経済産業省

資料６－３

ERABサイバーセキュリティガイドラインの改定状況について

２０２５年2月４日

資源エネルギー庁

１．前回の振り返り及び本日の趣旨

- 前回、ERABサイバーセキュリティガイドラインの想定する改定点、改定の進め方とその状況について御報告した。
- その後、改定作業を進め、改定後のERABサイバーセキュリティガイドライン（案）について、パブリックコメント（実施期間：2024年12月25日～2025年1月31日）が終了したところ。
- 本日は改定プロセスや概要について、御報告させていただく。

【参考】想定する改定点について

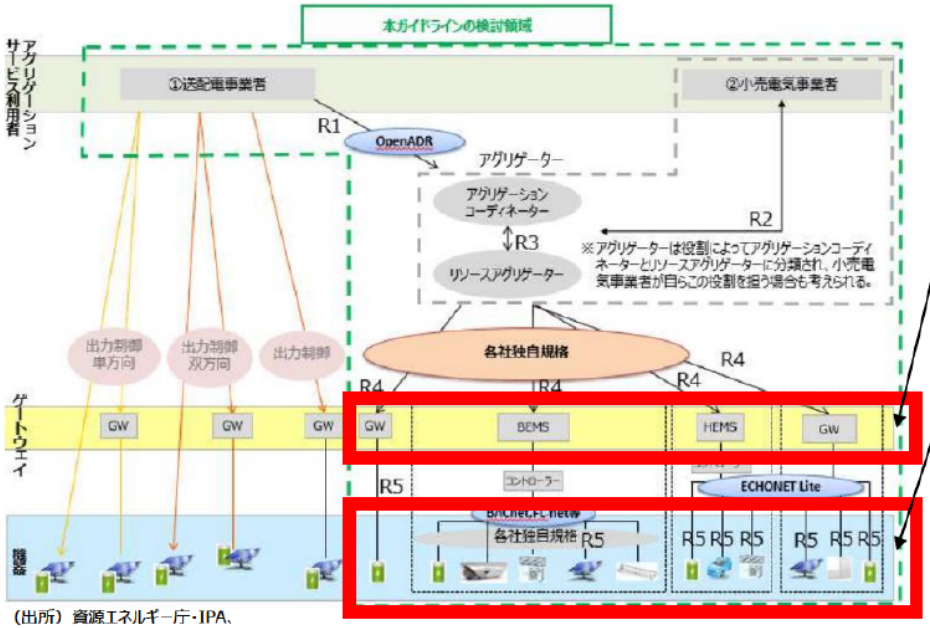
想定する改定点について

- 現行ガイドラインからの主な改定箇所は、以下項目を想定している。

  ① 物理的なGWを介さないDRサービス

  ② 末端のIoT機器等の脆弱性に起因する脅威

  ③ アグリゲーターが機器から取得する情報に起因するリスク



(出所) 資源エネルギー庁・IPA、
エネルギー・リソース・アグリゲーション・ビジネスに関するサイバーセキュリティガイドライン Ver2.0 赤枠加筆

① 物理的なGWを介さないDRサービス

これまでのガイドラインでは、機器を制御する際に物理的なGWを介することを主に想定していた。このGWがクラウド上にある場合もしくは物理的なGWを介さない場合の対応を検討し、記載する。

② 末端のIoT機器等の脆弱性に起因する脅威

インターネットに接続されるIoT製品の数が急速に増加したことに伴い、IoT製品の脆弱性を狙ったサイバー脅威も増加傾向にある。そこで、「IoT製品に対するセキュリティ適合性評価制度」を参考に対応を検討し、記載する。

