

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」の概説

2024/07/26

日立チャネルソリューションズ株式会社
情報セキュリティ統括センタ

※ 本資料では、経済産業省が構築中の「IoT製品に対するセキュリティ適合性評価制度」について説明していますが、まだ未確定の部分が存在し、実際の制度運用では本説明と異なる場合があることをご了承願います。

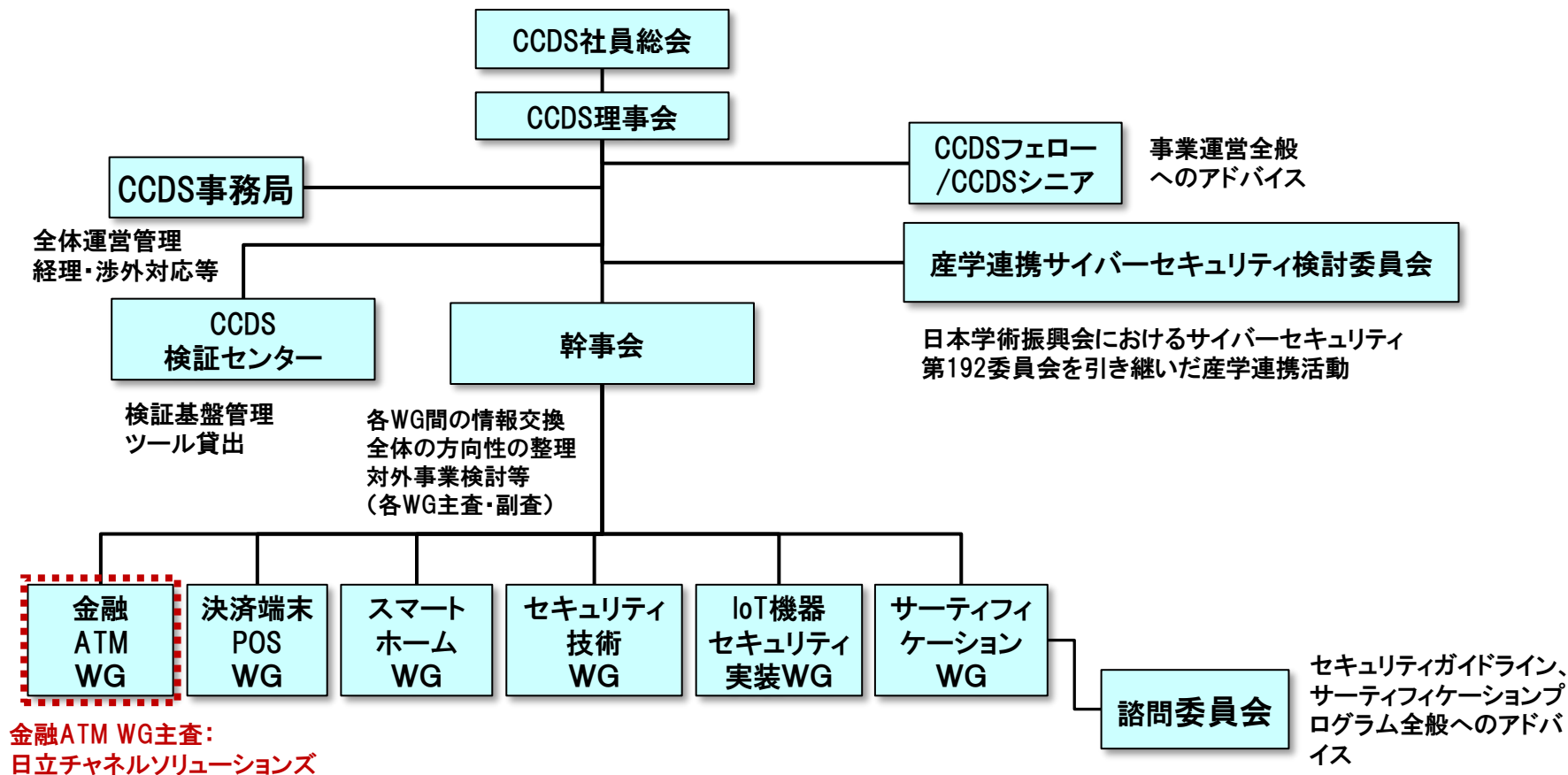
Contents

1. 重要生活機器連携セキュリティ協議会(CCDS)の取り組み
2. 「IoT機器に対するセキュリティ適合性評価制度」のポイント
3. ☆1セキュリティ要件の概要

1. 重要生活機器連携セキュリティ協議会(CCDS)の取り組み

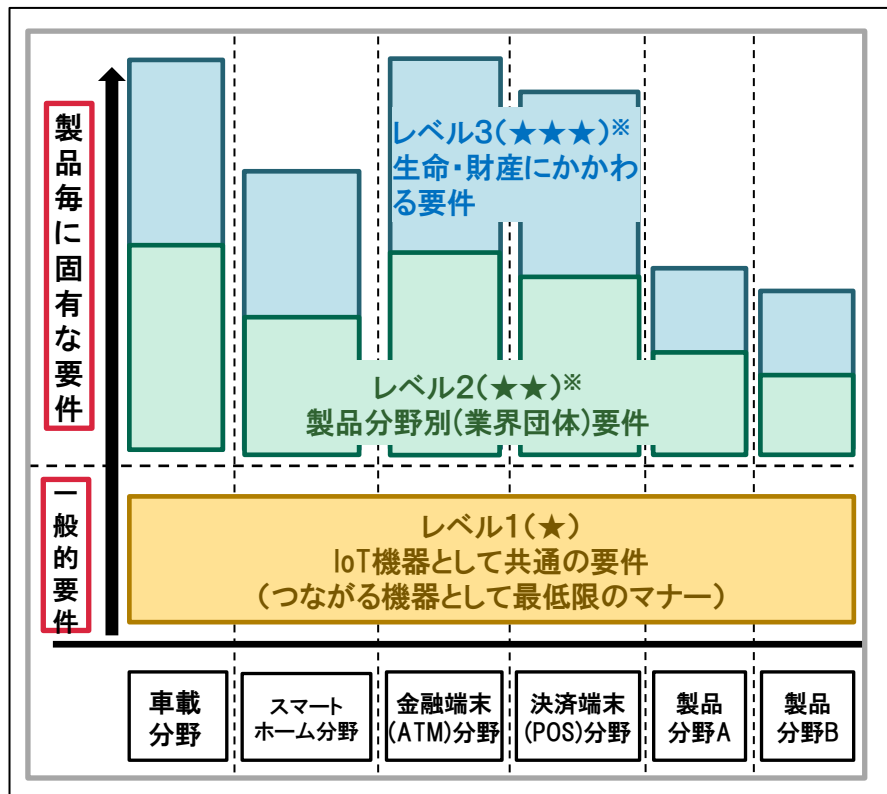
1-1 重要生活機器連携セキュリティ協議会 (CCDS) の概要

- ・ 名 称 : 一般社団法人 重要生活機器連携セキュリティ協議会
 - 英名 : Connected Consumer Device Security council (CCDS)
- ・ 設 立 : 2014年10月6日
- ・ 会 長 : 徳田英幸 (情報通信研究機構 理事長、慶應大学 名誉教授)
- ・ 代表理事 : 荻野 司 (情報セキュリティ大学院大学 客員教授)
- ・ 理 事 : 江崎 浩 (東京大学大学院 教授)
後藤 厚宏 (情報セキュリティ大学院大学 学長、SIP Program Director)
松本 勉 (産業技術総合研究所フェロー、CPSEC研究センター長)
- ・ 会員数 : 223 (正会員以上 : 51、一般会員 : 123、学術系 : 31、協賛:18) (2024年6月)
- ・ 主な事業 :
 1. 生活機器の各分野におけるセキュリティに関する**国内外の動向調査**、内外諸団体との交流・協力
 2. 生活機器の安全と安心を両立する**セキュリティ技術の開発**
 3. **セキュリティ設計プロセスの開発**や**検証方法のガイドラインの開発、策定**、および、**国際標準化の推進**
 4. 生活機器の**検証環境の整備・運用管理**及び検証事業、セキュリティに関する**人材育成**や**広報・普及啓発活動**等

