令和２年度中小企業サイバーセキュリティ対策支援体制構築事業

（サイバーセキュリティお助け隊事業）

（実証対象：北海道）

成果報告書

請負事業者：東日本電信電話株式会社

IPA 独立行政法人情報処理推進機構
Information-technology Promotion Agency, Japan

目次

サマリー

本報告書は、東日本電信電話株式会社（以下「NTT 東日本」という。）が「令和 2 年度中小企業サイバーセキュリティ対策支援体制構築事業」において実施した実証内容を報告するとともに、結果に基づき中小企業のサイバーセキュリティ対策について提言するものである。

北海道内の中小企業 143 社を対象に、以下の 4 つのサイバーセキュリティ対策サービスを提供し、それぞれの結果から、中小企業のサイバーセキュリティ対策の実態を把握し、今後中小企業が継続的に利用可能なサービスおよび保険について検討を実施した。

- セキュリティ対策機器（UTM）
- 標的型攻撃メール訓練（メールセキュリティ対策）
- Web の脆弱性診断（ホームページ脅威の診断）
- 情報セキュリティ e ラーニング（スキル醸成）

1. サイバーセキュリティ対策の現状について

1.1 サイバー攻撃の現状、サイバーセキュリティ脅威のトレンド・動向

昨今、中小企業を含む取引先や海外展開を進める企業の海外拠点、更には新型コロナウイルスの感染拡大に伴うテレワークの増加に起因する隙など、攻撃者が利用するサプライチェーン上の「攻撃起点」が拡大している。この状況を踏まえ、経済産業省は、2020 年 12 月 18 日にサイバーセキュリティの取組の強化に関する通達を行った。その中で経済産業省は、最近の攻撃の特徴と目的を明らかにし、企業やその関係機関等が対応する際に注意すべき点を整理することで、企業の経営者の方々に対し、サイバーセキュリティの取組について一層の強化を促すとしている。通達の中で経済産業省は、以下の 3 点をサイバー攻撃の現状として分析している。

（1）中小企業を巻き込んだサプライチェーン上での攻撃パターンの急激な拡がり

昨今、中小企業を含む取引先や海外展開を進める企業の海外拠点、更には新型コロナウイルスの感染拡大に伴うテレワークの増加に起因する隙など、攻撃者が利用するサプライチェーン上の「攻撃起点」がますます拡大している。

（2）大企業・中小企業等を問わないランサムウェアによる被害の急増

暗号化したデータを復旧するための身代金の要求に加えて、暗号化する前にあらかじめデータを窃取しておき、身代金を支払わなければデータを公開するなどと脅迫する、いわゆる「二重の脅迫」を行うランサムウェアの被害が国内でも急増しつつある。背景には、攻撃者の側でランサムウェアの提供や身代金の回収を組織的に行うエコシステムが成立し、高度な技術を持たなくても簡単に攻撃を行えるようになっていることがある。

（3）機微性の高い情報の窃取等を目的としたと考えられる海外拠点を経由した攻撃

ビジネスのグローバル化に伴い海外拠点と密に連携したシステム構築が進む一方で、十分な対策を採らないまま海外と日本国内のシステムをつなげてしまった結果、セキュリティ対策が不十分な海外拠点で侵入経路を構築され、国内に侵入されるリスクが増大している。

経済産業省からの注意喚起は、中小企業に対するサイバーセキュリティ対策を強く促すものとなっている。このことから、サイバーセキュリティの脅威は社会インフラや大企業だけではなく、中小企業にも影響を及ぼし始めていることがうかがえる。

経済産業省が現在の被害状況から注意喚起している主なサイバー攻撃を紹介する。

（１）Emotet（エモテット）

Emotet と呼ばれるウイルスへの感染を誘導する高度化した攻撃メールが国内外の組織へ広く着信する。実在の相手の氏名、メールアドレス、メールの内容等の一部を流用して正規のメールへの返信を装うなど、業務上開封してしまいそうな巧妙な文面となっている場合が多い。

2020 年 7 月末から国内外に向けて Emotet に感染させるメールの配信活動が活発化している。過去に感染した被害組織から窃取された情報を使ってなりすまされたメールが配信されている。Emotet は、情報の窃取等の直接攻撃に悪用されることに加え、他のウイルス等による攻撃の侵入口として悪用されるウイルスでもあり、一度感染すると拡散していく傾向がある。

（2）ネットワーク貫通型：VPN 機器の脆弱性を悪用したネットワークへの侵入

VPN 機器の脆弱性が相次いで報告され、そうした脆弱性を悪用するコードが公開されるなど深刻な状況が発生している。攻撃者はこうした脆弱性を通じて直接的に社内ネットワークへ侵入し、攻撃を展開する。

2020 年 8 月、Pulse Secure 製 VPN 機器の脆弱性が悪用され、国内外 900 以上の事業者から VPN の認証情報が流出した。2020 年 11 月、Fortinet 製品における VPN 機能の脆弱性により影響を受ける約 5 万台の機器に関する情報が公開された。認証情報等が悪用されることで容易に侵入される恐れがある。

（3）ランサムウェア（Ransomware）とその手口の変化（二重の脅迫）

ランサムウェアとは、「Ransom（身代金）」と「Software（ソフトウェア）」を組み合わせた造語である。感染したパソコンのデータを暗号化するなど使用不可能にし、その解除と引き換えに金銭を要求するという特徴がある。

ターゲットとなる企業・組織内のネットワークへ侵入し、パソコン等の端末やサーバー上のデータを窃取した後に一斉に暗号化してシステムを使用不可能にし、脅迫する。

システムの復旧に対する金銭要求に加えて、窃取したデータを公開しない見返りの金銭要求も行うので、二重の脅迫となる。

（4）海外拠点経由の攻撃

ビジネスのグローバル化に伴って、海外拠点とのネットワークを国際 VPN 等により WAN（広域社内ネットワーク）に取り込んで構築しているケースが増加している。海外とのビジネス効率化に寄与する一方で、海外拠点への不正侵入によって、即国内ネットワークまで侵入される危険も伴っている。

海外拠点（海外支社のほか、関連会社、提携先、取引先等を含む）においては様々な原因により、日本国内と同等なレベルのセキュリティ対策が十分に採れないケースが多い。例えば、安価だが品質管理が不十分なソフトウェアが利用されているケース（コピー版等の利用により最新の脆弱性管理が適用されない）、本社のガバナンスが行き届かず、システムの脆弱性が放置され、インシデントの監視・対応体制も十分に確保できていないケース、 従業員教育が十分でなく、私用の機器やソフトウェアなどが許可なくシステムに接続されているケース、信頼性の低いプロバイダを利用せざるを得ないケースなどが考えられる。このような国内環境よりも脆弱な海外拠点において不正侵入を許してしまい、そこを足掛かりに、国内システムの奥深くまで到達されるケースが増加している。

2020 年のサイバー攻撃の影響を日本企業はどのように認識しているのか。サイバーセキュリティを検知、対策することを専門とするマカフィー株式会社が発表した 2020 年の 10 大セキュリティ事件を紹介する。この情報は、日本国内の経営層や情報システム部門などのビジネスパーソンを対象に独自に実施した「2020 年のセキュリティ事件に関する意識調査」の結果に基づくものである（表 1）。

表 1 2020 年のセキュリティ事件に関する意識調査

1 位 （59.2%）	携帯電話会社の電子決済サービスを通じて、利用者の預金が何者かに不正に引き出されたことが判明（9 月）
2 位 （37.7%）	ゲームメーカーが 11 月 16 日、サイバー犯罪集団からの不正アクセスを受け、顧客や取引先に関する情報が最大で 35 万件流出した可能性があると発表（11 月）
3 位 （36.5%）	AI を使ってポルノ動画に写った人物の顔を芸能人の顔にすり替えた“ディープフェイクポルノ動画”を公開したとして、男性 2 人を名誉毀損と著作権法違反の疑いで逮捕（10 月）
4 位 （35.4%）	新型コロナウイルス感染症対策として 10 万円の特別定額給付金の給付が各自治体で始まるなか、自治体などのホームページを模倣したフィッシングサイトが相次いで確認（5 月）
5 位 （35.1%）	米海軍はサイバーセキュリティ上の懸念を理由に、政府支給のモバイルデバイスで中国製アプリケーション「TikTok」を使用することを禁止した（2019 年 12 月）
6 位 （33.5%）	総合電機メーカーがサイバー攻撃を受け、個人情報や機密情報が流出したおそれがあると発表（1 月）
7 位 （32.9%）	総合電機メーカーへのサイバー攻撃で、防衛関係の機密情報が同社から漏えいした疑いがあることが判明（5 月）
8 位 （31.4%）	納税などに関する大量の個人情報や秘密情報を含む地方自治体の行政文書が蓄積されたハードディスク（HDD）が、ネットオークションを通じて転売され、流出していた（2019 年 12 月）
9 位 （30.9%）	「Zoom」の「Windows」版クライアントについて、攻撃者がグループチャットのリンク共有機能を悪用した場合、リンクをクリックした人の Windows のネットワーク認証情報が漏えいする可能性があることが明らかに（4 月）
10 位 （30.2%）	電気通信事業者等を傘下に置く持株会社の機密情報を不正に取得したとして、同社元社員を逮捕。容疑者が取得した機密情報は在日ロシア通商代表部の職員らに譲渡されたとみられる（1 月）

この意識調査において、サイバーセキュリティ攻撃に関する事案が上位 5 件（1 位、2 位、4 位、5 位、6 位）を占めている。この結果から、サイバー攻撃の頻度、対象が確実に拡大しており、日本企業はその脅威を身近なものとしてとらえ、サイバーセキュリティ対策の必要性を実感していると考えられる。

一般企業は、今後どのようなサイバーセキュリティ対策を採るべきか、トレンドマイクロ株式会社（以下、トレンドマイクロ）が、2021 年の国内外における脅威動向を予測したレポート「2021 年セキュリティ脅威予測」のリリース文（2020 年 12 月 22 日公開、URL：https://www.trendmicro.com/ja_jp/about/press-release/2020/pr-20201222-01.html）を紹介する（文体を変更して引用）。

（1）自宅のテレワーク環境がサイバー攻撃の弱点に

2020 年を通して、新型コロナウイルス感染症（COVID-19）の拡大防止のため自宅のホームネットワークから業務を行うテレワークが増加。今後、サイバー攻撃者が脆弱なホームネットワークから従業員の自宅のコンピュータを乗っ取って、組織ネットワークへ侵入することが顕著になることが予想される。

テレワーク環境への侵入を狙うサイバー攻撃者にとって、自宅の「ルータ」は格好の標的となる。侵入済みのルータへのアクセス権をアンダーグラウンド市場で販売する傾向が予想される。加えて、企業の経営幹部や IT 管理者のテレワーク環境など、サイバー攻撃者にとって価値の高いホームネットワークへのアクセス権を提供するアンダーグラウンドのサービスは需要が高くなるとみられる。

テレワーク環境のコンピュータと組織ネットワークとの通信を保護する仮想プライベートネットワーク（VPN：Virtual Private Network）においても、VPN システムの脆弱性による侵入やアンダーグラウンド市場で脆弱性が適用されていないシステムのリストが確認されており、多くの組織にとって、今後 VPN の脆弱性に一層注意する必要がある。

また、テレワークの普及により業務用 PC を私的利用することが更に増加することが伺える。プライベートで利用したオンライン会議システム、クラウドサービスなどから脅威が業務用 PC に侵入し、更に組織ネットワークへ脅威が拡散することが考えられる。法人組織のシステム担当者は、重要な情報や社内の機微なシステムにアクセスするデバイスに対して、ゼロトラストの考えに沿ったセキュリティポリシーを適応することが重要となる。また従業員への教育面においても、ホームネットワーク内のルータやデバイス、クラウドサービスの利用方針を定めて教育を行うことが重要である。

