産業サイバーセキュリティ研究会
ワーキンググループ2(経営・人材・国際)(第3回) 議事概要

1. 日時・場所

日時:平成30年11月9日(金) 14時00分～16時00分

場所:経済産業省本館17階 第1共用会議室

2. 出席者

委員 :梶浦委員(座長)、岩下委員(欠席)、上野委員、小原委員、小松委員(代理:岡本様)、武智委員、塚本委員、名和委員(欠席)、林委員、藤原委員、丸山委員(代理:北野様)、宮嵜委員、宮下委員、湯淺委員、横浜委員(代理:荒金様)

オブザーバ:内閣官房 内閣サイバーセキュリティセンター、警察庁、総務省、外務省、文部科学省、防衛省、独立行政法人情報処理推進機構(IPA)、独立行政法人国立高等専門学校機構、一般社団法人日本サイバーセキュリティ・イノベーション委員会(JCIC)、株式会社アイ・アールジャパン

経済産業省:商務情報政策局 西山局長、大臣官房サイバーセキュリティ・情報化審議官 三角審議官、大臣官房審議官(商務情報政策局担当)成田審議官、奥家サイバーセキュリティ課長、土屋サイバーセキュリティ課企画官

3. 配付資料

資料1 議事次第・配付資料一覧

資料2 委員等名簿

資料3 事務局説明資料

資料4 一般社団法人日本サイバーセキュリティ・イノベーション委員会 資料(取締役会で議論するためのサイバーリスクの数値化モデル)

資料5 株式会社アイ・アールジャパン 資料(取締役会実効性評価を通じたサイバーリスクへの対応強化の現状)【非公開】

資料6 産業横断サイバーセキュリティ人材育成検討会 資料(産業横断サイバーセキュリティ人材育成検討会 人材育成に関する各種取り組みとの連携の在り方について)

資料7 サイバーセキュリティ人材育成スキーム策定共同プロジェクト 資料(NEC・日立・富士通による「サイバーセキュリティ人材育成スキーム策定共同プロジェクト」のご紹介

4. 議事内容

冒頭、西山局長から以下のとおり挨拶。

- コネクテッドインダストリーズ等により創出される「つながり」が拡大するのに伴い、その裏側で、サイバーセキュリティの問題が非常に重要になっており、その中で、この WG2 で取り上げるサイバーセキュリティに係る経営や人材の問題、国際的な関係は、非常に重要な要素である。
- 先日開催した ASEAN 諸国向け日米共同演習等の様々な実践的な取組と、研究会・WG を一体的に進めていく必要があると考えており、それらの成果についても報告していきたいと思うので、活発なご議論をお願いしたい。

次に梶浦座長から以下のとおり挨拶。

- 経営・人材・国際という非常に重要な 3 テーマをあずかる WG2 を開催することができた。
- 本日の WG2 の開催について、2、3 日前に報道で取り上げられており、また、この会合の開催に伴いセキュリティ関連企業株が上昇しているという報道もあった。
- 世間の注目は非常に高まっているところであり、このような中で有識者の方々から忌憚のないご意見を賜りたい。

本日の資料の中には投影のみの資料があるため、事務局より写真撮影は遠慮して頂きたい旨、発言があった。

ここから梶浦座長が議事進行をした。

事務局から、資料の確認、委員・オブザーバの紹介を行った後、資料 3 について説明を行った。

続いて、関係企業・団体プレゼンテーションとして、一般社団法人日本サイバーセキュリティ・イノベーション委員会から資料 4 について、株式会社アイ・アールジャパンから資料 5 について、産業横断サイバーセキュリティ人材育成検討会副会長、サイバーセキュリティ人材育成スキーム共同作成プロジェクト構成員である武智委員から資料 6 と資料 7 についてそれぞれ説明を行った。

