【本案の留意事項】
※本案は内容確認用にPDFファイルで公開していますが、最終的には入力可能なエクセルファイル等でチェックリストを提供する予定です。
※「基本情報」の詳細は検討中であり、本案には当該シートの内容は含まれておりません。
※「FAQ」は本制度開始時に本制度のHP等で公開される予定のものです。

IoT製品のセキュリティ適合性評価制度
☆1チェックリスト（案）

1. 本チェックリストの目的・位置づけ

本チェックリストは、「IoT製品のセキュリティ適合性評価制度（以降、「本制度」と言います。）」における☆1の適合基準への準拠を評価するためのチェックリストです。
本制度における☆1のラベルを取得するために、本チェックリストを使用して、対象のIoT製品に対する適合基準への準拠状況を評価・記入することが必要となります。
本チェックリストを使用する際には、本シートの「3.チェックリストの使い方」及び関連する「FAQ」をご一読ください。

2. 対象事業者

本チェックリストは、スマート家電やネットワークカメラ等のIoT製品を対象に、本制度における☆1ラベルの取得を希望する事業者（製品の製造業者のほか、販売代理店等を含む）の活用を想定しています。また、事業者より評価を依頼された評価機関・検証事業者による活用も可能です。

3. チェックリストの使い方

本チェックリストは、「基本情報」「#1~16（☆1評価項目番号）」「評価結果一覧」「用語集」のシートで構成されます。「基本情報」「#1~16」のシートに情報を入力・選択することで、結果が「評価結果一覧」のシートに表示されます。「用語集」では、本チェックリストで使用している用語についての説明を記載しています。
本チェックリストを用いて申請を行う事業者は、「基本情報」にて、「1. 申請企業／申請者に関する情報」、「2. 製品に関する情報」、「3. 製造業者に関する情報」、「4. 適合宣言に関する情報」、「5. 申請内容に関する確認、規程への了承」に対する記載・選択のほか、「#1~16」の各シートにおいて、「評価結果」「エビデンスの名称」「エビデンスに基づく根拠／NAであることの理由」の記載・選択が必要になります。
※ 申請を行う事業者が記載・選択する必要があるセルは薄緑色塗りされています。

「評価結果」については、「#1~16」の各シートに記載の「評価手順」及び「評価ガイド」に基づく評価を実施し、「適合している（Y）」、「対象外（NA）」のいずれかを選択ください。なお、各シートに記載の「NAとなるための条件」を満足していない場合、「対象外（NA）」を選択することはできません。
・「適合している（Y）」場合、評価に用いた技術文書（エビデンス）の名称、その根拠をそれぞれ記載ください。根拠においては、以下の内容を最低限記載ください。
 - 「ドキュメント評価」に基づく評価の場合：閲覧した技術文書やウェブサイト等の名称、文書番号、記載箇所（ページ番号、章番号、URL等）
  ※ 市販前製品
 - 「実機テスト」に基づく評価の場合：実機テストの結果が確認できるエビデンス（写真、動画、スクリーンショット、ログ（システム出力）等）の名称
  ※ 製品の開発時点で実施したテストの結果や、他の認証（Common Criteria等）の取得時に作成したエビデンスを、本制度における実機テストのためのエビデンスとして流用することも可能です。
・「対象外（NA）」の場合、評価に用いた文書等のエビデンスの名称と、NAであることの理由をそれぞれ記載ください。「NAであることの理由」には、脅威に対して適切な対策が講じられていると判断するための根拠を記載ください。

「評価手順」には、各項目に対する指定された評価手順が記載されています。評価の際には、指定された評価手順を、「評価ガイド」に従って全て実施する必要があります。

例1：評価結果「Y」の場合の記入例

☆1評価項目番号	1
評価結果	Y
エビデンスの名称	・製品仕様書
エビデンスに基づく根拠／NAであることの理由	・「製品仕様書」（文書番号：SA01-AA）の第8.2.1項（P.20）に記載のとおり、デフォルトパスワードは、初回起動時にユーザによるパスワード変更を必須とする機能を実装し、当該機能において設定可能なパスワードとして、8文字以上のパスワードの設定を強制させている。
セキュリティ要件（大項目）	1. 汎用のデフォルトパスワードを使用しない
セキュリ…	…製品に対してユーザを認証するために…メカニズムは、製品用途の特性等…スクを低…使用していなければ…

例2：評価結果「NA」の場合の記入例

☆1評価項目番号	8
評価結果	NA
エビデンスの名称	・製品マニュアル
エビデンスに基づく根拠／NAであることの理由	・「製品マニュアル」（文書番号：SA01-MA）の第10.1.1項（P.20）に記載のとおり、本製品ではソフトウェアをネットワーク経由でアップデートする仕組みが存在せず、自社に返送していただきアップデートの対応をするか、自社技術者が製品納入先に伺ってアップデートの対応をするため。
セキュリティ要件（大項目）	3. ソフトウェアを最新の状態に保つ
セキュリ…	…製品においてアップデートメカニズムが…場合、セキュアなアップデートメカニ…ために、ベスト…製品技術を使用しな…

「基本情報」「#1~16」のシートに入力した結果は「評価結果一覧」のシートに表示されます。「評価結果一覧」の適合確認に「YES」と表示されない場合、ラベルは取得できません。「YES」と表示されない場合、「基本情報」や「#1~16」のシートにおいて、必要事項が記入されていない可能性があります。

4. 注意事項

・本チェックリストは日本語にて記入ください。また、評価に活用できるエビデンスは日本語又は英語にて作成されている必要があります。その他の言語で記載されたエビデンスは認められません。
・☆1適合基準は、☆1において守るべき資産や対抗すべき脅威等に基づいて求められるセキュリティ要件を示したものであり、サイバー攻撃を受けた場合の完璧な被害防止を保証するものではありません。
・付与されたラベルには有効期限があり、定期的に更新する必要があります。
・申請内容に虚偽がある場合、ラベルの取り消し措置等が行われる可能性があります。

