経済産業省

資料５－３

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

２０２４年１０月２２日

資源エネルギー庁

1．電力サブワーキング（第16回）の振り返り

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。**また、末端のIoT機器等における脆弱性対応の高度化に向け、**脆弱性情報の共有や管理等のあり方についても整理することが必要ではないか。**
  その上で、**既存ガイドラインへの影響や整合性等を確認した上で、どのようにこれらを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、事業者のビジネス環境を考慮したうえで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**サイバー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。**

12

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 - 2

2．ERABサイバーセキュリティーガイドラインについて ①

ガイドラインの構成

ERABサイバーセキュリティガイドラインは、アグリゲーターをはじめとするERAB事業者が取り組むべきサイバーセキュリティ対策を整理したもの。2017年に初版を策定し、2019年12月に改正版（Ver 2.0）を公表。

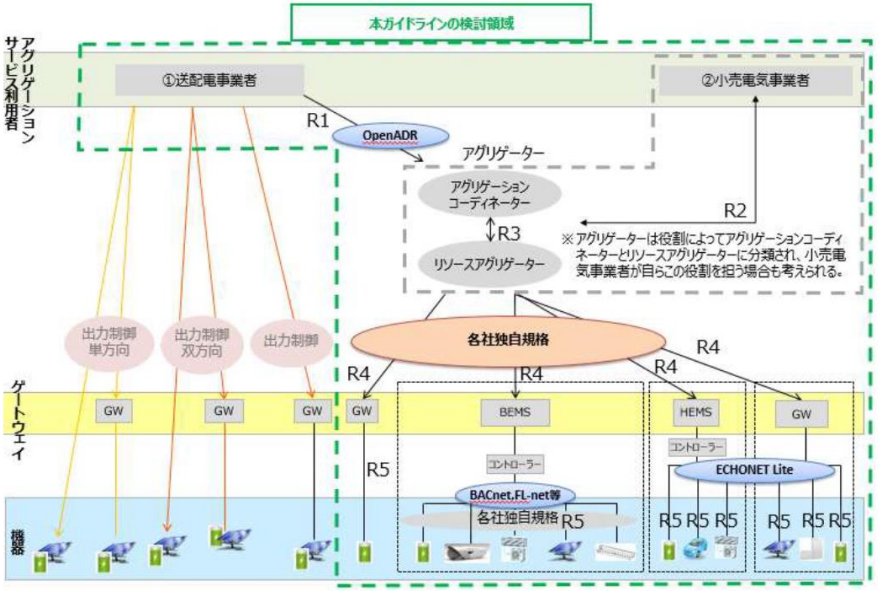
《ERABセキュリティガイドラインの構成》

1. はじめに
2. ガイドラインの位置づけ
3. ERABシステム
   - 3.1. ERABシステムの構成
   - 3.2. ERABシステムが留意すべき基本方針
   - 3.3. ERABシステムが想定すべき脅威
   - 3.4. ERABシステムが維持すべきサービスレベル
   - 3.5. ERABシステムにおけるシステム重要度の分類
   - 3.6. ERABシステムにおけるサイバーセキュリティ対策
   - 3.7. 取扱情報の差異によるERABシステムの分類
   - 3.8. 標準対策要件に基づく詳細対策要件の設計
   - 3.9. ガイドラインの継続的改善
4. 本ガイドラインを踏まえた各事業者における対策の在り方
   - 4.1. ERABに参画する各事業者によるPDCAサイクルによる継続的なセキュリティ対策の実施

2．ERABサイバーセキュリティーガイドラインについて ②

ガイドラインの対象となるシステム

ERABシステムは、送配電事業者の簡易指令システム、小売電気事業者のシステム、アグリゲーションコーディネーター（AC)のシステム、リソースアグリゲーター（RA）のシステム、HEMS等エネルギーマネジメントシステム、エネルギー機器と外部システムとのゲートウェイ（GW）及びERABの制御対象機器より構成される。



出所：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（令和元年12月27日改定、資源エネルギー庁　独立行政法人情報処理推進機構[IPA]）

2．ERABサイバーセキュリティーガイドラインについて ③

ガイドラインの位置付け

ERABに参画する各事業者が実施すべき最低限のサイバーセキュリティ対策の要求事項を示したガイドラインであり、各事業者はガイドラインを踏まえて、自らの責任においてセキュリティ対策を講ずることが求められる。

