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5回会合)
議事要旨

1. 日時・場所

日時:令和7年3月4日（火） 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、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 情報処理安全確保支援士会発表資料

資料4 グーグル合同会社発表資料【委員限り】

資料5 事務局説明資料(修正版・抄)

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。

情報処理安全確保支援士会から資料 3 について、グーグル合同会社から資料 4 について、事務局から資料 5 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。

■　資料 3 について

情報処理安全確保支援士会の資料３の内容に基づき、以下のとおり、委員より意見があり、情報処理安全確保支援士会より応答があった。

＜中小企業への支援について＞

・　中小企業では自社のセキュリティに関するニーズや課題を把握できていない点に根本的な問題があると考えられる。中小企業に対してセキュリティ支援を行う際に、工夫をされている点はあるか。
→通常業務の上で必要となる IT サービスの選択やポリシーを作成する際にはじめてセキュリティに焦点があたる。SaaS や IaaS 等の IT サービス選択の支援からセキュリティに係る支援につながることが多い。

・　九州には、情報処理安全確保支援士の支援が必要な工場が散らばっている。情報処理安全確保支援士の多くは

大都市の福岡に集中していると考えられるが、支援が必要なユーザ企業は他県にも広がっていると認識している。一方で、福岡以外の地域においては、県内のユーザ企業と情報処理安全確保支援士を結びつけることは難しい場合も考えられる。考えつく対処方法はリモート対応であるが、中小企業は対面での支援を望んでいる場合も多く、その点ご意見を伺いたい。

→全都道府県で情報処理安全確保支援士は登録されているが、地方に行けば行くほど、個人事業主である情報処理安全確保支援士が登録されている傾向にあると考えている。まずは、地域にいる情報処理安全確保支援士を把握した上で、リストを定期的にメンテナンスすることが重要である。弊会としても、全国の実際に派遣可能な情報処理安全確保支援士を把握する取組に注力したいと考えている。

→支援形態について、当面はリモート対応に頼らざるを得ないと考えているが、地域ごとに継続的な取組を回してくという観点から、例えば、九州では、九州管内でコミットできる情報処理安全確保支援士をアサインすることが必要である。弊会では、経済産業局と同じブロックごとに地域会が組織されているので、日常的にはリモート対応とした上で、できる機会があれば、対面での支援も行えるように整備をしていきたいと考えている。

・ 地方では、個人事業主の情報処理安全確保支援士が多いと伺ったが、その理由をお伺いしたい。

→実態として、試験に合格したとしても大半は情報処理安全確保支援士に登録しない。登録する方は、会社が登録費用等を負担する場合か、自費で登録費用を負担する場合の 2 パターンである。前者は、福利厚生が手厚い大都市に多く、地方には少ない。結果的に後者である個人事業主の情報処理安全確保支援士が、地方に多くいるようにみえるということではないか。

＜情報処理安全確保支援士のスキル育成について＞

・ 業務の範囲を広くすればするほど、その業務が本当にできるのかの信憑性の問題が出てくると認識しているが、見解をお聞きしたい。

→他の士業にもあてはまることではあるが、コンサルティングをサービスとして提供してこなかった方々にとっては、背伸びが必要となる。また、実態として、情報処理安全確保支援士はエンジニア出身が多く、サービスのデリバリに慣れていない方々も結構いらっしゃると認識しており、能力担保のために、研修等で適宜補足することが望ましい。

・ 具体的な経験について客観的に判断することは難しく、事実に基づいたものをアクティブリストに掲載すべきという指摘には同意する。一方で、セキュリティというテーマに対して、様々な課題があり、その課題をカテゴライズして、検索ワードとして引っ掛けることにより、有効な方を紹介できるようにするという思惑があるが、その点ご意見を伺いたい。
・ エンジニア出身の情報処理安全確保支援士が多いというお話があったが、企業支援となると経営コンサルティングの要素と組み合わせる必要があると考える。そうした情報処理安全確保支援士は大企業を中心とした企業内部にいらっしゃると考えるが、兼業副業が禁止になっている場合も多い。アクティブリストの母数の課題についても言及されていたが、訓練機会の提供含め、活性化させるための政策としてどのようにお考えか。

