経済産業省

資料４

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の改定について

2024年8月2日

資源エネルギー庁

ERABサイバーセキュリティガイドラインについて

- 資源エネルギー庁は、**エネルギー・リソース・アグリゲーション・ビジネス（以下、ERAB）　に参画する各事業者が取り組むべきサイバーセキュリティ対策の指針**として、ERABに関するサイバーセキュリティガイドライン（以下、「ERABサイバーセキュリティガイドライン」）を**2017年４月に策定**。
- ERABサイバーセキュリティガイドラインは、**事業環境の変化に応じて改定**しており、直近では、**2019年12月に改定**。
- 一方、ERABの拡大や事業環境が変化していることに伴い、**当初想定されていなかった脅威やゲートウェイ（以下、「GW」）を介さないDR事業者と機器等の連携の仕組みの活用が、近年増加**している。
- また、IoT機器の増加に伴い、**IoT機器の脆弱性を狙ったサイバー脅威**も高まってきたことを受け、IoT機器のセキュリティに関して、**評価制度やガイドライン等の検討も進展**している。
- 加えて、**ヒートポンプ給湯機**については、他のリソースに先立ち**機器のDRready要件を検討**しており、ERABを行う上で必要な**機器のセキュリティの要件についても議論**されている。
- これらの状況を踏まえ、**ERABサイバーセキュリティガイドラインを改定**することとしたい。

【参考】アグリゲーター及びDERのセキュリティ対策推進の方向性について

- 今後、太陽光発電をはじめとして、DERの更なる追加が見込まれるところ、まずは、**近年のIoTに関する脅威動向や取組動向を踏まえつつ、末端のIoT機器等に求められるセキュリティ対策を整理することが必要ではないか。その上で、どのようにそれをERABセキュリティガイドラインの改定に取り組んでいくか検討すべきではないか**。
- また、**詳細対策要件の策定が進められるよう、参考となる考え方の整理や、ERABに参画する事業者が相談できる体制の整備等について、検討する必要があるのではないか。**
- 業界としてアグリゲーターのセキュリティ対策の実態把握をするために、広域機関の会員が提出する**セキュリティリスク点検ツールの**結果については、広域機関と資源エネルギー庁の間で連携していく。**点検結果の集計時期や連携される情報等について、検討する必要があるのではないか。**

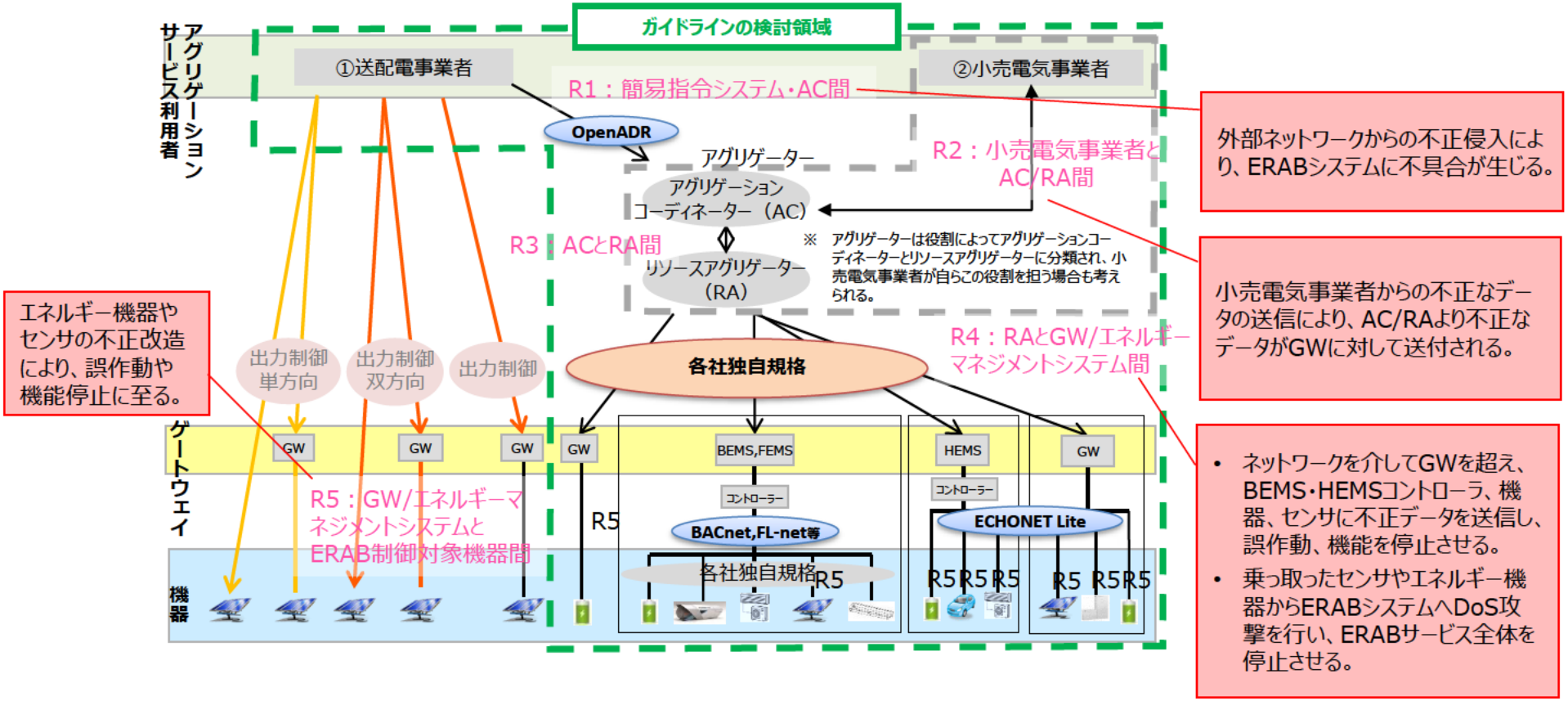
（出所）第16回 産業サイバーセキュリティ研究会ワーキンググループ１
（制度・技術・標準化）電力ＳＷＧ（2024年2月1日）資料6-2

