参考資料_★3 適合基準案_ガイダンス文書あり（通信機器）

適合基準番号 : S3.1-02

★3 適合基準

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 8 文字以上のパスワードであること。

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

対象外（NA）となるための条件、基準の補足説明

【対象外（NA）となるための条件】

パスワード利用した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認証が必要ない根拠を記載すること）

【用語定義：ユーザ】

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

★3 評価手法

・ドキュメント評価：

対象とする

・実機テスト：

対象とする

★3 適合ガイド（製造業者向け）

本適合基準では、

・IoT 製品が安全なパスワードを使用して運用されるための対策が取られること

を要求する。

ネットワークを介したユーザ認証の仕組みにおいて、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として、以下の適合要件１、２のいずれかを満たす実装がされていること。

適合要件 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、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

適合要件 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。
IoT 機器は、この時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ユーザに警告する実装でなければならない。
容易に推測可能でないパスワードとしては、以下の①～④の実装が考えられる。これに類するか、それ以上の実装であること。
どのように実装するかは製造業者が選定できる。
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)
②ランダム性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

★3 評価ガイド（製造業者・評価機関向け）
評価機関は、以下の【ドキュメント評価】及び【実機テスト】の結果が「適合（Y)」の場合に限り、本適合基準の評価結果を「適合（Y)」と判断する。

【技術文書】
製造業者は、以下の技術文書を評価機関に提出する。
技術文書 1 ： IoT 製品で使用する全てのパスワード認証機能のリスト
技術文書 1 に含まれるすべてのパスワード認証機能について、技術文書 2 － 1)、又

は、技術文書２－２）を提出する。
技術文書２－１）：適合要件１にて適合するパスワード認証の場合、デフォルトパスワードの仕様が記載された文書であり、適合要件１に適合することの根拠が記載されている文書（製造工程を指示する文書等）
技術文書２－２）：適合要件２にて適合するパスワード認証の場合、パスワード認証機能の仕様が記載された文書であり、適合要件２に適合することの根拠が記載されている文書（設計仕様書等）

【ドキュメント評価】
評価機関は、技術文書１に記載された全ての認証機能について、評価項目１、又は２の評価を実施する。全ての評価結果が「適合（Y)」の場合にのみ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：
適合要件１で適合する場合は、該当するパスワード認証機能についての技術文書２－１）に、設定されるデフォルトパスワードが、適合要件１ A)～D)の条件に一致しないパスワードであることが明記されていることを確認する。
評価項目２：
適合要件２で適合する場合は、該当するパスワード認証機能についての技術文書２－２）に、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こと、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は、容易に予測可能でない８文字以上のパスワードであることを強制するか、容易に予測可能でない８文字以上のパスワードでない場合にユーザに警告を表示する機能を有することが、が明記されていることを確認する。
容易に予測可能でないパスワードの条件は、適合要件１と同じとする。

【実機テスト】
評価機関は、実機において、技術文書１に記載された全てのパスワードに基づく認証機能について、評価項目３の評価を実施する。全ての評価結果が「適合（Y)」の場合にのみ実機テストの評価結果は「適合（Y)」となる。
評価項目３：
ドキュメント評価の結果、適合要件２を満たすことによって適合と判断する全ての IoT 機器のパスワードに基づく認証機能について、設定しようとした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ない場合に、対象製品がそれを検出する機能があることを確認する。
検出した場合には、そのパスワードの設定を拒否するか、ユーザに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ないことを警告することを確認する。

適合基準番号 : S3.1-01

★3 適合基準

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。
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すること。

対象外（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
・ログ（テレメトリデータ・監査ログ）
・プログラムコード（ソフトウェア）
・IoT 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

【用語定義：ユーザ】
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

★3 評価手法

・ドキュメント評価：
対象とする
・実機テスト：
対象とする

★3 適合ガイド（製造業者向け）

本適合基準では、
・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（読出、書込、更新、削除）において適切な認証に基づいてアクセス制御されていること
を要求する。
適切な認証に基づくアクセス制御は、以下の適合要件 1 ～ 4 を満たすこと。
適合要件 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、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。

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 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

＊)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）

適合要件２：

機密セキュリティパラメータの変更においては、たとえ認証済みであっても改めて認証を要求すること。

適合要件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。

適合要件４：

IoT 製品の初期状態において、IoT 製品の利用のために不要なアカウント**)が、削除または無効化されていること。

**)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

★3 評価ガイド（製造業者・評価機関向け）

評価機関は、以下の【ドキュメント評価】及び【実機テスト】の結果が「適合（Y)」の場合に限り、本適合基準の評価結果を「適合（Y)」と判断する。

【技術文書】

製造業者は、以下の技術文書を評価機関に提出する。

技術文書１：IoT 製品の守るべき情報資産のリスト

技術文書１に含まれるすべての守るべき情報資産について、技術文書２を提出する。

技術文書２：守るべき情報資産に対するアクセス制御の仕様が記載された文書であり、適合要件１・適合要件３に適合することの根拠が記載されている文書
技術文書３：IoT 製品の機密セキュリティパラメータのリスト
技術文書３に含まれる全ての機密セキュリティパラメータについて、技術文書４を提出する。
技術文書４：機密セキュリティパラメータの変更手順の仕様が記載された文書であり、適合要件２に適合することの根拠が記載されている文書
技術文書５：IoT 製品の初期状態において有効になっているアカウントのリスト

【ドキュメント評価】
評価機関は、技術文書１に記載された全ての守るべき情報資産について、評価項目１の評価を実施、技術文書３に記載された全ての機密セキュリティパラメータについて、評価項目２の評価を実施及び評価項目３の評価を実施する。全ての評価結果が「適合（Y)」の場合にのみ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 製品の守るべき情報資産について、そのアクセス制御が、該当の技術文書２に明記されていることを確認する。また、そのアクセス制御の方法が適合要件１の要件を満たすことを確認する。
評価項目２：
IoT 製品の機密セキュリティパラメータについて、その変更手順が該当の技術文書４に明記されていることを確認する。また、変更手順が適合要件２の要件を満たすことを確認する。
評価項目３：
技術文書５に記載の IoT 製品の初期状態において有効になっているアカウントに IoT 製品の利用のために不要なアカウントが含まれていないことを確認する。

【実機テスト】
評価機関は、実機において、技術文書１に記載された全ての守るべき情報資産のアクセス制御について、それぞれ評価項目４の評価を実施する。また、技術文書３に記載された全ての守るべき情報資産について、評価項目５の評価を実施する。全ての評価結果が「適合（Y)」の場合にのみ実機テストの評価結果は「適合（Y)」となる。
評価項目４：
守るべき情報資産について該当する技術文書２に記載されたアクセス制御が実装されていること、および接続が技術文書２の通りにタイムアウトすることを確認する。
評価項目５：
機密セキュリティパラメータについて該当する技術文書４に記載された変更手順が実装

されていることを確認する。

適合基準番号 : S3.1-03

★3 適合基準

IoT 製品に対するネットワークを介した他の IoT 機器又はユーザからのアクセスの認証において使用される認証値の変更について、認証の種類（パスワード、トークン、指紋等）に依らず、その認証値の変更を可能とすること。

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】

ー

【用語定義：認証値】

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

【用語定義：ユーザ】

ユーザの対象範囲には、IoT 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

★3 評価手法

・ドキュメント評価：

対象とする

・実機テスト：

対象とする

★3 適合ガイド（製造業者向け）

本適合基準では、

・IoT 製品に対するユーザ認証にて使用される認証値が変更できること

を要求する。

認証値の変更について、以下の適合要件 1 と 2 の両方を満たすこと。

適合要件 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。
適合要件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。

★3 評価ガイド（製造業者・評価機関向け）

評価機関は、以下の【ドキュメント評価】及び【実機テスト】の結果が「適合（Y)」の場合に限り、本適合基準の評価結果を「適合（Y)」と判断する。

【技術文書】
製造業者は、以下の技術文書を評価機関に提出する。
技術文書１：IoT 製品で使用する全てのユーザ認証機能のリスト
技術文書１に含まれるすべてのユーザ認証機能について、技術文書２及び技術文書３を提出する。
技術文書２：ユーザ認証機能の仕様が記載された文書であり、適合要件１に適合することの根拠が記載されている文書
技術文書３：ユーザに提供される文書であり、ユーザ認証で使用する認証値を変更する手順が記載された文書

【ドキュメント評価】
評価機関は、技術文書１に記載された全てのユーザ認証機能について、評価項目１、２の評価を実施する。全ての認証機能について、評価項目１、２の全ての評価結果が「適合（Y)」の場合にのみ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２に、認証の種類（パスワード、トークン、指紋等）に依らず、その認証値を変更する機能を有することが明記されていることを確認する。
評価項目２：
技術文書３に、その認証値を変更する手順が明記されていることを確認する。

【実機テスト】
評価機関は、実機において、技術文書１に記載された全てのユーザ認証機能について、評価項目３の評価を実施する。評価項目３の評価結果が「適合（Y)」の場合にのみ実機テストの評価結果は「適合（Y)」となる。
評価項目３：
技術文書３に記載された手順に従って、認証値が変更できることを確認する。

適合基準番号 : S3.1-04

★3 適合基準

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

【用語定義：ユーザ】

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

★3 評価手法

・ドキュメント評価：

対象とする

・実機テスト：

対象とする

★3 適合ガイド（製造業者向け）

本適合基準では、

・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

を要求する。

ネットワークを介したユーザ認証の仕組みは、以下の適合要件１、２のいずれかを満たすこと。

適合要件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。

これに加えて、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、評価項目 1

と同様の認証試行制限の対応をしていること。
③アカウントごとにユニークな URL で認証を行うこと。
④CAPTCHA が使用されていること。

適合要件 2：
多要素認証が使用されていること。
注）★3 では、パスワード総当たり攻撃だけでなく、その他の総当たり攻撃（パスワードスプレー攻撃など）に対する対策をとることを求める。

★3 評価ガイド（製造業者・評価機関向け）

評価機関は、以下の【ドキュメント評価】及び【実機テスト】の結果が「適合（Y)」の場合に限り、本適合基準の評価結果を「適合（Y)」と判断する。

【技術文書】
製造業者は、以下の技術文書を評価機関に提出する。
技術文書 1 ：IoT 製品で使用するすべてのパスワードを利用したユーザ認証機能のリスト
技術文書 1 に含まれるすべてのユーザ認証機能について、技術文書 2 を提出する。
技術文書 2 ：ユーザ認証機能の仕様が記載された文書であり、適合要件 1 または 2 のいずれかに適合することの根拠が記載されている文書

【ドキュメント評価】
評価機関は、技術文書 1 に記載されたすべてのユーザ認証機能について、評価項目 1 の評価を実施する。全ての評価結果が「適合（Y)」の場合にのみ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 2 に、適合要件 1 又は 2 のいずれかを満たす総当たり攻撃を困難にする仕組みを実装していることが、明記されていることを確認する。

【実機テスト】
評価機関は、実機において、技術文書 1 に記載された全てのユーザ認証機能について、評価項目 2 の評価を実施する。実施した全ての評価項目の評価結果が「適合（Y)」の場合にのみ実機テストの評価結果は「適合（Y)」となる。
評価項目 2 ：
技術文書 2 に記載された、総当たり攻撃を困難とするユーザ認証の仕組みが機能することを確認する。

適合基準番号 : S3.1-05

★3 適合基準

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つこと。

IoT 製品で使用する電子証明書は、更新可能とすること

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】

IoT 製品において、認証のために電子証明書を使用していない

★3 評価手法

・ドキュメント評価：

対象とする

・実機テスト：

対象とする

★3 適合ガイド（製造業者向け）

本適合基準では、

IoT 製品において認証のために使用する電子証明書が十分なセキュリティ強度を持つこと、危殆化した場合に電子証明書をセキュアな電子証明書に更新可能であること、製品のクラスに対する自動化された攻撃のリスクを低減するメカニズムで生成されること

を要求する。

IoT 製品において認証のために使用する電子証明書は、以下の適合要件 1～4 のすべてを満たすこと

適合要件１：電子証明書で使用する暗号技術は、CRYPTREC で認められた暗号技術*)を使用すること

適合要件２：IoT 製品において使用する電子証明書は更新可能であること

適合要件３：IoT 製品において使用する電子証明書を失効する仕組み、あるいは、その他の方法で IoT 製品への認証ができなくする仕組みを持つこと

適合要件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 IoT 機器毎に固有であること

*)CRYPTREC で認められた暗号技術:

「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

―

★3 評価ガイド（製造業者・評価機関向け）

評価機関は、以下の【ドキュメント評価】及び【実機テスト】の結果が「適合（Y)」の場合に限り、本適合基準の評価結果を「適合（Y)」と判断する。

【技術文書】

製造業者は、以下の技術文書を評価機関に提出する。

技術文書１：IoT 製品で使用するすべての電子証明書を使用する認証機能のリスト

技術文書１に含まれるすべての電子証明書を使用する認証機能・生成メカニズムについて、技術文書２を提出する。

技術文書２：電子証明書・生成メカニズムを使用する認証機能の仕様が記載された文書であり、適合要件１～４のすべてに適合することの根拠が記載されている文書

【テストデータ】

製造業者は実機テストにおいて使用する以下のデータを評価機関に提出する。

テストデータ１：技術文書１に記載されたそれぞれの認証に使用する電子証明書のサンプル

【ドキュメント評価】

評価機関は、技術文書１に記載されたすべての電子証明書を使用する認証機能について、評価項目１～４の評価を実施する。全ての評価結果が「適合（Y)」の場合にのみ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２に、電子証明書で使用する暗号アルゴリズムが適合要件１を満たすことを確認する。

評価項目２：

技術文書２に電子証明書が更新可能であることが明記されていることを確認する。

評価項目３：

技術文書２に、電子証明書を失効する仕組み、あるいは、その他の方法で IoT 製品への認証ができなくする仕組みが明記されていることを確認する。

評価項目４：

技術文書 2 により、電子証明書秘密鍵の生成メカニズムが明記されており、IoT 機器毎に固有となることを確認する。

【実機テスト】
評価機関は、実機において、技術文書 1 に記載された全ての電子証明書を使用する認証機能について、評価項目 5、6 の評価を実施する。実施した全ての評価項目の評価結果が「適合（Y)」の場合にのみ実機テストの評価結果は「適合（Y)」となる。
評価項目 5 ：
テストデータ 1 として提供された電子証明書を確認し、適合要件 1 を満たす暗号アルゴリズムが使用されていることを確認する。
評価項目 6 ：
技術文書 2 に記載された電子証明書を失効する仕組み、あるいは、その他の方法で IoT 製品への認証をできなくする仕組みを実行し、当該証明書を利用した認証が出来なくなっていることを確認する。