③ アグリゲーターが機器から取得する情報に起因するリスク

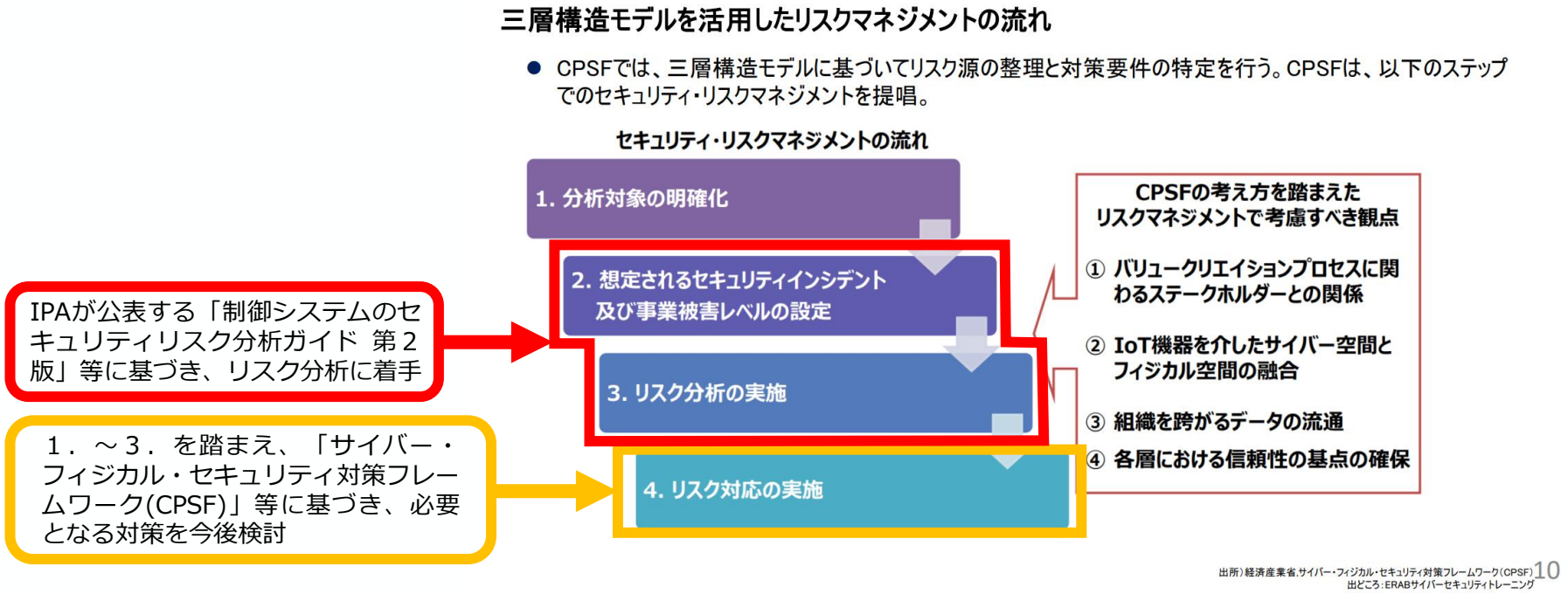
機器の利用状況から、利用者の在・不在が推測できる情報等、制御対象機器に関連する情報が多様化したことによるセキュリティリスクが懸念されている。
本リスクを踏まえた対応を検討し、記載する。

5

出所：第10回 次世代の分散型電力システムに関する検討会 資料４

【参考】ガイドラインの改定状況

- 「制御システムのセキュリティリスク分析ガイド 第２版（2023年3月、IPA）」等に基づき、**「想定されるセキュリティインシデント及び事業被害レベルの設定」「リスク分析の実施」に着手**。



出所：第16回ワーキンググループ1（電力サブワーキンググループ）資料６-１　事務局にて加筆

2．改定に向けた検討内容

- 物理的なゲートウェイを介さずに通信・制御を行うDRサービスや、IoT機器の脆弱性を狙った脅威、プライバシー性の高い情報に関する脅威の増加といった変化に起因して、起こり得る新たな脅威の想定やリスクシナリオの検討を行った上で必要となる対策の検討を実施。

