★3セキュリティ要件・適合基準案（通信機器）

適合基準番号	セキュリティ要件（Security Requirement）		★3適合基準	対象外（NA）となるための条件、基準の補足説明	★3評価手法	【参考】海外既存制度・文書で求められるセキュリティ要件との関係性	【参考】国内既存制度・文書で求められるセキュリティ要件との関係性
	カテゴリ	要件					
S3.1-02	1.脆弱な認証・認可メカニズム（例： 汎用のデフォルトパスワード、脆弱なパスワード）を使用しない	1-2. プリインストールされた固有のパスワードを使用する場合、自動化された攻撃への耐性をもつために、パスワードは十分なランダム性を保有しなければならない。	IoT製品に対するネットワークを介したユーザ認証の仕組みにて、パスワードを使用するIoT製品において、IoT製品導入時にデフォルトパスワードが使用される場合に、以下の①・②のいずれかの基準を満たすこと。 ①デフォルトパスワードは、IoT機器毎に異なる一意の値で、容易に推測可能でない8文字以上のパスワードであること。 ②デフォルトパスワードは、初回起動時にユーザによるパスワード変更を必須とする機能を実装し、当該機能において設定可能なパスワードとして、容易に推測可能でない8文字以上のパスワードの設定を強制させること。	【対象外（NA）となるための条件】 パスワード利用した認証の仕組みがない（「NAであることの理由」に、脅威に対抗するためにパスワード利用した認証が必要ない根拠を記載すること） 【用語定義：ユーザ】ユーザの対象範囲には、IoT 機器の利用者、管理者、ベンダーの カスタマーエンジニア、所有者等、当該 IoT 機器内の守るべき情報資産へのアクセスができ る当該 IoT 機器を使用する自然人及び組織すべてを含んでいなければならない	・ドキュメント評価：対象とする ・実機テスト：対象とする	【ETSI EN 303 645】5.1-2 M F 【英国PSTI Act】SCHEDULE 1: 1-(2)、1-(3) 【米国NISTIR 8425】インターフェイスへの論理アクセス 1-b 【シンガポールCLS】[＊]5.1-1 、5.1-2 【IEC 62443-4-2】CR1.5 認証コードの管理、CR1.7 パスワードベース認証の強度	【総務省 端末設備等規則】第三十四条の十(二) 【CCDSサーティフィケーションプログラム】1-1アクセス制御及び認証【必須】②、、1-1-2認証情報の変更【必須】② 【BMSec】デフォルトパスワードの変更 IA-2 b)-2)、e)-2) 2.2) 【特定用途機器PP】FMT_IPWD_EXT（拡張：初期パスワードの設定）
S3.1-01	1.脆弱な認証・認可メカニズム（例： 汎用のデフォルトパスワード、脆弱なパスワード）を使用しない	1-3. 製品に対してユーザを認証するために使用される認証メカニズムは、製品用途の特性等に適した想定するリスクを低減できる技術を使用していなければならない。	IoT 製品に対するIP通信を介した守るべき情報資産への他の IoT 機器又はユーザからのアクセスに対して、適切な認証に基づくアクセス制御が行われていること。 また重要な設定変更等の操作については上記認証手段を再度実施すること。	【用語定義：守るべき情報資産】 以下の情報： ・通信機能に関する設定情報 ・セキュリティ機能に関する設定情報 ・ログ（テレメトリデータ・監査ログ） ・プログラムコード（ソフトウェア） ・IoT機器の意図する使用において、IoT機器が収集し、保存又は通信する、個人情報等の一般的に機密性が高い情報 【用語定義：ユーザ】 ユーザの対象範囲には、IoT 機器の利用者、管理者、ベンダーの カスタマーエンジニア、所有者等、当該 IoT 機器内の守るべき情報資産へのアクセスができ る当該 IoT 機器を使用する自然人及び組織すべてを含んでいなければならない	・ドキュメント評価：対象とする ・実機テスト：対象とする	【ETSI EN 303 645】5.1-3 M F、5.11-1 M、5.5-5 M F 【米国NISTIR 8425】インターフェイスの論理アクセス2-b 【EU-CRA】ANNEX I 1.(2)(d)、ANNEX I 1.(2)(f) 【シンガポールCLS】[＊]5.1-3、[＊＊]5.5-5 【IEC 62443-4-2】CR1.5 認証コードの管理、CR1.6、NDR1.6 無線アクセスの管理、CR2.12 否認防止、CR3.9 監査情報の保護、CR6.1 監査ログのアクセス性	【総務省 端末設備等規則】第三十四条の十(一) 【CCDSサーティフィケーションプログラム】1-1アクセス制御及び認証【必須】④、1-1-1TCP・UDPポートの無効化【推奨】②、1-2データ保護【必須】③、1-3 ソフトウェア更新【推奨】③ 【BMSec】管理者の認証 IA-1、機器のセキュリティ設定管理 MT-1 【RBSS】防犯カメラ認定基準　高度セキュリティ機能 4、デジタルレコーダ認定基準　高度セキュリティ機能 4 【特定用途機器PP】FAU_STG（保護された監査証跡格納）、FIA_UAU（認証のタイミング）、FMT_SMR（セキュリティの役割）、FIA_UID（アクション前の利用者識別）
S3.1-03	1.脆弱な認証・認可メカニズム（例： 汎用のデフォルトパスワード、脆弱なパスワード）を使用しない	1-4. 製品に対するユーザ認証において、製品は使用される認証値を変更するためのシンプルなメカニズムを、ユーザ又は管理者に提供しなければならない。	IoT 製品に対するネットワークを介した他のIoT機器又はユーザからのアクセスの認証において使用される認証値の変更について、認証の種類（パスワード、トークン、指紋等）に依らず、その認証値の変更を可能とすること。	【対象外（NA）となるための条件】 － 【用語定義：認証値】 IoT製品に対する認証の仕組みで使用される属性の個別値。（例： パスワードに基づく認証の仕組みである場合、認証値は文字列となる。生体指紋認証である場合、認証値は例えば左手の人差し指の指紋データとなる。） 【用語定義：ユーザ】 ユーザの対象範囲には、IoT 機器の利用者、管理者、ベンダーの カスタマーエンジニア、所有者等、当該 IoT 機器内の守るべき情報資産へのアクセスができ る当該 IoT 機器を使用する自然人及び組織すべてを含んでいなければならない	・ドキュメント評価：対象とする ・実機テスト：対象とする	【ETSI EN 303 645】5.1-4 M F 【シンガポールCLS】[＊]5.1-4 【IEC 62443-4-2】CR1.5 認証コードの管理	【CCDSサーティフィケーションプログラム】1-1-2認証情報の変更【必須】① 【BMSec】デフォルトパスワードの変更 IA-2 【RBSS】デジタルレコーダ認定基準　高度セキュリティ機能 2 【特定用途機器PP】FMT_IPWD_EXT（拡張：初期パスワードの設定）
S3.1-04	1.脆弱な認証・認可メカニズム（例： 汎用のデフォルトパスワード、脆弱なパスワード）を使用しない	1-5. 機器が、制約のある機器ではない場合、ネットワークを介して行われる認証に対する総当たり攻撃等のブルートフォース攻撃が実行できないようにするメカニズムを保有しなければならない。	IoT機器に対するネットワークを介したユーザ認証の仕組みについて、総当たり攻撃を困難とすること。	【用語定義：ユーザ】 ユーザの対象範囲には、IoT 機器の利用者、管理者、ベンダーの カスタマーエンジニア、所有者等、当該 IoT 機器内の守るべき情報資産へのアクセスができ る当該 IoT 機器を使用する自然人及び組織すべてを含んでいなければならない	・ドキュメント評価：対象とする ・実機テスト：対象とする	【ETSI EN 303 645】5.1-5 M C F 【EU-CRA】ANNEX I 1.(2)(d) 【シンガポールCLS】[＊]5.1-5 【IEC 62443-4-2】CR1.11 ログイン試行の失敗	【総務省 端末設備等規則】第三十四条の十(一) 【CCDSサーティフィケーションプログラム】1-1アクセス制御及び認証【必須】③ 【BMSec】認証失敗時のアクション IA-3 【特定用途機器PP】FIA_AFL（認証失敗時の取扱い）