※「基本情報」シートの内容が転写されます。

申請企業の名称	-
製品の名称	-
製品の型式番号	-
製品の製造業者の名称（企業名称）	-
製造国又は地域	-
評価者の所属企業名称	-
評価完了日	-

適合確認

※ YESと表示されない場合、ラベル申請はできません。

☆1評価項目番号	セキュリティ要件（大項目）	セキュリティ要件	☆1 適合基準	NAとなるための条件、基準の補足説明	評価結果	エビデンスの名称	エビデンスに基づく根拠
1	1. 汎用のデフォルトパスワードを使用しない	1-3. 製品に対してユーザを認証するために使用される認証メカニズムは、製品用途の特性等に適した想定するリスクを低減できる技術を使用していなければならない。	TCP/UDP通信を介した守るべき情報資産への他の機器又はユーザからのアクセスに対して、適切な認証に基づくアクセス制御が行われていること。 なお、電気通信事業法に基づく端末機器セキュリティに係る技術基準を含めた技術基準適合認定を受けた製品（技適[T]マーク又は[A]マークが付与された製品）は、本適合基準に適合しているとみなす。（この場合、「基本情報」シートに「電気通信事業法に基づく技術基準適合認定番号等（技適[T]マークの設計認証番号又は[A]マークの技術基準適合認定番号）」を記入のこと。）	【NAとなるための条件】 ・TCP/UDP通信を介した守るべき情報資産への認証及びアクセスの仕組みがない（「NAであることの理由」に、外部からの不正アクセスに対抗するために認証及びアクセスが必要ない根拠を記載すること） 【用語定義：守るべき情報資産】 以下のすべての情報： ・通信機能に関する設定情報 ・セキュリティ機能に関する設定情報 ・機器の意図する使用において、機器が収集し、保存又は通信する、個人情報等の一般的に機密性が高い情報	-	-	-
2	1. 汎用のデフォルトパスワードを使用しない	1-2. プリインストールされた固有のパスワードを使用する場合、自動化された攻撃への耐性をもつために、パスワードは十分なランダム性を保有しなければならない。	機器に対するネットワークを介したユーザ認証の仕組み、又は、機器初期設定時のクライアント認証の仕組みにてパスワードやパスコードを使用する製品において、製品導入時にデフォルトパスワードが使用される場合に、以下の①・②のいずれかの基準を満たすこと。 ① デフォルトパスワードは、機器毎に異なる一意の値で、容易に推測可能でない6文字以上のパスワードであること。 ② デフォルトパスワードは、初回起動時にユーザによるパスワード変更を必須とする機能を実装し、当該機能において設定可能なパスワードとして、8文字以上のパスワードの設定を強制させること。	【NAとなるための条件】 ネットワークを介したユーザ認証の仕組みがない（「NAであることの理由」に、脅威に対抗するためにユーザ認証が必要ない根拠を記載すること）	-	-	-
3	1. 汎用のデフォルトパスワードを使用しない	1-4. 製品に対するユーザ認証において、製品は使用される認証値を変更するためのシンプルなメカニズムを、ユーザ又は管理者に提供しなければならない。	機器に対するネットワークを介したユーザ認証において使用される認証値の変更について、認証の種類（パスワード、トークン、指紋等）に依らず、その認証値の変更を可能とすること。	【NAとなるための条件】 ・ネットワークを介したユーザ認証の仕組みがない（「NAであることの理由」に、外部からの不正アクセスに対抗するためにユーザ認証が必要ない根拠を記載すること） 【用語定義：認証値】 製品に対する認証の仕組みで使用される属性の個別値。 （例： パスワードに基づく認証の仕組みである場合、認証値は文字列となる。生体指紋認証である場合、認証値は例えば左手の人差し指の指紋データとなる。）	-	-	-
4	1. 汎用のデフォルトパスワードを使用しない	1-5. 機器が、制約のある機器ではない場合、ネットワークを介して行われる認証に対する総当たり攻撃等のブルートフォース攻撃が実行できないようにするメカニズムを保有しなければならない。	機器が、制約のある機器ではない場合、機器に対するネットワークを介したユーザ認証の仕組みについて、総当たり攻撃を困難とすること。	【NAとなるための条件】 以下のいずれかの条件に該当する。（OR条件） ・機器に対するネットワークを介したユーザアクセスの仕組みがない（「NAであることの理由」に、外部からの不正アクセスに対抗するためにユーザアクセスが必要ない根拠を記載すること） ・機器が「制約のある機器」に該当する（「NAであることの理由」に、機器が「制約のある機器」に該当することを示す根拠を記載すること） 【用語定義：制約のある機器】 データを処理する機能、データを通信する機能、データを保存する機能、又はユーザと対話する機能のいずれかにおいて、意図された使用のために物理的な制約がある機器。（このような機器の例は「用語集」を参照。）	-	-	-
5	2. 脆弱性の報告を管理するための手段を導入する	2-1. 製造業者は、脆弱性開示ポリシーを公開しなければならない。このポリシーには、少なくとも以下が含まれていなければならない ・問題を報告するための連絡先情報 ・以下のタイムラインに関する情報 1）最初の受領確認 2）報告された問題が解決されるまでの状況の更新	製造業者は、以下の①～③のすべての情報を含む脆弱性開示ポリシーを公開（例：製造業者のウェブサイトへの掲載）すること。 ① 製品のセキュリティの問題に関して、製造業者へ報告するための連絡先（例：製造業者等のウェブサイトのURL、電話番号、メールアドレス） ② 製造業者が製品のセキュリティに関する報告を受領した後に行う手続き及びその概要 ③ 脆弱性が解決されるまでの製品や脆弱性の状況更新に関する手続き及びその概要	–	-	-	-
6	3. ソフトウェアを最新の状態に保つ	3-1. 製品に含まれる特定のソフトウェアコンポーネントについて、アップデート可能にしなければならない。	製品に含まれるソフトウェアコンポーネントのアップデート機能について、以下の①～③のすべての基準を満たすこと。 ①製品のファームウェア（ソフトウェア）パッケージについて、アップデートが可能であること。 ②ファームウェア（ソフトウェア）パッケージのバージョンの確認が行えるなど、最新のファームウェア（ソフトウェア）がインストールされていることを確認する手段を有すること。 ③アップデートされたファームウェア（ソフトウェア）パッケージのバージョンが電源OFF後も維持されること。 なお、電気通信事業法に基づく端末機器セキュリティに係る技術基準を含めた技術基準適合認定を受けた製品（技適[T]マーク又は[A]マークが付与された製品）は、本適合基準に適合しているとみなす。（この場合、「基本情報」シートに「電気通信事業法に基づく技術基準適合認定番号等（技適[T]マークの設計認証番号又は[A]マークの技術基準適合認定番号）」を記入のこと。）	–	-	-	-
7	3. ソフトウェアを最新の状態に保つ	3-3. 製品においてアップデートメカニズムが実装されている場合、そのアップデートは、ユーザが簡単に適用できるものでなければならない。	ユーザがアップデートを適用する際、容易かつ分かりやすい手順でソフトウェアのアップデートを実行可能とすること。	–	-	-	-
8	3. ソフトウェアを最新の状態に保つ	3-7. 製品においてアップデートメカニズムが実装されている場合、セキュアなアップデートメカニズムを容易にするために、ベストプラクティスの暗号技術を使用しなければならない。	ソフトウェアをネットワーク経由でアップデートする際、ソフトウェアの完全性をアップデート前に確認できる仕組みを有すること。	【NAとなるための条件】 ソフトウェアをネットワーク経由でアップデートする仕組みが存在しない（「NAであることの理由」に、想定するアップデートの仕組みを記載すること）	-	-	-
9	3. ソフトウェアを最新の状態に保つ	3-8. 製品においてアップデートメカニズムが実装されている場合、セキュリティアップデートは、適時でなければならない。	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。	–	-	-	-
10	3. ソフトウェアを最新の状態に保つ	3-14. 製品のモデル名称は、製品上のラベル又は物理的インタフェースを介して、ユーザに対して明確に認識可能でなければならない。	製品の型式番号は、以下のいずれかの方法でユーザへ提供すること。 ① 製品本体に、製品の型式番号を直接記載すること。 ② 製品のGUI、ウェブUI等や、製品に付帯するソフトウェア、アプリケーション（スマホアプリなど）のGUI、ウェブUI等から、ユーザが型式番号を認識できるようにすること。	–	-	-	-
11	4. 機密セキュリティパラメータをセキュアに保存する	4-1. 製品のストレージにある機密セキュリティパラメータは、製品によってセキュアに保存されなければならない。	製品のストレージに保存される守るべき情報資産（SDカード等、ストレージメディアに保存される守るべき情報資産も含む。）が、ネットワーク経由の不正アクセスに対して、セキュアに保存されること。	【用語定義：守るべき情報資産】 以下のすべての情報： ・通信機能に関する設定情報 ・セキュリティ機能に関する設定情報 ・機器の意図する使用において、機器が収集し、保存又は通信する、個人情報等の一般的に機密性が高い情報	-	-	-

☆1評価項目番号	セキュリティ要件（大項目）	セキュリティ要件	☆1 適合基準	NAとなるための条件、基準の補足説明	評価結果	エビデンスの名称	エビデンスに基づく根拠
12	5. セキュアに通信する	5-1. 製品は、ベストプラクティスの暗号技術を使用してセキュアに通信をしなくてはならない。	ネットワーク経由で伝送される守るべき情報資産について、情報の盗聴に対する以下のいずれかの保護対策が行われていること。 ① 他のIoT機器やサーバ（クラウド上のサーバを含む）へネットワークを介して伝送される守るべき情報資産について、情報の盗聴に対する保護対策を機器自らが行う。 ② 他のIoT機器やサーバ（クラウド上のサーバを含む）へネットワークを介して伝送される守るべき情報資産について、保護された通信環境（VPN環境や専用線を経由した接続環境）においてのみ伝送される。	【NAとなるための条件】 ネットワーク経由で伝送される守るべき情報資産が存在しない （「NAであることの理由」に、ネットワーク経由で伝送される守るべき情報資産が存在しないことを示す根拠を記載すること） 【用語定義：守るべき情報資産】 以下のすべての情報： ・通信機能に関する設定情報 ・セキュリティ機能に関する設定情報 ・機器の意図する使用において、機器が収集し、保存又は通信する、個人情報等の一般的に機密性が高い情報	-	-	-
13	6. 露出した攻撃面を最小化する	6-1. すべての未使用の物理的インタフェース及び論理的インタフェースは無効化しなければならない。	製品において、外部からサイバー攻撃を受けるリスクを低減するために、製品の利用上不要かつ攻撃を受けるリスクがある物理的インタフェース及び論理的インタフェースを無効化するとともに、製品に対する脆弱性検査を実施すること。具体的には、以下の①・②のすべての基準を満たすこと。 ①製品において、高頻度で利用され、脆弱性などのリスクが想定される以下のインタフェースについて、製品の利用上不要かつ攻撃を受けるリスクがあるインタフェースを無効化すること。 A) TCP/UDPポート B) Bluetooth C) USB ②製品に対して脆弱性スキャンツールによる既知の脆弱性検査を実施し、攻撃に悪用される可能性がある脆弱性が検出されないこと。	–	-	-	-
14	9. 停止に対してレジリエントなシステムにする	9-1. データネットワークと電源の停止の可能性を考慮して、レジリエンスを製品とサービスに組み込まなければならない。	停電等による電力供給の停止やネットワークの停止により、機器の電源がOFFになった後、電力供給が再開され、ネットワーク機能が復帰した際に、アクセス制御の際に使用する認証値（パスワード、秘密鍵など）の設定及びアップデートが完了したソフトウェアが工場出荷時の初期状態に戻ることなく、電源OFFになる直前の状態を維持できること。 なお、電気通信事業法に基づく端末機器セキュリティに係る技術基準を含めた技術基準適合認定を受けた製品（技適[T]マーク又は[A]マークが付与された製品）は、本適合基準に適合しているとみなす。（この場合、「基本情報」シートに「電気通信事業法に基づく技術基準適合認定番号等（技適[T]マークの設計認証番号又は[A]マークの技術基準適合認定番号）」を記入のこと。）	–	-	-	-
15	11. ユーザが簡単にデータを消去できるようにする	11-1. ユーザは、簡単な方法で製品からユーザデータを消去できるような機能を提供されなければならない。	製品利用中に製品のストレージに保存されたデータの削除機能について、以下の①・②のすべての基準を満たすこと。 ① ユーザによって、機器本体や関連サービス（モバイルアプリケーション等）を介して、ユーザに関する少なくとも以下のデータを削除できること。 A) 製品利用中に取得した情報資産（個人情報含む） B) ユーザ設定値 C) ユーザが設定した認証値、製品利用中に取得した暗号鍵やデジタル署名 ② データ削除後も、アップデートされたセキュリティ機能に関するファームウェア（ソフトウェア）パッケージのバージョンは維持されること。	–	-	-	-
16	17. 製品に関する情報提供を行う	17-2. 製造業者は、製品をセキュアに設定・利用・廃棄する方法について、ユーザに提供しなければならない。	製造業者は、製品のサイバーセキュリティに関する情報提供について、以下の①～⑤のすべての基準を満たす対応を行うこと。 ①初期設定の方法など、製品の利用上、サイバーセキュリティに影響が生じる設定や使用方法について、安全に利用できる手順を周知すること。 ②製品のセキュリティアップデートの内容や必要性、アップデートを行わない場合の影響などを周知すること。 ③アップデートを行わなかったときに想定される事故や障害・一般的に想定される事故や障害に対して、免責事項を周知すること。 ④対象製品やサービスのサポート期限又はサポート終了時の方針を周知すること。 ⑤製品内に守るべき情報資産が残留したまま廃棄や中古販売することで想定されるリスクや、データ消去を含む製品の安全な利用終了方法を周知すること。	–	-	-	-

