JST-EG-01-01-2024

セキュリティ要件適合評価及びラベリング制度（JC-STAR）★1 評価ガイド

令和６年１２月

独立行政法人情報処理推進機構

目次

1. はじめに

本ガイドは、「★1 レベル適合基準・評価手法」に記載された評価手法で求められる評価内容について、具体的にどのように評価を行うかを記載したものである。

1.1 チェックリストの記載方法

チェックリストに記載する評価結果は、本ガイドに記載されている評価項目及び評価手順に従って実施する必要がある。

【評価結果について】

★1 適合基準の 16 個の評価項目それぞれについて、本ガイドに基づく評価を実施し、「適合（Y）」、「非適合（N）」、「対象外（NA）」のいずれかを結論を得る。なお、対象外（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ないことに留意されたい。

【注意】 16 個の評価項目の評価結果のうち、一つでも「非適合（N）」があると適合ラベルの申請はできない。

【証跡（エビデンス）について】

- 「適合（Y）」の場合、以下の内容を含む証跡（エビデンス）の情報を各評価項目のチェックリスト欄に記載する。
  - 「ドキュメント評価」に基づく評価の場合：
    評価に用いた技術文書や社内文書・規程等の名称、ウェブサイト、文書番号等の情報、及び根拠が記載された該当箇所がわかる情報（名称、文書番号、ページ番号、章番号、URL 等）
  - 「実機テスト」に基づく評価の場合：
    実機テストの検証結果が確認できる情報・文書等の名称（写真、動画、スクリーンショット、ログ（システム出力）等）、及び評価結果の概要
    - 製品の開発時点で実施したテスト結果や、他の認証（Common Criteria 等）の取得時に作成・評価した文書類を、本制度における実機テストのための証跡（エビデンス）として流用することは可能である。その場合には、当該文書等を証跡（エビデンス）として保管すること
- 「対象外（NA）」の場合、「対象外（NA）」であることの理由を説明する文書等の証跡（エビデンス）を用意する必要がある。「対象外（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（なぜ対象外となっても問題がないのか／代替策で対応しているのか）と判断するための根拠を記載する。具体的に記載する内容については、

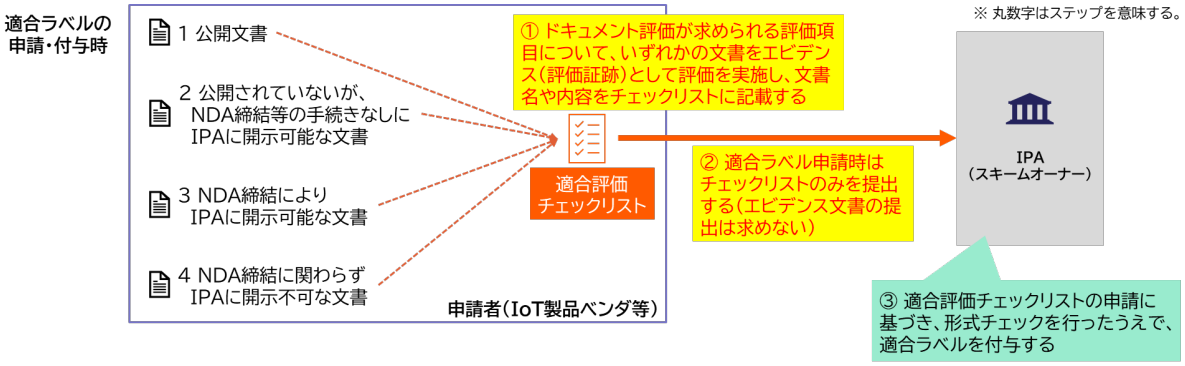
各評価項目において「対象外となるための条件」に記載されているので、それに従って理由を説明しなければならない。

1.2 証跡（エビデンス）の取扱いについて

★1 評価においては、ドキュメント評価の対象とする文書等をどのように用意するかは IoT 製品ベンダーが選択できる形式とする。1.1 節で記載されているように、各評価項目について、用意した文書等の証跡（エビデンス）に基づいて評価を実施し、当該文書名や評価結果をチェックリストに記載する。

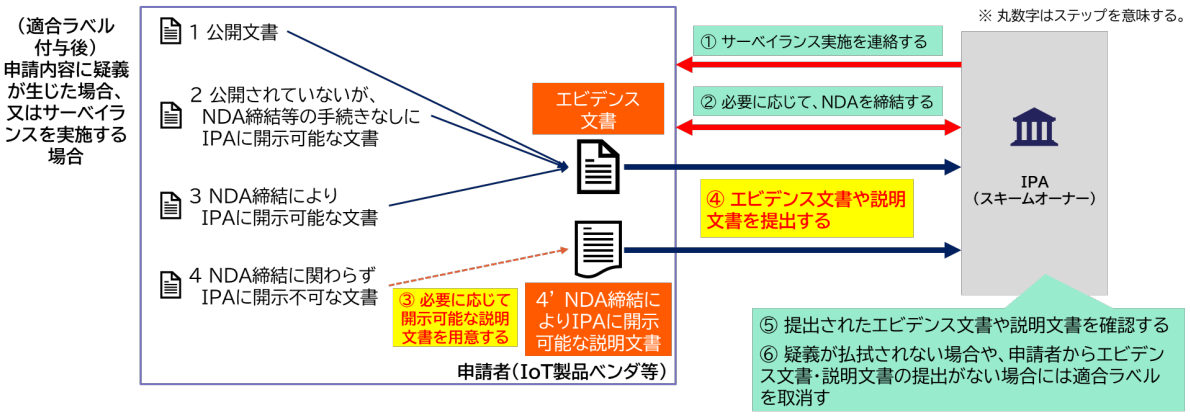
【申請時点での取扱い】

- 適合ラベル申請時は、適合評価チェックリストの提出のみを申請者に求め、証跡（エビデンス）の提出は求めない
- 適合ラベルの有効期間中、証跡（エビデンス）となる文書類の保管を義務付ける



【サーベイランス等での取扱い】

- 適合ラベル付与後、申請内容に疑義が生じた場合又はサーベイランスを実施する場合、IPA は証跡（エビデンス）の文書類の提出を求める。「NDA 締結に関わらず IPA 提示不可な文書」については、別途開示可能な説明文書による説明を認める
- 適切な説明と認められない場合は適合ラベルを取消す



1.3 JC-STAR 評価機関・JC-STAR 検証事業者等、外部機関の利用について

★1 の自己適合宣言では、IoT 製品ベンダー自身による自己適合評価を想定しているものの、★1 の適合基準・評価手順にもツールを使用した実機テストが含まれており、自社の既存体制や既存設備で十分な適合評価を実施できない、評価にかかるコストや時間、稼働を削減したい等の理由により、評価やチェックリストの作成を JC-STAR 評価機関や JC-STAR 検証事業者等の外部機関に依頼することができる。

JC-STAR 評価機関とは、製品評価技術基盤機構（NITE）の製品評価技術基盤機構認定制度(ASNITE)の中に、JC-STAR の★3 以上の評価を行える事業者について ISO/IEC17025 に基づく JC-STAR 評価機関認定制度を設け（2025 年度以降）、適切な能力及び体制を整備した事業者を「JC-STAR 評価機関」として認定する予定である。★1 の適合評価を JC-STAR 評価機関に依頼することも可能で、チェックリスト全体を JC-STAR 評価機関が作成した場合、「JC-STAR 評価機関による適合評価」として適合ラベルの申請ができる。なお、JC-STAR 評価機関認定制度による認定が開始されるまでの期間は、「IT セキュリティ評価及び認証制度（JISEC）」において製品分野「ソフトウェア」の評価及び ST 確認を実施する評価機関を、「JC-STAR 評価機関」相当とみなす暫定措置をとる。これらの評価機関については、JISEC の評価機関リストのページを参照されたい。

JC-STAR 検証事業者とは、経済産業省が策定した「情報セキュリティサービス基準」への適合性について審査及び登録する「情報セキュリティサービス基準審査登録制度」の「機器検証サービス（2023 年 9 月より募集開始）」区分にサービスが登録されている事業者のことを指す。チェックリスト全体を JC-STAR 検証事業者が作成した場合、「JC-STAR 検証事業者による適合評価」として適合ラベルの申請ができる。機器検証サービスの登録事業者については、情報セキュリティサービス基準適合サービスリストの機器検証サービスリストを参照されたい。

【外部機関を利用した際のチェックリストの取扱い】

- JC-STAR 評価機関又は JC-STAR 検証事業者に評価を依頼しチェックリストを作成してもらったときには、「チェックリスト」の評価方法で「適合評価外部依頼」を選択できる。
- ただし、JC-STAR 評価機関又は JC-STAR 検証事業者において、ベンダーからのエビデンス文書を受領できなかったことに起因して評価ができなかった項目が一つでもある場合のチェックリストは、全体を「申請者による自己評価結果」とし、「JC-STAR 評価機関又は JC-STAR 検証事業者が実施した評価結果」とはみなさない
- JC-STAR 評価機関又は JC-STAR 検証事業者以外の外部機関を利用すること自体は問題ない。ただし、「チェックリスト」の評価方法では「自己適合評価」を選択する必要がある

2. ★1 レベル適合基準の考え方

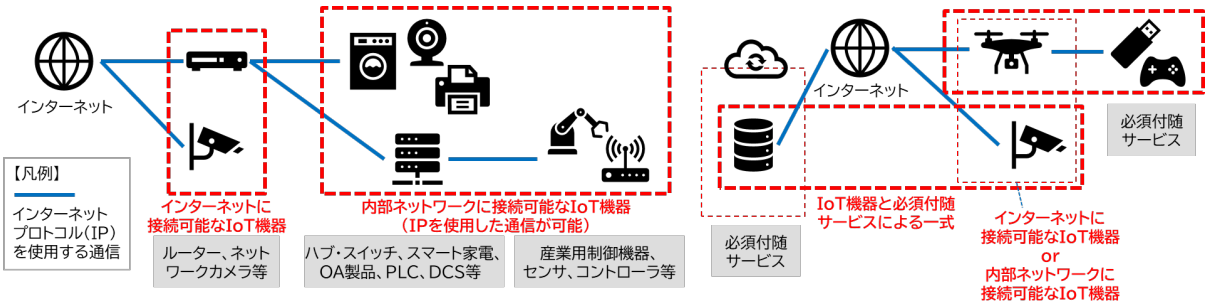
2.1 対象となる IoT 製品（の定義）の考え方

本制度は、以下の条件すべてを満たす IoT 製品に対して必要なセキュリティ機能を予め具備することを求めることに主眼がある。この意図は、【インターネットにつながる可能性がある】IoT 製品の中でも調達者・利用者が**【購入時点で具備されているセキュリティ機能を使い続ける】**しかセキュリティを確保する手段がない製品に対して、**【製品購入前】**に必要なセキュリティ機能が予め**【具備されているかを確認】**することが重要であり、その確認手段として**【適合ラベルという形で可視化】**するというものである。

