経済産業省

資料４－２

経済産業省におけるサイバーセキュリティ施策の取組状況について

令和６年２月２２日

経済産業省

- 2022年１１月より「IoT機器に対するセキュリティ適合性評価制度構築に向けた検討会」を開催しており、2024年3月に最終取りまとめを公表し、パブコメ実施予定。
- 本制度は幅広いIoT製品を対象としつつ、製品ごとの特性に応じた基準を既存の制度を活かしながら設けられるよう、複数のレベル（☆1～☆4）を用いた制度を想定。
- ☆1は、幅広いIoT製品を対象に、統一的な最低限の適合基準を想定し、評価方法はチェックリストに基づく自己適合宣言を想定。☆2以上は、製品類型ごとに適合基準を策定することを想定。
- ☆１については2024年7月～9月頃に制度開始案内、2024年度末の運用開始を予定。☆２以上については2025年度下期以降に一部のIoT製品類型に対する制度の開始を目指す。併せて、欧米等の諸外国と制度調和と政府調達含めた各種調達要件等への反映について関係省庁と調整を実施。

IoTセキュリティ適合性評価制度設立の目的

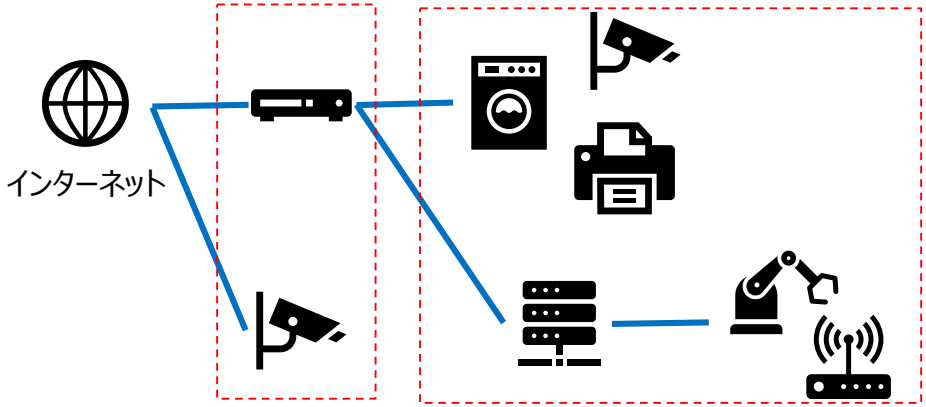
- 政府機関等・企業等のセキュリティ対策において、調達する製品や製品ベンダーのセキュリティも含めた広義なサプライチェーンリスク管理の取り組みが広がっている。しかしながら、**IoT製品の選定時や調達時に、そのセキュリティ機能や対策状況を自組織で確認（第二者評価）できているケースは少ない**のが現状である。そこで、第二者評価を代替する仕組みとして、**共通的な物差しでIoT製品のセキュリティを第三者が評価し、その結果に対して認証を付与する制度**が必要である。（目的①：**政府機関等・企業等のIoT製品調達ニーズへの対応**）
- 様々な機器がネットワークに接続されることで、十分なセキュリティ知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**

