型	自動型	イベント毎						XX	
JP	**セキュアコンポーネント** ***証明済みデバイス***	**CMP-05**		試験を通過し、自社の法令および規制に基づく順守義務に適合するデバイスセキュリティ認証を取得したIoT製品を超脱します。 デバイス認証は、業界、環境、使用方法、およびその他の要求水準の高い用途によって異なります。	高	高	高	セルラーネットワークを使用するデバイスには、GCF（Global Certification Forum）およびPTCRB（PCS Type Certification Review Board）のテストが必要です。 人体の近くで使用される装置はSAR（比吸収率）テストを必要とします。 CTIAは、IoTデバイス用のベースラインセキュリティ証明書を提供した最初の組織で	CTIAは現時点でセキュリティテスト企画を持っている。 - https://api.ctia.org/wp-content/uploads/2018/08/CTIA-IoT-Cybersecurity-Certification-Test-Plan-V1_0.pdf	予防型	手動型	イベント毎			XX			XX	
JP	**責任** ***責任の制限***	**LBT-01**	GRM-10	公衆や作業者と物理的にインターフェイスするIoTシステムの責任発生の可能性を検証します。安全上の制限事項を定め、警告通知を掲示します。	中	中	中	通知には、タイプ1の危険（過熱、衝撃などのデバイスのリスク）とタイプ2の危険（デバイスの操作または故障による危険）の両方を含める必要があります。		予防型	自動型	四半期ごと			XX				

JP	**事業継続** *継続計画*	**BCN-01**	BCR-01	事業継続計画を作成しシステム所有者の詳しい連絡先情報を記載します。これらの連絡先に警報を発報するシステムを作成し、IoTシステムが侵害されたり使用不能になった場合に、通知します。	中	中	中	NISTには、次の場所に継続計画ガイドがあります。 https://ithandbook.ffiec.gov/media/22151/ex_nist_sp_800_34.pdf	CSA CCM BCR-01から派生：事業継続計画の計画と開発のための一貫性のある一律のフレームワークを策定し、文書化し、適用します。それにより、すべての事業継続計画が、優先順位付けにおいて、テスト、保守、および情報セキュリティ要件に対して一貫性を保つようにします。	検知型	手動型	イベント毎	XX	XX	XX	XX	XX	XX	XX
JP	**脅威管理と緩和策** *脅威モデリング*	**TMM-01**	TVM-02	デバイスまたはシステム開発の開始時に脅威モデリングを実施します。コンポーネント、データフロー、および高価値コードの識別を含む、脅威のモデリングに標準化されたアプローチを使用します。脅威の定義、脅威の優先順位付け（評価など）、および緩和策の特定。脅威モデルの出力をシステム要件のバックログに伝え、製品またはシステムのライフサイクル全体にわたってこれらの要件を完了まで追跡します。	中	中	中	利用可能な脅威モデリングの手法は多数あります。カーネギーメロンのOCTAVE Allegro方式は、脅威モデリングのフレームワークを提供します。MicrosoftのSecure Development Lifecycleは、IoTに適用することもできます。MicrosoftにはSTRIDEと呼ばれる脅威分類支援機能があり、システムに関連する脅威をアナリストが識別するのに役立ちます。 STRIDEは、なりすまし(Spoofing)、改ざん(Tampering)、否認(Repudiation)、情報漏えい(Information disclosure)、サービス拒否(Denial of Service)、特権エスカレーション(Elevation fo Privilege)を意味します。各カテゴリに対して脅威が適切に特定されると、MicrosoftのDREADモデルを使用して脅威を評価できます。 DREADは、リスク評価プロセスで何を取り入れたかを記録するのに役立ちます：損害(Damage)、再現性(Reproducibility)、悪用危険度(Exploitability)、影響を受けるユーザ(Affected Users)、発見可能性(Discoverability)。脅威モデリングツールは、Webからダウンロードできます。 Microsoftのツールは、https://www.microsoft.com/en-us/sdl/adopt/threatmodeling.aspx	クラウドセキュリティアライアンスの繋がる世界を破綻させないために @ https://downloads.cloudsecurityalliance.org/assets/research/internet-of-things/future-proofing-the-connected-world.pdf Microsoft Threat Modeling @ https://docs.microsoft.com/en-us/azure/iot-accelerators/iot-security-architecture	予防型	半自動型	常時	XX	XX	XX	XX	XX	XX	XX
JP	**脅威管理と緩和策** *セキュリティ要件の検証*	**TMM-02**	TVM-02 BCR-02	セキュリティテストを作成し、各製品またはシステムリリースでそれらのテストを実行することにより、セキュリティ要件を検証します。	低	低	低			予防型	半自動型	常時	XX	XX	XX	XX	XX	XX	XX
JP	**脅威管理と緩和策** *脅威インテリジェンスフィード*	**TMM-03**	SEF-05	自社の業種に対応する脅威インテリジェンスの情報を入手します。自社のシステムを標的とする可能性が高い攻撃者のタイプとその動機を理解し、最新の状態に保ちます。	中	中	中	エンタープライズIoTシステムのセキュリティ状態の状況認識を維持することで、攻撃者とその動機、新しい攻撃手法、IoTデバイスを標的とする新しいボットネット、新たに発見された脆弱性を監視できます。状況認識を維持するためにリソースを割り当て、特定のIoT実装の脅威レベルが増加したときに必要に応じてアクションを実行します。		予防型	半自動型	常時	XX	XX	XX	XX	XX	XX	XX
