

ERABに関するサイバーセキュリティ

令和2年3月19日

資源エネルギー庁
新エネルギーシステム課

ERABサイバーセキュリティWGの開催実績、ガイドライン策定/改定実績

第1回	2016年8月30日	議事：本WGの意義・位置付け、今後の進め方 など
第2回	2016年10月6日	議事：ERABにおいて想定される脅威・リスク など
第3回	2016年11月29日	議事：ECHONETコンソーシアムでの検討事項 など
第4回	2016年12月20日	議事：PDCAによるセキュリティ対策のあり方 など
第5回	2017年1月17日	議事：サイバーセキュリティガイドライン案 など
第6回	2017年2月13日	議事：サイバーセキュリティガイドライン最終案 など
⇒ 2017年4月26日 ERABサイバーセキュリティガイドラインを策定		
第7回	2017年8月31日	議事：本WGで議論する論点 など
第8回	2017年9月12日	議事：サイバーセキュリティガイドライン Ver1.1（案） など
⇒ 2017年11月29日 ERABサイバーセキュリティガイドラインVer1.1に改定		
第9回	2018年9月11日	議事：簡易指令システムを經由して中央給電システムとコーディネーターのシステムが接続する場合のサイバーセキュリティ対策の検討 など
第10回	2019年3月4日	議事：ガイドライン改定案に関する議論 など
第11回	2019年7月24日	議事：サイバーセキュリティガイドライン改定に向けた進め方
第12回	2019年8月29日	議事：海外有識者によるサイバーセキュリティガイドラインへのレビュー など
第13回	2019年10月1日	議事：サイバーセキュリティガイドライン改定案
第14回	2019年11月22日	議事：サイバーセキュリティガイドライン改定の進め方 など
⇒ 2019年12月27日 ERABサイバーセキュリティガイドラインVer2.0に改定		

今年度のサイバーセキュリティWGの実施内容

- サイバーセキュリティWGでは、海外調査や海外有識者によるレビューの結果をガイドライン改定案として反映し、議論を行ってきた。
- 第14回WGでは、需給調整市場参入に間に合わせるため、更に一部の記載事項を修正した改定原案について議論を行い、その後のパブリックコメントを経て、2019年12月27日に「ERABに関するサイバーセキュリティガイドラインVer.2.0」として公開した。

今年度のスケジュール

		1Q	2Q	3Q	4Q
サイバーセキュリティWG			● 第11回 海外事例と事業者 ヒア結果の共有	● 第12回 海外有識者に よるレビュー	● 第13回 改定案議論
	ガイドライン 改定案の作成		→		
	ガイドラインの 改定手続				● 改定版(Ver2.0)公表
				● 第14回 改定原案議論	● パブリックコメント
ERAB検討会				● ガイドライン改定案の報告	● ガイドライン改定版の報告
市場化に向けた 取組					→ TSOがACに求める セキュリティ規定の策定※ 1 → 詳細対策要件の作成※ 2

※ 1 簡易指令システムとアグリゲーターシステムとの接続に関して、TSOがACに求めるセキュリティ要件のこと。

※ 2 ERABに参画する事業者は、ガイドラインを基に具体的な対策事項を定めた詳細対策要件を作成することが求められる。

第14回WGにおける修正事項

- ERABサイバーセキュリティガイドラインでは、アグリゲーションコーディネーターとその保有するシステムに対して、送配電事業者が、「電力制御システムセキュリティガイドライン」と「本ガイドライン」に基づき別途要件を定義したセキュリティ対策に準拠したサービスレベルを要求している。
- Ver.1.2では、「有事の際の対応計画に基づいた訓練の継続的实施」について、両ガイドラインの整合性が取れていなかったため、当該事項を【推奨】から【勧告】に修正し、ガイドライン改定原案とした。