その後、以下のとおり自由討議を行った。

（1）サイバーセキュリティ経営について

〇荒金様

- 経営の観点からサイバーセキュリティを考えたときに、リスクをどうとらえるか、それをどのように自社のビジネスにブレイクダウンして、実効性を持たせていくために、取締役会レベルから現場まで、幅広い計画、戦略や、計画、実行、そしてフィードバックを考えていく必要がある。
- セキュリティの専門的な知識だけでなく、経営的な観点での知識、経験が必要である。中小企業を含めた広い範囲だと、違った観点でのそれぞれの企業や業態、規模を含めての実効が重要である。
- 100%のセキュリティを求めるのは、企業経営の観点からすると現実的ではない。バランスをとりながら行うことが重要である。
- リスクが発生する確率と被害の影響に関して、確率が出しづらいというのは、その通りである。サイバー攻撃というのは自然災害と違って、確率ではなく、攻撃者が狙うか狙わないかという恣意的な部分に依存するものでもある。昨今の非常に洗練された攻撃を考えると、確率を考えるというよりは、もし狙われたら、ほぼ 100%で被害を受けるという前提をある程度持つことが必要と思う。
- もう一つ、狙われた時の影響という観点において、昨今、事業継続に影響を与えるような攻撃が相次いで発生している。企業によっては重大な被害を受けるものもあった。例えばこの事業が 1 週間止まったら、それは経営的にどう考えるのかといった、それぞれの企業のアセットや事業そのものに対してどのような重みをおくべきであるかというところまで踏み込んだ検討が必要である。

〇上野委員

- 今どきの経営層もサイバーセキュリティが経営リスクの一つであることは理解している。しかし、セキュリティ対策をどこまで行うべきか苦慮している状況である。JCIC がまとめた情報漏洩に伴う株価下落率などの資料は意識喚起には有効であろう。
- しかしながら、事故を回避するためにはなにをすべきかを具体化しない限り対策にはつながらない。そのためには自社の対策状況の課題、これは絶対的な指標があるわけではないので、相対的な評価に基づき具体化する必要がある。例えば本 WG で進めているベンチマークなどが自社の立ち位置と課題を知る意味で有効

であろう。
・ 立ち位置を知れば、なにをすべきかを絞り込むことはできる。が、セキュリティ対策は保険と同じで、具体的な対策をどこまで講じるべきかを決めるのは難しい。その一助とすべくサイバーセキュリティ人材育成検討会では会員企業の対策状況を個社が特定できないように配慮しながら公開したいと考えている。

○藤原委員
・ セキュリティの担当者たちがどれだけ危機感を持って話しても、経営層に中々サイバーセキュリティの重要性が伝わり難いと思いながら孤独な戦いを強いられている中で、彼らのモチベーションを維持するのが大変だという話を CISO の方々などから聞いている。彼らにモチベーションを持って戦っていただくためには、経営層に理解してもらう必要がある。
・ 経営層に理解させるには、セキュリティリスクを数値化して伝えることが重要である。このための数値化モデルは、日本サイバーセキュリティ・イノベーション委員会の Web サイトで「取締役会で議論するためのセキュリティリスクの数値化モデル（以降、数値化モデルとする）」Excel ファイルにてダウンロードできる。数千件以上ダウンロードされているので、かなりニーズが高いと感じている。この数値化モデルは経営層を説得できる材料にもなるはずであるので、もう少しこのモデルを深堀していきたい。
・ また、これからの課題として、すでにセキュリティリスクを経営課題ととらえている企業において、取締役会、ボードミーティングで、どのような取り上げ方をしているかを深堀して、事例として皆様にお見せしたい。

○小原委員
・ この数値化モデルは、メディアでも取り上げられて大分反響があったと理解しており、一石を投じた。
・ ISF（Information Security Forum）の中で議論されていたことをご参考に報告する。経営層の数字の見方と CISO の数字の見方は、真逆である。CISO は未来から現在を見て、経営層は現在から未来を見ており、方向が逆なので、そこを十分に理解する必要がある。経営層は KPI を意識し、一年後、二年後、三年後にいくら売り上げが伸びるとか、利益率はいくらなどという見方をする。一方で、CISO は KRI（key risk indicator）で意識し、リスクがどれくらいの確率で起きるかという議論になる。そうすると、今度はその確率をどうコントロールしていこうかという議論になる。その際に大事になるのは、地味だがスコープを決めることと、データを確実に取得することである。どれくらいの確率であるとか、どういう目盛り(Calibration)で捉えるか等を議論できると理解が深まる。そのあとレビューをどのようにすべきかの議論に繋がる。
・ セキュリティに関しては、定性評価という伝統的な方法がある。どういうリスクについては定性評価を用いて、どういうリスクについては定量評価を用い、場合によっては両方の評価方法を用いるといったことを、産業や企業の形、或いは状況に応じてどのように使い分けるべきかといった議論をフォーラムの中で行っている。

