経済産業省

特定分野システムのIoT製品における JC-STAR制度活用ガイド （1.1版）

2025年3月

経済産業省 商務情報政策局
サイバーセキュリティ課

はじめに

【本ガイドの位置づけ】

本ガイドは、特定の分野や業界において類似の汎用的な構成で利用されるシステム（以下、特定分野システム）に組み込まれて調達され、利用されるようなIoT製品に対するセキュリティ要件を定め、IoT製品に対するセキュリティ要件適合評価及びラベリング制度（JC-STAR制度）[1]の活用を検討する際に参考となる情報を提供します。

〔特定分野システムの例〕

- ✓ スマートホームシステム
- ✓ 工場システム
- ✓ ビルシステム

【本ガイドの想定利用者】

- IoT製品が組み込まれている特定分野システムのセキュリティを検討している業界団体やワーキング・グループ（WG）など

1: IPA「セキュリティ要件適合評価及びラベリング制度（JC-STAR）」 https://www.ipa.go.jp/security/jc-star/index.html

JC-STAR制度の概要

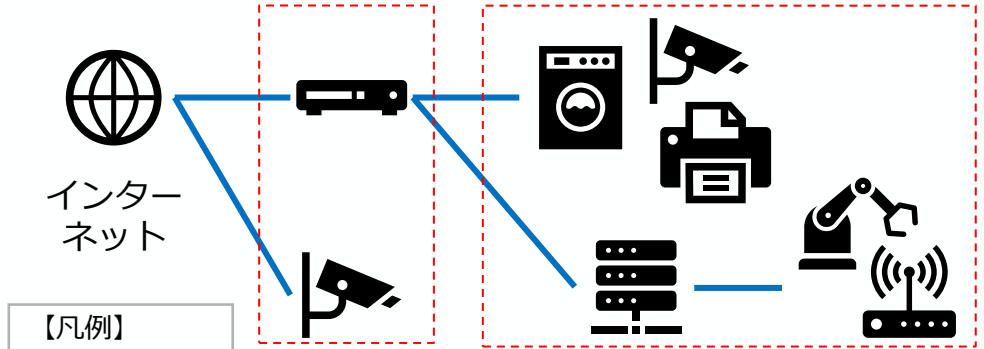
- 2022年11月より検討会[1]を開催し、2024年3～4月のパブリック・コメントを経て、8月に制度構築方針[2]を公表しました。それに従い、9月30日にIPAから**「JC-STAR」という制度名にて制度開始の案内**[3]を実施しました。
- **★１については2024年度中の制度開始**を予定しています。また、**政府調達等の要件**等とすべく関係省庁と議論を行っているほか、**米欧等の諸外国との制度調和**を図るため議論を行っています。

制度名称・ロゴ・ラベル

セキュリティ要件適合評価及びラベリング制度
JC-STAR
(Labeling Scheme based on Japan Cyber-Security Technical Assessment Requirements)

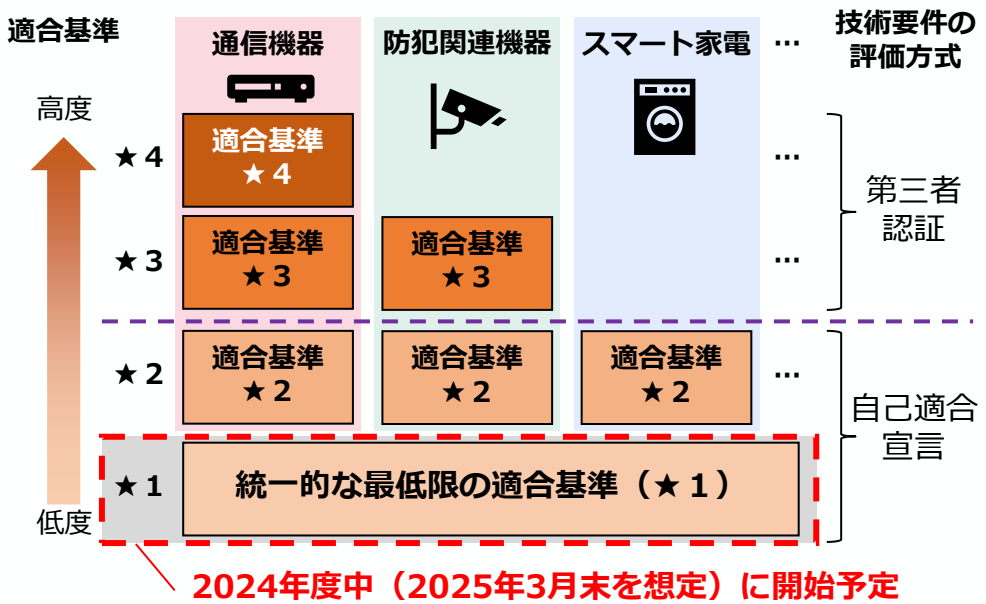
JAPAN CYBERSECURITY LABEL
ジャパン・サイバーセキュリティ・ラベル
★★★★
JC-STAR
Registered ID: 0123456789012345
Information-technology Promotion Agency, JAPAN (IPA)

対象製品の概要



※ 国内外の一部の既存制度と同様に、利用者がソフトウェア製品等により容易にセキュリティ対策を追加することができる汎用的なIT製品（パソコン、タブレット端末、スマートフォン等）は対象外とする。

