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Ver3.0（案）の改定内容について

株式会社野村総合研究所

コンサルティング事業本部
ICT・コンテンツ産業コンサルティング部

2024年12月18日

Envision the value,
Empower the change

物理的なゲートウェイを介さずに通信・制御を行うDRサービスや、IoT機器の脆弱性を狙った脅威、プライバシー性の高い情報に関する脅威の増加といった変化に起因して、起こり得る新たな脅威の想定やリスクシナリオの検討を行った上で必要となる対策の検討を実施した

背景

1. IoTデバイスの導入数の増加に伴い、物理的なゲートウェイを介さずに通信・制御を行うDRサービスが増加している。
2. IoT製品の増加に伴い、IoT製品の脆弱性を狙ったサイバー脅威も増加してる。
3. 対象デバイスから取得できる関連情報（在宅・不在情報）の多様化により、犯罪の脅威が増大している。

検討内容

1. <u>物理的なゲートウェイを介さないDRサービス</u>
   ゲートウェイがクラウド上にある、物理ゲートウェイを介さないDRサービスに必要な対策を検討した。
2. <u>IoTデバイスの脆弱性に起因する脅威</u>
   ERABで制御されるIoTデバイスの要件を検討した。(セキュリティ要件適合評価及びラベリング制度(JC-STAR)を参照する)
3. <u>デバイスから奪取される可能性のある情報（在宅/不在情報）に起因するリスク</u>
   制御対象デバイスおよび関連情報の多様化に伴うセキュリティリスクに対処するために必要な要件を検討した。

実施項目

1. **リスク分析シートの作成**
   （ERABシステムのリバイス、脅威の想定、シナリオ検討、リスク分析、必要となる対策の検討）
2. **ERABサイバーセキュリティガイドラインの改定**
   （改定方針の検討、新たに盛り込むべき事項の整理、改定案の作成）

前回の振り返り

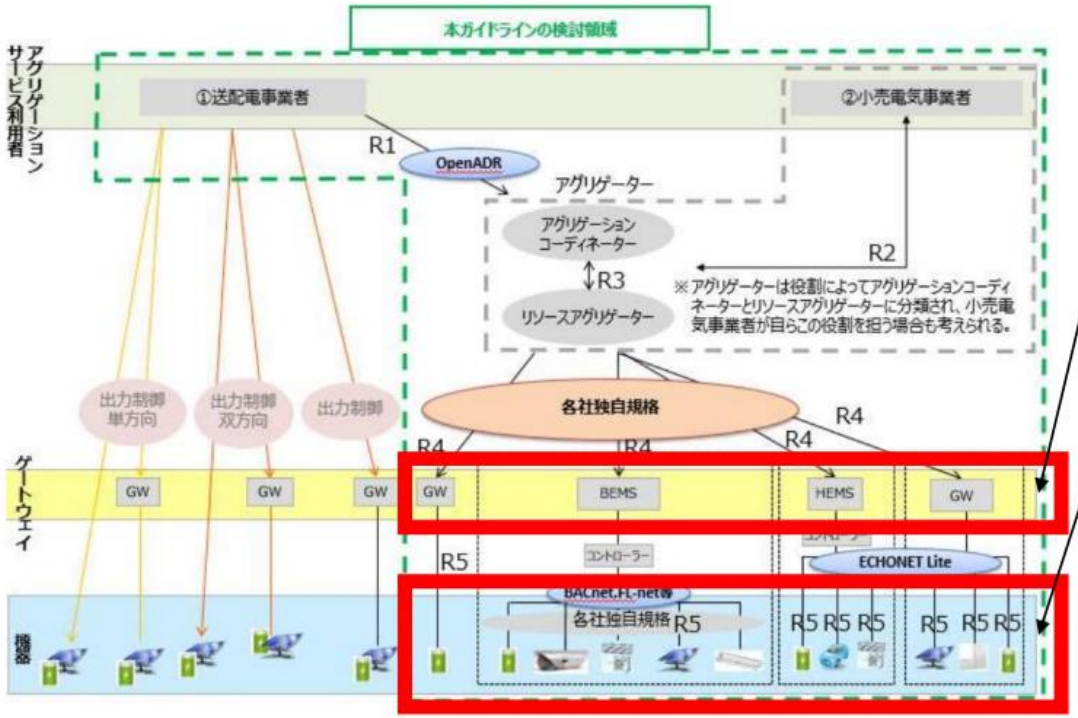
【参考】ERABサイバーセキュリティガイドラインの改定検討領域

- 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



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後、記載。

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後、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、制御対象機器及び関連の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後、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 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（事務局提出資料）

ERABサイバーセキュリティガイドラインの改定業務の概要

ERABサイバーセキュリティガイドラインの改定案作成のプロセス

ERABシステムのリバイス

複数の異なる事業者によるERAB制御対象のエネルギー機器の遠隔制御、コントローラーの設置環境の多様化（クラウド環境等）、物理的なゲートウェイを介さないERAB制御対象のエネルギー機器の遠隔制御など、実態に即したERABシステムの新しいユースケースを整理した。

リスクシナリオの作成

現在のERABシステムの新しいユースケースにおいて想定される脅威を想定リスクシナリオとして洗い出した。

以下の有識者や業界団体の意見を伺いながら、検討を実施。

- 情報処理推進機構(IPA)
- 梅嶋真樹氏（慶應義塾大学サイバー文明研究センター(CCRC)）
- エネルギーリソースアグリゲーション事業協会(ERA)
- エコーネットコンソーシアム

リスク値の算定

各リスクシナリオにおける対応優先度の高いリスクを抽出するために、情報処理推進機構（IPA）が策定する「制御システムのセキュリティリスク分析ガイド 第2版」の考え方に基づいてリスクの評価を実施した。

