経済産業省

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

2023年 3月 17日

【参考】適合性評価制度の背景となる課題

第2回検討会資料より

- IoT製品の安全性確保に向けては、以下に示すとおり、IoT製品ベンダーにおける課題、IoT製品利用者・調達者における課題及び国民全体の課題が存在すると考えられることを提示した。

【IoT製品ベンダーにおける課題】

- IoT製品に対するセキュリティ対策状況が適切に評価されず、製品価値の向上につながらないおそれがある。
- 既存制度の認証取得による明確なインセンティブが存在せず、認証を取得してもコスト増のみで、製品売上につながらないおそれがある。
- 諸外国の制度と協調的な制度が構築されない場合、諸外国の制度の適合性評価を受ける際に別途の負担が必要となる。

IoT製品利用者・調達者における課題

- 現状ではセキュリティ対策状況が可視化されていないため、適切な対策が施されたIoT製品を選ぶことができないおそれがある。
- 適切な対策が施されたIoT製品を利用できない場合、当該IoT製品がサイバー攻撃を受け、利用者に対して悪影響を及ぼすおそれがある。

【国民全体の課題】

- マルウェア攻撃によりIoT製品がボット化して他のシステムに悪影響を及ぼすリスク、不正アクセスにより利用者のプライバシー侵害に関するリスク、サイバー攻撃により人体への物理的影響を及ぼすリスク等、IoT製品を狙ったサイバー脅威が高まっている。
- 諸外国はIoT製品に対するセキュリティ対策の取組を進めているところ、十分な取組を実施しない場合、我が国のIoT製品が集中的に狙われ、国内のシステムや国民の生活に悪影響を及ぼすおそれがある。

１．前回の検討会のご指摘事項

２．政府の関与や検討体制のあり方

３．適合性評価制度で対象とする製品範囲

４．適合性評価制度で活用する適合性評価スキーム

５．諸外国の適合性評価制度との国際連携

前回の検討会のご指摘事項

カテゴリ		主なご指摘事項
政府の関与や検討体制のあり方について		• 基準の作り方を検討すべきである。小規模な検討グループを作り、関連基準の重複等を調査し、本制度で採用する部分を整理すると良いのではないか。 • セキュリティの確保された社会を構築するという、社会に対する貢献も重要であるため、視点に入れていただきたい。
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」として、技適の対象より広げる方向性は良い。 • 製品によって使われる環境が異なり、リスクも変わる点について議論する必要がある。 • 「間接的又は直接的にインターネットに接続する製品」という表現は、技術的な観点では曖昧なので、より範囲が明確になるように議論したい。 • 特に産業系の機器ではシステムとしてセキュリティを守る観点で作られたガイドラインに沿って対応している現状を踏まえて議論を進めていきたい。 • 製品単位で評価する方針で良いのか、構成部品やプログラムまで評価すべきかについて検討した方が良い。
制度で用いる適合性評価基準について		• ETSI EN 303 645はセキュリティ要件として過度に厳密ではないため、基準として適している。 • 欧州や米国による国際標準を軸とすることは賛成だが、それらの基準の要素をどれだけ取り入れたかについては明確にしながら検討を進めていただきたい。 • 任意制度を前提とするのであれば、評価基準を細分化せず、一つの基準で広い範囲をカバーできた方がメーカーとしてはありがたい。 • 国際競争力を考え、国際標準に合わせる点と、日本が優位性を取れる点も含めて、検討していく必要がある。
制度で用いる適合性評価スキームについて		• 評価や認証にかかる費用及び期間を算出する必要がある。認証要件や評価品質を均一化するための方法論によっても、取得期間やコストは変わる。 • IoT製品は製品寿命が長くないため、サーベイランスの視点から更新制度を設けるかについては検討が必要である。 • Sマークの知名度を活用するメリットは理解するが、既存のマークと新しいマークは違う意味を持つことをはっきりさせた方が良い。
その他	制度の目的	• 誰に対してどのようなメリットを与えるために本制度を立ち上げるか、前提条件を関係者で共有する必要がある。 • 認証を取ることでどのようなメリットがあるかについて、投資対効果として考え、市場原理を考慮して制度設計を行う必要がある。
	プロモーション	• 多少高価でもセキュリティを講じるIoT製品が積極的に購入されるような社会の仕組みの構築や制度のプロモーションに向けた具体的な検討をお願いしたい。
	インセンティブ	• 調達要件として市場を守るといった取組を行えれば、足並みを揃えて本制度を普及させることができるのではないか。 • セキュリティを自ら守る必要があるとメーカーに認識いただかなければ、本制度は普及しないのではないか。 • メーカーや販売側に対して適切なインセンティブを設けることと、購入する側が安心できる製品を適切に選択できることの両立が、重要だと認識している。 • 海外メーカーが日本での販売に躊躇しないようにしていただきたい。国際的に商品展開をするベンダーの競争力を削がないようにすることが重要である。
	事案への対応	• 消費者のセキュリティに関する利益を守る人はたくさんおり、損害が生じた場合に補填を行う保険制度も社会的な仕組みとして確立している。 • 事故により消費者から訴えられた場合、ステークホルダーが複数存在する可能性があるため、広く考慮や目配りが必要である。

