

**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4回） 議事要旨**

1 日 時

平成31年3月18日（月）10:00～12:00

2 場 所

総務省8階 第1特別会議室

3 出席者

（構成員）後藤主査、稲葉構成員、大高構成員、岡本構成員、関構成員、宇都田氏（武智構成員代理）、手塚構成員、長谷川構成員、水越構成員、与儀構成員（オブザーバー）大能内閣サイバーセキュリティセンター参事官補佐、伊奈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、木村参事官（総括担当）、赤阪参事官（政策担当）、近藤参事官（国際担当）、豊重サイバーセキュリティ統括官室参事官補佐、三木地域情報政策室企画官

4 配付資料

資料4-1 「サイバーセキュリティ人材育成分科会」第1次取りまとめ骨子案
参考資料4-1 サイバーセキュリティ人材育成分科会（第3回）議事要旨

5 議事要旨

（1）開 会

（2）議 題

① 前回会合の振り返り

事務局から参考資料4-1に基づき、前回会合の振り返りが行われた。

② 第1次取りまとめ骨子案について

事務局から資料4-1について説明が行われた。

③ 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：資料4-1の2ページ目について、東京商工会議所の調査結果を引用し、「中小企業のセキュリティ意識は低い」と記載されているが、調査の中身を見ると、セキュリティ意識に課題があるとは書いておらず、セキュリテ

ィ対策をやらなければいけないとは思っているが、取組が進んでいないとか、不安を抱えたまま事業を進めざるを得ないとか、優先順位が上がらないとかいった書き方にすべき。

稲葉構成員：セキュリティファシリテーターとは実際に何をする人か。

豊重参事官補佐：中小企業等の担当者が集まる場において、セキュリティについて講師の役割を担う人をファシリテーターと呼び、その人に対してセキュリティ対策の教え方を教える講習を実施することによって、裾野までセキュリティ対策が広がることを期待している。

稲葉構成員：もう少し具体的なイメージはあるか。セキュリティに関する講習といっても、セキュリティは大事なのでやりましょうというだけか、それとも、具体的な対策まで踏み込んで教えるのか。

赤阪参事官：中部や関西では、地域の中核的な企業や人が、自分の企業の組織内だけではなく、周りの企業や自治体も含めて地域全体としてのセキュリティの意識を上げていこうという活動をしており、そのような地域ごとの取組をこれから広げていくために、自分たちの地域の中で、周りを巻き込んで引っ張っていけるリーダー的な存在を育成するところから始められないかという問題意識である。

セキュリティに限らず、地域の情報化についても、地域や自治体を引っ張っている人がいるところが非常に進んでいる。そういったリーダーを育成するためのカリキュラムやプログラムを開発してモデルをつくることで、ほかの地域にもひな形として広げていくことができなかと考えているところ。

稲葉構成員：関西サイバーセキュリティ・ネットワークで中心的な役割を担っている人のような人材を育てるというイメージか。

赤阪参事官：関西の取組でも、コミュニティに集まっているのは大企業が中心であり、これから中小企業にも広げていこうということだったが、中小企業に広げていく際に参考となるモデルを作りたいという問題意識である。

後藤主査：中小企業をセミナー等と呼ぶためには、経営課題といった、中小企業の課題やニーズを広く捉えたファシリテーターが、セキュリティについても重要性を説いてくれるといいという指摘もあったが、その点についてはどのように考えているか。

赤阪参事官：セキュリティに対するモチベーションやインセンティブを働かせるうまい伝え方をファシリテーターに対するプログラムの大きな要素として組み込んでいければよいと考えている。

与儀構成員：ファシリテーターの取組を推進していく上で、ファシリテーターが企業に所属している場合、講習会等に所属会社がポジティブに送り出せるようにすることが重要。例えば、認定ファシリテーターといった称号を与えることにより、企業の業務が終わった後のファシリテーターとしての活動を会社が応援できる工夫があるとよい。

大高構成員：ファシリテーターといっても、求められるレベル感は様々であり、中小企業の経営層にセキュリティは必要と意識づけるには、セキュリティ人材というよりも、営業に近いような人材が非常に重要。セキュリティの取組が、地域の中でも、だんだん周りの企業で広がっているようなことを、企業同士のコミュニケーションの中に入り込んで営業する仕組みが必要。