適合基準番号 : S3.1-06

★3 適合基準

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ていること。

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】
IoT 製品において、SSH を公開鍵認証にて利用していない

★3 評価手法

・ドキュメント評価：
対象とする
・実機テスト：
なし

★3 適合ガイド（製造業者向け）

本適合基準では、
IoT 製品において SSH を公開鍵認証にて利用する場合、利用する暗号技術が十分なセキュリティ強度をもつこと
を要求する。

IoT 製品の SSH の公開鍵認証機能は、以下の適合要件１、２の両方を満たすこと
適合要件１：SSH の公開鍵認証機能で使用する暗号技術は、CRYPTREC で認められた暗号技術*)を使用すること
※対象の暗号技術には、公開鍵認証で使用する公開鍵アルゴリズム、ハッシュアルゴリズムを含む
適合要件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

*)CRYPTREC で認められた暗号技術:
「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

★3 評価ガイド（製造業者・評価機関向け）

評価機関は、以下の【ドキュメント評価】の結果が「適合（Y)」の場合に限り、本適合要件の評価結果を「適合（Y)」と判断する。

【技術文書】
製造業者は、以下の技術文書を評価機関に提出する。
技術文書１：SSH の公開鍵認証の仕様が記載された文書であり、適合要件１、２のすべてに適合することの根拠が記載されている文書

【ドキュメント評価】
評価機関は、評価項目１、２の評価を実施する。すべての評価結果が「適合（Y)」の場合にのみ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１に、SSH の公開鍵認証で使用する暗号アルゴリズムが適合要件１を満たすことを確認する。
評価項目２：
技術文書１に SSH の公開鍵認証で使用する公開鍵が更新可能であることが明記されていることを確認する。

適合基準番号 : S3.1-07

★3 適合基準

IoT 製品において VPN ゲートウェイ機能をもつ場合は、以下の①～②の基準をすべて

満たすこと。
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、基準の補足説明

【対象外（NA）となるための条件】
IoT 製品において、VPN ゲートウェイ機能を持たない。

【用語定義：VPN ゲートウェイ機能】
内部ネットワークとインターネット等の外部ネットワークの境界に置かれ、ユーザとの間に暗号化された通信経路を作成する機能

★3 評価手法

・ドキュメント評価：
対象とする
・実機テスト：
なし

★3 適合ガイド（製造業者向け）

本適合基準では、
IoT 製品において VPN ゲートウェイ機能をもつ場合、VPN 接続*1)において厳格なユーザ認証及び機器の接続制限を行う方式を実装すること
を要求する。
IoT 製品のユーザ認証機能は、以下の適合要件 1 を満たすこと
適合要件 1 ：利用されるユーザ認証の方法が、多要素認証またはそれに類する実装*2)であること
IoT 製品の機器認証機能は、以下の適合要件 2 を満たすこと
適合要件 2 ：
利用される機器の接続制限の方式が、証明書を用いた機器の認証、または事前に機器を一意に識別できる情報を登録する方式であること。ただし、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。
VPN 接続における VPN プロトコルは、以下の適合要件 3 を満たすこと
適合要件 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）が使用できること。

*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。

*2)それに類する実装：
FIDO 認証、または、一部の 2 段階認証と呼ばれる方式を含む。一部の 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。一部の 2 段階認証を用いることのリスクを評価した上で利用する必要がある。

＜補足説明＞
本セキュリティ要件は政府機関等の対策基準策定のためのガイドライン（令和 7 年度版）6.4.1(2)-5 に準拠する。

★3 評価ガイド（製造業者・評価機関向け）
評価機関は、以下の【ドキュメント評価】の結果が「適合（Y)」の場合に限り、本適合要件の評価結果を「適合（Y)」と判断する。

【技術文書】
製造業者は、以下の技術文書を評価機関に提出する。
技術文書 1 ：VPN 接続におけるユーザ認証方式が記載された文書
技術文書 2 ：VPN 接続における機器の接続制限の方式が記載された文書
技術文書 3 ：VPN 接続において利用可能な VPN プロトコルが記載された文書

【ドキュメント評価】
評価機関は、評価項目 1 、 2 の評価を実施する。すべての評価結果が「適合（Y)」の場合にのみ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 1 に、利用されるユーザ認証の方法が、多要素認証またはそれに類する実装であることが明記されていることを確認する。
評価項目 2 ：
技術文書 2 に、利用される機器の接続制限の方式が、証明書を用いた機器の認証、または事前に機器を一意に識別できる（偽装や搾取が容易ではない）情報を登録する方式であることが明記されていることを確認する。

評価項目３：
技術文書３の記載に、一般的に安全と認知されているプ VPN ロトコル（例：OpenVPN、IPsec、IKEv2 など）が含まれていることを確認する。

適合基準番号 : S3.1-08

★3 適合基準

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

★3 評価手法

・ドキュメント評価：
対象とする
・実機テスト：
なし

★3 適合ガイド（製造業者向け）

本適合基準では、
IoT 機器は、接続する機器を識別し、接続を許可、または拒否する方式を実装することを要求する。
IoT 機器に接続する機器の識別方式は、以下の適合要件１を満たすこと
適合要件１：
利用される識別方式が、MAC アドレスなど一意に機器を識別できる値を使用したもの、もしくはクライアント証明書を用いた方式であること。

＜補足説明＞
本セキュリティ要件は政府機関等の対策基準策定のためのガイドライン（令和７年度版）6.4.1(1)-3 に準拠する。
本セキュリティ要件ではネットワークを構成するインテリジェントスイッチなどの通信機器に、無許可の機器の接続を拒否する機能が実装されていることを要求している。外部から内部ネットワークへの接続のゲートウェイとなる通信機器に関しては 1-8 のセキ

ュリティ要件において、さらに厳格な機器の接続制限機能が実装されていることを要求している。

★3 評価ガイド（製造業者・評価機関向け）

評価機関は、以下の【ドキュメント評価】の結果が「適合（Y)」の場合に限り、本適合要件の評価結果を「適合（Y)」と判断する。

【技術文書】

製造業者は、以下の技術文書を評価機関に提出する。

技術文書１：各ポートに接続される機器を識別し、接続を許可または拒否する機能について記載された文書

【ドキュメント評価】

評価機関は、評価項目１の評価を実施する。評価結果が「適合（Y)」の場合にのみ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１に記載された機器の識別方式が、MAC アドレスなど一意に機器を識別できる値を使用したもの、もしくはクライアント証明書を用いた方式であることを確認する。

適合基準番号 : S3.1-09

★3 適合基準

製造業者は、以下の①～④のすべての情報を含む脆弱性開示ポリシーを公開（例：製造業者のウェブサイトへの掲載）すること。

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

②製造業者が IoT 製品のセキュリティに関する報告を受領した後に行う手続き（セキュリティに関する報告をどのように受付け、その後にどのような手続き・方法で報告者と連絡を取り合うのか、報告に対してどのような対応をするのか、善意の報告に対する法的免責付与の宣言等）及びその概要

③脆弱性が解決されるまでの IoT 製品や脆弱性の状況更新に関する手続き（脆弱性が解決されるまでどのように調査や対策が行われ、どのようにその状況が管理・公表されるのか、報告者に対してどのような対応をするのか等）及びその概要

④脆弱性の対応について、適切な報告先機関へタイムリーに報告することの宣言

対象外（NA）となるための条件、基準の補足説明

―

★3 評価手法

・ドキュメント評価：

対象とする

・実機テスト：

なし

★3 適合ガイド（製造業者向け）

本適合基準では、

・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

を要求する。

脆弱性ポリシーの開示において、以下の適合要件１～５のすべてを満たすこと。

適合要件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。

適合要件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。

適合要件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。

適合要件４：

脆弱性開示ポリシーは、ユーザがアクセス可能な媒体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、公開する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。

適合要件５：

脆弱性の対応について以下のような IPA または指定機関に報告するタイムラインの宣言がされていること。なお、報告する脆弱性対象については製造業者にて判断基準を定めること。

製造業者が設定するタイムライン例

・早期警戒通知：製造業者が脆弱性を認知してから 24 時間以内
・脆弱性通知：製造業者が脆弱性を認知してから 72 時間以内
・最終報告：是正措置・緩和措置が利用可能となってから 14 日以内

★3 評価ガイド（製造業者・評価機関向け）

評価機関は、以下の【ドキュメント評価】の結果が「適合（Y)」の場合に限り、本適合基準の評価結果を「適合（Y)」と判断する。

【技術文書】

製造業者は、以下の技術文書を評価機関に提出する。

技術文書１：脆弱性開示ポリシーを記載した文書(ユーザに提供する文書)

技術文書２：技術文書１を公開する計画を記載した文書（技術文書１が未公開の場合）

【ドキュメント評価】

評価機関は、技術文書１について、評価項目１、２の評価を実施する。評価項目１、２の全ての評価結果が「適合（Y)」の場合にのみ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１がユーザに提供されることを確認する。

IoT 製品が発売前で、技術文書１が未公開の場合は、技術文書２に IoT 製品の発売前に公開される計画が明記されていることを確認する。

（※適合要件４に対応）

評価項目２：

脆弱性開示ポリシーが、適合要件１～３、５の全てを満たすこと確認する。

適合基準番号 ：S3.1-10

★3 適合基準

IoT 製品に含まれるソフトウェアコンポーネントのアップデート機能について、以下の①～④のすべての基準を満たすこと。
①IoT 製品のファームウェア（ソフトウェア）パッケージについて、アップデートが可能であること。
②ファームウェア（ソフトウェア）パッケージのバージョンの確認が行えるなど、最新のファームウェア（ソフトウェア）がインストールされていることを確認する手段を有すること。
③アップデートされたファームウェア（ソフトウェア）パッケージのバージョンが電源 OFF 後も維持されること。
④自動アップデート機能を有すること。

対象外（NA）となるための条件、基準の補足説明

―

★3 評価手法

・ドキュメント評価：
対象とする
・実機テスト：
対象とする

★3 適合ガイド（製造業者向け）

本適合基準では、
・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有すること
を要求する。
アップデート機能は、以下の適合要件１～４のすべてを満たすこと。
適合要件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機能を有すること。
適合要件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。
適合要件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。

適合要件４：
自動アップデートの機能を有すること。あるいは、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。

＜補足説明＞
自動アップデート機能を初期状態で有効にすることを求めない。

★3 評価ガイド（製造業者・評価機関向け）

評価機関は、以下の【ドキュメント評価】及び【実機テスト】の結果が「適合（Y)」の場合に限り、本適合基準の評価結果を「適合（Y)」と判断する。

【技術文書】
製造業者は、以下の技術文書を評価機関に提出する。
技術文書１：ソフトウェアコンポーネントのアップデート機能の仕様を記載した文書
技術文書２：ソフトウェアコンポーネントのバージョンの確認方法等、最新のソフトウェアコンポーネントがインストールされていることの確認方法を記載した文書（ユーザに提供する文書）
技術文書３：ソフトウェアコンポーネントのアップデート手順を記載した文書。（自動アップデート機能の有効／無効を切り替える機能を有する場合は、自動アップデート機能の有効／無効を切り替える手順を含む。）（ユーザに提供する文書）

【ドキュメント評価】
評価機関は、製造業者から提供されたドキュメント（技術文書）によって、評価項目１～２の評価を実施する。評価項目１～２の全ての評価結果が「適合（Y)」の場合にのみ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１に、ソフトウェアコンポーネントのアップデート機能を有することが明記されていることを確認する。
また、アップデート機能は、自動で実行可能であること、あるいは、アップデートが実施されていない場合に警告を表示する機能を有することが明記されていることを確認する。
評価項目２：
技術文書２に、ソフトウェアコンポーネントのバージョンの確認方法等、最新のファームウェアがインストールされていることの確認方法が明記されていることを確認する。

【実機テスト】

評価機関は、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３～５の全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３：

技術文書３に記載されたソフトウェアコンポーネントのアップデート手順に従って操作し、正常にアップデートが完了できることを確認する。

評価項目４：

IoT 製品が自動アップデート機能を有する場合は、自動アップデート機能の有効／無効を切り替える機能を有する場合、技術文書３に記載された自動アップデート機能の有効／無効を切り替える手順に従って操作し、自動アップデート機能が有効化／無効化できることを確認する。有効化した後、正常にアップデートできることを確認する。

IoT 製品がアップデートが実施されていない場合に警告を表示する機能を有する場合は、仕様通り警告が表示されることを確認する。

評価項目５：

IoT 機器の電源を OFF/ON し、アップデートされたソフトウェアコンポーネントのバージョンが電源 OFF 後も維持されることを確認する。

適合基準番号 : S3.1-11

★3 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。

対象外（NA）となるための条件、基準の補足説明

【用語定義：ユーザ】

ユーザの対象範囲には、IoT 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

★3 評価手法

・ドキュメント評価：

対象とする

・実機テスト：

なし

★3 適合ガイド（製造業者向け）

本適合基準では、

・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要求する。

ソフトウェアのアップデートに関する手順は、以下の適合要件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。

適合要件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。

適合要件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。

適合要件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。

適合要件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明示されていること。

＜補足説明(★１評価ガイドを踏襲）＞

「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。

★3 評価ガイド（製造業者・評価機関向け）

評価機関は、以下の【ドキュメント評価】の結果が「適合（Y)」の場合に限り、本適合基準の評価結果を「適合（Y)」と判断する。

【技術文書】

製造業者は、以下の技術文書を評価機関に提出する。

技術文書１：ソフトウェアコンポーネントのアップデート手順を記載した文書。(自動アップデート機能の有効／無効を切り替える機能を有する場合は、自動アップデート機能の有効／無効を切り替える手順を含む。)（ユーザに提供する文書（＊））

（上記技術文書は、S3.1-10（3-1)の技術文書３と記載すべき内容は同一）

（＊）ユーザに提供する文書がリリース前等存在しない場合は、手順書にて評価を実施する。

【ドキュメント評価】
評価機関は、製造業者から提供されたドキュメント（技術文書）によって、評価項目１、２及び手動でのアップデートをサポートする場合には評価項目３の評価を実施する。評価項目１～３の全ての評価結果が「適合（Y)」の場合にのみ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１がユーザが確認できる媒体（マニュアル、製品 HP 等）で、ユーザに提供されていることを確認する。
評価項目２：技術文書１に、自動アップデートが失敗した場合の対応方法が記載されていることを確認する。
評価項目３：IoT 製品が手動アップデート機能を提供する場合は、技術文書１に、A)～C)のいずれかに類するソフトウェアコンポーネントをアップデート実行する手順が明示されていることを確認する。
A)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
B)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
C)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

