★1 適合基準・評価ガイドの説明

（独）情報処理推進機構セキュリティセンター

IPA Better Life with IT

©2024 独立行政法人情報処理推進機構（IPA）

注意

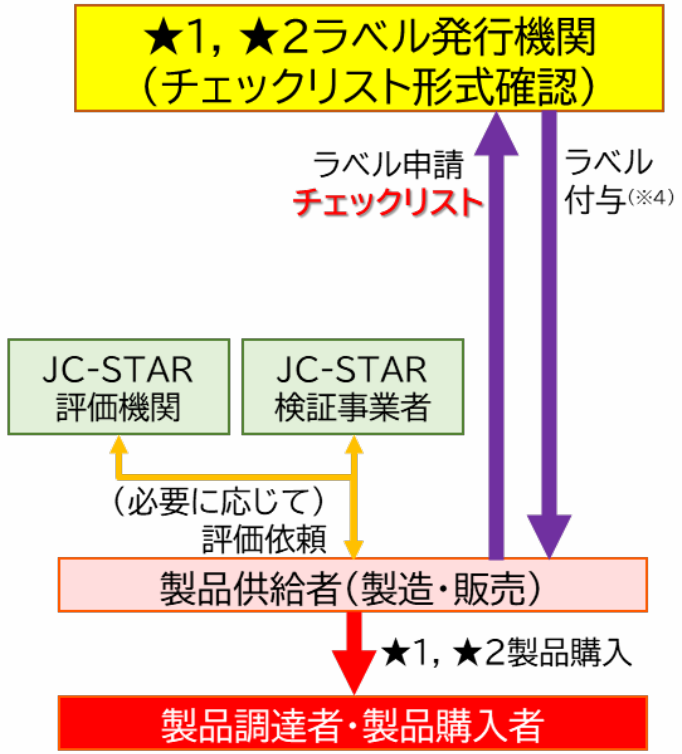
- **2024年11月28日時点での「★1申請手続き」と「★1適合基準・評価ガイド」に対する概要説明です。**
- **今後の「★1申請手続き」の検討状況によっては、制度開始までに一部内容が修正される可能性があります。**
  - 実際の申請に当たっては最新情報を利用してください。
- **「★1適合基準」については、12月6日までに修正版を出す予定です。**
  - 基本的にはエディトリアル（表記ブレ・誤記・用語不統一）の修正です。
  - 今までにいただいた質問とその回答を踏まえ、一部内容を明確化・修正をしました。
  - 修正箇所はわかるように周知します。
- **「★1評価ガイド」についても12月6日までに公開します。**
  補足説明については、今後頂く質問とその回答を踏まえて、必要に応じて適宜更新していく予定としています。

©2024 独立行政法人情報処理推進機構（IPA）

（C）★1適合ラベルの申請

（C-1）適合ラベルの申請方法を教えてください

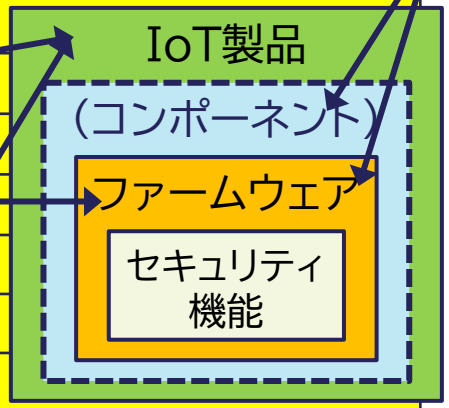
1. IoT製品ベンダー
   - ★1適合基準・評価手順に従って自ら評価を行い、**チェックリスト**を作成
   - 必要に応じて、JC-STAR評価機関・検証事業者等に評価を依頼可
2. IoT製品ベンダー
   - **申請書**と作成したチェックリストを添えて、IPAにラベル申請
   - チェックリストの提出に当たり、IPAへの証跡提出は不要
   - 適合ラベルの有効期間中は証跡の保管義務があることに留意
3. IPA 【申請後、おおむね**2週間程度**を想定】
   - 経済産業省とともに必要な確認作業を行ったうえで、ラベル申請受理
4. IoT製品ベンダー
   - 申請が受理されたら、新規申請手数料をIPAに支払い
5. IPA 【支払確認後、おおむね**2週間程度**を想定】
   - そのIoT製品に対する適合ラベルを付与



©2024 独立行政法人情報処理推進機構（IPA）

★1の申請に当たって　－　適合ラベル発行申請書

申請者区分	● 申請製品の製造ベンダー自身による申請【自社ブランドでのIoT製品】 ● 申請代理
申請企業名	
法人番号（13桁）、又は法人登記簿謄本等	
申請者情報	
代理申請企業名	
法人番号（13桁）、又は法人登記簿謄本等	
代理申請者情報	
製品類型	
製品名称	
製品型番	
ファームウェアバージョン	
サポート期間	
製品概要・製品ホームページURL	
製造ベンダーの名称	
製造方法区分	● 自社製造 ● OEM/ODM製造
OEM/ODM製造企業名	
製造国・地域	



ファームウェア開発・保守方法区分	● 自社開発部門・保守部門のみ ● 委託先企業も利用 ● コンポーネント生産会社から供給
実際のファームウェア開発・保守を行う企業名称	
コンポーネントの適合ラベル	
製品に関する問合せ窓口	
製品に関する不具合・脆弱性の届出窓口	
脆弱性開示ポリシー	
ラベル取得製品リストへの掲載日の希望	
適合評価方法	● 自己評価 ● JC-STAR評価機関での評価 ● JC-STAR検証事業者での評価
評価機関名・検証事業者名	
評価完了日（申請日の90日前以内）	
他認証情報	
同意・確認	● 申請内容の真正性宣言 ● 規程遵守 ➢ サポート期間内セキュリティアップデート提供（不具合・脆弱性対応） ➢ 証跡保管 ● 法令等の基準への遵守 ● 過去5年以内の適合ラベル取消しがない

©2024 独立行政法人情報処理推進機構（IPA）

★1の申請に当たって　－　チェックリスト

★1適合基準番号	S1.1-01
評価結果	● Y(適合) ● N(非適合) ● NA(対象外) ➡ 一つでも「N(非適合)」があると申請不可
証跡(エビデンス)の名称	● 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	● 「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

➡ 申請段階では証跡(エビデンス)の提出は不要

©2024 独立行政法人情報処理推進機構(IPA)

