第3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11月22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。

■　セキュリティ・キャンプに関する継続的な検討事項について

＜新たなキャンプ（セキュリティ・キャンプ・コネクト（仮称））について＞

- セキュリティ・キャンプ・コネクト（仮称）について、これまでの議論を踏まえても特に異論はない。ただし、本取組の対象者である「特定の専門領域における高度な知見・技能を有するもの」として、そこまで裾野を広げられるかが課題。「新たなキャンプ（セキュリティ・キャンプ・コネクト（仮称））の骨子」(P.8)に、対象分野の例として AI が挙げられており、AI や量子コンピュータのような技術分野が対象として考えられるが、対象をそれ以外の社会科学系の領域へ広げるかが、今後の議論のポイントになる。
- セキュリティ・キャンプ・コネクト（仮称）について、サイバーセキュリティは総合力が必要となるため、様々な分野と結びつく必要があり、方向性は非常に良い。また、対象分野の例として挙げられている AI はサイバーセキュリティと親和性が高いと認識している。そうした学問的な分野以外では、産業分野(例:自動車分野、宇宙分野)とのコラボレーションもあり得る。産業分野の方が比較的に講師も見つけやすい可能性がある。
- セキュリティ・キャンプ・コネクト（仮称）の講師としては、各産業分野において、現場で目の前の問題に向き合い、実践的に取り組んでいる技術者がいると考えられる。また、既存のセキュリティ・キャンプは、セキュリティの関する知識技能を体系立てているというよりかは、むしろ受講生の興味を起点にしているケースも多いため、企業内に

おいて問題解決に取り組んでいる人材が講師を受け持つことは、受講生にとっても魅力的にみえると考えられる。

- セキュリティ・キャンプ・コネクト（仮称）はよい取組と考えられるが、対象分野の区切り方は検討したい。対象分野は汎用的な技術領域と特定事業領域の双方があり得る。どちらも対象に含めればよいと考えているが、対象とするテーマの方針を明確に打ち出すべきではないか。DX を進めるユーザ企業では、事業リスクを考えると、汎用的技術領域ではなく特定事業領域のセキュリティエキスパートが即戦力として望まれている印象がある。セキュリティ・キャンプ・コネクト（仮称）の方針によって、招聘する講師はアカデミア系の人材か事業部門系の人材かで異なってくる。
- セキュリティ・キャンプは実施すること自体にも意味があると認識している。今回のセキュリティ・キャンプ拡充についても、非常に意味のある良い取組であると考える。
- 「KOSEN Security Educational Community」（以下、「K-SEC」という）や「成長分野を支える情報技術人材の育成拠点の形成」（以下、「enPiT」という）の関わりのある立場からセキュリティ・キャンプ・コネクト（仮称）についてコメントしたい。K-SEC では、「AI とセキュリティ」や「IoT とセキュリティ」の講義を行い、enPiT でも同様の取組を行っている。国立高専機構や一部の enPiT 校の取組を参考にしつつ、これらの組織と連携しながら進めていただくとよい。
- セキュリティ・キャンプ・コネクト（仮称）には賛同するが、講師の確保に課題が残ると認識している。講師の自主性に頼らず、講師の輪を広げていくことが課題である。
- セキュリティ・キャンプ・コネクト(仮称)の対象分野には産業分野等の観点もあるが、ロールやスキルの観点もある。デジタルスキル標準に示されたロール(例:ビジネスアーキテクト＋セキュリティ、デザイナー＋セキュリティ)ごとに、今までの施策と整合をとりながら対象分野を整理していくのがよい。
- セキュリティ・キャンプ・コネクト(仮称)は非常に良い取組と認識しているが、専門領域の特定が難しい。産業要素で領域を特定した場合、実務に直結する一方で、業界ごとの固有の考え方を考慮する場合、制度の設計が難しくなる可能性がある。軌道に乗せるという意味では、技術要素の汎用的なもの(例:AI、量子コンピュータ)を対象分野としてスタートした方が入りやすいのではないか。技術×セキュリティで考えるとわかりやすい。ただし、産業分野を考慮したものもあるとよいため、優先順位を考慮して取組を進めていただきたい。
- セキュリティ・キャンプ・コネクト(仮称)には、産業用と技術用の 2 つのベクトルがある。名称で区別(例:産業コネクト/テックコネクト)することも考えられる。初めから体系立てて進めるのではなく、ニーズのある分野(例:産業用であれば自動車、電力・技術用であれば AI・IoT・量子コンピュータ)から始め、対象分野を広げていくとよい。そのニーズのある分野に講師の方々も集まってくるのではないか。最終的には、産学連携で自走する形が望ましい。
- enPiT のように、こうした取組(例:セキュリティ・キャンプ・コネクト（仮称）)への参加が大学の単位に認められるようになれば、より学生にたいして広めやすくなるのではないか。
- enPiT は、大学内の手続を踏んでおり、大学院レベルの授業の一つとなっている場合は、参加が単位になる。
- セキュリティ・キャンプそのものを様々な大学の単位として認めてもらうことも有望と考えられる。まったく不可能ではないと認識している。
- enPiT の中でもベーシックである Basic SecCap が大学の学部の単位となる場合がある。公的なもので認定しやすいものとわかれば、あとは各大学の判断となる。経済産業省側から公的なものとアナウンスいただければ、大学側も公的なものとして認定しやすい。
- セキュリティ・キャンプが大学の単位として認められる場合、受講する側のインセンティブとなる。

