JST-CR-01-01-2024R1

セキュリティ要件適合評価及びラベリング制度（JC-STAR）★1 レベル適合基準・評価手法

令和６年１２月

独立行政法人情報処理推進機構

目次

1. はじめに

セキュリティ要件適合評価及びラベリング制度(JC-STAR: Labeling scheme based on Japan Cyber-Security Technical Assessment Requirements)は、ETSI EN 303 645 や NISTIR 8425 等とも調和しつつ、独自に定める適合基準（セキュリティ技術要件）に基づき、IoT 製品等に対する適合基準への適合性を確認・可視化する日本の制度である。制度詳細については以下を参照のこと。

制度詳細：https://www.ipa.go.jp/security/jc-star/index.html

JC-STAR では、求められるセキュリティ水準に応じたセキュリティ技術要件として、最低限の脅威に対応するための製品共通の適合基準・評価手順（★1）と IoT 製品類型ごとの特徴に応じた適合基準・評価手順（★2～★4）という 4 段階の要件レベルが設定されている。

本資料は、『**★1 の適合基準について**』について記載したものである。

表 1　JC-STAR での要件レベルの位置づけ

<table>
<tr><th>レベル</th><th>位置付け</th><th>適合基準</th><th>評価方式</th></tr>
<tr><td>★4</td><td rowspan="2">政府機関等や重要インフラ事業者、地方公共団体、大企業の重要なシステムでの利用を想定した製品類型ごとの汎用的なセキュリティ要件を定め、それを満たすことを独立した第三者が評価して示すもの</td><td rowspan="3">製品類型別</td><td rowspan="2">第三者認証</td></tr>
<tr><td>★3</td></tr>
<tr><td>★2</td><td>製品類型ごとの特徴を考慮し、★1 に追加すべき基本的なセキュリティ要件を定め、それを満たすことを製品ベンダーが自ら宣言するもの</td><td rowspan="2">自己適合宣言</td></tr>
<tr><td>★1</td><td>製品として共通して求められる最低限のセキュリティ要件を定め、それを満たすことを製品ベンダーが自ら宣言するもの</td><td>製品類型共通</td></tr>
</table>

1.1　適合ラベルとは

適合ラベルとは、定められた適合基準や評価ガイドに従い、その適合基準が想定する脅威に対抗するために IoT 製品のセキュリティ機能として**最低限満たしてほしい水準を達していることを示すもの**である。IoT 製品が適合ラベル取得済みであることを訴求するために、IoT 製品ベンダーは、製品本体、パッケージ、取扱説明書、マニュアル、パンフレット、ホームページ等に、適合ラベルを記載・添付・使用することができ、これにより、セキュリティ対策の取組を調達者・購入者にアピールすることができるようになる。

図 1　★1 の適合ラベル

なお、適合ラベルの取得・維持に際して以下の点に留意すること。

- 定められた適合基準に適合していることを示すものであって、完全・完璧なセキュリティが確保されていることを保証するものではない。
- ★1、★2 は、IoT 製品ベンダーが本制度で定められた適合基準・評価手順により自己評価を行った結果を記載したチェックリストに基づき、IPA が適合ラベルを付与する自己適合宣言方式である。適合ラベル交付時に定められた適合基準に適合しているかを IPA は確認しない。つまり、評価の信頼性はベンダーの信頼性に依存することになる。
- ★3、★4 は、政府機関等や重要インフラ事業者等向け製品を想定し、独立した第三者評価機関による評価報告書に基づき、IPA が認証・適合ラベルを付与することでより高い信頼性を確保する。
- 証跡の保管義務を、IoT 製品ベンダーに課す。

一方、ラベル付与製品に対して、適合基準への適合に疑義が生じた場合に、IPA は事後的に**検査やサーベイランス**を行える権利を有し、必要に応じて、証跡提出や適合評価の再実施と報告を要求する。そして、サーベイランスの結果次第では、適合ラベルの取り消しもあり得る仕組みを入れることで信頼性のバランスをとっている。

適合ラベルには、IoT 製品が取得した適合ラベルのレベルと登録番号のほか、その IoT 製品情報を確認するため、IPA が管理する「（ラベル付与製品ごとの）適合ラベル取得 IoT 製品情報ページの URL を埋め込んだ**二次元バーコード**が組み込まれる。製品情報ページでは、適合ラベルが付与された IoT 製品に対して、申請者情報、製品情報、適合ラベル情報、セキュリティ情報（アップデート情報や脆弱性情報等）、問合せ先情報など、多岐に渡る情報を最新に維持しながら一次元的に提供できる仕組みを取り入れている。

表 2　適合ラベル情報でのステータス表示

適合ラベルのステータス	概要
有効（Active）	適合ラベルが有効期間内にあり、失効又は取消しに該当する事由がない状態。

失効猶予（延長申請中（Extension procedure in progress））	適合ラベルの有効期間が満了しているが、有効期間の延長申請手続きが行われている状態。
失効（有効期限切れ（Expired））	適合ラベルの有効期間が満了した後、有効期間の延長が行われていない状態。
失効（自主取下げ（Withdrawn））	適合ラベルの有効期間内に、IoT 製品ベンダーからの申し出により、適合ラベルの効力を失効させた状態。
取消し（Revoked）	適合ラベルの有効期間内に、適合ラベルの取消し事由に該当する事象が発生し、定められた期間内にその事由を解消するための是正がなされなかった場合に、IPA が強制的に適合ラベルの効力を停止させた状態。

