経済産業省

資料５－２

電力SWG向け
IoT製品に対するセキュリティ適合性評価制度
（JC-STAR制度）の概要

2024年10月

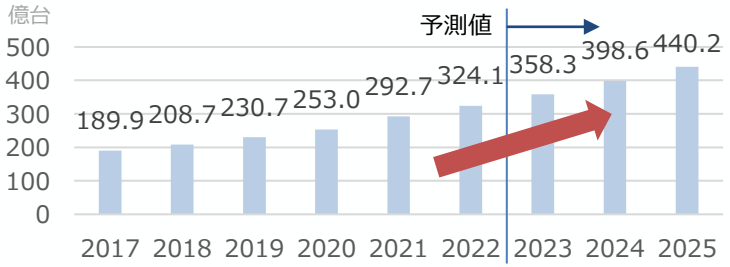
経済産業省 商務情報政策局
サイバーセキュリティ課

IoT機器の利用拡大に伴い増加するリスク・経営への影響

- IoT機器の増加に加え、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おり、経営に影響を与えるセキュリティインシデントも起きている。

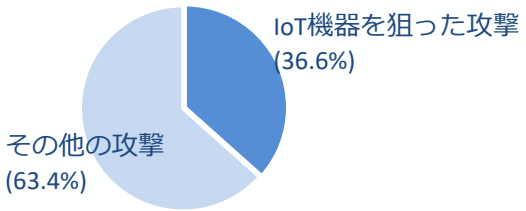
IoT機器の増加

〔IoT機器の増加〕



世界のIoT機器数の推移及び予測(※1)

〔IoT機器を狙った攻撃の割合〕



ダークネットにおける年間観測パケット数の割合(※2)

IoTのセキュリティインシデントによる経営への影響(※3)

操業停止や逸失利益の発生を含む事業への直接的な影響

半導体製造工場の制御装置に対する攻撃によって、**3日間の操業停止、営業機会損失が発生(売上高(四半期)の3%損失)**[台湾:2018]

石油化学工場の安全計装システムを対象とした攻撃による**操業停止。プラント爆発のおそれ**[サウジアラビア:2017]

脆弱性対応や損害賠償を含む追加費用の発生

脆弱性発見による自動車140万台のリコールの発生。脆弱性等の対応で、**2億9900万ユーロ(約394億円)の赤字を計上**(四半期の最終損益) [米国:2015]

評判の低下等より生じる競合優位性の低下

高級ホテルで客室のカードキー発行システムがランサムウェアに感染し、一切のシステム操作が不可能となった。客室扉の施錠、開錠が不可能となり、宿泊客が閉め出される事態が発生。**サービスの品質が著しく低下**[オーストリア: 2017]

(※1)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
(※2)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
(※3)各種公開情報に基づき経済産業省作成

IoT製品に対するセキュリティ適合性評価制度の概要

- 2022年11月より検討会(※1)を開催し、2024年3～4月のパブコメを経て、8月に制度構築方針を公表。**9月30日にIPAから「JC-STAR」という制度名にて制度開始の案内**(※2)を実施。
- **★１については2024年度中の制度開始**を予定。**政府調達等の要件**等とすべく関係省庁と議論中。**米欧等の諸外国との制度調和**を図るため議論中。

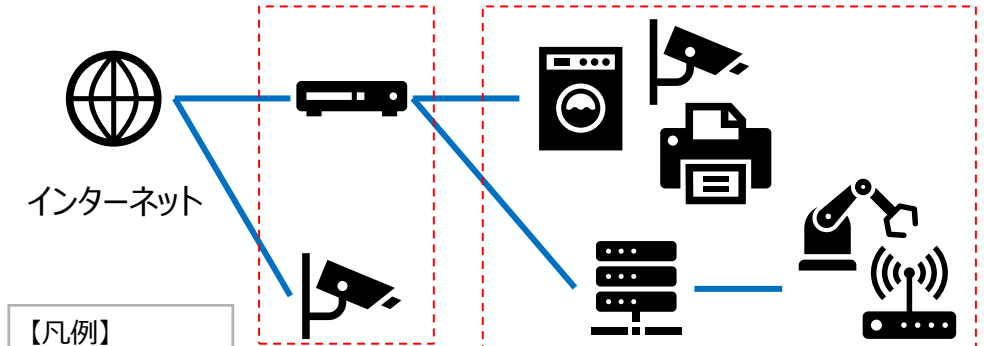
制度名称・ロゴ・ラベル

セキュリティ要件適合評価
及びラベリング制度
JC-STAR
(Labeling Scheme based on
Japan Cyber-Security Technical
Assessment Requirements)