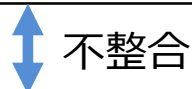
Ver.1.2での規定

○ERABサイバーセキュリティガイドライン

4.1.4各事業者における監視・対応体制等

【推奨】

・有事の際の対応計画に基づいた訓練を継続的に実施すること。



不整合

○電力制御システムセキュリティガイドライン

第7-4条 周知と訓練

【勧告】

・セキュリティ事故発生時の対応に関する周知や訓練を定期的に行うこと。

改定原案での規定

○ERABサイバーセキュリティガイドライン

4.1.4各事業者における監視・対応体制等

【勧告】

・有事の際の対応計画に基づいた訓練を継続的に実施すること。

公表された改定版（Ver.2.0）の主な改定事項

- 改定原案での修正事項、及び第13回WGまでの議論事項を反映したものをVer.2.0の原案とし、それに対して2019年11月27日～2019年12月26日の期間でパブリックコメントを実施した。

ガイドラインVer2.0での主な改定事項

1. サイバー・フィジカル・システムの相互運用性の確保（1）

ERABシステムは、情報の保護だけでなく、物理的に電力システムが動作し続けるためのレジリエンスを確保するため、サプライチェーン全体におけるセキュリティ対策を策定する旨を追記。

2. 事故発生時の対応（3.6, 3.8, 4.1.4）

ERAB事業者に対して、事故発生時の被害を考慮し、当該被害を最小限にとどめるための対応及び体制を構築する旨を記載。

3. 勧告項目の実装の実現性の検証（3.6, 4.1, 4.1.3）

ERAB事業者に対して、第三者による監査や教育プログラム等により勧告項目の実装を検証する旨を追記。

4. ERAB事業者の間における連携体制の構築（3.2, 4.1, 4.1.4）

ERAB事業者に対して、セキュリティ管理責任者を任命し、当該者間で情報共有できる体制を構築する旨、また責任分界点を明確化する旨を追記。

サイバーセキュリティWGの今後の検討事項（案）

- 各ERAB事業者は、標準対策要件であるERABセキュリティガイドラインの項目を踏まえた上で、実運用に耐える詳細対策要件を策定することが求められる。
- ERAB事業者が詳細対策要件を設計するに当たり、ガイドラインへの理解を深める参考となる補足資料を取りまとめることを検討する。
- また、ERAB事業者は、適切なセキュリティ対策が行えるよう、セキュリティ教育・訓練を計画し実施することが求められており、ガイドラインの勧告項目の実装に役立つユースケース等の整理を行う。

今後のスケジュール（案）

	1Q	2Q	3Q	4Q
ERABサイバーセキュリティガイドラインに関する補足資料の取りまとめ		補足資料の取りまとめに向けた検討 → ● 補足資料の取りまとめ		
ユースケース等の整理		ユースケース等の検討 → ● ユースケース等の策定		ユースケース等の検証

參考資料

ERABサイバーセキュリティガイドラインとは

- 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に参画する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年初版を策定し、2019年12月27日に改正版（ver2.0）を公表した。
- 2021年4月に開設する需給調整市場に参入する事業者は、市場運営者が定める規程等に基づき**本ガイドラインの準拠**が求められる予定。

