経済産業省

IoT製品に対する
セキュリティ適合性評価制度構築方針
～概要説明資料～

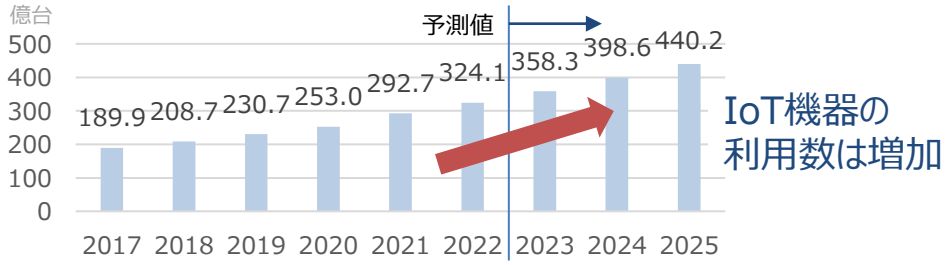
2024年 8月

目次

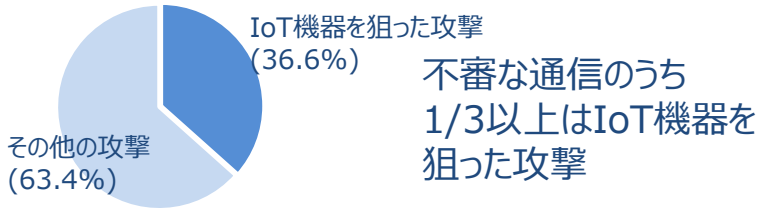
1. 制度構築の背景・検討経緯

- IoT機器の急増に加え、IoT機器を狙った攻撃も多く、**IoT機器の脆弱性を狙ったサイバー脅威が高まってきている**といえる。
- **諸外国でもIoT製品のセキュリティ対策に関する制度検討が進んでおり**、我が国のIoT製品がグローバルマーケットから弾き出されないよう、諸外国の取組状況を考慮する必要がある。
- 我が国も、IoT製品のセキュリティ対策を支援するガイドライン等の発表を行ってきたが、IoT製品ベンダーの自主的な取組を求めるものであった。諸外国の取組も踏まえて、**共通的な物差しで製品のセキュリティ機能を評価・可視化**し、**調達者が求めるセキュリティ水準のIoT製品を容易に選定**できるようにし、適切なセキュリティ対策が講じられているIoT製品が広まる仕組みの構築が必要である。
- こうした観点で制度の検討を行うため、経済産業省は、**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(※1)」を開催し、2024年3月に最終とりまとめを公表**した。最終取りまとめを踏まえ、**制度構築方針案を作成**した。

ネットワークに接続される機器(IoT機器)は増加傾向、IoT機器を狙った攻撃は多い



世界のIoT機器数の推移及び予測(※2)



ダークネットにおける年間観測パケット数の割合(※3)

会議体	主な活動内容
IoT製品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	• 第1回(2022年11月)～第7回(2024年3月)を開催 • 現状の課題、適合性評価制度構築の目的、構築すべき適合性評価制度の内容等について議論 • 2023年5月に中間とりまとめ、**2024年3月に最終とりまとめを公表**
IoT製品のセキュリティ適合性評価制度における基準等の策定に向けたプレ検討委員会	• 第1回(2023年8月)～第4回(2024年2月)を開催 • 構築する適合性評価制度において求めるべきセキュリティ要件（全体）案を議論・策定 • ☆1で求めるセキュリティ要件案、適合基準、評価手順案を議論・策定 • ☆1の基準を用いて、実際の製品に対する適合性評価の検証（実証）を実施

(※1)経済産業省「ワーキンググループ3（IoT製品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）」https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/index.html
(※2)総務省「情報通信白書令和4年版 データ集」、「情報通信白書令和5年版 データ集」の「3章関連データ」より作成
(※3)NICT「NICTER観測レポート2023」の1年間にダークネットで観測されたTCPとUDPの攻撃パケット(調査目的を除く)の上位10種類のポートから、主にIoT機器に関連したポート(23/TCP、22/TCP、8080/TCP、5555/TCP、37215/TCP、5060/UDP)のパケットを集計

2. 目的と位置付け

- IoT製品に対する適合性評価制度を国内で構築し、広く普及させ、そして社会に浸透させるためには、まずは**調達者が自身を守るために、求めるセキュリティ水準のラベルが付与された製品を優先的に選択するようになること**が必要不可欠である。そのうえで、IoT製品ベンダーの積極的なラベル取得を促すため、以下の三つを主目的として制度を構築する。

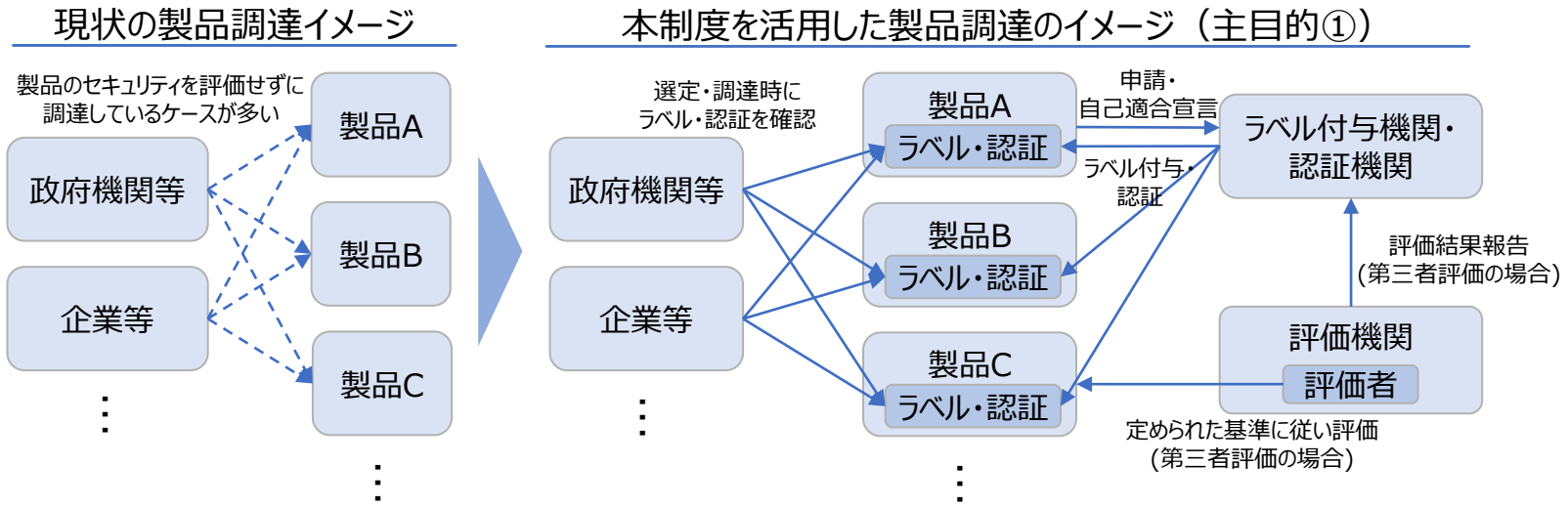
  ① **政府機関や企業等で調達する製品について、共通的な物差しでIoT製品のセキュリティを評価・可視化**できるようにすることで、各組織の求めるセキュリティ水準を満たしたIoT製品の選定・調達を容易にする。

  ② 特定分野のシステムに組み込まれて調達・利用されるIoT製品に求められるセキュリティ要件を定め、必要な認証・ラベルを各業界団体等で指定できるようにすることで、当該**特定分野において求められるセキュリティが確保されたIoT製品のみが採用される**ようにする。

  ③ **諸外国の制度と協調的な制度を構築し、相互承認を図る**ことで、IoT製品を海外に輸出する際に求められる適合性評価にかかるIoT製品ベンダーの負担を軽減する。