1.2　適合ラベルが取得できる対象範囲

適合ラベルが取得できる対象範囲は、インターネットプロトコル（IP）を使用したデータの送受信機能を持つものであって、以下の条件を満たす**「IoT 製品」**である。IP が使用できるものであれば、インターネットに直接接続できないものであっても、別の機器に接続してインターネットにつなぐことができる場合には対象となる。一方、現時点では「システム」は対象外である。

- 「IoT 製品」とは、供給者により販売又は利用者による購入の単位となるものであって、意図した目的を達成するための単独の**「IoT 機器」**、又は**「IoT 機器」と「必須付随サービス」とで構成**される一式を指す。

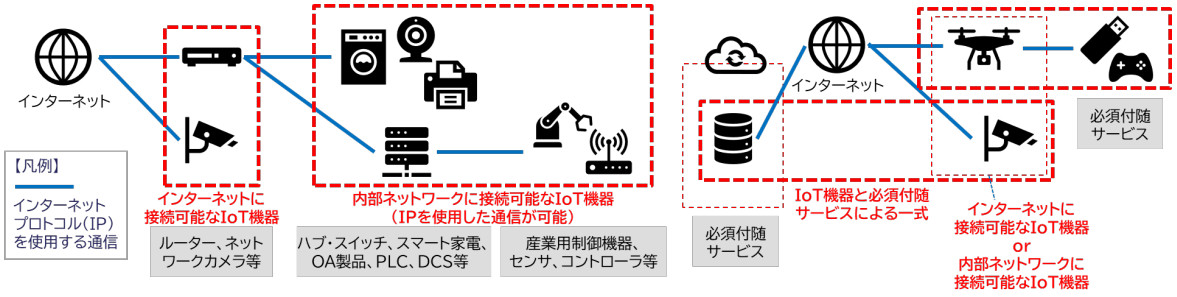

図 2　適合ラベルの対象範囲

- 「IoT 機器」とは、インターネットプロトコル（IP）を使用したデータの送受信機能を持つ、インターネットに接続可能な機器であって、利用者自身によって、当該 IoT 機器本体に対してソフトウェア製品のインストール等により容易にセキュリティ対策を追加することが困難であるものを指す。
- 「必須付随サービス」とは、IoT 製品が意図した目的を提供するために、IoT 機器と一体で提供することが必須となるデジタルサービスを指す。当該 IoT 機器本体だけでは、当該 IoT 製品が意図した目的を提供できない場合に、当該 IoT 機器に付随して提供される。

- 「内部ネットワーク」とは、GW や FW 等によりインターネットから区切られたネットワークを指す。

1.3 ★1 の自己適合宣言に基づく適合ラベル付与の流れ

申請を行う適合ラベルのレベルの違いにより、手続きが異なる。

＜手順＞

1. IoT 製品ベンダーは、適合ラベルを取得しようとする IoT 製品が求められるセキュリティ要件を満たすことを示すために、★1 についての適合基準及び評価手順に従って自ら評価を行い、チェックリストを作成する。なお、必要に応じて、外部の JC-STAR 評価機関や JC-STAR 検証事業者に評価を依頼してもかまわない。
2. IoT 製品ベンダーは、作成したチェックリストを添えて、IPA にラベル申請を行う。なお、チェックリストの提出に当たり、IPA への証跡提出は不要だが、適合ラベルの有効期間中は証跡の保管義務があることに留意されたい。
3. IPA は、経済産業省とともに必要な確認作業を行ったうえで、ラベル申請を受理する。
4. 申請が受理されたら、IoT 製品ベンダーは新規申請手数料を IPA に支払う。
5. IPA は、その IoT 製品に対する適合ラベルを付与[1]する。

1.4 ★1 の有効期間

適合ラベルの発行日から 2 年間（申請すれば 2 年以内の有効期間も設定可能）である。有効期間を延長したい場合は改めて自己適合宣言に基づく延長申請を行い、申請が認められれば 2 年間（申請すれば 2 年以内も設定可能）有効期間が延長される。なお、有効期間内に適合基準のメジャーな改訂（適合基準の項目追加や大幅な変更等）があり、その猶予期間（旧版と並存させる移行期間）が終了したとしても、途中でラベルを失効しない。

ただし、有効期間内に自己適合宣言の評価に影響を及ぼすレベルでの IoT 製品のセキュリティ仕様等の変更があった場合は、IoT 製品ベンダー自身で確認を行ったうえで IPA に報告し、その時点で適合ラベルは失効する（自主取下げ扱い）。

[1] IPA は、ラベル取得の申請に対して、ラベル発行前にサプライチェーン・リスクについて経済産業省を含めた政府関係機関に照会をかけ、その照会結果に基づきラベルを付与する。