★3セキュリティ要件・適合基準案（通信機器）

適合基準番号	セキュリティ要件（Security Requirement）		★3適合基準	対象外（NA）となるための条件、基準の補足説明	★3評価手法	【参考】海外既存制度・文書で求められるセキュリティ要件との関係性	【参考】国内既存制度・文書で求められるセキュリティ要件との関係性
	カテゴリ	要件					
S3.1-05	1.脆弱な認証・認可メカニズム（例： 汎用のデフォルトパスワード、脆弱なパスワード）を使用しない	1-6. 製品において使用する電子証明書はセキュアに保たれなければならない。	IoT製品において認証のために使用する電子証明書は、十分なセキュリティ強度を持つこと。 IoT製品で使用する電子証明書は、更新可能とすること	【対象外（NA）となるための条件】 IoT製品において、認証のために電子証明書を使用していない	・ドキュメント評価： 対象とする ・実機テスト： 対象とする		
S3.1-06	1.脆弱な認証・認可メカニズム（例： 汎用のデフォルトパスワード、脆弱なパスワード）を使用しない	1-7. 製品においてSSHを公開鍵認証にて利用する場合は、セキュアな暗号アルゴリズムによって公開鍵認証をセキュアに保たならければならない。	IoT製品においてSSHを公開鍵認証にて利用する場合は、公開鍵認証機能は、セキュアな暗号アルゴリズムを使用していること。	【対象外（NA）となるための条件】 IoT製品において、SSHを公開鍵認証にて利用していない	・ドキュメント評価： 対象とする ・実機テスト： なし		
S3.1-07	1.脆弱な認証・認可メカニズム（例： 汎用のデフォルトパスワード、脆弱なパスワード）を使用しない	1-8. 製品においてVPN接続を行う場合は、厳格なユーザ認証及び機器の接続制限を行わなければならない。	IoT製品においてVPNゲートウェイ機能をもつ場合は、以下の①～②の基準をすべて満たすこと。 ①ユーザ認証において多要素認証を行う機能を有すること。 ②接続元の機器等を制限する機能を有すること。	【対象外（NA）となるための条件】 IoT製品において、VPNゲートウェイ機能を持たない。 【用語定義：VPNゲートウェイ機能】 内部ネットワークとインターネット等の外部ネットワークの境界に置かれ、ユーザとの間に暗号化された通信経路を作成する機能	・ドキュメント評価： 対象とする ・実機テスト： なし		政府機関等の対策基準策定のためのガイドライン（令和７年度版）6.4.1(2)-5
S3.1-08	1.脆弱な認証・認可メカニズム（例： 汎用のデフォルトパスワード、脆弱なパスワード）を使用しない	1-9. 製品は、無許可の機器の接続を拒否しなければならない。	IoT機器は、接続する機器を識別し、無許可の機器の接続を拒否する機能を有すること。	【対象外（NA）となるための条件】 IoT機器において、L2/L3スイッチングまたはルーティング機能を持たない。	・ドキュメント評価： 対象とする ・実機テスト： なし		政府機関等の対策基準策定のためのガイドライン（令和７年度版）6.4.1(1)-3
S3.1-09	2. 脆弱性の報告を管理するための手段を導入する	2-1. 製造業者は、脆弱性開示ポリシーを公開しなければならない。このポリシーには、少なくとも以下が含まれていなければならない ・問題を報告するための連絡先情報 ・以下のタイムラインに関する情報 1) 最初の受領確認 2) 報告された問題が解決されるまでの状況の更新	製造業者は、以下の①～④のすべての情報を含む脆弱性開示ポリシーを公開（例：製造業者のウェブサイトへの掲載）すること。 ①IoT 製品のセキュリティの問題に関して、製造業者へ報告するための連絡先（例：製造業者等のウェブサイトのURL、電話番号、メールアドレス） ②製造業者がIoT製品のセキュリティに関する報告を受領した後に行う手続き（セキュリティに関する報告をどのように受付け、その後にどのような手続き・方法で報告者と連絡を取り合うのか、報告に対してどのような対応をするのか、善意の報告に対する法的免責付与の宣言等）及びその概要 ③脆弱性が解決されるまでのIoT製品や脆弱性の状況更新に関する手続き（脆弱性が解決されるまでどのように調査や対策が行われ、どのようにその状況が管理・公表されるのか、報告者に対してどのような対応をするのか等）及びその概要 ④脆弱性の対応について、適切な報告先機関へタイムリーに報告することの宣言	—	・ドキュメント評価： 対象とする ・実機テスト： なし	【ETSI EN 303 645】5.2-1 M、5.2-2 R 【英国PSTI Act】SCHEDULE 1: 2-(2), 2-(3) 【米国NISTIR 8425】情報及び問合せの受付1, 1-a, 1-b、教育及び意識向上、ドキュメンテーション 1-g 【EU-CRA】Article 13 7、Article 13 8、Article 13 16、Article 13 17、Article 13 21、Article 14 1、Article 14 2(a)、Article 14 2(b)、Article 14 2(c)、Article 14 3、Article 14 4、Article 14 6、Article 14 7、Article 14 8、ANNEX Ⅰ 1.(2)(a)、ANNEX Ⅰ 2.(5)、ANNEX Ⅰ 2.(6)、ANNEX Ⅰ 2.(7)、ANNEX Ⅱ 1、ANNEX Ⅶ 2(a)、ANNEX Ⅱ 2 【シンガポールCLS】[＊]5.2-1 【IEC 62443-4-1】DM-1 セキュリティ関連の問題の通知を受け取る、DM-2 セキュリティ関連の問題のレビュー、DM-3 セキュリティ関連の問題を評価する、DM-4 セキュリティ関連問題への対応、SG-3 セキュリティ強化のガイドライン	【CCDSサーティフィケーションプログラム】2-1連絡窓口・セキュリティサポート体制【必須】①② 【BMSec】問い合わせ窓口 FR-1、ファームウェアの提供 FR-2

