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4回) 議事概要

1. 日時・場所

日時:平成31年3月29日(金) 16時00分～18時00分

場所:経済産業省別館11階 1111各省庁共用会議室

2. 出席者

委員 :梶浦委員(座長)、岩下委員、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、林委員、藤原委員、丸山委員、宮嵜委員、宮下委員、湯淺委員、横浜委員(代理:松原様)

オブザーバ:内閣官房、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、株式会社アイ・アールジャパン

経済産業省: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、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 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5 一般社団法人日本情報システムユーザー協会(JUAS)資料(ユーザ企業におけるセキュリティ体制の構築及び戦略マネジメント層の育成に関する実態調査 報告)

資料6 独立行政法人 情報処理推進機構(IPA)資料(登録セキスペ実態調査 報告)(非公開)

参考1 サイバーセキュリティ経営ガイドラインVer.2.0 実践のためのプラクティス集

参考2 中小企業の情報セキュリティ対策ガイドライン第3版

4. 議事内容

冒頭、梶浦座長から以下のとおり挨拶。

- WG2 は、与えられているテーマが、経営、人材、国際と多方面で、幅広い見識の皆様にお集まり頂き、多方面から意見を頂いてきた。
- 先週、OECD のワシントン D.C.のイベントに行ってきた。ゴーイング・デジタルというものを OECD では数年にわたって続けてきた。その中の一つに、サイバーセキュリティの話題があった。人材不足、人材の配置、経営者の意識不足、情報共有の仕組み不足。日本で起きていること、いま皆様にご議論いただいていることと変わらないことが、各国で議論されている。決して日本として周回遅れではないと確信している。
- 本日も忌憚のないご意見を頂きたい。

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、委員とオブザーバの紹介を行った

事務局から、本日は小松委員の代理として、岡本様、横浜委員の代理として、松原様が、出席の発言があった。

また、オブザーバとして、株式会社アイ・アールジャパン、独立行政法人国立高等専門学校機構、独立行政法人情報

処理推進機構(IPA)が出席の発言があった。

事務局から、資料 3 についての説明を行った。

続いて、関係企業・団体プレゼンテーションとして株式会社アイ・アールジャパンから、資料 4 について宮下委員から、資料 5 及び資料6について、独立行政法人情報処理推進機構(IPA)から、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)　経営に関して

○岩下委員

- 基本的にセキュリティは、目的ではなく手段。セキュリティが高いだけで良いことはない。不正アクセスや情報漏えいが無いのが当たり前。その上で、自分たちのビジネスが上手くいけば良い。それがセキュリティの本質。
- 総務省の通信白書での日本、アメリカ、イギリス、ドイツの IT の活用度調査で、日本は、トリプルスコアで負けている。日本は、IT を活用していないから、セキュリティが高いと見える面があるのではないか。また、ネットワークがクローズドなネットワークなので安心している面もある。
- IT を活用して生産性を上げるということと、セキュリティを上げることを同時進行していく必要がある。

○小原委員

- ISF(Information Security Forum)での成熟度の考えを共有したい。ISF での成熟度は、情報セキュリティと、ビジネスとをつなぐ触媒、カタリストであるという話をしている。成熟度のベンチマークは、4 つの視点がある。1)スタンダードに対してどうか、2)組織内でデコボコを比較する、3)同業他社と比較してどうか、4)取引先のセキュリティのマチュリティはどうか。それらを調べた結果の活かし方は、2つあり、経営のパフォーマンス・事業計画への影響、個別のセキュリティ施策、ミッションアシュアランスがどの程度できているか。いくつかの視点で成熟度を考えている。
- 持続的な成長のために、セキュリティを行っているので、持続的な成長に、どの程度効いているかの議論が、展開されると望ましい。

○名和委員

- 全体の資料を見て、現場とのギャップがあるように思う。あくまで現実は、インシデントが発生し、経営層へ報告のタイミングで、同席という立場だが、官が言っているからやらないといけない、と言っているだけ。それ以外の言葉を聞いたことがない。CISO が外部から入ってきて、やらなければと言ってやっている。CISO の下にいるセキュリティ人材の労力の 8 割は、経営層への説得という、残念な結果になっている。
- ベストプラクティスの位置づけだが、経営層が自ら自発的に、能動的に行うようには書かれていない。経営層にも自ら動く教育が必要。そのためにはファクト、数字が必要。傷みが伴うのは数字。