セキュリティの必要性を感じた企業が駆け込める、互助会的、駆け込み寺的な組織が商工会議所や自治体にあり、そこに相談に行くとファシリテーターがいて、相談に乗ってくれるという仕組みも必要。

しかし、現状は、セキュリティ研修や講習会に人が集まらないというギャップが大きな課題としてあり、セキュリティの大切さをしっかりとすり込むファシリテーターも必要。

単に一言でファシリテーターという人材をつくるよりは、役割分担を明確にしたほうがよいのではないか。

宇都田氏：中小企業の社長や、従業員数が10人以下、5人以下の企業の社長の間でも、セキュリティに関する意識や雰囲気醸成できている地域は、顔が見える信頼関係の中で、地域で雰囲気を醸成できている。信頼関係ができると、核となる人を中心に、周りの企業等もセキュリティに取り組まなければならないという意識が出てくるので、ファシリテーターの育成という取組は非常に有効。

中小企業や従業員数が10人、5人の企業の意識をどう向上させていくか、まだ届いてないところにどうリーチしていくかという仕組みづくりをうまく工夫していけば、より取組が広がっていくのではないか。

手塚構成員：ファシリテーターというと、その人の力量や熱意といった属人的な部分に依存するところが大きいため、どのような仕組みで、ファシリテーターが地域の体制に入っていけばいいのかという形づくりの検討も必要。

関構成員：ファシリテーターは非常に重要であるが、いかにして育てるかという方法は難しい課題。セキュリティだけを知っている人を育てても、そもそもセキュリティに興味のないところには届かないだろう。

一人の力で入り込んで説得をし、セキュリティに興味を持ってもらうことは非常に難しいと考えられるので、チームで対応するという観点が必要である。コミュニティの中で、経営層のレベルにセキュリティに投資をしなければいけないという話をできる人もいれば、ペネトレーションテストをできる人もいるといった役割分担があるからこそ、関西の取組もうまく回っているのだろう。

ファシリテーターを一人の人材モデルとして考えるのではなく、エリアごとに機能があって、それぞれのパーツ、レベル感を担う人材をどう育てるかという、もう少し解像度を上げた議論が今後は必要。

水越構成員：ファシリテーターの考え方には賛同。

ただし、ファシリテーターの知識を時代に合ったものにしていく仕組みを埋め込んでおく必要がある。

また、リスクをあおるだけではなく、ソリューションと一緒に提供することも求められるため、セキュリティ事業との連携まで含めて制度設計をすることが必要。

後藤主査：ファシリテーターが活動する「地域」は、どの程度の規模が適当か。

大高構成員：都道府県単位というのが一つの目安になる。

後藤主査：人材マッチングやシェアリングについて意見はあるか。

長谷川構成員：人材のシェアリングのために、我々はクロスアポイントメントを通じた大学等との産学連携に取り組んでいるほか、サバティカルイヤーの間に、教員や官の職員が民間に出てくることができる仕組みづくりを作れないか、高専機構と検討しているところ、企業が人を出したがらず、実務経験者の交流になかなか結びつかないという問題に直面している。

関構成員：シェアリングの場合、県単位よりもう少し広い単位になるのではないか。関西サイバーセキュリティ・ネットワークのような、既にコミュニティのあるところとうまく連携しながら、どの団体がどのエリアで活動しているというデータを総務省で取りまとめ、地域情報化アドバイザーのような形で、県から依頼できるという仕組みをつくるのが現実的ではないか。企業からも人を出しやすくなるように、認定制度なども組み合わせ、うまく地域のコミュニティに参加する動線ができるとうい。

後藤主査：ビジネスの観点から、企業側の目線を見た場合に、どのような性質のコミュニティであれば、インセンティブを働かせやすいか。

長谷川構成員：クロスアポイントメントの例で見ると、講師としてのキャリアプランが生まれるといった、キャリアプランに結びつくものが個人のモチベーションやインセンティブとしては大きいと感じる。

与儀構成員：全部オンサイトでするわけではなく、ウェブ画面上でアドバイス等を行えるプラットフォームの構築やその利活用も非常に重要。

また、Secure SketCHのような、各企業共通で使えるシステムもうまく利活用すると良いのではないか。今までは大企業しかセキュリティ可視化のコンサルティングを受けられていなかったが、Secure SketCHには地方の中小企業からも入力や登録が増えてきている。首都圏の企業以外にも広がりが見え始めており、このようなツールがあるということを知れば、利用者も増えるだろうから、うまく情報提供をすることも必要。

