6月14日14時公表予定

資料14－4

「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

2019年6月

目　次

1　はじめに

○　近年、IoT機器の増大や巧妙化・複雑化するサイバー攻撃により、民間企業等において情報漏えい等の被害が発生しており、サイバーセキュリティ人材を育成することは急務である。

○　サイバーセキュリティ人材の不足が叫ばれて久しく、さらにサイバーセキュリティ人材が地域的に偏在しており、地方においては一層厳しい状況にある。また、サイバー空間の攻撃者は地理的な距離に関係なく、弱いところをターゲットとすることから、「地域力」を結集・活用してセキュリティ人材の裾野を広げ、底上げすることが必要である。

○　こうした状況を踏まえ、サイバーセキュリティ人材育成分科会は、我が国のサイバーセキュリティ人材に係る現状と課題を整理し、その課題を解決するための方策について検討を行うことを目的として、サイバーセキュリティタスクフォースの下に開催される会合として、2018年12月に設置され、特に地域におけるサイバーセキュリティ人材の現状と課題を整理した上で、地域におけるサイバーセキュリティ人材育成に向けた方策について検討を行った。

【開催状況】

第1回 2018年12月25日
（中部地域における周知啓発の取組、地域におけるサイバーセキュリティ人材を育成するためのアイデア　等）

第2回 2019年1月17日
（関西地域におけるサイバーセキュリティ人材育成に向けた取組状況と課題、沖縄におけるセキュリティ人材の育成と雇用構想）

第3回 2019年2月12日
（藤沢市のITガバナンスと人材育成の取組、小規模・零細企業のセキュリティ対策、高専における情報セキュリティ人材育成）

第4回 2019年3月18日
（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）

第5回 2019年4月25日
（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）

2　地域のセキュリティを巡る現状・課題

地域課題の解決のためには、Society5.0の実現が不可欠であり、5G、IoT、AI等の様々な技術を活用し地域活性化を図ることが求められる。その基盤として、地域におけるサイバーセキュリティの確保が今後ますます重要となるところ、地域のサイバーセキュリティを巡る現状・課題として、次の三つの偏在が存在している。

（１）研修機会の偏在

サイバーセキュリティに関する研修や気づきを得る機会は、全国で万遍なく開催されている状況とは言えず、都市部に集中しており、地方での開催は少ないといった研修機会の偏在が見られる。

⇒　地方ではもともと気づきの機会がないため、研修があっても参加者が少なく、参加ニーズがないことから、地方で研修が開催されないといった悪循環が生じている。

（２）組織体制の偏在

地域におけるサイバーセキュリティ上の課題として、都市部に集中する大企業と比べて、地方の中小企業では十分にサイバーセキュリティ体制が構築されていないといった組織体制の偏在が見られる。

⇒　規模の小さな中小企業が多い地方においては、サイバーセキュリティ対策として何をすればいいか分からないが、サイバーセキュリティの専門人材を雇用することや専門組織を設置する余裕がなく、いつまでもサイバーセキュリティ対策が進まないといった悪循環が生じている。

（３）就業機会の偏在

セキュリティ企業においても人材は不足しており、地方や中小企業向けのビジネスには十分に手が回っていない状況がある。また、地方においてはセキュリティに関する雇用の受け皿がなく、都市部と地方ではセキュリティに関する就業機会の偏在が見られる。

⇒　地域においてセキュリティに関する雇用の受け皿が無いため、地域の若年層がセキュリティ人材を目指さない、あるいは、セキュリティに興味があっても地元に残らないという状況があり、地域におけるセキュリティ人材がさらに不足するといった悪循環が生じている。

2(１) 研修機会の偏在

現状・課題

○ サイバーセキュリティに関する研修や気づきを得る機会は都市部に集中しており、地方での開催は少ない。
→参考1参照

○ 国立研究開発法人情報通信研究機構(NICT)が実施している実践的サイバー防御演習(CYDER)は数少ない全国で実施している演習である。東京・大阪・愛知・福岡の参加率(定数充足率)はそれぞれ90.6%・69.6%・54.2%・52.1%である一方、それ以外の地域の平均参加率は36.9%である(全国平均は45.9%)。

○ CYDERの受講自治体においては、都道府県庁はほとんど受講している一方、町・村の受講率は12%である。
→参考2参照

○ 企業においても、規模が小さいほどセキュリティに不安があると答える割合は少ない状況にある。

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、以下のとおり(＊)。

従業員数1～5人:19%、従業員数6～20人:34%、従業員数21～50人:42%、従業員数51人～100人:41%

(＊)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)

○ 他方で、地域の中小企業においても、サプライチェーンの一翼を担うなど重要な役割であり、セキュリティ対策に関する意識を高めることが重要である。

○ 地方ではもともと気づきの機会がないため、研修があっても参加者が少なく、参加ニーズがないことから、地方で研修が開催されないといった悪循環が生じていることから、気づきの機会を創出することが必要である。

