東北経済産業局 御中

令和 3 年度中小企業サイバーセキュリティ対策支援促進事業

(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 4 年 2 月 28 日

特定非営利活動法人
みちのく情報セキュリティ推進機構

目　次

１． はじめに

中小企業は、令和 2 年度から続く新型コロナウイルス対策の対応により、テレワーク等業務のデジタル化を急速に進める中、情報漏洩やサイバー攻撃の脅威等といった潜在リスクが増大してきている。

このような中、中小企業が、デジタル化によるリスクに対応しつつ、その恩恵を享受するためには、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が急務となっており、引き続き、地域における情報セキュリティ対策・サイバーセキュリティ対策に関する積極的な情報発信、人材育成の支援が必要な状況である。

そのために、令和 3 年度は令和 2 年度で実施した事業を踏まえ、東北地域の情報セキュリティ向上のためのコミュニティ形成を促進するため、東北管内の中小企業へのデジタル化・セキュリティに関する状況及び意識調査、デジタル化の事例紹介やサイバー攻撃の最新の脅威動向等についてのセミナーの開催、セキュリティ対策の強化に向けたモデル事業（企業に対する個別アドバイス）の実施、検証を行った。

２． デジタル化・セキュリティに関する状況・意識調査の実施

２.１ 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県の中小企業へアンケート調査を実施するにあたり、調査対象企業数を合計 2100 社とし、各県各業種等の企業選定については以下の①及び②により行った。

① 産業大分類別事業所数に基づく東北６県の中小企業 2000 社へのアンケート

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 社へアンケートを実施することとした。

② プライバシーマーク取得済みの東北６県の中小企業 100 社へのアンケート

令和 2 年度のアンケート調査時よりアンケート回収数の拡大を図るため、あらたに、東北 6 県のプライバシーマーク認証取得企業（全 361 社（2021 年 3 月 31 日現在） ＜一般財団法人日本情報経済社会推進協会(JIPDEC)がホームページに公表 https://entity-search.jipdec.or.jp/pmark＞）から中小企業 100 社を無作為に抽出し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 2100 社に対して、『「デジタル化・セキュリティに関する状況・意識調査」アンケート調査票』を同封し、宅配ＤＭ便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『「デジタル化・セキュリティに関する状況・意識調査」アンケート調査票』を郵送、Fax、メールにて行うと共に、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。調査事項は以下のとおりである。

1．企業属性について

1-1　貴社の従業者数（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　取引関係について、現在発注側からデジタル化（例：受発注システム等）の要望がありますか？

2-3　取引先との受発注において、主たる手段は何ですか？

2-4　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？

2-5　テレワークのシステムを導入していますか？

2-6　（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？

2-7　（上記で、実施している場合）今後とも継続する予定ですか？

2-8　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？

2-9　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ビジョンを策定していますか？

2-10　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具体的な戦略を策定していますか？

2-11　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を整備していますか？

2-12　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？

2-13　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？

2-14　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？

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　社内の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を行う情報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？

4-8　情報セキュリティに関する外部認証の取組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情報や脆弱性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情報や脆弱性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、相談してみたいことがあれば、自由に記入してください。

2.2 アンケート調査結果

東北６県の中小企業 2100 社へアンケート調査票を送付し、701 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。

このアンケート調査の回答を調査テーマ別の考察と「業種別」・「県別」の考察を分けて行った。その内容を以下に示す。

（１）　調査結果についての調査テーマ別の回答と考察

アンケート調査の回答（701 社分）を 5 つの調査テーマ別に考察を行った。その内容を以下に示す。

① デジタル化の状況について

●デジタル化の進捗状況については、昨年度と比較してデジタル化への取り組みが「あまり進んでいない」企業が少なくなっており、一方で「ある程度進んでいる（Web 会議の導入、給与計算、受発注、勤怠管理等一部の業務プロセス(生産プロセスを除く)の効率化）」企業が多く見られ、一定程度の進捗はあるものと推察される。

●取引関係における発注側からのデジタル化の要望については、「ない」と回答した企業が半数程度見られた。

●取引先との受発注における主たる手段は、電話や FAX 等といった回答が多く見られ、デジタル化による効率化の余地があり、促す取組も必要と推察される。

② 社内のデジタル化を進めるにあたっての課題について

●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、昨年度と比較して「人員（従業員自体）が不足している」との回答が多く見られた。

●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、昨年度と比較して「育成ができていない」との回答も少々多く見られ、デジタル化を進めるための人員及び育成が依然不足しているものと推察される。

③ 自社のセキュリティポリシーの策定状況

●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)の策定状況について、昨年度と比較して、「策定していない」との回答が多く見られ、昨年度からほとんどセキュリティポリシーの策定が進んでいないものと推察される。

④ 「SECURITY ACTION」の取組状況

●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)の取組状況については、昨年度と同様、「制度を知らない」、「制度は知っているが取り組んでいない」との回答が多く見られた。しかし、昨年度は「二つ星を宣言している」企業がなかったが、今年度は「二つ星を宣言している」との回答がわずかであるが見られた。

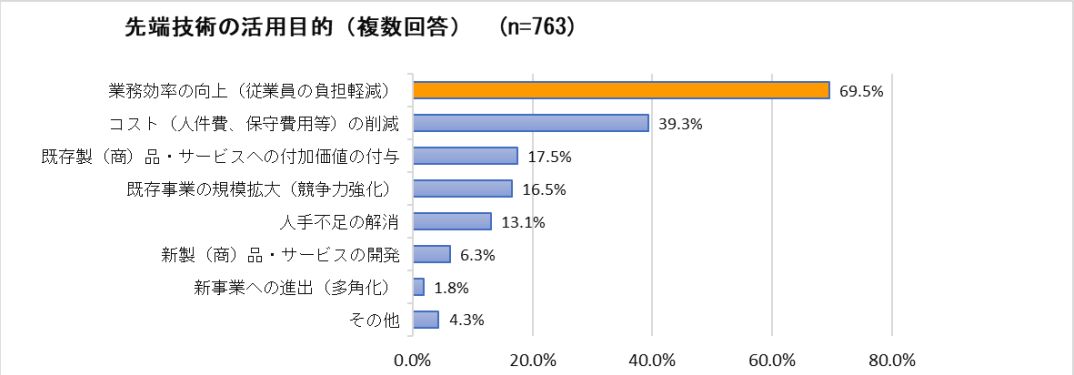
⑤ サイバーセキュリティの取組みにあたっての課題

●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は、昨年度と比較し、「人員が不足している」との回答が多く見られた。

●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育成についての課題は、昨年度と比較し、「育成ができていない」との回答が多く見られた。

サイバーセキュリティ対策を推進しつつあるものの、人材育成が不十分で、サイバーセキュリティ対策要員が不足している現状が推察される。

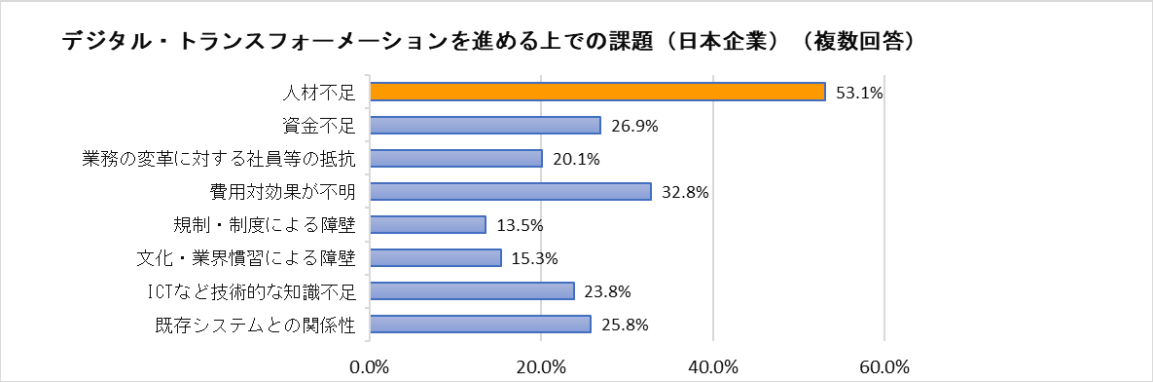
《 参考情報 》



【参考図１】先端技術の活用目的

日本企業の ICT 投資は業務効率を目的としたものが中心であり、事業拡大や新規事業進出といったビジネスモデルの変革を伴うようなデジタル化（デジタル・トランスフォーメーション：DX）は広がっていない。

