「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）」に関する意見公募手続の結果について

令和 7 年 2 月 28 日
資源エネルギー庁
省エネルギー・新エネルギー部
新エネルギーシステム課

「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）」について、令和 6 年 12 月 25 日から令和 7 年 1 月 31 日まで意見公募手続を実施しました。

提出意見と提出意見に対する考え方については別紙のとおりです。

ご協力いただき、ありがとうございました。

１．実施期間

令和 6 年 12 月 25 日（水）～令和 7 年 1 月 31 日（金）

２．実施方法

電子政府の総合窓口「e-Gov」、郵送、電子メール

３．提出意見数（提出者数）

45 件（12 者）

※別紙では、同一の趣旨の意見をまとめて整理して示しているため、上記提出意見数と別紙の提出意見数は一致しません。

４．提出意見と提出意見に対する考え方

別紙のとおり

（別紙）

提出意見と提出意見に対する考え方

「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）」
に対する提出意見と提出意見に対する考え方は以下のとおりです。

| | 提出意見 | 提出意見に対する考え方 |
|---|---|---|
| 1 | ■該当箇所<br>・ガイドライン改定案　6 ページ<br>・3.1. ERAB システムの構成<br>「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」<br><br>■意見内容<br>同資料 P7 の図 1 で示される右端の R6 のルートを指しているという認識でよいか。 | ご理解のとおりです。 |
| 2 | ■該当箇所<br>・ガイドライン改定案　7 ページ<br>・3.1. ERAB システムの構成<br>「図１　ERAB システムにおける全体図」<br><br>■意見内容<br>「リソースアグリゲーター」と「アグリゲータのコントローラー」間、または「リソースアグリゲーター」と「機器メーカー等サードパーティのコントローラー」間の通信区分の記載が図の中にありませんが、何になりますでしょうか。ご記載いただきたく思います。 | 「リソースアグリゲーター」と「アグリゲーターのコントローラー」は、どちらもリソースアグリゲーターのシステム内にあることを想定しており、「リソースアグリゲーター」と「アグリゲーターのコントローラー」間は、事業者間のインターフェースとして定めておりません。明確化を図るため、「アグリゲーターのコントローラー」を「リソースアグリゲーターのコントローラー」と修正させていただきます。<br>「リソースアグリゲーター」と「機器メーカー等サードパーティのコントローラー」間については、「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「GW |

| | | |
|---|---|---|
| | ■理由<br>通信区分が分からない場合、どの通信区分の対策要件を適用すればよいか分からないためです。 | 又はBEMS・HEMS等エネルギーマネジメントシステム」と通信するR4に含まれる場合と「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R6に含まれる場合があります。明確化を図るため、図１の「リソースアグリゲーター」と「機器メーカー等サードパーティのコントローラー」間に「R4又はR6※2」、注釈として「※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。」を追記させていただきます。 |
| 3 | ■該当箇所<br>・ガイドライン改定案　7ページ<br>・3.1. ERABシステムの構成<br>「図１　ERABシステムにおける全体図」<br><br>■意見内容<br>R6 の範囲について、リソースアグリゲーター～機器メーカー等のコントローラの事も含めているという解釈で問題ないか。<br>可能であればR4、R5のGWの機能の詳細も教えて頂けないか。 | 「リソースアグリゲーター」と「機器メーカー等サードパーティのコントローラー」間については、「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「GW又はBEMS・HEMS等エネルギーマネジメントシステム」と通信するR4に含まれる場合と「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R6に含まれる場合があります。明確化を図るため、図１の「リソースアグリゲーター」と「機器メーカー等サードパーティのコントローラー」間に「R4又はR6※2」、注釈として「※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。」を追記させていただきます。 |