１．前回の検討会のご指摘事項

２．政府の関与や検討体制のあり方

３．適合性評価制度で対象とする製品範囲

４．適合性評価制度で活用する適合性評価スキーム

５．諸外国の適合性評価制度との国際連携

政府の関与や検討体制のあり方①

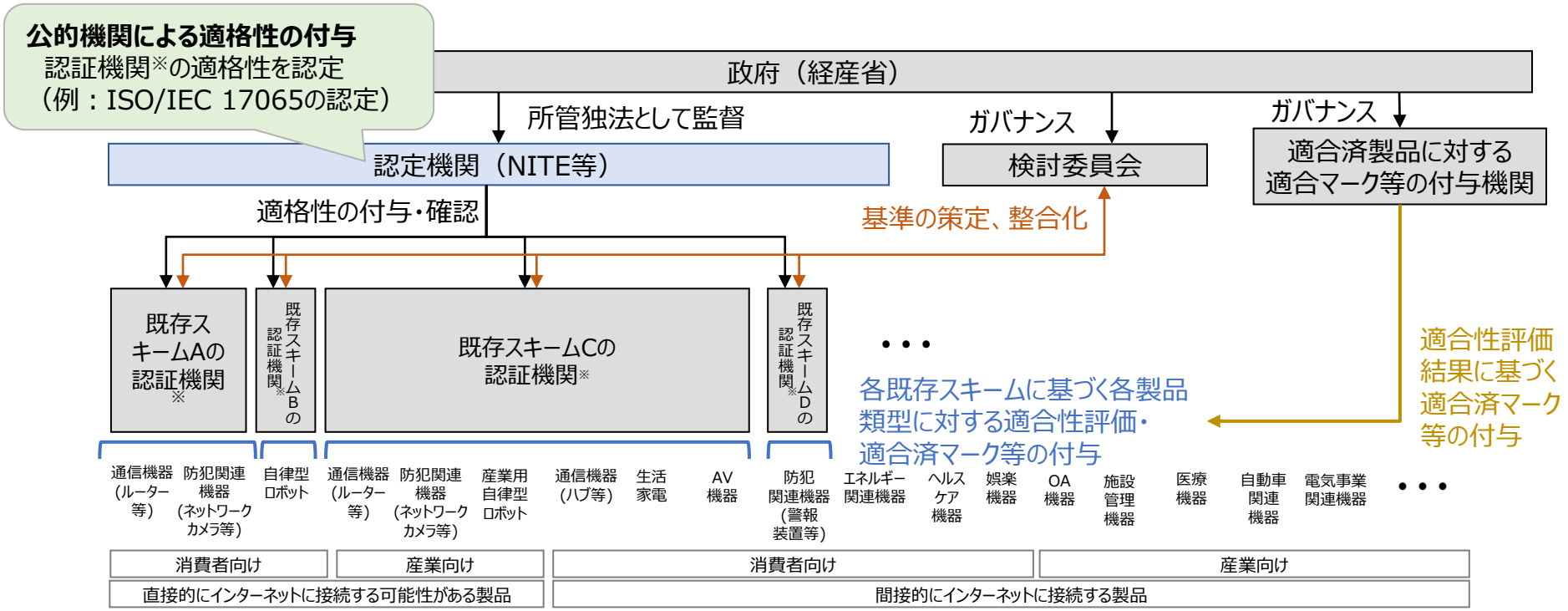
認証機関との連携

中間とりまとめ案の記載事項	• 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。

【討議事項1-①】

- 経産省の独法（例えば、NITE）を認定機関とし、この認定機関がIECに基づき認証機関としての適格性を認定する構造とすれば、経産省は独法の監督を行っていることから、経産省－認定機関－認証機関が一気通貫で関係することになり、結果、政府のガバナンスのもとで各認証機関の適格性が維持される構造を構築できるのではないか。

✓ 上記の仮説は妥当か。留意事項や懸念点はあるか。



※1 認証スキームを運用する第三者適合性評価機関を意味する（ISO/IEC 17065）。なお、製品に対する試験を行う場合には、ISO/IEC 17025等に基づく試験機関の適格性の認定も必要となる。

【参考】独立行政法人製品評価技術基盤機構（NITE）の認定制度概要

- NITEにおける適合性認定分野における業務として、①法律等に基づく認定業務、②認証機関の登録のための調査等関係業務が存在。
- ①法律等に基づく認定業務として、計量法に基づくJCSS及びMLAP、JIS法に基づくJNLAのほか、**これら3つの認定制度で対応できない部分を対象にNITE独自に認定する製品評価技術基盤機構認定制度（ASNITE）**が存在（計４類型）。
- ASNITEの認定の要件は、試験所に関する基準（＝ISO/IEC 17025）、標準物質生産者に関する基準（＝ISO 17034）、製品認証機関に関する基準（＝ISO/IEC 17065）及び各制度ごとに固有の認証スキーム（規則及び手順）に適合していることである。現在、認定対象別に、ASNITE-C、T、R、Pの4つのプログラムを開発・運営中である。