○梶浦座長

- リーダーの責任については OECD の会合でも話題に出てきた。チャンスがあるとすれば、アイ・アール ジャパンの言われていた、物言う株主。大きな損出が出る前に株主が物を言って、経営者の目を開かせるのは、一つのチャンスかと思う。

○藤原委員

- サイバーセキュリティは投資という話があったが、社長や経営陣に、サイバーセキュリティは投資だ、というとリターンを期待されるので上手くいかない。サイバーセキュリティは、事業を拡大させるために必要なもの、という説明をしていくべきではないか。

○塚本委員

- JUAS のサイバーセキュリティ経営の促進に向けた課題で、最近インシデントが少ないので、経営者の関心が下がっているところは、興味深い。IoT 関係のビジネスで、IT を使っている場面が、増えているにもかかわらず、個人情報の漏洩が無い、というだけで、経営者の関心が下がってしまうというのは、自分たちが、何をしているのかを、きちんと把握していないのではという気もした。
- 自社のアメリカの K10（有価証券報告書）を見ていると、リスクファクタの 7 つ目のところに、サイバーセキュリティがある。経営者が意識して書くようになると、サイバーセキュリティを含めて、より意識が上がるのでは、と思った。

○丸山委員

- 年齢層の高い経営者の方は、IT リテラシーが高くないので、日常の意思決定とセキュリティの間に距離感があると常々思っている。機関投資家と、投資家を交えて話をするのは良い手だと思った。
- コーポレートガバナンスができていないにもかかわらず、セキュリティだけでグループのガバナンスを効かせるのは無理。まずは、最適なガバナンス形態と、それに合ったセキュリティガバナンスができるような形にする必要がある。

○林委員

- 私は、1992 年に NTT アメリカの社長になり、ニューヨークへ赴任した。情報ハイウェイや、マルチメディアが興隆してくる時期だった。直感的に感じたのは、アメリカの経営陣は、これをどうやってビジネスに結びつけるか、とても敏感だったこと。日本では、80 年代を経験していたので、アメリカからはもう学ぶものがない、という感じだった。
- アメリカの生産性の改善は分かってもらえたが、全然分かってもらえなかったのは、ホワイトカラーの生産性。日本側に情報ハイウェイは、ホワイトカラーの生産性向上だ、と記事に書いたこともある。米国ではレイオフできるのでインセンティブがあった。今はずいぶん変わったと思う。労働力の効率化は、マイナス評価だったが、プラスになった。別の観点から見ると、働き方改革とつなげるなど、大きな議論をして欲しい。

○奥家課長

- 中小企業に、シンクライアントサービスの話をしている企業の例では、セキュリティ対策というよりも、テレワークできるようになると説明しようとしている。セキュリティ対策は、働き方改革と直結している技術要素が多い。色々なメッセージの出し方を考えていく価値はあると思う。

○上野委員

- 経営の意識は揺らぐので、定常的・継続的な対策と繋げていくためには、コーポレートガバナンスコードが有効。現場に落としていくには、プラクティス、可視化が有効。全体として一貫性を持ってまとまってきたと感じている。
- 新しいことをやろうとするときの、コーポレートガバナンスコードとのバランスが、課題。プラクティスは、まとまったが、セキュリティの鮮度サイクルが非常に早いので、継続的にやることが重要。

(2)　人材に関して

○小原委員

- 戦略マネジメント層に関しては、セキュリティ統括機能は、人材でもあるが、機能。機能は、組織として機能すれば良い。機能の定義を、ガバナンスコードへ反映できれば面白いのでは、と思う。組織内で機能する姿を描けると良い。

○梶浦座長

・ 機能については、事例集を示していくのが良いのではないかと思う。

○藤原委員

・ プラスセキュリティ人材は、セキュリティが専門ではないが、セキュリティを知っている人材。防火担当責任者のようなイメージ。ジョブローテーションを活用し、人材不足に対応できるのではと思う。