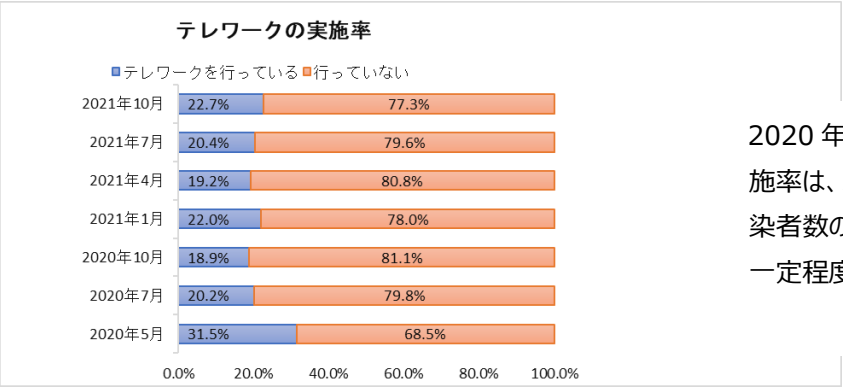
（出典）財務省（平成 30 年）「財務局調査による「先端技術（IoT、AI 等）の活用状況」について」



【参考図２】デジタル・トランスフォーメーションを進める上での課題

我が国の ICT 人材は ICT 企業に偏在しており、企業が DX を進める上で人材不足が大きな課題である。

（出典）総務省 「令和 3 年版情報通信白書」



2020 年 7 月調査以降、テレワーク実施率は、新型コロナウイルスの新規感染者数の状況に関わらず約 2 割と、一定程度定着している。

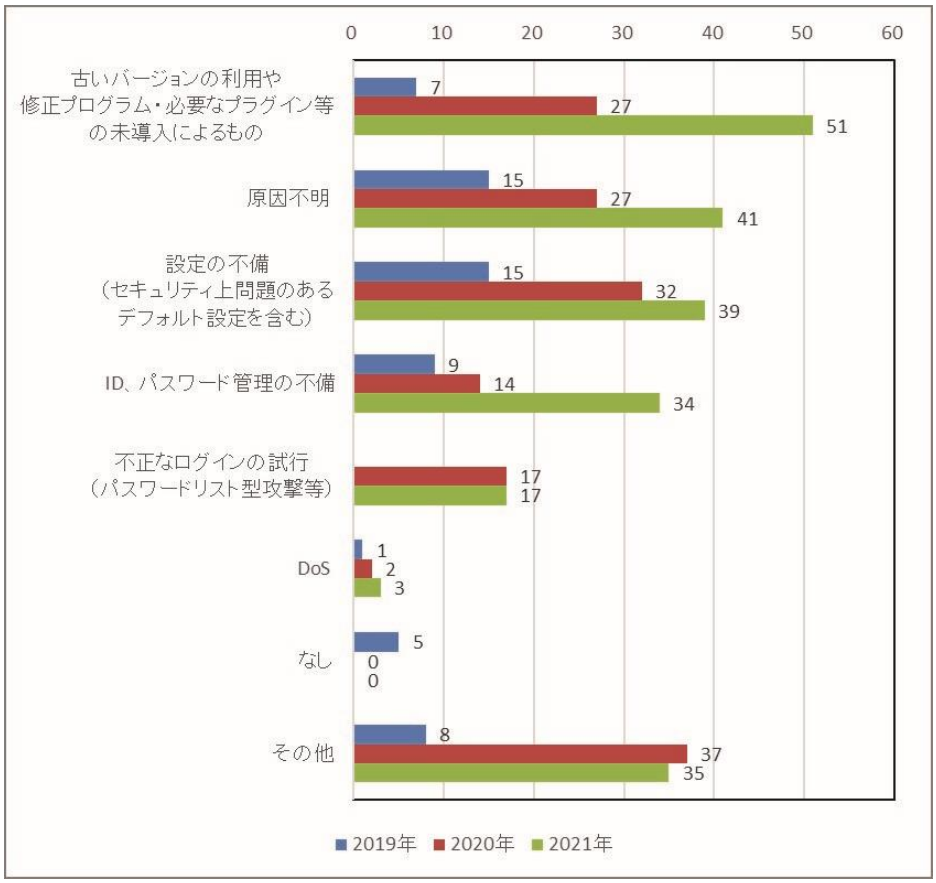
【参考図３】テレワークの実施率

(出典) 公益財団法人日本生産性本部 「第 7 回働く人の意識に関する調査」

【参考図４】不正アクセス届出件数の年別推移

2021 年に寄せられた不正アクセス届出は、年間で前年の 187 件より 56 件（約 29.9%）多い、243 件の届出があった。このうち、実被害があった届出は 197 件であり、全体の約 81.1%を占めた。

（出典）独立行政法人情報処理推進機構「コンピュータウイルス・不正アクセスの届出状況［2021 年（1 月～12 月）］」



【参考図５】不正アクセス原因別件数の推移（2019～2021 年）

2021 年において最も多く見られた被害原因は、「古いバージョンの利用や修正プログラム・必要なプラグイン等の未導入によるもの」で 51 件あり、次いで「設定の不備」が 39 件、「ID、パスワード管理の不備」が 34 件であった。

（出典）独立行政法人情報処理推進機構「コンピュータウイルス・不正アクセスの届出状況［2021 年（1 月～12 月）］」

（２） 調査結果についての業種別の回答と考察

アンケート調査の回答（701 社分）を業種別に考察を行った。その内容を以下に示す。

① デジタル化の状況について

●「情報通信業」においては全ての企業が「ある程度進んでいる（Web 会議の導入、給与計算、受発注、勤怠管理等一部の業務プロセス(生産プロセスを除く)の効率化）」と回答しており、デジタル化が進んでいる状況が推察される。

●取引関係における発注側からのデジタル化の要望については、「金融・保険業」は「ある」との回答が多く見られ、発注側からのデジタル化の要望が多い業種となっている。

●取引先との受発注における主たる手段は「情報通信業」と「専門・科学技術、業務支援サービス業」の業種においては、「E-Mail」、「取引先との受発注システム」との回答が多く見られ、デジタル化が進んでいる状況が推察される。

●テレワークの導入状況については、「情報通信業」と「専門・科学技術、業務支援サービス業」は「導入している」との回答が多く見られた。

なお、今後もテレワークを継続するか否かについては、新型コロナウイルス禍が終息した際の対応が業種により異なるものと推察される。

●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ビジョンの策定状況については「不動産業」と「保健衛生・社会事業」は「策定する予定はない」との回答が多く見られた。

●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の有無については、「金融・保険業」、「情報通信業」及び「保健衛生・社会事業」は「十分意識している」との回答が多く見られた。

●セキュリティリスク対策としての予算の確保状況については「情報通信業」は「十分確保している」との回答が多く見られた。

② 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について

●社内のデジタル化を進めるにあたって推進する人材に関する課題については、「金融・保険業」は「デジタル化を推進できる人材が不足している」との回答が多く見られた。

●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関する課題については、「金融・保険業」などは「育成が十分でない」との回答が多く見られた。

デジタル化が進んでいる業種においては、人材育成に取り組んでいるものの育成が十分ではなく、デジタル化を進めるための要員が不足しているものと推察される。

●社内のデジタル化を推進する人材の確保と育成に関する今後の取り組みについては、「運輸・郵便業」と「不動産業」は「現状のまま」との回答が多く見られ、現在の要員でのデジタル化推進人材の育成を行わず「新たな人材を確保し育成する」ものと推察される。

③ 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について

●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)の策定状況については、「金融・保険業」などは「策定済み」との回答が多く見られ、業務内容に対応して情報セキュリティ対策が進んでいるものと推察される。

●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関する課題については、「農林水産業」などの業種では「人員が不足している」との回答が多く見られた。

●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育成に関する課題については、「金融・保険業」などは「育成が十分でない」との回答が多く見られた。