適合基準番号 : S3.1-12

★3 適合基準

ソフトウェアをアップデートする際に以下①から③全てを満たす機能があること。
①ソフトウェアの完全性及び真正性をアップデート前に IoT 製品が確認できる仕組みを有すること。
②真正性を満たさない場合は更新を中断すること。
③アンチロールバックの機能を有すること。

対象外（NA）となるための条件、基準の補足説明

―

★3 評価手法

・ドキュメント評価：

対象とする

・実機テスト：

対象とする

★3 適合ガイド（製造業者向け）

本適合基準では、

・IoT 製品の技術文書において、ソフトウェアの完全性及び真正性をアップデート前に確認できる仕組みが実装されていること

を要求する。

ソフトウェアの完全性及び真正性を確認する仕組みは、以下の適合要件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おり、かつ適合要件３及び４を満たすこと。

適合要件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。

適合要件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。

適合要件３：

適合要件 1、２で利用するデジタル署名で使用する暗号技術は、CRYPTREC で認められた暗号技術*)を使用すること。

適合要件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または以前のバージョンであることが確認されていた場合にはアップデートが中止されること。

ただし、本適合要件は、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。

*)CRYPTREC で認められた暗号技術:

「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

★3 評価ガイド（製造業者・評価機関向け）

評価機関は、以下の【ドキュメント評価】及び【実機テスト】の結果が「適合（Y)」の場合に限り、本適合基準の評価結果を「適合（Y)」と判断する。

【技術文書】

製造業者は、以下の技術文書を評価機関に提出する。

技術文書１：ソフトウェアコンポーネントのアップデート仕様を記述した文書であり、更新ソフトウェアの完全性及び真正性の確認方法が記載されている文書

【実機テスト用データ】

製造業者は、実機テストのために、以下のテストデータを評価機関に提出する。

テストデータ１：正当なデジタル署名が付与された更新ソフトウェア

テストデータ２：不正なデジタル署名が付与された更新ソフトウェア

テストデータ３：以前のバージョンが付与された更新ソフトウェア

【ドキュメント評価】

評価機関は、製造業者から提供されたドキュメント（技術文書）によって、評価項目１、２のいずれか（またはその両方)、及び評価項目３の評価を実施する。評価項目１、２のいずれか（またはその両方)、及び評価項目３の評価結果が「適合（Y)」の場合にのみドキュメント評価の評価結果は「適合（Y)」となる。

※更新ソフトウェアの完全性、及び真正性を確認するために実装している機能に応じて、適合要件１に該当する機能を有する場合は評価項目 1、適合要件２に該当する機能を有する場合には評価項目２の評価を行う。両方の機能を有する場合は評価項目１、２の両方の評価を行う。

評価項目１：

技術文書１に、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仕様であることが明記されていることを確認する。

評価項目２：

技術文書１に、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

れる仕様であることが明示されていることを確認する。
評価項目３：
評価項目 1、２ で利用するデジタル署名で使用する暗号技術は、CRYPTREC で認められた暗号技術*)を用いていることを確認する。

【実機テスト】
評価機関は、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セキュアな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４～６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４：
テストデータ２を使用してアップデートのテストを実施し、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、IoT 機器、または、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を確認する。
評価項目５：
テストデータ３を使用してアップデートのテストを実施し、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、IoT 機器、または、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バージョンの確認を行い、以前のバージョンであることを確認された場合にはアップデートが中止されることを確認する。
評価項目６：
テストデータ１に付与された電子署名を確認し、更新ソフトウェアに付与されるデジタル署名に利用する暗号技術が、CRYPTREC で認められた暗号技術*)を利用していることを確認する。

*)CRYPTREC で認められた暗号技術:
「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

適合基準番号 : S3.1-13
★3 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。

対象外（NA）となるための条件、基準の補足説明

―

★3 評価手法

・ドキュメント評価：
対象とする
・実機テスト：
なし

★3 適合ガイド（製造業者向け）

本適合基準では、
・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を規定していること
を要求する。
これらの方針や指針において、以下の適合要件１～３のすべてを満たすこと。
適合要件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）等の指針が規定されていること。
適合要件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。
適合要件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。

※： 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

★3 評価ガイド（製造業者・評価機関向け）

評価機関は、以下の【ドキュメント評価】の結果が「適合（Y)」の場合に限り、本適

合基準の評価結果を「適合（Y)」と判断する。

【技術文書】
製造業者は、以下の技術文書を評価機関に提出する。
技術文書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方針や指針を規定している文書

【ドキュメント評価】
評価機関は、製造業者から提供されたドキュメント（技術文書）によって、評価項目１～３の評価を実施する。評価項目１～３の全ての評価結果が「適合（Y)」の場合にのみ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１に、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）等の指針が明記されていることを確認する。
評価項目２：
技術文書１に、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明記されていることを確認する。
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は、技術文書１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を確認する。　（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であるかどうかは、製造業者からの申告に基づく。）

適合基準番号 : S3.1-14

★3 適合基準

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、基準の補足説明

【用語定義：ユーザ】

ユーザの対象範囲には、IoT 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

★3 評価手法

・ドキュメント評価：
対象とする
・実機テスト：
対象とする

★3 適合ガイド（製造業者向け）

本適合基準では、
・IoT 製品の型番についてユーザが確認できる方法が、ユーザに提供されていることを要求する。
ユーザが確認できる方法の提供は、以下の適合要件１、２のいずれかを満たすこと。
適合要件１：
IoT 製品本体に IoT 製品の型番及びシリアル番号が記載されていること。
適合要件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 製品の型番及びシリアル番号を確認できる仕組みがあること。
＜補足説明＞
「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。

★3 評価ガイド（製造業者・評価機関向け）

評価機関は、以下の【ドキュメント評価】及び【実機テスト】の結果が「適合（Y)」の場合に限り、本適合基準の評価結果を「適合（Y)」と判断する。

【技術文書】
製造業者は、以下の技術文書を評価機関に提出する。
技術文書１：IoT 製品の型番を確認する方法を記載した文書（ユーザに提供する文書）

【ドキュメント評価】
評価機関は、製造業者から提供されたドキュメント（技術文書）によって、評価項目１、２の評価を実施する。評価項目１、２の評価結果が「適合（Y)」の場合にのみド

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１が、ユーザに提供される文書であることを確認する。
評価項目２：
技術文書１に記載された IoT 製品の品番及びシリアル番号を確認する手順は、適合要件１又は適合要件２のいずれかを満たすことを確認する。

【実機テスト】
評価機関は、対象 IoT 製品の型番及びシリアル番号が確認できることを実機テストにより評価する。評価項目３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３：
技術文書１に記載された手順に従って、型番及びシリアル番号が確認できることを確認する。

適合基準番号 : S3.1-15

★3 適合基準

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、運用を行うこと。具体的には以下の①～③のすべての基準を満たすこと。

①製品出荷後の運用フェーズにおける既知の脆弱性管理のため、製品の構成要素であるソフトウェア（サードパーティコンポーネントを含む）の SBOM を作成し、サポート期間内において更新を行うこと。

②サポート期間内においては、SBOM の情報に基づいて定期的に脆弱性の確認を行い、対応優先度を判断した上で、更新あるいは運用対処等を行うプロセスを有すること。

③サポート期間内においては、SBOM の情報に基づき、使用するコンポーネントのライセンス管理を行うプロセスを有すること。

対象外（NA）となるための条件、基準の補足説明

―

★3 評価手法

・ドキュメント評価：

対象とする

・実機テスト：

なし

★3 適合ガイド（製造業者向け）

本適合基準では、

・該当の IoT 製品に関して、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、機械可読な形式のソフトウェア部品表（SBOM）の作成、運用に関するプロセスが規定されていること

を要求する。

SBOM の作成、運用においては、以下の適合要件 1 ～ 3 のすべてを満たすこと。

適合要件 1 ：

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全てのコンポーネントが、SBOM として記述されていること。SBOM を作成、生成するプロセスを規定していること。サポート期間、及び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。

適合要件 2 ：

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。脆弱性が含まれるコンポーネントについては、IoT 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。

適合要件 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)のライセンス管理を行うプロセスを規定していること。

【補足 1：IoT 製品における 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

【補足 2：SBOM を記述する階層について】

SBOM を記述する階層は、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

個別に判断するものとする。

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を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 スクリプトなど、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

【補足 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）

【補足 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　, バージョン 1.4 以上
- Software Package Data Exchange (SPDX)、バージョン 2.3 以上
- 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

【補足 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

★3 評価ガイド（製造業者・評価機関向け）

評価機関は、以下の【ドキュメント評価】の結果が「適合（Y)」の場合に限り、本適合基準の評価結果を「適合（Y)」と判断する。

【技術文書】

製造業者は、以下のドキュメントを技術文書として評価機関に提出する。

技術文書１：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、機械可読な形式のソフトウェア部品表（SBOM）

技術文書２：SBOM を作成・生成するプロセス、サポート期間、およびサポート期間内において SBOM を更新することが規定された文書

技術文書３：定期的に脆弱性が含まれるコンポーネントが含まれていないことを確認し、対処する運用が規定された文書

技術文書４：ライセンス管理を行うプロセスが規定された文書

【ドキュメント評価】

評価機関は、製造業者から提供されたドキュメント(技術文書）によって、評価項目１～４の評価を実施する。全ての評価項目の評価結果が「適合（Y)」の場合にのみ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 1 において、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全てのコンポーネントが、SBOM として記述されていることを確認する。

評価項目 2 ：
技術文書 2 において、SBOM を作成・生成するプロセス、サポート期間、及びサポート期間内において SBOM を更新することが明記されていることを確認する。

評価項目 3 ：
技術文書 3 において、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、脆弱性が含まれるコンポーネントについては、IoT 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が明記されていることを確認する。

評価項目 4 ：
技術文書 4 において、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が明記されていることを確認する。

適合基準番号 : S3.1-16

★3 適合基準

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

【用語定義：守るべき情報資産】
以下の情報：
・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
・ログ（テレメトリデータ・監査ログ）
・プログラムコード（ソフトウェア）
・IoT 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

★3 評価手法

・ドキュメント評価：
対象とする
・実機テスト：
なし

★3 適合ガイド（製造業者向け）

本適合基準では、
・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
を要求する。
セキュアに保存されていることは、以下の適合要件 1 ～6 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。）が取られていること。
適合要件 1 ：
機密性の保護が必要な守るべき情報資産は、CRYPTREC で認められた暗号技術*)によって暗号化された上で保存されること。
適合要件 2 ：
完全性の保護が必要な守るべき情報資産は、CRYPTREC で認められた暗号技術*)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。
適合要件 3 ：
完全性の保護が必要な守るべき情報資産は、CRYPTREC で認められた暗号技術*)である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。
適合要件 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。
適合要件 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。
適合要件 6 ：
守るべき情報資産のうちログ（テレメトリデータ・監査ログ）については適合要件 1 による保護が行われていること
*)CRYPTREC で認められた暗号技術:
「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

★3 評価ガイド（製造業者・評価機関向け）

評価機関は、以下の【ドキュメント評価】の結果が「適合（Y)」の場合に限り、本適合基準の評価結果を「適合（Y)」と判断する。

【技術文書】

製造業者は、以下の技術文書を評価機関に提出する。

技術文書１：IoT 製品の守るべき情報資産のリスト

技術文書１に含まれるすべての守るべき情報資産について、技術文書２、３を提出する。

技術文書２：守るべき情報資産のセキュリティ要件が記載されている文書

技術文書３：守るべき情報資産のストレージ上での保存の仕様が記載された文書であり、適合要件１～５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ことの根拠が記載されている文書

【ドキュメント評価】

評価機関は、技術文書１に記載された全ての守るべき情報資産について、評価項目１の評価を実施する。全ての評価結果が「適合（Y)」の場合にのみ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３に、守るべき情報資産の保護対策が、適合要件 1～５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ことが明記されていることを確認する。

また、守るべき情報資産に対する保護対策が、技術文書２に記載されているセキュリティ要件に基づいて適切であることを確認する。

適合基準番号 : S3.1-17

★3 適合基準

IoT 製品で使用されるハードコードされた機密セキュリティパラメータ（機器固有の識別子やアイデンティティを証明するための認証コードなど）の改ざん防止のため、以下①・②すべての基準を満たすこと。

①ハードコードされた機密セキュリティパラメータの全容を把握し、一覧化できていること。

②すべての機密セキュリティパラメータは、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、基準の補足説明

【NA となるための条件】

・対象製品においてハードコードされた機密セキュリティパラメータが存在しない

（「NA であることの理由」に、ハードコードされた機密セキュリティパラメータが存在しないことを明示すること）

【機密セキュリティパラメータ】

重要なセキュリティパラメータに以下の要素を加えたもの

・ソフトウェア検証に使用される公開鍵

・証明書の公開要素

・機器固有の ID

★3 評価手法

・ドキュメント評価：

対象とする

・実機テスト：

なし

★3 適合ガイド（製造業者向け）

本適合基準では、

・IoT 製品で使用されるハードコードされた機密セキュリティパラメータの保護手段として、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

を要求する。

セキュリティパラメータ及び保護手段の記述、および実装については、以下のすべての適合要件を満たすこと。

適合要件１：

ハードコードされた機密セキュリティパラメータが一覧化されていること。

適合要件２：

すべてのハードコードされた機密セキュリティパラメータが、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
・難読化や暗号化などソフトウェアによる保護

【補足１：物理的保護の例外事項】
・機器の設置環境が、セキュリティエリア(*1)への設置を前提としている場合、その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。

(*1)：物理的セキュリティに配慮された施設内の共用エリア以外の区画

★3 評価ガイド（製造業者・評価機関向け）

評価機関は、以下の【ドキュメント評価】の結果が「適合（Y)」の場合に限り、本適合基準の評価結果を「適合（Y)」と判断する。

【技術文書】
製造業者は、以下のドキュメントを技術文書として評価機関に提出する。
技術文書１：メモリにハードコードされている全ての機密セキュリティパラメータ一と、それらの改ざんからの保護手段が記載された文書

【ドキュメント評価】
評価機関は、製造業者から提供された提供された技術文書１によって、評価項目１，２の評価を実施する。全ての評価項目の評価結果が「適合（Y)」の場合にのみ、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１に、ハードコードされた機密セキュリティパラメータが一覧化されていることを確認する。

評価項目２：
それらすべてのハードコードされた機密セキュリティパラメータが、以下のいずれかの手段により改ざんから保護されることが明記されていることを確認する。

・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
・難読化や暗号化などソフトウェアによる保護

適合基準番号 : S3.1-18

★3 適合基準

ソースコードに記載された機密セキュリティパラメータに重要なセキュリティパラメータが含まれていないことを確認するため、以下①・②すべての基準を満たすこと。

①ソースコードにハードコードされている機密セキュリティパラメータの全容を把握し、一覧化できていること。
②機密セキュリティパラメータのうち、IoT 製品の運用中に利用される重要なセキュリティパラメータが、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、基準の補足説明

