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6回) 議事概要

1. 日時・場所

日時:令和2年8月25日(火) 10時00分～12時00分

場所:TKP虎ノ門駅前カンファレンスセンター ホール2A／オンライン併催

2. 出席者

委員 :梶浦委員(座長)、岩下委員、小原委員、小松委員、武智委員、塚本委員、名和委員、藤原委員、丸山委員、宮嵜委員、宮下委員、湯淺委員、松原様(横浜委員代理)、和田委員

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、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:商務情報政策局 平井局長、大臣官房サイバーセキュリティ・情報化審議官 江口審議官、奥家サイバーセキュリティ課長

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 日本サイバーセキュリティ・イノベーション委員会 政策提言

資料5 サイバーセキュリティ経営ガイドライン Ver2.0 付録F サイバーセキュリティ体制構築・人材確保の手引き 第1版(ドラフト)

4. 議事内容

事務局から、資料の確認と委員の紹介を行った。

事務局から、本日も現下の状況を踏まえて、会議室に出席の委員とオンラインで出席の委員のハイブリッド形式で開催との発言があった。事務局から、横浜委員の代理として、松原様が出席の発言があった。

続いて事務局から、資料3についての説明を行った。

(1)経営に関して

○和田委員

- 経団連のサイバーリスクハンドブックなどが出てきて社長から役員全員に配布されるなど、経営者の意識は高くなってきていると思っている。

○岩下委員

- 資料3の4ページのサイバーセキュリティ経営の実現についての3ステップは、考え方自体は良い方向だと思うが、もう少し実践的な部分の意識を高めるような工夫が必要。出てこない情報を密接な人間関係によってお互いに共有しあうことも非常に大事だと思う。

○宮下委員

- JUAS で可視化ツールのベータ版に対するユーザ企業の評価をやっている。18社に実際に使っていただいた結果は、そのまま使える、もしくは一部の修正で使えるという方が95%でかなり良い評価をいただいた。定量的なアプロ

ーチや、具体的な事例を入れてもらえるとよいという意見があった。今後もヒアリングを継続してフィードバックしたい。

（2）中小・地域に関して

○宮嵜委員

・ 昨年、お助け隊を神奈川地区で実施した。中小企業での導入には意識のレベルの差もあって難しいところもあった。中小企業は、コスト、投資にかなり抵抗感がある。コストを下げるような工夫を考えたい。

○湯淺委員

・ 警察庁が各都道府県警に中小企業も巻き込んだ形でサイバー犯罪対策のコミュニティを作るよう数年前に指示している。そのような既存の地域コミュニティとも連携しながらやっていただくとより効果的ではないかと思った。

○名和委員

・ 既存の中小企業コミュニティがかなり活性化し、密になっている。関連省庁を巻き込むなど仲間になっていくような形でやっていくのが中核になるひとつのヒントかなと思っている。

○松原様（横浜委員代理）

・ 地域の中心的役割を担っている先生や企業の方と一緒に協力することで、地域に根差しやすい取り組みを進めていくことが重要。中部 ISAC など成功しているところは、地域の大学の先生や企業のサイバーセキュリティ専門家が中心的な役割を担って、地元の企業と目標設定し、定期的にミーティングを重ねることで次第に信頼の輪を広げている。

○小松委員

・ 大阪商工会議所は、セキュリティ対策について積極的に取り組みを進めており、各地の商工会議所でも大阪商工会議所のように、セキュリティ対策に関する普及活動に積極的に取り組みたい、という意識も高まっている。この機会に後押しできればと思っている。

○藤原委員

・ 地域 SECUNITY やコンソーシアムの取組については、中央のメディアだけでなくて地方紙などローカルメディアの巻き込みが大切ではと感じている。活動に当たって、ローカルメディアとの連携を行うべき。

○梶浦座長

・ やはり最後は地域でキーになる企業なり組織なり人を見つけ出して支援していくというところに尽きる。ご指摘は、サプライチェーン・サイバーセキュリティ・コンソーシアムの運営に当たって留意していく。