後藤主査：コミュニティ単位のデータベースという話が出ているが、個人のレベルのデータベースについてはどうか。

アメリカでは、トップレベルに近いセキュリティ人材のデータベースが作成されており、どこの州には人が足りないといった情報が可視化される一方、給与の高騰に結びついているという話もあるが、そのような取組は日本にマ

ツチするか。

今回検討するのは、もう少し地味なレベルであるが、個人情報取扱という負担もある中で、積極的にデータベースをつくっていけるか。

大高構成員：普段からセキュリティ人材として活動している人であれば登録してくれるだろうが、登録したくない人材もいるだろう。

中小企業であれば、こういうサービス、こういう CIS0 が欲しいということにいきなりはならず、駆け込み寺に駆け込んで、Secure SketCH のようなセキュリティサービスは何を導入したらよいかや、そのサービスを導入するのであれば、どのような人材が必要かといった情報を入手できるほうがよく、そのような情報を、県単位の駆け込み寺的な組織間で、全国規模で流通させるのがよいのではないか。そのような駆け込み寺があれば、人材の就労支援や活動の居場所作りにもつながるだろう。

与儀構成員：弁護士ドットコムというサービスでは、士業である弁護士が登録して一般の方々からの質問に答え、課金をすれば前のデータなども見られるようになる。弁護士のナレッジを提供し、相談者にいい回答をしていたら、次の仕事にもつながっていく。

セキュリティ人材のデータベースでも、教えたい人と教えてほしい人がうまくマッチングし、前の回答も有効活用できるという形にするのが良いのではないか。

後藤主査：脆弱性の情報のフォーマットや、人材のスキルマップなど、議論が様々あり、固まっていない現状でも、データベースは作れるか。

与儀構成員：例えば、ウイルス対策やインシデント対応をどのようにすればよいかといった中小企業から出てくる質問のレベルであれば、大体はレベルが定義できる。また、セキュリティ対策について同じ悩みを持つ人が、特に地方の中小・中堅企業間では多いと考えられ、先例を見れば解決できることもあるのではないだろうか。

水越構成員：事前の予防だけでなく、事後の対処にすぐに駆けつけるというサービスも併せて両面やるのが良いのではないか。

後藤主査：事前と事後では、コミュニティのつくり方やサービスの受け皿は異なるか。

水越構成員：明らかに違う。事後であれば、警察へ行く前の相談に乗るということもあるだろう。

後藤主査：人材マッチングに関する議論は、人の部分がバーチャル化され、組織やコミュニティレベルでのマッチングという議論がでてきた。また、マッチングにひもづくサービスとの関係も、事前と事後で二種類に分かれるという話もあった。

稲葉構成員：セキュリティファシリテーターのレベルはいろいろなレベルがあり、求められるレベルが、ツールをつくって、中小企業の社長にセキュリティっ

てこういうことだと教えることや、入門編を教えることであれば、比較的誰でもできるだろう。

ただ、本当に中小企業の社長にセキュリティに取り組んでもらうのであれば、セキュリティが大事と伝えるだけではなく、経営に口を出せる人が、特にvCISOでは必要になり、中小企業の社長が信頼できるくらいの人材を育成しなければならない。資料4-1に記載されている、セキュリティママや、副業オーケーのアナリスト等を、中小企業の社長が信頼できるレベルにするためには、相当な教育が必要になるだろう。

また、セキュリティは非常にセンシティブであり、倫理的な点も非常に問題。vCISOという、センシティブなところを扱う人材を産み出そうとするのであれば、vCISOが企業に言って誘導しようと思えば何でもできてしまうという問題も考えていく必要がある。

後藤主査：誰がその地域の産業において一番影響力があるかというデータは、総務省として持っているか。

赤阪参事官：総合通信局が地域の企業等と懇談会等を形成していることもあるが、各地域で誰がキーパーソンかというところまでは、全国的にはフォローできていないだろう。

総務省では地域情報化アドバイザーという施策において、オープンデータやセキュリティ、システムといったように、アドバイザーの得意分野やスキルをマッピングして、自治体側がそれを見てマッチングするという取組を進めている。