NITE認定センターにおける認定事業

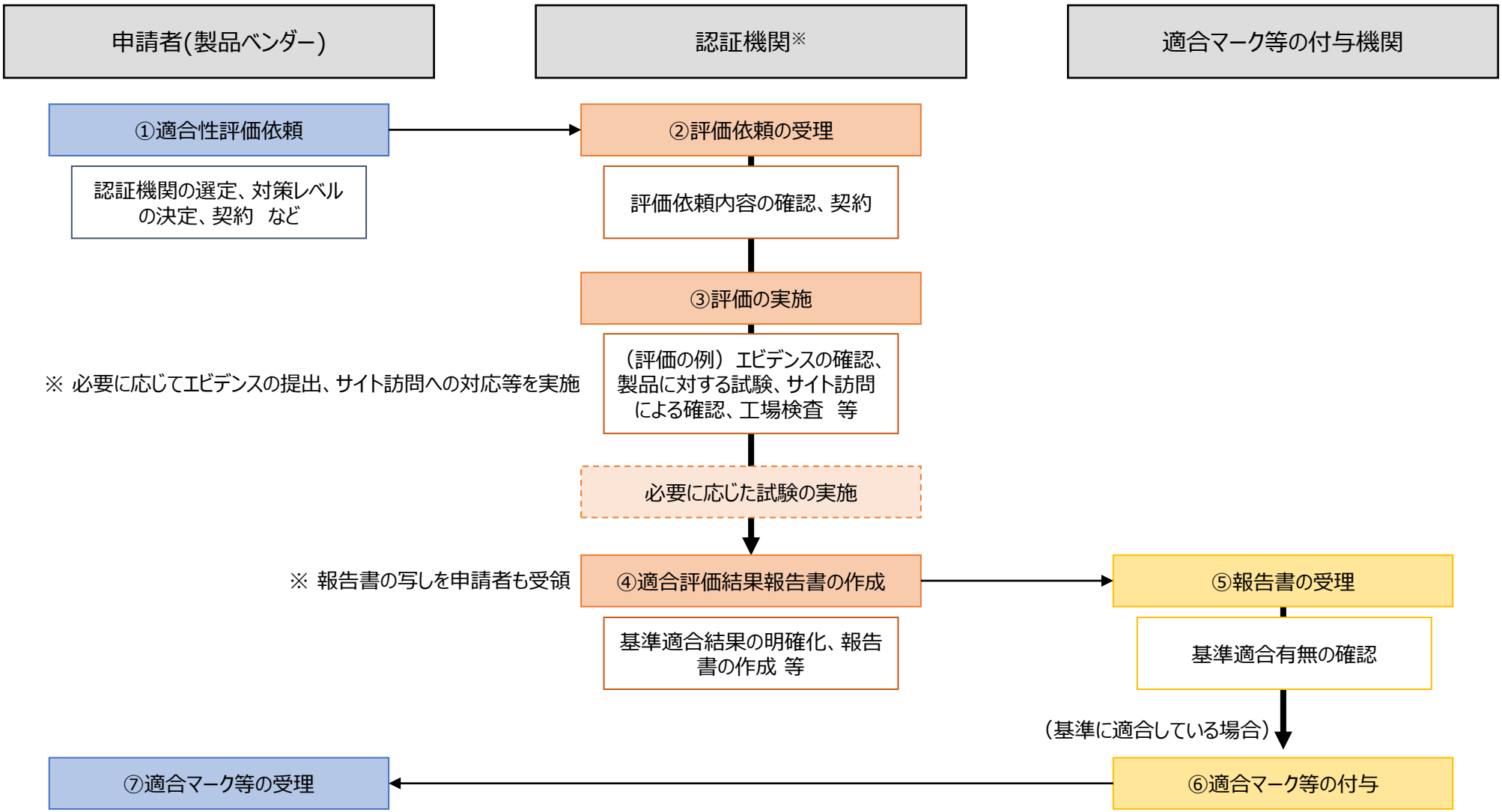
ASNITEプログラムの概要

プログラム	認定対象の適合性評価機関	認定基準	適合性評価活動の例	ベネフィット
ASNITE-C（Calibration Laboratories）	校正事業者 ※試験に用いる試験器が正確な値になるよう調整し校正証明書を発行	ISO/IEC 17025	電動自動車の接近通報音の試験器を国際規格にしたがって校正。自動車メーカー所有の試験器によるデータの信頼性確保	メーカーが海外に輸出する場合の、相手国における円滑な受け入れ
ASNITE-T（Testing Laboratories）	試験事業者 ※試験規格にもとづいた製品試験を実施し試験証明書を発行	ISO/IEC 17025	JIS以外の国際規格等に定められた抗ウイルス性試験を実施することによりプラスチック製品、液剤等の取引の信頼性確保	生活に身近な抗ウイルス関連製品に対する、市場や消費者に安全な製品の提供
ASNITE-R（Reference Material Producers）	標準物質生産者 ※測定の基準となる標準物質を生産	ISO 17034	産総研等の標準物質生産者の信頼性確保	標準物質の供給体制整備
ASNITE-P（Product Certification Bodies）	試験認証機関 ※基準にあった信頼できる製品であることを認証	ISO/IEC 17065	エシカルなアパレル製品を対象としたTextile Exchange 認証。国内メーカーが、日本で認証を受けることにより、国際的なアパレル企業の調達基準をクリアすることが可能となる	国際的な企業の調達基準となっている海外認証を、国内で取得することによる負担軽減

出所）https://www.nite.go.jp/data/000096939.pdf, https://www.nite.go.jp/iajapan/asnite/outline/index.html

【参考】想定される適合性評価・マーク等付与のプロセス（イメージ）

（認証機関による評価の場合）



※ 認証スキームを運用する第三者適合性評価機関を意味する（ISO/IEC 17065）。なお、製品に対する試験を行う場合には、ISO/IEC 17025等に基づく試験機関の適格性の認定も必要となる。

政府の関与や検討体制のあり方②

認定基準等を検討する委員会の構築

第２回のご指摘事項	• 基準の作り方を検討すべきである。小規模な検討グループを作り、関連基準の重複等を調査し、本制度で採用する部分を整理すると良いのではないか。
中間とりまとめ案の記載事項	• 具体的な適合性評価基準の策定に当たっては、IoT製品やリスク、海外制度等について専門的な知見が必要となることから、それぞれの関係者に利益がもたらされる形で本制度の目的を達成するためには、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、具体的な方針について、詳細に検討を行っていく必要がある。

【討議事項1-②】

どのような基準とすべきか、どの製品にどのレベルの基準を当てはめるべきか、といった点については、専門的な知見を要することから、専門家からなる検討委員会を構築し、政府の方針の下に当該事項を検討することが適当であると考えられる。

✓ 検討委員会の位置づけ、体制、構成員はどのようなものが望ましいか。

＜構成員のイメージ＞

・IoTセキュリティに関する有識者、関連する制度・適合性評価スキームの運用主体　等

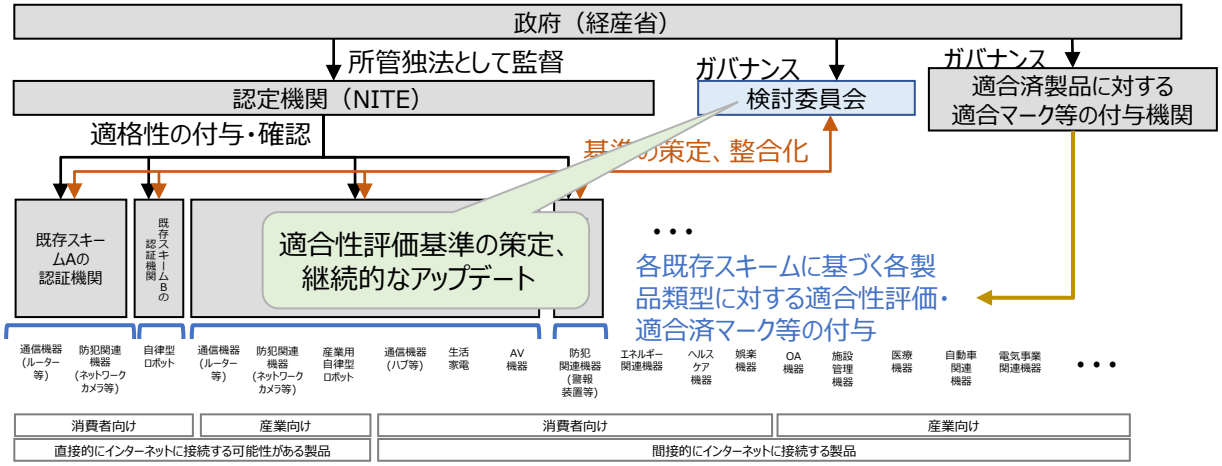
✓ 検討委員会はどのような事項を検討する場とすべきか。

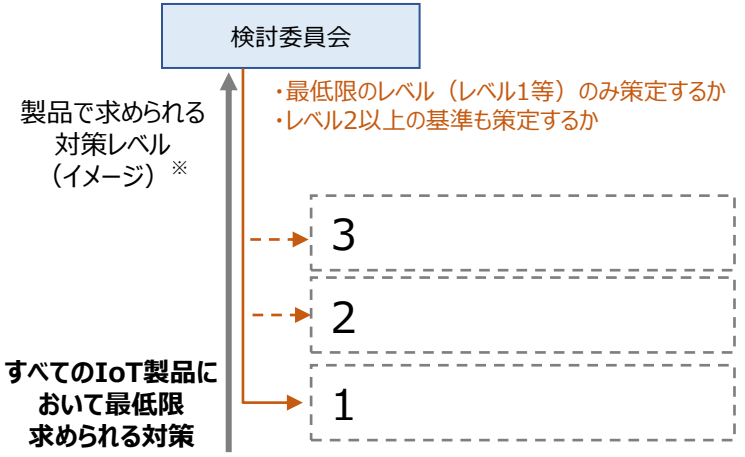
✓ 特に基準については、最低限のレベル（レベル1等）のみ議論するか、それ以上のレベルも議論すべきか。