2. 適合基準類の考え方

2.1 適合基準類の構成

★1 適合基準類は、**「★1 セキュリティ要件」「★1 適合基準」「★1 評価手順」**の 3 点より構成される。

- 「★1 セキュリティ要件」とは、★1 に想定される脅威や保護すべき情報資産等を考慮し、その脅威に対抗するために IoT 製品の★1 のセキュリティ機能として具備すべきセキュリティ要件を設定したものである。なお、★1 では、特定の製品類型に絞らず、広範な IoT 製品を対象とした、最低限の脅威に対応するための統一的な基準とする。
- 「★1 適合基準」とは、★1 セキュリティ要件に準拠するために IoT 製品が適合すべき基準として設定されるものである。対象となるセキュリティ要件の各項目に対して、★1 のセキュリティ機能が具備されていると認めるための最低限満たしてほしい具体的水準を示す。
- 「★1 評価手順」とは、IoT 製品に具備されたセキュリティ機能が★1 適合基準に適合しているかを評価・判断するための手順書（評価手法及び評価ガイドによって構成される）となるものである。評価者は、この評価手順に従って評価を行う必要がある。

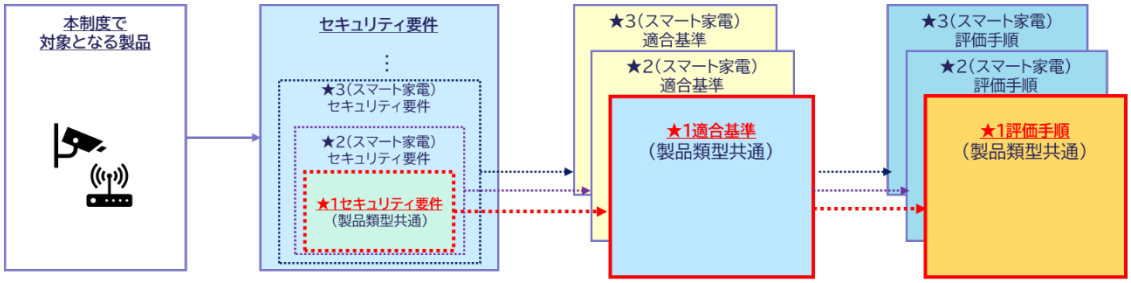

図 3 ★1 適合基準類の構成

セキュリティ要件（全体集合）は、将来的な相互承認の実現を見据え、ETSI EN 303 645、NISTIR 8425、EU-CRA 等の国内外のセキュリティ要件の集合関係を踏まえ、重ね合わせの関係（∪）にある要件を、本制度で対象となる IoT 製品において求められうるセキュリティ要件の全体集合（ロングリスト）として整理したものである。

2.2 ★1 の位置付け

★1 では、以下の 3 点を最低限実現することが求められる。

- ★1 の適合基準への適合により、**最低限の脅威に対抗**できる。
  - 特定の製品類型に絞らず、広範な IoT 製品を対象とした、最低限の脅威に対応するための統一的な基準とする。
- ★1 の適合基準への**評価は、低コストかつ自己適合宣言で対応**できる。

- IoT 製品ベンダー自身による自己適合宣言を許容する。
- 検証や評価を行う担当者が、チェックリストや評価ガイドを見て低コストで自己評価可能なレベルとする。
- 適合性評価チェックリストの申請に基づきラベルを付与する（IPA はチェックリストの内容確認は実施しない）

● ★1 の適合基準は、**海外制度と国際連携可能な基準**とする。

- シンガポール CLS 要件や英国 PSTI 法など、海外制度と国際連携可能な要件とする。

上記の★1 の位置付け（前提）を踏まえ、★1 におけるセキュリティ要件を、★1 で主に守るべき資産、アタックサーフェスから★1 で考慮すべき主な脅威を整理した上で、当該脅威に対して★1 で実現すべき対策を実現するためのセキュリティ要件としてロングリストより抽出した。

