四国経済産業局　御中

「令和３年度四国地域の中小企業サイバーセキュリティ対策促進事業」
調査報告書（公表用）

令和４年２月 28 日

株式会社ＩＴブレイン

目次

1　始めに

近年、サプライチェーン全体で対策が不十分な中小企業を対象とするサイバー攻撃により、それらの中小企業とサプライチェーンを共有する大企業等への影響が顕在化してきており、中小企業のサイバーセキュリティ対策は喫緊の課題となっている。

令和２年度に経済産業省で実施した「サイバーセキュリティお助け隊」の実証事業の中でも、四国内の中小企業において、業種や規模を問わず例外なくサイバー攻撃を受けている一方で、セキュリティ対策にかける問題意識や対策が十分でないという実態が明らかになった。

また、昨今の新型コロナウイルス感染症の影響により、中小企業においてもテレワークの導入が広まる中、混乱に乗じてランサムウェアや不正アプリ等による攻撃が海外を中心に増加しており、中小企業へのサイバー攻撃を通じたサプライチェーン全体への脅威は増大している。

中小企業におけるサイバーセキュリティの取組は、我が国の産業に対する世界の信頼に直結する重要な課題であり、サイバーセキュリティ対策強化を中小企業・地域まで展開していく必要がある。

特に四国地域においては、中小企業等が有効なサイバーセキュリティ対策をとるための情報共有等の枠組みが不足しているため、地域に根付いたサイバーセキュリティに関するコミュニティ（以下「地域 SECUNITY」と呼ぶ。）を形成して、情報共有等を強化していくことが重要である。

そこで、本事業では、四国地域の関係機関等と連携して地域 SECUNITY の形成を促進し、サイバーセキュリティに関する施策の普及や情報共有等を支援するため、以下に示す通り、四国地域の産・官・学・コミュニティより招いたセキュリティ関連の関係者による地域 SECUNITY の形成・継続・発展に関する意見交換会（以下、「四国地域の中小企業サイバーセキュリティ関係者会議」と呼ぶ。）を企画・実施するとともに、会議内容を踏まえた形で中小企業向けのサイバーセキュリティセミナー及びセキュリティ相談会を開催した。

なお、本事業は、昨年度愛媛県を中心として実施された令和２年度中小企業サイバーセキュリティ対策推進事業（地域 SECUNITY 形成促進事業）を継承する形で、徳島県を中心に実施した。

2　四国地域の中小企業サイバーセキュリティ関係者会議委員の選定とヒアリング調査

2.1　四国地域の中小企業サイバーセキュリティ関係者会議委員の選定

四国地域の中小企業サイバーセキュリティ関係者会議を行うにあたり、四国地域の中小企業サイバーセキュリティ関係者会議委員（以下「委員」と呼ぶ）を選定するため、徳島県を中心に四国地域の民間団体・企業、教育機関、地方自治体、国の機関等のセキュリティノウハウ・スキルを持ったキーパーソンや、継続的に四国地域内で地域セキュリティコミュニティの活動をしている人材等を抽出し、その中から、四国経済産業局との協議の上、以下のヒアリング調査をおこなえた９名を委員として選定した。

2.2　ヒアリング調査の実施概要

委員選定にあたり、実施したヒアリング調査方法は以下の通りである。

(1) 委員の経歴並びに定見のヒアリング調査

主に徳島県の機関を中心に継続的に人材育成や情報提供等の対外的活動を行っている官公庁、大学・高専等の教育者、企業従業者および既存コミュニティから候補者を絞り、直接電話で本事業の趣旨を説明するとともに、委員就任承諾を得られた方の経歴並びに中小企業のサイバーセキュリティ対策に関する定見についてヒアリング調査を行った。

(2) ヒアリング調査方法

事前に調査ポイントを定め電話にてヒアリングを実施した。調査ポイントは以下の通りである。

尚、調査は、令和 3 年 10 月 21 日～10 月 29 日に実施した。

1）. 経歴

1）-1 氏名、所属組織、所属部署、役職／職種 等

1）-2 情報セキュリティに関するご自身の経歴・情報セキュリティに関する業務・活動・研究等

2）. 中小企業支援についての分析・考察

2）-1 中小企業の課題

2）-2 有効な支援策

3）. 地域コミュニティに対する意識・意見等

2.3 ヒアリング調査結果

(1) 委員の経歴

委員は、『サイバーセキュリティシンポジウム道後』 実行委員の方をはじめ、中小企業ＤＸ化支援に携わる方、サイバーセキュリティ講師経験者、セキュリティ勉強会開催者やサプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）会員の組合団体メンバー等で構成した。

(2) 中小企業支援についての分析・考察について

徳島県のサイバーセキュリティ被害報告は現時点では無いが、セキュリティ対策をしっかり行うにはコストと手間暇がかかることをしっかり認識してもらう必要があり、セミナーなどで経営者層を啓蒙する必要があるので、徳島県に特化した身近で身につまされるセミナー内容にすることで、危機感を感じてもらうことが出来ると考えている。

また、困った時に対応すれば良いという意識が強く、セキュリティに対して関心が低い。その中でどの様にセキュリティ対策を意識付けするかが課題である。ただ、サプライチェーンを組んだ中小企業を起因とした大企業へのセキュリティ事故が発生すると、多額の損害賠償を求められ小規模な会社は存続に関わる事態になりうるので、セキュリティ対策とリスク移転が必要になっているなどの認識であった。

他に参考となる意見として、以下を提示する。

- 中小企業はセキュリティに向ける人的余力がない。このため自社のネットワークやファイルサーバなどのインフラ構

築についても業者まかせになっており、自社にどの様な脆弱性があるかチェックできる体制がない。この中でどの様にしてセキュリティを確保するかが課題になっている。

- セキュリティは人に依存する部分が多いので、e ラーニングや IPA 教材などを活用することで、社員教育が徹底できるのではないかと考えている。

(3) 地域コミュニティに対する意識・意見等について

地域コミュニティは年 1 回だけの活動だけではなく、年間を通じて活動することでコミュニティの醸成を図る必要があると考えている。定期的な開催(例えば月、週、曜日を固定)で活動を行い、出席を強制しない会議にすれば集まりやすいのではと考えられ、活動を四国全域でセミナー開催するなど活動を広げていく必要もある。中小企業の経営者にターゲットを絞った啓蒙活動をすることで、危機意識を持ってもらえ、コミュニティへの参加意欲を作ることが出来るのではないかと考えている。また、相談についてはハードルを低くし、気軽に相談に行けるという雰囲気つくりも大切で、特に情報関連は専門知識を要するが、専門用語を使わないで、わかりやすく説明するような心がけが必要であるとの意見であった。

コミュニティでは年齢に関係なく理解できるよう、専門用語を翻訳して説明できる場にするのが大事だと考えるとの意見もあった。その他、コミュニティのあるべき姿に関して参考になる意見を以下に提示する。

- コミュニティを一から作っても維持が難しいと考え、業界団体、中央会、商工会議所、同友会など既存のコミュニティを元に広めてゆくことで定着させることが出来ると考える。集まった人の中でセキュリティに関心の高い人達でコミュニティを深めて行くようにした方が良い。
- コミュニティは信頼関係の中で地元貢献の活動にするなど、気軽に相談できる場にすることが大事である。
- コミュニティ費用捻出についてはボランティア精神と例えば謝金を不要とする県警などにセミナー講師を依頼するなど工夫が必要であると考える。
- コミュニティではセミナーで関心を持ってもらったうえ、セミナーだけではイメージが湧きにくいのでロールプレイングの様な実技をすることで、参加者がセキリティを実感できるようにする工夫が必要である。
- 会議をオンライン開催して時間を節約するのは参加の障壁をなくすのでいい方策だと思う。ただ中小企業の中には Web 会議に慣れていない、あるいは企業によってはまだ電話と FAX を活用している所もあり、難しい面もある。安価な Web 会議専用端末などが出てくれば、その障壁も低くなるのではと考える。

3　第１回_四国地域の中小企業サイバーセキュリティ関係者会議

選定した９名の委員による「第１回_四国地域の中小企業サイバーセキュリティ関係者会議」をオンラインで開催し、セキュリティ意識向上の施策、本事業の一環で開催するサイバーセキュリティセミナー内容と講師並びにセキュリティ相談会の開催、およびコミュニティを継続させる方策についての意見を交換した。

3.1　会議概要

- 目 的：

地域 SECUNITY の形成及び、中小企業サイバーセキュリティに関する施策の普及・情報共有等を促進する

ため、四国地域の関係機関等と連携した意見交換会を実施する。

- 日 時：令和３年 11 月４日（木）15：00～16：00
- 場 所：オンライン会議(Web-EX Meetings)
- 会議メンバー：

  下記関係機関等所属の委員９名（順不同、所属組織名のみ記載）

  ・四国総合通信局 情報通信部
  ・徳島県 商工労働観光部
  ・徳島県警察本部 生活安全部生活環境課
  ・四国ＩＴ 協同組合 四国各県代表者
  ・徳島県ＩＴコーディネーター
  ・阿南工業高等専門学校
- オブザーバー：

  ・四国経済産業局 地域経済部 製造産業・情報政策課
- ファシリテーター（進行）：

  ・株式会社ＩＴブレイン

3.2 会議内容

3.2.1「セキュリティ意識向上の施策に関する意見交換」

中小企業のセキュリティ意識向上の施策についての意見は以下のような内容であった。

徳島県内の中規模病院で発生したランサムウェア攻撃があり（令和３年 10 月 31 日）、８万件以上のデジタルカルテが暗号化された。報道どおり、バックアップデータも含め暗号化されたため、業務に大きな支障がでているとのことで、サイバー攻撃に対しての注意喚起が出されているとの話があった。

これに関係して、身近でサイバー攻撃の事故が発生すると、無関心な人も真剣に考えるようになる。サイバー攻撃に対する完全なる防御策はないので、復旧の方を早急に考えたほうがよい。セキュリティ対策は無いものという観点での事後対応が必要となるとの意見がでた。一方、原因の９割は人為的なもので、人がある程度の事をやれば防御できるので定期的な勉強は必要である。また、標的型メール訓練を試しにやってみるなど、疑似体験も必要であり、経験しないと改善されないとの意見もあった。他に参考となる意見として、以下を提示する。

- セキュリティという観点ではないが、補助金融資を行っているなかで、セキュリティ以前に企業間でのＤＸ、ＩＴの格差がひろがっていると感じている。セキュリティ対策は導入してもらう価値があるので、これからは、最初からセキュリティ対策も含め進めていく。
- 顧客からセキュリティについての相談を受けることがあるのだが、普段から意識しておらず、被害にあってから困って相談にくるのが実態である。UTM を導入しているが置いてあるだけで活用はしていないとか、リテラシーがないのでパソコンの Windows アップデートもしたことがないというのが現状である。

3.2.2「セミナーの内容と講師、並びにセキュリティ相談会に関する意見交換」

ランサムウェア攻撃が頻繁に行われている事実を中小企業に認識してもらうことが必要である。被害を受けた病院

の話をしてもらうことで、参加者の危機意識を高めることが出来る等の意見が出された。また、セキュリティ啓発については、民間からではなく公的な組織から発信してもらったほうがよく、県警から話してもらうと効果が大きいなどの意見が出され、上記「セキュリティ意識向上の施策に関する意見交換」の内容も踏まえて、実施予定のサイバーセキュリティセミナー内容と講師およびアンケートについての方向性を得ることができた。