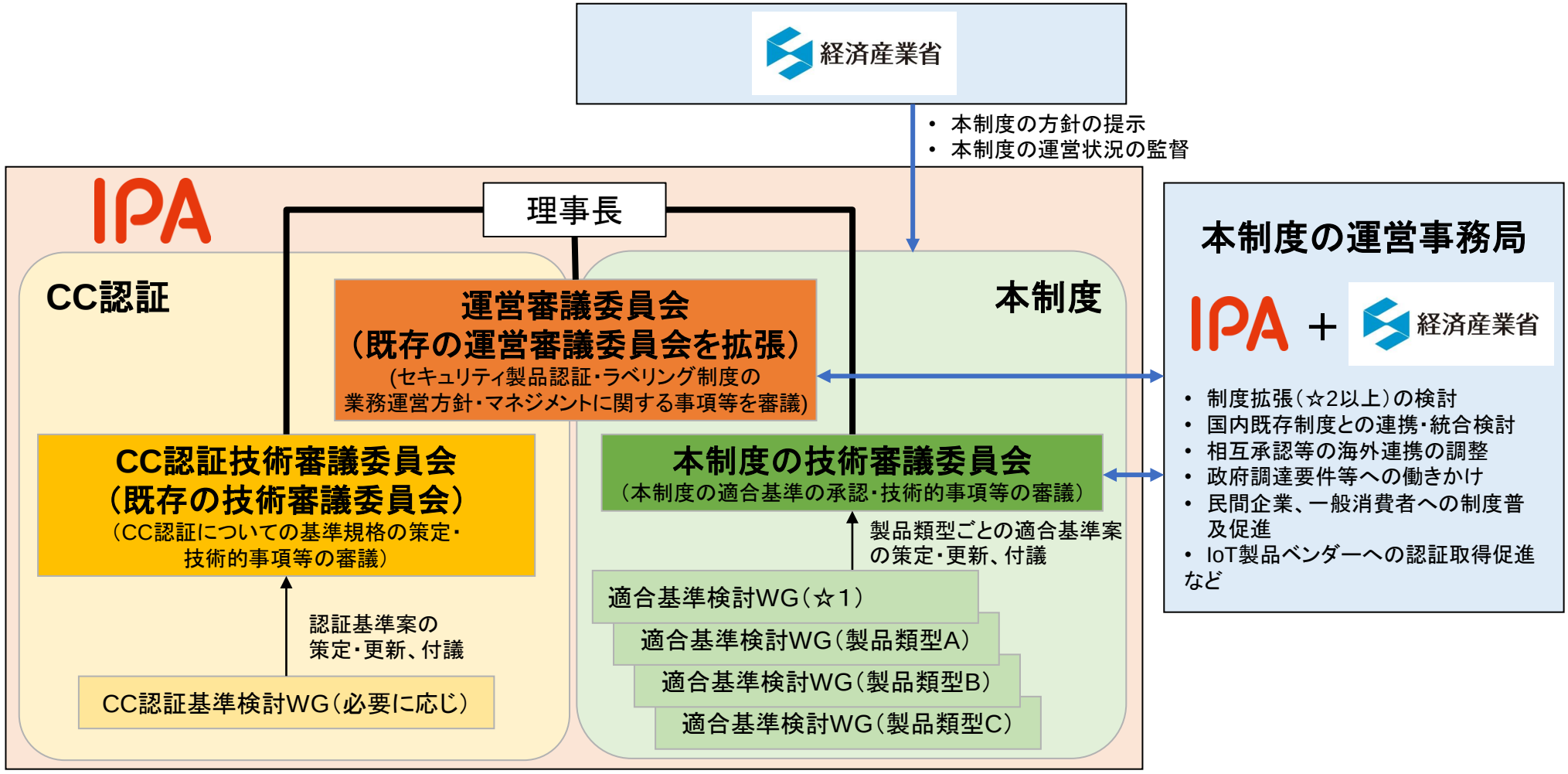
- 本制度は、国内の既存制度と将来的な統合や棲み分け・連携の方針を合意しながら、**任意制度**として構築する。適合性評価を受けた製品に対してセキュリティ要件に応じたラベルを付与することで、製品の付加価値向上に繋げる。

- 主目的①に関して、**まずは政府機関等、重要インフラ事業者、地方公共団体等にラベル付与製品の選定を調達要件に含める**ことを働きかけ、それらのIoT製品ベンダーに本制度のラベルを取得することを促していき、制度が着実に広まる中で、民間の大企業の調達要件での活用、中小企業や消費者への普及を図る



3.1. 運用体制

- 経済産業省の示す基本方針に従い、同省の監督のもと、本制度を構築し、運営する**スキームオーナーをIPA**とする。IPAが運営するJISEC制度を、CC認証のみの対象から本制度を含む形に拡張させる枠組みとする。（現行の運営審議委員会を拡張）
- 本制度の**技術審議委員会**は、プレ委員会を引き継ぐ形で**新設**し、本制度についての**適合基準の承認・技術的事項等を審議**する。
- ☆1および☆2以上の各製品類型ごとの適合基準案の策定は、本制度の技術審議委員会の配下に設置する適合基準検討WGにて行う。**各WGは、当該製品類型のIoT製品ベンダーや主な調達組織、それらの関連機関・団体を中心に構成**する想定である。
- **経済産業省も運営事務局に加わり**、制度の拡張・普及や海外との相互承認・連携等について推進する。