参考1　サイバーセキュリティに関する研修の開催状況

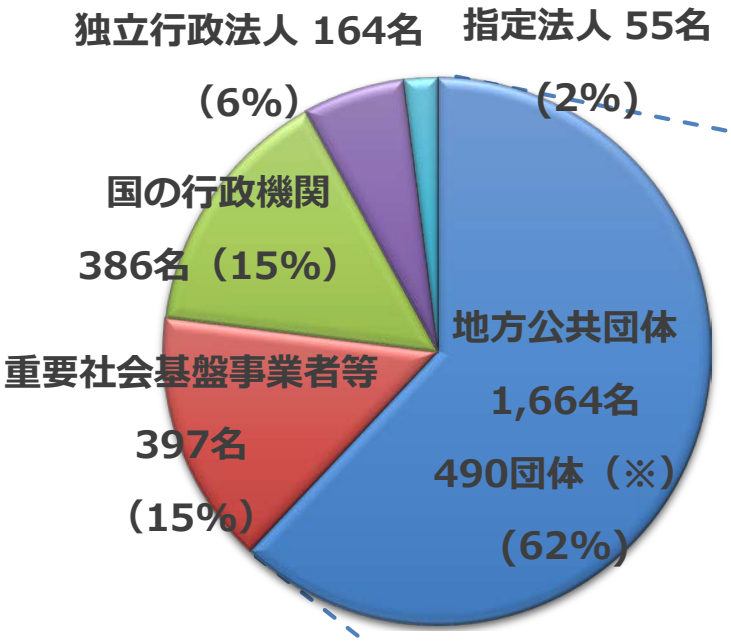
○　サイバーセキュリティに関する研修は都市部で開催されることが多い。

会社名等	コース名	開催地　回数(2018年度)
NECマネジメントパートナー	実践！サイバーセキュリティ演習 -インシデントレスポンス編-	東京　8回
アイ・ラーニング	日本IBM CSIRT研修(Computer Security Incident Response Team)	東京　3回
富士通ラーニングメディア	サイバーレンジによる実践的防御演習基礎	東京　5回
日立インフォメーションアカデミー	Certified Ethical Hacker	東京　4回
CTCテクノロジー	CSIRT構築・運用支援研修	東京　2回
サイバーディフェンス研究所	基礎・APT対処演習	東京　2回
情報通信研究機構(NICT)	実践的サイバー防御演習(CYDER)	全国　107回 (各都道府県で開催)
情報処理推進機構(IPA)	講習能力養成セミナー	全国　21回 (20の都道府県で開催)

出典：民間企業等が開催するサイバー演習等のデータをもとに総務省作成(2018年12月時点調べ)

参考2　実践的サイバー防御演習（CYDER）の受講実績（2018年度）

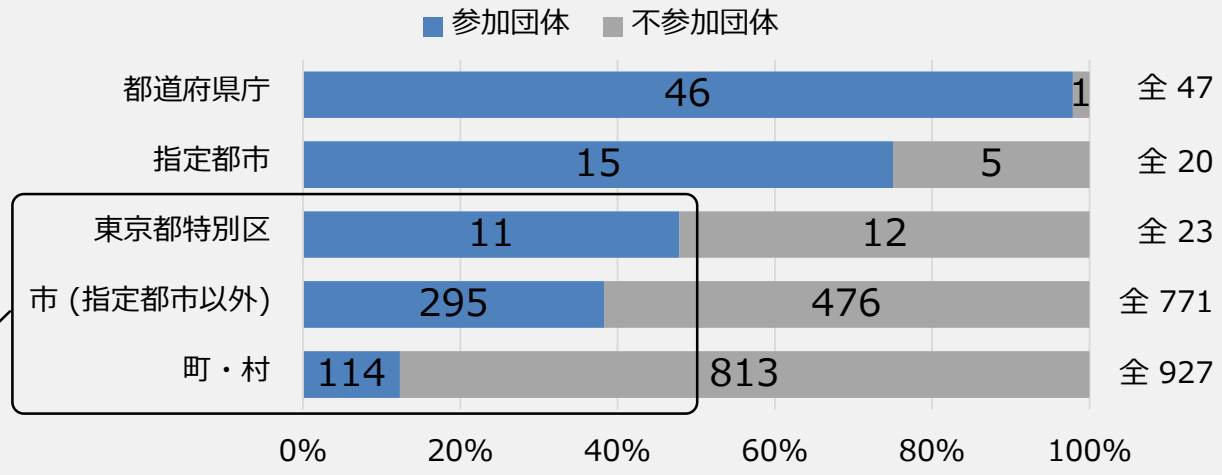
① 組織別の受講者数（全コース総数2,666名）



（※）地方公共団体481団体に加え、医療広域連合等９団体が受講

東京都特別区及び市は
半数以下であり、
町・村は12%

②地方公共団体（全1,788団体中481団体が受講）



2(2) 組織体制の偏在

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、また、存在する場合もその大半は兼任という状況にある。**→参考3参照**

○ CISOの設置率は、1,000名以上の企業では33.8%、企業全体では25.6%にとどまっており、また、同じようにCSIRTの設置率でも、1,000名以上の企業では40%、企業全体では16.5%にとどまっている。規模が小さい組織ほど、セキュリティ体制が整っていない状況にある。**→参考4参照**

○ CISO、CSIRT等の体制が無い組織では、体制のある組織と比べてセキュリティ・インシデント発生時の訓練を実施していないなど、セキュリティ対策の取組状況と直結している。**→参考5参照**

○ 規模の小さな中小企業が多い地方においては、サイバーセキュリティ対策として何をすればいいか分からないが、サイバーセキュリティの専門人材を雇用することや専門組織を設置する余裕がなく、いつまでもサイバーセキュリティ対策が進まないといった悪循環が生じている。

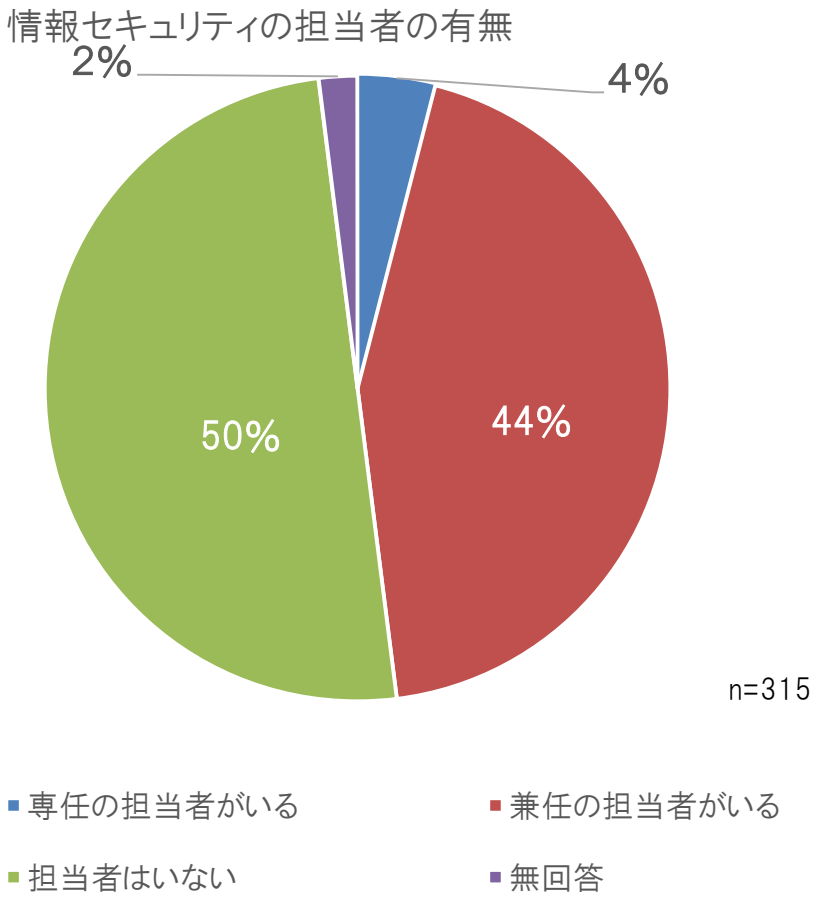
○ 「サイバーセキュリティ戦略」(2018年7月閣議決定)では、経営層の意識改革、戦略マネジメント層(※)及び実務者層・技術者層の育成・確保が重要であるとされている。