【参考】ERABシステムの概要と想定されるサイバーセキュリティ脅威

（出所）第16回 産業サイバーセキュリティ研究会ワーキンググループ1
（制度・技術・標準化）電力SWG（2024年2月1日）資料6-2

- ERABシステムでは、**送配電事業者、アグリゲーションコーディネーター（AC）、リソースアグリゲーター（RA）、小売電気事業者など多くのステークホルダーが関与**する。
- 「ERABサイバーセキュリティガイドライン」では、ERABシステムのレイヤーを整理した上で、ERABシステムにおいて想定されるセキュリティ脅威が示されている。

ERABシステムの概要と想定されるサイバーセキュリティ脅威



（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

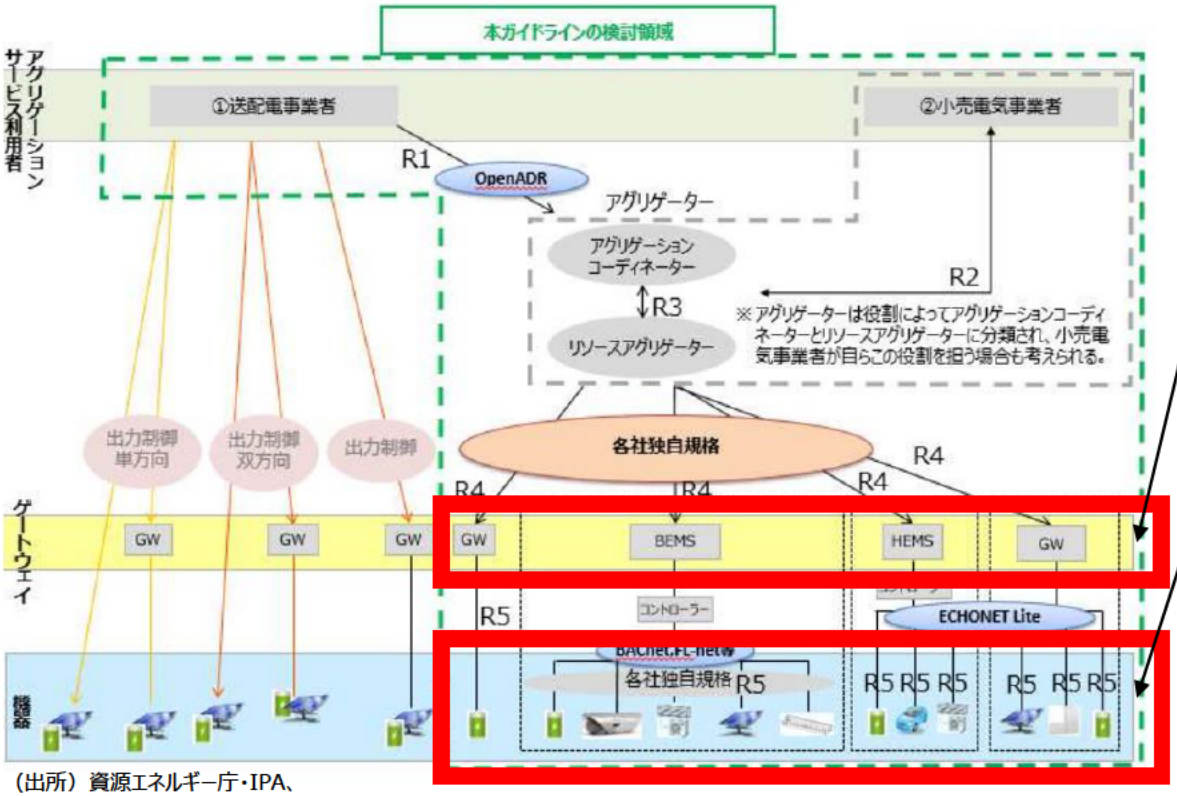
想定する改定点について

- 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。

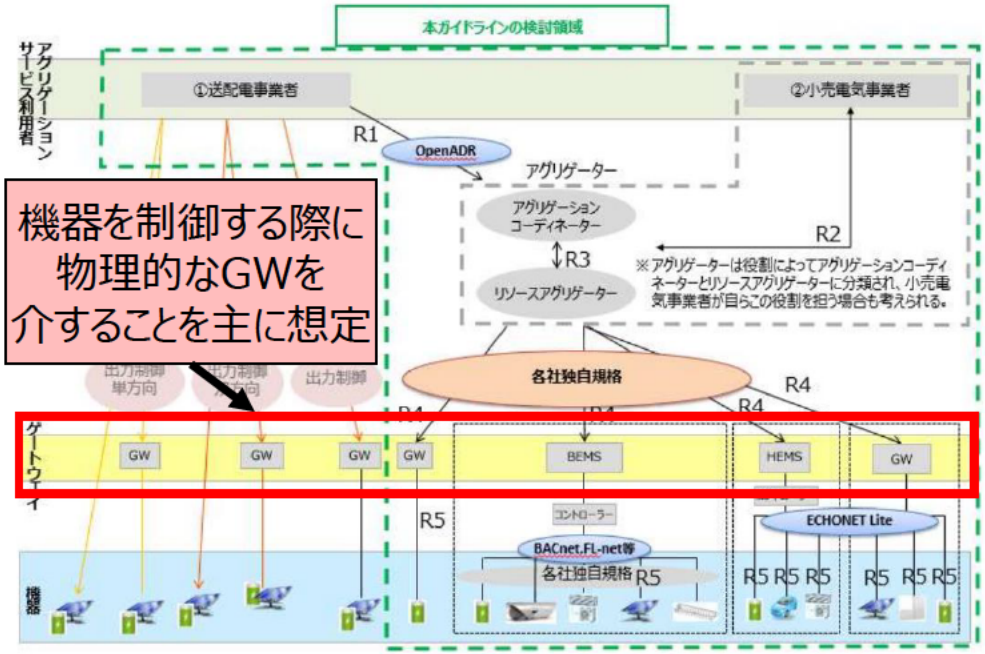
③ アグリゲーターが機器から取得する情報に起因するリスク

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。

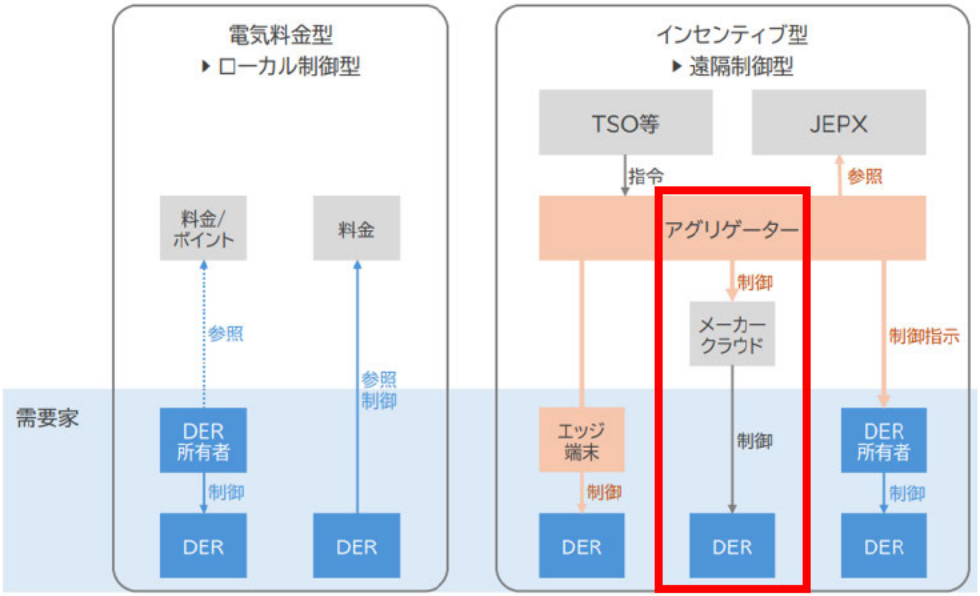
① 物理的なGWを介さないDRサービスについて