→情報セキュリティの中でも、ガバナンスやポリシーメイキングといったマネジメント要素が強い部分と、SOC 対応や脆弱性の検知等のテクニカル要素が強い部分があり、情報処理安全確保支援士が持っている専門性を可視化することは必要である。自己宣言となるが、取り扱っている分野については表示する必要があると考えている。

→ユーザ企業にはマネジメント寄りの情報処理安全確保支援士が多く、兼副業が認められれば外部での活動ができることが多い。一方で、セキュリティベンダでは、同種業種の兼副業の許可が下りないことが多い。人材を増やす過程では、ユーザ企業に所属する情報処理安全確保支援士を兼副業人材として増やしていくことが重要である。ただし、コンサルタントとしての所作はトレーニングが必要である。例えば、経済産業省が所管している弁理士資格では、

5 日間の研修受講と、支援先に対する派遣経験が認められればアクティブリストへの掲載が許可される仕組みとなっている。自己負担の研修だと、受講者の伸びが期待しにくいため、フォローの仕組みについて検討していくべきである。

＜他機関や他制度との連携について＞

・ 支援機関との連携が重要と理解したが、大阪商工会議所とは具体的にどのような連携を行ったか。また、どのような支援があると活動がスムーズに広がるかについてお伺いしたい。
→大阪商工会議所は、「サイバーセキュリティお助け隊サービス」のパッケージを持っていたこともあり、大阪地域で支援可能な情報処理安全確保支援士の派遣紹介を行う等、会員企業に対する人的支援等を実施した。
→その他の支援機関については、商工会議所や地域の業界団体に加えて、中小企業と日常的に接点をもつ銀行等の金融機関や税理士、社会保険労務士等との連携により、セキュリティを入り口としない潜在的な層にアプローチができると考えられる。例えば、通常、セキュリティに関心のない層に対してセキュリティでイベントを実施しても集客ができないため、税務相談や労務相談を実施しているタイミングに合わせてセキュリティ相談を実施するのが良いと考えている。こうした既存の取組前例がある他士業を中心に連携を強化したい。また、中小企業庁にも積極的に支援いただきたいと考えている。

・ 大阪商工会議所との連携は伺ったが、規模の大きい東京商工会議所との連携は行っているか。
・ 地域における支援機関の立ち位置や、支援機関に寄せられる相談の中で、今回アクティブリストに登録されるような方々が役立つケースはあるのかなど、実態を教えていただきたい。
→東京商工会議所からは IT サービスについて紹介いただくことはあるが、コンサルティングの面で具体的な連携は行っていない。
→過去の中小企業 119 専門家派遣事業において、情報セキュリティを切り口として、地域の中小企業から支援機関に対して寄せられた相談はほぼなかったという実態がある。問題を紐解いていった結果、根源は情報セキュリティの問題だった可能性のあるものも存在したかもしれないが、中小企業が情報セキュリティの問題を認識しなければ、そもそも情報セキュリティの専門家リストを開くにまで至らない地域支援機関が大半であると考える。

・ セキュリティプレゼンテーター制度に登録している情報処理安全確保支援士について参考までにお伺いしたい。セキュリティプレゼンテーター制度を通じた相談や企業支援の実績について教えていただきたい。
→弊会全体として統制をとっているわけではないが、セキュリティプレゼンテーター制度に登録している情報処理安全確保支援士は相当数いる。正式に把握しているわけではないところ、企業への派遣実績は多いようであるが、その後の有償の役務提供契約には、中々つながっていないと認識している。

■ 資料 4 について
グーグル合同会社の資料４（非公開）の内容に基づき、以下のようなプレゼンが行われた。
・ 組織の大小にかかわらず、求められるセキュリティ対策に大きな差はない。一方で、大企業であっても様々な対策を実施する中で疲弊している現状があり、中小企業が適切なセキュリティ対策を実施することは非常にハードルが高い。
・ サイバーセキュリティはテクノロジーの話ではなく、ビジネスのリスクの一つであり、経営者がリスク管理として認識して取組むことが重要。また、テクノロジーが進化しても、人の脆弱性を突かれて、攻撃を受けてしまうことがある。よって、社内人材のリテラシーを最低限のレベルまで高めることが必要。

