資料６－２

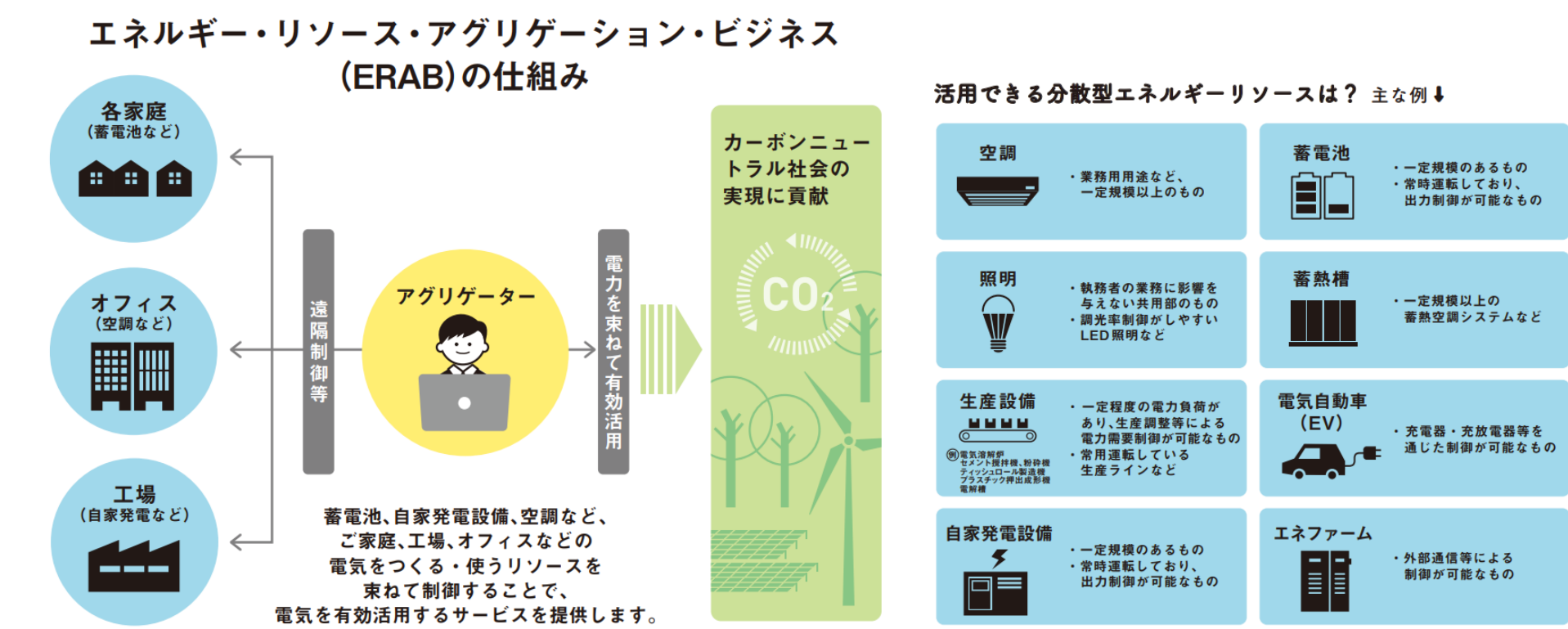
アグリゲーター及び分散型エネルギー源（DER）のセキュリティ対策について

2024年 2月 1日

アグリゲーター／ERABとは

- 分散型エネルギー源（DER）や需要家側エネルギーリソース（太陽光発電、定置用蓄電池、ネガワット等）の導入拡大に伴い、新たなビジネス領域として、**エネルギー・リソース・アグリゲーション・ビジネス（ERAB）が注目**されている。

- 契約に基づき、**自家発電設備・空調・蓄電池等のリソースを遠隔制御することで電力を束ねる事業者**をアグリゲーターと呼び、**一定の要件を満たすアグリゲーターは電気事業法上「特定卸供給事業者」として、事業に当たって資源エネルギー庁への届出が必要**となる。



出所）資源エネルギー庁、みんなの電気を賢く使う エネルギー・リソース・アグリゲーション・ビジネス（ERAB）
https://www.enecho.meti.go.jp/category/saving_and_new/advanced_systems/vpp_dr/files/erab_tirashi.pdf

