独立行政法人
情報処理推進機構
Innovation Platform Agency, Japan

JST-RC-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適合要件

令和８年６月

独立行政法人情報処理推進機構

目次

1. はじめに

本文書は、製造業者と評価機関向けの資料であり、「通信機器★３セキュリティ要件(JST-SR-03-01-2026)」に記載されているセキュリティ要件について、適合するための具体的な要件を適合要件として記載したものである。

2. JC-STAR★３で実現したいセキュリティレベルの考え方

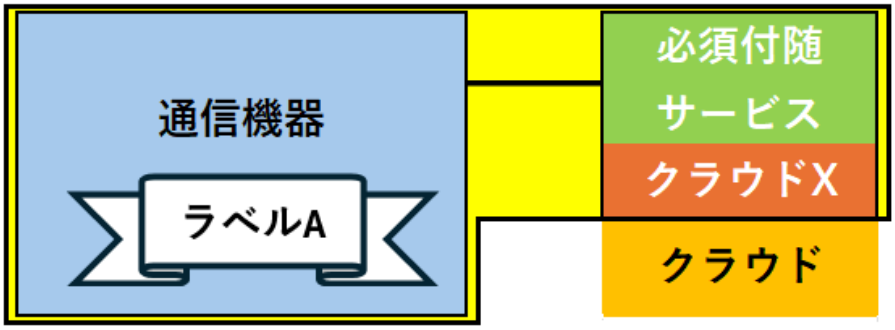
2.1 スコープ対象となる通信機器の考え方

JC-STAR★３通信機器(以下、★３通信機器)にてスコープ対象範囲は、「通信機器★３セキュリティ要件」の「2.1 ★３適合ラベル(通信機器)の主な対象範囲」を参照すること。

2.2 「必須付随サービス」の考え方

JC-STAR における「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。「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デジタルサービスのことである。

例えば、通信機器が保存した通信アクセスに関するログを特定のクラウドサービスに送信、保存するように設定されている場合、当該サービス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、「通信機器」、「クラウドサービス」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「通信機器」に対して付与される。



(注釈)クラウド X: サービスが直接的に利用するクラウド領域

図 1. IoT 機器と必須付随サービスの関係

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。例えば、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)などのデジタルサービスを含めることができる。

一方、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「外部システム」となるので、注意すること。

本文書では、必須付随サービスと外部システムとを区別する要素は、システム上で提供するサービスが IoT 機器の製造業者の管理下で提供されるか否かである。つまり、製造業者の

管理下で提供される場合は「必須付随サービス」といい、製造業者ではなく利用者の管理下で利用する場合は「外部システム」という。

2.3 ★３通信機器で実現したいセキュリティの考え方

★３レベルでは、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調達、利用される通信機器を対象とし、リスク分析より選出した攻撃手法に対抗することを目的としている。このため、運用中の IoT 製品に対して、一般に入手可能なツール及び専門的な知見を持って行う攻撃(情報セキュリティ評価認証制度の CEM[1]における強化基本“Enhanced Basic”の攻撃能力を有する攻撃者による攻撃)に対抗できることを想定している。

この目的を鑑み、本適合要件で対象としている★３通信機器では、以下の攻撃手法への対策を要求する。

① 脆弱なパスワードを使用することにより起きる外部からの意図しないアクセス攻撃に対する対策
② 脆弱性の放置による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、又はマルウェア感染や攻撃の踏み台への対策
③ 意図しないインタフェース経由による外部からの意図しないアクセスによる、情報漏洩、改ざん、機能異常の発生につながる攻撃、マルウェア感染や攻撃の踏み台への対策
④ 機密通信情報[2]の通信を盗聴される攻撃への対策
⑤ 廃棄・転売等された機器から、セキュア保存情報[2]が盗み取られる攻撃への対策
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への対策
⑦ 監査ログ、テレメトリデータ等のログの記録
⑧ 保存されているセキュア保存情報への攻撃への対策
⑨ サービス不能攻撃への対策
⑩ 物理的な攻撃への対策

---

1 https://www.enisa.europa.eu/sites/default/files/publications/ENISA_candidate%20scheme_EUCC.pdf(BACKGROUND INFORMATION, Table B.2, Table B.3)
https://www.ipa.go.jp/security/jisec/about/cdk3vs000000240h-att/CEMV3.1R5-J1.0.pdf(B.4.2.3 攻撃能力の計算)

2 「機密通信情報」と「セキュア保存情報」
これらの用語については、「2.4 ★３通信機器での守るべき情報資産の種類」を参照

⑪　意図しない入力、データによる攻撃への対策
⑫　意図しないソフトウェアを起動させる攻撃への対策
⑬　サプライチェーン攻撃への対策

以上の攻撃手法への対策を前提として、通信機器で主に想定される情報資産、アタックサーフェス、脅威や対策などを検討し、「通信機器★３セキュリティ要件」を定めている。

本文書では、通信機器★３セキュリティ要件を満たしていることの条件となる「通信機器★３適合要件」を定める。また、本適合要件を満たしているかを判断する評価手順については「通信機器★３評価ガイド」を参照のこと。

2.4 ★３通信機器での守るべき情報資産の種類

「情報を守る」には二つの意味がある。一つは「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」、すなわち「情報の機密性(Confidentiality)を守る」という意味であり、もう一つは「情報の改ざんや偽造により、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かかわらず、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」、すなわち「情報の完全性(Integrity)を守る」という意味である。

そこで、「機密性」「完全性」のどちらかでも守る必要がある情報のことを「守るべき情報資産」と呼ぶこととし、通信機器でのユースケースや実装環境などを考慮して、★３通信機器としての「守るべき情報資産」を表１に定める。これらについては、情報資産ごとに必要性に応じて「機密性」もしくは「完全性」を守ることを要求する。

また、「ネットワークを介して通信されるときに機密性を守るべき情報資産」のことを「機密通信情報」と呼び、適切な暗号化を行う通信プロトコルで通信することを要求する。この対象となる情報資産を表 1①に定める。

「IoT 機器へ保存される守るべき情報資産」のことを「セキュア保存情報」と呼び、適切に「機密性」もしくは「完全性」を守ることを要求する。この対象となる情報資産を表 1②に定める。

なお、表 1 はすべての★３通信機器に対して共通してセキュアな管理を要求する最低限の「守るべき情報資産」の種類であり、独自にこれらに含まれない情報資産を「守るべき情報資産」として扱うことを妨げるものではない。

表 1. 通信機器での守るべき情報資産の種類

①：機密通信情報、②：セキュア保存情報

凡例：〇が対象、－は対象外

★３通信機器が扱う情報資産	保護対象となる情報	①	②
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、パスワードや PIN などの認証値、証明書のプライベート要素。	○	○
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。	ー	○
通信機能に関する設定情報(*1)	通信を行うための前準備として事前に設定する情報。 例： 通信設定：IP アドレス、サブネットマスク、デフォルトゲートウェイ、DNS サーバ、ドメイン名など。 ルーター設定機能：ルーティング、QoS、DHCP（サーバ/リレーエージェント）など。 機能設定：HTTP ポートの変更設定(HTTP/HTTPS)、IEEE 802.1X ネットワークアクセスコントロール設定。	○	○
セキュリティ機能に関する設定情報(*1)	セキュリティ機能を有効にするための前準備として事前に設定する情報。 例： ルーターでの設定情報：ファイアウォール、VPN、ログ、統計管理など。 ファイアウォールでの設定情報：フィルタリング、管理者アクセスを許可するネットワーク、アプリケーションコントロールなど。 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、ユーザ権限設定。	○	○
アラート情報	通信機器にて異常を知らせる信号、異常の具体的な内容、セキュリティに関する異常などを検知したときに発報されるアラート情報。	○	ー
プログラムコード	ソフトウェア。	ー	○
	通信機器動作中のテレメトリデータ(例：メトリック)。	ー	○

ログ(テレメトリデータ・監査ログ)	通信機器動作中の監査ログ(通信ログ、イベントログ等も含む)(*2)。	○	○

(*1):機能を有効にするための前準備として通信することを想定する。

(*2):通信機器での監査ログは、通信ログやイベントログ等を想定し、監査ログに個人情報が含まれている可能性があるので、「機密性」を守る対象とする。

2.5 セキュアな保存(保護方法)の考え方

前節の「守るべき情報資産」のセキュアな保存に対しては、「機密性」と「完全性」のいずれか、又はその両方の保護が必要である。

- 「機密性」の保護:情報資産が外部に不正に漏洩しないように保護。
- 「完全性」の保護:情報資産が偽造・改ざんされないように保護。

★3通信機器では、通信機器のライフサイクルの運用中の状態を考慮し、守るべき情報資産のセキュアな保存方法として、以下のいずれかを要求する。

① 暗号技術を利用した対策。「機密性保護」の場合には暗号化、「完全性保護」の場合は署名やメッセージ認証が求められる。なお、保護するために使用される暗号技術は、「電子政府における調達のために参照すべき暗号のリスト(CRYPTREC 暗号リスト)」のうち「電子政府推奨暗号リスト」に記載された暗号技術であって、「暗号強度要件(アルゴリズム及び鍵長選択)に関する設定基準」の規定に合致する鍵長を用いた暗号技術を使用していること。

② OS 提供のサンドボックスやセキュリティチップのセキュア領域への保存。

③ 容易に取り外せないストレージ領域にて直接的なデータへのアクセスができない領域への保存。

2.6 セキュアな通信の考え方

★3通信機器では、ネットワーク経由で伝送される「機密通信情報」は、盗聴及び偽造・改ざんへの対策として「機密性」と「完全性」の両方の保護を要求する。さらに、通信先の正当性確認のため、「真正性」の確認も要求する。

したがって、使用されるネットワークに対して以下の対策が必須である。

- 通信先の正当性が確認できる対策、又は正当な通信先のみに接続可能なアクセス制御機能(例:ホワイトリスト方式の接続)。
- 機密通信情報の盗聴及び偽造・改ざんに対する「機密性」と「完全性」の保護対策。なお、この対策としては、通信先とのエンド・ツウ・エンドで暗号技術を用いた対策を必須とする。

- Secure by Default の観点より、上記の保護機能が初期状態で有効であること。

通信先とのエンド・ツウ・エンドで暗号技術を用いた対策に使用される暗号技術や通信プロトコルなどは、「電子政府における調達のために参照すべき暗号のリスト(CRYPTREC 暗号リスト)」のうち「電子政府推奨暗号リスト」に記載された暗号技術であって、「暗号強度要件(アルゴリズム及び鍵長選択)に関する設定基準」の規定に合致する鍵長を用いた暗号技術を使用していることが必要である。

また、★３通信機器では、必須付随サービスにアプリケーションが含まれる場合に、そのアプリケーションから「機密通信情報」が送信される場合は、当該アプリケーションにも上記の保護対策が要求される。

さらに、政府統一基準を鑑み、無線 LAN においては、無線通信の暗号化、及び 802.1x による機器認証を行うことを要求する。

2.7 個人情報の扱いについての考え方

通信機器では、監査ログなどが収集されるため、利用目的によってはそれらの情報が個人情報保護法上の「個人情報」に該当する可能性がある。そのため、★３通信機器では「個人情報」に対する安全管理措置の機能を有することを必須要件として求める。

具体的には、監査ログなどに対して、通信時及び保存時の両方で機密性の保護を要求する。また、保存の必要がなくなった場合に、★３通信機器として要求されている消去レベルでの消去機能により削除できることを要求する。消去レベルについては、「データ消去についての考え方」を参照のこと。

2.8 データ消去についての考え方

★３通信機器では、ライフサイクルの「破棄」における情報漏洩を考慮し、通信機器を破棄する前に運用中に生成されたデータや設定情報などについて削除できる機能を要求する。「削除」のレベルは、NIST SP800-88 Rev.2[3]によれば削除したデータの復元可能性に応じて「Clear」「Purge」「Destroy」の３段階あるが、★３通信機器では、単純な非侵襲のデータ回復技術(市販のデータ復旧ソフトによるサルベージ等)から保護できるセキュリティレベルである「Clear」レベルで削除されるものとする。

なお、適切な暗号化消去機能を備え、デフォルトで利用可能になっている場合には、暗号化消去によるデータ消去は「Purge」レベル相当として扱う。

[3] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r2.pdf

2.9 SBOM についての考え方

★３通信機器では、サプライチェーンリスクに対応しサードパーティコンポーネントの脆弱性を管理することを目的として、機械可読な形式及びヒューマンリーダブルなソフトウェア部品表(SBOM：Software Bill of Materials)を作成し、また SBOM を利用した脆弱性管理プロセスの構築を求める。

