JST-CR-03-01-2026

セキュリティ要件適合評価
及びラベリング制度(JC-STAR)
通信機器★３セキュリティ要件

令和８年２月

独立行政法人情報処理推進機構

目次

1. はじめに

1.1 JC-STAR とは

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、独自に定める適合要件(セキュリティ技術要件)に基づき、IoT 製品等に対する適合要件への適合性を確認・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要件・評価手順(★1)と IoT 製品類型ごとの特徴に応じた適合要件・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。
★3 で対象となる IoT 製品は、政府機関等や重要インフラ事業者、地方自治体、大企業に調達、設置が想定される IoT 機器を含む製品である。本文書では、「通信機器」を対象とした★3 レベルの要件について記載している。

表 1. JC-STAR での要件レベルの位置付け

<table>
<tr><th>レベル</th><th>位置づけ</th><th>適合要件</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、地方自治体、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">第三者評価</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>

1.2 適合ラベルとは

適合ラベルとは、定められた適合要件や評価ガイドに従い、その適合要件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**満たすべき水準に達している**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. ★3 の適合ラベル(サンプル)

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。
定められた適合要件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要件・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要件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の実施と、その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。
- 海外制度との相互承認を行う場合には、JC-STAR で要求する期間よりも長期間にわたってエビデンスの提出が求められる場合があるので、証跡の保管期間について留意する。

一方、ラベル付与製品に対して、適合要件への適合に疑義が生じた場合に、IPA はサーベイランスを行うことがあり、必要に応じて、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要件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)、問合せ先情報等、多岐に渡る情報を最新に維持しながら一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。もはや適合ラベルの効力がない状態
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。もはや適合ラベルの効力がない状態
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。もはや適合ラベルの効力がない状態

1.3 ★3 の適合評価・認証に基づく適合ラベル付与の流れ

JC-STAR では、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。
★3 レベルの適合評価は、IPA で認められた第三者評価機関(JC-STAR 評価機関)での実施が必須である。
適合ラベルの申請からラベル付与までの主な手順は以下の通りである。詳しくは、ホームページにて最新の手順を確認すること。

申請手続き・報告手続き
https://www.ipa.go.jp/security/jc-star/shinsei/index.html

【手順】

1. IoT 製品ベンダーは、IPA に適合ラベルの取得申請を行う。
2. IPA は、経済産業省とともに必要な確認手続を行う。確認手続の結果、申請受理可と判断されると「申請受付受理書兼申請手数料通知書」が発行される。内容に不備があ

った場合は申請差戻となり、書類の再提出が必要である。また、申請受理不可の場合は、申請は却下され、手続きは終了する。

3. IoT 製品ベンダーは「申請受付受理書兼申請手数料通知書」を受領したら、申請手数料を IPA に支払う。
   所定の申請手数料の振込が行われるまで、IPA は認証作業を開始しないことに留意すること。
4. IoT 製品ベンダーは、評価機関を「JC-STAR 評価機関」より選択し、当該評価機関へ「申請受付受理書」を示したうえで、適合評価を依頼する。
   なお、ラベル申請や評価依頼に先だって、JC-STAR 評価機関に相談することは可能である。
5. 適合評価依頼後、IoT 製品ベンダーは評価機関から「評価機関評価業務適格性チェックリスト」が発行されるので、当該チェックリストを IPA へ提出する。
   その後、IPA から「認証作業担当通知書」が送付される。
6. 評価機関は、★3(レベル 3)についての適合要件及び評価手順に従って適合評価を行い、IPA に対して評価結果を記載した「適合評価報告書」を提出する。
7. IPA は「適合評価報告書」に基づき認証作業を実施する。報告書の内容に疑義がある場合には認証レビューを発行し、追加評価を要求する。最終的に認証可と判断されたら、IPA は申請対象の IoT 製品に対する適合ラベルを付与する。
   なお、「申請受付受理書兼申請手数料通知書」の発行日から原則 12 ヶ月以内に認証作業が終了しなかった場合、認証不可となり、申請は却下される。

1.4 ★3 の有効期間

適合ラベルの有効期間は発行日から 2 年間(申請すれば 2 年以内の有効期間も設定可能)とする。

有効期間を延長したい場合は、IoT 製品ベンダーは IPA へ延長申請を行い、申請書類等について必要な確認手続が行われる。確認手続の結果、延長可と判断された場合は、適合ラベルの有効期限が 1 年間(申請すれば 1 年以内も設定可能)延長される。延長申請は最大 3 回とし、最長で初回適合ラベル発行日から合計 5 年間まで有効期間を延長することができる。

合計 5 年を超える場合は、有効期間内に改めて★3 適合ラベル付与の再認証が必要となる。

なお、有効期間内に★3 適合要件のメジャーな改訂(適合要件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)が終了しても、途中で適合ラベルの失効とはならない。

ただし、猶予期間後の有効期間の延長については、延長申請が行えず、★3 適合ラベル付与の再認証が必要となる。

有効期間内に★3 適合評価の結果に影響を及ぼすような、IoT 製品のセキュリティ機能等の変更があった場合は、評価機関での再評価が必要になる場合がある。
有効期間内にファームウェアの更新や、IoT 製品に更新、変更等があった場合は、別途、IPA のホームページを参照し、対応をすること。

1.5 ★3 適合基準類の構成

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

- **「★3 セキュリティ要件」とは、**★3 レベルの IoT 製品として、満たす必要のあるセキュリティ対策や基準等のことである。
- **「★3 適合要件」とは、**★3 セキュリティ要件に記載してある対策、基準に対して、★3 レベルの IoT 製品として具備する必要がある機能や、IoT 製品ベンダーが対応する必要のある対策など、具体的に満たす必要のある要件のことである。
- **「★3 評価ガイド」は、**★3 適合要件に対して、要求したことが満たされているか確認するための評価方法を【ドキュメント評価】と【実機評価】として記載したものである。