DERの担い手としてのアグリゲーター（特定卸供給事業者）の状況

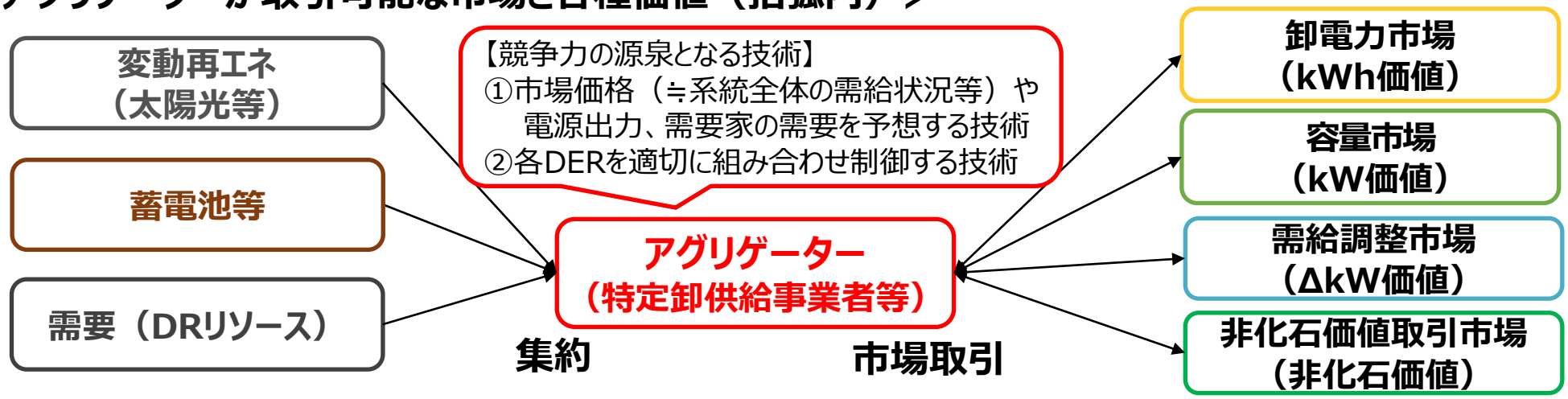
- **アグリゲーター**は、DERの持つ各種価値を集約し、**市場取引等で活用する主体の総称**を指す。**特定卸供給事業者や小売電気事業者等がその役割を果たしうる**。2024年1月2日時点で61社が**特定卸供給事業者**として登録されている。

実ビジネス化しているアグリゲーター（ライセンス取得者）の例

株式会社エナリス	株式会社 タクマエナジー	積水化学工業株式会社	オリックス株式会社	パシフィックパワー株式会社
アズビル株式会社	東北電力株式会社	大阪瓦斯株式会社	Goal Connect 株式会社	株式会社グローバルエンジニアリング
九州電力株式会社	電源開発株式会社	テス・エンジニアリング株式会社	アーバンエナジー株式会社	MCリテールエナジー株式会社
エネルエックス・ジャパン株式会社	株式会社ＵＰＤＡＴＥＲ	東邦ガス株式会社	カスタマイズドエナジーソリューションズジャパン株式会社	東京電力エナジーパートナー株式会社
北陸電力株式会社	三菱重工業株式会社	北海道電力株式会社	四国電力株式会社	中部電力ミライズ株式会社