○松原様（横浜委員代理）

・ 人材不足に伴う問題については、米サンフランシスコで開催された RSA での人材不足の次の段階の話題があったので共有したい。基調講演で繰り返し出てきたのは人材のストレス。人が足りないので忙しい、SOC だとアラートが多い。燃え尽き症候群になりやめてしまう。残されたものは、さらに過労が重なり、ストレスが高まるという、悪循環に陥っている。そこをどうすれば良いか。まず、しなければいけないのは、ストレスの軽減。チーム内でのコミュニケーションが大事。その他の一因は、機微な仕事なので、ストレスを外部に出せないこと。職場のコミュニケーションが大事。如何に潤滑油を入れていくかが、リーダーシップの役割ということだった。

○宮嵜委員

・ ベンダにノウハウがあることや、IT 人材やセキュリティ人材が、多いのは分かっているが、それでセキュリティ対策が十分に出来ているか疑問。例えば、デフォルトのパスワードがそのまま設定されていたり、メンテナンスのためにパスワードがたらい回しになっている。ベンダ独自のパスワード設定などは、ダークネット上などにある。資格だけではなく、訓練をすることが大事。訓練する場を作ることが必要。

○宮下委員

・ 事業部におけるセキュリティには、使うセキュリティと売るセキュリティがある。ある会社は、売るセキュリティは、セキュリティ担当者を置いてきちんとやる。セキュリティ・バイ・デザインでやる会社もある。一方で、事業部にはあまりセキュリティのことは言わないで、のびのびやらないと事業のアイデアが出てこない、という会社もある。自由にやらせて、歯止めとして品質保証部門やセキュリティ部門がチェックする方が良いと、いうところもある。会社の事業の内容によって異なる。そういう視点も必要。
・ 5 年後に、定年再雇用の人が 20%となる会社が、3 割になると言われている。その時代になった時に、そのような人材の活用としてセキュリティ人材に求められるのは、高度な専門知識より、判断力やマネージメント力。シニアの人に専門知識はなかなか難しいが、マネジメント力は活かせる。そういった活用を考えていくのが、ポイントではないかと思う。

○丸山委員

・ 専門人材は、人材マーケットをきちんと作らないと、社会として育成できないと思う。
・ IoT などが出てきているが、セキュリティの前に IT リテラシー、基礎的な知識が必要。

○武智委員

・ 産業横断サイバーセキュリティ人材育成検討会でやっているのは、基本的には企業の中を今どうするか。タイムスパンは、ここ数年、前提は CISO、CIO にあまりリテラシーが無いこと。
・ 今後、人材の話を進めていく上で、長期スパンでどう考えるか、という視点を入れた方が良いと思っている。
・ 取締役が持つべき機能についても、あまり議論できていない。リテラシーを持っていない前提だったので。

・　資料3　p.40 のトップガン人材のところの話ができていない。今後やるべきと思う。

○上野委員

・　やめる若手の 7-8%はメンタル系疾患を抱えている。人材育成での大きな課題と思っている。

(3)　　地域に関して

○藤原委員

・　地方は、まだまだで、一般の方々へ伝えていくことはハードルが高いと思っている。皆様のご尽力により、十分な下地は整ったと思う。これから新しいステージに入って、これまでは伝える側の気持ちが強かったが、これからはどうやったら伝わるか、何を伝えたいかを前面に立てて考えていくのが、一つの手だと思う。

○宮嵜委員

・　企業や、地域によって温度差がかなりある。大阪の方では、特に温度差が大きくなっている感じがする。その中でも中小企業は、まだ、何故やらなければいけないのか、からのスタート。ボトムから上げていく必要がある。
・　サプライチェーンリスクについては、インシデントが起きた時には、取引に関して、経営危機に陥るというような話をしないと、なかなか腑に落ちないという感じがしている。税理士等と組みながら、如何に広げていくか、取り組んでいる。IPA で作られている中小企業の情報セキュリティ対策ガイドラインや、セキュリティアクションの宣言は、有効だと感じている。

梶浦座長よりまとめ

・　マチュリティ、成熟度をキーに色々なご意見を頂けた。一番関心があったのが、物言う株主。経営者のリテラシーもそうだが、メディアのリテラシーも上げて頂きたい。ご議論ありがとうございました。

○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く。

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