- **<u>ERABにおける機器の制御モデル</u>**として、従来のBEMSやHEMS等、物理的なGWを介して通信・制御を行うモデルに加え、**<u>メーカークラウドなど、物理的なGWを介さずに通信・制御を行うDRサービスが増加</u>**してきている。
- 上記のような前回のERABサイバーセキュリティガイドライン改定時からの環境変化を踏まえ、**<u>セキュリティ対策の要件事項及び対応方針</u>**を検討後、記載する。

〈ERABシステムにおける全体図〉



〈メーカークラウドを通じ、通信・制御を行うDRのイメージ〉



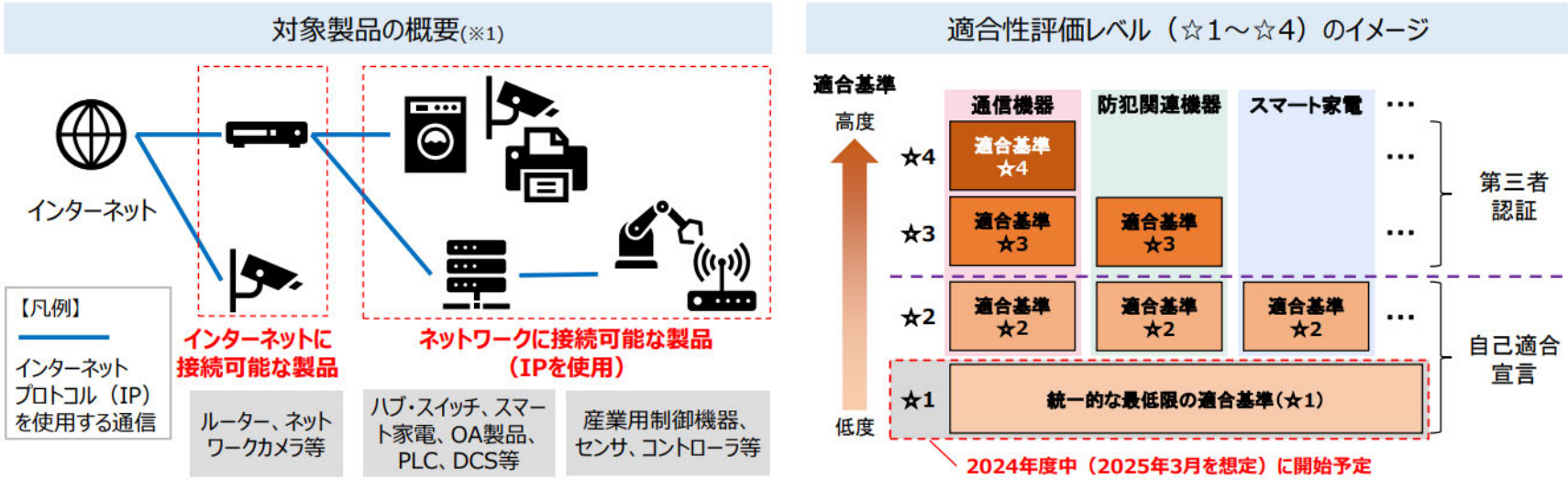
（出所）資源エネルギー庁・IPA、
エネルギー・リソース・アグリゲーション・ビジネスに関するサイバーセキュリティガイドライン Ver2.0　赤枠加筆