＜修了生コミュニティについて＞

- 本取組に前向きで優秀な修了生と協力していくべき。
- 修了生コミュニティの設立はよい取組である。修了生においては、自身の持つ技術をブラッシュアップする必要がある。また、自身の知識・技術レベルの現在地を測る機会、参加者が相互に交流する機会として、修了生コミュニティの取組は進めていただければよい。

- 修了生コミュニティの整備は非常に重要である。セキュリティ・キャンプに参加する方は、参加時点で一定の実力があり、その後最先端の人材として育っていく可能性が高い。政府や高いレベルが要求される領域で、強固なコミュニティをもって人材を育てていく必要がある。
- K-SEC や enPiT においても同様の取組があるが、過去にセキュリティ・キャンプに参画された方を講師やチューターとして、優先的に修了生コミュニティへ招くことができないか。また、招かれた側としても講師やチューターとしていきなり参画することは敷居が高いため、修了生コミュニティにおいて、これらの候補者に対して育成支援をしていくことが望ましいのではないか。
- 修了生コミュニティの中から、講師やチューターの候補者が育成されていく循環が望ましい。
- 修了生の輪は重要である。セキュリティ・キャンプ・コネクト(仮称)において参加者の裾野を広げることに併せて、セキュリティのコアな部分を担っていない学生や講師も入っていけるようなコミュニティになるとよい。
- 情報交換ができるため、修了生コミュニティはよい取組である。集まった方が社会課題等について議論をしつつ、自身の貢献内容について議論していただいたり、修了生同士で課題解決を行っていただいたりする場になるとよい。参加する側としても修了生コミュニティは興味深い場になると思われる。
- 修了生コミュニティの設立には賛成ではあるが、コストの問題が議論されていない。コミュニティの運営コストは誰かが負担する必要がある。設立時点では経済産業省からの支援があるとしても、その支援は永続的ではないのではないか。そのような仕組みについての検討が必要である。

■ 登録セキスペに関する継続的な検討事項について

＜登録セキスペアクティブリストについて＞

- 人材データベースを構築しても、デジタルに判断できない要素が多く、使い勝手に課題が出てくる。網羅的な情報をデジタルにスクリーニングするというよりも、共通的な情報は少なくした上で、ある産業における実務経歴等のナラティブなデータを可能な限り掲載した方がよい。また、保有している他の資格情報（例:弁護士、税理士、司法書士、中小企業診断士）は掲載するべきである。例えば、中小企業診断士を保有している人材は経営を理解をしていると想定され、セキュリティ以外の能力も可視化された方がよいのではないか。
- リストに登録されている個人が、どのような枠組みで活動をするのか。資格保有者は通常組織に所属しており、その資格保有者にどのように仕事を依頼すればよいか不透明であるため、活用の枠組みについては検討が必要である。
- リストへの登録メリットを明確にできれば、登録希望者が増える可能性がある。
- どのように活用されるかのビジネスイメージを明確にすべきである。セキュリティに関する講師や企業に対してコンサルができる人材を探すことができるデータベースという趣旨自体はよい。一方で、継続的にデータベースをメンテナンスする際、制度運営者が各人の属性を更新するわけにはいかないため、登録者自身が情報をアップデートするためのインセンティブが必要になる。セキュリティプロフェッショナル認定資格制度（CISSP）では、自身で実務経験等のポイントを登録することとなっており、資格更新と連動している。企業に所属している登録セキスペについては、検索に引っかからない形にすればよいのではないか。また、既存の資格者一覧のデータベースと連動させ、外部への情報公開に同意を得た登録セキスペのみ検索に引っかかるというような機能を追加するべきではないか。
- 登録者自身が活用するものと位置づける必要があり、アクティブになるよう登録者自身がデータをアップデートすべきである。また、アクティブリストを見る側の導線として、商工会議所等との支援機関との協力が必要ではないか。
- 当然にやっていただいた方がよい取組であると認識している。アクティブリストを多くの方に閲覧いただくため、DX プラットフォームとの連携は考えられる。特に中小企業の中では、セキュリティ人材は不要であると考える企業もあると思うが、DX 人材であれば興味をもつ企業がいると考えらえる。企業の事業を考える上で登録セキスペが必要であるというメッセージを出していただきたい。