そのため、本制度では「インターネットと通信できる IoT 機器（条件①②③）でありながらも、購入時点で IoT 製品に具備されているセキュリティ機能を利用し、（脆弱性対策のためのアップデート以外の）新たなセキュリティ対策を後から追加することが難しい／想定しない IoT 機器（条件④）」に合致する IoT 製品を対象とする。

例示として記載されている製品以外にも、条件①～④のすべてに該当する IoT 製品は対象となり得る。一方、PC やスマートフォン、タブレットなどが対象から除外されているのは、条件④を満たさないためである。適合ラベル取得検討中の IoT 製品が対象となるかどうかについては、条件①～④のすべてに該当するかどうかによって判断されたい。

① 機器が含まれている（機器に対してラベルが付与される）
② インターネットプロトコル（IP）を使用したデータの送受信機能を持つ
③ 直接・間接を問わず、インターネットにつながる（可能性がある／否定できない）
④ 購入時に具備されているセキュリティ機能を利用し、アップデート以外で（調達者・利用者が自らの意志で）後からセキュリティ機能を追加することが困難／できない



【補足】

- 条件①は、適合ラベルが付与される対象が機器であるため、ソフトウェアやクラウドサービスなど、機器がない場合は対象外となることを意味している。
- 条件②と条件③は、インターネット側からの攻撃ができる可能性がある場合は対象になるということを意味している。このため、直接・間接を問わず、インターネットにつながる場合には対象となる。

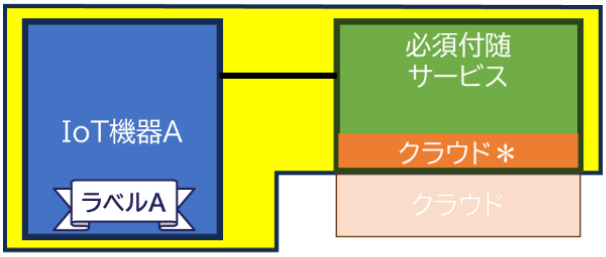
- 例えば、インターネット側からの通信に対して、VPN 装置や FW 装置などの論理的な制御（アクセス制御）によって境界防御が行われており、内部への通信が制限されるような環境であっても、当該アクセス制御に対する不正アクセス等のリスクがあるため、完全にインターネットから分離されているとは判断できない。このため、論理的な制御（アクセス制御）によってインターネットから分離されている内部におかれる機器についても「インターネットにつながる可能性がある／否定できない」と判断され、本制度の対象範囲に含まれる
- インターネットにつながる機器によって、インターネット側からの通信に対して何らかの変換処理等が実施され、当該機器より内部にある機器に対してインターネットからの直接通信を許可しないように、物理的分離、又は完全な論理的切断による分離されている環境であれば、完全にインターネットから分離されていると判断される。この場合には、当該機器から内部におかれる機器は「インターネットにつながる可能性がない」と判断できるので、本制度の対象範囲外となる。ただし、機器によっては「インターネットにつながる可能性がなく本制度の対象外なので、適合ラベルを取っていない」のか、「インターネットにつながる可能性があり本制度の対象に含まれるが、適合ラベルを取っていない」のかの判断が調達者・利用者にとって難しいケースが考えられる。このような場合には、IoT 製品ベンダーの自主的な判断により、本来は対象外であっても適合ラベルの取得申請をすることができる

- 条件④は、当該 IoT 製品に対して IoT 製造ベンダー以外が供給する別の対策ソフトウェア等を組み込むことができない／困難であるということを意味している。なお、IoT 製造ベンダー自身がアップデートにより新たなセキュリティ機能を追加することは、「サポート」の一環であり、条件④の「後からセキュリティ機能を追加」に該当しないことに注意されたい
- PC やスマートフォン、タブレットなどは、条件④を満たさないため原則的には本制度の対象から除外される。ただし、以下の条件のすべてを満たしていれば、PC やスマートフォン、タブレットなどがベースとなっていても IoT 製品としてラベルの取得は可能である
  I. セキュリティ機能のインストール（追加すること）を完全に自社のアプリ又は OS が制御しており、当該アプリ又は OS の管理機能を回避して（アップデート提供される場合を除いた、一切の）セキュリティ機能のインストールができないように作られている
  II. 自社アプリを削除したりフォーマットや OS の入替等をしたりしても、汎用の PC・タブレットとして利用できるようにならない対策がされている
  III. 汎用 OS ベンダーが提供する脆弱性対応の適用を適切にコントロールできる（ディストリビューションとして OS セキュリティパッチの独自配布等）

2.2 必須付随サービスの考え方

必須付随サービスとは、対象となる「IoT 機器」が「必ずセットで利用するサービス」のことを指す。具体的には、【当該 IoT 機器本体だけでは、当該 IoT 製品が意図した目的を提供できない】場合に、当該 IoT 機器に付随して提供されるサービスのことである。

例＞ NW カメラ(IoT 機器 A)が撮影した映像を特定のクラウドサービス X に保存するように設定されている場合、当該サービス X は必須付随サービスである。この場合、適合ラベルの評価対象範囲は、「IoT 機器 A」、「クラウドサービス X」及びその両者をつなぐ通信路全体となる。なお、適合ラベルは「IoT 機器 A」に対して付与される。



＊：サービスが直接的に利用するクラウド領域

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

2.3 ★1 で実現したいセキュリティ水準の考え方

★1 では、特定の製品類型に絞らず、広範な IoT 製品を対象とした統一的な基準とする観点から、どのような IoT 製品であれ対策すべき最低限の脅威に対抗することを目的とする。この目的に鑑み、★1 で実現したいセキュリティ水準の考え方は、以下のものである。

① マルウェアに感染してボット化するのを防ぐ。とりわけ、感染した機器からの感染拡大を防止する
② インターネット側からの遠隔攻撃を主に想定し、スクリプトキディレベル（限定的な専門知識のみを有し、インターネットやダークウェブなどで公開されているクラックツール等を用いてシステムの脆弱性を利用して攻撃するレベル）の攻撃（不正アクセスや盗聴など）に対して実用的な耐性を持たせる
③ 製品不具合や脆弱性に対する対応・サポート方針を明確化し、適合ラベル有効期間内のサポート（アップデートファイルの提供等）が確実に提供されるようにする

④　廃棄・転売時に、IoT 製品の運用中に生成されたデータを適切に削除することができるなど、守るべき情報が漏えいする脅威に対して適切に対策されている

以上の考え方を前提として、★1 で主に想定する情報資産、アタックサーフェス、脅威や対策などを検討し、適合基準や評価手法・評価項目として定められている。

2.4　守るべき（保護すべき）情報資産の考え方

★1 では、①運用中はインターネット側から遠隔攻撃される想定（紛失・盗難、不法侵入等による物理的接触に伴う攻撃は想定しない）、②廃棄・転売時には運用中に生成された情報資産は削除されている状態（情報の削除機能が有効に働き、利用者がその機能を利用して当該情報資産を削除したうえで廃棄・転売を行うと想定）を前提する。

★1 において守るべき情報資産とは、そのような前提においても、どのように保護するのかを考える必要がある情報資産のことである。

【★1 での保護対象の情報資産の例】

例えば、★1 での保護対象を以下のように考えることができる。

- 「有線通信機能」「無線通信機能」「セキュリティ機能」は、製造ベンダーが管理すべき機能であり、ライフサイクルを通じて保護すべき情報資産である、
- 「IoT 機能（通信機能）に関する設定情報」「セキュリティ機能に関する設定情報」は、運用中に常時利用される情報であるので、運用中は保護すべき情報資産である。廃棄・転売時は情報削除又はデフォルト化する。
- 「機器が収集し、保存又は通信する、一般的に機密性が高い情報」は、原則的には保護すべき情報資産である。ただし、当該情報の保存方法により、例えば、以下のように扱い方を分けることができる。
  - 無期限に保存され続ける、又はインターネットから呼び出せるなら運用中は保護すべき情報資産として扱う。
  - 合理的期間経過後に自動的に削除・破棄される設定になっているなら保護対象外の情報資産として扱うことができる。廃棄・転売時は情報削除を必須とする。

2.5　セキュアな保存（保護方法）の考え方

守るべき情報資産に対する「守る」手段として、必ずしも機密性保護だけを意味するものではない。例えば、一言「IoT 機能（通信機能）に関する設定情報」といっても、「機密性保護」が必要な情報、「完全性保護」が必要な情報、「真正性確認」が必要な情報、そういった保護までは必要としない情報とに分類される（情報によっては複数に該当することもある）。その分類に応じ

て、「機密性保護」「完全性保護」「真正性確認」のいずれかが必要となる情報資産については、それぞれに対応する対策が必要となる。

① 外部に不正に漏えいしないように保護する必要がある情報資産に対しては、「機密性」を保護することが必要
② 改ざんされないように保護する必要がある情報資産に対しては、「完全性」を保護することが必要
③ 情報資産の作成者や提供者をなりすまされないようにする必要がある情報資産に対しては、「真正性」を確認できることが必要

例えば、「セキュアな保存」では、保護が必要な情報資産について、それぞれ必要となる「保護をどのように施してセキュアに保存」するのかまで定めることが重要である。

★1 では、「セキュアな保存」は、以下の 2 つの脅威の対策を想定している。

1）ネットワークを介した、アクセス制御を介さない不正アクセス
2）ネットワークを介さない、アクセス制御を介さない不正アクセス

ここで、「アクセス制御を介さない不正アクセス」とは、正当なアクセス制御を行うインタフェースを経由しない不正アクセスのことで、例えば、マルウェアが不正な権限でファイルを搾取したり、廃棄された IoT 機器のストレージに直接アクセスするような場合を想定している。(「アクセス制御を介した不正アクセス」に対しては、本制度ではユーザ認証を適切に行う対策により、その脅威に対抗しているとみなす。)

具体的には、★1 では、攻撃者の能力を「スクリプトキディレベル」と想定することから、インターネットやダークウェブ等で公開されているクラックツール等を用いてシステムの脆弱性を利用した攻撃や廃棄・転売された IoT 機器が保持し続ける守るべき情報資産への物理的な不正アクセスが想定される脅威である。そのような脅威に対する対策を行うとの考え方から、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取られている場合に「セキュアな保存」とみなす。特に、ｄ.～ｆ.については「機密性」と「完全性」の保護が同時に達成されていると判断する。

a. 機密性を保護すべき守るべき情報資産は、適切な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ている
b. 完全性を保護すべき守るべき情報資産は、適切な暗号技術を利用した署名によってデータの完全性が保護されている
c. 完全性を保護すべき守るべき情報資産は、適切なハッシュ関数を用いたメッセージダイジェストによってデータの完全性が確認されている
d. 守るべき情報資産は、セキュリティチップなどハードウェア機能として提供されるセキュア領域に保存されている
e. 守るべき情報資産は、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によるセキュア領域に保存されている

f. 守るべき情報資産は、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であって、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に保存されている、又はそのようなインタフェースを備えない