（出所）第1回 DRready勉強会　資料7 エネルギーリソースアグリゲーション事業協会提出資料　赤枠加筆

② 末端のIoT機器等の脆弱性に起因する脅威について

- **<u>IoT機器の脆弱性を狙ったサイバー攻撃が増加傾向</u>**にある。
- このような状況を鑑み、我が国でも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、**<u>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を構築</u>**すべく、**<u>IoT製品に対するセキュリティ適合性評価制度の検討</u>**が行われた。
- 本制度の検討結果や近年のIoT機器に関する脅威動向・取組動向を踏まえ、**<u>ERABの制御対象となるIoT機器に必要な要求事項を検討</u>**後、記載する。

〈IoT製品に対するセキュリティ適合性評価制度における対象製品と適合性評価レベル〉



(※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。

（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案～概要説明資料～

【参考】IoT機器の増加状況

1. 背景｜IoT機器の増加

近年、IoT機器の台数は急速に増加しており、今後も増加の一途を辿ることが予想されている。

- 近年、インターネットに接続される**IoT機器の数は急速に増加**している。
- 世界のIoT機器数について、2021年には292億台程度であるが、2023年には323億台、2023年には358億台、2024年には400億台程度と、**今後も増加の一途を辿ることが予想されている**。

世界のIoT機器数の推移及び予測

※ ここでのIoT機器とは、固有のIPアドレスを持ちインターネットに接続が可能な機器及びセンサーネットワークの末端として使われる端末等を指す。

出所）総務省、令和4年度情報通信白書 https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r04/html/nb000000.html

Copyright © Mitsubishi Research Institute

（出所）第1回 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

【参考】IoT機器を対象としたサイバー攻撃の脅威

MRI

1. 背景｜IoT機器を対象としたサイバー脅威

IoT機器数の急激な増加に伴い、IoT機器の脆弱性を狙ったサイバー脅威も増加傾向にある。脅威の高まりを受け、各国はIoT機器の安全性確保に向けた取組に力を入れている。

- IoT機器数の急激な増加に伴い、IoT機器の脆弱性を狙ったサイバー脅威も増加傾向にある。
- Kasperskyの調査によれば、**2021年上半期だけで、2020年の2倍以上のIoT機器に対するサイバー攻撃が発生**した。
- また、IBM Security X-Forceの調査によれば、2019年第3四半期から2020年第4四半期にかけて、**IoT機器を対象としたマルウェアの活動が3,000%増加**した。
- 同調査によれば、2020年から2021年にかけて脆弱性全体の増加率は0.4%の増加に留まった一方で、**IoT機器関連の脆弱性の件数は16%も増加**した。
- 加えて、Checkpointの研究者は、IoT機器に対するサイバー攻撃は日々増加するだけでなく、**洗練かつ広範で破壊的になりつつある**ことを指摘している。
- IoT機器に対する脅威の高まりを受け、各国はIoT機器の安全性確保に向けた取組に力を入れている。

IoT機器を対象としたサイバー脅威に関する動向

IoT機器を対象としたサイバー攻撃の増加率	200% (2020年一年間→2021年上半期)
IoT機器を対象としたマルウェア活動の増加率	3,000% (2019年第3四半期→2020年第4四半期)
IoT機器に関係する脆弱性件数の増加率	16% (2020年→2021年)

出所）Threatpost, IoT Attacks Skyrocket, Doubling in 6 Months https://threatpost.com/iot-attacks-doubling/169224/
IBM Security X-Force, X-Force 脅威インテリジェンス・インデックス 2022 https://www.ibm.com/security/jp-ja/data-breach/threat-intelligence/, https://www.ibm.com/downloads/cas/QA59ZP3P
Checkpoint, Protecting IoT Devices from Within – Why IoT Devices Need A Different Security Approach? https://blog.checkpoint.com/2022/07/25/protecting-iot-devices-from-within-why-iot-devices-need-a-different-security-approach/

