資料 6-2

10/4 ERAB 検討会時点

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 Ver1.3（原案）

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 xx 月 xx 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 4
2. ガイドラインの位置づけ 5
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 7
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 8
3.5. ERAB システムにおけるシステム重要度の分類 9
3.6. ERAB システムにおけるサイバーセキュリティ対策 10
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） 11
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） 11
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） 12
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） 12
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） 12
3.7. 取り扱い情報の差異による ERAB システムの分類 13
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 13
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 14
3.8. 標準対策要件に基づく詳細対策要件の設計 14
3.9. ガイドラインの継続的改善 15
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 16
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 16
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 17
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 17

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 17
4.1.4. 各事業者における監視・対応体制等..... 18

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、エネファーム、ネガワット等）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・需要家側デバイ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、エネルギー・リソース・アグリゲーション・ビジネス（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、再エネ発電事業者など、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、負荷機器・設備等を、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のシステムといえる。

ERABの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や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、これまで各需要家等内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ために、ERAB検討会の下部組織として「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・リスク比較を行い、以下4点の結論を得た。

第一に、ERABの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」のアプローチを提案している。

- 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採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、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、小売電気事業者、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（平成28年7月）」等の他の類似の取り組みと十分に同期した取り組みとすることが、対策の実効性を強化する。

その結果、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」を平成29年4月26日に策定した。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て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日に「ERABに関するサイバーセキュリティガイドライン Ver1.1」を改訂した。

今般、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することを想定して、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　Ver1.2」に改訂する。

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[2]」及び「IoT開発におけるセキュリ

[1] https://www.meti.go.jp/press/2019/04/20190418002/20190418002-2.pdf
[2] 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、2016年。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

ティ設計の手引き[3]」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。なお、本ガイドラインは法令等に明示的に位置付けることは行わない。

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[4]、エネルギー機器と外部システムとのゲートウェイ（GW)、ERAB 制御対象のエネルギー機器から構成される。

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。このモデルでは、GW とコントローラの組み合わせにより、オンサイトの機器からデータを収集し、ヘッドエンドシステムへと送信する。クラウドサービスを含むヘッドエンドシステムでは、受信したデータに基づき GW 及びコントローラの管理やサービスの提供を行う。また、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また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 または BEMS・HEMS 等エネルギーマネジメントシステム間（R4）である。

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する場合と ERAB 制御対象のエネルギー機器が置かれた HAN(Home Area Network)内に設置す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[5]。

さらに、需要家側に設置される ERAB 制御対象のエネルギー機器は、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(R5)を持つ。これらのエネルギー機器は、GW[6]を介して ERAB システムに直接接続するユースケースと HEMS コントローラ等の EMS コントローラを介して ERAB システムに接続されるユースケースが考えられる。

Electrotechnical Standards and Codes Committee)

[3] 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]、2016 年

[4] 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

[5]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

[6]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機能を有する。

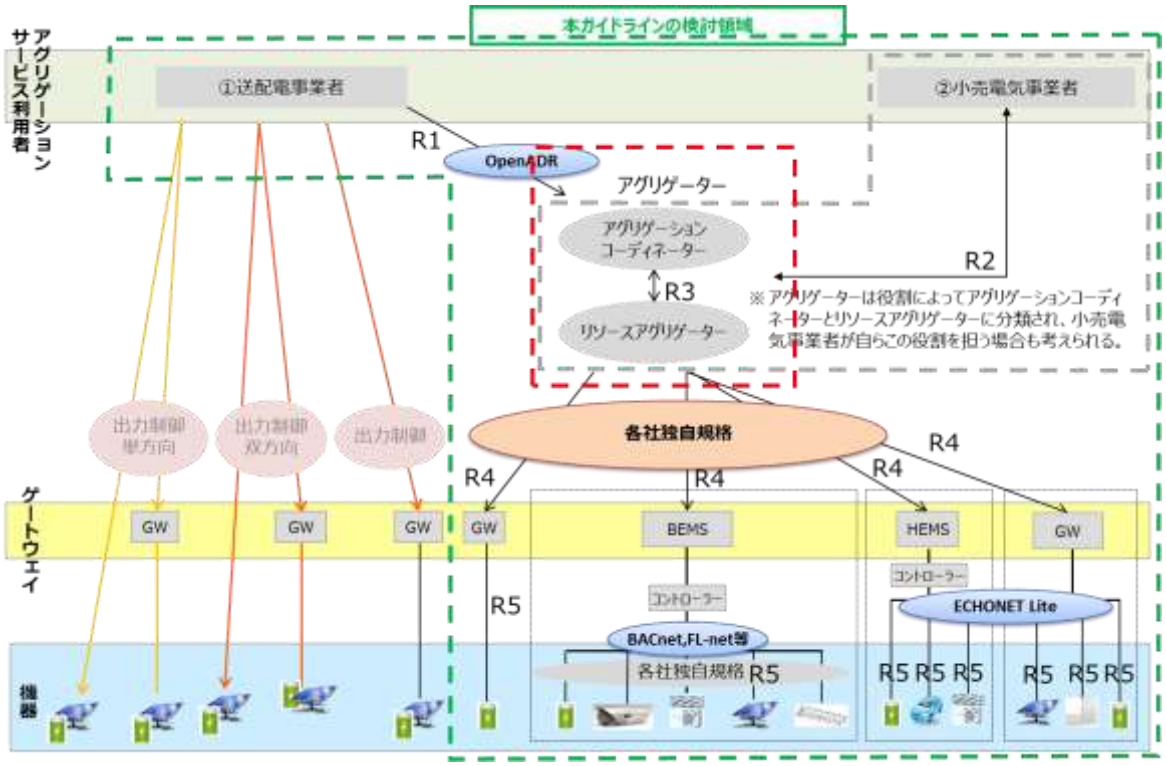

図１　ERAB システムにおける全体図

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[7]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[8]。