(※)経営層が示す経営戦略や事業戦略の下、組織がマネジメントすべき様々なリスクの一つとして、業務やサービス等を実現するために必要なサイバーセキュリティに係るリスクを認識し、事業継続と価値創出に係るリスクマネジメントを中心となって支える立場として、社内外の実務者・専門家を活用・指揮しつつ、対策や事案への対応を実践する役割を担う層を「戦略マネジメント層」と位置付けている。

○ 一方、人材が少ない中小企業では戦略マネジメント層が果たすべき役割を経営層自ら担わざるをえない状況にある。

参考3　情報セキュリティの担当者の有無

○　中小企業の過半数で、情報セキュリティ担当者がいない。担当者がいる場合でも、4割が他の業務との兼任。

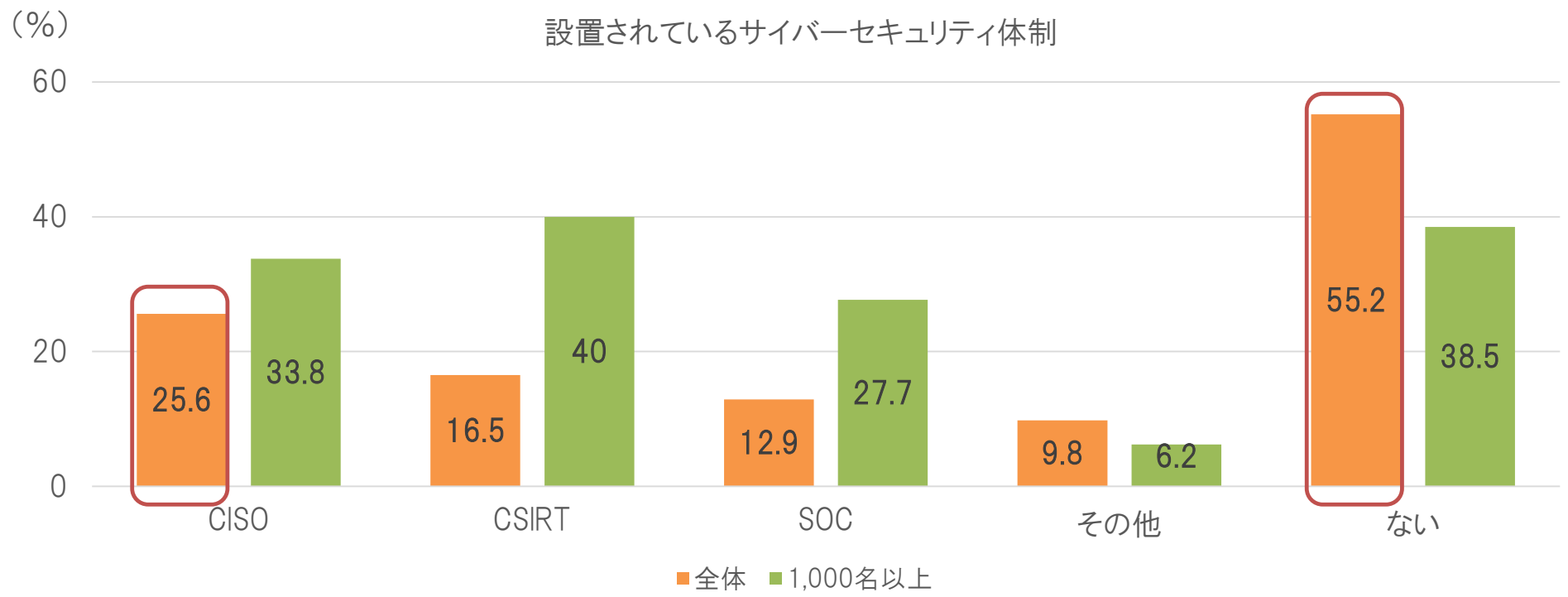


出典：大阪商工会議所「中小企業におけるサイバー攻撃対策に関するアンケート調査」（2017年6月）をもとに総務省作成
http://www.osaka.cci.or.jp/Chousa_Kenkyuu_Iken/Iken_Youbou/k290630cyb_ank.pdf

参考4　CISO、CSIRT等の規模別の設置割合

○　過半数の企業ではサイバーセキュリティ体制を構築していない状況であり、サイバーセキュリティ体制があると回答した企業のなかで最も多く設置されているのはCISOである。