ガイドラインの記載事項は、実装を必須として義務づけられる【勧告】と、実装を検討すべき内容である【推奨】に分類される。

ガイドラインの基本方針

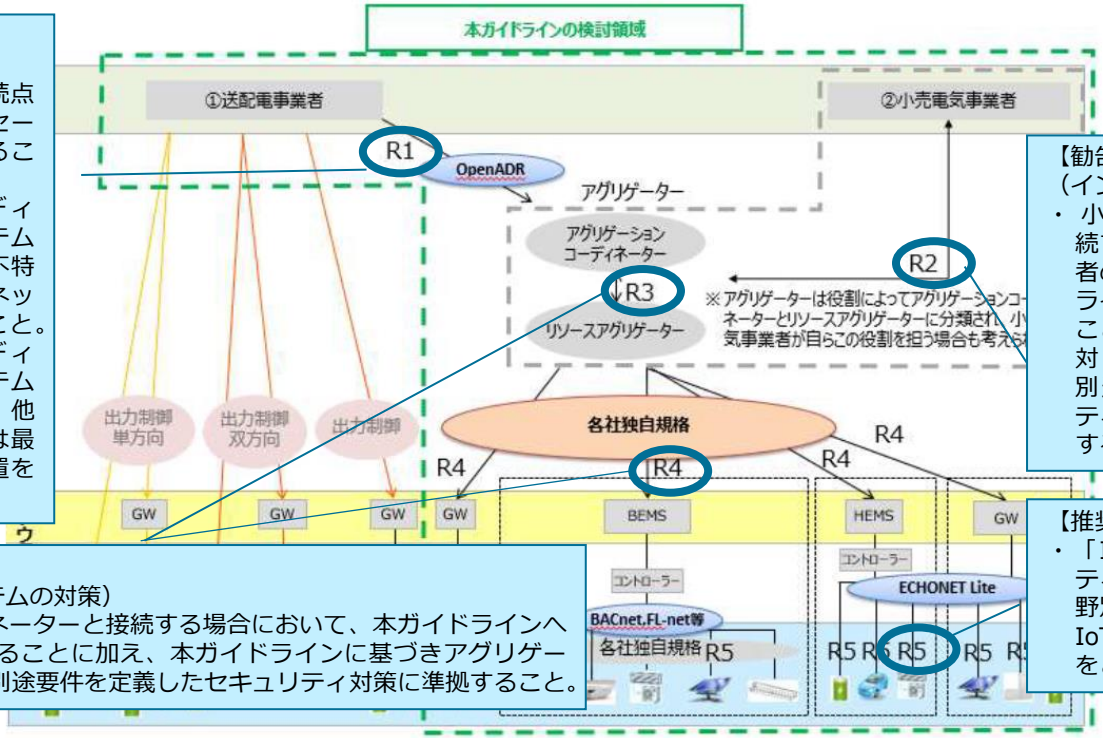
【勧告】として、ERAB事業者は、脆弱性対策情報の利用者への通知の実施や、脆弱性対策情報・脅威情報の共有の取組について定め、それについて協力することが求められる。

【推奨】として、ERABシステムは、取り扱うハードウェアとそれが保有するデータの機密性、完全性、可用性の３要件に留意したシステム設計を行うことが求めらる。

2．ERABサイバーセキュリティーガイドラインについて ④

【勧告】【推奨】の例（一部抜粋）

【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認証、通信メッセージは暗号化により保護すること。
・アグリゲーションコーディネーターの簡易指令システムとの直接的な接続部は、不特定多数がアクセスできるネットワークと原則分離すること。
・アグリゲーションコーディネーターの簡易指令システムとの直接的な接続部は、他ネットワークとの接続点は最小化し、接続点に防御措置を講じること。



【勧告】
（インターフェースの対策）
・ 小売電気事業者のシステムと接続する場合には、小売電気事業者の保有するシステムをガイドラインに準拠することを求めること。また、小売電気事業者に対して、ガイドラインに基づき別途要件を定義したセキュリティ対策を構築し、それに準拠することを求めること

【勧告】
（事業者とその保有するシステムの対策）
・アグリゲーションコーディネーターと接続する場合において、本ガイドラインへ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。

