東北経済産業局　御中

令和２年度中小企業サイバーセキュリティ対策促進事業

(東北地域セキュリティコミュニティ形成促進支援事業)

報告書

令和３年 ３月 30 日

株式会社ブレインワークス

目 次

1　始めに

コロナ禍である現在、中小企業においてもテレワーク等のニューノーマルな働き方を狙った攻撃の脅威が増大しており、ランサムウェアによる被害や標的型攻撃による機密情報の窃取、サプライチェーンの弱点を悪用した攻撃等にも引き続き注意を払う必要がある。従って、情報セキュリティ対策やサイバーセキュリティ対策の強化は益々重要な経営課題になってきていると言える。

これに向けた対策として本事業では、地域におけるセキュリティコミュニティを形成し、中小企業のセキュリティ対策に関する意識向上・人材育成、関係者間の情報共有（「共助の関係の形成」）の実現を目指すために、先ずは、その在り方を取りまとめることとする。

そのために、以下に示す通り、キーパーソン、地域団体（自治体、教育機関、中小企業、ベンダー、関係団体等）、情報処理安全確保支援士（登録情報セキュリティスペシャリスト（以下、「登録セキスペ」という。））の事態調査、セキュリティ対策の強化に向けたモデル事業（企業に対する個別指導）やスキルアップイベント等を実施し、検証を行った。

2　地域のキーパーソン等発掘調査

2.1　ヒアリング調査の実施概要

東北地域におけるセキュリティノウハウ・スキルを持ったキーパーソンなど、継続的に東北地域内で活動できる地域セキュリティコミュニティの活動人材の発掘や管内セキュリティベンダーを把握するため、東北各県でセキュリティに関わっている大学等の先生、企業従業者、地域コミュニティのリーダー等の地域のキーパーソンになり得る方々へヒアリング調査を行い、キーパーソン等発掘調査を実施した。ヒアリング調査対象者の選定条件、及びヒアリング調査方法は以下の通りである。

（1）ヒアリング調査対象者の選定条件

継続的に東北地域内で主に人材育成や情報提供等の対外的活動を行っている大学等の先生、企業従業者等を選定した。なお、企業については、セキュリティ対策強化につながるソフトウェアやサービスを提供しているという条件も加えている。ヒアリング調査対象者は【別紙 1】「地域のキーパーソン等発掘調査 ヒアリング先リスト」に示している。

（2）ヒアリング調査方法

Webex-Meetings を利用し、オンラインで 30 名（大学等の先生：14 名、企業従事者：8 名、地域コミュニティのリーダー：6 名、他：1 名）に対してヒアリング調査を実施した。なお、事前にヒアリング調査票を送付し、ヒアリング事項を通知することで、効率的に進める工夫を行った。ヒアリング事項は以下の通りである。

1．所属組織及び所属先におけるご自身の情報
- 1-1　氏名
- 1-2　所属組織
- 1-3　所属部署
- 1-4　役職／職種
- 1-5　所属組織の業務内容／活動内容／研究内容、所属組織におけるご自身の役割
- 1-6　情報セキュリティに関する業務／活動／研究を行って得られる成果
- 1-7　所属組織が実施する業務／活動／研究／の目的（狙い）
- 1-8　情報セキュリティに関するご自身／所属組織の目標
- 1-9　情報セキュリティに関するご自身の経歴

2．中小企業への支援に関する意見等

2-1　中小企業の課題について（予算、人材、経営者の意識等の観点から）
2-2　自社の製品・サービス／活動内容／研究成果の中小企業への有用性
2-3　中小企業の人材育成のあり方
2-4　中小企業に対する意識向上策
2-5　中小企業への支援のあり方（官・学の関わり方、産・学・官での連携方法等）

3．地域コミュニティに対する意識・意見等

3-1　中小企業へのセキュリティ対策に関する意識の向上・人材育成、関係者間の情報共有を目的とする地域コミュニティに対する意識（考え）
3-2　地域コミュニティの中核を担う人物像
3-3　地域コミュニティの活性化方法
3-4　地域コミュニティに対する期待（あるべき姿）
3-5　地域コミュニティにおけるご自身の役割（貢献の仕方）

4．その他

4-1　地域キーパーソンとして、他に候補になりそうな方をご存知でしたら、ご紹介願います

2.2　ヒアリング調査結果

（1）中小企業支援についての分析と考察

総じて中小企業は、予算が十分に確保できておらず、セキュリティスキルの高い人材がいない、また、経営者の意識も不十分であるという認識が多くを占めた。大学等の先生や企業従事者からは、支援策についてはコミュニティ形成の重要性を訴える意見や地域の IT ベンダーが果たす役割も大きい、また、セキュリティ対策や人材育成については強制的な制度等がないと前向きにならないという意見が複数出てきた。他に参考となる意見として以下を提示する。

【大学等の先生からの意見】

- セキュリティ対策を行うことは顧客・消費者保護のための責務であり、信頼される企業に成長するための投資でもある（コストではない）。この考え方が経営者の意識改革につながり、中小企業に浸透すれば、トップダウンで予算の獲得や人材の確保を行うことにつながると思う。
- セキュリティ対策に取り組むにあたっては、各々が実施するより企業コミュニティを形成し、学ぶ場を作れば低コストかつ高効率に行うことができると考える。このような活動やセキュリティ対策を実施することへの補助があるのが望ましい。また、困った時の相談先としてコミュニティが機能すれば、支援につながると思う。
- 中小企業に求められるセキュリティの意識は、業種・業態によりその程度が異なると思う。外部に流出してはならない重要情報を保有する企業へは事故発生時に必要な被害対応コストを明確に示して意識向上を促す方法もあるのではないかと思う。
- 中小企業への支援のあり方については、官・学が縛ることなく、民間の企業や団体が自由に支援を行う形が良いかと考えている。

【企業従業者からの意見】

- 人材面で求められるのは IT スキルだけではなく、自社の事業内容と情報資産の把握も重要である。
- セミナーによる支援は有効ではあるが、セキュリティの専門家だけではなく、弁護士や社労士等による講演があると、より身近に感じることができ、参加者が増えると考えている。

- 中小企業はサプライチェーンの上流からの圧力がかからないと動かないと思う。また、セキュリティについて相談できる専門家がどこにいるのか分からないため、前向きに対策を行おうとする意識が欠けているのではないかと考えている。

【地域コミュニティのリーダー（イベント運営の代表等）からの意見】

- 自社のリスクを把握し、想定被害が明確になり、必要な対策が可視化できれば、予算の確保ができるのではないか。
- 中小企業で人材を育成することは難しいと思うので、学生を育て、企業に送り込むことが有効だと思う。
- 成長期にある企業の場合はセキュリティに対する意識が高いと感じているが、そうでない企業は予算や人材に関して前向きな姿勢が見られない。

国や自治体の支援のもと、企業を中核とした地域コミュニティが中小企業の人材育成に貢献し、その結果、セキュリティ対策の強化をもたらすことは十分可能である。人材育成の対象としては、やがて中小企業で働く学生を含めることも重要である。課題は、いかにして経営者の意識改革をもたらすかであり、これが実現すると予算確保が進むものとなる。

（２）地域コミュニティに対する意識・意見等

地域コミュニティにおいては継続することと活性化が重要な要素である。それを実現するためには、参加しやすく企業と学生が一体化できる環境を作ることが重要であるという意見が大学等の先生や地域コミュニティのリーダー（イベント運営の代表等）から複数あった（学生が参加できると常に新しいメンバーを取り込むことができる）。また、コミュニティでは広く IT 全般を学ぶ機会を与え、その中でセキュリティを取り上げることも継続と活性化に有効で、効果的に人材育成ができるのではないかと考える。

コミュニティのあるべき姿（理想型）に関して、参考になる意見を以下に提示する。

【大学等の先生からの意見】

- 中小企業支援という観点に立てば、企業にとって有用なセキュリティに関する製品やサービスについての情報交換ができるコミュニティが必要で、それがセキュリティベンダーとユーザー企業の接点になり、両者にとって有益な場になることが理想である。但し、セキュリティベンダーの単なる営業の場とならないことが重要である。
- 多様性が必要で、常に新たな情報やノウハウを提供できる環境が重要である。
- 若者の人材育成をしていくことが大切である。育成した人材が地域に出て行き、啓蒙活動（セミナーなど）を若者視点でできると良いと思う。

【企業従業者からの意見】

- 自身のコミュニティ運営をしていた経験から仕事と結びつかないコミュニティは意識がそれほど高くない人が集まる傾向があり、仕事と直結するコミュニティは意識が高い人が集まる傾向があると感じた。
- コミュニティが高い目標を設定することで、それに同調する意識の高い人が集まる傾向が高くなり、それが高いレベルの活動につながっていくという好循環を生むことになるのではと思う。
- コミュニティに参加するインセンティブがあると参加者が増える傾向があると思うので、それが中小企業に対して明確であることが理想である。

【地域コミュニティのリーダー（イベント運営の代表等）からの意見】

- あるべき姿は、ファンになってくれる人（仲間）でネットワークを形成し、困ったときに助け合うなどの共助の環境ができることである。

- コミュニティ活動においては、ルールで活動を制限しない方が良く、初めての人でも参加し易い環境を作る必要があると思う。
- 誰が来てもいい、いつ来てもいい、また、いつでも離れることができるオープンマインドな状態であることを期待したい。

中小企業にとって地域コミュニティは、助けてもらうことができる場、知識や情報を得る場、参加することによるメリットが得られる場であることが重要である。

そして、コミュニティの中核を担う地域のキーパーソンには、セキュリティに関する技術やノウハウを持っている企業の方が適任であるという意見が多い一方、大学等の先生からは利益相反という観点で注意が必要という意見があった。その他、地域のキーパーソンに求められる資質や条件として、ビジネス環境全体を見渡せる力とコミュニティポリシーを浸透させる力（大学等の先生から）、自分の意見を強要しない、情報共有を頻繁に行う、他メンバーの意見をよく聞く、自分から進んでコミュニティ運営を行う、自分の利益だけを求めてメンバーを利用しない（企業従事者から）、ファンを作る力（地域コミュニティのリーダー（イベント運営の代表等）から）などの提示があった。つまり、技術志向の強い人というよりは、様々なヒューマンスキルを持ち合わせ、地域全体の利益を考えることのできる人が地域のキーパーソンの人物像になるということである。

なお、個々のヒアリング調査結果は【別紙 2】「地域のキーパーソン等発掘調査ヒアリング調査報告書」に示す通りである。

3　中小企業に対するセキュリティに関する意識調査

3.1　アンケート調査の実施概要

（1）　調査対象とした中小企業の選定方法

東北 6 県の中小企業 2000 社へアンケート調査を実施するにあたり、各県各業種の企業選定については以下のように行った。

山形県の Web サイトに掲載されていた「山形県の事業所【平成 28 年経済センサス-活動調査結果（確報）】」の「表 7 東北各県における産業大分類別事業所数」から東北 6 県の業種別（16 業種）事業所数及び業種別事業所構成比を把握することができ、これを基に、鉱業は製造業へ統合し、生活関連サービス業、複合サービス事業、サービス業をあわせてその他のサービス業として県別に 14 業種別の事業所数割合を算出した。その結果、東北 6 県全体を約 2000 社としたときの各県及び各業種の事業所数を求めることができたことから、東北 6 県の該当業種の中小企業を当該事業所数割合で無作為に抽出し、2000 社（実際には 2001 社）へアンケートを実施することとした。

（2）　調査方法

上記で抽出した中小企業に対して、「サイバーセキュリティアンケート調査票」を同封し、郵送にてアンケート調査依頼を実施した。

アンケート調査結果の回収は、記入した「サイバーセキュリティアンケート調査票」を郵送、Fax、メール返信にて行うと共に、アンケート調査回答用 Web サイトを制作し、Web での回答も受け付けることにした。調査事項は以下の通りである。

1．企業属性について

1-1　貴社の従業者（派遣、アルバイト・パートを含む）をお尋ねします。該当するものを選択してください。

1-2　貴社の資本金をお尋ねします。該当するものを選択してください。

1-3　貴社の業種をお尋ねします。該当するものを選択してください。

2．デジタル化の状況

2-1　デジタル化の進捗状況はいかがですか？

2-2　取引先との受発注において、主たる手段は何ですか？

2-3　この 1 年間で情報システムにかけた費用はどのくらいですか？

2-4　テレワークのシステムを導入していますか？

2-5　（テレワークのシステムを導入している場合）全社員（正社員）の何割程度が実施していますか？）

2-5　（テレワークのシステムを導入している場合）全社員（正社員）の何割程度が実施していますか？

2-6　（上記で、実施している場合）今後とも継続実施する予定ですか？

2-7　既存の IT システムの状況（老朽化・複雑化・ブラックボックス化）について把握していますか？

2-8　デジタル化の進展やデジタルビジネスへの対応に向けた戦略の策定について

2-9　デジタル化の進展やデジタルビジネスへの対応に向けた組織体制の整備について

2-10　サイバー攻撃や情報漏洩等のセキュリティリスクへの危機意識はありますか？

2-11　従業者に対してサイバーセキュリティに関する注意喚起や指示・指導を行うのはどなたですか？

2-12　セキュリティリスク対策としての予算の確保状況はいかがですか？

3．デジタル化を推進する人材の育成と確保及び組織的な対応

3-1　社内のデジタル化を進めるにあたって、推進する人材についての課題はありますか？デジタル化の進捗状況はいかがですか？

3-2　社内のデジタル化を進めるにあたって、推進する 3-2　社内のデジタル化を進めるにあたって、推進する人材育成についての課題はありますか？

3-3　社内のデジタル化を推進する人材の確保と育成について、今後どのように取り組みたいと考えていますか？

3-4　社内でデジタル化に関する業務をされている方はどなたですか？

4．サイバーセキュリティに関する人材の育成と確保及び組織的な対応

4-1　自社のセキュリティポリシー(情報セキュリティを保つための全体的な指針や方針を定めたルール)を策定していますか？

4-2　サイバーセキュリティに取り組むにあたって、セキュリティ対策を推進する人材について課題はありますか？

4-3　サイバーセキュリティに取り組むにあたって、セキュリティ対策を推進する人材の育成について課題はありますか？

4-4　セキュリティ対策を推進する人材の確保と育成について、今後どのように取り組みたいと考えていますか？

4-5　社内でセキュリティに関する業務をされている方はどなたですか？

4-6　社内のサイバーセキュリティ対策に関する検討などを行うセキュリティ委員会は設置されていますか？

4-7　中小企業自らが情報セキュリティ対策に取り組むことを自己宣言する制度である「SECURITY ACTION」（IPA:独立行政法人情報処理推進機構）の取組み状況はいかがですか？