本適合要件では、SBOM の適用対象を、「サードパーティコンポーネントを含む、通信機器で使用されるすべてのコンポーネント」と「必須付随サービス」とする。ただし、現状では SBOM の作成においてグローバルなベストプラクティスとなる基準が存在しないため、本適合要件においては SBOM が扱う階層レベルについて定めず、通常想定される脆弱性の管理に適した範囲で、製造業者が個別に判断してよいものとする(今後の SBOM の動向によっては階層レベルを定めることはあり得る)。

また作成した SBOM については、最初に作成するだけでなく、製造業者がセキュアな SBOM 管理として十分と考える頻度で脆弱性の有無(ライセンスを含めて)を定期的又は逐次確認し、必要な脆弱性対策や SBOM 更新を行う管理プロセスを構築することを併せて要求する。

2.10　★３通信機器適合試験でのペネトレーションテストについて

★３通信機器の適合評価では、評価機関によるペネトレーションテストが実施される。

本適合要件では、2.3 節で説明した攻撃能力を有する攻撃者による攻撃を前提として、少なくとも以下のすべてのペネトレーションテストの項目を実施する。

- ネットワーク診断ツールによる開放ポートに対する公知の脆弱性の検出。
- Web アプリケーション診断ツールによる公知の脆弱性の検出。
- パケットキャプチャツールによる IoT 機器から外部への不正な通信の検出。
- プロキシツールによる Web アプリケーション動的コンテンツに対する脆弱性の検出。
- デバッグポートへの接続ツールによるデバッグ行為可否の確認。

製造業者は、評価機関によるペネトレーションテスト期間中にセキュリティ課題が報告された場合は、その箇所を是正し、すべてのセキュリティ課題を解消しなければならない。

2.11　サポートの提供義務について

適合ラベルの有効期間内については、製品不具合や脆弱性への対応のためのセキュリティパッチ/アップデートファイルの提供(セキュリティパッチ/アップデートファイルが提供できない場合は製品交換等の代替対策を含む)をサポートとして提供する義務がある。適合ラベルの有効期間中のサポートを提供する義務を課すのは、IoT 製品の不具合修正・脆弱

性が発見されたにもかかわらず、セキュリティパッチ/アップデートファイルの提供がきちんと行われず、その不具合・脆弱性が修正されずに放置され続けることを防止するためである。

したがって、当該 IoT 製品の全利用者に対して等しくセキュリティパッチ/アップデートファイルが提供されることが必要となるため、サポートの提供方法として以下のいずれかを義務付ける。

① サポート期間は、全利用者に対して無償でサポートを提供する。

② 保守契約や販売契約等の別途契約を締結することを条件としたうえで、当該契約を締結した調達者に対してのみ販売する（レンタル/リースを含む）場合に限り、有償でのサポートの提供を認める。

適合ラベルの有効期間は延長申請を行うことにより延ばすことができるが、延長される最長可能有効期間よりもサポート終了日が早い場合にはサポート終了日までの有効期間となる。また、有効期間内の途中でサポートを取りやめることになった場合には、サポートを取りやめる期日をもって適合ラベルは失効する(有効期間はサポートを実施する期日まで)。

一方、製品販売終了などにより適合ラベルの延長を行わず、失効する場合であっても、無償のサポート期間が継続している場合には「失効－無償サポート継続中」として扱う。また、無償のサポート期間終了後に有償のサポートを継続する場合には、適合ラベルとしては「失効－有効期限切れ」とするが、「サポート情報」及び「アップデート情報」の欄に「有償サポートが継続」している旨の情報を記載することができる。

3. ★３通信機器の適合要件

【★３適合要件の構成】

各セキュリティ要件には、IoT 製品に求められる適合要件が紐づいており、以下のような構成で記載されている。

表 2. 適合要件の構成

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要件。
対象外(NA)となるための条件	★３セキュリティ要件の対象外となるための条件。対象外(NA)に該当すると主張する場合には、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説明資料を評価機関に提供する必要がある。

★３適合要件	
1. 適合要件	★３セキュリティ要件に記載してある対策、要件に対して、★３レベルの IoT 製品として具備する必要がある機能や、製造業者が対応する必要のある対策を要求し、その要求に対して満たす必要のある要件。
2. 補足説明	
2.1 適合要件の補足説明	本適合要件に関する補足説明、適合判断のための補足説明や要件解釈の考え方をまとめている。
2.2 用語	本適合要件のなかで使われる用語の説明。

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

アクセスの仕組みがない(「対象外(NA)となることの理由」に、外部からのアクセスがない根拠を記載すること)。

1. **★３適合要件**

他の IoT 機器又はユーザからのアクセスにおいて、適切な認証に基づく★３セキュリティ要件を満たすためのアクセス制御として、以下の要件１～７のすべてを満たすこと。

要件１：

IoT 製品の意図される使用上必要な通信(以下に示す「例外となるプロトコル(*1)」を除く)について、他の IoT 機器又はユーザからのアクセスに対して、以下の①と②の両方が満たされていること。

① 適切な認証に基づくアクセス制御が行われており、アクセスが許可された他の IoT 機器又はユーザに対してのみ当該 IoT 製品へのアクセスが許可されること。

② 利用される認証の方法が、以下のいずれかに類する実装又はそれ以上の実装であること。

A) ユーザ認証に使用されるパスワードによるユーザ認証が S3.1-02 に準拠した実装
B) 複数の認証要素を利用した多要素認証機能の実装
C) デジタル証明書や公開鍵を使用した認証機能の実装
D) OpenID Connect、FIDO 等の標準的な認証方式に基づいた外部認証サービスによる認証機能の実装

(*1)：例外となるプロトコル
例１：ARP、ICMP(TCP/UDP より下位のレイヤのプロトコルであるため)
例２：DHCP、DNS、NTP(認証に対応していないプロトコルであるため)

要件２：

SSP(Sensitive Security Parameter)又はセキュリティに関する設定情報の設定変更を行う場合は別途、特別な認証を要求すること。

要件３：

認証メカニズムにおいて継続的なアクセスをセッション等で管理する場合、タイムアウト制限を設けること。

要件４：

初期状態において、利用のために不要なアカウント(*2)が削除又は無効化されていること。

(*2)：不要なアカウントの例：製品開発時に利用していたデバッグアカウント等

要件５：

ユーザが任意で権限を最小化できるよう、IoT 製品へ権限制御のメカニズムを設計・実装をすること。

要件６：

IoT 製品へのユーザからのネットワークを介さないアクセスに対して、以下の①と②の両方が満たされていること。

① 適切な認証に基づいてアクセスが許可されたユーザに対してのみ当該 IoT 製品へのアクセスが許可されること。

② 利用される認証の方法が、以下のいずれかに類する実装又はそれ以上の実装であること。

A) ユーザ認証に使用されるパスワードによるユーザ認証が S3.1-02 に準拠した実装

B) 所持による認証の実装

C) 生体認証の実装

要件７：

通信を許可する対象を IP アドレスなどで制限する機能を実装していること。

2. 補足説明

2.1. 適合要件の補足説明

2.1.1. 権限制御のメカニズムについて

権限制御のメカニズムとは、ユーザ又はソフトウェアプロセス又はデバイスに割り当てるロールを設定できる機能(最低でも管理者と一般ユーザを区分できること)のことである。

2.2. 用語

【SSP(Sensitive Security Parameter)】
CSP(Critical Security Parameter)と PSP(Public Security Parameter)を合わせた情報資産のこと。2.4 節を参照。

【ユーザ】
ユーザの対象範囲には、IoT 製品の利用者、管理者、製造業者のカスタマーエンジニア、所有者等、当該 IoT 製品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のいずれかの要件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 機器ごと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 初回起動時にユーザによるパスワード変更を必須とする機能を実装し、当該機能において設定可能なパスワードとして、容易に推測可能でない 8 文字以上のパスワードの設定を強制させること。

対象外(NA)となるための条件

パスワードを利用したユーザ認証の仕組みがない(「対象外(NA)となることの理由」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. **★３適合要件**

ユーザ認証の仕組みにおいて、★３セキュリティ要件を満たすためのパスワードを利用した IoT 製品導入時のデフォルトパスワードに関する対策として、以下の「要件１」又は「要件２－１と要件２－２の両方」のいずれかを満たすこと。

要件１：

デフォルトパスワードは、IoT 機器ごとに異なる一意で、以下の A)～D)のいずれにも該当しない、8 桁以上のパスワードであること。

A) 共通する文字列や単純なパターンが存在するパスワード(例："admin"、"root"、"QWERTY"など)

B) 覚えやすい有名な固有名詞や、人名、地名などを利用したパスワード(例："baseball"、"mustang"、"michael"など)

C) 増加するカウンターに基づくパスワード(例：”123456”、"aaaaaaaa"、"1234abcd"、"password1"など)

D) MAC アドレス、Wi-Fi の SSID、IoT 製品のシリアル・型番・名前(略称)などの公開情報に基づくパスワード

要件２－１：

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を強制させること。なお、ネットワークを介したユーザ認証の仕組みを有するが、ネットワーク機能を使用せずに利用可能な IoT 製品の場合、ネットワークを介したユーザ認証で利用するパスワードについ

て、初回起動時ではなく、ネットワーク機能を初めて使用する時にユーザによるパスワード変更を必須とすることでもよい。

要件２－２：

設定するパスワードが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を強制するか、容易に推測可能でない 8 文字以上のパスワードでない場合にユーザに警告する機能を有すること。容易に推測可能でないパスワードであるか否かの判断方法としては、以下の①～④が考えられる。これに類するか、それ以上の判断ができる方法を実装すること。

① 上記の A)～D)の条件に一致しないパスワード(辞書攻撃耐性がある)であることを確認する
② ランダム性判定のインジケータを使用する
③ 文字種数と長さの条件を付ける
④ 自動生成するパスワードを強制する

2. 補足説明

2.1. 適合要件の補足説明

該当事項なし

2.2. 用語

【ユーザ】

ユーザの対象範囲には、IoT 製品の利用者、管理者、製造業者のカスタマーエンジニア、所有者等、当該 IoT 製品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)によらず、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

ユーザ認証及び機器認証の仕組みがない(「対象外(NA)となることの理由」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及び機器認証が必要ない根拠を記載すること)。

1. **★３適合要件**

ユーザ認証及び機器認証の仕組みにおいて、★３セキュリティ要件を満たすための認証値の変更方法として、以下の要件１～４のすべてを満たすこと。

要件１：

ユーザ認証については、認証の種類(パスワード、トークン、指紋等)によらず、ユーザ自身によって認証値の変更が可能であること。

要件２：

要件１での変更手順がマニュアル等によってユーザに提供されていること。

要件３：

認証値の変更においては、たとえ認証済みであっても改めて認証を要求すること。

要件４：

要件１での認証値の変更をユーザが自ら行えない場合にユーザからの要求によって、また管理者の権限として、認証値の再設定又は初期化が行える仕組みを有すること。また、要件１とは異なる方法で認証値の再設定又は初期化が行えること。

2. **補足説明**

2.1. 適合要件の補足説明

該当事項なし

2.2. 用語

【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、認証値はパスワード情報となる。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。）

【ユーザ】
ユーザの対象範囲には、IoT 製品の利用者、管理者、製造業者のカスタマーエンジニア、所有者等、当該 IoT 製品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

ユーザ認証の仕組みがない(「対象外(NA)となることの理由」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)。

1. **★３適合要件**

ユーザ認証の仕組みにおいて、★３セキュリティ要件を満たすための総当たり攻撃を困難とする仕組みとして、以下の「要件１－１及び要件１－２の両方」又は「要件２」のいずれかを満たすこと。

要件１－１：

ユーザ認証について、認証試行の「一定回数(*1)」の連続失敗に対し、下記に類する認証試行制限の対応をしていること。

A) 追加の認証禁止
B) 認証の一定期間停止
C) 認証応答発行の一定時間遅延

(*1)：一定回数とは、IoT 機器の規定値(1 回以上)又は許容可能な値の範囲で管理者が割り当てた値とする。

要件１－２：

ネットワークを介したユーザ認証の仕組みが有する場合、以下の①～④のいずれかに類する、あるいはそれ以上の対策を行うこと。

① 特定の機器やブラウザからの認証のみを受け付けること(Device Cookie)。
② 特定の IP アドレスからの認証試行の「一定回数」の連続失敗に対し、当該 IP アドレスに対して要件１－１と同様の認証試行制限の対応をしていること。
③ ユーザ認証のアカウントごとにユニークな URL で認証を行うこと。
④ CAPTCHA を使用すること。

