黄色ハイライト箇所が、パブリックコメント後の改定点

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）
（パブリックコメント後）

策定　平成 29 年 4 月 26 日

改定　平成 29 年 11 月 29 日

改定　令和元年 12 月 27 日

改定　令和●年●月●日

資源エネルギー庁
独立行政法人情報処理推進機構[IPA]

目次

1. はじめに 3
2. ガイドラインの位置づけ 6
3. ERAB システム 6
3.1. ERAB システムの構成 6
3.2. ERAB システムが留意すべき基本方針 8
3.3. ERAB システムが想定すべき脅威 8
3.4. ERAB システムが維持すべきサービスレベル 9
3.5. ERAB システムにおけるシステム重要度の分類 10
3.6. ERAB システムにおけるサイバーセキュリティ対策 11
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） 12
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又はリソースアグリゲーター間のインターフェース） 12
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） 13
3.6.4. R4（リソースアグリゲーターと GW 又は 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） 13
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） 14
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） 15
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 15
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 16
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 17
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 17
3.8. 標準対策要件に基づく詳細対策要件の設計 18
3.9. ガイドラインの継続的改善 19
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 20
4.1. ERAB に参画する各事業者による PDCA サイクルを用いた継続的なセキュリティ対策の実施 20
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 20
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 21
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 21
4.1.4. 各事業者における監視・対応体制等 21

1. はじめに

東日本大震災以降、分散型・需要家側エネルギーリソース（太陽光発電、定置用蓄電池、電気自動車、ヒートポンプ給湯機、家庭用燃料電池等）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。

電力システム改革やIoTの発展を踏まえ、アグリゲーションビジネスを新たなエネルギー産業として育成していくことは、分散型・需要家側エネルギーリソースを全体のエネルギーシステムの中で効果的に活用していくためにも重要な課題である。

また、平成27年11月26日の“未来投資に向けた官民対話”の場において、家庭の太陽光発電やIoTを活用し、節電した電力量を売買できる「ネガワット取引市場」を、平成29年までに創設し、そのために、平成28年度中に、事業者間の取引ルールを策定し、エネルギー機器を遠隔制御するための通信規格を整備する、という総理指示が出された。

それらを受けて、我が国においては、IoTを活用して需要家等の機器を統合することで、あたかも一つの発電所（仮想発電所:Virtual Power Plant）のように機能させ、市場取引や相対取引を通じて、系統の調整力としても活用できるようにする、ERABの実現が目指されている。

ERABでは、アグリゲーターが中核的な役割を担い、送配電事業者、小売電気事業者、BEMSやHEMS等を運用するエネルギーマネジメント事業者、需要家、再エネ発電事業者等、多様な受け手との相互接続を通して、様々なサービスが行われることが考えられる。

また、送配電事業者や小売電気事業者は、アグリゲーターに依頼して、需要家等の創エネルギー機器・設備、蓄エネルギー機器・設備、エネルギー消費機器・設備等（以下「ERAB 制御対象のエネルギー機器」という。）を、ネガワット取引や上げ DR のような新たな電力取引形態に対応した形式で最適遠隔制御できるようになる。そのために必要な基盤が ERAB システムと言える。

ERAB システムにおいては、多様なシステムがインターネットなど公衆網や VPN、専用線など多様な品質のネットワークを介して相互接続することで運用される。特に、これまで各需要家内等でしか活用されていなかったエネルギー機器が外部のシステム・ネットワークに繋がる点は大きな特徴である。

このような中、いずれかの事業者のサイバーセキュリティ対策が脆弱であった場合、需要家の電気の利用に影響を及ぼすことが懸念されるため、資源エネルギー庁では、ERAB の中でも特にサイバーセキュリティのあり方に焦点を当てて検討する ERAB 検討会の下部組織「サイバーセキュリティ WG」を設置した。

サイバーセキュリティ WG は、検討に際して、アグリゲーターが ERAB の主なサービスモデルから得られる付加価値と付加価値創造のプロセスで発生する脅威・リスクの比較を行い、以下 4 点を整理した。

第一に、ERAB システムはサイバー・フィジカル・システムであり、電力システムを運用する機器の物理的及び電気的特性と、その機器のサイバーによる制御を組み合わせたものである。サイバー・フィジカル・システムにおけるサイバーセキュリティの対策要件は、一般的な IT システムと大きく異なり、情報の保護だけでなく、物理システムが動作し続けるためのレジリエンスも確保する必要がある。サイバー・

