経済産業省

資料３

一部非公開・
構成員限り

IoT製品に対するセキュリティ適合性評価制度に関する実証について

2024年 3月 4日

本日の議題

【ご報告事項】

- **適合性評価の実証結果について（資料3）**
- 各レベル（☆１～☆４）の位置付け（資料4）
- 調達者の本制度活用に関する調整状況（資料4）
- 本制度の賛同団体（資料4）

【ご議論いただきたい事項】

- 有効期限の設定（資料4）
- 本制度のロードマップ案（資料4）
- 最終とりまとめ案（資料5）

１．今年度の実証の概要

２．評価検証の実施結果

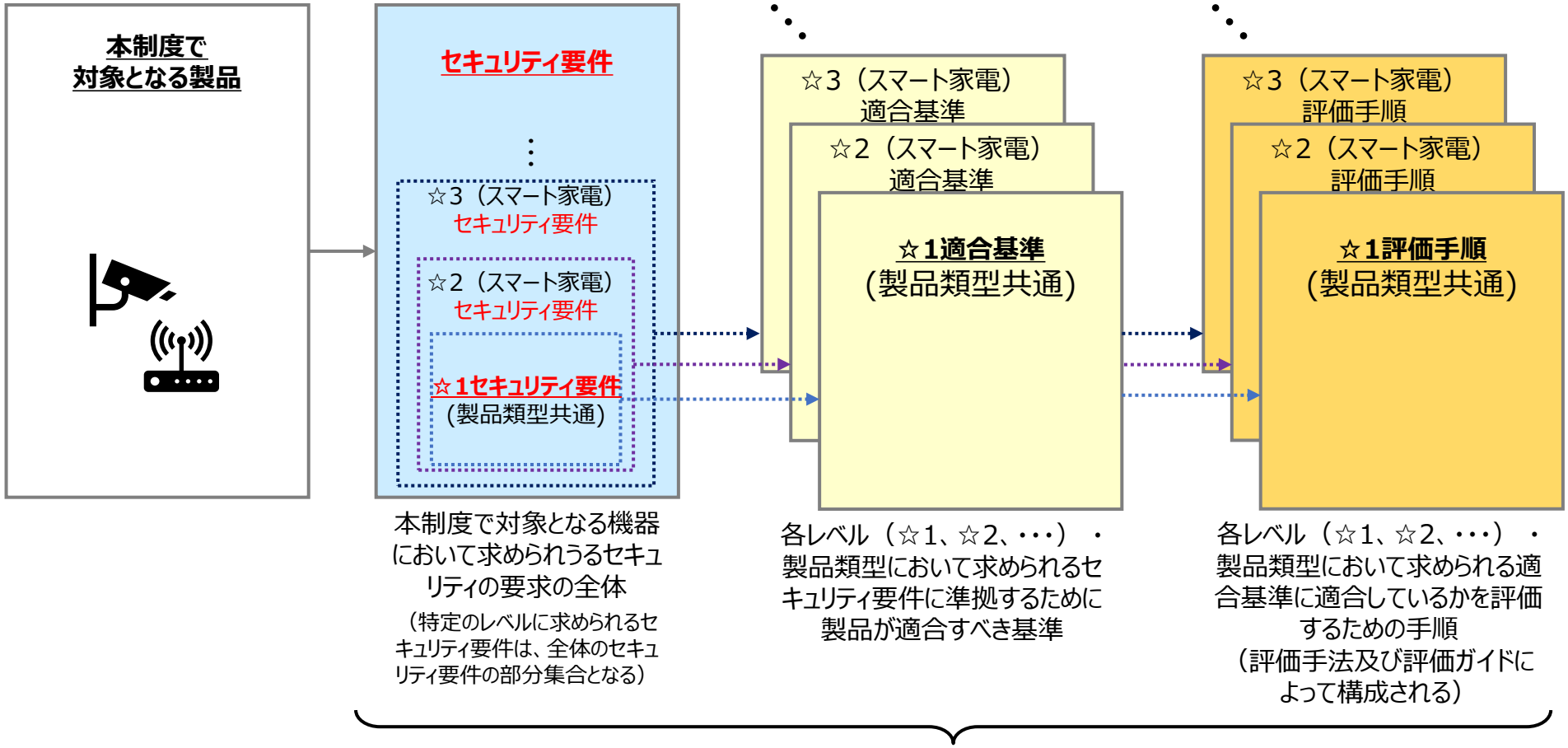
３．実証に関するまとめ・今後の予定

参考資料

適合性評価に関する実証の概要

第5回検討会（2023年10月3日）
資料3(P.3)一部修正

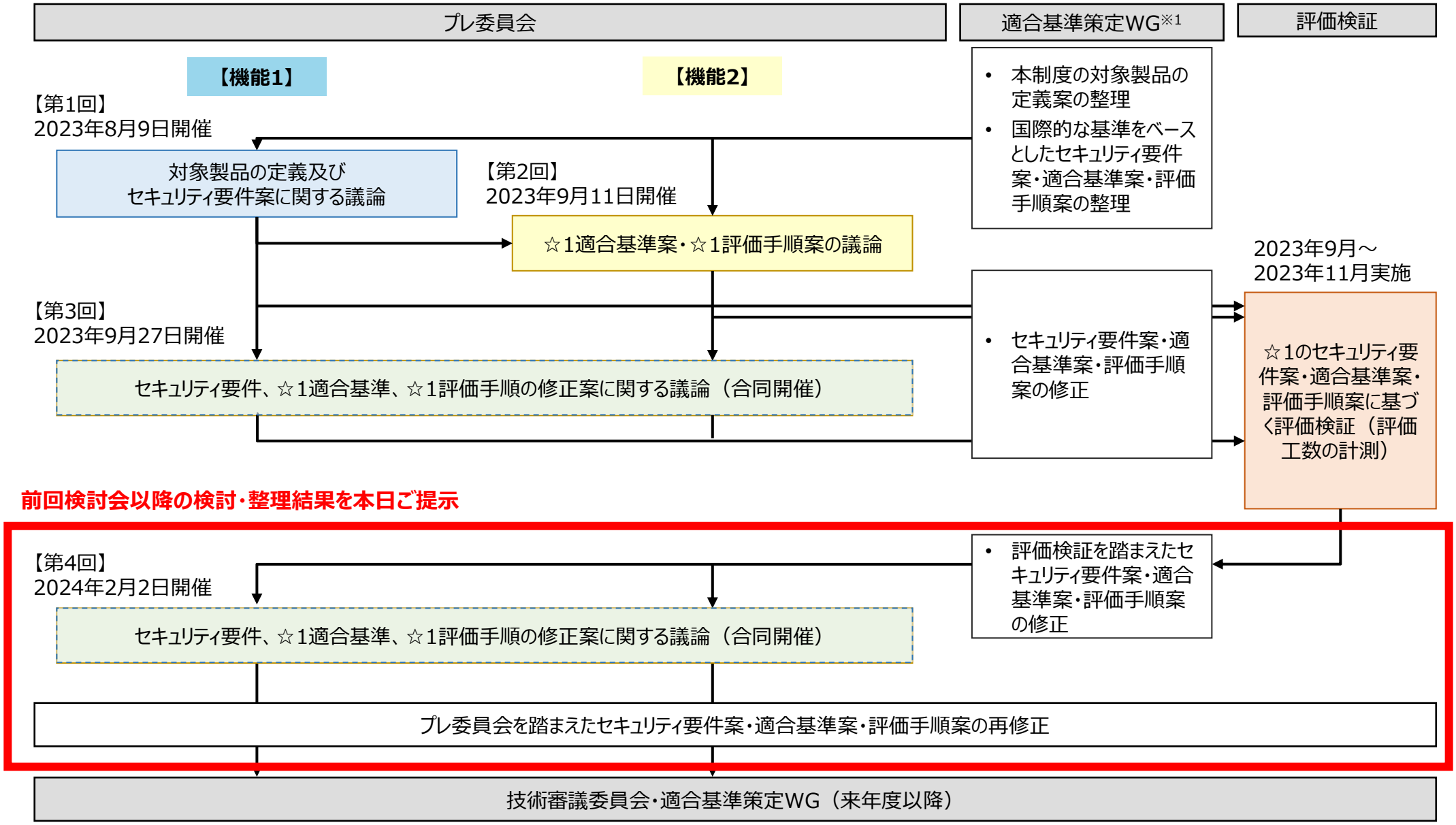
- 今年度、実際の製品に対する適合性評価の評価検証を行い、関係者にどの程度のコストが発生しうるかを検証した。
- プレ委員会を設置し、☆1（最も低レベルの評価基準）のセキュリティ要件案・適合基準案・評価手順案を議論・策定し、これらに基づき、実際のIoT製品に対する適合性評価の評価検証を行った。
- そして、評価検証結果を踏まえ、要件や基準等の見直しを行った。
- なお、これまで「要求基準」と呼称していた項目について、基準を示しているものではなく、誤解を招くおそれがあるところ、**「Security Requirement」に対応する名称として「セキュリティ要件」に変更**した。