（2）新型コロナウイルスへの便乗と医療機関を狙ったサイバー攻撃の深刻化

サイバー犯罪者は、新型コロナウイルスに対する人々の不安に便乗し、サイバー攻撃を行っており、この傾向は 2021 年も継続するであろう。2020 年には、新型コロナウイルスの感染状況やワクチン関連の情報に偽装した不正サイトや不正メールを確認したほか、日本国内ではマスク不足に便乗した偽の通販サイトや偽の給付金の申請サイトなどを確認した。今後も、世界的な新型コロナウイルスの動向や国内の行政機関の方針に便乗したサイバー犯罪が継続することが懸念される。

2020 年 10 月には、米国のサイバーセキュリティ・インフラセキュリティ庁（CISA：Cybersecurity and Infrastructure Security Agency）から医療機関へのサイバー攻撃に関する警告が発表された。更に 2020 年 12 月には、欧州医薬品庁（EMA：European Medicines Agency）がサイバー攻撃により新型コロナウイルスのワクチンに関する申請文書が不正アクセスを受けたことが報道された。2021 年は新型コロナウイルスに対するワクチンの開発や治験、提供が進むことで、ワクチン開発関連組織へのサイバー偵察・情報窃取が行われることが懸念される。

（3）修正プログラム適用までの空白期間を狙う「N デイ脆弱性」の悪用が横行

サイバー攻撃に悪用される脆弱性（システムのセキュリティ上の欠陥・バグ）は、修正プログラム（パッチ）が提供されていない未知の脆弱性である「ゼロデイ脆弱性」が注目される傾向にある。しかし、2021年はベンダーにより修正プログラムが提供されている既知の脆弱性「Nデイ脆弱性」が重大な懸念を引き起こすと考えられる。

Nデイ脆弱性は、該当のソフトウェアやシステム開発企業から公開開示文書などが公開されており、悪用できる方法を探しているサイバー攻撃者にとって、悪用できる脆弱性の特定が容易となる。加えて、2020年はVPNの脆弱性を狙う攻撃を多く確認したほか、既知の脆弱性が多数悪用されていたことを確認している。

今後、こうした「Nデイ脆弱性」の情報や脆弱性を抱えたシステムへの攻撃ツールの売買がアンダーグラウンド市場で活況となる可能性もある。テレワーク時代を迎えて、多くのシステムが外部からのアクセスを前提とする中、改めて脆弱性の有無の確認や不要になったサービスの停止などの対応が求められる。

未知のサイバー攻撃は検知不能であるため、サイバーセキュリティ対策の予防的措置としては、既知のサイバー攻撃の拡散に対して、企業が徹底した対策を採ることが重要である。サイバー攻撃の対象は、脆弱性が比較的高くなるリモートワーク、海外に触手を伸ばしており、日本の中小企業も標的となる可能性が十分にある。事業規模にかかわらず、十分な対策をしておかなければ、大きな損失を被りかねない状況であることを認識し、対策に努めなければならない。

1.2 企業におけるサイバーセキュリティ対策状況

経済産業省は、「1.1　サイバー攻撃の現状、サイバーセキュリティ脅威のトレンド・動向」で紹介した注意喚起の中で、経営者に対して以下を提言している。

- ✓ サイバー攻撃による被害が深刻化し、被害内容も複雑になっており、経営者の一層の関与が必要となる。
- ✓ ランサムウェア攻撃によって発生した被害への対応は企業の信頼に直接かかわる重要な問題であり、その事前対策から事後対応まで、経営者のリーダーシップが求められる。
- ✓ サイバーセキュリティを踏まえた事業のグローバル・ガバナンス構築の必要がある。
- ✓ 改めて「基本行動指針（共有・報告・公表）」に基づいた活動を徹底して欲しい。

つまり、経営者が危機意識を持ち、率先して社内だけでなく、事業領域全体におけるサイバーセキュリティ対策への取組が必要とのことである。

それでは、中小企業の経営者はどのような対応を取るべきか、サイバー攻撃の特性から考える必要がある。サイバー攻撃は、その種類によりセキュリティ対策の方法が異なる。単一の攻撃を防ぐだけでは情報セキュリティを担保することはできない。様々な攻撃から防御するためには、3つの「させない」（入口・出口・内部対策）を複合的に行う必要がある。

（1）侵入させない（入口対策）

「侵入させない」すなわち入口対策では、攻撃者や有害な Web サイトなどから配信される、インターネットを経由した不正侵入やウイルス付きのメールをブロックする。自社内に侵入をさせないことで攻撃を未然に防ぐ。

（2）外部通信させない（出口対策）

「外部通信させない」すなわち出口対策では、C&C サーバー（外部から侵入して乗っ取ったコンピューターを利用したサイバー攻撃で、踏み台のコンピューターを制御したり命令を出したりする役割を担うサーバーコンピューター）との通信をブロックする。侵入してしまったウイルスは、外部と通信することで更に拡散し被害を増大させる。例えば、感染した端末から機密情報を格納するサーバーにアクセスするなどの二次攻撃を行う。外部との通信をブロックすることで、情報を持ち出されるリスクを低減する。

（3）活動させない（内部対策）

「活動させない」すなわち内部対策では、端末のウイルス対策・脆弱性対策、世代管理バックアップ対策を行うことはもちろん、ネットワークの脅威監視・内部拡散防止を実行する。感染してしまった端末から更に拡散する等の活動をさせないことでウイルスの拡散を防ぐ。

上記が、会社としてサイバー攻撃に備える、予防措置、事後措置である。しかしそれだけでは不十分である。なぜなら、Emotet のような標的型攻撃（なりすまし）は従業員の不注意を利用して侵入を試みるからである。そのため、従業員のセキュリティ意識向上も重要な対策となる。

サイバー攻撃の第一歩はメールで行われることが増加している。特に標的型攻撃ではその手口も巧妙化しており、実在する企業のなりすましや業務に関係があることを装う件名や本文など、思わず開封してしまう巧みなメールになっている。

送信元が不明なメールは開かない、業務外の怪しい Web サイトにはアクセスしない。情報セキュリティポリシーに従って IT 部門がルールを定めても、従業員が遵守徹底しなければ企業はサイバー攻撃の脅威にさらされることになる。従業員にサイバーセキュリティ対策を意識付けし、行動規範を遵守させなければならない。e ラーニングや社内研修などを通じて情報の取り扱い方を教育し、徹底することがサイバーセキュリティ対策の重要な鍵となる。従業員に対する継続的なサイバーセキュリティ対策教育や、部門ごとにセキュリティ管理者を決めて定期的なチェックの実施、新入社員向け研修にサイバーセキュリティ対策を組み込み、情報保護に厳しい会社であると入社時から意識付けすることなどが効果的である。

座学による研修に加え、実施訓練も有効な手立てとなる。実際にサイバー攻撃を受けることで、従業員自らの意識レベルを認識し、さらなる意識向上につながる。実施訓練としては、Emotet、フィッシング詐欺など、実際の攻撃をモデルとして、従業員に模擬攻撃を行い、その結果をもとに個人や部署ごとのセキュリティレベルをスコア化する。スコアに合わせて、従業員に必要な教育を再度受講させ、意識の徹底を図る。

このように、企業では、システム環境面での対策、従業員の意識改革面における対策の両面から取り組む必要がある。システム環境面は即時対応可能だが、従業員の意識改革には時間を要すると考えられるため、まずはシステム環境のセキュリティ対策を整備し、そのうえで従業員教育を徹底することが効果的である。

2. 実証開始時の北海道内における中小企業のセキュリティ対策の現状

2.1 北海道における実証事業の概要

2.1.1　背景

近年、サプライチェーン全体の中で対策が弱い中小企業を対象とするサイバー攻撃やそれに伴う大企業等への被害が顕在化してきているものの、多くの中小企業は IT やサイバーセキュリティに関する知識が乏しく、IT に関するトラブルが発生した際にシステムによる不具合が原因なのか、サイバー攻撃が原因であるか自社で判断することが困難な状況である。

上記の情勢を鑑み、中小企業の実態やニーズに合致した持続可能なセキュリティ対策支援体制を構築し中小企業に活用してもらうことで、中小企業のセキュリティ対策強化を図る。

2.1.2　実証の目的

中小企業の実態に合ったサイバーセキュリティ対策の定着のため、持続可能な中小企業サイバーセキュリティ対策支援体制を構築すること。

2.1.3　地方圏を選定した実証について

3 大都市圏と地方圏を比較した場合、サイバーセキュリティセミナー等の啓発機会や、サイバーセキュリティ対策支援企業数（技術者の要員数）は少ないと想定する。

地方圏におけるサイバーセキュリティの取組は日本全体のサイバーセキュリティ対策向上につながる重要課題であり、2019 年 4 月に経済産業省「産業サイバーセキュリティの加速化指針」で示されたアクションプランと合致する。

それらを踏まえ、啓発機会や専任人材が少ない地方圏にて本実証を実施することにより、様々な地域でのモデル化が可能である。

2.1.4　北海道での実証について

①産業特性から

平成 28 年経済センサス（※1）によると、地方圏の中で北海道は事業所数が最も多く、特に”第一次産業““観光業”において独自性を有しており、日本を代表する産業となっている。

第一次産業では、全国の第一次産業全体の 12%を北海道企業が占め、食品工業では製品出荷額・事業所数ともに全国一位、更にそれらを取り巻く運輸・建設・卸売業等のサプライチェーンが、道内外の多くの企業によって構築されており、「日本の食料基地」として全国各地域とのつながりが深く様々な影響があると考える。

観光業では、訪日外国人の 1 割ものシェアを持ち、国内客にも人気が高い観光地を中心とした宿泊業や小売業等多数の中小企業による産業構成を確立、特に 2020 年は道内 7 空港民営化が始まり、各空港からの MaaS 構築の検討等、北海道の観光業はさらなる進歩を目指している。

そのため、道内外の関連産業・企業とのサプライチェーンに及ぼすセキュリティリスク影響等を検証可能である。

②地域特性から

北海道の面積は 83,424 平方キロメートルで日本全体の 22%を占める。広大な地域ではあるが人口・産業は札幌一極集中の色が極めて濃くなっている。

札幌を除く地方圏においては、旭川市や函館市、苫小牧市、帯広市など人口 10 万人を超す中核都市が点在、経済圏を形成しており、その特徴はまさに「札幌一極集中+超広域分散型」であり、「小さな日本」ともいうことができる。

そのため、大都市型・地方型双方の地域特性を持つ北海道での実証は、道内外を問わず、今後のさらなる広域展開を考慮した取組を推進することにつながる。

③セキュリティ意識から

北海道は産業特性で記載した通り、日本有数の第一次産業シェアを持つ。その特性から、近年は農業・漁業等に ICT を積極的に活用して産業振興、後継者不足といった課題に取り組んでいる。

ICT 利活用により一層の生産性向上に寄与できる第一次産業中心のサプライチェーンや観光業のほか、ワーケーションにおいても更なる ICT 普及を推進している。しかしながら、民間セキュリティ事業者の調査によると、「セキュリティ対策を業務運営・組織運営のリスクと認識しているか」との問いに対し、全国よりも北海道の方が「認識していない・分からない」と回答した事業者の割合が高く（全国平均 25%、北海道 41%）、リスク認識不足が著しいため今後改善の余地があるため北海道の企業のセキュリティ意識向上は急務かつ必須である。