【NA となるための条件】
ソースコードに機密セキュリティパラメータが存在しない（「NA であることの理由」に、ソースコードにハードコードされた機密セキュリティパラメータが存在しないことを明示すること）

【重要なセキュリティパラメータ】
セキュリティに関連する情報であって、その開示または変更が、暗号モジュールのセキュリティを危殆化し得るもの。
（例：共通鍵・秘密鍵・パスワードや PIN などの認証データなど）

★3 評価手法

・ドキュメント評価：
対象とする
・実機テスト：
なし

★3 適合ガイド（製造業者向け）

本適合基準では、
・IoT 製品で使用される重要なセキュリティパラメータが、ソースコードにハードコーディングされていないこと
を要求する。
これらの要求に対して、以下の適合要件１～２のすべてを満たすこと。

適合要件１：
ソースコードにハードコーディングされた機密セキュリティパラメータが一覧化されていること。

適合要件２：
一覧化されたセキュリティパラメータに、IoT 製品の運用中*)に利用される重要なセキュリティパラメータが含まれていないこと。

*)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。開発時や出荷時のテスト、初期設定時、改修・故障解析時などを除くもの。

★3 評価ガイド（製造業者・評価機関向け）

評価機関は、以下の【ドキュメント評価】の結果が「適合（Y)」の場合に限り、本適合要件の評価結果を「適合（Y)」と判断する。

【技術文書】
製造業者は、以下のドキュメントを技術文書として評価機関に提出する。
技術文書１：ソースコードにハードコーディングされている機密セキュリティパラメータの一覧
技術文書２：ソースコードにハードコーディングされている重要なセキュリティパラメータの IoT 製品運用中の有効/無効状態の一覧

【ドキュメント評価】
評価機関は、製造業者から提供された技術文書１，２によって、評価項目１，２の評価を実施する。全ての評価項目の評価結果が「適合（Y)」の場合にのみ、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１に、ソースコードにハードコーディングされた機密セキュリティパラメータが一覧化されていることを確認する。

評価項目２：
技術文書２に記載された重要なセキュリティパラメータが IoT 製品運用中では無効状態になっていることを確認する。

*) IoT 製品の運用期間外とは開発時・製造時や出荷テスト時、故障解析時などである。

適合基準番号 : S3.1-19

★3 適合基準

IoT 製品で使用される重要なセキュリティパラメータのうち、ソフトウェアアップデートの完全性及び真正性チェック、及び付随サービスとの通信の保護に使用される重要なセキュリティパラメータは、IoT 機器毎に固有であること。

対象外（NA）となるための条件、基準の補足説明

【重要なセキュリティパラメータ】

セキュリティに関連する情報であって、その開示または変更が、暗号モジュールのセキュリティを危殆化し得るもの。

（例：共通鍵・秘密鍵・パスワードや PIN などの認証データなど）

★3 評価手法

・ドキュメント評価：

対象とする

・実機テスト：

なし

★3 適合ガイド（製造業者向け）

本適合基準では、

・IoT 製品の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や、付随サービスとの通信の保護に使用される重要なセキュリティパラメータは、製品のクラスに対する自動化された攻撃のリスクを低減するメカニズムで生成されること

を要求する。

これらの要求に対して、以下の適合要件を満たすこと。

適合要件 1 ：

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や、付随サービスとの通信の保護に使用される重要なセキュリティパラメータの生成メカニズムが定められていること。

適合要件２：
生成メカニズムにより、重要なセキュリティパラメータがIoT機器毎に固有であること。

補足：
例えば、「IPAの暗号アルゴリズム確認登録簿」に登録された乱数生成器は、生成メカニズムにおける十分なエントロピー源と見なすことができる。

★3 評価ガイド（製造業者・評価機関向け）

評価機関は、以下の【ドキュメント評価】の結果が「適合（Y)」の場合に限り、本適合基準の評価結果を「適合（Y)」と判断する。

【技術文書】
製造業者は、以下のドキュメントを技術文書として評価機関に提出する。
技術文書１：共通鍵暗号方式に利用される共通鍵、及び公開鍵暗号方式に利用される秘密鍵の生成メカニズムが記載されている仕様書

【ドキュメント評価】
評価機関は、製造業者から提供された技術文書１によって、評価項目１の評価を実施する。評価項目１の評価結果が「適合（Y)」の場合にのみ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１により、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や、付随サービスとの通信の保護に使用される重要なセキュリティパラメータの生成メカニズムが明記されており、IoT機器毎に固有となると判断できる。

適合基準番号：S3.1-20

★3 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以下のすべての保護対策が行われていること。
① IoT製品は守るべき情報資産の送信先の正当性を確認する。
② IoT製品が保護されたネットワーク以外のネットワークを介して守るべき情報資産を通信する場合は、IoT製品が自ら情報の盗聴・改ざんに対する保護対策を行う。
③ IoT製品が保護されたネットワークのみを介して守るべき情報資産を通信する場合

は、IoT 製品自ら情報の改ざんに対する保護対策を行う。

対象外（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

・ログ（テレメトリデータ・監査ログ）

・プログラムコード（ソフトウェア）

・IoT 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

【用語定義：保護されたネットワーク】

以下のネットワーク：

・VPN 環境

・専用線を経由した接続環境

・物理的／論理的に保護されたネットワーク環境

★3 評価手法

・ドキュメント評価：

対象とする

・実機テスト：

対象とする

★3 適合ガイド（製造業者向け）

本適合基準では、

・伝送される守るべき情報資産について、情報の盗聴・改ざんに対する保護対策が実装されていること

を要求する。

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する。

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の情報の盗聴・改ざんに対する保護対策は、以下の適合要件１～３のすべてを満たしていること。ただし、守るべき情報資産を送受信する通信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。

適合要件１：

IoT 機器が、適切な認証によって通信先の正当性を確認すること。
適合要件２：
IoT 機器が守るべき情報資産を送受信する通信が、保護された通信環境以外を経由するか否かによって以下の適合要件２－１又は適合要件２－２を満たすこと。
適合要件２－１：
IoT 機器が守るべき情報資産を送受信する通信が、保護された通信環境以外を経由する場合においては、以下の A)、B）のいずれかの対策が取られること。
A）CRYPTREC で認められた暗号技術*)を採用した通信プロトコルにて伝送すること。
B)「★1 適合基準 S3.1-16」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。
適合要件２－２：
IoT 機器が守るべき情報資産を送受信する通信が、保護された通信環境のみを経由する場合においては、保護された通信環境においてのみ使用するようユーザ向けに明示していること、ならびに、以下の C)、D）のいずれかの対策が取られること。
C)CRYPTREC で認められた暗号技術*)を採用した通信プロトコルにて伝送すること。
D)CRYPTREC で認められた暗号技術*)を採用したメッセージダイジェスト、電子署名により守るべき情報資産の改ざんを防止する、又は、CRC コード等により守るべき情報資産の改ざんを防止すること。
適合要件３：
情報の盗聴・改ざん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。

*)CRYPTREC で認められた暗号技術:
「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

★3 評価ガイド（製造業者・評価機関向け）
評価機関は、以下の【ドキュメント評価】及び【実機テスト】の結果が「適合（Y)」の場合に限り、本適合基準の評価結果を「適合（Y)」と判断する。

【技術文書】
製造業者は、以下の技術文書を評価機関に提出する。
技術文書１：IoT 製品の伝送される守るべき情報資産のリスト
技術文書１に含まれるすべての守るべき情報資産について、技術文書２、及び、必要に

応じて技術文書３，４を提出する。
技術文書２：守るべき情報資産の通信の仕様が記載された文書であり、適合要件１～３に適合することの根拠が記載されている文書
技術文書３：(通信経路が保護された通信環境だけを経由する場合のみ）通信を保護された通信環境においてのみ使用することが記載された文書（ユーザに提供する文書）
技術文書４：(通信経路が保護された通信環境だけを経由する場合であって、技術文書３がユーザに未提供である場合のみ）技術文書３をユーザに提供する計画が記載されている文書

【ドキュメント評価】
評価機関は、技術文書１に記載された全ての守るべき情報資産の通信について、評価項目１～５の評価を実施する。全ての評価結果が「適合（Y)」の場合にのみ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２に、IoT 機器は適切な認証に基づいて通信先の正当性を確認する実装であることが明記されていることを確認する。
評価項目２：
通信経路が保護された通信環境だけを経由しない場合、技術文書２に、適合要件２の A)または B)を満たす実装であることが明記されていることを確認する。
評価項目３：
通信経路が保護された通信環境だけを経由する場合、技術文書２に、適合要件２の C)または D)を満たす実装であることが明記されていることを確認する。
評価項目４：
通信経路が保護された通信環境だけを経由する場合、技術文書３がユーザに提供されること、又は、ユーザに未提供の場合は技術文書４に提供される計画が明記されていることを確認する。
評価項目５：
技術文書２に、情報の盗聴・改ざん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記されていることを確認する。

【実機テスト】
評価機関は、技術文書１に記載されたすべての守るべき情報資産の通信について、全ての通信が保護されていることを実機テストにより評価する。以下の評価項目６、７の全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６：

守るべき情報資産を通信する通信において使用する暗号技術が CRYPTREC で認められた暗号技術*)であることを確認する。TLS 通信においては、CRYPTREC で認められていない暗号技術が使用できないことを確認する。
ただし、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）においてのみ使用する IoT 機器の場合で、改ざん防止に CRC コードなど CRYPTREC 暗号リストに記載の暗号以外の技術を使用する場合は本評価項目の対象外とする。
評価項目 7 ：
情報の盗聴・改ざん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を確認する。

*)CRYPTREC で認められた暗号技術:
「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

適合基準番号 : S3.1-21

★3 適合基準

IoT 製品で利用する重要なセキュリティパラメータの生成・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ること。

対象外（NA）となるための条件、基準の補足説明

【重要なセキュリティパラメータ】
セキュリティに関連する情報であって、その開示または変更が、暗号モジュールのセキュリティを危殆化し得るもの。
（例：共通鍵・秘密鍵・パスワードや PIN などの認証データなど）

★3 評価手法

・ドキュメント評価：
対象とする
・実機テスト：
なし

★3 適合ガイド（製造業者向け）

本適合基準では、
・IoT 製品で利用する重要なセキュリティパラメータの生成・配布・保管・更新・廃棄・失効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ることを要求する。
これらの要求に対して、以下の適合要件を満たすこと。

適合要件１：
IoT 製品で利用する重要なセキュリティパラメータについて、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に明示すること。

【補足１：重要なセキュリティパラメータのライフサイクル・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。

★3 評価ガイド（製造業者・評価機関向け）
評価機関は、以下の【ドキュメント評価】の結果が「適合（Y)」の場合に限り、本適合基準の評価結果を「適合（Y)」と判断する。

【技術文書】
製造業者は、以下のドキュメントを技術文書として評価機関に提出する。
技術文書１：IoT 製品で利用する重要なセキュリティパラメータの一覧
技術文書２：IoT 製品で利用する重要なセキュリティパラメータの管理プロセスが規定された文書

【ドキュメント評価】
評価機関は、製造業者から提供された技術文書１，２によって、評価項目１の評価を実施する。全ての評価項目の評価結果が「適合（Y)」の場合にのみ、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１に記載された重要なセキュリティパラメータについて、技術文書２に、生成・配布・保管・更新・廃棄・失効の各ライフサイクルで、アクセスコントロールや権限分離、暗号化による保護、システム的な対応等によるセキュアな管理プロセスが規定されていることを確認する。
セキュアな管理プロセスの例：

１）生成（Generation）
・安全な方法で生成する：信頼できる乱数生成器（CSPRNG）を使用する。
・属性設定：種類（対称鍵／非対称鍵／PIN／パスワード)、用途（暗号化／署名／認証など)、有効期間などを定義する。
２）登録・配布（Registration & Distribution）
・登録の管理：生成されたデータを CKMS（暗号鍵管理システム）等に登録し、メタ情報（ID、用途、有効期限など）を付与する。
・安全な配布：安全なチャネル（例えば TLS、ハードウェアセキュリティモジュール）を通じて、利用者やシステムに重要なセキュリティパラメータを配布する。
３）保管（Storage）
・安全な場所に保管する：例えば、HSM（Hardware Security Module）や暗号化されたストレージに保存する。
・バックアップを行う：災害対策として、暗号化されたバックアップを安全な場所に保管する。
・アクセスログを残し、監査可能な状態にする。
４）更新（Update）
・定期的な更新：有効期間が終了する前に新しい重要なセキュリティパラメータを生成・配布し、定期的な更新を行う。
・影響範囲の確認：更新による影響（データ再暗号化など）を事前に評価し更新方法を決定する。
５）破棄（Destruction）
・完全な削除：復元不可能な方法で破棄（例：ゼロ化、物理破壊)。
・記録保持：破棄の日時、方法、責任者などを記録する。破棄処理のログを残し、監査可能な状態にする。
６）失効（Revocation）
・失効理由の管理：漏洩、使用終了、ポリシー変更など。
・通知と対応：関係者への通知、代替データの配布、再暗号化、サービスの停止、製品の破棄などの対応が必要。

適合基準番号 : S3.1-22

★3 適合基準

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】
IoT 製品において、無線 LAN 機能を持たない。

★3 評価手法

・ドキュメント評価：
対象とする
・実機テスト：
なし

★3 適合ガイド（製造業者向け）

本適合基準では、
IoT 製品において無線 LAN 機能をもつ場合、適切な方式による無線通信の暗号化、及び 802.1X による機器認証を行う機能を実装すること
を要求する。
IoT 製品の無線通信の暗号化機能は、以下の適合要件 1 を満たすこと
適合要件 1 ：
利用される無線通信のセキュリティ規格が、WPA3 Enterprise（Wi-Fi Protected Access 3 Enterprise)、または WPA2 Enterprise（Wi-Fi Protected Access 2 Enterprise）方式をサポートしていること。
IoT 製品の 802.1X による機器認証機能は、以下の適合要件 2 を満たすこと
適合要件 2 ：
IEEE 802.1X 認証で用いる EAP（PPP Extensible Authentication Protocol）の規格が TLS、TTLS、PEAP、または EAP-FAST の認証方式をサポートしていること。