- 資産ベースのリスク分析・評価
- 事業被害ベースのリスク分析・評価

リスクに応じた必要対策の検討

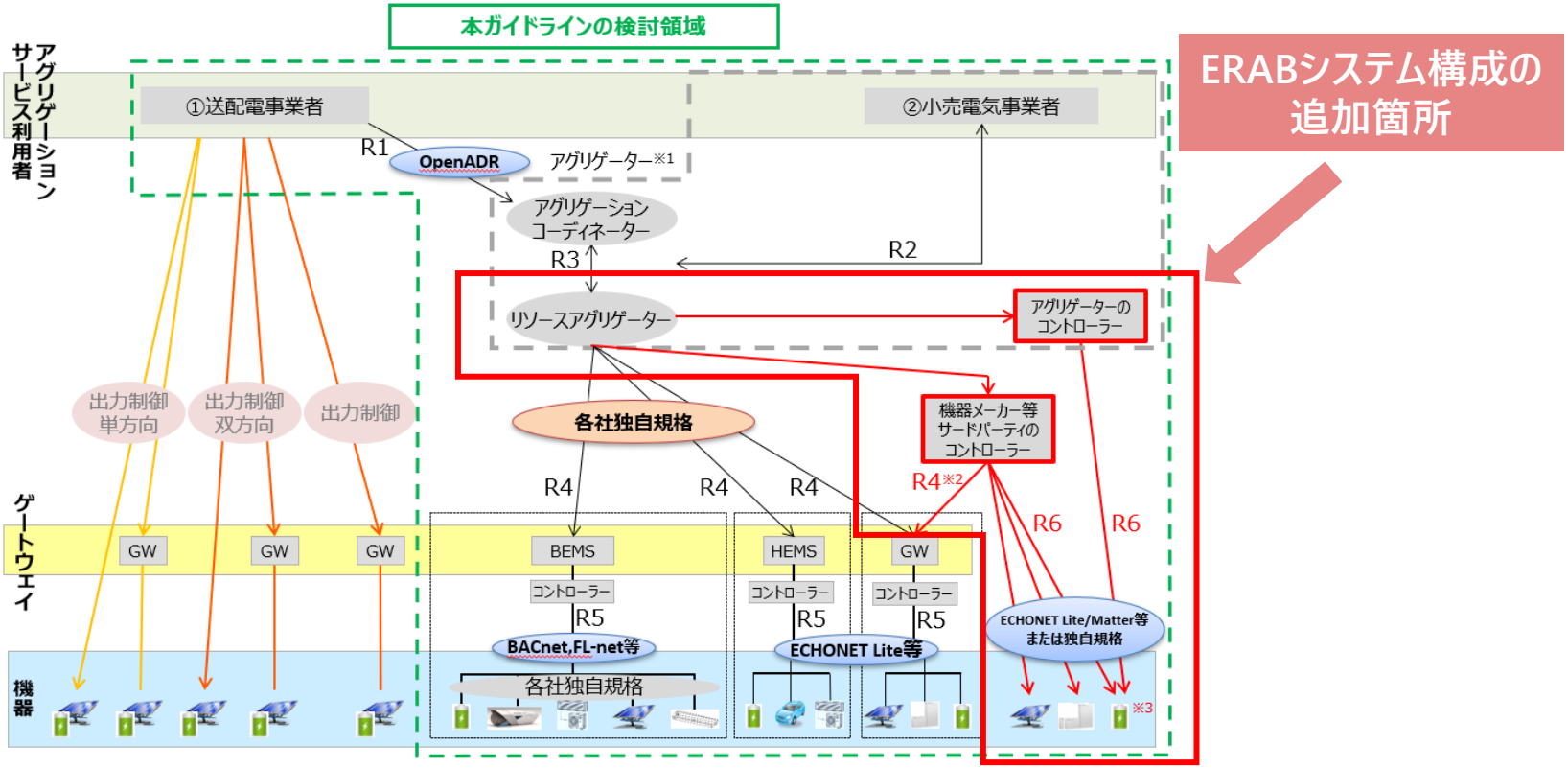
各リスクシナリオの脅威に有効となる対策を、経済産業省が策定する「サイバー・フィジカル・セキュリティ対策フレームワーク」との紐づけにより、新たに盛り込むべき対策要件として整理した。
さらに、当該対策要件とERABサイバーセキュリティガイドライン2.0版（現行版）の内容を照らし合わせ、脅威への対処が可能であり、かつ経済合理性も認められるサイバーセキュリティ対策を抽出し、改定案を作成した。

ERABサイバーセキュリティガイドライン改訂案

ERABシステムにおける全体図

ERABシステム構成の追加箇所

- 単一の機器に複数の異なる仕様のプロトコルスタックを共存させる方法を用いて、複数の異なる事業者(リソースアグリゲーター、機器メーカー等サードパーティ)が、同一のERAB制御対象のエネルギー機器との通信・制御を実施するユースケースを追加。
- 機器メーカー等サードパーティのコントローラーを経由して、直接または需要家側のルータ経由でのERAB制御対象のエネルギー機器との通信・制御を実施するユースケースを追加。



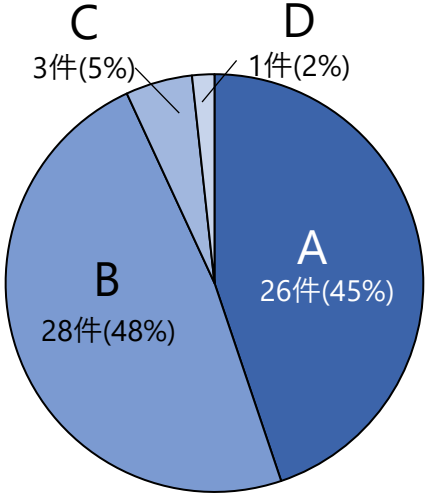
※1　アグリゲーターは、役割によってアグリゲーションコーディネーターとリソースアグリゲーターに分類され、小売電気事業者が自らこの役割を担う場合も考えられる。
※2　HEMSやBEMSと連携することも考えられる。
※3　単一の機器に、複数の異なる仕様のプロトコルスタックが共存する場合がある。