2.1.5　実証期間

2020 年 10 月 1 日～2020 年 12 月 31 日

2.1.6　実証参加企業

①実証参加企業数：143 社（当初目標：100 社）

②実証参加企業募集活動

以下の方法により実証参加企業を募った。当初は 100 社程度の参加募集を見込んでいたところ 171 社から参加申込を受け、最終的に 143 社の中小企業が実証事業に参加した。特に NTT 東日本

北海道事業部の顧客基盤から 165 社の参加申込を受けた。

それぞれの詳細内容は以下のとおり。

・セキュリティセミナーおよび説明会による募集

新型コロナウイルスの影響により集合形式の説明会自体が敬遠されたことから、説明会参加企業数は当初の目論見である 3 日程合計の 150 社を大きく下回った。また、説明会に参加した 24 社のうち 5 社から実証事業の参加申込を受けた。説明会の概要は以下のとおり。

＜開催日程＞

2020 年 9 月 9 日（水）10:00～11:00（北海道経済センター＋オンライン）

2020 年 9 月 30 日（水）10:00～11:00（北海道経済センター＋オンライン）

2020 年 9 月 30 日（水）14:00～15:00（北海道経済センター＋オンライン）

＜実証参加企業数＞

24 社、29 名（全 3 日程の合計）

＜説明会内容＞

サイバーセキュリティセミナー（企業を取り巻く情報セキュリティ環境について）

サイバーセキュリティお助け隊実証事業概要

SECURITY ACTION に関する概要説明（IPA）

＜説明会への募集方法＞

- 地域団体、連携する法人団体への勧奨による募集
  日本電信電話ユーザ協会、札幌商工会議所をはじめとした商工会議所と連携し、各団体の発行する情報誌やメルマガにて募集を募った。
- NTT 東日本北海道事業部の顧客基盤への勧奨による募集
- HAISL（北海道地域情報セキュリティ連絡会）加盟団体の関連企業への勧奨による募集

・NTT 東日本北海道事業部、東京海上日動、北洋銀行の顧客基盤への勧奨による募集

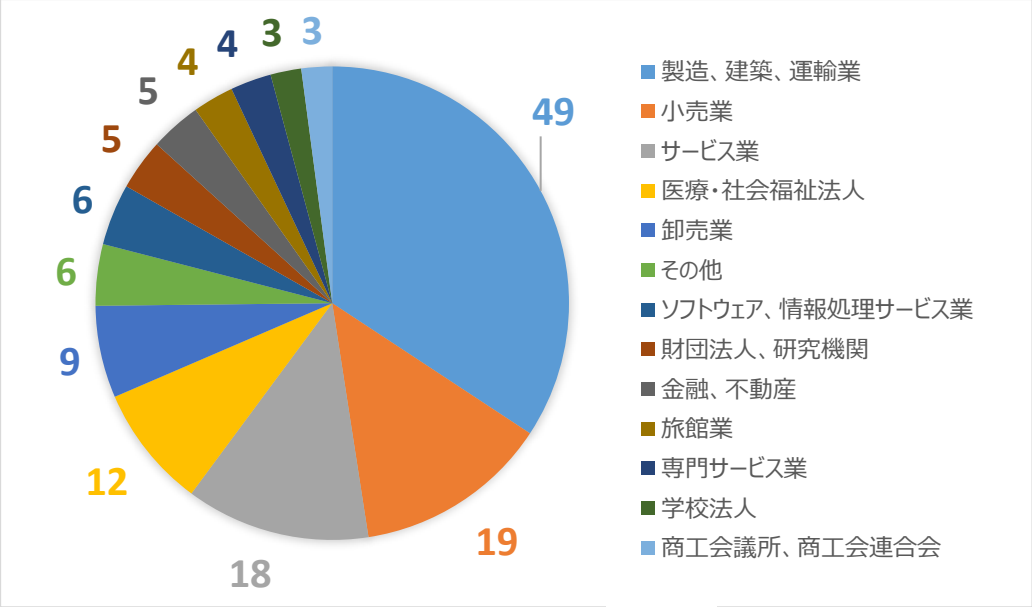
それぞれの顧客基盤へのアプローチにより、合計 166 社より参加申込を受けた。

特に NTT 東日本北海道事業部の顧客基盤からの募集が効果的であった要因として、現時点でサイバーセキュリティ対策に興味を示している中小企業を中心に募集をかけたことがあげられる。

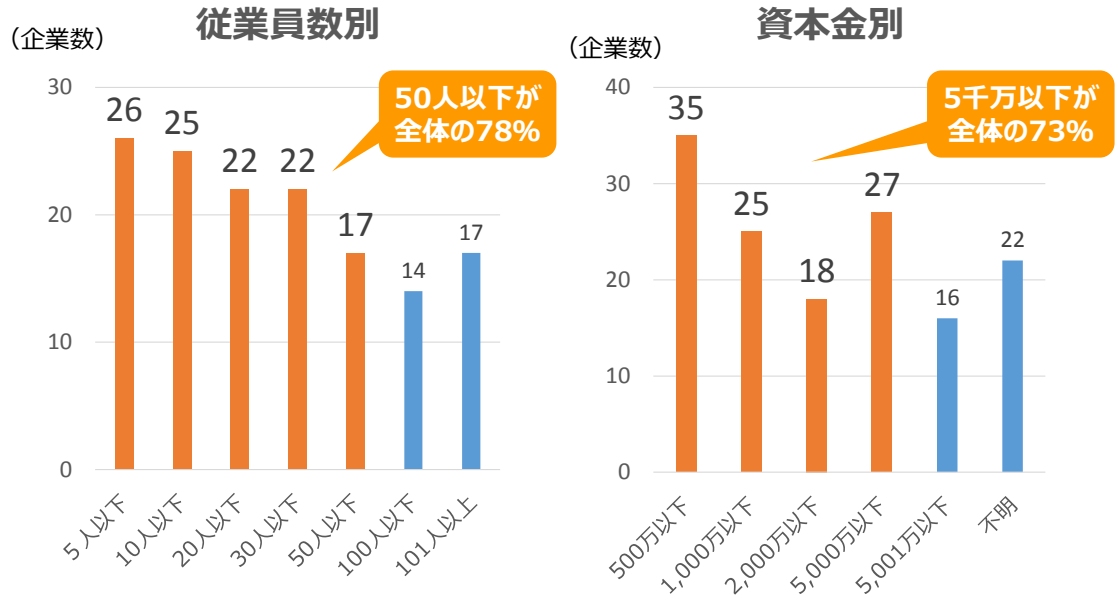
③実証参加企業の属性

実証参加企業の 143 社の業種は下図のとおり。

「製造、建築、運輸業」「小売業」「サービス業」で 60%程度を占める。



実証参加企業の従業員は下図のとおりである。



業種および企業規模から見ても、当初見込み通りの企業が実証参加した。

2.1.7　提供サービス概要

本実証事業においては、以下の 4 つのサイバーセキュリティ対策サービスを提供し、一元的な問合せ窓口となるセキュリティサポートデスクを設置する。

- セキュリティ対策機器（UTM）
- 標的型攻撃メール訓練（メールセキュリティ対策）
- Web の脆弱性診断（ホームページ脅威の診断）
- 情報セキュリティ e ラーニング（スキル醸成）

2.2 導入済サービスと割合

2020 年 10 月から、北海道における中小企業のセキュリティ対策の調査を行うにあたり、各企業のセキュリティの現状を把握すべく、アンケート調査を行った。

2.2.1　アンケート内容

＜対象者＞　説明会参加企業・実証参加企業
＜回答数＞　73 社
＜実施日＞　2020 年 10 月 1 日～12 月 31 日の期間で実施

＜実証開始時アンケート内容＞

Q1.サイバーセキュリティ対策に関心をお持ちですか
1.　すぐにでも、検討しようと思った
2.　とても関心があり、いずれ検討しようと思った
3.　関心はあるが、検討するかは分からない
4.　関心はない

Q２．ご存知のセキュリティ脅威がございましたらお答え願います。（いくつでも）
1.　標的型攻撃による機密情報の窃取
2.　内部不正による情報漏えい
3.　ビジネスメール詐欺による金銭被害
4.　サプライチェーンの弱点を悪用した攻撃
5.　ランサムウェアによる被害
6.　予期せぬ IT 基盤の障害に伴う業務停止
7.　不注意による情報漏えい
8.　IoT 機器の不正利用
9.　妨害攻撃によるサービスの停止
10.　インターネット上のサービスからの個人情報の窃取

Q3. 貴社で過去に被害のあったセキュリティ脅威がありましたらお答え願います。（いくつでも）

1. 標的型攻撃による機密情報の窃取
2. 内部不正による情報漏えい
3. ビジネスメール詐欺による金銭被害
4. サプライチェーンの弱点を悪用した攻撃
5. ランサムウェアによる被害
6. 予期せぬ IT 基盤の障害に伴う業務停止
7. 不注意による情報漏えい
8. IoT 機器の不正利用
9. 妨害攻撃によるサービスの停止
10. インターネット上のサービスからの個人情報の窃取

Q4. 貴社で導入しているサイバーセキュリティ対策をお教えください。（いくつでも）

1. ウイルス対策ソフト
2. 出入口対策
3. 社員教育
4. セキュリティ管理者の設置
5. セキュアな無線環境
6. セキュアな拠点間通信
7. 重要なファイルのバックアップ
8. サイバーリスク保険加入
9. セキュリティポリシーの策定

Q5. 貴社で今後導入を検討しているサイバーセキュリティ対策をお教えください。（いくつでも）

1. ウイルス対策ソフト
2. 出入口対策
3. 社員教育
4. セキュリティ管理者の設置
5. セキュアな無線環境
6. セキュアな拠点間通信
7. 重要なファイルのバックアップ
8. サイバーリスク保険加入
9. セキュリティポリシーの策定

Q6. 現在セキュリティ対策にかけている月額費用はいくらぐらいですか。

1. 3,000 円以下

2. 3,000 円～5,000 円
3. 5,000 円～10,000 円
4. 10,000 円～20,000 円
5. 20,000 円～
6. 費用はかけていない

Q7. 今後セキュリティ対策にかける月額費用はいくらぐらいを見込んでいますか。

1. 3,000 円以下
2. 3,000 円～5,000 円
3. 5,000 円～10,000 円
4. 10,000 円～20,000 円
5. 20,000 円～
6. 費用はかけていない

Q8. サイバーセキュリティ対策に関して、貴社の課題を教えてください

1. セキュリティポリシーの策定
2. 管理体制の構築
3. リスクの洗い出し、評価
4. グループ会社、取引先も含めた対策の実施
5. セキュリティ対策費予算の確保
6. セキュリティ対策専門人材の確保
7. インシデント発生時の体制の構築
8. 情報収集（最新技術動向や事故事例）
9. なし

Q9. 以下の項目の中で、過去に貴社の取引先企業から実施を義務付けられたものがあれば教えてください（いくつでも）

1. ウイルス対策ソフト
2. 出入口対策
3. 社員教育
4. セキュリティ管理者の設置
5. セキュアな無線環境
6. セキュアな拠点間通信
7. 重要なファイルのバックアップ
8. サイバーリスク保険加入
9. セキュリティポリシーの策定
10. SECURITY ACTION の自己宣言

