セキュリティ要件（Security Requirement）		☆1セキュリティ要件の該当有無	☆1評価項目番号	☆1適合基準（☆1 Conformance Criteria）	NAとなるための条件、基準の補足説明	☆1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							
1. 汎用のデフォルトパスワードを使用しない	1-1. パスワードが使用され、工場出荷時のデフォルト以外の状態にある製品において、すべてのパスワードは、機器ごとに固有であるか、又はユーザによって定義されるものでなければならない。	✓	–	評価項目番号＃2の適合基準に統合	–	–	【ETSI EN 303 645】5.1-1 M C (1) 【英国PSTI Act】SCHEDULE 1: 1-(2) 【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 【IEC 62443-4-2】CR1.5, CR1.7	【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）
1. 汎用のデフォルト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。	✓	2	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、又は、機器初期設定時のクライアント認証の仕組みにてパスワードやパスコードを使用する製品において、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、機器毎に異なる一意の値で、容易に推測可能でない6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、8文字以上のパスワードの設定を強制させること。	【NAとなるための条件】 ネットワークを介したユーザ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ユーザ認証が必要ない根拠を記載すること）	ドキュメント評価：①、② 実機テスト：なし	【ETSI EN 303 645】5.1-2 M C (2) 【英国PSTI Act】SCHEDULE 1: 1-(3) 【シンガポールCLS】[＊]5.1-2 【IEC 62443-4-2】CR1.7	【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 【特定用途機器PP】FMT_IPWD_EXT（拡張：初期パスワードの設定）
1. 汎用のデフォルト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。	✓	1	TCP/UDP通信を介した守るべき情報資産への他の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。 なお、電気通信事業法に基づく端末機器セキュリティに係る技術基準を含めた技術基準適合認定を受けた製品（技適[T]マーク又は[A]マークが付与された製品）は、本適合基準に適合しているとみなす。（この場合、「基本情報」シートに「電気通信事業法に基づく技術基準適合認定番号等（技適[T]マークの設計認証番号又は[A]マークの技術基準適合認定番号）」を記入のこと。）	【NAとなるための条件】 ・TCP/UDP通信を介した守るべき情報資産への認証及びアクセスの仕組みがない（「NAであることの理由」に、外部からの不正アクセスに対抗するために認証及びアクセスが必要ない根拠を記載すること） 【用語定義：守るべき情報資産】 以下のすべての情報： ・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 ・機器の意図する使用において、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】5.1-3 M 【英国PSTI Act】SCHEDULE 1: 1-(3) 【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.(3)(b) 【シンガポールCLS】[＊]5.1-3 【IEC 62443-4-2】CR1.5	【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、1-2データ保護【必須】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 【特定用途機器PP】FIA_UAU（認証のタイミング）、FMT_SMR（セキュリティの役割）
1. 汎用のデフォルト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。	✓	3	機器に対するネットワークを介したユーザ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。	【NAとなるための条件】 ・ネットワークを介したユーザ認証の仕組みがない（「NAであることの理由」に、外部からの不正アクセスに対抗するためにユーザ認証が必要ない根拠を記載すること） 【用語定義：認証値】 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。）	ドキュメント評価：対象とする 実機テスト：なし	【ETSI EN 303 645】5.1-4 M C (8) 【シンガポールCLS】[＊]5.1-4 【IEC 62443-4-2】CR1.5	【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）