制度の概要（イメージ）

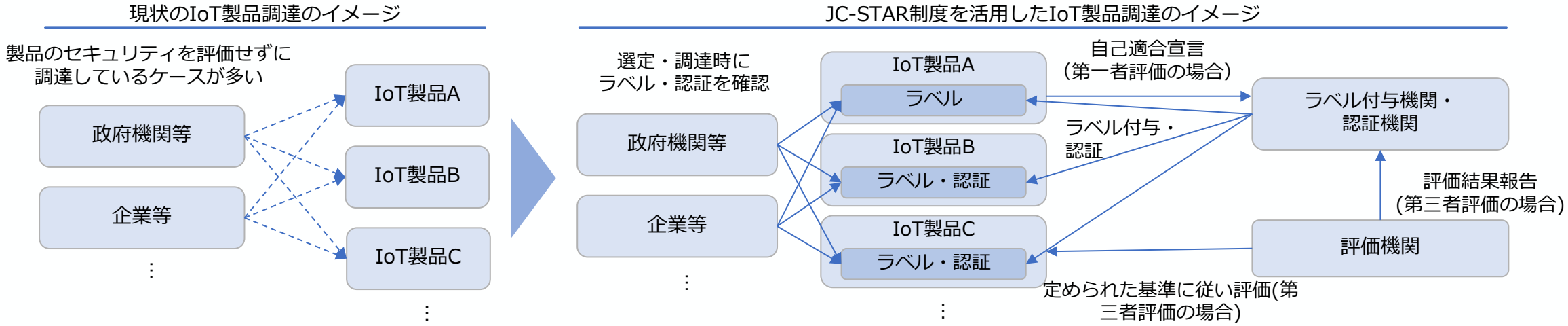


1: 経済産業省「ワーキンググループ3（IoT製品に対するセキュリティ適合性評価制度構築に向けた検討会）」 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/index.html
2: 経済産業省「IoT製品に対するセキュリティ適合性評価制度構築方針（2024年8月23日）」 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/20240823.html
3: IPA「IoT製品に対するセキュリティ要件適合評価・ラベリング制度を開始します」 https://www.ipa.go.jp/pressrelease/2024/press20240930.html

JC-STAR制度の目的と位置付け

- IoT製品に対するセキュリティ適合性評価制度を国内で構築し、そのラベル・認証を広く普及させ、社会に浸透させるため、まずは**調達者が自身を守るために、求めるセキュリティ水準のラベルが付与された製品を優先的に選択**できるようにします。（調達ニーズへの対応）
- 本ガイドは、主目的②の特定分野のシステムにて調達・利用されるIoT製品において、実質的な業界標準としてラベル取得製品が調達されることで、当該分野でのセキュリティの確保に貢献することを目的としています。

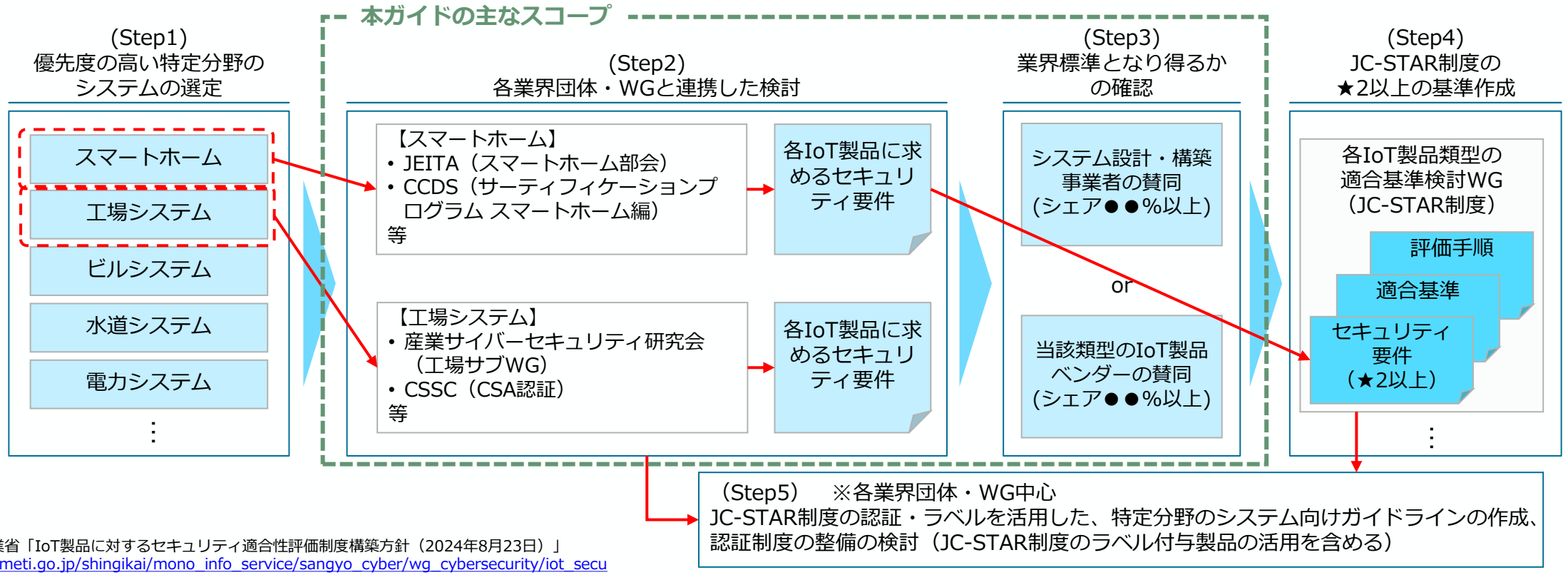
調達ニーズへの対応			ラベル取得のインセンティブ	
主目的① 【調達要件】	**政府機関や企業等で調達する製品**について、**共通的な物差しでIoT製品のセキュリティを評価・可視化できるようにする**ことで、各組織の求めるセキュリティ水準を満たしたIoT製品の選定・調達を容易にする。	左記に加え	主目的③ 【相互承認】	**諸外国の制度と協調的な制度を構築し、相互承認を図る**ことで、IoT製品を海外に輸出する際に求められる適合性評価にかかるIoT製品ベンダーの負担を軽減する。
主目的② 【業界標準】	特定分野のシステムにて調達・利用されるIoT製品に対し、必要な認証・ラベルを各業界団体等で指定できるようにし、当該**特定分野において必要なセキュリティが確保されたIoT製品のみが採用される**ようにする。			