＜補足説明＞
本セキュリティ要件は政府機関等の対策基準策定のためのガイドライン（令和 7 年度版）6.4.3(1)-1 に準拠する。

★3 評価ガイド（製造業者・評価機関向け）

評価機関は、以下の【ドキュメント評価】の結果が「適合（Y)」の場合に限り、本適合要件の評価結果を「適合（Y)」と判断する。

【技術文書】
製造業者は、以下の技術文書を評価機関に提出する。
技術文書 1 ：無線通信のセキュリティ規格が記載された文書
技術文書 2 ：無線通信における機器認証方式が記載された文書

【ドキュメント評価】

評価機関は、評価項目１、２の評価を実施する。すべての評価結果が「適合（Y)」の場合にのみ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１に記載されたセキュリティ規格に、WPA3 Enterprise（Wi-Fi Protected Access 3 Enterprise)、または WPA2 Enterprise（Wi-Fi Protected Access 2 Enterprise）が含まれていることを確認する。

評価項目２：

技術文書２に、802.1X 認証で用いる EAP の規格が TLS、TTLS、PEAP、または EAP-FAST の認証方式をサポートしていることが明記されていることを確認する。

適合基準番号 : S3.1-23

★3 適合基準

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

―

★3 評価手法

・ドキュメント評価：

対象とする

・実機テスト：

対象とする

★3 適合ガイド（製造業者向け）

本適合基準では、

・IoT 製品で利用するすべてのインタフェースを洗い出し、利用目的等を明確化すること

・IoT 製品の利用上不要なものが含まれていないこと

・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

を要求する。

これらの要求に対して、以下の適合要件 1 ～5 のすべてを満たすこと。

適合要件 1 ：

IoT 製品が利用する TCP/UDP ポート、Bluetooth プロファイル、USB クラスについて、A)～C)を満たすこと

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。

適合要件 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、「物理的に無効化しているインタフェースはない。」ことを明確にすること。

適合要件 3 ：

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。
適合要件 4 ：
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ないこと
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ないこと
[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
適合要件 5 ：
適合要件 4 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
- 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

★3 評価ガイド（製造業者・評価機関向け）
評価機関は、以下の【ドキュメント評価】及び【実機テスト】の結果が「適合（Y)」の場合に限り、本適合基準の評価結果を「適合（Y)」と判断する。
【技術文書】
製造業者は、以下の技術文書を評価機関に提出する。
技術文書 1 ：IoT 製品が利用する TCP/UDP ポート、Bluetooth プロファイル、USB

クラスのリスト
それぞれの TCP/UDP ポート、Bluetooth プロファイル、USB クラスについて適合要件 1 を満たす根拠が記載されていること
技術文書 2 ：物理的に無効化しているインタフェースのリスト
全ての物理的に無効化しているインタフェースについて、物理的無効化の方法が記載されていること。
そのようなインタフェースが存在しない場合は、存在しないことが明記されている文書。
技術文書 3 ：製造業者が攻撃に悪用されるリスクが特に高いと判断したポート（例えば telnet（23/TCP 及び 2323/TCP）等）のリスト。そのようなポートが存在しない場合は、存在しないことが明記されている文書。
技術文書 4 ：製造業者が攻撃に悪用されるリスクが特に高いと判断したポートの攻撃状況を把握し、必要に応じて適切な対処ができる管理プロセスを規定した文書（製造業者が攻撃に悪用されるリスクが特に高いと判断したポートが存在する場合のみ）
技術文書 5 ：残存脆弱性のリスト。全ての残存脆弱性について、セキュリティ上問題ないと判断した理由が明記されていること
※残存脆弱性は、脆弱性検査などによって存在することが確認されたが、製造業者が IoT 製品の利用においてセキュリティ上問題ないため修正せず保持することと判断した脆弱性である。

【ドキュメント評価】
評価機関は、製造業者から提供されたドキュメント(技術文書）によって、IoT 製品の全てのインタフェースを特定する。特定したそれぞれのインタフェースについて、評価項目 1 ～ 5 の評価を実施する。全ての評価結果が「適合（Y)」の場合にのみ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 1 に、インタフェースの利用目的、利用条件が明記されていることを確認する。
評価項目 2 ：
技術文書 1 にて、インタフェースが TCP/UDP ポート、Bluetooth、又は USB ポートである場合、それぞれ、以下の条件を満たすことを確認する。
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、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３：
インタフェースのうち、物理的に無効化しているインタフェースがある場合は、技術文書２に無効にしているインタフェース及び無効化の方法を明記していることを確認する。
そのようなインタフェースがなければ、技術文書２に、「物理的に無効化しているインタフェースはない。」ことが明記されていることを確認する。
評価項目４：
技術文書３で、攻撃に悪用されるリスクの特に高いポートの利用の有無を確認する。
攻撃に悪用されるリスクの特に高いポートを利用している場合には、技術文書４に、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規定していることを確認する。
そのようなポートを利用していなければ、技術文書３に、「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。」ことを明記していることを確認する。
評価項目５：
技術文書５にて、全ての残存脆弱性について、以下の観点で、問題ないと判断した理由が妥当であることを確認する。
- 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

【実機テスト】
評価機関は、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６～８の全てを満たしていることが確認できた場合に限り、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６：

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。技術文書１に記載されている以外のポートが全て無効化されていることを確認する。技術文書２で開放していると明記されていない TCP／UDP ポートが検知されなければ本評価項目は「適合（Y)」、一つでも検知されれば本評価項目は「非適合（N)」となる。

評価項目７：

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「適合（Y)」、確認できなければ「非適合（N)」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８を実施する。評価項目７が「適合（Y)」となった場合は、評価項目８も「適合（Y)」となる。

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、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]：https://nvd.nist.gov/vuln/search

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：

技術文書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：

技術文書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８：

評価項目７の i)、ii）のいずれか条件において残存脆弱性が検出された場合、検出されたすべての残存脆弱性が、技術文書５に記載された残存脆弱性に含まれていることを確認する。

技術文書５に含まれない残存脆弱性が一つでもある場合は、本評価項目は「非適合

（N)」となる。

適合基準番号 : S3.1-24

★3 適合基準

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ていること。

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、基準の補足説明

―

★3 評価手法

・ドキュメント評価：
対象とする
・実機テスト：
対象とする

★3 適合ガイド（製造業者向け）

本適合基準では、
・初期化状態において、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セキュリティ関連情報が最小化されていること
を要求する。
この要求に関して、以下の適合要件 1 を満たすこと。

適合要件 1 ：
初期設定及び認証なしで開示されているすべてのセキュリティ関連情報の一覧および開示理由（開示されたセキュリティ関連情報が製品の動作上必要である理由）を IoT 製品の技術文書に明示すること。

★3 評価ガイド（製造業者・評価機関向け）

評価機関は、以下の【ドキュメント評価】及び【実機テスト】の結果が「適合（Y)」の場合に限り、本適合基準の評価結果を「適合（Y)」と判断する。

【技術文書】
製造業者は、以下のドキュメントを技術文書として評価機関に提出する。
技術文書１：ネットワークインタフェースにアクセスした際に非認証状態で表示されるセキュリティ関連情報とその開示理由が記載された一覧

【ドキュメント評価】
評価機関は、製造業者から提供された技術文書１によって、評価項目１の評価を実施する。評価項目の評価結果が「適合（Y)」の場合にのみ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１の一覧に全ての開示されるセキュリティ関連情報、およびその開示理由が明記されていることを確認する。

【実機テスト】
評価機関は、実機テストにより評価項目２の評価を実施する。評価項目の結果が「適合（Y)」の場合にのみ本適合基準の評価結果が「適合（Y)」となる

評価項目２：
技術文書１の一覧にあるセキュリティ関連情報が認証なしで確認できること、及び一覧に無いセキュリティ関連情報は認証なしで一切開示されないことを確認する。

適合基準番号 : S3.1-25

★3 適合基準

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ること。

①IoT 機器の不必要な物理的インタフェースは、露出から保護する仕組みを有すること。
②IoT 機器のデバッグインタフェースを物理的また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、基準の補足説明

―

★3 評価手法

・ドキュメント評価：
対象とする
・実機テスト：
対象とする

★3 適合ガイド（製造業者向け）

本適合基準では、
・IoT 機器において、不必要なインタフェースが無効化されていること
を要求する。
この要求に関して、以下のすべての適合要件を満たすこと。

適合要件 1 ：
不必要な物理インタフェースは、外部露出から保護する仕組みを有すること。
適合要件 2：
JTAG、UART 等のデバッグインタフェースは物理的または論理的に無効化されていること。
【補足 1 ：物理インタフェースの保護の例】
・機器への電力供給のみに使用される予定の USB ポートは、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されている。（データ通信に利用される信号線を物理的に無効化する）

【補足 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
…など

【補足 3 ：デバッグインタフェースの無効化の例】
・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。
・出荷後も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する。

・製造業者のメンテナンスにおける一時的なデバックインタフェースの無効化の解除を妨げるものではない。

【補足４：物理的保護の例外事項】
・機器の設置環境が、セキュリティエリア(*1)への設置を前提としている場合、その旨の注意をユーザに明示することを条件に、適合要件１．２を満たしているとみなす。

(*1)：物理的セキュリティに配慮された施設内の共用エリア以外の区画

【補足５：不必要な物理的インタフェースの定義】
・IoT 機器として、恒久的に使用されない物理的インタフェースのこと

★3 評価ガイド（製造業者・評価機関向け）

評価機関は、以下の【ドキュメント評価】及び【実機テスト】の結果が「適合（Y)」の場合に限り、本適合要件の評価結果を「適合（Y)」と判断する。

【技術文書】
製造業者は、以下の技術文書を評価機関に提出する。
技術文書１：物理インタフェースの物理的配置が判別できる筐体設計図
技術文書２：JTAG、UART 等のデバッグインタフェースが出荷時に無効化されることが記載されている文書
技術文書３：搭載されているすべての物理インタフェースの利用目的

【ドキュメント評価】
評価機関は、製造業者から提供されたドキュメント(技術文書）によって、評価項目１,２の評価を実施する。評価項目１,２の全ての評価結果が「適合（Y)」の場合にのみ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１にて、技術文書３に記載されている利用目的のない不必要な物理インタフェースは、外部露出していないことを確認する。
評価項目２：
技術文書２に、JTAG、UART 等のデバッグインタフェースは物理的（*1）または論理的（*2）に無効化されていることが明記されていることを確認する。

【実機テスト】

評価機関は、実機テストにより評価項目３，４の評価を実施する。全ての評価項目の結果が「適合（Y)」の場合にのみ本適合基準の評価結果が「適合（Y)」となる

評価項目３：
技術文書３に利用目的が記載されていない物理インタフェースは、外部露出から保護されていることを目視にて確認する。

評価項目４：
論理的に無効化されているデバックインタフェースが存在する場合、そのデバッグインタフェースに対してコマンドまたはデバッグ操作が行えないことを確認する。

（*1)：物理的無効化の例
・ 強化されたエンクロージャ（筐体に高強度の素材を使用すること）
・ 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)：論理的無効化の例
・強固なパスワード(要件 1-2 を参照)や多要素認証(要件 1-8 を参照)等によるアクセスコントロール
・ソフトウェアによる論理的無効化

適合基準番号 : S3.1-26

★3 適合基準

製造業者は、IoT 製品の設計および実装において、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すること。

対象外（NA）となるための条件、基準の補足説明

―

★3 評価手法

・ドキュメント評価：
対象とする
・実機テスト：
対象とする

★3 適合ガイド（製造業者向け）

本適合基準では、

・IoT 機器において、必要とされるサービスのみが有効であること

を要求する。

この要求に関して、以下の全ての適合要件を満たすこと。

適合要件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)、およびそのサービスが対象 IoT 機器の意図された使用または操作に必要最小限であること。

適合要件２：

IoT 機器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（NTP の monlist コマンド, DNS ANY リクエスト, UPnP の SSDP など）に応答しないこと。

※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。NTP の monlist 機能を無効化（disable）する。DNS のオープンリゾルバを停止する。UPnP 機能を停止するなどにより対策していること。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。

適合要件３：

LAN および 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。

補足)：運用上、制限された環境下で、必要に応じて、有効化することを妨げない。

★3 評価ガイド（製造業者・評価機関向け）

評価機関は、以下の【ドキュメント評価】及び【実機テスト】の結果が「適合（Y)」の場合に限り、本適合基準の評価結果を「適合（Y)」と判断する。

【技術文書】

製造業者は、以下の技術文書を評価機関に提出する。

技術文書１：デフォルトで有効となる全てのサービス（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）と設定、その役割（必要性）について記載されている仕様書

【ドキュメント評価】

評価機関は、製造業者から提供された技術文書 1 によって、評価項目 1 , 2 の評価を実施する。評価項目 1 , 2 の全ての評価結果が「適合（Y)」の場合にのみ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 1 に記載されている全てのサービスが、対象 IoT 製品の意図された使用または操作に必要最小限であることを確認する。

評価項目 2 ：
技術文書 1 に記載されたサービスのうち、IoT 製品がサービス不能攻撃の踏み台として利用されるサービスにおいて、リクエスト（NTP の monlist コマンド, DNS ANY リクエスト, UPnP の SSDP など）に応答しない設定もしくは対策がされていることを確認する。

【実機テスト】
評価機関は、実機テストにより評価項目 3 の評価を実施する。また、評価項目 4 の不要なサービスポートの無効化について、要件 16-3 の実機テスト結果により評価する。評価項目の結果が「適合（Y)」の場合にのみ本適合基準の評価結果が「適合（Y)」となる。

評価項目 3：
IoT 製品がサービス不能攻撃の踏み台として利用される代表的なリクエスト（NTP の monlist コマンド, DNS ANY リクエスト, UPnP の SSDP など）に応答しないこと。応答により確認できない場合は、対策済のバージョンであることの確認を行う。

評価項目 4 ：
対象製品で使用を前提としないが、標準で具備されている LAN 及び WAN インタフェースのサービスが、不要である場合に、ポートスキャンにて無効化されていることの確認を行う。
【主なサービス例】
A) SSH
B) NAT-PMP
C) PCP
D) Remote Administration
E) SNMP
F) Telnet

G) UPnP
H) VoIP
I)CWMP

適合基準番号 : S3.1-27

★3 適合基準

製造業者は、IoT 製品に展開されるソフトウェアの実装およびテストにおいて、コード最小化のための手法を採用すること。

対象外（NA）となるための条件、基準の補足説明

―

★3 評価手法

・ドキュメント評価：
対象とする
・実機テスト：
なし

★3 適合ガイド（製造業者向け）

本適合基準では、
・セキュリティリスクの軽減のため、コード最小化手法を採用していること
を要求する。
この要求に関して、以下の適合要件 1 , 2 を満たすこと。

適合要件 1 ：
コードの最小化を行うため、製品特性に併せて、以下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。

