経済産業省

資料４

一部非公開

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 10月 3日

本日の議題

【御報告事項】

- 適合性評価の実証状況について【資料３】

【御議論いただきたい事項】

- 発展JISEC認証スキーム体制案【本資料】
- 本制度における☆1の位置づけ（要求レベル）について【本資料】
- 適合性評価済製品におけるセキュリティ事案への対応について【本資料】
- 適合性評価制度活用を促す仕掛けについて【本資料】

1. これまでの検討会でのご指摘事項

2. 発展JISEC認証スキーム体制

3. 本制度における☆1の位置づけ（要求レベル）

4. 適合性評価済製品におけるセキュリティ事案への対応

   4-1. 法的な論点整理

   4-2. リスクに対応するための資源の確保策

   4-3. 評価済み製品の有効期限、サーベイランス、取り消し

5. IoT製品ベンダーの能動的な制度活用を促す仕掛け

   5-1. 調達要件との連携、消費者に対する需要喚起策

   5-2. 諸外国の適合性評価制度との国際連携

   5-3. IoT製品ベンダーや認証機関等に対する支援策

6. 今年度の検討方針

第４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について	• 制度において、コストとスケーラビリティは重要な観点である。国が主導する部分と産業界に委譲する部分を分け、運用コストを国に依存しない仕組みが必要となる。 • 国内で複数のスキームが林立することは良くないので、スキームの統合について引き続き検討していただきたい。
検討体制のあり方について	• 制度の基準に関する議論において、ユーザー（調達者）組織の参画が重要となる。ユーザーも含めて基準を議論することが重要である。 • 今年度はプレ検討委員会で適合基準を議論するということであるが、運用が始まった後でもベンダーの意見を反映できるような体制を構築していただきたい。
責任分界について	• 社会的にコストを負担する構造も考えていく必要がある。社会の関与の仕方も念頭に置きつつ、本制度について発信することが望ましい。 • 今後、保険等の責任を社会全体で負担する仕組みを考慮しつつ制度を構築していけると良い。 • 責任分界の問題を議論するにあたって、契約書モデルや契約条項モデルを作ることで具体的な議論を行うことができる。
適合性評価の要件・基準について	• 評価基準においては、対策の実装段階、ライフサイクル、利用者の保守運用能力を考慮していただきたい。 • 技術の進歩に従って、セキュリティ要件を更新していくことが大切である。
評価コストについて	• 評価者が基準の変化に追随するためのコスト、及び評価基準の変化に対応するためのベンダー側のコストも考慮いただきたい。 • 評価コストについて、家電業界は機能維持の知見を持っているため、家電業界とも協力しつつ、製品の能力維持に関するコストについて検討していただきたい。
製品類型やレベルについて	• ☆2以降で製品類型ごとに基準等を策定するとのことであるが、どの製品類型に該当するか分からない製品も出た場合に相談できる窓口があると良い。 • 各レベルの定義を詳細化する必要がある。製品の用途を考慮いただきたい。調達者にとってどのレベルの製品を調達すべきかの判断材料となる。 • 全てのIoT製品の類型に対して基準を作ることは不可能であるため、製品をうまくグルーピングする必要がある。諸外国の取組等を参照すると良い。
サーベイランスや有効期限について	• 適合性評価済み製品に関する取得時期や有効期限等の最新情報に辿り着けるような仕組みを検討していく必要がある。QRコードの付与も1つの手段である。 • IoT製品の脆弱性の検知・共有・活用の課題もある。米国のように、QRコードにより製品の詳細なプロファイルを確認できるなど、脆弱性管理と連動できればよい。 • ☆1の自己適合宣言に関して、ランダムで製品の試買テストを行うなど、自己適合宣言の品質を担保するための仕組みが必要になる。
国際連携について	• ISO/IEC 27404においても相互承認の重要性が挙げられている。日本の制度が国際的にガラパゴス化しないようにしたほうが良い。 • 国際的な相互承認が理想であるが、困難であれば、制度間の要件の差分を確認して部分的に評価するといった仕組みも考えていければ良い。
ベンダーにおける活用について	• セキュリティの知見が不足するベンダーも多く存在するため、本制度に関する教育プログラムやセミナーを開催することを検討いただきたい。 • コストがかかる取組であるので、インセンティブも検討していただけると良い。補助金など、ベンダーが取り組みやすくなる仕組みがあると良い。 • 自己適合宣言の運用モデルやベストプラクティスが提示されることで、ベンダーとしては対応しやすくなる。
調達者、消費者における活用について	• 人材育成に関して、IPAに閉じた検討をするのではなく、民間と連携することが重要である。 • 普及活動について、家電量販店や通販サイト等の販売者に対する広報も必要となる。本制度にうまく誘導できるような広報活動が必要となる。 • 本制度は社会インフラの一部となるので、消費者も社会的コストを担っていく一員としての理解や知識を持つために行政等からの教育や啓発が必要である。 • 制度の継続的維持のためには、開発・認証・購入のサイクルを回す必要がある。制度が利用されないと、予算を多く割かないと維持できない制度になってしまう。 • 政府調達時にセキュリティが脆弱な製品が紛れた場合の対処法についても検討する必要がある。本制度をすり抜けた場合の対応についても、検討が必要である。 • IoT機器を活用したシステムやサービスにも対応した適合性評価制度の検討を進める必要がある。
評価機関への支援について	• ISO/IEC 17025のレベルで全ての評価機関の適格性を担保することは難しいのではないか。評価を行う人材の育成も意識することが重要である。 • 適合性評価に用いるツールをOSSとして無償提供することは制度にとってプラスに働く。既存の取組を参照しつつ、本制度を検討していくと良い。

【参考】第３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. これまでの検討会でのご指摘事項

2. 発展JISEC認証スキーム体制

3. 本制度における☆1の位置づけ（要求レベル）

4. 適合性評価済製品におけるセキュリティ事案への対応

- 4-1. 法的な論点整理
- 4-2. リスクに対応するための資源の確保策
- 4-3. 評価済み製品の有効期限、サーベイランス、取り消し

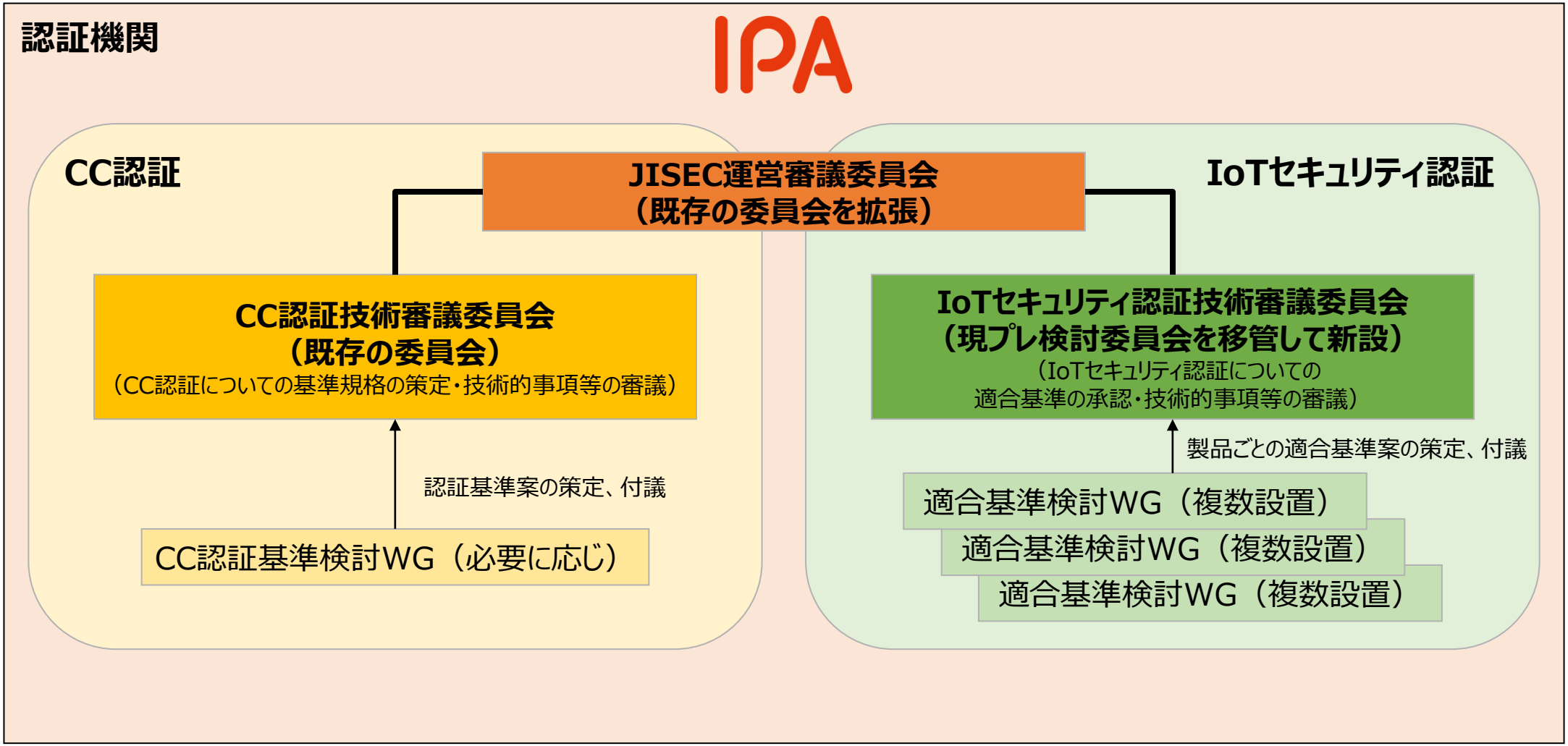
5. IoT製品ベンダーの能動的な制度活用を促す仕掛け

- 5-1. 調達要件との連携、消費者に対する需要喚起策
- 5-2. 諸外国の適合性評価制度との国際連携
- 5-3. IoT製品ベンダーや認証機関等に対する支援策

6. 今年度の検討方針

発展JISEC認証スキーム体制案

- 第４回検討会では、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方針で合意が得られた。
- IPAにおいて、**本制度とCC認証を合わせ発展JISEC認証スキームとする体制（認証制度運営審議委員会およびCC認証技術審議委員会、IoTセキュリティ認証技術審議委員会を設置）**で制度設計する方針で良いか。



1. これまでの検討会でのご指摘事項

2. 発展JISEC認証スキーム体制

3. 本制度における☆1の位置づけ（要求レベル）

4. 適合性評価済製品におけるセキュリティ事案への対応

- 4-1. 法的な論点整理
- 4-2. リスクに対応するための資源の確保策
- 4-3. 評価済み製品の有効期限、サーベイランス、取り消し

5. IoT製品ベンダーの能動的な制度活用を促す仕掛け

- 5-1. 調達要件との連携、消費者に対する需要喚起策
- 5-2. 諸外国の適合性評価制度との国際連携
- 5-3. IoT製品ベンダーや認証機関等に対する支援策