3.2.3「コミュニティを継続させる方策に関する意見交換」

『サイバーセキュリティシンポジウム道後』では、最先端のメンバーが集まっており、地域への恩恵として、一般向けのサブプログラムもある。現時点でいまだセキュリティのコミュニティは形成手前の段階であり、広める手立てとしては啓蒙活動を続けていくことが肝要である。啓蒙活動としては、４県ともバックグラウンドは県警とし、ＩＴ技術者とセキュリティ対策の必要性を一般向けに説明する説明者が要る。技術者だけだとどうしても話が難しくなるので専門用語を使わない説明者が必要である。などの意見が発せられた。その他としては、セキュリティについて相談先がわからないため、困った時に的はずれな人に相談して、適切なセキリティ対策の対応がなされていないというケースが散見されるため、相談できる窓口が継続的にないといけないので、公的なしっかりとした窓口が必要だと考えるなどの意見もあった。

3.3　会議総括

偶然にも、徳島県の病院でランサムウェア被害が発生し、ニュース等で大きく取り上げられた。身近でサイバーセキュリティ事故が発生すると、危機感が高まり、このようなランサムウェア攻撃が頻繁に行われている事実を中小企業に認識してもらいやすくなると考えられる。実際の被害に関連した話題を挙げることで、参加者の危機意識を一層高めることが出来る等の意見が出されたので、12 月中旬実施予定のセミナー企画については、訴求性の高い方向性を得ることができた。

万全なセキュリティ体制を作るのは難しいが、人的セキュリティホールからの侵入の割合が高いので、標的型メール攻撃訓練のようなツールを活用した訓練など、定期的なセキュリティ教育が必要であり、困った時に近隣のセキュリティの専門家でない人に相談してしまわない様に、気軽に相談できて適切な対策について専門用語を使わずに説明できる専門家相談窓口設置などの継続性が重要である。更に、情報漏洩事故による損害賠償などに備え、保険等によるリスク移転の認識を持ってもらうことも必要となっている。

また、『サイバーセキュリティシンポジウム道後』の一般向けサブプログラムの中小企業への展開については、四国地域全体への普及を今後是非検討してもらいたい案件の一つとなった。

4　中小企業向け サイバーセキュリティセミナー

4.1　サイバーセキュリティセミナー実施状況

本事業を通じてサイバーセキュリティセミナーを実施した。セミナーのテーマは、「第１回_四国地域の中小企業サイバーセキュリティ関係者会議」の結果により、ランサムウェア攻撃を受けた徳島県の病院の件を絡めた形でのサイバー犯罪事例及び中小企業のセキュリティ対策として実施した。申込者数 64 名、参加者数延べ 52 名。
また、セミナー参加者を対象にアンケートを実施しセキュリティの現状および意識を調査した。

4.2 サイバーセキュリティセミナー実施概要

- 目 的：
  近年、サプライチェーン全体で、対策が不十分な中小企業を対象とするサイバー攻撃により、それらの中小企業とサプライチェーンを共有する大企業等への影響が顕著化してきており、中小企業のサイバーセキュリティ対策は喫緊の課題となっている。また、経済産業省のＤＸ認定制度では、サイバーセキュリティ対策も認定項目の一つとなっており、ＤＸとセキュリティ対策は両輪で推進することが重要で、セキュリティに関する知識向上の一環として、「中小企業向け サイバーセキュリティセミナー」をオンライン開催する。
- 主 催：経済産業省四国経済産業局
- 事務局：株式会社ＩＴブレイン
- 開催日時：令和３年 12 月 10 日（金）13：30～15：20
- 開催方法：オンライン（Web-EX Meetings を利用）
- 定 員：概ね 50～60 名程度予定(令和３年 11 月 19 日より申込開始)
- 参加料：無料
- 対象者：四国地域の中小企業経営者、企業・組織のセキュリティ担当者や関係者等
- セミナー内容：

  ＜１部＞

  テーマ：「昨今のサイバー犯罪の現状」

  概要：サイバー攻撃・サイバー犯罪・ランサムウェア攻撃（徳島事案）の事例についての講演

  講師：徳島県警生活安全部生活環境課サイバー犯罪対策室

  ＜２部＞

  テーマ：「中小企業が行うべきセキュリティ対策」

  概要：サイバー犯罪情勢（徳島の病院事例含む）とセキュリティ対策の紹介についての講演

  講師：独立行政法人情報処理推進機構（IPA）
- 参加者募集方法：

  (1) 四国経済産業局のホームページによる案内やメルマガでの告知

  (2) 中小機構四国本部と四国４県中央会への周知依頼

  (3) とくしま産業振興機構 平成長久館主催セミナーでの告知依頼

  (4) イベント告知媒体は以下を利用した

  ・こくちーず

  (5) 委員へ告知を依頼した

  (6) 四国４県の産業支援財団、産業振興機構(センター)のホームページによる案内やメルマガでの告知を依頼した

  (7) 四国４県の商工会議所のホームページによる案内を依頼した

  (8) 教育機関の先生へ学生への案内を依頼した
- 参申込方法：Web サイトよりの申込

申込者数 64 名

4.3 サイバーセキュリティセミナー実施報告

- セミナー参加者は延べ 52 名であり、このうち関係者および講師を除いた一般参加者は延べ 40 名であった。
- 「第 1 回中小企業サイバーセキュリティ関係者会議」の結果を受け、徳島県のサイバーセキリティ事故に関連するセミナーテーマを選定した。セミナーへの反響はアンケートの回答から概ね好評で、また、サイバーセキュリティ対策への意識付けにつながった。

4.4 サイバーセキュリティセミナーアンケート実施報告

(1) 調査の対象

「中小企業向け サイバーセキュリティセミナー」の参加者を対象とした。

(2) 調査の実施方法

「中小企業向け サイバーセキュリティセミナー」の参加者にセミナー内でアンケートの回答を依頼した。またセミナー終了後、参加者にアンケート依頼メールを送信し、匿名で回答を求めた。

アンケートは調査回答用 Web ページを作成し、Web で回答を受け付けた。一部 Web ページが組織のインターネットセキュリティの関係でアクセスできないケースがあり、Word 文書で回答してもらい、代理で Web ページに入力した。

調査事項は以下の通りである。

1).あなたが所属している会社（組織）についてお尋ねします。

問 1． 従業員数として、あてはまるものを一つ選択してください。（従業員数には契約社員やパートタイムの社員を含み、派遣社員や委託先の常駐者は含めないこととします）

問 2． 資本金について、該当するものを選択してください。

問 3． 業種として、最も近いものを一つ選択してください。

2).今回のセミナーおよびサイバーセキュリティ相談等についてお尋ねします。

問 4． 今回のセミナーイベントは、何でお知りになりましたか。(複数可)

問 5． セミナー＜1 部＞「昨今のサイバー犯罪の現状」のご感想をお聞かせください。

問 6． セミナー＜2 部＞「中小企業が行うべきセキュリティ対策」のご感想をお聞かせください。

問 7． 今回のセミナー全体についてのご意見・ご感想をお聞かせください。

問 8． 本日のセミナーを受けて、貴社のサイバーセキュリティ対策を進めたいと思いましたか？

問 9． 今後、セミナー等でサイバーセキュリティ対策に関して取り上げてもらいたいテーマがあれば、下記に具体的にご記入ください。

問 10． ＩＴ関連の不明点やサイバーセキュリティ対策で困ったことがあった場合、どこに相談することが多いです

か？(複数可)

問 11. もし、サイバーセキュリティのコミュニティに参加するとしたら、コミュニティ参加費用年会費はいくらまでなら参加を考えますか？

3). サイバーセキュリティのコミュニティ関連についてお聞きします。

問 12. あなたが所属している会社（組織）では、サイバーセキュリティ対策に関する最新情報をどこから得ていますか？次の中からよく利用するものを選択してください。（複数可）

問 13. あなたはサイバーセキュリティ分野のコミュニティ活動や勉強会に参加したことがありますか？（あてはまるものをすべて選択してください。）

問 14. 問 13 で「所属している県やその近隣で開催されているコミュニティ活動や勉強会に参加したことがある」と回答された方にお尋ねします。差し支えない範囲で、参加された活動の内容を記入してください。

問 15. 問 13 で「コミュニティ活動や勉強会には参加したことがない」を選択した方にお尋ねします。勉強会やコミュニティ活動に参加したいと考えますか？（あなたの考えに最も近いものを一つ選択してください。）

問 16. 問 15 で「条件に合うものがあればぜひ参加したい」「条件によっては参加を検討したい」を選択した方にお尋ねします。サイバーセキュリティ分野のコミュニティ活動や勉強会を通じて得たいとお考えの情報や知識として、あてはまるものをすべて選択してください。

問 17. あなたが所属している組織では、サイバー保険等のようなリスク移転機能を活用していますか？活用している場合、どのような目的で活用しているか、あてはまるものをすべて選択してください。

(3) アンケート総括

① セミナーについて今回身近に起こったサイバーセキュリティ事故を受け、内容が非常に良かったとの感想が多い。また、回答者の 75%は、セミナーを受講した結果、サイバーセキュリティ対策を進めたいとの前向きな回答が得られた。

② 今後のセミナーテーマの希望として具体的・実践的な内容を求めている傾向がある事がわかった。

③ 今までサイバーセキュリティ分野のコミュニティ活動や勉強会に参加したことがないという回答が約半数あった。一方今後、「条件に合うものがあればぜひ参加したい」あるいは「条件によっては参加を検討したい」という意見が６割を超えており、条件があえばコミュニティへの参加意欲が高いことがわかった。

④ 小規模組織のなかには、会社の系列や懇意にしＩＴ関連の取引先がないため、相談や情報収集を得るルートがないことがわかった。

⑤ サイバー保険等のリスク移転について約 6 割の企業で対策がされておらず、インシデント発生時に中小企業の存続に関わる事態も想定される。特に零細企業については全く対策がされていない実態がわかった。

4.4.1アンケート調査結果

「中小企業向け サイバーセキュリティセミナー」の一般参加者 40 名中 28 名の回答が得られ、回収率は約 70%であった。

また、クロス設問が３問あったが、問 14 における無効回答数が１、問 15 における無効回答数が６、問 16 における無効回答数が９あった。

アンケート結果より、セミナー参加者は、情報通信業、専門・科学技術、業務支援サービス業を中心とした、少な

からずサイバーセキュリティに関心があるとみられる業種が主体であった。

アンケート調査結果の設問ごとの集計結果と考察は、別添　アンケート調査結果を参照。

4.4.2セミナーへの質問事項

「中小企業向け　サイバーセキュリティセミナー」では質問の時間は設けず、イベント後に実施したセミナーアンケートの中で質問事項とメールアドレスを入力してもらう形で質問を受け付けた。質問件数は１部２件、２部１件。集計後、講演者にメールで質問し、回答を質問者にメールアドレス宛に返した。

内容については、表 4.4.2-1　セミナー＜１部＞「昨今のサイバー犯罪の現状」に関する質問事項、及び　表 4.4.2-2　セミナー＜２部＞「中小企業が行うべきセキュリティ対策」に関する質問事項に示す。