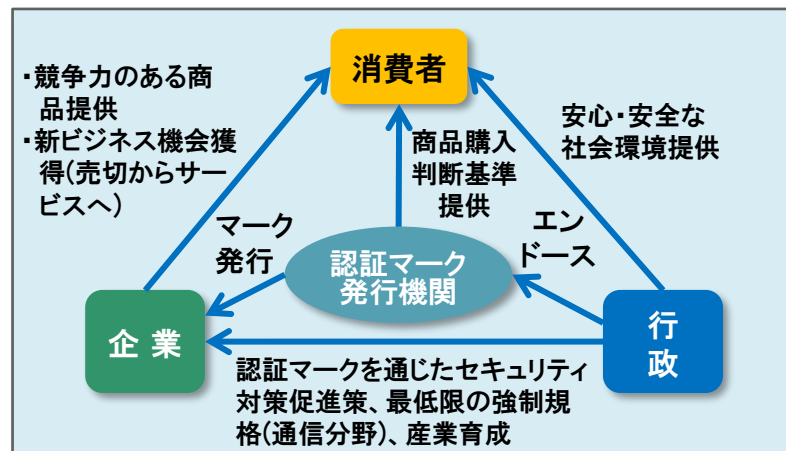


1-3 CCDSサーティフィケーションプログラムの概要

プログラムのレベル構成



プログラムのスキーム



プログラムのポイント

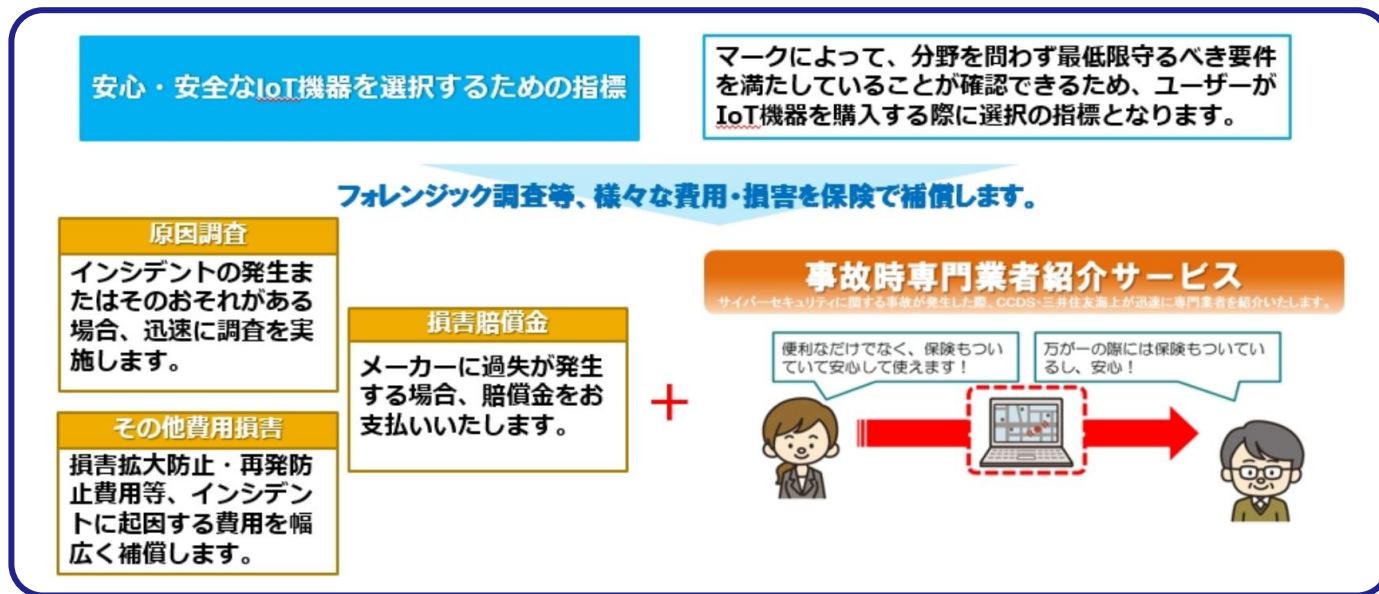
1. 任意マーク(罰則なし)
2. 自主検査と第三者検査のいずれか選択可能
3. 第三者機関によるマーク付与の意味 (検証結果保持と追跡可能)
4. マークの毎年更新(新規攻撃への対応)
5. セキュリティ対策の普及促進策⇒例えば税制優遇、助成金

※ 製品に加え、サービスが対象に含まれる

1-4 国内初となるIoTサイバー保険の自動付帯

■ IoTサイバー保険の自動付帯により、最高3000万円までの賠償/費用損害を補償※

三井住友海上火災保険株式会社、損害保険ジャパン株式会社、東京海上日動火災保険株式会社と連携して国内初となる「IoT機器保険付認証制度」を構築し、マーク付与製品に対してサイバー保険を自動付帯する。



※ 詳細は右のリンクを参照。
[CCDSサーティフィケーションプログラム規程 ver2.0.pdf](#)
[規程別紙3\)IoTサイバー保険 事故受付票 v1.0.xls \(live.com\)](#)
[規程別紙4\)IoTサイバー保険 補償範囲 v1.0](#)

1-5 CCDSサーティフィケーション取得製品・サービス

■ 現在までのCCDSサーティフィケーション取得実績

レベル	企業名	マーク 年度	製品・サービス名称	型式番号	製品URL	登録日
Lv.1 (★)	株式会社JVCケンウッド	2019	CONNECTED CAM	GY-HC900CH	製品HP	2020/4/1
Lv.1 (★)	オムロンソーシアルソリューションズ 株式会社	2019	CATS300/900 Base ユニット	3M8CR-Base	製品HP	2020/5/11
Lv.1 (★)	文化シャッター株式会社	2019	ワイヤレス通信機2	SCX1801	製品HP	2020/5/15
Lv.1 (★)	リンナイ株式会社	2019	無線LAN 対応リモコン	MC-301Vシリーズ/MC-302Vシリーズ	製品HP	2021/1/22
Lv.1 (★)	株式会社アルファ	2019	電気錠操作盤	WS800-W-SH-PFH (Cn-83)	製品HP	2021/1/22
Lv.1 (★)	日立チャネルソリューションズ株式会社	2019	自動受付精算機	—	製品HP	2021/1/22
Lv.2(★★)	積水ハウス株式会社	2021	PLATFORM HOUSE touch	—	サービスHP	2021/8/2
Lv.1(★)	日立チャネルソリューションズ株式会社	2021	現金入出金端末	TS-E462	—	2023/3/31
Lv.1(★)	日立チャネルソリューションズ株式会社	2023	AKe-Sx(ATMベース機)	AKe-Sx+AKe-Cube	—	2023/3/31
Lv.1(★)	富士通フロンテック株式会社	2023	FACT-X(ATMベース機)	—	—	2023/3/9
Lv.1(★)	文化シャッター株式会社	2023	ワイヤレス通信機2	SCX1801	製品HP	2023/10/1 7
Lv.1(★)	オムロンソーシアルソリューションズ 株式会社	2023	キャッシュレス端末JET-S eZCATS-100	3M8CX	製品HP	2023/11/2 2
Lv.1(★)	株式会社アルファ	2023	電気錠操作盤	WS800-W-SH-PFH (Cn-83)	製品HP	2024/1/31
Lv.2 (★★)	積水ハウス株式会社	2023	PLATFORM HOUSE touch	—	サービスHP	2024/4/15

