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

2019年3月18日

地域におけるサイバーセキュリティ人材育成に関する取組の方向性

1. 地域におけるセキュリティファシリテーターの育成

2. 地域でのセキュリティ人材のシェアリング（人材マッチング）

3. 地域における人材エコシステムの形成（若手人材の育成と就労支援）

1．地域におけるセキュリティファシリテーターの育成

現状・課題

○　中小企業のセキュリティ意識は低い（※）。サプライチェーンの一端を担う地域の中小企業がリスクとなるおそれがあり、セキュリティ意識の向上が必要。

（※）ICTを活用する上での課題として、情報漏えい等セキュリティに不安があると答えた割合は、従業員100人以上の企業では50%であるのに対して、従業員5人以下の企業では19%であり、より小さな企業ほどセキュリティ意識に課題（＊）

（＊）出典：東京商工会議所生産性向上委員会「生産性向上・ICT活用状況に関するアンケート調査結果報告書」（2017年3月2日）

○　また、地方では研修機会が少なく、機会があっても参加しない。

先進的な取組

事例1:中部・関西における取組

地域の中核企業が取引関係の枠を超えて、周辺の企業等と顔の見えるネットワークを構築し、セキュリティ対策について啓発し合っている。

○　中部地域における取組：CCSC（中部サイバーセキュリティコミュニティ）

大学や中部地域の企業等が集まり、中部地域インフラ事業者等合同訓練等を実施。訓練を通して、組織間で情報連携に取り組んでいる。また、大学と企業が連携して、共同研究や実証の取組も行っている。

○　関西地域における取組：関西サイバーセキュリティ・ネットワーク

産官学が連携して、企業担当者向けのサイバーセキュリティ・リレー講座、企業経営者層向けセミナー・イベント、サイバーセキュリティ関連の取組情報の共有等の取組を行っている。

1．地域におけるセキュリティファシリテーターの育成

先進的な取組

事例2：米国ボストンにおけるISAOの事例

ACSC（advanced cyber security center）は、ボストンにある大学や企業（特に金融機関）が中心となり、サイバーセキュリティの情報共有等を行っている非営利団体。ボストンは金融機関が数多く存在し、サイバーセキュリティに対する意識が高いことが発足のきっかけ。ボストンという地域に特化しているため人が集まりやすく、フェイス・トゥ・フェイスでの活動が活発。特に、CISOが2週間に一回、フェイス・トゥ・フェイスでディスカッションを行う機会もある。

団体の活動を継続するため、各企業から拠出金を募っており、それを原資にサイバーセキュリティ人材を雇い、参加企業間でシェアしている。また、ボストンには世界的に著名な大学が立地することから、優秀なエンジニアがACSCに学生時代から所属し、就職時もボストンの企業を選ぶというケースも存在。さらに、ACSCに加入していることでサイバーセキュリティ保険加入の際の保険料も安くなることで、その分新しいイノベーションに投資できることが、ACSCに所属するメリットとなっている。

取組の方向性

○　地方でのサイバーセキュリティ研修機会の拡大やインセンティブの創出

○　地域単位での共助の仕組みを構築し、地域のセキュリティファシリテーターを育成

・地域でのコーディネーターとして、地域のファシリテーターが核となって、周辺の中堅・中小企業、自治体等にサイバーセキュリティ講習等を実施。

・セキュリティファシリテーターとなる人に、中小企業等へのセキュリティ対策の教え方を教える講習を実施。

⇒　インセンティブでモチベーションを働かせつつ、必要なセキュリティ対策について学んでもらうためのカリキュラムやテキスト、ツール等の作成

1．地域におけるセキュリティファシリテーターの育成

主な意見

○　地域のコミュニティを形成し、ワークショップ形式で双方向に学ぶことのできる研修やイベントを継続的に行い、企業の垣根を越えて、他事業者とのコミュニケーションをフェイス・トゥ・フェイスで行うことは重要。

○　サイバーセキュリティ人材の不足については、CxO（CEO、CIO、CTO等）のクラスには伝わっていないのではないかと感じている。ISAOの考え方のように、地域のマルチステークホルダーにサイバーセキュリティ人材への意識を醸成させ、組織化し、教育システムを共通化していくことが非常に重要。

○　地域においてコミュニティを主導していくファシリテーターの育成が必要。また、コミュニティの中で、若手にどうやって知識やスキルを移行し、コミュニティを仕切る力を渡していくか考えることが必要。