ERABシステムで想定される脅威を洗い出し、リスク評価を実施

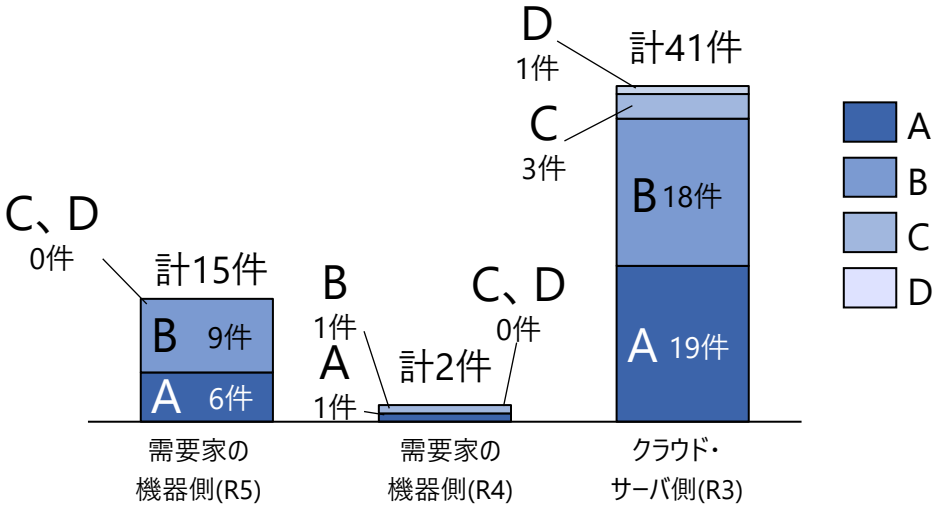
追加されたリスクシナリオ（58件）における脅威・攻撃シナリオの内訳

脅威・攻撃シナリオ	該当シナリオ数
不正アクセス	15
マルウェア感染	7
設定ミス	6
機器のなりすまし	4
DoS/DDoS攻撃	4
中間者攻撃	4
ランサムウェア感染	3
災害・障害等	3
パスワード総当たり攻撃	2
フィッシング攻撃	2
Webサイトの改ざん	2
内部者攻撃	2
セキュリティ機能の設定の不備	2
誤操作	1
機器製造時のマルウェア混入	1

追加されたリスクシナリオ（58件）におけるリスクレベル



各インターフェースにおけるリスクレベルの内訳



※A（リスクが非常に高い）～ D（リスクが低い）

リスクに応じた必要対策の検討

リスクレベルが高いリスクシナリオにおける、リスクの高い資産に対して必要な対策を検討した

- 事業被害ベースのリスクシナリオのうち、リスクレベル「A」または「B」に相当するものについては、内部ネットワークで利用される需要家側のルータや通信プロトコル等の脆弱性に関連するものが多く含まれていることが確認できた。
- その上で、リスクレベル「A」または「B」に相当するものについては、すべて資産ベースでのリスクを重層的に評価し、リスクの高い資産に対して、脅威・リスクへの対処が可能で、経済合理性が認められる必要な対策を検討した。
- 対策については、機器のセキュリティ強化、機器やソフトウェア・プロトコル等の脆弱性対策、通信先の制限対策、クラウド・サーバー側のセキュリティ対策や不正ログイン対策、システムのデータバックアップ対策が強化がポイントであることが分かった。
- 加えて、ERABに参加する各事業者の自組織における、資産の脆弱性確認、システムの設定確認、異常確認等の基本的な対策の根本的確保、自組織で確認された脆弱性情報やシステム異常情報等の関係者への共有が強化のポイントであることが分かった。
- なお、結果的に、上記のリスクの高い資産への対策によって、リスクレベル「C」または「D」に相当するリスクシナリオについても、対応可能であることを確認できた。

リスクに応じた必要対策の検討

機器のセキュリティ強化、機器やソフトウェア・プロトコル等の脆弱性対策、クラウド・サーバー側のセキュリティ対策や不正ログイン対策、システムのデータバックアップ対策が強化のポイント

ERABシステムに 新たに追加された機能	脅威・リスクとの関係
●GWを介さないERAB制御対象のエネルギー機器との通信	●GW配下ではなくなるため、ERAB制御対象のエネルギー機器や制御用通信が直接、攻撃者の標的となり、不正アクセスや通信路上での盗聴・改ざん、なりすましなどのインターネット上の脅威にさらされる可能性がある。【脅威・リスクⅠ】
●クラウド環境上のコントローラー機能を用いた、外部からのERAB制御対象のエネルギー機器の遠隔制御 ●ERAB制御対象のエネルギー機器から取得した情報のクラウド環境上での保存	●コントローラー機能が実装されているクラウドサーバーやその管理用インターフェースが攻撃者の標的となり、不正侵入やマルウェア感染、乗っ取りなどの外部脅威や、内部者による脅威にさらされる可能性がある。【脅威・リスクⅡ】 ●データベースサーバーやクラウドストレージ等に保存されているERAB制御対象のエネルギー機器から取得した情報が外部に漏洩した場合、プライバシーの侵害や犯罪に繋がる可能性がある。【脅威・リスクⅢ】

ERABに参加する各事業者の自組織における基本的な対策の根本的確保や、自組織で確認された脆弱性情報やシステム異常情報等の関係者への共有が強化のポイント

ERABシステムに新たに追加された機能	脅威・リスクとの関係
● 複数事業者による多様なネットワークを介した同一のERAB制御対象のエネルギー機器への通信・制御	● ERABシステムにおいて、以下の課題が見られる中、1つのシステムとしてセキュリティ確保の全体的な管理が行なわれていないため、特定のERAB制御対象のエネルギー機器等で発生したインシデントの影響が、ERABシステム全体に波及する可能性がある。【脅威・リスクIV】 • ERABシステムを構成する各システムコンポーネントの管理主体が多岐にわたる。 • 新たに機器メーカー等のサードパーティの資産についても、ERABシステムに接続されるようになっている。 • 各システムコンポーネント間で使用されるプロトコルについて、特定の規格のプロトコルのみが採用される状況になっていない。