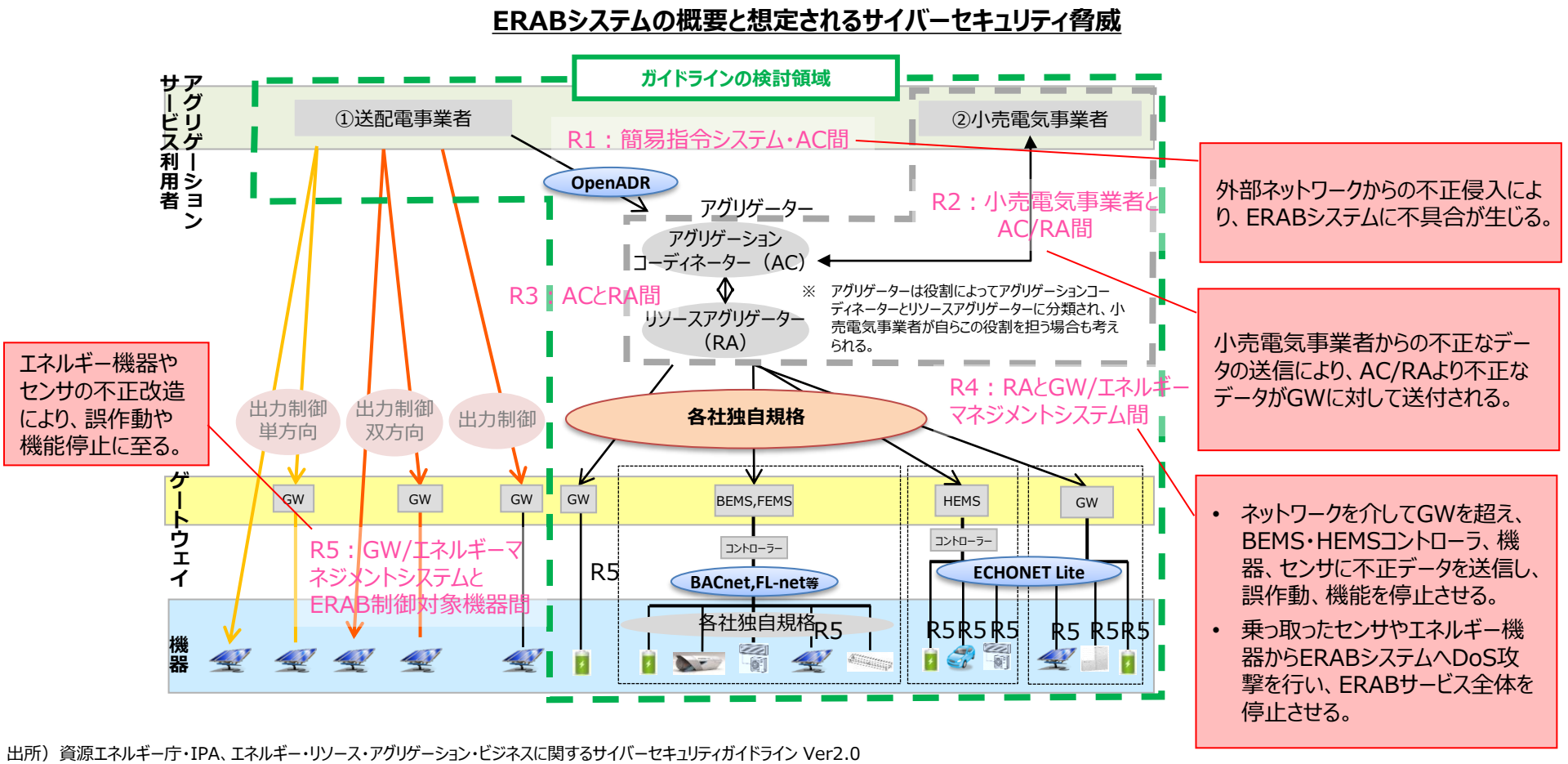
等　合計61社（2024年1月2日時点）

＜アグリゲーターが取引可能な市場と各種価値（括弧内）＞



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

- 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に関する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。