★3セキュリティ要件・適合基準案（通信機器）

適合基準番号	セキュリティ要件（Security Requirement）		★3適合基準	対象外（NA）となるための条件、基準の補足説明	★3評価手法	【参考】海外既存制度・文書で求められるセキュリティ要件との関係性	【参考】国内既存制度・文書で求められるセキュリティ要件との関係性
	カテゴリ	要件					
S3.1-10	3. ソフトウェアを最新の状態に保つ	3-1. 製品に含まれる特定のソフトウェアコンポーネントについて、アップデート可能にしなければならない。	IoT製品に含まれるソフトウェアコンポーネントのアップデート機能について、以下の①～④のすべての基準を満たすこと。 ①IoT製品のファームウェア（ソフトウェア）パッケージについて、アップデートが可能であること。 ②ファームウェア（ソフトウェア）パッケージのバージョンの確認が行えるなど、最新のファームウェア（ソフトウェア）がインストールされていることを確認する手段を有すること。 ③アップデートされたファームウェア（ソフトウェア）パッケージのバージョンが電源OFF後も維持されること。 ④自動アップデート機能を有すること。	—	・ドキュメント評価： 対象とする ・実機テスト： 対象とする	【ETSI EN 303 645】5.3-1 R F、5.3-4A R F、5.3-4B R F 【米国NISTIR 8425】ソフトウェアの更新 1、ソフトウェアの更新 2 【EU-CRA】Article 13 9、ANNEX Ⅰ1.(2)、ANNEX Ⅰ1.(2)(c)、ANNEX Ⅰ2.(7) 【シンガポールCLS】[＊＊＊]CK-LP-03 【IEC 62443-4-1】SM-6 ファイルの完全性、SUM-1 セキュリティ・アップデート資格 【IEC 62443-4-2】CR4.3 暗号化の使用、CR3.10、EDR3.10、HDR3.10、NDR 3.10 アップデートのサポート	【CCDSサーティフィケーションプログラム】1-3ソフトウェア更新【必須】①【推奨】① 【BMSec】ファームウェアアップデート機能PT-1 b)-4)、e)-1) 【特定用途機器PP】FMT_SMF（管理機能の特定）
S3.1-11	3. ソフトウェアを最新の状態に保つ	3-3. 製品においてアップデートメカニズムが実装されている場合、そのアップデートは、ユーザが簡単に適用できるものでなければならない。	ユーザがアップデートを適用する際、容易かつ分かりやすい手順でソフトウェアのアップデートを実行可能とすること。	【用語定義：ユーザ】 ユーザの対象範囲には、IoT 機器の利用者、管理者、ベンダーの カスタマーエンジニア、所有者等、当該 IoT 機器内の守るべき情報資産へのアクセスができ る当該 IoT 機器を使用する自然人及び組織すべてを含んでいなければならない	・ドキュメント評価： 対象とする ・実機テスト： なし	【ETSI EN 303 645】5.3-3 M F 【EU-CRA】Article 13 11、ANNEX Ⅰ2.(8) 【シンガポールCLS】[＊]5.3-3 【IEC 62443-4-1】SUM-4 セキュリティアップデートの配信	【総務省 端末設備等規則】第三十四条の十(三) 【CCDSサーティフィケーションプログラム】1-3ソフトウェア更新【必須】① 【BMSec】ファームウェアアップデート機能　PT-1 b)-4)、e)-1) 【特定用途機器PP】FMT_SMF（管理機能の特定）
S3.1-12	3. ソフトウェアを最新の状態に保つ	3-7. 製品においてアップデートメカニズムが実装されている場合、セキュアなアップデートメカニズムを容易にするために、ベストプラクティスの暗号技術を使用しなければならない。	ソフトウェアをアップデートする際に以下①から③全てを満たす機能があること。 ①ソフトウェアの完全性及び真正性をアップデート前にIoT製品が確認できる仕組みを有すること。 ②真正性を満たさない場合は更新を中断すること。 ③アンチロールバックの機能を有すること。	—	・ドキュメント評価： 対象とする ・実機テスト： 対象とする	【ETSI EN 303 645】5.3-2 M C、5.3-7 M F、5.3-9 R F 【米国NISTIR 8425】ソフトウェアの更新 1 【EU-CRA】ANNEX Ⅰ1.(2)(g)、ANNEX Ⅰ2.(7) 【シンガポールCLS】[＊]5.3-2、5.3-7、5.3-10 【IEC 62443-4-1】SM-6 ファイルの完全性 【IEC 62443-4-2】CR3.1 通信の完全性、CR3.2、SAR3.2、EDR3.2、HDR3.2、NDR3.2 悪意あるコードからの保護、CR4.3 暗号化の使用	【総務省 端末設備等規則】第三十四条の十(三) 【CCDSサーティフィケーションプログラム】1-3ソフトウェア更新【必須】①【推奨】①、② 【BMSec】ファームウェアアップデート機能PT-1 b)-3) 【特定用途機器PP】FMT_SMF（管理機能の特定）
S3.1-13	3. ソフトウェアを最新の状態に保つ	3-8. 製品においてアップデートメカニズムが実装されている場合、セキュリティアップデートは、適時でなければならない。	製造業者は、セキュリティ課題に対する迅速なアップデートを目的として、セキュリティアップデートの優先度を決定するための方針や指針を文書化すること。	—	・ドキュメント評価： 対象とする ・実機テスト： なし	【ETSI EN 303 645】5.3-8 M C 【EU-CRA】Article 14 5(a)、Article 14 5(b)、ANNEX Ⅰ2.(2)、ANNEX Ⅰ2.(7)、ANNEX Ⅰ2.(8) 【シンガポールCLS】[＊]5.3-8 【IEC 62443-4-1】SUM-5 セキュリティパッチのタイムリーな提供	【CCDSサーティフィケーションプログラム】2-1連絡窓口・セキュリティサポート体制【必須】② 【BMSec】ファームウェアアップデート機能　PT-1 b)-4)、e)-1) 【特定用途機器PP】FMT_SMF（管理機能の特定）