本文書では、「★3 セキュリティ要件」までを記載している。
実際の適合評価・認証にあたっては、本文書での「★3 セキュリティ要件」を満たしていると判断するためには「★3 適合要件」を満たしていることが求められる。
また、「★3 適合要件」を満たしているかどうかの具体的な判断は、「★3 評価ガイド」に記載の評価方法により行われる。
つまり、本文書での「★3 セキュリティ要件」だけを見て、自らの解釈で対策をとったとしても、「★3 適合要件」並びに「★3 評価ガイド」に照らし合わせた適合評価で認証されない限り、適合ラベルが取得できないことに留意されたい。

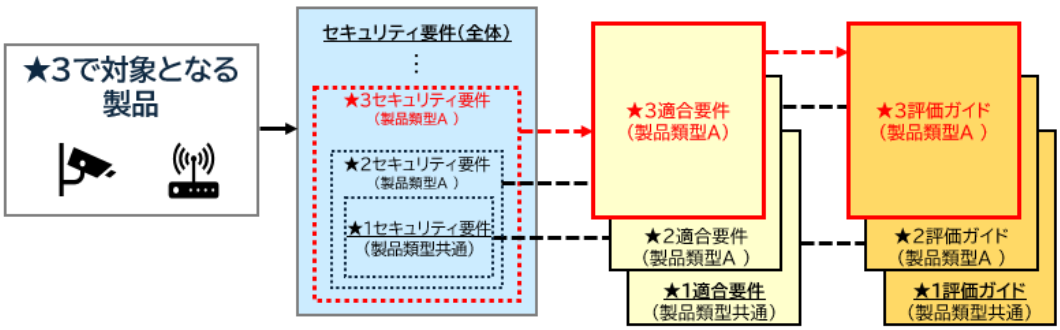


図 2. ★3 適合基準類の構成

本文書で対象となる★3 通信機器にて考慮した国内外のセキュリティ要件を以下に示す。

表 3. 国内外のセキュリティ要件

No	制度・ガイドラインの名称
1	ETSI EN 303 645 V3.1.3 (2024-09)
2	Cybersecurity Labelling Scheme (CLS) Publication No.4 Version 1.2 April 2025
3	Cyber Resilience Act(CRA)23 October 2024
4	Radio Equipment Directive(RED): 28.12.2024
5	EN 18031-1 / -2 / -3:2024
6	IEC 62443-4-1 2018
7	IEC 62443-4-2 2019
8	NIST IR 8425 September 2022
9	UK PSTI 法 Regulation 2023
10	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)の一部改定(令和 7 年 9 月)
11	CCDS IoT 機器セキュリティ要件適合基準ガイドライン 2025 年版 Ver.1.0
12	特定用途機器 共通セキュリティプロテクションプロファイル 1.0 版
13	BMSec ネットワーク機能付き事務機セキュリティガイドライン Ver.1.00
14	総務省 端末設備等規則　令和 7 年 10 月 1 日 施行

【注意】

本文書「★3 セキュリティ要件」は、「★1 レベル適合基準・評価手法」に相当する文書である。

「★3 セキュリティ要件」は、「★1 レベル適合基準・評価手法」と項目名、記載事項の位置づけを変更しているので注意されたい。

「★3 セキュリティ要件」と、「★1 レベル適合基準・評価手法」の項目名、記載事項の違いを表 4 に示す。

表 4. 「★3 セキュリティ要件」と「★1 レベル適合基準・評価手法」の項目名、記載事項

記載事項	★1 レベル適合基準・評価手法	★3 セキュリティ要件
セキュリティ要件の分類	セキュリティ要件カテゴリ	カテゴリ
セキュリティ要件の表題	セキュリティ要件	(廃止)
JC-STAR の求めるセキュリティ要件の記述	適合基準	セキュリティ要件
対象外(NA)となるための	対象外(NA)となるための条件、	対象外(NA)となるための条件、

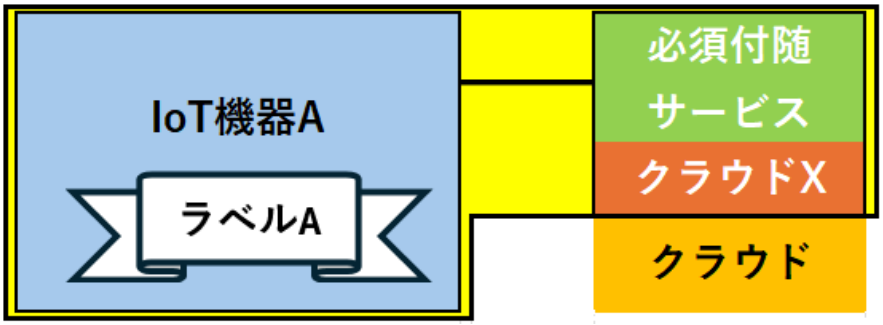
条件、基準の補足説明	基準の補足説明	基準の補足説明
評価手法の概要	評価手法	(削除、★3 評価ガイドに記載)

★1 レベル適合基準・評価手法での、「セキュリティ要件」はセキュリティ要件の表題であるにもかかわらず、要件内容とも読み取れる表記になっており、JC-STAR で求める要件と紛らわしい記載となっていた。このため、JC-STAR で求めるセキュリティ要件を明確にするため、上記のように記載項目を変更した。
また、本文書は★3 セキュリティ要件を定義するための文書であるため、「評価手法」の記載は本文書から削除し、「★3 評価ガイド」にて詳細を解説する。
★1 レベル適合基準・評価手法(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)も次回の改定時に、上記の表記内容に従って項目名を変更する予定である。

