経済産業省

資料３－２

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

2023年 7月 19日

本日御議論いただきたいこと

- 今年度の適合性評価の実証方針について【資料３－１】
- **検討を進める具体的な適合性評価スキームについて【本資料】**

１．前回の検討会のご指摘事項

２．本制度における適合性評価スキーム（案）

前回の検討会のご指摘事項

カテゴリ	主なご指摘事項
適合性評価スキームの方式※について	• 方式2の場合、IoT領域で新しいビジネスが生じた場合に、分類が難しく、どのカテゴリーに合致するかの判断ができないおそれがある。最低限求められるレベルを設定する意味では、方式1も検討すべきである。最終的には方式1と方式2のハイブリットになることがベストだと考えている。 • 米国では、方式1と方式2の間をとった方式1.5のようなスキームを採用している。ベーシックな統一的スキームが一番下にあり、その上に既存スキームが乗っているイメージである。本制度でも、そのような方式1.5を採用するのが良いと思われる。
認定機関や認証機関について	• セキュリティ領域に関する経済産業省の関係組織でいえば、IPAが最も馴染みがあるため、認定の部分に関してIPAにも関与いただきたい。 • 本制度がどのように使われるか、そしてどのように優位性を確立できるかという点についても、認定機関で議論いただきたい。 • IoT機器に対して広く対応していく認証機関を後押ししなければ、うまく制度が回らないと考えている。
活用し得る既存制度について	• Sマークはセキュリティの分野に馴染まないのではないかという意見が出ている。 • IPAが運営するJISECを利用した方が早く制度を構築できると感じた。
検討体制のあり方について	• IoT製品を供給する実業界に力点をおく実務的な委員会を構築いただきたい。 • 評価基準等を検討する委員会の構築はベンダーにとっても関心が強いため、その検討にはベンダーも関与したい。
制度の果たすべき役割や位置づけについて	• セキュリティが果たす効果や機能について、ベンダーや国民、世界の人々がどういった利益を受けるのかを中心に、考える必要がある。 • 本制度を通じて、技術的な担保とは別の安心を購入者や利用者に対して提供するためにはどうすべきかについて、議論した方が良い。 • 産業経済や社会の活力向上に資するという積極的な位置づけで、規制についても検討を行う必要がある。
製造物責任について	• 製品を作ったベンダーとして、本制度の認証を取得することによって一定程度の責任を果たしていると判断されるのであれば、認証を取得するインセンティブに繋がると考える。利用者側としても、粗悪な製品ではなく、認証を取得している正しい製品を選んだという説明責任が果たせる。製品のサポート期間・期限に関しても、責任に伴って議論する必要がある。 • 誰かの責任を追及することなく被害が公平に分担される社会の構築に資する制度の提言について、日本がリードできると良い。
適合性評価の要件・基準について	• 製品サポートが終了した場合に使用してはならない製品群なのか否かについて、ユーザ側が分かる形にする必要がある。 • 基準を一部満たさなくなった製品が出てきた場合、他の機能で補うことができるか否かについて整理すべきである。
サーベイランスや有効期限について	• IoT機器のライフタイムを考えると、サーベイランスまで要求する必要はなく、一回きりの認証でも十分と考える。 • IoT機器の定期レビューをどのようなタイミングで行い、持続感染性のマルウェアの脅威をどのように排除していくかという点は重要な課題になる。 • 認証の有効期限の設定に関する議論は最初の段階で行うべきである。
国際連携について	• 諸外国の制度と全く異なった制度を作ることは避けるべきである。 • 本制度を活用した製品がグローバルで通用するか否かは、本制度を活用するインセンティブに大きく関わる部分だと認識している。 • 国際的なハーモナイゼーションを考える際、製品については先手を取られているため、要素や責任の部分で勝負する、新機軸を打ち出す、といった視点があっても良い。
制度のプロモーションについて	• エアコンの統一省エネラベルのように、「製品を選ぶ理由付けとなるマーク」が付与されるのであれば、メーカーも認証取得に向けて努力すると思われる。 • 本制度をプロモーションするうえで、2025年の大阪万博が期待できると考えている。開催までに制度の構築が間に合えば良い。

※ 適合性評価スキームの方式について

✓ 方式1：広範なIoT製品が活用可能な統一的なスキーム（既存スキームの活用も考慮）を用意し、レベル1については、統一的なスキームで適合性評価・マーク等の付与を行う。より高いレベル（2,3・・・）に関する適合性評価を行う場合のみ、既存スキームにて適合性評価・マーク等の付与を行う。

✓ 方式2：各レベルの基準を各スキームに落とし込み、それぞれのスキームにおいて適合性評価・マーク等の付与を行う。

１．前回の検討会のご指摘事項

２．本制度における適合性評価スキーム（案）

適合性評価制度における適合性の方式

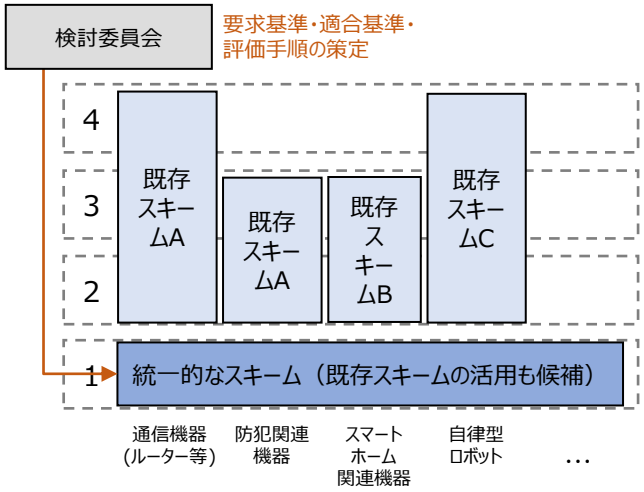
第３回のご指摘事項	• 方式2の場合、IoT領域で新しいビジネスが生じた場合に、分類が難しく、どのカテゴリーに合致するかの判断ができないおそれがある。最低限求められるレベルを設定する意味では、方式1も検討すべきである。最終的には方式1と方式2のハイブリットになることがベストだと考えている。 • 米国では、方式1と方式2の間をとった方式1.5のようなスキームを採用している。ベーシックな統一的スキームが一番下にあり、その上に既存スキームが乗っているイメージである。本制度でも、そのような方式1.5を採用するのが良いと思われる。
中間とりまとめの記載事項	• 適合性評価制度の運用に当たっては、既存の評価スキームを活用した制度とすることが適当である。

製品類型ごとにリスクの度合いが異なるところ、求められる対策レベルも製品類型ごとに異なる。複数の対策レベルについて評価を行う方式として、前回検討会では方式1・方式2の２つの方式を提示したが、**前回検討会での御意見を踏まえ、方式1の統一的スキームとして扱うことで基準の整合性が図れる点、方式2の同一製品においてレベルを１つのスキームで完結できる点を取り入れた、新たな方式が考えられる。**

- ✓ 方式1. 広範なIoT製品が活用可能な統一的なスキーム（既存スキームの活用も考慮）に基づき、☆1については、統一的なスキームで適合性評価・マーク等の付与を行う。より高いレベル（☆2,☆3,・・・）に関する適合性評価を行う場合のみ、既存スキームにて適合性評価・マーク等の付与を行う。
- ✓ 方式2. 各レベルの基準を各スキームに落とし込み、それぞれのスキームにおいて適合性評価・マーク等の付与を行う。
- ✓ **新方式.** 広範なIoT製品が活用可能な一つの既存スキームに基づき、☆1については、統一的な適合基準に基づき適合性評価・マーク付与を行う。より高いレベル（☆2,・・・）については、製品類型ごとに適合基準を策定し、適合性評価・マーク付与を行う。評価済み製品が次のレベルの評価を受ける際、既存の評価結果を流用できる方式とする。