フィジカル・システムに対して、経済産業省は「サイバー・フィジカル・セキュリティ対策フレームワーク」[1]を策定し、サプライチェーン全体の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「三層構造」のアプローチにより整理した上で、バリュークリエーションプロセスを構成する要素である、ソシキ、ヒト、モノ、データ、プロシージャ、システムの６つの構成要素におけるリスク源に対してセキュリティ対策を講じることを求めている。

- 第 3 層（サイバー空間におけるつながり）：データの信頼性を確保
- 第 2 層（フィジカル空間とサイバー空間のつながり）：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
- 第 1 層（企業間のつながり）：適切なマネジメントを基盤に各主体の信頼性を確保

第二に、ERAB において想定される脅威・リスクは、各アグリゲーターが取り得るサービスモデルによって種類や発生可能性等が大きく異なり、ERAB に参画する各事業者（具体的には、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、エネルギーマネジメント事業者（再生可能エネルギー発電事業者、需要家に設置される機器・設備メーカーを指す））が独自に脅威・リスクの評価を適切に実施することが必要である。小売電気事業者が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の役割に該当するサービスまで提供するようなモデルも考えられるが、こうした場合は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の立場からも脅威・リスクを評価する必要がある。

第三に、ERAB 全体への影響とその発生頻度という判断基準で対処優先順位が高いと判断される対策に対して、ERAB に参画する各事業者間で共有することが必要である。

第四に、セキュリティ対策の検討においては、IoT 推進コンソーシアム、経済産業省、総務省が共同で取りまとめた「IoT セキュリティガイドライン ver1.0」[2]等の他の類似の取組と十分に同期した取組とすることが、対策の実効性を強化する上で重要である。

平成 29 年 4 月 26 日、ERAB に参画する各事業者が取り組むべき標準対策要件を記載することを目的に「ERAB に関するサイバーセキュリティガイドライン Ver1.0」を策定した。その後、送配電事業者から発動指令を受けることを想定した、ERAB システムにおけるサイバーセキュリティ対策を追加するため、平成 29 年 11 月 29 日、「ERAB に関するサイバーセキュリティガイドライン Ver1.1」に改定した。

令和元年 12 月 27 日には、送配電事業者のシステム（簡易指令システム）に対して、アグリゲーションコーディネーターやリソースアグリゲーターのシステムが接続[3]されることを想定した、ERAB システムや ERAB に参画する各事業者に求められるサイバーセキュリティ対策を追加するため、「ERAB に関するサイバーセキュリティガイドライン Ver2.0」に改定した。

---

[1] https://www.meti.go.jp/policy/netsecurity/wg1/CPSF_ver1.0.pdf
[2] IoT 推進コンソーシアム　総務省　経済産業省『IoT セキュリティガイドライン ver1.0』、平成 28 年 7 月 IoT 推進コンソーシアム　IoT セキュリティワーキンググループ公表資料
[3] 送配電事業者のシステムと相互接続されるのは、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である。

また、前回改定時からの変化として、需要家側のネットワーク環境に配置されたコントローラーだけではなく、複数のクラウド環境上のコントローラー経由で需要家が持つERAB制御対象のエネルギー機器と相互接続され、一つの ERAB システムを形成するユースケースがある。このユースケースにおいては、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ERAB制御対象のエネルギー機器が、複数の異なる事業者（例えば、リソースアグリゲーターと機器メーカー、リソースアグリゲーターと当該リソースアグリゲーターのシステムと連携してERAB制御を実現する他のリソースアグリゲーター）により遠隔制御される新しいユースケースが報告されている。加えて、ERAB に参画する各事業者のシステムとERAB制御対象のエネルギー機器との通信については、需要家側のネットワーク環境（需要家側ゲートウェイ（GW）[4]の内側）とクラウド環境等の需要家側のネットワーク環境の外側（需要家側GW の外側）との境界に位置する GW を介さずに、ERAB 制御対象のエネルギー機器と直接通信をしたり、需要家側のルーター経由で間接通信したりする等、これまでにはない新しいユースケースも報告されている。なお、需要家側のERAB制御対象のエネルギー機器を管理するコントローラーについては、これまでの需要家側 GW の内側に設置されるユースケースとは別に、需要家側 GW の外側に一部又は全部が設置される新しいユースケースも報告されている。