**プレ委員会を通じて、☆1のセキュリティ要件案・適合基準案・評価手順案を作成、
実際の製品に対する評価検証を実施した。
そして、評価検証結果を踏まえて、要件や基準等の見直しを行った。**

実証プロセス

第5回検討会（2023年10月3日）
資料3(P.6)一部修正



※1 今年度は事務局が適合基準策定WGの役割を担い、事務局にて、セキュリティ要件案・適合基準案・評価手順案の検討・作成を行う。

１．今年度の実証の概要

２．評価検証の実施結果

３．実証に関するまとめ・今後の予定

参考資料

評価検証対象製品・評価機関について

第6回検討会（2023年12月12日）
資料3(P.22)一部修正

- 9月から11月にかけて、以下に示す製品に対して、プレ委員会を通じて策定した☆1のセキュリティ要件・適合基準・評価手順に基づき、**IoT製品ベンダーによる自己評価**のほか、**検証事業者及びISO/IEC 17025に基づき認定機関より認定されたJISEC制度評価機関による第三者評価の評価検証を行った。**

評価検証対象製品

ベンダー	製品類型	主な提供先
A社	スマート空気清浄機	消費者
B社	スマート洗濯機	消費者
C社	有線LANルーター（2製品）	法人
	L2スイッチ	法人
	ワイヤレススピーカー	消費者
D社	無線LANルーター	消費者
	モバイルルーター	消費者、法人
E社	有線LANルーター	消費者
	無線LANルーター	法人