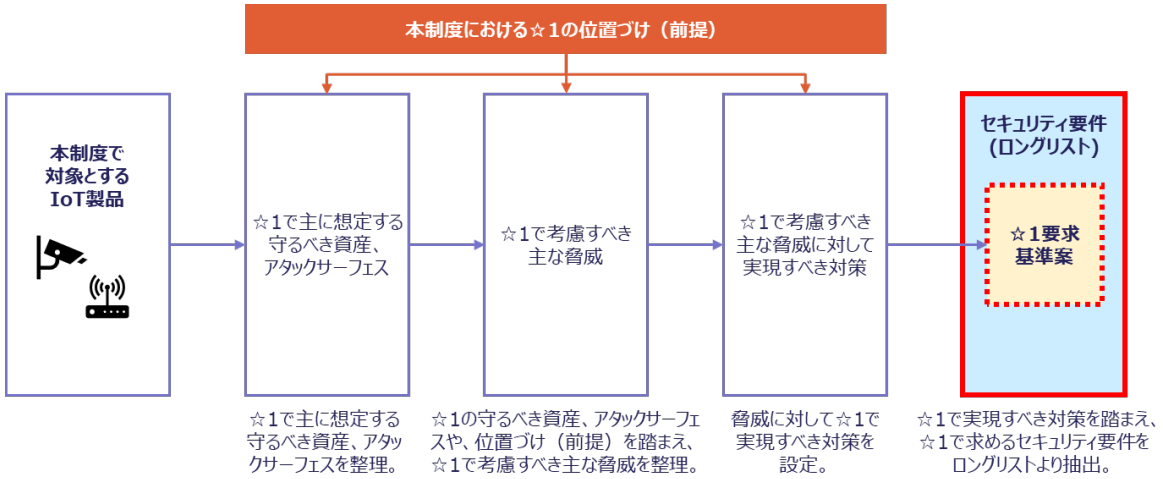

図 4　★1 セキュリティ要件の抽出プロセスのイメージ

IoT 製品において情報に関する守るべき資産（下表の 4 つの資産を考慮）について、★1 で守るべき資産として以下を対象とする。

表 3　★1 で対象とする守るべき資産一覧

IoT 製品において守るべき資産	★1 で想定する守るべき資産	★2 以上で想定する守るべき資産
1．IoT 機能 機器やシステムが IoT につながるための機能	● **有線通信機能** ● **無線通信機能**	• 有線通信機能 • 無線通信機能
2．本来情報 「モノ」本来の機能、セキュリティ対策・セーフティ対策のための機能	● **セキュリティ機能**	• セキュリティ機能 • 製品本来の機能 • セーフティ関連機能
3．情報 ユーザの個人情報、収集情報、各機能の設定情報など	● **IoT 機能（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、個人情報の一般的に機密性が高い情報**	• 設定情報 • 個人情報 • 収集情報 • 接続先機器に関する情報 等
4．その他の物理的資産	-	• 人的資産 • 物理的資産

★1 が対象とするアタックサーフェスとしては、(1) 通常使用 I/F、(2) 保守用 I/F、(3) 未使用 I/F、(4) 潜在的攻撃点、(5) 製品廃棄時の物理的接触の 5 つである。なお、★1 で対抗する脅威のレベルを踏まえ、「製品運用時の物理的接触」や「製品開発・調達等のサプライチェーンにおける接触」のアタックサーフェスは想定しない。

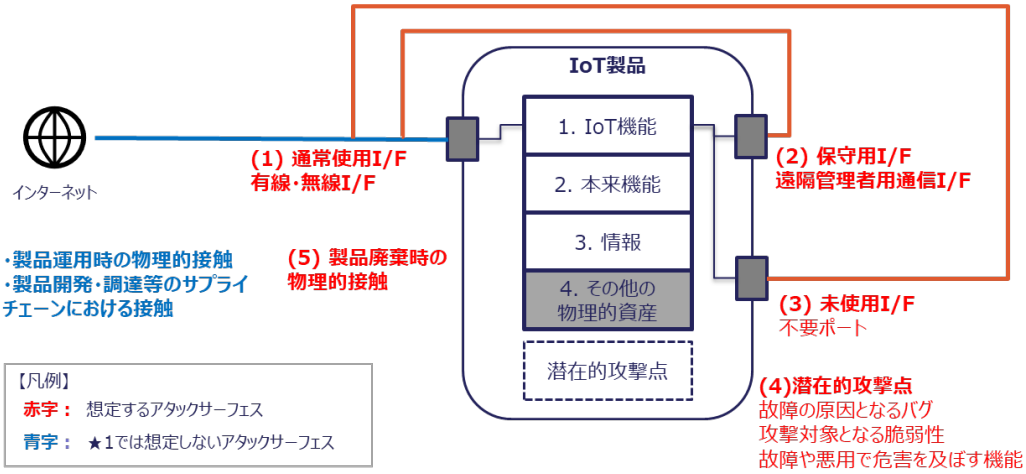

図 5　★1 で対象とするアタックサーフェス

★1 で対象とする守るべき資産及びアタックサーフェスを踏まえ、★1 における IoT 製品に対する脅威として以下のものを対象とする。

なお、「製品運用時の物理的接触」と「製品開発・調達時のサプライチェーンにおける接触」のアタックサーフェスは対象としないため、「物理的不正操作（運用時）」や「物理的破壊・窃盗（運用時）」「不正改造」の脅威は対象外とする。また、STRIDE モデルでは「否認」が一つの脅威として挙げられているが、★1 で対象とする守るべき資産に「否認」の影響を受ける資産はないため、当該脅威は対象外としている。