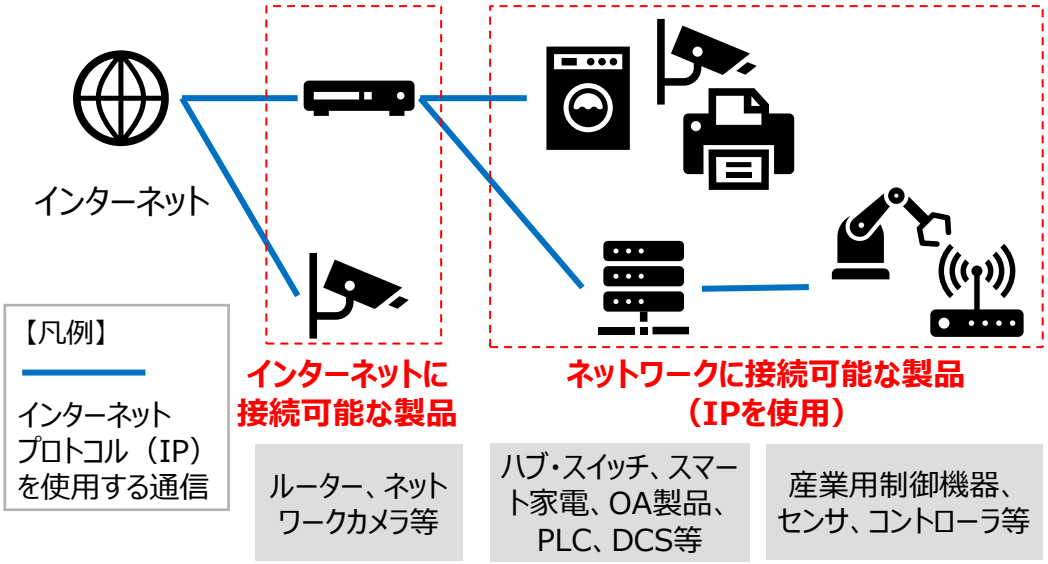


制度構築方針案
3.2～3.3

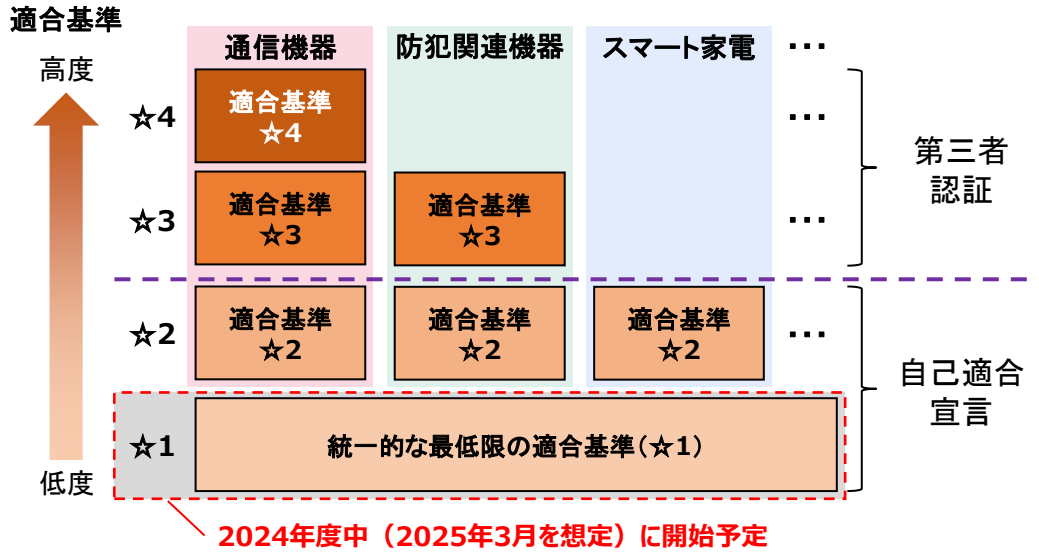
3.2. 対象製品と適合性評価レベル

- **インターネットに直接接続されない製品も含め**、インターネットプロトコルを使用する通信機能を持つ**幅広いIoT製品を制度の対象**とする。また、**消費者向け、企業・産業向けを問わず対象**とする。
- IoT製品共通の最低限の脅威に対応するための基準（☆1）及びIoT製品類型ごとの特徴に応じた基準（☆2～☆4）を定め、**求められるセキュリティ水準に応じた複数の適合性評価レベルを用いた制度**とする。

対象製品の概要(※1)



適合性評価レベル（☆1～☆4）のイメージ

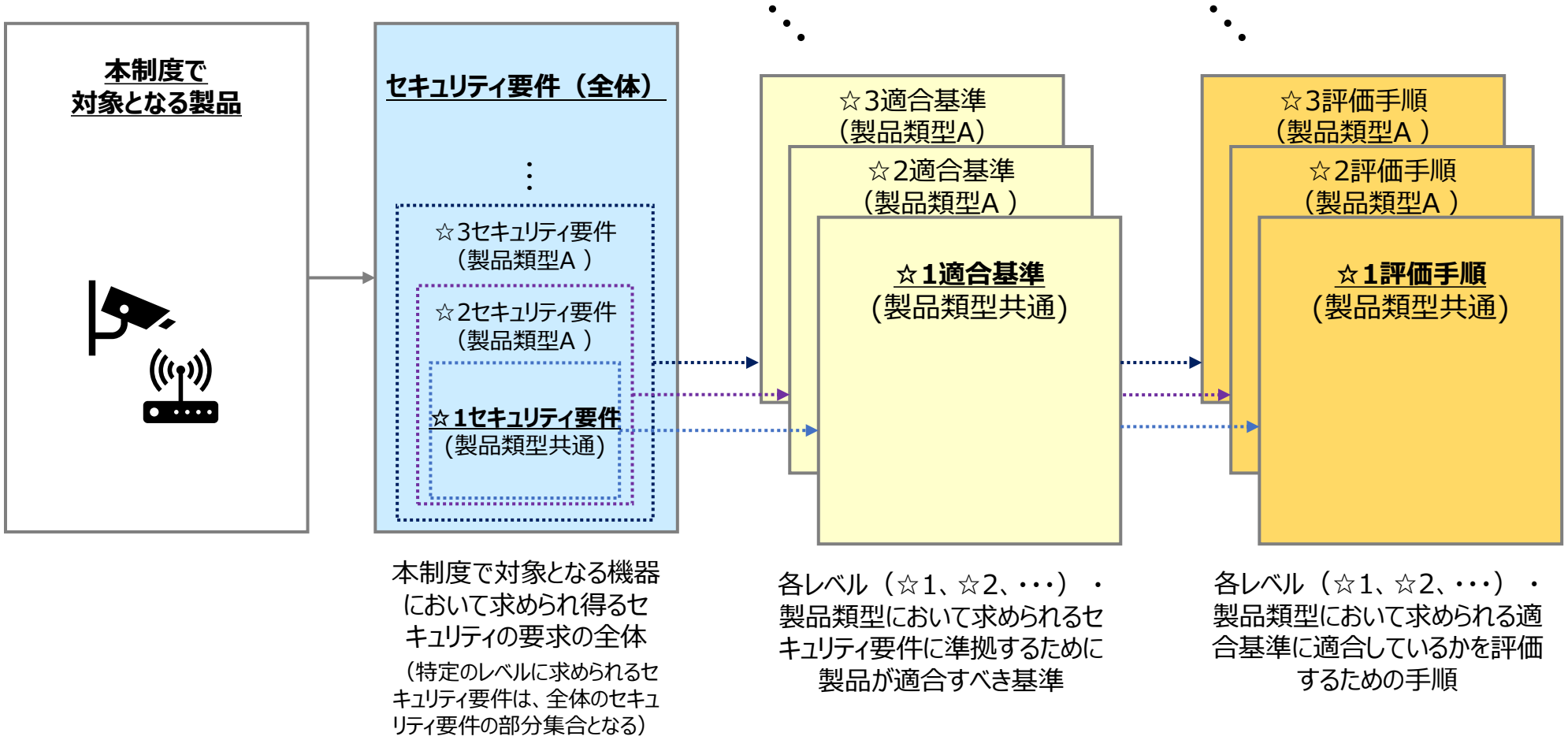


レベル	位置付け	適合基準	評価方式
☆3以上	**政府機関等や重要インフラ事業者、大企業の重要なシステムでの利用を想定**したIoT製品類型ごとの汎用的なセキュリティ要件を定め、それを満たすことを**独立した第三者が評価して示す**もの	製品類型別	第三者認証
☆2	**IoT製品類型ごとの特徴を考慮**し、☆1に追加すべき基本的なセキュリティ要件を定め、それを満たすことを**IoT製品ベンダーが自ら宣言**するもの	製品類型別	自己適合宣言
☆1	IoT製品として共通して求められる**最低限のセキュリティ要件**を定め、それを満たすことを**IoT製品ベンダーが自ら宣言**するもの	製品類型共通	自己適合宣言

(※1)国内外の一部の既存制度と同様に、利用者がソフトウェア製品等により容易にセキュリティ対策を追加することができる汎用的なIT製品（パソコン、タブレット端末、スマートフォン等）は対象外とする。