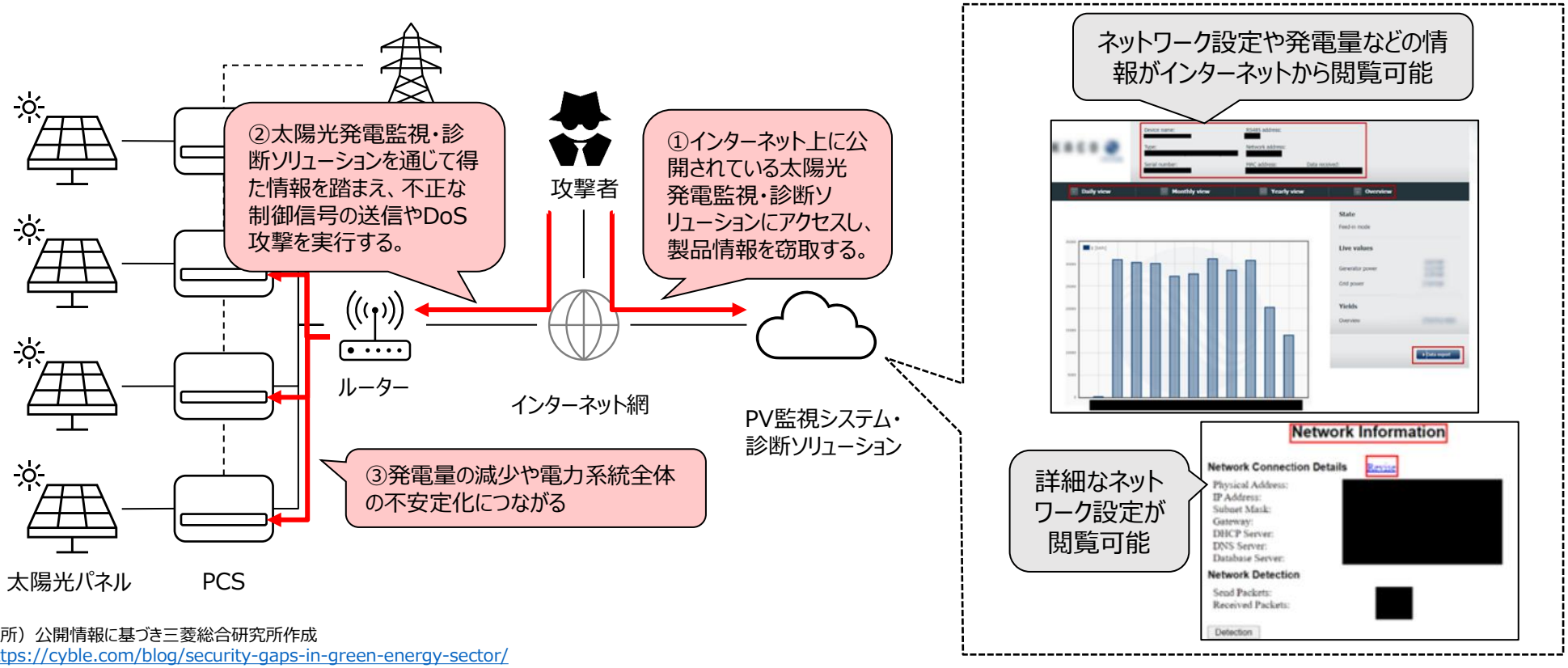


出所）資源エネルギー庁・IPA、エネルギー・リソース・アグリゲーション・ビジネスに関するサイバーセキュリティガイドライン Ver2.0
https://www.enecho.meti.go.jp/category/saving_and_new/advanced_systems/vpp_dr/files/20171129002-1.pdf

（DER設備に関する脅威事例）インターネットからアクセス可能なPV監視・診断ソリューション

- 2023年7月、サイバーセキュリティ企業のCyble社は、**130,000件以上のPV（太陽光発電）監視・診断ソリューションがインターネット上からアクセス可能である**ことを報告した。
- 同社は、PV監視・診断ソリューションを通じて、**攻撃者が製品情報を閲覧可能な状態である**ことから、**潜在的な攻撃の対象となっていると警告**した。
- 公開されていたソリューションのベンダーには、Solar-Log社、SMA社のほか、国内ベンダーのコンテック社も含まれていた。

実際にインターネットからアクセス可能であったページと情報を悪用した攻撃のイメージ



出所）公開情報に基づき三菱総合研究所作成
https://cyble.com/blog/security-gaps-in-green-energy-sector/

（DER設備に関する脅威事例）PVインバーターにおける脆弱性の公開

第7回電力SWG
資料5-1より

- 2017年、**独SMA社のPVインバーターにおける14の脆弱性が公開**された。
- これらの脆弱性を悪用することで、最終的に電力系統が停電に陥ると指摘された。
  ※ SMA社は不完全な情報・分析であると反論しつつ、深刻な脆弱性に関しては修正を実施した。

《報告された主要な３つの脆弱性》

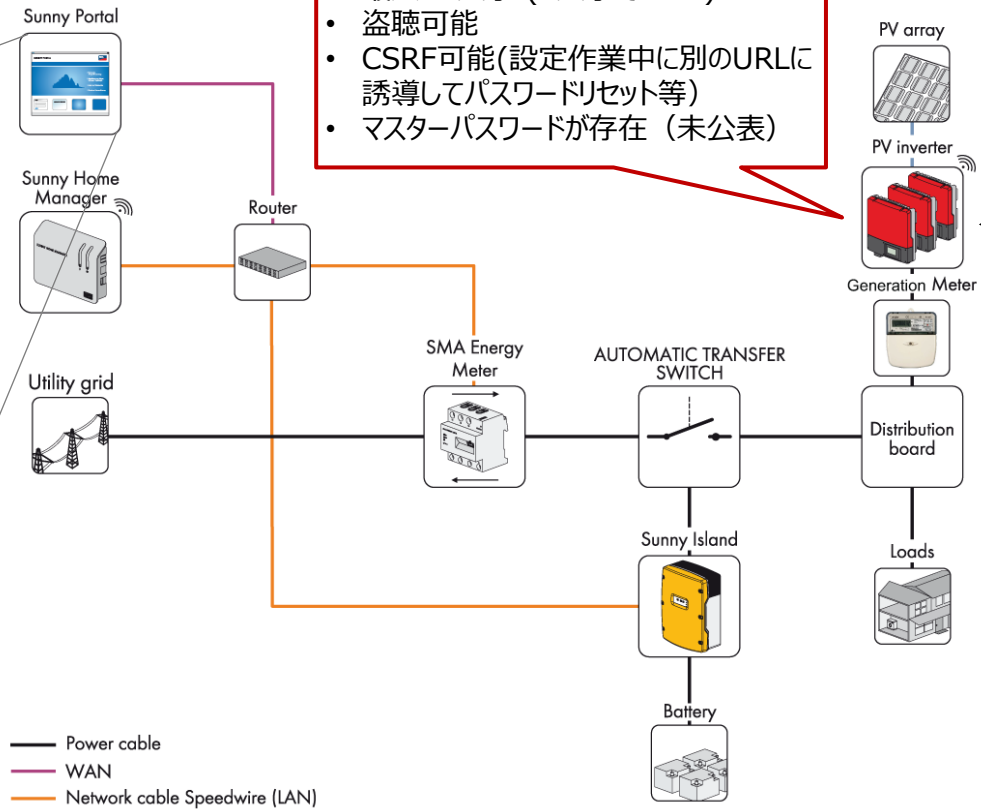
1.他者管理のPVインバータの情報窃取

PVインバータへのイベントログ問合せ先を書き換えることで、自分の管理していないPVインバータの情報まで入手可能。
(SMAは関連サービスを届出翌日に停止)