＜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

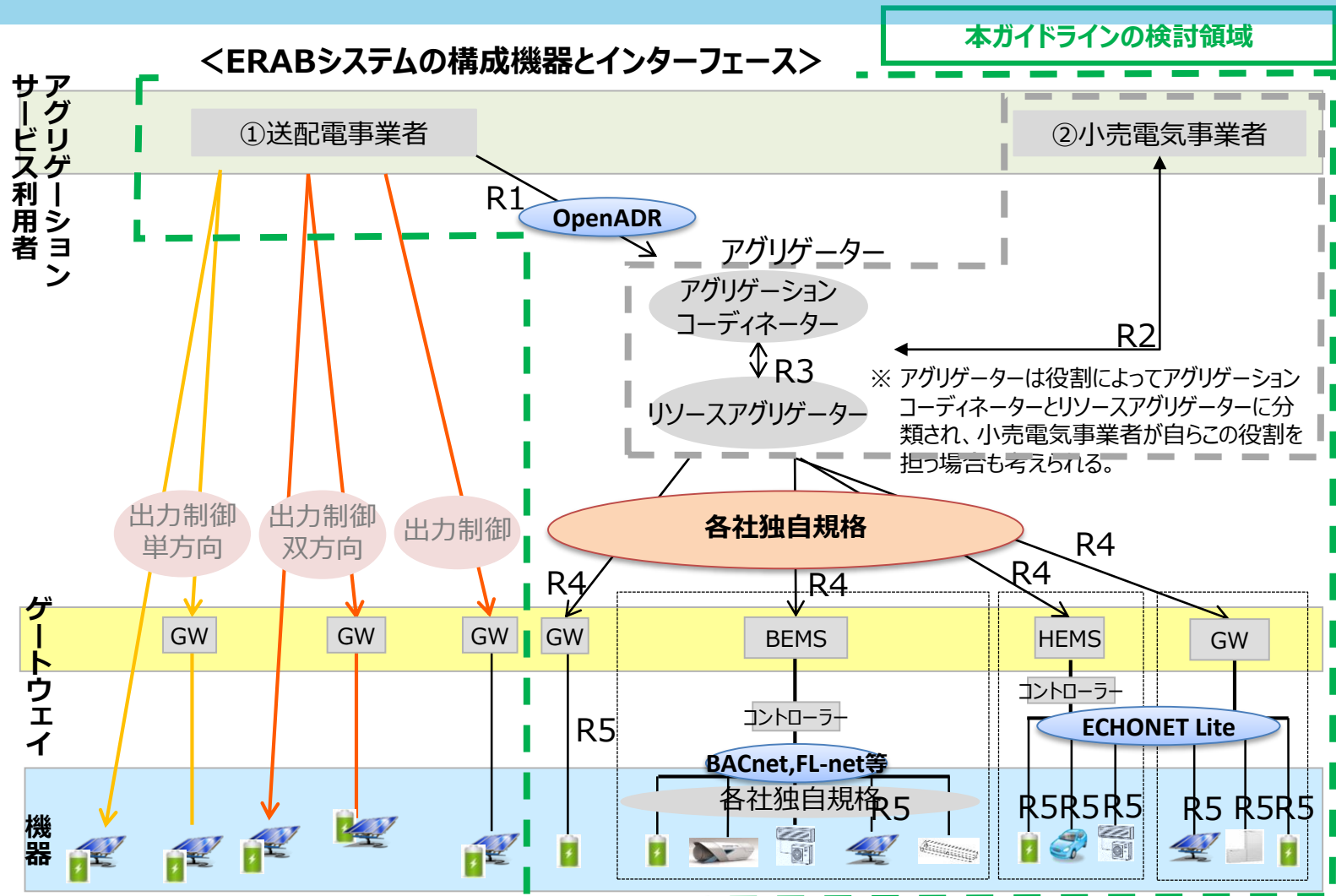
3.9. ガイドラインの継続的改善

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

ガイドラインの対象となるERABシステム(3.1.関係)

- ガイドラインの対象は、送配電事業者、小売電気事業者、アグリゲーションコーディネーター、リソースアグリゲーターにおける各システム※、エネルギーマネジメントシステム、エネルギー機器のゲートウェイ（GW）、制御対象のエネルギー機器である（ERABシステムという）。
※送配電事業者についてはアグリゲーター等に対して制御指令を出す簡易指令システムを指す



本ガイドラインの位置づけと基本方針(3.2.関係)

● ガイドラインの位置づけ

- **最低限のサイバーセキュリティ対策の要求事項**であり、ERAB事業者は本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**。
- 本ガイドラインの記載事項は、事業者が**実装を義務づけられる【勧告】**と**実装を検討すべき内容である【推奨】**に分かれる。

● 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。
- 【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。

ERABシステムにおけるサイバーセキュリティ対策(3.6.関係)