1. 汎用のデフォルト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。	✓	4	機器が、制約のある機器ではない場合、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。	【NAとなるための条件】 以下のいずれかの条件に該当する。（OR条件） ・機器に対するネットワークを介したユーザアクセスの仕組みがない（「NAであることの理由」に、外部からの不正アクセスに対抗するためにユーザアクセスが必要ない根拠を記載すること） ・機器が「制約のある機器」に該当する（「NAであることの理由」に、機器が「制約のある機器」に該当することを示す根拠を記載すること） 【用語定義：制約のある機器】 データを処理する機能、データを通信する機能、データを保存する機能、又はユーザと対話する機能のいずれかにおいて、意図された使用のために物理的な制約がある機器。（このような機器の例は「用語集」を参照。）	ドキュメント評価：なし 実機テスト：対象とする	【ETSI EN 303 645】5.1-5 M C (5) 【EU-CRA】ANNEX I 1.(3)(b) 【シンガポールCLS】[＊]5.1-5 【IEC 62443-4-2】CR1.11	【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）
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	✓	5	製造業者は、以下の①～③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。 ① 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及びその概要 ③ 脆弱性が解決されるまでの製品や脆弱性の状況更新に関する手続き及びその概要	–	ドキュメント評価：①、②、③ 実機テスト：なし	【ETSI EN 303 645】5.2-1 M 【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 【EU-CRA】ANNEX I 2.(5)、ANNEX I 2.(6)、ANNEX II 1、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	【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】① 【BMSec】問い合わせ窓口 FR-1

セキュリティ要件（Security Requirement）		☆1セキュリティ要件の該当有無	☆1評価項目番号	☆1適合基準（☆1 Conformance Criteria）	NAとなるための条件、基準の補足説明	☆1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							
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。	✓	6	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①～③のすべての基準を満たすこと。 ①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。 なお、電気通信事業法に基づく端末機器セキュリティに係る技術基準を含めた技術基準適合認定を受けた製品（技適[T]マーク又は[A]マークが付与された製品）は、本適合基準に適合しているとみなす。（この場合、「基本情報」シートに「電気通信事業法に基づく技術基準適合認定番号等（技適[T]マークの設計認証番号又は[A]マークの技術基準適合認定番号）」を記入のこと。）	–	ドキュメント評価：なし 実機テスト：①、②、③	【ETSI EN 303 645】5.3-1 R 【米国NISTIR 8425】ソフトウェアの更新 1 【EU-CRA】ANNEX I 2.(8) 【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 暗号の使用、CR3.10 EDR3.10、 HDR3.10 NDR 3.10、アップデートをサポート	【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 【特定用途機器PP】FMT_SMF（管理機能の特定）
3. ソフトウェアを最新の状態に保つ	3-2. 機器が、制約のある機器でない場合、アップデートをセキュアにインストールするためのアップデートメカニズムを備えていなければならない。	✓	–	評価項目番号#6及び#8の適合基準に統合	–	–	【ETSI EN 303 645】5.3-2 M C (5) 【米国NISTIR 8425】ソフトウェアの更新 1 【シンガポールCLS】[＊]5.3-2	【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 【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）