★3セキュリティ要件・適合基準案（通信機器）

適合基準番号	セキュリティ要件（Security Requirement）		★3適合基準	対象外（NA）となるための条件、基準の補足説明	★3評価手法	【参考】海外既存制度・文書で求められるセキュリティ要件との関係性	【参考】国内既存制度・文書で求められるセキュリティ要件との関係性
	カテゴリ	要件					
S3.1-14	3. ソフトウェアを最新の状態に保つ	3-14. 製品のモデル名称は、製品上のラベル又は物理的インタフェースを介して、ユーザに対して明確に認識可能でなければならない。	IoT製品の型番は、以下のいずれかの方法でユーザへ提供すること。 ①IoT製品本体に、IoT製品の型番及びシリアル番号を直接記載すること。 ②IoT製品のGUI、ウェブUI等や、IoT製品に付帯するソフトウェア、アプリケーション（スマホアプリなど）のGUI、ウェブUI等から、ユーザが型番及びシリアル番号を認識できるようにすること。	【用語定義：ユーザ】 ユーザの対象範囲には、IoT 機器の利用者、管理者、ベンダーの カスタマーエンジニア、所有者等、当該 IoT 機器内の守るべき情報資産へのアクセスができ る当該 IoT 機器を使用する自然人及び組織すべてを含んでいなければならない	・ドキュメント評価： 対象とする ・実機テスト： 対象とする	【ETSI EN 303 645】5.3-16 M 【米国NISTIR 8425】機器の識別 1、情報発信 2 【EU-CRA】ANNEX II 3、ANNEX VII 1(c)、ANNEX VII 1(d) 【シンガポールCLS】[＊]5.3-16 【IEC 62443-4-2】CR1.2 ソフトウェアプロセス及びデバイスの識別及び認証	【CCDSサーティフィケーションプログラム】1-1アクセス制御及び認証【必須】①
S3.1-15	3. ソフトウェアを最新の状態に保つ	3-15. ソフトウェア識別情報及びコンポーネント情報等を含んだ、機械可読な形式のソフトウェア部品表（SBOM）を作成しなければならない。	IoT製品で使用されるサードパーティコンポーネントを含めた一意に識別可能なソフトウェア部品表（SBOM）を作成し、運用を行うこと。具体的には以下の①～③のすべての基準を満たすこと。 ①製品出荷後の運用フェーズにおける既知の脆弱性管理のため、製品の構成要素であるソフトウェア（サードパーティコンポーネントを含む）のSBOMを作成し、サポート期間内において更新を行うこと。 ②サポート期間内においては、SBOMの情報に基づいて定期的に脆弱性の確認を行い、対応優先度を判断した上で、更新あるいは運用対処等を行うプロセスを有すること。 ③サポート期間内においては、SBOMの情報に基づき、使用するコンポーネントのライセンス管理を行うプロセスを有すること。	—	・ドキュメント評価： 対象とする ・実機テスト： なし	【ETSI EN 303 645】5.2-3 R、5.3-15A R C、5.3-15B R C 【EU-CRA】ANNEX I 2.(1)、ANNEX VII 2.(b)、ANNEX VII 2.(c)、ANNEX VII 8 【シンガポールCLS】[＊＊＊]CK-LP-03、[＊＊＊]CK-LP-06、 【IEC 62443-4-1】DM-2 セキュリティ関連の問題のレビュー	【BMSec】構成管理 CM-1
S3.1-16	4. 機密セキュリティパラメータをセキュアに保存する	4-1. 製品のストレージにある機密セキュリティパラメータは、製品によってセキュアに保存されなければならない。	IoT製品のストレージに保存される守るべき情報資産（SDカード等、ストレージメディアに保存される守るべき情報資産も含む。）は、セキュアに保存されること。	【用語定義：守るべき情報資産】 以下の情報： ・通信機能に関する設定情報 ・セキュリティ機能に関する設定情報 ・ログ（テレメトリデータ・監査ログ） ・プログラムコード（ソフトウェア） ・IoT機器の意図する使用において、IoT機器が収集し、保存又は通信する、個人情報等の一般的に機密性が高い情報	・ドキュメント評価： 対象とする ・実機テスト： なし	【ETSI EN 303 645】5.4-1 M F 【米国NISTIR 8425】データ保護 1、インターフェイスへの論理アクセス 2-a 【シンガポールCLS】[＊＊]5.4-1 【IEC 62443-4-2】CR1.5 認証コードの管理、CR1.9 公開鍵ベースの認証の強度、CR1.14 対照鍵ベースの認証の強度、CR3.8 セッションの完全性、CR3.9 監査情報の保護、CR3.12、EDR3.12、HDR3.12、NDR3.12 製品サプライヤの信頼の起点のプロビジョニング、CR3.13、EDR3.13、HDR3.13、NDR3.13 アセットオーナーの信頼の起点のプロビジョニング、CR4.1 情報の機密性	【CCDSサーティフィケーションプログラム】1-2データ保護【必須】①③ 【特定用途機器PP】FAU_STG（保護された監査証跡格納）、FMT_MTD（TSFデータの管理）
S3.1-17	4. 機密セキュリティパラメータをセキュアに保存する	4-2. ハードコードされた機器ごとに固有のIDがセキュリティ目的で製品で使用される場合、物理的、電気的、又はソフトウェアなどの手段による改ざんに耐えられるように実装しなければならない。	IoT製品で使用されるハードコードされた機密セキュリティパラメータ（機器固有の識別子やアイデンティティを証明するための認証コードなど）の改ざん防止のため、以下①・②すべての基準を満たすこと。 ①ハードコードされた機密セキュリティパラメータの全容を把握し、一覧化できていること。 ②すべての機密セキュリティパラメータは、物理的、電気的、又はソフトウェアなどの手段により改ざんに耐えられるように実装されていること。	【NAとなるための条件】 ・対象製品においてハードコードされた機密セキュリティパラメータが存在しない（「NAであることの理由」に、ハードコードされた機密セキュリティパラメータが存在しないことを明示すること） 【機密セキュリティパラメータ】 重要なセキュリティパラメータに以下の要素を加えたもの ・ソフトウェア検証に使用される公開鍵 ・証明書の公開要素 ・機器固有のID	・ドキュメント評価： 対象とする ・実機テスト： なし	【ETSI EN 303 645】5.4-2 M F 【シンガポールCLS】[＊＊]5.4-2 【IEC 62443-4-2】CR1.5 認証コードの管理、CR3.11、EDR3.11、HDR3.11、NDR3.11 物理的耐タンパー性及び検出	

★3セキュリティ要件・適合基準案（通信機器）

適合基準番号	セキュリティ要件（Security Requirement）		★3適合基準	対象外（NA）となるための条件、基準の補足説明	★3評価手法	【参考】海外既存制度・文書で求められるセキュリティ要件との関係性	【参考】国内既存制度・文書で求められるセキュリティ要件との関係性
	カテゴリ	要件					
S3.1-18	4. 機密セキュリティパラメータをセキュアに保存する	4-3. 製品のソフトウェアのソースコードにハードコードされた重要なセキュリティパラメータを使用してはならない。	ソースコードに記載された機密セキュリティパラメータに重要なセキュリティパラメータが含まれていないことを確認するため、以下①・②すべての基準を満たすこと。 ①ソースコードにハードコードされている機密セキュリティパラメータの全容を把握し、一覧化できていること。 ②機密セキュリティパラメータのうち、IoT製品の運用中に利用される重要なセキュリティパラメータが、①の一覧に含まれていないこと。	【NAとなるための条件】 ソースコードに機密セキュリティパラメータが存在しない（「NAであることの理由」に、ソースコードにハードコードされた機密セキュリティパラメータが存在しないことを明示すること） 【重要なセキュリティパラメータ】 セキュリティに関連する情報であって、その開示または変更が、暗号モジュールのセキュリティを危殆化し得るもの。 （例：共通鍵・秘密鍵・パスワードやPINなどの認証データなど）	・ドキュメント評価： 対象とする ・実機テスト： なし	【ETSI EN 303 645】5.4-3 M 【シンガポールCLS】[＊＊]5.4-3	
S3.1-19	4. 機密セキュリティパラメータをセキュアに保存する	4-4. ソフトウェアアップデートの完全性及び真正性チェック、及び製品のソフトウェアにおける付随サービスとの通信の保護に使用される重要なセキュリティパラメータは、機器ごとに固有でなければならず、製品のクラスに対する自動化された攻撃のリスクを低減するメカニズムで生成されるものとしなければならない。	IoT製品で使用される重要なセキュリティパラメータのうち、ソフトウェアアップデートの完全性及び真正性チェック、及び付随サービスとの通信の保護に使用される重要なセキュリティパラメータは、IoT機器毎に固有であること。	【重要なセキュリティパラメータ】 セキュリティに関連する情報であって、その開示または変更が、暗号モジュールのセキュリティを危殆化し得るもの。 （例：共通鍵・秘密鍵・パスワードやPINなどの認証データなど）	・ドキュメント評価： 対象とする ・実機テスト： なし	【ETSI EN 303 645】5.4-4 M F 【シンガポールCLS】[＊＊]5.4-4 【IEC 62443-4-1】SM-8 秘密鍵の管理 【IEC 62443-4-2】CR3.8 セッションの完全性	【CCDSサーティフィケーションプログラム】1-3ソフトウェア更新【必須】④
S3.1-20	5. セキュアに通信する	5-1. 製品は、ベストプラクティスの暗号技術を使用してセキュアに通信をしなくてはならない。	ネットワーク経由で伝送される守るべき情報資産について以下のすべての保護対策が行われていること。 ① IoT製品は守るべき情報資産の送信先の正当性を確認する。 ② IoT製品が保護されたネットワーク以外のネットワークを介して守るべき情報資産を通信する場合は、IoT製品が自ら情報の盗聴・改ざんに対する保護対策を行う。 ③ IoT製品が保護されたネットワークのみを介して守るべき情報資産を通信する場合は、IoT製品自ら情報の改ざんに対する保護対策を行う。	【用語定義：守るべき情報資産】 以下の情報： ・通信機能に関する設定情報 ・セキュリティ機能に関する設定情報 ・ログ（テレメトリデータ・監査ログ） ・プログラムコード（ソフトウェア） ・IoT機器の意図する使用において、IoT機器が収集し、保存又は通信する、個人情報等の一般的に機密性が高い情報 【用語定義：保護されたネットワーク】 以下のネットワーク： ・VPN環境 ・専用線を経由した接続環境 ・物理的／論理的に保護されたネットワーク環境	・ドキュメント評価： 対象とする ・実機テスト： 対象とする	【ETSI EN 303 645】5.5-1 M、5.5-2 R、5.5-6 R F、5.5-7 M F、5.8-2 M F 【米国NISTIR 8425】データ保護 1、データ保護 3 【EU-CRA】ANNEX I 1.(2)(e)、ANNEX I 1.(2)(m)、ANNEX I 2.(3) 【シンガポールCLS】[＊＊]5.5-1、5.5-7、5.8-2、CK-LP-02 【IEC 62443-4-1】SD-3 セキュリティ設計レビュー、SM-8 秘密鍵の管理 【IEC 62443-4-2】CR1.5 認証コードの管理、CR1.8 公開鍵基盤証明書、CR1.9 公開鍵ベースの認証の強度、CR1.14 対照鍵ベースの認証の強度、CR3.1 通信の完全性、CR3.12、EDR3.12、HDR3.12、NDR3.12 製品サプライヤの信頼の起点のプロビジョニング、CR3.13、EDR3.13、HDR3.13、NDR3.13 アセットオーナーの信頼の起点のプロビジョニング、CR4.3 暗号化の使用	【CCDSサーティフィケーションプログラム】1-2データ保護【必須】②、1-2データ保護【推奨】①、1-4-1Wi-Fiの認証方式【必須】①、1-4-2Bluetoothの対策【必須】① 【BMSec】インターネット通信データ保護TP-1 【RBSS】防犯カメラ認定基準　高度セキュリティ機能 2、デジタルレコーダ認定基準　高度セキュリティ機能 2
S3.1-21	5. セキュアに通信する	5-8. 製造業者は、製品に関連する重要なセキュリティパラメータについて、セキュアな管理プロセスに従わなければならない。	IoT製品で利用する重要なセキュリティパラメータの生成・配布・保管・更新等の各ライフサイクルにおいて、セキュアな管理プロセスを実施していること。	【重要なセキュリティパラメータ】 セキュリティに関連する情報であって、その開示または変更が、暗号モジュールのセキュリティを危殆化し得るもの。 （例：共通鍵・秘密鍵・パスワードやPINなどの認証データなど）	・ドキュメント評価： 対象とする ・実機テスト： なし	【ETSI EN 303 645】5.5-8 M C 【シンガポールCLS】[＊＊]5.5-8 【IEC 62443-4-2】CR1.3 アカウントの管理、CR1.4 識別子の管理	