このような状況を踏まえ、新しいユースケースを対象とし、独立行政法人情報処理推進機構（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」[5]の考え方に基づいたリスクアセスメントを実施した結果、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）といった危険度の高いリスクが多数存在することが確認された。そこで、「サイバー・フィジカル・セキュリティ対策フレームワーク」の考え方に基づいたサイバーセキュリティ対策を検討し、経済合理性が認められる対策を抽出した。これらのセキュリティ対策は、ERAB 制御対象のエネルギー機器が十分なコンピューティングリソースを持たない場合が多く、またERAB制御対象のエネルギー機器や宅内ルーターを含め、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というサプライチェーン構成上の特徴があることから、ERABシステム全体でのセキュリティ設計をする必要性があることを確認できた。

以上を踏まえ、新たなユースケースに係るセキュリティ対策等を追加するため、「ERABに関するサイバーセキュリティガイドライン Ver3.0」に改定する。

[4] 日本電機工業会の HEMS の定義においてはサービス連携機能とコントローラー機能を有する。
[5] 情報処理推進機構［IPA］セキュリティセンター『制御システムのセキュリティリスク分析ガイド　第2版』、情報処理推進機構［IPA］

2. ガイドラインの位置づけ

本ガイドラインは、「電力制御システムセキュリティガイドライン」[6]、「IoT 開発におけるセキュリティ設計の手引き」[7]及び「サイバー・フィジカル・セキュリティ対策フレームワーク」の考え方に基づいた、ERAB のサービスレベルを維持するために、ERAB に参画する各事業者が実施すべき最低限のセキュリティ対策の要求事項である。従って ERAB に参画する各事業者は、本ガイドライン等を踏まえ、自らの責任においてセキュリティ対策を講ずることとなる。

本ガイドラインにおける用語において、勧告とは、本ガイドラインが ERAB に参画する各事業者がその実装を必須として義務付けられる内容と定義する。

一方、推奨とは、本ガイドラインがその実装を ERAB に参画する各事業者が各自の責任において、その実装を検討すべき内容と定義する。

3. ERAB システム

3.1. ERAB システムの構成

ERAB システムは、送配電事業者のシステム（簡易指令システム）、小売電気事業者のシステム、アグリゲーションコーディネーターのシステム、リソースアグリゲーターのシステム、HEMS・BEMS 等エネルギーマネジメントシステム[8]、需要家側のネットワーク環境とクラウド環境等の需要家側のネットワーク環境の外側との境界に位置する GW、コントローラー、ERAB 制御対象のエネルギー機器から構成されている。コントローラーについては、需要家側 GW の内側に位置する場合又は需要家側 GW の外側に位置する場合があり、需要家側 GW の外側に位置する場合においては、アグリゲーターが保有するコントローラーと機器メーカー等サードパーティが保有するコントローラーがある。

このモデルについて大別すると、以下に示す２種類のユースケースが存在する。

- 需要家側 GW とコントローラーの組合せにより、オンサイトの ERAB 制御対象のエネルギー機器からデータを収集し、アグリゲーターのシステムへと送信する。クラウドサービスを含むアグリゲーターのシステムでは、受信したデータに基づき、GW やコントローラーの管理、サービスの提供を行う。
- 需要家側 GW を介さずに、オンサイトの ERAB 制御対象のエネルギー機器から直接又は需要家側のルーター経由でデータを収集し、アグリゲーターのコントローラー又は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、アグリゲーターのシステムへと送信する。クラウドサービスを含むアグリゲーターのシステムでは、受信したデータに基づき、アグリゲーターのコントローラーや

[6] 日本電気協会情報専門部会『電力制御システムセキュリティガイドライン』、日本電気協会。日本電気技術規格委員会が定める「日本電気技術規格委員会規格（JESC 規格）」に該当する。（JESC: Japan Electrotechnical Standards and Codes Committee）