☆1評価項目番号	1
評価結果	
エビデンスの名称	
エビデンスに基づく根拠／NAであることの理由	
セキュリティ要件（大項目）	1. 汎用のデフォルトパスワードを使用しない
セキュリティ要件	1-3. 製品に対してユーザを認証するために使用される認証メカニズムは、製品用途の特性等に適した想定するリスクを低減できる技術を使用していなければならない。
☆1 適合基準	TCP/UDP通信を介した守るべき情報資産への他の機器又はユーザからのアクセスに対して、適切な認証に基づくアクセス制御が行われていること。 なお、電気通信事業法に基づく端末機器セキュリティに係る技術基準を含めた技術基準適合認定を受けた製品（技適[T]マーク又は[A]マークが付与された製品）は、本適合基準に適合しているとみなす。（この場合、「基本情報」シートに「電気通信事業法に基づく技術基準適合認定番号等（技適[T]マークの設計認証番号又は[A]マークの技術基準適合認定番号）」を記入のこと。）
NAとなるための条件、基準の補足説明	【NAとなるための条件】 ・TCP/UDP通信を介した守るべき情報資産への認証及びアクセスの仕組みがない（「NAであることの理由」に、外部からの不正アクセスに対抗するために認証及びアクセスが必要ない根拠を記載すること） 【用語定義：守るべき情報資産】 以下のすべての情報： ・通信機能に関する設定情報 ・セキュリティ機能に関する設定情報 ・機器の意図する使用において、機器が収集し、保存又は通信する、個人情報等の一般的に機密性が高い情報
☆1 評価手法	ドキュメント評価：対象とする 実機テスト：なし
☆1 評価ガイド	［ドキュメント評価］ 製品の技術文書において、他の機器又はユーザからの守るべき情報資産へのアクセスに対する以下の仕組みが明示されていることを評価する。以下の仕組みが明示されている場合に限り、本適合基準の評価結果が「Y」となる。 ・製品の意図される使用上必要なTCP/UDP通信（以下に示す「例外となるプロトコル」を除く）については、守るべき情報資産への他の機器又はユーザからのアクセスに対して、適切な認証に基づくアクセス制御が行われていること。また、利用される認証又はアクセス制御の方法が、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）IDとパスワードによるユーザ認証が実装され、使用されるパスワードについて、評価項目番号＃2の①・②両方のいずれの基準を満たす。 B）複数の認証要素を利用した多要素認証を行う。 C）デジタル証明書を使用した認証を行う。 D）Web APIの認証において、OpenID Authentication等の標準的な認証方式に基づく認証を行う。 E）通信を許可する対象をIPアドレスなどで制限する。 F）通信を許可する対象をLAN内の機器のみに制限する。 【参考情報：例外となるプロトコルの例】 ・ARP、ICMP（TCP/UDPより下位のレイヤのプロトコルであるため） ・DHCP、DNS、NTP（認証に対応していないプロトコルであるため）
☆1評価に当たって参考となるガイドライン等	【評価に当たって参考となるガイドライン等】 ・ETSI TS 103 701 [5.1.3 Test group 5.1-3], [5.5.5 Test group 5.5-5] https://www.etsi.org/deliver/etsi_ts/103700_103799/103701/01.01.01_60/ts_103701v010101p.pdf ・CCDS: IoT機器セキュリティ要件適合基準ガイドライン 2023年版 [7.1-1 アクセス制御及び認証], [7.1-2 データ保護] https://www.ccds.or.jp/public/document/other/CCDS_SecGuide-IoTReq_Criteria_2023_v1.0_jpn.pdf ・RFC 6749 “The OAuth 2.0 Authorization Framework”

☆1評価項目番号	2
評価結果	
エビデンスの名称	
エビデンスに基づく根拠／NAであることの理由	
セキュリティ要件（大項目）	1. 汎用のデフォルトパスワードを使用しない
セキュリティ要件	1-2. プリインストールされた固有のパスワードを使用する場合、自動化された攻撃への耐性をもつために、パスワードは十分なランダム性を保有しなければならない。
☆1 適合基準	機器に対するネットワークを介したユーザ認証の仕組み、又は、機器初期設定時のクライアント認証の仕組みにてパスワードやパスコードを使用する製品において、製品導入時にデフォルトパスワードが使用される場合に、以下の①・②のいずれかの基準を満たすこと。 ① デフォルトパスワードは、機器毎に異なる一意の値で、容易に推測可能でない6文字以上のパスワードであること。 ② デフォルトパスワードは、初回起動時にユーザによるパスワード変更を必須とする機能を実装し、当該機能において設定可能なパスワードとして、8文字以上のパスワードの設定を強制させること。
NAとなるための条件、基準の補足説明	【NAとなるための条件】 ネットワークを介したユーザ認証の仕組みがない（「NAであることの理由」に、脅威に対抗するためにユーザ認証が必要ない根拠を記載すること）
☆1 評価手法	ドキュメント評価：①、② 実機テスト：なし
☆1 評価ガイド	［ドキュメント評価］ 製品の技術文書において、製品導入時にデフォルトパスワードに関する対策が明示されていることを評価する。デフォルトパスワードに関して、以下の①～②のいずれかを満たす実装が明示されている場合に限り、本適合基準の評価結果が「Y」となる。 ① デフォルトパスワードは、機器毎に異なる一意で、以下の1.～4.のいずれにも該当しない、6桁以上のパスワードである。 1. 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） 2. 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） 3. 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） 4. MACアドレス、Wi-Fi®SSID、製品のシリアル・型式番号・名前（略称）などの公開情報に基づくパスワード ② デフォルトパスワードは、初回起動時にユーザによるパスワード変更を必須とする機能を実装し、当該機能において設定可能なパスワードとして、8文字以上のパスワードを強制させる。なお、ネットワーク機能を使用せずとも利用可能な製品の場合、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、本条件を満たしていると見なす。 ※ 管理者がメンテナンス時に利用するための認証についても対象とする。
☆1評価に当たって参考となるガイドライン等	【評価に当たって参考となるガイドライン等】 ・ETSI TS 103 701 [5.1.2 Test group 5.1-2] https://www.etsi.org/deliver/etsi_ts/103700_103799/103701/01.01.01_60/ts_103701v010101p.pdf ・CCDS: IoT機器セキュリティ要件適合基準ガイドライン 2023年版 [7.1-1 アクセス制御及び認証] https://www.ccds.or.jp/public/document/other/CCDS_SecGuide-IoTReq_Criteria_2023_v1.0_jpn.pdf ・英国NIST：NIST SP 800-63-3 Digital Identity Guidelines https://pages.nist.gov/800-63-3/ ・英国NCSC：PwnedPasswordsTop100k https://www.ncsc.gov.uk/static-assets/documents/PwnedPasswordsTop100k.txt

☆1評価項目番号	3
評価結果	
エビデンスの名称	
エビデンスに基づく根拠／NAであることの理由	
セキュリティ要件（大項目）	1. 汎用のデフォルトパスワードを使用しない
セキュリティ要件	1-4. 製品に対するユーザ認証において、製品は使用される認証値を変更するためのシンプルなメカニズムを、ユーザ又は管理者に提供しなければならない。
☆1 適合基準	機器に対するネットワークを介したユーザ認証において使用される認証値の変更について、認証の種類（パスワード、トークン、指紋等）に依らず、その認証値の変更を可能とすること。
NAとなるための条件、基準の補足説明	【NAとなるための条件】 ・ネットワークを介したユーザ認証の仕組みがない（「NAであることの理由」に、外部からの不正アクセスに対抗するためにユーザ認証が必要ない根拠を記載すること） 【用語定義：認証値】 製品に対する認証の仕組みで使用される属性の個別値。（例： パスワードに基づく認証の仕組みである場合、認証値は文字列となる。生体指紋認証である場合、認証値は例えば左手の人差し指の指紋データとなる。）
☆1 評価手法	ドキュメント評価：対象とする 実機テスト：なし
☆1 評価ガイド	［ドキュメント評価］ 製品の技術文書において、製品に対するユーザ認証において使用される認証値の変更に関する記載があることを評価する。以下の情報が明示されている場合に限り、本適合基準の評価結果が「Y」となる。 ・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ある
☆1評価に当たって参考となるガイドライン等	【評価に当たって参考となるガイドライン等】 ・ETSI TS 103 701 [5.1.4 Test group 5.1-4], [5.4.2 Test group 5.4-2] https://www.etsi.org/deliver/etsi_ts/103700_103799/103701/01.01.01_60/ts_103701v010101p.pdf ・CCDS: IoT機器セキュリティ要件適合基準ガイドライン 2023年版 [7.1-1 アクセス制御及び認証] https://www.ccds.or.jp/public/document/other/CCDS_SecGuide-IoTReq_Criteria_2023_v1.0_jpn.pdf 【備考】 パスワードによる認証の場合、ユーザID及びパスワードなどが製品のソフトウェアにハードコーディングされていないことが前提となる。