JC-STAR

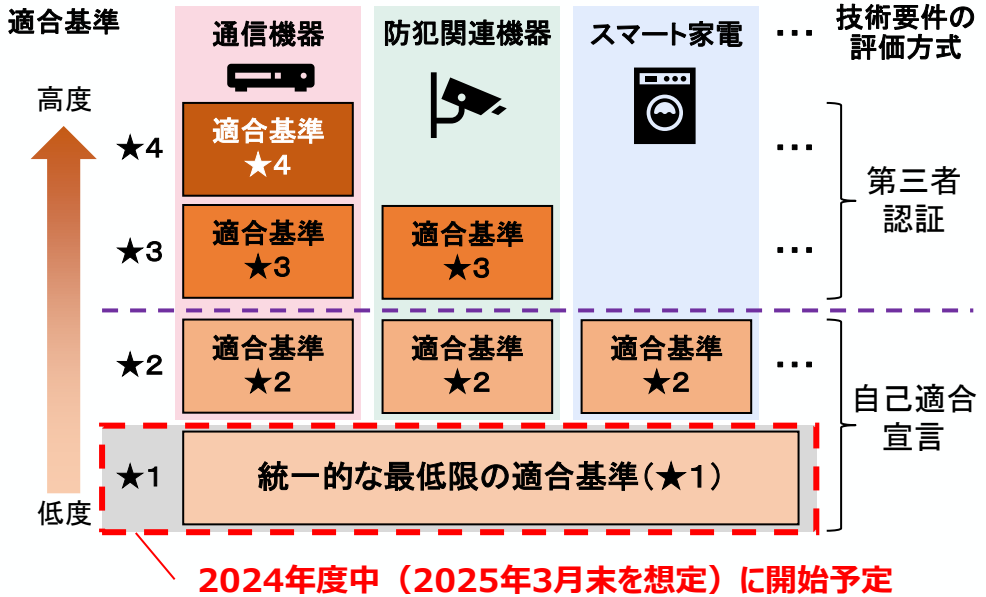
JAPAN CYBERSECURITY LABEL
ジャパン・サイバーセキュリティ・ラベル
★★★★
JC-STAR
Registered ID: 0123456789012345
Information-technology Promotion Agency, JAPAN (IPA)

対象製品の概要



※ 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。

制度の概要（イメージ）

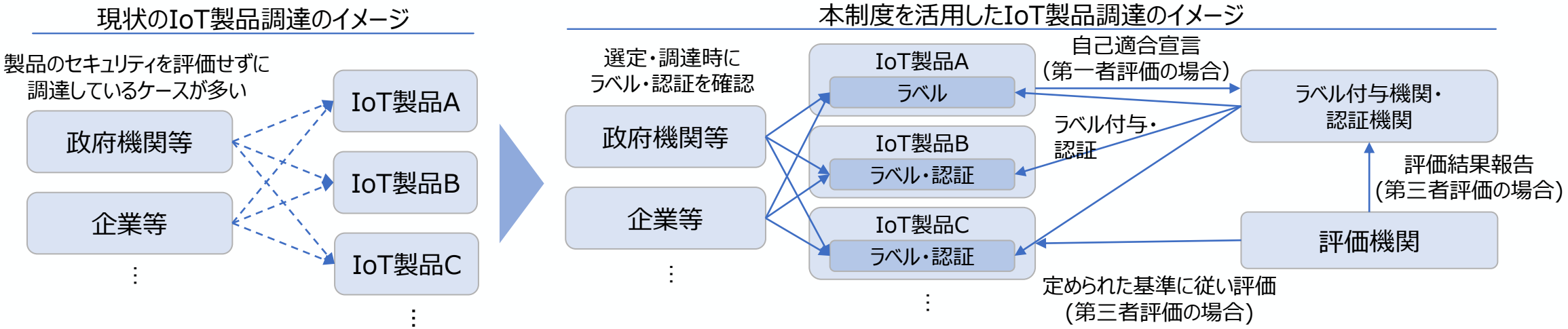


(※1)経済産業省「ワーキンググループ3（IoT製品に対するセキュリティ適合性評価制度構築に向けた検討会）」https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/index.html
(※2)IPA「IoT製品に対するセキュリティ要件適合評価・ラベリング制度を開始します」https://www.ipa.go.jp/pressrelease/2024/press20240930.html

