経済産業省

資料４－１

第13回ERAB検討会

ERABサイバーセキュリティガイドラインの対策例等の策定

令和2年10月21日
資源エネルギー庁
省エネルギー・新エネルギー部
新エネルギーシステム課

本日ご議論いただきたい事項

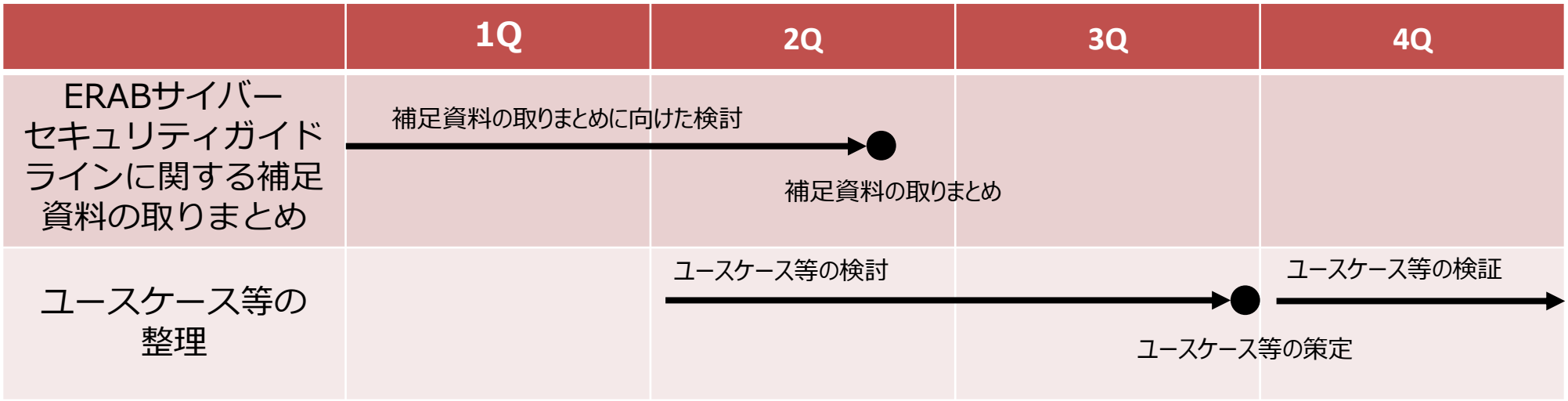
- 本年3月のERAB検討会において、今年度は、詳細対策要件の設計に参考となるERABサイバーセキュリティガイドラインの補足資料および勧告項目の実装に役立つユースケース等の整理を行うこととされた。
- これまで事業者からいただいた意見および重要インフラに求められているリスクアセスメントの結果を踏まえ、補足資料として、**ERABサイバーセキュリティガイドラインの対策例を整理**した。
- また、事業者が適切にサイバーセキュリティ対策の実施が可能となるため、**IPAが、ERABシステムにおける三層構造の標準ユースケース及びユースケースに基づくリスク分析の更新とサイバーセキュリティに関するトレーニングプログラムを開発**することとなった。
- 本日は、**対策例、トレーニングプログラムの開発、今後の進め方**について、ご議論いただきたい。

出所）2020年3月19日、第11回エネルギー・リソース・アグリゲーション・ビジネス検討会　資料6を基に一部編集

【参考】2020年度サイバーセキュリティWGの検討事項

- 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、実運用に耐えう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。

2020年度のスケジュール



背景

- 2019年12月に、パブリックコメントの実施を経て、ERABサイバーセキュリティガイドライン Ver2.0を公表した。
- 今後、**ERAB事業者は、**標準対策要件であるERABサイバー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うる**詳細対策要件を策定**することが求められる。他方、昨年度のサイバーセキュリティWGにおける議論やパブリックコメントでは、事業者によりガイドラインの理解が異なることから、詳細対策要件にて定める対策も事業者によって異なる可能性があるとの懸念や、具体例の提示の要望等が示された。
- そのため、今年度、ERAB事業者が詳細対策要件を設計するに当たり、参考となる**ガイドラインの勧告事項・推奨事項に対する対策例を取りまとめる**こととした。
- また、ユースケース等の開発については、**ERABサイバーセキュリティガイドラインを資源エネルギー庁と共管で策定しているIPAがトレーニングプログラムの開発**することとなったため、その開発の中で実施することとした。

【参考】ERABサイバーセキュリティガイドラインに対するパブリックコメントの意見概要 (1)