JC-STARにおける★1の位置付け

★1では、以下の3点を最低限実現することが求められる

- ★1の適合基準への適合により、**最低限の脅威に対抗**できる
  - ✓ 特定の製品類型に絞らず、**広範なIoT製品を対象とした、最低限の脅威に対抗するための統一的な基準**とする
- ★1の適合基準への**評価は、低コストかつ自己適合宣言で対応**できる
  - ✓ ベンダ自身による**自己適合宣言を許容**する
  - ✓ 検証や評価を行う担当者が、**チェックリストや評価ガイドを見て低コストで自己評価可能なレベル**とする
  - ✓ **適合性評価チェックリストの申請に基づきラベルを付与**する（IPAはチェックリストの内容確認は実施しない。）
- ★1の適合基準は、**海外制度と国際連携可能な基準**とする
  - ✓ シンガポールCLS＊1要件や英国PSTI法など、**海外制度と国際連携可能な要件**とする

©2024 独立行政法人情報処理推進機構（IPA）

★1で実現したいセキュリティ水準の考え方

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 廃棄前に、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**

©2024 独立行政法人情報処理推進機構（IPA）

★1で想定する守るべき資産

- IPA文書及びCCDS文書を踏まえ、IoT製品において守るべき資産として、以下の4つの資産を考慮
- ★1で想定する守るべき資産としては、以下に限定
  - ✓ 情報に関する守るべき資産について、IoT機能やセキュリティ機能に関する設定情報のほか、**意図された機器の使用において、機器が収集し、保存又は通信する、個人情報等の一般的に機密性が高い情報**を対象

IoT製品において守るべき資産	★1で想定する守るべき資産	★2以上で想定する守るべき資産
1. IoT機能 機器やシステムがIoTにつながるための機能	• **有線通信機能** • **無線通信機能**	• 有線通信機能 • 無線通信機能
2. 本来機能 「モノ」本来の機能、セキュリティ対策・セーフティ対策のための機能	• **セキュリティ機能**	• セキュリティ機能 • 製品本来の機能[1] • セーフティ関連機能[2]
3. 情報 ユーザの個人情報、収集情報、各機能の設定情報など	• **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** • **機器の意図する使用[3]において、機器が収集し、保存又は通信する、個人情報等の一般的に機密性が高い情報[4]**	• 設定情報 • 個人情報 • 収集情報 • 接続先機器に関する情報　等
4. その他の物理的資産 ユーザの健康・生命やIoT機器が内蔵する物理的資産	ー	• 人的資産[5] • 物理的資産[6]

1: 例えば、エアコンであれば冷暖房、ドローンであれば飛行のような固有の機能のこと。
2: 現在の社会の価値観に基づいて、与えられた状況下で、受け入れられないリスクの発生を防ぐ機能のこと。
3: 製品もしくはシステムとともに提供される情報に従った使用、又はそのような情報がない場合には、一般的に理解されている方法による使用のこと。(JIS Z 8051:2015)
4: 個人情報に関する意図する使用を持たないが、その機器によって扱われる情報に個人情報が含まれうる機器の場合、想定される運用環境において盗聴の脅威に関して許容不可能な脅威がある場合に限り、対象情報を保護資産として扱う。
例えば、防犯カメラが収集する特定の個人が識別可能な映像(個人情報)などが該当するが、ルータに伝送される個人情報は「意図された機器の使用において、機器が収集」することに該当しないため、対象外となる。
5: 利用者の健康など、利用者の物理的安全性のこと
6: 製品本体や関連する物理的機器のこと

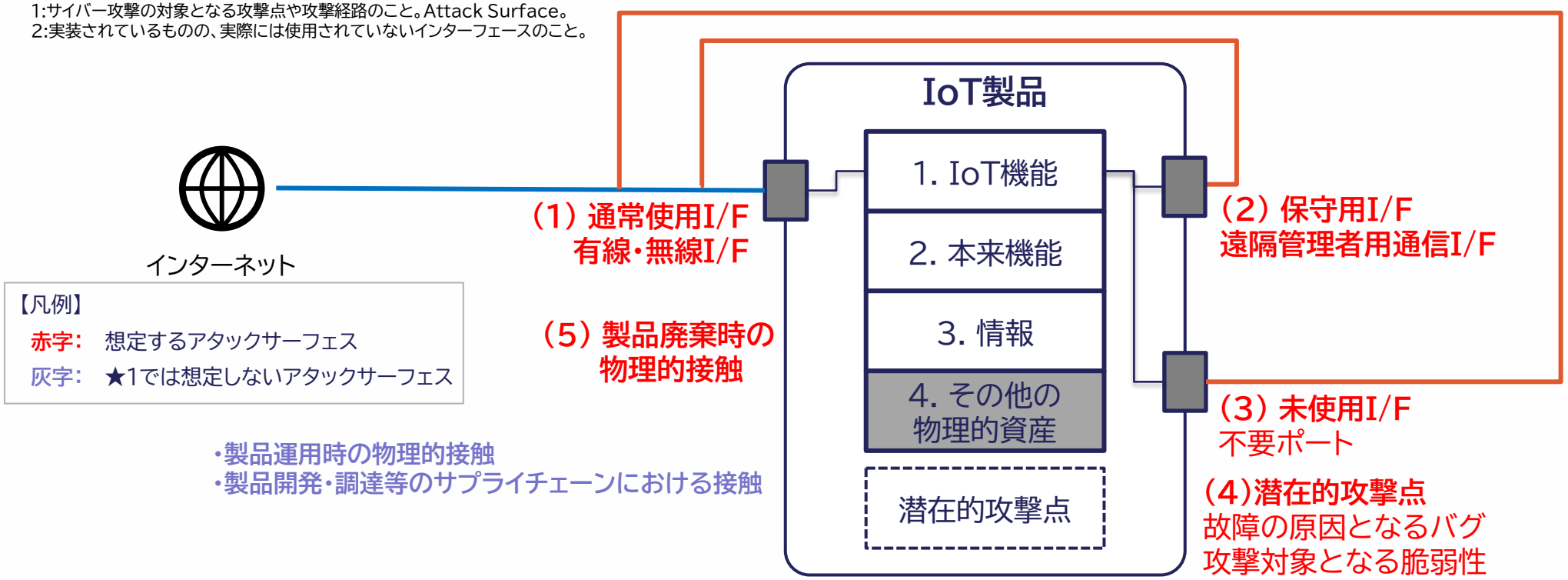
出所)IPA つながる世界の開発指針　第2版　https://www.ipa.go.jp/publish/qv6pgp000000114a-att/000060387.pdf
CCDSサーティフィケーションプログラム IoT機器に対するリスク分析のガイド　https://www.ccds.or.jp/certification/document/ccds_risk_analysis_process.pdf

©2024 独立行政法人情報処理推進機構(IPA)

