第2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8月7日（水） 10時00分～12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、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 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 の説明があり、続けて自由討議が行われたところ、概要は以下のとおり。

＜登録セキスペの活用及び制度の見直し＞

- 企業の方と会話する中では、通常の事業会社では、技術的な専門職の人材も一定の割合で必要との声もあるが、どちらかというとマネジメント系の人材の方が求められている印象がある。
- 特定講習は技術よりのものが多く、監査やマネジメントに関するものは少数である。技術系の講習とマネジメント系の講習のバランスが是正されるのであれば、企業での活用につながり得る。
- 企業内で登録セキスペに活躍いただくには、セキュリティの専門スキルに加えて自社事業への理解やソフトスキル（問題解決力など）も併せて求められる。
- 大学の社会人向け講座を受講している登録セキスペの方からは、普段から勉強していることが認められないのは残念とのご意見をいただくことがある。実際に、大学の社会人向け講座には実践的な要素も含まれており、そうした講座を受講されている方は普段からサイバーセキュリティ関連情報を収集しているが、資格継続の役に立っていない。そのような経験が資格継続に認められる制度があるとよい。
- 登録セキスペの一番の課題は、登録セキスペを求める企業側と登録セキスペ側のミスマッチにある。企業経営者は、ビジネス面で事業継続やリスクマネジメントの推進を求めている。登録セキスペがそれらに対応するためには、制度のスコープの見直しが必要ではないか。また、オンライン講習の内容とそうしたスコープ

が適合しているかどうかを確認すべきである。例えば、医者の中でも心療医から外科医まで様々であり、登録セキスペにも技術寄りの人材とマネジメント寄りの人材がいる。

- 中小企業の対策については、資料3でもまとめられている通り、限られたリソースの中でどうやって対策を実施していくかということに尽きる。資料3 P.18にあるように、厳選した特定のセキュリティ要件と包括的なセキュリティ対策、ベストプラクティスをしっかり示すべきである。そのための各種ガイドラインが発行されているが、中小企業の方々がガイドラインだけで自ら対策を実施するのは現実的には難しいため、何をどのように実施するかなどを登録セキスペがサポートできるような仕組みが必要であり、政府としても強くメッセージを出していくことが重要である。
- 資料3 P.37に示されている通り、登録セキスペは企業内部に置かれるべき人材として期待が高まっている点については妥当と考える。制度創設当初から、企業内部のセキュリティ人材をどのように育成確保していくかが重要であることが議論されてきた。
- 資料3 P.38の更新制度について、これから更にユーザー企業や中規模の企業にも登録セキスペを増やしていかなくてはならない中、案としては非常に良いと思うが、基準をどうするかという点が重要である。例えば、実務経験に基づく更新については、実務経歴書等を提出させて終わりとするのではなく、それらを事務局でチェックする形になるのではないか。一般社団法人日本内部監査協会では、公認内部監査人(Certified Internal Auditor、以下、「CIA」という。）の資格を取得するのが難しい方向けに、内部監査士という資格があるが、その講習会において1万字程度の論文を課し、資格を認定しているケースもある。ただし、論文のテーマや毎年同じテーマで良いのかなどの検討が必要となる。またIPAでは大規模な論文試験等を行っているため、実現可能性として論文試験による認定も考えられなくはない。
- 試験の見直しという観点では、情報処理安全確保支援士試験ではテクニカル寄りの出題が中心になっており、マネジメント寄りの出題は少ない。ITSS レベル 4 においてマネジメント寄りの出題は難しいため、継続的な更新講習でカバーしていくことが必要と考えられる。
- 更新制度において、講習の考え方や講習制度そのものを変えていく必要がある。講習自体が義務講習と表現されているが、登録セキスペが自ら受講するための取組になっていない。ベンダーが提供する講習以外では、NICTのCYDER(実践的サイバー防御演習)やIPAのICSCoE(産業サイバーセキュリティセンター)など、選択肢が少ない。今の制度では、マネジメントやBCPに係る講習には対応できない可能性があり、見直していく必要がある。講習は、更新の条件になっており、更新制度と講習制度は表裏一体である。
- 更新について他の制度と比較すると、CISSPやCIAの場合は、更新する上での選択肢が多く、外部のイベントで有資格者の仲間に出会う。そうした外部のイベントでは、学習の場があり知識の維持向上がなされ、コミュニティも形成されており、メリットになっている。
- 企業とのマッチングのためのアクティブリストについて、そもそも登録セキスペがアクティブリストに登録しないと始まらない。また、アクティブリストの項目が例示されている様なもののみの場合、登録セキスペが数年に一度しかアクセス更新しないようなものになる可能性がある。ポータルサイトを作り、登録セキスペがサイトへアクセスし、情報を登録・更新するようにする必要がある。また、現行の登録セキスペ検索システムは、企業の方にほとんど参照されていないと認識している。アクティブリストについても、登録セキスペがサイトを積極的に活用し、企業の方々が参照する仕組みを作る必要がある。そのためには、登録セキスペの知名度やブランドの強化が重要になるのではないか。
- 毎年受講するオンライン講習と3年に一度の実践講習又は特定講習があるが、現状この講習が免許更新のための義務となっている。講習の目的としては、スキルの維持・向上のため、あるいは、スキルの測定のための両者が考えられるが、現状は中途半端になっている。例えば、IPAによる毎年のオンライン講習ではスキルの測定を行い、実践講習又は特定講習ではスキルの維持・向上を図るといったことが考えられる。各講習