1.6 「IoT 製品」と「IoT 機器」の説明

「IoT 製品」の定義には、「IoT 機器」と「必須付随サービス」が含まれている。
「必須付随サービス」とは、対象となる「IoT 機器」が「必ずセットで利用するサービス」のことを指す。具体的には、【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サービスのことである。

- 例:IoT 機器 A で生成されたデータを特定のクラウドサービス X に保存するように設定されている場合、当該サービス X は必須付随サービスである。この場合、適合ラベルの評価対象範囲は、「IoT 機器 A」、「クラウドサービス X」及びその両者をつなぐ通信路全体となる。なお、適合ラベルは「IoT 機器 A」に対して付与される。
  「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。



クラウド X: サービスが直接的に利用するクランド領域

図 3. IoT 製品、IoT 製品の区分例

必須付随サービスの提供形態については「対抗となる IoT 機器とセットで提供」されるという条件以外の制約はない。ただし、IoT 機器からみて対向となるサービスが特定されない場合、そのサービスは必須付随サービスに該当しないので、注意すること。

2. ★3 通信機器について

2.1 ★3 適合ラベル(通信機器)の主な対象範囲

★3 適合ラベルが想定する「通信機器」とは、一般家庭向けの通信機器(ホームルータや家庭用 Wi-Fi ルータ等)ではなく、**政府機関等や重要インフラ事業者、地方自治体、大企業において主に調達・設置される、IP パケットを扱う代表機能及び管理機能等を有する通信機器**である。

例えば、以下のような場所に設置されることを想定している。

- 要管理対策区域(例:セキュリティエリア、サーバールーム等)
- 施設内の施錠管理されたラック等の内部
- 物理的セキュリティに配慮された施設内の共用エリアの区画
  (例:政府機関の執務室、関係者エリア等)
- 施設内の共用エリアの区画(例:市役所の待合ホール、共有エリア、アトリウム等)

図 4 に示すような利用形態における、ルーティング/スイッチング、フィルタリング、VPN 等の機能を有する通信機器が該当する(例:赤枠の機器+緑枠の必須付随サービス)。

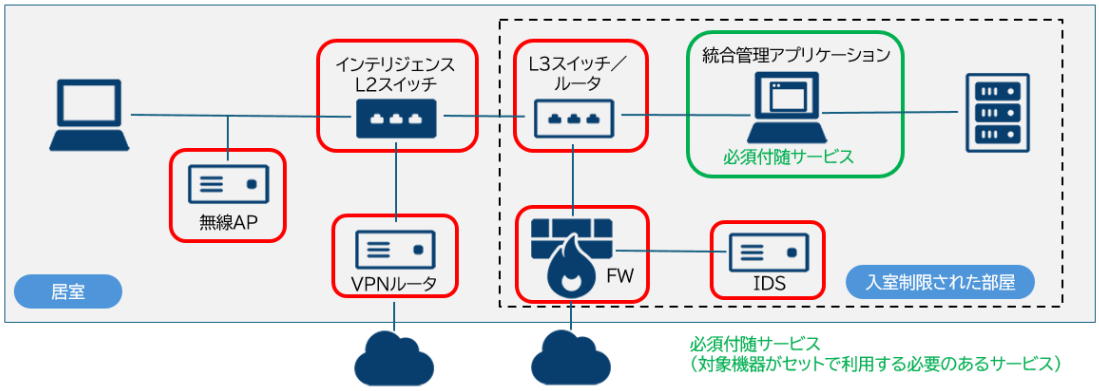


図 4. ★3 通信機器の例

3. ★3 通信機器のセキュリティ要件について

3.1 ★3 通信機器のセキュリティ要件導出の考え方

★3 通信機器のセキュリティ要件、適合要件の導出にあたっては、政府等向けの通信機器として考慮すべき主な脅威と通信全般での脅威について検討し、その脅威リストを基に CAPEC にて攻撃手法を抽出した。具体的には、一定程度の専門知識を有し、公開されていない情報や簡素なツールも用いて攻撃を行う中級クラスの攻撃者による過去のインシデント事例を防止できるレベルを想定して、考慮すべき脅威をリストアップした。

- Mirai や Mirai 亜種による攻撃(BoT 化リスクへの対応)
- 自動化された攻撃によるマルウェア感染(悪意のあるコードの混入リスクへの対応)
- 正規の ID・パスワードを用いた侵入(内部ネットワークへの侵入リスクへの対応)
- 踏み台による他の機器への攻撃(踏み台となるリスクへの対応)
- 既知及び未知の脆弱性を悪用した攻撃(脆弱性対応・脆弱性検査不備リスクへの対応)
- 政府・自治体・企業を標的としたサービス不能攻撃(悪意のある攻撃リスクへの対応)
- サプライチェーンにおけるバックドアを仕込んだ攻撃(サプライチェーンリスクへの対応)