○宮下委員
・ ユーザー企業で、現場や担当者から経営層に伝えても理解しているとの返事はあるが、現実感を持って理解してもらうのは難しい所がある。数値化モデルは経営層の理解を進めるためにも重要である。
・ 数値化モデルのような共有モデルは、事業に対してセキュリティリスクが発生すると事業面や経営面で見たときにどのようなインパクトがあるのかという視点が入ると、経営層も理解しやすくなり、前向きにとらえるはずである。そういう事例があれば、共有してほしい。
・ 経営層はリスクの話ではなく、ビジネスそのものに影響があると言った方が関心を持つ。経営にリスクを説

明しても、経営層の関心が違っていましたという事例も出ている。

○林委員

・ 官庁に勤めている方は、大体その官庁か局単位の“なんとか六法”があり、机の上に置きながら仕事をしている。これは、ボディ・オブ・ナレッジの基になっているので、例えば“情報セキュリティ六法”などを整備する必要がある。
・ 法律は一番保守的な学問であるので、専門にしている人たちも保守的であり、CISO や CIO の方針に対して、ゼネラル・カウンセル（法務担当役員）などの法的なバックグランドがある人は、職務上、やや足を引っ張る方向になることもある。
・ しかし法曹界でも、サイバーセキュリティ自体は関心高く、コーポレートガバナンスにも連動していくので、無視できなくなりつつある。
・ アメリカでは、サイバー・スレッド・インディケーター（CTI）やディフェンシブ・メジャー（DM）などを共有する際、民事や刑事のペナルティを課せられない等の免責規定など、様々なことが整備されている。日本においても、そのような免責事項を整備すべきか、検討する必要がある。同様に、限定提供情報という概念が知的財産の分野で主体的に検討されており、セキュリティ分野においては脆弱性情報等に関しても同様の扱いを検討すべきである。

○上野委員

・ 2007 年に金融商品取引法が施行されて、各企業が慌てて対応したことがあった。同様に、コーポレートガバナンスコードへの対応状況が公表されると、いわゆる経営の通信簿が付けられて公表されることになるので、経営のリーダーシップを引き出す一つのファクターになると期待している。
・ セキュリティ対応は、基本的にリスク対応や守りの投資、コストであるので、どこまでやればいいのかというのは相対評価でしかない。その相対評価の中で、人並みになるのに何をすればいいのかを検討することで、経営層のさらなる意識改革につながっていく。
・ 産業横断サイバーセキュリティ人材育成検討会の中で様々な事例を共有しているが、非常にレベルの高い管理を行っている企業は、「数える」ということをしている。例えば、管理下の PC は何台あるか、それを誰が使っているか、修正プログラムをあてるべきサーバは何台あるか、ということを経営層にきちんと報告されている。
・ 最近よく議論になるのは、日々の構成管理の重要性についてである。“セキュリティ構成ガイドライン”といった構成管理ガイドラインが整備されると、これに基づいた取組みが可能となる。
・ コーポレートガバナンスコードという非常にマクロなところ、ベンチマークという一定の指標に基づくミクロなところ、さらに、実態として何をするのかという具体的なところの三点セットがまとまると、経営と現場がスムーズにつながって共有できる状態になると考える。

○宮嵜委員

・ 現場を回っているが、大きな企業の経営層はある程度セキュリティリスクに対しては、経営リスクという認識がある。一方で、地方に行くと、中小の経営層は、まだまだ認識が浸透していない。まさにその辺のレベルから上げる必要があるのが、日本の現状である。昨今言われているサプライチェーンだとか、取引企業や関連企業だとかは、まだまだそのような状態である。セキュリティリスクを経営リスクと認識していない中小の経営層に対して、まずどのように理解してもらうかを早急に考える必要がある。大手企業だけがリスクを認識し、自分の所だけを守り、BCP をしっかり整備しても、サプライチェーン全体で考えるとリスクは残