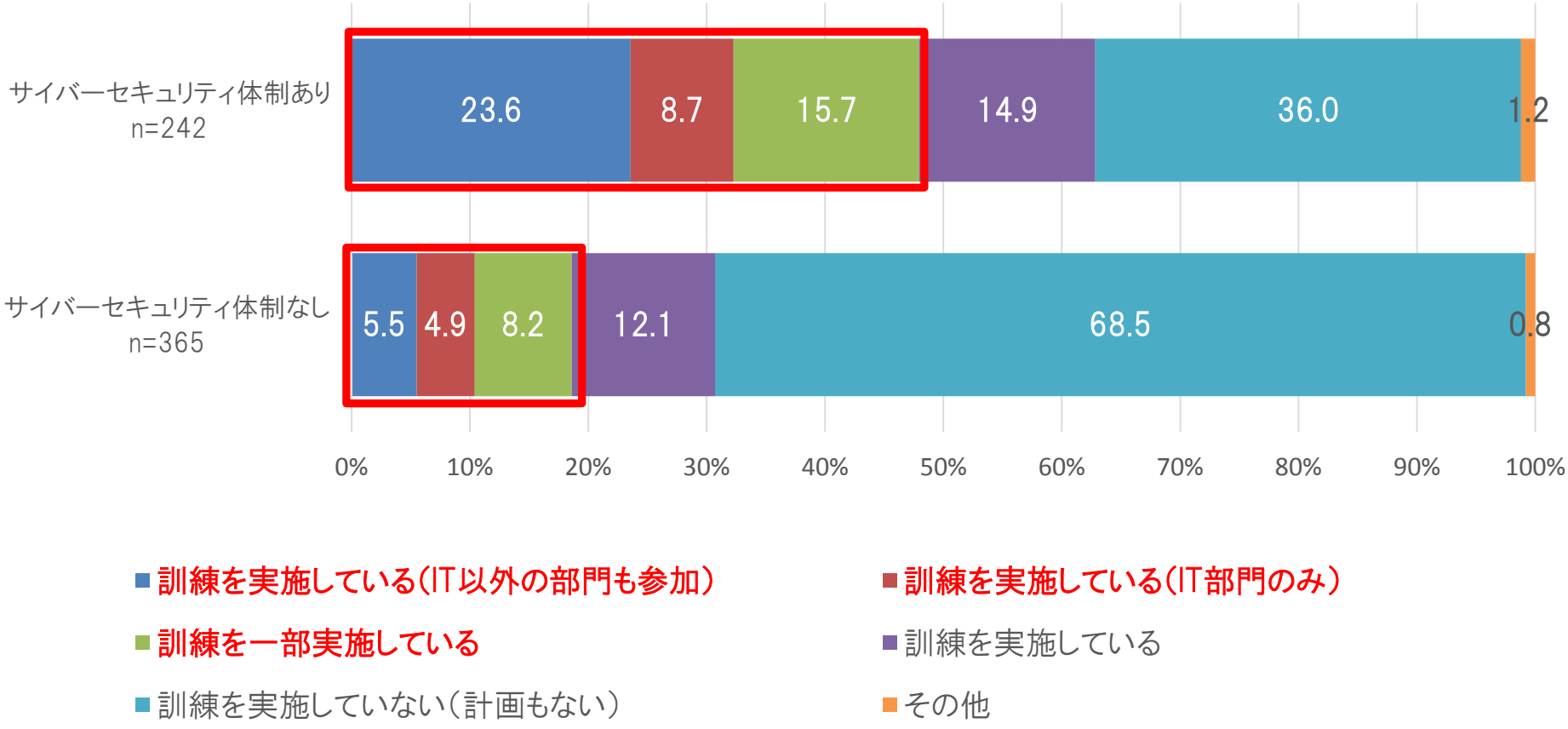
○　従業員数1,000名以上の企業以外では、CISO、CSIRT、SOCの設置が進んでいない。



出典：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

参考５　セキュリティ・インシデント発生時の訓練実施状況

○　サイバーセキュリティ体制の有無で比較すると、体制のある組織・企業では、「訓練を実施している（IT以外の部門も参加）」、「訓練を実施している（IT部門のみ）」、「訓練を一部実施している」の合計が48.0%と半数近い。一方、体制が無い場合には、同合計が18.6%となっており、30ポイント近い差が出ている。



出典：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(３) 就業機会の偏在

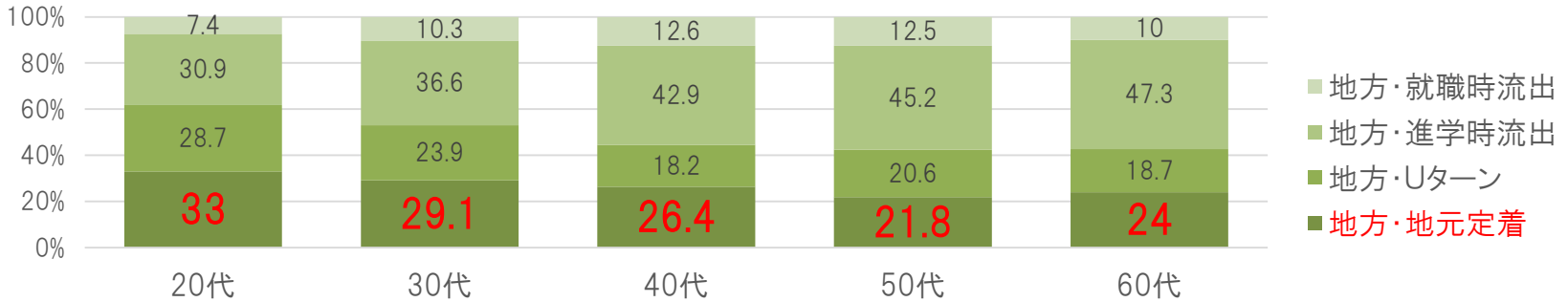
現状・課題

○ セキュリティ企業においても人材は不足しており、地方や中小企業向けのビジネスには十分に手が回っていない状況がある。

○ 地方においてはそもそもニーズが少ない、案件の金額が小さいなどの要因から、それぞれの地域においてもセキュリティに関する雇用の受け皿が育ちにくい。

○ 地域においてセキュリティに関する雇用の受け皿が無いため、地域の若年層がセキュリティ人材を目指さない、あるいは、セキュリティに興味があっても地元に残らないという状況があり、地域におけるセキュリティ人材がさらに不足するという悪循環が生じている。

○ 若者の地元志向は強くなっており、セキュリティについての雇用の受け皿が形成されれば、若者が地域に根付く可能性がある。



(＊)図出典：独立行政法人労働政策研究・研修機構「若者の地域移動−長期的動向とマッチングの変化−」JILPT 資料シリーズ No.162(2015年10月)

○ セキュリティ人材が都市部に集中する状況から、地方でのセキュリティに関する取組を活性化し、それを担う人材をそれぞれの地域でも自律的に輩出していく環境を構築していくことが必要である。