★1で想定するアタックサーフェス

- IPA文書及びCCDS文書を踏まえ、★1取得が想定される製品におけるアタックサーフェス[1]としては、「(1) 通常使用I/F」、「(2) 保守用I/F」、「(3) 未使用I/F[2]」、「(4) 潜在的攻撃点」、「(5) 製品廃棄時の物理的接触」の5つのアタックサーフェスを想定
  - ✓ ★1で対抗する脅威のレベルを踏まえ、「製品運用時の物理的接触」や「製品開発・調達等のサプライチェーンにおける接触」のアタックサーフェスは★1では想定しない

1:サイバー攻撃の対象となる攻撃点や攻撃経路のこと。Attack Surface。
2:実装されているものの、実際には使用されていないインターフェースのこと。

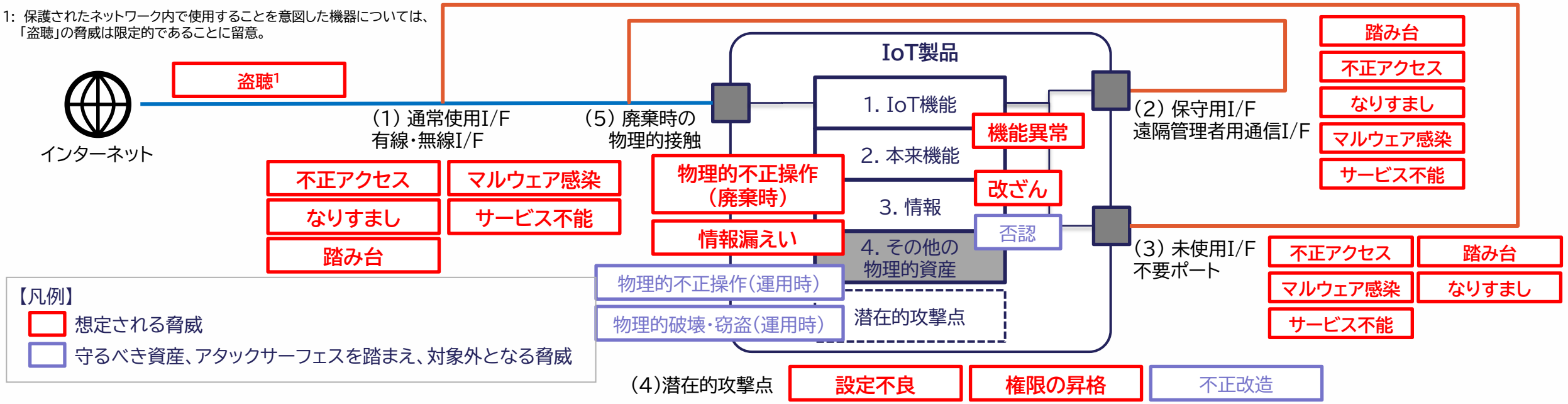


出所)IPA つながる世界の開発指針 第2版 https://www.ipa.go.jp/publish/qv6pgp000000114a-att/000060387.pdf
CCDSサーティフィケーションプログラム IoT機器に対するリスク分析のガイド https://www.ccds.or.jp/certification/document/ccds risk-analysis-process.pdf

©2024 独立行政法人情報処理推進機構(IPA)

★1で想定される脅威

- ★1で想定する守るべき資産及びアタックサーフェスを踏まえ、IoT製品に対して想定される脅威を以下のようにマッピング。なお、脅威は、IPA文書及びCCDS文書を参照して整理
  - ✓ 「製品運用時の物理的接触」と「製品開発・調達等のサプライチェーンにおける接触」のアタックサーフェスを想定しないため、「物理的不正操作（運用時）」「物理的破壊・窃盗（運用時）」「不正改造」の脅威は対象外
  - ✓ STRIDEモデルでは「否認」が一つの脅威として挙げられているが、★1で想定する守るべき資産として「否認」の影響を受ける資産を考慮していないため、当該脅威は対象外



出所）IPA つながる世界の開発指針 第2版 https://www.ipa.go.jp/publish/qv6pgp000000114a-att/000060387.pdf
IPA IoT開発におけるセキュリティ設計の手引き https://www.ipa.go.jp/security/iot/ug65p90000019832-att/ssf7ph0000002vih.pdf
CCDSサーティフィケーションプログラム IoT機器に対するリスク分析のガイド https://www.ccds.or.jp/certification/document/ccds_risk-analysis-process.pdf

©2024 独立行政法人情報処理推進機構（IPA）

脅威に対抗するために★1で実現すべき対策

★1で考慮すべき主な4つの脅威に対し、★1の位置付けや海外制度の基準等を踏まえ、製品／製品ベンダにおいて実現すべき対策を以下のとおり選定

★1で考慮すべき主な脅威			脅威に対抗するために★1で実現すべき対策			
			製品における対策		製品ベンダにおける対策	
			カテゴリ	対策	カテゴリ	対策
1.	①弱い認証機能により、	外部からの不正アクセスの対象となり、マルウェア感染や踏み台となる攻撃等を受けることで、情報漏えい、改ざん、機能異常の発生につながる脅威	識別・認証、アクセス制御	• 容易に推測できるパスワードが設定できない仕組みを導入する • セキュアな認証の仕組みを提供する • ブルートフォースによる認証試行を防ぐ仕組みを提供する	情報提供	• セキュアな利用方法に関する情報を提供する
	②脆弱性の放置により、		脆弱性対策、ソフトウェアの更新	• 深刻度の高い既知の脆弱性及び主要なCWEに対する対策を行う • ソフトウェアコンポーネントがアップデート可能な仕組みを導入する	情報・問い合わせの受付、情報提供	• 製品に関する情報及び脆弱性に関する情報を提供する • セキュリティパッチの適用方法に関する情報を提供する
	③未使用インタフェースの有効化により、		インターフェイスへの論理アクセス	• 不要なインタフェースを無効化する	―	―
			データ保護	• 機器が保有する守るべき情報を保護するための機能を提供する（①～③の脅威に共通する対策）	―	―
2. 機器の通信が盗聴され、守るべき情報が漏えいする脅威			データ保護	• インターネット経由で伝送される守るべき情報を保護するために情報の漏えいや変更に対する保護対策を実装する	―	―
3. 廃棄・転売等された機器から、守るべき情報が漏えいする脅威			データ保護	• 機器の利用中に機器内に保存された守るべき情報を製品本体や関連サービスを介して削除できる機能を提供する • 機器に当初から搭載されている守るべき情報を保護するための機能を提供する	情報提供	• セキュアな廃棄方法に関する情報を提供する
4. ネットワーク切断や停電等の事象が発生した際に、セキュリティ機能に異常が発生する脅威			レジリエンスの向上	• ネットワーク切断や停電等の事象が発生し、復旧した場合でも、認証情報やソフトウェア設定は初期状態に戻らず、電源OFF前の状態を提供する	―	―