Sunny Portalとは、PV管理者用のWebサービス

2.パスワードに関する脆弱性

- 最大12文字 (1文字でもOK)
- 盗聴可能
- CSRF可能(設定作業中に別のURLに誘導してパスワードリセット等)
- マスターパスワードが存在（未公表）



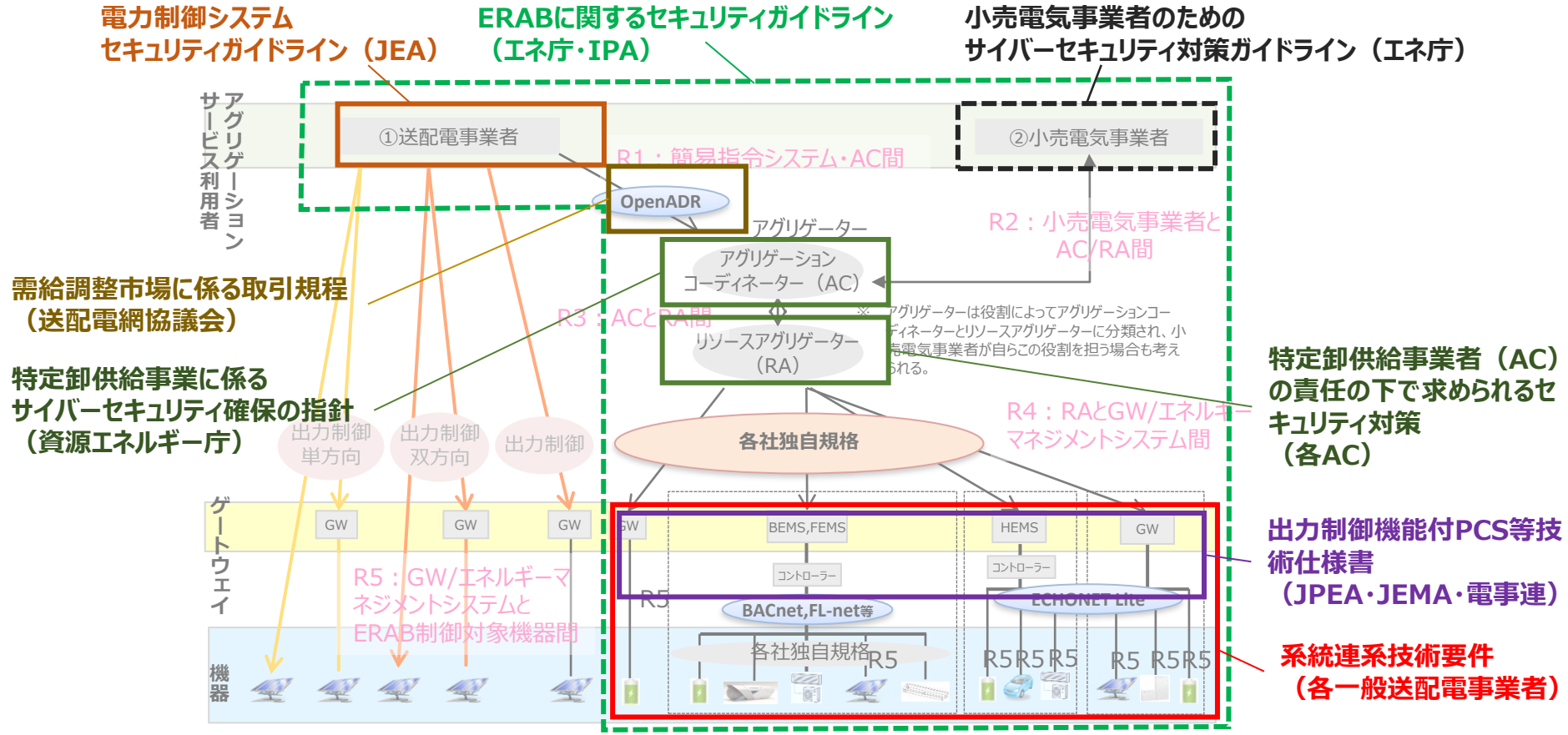
3. 改ざんしたファームウェアのアップデート

自分でインストールしていないPVインバータに対しても、SMAの管理ツールから攻撃者が改ざんしたファームウェアへアップデート可能。

出所）公開情報に基づき三菱総合研究所作成
https://horusscenario.com/, https://www.esi-africa.com/wp-content/uploads/2015/05/Hilton-Hunkin.pdf