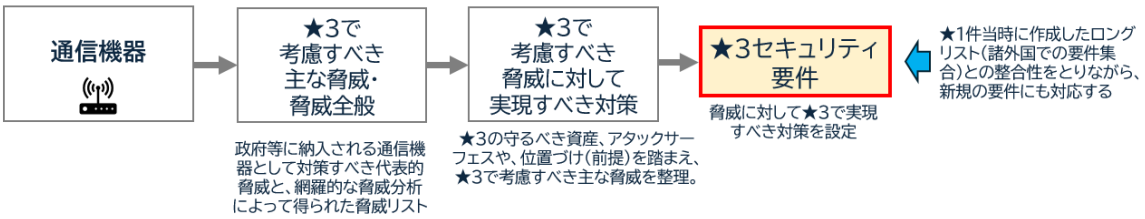


図 5. ★3 セキュリティ要件の抽出プロセスのイメージ

セキュリティ要件は、以下の 3 つの視点から、IoT 製品自体又は IoT 製品ベンダーにおいて実現すべき対策として選定し、表 5 の通り取りまとめた。

1) 上記の分析でリストアップされた脅威に基づく、通信機器に対する主な攻撃手法への対策
2) ★1 でも要求されている対策
3) 通信機器に対する他制度・規格との水準を考慮し、必要と判断した対策

なお、セキュリティ要件に対して具備する必要がある機能や、IoT 製品ベンダーが対応する必要のある対策など、具体的に満たす必要のある★3 適合要件は、「適合要件・評価ガイド」に記載される。

表 5. 攻撃手法に対抗するために★3 で実現すべきセキュリティ要件

★3 で考慮すべき主な攻撃手法	攻撃手法に対抗するために★3 で実現すべきセキュリティ要件					
	IoT 製品が担う対策			IoT 製品ベンダーが担う対策		
	対策種別	★3 適合要件の概要	要件番号	対策種別	★3 適合要件の概要	要件番号
1.脆弱なパスワードの使用による、外部からの意図しないアクセス攻撃	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	S3.1-02	情報提供	･セキュアな利用方法に関する情報を提供する	S3.1-03
		･セキュアな認証の仕組みを提供する	S3.1-01			
			S3.1-05			
			S3.1-06			
			S3.1-07			
		･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	S3.1-04			
2.脆弱性の放置により未対応の脆弱性を含んだ状態による、情報漏洩、改ざん、機能異常の発生につながる攻撃	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	S3.1-43	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	S3.1-14
		･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	S3.1-10		･脆弱性開示ポリシーの公開	S3.1-09
		･自動更新機能の実装	S3.1-10			S3.1-44
		・不正なアップデートパッケージが適応されない対策を行う	S3.1-12	更新方法の開示	･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	S3.1-11
			S3.1-19	アップデートパッチの管理	・最新のパッチを適用できるよう管理する	S3.1-13

3.意図しないインタフェース経由による外部からのアクセスによる、情報漏洩、改ざん、機能異常の発生につながる攻撃	接続される機器の管理	フィルタリング機能	S3.1-08	-		
	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	S3.1-23			
		･最小限の実行権限	S3.1-28			
	物理インタフェースへのアクセス	･使用しないインタフェースを無効化する	S3.1-25			
		･デバッグインタフェースの無効化	S3.1-25			
		･最小限の実行権限	S3.1-28			
	最小限のソフトウェアサービス	･デフォルトで有効なソフトウェアサービスは必要最小限である	S3.1-24			
			S3.1-26			
			S3.1-27			
4.守るべき情報資産の機器間通信の盗聴	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洩や変更に対する保護対策を実装する	S3.1-20	管理プロセス	・暗号鍵の安全な管理	S3.1-21
			S3.1-22			
5.廃棄・転売等された機器から、守るべき情報資産の盗み取り	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	S3.1-36	情報提供	･セキュアな廃棄方法に関する情報を提供する ･初期化方法に関する情報を提供する ･データの削除方法を提供する	S3.1-36
		･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	S3.1-16			S3.1-37
		･機器の初期化機能を提供する	S3.1-37			

6.セキュリティ機能の異常を目的としたネットワーク切断や停電等の攻撃	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	S3.1-33 S3.1-34	-		
7.保存されているテレメトリデータへの攻撃	データ保護	・機器が保有する守るべきテレメトリデータを保護するための機能を提供する	S3.1-35 S3.1-40	情報提供	・セキュアな廃棄方法に関する情報を提供する	S3.1-45
					・機器に収集されるテレメトリデータのデータ種別に関する情報を提供する	S3.1-32 S3.1-41
8.保存されている守るべき情報資産への攻撃	データ保護	・機器が保有する守るべき情報資産を保護するための機能を提供する	S3.1-16 S3.1-17 S3.1-18	情報提供	・セキュアな廃棄方法に関する情報を提供する	S3.1-36
		・ユーザーが個人情報や設定情報等を削除/破棄できる機能の実装を提供する	S3.1-36 S3.1-42		・機器に収集される個人情報のデータ種別に関する情報を提供する	S3.1-39
9.サービス不能攻撃	レジリエンスの向上	・サービス不能攻撃によるネットワーク負荷状態からの復元機能を提供する	S3.1-46	-		
10.物理的な攻撃	筐体のタンパー性	・筐体に対する物理的な破壊・改変行為を防ぐ仕組みを提供する	S3.1-47	-		
11.意図しない入力、データによる攻撃	入力データの確認	・機器に入力されるデータの妥当性を確認する機能を提供すること	S3.1-38	-		
12.意図しないソフトウェアを起動させる攻撃	セキュアブート	・起動するソフトウェアの完全性を検証する機能を提供すること	S3.1-31	-		

13.サプライチェーン攻撃	ソフトウェアの管理	・安全性が確保されたサードウェアコンポーネントが組み込まれること	S3.1-30	SBOM(Software Bill of Materials)の導入	・SBOM を作成し、脆弱性やライセンスなどソフトウェアコンポーネントの管理を行う	S3.1-15
					・ソフトウェアの開発はセキュアに管理されていること	S3.1-29