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。	✓	7	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。	–	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 C (12) 【EU-CRA】ANNEX I 2.(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) 【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. 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。	✓	8	ソフトウェアをネットワーク経由でアップデートする際、ソフトウェアの完全性をアップデート前に確認できる仕組みを有すること。	【NAとなるための条件】 ソフトウェアをネットワーク経由でアップデートする仕組みが存在しない（「NAであることの理由」に、想定するアップデートの仕組みを記載すること）	ドキュメント評価：対象とする 実機テスト：なし	【ETSI EN 303 645】5.3-7 M C (12) 【米国NISTIR 8425】ソフトウェアの更新 1 【シンガポールCLS】[＊]5.3-7 【IEC 62443-4-2】CR4.3 暗号の使用	【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】② 【特定用途機器PP】FMT_SMF（管理機能の特定）
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。	✓	9	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 (12) 【EU-CRA】ANNEX I 2.(2)、ANNEX I 2.(7)、ANNEX I 2.(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. ソフトウェアを最新の状態に保つ	3-10. 製品においてアップデートメカニズムが実装され、ソフトウェアアップデートがネットワークインタフェースを介して配信される場合、製品は、信頼関係を介して各アップデートの真正性及び完全性を検証しなければならない。	✓	–	評価項目番号#8の適合基準に統合	–	–	【ETSI EN 303 645】5.3-10 M (11,12) 【EU-CRA】ANNEX I 1.(3)(e) 【シンガポールCLS】[＊]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	【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 【特定用途機器PP】FMT_SMF（管理機能の特定）
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。	✓	10	製品の型式番号は、以下のいずれかの方法でユーザへ提供すること。 ① 製品本体に、製品の型式番号を直接記載すること。 ② 製品のGUI、ウェブUI等や、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、ユーザが型式番号を認識できるようにすること。	–	ドキュメント評価：なし 本体確認・実機テスト：①又は②	【ETSI EN 303 645】5.3-16 M 【米国NISTIR 8425】情報発信 2 【EU-CRA】ANNEX II 3 【シンガポールCLS】[＊]5.3-16	
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。	✓	11	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。）が、ネットワーク経由の不正アクセスに対して、セキュアに保存されること。	【用語定義：守るべき情報資産】 以下のすべての情報： ・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 ・機器の意図する使用において、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 【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　認証管理、CR1.9 公開鍵ベースの認証強度、CR1.14 共通鍵ベースの認証強度、CR3.8 セッションの完全性、CR4.1 情報の機密性、CR3.12 EDR3.12 HDR3.12 NDR3.12 信頼のための製品サプライヤーの情報等の提供、CR3.13 EDR3.13 HDR3.13 NDR3.13 資産保有者の情報等の提供	【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】FMT_MTD（TSFデータの管理）

セキュリティ要件（Security Requirement）		☆1セキュリティ要件の該当有無	☆1評価項目番号	☆1適合基準（☆1 Conformance Criteria）	NAとなるための条件、基準の補足説明	☆1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							
