資料５－２

一部非公開

新規プレーヤーのサイバーセキュリティ対策確保の方策について

令和３年２月１５日

資源エネルギー庁電力産業・市場室

1. アグリゲーターライセンスのサイバーセキュリティ対策について

2. 小売電気事業者のためのサイバーセキュリティ対策ガイドラインについて

1. アグリゲーターライセンスのサイバーセキュリティ対策について

2. 小売電気事業者のためのサイバーセキュリティ対策ガイドラインについて

アグリゲーターライセンスのサイバーセキュリティ対策に係る議論の経緯

- 昨年成立した「強靱かつ持続可能な電気供給体制の確立を図るための電気事業法等の一部を改正する法律」において、**アグリゲーターが「特定卸供給事業者」として電気事業法上に新たに位置付けられた**ところ。
- この特定卸供給事業者については、持続可能な電力システム構築小委員会の中間とりまとめにおいて、「**アグリゲーターにおいて特に対策が必要と考えられるサイバーセキュリティについて、対策が不十分な事業者に対応する観点から、変更命令等の対象とすることが適当である**」と整理され、求めるべき**具体的対策内容について、第７回電力SWGにおいても御議論いただいた**。
- 昨年12月に開催された第８回持続可能な電力システム構築小委員会において、第7回電力SWGの御議論に基づき、**特定卸供給事業（アグリゲーター）届出に係る変更命令等の基準を整理**したので、御報告する。

アグリゲーターライセンスのサイバーセキュリティ対策の基準について

- 電力SWGにおける議論を踏まえ、発電事業者等のサイバーセキュリティ対策を定めた**「電力制御システムセキュリティガイドライン」**とアグリゲーション事業者の自主的なガイドラインとして定められた**「ERABに関するサイバーセキュリティガイドライン」**の**勧告事項**について、特定卸供給事業の**届出時にこれらが満たされていない場合は、変更命令等の対象**になることと整理した。
- また、**届出後の業務実施中**において、仮に**特定卸供給事業者のサイバー対策が不十分**であり、これによって**特定卸供給事業者による電力供給に支障が生じ、又は生ずるおそれがあるとき**は、「特定卸供給事業の運営が適切でないため、電気の使用者の利益の保護又は電気事業の健全な発達に支障が生じ、又は生ずるおそれがあると認めるとき」に該当するため、**業務改善命令の対象とする**ことと整理した。

＜参考＞電制ガイドライン・ERABガイドラインにおける勧告事項

- **組織**
  - **体制（経営層の責任等）**
  - **役割（責任者の任命、委託先管理等）**
  - **セキュリティ教育**
- **文書化**
  - **文書管理、実施状況の報告**
- **セキュリティ管理**
  - **セキュリティ管理（セキュリティマネジメントシステムの構築）**
- **設備・システムのセキュリティ**
  - **外部ネットワークとの分離**
  - **他ネットワークとの接続（接続点の最小化、防御等）**
  - **通信のセキュリティ（暗号化、通信プロトコル等）**
  - **機器のマルウェア対策**
  - **アクセス制御（接続制御、通信相手の認証等）**
- **運用・管理のセキュリティ**
  - **外部記憶媒体等のマルウェア対策**
- **セキュリティ事故の対応**
  - **情報の収集（セキュリティ事故対応に必要な情報の収集）**
  - **セキュリティ事故の対応（対応体制、手順の明確化等）**
  - **セキュリティ事故の報告と情報共有**
  - **周知と訓練（訓練の定期的実施　等）**

赤字：電制ガイドラインの勧告事項
青字：ERABガイドラインの勧告事項

下位のアグリゲーターとの関係について

- 特定卸供給事業者として電気事業法上の規制対象となるのは**最上位のアグリゲーター**のみであり、**下位のアグリゲーターは規制対象とならず、変更命令等や業務改善命令の対象にもならない**。
- しかしながら、多様なシステムがインターネット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というアグリゲーション事業の特性を踏まえると、**下位のアグリゲーターにおいてもしっかりとサイバーセキュリティ対策を実施することが必要**。
- この点、ERABガイドラインでは、**下位のアグリゲーター**に対し、ERABガイドラインへの準拠に加え、**最上位のアグリゲ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**が求められている。
- 上記を踏まえ、特定卸供給事業の届出に係る変更命令等の基準においても、**最上位のアグリゲーターに対し、下位のアグリゲーターに求めるセキュリティ対策要件の策定を求め**、これにより、アグリゲーター間の契約により担保されるサイバー対策の水準を届出時に確認し、ERABガイドラインの勧告事項相当の対策が求められていないと認められる場合は、**最上位のアグリゲーターに対する変更命令等や業務改善命令の対象とする**こととした。

1. アグリゲーターライセンスのサイバーセキュリティ対策について

2. 小売電気事業者のためのサイバーセキュリティ対策ガイドラインについて

パブリックコメントの実施等について

- 第10回電力SWGにおいてガイドライン案審議を実施、事務局から提示したガイドライン案でパブリックコメントを行うことについて、御了解をいただいた。
- これを受け、12月18日から１月16日までパブリックコメントの募集を実施。合計２者からの意見が寄せられた。
- 寄せられた意見等を踏まえ、別添のガイドライン案のとおり、修正を行ったところ。
- また、本内容について、小売電気事業者のサイバーセキュリティ対策に係る勉強会（書面開催）において、構成員の意見を確認したところ、特に意見はなかった。
- 本日、パブリックコメント等を踏まえた内容について御確認いただきたい。その後、本日の御議論を反映した上で、本ガイドラインを公表することとしてはどうか。

パブリックコメントでの主な御意見の概要

寄せられた主な御意見	御意見に対する考え方（案）
顧客との各種のネットワーク経由での連絡等（ホームページを通してのもの、電子メールを通してのもの等）においては、一般的なサイバーセキュリティについて、まず妥当かつ確立されたものを導入・実装していく事が重要であると考える。 HTTPS及びTLSは当然であるが、メールのTLS保護（SMTPoverTLS及びSTARTTLS。ネットワーク中を平文で重要情報を含むメールが行き来する事の無いように、また相手を認証しての通信が行われるようにするためにも、これは必須的に必要と考えられるものである。）及び電子署名（重要情報を含むメールには電子署名があるべきである。）、SSH（トンネル用ツールとしての利用を各所で行っていくと簡易にセキュリティレベルを大きく上げる事が可能と思われる。）の利用については確実に行っていくべきと考える。 （その様な事によって、各所でのユーザアカウントやパスワードの漏えいが少なくなり、またフィッシング的事態や盗聴の被害も減少する事になるかと思われる。また万が一の際の刑事捜査等においても不正アクセス関係の明確な犯罪行為の存在によって捜査・公訴が行いやすくなるかと考える。） これらについては、（有料となる認証局証明書の発行以外（※なお、現在では））およそ無料で可能となるソフトウェア的な手法となるもののはずだが、この様な低費用かつ妥当なセキュリティ関係措置が、地道に、確実になされていく事で、大きくサイバーセキュリティが向上するのではないかと考える。 ガイドラインにおいて、CSO、CISOの語句についての記述が無かったが、これらについては、市井における各種のWebサイトの記事との対応付けを行うためにも、記述を行っておく方が良いのではないかと思われた。	御指摘を踏まえ、需要家向けのポータルサイト等の通信の安全性の保護について記載させていただきます。 また、本ガイドラインで踏襲しているサイバーセキュリティ経営ガイドラインでの表現と整合をとり、CISOについて補足の記載させていただきます。

（参考）ガイドラインの策定に向けたスケジュール（案）