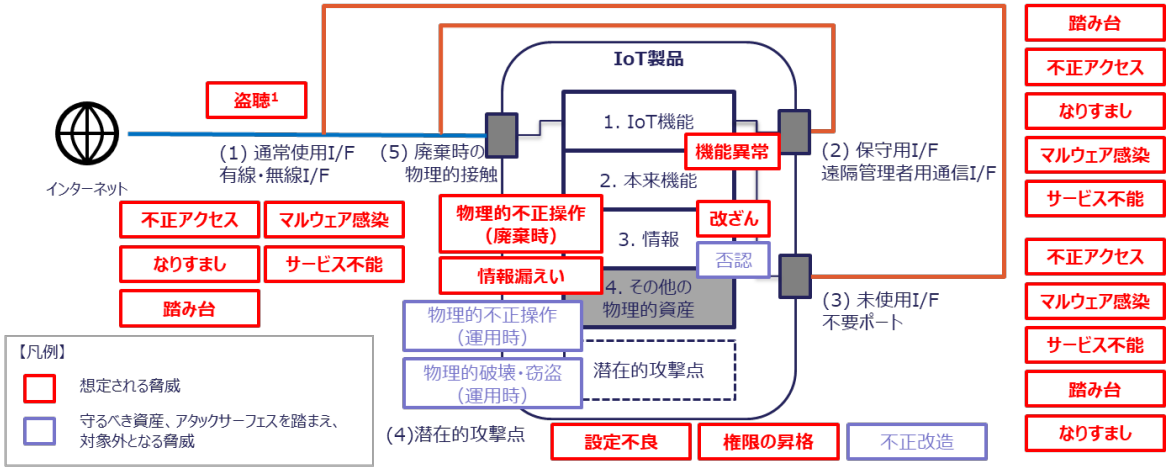

図 6　★1 で対象とする脅威

★1 で対象とすべき脅威に対し、★1 の位置付けや海外制度の基準等を踏まえ、IoT 製品/IoT 製品ベンダーにおいて実現すべき対策を以下の通り選定した。

表 4　脅威に対抗するために★1 で実現すべき対策一覧

★1 で考慮すべき主な脅威			脅威に対抗するために★1 で実現すべき対策			
			IoT 製品における対策		IoT 製品ベンダーにおける対策	
			カテゴリ	対策	カテゴリ	対策
1.	①弱い認証機能により、	外部からの不正アクセスの対象となり、マルウェア感染や踏み	識別・認証、アクセス制御	• 容易に推測できるパスワードが設定できない仕組みを導入する • セキュアな認証の仕組みを提供する • ブルートフォースによる認証試行を防ぐ仕組みを提供する	情報提供	• セキュアな利用方法に関する情報を提供する

	②脆弱性の放置により、	台となる攻撃等を受けることで、情報漏えい、改ざん、機能異常の発生につながる脅威	脆弱性対策、ソフトウェアの更新	• 深刻度の高い既知の脆弱性及び主要な CWE に対する対策を行う • ソフトウェアコンポーネントがアップデート可能な仕組みを導入する	情報・問い合わせの受付、情報提供	• 製品に関する情報及び脆弱性に関する情報を提供する • セキュリティパッチの適用方法に関する情報を提供する
	③未使用インタフェースの有効化により、		インタフェースへの論理アクセス	• 不要なインタフェースを無効化する	–	–
			データ保護	• 機器が保有する守るべき情報を保護するための機能を提供する（①～③の脅威に共通する対策）	–	–
2. 機器の通信が盗聴され、守るべき情報が漏えいする脅威			データ保護	• インターネット経由で伝送される守るべき情報を保護するために情報の漏えいや変更に対する保護対策を実装する	–	–
3. 廃棄・転売等された機器から、守るべき情報が漏えいする脅威			データ保護	• 機器の利用中に機器内に保存された守るべき情報を製品本体や関連サービスを介して削除できる機能を提供する • 機器に当初から搭載されている守るべき情報を保護するための機能を提供する	情報提供	• セキュアな廃棄方法に関する情報を提供する
4. ネットワーク切断や停電等の事象が発生した際に、セキュリティ機能に異常が発生する脅威			レジリエンスの向上	• ネットワーク切断や停電等の事象が発生し、復旧した場合でも、認証情報やソフトウェア設定は初期状態に戻らず、電源 OFF 前の状態を提供する	–	–

3. ★1 の適合基準

【セキュリティ要件カテゴリ】
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
【セキュリティ要件】
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。

【セキュリティ要件カテゴリ】
5. セキュアに通信する
【セキュリティ要件】
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。

【★1 適合基準 S1.1-01】

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。

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 IoT 製品（技適[T]マーク又は[A]マークが付与された IoT 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。）

対象外（NA）となるための条件、基準の補足説明
【対象外（NA）となるための条件】
IP 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（「対象外（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

- 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

★1 評価手法

- ドキュメント評価：対象とする
  IoT 製品の技術文書において、他の IoT 機器又はユーザからの守るべき情報資産へのアクセスに対する適切な認証に基づくアクセス制御の方法が明示されていることを評価する。
- 実機テスト：なし

なお、評価方法の詳細については『★1 評価ガイド』を参照すること。

【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

【ETSI EN 303 645】5.1-3 M, 5.5-5 M
【英国 PSTI Act】SCHEDULE 1: 1-(3)
【米国 NISTIR 8425】インタフェースの論理アクセス 2-b
【EU-CRA】ANNEX I 1.(3)(b)
【シンガポール CLS】[＊]5.1-3, [＊＊]5.5-5
【IEC 62443-4-2】CR1.5、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

【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

【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、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】FIA_UAU（認証のタイミング）、FMT_SMR（セキュリティの役割）、FAU_UID（アクション前の利用者識別）

【セキュリティ要件】
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。
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。

【★1 適合基準 S1.1-02】

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、又は、IoT 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 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。

対象外（NA）となるための条件、基準の補足説明

【対象外（NA）となるための条件】

ネットワークを介したパスワードを利用したユーザ認証の仕組みがない（「対象外（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を利用したユーザ認証が必要ない根拠を記載すること）

★1 評価手法

- ドキュメント評価：対象とする
  IoT 製品の技術文書において、ネットワークを介したユーザ認証の仕組みにて、パスワード利用した IoT 製品導入時にデフォルトパスワードに関する対策が明示されていることを評価する。
- 実機テスト：なし

なお、評価方法の詳細については『★1 評価ガイド』を参照すること。

【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

【ETSI EN 303 645】5.1-1 MC (1), 5.1-2 MC (2)
【英国 PSTI Act】SCHEDULE 1: 1-(2), 1-(3)
【米国 NISTIR 8425】インタフェー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, CR1.7