★3セキュリティ要件・適合基準案（通信機器）

適合基準番号	セキュリティ要件（Security Requirement）		★3適合基準	対象外（NA）となるための条件、基準の補足説明	★3評価手法	【参考】海外既存制度・文書で求められるセキュリティ要件との関係性	【参考】国内既存制度・文書で求められるセキュリティ要件との関係性
	カテゴリ	要件					
S3.1-22	5. セキュアに通信する	5-11. 製品は、無線LAN機能をもつ場合に、無線通信区間において暗号化および機器認証を行わなければならない。	無線LAN機能をもつIoT製品は、無線通信区間において適切な方式による通信の暗号化、及びIEEE 802.1Xによる機器認証を行う機能を有すること。	【対象外（NA）となるための条件】 IoT製品において、無線LAN機能を持たない。	・ドキュメント評価： 対象とする ・実機テスト： なし		政府機関等の対策基準策定のためのガイドライン（令和７年度版）6.4.3(1)
S3.1-23	6. 露出した攻撃面を最小化する	6-1. すべての未使用の物理的インタフェース及び論理的インタフェースは無効化しなければならない。	IoT製品において、外部からサイバー攻撃を受けるリスクを低減するために、IoT製品の利用上不要かつ攻撃を受けるリスクがあるインタフェースを無効化するとともに、IoT製品に対する脆弱性検査を実施すること。具体的には、以下の①・②のすべての基準を満たすこと。 ①IoT製品において、高頻度で利用され、脆弱性などのリスクが想定される以下のインタフェースについて、IoT製品の利用上不要かつ攻撃を受けるリスクがあるインタフェースを無効化すること。 A) TCP/UDPポート B) Bluetooth C) USB ②IoT製品に対して脆弱性スキャンツールによる既知の脆弱性検査を実施し、攻撃に悪用される可能性がある脆弱性が検出されないこと。	—	・ドキュメント評価： 対象とする ・実機テスト： 対象とする	【ETSI EN 303 645】5.6-1 M F 【米国NISTIR 8425】インターフェイスへの論理アクセス 1-a 【EU-CRA】ANNEX Ⅰ 1.(2)(j) 【シンガポールCLS】[＊＊]5.6-1 【IEC 62443-4-2】CR7.7 最小機能	【CCDSサーティフィケーションプログラム】1-1-1TCP・UDPポートの無効化【必須】①、1-4-2Bluetoothの対策【必須】② 【BMSec】PSTNファクスとネットワーク間の分離 NI-1、脆弱性スキャナーによる検証　VA-1、未使用TCP/UDPポートのクローズ　VA-2、デバッグポートのクローズ　VA-3
S3.1-24	6. 露出した攻撃面を最小化する	6-2. 初期化状態において、製品のネットワークインタフェースは、認証されていないセキュリティ関連情報の開示を最小化しなければならない。	初期化状態において、IoT製品で有効化されたネットワークインタフェースから認証なしで閲覧可能な以下を含むセキュリティ関連情報を最小化していること。 A) 機器の設定情報 B) カーネルのバージョン C) ソフトウェアのバージョン	—	・ドキュメント評価： 対象とする ・実機テスト： 対象とする	【ETSI EN 303 645】5.6-2 M 【米国NISTIR 8425】インターフェイスへの論理アクセス 2-a 【シンガポールCLS】[＊＊]5.6-2 【IEC 62443-4-2】CR1.10 認証コードのフィードバック	【CCDSサーティフィケーションプログラム】1-1-1TCP・UDPポートの無効化【必須】②、1-4-2Bluetoothの対策【必須】②
S3.1-25	6. 露出した攻撃面を最小化する	6-3. 機器のハードウェアは、物理インタフェースを不必要に攻撃にさらしてはならない。	IoT機器は、物理的な攻撃に対して、以下の①・②のすべての保護対策が行われていること。 ①IoT機器の不必要な物理的インタフェースは、露出から保護する仕組みを有すること。 ②IoT機器のデバッグインタフェースを物理的または論理的に無効化していること。	—	・ドキュメント評価： 対象とする ・実機テスト： 対象とする	【ETSI EN 303 645】5.6-3 R、5.6-4A M F、5.6-4B R F 【米国NISTIR 8425】インターフェイスへの論理アクセス 1-a 【EU-CRA】ANNEX Ⅰ 1.(2)(j) 【シンガポールCLS】[＊＊]5.6-4 【IEC 62443-4-2】CR2.13、EDR2.13、HDR2.13、NDR2.13 物理的な診断及び試験インタフェースの使用、CR7.7 最小機能、CR5.3、NDR5.3 汎用個人間の通信の制限	【CCDSサーティフィケーションプログラム】1-4-3USBのアクセス制御【必須】①【推奨】①② 【BMSec】未使用TCP/UDPポートのクローズ VA-2、デバックポートのクローズ VA-3 【RBSS】防犯カメラ認定基準　高度セキュリティ機能 4、デジタルレコーダ認定基準　高度セキュリティ機能 4