Q10. 貴社は現在テレワークを導入していますか

1. 導入している（週 3 日以上）
2. 導入している（週 1～2 日程度）
3. 導入していない

Q11. （Q10 で「導入している」と回答された方に伺います）実施しているセキュリティ対策や運用ルールがあれば教えてください（自由回答）

Q12. （Q10 で「導入していない」と回答された方にお伺いします）テレワーク導入に関する懸念事項があれば教えてください（自由回答）

Q13. 業務で利用されているサービスについて教えてください

＜ストレージサービス＞

1. Microsoft365（OneDrive）
2. Google Workspace※（Google ドライブ）
3. Dropbox
4. Box
5. その他
6. 利用なし
7. わからない

Q13. 業務で利用されているサービスについて教えてください

＜WEB 会議＞

1. Microsoft365（Microsoft Teams）
2. Google Workspace※（Google Meet）
3. Zoom
4. Cisco Webex
5. その他
6. 利用なし
7. わからない

Q14. Q13 で「利用なし」をお選び頂いた方にお伺いします。今後クラウドサービスを導入される予定はありますか

1. 検討予定あり
2. 検討していない
3. わからない

Q15. 検討しているクラウドサービスについて教えてください （差支えなければ導入予定サービスがお決まりの場合、サービス名もご記入ください）

1. メールサービス
2. ストレージサービス
3. WEB 会議
4. スケジュール管理
5. チャット

2.2.2 アンケート回答企業の属性

アンケート回答企業 73 社の規模は以下のとおり。

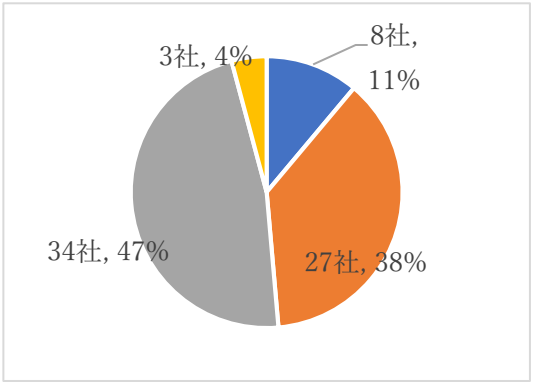
表 2 企業規模ごとの回答企業数

企業規模	回答企業数（社）
~20 名	40
21 名~100 名	25
101 名~	8

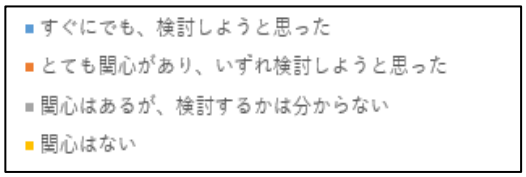
2.2.3 個別回答結果

① Q1：サイバーセキュリティ対策に関心をお持ちですか

サイバーセキュリティに関しては、回答会社の 49%が関心を持ち、対応を検討している。企業規模に比例して、対応を検討している企業の割合は高くなっている。
しかし、いずれの企業規模においても「いずれ検討」（オレンジ）が、「すぐにでも検討」（ブルー）を上回っており、サイバーセキュリティ対策の必要性を感じつつも、まだ喫緊の課題として認知されていないことが見受けられる。以下に企業規模ごとの回答の割合を示す。



＜凡例＞



＜図の数字＞
社数、割合（%） 以下円グラフは同様

図 1 サイバーセキュリティ対策への関心

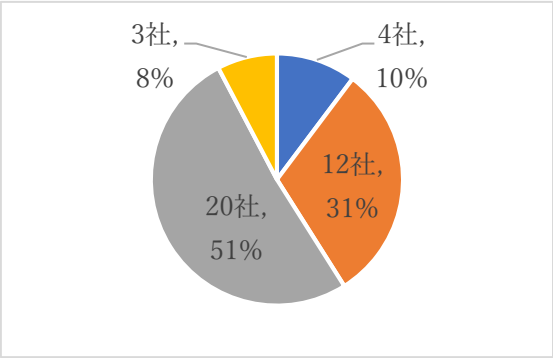


図 2 Q1 への回答（~20 名）

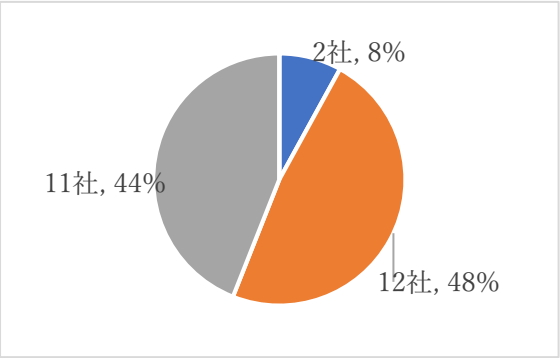


図 3 Q1 への回答（21 名~100 名）

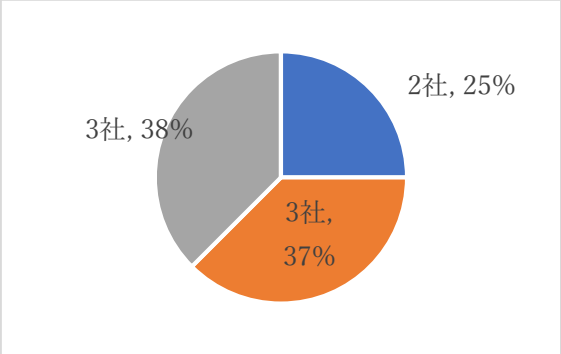


図 4 Q1 への回答（101 名~）

② Q2：ご存知のセキュリティ脅威がございましたらお答え願います。（いくつでも）

主要なセキュリティ脅威について、企業の認知度を確認した。メールも含む、ネットワーク環境を利用したセキュリティ脅威の認知度が高かった。その反面、IoT 機器の不正利用や、サプライチェーンの弱点を悪用した攻撃に対する認知度は低いという結果が出た。これは、各企業が事業でネットワーク環境を利用しているものの、業務の DX 化は進んでいないため、業務ツールや業務プロセスに関する脅威については脅威と捉えていない可能性が考えられる。

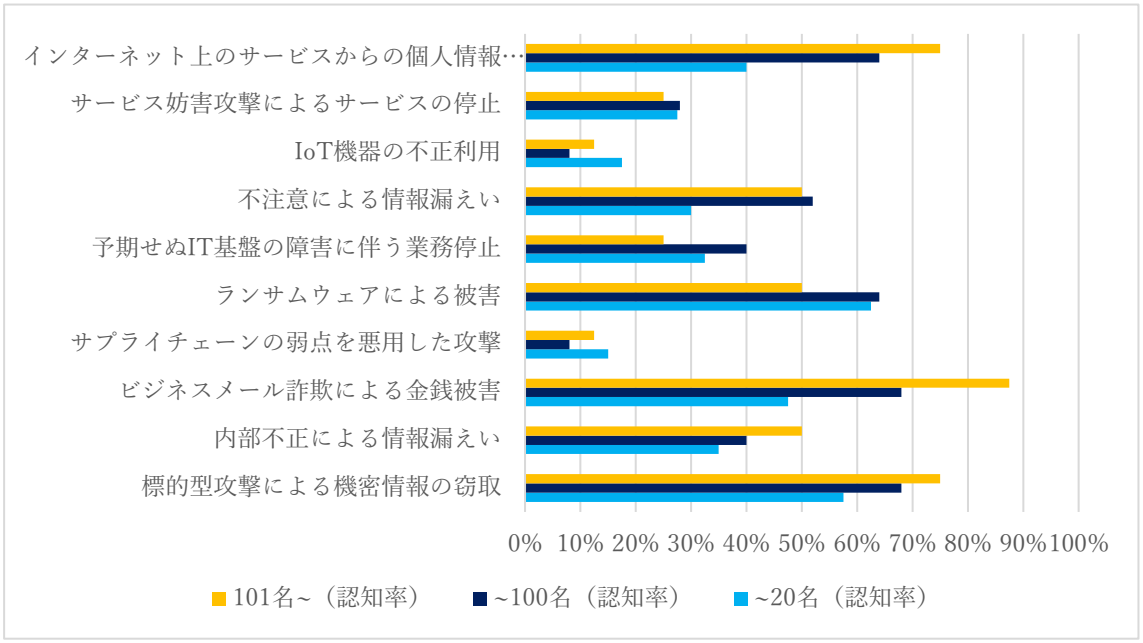


図 5 Q2 への回答

③ Q3：貴社で過去に被害のあったセキュリティ脅威がありましたらお答え願います。(いくつでも)

企業が被害にあったセキュリティ脅威としては、101 名以上規模の会社におけるランサムウェアによる被害が突出している。メール添付ファイルの不用意な確認、インターネットからのファイルダウンロード等が起因するものと考えられる。社員一人ひとりのセキュリティ脅威に関する教育が必要と考えられる。

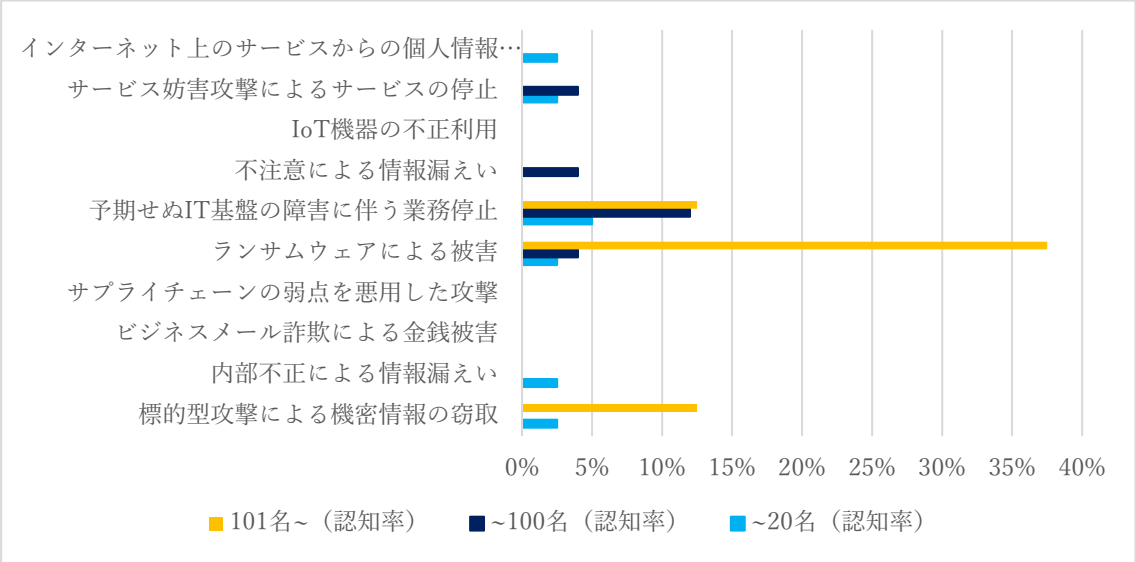


図 6 Q3 への回答

④ Q4：貴社で導入しているサイバーセキュリティ対策をお教えください。（いくつでも）

サイバーセキュリティ対策に関しても、企業規模が大きいほど対策が進んでいることが確認できた。中でも、重要なファイルのバックアップ、ウイルス対策ソフトの導入が進んでおり、101 名以上の企業は、全社導入している。100 名以下の企業でもウイルス対策ソフトの導入は 90%以上が導入しているという結果が出た。

システム対応は行っているものの、社員教育は企業規模問わず実施しているのは 20%以下で、社員教育のように長期的な対策については、コスト、時間、要員を投資するゆとりがないことがうかがえる。