3　地域におけるセキュリティ人材育成に向けた方策

1. 研修機会の偏在

気づきの機会がない
研修があっても参加者が少ない
地方で研修が開催されない
悪循環

2. 組織体制の偏在

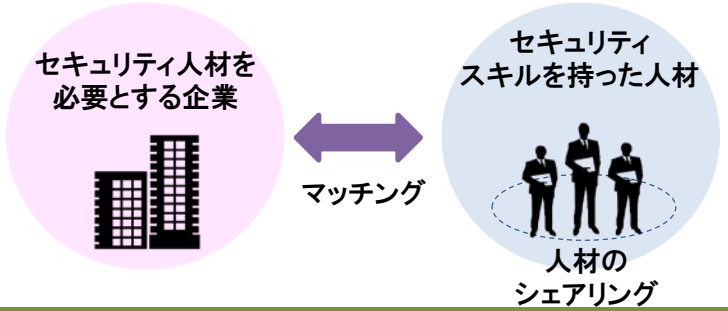
何をすればよいかわからない
専門人材を雇用できない
対策が進まない
悪循環

3. 就業機会の偏在

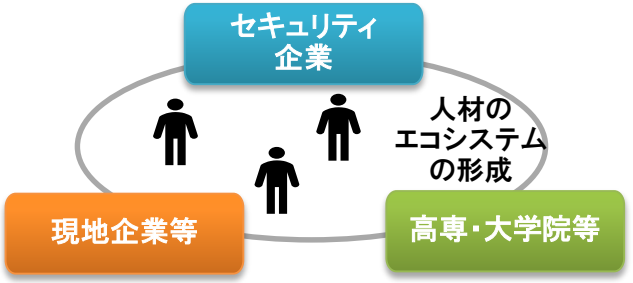
雇用の受け皿がない
地域の若年層がセキュリティ人材を目指さない
地域におけるセキュリティ人材がさらに不足
悪循環

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



3. 地域におけるセキュリティ人材のエコシステムの形成



3(１) 地域におけるセキュリティファシリテーターの育成

基本的考え方

○ サイバーセキュリティ対策ではセンシティブな情報を取り扱い、倫理的な側面も問題になることから、顔が見え、信頼できるコミュニティの中で啓発し合うことが有効ではないか。

○ このようなコミュニティを構築するためには、地域の中核企業やリーダーが中心となって、取引関係にかかわらず「共助」の考えの下、地域全体のセキュリティ対策を底上げすることが必要ではないか。

（例）中部サイバーセキュリティコミュニティ（CCSC）の取組
関西サイバーセキュリティ・ネットワークの取組
米国ボストンにおけるISAO(※)の取組

→参考6参照

（※） ISAO(Information Sharing and Analysis Organization)：サイバーセキュリティに関する情報を複数の組織で共有するコミュニティ活動

○ 地域ではセキュリティを教える人が少ないので、まず教える人を教えることが必要ではないか。

○ その際、単にセキュリティの重要性を指摘したり、セキュリティの知識を提供したりするだけでは、関心の低い中小企業等には訴求しないことから、コミュニティに参加してもらうための営業的なセンスのあるスキルを持った人材が必要ではないか。

○ また、農業や町工場など、さまざまな地場産業においてもIoTが拡がりつつあり、IoTの利活用におけるセキュリティ対策など、新たな動向にも対応することが必要ではないか。

参考6　地域におけるコミュニティの事例

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（中部電力等）等が集まり、組織間で情報連携に取り組んでいる。

○　中部地域インフラ事業者等合同訓練を実施。サイバー攻撃が発生したときに何が起こり得るかを重要インフラ事業者間で共有し、地域にいかに被害を少なくするかといった観点から訓練を実施している。また、訓練に向けたシナリオ検討を若手人材が行い、シナリオをディスカッションする中でコミュニティができ、顔が見える関係であるからこそ、情報交換がしやすくなる人間関係が構築されている。また、訓練を行う際、自社の対処だけでなく他社の対処の方法を見ることも刺激になっている。

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。

○　関西情報センターが行うサイバーセキュリティ研究会は、企業の枠を越えてさまざまな企業のサイバーセキュリティ担当者が参加することができ、情報交換できる場として、関西全体のセキュリティレベルを向上していく取組を行っている。

米国ボストンにおけるISAOの取組

○　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である。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している。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。

3（１） 地域におけるセキュリティファシリテーターの育成

具体的方策

○　地域の中小企業等のセキュリティ意識を高めるためには、地域での顔の見えるコミュニティ活動を活性化することが重要であり、そのような活動を中核としてリードするファシリテーターを育成するためのモデル事業を実施する。

○　当該モデル事業を通じて、ファシリテーターを育成するためのカリキュラムの体系化・研修コンテンツを作成する。その際、ファシリテーターに求められるスキルとして、対象のレベルに応じたセキュリティに関する知識だけでなく、企業の経営課題や利益（儲け）など、企業の経営層等の関心を惹くような内容を含め、地域の多様なステークホルダーを巻き込むためのノウハウも盛り込むことが必要。

○　ファシリテーターのモチベーションの維持や、所属組織が送り出しやすい環境を整えるため、ファシリテーターに肩書き（ステータス）を与えることも考えられる。

○　また、ファシリテーターは古い知識ではなく最新の知識を習得していることが必要であり、最新情報を常にアップデートすることが地域での信頼を得続けるためにも重要である。地域におけるSociety5.0の進展状況を踏まえ、IoT等のセキュリティ対策に関する知識やスキルも必要となる。

○　モデル事業の成果を全国に横展開することで、様々な地域におけるサイバーセキュリティに関するコミュニティ活動の活性化を図る。

3（２） 地域におけるセキュリティ人材のシェアリング

基本的考え方

○　ファシリテーターの活動等を通じて、セキュリティに関心が高まった企業等に対し、具体的に何をどうすればよいのかを見える化することが有効ではないか。

（例）NRIセキュアテクノロジーズ「Secure SketCH」**→参考7参照**

○　中小企業1社でセキュリティの専門家を雇ったり、専門組織のコンサルを受けることはできなくても、複数の企業が共同でシェアすることができるのではないか。

○　その際、監査やリスクマネジメント経験のあるシニア人材、U･I･ターン人材、人生100年時代のセカンドキャリアを地域への貢献に活かそうとする人材、産休･育休からキャリア復帰を目指す女性人材などの活用が考えられるのではないか。

