経済産業省

資料７

電力分野におけるサイバーセキュリティについて

２０１９年１１月６日

資源エネルギー庁

本日御議論いただきたいこと

- 近年、サイバー攻撃の事案は増加傾向にあるところ、サイバー攻撃には、大規模停電のように生命・財産を脅かすものがあることから、国民の安全に責任を持つ政府と、電力の安定供給に責任を持つ事業者が連携し、対策に取り組む必要がある。
- 前回の基本政策小委員会において、現在、産業サイバーセキュリティ研究会のワーキンググループ１（制度・技術・標準化）の下、電力SWG（サブワーキンググループ）において、以下の対策について検討が進められていることを御報告させていただいたところ。

  ①サプライチェーンリスクへの対応

  ②大手電気事業者への対応

  ③新規プレーヤーへの対応
- 上記のうち、③の検討に向け、小売電気事業者及びアグリゲーターに対して求めるべきサイバーセキュリティ対策を検討する観点から、電力SWGにおいて、事業者のサイバーセキュリティ対策の成熟度を把握するための実態調査が実施される予定。
- 本日は、当該実態調査の内容について御報告させていただきたい。

（参考）産業サイバーセキュリティ研究会ワーキンググループ１における検討体制

- 産業サイバーセキュリティ研究会のワーキンググループ１（制度・技術・標準化）の下、電力SWG（サブワーキンググループ）にて検討・議論を行っている。

産業サイバーセキュリティ研究会

WG１　制度・技術・標準化　［2018年2月～（５回開催）］
2019年４月 フレームワークの策定・公表

標準モデル

Industry by Industryで検討（分野ごとに検討するSWGを設置）

- **ビル**（エレベーター、エネルギー管理等）　［2018年２月～（９回開催）］ 2019年6月　ガイドライン第1版を公開
- **電力**　［2018年6月～（６回開催）］
- **防衛産業**　［2018年３月～（３回開催※）］ （防衛装備庁 情報セキュリティ官民検討会） ※防衛産業SWGとして開催した回数のみ
- **自動車産業**　［2019年4月～（２回開催）］
- **スマートホーム**　［2018年３月～（９回開催）］ 2019年度までにガイドライン取りまとめを目指す（予定） (JEITA スマートホーム部会 スマートホームサイバーセキュリティWG)
- **その他コネイン関係分野**

（参考）電力SWG（サブワーキンググループ）における議論

- 電力SWGでは、サプライチェーンリスクへの対応、大手電気事業者への対応、新規プレーヤーへの対応にわけて、それぞれの対策について検討が進められている。
- 電力システムのデジタル化、オンライン化の進展に伴い、更に包括的な対策を進めていくことが重要。

＜構成員＞座長：渡辺　研司　名古屋工業大学大学院教授

有識者（大学教授、弁護士等）、電気事業者、業界団体

＜方向性＞

- 電力制御系システムに関するセキュリティ向上策
  → **「電力制御システムセキュリティガイドライン」への提言**（サプライチェーンのリスクマネジメントや緊急時対応の強化）
  →2020年**東京オリパラへの対応を視野に、短期的に対応すべき事項と、より中長期で見て対応すべき事項を整理**して検討

- 電力自由化等に伴う多種多様なプレイヤー参入による、制御系システム周辺に拡がりつつあるサイバーセキュリティリスクへの対応策
  →**制御系システムに関連した分野・事業者におけるセキュリティ向上**のあり方を検討

- 業界全体の取組向上に資する基盤整備
  → **情報共有の更なる強化、諸外国との連携強化、人材育成基盤の強化**　等

＜中長期的に検討していく課題＞

- **サプライチェーンリスクへの対応**について
  ・海外の事業者や国内他分野の動向を踏まえると、日本の電力分野においてはどのようなリスクが存在するか。
  ・日本の電力分野の関係者が継続的に取り組むべき事項は何か。
- **大手電気事業者**のサイバーセキュリティ対策について
  ・大手電気事業者のサイバーセキュリティ対策の取組の現状分析と、今後取り組むべき事項は何か。
- **新規プレーヤー**のサイバーセキュリティ対策について
  ・新規プレーヤー等のサイバーセキュリティ対策の取組の現状分析と、今後取り組むべき事項は何か。

電気事業法令におけるサイバーセキュリティ関連規定の整備

- 電気事業法第39条により、事業用電気工作物を設置する者に対して、省令で定める技術基準への適合維持を義務付けており、技術基準において、一般送配電事業、送電事業、特定送配電事業及び発電事業の用に供する電気工作物の運転を管理する電子計算機に係るサイバーセキュリティの確保を規定。（技術基準の解釈として、『電力制御システムセキュリティガイドライン』及び『スマートメータシステムセキュリティガイドライン』を参照）
- 一方で、小売電気事業者の保有するシステムや、家庭用のエネルギーリソースを束ねてビジネスを行うアグリゲーター（現状では電気事業法の規制の対象外）のシステムは、この規制の対象となっていない。