ERABシステムが準拠すべきセキュリティガイドライン等

- ERABシステムに求められるセキュリティガイドラインとして、**システム全体に対する「ERABに関するサイバーセキュリティガイドライン（以下、ERABセキュリティガイドライン）」があるほか、個々のステークホルダーに対するガイドラインが整備**されている。
- 末端のリソースに関して、系統に接続する設備は「系統連系技術要件」に基づく対策が求められるほか、出力制御機能付PCSについて、セキュリティの要件を含んだ技術仕様書が公開されている。



出所）各種ガイドラインに基づき三菱総合研究所作成

※ 実線は義務で対策が求められるガイドライン等、点線は任意で対策が求められるガイドライン等を意味する。

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においても、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**」が勧告事項として、定められている。
- 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）では、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。 ※ 2023年度はプログラム更新のため休止。

開催概要

IPA

テーマ

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

※ERAB：Energy Resource Aggregation Businesses

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

➢ **ITパスポート試験合格者相当の知識を有していることを推奨します**

※AC：Aggregation Coordinator
RA：Resource Aggregator

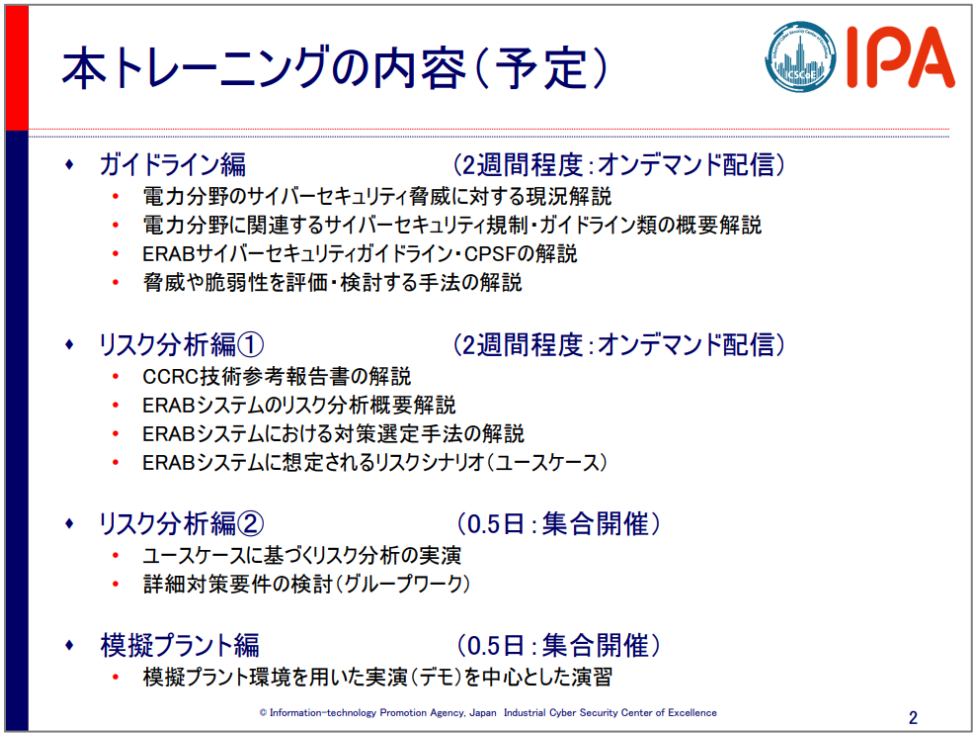
開催日程・場所

下記の日程で本トレーニングを構成しています（全日程にご参加いただきます）

- **2022年10月3日（月）　オンライン開催**
  ～ 2022年10月14日（金）　（e-Learning システムを用いたオンデマンド配信）
- **2022年10月17日（月）　集合開催**（東京都千代田区外神田4-14-1 秋葉原UDX 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　：20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



本トレーニングの内容（予定）

IPA

- **ガイドライン編**　（2週間程度：オンデマンド配信）
  - 電力分野のサイバーセキュリティ脅威に対する現況解説
  - 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・CPSFの解説
  - 脅威や脆弱性を評価・検討する手法の解説
- **リスク分析編①**　（2週間程度：オンデマンド配信）
  - 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）
- **リスク分析編②**　（0.5日：集合開催）
  - 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）
- **模擬プラント編**　（0.5日：集合開催）
  - 模擬プラント環境を用いた実演（デモ）を中心とした演習