セキュリティでもそのような取組ができないかという問題意識を出発点として、自分の企業が何ができていないかを可視化できる仕組みを用いつつ、自分たちではどうしていいかわからないということであれば、専門家からアドバイスをもらえる仕組みができないかと考えている。

セキュリティ人材側についても、例えばシニア層の、従前各企業でセキュリティや企業のリスクマネジメントや監査を担当されていた方や、セカンドキャリア的に地域に戻って活動しようとしている方、一時的にお子さんを出産されたりした方のキャリアをお手伝いできるのではないかと、という問題意識もある。

後藤主査：産業中心の地域や自治体中心の地域といったように、幾つかパターンがあると、人材のデータベースについて類型化して議論がしやすいのではないだろうか。

若手人材の育成と就労支援といった人材のエコシステムについて意見はあるか。

与儀構成員：セキュリティベンダが連合で沖縄に新組織をつくり、基礎的な業務を委託することができないかという検討を進めているところ、地域のセキュリティ人材が増加して雇用につながるモデルであること、最終的には地域で

自走可能なモデルであることが重要という観点から、雇用は沖縄電力グループやりゅうせきグループといった、地場の企業が中心になって推進することとしている。セキュリティベンダの連合による新組織は、主に基礎的な業務が遂行できるスキルを習得できるカリキュラムを作成し、トレーナーを派遣してOJTを含む教育を実施。セキュリティ企業は、その教育に応じた業務を委託することを前提として教育を行い、就労にダイレクトにつなげていくことを目指す。

最終的には、地場の企業が新たなサービスなどを開発、提供していくことで、大手セキュリティベンダがカバーし切れない中小、中堅企業などにも安価なサービス等をリリースしていくことができれば、相対的に地域のセキュリティレベルが上がるだろうということを考え、一般社団法人の枠組みを形成し、そこで教育、OJT等の場を持ち、地場の企業のほうからそこに勉強しにきてもらい、そこを経由して地場の企業に就職するというモデルを構築予定。4月以降の一般社団法人化を目指し、最終検討に入っているところ。

宇都田氏：地域の人材育成のエコシステムの形成に関して、大学院や高専との連携は非常に有効。

沖縄での取組の紹介もあったが、地域において、サイバーセキュリティに関して高い能力や意識を持つ学生を、どう短期的に育成していくかが非常に重要。そのためには、演習を含めた共通的なプラットフォームで実践していくという方法が良いのではないか。

また、学生の中には単に技術一筋だけではなく、海外に行きたいとか、海外の研究者とダイレクトにコミュニケーションしてみたいとか、その中で、日本のサイバーセキュリティやITセキュリティベンダがどうあるべきかを考えたいとか、非常に強い意識を持った学生もいるので、そのような学生にASEANとの連携も含め、どのように場を提供していくかが重要。

後藤主査：高専では、建築のような、情報ではない学科の学生にもセキュリティを教える講座を提供しており、若いころからセキュリティもしっかり勉強しつつ、専門は建築や機械といった広がりのある人材を育成でき、セキュリティ専門人材は要らないが、セキュリティをわかっている人が横にいてほしいという地域の企業にとっては非常に有益ではないか。

文科省でも、学部レベルでのセキュリティ教育を推進しているが、本来の授業で手一杯で、セキュリティのコースをやりたくても入れられない状態。

関構成員：SecHack365やセキュリティ・キャンプを経験している高度なレベルの学生は、どれぐらいセキュリティ系の企業に就職しているか。

与儀構成員：6、7年前は、セキュリティ・キャンプをトップで出た学生も日系企業に就職できずに外資に行くというような状況であったが、今はセキュリティベンダ等がかなり食指を高くしており、状況はかなり好転してきている。

長谷川構成員：セキュリティ・キャンプやSecHack365、JNSAが開催しているCTF

であるセキュコンに参加した学生がセキュリティベンダに就職する率は非常に高い。

そのようなレベルの学生に限らず、潜在的な層にも裾野を広げていく必要があり、JNSAでも合同インターンシップを開催しているが、セキュリティやクラウド、AIの仕事が具体的に何か、よく分かっていない学生も多く、知ってもらう機会も作る必要があると感じている。