電力制御システム セキュリティガイドライン

（共通事項）
■ セキュリティ管理組織の設置及びマネジメントシステムの構築、教育の実施等を記載。

設備・システム
・ネットワーク分離 ・通信データ保護
・不正処理防止 ・アクセス制御

運用・管理
・セキュリティ仕様 ・データ管理
・管理者権限割当 ・セキュリティパッチ

安定供給等の観点から、システムの重要度を定義
↓
重要度に応じた追加的セキュリティ対策を提示

・ログの取得 ・入退管理

スマートメーターシステム セキュリティガイドライン

（共通事項）
■ セキュリティ管理組織の設置及びマネジメントシステムの構築、教育の実施等を記載。

機器
・セキュリティ仕様 ・ファームウェアアップデート

通信
・通信プロトコル ・暗号 ・ネットワーク分離

システム
・コマンド管理 ・外部記憶媒体利用制限

運用
・管理者権限管理 ・ログ取得 ・データ管理

物理
・セキュリティ区画保護 ・アクセス管理

実態調査の目的

- 電力システム改革に伴い、小売電気事業に多くの新電力が参入するとともに、分散型電源を活用したアグリゲーター事業を行う事業者も出現するなど、多くの新規プレーヤーが電力分野において事業に取り組んでいる状況。
- 今後も多くの新規プレーヤーが参入すると考えられるところ、このような事業者に対しても適切にサイバーセキュリティ対策を求める必要があると考えられる。
- このため、電力システムにおける包括的なサイバーセキュリティ対策を検討する観点から、小売電気事業者及びアグリゲーターにおけるサイバーセキュリティ対策の実態について調査を実施する。
- 併せて、経営者のリスク認識を問うことによる会社全体としてのセキュリティ意識の向上や、自社のサイバーセキュリティ対策の実施状況の見直しによるサイバーセキュリティ強化を促す。

※　本調査は、11月上中旬発送、12月上旬回答締切予定。調査結果については①資源エネルギー庁にて適正に取り扱い、②各事業者の匿名性を確保の上、電力SWGや審議会における審議においてのみ使用する。

実態調査の対象

- 小売電気事業者及びアグリゲーターだけでなく、比較対象として、既に電気事業法において電気工作物へのサイバーセキュリティ対策の実施が義務付けられている発電事業者も調査対象に含める。
  ※　調査対象は、発電事業者（563社）、小売電気事業者（431社）、及びアグリゲーター（実証事業参加事業者：18社）とする予定。
- この調査は、各事業者のサイバーセキュリティ対策状況を把握するため、記名式で実施する。無記名で行う方が回答率が高まるとの意見もあるが、電力システム全体のサイバーセキュリティを確保するためには、全事業者の意識向上と具体的な取組が不可欠であるため、この調査に対する回答を行わなかった事業者を特定し、啓発を図っていく観点からも、記名式で行うこととしたい。
- 調査の対象となる事業者においては、こういう趣旨も御理解の上、調査への協力をお願いしたい。

※ 発電事業者は2019年5月に発電実績のある事業者、小売電気事業者は同月に需要実績のある事業者を対象とし、アグリゲーターは、アグリゲーター事業に参画している一部の事業者を対象とする。

設問設計の基本方針（１）

- 調査項目は、電力系統に影響を及ぼす可能性のあるシステムに対する規制の観点から、「電力制御システムセキュリティガイドライン」をベースラインとして設計。
- 加えて、小売事業者向けのITシステムセキュリティやアグリゲーターのセキュリティ対策の観点から、「サイバーセキュリティ経営ガイドライン」や「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」等のガイドラインにおいて記載されている対策項目も参照し、セキュリティ対策の実態をマネジメント面・技術面の双方から調査を実施。

設問設計の基本方針（２）

- 設問を設計する際には、ガイドラインで求められている事項そのものではなく、求められているセキュリティ対策を実施していることが客観的に分かるように設問を作成。
- 専門家の集まる電力SWGにおいて、更なる詳細を詰めた上で具体的な調査項目を設計することとしたい。