【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

【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）

【セキュリティ要件】
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。

【★1 適合基準 S1.1-03】

IoT 製品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。

対象外（NA）となるための条件、基準の補足説明
【対象外（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（「対象外（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】
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。）

★1 評価手法

- ドキュメント評価：対象とする
  IoT 製品の技術文書において、IoT 製品に対するユーザ認証にて使用される認証値の変更に関する記載があることを評価する。
- 実機テスト：なし

なお、評価方法の詳細については『★1 評価ガイド』を参照すること。

【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
【ETSI EN 303 645】5.1-4 MC (8)
【シンガポール CLS】[＊]5.1-4
【IEC 62443-4-2】CR1.5

【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
【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）

【セキュリティ要件】
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。

【★1 適合基準 S1.1-04】

IoT 機器が、制約のある機器ではない場合、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。

対象外（NA）となるための条件、基準の補足説明

【対象外（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）

- 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がない（「対象外（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）
- IoT 機器が「制約のある機器」に該当する（「対象外（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 IoT 機器の例は「用語集」を参照。）

★1 評価手法

- ドキュメント評価：なし
- 実機テスト：対象とする
  実機テストによって、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仕組みであることを評価する。

なお、評価方法の詳細については『★1 評価ガイド』を参照すること。

【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

【ETSI EN 303 645】5.1-5 MC (5)

【EU-CRA】ANNEX I 1.(3)(b)
【シンガポール CLS】[＊]5.1-5
【IEC 62443-4-2】CR1.11

【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

【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）

【セキュリティ要件カテゴリ】
2. 脆弱性の報告を管理するための手段を導入する
【セキュリティ要件】
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

【★1 適合基準 S1.1-05】

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 IoT 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及びその概要

対象外（NA）となるための条件、基準の補足説明

【対象外（NA）となるための条件】
該当事項なし

★1 評価手法

- ドキュメント評価：対象とする
  IoT 製品のウェブサイト等、ユーザがアクセス可能な媒体において、脆弱性開示ポリシーが明示されていることを評価する。
- 実機テスト：なし

なお、評価方法の詳細については『★1 評価ガイド』を参照すること。

【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

【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

【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

【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

【セキュリティ要件カテゴリ】
3. ソフトウェアを最新の状態に保つ
【セキュリティ要件】
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。
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。

【★1 適合基準 S1.1-06】

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①～③のすべての基準を満たすこと。

① IoT 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 IoT 製品（技適[T]マーク又は[A]マークが付与された IoT 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。）

対象外（NA）となるための条件、基準の補足説明

【対象外（NA）となるための条件】

該当事項なし

★1 評価手法

- ドキュメント評価：なし
- 実機テスト：対象とする
  対象 IoT 製品に含まれるソフトウェアコンポーネントに対するアップデート機能を実機テストにより評価する。

なお、評価方法の詳細については『★1 評価ガイド』を参照すること。

【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

【ETSI EN 303 645】5.3-1 R, 5.3-2 MC (5)
【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, [＊]5.3-2
【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

【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

【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）

【セキュリティ要件】

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。

【★1 適合基準 S1.1-07】

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。

対象外（NA）となるための条件、基準の補足説明

【対象外（NA）となるための条件】

該当事項なし

★1 評価手法

- ドキュメント評価：対象とする
  IoT 製品のマニュアル、ウェブサイト等、ユーザがアクセス可能な媒体において、ソフトウェアのアップデートに関する容易かつ分かりやすい手順が明示されていることを評価する。
- 実機テスト： なし

なお、評価方法の詳細については『★1 評価ガイド』を参照すること。

【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

【ETSI EN 303 645】5.3-3 MC (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

【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

【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）

【セキュリティ要件】

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。

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。

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。

【★1 適合基準 S1.1-08】

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。

対象外（NA）となるための条件、基準の補足説明

【対象外（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（「対象外（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）

★1 評価手法

- ドキュメント評価：対象とする
  IoT 製品の技術文書において、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の実装が明示されていることを評価する。
- 実機テスト： なし

なお、評価方法の詳細については『★1 評価ガイド』を参照すること。

【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

【ETSI EN 303 645】5.3-2 MC (5), 5.3-7 MC (12), 5.3-10 M (11,12)
【EU-CRA】ANNEX I 1.(3)(e)
【米国 NISTIR 8425】ソフトウェアの更新 1
【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 暗号の使用

【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

【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】①②
【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）

【セキュリティ要件】

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。

【★1 適合基準 S1.1-09】

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。

対象外（NA）となるための条件、基準の補足説明

【対象外（NA）となるための条件】

該当事項なし

★1 評価手法

- ドキュメント評価：対象とする
  組織の規程類、方針、手順書等又は IoT 製品の技術文書において、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が明示されていることを評価する。
- 実機テスト： なし