プレ委員会を通じて策定した、☆1のセキュリティ要件案・適合基準案・評価手順案案に基づき、適合性評価を実施

製品ベンダーによる自己評価

製品ベンダー自身による対象製品に対する自己評価を実施した。

検証事業者による第三者評価

検証事業者による第三者評価を実施した。

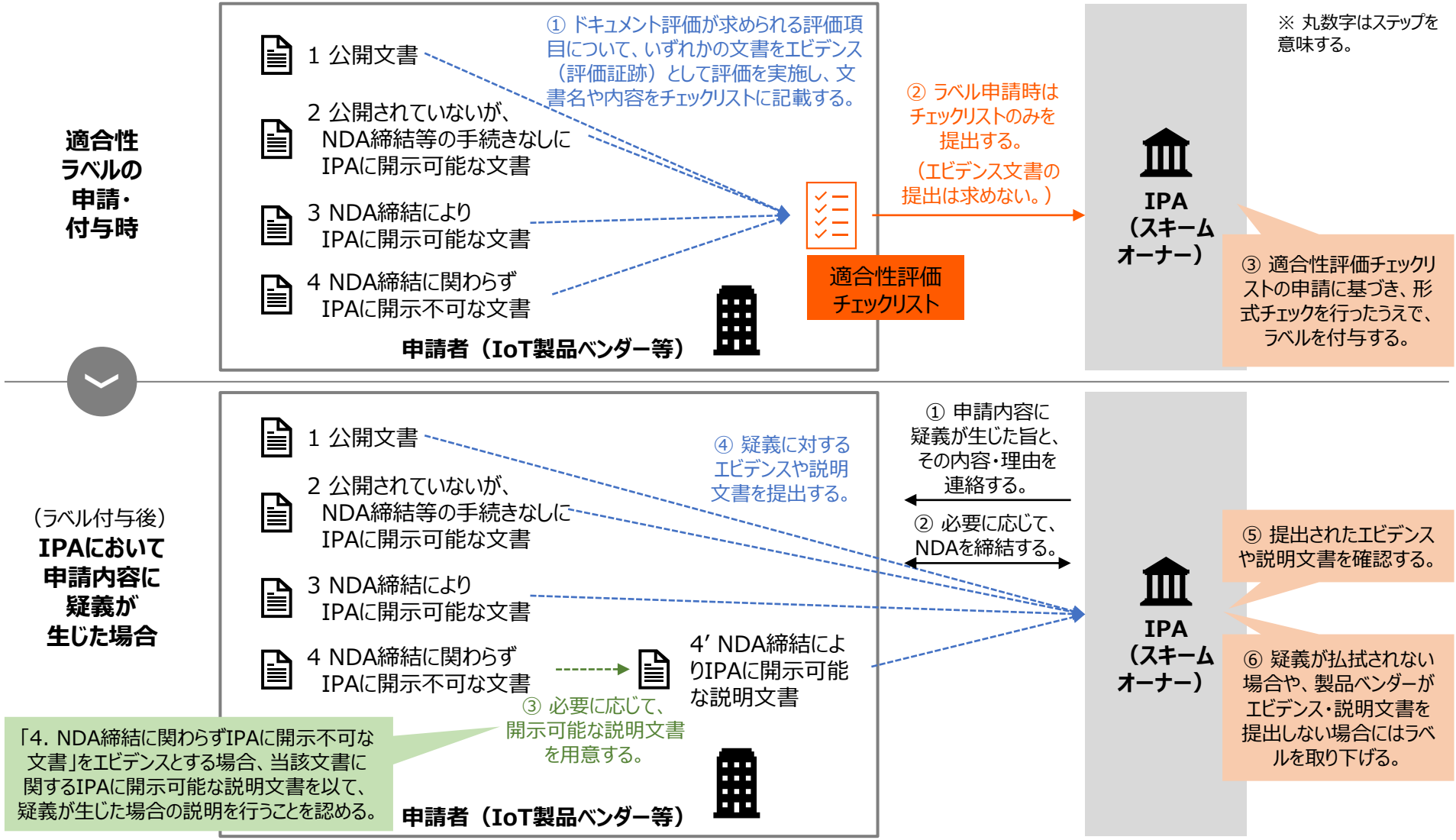
評価機関による第三者評価

ISO/IEC 17025に基づき認定されたJISEC制度の国内の評価機関による第三者評価を実施した

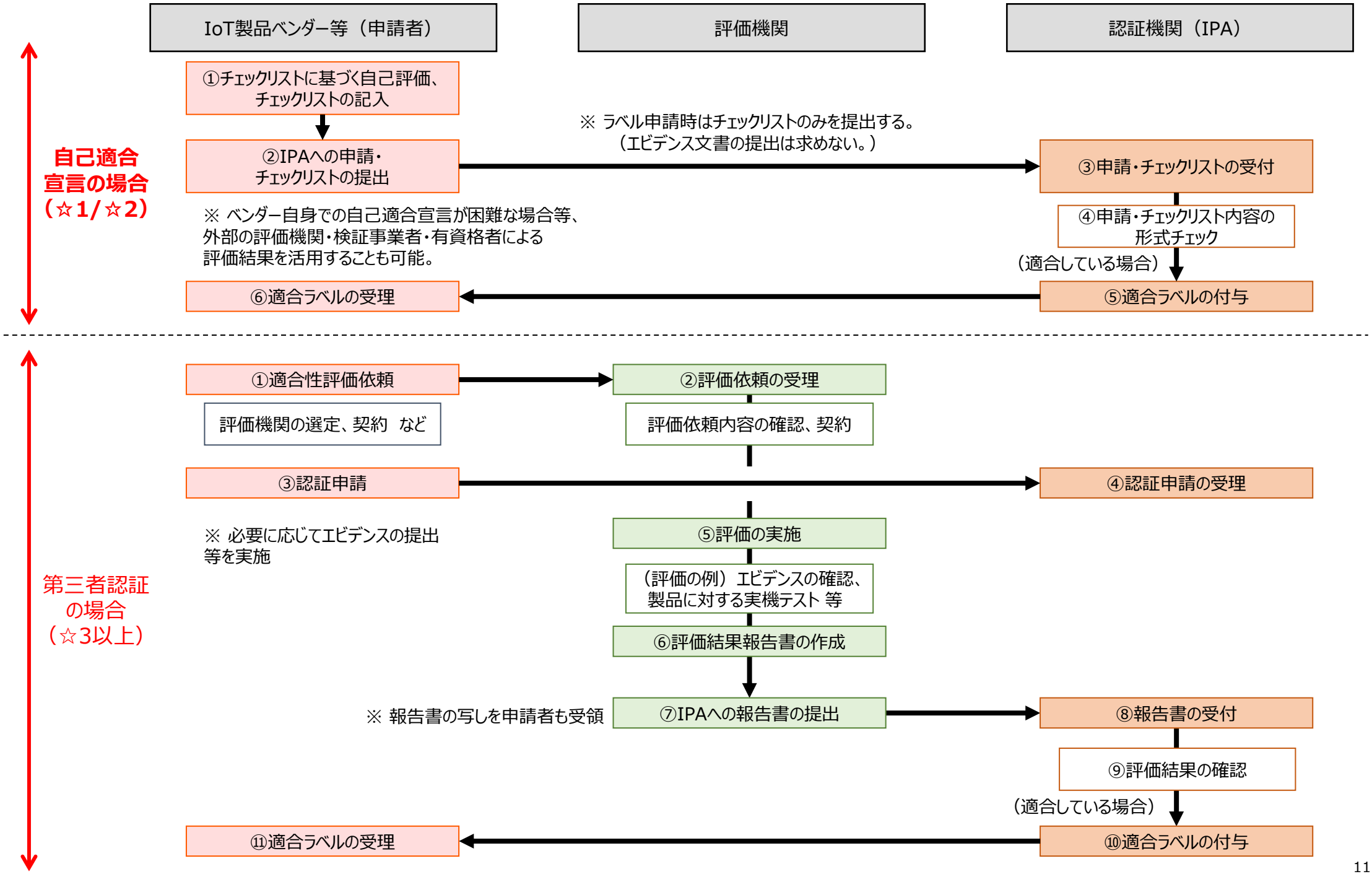
※ 全製品について、製品ベンダーによる自己評価と評価機関による第三者評価を実施。
一部の製品について検証事業者による第三者評価を実施。

☆1における文書等の取扱いについて

- ☆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ーが選択**できる形式とする。
- **ラベル申請・付与時**は、**適合性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。**
- 一方、ラベル付与後、IPAにおいて**申請内容に疑義が生じた場合、疑義に対するエビデンス文書の提出を求める**。この際、「4.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を以て、疑義が生じた場合の説明を行うことを認める**。



【参考】適合性評価・申請・ラベル付与のプロセス



FAQの策定について

- 評価検証を通じて得られた結果や指摘事項等を踏まえ、**IoT製品ベンダー、検証事業者、評価機関及びスキームオーナーの双方の負担を軽減するために、以下のような内容を含むFAQを作成する**。

大項目	中項目	FAQに追加する質問（案）
適合性評価の方法	評価方法やチェックリストの記入方法について	• 評価にあたって準備すべきことは何か。 • どのように脆弱性スキャン・ポートスキャンを行えばよいか。 • 一つでも「N」があった場合、ラベルは取得できないのか。
	評価者について	• 適合性評価は誰が実施する必要があるか。 • 第三者に評価を依頼する場合、どのようにして評価事業者を選定すればよいか。 • 第三者に評価を依頼する場合に留意すべき事項はあるか。
	エビデンスについて	• 評価に当たってのエビデンスをどのように選択する必要があるか。 • エビデンスとなる文書が存在しない場合、どのように対応する必要があるか。 • エビデンスとなる文書が第三者提供できない場合、どのように対応する必要があるか。
ラベルの申請・取得方法	申請方法について	• どのようにしてラベルの申請を行う必要があるか。 • ラベルの申請・取得に要する費用はいくらか。 • ラベルの申請時にエビデンスを添付することは必要か。
	申請内容の審査について	• 申請内容はどのように審査されるのか。 • 申請内容は誰によって審査されるのか。 • 審査はどの程度の期間を要するのか。 • 審査結果に異議がある場合に、どのような対応をすべきか。
ラベル取得後の対応	ラベルの取扱について	• 取得したラベルはどこに貼り付ける必要があるか。 • ラベルの期限はどの程度か。 • ラベルの期限が切れた場合、どのような対応をすべきか。 • ラベルを取得した製品について、利用者や調達者はどのようにして知ることができるのか。
	求められる対応について	• ラベル取得後、どのような対応が求められるか。 • 申請内容に疑義が生じた場合に追加対応が求められるとのことだが、どのような対応が生じる可能性があるか。

※ これらの項目に加え、適合性評価制度全体に係るFAQも用意する。
（質問項目例）IoT適合性評価制度とは何か、制度の運営者は誰か、☆による違いは何か、海外制度との連携はされているか、他の国内制度との連携はされているか、要件等は今後も変更する可能性があるか 等

セキュリティ要件・適合基準・評価手順の修正

- 評価検証で使用した☆1セキュリティ要件案・適合基準案・評価手順案に対し、実証参加者（製品ベンダー、検証事業者及び評価機関）及びプレ委員会の構成員より多数の指摘事項をいただいた。
- **いただいた指摘事項を踏まえ、☆1セキュリティ要件・適合基準・評価手順を修正**した。主な修正内容は以下のとおり。
  （詳細は参考資料1参照）

評価項目番号※	適合基準・評価手順の主な修正内容
1	• すべてのアクセスではなく、ユーザからの守るべき情報資産へのアクセスに対して、アクセス制御を求める適合基準に修正。 • アクセス制御の実装例を追加。
2	• 対象とするユーザ認証の仕組みについて、機器初期設定時のクライアント認証の仕組みにおいてWi-Fiパスワードやパスコードを使用する製品と、対象を明確化。 • NIST SP 800-63に基づき、パスワードの要件を明確化。
3	• 管理者以外による認証値の設定変更に関して基準を修正。
4	• 対象外（NA）となるための条件について、「ネットワークを介したユーザ認証の仕組みがない」と条件を詳細化。
5	• 評価方法に関する補足説明を追加。
6	• ファームウェア（ソフトウェア）のインストールが正常に完了したことを確認する手段に関する適合基準について、新製品では更新版のファームウェアが用意されていない可能性を踏まえ、バージョンを確認する手段を求める適合基準に修正。
7	• 参考情報及び評価方法に関する補足説明を追加。
8	• 対象とするソフトウェアアップデートの仕組みについて、ネットワーク経由でのアップデートの仕組みに対象を限定。 • 適合基準について、「ソフトウェアの完全性をアップデート前に確認できる仕組みを有すること」に修正。

評価項目番号※	適合基準・評価手順の主な修正内容
9	• 参考情報に関する補足説明を追加。
10	修正なし
11	• 製品のストレージに保存される守るべき情報資産について、セキュアに保存されることを求める適合基準に修正。（必ずしも暗号化を求めるものではない。） • 暗号化に関する保護対策例を明確化。
12	• インターネット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行われていることを求める適合基準に修正。 • 暗号化に関する保護対策例を明確化。
13	• 脆弱性診断の方法、脆弱性スキャンツールの使い方に関する補足説明を追加。 • 攻撃に悪用されるおそれのあるTCP23（telnet）の停止を明示的に追加。
14	• 電気通信事業法に基づく技術基準適合認定を受けた製品は、その認定を以て、適合基準への適合を認めることを明記。
15	• 実機テストに関する補足説明を追加。
16	• 免責事項の周知に関して、「アップデートを行わなかったときに想定される事故や障害・一般的に想定される事故や障害」に対する免責事項と、対象を明確化。 • サポート期限やサポート終了時の方針に関して、「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」と、どちらかの対応を求める表現に明示的に修正。