3.3. セキュリティ要件・適合基準・評価手順（1/3）

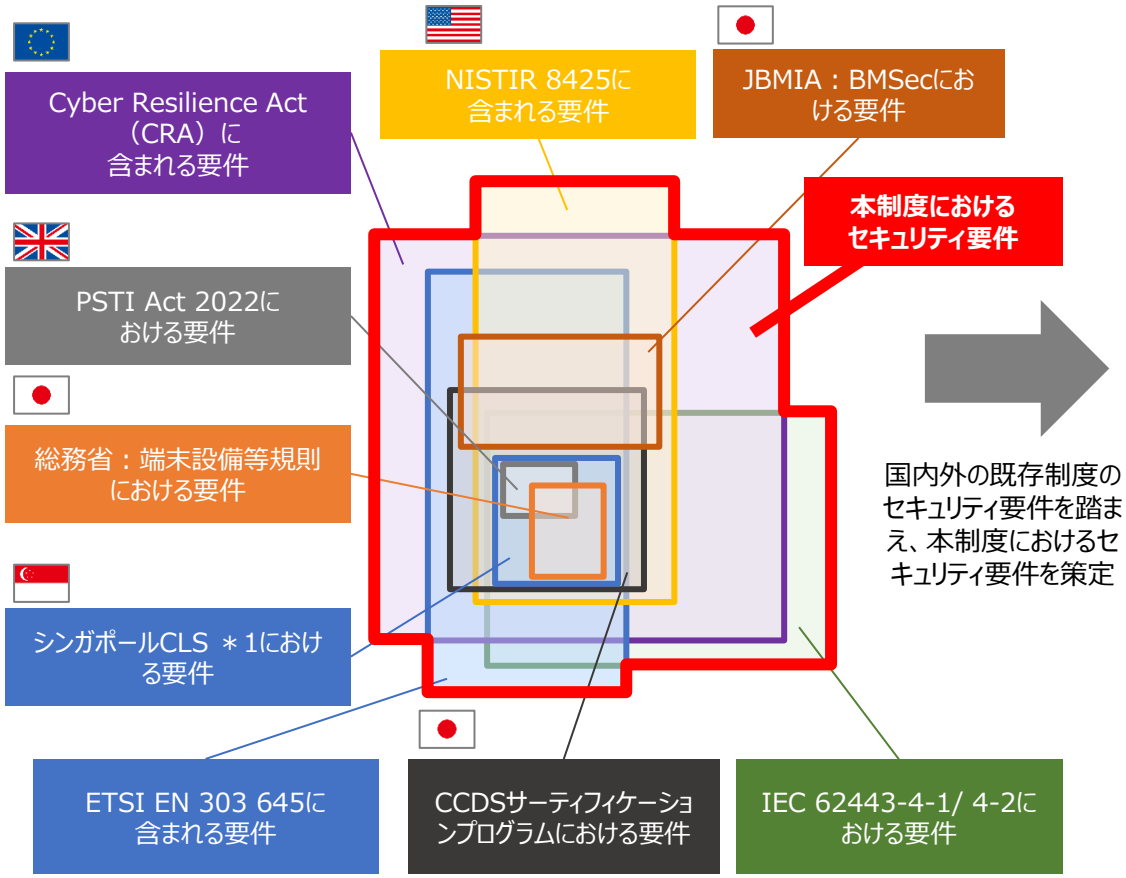
- 実際のIoT製品（10製品）に対する適合性評価の実証結果も踏まえて、プレ委員会にて議論・策定した**☆1（最も低レベルの基準）のセキュリティ要件・適合基準・評価手順の案**を引き継ぎ、本制度の技術審議委員会で制度開始時に利用する☆1の適合基準等を定める。
- ☆2以上のセキュリティ要件・適合基準・評価手順は、**2024年度以降に優先度の高い製品類型を特定**したうえで、**関連する業界団体やワーキンググループと連携**しながら、各適合基準検討WGを設置し、具体的な基準等に関して議論・検討を進めて定める。



3.3. セキュリティ要件・適合基準・評価手順（2/3）

- セキュリティ要件は、本制度で対象となるIoT製品において求められ得る要件の全体（全体リスト）であるため、**ETSI EN 303 645、NISTIR 8425、EU-CRA等の国内外のセキュリティ要件の集合関係**を踏まえ、**重ね合わせの関係にあるセキュリティ要件の全体リストを整理**した。
- セキュリティ要件の具体的な記載について、国際的に広く活用されているETSI EN 303 645の記載を参考にしつつ、プレ委員会で挙げられた意見を踏まえ、表現の見直しを行った。なお、**今後も国際連携や国際標準の検討を見据え、表現やカテゴリ（大項目）の見直し**を行っていく。

諸外国制度において求められるセキュリティ要件の関係性イメージ



本制度におけるセキュリティ要件（全体リスト）のイメージ

セキュリティ要件案	
1. 汎用のデフォルトパスワードを使用しない	1-1. パスワードが使用され、工場出荷時のデフォルト以外の状態にある製品において、すべてのパスワードは、機器ごとに固有であるか、又はユーザによって定義されるものでなければならない。
	1-2. プリインストールされた固有のパスワードを使用する場合、自動化された攻撃への耐性をもつために、パスワードは十分なランダム性を保有しなければならない。
	1-3. 製品に対してユーザを認証するために使用される認証メカニズムは、製品用途の特性等に適した想定するリスクを低減できる技術を使用していなければならない。
	1-4. 製品に対するユーザ認証において、製品は使用される認証値を変更するためのシンプルなメカニズムを、ユーザ又は管理者に提供しなければならない。
	1-5. 製品が、制約のある機器ではない場合、ネットワークを介して行われる認証に対する総当たり攻撃等のブルートフォース攻撃が実行できないようにするメカニズムを保有しなければならない。
2. 脆弱性の報告を管理するための手段を導入する	2-1. 製造業者は、脆弱性開示ポリシーを公開しなければならない。このポリシーには、少なくとも以下が含まれていなければならない ・問題を報告するための連絡先情報 ・以下のタイムラインに関する情報 1) 最初の受領確認 2) 報告された問題が解決されるまでの状況の更新
	・・・
・・・	・・・

3.3. セキュリティ要件・適合基準・評価手順（3/3）

- ☆1で考慮する脅威は、☆1で主に想定する守るべき資産、アタックサーフェスを踏まえ、プレ委員会で整理したものである。
- 想定脅威に対して、☆1で必要なセキュリティ要件を全体のリストから抽出し、国内外の基準を参照して**☆1の適合基準（評価手順としては16項目に集約）を作成**している。

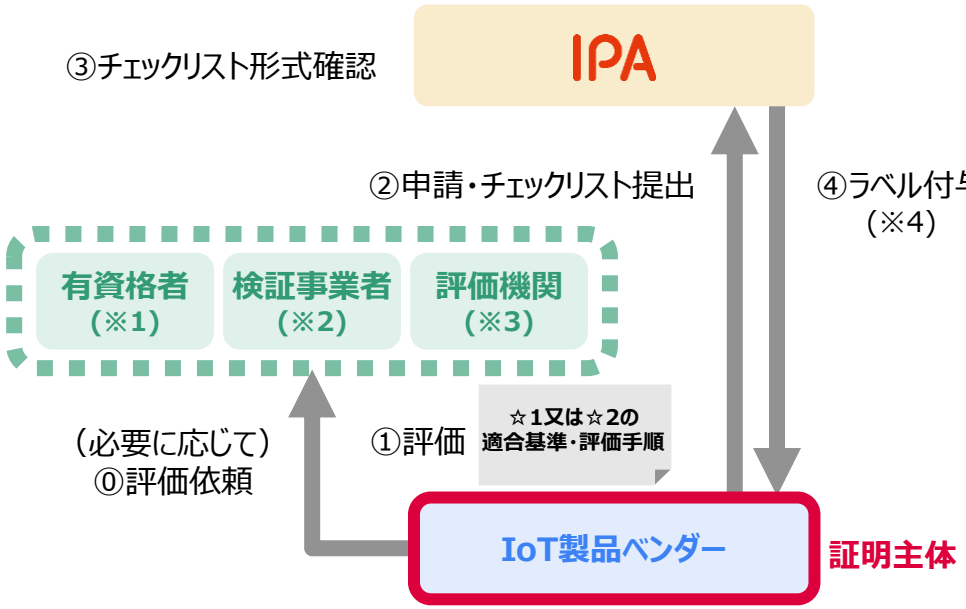
☆1で考慮する主な脅威			脅威に対抗するために☆1で求める適合基準			
			IoT製品に対する適合基準		IoT製品ベンダーに対する適合基準	
			カテゴリ	適合基準の概要	カテゴリ	適合基準の概要
1.	①弱い認証機能により、	外部からの不正アクセスの対象となり、マルウェア感染や踏み台となる攻撃等を受けることで、情報漏えい、改ざん、機能異常の発生につながる脅威	識別・認証、アクセス制御	(1)適切な認証に基づく**アクセス制御**[1-3,5-5] (2)**容易に推測可能なデフォルトパスワードの禁止**[1-2,1-1] (3)パスワード等の認証値の変更機能[1-4] (4)ネットワーク経由のユーザ認証に対する**総当たり攻撃からの保護**[1-5]	情報提供	(16)ユーザへの**セキュアな利用・廃棄方法に関する情報提供**(初期設定手順、セキュリティ更新、サポート期限、安全な廃棄手順等)[17-12,17-3,17-5,17-8,17-10]
	②脆弱性の放置により、		脆弱性対策、ソフトウェア更新	(6)ソフトウェアコンポーネントのアップデート機能[3-1,3-2] (7)**容易かつ分かりやすいアップデート手順**[3-3] (8)アップデート前のソフトウェアの完全性の確認機能[3-7,3-2,3-10] (10)ユーザが型式番号を認識可能とする記載・機能[3-16]	情報・問い合わせの受付、情報提供	(5)連絡先・手続き等の**脆弱性開示ポリシーの公開**[2-1] (9)セキュリティアップデートの優先度決定方針の文書化[3-8]
	③未使用インタフェースの有効化により、		インターフェイスへの論理アクセス	(13)**不要かつリスクの高いインタフェースの無効化**(物理的・論理的な通信ポート等)[6-1]	－	－
	①～③共通		データ保護	(11)製品に保存される守るべき情報の保護(**保存データの暗号化、匿名化**等)[4-1]	－	－
2. 機器の通信が盗聴され、守るべき情報が漏えいする脅威			データ保護	(12)ネットワーク経由で伝送される守るべき情報の保護(**通信の暗号化、保護された通信環境の利用**等)[5-1,5-7]	－	－
3. 廃棄・転売等された機器から、守るべき情報が漏えいする脅威			データ保護	(15)**製品内に保存される守るべき情報の削除機能**[11-1]	情報提供	※(16)に含む
4. ネットワーク切断や停電等の事象が発生した際に、セキュリティ機能に異常が発生する脅威			レジリエンス向上	(14) 停電・ネットワーク停止等からの復旧時の**認証情報やソフトウェア設定の維持**(初期状態に戻らないこと)[9-1]	－	－