る。
・ 資料 3 の 24 ページのサイバーセキュリティお助け隊に関連して、我々も日本全国各地の代理店網を使いながらセミナー等も開催しつつ、そのサイバーセキュリティのレベルの底上げに、取り組んでいる。経営という視点で、確実に対応する必要がある。

○岡本様
・ 日本商工会議所は、セキュリティ対策の推進の前に、そもそも中小企業での IT 活用を推進する活動を行っている。そうした中、今年は IT 導入補助金として 500 億円という非常に大きな額が確保され、「SECURITY ACTION」を宣言するのが申請の条件になった。IT 導入の最初の段階でセキュリティについて考えるきっかけになったとすれば、非常にいい機会だった。
・ 中小企業数は国内に 380 万者と多いことから、サイバーセキュリティお助け隊という形で中小企業の実態を把握することにより、セキュリティに関するニーズを把握していただけることは非常に心強い。どのようなことをすれば中小企業のセキュリティ対策が進展するかを一緒に検討したい。
・ IPA は IT リテラシーに関する IT パスポート、セキュリティに関する情報セキュリティマネジメントといった資格を用意している。これらの資格を取得したからといって十分とは限らないが、「SECURITY ACTION」は組織としてファーストステップであり、IT パスポートは IT リテラシーのファーストステップ、情報セキュリティマネジメントはセキュリティのファーストステップとして、三点セットで進めようと考えている。

○藤原委員
・ サイバーセキュリティお助け隊に関連して、地方創生等の他の政策とかけ合わせることで、より相乗効果が出ると認識している。例えば、地方大の先生方とよく議論をするが、地方でサイバーセキュリティを学んだ学生たちが卒業すると、生まれ育った地域に住みたいという意識が高いにも関わらず、働き場所の都合で東京や大阪といった都会で就業する。都会でサイバーセキュリティの専門家として育ち、地元に戻って地域に根付いた活動を行えば、地方創生の観点でもさらにプラスの要因になる。様々な政策と一体化した活動により、よりサステーナブルになる。

○奥家課長
・ 法律的な課題に関して、例えばアメリカは、情報提供、情報共有の際のリライアビリティ・プロテクションが導入されており、いくつかのケースがあって、その辺は把握している。例外措置を行うことが定義づけされて初めて、リライアビリティ・プロテクションを導入することが可能となる。日本の場合、どのようなケースにおいてリライアビリティ・プロテクションを導入するべきであるかの定義がまだできていないのが、導入されていない一番大きいポイントである。
・ リライアビリティ・プロテクションは、免責をするというアプローチの仕方と、NISC で中心に議論して国会に提出されているサイバーセキュリティ基本法の情報を提供する義務を持たすというアプローチの仕方がある。後者のアプローチの仕方を意識してリライアビリティ・プロテクションを意識している。
・ 限定共有情報に関しては、日本がコネクテッドインダストリーズや Socety5.0 みたいな社会が実現したときのデータの持ち合いとなったものである。今までは個社が営業秘密で単独でもっていた情報だが、グローバルつながって付加価値を創造する社会になってきているため、その中で企業機密に近い情報として守るべき情報や共有するべき情報の新しい概念や定義、枠組みを整備することで、プロテクションすることが出来る。
・ 付加価値の作り方が変わったことに対して、付加価値の原点になっている営業機密に関して、個社だけに置かれず共有することがコアになる概念をスコープ入れることがポイントである。

・ そういった情報を区分して管理していくということが重要になることを視野は入れており、産業サイバーセキュリティ研究会 WG1 のサイバー・フィジカル・セキュリティ対策フレームワークの議論の中で情報を区分して、それに見合った対応しなければいけないと記載している。
・ 一方で、企業間の契約の最終段階において保険に加入する規程は、アメリカと比べて日本はほとんどない。法的な措置の仕方についてのマチュアリティや契約に関して、事例をまとめて検討する必要がある。
・ ただ一方で、産業構造の違いがあるので、その辺はセキュリティという観点だけではなく、幅広い視点でみていく必要がある。可能な限り情報収集を行っているが、本 WG において各委員からの共有もお願いする。