Copyright © Mitsubishi Research Institute

（出所）第1回 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

【参考】IoT製品に対するセキュリティ適合性評価制度 ☆１の要件

3. 構築するセキュリティ適合性評価制度の概要

3.3. セキュリティ要件・適合基準・評価手順（3/3）

制度構築方針案
3.4

- ☆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。

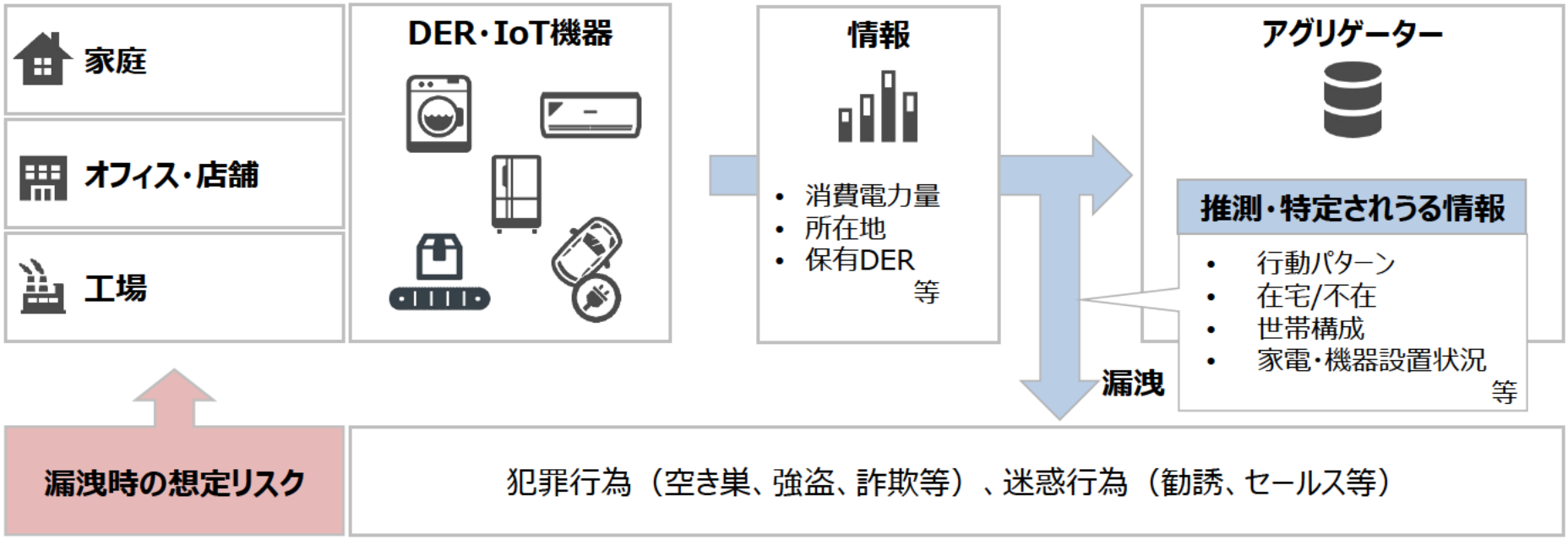
☆1で考慮する主な脅威			脅威に対抗するために☆1で求める適合基準			
			IoT製品に対する適合基準		IoT製品ベンダーに対する適合基準	
			カテゴリ	適合基準の概要	カテゴリ	適合基準の概要
1.	①弱い認証機能により、	外部からの不正アクセスの対象となり、マルウェア感染や踏み台となる攻撃等を受けることで、情報漏えい、改ざん、機能異常の発生につながる脅威	識別・認証、アクセス制御	(1)適切な認証に基づく**アクセス制御**[1-3,5-5] (2)**容易に推測可能なデフォルトパスワードの禁止**[1-2,1-1] (3)パスワード等の認証値の変更機能[1-4] (4)ネット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。