出所）経済産業省「IoT製品に対するセキュリティ適合性評価制度構築方針（2024年8月23日）」 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/20240823.html

特定分野システムに関する業界団体・WGとの連携

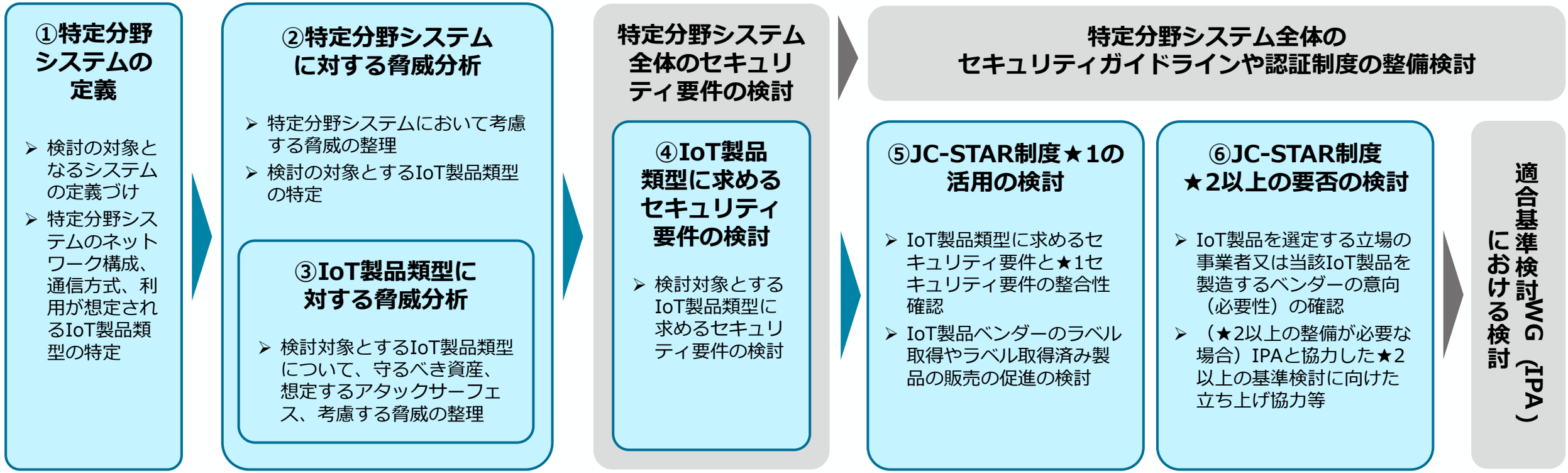
- 特定分野システムに組み込まれて調達されるIoT製品について、検討優先度の高い分野の業界団体等と連携し、各システムに組み込まれるIoT製品に求めるセキュリティ要件や★2以上の適合基準をその必要性も含めて検討することとしています。
- 想定される各業界団体・WGとの連携ステップは以下のとおりです。本ガイドでは、**特定分野システムの各IoT製品に求めるセキュリティ要件の検討（Step2）に当たって参考となる情報を提供**するほか、**JC-STAR制度での基準策定に当たり、業界標準となり得るかの確認（Step3）において参考となる情報を提供**します。



出所）経済産業省「IoT製品に対するセキュリティ適合性評価制度構築方針（2024年8月23日）」
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/20240823.html