©2024 独立行政法人情報処理推進機構（IPA）

★1のセキュリティ要件・適合基準

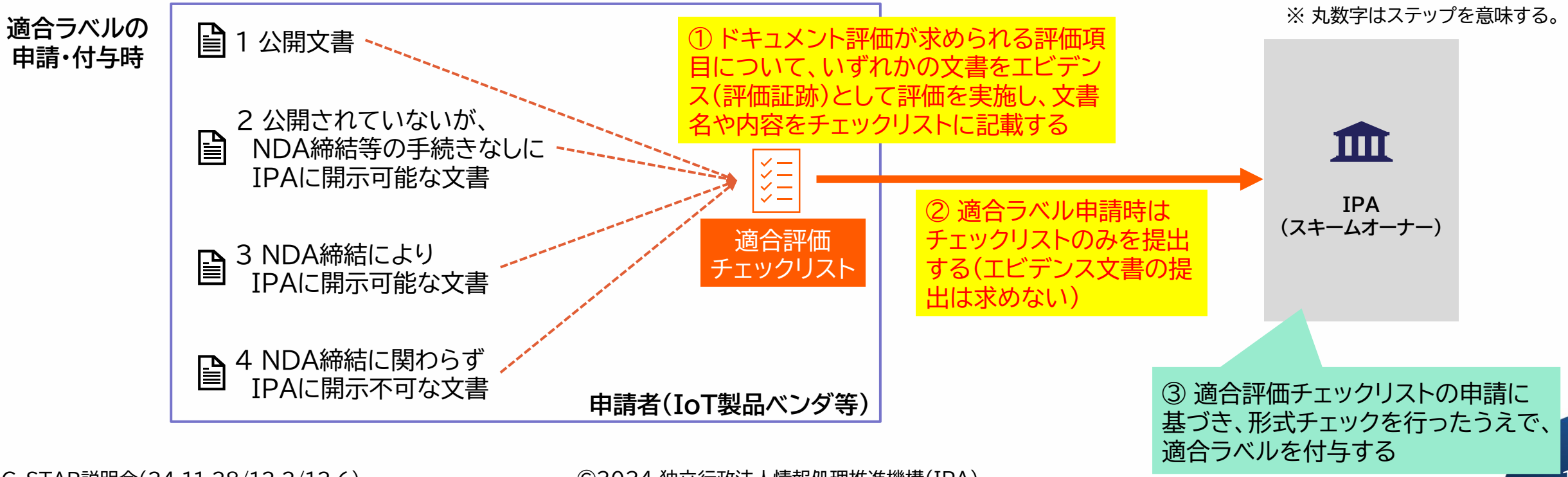
★1で考慮する主な脅威			脅威に対抗するために★1で求める適合基準			
			IoT製品に対する適合基準		IoT製品ベンダーに対する適合基準	
			カテゴリ	適合基準の概要	カテゴリ	適合基準の概要
1.	①弱い認証機能により、	外部からの不正アクセスの対象となり、マルウェア感染や踏み台となる攻撃等を受けることで、情報漏えい、改ざん、機能異常の発生につながる脅威	識別・認証、アクセス制御	(1)適切な認証に基づく**アクセス制御**[1-3,5-5] (2)**容易に推測可能なデフォルトパスワードの禁止**[1-2,1-1] (3)パスワード等の認証値の変更機能[1-4] (4)ネットワーク経由のユーザ認証に対する**総当たり攻撃からの保護**[1-5]	情報提供	(16)ユーザへの**セキュアな利用・廃棄方法に関する情報提供**(初期設定手順、セキュリティ更新、サポート期限、安全な廃棄手順等)[17-12,17-3,17-5,17-8,17-10]
	②脆弱性の放置により、		脆弱性対策、ソフトウェア更新	(6)ソフトウェアコンポーネントのアップデート機能[3-1,3-2] (7)**容易かつ分かりやすいアップデート手順**[3-3] (8)アップデート前のソフトウェアの完全性の確認機能[3-7,3-2,3-10] (10)ユーザが製品型番を認識可能とする記載・機能[3-16]	情報・問合せの受付、情報提供	(5)連絡先・手続き等の**脆弱性開示ポリシーの公開**[2-1] (9)セキュリティアップデートの優先度決定方針の文書化[3-8]
	③未使用インタフェースの有効化により、		インタフェースへの論理アクセス	(13)**不要かつリスクの高いインタフェースの無効化**(物理的・論理的な通信ポート等)[6-1]	―	―
	①～③共通		データ保護	(11)製品に保存される守るべき情報の保護(**保存データの暗号化、物理的保護による保存、OSセキュア管理**等)[4-1]	―	―
2. 機器の通信が盗聴され、守るべき情報が漏えいする脅威			データ保護	(12)ネットワーク経由で伝送される守るべき情報の保護(**通信の暗号化、保護された通信環境の利用**等)[5-1,5-7]	―	―
3. 廃棄・転売等された機器から、守るべき情報が漏えいする脅威			データ保護	(15)**製品内に保存される守るべき情報の削除機能**[11-1] ※(11)も含む	情報提供	※(16)に含む
4. ネットワーク切断や停電等の事象が発生した際に、セキュリティ機能に異常が発生する脅威			レジリエンス向上	(14) 停電・ネットワーク停止等からの復旧時の**認証情報やソフトウェア設定の維持**(初期状態に戻らないこと)[9-1]	―	―

※「適合基準の概要」欄の末尾の"[N-N]"は対応するセキュリティ要件の項目番号(複数の場合、代表的な要件を先頭に記載)を示す。セキュリティ要件は17個の大項目に分類
※ 複数の脅威に対応するための適合基準もあるが、代表的なものにマッピングしている。

©2024 独立行政法人情報処理推進機構(IPA)

★1における文書等の取扱いについて(1/2)