ERABサイバーセキュリティガイドラインに新しく盛り込むべき事項

詳細な改定内容（【追加】3.2. ERABシステムが留意すべき基本方針）

対策要件の追加が必要と考えられる理由とその対策

●追加要件が必要な理由となる脅威・リスク：【脅威・リスクIV】

- ERABシステムにおいて、以下の課題が見られる中、1つのシステムとしてセキュリティ確保の全体的な管理が行なわれていないため、特定のERAB制御対象のエネルギー機器等で発生したインシデントの影響が、ERABシステム全体に波及する可能性がある。
  - ERABシステムを構成する各システムコンポーネントの管理主体が多岐にわたる。
  - 新たに機器メーカー等のサードパーティの資産についても、ERABシステムに接続されるようになっている。
  - 各システムコンポーネント間で使用されるプロトコルについて、特定の規格のプロトコルのみが採用される状況になっていない。

●全般的な対策

- このような状況下で、需要家を含む利用者が、アグリゲーションの制御対象リソースの管理主体となる場合も見られる中、利用者が、同リソースの脆弱性対策情報・脅威情報について何も把握していないという状況を発生させないように、情報共有体制を構築することが重要。

新しく盛り込むべき事項の方向性

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、自組織の管理するERABシステムの利用者（ERAB制御対象のエネルギー機器の設置場所の需要家を含む。）へ脆弱性対策情報・脅威情報の通知を行うこと。
- 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。

（以下、略）

ERABサイバーセキュリティガイドラインに新しく盛り込むべき事項

詳細な改定内容（【追加】3.3. ERABシステムが想定すべき脅威）

対策要件の追加が必要と考えられる理由とその対策

●追加要件が必要な理由となる脅威・リスク：【脅威・リスクⅠ、Ⅱ及びⅢ】

- リスク評価を行った結果、不正アクセス、不正操作、機能停止、情報の窃取、情報の改ざん、プロセスの不正な実行、高負荷攻撃（バッファーオーバーフロー攻撃、DoS/DDoS攻撃）、不正送信、バックドアを悪用する攻撃、マルウェア感染、ランサムウェア感染、盗聴、異常動作（誤動作）等の危険度の高いリスクが多数存在することを確認できた。

●全般的な対策

- このようなさまざまなリスクを想定し、必要な対策を講じることが重要。

新しく盛り込むべき事項の方向性

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。

- 標的型攻撃、不正アクセス、不正操作、機能停止、情報の窃取、情報の改ざん、プロセスの不正な実行、高負荷攻撃（バッファーオーバーフロー攻撃、DoS/DDoS攻撃）、不正送信、バックドアを悪用する攻撃、マルウェア感染、ランサムウェア感染、盗聴、異常動作（誤動作）等の多様なリスクを想定すること。
- 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。

（以下、略）

ERABサイバーセキュリティガイドラインに新しく盛り込むべき事項

詳細な改定内容（【追加】3.4. ERABシステムが維持すべきサービスレベル）

対策要件の追加が必要と考えられる理由とその対策

●追加要件が必要な理由となる脅威・リスク：【脅威・リスクⅠ、Ⅱ】

- GW配下ではなくなるため、ERAB制御対象のエネルギー機器や制御用通信が直接、攻撃者の標的となり、不正アクセスや通信路上での盗聴・改ざん、なりすましなどのインターネット上の脅威にさらされる可能性がある。
- インターネットとの通信を行えるコントローラーやERAB制御対象のエネルギー機器が、インターネット上のさまざまな脅威の標的となっている。

●全般的な対策

- インターネットとの通信が行える幅広いIoT製品を対象として、共通的な物差しで製品に具備されているセキュリティ機能を評価・可視化することを目的とした「セキュリティ要件適合評価及びラベリング制度（JC-STAR）」が、2025年3月から運用開始されることに伴い、IoT機能を有するコントローラーやERAB制御対象のエネルギー機器においても、同制度との効果的な連携を図ることにより、セキュリティを強化することが重要。

新しく盛り込むべき事項の方向性

3.4. ERABシステムが維持すべきサービスレベル

【勧告】

各事業者及びその保有するシステムは以下の定義でのサービスレベルの確保が求められる。

- 容量市場、需給調整市場等における要求事項に準拠したサービスレベル
- 簡易指令システムを有する事業者とそのシステム：「電力制御システムセキュリティガイドライン」に準拠したサービスレベル
- 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：本ガイドラインに準拠したサービスレベル、加えて簡易指令システムとの直接的な接続部においては「電力制御システムセキュリティガイドライン」に準拠したサービスレベル、簡易指令システムを運用する送配電事業者が「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
- リソースアグリゲーターとその保有するシステム：アグリゲーションコーディネーターと接続する場合は、本ガイドラインに準拠したサービスレベル、加えて、アグリゲーションコーディネーターが「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
- ERAB制御対象のエネルギー機器やGW等：「セキュリティ要件適合評価及びラベリング制度（JC-STAR）」が定めるIoT製品に対するセキュリティ要件に準拠したサービスレベル（現時点においては、★１（レベル１）以上を満たすこと。なお、今後、製品類型ごとの特徴を考慮した★２（レベル２）以上の詳細要件が決定した場合においては、★２（レベル２）以上を満たすことが望ましい。）

ERABサイバーセキュリティガイドラインに新しく盛り込むべき事項

詳細な改定内容（【追加】3.6. ERABシステムにおけるサイバーセキュリティ対策）　1/3

対策要件の追加が必要と考えられる理由とその対策

●追加要件が必要な理由となる脅威・リスク：【脅威・リスクⅠ、Ⅱ、Ⅲ及びⅣ】

- リスク評価を行った結果、不正アクセス、不正操作、機能停止、情報の窃取、情報の改ざん、プロセスの不正な実行、高負荷攻撃（バッファーオーバーフロー攻撃、DoS/DDoS攻撃）、不正送信、バックドアを悪用する攻撃、マルウェア感染、ランサムウェア感染、盗聴、異常動作（誤動作）等の危険度の高いリスクが多数存在することを確認できた。