2.6 セキュアな通信が求められる（or 除外可能な）範囲の考え方

★1 では、運用中は「インターネット側からの遠隔攻撃」を主に想定することから、セキュアな通信が求められる対象となる IoT 機器、及びセキュアな通信が求められる対象外とすることができる IoT 機器の範囲を以下のように考える。

A) インターネット側からつなげられる可能性がある範囲内にある IoT 機器はセキュアな通信が求められる対象である。
ここで、「つなげられる可能性がある」とは、インターネットと直接通信できる状態にあるということのほかに、「論理的には、許可なくインターネットと直接通信できないようにアクセス制御されていても、そのアクセス制御を行う部分がインターネットから呼び出せる」場合を含む。例えば、ログイン画面を表示する場合などがある。また、VPN 装置やルータ等によりインターネットから隔離された閉域ネットワーク内に置かれる IoT 機器であっても、当該 VPN 装置やルータ等を経由してインターネットと通信できる状態になりうるのであれば対象である。

B) VPN 装置やルータ等によりインターネットから隔離された閉域ネットワーク内に置かれ、かつその機器によってインターネット側からつなげられる可能性を遮断できる（インターネットとは通信が許可されない）IoT 機器に対しては、「インターネット側からの通信を遮断する機器に接続して利用する」旨の注意をユーザに明示することを条件に、セキュアな通信が求められる対象外とすることができる。具体的には、入室管理されたエリアで使用する有線ネットワーク環境やWPA2／WPA3によって接続する機器を制限するように構成された無線 LAN 環境等で構成され、VPN 装置／ルータ／ファイアウォール等でインターネットから分離されたネットワーク環境が想定され、そのネットワーク環境内であればインターネットからの不正なアクセスに対して必要な保護対策が取られているので通信が暗号化されていなくても盗聴のリスクが防がれていると判断される。
例えば、ホームルータの設定によってインターネット側からのアクセスが遮断されたホームネットワーク内で利用する IoT 製品に対しては、「本製品は、インターネットからのアクセス可否を安全に管理しているホームルータに接続して利用してください。」などの注意をユーザに明示することで、通信の暗号化を行わないケースが想定される。

2.7 サポート提供の義務について

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。

★1 の有効期間は原則 2 年であるが、申請時点で 2 年以内にサポートが終了することが予めわかっている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）。

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関わらず、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販売条件としたうえで、当該契約を締結した調達者に対してのみ販売する場合に限り、有償でのサポートの提供を認める。

なお、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. ★1 適合評価ガイド

本節は、★1 適合基準の各要件について、当該要件の評価結果が「適合（Y）」「非適合（N）」「対象外（NA）」のいずれかになるかを具体的に判断するための評価ガイドである。評価者は、本評価ガイドに記載の内容に従って評価を実施し、その結果を★1 チェックリストの該当箇所に記入する。

【★1 適合評価ガイドの構成】

適合基準ごとに以下のような構成で記載されている。

【★1 適合基準　S1.1-xx】	適合基準番号
★1 適合基準	（★1 レベル適合基準・評価手法からの引用） ★1 適合基準の要件
対象外(NA)となるための条件、基準の補足説明	（★1 レベル適合基準・評価手法からの引用） ★1 適合基準の対象外となるための条件、及び★1 適合基準の補足説明。 対象外（NA）と判定する場合には、評価者は本項目に記載された「対象外（NA）となるための条件」を満たしていることの証跡（エビデンス）を保管する必要がある。
★1 評価手法	（★1 レベル適合基準・評価手法からの引用） 適合評価のために実施する評価手法

★1 評価ガイド	
1.　適合評価基準	当該適合基準に対して「適合（Y）」「非適合（N）」のいずれかになるかを具体的に判断するために実施すべき評価項目と、「適合（Y）」と判定するための基準が定められている。 評価者は、各評価項目に記載の内容に従って評価を実施し、最終的な判定結果を得ること。また、その判定に利用した文書類や評価報告書等を証跡（エビデンス）として保管する必要がある。
2.　補足説明	
2.1.　適合判断基準に関する補足説明	適合評価基準の内容についての補足説明、適合判断のための補足説明や基準解釈の考え方、用語の補足説明等を参考にまとめている。
2.2.　例外的なケースでの適合判断	例外的なケースでの適合判断の考え方をまとめている。 例外的なケースに該当する IoT 機器に対してのみに適用される基準や補足説明が整理されたものであり、限定的

	な利用環境で使われることを前提として、通常とは異なる判定基準によって「適合（Y）」「非適合（N）」の判定を行う際の考え方や利用条件を設ける際の考え方が示されている。

【★1 チェックリストでの記載】

チェックリストでは、適合基準の要件ごとに評価結果を記入する「評価結果記入シート」と、「評価結果一覧」シートとで構成されている。なお、「評価結果一覧」シートは、「評価結果記入シート」の記入内容が自動転記される。

評価者は、適合基準の要件ごとに本評価ガイドに記載の内容に従って実施した評価結果を当該要件の「評価結果記入シート」に記入する。記入する内容は以下の通りである。

★1 適合基準番号	S1.1-01
評価結果	「適合（Y）」「非適合（N）」「対象外（NA）」のいずれかを選択する
証跡（エビデンス）の名称	以下の情報を記載する 【ドキュメント評価】 ● 評価に用いた技術文書等の名称 ● 評価に用いた社内文書・規程等の名称 【実機テスト】 ● 実機テストの検証結果が確認できる情報・文書の名称（報告書、写真、動画、スクリーンショット、ログ（システム出力）等） ※ 製品開発時点で実施したテスト結果や、他認証取得時の評価結果の再利用可
証跡（エビデンス）に基づく根拠／対象外（NA）であることの理由	評価項目ごとに以下の情報を記載する ● 「ドキュメント評価」に基づく評価の場合： 証跡（エビデンス）に基づく根拠が記載された該当箇所がわかる情報（名称、文書番号、記載箇所（ページ番号、章番号、URL 等）） ● 「実機テスト」に基づく評価の場合： 評価結果の概要 ● 「対象外（NA）」である場合： 脅威に対して適切な対策が講じられている（なぜ対象外（NA）と判断しても問題がないのか／代替策で対応しているのか）と判断するための根拠を補足説明に従って記載

【★1 適合基準 S1.1-01】

適合要件

IoT 製品に対する IP 通信を介した守るべき情報資産への他の IoT 機器又はユーザからのアクセスに対して、適切な認証に基づくアクセス制御が行われていること。

なお、電気通信事業法に基づく端末機器セキュリティに係る技術基準を含めた技術基準適合認定を受けた IoT 製品（技適[T]マーク又は[A]マークが付与された IoT 製品）は、本適合基準に適合しているとみなす。（この場合、「基本情報」シートに「電気通信事業法に基づく技術基準適合認定番号等（技適[T]マークの設計認証番号又は[A]マークの技術基準適合認定番号）」を記入のこと。）

対象外（NA）となるための条件、基準の補足説明

【対象外（NA）となるための条件】

IP 通信を介した守るべき情報資産への認証及びアクセスの仕組みがない（「NA であることの理由」に、外部からの不正アクセスに対抗するために認証及びアクセスが必要ない根拠を記載すること）

【用語定義：守るべき情報資産】

以下のすべての情報：

- 通信機能に関する設定情報
- セキュリティ機能に関する設定情報
- IoT 機器の意図する使用において、IoT 機器が収集し、保存又は通信する、個人情報等の一般的に機密性が高い情報

★1 評価手法

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

★1 評価ガイド

1. 適合判断基準

本適合要件に対して、以下のドキュメント評価の評価結果が「適合（Y）」となった場合に限り、最終的に「適合（Y）」と判定される。

【ドキュメント評価】

IoT 製品の技術文書において、他の IoT 機器又はユーザからの守るべき情報資産へのアクセスに対する、適切な認証に基づくアクセス制御の方法が明示されていることを評価する。以下の評価項目 1 を満たすことが確認できる場合に限り、本適合要件のドキュメント評価の評価結果は「適合（Y）」となる。

評価項目 1：

IoT 製品の意図される使用上必要な IP 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、他の IoT 機器又はユーザからの守るべき情報資産へのアクセスに対して、以下の①と②の両方が満たされていることを確認する。

① 適切な認証に基づくアクセス制御が行われており、守るべき情報資産への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情報資産へのアクセスが許可されること。

② 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） 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、「★1 適合基準 S1.1-02」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） デジタル証明書を使用した認証機能の実装

D） OpenID Connect 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

E） 通信を許可する対象を IP アドレスなどで制限する機能の実装

F） 通信を許可する対象を LAN 内の機器のみに制限する機能の実装

＊ 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）

2. 補足説明

2.1. 適合判断基準の補足説明

2.1.1. ユーザの対象範囲

評価項目 1 の①におけるユーザの対象範囲には、IoT 機器の利用者、管理者、ベンダーのカスタマーエンジニア、所有者等、当該 IoT 機器内の守るべき情報資産へのアクセスができる当該 IoT 機器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。また、この対象に含まない者に対しては一切のアクセスを拒否しなければならない。

これらの条件が満たされない場合も、本適合要件は「非適合（N）」となる。

2.1.2. カスタマーエンジニアの認証

カスタマーエンジニアに対する認証についても本適合要件への適合を求める。

ただし、必ずしも一般利用者と同等の認証方法や利用環境における運用を求めることはしない。カスタマーエンジニアの利用環境において、利用ポートの制限、アクセス範囲の制限、カスタマーエンジニア機能の制限がされていること等を理由として、IoT 製品ベンダーがセキュリティ上適切と判断した場合、評価項目 1 の②とは異なるカスタマーエンジニア専用の認証方式を採用することが可能である。その際は、セキュリティ上適切と判断した根拠（利用制限などの条件等）と採用した認証方式の説明を技術文書に明記することによって、評価項目 1 の②の評価を除外することができる。その明記がない場合には、評価項目 1 の②も満たさなければならない。

2.1.3. 守るべき情報資産の対象範囲

守るべき情報資産の対象範囲は、2.4 節を参考に決定すること。また、評価項目 1 の①におけるアクセス制御がその範囲に対して適切に機能することが必要である。アクセス制御がその範囲に対して適切に機能することが確認できない場合は、本適合要件は「非適合（N）」としなければならない。

なお、個人情報等の一般に機密性が高い情報について、IoT 機器内のキャッシュやメモリ等に一時的に保存されるケースでは、必要な処理後又は一定時間経過後に自動消去されるような機能がデフォルトで有効になっていることを前提として、当該 IoT 機器を「保護されたネットワーク環境*) 内で利用する」旨の注意をユーザに明示することを条件として、当該情報を「守るべき情報資産」の対象から除外することができる。この場合、除外時した根拠を証跡（エビデンス）に明記しておかなければならない。