| | | |
|---|---|---|
| | | なお、「GW」については、物理的なネットワークの分界点を表しており、その機能は事業者ごとに異なるため、詳細についてお答えすることはできません。 |
| 4 | ■該当箇所<br>・ガイドライン改定案　7 ページ<br>・3.1. ERAB システムの構成<br>「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。」<br><br>■意見内容<br>R6 の通信経路で、①リソースアグリゲーター(RA)と要家側 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間、②各コントローラーと機器間で担当する事業者が異なり、責任分界点があるケースが想定される。<br>そこで、R6①と R6②のように明確に分けた定義をすることを以下のように提案する。<br>「現状の定義に下記を追加。RA と需要家側 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間を R6①、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と ERAB 制御対象のエネルギー機器間を R6②と定義する。」 | 本ガイドラインにおいて求める標準対策要件が同様の記載となることから、改定案の記載とさせていただきます。 |
| 5 | ■該当箇所<br>・ガイドライン改定案　7 ページ<br>・3.1. ERAB システムの構成<br>「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 | ご理解のとおりです。 |

| | | |
|---|---|---|
| | 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。」<br><br>■意見内容<br>R6 の対象となる「機器メーカー等サードパーティのコントローラー」は「蓄電池などの機器メーカーが管理するクラウドサービスで提供されるコントローラー」が含まれると理解してよいか？ | |
| 6 | ■該当箇所<br>・ガイドライン改定案　7 ページ<br>・3.1. ERAB システムの構成<br>「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。」<br><br>■意見内容<br>「機器メーカー等サードパーティのコントローラー」としてクラウド側の HEMS のサービス連携機能を介して宅内の GW と接続される場合には、RA と機器メーカー等サードパーティのコントローラー間については、R4 の対象との理解で良いか？ | 「リソースアグリゲーター」と「機器メーカー等サードパーティのコントローラー」間については、「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「GW 又は BEMS・HEMS 等エネルギーマネジメントシステム」と通信する R4 に含まれる場合と「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 R6 に含まれる場合があります。「機器メーカー等サードパーティのコントローラー」と「GW」間は、R4 となります。明確化を図るため、図１の「リソースアグリゲーター」と「機器メーカー等サードパーティのコントローラー」間に「R4 又は R6※2」、注釈として「※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。」を追記させていただきます。 |
| 7 | ■該当箇所<br>・ガイドライン改定案　8 ページ<br>・3.2. ERAB システムが留意すべき基本方針 | リスクアセスメントの結果等を踏まえ、改定案の記載としています。<br>なお、具体的なサイバーセキュリティ対策は、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 |

| | | |
|---|---|---|
| | 「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。」<br><br>■意見内容<br>対象となる利用者について、低圧においては機器メーカを対象とする、さらに電力値（10kW 以上など）で限定化するなど、絞り込みが必要ではないでしょうか。<br><br>■理由<br>理由として、低圧の一般家庭のお客さまは通知を受け取っても、対応できるお客さまは少ないのが実態と考えると、機器メーカへの通知の方が効果的であり、なおかつ、低圧の利用者を含めると膨大な数となり、対応することは現実的ではないと考えました。 | 件の考え方に基づき、自らの責任で策定することとしています。 |
| 8 | ■該当箇所<br>・ガイドライン改定案　8ページ<br>・3.2. ERABシステムが留意すべき基本方針<br>「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。」<br><br>■意見内容<br>具体的には、どのような通知をすればよいでしょうか。<br>例えば、利用者との契約締結時に同一ページの注釈10にある脆弱性対策情報データベースJVN iPedia （https://jvndb.jvn.jp/）を紹介し、適宜確認することをお伝えすることは、脆弱性対策情報・脅威情報の通知を行うことを満足しますでしょうか。 | 具体的なサイバーセキュリティ対策は、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基づき、自らの責任で策定するものであり、その対策は個別事案に拠るため、通知が必要な具体的な情報については、お答えできません。 |