【推奨】
・「IoT 開発におけるセキュリティ設計の手引き」、「製品分野別セキュリティガイドライン IoT-GW 編」等を参照した対策をとること。

3．想定する改定点について

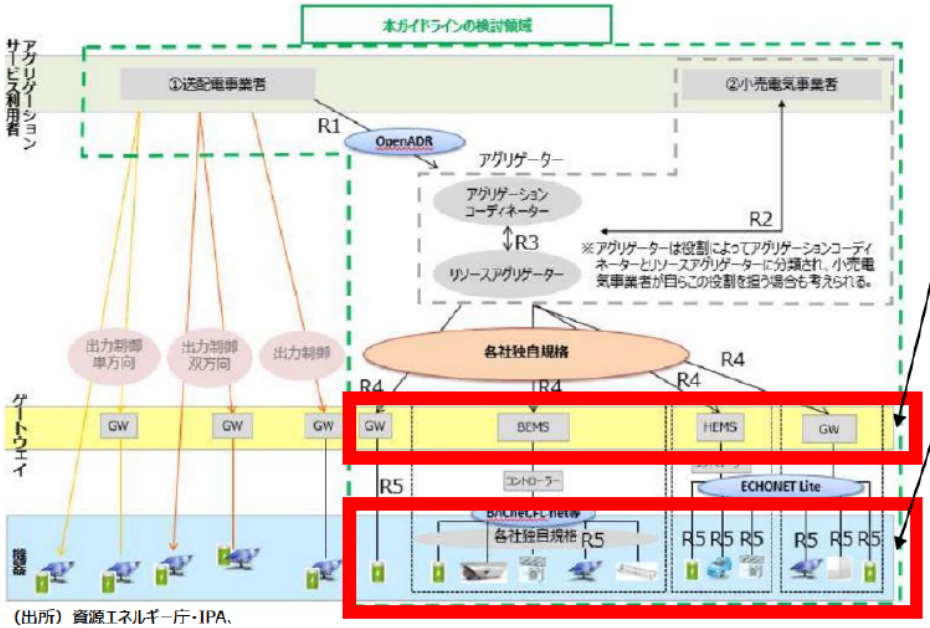
想定する改定点について

- 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。

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

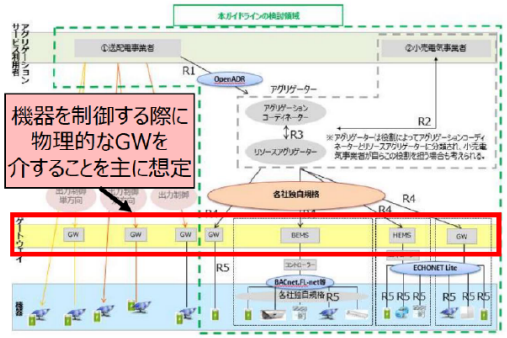
3．想定する改定点について ①

① 物理的なGWを介さないDRサービスへの対応

① 物理的なGWを介さないDRサービスについて

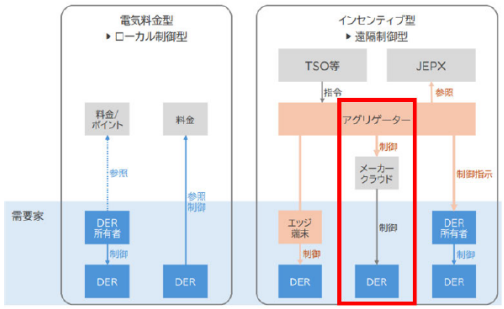
- **ERABにおける機器の制御モデル**として、従来のBEMSやHEMS等、物理的なGWを介して通信・制御を行うモデルに加え、**メーカークラウドなど、物理的なGWを介さずに通信・制御を行うDRサービスが増加**してきている。
- 上記のような前回のERABサイバーセキュリティガイドライン改定時からの環境変化を踏まえ、**セキュリティ対策の要件事項及び対応方針**を検討後、記載する。

〈ERABシステムにおける全体図〉



（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

〈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）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