セミナーの質問についても具体的運用方法についての内容であり、具体的・実践的な内容を求めていることがわかる。

表 4.4.2-1　セミナー＜１部＞「昨今のサイバー犯罪の現状」に関する質問事項

No.	質問	回答(概要)	応答
1	半田病院様の運用はどのようになっていたのか細かくしりたい。リモートの出入り口やインターネットの有無、バックアップの方法など。	半田病院様の事案については現在捜査中であり，当県警からの回答は控えさせていただきます。	―
2	「対策の第一歩として」のページに、「被害想定訓練を実施する。」と書いてあります。被害想定訓練とは、具体的にどういった内容でしょうか？	①不審メール（ウイルス添付）などに対する対応訓練 ②システムが使用できなくなったことを想定した，手動での業務実施訓練 ③システムの復旧訓練（システムやデータなどが復旧可能か） ④被害発生に対する広報訓練（実施判断／広報内容など） などが考えられますが，各会社の業務内容，構築システムなどにより訓練内容は変わるので検討が必要です。	具体的な想像が付いて、よく分かりました。

表 4.4.2-2 セミナー＜２部>「中小企業が行うべきセキュリティ対策」に関する質問事項

No.	質問	回答(概要)	応答
1	メールの圧縮添付ファイルにパスワードを掛ける方々が多いが添付にランサムを仕込まれていた場合はサンドボックス上でも検出不可(開くまで分からない)。 パスワード無しの場合はサンドボックスで検出可能。IPA 様からリスク及び良い運用方法を広めて欲しい。	パスワード付 ZIP ファイルがウイルスであった場合、ウイルス検知ができないので技術的にブロックすることは困難で、誤って開いてしまうリスクは高くなります。また、攻撃が巧妙化しているため「不審なメールの添付ファイルは開かない」といった人的な注意・判断に依存した場合も完全に防ぐことは困難と考えられます。 感染の影響が深刻である場合は、感染を想定し被害を最小限に抑える方法を考えます。 これには、主な感染経路であるインターネットに接続する LAN 端末と、感染を避けなければならない重要な情報システムとをネットワーク上分離する等があります。 また、Web メールを使う場合に、受信サーバ側で受信した添付ファイルを展開し、ウイルスを検知した場合はクライアント端末へのダウンロードをブロックする、といったサービスも販売されているようですので、お調べください。	―

5 セキュリティ相談会

本事業を通じて以下のセキュリティ相談会を実施した。

5.1 相談対応形態

セキュリティ相談会申込者は、香川県１社、徳島県２社の計３社あった。

セキュリティ相談会は、イベント同日の「中小企業向け サイバーセキュリティセミナー」講演後に時間を設けていたが、当日相談希望者が欠席したので、別日実施することで改めて連絡をとった。先方の都合等もあり実施可能となったのは、徳島県の１社のみであった。

- 日 時：令和３年 12 月 28 日（水）10：30～11：30
- 場 所：オンライン会議(Web-EX Meetings)
- 相談者：１社（２名）

5.2 相談内容とその回答

相談者の相談内容及びその回答を、表 5.2 相談内容 に示す。

表 5.2 相談内容

No.	相談内容	回答(概要)	応答
1	毎日、メールの中にあの手この手を使った迷惑メールが潜んでいて、手口が巧妙で見分けるのにも一苦労しており、良い方法があれば教えて戴きたい。	以下、３つのツールを使い段階的に防御する。 ①プロバイダの迷惑メール対策機能を使う。サービスが有効になってない可能性があるので、プロバイダに設定を確認していただく。 ②投資が必要だが UTM を導入しネットワークの入口でブロックする。 ③Gmail などを使い、スパムメール振分け機能を活用する。 また、ツールは完璧でなくすり抜けるメールもあり、最終的には人に依存するので、教育訓練などが必要です。	具体的な対策がわかり、大いに参考になった。現在、アドバイスに基づき、対策を準備している。

5.3 相談対応に関する所感

今回のセキュリティ相談会申し込みは３件と少なかったが、これはオンライン開催の「中小企業向け サイバーセキュリティセミナー」付随の相談会の為、限定的開設であり周知期間が短く広く周知されなかったのも一因と考えられる。また、公的な機関が主催であり、相談者が自社のセキュリティ対策状態を咎められると感じた恐れもある。実際、実施した相談会において、本事業主催者四国経済産業局の同席の了承を相談者から得ることが出来なかった。

実績としては 1 件の相談のみとなってしまったが、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は、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られる。

今回はコロナ禍で、オンライン開催であったため、相談がしにくい環境であったかとも思われる。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方法や、SNS を活用する方法も考えられる。

Web サイトによる相談対応の場合、Q A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。

6 第２回_四国地域の中小企業サイバーセキュリティ関係者会議

サイバーセキュリティセミナー及びセキュリティ相談会のイベント実施後、「第２回_四国地域の中小企業サイバーセキュリティ関係者会議」をオンラインで開催し、イベント報告をした後、セミナーアンケート結果などをもとに今後のイベント企画指針や方向性およびコミュニティの更なる発展に関する方策について意見を交換した。

尚、イベント報告の内容については、４章、５章に既出であるため、ここでは省略とする。

6.1 会議概要

- 目 的：

地域 SECUNITY の形成及び、中小企業サイバーセキュリティに関する施策の普及・情報共有等を促進するため、四国地域の関係機関等と連携した意見交換会を実施する。（実施イベントの報告会含む）

- 日 時：令和４年１月 19 日（水）10：30～11：30
- 場 所：オンライン会議(Web-EX Meetings)
- 会議メンバー：

  下記関係機関等所属の委員８名（順不同、所属組織名のみ記載）

  ・四国総合通信局 情報通信部

  ・徳島県警察本部 生活安全部生活環境課

  ・四国ＩＴ 協同組合 四国各県代表者

  ・徳島県ＩＴコーディネーター

  ・阿南工業高等専門学校
- オブザーバー：

  ・四国経済産業局 地域経済部 製造産業・情報政策課
- ファシリテーター（進行）：

  ・株式会社ＩＴブレイン

6.2 会議内容

6.2.1「今後のイベント企画指針や方向性に関する意見交換」

一般的に、セミナーは参加者の対象を明確にすることが必要であるとの意見が多くあり、例えば役割に応じＩＴ担当責任者、経営者、ＰＣ利用者等に分ける、あるいはセキュリティ関連知識に応じて初級、中級、上級、管理者に分け、対象ごとのセミナーテーマや内容を選択しなければならないことなどが示された。

セミナーテーマに関しては、身近な参考事例を扱うほうがよく、今回はランサムウェアを取り上げ、タイムリーなテーマであり、良かったとの意見が多かった。このようなセミナーは継続的に行うことが大切であり、災害対策は、“喉元過ぎれば”のことわざ通り、半年、一年経つうちに忘れる。継続は力なりで、これからも続けていくことが大事である。実例紹介などで被害者が苦労した話しなどを行ったりすることで関心を持ってもらえるのではないかなどの意見があがった。他に参考となる意見として、以下を提示する。

- 困りごとをどこに相談したらよいかという話がでる。広く周知するためには、ＩＴ関係ではない団体のなかで案内したほうが広く届くのではないかと思う。敷居を低くする（LINE相談、SNS相談、漫画、アニメなど活用する）などで、今まで触れてなかった方へ届くような工夫が必要だと思う。
- 現在、IPA でセキュリティ俳句やセキュリティポスターのコンクールをしているが、今後、低年齢層から植え付けていくのはどうかと考えている。サイバーセキュリティに関する映画を観てもらうのも若い人には効果が大きいと考える。
- セミナーは参加費によって集まる人が違ってくる。本当に困っているなら有料でも集まるので、参加費についても一考の余地はあると思う。無料で啓発主眼なら継続が大事である。
- 事例検討、便利ツール紹介、訓練なども有効である。現在、メール誤送信勉強会などやっているが、技術的イベント、従業員教育など、対象者に応じたセミナーが定期的にあればよいと思う。

6.2.2「コミュニティの更なる発展に関する意見交換」

コミュニティは、他の中小企業の団体（商工会議所、中小機構など）と連携し、中小企業経営者の集まりの中に入りこんでゆくのが手っ取り早いという意見が出た。また、コミュニティの活動についてはセミナーだけでなく、意見交換する場とするのが良いという意見や、セキュリティ対策は保険のようなものなので、被害額のシミュレーションを行い、リアリティを持つことで経営者層に危機感を持ってもらうなどの工夫も必要との意見があった。

地域 SECUNITY については、総務省でも力を入れて進めており、興味を持っていない中小企業に参加してもらいたいと思っている。『サイバーセキュリティシンポジウム道後』を核として、中小企業と関連が深い四国経済産業局と協力して推進していければとの意見があった。他に参考となる意見として、以下を提示する。

- ターゲットを誰にするのかというのもコミュニティ形成においては重要である。さらに、現代のデジタルネイティブな子供たちへ、小さいころから教育していく場にすることも必要だと考える。
- 法テラスのような無料相談所を参考に、セキュリティに関しても行政に気軽に相談できるところがあればよいと思う。補助金などを活用し、安い費用で相談できる環境つくりが必要である。
- 情報産業協会や県警にも協力してもらって、コミュニティに出向いていけるようなものを、作っていけば良いと思う。
- 病院の事例は、たまたま表に出てきたもので、実は表に出てこない攻撃が沢山ある。流出したデータベースがあるダークサイドを紹介し、怖さを認識させることができたらと思う。
- 相談に関しては全国の「よろず支援拠点」にも常設の相談窓口があり活用して欲しい。

6.3　会議総括

今回のイベントは、病院事故の直後で当該事例を扱うことにより反響があったという指摘のように、今後のセミナー開催においては、身近な事例紹介などフレッシュで話題性のある話しなどを折り込むことでより関心が深まると思われる。また、セミナーについては、職位や知識レベルに応じた対象を明確とすることが必要で、これはセミナー開催の考慮点となる。セミナーは継続的に行い啓蒙することも重要であることが指摘された。

コミュニティの進め方としては、商工会議所、中小機構など、経営者の集まりのある団体に入りこむことで手早く浸透することが出来る。その中で事故時の被害額をシミュレーションするなど、経営者に認識してもらう場にすることが必要などの意見があり、今後の中小企業経営者へのアプローチの参考となると考えられる。

総務省の『サイバーセキュリティシンポジウム道後』を核として、中小企業と関連が深い四国経済産業局と協力して推進していければと思っているとの意見があり、今後、四国地域ならではの取り組みに発展する可能性を伺えた。

7　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、人的にも資金的にも制限がある中で情報セキュリティ対策に向ける余力がなく、脆弱性をかかえたままで、ＩＴインフラを活用せざるを得ない環境にある。多分に漏れず四国地域も同様である。

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の形成を促進し、中小企業のセキュリティ対策に関する意識向上やセキュリティコミュニティを継続・発展させるための施策について四国地域の中小企業サイバーセキュリティ関係者会議を開催し意見交換することで、地域に即した対策の方向性と関係者間の情報共有を実現すると共に、当該会議で出された方針をもとにサイバーセキリティセミナー及びセキュリティ相談会のイベントを企画・実施し、アンケート等で中小企業の実態と意識を収集した。

まず、意見交換についてであるが、２回開催した四国地域の中小企業サイバーセキュリティ関係者会議では、本報告書に示すように、各委員より様々な意見を頂き、非常に有意義な意見交換会になったと思う反面、それぞれの委員や委員の所属組織で実施している中小企業に対する施策等の一部（相談窓口など）については、相互認識が薄い部分もあり、共助の関係の形成が十分とは言い難いところもあった。

地域 SECUNITY を形成し、本事業で得られた意見・情報等を参考にした有益な中小企業のセキュリティ支援を行うためには、今回実施したような有識者の意見交換会を継続的・定期的に実施し、産・官・学の関係者間で連携した共助関係の形成による情報支援が不可欠と考えられる。