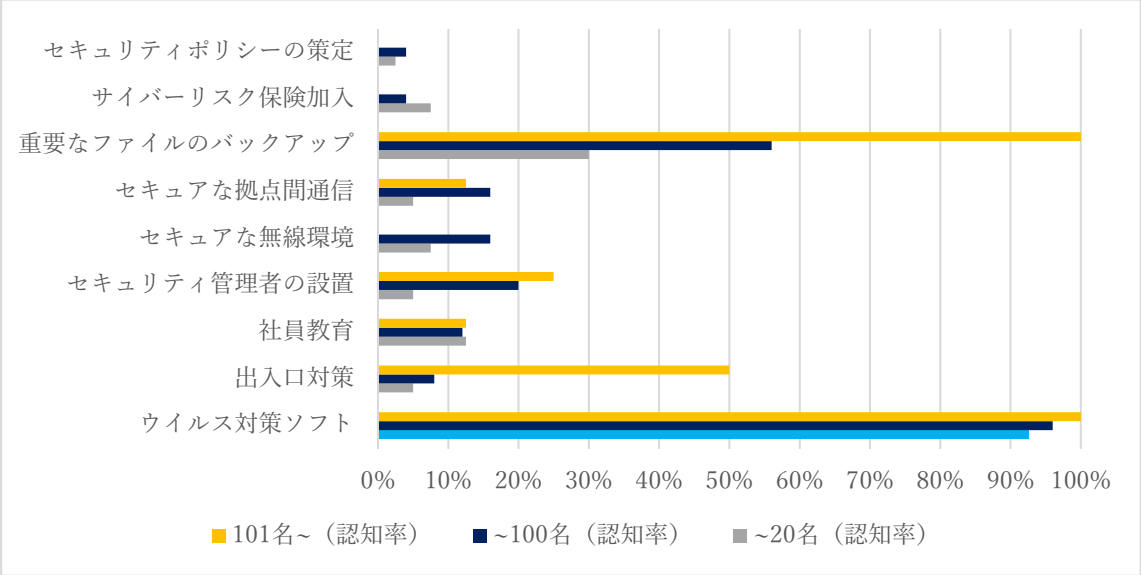


図 7 Q4 への回答

⑤ Q5：貴社で今後導入を検討しているサイバーセキュリティ対策をお教えください。(いくつでも)

ここでは、Q4 で既に導入しているサイバーセキュリティ対策に加えて、どのような対策で事業を防御しようと考えているのか、企業規模別に実装割合を確認した。

全体的には、ウイルス対策ソフトは全社対策の方針となった。社員教育や出入り口対策についても関心が高いことがうかがえる。

セキュアな拠点間通信やサイバーリスク保険加入への関心は低く、対策の難易度の低いもの、コストメリットを感じやすいものへの対応が優先されているという結果となった。

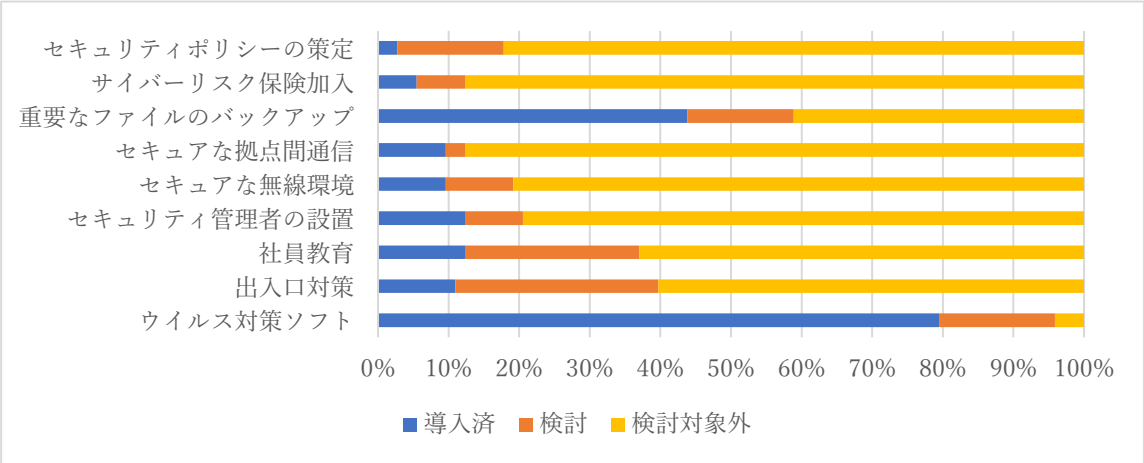


図 8 Q5 への回答（全体）

以降では、企業規模ごとの傾向を確認する。

20 名以下の企業では、現時点、対応していないことが多く、検討対象も大きい割合となった。101 名以上の企業で完全導入しているファイルのバックアップやウイルス対策ソフトの導入を検討している企業が多く、企業規模の大きい企業を模範に対応を検討していると考えられる。

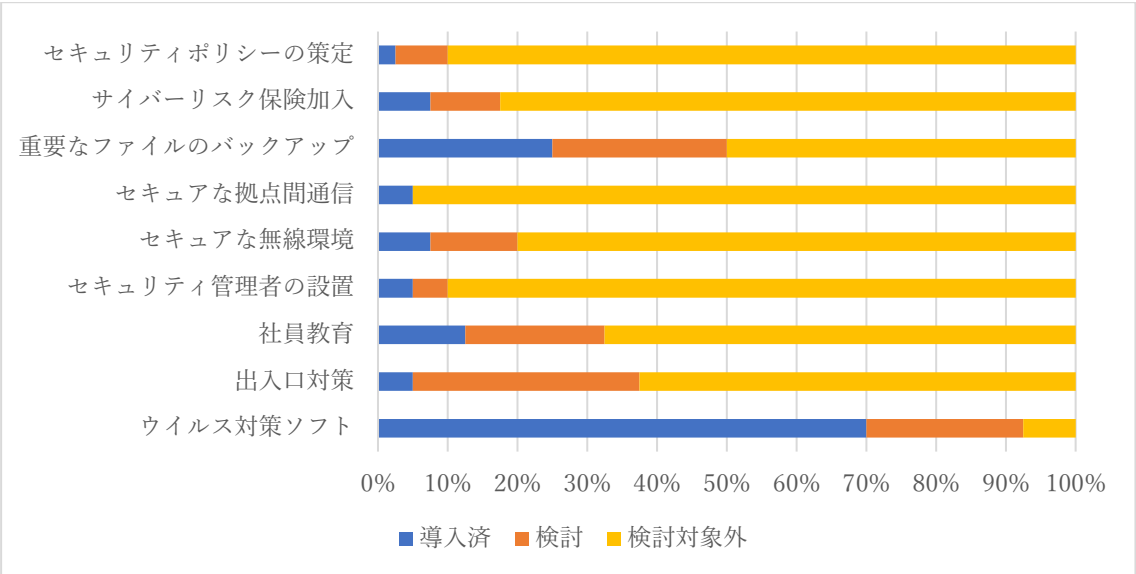


図 9 Q5 への回答（~20 名）

21 名~100 名以下の企業では、101 名以上の企業で完全導入しているファイルのバックアップについては、実施する企業は既に取り組み済みと考えられる。ウイルス対策ソフト導入は全社検討となった。社員養育、出入り口対策への関心の高さがうかがえる。

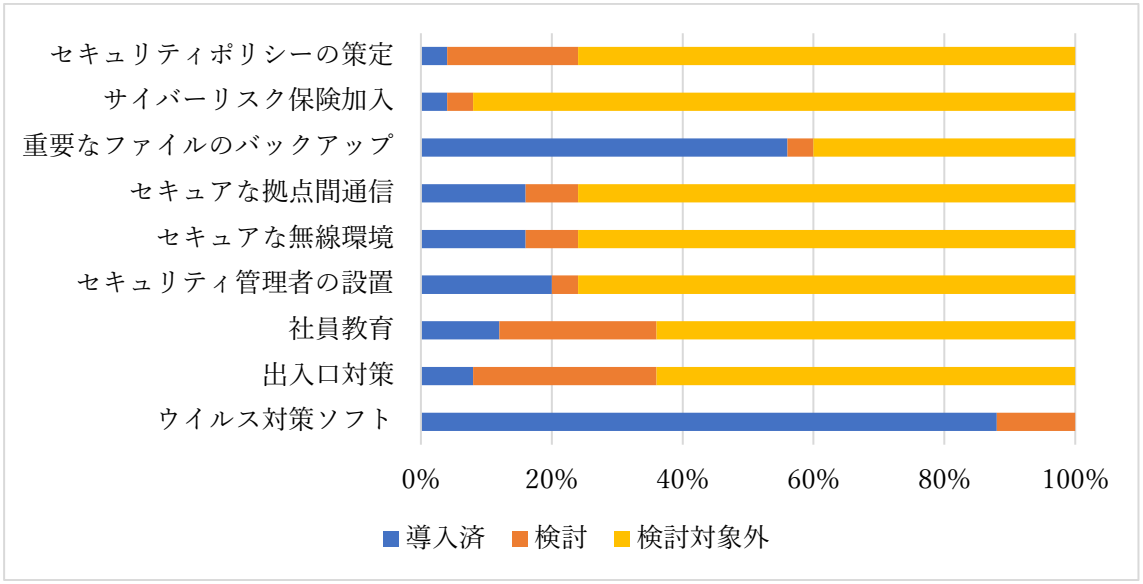


図 10 Q5 への回答（21~100 名）

101 名以上の企業では、システム的な対応の実装よりも、セキュリティポリシーの策定、セキュリティ管理者の設置、社員教育といった、内部統制を検討している傾向となった。

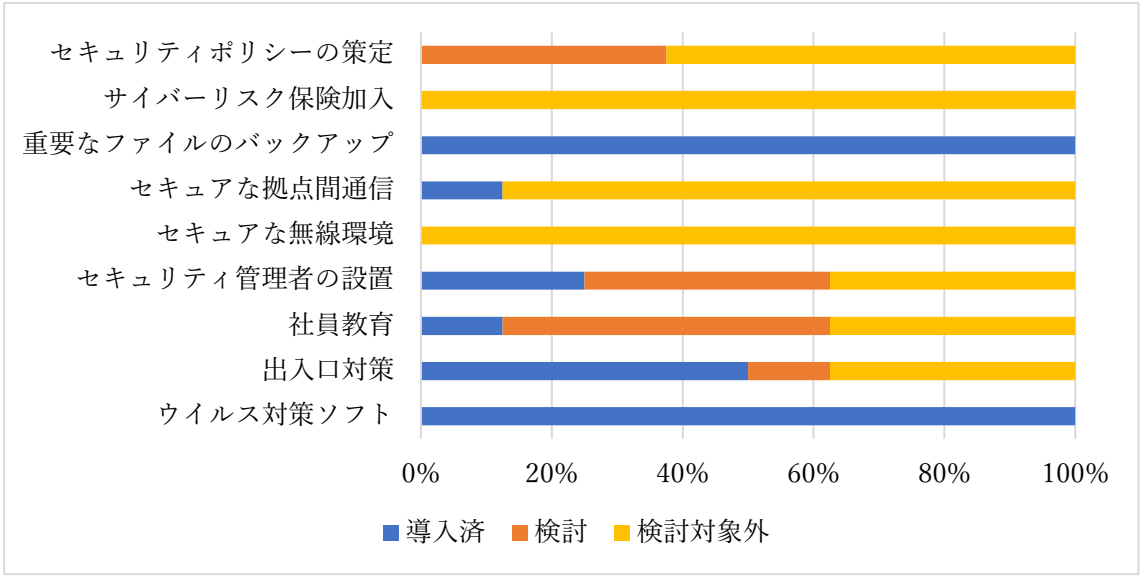


図 11 Q5 への回答（101 名~）

⑥ Q6：現在セキュリティ対策にかけている月額費用はいくらぐらいですか。

セキュリティ対策コストは、企業規模に比例すると考えられるため、全体統計は割愛し、企業規模ごとにその傾向を確認する。

20 名以下の企業の投資額は、
費用をかけない企業も含め 5000 円未満が 78%を占めた。

セキュリティ対策に取り組む資金のゆとりがないこと、セキュリティ対策の即時性が期待できない（狙われる対象ではないとの思い込み）があり、投資に対して消極的になっているものと考えられる。

