セキュリティ要件（Security Requirement）		☆1セキュリティ要件の該当有無	【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。	✓	【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。	✓	【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。	✓	【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。	✓	【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。	✓	【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	✓	【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
2. 脆弱性の報告を管理するための手段を導入する	2-2. 製造業者は、製品に関し開示された脆弱性には、タイムリーな方法で対処しなければならない。		【ETSI EN 303 645】5.2-2、R 【米国NISTIR 8425】ドキュメンテーション 1-g 【EU-CRA】ANNEX I 2.(7)、Article 10 12 【IEC 62443-4-1】DM-2 セキュリティ関連の問題を見直す、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	【BMSec】ファームウェアの提供 FR-2
2. 脆弱性の報告を管理するための手段を導入する	2-3. 製造業者は、定められたサポート期間中、販売、製造された製品及び運用するサービス内のセキュリティ脆弱性を継続的に監視し、特定し、修正しなければならない。		【ETSI EN 303 645】5.2-3 R 【EU-CRA】ANNEX I 1.(3)(k) 【IEC 62443-4-1】DM-2 セキュリティ関連の問題を見直す	
2. 脆弱性の報告を管理するための手段を導入する	2-4. 製造業者は、製品に含まれる脆弱性が悪用された事実を知り得た場合に、指定された期間以内に、指定された組織に対して、指定された内容を報告しなければならない。		【EU-CRA】Article 11 1、Article 11 2 、Article 11 4、Article 11 7 【IEC 62443-4-1】SG-3 セキュリティ強化のガイドライン	
2. 脆弱性の報告を管理するための手段を導入する	2-5. 製造業者は、セキュリティの問題管理プロセスを継続的に更新しなければならない。		【IEC 62443-4-1】DM-6 セキュリティ上の欠陥の管理方法を定期的に見直す	
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。	✓	【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。	✓	【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。	✓	【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	3-4. 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、そのアップデートには、自動化メカニズムを使用しなければならない。		【ETSI EN 303 645】5.3-4 R C (12) 【米国NISTIR 8425】ソフトウェアの更新 2 【EU-CRA】ANNEX I 1.(3)(k)	【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	3-5. 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、初期化後に、定期的にセキュリティアップデートが利用可能かどうかを確認しなければならない。		【ETSI EN 303 645】5.3-5 R C (12) 【米国NISTIR 8425】情報発信 1a 【EU-CRA】ANNEX I 1.(3)(k)	【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	3-6. 製品においてアップデートメカニズムが実装され、自動化されたアップデートメカニズムやアップデート通知メカニズムをサポートしている場合、これらは初期化された状態で有効であり、ユーザがセキュリティアップデートやアップデート通知のインストールを有効、無効、又は延期できるように設定可能にしなければならない。		【ETSI EN 303 645】5.3-6 R C (9, 12)	【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】④ 【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。	✓	【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。	✓	【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	3-9. 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、ソフトウェアアップデートの真正性と完全性を検証しなければならない。		【ETSI EN 303 645】5.3-9 R C (12) 【EU-CRA】ANNEX I 1.(3)(e) 【IEC 62443-4-1】SM-6 ファイルの完全性 【IEC 62443-4-2】CR4.3 暗号の使用、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 【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	3-10. 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。	✓	【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	3-11. 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。		【ETSI EN 303 645】5.3-14 R C (3,4) 【米国NISTIR 8425】情報発信 1	