残念ながら、イベント実施直前に徳島県の病院でランサムウェア事件が発生してしまい、報道等で大きく取り上げられた。事件発覚前の委員への事前ヒアリングでは、サイバー犯罪の目的が愉快犯的なものから金銭的なものに変わり、中小企業でも攻撃対象になることなど、各委員が普段から危惧していたことが現実のものとなってしまったが、これを一過性の話題とせず、中小企業へ響く形での周知事例として活用できるよう当該事件を分析していくことも必要である。

ランサムウェアの実態については、警視庁のレポート（図 7.1 ランサムウェア被害の被害企業・団体等の規模別報告件数）でも示されている通り、令和３年上半期の被害件数（61 件）の内訳を被害企業・団体等の規模別にみると、大企業は 17 件、中小企業は 40 件とその規模を問わず、被害が発生している。委員の意見にもあったように、この事実のとらえ方・事例の分析による訴求性の高い周知方法（対岸の火事ではなく、明日は我が身等ととらえられるような）について一考の余地がありそうである。支援対象とする中小企業には、規模・業種・環境等が異なるため、事例においても必要とする支援レベル別に分類することも必要であると考える。

また、今回のサイバーセキュリティセミナーアンケートから得られた考察として以下がある。

- 中小企業が求めている具体的・実践的・現実的な情報や知識が得られる場にすることで継続的なコミュニティ形成につなげられる事が期待できる。
- サイバー保険等のリスク移転について零細企業においては全く対策されておらず、トラブル時の被害の大きさとリスク移転の必要性について広く周知することが必要である。

ランサムウェア攻撃の金額面の実態も同じく警視庁のレポートで示されているが、被害に関連して要した調査・復旧費用の総額は、39 件の有効な回答のうち、一千万円以上の費用を要したものが 15 件で、全体の 39%を占めている（図 7.2 ランサムウェア被害の調査・復旧費の総額）となっており、被害規模によっては零細企業の存続に関わる額になっている。このような情報も先程の事例分類の情報に併せ、いつでも提供できるような情報支援体制も必要である

と思う。

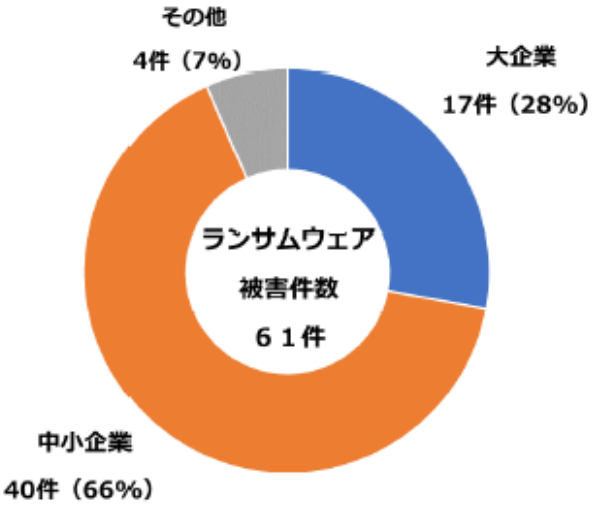
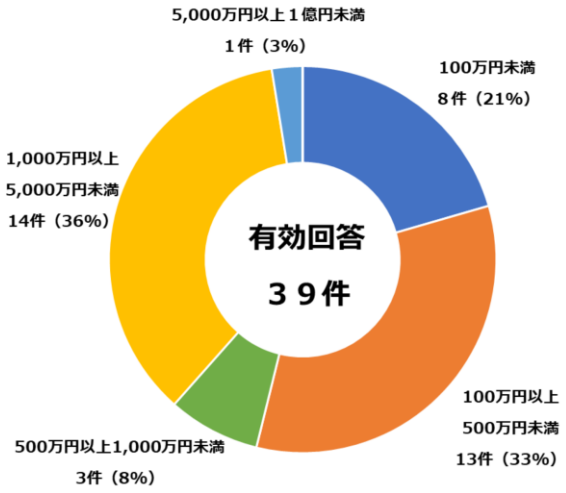


図 7.1 ランサムウェア被害の被害企業・団体等の規模別報告件数[1]



注　図中の割合は小数点第１位以下を四捨五入しているため、総計が必ずしも100にならない。

図 7.2 ランサムウェア被害の調査・復旧費の総額 [1]

[1] 出展：サイバー空間をめぐる脅威の情勢等｜警察庁 Web サイト
https://www.npa.go.jp/publications/statistics/cybersecurity/index.html
の「令和３年上半期におけるサイバー空間をめぐる脅威の情勢等について(4.58MB)」より

コミュニティの活動についてはセミナーだけでなく、相談や意見交換などを通じて中小企業が具体的な情報を得る場にすることが必要である。例えば、「第１回_四国地域の中小企業サイバーセキュリティ関係者会議」で指摘された標的型メール攻撃訓練などについてどのような訓練があるか、費用はどの程度かかるかなど、具体的な情報を得られる場にすることが必要である。中小企業がコミュニティに参加することの目的は深い専門知識の吸収ではなく、会社規模や保有する情報資産に応じた情報の収集である。(図 7.3 コミュニティの構成と各組織の役割)

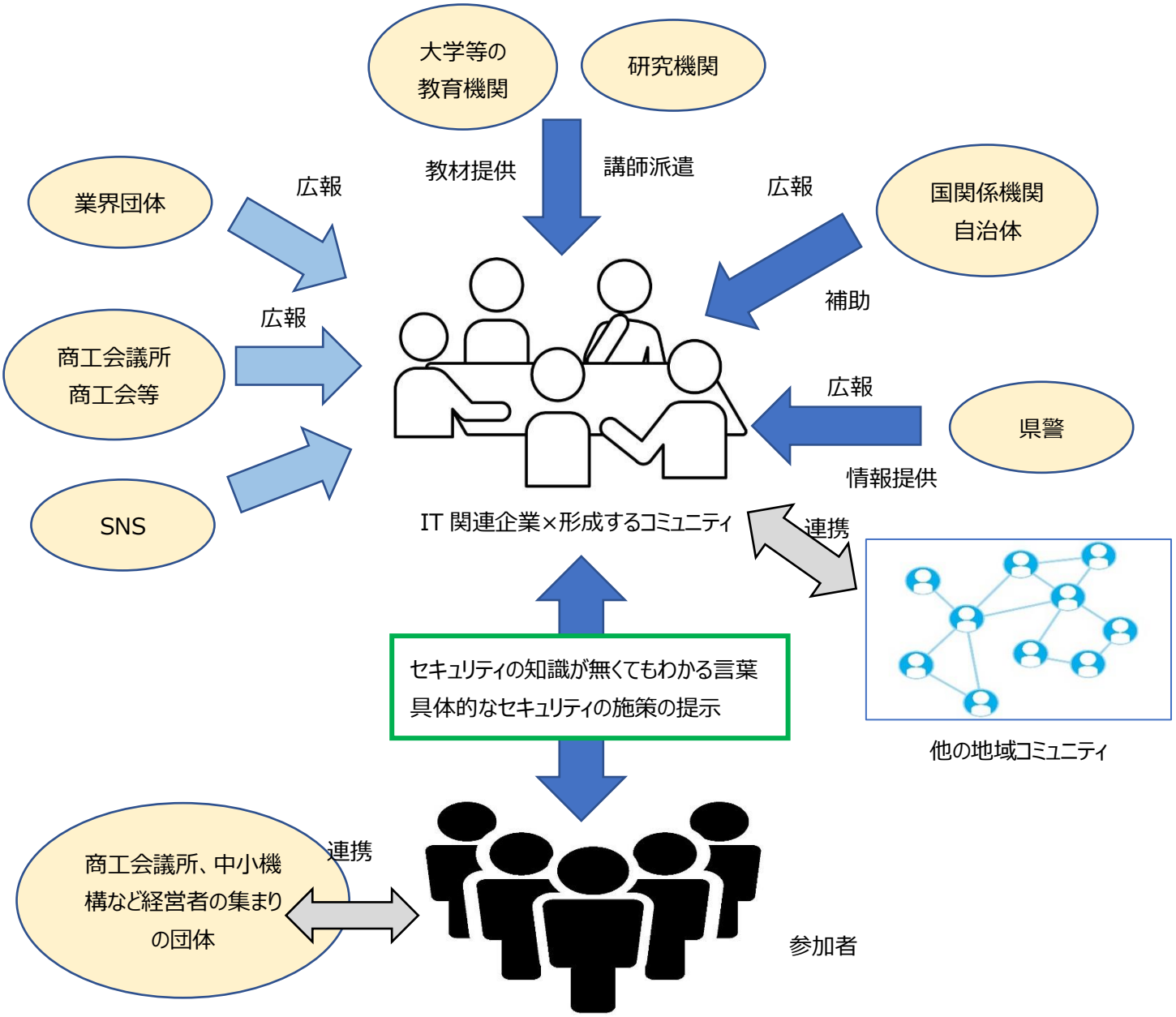


図 7.3 コミュニティの構成と各組織の役割

「第１回_四国地域の中小企業サイバーセキュリティ関係者会議」の 3.2.3「コミュニティを継続させる方策に関する意見交換」や、4.4 サイバーセキュリティセミナーアンケート実施報告(3)アンケート総括の④にあるように、小規模組織のなかには、グループ会社や懇意にしたＩＴ関連の取引先がないため、適切な相談先やセキュリティ対策の情報を得るルートがない。しかし人的資源が限られている中小企業が自前でサイバーセキュリティ対策をとることは困難で、何も対策を取らないで放っておかないためには、相談窓口やセキュリティ対策代行に頼るしかない。

相談窓口としては常設の公的な相談窓口が必要で、「第２回_四国地域の中小企業サイバーセキュリティ関係者会議」で紹介された「よろず支援拠点」や「独立行政法人情報処理推進機構（IPA）」などの相談窓口の活用が望まれる。また、セキュリティ対策支援については「中小企業向け サイバーセキュリティセミナー」で独立行政法人情報処理推進機構（IPA）講師から紹介された「サイバーセキュリティお助け隊」の活用などが有効と考えられる。(図 7.4 相談窓口とセキュリティ支援)

このような機関の存在を知らない中小企業へ広く周知するためには、地域コミュニティや経営者層にパイプがある商工会議所、中小機構などの団体でプッシュ型広報などを行うことで認知度を上げることが必要である。