適合要件 2 ：
IoT 製品に実装されている機能一覧を技術文書に明示すること。

★3 評価ガイド（製造業者・評価機関向け）

評価機関は、以下の【ドキュメント評価】の結果が「適合（Y)」の場合に限り、本適合基準の評価結果を「適合（Y)」と判断する。

【技術文書】

製造業者は、以下の技術文書を評価機関に提出する。

技術文書１：コードの最小化に関するプロセスが規定されている文書

技術文書２：IoT 製品の機能の一覧が記載されている文書

【ドキュメント評価】

評価機関は、製造業者から提供された技術文書１，２によって、評価項目１,２の評価を実施する。評価項目１,２の全ての評価結果が「適合（Y)」の場合にのみ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：

コードの最小化を行うため、以下のいずれかに類する手法又はそれ以上の手法を採用していることを確認する。

A）自動化ツールを使用して、デッド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。

評価項目２：

IoT 製品の機能について網羅的に記載されたドキュメントが存在することを確認する。

適合基準番号：S3.1-28

★3 適合基準

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および実装を行っていること。具体的には、以下の基準を満たすこと。

①デフォルト権限の最小化

ユーザがデバイスを初めて使用する際に、不必要に広範な権限が付与されないようデフォルトの権限設定を必要最小限に留めること。

対象外（NA）となるための条件、基準の補足説明

【用語定義：ユーザ】

ユーザの対象範囲には、IoT 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

★3 評価手法

・ドキュメント評価：
対象とする
・実機テスト：
なし

★3 適合ガイド（製造業者向け）

本適合基準では、
・製品のデフォルト権限の最小化および権限管理機能の実装が実現されていること
を要求する。
この要求に関して、以下のすべての適合要件を満たすこと。

適合要件１：
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。
以下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。
―

★3 評価ガイド（製造業者・評価機関向け）

評価機関は、以下の【ドキュメント評価】の結果が「適合（Y)」の場合に限り、本適合基準の評価結果を「適合（Y)」と判断する。

【技術文書】
製造業者は、以下の技術文書を評価機関に提出する。
技術文書１：デフォルト権限の最小化および権限管理機能について記載された文書

【ドキュメント評価】
評価機関は、製造業者から提供された技術文書１によって、評価項目１の評価を実施す

る。評価項目１の評価結果が「適合（Y)」の場合にのみ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：
デーモン／プロセスなどのデフォルトの権限が、必要最低限となるように設定されることが明記されていることを確認する。

適合基準番号 : S3.1-29

★3 適合基準

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すること。具体的には、最低限以下の実施を含む。
①セキュリティに配慮したコーディング規約や実装原則を規程する
②コーディング規約を技術者に周知し教育を行う
③作成されたコードのレビュー・セキュリティテストを行う
④コーディング規約や実装原則を更新する

対象外（NA）となるための条件、基準の補足説明

―

★3 評価手法

・ドキュメント評価：
対象とする
・実機テスト：
なし

★3 適合ガイド（製造業者向け）

本適合基準では、
・セキュアな開発プロセスに沿って製品に展開されるソフトウェアの実装が行われていること
を要求する。
この要求に関して、以下のすべての適合要件を満たすこと。

適合要件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。

適合要件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。

適合要件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プロセスが存在すること。

適合要件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。
【補足１：セキュアな開発プロセスの例】
IPA が発行する「脆弱性対処に向けた製品開発者向けガイド」「IoT 開発におけるセキュリティ設計の手引き」等が参考となる。

★3 評価ガイド（製造業者・評価機関向け）
評価機関は、以下の【ドキュメント評価】の結果が「適合（Y)」の場合に限り、本適合基準の評価結果を「適合（Y)」と判断する。

【技術文書】
製造業者は、以下の技術文書を評価機関に提出する。
技術文書１：コーディング規約もしくはコードの実装原則が規定された技術文書
技術文書２：コーディング規約もしくはコードの実装原則を技術者に教育するプロセスが規定された技術文書
技術文書３：コードレビューのプロセスが規定された技術文書
技術文書４：コーディング規約もしくはコードの実装原則を更新するプロセスが規定された技術文書

【ドキュメント評価】
評価機関は、製造業者から提供された技術文書１～４によって、評価項目１～４の評価を実施する。全ての評価項目の評価結果が「適合（Y)」の場合にのみ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：
公表されているセキュリティに配慮したコーディング規約や実装原則等のベストプラクティスを参考に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。

評価項目２：

コーディング規約や実装原則等を技術者に周知し教育するプロセスが存在していることを確認する。

評価項目３：
IoT 製品に実装されたコードがコーディング規約や実装原則等に準拠しているかを確認するコードレビューのプロセスが存在していることを確認する。

評価項目４：
規定されたコーディング規約や実装原則等を更新するプロセスが存在することを確認する。

適合基準番号 : S3.1-30

★3 適合基準

IoT 製品にサードパーティコンポーネントを組み込む際に、既知の脆弱性が含まれないよう、以下の基準①・②の全てを満たすプロセスを採用していること。

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、基準の補足説明

【NA となるための条件】
対象の IoT 製品においてサードパーティコンポーネントを使用していない（「NA であることの理由」に、サードパーティコンポーネントを使用していないことを明示すること）

★3 評価手法

・ドキュメント評価：
対象とする
・実機テスト：
なし

★3 適合ガイド（製造業者向け）

本適合基準では、

・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、既知の脆弱性が存在する可能性を低減するプロセスを採用していること。
を要求する。
この要求に関して、以下のすべての適合要件を満たすこと。

適合要件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ついて、脆弱性を管理するプロセスが規定されていること。以下はプロセスの例となる。
A）サードパーティからソースコードが提供された場合に、静的アプリケーションセキュリティテスト（SAST）を実施する。
B）サードパーティコンポーネントを含む SBOM を作成し、ソフトウェア構成分析（SCA）を実施する。
C）サードパーティコンポーネントについて、サードパーティから脆弱性情報を入手することを契約により保証する。
D) CVE など公開された脆弱性情報を収集するツールまたはサービスを利用する。

適合要件２：
発見された既知の脆弱性の対処を行うプロセス（サードパーティから提供されたパッチを適用するフローなど）が規定されていること。

★3 評価ガイド（製造業者・評価機関向け）
評価機関は、以下の【ドキュメント評価】の結果が「適合（Y)」の場合に限り、本適合基準の評価結果を「適合（Y)」と判断する。

【技術文書】
製造業者は、以下の技術文書を評価機関に提出する。
技術文書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ついて、脆弱性を管理するプロセスが規定された文書

【ドキュメント評価】
評価機関は、製造業者から提供された技術文書１によって、評価項目１,２の評価を実施する。全ての評価項目の評価結果が「適合（Y)」の場合にのみ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：
サードパーティコンポーネントに既知の脆弱性が存在する可能性を低減するようなプロ

セスが明記されていることを確認する。

評価項目２：
脆弱なサードパーティコンポーネントや古いサードパーティコンポーネントにパッチを適用するためのプロセスが明記されていることを確認する。

適合基準番号 : S3.1-31

★3 適合基準

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すること。
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うこと。

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、基準の補足説明

―

★3 評価手法

・ドキュメント評価：
対象とする
・実機テスト：
なし

★3 適合ガイド（製造業者向け）

本適合基準では、
・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を行うセキュアブートのメカニズムが実装されていること
を要求する。
この要求に関して、以下のすべての適合要件を満たすこと。

適合要件１：
デジタル署名などの検証により、セキュアブートメカニズムが実装されていること。

適合要件２：

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

【補足１：セキュアブートに求める範囲】

セキュアブートに求める範囲として、真正性の検証のためのセキュアブートメカニズムの実装は求めない。

★3 評価ガイド（製造業者・評価機関向け）

評価機関は、以下の【ドキュメント評価】の結果が「適合（Y)」の場合に限り、本適合基準の評価結果を「適合（Y)」と判断する。

【技術文書】

製造業者は、以下の技術文書を評価機関に提出する。

技術文書１：セキュアブートのメカニズム（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を検証するメカニズム）が記載された仕様書

【ドキュメント評価】

評価機関は、製造業者から提供された技術文書１によって、評価項目１,２の評価を実施する。全ての評価項目の評価結果が「適合（Y)」の場合にのみ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：

デジタル署名やハッシュ値などの検証により、セキュアブートメカニズムが実装されていること。

評価項目２：

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

適合基準番号 : S3.1-32

★3 適合基準

製造業者は、IoT 機器がセンシングを行う場合に、以下の基準を満たす対応を行うこと。

①センシングする情報について、収集の目的およ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、基準の補足説明

【NA となるための条件】

通信機器がセンシングを行わない場合

★3 評価手法

・ドキュメント評価：

対象とする

・実機テスト：

なし

★3 適合ガイド（製造業者向け）

本適合基準では、

・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 機器のセンシング情報に関する情報提供をすること

を要求する。

IoT 機器のセンシング情報に関する情報提供は、以下の適合要件を満たしていること

適合要件１：

センシングを行う情報の種別、収集の目的や機能が明記されていること。

適合要件２：

適合要件１の記載がユーザにとって明確であること。

★3 評価ガイド（製造業者・評価機関向け）

評価機関は、以下の【ドキュメント評価】の結果が「適合（Y)」の場合に限り、本適合基準の評価結果を「適合（Y)」と判断する。

【技術文書】

製造業者は、以下の技術文書を評価機関に提出する。

技術文書１：ユーザマニュアル（ユーザに提供されることが明確な文書やウェブサイト）

【ドキュメント評価】

評価機関は、製造業者から提供されたドキュメント（ユーザマニュアル等）によって、評価項目１,２の評価を実施する。評価結果が「適合（Y)」の場合にのみ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 機器のセンシング情報について、センシングを行う情報の種別、収集の目的や機能が明記されていることを確認する。
評価項目２：
技術文書１の記載内容について、専門用語等を多用せず平易で理解しやすい表現で示した情報であることを確認する。

適合基準番号 : S3.1-33

★3 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、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。

対象外（NA）となるための条件、基準の補足説明

―

★3 評価手法

・ドキュメント評価：
対象とする
・実機テスト：
対象とする

★3 適合ガイド（製造業者向け）

本適合基準では、
・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 機器に対して、電源供給の停止、及びネットワーク断に対して耐性を持つこと
を要求する。

電源供給の停止、及びネットワーク断に対して耐性を持つことは、以下の適合要件１，２を満たすこと
適合要件１：
IoT 機器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、アップデート状態及び設定値等が維持されていること。
適合要件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、アップデート状態及び設定値等が維持されていること。

★3 評価ガイド（製造業者・評価機関向け）

評価機関は、以下の【ドキュメント評価】及び【実機テスト】の結果が「適合（Y)」の場合に限り、本適合基準の評価結果を「適合（Y)」と判断する。

【技術文書】
製造業者は、以下の技術文書を評価機関に提出する。
技術文書１：IoT 機器の電源供給が停止時のふるまいの仕様（どのような情報が保持されるか、電源復帰後の動作など）を記載した文書
技術文書２：IoT 機器のネットワーク断時のふるまいの仕様（どのような情報が保持されるか、ネットワーク再接続後の動作など）を記載した文書

【ドキュメント評価】
評価機関は、製造業者から提供されたドキュメント(技術文書）によって、評価項目１,２の評価を実施する。評価項目１,２の全ての評価結果が「適合（Y)」の場合にのみ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１に、IoT 機器が電源供給の停止後、電源が復帰した場合に、工場出荷時の初期設定に戻ることなく、電源供給の停止直前の認証値及びアップデートが維持される実装であることが明記されていることを確認する。
評価項目２：
技術文書２に、IoT 機器が通信ケーブルや無線接続が切断し、再接続した場合に、工場出荷時の初期設定に戻ることなく、通信ケーブルや無線接続を切断する直前の認証値及びアップデートが維持される実装であることが明記されていることを確認する。

【実機テスト】
評価機関は、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 機器に対して、実機を用いて評価項目３，４の評価を実施する。以下の評価項目３、４の全ての評価結果が「適合（Y)」の場合にのみ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：
IoT 機器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、電源供給の停止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を確認する。
評価項目４：
通信ケーブルや無線接続を切断する。その後、通信ケーブルや無線接続を再接続した後、工場出荷時の初期状態に戻ることなく、通信ケーブルや無線接続を切断す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を確認する。

適合基準番号 : S3.1-34

★3 適合基準

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有すること。

対象外（NA）となるための条件、基準の補足説明

―

★3 評価手法

・ドキュメント評価：
対象とする
・実機テスト：
対象とする

★3 適合ガイド（製造業者向け）

本適合基準では、
・バックアップ実施機能を有し、バックアップを実施した直前の IoT 機器の設定状態を正しく保持、復元できること
・バックアップ実施機能へのアクセスが管理者のみに許可されていること
を要求する。

これらの要求に関しては以下の適合要件をすべて満たすこと
適合要件１：
バックアップ実施機能を有し、バックアップを実施した直前の構成（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。
適合要件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。
―

★3 評価ガイド（製造業者・評価機関向け）

評価機関は、以下の【ドキュメント評価】および【実機テスト】の結果が「適合（Y)」の場合に限り、本適合基準の評価結果を「適合（Y)」と判断する。

【技術文書】
製造業者は、以下のドキュメントを技術文書として評価機関に提出する。
技術文書１：構成（設定値、認証値等）のバックアップに関する機能仕様書

【ドキュメント評価】
評価機関は、製造業者から提供された技術文書１によって、評価項目１,２の評価を実施する。全ての評価項目の評価結果が「適合（Y)」の場合にのみ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：
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（設定値、認証値等）がバックアップファイルに保存される機能が明記されていることを確認する。
評価項目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が明記されていることを確認する。

【実機テスト】
評価機関は、評価項目３に従ってバックアップ機能が実装されていることを、実機テストにより評価する。以下の評価項目の評価結果が「適合（Y)」の場合にのみ実機テストの評価結果は「適合（Y)」となる。
評価項目３：
バックアップ機能によりバックアップファイルを生成後、工場出荷状態など設定変更した状態から、バックアップ機能を実施した直前の構成に復元できること。

適合基準番号 : S3.1-35

★3 適合基準

IoT 製品から収集したログ（テレメトリデータ・監査ログ）を検証し、セキュリティ上の異常を検知すること。具体的には、以下①～③すべての基準を満たすこと。

①IoT 製品に対し、ログ（テレメトリデータ・監査ログ）の取得機能および保存機能を実装すること。最低でも、ファームウェア（ソフトウェア）又は OS により生成されたログ（テレメトリデータ・監査ログ）を取得・保存する。記録するセキュリティイベントの対象として機器やネットワークの切断（再接続）の記録、ログイン試行（成功時、失敗時）の記録、閾値を越えるログイン試行の記録と、それに対する機器側の対応の記録、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）を取得・保存する機能を有する。