デジタル化が進んでいる業種においては、人材育成に取り組んでいるものの育成が十分ではなく、セキュリティ対策を推進するための要員が不足しているものと推察される。

●セキュリティ対策を推進する人材の確保と育成に関する今後の取り組みについては、「運輸・郵便業」と「不動産業」は「現状のまま」との回答が多く見られ、現在の要員でのセキュリティ対策推進人材の育成を行わず「新たな人材を確保し育成する」ものと推察される。

●社内のサイバーセキュリティ対策に関する検討を行う情報セキュリティ委員会の設置状況については、「情報通信業」は「設置している」との回答が多く見られた。

●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)の取組状況については、「情報通信業」は「制度は知っているが取り組んでいない」との回答が多く見られた。

●情報セキュリティに関する外部認証の取得状況については、「情報通信業」は「プライバシーマークを取得済み」との回答が多く見られた。

④ 脆弱性情報の適切な把握について

●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状況については、「情報通信業」は「定期的に収集している」との回答が多く見られた。デジタル化が進んでいる業種ほど積極的に脅威情報や脆弱性情報を収集している状況であることが推察できる。

⑤ インシデント(セキュリティ事故)発生時の備えについて

●インシデントが発生した場合に備えた緊急時の連絡・報告体制については、「金融・保険業」、「情報通信業」は「社内の体制はできている」との回答が多く見られた。自社だけではなく委託先を含めた体制を構築している企業も多いことが推察される。

⑥ サプライチェーン全体のリスク認識について

●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の管理責任については、「農林水産業」と「不動産業」は「わからない」との回答が多く見られた。

●委託先や下請け等の外部組織との情報の取り扱いに関する注意事項の共有方法については、「農林水産業」などは「共有していない」との回答が多く見られた。

今回の調査において、委託先や下請け等の外部組織との情報の取り扱いに関する注意事項の共有を行っていないと回答した企業が多く見られ、今後は契約書等の書面で共有することが必要であると考える。

（3） 調査結果についての県別の回答と考察

アンケート調査の回答（701 社分）を県別に考察を行った。その内容を以下に示す。

① デジタル化の状況について

●デジタル化の進捗状況については、青森県と岩手県の企業は「あまり進んでいない（E-mail、表計算ソフト等の導入程度）との回答が多く見られ、デジタル化が進んでいないと推察される。

●取引関係における発注側からのデジタル化の要望については、山形県の企業は「ある」との回答が多く見られ、発注側からのデジタル化の要望が多い県となっていると推察される。

●取引先との受発注における主たる手段は、福島県の企業は「取引先との受発注システム」との回答が多く見られ、デジタル化が進んでいる状況が推察される。

●テレワークの導入状況については、宮城県の企業は「導入している」との回答が多く見られた。

今後もテレワークを継続するか否かについては、新型コロナウイルス禍が終息した際の対応に苦慮しているものと推察される。

●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ビジョンの策定状況については、岩手県と山形県の企業は「すでに策定済み」との回答が多く見られた。

また、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具体的な戦略の策定状況については、青森県、岩手県、秋田県の企業は「策定する予定はない」との回答が多く見られた。

●セキュリティリスク対策としての予算の確保状況については、青森県の企業は「ほとんど確保していない」との回答が多く見られた。

② 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について

●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関する課題については、宮城県の企業は「育成が十分でない」との回答が多く見られた。

デジタル化が進んでいる県においては、人材育成に取り組んでいるものの育成が十分ではなく、デジタル化を進めるための要員が不足しているものと推察される。

●社内のデジタル化を推進する人材の確保と育成に関する今後の取り組みについては、現在の要員でのデジタル化推進人材の育成を行わず「新たな人材を確保し育成する」ものと推察される。

③ 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について

●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)の策定状況については、宮城県の企業は「策定済み」及び「現在、策定中」との回答が多く見られ、情報セキュリティ対策が進んでいるものと推察される。

●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関する課題については、宮城県の企業は「人材が不足している」との回答が多く見られた。

●セキュリティ対策を推進する人材の確保と育成に関する今後の取り組みについては、岩手県の企業は「新たな人材を育成する」との回答が多く見られ、当該企業においては現在の要員でのセキュリティ対策推進人材の育成を行わず「新たな人材を確保し育成する」ものと推察される。

●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)の取組状況については、福島県の企業は「制度は知っているが取り組んでいない」との回答が多く見られた。

●情報セキュリティに関する外部認証の取得状況については、秋田県の企業は「プライバシーマークを取得済み」との回答が少なく見えた。

④インシデント(セキュリティ事故)発生時の備えについて

●インシデントが発生した場合に備えた緊急時の連絡・報告体制については、山形県及び福島県の企業は「委託先等の社外を含めた体制がある」との回答が多く見られ、自社だけではなく委託先を含めた体制を構築している企業も多いことが推察される。

⑤ サプライチェーン全体のリスク認識について

●委託先や下請け等の外部組織との情報の取り扱いに関する注意事項の共有方法については、青森県及び山形県の企業は「共有していない」との回答が多く見られた。

今回の調査において、委託先や下請け等の外部組織との情報の取り扱いに関する注意事項の共有を行っていないと回答した企業が多く見られたが、今後は契約書等の書面で共有することが必要であると考える。

（４） 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、ほぼ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想定されるため、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、情報セキュリティの三大要素である情報の機密性・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、定期的なデジタル化対応セミナーやサイバーセキュリティ対策セミナーの開催とともに、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る。

3. デジタル化・セキュリティセミナーの開催

3.1 デジタル化・セキュリティセミナーの開催概要

デジタル化・セキュリティセミナーの開催概要は【表１】のとおりである。

【表１】デジタル化・セキュリティセミナーの開催概要

1	目的	企業・組織のセキュリティ担当者やセキュリティ技術に興味がある社会人や学生を対象に、デジタル化の事例紹介、サイバー攻撃の最新の脅威動向、取るべき対策、取組事例等について 3 回程度（参加者レベルに応じた開催を想定）セミナーをオンラインにて開催する。また、開催にあたって、セキュリティに関する質問事項を事前に伺い、セミナー内にて回答するなどの相談対応を併せて行う事で、参加者の理解を促進する。
2	セミナー名称	デジタル化・サイバーセキュリティセミナー
3	主催	経済産業省東北経済産業局
4	共催	特定非営利活動法人みちのく情報セキュリティ推進機構（MISEC）
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 12 月　2 日(木) 13:30～15:30 第２回　2021 年 12 月 23 日(木) 13:30～15:30 第３回　2022 年　1 月 20 日(木)　13:30～15:30
7	会場	オンライン。 第 1 回及び第 2 回は”コクリポウェビナー”を利用し、会場を N-oval ビル　2 階とする。 なお、第 3 回は都合により外部の会場を借用し、“Microsoft Teams ウェビナー”を利用する。 主催者及び講師は、各々の会場に集合。なお、講師は会場以外からの参加も可能とする。また、急用のため当日欠席の場合は事前収録の動画のみでの登壇も可能とする。
8	対象者	第１回　企業・組織のセキュリティ担当者向け、及びセキュリティ技術に興味のある社会人、学生向け 第２回　企業・組織のセキュリティ担当者向け、及びセキュリティ技術に興味のある社会人、学生向け 第３回　経営者向け、及び企業・組織のセキュリティ担当者向け
9	参加費	無料
10	参加募集人数	各回　最大 100 人
11	参加申込方法	個人情報保護の観点から外部 Web サイトからの直接申込みを受け付けず、関係各協力団体からメールで周知するセミナー案内文書に記述した東北経済産業局のセミナー参加申込書の URL へ、参加希望者が直接アクセスし必要事項を記入いただく。