☆1評価項目番号	4
評価結果	
エビデンスの名称	
エビデンスに基づく根拠／NAであることの理由	
セキュリティ要件（大項目）	1. 汎用のデフォルトパスワードを使用しない
セキュリティ要件	1-5. 機器が、制約のある機器ではない場合、ネットワークを介して行われる認証に対する総当たり攻撃等のブルートフォース攻撃が実行できないようにするメカニズムを保有しなければならない。
☆1 適合基準	機器が、制約のある機器ではない場合、機器に対するネットワークを介したユーザ認証の仕組みについて、総当たり攻撃を困難とすること。
NAとなるための条件、基準の補足説明	【NAとなるための条件】 以下のいずれかの条件に該当する。（OR条件） ・機器に対するネットワークを介したユーザアクセスの仕組みがない（「NAであることの理由」に、外部からの不正アクセスに対抗するためにユーザアクセスが必要ない根拠を記載すること） ・機器が「制約のある機器」に該当する（「NAであることの理由」に、機器が「制約のある機器」に該当することを示す根拠を記載すること） 【用語定義：制約のある機器】 データを処理する機能、データを通信する機能、データを保存する機能、又はユーザと対話する機能のいずれかにおいて、意図された使用のために物理的な制約がある機器。（このような機器の例は「用語集」を参照。）
☆1 評価手法	ドキュメント評価：なし 実機テスト：対象とする
☆1 評価ガイド	［実機テスト］ 対象製品に対する実機テストによって、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ついて、総当たり攻撃を困難とする仕組みを評価する。以下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いる場合、本適合基準の評価結果は「Y」となる。 ・ネットワークを介したユーザ認証について、認証試行が一定回数※失敗することで、追加の認証試行が禁止する。 ・ネットワークを介したユーザ認証について、認証試行が一定回数※失敗することで、認証が一定期間停止する。 ・ネットワークを介したユーザ認証について、認証試行が連続して失敗した際に、認証応答の発行が一定時間遅延される。 ・多要素認証が使用されている。 ※ 一定回数の失敗とは、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。
☆1評価に当たって参考となるガイドライン等	【評価に当たって参考となるガイドライン等】 ・ETSI TS 103 701 [5.1.5 Test group 5.1-5] https://www.etsi.org/deliver/etsi_ts/103700_103799/103701/01.01.01_60/ts_103701v010101p.pdf ・CCDS: IoT機器セキュリティ要件適合基準ガイドライン 2023年版 [7.1-1 アクセス制御及び認証] https://www.ccds.or.jp/public/document/other/CCDS_SecGuide-IoTReq_Criteria_2023_v1.0_jpn.pdf

☆1評価項目番号	5
評価結果	
エビデンスの名称	
エビデンスに基づく根拠	
セキュリティ要件（大項目）	2. 脆弱性の報告を管理するための手段を導入する
セキュリティ要件	2-1. 製造業者は、脆弱性開示ポリシーを公開しなければならない。このポリシーには、少なくとも以下が含まれていなければならない ・問題を報告するための連絡先情報 ・以下のタイムラインに関する情報 1) 最初の受領確認 2) 報告された問題が解決されるまでの状況の更新
☆1 適合基準	製造業者は、以下の①～③のすべての情報を含む脆弱性開示ポリシーを公開（例：製造業者のウェブサイトへの掲載）すること。 ① 製品のセキュリティの問題に関して、製造業者へ報告するための連絡先（例：製造業者等のウェブサイトのURL、電話番号、メールアドレス） ② 製造業者が製品のセキュリティに関する報告を受領した後に行う手続き及びその概要 ③ 脆弱性が解決されるまでの製品や脆弱性の状況更新に関する手続き及びその概要
NAとなるための条件、基準の補足説明	–
☆1 評価手法	ドキュメント評価：①、②、③ 実機テスト：なし
☆1 評価ガイド	［ドキュメント評価］ 製品のウェブサイト等、ユーザがアクセス可能な媒体において、脆弱性開示ポリシーが明示されていることを評価する。脆弱性開示ポリシーにおいて、以下の①～③のすべての情報が明示されている場合※に限り、本適合基準の評価結果が「Y」となる。 ① 製品のセキュリティの問題に関して、製造業者へ報告するための連絡先（例：製造業者のウェブサイトのURL、電話番号、メールアドレス） ② 製造業者が製品のセキュリティに関する報告を受領した後に行う手続きがあること及びその概要（詳細な手続きを公開する必要はなく、当該手続きがあることと、その手続きの概要を公開することが求められる） ③ 脆弱性が解決されるまでの製品や脆弱性の状況更新に関する手続きがあること及びその概要（詳細な手続きを公開する必要はなく、当該手続きがあることと、その手続きの概要を公開することが求められる） サポートメールアドレスやサポートヘルプデスクを設置していることの公開のみでは、脆弱性開示ポリシーがユーザに明示されているとはみなされない。 ※　市販前製品について、評価時に脆弱性開示ポリシーが公開されていない場合、公開見込みが分かる情報（例：公開予定画面）をエビデンスとし、以下の内容を「エビデンスに基づく根拠」に記載することで、本適合基準の評価結果が「Y」となる。 ・公開予定日（製品販売日以前に限る） ・公開方法・公開場所 ・公開予定内容（①～③のすべての情報を含むこと）
☆1評価に当たって参考となるガイドライン等	【評価に当たって参考となるガイドライン等】 ・ETSI TS 103 701 [5.2.1 Test group 5.2-1] https://www.etsi.org/deliver/etsi_ts/103700_103799/103701/01.01.01_60/ts_103701v010101p.pdf ・CCDS: IoT機器セキュリティ要件適合基準ガイドライン 2023年版 [7.2-1 連絡窓口・セキュリティサポート体制] https://www.ccds.or.jp/public/document/other/CCDS_SecGuide-IoTReq_Criteria_2023_v1.0_jpn.pdf

☆1評価項目番号	6
評価結果	
エビデンスの名称	
エビデンスに基づく根拠	
セキュリティ要件（大項目）	3. ソフトウェアを最新の状態に保つ
セキュリティ要件	3-1. 製品に含まれる特定のソフトウェアコンポーネントについて、アップデート可能にしなければならない。
☆1 適合基準	製品に含まれるソフトウェアコンポーネントのアップデート機能について、以下の①～③のすべての基準を満たすこと。 ①製品のファームウェア（ソフトウェア）パッケージについて、アップデートが可能であること。 ②ファームウェア（ソフトウェア）パッケージのバージョンの確認が行えるなど、最新のファームウェア（ソフトウェア）がインストールされていることを確認する手段を有すること。 ③アップデートされたファームウェア（ソフトウェア）パッケージのバージョンが電源OFF後も維持されること。 なお、電気通信事業法に基づく端末機器セキュリティに係る技術基準を含めた技術基準適合認定を受けた製品（技適[T]マーク又は[A]マークが付与された製品）は、本適合基準に適合しているとみなす。（この場合、「基本情報」シートに「電気通信事業法に基づく技術基準適合認定番号等（技適[T]マークの設計認証番号又は[A]マークの技術基準適合認定番号）」を記入のこと。）
NAとなるための条件、基準の補足説明	_
☆1 評価手法	ドキュメント評価：なし 実機テスト：①、②、③
☆1 評価ガイド	[実機テスト] 対象製品の実機テストにより評価する。以下の①～③のテストをすべて行い、いずれも確認できた場合に限り、本適合基準の評価結果が「Y」となる。 ①製品のファームウェア（ソフトウェア）パッケージについてアップデート※の操作を行い、正常にアップデートが完了できる。 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。 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後も最新の状態が維持される。 ※ アップデートの方法について、自動的に開始される方法、あるいは明示的に管理責任を有する保守担当者や特権ユーザが手動で実施する方法のどちらも対象とする。
☆1評価に当たって参考となるガイドライン等	【評価に当たって参考となるガイドライン等】 ・ETSI TS 103 701 [5.3.1 Test group 5.3-1] https://www.etsi.org/deliver/etsi_ts/103700_103799/103701/01.01.01_60/ts_103701v010101p.pdf ・CCDS: IoT機器セキュリティ要件適合基準ガイドライン 2023年版 [7.1-3 ソフトウェア更新] https://www.ccds.or.jp/public/document/other/CCDS_SecGuide-IoTReq_Criteria_2023_v1.0_jpn.pdf