（2）サイバーセキュリティ人材の育成について

○湯淺委員

・ 以前より企業が求める人材のニーズに対して大学や教育機関が応えてくれないというような不満もあったかと思うが、見える化をすることで、企業の中でどういうスペシャリティーを持った人材が必要で、企業で人材が現実的に活用されているということがわかる。それに応えるためには、どのような教育プログラムを作っていけばよいのか、わかりやすくなる。
・ 一方で本日の議論は、現実に企業で活躍している人材や企業が必要としている人材についての見える化をしていただいていると思うが、むしろもう少し上のレベルで、戦略的に育成していくべき人材はどこなのかという議論が必要だとの印象も受ける。資料 3 の 32 ページの人材育成のピラミッドの中で、右側が技術寄り、左側が経営寄りだとすると、依然として左側（総務系、経営系）の整理があいまいである。大学側としても考えていかなくてはならない。
・ 高専との連携については、私ども情報セキュリティ大学院大学も、木更津高専との交流がある。最近は成長分野を支える情報技術人材の育成拠点の形成(enPiT)における高度 IT 人材の育成では、当初は大学院生向けであったが、大学の学部生向けの展開が開始されている。
・ ただ、資料 3 の 45 ページ左側に示されるような 1%部分の人材（主にセキュリティ企業で活躍するトップガン人材。以下、“1%人材”とする）というのはトップレベルなので、いろいろと教育できているが、残りの 20%部分の人材（同じく資料 3 の 45 ページ左側に示される、主に IT 企業で活躍する情報系人材。以下、“20%人材”とする）と 80%の人材（同じく資料 3 の 45 ページ左側に示される、主にユーザー企業で活躍する非情報系人材。以下、“80%人材”とする）を学部や高専のどのくらいのレベルから教育していくかについてが、手探りの状態である。今後、そのレベル感やボリューム感を考えていかなければいけないというのが印象である。

○武智委員

・ 技術寄りの人材定義のところは、次第に明確になってきている。戦略マネジメント層の育成については、IPA 産業サイバーセキュリティセンターの戦略マネジメント系セミナーの活動に関わっているが、どう教えればよいか難しいと感じている。企業においてもセキュリティをどう扱うかというプラクティスの蓄積がない。
・ 資料 3 の 45 ページの高専における学生の内訳に関連して、企業では“80%人材”のような、主にユーザー企業で活躍する非情報系人材をどう育てるかが問題。“1%人材”はベンダー企業や政府等で、“20%人材”は IT ベンダー企業等で育成しているが、“80%人材”をどう育成するかについて、大学で何を学ぶかを含めて整理が足りていない。産業横断サイバーセキュリティ人材育成検討会でも産学連携に手探りで取り組んでいるが、なかなかうまくいかないところもあり、今後の課題だと思っている。

○宮下委員

・ ユーザー企業にいる人材のほとんどは“80%人材”に当たると思う。通常、一般のユーザー企業が採用を行う際、セキュリティ人材という観点で採用を行うことはほとんどない。日本の新卒の採用形態は、通常はその企業の業務や事業に関連して採用された人材の中から、IT やセキュリティといった役割、タスクにアサインされるケースが多い。
・ その場合に、学において、最低限、のリスク、セキュリティに関するリテラシーは十分に教育する必要があると思う。他方で、セキュリティに対するリスクは、企業の形態、業種、規模によって異なるので、企業と連携しながら、どのように育成するかを検討することが必要である。
・ JUAS で実施している情報セキュリティワーキンググループでの議論を聞いていると、突然セキュリティ担当にアサインされ、何をすればいいのか困惑する方が結構多い。そういう人たちをどう支援していくかが重要である。TIPS 集を作成しているので、これをベースにして、教育などのプログラムを作成していけたらと考えている。