●全般的な対策

- ERABシステムについては、今後も新たなユースケースが創出されていくため、本改定の際に行ったようなリスク分析を行うことにより、想定される新たな脅威やリスクを認識し、そのような脅威やリスクに適切に対処していくことが重要。

新しく盛り込むべき事項の方向性

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：システムが扱う資産ベース及び攻撃シナリオベースによるリスク分析を行うこと。

Step5：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。

Step6：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。

Step7：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。

Step8：事故発生時の対応方法を設計・運用及び訓練すること。

Step9：自組織の資産の脆弱性を特定、文書化し、それをリソースアグリゲーターとの間で共有すること。

（以下、略）

ERABサイバーセキュリティガイドラインに新しく盛り込むべき事項

詳細な改定内容（【追加】3.6. ERABシステムにおけるサイバーセキュリティ対策）　2/3

対策要件の追加が必要と考えられる理由とその対策

●追加要件が必要な理由となる脅威・リスク：【脅威・リスクIV】

- ERABシステムにおいて、以下の課題が見られる中、1つのシステムとしてセキュリティ確保の全体的な管理が行なわれていないため、特定のERAB制御対象のエネルギー機器等で発生したインシデントの影響が、ERABシステム全体に波及する可能性がある。
  - ERABシステムを構成する各システムコンポーネントの管理主体が多岐にわたる。
  - 新たに機器メーカー等のサードパーティの資産についても、ERABシステムに接続されるようになっている。
  - 各システムコンポーネント間で使用されるプロトコルについて、特定の規格のプロトコルのみが採用される状況になっていない。

●全般的な対策

- このような状況下において、ERABに参画する各事業者が、自ら管理主体となっているERABシステム上の資産の脆弱性情報を把握し、リソースアグリゲーターとの間で資産の脆弱性情報に関する情報共有体制を構築することが重要。

新しく盛り込むべき事項の方向性

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：システムが扱う資産ベース及び攻撃シナリオベースによるリスク分析を行うこと。

Step5：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。

Step6：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。

Step7：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。

Step8：事故発生時の対応方法を設計・運用及び訓練すること。

Step9：自組織の資産の脆弱性を特定、文書化し、それをリソースアグリゲーターとの間で共有すること。

（以下、略）

詳細な改定内容（【追加】3.6. ERABシステムにおけるサイバーセキュリティ対策）　3/3

対策要件の追加が必要と考えられる理由とその対策

●追加要件が必要な理由となる脅威・リスク：【脅威・リスクⅡ、Ⅲ】

- コントローラー機能が実装されているクラウドサーバーやその管理用インターフェースが標的となり、不正侵入やマルウェア感染、乗っ取りなどの外部脅威や、内部者による脅威にさらされる可能性がある。
- データベースサーバーやクラウドストレージ等に保存されているERAB制御対象のエネルギー機器から取得した情報が外部に漏洩した場合、プライバシーの侵害や犯罪に繋がる可能性がある。

●全般的な対策

- ERABシステムにおいては、今後もクラウドサービスの利用が増えることが予想される中で、直近に発生しているクラウドサーバーやその管理用インターフェースを標的とした不正ログインによる被害やランサムウェアによる被害に対して、適切に対処することが重要。

新しく盛り込むべき事項の方向性

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】

（中略）

- 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】
- ERABに参画する各事業者は、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、ERAB制御対象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】
- ERABに参画する各事業者は、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、ERAB制御対象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】
- ERABに参画する各事業者は、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、ERABシステムを構成するERAB制御対象のエネルギー機器や外部記憶媒体等へのマルウェア対策を行うこと。また、システムにおける管理者権限の割当や管理者権限の悪用防止対策（管理者アカウントのライフサイクル管理を考慮した安全な管理、端末認証との連携等）を適切に行うとともに、不正な行為やプログラムの実行を阻止し、本来の操作によらない処理が発行されないよう仕組みを講じることが求められる。ERABシステムを構成するERAB制御対象のエネルギー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。また、ランサムウェア被害に備えるため、システムのバックアップデータを定期的に取得し、安全な場所で適切に管理すること。【マルウェアへの対策】

ERABサイバーセキュリティガイドラインに新しく盛り込むべき事項

詳細な改定内容（【追加】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（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）他）

対策要件の追加が必要と考えられる理由とその対策

●追加要件が必要な理由となる脅威・リスク：【脅威・リスクⅣ】

- ERABシステムにおいて、以下の課題が見られる中、1つのシステムとしてセキュリティ確保の全体的な管理が行なわれていないため、特定のERAB制御対象のエネルギー機器等で発生したインシデントの影響が、ERABシステム全体に波及する可能性がある。
  - ERABシステムを構成する各システムコンポーネントの管理主体が多岐にわたる。
  - 新たに機器メーカー等のサードパーティの資産についても、ERABシステムに接続されるようになっている。
  - 各システムコンポーネント間で使用されるプロトコルについて、特定の規格のプロトコルのみが採用される状況になっていない。

●全般的な対策

- このような状況下で、機器等の不正接続やなりすまし、不正送信による被害を防ぐことが求められるため、通信先の制限が重要。
- また、機器の開発時にバックドアが仕掛けられた場合の攻撃者のC&Cサーバーとの通信についても制限することが重要。

新しく盛り込むべき事項の方向性

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（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）

【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、ホワイトリスト等を用いた通信先の制限、認証、通信メッセージの暗号化により保護すること。

（中略）

- 開放されているネットワークポートを確認し、不要なポートを物理的又は論理的に閉塞すること。

同様の修正を、以下においても実施する。

- 3.6.2. 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）
- 3.6.3. 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）
- 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）

ERABサイバーセキュリティガイドラインに新しく盛り込むべき事項

詳細な改定内容（【追加】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））　1/2

対策要件の追加が必要と考えられる理由とその対策

●追加要件が必要な理由となる脅威・リスク：【脅威・リスクⅠ、Ⅱ】

- コントローラー機能が実装されているクラウドサーバーやその管理用インターフェースが標的となり、不正侵入やマルウェア感染、乗っ取りなどの外部脅威や、内部者による脅威にさらされる可能性がある。
- インターネットとの通信を行えるコントローラーが、インターネット上のさまざまな脅威の標的となっている。