特定分野システムにおけるIoT製品セキュリティ要件検討の流れ

- 本ガイドでは、特定分野システムにおけるIoT製品セキュリティ要件を検討するに当たって、参考となる情報をフェーズごとに概説します。

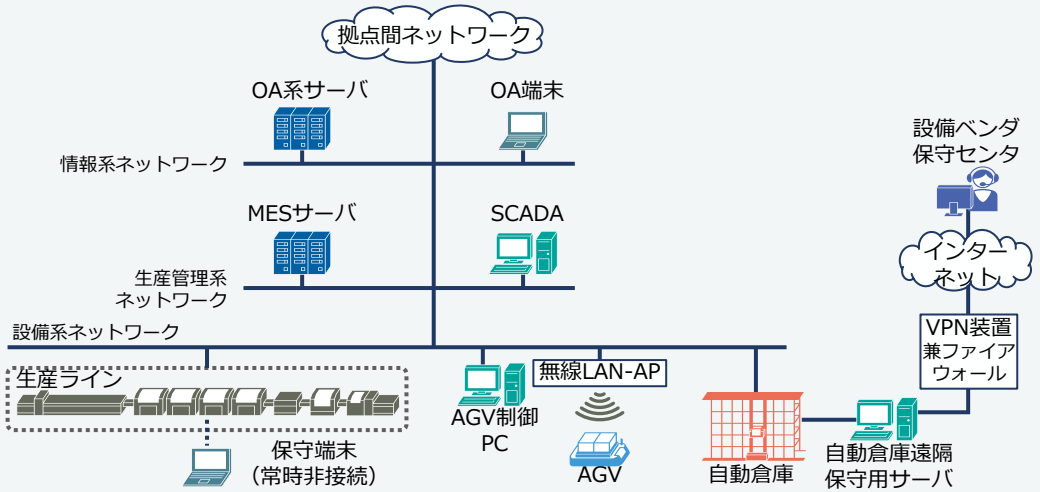


※本ガイドで概説している部分（①～⑥）を水色で示しています。

①特定分野システムの定義

- **検討の対象となるシステムを定めましょう。**
  - どのようなシステムを検討の対象とするかについて、定義づけしましょう。
    - 例１：スマートホームシステムの場合、HEMSゲートウェイを介したネットワーク接続がなされる構成や、スマートホーム機器のクラウドと直接的やり取りをする構成など、システムの典型的な構成パターンは複数に分類されます。
    - 例２：工場システムの場合、加工・組立を行う工場システム（FA）とプラント制御を行う工場システム（PA）が想定されます。システム構成に大きな差異はありませんが、制御の特性や性能の違いが異なるほか、取り扱い製品による危険性も異なるため、想定されるリスクやセキュリティ要件が異なります。
  - 特定分野システムにおけるIoT製品セキュリティ要件を検討するに当たって、どのようなシステム構成を検討対象とする特定分野システムとするのかを決定しましょう。

- **特定分野システムのネットワーク構成、通信方式、利用が想定されるIoT製品類型を特定しましょう。**
  - システム内にどのような構成要素が存在し、それぞれがどのような通信方式で繋がっているかをモデル図（システムの各機能がどのインターフェースを経由してどういった外部システムと連携しながら動作するかを表す図）で表しましょう。
  - また、システム内で利用が想定されるIoT製品類型をリスト化しましょう。



モデル図のイメージ（工場システム）[1]

1: 経済産業省「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」https://www.meti.go.jp/policy/netsecurity/wg1/factorysystems_guideline.html

②特定分野システムに対する脅威分析

- **検討対象とする特定分野システムにおいて守るべき資産を洗い出しましょう。**
  - 特定分野システムを構成する資産を一覧整理するとともに、その資産の重要度を踏まえ、どのような資産を守るべきかを整理しましょう。
  - 詳細な実施方法については、「制御システムセキュリティリスク分析ガイド[1]」等をご覧ください。
- **検討対象とする特定分野システムに対して脅威の整理（リスク分析）を行いましょう。**
  - 特定分野システムの守るべき資産に対して想定される攻撃者（脅威源）を整理のうえ、守るべき資産に対して想定される脅威を整理しましょう。
  - 攻撃者の分類や脅威の整理（リスク分析）の詳細な実施方法については、「制御システムセキュリティリスク分析ガイド[1]」等をご覧ください。また、特定分野システムに対するリスク分析実施時に参考となるリスクの考え方や基準については、「IoTセキュリティ・セーフティ・フレームワーク（IoT-SSF）[2]」等をご覧ください。
- **リスク分析結果を踏まえ、セキュリティ要件の検討対象とするIoT製品類型を特定しましょう。**
  - 特定分野システムを構成するIoT製品のうち、資産重要度の高いIoT製品やリスクの度合いが高いIoT製品など、セキュリティ要件を検討すべき優先度の高いIoT製品類型を特定しましょう。
  - 資産重要度の高いIoT製品の観点としては、攻撃を受けた場合に特定分野システムの運用に長期間影響を及ぼす可能性のある製品や、攻撃を受けた場合に人的／環境被害が発生するおそれがある製品などが挙げられます。
  - リスク度合いの高いIoT製品の観点としては、論理的アクセス・物理的アクセスが容易な製品、攻撃実施に当たっての情報の入手が容易な製品など、脅威の発生可能性が高い製品が挙げられます。

1: IPA「制御システムのセキュリティリスク分析ガイド」https://www.ipa.go.jp/security/controlsystem/riskanalysis.html
2: 経済産業省「IoTセキュリティ・セーフティ・フレームワーク（IoT-SSF） Ver1.0」 https://www.meti.go.jp/policy/netsecurity/wg1/wg1.html

③IoT製品類型に対する脅威分析

- **検討対象とするIoT製品類型において守るべき資産を洗い出しましょう。**
  - IoT機能（機器やシステムがIoTにつながるための機能）、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）、情報（ユーザの個人情報、収集情報、各機能の設定情報など）、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）といった分類に沿ってどのような資産を守るべきかを整理しましょう。
  - 参考として、JC-STAR制度の★1で想定している守るべき資産はP.10のとおりです。
- **検討対象とするIoT製品類型において想定されるアタックサーフェスを整理しましょう。**
  - 入出力インターフェースや潜在的攻撃点、物理的接触といったアタックサーフェス（サイバー攻撃の対象となる攻撃点や攻撃経路）について、作成したモデル図をもとに整理しましょう。
  - 参考として、JC-STAR制度の★1で想定しているアタックサーフェスはP.11のとおりです。
- **検討対象とするIoT製品類型において考慮する脅威を整理しましょう。**
  - 守るべき資産及び想定されるアタックサーフェスを踏まえ、STRIDEモデル（Spoofing（なりすまし）、Tampering（改ざん）、Repudiation（否認）、Information Disclosure（情報漏えい）、Denial of Service（サービス拒否）、Elevation of Privilege（権限昇格）の6つの脅威の性質から脅威を洗い出していく手法）等を参考に、考慮する脅威を整理しましょう。
  - 脅威分析の詳細な実施方法については、「機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き 別冊[1]」や「IoT開発におけるセキュリティ設計の手引き[2]」をご覧ください。
  - 参考として、JC-STAR制度の★1で想定している脅威や守るべき資産との関係性はP.12～14のとおりです。