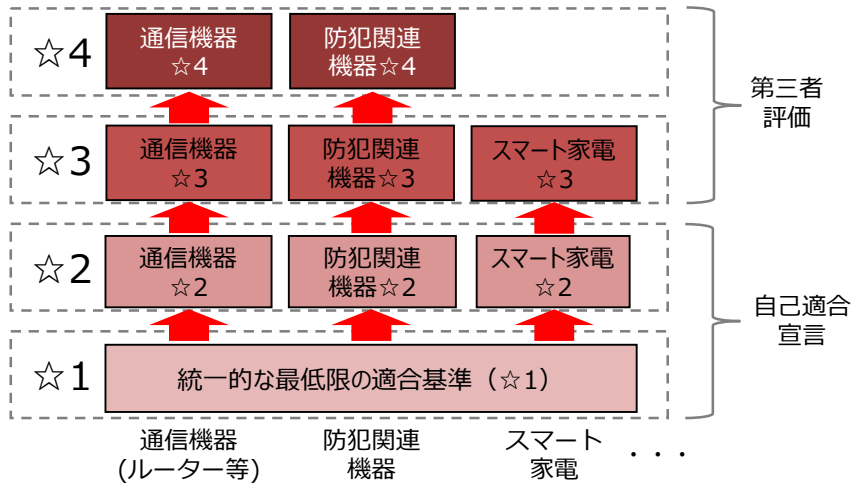
IoTセキュリティ適合性評価制度の概要

- 2022年11月より「**IoT機器に対するセキュリティ適合性評価制度構築に向けた検討会**」を開催。現在検討中の制度では、**インターネットに直接的に接続される製品及び間接的に接続されるIoT製品を対象**とする予定。
- 幅広いIoT製品を対象としつつ、製品ごとの特性に応じた基準を既存の制度を活かしながら設けられるよう、**複数のレベル（☆）を用いた制度**を想定。**☆1は、幅広いIoT製品を対象に、統一的な最低限の適合基準**を想定し、評価方法はチェックリストに基づく**自己適合宣言**を想定。**☆2以上は、製品類型ごとに適合基準を策定**することを想定し、評価方法はチェックリストに基づく**自己適合宣言（☆2）及び実機試験・侵入試験等の第三者評価（☆3以上）**を想定。なお、どの程度の第三者評価をどのレベルで求めるかは今後製品類型ごとに要検討。
- **☆1については2024年度中の制度開始**を予定。**米欧等の諸外国との制度調和を図るため並行して議論**中。

