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 12月 12日

第５回検討会のご指摘事項（1/2）

カテゴリ	主なご指摘事項
対象製品について	• 制御系の末端機器も技術的に進化している。単純に対象から除外すべきではなく、分類の詳細化が必要である。 • 工場内の設備であるからといって、セキュリティの重要性を軽視すべきではない。
各レベルの位置づけについて	• ☆1のセキュリティ脅威に関連する部分で、個人情報に言及すべきである。 • ☆1で、ホームユースやプライベートユースに限るべきではない。☆1はIoT製品に最低限適用すべき基準であり、☆2は製品類型ごとに存在する特殊なセキュリティ要件に対応するために満たすべき基準と考える。
責任分界について	• 自己適合宣言については、負うべき責任の範囲の検討が今後必要である。また、第三者評価についても、責任の範囲や保証内容について検討が必要である。責任の観点をコストとのバランスで考慮することが重要である。 • 責任の量は、自己適合宣言と第三者認証の場合で変わらず、誰が責任を負うかが変わる。取得難易度を調整するためには、責任の量を変更する必要がある。 • 日本国の競争力を培うためには責任を負う主体が制度を構築する必要がある。メーカからすると、責任やファンドについてどのように対処するかという問題が解決されない限り、制度への参加が難しい。段階的に進める必要があると考えているが、少なくともIPAにおいては、制度運営者の監督、製品に関する評価、そして設計レベルの評価等について責任を負う必要があり、何らかの責任を果たさない限り、制度自体が活用されない可能性が高い。 • 既存の保険や情報セキュリティ早期警戒パートナーシップ制度だけでなく、より包括的なアプローチが必要である。保険数理と業規制の拘束を強く受ける保険だけでなく、より柔軟な制度設計が可能となる信託制度を活用し、社会的に校正して制度運用の資金供給に利用するなどの活用なども考慮し、より幅広い視野で検討することが望ましい。 • 責任の追及を容易にする制度設計も重要である。被害が発生した場合、集団訴訟のような手続きで被害者全体を救済できる制度も検討するべきである。 • 保険制度の活用について、前例がないことを理由に導入しないと結論付けることに疑念がある。CCDSのように、制度内で保険を適用し、運用している民間企業が存在するため、公的機関が同じように対応できないことに疑問を感じる。制度の普及を促進するためにも、セーフティネットとしての保険が必要であり、公的機関としてその負担を引き受けるべきだと考える。現在の状況を改善し、制度設計を進めるために、責任の所在を明確にしながら検討を進めていただきたい。 • 保険は、技術や制度では対応できない、想定外の事態に備えるためのものである。しかし、誰も責任を負わない状況で保険を導入すると、事故率を計算できない状態で保険が提供されることになりかねない。制度を構築する責任、検査を実施する責任など、責任の範囲を明確にしないと保険制度が機能しない。
適合性評価の要件・基準について	• 扱う個人情報を具体的に列挙することは、☆1の段階で要求するべきである。 • 制御系に接続される機器が☆1の要件を全て満たすことは、現在の技術では実現不可能である。欧州側も産業用機器とIoT製品を区別して考慮している。☆1の要件を求めるべき箇所は、インターネット経由でデータを送受信する箇所に限定されるべきである。 • データ保護の対策実装可能性は考慮すべきである。一方で、データの汚損が発生した場合、ロボットが正常に停止できるかなど、安全性が確保されているかが鍵となる。 • 現在の製品とシステムを保護するためのガイドラインと、今後市場に出る製品に対する要件を混同しないようにするべきである。 • セーフティ機能に関する要件を☆の取得条件に含めることも考慮すべきである。ただし、☆1及び☆2のどちらで要求するかの検討も必要である。 • IoT製品のセキュリティを製品単体で担保するか、システムとして担保するかは、開発ベンダーの自由な裁量に委ねるべきである。また、サポートの提供方法は開発ベンダーが自由に決定できるようにするべきであり、その判断に資する基準を提供することが重要だと考える。 • 防御だけでなく、システムが侵害された場合の復旧力（レジリエンス）も考慮する必要がある。

第５回検討会のご指摘事項（2/2）

カテゴリ	主なご指摘事項
サーベイランスや有効期限について	• 自己適合宣言時に、サーベイランスにコストをかけることについて疑問を抱いている。サーベイランスを行うことでメーカに追加のコストがかかることは問題である。 • 責任の所在が明確でない制度でサーベイランスを進めるべきかどうかについて疑問が残る。 • 製品の寿命が長い場合、サーベイランスが適切だが、IoT製品など寿命の短い製品に対してサーベイランスを行うことは、コスト面で疑問視される。 • サーベイランスに関して、メーカとしては自己適合宣言を得るために必要な要素とも理解できる。サーベイランスによってランダムに検査され、違反があれば認証が取り消されるという抑止策が存在するため、不適切な自己検査は行えなくなる。 • 本制度案では有効期限がサポート期限と解釈される可能性がある。アップデートだけがサポートではない。サポート期間に関する要求もメーカに求める場合は、その内容も含めて要件に明示的に記載する必要がある。一方で、セキュリティは時間とともに弱化するものであるため、設定された要件を満たすことはその時点での証明であり、有効期限を設ける必要はないと考える。 • 有効期限について、メーカ側から見た有効期限と認識した。製品のリリース日を起点としている一方、ユーザの視点からは購入日が重要である。期限の設定ついては、複雑で、継続的な議論が必要だと考えている。
ラベルについて	• ファームウェアのアップデートがある場合、特に発売後に実施されるアップデートの判断方法について、今後議論したい。ラベルの表示やQRコードの遷移先による情報提供を通じて、前提条件（評価日、評価時のファームウェアなど）を確認できると良い。 • 有効期限の「ラベルへの表示」は、ラベルを交換しなければならない手間を考慮すると避けるべきである。情報へのアクセスがQRコードを介して行われる場合、小さな製品では本体への表示が難しいこともあるので、梱包箱や取扱説明書に情報を記載する方法も許容していただきたい。
調達者、消費者における活用について	• アップデートができない又はしないユーザも存在するため、そのような場合の対応についても検討が必要である。セキュリティアップデートの提供は、製造者としての責任と考える。一方で、セキュリティアップデートを適切に適用することも、ユーザとしての責務であることを強調すべきである。 • 認証取得製品の使用を強制するアプローチは違和感がある。認証を取得していない製品や、製品の認証レベルに基づいて、システム設計時に検討すべき要素を訴求する方法が良い。初めは認証を取得していない製品が多いため、調達要件を普及度に合わせることが重要である。 • ユーザの責任や普及啓発策、需要喚起策について、消費者のレベル（セキュリティに対する知識への有無）を分けて考える必要がある。また、製品の生活への影響度を考慮に入れるべきであり、セキュリティ対策について受動的な姿勢の消費者がいることを考慮すべきである。それぞれの区分けに基づいて、具体的な対策と費用を考えることが重要である。消費者のレベル分け、責任の範囲、費用、社会的な資金の流れを考慮しながら検討していただきたい。 • ユーザの責務について、ユーザを消費者及び法人で分けて考えるべきである。今回の☆1において主要なユーザが消費者であることを考えると、ユーザに過度な責務を負わせることは問題であると感じる。ただし、例えばユーザが設定で自動更新をオフにすることも可能な場合がある。そのような場合にユーザを免責にすることは、メーカとしては納得できない。
評価機関への支援について	• 日本国内の企業が国外の評価機関を使用している中で、この制度が普及するかどうか不透明である。責任問題は重要であるが、審査を簡素化し評価機関の持続可能性を確保する必要があると認識している。
他制度との連携について	• 情報セキュリティ早期警戒パートナーシップとの連携について、高いレベルでは早期対応につながると感じる。しかし、IoT製品を対象とした脆弱性の共有に関して、パッチが完成し、メーカの準備が整った段階で情報を提供する仕組みがまだ整備されていないように感じる。今後この箇所について具体的に考えていく必要がある。 • 情報セキュリティ早期警戒パートナーシップについて、国内に数が多い製品であれば情報共有が可能だが、国内に数台しかない製品では情報共有が難しい場合がある。制度の対象製品に関して、使用されているデバイスに関してはパートナーシップが効果的であると認識しているが、輸入の妨げにならない範囲で検討する必要があると感じる。 • 情報セキュリティ早期警戒パートナーシップだけに依存することは難しいと感じる。現実には様々な状況があるため、これらを考慮しつつ検討を進めたい。

本日の議題

【御報告事項】

- 適合性評価の実証状況について

【御議論いただきたい事項】

- **制度の必要性及び目的**
- 制度及び各レベルの位置づけ
- IoT製品ベンダーの能動的な制度活用を促す仕掛け
- 適合性評価済製品におけるセキュリティ事案への対応
- 最終とりまとめの骨子案

IoTセキュリティ適合性評価制度設立の目的

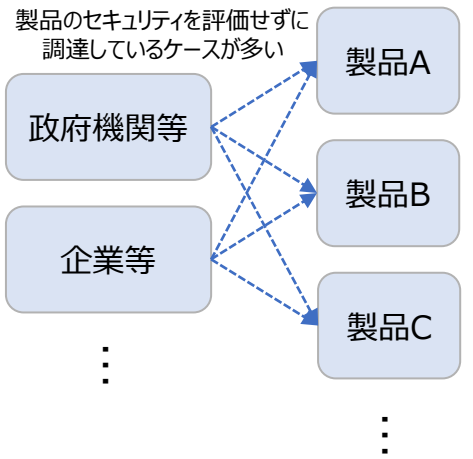
- 政府機関等・企業等のセキュリティ対策において、調達する製品や製品ベンダーのセキュリティも含めた広義なサプライチェーンリスク管理の取り組みが広がっている。しかしながら、**IoT製品の選定時や調達時に、そのセキュリティ機能や対策状況を自組織で確認（第二者評価）できているケースは少ない**のが現状である。そこで、第二者評価を代替する仕組みとして、**共通的な物差しでIoT製品のセキュリティを第三者が評価し、その結果に対して認証を付与する制度**が必要である。（目的①：**政府機関等・企業等のIoT製品調達ニーズへの対応**）
- 様々な機器がネットワークに接続されることで、十分なセキュリティ知識のない中小企業や一般消費者が意識しないまま、サイバーセキュリティリスクに晒されることとなり、情報漏えいやボット化による他者への攻撃に悪用されるなどの被害にあう可能性がある。**国民が安心してネットワークを使用したサービスを利用できるよう**、特にリスクの高いサービス分野において使用される**IoT機器の最低限のセキュリティ基準を整備**し、当該分野のIoT機器はその基準を満たしたもののみを流通させる必要がある。（目的②：**特定分野で使用されるIoT機器の最低限のセキュリティ確保**）