☆1評価項目番号	7
評価結果	
エビデンスの名称	
エビデンスに基づく根拠	
セキュリティ要件（大項目）	3. ソフトウェアを最新の状態に保つ
セキュリティ要件	3-3. 製品においてアップデートメカニズムが実装されている場合、そのアップデートは、ユーザが簡単に適用できるものでなければならない。
☆1 適合基準	ユーザがアップデートを適用する際、容易かつ分かりやすい手順でソフトウェアのアップデートを実行可能とすること。
NAとなるための条件、基準の補足説明	–
☆1 評価手法	ドキュメント評価：対象とする 実機テスト：なし
☆1 評価ガイド	［ドキュメント評価］ 製品のマニュアル、ウェブサイト等、ユーザがアクセス可能な媒体において、ソフトウェアのアップデートに関する容易かつ分かりやすい手順が明示されていることを評価する。以下のいずれかに類するアップデート方法（ただし、これらに限定されず、1つの製品で複数のアップデート方法を採用することも許容される。）の手順が明示されている場合、本適合基準の評価結果は「Y」となる。 ・自動的にアップデートが実行される。 ・ユーザが、製品の関連サービス（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できる。 ・ユーザが、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できる。 ・ユーザが、製品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し、製品に対してアップデートを実行できる。
☆1評価に当たって参考となるガイドライン等	【評価に当たっての参考文書】 ・ETSI TS 103 701 [5.3.1 Test group 5.3-3] https://www.etsi.org/deliver/etsi_ts/103700_103799/103701/01.01.01_60/ts_103701v010101p.pdf ・CCDS: IoT機器セキュリティ要件適合基準ガイドライン 2023年版 [7.1-3 ソフトウェア更新] https://www.ccds.or.jp/public/document/other/CCDS_SecGuide-IoTReq_Criteria_2023_v1.0_jpn.pdf

☆1評価項目番号	8
評価結果	
エビデンスの名称	
エビデンスに基づく根拠／NAであることの理由	
セキュリティ要件（大項目）	3. ソフトウェアを最新の状態に保つ
セキュリティ要件	3-7. 製品においてアップデートメカニズムが実装されている場合、セキュアなアップデートメカニズムを容易にするために、ベストプラクティスの暗号技術を使用しなければならない。
☆1 適合基準	ソフトウェアをネットワーク経由でアップデートする際、ソフトウェアの完全性をアップデート前に確認できる仕組みを有すること。
NAとなるための条件、基準の補足説明	【NAとなるための条件】 ソフトウェアをネットワーク経由でアップデートする仕組みが存在しない（「NAであることの理由」に、想定するアップデートの仕組みを記載すること）
☆1 評価手法	ドキュメント評価：対象とする 実機テスト：なし
☆1 評価ガイド	[ドキュメント評価] 製品の技術文書において、ソフトウェアの完全性をアップデート前に確認できる仕組みの実装が明示されていることを評価する。以下のいずれかに類する仕組み又はそれ以上の仕組みの実装が明示されている場合、本適合基準の評価結果は「Y」となる。 ・アップデートソフトウェアをインストールする前に、付与されたハッシュ値※との照合を行い、照合の結果、不一致が確認された場合にはインストールを中止する。 ・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、更新ソフトウェアウェアに付与されたハッシュ値※との照合を行い、照合の結果、不一致が確認された場合にはインストールを中止する。 ※ ハッシュ値については、「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」のハッシュ関数によってハッシュ化された値であること。
☆1評価に当たって参考となるガイドライン等	【暗号技術に関連するガイドライン】 -「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)」 （最終改訂: 2022年3月30日、CRYPTREC LS-0001-2022） -「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」 （初版：2022年6月、CRYPTREC LS-0003-2022） ※［上記ガイドラインの補足文書］ -「CRYPTREC 暗号技術ガイドライン (SHA-1) 改定版」 (CRYPTREC GL-2001-2013R1) -「CRYPTREC暗号技術ガイドライン(軽量暗号)」(CRYPTREC GL-2003-2016JP) -「暗号鍵設定ガイダンス」(CRYPTREC GL-3003-1.0) -「暗号鍵管理システム設計指針 (基本編) 」(CRYPTREC GL-3002-1.0) -「TLS暗号設定ガイドライン」(CRYPTREC GL-3001-3.0.1) 【評価に当たって参考となるガイドライン等】 ・ETSI TS 103 701 [5.3.7 Test group 5.3-7] https://www.etsi.org/deliver/etsi_ts/103700_103799/103701/01.01.01_60/ts_103701v010101p.pdf ・CCDS: IoT機器セキュリティ要件適合基準ガイドライン 2023年版 [7.1-3 ソフトウェア更新] https://www.ccds.or.jp/public/document/other/CCDS_SecGuide-IoTReq_Criteria_2023_v1.0_jpn.pdf

☆1評価項目番号	9
評価結果	
エビデンスの名称	
エビデンスに基づく根拠	
セキュリティ要件（大項目）	3. ソフトウェアを最新の状態に保つ
セキュリティ要件	3-8. 製品においてアップデートメカニズムが実装されている場合、セキュリティアップデートは、適時でなければならない。
☆1 適合基準	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。
NAとなるための条件、基準の補足説明	–
☆1 評価手法	ドキュメント評価：対象とする 実機テスト：なし
☆1 評価ガイド	組織の規程類、方針、手順書等又は製品の技術文書において、セキュリティアップデートの優先度を決定するための方針や指針が明示されていることを評価する。以下のいずれかに類する内容（ただし、これらに限定されず、かつ、必ずしもすべての条件を満たす必要はない。）が明示されている場合、本適合基準の評価結果は「Y」となる。 ・対応する脆弱性の深刻度や重要度の指標、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） ・PSIRTやインシデントレスポンスの組織体制や、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 ・複数のステークホルダーによって開発・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）
☆1評価に当たって参考となるガイドライン等	【評価に当たって参考となるガイドライン等】 ・ETSI TS 103 701 [5.3.7 Test group 5.3-8] https://www.etsi.org/deliver/etsi_ts/103700_103799/103701/01.01.01_60/ts_103701v010101p.pdf ・CCDS: IoT機器セキュリティ要件適合基準ガイドライン 2023年版 [7.2-1 連絡窓口・セキュリティサポート体制] https://www.ccds.or.jp/public/document/other/CCDS_SecGuide-IoTReq_Criteria_2023_v1.0_jpn.pdf

☆1評価項目番号	10
評価結果	
エビデンスの名称	
エビデンスに基づく根拠	
セキュリティ要件（大項目）	3. ソフトウェアを最新の状態に保つ
セキュリティ要件	3-14. 製品のモデル名称は、製品上のラベル又は物理的インタフェースを介して、ユーザに対して明確に認識可能でなければならない。
☆1 適合基準	製品の型式番号は、以下のいずれかの方法でユーザへ提供すること。 ① 製品本体に、製品の型式番号を直接記載すること。 ② 製品のGUI、ウェブUI等や、製品に付帯するソフトウェア、アプリケーション（スマホアプリなど）のGUI、ウェブUI等から、ユーザが型式番号を認識できるようにすること。
NAとなるための条件、基準の補足説明	–
☆1 評価手法	ドキュメント評価：なし 本体確認・実機テスト：①又は②
☆1 評価ガイド	※ 以下の①又は②のいずれかの評価結果が「Y」である場合、本適合基準全体の評価結果が「Y」となる。 ［本体確認］ ① 製品本体を確認し、製品の型式番号が記載されていることを確認する。型式番号が記載されている場合、本適合基準の評価結果は「Y」となる。 ［実機テスト］ 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、製品の型式番号を確認する。型式番号を確認できる場合、本適合基準の評価結果は「Y」となる。
☆1評価に当たって参考となるガイドライン等	【評価に当たって参考となるガイドライン等】 ・ETSI TS 103 701 [5.3.16 Test group 5.3-16] https://www.etsi.org/deliver/etsi_ts/103700_103799/103701/01.01.01_60/ts_103701v010101p.pdf