【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[9]に留意したシステム設計を行うこと

[7] 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。

[8] 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

[9]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

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検討を進めることが必要である。

- 標的型攻撃も想定すること。
- 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必要があること

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。例えば、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 を介してその配下に位置する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 コントローラ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、その脅威に対応をするため、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。その結果として 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管理に留意することが求められる。

その際、各事業者及びその保有システムは以下の定義でのサービスレベル確保が求められる。

- 容量市場、需給調整市場等における要求事項
- 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[10]
- 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

[10]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

レベル[11]、加えて簡易指令システムとの直接的な接続部[12]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」への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[13]、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

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、それぞれ次に定めることころによる。ERAB に参画する各事業者は、自らのシステムを以下の分類に従って分類すること。

「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。

[11]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

[12] 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出来る。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」への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。

[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

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

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が求められる。

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。

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。【脅威分析】

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。【対策検討】

Step4：脅威に対抗する対策の候補（ベストプラクティス）の明確化。

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の選定。

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。

Step7：事故発生時の対応方法を設計・運用及び訓練。

・ 相互接続の中止

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[14]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。

・ なりすまし対策

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・リスクが想定される。

・ データ等の改ざん対策

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・リスクが想定される。

・ マルウェアへの対策

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が求められる。システムにおける管理者権限の割当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。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が求められる。

14 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。尚、係争時の対処方法に関しては、継続協議とする。

本ガイドラインは、上記の IoT システムの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以下の対応を求める。

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。
- 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[15]は、「電力制御システムセキュリティガイドライン」への準拠、「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）

- 相互認証、通信の暗号化により保護すること
- 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
- 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[16]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簡易指令システムとの直接的な接続部[17]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。

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）

【勧告】

（インターフェースの対策）

- 相互認証、通信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へ準拠することを求めること[18]。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。

---

[15]脚注 12 と同じ
[16]脚注 14 と同じ
[17]脚注 14 と同じ
[18]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

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、本ガイドラインへの準拠することが必須とされる[19]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）

・ 相互認証、通信の暗号化により保護すること。

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）

・ 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、本ガイドラインへの準拠することが必須とされる[20]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、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、BEMS・HEMS等のサーバーとGW間の通信路[21]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、上記の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。

（インターフェースの対策）

・ 相互認証、通信の暗号化により保護すること。

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[22]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）

---

[19] 脚注18と同じ

[20] 脚注19と同じ

[21] 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コントローラ機能間の通信路となる。

[22] 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、またはGW機能を有する)BEMS・HEMSコントローラとその配下の機器やセンサの間」

・ ERAB 制御対象のエネルギー機器、センサには、リソース制約が存在する機器が存在し、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」[23]、「製品分野別セキュリティガイドライン IoT-GW 編」[24]等を参照した対策が必要である。

（インターフェースの対策）

・ 相互認証、通信の暗号化により保護すること。

3.7. 取り扱い情報の差異による ERAB システムの設計

【勧告】

・ ERAB に参画する各事業者は、取り扱い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あ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。

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

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（平成 28 年 8 月 26 日公表）」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の要件として、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、以下の項目の明確化を必要としている。

a) 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。

b) 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

[23] 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]、2016 年

[24] CCDS セキュリティガイドライン WG ホーム GW SWG『製品分野別セキュリティガイドライン IoT-GW 編』重要生活機器連携セキュリティ協議会[CCDS]、2017 年

する安全確保に必要な要件を明確化する。

c) 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。

d) 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。

e) 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。

f) 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。

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

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、個人情報保護法に依拠した対策が必要となる。

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[25]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[26]「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[27]（平成 28 年 11 月（平成 29 年 3 月一部改正）、個人情報保護委員会）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」（平成 29 年個人情報保護委員会告示第１号）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、統一的な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となる。

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

[25] 個人情報保護法第 20 条に規定
[26] 個人情報保護法第 8 条に規定
[27] 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。

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毎に想定される脅威、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など、構成要素毎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、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」[28]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」を前提とする。

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毎に想定される脅威、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。

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。

[28] 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]、2016

・ 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機関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・更新されることが勧告される。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勧告される。

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。

また、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践する。

・ 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
・ 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
・ セキュリティに関連する情報を文書化し、管理する
・ 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
・ 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。またセキュリティ教育・訓練の効果についても確認する

なお、その前提として、ERAB に参画する各事業者においては、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。他方、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。

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、事業者毎にその発生するリスク、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。

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

「2.5.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サイクルによる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[29]の活用は役立つ。

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、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[30]に準じた第三者による外部監査を受けること。これは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からである。

[29] 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

[30] 脚注29と同じ

4.1.4. 各事業者における監視・対応体制等

【勧告】

- 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[31]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 に参画する各事業者による活用が可能である。
- ERAB に参画する各事業者においては、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。
- ERAB に参画する各事業者においては、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すること。
- インシデントへの対応については、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。

【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。
- 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。
- 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。

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）[32]

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	① インシデントへの二次対応・応援

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

[32] 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

	③ セキュリティに関するログの横断的分析等の実施	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