サイバーセキュリティタスクフォース
サイバーセキュリティ人材育成分科会（第５回）　議事要旨

１　日　時

平成 31 年４月 25 日（木）10:00～11:00

２　場　所

総務省 10 階　総務省第１会議室

３　出席者

（構成員）後藤主査、園田主査代理、稲葉構成員、大高構成員、岡本構成員、関構成員、武智構成員、水越構成員、与儀構成員

（オブザーバー）河本経済産業省サイバーセキュリティ課課長補佐

（総務省）竹内サイバーセキュリティ統括官、泉大臣官房審議官、赤阪参事官（政策担当）、豊重サイバーセキュリティ統括官室参事官補佐、駒崎地域情報政策室課長補佐

４　配付資料

資料５－１　「サイバーセキュリティ人材育成分科会」第１次取りまとめ案

参考資料５－１　サイバーセキュリティ人材育成分科会（第４回）議事要旨

５　議事要旨

（１）開　会

（２）議　題

①　第１次取りまとめ案について

事務局から資料５－１について説明が行われた。

②　意見交換

事務局からの説明の後、意見交換が行われた。主な意見等は次のとおり。

岡本構成員：ファシリテーターとはどのような人を想定するか。資格で言えば情報処理安全確保支援士、IT コーディネータが想定されるが、そのような資格を有する人はどちらかといえば都会に多くいるため、地方に来てもらったり、地方で育てたりすることも必要。

企業に対して、IT やセキュリティの専門家が難しい話をしても理解してもらえないこともある。商工会議所の経営指導員は日々様々な相談を企業から受けているため、ファシリテーターに対し、どのように伝えれば企業に理

解してもらえるかを教えることもできるのではないか。専門家一人が全ての分野に通じることは難しいため、チームで対応する体制が作れれば良い。

資料５－１中で用いられている「組織能力」という用語について、大企業は能力が高く中小企業が低いという誤解を与えかねず、組織力や組織体制、専門体制といった用語に修正いただきたい。

武智構成員：地域におけるセキュリティのエコシステムの形成について、基礎人材や実務者層、トップ層向けといったパターン、企業の規模ごとのパターン、高専向けのパターンなど、モデル事業もいくつかのパターンが考えられる。零細企業と従業員1,000人以上の企業、あるいは企業と高専とでは、教育のコンテンツやモデルの作り方が異なってくる。全てのパターンを網羅するのは難しいだろうが、バランスはうまくとる必要があるだろう。

与儀構成員：輩出するセキュリティ人材のイメージを明確化することも重要。セキュリティ人材にも、インシデントレスポンスを行う人材やマルウェア解析を行う人材など、様々な種類がある。国内で不足している人材を育成し、我が国のセキュリティレベルを向上させるという観点だけでなく、採用する企業側において人材をどのように活用するかというマッチングの観点も重要。

武智構成員：ユーザー企業におけるセキュリティ人材と、ITやセキュリティベンダーにおける人材とでは、求められる人材像やキャリアパスが異なるため、切り分けて考える必要がある。

企業の中でも、セキュリティの担当者と戦略マネジメント層、CISOとでは求められる資質が異なる。戦略マネジメント層は全体的に分かっている必要がある一方、CISOはよりビジネスに即した観点を求められる。人材ごとに求められる資質を整理した上でモデル事業を展開すべき。

業態によっても事情が異なり、石油化学のような昔からあるプラントの製造メーカーの場合、OTのセキュリティ人材がどれくらい必要かという数字を把握できていないケースもあるため、どの程度セキュリティ人材がいるかという調査も今後必要になるかもしれない。

水越構成員：地域におけるセキュリティ人材のエコシステムの形成について、特定の企業に所属するイメージが強いと感じられる。シェアリングとも組み合わせ、人材だけではなくビジネスモデルまで含めたエコシステムというモデルが構築できると良い。中小企業でセキュリティ人材を何人も雇うことができないという状況の対策として、シェアリングを行うならば、人材のエコシステムにもシェアリングを踏まえた考え方を導入するとより現実的になるのではないか。１つの企業に所属するという前提ではなく、複数の企業への所属を前提にしたり、人材のローテーションを前提にモデル事業を展開すると有効だろう。

関構成員：エコシステムが一番難しく、市場として成立させないとビジネスとして回っていかない。人材だけ育成しても、活躍する場を作らないと意味が無

い。経営層側がセキュリティに対してお金を投資する気になってもらうことが一番重要であり、人材育成だけでなく、どのように経営層に対してセキュリティ意識を持ってもらうかという点について、もう少し踏み込んだ形でのアウトプットがあっても良いのではないか。

例えば、中小企業診断士のような既に企業の経営者層に対してコミュニケーションをとっている人たちに、セキュリティに関してインプットし、経営指導の中でセキュリティの意識付けをしてもらうことも重要。新しくファシリテーターを育成することも重要であるが、商工会議所のような既に中小企業とコミュニケーションをとっている主体に対してアプローチをすることも重要であり、他省庁とも連携しながら施策を進めていくことがエコシステム形成にとって重要。

資料５－１中、セキュリティ女子という用語が用いられているが、「女子」という表現は避けたほうが良いのではないか。

園田主査代理：セキュリティファシリテーターについて、ファシリテーターとして必要なスキルはいくつも資料５－１中にも記載されているが、ファシリテーターになることのメリットが不明確。

