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
Ver1.1

策定　平成 29 年　4 月 26 日

改定　平成 29 年 11 月 29 日

資源エネルギー庁
独立行政法人情報処理推進機構[IPA]

目次構成

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、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、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、エネルギー・リソース・アグリゲーション・ビジネス（以下、「ERAB」という。）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 3 点の結論を得た。

第一に、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。

第二に、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。

第三に、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。今般、送配電事業者システムとの連携に関する 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、「ERABに関するサイバーセキュリティガイドライン Ver1.1」に改訂する。

2. ガイドラインの背景と方向性等

2.1. ガイドラインの背景

ERABにおけるサイバーセキュリティ対策は、基本は ERABに参画する各事業者が取り組むべきものである。一方、ERAB システムは、送配電事業者から需要家保有のエネルギー機器までが繋がっており、いずれか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への懸念が存在する。他方で、ERAB に参画する各事業者にとって、サイバーセキュリティ対策にかかる費用負担が過重なものになれば、ERABの足かせになることが懸念される。

それらを踏まえ、ERABの黎明期においては、ERABの健全な育成・発展の促進ならびに ERABに関わるステークホルダーの便益の増進およびリスクの抑制に十分配慮しつつ、実現可能なサイバーセキュリティ対策を実装・運用することが不可欠である。

なお、ＥＲＡＢにおけるサイバーセキュリティ対策は、IoTセキュリティガイドラインのIoTセキュリティ対策の考え方を基本とする。

2.2. ERAB システムの構成

ERAB システムは、送配電事業者システム、小売電気事業者システム、リソースアグリゲーターシステム、HEMS・BEMS 等エネルギーマネジメントシステム、エネルギー機器から構成される。

また、インターフェースは、リソースアグリゲーターシステムと送配電事業者システム間（R1）、リソースアグリゲーターシステムと小売電気事業者システム間（R2）、リソースアグリゲーターシステム間(R3)、リソースアグリゲーターシステムとエネルギーマネジメントシステム【HEMS・BEMS 等】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 [1]。

一方、需要家側に設置される ERAB 制御対象のエネルギー機器は、インターフェース(R5)を持つ。エネルギー機器は、GW[2]を介してリソースアグリゲーターシステムに直接接続するケースと HEMS コントローラ等の EMS コントローラを介して R4 の接続点を介してリソースアグリゲーターシステムに接続されるケースがある。

