

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
サイバーセキュリティ人材の育成促進に向けた検討会(第6回会合)
議事要旨

1. 日時・場所

日時:令和7年4月3日(木) 10時00分～11時50分

場所:オンライン開催

2. 出席者

委員 :三谷委員(座長)、北野委員、小出委員、武智委員、田中委員、長谷川委員、平山委員、藤本委員、丸山委員

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、総務省 サイバーセキュリティ統括官室、経済産業省 商務情報政策局 情報技術利用促進課、独立行政法人情報処理推進機構、日本商工会議所、一般社団法人情報処理安全確保支援士会

事務局 :経済産業省 商務情報政策局 サイバーセキュリティ課

3. 配付資料

資料1 議事次第・配布資料一覧

資料2 委員等名簿

資料3 東邦ガス情報システム株式会社発表資料

資料4 三井物産セキュアディレクション株式会社発表資料

資料5 事務局説明資料(修正版・抄)

参考資料 サイバーセキュリティ産業振興戦略

4. 議事内容

武尾サイバーセキュリティ課長より冒頭の挨拶があった後、三谷座長が、議事進行をした。

東邦ガス情報システム株式会社から資料3について、三井物産セキュアディレクション株式会社から資料4について、事務局から資料5について説明を行い、続けて自由討議が行われたところ、概要は以下のとおり。

■ 資料3について

東邦ガス情報システム株式会社の資料3の内容に基づき、以下のとおり、委員より意見があり、東邦ガス情報システム株式会社より応答があった。

<ガイドラインのあり方について>

- ・ 既存のガイドラインが多くある中で、どういう対象に対して、何が不足しているのか。
 - 不足しているというより、ガイドラインが多く策定されていることが課題と認識。例えば、内部不正については、経営ガイドラインには含まれている一方で、中小企業向けのガイドラインには含まれておらず、網羅性の観点から、マッピング(ガイドラインのガイドラインのようなもの)が欲しいところ。IPAの中小企業の情報セキュリティ対策ガイドラインの解説ページには2つ(「中小企業の情報セキュリティ対策ガイドライン」と「5分でできる!情報セキュリティ自社診断」)のリンクしかない。また、「人材確保・育成の実践的方策ガイドβ版」においても内部不正を防ぐのであれば、

こういうものがあるといったような全体像を示すと良い。結局どれを実施すればいいのか分からないといった問合せが来るため、今あるガイドラインを整理した上で、必要なものを参照できるようになると良い。なお、ガイドラインの内容として、大きく不足しているものはないという認識。

<登録セキスぺの活用方法>

- ・ 情報処理安全確保支援士試験に合格したとしても、情報処理安全確保支援士として登録を行わない方がいる。登録のメリットを感じていないため、登録を行っていないと理解しているが、いかがか。
→セキュリティに関するとところで、情報処理安全確保支援士に合格される方のモチベーションから考えると、セキュリティを勉強し、会社等にそれなりに勉強したことを示す観点では、一番目指しやすいものと考えている。一方、サイバーセキュリティに係るコンサルタント等より幅広く活動されるのであれば、情報処理安全確保支援士だけでは足りず、CISSPのような資格が重要視され、情報処理安全確保支援士は CISSP のような難関資格の通過点として認識されているので、現状では、情報処理安全確保支援士資格を維持するためのインセンティブが少ない。政府向けのビジネスや調達に参入するようなことがなければ、中々維持しない。情報処理安全確保支援士資格を維持するよりは、CISSP を保有していれば十分と認識されている。
- ・ アクティブリストの活用シナリオを作った上で、継続的に改善していくことが必要である。活用される PDCA が必要というのは重要な指摘として聞いていた。活用のシナリオには、アクティブリストに登録する方々の過去の実績を考慮する必要があるが、他に必要となるシナリオがあればご教示いただきたい。
→現場の方が気にされるところは、どこまで信用できるかという実績の観点とコストの観点だと認識している。アクティブリストの実績欄はカテゴライズすると良い。情報処理安全確保支援士が抜け漏れなく入力をしやすくなるような例示があると良いと思う。
- ・ みなし受講についてお伺いしたい。費用負担と情報処理安全確保支援士のレベルのバランスで、本検討会でも活発に議論がされてきた。みなし受講を実施した場合、情報処理安全確保支援士のレベルは維持できると考えるか。
→みなし受講の妥当性評価は難しい。e-learning で毎年実施している講習は、網羅性の観点から設定されている一方で、実践講習では特定のトピックの深掘りや、グループ討議等を行っていることを念頭に置くと、所属組織で実施する業務においては、例えば例年の標的型メール訓練を実施した経験では十分ではなく、上流工程の検討や規格検討のような業務であればみなし受講として許容されるのではないか。分かりやすい基準を設定し、例を提示すると良い。正直、上司による評価は難しいと思うので、業務の内容面から許容できるラインを検討されたいかと思う。また、実際に中小企業向けの指導の方が実施して得られる経験値の方が相当多いのではと考える。
- ・ 普及施策の中で、セキュリティの講習に来る方は、意識が高く、本当にリーチしたい人には伝わっていないのではとのご指摘は重要であり、いかに裾野を広げていくかが大きなテーマだと思う。地方で中小企業の会など色々あるが、横との連携を含め、セキュリティ対策の普及の裾野を広げていく工夫等の考えをお持ちでしたら伺いたい。
→普及策については、ネットワークが重要である。サプライチェーン上流のルートからのつながりやユーザ会等における分野ごとの交流も考えられる。さらに、サイバーセキュリティに係る勉強会を活用していくのも良い。中小企業の方同士の意見交換等も大事で、発言力のあるところから全方位で施策を展開していくことが望ましく、また、口コミのような形も考えられる。
- ・ 「登録セキスぺの副業禁止」ということについて確認したい。企業に対して直接的な指示は難しいと思うが、中小企業支援に携わる登録セキスぺの裾野を広げる観点から、国に対して期待するものは何か。