1: 経済産業省「機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き」 https://www.meti.go.jp/policy/netsecurity/vendor.html
2: 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/iotguide.html

【参考】★1で想定する守るべき資産

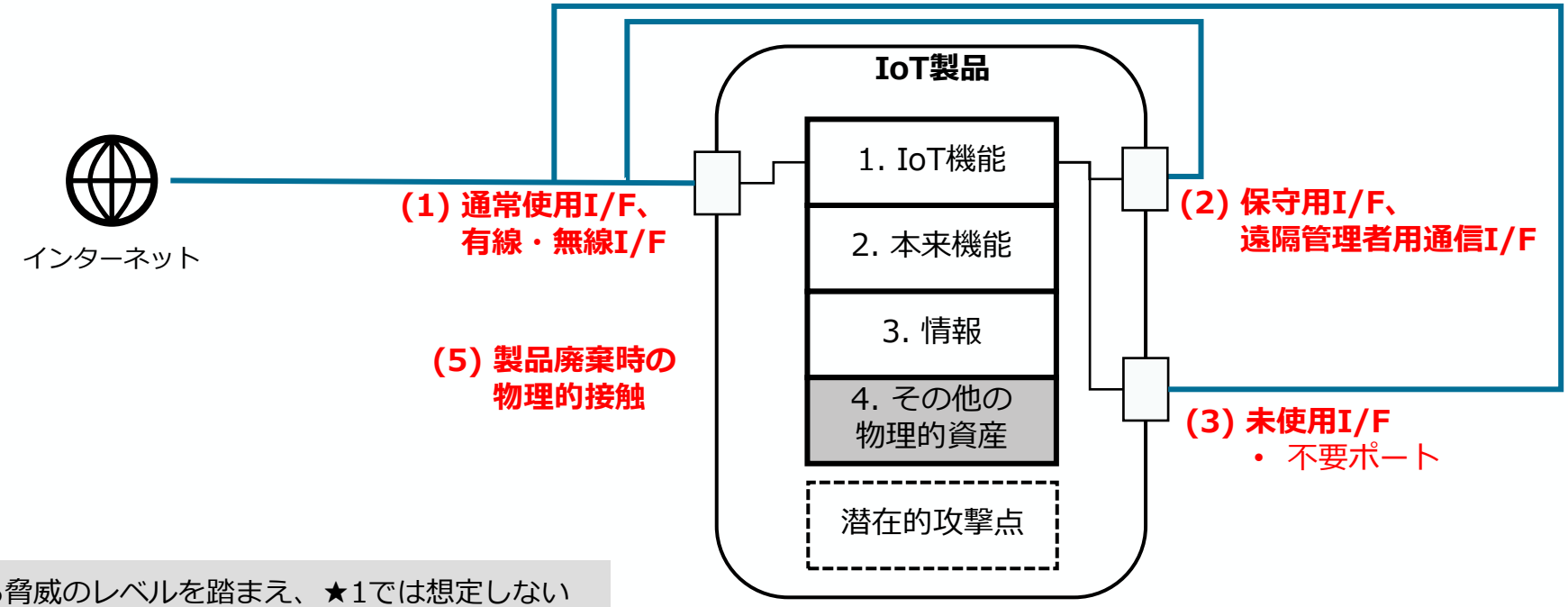
- ★1で想定する守るべき資産は、以下としました。
- なお、情報に関する守るべき資産について、IoT機能やセキュリティ機能に関する設定情報のほか、意図された機器の使用において、機器が収集し、保存又は通信する、個人情報等の一般的に機密性が高い情報を対象とします。

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	• **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	―	• 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はないが、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