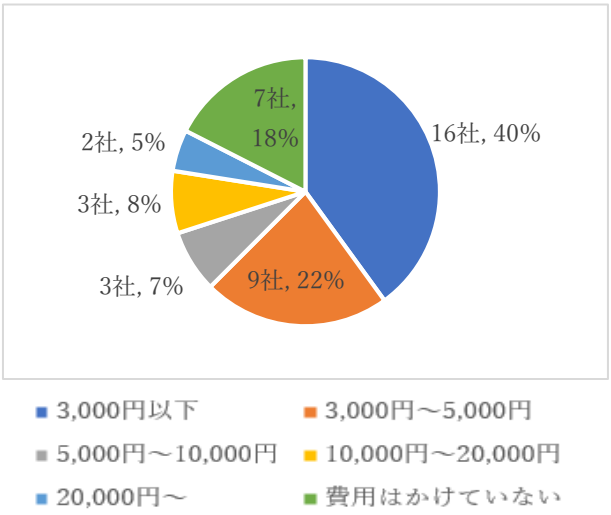


図 12 Q6 への回答（~20 名）

21 名以上 100 名以下の企業では費用をかけない企業は 10%未満、1 万円以上の費用をかける企業が 61%となる。しかし、費用 3 千円未満の企業も 22%であり、企業のポリシーによって投資金額は異なることが確認できる。

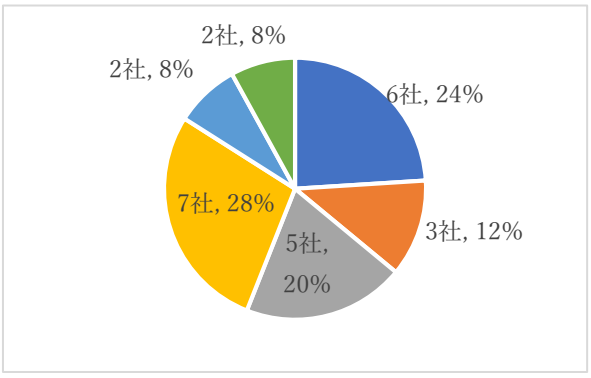


図 13 Q6 への回答（21~100 名）

101 名以上の企業では、費用をかけない企業はなく、63%の企業
が 2 万円以上をセキュリティ対策に投資している。セキュリティ対策への投資が 2 万円未満の会社は分散しており、多くの企業がセキュリティ対策費用の必要性を認識し、実施していることが確認できる。

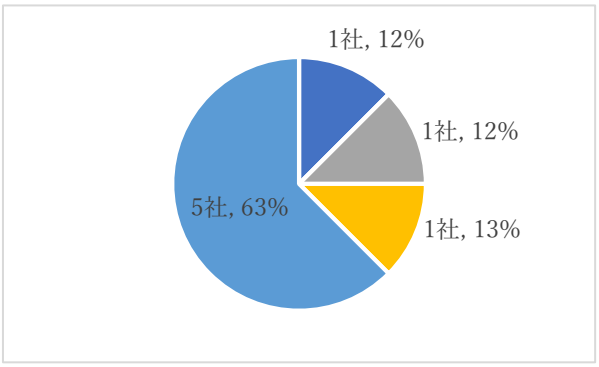


図 14 Q6 への回答（101 名~）

⑦ Q7：今後セキュリティ対策にかける月額費用はいくらぐらいを見込んでいますか。

当該アンケートに関しては、101 名以上の企業も含め、投資しないと回答する企業が存在する。おそらく、現状に加えた追加費用と捉えた企業と、今後の投資額と捉えた企業が混在すると考えられる。

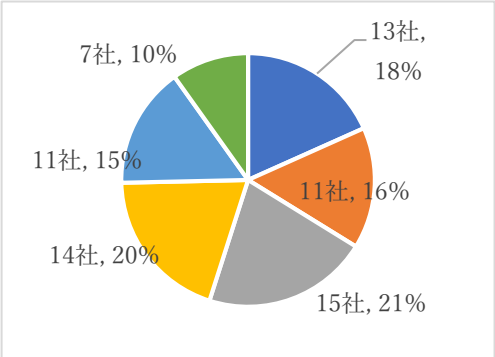


図 15 Q7 への回答（全体）

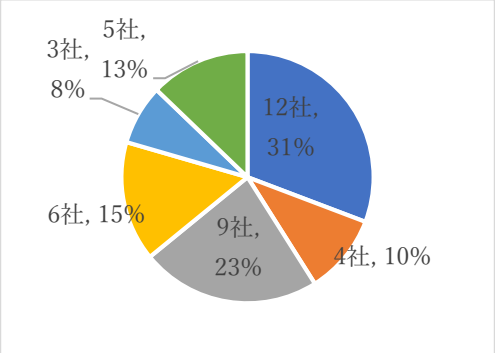


図 16 Q7 への回答（~20 名）

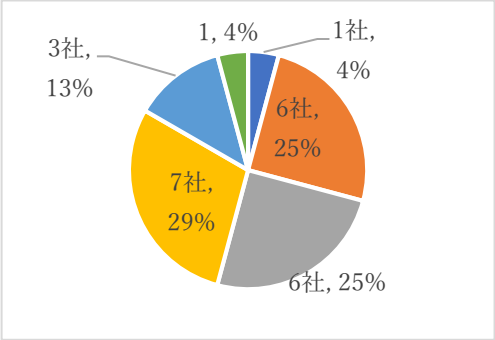


図 17 Q7 への回答（21~100 名）

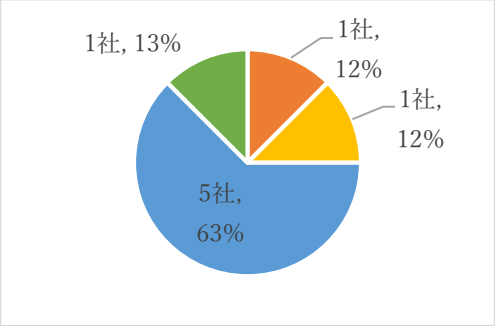


図 18 Q7 への回答（101 名~）

＜凡例＞

⑧ Q8：サイバーセキュリティ対策に関して、貴社の課題を教えてください

サイバーセキュリティ対策に関する課題認識に関しても、規模が大きい企業のほうが認識しているという結果となった。管理体制の構築は、企業規模問わず課題と認識しており、各社とも、対策を推進するための体制づくりが必要と考えている。101 人以上の企業については、インシデント発生時の体制の構築や、セキュリティ対策専門人材の確保も高い比率で課題と認識しており、リソース不足が問題であると考えられる。

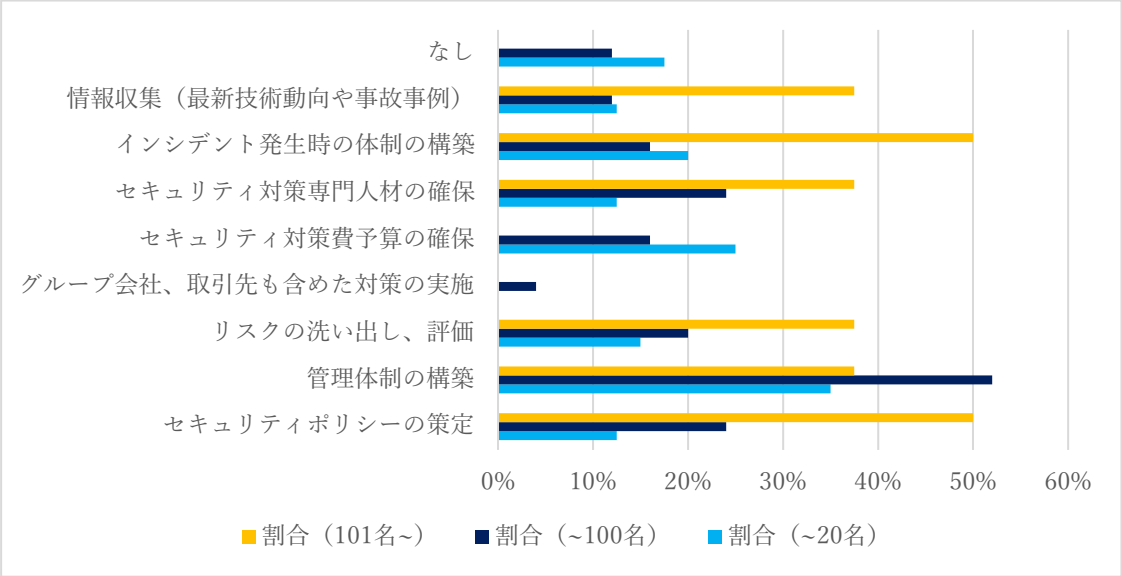


図 19 Q8 への回答

⑨ Q9：以下の項目の中で、過去に貴社の取引先企業から実施を義務付けられたものがあれば教えてください（いくつでも）

アンケートの回答を見る限り、取引先からセキュリティ対策を詳細に指示されている企業は少ないことが見受けられる。ウイルス対策ソフトに関しても、義務付けられている企業は少なく、多くの企業が自発的にセキュリティ対策を行っており、サプライチェーン（バリューチェーン）上の統制は取られていないことがうかがえる。

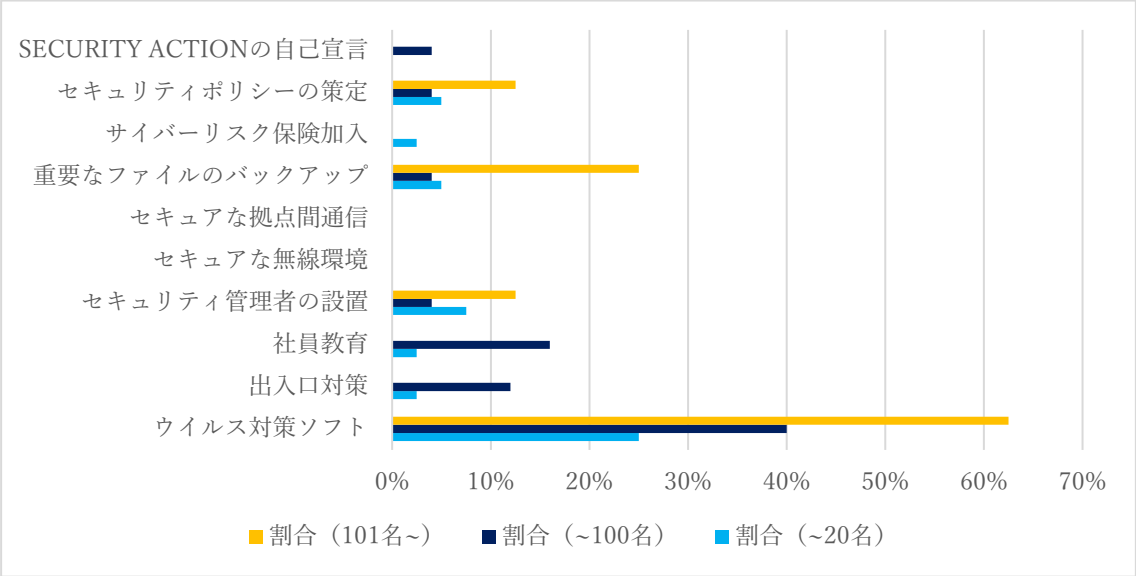


図 20 Q9 への回答

⑩ Q10：貴社は現在テレワークを導入していますか

テレワークを導入している企業は全体で８社、11%と低い。中小企業は、物流や生産ラインに従事するケースが多く、製品を直接取り扱う比率が高い。そのため、テレワークを導入するメリットを感じにくいこと、テレワークに対する投資余力がないことを主要因として、テレワークの導入が進んでいないと考えられる。