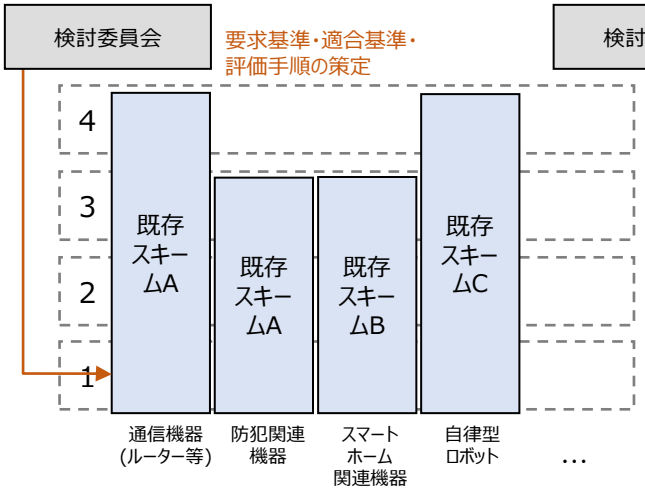
方式1

☆1のみ、統一的なスキームで適合性評価・マーク等の付与を行う方式。



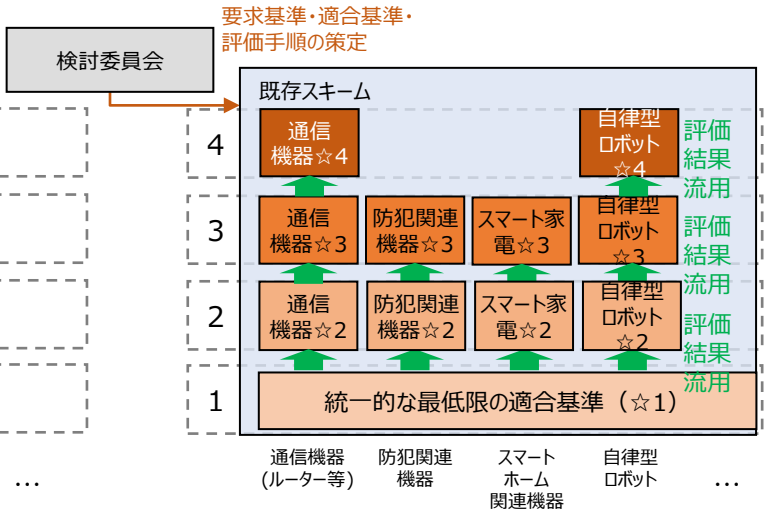
方式2

各スキームにおいて、対策レベルに応じた適合性評価・マーク等の付与を行う方式。



新方式

一つの既存スキームに基づき、☆1は適合基準に基づく適合性評価・マーク付与、☆2以上は製品類型ごとの適合基準に基づく適合性評価・マーク付与を行う方式。

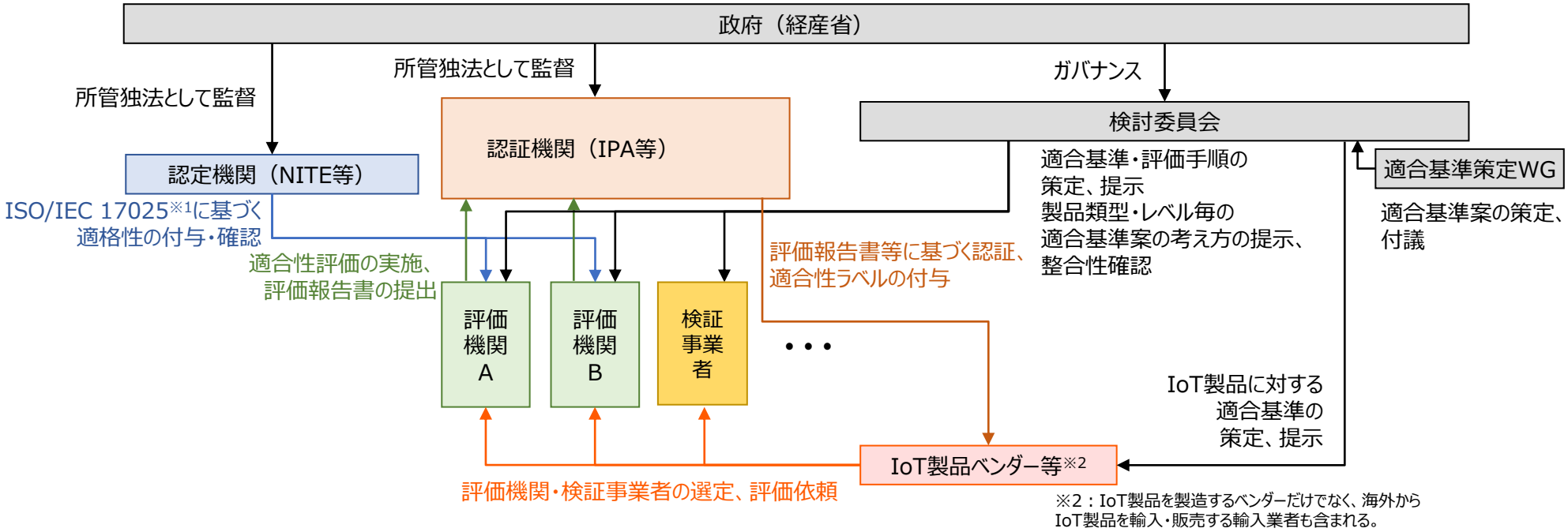


※ 4段階に分けることは一例であることに留意。

JISEC制度をベースとした適合性評価制度の全体像

第３回のご指摘事項	• セキュリティ領域に関する経済産業省の関係組織でいえば、IPAが最も馴染みがあるため、認定の部分に関してIPAにも関与いただきたい。 • IPAが運営するJISECを利用した方が早く制度を構築できると感じた。
中間とりまとめの記載事項	• 各主体の適格性について、政府のガバナンスが効く構造を構築することが重要となる。 • 適合性評価制度の対象製品範囲は「間接的又は直接的にインターネットに接続する製品」とすることが適当である。 • 適合性評価制度で用いる適合性評価基準については、国際的な標準を参照の上、国際的な標準と整合的な形で構築していくことが適当である。 • 各分野の専門家を招聘し、評価基準等を検討する委員会を設置することが適当と考えられる。

これまでの議論を踏まえ、本制度の各主体の適格性について、政府のガバナンスが効く構造が重要となる。また、制度の対象製品について、「間接的又は直接的にインターネットに接続する製品」とすることが適当であるほか、適合性評価基準については、国際的な標準と整合的な形で構築していくことが適当である。こうした点を踏まえると、**IPAのJISEC認証制度（ITセキュリティ評価及び認証制度）を参照しつつ、これを拡張する形の制度を構築することが考えられる**。（新方式とも整合的）