https://www.ccds.or.jp/certification/certification_devices-sevices.htmlより引用

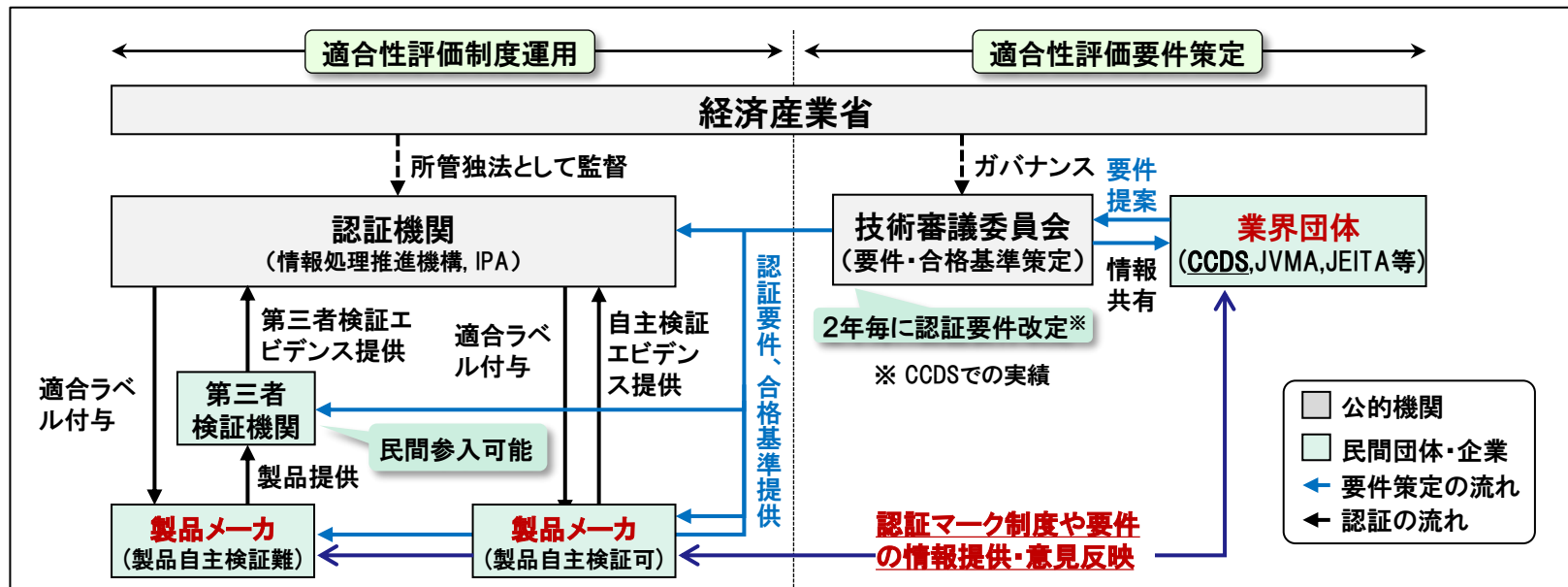
2. 「IoT機器に対するセキュリティ適合性評価制度」のポイント

2-1 経済産業省「IoT機器に対するセキュリティ適合性評価制度」の概要

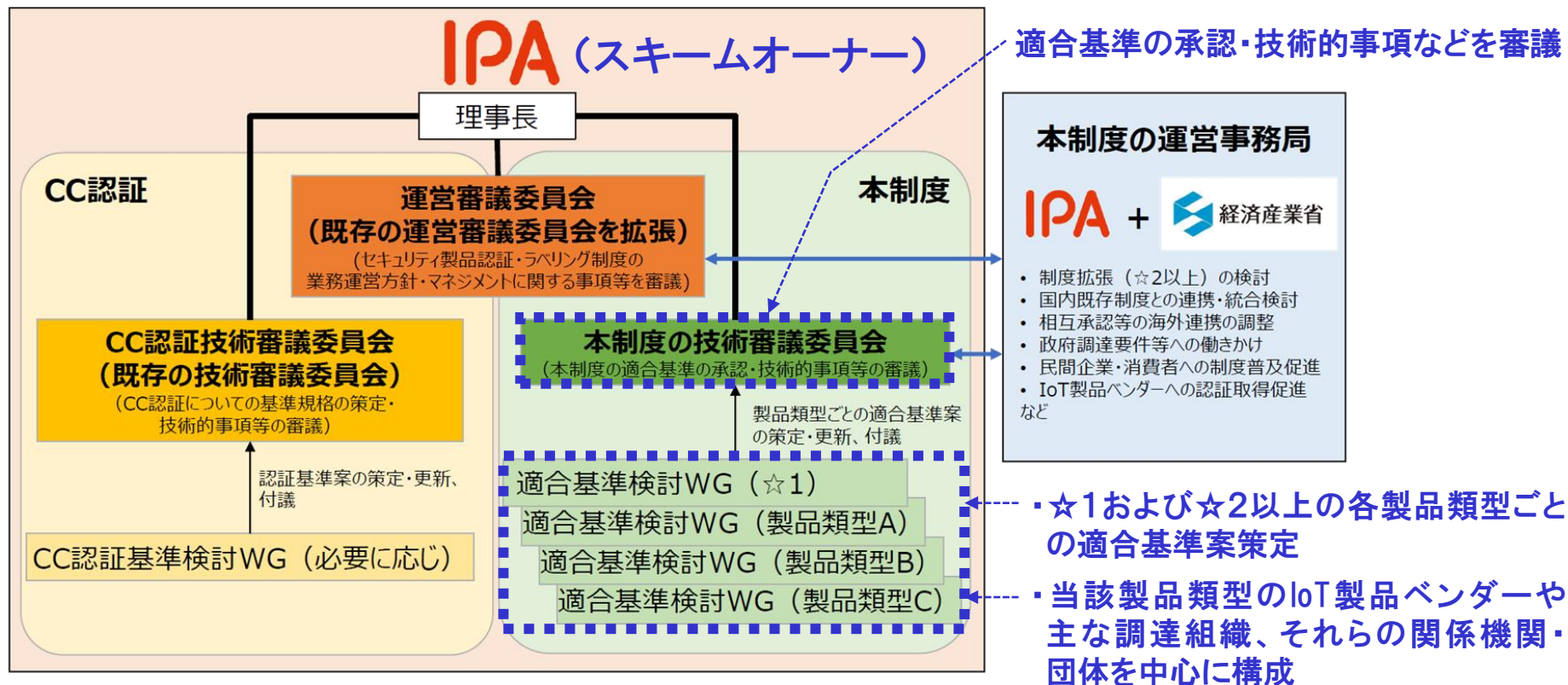
■ 経済産業省「IoT機器に対するセキュリティ適合性評価制度」の概要

- ◆ 情報処理推進機構(IPA)を認証機関とする、経済産業省のセキュリティ適合性評価制度を2025年3月から開始見込み。
- ◆ IoTデバイスだけでなく、システムも認証対象(☆2以上)となる。
- [ポイント] 経済安全保障上の課題としても挙げられ、国の施策として対応が加速。 ➡ 脆弱性な製品が市場淘汰の可能性

自己適合宣言(☆1、☆2)によるセキュリティ適合性評価制度の運営

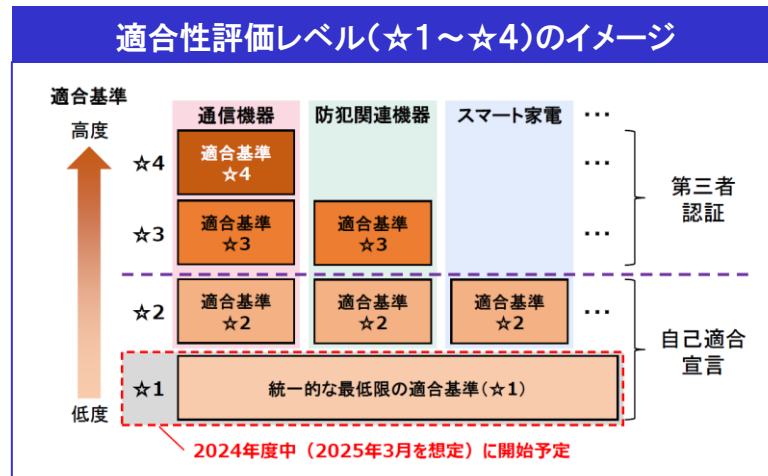
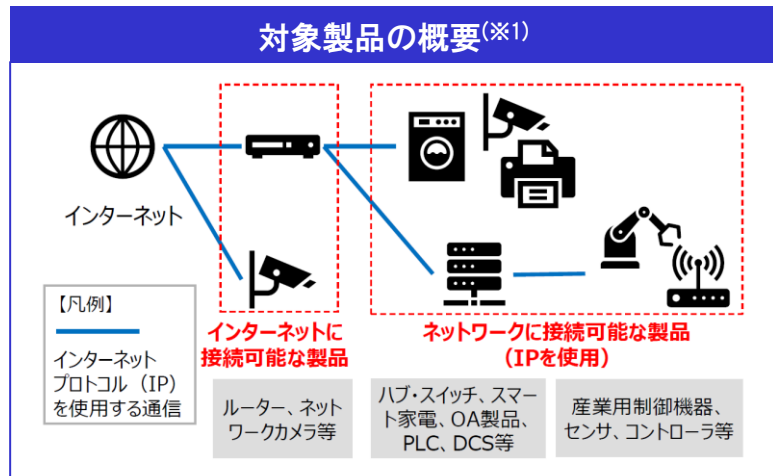