5．脆弱性情報の適切な把握

5-1 Web サイト等による自社に関係する脅威*1 情報や脆弱性*2 情報の収集状況はいかがですか？

5-2 自社に関係する脅威*1 情報や脆弱性*2 情報を収集する方はどのようになっていますか？

6．インシデント（セキュリティ事故）発生時の備え

6-1 インシデントが発生した場合に備え、緊急時の連絡・報告体制はどのようになっていますか？

6-2 インシデントが発生した場合、被害を最小限に抑えるための緊急時対応はどなたが中心になって行いますか？

7．サプライチェーン全体のリスク認識

7-1 委託先や下請け等の外部の組織に重要な情報を提供する場合、管理責任についてどのように考えていますか？

7-2 委託先や下請け等の外部組織と情報をやり取りする際に、情報の取り扱いに関する注意事項はどのように共有していますか？

8．サプライチェーン全体のリスク認識

8-1 情報セキュリティ対策について分からないこと、困っていること、相談してみたいことがあれば、自由に記入してください。

3.2　アンケート調査結果

（1）　調査結果についての分析と考察

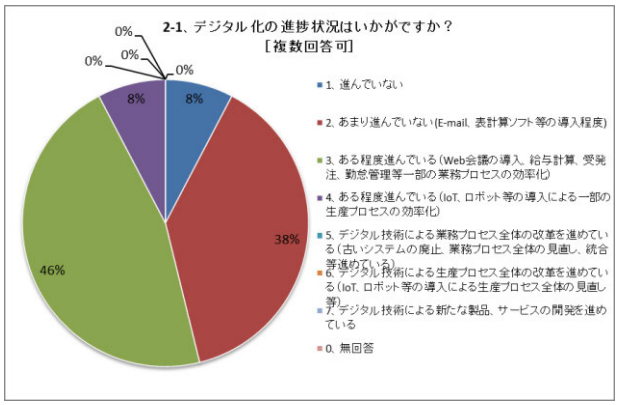
東北 6 県の中小企業 2001 社へアンケート調査票を送付し、569 社（設問 1 項目以上の回答あり）から回収することができた（回収率 28%）。このアンケート調査の回答を「業種別」、「資本金 1 億超と資本金 1 億以下」、「県別」に集計した結果について分析及び考察を行った。その内容を以下に提示する。

① 業種別集計結果の分析と考察

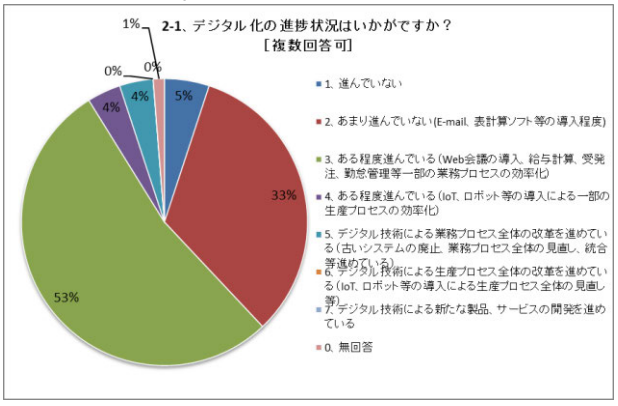
デジタル化への取り組みについては進捗状況、戦略策定及び組織体制の整備に注目すると、農林水産業、建設業、電気・ガス・水道・廃棄物処理業が遅れている（【グラフ 1】～【グラフ 3】、【グラフ 6】～【グラフ 8】、【グラフ 11】～【グラフ 13】参照）。しかし、社内のデジタル化を進めるにあたって「推進する人材に課題はない」、また「推進する人材育成に課題はない」と回答している業種で、農林水産業（前者：25%、後者：42%）と建設業（前者：21%、後者：24%）は、その割合がいずれも 20%以上であり、潜在している課題への気づきがない可能性がある（【グラフ 16】～【グラフ 18】、【グラフ 21】～【グラフ 23】参照）。その一方、金融・保険業、情報通信業は取り組みが他業種に比べ、進んでいる。（【グラフ 4】～【グラフ 5】、【グラフ 9】～【グラフ 10】、【グラフ 14】～【グラフ 15】、及び【グラフ 19】～【グラフ 20】、【グラフ 24】～【グラフ 25】参照）