＜NRIセキュアテクノロジーズ発表資料（サイバーセキュリティ人材育成分科会（第1回）資料1－4）より＞

都市部におけるセキュリティ人材の状況を見ると、雇用形態に関する悩みを持つ人も多い。

・　アーリーリタイヤしたスペシャリストや定年退職をしたセキュリティマネジメントに従事していた人は、退職後もフルタイムでは働きたくないものの、週に2日程度働いて、ワーク･ライフ･バランスを充実させたいと考えている。

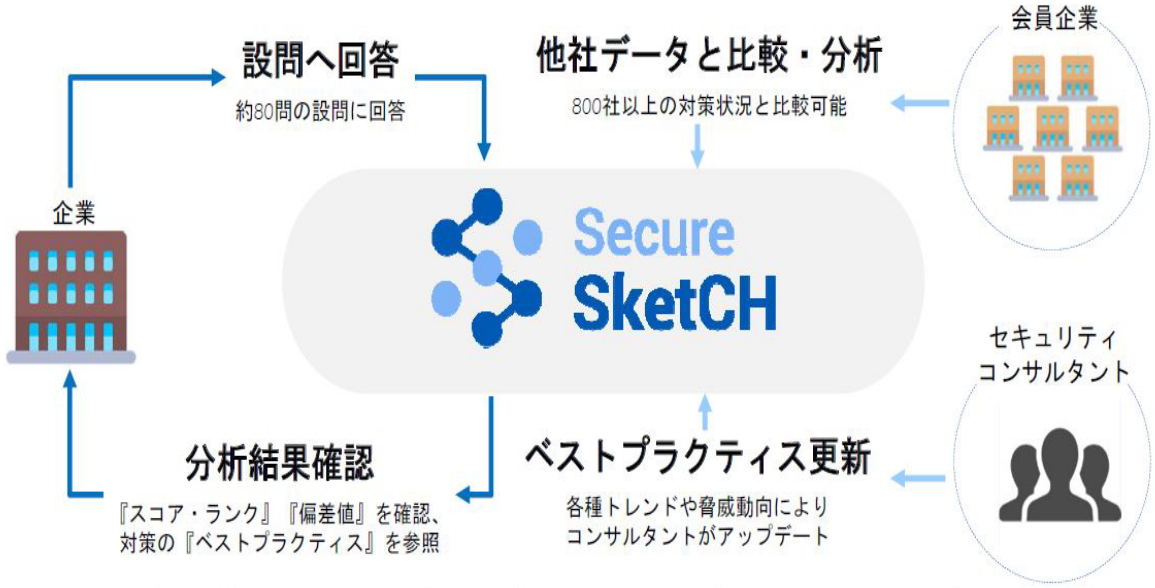
・　独立したコンサルタントや副業可能なアナリストとして働いている人は、特定の企業の案件だけでなく、さまざまな企業の案件に携わりたい、空いている時間を副業に使いたいと考えている。

・　セキュリティの仕事を現場の第一線で行っていた女性で、育児等のタイミングで一旦リタイアし、育児が落ち着いてきたタイミングで仕事に復帰したい人は、復帰に向けて、在宅で育児の合間でできる仕事があればしたいと考えている。

参考7　Secure SketCHの概要

○　企業等の自らの組織におけるサイバーセキュリティ対策の実施状況について、見える化を行うことで、自らの組織において弱点となっているサイバーセキュリティの状況を知ることができ、弱点となって対策が必要な部分について講ずるべきサイバーセキュリティ対策について、専門家の派遣を求めることが可能となる。

○　自らの組織のサイバーセキュリティ対策の状況を見える化するサービスとして、例えば、NRIセキュアテクノロジーズの提供する無料ツールに「Secure SketCH」がある。約80問の設問に回答することで、約1,800社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。



図出典：サイバーセキュリティ人材育成分科会（第1回）資料1－4

3(２) 地域におけるセキュリティ人材のシェアリング

具体的方策

○ セキュリティ人材を効率的・効果的にシェアするために、セキュリティ人材の得意分野や知識レベルで細分化し、セキュリティの専門家や専門組織のデータベース化を行う。

○ 企業等において必要なセキュリティ対策の優先度に応じて、体制の整備や設備の導入など、組織として講ずるべき措置について助言等を行うことができるセキュリティの専門家や専門組織をマッチングし、複数の中小企業等でシェアするためのモデル事業を実施する。

＜検証事項＞

- ユーザー側の企業等のニーズの把握（どのような相談内容が多いか等）
- 供給側のセキュリティ専門家等の人材のボリュームやセキュリティの知識レベル
- 派遣を希望する期間、頻度（週1、月1等）等
- マッチングに最適な地域の規模　等

＜参考：地域情報化アドバイザー派遣制度＞

ICTを利活用した取組を検討する地方公共団体等からの求めに応じ、ICTの知見等を有する「地域情報化アドバイザー」を派遣**→参考8参照**

○ その際、ユーザー側の企業等にセキュリティの専門家等が全ての助言を対面で行うのではなく、ICTを活用してリモートで対応する仕組みを構築することも必要である。

＜参考：弁護士ドットコム＞

弁護士ドットコムは、弁護士の3人に1人超が登録しており、約14,000人の弁護士が登録している。月刊サイト訪問者数は1,150万人の日本最大級の法律相談ポータルサイトであり、無料で相談をすることが可能。取扱分野や営業時間など、様々な条件で弁護士を探すことが可能で、弁護士のプロフィールには自己紹介や取り扱った事件、料金表など、豊富な情報が掲載されている。（出典：弁護士ドットコム　https://www.bengo4.com/）