*) 保護されたネットワーク環境とは、インターネット側からの通信を遮断する機器（ゲートウェイやファイアウォール、VPN 装置等）によりインターネットからは隔離された通信環境のこと。

2.1.4. 技適マーク認定製品に対する試験結果の再利用

電気通信事業法に基づく端末機器セキュリティに関わる技術基準（端末設備規則第三十四条の十）の要件を満した技適マーク（[T]マーク又は[A]マーク）付与製品においては、本適合要件でのドキュメント評価を、技術適合認定を受けた際の試験結果によって代用することができる。この場合は、証跡（エビデンス）に基づく根拠として、「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）」を受けた際の試験結果を保管しておくこと。

2.2. 例外的なケースでの適合判断

2.2.1. IoT 機器のネットワーク接続制御による代替アクセス制御

★1 では、IoT 機器がネットワークに接続するたびに接続可否の確認を行う「ネットワークアクセス認証」に基づくアクセス制御が実施されている場合、当該 IoT 機器に「ユーザ認証」や「機器認証」によるアクセス制御機能がなくても、以下の条件①～⑤をすべて満たしている場合に限り、当該「ネットワークアクセス認証に基づくアクセス制御」をもって「適切な認証に基づくアクセス制御」が実行されているとみなす。

① VPN 装置やルータ等の別の機器によりインターネットから隔離された閉域ネットワーク内に接続することを前提とし、当該ネットワークに接続するたびに接続可否の確認が実施されること。

② 上記①での機器によって、当該 IoT 機器に対してインターネット側からつなげられる可能性を遮断できる（インターネットとは通信が許可されない）ように設定されていること。

③ 当該 IoT 機器を利用するユーザが何等かの手段により正規のユーザであることが担保されていること。例えば、正規のユーザでなければ立ち入ることができない場所に当該 IoT 機器が置かれている等。

④ ユーザが入手・確認しやすいマニュアル等に、「信頼できる利用者以外には使わせない」及び「インターネット側からの通信を遮断する機器に接続して利用する」旨の注意喚起がされていること。

⑤ 技術文書に、「ユーザ認証」や「機器認証」によるアクセス制御機能ではなく、「ネットワークアクセス認証」に基づくアクセス制御機能が用いられていること、及びその機能的な仕組みが明示されていること。

【★1 適合基準 S1.1-02】

適合要件

IoT 製品に対するネットワークを介したユーザ認証の仕組みにて、パスワードを使用する IoT 製品において、IoT 製品導入時にデフォルトパスワードが使用される場合に、以下の①・②のいずれかの基準を満たすこと。

① デフォルトパスワードは、IoT 機器毎に異なる一意の値で、容易に推測可能でない 6 文字以上のパスワードであること。

② デフォルトパスワードは、初回起動時にユーザによるパスワード変更を必須とする機能を実装し、当該機能において設定可能なパスワードとして、8 文字以上のパスワードの設定を強制させること。

対象外（NA）となるための条件、基準の補足説明

【対象外（NA）となるための条件】

ネットワークを介したパスワード利用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パスワード利用したユーザ認証が必要ない根拠を記載すること）

★1 評価手法

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

★1 評価ガイド

1. 適合判断基準

本適合要件に対して、以下のドキュメント評価の評価結果が「適合（Y）」となった場合に限り、最終的に「適合（Y）」と判定される。

【ドキュメント評価】

IoT 製品の技術文書において、ネットワークを介したユーザ認証の仕組みにて、パスワード利用した IoT 製品導入時にデフォルトパスワードに関する対策が明示されていることを評価する。デフォルトパスワードに関して、以下の評価項目 1、2 のいずれかを満たす実装がされていることを確認できる場合に限り、本適合要件のドキュメント評価の評価結果が「適合（Y）」となる。

評価項目 1：

デフォルトパスワードは、IoT 機器毎に異なる一意で、以下の A）～D）のいずれにも該当しない、6 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） 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

評価項目 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に利用可能な IoT 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もよい。

2. 補足説明

2.1. 適合判断基準の補足説明

2.1.1. 対象とするユーザ認証

本適合要件の対象とするユーザ認証は、自然人又は組織による認証であり、機器同士で連携するために行う機器間の認証（機器認証）は含まない。ただし、自然人の代わりとして、対象とする IoT 機器へのアクセスを代行させるために使用する機器等による知識情報に基づいた認証は、ユーザ認証に含める（機器認証とはみなさない）。

2.2. 例外的なケースでの適合判断

2.2.1. 管理者及びカスタマーエンジニアの認証におけるパスワードの扱い

管理者及び IoT 製品ベンダーのカスタマーエンジニアがメンテナンス時に利用するためのパスワードを使用した認証についても、本適合要件の評価対象である。

ただし、ネットワークを介さずに、IoT 機器に備え付けられたメンテナンス用インタフェースやメンテナンスポートを管理者やカスタマーエンジニアが直接操作してパスワードを使用して行うユーザ認証に限り、当該ユーザ認証で利用するパスワードに関しては本適合要件の対象外にできる。その場合、対象外とした根拠を技術文書に明記しておかなければならない。

2.2.2. 設置時に自動的にネットワーク接続する機能を有する IoT 機器に対する適合判断

設置時に自動的にネットワーク接続する機能を有する IoT 機器については、以下の①～③の条件をすべて満たす場合に限り、例外的に、ネットワークを介したユーザ認証の仕組みがない機器として「対象外（NA）」とすることができる。この場合、「対象外（NA）」と判断した根拠を証跡（エビデンス）に明記しておかなければならない。

① 設置時にインターネット経由のユーザ認証を行うユーザアカウントが無い
② インターネットを経由しない、ローカルアクセスしかできないユーザ認証を行うアカウントにて、デフォルトパスワードが設定されている
③ 当該 IoT 機器を「保護されたネットワーク環境*) 内で利用する」旨の注意が明示されている

*）保護されたネットワーク環境とは、インターネット側からの通信を遮断する機器（ゲートウェイやファイアウォール、VPN 装置等）によりインターネットからは隔離された通信環境のこと。

【★1 適合基準 S1.1-03】

適合要件

IoT 製品に対するネットワークを介したユーザ認証において使用される認証値の変更について、認証の種類（パスワード、トークン、指紋等）に依らず、その認証値の変更を可能とすること。

対象外（NA）となるための条件、基準の補足説明

【対象外（NA）となるための条件】

ネットワークを介したユーザ認証の仕組みがない（「NA であることの理由」に、外部からの不正アクセスに対抗するためにユーザ認証が必要ない根拠を記載すること）

【用語定義：認証値】

IoT 製品に対する認証の仕組みで使用される属性の個別値。（例： パスワードに基づく認証の仕組みである場合、認証値は文字列となる。生体指紋認証である場合、認証値は例えば左手の人差し指の指紋データとなる。）

★1 評価手法

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

★1 評価ガイド

1. 適合判断基準

本適合要件に対して、以下のドキュメント評価の評価結果が「適合（Y）」となった場合に限り、最終的に「適合（Y）」と判定される。

【ドキュメント評価】

IoT 製品の技術文書において、IoT 製品に対するユーザ認証にて使用される認証値の変更に関する記載があることを評価する。以下の評価項目 1 と 2 の両方が満たすことが確認できる場合に限り、本適合要件のドキュメント評価の評価結果が「適合（Y）」となる。

評価項目 1：

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ことが明示されていること。

評価項目 2：

上記機能の利用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。

2. 補足説明

2.1. 適合判断基準の補足説明

2.1.1. ユーザの対象範囲

本適合要件におけるユーザの対象範囲は、ネットワークを介したユーザ認証を行うすべてのものに対してである。IoT 機器の利用者、管理者、ベンダーのカスタマーエンジニア、所有者等、当該 IoT 機器でネットワークを介したユーザ認証を行う自然人又は組織、自然人の代わりとして IoT 機器にアクセスする機器等のすべてを含んでいなければならない（機器同士で連携するために接続する別の機器はユーザに含まない。すなわち、機器認証は対象外である。）。この条件が満たされない場合は、本適合要件は「非適合（N）」となる。

2.2.2. カスタマーエンジニア等、特定ユーザに対する認証値の変更手順の提供

評価項目 2 において、認証値の変更をするための利用手順を提供する先の「ユーザ」について、該当する人を限定することは問題ない。また、「ユーザ」の違いによって提供する内容が異なってもよい。重要なことは、ユーザが自ら利用するユーザ認証に関する認証値の変更が可能であり、その変更手順が提供されていることであり、他の人が利用するユーザ認証に関する認証値の変更手順の提供まで求めるものではない。

例えば、カスタマーエンジニアが利用するユーザ認証に関しては「ユーザ＝カスタマーエンジニア（一般利用者は含まない）」と解釈してよい。この場合には、カスタマーエンジニアに対するマニュアル等に認証値の変更手順が記載されていればよく、一般利用者向けのマニュアル等に記載する必要はない。システム管理者が利用するユーザ認証等についても同様である。

2.2. 例外的なケースでの適合判断

該当事項なし

【★1 適合基準 S1.1-04】

適合要件

IoT 機器が、制約のある機器ではない場合、IoT 機器に対するネットワークを介したユーザ認証の仕組みについて、総当たり攻撃を困難とすること。

対象外（NA）となるための条件、基準の補足説明

【対象外（NA）となるための条件】

以下のいずれかの条件に該当する。（OR 条件）

- IoT 機器に対するネットワークを介したユーザ認証の仕組みがない（「NA であることの理由」に、外部からの不正アクセスに対抗するためにユーザ認証が必要ない根拠を記載すること）
- IoT 機器が「制約のある機器」に該当する（「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。

★1 評価手法

- ドキュメント評価：なし
- 実機テスト：対象とする
  実機テストによって、IoT 機器に対するネットワークを介したユーザ認証の仕組みについて、総当たり攻撃を困難とする仕組みであることを評価する。

★1 評価ガイド

1. 適合判断基準

本適合要件に対して、以下の実機テストの評価結果が「適合（Y）」となった場合に限り、最終的に「適合（Y）」と判定される。

【実機テスト】

対象 IoT 機器に対する実機テストによって、当該 IoT 機器に対するネットワークを介したユーザ認証の仕組みについて、総当たり攻撃を困難とする仕組みであることを評価する。以下の評価項目１、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いることが確認できる場合に限り、本適合要件の実機テストの評価結果は「適合（Y）」となる。

評価項目 1：

ネットワークを介したユーザ認証について、認証試行の「一定回数※」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

※ 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。

評価項目 2：

多要素認証が使用されていること。

2. 補足説明

2.1. 適合判断基準の補足説明

2.1.1. 認証試行失敗時の認証試行制限について

評価項目 1 において、ユーザ認証の一定回数連続失敗時に認証試行の制限が求められる対象は、認証に失敗したアカウントに対してのものであり、必ずしも IoT 機器本体としての認証試行制限まで求めるものではない。実機テストにより、認証に失敗したアカウントに対して認証試行の制限がなされていることが確認できれば、評価項目 1 を満たしていると判断してよい。