IoTセキュリティ適合性評価制度の目的と位置付け

- IoT製品に対するセキュリティ適合性評価制度を国内で構築し、そのラベル・認証を広く普及させ、社会に浸透させるため、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**できるようにする。（調達ニーズへの対応）
- そのうえで、**IoT製品ベンダーが積極的にラベル取得するインセンティブ**を与える。

調達ニーズへの対応		ラベル取得のインセンティブ	
主目的① 【調達要件】	**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。	左記に加え	主目的③ 【相互承認】
主目的② 【業界標準】	特定分野のシステムにて調達・利用されるIoT製品に対し、必要な認証・ラベルを各業界団体等で指定できるようにし、当該**特定分野において必要な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。		**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。



IoTセキュリティ適合性評価制度について諸外国との比較

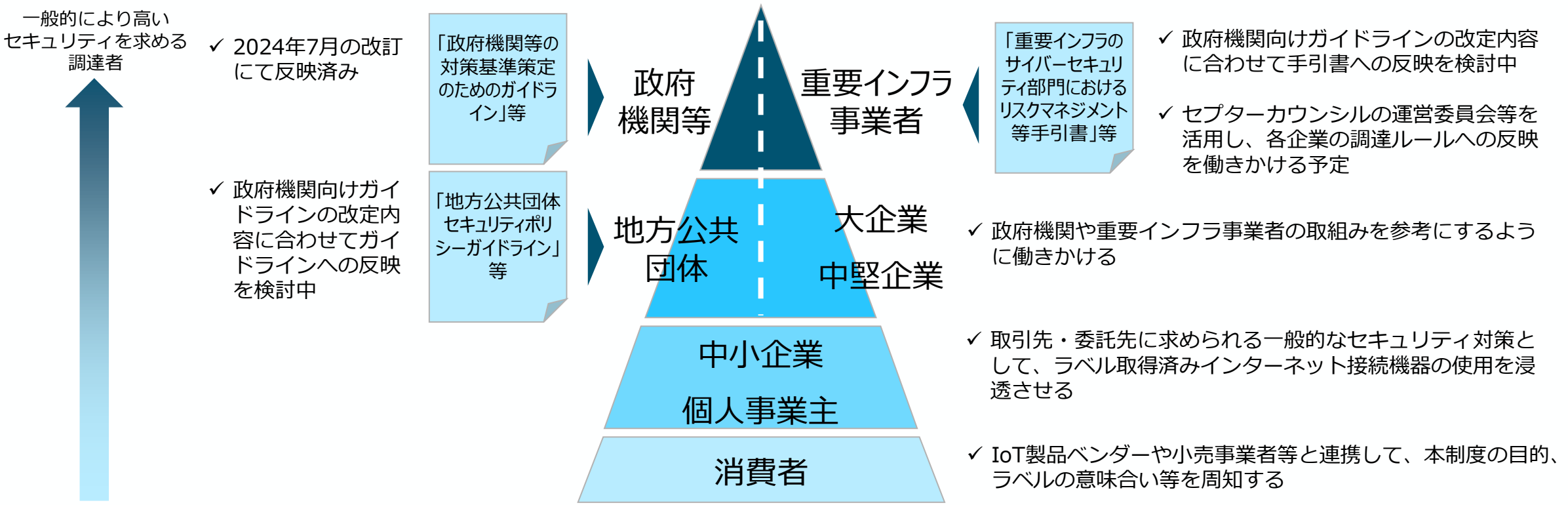
- 諸外国でも同様の制度検討が進んでいる。国内IoT製品ベンダーの負担を抑えるため、主要国制度の基準も参考にしながら本制度の基準を検討し、**相互承認の調整**を図る方針。
- 日米（首脳級）、日EU（閣僚級）、G7（首脳級）等にて、相互承認に向けて取組む旨合意。

国・地域	日本	シンガポール	英国	米国	EU
制度名	セキュリティ要件適合評価及びラベリング制度（JC-STAR）	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	• ★1：2025年3月末開始予定 • ★2以上：2025年度下期以降開始予定	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	消費者用無線IoT製品	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：第三者認証	• ＊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