JP	**脅威管理と緩和策** *製品の脆弱性*	**TMM-04**	TVM-02	製品の依存関係など、製品で新たに特定された脆弱性を監視します。サプライヤからの新しいパッチのリリースをモニタします。	低	低	低	最新のナレッジベースを備えた脆弱性スキャナーは、デバイスが新しいリスクや新たなリスクにさらされているかどうかを検出するのに役立ちます。		検知型	半自動型	常時	XX	XX	XX	XX	XX	XX	XX
JP	**脅威管理と緩和策** *ボットネット*	**TMM-05**		IoTデバイスをターゲットとする新しいボットネットを監視し、関連する特性（ポート/サービス）を直ちにネットワークセキュリティチームに伝えて、アクションを起こすようにします。	低	低	低	これには、企業内の接続されたデバイスの固有の脅威を理解するために、セキュリティオペレーションセンターアナリストの教育が必要です。		検知型	半自動型	常時	XX	XX	XX			XX	
JP	**脆弱性** *脆弱性管理*	**VLN-01**	TVM-02	IoTシステム用の脆弱性管理プログラムを策定します。IoTデバイスで、定期的または継続的に脆弱性評価を（少なくとも年に1回）実行します。IoTプロトコル仕様の更新をフォローし、ライブラリ内で今後発生するセキュリティ/プライバシーの更新を把握します。配備したIoTデバイス/システムに関連する脆弱性情報に基づいてリスクの一覧を更新され た状態に保ちます。	中	中	中	システム内で使用中のプロトコルを追跡し、基礎となる仕様が更新されたときにライブラリが適時に更新されるようにします。		予防型	手動型	常時	XX	XX	XX	XX		XX	XX
JP	**インシデント管理** *証拠保全の一貫性*	**IMT-01**	SEF-03	すべての監査の仕様と手順を文書化します。割り当てられた監査グループのメンバーのみが監査ログを読み取ることができ、ユーザーがこれらのログに書き込めないことを確認します。監査ログデータのオフロード（例：デバイスからクラウドまたはゲートウェイへ）に際して完全性が保護（例：HMACまたはデジタル署名）され、ログの完全性が長期の保存に対して確保されるようにします。すべての場合において、レビューの前にログファイルの完全性を検証します。	中	中	中	これは証拠保全の一貫性とフォレンジック調査にとって重要です。		予防型	手動型	イベント毎	XX	XX	XX			XX	
JP	**インシデント管理** *インシデント対応*	**IMT-02**	SEF-04	IoTインシデント管理計画を策定します。各IoTシステムのビジネスおよび技術的な連絡先（PoC）を特定し、セキュリティインシデントが発生した場合の役割と責任を通知します。インシデント対応におけるサードパーティ組織（ベンダーやサービスプロバイダーなど）の役割を定義します。デバイスから取得したログ/監査データの証拠保全の一貫性（chain-of-custody）を定義します。デバイスで実行する必要があるエスカレーション手順とフォレンジック対応を定義および確立します。ネットワークデバイスからリアルタイムで自動的にフォレンジック（データ）を取得する機能を検討するよう	高	高	高	インシデントが発生する前に、インシデントへの適切な対応を計画する必要があります。 ITILとISACAは、効果的なインシデント管理プロセスを確立するためのガイダンスを提供しています。 CSIRTは、トレーニングやコンピューターセキュリティ対応チームハンドブックなどのリソースを提供します。インシデント証拠の不適切な取り扱いは、訴訟対応を困難にする可能性があります。	CSA CCM SEF-04から派生：情報セキュリティインシデントが発生した場合、所管の法管轄に基づいて起こりうる法的手続きに対応して証拠を提示するには、適切なフォレンジック手順と証拠保全の連鎖体系が必要です。セキュリティ侵害によって影響を受ける顧客その他の外部のビジネス利害関係者は、通知があれば、法的に許諾された範囲で、フォレンジック調査に参加する機会が与えられなければいけません。	是正型	手動型	年に1回	XX	XX	XX	XX	XX	XX	XX
JP	**物理セキュリティ** *物理的アクセス*	**PHY-01**	DCS-09	IoTエッジデバイスへの物理的アクセスを制限し、物理的アクセスの試みを警告する物理的セキュリティプロセスを確立します。	中	中	中	物理的なアクセスにより、盗難、損傷、コンポーネントへの不正アクセス、デバイスポートへのリード線の取り付け、およびデバイスの侵害またはさらなるアクセスのためのデバイス動作の不正監視のリスクが高まります。		予防型	手動型	常時	XX	XX	XX			XX	
JP	**誤使用** *資格情報の失効*	**MSU-01**		誤使用パターンを定義し、資格情報を失効するためのポリシーを確立します。不正行為を報告および判断するための手順を実装します。承認取り消し後1日以内に資格情報を失効させるための手順を確立して実装します。	高	高	高			予防型	自動型	常時	XX	XX	XX	XX	XX	XX	XX
JP	**誤使用** *振る舞い分析*	**MSU-02**	IVS-01	ほぼリアルタイムでデバイスの使用状況とデバイスの誤使用に関するデータストリームを収集して分析する分析ツールを使用します。	高	高	高	例としては、Azure Stream Analytics（Azure IoT HubとSuiteを含む）、AWS IoT Analytics、SAP Analyticsクラウド、IBM Watson IoTプラットフォーム、Cisco Data Analytics、およびOracle StreamとOracle Edge Analyticsがあります。		検知型	自動型	常時			XX	XX		XX	XX
