産業サイバーセキュリティ研究会　WG１ 電力 SWG（第４回）議事要旨（案）

日時　：　平成３１年２月２２日（金）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

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

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

新　　誠一　電気通信大学大学院

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

手塚　悟　　慶應義塾大学大学院

新田　哲　　JFE ホールディングス株式会社・JFE スチール株式会社

議題

１．サプライチェーンリスクへの対応について

２．サイバーセキュリティ対策の実態把握について

３．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．サプライチェーンリスクへの対応について

（１）「サプライチェーンリスクへの対応について」を事務局より説明。

（２）「IT 調達に係る国の物品等又は役務の調達方針及び調達手続に関する申合せ」を事務局より説明。

（３）「政府機関等の情報セキュリティ対策のための統一基準（平成 30 年度版）（抜粋）」を事務局より説明。

（4） 「サプライチェーン・サイバーセキュリティ等に関する海外の動き」を経済産業省商務情報政策局サイバーセキュリティ課より説明。

（5） 「サプライチェーンリスクに関する国内他分野の動向」を事務局より説明。

（6） 自由討議

- サプライチェーンにおけるセキュリティ対策は、効果と同時にコストが生じるので、そのコストをどう負担するのか、セキュリティ上の脅威と対策レベルをどうするのか、市場戦略をどうするか等の観点を入れながら考えていかなければならない。
  - サプライチェーンリスク対策において発生するコストについては、その削減を図る観点だけではなく、調達先を育てるという観点、供給者との互恵関係という視点が必要ではないか。また、サイバーセキュリティ対策は社会全体にとって重要な問題であるから、どのようにコストに関する社会的受容性を高めていくのか、考えなければならない。
- 日本の戦略として、海外の認証の動向等に追従していくということであれば、海外の動きに対応できる体制を整えていくことが必要である。一方、日本が標準化を先導するという戦略であれば、実際に事案が起きた際に、膨大なサプライチェーンの中で何が原因で誰に責任があるのか等を適切に把握できる仕組みが必要である。
  - 「サイバー・フィジカル・セキュリティ対策フレームワーク」を上手く活用すれば、ガイドラインや認証等においてリードしていくことができる材料になるのではないか。
- リスクに対するアプローチとして、リスクをガイドラインで抑え込むということが果たして可能かということを考える必要がある。例えば、ドイツの製鉄所の事案等は結局、標的型攻撃であり、従来のガイドラインベースのアプローチでは抑え込めないところにリスクが顕在化している問題である。「Consequence Driven」という最悪の事態を想定しそこから逆行分析をする手法がある。このような相互補完的アプローチも必要である。
  - 標的型攻撃のように、今後のサイバー攻撃に対しては、最終的にはシステムで抑える、プラットフォーム的なところに技術として安全性を保障するようなアプローチも実施していく必要がある。
  - あらゆることに備えるシステムを作ろうとするとコストが膨大になるので、完全ではないものの、それを育てていく、ということに投資していくことが必要ではないか。

２．サイバーセキュリティ対策の実態把握について

（1） 「サイバーセキュリティ対策の実態把握」を事務局より説明。

（2） 「電力 ISAC の活動について～情報共有を中心に」を電力 ISAC より説明。

（3） 自由討議

- 事業者側はセキュリティを気にして情報を提供しにくい環境にあると思われるが、実際に事案が発生した際には速やかにエビデンスとともに資料やデータを提出できるような態勢が必要である。

- 現状把握の一つの方法として、各電力事業者は自社の対策を相当に実施していると思われるので、お互いに協力してまだ十分に対策がし切れていないところを探せばよい。例えば、監査役監査や内部監査・検査の計画や手法、構造を調べてみるとわかることも多いのではないか。

- 欧州では、NIS Directive により重要インフラに関する報告義務を各国に課している。そういうEU 圏と日本は法的にリーガルフレームワークが互換である、そういうリーガルランドスケープにあるのだという認識が必要である。

- 米国では、エネルギー省が C2M2 というガイドラインを策定し、米国の 2,000 社以上の電力事業者がサイバーセキュリティ成熟度モデルで自己点検できるようになっている。ただし、セキュリティ対策の取組み状況を紙で報告させると膨大な量になり多大なコストが掛かることになるので注意が必要である。また、米国の SEC ディスクロージャーガイダンスではサイバーセキュリティに関する事項の開示が定められている。日本の上場企業もどのように開示していくべきかというレベルの議論も必要ではないか。

- 今後どのような情報をどう効率的に集めるかという問題は、議題１における議論と接合した範囲の情報まで目を広げて収集をお願いしたい。

３．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について」を事務局より説明。

（２） 「会員企業の情報セキュリティ対策ベンチマーク自己診断結果について」を電力広域的運営推進機関より説明。

（３） 自由討議

- 今回の自己診断の趣旨は、主に追加した 3 項目についてしっかりと確認したいということであり、まずは会員企業自身がどのあたりに位置付けられ、弱ければ危機感を持っていただくというファーストステップとして実施したものである。

  - 次のステップに進める検討を行うのであれば、C2M2 を検討候補にするとよいのではないか。ただし、結構深いので対象は選ぶ必要があるかもしれない。また、電力業界向けの独自項目についても、大変立派な取り組みなのでここも拡張することを考えられたら良いのではないか。

  - C2M2 をそのまま利用すると、日本の事業者の観点からするとちょっと記載粒度が不足する点もあるので、調整が必要である。また、マネジメントレベルの自己評価なので、それだけでは不足する点はシステムレベルで評価する等の工夫も必要である。

  - 平均値で纏めている点に加えて、分布も含めて分析されると良いのではないか。30 あるドメイン毎に分布のグラフや指標のレベル等が非常に重要だ。

  - 成熟度５の会員企業には、是非ヒアリングをしてもらいたい。また、ベストプラクティスとして共有し、場合によっては表彰するようなことがあっても良いのではないか。

  - 独自追加項目は非常に良い項目が追加されている。今後は、システムとしてどのように最低限出来ているかと言う点とネットワークのアクセス管理などの具体的な運用の項目を明確に分けて整理されると、より一層議論が深まるのではないか。

- 新規プレーヤーも多様化している。その中で、サイバーセキュリティに関わる人材がどのように育成され、どのようなキャリアパスを歩んでいくのか、これらをきちんと調べていただき、具体的な事実を把握したうえで対策を講じていただきたい。

（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