2-2 適合基準策定や更新の運用体制



※ IoT製品に対するセキュリティ適合性評価制度構築方針案(概要説明資料)より引用し、筆者で追記・加工
<https://www.meti.go.jp/press/2023/03/20240315005/20240315005-33rr.pdf>

2-3 対象製品と適合性評価レベル



レベル	位置付け	適合基準	評価方式
☆3以上	政府機関等や重要インフラ事業者、大企業の重要なシステムでの利用を想定	製品類型別	第三者認証
☆2	IoT製品類型ごとの特徴を苦慮し、☆1に追加すべき基本的なセキュリティ要件を定義		自己適合宣言
☆1	IoT製品として共通して求められる最低限のセキュリティ要件を定義	製品類型共通	

※1 国内外の一部の既存制度と同様に、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

※2 IoT製品に対するセキュリティ適合性評価制度構築方針案(概要説明資料)より引用し、筆者で追記・加工

<https://www.meti.go.jp/press/2023/03/20240315005/20240315005-33rr.pdf>

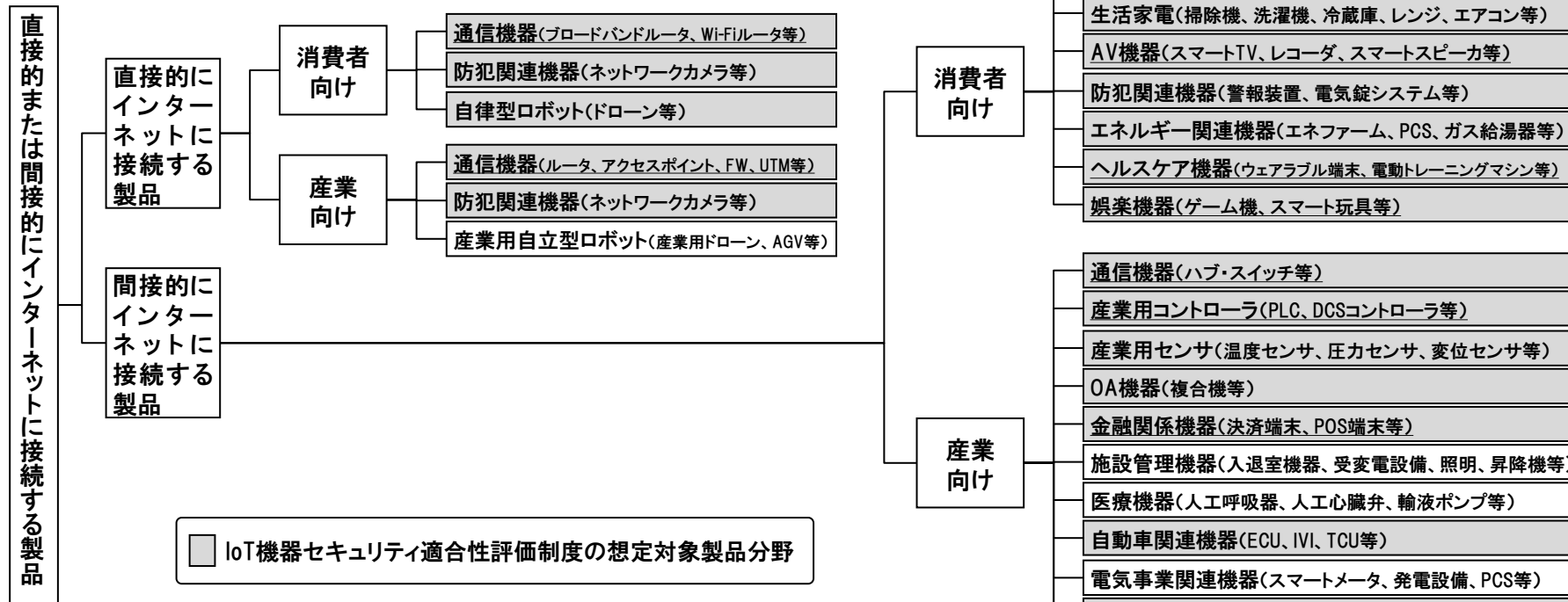
2-4 ラベルの意味合いと信頼性確保の仕組み

- 本制度のラベルは、定められた適合基準への適合を示すもの  セキュリティ完全確保の保証ではない
- ラベルの表示義務は設けない
- 本制度のロゴ及びラベル付与製品毎の情報提供ページのURLを埋め込んだQRコードを掲載（一手段）
- 自己適合宣言の有効期限：ラベル取得日を起点として最大2年間
- スキームオーナーは、ラベル付与製品に対して検査やサーベイランスを行える権利を有する

評価レベル	ラベルの意味合い
☆1、☆2 (自己適合宣言)	● 適合基準へ適合の証明主体：「IoT製品ベンダー自身」 ● IoT製品ベンダ：適合基準へ適合していることを自ら宣言 ● IPA：評価結果を記載したチェックリストの形式確認
☆3以上 (第三者認証)	● 適合基準へ適合の証明主体：「IPA」 ● IoT製品ベンダ：評価対象製品と関連文書を評価機関に提供 ● 評価機関：適合基準及び評価手順に従い評価 ● IPA：評価機関による評価結果を確認の上で、当該基準への適合を認証