調達者への制度展開戦略と初期ターゲット

- 今年度、**政府機関等、重要インフラ事業者、地方公共団体**向けの各ガイドライン類に本制度の**ラベル付与製品の調達に関する方針を盛り込む**よう協議を進める。
- 併せて、IoT製品ベンダー・団体等にラベル取得を働きかけ、および民間企業・消費者に本制度の目的やラベルの意義等の周知を行い、ラベル取得製品の調達・購入を浸透させていく。



（参考）政府統一基準群のガイドラインへの反映

- 2024年7月に公開された政府統一基準群のガイドラインに、今後の本制度活用を反映済み。

「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）の一部改定（令和６年７月）」（抜粋）

4.3　機器等の調達

4.3.1　機器等の調達

（解説）

本制度☆１適合基準相当の内容

- **基本対策事項 4.3.1(1)-2「必要なセキュリティ機能が適切に実装されていること」について**

　必要なセキュリティ対策を実施するためには、機器等に必要なセキュリティ機能が適切に実装されていることが求められる。例えば、IoT 機器等に必要なセキュリティ機能の具体例としては、少なくとも以下の内容が考えられる。

  - 容易に推測可能な初期パスワードの設定禁止
  - 主体認証のネットワークを介した総当たり攻撃対策
  - 容易に行えるソフトウェアの脆弱性対策（アップデート等）
  - 機器内のセキュリティパラメータの保護
  - 安全な通信の確保
  - 利用者が作成したデータの容易な消去
  - 利用しない機能や通信ポートの無効化

本制度の活用方針

　機器等に必要な情報セキュリティ対策が適切に実装されていることを確認するには、機器等の仕様書の確認、製造者へのヒアリングの実施のほか、次の「IoT 製品のセキュリティ適合性評価制度」の活用が考えられる。

　IoT 機器等に対する要求すべきセキュリティ要件に関連して、2024 年度中（2025 年３月頃）に「IoT 製品に対するセキュリティ適合性評価制度」の☆１のラベル付与が開始される予定であり、今後の調達における活用が考えられる。☆１は機器等共通の最低限満たすべきセキュリティ項目を満たしていることを製造業者が自己で評価し、その適合性を宣言することで取得可能となるものである。☆１の取得を確認することで、上記に記載しているセキュリティ機能の実装状況の確認の代用とすることができる。

　また同制度では、製品種別毎により高度なセキュリティ適合基準に対する評価を行う☆２（自己適合宣言）、☆３以上（第三者認証）が順次整備される予定である。制度整備の状況を踏まえつつ、2025 年度中に同制度の☆１以上を取得していることを機器等の選定基準に含めるとともに、以降も、☆２、☆３以上の対象機器の拡充に応じて選定基準への反映を順次行っていく予定である。

