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（第4回会合）
議事要旨

1. 日時・場所

日時：令和7年2月7日（金） 13時00分～15時00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 事務局説明資料

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。

事務局から資料 3 の説明が、大阪商工会議所からプレゼンテーションが行われ、続けて自由討議が行われたところ、概要は以下のとおり。

＜大阪商工会議所プレゼンテーション概要＞

■　中小企業の実態・課題等

・　中小企業のセキュリティ意識と対策はこの 5 年のスパンで見ると一定の向上は見られるが、サイバー攻撃が多様化、高度化、巧妙化している現状を鑑みると、まだ意識も対策も不十分である。セキュリティ対策が売上を生まないことで、中小企業はセキュリティ対策に係る費用を少ないほど良いという発想。なぜ、セキュリティ対策が必要なのかを訴求する必要がある。

・　セキュリティに関しては、中小企業側の需要が小さいからマーケットとして未成熟であり、供給側も脆弱という悪循環が続いている。それを打破し、政府の支援の下で、供給を先行させたのがサイバーセキュリティお助け隊サービスであり、需要開拓型ビジネスと呼べる。おそらく登録セキスペとアクティブリストもそのような形で展開するものと考える。

・　現状、中小企業や支援機関のほとんどの職員は、登録セキスペを知らない。したがって、コンサルタントとして独立している人は、中小企業診断士を併せて持っている人が多い。つまり、サイバーセキュリティだけでは業として成り立っていない。

・　適切な相談先が無く、各社の事情に即していない製品が導入されるケースも少なくない。一方で、対策をしていない

企業は、ウイルス対策ソフトしか入れておらず、対策が二極化している。

■ 中小企業の相談先、他の資格との連携

・ 中小企業からのサイバーセキュリティに関する相談先の大半が各地域の IT ベンダーとなるところ、IT ベンダーは必ずしもセキュリティの専門家ではない。DX とセキュリティは両輪で進める必要があるが、中小企業のセキュリティ意識を向上させて、登録セキスペの活用を促進するという意味では、攻めの IT（DX）と守りの IT（セキュリティ）を分けて考えることも必要ではないか。

・ 現状、税理士や社会保険労務士、金融機関がまず中小企業から相談を受け、結節点になって他の専門家に相談するという事例は少ない。ただし、中小企業の一次相談窓口になる等、中小企業側、士業団体・金融機関側両者にとっても一定のニーズはあり、こうした団体等に対して、今回の成果物を訴求していくことは効果的と考える。

・ 商工会議所や商工会でサイバーセキュリティに特化して相談に乗れる職員は殆どおらず、外部から相談ブースに来る専門家も DX 系の専門家が大半であり、必ずしもサイバーセキュリティの専門家ではない。

・ 登録セキスペは、専門的な用語や難解な概念を分かりやすく説明する能力、経営面にコミットできる能力が求められている。また、個々の登録セキスペは個人事業主であることが多く、ソリューションとなる機器やサービスを持っていないことが弱み。

・ セキュリティに関する相談は、自社にどのような製品やサービスが適切かと言う観点でなされる。セキュリティは、本来は経営全般、広範囲な領域に及ぶものであり、それらに対応できる登録セキスペが求められている。

■ 登録セキスペアクティブリストについて

・ IPA の既存検索サービスに付属する形にするのが良い。また、中小企業は最初の第一歩が踏み出しづらいという意味で、初回無料かどうかは項目として記載して欲しい。

・ リストを作った以上、存在を知らしめる広報手段が必要。支援機関に積極的に使っていただく前提として、攻めの DX と守りのセキュリティはそれぞれ専門分野が違うという基本認識を持ってもらうことが必要。この切り分けが十分でないと、セキュリティに関しても、既存の IT や DX 関連の相談先で良いという事になってしまう。

・ 各地の商工会議所や支援機関は公的な存在が多いことからも、登録セキスペ個人が支援機関に売り込むのではなく、情報処理安全確保支援士会が組織としてリストを売り込む方が良いので、政府は同支援士会を支援する必要がある。

・ 商工会や商工会議所等の支援機関自身も中小企業であるから、実践的方策ガイドやアクティブリストを支援機関に自ら使ってもらい、会員企業に広げていく事が必要ではないか。また、支援機関としては、アクティブリストによって、支援の項目や件数が増加すること、専門家との結節点が増えることはメリットである。

■ 実践的方策ガイドについて

・ 外部人材活用に関して、中小企業における事例を追加して欲しい。何をどこまで内部の人材が実施し、どのような理由で何を外部にお願いしたのか、事例が有効。

■ 施策の普及策

・ 中小企業へのセキュリティ啓発は、継続することが重要であり、粘り強くセミナー等を実施すべきである。また、セミナー等で紹介される事例は、現状、大企業や海外の事例のものが多いため、もっと中小企業(例:従業員数 20 名以下)