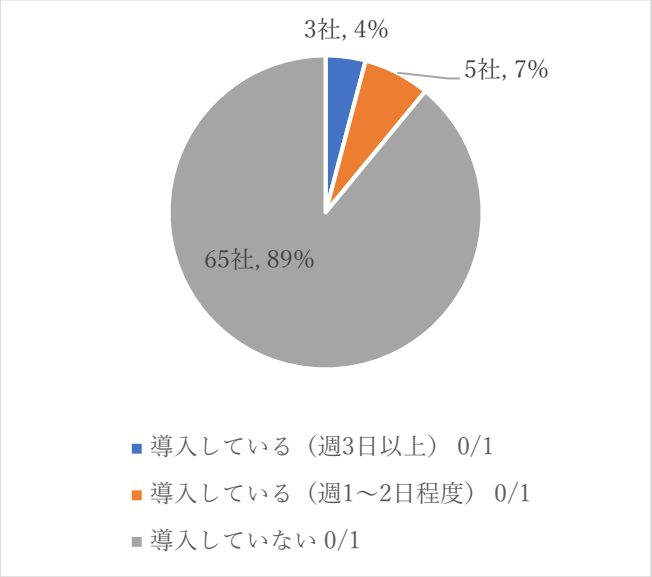


図 21 Q10 への回答

⑪ Q11：(Q10 で「導入している」と回答された方に伺います）実施しているセキュリティ対策や運用ルールがあれば教えてください（自由回答）

実施した企業は、取り急ぎ対応を優先し、制度化、セキュリティは今後の対応になっている場合が多い。以下、コメントをそのまま記載。

- ✓ 機密保持契約書の取り交わし
- ✓ VPN 接続の弱点をつかれる
- ✓ リモートアクセス（VPN）の導入
- ✓ テレワークは一部の社員が行っています。運用ルールは今後策定する予定です

⑫ Q12：(Q10 で「導入していない」と回答された方にお伺いします）テレワーク導入に関する懸念事項があれば教えてください（自由回答）

テレワーク導入への懸念は、業務上の対応が困難、インフラ・セキュリティ面での不安に大別される。以下コメントをそのまま記載。

- ➢ 業務特性
  - ✓ 貨物自動車運送業なので、乗務員への指示や配車、荷主・下請けからの電話対応など、テレワーク導入には厳しい状況にある
  - ✓ 社内の書類が見られないので難しい
  - ✓ 当社業務内容がテレワークに不向きである
  - ✓ 現在必要としてないため、今後は状況により必要となれば導入する
  - ✓ 業種的にムリ

- ✓ 製造業なので、テレワークでは仕事にならない
- ✓ 対面で接客することが多いので、基本なしです
- ✓ テレワークで対応できる業務がほぼない
- ✓ 業務上難しい
- ✓ 業務的に該当しない

➢ インフラ、セキュリティ

- ✓ パソコンがデスクトップである
- ✓ テレワークに関する規定が無い
- ✓ ハードウェア的に対応出来ていない
- ✓ セキュアな院内インフラの構築を最優先にしています
- ✓ クラウドでのデータ保存等やセキュリティの知識が不足している
- ✓ 現状の人員や業務内容ではテレワークの導入は困難な状況である
- ✓ データの管理とバックアップ
- ✓ ネットワークの構築導入に向けての社員教育
- ✓ 費用・設備・環境・管理
- ✓ 機器の設定、テレワーク用ソフトの導入
- ✓ 1.テレワークに対応できる社内制度づくり　2.情報漏えいなどのセキュリティ対策　3.情報セキュリティについての社員教育
- ✓ 情報流出・紛失
- ✓ 設備投資に対する費用対効果

➢ その他

- ✓ テレワークの導入予定がない
- ✓ テレワークは必要ないから
- ✓ 色々な弊害がありすぎて今のところできない
- ✓ 個々の運用のレベル UP
- ✓ 自宅が事務所

⑬ Q13：業務で利用されているサービスについて教えてください

ア）ストレージサービス

ストレージサービスは、利用している企業が少ないという結果となった。テレワークを実施していないため、資料の管理は概ね社内サーバーで完結しているものと思われる。ストレージサービスに関しては、規模の小さい企業のほうが様々なツールを使っているという結果となった。これは、社内的な規制が緩く、無償ツールも積極的に使える環境にあることが想定される。

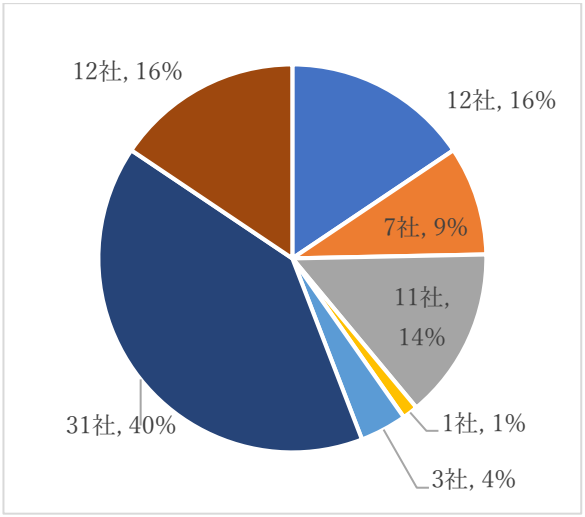


図 22 Q11（ストレージ）への回答（全体）

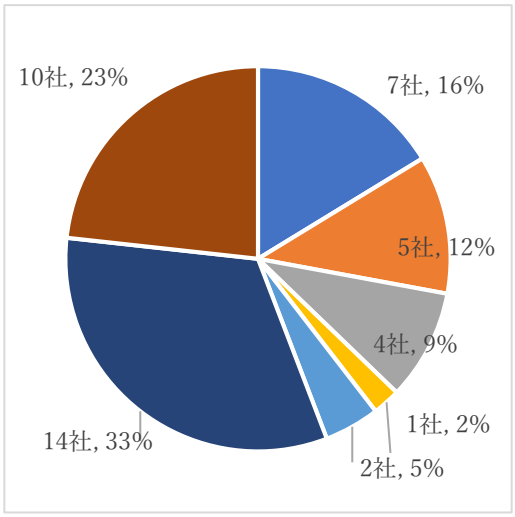


図 23 Q11（ストレージ）への回答（~20 名）

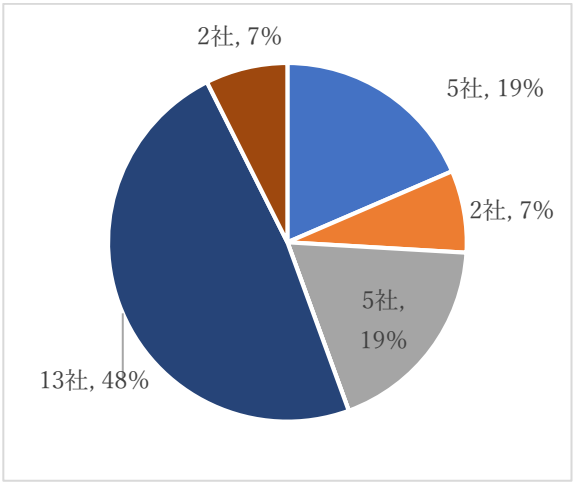


図 24 Q11（ストレージ）への回答（21~100 名）

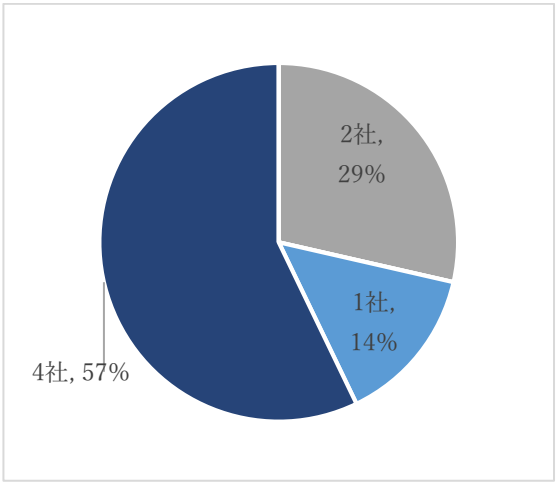


図 25 Q11（ストレージ）への回答（101 名~）

＜凡例＞

凡例以外のストレージサービス利用については以下（そのまま記載）。

- ✓ 取引先の専用ストレージサービス
- ✓ 外付け HDD
- ✓ iCloud drive

質問の捉え方によって、企業の回答がわかれた可能性がある。

イ）Web 会議

Web 会議は、全体では半分の企業が利用しているという結果となった。その中でも、規模が大きくなるに従って、利用率が高い状況であった。利用するツールは企業規模にかかわらず Zoom が最も多く、選定条件として、知名度、操作性、利便性が重視されていると考えられる。

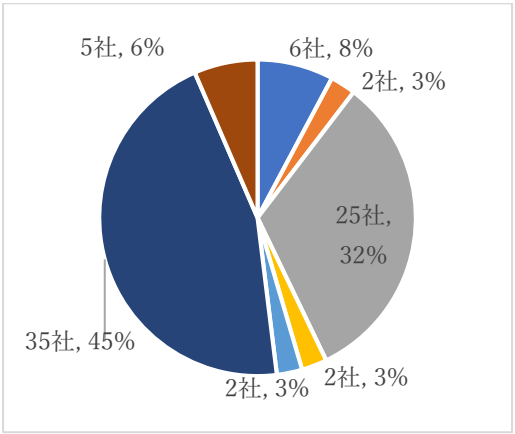


図 26 Q11（Web 会議）への回答（全体）

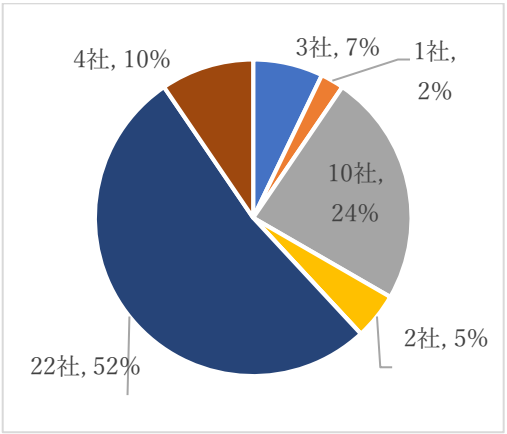


図 27 Q11（Web 会議）への回答（~20 名）

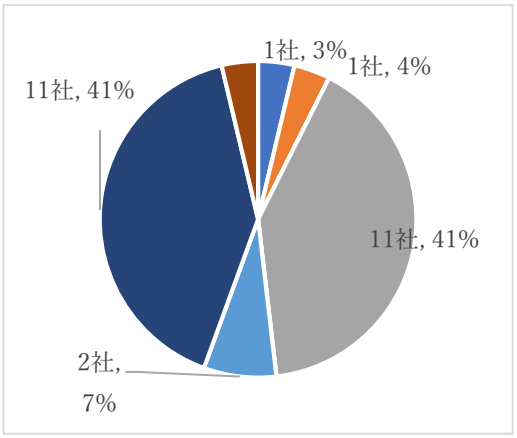


図 28 Q11（Web 会議）への回答（21~100 名）

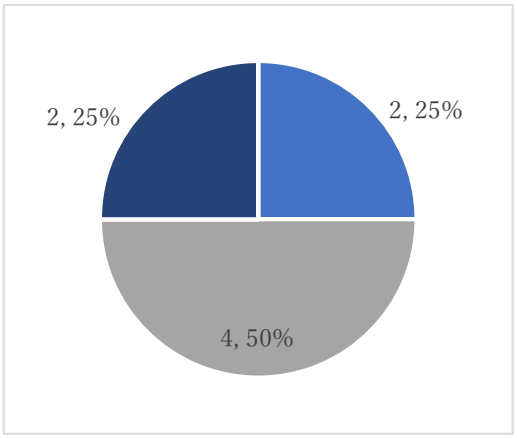


図 29 Q11（Web 会議）への回答（101 名~）

＜凡例＞

凡例以外のストレージサービス利用については以下（そのまま記載）。

- ✓ Skype　2 社

⑭ Q14：Q13 で「利用なし」をお選び頂いた方にお伺いします。今後クラウドサービスを導入される予定はありますか

現在、クラウドサービスを利用していない企業は、積極的なクラウド利用を考えていない場合が多い。これは、Q12 におけるフリーコメントの記載の通り、業務をクラウド化適用できるように見直す、IT 投資をする、といった対応を行う余裕がないことが原因と考えられる。