12	参加募集方法	①東北経済産業局による案内 ②東北地域情報サービス産業懇談会（TISA）へ案内を依頼 ③MISEC からの案内（TPJC、みちのく情報セキュリティ推進センター） ④一般社団法人宮城県情報サービス産業協会（MISA）へ案内を依頼 ⑤各県商工会議所　＜青森県、岩手県、宮城県、秋田県、山形県、福島県＞ ⑥東北経済産業局からの大学向けメルマガによる案内
13	講演内容	各回の講演内容は以下のとおり
	第１回 （企業・組織のセキュリティ担当者向け及びセキュリティ技術に興味のある社会人、学生向け）	①2021 年のサイバーセキュリティ脅威動向と今求められる対策（13:35～14：20） （講師）キャノン IT ソリューションズ㈱ セキュリティ・エバンジェリスト 西浦 真一氏 ②身に迫るサイバーテロ　来るべきデジタル化の大波に備える　（14:20～15:00） （講師）株式会社サイバー・ソリューションズ 代表取締役社長 キニ・グレン・マンスフィールド氏 ③中小企業における情報セキュリティの最新動向と対策　（15:00～15:30） （講師）独立行政法人情報処理推進機構 セキュリティセンター 企画部 中小企業支援グループ 研究員 佐藤 裕一氏
	第２回 （企業・組織のセキュリティ担当者向け及びセキュリティ技術に興味のある社会人、学生向け）	①　ネット犯罪・情報漏えいの実態と対策方法について　（13:35～14：20） （講師）株式会社高山 サイバーセキュリティチームリーダー 盛 柾貴氏 ②　改正個人情報保護法とデジタル化対応　（14:20～15:00） （講師）特定非営利活動法人みちのく情報セキュリティ推進機構 情報セキュリティ推進センター センター長　小松澤 美喜夫氏 ③中小企業における情報セキュリティの最新動向と対策　（15:00～15:30） （講師）独立行政法人情報処理推進機構 セキュリティセンター 企画部 中小企業支援グループ 研究員 佐藤 裕一氏
	第３回 （経営者向け及び企業・組織のセキュリティ担当者向け）	①　社会のデジタル化とサイバーセキュリティ　（13:35～14：25） （講師）宮城県警察本部生活安全部サイバー犯罪対策課 課長補佐 五十嵐文晴氏 ②中小企業における情報セキュリティの最新動向と対策　（14:25～15:15） （講師）独立行政法人情報処理推進機構 セキュリティセンター 企画部 中小企業支援グループ 研究員 佐藤 裕一氏 ③「東北地域セキュリティコミュニティ形成促進支援事業」の紹介（15:15～15:30） （講師）特定非営利活動法人みちのく情報セキュリティ推進機構 情報セキュリティ推進センター センター長 小松澤 美喜夫氏

3.2 デジタル化・セキュリティセミナーの実施報告

デジタル化・セキュリティセミナーの実施報告は以下のとおり。

（1）第 1 回セミナーの実施報告

①実施日時　　：　令和 3 年 12 月 2 日（木）13:30～16:00
②参加申込者数　：　84 人（参加申込締切日：11 月 30 日）
③当日参加者数　：　64 人
④終了後アンケート回答者数　：　46 人（回収率 72%）

終了後に実施した第 1 回セミナーのアンケート結果は【表 3 】のとおり

（2）第 2 回セミナーの実施報告

①実施日時　　：　令和 3 年 12 月 23 日（木）13:30～15:35
②参加申込者数　：　88 人（参加申込締切日：11 月 30 日）
③当日参加者数　：　53 人
④終了後アンケート回答者数　：　40 人（回収率 75%）

終了後に実施した第 2 回セミナーのアンケート結果は【表 4 】のとおり

（3）第 3 回セミナーの実施報告

①実施日時　　：　令和 4 年 1 月 20 日（木）13:30～15:30
②参加申込者数　：　76 人（参加申込締切日：11 月 30 日）
③当日参加者数　：　43 人
④終了後アンケート回答者数　：　16 人（回収率 37%）

終了後に実施した第 3 回セミナーのアンケート結果は【表 5 】のとおり

（4）セミナーにおける相談対応内容

セミナー開催にあたって、セキュリティに関する質問事項を事前（セミナー参加申込み時）に「セキュリティに関する問合せ」として伺い、セミナー内にて回答するなどの相談対応を併せて行う事で、参加者の理解を促進することに努めた。

セキュリティに関する問合せの内容と対応状況は【表 2 】のとおりであり、セミナー参加者に共通する問合せ内容については、第 2 回セミナー終了時に主催者側（事務局）から参加者全員へ向けて回答を行った。なお、問い合わせ内容が問合せ者に限定されるものについては、後日、主催者から問合せ者宛にメールで回答を行った。

【表２】セキュリティに関する問合せの内容と対応状況

No.	問い合わせ内容	回答内容	回答方法
1	セキュリティ対策として、パソコンでワイヤーウオールを設定したり、ウイルス対策ソフトを導入するなど、パソコン本体での対策だけでは不十分で、WiFi など通信系での対策もとる必要がある、という理由と、その意味、対策と、その有効性などについて知りたいです。	パソコンのファイアウォール（パーソナルファイアウォール）の注意点は、 ①アクセス許可したサービスから感染する可能性があること。 ②OS 標準搭載のファイアウォール（WindowsDefender）では不十分な可能性もある。 また、一般的なウイルス対策ソフトは、 ③既知のウイルスに対しては最新のパターンファイルに更新していれば有効ですが、新種／亜種のウイルスなどの日々変化する攻撃に対してはまだウイルス対策ソフトが未対応であることから安全というわけではありません。 また、④従業員が不適切なウェブサイトにアクセスしたりフリーソフトをインストールしたりする行為を防ぐこともできません。 このような場合は、例えば、補完する製品として中小企業向けに安価かつ効果的な「サイバーセキュリティお助け隊」（注）が提供するパッケージサービスを導入することも 1 例としてご検討をお願い致します。 なお、その前に、本日のご講演でご説明しました基本的なセキュリティ対策（最新の OS／パターンファイルへの更新、従業員のセキュリティ教育、重要ファイルの定期的なバックアップ等）を行うことが必須であると考えます。 （注）「サイバーセキュリティお助け隊」が提供するパッケージサービスは、現在 5 サービスが提供中です。詳細は IPA のホームページをご参照ください。	セミナー終了時に回答
2	中小企業が自分事としてとらえることができるにはどうしたらよいか？ニュースでは主に大企業の事例が中心のため、どうしても身近に感じることができないのではないか。 中小企業のサイバーインシデント事例に特化した集約と発信の仕	セキュリティ対策にこれから取り組まれる中小企業向けに、独立行政法人情報処理推進機構（IPA）や警察庁において以下の資料を公表していますのでご参考にしてください。　⇒【参考１】	個別にメールで回答

	組みが構築できるとよいと考えています。		
3	私共のような公設試験研究機関の場合、機械装置を貸し出すことがありますが、試験用の機器の多くがウイルス対策ソフトの導入を勧めていない（不可の場合もある）ため、セキュリティに不安があります。 物理的に USB メモリを使用させないようにしたり、対策はしてますが、使用者のモラルに頼るしかないのが現状です。 こういった装置に対するセキュリティ対策で有効なものがあれば教えていただければ助かります。	「機械装置」が市販のサーバー、PC、タブレット、スマホ等のコンピュータである場合は、貸し出し期間中にウイルスに感染してしまう、あるいは使用者が故意に不正プログラムをインストールする、などのリスクが想定されます。その場合の対策としては以下が考えられます。 1)貸出用装置は管理者権限で使用できない状態にする（OS でアクセス権の設定が可能な場合は、システムファイルにアクセスできない、ソフトウェアをインストールできないなど制限がある一般ユーザーアカウントでログインして使用してもらう。 2)返却時に OS のクリーンインストールまたはウイルススキャン※を行う。 ※独自の不正プログラムの場合などは検知できない場合もあります。	個別にメールで回答
4	1～3 回目の IPA 講演については、内容は別になりますでしょうか。	第 1 回、第 2 回はほぼ同内容で、第 3 回は 1,2 回の内容に、経営者向け資料を加える予定です。	個別にメールで回答
5	UTM は設置しているが、その他に対策が必要なものは何でしょうか。	UTM（統合型脅威監視装置）は 1 台で最低限のセキュリティ対策が簡単に行えるメリットがあり、ネットワーク規模が小さい中小企業の場合は UTM でも十分なセキュリティ対策を行えるということが言えますが、デメリットもあり、 ①UTM だけでは有効なウイルス対策は行えない。従ってウイルス対策ソフトが必要です。 ＜例＞UTM の機能にもよりますが、UTM をすり抜けて社内の端末（パソコン）がサイバー攻撃を受けるリスクがあります。特にテレワーク等により社外のインターネット回線等を利用して業務を行う機会も増えており、この場合は UTM では脅威を除去できないことがあります。 ②多数の機能を同時に使うと性能が落ちるものがあります。 ③UTM がダウンした場合のリスクが大きい。	セミナー終了時に回答