6. 今年度の検討方針

本制度における☆1の位置づけ（要求レベル）について（1/2）

- プレ委員会において、☆1の要求基準等を議論するに当たって、☆1の位置づけ（要求レベル）を明確化し、☆1で担保する安全性について共通認識を持った上で議論を進めるべきとの意見が挙げられた。
- ☆1の位置づけ（要求レベル）は、制度設計全体にも影響を及ぼすところ、本検討会においても議論いただきたく、**☆1においてラベル取得を想定する製品、ユーザ・IoT製品ベンダーにおける便益、評価のしやすさ・信頼性、国内外制度との連携、考慮する脆弱性を以下のように整理してはどうか**。
- また、これらの整理を踏まえ、**☆1において考慮すべき主なセキュリティ脅威として、7つのセキュリティ脅威が想定されるが、過不足はあるか**。

区分	☆1	☆2	☆3	☆4
ラベル取得が想定される主な製品	• セキュリティに詳しくないユーザが、ホームユース又はプライベートユースで使う消費者向けIoT製品 (個人が、セキュリティ以外の機能や価格で選ぶ可能性が高いIoT製品) • 他のセキュリティ製品・機能と合わせてセキュリティ対策を行う必要がある企業向けIoT製品 ※☆1では、製品類型を問わず広範なIoT製品を対象とした適合基準を策定する。	• 企業向けに利用される可能性があるIoT製品（企業向けだが、セキュリティ以外の機能や価格で選ばれる可能性が高いIoT製品） ※☆2以降では、製品類型ごとに適合基準を策定する。	• 企業や産業向けに利用され、機能や価格とともにセキュリティ対策状況も重視されるIoT製品	
ユーザにおける便益	• 一定程度のセキュリティ対策に取り組んでいる製品であることが確認できる	• 基本的なセキュリティ対策について、技術的に検証されている製品であることが確認できる（中小企業・組織レベルの利用を想定）	• 機器調達におけるサプライチェーンリスク管理で要求される、製品固有や組織の主要なセキュリティ要件に対応していることが、客観的に評価された製品であることが確認できる（大企業・組織レベルの利用を想定、自社での評価に代替できる）	
IoT製品ベンダーにおける便益	• 製品価格への転嫁が軽微な安価なコストでラベルを取得でき、一定程度のセキュリティ対策を実施していることを示すことができる • ラベルを取得することで、製品の競争力が一定程度増加する	• ラベルを取得することで、一般企業・組織の調達条件を満たし、製品の売上増加に寄与する	• ラベルを取得することで、高いセキュリティレベルが求められる企業・組織の調達条件を満たし、製品の売上増加に寄与する	
評価のしやすさ、信頼性	• 文書に基づく机上評価が中心で、IoT製品ベンダーのIT担当者やセキュリティ担当者がチェックリストとガイドラインを見て自己評価できるレベル（検証や評価のスキルを持たない担当者でも評価が可能） ※ 実機テストでは、製品の最終段階に別途実施したテストの評価結果の確認を行うことも許容する。	• 実際の機器の動作による裏付けが必要な機能については、技術的な評価を行うレベル（評価スキルを持った評価者による評価が必要）	• 評価能力が第三者によって認められた評価機関により評価を行うレベル（評価の信頼性と客観性を担保する）	

（次ページに続く）

※ ☆2以降の位置付け（要求レベル）についても今後詳細化する。

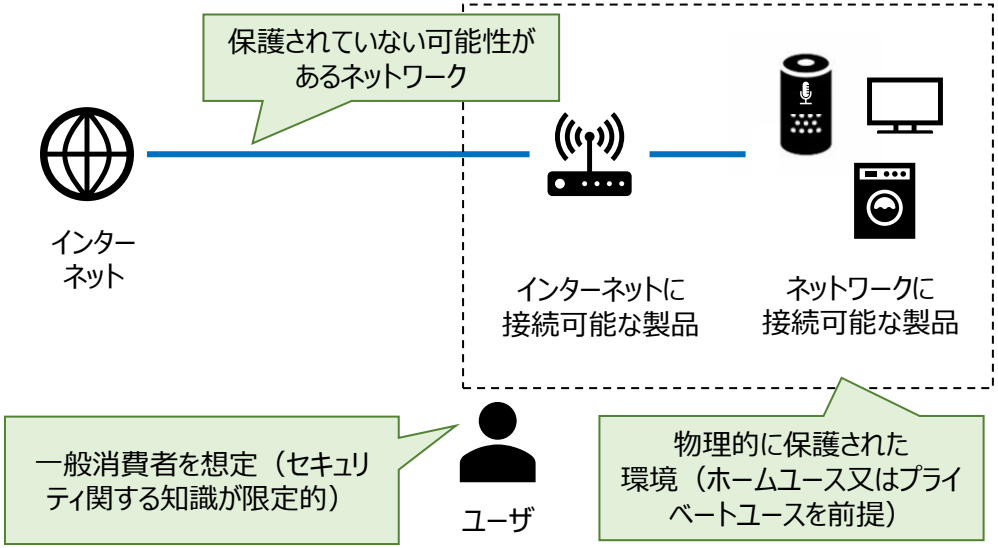
本制度における☆1の位置づけ（要求レベル）について（2/2）

区分	☆1	☆2	☆3	☆4
国内既存制度との連携	• 総務省（端末設備等規則）：求められる要件を包含する • CCDSサーティフィケーションプログラム：☆1の一部の要件を包含する	• CCDSサーティフィケーションプログラム：☆1のすべての要件を包含する • JBMIA BMSec：求められる要件を包含する	• CCDSサーティフィケーションプログラム：☆2の製品別のすべての要件を包含する	• CCDSサーティフィケーションプログラム：☆2の製品別のすべての要件を包含する
諸外国制度との連携	• シンガポールCLS：＊1要件を包含する • 英国PSTI法：求められる要件を包含する • ETSI EN 303 645：M/MCの要件（必須要件）の一部を包含する • 米国Cyber Trust Markの要件を包含する※ • EU CRA：デジタル製品に求められる一部の要件を包含する※ ※ 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。	• シンガポールCLS：＊2要件を包含する • ETSI EN 303 645：M/MCの要件（必須要件）をすべて包含する • EU CRA：デジタル製品に求められる要件を包含する※	• シンガポールCLS：＊3～＊4要件を包含する • ETSI EN 303 645：R/RCの要件（勧告）を包含する • EU CRA：重要なデジタル製品（低リスク）に求められる要件を包含する※	• シンガポールCLS：＊3～＊4要件を包含する • ETSI EN 303 645：R/RCの要件（勧告）を包含する • EU CRA：重要なデジタル製品（高リスク）に求められる要件を包含する※
考慮する脆弱性	• 過去に複数発生した大規模インシデントに起因した脆弱性（Mirai等） • 深刻度の高い（CVSS v3基本評価基準7.0以上）既知脆弱性のうち、悪用される可能性がある脆弱性	• 過去に発生したインシデントに起因した脆弱性 • 深刻度の高い（CVSS v3基本評価基準7.0以上）既知脆弱性のうち、悪用される可能性がある脆弱性	• 過去に発生したインシデントに起因した脆弱性 • 今後顕在化が想定される脆弱性 • 深刻度が中程度以上（CVSS v3基本評価基準4.0以上）既知脆弱性のうち、悪用される可能性がある脆弱性	
考慮すべき主なセキュリティ脅威	① 汎用のデフォルトパスワードを使用することで攻撃者の標的となり、外部からの不適切なアクセスが可能となる脅威【弱い認証機能】 ② セキュリティパッチが適用されず、脆弱性を放置したままの状態で継続利用されることで、外部から不正アクセスや攻撃の対象となり、機器を不正利用される脅威【脆弱性管理の不備】 ③ マルウェア等を用いて外部からの不正アクセスを受け、機器が内部に保有している設定情報等が漏えい・改ざんされる脅威【マルウェア混入による情報漏えい、改ざん】 ④ 機器の通信が盗聴され、通信データ等が漏えいする脅威【盗聴】 ⑤ ネットワーク切断や停電等の想定外の事象が発生した際に、意図しないセキュリティ設定となる脅威【セキュリティ管理の不備】 ⑥ 未使用インタフェースの有効化や廃棄対象機器への情報等の残留に起因する脅威【機器設定管理の不備】 ⑦ マルウェア等を用いて外部からの不正アクセスを受け、他の外部機器へ不正アクセス等を行う中継地点（踏み台）として使用される脅威【マルウェア混入による踏み台】	☆1のセキュリティ脅威に加え、 ⑧ マルウェア等を用いて外部からの不正アクセスを受け、利用する組織内部の不正アクセス等を行うバックドアとして使用される脅威【バックドア】 ⑨ 正規のユーザが製品本来の機能を利用できなくなる脅威【サービス不能（DoS）】	☆2のセキュリティ脅威に加え、 ⑩ 利用する組織内部からの不正アクセス等により、不正アクセスや設定情報等の漏えい・改ざんを受ける脅威【情報漏えい、改ざん】 ⑪ 開発段階で不正なプログラムが埋め込まれる脅威【サプライチェーン攻撃】 ⑫ 物理的に接触した攻撃者によってハードウェア／ソフトウェアが不正に改造される脅威【不正改造】	

【参考】☆1取得が想定される製品のユースケース・守るべき資産について

- 本制度の対象製品について、☆1の位置づけ（要求レベル）を前提とした場合、以下のユースケースが想定される。
- IoT製品における守るべき資産に関して、IPA「つながる世界の開発指針」（3.1 守るべきものの整理）では、「IoT機能」「本来機能」「情報」「その他」の4つの資産が、IoT製品において「守るべきもの」として挙げられている。また、CCDS「IoT機器に対するリスク分析のガイド」では、これらの機能や情報に加え、「健康、人命」といった利用者の物理的安全性が明示的に考慮されている。
- これらの整理を踏まえ、利用者の物理的安全性を4つ目の資産として考慮した「1. IoT機能」「2. 本来機能」「3. 情報」「4. その他の物理的資産」の4つの資産が、IoT製品において守るべき資産として想定される。
- そのうち、☆1製品で想定する守るべき資産として、ユースケースを踏まえ、以下に示す機能・情報等が想定される。

☆1で想定するIoT製品のユースケース（案）



想定する守るべき資産（案）

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 等	• 設定情報 • 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コンポーネントが内蔵する物理的資産	ー	• 人的資産[3] • 物理的資産[4]

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: 事故や誤動作が発生してもユーザの身体や生命、財産を防ぐための機能のこと
3: 利用者の健康など、利用者の物理的安全性のこと
4: 製品本体や関連するコンポーネントのこと