2.2. 例外的なケースでの適合判断

該当事項なし

【★1 適合基準 S1.1-05】

適合要件

製造業者は、以下の①～③のすべての情報を含む脆弱性開示ポリシーを公開（例：製造業者のウェブサイトへの掲載）すること。

① IoT 製品のセキュリティの問題に関して、製造業者へ報告するための連絡先（例：製造業者等のウェブサイトの URL、電話番号、メールアドレス）

② 製造業者が IoT 製品のセキュリティに関する報告を受領した後に行う手続き及びその概要

③ 脆弱性が解決されるまでの IoT 製品や脆弱性の状況更新に関する手続き及びその概要

対象外（NA）となるための条件、基準の補足説明

【対象外（NA）となるための条件】

該当事項なし

★1 評価手法

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

★1 評価ガイド

1. 適合判断基準

本適合要件に対して、以下のドキュメント評価の評価結果が「適合（Y）」となった場合に限り、最終的に「適合（Y）」と判定される。

【ドキュメント評価】

IoT 製品のウェブサイト等、ユーザがアクセス可能な媒体において、脆弱性開示ポリシーが明示されていることを評価する。以下の評価項目１～４のすべてが満たすことが確認できる場合に限り、本適合要件のドキュメント評価の評価結果が「適合（Y）」となる。

評価項目１：

脆弱性開示ポリシーに、IoT 製品のセキュリティの問題に関して、製造業者へ報告するための連絡先（例：製造業者のウェブサイトの URL、電話番号、メールアドレス）が記載されていること。

評価項目２：

脆弱性開示ポリシーに、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（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、その後にどのような手続き・方法で報告者と連絡を取り合うのか、報告に対してどのような対応をするのか、善意の報告に対する法的免責付与の宣言等といった、概要を公開することが求められる）が記載されていること。

評価項目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等の概要を公開することが求められる）が記載されていること。

評価項目 4：

脆弱性開示ポリシーが、ユーザがアクセス可能な媒体に掲載されていることを確認する。ユーザがアクセス可能な媒体に掲載されている根拠として、チェックリストには脆弱性開示ポリシーが掲載されている場所を記載すること。

ただし、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に限り、公開する予定の脆弱性開示ポリシー、及び公開見込みが分かる情報（例：公開予定の URL や掲載場所等）を明記した文書を証跡（エビデンス）として用意し、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、本評価項目は確認されたものとする。

以下の記載があること。

A） 公開予定日（IoT 製品販売日以前に限る）

B） 公開方法・公開場所

C） 公開する予定の脆弱性開示ポリシー（別添でも構わない）

2. 補足説明

2.1. 適合判断基準の補足説明

該当事項なし

2.2. 例外的なケースでの適合判断

該当事項なし

【★1 適合基準 S1.1-06】

適合要件

IoT 製品に含まれるソフトウェアコンポーネントのアップデート機能について、以下の①～③のすべての基準を満たすこと。

① IoT 製品のファームウェア（ソフトウェア）パッケージについて、アップデートが可能であること。

② ファームウェア（ソフトウェア）パッケージのバージョンの確認が行えるなど、最新のファームウェア（ソフトウェア）がインストールされていることを確認する手段を有すること。

③ アップデートされたファームウェア（ソフトウェア）パッケージのバージョンが電源 OFF 後も維持されること。

なお、電気通信事業法に基づく端末機器セキュリティに係る技術基準を含めた技術基準適合認定を受けたIoT製品（技適[T]マーク又は[A]マークが付与されたIoT製品）は、本適合基準に適合しているとみなす。（この場合、「基本情報」シートに「電気通信事業法に基づく技術基準適合認定番号等（技適[T]マークの設計認証番号又は[A]マークの技術基準適合認定番号）」を記入のこと。

対象外（NA）となるための条件、基準の補足説明

【対象外（NA）となるための条件】

該当事項なし

★1 評価手法

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

★1 評価ガイド

1. 適合判断基準

本適合要件に対して、以下の実機テストの評価結果が「適合（Y）」となった場合に限り、最終的に「適合（Y）」と判定される。

【実機テスト】

対象IoT製品に含まれるソフトウェアコンポーネントに対するアップデート機能を実機テストにより評価する。以下の評価項目1～3のすべてを満たすことが確認できる場合に限り、本適合要件の実機テストの評価結果が「適合（Y）」となる。

評価項目1：

IoT 製品のファームウェア（ソフトウェア）パッケージについてアップデートの操作を行い、正常にアップデートが完了できること。

評価項目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。

評価項目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。

2. 補足説明

2.1. 適合判断基準の補足説明

2.1.1. 評価項目 1 で確認するアップデートの方法

アップデートの方法について、①自動的に開始される方法、②ユーザが手動で実施する方法、③明示的に管理責任を有する、カスタマーエンジニア等の保守担当者や特権ユーザのみが実施する方法がある。評価項目 1 では、当該 IoT 機器に実装されているアップデート方法のすべてを対象として適合判断を実施しなければならない。

2.1.2. 評価項目 2 における最新ファームウェア（ソフトウェア）バージョンの確認方法

最新のファームウェア（ソフトウェア）にアップデートされていることの確認方法としては、以下のようなやり方がある。必ずしも「ファームウェア（ソフトウェア）のバージョン」表示を IoT 機器に求めているわけではない。

例 1： IoT 機器のディスプレィにファームウェア（ソフトウェア）のバージョン情報やインストール状況を表示し、当該 IoT 機器にインストールされているファームウェア（ソフトウェア）が最新であることが確認できる

例 2： PC やスマートフォンを接続し、PC やスマートフォン上にファームウェア（ソフトウェア）のバージョン情報やインストール状況を表示し、当該 IoT 機器にインストールされているファームウェア（ソフトウェア）が最新であることが確認できる

例 3： IoT 機器に搭載されている LED 等の点灯・点滅により、バージョン情報は表示されないものの、当該 IoT 機器に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か否かを確認できる

例 4： 自社のホームページでファームウェア（ソフトウェア）のバージョン確認ツールを提供し、当該確認ツールを利用して当該 IoT 機器に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か否かを確認できる

2.1.3. アップデートが必要なソフトウェアコンポーネントの対象範囲

本適合要件において、アップデートが必要なソフトウェアコンポーネントとは、セキュリティ対策の実施が必要なソフトウェアコンポーネントのことであり、IoT 製品ベンダーにて対象が選定される。そのようなソフトウェアコンポーネントには、具体的には、セキュリティ機能を有しており、セキュリティ上の不具合や脆弱性等が発見されたときには、セキュリティ機能を維持するためにセキュリティパッチを提供することが必要となるファームウェア（ソフトウェア）が含まれる。

最低限、申請書に記載したファームウェア（ソフトウェア）については必ずアップデートできる対象としておかなければならない。

2.1.4. 技適マーク認定製品に対する試験結果の再利用

電気通信事業法に基づく端末機器セキュリティに関わる技術基準（端末設備規則第三十四条の十）の要件を満した技適マーク（[T]マーク又は[A]マーク）付与製品においては、本適合要件での実機テストによる評価を、技術適合認定を受けた際の試験結果によって代用することができる。この場合は、証跡（エビデンス）に基づく根拠として、「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）」を受けた際の試験結果を保管しておくこと。

2.2. 例外的なケースでの適合判断

2.2.1. アップデート機能を利用しない代替アップデート

IoT 機器の中には、何らかの制約やビジネス的事由等により、IoT 製品に含まれるソフトウェアコンポーネントに対するアップデート機能そのものを有しないことがありうる。しかし、そのような IoT 機器であっても、セキュリティ上の不具合や脆弱性等が発見されたときには、セキュリティ機能を維持するために何らかの対策（代替アップデート）を実施しなければならない。

そのため、セキュリティ対策の実施が必要なソフトウェアコンポーネントにもかかわらずアップデートができない場合には、実機テストの代替として、アップデートできない理由及び脆弱性発覚時のアップデートに代わる適切な代替手段を文書化し、証跡（エビデンス）として残すことにより本適合要件を「適合（Y）」とすることができる。なお、脆弱性を修正するための適切な代替手段が用意できない場合には、本適合要件は「非適合（N）」となる。

アップデート機能を利用しない代替アップデートが必要となる例

- 例 1： 製造時に一度だけ書き込まれ以降更新ができないブートローダーのようなソフトウェアを利用している
- 例 2： IoT 機器に複数のマイクロコントローラーが組み込まれておりその一部のソフトウェアの書き換え不可となっている
- 例 3： 法令・規制等により、ソフトウェアアップデートが禁止又は制約されている
- 例 4： IoT 機器の物理的リソース上の制約により、当該 IoT 機器にアップデート機能を入れることができない
- 例 5： ビジネス上の理由により、IoT 機器にアップデート機能を組み入れる代わりに、脆弱性対応した代替機器への交換等の代替アップデートを実施する

【★1 適合基準 S1.1-07】

適合要件

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とすること。

対象外（NA）となるための条件、基準の補足説明

【対象外（NA）となるための条件】

該当事項なし

★1 評価手法

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

★1 評価ガイド

1. 適合判断基準

本適合要件に対して、以下のドキュメント評価の評価結果が「適合（Y）」となった場合に限り、最終的に「適合（Y）」と判定される。

【ドキュメント評価】

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

以下の評価項目１～４のいずれかに類するアップデート方法（複数のアップデート方法を採用することは許容される。）の手順が明示されていることが確認できる場合に限り、本適合要件のドキュメント評価の評価結果は「適合（Y）」となる。

評価項目１：

自動的にアップデートが実行されることが明示されていること。また、自動アップデートに失敗した場合の対応方法が明示されていること。

評価項目２：

ユーザが、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明示されていること。

評価項目３：

ユーザが、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明示されていること。

評価項目４：

ユーザが、IoT 製品ベンダー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、インストールによるアップデートを実行する手順が明示されていること。

2. 補足説明

2.1. 適合判断基準の補足説明

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. カスタマーエンジニアによるアップデート

カスタマーエンジニアによるソフトウェアアップデートについても、本適合要件の対象である。

ただし、その場合のアップデート手順の開示範囲は IoT 製品ベンダーとカスタマーエンジニア間とし、カスタマーエンジニアがアクセス可能な媒体にアップデート手順が明示されていればよく、一般利用者への開示までは必要ない。また、容易かつ分かりやすい手順についても、カスタマーエンジニアが問題なくアップデート作業ができる手順であれば問題ない。