3. ソフトウェアを最新の状態に保つ	3-12. ソフトウェアコンポーネントがアップデート可能ではなく、機器に制約がある場合、機器は分離可能にしなければならない。		【ETSI EN 303 645】5.3-15 R C (3,4) 【IEC 62443-4-2】CR2.6 リモート・セッションの終了、CR5.1 ネットワーク・セグメンテーション	
3. ソフトウェアを最新の状態に保つ	3-13. ソフトウェアコンポーネントがアップデート可能ではなく、機器に制約がある場合、ハードウェアは交換可能にしなければならない。		【ETSI EN 303 645】5.3-15 R C (3,4)	

セキュリティ要件（Security Requirement）		☆1セキュリティ要件の該当有無	【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	3-14. 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。	✓	【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	
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。		【EU-CRA】ANNEX I 2.(1) 【シンガポールCLS】[＊＊＊]CK-LP-06	【BMSec】構成管理 CM-1
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。	✓	【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）
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。		【ETSI EN 303 645】5.4-2 M C (10) 【シンガポールCLS】[＊＊]5.4-2 【IEC 62443-4-2】CR1.5 認証管理、CR3.11 EDR3.11 HDR3.11 NDR3.11 物理的な改ざん防止と検出	
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。		【ETSI EN 303 645】5.4-3 M 【シンガポールCLS】[＊＊]5.4-3	
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関連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。		【ETSI EN 303 645】5.4-4 M 【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【推奨】①②
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。	✓	【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	5-2. 製品は、ネットワーク及びセキュリティ機能、特に暗号技術の分野においてレビュー又は評価された実装を使用しなければならない。		【ETSI EN 303 645】5.5-2 R 【米国NISTIR 8425】データ保護 1 【EU-CRA】ANNEX I 2.(3) 【シンガポールCLS】[＊＊＊]CK-LP-02 【IEC 62443-4-1】SD-3 セキュリティ設計レビュー 【IEC 62443-4-2】CR1.8 公開鍵証明書、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、CR3.12 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【推奨】①②
5. セキュアに通信する	5-3. 暗号アルゴリズムとプリミティブは、アップデート可能にしなければならない。		【ETSI EN 303 645】5.5-3 R	【特定用途機器PP】FMT_SMF（管理機能の特定）
5. セキュアに通信する	5-4. 初期化された状態のネットワークインタフェースを経由した製品の機能へのアクセスは、そのインタフェースでの認証後にのみ可能にしなければならない。		【ETSI EN 303 645】5.5-4 R 【米国NISTIR 8425】インターフェイスへの論理アクセス 1-c, 2-b, 2-c 【EU-CRA】ANNEX I 1.(3)(b) 【IEC 62443-4-2】CR1.1 ユーザ識別と認証、CR1.6 NDR1.6 無線アクセス管理、CR1.12 システム使用通知、CR2.1 認可の実施、CR1.13 NDR1.13 信頼できないネットワーク経由のアクセス、CR2.2 ワイヤレス使用制御、CR2.12 否認防止	【RBSS】デジタルレコーダ認定基準 セキュリティ機能 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。	✓	【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	5-6. 重要なセキュリティパラメータは、転送中は暗号化されることが望ましく、その暗号化は技術の特性、リスク及び用途に適切なものにしなければならない。		【ETSI EN 303 645】5.5-6 R 【EU-CRA】ANNEX I 1.(3)(c) 【IEC 62443-4-1】SM-8 秘密鍵の管理 【IEC 62443-4-2】CR1.5 認証管理、CR3.1 通信の完全性、CR4.3 暗号の使用	【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
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。	✓	【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】