対象

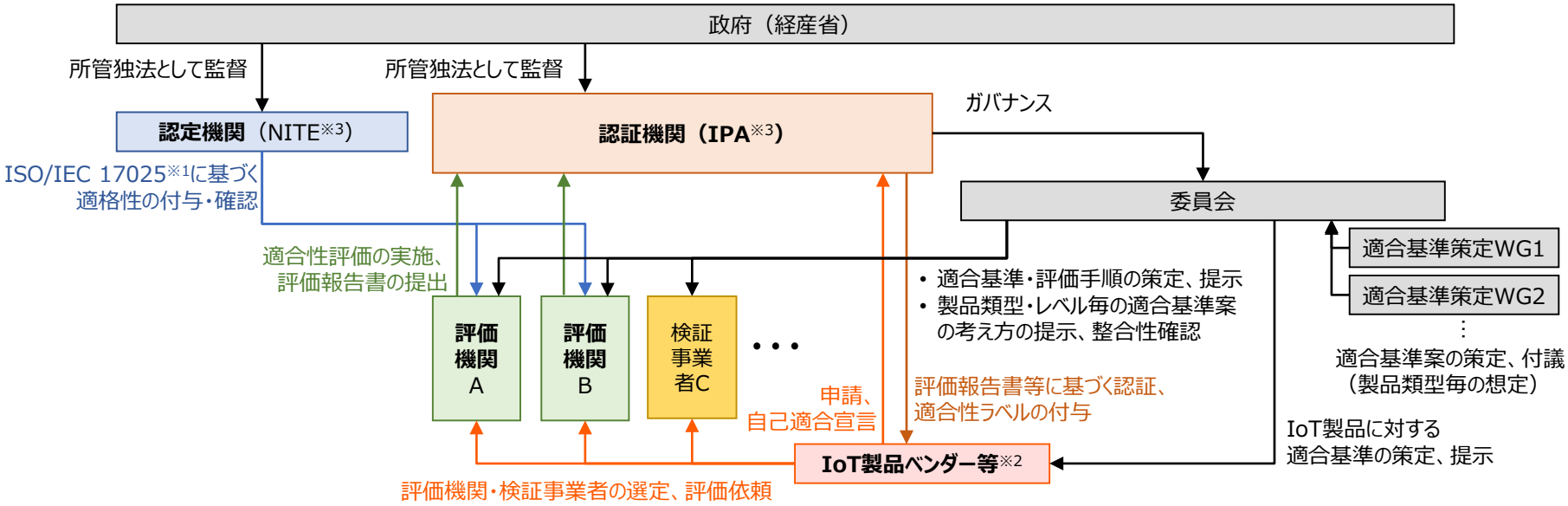


制度概要（検討中）



IoTセキュリティ適合性評価制度の全体スキーム

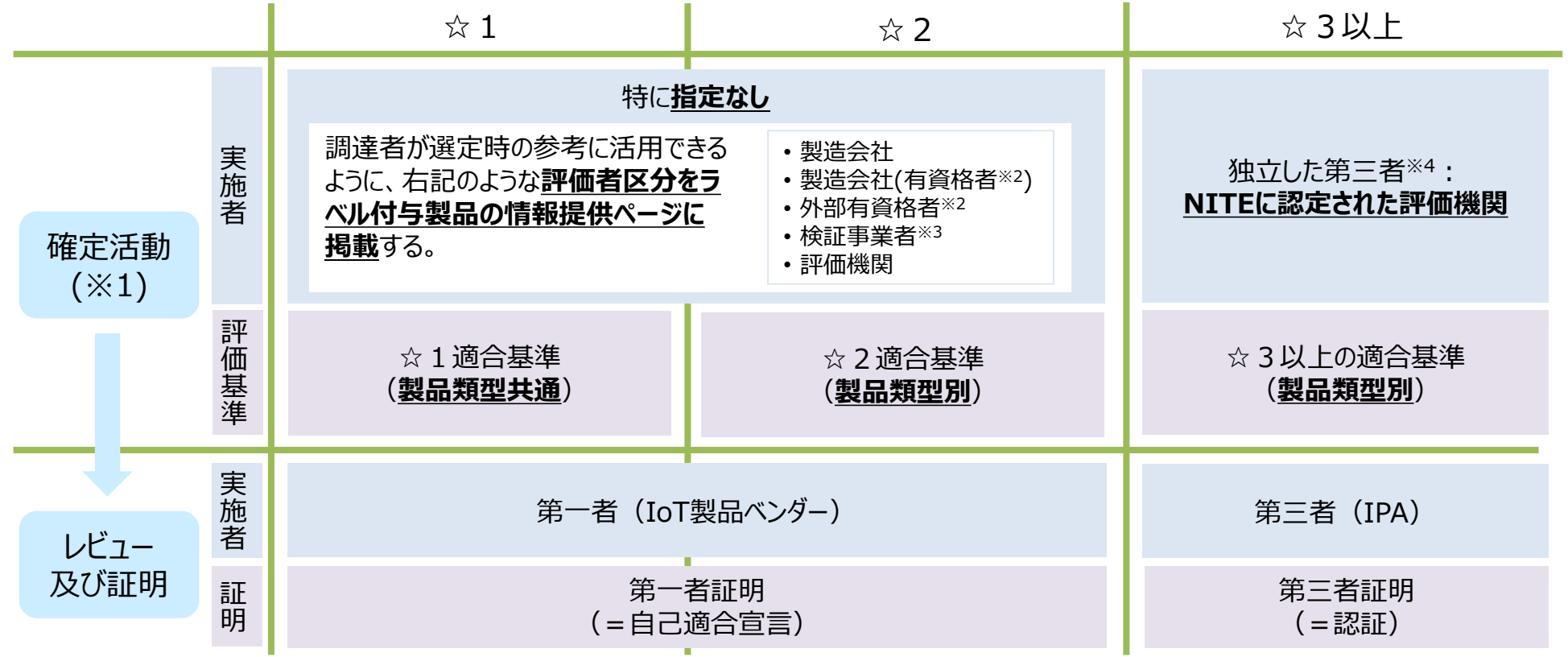
- 検討会での議論を踏まえ、本制度の各主体の適格性について、政府のガバナンスが効く構造が重要。かかる観点から、**CC認証の知見があるIPAのJISEC認証制度**（ITセキュリティ評価及び認証制度）**を拡張する形の制度**を構築予定。
- **2023年度末までに要求基準・適合基準の検討**および**ルーター、スマート家電、ネットワークカメラ等を対象とした評価検証**を実施中。