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. これまでの検討会でのご指摘事項
2. 発展JISEC認証スキーム体制
3. 本制度における☆1の位置づけ（要求レベル）
4. 適合性評価済製品におけるセキュリティ事案への対応
   - **4-1. 法的な論点整理**
   - 4-2. リスクに対応するための資源の確保策
   - 4-3. 評価済み製品の有効期限、サーベイランス、取り消し
5. IoT製品ベンダーの能動的な制度活用を促す仕掛け
   - 5-1. 調達要件との連携、消費者に対する需要喚起策
   - 5-2. 諸外国の適合性評価制度との国際連携
   - 5-3. IoT製品ベンダーや認証機関等に対する支援策
6. 今年度の検討方針

法的な論点整理

第３・４回のご指摘事項	• 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。
中間とりまとめの記載事項	• 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。利用者の立場から見ても、認証を取得した製品を選んだという説明責任が果たせることは重要であると考えられる。

適合性評価済み製品にインシデント※1が生じた場合の各ステークホルダーの責任を整理し、その責任に応じたインシデント対応策を検討する。

各ステークホルダーの責任

- ラベルはIoT製品の完全なセキュリティを保証するものではなく、製品の推奨を示すものではない旨、またIPAはIoT製品に関するいかなる保証も行わない旨を言及する。
- 製品が実際には適合基準を満たしていなかった場合、評価者は、その原因について明らかにし、改善する必要がある。
- 認証機関（IPA）は、適合基準に対する不適合について調査し、ラベルの取り消しを行う必要がある。
- 制度全体としては、利用者・調達者に対する啓発活動を実施する必要があるほか、評価機関の認定基準、検証事業者の定義、自己適合宣言方法等の妥当性について検証を行う必要がある。適合基準ではインシデントを防ぎきれなかった事案が頻発した場合、適合認証技術審議委員会で適合基準の妥当性について検証する必要がある。

本制度のメリット

- 利用者・調達者にとっては、適合性評価済製品を利用・調達することにより、利用者・調達者としての一定の責務を果たしているとみなせる可能性がある。
- IoT製品ベンダー等にとっては、製造物責任における「欠陥」の有無や不法行為責任における過失の有無、債務不履行責任における「債務者の責めに帰することができない事由」の判断の際に、製品が適合性評価を受けることで一定基準のセキュリティ対策を行っているとみなせる※2可能性がある。

※1：本資料における「インシデント」とは、サイバー攻撃等により、利用者・調達者に被害が生じた場合をいう。
※2：「一定基準のセキュリティ対策を行っているとみなせる」とは、「適合性評価制度の定める方法により同制度が定めた基準に適合すると認定を受けた事実を立証できる。また同水準のセキュリティ対策を行った推認を受ける可能性がある」との意味である。

適合性評価済み製品にインシデントが生じた場合の認証機関の責任

- IPAのJISEC制度やJCMVP制度では、認証書が保証書ではない旨や製品の推奨を示すものではない旨が言及されている。また、製品に関するいかなる保証も行わない旨が言及されている。
- シンガポールのCLSでも、試験やラベルに関して、いかなる種類の表明、保証、誓約も行わない旨が言及されている。
- ドイツのIT Security Labelでは、ラベルはIT製品が完全に安全であることを保証するものではなく、製造者が常に指定された基準を満たすことを保証するものではない旨が言及されている。
- 本制度においても、ラベルはIoT製品の完全なセキュリティを保証するものではなく、製品の推奨を示すものではない旨、またIPAはIoT製品に関するいかなる保証も行わない旨を言及した方が良いのではないか。

IPAの認証制度における免責に関する言及

制度名	JISEC制度	JCMVP制度
免責に関する言及	認証書は独立行政法人情報処理推進機構または認証書を承認し、もしくは効力を与えるその他の組織による**IT製品の推奨を示すものではなく**、独立行政法人情報処理推進機構または認証書を承認または効力を与えるその他の組織は、明示あるいは黙示を問わず、**IT製品に関するいかなる保証も行わない**。	暗号モジュール認証書は独立行政法人情報処理推進機構による**暗号モジュール製品等の保証書ではない**。また、独立行政法人情報処理推進機構は、明示、黙示を問わず、**暗号モジュールを用いた暗号モジュール製品等に関していかなる保証も行わない**。なお、本認証書を、不正に使用した場合、並びに誤解を招くような方法で広告又は説明等に使用した場合には、暗号モジュール認証の取消を行うことがある。

海外のIoTラベリング制度における免責に関する言及

国	シンガポール	ドイツ
制度名	Cybersecurity Labelling Scheme (CLS)	IT-Sicherheitskennzeichen (IT Security Label)
免責に関する言及	CSAは試験や付与されたラベルに関して、明示、黙示、法定を問わず、**いかなる種類の表明、保証、誓約も行わない**。いかなる人も自己責任で使用・信頼すること。	**IT製品が完全に安全であることを保証するものではなく**、ラベルの有効期限が切れた後を含め、**製造者が常に指定された基準を満たすことを保証するものではない**。

出所）CSA、Cybersecurity Labelling Scheme (CLS) Publication No. 1 https://www.csa.gov.sg/docs/default-source/our-programmes/certification-and-labelling-scheme/cls/publications/pub-cls-pub-1-overview-of-cls-v12.pdf?sfvrsn=b559ba25_0
BSI、IT Security Label https://www.bsi.bund.de/EN/Themen/Verbraucherinnen-und-Verbraucher/IT-SiK-fuer-Verbraucher/IT-SiK-fuer-Verbraucher_node.html

適合性評価済み製品にインシデントが生じた場合の各ステークホルダーの責任

- 適合性評価済み製品にインシデントが生じた場合、インシデントの原因やケースによって、各ステークホルダーが負うべき責任が変わる。
- 利用者・調達者にとっては、適合性評価済製品を利用・調達することにより、利用者・調達者としての一定の責務を果たしているとみなせる可能性がある。
- IoT製品ベンダー等にとっては、製造物責任における「欠陥」の有無や不法行為責任における過失の有無、債務不履行責任における「債務者の責めに帰することができない事由」の判断の際に、製品が適合性評価を受けることで一定基準のセキュリティ対策を行っているとみなせる可能性がある。

適合性評価済み製品にインシデントが生じた場合の各ステークホルダーの責任（ケース別）

インシデントの原因	ケース	利用者・調達者	IoT製品ベンダー等	評価機関・検証事業者	認証機関（IPA）	制度全体（スキームオーナー）
A) 利用者の設定や使い方の問題	A-1) 設定や使い方についてIoT製品ベンダー等が適合基準で定められた情報を適切に提供していた場合	生じた損失について補填する責任有	–	–	–	適合基準の妥当性について検証の必要有
	A-2) 設定や使い方についてIoT製品ベンダー等が適合基準で定められた情報を適切に提供していなかった場合	生じた損失について補填する責任有※1	不法行為責任や債務不履行責任に問われる可能性有 （自己評価の場合）適合基準に対する適合の判断を誤った原因を明らかにする責任有	（第三者評価の場合）適合基準に対する不適合を見抜けなかった原因を明らかにする責任有	適合基準に対する不適合について調査する責任有	評価機関の認定基準、検証事業者の定義、自己適合宣言方法等の妥当性について検証の必要有
B) IoT製品固有のセキュリティの問題	B-1) 製品が実際には適合基準を満たしていなかった場合		製造物責任や不法行為責任、債務不履行責任に問われる可能性有 （自己評価の場合）適合基準に対する適合の判断を誤った原因を明らかにする責任有			
	B-2) 適合基準ではインシデントを防ぎきれなかった場合		製造物責任や不法行為責任、債務不履行責任に問われる可能性有※2	–	–	適合基準の妥当性について検証の必要有

※1 適合性評価済製品を利用・調達することにより、利用者・調達者としての一定の責務を果たしているとみなせる可能性有

※2 不法行為責任における過失の有無や、債務不履行責任における「債務者の責めに帰することができない事由」の判断の際に、製品が適合性評価を受けることで一定基準のセキュリティ対策を行っているとみなせる可能性有

赤文字は法的責任

適合性評価済み製品におけるインシデントへの対応策

- 本制度のステークホルダーそれぞれが負うべき責任を踏まえ、インシデントへの対応策を実施する必要がある。
- 製品が実際には適合基準を満たしていなかった場合、評価者は、その原因について明らかにし、改善する必要がある。認証機関は、適合基準に対する不適合について調査し、ラベルの取り消しを行う必要がある。
- 制度全体としては、利用者・調達者に対する啓発活動を実施する必要があるほか、評価機関の認定基準、検証事業者の定義、自己適合宣言方法等の妥当性について検証を行う必要がある。さらに、インシデントが頻発した場合、適合基準の妥当性について検証する必要がある。

適合性評価済み製品に対するインシデント対応策（ケース別）

インシデントの原因	ケース	利用者・調達者	IoT製品ベンダー等	評価機関・検証事業者	認証機関（IPA）	制度全体（スキームオーナー）
A) 利用者の設定や使い方の問題	A-1) 設定や使い方についてIoT製品ベンダー等が適合基準で定められた情報を適切に提供していた場合	• 関係各所と連携し、インシデント対応を実施する	–	–	–	• 利用者・調達者に対する啓発活動を実施する
	A-2) 設定や使い方についてIoT製品ベンダー等が適合基準で定められた情報を適切に提供していなかった場合		• インシデントの原因を調査する • 関係各所と連携し、インシデント対応を実施する • （自己評価の場合）適合性評価を適切に行えなかった原因をもとに改善を行う	• （第三者評価の場合）適合性評価を適切に行えなかった原因をもとに改善を行う	• インシデントの原因について確認し、適合基準に対する不適合を理由としてラベルの取り消しを行う	• 適合認証技術審議委員会で評価機関の認定基準、検証事業者の定義、自己適合宣言方法等の妥当性について検証する
B) IoT製品固有のセキュリティの問題	B-1) 製品が実際には適合基準を満たしていなかった場合					
	B-2) 適合基準ではインシデントを防ぎきれなかった場合	• 関係各所と連携し、インシデント対応を実施する • より高いレベルの製品の調達を検討する	• インシデントの原因について調査する • 関係各所と連携し、インシデント対応を実施する • より高いレベルのラベルの取得を検討する	–	–	• 適合認証技術審議委員会で適合基準の妥当性について検証する

【参考】セキュリティ事案が生じた際に、問われ得る法的責任

- IoT製品にセキュリティ事案が生じた際に、各ステークホルダーに問われ得る法的責任として、製造物責任、不法行為責任、債務不履行責任が挙げられる。

責任者	製造物責任	不法行為責任	債務不履行責任
IoT製品メーカー	製造物の「欠陥」により、他人の生命、身体又は財産を侵害した場合※1	故意又は過失によって他人の権利又は法律上保護される利益を侵害した場合	債務を負っており、メーカがその債務の本旨に従った履行をしないとき又は債務の履行が不能である場合※2
部品ベンダ			
ソフトウェアベンダ	-		
利用者・調達者			