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。	✓	12	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、情報の盗聴に対する以下のいずれかの保護対策が行われていること。 ① 他のIoT機器やサーバ（クラウド上のサーバを含む）へネットワークを介して伝送される守るべき情報資産について、情報の盗聴に対する保護対策を機器自らが行う。 ② 他のIoT機器やサーバ（クラウド上のサーバを含む）へネットワークを介して伝送される守るべき情報資産について、保護された通信環境（VPN環境や専用線を経由した接続環境）においてのみ伝送される。	【NAとなるための条件】 ネットワーク経由で伝送される守るべき情報資産が存在しない（「NAであることの理由」に、ネットワーク経由で伝送される守るべき情報資産が存在しないことを示す根拠を記載すること） 【用語定義：守るべき情報資産】 以下のすべての情報： ・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 ・機器の意図する使用において、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：①又は② 実機テスト：なし	【ETSI EN 303 645】5.5-1 M 【米国NISTIR 8425】データ保護 3 【EU-CRA】ANNEX I 1.(3)(c) 【シンガポールCLS】[＊＊]5.5-1 【IEC 62443-4-2】CR3.1 通信の完全性、CR4.3 暗号の使用	【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、1-4-1Wi-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
5. セキュアに通信する	5-5. ネットワークインタフェースを介してセキュリティに関連する設定の変更を可能にする製品の機能は、認証後にのみアクセス可能でなければならない。ただし、製品が依存するネットワークサービスプロトコルで、製品の動作に必要な設定を製造業者が保証できない場合は、例外とする。	✓	–	評価項目番号＃1の適合基準に統合	–	–	【ETSI EN 303 645】5.5-5 M 【EU-CRA】ANNEX I 1.(3)(b) 【シンガポールCLS】[＊＊]5.5-5 【IEC 62443-4-2】CR1.6 NDR1.6 無線アクセス管理、CR2.12 否認防止、CR6.1 監査ログのアクセシビリティ	【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、1-3 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_UID（アクション前の利用者識別）
5. セキュアに通信する	5-7. 製品は、リモートアクセス可能なネットワークインタフェースを介して通信される重要なセキュリティパラメータの機密性を保護しなければならない。	✓	–	評価項目番号＃12の適合基準に統合	–	–	【ETSI EN 303 645】5.5-7 M 【EU-CRA】ANNEX I 1.(3)(c) 【シンガポールCLS】[＊＊]5.5-7 【IEC 62443-4-2】CR3.1 通信の完全性、CR4.3 暗号の使用	【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、1-4-1Wi-Fiの認証方式【必須】
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。	✓	13	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、製品の利用上不要かつ攻撃を受けるリスクがある物理的インタフェース及び論理的インタフェースを無効化するとともに、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。 ①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、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 ②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：① 実機テスト：①、② ※①は、ドキュメント評価と実機テストの双方を実施すること	【ETSI EN 303 645】5.6-1 M 【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.(3)(h) 【シンガポールCLS】[＊＊]5.6-1 【IEC 62443-4-2】CR7.7 最小の機能性	【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 【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
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。	✓	14	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、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。 なお、電気通信事業法に基づく端末機器セキュリティに係る技術基準を含めた技術基準適合認定を受けた製品（技適[T]マーク又は[A]マークが付与された製品）は、本適合基準に適合しているとみなす。（この場合、「基本情報」シートに「電気通信事業法に基づく技術基準適合認定番号等（技適[T]マークの設計認証番号又は[A]マークの技術基準適合認定番号）」を記入のこと。）	–	ドキュメント評価：なし 実機テスト：対象とする	【ETSI EN 303 645】5.9-1 R 【EU-CRA】ANNEX I 1.(3)(f) 【IEC 62443-4-2】CR7.1 サービス妨害からの保護、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