中小企業はこれらを利用することで、適切なサイバーセキュリティ対策を打てるようになることが期待される。

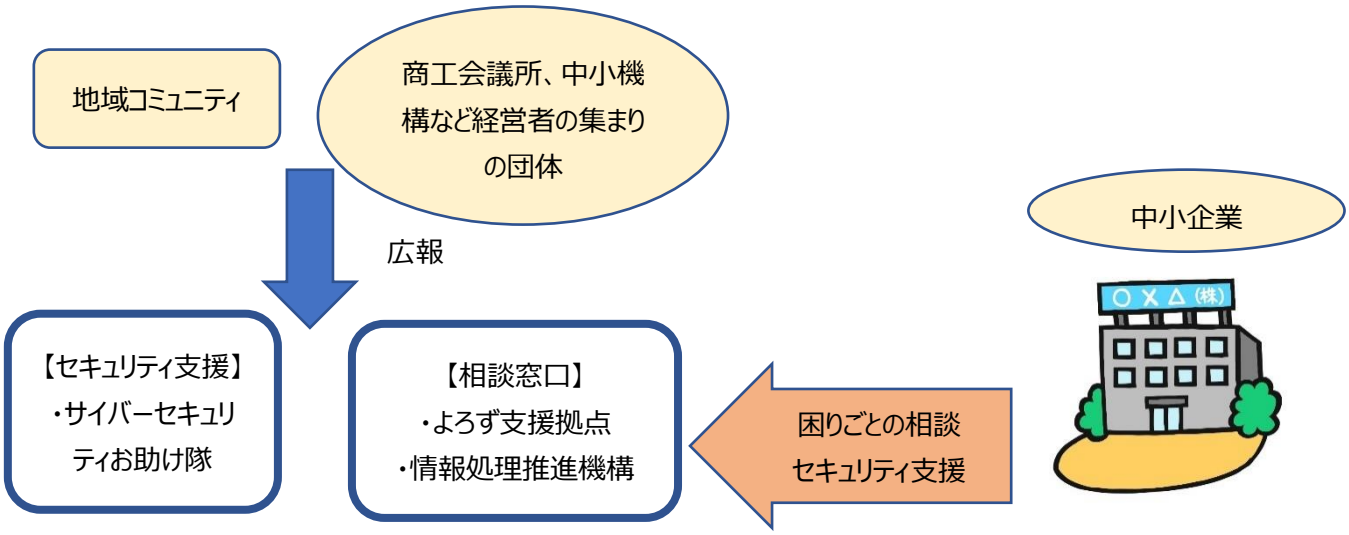


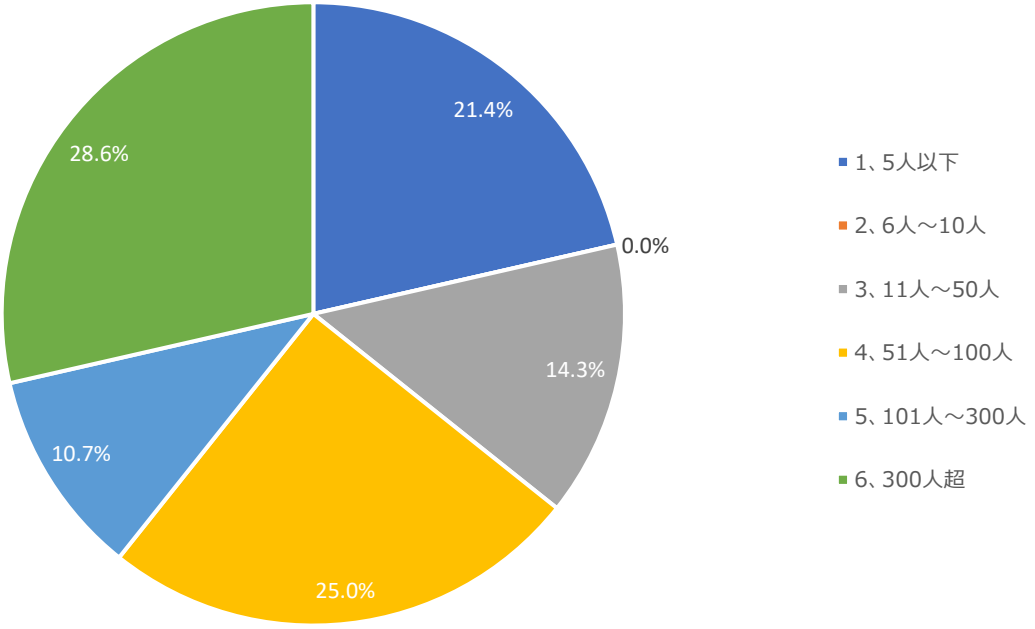
図 7.4 相談窓口とセキュリティ支援

最後に、今回２回実施した四国地域の中小企業サイバーセキュリティ関係者会議の中で意見として挙がった『サイバーセキュリティシンポジウム道後』サブプログラムの四国地域全体への展開は、モデルケースとして是非実現していただきたいと考えている。