3.2 ★3 通信機器での守るべき情報資産

★3 通信機器として、守るべき情報資産を表 6 のように定義する。
なお、「守る」には、「不正な開示や暴露により、本来は保護されているべき情報が非権限者に漏洩し、不正アクセスやデータ漏洩などのセキュリティ上の問題が生じないように対策する」という意味の「機密性を守る」という場合と、「改ざんにより、情報の信頼性や完全性が損なわれ、危険な状態になっているにも関わらず、その情報を信じて使用してしまうことがないように対策する」という意味の「完全性を守る」という場合がある。
表 6 において、CSP(Critical Security Parameter)はいかなる場合でも例外なく「機密性」と「完全性」の両方を守る必要がある情報資産に該当する。それ以外の情報資産は、「完全性」を守る必要はあるが、「機密性」を守るところまで求められるかは利用環境やユースケースなどに依存することに留意する。

表 6. 通信機器での守るべき情報資産

守るべき情報資産	保護対象となる情報
CSP (Critical Security Parameter)	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
SSP (Sensitive Security Parameter)	CSP(Critical Security Parameter)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
セキュリティ機能に関する設定情報	認証情報(ユーザ認証/ホスト認証)、電子証明書、改ざん検出設定、ユーザ権限設定

通信機能に関する設定情報	設定した IP アドレス情報(IPv4、IPv6)、VLAN 設定、DHCP サーバー設定、Wi-Fi の SSID
ログ(テレメトリデータ・監査ログ)	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)	ソフトウェア
その他	IoT 製品の意図する使用において、IoT 製品が収集し、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

3.3 対策の分類カテゴリ

表 5 に示すように、様々な攻撃手法に対抗するために実現すべき対策は色々ある。
そこで、類似の対策をまとめた分類カテゴリを、以下の通り、定義する。
適合要件はこの分類カテゴリに沿って整理する。なお、全てのカテゴリの対策が必要というわけではないことに留意されたい。

表 7. 対策の分類カテゴリ

分類カテゴリ	概要
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	簡単に不正アクセスされたり、権限奪取されたりして、セキュリティ上の問題を引き起こさないようにするための対策
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	製品に影響する脆弱性の情報を迅速に収集できるように、セキュリティ研究者やその他の人々が問題を報告できるプロセス、及び脆弱性報告があった場合の対処方針を明確にするための対策
カテゴリ 3： ソフトウェアを最新の状態に保つ	発見又は報告された脆弱性が対処されないまま、製品が利用され続けないようにするための対策
カテゴリ 4 ： セキュアに保存する	保存される守るべき情報資産を情報漏洩や改ざんから保護するための対策
カテゴリ 5 ： セキュアに通信する	通信経路において伝送される守るべき情報資産を盗聴や改ざんから保護するための対策

カテゴリ 6 ： 露出した攻撃面を最小化する	攻撃によるリスクを減らすために、アクセス可能な機能やインタフェースを最小限にする対策
カテゴリ 7 ： ソフトウェアの完全性を確実にする	攻撃者によって改ざんされたソフトウェアが、製品にインストールされたり動作したりしないように、ソフトウェアの完全性を守るための対策
カテゴリ 8 ： 個人データがセキュアであることを確実にする	個人データを保護するための対策
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	電力供給やネットワークの停止に対して、システムに一定の耐性を持たせ、安全な運用ができることを求める対策
カテゴリ 10 ： システムのテレメトリデータを検証・保護する	ログやテレメトリデータを取集することで、運用時にセキュリティ上の異常を検出することができるようにするための対策
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	製品の譲渡や廃棄によって、製品の利用時に生成・蓄積されたデータ(特に利用者に関連するデータ)が漏洩しないようにするための対策
カテゴリ 12 ： 製品の設置及びメンテナンスを容易にする	製品の導入時やその後の運用において、ユーザが容易に安全な設定を行えるようにする対策
カテゴリ 13 ： 入力データの妥当性を確認する	受け取ったデータの形式をチェックすることで、攻撃者による不正なコードを含んだ入力から製品を保護するための対策
カテゴリ 14 ： 個人データを適切に処理する	製品が個人データを収集又は利用する場合に、ユーザの意図していない不正な目的で利用されないようにするための対策
カテゴリ 15 ： 製品を識別可能にする	セキュリティ機能において、対象機器を一意に識別できるようにするための対策
カテゴリ 16 ： 脅威を特定しテストする	製品の利用上、想定される脅威を分析し、必要なセキュリティ機能が実装されていることをテストして確認し、セキュリティリスクを低減するための対策

カテゴリ 17 ： 製品に関する情報提供を行う	製造業者に対して、製品を安全に利用するために必要な情報をユーザへ提供することを求める対策
カテゴリ 18 ： 文書化する	製造業者に対して、製品開発ライフサイクルにおけるセキュリティ関連文書の作成及び保管を求める対策
カテゴリ 19 ： 製品の可用性を確実にする	製品の可用性を守るために有効な設計、実装を求める対策
カテゴリ 20 ： セキュアなセッションを確立する	通信における、なりすましや改ざん、盗聴から保護し、安全な通信を確立するための対策
カテゴリ 21 ： ハードウェアの完全性を確実にする	製品に対する物理的な破壊、改ざんなどの脅威から保護するための対策

4. ★3 通信機器のセキュリティ要件

【★3 セキュリティ要件の構成】

セキュリティ要件ごとに以下のような構成で記載されている。

表 8. セキュリティ要件の構成

カテゴリ	求められる★3 セキュリティ要件への対策が該当する分類カテゴリ
セキュリティ要件番号：S3.1-xx	セキュリティ要件番号
★3 セキュリティ要件	★3 レベルの IoT 製品として、満たす必要のあるセキュリティ対策や基準。
対象外(NA)となるための条件、基準の補足説明	★3 セキュリティ要件の対象外となるための条件、及び★3 セキュリティ要件の補足説明。 対象外(NA)と判定する場合には、評価者は本項目に記載された「対象外(NA)となるための条件」を満たしていることの証跡(エビデンス)を保管する必要がある。