ERABガイドラインの節番号	パブリックコメントでの意見（抜粋・一部表現修正）
3.2. ERAB システムが留意すべき基本方針	• 「ERABに参画する各事業者」の定義を明確化すべきではないか。 • 脆弱性の情報共有は重要だが、脆弱性の通知は勧告事項でなくても良いのではないか。 • データだけでなく、プログラムやソフトウェアの機密性、完全性、可用性も重要ではないか。 • 機密性、完全性、可用性に加え、否認防止にも留意したシステム設計が必要ではないか。
3.3. ERAB システムが想定すべき脅威	• 閉域網でのセキュリティ脅威を具体的に記載スベきではないか。 • 正規ルートで持ち込まれた機器にあらかじめ脅威が仕込まれていた場合のインシデント対応を含めるべきではないか。
3.4. ERAB システムが維持すべきサービスレベル	• 送配電事業者の簡易指令システムに対して直接接続がなされるのはACのみであるため、誤解の無いよう表現を修正すべきではないか。
3.5. ERAB システムにおけるシステム重要度の分類	• 分類の基準となる「需要規模50万kW」の考え方や根拠等について、補足説明が必要ではないか。
3.6. ERAB システムにおけるサイバーセキュリティ対策	• Step2、Step3の具体例があれば記載していただきたい。 • Step5では被害レベルの過小見積・申告も含まれるのではないか。 • Step6における監査の主体者、監査対象を具体化すべきではないか。 • Step6における第三者による監査（認証を含む）が勧告事項・推奨事項どちらに当たるのか不明である。 • Step6の「教育プログラム等」について、一定の基準を満たしたうえでの自己監査を包含するものと解釈できるのか。 • 相互接続の中止について、各事業者が接続相手が正しく対策を実装しているかを確認することは困難であると考える。専門の第三者機関による認証や何らかの認証を取得した事業者のシステムが接続できる等、各事業者にセキュリティの専門家がいない場合でも対策の確認ができるようにすべきではないか。 • 機器設計・生産時からの対策については、設計時や生産時ハードウエアやソフトウェアに脅威が紛れ込まないような対策を考慮すべきではないか。 • 認証と通信暗号化について、両者の関係を明示すべきではないか。 • 「外部システムとの相互接続点」がどれを指すか不明であり、明示すべきではないか。 • 「通信の暗号化」にMACアドレス等の改ざん検知も含んでいるのであれば明示すべきではないか。 • 「不特定多数がアクセスできるネットワーク」について、具体的に明示すべきではないか。 • 「接続点の防御措置」とは相互認証と通信の暗号化及びMACアドレス検証を指しているのか。それ以外のフィルタや検知なども含むのであれば、具体的に明示すべきではないか。

【参考】ERABサイバーセキュリティガイドラインに対するパブリックコメントの意見概要 (2)

ERABガイドラインの節番号	パブリックコメントでの意見（抜粋・一部表現修正）
3.7. 取扱情報の差異による ERAB システムの設計	• 家庭に設置するHEMS機器やコントローラなど末端に設置する機器について、個人情報を取り扱うシステムに該当するか否かを明記すべきではないか。
3.8. 標準対策要件に基づく詳細対策要件の設計	• 「構成要素毎に実施すべき対策」や「ERAB システムに関係する特定のテーマに応じた対策」が何を指すのか不明確であるため、明示すべきではないか。
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	• セキュリティ管理責任者をどのような組織単位で置くのかを明確化すべきではないか。 • 「当該管理者間で情報共有」について、この当該管理者間は事業者内での情報共有を指すのか。もしくは、事業者間を指すのか。 • 対策として設置すべき組織、人（責任者）、組織間の関係が分かりづらく、明確化すべきではないか。 • セキュリティ対策の検証・改善の頻度はどの程度が適切なのか。 • 第三者認証の実施が強く推奨とあるが、実施主体、実施方法、強制力等が不明確であるため、解釈集等で具体的に定義すべきではないか。 • 第4.1.4.項の「脆弱性関連情報」は公開された脆弱性であるのか。各事業者が個別に脆弱性を知った場合、公開前に関係者間で共有し、対策し、その後、脆弱性の公開が望ましいと考えられるが、その内容は含まれるのか。

【参考】広域機関 需給調整市場(三次調整力②)に関するパブリックコメントの意見概要

- 電力広域的運営推進機関は、2021年度の需給調整市場開設・市場運営等に係る詳細検討のために、「需給調整市場検討小委員会」において整理した三次調整力②に関する事項について、パブリックコメント※を実施した。
- パブリックコメントにおける意見のうち、ERAB事業者のサイバーセキュリティに関する意見は以下のとおりであった。

※ 2019年4月26日～2019年5月17日の期間で実施

広域機関パブリックコメントでのサイバーセキュリティ関連の意見（一部表現修正）
ERABセキュリティガイドラインVer1.2には、ACが簡易指令システムへの接続の際、「簡易指令システムを運用するTSOが別途定める相互接続に関するセキュリティ要求事項に準拠すること」と記載されており、その内容はいつ提示されるのか。
事前審査において、セキュリティの審査も行うのであれば、そのスケジュールも示しておく必要があるのではないか。
サイバーセキュリティの審査は、NIST7628に示される具体的なセキュリティ対策などの推奨事例、要件を示すべきではないか。
ACとRAのセキュリティレベルを同一ではなく、差異を設けるべきではないか。