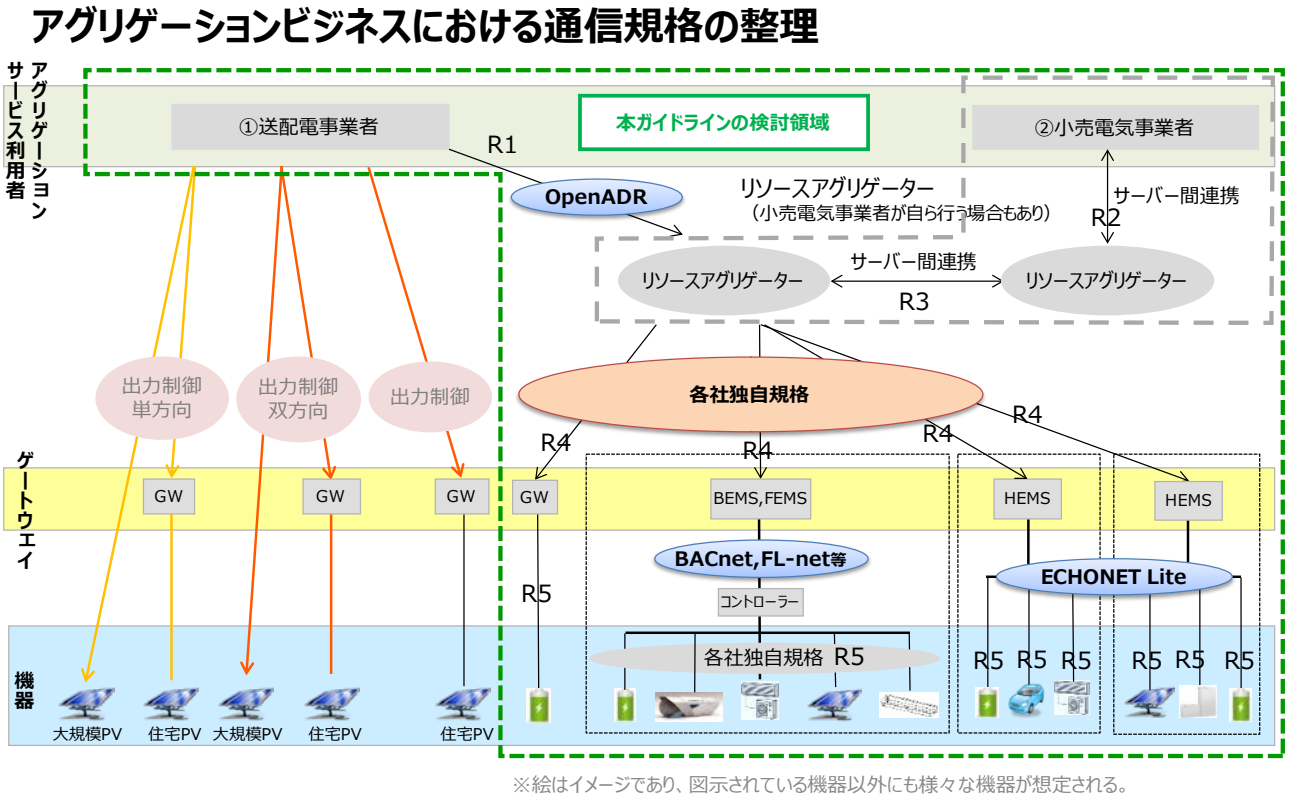

図 1　ERAB システムにおけるインターフェース

2.3. ERAB システムが想定すべき脅威

ERAB システムは、現在構築が進められているところであるため、現時点でその脅威を網羅的に想定することは容易ではないが、例えば以下の観点を前提として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
- 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

[1]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

[2]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。

必要があること

2.4. ERAB システムが維持すべきサービスレベル

ERAB システムは、特にリソースアグリゲーターが保有するシステムは、小売電気事業者や送配電事業者等の電力システムとの直接的な接続が予定される。その際、事業者は、電力システムのセキュリティ設計に準拠、連携した対策が必要となる。特に、アグリゲーターが送配電事業者と直接的に接続する場合には、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必要があり、アグリゲーターも適切なセキュリティ対策を検討する必要がある。今後、認定アグリゲーター要件等において、実装検討を深める。

3. ガイドラインの方向性

3.1. ガイドラインの位置付け

本ガイドラインは、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。なお、法令等に明示的に位置付けることは行わず、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、本ガイドラインにおける用語において、勧告とは、本ガイドラインがその実装を必須として義務付けるべきと定義することであり、推奨とは、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。

3.2. ERAB システムが留意すべき基本方針

- ERAB システムは、機密性、完全性、可用性の 3 要件 [3]に留意したシステム設計を行うこと（推奨）
- 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 [4]を行うこと（勧告）
- ERAB に参画する各事業者は、脆弱性情報が公知になった際に、悪用される危険性が高まるため、一斉に伝えられるようにしておくこと [5]（勧告）

---

[3]「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 日内閣サイバーセキュリティセンター編）」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

[4] 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。

[5] 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 （http://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

3.3. ERAB システムにおけるサイバーセキュリティ対策

ERAB システムでは、エネルギー機器に対するなりすましや改ざん、不正操作、ネットワークに対する盗聴や改ざん等といった想定される脅威・リスクの発現を防ぐための対策が求められる。