☆1評価項目番号	11
評価結果	
エビデンスの名称	
エビデンスに基づく根拠	
セキュリティ要件（大項目）	4. 機密セキュリティパラメータをセキュアに保存する
セキュリティ要件	4-1. 製品のストレージにある機密セキュリティパラメータは、製品によってセキュアに保存されなければならない。
☆1 適合基準	製品のストレージに保存される守るべき情報資産（SDカード等、ストレージメディアに保存される守るべき情報資産も含む。）が、ネットワーク経由の不正アクセスに対して、セキュアに保存されること。
NAとなるための条件、基準の補足説明	【用語定義：守るべき情報資産】 以下のすべての情報： ・通信機能に関する設定情報 ・セキュリティ機能に関する設定情報 ・機器の意図する使用において、機器が収集し、保存又は通信する、個人情報等の一般的に機密性が高い情報
☆1 評価手法	ドキュメント評価：対象とする 実機テスト：なし
☆1 評価ガイド	[ドキュメント評価] 製品の技術文書を閲覧することで、製品のストレージに保存される守るべき情報資産（ストレージメディアに保存される守るべき情報資産も含む。）が、ネットワーク経由の不正アクセスに対して、セキュアに保存されることを評価する。以下のいずれかに類する保護対策又はそれ以上の対策が明示されている場合、本適合基準の評価結果は「Y」となる。 ・守るべき情報資産は、「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」に記載の暗号技術を採用した暗号化方式によって暗号化された上で保存される。 ・守るべき情報資産は、「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」に記載のハッシュ関数によってハッシュ化された上で保存される。 ・守るべき情報資産は、仮想化技術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。 ・製品に保存される個人情報は、匿名加工情報又は仮名加工情報に変換した上で保存される。
☆1評価に当たって参考となるガイドライン等	【暗号技術に関連するガイドライン】 -「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)」（最終改訂: 2022年3月30日、CRYPTREC LS-0001-2022） -「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」（初版：2022年6月、CRYPTREC LS-0003-2022） ※［上記ガイドラインの補足文書］ -「CRYPTREC 暗号技術ガイドライン (SHA-1) 改定版」(CRYPTREC GL-2001-2013R1) -「CRYPTREC暗号技術ガイドライン(軽量暗号)」(CRYPTREC GL-2003-2016JP) -「暗号鍵設定ガイダンス」(CRYPTREC GL-3003-1.0) -「暗号鍵管理システム設計指針 (基本編) 」(CRYPTREC GL-3002-1.0) -「TLS暗号設定ガイドライン」(CRYPTREC GL-3001-3.0.1) 【評価に当たって参考となるガイドライン等】 ・ETSI TS 103 701 [5.4.1 Test group 5.4-1] https://www.etsi.org/deliver/etsi_ts/103700_103799/103701/01.01.01_60/ts_103701v010101p.pdf ・CCDS: IoT機器セキュリティ要件適合基準ガイドライン 2023年版 [7.1-2 データ保護] https://www.ccds.or.jp/public/document/other/CCDS_SecGuide-IoTReq_Criteria_2023_v1.0_jpn.pdf

☆1評価項目番号	12
評価結果	
エビデンスの名称	
エビデンスに基づく根拠／NAであることの理由	
セキュリティ要件（大項目）	5. セキュアに通信する
セキュリティ要件	5-1. 製品は、ベストプラクティスの暗号技術を使用してセキュアに通信をしなくてはならない。
☆1 適合基準	ネットワーク経由で伝送される守るべき情報資産について、情報の盗聴に対する以下のいずれかの保護対策が行われていること。 ① 他のIoT機器やサーバ（クラウド上のサーバを含む）へネットワークを介して伝送される守るべき情報資産について、情報の盗聴に対する保護対策を機器自らが行う。 ② 他のIoT機器やサーバ（クラウド上のサーバを含む）へネットワークを介して伝送される守るべき情報資産について、保護された通信環境（VPN環境や専用線を経由した接続環境）においてのみ伝送される。
NAとなるための条件、基準の補足説明	【NAとなるための条件】 ネットワーク経由で伝送される守るべき情報資産が存在しない（「NAであることの理由」に、ネットワーク経由で伝送される守るべき情報資産が存在しないことを示す根拠を記載すること） 【用語定義：守るべき情報資産】 以下のすべての情報： ・通信機能に関する設定情報 ・セキュリティ機能に関する設定情報 ・機器の意図する使用において、機器が収集し、保存又は通信する、個人情報等の一般的に機密性が高い情報
☆1 評価手法	ドキュメント評価：①又は② 実機テスト：なし
☆1 評価ガイド	[ドキュメント評価] 製品の技術文書を閲覧することで、ネットワーク経由で伝送される守るべき情報資産について、情報の盗聴に対する保護対策が実装されていることを評価する。製品と連動するアプリがある場合、守るべき情報資産として、アプリから送信される情報も対象とした評価を行う。以下の①-A)、①-B)、②のいずれかについて確認できた場合、本適合基準の評価結果は「Y」となる。 ①-A) 製品の技術文書を閲覧し、守るべき情報資産をネットワーク経由で伝送する際に、「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」に記載の暗号技術を採用した通信プロトコルにて伝送することが明示されていることを確認する。 ①-B) 製品の技術文書を閲覧し、評価項目番号＃11に記載の保護対策を講じた守るべき情報資産がネットワークを経由して伝送されることが明示されていることを確認する。 ② 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、保護された通信環境（VPN環境や専用線を経由した接続環境）においてのみ製品を利用するよう、ユーザ向けに明示されていることを確認する。
☆1評価に当たって参考となるガイドライン等	【暗号技術に関連するガイドライン】 -「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)」 （最終改訂: 2022年3月30日、CRYPTREC LS-0001-2022） -「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」 （初版：2022年6月、CRYPTREC LS-0003-2022） ※［上記ガイドラインの補足文書］ -「CRYPTREC 暗号技術ガイドライン (SHA-1) 改定版」 (CRYPTREC GL-2001-2013R1) -「CRYPTREC暗号技術ガイドライン(軽量暗号)」(CRYPTREC GL-2003-2016JP) -「暗号鍵設定ガイダンス」(CRYPTREC GL-3003-1.0) -「暗号鍵管理システム設計指針 (基本編) 」(CRYPTREC GL-3002-1.0) -「TLS暗号設定ガイドライン」(CRYPTREC GL-3001-3.0.1) 【評価に当たって参考となるガイドライン等】 ・ETSI TS 103 701 [5.4.1 Test group 5.5-1] https://www.etsi.org/deliver/etsi_ts/103700_103799/103701/01.01.01_60/ts_103701v010101p.pdf ・CCDS: IoT機器セキュリティ要件適合基準ガイドライン 2023年版 [7.1-2 データ保護] https://www.ccds.or.jp/public/document/other/CCDS_SecGuide-IoTReq_Criteria_2023_v1.0_jpn.pdf

☆1評価項目番号	13
評価結果	
エビデンスの名称	
エビデンスに基づく根拠	
セキュリティ要件（大項目）	6. 露出した攻撃面を最小化する
セキュリティ要件	6-1. すべての未使用の物理的インタフェース及び論理的インタフェースは無効化しなければならない。
☆1 適合基準	製品において、外部からサイバー攻撃を受けるリスクを低減するために、製品の利用上不要かつ攻撃を受けるリスクがある物理的インタフェース及び論理的インタフェースを無効化するとともに、製品に対する脆弱性検査を実施すること。具体的には、以下の①・②のすべての基準を満たすこと。 ①製品において、高頻度で利用され、脆弱性などのリスクが想定される以下のインタフェースについて、製品の利用上不要かつ攻撃を受けるリスクがあるインタフェースを無効化すること。 A) TCP/UDPポート B) Bluetooth C) USB ②製品に対して脆弱性スキャンツールによる既知の脆弱性検査を実施し、攻撃に悪用される可能性がある脆弱性が検出されないこと。
NAとなるための条件、基準の補足説明	_
☆1 評価手法	ドキュメント評価：① 実機テスト：①、② ※①は、ドキュメント評価と実機テストの双方を実施すること
☆1 評価ガイド	[ドキュメント評価] ① 製品の技術文書を閲覧することで、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が無効化されていることを評価する。以下のA)～C)のすべてについて確認できた場合に限り、①に関するドキュメント評価の評価結果は「Y」となる。 A) TCP/UDPポート インバウンド通信において開放（LISTEN）しているTCP・UDPポートについて、対象のポート番号、利用用途、開放タイミング及び利用条件が明示されている。IPv6に対応した製品の場合、IPv4とIPv6の両方を対象とする。なお、攻撃に悪用されるリスクのあるtelnet（23/TCP及び2323/TCP）を利用している場合、その利用目的、開放タイミング及び利用条件を「エビデンスに基づく根拠」の欄に明記すること。 B) Bluetooth 製品がBluetoothを利用する場合、利用するBluetoothのプロファイル、利用目的が明示されている。廃止されたプロファイルを利用していないことを確認する。 C) USB 製品がUSBを利用する場合、利用するUSBデバイスクラスのクラス名、利用目的が明示され、不要なデバイスクラスについては無効化されていることを確認する。 [実機テスト] ① 対象製品の実機テストにより、A) TCP/UDPポートに関して、製品の利用上不要なインタフェースが無効化されていることを評価する。ポートスキャンツールを利用し、インバウンド側のTCP/UDPの開放ポートが、ドキュメント評価で得られた結果と一致していることを確認できた場合、実機テストによる本適合基準の①に関する評価結果は「Y」となる。 ② 脆弱性スキャンツールを利用した実機テストにより、攻撃に悪用される可能性がある脆弱性が検出されないことを評価する。以下のA)～B)の両方について確認できた場合に限り、実機テストによる本適合基準の②に関する評価結果は「Y」となる。 A) 開放されているポートについて、CVSSv3基準Severity 7.0以上の脆弱性が検出されないこと。 B) 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ないこと。脆弱性スキャンツールによるスキャンを実施し、[検索条件]に該当する脆弱性が検出されていないこと。 [URL] 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 なお、A)～B)において脆弱性が検出された場合でも、当該脆弱性の精査を行い、下記のいずれかに該当する場合は、実機テストによる本適合基準の②に関する評価結果は「Y」となる。 ・誤検知である場合 ※検出された脆弱性に対応する機能が、未実装である場合など ・運用対策を含む対策により、既に対策済みである場合 ・検出された脆弱性が実際の利用環境おいては、影響がないことを証明可能な場合 ・Exploit Codeを用いた実証テストを追加で実施し、攻撃が成功しない場合 ドキュメント評価による①、実機テストによる①・②のすべての評価結果が「Y」である場合に限り、本適合基準全体の評価結果が「Y」となる。
☆1評価に当たって参考となるガイドライン等	【①の実機テストに関するポートスキャンツール】 経済産業省「機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き」で記載のとおり、ポートスキャンにおいては、nmapやarp-scan等のツールが利用可能である。 [例：nmapにおけるスキャンコマンド] 下記のコマンドで、TCP/UDPの全ポートをポート1から順にスキャンを行う。 nmap -r -sS -sU -Pn -p 0-65535 "IPアドレス" 【②の実機テストに関する脆弱性スキャンツール】 経済産業省「機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き」で記載のとおり、ポートスキャンにおいては、Greenbone Vulnerability Management (GVM)、Nessus、Vuls等のツールが利用可能である。 [例：Greenbone Vulnerability Management (GVM)におけるスキャン手順] ・Targetの設定 －Port list：「All TCP and Nmap top 100 UDP」 ※ポートスキャンの結果、上記設定に含まれないUDPポートが検出された場合には、UDPの対象ポートリストを追加して作成し、設定する。 ・Scan Taskの設定 －Scanner：「OpenVAS Default」 －Scan Config：「Full and fast」 【評価に当たって参考となるガイドライン等】 ・ETSI TS 103 701 [5.6.1 Test group 5.6-1] https://www.etsi.org/deliver/etsi_ts/103700_103799/103701/01.01.01_60/ts_103701v010101p.pdf ・CCDS: IoT機器セキュリティ要件適合基準ガイドライン 2023年版 [7.1-1-1 TCP・UDP ポートの無効化] https://www.ccds.or.jp/public/document/other/CCDS_SecGuide-IoTReq_Criteria_2023_v1.0_jpn.pdf ・経済産業省：機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き https://www.meti.go.jp/policy/netsecurity/wg3/proven_in_japan.html