設問の例

電力制御システムセキュリティガイドライン	設問案
１．経営層の責任 経営層は電力制御システム等におけるセキュリティの確保について責任を負うこと。 ２．管理組織の設置 目的実現のためのセキュリティ管理責任組織を設置し、セキュリティガバナンスの構築を行うこと。 ３．目的の明確化 電力制御システム等のセキュリティの実施目的を明確にすること。	・経営責任者が、サイバーセキュリティを経営戦略の一部に位置づけているか。 ・経営陣は、電力関連システムのセキュリティ対策を推進する責任組織のために、必要な予算・人員等を確保しているか。 ・組織全体のセキュリティ対策を推進する責任者として、最高情報セキュリティ責任者（CISO等）が任命され、電力関連システムのセキュリティ対策への責任も負っているか。 ・電力の安定供給のために自社が果たすべきサイバーセキュリティ上の役割、責任、リスクマネジメント方針等が、経営会議等の議題に含まれているか。 ・組織全体の対応方針がセキュリティポリシーとして策定され、経営責任者によって承認されているか。 など
１．責任者の設置 電力制御システム等のセキュリティ管理責任者を任命すること。 ２．役割の定義 電力制御システム等のシステム関係者の役割を明確にすること。 ３．委託先等の対応 電力制御システム等に関連する委託先等の役割を明確にすること。	・セキュリティ管理者、システム管理者、システム利用者といった役割毎にセキュリティ上の責任と使命を文書化しているか。 ・セキュリティポリシーには、ビジネスパートナーや委託先に求める責任と役割に関する事項が規定されているか。 ・ビジネスパートナーや委託先が実施すべきセキュリティ対策事項は、契約書や仕様書の文面へ明確に記述しているか。 ・ビジネスパートナーや委託先からセキュリティ対策状況の報告を受けているか。

設問設計の基本方針（３）

- 設問項目の大枠については、以下のとおり。

項目	設問案
組織的セキュリティ対策（共通） ・経営層の関与状況 ・体制の確立 ・インシデント発生時の対応 ・セキュリティ教育の実施状況	• 経営責任者が、サイバーセキュリティを経営戦略の一部に位置づけているか • セキュリティ対策を推進する責任組織のために、必要な予算・人員を確保しているか • セキュリティ管理者やシステム管理者等、責任と使命を文書化しているか など
電力制御システムに関するセキュリティ対策（※） ・ネットワークのセキュリティ対策状況 ・機器／システムのセキュリティ対策状況 ・管理／運用に関するセキュリティ対策状況	• 外部ネットワークと電力制御システムは原則接続していない構成としているか など
インターネットサービスに関するセキュリティ対策 ・クラウドサービスの利用状況 ・サービスアプリケーションに関するセキュリティ対策 ・システム基盤のセキュリティ対策 ・サービスの管理・運用に関するセキュリティ対策	• 外部からの不正なリクエストを遮断するための対策を実装しているか など
ERABシステムに関するセキュリティ対策（※） ・システム基盤／運用に関するセキュリティ対策	• DR指令機能を担うサーバーは別ネットワークへ配置し、外部脅威から保護しているか など

※　対象となる機器やシステムを保有している事業者が対象

（参考）サイバーセキュリティ経営ガイドライン

平成27年12月28日策定
平成28年12月8日改訂（Ver.1.1）
平成29年11月16日改訂（Ver2.0）

- セキュリティはコストではなく投資であると位置づけ、経営者がリーダーシップを取ってセキュリティ対策を推進していくことが重要であることを示したガイドラインを公表。

１．経営者が認識すべき３原則

（１）経営者が、**リーダーシップを取って対策**を進めることが必要
（２）自社のみならず、**ビジネスパートナーを含めた対策**が必要
（３）平時及び緊急時のいずれにおいても、**関係者との適切なコミュニケーション**が必要

２．経営者がCISO等に指示すべき１０の重要事項

リスク管理体制の構築

（１）組織全体での対策方針の策定
（２）方針を実装するための体制の構築
（３）予算・人材等のリソース確保

リスクの特定と対策の実装

（４）リスクを洗い出し、計画の策定
（５）リスクへの対応
（６）PDCAの実施

インシデントに備えた体制構築

（７）緊急対応体制の構築
（８）復旧体制の構築

サプライチェーンセキュリティ

（９）サプライチェーンセキュリティの確保

関係者とのコミュニケーション

（10）情報共有活動への参加

（参考）ERABサイバーセキュリティガイドライン

- ERABサイバーセキュリティガイドラインは、**アグリゲーターが取り組むべきサイバーセキュリティ対策**を整理したもの。

ERABセキュリティガイドラインの概要

1. ガイドラインの位置づけ
- 「電力制御システムセキュリティガイドライン」と「IoT開発におけるセキュリティ設計の手引き」の考え方に基づき、事業者が実施すべき最低限のセキュリティ対策を整理したもの。
- 事業者が実装を必須として義務付けられる【勧告】、と実装を検討すべき【推奨】に分けて規定。

2. ERABシステム
- システム構成
- 基本方針
- 想定すべき脅威
- 維持すべきサービスレベル
- システム重要度の分類
- サイバーセキュリティ対策
- 取り扱い情報の差異によるシステムの分類
- 詳細対策要件の設計
- ガイドラインの継続的改善

3. 事業者における対策の在り方
- 本ガイドラインを標準対策要件とし、事業者が実運用に耐えうる「詳細対策要件」を策定