※「適合基準の概要」欄の先頭の"(N)"は対応する☆1評価項目番号を、末尾の"[N-N]"は対応するセキュリティ要件の番号(複数の場合、代表的な要件を先頭に記載)を示す。
※ 複数の脅威に対応するための適合基準もあるが、代表的なものにマッピングしている。

3.4. 適合性評価の主体

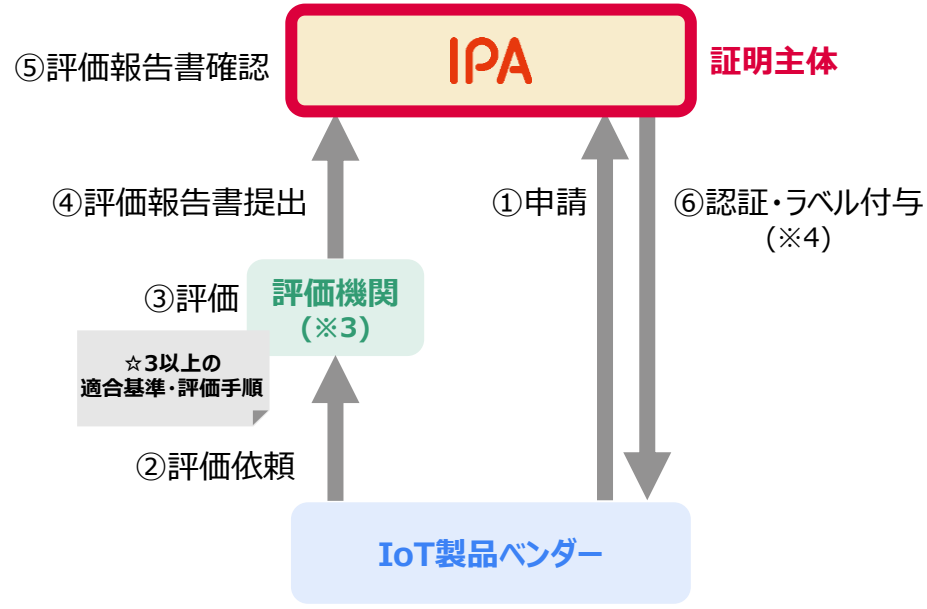
- 制度を広く普及させるため**☆1、☆2は自己適合宣言によるラベル付与**とし、高い信頼性が求められる**☆3以上は独立した第三者による評価を受ける第三者認証**とする。
- ☆1、☆2では、IoT製品ベンダーの自己評価に加え、**有資格者(※1)や検証事業者(※2)、評価機関等への評価の委託も可能**である。
- ☆3以上では、**ISO/IEC17025に基づく本制度の評価機関認定(※3)を受けた評価機関による評価**を求める。

☆1、☆2（自己適合宣言）



① IoT製品ベンダーは、 ☆1又は☆2の適合基準・評価手順を用いて評価を実施し、チェックリストを作成する。
なお、有資格者や検証事業者、評価機関等に評価を委託してもよい。
※ ☆２において有資格者や検証事業者、評価機関による評価実施を求めるかは別途検討
② IoT製品ベンダーは、IPAに申請を行い、チェックリストを提出する。
③ IPAは、チェックリストの形式確認を行う。
④ IPAは、申請されたIoT製品に対し、ラベルを付与する。

☆3以上（第三者認証）



① IoT製品ベンダーは、IPAに申請を行う。
② IoT製品ベンダーは、評価機関に対して、評価依頼を行う。
③ 評価機関は、☆3以上の適合基準・評価手順を用いて評価を実施する。
④ 評価機関は、評価報告書をIPAに提出する。
⑤ IPAは、認証機関として、評価報告書の内容に問題がないか確認する。
⑥ IPAは、申請されたIoT製品に対し、認証・ラベルを付与する。

(※1)指定資格の保有者（情報処理安全確保支援士等）が、IoTセキュリティ評価に関する研修受講完了又は評価ガイドラインを理解していることの宣誓したうえで、評価又は評価結果の確認を実施した場合に「有資格者」による評価とする。
(※2)情報セキュリティサービス基準への適合性について審査及び登録する情報セキュリティサービス基準審査登録制度の機器検証サービス（2023年9月より募集開始）にサービスが登録されている事業者を「検証事業者」とする。
(※3)製品評価技術基盤機構（NITE）の製品評価技術基盤機構認定制度(ASNITE)の中に、本制度の☆3以上の評価を行える事業者についてISO/IEC17025に基づく評価機関認定制度を設け（2024年度以降、別途検討）、適切な能力及び体制を整備した事業者を「評価機関」として認定する。
(※4) IPAは、ラベル取得の申請に対して、ラベル発行前にサプライチェーン・リスクについて経済産業省を含めた政府関係機関に照会をかけ、その照会結果に基づきラベルを付与する。

3.5. ラベルの意味合いと信頼性確保の仕組み

制度構築方針案
3.6～3.7

- 本制度の**ラベルは、あくまで定められた適合基準への適合を示すもの**であり、ラベルが付与されているからといって、IoT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ものではない。
- 本制度は任意制度であるため、**ラベルの表示義務は設けない**。製品本体、パッケージ、マニュアル、パンフレット、Webサイト等に掲載する場合は、**本制度のロゴ**及びラベル付与製品毎の**情報提供ページのURLを埋め込んだQRコードを掲載**する。
- 自己適合宣言の有効期限は**ラベル取得日を起点として最大2年間**とし、その後ラベルを継続する場合は**自己適合宣言**を再度行う。
- **スキームオーナーはラベル付与製品に対して検査やサーベイランスを行える権利を有する**。☆1では、コストの観点から定期的なサーベイランスは行わず、**基準への適合に疑義が生じた場合に、必要に応じ、証跡提出の要求やサーベイランス**の実施を行う。

各評価レベルにおけるラベルの意味合い

評価レベル	ラベルの意味合い
☆1、☆2 （自己適合宣言）	ラベル取得時点において定められた適合基準へ適合していることについて、IoT製品ベンダー自らが宣言したことを示すもの。（証明主体はIoT製品ベンダー自身） IPAはラベル付与機関として評価結果を記載したチェックリストの形式確認は行うが、IoT製品のセキュリティ適合性等を、IPAが認証するものではない。
☆3以上 （第三者認証）	ラベル取得時点（再評定時を含む）において定められた適合基準へ適合していることについて、認証機関となるIPAが認証したことを示すもの。（証明主体はIPA） IPAは、独立した第三者である評価機関が本制度の定める適合基準及び評価手順に従い評価した結果を確認したうえで、当該基準への適合に対する認証を行う。ただし、IPAは、評価機関による評価の結果を適切に確認する責任を負う一方、ラベルを取得した当該IoT製品に対して、明示あるいは黙示を問わず、いかなる保証も行わない。

