第1回
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）
サイバーセキュリティ人材の育成促進に向けた検討会
議事要旨

1. 日時・場所

日時：令和6年7月3日（水） 15時00分～17時00分

場所：ハイブリット開催

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

事務局　　：経済産業省 商務情報政策局 武尾サイバーセキュリティ課長、金田国際サイバーセキュリティ企画官

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 設置趣旨・運営規則

資料4 事務局説明資料

4. 議事内容

冒頭、事務局より、本検討会の趣旨についての説明があった後、三谷座長より挨拶があった。

次に、事務局による資料の確認、委員による自己紹介が行われた後、事務局より資料 4 の説明が行われた。その後、自由討議が行われたところ、概要は以下のとおり。

＜セキュリティ・キャンプの拡充について＞

- セキュリティ・キャンプは上手くいっているという話を聞いている。育成数の拡大を目指すことと、定量的目標を決める点は賛同するが、To-Be を描くことと、As-Is を認識することが必要。独立行政法人情報処理推進機構（以下「IPA」という。）産業サイバーセキュリティセンター(以下「ICS-CoE」という。)が実施している中核人材育成プログラムについては、修了生同士が活発につながっている一方で、セキュリティ・キャンプの修了生同士のつながりについて、現状がどのようになっているのかを明確にすべき。
- これまで 20 年で 1,000 人を輩出したというと、育成数が若干少ないように思われるが、ある程度選抜され、非常に丁寧に講師からもフォローされており、育成の密度が高いともいえる。修了者の活躍は非常に良いアウトプットだと思う。
- 現状の枠組みの良い部分は維持しつつ、落とさざるを得なかったが優秀だった応募者に対して、しっかりと育てる、再度応募してもらう、地方キャンプに回っていただくなどのフォローが可能になると良い。
- 現状の取組は高く評価できる。トップガンの育成の点で上手く言っていると言える。
- 一方で、講師個人のモチベーションによって運用が回っている部分があり、仕組みとして十分でない面もある。セキュリティ・キャンプを持続的な取組とするため、講師の負荷を軽くするような組織的な取組を期待する。

- また、どのような視点をもって拡大をするのかという観点が重要。トップガンを増やすことは難しいかもしれないが、裾野を拡げようとした場合にどのような取組が必要か。セキュリティ業界としてはトップガンも取りたいが、ある企業では文系と理系の人材を半々程度採用していると聞いたことがある。トップガンの人材拡大と、裾野の拡大は分けて考えるべきではないか。
- JNSA として自身が関わる範囲で複数の取組(例:学生向けの講演、高専生への教育)を行っているが、現場の学生からはセキュリティ・キャンプが目指すべき上位の取組と認識されている。セキュリティ・キャンプにおいて求められている能力が高いとみなされていることから、応募等をあきらめてしまう学生も現状多くみられる。
- 現在は学生個人に対するアプローチが中心となっているが、研究室単位や学科単位、同好会単位、警察等が主導するサイバーボランティア等の単位でリーチすることも検討するべきではないか。
- 学生は応募するために課題を解く必要があるが、その課題を解けないためにくじけてしまい、応募に至らない学生が多いと思料している。
- 育成する人数を増やすことが重要。大学時代に教授から言われて衝撃的だったのは、学部生として 300 人が入学すると、10 年に 1 人程度フィールズ賞を取得する者が出てくるということだった。応募する前にくじけている人がいることもいることを踏まえると、相当な人数がセキュリティ人材の育成対象として関わっているものと考えられる。セキュリティ・キャンプの募集人数を 2 倍程度に増やしてみてはどうか。卒業者のプライドを社会にも認めてもらえるような環境を作れると良い。
- セキュリティ・キャンプはトップガンと裾野拡大の二兎を追っているが、双方の取組を分けても良いかもしれない。
- 根源的な話として、11 万人のセキュリティ人材が不足する中で、セキュリティ・キャンプで育成する人材はそのうち年間 50～80 人程度である。セキュリティ人材を育てる必要があるとされているが、トップガン等の各カテゴリの人材をそれぞれどの程度育成するのかを明確にすべきではないか。To-Be のひとつとして、セキュリティ・キャンプを通じてトップガンに相当する人材を何人育成するかなどを確認すべきである。10 倍に増やすのであれば全く発想を変える必要がある。2 倍にするならば拡充という路線で対応できるかもしれない。
- 具体的な数字を出すための議論はどうすれば可能となるか。産業横断サイバーセキュリティ検討会にて、企業の担当者と会話するが、自社にいる専門的な要員の数を企業内で把握するだけでも困難と聞く。
- 厳密に数値を算出するのは難しいと思われるが、大まかな規模感は把握しておくべき。企業の担当者と話すと、どのような種類の人材が何人いるかを把握できている企業が少ないという点は同意。
- また、トップガンも必要だが、高度専門人材や専門人材、セキュリティ以外の実務経験に優れた人材が必要なこともある。例えば、それぞれのレイヤーで何割の人材が割り当てられるべきかといった議論ができればと思う。
- 改善の上で積み上げていくことの方が実務的。応募倍率から考えるに、原石はまだまだ潜んでいる。
- 拡大していく上では教える側の体制も重要。修了生を講師に参画させる等の組織的な仕組みが必要ではないか。
- 20 年前の立ち上げ時の体制がそのまま続いている。今年は例年使用している会場の建替えもあり、会場も変えなければいけない時期に来ていると思われる。
- 拡大していく方針については合意が取れた。その上で、どのように拡大していくかというストラテジーの検討が必要な点とそのために必要なエビデンスを把握していくべきという点の双方を捉えて方向性を検討していけると良い。

