産業サイバーセキュリティ研究会　WG１ 電力 SWG（第２回）議事要旨

日時　：　平成３０年９月４日（火）１５時００分～１７時３０分

出席者：

（座長）渡辺　研司　　名古屋工業大学大学院

青木　一彦　　電気事業連合会

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

桑名　利幸　　情報処理推進機構

高倉　弘喜　　国立情報学研究所

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

中谷　昌幸　　JPCERT/CC

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．第１回の議論内容と第２回の論点等について

２．事業者におけるサイバーセキュリティ対策の取り組み報告

３．自由討議

４．サイバーセキュリティ課からの取り組み報告

要旨

１．第１回の議論内容と第２回の論点等について

・「電力分野におけるサイバーセキュリティを取り巻く状況と目指す方向」、「電力 SWG での検討全体像（案）」及び「第１回の議論内容と第２回の論点」について説明。

２． 事業者におけるサイバーセキュリティ対策の取り組み報告

（１） 危機管理体制等について

・ 危機管理の一例として、リスク管理委員会を設置し、当該委員会が（サイバーセキュリティを含む）グループ全体のリスク管理を一元的に統括し、リスク顕在化時の委員長の意思決定を補佐している。またサイバーセキュリティに関しては外的要因の変化・対策進捗状況を定期的に取締役会に報告している。

・ 非常災害対策本部内にサイバーセキュリティ班を設置し、非常災害体制とセキュリティ管理体制が連携している。

・ Security Incident Response Team （SIRT）と Security Operation Center（SOC）の役割分担を定義し、機能を分担している。

（２） 合同演習の実施等について

・ 社外連携の一例として、重要インフラ・重要産業事業者、大学、行政・警察など、セキュリティ情報の共有・施策連携を目的としたコミュニティ活動、合同演習に参加している。

・ 社外連携は、情報共有や知見獲得、有事対応能力の強化に加えて、セキュリティ人財の育成及びモチベーション向上の観点でも有用である。

（３） 人材の育成等について

・ 人材育成の一例として、既存組織体を活用した３つの専門技術部会（情報システム・制御・エネルギー）が相互に連携し、それぞれが有する知識やノウハウの共有を進めている。

・ 制御セキュリティ人材の育成として、情報処理推進機構（IPA）の産業サイバーセキュリティセンター（ICSCoE）の中核人財育成プログラムに人員を派遣している。

３．自由討議

（１） 危機管理体制の構築、人材の育成

・ IT と OT のセキュリティ体制を組織的、人材育成・交流の面で融合していく必要がある。

  ➢ 組織的には、元々IT 部門が担当していたセキュリティ管理を社長直属組織とし、ここに IT 部門と OT 部門のメンバーを集めて議論ができる体制とした例もある。

  ➢ OT と IT では可用性、機密性等の考え方の違いがあるので、相互に補完していくためにも、OT から IT に対して与えられる気づきにはどのようなものがあるかという点は体制構築を考えるうえで重要である。

  ➢ 一般電気事業者・ベンダーが，これまで培ってきた安全・安定供給の知見を IT，OT セキュリティに生かすことが能率的だ。

・ 人材育成・交流の点では、IPA の ICSCoE に OT 部門と IT 部門のメンバーを派遣し交流している例もある。OT 部門のメンバーにとっては、リスクを肌で感じる重要な機会となり意識も変わってきたという意見もある。

・ 電力の安定供給のための安全、可用性の確保が一番重要だ。

・ リスク評価の実施にあたっては、情報セキュリティ部門とライン部門が共同で実施することが重要である。また、社内管理体制としては、ライン部門に対する規程を策定しマネジメントサイクルを回す、インシデントレスポンスや社外コミュニケーション、ガバナンス教育等を実施していくような組織を作ることが重要である。

・ セキュリティと事業をバランスさせるためには、品質・マネジメント・プロセスの観点で、事業者が健全に事業を実施できるような適切な人材構成とすることが重要である。

・ これまで制御系が日本の品質を支えてきたと認識を新たにした。そのうえで、OT と IT の接点となる組織をどのように位置づけるかという視座が重要である。

・ 体制を構築する際には短期、長期を考える必要があり、大切なのは経営トップがどのようなメッセージを出すかだ。また、IT と OT のリスク管理をどう融合させるかを検討すべきである。

（２） 事象発生時の対応強化

・ 危機管理体制については適切な相手との連携が大事だということが各事業者からの報告に共通している点である。

  ➢ 特に、自治体、警察とは常に意思疎通ができるような連携体制を作ることが重要である。

  ➢ 災害時と同様に、電力の安定供給ができなくなった場合には自治体や警察等に情報が連携され対応される枠組みが必要であり、この枠組みはサイバーだけの為に構築される必要はなく、既存の災害対応の枠組みに接続されるようにする必要がある。

・ ２０２０年を見据えると送配電の分離を念頭に、発電事業者と送配電事業者との関係でどのようにセキュリティ対策を実施するか、どのような役割分担と体制を構築するかを考える必要がある。また、新規参入事業者とどのように連携していくかも検討が必要である。

  ➢ 現在、新規参入事業者にも電力 ISAC への加入を依頼しており、情報共有体制が進められているところだ。

・ 危機管理や人材育成等の各論に偏ることなく議論するためにはフレームワークが必要であり、経済産業省から説明があった「サイバー・フィジカル・セキュリティ対策フレームワーク」は重要である。また、電力事業者にとっては何よりも Safety（安全）が重要である。

・ 「戦略マネジメント層」が経営層の直下であれば専属のメンバーで良いと思うが、その候補となる層のメンバーは専属ではないが求められる役割は果たすことができて普段は本業を行っている人、そのような人が各部署にいなければ実効性は上がらない。

  ➢ 「戦略マネジメント層」の候補としては、セキュリティに関する研修受講や資格取得の地道な取り組みを行いながら、経営層とのパスを持つ経験豊富な社員等を適材適所で配置していく必要がある。

  ➢ 長期的には、職種によって流動する人材を作るのか否かは考える必要がある。

- 「戦略マネジメント層」には経営層とセキュリティ部門の単なる橋渡しではなく、サイバーセキュリティを最大のビジネスリスクの一つとして認識したうえで、中期経営計画の策定やセキュリティ予算の割り当てを行う役割が求められている。
- 「戦略マネジメント層」は専門職ではなくライン職として経営ファクターで物事を考えられる人材を育てていく必要がある。

・ 危機管理体制や「戦略マネジメント層」の育成等の企業の取り組みが開示され、社会から評価されてその企業価値に結びついていくようなことがあると企業も取り組みやすいのではないか。

- WG２でいかにサイバー経営に取り組むかということを議論している。その中で、例えばコーポレートガバナンス・コードで求められている取締役会の実効性評価の項目にサイバーセキュリティを加えることで、サイバー経営への取り組みを促す等の議論があった。

４． サイバーセキュリティ課からの取り組み報告

・ 「サイバー・フィジカル・セキュリティ対策フレームワーク」を説明。

（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