		課題	解決方法	制度普及のポイント
目的①	政府機関等・企業等のIoT製品調達ニーズへの対応	IoT製品の選定時や調達時に、そのセキュリティ機能や対策状況を自組織で確認（第二者評価）できているケースは少ない	共通的な物差しでIoT製品のセキュリティを第三者が評価し、その結果に対して認証を付与する制度を整備（→主に☆3、☆4の活用を想定）	政府機関等・企業等の**多くの調達者が**その認証が必要であると認知し、**選定・調達要件に入れる**
目的②	特定分野で使用されるIoT機器の最低限のセキュリティ確保	十分なセキュリティ知識のない中小企業や一般消費者が意識しないまま、サイバーセキュリティリスクに晒される	特にリスクの高いサービス分野において使用されるIoT機器の最低限のセキュリティ基準を整備（→☆1以上の活用を想定）	特定業界の主要な提供者が協力して認証・ラベル取得を行い、**取得済み製品の供給を実質的な業界標準にする**

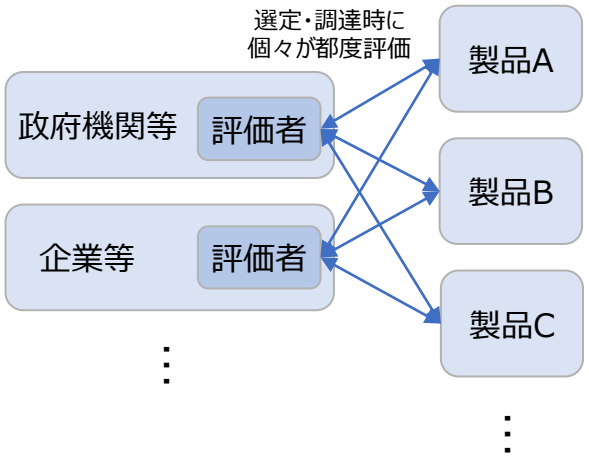
【目的①】政府機関等・企業等のIoT製品調達ニーズへの対応

- 政府機関等・企業等のセキュリティ対策において、**調達する製品や製品ベンダーのセキュリティも含めた広義なサプライチェーンリスク管理の取り組みが広がっている**。
- その際、IoT製品のセキュリティに関して、選定時や調達時に、その**セキュリティ機能や対策状況を自組織で確認すること（第二者評価）が本来必要であるが、そのための確認プロセスを整備できている政府機関等・企業等は少ないのが現状**である。一方、仮に政府機関等・企業等がそのプロセスを整備する場合、調達を行う各組織においてその**確認のための知識と工数が必要**となり、またIoT製品ベンダーは各者から**異なる要件に対して繰り返し回答・対応が求められ**、双方対応しきれなくなる。
- そこで、第二者評価を代替する仕組みとして、**共通的な物差しでIoT製品のセキュリティを第三者が評価し、その結果に対して認証を付与する制度**を整備する。政府機関等・企業等は**認証取得の確認をベースとして活用**しながら、必要な場合に追加的な確認を実施することで、各組織の求めるセキュリティ水準のIoT製品を選定・調達することが可能となる。
- **政府機関等の第二者評価の代替として公平・中立な認証を行うためには公的機関（IPA）が認証機関**となり、制度を維持・運営していくことが望ましい。

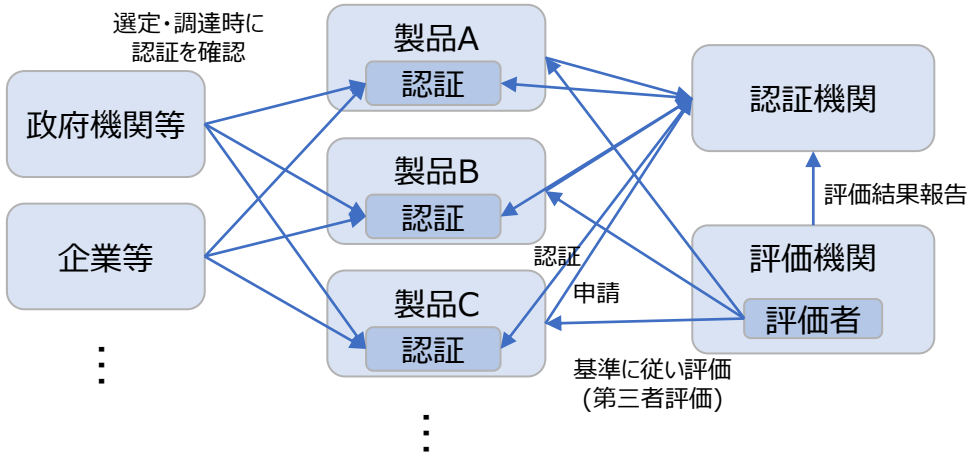
現状のイメージ



第二者評価のイメージ

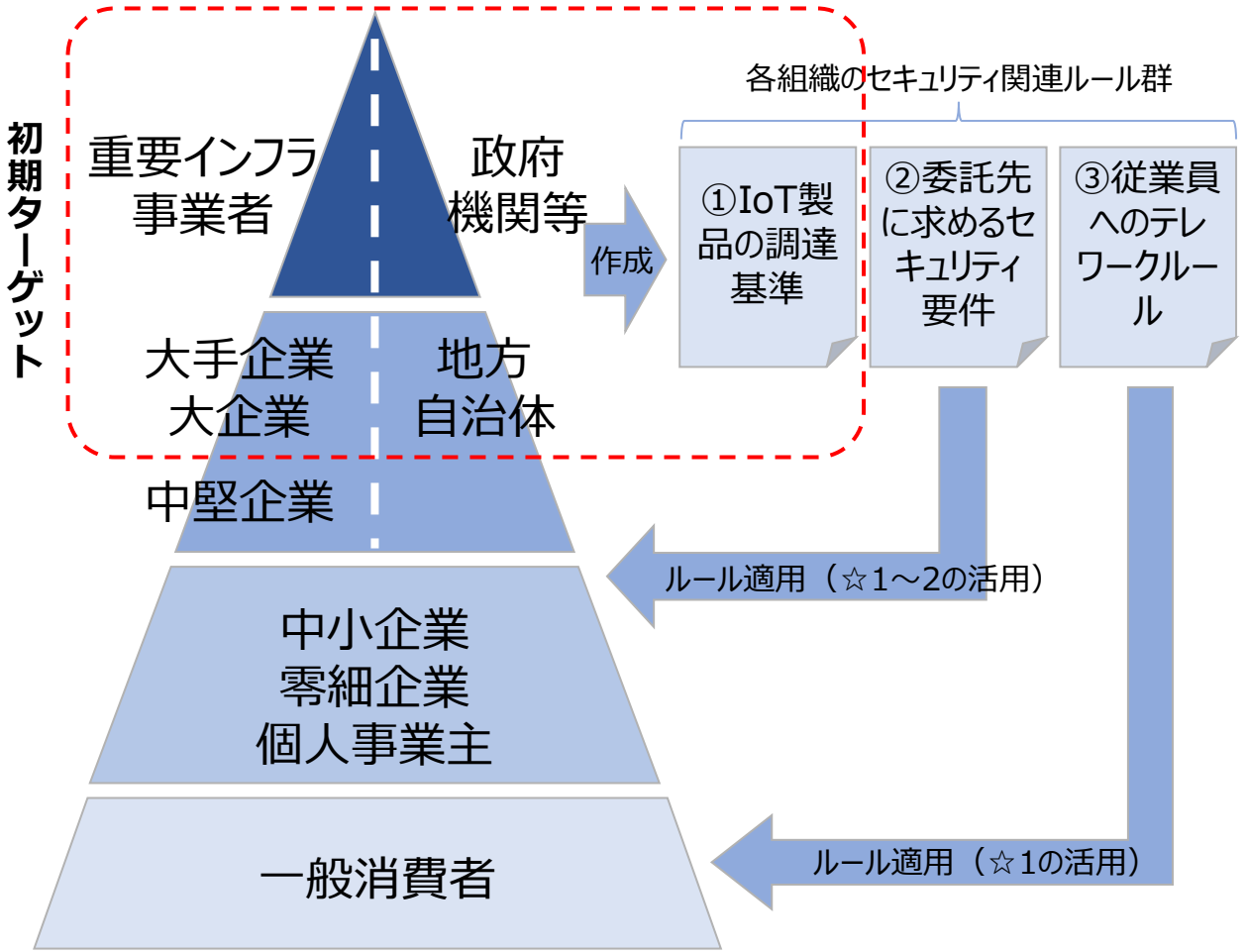


第三者評価・証明（＝認証）のイメージ



【目的①】展開戦略と初期ターゲット

- **政府機関等・地方自治体**および**重要インフラ事業者を含む大手企業・大企業を初期ターゲット**とし、セキュリティ関連ルール等に**①のIoT製品調達時の認証取得済み製品の選定を含める**ことをまずは目指す。
- **政府機関等・地方自治体には、強制力を持たせる**ようにNISC・デジ庁・総務省と必要性を合意し、各種基準に盛り込む。
- **重要インフラ事業者には、NISCと協議して行動計画に含め**たうえで、所管省庁・業界団体と連携して取り組みを促す。
- その他の民間企業への直接的な強制・推奨は難しいため、各業界団体や各業種のISAC等と連携して取り組みを促す。