- **ERAB事業者に対して、以下の手順によるサイバーセキュリティ対策を義務づけ**
 - Step 1 対象とするIoT製品やサービスのシステムの全体構成及び責任分界点を明確化
 - Step 2 システムにおいて、保護すべき情報・機能・資産を明確化
 - Step 3 保護すべき情報・機能・資産に対して、想定される脅威を明確化
 - Step 4 脅威に対抗する対策の候補（ベストプラクティス）を明確化
 - Step 5 どの対策を実装するか、脅威レベルや被害レベル、コスト等を考慮して選定
 - Step 6 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
 - Step 7 事故発生時の対応方法を設計・運用及び訓練を実施
- **その他に、勧告事項の準拠が確認できない際の相互接続の中止、なりすまし対策、データ等の改ざん対策、マルウェアへの対策を義務づけている。**

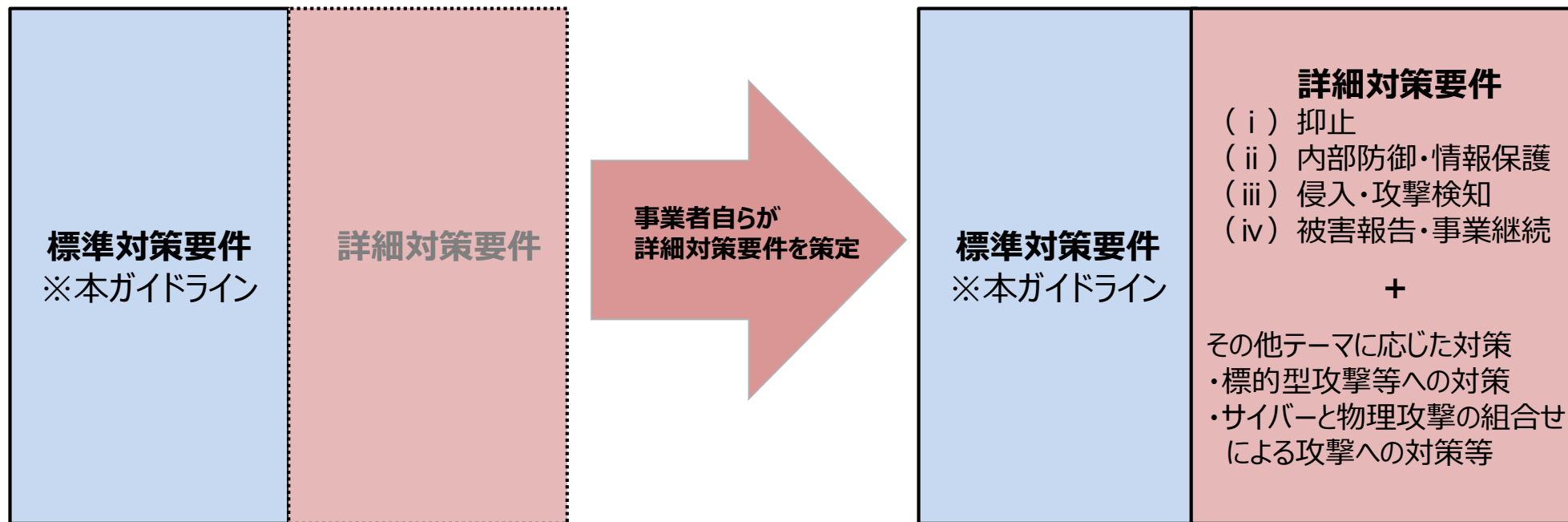
システム間の各インターフェースにおけるサイバーセキュリティ対策(3.6.関係)

- 各システム間のインターフェースに共通する対策として、**外部システムとの相互接続点における認証、通信メッセージの暗号化**を求めている。更に、以下のインターフェース別に対策を求めている。

- ① **アグリゲーションコーディネーターのシステム及びR1（簡易指令システムとアグリゲーションコーディネーター間のインターフェース）**
 - 簡易指令システムとの直接的な接続部は、送配電事業者が別途定めるセキュリティ要求事項に準拠すること。
- ② **R2（小売電気事業者とアグリゲーションコーディネーターまたはリソースアグリゲーター間のインターフェース）**
 - 小売電気事業者のシステムと接続する場合には、小売電気事業者に対して本ガイドラインへの準拠を求めること。
- ③ **リソースアグリゲーターのシステム及びR3（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間のインターフェース）**
 - 本ガイドラインへの準拠に加え、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。
- 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）**
 - 本ガイドラインへの準拠に加え、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。
- 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のインターフェース）**
 - 推奨事項として、「IoT開発におけるセキュリティ設計の手引き」等の参照した対策を取ること。