また、第二新卒を含め、キャリア採用者が学生に比べてIT業界やセキュリティ業界に興味を持たないという課題もあり、その裾野を広げる仕組みも必要と感じているところ。

与儀構成員：サイバーセキュリティ人材の、ヘッドハンターのインセンティブが最近100%になったという情報がある。紹介料100%を払ってでもその人材が欲しいという企業に、ヘッドハンターたちは優先的に人材を紹介しているようだ。

アメリカでは既にサイバーセキュリティという業種の給与が高騰しているが、早晚日本もそういう流れは来るのではないか。

後藤主査：今議論をしている、地域のサイバーセキュリティ人材もその影響を受けるか。

与儀構成員：サイバーセキュリティ人材への待遇や仕事の受け皿にも地域間格差が存在し、地域には仕事を作らないと、人は増えないだろう。

稲葉構成員：セキュリティについて勉強したいという意欲が高い学生は、勉強すればするほど、自分の力を試すため、レベルの高い会社や外資系企業に就職しようとする。

地域でセキュリティ人材に働いてもらうためには、地元を活性化したいという気持ち、地域愛が重要。Uターン人材のような、一回首都圏に出たが、やはり地元が好きなので戻りたいという学生のほうが狙い目ではないか。セキュリティ人材に対するニーズが非常に高いが故に、地方に行かなくても済むという状況で、地方に行きたいという人をどうやって増やすかという観点が必要。

手塚構成員：現在就職している方たちは、大学教育でサイバーセキュリティという分野がなかった。30代後半ぐらいの人たちを含め、そのような人達に対しどうやって教育していくかということも地域にとっては非常に重要な課題で、若手人材とセットで、地域の高専等を拠点にして育成する仕掛けを作る必要がある。

ファシリテーターが属人的にならないようにする仕掛けとしてシェアリングをどのようにしていくか、教育の場、インキュベーションの場をどうやって地域に造成していくか、それを産業界、地方自治体、大学、どこの拠点に設けるか。地域の特性も検討しつつ、日本全体としてはボトムアップを合わせていくという視点も踏まえて考えていく必要がある。

宇都田氏：セキュリティの基礎知識や基礎能力を有する人材に、地域にどうセキュリティを教えたいか、地域の中小企業をどう元気づけたいかという思いを動機づけすることや、その人材を可視化することが重要。

地域の中小企業側からしても、地域愛や地域が好きだというモチベーションが見えれば、この人に任せておけば大丈夫という信頼感も生まれる。

後藤主査：シェアリングといっても、中小企業であれば、一人の専門家を雇うことではないため、本業とセキュリティの兼務（シェア）、複数の組織におけるセキュリティ人材のシェア、二つの観点がある。

セキュリティだけではなくて本業も見ていくという発想で、地域のリターンやシェアリングも考えていかなければいけないだろう。

関構成員：セキュリティファシリテーターという役割を、地域愛ということも含めて、地域でのイネーブラーとして、事例をたくさん知っており、セキュリティに関するリスクを経営層に伝わる言葉で話せたり、地域のコミュニティや勉強会を作れたりといったスキルと、セキュリティそのものの技術的なスキルとに分けて考える必要がある。

大高構成員：どこにいても学べるとか、地方で働きながらスキルを身につける場に行けるとか、セキュリティ人材のスキルを維持できる環境がないと、モチベーションや地域愛だけではうまく回らない。

また、就労支援という観点から、セキュリティを本業としてファシリテーターとなるのか、本業を持ちながらファシリテーターをやるのかということも踏まえつつ、セキュリティに対する知識をずっと維持できるような環境づくりも非常に重要。

そのような仕組みを用意できて初めて、東京集中ではない形を構築できる。

後藤主査：最新情報を常にアップデートすることで、地域での信頼を得続けることも大切。

顔が見える、信頼できる体制が必要とか、セキュリティの知識よりも営業のセンスが必要とか、ファシリテーターも個人ではなくチームかもしれないし、データベースも個人のデータベースよりもコミュニティのデータベースかもしれないという意見があった。

人材マッチングなどでも、最後は経営に助言する必要があるので、信頼を得られる、倫理観がしっかりしている体制でなければいけないという意見もあった。

さらに、地方に一旦戻ってしまうと、なかなか勉強できないというのでは困り、常にセキュリティの知識を、地方にいても簡単に最新のものにアップデートできるような体制が必要という指摘もあった。

④ その他

事務局から、次回の日程について説明があった。

(3) 閉会

以上