		このような場合、デメリットを補完する対策としてサイバーセキュリティお助け隊が提供するパッケージサービスとの併用も 1 例としてご検討をお願い致します。 なお、本件につきましても、本日のご講演でご説明しました基本的なセキュリティ対策（最新の OS／パターンファイルへの更新、従業員のセキュリティ教育、重要ファイルの定期的なバックアップ等）を行うことが必須であると考えます。	
6	中小企業において必ず行うべきセキュリティ施策に関して伺いたい。	以下の資料の中で必ず実施すべき基本的対策として、独立行政法人情報処理推進機構（IPA）において「情報セキュリティ 5 か条」を公表していますのでご参考にしてください。　⇒【参考 2】	個別にメールで回答
7	他社でどのようなセキュリティ対策をしているか、事例があれば紹介してほしい。	他社様のセキュリティ対策事例をそのままご紹介することは難しいため、独立行政法人情報処理推進機構（IPA）や警察庁において以下の資料を公表していますので、ご参考にしてください。 ⇒【参考 1】	個別にメールで回答

【参考 1】
IPA「中小企業の情報セキュリティ対策ガイドライン」
https://www.ipa.go.jp/security/keihatsu/sme/guideline/
（中小企業にも被害が及んでいることが解る資料）
IPA「中小企業におけるセキュリティ対策状況等の実態把握」
https://www.ipa.go.jp/security/fy2020/reports/sme/otasuketai_houkoku.html
警察庁「サイバー空間をめぐる脅威の情勢等」
https://www.npa.go.jp/publications/statistics/cybersecurity/index.html

【参考 2】
IPA「中小企業の情報セキュリティ対策ガイドライン」
https://www.ipa.go.jp/security/keihatsu/sme/guideline/
情報セキュリティ 5 か条
https://www.ipa.go.jp/files/000055516.pdf

【表３】第１回セミナーアンケート結果

項目番号	調査事項	回答内容	回答数	比率
１．本セミナー全般について				
1-1	本セミナー参加の目的について、お尋ねします。 該当するものを選択してください。	①自社のデジタル化・セキュリティ対策のための情報収集	36	78.3%
		②販売等、顧客のための情報収集	4	8.7%
		③支援機関としての情報収集	3	6.5%
		④教育・研究機関としての情報収集	3	6.5%
		⑤その他	0	0.0%
		⓪ 無回答	0	0.0%
		計	46	100.0%
1-2	本セミナーに対する満足度について、お尋ねします。 該当するものを選択してください。	①満足	8	17.4%
		②やや満足	16	34.8%
		③普通	17	37.0%
		④やや不満	5	10.9%
		⓪ 無回答	0	0.0%
		計	46	100.0%
２．本セミナーの講演内容について				
2-1	【講演１】の理解度について、お尋ねします。 該当するものを選択してください。	①十分に理解できた	12	26.1%
		②理解できた	31	67.4%
		③あまり理解できなかった	3	6.5%
		④理解できなかった	0	0.0%
		⓪ 無回答	0	0.0%
		計	46	100.0%
2-2	【講演２】の理解度について、お尋ねします。 該当するものを選択してください。	①十分に理解できた	7	15.2%
		②理解できた	32	69.6%
		③あまり理解できなかった	6	13.0%
		④理解できなかった	1	2.2%
		⓪ 無回答	0	0.0%
		計	46	100.0%
2-3	【講演３】の理解度について、お尋ねします。 該当するものを選択してください。	①十分に理解できた	15	32.6%
		②理解できた	29	63.0%
		③あまり理解できなかった	2	4.3%
		④理解できなかった	0	0.0%
		⓪ 無回答	0	0.0%
		計	46	100.0%

【表４】第２回セミナーアンケート結果

項目番号	調査事項	回答内容	回答数	比率
１．本セミナー全般について				
1-1	本セミナー参加の目的について、お尋ねします。 該当するものを選択してください。	①自社のデジタル化・セキュリティ対策のための情報収集	29	72.5%
		②販売等、顧客のための情報収集	2	5.0%
		③支援機関としての情報収集	5	12.5%
		④教育・研究機関としての情報収集	3	7.5%
		⑤その他	1	2.5%
		⓪ 無回答	0	0.0%
		計	40	100.0%
1-2	本セミナーに対する満足度について、お尋ねします。 該当するものを選択してください。	①満足	2	5.0%
		②やや満足	17	42.5%
		③普通	15	37.5%
		④やや不満	4	10.0%
		⑤不満	2	5.0%
		⓪ 無回答	0	0.0%
		計	40	100.0%
２．本セミナーの講演内容について				
2-1	【講演１】の理解度について、お尋ねします。 該当するものを選択してください。	①十分に理解できた	15	37.5%
		②理解できた	25	62.5%
		③あまり理解できなかった	0	0.0%
		④理解できなかった	0	0.0%
		⓪ 無回答	0	0.0%
		計	40	100.0%
2-2	【講演２】の理解度について、お尋ねします。 該当するものを選択してください。	①十分に理解できた	7	17.5%
		②理解できた	23	57.5%
		③あまり理解できなかった	9	22.5%
		④理解できなかった	1	2.5%
		⓪ 無回答	0	0.0%
		計	40	100.0%
2-3	【講演３】の理解度について、お尋ねします。 該当するものを選択してください。	①十分に理解できた	14	35.0%
		②理解できた	24	60.0%
		③あまり理解できなかった	2	5.0%
		④理解できなかった	0	0.0%
		⓪ 無回答	0	0.0%
		計	40	100.0%

【表５】第３回セミナーアンケート結果

項目番号	調査事項	回答内容	回答数	比率
１．本セミナー全般について				
1-1	本セミナー参加の目的について、お尋ねします。 該当するものを選択してください。	①自社のデジタル化・セキュリティ対策のための情報収集	13	81.3%
		②販売等、顧客のための情報収集	3	18.8%
		③支援機関としての情報収集	0	0.0%
		④教育・研究機関としての情報収集	0	0.0%
		⑤その他	0	0.0%
		⓪ 無回答	0	0.0%
		計	16	100.0%
1-2	本セミナーに対する満足度について、お尋ねします。 該当するものを選択してください。	①満足	7	43.8%
		②やや満足	4	25.0%
		③普通	5	31.3%
		④やや不満	0	0.0%
		⑤不満	0	0.0%
		⓪ 無回答	0	0.0%
		計	16	100.0%
２．本セミナーの講演内容について				
2-1	【講演１】の理解度について、お尋ねします。 該当するものを選択してください。	①十分に理解できた	7	43.8%
		②理解できた	8	50.0%
		③あまり理解できなかった	1	6.3%
		④理解できなかった	0	0.0%
		⓪ 無回答	0	0.0%
		計	16	100.0%
2-2	【講演２】の理解度について、お尋ねします。 該当するものを選択してください。	①十分に理解できた	6	37.5%
		②理解できた	9	56.3%
		③あまり理解できなかった	0	0.0%
		④理解できなかった	1	6.3%
		⓪ 無回答	0	0.0%
		計	16	100.0%
2-3	【講演３】の理解度について、お尋ねします。 該当するものを選択してください。	①十分に理解できた	4	25.0%
		②理解できた	8	50.0%
		③あまり理解できなかった	3	18.8%
		④理解できなかった	1	6.3%
		⓪ 無回答	0	0.0%
		計	16	100.0%