JP	**誤使用** *企業規模の監視*	**MSU-03**		権限の昇格、ファームウェアアップデートイベントの成功/失敗、IoTデバイスとサービスソフトウェアの設定変更、アカウントの変更、そして改ざんイベントを含む、セキュリティ関連のすべてのイベントを定義します。それらのイベントおよびその他の関連するセキュリティイベントを、IoTシステム全体にわたり監視します。監視対象にはあらゆるデバイス、クラウドサービス、モバイルまたはネットワークサービスそしてストレージシステムを含みます。セキュリティイベントの種類ごとにしきい値を定義し、しきい値を超えたときに調査を開始するようにします。	中	中	中			検知型	自動型	常時			XX	XX	XX	XX	XX
JP	**誤使用** *ロギング*	**MSU-04**	IVS-01	失敗したリモートアクセス試行（SSH、Webなど）をすべて記録します。 30分以内に5回連続してアクセスの失敗が検出されると自動的にセキュリティ管理者に警告するプロセスを作成します。	中	中	中	組織は、IoTシステムに固有のセキュリティ関連のイベントを定義し、それらのイベントからのデータを監視する必要があります。		検知型	自動型	イベント毎	XX	XX	XX			XX	
JP	**誤使用** *イベントデータ*	**MSU-05**	IVS-01	セキュリティイベントデータを自動的にクラウドに送信して保存および分析します。送信者、受信者、タイムスタンプ、データ、およびイベントタイプを最低限記録してください。	中	中	中			検知型	自動型	常時			XX			XX	

JP	**誤使用** *ワイヤレス検知*	MSU-06	IVS-12	企業全体にわたるIoTの無線通信の検出機能を設置します。構内で動作している不正なワイヤレスデバイスを調査により検出します。既知のボットネットのC&Cアドレス/ポートへのネットワーク通信を調査により検出します。ベンダーのIPアドレスへの不正な通信を調査により検出します。発見したデバイス/通信をただちに無効にして、違反の原因を調査します。想定外の違反が発生したときにユーザーに警告するシステムを実装します。	高	高	高	特定のIoTシステムの誤使用や悪用を監視するためのパターンを定義することで、SIEM内でシステムを監視するためのルールを作成することができます。	OpenDNSレポートを参照	検知型	自動型	常時				XX				
JP	**安全な運用** *安全への影響*	SOP-01	GRM-10	IoTシステムの安全性への影響を評価し、すべての安全性リスクを記録し、これらのリスクに優先順位を付け、そして各リスクに対する緩和策を実装します。安全要求事項を実行させるために、デバイスおよび使用環境に対するコントロールを組み込みます。	中	中	中	安全上のリスクには、感電や火災のリスクなど、電子機器の使用による一般的なリスクが含まれます。 IoTデバイスには、動作障害による安全上のリスクもあります。		予防型	半自動型	イベント毎	XX	XX	XX	XX	XX	XX	XX
JP	**安全な運用** *フォールトツリー分析*	SOP-02		IoTシステムに関連する安全上のリスクを識別して優先順位を付けるために、フォールトツリー分析（FTA）を実行します。	中	中	中	安全上のリスクを優先する場合は、不適切な使用による安全上のリスクも考慮してください。		予防型	半自動型	イベント毎	XX	XX	XX	XX	XX	XX	XX
JP	**安全な運用** *ロギングシステム*	SOP-03	IVS-01 IVS-07	組織のロギング機能を設計および実装します。証拠保全の一貫性(Chain of Custody)を可能にするために、生成から保管までのすべてのログの完全性を保護します。	中	中	中	信頼できるログは優れた検知型コントロールであり、根本原因の分析に役立ちます。		予防型	自動型	常時			XX			XX	
JP	**クラウドサービス** *クラウドサーバ*	CLS-01	IAM-02	すべてのクラウドサーバーに一意のIDを割り当てます。サーバーが相互に、およびすべてのゲートウェイに対して認証することを要求します。	中	中	中			予防型	自動型	常時							XX
JP	**クラウドサービス** *クラウドゲートウェイ*	CLS-02	IAM-08 IVS-06	信頼できるデバイスからの通信のみを受け入れ、暗号化通信を要求するようにクラウドゲートウェイを構成します。クラウドゲートウェイ上の許可されたポートとプロトコルを文書化し、許可されていないポート/プロトコルを無効にします。システムと通信しようとする不正なデバイスをブラックリストに追加し、そのアクションを記録して管理者に報告します。	中	中	中			予防型	自動型	常時							XX
JP	**クラウドサービス** *クラウドゲートウェイ閉鎖*	CLS-03		通信が完了したらクラウドへの接続を閉じ、データを再度送信する必要があるときに新しい接続を開始するようにゲートウェイを構成します。	中	中	中			予防型	自動型	常時						XX	XX
JP	**クラウドサービス** *クラウドプライバシー*	CLS-04	STA-05	クラウドサービスプロバイダー（CSP）と協力して、クラウド内で処理されたデータが、法的、法定、および法令順守の義務に適合するプライバシーガイドラインを満たしていることを確認します。データをCSPに移行する前に、プライバシーバイデザイン原則の適用を検討します。それにより、（CSPによるSLA違反の場合）データ管理者がデータの復旧と保持ができるようになります。	中	中	中		設計によるプライバシーの7つの原則 https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf ヨーロッパのデータ保護規制 https://eugdpr.org/ CSA GDPRリソースセンター https://gdpr.cloudsecurityalliance.org/	予防型	自動型	常時							XX
JP	**クラウドサービス** *セキュリティガイダンス*	CLS-05		クラウドサービスをセキュアに設定します。利用する特定のCSPに適用できるCSPセキュリティガイダンスの指示内容に従ってください。	低	低	低			予防型	自動型	イベント毎							XX
JP	**クラウドサービス** *クラウド基盤のアップデート*	CLS-06	TVM-02	すべてのクラウドインフラストラクチャを最新かつパッチ適用済みの状態に保ちます。	低	低	低			予防型	自動型	常時							XX
