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　電力サブワーキング（第 19 回）
議事要旨

日時：2026 年 2 月 12 日（木）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）	安部　浩幸	東京電力ホールディングス株式会社
	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
	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
	藤山　徹	一般社団法人送配電網協議会
	新田　哲	JFE スチール株式会社

議題
１．電力分野のサイバーセキュリティ対策の近況について
２．サプライチェーン・リスクへの対応とリスク点検ツールの活用について
３．分散型電源のサイバーセキュリティ対策について

要旨
１．電力分野のサイバーセキュリティ対策の近況について
（１）資料３に基づき、「電力分野のサイバーセキュリティ対策の近況について」を事務局より説明
（２）自由討議
- 資料 p.27 にて、JC-STAR★1 についての記載があるが、現状でも★2 以上の議論を進めて行こうとしていると認識している。その旨を何らか記載いただけると良いのではないか。
- グローバルの動向について、今後の調査分析の対象としては EU も重要な存在。EU では、重要インフラ設備のセキュリティ対策として NIS2 指令が該当し、機器の認証制度として欧州サイバーレジリエンス法（CRA）が該当すると考えられる。グローバルでは早めの対応を一生懸命進めている中で、ヨーロッパは第三者認証に進もうとしている。では日本はどうするのかという点を経産省中心に考えていただきたい。
- 各国が別々の認証制度を導入した場合、ベンダーは複数の認証を取らなければならなくなるため、真に電力業界としてやらなければならない対策を進めていただきたい。
- 海外の認証制度はそれぞれ要件が異なる点がある。日本製品を海外市場に展開していくことを考えるのであれば、海外基準とのマッピングやギャップ分析も必要と考える。

- 12 月末にポーランドにてサイバー攻撃事例があり、マルウェアによるデータ破壊があった。当該マルウェアは VPN 経由で侵入し、多要素認証等が実施されていなかったのが事例発生の原因であると考えられる。当事例から、認証情報の適切な管理や脆弱性管理等の実施の必要性が高まっている。設備が攻撃されたわけではなく、グリッドコネクションポイントが攻撃された事例ではあるため、日本に該当する設備があるかは不明だが、参考にしていただきたい。

２．サプライチェーン・リスクへの対応とリスク点検ツールの活用について

（１）資料４－１に基づき、「サプライチェーン・リスクへの対応とリスク点検ツールの活用について」を事務局より説明

（２）資料４－２に基づき、「電気事業者におけるサイバーセキュリティの状況について」を電気事業連合会より説明

（３）自由討議

- サプライチェーン・リスクでは、内部・外部の区切りが曖昧になってきており、内部リスクの管理も重要。状態は常に変化しており、「いつもと違う変化」を検知可能な機能が必要。しかしながら、偽陽性の多発等により検知ツールが現場の実効性を低下させていることも多い。監視（モニタリング）方法の最新状況についても、ガイドラインでの情報提供や点検ツールでの確認事項の一つになるのではないか。
- サプライチェーン評価制度は情報処理推進機構（IPA）でも検討を進めているが、リスク点検ツールについては、電力広域的運営推進機関（OCCTO）と連携しながら引き続き力を入れてほしい。
- リスク点検ツールは、各社の自己評価によるアンケートのため、回答者のセキュリティ知識や専門性が事業会社によって異なっていると想像される。事業者の回答が情報処理安全確保支援士等のセキュリティ資格保有者の回答であるか等の要素も考慮した方が良いのではないか。
- 他の政策との連動制という意味では、例えば総務省の CYDER（Cyber Defense Exercise with Recurrence：実践的サイバー防御演習）のような他のトレーニングへの参加状況等も含めて、参考情報として聴取してみてはどうか。
- 規模のレベルは違うが、我々もグループ会社に対してサイバーセキュリティ対策の状況を可視化する取組を行っている。その際に、平均値の評価では個社ごとのばらつきが特定できないと感じた。標準偏差を考慮する、中央値または最低レベルのグループの分析といった、別の視点も重要だと考える。
- 経産省ではセキュリティ対策評価制度を検討していると認識。電力業界はセキュリティに関して他分野と比べてしっかりと取り組みを行っている一方で、電力業界におけるガイドラインやリスク点検ツールと、現在検討しているセキュリティ対策評価制度との整合性や連動についても検討しなければ、個社から見れば必要以上に負荷が増えていく恐れがある。
- リスク点検ツールを今後アップデートする際は、セキュリティ対策評価制度とのすり合わせも重要。また、サプライヤーには電力業界に限らず様々な業界の顧客から発注が来るので、他業界の取組についても注視する必要がある。他業界との情報共有をしつつ、アップデートを進めていけたら良いと思う。

３．分散型電源のサイバーセキュリティ対策について

（１）資料５に基づき、「分散型電源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）自由討議

- 電力会社には、専用 OS を使っているから大丈夫という心持ちではなく、脆弱性対策が恒常的に提供される OS を使っていなければならないという意識を持ってほしい。
- JC-STAR★1 のグリッドコード化については、我々のような系統運用する事業者からすると非常にありがたい内容であり、これまでの調整に感謝申し上げる。
- 分散型電源のセキュリティ対策について、設置後の脆弱性対応が懸念である。例えば、JC-STAR ラベルは取得した後も２年ごとに更新するタイミングがあると思うが、そうした点にもしっかりと対応していく必要がある。また、既に系統接続している電源についても、インセンティブがあれば JC-STAR★1 の取得につながると思われる。
- 日々巧妙化する手口が深刻なセキュリティ事故を引き起こす例が増えつつあり、セキュリティ対策の在り方が問われている。韓国 SK テレコムのセキュリティ事故がその一例であり、統計的技術・学習型技術で異常を検知できないことも本件の背景である。このサブワーキングに対しては、こうした状況の変化を踏まえて、ガイドラインやリスク点検ツールの中身を常に刷新していくことが、求められていくと感じている。
- JC-STAR★1 取得ができていない機器は系統から切り離すことも考えられるのではないか。系統から切り離すのが困難な場合は、代替措置として監視のレベルを上げる等の対策が必要と考える。
- JC-STAR★1 はエントリーレベルの基準になっており、電力システムでは★2 以上をいずれは求めていくべきである。日本の電力関係の機器・素材は世界的にも評価が高く、運用においても高いクオリティを担保できている。日本製品がグローバルマーケットを狙うことも考えると、より高いレベルでのサイバーセキュリティ対策を求めていくことも考えらえるのではないか。また、基準を満たせていないものが一定程度市場に残るという話もあったが、それらへの対応も考えていく必要がある。
- 攻撃の事例が増えて、機器の脆弱性情報も多く公開されてきた。制御機器における特定の脆弱性の傾向を踏まえて、様々なシナリオを想定した対策を行う必要があるのではないいか。
- 紹介いただいた ASEAN 経済研究センター（ERIA）の取組について、今後 NCO や METI との連携も重要になる。技術的バックグラウンド・マーケット・政府とのより深い連携を推進するべきである。
- ASEAN 向けの展開等を考えているのであれば、今後は英語での情報発信もお願いしたい。

以上