なお、評価方法の詳細については『★1 評価ガイド』を参照すること。

【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

【ETSI EN 303 645】5.3-8 MC (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

【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

【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）

【セキュリティ要件】

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。

【★1 適合基準 S1.1-10】

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。

① IoT 製品本体に、IoT 製品の型番を直接記載すること。

② IoT 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、ユーザが型番を認識できるようにすること。

対象外（NA）となるための条件、基準の補足説明

【対象外（NA）となるための条件】

該当事項なし

★1 評価手法

- ドキュメント評価：なし
- 実機テスト： 対象とする
  IoT 製品の型番について、ユーザ確認出来る方法が、ユーザに提供されていることを評価する。

なお、評価方法の詳細については『★1 評価ガイド』を参照すること。

【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

【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

【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

該当事項なし

【セキュリティ要件カテゴリ】

4. 機密セキュリティパラメータをセキュアに保存する

【セキュリティ要件】

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。

【★1 適合基準 S1.1-11】

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。

対象外（NA）となるための条件、基準の補足説明

【対象外（NA）となるための条件】

該当事項なし

【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
- 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

★1 評価手法

- ドキュメント評価：対象とする
  IoT 製品の技術文書において、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。）が、セキュアに保存されていることを評価する。
- 実機テスト：なし

なお、評価方法の詳細については『★1 評価ガイド』を参照すること。

【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

【ETSI EN 303 645】5.4-1 M
【米国 NISTIR 8425】データ保護 1、インタフェー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

【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

【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）

【セキュリティ要件カテゴリ】
5. セキュアに通信する
【セキュリティ要件】
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。
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。

【★1 適合基準 S1.1-12】

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 IoT 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。

対象外（NA）となるための条件、基準の補足説明

【対象外（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（「対象外（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
- 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

★1 評価手法

- ドキュメント評価：対象とする
  IoT 製品の技術文書において、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保護対策が実装されていることを評価する。IoT 製品と連動するアプリがある場合、守るべき情報資産として、アプリから送信される情報も対象とした評価を行う。
- 実機テスト：なし

なお、評価方法の詳細については『★1 評価ガイド』を参照すること。

【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

【ETSI EN 303 645】5.5-1 M, 5.5-7 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, 5.5-7
【IEC 62443-4-2】CR3.1 通信の完全性、CR4.3 暗号の使用

【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

【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

【セキュリティ要件カテゴリ】
6. 露出した攻撃面を最小化する
【セキュリティ要件】
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。

【★1 適合基準 S1.1-13】

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。

① IoT 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

② IoT 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。

対象外（NA）となるための条件、基準の補足説明

【対象外（NA）となるための条件】
該当事項なし

★1 評価手法

- ドキュメント評価：対象とする
  IoT 製品の技術文書において、IoT 製品で利用するすべてのインタフェースが洗い出されており、利用目的等が明確化されていること及び IoT 製品の利用上不要なものが、含まれていないことを確認し、評価する。また、攻撃に悪用されるリスクの特に高いポートの利用時は、攻撃状況を把握し、必要に応じて適切な対処ができる管理プロセスを有していることが技術文書に明示されていることを評価する。
- 実機テスト：対象とする

ポートスキャン及び脆弱性スキャンツールを利用した実機テストにより、IoT 製品の利用上不要なインタフェースが無効化されていること、及び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を評価する。

※ 原則ドキュメント評価と実機テストの双方を実施すること。ただし、実機テストに関しては、推奨のポートスキャンツール及び脆弱性検査ツールが無い場合は、対象外（ドキュメント評価のみ）とする。

なお、評価方法の詳細については『★1 評価ガイド』を参照すること。

【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

【ETSI EN 303 645】5.6-1 M
【米国 NISTIR 8425】インタフェー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

【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

【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

【セキュリティ要件カテゴリ】
9. 停止に対してレジリエントなシステムにする
【セキュリティ要件】
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。

【★1 適合基準 S1.1-14】

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、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。

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 IoT 製品（技適[T]マーク又は[A]マークが付与された IoT 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。）

対象外（NA）となるための条件、基準の補足説明

【対象外（NA）となるための条件】

該当事項なし

★1 評価手法

- ドキュメント評価：なし
- 実機テスト：対象とする
  工場出荷時からアクセス制御の際に使用する認証値の変更を行い、かつ、ソフトウェアのアップデートを行った IoT 製品に対して、実機テストにより評価する。

なお、評価方法の詳細については『★1 評価ガイド』を参照すること。

【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

【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

【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

【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

【セキュリティ要件カテゴリ】

11. ユーザが簡単にデータを消去できるようにする

【セキュリティ要件】

11-1. 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ユーザに提供しなければならない。

【★1 適合基準 S1.1-15】

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

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。

対象外（NA）となるための条件、基準の補足説明

【対象外（NA）となるための条件】

該当事項なし

★1 評価手法

- ドキュメント評価：対象とする
  IoT 製品の技術文書において、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、ユーザに関する情報を消去できる機能を有することを評価する。
- 実機テスト：対象とする
  実機テストにより、ユーザに提示された手順によるデータ削除機能の動作及びデータ削除後にファームウェア（ソフトウェア）のバージョンが維持されていることを評価する。

なお、評価方法の詳細については『★1 評価ガイド』を参照すること。

【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

【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

【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

【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）

【セキュリティ要件カテゴリ】

17. 製品に関する情報提供を行う

【セキュリティ要件】

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。

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。
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。
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。
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。

【★1 適合基準 S1.1-16】

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。
② IoT 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。
⑤ IoT 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。

対象外（NA）となるための条件、基準の補足説明

【対象外（NA）となるための条件】

該当事項なし

【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
- 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