| | | |
|---|---|---|
| | ■理由<br>通知対象の利用者が多いと、都度通知をすることは現実的に不可能であり、具体的かつ現実的に可能な対応の例をガイドライン等に記載いただきたく思います。 | |
| 9 | ■該当箇所<br>・ガイドライン改定案　8ページ<br>・3.2. ERABシステムが留意すべき基本方針<br>「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。」<br><br>■意見内容<br>当社は、特定のハードウェアに依存しないソフトウェアコントローラを用いたアグリゲーションシステムを志向しています。以下の意見は、この立場として記載しています。<br>「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、「脅威情報の通知を行うこと」が今回追加されました。ここで記載されている「脅威情報」の定義が必要と考えます。<br>今回検討された、「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）改定内容の概要」p.6記載の脅威・攻撃シナリオは、公開されていません。<br>攻撃に利用されることなどを考えて公開されていないと理解しています。<br>該当箇所の「脅威情報」は、脆弱性対策が存在する公開できる情報をさしていると理解しました。<br>この理解が正しくないのであれば、本ガイドラインの読者に正確な意図を伝えるために、もう少し具体的に記載するのはいかがでしょうか？ | ご理解のとおりです。<br>なお、脅威情報は、「3.6. ERABシステムにおけるサイバーセキュリティ対策」のStep4のリスク分析の結果に基づき、利用者に対して共有すべき脅威情報があれば、共有していただく必要があると考えております。 |
| １０ | ■該当箇所<br>・ガイドライン改定案　10ページ | ①機器が含まれている（機器に対してラベルが付与される） |

| | | |
|---|---|---|
| | ・3.4. ERAB システムが維持すべきサービスレベル<br>「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。)」<br><br>■意見内容<br>本項目の対象は IoT 機器であるため、インターネットを介して通信を行う機能が備わっている設備が対象であり、通信線がつながっている設備でも全てが対象とはならない理解でよいでしょうか。<br>例えば、PLC や LAN ケーブルではない通信線を使用しているものは、対象外でしょうか。具体的な範囲が分かるような記載をお願いしたく思います。<br><br>■理由<br>審査合格が必要な対象機器を把握したいためです。 | ②インターネットプロトコル（IP）を使用したデータの送受信機能を持つ<br>③直接・間接を問わず、インターネットにつながる（可能性がある／否定できない）<br>④購入時に具備されているセキュリティ機能を利用し、アップデート以外で（調達者・利用者が自らの意思で）後からセキュリティ機能を追加することが困難／できない<br>IoT 製品（供給者による販売又は利用者による購入の単位となるものであって、意図した目的を達成するための単独の IoT 機器、又は IoT 機器と必須付随サービスとで構成される一式）が対象となります。<br>詳細は、制度説明 HP をご確認下さい。<br>https://www.ipa.go.jp/security/jc-star/index.html<br>なお、3.3.章に記載の通り、ERAB システムが想定すべき脅威について、「閉域網だから安全であるという考えに立脚しないこと」を前提として対策の検討を進めることを要求事項としていることにご留意ください。 |
| １１ | ■該当箇所<br>・ガイドライン改定案　10 ページ<br>・3.4. ERAB システムが維持すべきサービスレベル<br>「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。)」 | ご理解の通りです。<br>既に導入済みの IoT 機器についてではなく、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、「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を求めています。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です。 |

| | | |
|---|---|---|
| | ■意見内容<br>本項目は、ガイドライン改定以降に新築または取替（リプレース）の機器が対象となりますでしょうか。<br>すでに運用済みの IoT 機器も対象となると、改修のための停止や、改修費用の発生など、影響が大きいため、確認させていただきたく思います。<br>仮に、運用済みの既設 Iot 機器も対象となる場合、いつまでに対応が必要でしょうか。ガイドライン上ではなくとも、公表いただきたく思います。<br><br>■理由<br>いつまでに、どの装置を対象に審査合格すればよいか、把握したいためです。 | 本ガイドラインは、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り、既に導入している IoT 機器が「セキュリティ要件適合評価及びラベリング制度(JC-STAR)」の★１を取得していない場合において、講じているセキュリティ対策が問題ないことを示しているものではございません。<br>なお、既設の機器に対しては、「3.6. ERAB システムにおけるサイバーセキュリティ対策」の Step4 のリスク分析を実施していただく必要があります。その上で、セキュリティ上の問題があれば、適切な手段を用いて対策を実施していただく必要があると考えております。 |
| １２ | ■該当箇所<br>・ガイドライン改定案　10 ページ<br>・3.4. ERAB システムが維持すべきサービスレベル<br>「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。)」<br><br>■意見内容<br>意見ではなく、確認となります。 | 本ガイドラインの公表後に新たに導入される IoT 製品が対象となります。<br>なお、既設の IoT 製品に対しては、「3.6. ERAB システムにおけるサイバーセキュリティ対策」の Step4 のリスク分析を実施していただく必要があります。その上で、セキュリティ上の問題があれば、適切な手段を用いて対策を実施していただく必要があると考えております。 |