＜検討事項のイメージ＞

・リスクレベルごとに適した適合性評価基準の検討

・いかなる既存制度をどの製品に当てはめるかの検討





※ レベルを3段階に分けることは一例であることに留意。

政府の関与や検討体制のあり方③

政府基本方針の策定

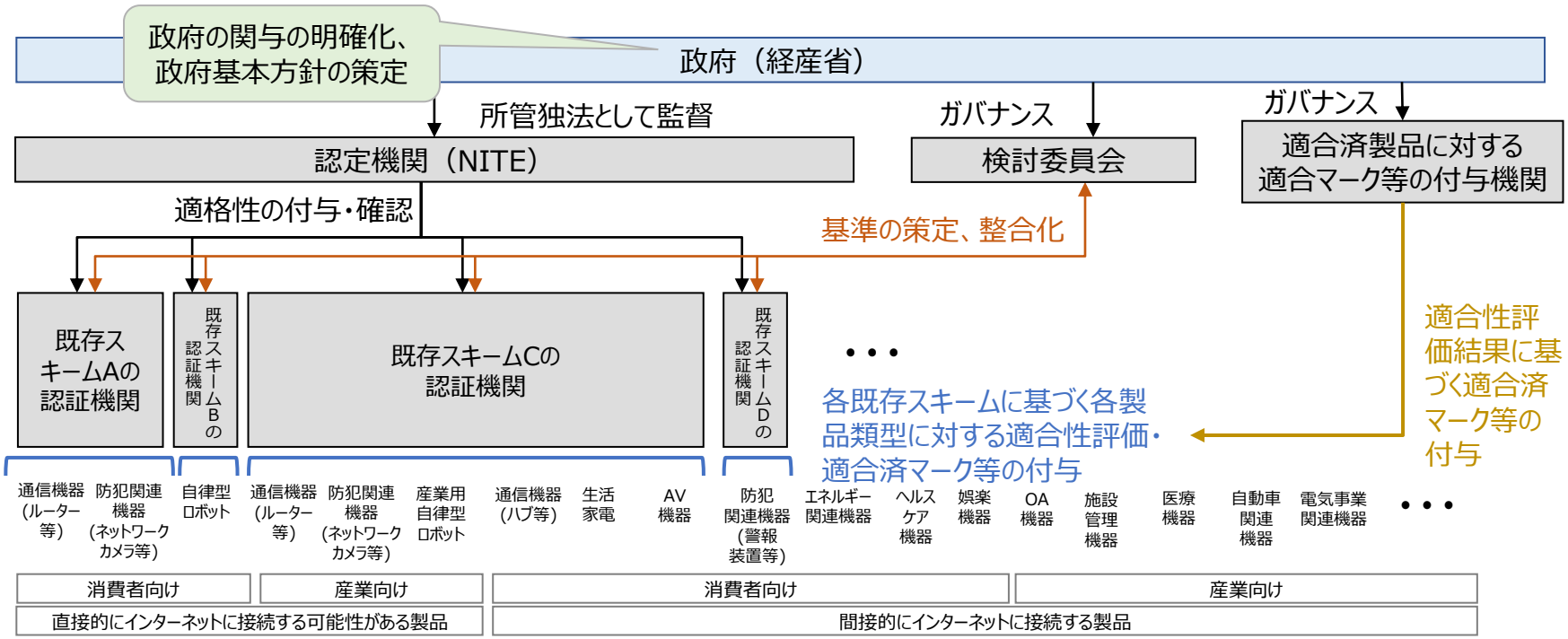
第２回のご指摘事項	• 基準の作り方を検討すべきである。小規模な検討グループを作り、関連基準の重複等を調査し、本制度で採用する部分を整理すると良いのではないか。 • セキュリティの確保された社会を構築するという、社会に対する貢献も重要であるため、視点に入れていただきたい。
中間とりまとめ案の記載事項	• 認証機関の適格性を向上させる観点や、基準等を検討する委員会のガバナンスの観点、複数になり得る認証機関の方向性を束ねる観点、企業の社会貢献の観点から、政府は基本方針のような形で大きな方向性を示していく必要がある。

【討議事項1-③】

✓ 政府が基本方針を示すにあたって、含めるべき内容や考慮すべき点はあるか。

＜基本方針記載事項の例＞

「背景、目的」「IoT機器のセキュリティ確保に向けた基本的な考え方」「対象とする製品類型」「評価基準」「認証スキーム」「普及啓発活動」



１．前回の検討会のご指摘事項

２．政府の関与や検討体制のあり方

３．適合性評価制度で対象とする製品範囲

４．適合性評価制度で活用する適合性評価スキーム

５．諸外国の適合性評価制度との国際連携

適合性評価制度で対象とする製品範囲①

第２回のご指摘事項	• 「間接的又は直接的にインターネットに接続する製品」として、技適の対象より広げる方向性は良い。 • 製品によって使われる環境が異なり、リスクも変わる点について議論する必要がある。 • 「間接的又は直接的にインターネットに接続する製品」という表現は、技術的な観点では曖昧なので、より範囲が明確になるように議論したい。 • 特に産業系の機器ではシステムとしてセキュリティを守る観点で作られたガイドラインに沿って対応している現状を踏まえて議論を進めていきたい。 • 製品単位で評価する方針で良いのか、構成部品やプログラムまで評価すべきかについて検討した方が良い。
中間とりまとめ案の記載事項	• 適合性評価制度で対象とする製品の範囲については、広範な製品類型が存在するIoT機器の大部分を対象とし得る制度とするため「間接的又は直接的にインターネットに接続する製品」とするべきである。 • その上で、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。

【討議事項2-①】

「直接的にインターネットに接続する可能性がある製品」に対しては、総務省の端末設備等規則によるセキュリティ対策が求められている。その上で、義務的な対策を超えてセキュリティ対策を行う事業者の取組を製品価値に繋げる仕組みを構築することが、能動的なセキュリティ対策を促すために効果的であると考えられる。