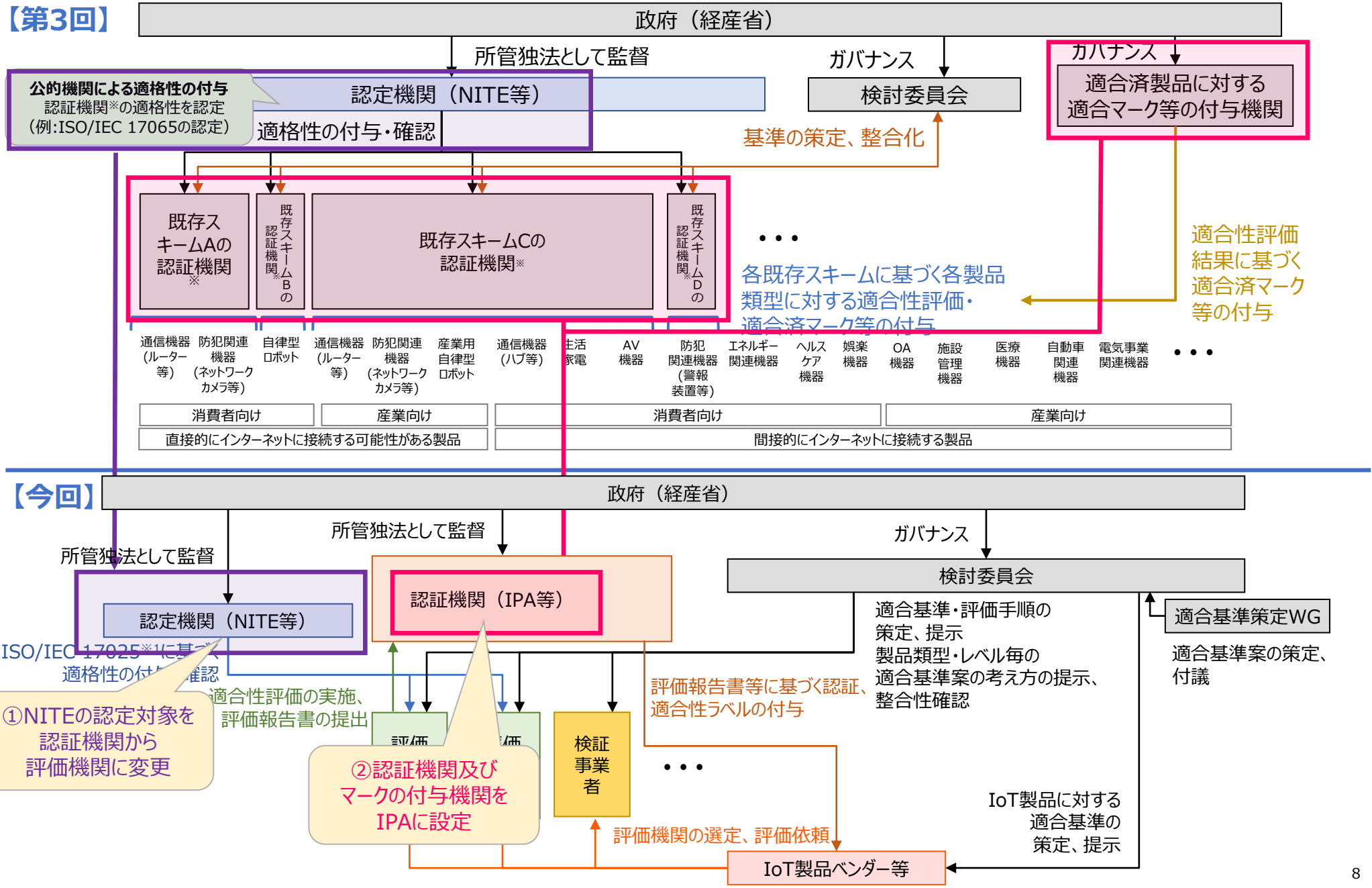


※2：IoT製品を製造するベンダーだけでなく、海外からIoT製品を輸入・販売する輸入業者も含まれる。

※1：ISO/IEC 17025（JIS Q 17025）は、試験所及び校正機関の試験・校正能力に関する一般要求事項を規定した国際標準であり、JISEC認証制度に基づくIT製品及びシステムのセキュリティ評価を行う試験事業者に求められる。なお、ISO/IEC 17065（JIS Q 17065）は、製品認証機関の認証能力に関する一般要求事項を規定した国際標準である。

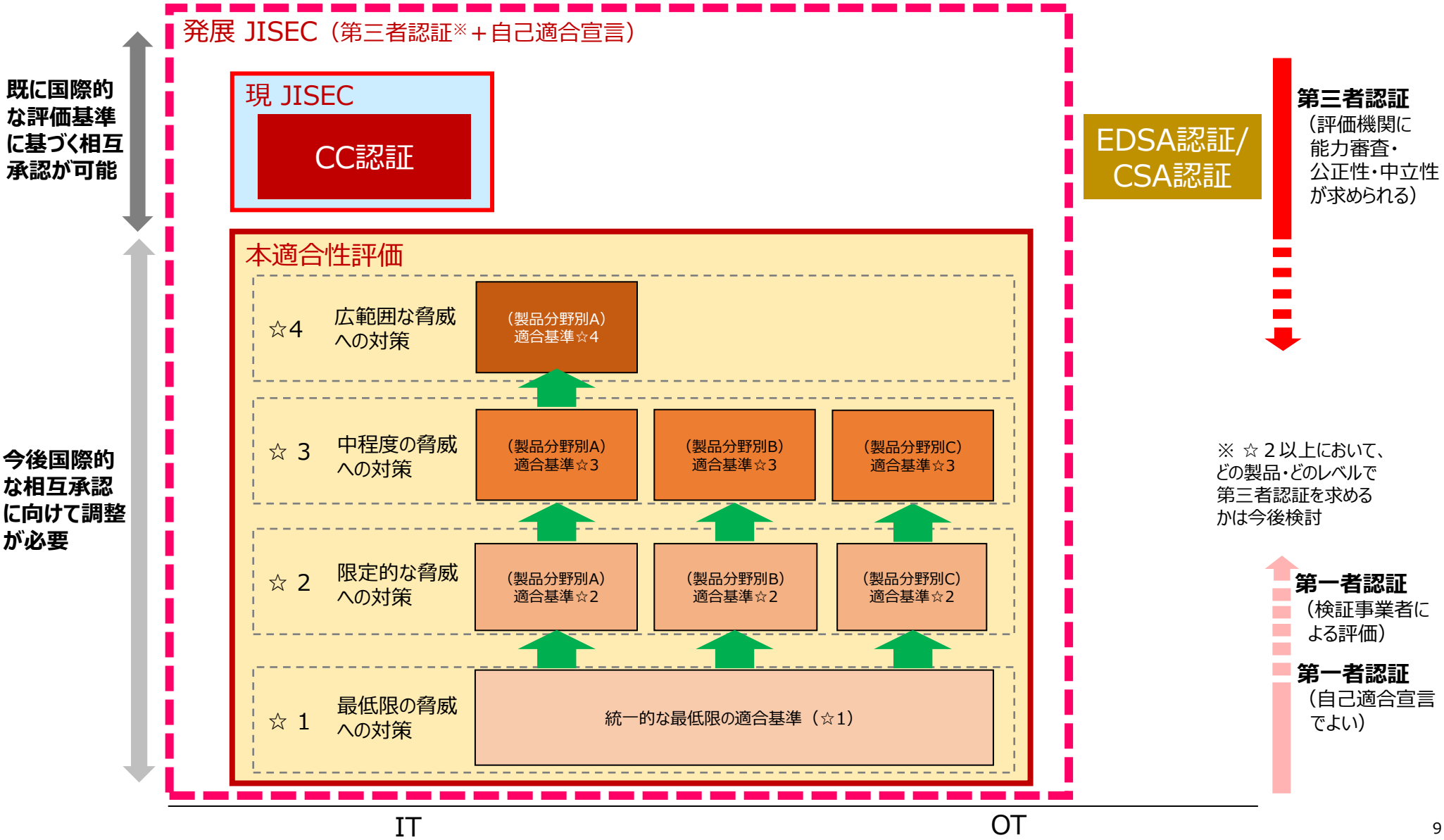
注）組織名称は制度発足時に変更となる可能性がある。

【参考】第3回検討会で示した適合性評価制度の全体像との違い

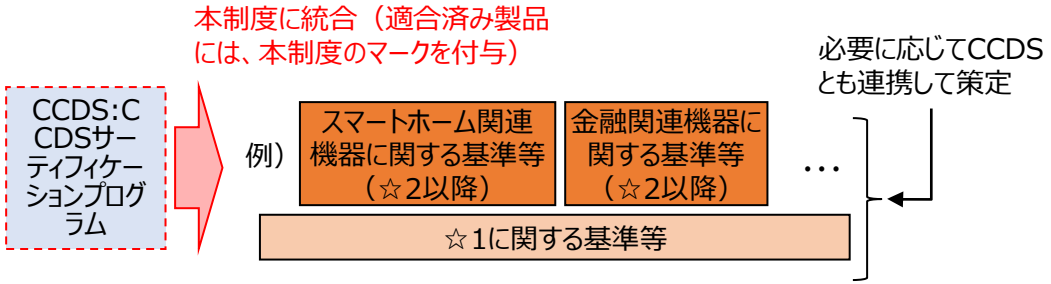
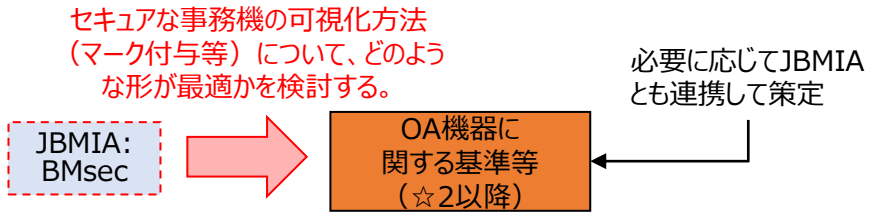
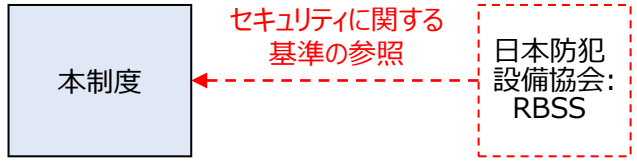


既存制度との関係性

現行のJISEC制度はCC認証のみを対象としているが、本適合性評価制度の構築にあたって、JISEC制度のこれまでの知見やリソースを有効に活用するために、JISEC制度を本適合性評価制度を含む形で拡張する新たな枠組みを立ち上げる。EDSA認証／CSA認証との整理は今後要検討。