実施項目

1. **リスク分析シートの作成**（ERABシステムのリバイス、脅威の想定、シナリオ検討、リスク分析、必要となる対策の検討）
2. **ERABサイバーセキュリティガイドラインの改定**（改定方針の検討、新たに盛り込むべき事項の整理、改定案の作成）

背景

1. IoTデバイスの導入数の増加に伴い、物理的なゲートウェイを介さずに通信・制御を行うDRサービスが増加している。
2. IoT製品の増加に伴い、IoT製品の脆弱性を狙ったサイバー脅威も増加してる。
3. 対象デバイスから取得できる関連情報（在宅・不在情報）の多様化により、犯罪の脅威が増大している。

検討内容

1. 物理的なゲートウェイを介さないDRサービス
   ゲートウェイがクラウド上にある、物理ゲートウェイを介さないDRサービスに必要な対策を検討した。
2. IoTデバイスの脆弱性に起因する脅威
   ERABで制御されるIoTデバイスの要件を検討した。
   (セキュリティ要件適合評価及びラベリング制度(JC-STAR)を参照する)
3. デバイスから奪取される可能性のある情報（在宅/不在情報）に起因するリスク
   制御対象デバイスおよび関連情報の多様化に伴うセキュリティリスクに対処するために必要な要件を検討した。

3．改定案作成のプロセス

ERABシステムのリバイス

複数の異なる事業者によるERAB制御対象のエネルギー機器の遠隔制御、コントローラーの設置環境の多様化（クラウド環境等）、物理的なゲートウェイを介さないERAB制御対象のエネルギー機器の遠隔制御など、実態に即したERABシステムの新しいユースケースを整理した。

リスクシナリオの作成

現在のERABシステムの新しいユースケースにおいて想定される脅威を想定リスクシナリオとして洗い出した。

リスク値の算定

各リスクシナリオにおける対応優先度の高いリスクを抽出するために、情報処理推進機構（IPA）が策定する「制御システムのセキュリティリスク分析ガイド 第2版」の考え方に基づいてリスクの評価を実施した。

