産業サイバーセキュリティ研究会 WG1 電力 SWG（第 17 回）議事要旨

日時　　：令和６年 10 月 22 日（火）８時３０分～１０時３０分

出席者　：

（座長）　渡辺　研司　　名古屋工業大学大学院

（委員）　稲垣　隆一　　稲垣隆一法律事務所

内田　忠　　電力 ISAC

江崎　浩　　東京大学大学院

大崎　人士　　産業技術総合研究所

奥村　智之　　日本電気協会

小野崎　勝徳　東京電力ホールディングス株式会社

門林　雄基　　奈良先端科学技術大学院大学

佐々木　勇人　一般社団法人 JPCERT コーディネーションセンター

新　誠一　　電気通信大学

高倉　弘喜　　国立情報学研究所

高橋　俊晴　　電気事業連合会（代理：後藤　正輝）

高見　穣　　情報処理推進機構

手塚　悟　　慶應義塾大学グローバルリサーチインスティテュート

議題

1.　サプライチェーン・リスクへの対策に関する手引き文書の作成について

2.　分散型電源のサイバーセキュリティ対策について

3.　リスク点検ツールの公開及び広域機関の取組との連携について

要旨

1. サプライチェーン・リスクへの対策に関する手引き文書の作成について

（1） 「サプライチェーン・リスクへの対策に関する手引き文書の作成について」を事務局より説明。

（2） 自由討議

- サイバーセキュリティ対策ツールのサプライチェーン・リスクについても考慮すべきである。
- サプライチェーン・リスクとして、悪意を持ったアクターが意図的にサプライチェーンを標的とした攻撃が想定される。ラテラルムーブメント対策を行うなど、自組織内で汚染されたソフトウェアの横展開を防ぐ方法を考えるべきである。
- 手引き文書について、サイバーセキュリティ基本法との関係性を触れるべきである。また、利用する主体を明確に記載すべきであり、「委託先等」の定義を明らかにするべきである。関連して、国内事業者が海外事業者と契約し、役務の提供が海外にて行われる場合を想定してスコープを整理すべきである。加えて、リスク点検ツールと手引き文書との関係性を記載すべきである。さらに、契約条項のモデルケースについても検討すべきである。
- サプライチェーン・リスクを考慮する際、事業者間の契約に関する観点が必要となる。規模が異なる事業者同士がコミュニケーションを行う際に、手引き文書を利用できるような内容にすべきである。
- エネルギー・サプライチェーン全体のリスクへの対応のために、他業種とのコラボレーションが必要であることを手引き文書には記載すべきである。電気事業連合会や電力 ISAC においては、他業種のセキュリティ関連団体とのコラボレーションを進めていただきたい。
- 正規ルートで販売される製品も脆弱性の影響を受ける可能性がある。対策による効果と負担のバランスを検討のうえ、対策の考慮だけで終わらないよう、手引き文書を作成すべきである。また、外国製品を導入しないことだけで安全を確保できるといった誤解を招くような記載は避ける必要がある。
- システムに対する攻撃に対して、運用管理の観点のみで保護するのは難しい。システム側の対策実装についても考慮すべきである。
- 委託先のセキュリティ状況が把握できることが理想であるが、完全に把握することは困難な場合もある。委託先の事業に影響を及ぼすリスクを中心に把握することが現実的ではないか。
- エネルギー業界特有の取組と、IoT 製品セキュリティなどの他産業にまたがる全体の取組とが連携されると良い。また、電力分野のセキュリティ対策に関する様々な

ガイドラインが存在する中で、参照先についての案内があると、事業者に浸透しやすいのではないか。

２．分散型電源のサイバーセキュリティ対策について

（１） 「小規模太陽光発電設備のサイバーセキュリティ対策の課題について」を事務局より説明。

（２） 「IoT 製品に対するセキュリティ適合性評価制度（JC-STAR 制度）について」を経済産業省サイバーセキュリティ課より説明。

（３） 「ERAB サイバーセキュリティガイドラインの改定状況について」を資源エネルギー庁新エネルギーシステム課より説明。

（４） 自由討論

- 小規模太陽光発電設備におけるリスクとしては、多数の設備の脆弱性が狙われ同時多発的にインシデントが発生することや、多数の設備を遠隔監視するプラットフォームが侵害されることが想定される。前者のリスクに対しては、機器での対策を検討すべきである。後者のリスクに対しては、プラットフォーム事業者に対する認定制度の構築が想定される。
- 小規模太陽光発電設備のリスクとして、事業者は銅線窃盗への対策に頭を悩ましている。物理的なセキュリティ対策についても考慮することが重要である。
- ユーザーに対する脆弱性の通知の取組を充実する必要があるが、通知だけでは対策の実効性に限界がある。パッチの自動アップデートなど、機器に対する直接的なアプローチについて、関係省庁と検討すべきである。
- 議論には様々な関係団体も参加させるべきである。電気工作物の安全対策においては、設置者だけでなく関連するサプライチェーン上の事業者についてもスコープに含めるべきかを検討すべきである。関連して、機器を出荷・設置するそれぞれの段階でのセキュリティ対策について、責任の所在を明確にすべきである。
- 小規模太陽光発電設備に対する不正な同時操作をどう防ぐかが論点であり、事業者の負担を考慮した対策検討が必要である。JC-STAR 制度との連携を考える際、JC-STAR 制度の適合基準が小規模太陽光発電設備において求められる対策として妥当かを検討すべきである。
- 小規模太陽光発電設備における対策は、資産の構成把握・構成管理を出発点とすべきである。

３．リスク点検ツールの公開及び広域機関の取組との連携について

（１）　「リスク点検ツールの公開及び広域機関の取組との連携について」を事務局より説明。

（以上）

お問合わせ先

資源エネルギー庁 電力産業・市場室

電話：03-3501-1748