○ モデル事業の成果を全国に横展開することで、地域におけるサイバーセキュリティに関する組織体制の底上げを図る。

参考8　地域情報化アドバイザー派遣制度

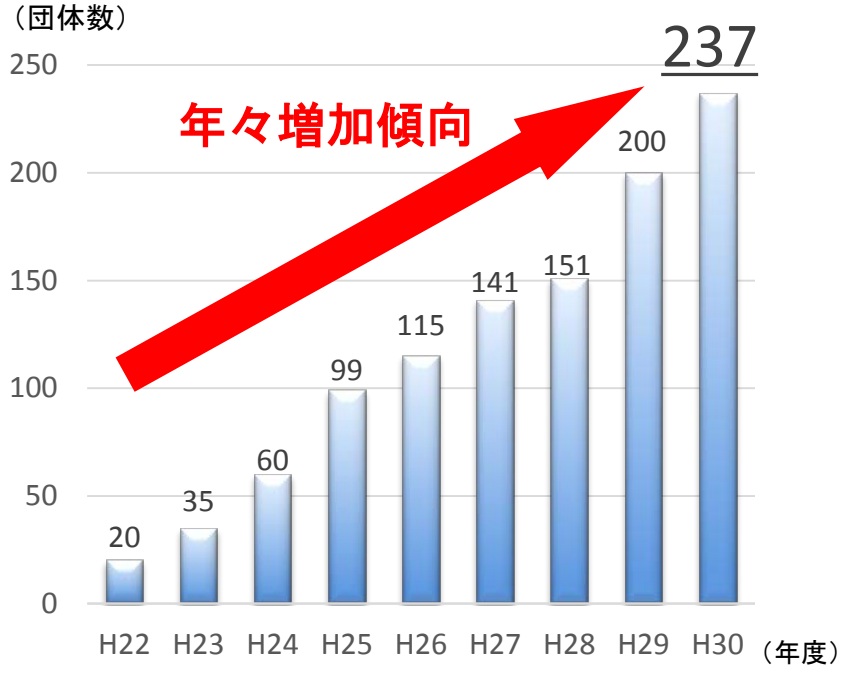
○　地域が抱える様々な課題を解決するため、ICTを利活用した取組を検討する地方公共団体等からの求めに応じ、ICTの知見等を有する「地域情報化アドバイザー」を派遣し、ICT利活用に関する助言等を行うことにより、地域におけるICT利活用を促進し、活力と魅力ある地域作りに寄与するとともに、地域の中核を担える人材の育成を図ることを目的としている。

○　依頼する際、課題やテーマが決まっている場合は、事務局からテーマに沿った支援が可能な人材を紹介することが可能であり、課題やテーマが漠然としている場合は、「ICT地域活性化サポートデスク」で相談が可能である。

派遣の仕組み

※平成31年度の総務省地域情報化アドバイザーは207名。

派遣団体数



3(３) 地域におけるセキュリティ人材のエコシステムの形成

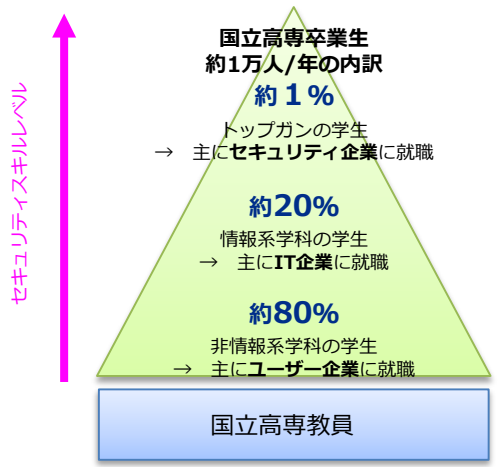
基本的考え方

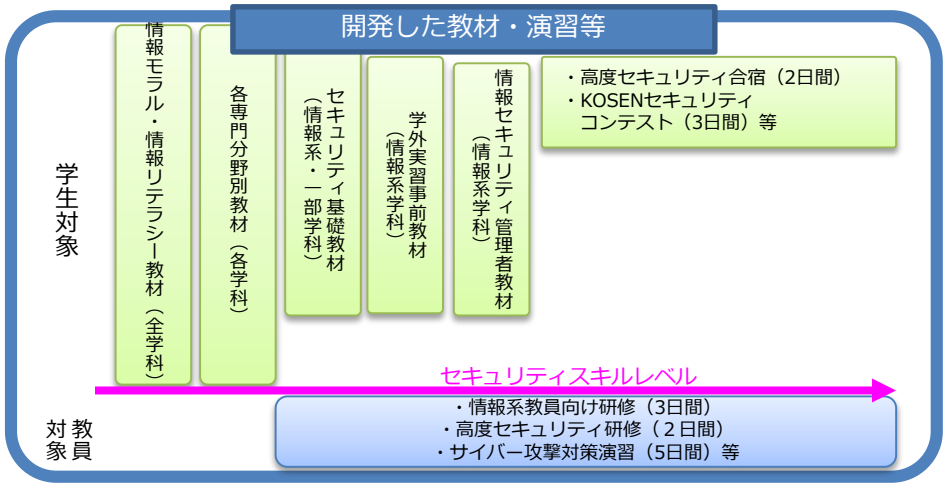
○ セキュリティ企業が共同で、ペネトレーションテストなど業務の一部を沖縄の企業にアウトソーシングする動きがあり、こうした取組を推進することは、地域におけるセキュリティビジネスを興すために有効ではないか。この取組に合わせ、学生等にセキュリティツールの使い方など、就業につながる実践的な研修を行うことで、地元志向の若手人材が地元で就業するサイクルを創り出すことができるのではないか。

○ 地域のセキュリティ人材が増加して雇用につながり、地域の中小企業等に安価なセキュリティサービスを提供することにより、地域全体のセキュリティレベルの向上が期待される。さらに高専や大学、大学院でのセキュリティ教育も強化されつつあり、それらの教育機関と連携することも有効ではないか。

＜参考：高専におけるセキュリティ教育＞

全体の約20%にあたる情報系学科の学生に専門的なセキュリティの教育を行っているほか、残り80%の非情報系学科の学生にもセキュリティを教育し、各専門分野において「守るべきものは何か」を知った人材を輩出。





図出典：産業サイバーセキュリティ研究会WG2（第3回）事務局説明資料
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_keiei/pdf/004_03_00.pdf