（５）第１回～第３回のセミナー開催におけるアンケート結果からの総括

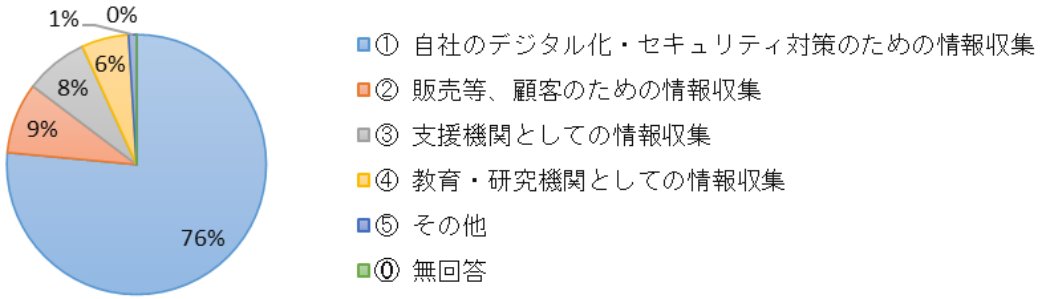
第１回セミナーから第３回セミナーの開催における終了後のアンケート結果を取りまとめると【グラフ１】、【グラフ２】、【グラフ３】のとおりである。

本セミナー参加の目的については、「自社のデジタル化・セキュリティ対策のための情報収集」が多数（76%）であり、本セミナーの開催目的を理解いただけたものと評価する。

本セミナーに対する満足度については、「満足」、「やや満足」を合わせると半数を超え（53%）、概ね評価が良かったと考える。

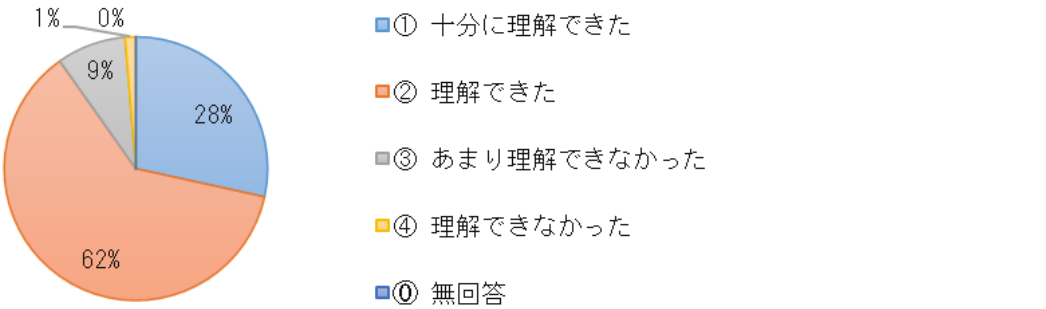
また、講演１から講演９の理解度について総合すると、「十分理解できた」と「理解できた」を合わせると90%であり、総じて各講演内容については理解をいただけたものと評価する。

【グラフ１】　本セミナー参加の目的について



【グラフ２】　本セミナーに対する満足度について

【グラフ３】　【講演1～９(総合)】の理解度について



また、自由記述でいただいた「今後開催希望するセミナー」と「意見・要望」を取りまとめると以下のとおりである（実際に記入された内容を編集し、趣旨を提示した）。

①今後開催希望するセミナー

・最新のサイバーセキュリティについて（他、同様な希望内容　5 件）
・具体的な対策事例や有効な対策商品について（他、同様な希望内容　5 件）
・個人情報保護法改正に伴う対策について（他、同様な希望内容　3 件）
・中小企業でも導入可能なセキュリティ対策について（他、同様な希望内容　1 件）
・身近なところでのヒヤリハット事例について（他、同様な希望内容　1 件）

②意見・要望

・講演資料の配布を希望する（他、同様な希望内容　6 件）
・講演途中での音声・映像の停止トラブルがあった（他、同様な指摘内容　5 件）

「今後開催を希望するセミナー」については、法律改正等の時期に合わせたタイムリーな講演テーマであることや、スタンダードな講演テーマ（最新のサイバーセキュリティ）が求められていると理解する。

４．セキュリティ対策支援モデル事業の実施

４.１ セキュリティ対策支援モデル事業の実施概要

「２.デジタル化・セキュリティに関する状況・意識調査の実施」におけるアンケート調査結果を踏まえ、情報セキュリティ対策に前向きな企業（モデル企業）を３社選定し、情報セキュリティの向上に向けてハンズオンでのアドバイスを行い、本取組みを事例化し「３.デジタル化・サイバーセキュリティセミナーの開催」における第３回セミナーの最終講演である「『東北地域セキュリティコミュニティ形成促進支援事業』の紹介」において発信した。

（１）モデル企業の選定方法

セキュリティ対策支援モデル事業のモデル企業の選定は以下の２段階の方法で行い、最終的に３社を選定した。

①モデル企業候補企業の選定

アンケート調査結果において、個別指導に関心があり、情報セキュリティ対策に前向きで以下の対応が必要なモデル企業候補企業として 10 社を選定した。

・近々にセキュリティ対策を導入予定であるが相談相手がいない。
・プライバシーマークや ISMS（ISO27001）の認証取得を行いたいが、適当なコンサルサル会社がいない。
・既にセキュリティ対策製品を導入しているが、問題・課題がある。等

②モデル企業の選定

上記のモデル企業候補企業（10 社）から以下の取組状況である企業を優先的に電話連絡により意向を確認し、モデル企業（3 社）を決定した。

・自社のセキュリティポリシーが未策定または策定中
・SECURITY ACTION 制度を知らない。

（２）モデル企業の概要及びセキュリティ対策の取組状況

選定したモデル企業３社の概要及びセキュリティ対策の取組状況は、アンケート回答内容から以下のとおりである。詳細を【表６】に示す。

①モデル企業３社の業種は「不動産業」、「宿泊・飲食サービス業」、「卸売・ 小売業」と区々であり、従業員数も「5 人以下」、「11～20 人」、「21～50 人」 と区々である。
②デジタル化の進捗状況については、「ある程度進んでいる(Web 会議の導入、給与計算、受発注、勤怠管理等一部の業務プロセス(生産プロセスを除く)の効率化)」は１社のみであり、他の２社は「あまり進んでいない(E-mail、表計算ソフト等の導入程度)」という状況である。
③セキュリティポリシーの策定状況については、「現在、策定中」は１社であり、他の２社は「策定していない」。
④「SECURITY ACTION」の取組状況については、３社とも「制度を知らない」という状況である。

【表６】モデル企業の概要及びセキュリティ対策の取組状況

	モデル企業名（仮称）	A社	B社	C社
1-1	従業員数	5人以下	11～20人	21～50人
1-2	業種	不動産業	宿泊・飲食サービス業	卸売・小売業
2-1	デジタル化の進捗状況	あまり進んでいない(E-mail、表計算ソフト等の導入程度)	ある程度進んでいる (Web会議の導入、給与計算、受発注、勤怠管理等一部の業務ﾌﾟﾛｾｽ(生産ﾌﾟﾛｾｽを除く)の効率化)	あまり進んでいない (E-mail、表計算ソフト等の導入程度)
2-5	テレワークのシステムの導入状況	導入していない	導入している	導入していない
2-13	従業者に対する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	行っていない	IT関連業務の担当者、管理職、経営者（役員含む）	管理職
4-1	セキュリティポリシーの策定状況	策定していない	現在、策定中	策定していない
4-7	SECURITY ACTIONの取組状況	制度を知らない	制度を知らない	制度を知らない
4-8	情報セキュリティに関する外部認証の取得状況	無回答	プライバシーマーク取得準備中	その他
8-1	情報セキュリティ対策について分からないこと、相談してみたいこと	セキュリティ・インシデント等全くわからない状態です。	－	セキュリティ対策としてUTMの導入、コピー機を情報漏洩対策済みのものに変えていますが、それ以上の対策は何か必要でしょうか？

（３）モデル企業へのアドバイス内容

選定したモデル企業へのアドバイスは１社あたり３回程度（うち、２回は訪問により実施。その他に電話・メールで実施）、ハンズオンでのアドバイス（個別アドバイス）を行うこととした。また、個別アドバイスを受けることでモデル企業は、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」制度の一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。個別アドバイスの実施プロセスは【図 1】のとおりである。