＜登録セキスペの活用及び制度の見直し＞

- 登録セキスペ資格を更新しない理由として、特にメリットがないとされている点が重要であり、資格の登録にも影響していると考えられる。
- また、資格登録や維持に係る金銭負担が大きいというのは何と比較されての意見なのかを明らかにしたい。おそらく、試験料金の値上げや、更新制の導入による費用負担の増加を踏まえて発言されていることが多いのではないか。資格保有のメリットがないのであれば、それは金銭負担の問題ではないということであり、また資格保有のメリットがある

のであれば、手間暇かけて維持をしていくということである。他資格の例も踏まえ検討をされたい。

- 講習の構造を変えるという方針も示されているが、制度変更によりスイッチングコストがかかる。具体的には、オンライン講習に実践的な要素を組み込む変更を行うには、新しい教材の開発のコストと運用開始までに相応の期間がかかる。ウェブサイトの作り方や運用の方法まで全て変わることから、現行制度でかかるコストよりも増える可能性もあるのではないか。
- 現状、登録セキスペは 2 万数千人であり、2030 年の目標を 5 万人とした場合に、どのような層に広げるかを議論すべきではないか。資料 4「登録セキスペが目指すべき人材像」では、2 つの目指すべき人材像(企業等の内部に1人は置かれるべき人材の到達点/企業等の外部から専門的なセキュリティ対策を実施できる人材)が示されているが、後者の割合が多く、前者の企業内で施策を推進できる登録セキスペが少ない。また、2 つの人物像は全く異なっている。登録セキスペを 5 万人必要とした場合に、提示した 2 つの人物像をどの程度の比率にするかが重要で、それによって拡大の方向性が変わってくる。
- ITSS レベル 4 に相当する単なる技術講習は民間でも提供可能と思うが、国からの役割の期待などは IPA の講習から示されているところ、そのようなものについては 3 年に一度でも民間からではなく IPA 等から示す必要があるのではないか。
- 資料 4「登録セキスペ義務講習の見直しについて②」にて、「オンライン講習」において、「実習、実技、演習又は発表その他実践的な方法を組み込む」とされているが、オンラインで実技等を講習するのは相当難しいのではないか。
- また、登録者には資格維持のために 3 年間で 10 万円以上費用負担を課しているが、その収入が登録セキスペ制度にどう生かされているか。講師や教材作成などに相応の費用がかかると思うが、オンライン講習の作成にはそれほど予算がかかっているわけではないと聞いている。そのあたりの収支構造のバランスも考慮の上、講習制度の見直しの実現可能性について検討されたい。
- 登録セキスペ義務講習の免除対象を、登録セキスペの中でセキュリティに関する実務要件を課している他の資格も保有する者についても拡大してはどうかという方向性の中で、セキュリティプロフェッショナル認定資格制度(CISSP)のポイント利用について言及があったが、国家資格である登録セキスペ制度が他国の民間の枠組みに乗るのは適切ではないのではないか。また、CISSP も必ずしも実践的な業務経験によりポイントが付与されている訳ではないことにも留意が必要。登録セキスペ制度独自でポイントの仕組みを作るということは考えられる。
- 登録セキスペは守秘義務が課され、国家資格であるゆえの厳格性がある。そうした特徴を踏まえ、登録セキスペの活用を促進するために、登録セキスペ自体のステータスを上げる取組も必要である。
- 登録セキスペの取得メリットが企業にとって明確に伝わっていない。個人中心の普及に留まっており、企業による活用をさらに検討できないか。
- また、登録セキスペの更なる登録者数拡大に向けて、別途検討が進められている「サプライチェーン強化に向けたセキュリティ・アーキテクチャ」(※)と連携をして面的に議論を進めるべきである。登録セキスペの重要インフラ企業必置化などを単体で進めるには限界がある。