対策例の整理やトレーニングプログラムの開発に向けた進め方

＜対策例の整理＞

- 対策例の開発を行うにあたり、各ERAB事業者におけるセキュリティリスクの確認のために、**ERABシステムにおけるリスク分析を実施することが重要**となる。これは、ガイドライン3.6項のStep3や４に規定されている。他方、ERABシステムは、2016年度より実証事業等を通じて構築されてきており、また並行して各種電力市場の要件が検討されてきたことから、**これまでERABシステムの包括的なリスク分析は実施されていない**。
- このため、経済産業省「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）」を参照の上、ERABシステムにおける三層構造の標準ユースケースに基づく**リスク分析を実施**した。それを踏まえて、リスク分析にて抽出された**リスク影響度を評価**することとした。
- **CPSFには、リスクに対する対策例を明記**しており、それらがERABサイバーセキュリティガイドラインの**勧告事項、推奨事項との対応表を整理**した（スライド12～23を参照）。

＜トレーニングプログラムの開発＞

- ガイドライン3.6項において、事業者は適切なサイバーセキュリティ対策が行えるよう、Step1～Step７のプロセスに基づき、**アセスメント結果を実施の上、各事業者の有する事業及びシステム特性を考慮したセキュリティ設計、教育プログラム等を計画し実施**することが求められている。
- ERABは緒に就いたばかりの事業であり、各事業者が独自にセキュリティ教育・訓練を実施することは困難であると考えられることから、**IPAと連携して、ERABの取引の実態に則したユースケースを整理の上、ERAB事業者向けのサイバーセキュリティトレーニングプログラムを開発**することとした。上記、**対策例の対応表は、研修にて使用**することとした。

【参考】ERABサイバーセキュリティガイドライン3.6項

- ERABサイバーセキュリティガイドラインは、Step1～Step 7 のプロセスに基づく基づく各事業者の有する事業及びシステム特性を考慮したセキュリティ設計を勧告として求めている

3.6. ERABシステムにおけるサイバーセキュリティ対策 【勧告】ERABに参画する各事業者は、ERABシステムでは、以下の手順を踏むこと	
Step1	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すること
Step2	システムにおいて、保護すべき情報・機能・資産を明確化すること
Step3	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すること
Step4	脅威に対抗する対策の候補（ベストプラクティス）を明確化すること
Step5	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すること
Step6	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
Step7	事故発生時の対応方法を設計・運用及び訓練すること

リスク分析の概要

- リスクアセスメントの実施は重要インフラに求められている。経済産業省の「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）」に基づき、ERABシステムを三層構造に分解（次頁参照）の上、**事業被害と発生頻度の両面から影響が大きいリスクを抽出**した。

CPSFの概要：CPSFにおける三層構造・6つの構成要素の概要

＜三層構造と６つの構成要素＞
サイバー・フィジカル一体型社会のセキュリティのためにCPSFで提示した新たなモデル

- CPSFでは、産業・社会の変化に伴うサイバー攻撃の脅威の増大に対し、リスク源を適切に捉え、検討すべきセキュリティ対策を漏れなく提示するための新たなモデル（**三層構造**と**６つの構成要素**）を提示。

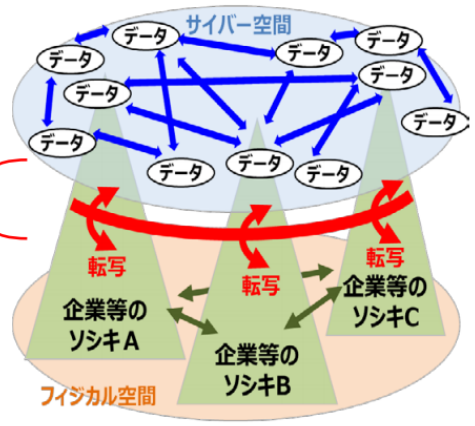
三層構造

「Society5.0」における**産業社会を３つの層に整理**し、セキュリティ確保のための信頼性の基点を明確化

サイバー空間におけるつながり
【第３層】
自由に流通し、加工・創造されるサービスを創造するための**データの信頼性**を確保

フィジカル空間とサイバー空間のつながり
【第２層】
フィジカル・サイバー間を正確に**“転写”する機能の信頼性**を確保
（現実をデータに転換するセンサーや電子信号を物理運動に転換するコントローラ等の信頼）