デジタル化の進捗状況

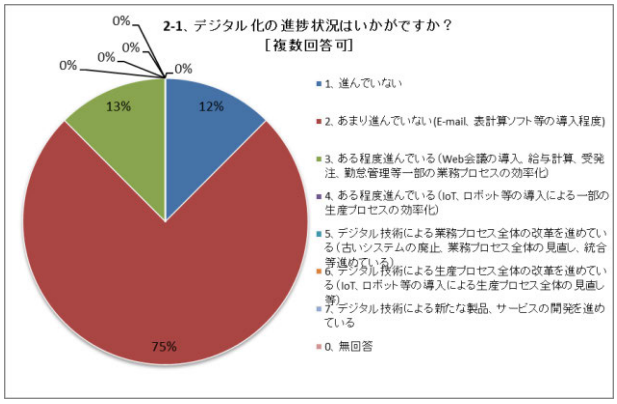
【グラフ 1】農林水産業



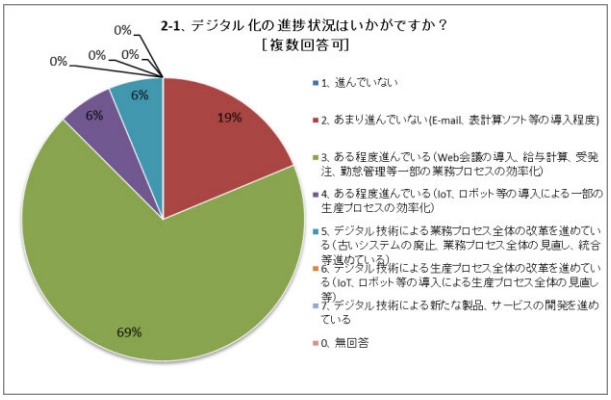
【グラフ 2】建設業



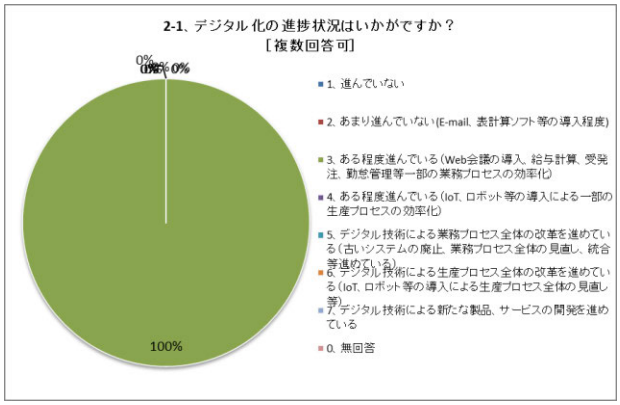
【グラフ 3】電気・ガス・水道・廃棄物処理業



【グラフ 4】金融・保険業

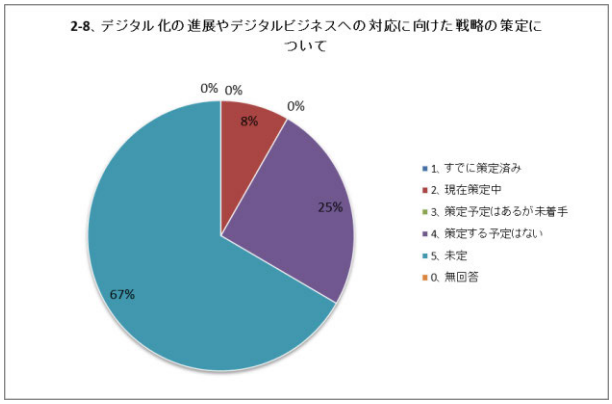


【グラフ 5】情報通信業

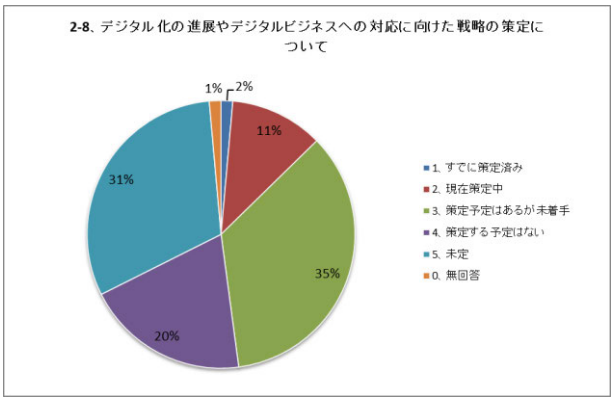


デジタル化の進展やデジタルビジネスへの対応に向けた戦略の策定

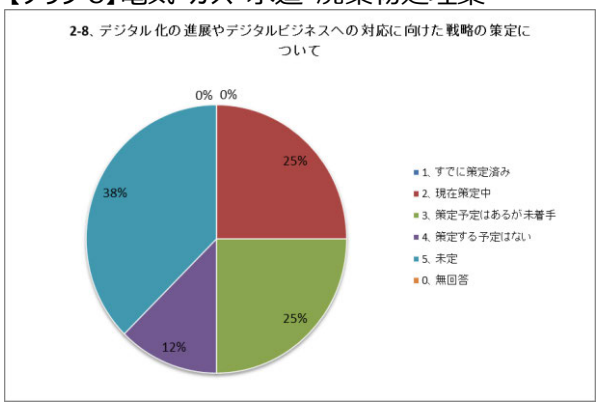
【グラフ 6】農林水産業



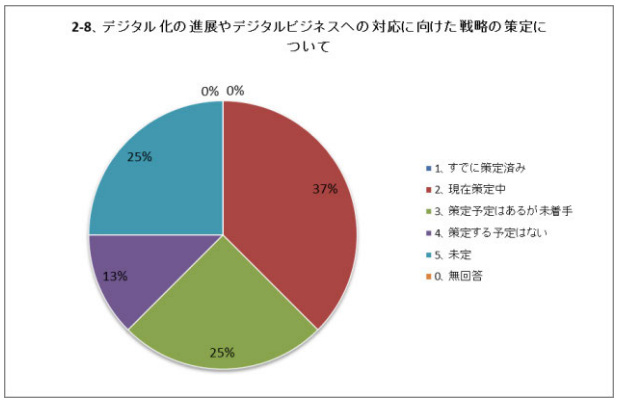
【グラフ 7】建設業



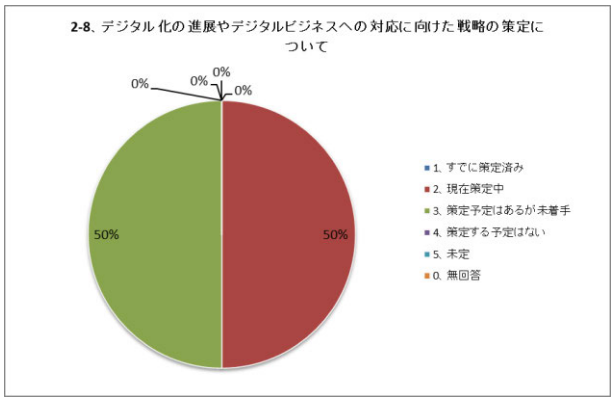
【グラフ 8】電気・ガス・水道・廃棄物処理業



【グラフ 9】金融・保険業

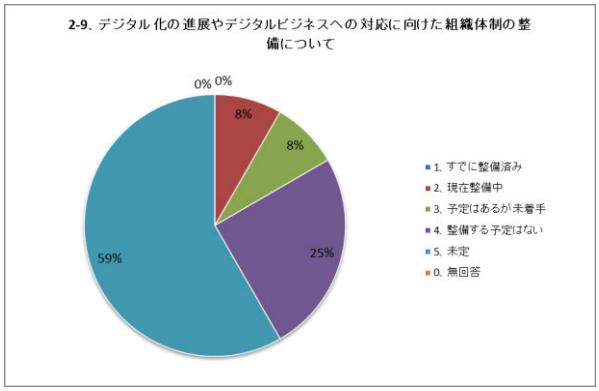


【グラフ 10】情報通信業

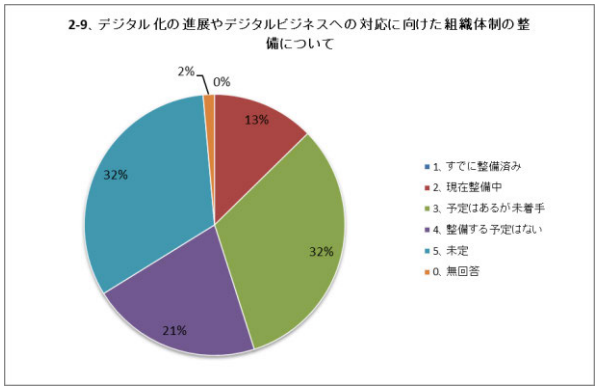


デジタル化の進展やデジタルビジネスへの対応に向けた組織体制の整備

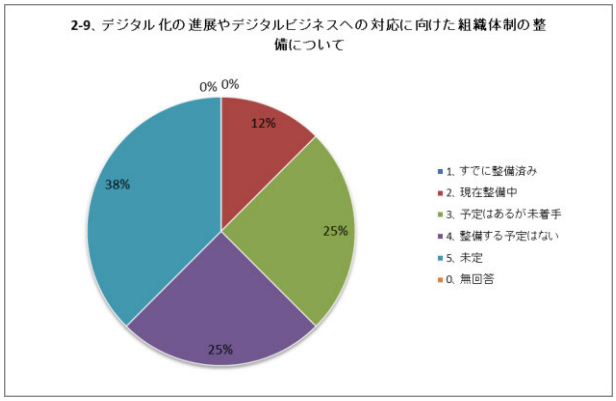
【グラフ 11】農林水産業



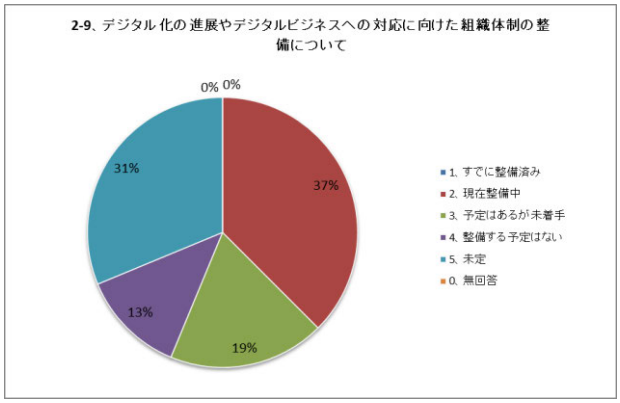
【グラフ 12】建設業



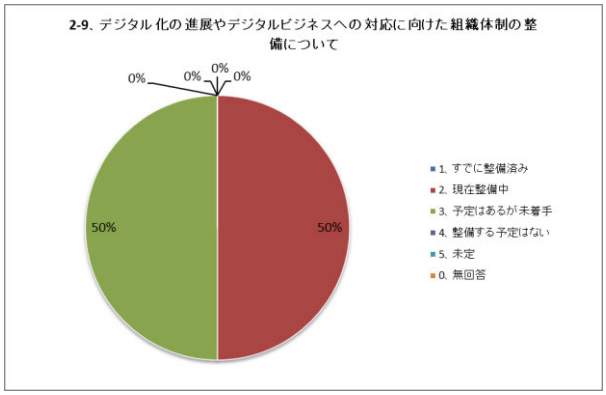
【グラフ 13】電気・ガス・水道・廃棄物処理



【グラフ 14】金融・保険業

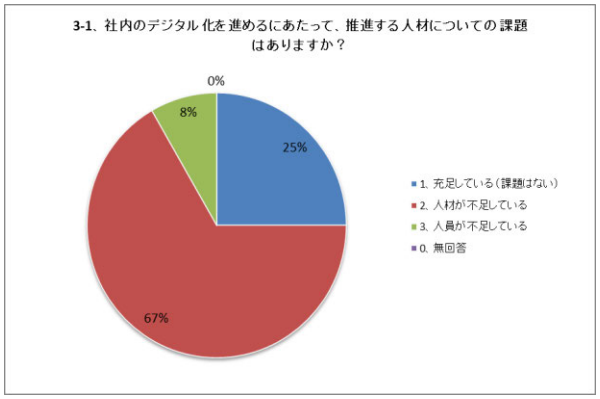


【グラフ 15】情報通信業

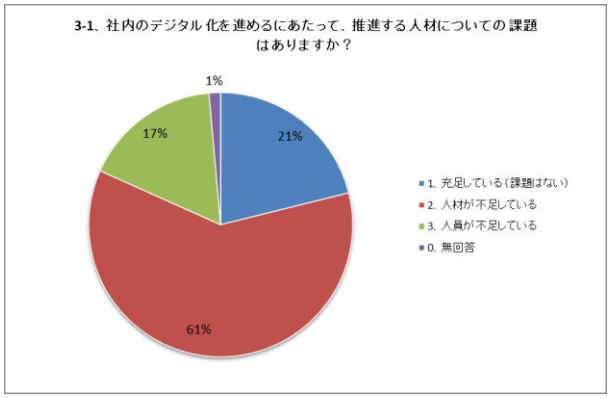


社内のデジタル化を進めるにあたって、推進する人材についての課題

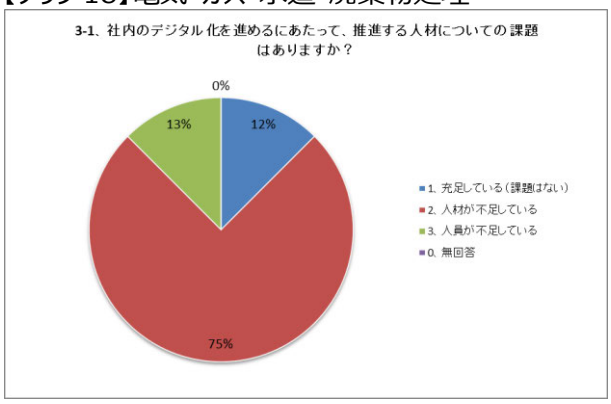
【グラフ 16】農林水産業



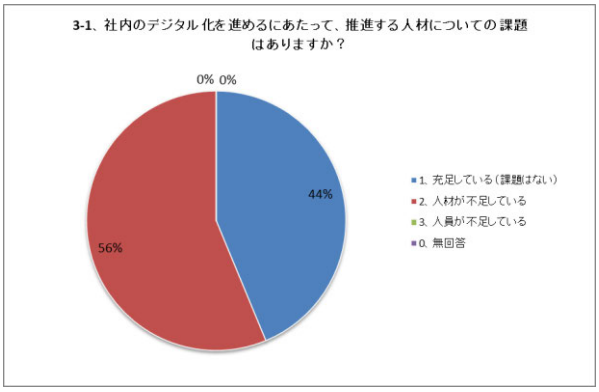
【グラフ 17】建設業



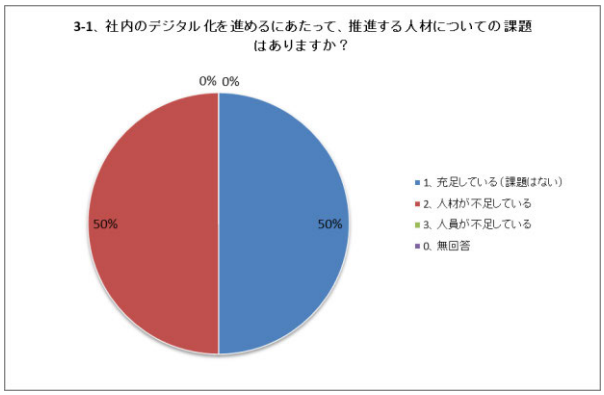
【グラフ 18】電気・ガス・水道・廃棄物処理



【グラフ 19】金融・保険業

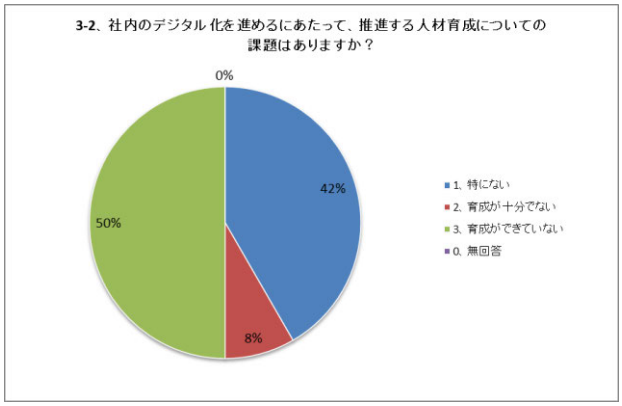


【グラフ 20】情報通信業

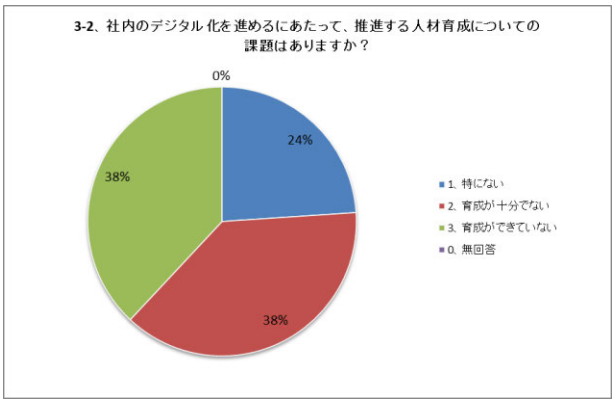


社内のデジタル化を進めるにあたって、推進する人材育成についての課題

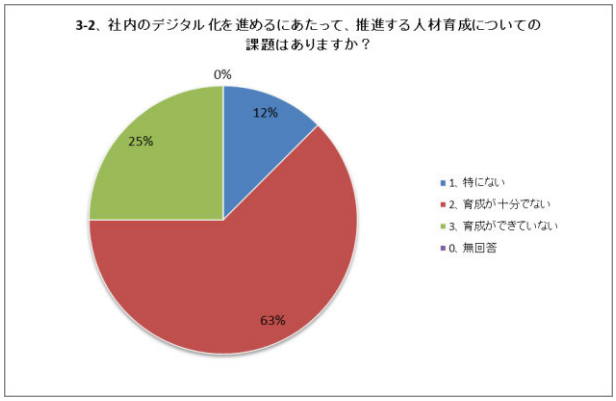
【グラフ 21】農林水産業



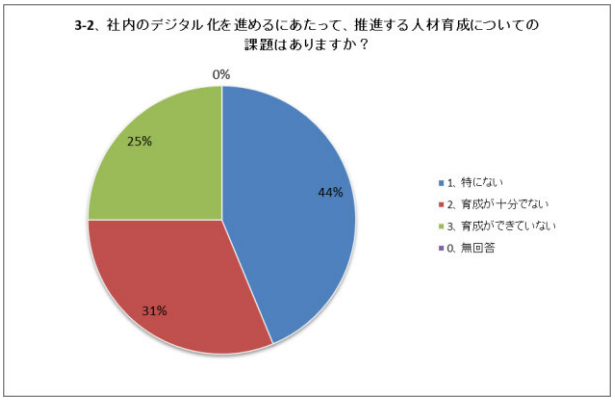
【グラフ 22】建設業



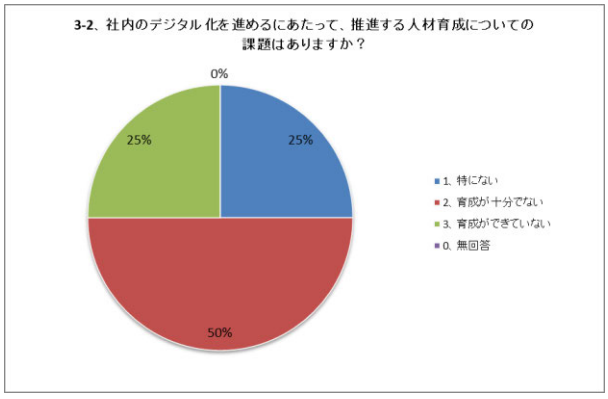
【グラフ 23】電気・ガス・水道・廃棄物処理



【グラフ 24】金融・保険業



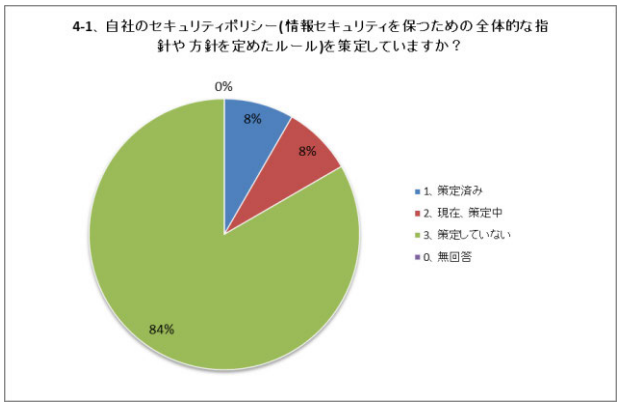
【グラフ 25】情報通信業



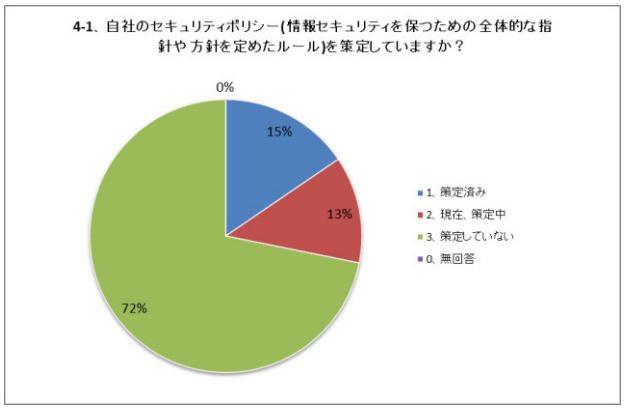
情報セキュリティ対策に関する取り組みに目を向けると、情報セキュリティを推進するにあたり最も重要なセキュリティポリシーの策定が全体的に遅れている。特に、未策定率の高い業種が農林水産業（84%）、建設業（72%）、宿泊・飲食サービス業（71%）である（【グラフ 26】～【グラフ 28】参照）。しかし、サイバーセキュリティに取り組むにあたって「セキュリティ対策を推進する人材について課題はない」、また「セキュリティ対策を推進する人材の育成について課題はない」と回答している業種で、農林水産業（後者：25%）と建設業（前者：22%、後者：25%）は、その割合がいずれも 20%以上であり、潜在している課題への気づきがない可能性がある（【グラフ 31】～【グラフ 33】、【グラフ 36】～【グラフ 38】参照）。その一方、金融・保険業、情報通信業では情報セキュリティに対する取り組みが他業種に比べ、進んでいる（【グラフ 29】～【グラフ 30】、【グラフ 34】～【グラフ 35】、及び【グラフ 39】～【グラフ 40】参照）。