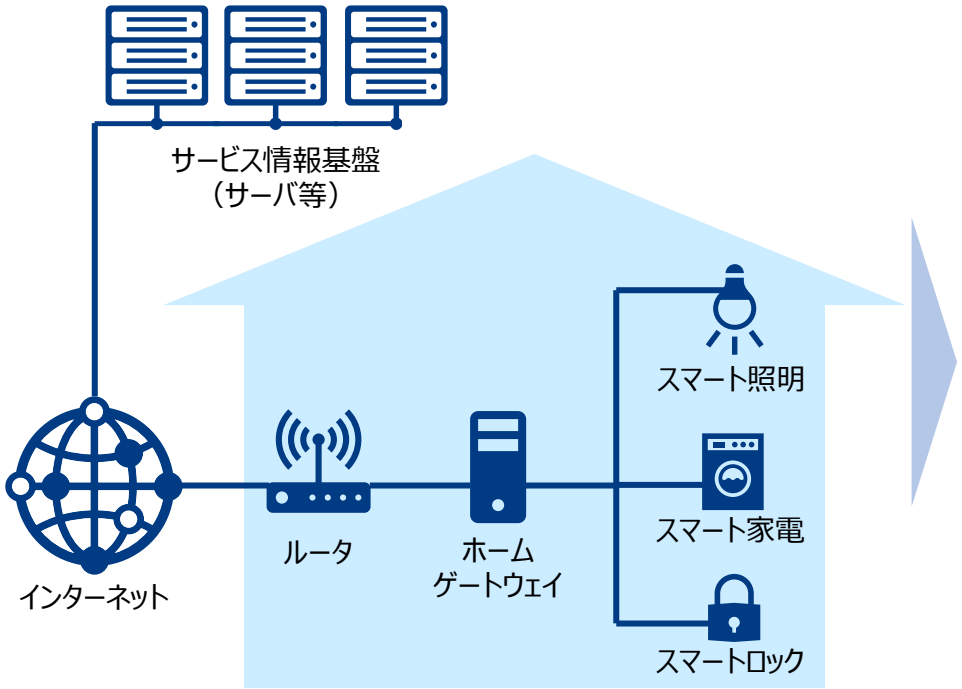


認証・ラベルの想定活用シーン	活用対象
① 自組織のセキュリティ対策のため、**IoT製品調達時に**、リスクに応じた段階の**ラベル取得済み製品を選定**する。	☆３～４の活用
② **委託先に対して、満たすべきセキュリティ要件のひとつ**として、認証・ラベル取得済みインターネット接続機器の使用を求める。	☆２の活用
③ 自組織の**従業員に対して、テレワークを実施する際に自宅で実施すべきセキュリティ対策のひとつ**として、認証・ラベル取得済みインターネット接続機器の使用を推奨する。	☆１の活用

【目的②】特定分野で使用されるIoT機器の最低限のセキュリティ確保

- IoT製品は、単体で比較・検討されて調達されるだけではなく、**特定分野のシステムに組み込まれて調達され、利用される**ケースもある。そのようなケースでは、最終調達者（ユーザー）がセキュリティを考慮したIoT製品を直接選定するのではなく、システムに組み込まれる段階で選定・調達される。（例）**スマートホーム、工場システム、ビルシステム**など
- **特定分野のシステムそれぞれの想定するユースケース、守るべき資産、脅威、リスクを定義**し、実施すべき対策のひとつとして、**組み込まれるIoT製品に求めるセキュリティ要件を定める**必要がある。当該要件で、IoT製品類型共通の☆1以上が必要となる場合に、**☆2以上の整備を本制度で検討**する。
- 各業界団体等では、特定分野のシステムのセキュリティに対して、**それぞれの用途や機能を考慮し、組み込むIoT製品のセキュリティ要件として必要な認証・ラベルを指定**する。その他のセキュリティ要件も含めたセキュリティガイドラインの作成や、システム全体としての認証制度等の整備を行い、**その準拠を業界標準とする**ことで、**当該特定分野のシステムにおいて、最低限のセキュリティが確保されたIoT機器のみが採用される**ことを目指す。

【特定分野のシステムのイメージ（スマートホームの例）】



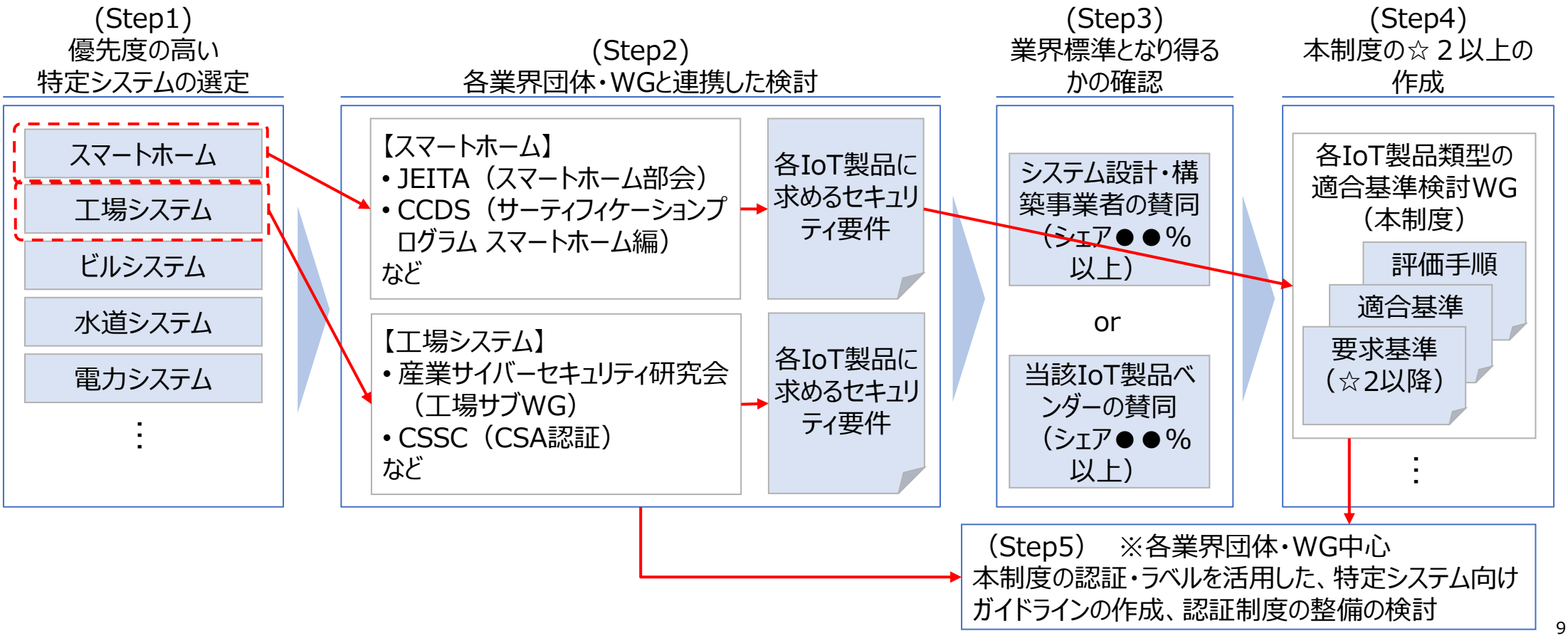
【各IoT製品に求める認証・ラベル指定のイメージ】

IoT製品	認証・ラベル	指定理由（例）
ルータ	☆2以上	• 外部からの侵入ルートになる可能性があるため
ホームゲートウェイ	☆2以上	• 外部からの侵入ルートになる可能性があるため
スマート照明	☆1以上	• 機器単体が侵害を受けても被害は限定的であるため
スマート家電	☆1以上	• 機器単体が侵害を受けても被害は限定的であるため
スマートロック	☆2以上	• 侵害が受けた場合、人的資産や物理的資産の損害に繋がる恐れがあるため

※ システムの重要度・規模やIoT製品の用途で指定する認証・ラベルを分けることもある。

【目的②】展開戦略と初期ターゲット

- 検討優先度の高い「特定分野のシステム」を選定し、各システム全体のセキュリティを考えている業界団体やワーキンググループと連携し、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を検討する。
- 各特定分野のシステムにおいて、IoT機器を選定する立場の事業者または当該IoT機器を生産するベンダーから、認証・ラベル制度の整備とその活用について一定割合以上の賛同が得られる場合（業界標準となり得ると判断される場合）、本制度として☆2以降の整備を進める。
- 各特定分野のシステム全体のセキュリティガイドラインの作成や、システム全体の認証制度等の整備は、各業界団体やワーキンググループで検討し、本制度はオブザーバーの立場で連携する。（公的機関でのシステム全体の認証制度の整備は、本制度とは分けてその必要性も含めて検討）



【参考】消費者向けIoT製品の展開戦略の整理

- 消費者向け製品は製品類型に応じた展開戦略を実施していく。

製品類型	展開戦略案
通信機器 （ブロードバンドルーター、Wi-Fiルーター、ハブ、スイッチ等）	政府機関等調達の範疇で検討（目的①） ※家庭用製品はスマートホームの範疇で検討（目的②）
自律型ロボット （ドローン等）	
防犯関連機器 （ネットワークカメラ、警報装置、電気錠システム等）	
生活家電 （掃除機、洗濯機、冷蔵庫、レンジ、エアコン等）	スマートホームの範疇で検討（目的②）
AV機器 （スマートTV、レコーダー、スマートスピーカー等）	
エネルギー関連機器 （エネファーム、PCS、ガス給湯器等）	
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等）	
娯楽機器 （ゲーム機、スマート玩具等）	