【参考】★1で想定するアタックサーフェス

- ★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ます。

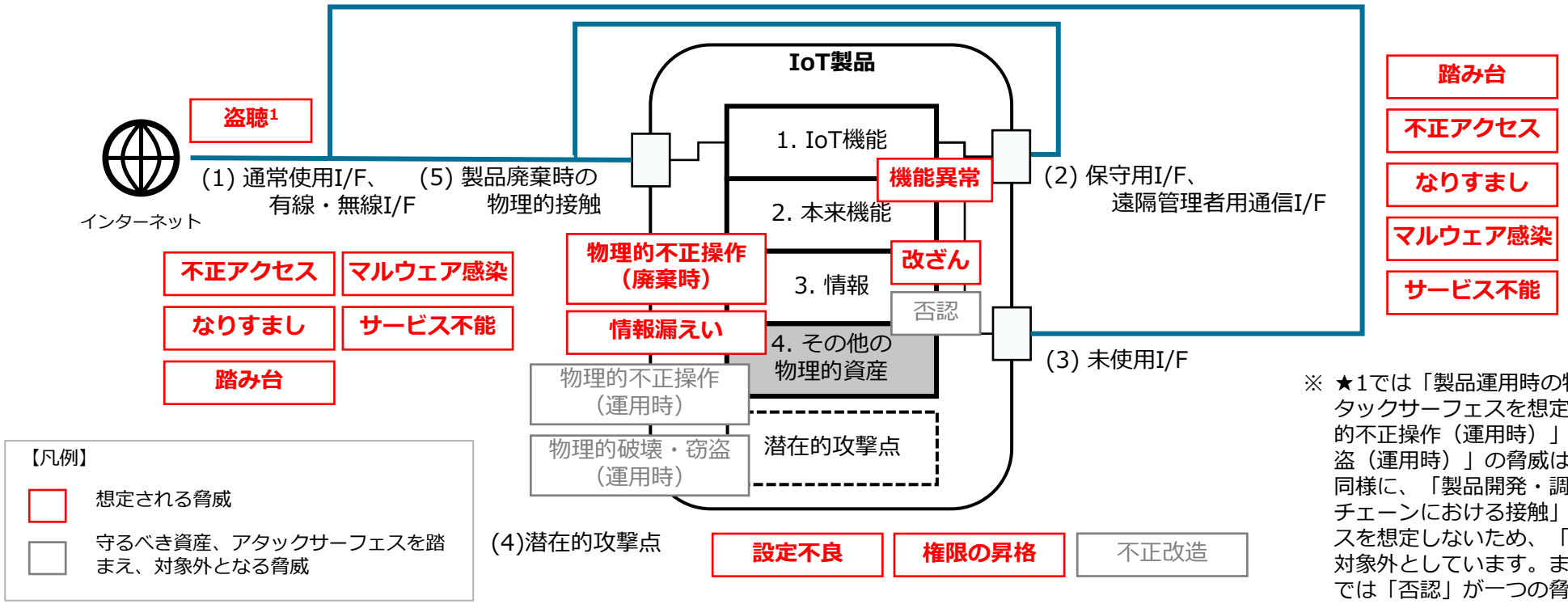


★1で対抗する脅威のレベルを踏まえ、★1では想定しないアタックサーフェス
- 製品運用時の物理的接触
- 製品開発・調達等のサプライチェーンにおける接触

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。

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



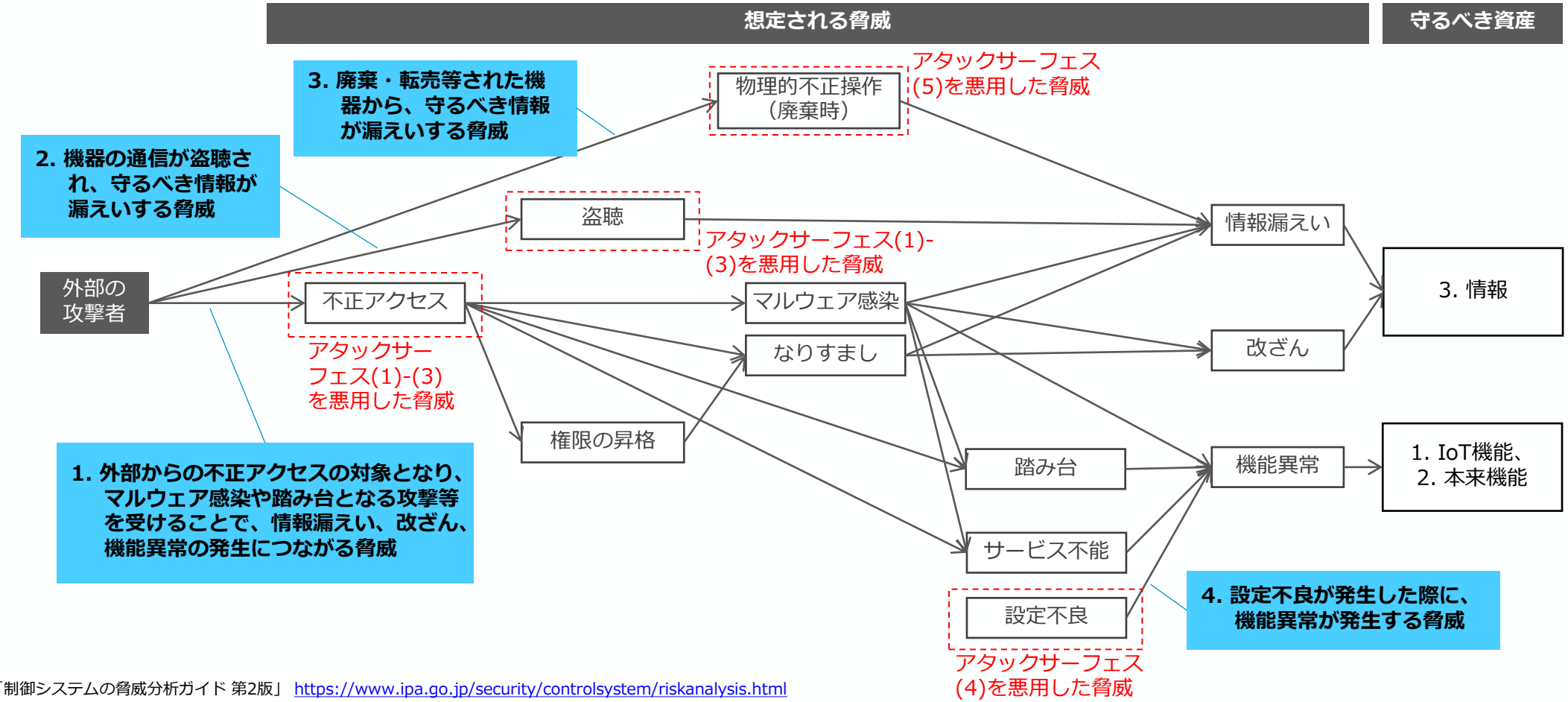
※ ★1では「製品運用時の物理的接触」のアタックサーフェスを想定しないため、「物理的不正操作（運用時）」や「物理的破壊・窃盗（運用時）」の脅威は対象外としています。同様に、「製品開発・調達等のサプライチェーンにおける接触」のアタックサーフェスを想定しないため、「不正改造」の脅威は対象外としています。また、STRIDEモデルでは「否認」が一つの脅威として挙げられていますが、★1で想定する守るべき資産として「否認」の影響を受ける資産を考慮していないため、当該脅威は対象外としています。