（3）人材に関して

○湯淺委員

・ 教育機関の取り組み、特に高専の取り組みが充実してきたと思う。課題は文科省からの予算が切れると自走しにくいこと。文科省とも調整をしていただき、継続的に支援をしていただける枠組みがあれば定着すると思っている。

○名和委員

・ 経営層や事業内容が変わった際に必要なくなった人材について、他社で必要とするところはある。こうした人材を業界あるいは会社間で融通する仕組みがあるとよいのではないか。

○和田委員

・ サイバーセキュリティ体制構築・人材確保の手引きには、我々が今まで検討してきた内容が多数盛り込まれており、そうした内容が経済産業省を通して広く普及していくのは本当にありがたい。

○宮下委員

・ 大企業であってもセキュリティは兼務の人が多い。プラス・セキュリティ人材の明確化と育成については検討を要すると思った。

○小松委員・丸山委員

- プラス・セキュリティ人材では、免許で例えると原付のようなレベル、または、簿記で例えると簿記三級のような、セキュリティの要点は知っているが、細かいことは分からないので専門家につなぐといった対応ができる人材がいればよいと考えている。既存の検定などにセキュリティの項目を入れるなどすれば、中小企業や個人事業主も含めてすそ野を広げられるような気がする。

○塚本委員

- サイバーセキュリティ体制構築・人材確保の手引きは、非常に分かりやすいため、企業のみならず IT を使う全ての団体、組織にとって役立つと考える。公表されたら広報、プロモーション活動をすると良いと思う。

○岩下委員

- サイバーセキュリティ体制構築・人材確保の手引きの24ページのコラムでセキュリティ統括機能と CSIRT の関係が書いてあるが、インシデント対応から切り離された統括機能はあり得ないと思う。どのような機能が必要かということを明示しつつ、現実的なセキュリティ対応を強調して実践的な対応を進めていくことが重要。

○武智委員

- 人材を大事にする仕組みとして、認定のような仕組みが重要。サプライチェーン・サイバーセキュリティ・コンソーシアムの中でも議論していただけるとありがたい。
- 現場とトップが有機的につながることが大事であり、切り離すべきではない。セキュリティ統括機能の考え方は、ユーザ企業には現場任せや丸投げが多いため、そこを是正するためにどうするかという問題意識から生まれた。

○松原様（横浜委員代理）

- 弊社の場合、CISO 主催で定期的に国内の事業会社のサイバーセキュリティ人材の勉強会と、年に 1 回国内外のサイバーセキュリティ人材を集めた会議を開催している。そこで、会社全体で経営層レベルと現場レベルが交流を深め、相談しやすい環境を整えている。

○梶浦座長

- 人材の流通に関しては、セキュリティ人材を登録する JTAG という制度が本格的にスタートすることになっている。
- CRIC の活動は大変有益。すそ野まで広がるかどうかということが今後の課題で、それがサプライチェーン・サイバーセキュリティ・コンソーシアムのひとつ大きなミッションだろうと理解している。
- プラス・セキュリティ人材は、私の感覚では、例えば経理、総務、人事などといった専門知識を持っていて、その能力の一割ぐらいのセキュリティ・リテラシーを持っている人を指す。少し広く捉えていただいた方が良いと思っている。
- ここで紹介しているものは、社会全体をなんとか最低レベル＋αまで持って行こうというぐらいの趣旨だと理解している。先端的な企業は反撃まで可能な程度の能力を持って欲しいと思っているが、それは今後の議論だと思う。

（4）サプライチェーン・サイバーセキュリティ・コンソーシアムについて

○湯淺委員

- 資料3の41ページでご説明いただいた基本行動指針について、情報漏洩が起きたときの公表に向けたマインドをどう持っていただくのかというのは、結構大きな課題ではないか。

○名和委員

- 資料3の43ページのコンソーシアムのイメージの図にあるお助け隊サービス審査機関に対してライフサイクルの記述がなく、慣れてきた頃に品質の悪いサービスがあることを評価できるのかが気になった。

○武智委員

- 2016年ぐらいから人材のことをやってきて、ついにここまできたというところがある。サプライチェーン・サイバーセキュリティ・コンソーシアムは、それをさらにまとめていくように感じているので、そこに期待したい。