本日の議題

【御報告事項】

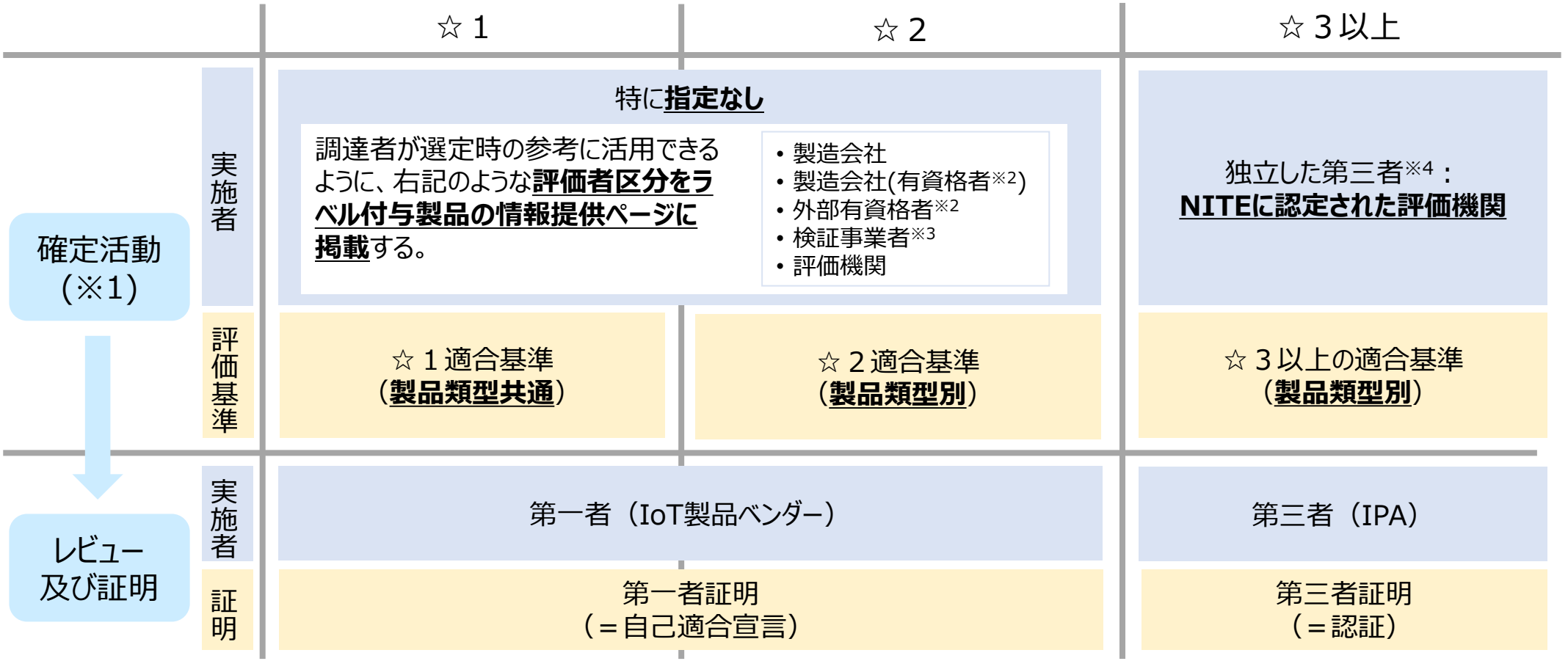
- 適合性評価の実証状況について

【御議論いただきたい事項】

- 制度の必要性及び目的
- **制度及び各レベルの位置づけ**
- IoT製品ベンダーの能動的な制度活用を促す仕掛け
- 適合性評価済製品におけるセキュリティ事案への対応
- 最終とりまとめの骨子案

本制度における確定活動の実施者と証明主体

- ☆１、☆２では、自己適合宣言のスキームを採用する。他方、**どのような評価者が評価を行ったかについて、ラベル付与製品の情報提供ページに掲載**し、評価能力のある者が評価を行ったかについて、調達者が識別できるようにする。
- ☆３以上では、**確定活動をNITEに認定された評価機関、レビュー及び証明（認証）をIPAが実施することを想定**している。



※1 適合性を判断するために必要なすべての情報を取得する活動、いわば事実を確認する活動。製品要求事項に関する情報をレビュー及び証明機能へのインプットとして提供するための、試験、測定、検査、設計評価、サービス及びプロセスの評価、監査などの適合性評価活動を含んでもよい。
※2 情報処理安全確保支援士等の指定資格保有が、評価の実施または評価結果の確認に関与することを条件とする。資格保有に加え、IoTセキュリティ評価に関する研修受講完了または評価ガイドラインを理解していることの宣誓を求める。指定資格を情報処理安全確保支援士に限定するか、同等の他資格も許容するかは今後検討する。
※3 情報セキュリティサービス審査登録制度の「機器検証サービス」分野にて、「情報セキュリティサービス基準適合サービスリスト」に登録されている事業者の想定。
※4 製造会社／申請者と利害関係がない独立した第三者。

本制度における☆1/☆2の申請・評価の流れ

通常の開発・購買活動 → 本制度導入による効果 → ラベル付与のための対応

- ☆1では、広範なIoT製品を対象とした、**最低限の脅威に対抗するための統一的な基準**とし、☆2では、**製品類型ごとに定義された一定程度の脅威に対抗できる、製品類型ごとの基準**とする。
- ☆1/☆2ではベンダー自身による自己適合宣言スキームを採用するが、**評価機関や検証事業者、有資格者に評価を依頼することも可能**とする。

☆1では、検証や評価を行う担当者が、チェックリストや評価ガイドを見て低コストで自己評価可能なレベルとする。

☆2では、製品類型ごとの要件を踏まえ、検証や評価を行う担当者が、実際に実機検証を実施し、適合確認を行うレベルとする。

IPA（スキームオーナー）

適合性評価チェックリストの提出・ラベル申請

ラベル付与

適合性評価チェックリストの申請に基づき、形式チェックを行ったうえで、ラベルを付与する。

IoT製品ベンダー

※代理店（輸入業者、ITベンダー等）による申請の場合、製品ベンダーの承諾を得た上で窓口となり、製品ベンダー自体が評価した内容を提出することとする。

製品の開発・販売

セキュリティ対策を実施していることの可視化

海外制度への対応

適合性評価チェックリストの記入（自己適合宣言）

シンガポールCLS＊1要件や英国PSTI法など、海外制度と国際連携可能な要件とする※。

対象となるIoT製品（イメージ）

製品の選定・購入

ラベルが付与された製品の選定・購入

製品ユーザー・調達者

評価結果の報告

評価依頼（自己適合宣言が困難な場合など）

ベンダー自身による自己適合宣言を許容する。

評価機関・検証事業者・有資格者

評価機関・検証事業者・有資格者による評価（自己適合宣言が困難な場合など）

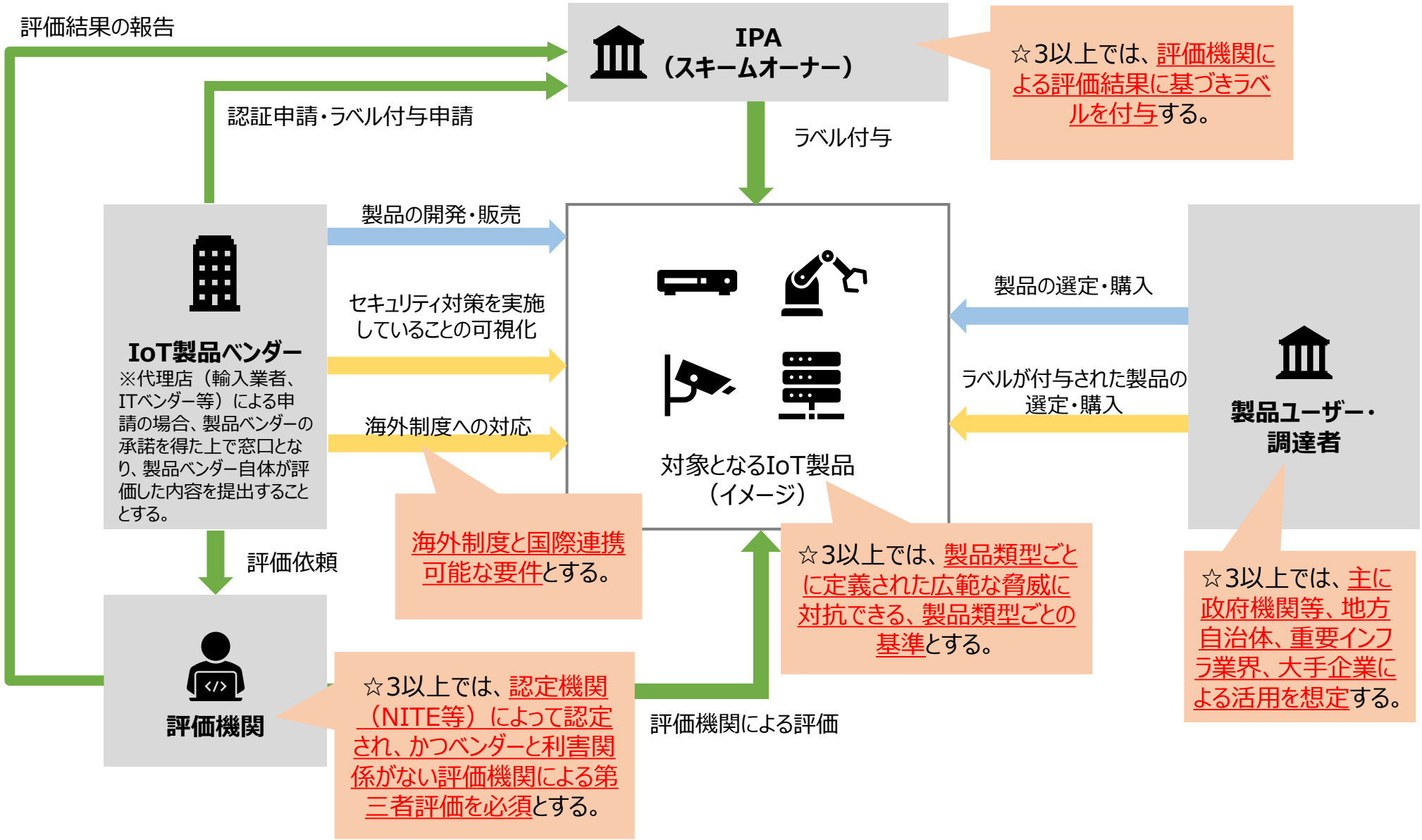
☆1では、特定の製品類型に絞らず、広範なIoT製品を対象とした、最低限の脅威に対抗するための統一的な基準とする。