  ※経産省「第 8 回 産業サイバーセキュリティ研究会 資料 3」
  (https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/pdf/008_03_00.pdf)
- 企業の中に登録セキスペを1人配置するということを、技術だけに求めるのは無理がある。令和 6 年 3 月に開催された第 10 回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において、ある委員からは、現状としては技術の点だけを見れば、登録セキスペの技術があれば資格はなくてもよい、ユーザー企業にとって資格を取得するメリットやそれがないと困るといったことがない限り、登録セキスペをわざわざ使うことはないといった指摘もあったところ。そうした点も踏まえると、「サプライチェーン強化に向けたセキュリティ・アーキテクチャ」と連携し、包括的にサイクルが回るように検討いただけるとよい。

- 費用が高いから継続しないということと、費用を安くすれば継続するということは必ずしもイコールではない。施策として安全な方法は、メリットを増進することが重要に思われる。例えば、最近では、上場企業においては、内部監査の体制等の非財務情報を有価証券報告書に掲載すべしいう議論の方向性もあり、この流れと並行してセキュリティについても、登録セキスペの資格者人数等の情報を有価証券報告書に掲載させるなど、幅広くメリットを検討されたい。
- また、資格維持の費用については、講習をオンラインで実施すれば費用を安くできるといことが現時点で見えているわけではない。そのような状況を踏まえると、ポイント制度を設け、登録者が勉強し続けられる仕組みを作る方法もあると思う。
- まずは登録セキスペのメリットを追求していくということについて異存はない。一方、企業等におけるセキュリティリスクへの対応を市場原理のみに任せるのは厳しいのではないかとも考える。サイバー攻撃が激化している中で、中小企業も含め全て自助努力で済ませようとするのは危険ではないだろうか。このような状況を踏まえ、登録セキスペをどうやって全国の企業にアサインしていくのかという方策の検討が必要である。講習制度の見直しについては、国の資格である点を意識して対応することが重要という点はよく理解した。その上でどのようなオプションを示すかについて議論していく必要がある。
- 東京商工会議所にて、DX を推進する中小企業向けにセキュリティの重要性を説明した際に共感いただけた。セキュリティ関係者だけでは輪が広がらないため、DX を推進している部署や団体を巻き込み、資料 4「活躍の場の拡大（登録セキスペと中小企業等とのマッチング事業）」にあるような活動を推進されたい。
- 現在検討中のデジタルガバナンス・コードへのインプットは行う必要があるのではないか。IR の議論と並行して検討をされたい。
- 登録セキスペのブランディングがうまくいっていないように思われる。登録者数が2万人で頭打ちとなり、メリットを感じられないというのは、ブランドが確立できていないということであり、例えば経済産業省の調査事業の調査項目として追加をするなど、様々な機会で「登録セキスペ」という言葉を使っていくべきである。
- ポイント制について、国家資格であるからといって必ずしもすべてを国の機関で行う必要はない。例えば、公認会計士資格では、公認会計士協会の研修を受けなくとも、社内の研修等一定の要件を満たせば CPE という単位を付与される。ただ、ポイント制の枠組みについては、国が定めるべきである。