（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案～概要説明資料～

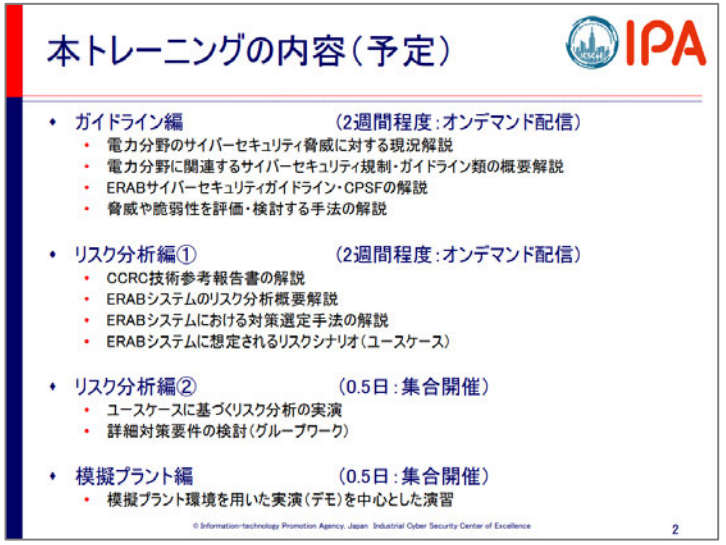
③ アグリゲーターが機器から取得する情報に起因するリスクについて

- DRサービスにて機器の制御を実施するに当たり、アグリゲーターは制御機器の稼働状況を把握するため、**機器の消費電力量等情報を収集する必要**がある。
- アグリゲーターが収集した機器の情報から、**利用者の在・不在が推測できる場合も存在し**、機器の情報を元にした犯罪へつながる脅威を含め、**情報のセキュリティリスクは高まっている**。
- このように情報に関する価値が多様化する中、現状想定されるセキュリティリスクを踏まえ、セキュリティ対策として**必要な要求事項**を検討後、記載する。



ERABシステムに関するセキュリティ教育プログラム

- ERABサイバーセキュリティガイドラインでは、対策事項の一つとして、「**第三者による監査（認証を含む）や教育プログラム等によって勧告指定項目を中心にその実装を検証すること**」を勧告として求めている。
- また、具体的な教育プログラムとして、IPAの産業サイバーセキュリティセンター（ICSCoE）において、ERAB事業者に対する**短期のサイバーセキュリティ教育プログラムを開催**している。
- ERABセキュリティガイドラインの改定内容を踏まえ、**プログラムを一部更新**し、**よりERABの実態に沿った内容にて開催予定**。



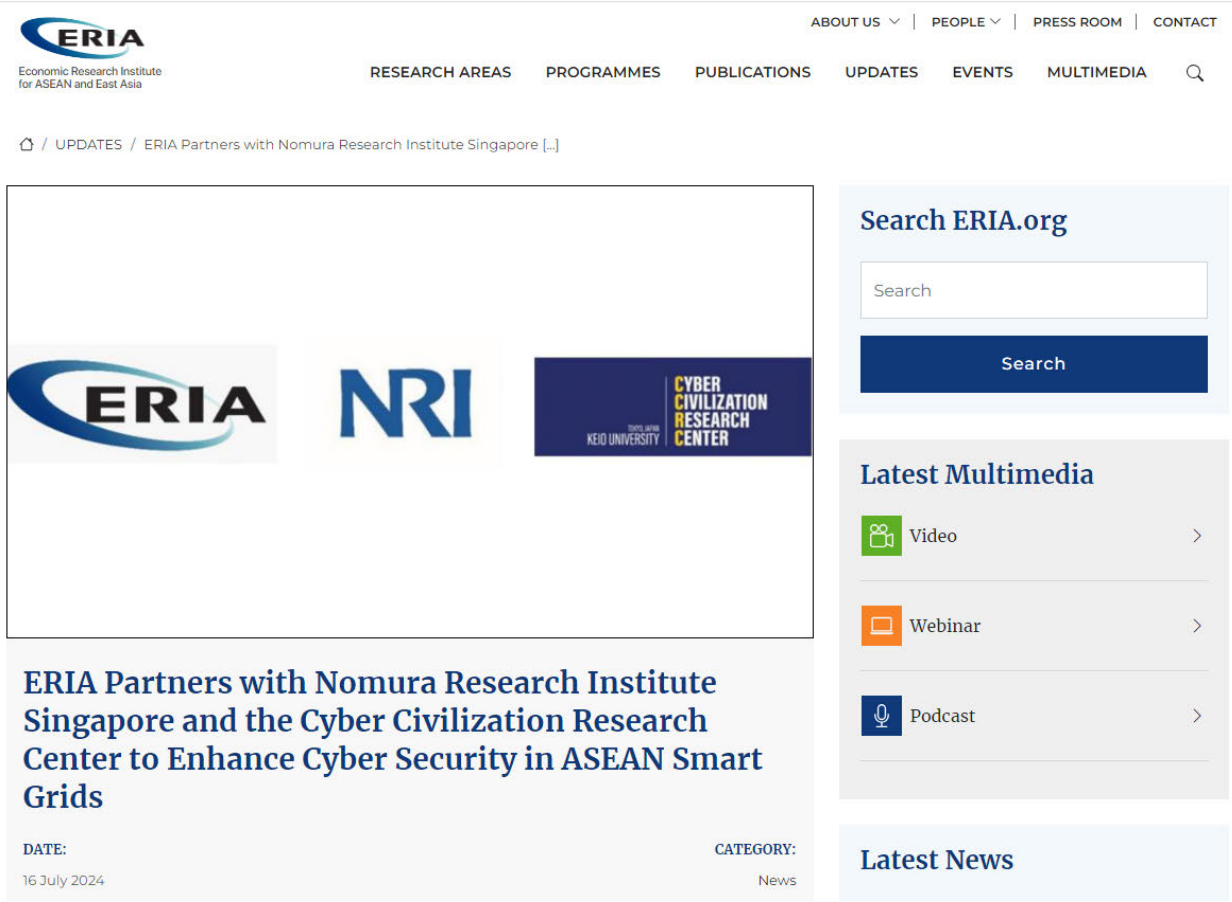
（出所）【実務者向けプログラム】令和４年度第１回（10月開催）ERABサイバーセキュリティトレーニング ご案内資料