コーチングスキルを向上させるための研修機会や講演をする機会、セキュリティファシリテーターになったばかりの人を指導する機会を設けるなど、ファシリテーターとして活躍する具体的なイメージやメリットを提示し、ファシリテーターになることを希望する人を増やす施策も必要。

岡本構成員から言及のあった経営指導員は、どのようなモチベーションで活動しているか。

岡本構成員：経営指導員の中には、中小企業大学校で講師として呼ばれるようなカリスマ的な指導員もおり、人に教える機会があるとモチベーションも上がっていくと感じている。

大高構成員：セキュリティ人材を目指す人たちが、どのようなモチベーションで目指すのか、ビジョンが描けることは非常に大切。

中小企業でセキュリティ人材に対するニーズの掘り起こしができていないために、セキュリティ人材が足りているように見えているのかもしれず、中小企業にセキュリティの重要性を刷り込む人材がまずは必要。

学生が就職する際に、セキュリティ人材には組織やグループといった居場所があり、安心して活躍できる場だというビジョンが描けるようになると良いのではないか。

後藤主査：最初の意識づけは、商工会議所の経営指導員のような人材が行い、セキュリティへの理解が深まれば、セキュリティのコンサルタントや技術的な指導員が必要となるように、段階を踏んでフェーズが上がっていくような形が良いのではないか。

稲葉構成員：ファシリテーターについて、非常に良い仕組みである一方、知り得

た情報をもとに悪いこともできてしまうというリスクもはらんでいる。ファシリテーターのマネジメントをするために、登録制や更新制のような仕組みを導入すべき。

中小企業のシステム構築担当者にインタビューをすると、セキュリティは守られて当然であるため普段は褒められないが、何かトラブルがあれば文句を言われるという、非常に心理的に厳しい業種と感じているようだ。そのような仕事であるにもかかわらず、さらにビジネス的にも回らないということになると、情報を漏えいさせて小銭稼ぎに走るといったように、悪い方向に簡単に走ってしまうため、福利厚生や生活の担保ができるような、ビジネスとして回るビジョンを示す仕組みづくりも必要ではないか。

与儀構成員：実践的サイバー防御演習（CYDER）では倫理規約への同意を求めているほか、民間の高度なセキュリティ研修においても、教わったことを悪用しないという規約にサインをするプロセスがとられている。

ファシリテーターの育成に関しては、Train the Trainer のような、高度な専門教育を行うトレーナーをトレーニングするためのプログラムを確立し、輩出される人材のレベルを一定以上に担保することが必要。

また、セキュリティ人材の処遇を変えられるのは、セキュリティ投資の決定権を持つ経営陣であり、最終的には社長が責任を持つものであるため、例えば、全国で社長向けセキュリティ勉強会を行うことを通じて、セキュリティ担当者のモチベーションを、特にユーザー企業で上げていく必要もある。

武智構成員：ファシリテーターをどのように育成し、レベルをそろえていくかという議論と、ファシリテーターが幸福感を覚えたり、金銭的にコンペンセイトされるという議論は分けて考えるべき。

また、決定権を持っている社長にセキュリティ人材の処遇の重要性を理解してもらうためには、社長に通じる言葉で話をすることが必要。ベンダーのみでサポートすることは難しく、官と一緒になってセミナー等を通じ、ファシリテーターやシェアリングの考え方をインプリメントする方法を議論していくことが重要。

後藤主査：経営指導からコンサル技術へといったような、キャリアのステップアップも重要である一方、自分が大事なことをやっているという意識づけも重要。それぞれを整理して議論しつつ、セキュリティ人材をサポートする役割についても考える必要がある。

大高構成員：中小企業に対し、Society5.0 に向けて、サイバー空間とフィジカル空間の融合には自らも役割を担っていることを気づかせることも必要。

後藤主査：Society5.0 や 5G の時代になると、今まで考えていなかったようなことがサイバーセキュリティ上の新たな課題になる。常に時代とともに変化するものであり、今回の施策も、ステップアップして変化に対応できるようにすべき。

関構成員：経営層にとって、働き方改革などと同様、セキュリティはやらなくて済むならあまり投資したくない領域。働き方改革の例でいえば、金融機関や社労士がセミナーを開催して啓蒙活動を行うことに対して補助金を渡している。セキュリティについても、セミナーを開くことがメリットになるように、セミナーを開催する費用に対して投資をするという方法も有り得る。

与儀構成員：経営層に対しては SDGs とリンクをさせると受けがよくなる。例えば８番の「働きがいも経済成長も」や、産業と技術革新の基礎をつくる９番等と結びつけ、国際的な SDGs の動きに合わせて総務省が行っている取組だと見せられるようにするのも良いのではないか。

大高構成員：行政にとって、SDGs はあらゆる分野で避けて通れないキーワードになっている。持続可能な社会を実現する中で、中小企業が継続していくためには、セキュリティ対策への経営資源の投資は避けて通れないといったように、SDGs の実現への寄与とサイバーセキュリティを紐付けるような意味づけを与えるのがよいのではないか。

水越構成員：昨今、攻撃者は組織犯罪として攻撃をする傾向にある。サイバー攻撃に遭った場合は犯罪被害であり、犯罪被害に遭わないためにはどうすれば良いかという認識を強く持ってもらうことも必要。

③　その他

事務局から、第１次取りまとめ案を意見公募手続にかける旨の説明があり、後藤主査から、提出された意見等を踏まえた修正については主査一任とする旨の提案があり、了承された。また、竹内統括官より挨拶があった。

（３）閉会

以上