要件２：

多要素認証を使用すること。

2. **補足説明**

2.1. 適合要件の補足説明

該当事項なし

2.2. 用語

【ユーザ】

ユーザの対象範囲には、IoT 製品の利用者、管理者、製造業者のカスタマーエンジニア、所有者等、当該 IoT 製品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

認証のために電子証明書を使用していない(「対象外(NA)となることの理由」に、認証のために電子証明書を使用していないと記載すること)。

1. **★３適合要件**

認証のために使用する電子証明書について、★３セキュリティ要件を満たすためのセキュリティ強度の担保、及び電子証明書のセキュアな更新を可能とする仕組みとして、以下の要件１～５のすべてを満たすこと。

要件１：

電子証明書で使用する暗号技術は、「電子政府における調達のために参照すべき暗号のリスト(CRYPTREC 暗号リスト)」のうち「電子政府推奨暗号リスト」に記載された暗号技術であって、「暗号強度要件(アルゴリズム及び鍵長選択)に関する設定基準」の規定に合致する鍵長を用いた暗号技術であること。

要件２：

更新する電子証明書の完全性及び真正性を確認した後に更新すること。また、完全性又は真正性が確認できない場合には更新を中止すること。

要件３：

外部からの正当な指示により電子証明書を失効させる仕組み、又はその他の方法で失効させた電子証明書を認証に利用できなくする仕組みを持つこと。

要件４：

生成メカニズムにより、電子証明書に対応する秘密鍵が機器ごとに固有であること。

要件５：

ルート証明書など、トラストアンカーの更新にあたっては、更新後、IoT 機器に不具合が発生しないよう、安全に更新できること。

2. **補足説明**

2.1. 適合要件の補足説明

2.1.1. 電子証明書について

電子証明書は信頼性が確保された証明書でなければならない。少なくとも、製造業者が正当であることを確認できる必要がある。そのような証明書には、公的証明書や製造業者自身が管理する、あるいは製造業者が契約しているCAが発行するルート証明書等がある。

2.1.2. 初回起動時のみ使用される電子証明書について

通常運用時に使用するための電子証明書の信頼性を確認するために、初回起動時のみ使用される電子証明書は要件２及び要件３の対象外としてよい。
ただし、このような電子証明書を通常運用時に使用してはならない。

2.1.3. トラストアンカーの安全な更新方法の例

例１：トラストアンカー及びトラストアンカーによって信頼性を証明するすべての証明書(コードサイニング証明書など)をファームウェアと同時に一括更新する

例２：古いルート証明書が有効な期間に、新しいルート証明書を追加することにより、新旧のルート証明書を保持し、更新前後の互換性を保証する更新メカニズムを採用する

2.2. 用語

該当事項なし

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

SSH を公開鍵認証にて利用していない(「対象外(NA)となることの理由」に、SSH を公開鍵認証にて使用していないと記載すること)。

1. **★３適合要件**

SSH を公開鍵認証にて利用する場合、★３セキュリティ要件を満たすセキュリティ強度の暗号技術を利用した認証を可能とするため、以下の要件１及び要件２の両方を満たすこと。

要件１：

SSH の公開鍵認証機能で使用する暗号技術は、「電子政府における調達のために参照すべき暗号のリスト(CRYPTREC 暗号リスト)」のうち「電子政府推奨暗号リスト」に記載された暗号技術であって、「暗号強度要件(アルゴリズム及び鍵長選択)に関する設定基準」の規定に合致する鍵長を用いた暗号技術であること。

要件２：

SSH の公開鍵認証で使用する公開鍵は更新可能であること。

2. **補足説明**

2.1. 適合要件の補足説明

該当事項なし

2.2. 用語

該当事項なし

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のすべての要件を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 VPN ゲートウェイ機能を持たない(「対象外(NA)となることの理由」に、VPN ゲートウェイ機能を持たないと記載すること)。

1. **★３適合要件**

VPN ゲートウェイ機能をもつ場合、VPN 接続(*1)において★３セキュリティ要件を満たすための厳格なユーザ認証及び機器の接続制限を行う機能として、以下の要件１～３のすべてを満たすこと。なお、必須付随サービス以外の外部システム連携によって多要素認証を行う機能を有する場合は、要件１～３に加え、要件４を満たすこと。

(*1) VPN 接続：

利用者が利用する機器から内部ネットワークへのリモートアクセス VPN が対象である。拠点間 VPN は対象外である。

要件１：

利用されるユーザ認証の方法が、多要素認証、又はそれに類する実装(*2)であること。

(*2)それに類する実装：

FIDO 認証、又は一部の 2 段階認証と呼ばれる方式を含む。

そのような 2 段階認証の例としては、利用者の携帯電話の電話番号や利用者の電子メールアドレスに対してワンタイムパスワードを送信して利用者に入力させる方法やスマートフォン等への認証要求を利用した認証方式などがある。2 段階認証を用いる場合には、リスクを評価したうえで利用する必要がある。

要件２：

利用される機器の接続制限の方式が、電子証明書を用いた機器の認証、又は事前に機器を一意に識別できる情報を登録する方式(ホワイトリスト方式)であること。ただし、ホワイトリスト方式では、MAC アドレスなどの偽装や情報窃取が容易な情報のみを用いた方式は認めない。

要件３：

VPN プロトコルとして、一般的に安全と認知されているプロトコル(例：OpenVPN、IPsec、

IKEv2 など)がデフォルトで使用されること。

要件４：

必須付随サービス以外の外部システム連携によって多要素認証機能を有する場合には、以下の要件をすべて満たすこと。

A) 多要素認証を行うための信頼できる外部システム連携が可能な条件を明示した文書をユーザに提供すること。そのうち、少なくとも一つは技術的に確認できる条件であること。

B) IoT 機器は、多要素認証を行うために連携する外部システムが A)の技術的に確認できる条件を満たすことを検証する機能を有すること。

C) IoT 機器は、多要素認証を行うために連携する外部システムとの通信において、S3.1-20 に準拠していること。

D) B)及び C)の機能・対策はデフォルトで有効であること。

E) 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、B)の機能を利用して外部システム連携を行うための手順を開示すること。

2. 補足説明

2.1. 適合要件の補足説明

2.1.1. 多要素認証の一つの認証要素として電子証明書を用いる場合

多要素認証の一つの認証要素として電子証明書を用いる場合は、その証明書によって接続先の確認を行う場合には、それをもって要件２に適合と判断することができる。

2.2. 用語

【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、利用者が利用する機器との間に暗号化された通信経路を作成する機能のこと。

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 L2/L3 スイッチング機能を持たない(「対象外(NA)となることの理由」に、L2/L3 スイッチング機能を持たないと記載すること)。

1. **★３適合要件**

無許可の機器の接続を拒否するために、IEEE 802.1X 認証を用いた方式などにより接続する機器を一意に識別し、その結果に基づき接続を許可又は拒否できなければならない。

2. **補足説明**

2.1. 適合要件の補足説明

2.1.1. 機器の一意識別について

MAC アドレスなど、偽装が容易な情報を利用した方式は「機器の一意に識別可能な方式」とはみなさない。

2.2. 用語

該当事項なし

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①～③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)と、④のプロセスを有しなければならない。

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。
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。
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プロセスを有すること。

対象外(NA)となるための条件

該当事項なし

1. **★３適合要件**

脆弱性開示ポリシーについては一般に公開するものとし、そのなかで★３セキュリティ要件を満たすために必要な公開内容としては、以下の要件１～５のすべてを満たすこと。

要件１：

脆弱性開示ポリシーに、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:製造業者のウェブサイトの URL、電話番号、メールアドレス)が記載されていること。

要件２：

脆弱性開示ポリシーに、製造業者が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(詳細な手続き等までを公開する必要はないが、セキュリティに関する報告をどのように受付け、その後にその報告に対してどのような手続き・方法・期間で対応をするなどといった、公開することが求められる概要)が記載されていること。

要件３：

脆弱性開示ポリシーに、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(詳細な手続き等までを公開する必要はないが、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などといった、公開することが求められる概要)が記載されていること。

要件４：

脆弱性開示ポリシーは、一般からアクセス可能な媒体(ホームページなど)に掲載されていること。販売開始前の IoT 製品であって、評価時に脆弱性開示ポリシーが公開されていない場合は、公開の計画があること。公開の計画には、公開予定の脆弱性ポリシー及び公開の方法(例：公開予定の URL や掲載場所等)の情報を含むこと。

要件５：

重大な脆弱性、インシデントが発生している又は発生する恐れを認識した脆弱性について、速やかに IPA 又は指定機関に報告するプロセスを有すること。

2. 補足説明

2.1. 適合要件の補足説明

2.1.1. 脆弱性開示ポリシーを一般に公開する意義

脆弱性開示ポリシーを一般に公開する意義は、製造業者自らでは把握していなかった潜在的な脆弱性を外部のセキュリティ研究者やエンジニアなどが発見した場合に、安心して報告してもらう環境を整えることにある。

具体的には、製造業者にとっては、脆弱性情報を早期に入手できる手段が広がり、迅速に脆弱性対策をできるようになると期待される。一方、製造業者が報告を受けた脆弱性に対してどのような対応をするのかを予め公表しておくことで、脆弱性の発見者にとっては、報告した脆弱性情報が適切に取り扱われるという安心感を与えることができる。

このような意義を考慮し、JC-STAR では、とりわけ

- 脆弱性情報の報告先
- 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(特に報告を受領した際の「受領通知」を送るまでの期間)
- 脆弱性が解決されるまでの IoT 製品及び脆弱性の状況更新に関する手続き及びその概要(特に対応状況をどの程度の頻度で(透明性を確保しつつ)行うか/連絡するか)

の公表を求めることとしている。

脆弱性開示ポリシーの参考情報としては、ISO/IEC 29147:2018(PSTI 法[4]では、そのなかの6.2.2項、6.2.5項、6.5項を指定)、Vulnerability Disclosure Policy Template[5]、ETSI EN 303 645 の 5.2-1 項がある。

なお、「脆弱性開示ポリシーを公開」することと「脆弱性情報を公開」することとは意味が異なることに留意されたい。

[4] https://www.legislation.gov.uk/uksi/2023/1007/schedule/2/paragraph/2
[5] https://www.cisa.gov/vulnerability-disclosure-policy-template

2.2. 用語

該当事項なし

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 製品に含まれるファームウェア(ソフトウェア)パッケージのアップデート機能について、以下の①～④のすべての要件を満たさなければならない。

① 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 オンラインアップデートを行える場合には自動アップデート機能を有すること。

対象外(NA)となるための条件

脆弱性対応をアップデートではない代替手段によって行う(「対象外(NA)となることの理由」に、アップデートによらずに脆弱性対応ができることの根拠を記載すること)。

1. **★３適合要件**

ソフトウェアのアップデート機能について、★３セキュリティ要件を満たすアップデートが実行できるようにするために、以下の要件１～４のすべてを満たすこと。なお、必須付随サービス以外の外部システム連携によって自動アップデートを行う機能を有する場合は、要件１～４に加え、要件５を満たすこと。

要件１：

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機能を有すること。

要件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。又は、最新のファームウェア(ソフトウェア)へのアップデートが実施されていないことの警告を自動表示する機能を有すること。

要件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。

要件４：

ネットワークを介してファームウェア(ソフトウェア)のアップデートを行う場合には、自動アップデートの機能を有すること。

要件５：

必須付随サービス以外の外部システム連携によって自動アップデートを行う機能を有する場合には、以下の要件をすべて満たすこと。

A) 自動アップデートを行うための信頼できる外部システム連携が可能な条件を明示した文書をユーザに提供すること。そのうち、少なくとも一つは技術的に確認できる条件であること。

B) IoT 機器は、自動アップデートを行うために連携する外部システムが A)の技術的に確認できる条件を満たすことを検証する機能を有すること。

C) IoT 機器は、自動アップデートを行うために連携する外部システムとの通信において、S3.1-20 に準拠していること。

D) B)及び C)の機能・対策はデフォルトで有効であること。

E) 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、B)の機能を利用して外部システム連携を行うための手順を開示すること。