※1 欠陥による被害が、その製造物自体の損害にとどまった場合は、不法行為責任や債務不履行責任を追及することになる。
※2 その債務の不履行が契約その他の債務の発生原因及び取引上の社会通念に照らして債務者の責めに帰することができない事由によるものであるときは、この限りでない。

被害者や債権者に過失があった場合は、過失相殺が適用される可能性がある。

出所）製造物責任法 https://elaws.e-gov.go.jp/document?lawid=406AC0000000085
民法 https://elaws.e-gov.go.jp/document?lawid=129AC0000000089

1. これまでの検討会でのご指摘事項
2. 発展JISEC認証スキーム体制
3. 本制度における☆1の位置づけ（要求レベル）
4. 適合性評価済製品におけるセキュリティ事案への対応
    - 4-1. 法的な論点整理
    - **4-2. リスクに対応するための資源の確保策**
    - 4-3. 評価済み製品の有効期限、サーベイランス、取り消し
5. IoT製品ベンダーの能動的な制度活用を促す仕掛け
    - 5-1. 調達要件との連携、消費者に対する需要喚起策
    - 5-2. 諸外国の適合性評価制度との国際連携
    - 5-3. IoT製品ベンダーや認証機関等に対する支援策
6. 今年度の検討方針

リスクに対応するための資源の確保策

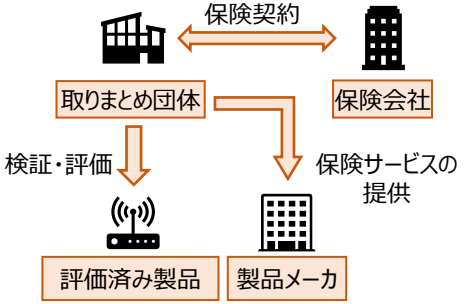
第３・４回のご指摘事項	• 誰かの責任を追及することなく被害が公平に分担される社会の構築に資する制度の提言について、日本がリードできると良い。 • 社会的にコストを負担する構造も考えていく必要がある。社会の関与の仕方も念頭に置きつつ、本制度について発信することが望ましい。 • 今後、保険等の責任を社会全体で負担する仕組みを考慮しつつ制度を構築していけると良い。
中間とりまとめの記載事項	• 事案発生時の法的な責任分担の整理に加え、例えば保険制度のような、事案発生時に対処を適切に行い、被害救済や原因是正に繋がる資源の確保策についても、どのような策が効果的か等について、必要に応じて検討する必要がある。

以下の施策の将来的な実現に向けて、検討を進めていく。

サイバー保険の活用促進

- IoT製品ベンダー、利用者・調達者、評価機関、認証機関等が各々の責任を果たしていたとしても、サイバー攻撃によって被害が発生する可能性をゼロにすることはできない。そのような事態に備え、サイバー保険の活用の促進について検討を行い、損害を広く分散する社会の構築を目指していくことが望ましい。いくつかの方向性が考えられるが、公的機関がサイバーセキュリティ保険を一括契約した前例がなく、☆１では自己適合宣言を採用するため保険料の料率が高くなると想定され、コストメリットが働かない可能性が高く、IPAが保険会社と一括契約を結ぶことは現実的ではない。
- そのため、民間事業者のサービスと連携していく方針とする。具体的には、以下の施策について当該事業者と検討を進めていくことが案として考えられる。

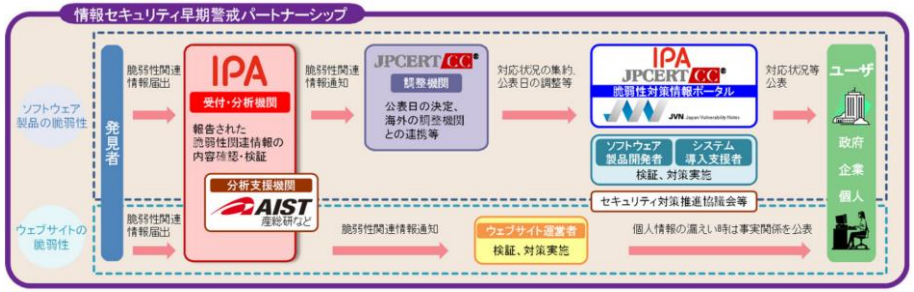
保険付帯検証・評価サービス
検証事業者や評価機関が評価を行って認証を取得した製品の利用者において発生したインシデント被害に対して、補償を行う。検証事業者や評価機関の取りまとめ団体を契約者とすることで、複数のIoT製品ベンダーや複数の製品に対して一括で保険加入が可能となる点において、保険料や保険申請・支払等におけるコストメリットが得られると考えられる。



適合性評価済みIoT製品に対するサイバー保険の割引サービス
保険会社が提供するサイバー保険の保険料について、適合性評価済みIoT製品を調達することで割引になるよう設定いただく。また、製品付帯サイバー保険の保険料について、通常のIoT製品よりも適合性評価済みIoT製品の方が安くなるよう設定いただく。

情報セキュリティ早期警戒パートナーシップとの連携

- 国内におけるソフトウェア等の脆弱性関連情報を適切に流通させるための枠組みである「情報セキュリティ早期警戒パートナーシップ」と連携を行い、認証済み製品に関して寄せられた脆弱性情報を情報セキュリティ早期警戒パートナーシップの受付にも共有し、早期の対応を促す仕組みを設けることが案として考えられる。



1. これまでの検討会でのご指摘事項
2. 発展JISEC認証スキーム体制
3. 本制度における☆1の位置づけ（要求レベル）
4. 適合性評価済製品におけるセキュリティ事案への対応
    - 4-1. 法的な論点整理
    - 4-2. リスクに対応するための資源の確保策
    - **4-3. 評価済み製品の有効期限、サーベイランス、取り消し**
5. IoT製品ベンダーの能動的な制度活用を促す仕掛け
    - 5-1. 調達要件との連携、消費者に対する需要喚起策
    - 5-2. 諸外国の適合性評価制度との国際連携
    - 5-3. IoT製品ベンダーや認証機関等に対する支援策
6. 今年度の検討方針

適合性評価済み製品に対する有効期限の設定

第３・４回のご指摘事項	• 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。 • 適合性評価済み製品に関する取得時期や有効期限等の最新情報に辿り着けるような仕組みを検討していく必要がある。QRコードの付与も1つの手段である。
中間とりまとめの記載事項	• 適合性評価結果の有効期限についてどう考えるか、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。

適合性評価済み製品に対しては、製品のライフタイムや評価に要するコスト、利用者・調達者におけるわかりやすさ等を考慮の上、定めることが望ましい。諸外国の制度等も参考に以下の方針で実施することが考えられる。

自己適合宣言の場合
- 有効期限は最大2年※とし、その期間中は製品に対するセキュリティアップデートを提供することとする。
- 有効期限が経過後、同じ製品で更新を希望する場合、改めて自己適合宣言を行うことを求める。

※サポート期間に合わせて、２年以内の有効期限も設定可

第三者認証の場合
- 有効期限は最大2年※とし、その期間中は製品に対するセキュリティアップデートを提供することとする。ただし、適合基準のメジャーアップデートや製品仕様の更新がない場合、最大5年までの延長を認める。
- 5年経過後、同じ製品で更新を希望する場合、改めて第三者評価を行うことを求める。

※サポート期間に合わせて、２年以内の有効期限も設定可

適合性評価済み製品が有効期限内かどうか等、製品に関する最新の情報を利用者・調達者が入手できるよう、有効期限についてのラベルへの表示やQRコードを用いた情報提供の手段を設ける。ただし、具体的な手段については、IoT製品ベンダーの意見や国際動向を踏まえながら引き続き検討を行う。

諸外国制度における有効期限の設定

国・地域	シンガポール	ドイツ	フィンランド
制度名	Cybersecurity Labelling Scheme (CLS)	IT Security Label	Finnish Cybersecurity Label
有効期限	最大3年間 （開発者が製品に対するセキュリティアップデートを行ってサポートする期間）	製品カテゴリーごとの別段の定めがない限り 通常2年間	申請プロセスの開始時に指定することができるが 製品のセキュリティアップデートが提供される期間を 超えることはできない （製品のセキュリティ機能が依然として要件を満たしていることを確認するため、年次審査が行われる）

Cybersecurity Labelling Scheme (CLS) Publication No. 1
https://www.csa.gov.sg/docs/default-source/our-programmes/certification-and-labelling-scheme/cls/publications/pub-cls-pub-1-overview-of-cls-v12.pdf?sfvrsn=b559ba25_0
BSI Process Description forthe Issuance of IT Security Labels
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/IT-Sicherheitskennzeichen/Process_Description_ITSecurityLabel.pdf?__blob=publicationFile&v=4
TRAFICOM Terms of Use
https://tietoturvamerkki.fi/sites/default/files/media/file/Terms%20of%20Use%20%E2%80%93%20Cybersecurity%20Label%20for%20IoT%20consumer%20devices.pdf

適合性評価済み製品に対するサーベイランスの実施

第３・４回のご指摘事項	• ☆1の自己適合宣言に関して、ランダムで製品の試買テストを行うなど、自己適合宣言の品質を担保するための仕組みが必要になる。
中間とりまとめの記載事項	• 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、特に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。

自己適合宣言の品質の確保や、適合性評価制度自体の信頼性確保のために、認証機関によるサーベイランスの仕組みを採り入れることが望ましい。

想定される仕組みの案

- 認証機関（IPA）は、適合性評価済み製品を検査やサーベイランスする権利を有する。
- 認証機関（IPA）に窓口を設け、適合性が疑わしい評価済み製品の通報を受け付ける。
- 通報内容等をもとに、検査やサーベイランスを実施すべき製品対象があるか否かについて、 1年に1度、認証機関（IPA）が確認を行う。
- 検査やサーベイランスでは、適合性評価済み製品が適合基準を満たしているかについて、評価手順に従って評価を行う。