○藤原委員
・ 資料 3 の 34 ページのセキュリティ人材のピラミッドに関連して、左側の経営戦略に関する人材を手厚くカバーしていくことが非常に重要であり、現在 JCIC でレポートをまとめている。ピラミッドの図において、特に左下にあたるような総務、法務、広報といった、全く技術分野ではない人にセキュリティリテラシーを持たせることが必要ではないかと考えている。
・ セキュリティリテラシーを持っている人材を、「プラスセキュリティ人材」と呼ぼうという話をしている。このプラスセキュリティ人材の育成に向けて、今後様々な取り組みがなされていくべきである。

○小原委員
・ この夏に ISF で人材に関してレポートを作ったので、概要を紹介する。セキュリティに関するワークフォース（workforce、労働力）がサステーナブル（sustainable、持続可能）でなければいけないという前提を置いた上で、2000 年から 2020 年に向かって求められる役割が変遷しており、異なる能力を持ったセキュリティ人材の需要が移っていくという。
・ 現在でもセキュリティ人材も IT だけを理解していれば十分だった時代から、経営に関することも理解していなければいけない時代になってきている。リーダーシップに関しても、最初は CIO が行っていたが、今は CISO が行っている。最近は CISO が CIO にレポートするのではなく、取締役会に CISO が直接話をすることになっているという事例もでてきている。
・ 今は、スキルや実際の経験等が役に立つが、これだけでは今後はコンピテンシー（行動特性）が不足するという議論がある。これから必要な能力は、従前の能力に加えて、アプティテュード（aptitude、適性）、アティテュード（attitude、姿勢）、ブロードエクスペリエンス（broad experience、幅広い経験）であり、要するに、経営を理解して取締役会でコミュニケーションができることである、という。一個人ではすぐには身につかないので、バジェットプランを踏まえて、色々な特性を持った人間のチームで全体の能力設計をすることが必要になる。
・ 現実的にはセキュリティはチームプレイというが、およそ半分はベンチにいる可能性もある。本当に全員野球をしてパフォーマンスを出せる設計を作ることが最適である、との指摘が興味深い。

○上野委員
・ セキュリティに関するスキルや知識を計測することは可能であり、技術者のレベル分けは可能である。一方、セキュリティに関して現場と経営層をつなぐ人材が、まさに課題である。経営層に対して、セキュリティ意

識の喚起やリスクを見える化して伝達することが、非常に重要である。適切に現場の言葉を経営層の言葉に換言していく人材が非常に大事で、産業横断サイバーセキュリティ人材育成検討会では、「セキュリティ統括人材」と呼び、育成する取り組みをしている。

・ セキュリティは、非常に専門的なフィールドであるで、アウトソーシングのフィールドがかなり大きい。そのアウトソーシングの現場で出てきたセキュリティに関するアラートやインシデントを、その企業の言葉に換言することが出来て、さらにはシステムが与える事業的な影響や経営の影響、対外的な影響を察知して経営層まで確実に報告して指示を受けるまで出来る、アウトソーシング先と自社組織の間をつなぐ人材が必要である。

・ そのような人材の育成方法は、小原委員の発言にあるエクスペリエンスやセンスの問題であり、様々なレポートが出てきている。非常に難しい問題なので試行錯誤して行う必要がある。当面は、経営企画の経験者やセキュリティの経験者など様々な人材を集めて、一つの組織として対応する枠組みが必要になってくるのではないかと考えている。

○北野様

・ サイバーセキュリティを仕事にしている人が、経営者がわかる言葉、興味を持つような方法で、サイバーセキュリティリスクや重要性を伝えるようになるべき。技術的なスキルセットに比べて、経営層にセキュリティに関する情報を伝えるためのスキルセットの定義が難しいというのが、皆さんの認識であると思う。セキュリティ技術者が経営層に歩み寄るためには、経営のことを勉強してみても良いのではないか。学術的には、経営学側に踏み込んでみてもいいのではと考えている。

・ 短時間でサイバーセキュリティ人材が経営のプロにはなれないが、企業が経営資源である人・モノ・金をどのようにコントロールしていくべきであるか、企業が戦略的に舵をどのようにきっていくべきであるか、ということをスキルセットやベースシップ、ナレッジとして習得しておくと、経営層の視点を理解することや経営層へのセキュリティに関する情報を伝達することができるようになるのではないか。