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

セキュリティ要件番号 ： S3.1-01

★3 セキュリティ要件

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なければならない。

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しなければならない。

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)。

基準の補足説明

【用語定義：守るべき情報資産】

以下の情報：

・CSP(Critical Security Parameter)

・SSP(Sensitive Security Parameter)

・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 製品の意図する使用において、IoT 製品が収集し、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：CSP(Critical Security Parameter)】
セキュリティに関連する情報であって、その開示又は変更が、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)

【用語定義：SSP(Sensitive Security Parameter)】
CSP(Critical Security Parameter)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

【用語定義：ユーザ】
ユーザの対象範囲には、IoT 製品の利用者、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 製品内の守るべき情報資産へのアクセスができる当該 IoT 製品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。

セキュリティ要件番号 ： S3.1-02
★3 セキュリティ要件
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さなければならない。
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
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)。

基準の補足説明

【用語定義：ユーザ】

ユーザの対象範囲には、IoT 製品の利用者、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 製品内の守るべき情報資産へのアクセスができる当該 IoT 製品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。

セキュリティ要件番号 ： S3.1-03

★3 セキュリティ要件

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、その認証値の変更が可能でなければならない。

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)。

基準の補足説明

【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 製品の利用者、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 製品内の守るべき情報資産へのアクセスができる当該 IoT 製品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。

セキュリティ要件番号 ： S3.1-04

★3 セキュリティ要件

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について、総当たり攻撃を困難としなければならない。

対象外(NA)となるための条件

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）。

基準の補足説明

【用語定義：ユーザ】

ユーザの対象範囲には、IoT 製品の利用者、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 製品内の守るべき情報資産へのアクセスができる当該 IoT 製品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。

セキュリティ要件番号 ： S3.1-05

★3 セキュリティ要件

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たなければならない。

IoT 製品で使用する電子証明書は、更新可能でなければならない。

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。

セキュリティ要件番号 ： S3.1-06

★3 セキュリティ要件

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なければならない。

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。

セキュリティ要件番号 ： S3.1-07

★3 セキュリティ要件

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さなければならない。

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。

基準の補足説明

【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。

セキュリティ要件番号 ： S3.1-08

★3 セキュリティ要件

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実装しなければならない。

対象外(NA)となるための条件

IoT 機器において、L2/L3 スイッチング又はルーティング機能を持たない。

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

セキュリティ要件番号 ： S3.1-09

★3 セキュリティ要件

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)しなければならない。

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

カテゴリ 3 ： ソフトウェアを最新の状態に保つ

セキュリティ要件番号 ： S3.1-10

★3 セキュリティ要件

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さなければならない。
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。

セキュリティ要件番号 ： S3.1-11
★3 セキュリティ要件
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でなければならない。

基準の補足説明

【用語定義：ユーザ】
ユーザの対象範囲には、IoT 製品の利用者、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 製品内の守るべき情報資産へのアクセスができる当該 IoT 製品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。

セキュリティ要件番号 ： S3.1-12
★3 セキュリティ要件
ソフトウェアをアップデートする際に以下①から③全てを満たす機能を実装しなければならない。
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。

セキュリティ要件番号 ： S3.1-13
★3 セキュリティ要件
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。

セキュリティ要件番号 ： S3.1-14

★3 セキュリティ要件

IoT 製品の型番は、以下のいずれかの方法でユーザへ提供しなければならない。

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。

基準の補足説明

【用語定義：ユーザ】

ユーザの対象範囲には、IoT 製品の利用者、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 製品内の守るべき情報資産へのアクセスができる当該 IoT 製品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。

セキュリティ要件番号 ： S3.1-15

★3 セキュリティ要件

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、運用を行わなければならない。具体的には以下の①～③のすべての基準を満たさなければならない。

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。

カテゴリ 4 ： セキュアに保存する

セキュリティ要件番号 ： S3.1-16

★3 セキュリティ要件

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なければならない。

基準の補足説明

【用語定義：守るべき情報資産】

以下の情報：

・CSP(Critical Security Parameter)

・SSP(Sensitive Security Parameter)

・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 製品の意図する使用において、IoT 製品が収集し、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：CSP(Critical Security Parameter)】

セキュリティに関連する情報であって、その開示又は変更が、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)

【用語定義：SSP(Sensitive Security Parameter)】

CSP(Critical Security Parameter)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

セキュリティ要件番号 ： S3.1-17

★3 セキュリティ要件

IoT 製品で使用されるハードコードされた SSP(Sensitive Security Parameter)(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さなければならない。

①ハードコードされた SSP(Sensitive Security Parameter)の全容を把握し、一覧化できていること。

②すべての SSP(Sensitive Security Parameter)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。

対象外(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 SSP(Sensitive Security Parameter)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 SSP(Sensitive Security Parameter)

が存在しないことを明示すること)。

基準の補足説明

【用語定義：CSP(Critical Security Parameter)】
セキュリティに関連する情報であって、その開示又は変更が、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)

【用語定義：SSP(Sensitive Security Parameter)】
CSP(Critical Security Parameter)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

セキュリティ要件番号 ： S3.1-18

★3 セキュリティ要件

ソースコードに記載されたSSP(Sensitive Security Parameter)にCSP(Critical Security Parameter)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さなければならない。
①ソースコードにハードコードされているSSP(Sensitive Security Parameter)の全容を把握し、一覧化できていること。
②SSP(Sensitive Security parameter)のうち、IoT製品の運用中に利用されるCSP(Critical Security Parameter)が、①の一覧に含まれていないこと。