2. 補足説明

2.1. 適合要件の補足説明

2.1.1. 自動アップデート機能を初期状態で有効状態について

アップデートを実行するとき、通信機器の再起動のために一時的な機能停止などが発生する場合がある。一時的な機能停止がユーザの意図に反して不適切なタイミングで発生することを防止する必要がある場合を鑑み、自動アップデート機能を初期状態で有効にすることは求めない。

2.2. 用語

該当事項なし

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。

対象外(NA)となるための条件

脆弱性対応をユーザによるアップデートではない代替手段によって行う(「対象外(NA)となることの理由」に、ユーザによるアップデートによらずに脆弱性対応ができることの根拠を記載すること)。

1. **★３適合要件**

ソフトウェアのアップデートについて、★３セキュリティ要件を満たす容易かつ分かりやすい手順で実行できるようにするために、以下の要件１～４のいずれかを満たすこと。なお、複数のアップデート方法を採用している場合には、それぞれについて該当する要件を満たすこと。

要件１：

ユーザに自動的にアップデートが実行されることがマニュアル等で周知されていること。また、自動アップデートに失敗した場合の対応方法も周知されていること。

要件２：

アップデートを行うユーザに、IoT 製品の必須付随サービス(モバイルアプリケーション等)を利用してアップデートを実行する手順がマニュアル等で周知されていること。

要件３：

アップデートを行うユーザに、IoT 製品のインタフェース(ウェブインタフェース等)を介してアップデートを実行する手順がマニュアル等で周知されていること。

要件４：

アップデートを行うユーザに、製造業者のウェブサイトからアップデートファイルをダウンロード等の方法により、アップデートファイルを入手し、インストールによるアップデートを実行する手順がマニュアル等で周知されていること。

2. **補足説明**

2.1. 適合要件の補足説明

2.1.1. 「容易かつ分かりやすい手順」について

本適合要件で求めている、容易かつ分かりやすい手順とは、専門的知識を有しないユ

ーザであっても、インストーラやマニュアル、作業手順書等の指示に従えば、通常はアップデートが成功するように作られている手順のことを意味する。

2.1.2. 「アップデートを行うユーザ」について

アップデートを行うユーザの範囲は、IoT 製品により異なる可能性がある。本適合要件での対象は、ユーザの中でも「アップデートを行うユーザ」に限定して、そのユーザに対して手順が周知されていればよい。

例えば、カスタマーエンジニアがアップデートを行う IoT 製品であれば、カスタマーエンジニアに対してアップデートを行う手順が周知されていればよく、必ずしも当該製品の利用者に周知する必要はない。一方、自動アップデートや利用者にアップデートを行わせる場合には、利用者に手順が周知されている必要がある。

2.2. 用語

【ユーザ】

ユーザの対象範囲には、IoT 製品の利用者、管理者、製造業者のカスタマーエンジニア、所有者等、当該 IoT 製品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の①から③のすべての要件を満たす機能を実装しなければならない。

① アップデート前にソフトウェアの完全性及び真正性を確認できる仕組みを IoT 製品が有すること。

② 真正性もしくは完全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。

対象外(NA)となるための条件

脆弱性対応をアップデートではない代替手段によって行う(「対象外(NA)となることの理由」に、アップデートによらずに脆弱性対応ができることの根拠を記載すること)。

1. **★３適合要件**

ソフトウェアのアップデートについて、★３セキュリティ要件を満たすためのアップデートをセキュアに実行する仕組みとして、以下の「要件１又は要件２のいずれかに類する仕組み又はそれ以上の仕組み」が実装されており、かつ「要件３及び要件４」を満たすこと。

要件１：

更新ソフトウェアでアップデートする前又はアップデート中に、更新ソフトウェアに付与されたデジタル署名又は完全性と真正性を同時に確認できるメッセージ認証による検証を行い、検証の結果、検証 NG が確認された場合にはアップデートが中止されること。

要件２：

更新ソフトウェアでアップデートする前に、PC やスマートフォン等の関連アプリケーションにおいて、更新ソフトウェアに付与されたデジタル署名による検証を行い、検証の結果、検証 NG が確認された場合にはアップデートが中止されること。

要件３：

要件 1、要件２で利用するデジタル署名又はメッセージ認証で使用する暗号技術は、「電子政府における調達のために参照すべき暗号のリスト(CRYPTREC 暗号リスト)」のうち「電子政府推奨暗号リスト」に記載された暗号技術であって、「暗号強度要件(アルゴリズム及び鍵長選択)に関する設定基準」の規定に合致する鍵長を用いた暗号技術を使用すること。

要件４：

更新ソフトウェアでアップデートする前に、更新ソフトウェアのバージョンを確認し、現

在のバージョンと同じ又は以前のバージョンであることが確認された場合にはアップデートが中止されること。なお、本要件は、必要に応じて過去のバージョンのソフトウェアをインストールする手段を有することを妨げないが、デフォルトで過去のバージョンの更新ソフトウェアでアップデート可能としてはならない。

2. 補足説明

2.1. 適合要件の補足説明

2.1.1. 完全性と真正性を同時に確認できるメッセージ認証

メッセージ認証の仕組みのなかでも「鍵付メッセージ認証」と呼ばれるものであり、送信者(本適合要件では更新ソフトウェアの提供サーバが該当)と受信者(IoT 機器に該当)だけが同じ秘密情報を所有している場合に、その秘密情報を使ってメッセージ認証を行う方式のことである。ただし、この秘密情報は一意の送信者と受信者だけが共有していなければならないため、本適合要件で使う場合には IoT 機器ごとに異なる固有の秘密情報を設定する必要がある。つまり、IoT 機器共通の秘密情報を使ってこの仕組みを採用することはできない。

2.2. 用語

該当事項なし

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しなければならない。

対象外(NA)となるための条件

該当事項なし

1. **★３適合要件**

セキュリティ課題への対応について、★３セキュリティ要件を満たすためのセキュリティ課題に対する迅速なアップデートを実現するための仕組みとして、以下の要件１～３のすべてを満たすこと。

要件１：

対応する脆弱性の深刻度や重要度の判断指標、脆弱性の種類(例：ファームウェア、ハードウェア、ソフトウェアなど)等のセキュリティアップデートの優先度を決定するための指針が規定されていること。

要件２：

インシデントレスポンスをハンドリングするための組織体制(PSIRT、インシデント対応体制等)、及び脆弱性情報の収集、トリアージや分析、対策、アップデートなど、一連の対応プロセスや方針が規定されていること。

要件３：

複数のステークホルダー(*1)によって開発・運用されている製品の場合に、ステークホルダー間の連絡体制(連絡先、連絡方法など)が記載されていること。

(*1)：ソフトウェアサプライチェーンのパートナー、製品のサービスに関わるプロバイダ等

2. **補足説明**

2.1. 適合要件の補足説明

該当事項なし

2.2. 用語

該当事項なし

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。

① IoT 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。

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、ユーザが型番及びシリアル番号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

該当事項なし

1. **★３適合要件**

製品の型番について、★３セキュリティ要件を満たすための情報提供の仕組みとして、以下の要件１又は要件２のいずれかを満たすこと。

要件１：

製品本体に当該製品の型番及びシリアル番号が記載されていること。

要件２：

製品の GUI、ウェブ UI 等や、製品に付帯するソフトウェア、アプリケーション(スマホアプリなど)の GUI、ウェブ UI 等に実際にアクセスすることで、当該製品の型番及びシリアル番号を確認できる仕組みがあること。

2. **補足説明**

2.1. 適合要件の補足説明

2.1.1. 「製品本体への直接記載」について

製品本体への直接記載は、ラベル貼付による記載でも適合とみなす。

2.2. 用語

【ユーザ】

ユーザの対象範囲には、IoT 製品の利用者、管理者、製造業者のカスタマーエンジニア、所有者等、当該 IoT 製品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①～④のすべての要件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うえで、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。

④ 製品出荷後に正規のアップデート以外の手段によってソフトウェアをインストールできないようにしておくこと、又は許可されたソフトウェアのみがインストールできる仕組みを設けること。

対象外(NA)となるための条件

該当事項なし

1. **★３適合要件**

サードパーティコンポーネントを含めたソフトウェア管理について、★３セキュリティ要件を満たすためのソフトウェア識別情報及びコンポ―ネント情報等を含んだソフトウェア部品表(SBOM)の作成、運用に関する仕組みとして、以下の要件１～８のすべてを満たすこと。

要件１：

サードパーティコンポーネントを含めたすべてのコンポーネントを対象に、機械可読な形式及びヒューマンリーダブルな SBOM を作成、生成するプロセスを規定していること。

要件２：

要件１に基づいて SBOM が作成されていること。

要件３：

作成した SBOM に基づいて、使用されるコンポーネント(サードパーティコンポーネントを含む)に、脆弱性が含まれる古いバージョンのものが含まれていないかを定期的に確認するプロセスを規定していること。また、サポート期間内において SBOM を更新することを規定していること。

要件４：

脆弱性が含まれるコンポーネントが検出された場合に、製品への影響から対応優先度を判断し、更新もしくは運用対処を決定するプロセスを規定していること。

要件５：

作成した SBOM に基づいて、使用されるコンポーネント(サードパーティコンポーネントを含む)のライセンス管理を行うプロセスを規定していること。

要件６：

製造業者は「定期的な脆弱性の確認」を行うために、セキュアな管理として十分であると想定する頻度を規定していること。

要件７：

要件１及び要件３～６について、技術文書等に明示されていること。

要件８：

要件８－１又は要件８－２を満たすこと。

要件８―１：

正規のアップデート以外の手段によってソフトウェアをインストールできないように設定をし、かつその設定を変更できないようにすること。

要件８―２：

正規のアップデート以外の手段でのソフトウェアのインストールを許可する場合には、以下の条件すべてを満たすこと。

① ユーザはインストールを許可された場合のみソフトウェアのインストールができる仕組みを設けること
② インストール可否の設定変更は管理者のみが実行できる仕組みとすること
③ インストールを許可する権限を管理者がユーザに与える仕組みを設けること
④ 製品出荷時にはインストール不可をデフォルト設定としておくこと

2. 補足説明

2.1. 適合要件の補足説明

2.1.1. SBOM の適用範囲

A) IoT 機器：対象となる IoT 機器のファームウェア

B) 必須付随サービス：製造業者がアップデートの責任を有するソフトウェア

2.1.2. SBOM を記述する階層について

SBOM の作成においてグローバルなベストプラクティスとなる基準が存在しないため、本適合要件においては SBOM が扱う階層レベルについて定めず、通常想定される脆弱性の管理に適した範囲で、製造業者が個別に判断してよいものとする。ただし、今後の SBOM の動向によっては階層レベルを定めることはあり得ることに留意されたい。

例） SBOM の記述対象を、主要コンポーネントと直接の依存関係のあるコンポーネントまでとした場合、以下の例のように、直接の依存関係があるコンポーネントまでを記述する。

A) 静的依存関係の例
- コンパイル時に必要となるライブラリやヘッダーファイル等のコンポーネント
- プログラムが外部ライブラリやファイルとのリンク時に必要となるコンポーネント
- パッケージマネージャー使用時にプログラミング環境が必要とするコンポーネント

B) 動的依存関係の例
- プラグインによる機能追加によって含まれるコンポーネント
- 動的リンクライブラリ(DLL)や共有ライブラリなどのコンポーネント
- JavaScript など、動的に生成されるコンポーネント

C) リモート依存関係の例
- インターネット経由でアクセスされるリソースやサービスなどのコンポーネント

2.1.3. SBOM のデータフィールドの例

CISA が最小要素として定義したデータフィールドの例を以下に示す。

- SBOM Author(SBOM 作成者)
- Software Producer(ソフトウェア開発元)
- Component Name(コンポーネント名)
- Component Version(コンポーネントバージョン)
- Software Identifiers(ソフトウェア識別子)
- Component Hash(コンポーネントハッシュ)
- License(ライセンス)

- Dependency Relationship(依存関係)
- Tool Name(ツール名)
- Timestamp(タイムスタンプ)
- Generation Context(生成コンテキスト)