諸外国制度におけるサーベイランスに関する取組

国・地域	シンガポール	ドイツ	フィンランド
制度名	Cybersecurity Labelling Scheme (CLS)	IT Security Label	Finnish Cybersecurity Label
スキームオーナー	Cybersecurity Certification Centre (CCC)	Federal Office for Information Security (BSI)	Finnish Transport and Communications Agency (TRAFICOM)
サーベイランスに関する規定	CCCは、ラベルが付与された製品について、**無作為の検査・サーベイランス・試験を実施する権利**を有する。監査の目的は、**ラベルが付与された製品がCLS出版物の要求事項に適合していることを確認**することである。	ラベルが付与された製品は、**BSIによる臨時および定期的なサンプリング調査の対象**となり、**その製品が製造者によって保証された機能を備えているかどうかがチェック**される。サンプリングは、製品や技術、またはラベルが付与されていないメーカの類似製品に起因して実施される場合がある。**製品について製造者の宣言からの逸脱が検出された場合、BSIは、**製品情報ページでの消費者への情報提供やラベルの取り消し等、**ラベルに対する消費者の信頼を保護するための適切な措置を実施**することができる。	**ラベルの使用は、抜き打ち検査やフィードバックなどにより監視**される。

Cybersecurity Labelling Scheme (CLS) Publication No. 1
https://www.csa.gov.sg/docs/default-source/our-programmes/certification-and-labelling-scheme/cls/publications/pub-cls-pub-1-overview-of-cls-v12.pdf?sfvrsn=b559ba25_0
BSI Process Description forthe Issuance of IT Security Labels
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/IT-Sicherheitskennzeichen/Process_Description_ITSecurityLabel.pdf?__blob=publicationFile&v=4
TRAFICOM Terms of Use
https://tietoturvamerkki.fi/sites/default/files/media/file/Terms%20of%20Use%20%E2%80%93%20Cybersecurity%20Label%20for%20IoT%20consumer%20devices.pdf
TRAFICOM The Finnish Cybersecurity Label
https://tietoturvamerkki.fi/sites/default/files/media/file/cybersecurity_label_presentation-280920.pdf

適合性評価済み製品に対する付与したラベルの取り消し

中間とりまとめの記載事項	• 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。

適合性評価制度の信頼性確保のために、適合性評価済み製品においても付与したラベルを取り消す仕組みを設ける。

- 適合性評価済み製品において以下の状況が発覚した場合、付与したラベルの取り消しを行う。
  - ✓ 申請内容が虚偽であることが発覚した場合
  - ✓ IoT製品ベンダー等が定められている義務を履行しない場合
  - ✓ 製品が適合基準を満たさなくなった場合
  - ✓ サーベイランスで不適合であることが発覚し、猶予期間中に適切な是正措置が行われなかった場合
- 悪質であった場合、もしくは利用者・調達者に与える影響が大きい場合、その旨を一般に周知する。

諸外国制度におけるラベルの取り消しに関する取組

国・地域	シンガポール	ドイツ	フィンランド
制度名	Cybersecurity Labelling Scheme (CLS)	IT Security Label	Finnish Cybersecurity Label
スキームオーナー	Cybersecurity Certification Centre (CCC)	Federal Office for Information Security (BSI)	Finnish Transport and Communications Agency (TRAFICOM)
ラベルの取り消しに関する規定	以下の場合、CCCはCLSラベルを取り消す権利を有する。 a. Testing Laboratory(TL)または開発者が、CLS出版物の条件やCCCと書面で合意したその他の条件に違反した場合 b. 開発者が、CLSラベルを損なう可能性があると CCCが判断する、既知または発見された脆弱性の開示を怠った場合 c. 開発者が、CCCから与えられた猶予期間中に、CCCが満足するような是正措置をとらなかった場合 d. 開発者が、CLSラベル、CLSステータス、またはCCCやCLSに関連する独自の名称やマークを悪用した場合 e. 開発者が、試験のアスペクトやCLSに基づくラベリングの効果について、虚偽の陳述を行った場合 f. CCCが、TLが公正かつ公平な試験を実施する能力を損なうような対立関係にあったと判断した場合 g. ラベルが貼付された機器が、ラベルが付与されたときの条件を満たさなくなったか、最初にラベルが貼付された後にCCCが導入したラベルの変更条件を満たさなくなった場合 h. 開発者がCCCに提出した成果物において虚偽の陳述または申告を行ったことがCCCにより発覚した場合	製造者の宣言や製造者の法的義務に違反した場合、情報が不正確または不完全であった場合、その他法的要件やBSIの要件を満たしていない場合、ラベルが取り消されることがある。この場合、セキュリティ上のやむを得ない理由により早急な措置が必要とされない限り、製造者には聴聞会で回答するための適切な猶予期間が与えられる。	TRAFICOMは、ラベルを申請した組織がラベルの使用に関する義務を履行しない場合、当該組織によるラベルの使用を禁止することができる。その場合、TRAFICOMはウェブサイト(www.tietoturvamerkki.fi)から当該製品に関する情報を削除し、必要に応じて別途一般に通知する。

【その他の参考事例】英国のPSTI法では、関連する義務（PSTI法で定められている製品セキュリティに関するメーカ、認定代理人、輸入業者、販売代理店の義務）を遵守しなかったと、蓋然性の均衡上、国務長官が納得した場合、国務長官はその者に罰則通知を与えることができる。

Cybersecurity Labelling Scheme (CLS) Publication No. 1
https://www.csa.gov.sg/docs/default-source/our-programmes/certification-and-labelling-scheme/cls/publications/pub-cls-pub-1-overview-of-cls-v12.pdf?sfvrsn=b559ba25_0
BSI Process Description forthe Issuance of IT Security Labels
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/IT-Sicherheitskennzeichen/Process_Description_ITSecurityLabel.pdf?__blob=publicationFile&v=4
TRAFICOM Terms of Use
https://tietoturvamerkki.fi/sites/default/files/media/file/Terms%20of%20Use%20%E2%80%93%20Cybersecurity%20Label%20for%20IoT%20consumer%20devices.pdf
Product Security and Telecommunications Infrastructure Act 2022 https://www.legislation.gov.uk/ukpga/2022/46/contents/enacted

1. これまでの検討会でのご指摘事項
2. 発展JISEC認証スキーム体制
3. 本制度における☆1の位置づけ（要求レベル）
4. 適合性評価済製品におけるセキュリティ事案への対応
    - 4-1. 法的な論点整理
    - 4-2. リスクに対応するための資源の確保策
    - 4-3. 評価済み製品の有効期限、サーベイランス、取り消し
5. IoT製品ベンダーの能動的な制度活用を促す仕掛け
    - **5-1. 調達要件との連携、消費者に対する需要喚起策**
    - 5-2. 諸外国の適合性評価制度との国際連携
    - 5-3. IoT製品ベンダーや認証機関等に対する支援策
6. 今年度の検討方針

各種調達要件との連携

第３・４回のご指摘事項	• 制度の継続的維持のためには、開発・認証・購入のサイクルを回す必要がある。制度が利用されないと、予算を多く割かないと維持できない制度になってしまう。
中間とりまとめの記載事項	• 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。

調達要件については、強制力の強さや調達主体によって、様々な施策案が考えられる。政府、重要インフラ、業界、地方公共団体の各調達主体に対し、それぞれの施策の実現可能性や有効性を精査し、取組を行うことが求められる。

施策分類	施策案	強制力	関連法律・文書
政府	• 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に、適合性評価を受けた製品の調達について記載する。 • 政府機関等の対策基準策定のためのガイドラインに、適合性評価を受けた製品の調達について記載する。 • IT製品の調達におけるセキュリティ要件リストに現在含まれていないIoT製品を加え、セキュリティ要件に適合性評価について加える。 • NISCによるIT調達の助言時に、適合性評価を受けた製品の調達を推奨する。助言の対象となる機器を拡張する。	強 ↕ 弱	【法律】 • サイバーセキュリティ基本法 【文書】 • 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 • 政府機関等の対策基準策定のためのガイドライン • 統一基準適用個別マニュアル群 • IT製品の調達におけるセキュリティ要件リスト • IT製品の調達におけるセキュリティ要件リスト活用ガイドブック • IT調達に係る国等の物品等又は役務の調達方針及び調達手続に関する申合せ
重要インフラ	• 事業法に基づき参照される規格等(例：電気事業法に基づく電力制御システム/スマートメーターシステムセキュリティガイドライン)に記載する。 • 経済安全保障推進法における基幹インフラ分野における事前審査制度と連携する。 • 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、適合性評価を受けた製品の調達について記載する。 • 重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針に、適合性評価を受けた製品の調達について記載する。	強 ↕ 弱	【法律】 • サイバーセキュリティ基本法 • 各重要インフラにおける事業法 • 経済安全保障推進法における基幹インフラ分野における事前審査基準 【文書】 • 重要インフラのサイバーセキュリティに係る行動計画 • 重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針 • 「策定指針」で定めた手順等を具体的に示すための「手引書」及び個別の対処方法、留意点等を示す「ガイダンス」
業界団体	• 所管官庁と連携し、各業界団体等が定める「業界標準」及び「ガイドライン」に、適合性評価を受けた製品の調達について記載するよう働きかける。	-	【文書】 • 各業界団体等が定める「業界標準」及び「ガイドライン」
地方公共団体	• 地方公共団体における情報セキュリティポリシーに関するガイドラインに、適合性評価を受けた製品の調達について記載する。	-	【文書】 • 地方公共団体における情報セキュリティポリシーに関するガイドライン

【参考】サイバーセキュリティ基本法

- サイバーセキュリティ基本法では、国の行政機関等におけるサイバーセキュリティの確保や重要社会基盤事業者等におけるサイバーセキュリティの確保の促進について規定されている。

（国の行政機関等におけるサイバーセキュリティの確保）

第十三条　国は、国の行政機関、独立行政法人（独立行政法人通則法（平成十一年法律第百三号）第二条第一項に規定する独立行政法人をいう。以下同じ。）及び特殊法人（法律により直接に設立された法人又は特別の法律により特別の設立行為をもって設立された法人であって、総務省設置法（平成十一年法律第九十一号）第四条第一項第八号の規定の適用を受けるものをいう。以下同じ。）等におけるサイバーセキュリティに関し、国の行政機関、独立行政法人及び指定法人（特殊法人及び認可法人（特別の法律により設立され、かつ、その設立等に関し行政官庁の認可を要する法人をいう。第三十三条第一項において同じ。）のうち、当該法人におけるサイバーセキュリティが確保されない場合に生ずる国民生活又は経済活動への影響を勘案して、国が当該法人におけるサイバーセキュリティの確保のために講ずる施策の一層の充実を図る必要があるものとしてサイバーセキュリティ戦略本部が指定するものをいう。以下同じ。）におけるサイバーセキュリティに関する統一的な基準の策定、国の行政機関における情報システムの共同化、情報通信ネットワーク又は電磁的記録媒体を通じた国の行政機関、独立行政法人又は指定法人の情報システムに対する不正な活動の監視及び分析、国の行政機関、独立行政法人及び指定法人におけるサイバーセキュリティに関する演習及び訓練並びに国内外の関係機関との連携及び連絡調整によるサイバーセキュリティに対する脅威への対応、国の行政機関、独立行政法人及び特殊法人等の間におけるサイバーセキュリティに関する情報の共有その他の必要な施策を講ずるものとする。