→「サイバーセキュリティ経営ガイドライン」等を通じたメッセージを想定している。例えば、10 か条の「社外交流」というキーワードがある。人材育成や地域貢献に寄与できるため積極的な貢献を望む旨のメッセージを「サイバーセキュリティ経営ガイドライン」等のガイドラインに盛り込めると良い。例えば規程類の制定に携わる機会は一般的に少ないが、社外交流等を行い得られた経験を自社に持ち帰ることによって、所属企業にも人材育成や地域貢献などの観点からメリットがあると考えられる。

- ・ プロボノのようなイメージだと理解した。社外との情報交換を行うことに意義があるという説明が必要であろう。
→副業を解禁することで本業が疎かになる可能性がある中、登録セキスペとして所属企業以外の支援に携わることが、必ずしも収入増加を目的としたものでない点が所属企業に伝わりにくい。所属企業としても許可をしてしまうと、本業との兼ね合いや離職を懸念している。所属企業にとってもメリットがあるとのメッセージが重要である。社外交流は若手にも経験や自信にもつながるため、登録セキスペの所属企業側にも理解いただける仕組みが重要である。
- ・ 副業禁止について確認したい。一律禁止や一律許可と両側に大きく振れがちである。イメージアップにもつながり得るため所属企業にとっても副業はメリットがあり、現業に対し、影響を及ぼさないとする条件を設けた上で、例外を一部認めていく方法があると考えているが、ご意見を伺いたい。
→一律解禁することは難しい可能性があるが、一部例外的に認めることは考えられる。ただし、サイバーセキュリティ分野のみ特例を認めていただくことも難しく、国からのメッセージがあると、調整がしやすいのではないかと。

■ 資料 4 について

三井物産セキュアディレクション株式会社の資料 3 の内容に基づき、以下のとおり、委員より意見があり、三井物産セキュアディレクション株式会社より応答があった。

<サイバーセキュリティの地域における普及活動について>

- ・ 地域のコミュニティとのつながりについて確認したい。行政機関、商工会議所、青年会議所及びロータリークラブとの関わりはあるか。
→Area Security Council (以下、ASC)は、地域 SECURITY からスタートしている。九州経済産業局に加えて、東北経済産業局とも連携を行っている。さらに、商工会議所とも連携を図っており、地域のネットワークに協力いただくことは効果的と認識している。
- ・ 地域での信頼の醸成が重要という点、また経営者、担当者、IT ベンダーが一緒になって取組を進めていくという点は、全く同意である。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(SC3)でも同様の取組を行っているが、まずはセミナーに参加いただき、経営者に理解していただくことが重要であり、その後 IT ベンダーの紹介に繋げていくのだが、それぞれの段階で、具体的に伴走支援はどのような形で行っているか。
→伴走支援の第一歩として、まずは、興味がない方に興味を持っていただくことが重要である。経営者が、知り合いの経営者をセミナーに呼ぶような流れが理想的である。セミナーに来ていただけない場合には、直接訪問するなどの草の根運動が重要である。セキュリティの意識が全くない中小企業は少なくなっているが、具体的な課題を認識できていないことが多い。そうした中小企業の経営者に気づきを与えるために、セミナーへ参加を促した上で、次のステップに進めるよう、IT 担当者を同席させるよう依頼している。また、誰からの発言なら行動に移していただけるのかをよく見極めている。
- ・ 自立して対策することが本来は望ましいが、セキュリティベンダ等に伴走してもらわなければ、中小企業は立ち行か

なくなるという現状も理解した。

- ・ 中小企業経営者を中心としたセミナー等の開催により、その参加企業が企画側で参加するという流れがあると認識した。個人の情報処理安全確保支援士が中小企業支援を自分の事業としてやっていく場合、最初はボランティアでやっていくというお話もあったが、そのボランティア期間はどのくらいなのか。また、その後どの位の割合の中小企業経営者が有償ベースでお願いするようなことになるのか感覚的なところを教えてください。