以上

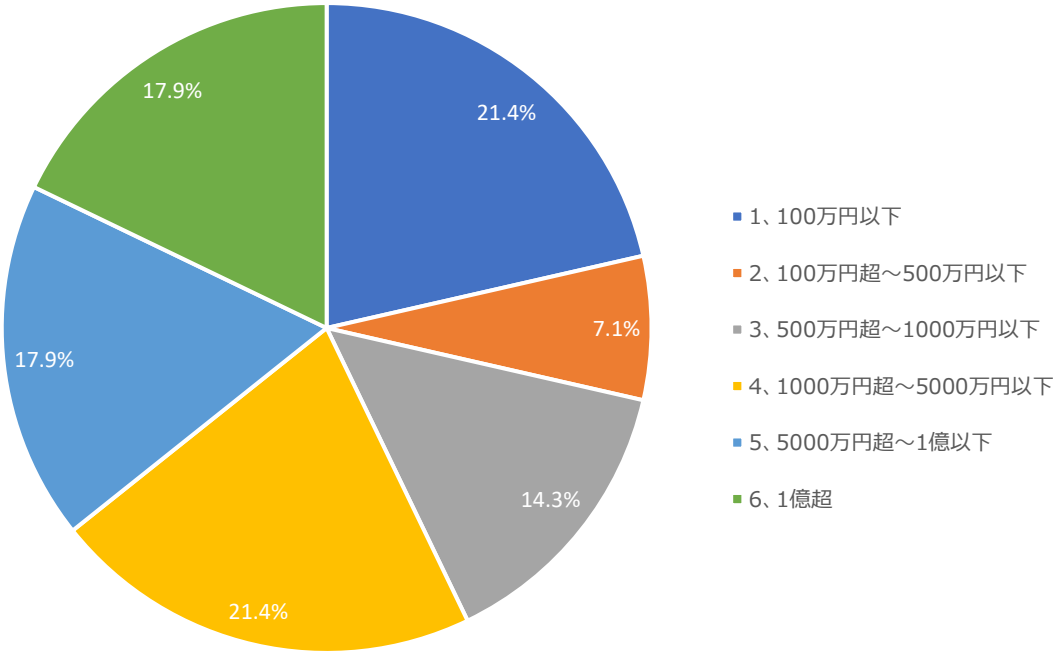
別添　アンケート調査結果

問１.従業員数として、あてはまるものを一つ選択してください。（従業員数には契約社員やパートタイムの社員を含み、派遣社員や委託先の常駐者は含めないこととします）



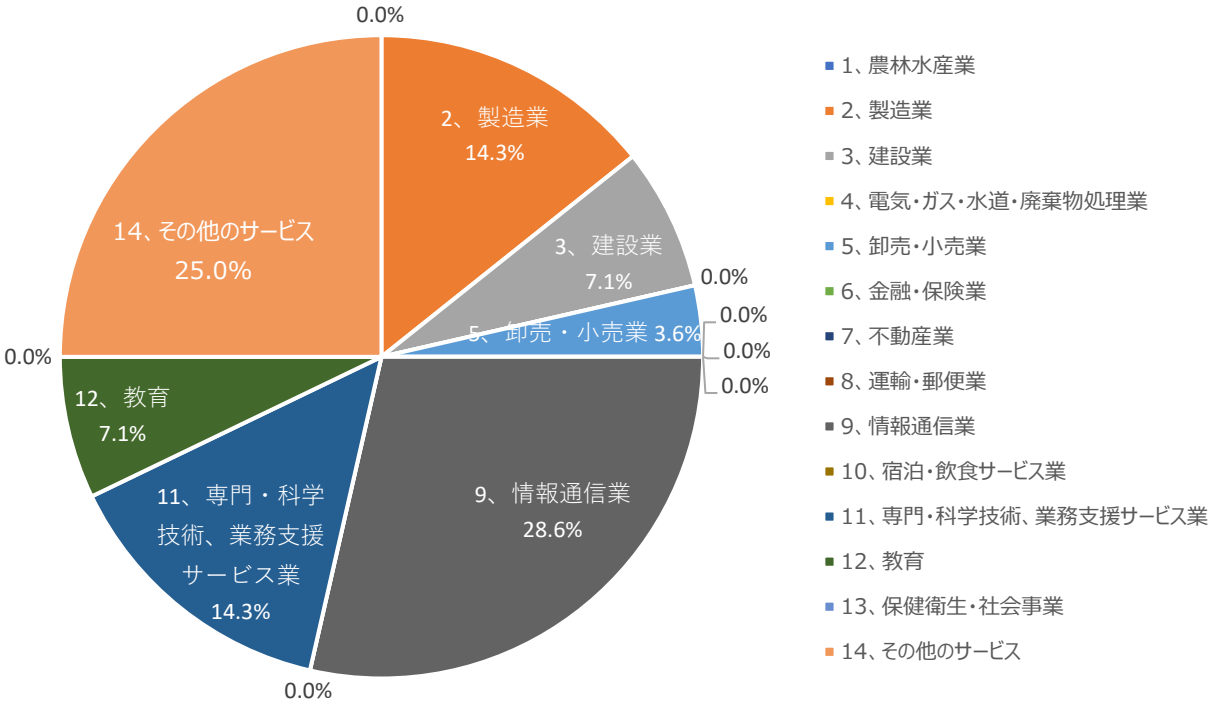
今回の参加者は、６割が 100 人未満の企業であった。

問２.資本金について、該当するものを選択してください。



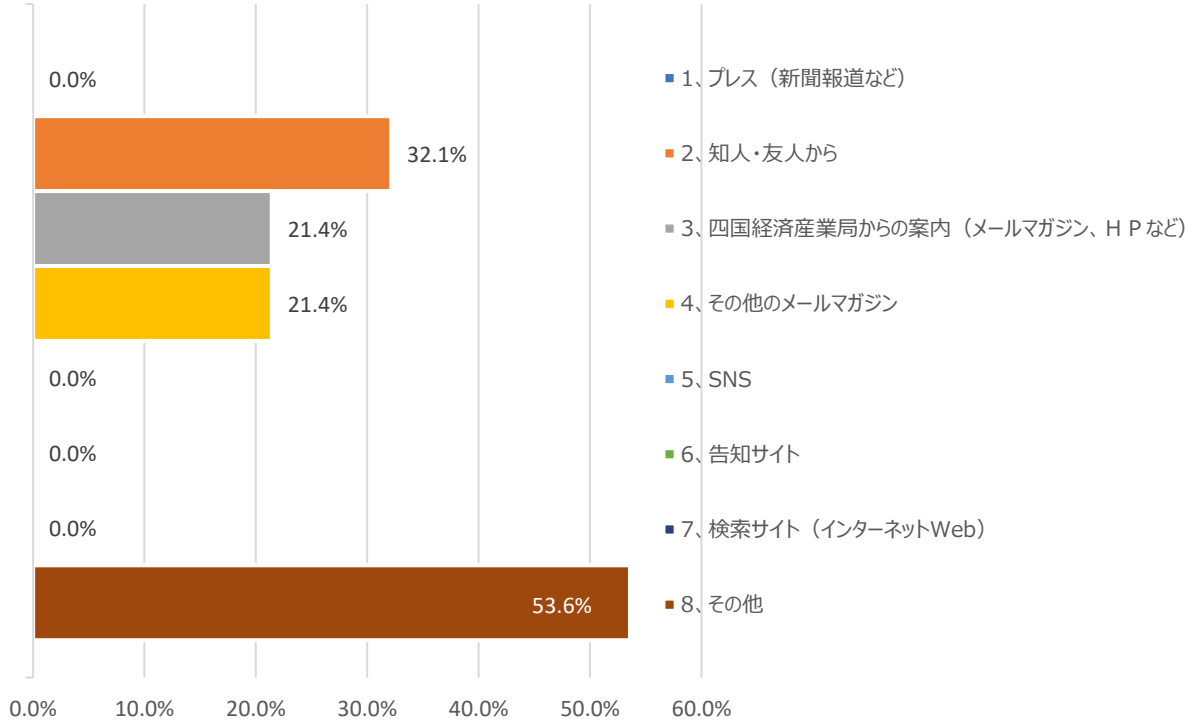
４割が 1000 万円以下であり、そのうち２割が 100 万以下であった。

問３.業種として、最も近いものを一つ選択してください。



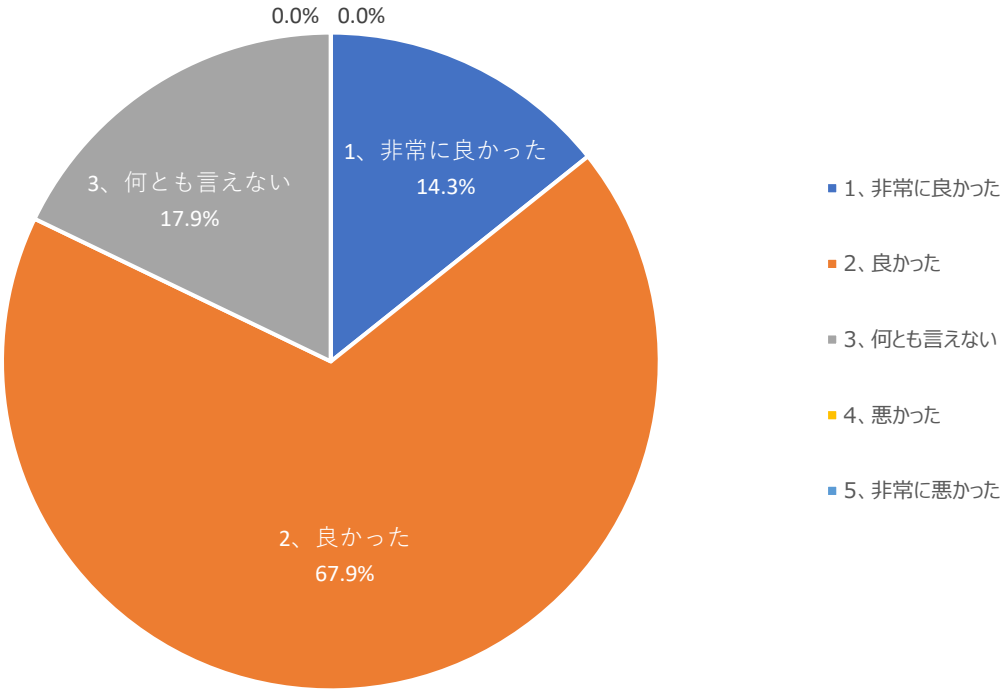
情報通信業、専門・科学技術、業務支援サービス業が多く、卸売・小売、建設は少なく、運輸は皆無であった。

問４.今回のセミナーイベントは、何でお知りになりましたか。(複数可)

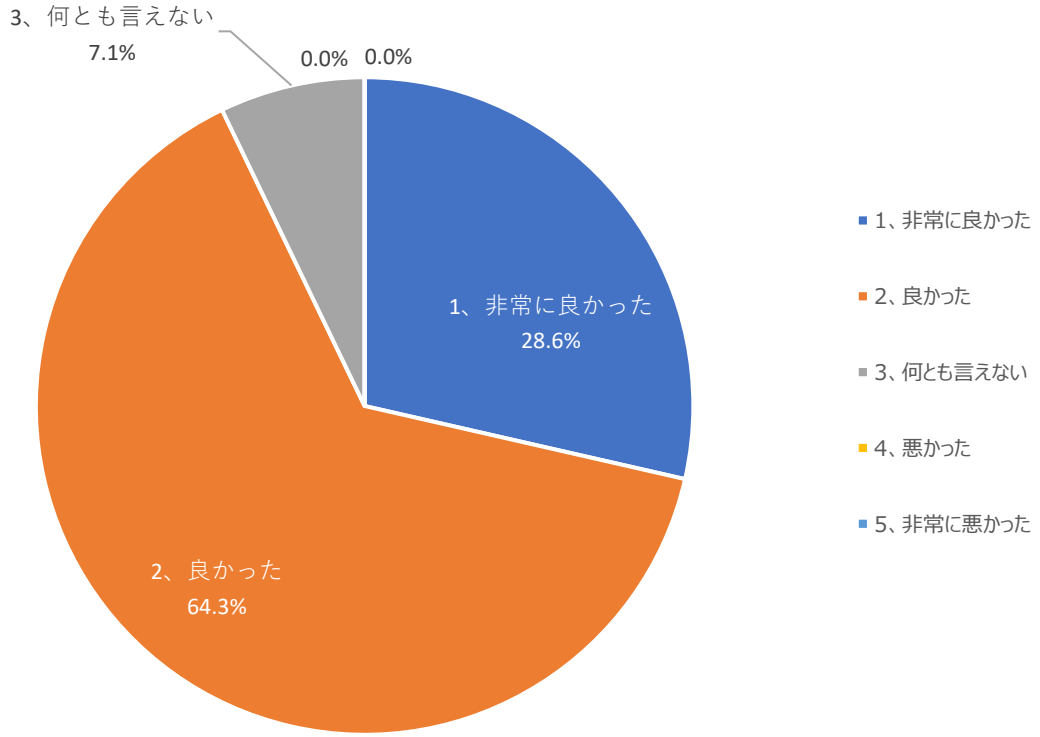


に対して、期間が短かったせいもあるが、告知・検索サイトはなく、メルマガ、口コミが多い。
新聞報道がどのように取り上げていたかは不明であるが、プレスから知ったとの回答が無かった。

問５.セミナー＜1 部＞「昨今のサイバー犯罪の現状」のご感想をお聞かせください。



問６.セミナー＜2 部＞「中小企業が行うべきセキュリティ対策」のご感想をお聞かせください。



両セミナーとも良かった、非常に良かったが８割を超えている。

資料の送付関連の問い合わせもあり、IPA は配布資料も多く、資料紹介や講演資料は欲しいと見える。

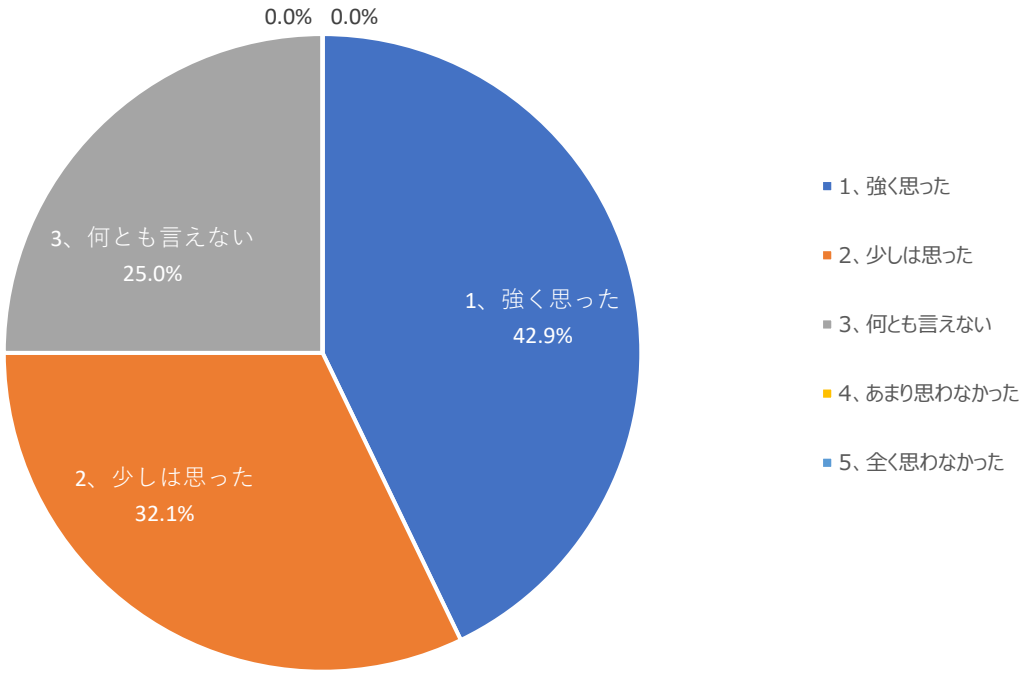
問７.今回のセミナー全体についてのご意見・ご感想をお聞かせください。

これについての記述式回答結果は、

- 最近偽装メールの多さに驚くとともに、情報セキュリティに関するコミュニケーションをとって知識を強化することが大切であると感じた。
- 社内のサイバーセキュリティについて、まず何をすれば良いのかが分からなかったが、IPA の充実したガイドラインがある等、情報を身に着ける方法が分かった。あとはこれを社内で浸透させて、セキュリティ意識を上げていきたいと思った。
- 自社はサイバーセキュリティに関しては担当の者がかなり強いファイアウォールを設定しているがそれでも怪しいメールは届いている。そこから先は各々が注意するしかないため、何か対策が必要と考える。
- 実際の事例が聞けて大変勉強になりました。今後のセキュリティ対策に活用したいと思います
- Web なので気楽に参加でき、便利。
- RAID では、マルウェア対策にはならないことが分かった
- 中小企業におけるサイバーセキュリティ対策の必要性、重要性を再度認識できました。
- 事例などの情報が役に立ちました。
- 徳島の例は、身近な内容なのでとても興味をそそられました。
- 非常に有意義なセミナーでした。
- 参考になりました。

など、徳島県で発生したランサムウェア攻撃をきっかけにして、セミナー受講により危機意識が見られる。
また、セキュリティ相談会の相談内容のもあったが、偽装メール対策についての関心が高いことがわかる。

問８.本日のセミナーを受けて、貴社のサイバーセキュリティ対策を進めたいと思いましたか？



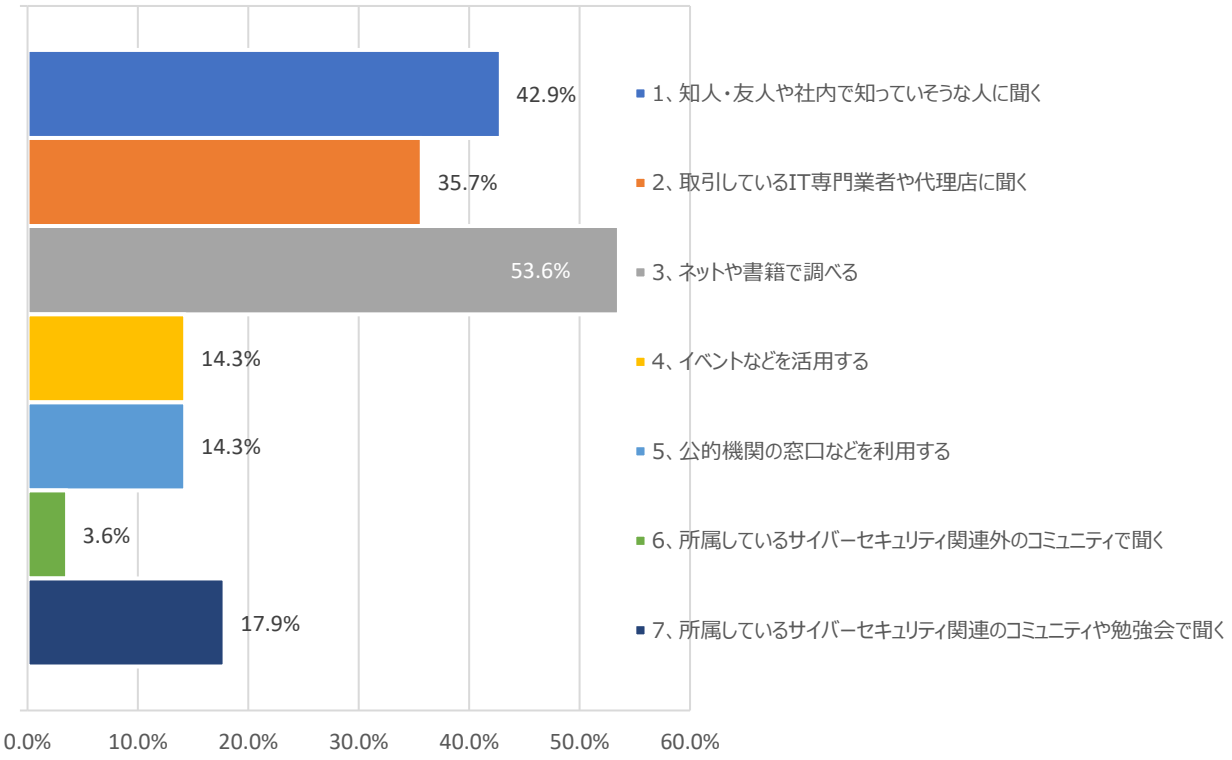
「強く思った」「少しは思った」との回答が 75%あり、セミナーに参加してセキュリティ対策の動機付けにつながる結果になった。