正しい事業者から正しい指令が発令されたことの認証と機器・システムへ正しい指令が送受信されることを担保することは ERAB システムの根幹であり、指令の真正性を阻害するような脅威・リスクについては、最大の脅威・リスクであると捉えることができる。

- なりすまし

  制御サーバーが、悪意を持った攻撃者によってなりすまされ、そこから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。

- 盗聴やデータ等の改ざん

  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。

そこで、本ガイドラインは、ERAB システムにおける各インターフェース別に対応を求める。

3.3.1.R1：送配電事業者とアグリゲーター間

- 相互認証、通信の暗号化により保護すること（勧告）
- 送配電事業者のシステム [6]への接続は特定されたアグリゲーターのシステムのみからの接続に限定すること（勧告）

※より多くのアグリゲーターの参画が見込まれる ERAB システムにおいては、特定できない相手からの、送配電事業者システムへの接続や、それを起因としたシステム障害、意図しないコントロール等を防ぐことが重要である。

3.3.2.R2～R3：各種制御サーバー間

- 相互認証、通信の暗号化により保護すること（勧告）

3.3.3.R4：アグリゲーターとエネルギーマネジメントシステム間

- 相互認証、通信の暗号化により保護すること（勧告）

※制御サーバーとコントローラ(ゲートウェイ)間の通信路 [7]として、公衆網が使われる場合を前提としている。

---

[6] 本項目で言う「送配電事業者のシステム」とは、バーチャルパワープラント構築実証事業等における簡易指令システムを指しており、簡易指令システムは、中央給電指令システムと独立し、相互に影響し合わないシステムであり、ネットワークについては物理的または論理的に分離されていることが前提となる。

[7] 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

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。

3.3.4.R5：コントローラと需要家側に設置される ERAB 制御対象のエネルギー機器間

・ コントローラ(ゲートウェイ)～需要家側に設置される ERAB 制御対象のエネルギー機器間を相互認証・通信の暗号化により保護すること（推奨）

コントローラ(ゲートウェイ)～需要家側に設置される ERAB 制御対象のエネルギー機器間は、リソース制約が存在する末端のエネルギー機器が存在し、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。これらの機器における相互認証と通信の暗号化によるサイバーセキュリティ対策は、機器間インターフェースの管理団体が定めたサイバーセキュリティ対策に準拠する等の方法による実装を推奨する。

3.4. 取り扱い情報の差異による ERAB システムの分類

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、「センサーデータを活用した 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。

3.4.1.センサーデータを活用した 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

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 システムおよび 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。

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。

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。

3.4.2.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

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[8]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[9]「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[10]（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。

3.5. 標準対策要件に基づく詳細対策要件の設計（勧告）

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

[8] 個人情報保護法第 20 条に規定

[9] 個人情報保護法第 8 条に規定

[10] 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。

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」[11]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（勧告）	・ 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

[11] http://www.ipa.go.jp/files/000052459.pdf

	物理攻撃の組合せによる攻撃への対策を規定

3.6. ガイドラインの継続的改善（推奨。一部勧告）

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・更新されることが推奨される。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（推奨）

ERAB に参画する各事業者は、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。

なお、その前提として、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。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（推奨）

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ことが推奨される。

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（推奨）

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ことが推奨される。

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 [12]に準じた第三者による外部監査を受けることが推奨される。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。

4.1.3.各事業者における監視・対応体制等（推奨）

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ことが推奨される。とりわけ、インシデント発生時には、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が推奨される。

また、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とともに継続的に訓練を実施することが推奨される。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が推奨される。

また、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・管理することが推奨される。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 （http://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 に参画する各事業者による活用が可能である。

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）[13]

機能名	平時の対応	有事の対応

[12]国際標準の例：CC（ISO/IEC 15408）、CSMS（IEC 62443-2）、ISMS（ISO/IEC 27001）等

[13] 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

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