の目的や位置づけ等を明確にする必要がある。

- マネジメント系の特定講習が少ないという問題があるが、そもそもマネジメント系の講習の応募が少ないというのが現状である。鶏と卵の関係で、民間企業でマネジメント系の講習を作っても受ける人が少ないため、講習数が伸びないといった現状もあるかもしれない。経産省や IPA でマネジメント系の特定講習を 1 つや 2 つ作り、特定講習の一つとして登録できるとよい。
- 登録セキスペの活用について、現状は内部人材ではなく外部人材の活用に留まっている。どの顧客にも大差ない形で非機能要件のところからセキュリティ対策を推奨することが多く、そうした状況が反映されている結果、登録セキスペが SIer やベンダーに偏っている。他方、企業や個社によって事業方針等は異なるため、機能要件と関係するセキュリティ要件を満たす、いわばセキュリティマネジメント系の業務を担当する企業内部の人材、あるいは外部人材として補い企業内部の人間のように活動する人材も必要ではないか。アクティブリストにおいても、非機能要件としてだけでなく機能要件として活動できる人材であるという点も反映できるとよいのではないか。このような人材を企業が採用することにより、マネジメント系の人材が増え、マネジメント系の講習の需要が増加するといった好循環を作ることができるとよいのではないか。
- 資料 3 P.14 のユーザー企業における登録セキスペの活用イメージについての理解が重要である。まずは、企業としてどこまでセキュリティ対策が義務なのか、ガイドラインという形で示されてはいるが、企業自身が十分に腹落ちしている必要がある。企業類型によって登録セキスペの使い方や役割が異なる。大企業や重要インフラ事業者等であれば社内で登録セキスペを抱えた方がよいし、中小企業や小規模企業では外部から登録セキスペを調達することになるであろう。企業としてセキュリティの対応をどうするべきか強めにメッセージとして出すか、「サプライチェーン強化に向けたセキュリティ対策評価制度」の中で言及していくか、又はインセンティブを含めて考えていくかなどは今後検討する必要がある。
- 重要インフラを扱うような事業者については、実践的な要素やセキュリティ対策の中身ついても理解している必要があるので、登録セキスペが企業内部に一人以上は置かれるべきという位置づけは納得感がある。
- 中小企業等については、セキュリティ対策をするにあたって外部人材の活用が必要となるが、懸念点として、外部人材を使うとコストが発生する。なぜコストをかけてでも登録セキスペを活用すべきかについて、企業に伝えることが重要である。
- 実務経験等を通じた更新負担軽減について賛成であるが、その制度の管理主体やその判断方法について議論が必要。管理主体として IPA が考えられるが、場合によっては民間団体の活用も考えられる。
- 登録セキスペの目指す人材像がぼやけているように思う。資料 3 P.3 で「登録セキスペが目指すべき人材像」として 2 つ(「企業等において、経営層、IT 部門、事業部門、管理部門等とのコミュニケーションや、IT／セキュリティベンダー企業との技術的調整を通じて、実施すべきセキュリティ対策を必要十分な水準で実現する人材。」(以下、「A 人材」とする。)、「企業等の外部等から、セキュリティコンサル（中小企業等支援を含む)、脆弱性診断、セキュリティ監視、セキュリティ監査等の専門的なセキュリティ対策を実施することができる人材。」(以下、B 人材とする。)の記載があるが、ぼやけている原因は A 人材と B 人材が「または」となっているためではないか。登録セキスペには A 人材と B 人材が存在することになる。A 人材は例えば中小企業の内部に在籍する一方で、B 人材は例えば外部の専門組織に在籍すると想定される。A 人材と B 人材では共通部分はもちろんあるが、研修のパターン等が異なるのではないか。
- A 人材と B 人材を分けて議論を行うべきではないか。A 人材と B 人材を分けて目指すべき人材像を理解すべきか、両方を兼ねた人材として目指すべき人材像を理解すべきかをはっきりさせたい。
- 登録セキスペ制度の当初の検討時には、目指すべき人材について、内部人材、外部専門人材というレベルまでは明確に議論していなかったと記憶している。人材が足りないという問題意識のもとで、どの職位にでも対応できるような、オールマイティな人材を育てることを目指していた。A 人材と B 人材を分けて議論すべ