・ グーグルのサイバーセキュリティ研究拠点では、人材育成は重点領域の一つとしている。
・ グーグルが提供している、「はじめてのサイバーセキュリティ」という無料の講座は、受講者として中小企業を想定。さらにレベルの高い有償の教育プログラムも提供している。
・ 本検討会で検討している、実践的方策ガイドを踏まえて、中小企業に受け取ってもらいやすいコンテンツを提供し、ユーザに届ける役割をグーグルが担うことができると考えている。
・ 中小企業の最大の問題は、対策しようというインセンティブが働かないことであり、社内のセキュリティ人材を確保するのはハードルが高い。人材育成は重要であるが、別の手段として、エンタープライズブラウザのようなセキュアなプラットフォームをサプライチェーン上流の企業が提供することが有効ではないかと考えている。
・ 共同 SOC の構築に向けた検討が進められている地域がある。海外では、その共同 SOC を人材育成の場にしている。即戦力のサイバーセキュリティ人材を育成することができる。

その後、以下の通り、委員より意見があり、グーグル合同会社より応答があった。

＜企業におけるリスクコミュニケーションについて＞

・ 中小企業経営者のセキュリティ意識があがらない現状がある。グーグル社でも、教育コンテンツを提供されているが、中小企業を対象としたものはもっと平易なものでないと難しいと感じた。経営者と責任者と実務者の 3 者間でリスクコミュニケーションをしていくことが必要である。リスクコミュニケーションとして、サイバーリスクについてディスカッションする場が必要である。この様な場でどのような議論をすれば良いか。事例があればお教えいただきたい。
→セキュリティ対策には脅威インテリジェンスが必要となる。攻撃者には得意な攻撃パターンがあるため、脅威を把握した上で自社のリスクに対応するセキュリティ対策を実施することが重要。一方で、脅威インテリジェンスといっても中小企業の経営者には理解が困難である。したがって、より身近な例をあげて、机上演習をすることが良いと考えている。例えば、「もしメールが止まったら、どのように業務を継続するか」、「PC が停止した場合、どこの部署が責任を追うか」等である。

・ セキュリティのオーナーシップの所在を明確にすることが重要。例えば、セキュリティ部門がパッチを適用しようとしても、取引上の理由でフロント部門から拒否されることがある。このような場合にセキュリティインシデントが起こり得るため、責任の所在がフロント部門にあることを示す必要がある。リスクシナリオからこのような会話ができると良い。
・ 日本語ではどちらも「責任」と訳されるが、英語では、「業務の実行責任」を意味する“responsibility”と「結果に対する責任」を意味する“accountability”の 2 つの言葉がある。この2つの責任は別の人が担うべきと考えるが、日本では、この点が整理されていないことが課題と感じる。
・ また、リスクコミュニケーションについては、御指摘の通りである。リスクシナリオは専門性がないと考えられないため、中小企業向けにリスクシナリオの具体的な例があると良い。例えば、グーグル社でリスクシナリオを考えやすくするツール等を所有しているかをお伺いしたい。
→ツールはないが、ホワイトペーパーとして脅威動向を公開している。ただし、セキュリティの知識が無い方は、ホワイトペーパーを読むことが難しい場合もある。ホワイトペーパーをどの程度消化できるか、リスクシナリオにどの程度至れるかは検討が必要である。例えば、IPA が公開している「情報セキュリティ 10 大脅威」をもとにプロモーションや啓蒙活動を行うことも考えられる。