- 資産ベースのリスク分析・評価
- 事業被害ベースのリスク分析・評価

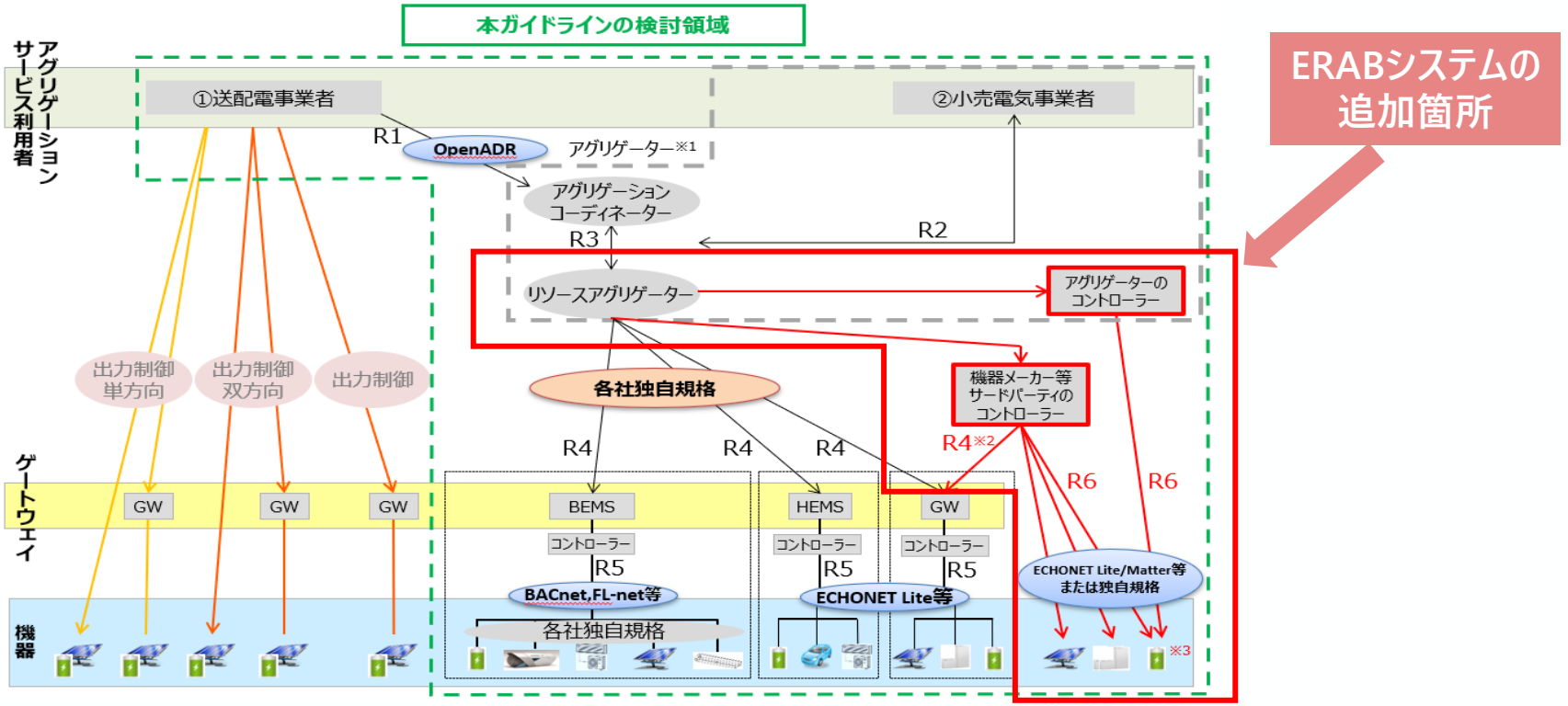
リスクに応じた必要対策の検討

各リスクシナリオの脅威に有効となる対策を、経済産業省が策定する「サイバー・フィジカル・セキュリティ対策フレームワーク」との紐づけにより、新たに盛り込むべき対策要件として整理した。
さらに、当該対策要件とERABサイバーセキュリティガイドラインVer2.0（現行版）の内容を照らし合わせ、脅威への対処が可能であり、かつ経済合理性も認められるサイバーセキュリティ対策を抽出し、改定案を作成した。

ERABサイバーセキュリティガイドライン改定案

4．ERABシステムのリバイス（追加箇所）

- 単一の機器に複数の異なる仕様のプロトコルスタックを共存させる方法を用いて、複数の異なる事業者(リソースアグリゲーター、機器メーカー等サードパーティ)が、同一のERAB制御対象のエネルギー機器との通信・制御を実施するユースケースを追加。
- 機器メーカー等サードパーティのコントローラーを経由して、直接または需要家側のルータ経由でのERAB制御対象のエネルギー機器との通信・制御を実施するユースケースを追加。



※1　アグリゲーターは、役割によってアグリゲーションコーディネーターとリソースアグリゲーターに分類され、小売電気事業者が自らこの役割を担う場合も考えられる。
※2　HEMSやBEMSと連携することも考えられる。
※3　単一の機器に、複数の異なる仕様のプロトコルスタックが共存する場合がある。