きかについては、重要な論点だと理解している。

- 講習を作成する側の人材について、マネジメント系を経験されている方を見つけるのにとても苦心している。試験も講習も作成者の経験や能力以上のものは作成できない。現在の特定講習も含めて仕組み自体を見直さない限り、ないものねだりになる可能性がある。
- 企業からするとセキュリティマネジメントや BCP 等といったマネジメント寄りの人材のニーズの方が高いようにみえる。一方で、講習では技術寄りの講習が人気であるという現実がある。この状況をどうみているのか。登録セキスペが現状ベンダーに多く在籍しているため、技術寄りの講習が人気という理解でいいのか。
- ベンダーの提供している講習が特定講習に多く選定されている現状であれば、技術寄りの講習が多くならざるを得ない。マネジメント系の講習を作成しようとした場合、声をかける人や企業が限定されている状況。
- A 人材/B 人材という整理は非常にわかりやすい。A 人材と B 人材の整理はシラバス等に幅広く影響が及ぶ。登録セキスペには、バランスよく各領域のスキルを一定のレベルまで習得している方と、ある領域のスキルが突出している方など様々であると理解している。どのタイプの方に対し、どのような業務が向いているかがレーダーチャート等でわかるとよいのではないか。企業で足りないとされている人材や役割を考えたときに、優先的なものは何かというところから考える必要がある。企業におけるロールやポジションによって求められるものが異なる中で、登録セキスペ制度をうまくアジャストするにはどうすればよいかを議論するべきではないか。
- 一方、制度自体が複雑になることはできるだけ避けるべきと考える。また、登録セキスペが企業の内外どちらで活躍するかは各人のキャリアパスの結果であるため、それぞれが別資格でなければならないということではないと理解している。ただ、そうした人材が 2 種類いるとした際に、研修の内容がどちらかに偏ることは避ける必要がある。
- 登録セキスペがどちらの人材としても活躍できるためのベースをどうするかについては、試験の側で考えていく必要があるが、資格更新については、多様性を持たせることが重要なのではないか。
- 経団連が 2020 年に「サイバーセキュリティ経営宣言」を公開した。「サイバーセキュリティは経営者の問題である」と言われるようになってから、まだ日が経っていない。また、内閣サイバーセキュリティセンター(NISC)から、「戦略マネジメント層」という言葉が世に出て、企業としてセキュリティの戦略等を考える人材が必要であると言われるようになってから数年しかたっていない。その戦略マネジメント層が具体的に何をすべきなのかというところまで落とし込めておらず、AI の登場などにより、企業としてセキュリティの戦略等を考えるべき領域も広がってきている。そうした状況下で、教育事業者がそうした領域を現時点でカバーすることは難しく、マネジメント系の講習が少ないという状況に繋がっていると理解している。
- 自身も戦略マネジメント系のセミナーに関わったが、対応可能な事業者は少ない印象である。とはいえ、世の中が変わってきている中で登録セキスペも変わる必要がある。マネジメント系の人材が必要であることを官からメッセージを出すことで教育事業者側の努力も期待できると考える。
- 登録セキスペのシラバスでマネジメント系の知識スキルのウェイトを現状よりも大きくしていくことで、登録セキスペを企業内に配置していくことをユーザー側に求めるメッセージとなるかもしれない。
- 企業としてセキュリティそのものに取組まなければならない中、登録セキスペを企業の内部に配置するのか外部人材として活用するかというロールについては、各企業判断によるところである。やるべきセキュリティ対策があって、それを実施するにあたっての基礎的な知識・スキル体系を登録セキスペが持っており、社内で活躍する方がセキュリティガバナンスや新しいマネジメントを進めていく上で有効であるということを示していくことができれば、企業も賛同すると考えられる。そうはいっても、中小企業等では登録セキスペを社内で抱えきれないため、アドバイザーとして外部の人材を使うことも想定される。
- 企業側が登録セキスペを確保することによりどのようなメリットがあるのか、メッセージとして伝えていか