の事例を生々しく発信すべきである。

・ 自社の HP や名刺に使える、ビジュアライズされたインセンティブ（Security Action 自己宣言のマーク、ISMS 認証のマーク）のような取組も重要である。

＜登録セキスペに係る施策の方向性について＞

■ アクティブリストについて

・ アクティブリスト対象者の詳細情報が掲載されている詳細ページは、標準フォーマットのようなものがあると利用者が比較検討することができる。その他、登録セキスペ自身の HP など掲載者がアピールしたいページがあるのであれば、それも合わせて詳細ページに掲載できると良いのではないか。中小企業にとってはどの業界を得意としているか等の詳細情報が重要であり、そのような情報を充実させるように議論していけると良い。

・ アクティブリストの項目については問題ないと考えているが、対象者をどのように検索できるのかという点が実は重要ではないか。例えば、コミュニケーション能力も登録セキスペには求められる。自社の製品やサービスに対して説明ができても、相談先の悩みに（例：何をすれば良いかわからない）に対して、的確に対応できる登録セキスペは限られている。得意分野が検索で分かるようになると良いのではないか。

・ アクティブリストは、中小企業や支援機関が登録セキスペを検索するためのアプローチに重点が置かれていると理解しているが、どこにどのようなニーズがあって、そこに自分がどう活躍できるのかという登録セキスペ側のアプローチを取り込むことはできないか。登録セキスペ側で魅力に感じることができるコンテンツを準備できると良い。

・ アクティブリストの良いところは、マネジメント指導テーマが類型化されている点である。掲載されている登録セキスペがどういう業務を経験しているのかが理解しやすい。同様に、マネジメント指導テーマ以外の業務についても、自由記述であると記載にバラつきが出てしまうため、定型化できると良い。

・ アクティブリストの見せ方について、「支援実績のあるマネジメント指導テーマ以外にも、発信したいメッセージがあるはずであり、そうした項目が目立つ工夫があると良いのではないか。

■ みなし受講について

・ 「更新時の義務講習に代替可能な実務経験の判断手法」に「所属組織（独立系の登録セキスペにあってはその顧客）が、一定の書式の下でこれを証した場合には、みなし受講を認める」とあるが、品質を担保できるか疑問であり、承認者が登録セキスペを理解していることを求めるべきではないか。例えば、登録セキスペの知り合いがいるのであれば、その数人（2～3 人）から承認をもらうのが良いのではないか。

・ 登録セキスペは業務独占がある資格ではないため、みなし受講のペナルティの実効性には疑問が残る。性善説に立つという点は理解できるものであり、全体の方向性としては良いが、不備の申請が発生しないとは必ずしも言えない状況であると考えている。その不備がすぐ見つかればよいが、それが長期的に見つからない状況になれば、資格の信頼性にも影響しかねない。

・ みなし受講申請者が登録セキスペの実務を行っているのであれば、所属組織はその方に相応のコストをかけている（例:外部のセミナーを受けさせている等）はずであるので、みなし受講申請になるべくコストがかからない形で、そうした客観的な資料を実務の傍証とするような仕組みを検討されてはどうか。

・ 「更新時の義務講習に代替可能な実務経験の判断手法」について、エンドーサーとして、上司の方だけでは不十分なのであれば、それに加えて登録セキスペの資格保有者も含むことも一案ではないか。CISSP においても同様の制度変更を行った。

・ 「みなし受講制度検討の背景とイメージ」について、そもそも義務講習の目的に立ち戻ると、常にリスクや技術が変化することを踏まえて自身の知識や経験をアップデートすることにあるが、一方で、それが資格更

新の大きな負担となっているため、その負荷を減らすために検討を行っていると理解している。そうした趣旨を踏まえると、例えば、「論文等の執筆」の中でも、高度な査読を通るようなものは、許容されても良いのではないか。みなし受講の対象を広げすぎてしまうと収拾がつかなくなってしまうことについては理解するが、対象となる活動のカテゴリーを一律で線引きしてしまうのではなく、更新の趣旨に基づき適合するものについては何等か許容する仕組みを検討することはできないか。ちなみに、CISSP では、専門家としての活動のみならず、社会貢献（例:子ども向けのサイバーセキュリティに関する講演）に資する活動も更新のためのポイントの加算の対象として認められている。

・ 登録セキスペの実務を見た上で、みなし受講を行うことには賛成する。ただし、懸念点としては、登録セキスペには、旧試験（情報セキュリティスペシャリスト試験）からの移行者を中心にセキュリティ専門というよりは SI に近い方も一定おられ、今の基準であると、みなし受講の対象者は限られるのではないか。エンジニア系は、セキュリティの業務が分かりにくい（みなし受講とするポイントが分かりにくい）のは事実であるが、IT の構築や SI に従事していて、セキュリティに関連する業務を実施している方も多いと考えるため、今後の検討の論点として提示したい。