✓ 「直接的にインターネットに接続する可能性がある製品」は、本制度の対象とすることが適当ではないか。

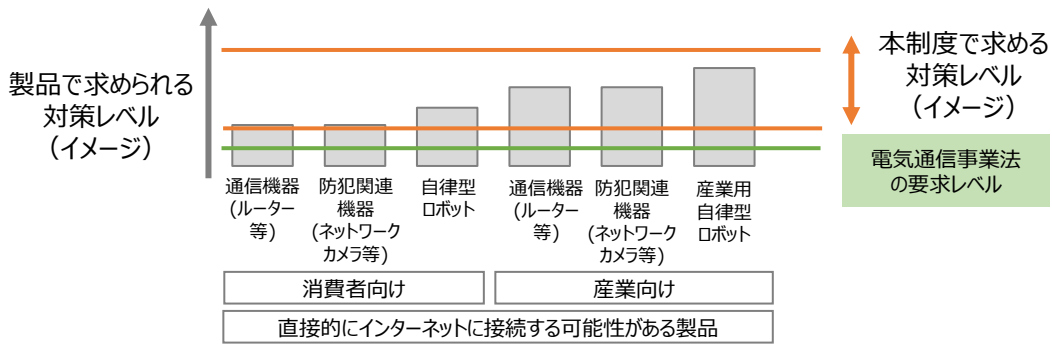
✓ 具体的にいかなる製品を対象とすべきかについて、どのような考え方で検討していくべきか。

✓ どの程度のレベルの基準を当てはめるかについては、特に製品が有するリスクを考慮することが重要と考えられるが、どの様なリスクを考慮すべきか。また、どのような考え方（IoT-SSF、62443等）を参照してリスク評価を行うべきか。

「直接的にインターネットに接続する可能性がある製品」における既存の適合性評価スキームの適用イメージ

（例1）防犯関連機器	• 防犯関連機器は、防犯機器の安全マークとして既に普及しているとの理由により、RBSSを活用することが適当であると考えられる。
（例2）通信機器	• 通信機器は、既に直接的にインターネットに接続する可能性がある製品を全て対象としていること、基準がETSI EN 303 645やNISTIR 8425といった国際的な規格を踏まえて策定しているとの理由により、CCDSサーティフィケーションプログラムを活用することが適当であると考えられる。

代表的な製品において求められる対策レベルのイメージ



適合性評価制度で対象とする製品範囲②

第２回のご指摘事項	• 「間接的又は直接的にインターネットに接続する製品」として、技適の対象より広げる方向性は良い。 • 製品によって使われる環境が異なり、リスクも変わる点について議論する必要がある。 • 「間接的又は直接的にインターネットに接続する製品」という表現は、技術的な観点では曖昧なので、より範囲が明確になるように議論したい。 • 特に産業系の機器ではシステムとしてセキュリティを守る観点で作られたガイドラインに沿って対応している現状を踏まえて議論を進めていきたい。 • 製品単位で評価する方針で良いのか、構成部品やプログラムまで評価すべきかについて検討した方が良い。
中間とりまとめ案の記載事項	• 適合性評価制度で対象とする製品の範囲については、広範な製品類型が存在するIoT機器の大部分を対象とし得る制度とするため「間接的又は直接的にインターネットに接続する製品」とするべきである。 • その上で、製品ごとのリスクや、既存の制度（技適、ガイドライン等）との関係等を考慮し、適合性評価制度の対象とすべきかの峻別を精緻に行っていくべきである。

【討議事項2-②】

- ✓ 「間接的にインターネットに接続する製品」のうち、消費者向けの製品については、義務的な規制がかかっておらず、かつセキュリティ対策要件を定めたガイドライン等に乏しいことから、本制度の対象とすることが適当ではないか。
- ✓ 具体的にいかなる製品を対象とすべきかについて、どのような考え方で検討していくべきか。
- ✓ どの程度のレベルの基準を当てはめるかについては、特に製品が有するリスクを考慮することが重要と考えられるが、どの様なリスクを考慮すべきか。また、どのような考え方（IoT-SSF、62443等）を参照してリスク評価を行うべきか。

「間接的にインターネットに接続する可能性がある製品」（消費者向け製品）における既存の適合性評価スキームの適用イメージ

（例1） 生活家電	• 生活家電は、現状、Sマークによる認証が行われている製品であり、Sマークは店頭普及率が高く認知されていること、国際的な認証スキームが活用可能であるといったメリットがあるため、Sマークを活用することが適当であると考えられる。 • なお、Sマークは、制度趣旨を踏まえると自己適合宣言を制度に含めることが困難、既存の認証機関においてセキュリティの評価が可能な認証機関が限定的であるといった課題があることから、電気製品認証協議会（SCEA）、認証機関（JQA、JET）といった機関と丁寧に検討を進めていくことが必要と考えられる。
（例2） 防犯関連機器	• 防犯関連機器は、防犯機器の安全マークとして既に普及しているとの理由により、RBSSを活用する方向を検討することが適当であると考えられる。 • なお、セキュリティの基準をどのように取り込むか、第三者評価をどのようなスキームで行うか、評価機関におけるセキュリティに関する評価能力の確保が課題となることから、公益社団法人日本防犯設備協会、主要ベンダー等と検討を進めていくことが必要と考えられる。
（例3） ヘルスケア機器	• ヘルスケア機器においては、業界団体等による認証制度が存在せず、間接的にインターネットに接続する製品を広く対象とできることから、CCDSを活用する方向を検討することが適当であると考えられる。 • ただし、現在の自主評価の扱いや国際的な認証スキームとの整合性が課題となることから、CCDS、主要ベンダー等と検討を進めていくことが必要と考えられる。

適合性評価制度で対象とする製品範囲③

第２回のご指摘事項	• 「間接的又は直接的にインターネットに接続する製品」として、技適の対象より広げる方向性は良い。 • 製品によって使われる環境が異なり、リスクも変わる点について議論する必要がある。 • 「間接的又は直接的にインターネットに接続する製品」という表現は、技術的な観点では曖昧なので、より範囲が明確になるように議論したい。 • 特に産業系の機器ではシステムとしてセキュリティを守る観点で作られたガイドラインに沿って対応している現状を踏まえて議論を進めていきたい。 • 製品単位で評価する方針で良いのか、構成部品やプログラムまで評価すべきかについて検討した方が良い。
中間とりまとめ案の記載事項	• 適合性評価制度で対象とする製品の範囲については、広範な製品類型が存在するIoT機器の大部分を対象とし得る制度とするため「間接的又は直接的にインターネットに接続する製品」とするべきである。 • その上で、製品ごとのリスクや、既存の制度（技適、ガイドライン等）との関係等を考慮し、適合性評価制度の対象とすべきかの峻別を精緻に行っていくべきである。

【討議事項2-③】

「間接的にインターネットに接続する製品」のうち、産業向けの製品については、国民経済への影響等を鑑みれば、CC認証等、高い要求基準を課す認証制度の普及を図っていくべきと考えられるが、様々な課題により普及率は低い現状にある。

- ✓ このような現状を鑑み、CC認証、CSA認証等の普及を促進していく必要は依然としてあるものの、広くセキュリティレベルの向上を図るために、「間接的にインターネットに接続する製品」のうち、産業向けの製品について、本制度の対象とすることが適当ではないか。
- ✓ 具体的にいかなる製品を対象とすべきかについて、どのような考え方で検討していくべきか。