○　現場の人たちのことを考えて、守れないレベルの厳しいセキュリティにするのではなく、ルールづくりやツールの導入など、セキュリティを守ってもらうための手段を考えることを通じて、セキュリティに関するスキルが伸びるということの繰り返しにより人材が育つ。

○　米国では、全てのステークホルダーが一緒になって、自衛団のような発想で、地域のサイバーセキュリティを確保するための取組がある。我が国でも、地域ごとに様々なステークホルダーが一緒になって、積極的に意見交換や情報交換を行うことを通じて、人材育成を行うことが必要。

2. 地域でのセキュリティ人材のシェアリング（人材マッチング）

現状・課題

○　セキュリティ担当者がいる中小企業は全体の半数弱で、いてもその大半は兼任（※）。

（※）専任の担当者がいる：4%、兼任の担当者がいる：44%、担当者はいない：50%、無回答：2%（*1）

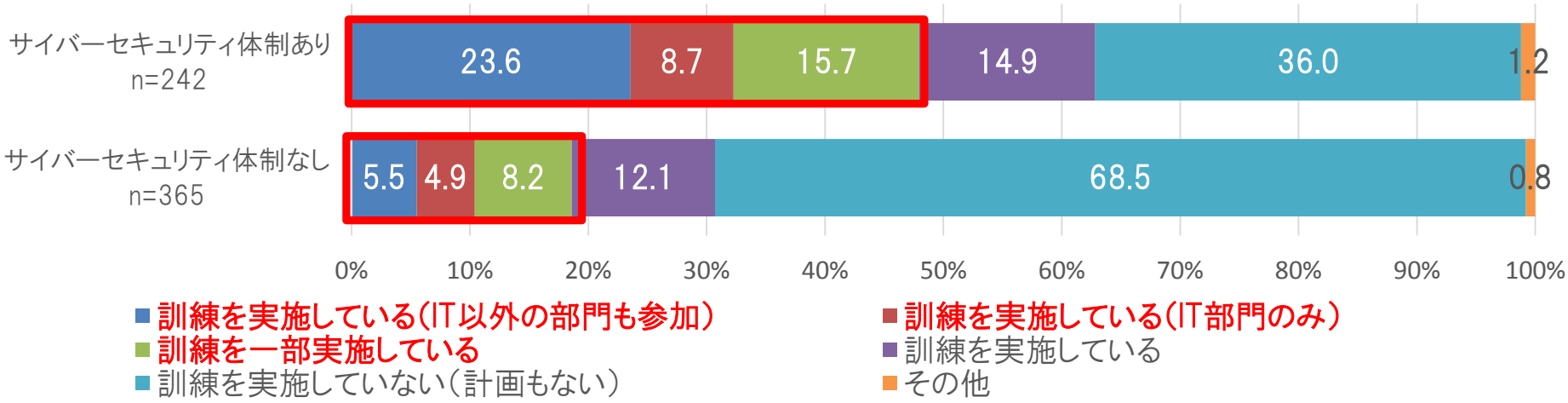
（*1）出典：大阪商工会議所「中小企業におけるサイバー攻撃対策に関するアンケート調査」（2017年6月）

・　例えば、東京都大田区の大田工業連合会の会員企業の約半数が3人以下の企業、約2割が10人以下の企業であり、これらの企業では専門人員を現実的に置くことができない。

・　仮に置いたとしても問題の発生頻度は低いことから費用対効果が合わない。

・　中小企業において、小さい規模の会社は狙われないのではないか、セキュリティ対策はコストである、面倒くさいといった意識も非常に強い。

○　サイバーセキュリティ体制がない組織では対策が進まない傾向にある（下図（*2））。



（*2）MS&ADインターリスク総研「企業の情報セキュリティ対策に関する実態調査報告書」（2018年12月）をもとに総務省作成

2. 地域でのセキュリティ人材のシェアリング（人材マッチング）

先進的な取組

事例1：vCISO（バーチャルCISO）

グローバルセキュリティエキスパートが提供するWebサービス。中堅・中小企業や個人事業主等、サイバーセキュリティ対策に問題を抱えている企業と、多様なスキルを持っているセキュリティ専門家をつなぎ合わせるためのマッチングサービス。各人材の強みを可視化することで、企業の特性に合わせマッチングがしやすくなっている。

事例2：セキュリティ対策ができていないところの見える化（Secure SketCH）

NRIセキュアテクノロジーズの提供する無料ツール。約80問の設問に回答することで、800社以上の他社データと比較・分析し、その企業のセキュリティ対策状況を偏差値として可視化できる。また、ベストプラクティスの参照や、地域企業のセキュリティ対策状況を俯瞰して管理することもできる。