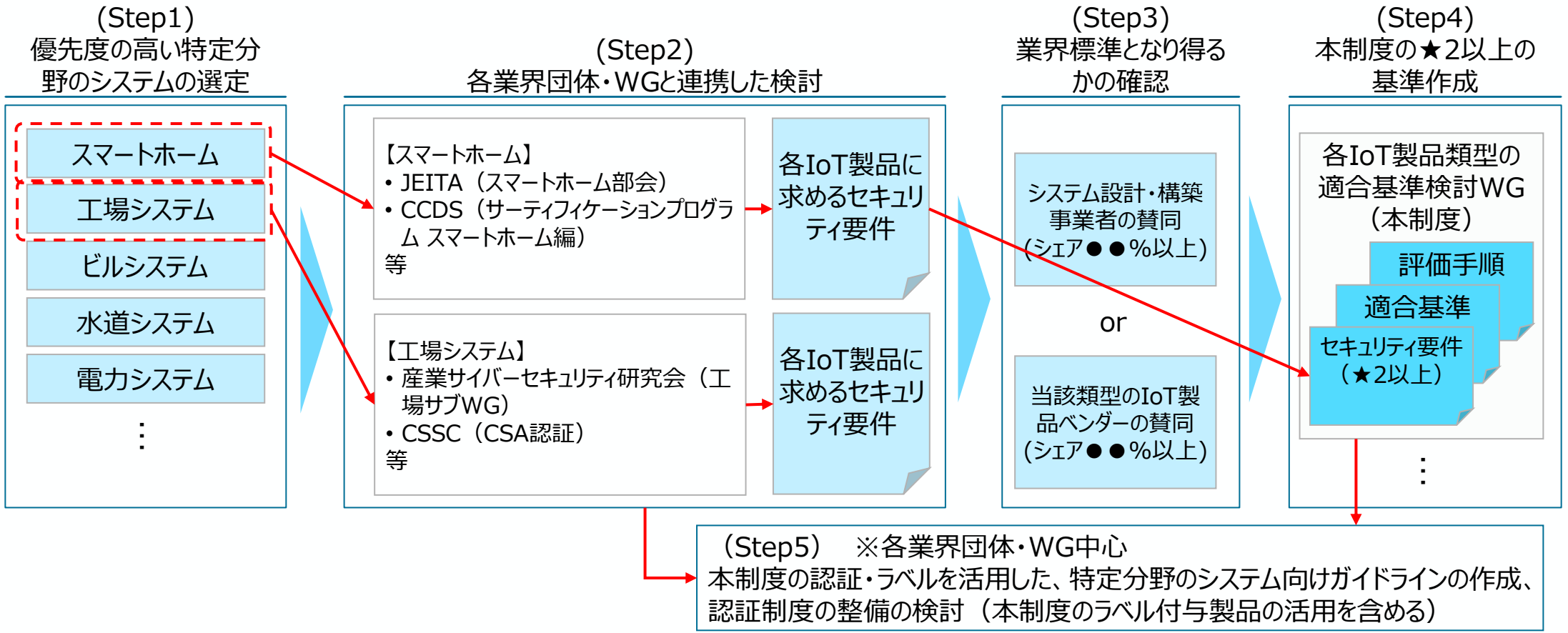
　情報システムの重要度に応じて「重要度：低」は☆１以上、「重要度：高～中」は少なくとも☆３以上の IoT 機器等を各機関等の選定基準に含めることの追加を検討している。なお、ラベル付与製品が普及する時期をめどに、政府機関等では求めるセキュリティ水準に応じたラベル付与製品の調達を必須化する方針である。

　参考：経済産業省「IoT 製品のセキュリティ適合性評価制度構築方針」
（https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/index.html）

（出典）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）の一部改定（令和６年７月）」（https://www.nisc.go.jp/pdf/policy/general/guider6.pdf）

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、検討優先度の高い分野の業界団体等と連携し、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する。



電力分野における活用

- 電力システムにおいても多くのIoT製品が活用されているところ、**事業者や系統全体の安全性確保のために、ラベルが付与された製品の積極的な調達・利用が望まれる。**
- 特に、現況の脅威の状況等を踏まえ、以下の製品類型での活用が期待される。

本制度の活用が期待される製品類型	背景
ERABシステムに用いられるIoT製品 （ゲートウェイ、コントローラ、ヒートポンプ給湯器等のDR-ready機器）	✓ エネルギー関連機器に対する脅威が増大している ✓ ERABセキュリティガイドラインに記載のとおり、ERABシステムはIoTシステムとしてのセキュリティが求められる
分散型電源の遠隔監視装置	✓ コンテック社の遠隔監視装置における脆弱性がインターネットバンキングの不正送金に悪用される事案が発生
分散型電源のPCS	✓ PCSにおいて複数の脆弱性が報告されている(※1) ✓ PCSに対するサイバー攻撃により、系統への悪影響を及ぼす可能性が報告されている(※2)

(※1) NIST, NIST IR 8498: Cybersecurity for Smart Inverters: Guidelines for Residential and Light Commercial Solar Energy Systems https://csrc.nist.gov/pubs/ir/8498/ipd
(※2) Willem Westerhof氏の報告（https://horusscenario.com/）やBert Hubert氏の報告（https://berthub.eu/articles/posts/the-gigantic-unregulated-power-plants-in-the-cloud/）など