（重要社会基盤事業者等におけるサイバーセキュリティの確保の促進）

第十四条　国は、重要社会基盤事業者等におけるサイバーセキュリティに関し、基準の策定、演習及び訓練、情報の共有その他の自主的な取組の促進その他の必要な施策を講ずるものとする。

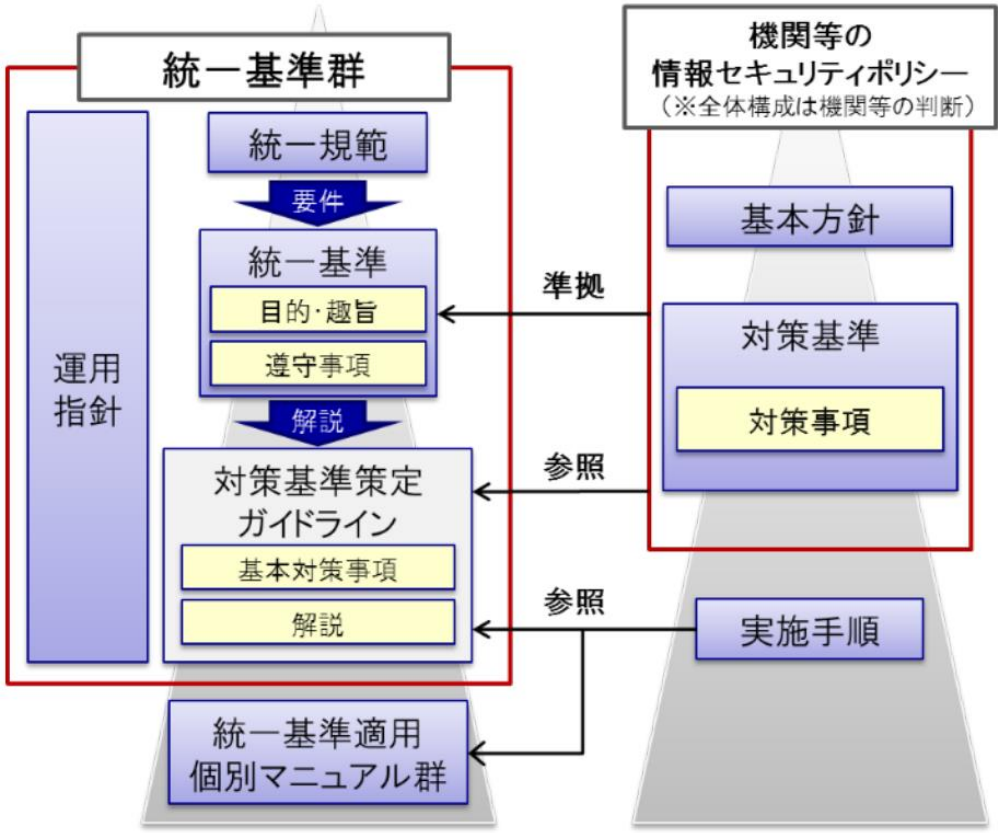
出所）サイバーセキュリティ基本法 https://elaws.e-gov.go.jp/document?lawid=426AC1000000104

【参考】政府や重要インフラにおけるサイバーセキュリティ対策の枠組み

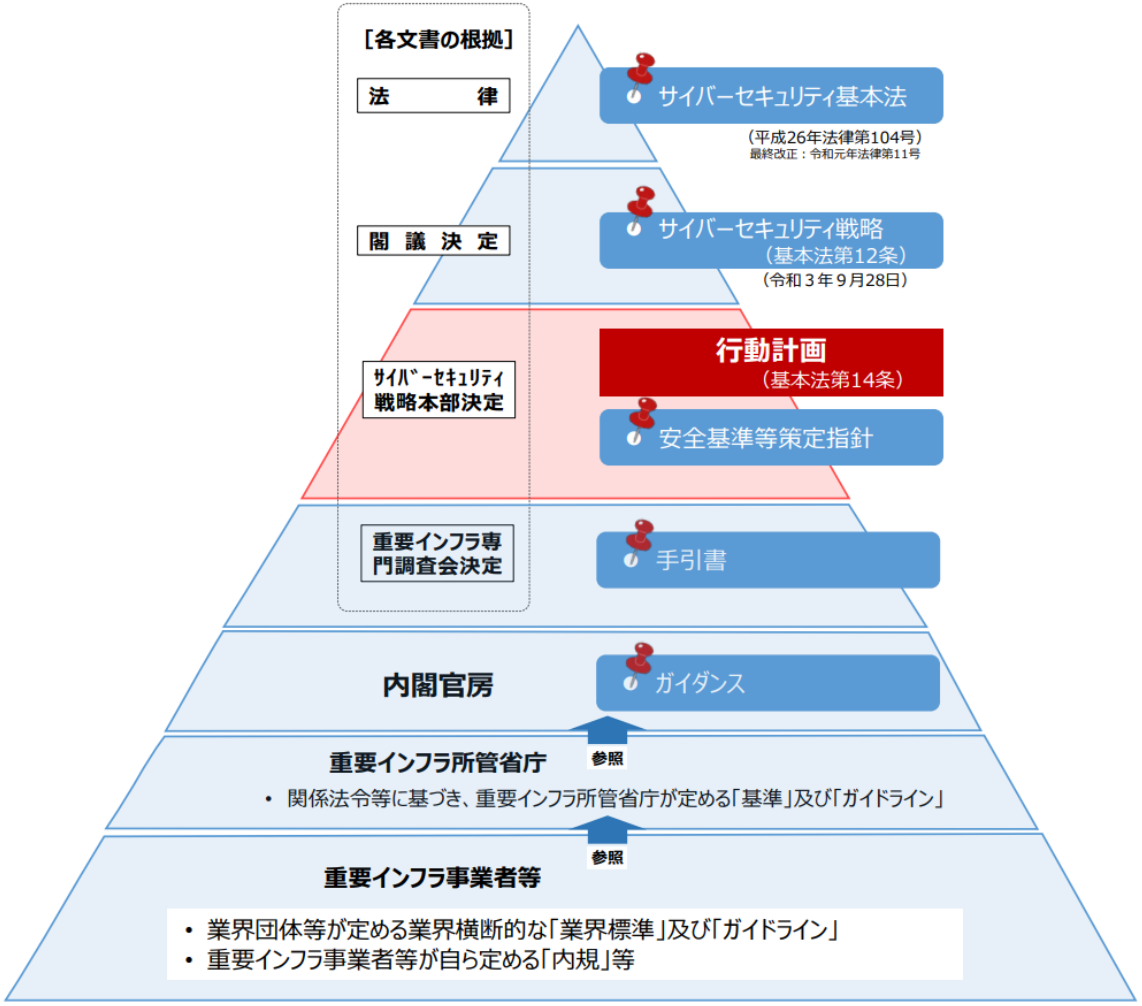
- サイバーセキュリティ基本法に基づき、政府調達に関しては「政府機関等のサイバーセキュリティ対策のための統一基準群」、重要インフラ調達に関しては「重要インフラ分野における情報セキュリティ確保に係る安全基準等」が策定されている。

政府におけるサイバーセキュリティ対策の枠組み

サイバーセキュリティ基本法
「サイバーセキュリティに関する統一的な基準の策定」



重要インフラにおけるサイバーセキュリティ対策の枠組み



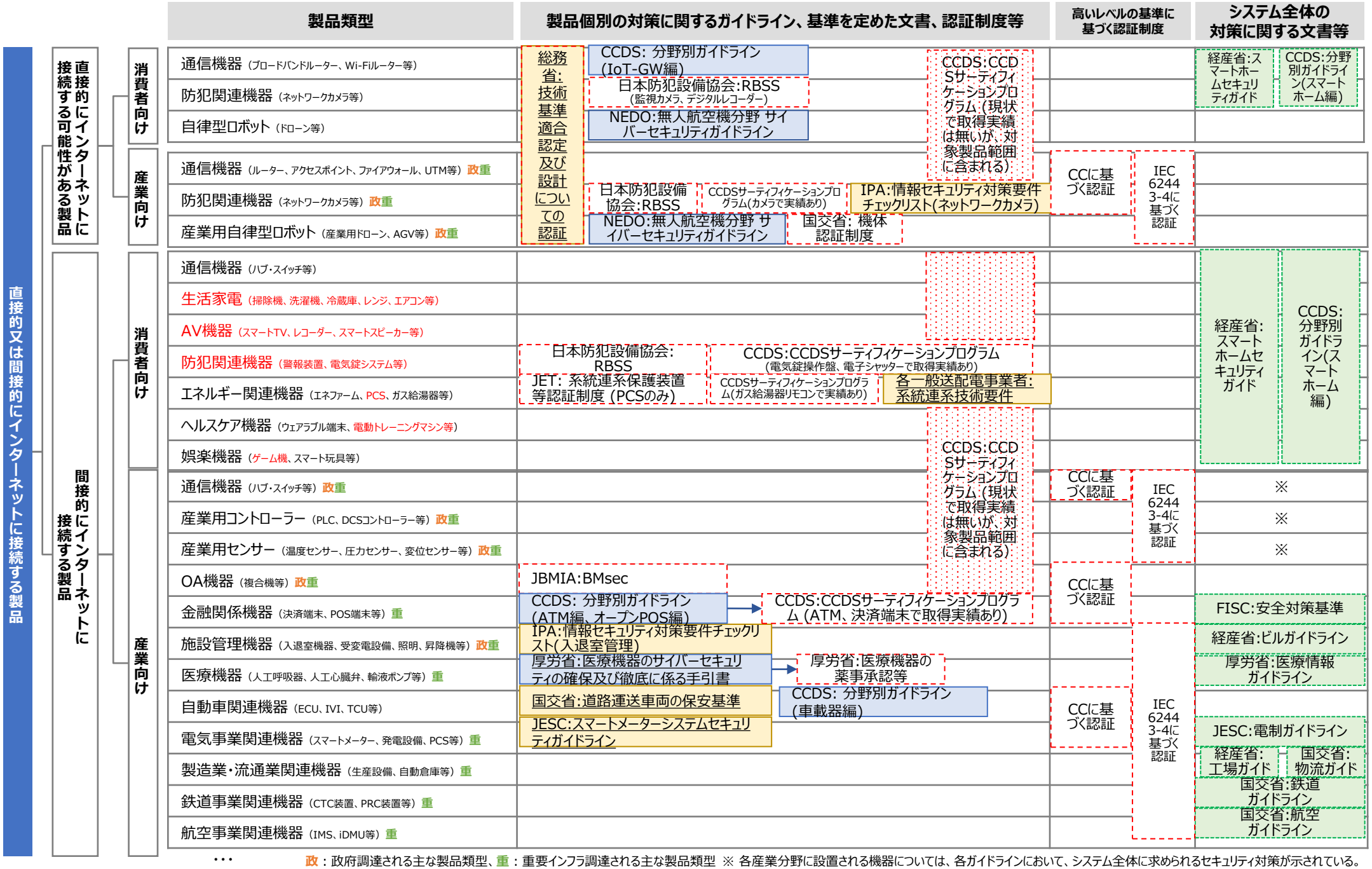
出所）NISC、政府機関等の対策基準策定のためのガイドライン https://www.nisc.go.jp/pdf/policy/general/guider3_2.pdf
サイバーセキュリティ戦略本部、重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針 第5版 https://www.nisc.go.jp/pdf/policy/infra/shishin5rev.pdf