取組の方向性

○　自社の状況に合わせて、地域の情報化やセキュリティのスキルを有する人材をマッチングする仕組みを構築

・マッチングの仕組みや契約の在り方を整理

・Uターン・Iターンセキュリティ人材、シニアセキュリティ人材、女性セキュリティ人材等の活用

○　一つの企業・組織で一人のセキュリティ担当者等を雇うのではなく、複数の企業・組織で必要なスキルを有する人材をシェアする仕組みを構築

⇒　<u>地域単位でスキルごとに人材をデータベース化</u>

2. 地域でのセキュリティ人材のシェアリング（人材マッチング）

主な意見

○　各企業の状況に合わせてどういうサイバーセキュリティ対策をしていくべきかを、vCISO（バーチャルCISO）のような人材が地域に拡散して、各企業に教えていくことが求められる。

○　首都圏を中心に、多様なセキュリティスキルを持った人材が雇用形態に関する悩みを持っている状況にある。アーリーリタイヤしたスペシャリスト、独立したコンサルタント、セキュリティママ、副業OKのアナリストといった人材が存在しており、人的リソースの偏りをなくす施策が必要。

○　地域の企業を包括的に守る「地域CISO」を育成し、「シェアする」ことが考えられる。例えば、「地域CISO」が地域のIT人材等にサイバーセキュリティのナレッジを教育することや、各企業に対して物理的に往訪するのではなく、リモートから支援をする仕組みも考えられる。その際、首都圏のセキュリティ人材のリソースもシェアすることや、個社の特性に合わせて、最適な人材をマッチングすることも考えられる。

3. 地域における人材エコシステムの形成（若手人材の育成と就労支援）

現状・課題

○　地域にセキュリティ人材の受け皿がなく、地域で若手人材が育たない・定着しないといった悪循環。

○　国全体のサイバーセキュリティ人材不足から、地域の中小企業のペネトレーションテスト等、一部の業務にセキュリティベンダの手が回らない。

先進的な取組

事例1:複数のセキュリティベンダが連携して、業務の一部を地域にアウトソーシング

セキュリティ基礎人材が働ける新組織を地域（沖縄）で設立し、その地域で基礎的なセキュリティスキルを学んだ人材ができる業務は、セキュリティベンダ各社がその地域に発注するスキームを構築する動きがある。

事例2：高専生が地域企業や若者・高齢者層へ講義

長崎県警の協力のもと、佐世保高専生が県内の小中学校でサイバーセキュリティに関する講義・デモを実施（平成29年度は中学校3校で実施、平成30年度は10校以上で実施予定）。

取組の方向性

○　雇用の受け皿と研修・演習機会の創出による地域での人材エコシステムの形成

○　民間等と連携した実践的な人材の育成

⇒　専門学校・大学等にツールの使い方等を学べる場を提供し、就業につながる即戦力を養う。

○　さらに、大学（院）や高専等と連携することで、下請け的な業務にとどまらず、ハイエンドな業務も含めて地場産業化し、より高度なエコシステムの形成も期待。

3. 地域における人材エコシステムの形成（若手人材の育成と就労支援）

主な意見

○　様々な人材育成プログラムにおいてサイバーセキュリティ人材の育成は進められているが、雇用（育成の出口）を考えなければ人材は停滞し続ける。サイバーセキュリティ人材の受け皿不足も問題。サイバーセキュリティ人材の働き場所を作り、我が国の企業のサイバーセキュリティに携わる環境を構築することが必要。

○　自治体、中小企業、教育機関等による地域におけるマルチステークホルダーによる人材育成のエコシステムの形成という、横串の観点で捉えることも必要。

○　高専等の教育機関において、建築等の分野を学ぶ専門人材に最新のセキュリティに関する内容を教えることにより、セキュリティスキルも併せ持った人材を育成することができる。好きで自発的、自律的にやっている学生に対しては、いかに時期や状況に合った機会を与えるかが重要。

○　セキュリティのトップ人材は、高専等の教育機関だけで育てることは困難であり、できるだけ外部のITベンダ、セキュリティベンダ、自治体等の協力を得ながらトップ人材を育てる環境をつくることが、トップ人材向けの教育には必要。

○　深刻化する人材不足に対して、セキュリティベンダが共同でセキュリティ人材育成を行い、リソースを確保するスキームも考えられる。OJTと研修プログラムを組み合わせて専門性を高め、高度人材にステップアップできる育成も必要。