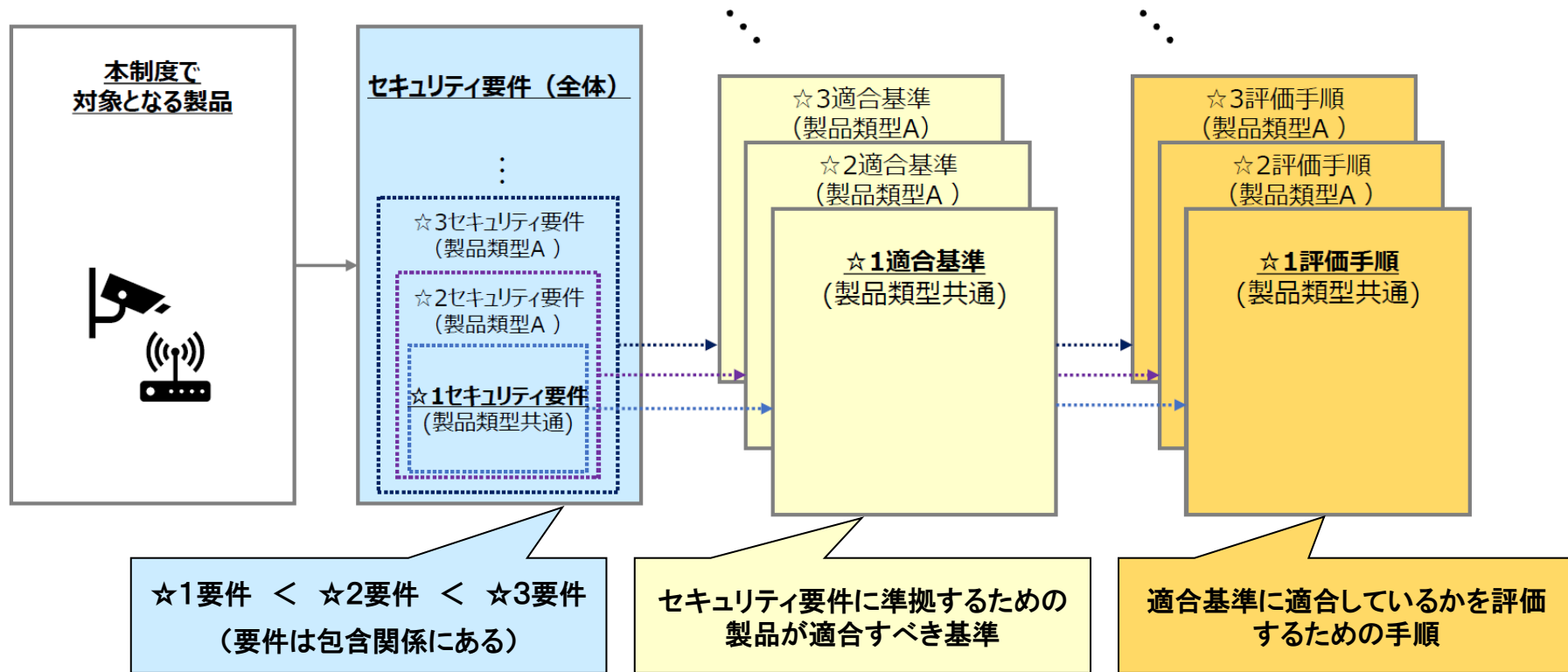
2-5 IoT機器セキュリティ適合性評価制度の想定対象分野

■ IoT機器セキュリティ適合性評価制度の想定対象分野(19分野)

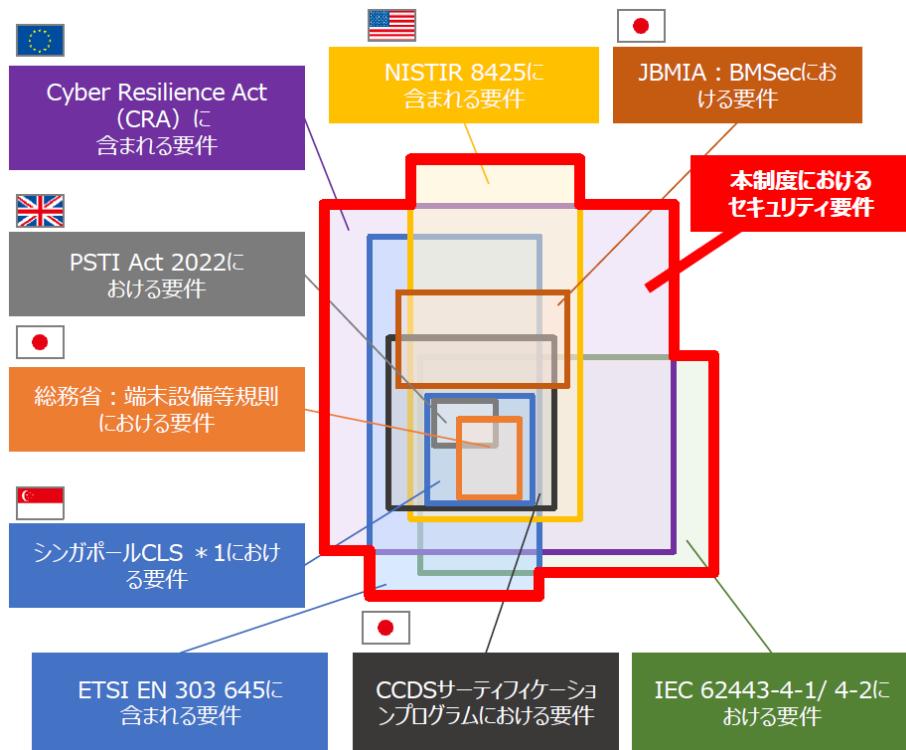


第5回 産業サイバーセキュリティ研究会 ワーキンググループ3 IoT製品に対するセキュリティ適合性評価制度構築に向けた検討会
資料4 IoT製品に対するセキュリティ適合性評価制度の構築について(一部非公開)、スライド28を基に作成
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/pdf/005_04_00.pdf

2-6 セキュリティ要件・適合基準・評価手順



■ 本制度のセキュリティ要件を策定するために行った、国内外のセキュリティ要件の集合関係の整理



2-9 調達要件への反映に関する働きかけ

- 政府機関等、重要インフラ事業者、地方公共団体におけるIoT製品調達時に、本制度のラベル付与製品を選定・調達することを求めていくように、関係者と調整を進める
- 主に調達されるIoT製品を中心に、その関連団体に対して、本制度との連携や会員企業への積極的なラベル取得の働きかけの賛同を得る

対象	主な調整先	調整状況・方向性
政府機関等	NISC 政府機関総合対策グループ 基本戦略第2グループ	● 「政府機関等のサイバーセキュリティ対策のための統一基準」およびそのガイドラインにてラベル付きIoT製品を各機関等の選定基準に含めることを検討 ● 政府機関等ではラベル取得済みIoT製品の調達を必須化する方針 ● 各府省庁の参加する会議の場などで周知
重要インフラ事業者	NISC 重要インフラ第1グループ	● 調達要件に関する記載を「重要インフラのサイバーセキュリティに係る行動計画」に紐づく安全基準等策定指針および手引書に入れる ● 調達ルールへの反映に関する働きかけは、四半期毎に実施しているセクターカウンシル(※2)の運営委員会を活用
地方公共団体	総務省 デジタル基盤推進室	● 地方公共団体セキュリティポリシーガイドラインに記載 ● 2024年度以降、検討会(※3)、自治体意見照会、パブコメを経てガイドライン改定を検討

※ IoT製品に対するセキュリティ適合性評価制度構築方針案(概要説明資料)より引用し、筆者で追記・加工
<https://www.meti.go.jp/press/2023/03/20240315005/20240315005-33rr.pdf>

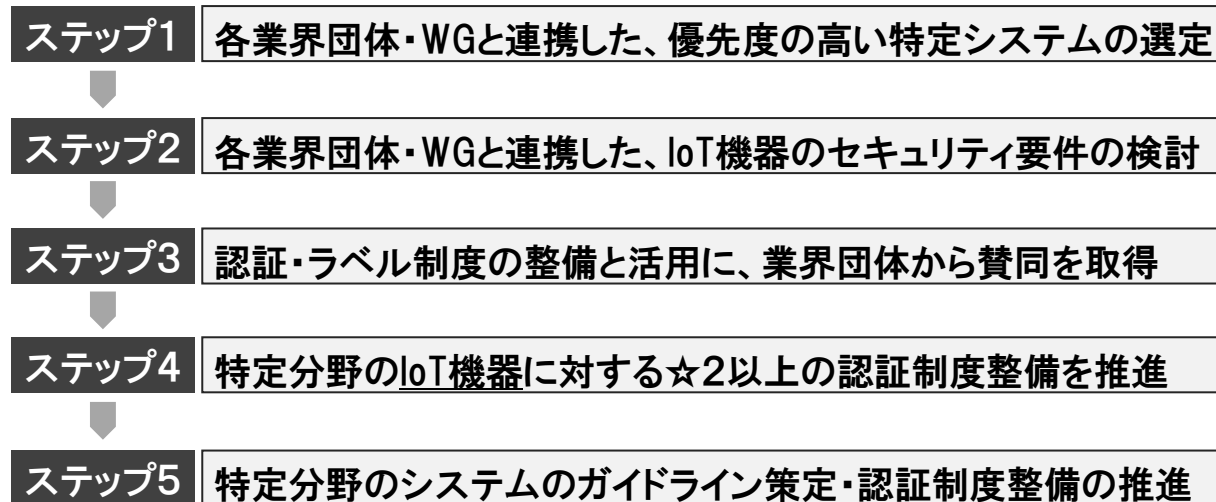
2-10 諸外国制度との連携

- 国内IoT製品ベンダーの負担を抑えるため、主要国制度の基準も参考にしながら本制度の基準を検討し、相互承認の調整を図る。
- ☆1開始の正式案内時に制度が既に導入されているシンガポールと英国とは、案内時に相互承認の方向性を提示する予定。欧米については、順次方向性を公表する。