6

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

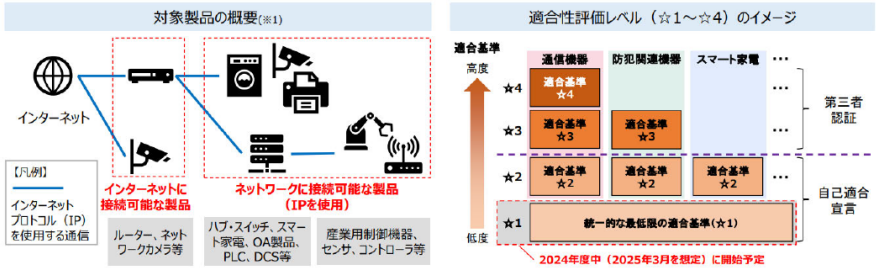
3．想定する改定点について ②

② 末端のIoT機器等の脆弱性に起因する脅威への対応

② 末端のIoT機器等の脆弱性に起因する脅威について

- **IoT機器の脆弱性を狙ったサイバー攻撃が増加傾向**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、**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**すべく、**IoT製品に対するセキュリティ適合性評価制度の検討**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、**ERABの制御対象となるIoT機器に必要な要求事項を検討**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～

7

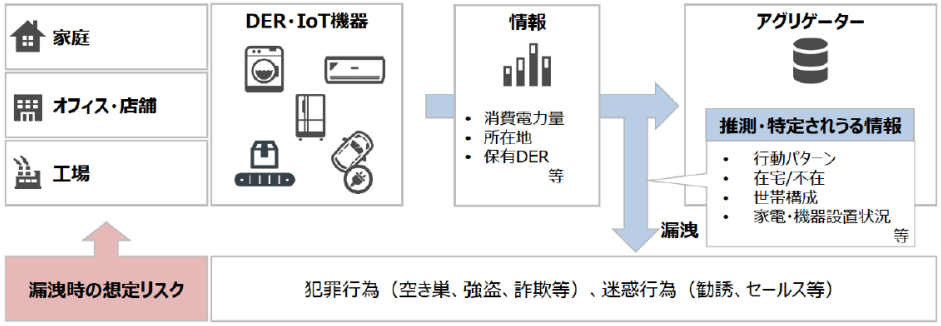
第10回 次世代の分散型電力システムに関する検討会　資料４

3．想定する改定点について ③

③ 機器から収集した情報のリスクへの対応

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。

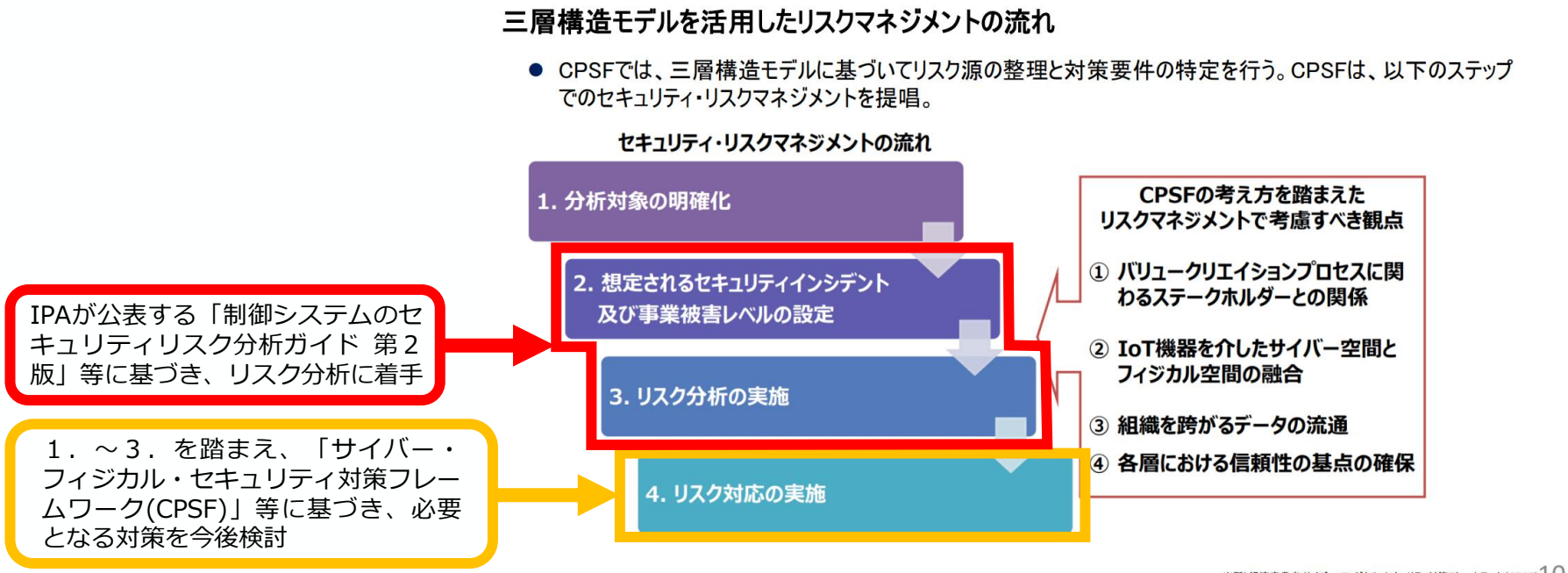


11

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

4．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

5．ERABシステムに関するセキュリティ教育プログラム

- 「実務者向けプログラム ERABサイバーセキュリティトレーニング 」について、**<u>リスク分析等のアップデート</u>**を行った上で、**<u>下記内容で開催予定</u>**。

開催概要

IPA

VPPの社会実装を見据えた、ERABにおけるサイバーセキュリティ対策

※VPP ： Virtual Power Plant

対象業界・対象者

ERAB事業者（AC、RA）等において
- 対策を検討し、立案・実施する実務者の方
- 対策の導入・実施を判断する責任者の方

※AC ： Aggregation Coordinator
RA ：Resource Aggregator

➢ **ITパスポート試験合格者相当の知識、およびOTの基礎知識を有していることを推奨します。**

日程・実施形式

日程	実施形式	
2024年11月25日（月） ～ 2024年12月9日（月）	オンライン実施	e-Learning システムを用いたオンデマンド配信
2024年12月11日（水） ～ 2024年12月12日（木）	集合実施	東京都千代田区外神田4-14-1 秋葉原UDX 北ウィング20階（N20F）

受講料・定員

- **受講料 ： 20万円（税込）** ※受講料には、交通費・食事代・通信費等は含みません。
- **定員 ： 40名** ※**最少催行人数10名**。定員になり次第、募集を締め切らせて頂きます。

1

本トレーニングの内容（予定）

IPA

オンライン実施

- **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解説