JP	**クラウドサービス** *IoTとクラウドのインタラクション*	CLS-07	IVS-01 SEF-03	すべてのAPI呼び出しを監視し、APIの不正使用が疑われる場合に警告します。	中	中	中			検知型	自動型	常時							XX
JP	**クラウドサービス** *クラウド認証*	CLS-08	IAM-09	クラウドサービスにアクセスするIoTデバイスを認証します。認証に失敗したデバイスのアクセスを拒否し、そのアクセス試行をログに記録します。セキュリティ管理者へのアラートをトリガーする一定時間内の失敗数のしきい値を設定し、アラートの配信方法を詳細に設定します。たとえば、デバイスが30分に5回以上認証に失敗した場合は、セキュリティイベントとしてシーケンスにフラグを立て、セキュリティ管理者に警告します。	低	低	低			予防型	自動型	常時							XX
JP	**クラウドサービス** *管理者のID*	CLS-09		IoTサービス管理コンソールへのアクセスに認証を要求します。管理コンソールにアクセスする各オペレーターおよび管理者に固有のIDを付与します。	低	低	低	このコントロールは（管理操作を誰が行ったかという）説明責任を実現します。		予防型	自動型	常時			XX	XX	XX	XX	XX
JP	**クラウドサービス** *システムのID*	CLS-10		管理システムのAPIにアクセスする各システムに固有のIDを設定します。	低	低	低			予防型	自動型	常時			XX	XX	XX	XX	XX
JP	**クラウドサービス** *APIに対する認証*	CLS-11	IAM-09	管理コンソールとAPIログインに認証のベストプラクティスを使用します。	中	中	中			予防型	自動型	常時			XX	XX	XX	XX	XX
JP	**クラウドサービス** *APIに対するネットワークアクセス*	CLS-12	IVS-06	管理コンソールおよびAPIへのネットワークアクセスを　送信元IPアドレスかデバイス認証（もしくは両方）によって制限します。	中	中	中			予防型	自動型	常時				XX			XX
JP	**クラウドサービス** *管理者操作のログ*	CLS-13	IVS-01	管理コンソールとAPIを介してすべての管理活動をログに記録して確認します。	中	中	中			検知型	自動型	常時				XX			XX
JP	**クラウドサービス** *コンピュータの保護*	CLS-14	TVM-01	管理コンソールまたはAPIにリモートからアクセスするために使用されるコンピュータをマルウェアやその他の脅威から保護します。	低	低	低			予防型	自動型	常時				XX			XX
JP	**クラウドサービス** *セキュアなOTA*	CLS-15		侵入や悪意のあるロジックから保護するために、Over-The-Air（OTA）アップデート用のセキュアなステージングシステムを実装します。ファイルをエッジデバイスに送信する前に、ファイルに整合性制御を適用します。	中	中	中			予防型	自動型	イベント毎	XX	XX	XX	XX		XX	XX
JP	**セキュア通信** *MQTT トピック*	COM-01		許可されたMQTTトピックを定義してください。ブローカー内にアクセス制御リストを作成して適用し、IoTデバイスがコンテンツをPublishしたり、許可されていないメッセージトピックをSubscribeしたりすることを制限します。	中	中	中	多くのIoT実装は、MQTTなどのPublish/Subscribeプロトコルを使用します。 システム内で使用される機密トピックに読み取り/書き込み制限を実装することを検討してください。		予防型	自動型	常時			XX	XX		XX	XX
JP	**セキュア通信** *MQTT 暗号化*	COM-02		パスワードフィールドのパスワードを含むすべてのMQTTメッセージがTLSを使用して暗号化されていることを確認してください。	低	低	低	デフォルトでは、MQTTはパスワードフィールドを暗号化しません。		予防型	自動型	常時			XX	XX		XX	XX
JP	**セキュア通信** *MQTT 認証*	COM-03		MQTTトランザクションの認証には、ネイティブのユーザー名/パスワード機能ではなく、証明書を使用します。	中	中	中	TLSが使用されている場合、クライアントはSSL証明書を使用してクライアントを認証できます。 クライアントは、LDAPまたはOAuthトークンを使用して認証したり、OS認証メカニズムを利用することもできます。 MQTTには、サーバーを認証するためのメカニズムはありません。 ただし、TLSの使用時またはVPNの使用時にSSL証明書を使用すると、クライアントが接続しようとしているサーバーを識別できます。	http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/errata01/os/mqtt-v3.1.1-errata01-os-complete.html#_Toc442180929 5.4.1 and 5.4.3	予防型	自動型	常時			XX	XX		XX	XX
JP	**セキュア通信** *MQTT 帯域幅調整*	COM-04		グローバルおよびクライアントごとの両方でMQTTサーバへの通信の帯域制御を検討してください。	高	高	高	サーバへの通信を帯域制御することで、サーバは過負荷から保護されますが、それにより、遅延や可用性の問題が発生する可能性があります。		予防型	自動型	常時			XX	XX		XX	XX
JP	**セキュア通信** *MQTT ファイアウォール*	COM-05		ファイアウォールを介してMQTT通信トラフィックをルーティングします。	中	中	中	IPアドレスまたはクライアント情報に基づいてトラフィックをブロックすることも候補のひとつです。		予防型	自動型	常時			XX	XX		XX	XX
JP	**セキュア通信** *最大メッセージ長*	COM-06		MQTTメッセージの最大長を短くして、攻撃者が大きなメッセージを送信してシステムに過負荷をかけることを制限します。	中	中	中	メッセージ長が小さいと、DoS攻撃を防ぐのに役立ちます。		予防型	自動型	常時				XX			