| | | |
|---|---|---|
| | 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について”新たに導入”という文言はどう解釈すれば良いか。<br>新たに導入とは具体的に”25 年 3 月の受付以降に販売・設置する製品”との理解で良いか。<br>また、既に設置済みの GW の扱いについてはどうか？明示して欲しい。<br><br>■理由<br>ERAB 制御対象のエネルギー機器や GW の JC-STAR 対応について製造メーカーの協力を求めるため。<br>また、今後の対応方針決めのため、確認させて欲しい。 | |
| １３ | ■該当箇所<br>・ガイドライン改定案　10 ページ、14 ページ<br>・3.4. ERAB システムが維持すべきサービスレベル<br>・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）<br>・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）<br>「セキュリティ要件適合評価及びラベリング制度（JC-STAR)」<br><br>■意見内容<br>当面は、適合ラベルの付与を必須要件とせず、各レベル相当のセキュリティ機能を満たすと ERAB 事業者が判断した場合であっても、当該要件を満たすと考えて良いか。<br><br>■理由<br>現時点では JC-STAR は他の認証との相互承認枠組みが整備されていない認識であり、海外ベンダー製 IoT 機器の採用が困難となるため。 | リスクアセスメントの結果等を踏まえ、「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。」を要求事項として求めております。<br>なお、本ガイドラインは、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り、既に導入している IoT 機器が「セキュリティ要件適合評価及びラベリング制度（JC-STAR)」の★１を取得していない場合において、講じてい |

| | | |
|---|---|---|
| | また既に海外製の IoT 機器を活用して事業を営む ERAB 事業者においては、機器の再選定だけでなく、接続するアグリゲーターシステムの改修など費用負担が発生する恐れがあるため。 | るセキュリティ対策が問題ないことを示しているものではございません。 |
| １４ | ■該当箇所<br>・ガイドライン改定案　10 ページ、14 ページ<br>・3.4. ERAB システムが維持すべきサービスレベル<br>・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）<br>・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）<br>「セキュリティ要件適合評価及びラベリング制度（JC-STAR)」<br><br>■意見内容<br>適合ラベルの対象範囲は、VPP システムに接続されるすべての機器（ルーター、監視端末、PLC 等）と認識した。<br>「IoT 製品に対するセキュリティ適合性評価制度構築方針」において、利用者がソフトウェア製品等により容易にセキュリティ対策を追加することができる汎用的な IT 製品は対象外とするとされているが、利用者が指定の電文以外の通信を遮断するようなプログラムレベルでのセキュリティ対策を実施している場合も、対象外となる認識でよいか。 | 利用者がソフトウェア製品等により容易にセキュリティ対策を追加することが出来る IT 製品については、「セキュリティ要件適合評価及びラベリング制度（JC-STAR)」の対象外とされており、本ガイドラインにおける「セキュリティ要件適合評価及びラベリング制度（JC-STAR)」に関する要求事項の対象とはなりません。<br>なお、利用者がソフトウェア製品等により容易にセキュリティ対策を追加することが出来る IT 製品以外の「セキュリティ要件適合評価及びラベリング制度（JC-STAR)」の対象となる IoT 製品については、「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。」を要求事項として求めております。 |
| １５ | ■該当箇所<br>・ガイドライン改定案　10 ページ、14 ページ<br>・3.4. ERAB システムが維持すべきサービスレベル<br>・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）<br>・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）<br>「セキュリティ要件適合評価及びラベリング制度（JC-STAR)」 | ERAB システムに関連する機器が、本ガイドラインの対象外となることはありません。<br>リスクアセスメントの結果等を踏まえ、改定案の記載としています。<br>なお、具体的なサイバーセキュリティ対策は、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基づき、自らの責任で策定することとしています。 |