問９.今後、セミナー等でサイバーセキュリティ対策に関して取り上げてもらいたいテーマがあれば、下記に具体的にご記入ください。

- 具体的な対策、被害の多いサイバー攻撃の手口など、
- セキュリティ規程の作り方、中小企業でもできるシステム運用方法
- ランサムウェア対策で、実際に取り組まれている事例（どのような仕組みで対策しているのか）を取り上げてほしい。
- どのようなバックアップであれば安全であるか。
- 被害の事例や対策の事例を教えていただきたいです。

など、事例も含め、具体的内容が好まれそうであり、セミナーテーマの選定では考慮が必要と思われる。

問 10. ＩＴ関連の不明点やサイバーセキュリティ対策で困ったことがあった場合、どこに相談することが多いですか？(複数可)



「ネットや書籍で調べる」「知人友人で知っていそうな人に聞く」の回答が多く、逆にコミュニティは少ない。
これらは専門性のないところで解決していると思われ、誤った情報をつかんでしまうこともあると思われる。

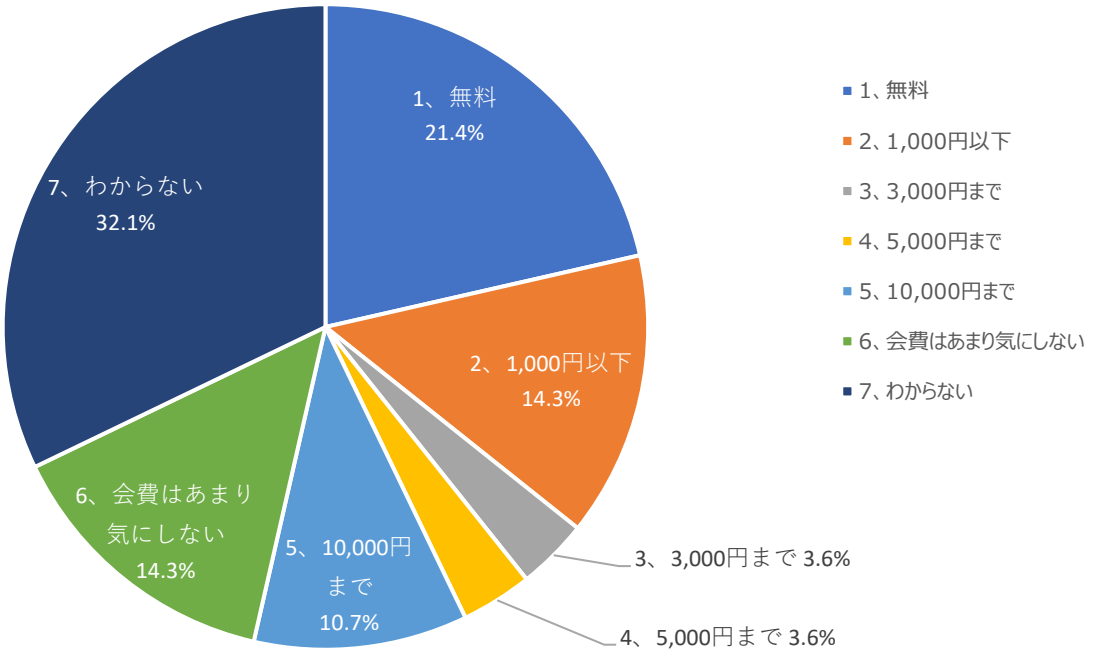
・事業規模に応じた分析

調査回答(複数選択)	従業員数	
	50 人以下	51 人以上
知人・友人や社内で知っていそうな人に聞く	70%	28%
ネットや書籍で調べる	70%	44%

調査回答(複数選択)	資本金	
	1,000 万円以下	1,000 万円超
知人・友人や社内で知っていそうな人に聞く	67%	25%
ネットや書籍で調べる	67%	44%

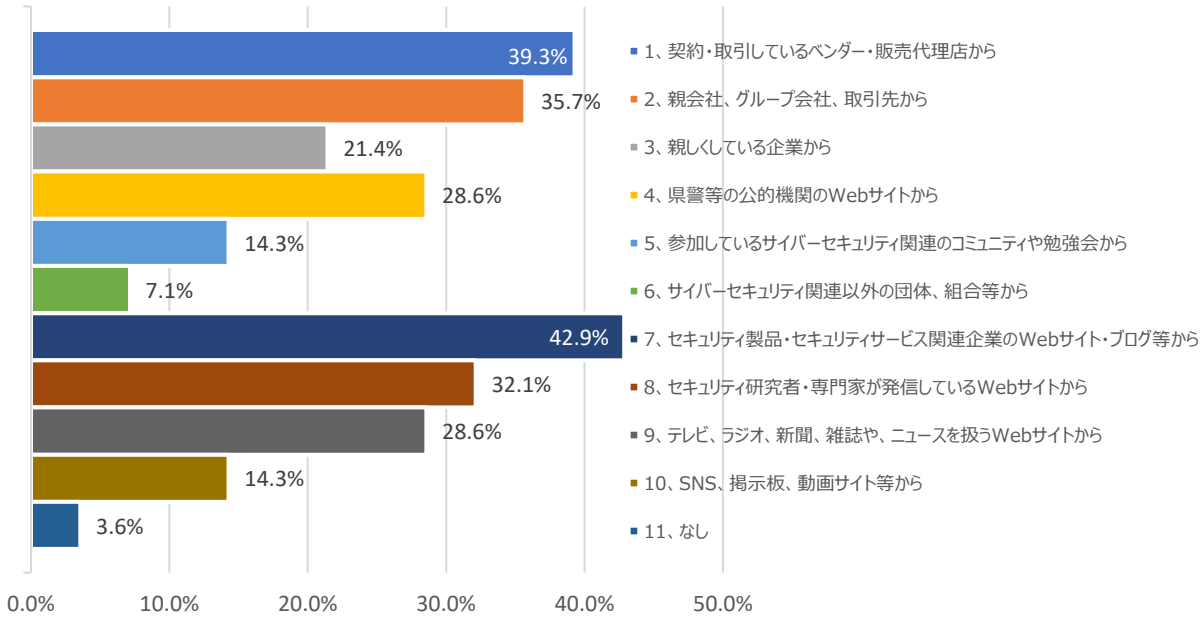
小規模な組織は「知人・友人や社内で知っていそうな人に聞く」「ネットや書籍で調べる」の比率が更に高く、相談する相手が限定され、適切な対策が打てていない恐れがある。

問 11.もし、サイバーセキュリティのコミュニティに参加するとしたら、コミュニティ参加費用年会費はいくらまでなら参加を考えますか？



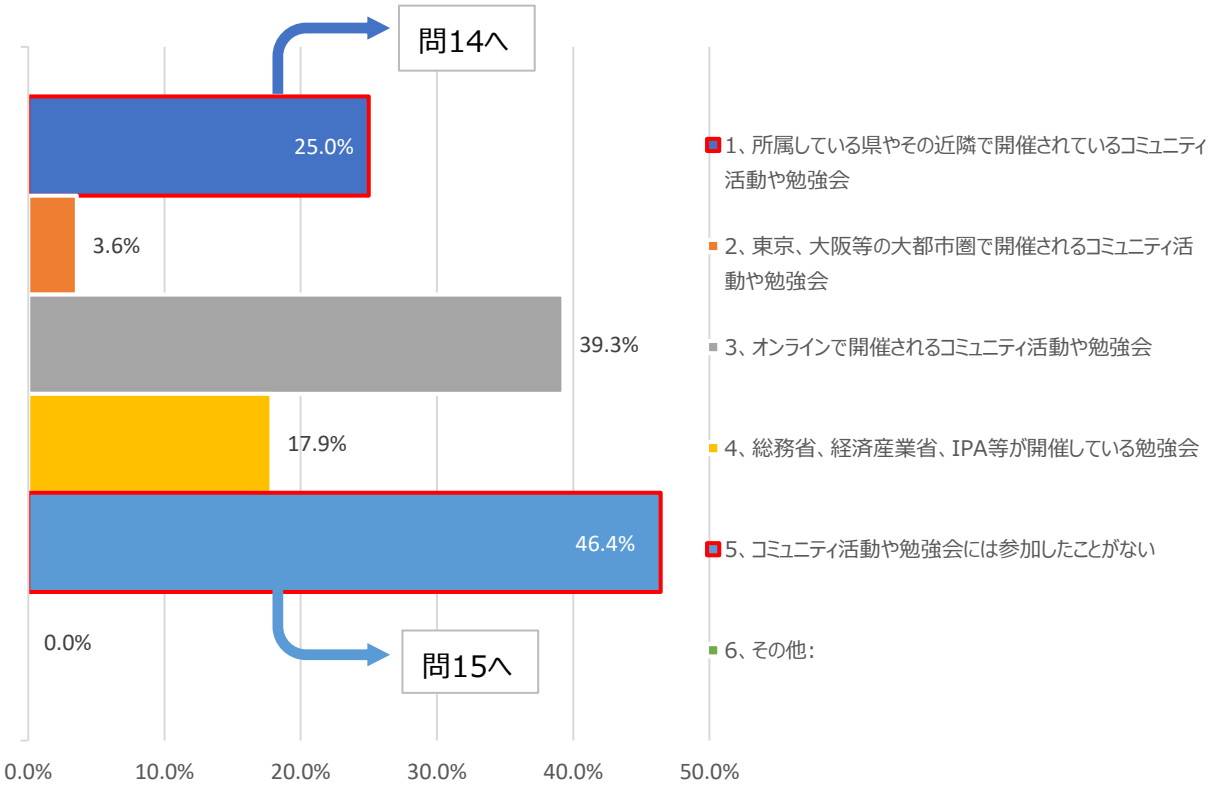
に対し、無料～3,000 円の回答が 4 割あり、コミュニティ参加の費用は制限されるのがわかる。一方、会費にこだわらないという意見も 14%程度ある。

問 12.あなたが所属している会社（組織）では、サイバーセキュリティ対策に関する最新情報をどこから得ていますか？



に対し、「契約・取引しているベンダー・販売代理店から」や「親しくしている企業から」という身近なところから及び、いろいろな Web サイトから情報収集している傾向が高く、「コミュニティや勉強会から」「団体、組合等」と回答したのは少ない。