なければいけない。

- セキュリティ人材の確保は、極論お金を積めば解決する。しかし、マーケットが機能しない中で、補助金制度や減税制度でその外部性を補正することが政府の役割と考える。軌道に乗れば補助金等は停止して、マーケットに任せるとよい。本気で取り組むならば、経産省で予算確保して推進すべきである。
- 医師制度において、合格試験は同じであっても、継続試験で専門別のトラックがあるのと同様に、登録セキスペの更新制度においても、試験は同じであっても、A 人材と B 人材それぞれにおいて更新のトラックを用意することもあり得るのではないか。
- 自社の若手には、スキルセットを 3 段階に分けて、1 階部分として IT スキル、2 階部分として応用技術としてのセキュリティスキル、そして 3 階部分としてそれらを基盤とした自分が得意とする深掘りした専門スキルを身につけて欲しいと説明している。登録セキスペで言えば、2 階部分を基礎として、そのうえで 3 階部分に専門スキルを構築するために、更新の際の講習で専門性の色をつけていくことが重要なのではないか。CISSP にも ISSMP や ISSEP 等の上位資格があるが、登録セキスペでも同様のイメージができるのではないか。
- 政策的には、国の補助も借りてトップダウンで取り組んでもよいのではないか。サイバーセキュリティ経営ガイドラインが策定されてから 10 年程度で経営トップの意識も変わったという肌感覚である。経営者・役員向けのご相談もある中、そのような方に対して登録セキスペの価値についてメッセージを出して、理解してもらう活動が必要である。
- セキュリティが重要と認識しつつそこから先の行動がないという状況において、何らかの支援が必要ではないか。経営者に対してのインセンティブが必要である。デジタルガバナンス・コードに係る DX 銘柄に指定されると株価にある程度影響もあると思う。現状のデジタルガバナンス・コード要求は抽象的であるので、「セキュリティ統括者を設置すること」「登録セキスペが社内に配置されていること」などより具体的にすれば企業側の行動も喚起できるのではないか。J-SOX に働きかけるのも実効性確保には強く作用すると考えられる。

