産業サイバーセキュリティ研究会 WG1 電力 SWG（第５回）議事要旨（案）

日時　　：　令和元年７月９日（火）１３時００～１５時００分

出席者　：

（座長）　渡辺　研司　　名古屋工業大学大学院

有村　浩一　　JPCERT/CC

稲垣　隆一　　稲垣隆一法律事務所

岩見　章示　　電力 ISAC

大崎　人士　　産業技術総合研究所

大友　洋一　　電気事業連合会

門林　雄基　　奈良先端科学技術大学院大学

桑名　利幸　　情報処理推進機構

谷口　浩　　東京電力ホールディングス株式会社

都筑　秀明　　日本電気協会

議題

１．大手電力会社のサイバーセキュリティ対策について（サプライチェーンへの対応含む）

２．新規プレーヤーのサイバーセキュリティ対策について

要旨

１．大手電力会社のサイバーセキュリティ対策について（サプライチェーンへの対応含む）

（１）　「米国サプライチェーン規制等の状況」を事務局より説明。

（２）　「CPIC の動向」を事務局より説明。

（３）　「C2M2 のご紹介」を桑名委員より説明。

（４）　「大手電力会社のサイバーセキュリティ対策の実態把握について」を事務局より説明。

（５） 自由討議

- これまで開催された SWG を通じて国内外のフレームワーク等の情報は集まりつつある。ここからは、電力事業者の意見も反映していく必要があると考える。電力事業者との対話を実施すべきではないか。
  - 実態把握が重要であるということに大きな異論はないだろう。主旨を明確にすること、機微情報を厳格に取扱うこと、得られた情報を行政規制には用いず各社のサイバーセキュリティ向上及び電力事業とそれを支えるサプライチェーンのセキュリティレベル向上のみに用いることを明確にし、効果的な対話とすることが重要である。
- 現状把握の基準として、成熟度評価の観点を含んだフレームワークは参考になる面もある。一方で確認のための労力やその実効性にも配慮が必要である。
  - マネジメントのアセスメントを行うためのフレームワークは、判定基準や技術的な要件が十分ではないことがあるため留意が必要である。対象に応じた必要な評価軸を検討すべきであり、成果の位置づけも議論が必要である。
  - 規制的なアプローチでは対処できないリスクは、リスク分析の手法を含んだフレームワークを参照し、考慮すべきである。高度に技術的な観点は、電力産業とサイバーセキュリティの規制や技術の双方に通じた専門家を交えた議論をすべきである。
- サプライチェーン規制については、国際水準と照らし合わせた際に問題が生じることが無いよう、引き続き状況を注視すべきである。

２．新規プレーヤーのサイバーセキュリティ対策について

（１） 「新規プレーヤーのサイバーセキュリティ対策の論点」を事務局より説明。

（２） 「海外セキュリティ対策調査」を事務局より説明。

（３） 自由討議

- 電力自由化に伴う電力設備の IT 化の状況も考慮した議論を進めるべき。現時点で、電力事業者の扱いではないが、密接な関わりがあるという観点では、アグリゲータのセキュリティ対策のあり方を知ることも重要であると考える。ヒアリング先にはアグリゲータも含めることが望ましい。
- 電力事業者のベンチマークの方法として、組織や体制の構築状況、ガイドラインの準拠状況も一つの基準となるが、技術的な能力も重要な基準である。フランスの認

証機関の先進的な取組みが参考になるのではないか。

- 英国は、日本の電力産業の事業モデルと非常に近く、系統運用事業者の取組状況は確認することを推奨したい。海外調査先から情報を入手するだけではなく、日本の状況も伝えることが必要である。
- ドイツは EU のビジネスモデルを理解した上で対象を選定する必要がある。評価の高い取組みを行っている大手電力事業者もある。
- 人材の運用や育成、評価をどのような観点や手法で実施しているかは確認したい。人材流動性が小さい日本の場合でも、海外の人材育成モデルを参考にできる部分はあるのではないか。

（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