情報提供ページの掲載情報案

掲載情報	掲載内容
本制度の概要	• 本制度の概要及び詳細説明HPのURL
製品情報	• 製品名 • 型式番号 • IoT製品の製造業者名　※公開/非公開は任意 • 製造国又は地域　※公開/非公開は任意 • 製品概要 • 製品WebサイトのURL • 製品の問い合わせ先 • 他認証の認証番号等
ラベル情報	• ラベル識別番号 • 当該製品の適合性評価レベル（☆1～☆4） • 当該製品の製品類型の名称　※☆2～☆4の場合 • 評価された適合基準のバージョン • 適合評価結果（チェックリスト又は評価報告書等） • ラベルステータス情報 • ラベル発行・更新日 • ラベルの有効期限 • 申請者名 • 評価者区分
安全情報	• 当該製品に関わる脆弱性情報 • 脆弱性の報告窓口のURL
その他セキュリティ関連情報	• 必要があれば、IoT製品ベンダーから調達者に向けたセキュリティ関連情報

4.1. 調達要件への反映に関する働きかけ

制度構築方針案
3.8.1

- **政府機関等、重要インフラ事業者、地方公共団体**におけるIoT製品調達時に、用途やそのリスクに応じて、**本制度のラベル付与製品を選定・調達することを求めていく**ように、関係者と以下の方向性で調整を進める。
- 調達時にラベル付与製品が普及しておらず、**セキュリティ面以外での比較ができなくなることを避ける**ため、これらの組織で主に調達されるIoT製品を中心に、その**関連団体に対して、本制度との連携や会員企業への積極的なラベル取得の働きかけの賛同**を得る。

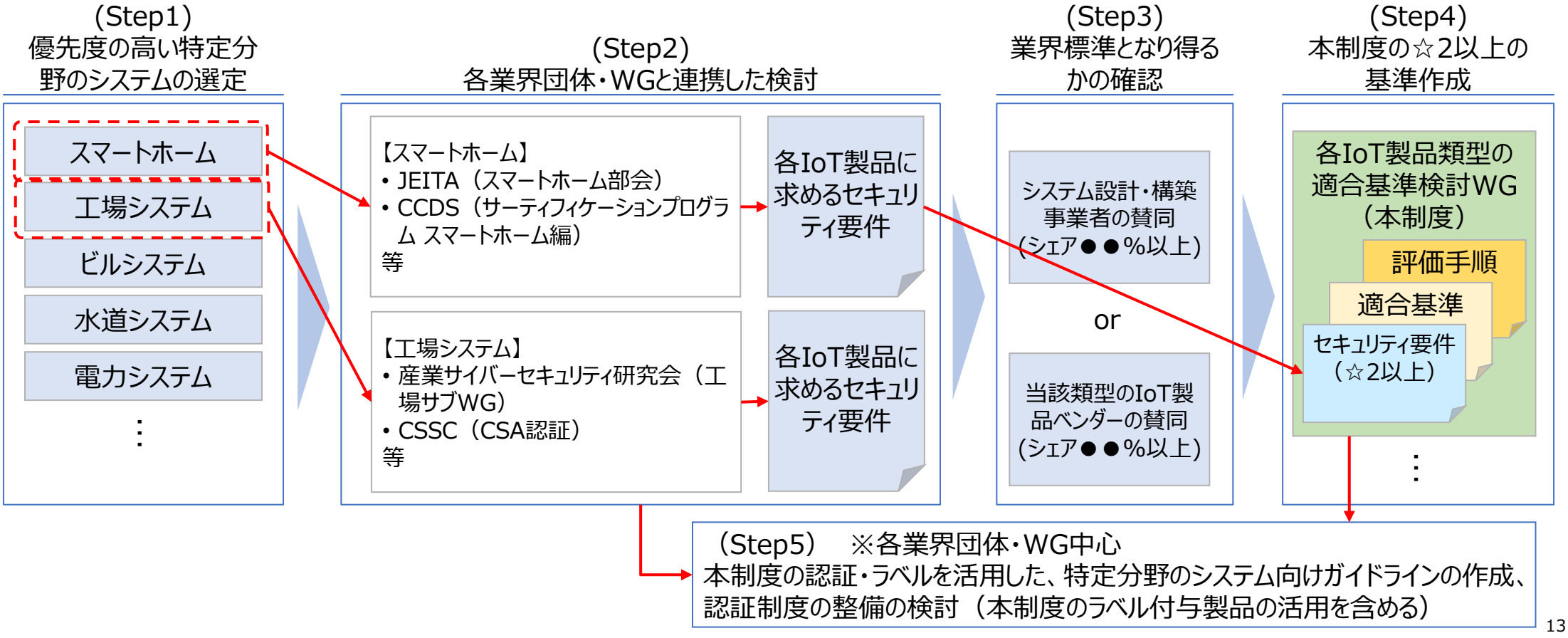
対象	主な調整先	調整状況・方向性
政府機関等	NISC 政府機関総合対策グループ 基本戦略第2グループ	• **2024年度以降の改定に合わせて、「政府機関等のサイバーセキュリティ対策のための統一基準」およびそのガイドラインに**、情報システムの重要度に応じて**「重要度：低」は☆1以上、「重要度：高～中」は少なくとも☆3以上のIoT製品を各機関等の選定基準に含める**ことの追加を検討する。 • ラベル取得済み製品が普及する時期をめどに、**政府機関等ではラベル取得済みIoT製品の調達を必須化**する方針。 • 統一基準やガイドラインへの反映に向けて、今後、各府省庁の参加する会議の場などで、本制度を活用した製品調達に関する周知を行っていくことも重要となる。
重要インフラ事業者	NISC 重要インフラ第1グループ	• 調達要件に関する記載は、**「重要インフラのサイバーセキュリティに係る行動計画」に紐づく安全基準等策定指針および手引書に入れる**こととなる。制度立ち上げのタイミングに合わせて、**2024年度以降、専門調査会(※1)の議案に指針への反映を入れていく**。 • 重要インフラ事業者への調達ルールへの反映に関する働きかけおよび各業界固有のシステムで用いられているIoT製品への☆2以上の必要性の確認は、**四半期毎に実施しているセプターカウンシル(※2)の運営委員会を活用**する。
地方公共団体	総務省 デジタル基盤推進室	• 政府統一基準群に記載された後、地方公共団体の状況に合わせて、**地方公共団体セキュリティポリシーガイドラインに記載**することが通例となっている。 • **2024年度以降、検討会(※3)、自治体意見照会、パブコメを経て改定を検討**することとなる。

(※1)NISC「重要インフラ専門調査会」 https://www.nisc.go.jp/council/cs/ciip/index.html
(※2)NISC「セプターカウンシル総会資料（セプターカウンシルの概要）」 https://www.nisc.go.jp/policy/group/infra/siryou/#si09
(※3)総務省「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の改定等に係る検討会」 https://www.soumu.go.jp/main_sosiki/kenkyu/chiho_security_r03/index.html

制度構築方針案
3.8.2

4.2. 特定分野のシステムに関する業界団体・WGとの連携

- 製品単体で比較されず、特定分野のシステムに組み込まれて調達されるIoT製品について、以下の観点で**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や☆**2以上の適合基準をその必要性も含めて検討**を検討する。
  - 意識しないまま**セキュリティ対策が十分でないIoT製品を利用している中小企業や消費者が多い**と考えられる分野のシステム
  - インシデント発生時の社会的な影響が大きい**重要インフラ分野**のシステム
- 各分野において、IoT機器を選定する立場の事業者又は当該IoT製品を製造するベンダーから、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以上の整備を進める。
- 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。