・ 資料 3 の 42 ページ右側に記載のある一橋大学のプログラムの様なカリキュラムやスキルセットを、高度マネジメント人材などの育成のために活用してもよいのではないか。

・ また、コミュニケーションスキルやロジカルシンキングといったソフトスキルをどう補っていくかを具体的に考える必要があると感じている。例えば、優秀な技術者が必ずしも優秀なコンサルタントになれるわけではなく、自分以外の、特にプロフェッショナルではない人たちに対して、どうわかりやすくロジカルに伝えることができるかが重要。

○塚本委員

・ サイバーセキュリティのエリアは、ニーズが高い上に、ベンダー企業間の異動以外に、ベンダー企業からユーザー企業、ユーザー企業からベンダー企業、官から民など、流動性が高い。スキルがあればどこでも行けるというところがポイントであり、労働人材の流動化促進の 1 つのロールモデルになる。

・ 高専との連携促進は非常にすばらしい取組みである。キャタピラージャパンは兵庫県の明石に工場があるが、高専の人たちに品質を支えてもらっている。“80%人材”に IT スキルを習得してもらうのは非常にありがたい。今までは組み立てラインに人をたくさん置いていたが、最近ではソフトウェア化が進んでいる。かつては、英語と IT のスキルは不要といわれてきたが、今はそうではなく、世の中の変化に応じたスキルへのキャッチアップに日々対応しているところとなる。現場に、IT 系のスキルもあり、メカも好きな人材に入社していただけると、21 世紀の日本の製造業の現場をリードし、支える人材になるので、ぜひ進めていただきたい。

○宮嵜委員

・ 金融の自由化になった 97 年以降、ほとんどのユーザー企業のシステム部門は、ベンダー企業に丸投げ状態が続いていた。合併等を繰り返す中で、中身がわからなくなってしまったため、ユーザー企業内にも有識者を増やしていこうということで、有識者のスキルマップを作成したものの、課題が二つくらいあった。一つは、スキルマップからキャリアパスがうまく導き出せなかったという課題と、もう一つが評価する上司がいなくなってしまっているという課題である。システム部門については、この 2 つが大きな課題であるが、サイバーセキュリティについても同じく、有識者を指導できる人がどれだけユーザー企業内にいるのかが大きな課題である。

・ 例えば、イスラエルでは 8200 部隊など作って、そこで実習ができるという仕組みを国として構築しているが、日本はどうか。資格ばかりを作り、自動車運転免許を持っているけど、車の運転をしたことが無いような人ばかりだと意味が無いので、擬似的にでも、防御と攻めを両方できるような環境や仕組み等の整備と併せて取組を進める必要がある。

○梶浦座長

・ 日本の IT 人材、セキュリティ人材の大多数がベンダー企業に偏っている。アウトソーシングとは、そもそも自社の人間でも時間をかければできるが、外部を使って効率化や大規模化を図るものであるが、丸投げ的なアウトソーシングが横行している。そういった中で、アウトソーシング先からその企業の経営層に対してセキュリティに関するアラートやインシデントを直接報告することは、なかなか難しい。

（3）サイバーセキュリティにおける国際連携について

○小原委員

・ 戦略人材層､あるいは CISO に加えて経営層も交えて様々な議論を､ISF では年に一回集まって行っている。国際という意味では、ISF の母体はイギリスであり、英国政府とも話をしていて、協力してイベントができないかと検討している。

・ 日本でもフォーラムのメンバーがおり､外国政府のリーチもあるので､日本の企業とコミュニティを作って、様々な経営にかかわる問題、あるいは経営とサイバーセキュリティに関する問題の議論の場を提供したい。

○荒金様

・ 国際的な協調や連携において、その企業のグローバル展開の観点から、日米欧それぞれで異なったレギュレーションや方向性に対応するのは非常に大変である。企業にとっては負荷が大きくなるので、実際のサイバー攻撃に対抗するような実効性を持たせるようなバランスが需要である。