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。		【ETSI EN 303 645】5.5-8 M 【シンガポールCLS】[＊＊]5.5-8、[＊＊＊]CK-LP-09 【IEC 62443-4-2】CR1.3 アカウント管理、CR1.4 識別子の管理	
5. セキュアに通信する	5-9. ゾーン境界に設置する製品に、通信を監視・制御する機能を実装しなければならない。		【IEC 62443-4-2】CR5.2 NDR5.2 ゾーン境界の保護	
5. セキュアに通信する	5-10. 製品間のすべての通信において、改ざんを検出するための機能を実装しなければならない。また、改ざんが検出された場合には、ユーザへの通知等のアクションが実行されなければならない。		【EU-CRA】ANNEX I 1.(3)(d)	【特定用途機器PP】FPT_ITI（TSF間改変の検出）
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。	✓	【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
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。		【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 認証機能のフィードバック	【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
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。		【ETSI EN 303 645】5.6-3 R 【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) 【IEC 62443-4-2】CR2.13 EDR2.13、HDR2.13 NDR2.13 物理診断およびテストインターフェイスの使用、CR7.7 最小の機能性、CR5.3 NDR5.3 汎用個人間通信の制限	【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 【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
6. 露出した攻撃面を最小化する	6-4. デバッグインタフェースが物理的にアクセス可能である場合に、ソフトウェアで無効化しなければならない。		【ETSI EN 303 645】5.6-4 M C (13) 【EU-CRA】ANNEX I 1.(3)(h) 【シンガポールCLS】[＊＊]5.6-4 【IEC 62443-4-2】CR2.13 EDR2.13、HDR2.13 NDR2.13 物理診断およびテストインターフェイスの使用、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】1-4-3USBのアクセス制御【必須】① 【BMSec】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
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。		【ETSI EN 303 645】5.6-5 R 【シンガポールCLS】[＊＊＊]CK-LP-05 【IEC 62443-4-2】CR7.7 最小の機能性	
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。		【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	
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。		【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 最小の機能性	【RBSS】デジタルレコーダ認定基準 セキュリティ機能 3, 4
6. 露出した攻撃面を最小化する	6-8. 製品には、メモリに対するハードウェアレベルのアクセス制御メカニズムを含めなければならない。		【ETSI EN 303 645】5.6-8 R	

セキュリティ要件（Security Requirement）		☆1セキュリティ要件の該当有無	【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			
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。		【ETSI EN 303 645】5.6-9 R 【EU-CRA】Article 10 9 【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
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。		【EU-CRA】Article 10 4、ANNEX I 1.(1)、Artice 10 2 【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	
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。		【ETSI EN 303 645】5.7-1 R 【EU-CRA】ANNEX I 1.(3)(e) 【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と認証、CR3.4 ソフトウェアと情報の完全性、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
7. ソフトウェアの完全性を確実にする	7-2. ソフトウェアに不正な変更が検出された場合、製品はユーザ及び／又は管理者に問題を警告し、警告機能を実行するために必要なネットワークよりも広いネットワークに接続しないようにしなければならない。		【ETSI EN 303 645】5.7-2 R 【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.(3)(g) 【IEC 62443-4-1】SM-6 ファイルの完全性 【IEC 62443-4-2】CR3.7 エラー処理、CR6.2 継続的モニタリング	