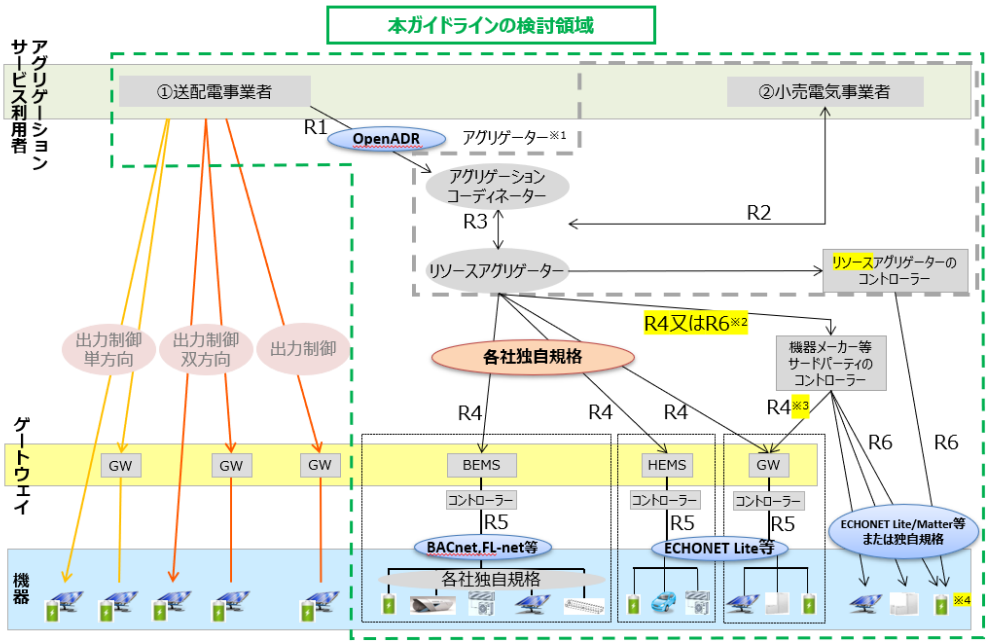
[7] 独立行政法人情報処理推進機構[IPA]技術本部セキュリティセンター『IoT 開発におけるセキュリティ設計の手引き』、情報処理推進機構[IPA]

[8] リソースアグリゲーターシステムと HEMS・BEMS 等エネルギーマネジメントシステムは一体形成される場合がある。

機器メーカー等サードパーティのコントローラー経由で、オンサイトの ERAB 制御対象のエネルギー機器の管理やサービスの提供を行う。

図 1 は、ERAB システムの構成機器とインターフェースを示している。インターフェースは、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（R1)、小売電気事業者とアグリゲーションコーディネーター又はリソースアグリゲーター間（R2)、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(R3)、リソースアグリゲーターと GW 又は BEMS・HEMS 等エネルギーマネジメントシステム間(R4)、需要家側に設置される GW と 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（R5)、リソースアグリゲーターが、需要家側 GW の外側に配置されたアグリゲーターのコントローラーや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 ERAB 制御対象のエネルギー機器と通信する、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（R6）である。

R4 については、GW と ERAB システムが直接接続するユースケースに加えて、HEMS、BEMS 等の EMS を介して ERAB システムに接続されるユースケースも考えられる。なお、R4 の接続点は、エネルギーマネジメントシステムのサービス連携機能がサーバー上に設置される場合と ERAB 制御対象のエネルギー機器が置かれた HAN(Home Area Network)内に設置される場合があることが日本電機工業会において定義されている[9]。



※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　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 GW と通信する場合は R4、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 ERAB 制御対象のエネルギー機器と通信する場合は R6 となる。

※3　HEMS や BEMS と連携することも考えられる。

※4　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。

図 1　ERAB システムにおける全体図

[9] 日本電機工業会 HEMS 専門委員会「外部システムとの連携における HEMS の定義」平成 28 年 9 月 14 日 ERAB 検討会提示資料

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[10]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[11]。

【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[12]に留意したシステム設計を行うこと。

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。

インターフェース R5 の機器としては、ERAB 制御対象のエネルギー機器に加えてセンサが想定される。例えば、需要家側のネットワーク環境とその外側との境界に位置する GW を介してその配下に位置する ERAB 制御対象のエネルギー機器やセンサと直接通信するユースケース、BEMS・HEMS のコントローラーを経由して間接通信するユースケースが報告されている。また、これらのユースケースにおいては、以下の脅威が論じられているが、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 のコントローラー、エンドポイントに位