★1 評価手法

- ドキュメント評価：対象とする
  IoT 製品のマニュアル、ウェブサイト等、ユーザがアクセス可能な媒体において、IoT 製品のサイバーセキュリティに関する情報提供が行われていることを評価する。

- 実機テスト：なし

なお、評価方法の詳細については『★1 評価ガイド』を参照すること。

【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

【ETSI EN 303 645】5.12-2 R, 5.3-11 RC (12), 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 1-b, 1-c, 1-d, 1-e, 2

【EU-CRA】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

【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、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

【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

【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、ファームウェアアップデート機能　PT-1、運用環境 PR-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_SMT（高信頼性タイムスタンプ）

Appendix. A 用語集

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、必須付随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 機器とその必須付随サービス。
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。
必須付随サービス	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： 必須付随サービスには、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。このサービスは必須付随サービスである。
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１： 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必須付随サービスのプロバイダなどがある。 注２：この定義は、「IoT 製品に対するセキュリティ適合性評価制度構築方針」における「IoT 製品ベンダー」に相当する。

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。

Appendix. B 修正履歴

2024.12.05　第 1.1 版（2024R1）公開

- ★1 適合基準 S1.1-01 に統合されたセキュリティ要件を追記。さらに「【参考】海外既存制度・文書」及び「【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」についても追記。
- ★1 適合基準 S1.1-01 の「★1 評価手法」における不明確な「以下の仕組み」部分を「適切な認証に基づくアクセス制御の方法」として表現を明確化。
- ★1 適合基準 S1.1-02 に統合されたセキュリティ要件を追記。さらに「【参考】海外既存制度・文書」及び「【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」についても追記。
- ★1 適合基準 S1.1-02 の「★1 適合基準」、「対象外（NA）となるための条件」の対象明確化のため、「パスコード」の記載を削除。
- ★1 適合基準 S1.1-02 の「★1 評価手法」の対象明確化のため、「ネットワークを介したユーザ認証の仕組みにて、パスワード利用した IoT 製品」と追記。
- ★1 適合基準 S1.1-04 の「対象外（NA）となるための条件」における、「★1 適合基準」との整合のため、「ユーザアクセス」を「ユーザ認証」に修正。
- ★1 適合基準 S1.1-06 に統合されたセキュリティ要件を追記。さらに「【参考】海外既存制度・文書」及び「【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」についても追記。
- ★1 適合基準 S1.1-06 の「★1 評価手法」が未記載であったため、評価手法を追記。
- ★1 適合基準 S1.1-08 に統合されたセキュリティ要件を追記。さらに「【参考】海外既存制度・文書」及び「【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」についても追記。
- ★1 適合基準 S1.1-10 の「★1 評価手法」が未記載であったため、評価手法を追記。
- ★1 適合基準 S1.1-11 の「対象外（NA）となるための条件」の該当有無が未記載であったため、「該当事項なし」であることを明記。
- ★1 適合基準 S1.1-11 の「★1 評価手法」において、「★1 適合基準」との整合のため、「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。）」に記載を統一。
- ★1 適合基準 S1.1-11 の「★1 評価手法」において、守るべき情報資産に対してセキュアに保存される必要があるアタックサーフェースが「ネットワーク経由の不正アクセス」以外であることを明確化するため、「ネットワーク経由の不正アクセスに対して」を削除。
- ★1 適合基準 S1.1-12 に統合されたセキュリティ要件を追記。さらに「【参考】海外既存制度・文書」及び「【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」についても追記。
- ★1 適合基準 S1.1-12 の「★1 評価手法」に対する記載レベル統一のために表現を修正。具体的な評価方法については「★1 評価ガイド」に移動。

- ★1 適合基準 S1.1-13 の★１評価手法に対する評価内容に不足があったため、「ドキュメント評価」及び「実機テスト」の不足部分の評価内容を追記。具体的な評価方法については「★1 評価ガイド」に移動。
- ★1 適合基準 S1.1-15 のセキュリティ要件において、ユーザが実施する要件であるように受け取られる誤解を避けるため、表現を修正。
- ★1 適合基準 S1.1-15 の「★１評価手法」に対する記載レベル統一のために表現を修正。具体的な評価方法については「★1 評価ガイド」に移動。
- ★1 適合基準 S1.1-16 に統合されたセキュリティ要件を追記。さらに「【参考】海外既存制度・文書」及び「【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」についても追記。
- ★1 適合基準 S1.1-16 の「対象外（NA）となるための条件」の該当有無が未記載であったため、「該当事項なし」であることを明記。
- ★1 適合基準 S1.1-16 の「★１評価手法」に対する記載レベル統一のために表現を修正。具体的な評価方法については「★1 評価ガイド」に移動。
- 「1.1 適合ラベルとは」中の「表２　適合ラベル情報でのステータス表示」におけるステータスから「サーベイランス実施中」を削除し、「失効猶予」を追記。
- 「2.2 ★１の位置付け」中の「表４　脅威に対抗するために★1 で実現すべき対策一覧」における、「3. 廃棄・転売等された機器から、守るべき情報が漏えいする脅威」に対する「対策」を追記。
- その他、誤記修正及び用語統一を実施。

2024.09.30　第１版（2024）公開