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
https://www.ipa.go.jp/jinzai/ics/short-pgm/erab/ngi93u000000kopy-att/000100496.pdf

アグリゲーターが抱えるセキュリティにおける課題

- これまで、アグリゲーターのセキュリティ対策に関する様々な取組が進められてきたところであるが、事業者や有識者と意見交換やヒアリングを実施したところ、以下の課題が確認された。
- 具体的には、ERABセキュリティガイドラインの準拠のために、**各社で詳細対策要件を作成することが求められている一方で、現状ではその作成が困難であることや、作成した詳細対策要件の妥当性を確認することが難しいことの課題**が挙げられた。
- 加えて、これまでのガイドラインでは具体的に想定してこなかった電力系統及びアグリゲーターシステムに接続する**末端のIoT機器等のセキュリティ対策に対するリスク**が示唆された。
- また、業界として、アグリゲーターにおけるセキュリティ対策の実態を把握出来ていない課題が挙げられた。

課題概要	課題内容
詳細対策要件の作成・確認について	• **ERABセキュリティガイドラインに準拠するための詳細対策要件を作成するのが難しい。** • チェックシートを作成する場合は、事業の重要度によって対策要件が変わることが望まれる。 • **自社で作成した詳細対策要件に抜け漏れがある可能性**がある。
末端のIoT機器等の脆弱性に起因する脅威について	• **ERABセキュリティガイドラインのR4,R5にあたるIoT機器等のセキュリティを高めることが望まれる。** • **特に太陽光のリソースは数が増えている一方、セキュリティの検討が不十分である。**
ガイドラインの定期アップデートについて	• アグリゲーションは一過性ではなく、様々な分散型エネルギー源が追加されるため、ガイドラインを定期的にメンテナンスする必要がある。

ERABセキュリティガイドラインにおける詳細対策要件に関する記載

- ERABセキュリティガイドラインでは、ERABに参画する事業者において、**具体的な対策を策定した「詳細対策要件」を自らの責任で策定することを勧告事項として求めている**。
- 詳細対策要件の内容について、脅威に対する対策例を詳細に検討し規定するほか、ERABシステムに関係する特定のテーマに応じた対策について規定することが求められているが、**具体的な策定方法、内容、対策のレベル感等については明記されていない**。

3.8.　標準対策要件に基づく詳細対策要件の設計

【勧告】

・　ERAB に参画する各事業者は、実運用に耐え得るべく、標準対策要件の考え方に基づき、具体的なサイバーセキュリティ対策を自らの責任で策定すること。

本ガイドラインは、標準対策要件を記載したものである。標準対策要件は、事故が起こり得ることを前提として継続的に対策を改善する必要があることを踏まえ、ERAB システムのセキュリティ対策に取り組むに際しての基本的な考え方、各セキュリティマネジメント要求事項を実施する目的・考え方等を規定するとともに、ERAB システムのサービスレベルを維持するために事業者が実施すべき最低限のセキュリティ対策を記載したものである。

詳細対策要件は、ERAB に参画する各事業者が、実運用に耐え得るべく、標準対策要件の考え方に沿って行われる具体的な対策を自らの責任で策定するものである。具体的には、ERAB システムの構成要素毎に想定される脅威、当該脅威と事業リスクとの相関関係を踏まえ、（ⅰ）抑止、（ⅱ）内部防御・情報保護、（ⅲ）侵入・攻撃検知、（ⅳ）被害把握・事業継続の各フェーズにおける当該脅威に対する対策例を詳細に検討し、規定する。これに加えて、標的型攻撃等への対策、サイバー攻撃と物理攻撃の組合せによる攻撃への対策など、構成要素毎に実施すべき対策ではなく、ERAB システムに関係する特定のテーマに応じた対策について規定する。

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
https://www.enecho.meti.go.jp/category/saving_and_new/advanced_systems/vpp_dr/files/20171129002-1.pdf

ERABセキュリティガイドラインにおける末端DERのセキュリティ対策に関する記載

- R4においては、インタフェースの対策として、**外部システムとの相互接続点における認証や通信の暗号化**が求められているほか、**アグリゲーションコーディネーター（AC）が作成する詳細対策要件に対する準拠**が求められている。そのため、**詳細対策要件が適切に策定されていない場合、ゲートウェイ設備の対策が不十分なものになるおそれ**がある。
- また、末端のR5においては、「IoT開発におけるセキュリティ設計の手引き」等を参照した対策が推奨されている。

3.6.4. R4（リソースアグリゲーターと GW または BEMS・HEMS 等エネルギーマネジメントシステム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）

- リソースアグリゲーターの制御対象の機器または 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[19]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。