[10] 通知方法に関しては ERAB に参画する各事業者の詳細対策要件に基づくものとする。

[11] 独立行政法人情報処理推進機構[IPA]は、IoT システムのものを含む脆弱性対策情報をデータベースとその利用機能（例えば製品名やバージョンで該当する脆弱性を全て検索する機能等）を合わせて、脆弱性対策情報データベース JVN iPedia （https://jvndb.jvn.jp/）として一般公開しており、脆弱性情報周知を図る手段の一つとして ERAB 事業に参画する各事業者による活用が可能である。

[12] 内閣サイバーセキュリティセンター「安全な IoT システムのためのセキュリティに関する一般的枠組み（平成 28 年 8 月 26 日)」においては、機密性、完全性、可用性、安全性の各項目を確保することと記載されている。本ガイドラインは、その基本方針に準拠している。

置する ERAB 制御対象のエネルギー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。

- ERAB 制御対象の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。
- ERAB 制御対象の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 ERAB 制御対象のエネルギー機器やセンサから 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 ERAB 制御対象のエネルギー機器やセンサを乗っ取り、GW 経由の需要家側のネットワーク環境の外部システムへの DoS 攻撃へ加担させる。
- ERAB 制御対象のエネルギー機器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。

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の管理に留意すること。

その際、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[13]
- 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[14]、加えて簡易指令システムとの直接的な接続部[15]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[16]、加えて、アグリゲーションコーディネータ

[13] 第 9 回 ERAB 検討会『サイバーセキュリティ WG 報告』、資源エネルギー庁 2019 年
[14] 脚注 13 と同じ
[15] アグリゲーションコーディネーターは、同システムにおいて、「簡易指令システムとの直接的な接続部」と「そうでない部分」を論理的もしくは物理的に分離設計することができる。分離設計が困難な場合は、アグリゲーションコーディネーターの全システムは、「電力制御システムセキュリティガイドライン」へ準拠することが必須とされ、「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の確保が必須とされる。
[16] 脚注 13 と同じ

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)」[17]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。）

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。ERAB に参画する各事業者は、自らのシステムを以下に基づき、分類すること。

「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。

重要度ごとの対象システム

重要度	対象システム
A	制御対象の需要規模が 50 万 kW 以上のシステム
B	制御対象の需要規模が 50 万 kW 未満のシステム

[17] 『セキュリティ要件適合評価及びラベリング制度（JC-STAR)』は、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制度であり、求められるセキュリティ水準に応じた４つの適合基準が定められている。このうち、IoT 製品共通の最低限の脅威に対応するための適合基準である★１（レベル１）については、独立行政法人情報処理推進機構［IPA］により 2025 年 3 月から制度運用が開始される。また、★２（レベル２）以上についても詳細要件が決まり次第、制度運用が開始される計画である。

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：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）[18]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。

・ 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[19]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、

[18] 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）を参照してベストプラクティスを導出する一助になる。

[19] 確認方法に関しては、各々の事業者が詳細対策要件に基づき相対による確認を行う。なお、係争時の対処方法に関しては、継続協議とする。

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】

本ガイドラインは、既述のシステムセキュリティにおける一般的な対応に加え、ERAB システムにおけるインターフェース別に、3.6.1.項から 3.6.6.項の対応を求める。

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】

（事業者とその保有するシステムの対策）

- 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当たり、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。
- アグリゲーションコーディネーターのシステムと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」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。

（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。
- アグリゲーションコーディネーターのシステムと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。
- アグリゲーションコーディネーターのシステムと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を最小化し、接続点に防御措置を講じること。
- 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。

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又はリソースアグリゲ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。
- アグリゲーションコーディネーター又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[20]。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

[20] 脚注 13 と同じ

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。

・ 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。

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）

【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[21]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。

（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。

・ 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。

3.6.4. R4（リソースアグリゲーターとGW又は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[22]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等のシステムとGW間の通信路[23]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、BEMS・HEMS等のシステムとGW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

[21] 脚注13と同じ
[22] 脚注13と同じ
[23] 日本電機工業会のHEMSの定義においては、アグリゲーターとエネルギーマネジメントシステムのサービス連携機能間の通信路及びエネルギーマネジメントシステムのサービス連携機能（サーバー上にある場合）とEMSコントローラー機能間の通信路となる。

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。

（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。

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[24]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」[25]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、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。