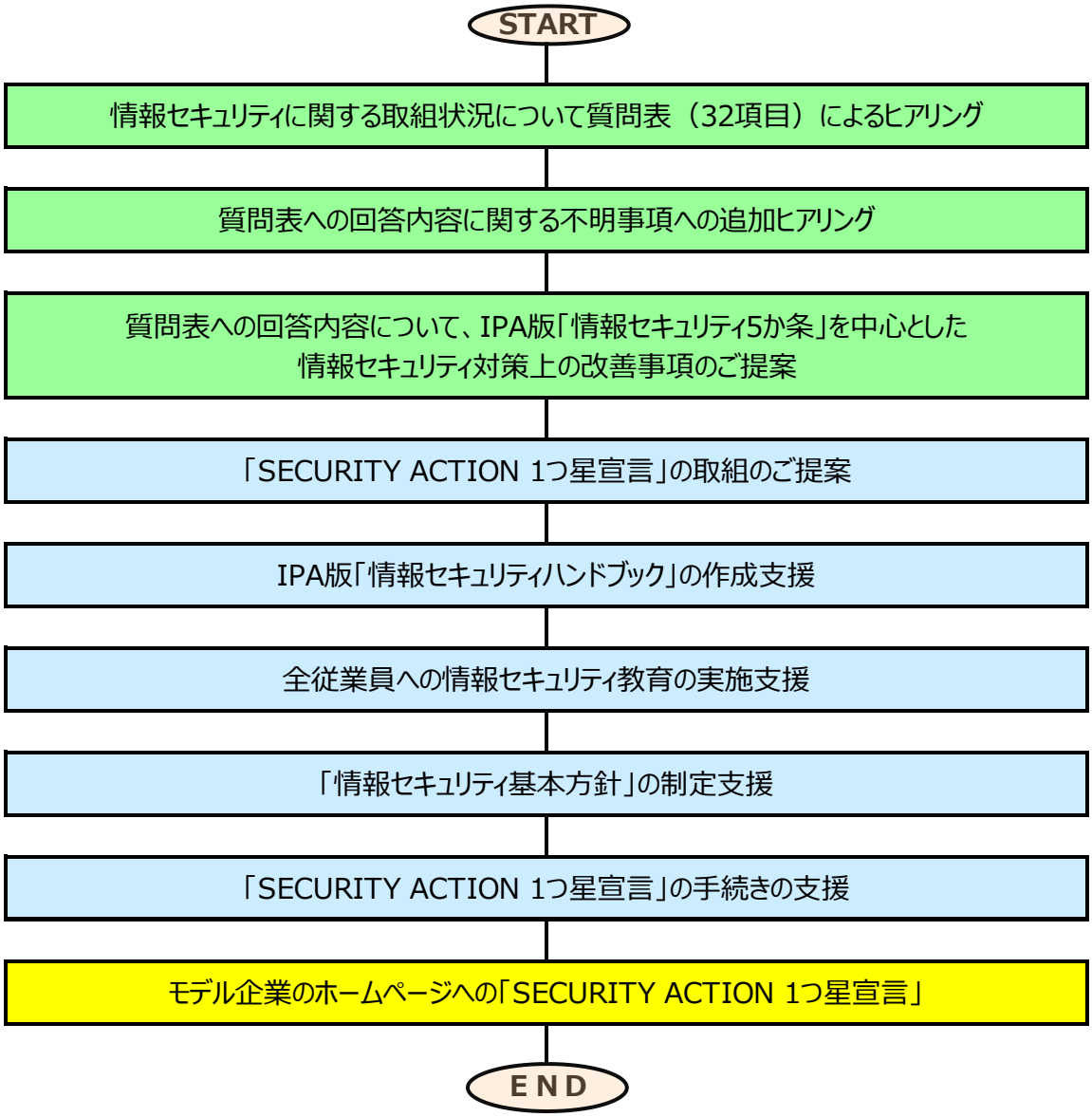


図１．モデル企業への個別アドバイスの実施プロセス

４.２ 個別アドバイスの実施結果

モデル企業（A 社・B 社・C 社）の 3 社へ個別アドバイスを実施し、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（改善事項）を検討し、「改善案」として提案した。

3 社の業種は異なり、いずれも比較的小規模な事業者ではあるが、経営トップが高いセキュリティ意識を持っていたことから、3 社とも個別アドバイスを受け入れ、これまでのセキュリティ対策状況は異なるものの、何れも改善案を反映した各社版「情報セキュリティハンドブック」を作成した。

IPA 版「情報セキュリティ 5 か条」及び、各社版「情報セキュリティハンドブック」を主な研修教材として全従業員を対象にした「情報セキュリティ研修」を初めて実施し、合わせて「情報セキュリティ基本方針」も策定することにより、早期の「SECURITY ACTION 一つ星」宣言を行う方針で取り組むこととなった。

モデル企業各社の課題とその対応方針の概要については、【表 7 】のとおりである。

４.３ 今後に向けた対策

モデル企業 3 社は、経営トップが高いセキュリティ意識を持っていたことから、3 社とも各社版「情報セキュリティハンドブック」を作成し、全従業員を対象にした「情報セキュリティ研修」を初めて実施し、「情報セキュリティ基本方針」も策定を完了し、現在、「SECURITY ACTION 一つ星」宣言を行う手続きを実施中であるため、ホームページへ「SECURITY ACTION 一つ星」を掲載するまでフォローアップを行う必要がある。

また、その後の効果的な支援は各モデル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、地域セキュリティコミュニティに積極的に参加いただき、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、A 社の社長には、地域の不動産業の団体に対しても情報セキュリティ向上のための知識とノウハウを提供することも効果的との要望を受けており、業界に特化したセミナーや勉強会の企画も必要と考える。

【表７】モデル企業各社の課題とその対応方針

モデル企業名	課　題	対応方針
Ａ社 （不動産業） （従業員 5人以下）	・セキュリティポリシーを策定していない	・「情報セキュリティ5か条」（ＩＰＡ版）を順守する。 ・「情報セキュリティハンドブック」を策定する。 ・「情報セキュリティ基本方針」を制定する。
	・従業員に対するサイバーセキュリティに関する注意喚起や指示・指導を行っていない。	・システム担当者（セキュリティ担当者を兼務）を定め、毎週月曜に全従業員へ周知する。（情報セキュリティハンドブックへ規定）
	・従業員から入社時に守秘義務を規定した誓約書を受領していない。	・全従業員から誓約書を取得する。
	・事務所の入退室の管理を行っていない。	・新たに「入退室管理簿」を作成し、入退室時に記入する。
	・緊急事態が発生した際の連絡先が明確でない。	・緊急時連絡先一覧を作成し明確化する。
	・重要書類を保管する書庫が施錠されていない。	・外出時や退社時には、重要書類を格納した社長管理の書庫を施錠する。
	・ＵＳＢメモリを外部に持ち出す場合がある。	・ＵＳＢメモリを外部に持ち出す場合に備えて、ＵＳＢメモリを暗号化する。
	・パソコンのシステムファイルやデータファイルのバックアップを行っていない。	・外付けハードディスクを2台調達し、週1回バックアップを実施する。
	・従業員に対する情報セキュリティ教育を実施していない。	・定期的に全従業員（年1回以上）を対象に「情報セキュリティ5か条」（ＩＰＡ版）と「情報セキュリティハンドブック」をテキストにして情報セキュリティ教育を行う。
Ｂ社 （宿泊・飲食 サービス業） （従業員 11～20人）	・セキュリティポリシーを策定予定も未だ策定していない	・「情報セキュリティ5か条」（ＩＰＡ版）を順守する。 ・「情報セキュリティハンドブック」を策定する。 ・「情報セキュリティ基本方針」を制定する。
	・プライバシーマーク取得準備中も未だ具体的に着手していない。	・先行して「SECURITY ACTION 一つ星」を宣言する。 ・プライバシーマークの取得に着手する際に別途連絡をいただく。
	・従業員から入社時に守秘義務を規定した誓約書を受領していない。	・全従業員から誓約書を取得する。
	・事務所の入退室の管理を行っていない。	・新たに「入退室管理簿」を作成し、全館不在時の入退室時に記入する。
	・ＵＳＢメモリを使用している（外部への持ち出しはしない）。	・ＵＳＢメモリを適切に管理するとともに、外部に持ち出す場合に備えて、ＵＳＢメモリを暗号化する。
	・従業員のパソコンのシステムファイルやデータファイルのバックアップを行っていない。	・外付けハードディスクへ週1回バックアップを2世代管理で実施する。
	・従業員に対する情報セキュリティ教育を実施していない。	・定期的に全従業員（年1回以上）を対象に「情報セキュリティ5か条」（ＩＰＡ版）と「情報セキュリティハンドブック」をテキストにして情報セキュリティ教育を行う。
Ｃ社 （卸売・ 小売業） （従業員 21～50人）	・セキュリティポリシーを策定していない	・「情報セキュリティ5か条」（ＩＰＡ版）を順守する。 ・「情報セキュリティハンドブック」を策定する。 ・「情報セキュリティ基本方針」を制定する。
	・ホームページにプライバシーポリシーを宣言しているがプライバシーマークを取得していない。	・先行して「SECURITY ACTION 一つ星」を宣言する。 ・プライバシーマークを取得する際に別途連絡をいただく。
	・事務所の入退室の管理を行っていない。	・新たに「入退室管理簿」を作成し、入退室時に記入する。
	・ＵＳＢメモリを使用している（外部への持ち出しはしない）。	・ＵＳＢメモリを適切に管理するとともに、外部に持ち出す場合に備えて、ＵＳＢメモリを暗号化する。
	・ＵＴＭを昨年度導入し、ＮＴＴ東日本のウイルス対策ソフトも導入しているが、監視、駆除・対策サポート等が含まれていない。	・ウイルス感染時等のパソコン等不具合発生時にパソコン購入先に相談し対応が可能とのことであるが、対応ができない場合はウイルス対策ソフトの契約内容を見直す必要がある。
	・従業員のパソコンのシステムファイルやデータファイルのバックアップを外付けハードディスクに自動で行っているが、事務所の机の下に置かれたままである。	・外付けハードディスクを施錠管理可能なキャビネット内へ置く。
	・従業員に対する情報セキュリティ教育を実施していない。	・定期的に全従業員（年1回以上）を対象に「情報セキュリティ5か条」（ＩＰＡ版）と「情報セキュリティハンドブック」をテキストにして情報セキュリティ教育を行う。