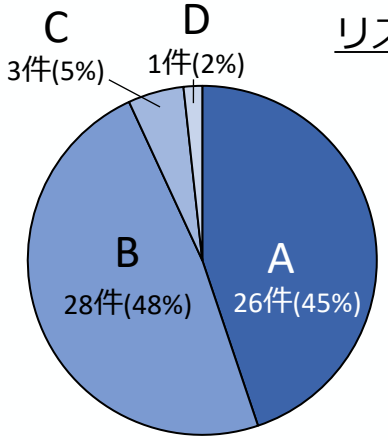
5．脅威の想定及びリスクシナリオの作成及びリスク値の算定

- ERABシステムで想定される脅威を洗い出し、リスク評価を実施。

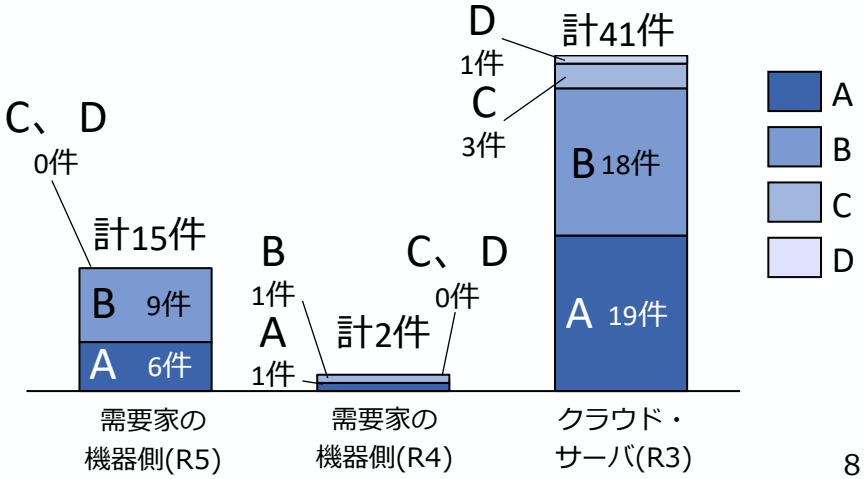
追加されたリスクシナリオ（58件）における脅威・攻撃シナリオの内訳

脅威・攻撃シナリオ	該当シナリオ数
不正アクセス	15
マルウェア感染	7
設定ミス	6
機器のなりすまし	4
DoS/DDoS攻撃	4
中間者攻撃	4
ランサムウェア感染	3
災害・障害等	3
パスワード総当たり攻撃	2
フィッシング攻撃	2
Webサイトの改ざん	2
内部者攻撃	2
セキュリティ機能の設定の不備	2
誤操作	1
機器製造時のマルウェア混入	1

追加されたリスクシナリオ（58件）におけるリスクレベル



各インターフェースにおけるリスクレベルの内訳



※A（リスクが非常に高い）～ D（リスクが低い）

6．リスクに応じた必要対策の検討

- 事業被害ベースのリスクシナリオのうち、リスクレベル「A」または「B」に相当するものについては、**内部ネットワークで利用される需要家側のルータや通信プロトコル等の脆弱性に関連するものが多く含まれている**ことが確認できた。
- その上で、リスクレベル「A」または「B」に相当するものについては、すべて資産ベースでのリスクを重層的に評価し、リスクの高い資産に対して、脅威・リスクへの対処が可能で、経済合理性が認められる必要な対策を検討した。
- 対策については、**機器のセキュリティ強化、機器やソフトウェア・プロトコル等の脆弱性対策、通信先の制限対策、クラウド・サーバー側のセキュリティ対策や不正ログイン対策、システムのデータバックアップ対策が強化のポイント**であることが分かった。
- 加えて、**ERABに参加する各事業者の自組織における、資産の脆弱性確認、システムの設定確認、異常確認等の基本的な対策の根本的確保、自組織で確認された脆弱性情報やシステム異常情報等の関係者への共有が強化のポイント**であることが分かった。
- なお、結果的に、上記のリスクの高い資産への対策によって、リスクレベル「C」または「D」に相当するリスクシナリオについても、対応可能であることを確認できた。