※ 実証参加者の指摘を踏まえ、実証段階から評価項目番号の＃1と＃2を入れ替えていることに留意。

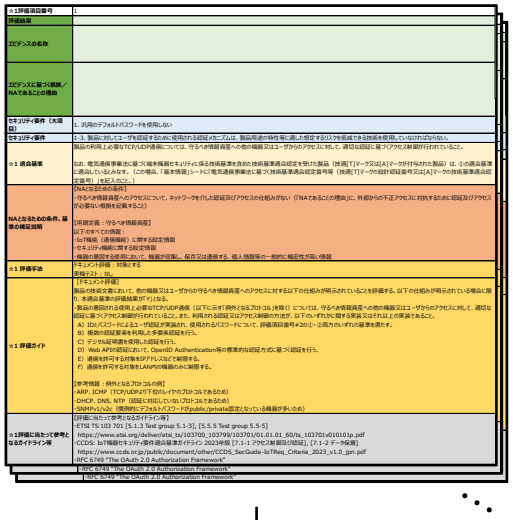
☆1適合性チェックリストについて

- 制度運用開始以降に活用する☆1適合性チェックリストについて、参考資料2に示すとおり作成した。

☆1適合性チェックリストの構造
（詳細内容は参考資料２を参照）

はじめに

基本情報



※「基本情報」シートの内容が転写されます。

申請企業の名称	0
製品の名称	0
製品の型式番号	0
製造国又は地域	0
適合宣言者の所属企業名称	0
適合宣言日	1900/1/0

適合確認

※ YESと表示されない場合、ラベル申請はできません。

☆1評価項目番号	セキュリティ要件（大項目）	セキュリティ要件	☆1 適合基準	NAとなるための条件、基準の補足説明	評価結果	エビデンスの名称	エビデンスに基づく根拠
1	1. 汎用のデフォルトパスワードを使用しない	1-3. 製品に対してユーザを認証するために使用される認証メカニズムは、製品用途の特性等に適した想定するリスクを低減できる技術を使用していなければならない。	製品の利用上必要なTCP/UDP通信については、守るべき情報資産への他の機器又はユーザからのアクセスに対して、適切な認証に基づくアクセス制御が行われていること。 なお、電気通信事業法に基づく端末機器セキュリティに係る技術基準を含めた技術基準適合認定を受けた製品（技適[T]マーク又は[A]マークが付与された製品）は、①の適合基準に適合しているとみなす。（この場合、「基本情報」シートに「電気通信事業法に基づく技術基準適合認定番号等（技適[T]マークの設計認証番号又は[A]マークの技術基準適合認定番号）」を記入のこと。）	【NAとなるための条件】 ・守るべき情報資産へのアクセスについて、ネットワークを介した認証及びアクセスの仕組みがない（「NAであることの理由」に、外部からの不正アクセスに対抗するために認証及びアクセスが必要ない根拠を記載すること） 【用語定義：守るべき情報資産】 以下のすべての情報： ・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において、機器が収集し、保存又は通信する、個人情報等の一般的に機密性が高い情報	-	-	-
2	1. 汎用のデフォルトパスワードを使用しない	1-2. プリインストールされた固有のパスワードを使用する場合、自動化された攻撃への耐性をもつために、パスワードは十分なランダム性を保有しなければならない。	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、又は、機器初期設定時のクライアント認証の仕組みにてパスワードやパスコードを使用する製品において、製品導入時にデフォルトパスワードが使用される場合に、以下の①・②のいずれかの基準を満たすこと。 ① デフォルトパスワードは、製品毎に異なる一意の値で、容易に推測可能でない6文字以上のパスワードであること。 ② デフォルトパスワードは、初回起動時にユーザによるパスワード変更を必須とする機能を実装し、当該機能において設定可能なパスワードとして、8文字以上のパスワードの設定を強制させること。	【NAとなるための条件】 ネットワークを介したユーザ認証の仕組みがない（「NAであることの理由」に、脅威に対抗するためにユーザ認証が必要ない根拠を記載すること）	-	-	-
				【NAとなるための条件】 ・ネットワークを介			

記載内容の反映

評価項目（#1～#16）ごとの評価シート

評価結果一覧シート

１．今年度の実証の概要

２．評価検証の実施結果

３．実証に関するまとめ･今後の予定

参考資料

実証に関するまとめ・今後の予定

- プレ委員会で議論したセキュリティ要件案・適合基準案・評価手順案に基づき、IoT製品（5ベンダー・10製品）に対して**適合性評価の評価検証を実施**し、**評価工数、基準案・手順案の妥当性、自己適合宣言による評価の妥当性等について確認を行った**。

- また、評価検証で得られた結果を踏まえて**セキュリティ要件案・適合基準案・評価手順案を修正した上で、プレ委員会で修正内容について議論を行った**。

- 今後、**①☆1のセキュリティ要件、②☆1適合基準、③各基準に対してNAとなるための条件の3点についてパブリックコメントを実施**し、**パブリックコメントを踏まえて修正した内容にて、制度を開始する**。なお、パブリックコメントにおいては、これら3点の**英語版も用意し、海外からの意見も受け付ける**。

- 来年度以降、☆2以上のセキュリティ要件、適合基準、評価手順に関する議論・検討を行う。☆2以上については、**優先度の高い製品類型について、関連する業界団体やワーキンググループと連携の上で、具体的な基準等に関して議論・検討を進める**。

１．今年度の実証の概要

２．評価検証の実施結果

３．実証に関するまとめ・今後の予定

参考資料

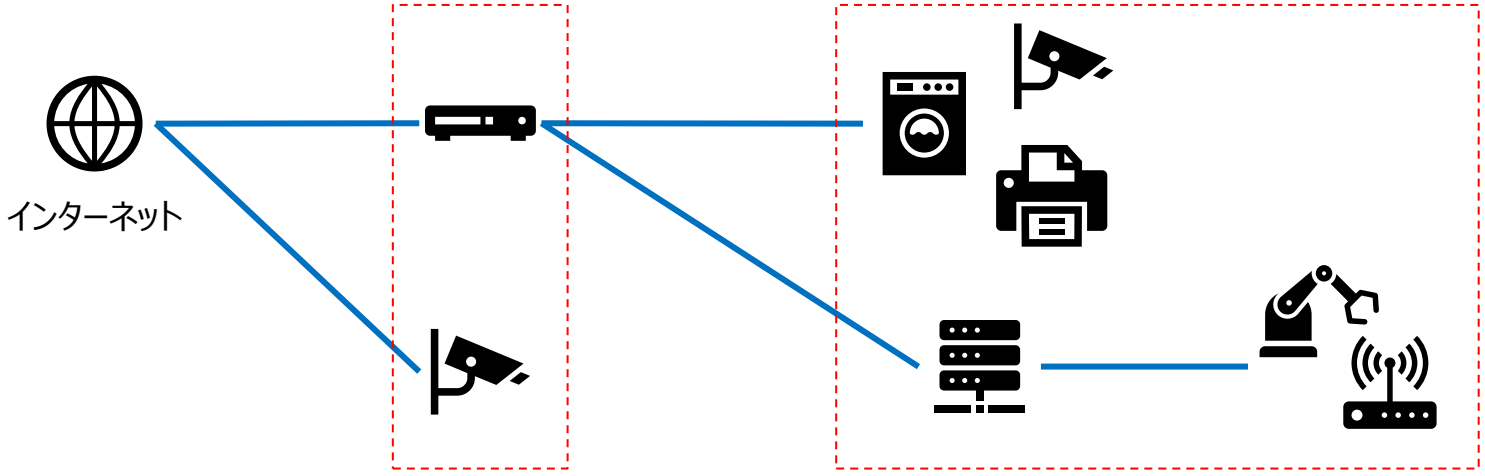
本制度における対象製品の定義

第6回親検討会（2023年12月12日）
資料3(P.6)一部修正

- 本制度では、**インターネットプロトコル（IP）を使用してデータを送受信する機能を持つ以下の機器**を対象とする。
  - **インターネットに接続可能な機器：IPを使用してインターネット上でデータを送受信する機能を持つ機器**
  - **ネットワークに接続可能な機器：IPを使用して、他の「インターネットに接続可能な製品」又は「ネットワークに接続可能な製品」に接続し、データを送受信する機能を持つ機器**
- これらを含めた対象製品※1のイメージは以下のとおり。
- ただし、広くITシステムで利用されており、利用者が任意のソフトウェアにより随時かつ容易にセキュリティ機能を変更することができる汎用的なIT製品（PC、タブレット端末等）は対象外とする※2。