５．地域セキュリティコミュニティのあり方に関する考察と提言

中小企業は、令和 2 年度から続く新型コロナウイルス対策の対応により、テレワーク等業務のデジタル化を急速に進める中、情報漏洩やサイバー攻撃の脅威等といった潜在リスクが増大してきている。

このような中、中小企業が、デジタル化によるリスクに対応しつつ、その恩恵を享受するためには、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が急務となっているが、中小企業自らが有効な情報セキュリティ対策やサイバーセキュリティ対策を行うことは人材面及び要員面から困難な状況であり、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、本事業では地域に根付いたセキュリティコミュニティの形成に向けて、中小企業のセキュリティ対策に関する意識・知識の向上、人材育成、関係者間の情報共有の強化を目指すこととし、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。

- デジタル化・セキュリティに関する状況・意識調査（アンケート調査）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
- デジタル化・セキュリティセミナーの参加者による事前質問から得られた企業等の疑問点
- セキュリティ対策支援モデル事業で実施した個別アドバイス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（（例）商工会議所、TISA 、MISA、テレコムサービス協会）、経済団体（東北経済連合会）、大学（（例）東北大学）等の教育機関、研究機関、国関係機関（（例）経済産業省、総務省）、自治体、県警（（例）宮城県警）、IT 系コミュニティ（（例）MISEC、仙台 CTF）などが、サイバーセキュリティに関する啓発、情報共有、人材育成を目的としたセミナーや研修・演習を実施している。

このような中、令和 3 年 10 月には東北経済産業局と東北総合通信局が事務局となって「東北地域サイバーセキュリティ連絡会」が発足し活動を開始し、東北地域においてもセキュリティコミュニティの中核が形成されたものと考える。

しかし、様々な脅威や脆弱性が高度化する昨今、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、まだまだ少ないのではないかと考える。

そこで、「東北地域サイバーセキュリティ連絡会」を中核にして地域に根付いたセキュリティコミュニティ（以下、上記関連団体及び「東北地域サイバーセキュリティ連絡会」を総称して「セキュリティコミュニティ」と略記）となるためには、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または業種に対するサポートが必要と考えており、そのような企業または業種に対するセキュリティ意識の向上と人材育成、情報共有をセキュリティコミュニティの役割としてはいかがかと思う。

そのセキュリティコミュニティの構成と各組織の役割については、【図２】のように考える。

中小企業にとって身近な IT 関連企業及び IT 系コミュニティが「東北地域サイバーセキュリティ連絡会」と連携して中心となり活動することがセキュリティ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、必要に応じて他の組織と連携することで、参加者が増えたり、活性化につながるものと考える。

なお、セキュリティコミュニティの継続性のためには、中心となり活動する IT 関連企業及び IT 系コミュニティに対して活動資金の援助が必須であると考える。特に IT 系コミュニティに所属する活動メンバーはボランティア的に活動する場合が多く、活動資金不足から十分な活動が行えない実態がある。

また、セキュリティコミュニティが開催するセミナーや研修等の参加者には、地域の中小企業だけではなく、大学などの学生も参加できるように連絡体制を整備すれば、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ものと考える。

「東北地域サイバーセキュリティ連絡会」には、国や他の地域のサイバーセキュリティ連絡会・協議会と連携を密にされ、最新のサイバーセキュリティ対策セミナー等を定期的に開催するなどサイバーセキュリティに関する最新情報等の提供活動を期待したい。また、東北地域の多くの中小企業に本セキュリティコミュニティの認識をしてもらうために、特に東北各県の商工会議所内に各県支部を置く等の対応により連携を太くすることにより、多くの中小企業がサイバーセキュリティに対する意識の向上及び人材育成が可能となる様、積極的な取組みを期待したい。

以上

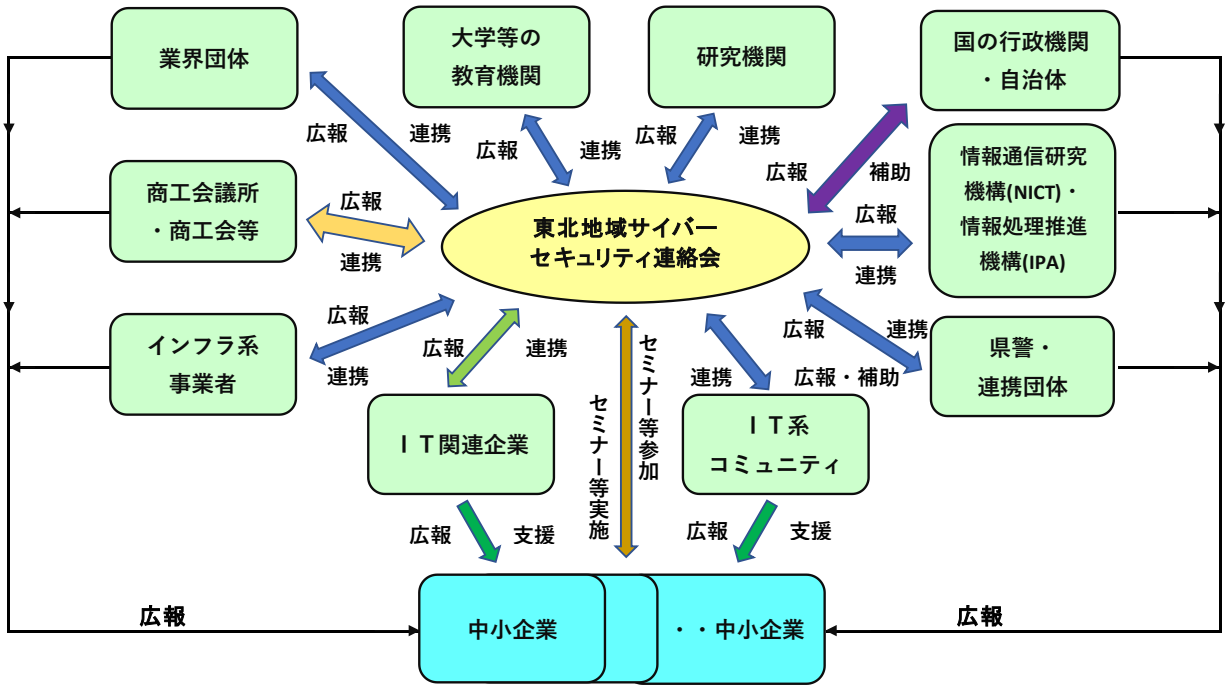


図２． セキュリティコミュニティの構成と各組織の役割