2.1.4. SBOMのフォーマットの例

1) 構造フォーマットの例

SBOM に必要なデータフィールドを満たすフォーマットの標準規格として、以下に準拠を推奨するフォーマットの例を示す。

- CycloneDX
- Software Package Data Exchange(SPDX)
- SPDX Lite ※手動でSBOMを作成する場合を想定

2) ファイルフォーマットの例

機械可読が可能な、SBOMのファイルフォーマットの例を、以下に示す。

- CycloneDXの場合：JSON、XML、Protocol Buffers(Protobuf)
- SPDXの場合：SPDX Tag/Value、RDF/XML、YAML、JSON
- SPDX Liteの場合：SPDX Tag/Value、RDF/XML、YAML、JSON

2.1.5. SBOMに含まれるコンポーネントの脆弱性の確認方法の例

A) ソフトウェアコンポーネント解析(SCA)ツールを活用した脆弱性の解析

※解析方法はバイナリ解析、ソースコード解析など、ツールによって異なる。

B) JVNなどの脆弱性報告サイトを活用した手動による確認

2.2. 用語

該当事項なし

カテゴリ４ ： SSP(Sensitive Security Parameter)を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セキュア保存情報(SD カード等、ストレージメディアに保存されるセキュア保存情報も含む。)は、セキュアに保存されなければならない。

対象外(NA)となるための条件

該当事項なし

1. **★３適合要件**

ストレージに保存されるセキュア保存情報に対する、★３セキュリティ要件を満たすためのセキュアに保存する仕組みとして、すべてのセキュア保存情報が、情報資産ごとに、以下の要件１及び「要件２～６のいずれかに類する保護対策又はそれ以上の対策」を満たすこと。加えて、リムーバルストレージを利用可能な場合には、要件７及び要件８も満たすこと。

なお、情報資産ごとに異なる対策を採用してもよい。また、複数の対策を併用してもよい。

要件１：

セキュア保存情報のうち、下記の情報資産については「機密性の保護」を行うこと。

- CSP(Critical 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
- 監査ログ

要件２：

機密性の保護が必要なセキュア保存情報は、「電子政府における調達のために参照すべき暗号のリスト(CRYPTREC 暗号リスト)」のうち「電子政府推奨暗号リスト」に記載された暗号技術であって、「暗号強度要件(アルゴリズム及び鍵長選択)に関する設定基準」の規定に合致する鍵長を用いた暗号技術による暗号化又はハッシュ化されて保存されること。

要件３：

完全性の保護が必要なセキュア保存情報は、「電子政府における調達のために参照すべき暗号のリスト(CRYPTREC 暗号リスト)」のうち「電子政府推奨暗号リスト」に記載された暗号技術であって、「暗号強度要件(アルゴリズム及び鍵長選択)に関する設定基準」の規定に合致する鍵長を用いた暗号技術を採用した署名によってデータの完全性が確認できる形で保存されること。

要件４：

完全性の保護が必要なセキュア保存情報は、「電子政府における調達のために参照すべき暗号のリスト(CRYPTREC 暗号リスト)」のうち「電子政府推奨暗号リスト」に記載された暗号技術であって、「暗号強度要件(アルゴリズム及び鍵長選択)に関する設定基準」の規定に合致するハッシュ関数を用いたメッセージ認証によってデータの完全性が確認できる形で保存されること。

要件５：

セキュア保存情報は、仮想化技術、iOS/Android 等の OS の機能として提供されるサンドボックス、又はセキュリティチップによるセキュア領域に保存されること。

要件６：

セキュア保存情報は、IoT 機器に組み込まれた容易に取り外せないストレージ領域にあって、外部から呼び出すインタフェースを経由した直接的なデータの読み書きができない領域又はそのようなインタフェースを備えない領域に保存されること。

要件７：

リムーバルストレージにセキュア保存情報の保存ができる機能を有する場合、「要件１」及び「要件２～４」を満たすように保存すること。

要件８：

他の機器でも読み込み可能な形式でリムーバルストレージに情報を保存できる機能を有する場合には、適切なアクセス制御のもとで必要な範囲でのみ読み込み可能な形で保存する仕組みを備えること。

2. 補足説明

2.1. 適合要件の補足説明

該当事項なし

2.2. 用語

【セキュア保存情報】

以下の情報のこと。2.4 節を参照。

- CSP(Critical Security Parameter)
- PSP(Public 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

- プログラムコード
- ログ(テレメトリデータ・監査ログ)

セキュリティ要件番号 ： S3.1-17

★３セキュリティ要件

IoT 製品で使用する CSP(Critical Security Parameter)は IoT 機器にハードコードしてはならない。

また、IoT 機器にハードコードされた PSP(Public 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、以下の①・②のすべての要件を満たさなければならない。

① IoT 機器にハードコードされた PSP(Public Security Parameter)の全容を把握し、一覧化できていること。

② ①の一覧に記載されたすべての PSP(Public 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

ハードコードした CSP(Critical Security Parameter)や PSP(Public Security Parameter)が存在しない(「対象外(NA)となることの理由」に、ハードコードした CSP(Critical Security Parameter)や PSP(Public Security Parameter)が存在しないことを明示すること)。

1. **★３適合要件**

★３セキュリティ要件を満たすためには、いかなる CSP もハードコードされていてはならないことを確認するため、以下の要件１を満たすこと。

また、ハードコードされた PSP がある場合、★３セキュリティ要件を満たすための PSP の保護手段として、以下の要件２及び要件３のすべての要件を満たすこと。ハードコードされた PSP がない場合、要件２及び要件３は対象外とする。

要件１：

いかなる CSP もハードコードされていないこと。

要件２：

ハードコードされた PSP が一覧化されていること。

要件３：

すべてのハードコードされた PSP が、以下のいずれかの手段により改ざんから保護されていること。

- Trusted Platform Module(TPM)やセキュアエレメントなど物理的な保護
- センサ検知後のデータ消去など電気的なタンパー応答の仕組みによる保護
- 暗号技術を利用したソフトウェア的な保護。ただし、「電子政府における調達

のために参照すべき暗号のリスト(CRYPTREC 暗号リスト)」のうち「電子政府推奨暗号リスト」に記載された暗号技術であって、「暗号強度要件(アルゴリズム及び鍵長選択)に関する設定基準」の規定に合致する鍵長を用いた暗号技術を用いている場合に限る。

2. 補足説明

2.1. 適合要件の補足説明

該当事項なし

2.2. 用語

【CSP(Critical Security Parameter)】

【PSP(Public Security Parameter)】

2.4 節を参照。

セキュリティ要件番号 ： S3.1-18

★３セキュリティ要件

ソースコードに直接記述された 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、以下の①・②のすべての要件を満たさなければならない。

① ソースコードに直接記述されている SSP(Sensitive Security Parameter)の全容を把握し、一覧化できていること。

② SSP(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(「対象外(NA)となることの理由」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)。

1. **★３適合要件**

ソースコードに直接 SSP が記述されている場合に、★３セキュリティ要件としてソースコードに CSP が含まれていないことを確認するため、以下の要件１及び要件２のすべてを満たすこと。

要件１：

ソースコードに直接記述されている SSP が一覧化されていること。

要件２：

一覧化された SSP に、運用中(*1)に利用される CSP(Critical Security Parameter)が含まれていないこと。

(*1)IoT 製品の運用中:

IoT 製品がユーザによって利用されている期間のこと。開発時や出荷前テスト、故障解析時などを除く。

2. **補足説明**

2.1. 適合要件の補足説明

該当事項なし

2.2. 用語

【CSP(Critical Security Parameter)】

【PSP(Public Security Parameter)】

2.4 節を参照。

【SSP(Sensitive Security Parameter)】
CSP と PSP を合わせた情報資産のこと。

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、及び必須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 機器ごとに固有でなければならない。

対象外(NA)となるための条件

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、及び必須付随サービスとの通信の保護で CSP を利用しない場合(「対象外(NA) となることの理由」に、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、及び必須付随サービスとの通信の保護で CSP を使用していないと記載すること)。

1. **★３適合要件**

IoT 製品のファームウェア(ソフトウェア)パッケージのアップデートの完全性及び真正性の検証や、暗号通信で利用する暗号鍵の共有などに使用する CSP(Critical Security Parameter)については、IoT 製品に対する自動化された攻撃のリスクを低減するために、以下の要件１及び要件２の両方を満たすこと。

要件１：

ファームウェア(ソフトウェア)パッケージのアップデートの完全性及び真正性チェックや､暗号通信で利用する暗号鍵の共有などに使用する CSP(Critical Security Parameter)が自動化された攻撃に対して耐性があるように生成されていること。

要件２：

要件１で生成される CSP(Critical Security Parameter)が IoT 機器ごとに固有であること。

2. **補足説明**

2.1. 適合要件の補足説明

本適合要件では､ファームウェア(ソフトウェア)パッケージのアップデートの完全性及び真正性のチェックに鍵付きメッセージ認証コードを利用する場合には､同じ製品クラスの IoT 製品であってもそれぞれ異なる CSP を割り当てることを求めている。一方、ファームウェア(ソフトウェア)パッケージのアップデートの完全性及び真正性のチェックにデジタル署名を利用する場合には、IoT 製品では CSP を使わないことに留意されたい。

2.2. 用語

【CSP(Critical Security Parameter)】

2.4節を参照。

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機密通信情報について以下の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。

① IoT 製品は機密通信情報の通信先の正当性を確認すること。

② 機密通信情報は、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こと。

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機密通信情報がない(「対象外(NA)となることの理由」に、ネットワーク経由で伝送される機密通信情報がないことを記載すること)。

1. **★３適合要件**

機密通信情報に対する、★３セキュリティ要件を満たすための通信の保護対策として、以下の要件１～６のすべてを満たすこと。IoT 製品と連動するアプリがある場合、アプリから送信される機密通信情報も通信先の正当性、及び情報の盗聴・改ざんに対する保護の対象とする。

要件１：

IoT 製品が、適切な認証によって通信先の正当性を確認すること。

要件２：

以下の A)又は B)のいずれかの対策をとっていること。

A) IoT 製品が機密通信情報を送受信する場合においては、「電子政府における調達のために参照すべき暗号のリスト(CRYPTREC 暗号リスト)」のうち「電子政府推奨暗号リスト」に記載された暗号技術であって、「暗号強度要件(アルゴリズム及び鍵長選択)に関する設定基準」の規定に合致する鍵長を用いた暗号技術を採用し、機密性と完全性を確保した通信プロトコルにて伝送すること。

B) S3.1-16 の要件２に準拠した暗号化をされたうえで保存された機密通信情報を復号せずにネットワークを経由して伝送すること。また、機密通信情報の完全性を「電子政府における調達のために参照すべき暗号のリスト(CRYPTREC 暗号リスト)」のうち「電子政府推奨暗号リスト」に記載された暗号技術であって、「暗号強度要件(アルゴリズム及び鍵長選択)に関する設定基準」の規定に合致する鍵長を用いた暗号技術によって確保すること。

要件３：

暗号化プロトコルで TLS を使用している場合は、CRYPTREC が公開している「TLS 暗号設定

ガイドライン」に記載されている、「推奨セキュリティ型」以上のプロトコルバージョンと暗号スイートの遵守項目を満たすこと。

要件４：

要件１～３の対策がデフォルトで有効に設定されていること。

要件５：

設定によって IoT 製品が利用可能な非暗号化プロトコルが一覧化されていること。また、それらがデフォルトでは利用不可となっていること。

要件６：

要件５でデフォルト無効化されている非暗号化プロトコルを利用できるようにするために、識別認証された特別な権限(管理者権限等)をもったユーザによってのみ有効化できる仕組みを有すること。また、有効化した場合のリスクなどセキュリティ上の注意がユーザにわかるように設定変更の方法を説明する箇所(例えばマニュアルなど)に周知すること。

2. 補足説明

2.1. 適合要件の補足説明

2.1.1. ネットワーク経由で伝送されない機密通信情報の例

リンクローカルアドレスを利用して、ネットワーク上で論理的に 1 対 1 の直接通信を実現して機密通信情報のやり取りを行う場合であっても、「ネットワーク経由で伝送される機密通信情報である」とみなされることに留意すること。

シリアルポートや USB 等を使い、物理的に 1 対 1 でしか接続できない方法を用いて機密通信情報のやり取りを行う場合に限り、「ネットワーク経由で伝送される機密通信情報ではない」とみなす。

2.2. 用語

【機密通信情報】

以下の情報のこと。2.4 節を参照。

- CSP(Critical 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
- アラート情報
- 監査ログ