既存制度との連携・合流（将来像）

既存適合性評価スキーム	概要	対象製品	本制度との連携イメージ（将来像）
CCDSサーティフィケーションプログラム （重要生活機器連携セキュリティ協議会(CCDS)）	• CCDSが定める「IoT機器セキュリティ要件ガイドライン」に基づき、指定検査資格者による検査により基準を満たしていると判断された場合、CCDSがマークを付与する仕組み	• インターネットに接続可能な機器及びシステム	• **CCDSサーティフィケーションプログラムを本制度に統合する。** • **策定する適合基準や評価手法について、これまでの検討実績や知見を踏まえ、必要に応じてCCDSとも連携して策定する。** 
BMSec（事務機セキュリティプログラム） （ビジネス機械・情報システム産業協会(JBMIA)）	• 「事務機セキュリティガイドライン」に基づきメーカー自身が自己適合宣言を行い、適合結果をJBMIAが確認・公開する仕組み	• エントリークラス/SOHO向けのOA機器	• **事務機の購入／調達者にとってより良い制度という観点でJBMIAにおいても検討を進める。** • **策定するOA機器の適合基準や評価手法について、これまでの検討実績や知見を踏まえ、必要に応じてJBMIAとも連携して策定する。** 
RBSS (日本防犯設備協会)	• 防犯機器に必要とされる機器と性能の基準を策定し、その基準に適合した機器を「優良防犯機器」と認定する仕組み	• 防犯カメラとデジタルレコーダ • LED防犯灯	• **RBSSのセキュリティ基準は、本制度で策定した基準を参照するものとする。（具体的な参照方法については継続検討）**  （基準に適合した製品については、RBSSのマークが付与される。）

【参考】製品に関する類型・既存の文書、認証制度等

【凡例】
- 製品個別のセキュリティ対策に関するガイドライン
- 製品個別のセキュリティ対策基準を定めた文書等（下線は義務）
- 製品個別のセキュリティ対策要件を含む認証制度
- システム全体のセキュリティ対策に関する文書等

赤字：Sマークによる認証が行われている製品

注）各製品類型に対するセキュリティ対策要件を定めたガイドラインや認証制度のうち、代表的なガイドライン、制度等をマッピングしている。ただし、CC（ISO/IEC 15408）に基づく認証制度については、グローバルで認証付与されている代表的な製品類型又はcPP(Collaborative Protection Profile)が用意されている製品類型に対してマッピングをしている。また、IEC 62443-4に基づく認証について、IEC 62443-4の対象である通信機能を有する産業用自動制御システムのコンポーネントに対してマッピングしている。

		製品類型	製品個別の対策に関するガイドライン、基準を定めた文書、認証制度等	高いレベルの基準に基づく認証制度	システム全体の対策に関する文書等
直接的又は間接的にインターネットに接続する製品	直接的にインターネットに接続する可能性がある製品	消費者向け	通信機器（ブロードバンドルーター、Wi-Fiルーターなど） 防犯関連機器（ネットワークカメラなど） 自律型ロボット（ドローンなど）	総務省：技術基準適合認定及び設計についての認証 CCDS：分野別ガイドライン（IoT-GW編） 日本防犯設備協会：RBSS（監視カメラ、デジタルレコーダー） NEDO：無人航空機分野 サイバーセキュリティガイドライン CCDS：CCDSサーティフィケーションプログラム（現状で取得実績は無いが、対象製品範囲に含まれる）		経産省：スマートホームセキュリティガイド CCDS：分野別ガイドライン（スマートホーム編）
		産業向け	通信機器（ルーター、アクセスポイント、ファイアウォール、UTMなど） 防犯関連機器（ネットワークカメラなど） 産業用自律型ロボット（産業用ドローン、AGVなど）	日本防犯設備協会：RBSS CCDSサーティフィケーションプログラム（カメラで実績あり） IPA：情報セキュリティ対策要件チェックリスト（ネットワークカメラ） NEDO：無人航空機分野 サイバーセキュリティガイドライン 国交省：機体認証制度	CC認証 IEC 62443-4に基づく認証	
	間接的にインターネットに接続する製品	消費者向け	通信機器（ハブ・スイッチなど） 生活家電（掃除機、洗濯機、冷蔵庫、レンジ、エアコンなど） AV機器（スマートTV、レコーダー、スマートスピーカーなど） 防犯関連機器（警報装置、電気錠システムなど） エネルギー関連機器（エネファーム、PCS、ガス給湯器など） ヘルスケア機器（ウェアラブル端末、電動トレーニングマシンなど） 娯楽機器（ゲーム機、スマート玩具など）	CCDS：CCDSサーティフィケーションプログラム（現状で取得実績は無いが、対象製品範囲に含まれる） 日本防犯設備協会：RBSS CCDS：CCDSサーティフィケーションプログラム（電気錠操作盤、電子シャッターで取得実績あり） JET：系統連系保護装置等認証制度（PCSのみ） CCDSサーティフィケーションプログラム（ガス給湯器リモコンで実績あり） 各一般送配電事業者：系統連系技術要件		経産省：スマートホームセキュリティガイド CCDS：分野別ガイドライン（スマートホーム編）
		産業向け	通信機器（ハブ・スイッチなど） 産業用コントローラー（PLC、DCSコントローラーなど） 産業用センサー（温度センサー、圧力センサー、変位センサーなど） OA機器（複合機など） 金融関係機器（決済端末、POS端末など） 施設管理機器（入退室機器、受変電設備、照明、昇降機など） 医療機器（人工呼吸器、人工心臓弁、輸液ポンプなど） 自動車関連機器（ECU、IVI、TCUなど） 電気事業関連機器（スマートメーター、発電設備、PCSなど） 製造業・流通業関連機器（生産設備、自動倉庫など） 鉄道事業関連機器（CTC装置、PRC装置など） 航空事業関連機器（IMS、iDMUなど）	CCDS：CCDSサーティフィケーションプログラム（現状で取得実績は無いが、対象製品範囲に含まれる） JBMIA：BMsec CCDS：分野別ガイドライン（ATM編、オープンPOS編） CCDS：CCDSサーティフィケーションプログラム（ATM、決済端末で取得実績あり） IPA：情報セキュリティ対策要件チェックリスト（入退室管理） 厚労省：医療機器のサイバーセキュリティの確保及び徹底に係る手引書 厚労省：医療機器の薬事承認等 国交省：道路運送車両の保安基準 CCDS：分野別ガイドライン（車載器編） JESC：スマートメーターシステムセキュリティガイドライン	CC認証 IEC 62443-4に基づく認証	※ FISC：安全対策基準 経産省：ビルガイドライン 厚労省：医療情報ガイドライン JESC：電制ガイドライン 経産省：工場ガイド 国交省：物流ガイド 国交省：鉄道ガイドライン 国交省：航空ガイドライン

※ 各産業分野に設置される機器については、各ガイドラインにおいて、システム全体に求められるセキュリティ対策が示されている。

☆1における自己適合宣言について

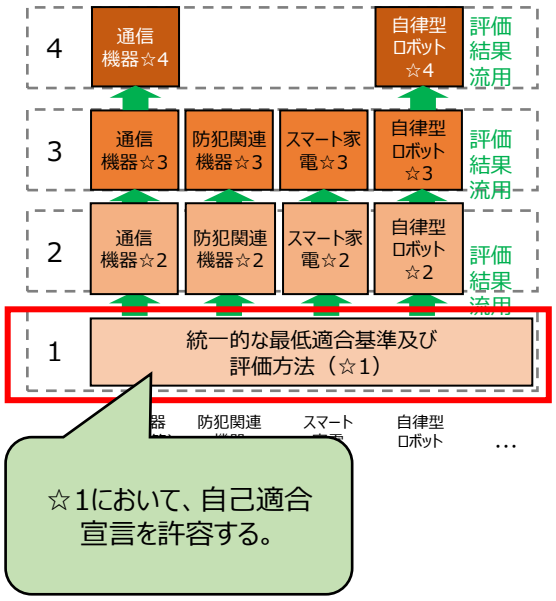
第３回のご指摘事項	• 諸外国の制度と全く異なった制度を作ることは避けるべきである。
中間とりまとめの記載事項	• 具体的に、どの製品類型に対して、どのスキームを活用するかについては、各製品が有するリスクや、事業への影響、普及効果、既存制度等を考慮し、精緻に検討を行っていく必要がある。