●全般的な対策

- 需要家側GWの外側にあるクラウドサーバー上に構築されたコントローラー機能について、適切なセキュリティ対策を行うことが重要。
- 需要家側GWの内側にあるIoT機能を有するコントローラーのセキュリティを強化することが重要。

新しく盛り込むべき事項の方向性

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）

- ERAB制御対象のエネルギー機器、GW又は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のシステム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。

（中略）

- リソースアグリゲーターは、リソースアグリゲーターとERAB制御対象のエネルギー機器が接続するネットワーク構成を確認すること。その際、ERAB制御対象のエネルギー機器を制御するコントローラーが、需要家側GWの内側に配置されているか、需要家側GWの外側にコントローラーの一部又は全部が配置されているかを分類し、各々において適切な対策を行うこと。

ERABサイバーセキュリティガイドラインに新しく盛り込むべき事項

詳細な改定内容（【追加】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））　2/2

対策要件の追加が必要と考えられる理由とその対策

●追加要件が必要な理由となる脅威・リスク：【脅威・リスクⅡ、Ⅳ】

- ERABシステムを構成する各システムコンポーネント間の通信で使用されるプロトコルについては、特定の規格のプロトコルのみが採用される状況になっていないため、なかには管理が行き届かない脆弱性を有するプロトコルを使用する事業者もみられる。また、直近においては、プロトコルの脆弱性に起因するサイバー攻撃も多く発生している。
- インターネットとの通信を行えるリソースアグリゲーターの制御対象の機器が、インターネット上のさまざまな脅威の標的となっている。

●全般的な対策

- プロトコルの脆弱性に起因するリスクに適切に対処することが重要。（②末端のIoT機器等の脆弱性に起因する脅威への対策）
- インターネットとの通信が行える幅広いIoT製品を対象として、共通的な物差しで製品に具備されているセキュリティ機能を評価・可視化することを目的とした「セキュリティ要件適合評価及びラベリング制度（JC-STAR）」が、2025年3月から運用開始されることに伴い、IoT機能を有するリソースアグリゲーターの制御対象の機器においても、同制度との効果的な連携を図ることにより、セキュリティを強化することが重要。

新しく盛り込むべき事項の方向性

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】

（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、ホワイトリスト等を用いた通信先の制限、認証、通信メッセージの暗号化により保護すること。
- 管理組織の特定が可能で、かつ脆弱性対策が設計可能であるプロトコルを採用すること。
- リソースアグリゲーターの制御対象にIoT製品を新たに導入する場合においては、「セキュリティ要件適合評価及びラベリング制度（JC-STAR）」が定める適合基準である★１（レベル１）以上※を満たす製品を選択すること。

  ※今後、製品類型ごとの特徴を考慮した★２（レベル２）以上の詳細要件が決定した場合においては、★２（レベル２）以上を満たす製品を選択することが望ましい。
- 開放されているネットワークポートを確認し、不要なポートを物理的又は論理的に閉塞すること。

ERABサイバーセキュリティガイドラインに新しく盛り込むべき事項

詳細な改定内容（【追加】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のインターフェース））

対策要件の追加が必要と考えられる理由とその対策

●追加要件が必要な理由となる脅威・リスク【脅威・リスクⅡ、Ⅳ】

- ERABシステムを構成する各システムコンポーネント間の通信で使用されるプロトコルについては、特定の規格のプロトコルのみが採用される状況になっていないため、なかには管理が行き届かない脆弱性を有するプロトコルを使用する事業者もみられる。また、直近においては、プロトコルの脆弱性に起因するサイバー攻撃も多く発生している。
- インターネットとの通信を行えるERAB制御対象のエネルギー機器が、インターネット上のさまざまな脅威の標的となっている。

●全般的な対策

- プロトコルの脆弱性に起因するリスクに適切に対処することが重要。（②末端のIoT機器等の脆弱性に起因する脅威への対策）
- インターネットとの通信が行える幅広いIoT製品を対象として、共通的な物差しで製品に具備されているセキュリティ機能を評価・可視化することを目的とした「セキュリティ要件適合評価及びラベリング制度（JC-STAR）」が、2025年3月から運用開始されることに伴い、IoT機能を有するERAB制御対象のエネルギー機器においても、同制度との効果的な連携を図ることにより、セキュリティを強化することが重要。

新しく盛り込むべき事項の方向性

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のインターフェース）

【推奨】

（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、ホワイトリスト等を用いた通信先の制限、認証、通信メッセージの暗号化により保護すること。
- 管理組織の特定が可能で、かつ脆弱性対策が設計可能であるプロトコルを採用すること。
- リソースアグリゲーターの制御対象にIoT製品を新たに導入する場合においては、「セキュリティ要件適合評価及びラベリング制度（JC-STAR）」が定める適合基準である★１（レベル１）以上※を満たす製品を選択すること。

  ※今後、製品類型ごとの特徴を考慮した★２（レベル２）以上の詳細要件が決定した場合においては、★２（レベル２）以上を満たす製品を選択することが望ましい。
- 開放されているネットワークポートを確認し、不要なポートを物理的又は論理的に閉塞すること。

ERABサイバーセキュリティガイドラインに新しく盛り込むべき事項

詳細な改定内容（【新設】3.6.6. R6（GWを介さずに直接通信するリソースアグリゲーターとERAB制御対象のエネルギー機器間のインターフェース））　1/2

対策要件の追加が必要と考えられる理由とその対策

●追加要件が必要な理由となる脅威・リスク：【脅威・リスクⅠ】

- GW配下ではなくなるため、ERAB制御対象のエネルギー機器や制御用通信が直接、攻撃者の標的となり、不正アクセスや通信路上での盗聴・改ざん、なりすましなどのインターネット上の脅威にさらされる可能性がある。