  ※本ガイドラインは、リソースアグリゲーター、BEMS・HEMS 等のサーバーと GW 間の通信路[20]として、公衆網が使われる場合を前提としている。なお、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、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うるものと考えられる。

（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。

3.6.5. R5（GW 配下で需要家側に設置される ERAB 制御対象のエネルギー機器間[21]のインターフェース）

【推奨】

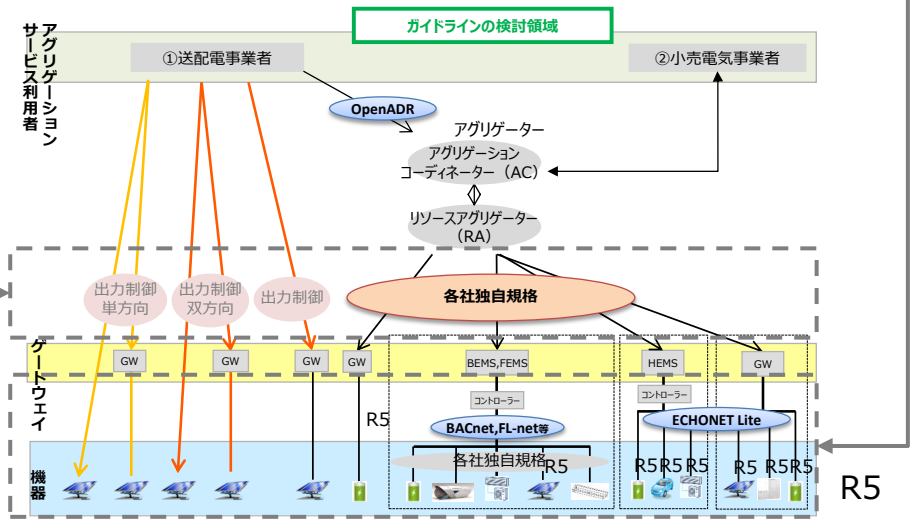
（事業者とその保有するシステムの対策）

- ERAB 制御対象のエネルギー機器、センサには、リソース制約がある機器が存在し、セキュリティ機能の追加・更新が困難な既設の設備等も含まれる。「IoT 開発におけるセキュリティ設計の手引き」[22]、「製品分野別セキュリティガイドライン IoT-GW 編」[23]等を参照した対策をとること。

（インターフェースの対策）

- 外部システム・機器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。

R4



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
https://www.enecho.meti.go.jp/category/saving_and_new/advanced_systems/vpp_dr/files/20171129002-1.pdf

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。**

【参考：IoTに関する取組動向】経産省におけるIoT製品に対する適合性評価制度の検討

- IoT製品のセキュリティ対策を適切に評価し、適切な対策が講じられているIoT製品が広まる仕組みの構築の必要性や諸外国の取組を踏まえ、経済産業省は、**IoT製品に対するセキュリティの適合性評価制度（ラベリング制度）を検討する「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」を2022年11月に設置し、2023年5月に中間報告をとりまとめた**。
- 委員は、学術界、法曹界、業界団体、企業、消費者団体から構成され、オブザーバとして、関係省庁、研究機関、認証機関が参画している。
- 2023年度中の最終報告に向け、今年度も議論を継続している。

中間報告（概要）

検討会において議論した事項

● **課題**

ベンダ、利用者、国民の三者において、以下の課題が存在。

✓ **ベンダ**： **対策が評価されず製品価値に繋がらない**。諸外国の制度対応負担が増加。
✓ **利用者**： **適切な対策の製品が可視化されていないため、適切な製品を選べない**。
✓ **国民**： 適切でない製品が多く流通した場合、IoTがボット化するなどして、**国内のシステムや国民生活に悪影響を及ぼす**。

● **構築すべき適合性評価制度**

✓ ベンダによる能動的なセキュリティ向上を促す観点や、特に中小企業の負担の観点から、**まずは任意制度として制度を運用することが適当**。**ただし、制度の浸透具合や、諸外国の動向によっては、法令に基づく義務化の検討も必要になり得る**。

✓ 対象製品範囲については、「**間接的又は直接的にインターネットに接続する製品**」とすることが適当。その上で、具体的な対象製品については今後要検討。

✓ 適合性評価基準については、国際的な標準を参照の上、**国際的な標準と整合的な形で構築していくことが適当**。その上で、具体的にいかなる製品にどのような基準を適用するかは今後要検討。

✓ 運用については、**既存の評価スキームを活用**した制度とすることが適当。その上で、具体的にどのようなスキームを活用すべきかは今後要検討。

今後議論が必要な事項

上記に加え、政府の関与や検討体制のあり方、IoT製品ベンダーの能動的な制度活用を促す仕掛け、適合性評価済製品におけるセキュリティ事案への対応。

出所）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