○小原委員

・ 検討すべき課題は 6 点あると思う。一番目は、国と企業の関係（税の公平性やインセンティブを含む）、二番目は、国際的な貢献寄与、三番目は何がリスクなのかということが本当に共有されるかということ、四番目は、経営の観点からの検討、五番目は、倫理的な視点の組み入れ、六番目は、事務局の作り方である。また、事務局が取り組むべき7つの視点 PESTLED を考えてみた。PESTLE（Politics、Economics、Social、Technology、Legal、Environment）に社会との共生という価値観を踏まえた上での D：Disclosure を追加したもの。会社はどのように社会と渡り合っていくのかという視点も加えていって欲しい。

○丸山委員

・ 倫理綱領などは、ちゃんと決めておかないと後になって修正できない。確かに色々な背景があるので、書けない項目があるにしても、骨のようなものはちゃんとあった方が良いと思った。

○和田委員

・ サプライチェーン・サイバーセキュリティ・コンソーシアムと NISC のサイバーセキュリティ協議会の違いは少し記載をしておいた方がわかりやすい。

○梶浦座長

・ 小原委員の視点は非常に重要なことだと思うが、多分ステップバイステップかと思う。良いアドバイスをいただいたと思うので考えていきたい。

（5）その他

○藤原委員

・ 日本サイバーセキュリティ・イノベーション委員会の提言では、全ての国民が全て平等にオンラインにアクセスできるようになって、はじめて新しい社会ができるのではないかと考えている。

○塚本委員

・ （配布された）日本サイバーセキュリティ・イノベーション委員会の提言の問題意識は、ACCJ としても近く、賛同している。イベント等何か協業できたらと考えている。

○和田委員

・ 弊社はコロナ禍で売り上げが伸びない分、DX なり、関連事業なりを増やしていくべきということで、DX 関連とセキュリティ予算については平年と変わらず付いているという状況。

○松原様（横浜委員代理）

・ コロナ禍で世界的に景気が悪化している中で、アメリカのベンダーの調査では、すでに5月の時点で4割の企業がサイバーセキュリティ予算を減らしている。サイバーセキュリティは大事なので、一緒にやりましょうと言い出しにくい雰囲気になった場合、どうしたら良いのかというのは、今のうちに考えておくべき。

○宮嵜委員

・ これからニューノーマルの時代になっていくと、中小企業でも、ネットに急遽移行していくようなお客様は多くなっていくのだろうと思っている。今年度は、そのあたりも状況を捉まえてフィードバックをしていきたい。

○宮下委員

・ JUAS で会員企業を調査した際、売上高が例えば10％以上減った場合でも IT 予算もしくはセキュリティ予算を増やすという企業と減らすという企業に二極化していた。企業によってセキュリティの重要性、インパクトの判断が異なるので、一方的に減る、もしくは増えるということにはならないと感じている。

○小松委員

・ コロナ禍で中小企業はキャッシュフローに余裕がなくなっている状態である。費用感の合わないセキュリティ対策は、中小企業には、なかなか普及しにくいことも意識する必要がある。

○梶浦座長

- JUAS にて成熟度に関する議論を継続的にやっていただいていることに関しては、この場で御礼申し上げたい。

自由討議の最後に、梶浦座長から以下のとおり総括がなされた。

- 広範な資料だったこともあり、色々な意見を頂いた。
- 実装という意味でまだ不足していることはあると思うが、ボトムアップのトライアルとしては、私自身はそれなりに評価している。
- 情報開示では、開示をすることが得になるというようなスキームの検討もいると思っている。
- 中小、地域に至っては人材も予算も不足している。それにも拘わらず、コロナ騒ぎで意図せずにデジタル化が進んでしまったことすらある。お助け隊でカバーしていくこともひとつだが、それで十分だとは思っていない。地域の事情などを教えてもらってトライアルを続けていかないといけないと思う。
- 国際についてもサプライチェーン・サイバーセキュリティ・コンソーシアムで深堀をさせて頂けるということなので、引き続き皆様のご協力を賜れればと思う。

最後に事務局から、今後のスケジュールについて以下のとおり連絡を行った後、閉会した。

- 今後のスケジュールについては後日ご連絡させて頂く。

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