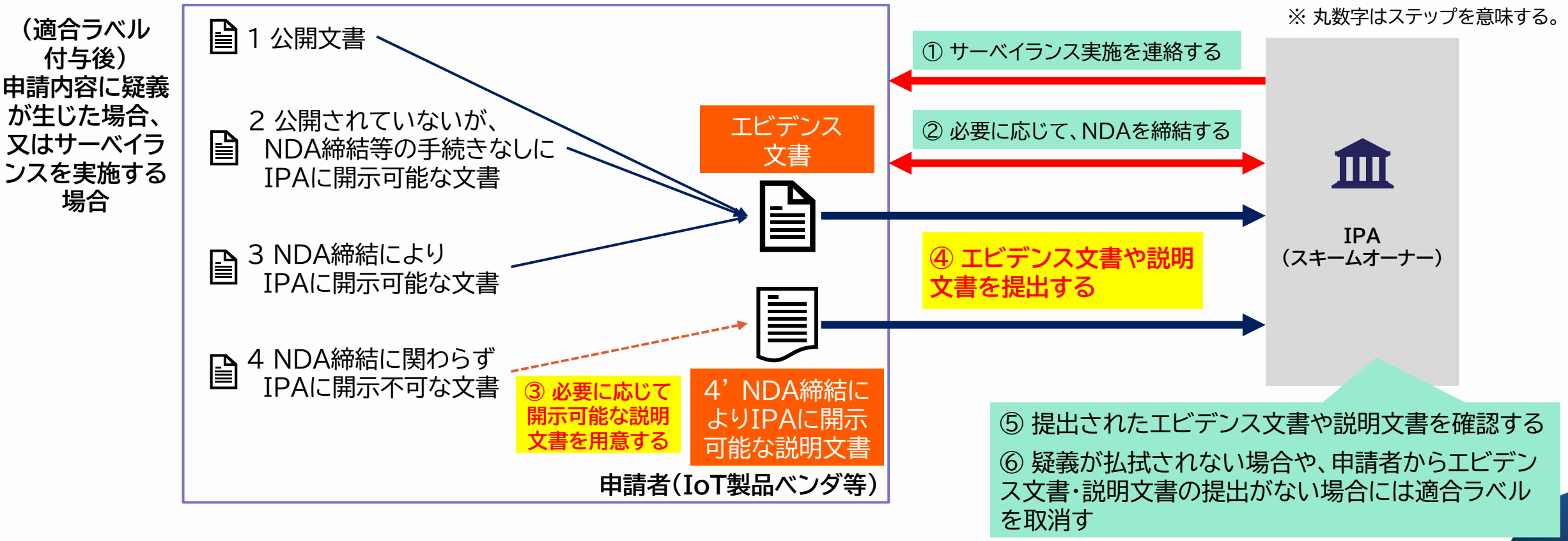
- ★1の評価において、**ドキュメント評価の対象とする文書等はベンダが選択**できる形式とする
  - ✓ 適合ラベル申請時は、適合評価チェックリストの提出のみを申請者に求め、**エビデンス文書の提出は求めない**
  - ✓ 適合ラベルの有効期間中、**エビデンス文書の保管を義務付け**
  - ✓ 第三者(評価機関・検証事業者)においてベンダのエビデンス文書を受領できなかったことに起因して評価ができなかった項目が一つでもある場合のチェックリストは、全体を「申請者による自己評価結果」とし、「第三者(評価機関・検証事業者)が実施した評価結果」とはみなさない



©2024 独立行政法人情報処理推進機構(IPA)

★1における文書等の取扱いについて(2/2)

- 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**エビデンス文書の提出を求める**
  - ✓ 「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釈明を認める
  - ✓ 適切な釈明と認められない場合は**適合ラベルを取消す**



©2024 独立行政法人情報処理推進機構(IPA)

評価についてのよくある質問

（A）「セキュアな保存」とは？

- **セキュアな保存**

  保護が必要な情報資産について、「**必要となる保護**」を実現する形で保存すること

  ① 外部に不正に漏えいしないようにする情報資産に対しては「**機密性を保護**」する形での保存が必要
  ② 改ざんされないようにする情報資産に対しては「**完全性を保護**」する形での保存が必要
  ③ 作成者がなりすまされないようにする情報資産に対しては「**真正性を確認**」できる形での保存が必要

- **★1でのセキュアな保存方法の考え方**

  ★1では、正当なアクセスコントロールを行うインタフェースを経由しない不正アクセスへの対策として、以下のいずれかの保存方法のことを「セキュアな保存」とみなす

  - 「**適切な暗号技術**」によって必要な保護（暗号化・署名・MAC）が施されたうえで保存されている
  - セキュアチップなど、「**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
  - 仮想化技術や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
  - 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てアクセス出来ない領域**」に保存されている

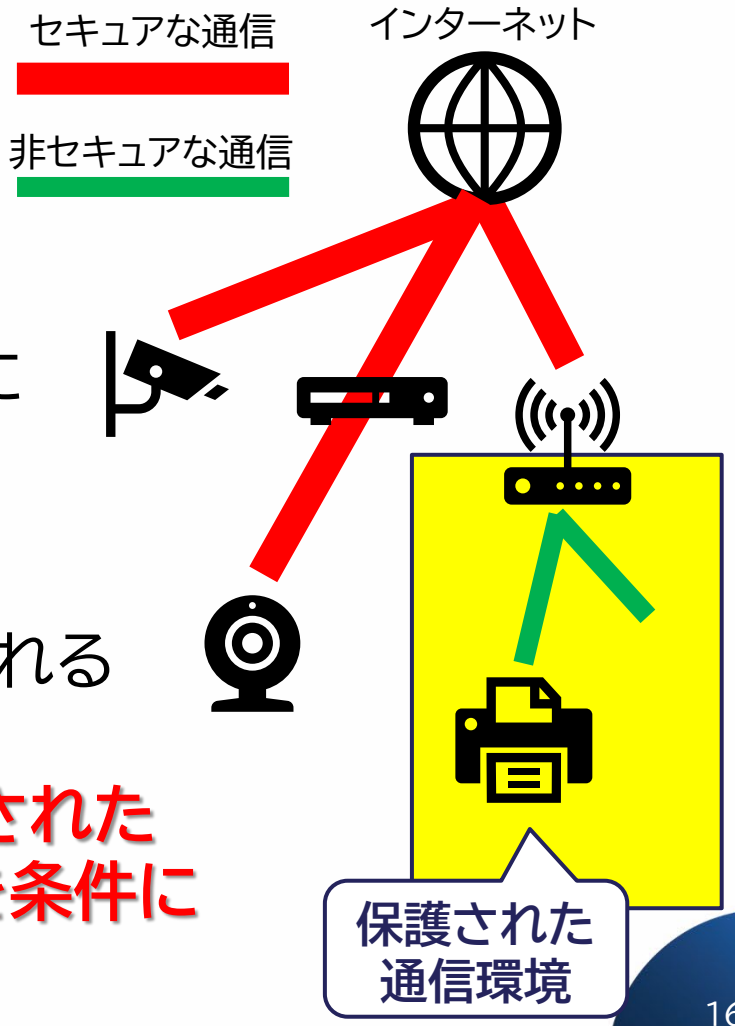
©2024 独立行政法人情報処理推進機構（IPA）

評価についてのよくある質問

（B）「セキュアな通信」が求められる範囲は？

- **セキュアな通信**
  通信内容の「**盗聴を防止**」する形で通信を行うこと

- **★1でのセキュアな通信が必要な範囲の考え方**
  ①インターネットを介した通信を行うIoT機器だけでなく、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機器も**すべてセキュアな通信が求められる対象**
  ※ 例えば、ログイン画面など、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。
  ②★1では、別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範囲内にある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より保護された通信環境に接続して利用する」旨の注意を明示することを条件に保護対策済み**とすることができる