- LinkedIn のようなイメージで登録セキスペ自身がアクティブリストを更新できるような仕組みにできると良いのではないか。
- 設計概念は非常によいと考えている。このリストの存在や仕組みが社会的に認知されることが必要である。社会で認知されている先行するマッチングサイトの優位性や利用者の使い勝手などについての事例を研究し、よい要素は取り入れていくことが必要ではないか。
- 探す側としては、その方がどのような実務経験をしているかという情報は重要であると考えているので、そのような情報も盛り込めるとよいのではないか。
- 登録セキスペアクティブリストの展開戦略について、今年度の実証事業の報告と合わせて、次回以降の検討会で示されたい。

＜更新講習のみなし受講制度について＞

- 社内の研修は能力の維持に役に立っており、そこが認められるとよいと考えているが、質の担保のために上司の承認を前提としては如何か。
- みなし受講制度が効率的で継続的に運用可能なものとなるのであれば、みなし受講制度の幅を広げることも考えられる。
- 大学で社会人向けに講義を行っている立場から、大学の講座とみなし受講が連動できるとよいが、その場合の手続が煩雑でないとありがたい。大学の教員のリソースも限られているので、研修内容を示すだけでよければ、事務を行う立場としては嬉しい。
- みなし受講制度の手続きを煩雑にしないということは、申請をする利用者側の負担を軽減するという観点からも重要である。
- 登録セキスペ自らが、みなし受講として認めてもらいたい実務経験等について申請を行い、みなし受講が認められた実務経験等をアクティブリスト等のデータベースに登録するという仕組みがよいのではないか。また、CISSP では国際会議でのセキュリティに関する役職等がポイントとして加算される。特に、経験年数が増えるとそうした役職を担うことが増えるため、登録セキスペにおいても同様の仕組みとなっているとよい。
- みなし受講制度の方向性は問題ない。ただし、提出されたたレポートを通じ、実務活動の信憑性を確認することは非常に大変である。また、登録セキスペが実務を行う際には、セキュリティの状況変化をフォローしなければならない。そうした観点を踏まえると、セミナー等からの情報収集を含む自己学習と併せて、所属組織がオーソライズした実務活動に係るレポートを審査する形でみなし受講を認めるのはどうか。実務活動の信憑性を担保する観点で、傍証的に外部セミナーをうまく使える可能性があると考える。特にユーザ企業は、セキュリティに関する情報収集を怠ってしまうケースも見られるが、セキュリティ業務を専門会社に委託したとしても、自社環境で整合性が取れているのかを自社内で確認し評価ができる必要あり、そうした意味でも外部セミナーは重要である。
- CISSP の有資格者にとっては、資格継続のクレジットになるシンポジウムへの参加がモチベーションになっており、登録セキスペにとっても、コミュニティ活動の一環として、シンポジウム等への参加がモチベーションになるのではないか。
- みなし受講制度については、既存の制度を簡易にする考え方やコストを下げる考え方を否定するものではないが、その結果、登録セキスペのブランドやイメージの低下は避けるべきであり、登録者のキャリアにとってマイナスにならないようなものとすることが重要である。
- 資料中、「(2)オンライン講習と実践・特定講習それぞれの意義」(P.34)の赤枠について、「実践・特定講習の受講義務は、必要以上の負担となっていると評価されることから、そうした者について受講を免除することは相当である」とされているが、負担となっていることをみなし受講制度を創設の理由とするのはふさわしくないのではないか。みなし受講制度創設すること自体には賛成であるが、登録セキスペ制度が一定期間運用され、既存の更新講習がなくとも経

験やスキルを保有していることが認められるため、制度創設するということではないか。今まで提供してきた更新講習の内容が削がれてしまう、登録セキスペ自体のレベルが下がってしまうという方向性にはならないように配慮されたい。