4.3. 諸外国制度との連携

- 諸外国においても同様のIoT製品の適合性評価制度の検討が進んでいる。国内IoT製品ベンダーの負担を抑えるため、主要国制度の基準も参考にしながら本制度の基準を検討し、**相互承認の調整**を図る。
- ☆1開始の正式案内時に制度が既に導入されている**シンガポールと英国とは、案内時に相互承認の方向性を提示**する予定。正式案内時に制度設計途中の見込みである**欧米については、順次方向性を公表**する。

国・地域	日本	シンガポール	英国	米国	EU
制度名	検討中	Cybersecurity Labelling Scheme (CLS)	Product Security and Telecommunication Infrastructure Act (PSTI法)	U.S. Cyber Trust Mark	Cyber Resilience Act (CRA) ※欧州委員会草案の内容
開始時期	• ☆1：2024年度下期(2025年3月)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（報告義務を除き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	消費者向け無線IoT機器	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（ただし、総務省技適の要件、CCDSの要件も参照のほか、事務局にて記載内容を検討）	• ＊1：ETSI EN 303 645の基準の一部(※1) • ＊2：＊2の基準に加え、ETSI EN 303 645の基準の一部(※2) • ＊3及び＊4：＊2の基準に加え、IMDA「IoT Cyber Security Guide」の基準	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	• 製造者への「セキュリティ特性要件に従った上市前の設計・開発・製造」、「上市後の積極的に悪用された脆弱性・インシデントの報告」等を義務付ける予定 • 法案の内容について（欧州委員会・議会・理事会間で）政治合意済。発効後、基準策定機関に対して法案に伴う基準の策定が命じられる予定。
評価方法	• ☆1、☆2：自己適合宣言 • ☆3以上：第三者	• ＊1及び＊2：自己適合宣言 • ＊3及び＊4：自己適合宣言及び評価機関による試験	自己適合宣言	第三者認証	• 「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) ETSI EN 303 645のサイバーセキュリティ規定5.1-1、5.1-2、5.1-3、5.1-4、5.1-5、5.2-1、5.3-2、5.3-3、5.3-7、5.3-8、5.3-10、5.3-13、5.3-16
(※2) ETSI EN 303 645のサイバーセキュリティ規定5.4-1、5.4-2、5.4-3、5.4-4、5.5-5、5.5-7、5.5-8、5.6-1、5.6-2、5.6-4、5.8-2、5.8-3、5.11-1、5.13-1及びデータ保護規定6.1、6.2、6.3、6.5

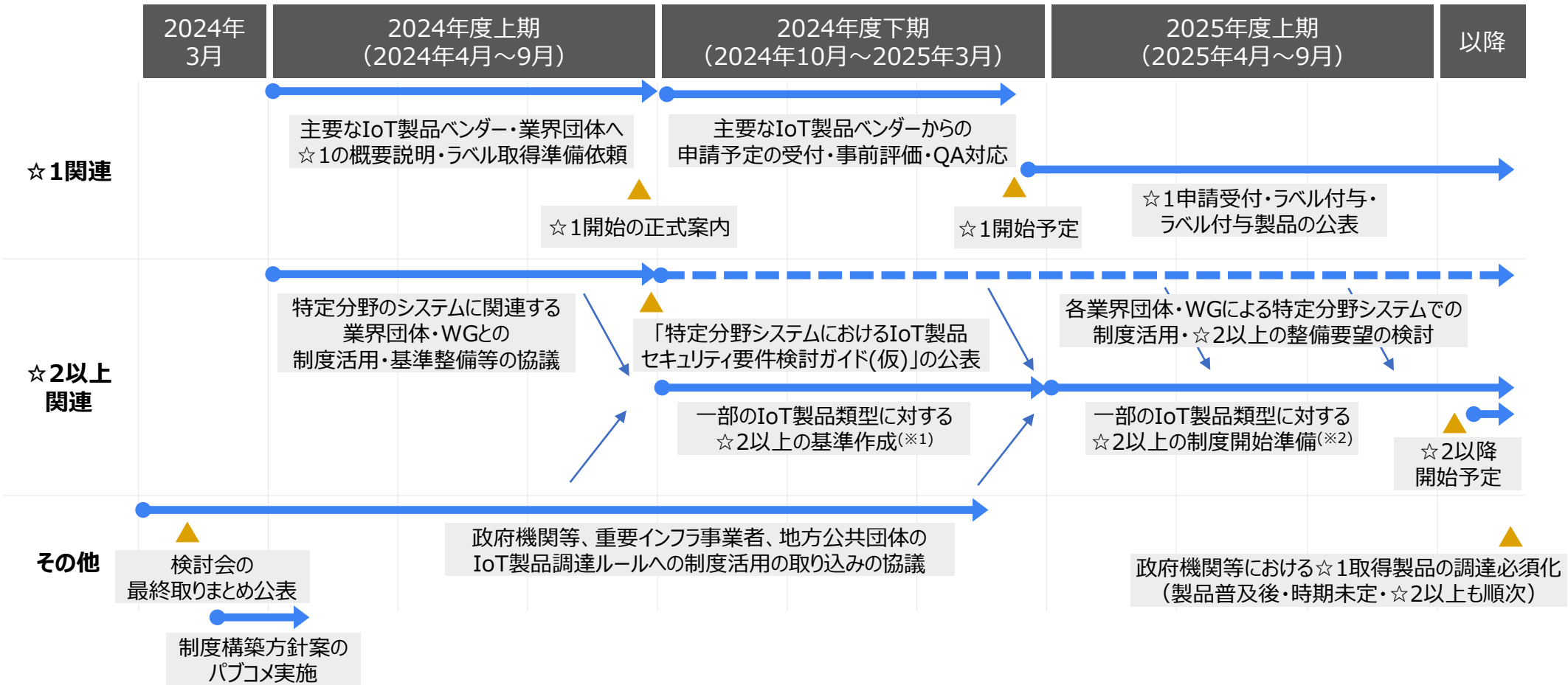
5. 制度発展に向けた施策

- 制度を普及させ、社会に浸透させていくため、以下のような施策の実施を検討していく。

分類	検討すべき施策の概要
IoT製品ベンダーへのラベル取得促進策	• IoT製品ベンダーに対する制度に関する説明や、**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、評価ガイド等）の提供** • 自己評価を行う際に活用できる**自動化ツールの提供** • **各種補助金制度との連携**や申請費用・第三者評価費用の割引キャンペーンの実施 • 海外のIoT製品ベンダーへの本制度の普及
調達者・利用者への制度普及促進策	• IoT製品ベンダーや**小売り事業者等と連携**して、本制度の目的、ラベルの意味合い等を消費者に伝えることによるラベル付与製品の需要喚起 • **各種補助金制度との連携**等による中小企業・小規模事業者等の調達者への需要喚起
評価機関・検証事業者への支援	• 適切な能力及び体制を整備した事業者を**「評価機関」として認定する制度**の整備 • 自己適合宣言における評価機関・検証事業者の活用促進 ➢ 自己適合宣言の評価に必要な能力や前提条件、想定工数等の提示 ➢ ラベル付与製品毎の**情報提供ページへの第三者評価であることの掲載** ➢ 中小企業のIoT製品ベンダー向けに、評価機関・検証事業者に委託して**自己適合宣言を実施する場合の補助金**等の支援
リスクに対応するための資源の確保策	• 事案が発生時に損害を広く分散するため、**商品付帯方式サイバー保険**との連携 • **情報セキュリティ早期警戒パートナーシップとの連携やSBOMの活用**等による、ラベル付与製品に関わる脆弱性関連情報の適切な共有体制、早期対応の仕組みの構築
制度全体の効率化	• 審査から登録廃止に至る**業務プロセスの効率化・簡素化**

6. 今後のスケジュール

- ☆**1**は、2024年半ばに制度開始の正式案内を行い、**2024年度中（2025年3月の想定）に制度の開始**を目指す。
- ☆**2以上**は、業界団体・WGとの制度活用・基準整備等の協議を行い、2024年度下期に一部のIoT製品類型に対する基準を作成する想定。**2025年度下期以降に当該製品類型に対する☆2以上の制度の開始**を目指す。
- 2024年度に、**政府機関等へのラベル取得済みIoT製品調達の必須化**の調整及び重要インフラ事業者・地方公共団体へのIoT製品調達ルールへの制度活用の取り込みの働きかけを行う。