②ログ（テレメトリデータ・監査ログ）は監査に必要な容量を確保し、保存容量を超過した場合には、古い記録から順次上書きするなど、管理上の対策を行う。なお、必要な保存容量については、製品ごとの利用用途を踏まえ、別途検討を行う。

③ログ（テレメトリデータ・監査ログ）上のセキュリティイベントの発生日時を記録するため、時間管理機能を有する。

対象外（NA）となるための条件、基準の補足説明

【用語定義：テレメトリデータ】
製品の使用に関する問題や情報を製造業者が特定するのに役立つ情報を提供することができる機器からのデータを指す。

【用語定義：監査ログ】
ユーザが製品におけるセキュリティ上の異常を検知できるようにするため、製品の処理内容やプロセス、および操作の履歴を、時系列かつ連続的に記録したデータを指す。

★3 評価手法

・ドキュメント評価：
対象とする
・実機テスト：
対象とする

★3 適合ガイド（製造業者向け）

本適合基準では、
・IoT 製品の技術文書において、IoT 製品から収集したログ（テレメトリデータ・監査ログ）を検証するための、セキュリティ上の異常を検知する機能を有すること
を要求する。

ログ（テレメトリデータ・監査ログ）の取得および検証に関しては、以下の適合要件 1～3 のすべてを満たすこと。
適合要件 1：
ログ（テレメトリデータ・監査ログ）の取得機能および保存機能が実装され、取得するログ（テレメトリデータ・監査ログ）には以下すべてのセキュリティイベントが含まれている。
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）閾値を越えるログイン試行の記録と、それに対する機器側の対応の記録
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（監査ログ取得が可能な場合）
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）

適合要件 2：
取得するログ（テレメトリデータ・監査ログ）については監査に必要な容量が仕様定義され、保存容量が超過した場合の管理対策が定められている。
適合要件 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の時間管理機能・時刻ソースによる IoT 機器の時刻同期機能が実装されている。

★3 評価ガイド（製造業者・評価機関向け）
評価機関は、以下の【ドキュメント評価】および【実機テスト】の結果が「適合（Y)」の場合に限り、本適合基準の評価結果を「適合（Y)」と判断する。

【技術文書】
製造業者は、以下のドキュメントを技術文書として評価機関に提出する。

技術文書１：ログ（テレメトリデータ・監査ログ）の取得および保存に関する機能性が記載された仕様書
技術文書２：時刻ソースを用いて IoT 機器の時刻を同期するための機能が記載された文書

【ドキュメント評価】
評価機関は、製造業者から提供されたドキュメント(技術文書）によって、評価項目１～３の評価を実施する。全ての評価項目の評価結果が「適合（Y)」の場合にのみ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１に、ログ（テレメトリデータ・監査ログ）の取得機能および保存機能の実装が明記されていること。取得する監査ログには以下すべてのセキュリティイベントが含まれていることを確認する。
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）閾値を越えるログイン試行の記録と、それに対する機器側の対応の記録
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（監査ログ取得が可能な場合）
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）

評価項目２：
技術文書１に、取得するログ（テレメトリデータ・監査ログ）については監査に必要な容量が仕様定義され、保存容量が超過した場合の管理対策が明示されていること。

評価項目３：
技術文書１に、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の時間管理機能が、技術文書２に時刻ソースを指定して時刻同期を行う機能が実装されていることが明記されていること。

【実機テスト】
評価機関は、実機テストにより評価項目４～６の評価を実施する。評価項目の結果が「適合（Y)」の場合にのみ本適合基準の評価結果が「適合（Y)」となる

評価項目４：
技術文書１に記載されたセキュリティイベントをトリガーするアクションを実行し、ログ（テレメトリデータ・監査ログ）にそれぞれのセキュリティイベントが記録されること。

評価項目５：
収集したログ（テレメトリデータ・監査ログ）において、発生日時が正常に記録されること。

評価項目６：
技術文書２に記載された時刻同期機能を実行して、指定した時刻ソースの値に IoT 機器の時刻が同期されること。

【評価補足１：時間管理機能に関する参考文献】
タイムスタンプの形式のための適切な参考文献は、ISO/IEC 8601:2004 である。一部の場所における夏時間などの定期的なタイムシフトイベントが考慮されるシステムを設計するときは、注意することが望ましい。

適合基準番号 : S3.1-36

★3 適合基準

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

D）ログ（テレメトリデータ・監査ログ）

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

対象外（NA）となるための条件、基準の補足説明

【用語定義：ユーザ】
ユーザの対象範囲には、IoT 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

★3 評価手法

・ドキュメント評価：
対象とする
・実機テスト：
対象とする

★3 適合ガイド（製造業者向け）

本適合基準では、
・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
を要求する。

ユーザに関する情報を削除する機能は、以下の適合要件１～３のすべてを満たしていること。
適合要件１：
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）～D）のすべての情報（データ）を削除するための消去方法を有すること。ただし、ユーザに関する情報であっても、製品特性の維持に必要であり、かつ機器の性能・健全性の保持や確認に必要な情報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署名
D） ログ（テレメトリデータ・監査ログ）
適合要件２：
データごとに用途、保存されるストレージに応じて適切に削除すること
適合要件３：
適合要件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。

★3 評価ガイド（製造業者・評価機関向け）

評価機関は、以下の【ドキュメント評価】及び【実機テスト】の結果が「適合（Y)」

の場合に限り、本適合要件の評価結果を「適合（Y)」と判断する。

【技術文書】
製造業者は、以下の技術文書を評価機関に提出する。
技術文書１：IoT 製品に保存されるユーザに関する情報のリスト
IoT 製品に保存されるユーザに関する情報は、以下に分類される情報はすべてリストに含めること
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
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)。
技術文書１に含まれる全てのユーザに関する情報について、技術文書２、３を提出する。
技術文書２：ユーザに関する情報の削除仕様（削除の方法、削除のレベルなど）を記載した文書
技術文書３：ユーザに関する情報の削除の手順を記載した文書(ユーザに提供する文書)

【ドキュメント評価】
評価機関は、技術文書１に記載された全てのユーザに関する情報について、評価項目１～３の評価を実施する。全てのユーザに関する情報について、評価項目１～３の全ての評価結果が「適合（Y)」の場合にのみ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２に、技術文書１に記載された全てのユーザに関する情報の消去方法が、データの種類、保存するストレージに応じて適切な消去方法を選定したこと、及びその理由が明記されていることを確認する。
評価項目２：
技術文書３に、ユーザに関する情報の消去方法が明記されていることを確認する。
適合要件３：
技術文書３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ることを確認する。

【実機テスト】

評価機関は、技術文書１に記載された全てのユーザに関する情報について、評価項目４、５の評価を実施する。全てのユーザに関する情報について、評価項目４，５の全ての評価結果が「適合（Y)」の場合にのみ実機テストの評価結果は「適合（Y)」となる。

評価項目４：

技術文書３に記載された手順に従って、ユーザに関する情報の削除を行い、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「適合（Y)」、削除できていなければ本評価項目は「非適合（N)」となる。

評価項目５：

評価項目４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「適合（Y)」、確認できなければ本評価項目は「非適合（N)」となる。

適合基準番号：S3.1-37

★3 適合基準

IoT 機器は、安全なデフォルト構成設定に復元できること。

対象外（NA）となるための条件、基準の補足説明

―

★3 評価手法

・ドキュメント評価：

対象とする

・実機テスト：

対象とする

★3 適合ガイド（製造業者向け）

本適合基準では、

・保守要員または管理者によって、機器を安全なデフォルト構成設定に復元できる機能を有すること

を要求する。

デフォルト構成設定機能に復元できる機能は、以下の適合条件のすべてを満たしていること

適合条件１：

技術文書に、デフォルト構成設定に復元できる機能に関する記載があること

適合条件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

適合要件３：

デフォルト構成設定への復元が実施された場合、復元以前のユーザに関する情報は適合基準 11-1 と同等のレベルで削除されること。

★3 評価ガイド（製造業者・評価機関向け）

評価機関は、以下の【ドキュメント評価】及び【実機テスト】の結果が「適合（Y)」の場合に限り、本適合要件の評価結果を「適合（Y)」と判断する。

【技術文書】

製造業者は、以下の技術文書を評価機関に提出する。

技術文書１：デフォルト構成設定に復元出来る機能仕様を記載した文書

技術文書２：デフォルト構成設定に復元出来る手順を記載した文書(ユーザに提供する文書)

【ドキュメント評価】

IoT 製品の技術文書を閲覧することで、製品を安全なデフォルト構成設定に復元できる機能が実装されていることを評価する。以下の評価項目１～３のすべてについて確認できた場合に限り、本適合基準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：

機器を安全なデフォルト構成設定に復元できる機能に関する技術文書があること。

評価項目２：

機器を安全なデフォルト構成設定に復元できる手順がマニュアル等にて閲覧可能であること

評価項目３：

機器を安全なデフォルト構成設定に復元できる機能によってユーザ情報が適合基準 11-

1 と同等のレベルで削除されること。

【実機テスト】
製品を安全なデフォルト構成設定に復元できる機能が、閲覧可能な手順によって、正常に動作することを評価する。以下の評価項目４、５の両方について、安全なデフォルト構成設定に復元できることを確認するテストを行い、確認できた場合に限り、本適合基準の実機テストの評価結果は「適合（Y)」となる。

評価項目４：
安全なデフォルト構成設定に復元できる手順において、工場出荷状態に復元できていることを確認する。

評価項目５：
安全なデフォルト構成設定に復元できる手順において、実際にユーザのデータが削除されていることを確認する。

適合基準番号 : S3.1-38

★3 適合基準

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すること。

対象外（NA）となるための条件、基準の補足説明

―

★3 評価手法

・ドキュメント評価：
対象とする
・実機テスト：
対象とする

★3 適合ガイド（製造業者向け）

本適合基準では、
・すべてのインタフェースについて、入力データの妥当性検証機能および不正な要求の拒否機能が動作していること
を要求する。

この要求に関して、以下のすべての適合要件を満たすこと。

適合要件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ことのリスト。一覧には少なくとも以下が一覧化されていること。
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

適合要件２：
適合要件１で一覧化されたインタフェース毎に、入力データの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ること。
A）正しいタイプ
B）許可された値
C）許可された基数
D）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

適合要件３：
IoT 製品において入力検証（Validation）機能が、仕様通りに動作していること。
【補足：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

★3 評価ガイド（製造業者・評価機関向け）
評価機関は、以下の【ドキュメント評価】及び【実機テスト】の結果が「適合（Y)」の場合に限り、本適合基準の評価結果を「適合（Y)」と判断する。

【技術文書】
製造業者は、以下の技術文書を評価機関に提出する。
技術文書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のリスト
技術文書２：入力データの妥当性検証の内容が記述された文書

【ドキュメント評価】

評価機関は、製造業者から提供されたドキュメント(技術文書）によって、評価項目１～２の評価を実施する。全ての評価項目の評価結果が「適合（Y)」の場合にのみ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１のリストが完全であるかどうかをチェックすること。少なくとも以下がリストに含まれていることを確認すること。
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

評価項目２：
技術文書２を参照し、それぞれのインタフェースに対応する入力データの妥当性検証内容に以下が含まれることを確認する。
A）正しいタイプ（許可されたデータ形式とデータ構造)
B）許可された値
C）許可された基数
D）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

【実機テスト】
評価機関は、技術文書１に記載されたすべてのインタフェースに関して、評価項目３の評価を実施する。評価項目の評価結果が「適合（Y)」の場合にのみ実機テストの評価結果は「適合（Y)」となる

評価項目３
すべてインタフェースに対して技術文書２を参照して不正な入力データを検証するテストデータを生成する。作成したテストデータにより入力検証（Validation）機能が、仕様通りに動作していることを確認する。

適合基準番号 : S3.1-39
★3 適合基準
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すること。

対象外（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】

IoT 製品が個人情報を収集・処理しない場合

★3 評価手法

・ドキュメント評価：

対象とする

・実機テスト：

なし

★3 適合ガイド（製造業者向け）

本適合基準では、

・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 製品から得られる個人データの種別や処理方法が記載されていること

を要求する。

個人データの利用ポリシーに関しては、以下のすべての適合要件を満たすこと。

適合要件１：

どの種別の個人データが取得されるかがユーザマニュアル等に明記されていること。

適合要件２：

個人データを処理する機能についてユーザマニュアル等に明記されていること。

適合要件３：

適合要件１～２の記載がユーザにとって明確であること。

★3 評価ガイド（製造業者・評価機関向け）

評価機関は、以下の【ドキュメント評価】の結果が「適合（Y)」の場合に限り、本適合基準の評価結果を「適合（Y)」と判断する。

【技術文書】

製造業者は、以下のドキュメントを技術文書として評価機関に提出する。

技術文書１：IoT 製品で収集・処理される個人情報に関する記載があるユーザマニュアル等

【ドキュメント評価】

評価機関は、製造業者から提供された技術文書１によって、評価項目１～３の評価を実施する。全ての評価項目の評価結果が「適合（Y)」の場合にのみ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 製品によって収集される個人情報とそのデータ種別が明示されていることを確認する。

評価項目２：
IoT 製品によって処理される個人情報とその方法が明示されていることを確認する。

評価項目３：
技術文書１の記載内容について、専門用語等を多用せず平易で理解しやすい表現で示した情報であることを確認する。

適合基準番号：S3.1-40

★3 適合基準

IoT 製品からテレメトリデータが取得され、かつ個人情報の処理を行う場合、以下の基準を満たすこと。

①個人情報の処理を、意図された機能にとって必要最小限のものに留めること。

対象外（NA）となるための条件、基準の補足説明

【NA となるための条件】
IoT 製品からテレメトリデータを取得しない又は IoT 製品からテレメトリデータを取得するが、個人情報の処理を行わない（「NA であることの理由」に、IoT 製品からテレメトリデータを取得しない又は機器からテレメトリデータを取得するが、個人情報の処理を行わないことを示す根拠を記載すること）

★3 評価手法

ドキュメント評価：
対象とする
実機テスト：なし

★3 適合ガイド（製造業者向け）

本適合基準では、
・テレメトリデータに含まれる個人情報の処理が必要最小限に留められていること
を
要求する。
この要求に関して、以下の適合要件 1 を満たすこと。

適合要件 1 ：
テレメトリデータに個人情報含まれる事が想定される範囲で、個人情報の扱いに対する、目的及び使用の範囲が、IoT 製品のマニュアル、ウェブサイト等、機器の利用者（一般消費者、機器管理者）がアクセス可能な媒体に明示されていること。