JP	**セキュア通信** *MQTT サービス*	**COM-07**		セキュアなアクセスによって堅牢化されたOSにのみMQTTブローカーをインストールしてください。	中	中	中	基盤となるソフトウェアまたはハードウェアに脆弱性があると、サービスをセキュアに保護できません。		予防型	自動型	常時			XX			XX	
JP	**セキュア通信** *TCP 通信*	**COM-08**	EKM-03	X.509認証（https://tools.ietf.org/html/rfc7525）のTLSを使用して、システムコンポーネント間のすべてのTCPベースの通信（例：REST、MQTT、AMQP）を暗号化します。	中	中	中	SSLおよびTLSバージョン1.0および1.1の使用は現在推奨されていません。 これを書いている時点で、NISTはTLSバージョン1.3またはバージョン1.2の使用を推奨しています。 使用中のIoTシステムが、最新版のNIST SP800-52で推奨されているTLSバージョンを使用していることを確認してください。	NIST SP 800-52 Revision 1 (Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations) @ http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf IETF RFC 7525 Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) @ https://tools.ietf.org/html/rfc7525 https://csrc.nist.gov/publications/detail/sp/800-52/rev-2/draft	予防型	自動型	常時			XX	XX	XX	XX	XX
JP	**セキュア通信** *UDP 通信*	**COM-09**	EKM-03	IETF RFC7525またはより新しい規格で指定されているDTLS (Datagram Transport Layer Security) プロトコルを使用して、システムコンポーネント間のすべてのUDPベースの通信（たとえばCoAP (Constrained Application Protocol) ）を暗号化します。	中	中	中	多くのIoTプロトコルはUDPベースの通信を必要とします。 これらのプロトコルでは、TLSは実行可能なオプションではないため、最適解はTLSのデータグラム向け同等機能であるDTLSを使うことです。 IETF Best Practice Guidance RFC 7525で指定されているように、UDPベースのプロトコルを保護するためにDTLSを実装してください。		予防型	自動型	常時			XX	XX	XX	XX	XX
JP	**セキュア通信** *無線 LAN 暗号化*	**COM-10**	EKM-03	IoTシステム内のすべての無線LAN通信を暗号化します。	低	低	低	暗号化は通信の機密性を保護し、中間者攻撃の有効性を低下させます。		予防型	手動型	常時			XX	XX	XX	XX	XX
JP	**セキュアなデータ** *データ分類*	**DAT-01**	DSI-01 DSI-04	IoTシステム内で収集、処理、保存されたデータを文書化します。 データの種類と価値（組織にとっての重要性と機微性）に基づいてそのデータを分類します。 システム内のデータの種類を識別するために使用できるメタデータでデータにタグを付けます。	低	低	低	効果的な管理には、データのセキュリティが危うくなった場合のデータの価値と組織への影響を理解することが必要です。 コントロールの程度はその価値に対応している必要があります。	CSA CCM DSI-01から派生：データとデータを含むオブジェクトには、データの種類、値、機密性、および組織に対する重要性に基づいて、データ所有者が分類を割り当てるものとします。	予防型	手動型	常時	XX	XX	XX	XX	XX	XX	XX
JP	**セキュアなデータ** *データセキュリティコントロール*	**DAT-02**	DSI-01	各データタイプの分類に基づいてデータセキュリティコントロールを実装します。	中	中	中	コントロールのレベルは、危険にさらされているデータの価値に基づくべきです。 ほとんど価値のないデータに対する強力なコントロールは、リソースの無駄遣いです。 貴重なデータに対するコントロールが弱い、または存在しないと、組織は許容できないリスクにさらされます。		予防型	手動型	常時			XX	XX	XX	XX	XX
JP	**セキュアなデータ** *データの情報源*	**DAT-03**	IAM-02 IAM-07 IAM-09	社内および第三者のデータの情報源の一覧をつくります。 IoTシステム内でホストされているすべてのデータに認証を適用します。 データの整理、削減、変更、集計に際して、システム全体を通じてデータの流れを追跡します。 これらの手順を作成する際には、セキュリティプロトコルの機能をテストして、自動化されたIoTの意思決定プロセスで用いられたデータについて、そのデータのソースと、そのデータに作用したすべてのユーザおよびプロセスを、効率的に特定できることを確認します。	中	高	中	自動化された処理はIoTシステム内で行われます。 これらの処理は、デバイスとデータの間の関係に基づいて行われます。 複数のIoTデバイスで発生するイベント間の因果関係を理解することが、IoTシステム内で発生する処理を調査する場合に役立ちます。		予防型	自動型	常時			XX	XX		XX	XX
JP	**セキュアなデータ** *保存データの暗号化コントロール*	**DAT-04**		IoTシステムでデータの一覧をつくった後、データを格納する場所とシステムを特定し、それらに保存データの暗号化の管理策を適用します。 機密情報を保存する際に、新しいシステムやコンポーネントがセキュリティの評価を受けずに実装されていないことを監視によって確認します。	中	中	中	NISTには、AESとTDEA（またはTDES）の2つの承認済みブロック暗号があり、いずれも推奨できます。 ただし、IoTデバイスでは計算リソースが限定されているため、軽量暗号が選択肢のひとつとして研究されています。	NISTは「軽量暗号」の研究と評価を行っています。 https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8114.pdf	予防型	自動型	常時			XX	XX	XX	XX	XX