※1：ETSI EN 303 645の定義を参照し、「IoT製品（IoT product）」には、IoT機器（IoT device）とその関連サービスを含む。
IoT機器とは、ネットワークに接続された（及びネットワークに接続可能な）機器で、関連サービス（IoT機器と共にIoT製品全体の一部であり、通常は製品の意図された機能を提供するために必要なデジタルサービス）との関係を持ち、電子機器として使用される機器を意味する。

※2：英国PSTI法、総務省端末設備等規則等の国内外制度も同様の理由で対象外としている。

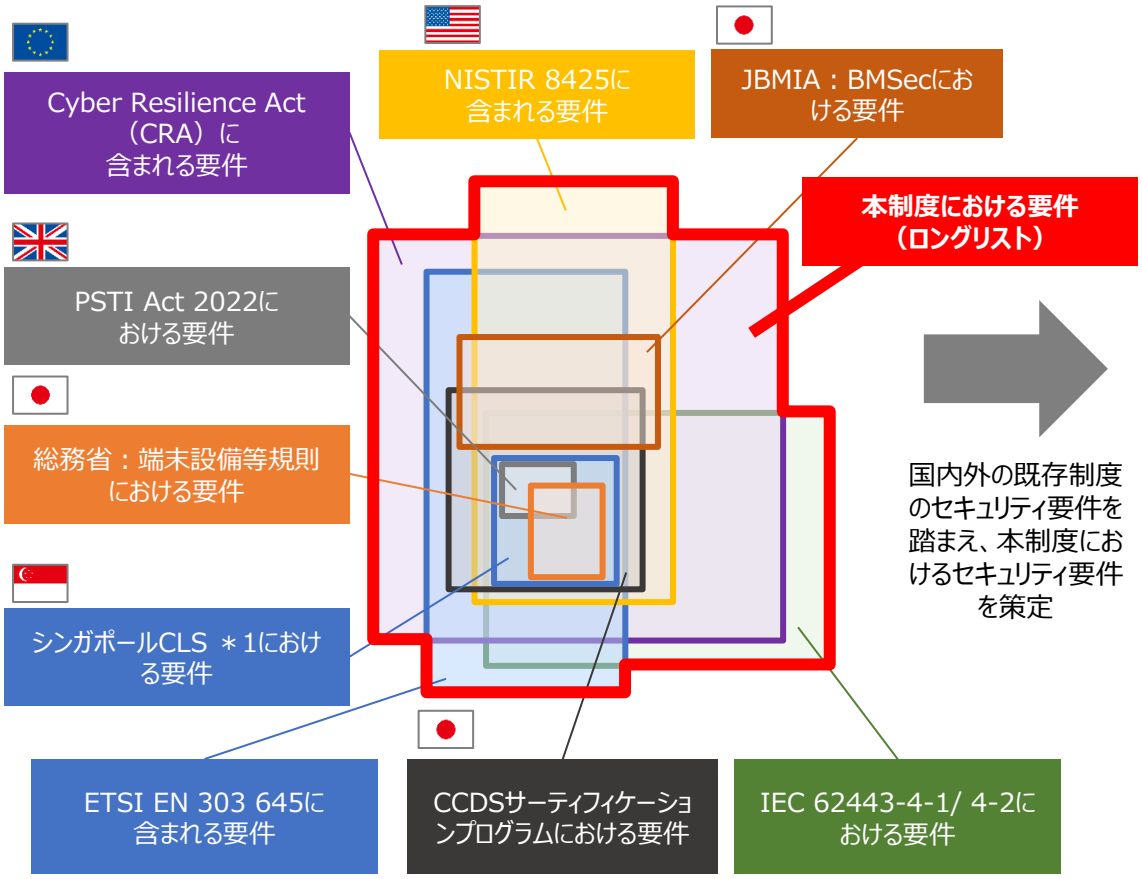


セキュリティ要件案について

第5回検討会（2023年10月3日）
資料3(P.9)一部修正

- セキュリティ要件は、本制度で対象となるIoT製品において求められうる要件の全体（ロングリスト）であるため、**ETSI EN 303 645、NISTIR 8425、EU-CRA等の国内外のセキュリティ要件の集合関係を踏まえ、重ね合わせの関係（∪（カップ））にあるセキュリティ要件のロングリストを整理した**。
- セキュリティ要件の具体的な記載について、国際的に広く活用されているETSI EN 303 645の記載を参考にしつつ、プレ委員会で挙げられた意見を踏まえ、表現の見直しを行った。なお、**今後も国際連携や国際標準の検討を見据え、表現やカテゴリ（大項目）の見直しを諮っていく**。