8. 個人データがセキュアであることを確実にする	8-1. 機器とサービス（特に関連サービス）間で通信される個人データの機密性は、ベストプラクティスの暗号技術を使用して保護しなければならない。		【ETSI EN 303 645】5.8-1 R 【EU-CRA】ANNEX I 1.(3)(c) 【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】1-2データ保護【必須】② 【RBSS】防犯カメラ認定基準 高度セキュリティ機能 3
8. 個人データがセキュアであることを確実にする	8-2. 機器と関連サービス間で通信される機密の個人データの機密性は、技術の特性と使用法に適した暗号技術によって保護されなければならない。		【ETSI EN 303 645】5.8-2 M 【EU-CRA】ANNEX I 1.(3)(c) 【シンガポールCLS】[＊＊]5.8-2 【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】1-2データ保護【必須】②
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。		【ETSI EN 303 645】5.8-3 M 【シンガポールCLS】[＊＊]5.8-3	
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。	✓	【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
9. 停止に対してレジリエントなシステムにする	9-2. 製品は、ネットワークアクセスが失われた場合にも動作を維持し、ローカルで機能し続け、電源損失が回復した場合にも正常に回復しなければならない。		【ETSI EN 303 645】5.9-2 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、CR7.4 制御システムの回復と再構成、CR7.5 非常用電源	
9. 停止に対してレジリエントなシステムにする	9-3. 製品は、インフラの能力を考慮し、期待された、運用可能な安定した状態で、秩序ある方法でネットワークに接続しなければならない。		【ETSI EN 303 645】5.9-3 R 【EU-CRA】ANNEX I 1.(3)(f) 【IEC 62443-4-2】CR2.7 同時セッション制御、CR7.1 サービス妨害からの保護、CR7.2 リソース管理	
9. 停止に対してレジリエントなシステムにする	9-4. アクセス制御や認証等の悪用防止メカニズムを用いて、インシデントの影響を軽減しなければならない。		【EU-CRA】ANNEX I 1.(3)(i)、Artice 10 2、ANNEX I 1.(1) 【IEC 62443-4-2】CR2.9 保管容量の監査、CR2.10 監査処理への失敗への対応、CR3.6 決定論的出力	
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。		【ETSI EN 303 645】5.10-1 R C (6) 【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.(3)(j) 【IEC 62443-4-2】CR2.8 監査可能な事象、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）
10. システムのテレメトリデータを検証・保護する	10-2. テレメトリデータは、データの暗号化やアクセス制御等のメカニズムによって保護しなければならない。		【IEC 62443-4-2】CR3.9 監査情報の保護	【特定用途機器PP】FAU_STG（保護された監査証跡格納）
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。	✓	【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）
11. ユーザが簡単にデータを消去できるようにする	11-2. ユーザは、簡単な方法で個人データを関連サービスから削除できるような、製品上の機能を提供されなければならない。		【ETSI EN 303 645】5.11-2 R 【米国NISTIR 8425】データ保護 2 【IEC 62443-4-2】CR4.2 情報の永続性	【BMSec】セキュリティ設定の初期化 MT-2、大容量記憶装置データ保護 DP-1 【特定用途機器PP】FMT_MTD（TSFデータの管理）
11. ユーザが簡単にデータを消去できるようにする	11-3. ユーザは、個人データを削除する方法について、明確な指示が与えられなければならない。		【ETSI EN 303 645】5.11-3 R 【米国NISTIR 8425】データ保護 2、教育及び意識向上 1-a 【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】セキュリティ設定の初期化 MT-2、大容量記憶装置データ保護 DP-1
11. ユーザが簡単にデータを消去できるようにする	11-4. ユーザは、サービス、機器、及びアプリケーションから個人データが削除されたことを示す明確な確認を提供されなければならない。		【ETSI EN 303 645】5.11-4 R 【IEC 62443-4-1】SG-4 安全な廃棄ガイドライン	
12. 製品の設置及びメンテナンスを容易にする	12-1. 製品の設置及び保守は、ユーザによる決定を最小限とし、ユーザビリティに関するセキュリティのベストプラクティスに従わなくてはならない。		【ETSI EN 303 645】5.12-1 R	【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【推奨】① 【特定用途機器PP】FMT_MOF（セキュリティ機能のふるまいの管理）
12. 製品の設置及びメンテナンスを容易にする	12-2. 製造業者は、使用する製品がセキュアにセットアップされているかどうかを確認する方法について、ユーザにガイダンスを提供しなければならない。		【ETSI EN 303 645】5.12-3 R 【米国NISTIR 8425】教育及び意識向上 1-a 【EU-CRA】ANNEX I 1.(2)、ANNEX I 1.(3)(a)	【BMSec】運用環境 PR-1