☆2では、製品類型ごとに定義された一定程度の脅威に対抗できる、製品類型ごとの基準とする。

本制度における☆3以上の申請・評価の流れ

通常の開発・購買活動　本制度導入による効果　ラベル付与のための対応

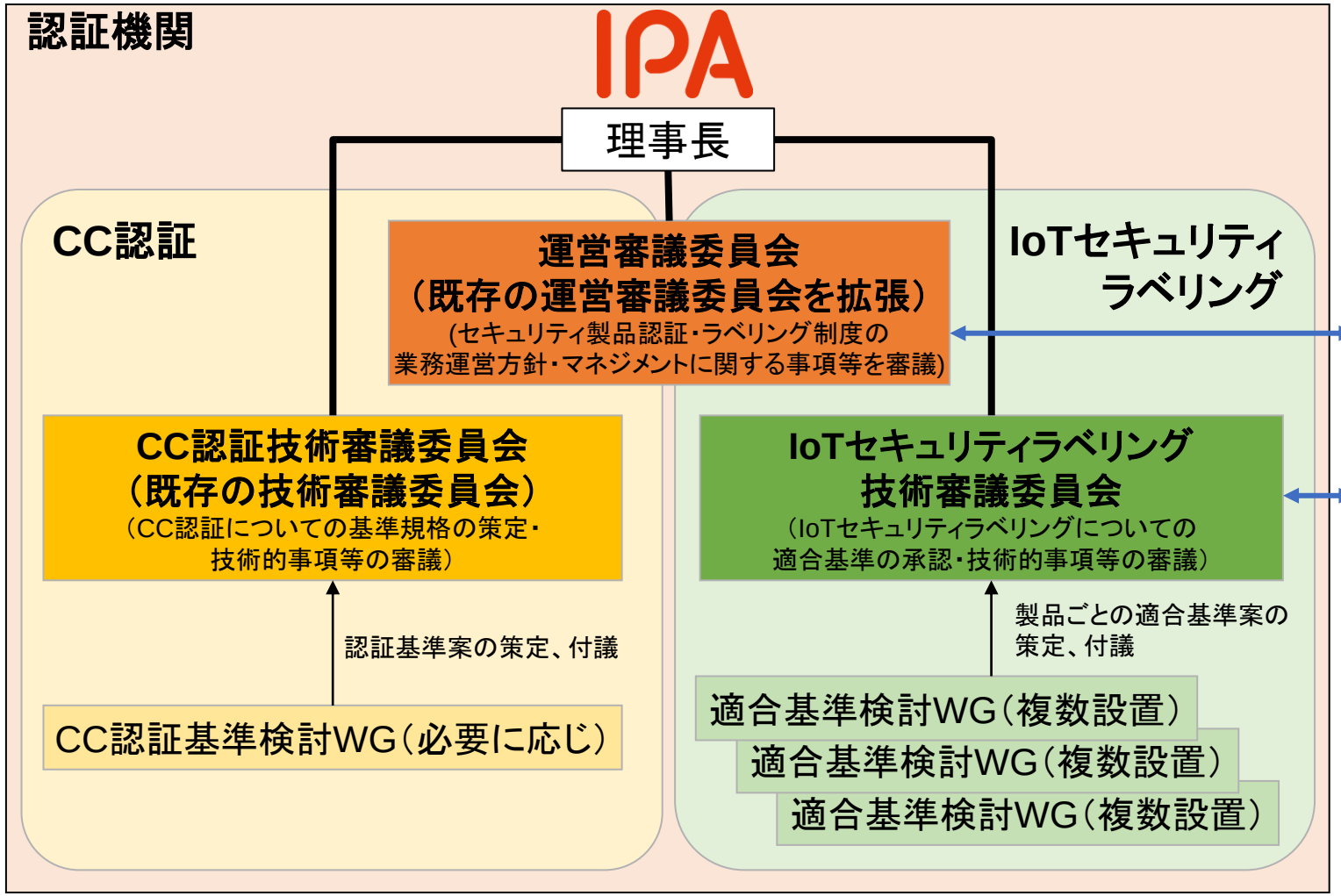
- ☆3以上では、**製品類型ごとに定義された広範な脅威に対抗できる、製品類型ごとの基準とする。**
- **☆3以上では、認定機関によって認定され、かつベンダーとの利害関係がない評価機関による、高信頼な第三者評価を必須**とする。



発展JISEC認証スキームの事務局・委員会の体制案

第5回検討会資料P.7を修正

- 現行JISEC制度（CC認証）とIoTセキュリティ適合性評価制度を**発展JISEC制度として、一体となった枠組みで運用**する。
- IoTセキュリティ適合性評価制度は、☆2以上を整備する製品類型の検討、国内既存制度との連携・統合の調整、相互承認等の諸外国との調整などが来年度以降もあるため、**IPAと経産省による運営事務局を設立**し、制度が軌道に乗るまでそれを維持する。



IoTセキュリティ認証制度
運営事務局（※）

IPA ＋ 経済産業省

- 制度拡張（☆2以降）の検討
- 国内既存制度との連携・統合検討
- 相互承認等の海外連携の調整
- 政府調達要件等への働きかけ
- 民間企業、一般消費者への制度普及促進
- IoT製品ベンダーへの認証取得促進

など

※以下の条件が満たされ、制度が軌道に乗った段階で、IPAによる運営とし、経済産業省は各委員会に委員またはオブザーバーとして関与する。

- 定常的に新規の認証申請がある。
- 主要な製品類型の☆2以降の制度化および既存制度との統合・すみ分けが合意されている。
- 海外の主要国との相互承認等の方向性が合意されている。

【参考】本制度と現行JISEC制度（CC認証）の比較

<table>
<tr><th>信頼性の評価レベル</th><th colspan="3">高</th><th colspan="3">中</th><th colspan="4">低</th></tr>
<tr><td rowspan="2">CCRA/相互承認の対象可否</td><td colspan="3">〇（強制相互承認対象外）</td><td colspan="3">〇（強制相互承認対象）</td><td colspan="4">×（相互承認対象外 ※各国制度と個別調整）</td></tr>
<tr><td colspan="2">JISEC(CC) – EAL 4</td><td>JISEC(CC) – EAL 2</td><td>JISEC(CC) – EAL 1</td><td>本制度 – ☆4</td><td>本制度 – 3</td><td>本制度 – ☆2</td><td>本制度 – ☆1</td></tr>
<tr><td>ソースコードチェック</td><td colspan="2">〇</td><td>×</td><td>×</td><td>要件による</td><td>×</td><td>×</td><td>×</td></tr>
<tr><td>ホワイトボックス侵入試験</td><td colspan="2">〇</td><td>〇</td><td>×</td><td>×</td><td>×</td><td>×</td><td>×</td></tr>
<tr><td>ブラックボックス侵入試験</td><td colspan="2">中程度</td><td>基本強化</td><td>基本</td><td>基本強化</td><td>基本</td><td>×</td><td>×</td></tr>
<tr><td>サイト訪問</td><td colspan="3">必要</td><td>不要（オンサイト試験実施の場合あり）</td><td colspan="2">必要になる場合あり（要件による）</td><td colspan="2">不要</td></tr>
<tr><td>セキュリティ脅威分析</td><td colspan="4">製品特性に応じた分析結果の明記が個別に必要</td><td colspan="4">対象脅威は事前指定（個別には対応不要）</td></tr>
<tr><td>セキュリティ対策網羅性</td><td colspan="4">製品特性に応じた脅威に対する対策網羅性の説明が個別に必要</td><td colspan="4">対象対策は機能要件・保証要件で事前指定
（個別には対応不要）</td></tr>
<tr><td>ST仕様書
（セキュリティ機能仕様書）</td><td colspan="4">TOEごとに作成が必要
※PPは製品分野ごとのセキュリティ機能要件／セキュリティ保証要件を決めたものであるが、PP適合であってもST仕様書の作成は必要</td><td colspan="4">作成不要</td></tr>
<tr><td rowspan="2">セキュリティ機能要件
セキュリティ保証要件</td><td colspan="4">TOEごとにST仕様書に明記（申請者が指定）</td><td colspan="4">製品群共通の適合要件としてセキュリティ要件を事前指定</td></tr>
<tr><td colspan="4">● 脅威に対抗するのに必要なセキュリティ機能要件をST仕様書に記載
● 保証レベルに応じた必要なセキュリティ保証要件をST仕様書に記載</td><td colspan="2">製品分野別政府調達要件をベース
（基本強化要件）</td><td>（基本要件）</td><td>製品分野別基本要件</td><td>全製品分野共通の最低要件</td></tr>
<tr><td>セキュリティ評価</td><td colspan="4">製品特性を考慮してCC/CEMの評価基準を適用した
独立した第三者機関による認証評価
（Attack based or Specification based）</td><td colspan="4">事前設定した評価基準に従った独立した第三者機関による評価
有資格者によるチェックリスト自己検査
チェックリスト自己検査
チェックリスト自己宣言</td></tr>
<tr><td>評価報告書</td><td colspan="4">ST仕様書に依存</td><td colspan="4">定型報告書 / チェックリスト</td></tr>
</table>