※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。
※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。
※3：組織名称は制度発足時に変更となる可能性がある。

【参考】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。

【参考】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）

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

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※。

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）

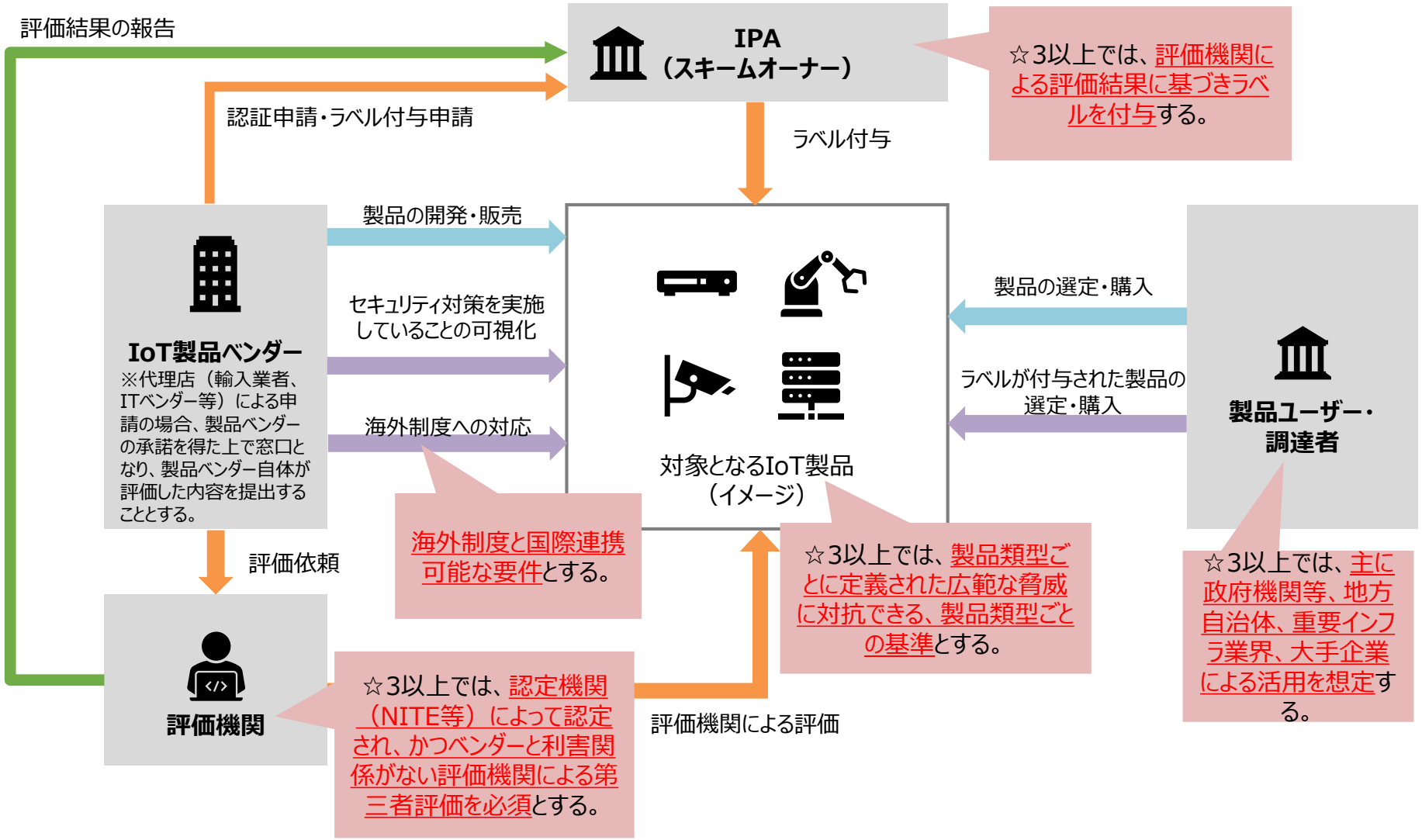
☆1では、特定の製品類型に絞らず、広範なIoT製品を対象とした、最低限の脅威に対抗するための統一的な基準とする。