→中小企業が最初から有料セミナーに参加することは少ない。無償でサービス提供できるところから入り、ニーズの引き出しやサイバーセキュリティお助け隊サービス等の紹介に繋がっている。また、情報処理安全確保支援士の方ではないが、ある独立されている方で、実務経験が少ないため、勉強をしようと様々なセミナーに参加し、有識者の方から色々な話が聞くことで研鑽になるというお話を伺っている。そのような方々が研鑽を積み、セミナー登壇者になるような流れを作りたい。また、収入の面についても、IPA の講師派遣事業などを活用して講演料を頂ける形となっているため、そうしたスポットでの活躍から、企業との顧問契約までステップアップすることを目指して活動したい。また、情報処理安全確保支援士と IT 担当者を繋いでいくことも重要である。

- ・ 情報処理安全確保支援士をコーディネートする取組もかなりのコストがかかるという認識である。そうしたコーディネート機能を担っている ASC の取組には頭が下がる思いであるが、そのコストはどのように工面しているか。

→時間的にも資金的にもかなり大変であるが、ASC の運営には多額の費用はかかっておらず、会費のほかボランティア部分もある。ただし、セキュリティに限らず ASC の会員間でビジネスに発展しているケースも見受けられる。実ビジネスにもなり企業間でつながりを持てるという点や、研鑽につながるという点など、参加者の方々には、様々なメリットを享受いただいていると認識している。

→ASC は単体ではなく、セキュリティのコミュニティや商工会議所等と連携した活動をするためのハブ機能を担っている。また、セミナーにはセキュリティ分野以外(例:農業分野)の団体様に登壇いただくことで、他分野にもセキュリティが浸透していくことを目指している。

- ・ ASC はセキュリティに関する取組を形にするために発足したものであるが、コミュニティの継続という観点で、その活動は確かに個人のボランティア精神に依存しているところもある。しかし、この枠組みがあることで得られるメリット(例:所属企業に対して説明ができる、外部予算を獲得できる)もある。時間的な制約がある中、共通の目的意識を持ち、お互いに協力している形で成り立っている。

- ・ コミュニティや協議会を形骸化させずに継続させる際の課題は何か。これまでの取組や今後の取組についても伺いたい。

→継続性の面では、金銭面の課題と人的な課題の 2 つが挙げられる。キーパーソンがいなくなると立ち消えてしまうことも多い。経済産業省にも後押しをしていただいております、継続することができているが、次世代にバトンを渡していく必要がある。また、最低限、事務局を維持するための会費は必要である。セミナーに登壇する方々への謝礼は IPA の補助金を活用している。

- ・ ASC に所属されている方のスキルや取得資格について確認したい。

→ASC の中では、当方が情報処理安全確保支援士資格を保有している。資格を取得している地域のコンサルタントと連携していくことが重要である。

<登録セキスぺの活用方法>

- ・ 中小企業の限られた体力やコストを考慮すると、情報処理安全確保支援士と中小企業が 1 対 1 になるのではなく、

情報処理安全確保支援士がコーディネーターとなり、複数の中小企業から報酬を少しずつもらうというやり方はいずれあるのか伺いたい。

→情報処理安全確保支援士自身がコーディネーター機能を担うことについて賛成である。その地域において、ある程度信頼を獲得されている方が、中小企業をコーディネートするという取組が必要であり、その役割を地域SECURITY が担うというイメージもついている。ただし、紹介する側としても、リストに書いてあるだけでは本当に支援ができるのか不安な点もあるため、業務ごとに伴走できることが示せるか、1回目は実際に対面で会ってみて伴走できることを確認できれば、安心して紹介できる。ただし、コーディネートに係る費用面の問題は残るが、コミュニティの中で会費をいただいているのであれば、無料で支援するということも考えられる。

- ・ 地方の特性として顔が見える関係を重要視されているが、情報処理安全確保支援士が大都市に集中している中で、どうしてもリモートなどにならざるを得ないところもあると思うが、その辺りの実効性をどのように考えているか。
→リモートの支援の実効性はあると考えており、我々も現にリモートの支援を行っている。対面でなくても、仲介者のコーディネートがうまく成り立てば、関係構築は可能である。

■ 資料5について

事務局より資料5の説明があり、以下の通り、委員より意見があった。

＜人材確保・育成の実践的方策ガイドβ版の普及施策について＞

- ・ 資料5「御議論いただきたい事項」(P.33)にも関連するが、見やすさの観点で「人材確保・育成の実践的方策ガイドβ版」のサマリ(経営者向けだけではなく担当者向けのもの)があると良いのではないかな。
- ・ ガイドラインがたくさん存在しており、どれを利用したらよいかわからないという問題があると認識している。利用者の「ペルソナ」を明確にした上で、そのペルソナごとに、どのように活用するかという「ジャーニーマップ」を作っていくという方策が考えられる。それぞれのガイドラインが日々アップデートされていく中で、学ぶべきことの全容が掴みにくくなっている。ガイドラインは、必ずしも経済産業省だけで閉じる問題ではないため調整は困難であることは認識しているが、このようなチャレンジが必要ではないかな。
- ・ 普及がうまくいっておらず、必要な方々に政策や成果物が届いていない印象を受ける。今後、普及活動の施策を深く議論できると良いのではないかな。

本日の議事はこれで終了した。

最後に事務局から、今後のスケジュールについて連絡を行った後、閉会した。

以上