JP	**セキュアなベンダからのリモートアクセス** *ベンダのサービスレベル契約*	**RMT-01**	STA-05	サプライヤとサービスレベル契約(SLA)を結びます。 これらのサービスレベル契約には、インシデント管理サポート（フォレンジック調査中のサポートを含む）、および最小限の脆弱性の開示とパッチの更新の両方のタイムラインが含まれるべきです。	中	中	中	SANSには、クラウドコンピューティングのサービスレベル契約におけるセキュリティに関する主要な指標を提案する論文があります。	https://www.sans.org/reading-room/whitepapers/cloud/proposal-standard-cloud-computing-security-slas-key-metrics-safeguarding-confidential-data-cloud-35872	予防型	自動型	常時			XX	XX	XX	XX	XX
JP	**セキュアなベンダからのリモートアクセス** *サードパーティのアクセス*	**RMT-02**	IAM-07	リースされたIoTデバイスへのサードパーティ（訳注：リース会社、保守会社、メーカーなど）からのアクセスと管理に関するポリシーと手順を確立します。 これには、組織外に送信可能なデータ（例：計測データ）、承認された役割、および組織のネットワーク内のデバイスを管理するための最低限のアクセスセキュリティ要件が含まれます。 これらの管理策を適用し、費用を管理します。	中	中	中	多くのIoT機器（例えば病院用スキャナー）はリース品であり、ベンダーによる管理を必要とします。 ベンダーによるIoTデバイスの設定とログへのアクセスは認証される必要があります。		予防型	自動型	常時			XX	XX		XX	XX
JP	**資格情報管理** *鍵管理プロセス*	**CRD-01**	EKM-03	IoTシステムのための安全な鍵管理手続きを整えるようにします。 それには最低限、鍵生成、鍵の変更、鍵の設定と転送、鍵の保管、鍵の期限管理、鍵のゼロ化/破壊を備える必要があります。 デバイスが十分にランダムなエントロピー源を備えているならば、鍵は可能な限りデバイス上で生成するべきです。 サービス側での（集中的な）鍵の生成と配布は、鍵マテリアルの配送に安全な輸送の仕組み（別チャネルでの配布（out-of-band provisioning）を含む）が使われる場合には、許容されます。	中	中	中			予防型	自動型	イベント毎			XX	XX		XX	XX
JP	**資格情報管理** *鍵管理ポリシー*	**CRD-02**	EKM-04	秘密鍵が複数のデバイスまたはグループ間で共有されないようにするためのポリシーを確立します。 鍵の生成のために可能な限り前方秘匿性 (forward-secrecy) を組み込んでください（例えば、静的メカニズムを使用しないでください）。 鍵は、許可されていないアクターによる鍵へのアクセスを制限できる安全な場所（ソフトウェアまたはハードウェア）に常に保存する必要があります。鍵は可能な限り3年以内、理想的には1年以内に有効期間を制限する必要があります。 鍵の更新に自動化されたメカニズムを使用します（ローテーションや派生など）。	中	中	中			予防型	自動型	年に1回	XX	XX	XX	XX		XX	XX
JP	**資格情報管理** *鍵管理ユーザグループ*	**CRD-03**		IoTデバイスおよびサービス用に安全に鍵管理を構成するための専用の鍵管理ユーザーグループを設定します。	高	高	高			予防型	手動型	イベント毎			XX	XX		XX	XX
JP	**資格情報管理** *セキュアな初期接続*	**CRD-04**		IoTデバイスをネットワークに安全に初期接続するためのプロセスを確立します。 自動登録が可能なIoTデバイスを優先してください。これらのデバイスは、製造元の資格情報がハードウェアに埋め込まれてプリロードされているためです。自動登録では、登録するデバイスのシリアル番号と公開鍵をロードするための信頼できる帯域外プロセスが必要です。 自動津録が利用できない場合は、ネットワークを利用する前に、デバイスのシリアル番号を登録し、ID / 鍵/証明書をデバイスに事前ロードするように信頼できる機能を設定してください。 すべての場合において、すべてのアカウント登録および更新コマンドを暗号化してください。	中	中	中			予防型	自動型	イベント毎	XX	XX	XX			XX	

JP	**資格情報管理** *デフォルトパスワード*	**CRD-05**		デフォルトのパスワードを含むデバイスを監査および識別し、配備後すぐに（できればネットワークに接続する前に）それらのパスワードを変更します。 他のデバイスとパスワードを共有しているデバイスを特定し、それらのパスワードをただちに変更します。 リモートアクセスキーを共有するデバイスを識別し、速やかに、それらのデバイスをそれぞれ固有の資格情報に更新します	低	低	低	1）さまざまなシステム（ゲートウェイとクラウドの両方）で適用できるパスワードポリシーがあるはずです。 2）オープンソースソフトウェアによって自動的に有効にされたデフォルトアカウントを無効にすることを検討し、代わりにR&Rマトリックスに従ってアカウントを作成してください。	IEEE Security Best Practices @ https://internetinitiative.ieee.org/images/files/resources/white_papers/internet_of_things_feb2017.pdf	是正型	自動型	常時	XX	XX	XX			XX	
JP	**資格情報管理** *リモートアクセス*	**CRD-06**		ネットワークを構成するIoTデバイスの数を考えると、IoTデバイスへのリモートアクセスには、可能な限りパスワードではなく証明書を使用することをお勧めします。 デバイスの数が増えると、パスワードの管理が難しくなります。 パスワードを使用してリモートでIoTデバイスにアクセスする場合は、少なくとも年に1回はそれらのパスワードを更新してください。 可能であれば、これらのパスワードを自動的に更新するメカニズムを実装してください。	中	中	中			予防型	手動型	年に1回	XX	XX	XX			XX	
