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

Ver.2.0 から Ver.3.0 への主な変更点

2025年5月

ナオサイバーテック株式会社

本資料は、資源エネルギー庁「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Ver.2.0からVer.3.0への主な変更点を、Google NotebookLMを活用して分析したものです。

- 「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Ver.3.0」
  https://www.enecho.meti.go.jp/category/saving_and_new/advanced_systems/vpp_dr/20250522.pdf
- 「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Ver.2.0」
  https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_denryoku/pdf/007_05_04.pdf

目次

1. 改定概要と背景

●改定日: 令和7年5月22日
- ➢(Ver.2.0 は令和元年12月27日改定)

●改定背景:
- ➢前回の改定以降の ERAB システムにおける構成やユースケースの変化
  - 新しいユースケースの出現
    （例: 複数のクラウド環境上のコントローラー経由接続、単一機器での複数プロトコル共存、GWを介さず直接/間接通信、需要家側GW外のコントローラー設置）
- ➢新しいユースケースを対象としたリスクアセスメントの結果、危険度の高いリスクが多数存在することが確認された。
- ➢サイバー・フィジカル・セキュリティ対策フレームワークの考え方に基づき検討。
- ➢ERAB システム全体でのセキュリティ設計が必要であることが確認された。

2. ERABシステムの構成とインターフェースの変更

●構成要素の明確化・追加:

- ERABシステムの構成要素として、「コントローラー」が明確に位置づけられた。
- コントローラーは需要家側 GW の内側または外側のどちらにも配置されうることが示された。

●インターフェースの追加:

- 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) が追加された。

3. 想定すべき脅威の拡大

●想定すべき脅威の観点の記述を強化:

- Ver.2.0 では「標的型攻撃を想定すること」などが記述されていた。
- Ver.3.0 ではこれに加え、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が明記された。

4. 維持すべきサービスレベルへの要求事項追加

●需要家側機器等に対する要求事項の追加:

- ERAB 制御対象のエネルギー機器や GW 等について、「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）以上を満たすことが求められるサービスレベルとして追加された。
- 将来的に★2（レベル2）以上の詳細要件が決定した場合、★2（レベル2）以上を満たすことが望ましいとされた。

5. サイバーセキュリティ対策の手順変更

●対策の手順が7ステップから9ステップに増加:

- Step4に「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」が追加。
- Step9に「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」が追加。

6. インターフェースごとの対策強化 (R1-R6共通)

●外部システムとの相互接続点における対策強化（勧告事項）：

➢Ver.2.0 での認証、通信メッセージの暗号化に加え、

- 「ホワイトリスト等を用いた通信先の制限」が追加。
- 「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」が追加。

7. インターフェースごとの対策強化 (R4, R5, R6)

- **プロトコルに関する要求事項の追加:**
  - R4、R5（推奨）、R6 インターフェースについて、「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」が追加。
- **IoT製品導入時の要求事項の追加:**
  - R4、R5（推奨）、R6 インターフェースにおいて、新たに IoT 製品を導入する場合、JC-STAR ★1（レベル1）以上を満たす製品を選択することが追加。

8. 取扱情報の差異や動作環境の差異によるシステム設計への考慮 (クラウドサービスの追加)

●システム設計における考慮事項の拡大:

- ➢Ver.2.0 では取扱情報の差異（センサーデータ vs. 個人情報）に応じた設計に言及。
- ➢Ver.3.0 ではこれに加え、「クラウドサービスを活用したシステム構築・運用に関する考慮事項」が追加された。
- ➢クラウドサービスの適合性確認、「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）」参照、強固な認証基盤の利用、管理用端末の制限等が勧告または言及されている。

9. 監視・対応体制等の強化

●監視・対応体制に関する勧告事項の追加・強化:

- ➢「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」が追加。
- ➢「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」が追加。
- ➢「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」が追加。
- ➢「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」が追加。
- ➢ERAB制御対象のエネルギー機器や GW が外部とも相互アクセス可能であるという認識に基づき、監視・対応体制等を検討することが明確化。

本資料に関するお問い合わせ

ナオサイバーテック株式会社

e-mail: info@naocybertech.jp
URL: https://www.naocybertech.jp/