対象外(NA)となるための条件

ソースコードにSSP(Sensitive Security parameter)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SSP(Sensitive Security Parameter)が存在しないことを明示すること)。

基準の補足説明

【用語定義：CSP(Critical Security Parameter)】
セキュリティに関連する情報であって、その開示又は変更が、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)

【用語定義：SSP(Sensitive Security Parameter)】

CSP(Critical Security Parameter)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

セキュリティ要件番号 ： S3.1-19

★3 セキュリティ要件

IoT 製品で使用される CSP(Critical Security Parameter)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 CSP(Critical Security Parameter)は、IoT 機器毎に固有でなければならない。

基準の補足説明

【用語定義：CSP(Critical Security Parameter)】

セキュリティに関連する情報であって、その開示又は変更が、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)

カテゴリ 5 ： セキュアに通信する

セキュリティ要件番号 ： S3.1-20

★3 セキュリティ要件

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なければならない。

①IoT 製品は守るべき情報資産の通信先の正当性を確認する。

②IoT 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。

③IoT 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。

基準の補足説明

【用語定義：守るべき情報資産】

以下の情報：

・CSP(Critical Security Parameter)

・SSP(Sensitive Security Parameter)

・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 製品の意図する使用において、IoT 製品が収集し、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：CSP(Critical Security Parameter)】
セキュリティに関連する情報であって、その開示又は変更が、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)

【用語定義：SSP(Sensitive Security Parameter)】
CSP(Critical Security Parameter)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

【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

セキュリティ要件番号 ： S3.1-21
★3 セキュリティ要件
IoT 製品で利用する CSP(Critical Security Parameter)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なければならない。
基準の補足説明
【用語定義：CSP(Critical Security Parameter)】
セキュリティに関連する情報であって、その開示又は変更が、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)

セキュリティ要件番号 ： S3.1-22
★3 セキュリティ要件

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 IEEE802.1X による機器認証を行う機能を実装しなければならない。

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。

カテゴリ 6 ： 露出した攻撃面を最小化する

セキュリティ要件番号 ： S3.1-23

★3 セキュリティ要件

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しなければならない。具体的には、以下の①・②のすべての基準を満たさなければならない。

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。

セキュリティ要件番号 ： S3.1-24

★3 セキュリティ要件

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なければならない。

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

セキュリティ要件番号 ： S3.1-25

★3 セキュリティ要件

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なけれ

ばならない。
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又は論理的に無効化していること。

セキュリティ要件番号 ： S3.1-26
★3 セキュリティ要件
製造業者は、IoT 製品の設計及び実装において、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しなければならない。

セキュリティ要件番号 ： S3.1-27
★3 セキュリティ要件
製造業者は、IoT 製品に展開されるソフトウェアの実装及びテストにおいて、コード最小化のための手法を採用しなければならない。

セキュリティ要件番号 ： S3.1-28
★3 セキュリティ要件
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及び実装を行っていなければならない。具体的には、以下の基準を満たさなければならない。
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。

基準の補足説明

【用語定義：ユーザ】
ユーザの対象範囲には、IoT 製品の利用者、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 製品内の守るべき情報資産へのアクセスができる当該 IoT 製品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。

セキュリティ要件番号 ： S3.1-29
★3 セキュリティ要件
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しなければならない。具体的には、最低限以下の実施を含まなければならない。

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

セキュリティ要件番号 ： S3.1-30
★3 セキュリティ要件
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なければならない。
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。

対象外(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)。

カテゴリ 7 ： ソフトウェアの完全性を確実にする

セキュリティ要件番号 ： S3.1-31
★3 セキュリティ要件
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しなければならない。
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わなければならない。
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

カテゴリ 8 ： 個人データがセキュアであることを確実にする

セキュリティ要件番号 ： S3.1-32
★3 セキュリティ要件
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わなければならない。
①センシングする情報について、収集の目的及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。

対象外(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。

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

セキュリティ要件番号 ： S3.1-33

★3 セキュリティ要件

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なければならない。

セキュリティ要件番号 ： S3.1-34

★3 セキュリティ要件

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実装しなければならない。

カテゴリ 10 ： システムのテレメトリデータを検証・保護する

セキュリティ要件番号 ： S3.1-35

★3 セキュリティ要件

セキュリティ上の異常を検知するために、IoT 製品はログ(テレメトリデータ・監査ログ)を記録する機能を実装しなければならない。具体的には、以下①～③すべての基準を満たさなければならない。

①IoT 製品に対し、ログ(テレメトリデータ・監査ログ)の取得機能及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、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)、ファイアウォールの動作状況の記録(ファイアウ

ォール機能が実装されている場合)、リモート管理サービスの動作状況の記録(CWMP などが有効化されている場合)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。

基準の補足説明

【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、及び操作の履歴を、時系列かつ連続的に記録したデータを指す。

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

セキュリティ要件番号 ： S3.1-36

★3 セキュリティ要件

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さなければならない。
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。

基準の補足説明

【用語定義：ユーザ】
ユーザの対象範囲には、IoT 製品の利用者、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 製品内の守るべき情報資産へのアクセスができる当該 IoT 製品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。