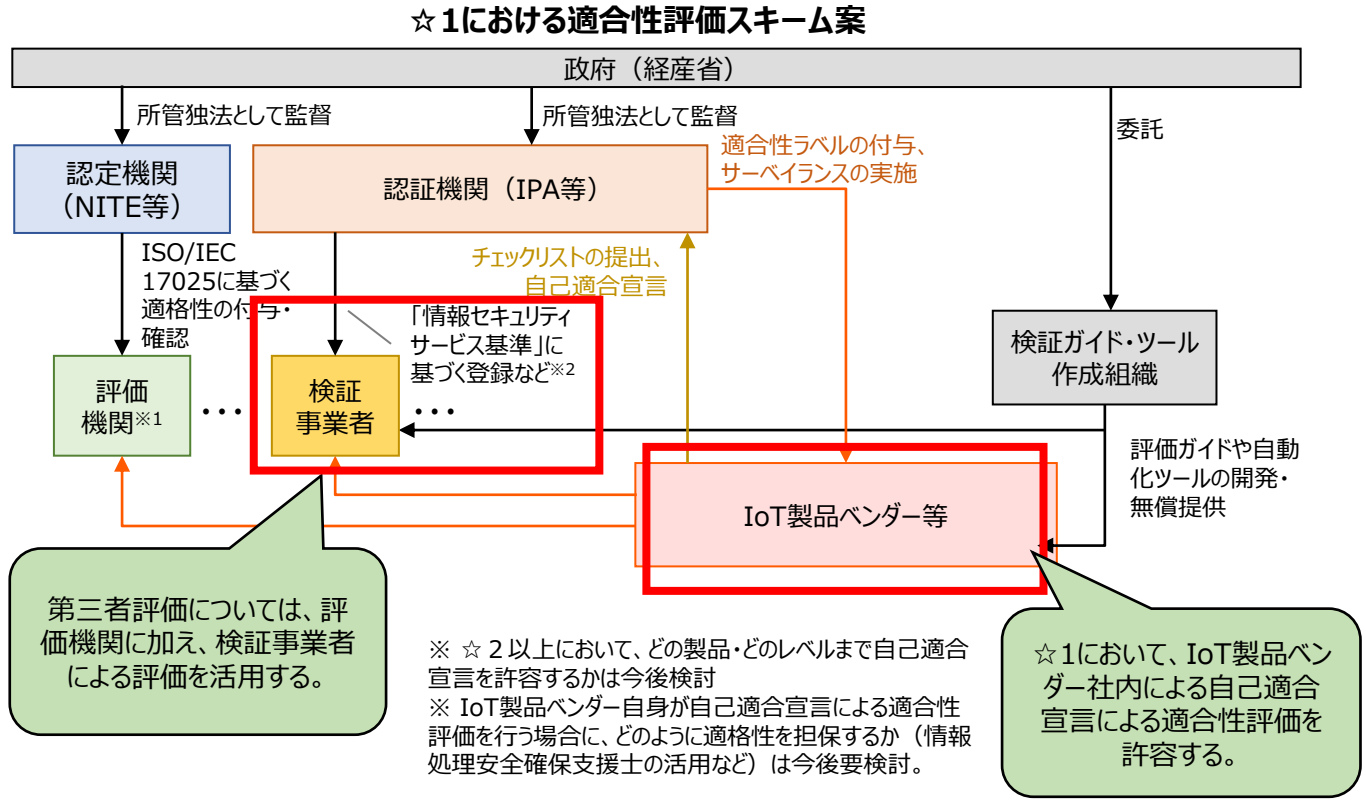
- 制度を広く普及させる観点や諸外国制度の動向を踏まえ、**最低限の適合性評価レベルである☆1においては、情報処理安全確保支援士等の活用などによりIoT製品ベンダーによる自己適合宣言を許容することが考えられる。**

※士業の活用により政府のガバナンス構造も一定程度保たれると考えられる。また、情報処理安全確保支援士などへのインセンティブにも資する。

- また、第三者評価については、**評価機関に加え、情報セキュリティサービス基準に登録された検証事業者による評価も活用することが考えられる**。

※信頼性の確保やリスクに備えるための措置として、有効期限の設定や、サーベイランスの実施、保険の適用等について今後要検討。





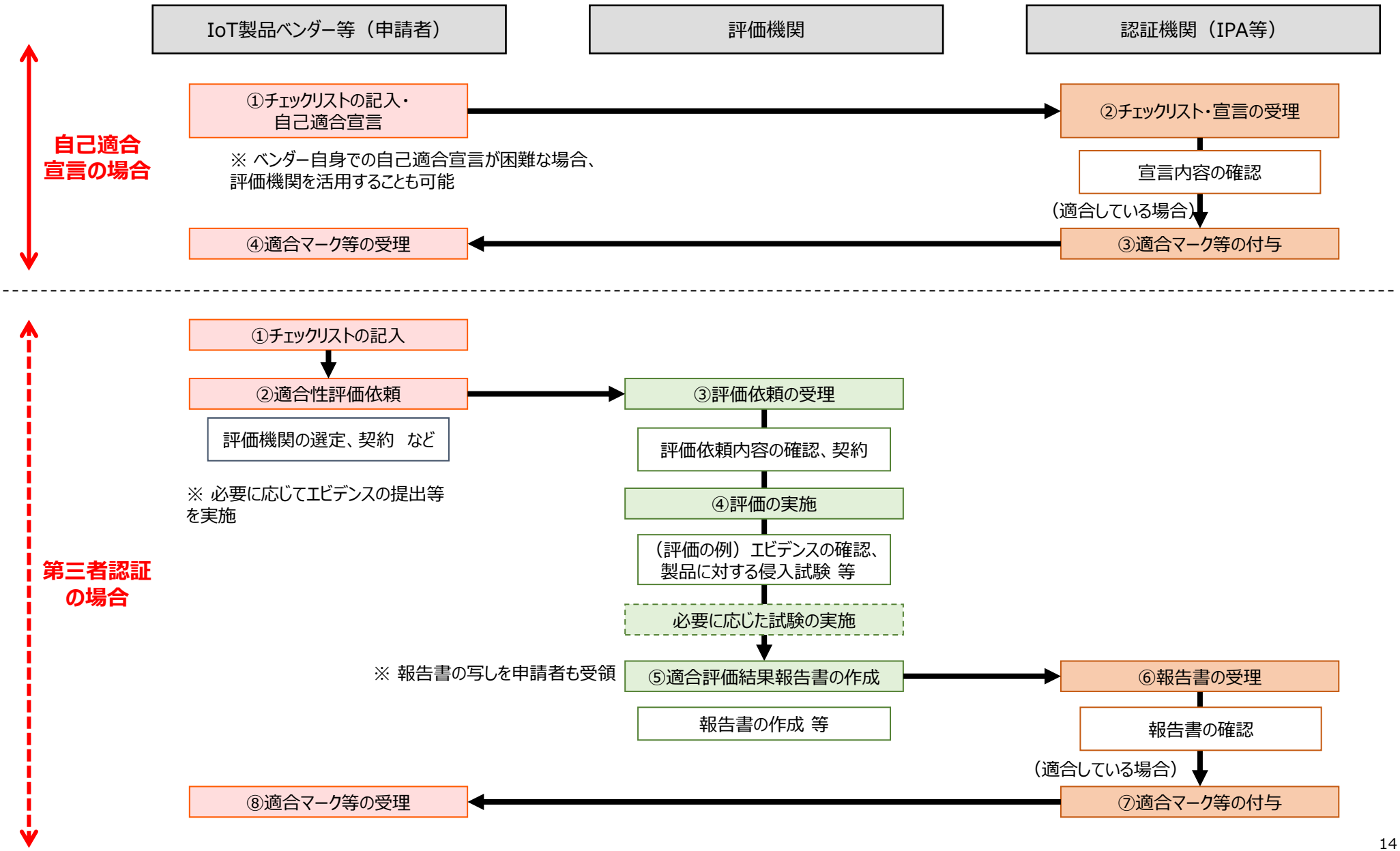
※1 本資料における「評価機関」とは、ISO/IEC 17025に基づき適格性が付与・確認された評価事業者を意味する。
※2 経済産業省の「情報セキュリティサービス基準」における「機器検証サービス」が2023年10月から開始予定である。ガバナンスの観点を踏まえ、本基準に基づき登録された検証事業者による評価結果の活用を許容することが想定される。

【参考】自己適合宣言／第三者認証の比較

評価方法	IoT製品ベンダーの対応	評価機関の対応	認証機関の対応	信頼の基点	既存のセキュリティ適合性評価制度
自己適合宣言	• 自身で対象製品に対する自己評価の実施、チェックシートの作成 • 認証機関へチェックシートの届出	ー※1	• 届出の受付 • チェックシートの確認（形式的なチェック） • （問題がない場合）認証・ラベルの付与	製品ベンダー	【国内】 • CCDSサーティフィケーションプログラム • BMSec（事務機セキュリティプログラム） 【海外】 • シンガポールラベリング制度（＊及び＊＊） • ドイツラベリング制度 • 欧州CRA（「重要なデジタル製品」以外の場合）
第三者認証	• 対象製品の評価を認証機関に依頼	• 第三者の立場で、対象製品の評価を実施し、評価結果報告書を作成 • 認証機関への届出	• 届出の受付 • 評価報告書の確認 • （問題が無い場合）認証・ラベルの付与	評価機関＋認証機関	【国内】 • JISEC（CC認証） 【海外】 • CC認証 • シンガポールラベリング制度（＊＊＊及び＊＊＊＊＊） • フィンランドラベリング制度 • 欧州CRA（「重要なデジタル製品」の場合）