[24] 具体的には「外部ネットワークと内部ネットワークの境界に位置する GW とエンドポイントに位置する機器やセンサ」や「(GW よりエンドポイント側に位置する、又は GW 機能を有する)BEMS・HEMS コントローラーとその配下の機器やセンサの間」。

[25] IPA 技術本部セキュリティセンター『IoT 開発におけるセキュリティ設計の手引き』、情報処理推進機構［IPA］

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[26]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。

（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。

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。

[26] 脚注 13 と同じ

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について、クラウドサービスごと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。

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】

・ 保有するデータを盗聴・改ざんされるという脅威・リスクへの対策が必要となる。個人情報に該当しない情報については、その適切な管理について、法律上明示的な義務は課されていない。しかし、内閣サイバーセキュリティセンター「安全な IoT システムのためのセキュリティに関する一般的枠組」に鑑みれば、個人情報に該当しない情報であっても、事業者がその保有する情報を適切に管理しなければならないことは当然であると考えられる。同枠組みにおいては、IoT システム及び IoT システム間の接続に係るセキュリティ確保のために、基本方針の設定、リスク評価、システム設計、システム構築、運用・保守の各段階で求められる要件を定義することが必要であり、以下の項目を明確化すること。
  - 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。
  - 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。
  - 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。
  - 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。

・ 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。
・ 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。
・ 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[27]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。また、個人情報の適切な管理に関するサービスレベルを維持するために事業者が実施すべき具体的な対策については、個人情報保護法に基づき個人情報保護委員会が定める[28]「個人情報の保護に関する法律についてのガイドライン（通則編）」他３編[29]や、「個人データの漏えい等の事案が発生した場合等の対応について」が存在する。ERAB に参画する各事業者は、「個人情報の保護に関する法律についてのガイドライン（通則編）」他３編や「個人データの漏えい等の事案が発生した場合等の対応について」に基づく対策を実施するとともに、各種ガイドライン等を参照しつつ、自主的に必要な対策を実施すること。

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）」[30]等を参照した対策をとること。

[27] 個人情報保護法第 20 条に規定
[28] 個人情報保護法第 8 条に規定
[29] 他３編とは、「外国にある第三者への提供編」、「第三者提供時の確認・記録義務編」、「匿名加工情報編」の３つを指す。
[30] 内閣官房内閣サイバーセキュリティセンター 重要インフラグループ『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）』、内閣官房内閣サイバーセキュリティセンター

・ 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。

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ごとに想定される脅威、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等、構成要素ごと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。

なお、詳細対策要件の設計においては、本ガイドラインに加え、独立行政法人情報処理推進機構[IPA]技術本部セキュリティセンターが発表する「IoT 開発におけるセキュリティ設計の手引き」[31]や日本電気技術規格委員会[JESC]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」、経済産業省が制定する「サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）」を前提とする。

[31] IPA 技術本部セキュリティセンター『IoT 開発におけるセキュリティ設計の手引き』、情報処理推進機構[IPA]

表１　標準対策要件と詳細対策要件

標準対策要件 ※本ガイドラインに相当	・ 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つつ、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・考え方等を規定したもの。 ・ 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規定したもの。
詳細対策要件	・ ERAB に参加する各事業者が、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規定したもの。 ・ 具体的には、ERAB システムの構成要素ごとに想定される脅威、当該脅威と事業リスクとの相関関係を踏まえつつ、（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､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を規定したもの。

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。
・ 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。

本ガイドライン（標準対策要件）と詳細対策要件は、社会変容、セキュリティインシデントの発生等に応じて、継続的にその内容を更新し、ERAB に参画する各事業者において最終的に求められる対策レベルに近づけていくことが重要である。

特に､詳細対策要件は､標準対策要件の考え方に沿って行われる具体的な対策例を規定するものであることから、一般的なセキュリティマネジメント要求事項等を規定した標準対策要件と比較して、その更新が求められる頻度は高いと考えられる。標準対策要件及び詳細対策要件の更新の頻度については、一義的には更新の主体となる事業者において判断されるべきものであるが、少なくとも詳細対策要件については、定期的にその内容が点検・更新されることが求められる。なお、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されることが求められる。

また､標準対策要件と詳細対策要件は相互に連携するものであるため､一方の見直しが行われた際に､他方の見直しが必要になると判断される場合は適切に対処することが重要である。