☆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。

【参考】本制度における☆3以上の申請・評価の流れ

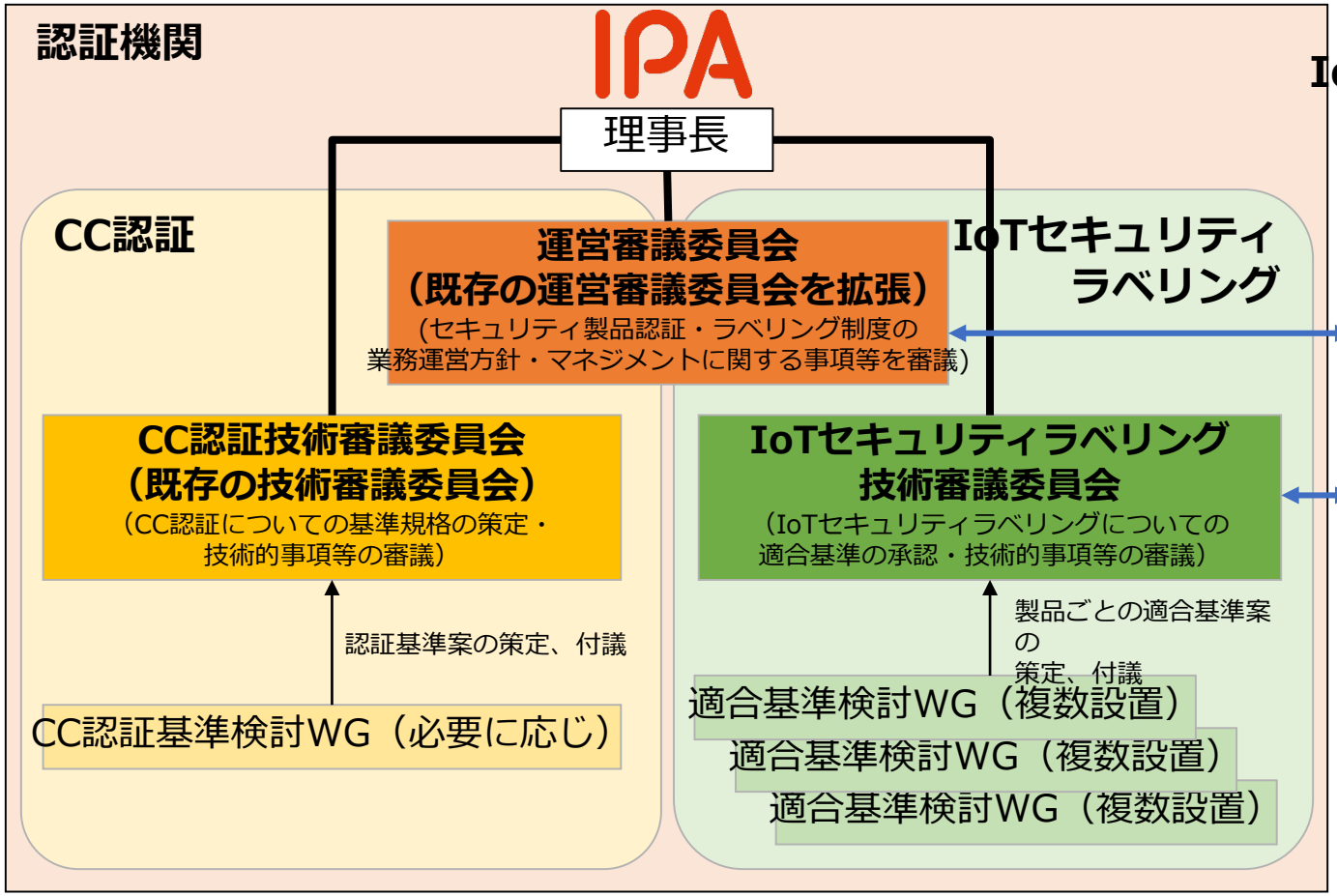
通常の開発・購買活動 → 本制度導入による効果 → ラベル付与のための対応

- ☆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。



【参考】発展JISEC認証スキームの事務局・委員会の体制案

- 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セキュリティラベリング制度
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