JP	**資格情報管理** *トラストアンカー*	**CRD-07**		デバイス証明書とトラストアンカーの安全な更新を管理するためのプロセスを確立し、技術をを取得します。 可能であれば自動更新機能を選択してください。 デバイストラストアンカーを更新するためのアクセスを許可された管理者に制限します。	低	低	低			予防型	半自動型	イベント毎			XX			XX	
JP	**資格情報管理** *証明書管理ポリシー*	**CRD-08**		証明書管理ポリシーを確立します。 証明書の割り当て前にデバイス識別情報の検証（enrollment）の最小要件を定義します。 デバイス識別情報の検証は、（ａ）人による審査、または（ｂ）（例えば製造業者により）確立された鍵情報に基づく自動プロビジョニングに基づくべきです。	中	中	中			予防型	手動型	イベント毎			XX			XX	
JP	**資格情報管理** *運用証明書*	**CRD-09**		運用証明書の有効期間を3年以内に設定します。 製造元は、有効期限なしでデバイスアイデンティティ証明書を埋め込むことができますが、これらの証明書は短期間の運用証明書を確立するためにのみ使用してください。	中	中	中			予防型	自動型	イベント毎			XX	XX	XX	XX	XX
JP	**資格情報管理** *自動証明書プロセス*	**CRD-10**		証明書の更新を含めた自動証明書（発行）プロセスを確立します。	中	中	中			予防型	自動型	常時			XX	XX	XX	XX	XX
JP	**資格情報管理** *証明書失効*	**CRD-11**		証明書失効のプロセスを確立します。これには、必要な報告経路、調査方法、および失効リストへの掲載の承認または不承認を決定する認証局が含まれます。	高	高	高			是正型	手動型	イベント毎			XX	XX	XX	XX	XX
JP	**End-of-Life** *End-of-Life の手順*	**EOL-01**	DSI-07	IoTシステムハードウェアのend-of-lifeの手順を定義します。機密情報を保管しているハードウェアについては、その手順は、ハードウェアを安全に破棄し、プロセスに参加している個人を含む破棄プロセスの監査ログを維持すべきです。	中	中	中	これらの手順では、プライバシーと重大性のリスク評価に基づいて、破棄する必要があるデータの種類と、いつ、どこで、または誰と、どの方法で、明確に定義する必要があります。	CSA CCM DSI-07からの派生：データの安全な廃棄とすべての記憶媒体からの完全な削除が実現できるような業務プロセスと技術的手段をサポートするような方針と手順を確立し、データがいかなるコンピュータフォレンジック手段によっても回復できないようにしなければいけません。	予防型	手動型	イベント毎	XX	XX	XX	XX	XX	XX	XX
JP	**システムコンポーネントの更新** *構成管理ボード*	**UPD-01**	CCC-03	IoTシステムへの修正/変更を吟味するために構成管理ボード（CCB）を確立します。 CCBは、アップデートのためのプロセスを定義する必要があります。これには、実施前のすべてのアップデートのテスト（機能、セキュリティ、相互運用性）を含める必要	中	中	中	構成管理ボードを使用することで、変更管理プロセスが確実に守られるようになります。		予防型	自動型	イベント毎	XX	XX	XX	XX	XX	XX	XX
JP	**システムコンポーネントの更新** *テストネットワーク*	**UPD-02**		IoTの実稼働環境をよく反映したテストネットワークを実装します。実運用に入る前に、テストネットワーク上のすべてのアップデート/パッチをテストします。	中	中	中	テストネットワークを使用して、アップデートが正しく機能していること、および新しいデバイスが導入されていることを確認できます。		予防型	半自動型	イベント毎	XX	XX	XX	XX	XX	XX	XX
JP	**システムコンポーネントの更新** *変更管理とテストプロセス*	**UPD-03**	CCC-03	システムの可用性、機密性、およびシステムとサービスの完全性に重点を置いて確立された、ベースライン、テスト、およびリリース標準を含む、品質変更管理およびテストプロセス（ITILサービス管理など）を定義し、それに従います。	中	中	中	不適切な変更管理プロセスでは、新しいリスクが発生したり、既存のセキュリティ管理の有効性が低下する可能性があります。	セキュリティを統合する変更管理プロセスを開発するためのリソースには、次のものがあります：http://www.iso27001security.com/ISO27k_Model_policy_on_change_management_and_control.docxは、ISO 27001に準拠した一般的な変更管理および制御ポリシーを提供します。https://www.us-cert.gov/sites/default/files/c3vp/crr_resources_guides/CRR_Resource_Guide-CCM.pdfは、US-CERTによる変更管理プロセスに関するガイドです。https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1493830822.pdfは、SANSによって発行された変更管理のためのテンプレートガイドです。	予防型	自動型	イベント毎	XX	XX	XX	XX	XX	XX	XX
JP	**システムコンポーネントの更新** *サードパーティのコード分析*	**UPD-04**		すべてのサードパーティのコードに対して静的および動的なセキュリティ分析スキャンを実行します。ソフトウェア構成分析ツールを使用して、既知の脆弱性を持つコンポーネントを特定します（たとえば、OWASPの依存関係チェック）。	中	中	中	サードパーティのコードを使用すると、余計な脆弱性が生じる可能性があります。セキュリティ分析のスキャンとツールを使用すると、一般的な脆弱性が存在し、対処する必要があるかどうかを識別できます。	OWASP組込みアプリケーションセキュリティプロジェクトは以下にSBOMの例を挙げています - https://scriptingxss.gitbooks.io/embedded-appsec-best-practices//executive_summary/10_third_party_code_and_components.html	予防型	自動型	年に1回	XX	XX	XX	XX	XX	XX	XX