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。

対象外(NA)となるための条件

該当事項なし

1. **★３適合要件**

CSP について、★３セキュリティ要件を満たすライフサイクルを実現するために、以下の要件１及び要件２のすべてを満たすこと。

要件１：

利用する CSP(Critical Security Parameter)について、ライフサイクルを定義し、それらの管理手法について実施すべきセキュアなプロセスを技術文書等に明示すること。

要件２：

CSP をセキュアに更新するためのプロセスを技術文書等に明示すること。

2. **補足説明**

2.1. 適合要件の補足説明

2.1.1. CSP(Critical Security Parameter)のライフサイクル・管理の例

IPA が発行する鍵管理ガイドライン「暗号鍵管理システム設計指針(基本編)」等を参考に定義を行う。暗号鍵のライフサイクル・暗号鍵のライフサイクル管理機能などが参考となる。

2.2. 用語

【CSP(Critical Security Parameter)】

2.4 節を参照。

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 IEEE 802.1X 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 製品に無線 LAN 機能を持たない(「対象外(NA)となることの理由」に、無線 LAN 機能を持たないことを記載すること)。

1. **★３適合要件**

無線 LAN による通信について、★３セキュリティ要件を満たすための通信の保護対策として、以下の要件１～４のすべてを満たすこと。

要件１：

WPA3 Enterprise(Wi-Fi Protected Access 3 Enterprise)、又は WPA2 Enterprise(Wi-Fi Protected Access 2 Enterprise)方式をサポートしていること。

要件２：

無線通信区間では、WPA2 以上で接続する設定をデフォルトで有効としておくこと。

要件３：

WEP 及び WPA はサポートしないこと、又はデフォルトで無効化しておくこと。

要件４：

IEEE 802.1X 認証で用いる EAP(PPP Extensible Authentication Protocol)の規格が TLS、TTLS、PEAP、又は EAP-FAST の認証方式をサポートしていること。

2. **補足説明**

2.1. 適合要件の補足説明

該当事項なし

2.2. 用語

該当事項なし

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のすべての要件を満たさなければならない。

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

該当事項なし

1. **★３適合要件**

サイバー攻撃を受けるリスクを低減するために、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、攻撃に悪用される可能性がある既知の脆弱性がない状態にするため、以下の要件１～４のすべてを満たすこと。

ただし、要件４において脆弱性が検出された場合は要件５を実施し、検出された脆弱性が攻撃に悪用される可能性があるかどうかの評価を行う。その評価により問題がないと判断された場合には「要件４は満たしている」と判定する。

要件１：

製品に搭載し、設定により利用可能となる以下のインタフェースに応じ、A)～C)の要件をすべて満たすこと。そのインタフェースがデフォルトで利用可能であるか否かは問わない。

A) TCP/UDP を搭載し利用可能である場合、以下の要件をすべて満たすこと。

- インバウンド通信において、デフォルトで開放(LISTEN)している TCP・UDP ポートについて、対象のポート番号、通信プロトコル、利用用途、開放タイミング及び利用条件が技術文書等に明示されていること。なお、IPv6 に対応した製品の場合は、IPv4 と IPv6 の両方を対象とする。
- 開放しているポートの中に利用する必要性がないポートや利用目的がはっ

きりしないポート等、利用上、デフォルトで開放しておくことが不要なポートが含まれていないこと。

B) Bluetooth を搭載し利用可能である場合、以下の要件をすべて満たすこと。
- すべての利用可能なBluetooth プロファイルが技術文書等に明示されていること。
- デフォルトで利用するBluetooth プロファイル、利用目的が技術文書等に明示されていること。
- デフォルトで利用するBluetooth プロファイルの中に利用上不要なプロファイルが含まれていないこと。

C) USB を搭載し利用可能である場合、以下の要件をすべて満たすこと。
- すべての利用可能なUSB デバイスクラスのクラス名が技術文書等に明示されていること。
- デフォルトで利用するUSB デバイスクラスのクラス名、利用目的が技術文書等に明示されていること。
- デフォルトで利用するUSB デバイスクラスの中に利用上不要なデバイスクラスが含まれていないこと。

要件２：

以下の要件をすべて満たすこと。
- 製品に搭載されているものの物理的対策又はそれに準ずる手段により、利用できる状態に変更できないインタフェース(無効化インタフェース)があれば、対象の無効化インタフェース及び無効化の手段を明確にすること。そのようなインタフェースがなければ、「物理的対策等による無効化インタフェースはない。」ことを明確にすること。
- 技術文書等に、無効化インタフェース及び無効化の手段の情報が明示されていること。

要件３：

以下の要件をすべて満たすこと。
- デフォルトで攻撃に悪用されるリスクの特に高いポート(例えばtelnet(23/TCP 及び 2323/TCP)等)を利用している場合には、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が存在すること。そのようなポートを利用していなければ、「攻撃に悪用されるリスクの特に高いポートは利用していない。」ことを明確にすること。
- 技術文書等に、その管理プロセスに関して明示されていること。

要件４：

脆弱性検査について、以下の要件をすべて満たすこと。

i) 開放されている TCP/UDP ポートについて、CVSSv3 基準 Severity 4.0 以上の脆弱性が検出されていないことを確認すること。

ii) http/https プロトコルを使用する設定や機能が実装されている場合、下記 URL に一覧表示される既知の脆弱性 CVE-ID に該当する脆弱性が検出されていないことを確認すること。

[URL]

NIST：NATIONAL VULNERABILITY DATABASE

https://nvd.nist.gov/vuln/search

[検索条件]

Search Type：Advanced

Category：「CWE-78 OS Command Injection」「CWE-89 SQL Injection」「CWE-352 Cross-Site Request Forgery(CSRF)」「CWE-22 Path Traversal」「CWE-300: Channel Accessible by Non-Endpoint」「CWE-79: Improper Neutralization of Input During Web Page Generation('Cross-site Scripting')」「CWE-384: Session Fixation」のすべてを対象とする

iii) 必要に応じ、脆弱性検査ツールを利用して脆弱性検査を実施すること。その際、利用した脆弱性検査ツール及び検査結果を技術文書等に明示するとともに、脆弱性が検出されていないことを確認すること。

要件５：

要件４にて脆弱性が検出された場合、検出されたすべての脆弱性について以下の分析及び評価を行い、当該脆弱性が当該 IoT 機器の利用上は問題ないことを確認すること。検出されたすべての脆弱性について問題がないことが確認できれば、「脆弱性の問題がない」と判断する。

- 検出された脆弱性が誤検知であるかどうかの分析、及びその脆弱性が当該 IoT 機器の利用上は問題ないかどうかの評価。
- 別途の対策により、その脆弱性に対して既に対策済みであるとみなせるかどうかの分析、及びその対策によって当該 IoT 機器の利用上は当該脆弱性の問題がないかどうかの評価。
- 検出された脆弱性が、当該 IoT 機器の実際の利用環境においては影響がないことを証明可能であるかどうかの分析、及び影響がないことを証明するための評価。

2. 補足説明

2.1. 適合要件の補足説明

2.1.1. 要件２での、物理的対策により利用できる状態に変更できないインタフェースの例

- ユーザの通常利用に必要のない RJ45 や USB ポートを、セキュリティねじ等により容易に開けられないようになっている筐体やカバーによって外部露出から保護する。
- 機器への電力供給のみに使用される予定の USB ポートについて、コマンド又はデバッグ操作も許可しないように物理的に構成する(データ通信に利用される信号線を物理的に無効化するなど)。

2.1.2. 要件２での、物理的対策に準ずる手段により利用できる状態ではないインタフェースの例

- ドライバを削除し、インタフェースが利用できない状態になっている。
- インタフェースを無効化したうえで設定変更機能を削除または未実装とする。

2.2. 用語

該当事項なし

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

対象外(NA)となるための条件

該当事項なし

1. **★３適合要件**

サイバー攻撃を受けるリスクを低減するために、ネットワークを介して認証なしで閲覧可能なセキュリティ関連情報を必要最小限に制限するため、以下の要件１～４のすべてを満たすこと。

要件１：

デフォルトでネットワークを介して認証なしで閲覧可能なすべてのセキュリティ関連情報の一覧及び閲覧可能としている目的(当該セキュリティ関連情報を閲覧可能とすることの妥当な目的)が、技術文書等に明示されていること。

要件２：

目的に照らして、ネットワークを介して認証なしで閲覧可能なすべてのセキュリティ関連情報の範囲が必要最小限に制限されていること。閲覧可能とする必要性が乏しいセキュリティ関連情報が含まれていないこと。

要件３：

デフォルトでネットワークを介して認証なしで閲覧可能なすべてのセキュリティ関連情報の一覧について、マニュアル等のユーザがアクセス可能な媒体によってユーザに提供すること。

要件４：

ネットワークを介して認証なしで閲覧可能なすべてのセキュリティ関連情報の対象を変更できる設定を有している場合には、以下の情報についてもユーザに提供すること。

- 閲覧可否の設定変更が行えるセキュリティ関連情報
- 閲覧可否の設定変更手順

2. 補足説明

2.1. 適合要件の補足説明

該当事項なし

2.2. 用語

該当事項なし

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。

① IoT 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。

② IoT 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。

対象外(NA)となるための条件

該当事項なし

1. **★３適合要件**

サイバー攻撃を受けるリスクを低減するために、インタフェースに対する保護対策として、以下の要件１～４のすべてを満たすこと。

要件１：

機器の意図した利用において不必要な物理インタフェースを露出から保護する仕組みを有すること。

要件２：

デバッグインタフェースを物理的手段又は論理的手段で無効化していること。

要件３：

要件１及び要件２で実施した保護対策の概要について、技術文書等に明示していること。

要件４：

デバッグインタフェースを有効化するための手順及び条件が、技術文書等に明示されていること。

2. **補足説明**

2.1. 適合要件の補足説明

2.1.1. 物理インタフェースの露出からの保護の例

- ユーザの通常利用に必要のない RJ45 や USB ポートを、セキュリティねじ等により容易に開けられないようになっている筐体やカバーによって外部露出から保護する。
- 機器への電力供給のみに使用される予定の USB ポートについて、コマンド又はデバッグ操作も許可しないように物理的に構成する(データ通信に利用される信号線を物理的に無効化するなど)。

2.1.2. 対象となるデバッグインタフェースの例

- JTAG(Joint Test Action Group)　※IEEE1149.1 規格
- Compact JTAG　※IEEE1149.7 規格
- UART(Universal Asynchronous Receiver/Transmitter)
- SWD(Serial Wire Debug)
- FINE

2.1.3. デバッグインタフェースの無効化の例

製造業者のメンテナンスにおける一時的なデバッグインタフェースの無効化の解除を妨げるものではないことに留意されたい。

- 物理的無効化の例
  - インタフェースは強固な筐体の中にあり、筐体はセキュリティねじ等により容易に開けられないようになっている。
  - インタフェースはねじ止めされた蓋によってアクセスできないようになっている。
- 論理的無効化の例
  - 出荷時のファームウェアバージョンでは、デバッグインタフェースの設定を無効化する。
  - 出荷後にデバッグインタフェースの利用が必要とされる場合、コンソール機能を無効化し、ログ出力の範囲を最小限に設定したうえで、デバッグインタフェースの設定を有効にする。

2.2. 用語

該当事項なし

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。

対象外(NA)となるための条件

該当事項なし

1. **★３適合要件**

サイバー攻撃を受けるリスクを低減するために、不必要なサービスが動作していないことの確認として、以下の要件１～３のすべてを満たすこと。

要件１：

デフォルトで有効になっているすべてのサービス(バックグラウンドプロセス、カーネル拡張、コマンド、プログラム又はツールなど)が、対象機器の意図された使用、操作、又は必要とされるサービスにとって必要最小限であること。

要件２：

製品がサービス不能攻撃の踏み台として利用されるリクエスト(最低限 NTP の monlist コマンド、DNS ANY リクエスト、UPnP の SSDP)に応答しないこと。また、リフレクション攻撃に対する修正済みのバージョンを利用すること。