JISEC(CC)認証制度

IoTセキュリティ適合性評価制度

本日の議題

【御報告事項】

- 適合性評価の実証状況について

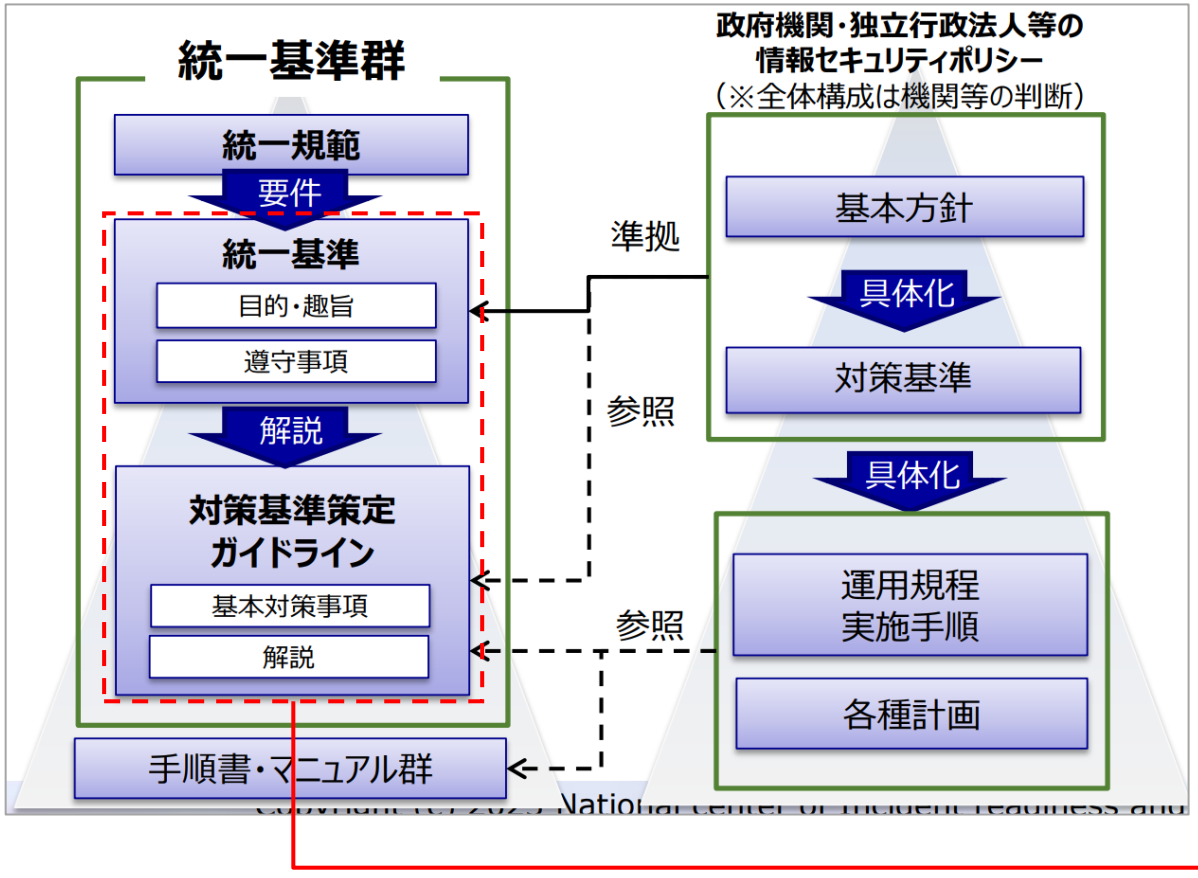
【御議論いただきたい事項】

- 制度の必要性及び目的
- 制度及び各レベルの位置づけ
- **IoT製品ベンダーの能動的な制度活用を促す仕掛け**
- 適合性評価済製品におけるセキュリティ事案への対応
- 最終とりまとめの骨子案

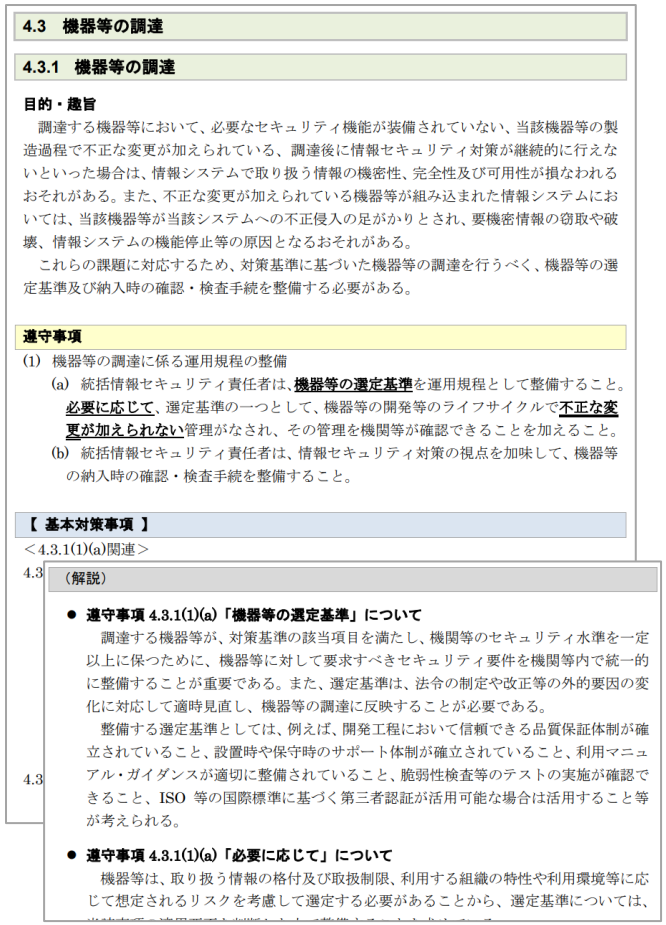
政府機関等のサイバーセキュリティ対策のための統一基準群の構成

- サイバーセキュリティ戦略本部は、サイバーセキュリティ基本法に基づき、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において、情報セキュリティのベースラインや、より高い水準の情報セキュリティを確保するための対策事項を規定している。
- 政府機関等のサイバーセキュリティ対策のための統一規範の実施のため必要な要件として、情報セキュリティ対策の項目ごとに政府機関等が遵守すべき事項が、「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（以下、統一基準）」で定められている。
- 統一基準の遵守事項を満たすためにとるべき基本的な対策事項の例示と、対策基準の策定及び実施に際しての考え方等を解説した「政府機関等の対策基準策定のためのガイドライン（以下、ガイドライン）」をNISCが発行している。
- **<u>統一基準およびガイドラインの「4.3.1 機器等の調達」に、選定基準の中に本適合性評価制度の活用を記載</u>**することが考えられる。

統一基準群（令和５年度版）文書体系



対策基準策定ガイドラインの「4.3.1 機器等の調達」の記載



4.3 機器等の調達

4.3.1 機器等の調達

目的・趣旨

調達する機器等において、必要なセキュリティ機能が装備されていない、当該機器等の製造過程で不正な変更が加えられている、調達後に情報セキュリティ対策が継続的に行えないといった場合は、情報システムで取り扱う情報の機密性、完全性及び可用性が損なわれるおそれがある。また、不正な変更が加えられている機器等が組み込まれた情報システムにおいては、当該機器等が当該システムへの不正侵入の足がかりとされ、要機密情報の窃取や破壊、情報システムの機能停止等の原因となるおそれがある。

これらの課題に対応するため、対策基準に基づいた機器等の調達を行うべく、機器等の選定基準及び納入時の確認・検査手続を整備する必要がある。

遵守事項

(1) 機器等の調達に係る運用規程の整備

(a) 統括情報セキュリティ責任者は、**<u>機器等の選定基準</u>**を運用規程として整備すること。**<u>必要に応じて</u>**、選定基準の一つとして、機器等の開発等のライフサイクルで**<u>不正な変更が加えられない</u>**管理がなされ、その管理を機関等が確認できることを加えること。

(b) 統括情報セキュリティ責任者は、情報セキュリティ対策の視点を加味して、機器等の納入時の確認・検査手続を整備すること。

【 基本対策事項 】

＜4.3.1(1)(a)関連＞

（解説）

- **遵守事項 4.3.1(1)(a)「機器等の選定基準」について**

調達する機器等が、対策基準の該当項目を満たし、機関等のセキュリティ水準を一定以上に保つために、機器等に対して要求すべきセキュリティ要件を機関等内で統一的に整備することが重要である。また、選定基準は、法令の制定や改正等の外的要因の変化に対応して適時見直し、機器等の調達に反映することが必要である。

整備する選定基準としては、例えば、開発工程において信頼できる品質保証体制が確立されていること、設置時や保守時のサポート体制が確立されていること、利用マニュアル・ガイダンスが適切に整備されていること、脆弱性検査等のテストの実施が確認できること、ISO 等の国際標準に基づく第三者認証が活用可能な場合は活用すること等が考えられる。

- **遵守事項 4.3.1(1)(a)「必要に応じて」について**

機器等は、取り扱う情報の格付及び取扱制限、利用する組織の特性や利用環境等に応じて想定されるリスクを考慮して選定する必要があることから、選定基準については、

統一基準の記載内容

上記遵守事項に対する基本対策事項と解説をガイドラインに記載

出所）NISC「統一基準群改定のポイント（令和５年度版）」https://www.nisc.go.jp/policy/group/general/kijun.html
NISC「政府機関等の対策基準策定のためのガイドライン（令和5年度版）」https://www.nisc.go.jp/pdf/policy/general/guider5.pdf