企業間のつながり
【第１層】
適切な**マネジメントを基盤に各主体の信頼性**を確保



６つの構成要素

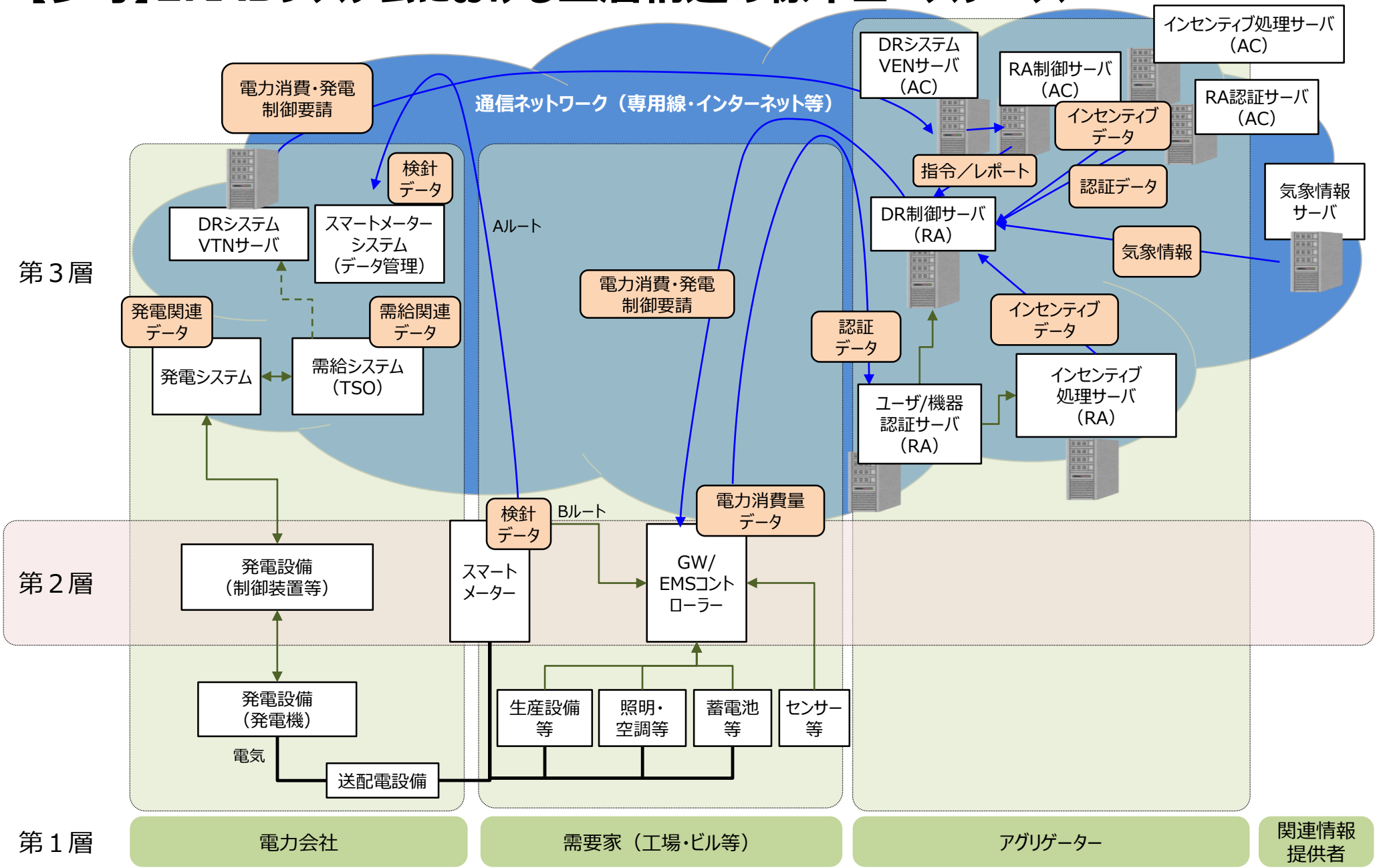
対策を講じるための単位として、**サプライチェーンを構成する要素を６つに整理**

構成要素	定義
ソシキ	• バリュークリエイションプロセスに参加する企業・団体・組織
ヒト	• ソシキに属する人、及びバリュークリエイションプロセスに直接参加する人
モノ	• ハードウェア、ソフトウェア及びそれらの部品 操作する機器を含む
データ	• フィジカル空間にて収集された情報及び共有・分析・シミュレーションを通じて加工された情報
プロシージャ	• 定義された目的を達成するための一連の活動の手続き
システム	• 目的を実現するためにモノで構成される仕組み・インフラ

2

経済産業省「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）のポイント」より

【参考】ERABシステムにおける三層構造の標準ユースケース



リスク分析の結果概要

- 「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）」に記載されるリスク分析プロセスに基づき、**ERABシステムの標準ユースケースを３層構造で整理**した。その上で、各層の機能に想定されるセキュリティインシデントに対し、**リスクの発生頻度と被害規模の観点からリスク影響度の評価（リスク分析）を実施**した。
- リスク分析の結果において影響が大きいと判断されたリスクへの対策に関しては、事業者が**CPSFに収録される対策要件と対策例をベストプラクティスとして参照し、詳細対策要件として設計・実施できるように整理した**（「【資料４－２】対策要件に応じたセキュリティ対策例」を参照）
- **ERABサイバーセキュリティガイドラインの勧告事項・推奨事項のCPSFに収録される対策要件・対策例との対応付け**を実施した（スライド12～23を参照）。これにより、**リスクの存在する層と推奨される対策の例を容易に参照**できるよう整理した。

ERABセキュリティガイドラインとCPSFの対応表【案】(1)