12. 製品の設置及びメンテナンスを容易にする	12-3. ユーザ及び管理者によって製品の構成設定を変更できる機能を実装しなければならない。		【米国NISTIR 8425】デバイスの構成 1 【IEC 62443-4-2】CR1.5 認証管理	
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。		【米国NISTIR 8425】デバイスの構成 2 【EU-CRA】ANNEX I 1.(3)(a)	【BMSec】セキュリティ設定の初期化 MT-2
12. 製品の設置及びメンテナンスを容易にする	12-5. ハードウェア、ソフトウェア、またはファームウェア等のコンポーネントに対し、構成設定を適用できる機能を実装しなければならない。		【米国NISTIR 8425】デバイスの構成 3 【IEC 62443-4-2】CR1.5 認証管理	
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。		【ETSI EN 303 645】5.13-1 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.(3)(e) 【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 入力検証	【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
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。		【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	
14. 個人データを適切に処理する	14-2. 個人データが消費者の同意に基づいて処理される場合、この同意は妥当な方法で取得されなければならない。		【ETSI EN 303 645】6.2 M C (7) 【シンガポールCLS】[＊＊]6.2	
14. 個人データを適切に処理する	14-3. 個人データの取得に同意した消費者は、いつでもそれを撤回できなければならない。		【ETSI EN 303 645】6.3 M 【シンガポールCLS】[＊＊]6.3	
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。		【ETSI EN 303 645】6.4 R C (6) 【EU-CRA】ANNEX I 1.(3)(e)	
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。		【ETSI EN 303 645】6.5 M C (6) 【米国NISTIR 8425】教育及び意識向上 1-a 【シンガポールCLS】[＊＊]6.5	
15. 製品を識別可能にする	15-1. ユーザ及び管理者よって、製品が一意に識別可能でなくてはならない。		【米国NISTIR 8425】機器の識別 1 【EU-CRA】ANNEX II 3 【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と認証	【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
15. 製品を識別可能にする	15-2. インベントリ管理メカニズムを製品に実装し、接続された製品のコンポーネントを管理する機能を実装しなければならない。		【米国NISTIR 8425】機器の識別 2 【IEC 62443-4-2】CR7.8 制御システム・コンポーネントのインベントリ	
16. 脅威を特定しテストする	16-1. 製品の機能に対して脅威分析を行い、製品を開発しなければならない。		【IEC 62443-4-1】SR-2 脅威モデル、SI-1 セキュリティ実装のレビュー	
16. 脅威を特定しテストする	16-2. 脅威分析結果に基づいて、複数のセキュリティ機能を実装しなければならない。		【IEC 62443-4-1】SD-2 深層防御	

セキュリティ要件（Security Requirement）		☆1セキュリティ要件の該当有無	【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			
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。		【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	
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。		【EU-CRA】Article 10 7、Article 10 8、Article 10 13、Article 20 2、Article 23 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
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。	✓	【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。	✓	【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	17-4. アップデートメカニズムが実装されている場合、ソフトウェアアップデートの適用により、製品の基本的な機能が阻害される場合には、製品からユーザに通知しなければならない。		【ETSI EN 303 645】5.3-12 R C (12) 【米国NISTIR 8425】情報発信 1 【EU-CRA】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、SUM-3 依存コンポーネント・OTのセキュリティ更新文書	【特定用途機器PP】FMT_SMF（管理機能の特定）
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。	✓	【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	17-6. 製造業者は、設計・製造・評価結果等の製品に関する情報を、指定された方法でユーザに提供しなければならない。		【米国NISTIR 8425】ドキュメンテーション 1-b 【EU-CRA】Article 10 3、Article 10 11、Article 24 1、Article 24 2、Article 24 3、Article 24 4、ANNEX V 5 【IEC 62443-4-1】SG-1 深層防御	