- みなし受講制度の対象となる実務経験について、実務報告書で確認できるとよいが、確認に大きな手間がかかることが予想される。申請者側に一定程度の縛りを設けることや、確認する側の体制についても検討されたい。
- 企業における実務経験について、情報の信頼性を含め、みなし受講として認められる実務経験なのかという点に深く入りすぎてしまうと、みなし受講制度の実現が難しくなってしまう。企業内における人事評価等と同じように、所属上長が認めている等のエビデンスを出すことができる仕組みができると良いのではないか。

＜情報処理安全確保支援士試験について＞

- 情報処理安全確保支援士試験の試験科目や試験区分に複数の選択肢を設けることも考えられるが、マネジメント系の知見は他の資格（例：中小企業診断士）でカバーすることもできる。情報処理安全確保支援士試験は技術的な資格試験と位置付けられており、複雑にしないほうがよいのではないか。
- 情報処理安全確保支援士試験の構造は複雑にしない方がよいと考えている。一方で、実際にマネジメント系の要素について課題認識はあると考えられるため、一般的なリスク管理のフレームワークやその中でのセキュリティマネジメント領域に関し、他の資格と連動するのか、一つの資格制度の中で扱うのかについては引き続き議論した方がよいのではないか。
- 情報処理安全確保支援士試験にマネジメントや管理の部分を増やすとしても、サイバーセキュリティに関連するものとして他の資格と切り分けられるとよい。
- 情報処理安全確保支援士試験について、これまではテクニカル系の知識が中心だったが、最近ではリスク分析のようなマネジメント寄りの内容も含まれるようになってきていると認識しており、マネジメント系の出題はあってもよいのではないか。午後試験の問題では、4 問中 2 問を選択する方式であるが、マネジメント系の問題を追加し、その問題を選択して登録セキスペになる者がでてきてもよいのではないか。
- 作問者がいなければ、その範囲の問題は試験に盛り込まれないことを前提として述べると、日本の試験と海外の試験では、マネジメント、ガバナンス系の内容に開きがある。海外では、マネジメントやガバナンスに知見のある人が作問等に貢献している。
- 現在の登録セキスペの更新講習では、情報セキュリティの実務を行う人材として習得しておくべきこととして、マネジメント、ガバナンス系の内容が相当程度含まれているため、補完的にうまく利用するとよい。登録セキスペの更新講習の作成者には、そうしたマネジメント、ガバナンス系の内容に関する知見を持っている方がいらっしゃる。
- 情報処理安全確保支援士試験の午前問題は基礎的な内容であるため変更の余地は少ないと考えるが、午後問題の選択問題にケーススタディとしてマネジメント系の問題を複数追加しては如何か。
- 例えば、登録セキスペアクティブリストにおいて、マネジメント系が得意な人材、技術系が得意な人材としてカテゴライズを考えているのであれば、午後問題において選択必修という要素を加えることも一案なのではないか。
- サイバーセキュリティの対応方針や管理方針の策定は非常に重要であり、それらに対する考えを引き出すような問いかけが試験に入ってくると非常にありがたい。午後問題にそのような要素が入るとよいのではないか。

＜登録セキスペの活用促進・活躍の場の拡大について＞

- デジタルガバナンスコードでセキュリティ施策の文言が入った。主に上場企業向けにはなるが、DX 認定と連動して、ガバナンス体制の構築において登録セキスペが必要である旨をメッセージとして出せるとよい。
- 監査スキル強化も言及されているが、非常に重要なことと理解している。信頼性を示すという観点において、ガバナンスが有効かどうかを監査することは非常に重要であり、登録セキスペのスキル強化、多様化という点においても監査スキルは強化すべきである。

・ 機微な情報を扱い得る者として、登録セキスペは国家資格として身元がはっきりしている。ここでは議題になっていないが、セキュリティクリアランス制度について、登録セキスペを保有していれば、一定の類型に該当する等の将来的な検討の余地があるのではないか。