・ そのようなものを「実践的方策ガイド」に盛り込めると良い。

＜セキュリティ人材の育成について＞

・ 共同 SOC は非常に効果的な取組と認識した。中小企業のセキュリティをどこかに任せるしかないという指摘もされているところである。

・ サイバーセキュリティの専門的な知識がない方々に対して、わかりやすく伝えることが重要である。この時、サイバーセキュリティのスキルセットではなく、ソフトスキルが必要となる。この点について、実際に人材教育を検討する中でどのように考えているか。
→グーグル社としても噛み砕いてわかりやすく提供できるところまで至っていないが、無償のコースも提供しているところ、多くの方を対象としたリテラシー向上に向けた動画配信の取組を行っている。ただし、忙しい中小企業の経営者がこのような動画を見ていただけるかは別の課題となる。

＜経済産業省や情報処理安全確保支援士との連携について＞

・ 中小企業や地方の企業ではリソースが少ない。グーグル社が IT やセキュリティを広く支援する活動の中で、情報処理安全確保支援士との連携・協力は可能か。
→可能である。グーグル社が主導することはないが、ブランディングを活用しつつ、議論ができれば良いと考えている。情報処理安全確保支援士と一緒に実験することも考えられるし、スケールする際には協力できると望ましいと認識している。

・ リソースは、ヒト、モノ、カネの 3 つである。ヒトは情報処理安全確保支援士、モノは経済産業省が設定する場である。グーグル社のようなスポンサーによってカネの面が工面できると恒常的な取組が可能となるが、そういう形でうまくできないかと考えている。また、様々な企業とも連携していただけると良い。
→経済産業省も推進する地域 SECUNITY の場を利用して、中小企業にアクセスし、コンテンツを広める活動をしたいと考えている。グーグル社としては 47 都道府県をまわる中小企業向けのセキュリティの啓発活動を検討中で、本取組に対し、関心があるところに適宜お声をかけていきたい。

＜中小企業におけるセキュリティのあり方や他国での状況について＞

・ 経済産業省ではここ 20 年ほど、中小企業のセキュリティレベル向上に向けた取組を進めている。個人的には、中小企業は個別にシステムを運用することをあきらめるべきではないかと考えている。コストの面でもセキュリティの面でも、中小企業は複雑な IT システムを持たない方が良い。自社内から PC やスマートフォンがなくなるわけではないが、クラウド等でセキュリティを一定程度担保できるのではないか。
→ご指摘の点には同感である。パスワード設定やパッチ適用がなくなり、セキュリティの概念や実際の対策がユーザから消えて見えなくなることが究極と考えている。いかにプラットフォーム側でセキュリティを担保していくかが必要であり、日本企業の 9 割以上を占める中小企業を救う手立てと考えている。

・ 中小企業では、セキュリティ投資のインセンティブ設計がなされていない。他国での状況をお伺いしたい。
→全ての国の状況を知っているわけではないが、米国を例にすると、契約の段階で企業はサイバー保険への加入有無を問われることが多い。また、サイバー保険に加入するためのクライテリアが設けられている。この仕組みが中小企業でのセキュリティ投資のインセンティブとなっている。日本では、契約においてサイバ

一保険の加入を求められない、サイバー保険に入るための敷居が低い状況。

■ 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。

＜実践的方策ガイドの修正について＞

・ 「実践的方策ガイド」についてコメントしたい。前回の検討会でも触れたが、Step1 と Step2 の間に情報資産を洗い出す工程に加えて、それらの情報資産がシステム的にどのように扱われているのかを整理する必要がある。どこに保管されているのかなどは情報資産の洗い出しで明確になるが、実際にはそれらがシステム的にうまく扱えるように整理し、（必要な場合には）システムを見直す必要があるとの指摘をしたが、（可能であれば、）「実践的方策ガイド」に盛り込んでいただきたい。

・ 経営者が企業全体のセキュリティ対策に責任をもつ必要がある。「実践的方策ガイド」では、経営者と担当者、従業員との関係性がわかりにくいようにみえる。経営者がセキュリティ担当者にセキュリティ対策実施を担当させ、従業員に（アウェアネス）教育を実施の上、各従業員が必要なセキュリティ対策を行えるようにするという構造を解りやすく示せると良い。

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