JP	**システムコンポーネントの更新** *ファームウェアイメージの保存*	**UPD-05**		すべてのIoTデバイスの完全性を担保されたファームウェアイメージを保存します。侵害または破損が疑われ、もしくは確認されたIoTデバイスを復元するためのプロセスを確立します。さまざまな種類のデバイスで、少なくとも年1回更新プロセスをテストします	低	低	低	保存されたファームウェアイメージは、必要な場合に信頼性の高いバックアップポイントを提供します。これらのバックアップをテストすることで、障害発生時に、バックアップイメージがない、バックアップ時に誤って保存された、または機能しなかったことに気付くのではなく、デバイスを確実に復元できるようにな		予防型	自動型	イベント毎	XX	XX	XX			XX	
JP	**システムコンポーネントの更新** *ソフトウェア署名の検証*	**UPD-06**		アップデートの前にファームウェア上のソフトウェア署名を検証するようにすべてのIoTデバイスを設定します。デバイス監査ログを監視して署名検証の失敗を特定します。すべての失敗を調査して根本的な原因を特定します	低	低	低	署名検証の失敗は、IoTデバイスの適切な機能に影響を与える可能性があり、攻撃者によるデバイスの偽装を示す可能性もあります。		予防型	半自動型	年に1回			XX			XX	
JP	**関与者のトレーニング** *管理者*	**TRN-01**	HRS-05 HRS-09 MOS-01 MOS-05	IoT管理者向けのセキュリティトレーニングプログラムを確立します。許容される使用ポリシー、組織内で使用されるIoT資産、IoTデバイスへの信頼のブートストラップ手順、IoTシステムのセキュリティ体制の監視、IoTデバイスを安全に管理するための承認済みプロセス、およびインシデント対応手順に関する情報を含めます。 IoTシステム管理者が毎年このトレーニングを受けるように要求してください	中	中	中	IoT管理者をトレーニングすることは、アクセスレベル、デバイスの使用を設定する能力、およびデバイスとネットワークの問題にさらされていることから重要です。		予防型	半自動型	イベント毎	XX	XX	XX	XX	XX	XX	XX

JP	**関与者のトレーニング** *利用者*	**TRN-02**	HRS-10	利用者セキュリティトレーニングプログラムを確立します。研修プログラムは、確立された方針と手順への意識と遵守を維持する上で、全職員にその役割と責任を認識させることに焦点を当てるべきです。これには、適用される法的、法定、および規制順守義務が含まれます。企業ネットワークでの従業員所有のIoTデバイスの使用に関連するポリシーや手順（スマートテレビ、ウェアラブルなど）も含め、トレーニングは安全で安全な職場環境の維持にも焦点を当てる必要があります。トレーニングには、IoTデバイスに関連するリスクとプライバシーへの影響に関する情報を含める必要があります。該当する場合は、企業のIoTデバイスとのインターフェイスの手順に関する情報を提供します。 IoTシステムのすべての利用者が毎年このトレーニングを受けるように要求してください	中	中	中	利用者セキュリティトレーニングは、年ごとに異なり、利用者の概念をテストすることが最も効果的です。セキュリティトレーニングも、組織の変化と新たなリスクを反映するように更新する必要があります。		予防型	自動型	年に1回	XX	XX	XX	XX	XX	XX	XX
JP					**IoT SYSTEM IMPACT LEVEL BY THE IoTシステムの影響度別集計**																
JP					**HIGH IMPACT LEVELS**																
JP					**影響度（高）**																
JP					**Confidentiality**	**Integrity**	**Availability**														
JP					**機密性**	**完全性**	**可用性**														
JP					17	18	17														
JP					**MEDIUM IMPACT LEVELS**																
JP					**影響度（中）**																
JP					**Confidentiality**	**Integrity**	**Availability**														
JP					**機密性**	**完全性**	**可用性**														
JP					106	105	106														
JP					**LOW IMPACT LEVELS**																
JP					**影響度（低）**																
JP					**Confidentiality**	**Integrity**	**Availability**														
JP					**機密性**	**完全性**	**可用性**														
JP					37	36	36														

Acknowledgments

Initiative Leads:

Brian Russell
Michael Roza

Key Contributors:

Hillary Baron
Luciano Ferrari
Aaron Guzman
Ankur Gargi
Sabri Khemissa
Douglas Mcdorman
Todd Nelson
Eric Palmer
J.R. Santos
Theodoros Stergiou
Srinivas Tatipamula
John Yeoh