| | | |
|---|---|---|
| | ■意見内容<br>【勧告】として規定されている、JC-STAR 制度において、ルーターも含まれており、ルーターは規定対象から除外頂きたい。<br>※ 出 典 :<br>https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/pdf/20240823_1.pdf<br><br>■理由<br>サービス加入者の宅内ルーターを使用するビジネスモデルにおいて事業者がお客様所有のルーターまでガバナンスをきかせる事が難しく、実質、家庭用ルーターを介した通信を行う ERAB 事業の普及拡大が困難となるため。 | |
| １６ | ■該当箇所<br>・ガイドライン改定案　11 ページ<br>・3.6. ERAB システムにおけるサイバーセキュリティ対策<br>「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。」<br><br>■意見内容<br>step4,9 が追加となっているが、「ERAB に参画する各事業者は、ERAB システムでは、(製品ライフサイクルにおいて) 以下の手順を踏むこと。」など、何の手順かわかるようにしていただきたい。<br><br>■理由<br>何の手順なのかが分かり難いので、分かり易く記載頂きたい。 | 製品ライフサイクルのみならず、ERAB システムにおけるサイバーセキュリティ対策の手順として記載しております。 |
| １７ | ■該当箇所<br>・ガイドライン改定案　11 ページ<br>・3.6. ERAB システムにおけるサイバーセキュリティ対策 | リスクアセスメントの結果の提示については、本ガイドラインの想定するリスク事案を公表することとなり、リスクの誘因となるため、差し控えさせていただきます。 |

| | | |
|---|---|---|
| | 「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。」<br><br>■意見内容<br>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リスク分析例をすべて提示していただきたい。<br><br>■理由<br>ERAB 事業者間で共通しているシステム構成もあると考えており、各事業者がゼロベースでフレームワークのリスク分析を行うのは非効率と思われるため。 | |
| １８ | ■該当箇所<br>・ガイドライン改定案　11 ページ<br>・3.6. ERAB システムにおけるサイバーセキュリティ対策<br>「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。」<br><br>■意見内容<br>リスク分析は、資産ベース、あるいは攻撃シナリオベースのいずれかでよいと思う。 | 資産ベースのリスク分析と攻撃シナリオベースのリスク分析は、その目的やアプローチの仕方が異なるため、どちらの分析も必要となります。<br>資産ベースのリスク分析は、自組織内で運用されている ERAB システムを構成する IT 資産について把握し、それらの IT 資産の重要度やリスクを分析することで、IT 資産を保護することを目的としております。<br>一方、攻撃シナリオベースのリスク分析は、自組織として回避したい事業被害について把握し、当該事業被害を起こし得る攻撃シナリオやリスクを分析することで、回避したい事業被害を起こさないようにすることを目的としております。 |
| １９ | ■該当箇所<br>・ガイドライン改定案　11 ページ<br>・3.6. ERAB システムにおけるサイバーセキュリティ対策<br>「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。」 | どの脆弱性情報をどこまで共有するかについては、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基づき、自らの責任で策定する詳細対策要件に拠ります。 |