諸外国制度において求められるセキュリティ要件の関係性イメージ



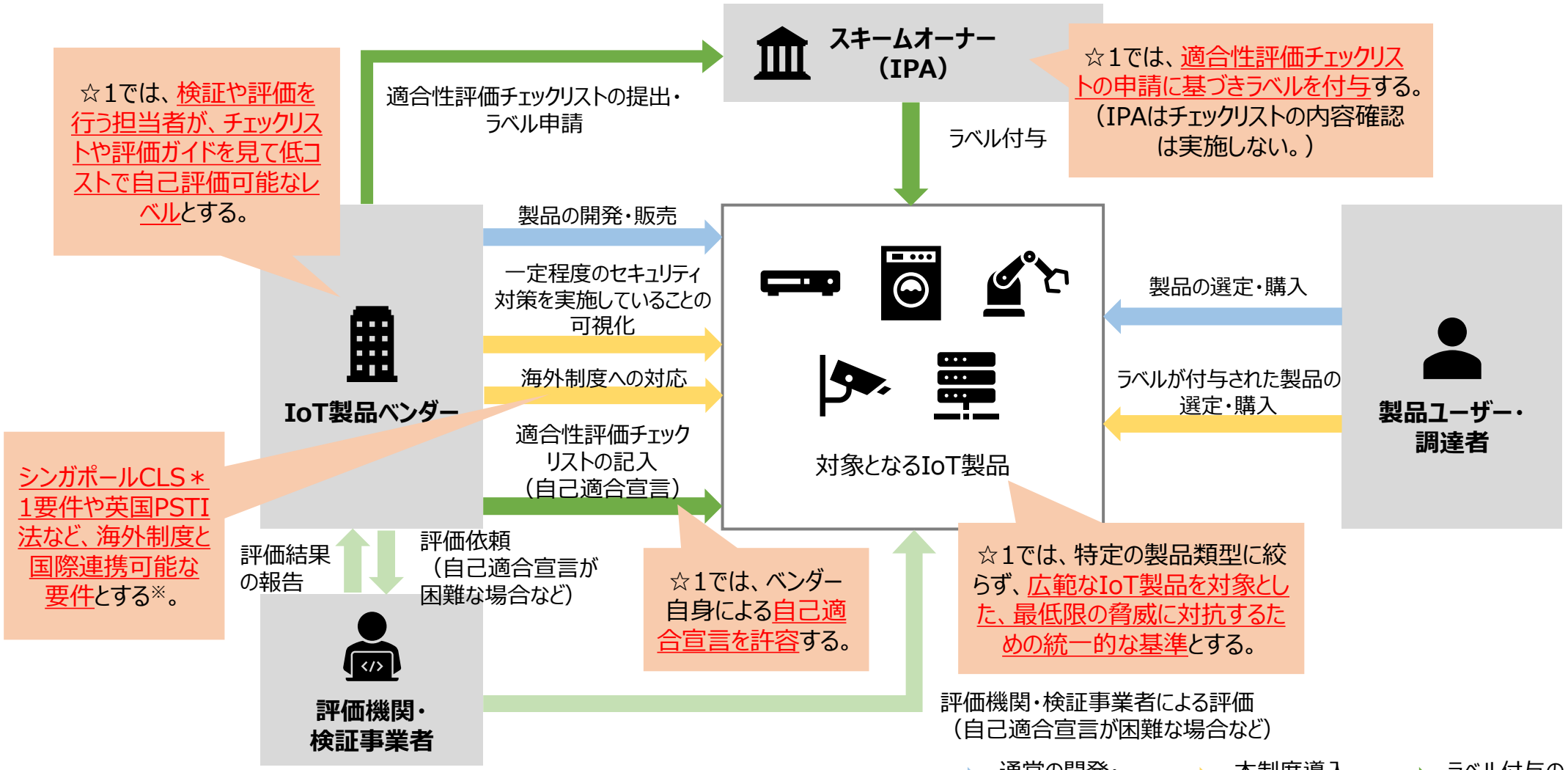
本制度におけるセキュリティ要件（ロングリスト）のイメージ

セキュリティ要件案	
1. 汎用のデフォルトパスワードを使用しない	1-1. パスワードが使用され、工場出荷時のデフォルト以外の状態にある製品において、すべてのパスワードは、製品ごとに固有であるか、又はユーザによって定義されるものでなければならない。
	1-2. プリインストールされた固有のパスワードを使用する場合、自動化された攻撃への耐性をもつために、パスワードは十分なランダム性を保有しなければならない。
	1-3. 製品に対してユーザを認証するために使用される認証メカニズムは、製品用途の特性等に適した想定するリスクを低減できる技術を使用していなければならない。
	1-4. 製品に対するユーザ認証において、製品は使用される認証値を変更するためのシンプルなメカニズムを、ユーザ又は管理者に提供しなければならない。
	1-5. 製品が、制約のある機器ではない場合、ネットワークを介して行われる認証に対する総当たり攻撃等のブルートフォース攻撃が実行できないようにするメカニズムを保有しなければならない。
2. 脆弱性の報告を管理するための手段を導入する	2-1. 製造業者は、脆弱性開示ポリシーを公開しなければならない。このポリシーには、少なくとも以下が含まれていなければならない： • 問題を報告するための連絡先情報； • 以下のタイムラインに関する情報： 1) 最初の受領確認； 2) 報告された問題が解決されるまでの状況の更新。
	…
…	…

本制度における☆1の位置付け（前提）

第6回親検討会（2023年12月12日）
資料3(P.9)一部修正

- これまでの親検討会／プレ委員会での議論を踏まえ、☆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
  - ✓ ☆1の適合基準への**評価は、低コストかつ自己宣言で対応**できる
  - ✓ ☆1の適合基準は、**海外制度と国際連携可能な基準**とする



※ 米国Cyber Trust Mark及びEU CRAの要件は現在検討中であるため、検討状況を注視しつつ、どのレベルで連携するかを検討する。

☆1で想定する守るべき資産

第6回親検討会（2023年12月12日）
資料3(P.10)一部修正

- 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、以下に示す4つの資産が挙げられる。
- これまでのプレ委員会での議論を踏まえ、**☆1で想定する守るべき資産としては、以下に限定**する。
- なお、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とする**。

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]

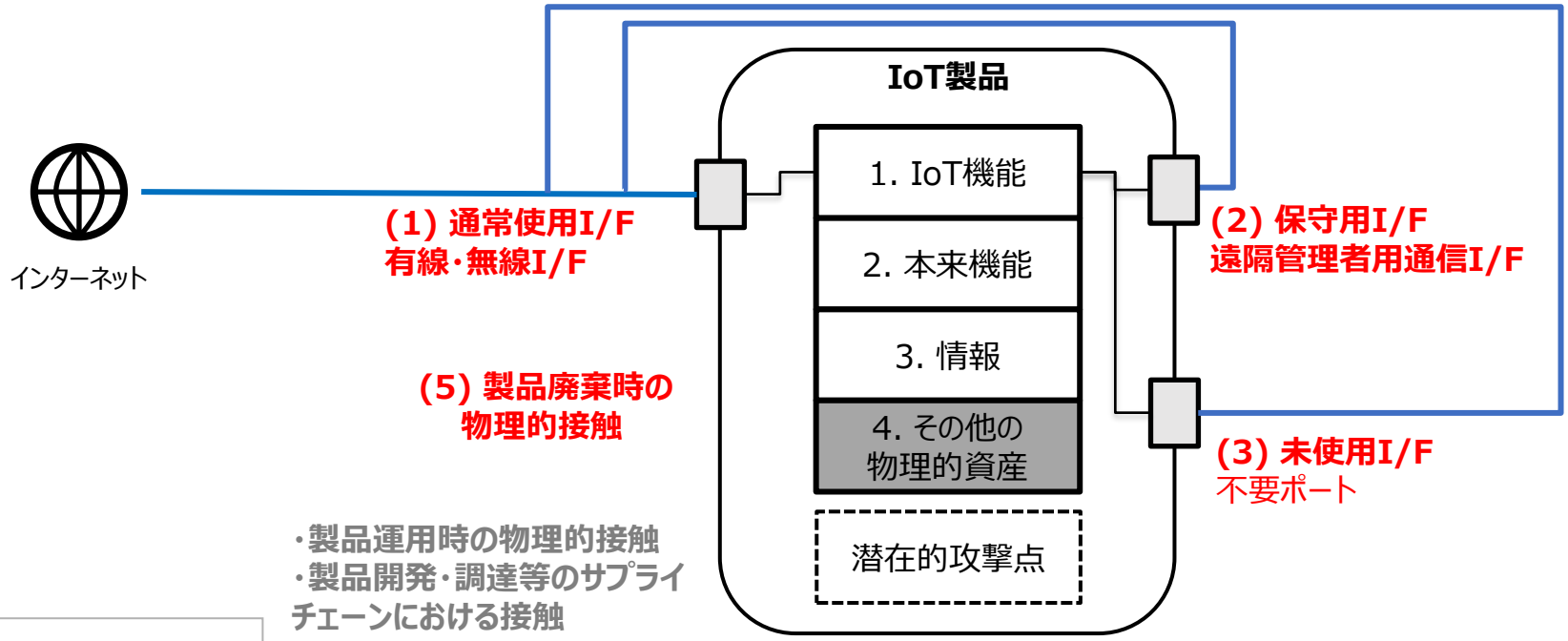
1: 例えば、エアコンであれば冷暖房、ドローンであれば飛行のような固有の機能のこと。
2: 現在の社会の価値観に基づいて、与えられた状況下で、受け入れられないリスクの発生を防ぐ機能のこと。
3: 製品もしくはシステムとともに提供される情報に従った使用、又はそのような情報がない場合には、一般的に理解されている方法による使用のこと。（JIS Z 8051：2015）
4: 個人情報に関する意図する使用を持たないが、その機器によって扱われる情報に個人情報が含まれうる機器の場合、想定される運用環境において盗聴の脅威に関して許容不可能な脅威がある場合に限り、対象情報を保護資産として扱う。例えば、防犯カメ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