○北野様

・ 世界的にデータローカライゼーションの動きが加速していると感じており、日本の企業の活動がグローバリゼーションしていくことと真逆の方向に力が働いている。重要なデータは国内に保存するべきとか、我が国のデータセンターを使用するべきとかが、日本の企業のグローバルな活動の少し阻害要因になりつつある。

・ GDPR 対応で様々な企業の取り組みを見たが、日本全体の産業界で見ると、多くのコストを使っていると認識している。同様に他の様々な国の法律での対応が必要になると、国際競争力を考えると、望ましくない。

・ 安全保障の問題に関して、少なくとも民間企業が産業界で事業活動をしていくうえで必要なデータの流通、データの活用とか、国際間でうまくデータを流通させるための基本的なルールや基準作りは、国の通商政策

の一部として考える必要がある。

・ 大きなテーマの一つとしてサイバーセキュリティや個人データの保護が上がっているが、グローバルなリスクとして経営も考える必要がある。グローバルガバナンスやリスクをグローバルでどうコントロールしていくか、海外で起こっているデータローカライゼーションにどのように目配りをしていくかということは、グローバルなグループ経営という視点では、十分に検討する必要がある。

○梶浦座長

・ 資料 3 の 53 ページの ASEAN 等向け日米サイバー共同演習概要に関連して、ASEAN の各国で大きな動きがあり、当然日本も国際的な流れに入っていくことになる。ルールは世界で共通が望ましいのは、まったくその通りであるので、インターネットエコノミーの世界では、可能な限りルールは全部共通にするべきであるということを産業界としてもずっと主張していたことでもある。

・ ただ、セキュリティに関しては、国際関係や国際情勢と密接な関係があり、安全保障の議論にもなる。ここは経済産業省の WG であるので、そこまでは踏み込むのは難しい。

・ グローバルにおいてのデータ流通に関しては長くかかわっており、フリー・フロー・オブ・データは、様々な競合や条約に入っているが、中に例外条項があり、サイバーセキュリティを言い訳にしたデータローカライゼーションというものは、昔からよくある。そのような制限を極力減らすための、例えば、ASEAN 地域であると RCEP、あるいは全世界で TiSA、もちろん、TPP の第 14 章、といった活動をしていきたい。

○奥家課長

・ 通商政策の中では、データ流通については、かなり大きなエリアになっている。APEC、世界データの CDP、TPP、RCEP でも大きいポイントになっており、通商政策サイドで検討をしている。様々な要素が絡んでおり、セキュリティ的な要素もあるのでし、新しい付加価値の源泉をどのようにグローバライズしていくのか、全ての要素が複雑に絡むので、一律にはいかないと思うが、通商政策サイドは戦略的に検討を進めている。

梶浦座長よりまとめ

・ 人材に関しては、幅広い人材モデルがあるということと、経営視点の人材育成の話があった。また、産学のギャップを埋めるためのロールの規程やそれを参考にしたカリキュラムの考え方についての発言や、高専、enPiT の発言もあった。技術的な人材に関してはかなり整理が進んできた一方で、経営側の人材は今後整理していくべきとの発言があった。また、差し迫った話として、突然セキュリティ担当にアサインされて困っているといった事例が、委員から提示された。さらに、アウトソーシングについての議論があった。契約にも関係してくる話である。また、ベンダー企業・ユーザー企業間や、官民間などの人材の交流が、セキュリティ分野を皮切りに盛んになっていくのではないかという発言もあった。

・ 経営に関しては、リスクの頻度やインパクトについての発言があった。コーポレートガバナンスコード、経営の見える化、サイバーリスクの見える化、こういうものが非常に有効であるということと、情報セキュリティ六法みたいなものの必要性などの発言があった。

・ 以上のような点で、おおむね事務局でまとめた資料に対して、肯定的な意見がほとんどであり、本 WG は、正しい方向に向いた議論をしていると感じた。

○事務局より次回日程について連絡

・ 今後のスケジュールについては後日ご連絡させて頂きたい。

以上

お問合せ先

商務情報政策局　サイバーセキュリティ課

電話:03-3501-1253