本制度を活用した政府機関等のIoT製品の選定・調達プロセス案

- 情報システムの重要度に応じ、「重要度：低」は☆1以上、**「重要度：高～中」は少なくとも☆3以上**のIoT製品を選定する。
- ラベル取得製品が普及する時期をめどに、**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**で、NISCと検討を進めている。

情報システムの分類基準（例）

重要度	判断基準	（参考）想定する情報システム
高	• 国家安全保障及び治安関係の業務を行う場合 • 機密性の高い情報を取り扱う場合並びに情報の漏えい及び情報の改ざんによる社会的・経済的混乱を招くおそれのある情報を取り扱う場合 • 番号制度関係の業務を行う場合等、個人情報を極めて大量に取り扱う業務を行う場合 • 機能停止等の場合、機関等の業務遂行に著しい影響を及ぼす場合 • 運営経費が極めて大きい場合 • 情報セキュリティインシデント発生時に「情報システムの重要度：高」に分類される他の情報システムに影響を与える場合	• 防災、経済、重要インフラに関係する情報システム • 基幹業務システム、LAN や職員が日常的に利用する PC やメール機能を管理する情報システム等の組織の業務の根幹を支える情報システム • 情報システムの基盤として利用する機関等が所管する情報システム（クラウドサービスを利用した共通基盤を含む） • 対国民向けの情報システムで社会的影響が大きい情報システム • 機密性 3 情報や特定個人情報を取り扱う情報システム • 極めて大量の要保護情報を取り扱う情報システム
中	• 「情報システムの重要度：高」を除く要保護情報を取り扱う場合 • 情報セキュリティインシデント発生時に「情報システムの重要度：中」に分類される他の情報システムに影響を与える場合	• 要保護情報を取り扱う情報システム（情報セキュリティインシデント発生時に他の情報システムへ影響を与える情報システムを含み、「情報システムの重要度：高」に想定される情報システムを除く。）
低	• 「情報システムの重要度：高、中」を除く全て	• 要保護情報の取扱いがない情報システム

IoTセキュリティ適合性評価制度を活用した選定・調達プロセス案

各政府機関等でのIoT製品の選定プロセス案	デジタル庁およびNISCの関与
• 少なくともIoTセキュリティ適合性評価制度の**☆3以上（第三者評価）を取得**している製品を選定 • 必要に応じ、当該情報システムや利用するIoT製品のリスクを考慮し、個別のセキュリティ要件の設定とその確認を実施（特に「重要度：高」の情報システム）	• 「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」に基づき、デジタル庁およびNISCと協議して調達するIoT製品を決定
	－
• IoTセキュリティ適合性評価制度の**☆1以上を取得**している製品を選定	－

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（令和5年度版）」https://www.nisc.go.jp/pdf/policy/general/guider5.pdf

政府機関等の調達において☆3～4の活用が想定されるIoT製品類型

- 対策基準策定ガイドラインの「5.1.1 情報システムの分類基準等の整備」に例示されている、**「重要度：高～中」の情報システムにおいて調達されるIoT製品**への活用を想定し、独立性を持った第三者評価を行う☆3以上の整備を検討する。
- 現状での候補として、**ネットワークカメラ、ドローン、ファイアウォール、ルーター（有線・無線）等を想定**している。

情報システムの分類基準（例）

重要度	判断基準	（参考）想定する情報システム
高	• 国家安全保障及び治安関係の業務を行う場合 • 機密性の高い情報を取り扱う場合並びに情報の漏えい及び情報の改ざんによる社会的・経済的混乱を招くおそれのある情報を取り扱う場合 • 番号制度関係の業務を行う場合等、個人情報を極めて大量に取り扱う業務を行う場合 • 機能停止等の場合、機関等の業務遂行に著しい影響を及ぼす場合 • 運営経費が極めて大きい場合 • 情報セキュリティインシデント発生時に「情報システムの重要度：高」に分類される他の情報システムに影響を与える場合	• 防災、経済、重要インフラに関係する情報システム • 基幹業務システム、LAN や職員が日常的に利用する PC やメール機能を管理する情報システム等の組織の業務の根幹を支える情報システム • 情報システムの基盤として利用する機関等が所管する情報システム（クラウドサービスを利用した共通基盤を含む） • 対国民向けの情報システムで社会的影響が大きい情報システム • 機密性 3 情報や特定個人情報を取り扱う情報システム • 極めて大量の要保護情報を取り扱う情報システム
中	• 「情報システムの重要度：高」を除く要保護情報を取り扱う場合 • 情報セキュリティインシデント発生時に「情報システムの重要度：中」に分類される他の情報システムに影響を与える場合	• 要保護情報を取り扱う情報システム（情報セキュリティインシデント発生時に他の情報システムへ影響を与える情報システムを含み、「情報システムの重要度：高」に想定される情報システムを除く。）
低	• 「情報システムの重要度：高、中」を除く全て	• 要保護情報の取扱いがない情報システム

【☆3～4が必要となる製品類型（候補）】

- **ネットワークカメラ**
- **ドローン**
- **ファイアウォール**
- **ルーター（有線・無線）**
- ⋮

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（令和5年度版）」https://www.nisc.go.jp/pdf/policy/general/guider5.pdf

本日の議題

【御報告事項】

- 適合性評価の実証状況について

【御議論いただきたい事項】

- 制度の必要性及び目的
- 制度及び各レベルの位置づけ
- IoT製品ベンダーの能動的な制度活用を促す仕掛け
- **適合性評価済製品におけるセキュリティ事案への対応**
- 最終とりまとめの骨子案

IPAが担う機能別の役割（案）

- IPAは本制度において、**スキームオーナー、ラベル付与機関、認証機関の機能を担う**。それぞれの機能によって、担うべき役割は異なる。
- **認証やラベルの付与により、製品のセキュリティが完全に確保されていることを保証するわけではない**。

IPAの機能	スキームオーナー（☆１以上）	ラベル付与機関（☆１以上）	認証機関（☆３以上）
定義	適合性評価システム又はスキームの基本的な規則を維持管理する主体	証明の結果を受けて、ラベルの付与を行う機関	適合性評価の対象を提供する人又は組織、及びその対象について使用者側の利害をもつ人又は組織の双方から独立した、人又は機関によって実施される証明を行う機関
担うべき役割	• 制度に関する規則を維持管理する • 評価機関・検証事業者の認定基準や適合基準、技術的事項の審議や妥当性の検証を行う • 経済産業省と協力して、利用者・調達者に対する制度の啓発活動を実施評価機関する	• 証明の結果を受けて、ラベルの付与を行う • 無許可でラベルを使用されないようにラベルを法的に保護する（ラベルの商標登録及び使用条件の明確化） • ラベルの使用を総合的に管理する規則を定める • ラベルの使用を保護し、監視する手段を設ける • **インシデントの報告を受け付け、必要に応じてサーベイランスを実施**する • ラベルの許可の取消し又は適切な法的処置を含め、**ラベルの不適切な使用を解消するための処置**をとる • **ラベルに関する苦情に対して対応処置**をとり、これらの記録を保管する • ラベル付与活動の実施の過程で得られた又は生成された全ての情報を管理する	• 認証の決定の根拠となる、十分な客観的証拠（確定活動の結果）を評価機関から入手し、確認する • 審査の結果に基づいて、適合の十分な証拠がある場合には認証の授与を決定し、又は十分な適合の証拠がない場合には認証を授与しない決定をする • 認証活動の実施の過程で得られた又は生成された全ての情報を管理する • 異議申立てを受領し、評価し、異議申立てに関して決定するための文書化されたプロセスをもつ • 異議申し立て処理プロセスの全ての段階の全ての決定に対する責任を負う
備考	-	ラベルの付与により、**製品のセキュリティが完全に確保されていることを保証するわけではない**。ラベルが付与された製品のセキュリティを原因としたインシデントが生じたとしても、ラベル付与機関が責任を負うことはない。	認証により、**製品のセキュリティが完全に確保されていることを保証するわけではない**。認証を受けた製品のセキュリティを原因としたインシデントが生じたとしても、認証機関が責任を負うことはない。

サイバー保険の活用について

- IoT製品ベンダーが安価かつ簡易にサイバー保険へ加入するための手段としては、検証事業者・評価機関が契約者となる評価・検証サービスへの商品付帯方式サイバー保険が実現可能性が高い。

保険会社へのヒアリング結果

- ラベル付与IoT製品を調達することで一般的なサイバー保険の保険料を割り引くことは難しい。
- 製造・販売した製品が原因で発生したサイバー事故による賠償損害や費用損害を補償する製品サイバー保険（契約者・被保険者はともにIoT製品ベンダー）【図1】は、どの保険会社も提供しておらず、新たな保険商品を開発するのはハードルが高い。
- 検証事業者・評価機関が提供する検証・評価サービスを受けた製品が原因で発生したサイバー事故による賠償損害や費用損害を補償する商品付帯方式サイバー保険（契約者は検証事業者・評価機関、被保険者は検証・評価サービスを依頼したIoT製品ベンダー）【図2】は実現可能性が高い。