| | | |
|---|---|---|
| | ■意見内容<br>攻撃に利用される可能性のある脆弱性対策が存在しない脆弱性情報の共有は、必要最小限の関係者への共有が望ましいと考えます。<br>セキュリティ関係者では、当たり前のことかもしれませんが、「リソースアグリゲーターとの間で共有」する場合の範囲や情報の取り扱いについて、ガイドラインに記載するのはいかがでしょうか？ | |
| ２０ | ■該当箇所<br>・ガイドライン改定案　11 ページ、22 ページ<br>・3.6. ERAB システムにおけるサイバーセキュリティ対策<br>・4.1.4. 各事業者における監視・対応体制等<br>「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。」<br><br>■意見内容<br>共有する脆弱性情報は、全てではなく、選定して共有することでよいでしょうか。<br><br>■理由<br>理由としては、当社システムの機器やプログラム、通信プロトコルに脆弱性が見つかった場合、システム連携する他社システムの事業者に脆弱性情報を開示することは当社システムの弱点を開示することになると考えます。<br>そのため、特定・文書化した脆弱性情報を全て共有するのではなく、ERAB 全体のセキュリティが強固になる情報のみに限定した方が、リスク低減できると考えたためです。 | 具体的なサイバーセキュリティ対策は、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基づき、自らの責任で策定するものであり、その対策は個別事案に拠るため、脆弱性情報を選定して共有することの是非については、お答えできません。<br>なお、脆弱性情報は、「3.6. ERAB システムにおけるサイバーセキュリティ対策」の Step4 のリスク分析の結果に基づき、リソースアグリゲーターに対して共有すべき脆弱性情報がある場合は、その脆弱性情報を共有していただく必要があると考えております。 |
| ２１ | ■該当箇所<br>・ガイドライン改定案　11 ページ、22 ページ<br>・3.6. ERAB システムにおけるサイバーセキュリティ対策<br>・4.1.4. 各事業者における監視・対応体制等 | 具体的なサイバーセキュリティ対策は、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基づき、自らの責任で策定するものであり、その |

| | | |
|---|---|---|
| | 「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。」<br><br>■意見内容<br>他社へ連携する具体的な情報共有の方法について、記載いただけないでしょうか。<br>なお、当社はACシステム、RAシステムを保有しており、改定文案を素直に読むと、ACシステムでは連携する他社RAさまへの情報提供、RAシステムでは制御対象のリソースを保有するお客さま等からの情報受領をイメージしておりますが、認識齟齬あればご指摘願います。<br><br>■理由<br>理由として、例えば「脆弱性のあるバージョン〇〇のミドルウェア□□を使用」と他社に連携すると、弱点を開示することとなり、情報漏洩リスクも高くなるため、具体的に何を伝えればいいか疑問に思ったためです。 | 対策は個別事案に拠るため、他社へ連携する具体的な情報共有の方法については、記載できません。 |
| ２２ | ■該当箇所<br>・ガイドライン改定案　14ページ<br>・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）<br>「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。」<br><br>■意見内容<br>「管理組織の特定が可能」とは、プロトコルを管理している団体の特定が可能との理解で合っておりますでしょうか。<br>別の意図であれば、具体的に分かるような表現としていただきたく思います。<br><br>■理由 | ご理解のとおりです。 |

| | | |
|---|---|---|
| | どのような対応をすればよいか、具体的に分からないためです。 | |
| ２３ | ■該当箇所<br>・ガイドライン改定案　14 ページ<br>・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）<br>・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）<br>「セキュリティ要件適合評価及びラベリング制度（JC-STAR)」<br><br>■意見内容<br>R6 の通信経路で、LTE のような通信手段を有した機器が直接クラウド側のコントローラーに接続する場合、宅内ルーターを介して機器がクラウド側のコントローラーに接続する場合があると想定しています。<br>一方、JC-STAR 制度では宅内ルーター・HEMS コントローラー・エネルギー機器を対象として検討が進められています。<br>セキュリティガイドラインでは、宅内ルーターに関する記載がないので、JC-STAR 制度との対応方針をより正確に理解できるように、JC-STAR 制度との関わりの情報量を上げることはいかがでしょうか？ | 「宅内ルーター」については、P7 図 1 の ERAB システムにおけるゲートウェイの機能の一部に含まれます。<br>「HEMS コントローラー」については、同図の「HEMS」の内側の「コントローラー」に含まれます。<br>「エネルギー機器」については、同図の「機器」に含まれます。<br>なお、同一の機器において、LTE といった携帯電話の通信網を介した通信と、宅内ルーターを介した通信の双方（いわゆるデュアルスタック）によりクラウド側のコントローラーに接続しているような場合があります。このような場合には、R6 が携帯電話の通信網を介した通信、R4 及び R5 が宅内ルーターを介した通信のインターフェースとなり、R4、R5、R6 に関わる JC-STAR 制度等の対応方針を満たす必要があります。 |
| ２４ | ■該当箇所<br>・ガイドライン改定案　14 ページ<br>・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）<br>・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）<br>「セキュリティ要件適合評価及びラベリング制度（JC-STAR)」<br><br>■意見内容 | ご理解のとおりです。<br>本ガイドラインは、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り、既に運用している IoT 機器が「セキュリティ要件適合評価及びラベリング制度(JC-STAR)」の★１を取得していない場合において、講じているセキ |