※例：産業システム全体としてのセキュリティ対策を求めたガイドラインが存在する分野については、既存制度を適用する優先順位は低い、等。

※既存制度を適用した場合には、ガイドラインにおいて、マーク取得を推奨するなど、連携することが効果的と考えられる。

- ✓ どの程度のレベルの基準を当てはめるかについては、特に製品が有するリスクを考慮することが重要と考えられるが、どの様なリスクを考慮すべきか。また、どのような考え方（IoT-SSF、62443等）を参照してリスク評価を行うべきか。
- ✓ 特に産業用については、システム全体のガイドラインも多く存在するところ、機器に既存制度を適用した場合、こうしたガイドラインとどう連携

「間接的にインターネットに接続する可能性がある製品」（産業向け製品）における既存の適合性評価スキーム

（例1） 医療機器	• 厚生労働省「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」による医療機器の薬事承認
（例2） スマートメーター	• 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」が、技術基準及び保安規程に位置付け（電気事業法の省令に根拠規定）

１．前回の検討会のご指摘事項

２．政府の関与や検討体制のあり方

３．適合性評価制度で対象とする製品範囲

４．適合性評価制度で活用する適合性評価スキーム

５．諸外国の適合性評価制度との国際連携

適合性評価制度で活用する適合性評価スキーム①

第２回のご指摘事項	• 任意制度を前提とするのであれば、評価基準を細分化せず、一つの基準で広い範囲をカバーできた方がメーカーとしてはありがたい。

【討議事項3-②】

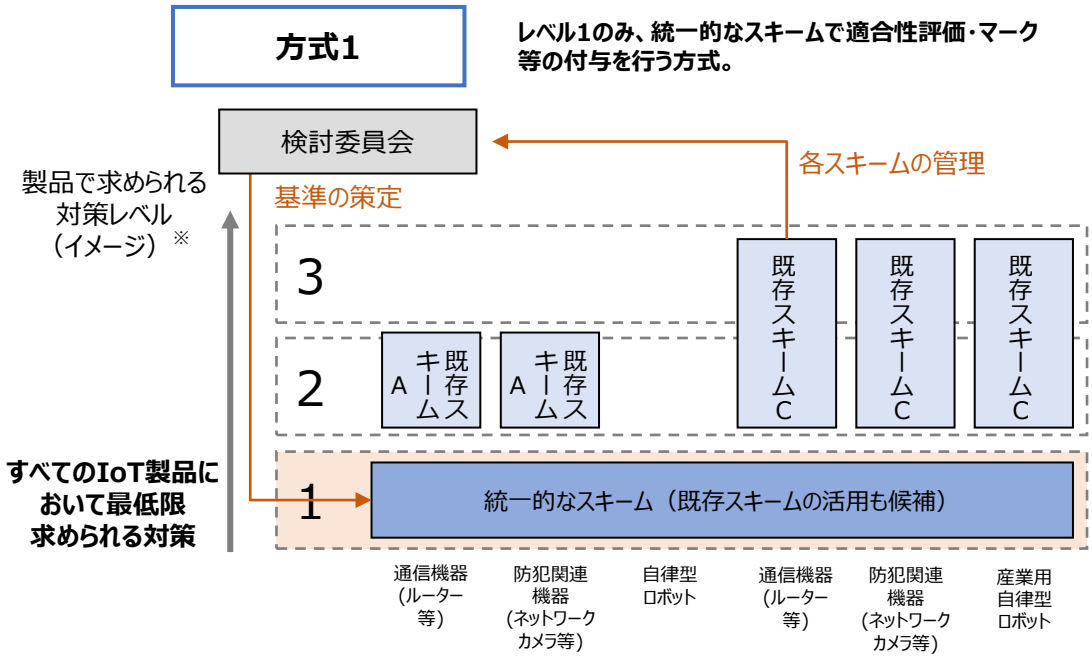
前述のとおり、専門家からなる検討委員会にて基準を検討するが、製品類型ごとにリスクの度合いが異なるところ、求められる対策レベルも製品類型ごとに異なる。このため、複数の対策レベルを設定することが想定されるが、IoT製品において最低限求められる対策をレベル1としたとき、大きく分けて以下の2つの方式でレベル1の適合性評価を行うことが想定される。

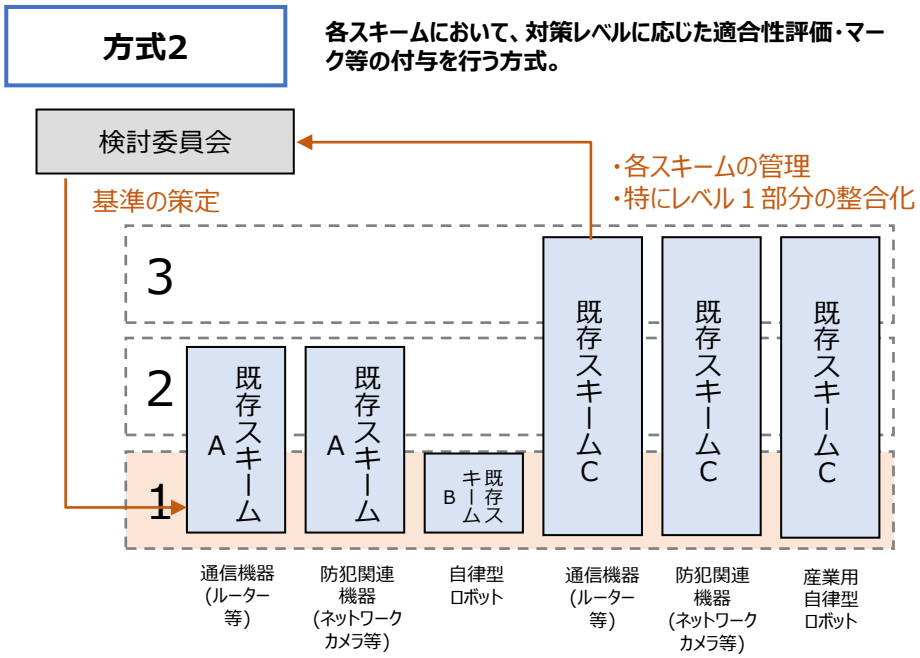
方式1. 広範なIoT製品が活用可能な統一的なスキーム（既存スキームの活用も考慮）を用意し、レベル1については、統一的なスキームで適合性評価・マーク等の付与を行う。より高いレベル（2,3・・・）に関する適合性評価を行う場合のみ、既存スキームにて適合性評価・マーク等の付与を行う。