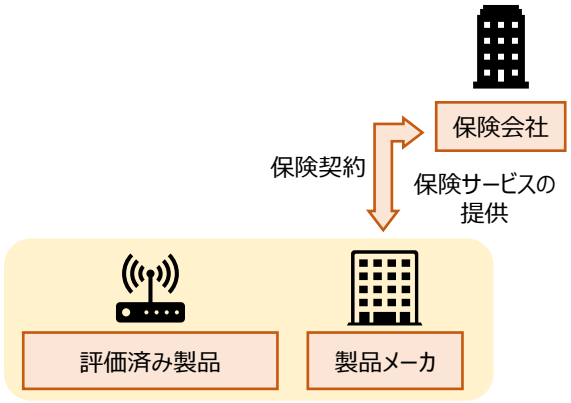


図１：契約者・被保険者がともに
IoT製品ベンダーとなる製品サイバー保険

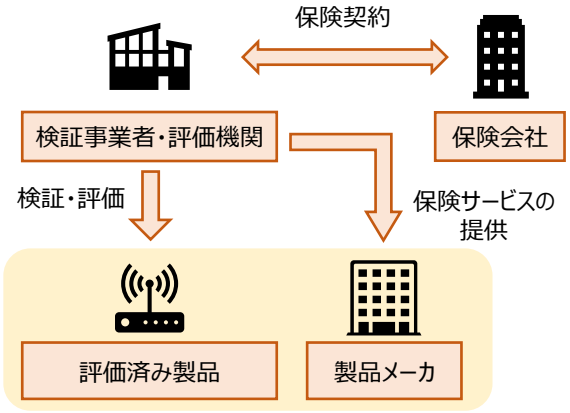
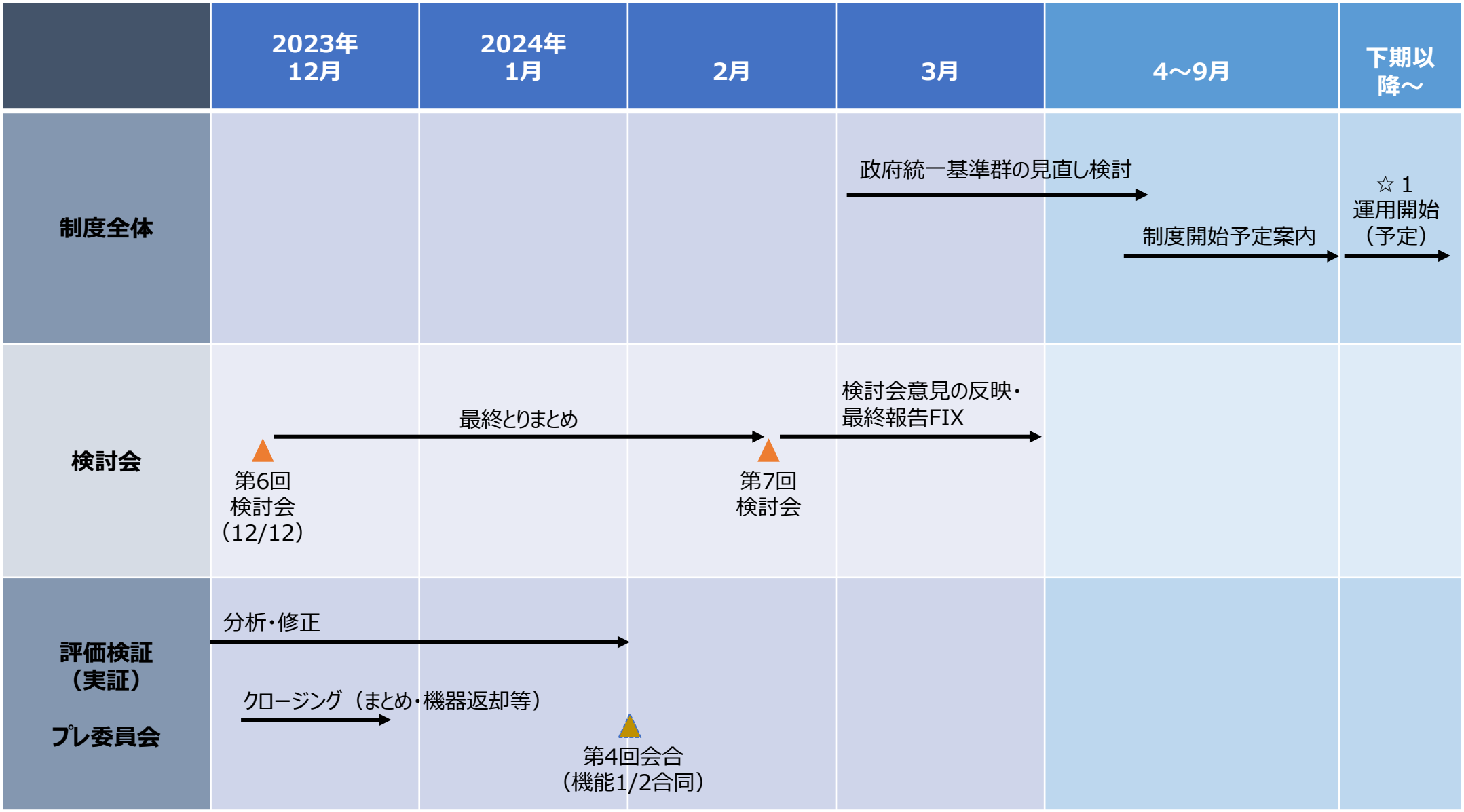


図２：検証事業者・評価機関が契約者、検証・評価サービスを依頼した
IoT製品ベンダーが被保険者となる商品付帯方式サイバー保険

サイバー攻撃による損害を広く分散する社会の構築を実現するために、IoT製品ベンダーが安価かつ簡易にサイバー保険へ加入できるようになることが望ましい。そのため、本制度における検証事業者・評価機関が契約者、検証・評価サービスを依頼したIoT製品ベンダーが被保険者となる、評価・検証サービスへの商品付帯方式サイバー保険の活用に関して検討を行う。

今後のスケジュール


2023年
12月
2024年
1月
2月
3月
4～9月
下期以
降～
制度全体
政府統一基準群の見直し検討
制度開始予定案内
☆１
運用開始
（予定）
検討会
最終とりまとめ
検討会意見の反映・
最終報告FIX
第6回
検討会
（12/12）
第7回
検討会
評価検証
（実証）
プレ委員会
分析・修正
クロージング（まとめ・機器返却等）
第4回会合
（機能1/2合同）

【参考】ISO/IEC 17000シリーズおよびJSAにおける用語の定義（1/2）

用語	定義	参照元	備考
適合性評価 (conformity　assessment)	製品、プロセス、システム、要員又は機関に関する規定要求事項が満たされていることの実証	ISO/IEC 17000:2004 [JIS Q 17000:2005]	適合性評価活動は、「選択」「確定」「レビュー及び証明」の活動の系列である
選択活動 (selection activity)	確定活動の準備を整える活動	https://www.jsa.or.jp/datas/media/10000/md_2481.pdf	例えば、適合性評価の方法の選択、対象を代表するサンプルの選択、試験すべき特性の選択など その後に行われる確定機能に必要な全ての情報及びインプットを収集又は作成するための、計画及び準備の活動を含む（ISO/IEC 17067:2013 [JIS Q 17067:2014]）
確定活動 (determination activity)	適合性を判断するために必要なすべての情報を取得する活動、いわば事実を確認する活動	https://www.jsa.or.jp/datas/media/10000/md_2481.pdf	例えば、試験によって製品の特性値を求めたり、組織のマネジメントシステムの実施状況を監査したりする活動など 製品要求事項に関する情報をレビュー及び証明機能へのインプットとして提供するための，試験，測定，検査，設計評価，サービス及びプロセスの評価，監査などの適合性評価活動を含んでもよい（ISO/IEC 17067:2013 [JIS Q 17067:2014]）
レビュー (review)	適合性評価の対象が、規定要求事項を満たしていることに関する選択活動及び確定活動、並びにこれらの活動の結果の適切性、十分さ及び有効性の検証	ISO/IEC 17000:2004 [JIS Q 17000:2005]	-
証明 (attestation)	レビューに従った決定に基づく、規定要求事項の充足が実証されたという表明の発行	ISO/IEC 17000:2004 [JIS Q 17000:2005]	-
第一者証明 (first-party attestation) (＝宣言、自己適合宣言) (=declaration)	適合性評価の対象を提供する人又は組織によって実施される証明	ISO/IEC 17000:2004 [JIS Q 17000:2005]	-
第三者証明 (third-party attestation) (＝認証) (=certification)	適合性評価の対象を提供する人又は組織、及びその対象について使用者側の利害をもつ人又は組織の双方から独立した、人又は機関によって実施される証明	ISO/IEC 17000:2004 [JIS Q 17000:2005]	-
認定 (accreditation)	適合性評価機関に関し、特定の適合性評価業務を行う能力を公式に実証したことを伝える第三者証明	ISO/IEC 17000:2004 [JIS Q 17000:2005]	-

【参考】ISO/IEC 17000シリーズおよびJSAにおける用語の定義（2/2）

用語	定義	参照元	備考
スキームオーナ (scheme owner)	適合性評価システム又はスキームの基本的な規則を維持管理する主体	https://www.jsa.or.jp/datas/media/10000/md_2481.pdf	-
	特定の認証スキームの開発及び維持に責任をもつ個人又は組織	ISO/IEC 17067:2013 [JIS Q 17067:2014]	
適合性評価機関 (conformity assessment body)	適合性評価サービスを実施する機関	ISO/IEC 17000:2004 [JIS Q 17000:2005]	第三者適合性評価の場合、認証機関とも呼ぶ
ラボラトリ (laboratory)	次の一つ以上の活動を実行する機関 「試験」「校正」「後の試験又は校正に付随するサンプリング」	ISO/IEC 17025：2017 [JIS Q 17025:2018]	-
規定要求事項 (specified requirement)	明示されたニーズ又は期待	ISO/IEC 17000:2004 [JIS Q 17000:2005]	本制度における適合基準にあたる
サーベイランス (specified requirement)	適合の表明の有効性を維持する基礎としての、適合性評価活動の系統だった反復	ISO/IEC 17000:2004 [JIS Q 17000:2005]	-