ただし、通信上必要で対策不可能なもの(SYN-ACK など)は対策から除外しても構わない。

要件３：

LAN 及び WAN インタフェースにおいて、不要なサービスをデフォルトで無効にすること。

2. **補足説明**

2.1. 適合要件の補足説明

該当事項なし

2.2. 用語

該当事項なし

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。

対象外(NA)となるための条件

該当事項なし

1. **★３適合要件**

セキュアなコーディングの一環として、コードの最小化を行うため、以下の A)又は B)のいずれかに類する手法を採用していること。

A) 自動化ツール(静的解析ツール、コンパイラ等)を使用して、デッドコード、不要なデバッグコードや未使用のコードを識別し、削除する。

B) パッケージマネージャー等を使用して、サービスやソフトウェアの操作に必要なコンポーネントのみをインストールする。

2. **補足説明**

2.1. 適合要件の補足説明

2.1.1. 適合要件の対象とするコードについて

本適合要件の対象とするコードは、自社開発したソースコードのみを対象とする。OSS などのサードパーティコンポーネントは対象外とする。

2.2. 用語

該当事項なし

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、以下のすべての要件を満たさなければならない。

① デフォルト権限の最小化
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。

対象外(NA)となるための条件

該当事項なし

1. **★３適合要件**

サイバー攻撃を受けるリスクを低減するために、ソフトウェアの利用権限の範囲を最小権限の原則に基づいて設定できることの確認として、デーモン/プロセスなどのデフォルトの権限が、最小になるよう設定されていること。

2. **補足説明**

2.1. 適合要件の補足説明

2.1.1. デフォルト設定における権限最小化の例である。

- 例１:「root」権限で実行される最小限のデーモン/プロセス。特に、ネットワークインタフェースを使用するプロセスには、「root」ユーザではなく、非特権ユーザを必要とする。
- 例２：マルチユーザオペレーティングシステム(例： Linux®)を含む機器上で動作するソフトウェアは、コンポーネントやサービスごとに異なるユーザを使用する。

2.2. 用語

【ユーザ】

ユーザの対象範囲には、IoT 製品の利用者、管理者、製造業者のカスタマーエンジニア、所有者等、当該 IoT 製品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、最低でも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定すること。
② コーディング規約を技術者に周知し教育を行うこと。
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こと。
④ コーディング規約や実装原則を更新すること。

対象外(NA)となるための条件

該当事項なし

1. **★３適合要件**

セキュアコーディングでソフトウェア開発が行われたことの確認として、以下の要件１～５のすべてを満たすこと。

要件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が規定されていること。

要件２：

コーディング規約を技術者に周知し教育を行うプロセスが存在すること。

要件３：

作成されたソースコードのレビュー・セキュリティテストを行うプロセスが存在すること。

要件４：

コーディング規約や実装原則を更新するプロセスが存在すること。

要件５：

開発されたソースコードが、上記要件１～４のプロセスを経て作成されていること。

2. **補足説明**

2.1. 適合要件の補足説明

2.1.1. 適合要件の対象とするコードについて

本適合要件の対象とするソースコードは、自社開発したソースコードのみを対象と

する。OSS などのサードパーティコンポーネントは対象外とする。

2.1.2. セキュリティに配慮したコーディング規約や実装原則

製造業者が以下にあげるような参考文書を参照し、ベストプラクティスに沿ったコーディング規約を整備していることを評価において確認する。

- セキュア・プログラミング講座（IPA）:
  https://www.ipa.go.jp/security/awareness/vendor/programming/index.html
- 安全なウェブサイトの作り方（IPA）:
  https://www.ipa.go.jp/security/vuln/websecurity.html
- セキュアコーディング（JPCERT/CC）:
  https://www.jpcert.or.jp/securecoding/
- SEC BOOKS ESCR Ver.3.0 組込みソフトウェア開発向けコーディング作法ガイド［C 言語版］ESCR Ver.3.0（IPA）:
  https://www.ipa.go.jp/sec/publish/tn18-004.html

2.2. 用語

該当事項なし

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①・②のすべての要件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(「対象外(NA)となることの理由」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)。

1. **★３適合要件**

脆弱性のあるサードパーティコンポーネントを使用しないため、S3.1-15 と併せて、以下の要件１及び要件２の両方を満たすこと。

要件１：

S3.1-15 要件２に基づき、利用しているサードパーティコンポーネントの SBOM が作成されていること。

要件２：

ファームウェア(ソフトウェア)パッケージ を開発する段階において、要件１で作成する SBOM を使用し、脆弱性のないサードパーティコンポーネントを組み込むこと。

2. **補足説明**

2.1. 適合要件の補足説明

該当事項なし

2.2. 用語

該当事項なし

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

対象外(NA)となるための条件

該当事項なし

1. **★３適合要件**

システム起動時にロードされるソフトウェアに対する、★３セキュリティ要件を満たすためのセキュアブートメカニズムとして、以下の要件１～４のすべての要件を満たすこと。

要件１：

デジタル署名又はそれと同等の対策を採用したセキュアブートメカニズムが実装されていること。

要件２：

実装されたセキュアブートメカニズムが、ソフトウェアの完全性保証を提供するのに適していること。

要件３：

デジタル署名又は暗号技術を利用する場合には、「電子政府における調達のために参照すべき暗号のリスト(CRYPTREC 暗号リスト)」のうち「電子政府推奨暗号リスト」に記載された暗号技術であって、「暗号強度要件(アルゴリズム及び鍵長選択)に関する設定基準」の規定に合致する鍵長を用いた暗号技術を採用していること。

要件４：

セキュアブートを利用するための設定手順などを示した情報をユーザが入手可能であること。

2. **補足説明**

2.1. 適合要件の補足説明

2.1.1. デジタル署名の検証に用いる証明書について

要件１においてデジタル署名の検証に用いる証明書は、信頼性が確保された証明書でなければならない。少なくとも、製造業者が正当であることを確認できる必要がある。そのような証明書には、公的証明書や製造業者自身が管理する、あるいは製造業者が契約しているCAが発行するルート証明書等がある。

2.1.2. セキュアブートに求める範囲

セキュアブートメカニズムに、ソフトウェアの真正性検証のための機能は求めない。

2.2. 用語

【ユーザ】

ユーザの対象範囲には、IoT製品の利用者、管理者、製造業者のカスタマーエンジニア、所有者等、当該IoT製品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 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、以下の要件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

IoT 機器にセンシングを行う機能がない場合(「対象外(NA)となることの理由」に、センシングを行う機能がないと記載すること)。

1. **★３適合要件**

通信機器が収集する個人情報のすべての種別がマニュアル、ウェブサイト等、ユーザがアクセス可能な媒体に明示されていること。特に、監査目的での監査ログにおける収集以外に個人情報の収集を行っている場合には、収集する個人情報の種別ごとに収集する目的と機能概要をユーザにわかりやすく説明しなければならない。

なお、本適合要件で対象となる個人情報は、デフォルトで収集するか否かによらず、すべてとする。

2. **補足説明**

2.1. 適合要件の補足説明

2.1.1. 通信機器にて想定されるセンシング機能の例

多要素認証で使用する生体情報センサーなど。

2.2. 用語

該当事項なし

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。

対象外(NA)となるための条件

該当事項なし

1. **★３適合要件**

予期せぬシステム障害に対して、★３セキュリティ要件を満たすための状態管理機能として、以下の要件１及び要件２のすべてを満たすこと。

要件１：

電源供給を停止させた(バッテリー駆動製品の場合、バッテリーを外すことで電源供給を停止させる)後、電源を復帰させたときに、工場出荷時の初期状態に戻ることなく、IoT 機器に保存されている認証値及び設定情報、ならびにアップデート状態が維持されていること。

要件２：

通信ケーブルや無線接続を強制切断後、再接続したときに、工場出荷時の初期状態に戻ることなく、IoT 機器に保存されている認証値及び設定情報、ならびにアップデート状態が維持されていること。

2. **補足説明**

2.1. 適合要件の補足説明

該当事項なし

2.2. 用語

該当事項なし

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。

対象外(NA)となるための条件

該当事項なし

1. **★３適合要件**

特定のタイミングでの設定状態に復旧できるように、★３セキュリティ要件を満たすための構成情報のバックアップ対策として、以下の要件１～３のすべてを満たすこと。

要件１：

バックアップ機能を有し、バックアップを実施した直前の構成情報(バックアップが必要と判断した設定値、認証値等)がバックアップファイルに保存されること。

要件２：

バックアップ機能によって正規に保存されたバックアップファイルのみから、バックアップを実施した直前の状態に復元できること。

要件３：

ユーザに対し、異なるバージョンのファームウェアでバックアップと復元を行った場合、IoT 機器が正常に作動しない可能性があること、バックアップ/復元を同一ファームウェアバージョンで行う旨の制限事項を周知していること。

2. **補足説明**

2.1. 適合要件の補足説明

該当事項なし

2.2. 用語

該当事項なし

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、以下の①～③のすべての要件を満たさなければならない。

① IoT 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、閾値を超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こと。

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、別途検討を行うこと。

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こと。

対象外(NA)となるための条件

該当事項なし

1. **<u>★３適合要件</u>**

セキュリティ上の異常検知に利用するために、★３セキュリティ要件を満たすためのログ(テレメトリデータ・監査ログ)の保護対策として、以下の要件１～４のすべてを満たすこと。必須付随サービスによって外部ストレージにログ保存を行う機能を有する場合は、要件１～４に加え、要件５を満たすこと。

また、必須付随サービス以外の外部システム連携によって外部システムにログ保存を行う機能を有する場合は、要件１～４に加え、要件５及び要件６も満たすこと。

<u>要件１：</u>

以下のセキュリティイベントすべてを対象とするログの取得機能及び保存機能が実装されていること。

A) 機器やネットワークの切断(再接続)の記録

B) ログイン試行(成功時、失敗時)の記録
C) 閾値を超えるログイン試行の記録
D) 時間変更時の記録(変更前と変更後の時刻を含む)
E) 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
F) ソフトウェア変更時の記録
G) ハードウェア変更時の記録(構成変更のログを記録する機能を有している場合)
H) 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)
I) 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)

要件２：

取得するログの保存容量、及び保存容量を超過した場合に継続してどのような処理が行われるのかを技術文書等に明示すること。なお、必須付随サービス又は外部システム連携によって外部ストレージにログ保存を行う場合であっても、通信障害により外部ストレージにログ保存ができない場合に備え、最低でも「通常想定される利用において 1 日程度のログ」を IoT 機器内に保存できる領域を確保すること。

要件３：

ログが保存容量を超過した場合に、ユーザが容易に視認できる警告表示又は通知を行うこと。

要件４：

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の時間管理機能、及び時刻ソースによる時刻同期機能が実装されていること。

要件５：

必須付随サービス又は外部システム連携によって外部ストレージなどの外部システムにログ保存を行う機能を有する場合には、以下の要件をすべて満たすこと。

A) 必須付随サービス・外部システムとのログにかかわる通信に対して、S3.1-20 要件１～３を満たす設定がデフォルトで有効であること。
B) 通信障害が解消した際に保存していたログを必須付随サービス・外部システムに自動的に送信すること。

要件６：

必須付随サービス以外の外部システム連携によって外部システムにログ保存を行う機能を有する場合には、以下の要件をすべて満たすこと。

A) ログ保存を行うための信頼できる外部システム連携が可能な条件を明示した文書をユーザに提供すること。そのうち、少なくとも一つは技術的に確認できる条件であること。

B) IoT 機器は、ログ保存を行うために連携する外部システムが A)の技術的に確認できる条件を満たすことを検証する機能を有すること。

C) B)の機能・対策はデフォルトで有効であること。

D) 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、B)の機能を利用して外部システム連携を行うための手順を開示すること。

2. 補足説明

2.1. 適合要件の補足説明

2.1.1. 構成変更によるハードウェア変更時の監査ログについて

「ハードウェア変更時の記録(監査ログ取得が可能な場合)」における「監査ログ取得が可能な場合」とは、インタフェースやストレージなどの IoT 機器の機能が変更されるユニットやモジュールの追加や変更が可能な IoT 機器において、ユニットやモジュールを追加、交換、抜去した際の構成変更のログを記録する機能を有している場合に、ハードウェア変更時の記録をもって監査ログとして利用できる場合のことである。

2.2. 用語

【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】

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のすべての要件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

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

該当事項なし

1. **<u>★３適合要件</u>**

製品利用中にストレージに保存された情報に対して、★３セキュリティ要件を満たすためのデータ削除機能として、以下の「要件１～３のすべて」又は「要件４～５のすべて」を満たし、かつ「要件６」を満たすこと。