この前提を踏まえて、カスタマーエンジニアによるソフトウェアアップデートに関する評価を実施すること。

2.2. 例外的なケースでの適合判断

該当事項なし

【★1 適合基準 S1.1-08】

適合要件

ソフトウェアをネットワーク経由でアップデートする際、ソフトウェアの完全性をアップデート前に確認できる仕組みを有すること。

対象外（NA）となるための条件、基準の補足説明

【対象外（NA）となるための条件】

ソフトウェアをネットワーク経由でアップデートする仕組みが存在しない（「NA であることの理由」に、想定するアップデートの仕組みを記載すること）

★1 評価手法

- ドキュメント評価：対象とする
  IoT 製品の技術文書において、ソフトウェアの完全性をアップデート前に確認できる仕組みの実装が明示されていることを評価する。
- 実機テスト：なし

★1 評価ガイド

1. 適合判断基準

本適合要件に対して、以下のドキュメント評価の評価結果が「適合（Y）」となった場合に限り、最終的に「適合（Y）」と判定される。

【ドキュメント評価】

IoT 製品の技術文書において、ソフトウェアの完全性をアップデート前に確認できる仕組みの実装が明示されていることを評価する。以下の評価項目 1 ～ 4 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であって、かつ評価項目 5 を満たすことが確認できる場合に限り、本適合要件のドキュメント評価の評価結果は「適合（Y）」となる。

評価項目 1 ：

アップデートソフトウェアをインストールする前又はインストール中に、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が中止されることが、明示されていること。

評価項目 2 ：

アップデートソフトウェアをインストールする前又はインストール中に、更新ソフトウェア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インストールが中止されることが、明示されていること。

評価項目 3 ：

アップデートソフトウェアをインストールする前に、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が中止されることが、明示されていること。

評価項目４：

アップデートソフトウェアをインストールする前に、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インストールが中止されることが、明示されていること。

評価項目５：

評価項目 1～4 で利用するハッシュ関数やデジタル署名について、「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」に記載されたアルゴリズムを利用していること。

2. 補足説明

2.1. 適合判断基準の補足説明

該当事項なし

2.2. 例外的なケースでの適合判断

該当事項なし

【★1 適合基準 S1.1-09】

適合要件

製造業者は、セキュリティ課題に対する迅速なアップデートを目的として、セキュリティアップデートの優先度を決定するための方針や指針を文書化すること。

対象外（NA）となるための条件、基準の補足説明

【対象外（NA）となるための条件】

該当事項なし

★1 評価手法

- ドキュメント評価：対象とする
  組織の規程類、方針、手順書等又は IoT 製品の技術文書において、セキュリティアップデートの優先度を決定するための方針や指針が明示されていることを評価する。
- 実機テスト：なし

★1 評価ガイド

1. 適合判断基準

本適合要件に対して、以下のドキュメント評価の評価結果が「適合（Y）」となった場合に限り、最終的に「適合（Y）」と判定される。

【ドキュメント評価】

組織の規程類、方針、手順書等又はIoT製品の技術文書において、セキュリティアップデートの優先度を決定するための方針や指針が明示されていることを評価する。以下の評価項目１～３のすべてを満たすことが確認できる場合に限り、本適合要件のドキュメント評価の評価結果は「適合（Y）」となる。

評価項目１：

セキュリティアップデートの優先度を決定するための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）等の指針が記載されていること。

評価項目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記載されていること。

評価項目３：

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）が記載されていること。

2. 補足説明

2.1. 適合判断基準の補足説明

2.1.1. 評価項目1で求められる内容

対応する脆弱性の影響度、深刻度、既に攻撃に利用されているか、対応の難易度等によってセキュリティアップデートを提供する適時性が変わってくる。このことから、評価項目1においては、例えば「緊急アップデート」で対応するのか「計画アップデート」で対応するのかを判断するために、「何を基準」に「どういったこと」が起きたら「何をするのか」の判断フロー・方針が文書化されていることが求められる。

2.2. 例外的なケースでの適合判断

該当事項なし

【★1 適合基準 S1.1-10】

適合要件

IoT 製品の型番は、以下のいずれかの方法でユーザへ提供すること。

① IoT 製品本体に、IoT 製品の型番を直接記載すること。

② IoT 製品の GUI、ウェブ UI 等や、IoT 製品に付帯するソフトウェア、アプリケーション（スマホアプリなど）の GUI、ウェブ UI 等から、ユーザが型番を認識できるようにすること。

対象外（NA）となるための条件、基準の補足説明

【対象外（NA）となるための条件】

該当事項なし

★1 評価手法

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

★1 評価ガイド

1. 適合判断基準

本適合要件に対して、以下の実機テストの評価結果が「適合（Y）」となった場合に限り、最終的に「適合（Y）」と判定される。

【実機テスト】

IoT 製品の型番についてユーザ確認できる方法が、ユーザに提供されていることを評価する。以下の評価項目 1 、 2 のいずれかを満たすことが確認できる場合に限り、本適合要件の実機テストの評価結果が「適合（Y）」となる。

評価項目 1 ：

IoT 製品本体を確認し、IoT 製品の型番が記載されていることを確認できること。

評価項目 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 等に実際にアクセスすることで、当該 IoT 製品の型番を確認できること。

2. 補足説明

2.1. 適合判断基準の補足説明

該当事項なし

2.2. 例外的なケースでの適合判断

該当事項なし

【★1 適合基準 S1.1-11】

適合要件

IoT 製品のストレージに保存される守るべき情報資産（SD カード等、ストレージメディアに保存される守るべき情報資産も含む。）は、セキュアに保存されること。

対象外（NA）となるための条件、基準の補足説明

【対象外（NA）となるための条件】

該当事項なし。

【用語定義：守るべき情報資産】

以下のすべての情報：

- 通信機能に関する設定情報
- セキュリティ機能に関する設定情報
- IoT 機器の意図する使用において、IoT 機器が収集し、保存又は通信する、個人情報等の一般的に機密性が高い情報

★1 評価手法

- ドキュメント評価：対象とする
  IoT 製品の技術文書を閲覧することで、IoT 製品のストレージに保存される守るべき情報資産（SD カード等、ストレージメディアに保存される守るべき情報資産も含む。）が、セキュアに保存されることを評価する。
- 実機テスト：なし

★1 評価ガイド

1. 適合判断基準

本適合要件に対して、以下のドキュメント評価の評価結果が「適合（Y）」となった場合に限り、最終的に「適合（Y）」と判定される。

【ドキュメント評価】

IoT 製品の技術文書において、IoT 製品のストレージに保存される守るべき情報資産（ストレージメディアに保存される場合を含む）が、セキュアに保存されていることを評価する。以下の評価項目１～５のいずれかに類する保護対策又はそれ以上の対策（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。）が明示されていることが確認できる場合に限り、本適合要件のドキュメント評価の評価結果は「適合（Y）」となる。

評価項目１：

機密性の保護が必要な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こと。

評価項目２：

完全性の保護が必要な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。

評価項目３：

完全性の保護が必要な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を用いたメッセージダイジェスト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。

評価項目４：

守るべき情報資産は、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。

評価項目５：

守るべき情報資産は、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。

2. 補足説明

2.1. 適合判断基準の補足説明

2.1.1. 守るべき情報資産の対象

本適合要件のセキュア保存が求められる守るべき情報資産の対象は、2.4 節の守るべき（保護すべき）情報資産の考え方を参考に、IoT 製品ベンダーが「守るべき情報資産である」と判

断した情報資産すべてである。対象とした情報資産すべてが、評価項目１～５のいずれかに示した方法で保存されることが求められる（情報資産ごとに異なる方法を採用してもよい。また、複数の方法を併用してもよい。）。

なお、IoT 機器での処理の都合上、一時的にキャッシュやメモリ等に保存する情報資産については、以下に示すようなセキュリティ対策を実施することを条件として、守るべき情報資産の対象外とすることができる。その場合、守るべき情報資産の対象外とする根拠として、実施するセキュリティ対策について技術文書等に明記しなければならない。この明記がない場合には、守るべき情報資産の対象外とすることはできない。

例１： インターネットから隔離され、保護されたネットワーク環境内での利用
例２： 守るべき情報資産への適切なアクセス制御の実施
例３： 処理終了後又は合理的期間経過後の自動消去

2.1.2. 評価項目 5 における 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

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とは、例えば基盤に直接実装された不揮発性メモリ（フラッシュ ROM 等）等のストレージ領域のことである。HDD や SSD 等、筐体内に格納されていても、取り外し可能なものは含まない。

2.1.3. 評価項目 5 における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

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とは、外部から呼び出すインタフェースを持たないソフトウェアコンポーネント（ブートモニタ、BIOS 等）からのみ読み書きができるストレージ領域であって、他のソフトウェアコンポーネントは直接・間接を問わず読み書きできない領域のことである。

2.2. 例外的なケースでの適合判断

該当事項なし

【★1 適合基準 S1.1-12】

適合要件

ネットワーク経由で伝送される守るべき情報資産について、情報の盗聴に対する以下のいずれかの保護対策が行われていること。

① 他の IoT 機器やサーバ（クラウド上のサーバを含む）へネットワークを介して伝送される守るべき情報資産について、情報の盗聴に対する保護対策を IoT 機器自らが行う。

② 他の IoT 機器やサーバ（クラウド上のサーバを含む）へネットワークを介して伝送される守るべき情報資産について、保護された通信環境（VPN 環境や専用線を経由した接続環境）においてのみ伝送される。

対象外（NA）となるための条件、基準の補足説明

【対象外（NA）となるための条件】

ネットワーク経由で伝送される守るべき情報資産が存在しない（「NA であることの理由」に、ネットワーク経由で伝送される守るべき情報資産が存在しないことを示す根拠を記載すること）

【用語定義：守るべき情報資産】

以下のすべての情報：

- 通信機能に関する設定情報
- セキュリティ機能に関する設定情報
- IoT 機器の意図する使用において、IoT 機器が収集し、保存又は通信する、個人情報等の一般的に機密性が高い情報

★1 評価手法

- ドキュメント評価：対象とする
  IoT 製品の技術文書において、ネットワーク経由で伝送される守るべき情報資産について、情報の盗聴に対する保護対策が実装されていることを評価する。IoT 製品と連動するアプリがある場合、守るべき情報資産として、アプリから送信される情報も対象とした評価を行う。
- 実機テスト：なし

★1 評価ガイド

1. 適合判断基準

本適合要件に対して、以下のドキュメント評価の評価結果が「適合（Y）」となった場合に限り、最終的に「適合（Y）」と判定される。

【ドキュメント評価】

IoT 製品の技術文書において、ネットワーク経由で伝送される守るべき情報資産について、情報の盗聴に対する保護対策が実装されていることを評価する。IoT 製品と連動するアプリがある場合、守るべき情報資産として、アプリから送信される情報も対象とした評価を行う。

以下の評価項目１と２の両方を満たしていることが確認できるか、もしくは評価項目３を満たしていることが確認できる場合に限り、本適合要件のドキュメント評価の評価結果は「適合（Y）」となる。