☆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が想定**される。

※ 本制度における☆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。



【凡例】

赤字： 想定するアタックサーフェス

灰字： ☆1では想定しないアタックサーフェス

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。

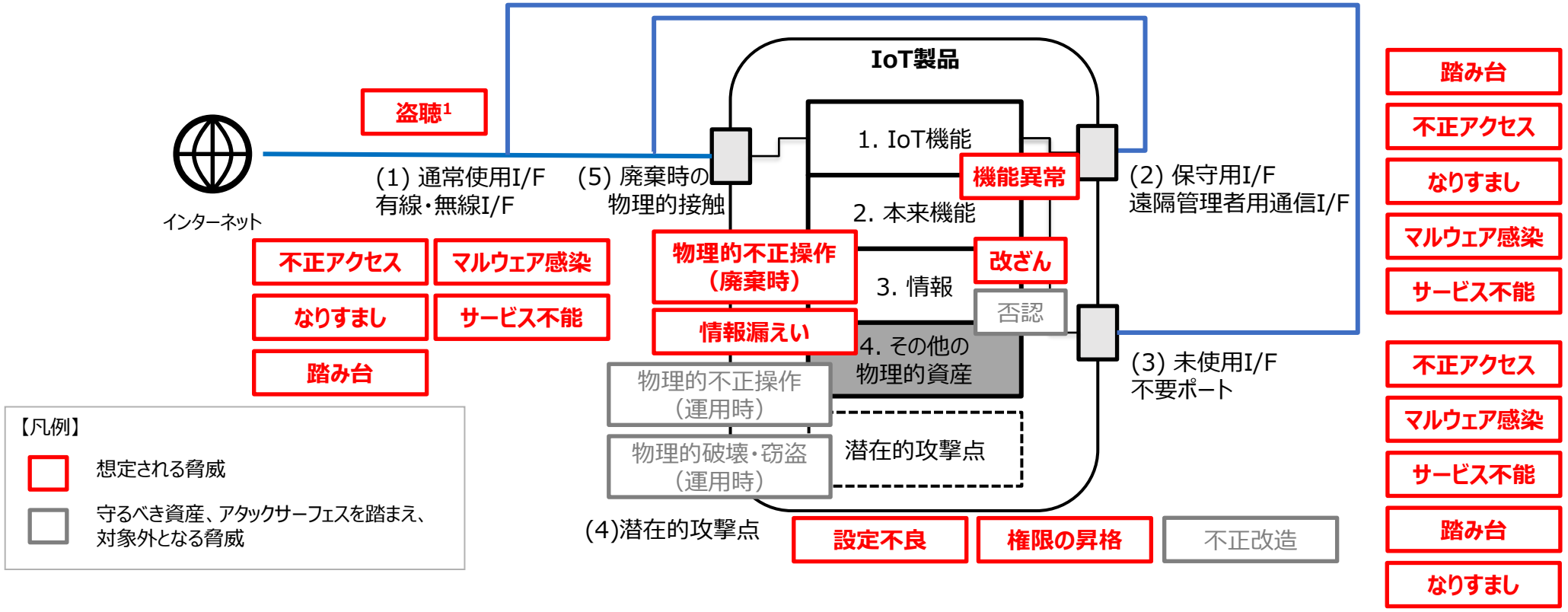
出所）IPA つながる世界の開発指針 第2版 https://www.ipa.go.jp/publish/qv6pgp000000114a-att/000060387.pdf
CCDSサーティフィケーションプログラム IoT機器に対するリスク分析のガイド https://www.ccds.or.jp/certification/document/ccds_risk-analysis-process.pdf

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は、一例として以下のようにマッピングできる。なお、脅威は、IPA文書及びCCDS文書を参照して整理した。

※ ☆1では「製品運用時の物理的接触」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）」や「物理的破壊・窃盗（運用時）」の脅威は対象外としている。同様に、「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、「不正改造」の脅威は対象外としている。

※ また、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、当該脅威は対象外としている。

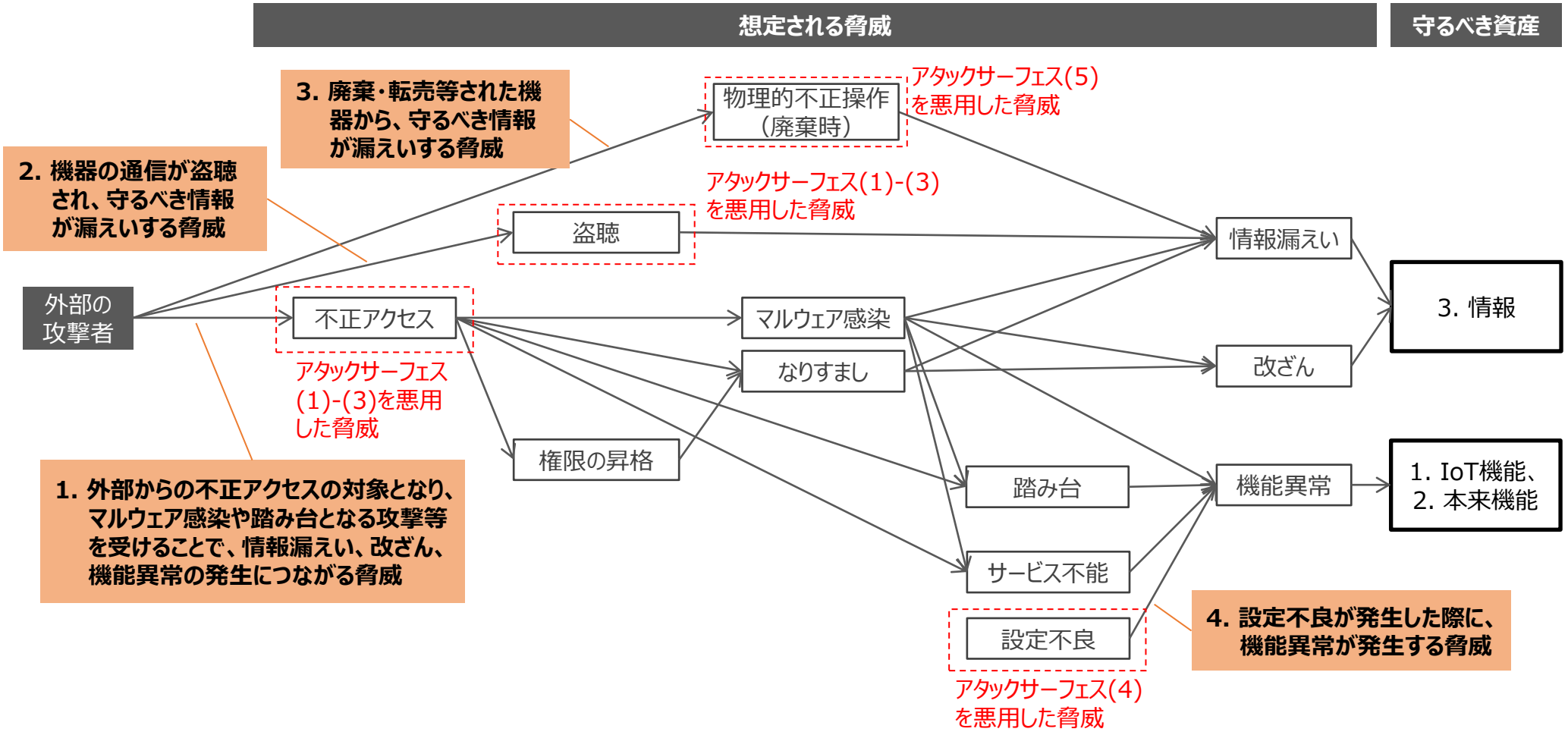


1: 保護されたネットワーク内で使用することを意図した機器については、「盗聴」の脅威は限定的であることに留意。

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

想定される脅威と守るべき資産との関係性

- 外部の攻撃者が☆1で想定する守るべき資産に影響を与えるための脅威のプロセス（ロジックモデル）は以下のように整理できる。
- 本プロセスに基づき、外部の攻撃者が最初に悪用する脅威を踏まえると、**対応すべき脅威は4つの脅威に集約**される。



参考）IPA 制御システムの脅威分析ガイド 第2版 https://www.ipa.go.jp/security/controlsystem/riskanalysis.html

☆1で考慮すべき主な脅威

第6回親検討会（2023年12月12日）
資料3(P.14)一部修正

- 前頁で示した4つの脅威に対して対応すべきである一方で、☆1の位置付けを踏まえると、すべての脅威への対応を求めることは困難と想定されるため、☆1で考慮する主な脅威として、条件の絞り込みを行った。
- これまでのプレ委員会で挙げられた近年のセキュリティ脅威や海外制度を踏まえ、**☆1で考慮する主な脅威として、以下の脅威に絞り込みを行った**。

【近年のIoTに関するセキュリティ脅威※】
- MiraiやMirai亜種による攻撃
- 自動化された攻撃によるマルウェア感染
- 正規のID・パスワードを用いた侵入
- 踏み台による他の機器への攻撃