- ERABサイバーセキュリティガイドラインの**勧告事項、推奨事項に対応するCPSFの対策要件との対応関係は以下のとおり**。
- ERAB事業者においては、自社のシステム構成や対策を導入・運用する際、CPSFが定める対策要件IDに紐づく**対策例をベストプラクティスとして参照**（ガイドライン3.6項のstep4（ベストプラクティスの特定）し、**対策を講じる**（step5（対策の選定））ことが望まれる。

節・項番号	ERABサイバーセキュリティガイドラインにおける対策要件	CPSFにおける主な対策要件ID
3.2. ERAB システムが留意すべき基本方針	《勧告》ERAB に参画する各事業者は、脆弱性対策情報の利用者への通知を行うこと。	CPS.AE-4 CPS.RP-2 CPS.CO-1
	《勧告》ERAB に参画する各事業者は、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。	CPS.AE-4 CPS.RP-2
	《推奨》ERAB システムは、そのシステムが取り扱うハードウェアとそのハードウェア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。	CPS.GV-3

ERABセキュリティガイドラインとCPSFの対応表【案】(2)

節・項番号	ERABサイバーセキュリティガイドラインにおける対策要件	CPSFにおける主な対策要件ID
3.3. ERAB システムが想定すべき脅威	《推奨》ERAB システムは、以下の観点を前提として対策の検討を進めること。 ・ERABシステムは、以下の観点を前提として対策の検討を進めること。 ・標的型攻撃を想定すること。 ・インシデント検知のためにシステムのログを取得すること。 ・閉域網だから安全であるという考えに立脚しないこと。 ・セキュリティ対策については、安全な状態が完全に達成されることはなく、継続的に対策を改善すること。	CPS.AM-1 CPS.IP-1 CPS.CM-1, 3, 6 CPS.DS-9, 10 CPS.DP-1, 3 , 4
	《推奨》インターフェース R5 の機器としては、エネルギー機器に加えてセンサが想定される。（中略） その脅威に対応するため、ERABシステムのセキュリティはIoTシステムとしてのセキュリティを求められる。 ・攻撃者がネットワークを介してGWを超えて、BEMS・HEMSコントローラ、エンドポイントに位置する機器やセンサに不正データを送信し、誤作動、機能を停止、データ取得を不可能にさせる。 ・エンドポイントに位置するエネルギー機器やセンサの内部データ改ざんや盗難が発生する。 ・エネルギー機器やセンサの不正改造により、誤作動、機能を停止させる。 ・乗っ取ったセンサやエネルギー機器からERABシステムを構成するサーバーへのデータ送信により処理負荷を増加させ、その結果としてERABサービス全体を停止させる。 ・攻撃者がエネルギー機器やセンサを乗っ取り、GW経由の外部システムへのDoS攻撃へ加担させる。 ・設備の破壊や停止の結果として、ERABサービスの停止、人命に関わる動作が誘発される。	CPS.AM-1, 6 CPS.GV-3 CPS.IP-1, 5, 6 CPS.SC-2, 3, 4, 6, 7, 8 CPS.AC-1, 2, 3 CPS.DS-9 CPS.CM-1, 2, 6 CPS.DS-13, 15
3.4. ERAB システムが維持すべきサービスレベル	《勧告》ERAB システムにおいては、送配電事業者の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が保有するシステムは、相互接続が行われる。サイバー攻撃等の影響が系統ネットワークに拡散するリスク管理に留意すること。（以下略）	CPS.DS-9 CPS.SC-3

ERABセキュリティガイドラインとCPSFの対応表【案】(3)

節・項番号	ERABサイバーセキュリティガイドラインにおける対策要件	CPSFにおける主な対策要件ID
3.5. ERAB システムにおけるシステム重要度の分類	《勧告》本ガイドラインにおいて、システム重要度の定義は、電力制御システムセキュリティガイドラインに基づき、以下に定めるところによる。 「重要度A」とは、電力の安定供給等に与える影響が比較的大きいと考えられるシステムをいう。 「重要度B」とは、電力の安定供給等に与える影響が限定的なシステムをいう。	–
3.6. ERAB システムにおけるサイバーセキュリティ対策	《勧告》ERAB に参画する各事業者は、ERAB システムでは、以下の手順を踏むこと。 Step1：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すること。	CPS.AM-1, 5 CPS.SC-1 CPS.SC-4 CPS.RM-2 CPS.DS-13
	Step2：システムにおいて、保護すべき情報・機能・資産を明確化すること。	CPS.AM-1, 5 CPS.RA-5 CPS.RM-2
	Step3：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すること。	CPS.RA-5, 6 CPS.RM-2
	Step4：脅威に対抗する対策の候補（ベストプラクティス）を明確化すること。	CPS.RA-5, 6 CPS.RM-2
	Step5：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すること。	CPS.RA-6 CPS.RM-2
	Step6：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。	CPS.AT-1, 2, 3 CPS.SC-6
	Step7：事故発生時の対応方法を設計・運用及び訓練すること。	CPS.RP-１, 2, 3 CPS.CO-１, 2, 3