©2024 独立行政法人情報処理推進機構（IPA）

評価についてのよくある質問

（C）「情報資産は全て保護対象」ですか？

- ★1での保護対象となる情報資産の考え方

  ★1では、「**運用中はインターネット側から遠隔攻撃**」される想定とし、「**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**」を前提し、その前提でどのように保護するのかを考える必要がある情報資産が保護対象である

- ★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

  a. 「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

  b. 「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。廃棄・転売時は情報削除又はデフォルト化

  c. 「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」について、
     - 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
     - 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
     - 廃棄・転売時は情報削除

©2024 独立行政法人情報処理推進機構（IPA）

評価についてのよくある質問

（D）「技術基準適合認定を受けていると適合基準への適合」とみなされるのはなぜですか？

- **評価結果の利活用が可能**
  当該適合基準への適合性を判断するために実施する評価内容について、技術基準適合認定を受けるために実施する評価内容のなかに同じものがあるため、その時の評価結果を証跡（エビデンス）として利活用できる
- **証跡の保管は必要**
  技術基準適合認定を受ける際に実施した評価結果をまとめた資料を証跡（エビデンス）として保管する
- **適合基準への適合をみなされるのは一部の要件についてのみ**
  評価結果が利活用できるのは、S1.1-01、S1.1-06、S1.1-14のみ。
  それら以外は適合評価を別途実施する必要あり

©2024 独立行政法人情報処理推進機構（IPA）

【★1適合基準S1.1-01】

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。）

- 評価手法
  - 【ドキュメント評価】
    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技術文書に明示されていることを評価する
    - ◆【評価項目】
      1. 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、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を確認する。

- 対象外となるための条件
  - 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
    → 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

©2024 独立行政法人情報処理推進機構（IPA）

【★1適合基準S1.1-01】

よくある質問

- 補足説明
  - 「ユーザ」の範囲は？
    → 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、所有者など、IoT機器を使用する自然人または組織
  - **「カスタマーエンジニア」はユーザの対象外としてほしい**
    → **対象外とはしないが、一般利用者と同等の認証方法、利用環境における運用を求めない。セキュリティ上適切と判断した利用制限がかかっているなどの条件が適切に説明されていれば、カスタマーエンジニア専用の認証方式を別に採用することが可能**
  - 「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」は守るべき情報資産か？
    → 「保護されたネットワーク環境内に設置」されることを前提として、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の実装等の対応が出来る機器についてのみ、当該情報は「守るべき情報資産」の対象外にすることが可能。その場合、除外時の理由については、証跡に残す

©2024 独立行政法人情報処理推進機構(IPA)

【★1適合基準S1.1-02】

修正あり

IPA

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~~やパスコード~~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。

- 評価手法
  - 【ドキュメント評価】
    IoT製品導入時にデフォルトパスワードに関する対策が技術文書に明示されていることを評価する
    - 【評価項目】
      以下の評価項目1、2いずれかを満たす実装が明示されていることを確認する
      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。
      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こと。

©2024 独立行政法人情報処理推進機構(IPA)

【★1適合基準S1.1-02】

よくある質問　修正あり

- 対象外となるための条件
  - ネットワークを介したパスワード~~やパスコード~~を利用したユーザ認証の仕組みがない
    → 脅威に対抗するためにパスワード~~やパスコード~~を利用したユーザ認証が必要ない根拠を記載
- 補足説明
  - 「カスタマーエンジニア」が使うデフォルトパスワードは対象外としてほしい
    → 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認証についても原則本適合基準の評価対象。ただし、メンテナンス用インタフェースにおいて、メンテナンス機器を直接メンテナンスポートに接続することを明示している場合は、カスタマーエンジニアの認証について対象外にすることが可能。その場合、除外時の理由については、証跡に残す
  - 設置時に自動的にネットワーク接続する機能がある場合、それはユーザ認証の仕組みがない（適合基準対象外）としてよいか？
    → 以下の条件の両方を満たしている場合に限り、保護されたネットワーク環境内に設置されることを条件として対象外としてよい。その場合、除外時の理由については、証跡に残す
    - 設置時にネットワークを介したユーザ認証を行うアカウントが無い
    - 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デフォルトパスワードが設定されている

©2024 独立行政法人情報処理推進機構（IPA）

【★1適合基準S1.1-03】

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。

- 評価手法
  - 【ドキュメント評価】
    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技術文書にあることを評価する
    - ◆【評価項目】
      以下の評価項目1、2両方の情報が明示されていることを確認する
      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。
      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。
- 対象外となるための条件
  - ネットワークを介したユーザ認証の仕組みがない
    → 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

©2024 独立行政法人情報処理推進機構（IPA）

【★1適合基準S1.1-03】

よくある質問

- 補足説明
  - カスタマーエンジニアが利用する認証値の変更手順は一般利用者に提供すべきものではないのではないか？
    → 認証値の変更機能の利用手順を提供する先の「ユーザ」について、該当する人に限定することは問題ない。例えば、カスタマーエンジニアが利用するものであれば「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

©2024 独立行政法人情報処理推進機構（IPA）

【★1適合基準S1.1-04】

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。

- 評価手法
  - 【実機テスト】
    対象機器に対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
    - ◆【評価項目】
      以下の評価項目1、2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を確認する
      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「一定回数失敗」に対し、下記に類する対応をしていること。
      2. 多要素認証が使用されていること。

©2024 独立行政法人情報処理推進機構(IPA)

【★1適合基準S1.1-04】

- 対象外となるための条件
  - 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アクセスの仕組みがない
      → 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
    - ◆ IoT機器が「制約のある機器」に該当する
      → 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
- 補足説明
  - 「追加の認証禁止」の対象は、アカウントか機器か？
    → アカウントが対象

©2024 独立行政法人情報処理推進機構（IPA）

【★1適合基準S1.1-05】

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

- 評価手法
  - 【ドキュメント評価】
    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
    - ◆【評価項目】
      1. 上記適合基準での①～③すべての情報が明示されていることを確認する。
         ただし、市販前IoT製品で、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、公開見込みが分かる情報（例：公開予定画面）を証跡（エビデンス）に示すことで代替可
- 対象外となるための条件
  - 該当なし