★3セキュリティ要件・適合基準案（通信機器）

適合基準番号	セキュリティ要件（Security Requirement）		★3適合基準	対象外（NA）となるための条件、基準の補足説明	★3評価手法	【参考】海外既存制度・文書で求められるセキュリティ要件との関係性	【参考】国内既存制度・文書で求められるセキュリティ要件との関係性
	カテゴリ	要件					
S3.1-26	6. 露出した攻撃面を最小化する	6-5. 製造業者は、意図された製品の用途又は操作に使用される、又は必要とされるソフトウェアサービスのみを有効にしなければならない。	製造業者は、IoT製品の設計および実装において、意図された機器の用途又は操作に使用される、又は必要とされるサービスのみを有効にすること。	—	・ドキュメント評価： 対象とする ・実機テスト： 対象とする	【ETSI EN 303 645】5.6-5 R 【EU-CRA】ANNEX I 1.(2)(i) 【シンガポールCLS】[＊＊＊]CK-LP-05 【IEC 62443-4-2】CR7.7 最小機能	
S3.1-27	6. 露出した攻撃面を最小化する	6-6. コードは、サービス／製品の操作に必要な機能に最小化しなければならない。	製造業者は、IoT製品に展開されるソフトウェアの実装およびテストにおいて、コード最小化のための手法を採用すること。	—	・ドキュメント評価： 対象とする ・実機テスト： なし	【ETSI EN 303 645】5.6-6 R 【シンガポールCLS】[＊＊＊]CK-LP-02、[＊＊＊]CK-LP-05 【IEC 62443-4-1】SI-1 セキュリティ実装のレビュー、SI-2 安全なコーディング標準	
S3.1-28	6. 露出した攻撃面を最小化する	6-7. ソフトウェアは、セキュリティと機能の両方を考慮し、必要最小限の権限で実行しなければならない。	製造業者は、IoT製品に展開されるソフトウェアについて、最小権限の原則に基づいた設計および実装を行っていること。具体的には、以下の基準を満たすこと。 ①デフォルト権限の最小化 ユーザがデバイスを初めて使用する際に、不必要に広範な権限が付与されないようデフォルトの権限設定を必要最小限に留めること。	【用語定義：ユーザ】 ユーザの対象範囲には、IoT 機器の利用者、管理者、ベンダーの カスタマーエンジニア、所有者等、当該 IoT 機器内の守るべき情報資産へのアクセスができ る当該 IoT 機器を使用する自然人及び組織すべてを含んでいなければならない	・ドキュメント評価： 対象とする ・実機テスト： なし	【ETSI EN 303 645】5.6-7 R 【IEC 62443-4-2】CR2.4、SAR2.4、EDR2.4、HDR2.4、NDR2.4 モバイルコード、CR7.7 最小機能	【RBSS】デジタルレコーダ認定基準 セキュリティ機能 3, 4
S3.1-29	6. 露出した攻撃面を最小化する	6-9. 製造業者は、製品に展開されるソフトウェアについて、セキュアな開発プロセスに従わなくてはならない。	製品の実装・テストフェーズにおいて、セキュアコーディングのプラクティスを実践し、作成したソースコードに対してレビューを実施すること。具体的には、最低限以下の実施を含む。 ①セキュリティに配慮したコーディング規約や実装原則を規程する ②コーディング規約を技術者に周知し教育を行う ③作成されたコードのレビュー・セキュリティテストを行う ④コーディング規約や実装原則を更新する	—	・ドキュメント評価： 対象とする ・実機テスト： なし	【ETSI EN 303 645】5.6-9 R 【EU-CRA】Article 13 14 【IEC 62443-4-1】SM-7 開発環境のセキュリティ	【CCDSサーティフィケーションプログラム】1-4-2Bluetoothの対策【必須】③ 【BMSec】構成管理 CM-1
S3.1-30	6. 露出した攻撃面を最小化する	6-10. ペネトレーションテストやコードレビューなどを通じて安全性が確保されたサードパーティ製コンポーネントのみを組み込まなくてはならない。	IoT製品にサードパーティコンポーネントを組み込む際に、既知の脆弱性が含まれないよう、以下の基準①・②の全てを満たすプロセスを採用していること。 ①明示的に利用しているサードパーティコンポーネントに関して脆弱性を管理すること。 ②脆弱性が検知された場合、適切な対応を行うこと。	【NAとなるための条件】 対象のIoT製品においてサードパーティコンポーネントを使用していない（「NAであることの理由」に、サードパーティコンポーネントを使用していないことを明示すること）	・ドキュメント評価： 対象とする ・実機テスト： なし	【EU-CRA】Artice 13 2、Article 13 5、ANNEX I 1.(1) 【シンガポールCLS】[＊＊＊]CK-LP-03 【IEC 62443-4-1】SM-9 外部提供コンポーネントに対するセキュリティ要件、SM-10 第三者サプライヤからのカスタム部品	

★3セキュリティ要件・適合基準案（通信機器）

適合基準番号	セキュリティ要件（Security Requirement）		★3適合基準	対象外（NA）となるための条件、基準の補足説明	★3評価手法	【参考】海外既存制度・文書で求められるセキュリティ要件との関係性	【参考】国内既存制度・文書で求められるセキュリティ要件との関係性
	カテゴリ	要件					
S3.1-31	7. ソフトウェアの完全性を確実にする	7-1. 製品は、セキュアブートメカニズムを使用してそのソフトウェアを検証しなければならない。	システムの起動プロセス中にロードされるソフトウェアの完全性の検証のため、IoT製品に対して、セキュアブートのメカニズムを実装すること。 セキュアブートメカニズムの例としては以下が挙げられる。これらのいずれかに類する実装を行うこと。 A) デジタル署名の検証 B) デジタル署名の検証と同等のセキュリティ対策	—	・ドキュメント評価： 対象とする ・実機テスト： なし	【ETSI EN 303 645】5.7-1 R 【EU-CRA】ANNEX I 1.(2)(g) 【IEC 62443-4-1】SM-6 ファイルの完全性 【IEC 62443-4-2】CR1.2 ソフトウェアプロセス及びデバイスの識別及び認証、CR3.4 ソフトウェア及び情報の完全性、CR3.14、EDR3.14、HDR3.14、NDR3.14 ブートプロセスの完全性	【CCDSサーティフィケーションプログラム】1-3ソフトウェア更新【推奨】①
S3.1-32	8. 個人データがセキュアであることを確実にする	8-3. 製品のすべての外部感知機能は、ユーザにとって明確で透明性のあるアクセス可能な方法で文書化されなければならない。	製造業者は、IoT機器がセンシングを行う場合に、以下の基準を満たす対応を行うこと。 ①センシングする情報について、収集の目的および機能の概要についてユーザマニュアル等に容易に理解できる内容を記載する。	【NAとなるための条件】 通信機器がセンシングを行わない場合	・ドキュメント評価： 対象とする ・実機テスト： なし	【ETSI EN 303 645】5.8-3 M F 【シンガポールCLS】[＊＊]5.8-3	
S3.1-33	9. 停止に対してレジリエントなシステムにする	9-1. データネットワークと電源の停止の可能性を考慮して、レジリエンスを製品とサービスに組み込まなければならない。	停電等による電力供給の停止やネットワークの停止により、IoT機器の電源がOFFになった後、電力供給が再開され、ネットワーク機能が復帰した際に、アクセス制御の際に使用する認証値（パスワード、秘密鍵など）の設定及びアップデートが完了したソフトウェアが工場出荷時の初期状態に戻ることなく、電源OFFになる直前の状態を維持できること。	—	・ドキュメント評価： 対象とする ・実機テスト： 対象とする	【ETSI EN 303 645】5.9-1 R 【EU-CRA】ANNEX I 1.(2)(h) 【IEC 62443-4-2】CR7.1 サービス不能攻撃からの保護、CR7.3 制御システムのバックアップ	【総務省 端末設備等規則】第三十四条の十(四) 【CCDSサーティフィケーションプログラム】1-1アクセス制御及び認証【必須】⑤、1-1-2 認証情報の変更【必須】④、1-3ソフトウェア更新【必須】②
S3.1-34	9. 停止に対してレジリエントなシステムにする	9-5. バックアップの実施により、インシデントの影響を軽減しなければならない。	IoT製品は、特定のタイミングの構成情報を正しく保持、復元できるバックアップ機能を有すること。	—	・ドキュメント評価： 対象とする ・実機テスト： 対象とする		