自社のセキュリティポリシー(情報セキュリティを保つための全体的な指針や方針を定めたルール)の策定

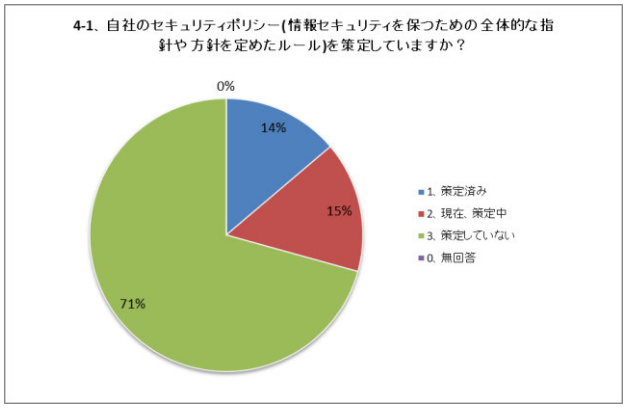
【グラフ 26】農林水産業



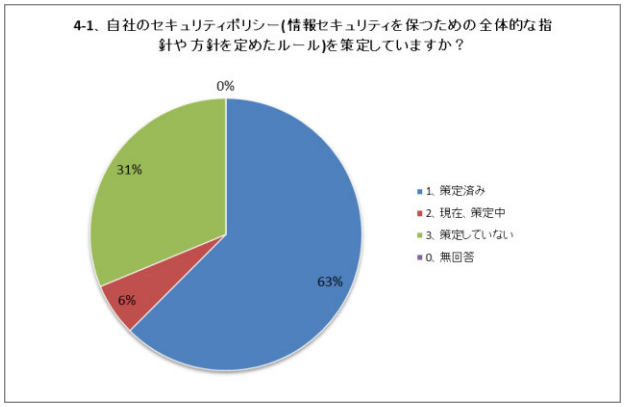
【グラフ 27】建設業



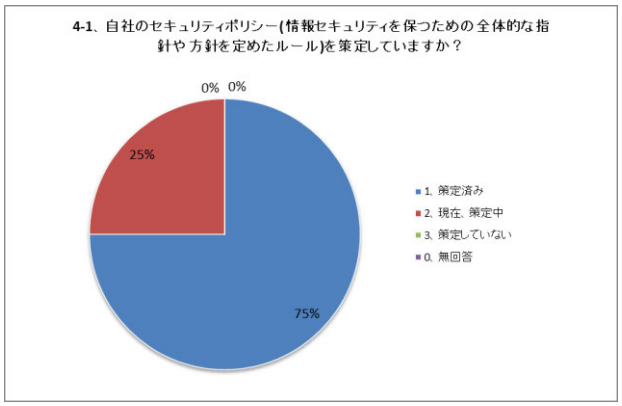
【グラフ 28】宿泊・飲食サービス業



【グラフ 29】金融・保険業

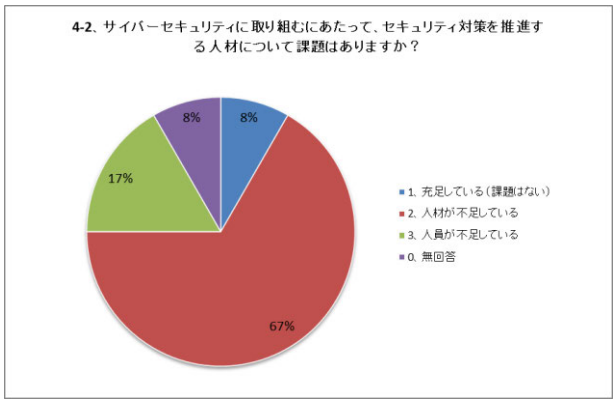


【グラフ 30】情報通信業

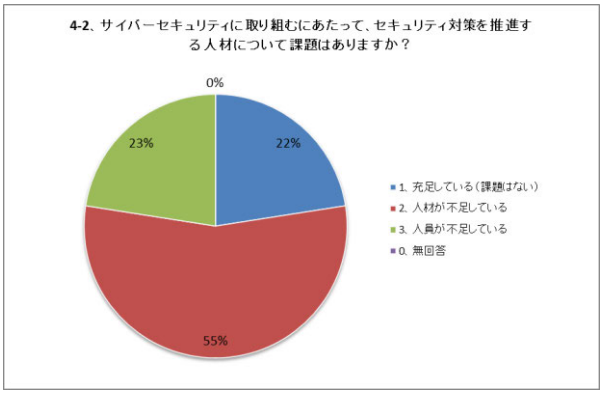


サイバーセキュリティに取り組むにあたって、セキュリティ対策を推進する人材についての課題

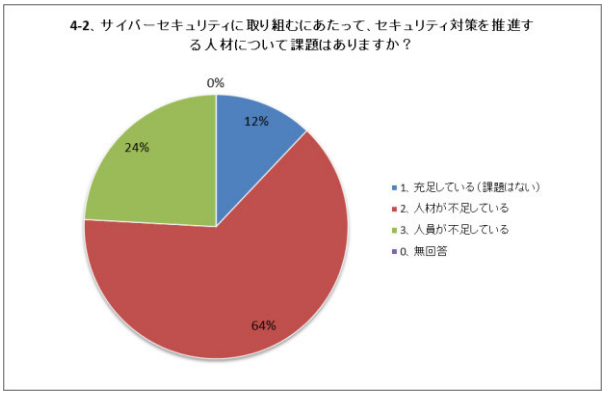
【グラフ 31】農林水産業



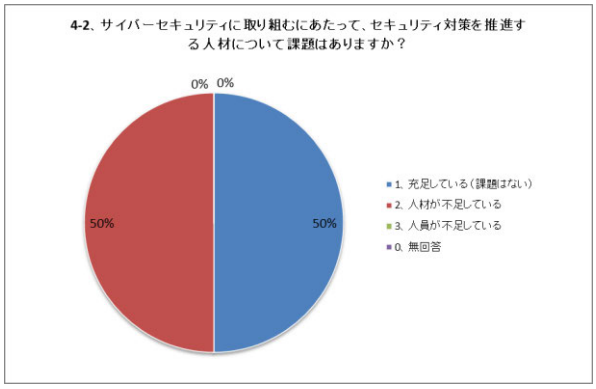
【グラフ 32】建設業



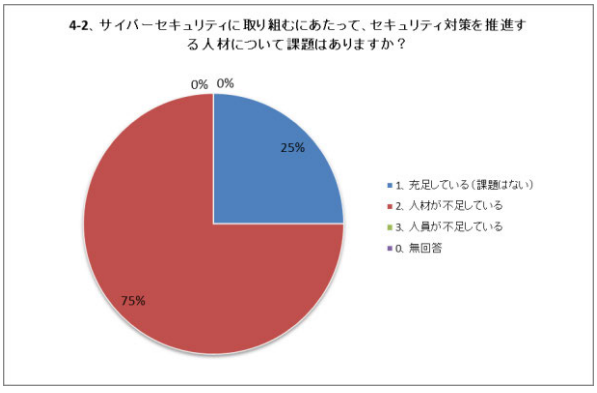
【グラフ 33】宿泊・飲食サービス業



【グラフ 34】金融・保険業

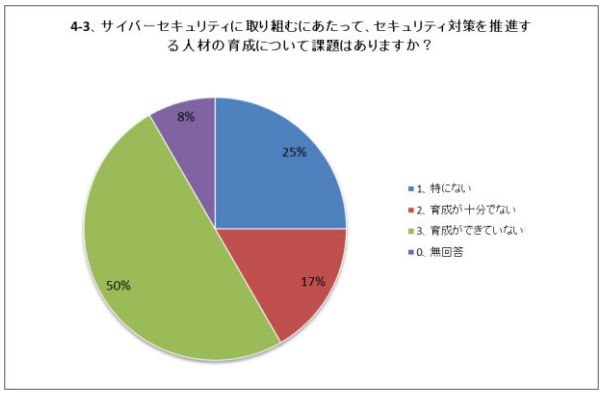


【グラフ 35】情報通信業

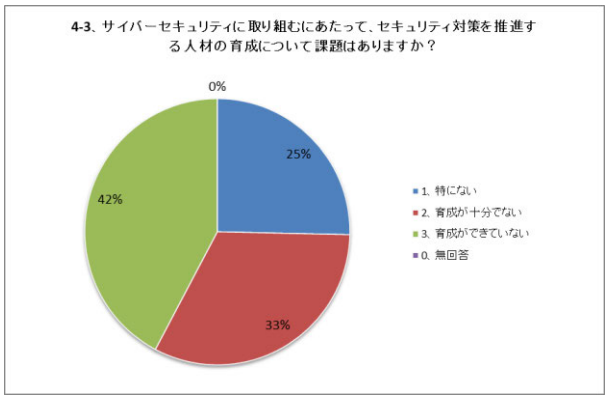


サイバーセキュリティに取り組むにあたって、セキュリティ対策を推進する人材の育成についての課題

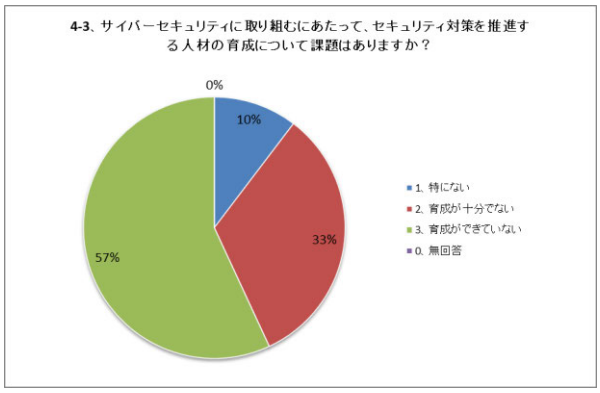
【グラフ 36】農林水産業



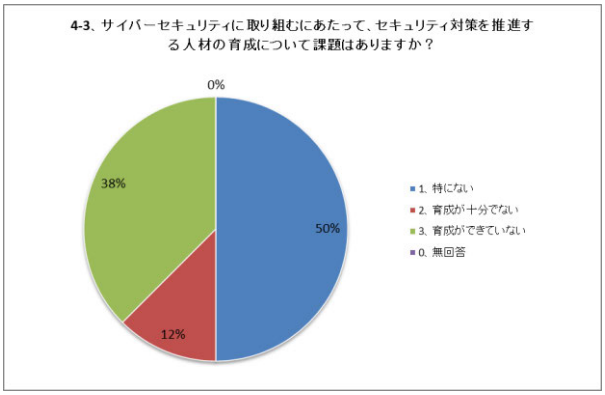
【グラフ 37】建設業



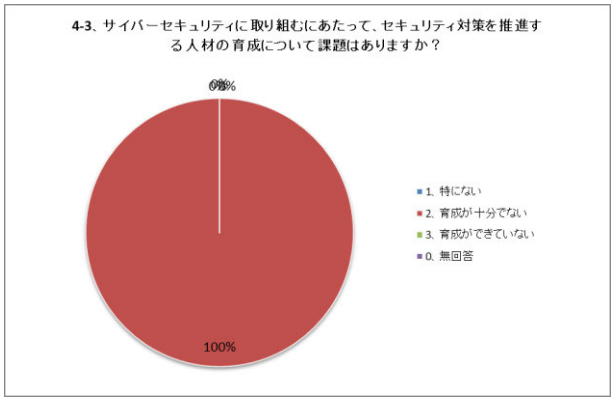
【グラフ 38】宿泊・飲食サービス業



【グラフ 39】金融・保険業



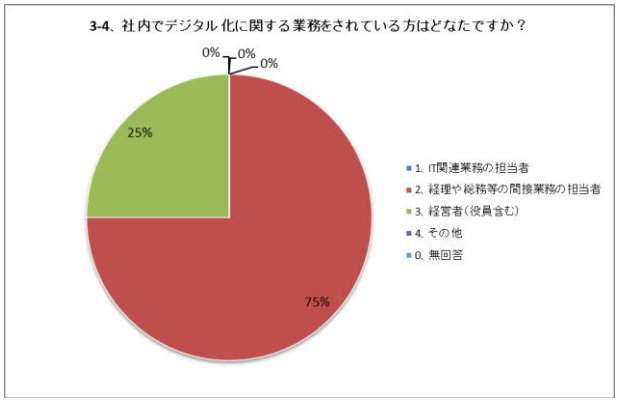
【グラフ 40】情報通信業



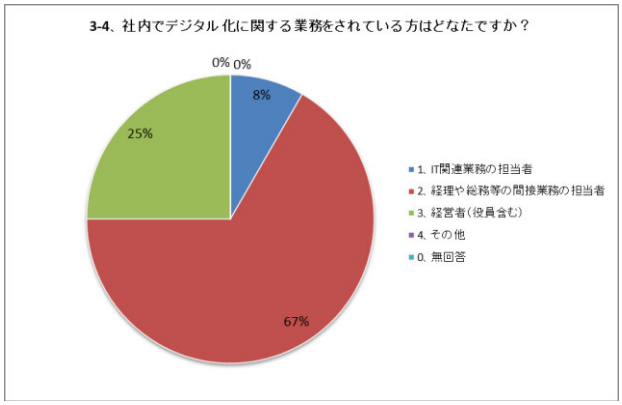
また、社内でデジタル化に関する業務をされている方と社内でセキュリティに関する業務をされている方は一致する傾向があり、多くの業種では双方とも経理や総務等の間接業務の担当者という回答が多かった（一例として【グラフ 41】～【グラフ 42】、【グラフ 45】～【グラフ 46】参照）。一方、製造業、専門・科学技術、業務支援サービス業、卸売・小売業、保健衛生・社会事業（特に最初の 2 業種）においては、双方とも経営者という回答が多く見受けられた（【グラフ 43】～【グラフ 44】、【グラフ 47】～【グラフ 48】参照）。