©2024 独立行政法人情報処理推進機構（IPA）

【★1適合基準S1.1-05】

- 補足説明
  - 特になし

©2024 独立行政法人情報処理推進機構(IPA)

【★1適合基準S1.1-06】

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。

- 評価手法
  - 【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
    - ◆【評価項目】
      1. 上記適合基準での①～③のテストをすべて行い、いずれも満たされていることを確認する。
- 対象外となるための条件
  - 該当なし

©2024 独立行政法人情報処理推進機構(IPA)

【★1適合基準S1.1-06】

よくある質問

- 補足説明
  - 「最新のファームウェア（ソフトウェア）のバージョン」表示がIoT機器でできなくてもよいか？
    → 例えば、以下のような方法のいずれでも構わない
    1. IoT機器のディスプレィにバージョン情報を表示する機能を有していること
    2. PCやスマートフォンを接続し、バージョン情報を表示する機能を有していること
    3. バージョン情報に限らず、アップデートが最新の状態が確認出来る機能を有していること
  - 全てのソフトウェアコンポーネントがアップデートできなければならないか？
    → 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を対象とし、IoT製品ベンダーにて対象を選定する。なお、申請書に記載したファームウェアは必ず含めること
  - 制約により／ビジネス的理由により、アップデートできない場合は対象外になりますか？
    → 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、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、エビデンスとして残すことにより実機テストの代替可

©2024 独立行政法人情報処理推進機構（IPA）

【★1適合基準S1.1-07】

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。

- 評価手法
  - 【ドキュメント評価】
    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
    - 【評価項目】
      評価項目1～4いずれかに類するアップデート方法の手順が明示されていることを確認する
      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。
      2. ユーザが、IoT製品の必須付随サービスを利用してアップデートが実行できることが明示されていること。
      3. ユーザが、IoT製品のインタフェース介してアップデートが実行できることが明示されていること。
      4. ユーザが、IoT製品のウェブサイトからアップデートファイルをダウンロードし、IoT製品に対してアップデートが実行できることが明示されていること。

©2024 独立行政法人情報処理推進機構(IPA)

【★1適合基準S1.1-07】

よくある質問

- 対象外となるための条件
  - 該当なし
- 補足説明
  - **容易かつ分かりやすい手順とはどのようなものですか？**
    - → **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、作業手順書などの指示に従えば、通常はアップデートが成功するように作られている、ということを意味する**
  - **カスタマーエンジニアがアップデートを行う場合は対象外としてもいいですか？**
    - → **カスタマーエンジニアがアップデートをする場合であっても、本適合基準の評価対象。ただし、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の開示までででよく、一般利用者への開示までは求めない。カスタマーエンジニアにとって、容易かつ分かりやすい手順でアップデートが実行できれば問題ない**

©2024 独立行政法人情報処理推進機構(IPA)

【★1適合基準S1.1-08】

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。

- 評価手法
  - 【ドキュメント評価】
    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技術文書に明示されていることを評価する
    - 【評価項目】
      評価項目1～3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ことを確認する
      1. アップデートソフトウェアインストール前に付与されたハッシュ値との照合を行い、照合の結果、不一致が確認された場合にはインストールが中止されることが明示されていること。
      2. 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。
      3. アップデートソフトウェアインストール前にデジタル署名による検証を行い、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。

©2024 独立行政法人情報処理推進機構(IPA)

【★1適合基準S1.1-08】

- 対象外となるための条件
  - 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
    → 想定するアップデートの仕組みを記載
- 補足説明
  - 特になし

©2024 独立行政法人情報処理推進機構(IPA)

【★1適合基準S1.1-09】

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。

- 評価手法
  - 【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
    - ◆【評価項目】
      評価項目1～3すべての類する内容が明示されていることを確認する
      1. 対応する脆弱性の深刻度や重要度の指標、脆弱性の種類が記載されていること。
      2. PSIRTやインシデントレスポンス等の組織体制や、脆弱性情報の収集、トリアージや分析、対策、アップデートなど、一連の対応プロセスが記載されていること。
      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。
- 対象外となるための条件
  - 該当なし

©2024 独立行政法人情報処理推進機構（IPA）

【★1適合基準S1.1-09】

- 補足説明
  - セキュリティアップデートを提供する場合、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、対応の難易度などによって適時性が変わってくることから、「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を評価

©2024 独立行政法人情報処理推進機構(IPA)

【★1適合基準S1.1-10】

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。

- 評価手法
  - 【実機テスト】
    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評価する
    - ◆【評価項目】
      評価項目1、2いずれかを確認する
      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。
      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(スマホアプリ等)のGUI、ウェブUI等に実際にアクセスすることで、IoT製品の型番を確認できること。
- 対象外となるための条件
  - 該当なし
- 補足説明
  - 特になし

©2024 独立行政法人情報処理推進機構(IPA)

【★1適合基準S1.1-11】

修正あり

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。

- 評価手法
  - 【ドキュメント評価】
    IoT製品のストレージメディアに保存される場合を含む守るべき情報資産が、~~ネットワーク経由の不正アクセスに対して、~~セキュアに保存されていることを技術文書で評価する
    - ◆【評価項目】
      評価項目1～5いずれかに類する保護対策又はそれ以上の対策が明示されていることを確認する
      1. 「CRYPTREC暗号リスト」の「電子政府推奨暗号リスト」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ていること。
      2. 「CRYPTREC暗号リスト」の「電子政府推奨暗号リスト」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されていること。
      3. 「CRYPTREC暗号リスト」の「電子政府推奨暗号リスト」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されていること。

©2024 独立行政法人情報処理推進機構（IPA）

【★1適合基準S1.1-11】

よくある質問

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ていること。
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てアクセス出来ない領域に保存されていること。

- 対象外となるための条件
  - 該当なし
- 補足説明
  - **一時的に保存される情報資産もセキュアに保存しなければならないですか？**
    → **一時的にキャッシュやメモリに保存される情報資産に対しては、以下のようなセキュリティ対策が技術文書等に明示されている場合、セキュアに保存すべき情報資産から除外できる。**
    - **保護されたネットワーク環境への設置**
    - **守るべき情報資産への適切なアクセスコントロールの実施**
    - **処理終了後の自動消去**
    - **定期的にキャッシュやメモリのクリアできる機能の実装**
  - 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何ですか？
    → 基盤に実装された不揮発性メモリ（フラッシュROM等）を想定。取り外し可能なものは含まない。