■ 政府側の支援策や取組について

・ マネジメント指導の費用について、企業がどこまでをコスト負担するのかについては引き続き検討が必要である。登録セキスペがマネジメント指導に類する活動を行うには相応の工数やパワーが必要になってくる。なぜセキュリティ対策を行うのかを経営層に理解してもらうことがハードルであり、経営者の理解を得るための支援の無償化には賛成するが、その先の個別企業のセキュリティ対策は自社の必要経費であると認めてもらわないと広がっていかないのではないか。

・ 「セキュリティ人材活用促進実証（相談会における具体的な相談内容）」にて実証のコメント（例:「何をどう始めていいか分からない」「対策の内容や進め方についての具体的なアドバイスを求める」）が掲載されているが、企業のことがわかっていないと外部から助言しにくいのではないか。内部に然るべきセキュリティ人材を置くべきということや、経営者が自社のセキュリティについて考えるべきというメッセージを政府から出していくことが必要ではないか。その中で、アクティブリスト等を使って、どういう人材が欲しいかということに落とし込んでいくべきではないか。

・ 「自社の判断・取組の妥当性を、専門家の第三者的な視点から確認したいというニーズ」について、どういう基準を誰が出すかという議論は必要ではないか。登録セキスペの方に聞いてもなかなか出てこないので、世間的にはこれくらいすべきという何かしらのメッセージは出さざるを得ないのではないか。例えば、家の防犯で考えてみると、「玄関に鍵をかけることは当たり前」で、「防犯カメラ設置をする人もいるし、そこまでしない家もある。」といったことは誰でも認識していることだといえる。そのような「普通、これぐらいはやっていて当たり前。」という共通認識を持たせることが大事ということである。そういう意味で「サイバーセキュリティお助け隊サービス」は「玄関に鍵をかけるのと同じ感覚として、最低限やっておくのがよい。」などといったトーンのメッセージを出しても良いのではないか。

＜人材の育成確保施策の方向性について＞

■ 実践的方策ガイドについて

・ 中小企業の課題は一歩目を踏み出せないことである。そこをフォローする趣旨で、実践的方策ガイドを作成する事は非常に良い。来年度にブラッシュアップする際には、見やすさに配慮いただきたい。

・ 「実践的方策ガイドにおける 4 つの Step」(P.48)の STEP1 において、資産の洗い出しにつまずきやすい。例えば、資産を(システム的に整理した形で)管理できていないとアクセスコントロールを効率的に実行することはできない。情報

セキュリティ 5 か条の次にはデータなどの資産とそれらが存在するシステムの見直しが必要になる。見ている限り、データとシステムの関係性の整理は今のガイドにはみられず、STEP1 と STEP2 の間に入ると考えられる。また、企業で一般的に存在するであろう情報資産の例示があると理解がしやすくなる。また、最初から完璧に実施する必要はないというメッセージも重要である。

- 「実践的方策ガイド」における事例は、セキュリティ対策を実施する必要があるか具体的に理解いただけるような内容である必要があり、記載方法を工夫されたい。サプライチェーン全体のセキュリティを確保するにあたり、中小企業の役割をしっかりと伝えるべきである。
- 実践的方策ガイド β 版（案）のブラッシュアップを行う際に、協力企業に対して政府として支援ができないか。仲間を募り、課題等を蓄積・整理できると良い。

■ ガイドライン（実践的方策ガイドを含む）の普及施策について

- 実践的方策ガイドのようなガイドの存在を知らない方も多い。企業の経営者や担当者に知っていただくための導線を工夫しなければいけない。過去にも、経済産業所やや JNSA が実施してきた取組が実を結んでいない。
- 商工会議所やロータリークラブ等の集まりに参加した際に感じたのは、情報セキュリティではなく、経営のデジタル化、DX が入り口になるということである。導線を設計する際に考慮されたい。
- 「Ⅰ 議論の全体像②（予算事業の結果等を踏まえた支援策）」のアンケート結果では、47%の中小企業が「対策の必要性を感じたことがない」と回答している。中小企業にもしっかりと対応いただくために、他のガイドや IPA の普及活動等と連携してうまく PR しながら進めていただきたい。
- 実施すべき事項がわからない、どこまで対策をすれば良いかわからないという点がポイントである。どのようにギャップを埋めるかを検討した上で、実践的方策ガイドでそのギャップを埋めることができると良い。
- セキュリティ政策を正しく普及させるための方策のみを切り出し、議論する場を設けたほうが良いのではないか。良いものを作っているのにも関わらず、認知が進まず使われないのは社会的にもったいない。

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