産業サイバーセキュリティ研究会　WG1 電力 SWG（第１回）議事要旨

日時　：　平成３０年６月１２日（火）１０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 |
| 阿部 | 克之 | 電気事業連合会 |
| 荒川 | 嘉孝 | 日本電気協会 |
| 中谷 | 昌幸 | JPCERT/CC |
| 岩見 | 章示 | 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 |
| 桑名 | 利幸 | 情報処理推進機構 |
| 高倉 | 弘喜 | 国立情報学研究所 |
| 手塚 | 悟 | 慶應義塾大学大学院 |
| 田中 | 道成 | JFE ホールディングス㈱ |

議題
１．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 SWG の運営について
２．電力 SWG の開催と経済産業省における電力分野のサイバーセキュリティ対策について
３．電力業界及び電力会社におけるサイバーセキュリティ対策について
４．自由討議

要旨
１．事務局
・産業サイバーセキュリティ研究会 WG1 電力 SWG の位置づけ等について説明。
・電力 SWG の設置についての説明と電力分野のサイバーセキュリティ対策についてご紹介。

２．電力業界のサイバーセキュリティ対策について
・電力分野における主要な取組の中で、①ガイドライン、②情報共有、③人材育成の３点について紹介。

・電力 ISAC の取組として、他分野との知見の交換を進めるため情報交換等を行っている。海外 ISAC との連携強化にも積極的に取組んでいる。

・電力 ISAC のワーキンググループ活動において、各社の取組について有識者の助言を添えたグッドプラクティスの共有等、情報交換を行っている。

・制御システムセキュリティセンターでの演習には、電力 ISAC メンバーでもある新電力も参加している。

・今後の課題としては、サプライチェーンにおけるリスク対策があげられる。

３．電力会社のサイバーセキュリティ対策について

・IT の担当部署が各電力設備・制御系システムを担う部署と連携し、サイバーセキュリティ対策のマネジメントをしている。

・サイバーセキュリティ対策における最新の情報を仕入れるには、関係者と face-to-face での関係を築くことが重要。

・教育・訓練や実務を通してどのようにセキュリティ人材を確保していくかが重要。

・今後の課題としては、限られたセキュリティ人材のなかで、いかに情報を見つけ、判断するかという点があげられる。

４．自由討議

（１）全体について

・日本の電力分野のサイバーセキュリティは諸外国よりは先をいっているのではと思う。数年前からはだいぶ急速な進展がうかがえる。一方で、旧来の状況からはサイバーセキュリティ対策の事情も変わってきており、世界的には、機器・ソフトウェアの識別やサプライチェーン管理についての要求をガイドラインに含めようとする動きがみられる。

・旧一般電気事業者以外の電気事業者におけるサイバーセキュリティ対策をしっかり講じる必要がある。太陽光発電設備も世の中に増えてきているなかで、新規参入者への対策をしっかりと行う必要がある。

・米国 E-ISAC では、周波数に乱れが生じたときにその原因が自然災害等の事故なのか、サイバー攻撃を受けたことによるのかを判断する。

・電力会社内における監査役の機能をより強くし、しっかりとレビュー機能を確保するべき。

・ストーリーで物を理解する人と、行動原理で物を理解する人がいる。このギャップを埋めるべく、サイバーセキュリティ対策にあたってはリスクシナリオを作成することが多い。組織にあっては、経営層を動かそうとすると、リスクのシナリオを作ることが重要。サイバー攻撃はなんらか対策の標準があれば完全に防げるというものではないので、事故が起きることを前提として、ある程度リスクシナリオベースでの対応を想定しておき、Consequence-driven で考える必要がある。

・電力業界はオールデジタル化に向かうのではと思う。第３層で運用管理していく部分をどれだけ強化できるかが重要。

・JPCERT/CC には、欧米の情報も少し入るが、ISAC 同士で外に出ない情報を連携するのが大事かとおもう。

・サイバーセキュリティ対策を講じつつ、コストの観点もあるので、バランスのとれた対応を行う必要がある。

・最近、エストニアでの大規模サイバー演習の話が報道であったが、それをそのまま日本でも応用できるかというとそうではない。サイバー攻撃のなかには電磁波の問題も入っている。幅広く業界を見ておく必要がある。

（２）人材育成について

・現場の人材が足りないという問題のなかで、シニア人材の活用という話がある。サプライチェーンのマネジメントも経験豊かな人間であればやりやすいはずで、ガバナンスはシニア、実運用は若い従業員、とチームでセキュリティ対策にあたることが有効かと思う。

・アメリカでもシニア層の活用は大事という話がある。現場が分かっているシニア（元工場長等）と若手職員でチームを組むことが必要。

・現場の人材が不具合の原因を設備不良と断定せずに、サイバー攻撃だと気付き、自ら対応を行うことが重要。

・事故扱いにしてそのままにしておくと、サイバー攻撃の場合はエスカレーションするということを、現場に慣れ親しんだ人間にしっかり伝えることが重要。

・技術の言葉がわかって、経営層にうまく伝えられる、いわゆる「橋渡し人材」の育成がとても難しい。サイバーセキュリティの世界でも現状過渡期にあると思う。

・IPA では、１００名規模で演習を実施している。参加者は３０～４０代が多い。

・現場で実務を担っていた人に判断能力を身に着けてもらう方が良いのではないか。人材がいないわけではない。その場にいる人材を育てる必要がある。

（３）サプライチェーン対策について

・こういった議論は非常に有効。一方で、サプライチェーンと一口にいっても幅広い。電力会社は様々な機器を購入している。優先順位を付けていかないと相当に混乱することが予想される。

・直接取引している分についてはサプライチェーンについてもある程度把握できるが、間接的な取引については実効性の担保が困難であることが実状。

・１つ１つの部品に問題があったときに、そのデバイスがどこのメーカーのものなのかは追いかけられず、解明するまでに１年かかるものもあると聞く。その間は脆弱性が放置されることになり非常に問題となる。

・諸外国含め外部のモデルを見ると、サイバーセキュリティ対策にコンサルの活用をしている者が多いのは事実。日本をみると、サプライチェーンは実はとても頑丈に守られている印象がある。アメリカ・ドイツとは状況が違う。海外の情報は知っておくべきだが、日本は日本の状況に合わせたサプライチェーンの検討をしていくべき。

・何か問題が起きたときに、どこが悪いか診断するのに３か月くらいかかる事例もある。IP アドレス、OS の情報・納品物に対してのトレーサビリティがない場合が多い。納品ベンダに対するガイドを作ったらよいのでは、という話もある。

・サプライチェーン対策にしっかり取り組んでいるのは航空業界。一方で、業界ごとにどこまでやるかの線引きが必要。

・業界ごとに運用が個別に違うので、大きなシナリオとしてはしっかり作りこんだうえで、そのなかでいかに業界ごとに取捨選択するかということだと思う。

・何をやるにしても、アベイラビリティのあることが重要。

・電力制御系システムガイドラインについては、本 SWG の議論をしっかり反映させて今後検討を行ってまいりたい。

（以上）

お問合せ先
産業保安グループ　電力安全課
電話：03-3501-1742
資源エネルギー庁　電力産業・市場室
電話：03-3501-1748