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。

参考）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

【参考】 ★1で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ます。
- 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ます。



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

【参考】★1で考慮する主な脅威

- 近年のセキュリティ脅威や海外制度を踏まえ、★1では以下の脅威を、主な脅威として考慮しています。

【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

【★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	★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。

④IoT製品類型に求めるセキュリティ要件の検討（1/2）

- **考慮する脅威に基づき、実施すべき対策及び各IoT製品類型に求めるセキュリティ要件を検討しましょう。**
  - 想定される対策候補一覧は以下に示すとおりです。
  - 単一の対策によって攻撃を完全に防ぐことは難しいため、複数の対策を組み合わせた多層防御を検討しましょう。
  - 検討の際は、実装対象のリソース、投入可能なコスト、インシデント発生時の経済的影響や回復困難性等を考慮しましょう。
  - インシデント発生時の経済的影響や回復困難性、セキュリティ・セーフティ要件の観点については、「IoTセキュリティ・セーフティ・フレームワーク（IoT-SSF）[1]」等をご参考ください。

1: 経済産業省「IoTセキュリティ・セーフティ・フレームワーク（IoT-SSF） Ver1.0」 https://www.meti.go.jp/policy/netsecurity/wg1/wg1.html

対策候補一覧（1/2）

対策候補	機能・目的	対応する脅威の例
脆弱性対策	開発段階での脆弱性混入を防止する。運用段階で検出された脆弱性を解消する(ソフトウェア更新の配布・適用やパッチ適用などを含む)。	ウイルス感染、不正アクセス
セキュア開発	実装時にセキュアプログラミングを実施する。また、セキュリティテストを実施したことを確認の上で出荷する。	ウイルス感染
サーバーセキュリティ	サーバのセキュリティ(設定情報を含む)を定期的に確認し、問題があれば修正する。	不正アクセス
FW機能	接続先を IPアドレス・ポート番号で制限する。	不正アクセス、DoS攻撃
サーバー認証	クライアントがサーバを認証することにより、サーバへの成りすましを防止する。	成りすまし、情報漏えい
フィルタリング	信頼できないウェブサイトへのアクセスを禁止する。また、信頼できないアドレスからのメール受信を拒否する。	ウイルス感染、SPAMメール
IDS/IPS	入出力データを監視し、不正アクセスの検知、抑止を行う。	不正アクセス、DoS攻撃
DoS対策	DoS攻撃(DDoS攻撃を含む)を遮断するための対策を実施する。	DoS攻撃
アンチウイルス	ウイルスを検知・除去して、ウイルス感染を防止する。	ウイルス感染

出所）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/iotguide.html

④IoT製品類型に求めるセキュリティ要件の検討（2/2）

対策候補一覧（2/2）

対策候補	機能・目的	対応する脅威の例
仮想パッチ	ソフトウェア更新等が実施できず、脆弱性を完全に除去できない場合、脆弱性を突いた攻撃を前段にてブロックする。	ウイルス感染
ユーザ認証	利用者を認証することにより、利用者の成りすましによる脅威を防止する。可能であれば、複数の認証要素を組み合わせた多要素認証技術を採用することが望ましい。	不正利用、不正アクセス、情報漏えい
メッセージ認証	通信相手から送信されたメッセージを認証することにより、通信相手への成りすましによる偽メッセージ送信や、メッセージの改ざんを防止する。	成りすまし、データ改ざん、不正コマンド
通信路暗号化	データの通信路を暗号化し、通信路上のデータが漏えいしたとしても、無価値化する(攻撃者にとって無意味なものとする)。また、通信路上でのデータの改ざんを検知する。	盗聴・改ざん
データ暗号化	データ自体を暗号化し、仮に蓄積時または通信時のデータが漏えいしたとしても、無価値化する(攻撃者にとって無意味なものとする)。	情報漏えい
データ二次利用禁止	データの目的外利用を禁止し、二次利用先からの漏えいを防止する。	情報漏えい
ホワイトリスト制御	予め許可したプログラム以外の動作を禁止し、ウイルス感染を防止する。	ウイルス感染
ソフトウェア署名	署名されたソフトウェアの動作のみ許可し、ウイルス感染したソフトウェアや不正改造されたソフトウェアの動作を防止する。	ウイルス感染、不正改造
出荷時状態リセット	IoT機器を出荷時状態にリセットして、データや出荷後の設定を全て削除する。	情報漏えい
セキュア消去	記録していた場所から復元不可能な様にした上で、データを消去する。	情報漏えい
耐タンパーH/W	筐体開封を検知して内部情報を自動消去する等、ハードウェア技術を用いて、内部構造や記憶しているデータの解析を困難とする。	情報漏えい、不正改造
耐タンパーS/W	プログラムやデータ構造の難読化等、ソフトウェア技術を用いて、内部構造や記憶しているデータの解析を困難とする。	情報漏えい、不正改造
遠隔ロック	遠隔操作によりIoT機器の機能をロックし、第三者による不正利用を防止する。	不正利用
遠隔消去	遠隔操作によりIoT機器内のデータを消去し、情報漏えいを防止する。	情報漏えい
ログ分析	各種ログを分析することで、不正アクセスを検知し、何が行われたかを突き止める。	不正アクセス
説明書周知徹底	使用上の注意事項を説明書に明記し、使用開始前の利用者の一読を周知徹底する。	(設定誤り・操作誤りに起因する各種脅威)

出所）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/iotguide.html

【参考】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、製品／IoT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、以下に示す対策を想定し、これらに応じたセキュリティ要件を定めました。

★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		IoT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	ー	ー
	①～③共通		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	ー	ー
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	ー	ー
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	ー	ー