●全般的な対策

- R6におけるERAB制御対象のエネルギー機器は、リソースアグリゲーターのシステムとインターネット経由で直接通信することから、R5におけるERAB制御対象のエネルギー機器と、R4におけるリソースアグリゲーターの制御対象の機器の２つの特徴を持つ。このため、従来のR5における対策に加えて、R4における対策を併せて実施することが重要。（**①物理的なGWを介さないDRサービスへの対策**）

新しく盛り込むべき事項の方向性

3.6.6. R6（GWを介さずに、直接通信するリソースアグリゲーターとERAB制御対象のエネルギー機器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）

- ERAB制御対象のエネルギー機器、GW又は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のシステム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。

  ※本ガイドラインのR6は、リソースアグリゲーターのシステムとERAB制御対象のエネルギー機器間の通信路として、公衆網が使われる場合を前提としている。なお、リソースアグリゲーターのシステムとERAB制御対象のエネルギー機器を通信端点とした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、エンドツーエンドで伝送路の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得るものと考えられる。
- リソースアグリゲーターは、リソースアグリゲーターとERAB制御対象のエネルギー機器が接続するネットワーク構成を確認し、適切な対策を行うこと。

ERABサイバーセキュリティガイドラインに新しく盛り込むべき事項

詳細な改定内容（【新設】3.6.6. R6（GWを介さずに直接通信するリソースアグリゲーターとERAB制御対象のエネルギー機器間のインターフェース））　2/2

対策要件の追加が必要と考えられる理由とその対策

●追加要件が必要な理由となる脅威・リスク：【脅威・リスクⅠ】

- GW配下ではなくなるため、ERAB制御対象のエネルギー機器や制御用通信が直接、攻撃者の標的となり、不正アクセスや通信路上での盗聴・改ざん、なりすましなどのインターネット上の脅威にさらされる可能性がある。

●全般的な対策

- R6におけるERAB制御対象のエネルギー機器は、リソースアグリゲーターのシステムとインターネット経由で直接通信することから、R5におけるERAB制御対象のエネルギー機器と、R4におけるリソースアグリゲーターの制御対象の機器の２つの特徴を持つ。このため、従来のR5における対策に加えて、R4における対策を併せて実施することが重要。（**①物理的なGWを介さないDRサービスへの対策**）

新しく盛り込むべき事項の方向性

3.6.6. R6（GWを介さずに直接通信するリソースアグリゲーターとERAB制御対象のエネルギー機器間のインターフェース）

【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、ホワイトリスト等を用いた通信先の制限、認証、通信メッセージの暗号化により保護すること。
- 管理組織の特定が可能で、かつ脆弱性対策が設計可能であるプロトコルを採用すること。
- リソースアグリゲーターの制御対象にIoT製品を新たに導入する場合においては、「セキュリティ要件適合評価及びラベリング制度（JC-STAR）」が定める適合基準である★１（レベル１）以上※を満たす製品を選択すること。

  ※今後、製品類型ごとの特徴を考慮した★２（レベル２）以上の詳細要件が決定した場合においては、★２（レベル２）以上を満たす製品を選択することが望ましい。
- 開放されているネットワークポートを確認し、不要なポートを物理的又は論理的に閉塞すること。

ERABサイバーセキュリティガイドラインに新しく盛り込むべき事項

詳細な改定内容（【追加】3.7. 取扱情報の差異や動作環境の差異によるERABシステムの設計）

対策要件の追加が必要と考えられる理由とその対策

●追加要件が必要な理由となる脅威・リスク：

【脅威・リスクⅡ、Ⅲ】

- コントローラー機能が実装されているクラウドサーバーやその管理用インターフェースが標的となり、不正侵入やマルウェア感染、乗っ取りなどの外部脅威や、内部者による脅威にさらされる可能性がある。
- データベースサーバーやクラウドストレージ等に保存されているERAB制御対象のエネルギー機器から取得した情報が外部に漏洩した場合、プライバシーの侵害や犯罪に繋がる可能性がある。

●全般的な対策

- ERABシステムにおいては、今後もクラウドサービスの利用が増えることが予想される中で、クラウドサービスを利用したERABシステムの設計時や構築時において、セキュリティを担保することが重要。

新しく盛り込むべき事項の方向性

3.7. 取扱情報の差異や動作環境の差異による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。

ERABシステムは、その想定される脅威・リスクにおいて、アグリゲーターが構築する付加価値に応じて大きく異なる特色を持つ。

ゆえに、ERABシステムのセキュリティ対策の枠組みを構築するに当たっての前提として、現時点で想定され、ERABに参画する各事業者が満たすべき最低限のサービスレベルを設定し、当該サービスレベルを実現するためのセキュリティ対策とすることが適当である。例えば、「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アグリゲーター」と「個人情報を活用したサービス構築を設計するアグリゲーター」とでは、必要とされる対策が異なる。

- ERABに参画する各事業者は、自組織の管理するクラウドサービスを活用したシステムの動作環境の差異を明確化し、その結果に見合ったシステムを設計すること。

ERABシステムには、事業者が各々の動作環境（ハードウェアやソフトウェア）を準備して、自らがコントロールするオンプレミスのシステムに加えて、クラウドサービスを活用して構築・運用するシステムがあり、クラウドサービスを活用したシステムでは、クラウド事業者の約款や利用規約等の取決めによって、セキュリティ担保のレベルや条件、クラウド事業者と利用者におけるセキュリティ対策の責任・役割分担が異なる。

ERABサイバーセキュリティガイドラインに新しく盛り込むべき事項

詳細な改定内容（【新設】3.7.3. クラウドサービスを活用したサービス構築を設計する事業者 ）

対策要件の追加が必要と考えられる理由とその対策

●追加要件が必要な理由となる脅威・リスク：【脅威・リスクⅡ、Ⅲ】

- コントローラー機能が実装されているクラウドサーバーやその管理用インターフェースが標的となり、不正侵入やマルウェア感染、乗っ取りなどの外部脅威や、内部者による脅威にさらされる可能性がある。
- データベースサーバーやクラウドストレージ等に保存されているERAB制御対象のエネルギー機器から取得した情報が外部に漏洩した場合、プライバシーの侵害や犯罪に繋がる可能性がある。