☆1評価項目番号	14
評価結果	
エビデンスの名称	
エビデンスに基づく根拠	
セキュリティ要件（大項目）	9. 停止に対してレジリエントなシステムにする
セキュリティ要件	9-1. データネットワークと電源の停止の可能性を考慮して、レジリエンスを製品とサービスに組み込まなければならない。
☆1 適合基準	停電等による電力供給の停止やネットワークの停止により、機器の電源がOFFになった後、電力供給が再開され、ネットワーク機能が復帰した際に、アクセス制御の際に使用する認証値（パスワード、秘密鍵など）の設定及びアップデートが完了したソフトウェアが工場出荷時の初期状態に戻ることなく、電源OFFになる直前の状態を維持できること。 なお、電気通信事業法に基づく端末機器セキュリティに係る技術基準を含めた技術基準適合認定を受けた製品（技適[T]マーク又は[A]マークが付与された製品）は、本適合基準に適合しているとみなす。（この場合、「基本情報」シートに「電気通信事業法に基づく技術基準適合認定番号等（技適[T]マークの設計認証番号又は[A]マークの技術基準適合認定番号）」を記入のこと。）
NAとなるための条件、基準の補足説明	_
☆1 評価手法	ドキュメント評価：なし 実機テスト：対象とする
☆1 評価ガイド	［実機テスト］ 工場出荷時からアクセス制御の際に使用する認証値の変更を行い、かつ、ソフトウェアのアップデートを行った製品に対して、実機テストにより評価する。以下のA)～B)の両方を確認できた場合に限り、本適合基準の評価結果が「Y」となる。 A) 製品に対する電源供給を停止させる（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）。その後、電源を復帰させた後、工場出荷時の初期状態に戻ることなく、電源OFFとなる直前の認証値及びアップデートが維持されることを確認する。 B) 通信ケーブルや無線接続を切断し、再接続した後、工場出荷時の初期状態に戻ることなく、電源OFFとなる直前の認証値及びアップデートが維持されることを確認する。
☆1評価に当たって参考となるガイドライン等	【評価に当たって参考となるガイドライン等】 ・ETSI TS 103 701 [5.9.1 Test group 5.9-1] https://www.etsi.org/deliver/etsi_ts/103700_103799/103701/01.01.01_60/ts_103701v010101p.pdf ・CCDS: IoT機器セキュリティ要件適合基準ガイドライン 2023年版 [7.1-3 ソフトウェア更新] https://www.ccds.or.jp/public/document/other/CCDS_SecGuide-IoTReq_Criteria_2023_v1.0_jpn.pdf

☆1評価項目番号	15
評価結果	
エビデンスの名称	
エビデンスに基づく根拠	
セキュリティ要件（大項目）	11. ユーザが簡単にデータを消去できるようにする
セキュリティ要件	11-1. ユーザは、簡単な方法で製品からユーザデータを消去できるような機能を提供されなければならない。
☆1 適合基準	製品利用中に製品のストレージに保存されたデータの削除機能について、以下の①・②のすべての基準を満たすこと。 ① ユーザによって、機器本体や関連サービス（モバイルアプリケーション等）を介して、ユーザに関する少なくとも以下のデータを削除できること。 A) 製品利用中に取得した情報資産（個人情報含む） B) ユーザ設定値 C) ユーザが設定した認証値、製品利用中に取得した暗号鍵やデジタル署名 ② データ削除後も、アップデートされたセキュリティ機能に関するファームウェア（ソフトウェア）パッケージのバージョンは維持されること。
NAとなるための条件、基準の補足説明	–
☆1 評価手法	ドキュメント評価：① 実機テスト：①、② ※①は、ドキュメント評価と実機テストの双方を実施すること
☆1 評価ガイド	［ドキュメント評価］ ①製品の技術文書において、ユーザによって、機器本体や関連サービス（モバイルアプリケーション等）を介して、ユーザに関する情報を消去できる機能を有することを評価する。少なくとも以下のデータを削除できる機能を有する場合、ドキュメント評価による本適合基準の①に関する評価結果は「Y」となる。 A) 製品利用中に取得した情報資産（個人情報含む） B) ユーザ設定値 C) ユーザが設定した認証値、製品利用中に取得した暗号鍵や署名 なお、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対象外となる。（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） ［実機テスト］ ① 対象製品の実機テストにより、上記A)～C)のいずれかのデータに関して、データ削除機能が動作することを評価する。実際にA)～C)のいずれかのデータを削除できる場合、実機テストによる本適合基準の①に関する評価結果は「Y」となる。なお、実機テストは、全ての対象データの削除を行わずに、削除対象となるデータの一部が実際に削除されていること確認するサンプルテストでも構わない。 ② 対象製品の実機テストにより、①の評価を行った後（データ削除後）も、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評価する。バージョン表示機能等でアップデートされたファームウェア（ソフトウェア）が維持されることを確認できた場合、実機テストによる本適合基準の②に関する評価結果は「Y」となる。 ドキュメント評価による①、実機テストによる①・②のすべての評価結果が「Y」である場合に限り、本適合基準全体の評価結果が「Y」となる。
☆1評価に当たって参考となるガイドライン等	【評価に当たって参考となるガイドライン等】 ・ETSI TS 103 701 [5.11.1 Test group 5.11-1] https://www.etsi.org/deliver/etsi_ts/103700_103799/103701/01.01.01_60/ts_103701v010101p.pdf ・CCDS: IoT機器セキュリティ要件適合基準ガイドライン 2023年版 [7.1-2-1 データ消去] https://www.ccds.or.jp/public/document/other/CCDS_SecGuide-IoTReq_Criteria_2023_v1.0_jpn.pdf