17. 製品に関する情報提供を行う	17-7. 製造業者は、製品の保守方法に関する情報を、指定された方法でユーザに提供しなければならない。		【米国NISTIR 8425】教育及び意識向上 1-b 【IEC 62443-4-1】SG-5 安全運用ガイドライン、SG-3 セキュリティ強化のガイドライン、SG-6 アカウント管理ガイドライン	【特定用途機器PP】FAU_SAR（監査レビュー）
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。	✓	【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	17-9. 製造業者は、業務停止に至る事態が発生する場合に、業務停止前に、当該情報を指定された方法でユーザに提供しなければならない。		【EU-CRA】Article 10 14	
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。	✓	【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
17. 製品に関する情報提供を行う	17-11. 製造業者は、製品に実装されたセキュリティ機能のテスト方法に関するガイダンスを、指定された方法でユーザに提供しなければならない。		【IEC 62443-4-2】CR3.3 セキュリティ機能の検証	
18. 文書化する	18-1. 製造業者は、セキュリティ要件を満たすために用いた手段に関するデータを文書化しなければならない。		【EU-CRA】Article 20 1、Article 23 1 【シンガポールCLS】[＊＊＊]CK-LP-01 【IEC 62443-4-1】SM-1 開発プロセス、SM-12 プロセス検証、SR-3 製品セキュリティ要件、SR-4 製品セキュリティ要件の内容、SG-2 環境に期待される深層防御対策 【IEC 62443-4-2】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】2-2製品に関する文書管理【必須】①
18. 文書化する	18-2. 製造業者は、作成した文書について、指定された期間内に継続的に更新しなければならない。		【EU-CRA】Article 23 2 【IEC 62443-4-1】SM-13 継続的改善、SR-5 セキュリティ要件の見直し、SG-7 書類審査	【CCDSサーティフィケーションプログラム】2-2製品に関する文書管理【必須】①
18. 文書化する	18-3. 製造業者は、製品に関する追加情報（利用目的や基本要件の遵守に影響を及ぼすソフトウェアのバージョン、製品の外観の写真、評価結果等の情報等）を文書化しなければならない。		【米国NISTIR 8425】ドキュメンテーション 1-d、情報発信 2 【EU-CRA】Article 20 3、Article 23 3、ANNEX IV 1、ANNEX IV 2、ANNEX IV 3、ANNEX IV 4、ANNEX IV 7、ANNEX IV 8、ANNEX V 1、ANNEX V 3、ANNEX V 6 【IEC 62443-4-1】SUM-3 依存コンポーネント・OTのセキュリティ更新文書	
18. 文書化する	18-4. 製造業者は、製品の設計、開発、生産及び脆弱性対応プロセスに関する情報を文書化しなければならない。		【米国NISTIR 8425】ドキュメンテーション 1-d, 1-e, 1-f、情報発信 2 【EU-CRA】ANNEX V 2、ANNEX V 7 【シンガポールCLS】[＊＊＊]CK-LP-02 【IEC 62443-4-1】SM-1 開発プロセス、SD-1 安全設計の原則、SD-4 安全設計のベストプラクティス	【CCDSサーティフィケーションプログラム】2-2製品に関する文書管理【必須】①
18. 文書化する	18-5. 製品に適用されない、又は実行されないと見なされる本文書の各推奨事項について、理由が記録されなければならない。		【ETSI EN 303 645】4.1 【米国NISTIR 8425】ドキュメンテーション 1-c 【EU-CRA】ANNEX V 4 【IEC 62443-4-1】SM-3 適用可能性の特定、SM-5 プロセススコーピング、SI-1 セキュリティ実装のレビュー 【IEC 62443-4-2】CR2.12 否認防止	【CCDSサーティフィケーションプログラム】2-2製品に関する文書管理【必須】①
18. 文書化する	18-6. 製造業者は、開発者が発見した、または第三者から提供された製品に関するセキュリティ情報を文書化し、リスク評価を更新しなければならない。		【EU-CRA】Article 10 5 【シンガポールCLS】[＊＊＊]CK-LP-08	
18. 文書化する	18-7. 製造業者は、製品が準拠すべき法律及び規制を文書化しなければならない。また、製品の寿命、運用コスト及びサポート期間を文書化しなければならない。		【米国NISTIR 8425】ドキュメンテーション 1-a 【EU-CRA】ANNEX IV 5、ANNEX IV 6 【IEC 62443-4-1】SUM-1 セキュリティ・アップデート資格	【CCDSサーティフィケーションプログラム】2-2製品に関する文書管理【必須】①
18. 文書化する	18-8. 製造業者は、製品の保守者に求められる要件及び考慮事項を文書化しなければならない。		【米国NISTIR 8425】ドキュメンテーション 1-e 【IEC 62443-4-1】SVV-5 テスターの独立性	
18. 文書化する	18-9. 製造業者は、製品のライフサイクルにおける組織的な役割と責任者を特定するプロセスを採用しなければならない。		【EU-CRA】Article 20 4 【IEC 62443-4-1】SM-2 責任の特定	
18. 文書化する	18-10. 製造業者は、セキュリティ専門知識を獲得することを目的とした研修を従業員に実施しなければならない。		【IEC 62443-4-1】SM-4 セキュリティの専門知識	