【ERABセキュリティの国際展開に関する取組】
日ASEANにおける分散型電源のサイバーセキュリティ対策の推進について

- 2024年度、東アジア・アセアン経済研究センター（ERIA）において、**ASEANにおける分散型エネルギーシステム（DES）とスマートグリッドの推進とサイバーセキュリティの確保に向けたプロジェクト**が実施されることとなっている。
- 2023年12月の**アジア・ゼロエミッション共同体（AZEC）首脳共同声明**において、「地域間連携及び**系統柔軟化の拡大**」、「**離島等における信頼性の高い再生可能エネルギーベースのマイクログリッド**」を進めることとされており、**分散型電源の活用とスマートグリッドの推進に向けて、実態調査やサイバーセキュリティの確保に向けた制度等の検討を行う本プロジェクトは、AZECの実現に貢献するもの**。
- 具体的な取組としては、以下を実施する予定
  - ASEAN各国における需要家側のエネルギーリソースの活用も含む分散型電源の普及の状況や法律などの制度整備の現状、及びサイバーセキュリティ確保についての現状調査を行う。
  - 慶応義塾大学サイバー文明研究センター（CCRC）やSOI ASIA（School on Internet Asia）と連携しながら、日ASEAN各国の有識者・実務者を集めた検討体制を構築し、調査結果を共有、分散型電源活用に向けて必要な課題を整理するとともに、分散型電源の信頼性を支えるサイバーセキュリティ確保について、日本のERABサイバーセキュリティガイドラインの考え方の共有、日ASEAN共通のセキュリティ課題の抽出、IECにおける取組の共有を行う。
  - 年度内に、本取組の各国への展開を念頭においたサイバーセキュリティワークショップを複数回実施する。
- **日本のERABの取組を、こうした国際展開の取組と連動させていくことで、日本の仕組みを国際的に普及させ、アグリゲーターなどが海外展開をしやすい環境づくりを進めていく**。

【参考】ERIAプレスリリース（2024年7月16日）

- 2024年7月16日、ERIAは、野村総合研究所（NRI）シンガポールおよび慶應義塾大学サイバー文明研究センター（CCRC）と共同で、**ASEANにおける分散型エネルギーシステム（DES）とスマートグリッドの推進とサイバーセキュリティの確保に向けたプロジェクト**を実施することを発表した。



出所）ERIA、
https://www.eria.org/news-and-views/eria-partners-with-nomura-research-institute-singapore-and-the-cyber-civilization-research-center-to-enhance-cyber-security-in-asean-smart-grids

ERABサイバーセキュリティガイドライン改定に向けた今後のスケジュール

- 関連事業者と連携の上、**今年度中のERABサイバーセキュリティガイドライン改定を目指す**。
- なお、改定案の公表は本検討会にて提示の上、パブリックコメントを実施する。

〈今後の進め方〉

項目	2024年度							
	8月	9月	10月	11月	12月	1月	2月	3月
次世代の分散型電力に関する検討会　開催予定日程	★			★		★		
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・文面案検討		■	■	■				
改定案原案公開				★				
パブリックコメント実施・回答・文面修正				■	■	■		
パブリックコメントの結果を踏まえた改定案公開						★		
IPA研修　実施予定日程				(★)	(★)			