産業サイバーセキュリティ研究会 WG1 電力 SWG（第 18 回）議事要旨

日時　　：令和 7 年 2 月 4 日（火）10 時 00 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

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

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

新田　哲　　JFE スチール株式会社

議題

1. 電力制御システムセキュリティガイドラインの改定について
2. サプライチェーン・リスクへの対策に関する手引き文書について
3. 分散型電源のサイバーセキュリティ対策について
4. リスク点検ツールに基づく自己診断結果の分析について

要旨

1. 電力制御システムセキュリティガイドラインの改定について

（1） 「電力制御システムセキュリティガイドラインの改定について」を電気事業連合会より説明。

2. サプライチェーン・リスクへの対策に関する手引き文書について

（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について」を事務局より説明。

（2） 自由討議

- 手引き文書について、サプライチェーン・リスクやサプライチェーン・セキュリティ対策を明確に定義すべきである。
- 手引き文書の内容が需要者側に偏重していないか精査し、必要に応じて供給者側が行うべき対策を追記すべきである。
- 手引き文書及び電力制御システムセキュリティガイドラインについて、サイバーセキュリティ、セキュリティ、リスクの 3 つの用語を各種の法令や戦略文書と整合性が取れる形で定義すべきである。なお、サイバーセキュリティについてはサイバーセキュリティ基本法に則って定義し、想定している脅威はサイバー攻撃に限らないこと明確にすべきである。
- 手引き文書について、運用・保守中の機器に脆弱性が見つかった場合の対処方法を記載すべきである。
- グループ組織を介したサイバー攻撃の記載があるが、これはサプライチェーン攻撃には含めず、アイランドホッピング攻撃と別の攻撃名で呼称されることが多い。このため、用語の類型については補足すべきである。
- 悪意がある主体の攻撃や不正行為はサプライチェーン・リスクの一部でしかない。これを手引き文書に明記しないと、手引き文書に従えばサプライチェーン・リスクがすべて解消されると誤解する事業者が出てくるおそれがある。
- 手引き文書について、組織のサプライチェーン・リスクへの対応状況の確認方法を具体化すべきである。リスク分析等の具体的な手順を記載するとユーザーは使いやすいのではないか。
- 中小事業者が手引き文書のすべての事項を最初から遵守することは難しい。ゆえに、中小事業者は PDCA サイクルを回すことが重要であり、その旨を通知又は手引き文書でアピールすべきである。

3. 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について」を事務局より説明。

（2） 「EX4Energy 株式会社における取組について」を EX4Energy 株式会社より説明。

（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） 「マイクログリッドにおけるサイバーセキュリティ対策について」を手塚委員より説明。

（5） 自由討議

- 広範囲のリスクに対する対策を考え、その一部としてサイバーセキュリティ対策を位置付け、安定に電力を供給できる体制を構築すべきである。
- 欧州や米国に遅れないようマイクログリッドの接続要件を整備すべきである。
- 太陽光発電設備は直接的な干渉にさらされやすいケースが多い。人的な脅威以外に自然災害や火災も含めてリスクアセスメントすべきである。
- PCS メーカー等に対し、JC-STAR 制度の★1 の取得は最低限であって、そのうえで★2 以降のステップが必要だと強調すべきである。米国や欧州の制度との整合性を図ったうえで、取組を進める必要がある。
- 電気事業者に対して JC-STAR 制度及びセキュリティが確保されたサービスの利用を推奨することはセキュリティ対策の実効性を高めるうえで有用な手段だろう。特に、各種ガイドラインに沿っての対策が難しい事業者に対して有用である。
- JC-STAR 制度の★1 の準拠が困難なメーカーをどう対処するかが重要である。この対処がないと、★2 以上のラベルを取得した製品の要求も意味がなくなってしまう。

4. リスク点検ツールに基づく自己診断結果の分析について

（1） 「リスク点検ツールに基づく自己診断結果の分析について」を事務局より説明。

（2） 自由討議

- 今回明らかになった課題の解決のために、対策に課題のある事業者区分からベンチマークする事業者を選び、対策方法に関するサクセスケースを他の事業者へ展開する取組が良いのではないか。対策方法や対策スケジュールの検討に当たっては生成 AI が活用できる。

- 対策に課題のある区分の事業者においては、サイバーセキュリティ対策に関心を持っていない事業者も多い。自発的な取組には限界があるため、サービス供給事業者側から、資金や能力が流れる構造を検討する必要がある。
- インシデント対応態勢の整備は、技術的な必要性に限らない。インシデントに関する報道等により自社の信頼性低下につながらないよう、速やかな対外応答の準備も重要となる。

（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