社内でデジタル化に関する業務をされている方

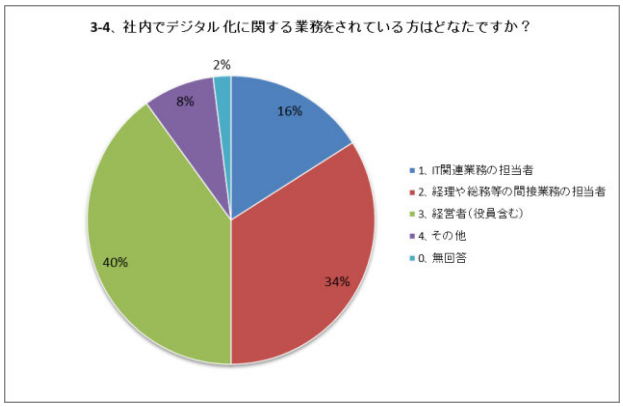
【グラフ 41】電気・ガス・水道・廃棄物処理業



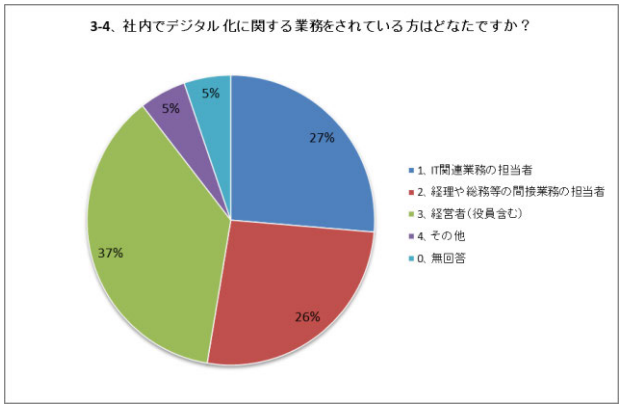
【グラフ 42】運輸・郵便業



【グラフ 43】製造業

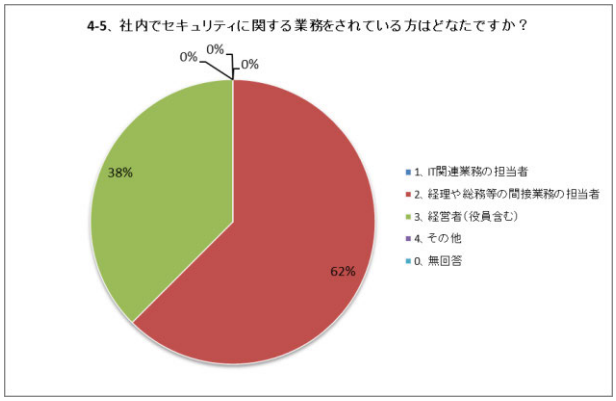


【グラフ 44】専門・科学技術、業務支援サービス業

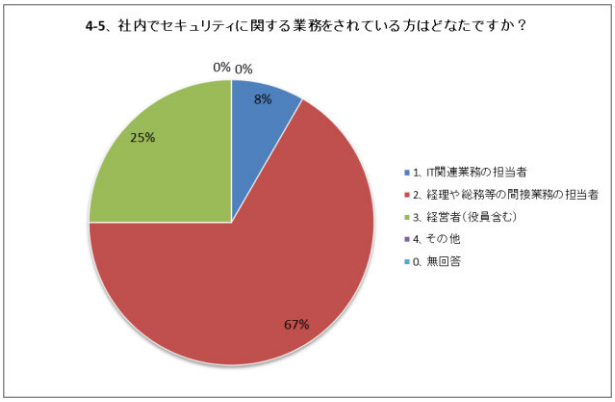


社内でセキュリティに関する業務をされている方

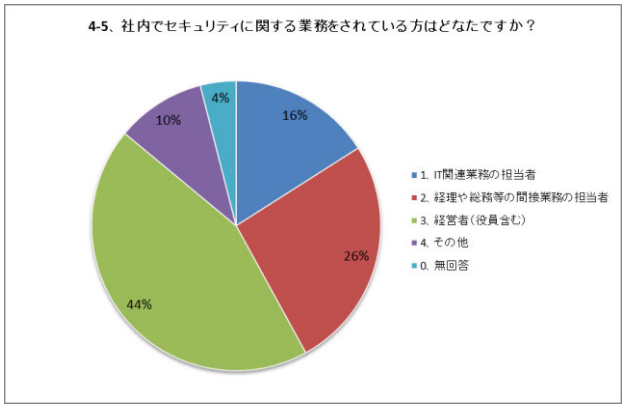
【グラフ 45】電気・ガス・水道・廃棄物処理業



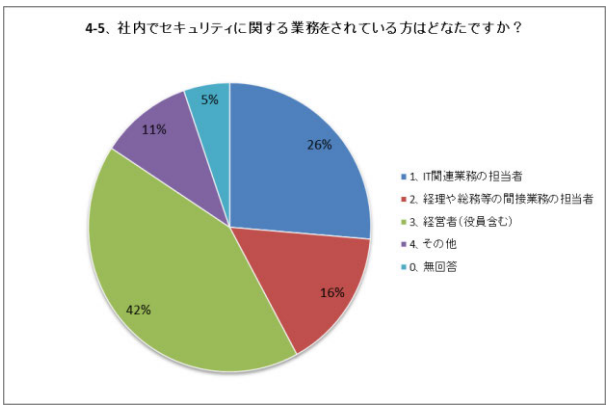
【グラフ 46】運輸・郵便業



【グラフ 47】製造業



【グラフ 48】専門・科学技術、業務支援サービス業



② 資本金 1 億超企業と資本金 1 億以下企業の集計結果の分析と考察

資本金 1 億超企業の主な業種は農林水産業と金融保険業で、資本金 1 億以下企業の主な業種は卸売小売業、建設業である。また、サンプル数は、資本 1 億円超 １６社、1 億円以下 ５４３社となっている。

両者で異なる結果が現れた調査事項は【表 1】の通りである。

【表 1】

調査事項	1 億超	1 億以下
デジタル化の進展やデジタルビジネスへの対応に向けた戦略の策定が策定済み、または策定中	12%	25%
デジタル化の進展やデジタルビジネスへの対応に向けた組織体制が整備済み、または整備中	6%	20%
従業者に対してサイバーセキュリティに関する注意喚起や指示・指導を行う方	管理職 44%	経営者 38%
社内でデジタル化に関する業務をされている方	経理・総務 81%	経営者 35%
自社のセキュリティポリシーを策定済み、または策定中	19%	39%
セキュリティ対策を推進する人材の育成が不十分、またはできていない	88%	76%
社内でセキュリティに関する業務をされている方	経理・総務 81%	経営者 37%
インシデントが発生した場合に備え、緊急時の連絡・報告体制がある	25%	38%
インシデントが発生した場合、被害を最小限に抑えるための緊急時対応を行う方	管理職 44%	経営者 43%
委託先や下請け等の外部組織と情報をやり取りする際に、情報の取り扱いに関する注意事項を共有する方法	契約書 56%、口頭 6%	契約書 41%、口頭 17%

本結果からは、上表より 1 億以下の企業の方が、デジタル化の進展やデジタルビジネスへの対応に向けた取り組み、及びセキュリティ対策が一部において進んでいることがうかがえる。また、1 億以下の企業は、デジタル化やセキュリティ対策において、経営者の役割と責任が大きいという結果が現れている。ただし、1 億超企業のサンプル数が少ないことを考慮する必要はあるであろう。

一方、以下の調査事項では、両者で同じような結果が現れた。

- 情報システム投資額が 500 万円未満（90%以上）
- セキュリティリスク対策としての予算をほとんど、または全く確保していない（約 40%）
- 社内のデジタル化を進めるにあたって、推進する人材育成が不十分、またはできていない（約 80%）
- Web サイト等による自社に関係する脅威情報や脆弱性情報の収集をしていない（約 60%）
- 自社に関係する脅威情報や脆弱性情報を収集する方が決まっている（12～14%）

1 億超企業の企業であっても情報システム投資額やセキュリティリスク対策としての予算、人材育成が十分ではなく、経営者の意識改革を促す対策が必要である。

③ 県別集計結果の分析と考察

県別の集計結果については、その差が顕著ではなかったが、岩手県は他県と比べデジタル化及び情報セキュリティ対策について遅れをとっている傾向が見受けられた（【表 2】）。

岩手県では社内でデジタル化及びセキュリティに関する業務をされているのが IT 関連業務の担当者でないケースが多いことから IT 関連の部署や担当者が少ないことが、遅れをとっている要因と考えることもできる。

【表 2】

調査事項	岩手県	他県
デジタル化の状況が進んでいない、又はあまり進んでいない	45%	41%以下
この 1 年間で情報システムにかけた費用が 100 万円未満	75%	55～67%
デジタル化の進展やデジタルビジネスへの対応に向けた戦略の策定は、すでに策定済み、又は策定中	19%	20～27%
＜補足＞戦略の策定予定はない、又は未定	63%	36～50%
デジタル化の進展やデジタルビジネスへの対応に向けた組織体制の整備は、すでに策定済み、又は策定中	13%	14～26%
サイバー攻撃や情報漏洩等のセキュリティリスクへの危機意識については、十分意識している	17%	25～32%
セキュリティリスク対策としての予算の確保状況で、ほとんど確保していない、又は全く確保していない	47%	30～42%
社内でデジタル化に関する業務をされている方は、IT 関連業務の担当者である	8%	15～20%
社内でセキュリティに関する業務をされている方は、IT 関連業務の担当者である	10%	14～21%
インシデントが発生した場合に備え、緊急時の連絡・報告体制については、委託先等の社外も含めた体制がある	12%	13～24%
委託先や下請け等の外部組織と情報をやり取りする際に、情報の取り扱いに関する注意事項は、契約書等の書面で共有している	40%	41～45%

（２） 今後の支援に必要と考えられる事項等

デジタル化と情報セキュリティ対策で進んでいる業種と遅れている業種は、企業規模によらず、同じであることが把握できた。規模が大きい企業が進んでいるという状況は見られなかったことから、企業規模は考慮せず、特定の業種に対して支援を行うことも検討の余地がある。

また、デジタル化が遅れている企業は、情報セキュリティ対策も進んでいないと予想されるため、両方を促進するための支援も必要と考えられる。重要なのはデジタル化を支援する際、利便性や効率性を追求するだけではなく、情報の機密性・完全性・可用性を高めることの重要性を訴え、その対策についても併せて支援することが必要である。

重点支援事項としては、先ず、デジタル化及び情報セキュリティ対策における人材確保と人材育成である。例えば、人材マッチングの場を作ること、産学連携のもと低費用で人材育成ができるスキームの構築なども支援策の一つになると考えている。

4 登録セキスペのセキュリティに関する活動調査

4.1 アンケート調査の実施概要と結果

（１） 実施方法

独立行政法人情報処理推進機構（IPA）から東北地方の登録セキスペに対し、Web アンケートへの回答依頼を行って頂き、36 名分の回答を得ることができた。

アンケート調査事項は、以下の通りである。

1．所属組織及び所属先におけるご自身の情報

1-1　氏名
1-2　所属組織
1-3　所属部署
1-4　役職／職種
1-5　所属組織の主な業務内容／活動内容
1-6　ご自身の業務内容／活動内容（特に情報セキュリティ関連）
1-7　情報セキュリティに関するご自身の経歴
1-8　所属組織におけるご自身の目標（情報セキュリティ関連）

2．地域中小企業向けの活動内容と地域中小企業の課題

2-1　所属組織の地域中小企業向けの業務（活動）について
2-2　ご自身（個人）の地域中小企業向けの業務（活動）について（希望も含めて）
2-3　地域中小企業の課題について
2-4　課題への対応策とご自身（個人）の関わり方について

3．地域中小企業のセキュリティ対策に関する連携と課題

3-1　所属組織における地域中小企業のセキュリティ対策強化に向けた活動（コミュニティ活動等）について、又は当該活動への連携可能性について
3-2　ご自身（個人）としての地域中小企業のセキュリティ対策強化に向けた活動（コミュニティ活動等）について、又は当該活動への連携可能性について
3-3　地域中小企業のセキュリティ対策強化に向けた活動（コミュニティ活動等）へ連携する際の課題について（所属組織及び個人）
3-4　地域中小企業のセキュリティ対策強化に向けた活動（コミュニティ活動等）へ連携する際の希望について

なお、アンケート調査結果は、【別紙 3】「登録セキスペ_Web アンケート回答結果」に取りまとめた。

（２）　アンケート調査結果から得られる登録セキスペの状況

所属組織内における情報セキュリティ対策の主導、セキュリティ製品の開発導入及び保守、顧客企業・団体等へのセキュリティ関連ソリューションの提案及び構築導入、セキュリティ関連のコンサルティングに従事している方がほとんどで、独立行政法人情報処理推進機構（IPA）による「情報処理安全確保支援士（登録セキスペ）の活動に関する実態調査」の結果と同様にシステム開発、クラウドサービス提供等の IT サービス提供事業者に所属している方が多い傾向が見受けられた。