【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

【参考】製品に関する類型・既存の文書、認証制度等（更新版）

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。



政：政府調達される主な製品類型、重：重要インフラ調達される主な製品類型 ※ 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。

IoT製品ベンダー等及びIoT製品調達企業への本制度の周知

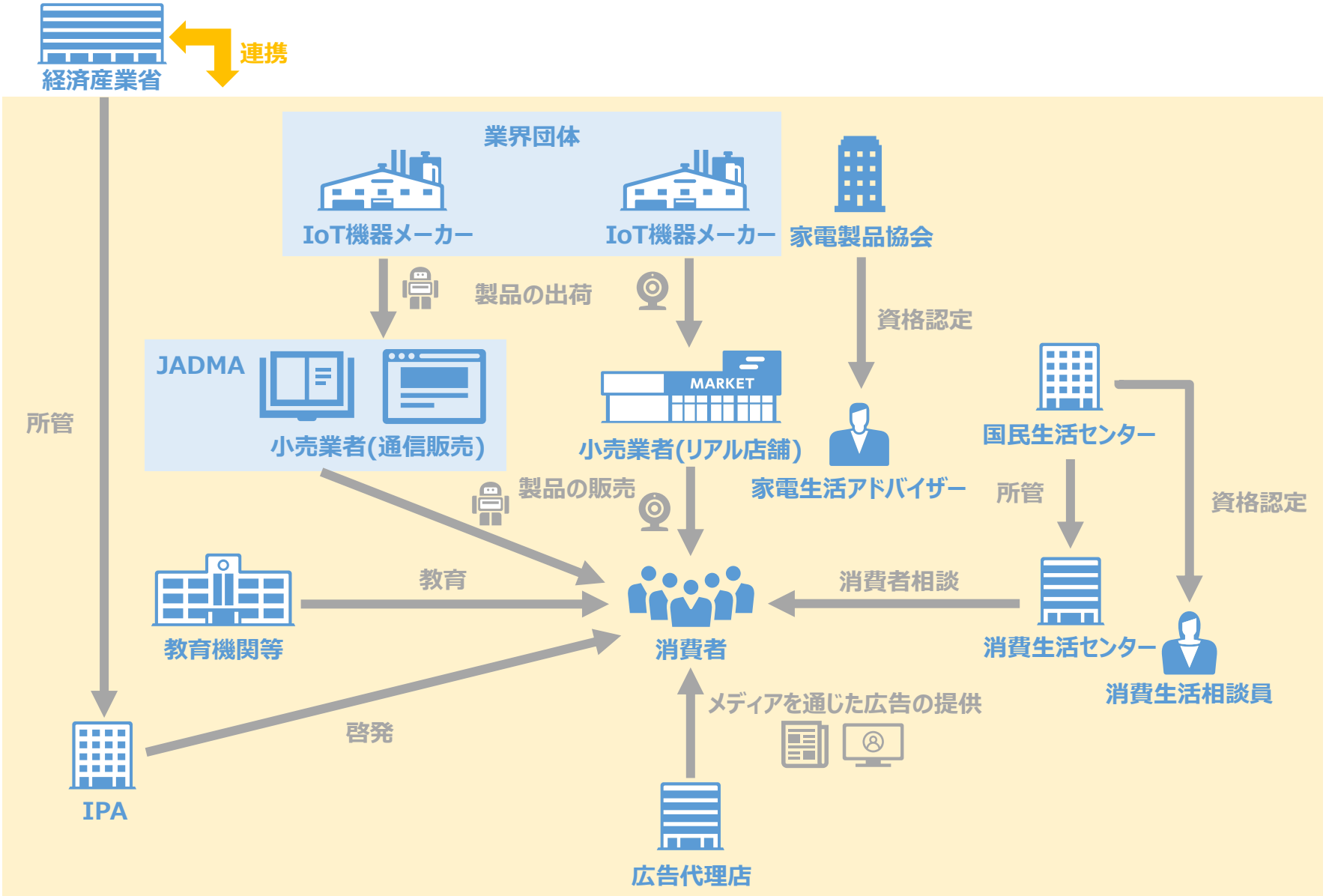
第３・４回のご指摘事項	• 本制度をプロモーションするうえで、2025年の大阪万博が期待できると考えている。開催までに制度の構築が間に合えば良い。 • セキュリティの知見が不足するベンダーも多く存在するため、本制度に関する教育プログラムやセミナーを開催することを検討いただきたい。

• IoT製品ベンダー等やIoT製品調達企業による認知度を高めるため、様々な団体等と連携し、本制度の周知を行う。

連携先	ターゲット	施策案
SC3	• IoT製品ベンダー等 • IoT製品調達企業	• 会員向け周知媒体を通じた周知 • 各団体・企業が実施しているIoT・セキュリティ関連の取組に合わせたセミナー・研修会での案内
IPA		• メールマガジン、SNSによる周知 • IoT・セキュリティ関連セミナー・研修会での案内
デジタル庁		• デジタル臨時行政調査会作業部会テクノロジーベースの規制改革推進委員会「テクノロジーマップ」への掲載
業界団体		• 各業界団体の周知媒体、関連会合における案内 • 各業界団体が実施しているIoT・セキュリティ関連の取組に合わせたセミナー・研修会での案内
ISAC		• 各ISACを通じた加盟企業への周知
展示会		• サイバーセキュリティ課からの講演での案内
各種ニュースサイト		• ニュースサイトへの案内記事掲載
JNSA	• IoT製品ベンダー等	• HP、メールマガジンを通じた会員への周知
主要IoT製品ベンダー		• 直接の案内・説明を通じた、積極的なラベル取得の働きかけ • 賛同企業の募集、本制度の最終とりまとめへの企業名掲載

消費者に対する需要喚起に関わる主なステークホルダー

- 消費者に対して、制度の概要を伝えるのみならず、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も含めて、ステークホルダーと連携しながら伝えることで、適合性評価を受けた製品の需要を喚起することが求められる。



消費者に対する需要喚起策（案）

第３・４回のご指摘事項	• 普及活動について、家電量販店や通販サイト等の販売者に対する広報も必要となる。本制度にうまく誘導できるような広報活動が必要となる。 • 本制度は社会インフラの一部となるので、消費者も社会的コストを担っていく一員としての理解や知識を持つために行政等からの教育や啓発が必要である。 • 制度の継続的維持のためには、開発・認証・購入のサイクルを回す必要がある。制度が利用されないと、予算を多く割かないと維持できない制度になってしまう。
中間とりまとめの記載事項	• 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。

消費者に対する需要関係策については、消費者がラベルが付与された製品を認知し、関心を持ち、実際に購入する行動につながるまで、消費者の購買行動のフェーズに応じた需要喚起策を、コストと効果を踏まえ、経済産業省及びIPAにおいて関係団体との連携のもと実施する。

フェーズ	需要喚起策（案）	協力機関（例）	コスト
認知・関心	ポスター制作・掲示	IPA、小売業者、消費生活センター、教育機関	小
	普及促進資料作成・配布	IPA、JADMA、小売業者、国民生活センター、消費生活センター、教育機関	小
	SNS発信	経済産業省 広報室	小
	ネット広告	広告代理店	小
	交通広告・新聞広告	広告代理店	中
	インフルエンサー・IPコンテンツコラボレーション	広告代理店	中
	動画制作・テレビCM	広告代理店	中
	促進協議会の組成	IoT機器業界団体、JADMA、国民生活センター、教育機関	大
欲求・行動	HP制作	経済産業省 広報室	小
	大手ECサイト等における検索条件への追加	JADMA、大手ECサイト	中
	消費生活相談員・家電生活アドバイザー向け説明資料の配布	国民生活センター、消費生活センター、JADMA、家電量販店	中
	家電量販店、大手ECサイト等と連携したプロモーション	家電量販店、大手ECサイト	中
	IoT機器メーカー・業界団体と連携したプロモーション	IoT機器メーカー・業界団体	中

1. これまでの検討会でのご指摘事項
2. 発展JISEC認証スキーム体制
3. 本制度における☆1の位置づけ（要求レベル）
4. 適合性評価済製品におけるセキュリティ事案への対応
    - 4-1. 法的な論点整理
    - 4-2. リスクに対応するための資源の確保策
    - 4-3. 評価済み製品の有効期限、サーベイランス、取り消し
5. IoT製品ベンダーの能動的な制度活用を促す仕掛け
    - 5-1. 調達要件との連携、消費者に対する需要喚起策
    - **5-2. 諸外国の適合性評価制度との国際連携**
    - 5-3. IoT製品ベンダーや認証機関等に対する支援策
6. 今年度の検討方針

諸外国の適合性評価制度との国際連携のあり方

第３・４回のご指摘事項	• ISO/IEC 27404においても相互承認の重要性が挙げられている。日本の制度が国際的にガラパゴス化しないようにしたほうが良い。 • 国際的な相互承認が理想であるが、困難であれば、制度間の要件の差分を確認して部分的に評価するといった仕組みも考えていければ良い。 • 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。
中間とりまとめの記載事項	• 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。

・☆１開始時に導入されている、シンガポールCLS（の＊１）と英PSTI法を内包するべく基準を設計する。
・☆１開始時に制度設計途中の見込みである欧CRA及び米Cyber Trust Mark（仮）については、差分を確認し、国内基準（☆１更新時又は来年度以降に検討をする☆２以上）で包含又は 追加対応を要する差分の公表等で対応する。
・国内制度設計と並行して、☆１相互承認に向けて諸外国と調整を行う。
・同時に、国際標準化に向けてISO/IEC 27404等の動きと連携をする。