本ガイドラインに基づく詳細対策要件の設計（3.8.関係）

- ERAB事業者に対して、**実運用に耐え得る具体的なサイバーセキュリティ対策（詳細対策要件）**を事業者自らの責任で策定することを求めている。
- 詳細対策要件の設計においては、本ガイドラインに加え、情報処理推進機構の「IoT開発におけるセキュリティ設計の手引き」や日本電気技術規格委員会が制定する「電力制御システムセキュリティガイドライン」を前提とする。



事業者における継続的なセキュリティ対策の在り方(4.関係)

- ERAB事業者に対して、**PDCAサイクル**（①セキュリティ対策の設定、②セキュリティ対策の実施、③セキュリティ対策の評価、④適切な改善策の設定・実施）による検証・改善を行い、**自主的にかつ継続的にセキュリティ対策を実施すること**を求めている。
- そのため、事業者は、**セキュリティ管理責任者の任命**など、適切な運用・管理体制を構築することが求められる。

【参考】サイバーセキュリティWGの概要

開催日程

第14回

2019年11月22日（金）

概要

- サイバーセキュリティガイドラインの一部修正
- ガイドライン改定スケジュールの検討
- 他の審議会での議論との関係性の整理

出席者

【出席者】（50音順、敬称略）

座長

梅嶋 真樹 慶應義塾大学 SFC研究所 AUTO-IDラボ・ジャパン 副所長

学識経験者

石井 英雄 早稲田大学 スマート社会技術融合研究機構 研究院教授
加藤 雅彦 長崎県立大学 情報システム学部 情報セキュリティ学科 教授
小林 和真 独立行政法人情報処理推進機構（IPA）専門委員
田居 久生 独立行政法人情報処理推進機構（IPA）セキュリティセンター
企画部 副部長
永宮 直史 特定非営利活動法人日本セキュリティ監査協会（JASA）
事務局長

事業者

片山 朋宏 大阪ガス株式会社 ガス製造・発電・エンジニアリング事業部
エンジニアリング部ICTソリューションチーム
沓掛 政志 東京電力パワーグリッド株式会社 系統運用部
系統制御グループ マネージャー
小林 将大 エネルエックス・ジャパン株式会社 渉外部 シニアマネージャー

関係機関

青木 一彦 電気事業連合会 情報通信部 副部長
内田 明生 ディアモンドリスpons推進協議会 理事長
山本 敏之 電力広域的運営推進機関 企画部 マネージャー

実証事業者

上田 智之 関西電力株式会社 地域エネルギー本部
地域エネルギー技術グループ 部長
宇佐美 重之 中部電力株式会社 販売カンパニー 総務部 システムグループ長
小林 輝夫 株式会社エナリス エナリスみらい研究所 ディレクター
柴本 真吾 東京電力ホールディングス株式会社 経営技術戦略研究所
リソースアグリゲーション推進室 課長
浜口 智洋 東北電力株式会社 企画部 デジタルイノベーション推進室 課長
樋口 智治 株式会社ローソン 開発本部 建設部 シニアマネージャー
福本 淳二 アズビル株式会社 ビルシステムカンパニー マーケティング本部
環境マーケティング部環境制御グループ マネージャー
宮原 泰徳 KDDI 株式会社 ライフデザイン事業本部 エネルギービジネス本部
エネルギービジネス企画部 担当部長
見山 雅英 九州電力株式会社 テクニカルソリューション統括本部 総合研究所
系統高度化グループ長
矢野 雄一 SB エナジー株式会社 戦略事業本部 IoT 事業部 マネージャー
淀瀬 健司 豊田通商株式会社 再生・新規電力事業部 新規事業グループ 課長補

【経済産業省】

省エネルギー・新エネルギー部 新エネルギーシステム課
電力・ガス事業部 電力基盤整備課
商務情報政策局 情報産業課
商務情報政策局 サイバーセキュリティ課