信頼性の評価レベル	高	中		低			
CCRA/相互承認の対象可否	○（強制相互承認対象外）	○（強制相互承認対象）		×（相互承認対象外 ※各国制度と個別調整）			
	JISEC(CC) – EAL 4	JISEC(CC) – EAL 2	JISEC(CC) – EAL 1	本制度 – ☆4	本制度 – 3	本制度 – ☆2	本制度 – ☆1
ソースコードチェック	○	×	×	要件による	×	×	×
ホワイトボックス侵入試験	○	○	×	×	×	×	×
ブラックボックス侵入試験	中程度	基本強化	基本	基本強化	基本	×	×
サイト訪問	必要		不要（オンサイト試験実施の場合あり）	必要になる場合あり（要件による）		不要	
セキュリティ脅威分析	製品特性に応じた分析結果の明記が個別に必要			対象脅威は事前指定（個別には対応不要）			
セキュリティ対策網羅性	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			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）			
ST仕様書（セキュリティ機能仕様書）	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			作成不要			
セキュリティ機能要件 セキュリティ保証要件	TOEごとにST仕様書に明記（申請者が指定） ● 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			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 製品分野別政府調達要件をベース（基本強化要件）	（基本要件）	製品分野別基本要件	全製品分野共通の最低要件
セキュリティ評価	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）			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			
評価報告書	ST仕様書に依存			定型報告書		チェックリスト	

JISEC(CC)認証制度

IoTセキュリティ適合性評価制度

【参考】製品に関する類型・既存の文書、認証制度等

※ 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。

【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

直接的又は間接的にインターネットに接続する製品			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ルーター等）	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）
			防犯関連機器（ネットワークカメラ等）			
			自律型ロボット（ドローン等）			
	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等）政重	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	
			防犯関連機器（ネットワークカメラ等）政重			
			産業用自律型ロボット（産業用ドローン、AGV等）政重			
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・スイッチ等）	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	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）
			生活家電（掃除機、洗濯機、冷蔵庫、レンジ、エアコン等）			
			AV機器（スマートTV、レコーダー、スマートスピーカー等）			
			防犯関連機器（警報装置、電気錠システム等）	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		
			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）			
	産業向け		通信機器（ハブ・スイッチ等）政重	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	※
			産業用コントローラー（PLC、DCSコントローラー等）政重			※
			産業用センサー（温度センサー、圧力センサー、変位センサー等）政重			※
			OA機器（複合機等）政重	JBMIA：BMsec	CCに基づく認証	
			金融関係機器（決済端末、POS端末等）重	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）		FISC：安全対策基準
			施設管理機器（入退室機器、受変電設備、照明、昇降機等）政重	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）	IEC 62443-4に基づく認証	経産省：ビルガイドライン
			医療機器（人工呼吸器、人工心臓弁、輸液ポンプ等）重	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		厚労省：医療情報ガイドライン
			自動車関連機器（ECU、IVI、TCU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）	CCに基づく認証	
			電気事業関連機器（スマートメーター、発電設備、PCS等）重	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		JESC：電制ガイドライン
			製造業・流通業関連機器（生産設備、自動倉庫等）重			経産省：工場ガイド 国交省：物流ガイド
			鉄道事業関連機器（CTC装置、PRC装置等）重			国交省：鉄道ガイドライン
			航空事業関連機器（IMS、iDMU等）重			国交省：航空ガイドライン
			・・・			

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。

【参考】諸外国の適合性評価制度との国際連携に向けて

- **☆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