問 13.あなたはサイバーセキュリティ分野のコミュニティ活動や勉強会に参加したことがありますか？（あてはまるものをすべて選択してください。）



に対し、参加したことがないとの回答が 46%と約半数あり、会社の規模(資本金)に関連がなく多数を占めている。

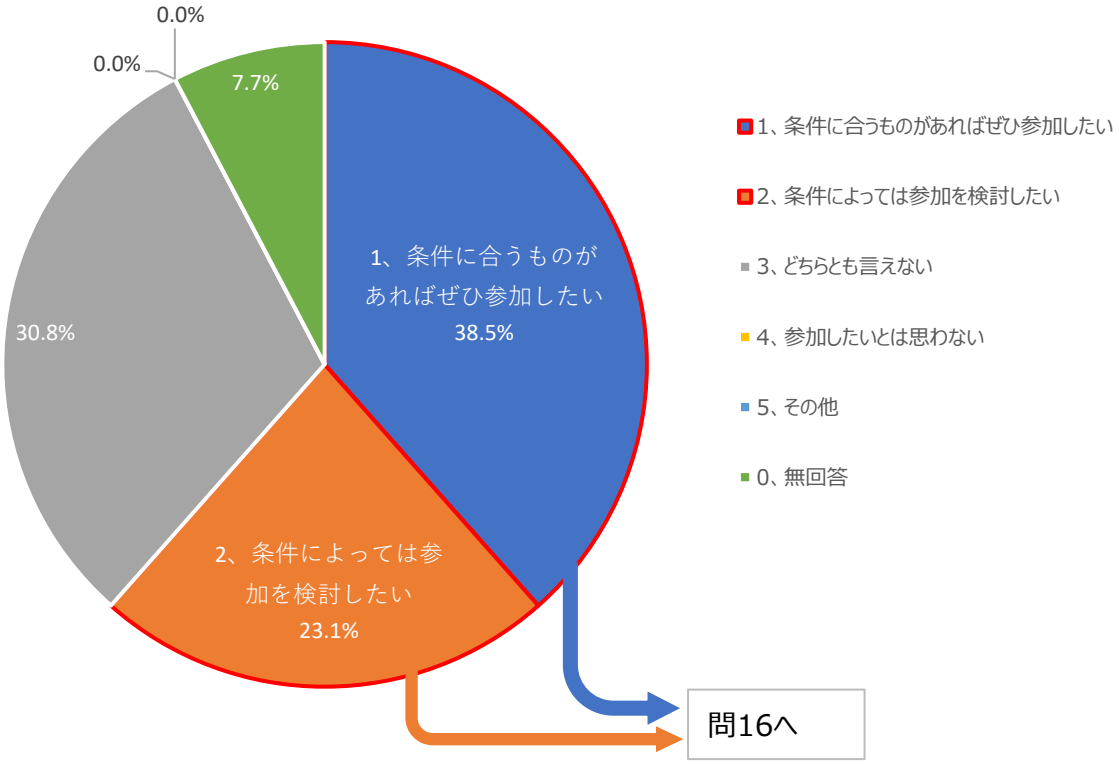
身近に参加できるコミュニティが存在しないか存在自体知らないという結果になっている。

問 14.問 13 で「所属している県やその近隣で開催されているコミュニティ活動や勉強会に参加したことがある」と回答された方にお尋ねします。差し支えない範囲で、参加された活動の内容を記入してください。

に対し、2 件の回答があった。

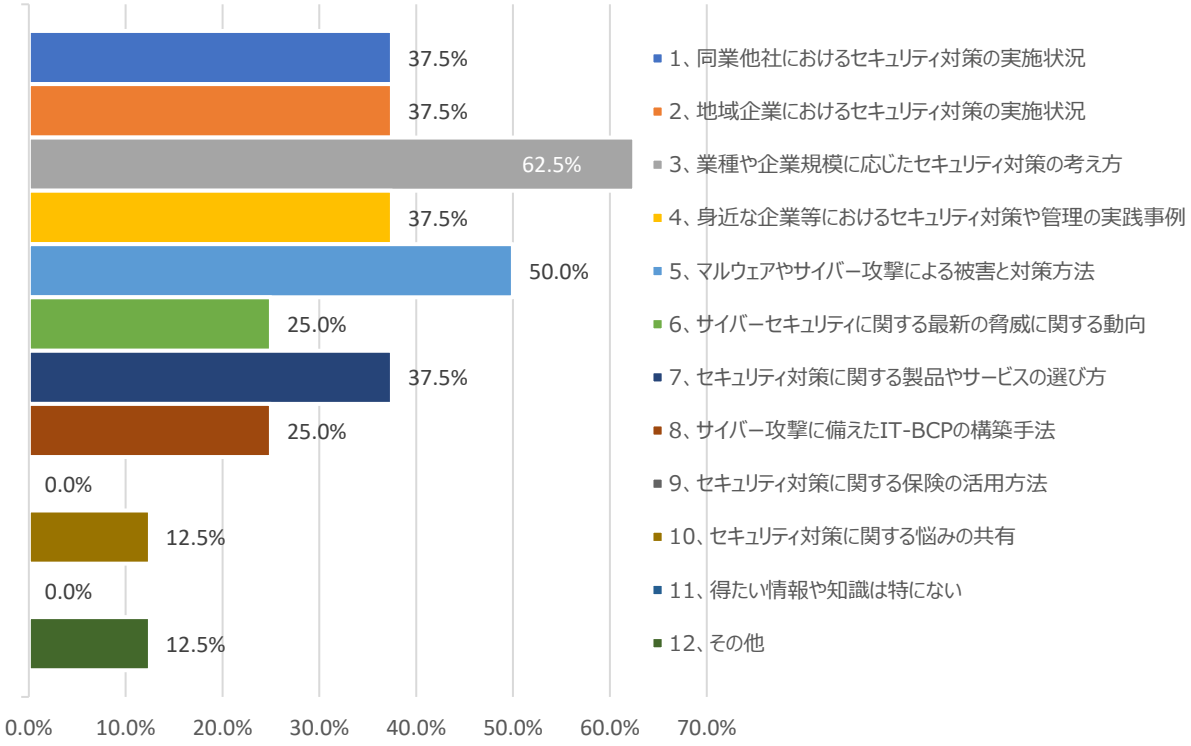
- 県警が開催する協議会
- サイバーセキュリティシンポジウム

問 15.問 13 で「コミュニティ活動や勉強会には参加したことがない」を選択した方にお尋ねします。勉強会やコミュニティ活動に参加したいと考えますか？（あなたの考えに最も近いものを一つ選択してください。）



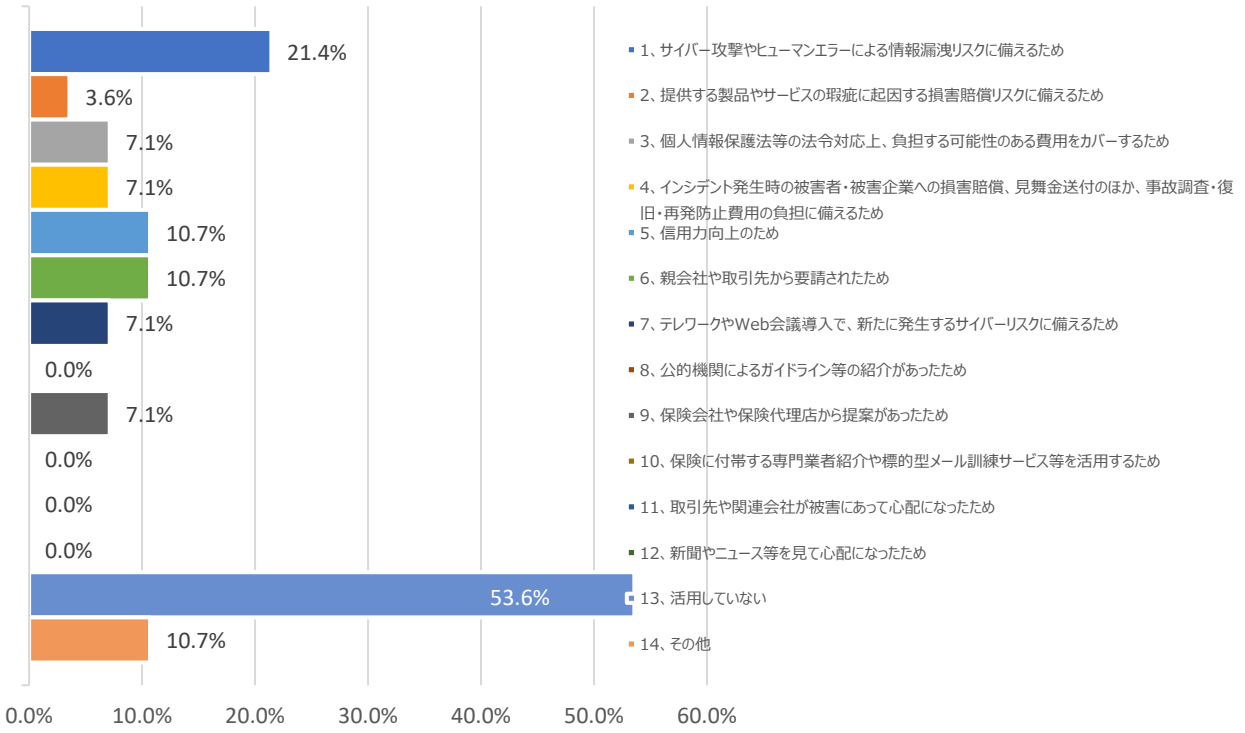
問 15 で、現在は参加していないが、今後参加したいかの問いに条件によって参加したいと考えており、ニーズに合ったコミュニティを形成することで、コミュニティ活動の継続が期待できる。

問 16.問 15 で「条件に合うものがあればぜひ参加したい」「条件によっては参加を検討したい」を選択した方にお尋ねします。サイバーセキュリティ分野のコミュニティ活動や勉強会を通じて得たいとお考えの情報や知識として、あてはまるものをすべて選択してください。



「業種や企業規模に応じたセキュリティ対策の考え方」を得たいとの回答が 60%以上あり、どのようなセキュリティ対策が必要かを模索しているのがわかる。
また、「業種や企業規模に応じたセキュリティ対策の考え方」、「マルウェアやサイバー攻撃による被害と対策方法」、「セキュリティ対策に関する製品やサービスの選び方」など具体的、実践的、現実的な内容が上位を占めている。

問 17.あなたが所属している組織では、サイバー保険等のようなリスク移転機能を活用していますか？活用している場合、どのような目的で活用しているか、あてはまるものをすべて選択してください。



「その他」を含め何らかのセキュリティ事故への備えをしているという回答が 46%程度あった。
一方「活用していない」に約半数が回答しており、リスク移転機能等、実際に起こってしまった後の対応はまた考えていない様である。

・事業規模に応じた分析と考察

調査回答(複数選択)	従業員数	
	50 人以下	51 人以上
活用していない	90%	33%

調査回答(複数選択)	資本金	
	1,000 万円以下	1,000 万円超
活用していない	100%	19%

更に資本金１,000 万円以下の企業は全く対策されておらず、中小規模の企業のリスク移転対策の必要性が大きい。
四国地域の中小企業サイバーセキュリティ関係者会議でも意見があったが、中小企業経由で大企業が狙われているので、損害賠償発生の注意喚起を進める必要がある。