7．ERABサイバーセキュリティガイドラインの改定箇所の例

（GWを介さずに直接通信するリソースアグリゲーターとERAB制御対象のエネルギー機器間のインターフェース（Ｒ６））（1/2）

対策要件の追加が必要と考えられる理由とその対策

●追加要件が必要な理由となる脅威・リスク：【脅威・リスクⅠ】

- GW配下ではなくなるため、ERAB制御対象のエネルギー機器や制御用通信が直接、攻撃者の標的となり、不正アクセスや通信路上での盗聴・改ざん、なりすましなどのインターネット上の脅威にさらされる可能性がある。

●全般的な対策

- R6におけるERAB制御対象のエネルギー機器は、リソースアグリゲーターのシステムとインターネット経由で直接通信することから、R5におけるERAB制御対象のエネルギー機器と、R4におけるリソースアグリゲーターの制御対象の機器の２つの特徴を持つ。このため、従来のR5における対策に加えて、R4における対策を併せて実施することが重要。

（①物理的なGWを介さないDRサービスへの対策）

新しく盛り込むべき事項の方向性

3.6.6. R6（GWを介さずに直接通信するリソースアグリゲーターとERAB制御対象のエネルギー機器間のインターフェース）

【勧告】

（事業者とその保有するシステムの対策）

- ERAB制御対象のエネルギー機器、GW又はBEMS・HEMS等エネルギーマネジメントシステムは、アグリゲーションコーディネーターのシステムと接続する場合において、本ガイドラインに準拠することが必須とされる ことに加え、本ガイドラインに基づきアグリゲーションコーディネーターが別途要件を定義したセキュリティ対策に準拠すること。

  ※本ガイドラインのR6は、リソースアグリゲーターのシステムとERAB制御対象のエネルギー機器間の通信路として、公衆網が使われる場合を前提としている。なお、リソースアグリゲーターのシステムとERAB制御対象のエネルギー機器を通信端点としたエンドツーエンドで伝送路の安全性・信頼性が確保されているネットワークが使われる場合には、エンドツーエンドで伝送路のセキュリティ担保を条件に、対策の強度に関して事業者に一定の裁量を認め得るものと考えられる。

- リソースアグリゲーターは、リソースアグリゲーターとERAB制御対象のエネルギー機器が接続するネットワーク構成を確認し、適切な対策を行うこと。

7．ERABサイバーセキュリティガイドラインの改定箇所の例

（GWを介さずに直接通信するリソースアグリゲーターとERAB制御対象のエネルギー機器間のインターフェース（Ｒ６））（2/2）

対策要件の追加が必要と考えられる理由とその対策

●追加要件が必要な理由となる脅威・リスク：【脅威・リスクⅠ】

- GW配下ではなくなるため、ERAB制御対象のエネルギー機器や制御用通信が直接、攻撃者の標的となり、不正アクセスや通信路上での盗聴・改ざん、なりすましなどのインターネット上の脅威にさらされる可能性がある。

●全般的な対策

- R6におけるERAB制御対象のエネルギー機器は、リソースアグリゲーターのシステムとインターネット経由で直接通信することから、R5におけるERAB制御対象のエネルギー機器と、R4におけるリソースアグリゲーターの制御対象の機器の２つの特徴を持つ。このため、従来のR5における対策に加えて、R4における対策を併せて実施することが重要。

（①物理的なGWを介さないDRサービスへの対策）

新しく盛り込むべき事項の方向性

3.6.6. R6（GWを介さずに直接通信するリソースアグリゲーターとERAB制御対象のエネルギー機器間のインターフェース）

【勧告】

（インターフェースの対策）

- 外部システムとの相互接続点において、ホワイトリスト等を用いた通信先の制限、認証、通信メッセージの暗号化により保護すること。
- 管理組織の特定が可能で、かつ脆弱性対策が設計可能であるプロトコルを採用すること。
- リソースアグリゲーターの制御対象にIoT製品を新たに導入する場合においては、「セキュリティ要件適合評価及びラベリング制度（JC-STAR）」が定める適合基準である★１（レベル１）以上※を満たす製品を選択すること。
  ※今後、製品類型ごとの特徴を考慮した★２（レベル２）以上の詳細要件が決定した場合においては、★２（レベル２）以上を満たす製品を選択することが望ましい。
- 開放されているネットワークポートを確認し、不要なポートを物理的又は論理的に閉塞すること。