  - 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**
  - CCRC技術参考報告書の解説
  - ERABシステムのリスク分析概要解説
  - 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）

集合実施

- **模擬プラント編**
  - リソース関連設備を用いたERABシステムのリスクの体感・解説
  - 模擬プラントを用いたERABシステムのリスクの体感・解説
- **リスク分析編②**
  - ユースケースに基づくリスク分析の実演
  - 詳細対策要件の検討（グループワーク）

3

出所：独立行政法人　情報処理推進機構HP

6. ERIAにおける日ASEANのERABセキュリティに関する取組（参考）
Research Study on Promoting Cyber Security for Distributed Energy Systems (DES) and Smart Grids in ASEAN

- 2024年10月15日、東アジア・ASEAN経済研究センター（ERIA）における、**日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**の初回ワークショップが開催された。

- 初回は、インドネシア・ジャカルタで開催され、慶応義塾大学梅嶋特任教授リードの下、インドネシア、マレーシア、タイの大学等のアカデミアや、インドネシア政府機関など、オンライン含め80人程度が参加した。ワークショップの議題は以下のとおり。

  - ✓ 本プロジェクトとワークショップの目的について：ERIAのAZEセンターNuki所長
  - ✓ 講演1 ERABとCPSFに関するIECの取組の紹介：慶応義塾大学サイバー文明研究センター梅嶋特任教授
  - ✓ 講演2 DESに関する動向とCPSFに関する日本のイニシアティブの紹介：エネ庁電力産業・市場室 加畑補佐
  - ✓ 講演3 ASEANにおけるDESとスマートグリッドのサイバーセキュリティ推進について：野村総合研究所シンガポール
  - ✓ パネルディスカッション：ASEANと日本のERAB取組の連携について
    パネルディスカッションでは、マレーシアNAv6のサイバーセキュリティセンター長、タイのチェラロンコン大学電気工学科准教授からプレゼンがあり、講演者とERABに関する連携について、ディスカッションが行われた。

- 今後は、2025年1月頃にマレーシア・ペナンにてテストベッドの見学と議論を行い、3月頃にプロジェクトのまとめとして、インドネシア・ジャカルタにて大規模カンファレンスを開催し、日ASEANにおける分散型電源のサイバーセキュリティに関する指針の策定を目指す。

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

7. 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、改定に当たっては、**専門家**からの意見に加え、事業者のビジネス環境を考慮するため、**業界団体（一般社団法人エネルギーリソースアグリゲーション事業協会）**にも意見をもらった上で、パブリックコメントを経て、**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				★	★			