地域中小企業との関わりについては、パッケージ製品やクラウドサービス（セキュリティ関連製品を含む）の提案及び導入、システム構築、情報セキュリティ体制整備に関する助言指導、情報セキュリティ教育の実施、全く関わっていない、という回答が多くあった。地域中小企業に対しては、リテラシーが低い、セキュリティに対する意識が乏しい、セキュリティに対策に講じる費用が少ないといった印象を持っているようである。

地域中小企業のセキュリティ対策強化に向けた活動（コミュニティ活動等）については、所属組織の業務との関連性が薄く難しいとの回答があった一方で、個人として取り組んでみたいという前向きな回答もあった。

また、当該活動（コミュニティ活動等）と連携する際の課題は、所属組織の業務と無関係、所属組織の業務時間との調整が必要、という回答が多く見受けられ、中には企業支援の経験と実績がないといった懸念もあった。連携する際の希望としては、経営者の意識改革を促す施策や企業へのインセンティブの提供を求める意見、自身のスキルとリソースに見合った支援であること、報酬の確保などの要望があり、これらについては考慮する必要がある。

4.2 ヒアリング調査の実施概要と結果

（1） 実施方法

アンケート調査結果の内容を深掘りすべく、回答して頂いた 36 名の登録セキスペへヒアリング調査（オンライン）の実施依頼を行い、14 名に対して実施することができた。

ヒアリング調査事項は、以下の通りである。

1. 氏名
2. 所属地域（県）
3. 所属組織
4. 所属部署
5. 役職／職種
6. 企業への支援実績（セミナー講師等も含む）
7. 今後の企業への支援について（予定、希望等）
8. 中小企業の重点課題についての考え、その対応策についての考え
9. 中小企業の課題対策におけるご自身（個人）の関わり方
10. 地域中小企業のセキュリティ対策強化に向けた活動（コミュニティ活動等）へ参加、又は連携する可能性について
11. 当事業における中小企業へのヒアリング、セキュリティ対策支援モデル事業（セキュリティコンサルティング）への参加の御協力について

なお、ヒアリング調査結果は、登録セキスペごとに【別紙 4】「登録情報セキュリティスペシャリストへのヒアリング事項」に取りまとめた。

（2） ヒアリング調査結果から得られる登録セキスペの状況

自社以外に対して地域中小企業へ情報セキュリティ関連の活動を行っている登録セキスペの業務内容についてアンケート調査から深掘りしたところ、第三者認証（プライバシーマーク、ISMS）取得に関するコンサルティング、経営コンサルティングの一環としての補足的なコンサルティング、国等の情報セキュリティに関する支援制度で実施したコンサルティング、という状況であった。

地域中小企業のセキュリティ対策強化に向けた活動については、個人的な活動が所属組織から認められている場合（副業可能など）、業務時間に余裕があれば参加又は連携できる可能性があるという前向きな回答をされた方が 8 名いた。ただ、活動のスケジュールについては早い段階から伝えておく必要があり、年度末などの繁忙期は難しいという現状を考慮する必要がある。

登録セキスペが個人として参加又は連携するだけではなく、所属組織の活動と何らかの形で連携することができれば更に前向きな方が増えてくるものと考えている。

5　中小企業のセキュリティに関する活動調査

5.1　ヒアリング調査の実施概要

（1）　調査対象企業の選定条件

「3．中小企業に対するセキュリティに関する意識調査」で実施したアンケート調査により回収できた569 社の回答内容から以下のいずれかの条件を満たす、146 社を抽出し、ヒアリング調査の対象とした。

- サイバー攻撃や情報漏洩等のセキュリティリスクへの危機意識が十分にあると回答した企業
- 情報セキュリティ対策について分からないこと、困っていること、相談してみたいことについての自由記入欄に、「対策方法が分からない」、「何をするべきなのか分からない」、「スキル、時間、予算の問題があり方策に苦慮している」という類いの記載がある企業

（2）　調査方法

ヒアリング調査対象とした 146 社の中で、従業員数が 50 人以下の企業に対し、課題や苦慮していることなどをヒアリング調査の自由記入欄に記載しているところを優先してヒアリングすることとした。

ヒアリングは電話等で行い、48 社から回答を得ることができた。ヒアリング調査事項は、以下の通りである。

1. 企業名
2. 対応者
3. 所属組織
4. 役職／職種
5. 【組織的対策の状況】セキュリティに関する社内ルールを策定しているか。社内管理体制（責任者・担当者等）を整備しているか
6. 【物理的対策の状況】重要書類の施錠保管、鍵管理、ノート PC・その他機器（スマホ、タブレット、携帯、USB メモリ等）の盗難防止対策の状況
7. 【技術的対策の状況】Windows アップデート、セキュリティ対策ソフトの導入・更新、導入ソフトウェアのアップデート、ホームページの脆弱性チェック、重要情報のバックアップといった対策の状況について
8. 【人的対策の状況】従業者への情報セキュリティに関する周知や注意喚起、研修の実施状況について
9. 情報セキュリティに関する重点課題について
10. 重点課題対策で困っていることや分からないことへの対応について
11. 情報セキュリティに関する情報や知識を得る方法、人材育成の方法を把握していますか？把握していない場合、相談する人はいますか？
12. 地域コミュニティや公的組織（団体）の勉強会・セミナー、Web サイトや SNS 等からの情報収集といったあまり費用をかけずに知識やノウハウを得る手段を利用してみたいと思いますか？
13. 当事業では情報セキュリティ対策支援（オンラインでのコンサルティング）を 1 回 1 時間程度で 2 月～3 月上旬にかけて 3 回に渡って無料で行いますが、ご関心はありますか？

なお、ヒアリング調査結果は、県別に【別紙 5】「中小企業へのヒアリング結果一覧（県別）」に取りまとめた。また、宮城県の 3 社については、登録セキスペに同席して頂き、アドバイス等を頂いた。

5.2 ヒアリング調査結果

（1） セキュリティ対策の取り組み状況に関する分析と考察

組織的対策として社内ルールを定めているのは過半数の 28 社であったが、見直しまで行っているのはその内 15 社である。責任者が明確になっている企業は約 8 割の 38 社であった。

物理的対策、技術的対策、人的対策の実施状況の中で注目すべき傾向は、技術的対策を「ほぼ実施している」と回答した企業が 8 割以上に達していることである。Windows アップデート、セキュリティ対策ソフトの導入・更新は浸透している状況がうかがえる。

課題については、「なし」という回答が 6 割程度あった一方、人材不足や意識が低いことを挙げている企業も 3 割近くあった。

地域コミュニティや公的組織（団体）の勉強会・セミナー、Web サイトや SNS 等からの情報収集といったあまり費用をかけずに知識やノウハウを得る手段については、8 割近くの企業が「利用している」又は「利用したい」と回答しており、低費用で参加できる地域コミュニティがあれば、前向きに検討して頂けるものと考える。

（2） 今後の支援に必要と考えられる事項等

先ずは、セキュリティ対策の重要性を訴える施策が必要である。そして、アンケート調査結果から得られた結果と同じく、情報セキュリティ対策における人材確保と人材育成についての支援が重点支援事項になると考えている。「3.中小企業に対するセキュリティに関する意識調査」-「3.2 アンケート調査結果」-「(2)今後の支援に必要と考えられる事項等」に示す通り、デジタル化及び情報セキュリティ対策における人材確保と人材育成を目的とした人材マッチングの場を作ること、また、産学連携のもと低費用で人材育成ができるスキームの構築などを地域コミュニティにて試みることも検討の余地がある。

また、社内ルールを策定し、見直しまで行っている企業が少ない傾向が見受けられるため、セキュリティ対策の第一歩であるルール作りに関しても啓発・啓蒙と支援を行う必要があると考える。
「SECURITY ACTION」制度の案内もその第一歩として有効である。

6 地域関係機関との連携による相談対応

6.1 連携したイベント及び相談対応形態

東北地域における各種機関が開催するセキュリティ関連イベントと連携し、イベント参加者等に対するセキュリティに関する出張相談対応を実施した。その際、IPA のセキュリティ啓発コンテンツである「情報セキュリティ 5 か条」、「 5 分でできる！情報セキュリティ自社診断」、弊社で作成した小冊子を配付できるよう用意した。

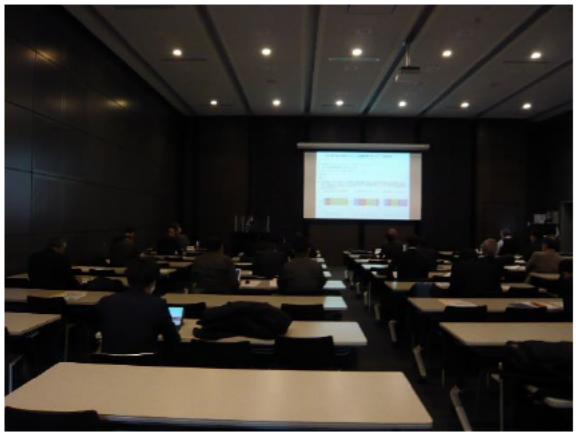
なお、イベントがオンラインでの開催の場合は、相談対応もオンラインで実施している。

連携したイベントの概要と相談対応の実施形態、相談件数は【表 3】の通りである。

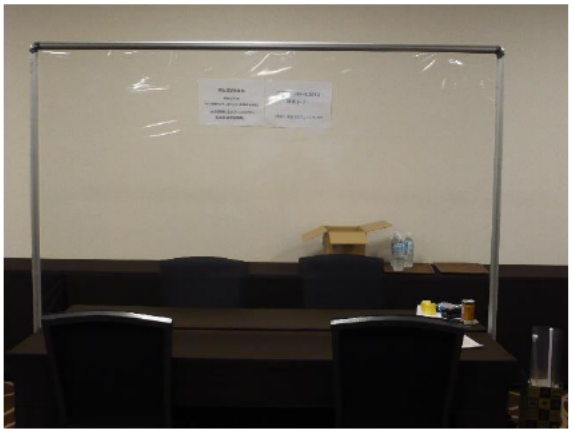
【表 3】

No.	連携イベントの概要	相談対応の実施形態	相談件数
1	【第 2 回いわて組込み技術研究会】 主催者：いわて組込み技術研究会、岩手県、（公財）いわて産業振興センター 日時：令和 2 年 12 月 23 日 13:00～13:30、16:00～16:30 場所：いわて県民情報交流センター（アイーナ） セミナー参加者：30 名	情報セキュリティ相談ブースを設け、相談受付を行った。 情報セキュリティ関連資料も配置。	なし
2	【サイバーセキュリティお助け隊 in 東北 成果報告会】 主催者：株式会社デジタルハーツ、独立行政法人情報処理推進機構（IPA） 日時：令和 3 年 1 月 19 日 16:45～17:00 場所：TKP ガーデンシティ PREMIUM 仙台西口 セミナー参加者：会場 5 名、オンライン 40 名以上	情報セキュリティ相談ブースを設け、相談受付を行った。情報セキュリティ関連資料も配置。	なし
3	【サイバーセキュリティセミナー；サイバーセキュリティの最新動向と中小企業が実施すべき対策】 主催者：東北経済産業局、東北地域情報サービス産業懇談会 日時：令和 3 年 1 月 27 日 16:05～17:00 場所：オンライン（Webex） セミナー参加者：72 名	イベント終了後、オンライン参加者で相談希望者がいれば、チャットと音声で相談を受ける。	相談 4 件 情報提供 1 件
4	【令和 2 年度第 5 回 IoT 等先進技術導入促進セミナー】 主催者：秋田県・秋田デジタルイノベーション推進コンソーシアム 日時：令和 3 年 1 月 28 日 15:00～15:15 場所：アキタパークホテル、オンライン（Zoom） セミナー参加者：会場 7 名、オンライン 16 名	イベント終了後、オンライン参加者で相談希望者がいれば、ブレイクアウトルームにて相談を受ける。	なし
5	【中小企業のための情報セキュリティセミナー ～できるところからはじめよう !! コストをかけずに SECURITY ACTION !!～】 主催者：独立行政法人情報処理推進機構（IPA） 日時：令和 3 年 2 月 19 日 17:15～18:00 場所：オンライン（Webex） セミナー参加者：不詳	イベント終了後、オンライン参加者で相談希望者がいれば、別途 Webex meetings のブレイクアウトルームにて相談を受ける。	なし

「第２回いわて組込み技術研究会」の会場



「サイバーセキュリティお助け隊 in 東北 成果報告会」の相談ブース



6.2 相談内容とその回答

令和３年１月 27 日に実施された「サイバーセキュリティセミナー；サイバーセキュリティの最新動向と中小企業が実施すべき対策」では４件の相談があり、情報提供も行った。その相談内容と回答は【表4】の通りである。