評価項目１：

技術文書に、以下の A）、B）のいずれかが明示されていること。

A） 「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。

B） 「★1 適合基準 S1.1-11」の評価項目 1 に準拠した暗号化をされたうえで保存された守るべき情報資産を復号せずにネットワークを経由して伝送することが明示されていること。

評価項目２：

技術文書に、情報の盗聴に対する保護対策の「初期設定が有効」に設定されていることが明示されていること。

評価項目３：

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、保護された通信環境（VPN 環境、専用線を経由した接続環境、物理的／論理的に保護されたネットワーク環境）においてのみ IoT 製品を利用するよう、ユーザ向けに明示されていること。

2. 補足説明

2.1. 適合判断基準の補足説明

2.1.1. インターネットを介する IoT 機器と必須付随サービスとの間の通信について

IoT 機器と必須付随サービスとの間の通信がインターネットを経由して行われる場合、又はインターネットから接続可能な通信経路を介して行われる場合、IoT 機器と必須付随サービスとの間で通信される守るべき情報資産も本適合要件での「ネットワーク経由で伝送される守るべき情報資産」に該当する。したがって、そのような利用環境での IoT 機器と必須付随サービスとの間の通信についても盗聴に対する保護対策をしなければならない。

一方、★1 では、インターネットを介さない IoT 機器と必須付随サービスとの間の通信については保護対策を必須とはしない。

2.2. 例外的なケースでの適合判断

2.2.1. インターネットとは通信ができない環境下において利用する場合の取扱い

2.6 節のセキュアな通信が求められる（or 除外可能な）範囲の考え方で示しているように、★1 では、VPN 装置やルータ等によりインターネットから隔離された閉域ネットワーク内に置かれ、かつその機器によってインターネット側からつなげられる可能性を遮断できる（インターネットとは通信が許可されない）IoT 機器に対しては、通信が暗号化されてい

なくてもインターネットからの不正なアクセスに対して必要な保護対策が取られていると判断される。したがって、本適合要件での情報の盗聴に対する保護対策として、通信の暗号化の代わりに、「インターネット側からの通信を遮断する機器に接続して利用する」旨の注意をユーザに明示することを条件に、評価項目 2 を満たしているとみなす。

2.2.2. 評価項目 2 の初期設定時の考え方

IoT 製品出荷時点の初期設定で「盗聴に対する保護対策が有効」にされていなければならない。ただし、以下の条件 A）と B）の両方を満たす場合に限り、その手続きを文書化して証跡（エビデンス）として残すことにより、例外的に「IoT 製品出荷時点では保護対策が無効」であっても、IoT 機器の工事設置時での初期設定の変更により「盗聴に対する保護対策が有効」であるとみなす。

A）工事設置業者による IoT 装置の設置が前提となっている（工事設置業者又はシステム管理者以外が設置しないことがマニュアル等に文書化されている）

B）設置時に当該 IoT 機器の設定で「盗聴に対する保護対策を有効化」するように指示する項目を、設置作業指示書やマニュアル等に注意・警告表示されている

これは、IoT 機器の工事設置時に保護対策を有効化する運用を行う場合、設置作業実施者を「工事設置業者又はシステム管理者」に限定し、さらに設置作業の一環として「盗聴に対する保護対策を有効化」する手順とすることにより、「盗聴に対する保護対策を有効化の設定もれ」のリスクを最小化することを意図している。一方、設置作業実施者が「工事設置業者又はシステム管理者」に限定できないのであれば、「盗聴に対する保護対策を有効化」するように設置作業指示書やマニュアル等に注意・警告表示されていてもその通りに実施されるかどうかは分からず、「有効化の設定もれ」のリスクが相当程度あると考えられるため、条件 A)を満たさない場合には「IoT 製品出荷時点では保護対策が有効」としなければならない。

【★1 適合基準 S1.1-13】

適合要件

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すること。具体的には、以下の①・②のすべての基準を満たすこと。

① IoT 製品において、高頻度で利用され、脆弱性などのリスクが想定される以下のインタフェースについて、IoT 製品の利用上不要かつ攻撃を受けるリスクがあるインタフェースを無効化すること。

A）TCP/UDP ポート
B）Bluetooth
C）USB

② IoT 製品に対して脆弱性スキャンツールによる既知の脆弱性検査を実施し、攻撃に悪用される可能性がある脆弱性が検出されないこと。

対象外（NA）となるための条件、基準の補足説明

【対象外（NA）となるための条件】

該当事項なし

★1 評価手法

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

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

★1 評価ガイド

1. 適合判断基準

本適合要件に対して、以下のドキュメント評価及び実機テストの両方の評価結果が「適合（Y）」となった場合に限り、最終的に「適合（Y）」と判定される。

【ドキュメント評価】

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

技術文書に明示されていることを評価する。以下の評価項目１～３のすべてを満たしていることが確認できる場合に限り、本適合要件のドキュメント評価の評価結果は「適合（Y）」となる。

評価項目１：

技術文書に IoT 製品対象のインタフェースに関する記載があること。

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、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明示されていること（IPv6 に対応した製品の場合、IPv4 と IPv6 の両方を対象とする。）、及びそ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、利用上不要なポートが含まれていないこと。

B） Bluetooth プロファイル

IoT 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こと、及びそ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 クラス

IoT 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ていること、及びそ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。

評価項目２：

IoT 製品が物理的に無効化しているインタフェースがあれば、無効にしているインタフェース及び無効化の方法が技術文書に明示されていること。そのようなインタフェースがなければ、「物理的に無効化しているインタフェースはない。」と明示されていること。

評価項目３：

技術文書において、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の記載があること。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。」と明示されていること。

【実機テスト】

A）TCP/UDP ポート、B）Bluetooth、C）USB を対象インタフェースとして、ポートスキャン及び脆弱性スキャンツールを利用した実機テストにより、IoT 製品の利用上不要なインタフェースが無効化されていること、及び攻撃に悪用される可能性がある脆弱性が検出されないことを評価する。以下の評価項目４と５の両方を満たしている（「合格」となる）ことが確認できる場合に限り、本適合要件の実機テストの評価結果は「適合（Y）」となる。

評価項目４：

TCP・UDP ポートに関して、IoT 製品の利用上不要なインタフェースが無効化されていることをポートスキャンにて確認する。特に、評価項目 1 で開放していると明記されている TCP・UDP ポート以外のポートがすべて無効化されていることを確認する。もし評価項目 1 で開放していると明記されていない TCP・UDP ポートで無効化されていないものが検知されなければ本評価項目は「合格」、一つでも検知されれば本評価項目は「不合格」となる。

評価項目 5 ：

以下の i）、ii）の両方について脆弱性検査ツールにて脆弱性がないことを確認する。なお、推奨される脆弱性検査ツールがない場合（現時点では Bluetooth と USB）には、iii）により脆弱性確認テストの代替として実施する。

脆弱性がないことが確認できれば本評価項目は「合格」、確認できなければ「不合格」となる。ただし、i）、ii）のいずれかにおいて脆弱性が検出された場合には、追加で評価項目 6 の分析及び評価を行い、検出されたすべての脆弱性について「脆弱性の問題がない」と確認できた場合は、本評価項目は「合格」となることに留意されたい。

i） 開放されている TCP・UDP 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を確認する。

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ないことを確認する。

[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」のすべてを対象とする

iii） 推奨の脆弱性検査ツールが無い場合は、以下の確認を実施する。

- Bluetooth の場合：
  評価項目 1 で利用する Bluetooth のプロファイルと明記されたもの以外の Bluetooth のプロファイルが利用できない状態又はデフォルト無効化の設定がされていること、及び廃止された Bluetooth のプロファイルが利用できないこと
- USB の場合：
  評価項目 1 で利用する USB デバイスクラスと明記されたもの以外のデバイスクラスが利用できない状態又はデフォルト無効化の設定がされていること

評価項目６：

評価項目 5 の i）、ii）のいずれかにおい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。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
- 運用対策を含む対策により、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. 適合判断基準の補足説明

2.1.1. インタフェース無効化の手段例

インタフェースを無効化する手段としては、「物理的に無効化」する手段と「論理的に無効化」する手段がある。

物理的手法による無効化とは、以下のような、攻撃者が容易に物理ポートにアクセスできない対策がされていることをいう。

例 1： インタフェースは筐体の中にあり、筐体はねじ止め等により容易に開けられないようになっている

例 2： 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

論理的手法による無効化とは、以下のような、攻撃者が不正にソフトウェアの構成を変更しない限り（すなわち、新たなソフトウェアをインストールしたり、設定を変更したりしない限り）、論理ポートにアクセスできないような対策がされていることをいう。

例 3： ドライバーをインストールしない

例 4： 不要な TCP/UDP ポートを無効化する

例 5： 不要な Bluetooth プロファイルをインストールしない

例 6： 不要な USB クラスをインストールしない

2.2. 例外的なケースでの適合判断

該当事項なし

【★1 適合基準 S1.1-14】

適合要件

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ること。

なお、電気通信事業法に基づく端末機器セキュリティに係る技術基準を含めた技術基準適合認定を受けた IoT 製品（技適[T]マーク又は[A]マークが付与された IoT 製品）は、本適合基準に適合しているとみなす。（この場合、「基本情報」シートに「電気通信事業法に基づく技術基準適合認定番号等（技適[T]マークの設計認証番号又は[A]マークの技術基準適合認定番号）」を記入のこと。）

対象外（NA）となるための条件、基準の補足説明

【対象外（NA）となるための条件】

該当事項なし

★1 評価手法

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

★1 評価ガイド

1. 適合判断基準

本適合要件に対して、以下の実機テストの評価結果が「適合（Y）」となった場合に限り、最終的に「適合（Y）」と判定される。

【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 IoT 製品に対して、実機テストにより評価する。以下の評価項目 1 と 2 の両方を満たしていることが確認できる場合に限り、本適合要件の実機テストの評価結果は「適合（Y）」となる。

評価項目１：

IoT 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ていること。

評価項目２：

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ていること。

2. 補足説明

2.1. 適合判断基準の補足説明

2.1.1. 技適マーク認定製品に対する試験結果の再利用

電気通信事業法に基づく端末機器セキュリティに関わる技術基準（端末設備規則第三十四条の十）の要件を満した技適マーク（[T]マーク又は[A]マーク）付与製品においては、本適合要件での実機テストによる評価を、技術適合認定を受けた際の試験結果によって代用することができる。この場合は、証跡（エビデンス）に基づく根拠として、「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）」を受けた際の試験結果を保管しておくこと。