| | | |
|---|---|---|
| | ”「IoT 製品を新たに導入する場合においては」と条件を付けて★１以上の製品を選択すること。”と記載されていることから、既に設定しているルーターを活用する場合、★1 の対応機器への買い替えは不要との解釈でよろしいでしょうか？ | ュリティ対策が問題ないことを示しているものではございません。<br>なお、既設のルーターに対しては、「3.6. ERAB システムにおけるサイバーセキュリティ対策」の Step4 のリスク分析を実施していただく必要があります。その上で、セキュリティ上の問題があれば、適切な手段を用いて対策を実施していただく必要があると考えております。 |
| ２５ | ■該当箇所<br>・ガイドライン改定案　14 ページ<br>・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）<br><br>■意見内容<br>ファイアウォールでインターネットと隔離した Closed なネットワーク内の機器は対象外とするなどの緩和措置を検討してほしい。<br><br>■理由<br>要求が厳しすぎると感じるため。 | リスクアセスメントの結果等を踏まえ、最低限のセキュリティ対策の要求事項を記載したものであり、緩和はできかねます。<br>なお、3.3.章にて ERAB システムが想定すべき脅威について、「閉域網だから安全であるという考えに立脚しないこと」を前提として対策の検討を進めることを要求事項として求めております。 |
| ２６ | ■該当箇所<br>・ガイドライン改定案　15 ページ<br>・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）<br>「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。」<br><br>■意見内容<br>ホワイトリスト（許可リスト）等による限定は、「機器メーカー等サードパーティのコントローラー」で既に持っている仕組みを活用するため、IP アドレ | 具体的なサイバーセキュリティ対策は、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基づき、自らの責任で策定するものであり、その対策は各々の ERAB システム構成等に拠るため、個別事案については、お答えできません。<br>なお、通信先の制限に用いる手法については、限定しておりませんが、IP アドレスやドメイン等の利用に対しても、「3.6. ERAB システムにおけるサイバーセキュリティ対策」の Step4 のリスク分析を実施していただく必要が |

| | | |
|---|---|---|
| | スやドメイン等で実現できれば問題ない、という解釈であっているか（固定された IP アドレスという意味合いだと、対応コスト、既存サービスへの影響が発生する）。 | あります。その上で適切な手法を選択していただく必要があると考えております。 |
| ２７ | ■該当箇所<br>・ガイドライン改定案　15 ページ<br>・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）<br>「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。」<br><br>■意見内容<br>「管理組織の特定が可能で、かつ脆弱性対策が可能であるプロトコルを採用すること。」と緩和可能か？<br>対策として、物理的なセキュリティが担保されている事で問題ないという事が言えるのではないか？ | リスクアセスメントの結果等を踏まえ、最低限のセキュリティ対策の要求事項を記載したものであり、緩和はできかねます。<br>なお、具体的なサイバーセキュリティ対策は、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基づき、自らの責任で策定するものであり、個別事案にはお答えできません。 |
| ２８ | ■該当箇所<br>・ガイドライン改定案　22 ページ<br>・4.1.4.　各事業者における監視・対応体制等<br>「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。」<br><br>■意見内容<br>共有先はどこまで含めるのか。<br>開示先によってはリスクが高くなる可能性がある。<br>共有先は限定されるのが望ましい。 | どの脆弱性情報をどこまで共有するかについては、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基づき、自らの責任で策定する詳細対策要件に拠ります。 |
| ２９ | ■該当箇所<br>・ガイドライン改定案　22 ページ | ご理解のとおりです。 |