ERABセキュリティガイドラインとCPSFの対応表【案】(4)

節・項番号	ERABサイバーセキュリティガイドラインにおける対策要件	CPSFにおける主な対策要件ID
3.6. ERAB システムにおけるサイバーセキュリティ対策	《勧告》ERAB に参画する各事業者は、相互接続相手に本ガイドラインの勧告内容の実装が確認できない場合には、ERAB システム全体のセキュリティ被害を最小化することを目的として、該当するシステム間での相互接続を速やかに中止すること。【相互接続の中止】	CPS.DS-9 CPS.SC-3
	《勧告》悪意を持った攻撃者によってなりすましが行われ、意図しない指令が発令されることにより、需要家側のエネルギー機器が不正に制御される脅威・リスクや、制御不能となる脅威・リスクを想定し、対策を取ること。【なりすまし対策】	CPS.AC-1, 3, 4, 8 CPS.AC-9
	《勧告》通信機器や通信路が、悪意を持った攻撃者によって盗聴・中間者攻撃され、情報が改ざんされることにより、需要家側のエネルギー機器が不正に制御される脅威・リスクを想定し、対策を取ること。【データ等の改ざん対策】	CPS.CM-3,4 CPS.SC-4 CPS.DS-15
	《勧告》システムには脆弱性に対処するセキュリティパッチを適用するとともに、システムを構成する機器や外部記憶媒体等へのマルウェア対策を行うこと。（中略）システムを構成する機器や外部記憶媒体、取り扱うデータを把握し、適切に管理及び保護すること。【マルウェアへの対策】	CPS.AM-1 CPS.IP-1,2 CPS.DS-9 CPS.CM-6

ERABセキュリティガイドラインとCPSFの対応表【案】(5)

節・項番号	ERABサイバーセキュリティガイドラインにおける対策要件	CPSFにおける主な対策要件ID
3.6.1. アグリゲーションコーディネーターのシステム及び R1	（事業者とその保有するシステムの対策） 《勧告》アグリゲーションコーディネーターは、送配電事業者との間で調整力契約を締結するにあたり、自身に加え、リソースアグリゲーターのセキュリティを含むサービス品質を確保し、送配電事業者に対して責任を持つこと。	CPS.SC-3, 7, 8
	《勧告》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、「電力制御システムセキュリティガイドライン」、「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」に基づき簡易指令システムを運用する送配電事業者が別途定める相互接続に関するセキュリティ要求事項に、準拠すること。	CPS.GV-2, 3
	（インターフェースの対策） 《勧告》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。	CPS.AC-3, 4, 6, 9 CPS.DS-2, 3, 4, 5
	《勧告》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。	CPS.DS-9
	《勧告》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。	CPS.DS-9
3.6.2. R2	（インターフェースの対策） 《勧告》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。	CPS.AC-3, 4, 6, 9 CPS.DS-2, 3, 4, 5
	《勧告》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が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、小売電気事業者の保有するシステムを本ガイドラインに準拠することを求めること。また、当該事業者に対して、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を構築しそれに準拠することを求めること。	CPS.DP-2 CPS.AT-1 CPS.GV-2
3.6.3. リソースアグリゲーターのシステム及び R3	（事業者とその保有するシステムの対策） 《勧告》リソースアグリゲーターとその保有するシステムは、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。	CPS.GV-2, 3
	（インターフェースの対策） 《勧告》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。	CPS.AC-3, 4, 6, 9 CPS.DS-2, 3, 4, 5

ERABセキュリティガイドラインとCPSFの対応表【案】(6)

節・項番号	ERABサイバーセキュリティガイドラインにおける対策要件	CPSFにおける主な対策要件ID
3.6.4. R4	（事業者とその保有するシステムの対策） 《勧告》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。	CPS.GV-2,3
	（インターフェースの対策） 《勧告》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。	CPS.AC-3, 4, 6, 9 CPS.DS-2, 3, 4, 5
3.6.5. R5	【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」、「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。	CPS.AM-1, 6 CPS.GV-3 CPS.IP-1, 5, 6 CPS.SC-2, 3, 4, 6, 7, 8 CPS.AC-1, 2, 3 CPS.DS-9 CPS.CM-1, 2, 6 CPS.DS-13, 15
	（インターフェースの対策） 《推奨》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。	CPS.AC-3, 4, 6, 9 CPS.DS-2, 3, 4, 5
3.7. 取扱情報の差異による ERABシステムの設計	《勧告》ERAB に参画する各事業者は、取扱情報の差異を明確化し、その結果に見合ったシステムを設計すること。（以下略）	CPS.IP-3

ERABセキュリティガイドラインとCPSFの対応表【案】(7)