【表４】

No.	相談内容	回答（概要）
1	クラウドのファイルストレージ内に様々な情報を格納する機会が増えて参りました。（Google Drive,Dropbox 等）その情報の中には個人情報も格納するケースが発生する可能性があります。セキュリティ確保の観点からすると、オンラインストレージへの機密情報の格納というのはいかがなものなのでしょうか？	クラウドがよい悪いでなく、管理がなされていないことが問題である。個人が勝手に利用することを禁止し、組織が管理する必要がある。
2	個人情報保護対策についていろいろと進めておりますが、情報収集の方法としてプライバシーマークの認証取得に関することや他のコンサルティングサービス以外で有効なものはありますか？	プライバシーマークは体制構築の標準であり、対策を進め方が明確であるというメリットと、審査を通り認証を受けたということがお客様に安心感を与える。ISMS も同様に候補になる。医療系であれば、厚生労働省から出ているガイドラインも参考にするのがよい。
3	ウイルス対策ソフトに関してが、Windows Defender が最新の状態であればウイルス対策としてはどれぐらい大丈夫なのでしょうか？Windows の標準機能においての有効性などについて教えていただければと思います。	パターンマッチング型のアンチウイルスソフトは、どれがよいと一概にいえない。比較調査結果もあるが、どれが秀でているといえない。パターンマッチング型はどれか一つ導入しておけばよい。さらに強固にしたいのであれば振る舞い検知型など、検知の方法が違うアンチウイルスソフトをいれるのがよい。
4	どのメーカーのワークフローを利用するかを検討しているのですが、機密情報の決済なども含まれることを考えると、セキュリティ面でどこのメーカーを選んだ方がいいのか、どういったポイントで選ぶのがいいのかなどがもしあればご教示いただきたいです。	クラウドサービスを利用する場合は、サービスの継続性があるものを選ぶことが必要である。選定の基準としては、近く始まる ISMAP 制度の活用をおすすめする。

情報提供	
1	最近のトピックとして以下の内容について紹介した。 ・情報セキュリティの専門家として情報処理安全確保支援士という資格があり、相談先として資格保有者を活用する方法がある。 ・スマホ決済に関するセキュリティについて

6.3 相談対応に関する所感

東北地域における各種機関が開催する 5 件のセキュリティ関連イベントと連携し、イベント参加者等に対するセキュリティに関する出張相談対応を実施した。実績としては 1 件のイベントで 4 件の相談と 1 件の情報提供を行うことができたが、イベント参加者のようなセキュリティに関心のある方へ、もっと多くの有益な情報提供を行うことが望ましいと考える。

今回はコロナ禍であるため、オンライン開催のイベントが多く、気軽に相談がしにくい環境もあったかと思われる。今後、できるだけ多くの方へ有益な情報をたくさん提供するには、別の手段で行うことの検討も必要と考える。例えば、相談用 Web サイトを用意し、一定期間受け付け、個別にメールで回答する。また、SNS を活用する方法もある。

Web サイトによる相談対応の場合、QA 内容の Web 公開について承諾を得ることができれば、それを公開することにより、他の多くの方への情報提供になるため大きい効果が期待できる。SNS を活用する場合は、公開型で行うのか、閉鎖されたチャット形式で行うのかなど、実施方法の検討が必要である。いずれにせよ、いつでも気軽に相談できること、また、相談対応者の確保と回答の迅速性が重要になる。

7 セキュリティ関連スキルアップイベントの開催

7.1 実施イベントの概要

【表 5】

1	目的	コロナ禍により、テレワーク等、業務のデジタル化が急速に進む中、情報漏洩、サイバー攻撃等の脅威など潜在リスクが増大している昨今、セキュリティに関する知識向上、人材育成の一環として、参加者の方々へ情報セキュリティ講座と併せてクイズを取り入れ、セキュリティに関する「学びの場」「腕試しの場」のご提供を目的として開催する。
2	イベントタイトル	「情報セキュリティスキルアップ オンラインイベント」
3	主催	経済産業省東北経済産業局
4	主管	株式会社ブレインワークス
5	特別協力	独立行政法人情報処理推進機構（IPA）
6	開催日時	第 1 回　2021 年 2 月 12 日（金）13:30～16:00 第 2 回　2021 年 2 月 18 日（木）13:30～16:00 第 3 回　2021 年 2 月 25 日（木）13:30～16:00 ※ 第 1 回～第 3 回の内容は全て同じ。
7	会場	オンライン、Cisco Webex-Meetings・Google Forms を利用

8	対象者	以下の方を含めサイバーセキュリティに興味・関心のある方 ・中小企業経営者、企業・組織のセキュリティ担当者や関係者等 ・学生及びその他セキュリティに興味のある方
9	参加者（実績）	第 1 回：19 名 第 2 回：11 名 第 3 回：13 名 ＊3 回のイベント参加者の東北域市区町村（判別つくもの）<順不同> 青森県平川市、岩手県盛岡市、岩手県紫波郡矢巾町、宮城県仙台市青葉区、宮城県仙台市宮城野区、宮城県仙台市若林区、宮城県石巻市、宮城県多賀城市、宮城県岩沼市、宮城県登米市、宮城県大崎市、秋田県秋田市、秋田県大館市、秋田県潟上市、山形県山形市、山形県米沢市、山形県鶴岡市、山形県村山市、山形県長井市、山形県天童市、福島県福島市、福島県郡山市、福島県いわき市、その他
10	参加費	無料
11	実施内容	1．「情報セキュリティ講座」 独立行政法人情報処理推進機 ・中小企業における情報セキュリティの最新動向と対策 ・「SECURITY ACTION」制度のご紹介 （第 1 回はライブ配信、第 2 回及び第 3 回は録画配信） 2．「クイズにチャレンジ」 株式会社ブレインワークス ・参加者は、入門編・マネジメント編・テクニカル編で構成されたクイズ（各編とも 24 問）に回答する。 ・各編とも回答後、参加者自身の Web ブラウザ画面で採点結果が表示される（Google Forms にて）。その後、正解発表と簡単な解説を行う。
12	申し込み方法	Web サイトからのお申込み
13	参加者募集方法	・イベント告知媒体の利用 せんだい E 企業だより(財団法人仙台市産業振興事業団) 仙台 NEWSCAST みやぎ産業振興機構ホットライン こくちーず ・「2.地域のキーパーソン等発掘調査」でヒアリング調査を行った大学等の先生へ学生への案内を依頼 ・東北経済産業局による案内　等

7.2 イベント実施報告

3 回のイベントの実施内容は、【表 5】11 の通りである。「クイズにチャレンジ」においては、各編とも Google Forms で 24 問のクイズに回答するフォームを作成し、回答後、採点結果が各自の Web ブラウザ画面に表示される仕組みを構築した。

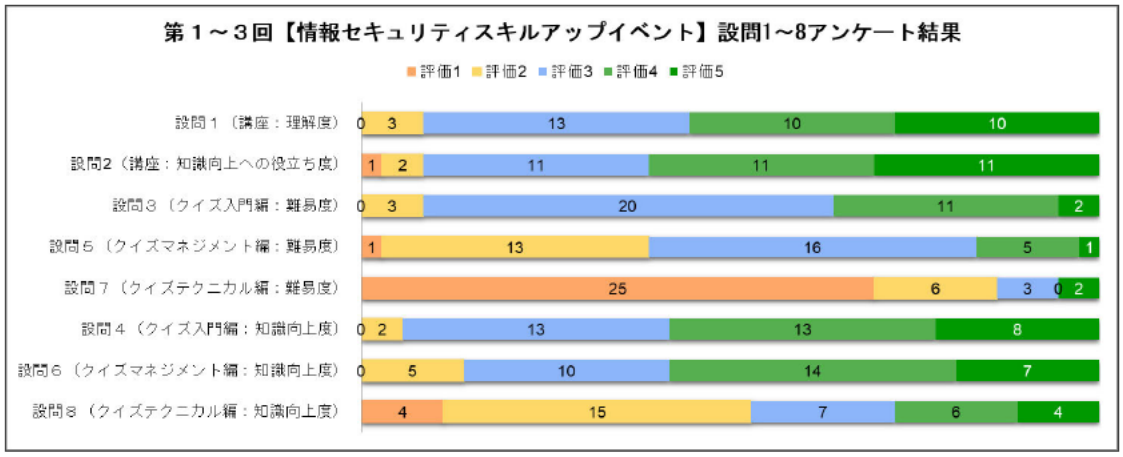
また、イベントの最後には、Web フォームによるアンケート調査も行った。その集計結果と考察を以下に提示する。

（1） 第 1～第 3 回の講座とクイズに関するアンケート回答内容の集計と考察

【表 6】

設問	【グラフ 49】評価 5 又は評価 4	【グラフ 49】評価 1 又は評価 2
[設問 1]情報セキュリティ講座の理解度	「十分に理解できた」又は「理解できた」：55.6%	理解が「できなかった」又は「あまりできなかった」：8.3%
[設問 2]情報セキュリティ講座の知識向上への役立ち度	「十分に役立つ」又は「役立つ」：61.1%	「まったく役立たない」又は「役立たない」：8.3%
[設問 3]クイズ（入門編）の難易度	「非常に簡単」又は「簡単」：36.1%	「非常に難しい」又は「難しい」：8.3%
[設問 4]クイズ（マネジメント編）の難易度	「非常に簡単」又は「簡単」：16.7%	「非常に難しい」又は「難しい」：38.9%
[設問 5]クイズ（テクニカル編）の難易度	「非常に簡単」又は「簡単」：5.6%	「非常に難しい」又は「難しい」：86.1%
[設問 6]クイズ（入門編）による知識向上度	「十分向上する」又は「向上する」：58.3%	「まったく向上しない」又は「向上しない」：5.6%
[設問 7]クイズ（マネジメント編）による知識向上度	「十分向上する」又は「向上する」：58.3%	「まったく向上しない」又は「向上しない」：5.6%
[設問 8]クイズ（テクニカル編）による知識向上度	「十分向上する」又は「向上する」：27.8%	「まったく向上しない」又は「向上しない」：52.8%

【グラフ 49】



情報セキュリティ講座については、「十分に理解できた」又は「理解できた」、「十分に役立つ」又は「役立つ」という回答が共に半数を超えたことから、理解したうえで、今後のセキュリティ対策に役立てることが可能な内容であったと評価する。講座の後半で説明している「SECURITY ACTION」制度を理解して頂くことで、今後の普及につながることを期待する。

一方、クイズにチャレンジでは、クイズの難易度が入門編、マネジメント編、テクニカル編の順に高くなっていることがうかがえる。通常、ある程度、難易度が高いことで知識の向上につながることが想定されるが、入門編とマネジメント編では「十分向上する」又は「向上する」という回答割合が同じで、難易度が高いテクニカル編の割合は低くなっている。これは、「理解することが難しく知識の向上につながらない」、「高度な知識は業務では不要である」、「業務で求められる分野の知識ではない」などといったことが要因ではないかと考えられる。3 編のクイズ全体（第 1～第 3 回）の知識向上度で「十分向上する」又は「向上する」という回答割合は、約 48%と半数近くであることから、ある程度「学びの場」に役立てることはできたものと評価する。

（2） 寄せられたご意見・ご感想からの考察

以下は、全体を通してのご意見・ご感想や今後のご要望等に関する自由記入型の設問への回答で注目すべきと考えたご意見・ご感想である（実際に記入された内容を編集し、主旨を提示した）。

- 各発表者ともに淡々とした話口調だったので聞きづらい印象を受けた。
- 講座の内容とクイズの難易度や分野に関連性がない。
- 基礎知識がある程度ないとクイズの回答は難しいと感じる。
- クイズの内容を読み解くのに時間が必要であり、やり方の工夫も必要かと思う。
- 定期的に情報セキュリティのセミナーなどを受講しているが、本日初めて聞いた内容もあった。技術の進歩や社会の変化によって新たな脅威や対策が生まれていることを深く実感した。
- セキュリティ対策では、PC 側の設定で対処しておくことや、攻撃に関する事例や対応策などを画像などで示してくれるとわかりやすい。
- クイズは講座で触れた内容についての確認問題という位置付けだと、もう少し身につくように思う。
- どこをターゲットにして教えているのかが分からない。複数回あるのなら、ターゲット層を分けて開催した方が有意義だと思う。

今回は、「学びの場」と共に「腕試しの場」を意識してイベントの企画を行ったことから講座とクイズへの回答という 2 本立ての構成になった。双方のコンテンツを作成したのは別組織であったことで、関連性がなかったことへのご指摘があったものと思う。イベント全体の方針や方向付けを明確にし、ディレクションを行う必要性を感じた次第である。

また、今回参加された方々は、様々な業種であり、セキュリティ知識のレベルや自組織内で実施しているセキュリティ対策も様々であると思われるため、全員に満足して頂ける内容にすることは難しいものと感じた。今後は、ご指摘にあった通りターゲット層を明確にする、複数回のイベントを実施する場合は、ターゲット層を分けてそれに見合った内容にするなどの検討も必要である。