★3セキュリティ要件・適合基準案（通信機器）

適合基準番号	セキュリティ要件（Security Requirement）		★3適合基準	対象外（NA）となるための条件、基準の補足説明	★3評価手法	【参考】海外既存制度・文書で求められるセキュリティ要件との関係性	【参考】国内既存制度・文書で求められるセキュリティ要件との関係性
	カテゴリ	要件					
S3.1-35	10. システムのテレメトリデータを検証・保護する	10-1. テレメトリデータが収集される場合、セキュリティ上の異常がないかどうかを調べなければならない。	IoT製品から収集したログ（テレメトリデータ・監査ログ）を検証し、セキュリティ上の異常を検知すること。具体的には、以下①～③すべての基準を満たすこと。 ①IoT製品に対し、ログ（テレメトリデータ・監査ログ）の取得機能および保存機能を実装すること。最低でも、ファームウェア（ソフトウェア）又はOSにより生成されたログ（テレメトリデータ・監査ログ）を取得・保存する。記録するセキュリティイベントの対象として機器やネットワークの切断（再接続）の記録、ログイン試行（成功時、失敗時）の記録、閾値を越えるログイン試行の記録と、それに対する機器側の対応の記録、時間変更時の記録（変更前と変更後の時刻を含む）、バックアップの取得・復元をはじめとする管理機能の利用記録、ソフトウェア変更時の記録、ハードウェア変更時の記録（監査ログ取得が可能な場合）を取得・保存する機能を有する。 ②ログ（テレメトリデータ・監査ログ）は監査に必要な容量を確保し、保存容量を超過した場合には、古い記録から順次上書きするなど、管理上の対策を行う。なお、必要な保存容量については、製品ごとの利用用途を踏まえ、別途検討を行う。 ③ログ（テレメトリデータ・監査ログ）上のセキュリティイベントの発生日時を記録するため、時間管理機能を有する。	【用語定義：テレメトリデータ】 製品の使用に関する問題や情報を製造業者が特定するのに役立つ情報を提供することができる機器からのデータを指す。 【用語定義：監査ログ】 ユーザが製品におけるセキュリティ上の異常を検知できるようにするため、製品の処理内容やプロセス、および操作の履歴を、時系列かつ連続的に記録したデータを指す。	・ドキュメント評価： 対象とする ・実機テスト： 対象とする	【ETSI EN 303 645】5.10-1 R F 【米国NISTIR 8425】サイバーセキュリティの状態認識 1 【EU-CRA】ANNEX I 1.(2)(l) 【IEC 62443-4-2】CR2.8 監査可能イベント、CR2.11 タイムスタンプ	【CCDSサーティフィケーションプログラム】3-1 ログの記録【推奨】①②③、3-1-1時間管理機能【推奨】① 【RBSS】防犯カメラ認定基準　高度セキュリティ機能 1、デジタルレコーダ認定基準　高度セキュリティ機能 1 【特定用途機器PP】FMT_MTD（TSFデータの管理）、FAU_GEN（監査データ生成）
S3.1-36	11. ユーザが簡単にデータを消去できるようにする	11-1. ユーザが簡単な方法で製品からユーザデータを消去できるような機能を提供しなければならない。	IoT製品利用中にIoT製品のストレージに保存されたデータの削除機能について、以下の①・②のすべての基準を満たすこと。 ①ユーザによって、IoT機器本体や必須付随サービス（モバイルアプリケーション等）を介して、ユーザに関する少なくとも以下のデータを削除できること。 A）IoT製品利用中に取得した情報資産（個人情報含む） B）ユーザ設定値 C）ユーザが設定した認証値、IoT製品利用中に取得した暗号鍵やデジタル署名 D）ログ（テレメトリデータ・監査ログ） ②データ削除後も、アップデートされたセキュリティ機能に関するファームウェア（ソフトウェア）パッケージのバージョンは維持されること。	【用語定義：ユーザ】 ユーザの対象範囲には、IoT 機器の利用者、管理者、ベンダーの カスタマーエンジニア、所有者等、当該 IoT 機器内の守るべき情報資産へのアクセスができ る当該 IoT 機器を使用する自然人及び組織すべてを含んでいなければならない	・ドキュメント評価： 対象とする ・実機テスト： 対象とする	【ETSI EN 303 645】5.11-1 M 【米国NISTIR 8425】データ保護 2 【EU-CRA】ANNEX I 1.(2)(m) 【シンガポールCLS】[＊＊]5.11-1 【IEC 62443-4-2】CR4.2 情報の永続性	【CCDSサーティフィケーションプログラム】1-2-1データ消去【必須】① 【BMSec】セキュリティ設定の初期化 MT-2 【特定用途機器PP】FMT_MTD（TSFデータの管理）
S3.1-37	12. 製品の設置及びメンテナンスを容易にする	12-4. ユーザ及び管理者によって、製品を安全なデフォルト構成設定に復元できる機能を実装しなければならない。	IoT機器は、安全なデフォルト構成設定に復元できること。	—	・ドキュメント評価： 対象とする ・実機テスト： 対象とする	【米国NISTIR 8425】デバイスの構成 2 【EU-CRA】ANNEX I 1.(2)(b)	【BMSec】セキュリティ設定の初期化 MT-2
S3.1-38	13. 入力データの妥当性を確認する	13-1. 製品のソフトウェアは、ユーザインタフェース経由、アプリケーションプログラミングインタフェース（API）経由、又はサービスと製品のネットワーク間で転送されるデータの入力の妥当性を確認しなければならない。	IoT製品のすべてのインタフェースに対して、入力されたデータの妥当性を検証し、入力データが無効で不正である場合は、要求を拒否する機能を実装すること。	—	・ドキュメント評価： 対象とする ・実機テスト： 対象とする	【ETSI EN 303 645】5.13-1A M、5.13-1B M 【米国NISTIR 8425】インターフェイスへの論理アクセス 2-a 【EU-CRA】ANNEX I 1.(2)(g) 【シンガポールCLS】[＊＊]5.13-1 【IEC 62443-4-1】SVV-1 セキュリティ要件テスト 【IEC 62443-4-2】CR3.5 入力のバリデーション	【CCDSサーティフィケーションプログラム】1-4-4インジェクション対策【必須】①