節・項番号	ERABサイバーセキュリティガイドラインにおける対策要件	CPSFにおける主な対策要件ID
3.7.1. センサデータを活用した IoT サービスに近似したサービスを設計する事業者	《勧告》IoT システムについて、範囲、対象を含めた定義を改めて明確にするとともに、IoT システムが多岐にわたることから、リスクを踏まえたシステムの特性に基づく分類を行い、その結果に応じた対応を明確化すること。	CPS.AM-1, 6 CPS.GV-3 CPS.IP-1, 5, 6 CPS.SC-2, 3, 4, 6, 7, 8 CPS.AC-1, 2, 3 CPS.DS-9 CPS.CM-1, 2, 6 CPS.DS-13, 15
	《勧告》IoT システムに係る情報の機密性、完全性及び可用性の確保並びにモノの動作に係る利用者等に対する安全確保に必要な要件を明確化すること。	
	《勧告》機能保証の制定を含め、確実な動作の確保、障害発生時の迅速なサービス回復に必要な要件を明確化すること。	
	《勧告》その上で、接続されるモノ及び使用するネットワークに求められる安全確保水準(法令要求、慣習要求)を明確化すること。	
	《勧告》接続されるモノ及びネットワークの故障、サイバー攻撃等が発生しても機密性、完全性、可用性、安全性の各項目が確保されるとともに、障害発生時の迅速なサービス復旧を行うことを明確化すること。	
	《勧告》IoT システムに関する責任分界点、情報の所有権に関する議論を含めたデータの取扱いの在り方を明確化すること。	
3.7.2. 個人情報を活用したサービス構築を設計する事業者	《勧告》保有するデータを盗聴・改ざんされるという脅威・リスクへの対策に加え、そのシステムが個人情報を扱う場合には、個人情報保護法に準拠した対策を取ること。	CPS.AM-6 CPS.GV-2, 3
	《勧告》ERAB に参画する各事業者が保有する情報のうち、個人情報については、個人情報保護法において、事業者に対して、個人データの安全管理措置義務を課すことにより、個人情報の適切な管理に関するサービスレベルの維持を義務付けている。（以下略）	CPS.AM-6 CPS.GV-2, 3

ERABセキュリティガイドラインとCPSFの対応表【案】(8)

節・項番号	ERABサイバーセキュリティガイドラインにおける対策要件	CPSFにおける主な対策要件ID
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。（以下略）	CPS.AC-1, 2 CPS.AT-1 CPS.AE-1, 4, 5 CPS.AM-4, 5, 6, 7 CPS.BE-2, 3 CPS.CM-2 CPS.DS-1, 7 CPS.GV-1, 2, 4 CPS.IP-1, 3, 7, 9, 10 CPS.IM-1, 2 CPS.MI-1 CPS.RA-1, 3 CPS.RP-1, 2, 4 CPS.RM-1 CPS.SC-1, 3, 5, 6, 9, 10, 11
3.9. ガイドラインの継続的改善	《勧告》ERAB に参画する各事業者は、詳細対策要件について、定期的にその内容を点検・更新すること。	CPS.AM-6 CPS.BE-2 CPS.SC-1, 2 CPS.IP-3
	《勧告》ERAB に参画する各事業者は、詳細対策要件について、脆弱性が顕在化するなど早急な対策が求められる際には随時更新すること。	

ERABセキュリティガイドラインとCPSFの対応表【案】(9)

節・項番号	ERABサイバーセキュリティガイドラインにおける対策要件	CPSFにおける主な対策要件ID
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	《勧告》ERAB に参画する各事業者は、経営層の責任の下、自社のセキュリティ対策の現状、自社が最終的に目指すべきセキュリティ対策を明確にした上で、詳細対策要件、その実現に向けたプロセスを検討すること。	CPS.SC-2 CPS.IP-3 CPS.IM-1
	《勧告》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）によるセキュリティ対策の検証・改善を行い、ERAB に参画する各事業者が自らの責任において自主的かつ継続的に更なる高みを目指す形でセキュリティ対策を実施すること。	CPS.AT-1 CPS.AE-3 CPS.BE-2 CPS.IP-7, 9 CPS.DP-4 CPS.RA-4 CPS.RP-1 CPS.RM-1
	《勧告》セキュリティ管理責任者を任命するとともに、当該管理者間で情報共有できる体制を構築すること。	CPS.BE-2
	《勧告》事業者内や取引先等の関係者に対してセキュリティに関する役割を明確にすること。	CPS.SC-1
	《勧告》セキュリティに関連する情報を文書化し、管理すること。	CPS.RA- 3 CPS.GV-1
	《勧告》セキュリティ対策の実施状況に関する報告事項を定め、適時に報告を行うこと。	CPS.AM-6 CPS.BE-2
	《勧告》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・訓練を計画し適時に実施すること。またセキュリティ教育・訓練の効果についても確認すること。	CPS.AT-1
	《勧告》ERAB に参画する各事業者は、セキュリティ管理を推進し、セキュリティガバナンスの構築を行う責任主体として、セキュリティ管理責任組織を設置し、当該組織の管理下にて PDCA サイクルを回すことができる運用・管理体制を構築すること。	CPS.SC-2 CPS.IP-3
	《勧告》セキュリティ対策の実施には上限がないため、対策の検討に際しては、実施に要するコストも勘案しつつ、過剰な投資を行うことなく必要十分な範囲で対策を講ずること。	CPS.SC-2 CPS.IP-3