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サイクルを用いた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。
- ERABに参画する各事業者は、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、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。
- ERABに参画する各事業者は、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。
- ERABに参画する各事業者は、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。
- ERABに参画する各事業者は、セキュリティに関連する情報を文書化し、管理すること。
- ERABに参画する各事業者は、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。
- ERABに参画する各事業者は、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。
- 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。
- ERABに参画する各事業者は、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。

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。

ERABに参画する各事業者がERABシステムに関するセキュリティ対策を設定するに際しては、事業者ごとに発生するリスク、許容できるリスクが異なると考えられることから、経営上のリスクを適切に評価した上で、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が求められる。

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。

ERABに参画する各事業者においては、自社が設定したセキュリティ対策を踏まえたERABシステムの構築を行うとともに、セキュリティ対策の実施状況の評価、セキュリティ対策の有効性の評価を行うことにより、自社のセキュリティ対策の改善を図る。

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。

「3.5.ERABシステムにおけるシステム重要度の分類」において「重要度A」に分類されるシステムは、そのシステムの電力安定供給等に与える影響を鑑み、第三者認証の実施が強く推奨される。

ERABに参画する各事業者が「4.1.ERABに参画する各事業者によるPDCAサイクルを用いた継続的なセキュリティ対策の実施」で示されたPDCAサイクルに基づき、セキュリティ対策の実施や改善を実施する際、国際標準[32]は参考となる。

本ガイドラインセキュリティ対策の実施状況の評価については、内部監査の実施することが望ましい。セキュリティ対策の有効性の評価については、内部監査に加え、国際標準[33]に準じた第三者による外部監査を受けることが望ましい。外部の組織による監査等を実施することで、セキュリティ対策の継続的改善の効果をより一層高めることが期待できる。

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。

※独立行政法人情報処理推進機構[IPA]は、IoTシステムにおける脆弱性対策情報をデータベースとその利用機能(例えば製品名やバージョンで該当する脆弱性を全て検索する機能等)を合わせて、脆弱性対策情報データベース JVN iPedia[34]として一般公開しており、脆弱性情報の周知を図る手

[32] 国際標準の例：CC (ISO/IEC 15408)、CSMS (IEC 62443-2)、ISMS (ISO/IEC 27001)、クラウド利用におけるISO/IEC 27017等

[33] 脚注3232と同じ

[34] https://jvndb.jvn.jp/

段の一つとしてERABに参画する各事業者による活用が可能である。

- 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。
  ※管理体制の構築の際には、スマートメーターシステムにおけるセキュリティ運用体制の例（表２）が参考となる。
- 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。
- 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。
- 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。
- 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、外部とも接続している需要家のネットワーク上の機器経由で需要家のネットワーク上の他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。

【推奨】

- 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。

表２　スマートメーターシステムにおけるセキュリティ運用体制の例（参考）[35]

機能名	平時の対応	有事の対応
セキュリティ統括	① 社内全体のセキュリティに関する取組の統括（リスク評価、ペネトレーションテスト等の計画・実施・管理） ② 経営層、関係各部へのセキュリティに関する情報の提供	① 経営層、関係各部へのセキュリティ事故に関する情報の提供 ② 行政機関等の外部への説明、社内の広報部門への情報提供
セキュリティ事故対応	① 有事の際の対応計画の策定、訓練の実施 ② 攻撃情報の提供、受領、分析 ③ セキュリティに関するログの横断的分析等の実施	① インシデントへの二次対応・応援 ② （必要に応じ）インシデント調査に係る外部リソースの調達 ③ インシデントの分析・報告書の作成
セキュリティ監視	① 運用監視機能への作業指示、作業結果管理 ② セキュリティに関するログの定型分析	① 運用監視機能からの連絡によるインシデントへの一次対応 ② インシデントに伴う、運用監視機能への緊急作業指示、作業結果管理
運用監視	① システムの監視（性能監視、死活監視、イベント監視等） ② インシデント検知時のセキュリティ監視への連絡 ③ 通常システムの運用業務	① セキュリティ監視機能からの指示に基づく対応作業の実施 ② （必要に応じ）事故対応で必要となるログの収集

[35] スマートメーター制度検討会セキュリティ検討ワーキンググループ報告書 別添「統一的なガイドラインの標準対策要件に盛り込むべき事項」をもとに記載。