●全般的な対策

- ERABシステムにおいては、今後もクラウドサービスの利用が増えることが予想される中で、クラウドサービスを利用したERABシステムの設計時や構築時、運用時において、セキュリティを担保することが重要。
- クラウド環境上に保存された情報の外部漏えいを防ぐため、強固な認証基盤や管理用端末の接続制限機能が備わっている安全なクラウドサービスを利用することが重要。（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への対策）

新しく盛り込むべき事項の方向性

3.7.3. クラウドサービスを活用したサービス構築を設計する事業者

【勧告】

- 外部の事業者が提供するクラウドサービスを利用して、アグリゲーションコーディネーターのシステム又はリソースアグリゲーターのシステムが構築・運用されている場合や、ERAB制御対象のエネルギー機器から取得した情報を当該クラウド環境に保存している場合、当該クラウドサービスに対して、3.6.で規定するマルウェアへの対策や、3.7.2.で規定する個人情報の適切な管理に関する対策、4.1.4.で規定する監視・対応体制等（勧告事項）に関する要求事項に対して、当該クラウドサービスが適合していることを確認すること。なお、ISMAPクラウドサービスリストに登録されているクラウドサービスを利用する場合には、上記の確認を省略することが可能である。
- 「クラウドを利用したシステム運用に関するガイダンス（詳細版）」等を参照した対策をとること。
- クラウドサービスを利用する管理者等を認証するために、十分に強固な認証基盤が提供されていることを確認し、その機能を利用した対策をとること。
- クラウドサービスを活用したシステムにログインすることのできる管理用端末を制限できることを確認し、その機能を利用した対策をとること。

ERABサイバーセキュリティガイドラインに新しく盛り込むべき事項

詳細な改定内容（【追加】4.1.4. 各事業者における監視・対応体制等）

対策要件の追加が必要と考えられる理由とその対策

●追加要件が必要な理由となる脅威・リスク：【脅威・リスクIV】

- ERABシステムにおいて、以下の課題が見られる中、1つのシステムとしてセキュリティ確保の全体的な管理が行なわれていないため、特定のERAB制御対象のエネルギー機器等で発生したインシデントの影響が、ERABシステム全体に波及する可能性がある。
  - ERABシステムを構成する各システムコンポーネントの管理主体が多岐にわたる。
  - 新たに機器メーカー等のサードパーティの資産についても、ERABシステムに接続されるようになっている。
  - 各システムコンポーネント間で使用されるプロトコルについて、特定の規格のプロトコルのみが採用される状況になっていない。

●全般的な対策

- このような状況下でERABシステムのセキュリティを担保するには、ERABに参加する各事業者の自組織でのセキュリティ対応を強化する必要があり、少なくとも脆弱性確認、設定ミス確認、システム異常確認については、システム接続先となっている事業者との間で確認された脆弱性情報やシステム異常情報の共有を含め、その責任・役割を果たしていくことが重要。

新しく盛り込むべき事項の方向性

4.1.4. 各事業者における監視・対応体制等

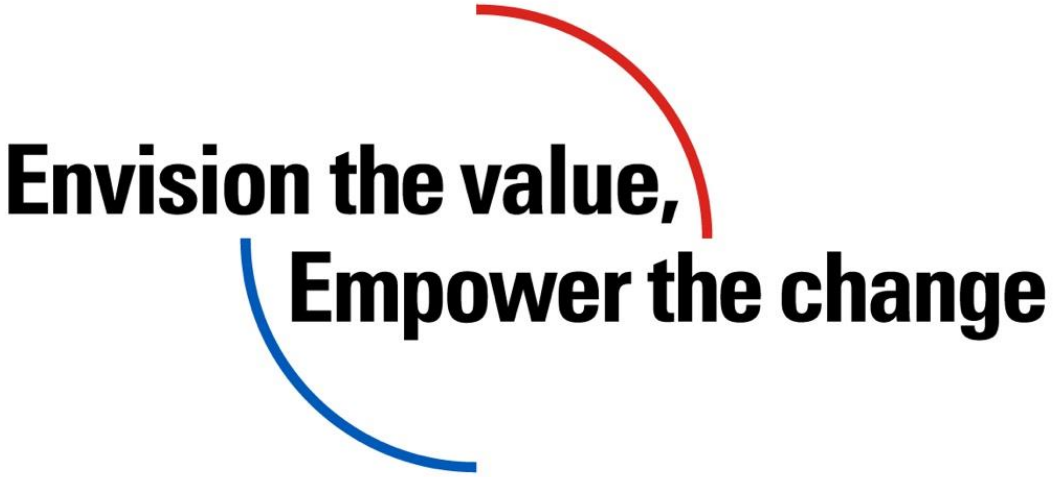
【勧告】

（中略）

- ERAB に参画する各事業者は、自組織の管理するERABシステムで利用する機器やソフトウェア、プロトコル等に対して、定期的に対処が必要な脆弱性の有無を確認できる体制を構築すること。
- ERAB に参画する各事業者は、自組織の管理するERABシステムに対して、定期的に機能や権限に関する設定ミスの有無を確認できる体制を構築すること。
- 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。※
- ERAB に参画する各事業者は、自組織の資産の脆弱性を特定、文書化し、それをリソースアグリゲーターとの間で共有すること。また、システムの異常を検知した場合、その情報を接続先の事業者との間で速やかに共有すること。
- ERAB制御対象のエネルギー機器やGWと外部が相互アクセス可能であるとの以下の認識に基づき監視・対応体制等の検討を行うこと。

外部からのアクセスのユースケースとして、需要家のネットワーク上の機器から同一ネットワーク上の機器にアクセスするケース、無線LANルーター経由で需要家のネットワーク上の機器にアクセスするケース、有線LANポート経由で需要家のネットワーク上の機器にアクセスするケースが考えられる。

※この対策要件は、元の【推奨】から、新たに【勧告】へと移行させるもの


Envision the value,
Empower the change