8 中小企業セキュリティ対策支援モデル事業

8.1 実施概要

「5 中小企業のセキュリティに関する活動調査」でヒアリングを実施した中小企業等からセキュリティ対策支援モデル企業を選定し、個別指導を実施した。

中小企業セキュリティ対策支援モデル事業の目的は、セキュリティ対策を実施する企業（指導先企業）や支援者側の課題を抽出し、今後の効果的な支援につなげることである。

中小企業セキュリティ対策支援モデル事業の企業選定は以下の方法で行い、3 社選定した。

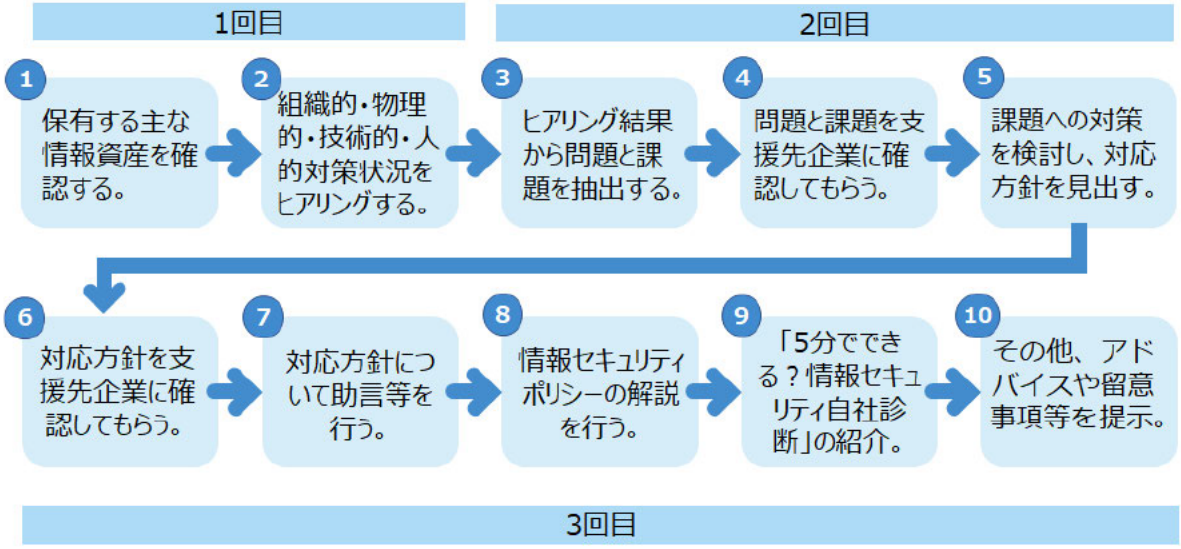
- 「5 中小企業のセキュリティに関する活動調査」におけるヒアリング調査で、個別指導に関心があるかを尋ね、関心がある場合は具体的な個別指導の内容を伝え、実施を希望した企業を選定
- 「7 セキュリティ関連スキルアップイベントの開催」のアンケート調査により、セキュリティ対策に前向きで個別指導に関心がある企業を抽出し、当該企業へ具体的な個別指導の内容を伝え、実施を希望した企業を選定
- 「2 地域のキーパーソン等発掘調査」でヒアリング調査を行ったコミュニティ主催者からの紹介で、セキュリティ対策に前向きで個別指導に関心がある企業へ具体的な個別指導の内容を伝え、実施を希望した企業を選定

なお、個別指導は、1 社あたり 3 回、オンライン（Webex-Meetings）で行うこととした。また、指導を受けることで企業は、独立行政法人情報処理推進機構（IPA）が提示している「情報セキュリティ 5 か条」等を基にした重要な情報セキュリティ対策の実施状況について助言を受けることができ、「SECURITY ACTION」制度の二つ星を宣言することができる状態になることを目指した。個別指導の実施プロセスは【図 1】の通りである。

なお、3 回目は登録セキスペに同席してもらい、【図 1】の 8～10 を担当して頂いた。

3 回の個別指導に関する計画及び報告については、【別紙 6】「中小企業セキュリティ対策支援モデル事業計画書兼報告書」に取りまとめた。また、指導先企業に関する現状、問題点等、課題、対応方針、助言（参考情報）を【別紙 7】「現状及び課題分析シート」に、今後の支援に向けた考察等を【別紙 8】「中小企業セキュリティ対策支援モデル事業についての総括」に、それぞれ取りまとめている。

【図 1】 実施プロセス



8.2 個別指導の実施結果

W 社・A 社・F 社の 3 社へ個別指導を実施し、現状と問題点を把握することができた。そこから課題を抽出し、その対応方針を検討した。

W 社・F 社のような小規模事業者の場合、経営トップが高い意識を持つことが重要で、それが従業員に伝わり、セキュリティ対策を定着させる必要がある。W社の現状は、社長はセキュリティ意識が高く社内の IT 環境を自ら構築し、様々な対策を行っていたが、足りない部分もあった。F 社の場合は、社長はリテラシー不足のところもあったが、セキュリティ対策を前向きに進めて行く姿勢が感じ取られた。

A 社のような複数の拠点を持つ企業の場合、拠点によってセキュリティ意識のレベルに差が出ることがあるが、平準化することは容易ではない。A 社も本社と施工現場で意識の乖離が見受けられ、定期的な研修の実施により改善に取り組んでいた。

課題とその対応方針の概要については、【表 7】の通りである。（詳細については、【別紙 7】「現状及び課題分析シート」を参照）

【表 7】

指導先企業	課題	対応方針
W 社 専門・科学技術、業務支援サービス業（従業員 20 人以下）	・セキュリティポリシーを策定していない ・業務用 PC の持ち出し、パスワード設定、私有媒体の使用、業務用 PC の自宅使用について、ルールがない状態で行われている ・重要情報のバックアップが不十分 ・社員への情報セキュリティに関する情報（脅威、攻撃手口、脆弱性）が不十分	・早急にルール化が必要な事項についてルールを明文化する（簡易的なルールを作成） ・持ち出し PC のドライブ、私有媒体の暗号化を行う ・セキュリティベンダーのメルマガ情報を社員へ周知する ・自宅のネットワーク環境の確認を行う
A 社 建設業（従業員 21 人以上の中小企業）	・セキュリティポリシーを策定していない ・業務用 PC の持ち出し、パスワード設定、私有媒体の使用について、ルールがない状態で行われている ・施工現場で重要書類及びノート PC の施錠保管が不十分	・早急にルール化が必要な事項についてルールを明文化する（簡易的なルールを作成） ・持ち出し PC のドライブの暗号化を行う ・施工現場への研修を継続し、施錠保管を徹底させる。 ・私有 USB メモリの使用実態を把握し、対策を検討する
F 社 保健衛生・社会事業（従業員 20 人以下）	・事務所保管のノート PC は盗難防止対策やディスクの暗号化が行われておらず、情報漏えい対策が不十分 ・タブレット端末（外部で利用）にパスコードや指紋認証等の認証設定が行われておらず、不正利用対策が不十分 ・セキュリティ対策ソフトが導入されておらず、マルウエア感染、フィッシング等に対する予防策が不十分 ・脅威や攻撃の手口、脆弱性等の情報収集方法が分からず、それらが社内で周知されていない ・セキュリティ対策を主導する人がおらず、育成が必要	・ノート PC においてはワイヤーロック等の盗難防止対策を行う ・タブレット端末にはパスコード又は指紋認証等の認証設定をする ・セキュリティ対策ソフトを導入する ・IPA のサイトやメルマガ等から定期的に情報収集を行い、社内でそれらを周知する ・セキュリティ人材の育成について検討を行う

8.3 今後に向けた対策

W社と F 社の場合、情報セキュリティ対策強化にあたって社長の意識と姿勢が重要ポイントとなるため、今後の効果的な支援は企業の実情を把握したうえで、社長へ有益な助言と情報を提供し、フォローアップを行うことである。そのためには、地域コミュニティにおいて個別にコミュニケーションをとることができる環境を作ることが有効である。なお、F 社の社長には、リテラシー向上のための知識とノウハウを提供することも効果的な支援であり、セミナーや勉強会の企画も必要と考える。

A 社の場合、情報セキュリティ対策強化のためには施工現場の意識改革が必要で、現在、社内研修を行っているところである。今後の効果的な支援は研修効果が上がるような情報を提供し、フォローアップを行うことであるが、場合によっては、地域コミュニティから外部講師を派遣することも研修効果を上げるための対策と考えている。

9　地域コミュニティのあり方に関する考察と提言

地域の中小企業は、単独で有効なサイバーセキュリティ対策を行うことは困難であり、また、セキュリティに関する人材育成・普及啓発の機会や情報共有の枠組みなどが不足している。そこで、本事業では地域におけるセキュリティコミュニティを形成し、中小企業のセキュリティ対策に関する意識向上・人材育成、関係者間の情報共有（「共助の関係の形成」）の実現を目指すこととし、本報告書に記載した施策を行うことで、以下を収集することができた。

- 地域のキーパーソンになり得る方々へのヒアリング調査から得た中小企業支援に関する意見や考え、地域コミュニティに対する意識・意見等
- 中小企業へのアンケート調査（意識調査）結果から得たデジタル化やセキュリティ対策に関する実態と意識
- 登録セキスペへのアンケート調査とヒアリング調査から得た登録セキスペの活動状況と地域の中小企業へのセキュリティ対策強化に向けた活動との連携の可能性
- 中小企業へのヒアリング調査から得た具体的なセキュリティ対策の実態と課題意識
- 地域関係機関が開催するイベントの参加者による質問から得られた企業等の疑問点
- 中小企業セキュリティ対策支援モデル事業で実施した個別指導から得られた個別企業の実態とセキュリティ対策への姿勢等

現在、IT 関連企業、業界団体、経済団体、大学等の教育機関、研究機関、国関係機関、自治体、県警、IT 系コミュニティなどが、サイバーセキュリティに関する啓発啓蒙、情報共有、人材育成を目的としたセミナーや研修、また、セキュリティ演習を実施している。しかし、様々な脅威や脆弱性がある昨今、地域の中小企業が基本的な対策を行うことに前向きになり、実践することにつながる有益な機会が、あまり与えられていないのではないかと考える。

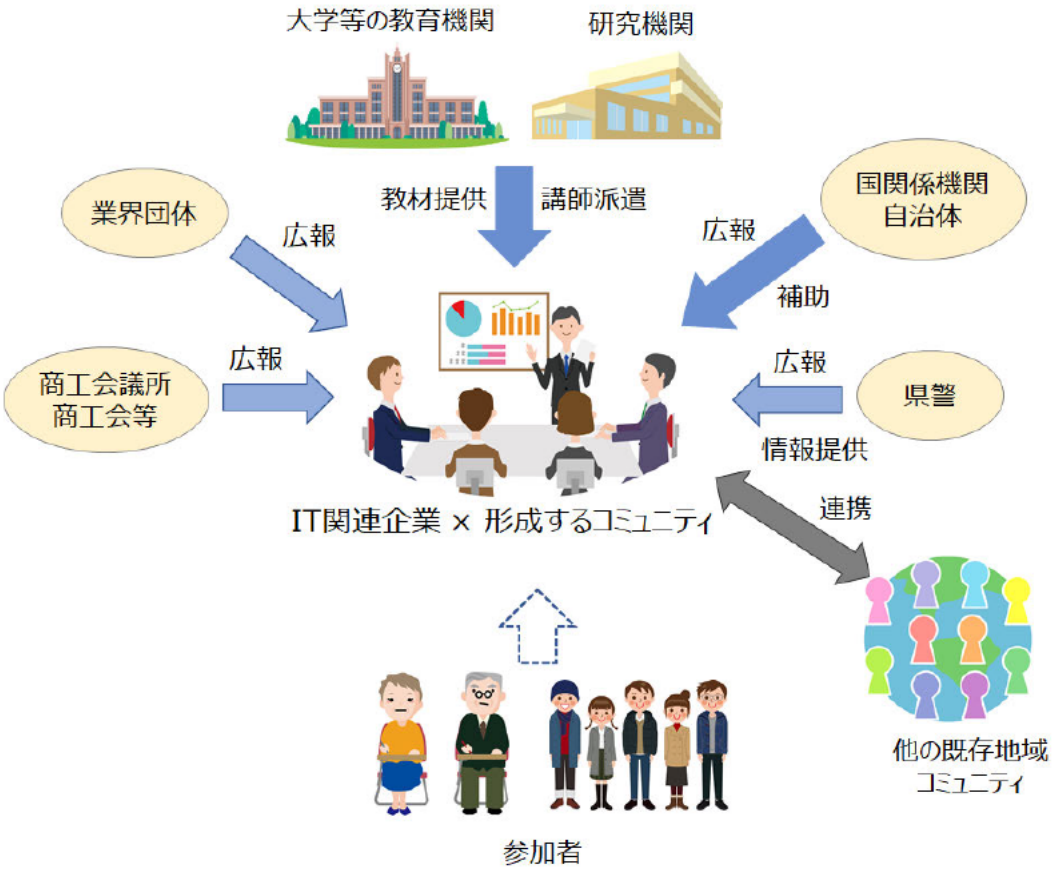
そこで、地域のセキュリティコミュニティを形成し、本事業で得られた上記のような情報等を参考にして有効な支援を行うためには上記の各組織が役割を明確にし、連携を図るとともに、支援対象とする中小企業像とコミュニティの役割を明確にする必要がある。基本的なセキュリティ対策を実施できていない企業と高度な対策を目指している企業では、求められる人材、知識、情報などが異なるためである。

先ずは、基本的なセキュリティ対策を実施できていない企業の底上げが必要かと考えており、そのような企業に対する意識向上と人材育成、情報共有をコミュニティの役割としてはどうかと思う。

そのコミュニティの構成と各組織の役割については、【図２】のように考えている。中小企業にとって身近な IT 関連企業と今後形成するコミュニティが連携して中核になり運営することがコミュニティの継続性と活性化の観点から望ましい。また、必要に応じ他の既存の地域コミュニティと連携することで、参加者が増えたり、活性化につながったりすることも考えられる。

一方、コミュニティの参加者は、地域の中小企業の他、大学などの学生も参加できれば、常に新しいメンバーが加わる環境ができ、企業の人材確保にもつながる可能性があると考える。

【図２】コミュニティの構成と各組織の役割



現在、地域では、北海道地域のセキュリティ対策の向上を目的として設立された北海道地域情報セキュリティ連絡会（HAISL）や関西のサイバーセキュリティ分野における産学官等の相互協力を促進するために発足した関西サイバーセキュリティ・ネットワーク（関西 SEC-net）が活動している。特に後者は、関西におけるセキュリティ推進基盤として産・学・官・コミュニティが連携し、各主体が実施していない領域の取組を補完的に実施し、人材発掘・育成、情報交換、機運醸成の場を提供するという他ではあまり見られない活動を行っており、参考にすべきと考えている。

最後に、地域の IT 関連企業と今後形成するコミュニティが連携を図り短期間でコミュニティを立ち上げ、また各組織とも連携し、協力を取り付けることで中小企業にとって有効なコミュニティの形成が実現することを期待する。

以上