セキュリティ要件（Security Requirement）		☆1セキュリティ要件の該当有無	☆1評価項目番号	☆1適合基準（☆1 Conformance Criteria）	NAとなるための条件、基準の補足説明	☆1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							
11. ユーザが簡単にデータを消去できるようにする	11-1. ユーザは、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されなければならない。	✓	15	製品利用中に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、機器本体や関連サービス（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) 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、製品利用中に取得した暗号鍵やデジタル署名 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。	–	ドキュメント評価：① 実機テスト：①、② ※①は、ドキュメント評価と実機テストの双方を実施すること	【ETSI EN 303 645】5.11-1 M 【米国NISTIR 8425】データ保護 2 【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）
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。	✓	16	製造業者は、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、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。 ②製品のセキュリティ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。 ⑤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】 以下のすべての情報： ・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 ・機器の意図する使用において、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：①、②、③、④、⑤ 実機テスト：なし	【ETSI EN 303 645】5.12-2 R 【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、情報発信 2 【EU-CRA】ANNEX II 4、ANNEX II 9 【IEC 62443-4-1】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】① 【BMSec】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
17. 製品に関する情報提供を行う	17-3.　アップデートメカニズムが実装されている場合、製造業者は、セキュリティアップデートが必要であることを、そのアップデートによって軽減されるリスクに関する情報とともに、認識可能で明らかな方法でユーザに通知しなければならない。	✓	–	評価項目番号＃16の適合基準に統合	–	–	【ETSI EN 303 645】5.3-11 R C (12) 【米国NISTIR 8425】情報発信 1c 1d 1e 【EU-CRA】ANNEX I 2.(4)、ANNEX I 2.(8) 【IEC 62443-4-1】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】② 【BMSec】ファームウェアの提供 FR-2
17. 製品に関する情報提供を行う	17-5. 製造業者は、ユーザが製品を廃棄する手順について、指定された方法でユーザに提供しなければならない。	✓	–	評価項目番号＃16の適合基準に統合	–	–	【米国NISTIR 8425】教育及び意識向上 1-c 【IEC 62443-4-1】SG-4 安全な廃棄ガイドライン	【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】⑤ 【BMSec】大容量記憶装置データ保護DP-1
17. 製品に関する情報提供を行う	17-8. 製造業者は、定められたサポート期間を、ユーザにとって明確で透明性のある方法で公表しなければならない。	✓	–	評価項目番号＃16の適合基準に統合	–	–	【ETSI EN 303 645】5.3-13 M 【英国PSTI Act】SCHEDULE 1: 3-(2), 3-(3), 3-(4) 【米国NISTIR 8425】教育及び意識向上 1-d, 1-e、情報発信 1b 【EU-CRA】ANNEX II 6、ANNEX II 7、ANNEX II 8 【シンガポールCLS】[＊]5.3-13 【IEC 62443-4-1】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】2-3利用者への情報提供【必須】④ 【特定用途機器PP】FPT_SMT（高信頼性タイムスタンプ）