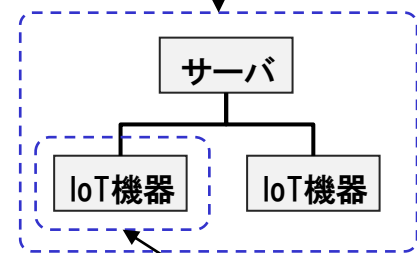
国・地域	 日本	 シンガポール	 英国	 米国	 EU
制度名	検討中	Cybersecurity Labelling Scheme (CLS)	Product Security and Telecommunication Infrastructure Act (PSTI法)	U.S. Cyber Trust Mark	Cyber Resilience Act (CRA) ※欧州委員会草案の内容
開始時期	☆1：2024年度下期(2025年3月)開始予定 ☆2以上：2025年度以降開始予定	2020年10月制度開始	2024年4月施行	2024年中に開始予定	未定 (報告義務を除き2027年開始想定)
任意/義務	任意	任意	義務	任意	義務
対象	IoT製品	消費者向けIoT機器	消費者向けIoT製品	消費者向けIoT機器(想定)	デジタル製品
適合基準	☆1：ETSI EN 303 645及びCLSの記載内容を中心に検討(ただし、総務省技適の要件、CCDSの要件も参照のほか、事務局にて記載内容を検討)	☆1：ETSI EN 303 645の基準の一部(※1) ☆2：☆2の基準に加え、ETSI EN 303 645の基準の一部(※2) ☆3及び☆4：☆2の基準に加え、IMDA「IoT Cyber Security Guide」の基準	ETSI EN 303 645の基準の一部(5.1-1、5.1-2、5.2-1、5.3-13)	NISTIR 8425をベースとした基準となる見込み	- 製造者への「セキュリティ特性要件に従った上市前の設計・開発・製造」、「上市後の積極的に悪用された脆弱性・インシデントの報告」等を義務付ける予定 - 法案の内容について(欧州委員会・議会・理事会間で)政治合意済。発効後、基準策定機関に対して法案に伴う基準の策定が命じられる予定。
評価方法	☆1、☆2：自己適合宣言 ☆3以上：第三者	☆1及び☆2：自己適合宣言 ☆3及び☆4：自己適合宣言及び評価機関による試験	自己適合宣言	検討中	「重要なデジタル製品」以外の製品：自己適合宣言 「重要なデジタル製品」のクラスⅠ(リスクが低い製品)でEUCCやEN規格の対象外の製品及びクラスⅡ(リスクが高い製品)の製品：第三者認証

2-11 経済産業省が念頭に置く☆2の展開戦略

■ 経済産業省が念頭に置く☆2の展開戦略の流れ



[ステップ2-1]
システム全体の要件策定



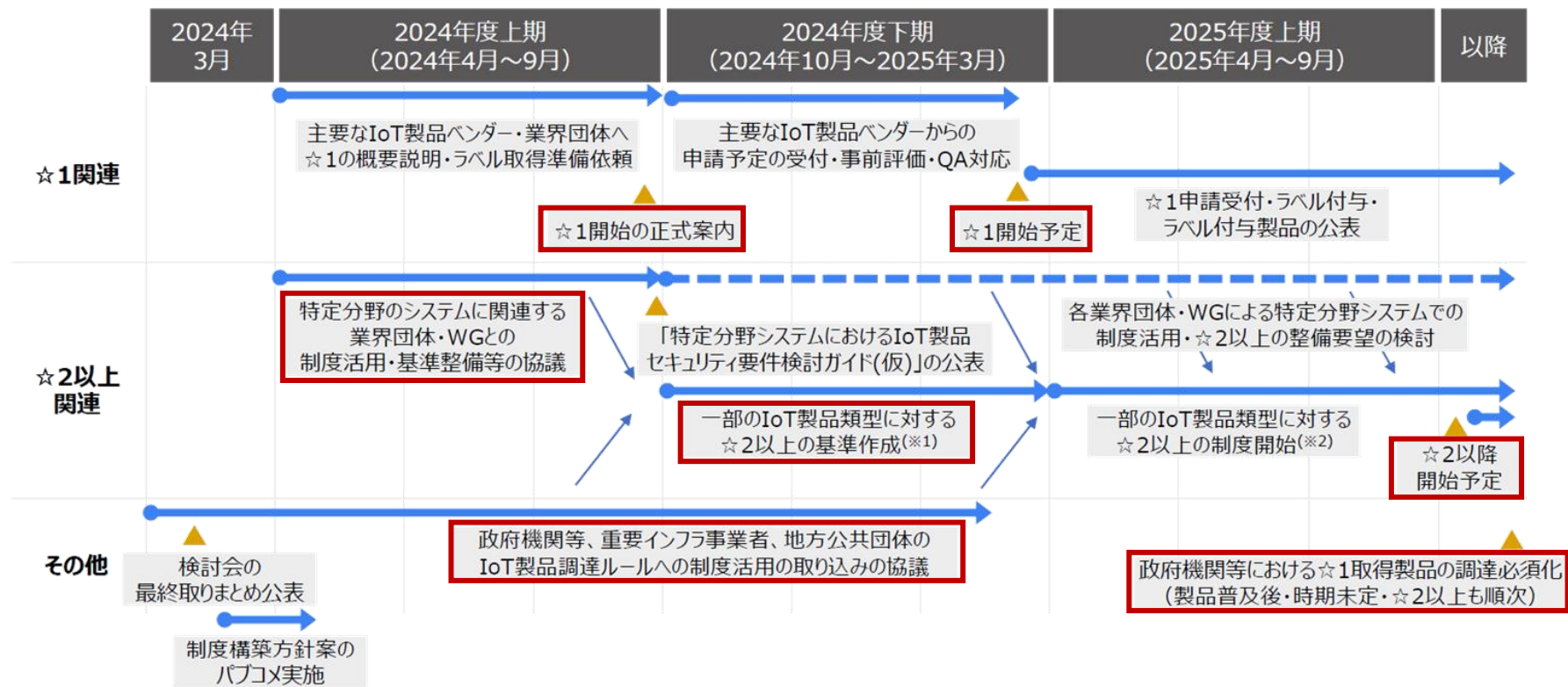
[ステップ2-2]
IoT機器の要件策定

※ 各業界団体・WGが中心、
経産省認証制度は連携

■ 上記流れにおけるポイント

- ステップ1: 海外との相互認証を見据えて、輸出企業を積極的に要件検討メンバに参画頂く
- ステップ2: システム全体(応用例)要件を先に検討後、システムを構成するIoT機器の要件を検討

2-12 今後のスケジュール



(※1)優先度の高い製品類型(2～3種の想定)が対象、基準が完成次第、順次☆2以降の開始予定を案内
(※2)以降、対象となる製品類型を順次拡張

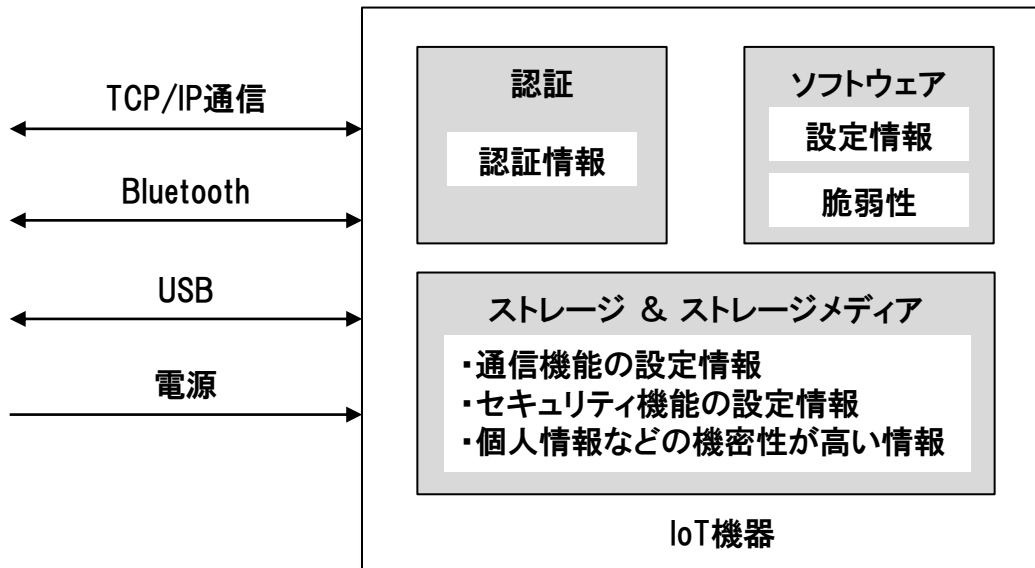
※ IoT製品に対するセキュリティ適合性評価制度構築方針案(概要説明資料)より引用し、筆者で追記・加工
<https://www.meti.go.jp/press/2023/03/20240315005/20240315005-33rr.pdf>