☆1評価項目番号	16
評価結果	
エビデンスの名称	
エビデンスに基づく根拠	
セキュリティ要件（大項目）	17. 製品に関する情報提供を行う
セキュリティ要件	17-2. 製造業者は、製品をセキュアに設定・利用・廃棄する方法について、ユーザに提供しなければならない。
☆1 適合基準	製造業者は、製品のサイバーセキュリティに関する情報提供について、以下の①～⑤のすべての基準を満たす対応を行うこと。 ①初期設定の方法など、製品の利用上、サイバーセキュリティに影響が生じる設定や使用方法について、安全に利用できる手順を周知すること。 ②製品のセキュリティアップデートの内容や必要性、アップデートを行わない場合の影響などを周知すること。 ③アップデートを行わなかったときに想定される事故や障害・一般的に想定される事故や障害に対して、免責事項を周知すること。 ④対象製品やサービスのサポート期限又はサポート終了時の方針を周知すること。 ⑤製品内に守るべき情報資産が残留したまま廃棄や中古販売することで想定されるリスクや、データ消去を含む製品の安全な利用終了方法を周知すること。
NAとなるための条件、基準の補足説明	–
☆1 評価手法	ドキュメント評価：①、②、③、④、⑤ 実機テスト：なし
☆1 評価ガイド	［ドキュメント評価］ ①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、初期設定の方法など、製品の利用上、サイバーセキュリティに影響が生じる設定や使用方法について、安全に利用できる手順が明示されていることを評価する。ID及びパスワード変更の実施手順、パスワード変更時に特定しにくい値を用いる方法等が明示されている場合、本適合基準の①に関する評価結果は「Y」となる。 ②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、製品のセキュリティアップデートの内容や必要性、アップデートを行わない場合の影響などが明示されていることを評価する。以下に類する内容又はそれ以上の内容が明示されている場合、本適合基準の②に関する評価結果は「Y」となる。 ［アップデートの目的］ －機能の追加や変更なのか、あるいは不具合や脆弱性の修正なのかを明示する ［不具合や脆弱性の情報］ －発生する問題の概要と製品ユーザへの影響を明示する －問題が発生するソフトウェア/ファームウェアバージョン情報を明示する ［アップデートの方法・手順］ －自動更新かマニュアル操作による更新が必要なのかを明示する －マニュアル操作による更新の場合は、具体的な手順や、アップデートプログラムの入手先（ウェブリンクやURL）を明示する －アップデートにより製品の機能に影響が出る場合や、製品に対するアップデートの実施が困難である場合は、その理由や対処方法を明示する ［アップデートの実行者］ －ユーザで行うのか、製造業者で行うのか、第三者（運用担当者、保守担当者など）で行うのかを明示する ③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、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が明示されていることを評価する。免責事項が明示されている場合、本適合基準の③に関する評価結果は「Y」となる。 ④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、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が明示されていることを評価する。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が明示されている場合、本適合基準の④に関する評価結果は「Y」となる。 ⑤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、製品内に守るべき情報資産が残留したまま廃棄や中古販売することで想定されるリスクや、データ消去を含む製品の安全な利用終了方法が明示されていることを評価する。製品内に守るべき情報資産が残留したまま廃棄や中古販売することで想定されるリスクや、データ消去を含む製品の安全な利用終了方法が明示されている場合、本適合基準の⑤に関する評価結果は「Y」となる。 ①～⑤のすべての評価結果が「Y」である場合に限り、本適合基準全体の評価結果が「Y」となる。
☆1評価に当たって参考となるガイドライン等	【評価に当たって参考となるガイドライン等】 ・ETSI TS 103 701 [5.3.11 Test group 5.3-11], [5.3.13 Test group 5.3-13], [5.11.3 Test group 5.11-3], [5.12.1 Test group 5.12-1]、 https://www.etsi.org/deliver/etsi_ts/103700_103799/103701/01.01.01_60/ts_103701v010101p.pdf ・CCDS: IoT機器セキュリティ要件適合基準ガイドライン 2023年版 [7.2-3 ユーザへの情報提供] https://www.ccds.or.jp/public/document/other/CCDS_SecGuide-IoTReq_Criteria_2023_v1.0_jpn.pdf

用語	意味
IoT機器	ネットワークに接続された（及びネットワークに接続可能な）機器で、関連サービスとの関係を持つもの。 注 1： IoT機器は、一般的にビジネスの環境においても使用される。 注 2： IoT機器は、多くの場合、消費者が小売り環境で購入することができる。IoT機器は、専門的に委託及び／又は設置することもできる。
IoT製品	IoT機器とその関連サービス。
外部感知機能	ある対象の情報を収集し、機械が取り扱うことのできる信号に置き換える素子や装置のこと。例：光学センサ、音響センサ、カメラ、マイク
管理者	機器のユーザに対して可能な最高の特権レベルを持つユーザ。これは、意図された機能に関連する設定を変更できることを意味する。
関連サービス	機器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のこと。 例：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）。
関連サービス	機器と共にIoT製品全体の一部であり、通常は製品の意図された機能を提供するために必要なデジタルサービス。 例 1： 関連サービスには、モバイルアプリケーション、クラウドコンピューティング／ストレージ、及びサードパーティのアプリケーションプログラミングインタフェース（API）を含めることができる。 例 2： ある機器は、機器の製造業者によって選択されたサードパーティのサービスにテレメトリデータを送信する。このサービスは関連サービスである。
技術文書	適合基準への適合を示す根拠となる文書で、製品の設計書、仕様書、開発手順書、マニュアル等のこと。公開・非公開の区分は問わない。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。
機密な個人データ	その開示が個人に害を及ぼす可能性が高いデータのこと。 「機密な個人データ」として扱われるものは、製品やユースケースによって異なるが、例えば、家庭用セキュリティカメラのビデオストリーム、支払い情報、通信データの内容、タイムスタンプ付きの位置データなどが例として挙げられる。
機密のセキュリティパラメータ	重要なセキュリティパラメータ及び公開セキュリティパラメータ。
機密の製造業者	他の多くのサプライヤの製品及びコンポーネントを含む可能性がある、組み立てられた最終IoT製品を作るエンティティ。
公開セキュリティパラメータ	セキュリティ関連の公開情報で、改ざんされるとセキュリティモジュールのセキュリティが侵害される可能性があるもの。 例 1： ソフトウェアアップデートの真正性／完全性を検証するための公開鍵。 例 2： 証明書の公開要素。
工場出荷時のデフォルト	工場出荷時の状態にリセットした後の状態、又は最終的な製造／組み立て後の機器の状態。 注： これには、物理的な機器と、組み立て後にその機器に存在するソフトウェア（ファームウェアを含む）が含まれる。
構成設定	情報システムのセキュリティ体制や機能に影響を与える、ハードウェア、ソフトウェア、またはファームウェアで変更できるパラメータのセットのこと。
個人データ	識別された、又は識別可能な自然人に関するあらゆる情報。 注： この用語は、周知の用語と整合させるために使用されているが、本文書内では法的意味を持たない。
自己完結型の環境	他のサービスに依存せず単独で利用できる環境のこと。
重要なセキュリティパラメータ	曝露又は改ざんによってセキュリティモジュールのセキュリティが侵害される可能性がある、セキュリティ関連の秘密情報。 例： 秘密の暗号鍵、パスワードなどの認証値、PIN、証明書のプライベート要素。
消費者	自己の商取引、ビジネス、工芸、専門的職業以外の目的のために行動している自然人。 注： あらゆる規模の企業を含む組織が、IoTを利用している。例えば、スマートテレビは会議室に頻繁に導入されているし、ホームセキュリティキットは小規模企業の敷地を保護することができる。
初期化	操作のために機器のネットワーク接続を有効化し、オプションとしてユーザ又はネットワークアクセスのための認証機能を設定するプロセス。
初期化状態	初期化後の機器の状態。
所有者	機器を所有するユーザ、又は購入したユーザ。
製造業者	サプライチェーン内の関連事業者（製品の製造業者を含む）。 注： この定義は、 IoT機器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。製品の製造業者以外にも、例えば目前の特定のケースに応じて、輸入業者、販売業者、インテグレータ、コンポーネント及びプラットフォームプロバイダ、ソフトウェアプロバイダ、IT 及び電気通信サービスプロバイダ、マネージドサービスプロバイダ及び関連サービスのプロバイダなどがある。
制約のある機器	データを処理する機能、データを通信する機能、データを保存する機能、又はユーザと対話する機能のいずれかにおいて、意図された使用のために物理的な制約がある機器。 注 1： 物理的な制約は、電源、バッテリ寿命、処理能力、物理アクセス、機能の制限、メモリの制限、又はネットワーク帯域幅の制限による場合がある。制約のある機器は、基地局やコンパニオンデバイスなどの別の機器によってサポートされることが必要となる場合がある。 例 1： バッテリを充電又は交換できない窓センサ。 例 2： ストレージの制限により、機器のソフトウェアをアップデートすることができないため、セキュリティの脆弱性を管理するためには、ハードウェアの交換又はネットワークの分離しか選択肢がない機器。 例 3： 様々な場所に配置できるようにバッテリを使用している低電力機器。これらの機器では、高電力な暗号化処理を実行するとバッテリの寿命が急速に短くなるため、アップデートの検証は基地局又はハブに頼っている。 例 4： Bluetooth ペアリングのためのバインドコードを検証するための表示画面がない機器。 例 5： 認証情報を入力する機能がない機器。（キーボードを介した入力機能など） 注 2： 有線接続された電源を有し、IP ベースのプロトコル及びそのプロトコルで使用される暗号プリミティブをサポートできる機器は、制約のある機器のある機器ではない。 例 6： コンセントを使って給電され、主に TLS（トランスポート層セキュリティ）を使用して通信を行う機器。
セキュリティアップデート	製造業者が発見した、又は製造業者に報告されたセキュリティの脆弱性に対処するためのソフトウェアアップデート。 注： 脆弱性の深刻度が、より高い優先度の修正を必要とする場合、ソフトウェアアップデートは純粋なセキュリティアップデートになり得る。
セキュリティモジュール	セキュリティ機能を実装する、ハードウェア、ソフトウェア、及び/又はファームウェアのセット。 例： 機器には、ハードウェアの信頼の基点、信頼できる実行環境内で動作する暗号化ソフトウェアライブラリ、及びユーザの分離やアップデートメカニズムなどのセキュリティを強化する OS 内のソフトウェアが含まれている。これらすべてが、セキュリティモジュールを構成している。
ゾーン	検討対象のシステムを、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。
デバイスごとに固有	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。

用語	意味
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）
汎用個人間通信	汎用個人間通信システムにおいて用いられる通信のこと。
汎用個人間通信システム	通常、制御システムの運用とは関係のない私的な目的で利用されるシステムのこと。 汎用個人間通信システムには、電子メールシステム、ソーシャルメディア（ツイッター、フェイスブック、画像ギャラリーなど）、実行可能ファイルの送信を許可するメッセージシステムなどが含まれる。
物理インタフェース	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。