国・地域					
制度名	発展JISEC制度	Cybersecurity Labelling Scheme (CLS)	Product Security and Telecommunication Infrastructure Act (PSTI法)	U.S. Cyber Trust Mark（仮）	Cyber Resilience Act CRA)
開始時期	☆1：2024年度下期開始予定 ☆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（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中（ただし、一部の記載については、総務省技適の要件、CCDSの要件の参照のほか、事務局にて記載内容を検討）	• ＊：ETSI EN 303 645の基準の一部※1 • ＊＊：＊の基準に加え、ETSI EN 303 645の基準の一部※2 • ＊＊＊及び＊＊＊＊：＊＊の基準に加え、IMDA「IoT Cyber Security Guide」の9つのライフサイクル基準	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	• 基本的な対策基準のほか、SBOM等に基づく脆弱性管理、脆弱性報告等、広範な基準が求められる予定 • 法案の内容について（欧州委員会・議会・理事会間で）政治合意がなされた後、法案に伴う基準がETSI EN 303 645等を参照して設定される予定
評価方法	☆1：自己適合宣言 ☆2：自己適合宣言（ただし、一定のスキル要件を満たした評価者による評価を求める） ☆3以上：第三者認証を求める方針	• ＊及び＊＊：自己適合宣言 • ＊＊＊及び＊＊＊＊：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

1. これまでの検討会でのご指摘事項
2. 発展JISEC認証スキーム体制
3. 本制度における☆1の位置づけ（要求レベル）
4. 適合性評価済製品におけるセキュリティ事案への対応
    - 4-1. 法的な論点整理
    - 4-2. リスクに対応するための資源の確保策
    - 4-3. 評価済み製品の有効期限、サーベイランス、取り消し
5. IoT製品ベンダーの能動的な制度活用を促す仕掛け
    - 5-1. 調達要件との連携、消費者に対する需要喚起策
    - 5-2. 諸外国の適合性評価制度との国際連携
    - **5-3. IoT製品ベンダーや認証機関等に対する支援策**
6. 今年度の検討方針

IoT製品ベンダーや認証機関等に対する支援策

第３・４回のご指摘事項	• セキュリティの知見が不足するベンダーも多く存在するため、本制度に関する教育プログラムやセミナーを開催することを検討いただきたい。 • コストがかかる取組であるので、インセンティブも検討していただけると良い。補助金など、ベンダーが取り組みやすくなる仕組みがあると良い。 • 自己適合宣言の運用モデルやベストプラクティスが提示されることで、ベンダーとしては対応しやすくなる。 • ISO/IEC 17025のレベルで全ての評価機関の適格性を担保することは難しいのではないか。評価を行う人材の育成も意識することが重要である。 • 適合性評価に用いるツールをOSSとして無償提供することは制度にとってプラスに働く。既存の取組を参照しつつ、本制度を検討していくと良い。
中間とりまとめの記載事項	• 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。

●IoT製品ベンダーに対する支援

- IoT製品ベンダーにヒアリングを行い、具体的な支援策を検討する。
- IoT製品ベンダーに対する費用補助は、シンガポールの事例を参考に、制度開始時点で適合性評価にかかる申請を無償とするなど、制度の普及を図る。
- IoT製品ベンダーに対しては、制度に関する教育や、自己適合宣言時に参考となるドキュメント（ベストプラクティス、評価ガイド）を提供する。将来的には、自動化ツールの提供等を検討する。

●評価機関・検証事業者に対する支援

- 評価機関については、ISO/IEC 17025の認定取得を促進する。
- ☆１の自己適合宣言については、製品の評価が可能な検証事業者として情報セキュリティサービス審査登録制度（機器検証サービス）への登録を促す。
- 評価機関・検証事業者の評価者に対し、適合基準や評価手順に関する教育を実施し、評価者の人材育成を継続的に実施する。

諸外国制度におけるIoT製品ベンダーへの支援に関する取組

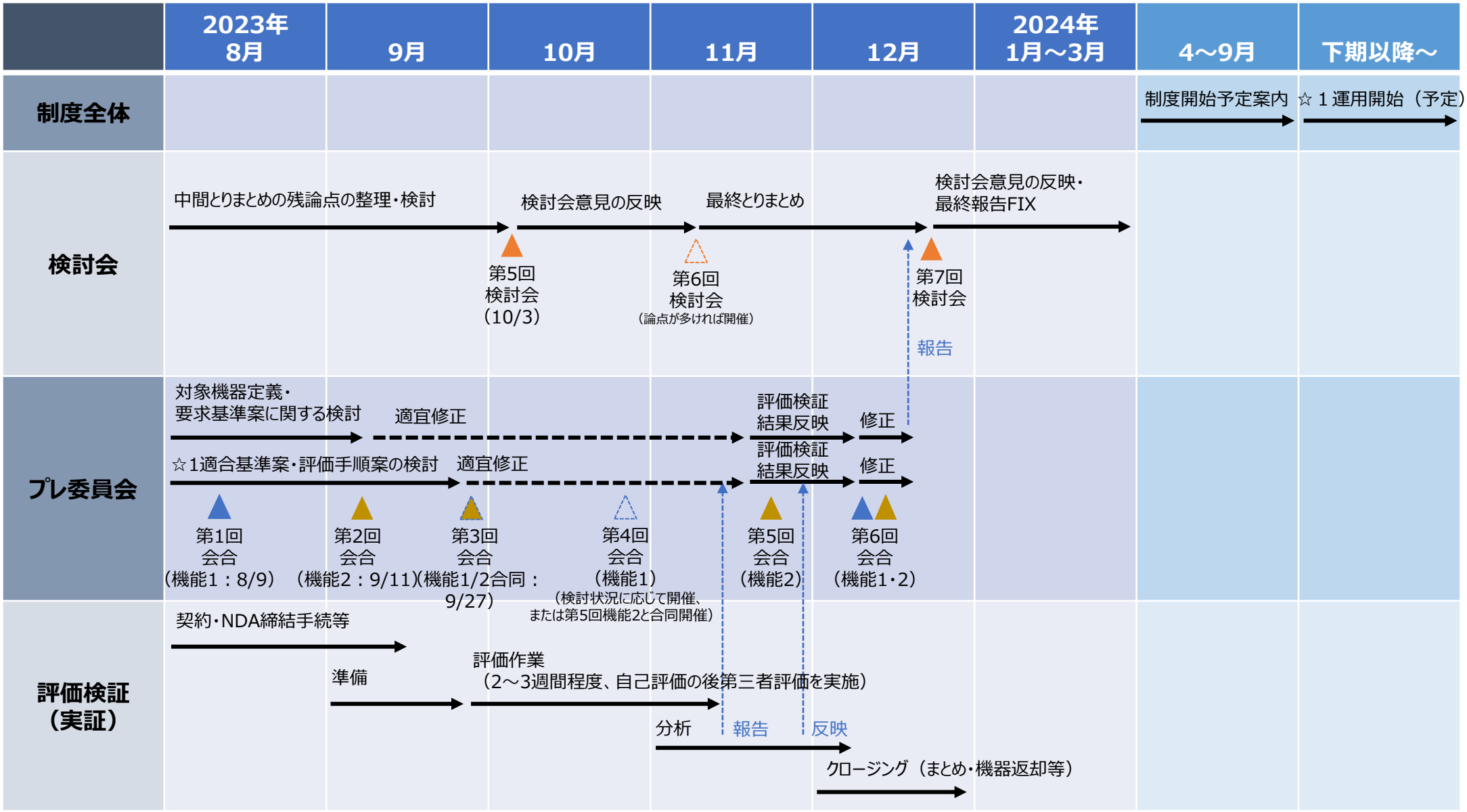
●IT製品ベンダーに対する支援（例）

＜シンガポール＞
シンガポールが実施しているセキュリティラベリング制度であるCybersecurity Labelling Scheme では、制度開始後1年間、適合性評価にかかる申請料を無償とすることで制度活用促進を図った。この結果、2023年2月時点で230製品以上にラベルが付与されている。

1. これまでの検討会でのご指摘事項
2. 発展JISEC認証スキーム体制
3. 本制度における☆1の位置づけ（要求レベル）
4. 適合性評価済製品におけるセキュリティ事案への対応
    - 4-1. 法的な論点整理
    - 4-2. リスクに対応するための資源の確保策
    - 4-3. 評価済み製品の有効期限、サーベイランス、取り消し
5. IoT製品ベンダーの能動的な制度活用を促す仕掛け
    - 5-1. 調達要件との連携、消費者に対する需要喚起策
    - 5-2. 諸外国の適合性評価制度との国際連携
    - 5-3. IoT製品ベンダーや認証機関等に対する支援策

6. 今年度の検討方針

今年度のスケジュール


2023年 8月
9月
10月
11月
12月
2024年 1月～3月
4～9月
下期以降～
制度全体
制度開始予定案内
☆１運用開始（予定）
検討会
中間とりまとめの残論点の整理・検討
検討会意見の反映
最終とりまとめ
検討会意見の反映・最終報告FIX
第5回 検討会 (10/3)
第6回 検討会 (論点が多ければ開催)
第7回 検討会
報告
プレ委員会
対象機器定義・要求基準案に関する検討
適宜修正
評価検証結果反映
修正
☆1適合基準案・評価手順案の検討
適宜修正
評価検証結果反映
修正
第1回 会合 (機能1：8/9)
第2回 会合 (機能2：9/11)
第3回 会合 (機能1/2合同：9/27)
第4回 会合 (機能1) (検討状況に応じて開催、または第5回機能2と合同開催)
第5回 会合 (機能2)
第6回 会合 (機能1・2)
評価検証（実証）
契約・NDA締結手続等
準備
評価作業 (2～3週間程度、自己評価の後第三者評価を実施)
分析
報告
反映
クロージング（まとめ・機器返却等）

「議論が必要な事項」の検討状況

- 中間とりまとめで示した「議論が必要な事項」は、第４回・第５回検討会で検討を進めている。
- 政府基本方針の策定や中間とりまとめに記載していなかった論点に関しては、これまでの議論を踏まえ、第６回／第７回検討会で検討を行う予定である。

議論が必要な事項			検討状況（どの検討会で検討した/するか）
中間とりまとめで示した論点	政府の関与や検討体制のあり方	認証機関との連携	検討済（第４回）
		評価基準等を検討する委員会の構築	
		政府基本方針の策定	今後検討予定（第６回／第７回）
	IoT製品ベンダーの能動的な制度活用を促す仕掛け	各種調達要件との連携、消費者に対する需要喚起策	検討進行中（第５回）
		諸外国の適合性評価制度との国際連携	
		IoT 製品ベンダーや認証機関等に対する支援策	
	適合性評価済製品におけるセキュリティ事案への対応	法的な論点整理	
		リスクに対応するための資源の確保策	
		評価済製品のサーベイランス、取り消し	
中間とりまとめに記載していなかった論点	制度の果たすべき役割や位置づけ	本制度を通じて各ステークホルダーがどのような利益を享受できるか	
	適合性評価制度の効率化に向けた検討	認証・管理業務の自動化	今後検討予定（第６回／第７回）
		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の開発・提供	
		☆2以上における脆弱性管理の自動化	
	今後の制度設計の方針	☆２以上製品の制度設計の優先順位	