| | | |
|---|---|---|
| | ・4.1.4. 各事業者における監視・対応体制等<br>「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。」<br><br>■意見内容<br>共有先は、接続先のリソースアグリゲータのみで、共有のやり方や内容は、リソースアグリゲータと協議の上決定する、という解釈であっているか。 | |
| ３０ | ■該当箇所<br>・ガイドライン改定案　22 ページ<br>・4.1.4. 各事業者における監視・対応体制等<br>「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。」<br>「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。」<br><br>■意見内容<br>本項目は低圧リソースも対象と思いますが、一般家庭のネットワークの監視・対応は現実的には困難と考えており、検討後の対応として、具体的にどのようなことを求めていらっしゃいますでしょうか。<br>例えば、需要家側ではなく、上位システム（AC システム、RA システム）により、感染防止をきちんと止める対策（検討の結果、監視はしないが、上位対策によりリスク低減を図る）ができていれば、本条項への対応として満足できている理解でよいでしょうか。 | ERAB システムに関連する機器が、本ガイドラインの対象外となることはありません。<br>具体的なサイバーセキュリティ対策は、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基づき、自らの責任で策定するものであり、その対策は個別事案に拠るため、監視・対応体制等の具体的な方法については、お答えできません。<br>なお、一般家庭のネットワークや無線 LAN ルーターに対しては、「3.6. ERAB システムにおけるサイバーセキュリティ対策」の Step4 のリスク分析を実施していただく必要があります。その上で、セキュリティ上の問題があれば、適切な監視・対応体制等の検討を実施していただく必要があると考えております。 |

| | | |
|---|---|---|
| | 具体的な対応の例などをガイドライン等へご記載いただきますよう、お願いいたします。 | |
| ３１ | ■該当箇所<br>・ガイドライン改定案　全体<br><br>■意見内容<br>この勧告事項をすべてやろうと思うとそれなりの費用が掛かる。<br>また、ERAB は中小企業も多く参入していることから、政府の方で、必要な費用負担支援策も検討してほしい。 | 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こととしています。 |
| ３２ | ■該当箇所<br>・ガイドライン改定案　全体<br><br>■意見内容<br>経済安全保障法においても、50 万 kW 以上の出力を管理する ERAB の場合は、同法案の対象となり、リスク管理措置が求められるが、このガイドラインにある事項を遵守する事で、同法案で求められているリスク管理措置をカバーできると考えてよいか。 | 経済安全保障法において求められるリスク管理措置と、本ガイドラインで求める対策要件は異なることから、本ガイドラインに準拠することで、経済安全保障法で求められているリスク管理措置に遵守していることにはなりません。 |
| ３３ | ■該当箇所<br>・ガイドライン改定版の準拠時期<br><br>■意見内容<br>本ガイドラインは 2024 年度中に改定し、公表するご予定と伺いましたが、施行開始（準拠しないといけない時期）は、いつとなりますでしょうか。<br>例えば、今回、JC-STAR のレベル 1 以上が IoT 製品に求められていますが、取得していないものは一定の時間がかかる可能性もあり、公表日のタイミングで準拠しないといけないものかが気になりました。<br>ガイドライン上ではなくとも、公表いただきたく思います。 | ガイドラインの公表以降においては、改定後の本ガイドラインの要求事項を満たすことにより、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に準拠していることとなります。 |

| | | |
|---|---|---|
| | ■理由<br>いつまでに、どの装置を対象に審査合格すればよいか、把握したいためです。 | |

※今回の改定案に直接関係のない７件については、御意見として承り、今後の参考とさせていただきます。