※1 ベンダーのみでの自己適合宣言が困難な場合に、評価機関が実施した評価結果を踏まえてベンダーが自己適合宣言する方式も想定される。

【参考】想定される適合性評価・マーク等付与のプロセス

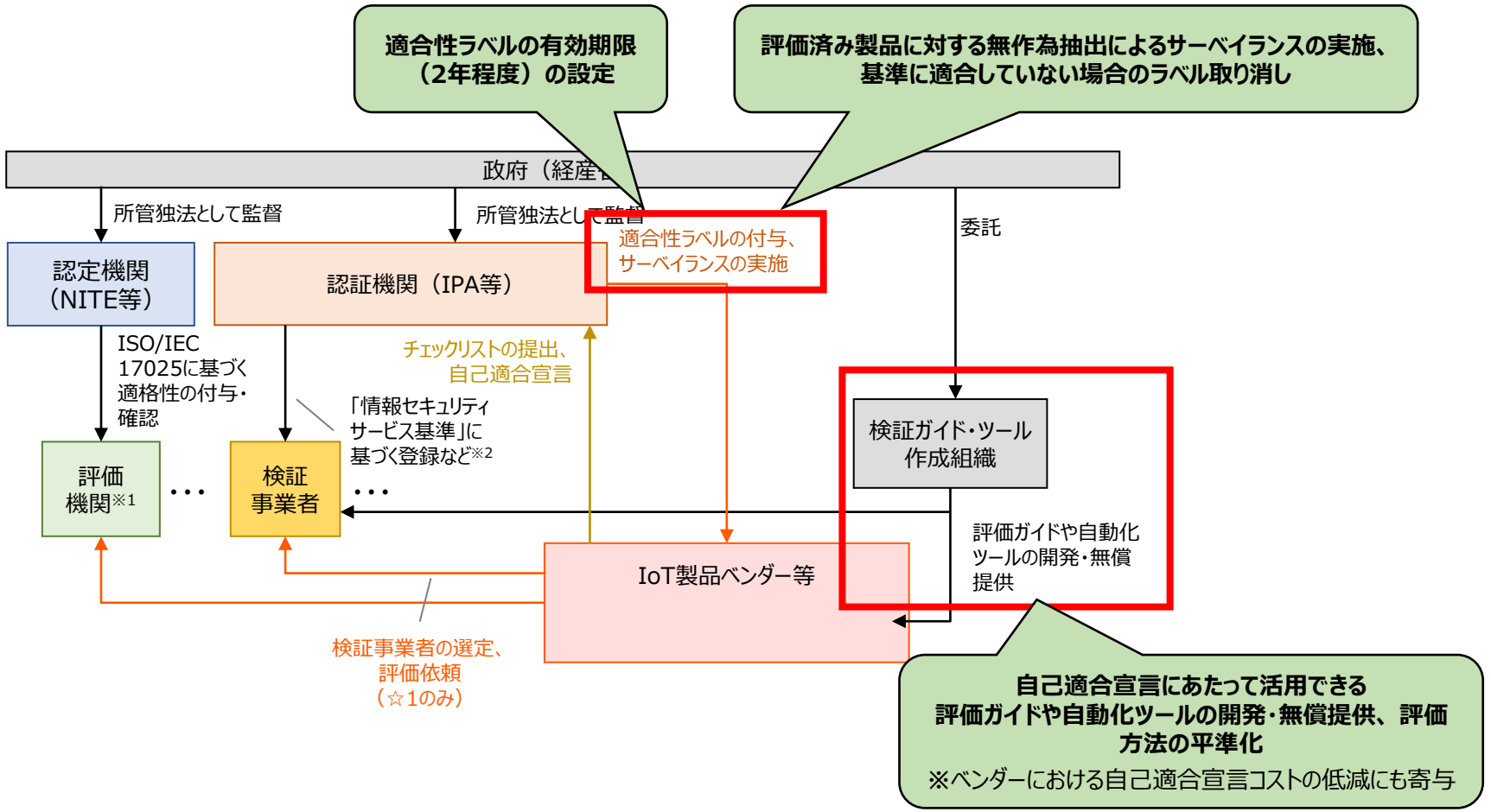


自己適合宣言による評価の信頼性を担保する取組

以下に示すような取組を講じることで、自己適合宣言による評価の信頼性を担保することが考えられる。

- 適合性ラベルの有効期限を設定し、更新する場合には改めて自己適合宣言を行うことを求める。有効期限としては、JISEC制度で許容しうる期限や関連制度における期限を踏まえ、2年程度とすることが想定される。
- 評価済み製品に対する無作為抽出によるサーベイランスを実施し、サーベイランスの結果、基準に適合していないと判断される場合にラベルの取り消しを行う。（参考：シンガポールのCLSにおいても同様の取組を実施している。）
- ベンダーが自己適合宣言にあたって活用できる評価ガイドや自動化ツールを開発・無償提供することで、評価方法を平準化する。

※この取組は、ベンダーにおける自己適合宣言の対応コストの低減にも寄与する。

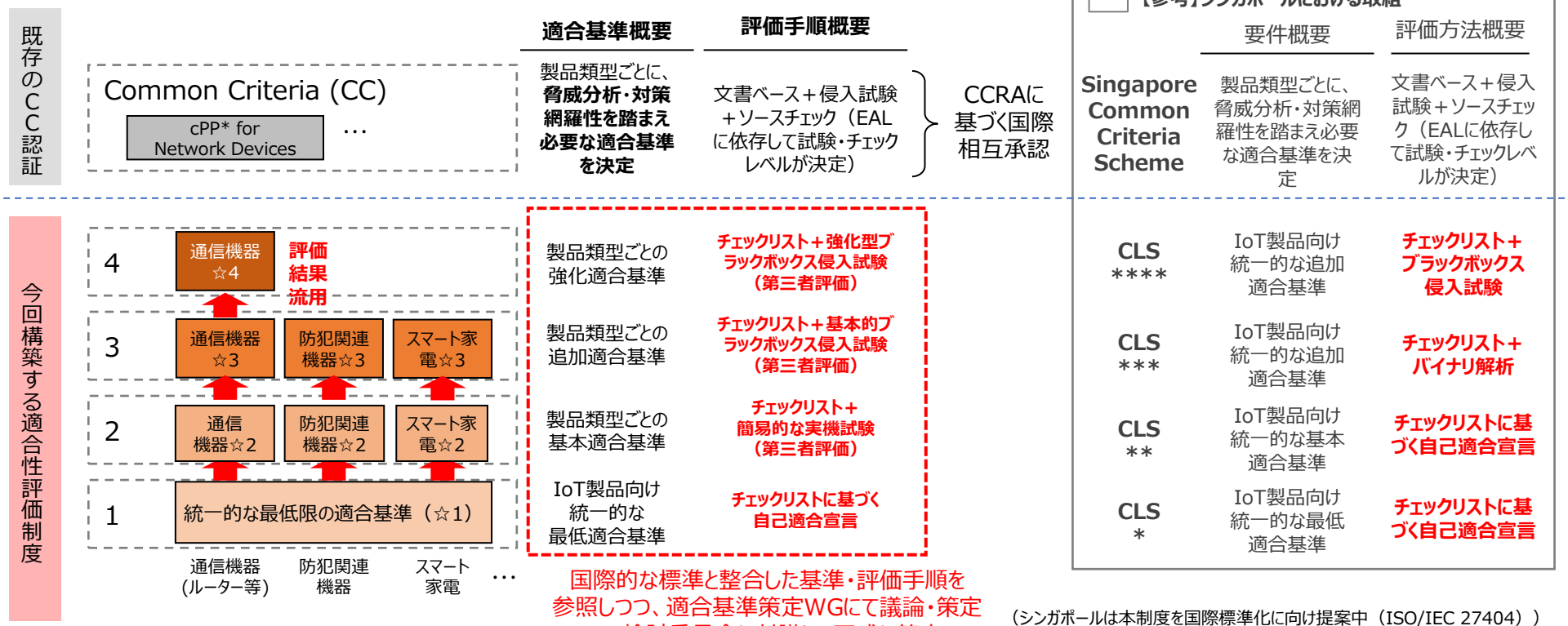


国際連携を想定した各レベルの評価手順

第３回のご指摘事項	• 諸外国の制度と全く異なった制度を作ることは避けるべきである。
中間とりまとめの記載事項	• 諸外国ではIoT製品の適合性評価制度の検討が進んでおり、この認証取得のために日本企業の負担が増えることが想定されるところ、適合性評価制度と諸外国の制度の連携を図ることで、負担幅を抑えることが重要と考えられる。 • 適合性評価制度で用いる適合性評価基準については、国際的な標準を参照の上、国際的な標準と整合的な形で構築していくことが適当である。