【参考】セキュリティ要件適合評価及びラベリング制度の概要

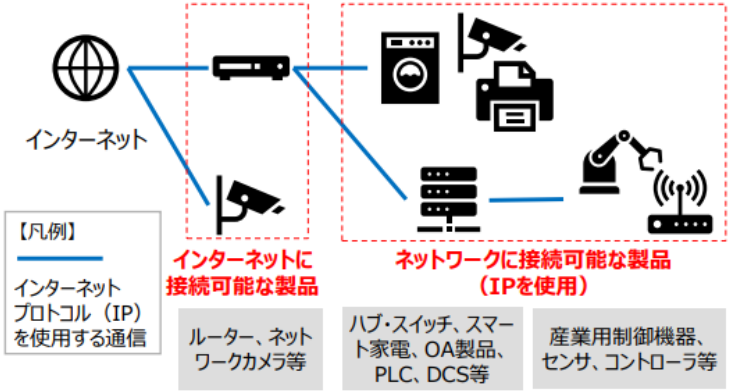
3. 構築するセキュリティ適合性評価制度の概要

3.2. 対象製品と適合性評価レベル

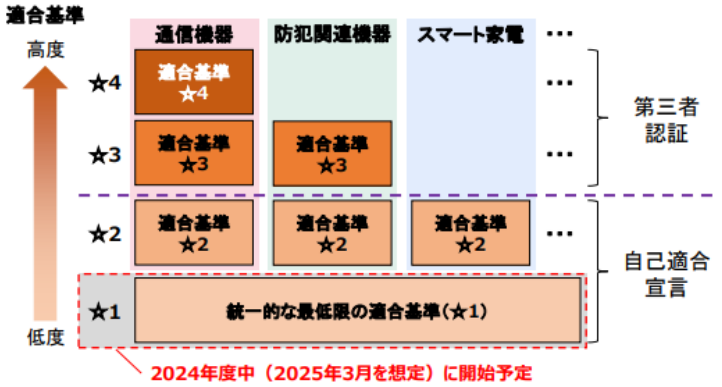
制度構築方針案
3.2～3.3

- **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		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	