ERABセキュリティガイドラインとCPSFの対応表【案】(10)

節・項番号	ERABサイバーセキュリティガイドラインにおける対策要件	CPSFにおける主な対策要件ID
4.1.1. ERAB に参画する各事業者におけるセキュリティ対策の設定・実施	《勧告》ERAB に参画する各事業者は、本ガイドラインに記載された要求事項にとどまらず、自社の ERAB システムが満たすべき対策を適切に設定すること。	CPS.CO-3 CPS.RM-1 CPS.SC-2 CPS.IP-3
4.1.2. ERAB に参画する各事業者におけるセキュリティ対策の検証・改善	《勧告》ERAB に参画する各事業者は、セキュリティ対策を踏まえた ERAB システムの構築、セキュリティ対策の実施状況の評価、改善を図ること。	CPS.SC-2 CPS.IP-3
4.1.3. ERAB に参画する各事業者におけるセキュリティ対策の第三者認証	《推奨》ERAB に参画する各事業者は、セキュリティ対策について一定以上の品質が担保された内部監査等を受けること。（以下略）	CPS.SC-6 CPS.AC-1, 3

ERABセキュリティガイドラインとCPSFの対応表【案】(11)

節・項番号	ERABサイバーセキュリティガイドラインにおける対策要件	CPSFにおける対策要件ID
4.1.4. 各事業者における監視・対応体制等	《勧告》ERAB に参画する各事業者は、事業者、システムの構築メーカー、事業者間の調整を担う機関、脆弱性関連情報の分析等を担う機関の間において、脆弱性関連情報を共有・管理すること。	CPS.AE-4 CPS.RP-2 CPS.CO-1
	《勧告》PDCA サイクルを回すことができる運用・管理体制を構築することを前提としつつ、システムの状況の監視やインシデントへの対応が可能な体制を構築すること。	CPS.AE-3 CPS.BE-2 CPS.CM-1, 5, 6 CPS.DP-2, 3, 4 CPS.IP-7 CPS.RA-2, 4 CPS.RM-1
	《勧告》インシデント発生時の被害を考慮し、そのインシデントがより大規模な事故に発展しないよう、その異常を最小限にとどめるための対応及び対応体制の構築をすること。	CPS.IP-10 CPS.CO-2

ERABセキュリティガイドラインとCPSFの対応表【案】(11)

節・項番号	ERABサイバーセキュリティガイドラインにおける対策要件	CPSFにおける対策要件ID
4.1.4. 各事業者における監視・対応体制等 （つづき）	《勧告》インシデントの対応について、単に体制を構築するのではなく、事故が実際に生じ得ることを前提とした上で、実際に対応を行えるよう有事の際の対応計画を策定すること。	CPS.RP-1, 2, 3 CPS.CO-1, 2, 3
	《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。	CPS.BE-3 CPS.AT-1, 2
	《推奨》システムの状況の監視については、システムの異常の予兆を検知するとともに異常の発生時にその要因を特定できるようにするため、収集すべきログを選別し、恒常的にその分析を行うこと。	CPS.CM-2, 5, 6, 7 CPS.CO-2, 3 CPS.RA-2 CPS.DS-6 CPS.MA-1, 2 CPS.PT-1 CPS.DP-1
	《勧告》システムに関連する施設や施設内に設置されるシステムについて、保護対象となるセキュリティ区画を明確にし、適切に保護するとともに、許可された者だけがアクセスできるよう入退管理を行うこと。システム調達時にはセキュリティ仕様を明確にし、設計・製造時等にその準拠性を確認するとともに、仕様変更時にはセキュリティ対策の再構築を行うこと。	CPS.AC-2

「ERABシステムに関するサイバーセキュリティ・レジリエンス・トレーニングプログラム」概要

- 事業の内容
  - ユースケースや教材の開発、トレーニングの試行実施等
- トレーニングの構成等
  - 集合研修とハンズオン演習の構成
    - 集合研修
      - 最大4日間の座学とする。オンラインでの実施（予定）
    - ハンズオン演習
      - 蓄電池を制御する模擬システムを構築し、当該システムへの攻撃を体験（1日の予定）
  - 2021年1月（予定）にトレーニングを試行的に実施

標準ユースケース、リスク分析、対策例の対応表の更新について

- 今後、ERAB事業の発展や技術の進歩により、**継続的に、標準ユースケース、リスク分析、対策例の対応表を更新することが必要**となる。
- これらの更新に当たっては、**トレーニングプログラムを実施するIPAにおける研修教材のアップデートと連携して実施する**。
- その際、**必要に応じて、本サイバーセキュリティWGと連携**することとしてはどうか。その**具体的な対応内容は座長に一任する**。

今後の進め方（案）

- **対策例（ガイドラインの対策とCPSF対策例との対応表）**や**トレーニングプログラムの開発に関する今後の進め方は以下のとおり**となる。