★3セキュリティ要件・適合基準案（通信機器）

適合基準番号	セキュリティ要件（Security Requirement）		★3適合基準	対象外（NA）となるための条件、基準の補足説明	★3評価手法	【参考】海外既存制度・文書で求められるセキュリティ要件との関係性	【参考】国内既存制度・文書で求められるセキュリティ要件との関係性
	カテゴリ	要件					
S3.1-39	14. 個人データを適切に処理する	14-1. 製造業者は、消費者に対し、製品及びサービスごとに、どのような個人データが、誰によって、どのような目的で処理されているかについての明確かつ透明性のある情報を提供しなければならない。これは、広告主を含む、関与する可能性のある第三者にも適用される。	製造業者はIoT製品から得られた個人情報が処理される場合、どのような個人情報が収集され、どのように処理される機能があるかを説明すること。	【NAとなるための条件】 IoT製品が個人情報を収集・処理しない場合	・ドキュメント評価： 対象とする ・実機テスト： なし	【ETSI EN 303 645】6.1 M 【米国NISTIR 8425】教育及び意識向上 1-a 【シンガポールCLS】[＊＊]6.1	
S3.1-40	14. 個人データを適切に処理する	14-4. テレメトリデータが収集される場合、個人データの処理は、意図された機能にとって必要最小限のものに留めなければならない。	IoT製品からテレメトリデータが取得され、かつ個人情報の処理を行う場合、以下の基準を満たすこと。 ①個人情報の処理を、意図された機能にとって必要最小限のものに留めること。	【NAとなるための条件】 IoT製品からテレメトリデータを取得しない又はIoT製品からテレメトリデータを取得するが、個人情報の処理を行わない （「NAであることの理由」に、IoT製品からテレメトリデータを取得しない又は機器からテレメトリデータを取得するが、個人情報の処理を行わないことを示す根拠を記載すること）	ドキュメント評価： 対象とする 実機テスト：なし	【ETSI EN 303 645】6.4 R F 【EU-CRA】ANNEX I 1.(2)(g)	
S3.1-41	14. 個人データを適切に処理する	14-5. テレメトリデータが収集される場合、どのようなテレメトリデータが収集され、それが誰によって、どのような目的で使用されているかについての情報が消費者に提供されなければならない。	IoT製品からログ（テレメトリデータ・監査ログ）を収集する場合、製造業者は、どのようなログ（テレメトリデータ・監査ログ）が収集され、それが誰によって、どのような目的で使用されているかについて周知すること。	【NAとなるための条件】 IoT製品からログ（テレメトリデータ・監査ログ）を収集する仕組みがない場合 【用語定義：テレメトリデータ】 製品の使用に関する問題や情報を製造業者が特定するのに役立つ情報を提供することができる機器からのデータを指す。 【用語定義：監査ログ】 ユーザが製品におけるセキュリティ上の異常を検知できるようにするため、製品の処理内容やプロセスを、時系列かつ連続的に記録したデータを指す。	・ドキュメント評価： 対象とする ・実機テスト： なし	【ETSI EN 303 645】6.5 M F 【米国NISTIR 8425】教育及び意識向上 1-a 【シンガポールCLS】[＊＊]6.5	
S3.1-42	14. 個人データを適切に処理する	14-6.IoT機器に保存および処理されるデータ、またはIoT機器によって必須付随サービスに提供されるデータは、適合基準14-1で特定された目的のために収集・処理に必要な範囲で限定され、特定された目的のいずれにも必要でなくなった場合には削除されなければならない。	IoT製品から得られた個人情報が処理される場合、IoT製品は収集や処理の範囲を限定する機能および不要になった個人情報を削除する機能を有すること。	【NAとなるための条件】 IoT製品が個人情報を収集・処理しない場合	・ドキュメント評価： 対象とする ・実機テスト： 対象とする	【ETSI EN 303 645】6.6 M F	
S3.1-43	16. 脅威を特定しテストする	16-3. 製品に対してペネトレーションテストを実施しなければならない。	製造業者は、第三者によるペネトレーションテストの結果検出されたセキュリティ課題が解消されていること。	—	・ドキュメント評価： なし ・実機テスト： 対象とする	【シンガポールCLS】[＊＊＊]CK-LP-02、[＊＊＊]CK-LP-07 【IEC 62443-4-1】SVV-1 セキュリティ要件テスト、SVV-3 脆弱性テスト、SM-11 安全保障に関連する問題を評価し、対処する、SVV-4 ペネトレーションテスト、SVV-5 テスターの独立性	

★3セキュリティ要件・適合基準案（通信機器）

適合基準番号	セキュリティ要件（Security Requirement）		★3適合基準	対象外（NA）となるための条件、基準の補足説明	★3評価手法	【参考】海外既存制度・文書で求められるセキュリティ要件との関係性	【参考】国内既存制度・文書で求められるセキュリティ要件との関係性
	カテゴリ	要件					
S3.1-44	17. 製品に関する情報提供を行う	17-1. 製品のセキュリティに関する情報が、指定された言語で、指定された主体に提供されなければならない。	ユーザに提供する製品のセキュリティに関する情報は、指定された言語でなければならない。	【用語定義：ユーザ】 ユーザの対象範囲には、IoT 機器の利用者、管理者、ベンダーの カスタマーエンジニア、所有者等、当該 IoT 機器内の守るべき情報資産へのアクセスができ る当該 IoT 機器を使用する自然人及び組織すべてを含んでいなければならない	・ドキュメント評価： 対象とする ・実機テスト： なし	【英国PSTI Act】SCHEDULE 1:2-(3) 【EU-CRA】Article 13 12、Article 13 13、Article 13 22、Article 28 2、Article 31 4 【シンガポールCLS】[＊＊＊]CK-LP-04 【IEC 62443-4-1】DM-5 セキュリティ関連の問題の開示	【BMSec】ファームウェアの提供 FR-2
S3.1-45	17. 製品に関する情報提供を行う	17-2. 製造業者は、製品をセキュアに設定・利用・廃棄する方法について、ユーザに提供しなければならない。	製造業者は、IoT製品のサイバーセキュリティに関する情報提供について、以下の①～⑤のすべての基準を満たす対応を行うこと。 ①初期設定の方法など、IoT製品の利用上、サイバーセキュリティに影響が生じる設定や使用方法について、安全に利用できる手順を周知すること。 ②IoT製品のセキュリティアップデートのリリース時にそのアップデートの内容や必要性、アップデートを行わない場合の影響などを周知する仕組みがあること。 ③アップデートを行わなかったときに想定される事故や障害・一般的に想定される事故や障害に対して、免責事項を周知すること。 ④対象製品やサービスのサポート期限又はサポート終了時の方針を周知すること。 ⑤IoT製品内に守るべき情報資産が残留したまま廃棄や中古販売することで想定されるリスクや、データ消去を含むIoT製品の安全な利用終了方法を周知すること。	【用語定義：守るべき情報資産】 以下の情報： ・通信機能に関する設定情報 ・セキュリティ機能に関する設定情報 ・ログ（テレメトリデータ・監査ログ） ・プログラムコード（ソフトウェア） ・IoT機器の意図する使用において、IoT機器が収集し、保存又は通信する、個人情報等の一般的に機密性が高い情報	・ドキュメント評価： 対象とする ・実機テスト： なし	【ETSI EN 303 645】5.3-11 R C、5.12-2 R、5.3-13 M 【英国PSTI Act】SCHEDULE 1: 3-(2)、3-(3)、3-(4) 【米国NISTIR 8425】ドキュメンテーション 1-a、1-d、教育及び意識向上 1-a、1-c、1-d、1-e、情報発信 1b 1c 1d 1e、情報発信 2 【EU-CRA】Article 13 18、Article 13 19、ANNEX I 2.(4)、ANNEX I 2.(8)、ANNEX II 4、ANNEX II 5、ANNEX II 6、ANNEX II 7、ANNEX II 8、ANNEX II 9、ANNEX VII 7 【IEC 62443-4-1】SG-3 セキュリティ強化のガイドライン、SG-4 安全な廃棄ガイドライン、SR-1 製品セキュリティの背景、SUM-2 セキュリティアップデートの文書化	【CCDSサーティフィケーションプログラム】2-3利用者への情報提供【必須】①②③④⑤ 【BMSec】大容量記憶装置データ保護DP-1、ファームウェアの提供 FR-2、運用環境 PR-1、ファームウェアアップデート機能 PT-1、インターネット通信データ保護 TP-1 【特定用途機器PP】FPT_STM（高信頼性タイムスタンプ）
S3.1-46	19. 製品の可用性を確実にする	19-1. サービス不能攻撃に有効な設計および実装を行わなければならない。	IoT機器はサービス不能攻撃によるネットワーク過負荷状態から復元の仕組みを有すること。	【用語定義：ネットワーク過負荷状態】 ネットワークに過剰な負荷がかかり、通信機器が正常に動作出来ない状態	・ドキュメント評価： 対象とする ・実機テスト： 対象とする		
S3.1-47	21. ハードウェアの完全性を確実にする	21-1. IoT機器に対する物理的な攻撃を防ぐ仕組みを実装しなければならない。	筐体（エンクロージャ）に対する物理的な破壊・改変行為によって、機器内のコンポーネントやインタフェースへ不正にアクセスされることを防ぐために、筐体の耐タンパー性を向上させる仕組みを実装すること。	—	・ドキュメント評価： 対象とする ・実機テスト： なし	【IEC 62443-4-1】EDR3.11 物理的耐タンパー性及び検出	