(※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。

6

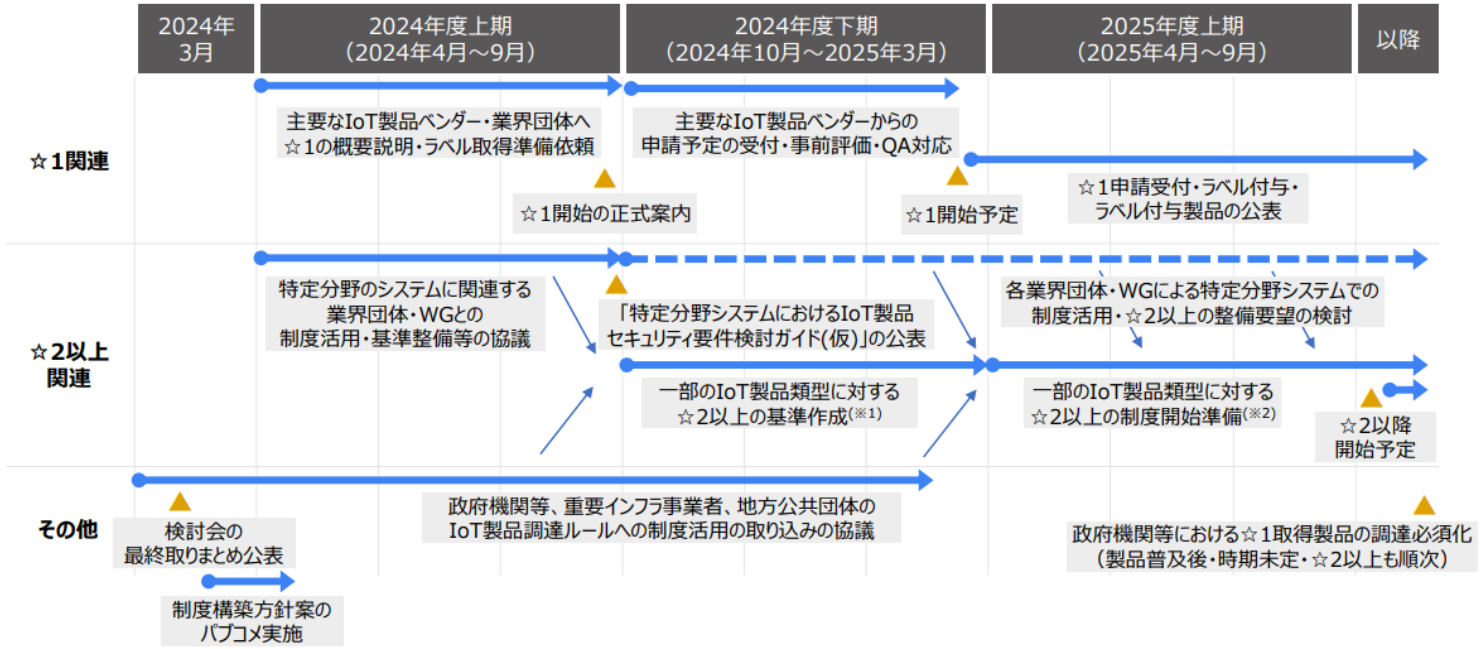
（出所）IoT製品に対するセキュリティ適合性評価制度構築方針（2024年8月23日）IoT製品に対する セキュリティ適合性評価制度構築方針 ～概要説明資料～

【参考】セキュリティ要件適合評価及びラベリング制度の概要

制度構築方針案
5

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

16

（出所）IoT製品に対するセキュリティ適合性評価制度構築方針（2024年8月23日）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～

8．今後のスケジュール

- 現在、改定（案）についてパブリックコメントが終了したところ。
- 今後、意見を集約を行い、その意見を踏まえた対応について、「次世代の分散型電力システムに関する検討会」にて、委員に確認いただいた上で、**2024年度中に公表予定。**

項目	2024年度							
	8月	9月	10月	11月	12月	1月	2月	3月
ERABサイバーセキュリティガイドライン改定								★
課題抽出・要件化・リスク評価表作成								
業界団体意見集約								
パブリックコメント								
IPA研修　実施予定日程				★	★			

（参考）ERABサイバーセキュリティトレーニング(2024)

- セキュリティインシデントの内容等を一部更新し、IPAにおいて実施。

2024年11月25日～12月9日　オンライン研修

ガイドライン編
- 電力分野のサイバーセキュリティ脅威に関する現況の解説
- 電力分野に関連するサイバーセキュリティ規制・ガイドライン類の概要
- ERABサイバーセキュリティガイドラインの解説
- サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）の解説
- 脅威や脆弱性を検討・評価する手法の解説

リスク分析編①
- ERABシステムのリスク分析概要
- ERABシステムにおける対策選定手法の解説
- ERABシステムに想定されるリスクシナリオ(ユースケース)

2024年12月11日、12日　集合研修

集中講義
- 最新情報提供
- オンデマンド配信内容に関する質疑
- ユースケースに基づくリスク分析の実演
- ERABサイバーセキュリティガイドラインの改訂方向性及びCCRC技術参考報告書の解説

模擬プラント編
- 模擬環境を用いたERABシステムのリスクの体感・解説

リスク分析編②
- グループワーク

参加機関数：24機関
参加者数　：36名

＜集合研修の様子＞