<u>要件１：</u>

製品利用中に当該製品のストレージに保存されたユーザに関する少なくとも以下の A)～C)のすべての情報(データ)及び S3.1-32 で明示された個人情報のすべてを、ユーザが削除するための機能を有すること。ただし、ユーザに関する情報であっても、ユーザに公開されない IoT 製品の設定情報(製品特性として必要な情報)及び製造業者が IoT 製品の性能やシステムの健全性を監視するために生成される技術データはユーザが削除できる情報の対象外とする(例：Self-Monitoring, Analysis and Reporting Technology(S.M.A.R.T.)、バッテリーの充電サイクル数、エラー履歴など)。

A) ユーザが IoT 製品を利用している最中に取得した情報資産(個人情報含む)

B) ユーザに関するユーザ設定値

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

<u>要件２：</u>

データごとの用途、保存されるストレージに応じて適切に削除すること。削除レベルは、単純な非侵襲のデータ回復技術(市販のデータ復旧ソフトによるサルベージ等)から保護できる「Clear」レベル以上とする。

要件３：

要件１に記載された削除機能の利用手順を、マニュアル等のユーザがアクセス可能な媒体によってユーザに提供すること。

要件４：

要件１に該当する情報(データ)が保存されている IoT 機器又は必須付随サービスにおいて、ユーザ自らが直接転売することができない又は困難な IoT 機器・必須付随サービスである場合に限り、専門の業者や IoT 製品ベンダーに依頼して当該情報(データ)を削除してもらうための連絡先や手順をユーザが確認しやすい手段で提供すること。

要件５：

要件４により､ユーザに代わって専門の業者や IoT 製品ベンダーが代行して情報(データ)を削除する場合には、削除代行者が単純な非侵襲のデータ回復技術(市販のデータ復旧ソフトによるサルベージ等)から保護できる「Clear」レベル以上で当該情報(データ)を削除していることを確認するプロセスを構築すること。

要件６：

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。

2. 補足説明

2.1. 適合要件の補足説明

該当事項なし

2.2. 用語

【ユーザ】

ユーザの対象範囲には、IoT 製品の利用者、管理者、製造業者のカスタマーエンジニア、所有者等、当該 IoT 製品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。

対象外(NA)となるための条件

該当事項なし

1. **★３適合要件**

必要に応じて、初期状態である安全なデフォルト構成設定に戻すための仕組みとして、以下の要件１～３のすべてを満たしていること。

要件１：

デフォルト構成設定に復元できる機能を有すること。

要件２：

安全なデフォルト構成設定に復元できる手順を、マニュアル等のユーザがアクセス可能な媒体によってユーザに提供すること。

要件３：

デフォルト構成設定に復元する手順の中に、S3.1-36 要件１の機能を利用して復元以前の情報を削除する手順を組み入れること。この手順を実施するのが自動か手動かは問わない。

2. **補足説明**

2.1. 適合要件の補足説明

2.1.1. 「安全なデフォルト構成設定」とは

「安全なデフォルト構成設定」とは、製造業者が規定した安全な構成、設定を指す。

「安全なデフォルト構成設定に復元」の例：アップデートしたファームウェア以外の、ユーザが変更した設定値や運用中に変更された設定情報等が工場出荷時の状態に戻ること。

2.2. 用語

該当事項なし

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。

対象外(NA)となるための条件

該当事項なし

1. **★３適合要件**

入力データに対して、★３セキュリティ要件を満たすための不正な入力を拒否する対策として、以下のすべての要件を満たすこと。

要件１：

入力データを受け入れて処理するすべてのインタフェースが一覧化されているリストを作成すること。当該リストには少なくとも以下が含まれていること。

A) ユーザからのデータ入力を可能にするユーザインタフェース

B) 外部ソースからのデータ入力を可能にするアプリケーションプログラミングインタフェース(API)

C) リモートアクセス可能な通信方法に従ってデータ入力を可能にするネットワークインタフェース

要件２：

要件１で一覧化されたインタフェースごとに、入力データの入力規則や妥当性検証の内容が定義されていること。検証内容には以下が含まれていること。

A) 正しいタイプ(入力が許可されたデータ形式とデータ構造)

B) 入力が許可された値域、基数、順序

C) 入力が許可された基数

D) 入力が許可された順序

E) サニタイズやエスケープ処理、破棄など不正データに対する処理の方法

要件３：

入力検証(Validation)機能が、仕様通りに無効で不正なリクエストを拒否する機能が動作していること。

2. **補足説明**

2.1. 適合要件の補足説明

2.1.1. 入力データの妥当性検証に関する参考文書

OWASP 「Input Validation Cheat Sheet」
https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html

2.2. 用語

該当事項なし

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

個人情報を収集・処理する機能を有しない場合(「対象外(NA)となることの理由」に、個人情報を収集・処理する機能を有しないと記載すること)。

1. **★３適合要件**

個人情報を収集・処理する機能を有している場合、個人情報の処理を意図した必要最小限のものに留めるため、★３セキュリティ要件を満たすための周知する内容として、以下の要件１～５のすべてを満たすこと。

要件１：

個人情報の処理のために IoT 製品が収集する個人情報のすべての種別を技術文書等に明示すること。

要件２：

要件１で明示した、収集される個人情報のすべてに対してどのような処理を行うのかを技術文書等に明示すること。

要件３：

要件２の内容によって処理された結果についてどのような取扱い方法(保存方法、提供方法、通知方法、削除方法など)で処理されるかを技術文書等に明示すること。

要件４：

要件１～３についてユーザにわかりやすく説明する資料を、マニュアル、ウェブサイト等のユーザがアクセス可能な媒体によってユーザに提供すること。

要件５：

要件２及び S3.1-32 で扱わない個人情報が要件１で含まれていないこと。

2. **補足説明**

2.1. 適合要件の補足説明

該当事項なし

2.2. 用語

該当事項なし

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)の収集にあたり、それに個人情報(個人関連情報を含む)が含まれる場合、収集する個人情報は監査の目的を達成するために必要最小限な範囲にとどめなければならない。

対象外(NA)となるための条件

ログに個人情報が含まれない場合(「対象外(NA)となることの理由」に、ログに個人情報が含まれないことを記載すること)。

1. **★３適合要件**

ログ(テレメトリデータ、監査ログ)に個人情報(個人関連情報を含む)を含む形で収集している場合、★３セキュリティ要件を満たすための仕組みとして、以下の要件１～３のすべてを満たすこと。

要件１：

ログに含まれる個人情報のすべての種別を技術文書等に明示すること。なお、監査目的以外でログを利用する場合には、S3.1-39 にも記載しなければならない。

要件２：

要件１で明示した個人情報が、監査におけるどのような目的で利用されるのかを技術文書等に明示すること。

要件３：

要件２の目的に照らして、要件１で明示する個人情報の収集範囲が必要最小限であること。

2. **補足説明**

2.1. 適合要件の補足説明

該当事項なし

2.2. 用語

該当事項なし

セキュリティ要件番号 ： S3.1-41

★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

個人情報を収集・処理する機能を有しない場合(「対象外(NA)となることの理由」に、個人情報を収集・処理する機能を有しないと記載すること)。

1. **★３適合要件**

個人情報を収集・処理する機能を有している場合、★３セキュリティ要件を満たすための削除機能として、以下の要件１及び要件２のすべてを満たすこと。

要件１：

収集した個人情報が不要になった時点(特定の期間や使用頻度、処理の完了、利用者によるデータの指定等)で、ユーザが個人情報及び処理結果を削除できる機能を有すること。ただし、S3.1-40 のために収集される個人情報は、管理者のみが削除できる対象としてもよい。

要件２：

個人情報及び処理結果が保存されるストレージに応じて適切に削除すること。削除レベルは、単純な非侵襲のデータ回復技術(市販のデータ復旧ソフトによるサルベージ等)から保護できる「Clear」レベル以上とする。

2. **補足説明**

2.1. 適合要件の補足説明

該当事項なし

2.2. 用語

該当事項なし

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 ： S3.1-42

★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。

対象外(NA)となるための条件

該当事項なし

1. **★３適合要件**

JC-STAR 評価機関により実施されたペネトレーションテストの結果、セキュリティ課題が報告されないこと、又は報告されたすべてのセキュリティ課題が解消されていなければならない。

2. **補足説明**

2.1. 適合要件の補足説明

2.1.1. ペネトレーションテストについて

実施する必要のあるペネトレーションについては、2.10 節を参照のこと。

2.2. 用語

該当事項なし

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 ： S3.1-43

★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。

対象外(NA)となるための条件

該当事項なし

1. **★３適合要件**

セキュリティに関する情報は、原則として日本語でユーザに提供しなければならない。
一次情報が日本語以外で作成されている場合には、当該言語のまま情報を提供するとともに、遅滞なく、日本語版、又は日本語での簡易版もしくは翻訳版を提供すること。特に、IPA 又は政府関係機関から日本語での情報提供が要求された場合には、速やかに対応しなければならない。
ただし、JC-STAR との相互承認による製品の場合には、英語での提供を可とする。

2. **補足説明**

2.1. 適合要件の補足説明

該当事項なし

2.2. 用語

【ユーザ】

ユーザの対象範囲には、IoT 製品の利用者、管理者、製造業者のカスタマーエンジニア、所有者等、当該 IoT 製品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 ： S3.1-44

★３セキュリティ要件

製造業者は、IoT 製品のセキュリティに関する情報提供について、以下の①～⑤のすべての要件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、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 製品内にセキュア保存情報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

該当事項なし

1. **★３適合要件**

セキュリティに関する情報提供について、★３セキュリティ要件を満たすための周知する内容として、以下の要件１～５のすべてを満たすこと。

要件１：

初期設定の方法やパスワード変更の実施手順等、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示した情報をユーザが入手可能であること。

要件２：

セキュリティアップデートの内容や必要性、アップデートを行わない場合の影響、デフォルトでは OFF にされているサービスを有効にする場合の影響等を周知する仕組みや実施方法が整備されていること。具体的には、セキュリティアップデートのリリース時に必要な情報をユーザに周知するために利用する媒体や周知方法、担当部署等、一連の仕組みや実施方法が明確になっていること。

要件３：

セキュリティアップデートを提供する際に、ユーザが入手・確認しやすいところに、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する免責事項なども周知するプロセスになっていること。

要件４：

適合ラベルの有効期間中のセキュリティアップデートを無償サポートとして提供すること。ただし、保守契約を締結しなければ販売・提供しない場合はこの限りではない。

要件５：

ユーザが入手・確認しやすいところで、IoT 製品内にセキュア保存情報が残留したまま廃棄や中古販売することで想定されるリスクや、データ消去を含む製品の安全な利用終了方法が説明されていること。

2. 補足説明

2.1. 適合要件の補足説明

該当事項なし

2.2. 用語

【セキュア保存情報】

以下の情報のこと。2.4 節を参照。

- CSP(Critical Security Parameter)
- PSP(Public 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
- プログラムコード
- ログ(テレメトリデータ・監査ログ)

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 ： S3.1-45

★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。

対象外(NA)となるための条件

該当事項なし

1. **★３適合要件**

★３セキュリティ要件を満たすために、IoT 機器へのサービス不能攻撃によるネットワーク過負荷状態(メモリ、CPU リソースの枯渇から復旧等)が解消後、自動で通信機器の機能が正常状態に復帰すること。

2. **補足説明**

2.1. 適合要件の補足説明

該当事項なし

2.2. 用語

【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できない状態。

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 ： S3.1-46

★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。

対象外(NA)となるための条件

該当事項なし

1. **★３適合要件**

筐体の耐タンパー性について、★３セキュリティ要件を満たすための物理的な破壊・改変行為から筐体(エンクロージャ)を保護するための仕組みとして、以下のすべてに類する実装又はそれ以上の実装がされていること。

A) 強化されたエンクロージャ(筐体に高強度の素材や構造等を使用すること)であること。具体的には、IEC 62262 保護等級 IK08 (5.0J)又はこれと同等以上の耐衝撃(バンダルレジスタンス又はプルーフ)構造であること。

B) 素手とプラス又はマイナスドライバでは、簡単に開けることができない構造(*1)であること。

(*1)：セキュリティネジ(一般的な工具では開けられない特殊なネジやボルト)を使用すること。

2. **補足説明**

2.1. 適合要件の補足説明

該当事項なし

2.2. 用語

該当事項なし

Appendix A: 修正履歴

2026.06.10 第1.0版（2026）公開