3. ☆1 セキュリティ要件の概要

経済産業省 産業サイバーセキュリティ研究会 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 最終とりまとめ
別添2 ☆1セキュリティ要件・適合基準を基に、筆者が本章を作成
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/pdf/20240315_3.pdf

3-1 ☆1のセキュリティ要件を説明するためのIoT機器モデル

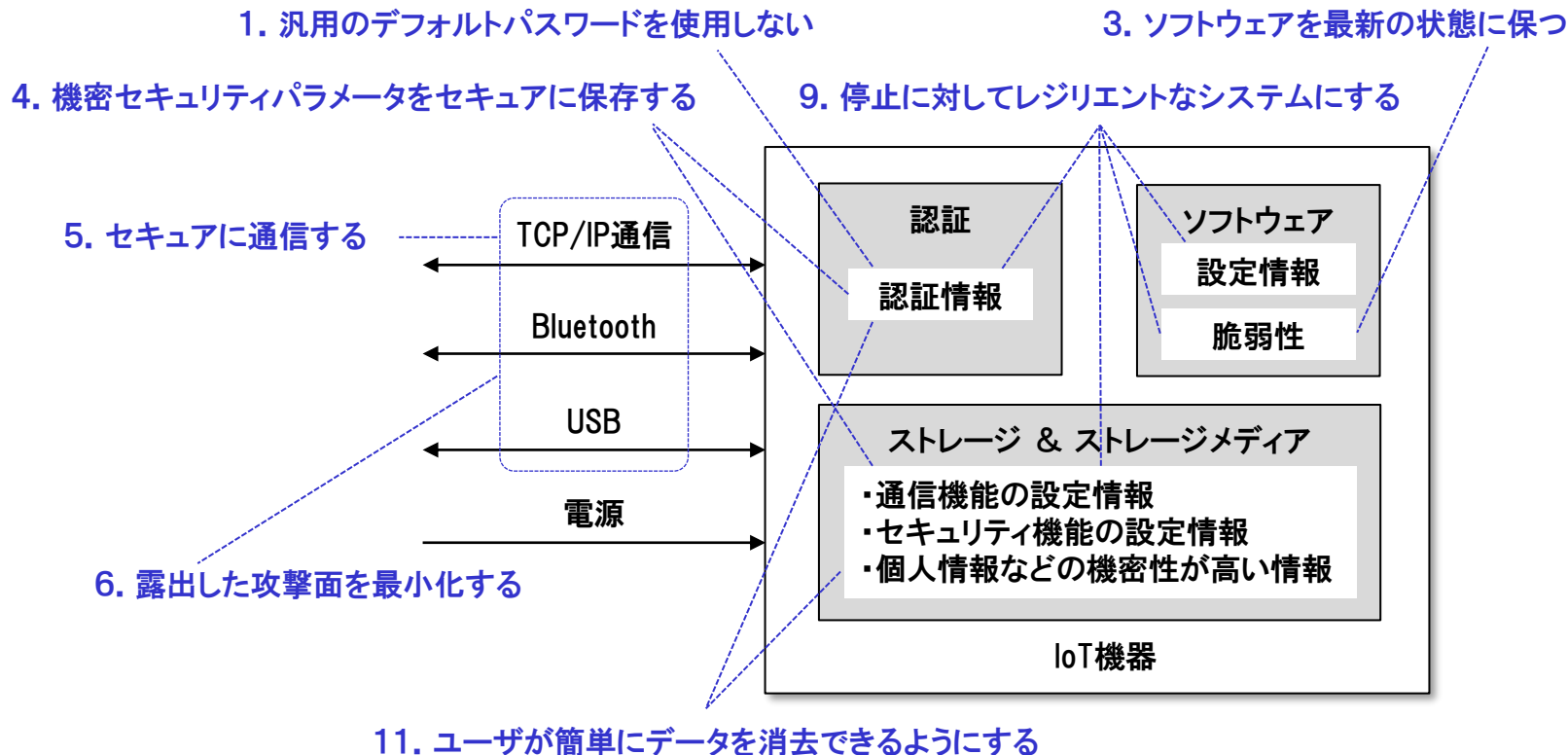
■ ☆1のセキュリティ要件※を説明するためのIoT機器モデル



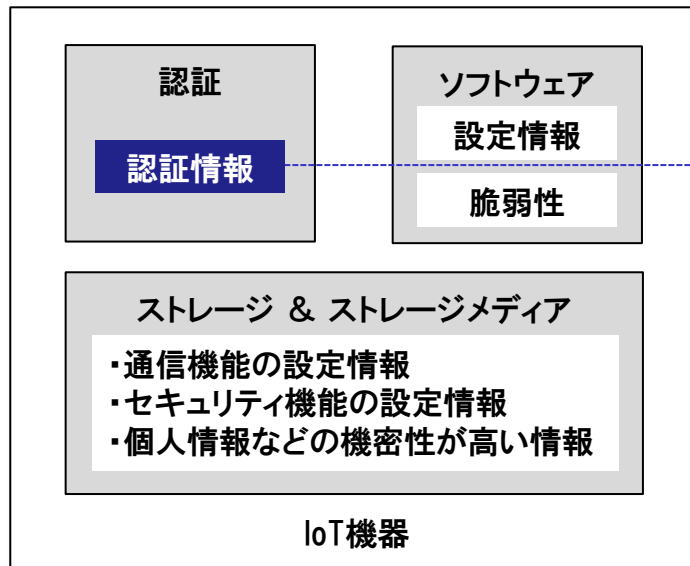
※ 2024年3月中旬から4月中旬にかけて、パブリックコメントを実施した結果は未反映なので、要件が変わる可能性もある。

3-2 ☆1のセキュリティ要件 その1（機能要件のカテゴリ）

■ ☆1のセキュリティ要件、機能要件のカテゴリ



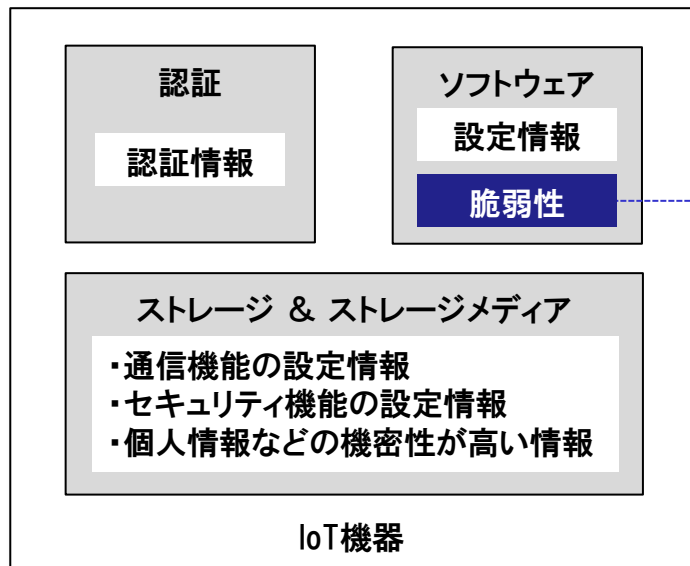
■ カテゴリ「汎用のデフォルトパスワードを使用しない」の詳細要件



1. 汎用のデフォルトパスワードを使用しない

- 1-1 すべてのパスワードは機器毎に固有かユーザによって定義
- 1-2 プリインストールされた固有パスワードは十分なランダム性が必要
- 1-3 想定するリスクを十分に低減できる技術を用いた認証メカニズム
- 1-4 認証値(認証情報)を変更するためのシンプルなメカニズムの提供
- 1-5 ブルートフォース攻撃が実行できないようなメカニズムの保有