■ 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について

＜中堅・中小企業向けの施策について＞

・ 中堅・中小企業に対しては、様々な施策があるが、セキュリティに係るコストをどのように負担いただくか、経営者の方にどう認識いただくかが課題である。
・ 公認会計士や税理士でも同様だが、登録セキスペのような専門人材を自社で抱えることが難しい企業が多いという前提のもとに、どのように複数の企業でシェアをして、リーズナブルに活用する仕組みが必要である。登録セキスペアクティブリスト等を活用しつつ、どのように実現していけるかが重要となる。
・ 登録セキスペの活用促進でもあったように、中堅・中小企業の経営者にとってセキュリティ対策の優先度は低い可能性がある。サプライチェーン対策評価制度とも連携していくことで、状況は改善するのではないか。
・ 中堅・中小企業のセキュリティについては JNSA の立場でも長く議論・展開してきた。しかし、近年実施していた中小企業基盤整備機構での講座提供はニーズがないとの理由で今年から停止した。IPA セキュリティセンターでも様々な取組がなされており、この課題は、長い期間をかけて、様々な方法や手段で実施してきた。これまでの実績（プレゼンター制度、セミナー制度など）や各種制度に対する反応を知りたい。セキュリティのセミナーを開催しても、行動に移さない中堅・中小企業は多い。同じような状況の積残しが増えていくおそれもある。過去の振返りも含めて議論させていただきたい。
・ 東京商工会議所には中小企業の DX 推進等の委員会が設けられているが、東京商工会議所の関係者によるとセキュリティとはあまり連携していないようである。
・ セキュリティに関して取組が進んでいる企業の表彰などを国として検討いただけないか。
・ 登録セキスペの活用とも関係するが、サイバーセキュリティお助け隊サービスや補助金を認知し、活用している中堅・中小企業の経営者は少ないので、単にセキュリティに関するコンサルだけでなく、その辺りの国の施策を広めていく役割としてセキスペに活躍してもらうという連携があると良い。

＜中堅・中小企業が実施するセキュリティ対策に応じた人材確保・育成の実践的方策ガイドについて＞

・ 「中堅・中小企業が実施するセキュリティ対策に応じた人材確保・育成の実践的方策ガイド」(以下、「実践ガイド」という) でまとめていただいた内容を淡々と進めていただくとよい。文章に留まらず、人材育成に焦点を当てたセミナーなども展開していくことが重要である。
・ 実践ガイドを策定することはよいが、他のガイドラインとの整合性は確保すべきである。サイバーセキュリティ経営ガイドラインとの関係性を含めて、体系的整理が必要である。また、現在、「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に関するサブワーキンググループ」にて検討しているサプライチェーン対策評価制度との整合はしっかりと確保されたい。
・ 実践ガイドは中小企業の情報セキュリティ対策ガイドラインを参照しているとのことだが、実践ガイド以前に、中小企業の情報セキュリティ対策ガイドラインの内容を見直されたい。リスクの算定が難しい、25 項目の内容が古い等の理由で、中小企業の情報セキュリティ対策ガイドラインに示された内容を実践することが難しい。
・ 実践ガイドは、抽象的な記載では行動変容につながらないと考えられるので、例えば半ページを割いて事例を示すことで、中堅・中小企業の経営者の目にとまるのではないか。具体的には、人材不足によってインシデント対応が遅れた事例や、セキュリティの技術面では、大企業にとっては当たり前の平易な対策でも、中堅・中小企業では実施で

きていない場合が多く、そのような事例があるとよい。

- 実践ガイドについては、わかりやすく作っていただいてよい。例えば、Yes/No だけで答えていく事で自社のセキュリティの状況が分かるような、誰でも活用可能なツールもあるとよい。
- 「(3)企業が実施するセキュリティ対策の状況に応じた人材確保・育成の方策」(P.52) の表はわかりやすい。中堅・中小企業で実施すべき対策を明示した上で、必要なセキュリティ人材や人材の確保・育成の方策に落とし込む点がよい。
- 既存のガイドラインを活用することはよい。双方をメンテナンスすることの難しさもあるが、双方がどこを参照しているか整理をして明確にすれば、メンテナンスもしやすくなる。
- 自社がどこまでの対策をすればよいのか、中堅・中小企業が知りたがっている各社の事例を紹介できるとよい。
- ガイドラインには、セキュリティに対してやる気がある方を対象としたガイドラインと、セキュリティに対してやる気がない方にやる気を出していただくためのガイドラインの 2 種類がある。実践ガイドは前者のようであるが、後者については読み物というよりも動画等を用意いただけるとよい。
- 「(3)企業が実施するセキュリティ対策の状況に応じた人材確保・育成の方策」(P.52)の内容はわかりやすい。他のガイド(例:NIST CSF や ISMS)とのリンクを示すこと、実践ガイドとサイバーセキュリティ経営ガイドラインとの関係性を示しては如何か。

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