※高いレベルの各スキームについても、基準の妥当性等について検討委員会に付議を行う。

方式2. レベル1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。

✓ どちらの方式を前提として検討していくべきであるか。





※ レベルを3段階に分けることは一例であることに留意。

【参考】方式毎のメリットと想定される懸念・課題

方式	**方式1** レベル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。
メリット	• ベンダにとってわかりやすい（製品ごとに取得ラベルを区別する必要がないため、手続きが一本化される。） • 消費者にとってわかりやすい。 • 検討委員会が策定したレベル1の基準を一つのスキームに用いるため、製品ごとに齟齬が生じない。	• 高いレベルが求められる製品類型においては、1つのスキームによるラベル付与で足りる。 • 広く普及している既存スキームが複数存在するため、当該スキームが対象としている製品類型については、本制度の活用のハードルが比較的低くなるほか、広報コストを低減できる。
想定される懸念・課題	• より高いレベルに関する適合性評価を行う場合、別スキームの適合性評価やマーク取得が必要となる。 • 普及促進策次第では、活用が低調となる可能性がある。	• 統一的な基準を検討委員会が提示しても、スキームごとの検討や仕組み次第では、スキームごとに不整合が生じる可能性がある。 • 検討委員会が策定したレベル1の基準を各スキームが用いることについて事前に各スキームオーナーと合意する必要があるが、合意が困難、あるいは期間を要する可能性がある。 • 製品類型ごとにスキームが異なるため、ベンダー社内の判断や手続に時間・手間を要する可能性がある。

【参考】適合マーク発行の類型

- 適合マーク発行の類型について、マーク発行者（国・独法・民間団体）と法的な紐づけ有無に基づき、大きく4つの類型に分類される。
- 法的な紐づけがある場合（類型A～C）においても、国自身が適合マークを発行するスキームは稀であり、一般的には、所管省庁の登録・認定を受けた認証機関によりマークが発行される。

<table>
<tr><th>マーク発行者</th><th>法的な紐づけあり</th><th>法的な紐づけなし</th></tr>
<tr><td>国</td><td>【類型A】<table><tr><td>消費者庁</td><td>特定保健用食品マーク（健康増進法）</td></tr></table></td><td>－</td></tr>
<tr><td>独法</td><td>【類型B】<table><tr><td>独立行政法人情報処理推進機構（IPA）</td><td>JISEC認証マーク（情報処理の促進に関する法律（情促法））</td></tr><tr><td>独立行政法人製品評価技術基盤機構（NITE）</td><td>ASNITE認定シンボル（独立行政法人製品評価技術基盤機構法（NITE法））</td></tr><tr><td>独立行政法人製品評価技術基盤機構（NITE）</td><td>JNLA認定シンボル（NITE法、工業標準化法（JIS法））</td></tr></table></td><td>－</td></tr>
<tr><td>民間団体</td><td>【類型C】 ※法に基づく登録を受けた機関がマークを付与<table><tr><td>電気安全環境研究所（JET）、日本品質保証機構（JQA）、UL Japan、テュフ・ラインランド・ジャパン、電磁総合技術センター、日本ガス機器検査協会　など</td><td>◇PSEマーク（電気用品安全法、NITE法）</td></tr><tr><td>UL Japan、テュフ・ラインランド・ジャパン、コスモス・コーポレーション、JATE（電気通信端末機器審査協会）　など</td><td>技適マーク（電波法、電気通信事業法）</td></tr><tr><td>日本穀物検定協会、日本食品分析センター、日本食品油脂検査協会　など</td><td>JASマーク（日本農林規格等に関する法律）</td></tr></table></td><td>【類型D】<table><tr><td>電気製品認証協議会（SCEA）</td><td>Sマーク</td></tr><tr><td>重要生活機器連携セキュリティ協議会（CCDS）</td><td>CCDSサーティフィケーションマーク</td></tr><tr><td>一般社団法人 ビジネス機械・情報システム産業協会（JBMIA）</td><td>BMSecマーク</td></tr><tr><td>公益社団法人日本防犯設備協会</td><td>優良防犯機器認定マーク（RBSSマーク）</td></tr><tr><td>一般財団法人VCCI協会</td><td>VCCIマーク</td></tr></table></td></tr>
</table>

【参考】遠隔操作機構に関するSマーク認証の運用基準

- Sマークにおいては、通信回線を利用して遠隔操作を行う機器に対して「電気用品安全法技術基準の解釈別表第八に係る遠隔操作機構に関するSマーク認証の運用基準第 2 版」（2020年7月20日改訂）を適用している。

- 遠隔操作を行う機器（右図）に対して、以下の要求事項が定められている。
  - 遠隔操作を行うことができる製品の判定方法
  - 通信回線の故障に対する安全状態の維持
  - 不意な動作の抑制対策
  - 動作の確実性
  - 使用する宅内通信回線における動作の円滑性
  - 公衆回線を利用する場合の安全対策
  - 2箇所以上からの遠隔操作
  - 誤操作防止対策
  - 出荷状態における遠隔操作機能の無効化

- この運用基準では、一部の製品で遠隔操作機構に対し、リスクアセスメントの実施が求められ、リスクアセスメントが行われた製品であることを識別する追加表示（RC Ready）も定められている。また、運用基準によりリスクアセスメントが要求されない製品についても、要望に応じてリスクアセスメントを実施した製品において表示することもできる。

JET RC Ready　　JQA RC Ready

遠隔操作を行う機器の分類

	分類	運用基準の適用
①	事業者が、遠隔操作機構も機器本体も製造する。	【システム全体に適用】 機器と遠隔操作機構とをあわせたシステムで運用基準を適用する。このため、認証においては機器に使用されるすべての遠隔操作機構について試験を実施する。かつ、遠隔操作機構の仕様変更等が生じた場合には、設計変更試験願いの提出が必要となる。
②	事業者が、遠隔操作機構の製造事業者に指示して遠隔操作機構の仕様を決めることができる。	
③	事業者がある程度の使用方法を決めるが、標準品を使用するために遠隔操作機構の仕様変更ができない。	【電気製品側だけに適用】 遠隔操作機構に関するＳマーク認証の運用基準のうち、機器に適用できる基準だけ適用し、遠隔操作機構だけに適用する基準は適用外とする。遠隔操作機構については、代表する任意のものを用いて確認試験することはあるが、遠隔操作機構の仕様変更等が生じた場合でも、設計変更試験願いの提出は不要とする。 認証書の付記として「遠隔操作機構（品名：○○○○）については、試験は対象外」である旨を記載する。
運用基準の適用と適用外の境界		
④	事業者に「○○対応」などの表示をするが、使用方法は、遠隔操作機構側（ﾕｰｻﾞｰ、ｼｽﾃﾑｲﾝﾃｸﾞﾚｰﾀｰ含む）任せとする。	使用方法が分からないため評価できない。 運用基準の対象外とする。
⑤	事業者は遠隔操作を意図したものではないが、赤外線リコモン等の受信部を利用して他の事業者が遠隔操作できるようにしてしまう。	遠隔操作の意図がないため、運用基準の対象外とする。