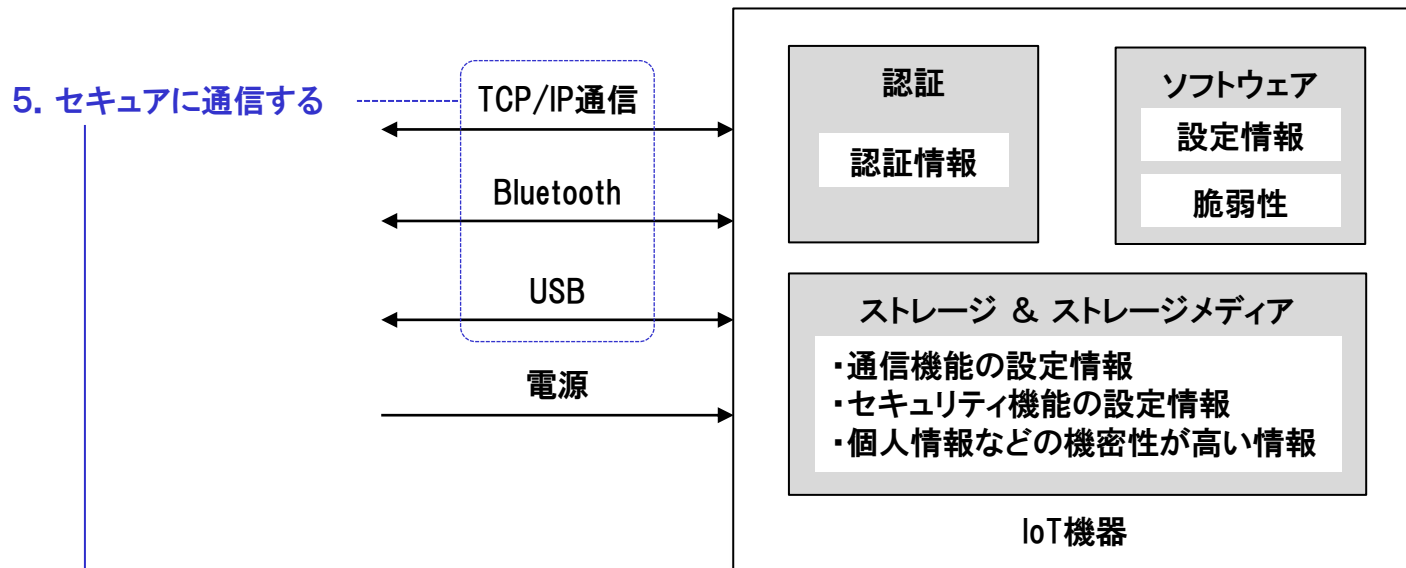
■ カテゴリ「ソフトウェアを最新の状態に保つ」の詳細要件



3. ソフトウェアを最新の状態に保つ

- 3-1 ソフトウェアコンポーネントがアップデート可能であること
- 3-2 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る
- 3-3 ユーザが簡単に適用できるアップデートメカニズムであること
- 3-7 セキュアなアップデートメカニズムのための暗号技術の使用
- 3-8 セキュリティアップデートの適時適用
- 3-10 ネットワークインタフェースを介してのアップデートの真正性及び完全性の検証
- 3-16 製品上のラベルまたは物理的インタフェースを介してユーザに明確に認識可能な製品のモデル名称の提供

■ カテゴリ「セキュアに通信する」の詳細要件



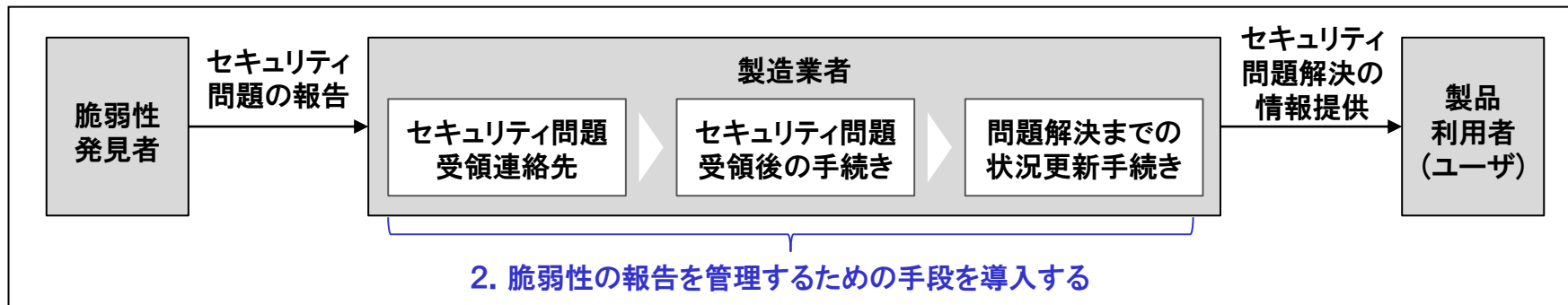
5-1 ベストプラクティスの暗号技術の使用

5-5 セキュリティ関連設定の変更可能にする製品機能は、認証後にのみアクセス可能とする

5-7 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の保護

3-6 ☆1のセキュリティ要件 その5（運用要件のカテゴリと詳細要件）

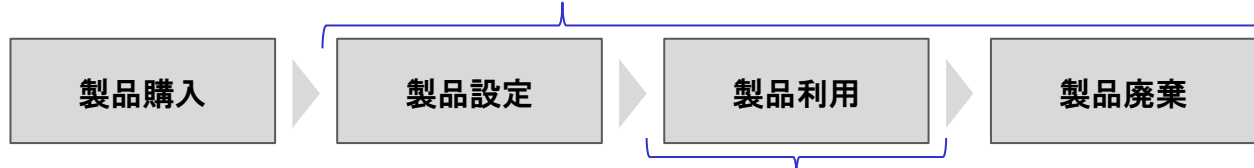
■ ☆1のセキュリティ要件、運用要件のカテゴリとその詳細要件



17. 製品に関する情報提供を行う

17-2 製品をセキュアに設定・利用・廃棄する方法のユーザへの提供

17-5 廃棄する手順を指定された方法でユーザへ提供



17-3 セキュリティアップデートの必要性とアップデートによって軽減されるリスク情報のユーザ提供

17-8 サポート期間のユーザへの明確で透明性のある公表

17-10 脅威を引き起こす可能性のある製品利用状況に関する情報のユーザへの提供

- IoT製品に対するセキュリティ適合性評価制度は、日米欧を含む全世界的な流れである。
- 本制度の普及当初は、補助金制度との連携含む、経済産業省の普及策もあり、事業優位性を得るために、積極的な適合ラベル取得を推奨する。
- 政府機関等、重要インフラ事業者、地方公共団体の調達では、実質的強制の可能性が高く、これら事業分野では適合ラベル取得は特に優先される。
- 日立チャネルソリューションズは、マストトップ社と共に本制度の第三者検証事業※に参入予定であり、自主検証に不安を抱えている企業に支援が可能である。

※ 機器検証サービス | 日立チャネルソリューションズ ([hitachi-ch.co.jp](https://service.hitachi-ch.co.jp))

<https://service.hitachi-ch.co.jp/common/service/security>

END

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」の概説

2024/07/26

日立チャネルソリューションズ株式会社
情報セキュリティ統括センタ



Hitachi Social Innovation is
POWERING GOOD