（参考）電力制御システムに関するガイドライン等

- 電力分野の既存のガイドラインにJC-STAR制度の活用を反映し、製品メーカーや調達者に働きかけることが考えられる。

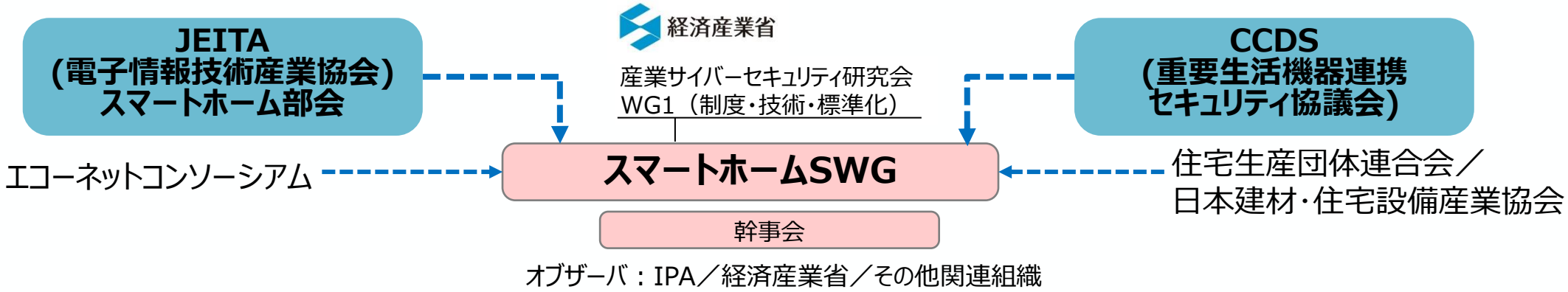
【参考】電力制御システムに対する取組（ガイドライン等）

	名称	主な対象	発行主体	概要
電制GL	**電力制御システムセキュリティガイドライン**	電気事業の用に供する電気工作物	日本電気協会	電気事業法、電気設備に関する技術基準を定める省令及びその解釈に基づき、電気事業の用に供する電気工作物に対しては、本ガイドラインに基づく対策が求められる。
スマメGL	**スマートメーターシステムセキュリティガイドライン**	スマートメーターシステム	日本電気協会	電気事業法、電気設備に関する技術基準を定める省令及びその解釈に基づき、スマートメーターシステムに対しては、本ガイドラインに基づく対策が求められる。
系統連系技術要件	**系統連系技術要件**	系統連系する発電設備	各一般送配電事業者	系統連系する発電設備にすべからく求められる対策。具体的には、ネットワーク接続点の保護、マルウェア対策、系統運用者に対するセキュリティ管理責任者の通知の3点が求められる。
PCS技術仕様	**出力制御機能付PCSの技術仕様**	出力制御機能付PCS	JPEA・JEMA・電事連	出力制御機能付PCSにおいて満たすべきサイバーセキュリティ対策の要件を示した技術仕様。
自家用GL	**自家用電気工作物に係るサイバーセキュリティの確保に関するガイドライン（内規）**	自家用電気工作物（発電設備と需要設備の両方を含む）	経済産業省	自家用電気工作物（発電設備と需要設備の両方を含む）に求められるサイバーセキュリティ対策事項を記載したガイドライン。
小売GL	**小売電気事業者のためのサイバーセキュリティ対策ガイドライン**	小売電気事業者	資源エネルギー庁	小売電気事業者が主体的に取り組むことが求められるサイバーセキュリティ対策に関して記載したガイドライン。
ERAB GL	**ERABに関するサイバーセキュリティガイドライン Ver2.0**	ERABに関する事業者	経済産業省・IPA	ERAB のサービスレベルを維持するために ERAB に参画する各事業者が実施すべき最低限のセキュリティ対策の要求事項を示したガイドライン。
特定卸供給の指針	**特定卸供給に係るサイバーセキュリティ確保の指針**	特定卸供給事業に関するシステム	資源エネルギー庁	特定卸供給事業を実施する上で確保すべきサイバーセキュリティとその対策の内容を示すことを目的とした指針で、特定卸供給事業の届出の際に、本指針に基づく対策実施状況を記載する必要がある。

（出典）資源エネルギー庁「電力分野におけるサイバーセキュリティについて（2024年4月17日）」（https://www.meti.go.jp/shingikai/enecho/denryoku_gas/denryoku_gas/pdf/073_07_00.pdf ）

（参考）スマートホーム分野での検討

- **スマートホーム分野は消費者向けのIoT製品の利用が拡大**している優先分野として、JEITA、CCDS等の関係者と連携し、2024年7月よりスマートホームSWGを拡大し、検討を開始。