【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(JISEC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に基づく認証 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）	日本防犯設備協会：RBSS JET：系統連系保護装置等認証制度（PCSのみ） 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） 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 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（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）	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 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）	CCに基づく認証 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．前回の検討会のご指摘事項

２．政府の関与や検討体制のあり方

３．適合性評価制度で対象とする製品範囲

４．適合性評価制度で活用する適合性評価スキーム

５．諸外国の適合性評価制度との国際連携

諸外国の適合性評価制度との国際連携

第２回のご指摘事項	• ETSI EN 303 645はセキュリティ要件として過度に厳密ではないため、基準として適している。 • 欧州や米国による国際標準を軸とすることは賛成だが、それらの基準の要素をどれだけ取り入れたかについては明確にしながら検討を進めていただきたい。 • 国際競争力を考え、国際標準に合わせる点と、日本が優位性を取れる点も含めて、検討していく必要がある。
中間とりまとめ案の記載事項	• 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、本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。

【討議事項4】

✓ 諸外国の適合性評価制度との連携について、以下の取組みが必要と思われるが、これ以外に気にとめるべき論点はないか。

(1)既に運用が開始されている制度との相互互換性

✓ シンガポール、フィンランド、ドイツなどが既に運用を開始しているラベリング制度について、相手国の制度の下に日本の認証機関を認定してもらうことが可能であるか。

✓ 不可能な場合には日本での本適合性評価制度の下において発行した証明書が相手国において受け入れ可能となるような適合性評価結果の受け入れのあり方（政府間MRA、認定機関間MRA、認証機関間MRA、試験レポートの相互受け入れ等）はどういうものを採用すべきか。

✓ 諸外国との相互互換性を構築・維持する上で、認定機関や認証機関に対してどのような支援が必要か。

(2)現在検討中であるが制度が運用されていない制度との連携

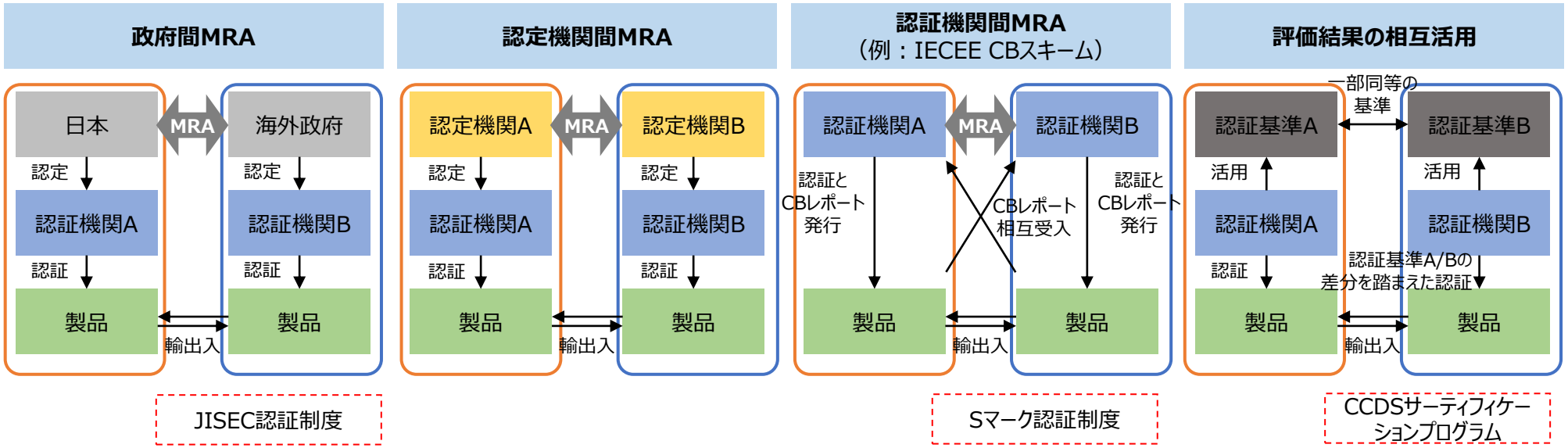
✓ EU：サイバーレジリエンス法、米国：消費者IoT機器ラベリング制度、英：PSTI法など、現在制度設計中の制度については、基準のハーモナイゼーションや適合性評価結果の相互受け入れ（上記（１）と同様）など、政府レベルでの議論を継続させることが必要。

(3)ISO/IECにおける動向

✓ シンガポールが自国のラベリングスキームをベースとしたIoT機器セキュリティに関する適合性評価のスキームをISO/IECに国際標準化提案していることから、国際標準化機関における議論を引き続き注視することが必要。

【参考】国際相互承認の方式

- 認証結果の国際相互承認の方式として、政府間のMRAによるスキーム、認定機関間のMRAによるスキーム、認証機関間の協定によるスキームが存在する。
- Sマーク認証制度では、IECEE CBスキームに基づく認証機関間の相互承認が活用できるほか、JISEC認証制度の場合、CCRA（Common Criteria Recognition Arrangement）に基づく国際相互承認が活用できる。
- これらのスキームは認証結果の国際相互承認に関するスキームであるが、CCDSサーティフィケーションプログラムでは諸外国の適合性評価結果が活用可能である。具体的には、CCDSサーティフィケーションプログラムの基準と諸外国の基準とは一部整合性があるため、諸外国での適合性評価結果が既に存在する場合は、その結果を活用しつつ、CCDSサーティフィケーションプログラムのみで求められる基準を追加評価することで、効率的に認証付与が可能となる。



出所）初回検討会におけるJQA大塚様資料に基づき三菱総合研究所作成

【参考】今後議論すべき事項①（中間報告記載の内容）

1. IoT製品ベンダーの能動的な制度活用を促す仕掛け

(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、その効果や具体的な喚起方法等について、検討する必要がある。

(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、本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。

(3) IoT製品ベンダーや認証機関等に対する支援策

- 適合性評価を行うには認証機関やベンダー、消費者等の関係者に様々なコストが発生すると考えられる。
- まずは、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。

【参考】今後議論すべき事項②（中間報告記載の内容）

2. 適合性評価済製品におけるセキュリティ事案への対応

(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、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) 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。

(3) 評価済製品のサーベイランス、取り消し

- 一度適合性評価を行った後の製品が、市中に流通した際に、不適合の状態でないかを監視（サーベイランス）し、不適合であった場合には取消措置を行える制度を整えることは、粗悪な製品の流通を防止することに有効であると考えられる。
- 一方で、現行制度の状況や、どのような者が運用するか、どのような仕組みとするか、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の議論が不十分であることから、まずは必要性について検討をする必要がある。