【参考】★1セキュリティ要件（1/2）

カテゴリ	要件
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、機器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. 機器が、制約のある機器ではない場合、ネットワークを介して行われる認証に対する総当たり攻撃等のブルートフォース攻撃が実行できないようにするメカニズムを保有しなければならない。
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
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。
	3-2. 機器が、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。
	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。
	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。
	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。
	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。
	3-14. 製品のモデル名称は、製品上のラベル又は物理的インタフェースを介して、ユーザに対して明確に認識可能でなければならない。

出所）経済産業省「IoT製品に対するセキュリティ適合性評価制度構築方針 別添」https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/20240823.html

【参考】★1セキュリティ要件（2/2）

カテゴリ	要件
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。
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。
	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。
	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。
6. 露出した攻撃面を最小化する	6-1. すべての未使用の物理的インタフェース及び論理的インタフェースは無効化しなければならない。
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。
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。
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。
	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。
	17-5. 製造業者は、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。
	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。
	17-10. 製造業者は、セキュリティリスク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。

出所）経済産業省「IoT製品に対するセキュリティ適合性評価制度構築方針 別添」https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/20240823.html

⑤JC-STAR制度★1の活用の検討

- **検討した各IoT製品類型に求めるセキュリティ要件について、JC-STAR制度の★1セキュリティ要件と整合性がある場合、特定分野システムのセキュリティ向上のために、対象IoT製品類型に対する★1の活用を促進しましょう。**
- **制度の活用を促進するために、どのようにして各IoT製品ベンダーのラベル取得やラベル取得済み製品の販売の促進を行うかについて、検討しましょう。**
  - まずは、制度の理解促進やメリットの共有のために、セミナーや説明会を実施することが効果的です。
  - IoT製品ベンダーに対しては、具体的なラベル取得プロセスや基準を説明することが効果的です。JC-STAR制度の★1は全製品類型共通の適合基準であるため、特定分野システム特有で留意すべき基準や評価方法がある場合、その内容を共有することで、IoT製品ベンダーは効率的にラベルを取得することができます。既に対応を進めているIoT製品ベンダーがいる場合、そのIoT製品ベンダーの経験談を共有することも効果的です。
  - また、ラベル取得済み製品の販売促進のために、調達者・販売者・利用者に対しても、制度の理解促進やメリットの共有を図ることが望まれます。
  - JC-STAR制度では、諸外国におけるIoT製品の適合性評価制度設立の動向も踏まえ、各国の制度との連携を図り、相互承認することも目指しています。ラベル取得のインセンティブを高めるために、各国制度との連携状況を確認し、IoT製品ベンダーに共有することも重要です。

⑥JC-STAR制度★2以上の整備要否の検討

- **検討したセキュリティ要件について、JC-STAR制度の★1セキュリティ要件では十分ではない場合、当該製品類型に対する★2以上の制度の整備を検討しましょう。**
  - ★2以上では、IoT製品類型ごとの特徴を考慮して適合基準を定めます。
  - ★2以上の整備に当たっては、 IoT製品を選定する立場の事業者又は当該IoT製品を製造するIoT製品ベンダーからの一定程度の賛同があるなど、業界標準となり得ると判断できることが重要です。
    - 例１：一定程度以上（50%程度以上など）のシェアを占めるIoT製品ベンダーが、★2以上が整備された場合、そのラベルを取得することに合意する場合
    - 例２：特定分野システムのセキュリティ対策に関する各種制度やガイドライン等において、JC-STAR制度のラベルを取得したIoT製品の調達・利用を必須又は強く推奨する方針である場合
    - 例３：IoT製品を選定してシステム設計・構築を行う立場の事業者のうち、主要な事業者（上位3社など）が、★2以上が整備された場合、そのラベルを取得したIoT製品を優先的に選定する方針に合意する場合
- **業界内での検討を踏まえ、★2以上の整備が必要と思われる場合は、IPAと協力して★2以上の基準検討を行いましょう。**
  - ★2以上の必要性や普及見込みに関する業界内での検討結果を踏まえ、IPAにて★2以上の整備要否や整備時期を判断します。
  - ★2以上の詳細な基準に関する議論・検討は、IPAが設置する各製品類型の適合基準検討WGにて行います。
  - 業界団体等、当該製品類型の関係者には、委員としての参画など、適合基準検討WGの立ち上げや検討に協力していただきます。
  - WGにおいては、実施した脅威分析や検討したセキュリティ要件の検討結果を踏まえ、★2以上のセキュリティ要件に対し、どのような適合基準・評価手順が必要となるかを議論・検討します。

【参考】★1適合基準（1/3）

ID	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。）
S1.1-02	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、又は、IoT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。
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。
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。
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
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。）

出所）IPA「★1（レベル1）適合基準・評価ガイド」 https://www.ipa.go.jp/security/jc-star/tekigou-kizyun-guide/label1/index.html

【参考】★1適合基準（2/3）

ID	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。
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。
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。
S1.1-10	IoT製品の型式番号は、以下のいずれかの方法でユーザへ提供すること。 ① IoT製品本体に、IoT製品の型式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、ユーザが型式番号を認識できるようにすること。
S1.1-11	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。
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。
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。

出所）IPA「★1（レベル1）適合基準・評価ガイド」 https://www.ipa.go.jp/security/jc-star/tekigou-kizyun-guide/label1/index.html

【参考】★1適合基準（3/3）

ID	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。）
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。
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。

出所）IPA「★1（レベル1）適合基準・評価ガイド」 https://www.ipa.go.jp/security/jc-star/tekigou-kizyun-guide/label1/index.html