(※1)優先度の高い製品類型(2～3種の想定)が対象、基準が完成次第、順次☆2以降の開始予定を案内
(※2)以降、対象となる製品類型を順次拡張

（参考）☆１のセキュリティ要件（1/2）

大項目	☆1セキュリティ要件案	☆1での抽出理由
1. 汎用のデフォルトパスワードを使用しない	1-1. パスワードが使用され、工場出荷時のデフォルト以外の状態にある製品において、すべてのパスワードは、機器ごとに固有であるか、又はユーザによって定義されるものでなければならない。	脅威1-①に対応するために、容易に推測できるパスワードが設定できない仕組みを導入することが求められるため。
	1-2. プリインストールされた固有のパスワードを使用する場合、自動化された攻撃への耐性をもつために、パスワードは十分なランダム性を保有しなければならない。	脅威1-①に対応するために、容易に推測できるパスワードが設定できない仕組みを導入することが求められるため。
	1-3. 製品に対してユーザを認証するために使用される認証メカニズムは、製品用途の特性等に適した想定するリスクを低減できる技術を使用していなければならない。	脅威1-①に対応するために、セキュアな認証の仕組みを提供することが求められるため。
	1-4. 製品に対するユーザ認証において、製品は使用される認証値を変更するためのシンプルなメカニズムを、ユーザ又は管理者に提供しなければならない。	脅威1-①に対応するために、セキュアな認証の仕組みを提供することが求められるため。
	1-5. 製品が、制約のある機器ではない場合、ネットワークを介して行われる認証に対する総当たり攻撃等のブルートフォース攻撃が実行できないようにするメカニズムを保有しなければならない。	脅威1-①に対応するために、ブルートフォースによる認証試行を防ぐ仕組みを提供することが求められるため。
2. 脆弱性の報告を管理するための手段を導入する	2-1. 製造業者は、脆弱性開示ポリシーを公開しなければならない。このポリシーには、少なくとも以下が含まれていなければならない ・問題を報告するための連絡先情報 ・以下のタイムラインに関する情報 1) 最初の受領確認 2) 報告された問題が解決されるまでの状況の更新	脅威1-②に対応するために、製品に関する情報及び製品の脆弱性に関する情報を提供することが求められるため。
3. ソフトウェアを最新の状態に保つ	3-1. 製品に含まれる特定のソフトウェアコンポーネントについて、アップデート可能にしなければならない。	脅威1-②に対応するために、ソフトウェアコンポーネントがアップデート可能な仕組みを導入することが求められるため。
	3-2. 製品が、制約のある機器でない場合、アップデートをセキュアにインストールするためのアップデートメカニズムを備えていなければならない。	脅威1-②に対応するために、ソフトウェアコンポーネントがアップデート可能な仕組みを導入することが求められるため。
	3-3. 製品においてアップデートメカニズムが実装されている場合、そのアップデートは、ユーザが簡単に適用できるものでなければならない。	脅威1-②に対応するために、ソフトウェアコンポーネントがアップデート可能な仕組みを導入することが求められるため。
	3-7. 製品においてアップデートメカニズムが実装されている場合、セキュアなアップデートメカニズムを容易にするために、ベストプラクティスの暗号技術を使用しなければならない。	脅威1-②に対応するために、ソフトウェアコンポーネントがアップデート可能な仕組みを導入することが求められるため。
	3-8. 製品においてアップデートメカニズムが実装されている場合、セキュリティアップデートは、適時でなければならない。	脅威1-②に対応するために、ソフトウェアコンポーネントがアップデート可能な仕組みを導入することが求められるため。
	3-10. 製品においてアップデートメカニズムが実装され、ソフトウェアアップデートがネットワークインタフェースを介して配信される場合、製品は、信頼関係を介して各アップデートの真正性及び完全性を検証しなければならない。	脅威1-②に対応するために、ソフトウェアコンポーネントがアップデート可能な仕組みを導入することが求められるため。
	3-16. 製品のモデル名称は、製品上のラベル又は物理的インタフェースを介して、ユーザに対して明確に認識可能でなければならない。	脅威1-②に対応するために、製品に関する情報及び製品の脆弱性に関する情報を提供することが求められるため。

（参考）☆１のセキュリティ要件（2/2）

大項目	☆1セキュリティ要件案	☆1での抽出理由
4. 機密セキュリティパラメータをセキュアに保存する	4-1. 製品のストレージにある機密セキュリティパラメータは、製品によってセキュアに保存されなければならない。	脅威1に対応するために、機器が保有する守るべき情報を保護するための機能を提供することが求められるため。
5. セキュアに通信する	5-1. 製品は、ベストプラクティスの暗号技術を使用してセキュアに通信をしなくてはならない。	脅威2に対応するために、インターネット経由で伝送される守るべき情報を保護するために情報の漏えいや変更に対する保護対策を実装することが求められるため。
	5-5. ネットワークインタフェースを介してセキュリティに関連する設定の変更を可能にする製品の機能は、認証後にのみアクセス可能でなければならない。ただし、製品が依存するネットワークサービスプロトコルで、製品の動作に必要な設定を製造業者が保証できない場合は、例外とする。	脅威1-①に対応するために、セキュアな認証の仕組みを提供することが求められるため。
	5-7. 製品は、リモートアクセス可能なネットワークインタフェースを介して通信される重要なセキュリティパラメータの機密性を保護しなければならない。	脅威2に対応するために、インターネット経由で伝送される守るべき情報を保護するために情報の漏えいや変更に対する保護対策を実装することが求められるため。
6. 露出した攻撃面を最小化する	6-1. すべての未使用の物理的インタフェース及び論理的インタフェースは無効化しなければならない。	脅威1-③に対応するために、不要なインタフェースを無効化することが求められるため。また、脅威1-②に対応するために、深刻度の高い既知の脆弱性及び主要なCWEに対する対策を行うことが求められるため。
9. 停止に対してレジリエントなシステムにする	9-1. データネットワークと電源の停止の可能性を考慮して、レジリエンスを製品とサービスに組み込まなければならない。	脅威4に対応するために、ネットワーク切断や停電等の事象が発生し、復旧した場合でも、認証情報やソフトウェア設定は初期状態に戻らず、電源OFF前の状態を提供することが求められるため。
11. ユーザが簡単にデータを消去できるようにする	11-1. ユーザは、簡単な方法で製品からユーザデータを消去できるような機能を提供されなければならない。	脅威3に対応するために、機器の利用中に機器内に保存された守るべき情報を製品本体や付随サービスを介して削除できる機能を提供することが求められるため。
17. 製品に関する情報提供を行う	17-2. 製造業者は、製品をセキュアに設定・利用・廃棄する方法について、ユーザに提供しなければならない。	脅威1-①に対応するために、製品のセキュアな利用方法に関する情報を提供することが求められるため。
	17-3. アップデートメカニズムが実装されている場合、製造業者は、セキュリティアップデートが必要であることを、そのアップデートによって軽減されるリスクに関する情報とともに、認識可能で明らかな方法でユーザに通知しなければならない。	脅威1-②に対応するために、セキュリティパッチの適用方法に関する情報を提供することが求められるため。
	17-5. 製造者等は、ユーザが製品を廃棄する手順について、指定された方法でユーザに提供しなければならない。	脅威3に対応するために、製品のセキュアな廃棄方法に関する情報を提供することが求められるため。
	17-8. 製造業者は、定められたサポート期間を、ユーザにとって明確で透明性のある方法で公表しなければならない。	脅威1-①に対応するために、製品のセキュアな利用方法に関する情報を提供することが求められるため。
	17-10. 製造者等は、脅威を引き起こす可能性がある製品の利用状況に関する情報について、指定された方法でユーザに提供しなければならない。	脅威1-①に対応するために、製品のセキュアな利用方法に関する情報を提供することが求められるため。