カテゴリ 12 ： 製品の設置及びメンテナンスを容易にする

セキュリティ要件番号 ： S3.1-37

★3 セキュリティ要件

IoT 機器は、安全なデフォルト構成設定に復元できなければならない。

カテゴリ 13 ： 入力データの妥当性を確認する

セキュリティ要件番号 ： S3.1-38

★3 セキュリティ要件

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しなければならない。

カテゴリ 14 ： 個人データを適切に処理する

セキュリティ要件番号 ： S3.1-39

★3 セキュリティ要件

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しなければならない。

対象外(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。

セキュリティ要件番号 ： S3.1-40

★3 セキュリティ要件

IoT 製品がログ(テレメトリデータ、監査ログ)を収集し、それに含まれる個人情報の処理を行う場合、以下の基準を満たさなければならない。

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。

対象外(NA)となるための条件

IoT 製品がログ(テレメトリデータ、監査ログ)を取得しない又は IoT 製品がログ(テレメトリデータ、監査ログ)を取得するが、個人情報の処理を行わない場合(「NA であることの理由」に、IoT 製品からログ(テレメトリデータ、監査ログ)を取得しない又は機器からログ(テレメトリデータ、監査ログ)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)。

セキュリティ要件番号 ： S3.1-41

★3 セキュリティ要件

製造業者は、IoT 製品がどのようなログ(テレメトリデータ・監査ログ)を記録し、どのような目的で使用するかについてユーザに開示しなければならない。

基準の補足説明

【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。

セキュリティ要件番号 ： S3.1-42

★3 セキュリティ要件

IoT 製品が個人情報を処理する場合、IoT 製品は収集や処理の範囲を限定するために、不要になった個人情報を削除する機能を持たなければならない。

対象外(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。

カテゴリ 16 ： 脅威を特定しテストする

セキュリティ要件番号 ： S3.1-43

★3 セキュリティ要件

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なければならない。

カテゴリ 17 ： 製品に関する情報提供を行う

セキュリティ要件番号 ： S3.1-44

★3 セキュリティ要件

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。

基準の補足説明

【用語定義：ユーザ】

ユーザの対象範囲には、IoT 製品の利用者、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 製品内の守るべき情報資産へのアクセスができる当該 IoT 製品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。

セキュリティ要件番号 ： S3.1-45

★3 セキュリティ要件

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わなければならない。

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。

基準の補足説明

【用語定義：守るべき情報資産】

以下の情報：

・CSP(Critical Security Parameter)

・SSP(Sensitive Security Parameter)

・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 製品の意図する使用において、IoT 製品が収集し、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：CSP(Critical Security Parameter)】

セキュリティに関連する情報であって、その開示又は変更が、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）

【用語定義：SSP(Sensitive Security Parameter)】
CSP(Critical Security Parameter)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

カテゴリ19 ： 製品の可用性を確実にする

セキュリティ要件番号 ： S3.1-46

★3 セキュリティ要件

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持たなければならない。

基準の補足説明

【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。

カテゴリ21 ： ハードウェアの完全性を確実にする

セキュリティ要件番号 ： S3.1-47

★3 セキュリティ要件

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しなければならない。

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、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、適合要件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。
SSP (Sensitive Security Parameter)	CSP(Critical Security Parameter)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
PSP (Public security Parameter)	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、又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。
CSP (Critical Security Parameter)	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。
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、ユーザーとの間に暗号化された通信経路を作成する機能
保護されたネットワーク	・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
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。
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、及び操作の履歴を、時系列かつ連続的に記録したデータを指す。
ネットワーク過負荷状態	IoT 機器から外部へ通信が行えない状態

Appendix B: 参照先リンク

既存制度・文書	Link
ETSI EN 303 645 V3.1.3 (2024-09)	https://www.etsi.org/deliver/etsi_en/303600_303699/303645/03.01.03_60/en_303645v030103p.pdf
Cybersecurity Labelling Scheme (CLS) Publication No.4 Version 1.2 April 2025	https://isomer-user-content.by.gov.sg/36/03b1d128-7284-40ac-bb1f-fdc94b5842a3/CCC%20SP-151-4%20CLS(IoT)%20Assessment%20Methodology%20v1.2.pdf
Cyber Resilience Act(CRA)23 October 2024	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202402847
Radio Equipment Directive (RED):28.12.2024	https://single-market-economy.ec.europa.eu/sectors/electrical-and-electronic-engineering-industries-eei/radio-equipment-directive-red_en
EN 18031-1 / -2 / -3: 2024	EN 18031-1：https://statics.teams.cdn.office.net/evergreen-assets/safelinks/2/atp-safelinks.html EN 18031-2：https://statics.teams.cdn.office.net/evergreen-assets/safelinks/2/atp-safelinks.html EN 18031-3：https://statics.teams.cdn.office.net/evergreen-assets/safelinks/2/atp-safelinks.html
IEC 62443-4-1 2018	https://webstore.iec.ch/en/publication/33615
IEC 62443-4-2 2019	https://webstore.iec.ch/en/publication/34421
NIST IR 8425 September 2022	https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8425.pdf
UK PSTI 法 Regulation 2023	https://www.legislation.gov.uk/uksi/2023/1007/schedule/1/made
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)の一部改定(令和７年９月)	https://www.cyber.go.jp/pdf/policy/general/guider7_9.pdf

CCDS IoT 機器セキュリティ要件適合基準ガイドライン 2025 年版 Ver.1.0	https://www.ccds.or.jp/public/document/other/CCDS_SecGuide-IoTReq_Criteria_2025_v1.0_jpn.pdf
特定用途機器 共通セキュリティプロテクションプロファイル 1.0 版	https://www.ipa.go.jp/security/jisec/pps/certified-pps/c0755_it2805.html
BMSec ネットワーク機能付き事務機セキュリティガイドライン Ver.1.00	https://bmsec.jbmia.or.jp/file/guide.pdf
総務省 端末設備等規則　令和 7 年 10 月 1 日 施行	https://laws.e-gov.go.jp/law/360M50001000031