3(３) 地域におけるセキュリティ人材のエコシステムの形成

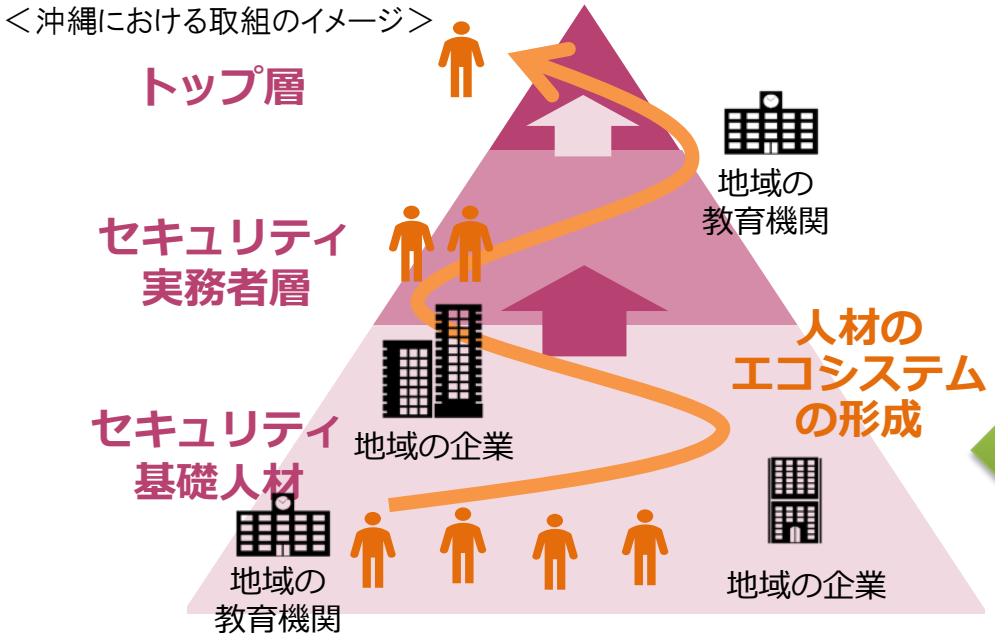
具体的方策

○ 地域におけるセキュリティ人材のエコシステムの形成を図るべく、民間による雇用の受け皿創出の動きに合わせ、そこで求められるスキルに合わせたツールの使い方など、就業につながる実践的な研修カリキュラムの体系化や研修コンテンツの作成を行うためのモデル事業を実施する。

○ さらに、地域の高専・大学・大学院等の高等教育機関と連携することにより、高度なセキュリティ人材の輩出や、下請的な業務にとどまらないハイエンドなセキュリティビジネスの地場産業化を通じて、より高次のエコシステムの形成が期待される。

○ モデル事業の成果を他地域に展開することで、それぞれの地域で自律的なセキュリティ人材の創出を図る。

＜沖縄における取組のイメージ＞



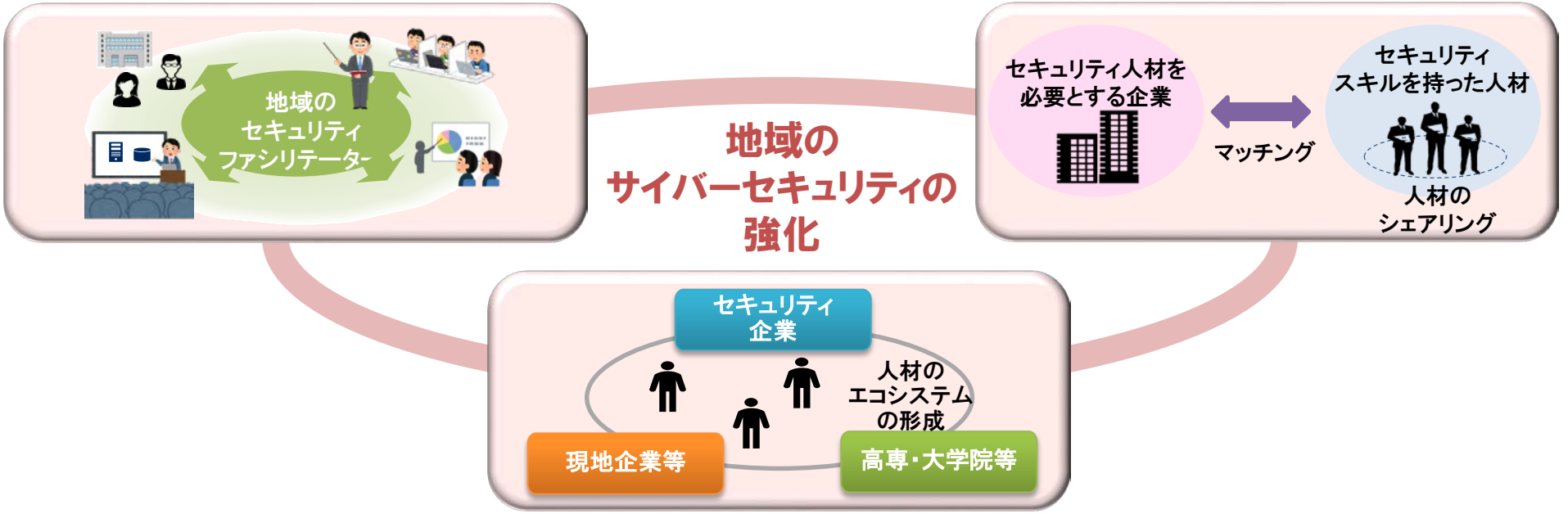
セキュリティ基礎人材の育成
→基礎的なセキュリティスキルを学んだ人材に雇用の受け皿を構築

沖縄電力やりゅうせきビジネスサービス等の現地企業とNRIセキュアテクノロジーズやトレンドマイクロ等のセキュリティベンダが協力して構築。

4 むすび

○ Society5.0がもたらすメリットを地域が享受するためには、その基盤として地域におけるセキュリティ活動の活性化が不可欠である。

○ 具体的には、地域におけるセキュリティファシリテーターの育成の取組を通じて、地域全体で面的にサイバーセキュリティの関心を高めることが求められる。その上で、サイバーセキュリティに関心を持った個別の中小企業等が専門家や専門組織を地域でシェアしながら、効率的に活用する仕組みの構築が求められる。また、こうした取組が地域に根付き自走するためには、それぞれの地域で活動を支える人材が育つエコシステムの形成が求められる。



○ セキュリティ人材の育成は一朝一夕にはならず地道な取組が必要である。セキュリティ対策においては、自助、共助、公助のバランスが求められる中で、地域における共助が全体を繋ぐ要となり得る。本分科会における検討結果に基づき、「地域」を切り口としたサイバーセキュリティ人材の育成に関するモデル事業を実施し、そのモデルを全国に横展開することで、Society5.0時代の持続可能な地域社会の実現に貢献することが期待される。