- 各レベルで求める具体的な適合基準のみならず、評価手順についても国際的な標準や制度を参照しつつ適合基準策定WGで議論・策定することが考えられる。適合基準策定WGで策定した案は検討委員会に付議され、検討委員会での議論後、正式に策定される。
- 評価済み製品が次のレベルの評価を受ける際、すでにある評価結果を流用できる方式とすれば、効率的な運用に繋がると考えられる。

※本制度に基づき評価した結果がCommon Criteria認証（CC認証）においても活用可能であれば、認証機関・評価機関の人材育成にも資するほか、CC認証の活用促進にも繋がると考えられる



※ 4段階に分けることは一例であることに留意。

（シンガポールは本制度を国際標準化に向け提案中（ISO/IEC 27404））

＊ cPP･･･CCRA加盟国が共同で作成する世界共通の適合基準のこと

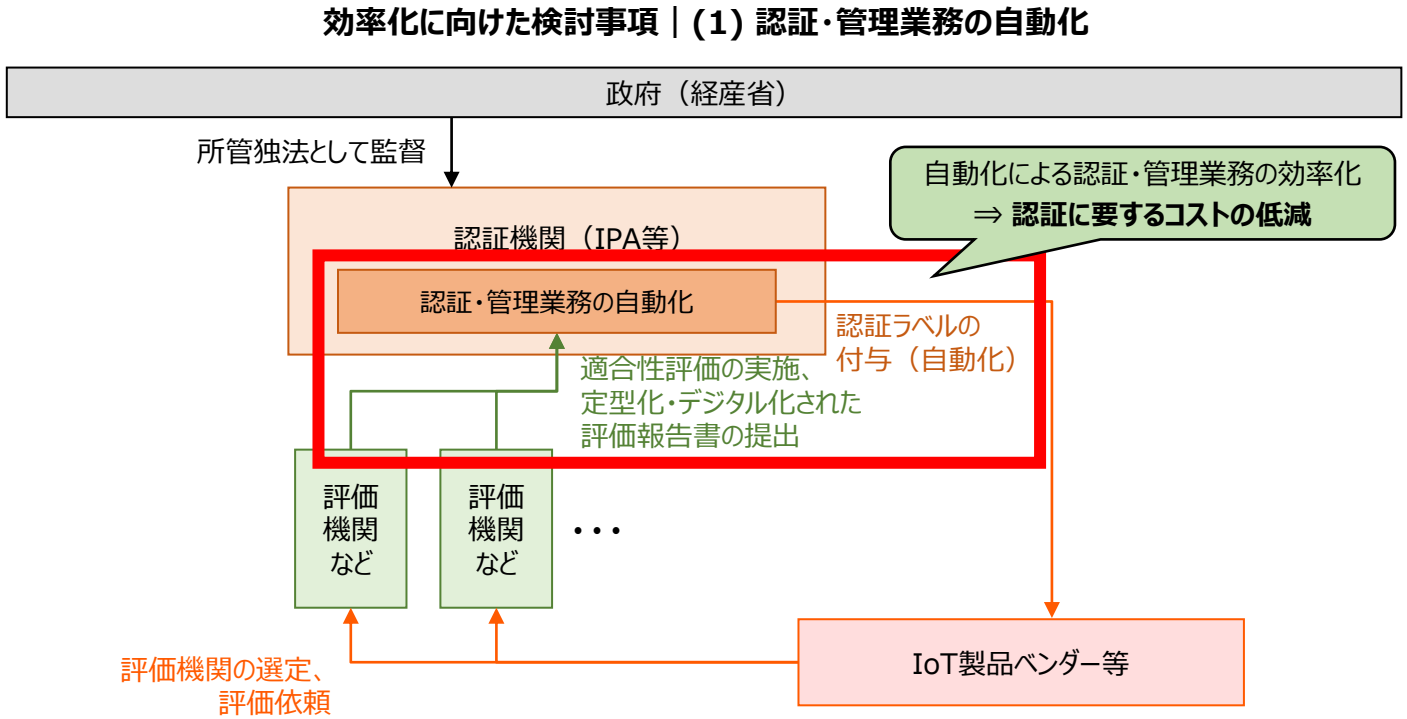
☆２以上製品の制度設計の優先順位

- ☆２以上の製品は、製品ごとに適合基準等を設定することから、優先順位を付けることが重要。
- 優先順位の考え方としては、例えば、①米欧を中心とした国々と我が国との輸出入量、②海外との相互承認において優先度の高い製品、③高い「対策水準」「評価水準」が求められる製品、④現状サイバー攻撃を受けており社会への影響がある製品等、いくつかの要素が考えられる。これらの要素を勘案し、優先度の高いものから制度を構築していくことが適当と考えられる。
- また、これらの製品について、☆２・３のいかなるレベルまで定めるかや、第三者認証／自己認証とするかについては、諸外国の制度設計の状況を踏まえつつ、各製品・レベルの適合基準策定WGにおける専門的な議論により策定されていくことが適当と考えられる。

※☆２☆３以上の機器については、おおむね業界団体を中心とした検討がなされることが想定されるが、安全保障の観点で特に重要な機器等がある場合など、機器によっては国が議論への関与を強めるべき場合もあると考えられる。いずれにせよ、機器ごとに柔軟に検討を行っていくことが必要。

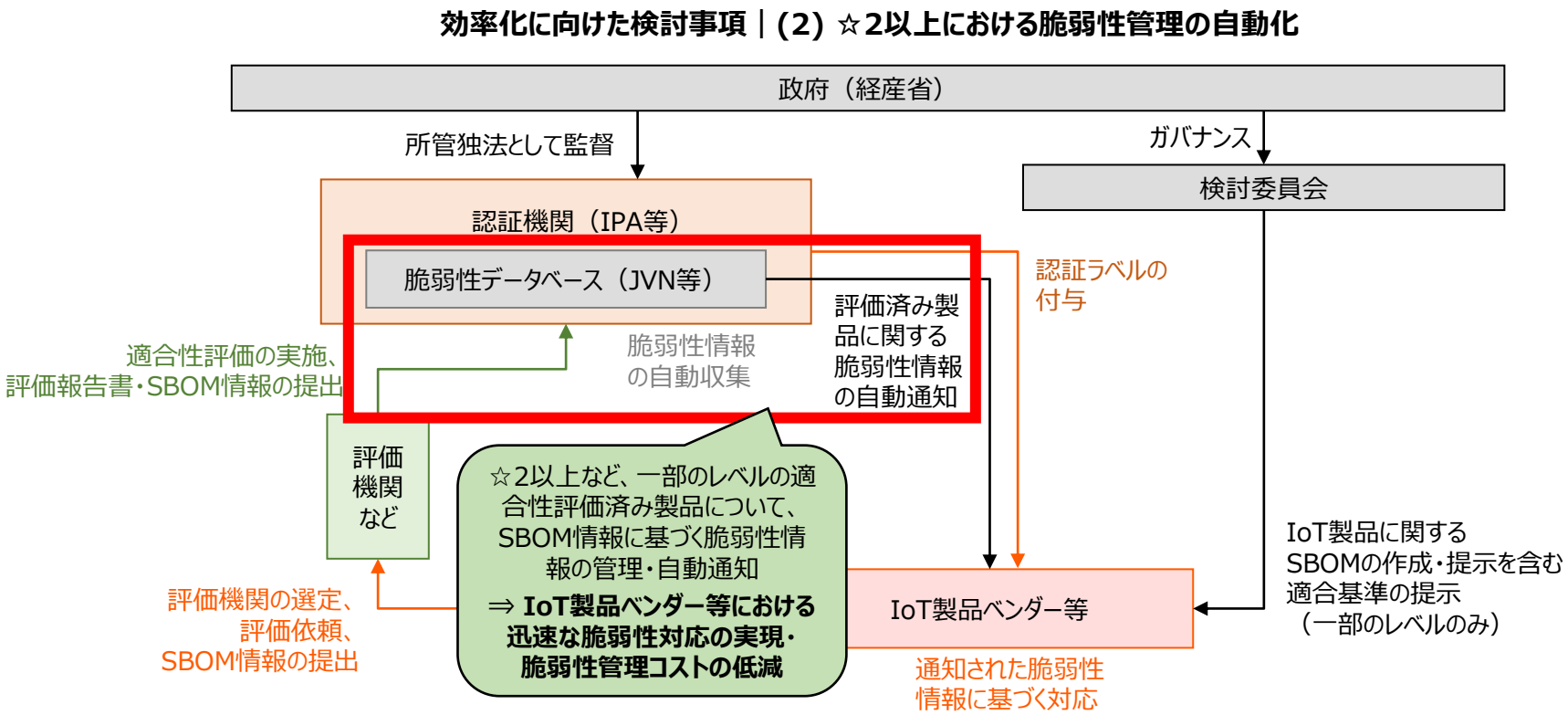
効率化に向けた検討事項｜(1) 認証・管理業務の自動化

- 認証や管理にかかる業務については、可能な限り効率化されることが望ましい。効率化により、認証に要するコストの低減が実現でき、最終的にはIoT製品ベンダー等の負担減、コスト減に繋がる。