2.1.2. 実機テストでの評価方法

実機テストでの評価方法としては、認証値及びアップデートの情報を UI 等で確認し、それが直前の状態から変わっていないことを確認することでもよい。

2.2. 例外的なケースでの適合判断

該当事項なし

【★1 適合基準 S1.1-15】

適合要件

IoT 製品利用中に IoT 製品のストレージに保存されたデータの削除機能について、以下の①・②のすべての基準を満たすこと。

① ユーザによって、IoT 機器本体や必須付随サービス（モバイルアプリケーション等）を介して、ユーザに関する少なくとも以下のデータを削除できること。

A）IoT 製品利用中に取得した情報資産（個人情報含む）

B）ユーザ設定値

C）ユーザが設定した認証値、IoT 製品利用中に取得した暗号鍵やデジタル署名

② データ削除後も、アップデートされたセキュリティ機能に関するファームウェア（ソフトウェア）パッケージのバージョンは維持されること。

対象外（NA）となるための条件、基準の補足説明

【対象外（NA）となるための条件】

該当事項なし

★1 評価手法

- ドキュメント評価：対象とする
  IoT 製品の技術文書において、ユーザによって、IoT 機器本体や必須付随サービス（モバイルアプリケーション等）を介して、ユーザに関する情報を消去できる機能を有することを評価する。
- 実機テスト：対象とする
  実機テストにより、ユーザに提示された手順によるデータ削除機能の動作及びデータ削除後にファームウェア（ソフトウェア）のバージョンが維持されていることを評価する。

★1 評価ガイド

1. 適合判断基準

本適合要件に対して、以下のドキュメント評価及び実機テストの両方の評価結果が「適合（Y）」となった場合に限り、最終的に「適合（Y）」と判定される。

【ドキュメント評価】

IoT 製品の技術文書において、ユーザによって、IoT 機器本体や必須付随サービス（モバイルアプリケーション等）を介して、少なくとも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。以下の評価項目１～２のすべてを満たしていることが確認できる場合に限り、本適合要件のドキュメント評価の評価結果は「適合（Y）」となる。

評価項目１：

技術文書に、IoT 製品利用中に当該 IoT 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）を削除するための消去方法が明示されていること。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）及びベンダーが 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）の消去方法
B） ユーザに関するユーザ設定値の消去方法
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署名の消去方法

評価項目２：

評価項目１に記載された削除機能の利用手順が、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されていること。

【実機テスト】

ユーザに提示された手順に従って、評価項目１の A）～C）に該当するデータが実際に削除できること、及びデータ削除後にファームウェア（ソフトウェア）のバージョンが維持されていることを評価する。以下の評価項目３と４の両方を満たしている（「合格」となる）ことが確認できる場合に限り、本適合要件の実機テストの評価結果は「適合（Y）」となる。

評価項目３：

ユーザに提示された手順に従って、評価項目１の A）～C）に該当するデータに関して削除を行い、実際にデータが削除されていることを確認する。削除されたことが確認できた場合、本評価項目は「合格」、削除できていなければ本評価項目は「不合格」となる。

なお、実機テストは、評価項目１の A）～C）ごとに、すべ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を確認するサンプルテストでもよい。

評価項目４：

評価項目３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が維持されることを確認する。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）のバージョンが維持されることを確認できた場合、本評価項目は「合格」、確認できなければ本評価項目は「不合格」となる。

2. 補足説明

2.1. 適合判断基準の補足説明

2.1.1. 削除（データ消去）レベルの考え方

★1 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（NIST SP800-88 Rev.1 での「Clear」レベル）での削除を求める。

NIST SP800-88 Rev1 日本語訳
https://www.ipa.go.jp/security/crypto/gmcbt80000005u4j-att/SP800-88rev1.pdf

データが保存されている媒体に応じて削除されたことの確認方法の例を以下に示す。

例１：汎用のストレージデバイス（HDD）の場合：
別の意味のない値で書き換えられている（ストレージデバイスへの標準的な読み書きコマンドを介して削除を実行できるレベル）ことを確認する、又は HDD の Secure Erase 機能を使用して消去されていることを確認する。

例２：汎用のストレージデバイス（SSD）の場合：
SSD の Enhanced Secure Erase 機能を使用して消去されていることを確認する。

例３：専用のストレージデバイス（HDD、SSD 等）以外のストレージデバイスにおいて、上書き機能がサポートされない場合：
工場出荷時にリセットしていたり、ファイルポインターを削除する機能のみが提供される場合は、IoT 機器の標準のインタフェースによってアクセスできない状態になっていることを確認する。

例４：必須付随サービスが、汎用の機器（PC、スマホ等）で実行されるアプリケーションの場合：
汎用の機器の機能で同等の削除が行われている（アプリケーションの削除プロセスにおいて自動的に削除される。削除すべきファイル等の情報をユーザに提示し、ユーザはそのファイルを汎用の機器の機能によって削除する等）ことを確認する。

例５：暗号化消去の技術によって消去する
クラウドサービスのオプション機能や PC の汎用 OS の機能等として暗号化消去が有効になっている媒体（領域）に保存される場合には、暗号化に利用する暗号鍵が消去されることを確認する。

2.2. 例外的なケースでの適合判断

2.2.1. ユーザが自ら削除できない場合の代替措置

本適合要件では、原則的に IoT 製品のストレージに保存されたユーザに関するデータはユーザ自身が削除できることを求めている。

しかし、ユーザ自身では削除できず、専門の業者や IoT 製品ベンダーに依頼して削除してもらう必要がある IoT 機器の場合には、「ユーザに関するデータは削除するには、専門の業者や IoT 製品ベンダーに削除依頼する処理が必要である」旨を、ユーザが入手・確認しやすいマニュアル等に明示することによって、本適合要件は「適合（Y）」とみなす。例えば、クラウドサービス（必須付随サービス）に保存されている情報で、ユーザが直接削除できない場合は、「当該情報のユーザからの削除依頼を IoT 製品ベンダーが受け付け、クラウドサービスからのデータ削除を実行する」旨をユーザに提示していることを条件に、本適合要件を「適合（Y）」と判断することができる。

【★1 適合基準 S1.1-16】

適合要件

製造業者は、IoT 製品のサイバーセキュリティに関する情報提供について、以下の①～⑤のすべての基準を満たす対応を行うこと。

① 初期設定の方法など、IoT 製品の利用上、サイバーセキュリティに影響が生じる設定や使用方法について、安全に利用できる手順を周知すること。

② IoT 製品のセキュリティアップデートのリリース時にそのアップデートの内容や必要性、アップデートを行わない場合の影響などを周知する仕組みがあること。

③ アップデートを行わなかったときに想定される事故や障害・一般的に想定される事故や障害に対して、免責事項を周知すること。

④ 対象製品やサービスのサポート期限又はサポート終了時の方針を周知すること。

⑤ IoT 製品内に守るべき情報資産が残留したまま廃棄や中古販売することで想定されるリスクや、データ消去を含む IoT 製品の安全な利用終了方法を周知すること。

対象外（NA）となるための条件、基準の補足説明

【対象外（NA）となるための条件】

該当事項なし

【用語定義：守るべき情報資産】

以下のすべての情報：

- 通信機能に関する設定情報
- セキュリティ機能に関する設定情報
- IoT 機器の意図する使用において、IoT 機器が収集し、保存又は通信する、個人情報等の一般的に機密性が高い情報

★1 評価手法

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

★1 評価ガイド

1. 適合判断基準

本適合要件に対して、以下のドキュメント評価の評価結果が「適合（Y）」となった場合に限り、最終的に「適合（Y）」と判定される。

【ドキュメント評価】

IoT 製品のマニュアル、ウェブサイト等、ユーザがアクセス可能な媒体において、IoT 製品のサイバーセキュリティに関する情報提供がされていることを評価する。以下の評価項目１～５のすべてを満たしている（「合格」となる）ことが確認できる場合に限り、本適合要件のドキュメント評価の評価結果は「適合（Y）」となる。

評価項目１：

初期設定の方法やパスワード変更の実施手順等、IoT 製品の利用上、サイバーセキュリティに影響が生じる設定や使用方法について、安全に利用できる手順を示した情報をユーザが入手可能であることを確認する。そういった情報が入手可能であることの根拠として、チェックリストに当該情報の入手方法を記載すること。チェックリストに入手方法が記載されている場合に、本評価項目は「合格」として扱う。

評価項目２：

技術文書により、IoT 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等を周知する仕組みや実施方法が整備されていることを確認する。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記されている場合に、本評価項目は「合格」として扱う。

評価項目３：

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が明示されていることを確認する。明示されている根拠として、チェックリストには免責事項が明示されている場所を記載すること。チェックリストに場所が記載されている場合に、本評価項目は「合格」として扱う。

評価項目４：

★1 では、適合ラベルの有効期間中のサポートの提供を必須としており、サポート期限についても適合ラベル取得製品ホームページにて周知を行うこととしている。したがって、本評価項目については、★1 適合ラベル申請書に記載するサポート期間に虚偽がなく、かつ適合ラベルの有効期間中のサポートの提供義務に同意して申請する限り、「合格」として扱う。なお、本評価項目の申請内容に虚偽があれば、自己適合評価結果いかんにかかわりなく、チェックリスト全体を「不合格」とし、適合ラベルの申請却下や取消しを含む措置をとる。

評価項目５：

ユーザが入手・確認しやすいところで、IoT 製品内に守るべき情報資産が残留したまま廃棄や中古販売することで想定されるリスクや、データ消去を含む製品の安全な利用終了方法が説明されていることを確認する。明示されている根拠として、チェックリストにそれらの情報が説明されている場所を記載すること。チェックリストに場所が記載されている場合に、本評価項目は「合格」として扱う。

2. 補足説明

2.1. 適合判断基準の補足説明

該当事項なし

2.2. 例外的なケースでの適合判断

該当事項なし

Appendix. A 用語説明

用語	説明
カスタマーエンジニア	ベンダー側の保守担当者を指す。
通信機能に関する設定情報	守るべき情報資産に値する、通信機能に関する設定情報例を以下に示す。 例 1 ：Wi-Fi の SSID 例 2 ：WPA 暗号キー（Wi-Fi パスワード）　等
セキュリティ機能に関する設定情報	守るべき情報資産に値する、通信機能に関する設定情報例を以下に示す。 例 1 ：TLS 通信設定情報 例 2 ：Firewall 設定情報　等
一般的に機密性が高い情報	評価対象の「IoT 機器の意図する使用において、IoT 機器が収集し、保存又は通信する、個人情報等の一般的に機密性が高い情報」は、想定する IoT 機器の利用目的、環境等を考慮し、IoT 製品の特性として、何がこれにあたるかを IoT 製品ベンダーが判断して決定する。例えば Web カメラの画像等、法令・規制に関わる情報が、一般的に機密性が高い情報にあたる。
IoT 製品のストレージ	IoT 製品のストレージ例を以下に示す。 IoT 機器内蔵のストレージ、必須付随サービスに含まれるストレージを対象とする。 例 1 ：フラッシュ ROM 例 2 ：HDD 例 3 ：SSD 例 4 ：リムーバブルストレージ　等

Appendix. B 修正履歴

2024.12.13　第 1 版公開