＜中堅・中小企業等の内部でセキュリティ対策を推進する者の育成・確保に向けた施策の検討＞

- 大手企業であっても、内部にセキュリティ人材を確保することが困難な中で、中堅・中小企業に対して、どの程度のレベルを求めるのか、現実的には厳しい議論となる。多くの中堅・中小企業では総務担当者が片手間でセキュリティ業務を実施しているところ、専門性が必要と言われて実施できる企業がどれほどあるか。自社でどの範囲を担うのか、専門性が求められる部分は外部の登録セキスペ等の専門人材を活用する等、内外の組み合わせの中でのレベル設定としなければ実務が回らないのではと危惧している。
- 自社の業務を理解している人材が、セキュリティスキルを身に着けて自らのビジネス、ミッションを守るという観点では、内部に適切なセキュリティ人材を抱えることは重要。自社で実施することの重要性を明確にした上で、どのようなスキルが必要か示すと良い。
- 資料 4「サイバーセキュリティ人材の育成・確保に向けた取組の方向性」では、専門人材という表現がなされている。専門と言う言葉を聞くと、中堅・中小企業からは、そのような人材は置けないという反応が予想される。本検討会で想定する人材に合ったネーミングであるか検討されたい。
- NISC では、橋渡し人材に代わるものとして「戦略マネジメント層」(※)というカテゴリを設けたが、役割としては様々なものが含まれている。セキュリティ人材の議論をする場合、必要なスキルやナレッジの話になるが、企業として重要となるのは必要な業務、役割である。中小企業では総務担当が広く業務を担当している。その方がどのような業務を担うかと、どのようなスキルやナレッジを有するかは別の問題である。

※参考資料:NISC「サイバーセキュリティ人材育成取組方針」
(https://www.nisc.go.jp/pdf/council/cs/dai18/18shiryou05.pdf)

- 北風を吹かせることになるかもしれないが、政府として中小企業においてもセキュリティを担当する方を配置するようにメッセージを出すべきである。自社にてセキュリティ人材を育てる必要が生じた段階で教材ベンダー等も動き始める可能性がある。例えば、米国の SP800-181　NICE フレームワークでもそのような動きがあった。
- 講習等はすべて民間に任せるべきではないが、方向性は政府から出していくのがよい。この時、スキルではなく、どういった役割が必要かを伝えるべき。マナビ DX(※)のように政府がお墨付きを与える仕組みがあると良い。
※マナビ DX(https://manabi-dx.ipa.go.jp/)
- 「産業横断サイバーセキュリティ研究会」(※)にて人材定義リファレンスを策定した際に、企業の中でセキュリティ全体を見る人が必要との意見があった。コンプライアンスに係る事例も参考にしつつ、セキュリティを統括する役割を企業内におくべきとのメッセージを出した。
※産業横断サイバーセキュリティ研究会(https://cyber-risk.or.jp/cric-csf/jinzai_reference_2016.html)
- 同一企業内でも部門によって扱う情報が異なる。また、企業の文化や海外取引の有無等によって、必要な社内の役割が異なってくる。
- 企業のセキュリティ対応組織が担当する業務範囲は常に変化していく。例えば、最近ではサイバーレジリエンス法やデータ法への対応は、社内においてどの部門が扱うべきか議論になった時、法対応として法務ではなく、技術的対応の要素もあるためか、サイバーセキュリティ部門に落ちてきている現状がある。
- 大企業は検討可能であるが、リソースが少ない中小企業に対しては How-To を示すガイドラインを渡すなどの支援が必要である。
- 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)においても同様の議論をしている。自動車工業会でもガイドラインを出しているが、Tier　が深い企業にそのガイドラインを浸透させるために苦労している。実装に落とす際に How-To が必要になる。この点を民間で行うか、ある程度は政府で行うかは議論がある。
- 上場企業に対してサプライチェーンのサイバーセキュリティ対策を内部統制報告書等で報告を義務付ける等すると、中小企業でも取り組まれるようになるのではないか。
- また、上場企業のサプライチェーンに含まれている企業でセキュリティ対策が実践されると、他の企業も対策を実施するようになると考えられる。
- 小さい会社でも経理担当がいるはずである。内部にできる人がいなければ税理士にお願いする。同様の仕組みがセキュリティでもできないか。経理における税理士がセキュリティにおける登録セキスペに該当する。
- 例えば、営業職でも簿記の知識は知っており、そのような知識は業務の中で必要な知識として捉えられている。セキュリティや個人情報の取扱いについても同様に、業務に必要な知識として教えることができないか。企業の大小は関係なく、すべての企業で「業務としてセキュリティが必要である」と伝えるべきではないか。
- セキュリティは典型的な外部性となっており、事故が起きるまで取組みが進まないのが実態である。
- プラス・セキュリティ人材も業務として何を行うかについての検討が進んでいる業界もある。一方で、そうでない業界に対しては業界団体に依頼するなどの施策を検討する必要もあり、SC3 も含めて働きかけが必要と認識している。

最後に事務局から、今後のスケジュールについて連絡が行われた後、閉会した。

以上