★3 評価ガイド（製造業者・評価機関向け）

評価機関は、以下の【ドキュメント評価】の結果が「適合（Y)」の場合に限り、本適合基準の評価結果を「適合（Y)」と判断する。

[技術文書]
製造業者は、以下のドキュメントを技術文書として評価機関に提出する。
・テレメトリデータに含まれる個人情報の扱いが記述された文書

【ドキュメント評価】
IoT 製品の技術文書などを確認し、テレメトリデータに含まれる個人情報の扱いが、明示されていることを評価する。以下の評価項目について明示されている場合に限り、本適合基準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 ：
テレメトリデータに含まれる個人情報を最小化するため、個人情報の取り扱いに対する、目的及び使用の範囲が、IoT 製品のマニュアル、ウェブサイト等、機器の利用者（一般消費者、機器管理者）がアクセス可能な媒体に明示され、確認できること。

適合基準番号 : S3.1-41

★3 適合基準

IoT 製品からログ（テレメトリデータ・監査ログ）を収集する場合、製造業者は、どのようなログ（テレメトリデータ・監査ログ）が収集され、それが誰によって、どのような目的で使用されているかについて周知すること。

対象外（NA）となるための条件、基準の補足説明

【NA となるための条件】

IoT 製品からログ（テレメトリデータ・監査ログ）を収集する仕組みがない場合

【用語定義：テレメトリデータ】

製品の使用に関する問題や情報を製造業者が特定するのに役立つ情報を提供することができる機器からのデータを指す。

【用語定義：監査ログ】

ユーザが製品におけるセキュリティ上の異常を検知できるようにするため、製品の処理内容やプロセスを、時系列かつ連続的に記録したデータを指す。

★3 評価手法

・ドキュメント評価：

対象とする

・実機テスト：

なし

★3 適合ガイド（製造業者向け）

本適合基準では、

・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 製品から収集・分析されるログ（テレメトリデータ・監査ログ）についての利用ポリシー等に関する情報提供をすること

を要求する。

ログ（テレメトリデータ・監査ログ）の利用ポリシーに関しては、以下の適合要件１～３を満たすこと。

適合要件１：

どの種別のログ（テレメトリデータ・監査ログ）が収集・分析されるかがユーザマニュアル等に明記されていること。

適合要件２：

誰がログ（テレメトリデータ・監査ログ）を収集・分析するのかがユーザマニュアル等に明記されていること。

適合要件３：

どのような目的でログ（テレメトリデータ・監査ログ）を収集・分析するのかがユーザ

マニュアル等に明記されていること。

★3 評価ガイド（製造業者・評価機関向け）

評価機関は、以下の【ドキュメント評価】の結果が「適合（Y)」の場合に限り、本適合基準の評価結果を「適合（Y)」と判断する。

【技術文書】

製造業者は、以下のドキュメントを技術文書として評価機関に提出する。

技術文書１：IoT 製品で収集・分析されるログ（テレメトリデータ・監査ログ）のデータ種別、収集及び分析を行う主体、収集・分析目的が記載された技術文書

【ドキュメント評価】

IoT 製品のユーザマニュアル等を閲覧することで、収集されるログ（テレメトリデータ・監査ログ）の利用ポリシーについて基準で要求されている内容が明示されていることを評価する。以下の評価項目１～３のすべてについて確認できた場合に限り、本適合基準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：

収集・分析されるログ（テレメトリデータ・監査ログ）とそのデータ種別が明示されていることを確認する。

評価項目２：

ログ（テレメトリデータ・監査ログ）の収集・分析を行う主体が明示されていることを確認する。

評価項目３：

ログ（テレメトリデータ・監査ログ）を収集・分析目的が明示されていることを確認する。

適合基準番号 : S3.1-42

★3 適合基準

IoT 製品から得られた個人情報が処理される場合、IoT 製品は収集や処理の範囲を限定する機能および不要になった個人情報を削除する機能を有すること。

対象外（NA）となるための条件、基準の補足説明

【NA となるための条件】
IoT 製品が個人情報を収集・処理しない場合

★3 評価手法

・ドキュメント評価：
対象とする
・実機テスト：
対象とする

★3 適合ガイド（製造業者向け）

本適合基準では、
・個人データの収集や処理の目的において、不要となった情報の削除を行う機能を有すること
を要求する。
各機能に関しては、以下のすべての適合要件を満たすこと。

適合要件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、利用者によるデータの指定等）で削除できる機能が存在すること。

★3 評価ガイド（製造業者・評価機関向け）

評価機関は、以下の【ドキュメント評価】および【実機テスト】の結果が「適合（Y)」の場合に限り、本適合基準の評価結果を「適合（Y)」と判断する。

【技術文書】
製造業者は、以下のドキュメントを技術文書として評価機関に提出する。
技術文書１：IoT 製品で収集・処理される個人情報の削除に関する機能が記載された技術文書

【ドキュメント評価】
評価機関は、製造業者から提供されたドキュメント(技術文書）によって、評価項目１の評価を実施する。全ての評価項目の評価結果が「適合（Y)」の場合にのみ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１に、不要になった（特定の期間や使用頻度、利用者によるデータの指定

等）個人情報を削除できる機能が記載されていることを確認する。

【実機テスト】
評価機関は、実機テストにより評価項目２の評価を実施する。評価項目の結果が「適合（Y)」の場合にのみ本適合基準の評価結果が「適合（Y)」となる

評価項目２：
技術文書１に記載された機能が正常に動作すること

適合基準番号 : S3.1-43

★3 適合基準

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ること。

対象外（NA）となるための条件、基準の補足説明

―

★3 評価手法

・ドキュメント評価：
なし
・実機テスト：
対象とする

★3 適合ガイド（製造業者向け）

本適合基準では、
・評価機関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ること。
を要求する。
この要求に関して、以下の適合要件を満たすこと。
適合要件１：
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、または報告された全てのセキュリティ課題が解消されていること。

★3 評価ガイド（製造業者・評価機関向け）

評価機関は、以下の【実機テスト】の結果が「適合（Y)」の場合に限り、本適合基準

の評価結果を「適合（Y)」と判断する。

【IoT 製品や製品マニュアルなど】
製造業者は評価者による【実機テスト】に際し、最低限以下を提供するものとする。但しこれに限定されない。
・IoT 製品
・管理操作が可能なアカウントやその旨が記載された製品マニュアル
・露出したデバッグインタフェースへの接続に要する情報
・通信先一覧が記載されたドキュメント

【ドキュメント評価】
無し

【実機テスト】
評価機関は製造業者から提供された IoT 製品や製品マニュアル等を参考情報とし、ペネトレーションテスト項目を考案し実施する。以下の全ての評価項目が確認できた場合に限り、本適合基準の実機テストの評価結果は「適合（Y)」となる。
評価項目１：
ネットワークインタフェースにおいて解放されている全ての TCP/UDP ポートへの診断を行い、公知の脆弱性が検出されないこと。

評価項目２：
Web ベースのユーザインタフェースの診断を行い、ロジックや作りこみによるものを含む脆弱性が検出されないこと。

評価項目３：
物理的にアクセス可能なデバッグインタフェースがあった場合、デバッグ行為が行えないこと。なお、物理的にアクセス可能なデバッグインタフェースには（21-1）の適合要件１を満たさずに取り外せる筐体やカバーで保護された物理インタフェースを含む。
また、デバックインタフェースの接続においては、製造業者の協力を得て実施する。

全ての実機テストの評価項目において、CVSS v3 基本評価基準 4.0 以上の脆弱性、もしくはセキュリティ要件が不適合となる挙動が検証された項目をセキュリティ課題として、評価者は製造業者に、再現可能な形式（再現手順、画面キャプチャーなど）で報告し、是正を求めるものとする。

評価項目４：
IoT 機器からの不正な通信（通信先一覧以外への通信）が検出されないこと。この評価は評価項目１,２を実施する際に常時通信をキャプチャすることにより実施する。

【補足】
・IoT 機器の破壊を目的とした検証は行わないものとする。(USB Killer などは実施しない)

適合基準番号 : S3.1-44

★3 適合基準

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、基準の補足説明

【用語定義：ユーザ】
ユーザの対象範囲には、IoT 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

★3 評価手法

・ドキュメント評価：
対象とする
・実機テスト：
なし

★3 適合ガイド（製造業者向け）

本適合基準では、
・ユーザに提供する製品のセキュリティに関する情報が、指定された言語であることを要求する。
この要求に関して、以下の適合要件を満たすこと。

適合要件１：
各適合基準でユーザに提供が求められている情報が指定された言語で記載されていること。

★3 評価ガイド（製造業者・評価機関向け）

評価機関は、以下の【ドキュメント評価】の結果が「適合（Y)」の場合に限り、本適合基準の評価結果を「適合（Y)」と判断する。

【技術文書】

製造業者は、以下の技術文書を評価機関に提出する。

技術文書１：

各適合基準でユーザに提供が求められている情報に関する文書

【ドキュメント評価】

評価機関は、製造業者から提供されたドキュメント（技術文書）によって、評価項目１の評価を実施する。評価項目１の評価結果が「適合（Y)」の場合にのみ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：

各適合基準でユーザに提供が求められている情報が指定された言語で記載されていること。

適合基準番号 : S3.1-45

★3 適合基準

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

【用語定義：守るべき情報資産】

以下の情報：

・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
・ログ（テレメトリデータ・監査ログ）
・プログラムコード（ソフトウェア）
・IoT 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

★3 評価手法

・ドキュメント評価：
対象とする
・実機テスト：
なし

★3 適合ガイド（製造業者向け）

本適合基準では、
・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をすること
を要求する。
IoT 製品のサイバーセキュリティに関する情報提供は、以下の適合要件１～５のすべてを満たしていること

適合要件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。
適合要件２：
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、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。
適合要件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。
適合要件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サポートとして提供すること。
適合要件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

★3 評価ガイド（製造業者・評価機関向け）

評価機関は、以下の【ドキュメント評価】の結果が「適合（Y)」の場合に限り、本適合基準の評価結果を「適合（Y)」と判断する。

【技術文書】
製造業者は、以下の技術文書を評価機関に提出する。
技術文書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記載した文書（ユーザに提供する文書）
技術文書２：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、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を規定した文書
技術文書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する免責事項を記載した文書（ユーザに提供する文書）
技術文書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サポートとして提供することを宣言する文書（JC-STAR ラベル申請書で差し支えない）
技術文書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、データ消去を含む製品の安全な利用終了方法を記載した文書（ユーザに提供する文書）

【ドキュメント評価】
評価機関は、製造業者から提供されたドキュメント（技術文書）によって、評価項目１～６の評価を実施する。評価項目１～６の全ての評価結果が「適合（Y)」の場合にのみ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１に、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が明記されていることを確認する。
評価項目２：
技術文書２に、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、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規定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確になっていること。
評価項目３：
技術文書３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記されていることを確認する。
評価項目４：
技術文書４に、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サポートとして提供することが宣言されていることを確認する。
評価項目５：
技術文書５に、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。
評価項目６：
技術文書１、技術文書３、技術文書５がユーザに提供されることを確認する。

適合基準番号 : S3.1-46

★3 適合基準

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有すること。

対象外（NA）となるための条件、基準の補足説明

【用語定義：ネットワーク過負荷状態】
ネットワークに過剰な負荷がかかり、通信機器が正常に動作出来ない状態

★3 評価手法

・ドキュメント評価：
対象とする
・実機テスト：
対象とする

★3 適合ガイド（製造業者向け）

本適合基準では、

・サービス不能攻撃によるネットワーク過負荷時に、通信機能が継続できること
を要求する。
この要求に関して、以下の適合要件が満たされていること。

適合要件１：
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解消後に、通信が再開されること。

★3 評価ガイド（製造業者・評価機関向け）

評価機関は、以下の【ドキュメント評価】及び【実機テスト】の結果が「適合（Y)」の場合に限り、本適合基準の評価結果を「適合（Y)」と判断する。

【技術文書】
製造業者は、以下の技術文書を評価機関に提出する。
技術文書１：IoT 機器の過負荷状態解消後のふるまいの仕様を記載した文書

【ドキュメント評価】
評価機関は、製造業者から提供されたドキュメント(技術文書）によって、評価項目 1 の評価を実施する。実施した評価項目の評価結果が「適合（Y)」の場合にのみ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 1 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において、過負荷状態解消後に、通信が再開されることが明記されていること。

【実機テスト】
評価機関は、サービス不能攻撃によるネットワーク過負荷時の IoT 製品の動作を実機テストにより評価する。以下の評価項目 2 を実施し、評価結果が「適合（Y)」の場合に限り、本適合基準の評価結果が「適合（Y)」となる。

評価項目２：
IoT 機器へのサービス不能攻撃を一定時間再現した後、正常に通信が再開されること。「一定時間」については IoT 製品製造業者が、定義するものとする。評価者は製造業者に仕様を確認の上、テストを実施すること。

適合基準番号 : S3.1-47

★3 適合基準

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すること。

対象外（NA）となるための条件、基準の補足説明

―

★3 評価手法

・ドキュメント評価：

対象とする

・実機テスト：

なし

★3 適合ガイド（製造業者向け）

本適合基準では、

・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が実装されていること

を要求する

この要求に関して、以下の適合要件１を満たすこと。

適合要件１：

筐体の耐タンパー性を向上させる仕組みが実装されていること。具体的には、以下のすべてに類する実装又はそれ以上の実装であること。

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）

B）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）

【補足１：耐タンパー性を向上させる仕組みの例】

A）耐衝撃（バンダルレジスタンス又はプルーフ）構造であることを確認する。

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出来ない構造であることを確認する。

【補足２：物理的保護の例外事項】

・機器の設置環境が、セキュリティエリア(*1)への設置を前提としている場合、その旨の注意をユーザに明示することを条件に、適合要件１を満たしているとみなす。

(*1)：物理的セキュリティに配慮された施設内の共用エリア以外の区画

★3 評価ガイド（製造業者・評価機関向け）

評価機関は、以下の【ドキュメント評価】の結果が「適合（Y)」の場合に限り、本適合基準の評価結果を「適合（Y)」と判断する。

【技術文書】

製造業者は、以下のドキュメントを技術文書として評価機関に提出する。

・物理的な破壊・改変行為から筐体（エンクロージャ）を保護する設計であることが記載された仕様書や証明書

【ドキュメント評価】

評価機関は、製造業者から提供された技術文書を確認し、以下のすべての評価項目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「適合（Y)」となる。

評価項目 1：

筐体の耐タンパー性を向上させる仕組みが実装されていること。具体的には、以下の全てに類する実装又はそれ以上の実装であること。

A）強化されたエンクロージャ（筐体に高強度の素材を使用すること）

B）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）