17. 製品に関する情報提供を行う	17-10. 製造業者は、セキュリティリスクを引き起こす可能性がある製品の利用状況に関する情報について、指定された方法でユーザに提供しなければならない。	✓	–	評価項目番号＃16の適合基準に統合	–	–	【米国NISTIR 8425】ドキュメンテーション 1-d 【EU-CRA】ANNEX II 5 【IEC 62443-4-1】SG-3 セキュリティ強化のガイドライン、SR-1 製品セキュリティの背景	【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】①③ 【BMSec】運用環境 PR-1

用語	意味
IoT機器／機器	ネットワークに接続された（及びネットワークに接続可能な）機器で、関連サービスとの関係を持つもの。 注 1： IoT機器は、一般的にビジネスの環境においても使用される。 注 2： IoT機器は、多くの場合、消費者が小売り環境で購入することができる。IoT機器は、専門的に委託及び／又は設置することもできる。
IoT製品／製品	IoT機器とその関連サービス。
外部感知機能	ある対象の情報を収集し、機械が取り扱うことのできる信号に置き換える素子や装置のこと。 例：光学センサ、音響センサ、カメラ、マイク
管理者	機器のユーザに対して可能な最高の特権レベルを持つユーザ。これは、意図された機能に関連する設定を変更できることを意味する。
関連サービス	機器と共にIoT製品全体の一部であり、通常は製品の意図された機能を提供するために必要なデジタルサービス。 例 1： 関連サービスには、モバイルアプリケーション、クラウドコンピューティング／ストレージ、及びサードパーティのアプリケーションプログラミングインタフェース（API）を含めることができる。 例 2： ある機器は、機器の製造業者によって選択されたサードパーティのサービスにテレメトリデータを送信する。このサービスは関連サービスである。
技術文書	評価手順で参照され、適合基準への適合を示す根拠となる技術仕様を記載した文書で、製品の設計書、仕様書、開発手順書、マニュアル等の文書、又はこれらの文書に基づき策定される文書のこと。公開・非公開の区分は問わず、申請者自身の判断に基づき選定できる。また、他標準で用いるフォーマットやフリーフォーマットでの技術仕様の記載も許容する。
機密の個人データ	その開示が個人に害を及ぼす可能性が高いデータのこと。 「機密な個人データ」として扱われるものは、製品やユースケースによって異なるが、例えば、家庭用セキュリティカメラのビデオストリーム、支払い情報、通信データの内容、タイムスタンプ付きの位置データなどが例として挙げられる。
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及び公開セキュリティパラメータ。
公開セキュリティパラメータ	セキュリティ関連の公開情報で、改ざんされるとセキュリティモジュールのセキュリティが侵害される可能性があるもの。 例 1： ソフトウェアアップデートの真正性／完全性を検証するための公開鍵。 例 2： 証明書の公開要素。
工場出荷時のデフォルト	工場出荷時の状態にリセットした後の状態、又は最終的な製造／組み立て後の機器の状態。 注： これには、物理的な機器と、組み立て後にその機器に存在するソフトウェア（ファームウェアを含む）が含まれる。
構成設定	情報システムのセキュリティ体制や機能に影響を与える、ハードウェア、ソフトウェア、またはファームウェアで変更できるパラメータのセットのこと。
個人データ	識別された、又は識別可能な自然人に関するあらゆる情報。 注： この用語は、周知の用語と整合させるために使用されているが、本文書内では法的意味を持たない。
自己完結型の環境	他のサービスに依存せず単独で利用できる環境のこと。
重要なセキュリティパラメータ	曝露又は改ざんによってセキュリティモジュールのセキュリティが侵害される可能性がある、セキュリティ関連の秘密情報。 例： 秘密の暗号鍵、パスワードなどの認証値、PIN、証明書のプライベート要素。
消費者	自己の商取引、ビジネス、工芸、専門的職業以外の目的のために行動している自然人。 注： あらゆる規模の企業を含む組織が、IoTを利用している。例えば、スマートテレビは会議室に頻繁に導入されているし、ホームセキュリティキットは小規模企業の敷地を保護することができる。
初期化	操作のために機器のネットワーク接続を有効化し、オプションとしてユーザ又はネットワークアクセスのための認証機能を設定するプロセス。
初期化状態	初期化後の機器の状態。
所有者	機器を所有するユーザ、又は購入したユーザ。
ストレージ	データ又は情報を保存し、そこからデータ又は情報を取り出すことができる媒体。
製造業者	サプライチェーン内の関連事業者（機器の製造業者を含む）。 注： この定義は、IoTエコシステムに関与する多様な主体及びそれらの主体が責任を共有する複雑な方法を認めている。機器の製造業者以外にも、例えば目前の特定のケースに応じて、輸入業者、販売業者、インテグレータ、コンポーネント及びプラットフォームプロバイダ、ソフトウェアプロバイダ、IT及び電気通信サービスプロバイダ、マネージドサービスプロバイダ及び関連サービスのプロバイダなどがある。

用語	意味