※ これまでのプレ委員会での意見に基づく

【☆1の位置付け（実現すべき事項）の概要】
- 最低限の脅威に対抗できる
- 低コストで自己評価できる
- 一部の海外制度の基準を包含する

☆1で考慮する主な脅威の絞り込み

想定される脅威（前頁より）	☆1で考慮する主な脅威	☆1での絞り込みの理由
1. 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	1. ①弱い認証機能、②脆弱性の放置、③未使用インタフェースの有効化により、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	すべての不正アクセスの脅威に対する対策を☆1で求めることは過大であると考えられるため。一方で、近年のセキュリティ脅威の状況や海外制度等を踏まえ、弱い認証機能、脆弱性の放置、未使用インタフェースの有効化に起因する脅威に対しては、最低限対策が必要と考えられるため。
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	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	–
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	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	–
4. 設定不良が発生した際に、機能異常が発生する脅威	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	海外制度等を踏まえ、すべての設定不良への対策を☆1で求めることは過大であり、最低限、総務省の端末設備等規則で求められる対策が必要と考えられるため。

※ 下線部分が「想定される脅威」との差分

脅威に対抗するために☆1で実現すべき対策

第6回親検討会（2023年12月12日）
資料3(P.15)一部修正

- ☆1で考慮すべき主な4つの脅威に対し、**製品／製品ベンダーにおいて実現すべき対策として、☆1の位置付けや海外制度の基準等を踏まえ、以下に示す対策が想定**される。

☆1で考慮すべき主な脅威（前頁より）			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		製品ベンダーにおける対策	
			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	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	–	–

☆1セキュリティ要件案（1/2）

大項目	☆1セキュリティ要件案	☆1での抽出理由
1. 汎用のデフォルトパスワードを使用しない	1-1. パスワードが使用され、工場出荷時のデフォルト以外の状態にある製品において、すべてのパスワードは、製品ごとに固有であるか、又はユーザによって定義されるものでなければならない。	脅威1-①に対応するために、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ことが求められるため。
	1-2. プリインストールされた固有のパスワードを使用する場合、自動化された攻撃への耐性をもつために、パスワードは十分なランダム性を保有しなければならない。	脅威1-①に対応するために、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ことが求められるため。
	1-3. 製品に対してユーザを認証するために使用される認証メカニズムは、製品用途の特性等に適した想定するリスクを低減できる技術を使用していなければならない。	脅威1-①に対応するために、セキュアな認証の仕組みを提供することが求められるため。
	1-4. 製品に対するユーザ認証において、製品は使用される認証値を変更するためのシンプルなメカニズムを、ユーザ又は管理者に提供しなければならない。	脅威1-①に対応するために、セキュアな認証の仕組みを提供することが求められるため。
	1-5. 製品が、制約のある機器ではない場合、ネットワークを介して行われる認証に対する総当たり攻撃等のブルートフォース攻撃が実行できないようにするメカニズムを保有しなければならない。	脅威1-①に対応するために、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ことが求められるため。
2. 脆弱性の報告を管理するための手段を導入する	2-1. 製造業者は、脆弱性開示ポリシーを公開しなければならない。このポリシーには、少なくとも以下が含まれていなければならない ・問題を報告するための連絡先情報 ・以下のタイムラインに関する情報 1) 最初の受領確認 2) 報告された問題が解決されるまでの状況の更新	脅威1-②に対応するために、製品に関する情報及び製品の脆弱性に関する情報を提供することが求められるため。
3. ソフトウェアを最新の状態に保つ	3-1. 製品に含まれる特定のソフトウェアコンポーネントについて、アップデート可能にしなければならない。	脅威1-②に対応するために、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ことが求められるため。
	3-2. 製品が、制約のある機器でない場合、アップデートをセキュアにインストールするためのアップデートメカニズムを備えていなければならない。	脅威1-②に対応するために、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ことが求められるため。
	3-3. 製品においてアップデートメカニズムが実装されている場合、そのアップデートは、ユーザが簡単に適用できるものでなければならない。	脅威1-②に対応するために、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ことが求められるため。
	3-7. 製品においてアップデートメカニズムが実装されている場合、セキュアなアップデートメカニズムを容易にするために、ベストプラクティスの暗号技術を使用しなければならない。	脅威1-②に対応するために、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ことが求められるため。
	3-8. 製品においてアップデートメカニズムが実装されている場合、セキュリティアップデートは、適時でなければならない。	脅威1-②に対応するために、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ことが求められるため。
	3-10. 製品においてアップデートメカニズムが実装され、ソフトウェアアップデートがネットワークインタフェースを介して配信される場合、製品は、信頼関係を介して各アップデートの真正性及び完全性を検証しなければならない。	脅威1-②に対応するために、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ことが求められるため。
	3-16. 製品のモデル名称は、製品上のラベル又は物理的インタフェースを介して、ユーザに対して明確に認識可能でなければならない。	脅威1-②に対応するために、製品に関する情報及び製品の脆弱性に関する情報を提供することが求められるため。

（次ページに続く）

☆1セキュリティ要件案（2/2）

大項目	☆1セキュリティ要件案	☆1での抽出理由
4. 機密セキュリティパラメータをセキュアに保存する	4-1. 製品のストレージにある機密セキュリティパラメータは、製品によってセキュアに保存されなければならない。	脅威1に対応するために、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ことが求められるため。
5. セキュアに通信する	5-1. 製品は、ベストプラクティスの暗号技術を使用してセキュアに通信をしなくてはならない。	脅威2に対応するために、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ことが求められるため。
	5-5. ネットワークインタフェースを介してセキュリティに関連する設定の変更を可能にする製品の機能は、認証後にのみアクセス可能でなければならない。ただし、製品が依存するネットワークサービスプロトコルで、製品の動作に必要な設定を製造業者が保証できない場合は、例外とする。	脅威1-①に対応するために、セキュアな認証の仕組みを提供することが求められるため。
	5-7. 製品は、リモートアクセス可能なネットワークインタフェースを介して通信される重要なセキュリティパラメータの機密性を保護しなければならない。	脅威2に対応するために、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ことが求められるため。
6. 露出した攻撃面を最小化する	6-1. すべての未使用のネットワークインタフェース及び論理インタフェースは無効化しなければならない。	脅威1-③に対応するために、不要なインタフェースを無効化することが求められるため。また、脅威1-②に対応するために、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ことが求められるため。
9. 停止に対してレジリエントなシステムにする	9-1. データネットワークと電源の停止の可能性を考慮して、レジリエンスを製品とサービスに組み込まなければならない。	脅威4に対応するために、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ことが求められるため。
11. ユーザが簡単にデータを消去できるようにする	11-1. ユーザは、簡単な方法で製品からユーザデータを消去できるような機能を提供されなければならない。	脅威3に対応するために、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ことが求められるため。
17. 製品に関する情報提供を行う	17-2. 製造業者は、製品をセキュアに設定・利用・廃棄する方法について、ユーザに提供しなければならない。	脅威1-①に対応するために、製品のセキュアな利用方法に関する情報を提供することが求められるため。
	17-3. アップデートメカニズムが実装されている場合、製造業者は、セキュリティアップデートが必要であることを、そのアップデートによって軽減されるリスクに関する情報とともに、認識可能で明らかな方法でユーザに通知しなければならない。	脅威1-②に対応するために、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ことが求められるため。
	17-5. 製造者等は、ユーザが製品を廃棄する手順について、指定された方法でユーザに提供しなければならない。	脅威3に対応するために、製品のセキュアな廃棄方法に関する情報を提供することが求められるため。
	17-8. 製造業者は、定められたサポート期間を、ユーザにとって明確で透明性のある方法で公表しなければならない。	脅威1-①に対応するために、製品のセキュアな利用方法に関する情報を提供することが求められるため。
	17-10. 製造者等は、脅威を引き起こす可能性がある製品の利用状況に関する情報について、指定された方法でユーザに提供しなければならない。	脅威1-①に対応するために、製品のセキュアな利用方法に関する情報を提供することが求められるため。