効率化に向けた検討事項｜(2) ☆2以上における脆弱性管理の自動化

- 将来的に、評価済み製品に関する脆弱性の自動管理を行うことで、適合性評価済み製品におけるセキュリティリスクを低減することが望まれる。
- このために、☆2以上など、一部のレベルの適合事項としてSBOMの作成・提示をIoT製品ベンダー等に求め、認証機関においては、当該SBOM情報に基づき、評価済み製品に関する脆弱性情報が明らかになった場合にベンダーに自動通知する対応が想定される。
- この対応により、IoT製品ベンダー等における迅速な脆弱性対応の実現や、脆弱性管理コストの低減といったメリットが得られる。



今年度の進め方

本日

本検討会（数回開催）

＜議論事項の例＞
- 評価スキームの具体化
- セキュリティ事案に対する検討
  （責任分界、保険の措置、脆弱性に対する対応等）
- 調達者、消費者における活用促進策
- IoT製品ベンダー等、評価機関等に対する支援策
- 国際連携方針
- ☆２以上製品の制度設計の優先順位

実証（プレ委員会＋評価検証）

＜実施事項＞
- プレ委員会設置
- 要求基準案、適合基準案、評価手順案の策定
- 評価作業、工数の計測
- 結果とりまとめ、コストの洗い出し
- 要求基準案、適合基準案、評価手順案の修正

本検討会の取りまとめ

2023年
12月末頃

【参考】構築すべき適合性評価制度（中間とりまとめ1.2節）

カテゴリ	構築すべき適合性評価制度（抜粋）	今後議論が必要な事項（抜粋）
1.2.1. 制度の位置づけ	• 検討会での議論を踏まえると、適合性評価制度は**まずは任意制度として運用することが適当**である。	• 任意制度として運用を開始しつつも、制度の浸透・活用の程度、国内IoT製品ベンダーによる対応状況、IoT製品に対する脅威の状況、諸外国の取組との整合性や国際的な動向等によっては、任意制度で措置されていた製品類型に対し、法令に基づく義務化に向けた検討を新たに行うことも必要になり得ると考えられる。 • 適切なルール設計は産業活動や社会の活力向上にも繋がるものであるため、こうした点も義務化に向けた検討を新たに行う場合に踏まえるべき重要な観点である。
1.2.2. 制度の対象となる製品範囲	• 適合性評価制度の**対象製品範囲は「間接的又は直接的にインターネットに接続する製品」とすることが適当**である。	• いかなる製品を対象にするかについては、各製品が有するリスクや、事業への影響、普及効果、既存制度等を考慮し、精緻に検討を行っていく必要がある。
1.2.3. 制度で用いる適合性評価基準	• 適合性評価制度で用いる適合性評価基準については、**国際的な標準を参照の上、国際的な標準と整合的な形で構築していくことが適当**である。	• 具体的な適合性評価基準の策定に当たっては、どのような体制で検討を行っていくか、いくつかのリスクレベルが想定されるところどの程度の基準を策定するべきか、いかなる製品類型に対しどのような考え方で基準を適用していくか、等の考え方について、国内外の関連する動向を踏まえつつ、詳細に検討を行っていく必要がある。
1.2.4. 制度で活用する適合性評価スキーム	• 適合性評価制度の運用に当たっては、**既存の評価スキームを活用した制度とすることが適当**である。	• 具体的に、どの製品類型に対して、どのスキームを活用するかについては、各製品が有するリスクや、事業への影響、普及効果、既存制度等を考慮し、精緻に検討を行っていく必要がある。 • 検討に当たっては、諸外国の制度との連携や、現行制度との整合性、運用能力等について、既存の評価スキームを所掌している機関と丁寧に検討を進めていくことが重要と考えられる。

【参考】今後議論が必要な事項（中間とりまとめ2章）

カテゴリ	論点	今後議論が必要な事項（抜粋）
2.1. 政府の関与や検討体制のあり方	2.1.1. 認証機関との連携	• 複数の既存スキームを活用する場合、適合性評価を行う認証機関が複数となり得ることや、認証取得数の増加に向けては認証機関の適格性が重要となることから、各主体の適格性について、政府のガバナンスが効く構造を構築することが重要となる。
	2.1.2. 評価基準等を検討する委員会の構築	• 各分野の専門家を招聘し、評価基準等を検討する委員会を設置することが適当と考えられることから、あるべき具体的な体制や方針について、詳細に検討を行っていく必要がある。
	2.1.3. 政府基本方針の策定	• 認証機関の適格性を向上させる観点や、基準等を検討する委員会のガバナンスの観点、複数になり得る認証機関の方向性を束ねる観点、企業の社会貢献の観点等から、政府は基本方針のような形で大きな方向性を示していく必要がある。
2.2. IoT製品ベンダーの能動的な制度活用を促す仕掛け	2.2.1. 各種調達要件との連携、消費者に対する需要喚起策	• ベンダーの能動的な制度活用を促す仕掛けとして、各種調達要件との連携や消費者に対する需要喚起策が想定される。今後、各種調達要件と連携について、その効果や、いかなる調達要件とどのように連携すべきか等について、その根拠付けと共に検討する必要がある。 • また、消費者に対する需要喚起策についても、適合性評価制度がどう安全・安心に繋がるのか、適合性の評価がなされていない製品とはどのような差があるのか、等の観点も踏まえ、その効果、他の取組との連携可能性、具体的な喚起方法等について、検討する必要がある。
	2.2.2. 諸外国の適合性評価制度との国際連携	• 諸外国ではIoT製品の適合性評価制度の検討が進んでおり、この認証取得のために日本企業の負担が増えることが想定されるところ、適合性評価制度と諸外国の制度の連携を図ることで、負担幅を抑えることが重要と考えられる。 • 今後、諸外国制度の動向を踏まえつつ、どの諸外国制度と、どのような国際相互承認方式で連携し、基準について具体的にどのように整合的に連携するか等について、検討する必要がある。
	2.2.3. IoT製品ベンダーや認証機関等に対する支援策	• どのような製品類型に対し、いかなる基準を適用することで、関係者にどの程度のコストが発生するかについて実証等を通じて検証する必要がある。 • その上で、制度普及を後押しする観点から、関係者において発生するコストを抑制するため支援策について、必要に応じて検討する必要がある。
2.3. 適合性評価済製品におけるセキュリティ事案への対応	2.3.1. 法的な論点整理	• 適合性評価を受けた製品に脆弱性が見つかり、セキュリティ事案につながるおそれがあることから、適合性評価を受けることでどのような責任分界につながるか、事案発生時にどのような関係者がどのような責任を負う必要があるか、どのような備えをしておくべきか、等について検討する必要がある。
	2.3.2. リスクに対応するための資源の確保策	• 事案発生時の法的な責任分担の整理に加え、例えば保険制度のような、事案発生時に対処を適切に行い、被害救済や原因是正に繋がる資源の確保策についても、どのような策が効果的か等について、必要に応じて検討する必要がある。
	2.3.3. 評価済製品のサーベイランス、取り消し	• サーベイランスについて、IoT製品のライフサイクルによっては、必ずしもそぐわない場合もあると想定される。現行制度の状況や、どのような製品類型を対象とするか、どのような者が運用するか、どのような仕組みとするか、適合性評価結果の有効期限についてどう考えるか、どの程度コストが発生するか、等の想定される基本的な事項について、必要性も含めて検討をする必要がある。