制約のある機器	データを処理する機能、データを通信する機能、データを保存する機能、又はユーザと対話する機能のいずれかにおいて、意図された使用のために物理的な制約がある機器。 注 1： 物理的な制約は、電源、バッテリ寿命、処理能力、物理アクセス、機能の制限、メモリの制限、又はネットワーク帯域幅の制限による場合がある。制約のある機器は、基地局やコンパニオンデバイスなどの別の機器によってサポートされることが必要となる場合がある。 例 1： バッテリを充電又は交換できない窓センサ。 例 2： ストレージの制限により、機器のソフトウェアをアップデートすることができないため、セキュリティの脆弱性を管理するためには、ハードウェアの交換又はネットワークの分離しか選択肢がない機器。 例 3： 様々な場所に配置できるようにバッテリを使用している低電力機器。これらの機器では、高電力な暗号化処理を実行するとバッテリの寿命が急速に短くなるため、アップデートの検証は基地局又はハブに頼っている。 例 4： Bluetooth ペアリングのためのバインドコードを検証するための表示画面がない機器。 例 5： 認証情報を入力する機能がない機器。（キーボードを介した入力機能など） 注 2： 有線接続された電源を有し、IP ベースのプロトコル及びそのプロトコルで使用される暗号プリミティブをサポートできる機器は、制約のある機器のある機器ではない。 例 6： コンセントを使って給電され、主に TLS（トランスポート層セキュリティ）を使用して通信を行う機器。
セキュリティアップデート	製造業者が発見した、又は製造業者に報告されたセキュリティの脆弱性に対処するためのソフトウェアアップデート。 注： 脆弱性の深刻度が、より高い優先度の修正を必要とする場合、ソフトウェアアップデートは純粋なセキュリティアップデートになり得る。
セキュリティモジュール	セキュリティ機能を実装する、ハードウェア、ソフトウェア、及び/又はファームウェアのセット。 例： 機器には、ハードウェアの信頼の基点、信頼できる実行環境内で動作する暗号化ソフトウェアライブラリ、及びユーザの分離やアップデートメカニズムなどのセキュリティを強化する OS 内のソフトウェアが含まれている。これらすべてが、セキュリティモジュールを構成している。
ゾーン	対象のシステムを、機能的、論理的、物理的な（場所を含む）関係に基づいて分割した各エンティティのこと。
ゾーン境界	ゾーン間の境界のこと。
ソフトウェアサービス	機能をサポートするために使用される機器のソフトウェアコンポーネント。 例： 機器のソフトウェア内で使用されるプログラミング言語のランタイム、又は機器のソフトウェアで使用されるAPI を公開するデーモン（暗号化モジュールの API など）
定義されたサポート期間	製造業者がセキュリティアップデートを提供する期間又は終了日付で表される最小期間。 注： この定義は、セキュリティの側面に焦点を当てており、保証などの製品サポートに関連する他の側面には焦点を当てていない。
機器ごとに固有	所定の製品クラス又はタイプの個々の機器毎に固有。
デバッグインタフェース	製造業者が開発中に機器と通信するため、又は機器の問題のトリアージを実行するために使用し、消費者向けの機能の一部としては使用されない物理インタフェース。 例： テストポイント、UART、SWD、JTAG。
テレメトリ	機器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。 例： IoT機器は、ソフトウェアの不具合を製造業者に報告し、製造業者が原因を特定して修正できるようにする。
認証値	認証メカニズムで使用される属性の個別値。 例： 認証メカニズムがパスワードの要求である場合、認証値は文字列とすることができる。認証メカニズムが生体指紋認証である場合、認証値は左手の人差し指の指紋とすることができる。
認証メカニズム	エンティティの真正性を証明するために使用される方法。 注：「エンティティ」は、ユーザ又はマシンのいずれかである。 例： 認証メカニズムには、パスワードの要求、QR コードのスキャン、又は生体認証用指紋スキャナの使用がある。
ネットワークインタフェース	ネットワークを介してIoTの機能にアクセスするために使用できる物理的インタフェース。
ハードコードされた機器ごとの固有ID	ソースコードに直に記述した機器ごとに固有の値のこと。 例：機器に固有のネットワークアクセスに使用されるマスターキー（秘密鍵）
物理的インタフェース	物理層で機器と通信するために使用する物理ポート又はエアインタフェース（無線、オーディオ、光など） 例： 無線、イーサネットポート、USB などのシリアルインタフェース、及びデバッグに使用されるもの。
分離可能	接続されているネットワークから取り外すことができ、生じた機能損失は、その接続性だけに関連し、その主な機能には関係しない。その代わりに、その環境内の機器の完全性が確実である場合に限り、他の機器と共に自己完結型の環境に置くことができる。 例： スマート冷蔵庫は、ネットワークに接続されたタッチスクリーンベースのインタフェースを備えている。このインタフェースは、冷蔵庫の中身の冷却を止めることなく取り外すことができる。
ベストプラクティスの暗号技術	対応するユースケースに適した暗号技術で、現在すぐに利用でき、実行可能な攻撃の兆候がない技術。 注 1： これは、使用される基本的な暗号だけでなく、実装、鍵生成、及び鍵の取り扱いについても当てはまる。 注 2： 標準開発機関や公的機関など複数の組織が、使用可能な暗号化手法のガイドとカタログを保持している。 例： 機器の製造業者は、IoT プラットフォームと共に提供される通信プロトコルと暗号化ライブラリを使用し、そのライブラリとプロトコルは、リプレイ攻撃などの実現可能な攻撃に対して評価されている。
ユーザ	自然人又は組織。
リモートアクセス可能	ローカルネットワークの外部からアクセスできるよう意図されている。
論理的インタフェース	ネットワークインタフェースを利用し、チャネル又はポートを介してネットワーク上で通信するソフトウェア実装。