産業サイバーセキュリティ研究会 WG1 電力 SWG（第１６回）議事要旨

日時　　：令和６年２月１日（木）９時３０分～１２時００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

大浪　哲　　電気事業連合会

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

新　誠一　　電気通信大学

高見　穣　　情報処理推進機構

議題

１．大手電力事業者のサイバーセキュリティに係る取組について

２．電力制御システムにおけるサプライチェーン・リスクに対する対応について

３．アグリゲーター及び分散型エネルギー源（DER）のセキュリティ対策について

４．電力分野におけるサイバーセキュリティリスク点検ツールについて

５．サイバー攻撃による被害に関する情報共有の促進に向けた検討について

要旨

１．大手電力事業者のサイバーセキュリティに係る取組について

（１）　「大手電力事業者のサイバーセキュリティに係る取組について」を電気事業連合

会より説明。

（２） 自由討議

- サイバー環境の急激な変化を考慮し、ガイドラインの改訂周期を検討すべきである。
- ガイドラインに記載された事項の解釈の幅を狭め、遵守評価の基準を明確化するべきである。

２．電力制御システムにおけるサプライチェーン・リスクに対する対応について

（１） 「電力制御システムにおけるサプライチェーン・リスクに対する対応について」を事務局より説明。

（２） 自由討論

- スピード感が重要であり、世界の動きに劣後しないことを前提に取組を進める必要がある。
- リスクの定義が現場での作業において重要であり、ガイドラインや提言においても明確な定義が求められる。また、リスク把握の手法が複数ある中で、リスク点検ツールの使用が有効であることを提言するべきである。
- サプライチェーン・リスクへの対応に当たっては、発注仕様書の記載方法と納品検査の方法が重要である。また、異なる業界間のガイドラインの整合性確保が課題であり、全ての重要インフラに共通の基本対策と電力分野における特異事項を整理されたい。
- 経済安全保障推進法の文脈では、サイバーとフィジカル両面のリスクに対する対策が必要である。
- 提言におけるセキュリティ管理に関する記載について、より詳細に、リスク分析を行うこと及びそれに基づいた対策を講じることに言及すべきである。
- 「ライフサイクル」という用語は「システムライフサイクル」と修正すべきである。
- 複数分野に跨るベースの基準を整備した上で、電力分野特有の要素を検討するべきである。この取組は、整合性の確保にとどまらず、国全体のセキュリティ確保に繋がる。
- 国においては、サプライチェーンにおける利害関係者が、必要な情報を取得又は提供し、利用することができる法的根拠を明らかにする措置を講じるべきである。

３．アグリゲーター及び分散型エネルギー源（DER）のセキュリティ対策について

（１）　「日本における ERAB システムに関するセキュリティ対策実践」を慶應義塾大学梅嶋准教授より説明。

（２）　「アグリゲーター及び分散型エネルギー源（DER）のセキュリティ対策について」を事務局より説明。

（３）　自由討論

- アグリゲーターや DER の進展において、ゼロトラスト・セキュリティの意識が重要であり、末端におけるリスク最小化が鍵である。
- ゲートウェイに基づくセキュリティ対策は過渡的な対策である。将来的に導入される機器に対して、ゼロトラストの観点も踏まえて適切に対策を行うこと、リスクを把握した上でシステム構築を進めることが重要である。
- IoT 製品の運用には、セキュリティオペレーションセンター（SOC）による監視が重要であり、SOC についても言及すべきである。
- ガイドライン上の文言において、対策の実施主体は明確にすべきである。
- 国外制度と本ガイドラインのアグリゲーターに対する要件の差異が懸念され、事業者視点からの検討での受容性向上が期待される。
- DER のセキュリティ対策においては、経済産業省で別途検討されている IoT 製品に対するセキュリティ適合性評価制度と整合性が確保されることが望ましい。

４．電力分野におけるサイバーセキュリティリスク点検ツールについて

（１）　「電力分野におけるサイバーセキュリティリスク点検ツールについて」を事務局より説明。

（２）　自由討論

- 広くツールが利用されるよう、ツールの提供形式を検討すべきである。
- リスク点検結果を踏まえ、事業者の依存関係や弱点などが自動的に解析されることが望ましい。また、専門的な内容も含まれるため、回答者の負担軽減を考慮したツールとする必要がある。
- ツールにおいて、リスク点検実施者の氏名と保有資格を記入する欄を設けること

が望まれる。その上で、公的支援を検討する場合は、適切な資格保有者に対する支援に限定することが妥当である。

- 税制や経費に関する優遇策が重要であり、認証実施主体の能力確保、責任強化及び慎重な認定者の選定が不可欠である。第三者認証以外では、組織内人材育成と外部向け能力発信の仕組みの検討が重要である。

５．サイバー攻撃による被害に関する情報共有の促進に向けた検討について

（１）　「サイバー攻撃による被害に関する情報共有の促進に向けた検討について」を経済産業省サイバーセキュリティ課より説明。

（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