＜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＞

- セキュリティに関する各種ガイドラインや、世の中で起きているインシデントもあり、経営層の意識もある程度向上しており、内部人材育成に関するモチベーションは高まっている。しかし、経営層から対応を依頼されても、情報システム部門など実際に対応する担当者が困っている部分があると聞いている。コミュニティに参加し、同じように困っているような人と情報交換をすることも有益である。大学でも座学やコンピューターサイエンスだけではなく、社会人向けにマネジメント含む実践的な教育を実施し、情報交換の場となっているが、企業に伝わっていない部分がある。ガイドラインを示すだけでなく、実際に何をすればよいのか、どのように情報を集め、学ぶことができるのかという部分を充実させることが、企業内の内部人材育成に必要ではないか。
- 中堅・中小企業については、セキュリティ対策はここまでして欲しいといういわゆる「守りのセキュリティ」に関して企業の規模に依ってランク分けする方向性でよいと考えるが、企業が小さくてもスタートアップ等で、DX を推進するような企業においては、セキュリティを考慮していないサービスや製品が出ることは、問題である。DX や「攻めのセキュリティ」を実施するような企業は異なる指標が必要と考えられる。
- 資料 3 P.29 にあるように「守りのセキュリティ」としては SECURITY ACTION の一つ星、二つ星で十分と思うが、「攻めのセキュリティ」については別の基準が必要である。また、これだけやっておけば大丈夫と思われないよう、全体像を理解いただきつつ最低限の対策を示せるような構成としていただきたい。
- 特に、②専任で推進する人材の確保が困難な企業に関して、中小企業の経営者は、高い専門的技術を有する人材を求めている訳ではなく、自社のセキュリティリスクを分析してどこにどのように対策すればよいか知

りたいと思われる。ガイドラインを読み解くなどしてそれを実践できる人材が社内にいないのが実状の課題である。このような企業の課題を含めて外部から登録セキスペが支援できる仕組みがあれば、課題解決に資すると思われる。

- セキュリティに関するガイドラインは様々出ているが、そのどれを活用するのか、どのように解釈するのかと言う点において難しいのが現状。既存の各種ガイドラインを利用者の視点から束ね直すようなことが必要ではないか。
- 中小企業にも様々な会社がある。SECURITY ACTION 制度において一つ星、二つ星を取得すべき業種や事業者、規模等をより明確に定義すべきではないか。例えば、サプライチェーンに属する企業であれば、この星を取るというような、実施してほしい内容があるのではないか。
- 東京都で「東京中小企業サイバーセキュリティ支援ネットワーク」という取組みを行っている。その中で、サイバーセキュリティ人材の育成等を目的とした「中小企業向サイバーセキュリティ対策継続支援事業」というものがあり、継続的なセミナーの開催、専門家の派遣を実施している。さらに、その事例集が出されており中小企業に有用なものである。
- 資料 3 P.40 に示されているセキュリティ統括機能は、「①専任で推進する人材の確保が可能な企業・目指すべき企業」にとって適切な考え方であるが、実際に、セキュリティ統括機能を担う人材が各種ガイドラインを解釈して実施するハードルは高い。個人的に 25 名程度のソフトウェア企業に対してコンサルティングを行った際、IPA「中小企業の情報セキュリティ対策ガイドライン」に附属する Excel を使ったが、専門家でも活用するのが難しいと感じた。専門家以外には活用できないと思われる。
- 成熟度モデルの議論が進められている中、国としてどのレベルまで対策し欲しいかを示していくことは重要である。そのうえで、中小企業対策としては、各種ガイドラインの整備や専門家を活用した継続的な支援、事例集、サイバーセキュリティお助け隊サービス、補助金を出すなど、合わせ技で地道にやっていくことが重要ではないかと考える。
- 中小企業から見ると、SECURITY ACTION 制度で要求している「情報セキュリティ５か条」や「５分でできる！情報セキュリティ自社診断」等の項目は、当然必要であるが、これだけをやれば良い訳ではない。内容が具体に寄り過ぎており、他にも実装すべき対策があるという不安があるのではないか。また、サイバーセキュリティの分野は技術的な進展が早く、変化が激しいことから、自社のセキュリティ対策が適切であるか、経営層が不安を感じる要因になっている。よって、SECURITY ACTION 制度で要求している項目にプラスして、サイバーセキュリティの原理原則を伝えるということも重要ではないか。
- サイバー空間は、事業や社会生活への影響が大きくなる一方で、法整備がされ安全が確保された実務空間と違い、自由度が高くあまり法整備されてこなかった。今回の議論を持って法整備というと一足飛びだが、経済産業省の頭の体操として、ガイドラインの整備をしつつも、将来的には法整備まで見越してもいいのではないか。

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