©2024 独立行政法人情報処理推進機構（IPA）

【★1適合基準S1.1-12】

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。

- 評価手法
  - 【ドキュメント評価】
    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技術文書で評価する
    - 【評価項目】
      評価項目1、2いずれかについて確認する
      1. 技術文書に以下が明示されていること。
         A) 暗号化されていない情報資産は、「CRYPTREC暗号リスト」の「電子政府推奨暗号リスト」記載の暗号技術を採用した通信プロトコルにて暗号化したうえで伝送する
         B) 「★1適合基準S1.1-11」で暗号化されて保存されている情報資産を伝送する

©2024 独立行政法人情報処理推進機構(IPA)

【★1適合基準S1.1-12】

よくある質問

2. ユーザがアクセス可能な媒体において、保護された通信環境（VPN環境や専用線を経由した接続環境）においてのみ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。

- 対象外となるための条件
  - 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
    → 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
- 補足説明
  - **インターネットとは通信ができない環境下においても保護対策は必要ですか？**
    → ★1では、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であり、かつ入室管理されたエリアやWPA2/WPA3によって接続機器が制限された等の利用環境であれば、その環境下に限り「保護された通信環境」とみなす。したがって、**「インターネット側からの通信を遮断する機器により保護された通信環境に接続して利用する」旨の注意を明示することを条件に保護対策済みとみなす**
  - **工事設置時に保護対策を有効化する（設置前はデフォルト無効）運用を行うことは問題ないですか？**
    → **「デフォルト有効」であることが原則。ただし、「工事設置業者の設置が前提（工事設置業者又はシステム管理者以外が設置しない）」及び「設置時の設定で「保護対策を有効化」するように作業指示書等に注意・警告表示」されている場合に限り、保護対策が行われているとみなす。**

©2024 独立行政法人情報処理推進機構（IPA）

【★1適合基準S1.1-13】

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。

©2024 独立行政法人情報処理推進機構(IPA)

【★1適合基準S1.1-13】

- 評価手法
  - 【ドキュメント評価】
    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が無効化されていること、及び攻撃を受けるリスクが高いが利用上の必要性があって無効化していないインタフェースに対する管理プロセスを有することを技術文書で評価する
    - ◆【評価項目】
      評価項目1～3すべてについて確認する
      1. 技術文書にIoT製品が有効にしている以下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：開放対象のポート番号、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
         B）Bluetoothプロファイル：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
         C）USBクラス：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
      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、それに関する情報が技術文書に明示されていること。
      3. 攻撃に悪用されるリスクの特に高いポート（例：TELNET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を有していることの記載が技術文書にあること。

©2024 独立行政法人情報処理推進機構（IPA）

【★1適合基準S1.1-13】

- 【実機テスト】
  脆弱性スキャンツールを利用した実機テストにより、A）TCP/UDPポート、B）Bluetooth、C）USB に対して、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
  - ◆【評価項目】
    評価項目4～6すべてについて実機テストを実施し、問題がないことを確認する
    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よって確認する。
    5. 以下の実機テストを実施し、脆弱性が検出されないことを確認する。脆弱性が検出された場合は評価項目5を合わせて実施する。
       A）開放ポートについて、CVSSv3基準Severity 7.0以上の脆弱性が検出されないことの確認
       B）http/httpsプロトコルを使用する設定や機能が実装されている場合、下記URLに一覧表示される既知の脆弱性CVE-IDに該当する脆弱性が検出されないことの確認
       C）脆弱性スキャンツールによるスキャンを実施し、[検索条件]に該当する脆弱性が検出されていないことの確認
       D）推奨の脆弱性検査ツールが無い場合は、Bluetoothであれば廃止されたプロファイルを利用していないこと、USBであれば不要なデバイスクラスを無効化していることを、技術文書で確認

©2024 独立行政法人情報処理推進機構(IPA)

【★1適合基準S1.1-13】

6. 評価項目5において脆弱性が検出された場合、当該脆弱性の分析及び評価を行い、問題がないことを確認する。
   A）誤検知であること（検出された脆弱性に対応する機能が、未実装である場合など）の分析及び評価
   B）運用対策を含む対策により、既に対策済みであることの分析及び評価
   C）検出された脆弱性が、実際の利用環境おいては影響がないことを証明可能であることの分析及び評価

- 対象外となるための条件
  - 該当なし
- 補足説明
  - インタフェースの無効化の手段
    - 物理的手法による無効化は、攻撃者が容易に物理ポートにアクセスできない対策
    - 論理的手法による無効化は、攻撃者が不正にソフトウェアの構成を変更しない（新たなソフトウェア／ドライバー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対策

©2024 独立行政法人情報処理推進機構(IPA)

【★1適合基準S1.1-14】

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。）

- 評価手法
  - 【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
    - 【評価項目】
      評価項目1、2両方について実機テストを実施し、問題がないことを確認する
      1. 電源供給の停止後に電源を復帰させても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。
      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。

©2024 独立行政法人情報処理推進機構（IPA）

【★1適合基準S1.1-14】

- 対象外となるための条件
  - 該当なし
- 補足説明
  - 特になし

©2024 独立行政法人情報処理推進機構(IPA)

【★1適合基準S1.1-15】

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。

- 評価手法
  - 【ドキュメント評価】
    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技術文書で評価する
    - ◆【評価項目】
      1. 上記適合基準での①についてのデータ削除方法が、マニュアル等のユーザがアクセス可能な媒体に明示されていることを確認する。

©2024 独立行政法人情報処理推進機構（IPA）

【★1適合基準S1.1-15】

よくある質問

- 【実機テスト】
  ユーザに提示された手順に従ってデータが実際に消去できること、及びデータ消去後にファームウェア(ソフトウェア)パッケージのバージョンが変わらないことを評価する
  - ◆【評価項目】
    評価項目2、3両方について実機テストを実施し、問題がないことを確認する
    2. ユーザに提示された手順に従って、上記適合基準①についてのデータが実際に消去される。
    3. 上記評価項目2の評価を行った後も、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。

■ 対象外となるための条件
- 該当なし

■ 補足説明
- **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

©2024 独立行政法人情報処理推進機構(IPA)

【★1適合基準S1.1-16】

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。

©2024 独立行政法人情報処理推進機構(IPA)

【★1適合基準S1.1-16】

- 評価手法
  - 【ドキュメント評価】
    ユーザがアクセス可能な媒体において、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
    - ◆【評価項目】
      評価項目1、2両方について確認する
      1. 上記適合基準での①③④⑤すべての情報がユーザがアクセス可能な媒体において明示されている。
      2. セキュリティアップデートのリリース時に、上記適合基準②に関する情報を作成し、周知するための仕組み及び実施方法について技術文書に記載されている。
- 対象外となるための条件
  - 該当なし
- 補足説明
  - 特になし

©2024 独立行政法人情報処理推進機構(IPA)

©2024 独立行政法人情報処理推進機構(IPA)