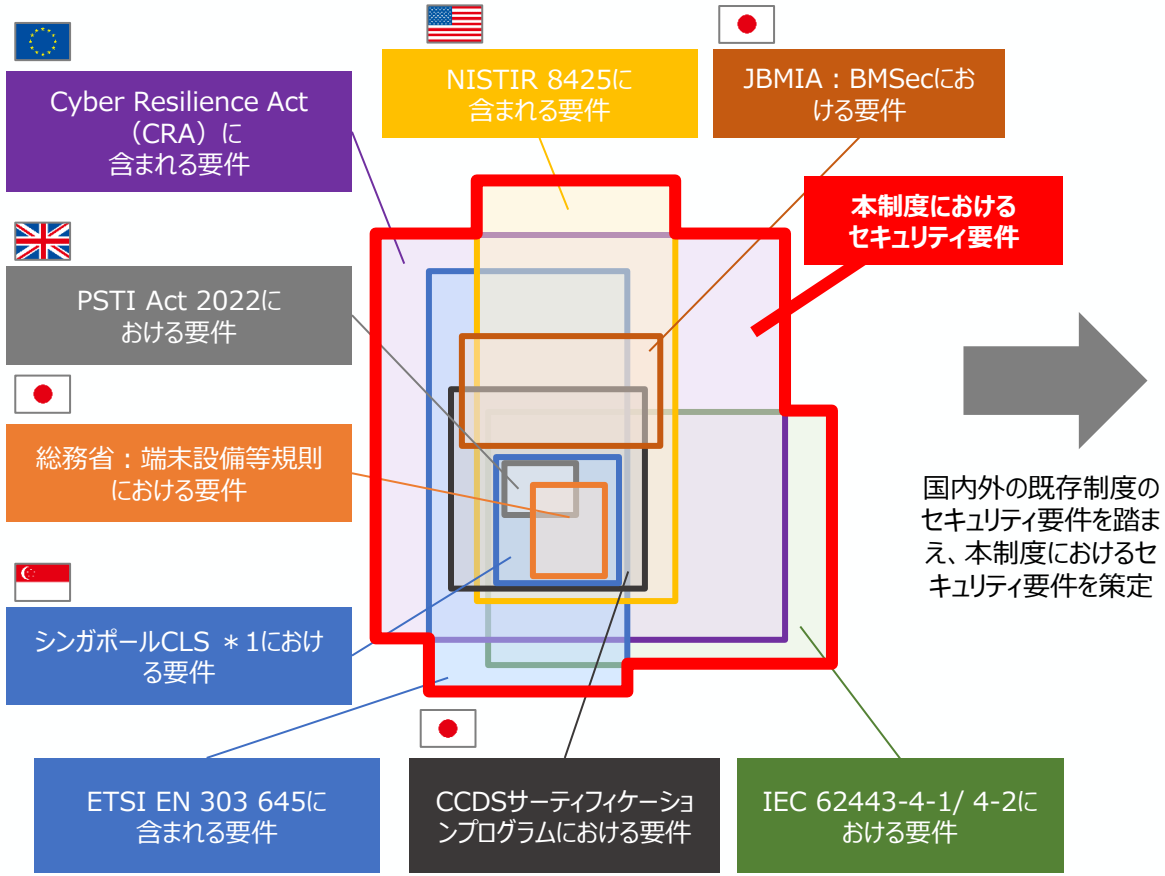
主査：JEITA/CCDSから選出、共同主査形式
委員：JEITA/CCDSの両会員企業から、IoT製品メーカ、ユーザを中心に委員を招聘する。
主な活動内容：
- **評価基準検討**
  - ースマートホームの定義
  - ースマートホームで実施すべきセキュリティ対策の検討
  - ースマートホーム関連の各IoT製品類型におけるIoTセキュリティラベル★１の活用及び★２以上の整備要否の検討
  - ー★２以上の整備のIoTセキュリティ適合性評価制度（IPA+経産省）への依頼
- **普及促進検討**
  - ースマートホームの普及・セキュリティ対策状況の現状確認、セキュリティを考慮した普及促進策の検討
  - ーIoT製品の販売・購入の促進施策の検討、IoT製品類型の活用に関する製品ベンダー、調達関係者との合意

（出典）2024年度第1回スマートホームSWG資料に基づき経済産業省作成

（参考）セキュリティ要件（全体リスト）の整理

- 本制度で使用するセキュリティ要件は、ETSI EN 303 645、NISTIR 8425、EU-CRA等の**国内外のセキュリティ要件の全体をカバー**するように整理し、作成した。（全101項目）

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
	・・・
・・・	・・・

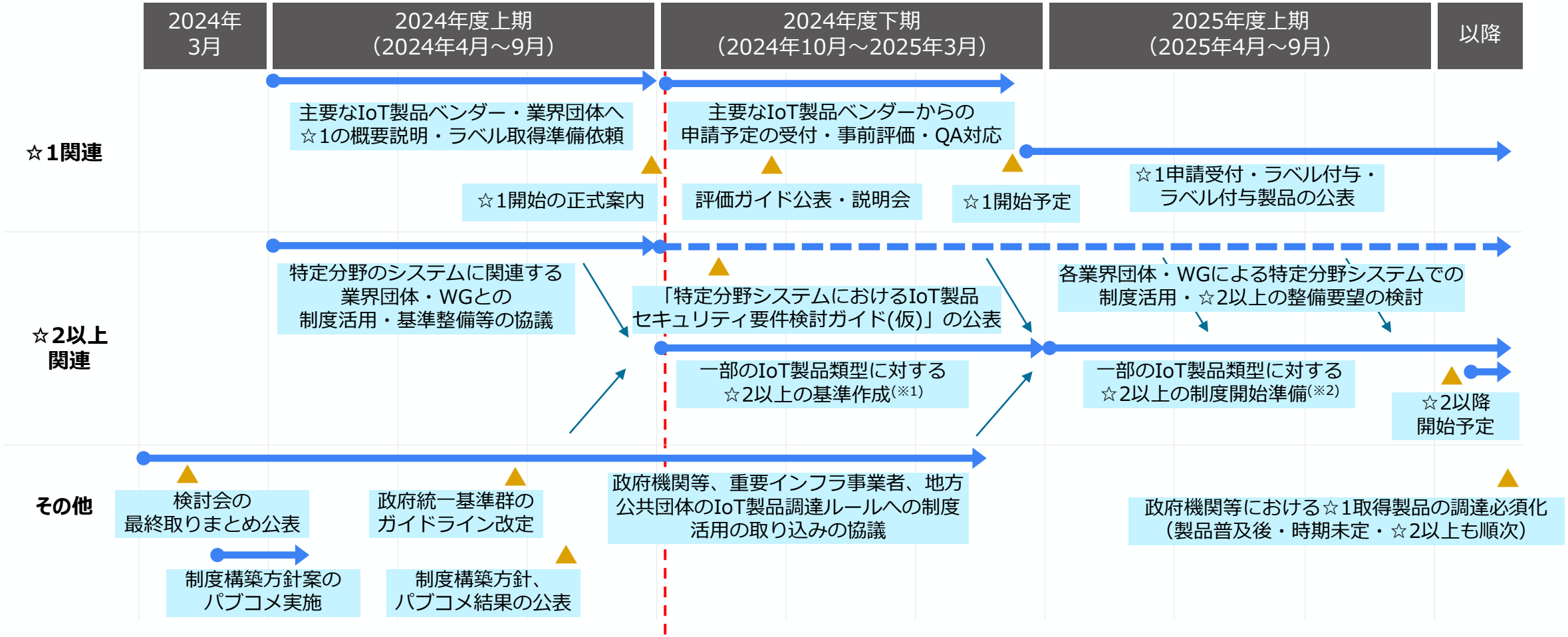
（参考）★１セキュリティ適合基準

- ★1で守るべき資産やアタックサーフェスから検討した想定脅威に対して、★1で対応するセキュリティ要件を全体リストから抽出し、**16項目の適合基準を作成**。

★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** (2)**容易に推測可能なデフォルトパスワードの禁止** (3)パスワード等の認証値の変更機能 (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**	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)
	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 (7)**容易かつ分かりやすいアップデート手順** (8)アップデート前のソフトウェアの完全性の確認機能 (10)ユーザが型式番号を認識可能とする記載・機能	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** (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)	–	–
	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)	–	–
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)	–	–
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**	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)	–	–

今後のスケジュール

- 2024年9月30日にIPAから制度開始の正式案内を実施。2025年3月末に☆１を開始予定。



(※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

経済産業省のサイバーセキュリティ政策ウェブページはこちら⇒
https://www.meti.go.jp/policy/netsecurity/index.html