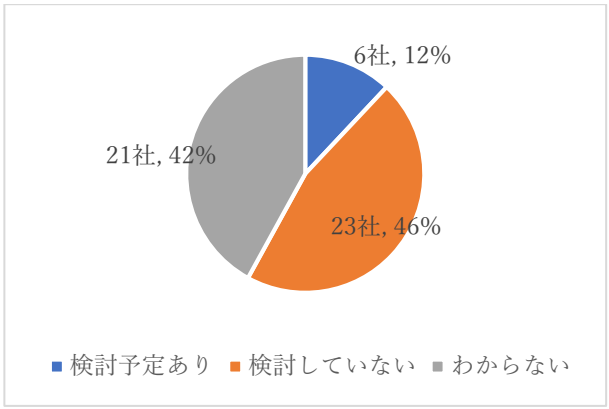


図 30 Q14 への回答（全体）

⑮ Q15：検討しているクラウドサービスについて教えてください （差支えなければ導入予定サービスがお決まりの場合、サービス名もご記入ください）

⑭で利用を検討しているクラウドサービスはストレージサービスや Web 会議との結果となった。各機能に対する製品名称は以下のとおり。

- チャット
  - ✓ Slack
- スケジュール管理
  - ✓ コメントなし
- Web 会議
  - ✓ コメントなし
- ストレージサービス
  - ✓ コメントなし
- メールサービス
  - ✓ コメントなし

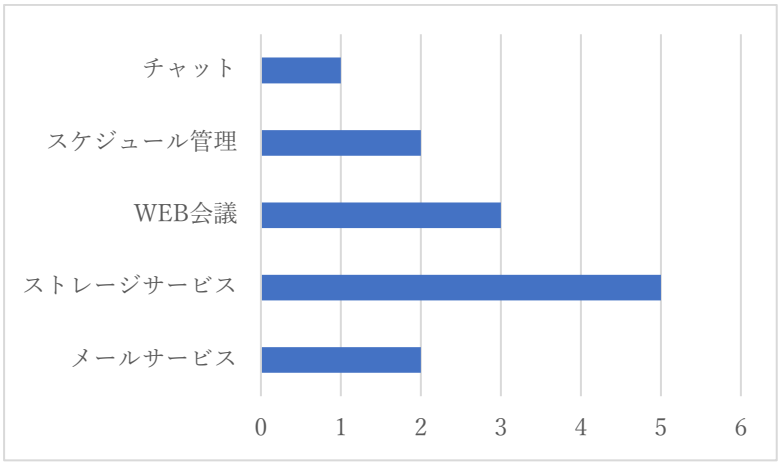


図 31 検討しているクラウドサービス

漠然と、導入したいと考えているものの、製品選定、導入の計画はできていない。

⑯ Q16：ご意見・ご要望を自由にご記入ください。（自由回答・任意）

フリーコメントが挙がってきたものは以下のとおり。

- ✓ セキュリティに対する知識が不足しており、専門家からの助言が必要な状態です。
- ✓ 中小企業では IT 系の専門家は少なく、総務などの者が兼務している状態だと思います。
- ✓ 実害があまり出ていない状態での費用捻出は難しく、経営層への説明もわかりやすく費用対効果が数字で分かるような説明がほしい所です。
- ✓ 小規模事業所でのテレワーク導入事例があれば情報提供いただきたい。
- ✓ 特にありませんが、当社のこの状態でセキュリティ対応大丈夫でしょうか？

2.3 サイバーセキュリティ対策の障壁把握

今回のアンケートにより、中小企業のサイバーセキュリティ対策の状況は概ね以下のとおりであることが確認できた。

- ✓ 主要なサイバーセキュリティ脅威は認識している。
- ✓ サイバーセキュリティ対策の必要性を感じている。
- ✓ セキュリティ脅威に直面した企業は少ないため、直面する課題との認識は低い。
- ✓ セキュリティ対策は限定的である（セキュリティソフト、バックアップ等が主な対策となっている）。
- ✓ セキュリティ対策への積極的な投資は考えていない企業が多い。
- ✓ セキュリティ対策の整備状況、意識は企業規模が大きいほど高まる。
- ✓ 更なるセキュリティ対策を検討する企業では、出入り口対策や社員教育を行う組織的な体制づくりを検討している。

このように、中小企業は、サイバーセキュリティに対する知識はあるものの、体制が未整備であること、ネットワークをインフラとして積極的に利用していない（現時点ではメールがコミュニケーションツールの主体）ことから、喫緊の課題としての危機感がないことが、サイバーセキュリティ対策が進まない要因と考えられる。

取引先企業からの外圧によりサイバーセキュリティ対策を求められる機会も少ない。中小企業は、限られた要員、予算での対応となるため、サイバーセキュリティ対策に十分なリソースを投入できていないのが実情である。特に従業員教育について、必要性は認めているものの、重要視されておらず、サイバーセキュリティ対策の定着化の障壁となっているものと考えられる。

この状況を打開するためには、企業自身によるサイバーセキュリティ対策への意識改革が求められると同時に、国や自治体からの更なるサポート（業種別、規模別ガイドラインの策定や、IT 専門家による助言、対応費用の助成等）により、企業の改革を支援することも検討の余地があると考えられる。

3. 実証開始時の中小企業における社員個々のサイバーセキュリティ意識の現状

3.1 サイバーセキュリティに関する知識の習得レベル

サイバーセキュリティ意識やリテラシーレベルの向上を目的に、2020 年 11 月 12 日から 2021 年 1 月 25 日までを受講期限として e ラーニングでは 2 つのコースを提供した。受講対象者は 429 名で、2021 年 1 月 13 日現在でのコースごとの受講者数および修了者数は以下表 3 のとおりである。

表 3 提供した e ラーニングの Web セキュリティ診断の実施結果

コース名	受講者数（割合[1]）	修了者数（割合[2]）
情報セキュリティの基礎	37 名（8.6%）	25 名（67.6%）
ケースで学ぶ！情報セキュリティの最新脅威 2020-2021 年版（標的型メール対応）	40 名（9.3%）	25 名（62.5%）

両コースとも講義の後に確認テストや総合テストに取り組む形で構成している。確認テストでの正答率は表 4 のとおりで、「情報セキュリティの基礎」の平均正答率は 92%、「ケースで学ぶ！情報セキュリティの最新脅威 2020-2021 年版（標的型メール対応）」の平均正答率は 78%だった。

表 4 提供した e ラーニングの Web セキュリティ診断の実施結果

「情報セキュリティの基礎」

カテゴリ	設問	正答率	カテゴリ	設問	正答率	カテゴリ	設問	正答率
確認テスト 1	1	87%	確認テスト 4	1	100%	総合テスト	1	69%
	2	83%		2	89%		2	96%
	3	93%		3	93%		3	96%
確認テスト 2	1	52%	確認テスト 5	1	100%		4	100%
	2	96%		2	85%		5	77%
	3	96%		3	100%		6	96%
確認テスト 3	1	93%					7	100%
	2	93%					8	100%
	3	100%					9	96%

[1] 受講対象者に占める受講者の割合を示す。受講者数は、コースにログインしたユーザーの数を指す。

[2] 受講者に占める修了者の割合を指す。修了者数は、コースを最後まで完遂した者を指す。

「ケースで学ぶ！情報セキュリティの最新脅威 2020-2021 年版（標的型メール対応）」

カテゴリ	設問	正答率	カテゴリ	設問	正答率
確認テスト 1	1	63%	総合テスト	1	8%
	2	100%		2	100%
確認テスト 2	1	96%		3	88%
	2	70%		4	81%
確認テスト 3	1	93%		5	38%
	2	70%		6	100%
確認テスト 4	1	78%		7	88%
	2	96%		8	81%

以下では正答率が低かった設問について紹介する。

まず、「情報セキュリティの基礎」では、確認テスト 2 設問 1、総合テスト設問 1、総合テスト設問 5 の計 3 問が特に正答率が低い設問であった。

確認テスト 2 設問 1

メールの誤送信について述べている次の文章で、間違っているものをすべて選びなさい。

A) 複数の相手に送信する場合、受信者のメールアドレスを知られたくない場合は、CC にアドレスを入力する。
B) 誤送信は人的ミスが原因であることが多いため、責任を追及されることはない。
C) 誤送信してしまったとしても、添付ファイルを暗号化したりパスワードをかけたりしていれば、受取人がファイルの中身を覗いてしまう可能性が低くなるので、情報漏えいのリスクは下がる。
D) すでにやりとりのある人にメールを送信する際でも、オートコンプリート（自動入力）機能を使用してメールアドレスを入力するべきではない。

総合テスト設問 1

情報セキュリティにおける「リスク分析」に関する説明で、正しいものを 1 つ選びなさい。

A) リスク分析における資産の価値はセキュリティを喪失した場合の影響の大きさとは関係ない。
B) リスク分析を行うには、その前に守るべきものを洗い出す必要がある。
C) リスク分析の見直しは行う必要がなく、最初に分析したものを守り続けるべきだ。
D) リスク分析における資産に対する脅威とぜい弱性の洗い出しは、ひとつの脅威に対してひとつのぜい弱性を洗い出す必要がある。

総合テスト設問 1

情報セキュリティのリスク分析をする意義としてあてはまるものはどれですか。すべて選びなさい。

A) 現在の情報セキュリティ対策では不足している部分が明らかになる。
B) すべての情報に対して一律の対策が講じられるようになる。
C) リスクの高い情報資産が何であるかが明確になる。
D) 社員の取扱いによる情報の消失や漏えい等の、リスクの内容や影響度が明らかになる。

次に、「ケースで学ぶ！情報セキュリティの最新脅威 2020-2021 年版（標的型メール対応）」では、確認テスト 1 設問 1、確認テスト 2 設問 2、確認テスト 3 設問 2、確認テスト 4 設問 1、総合テスト設問 1、総合テスト設問 5 の計 6 問が特に正答率が低い設問であった。

確認テスト 1 設問 1

情報セキュリティによって組織が防ぐべき事態として正しいものを選びなさい。

A) 情報漏えいや業務の停止
B) 権利侵害
C) 詐欺被害
D) 発表情報の間違い
E) 上記のすべて

確認テスト 2 設問 2

利用している業務システムのログインパスワードに安易なもの（「ABC」など）を設定していた場合に、発生する可能性の最も大きい情報セキュリティ事件・事故を、以下から 1 つ選びなさい。

A) 安易なパスワード設定によって発生するシステム停止や業務遅延。
B) 不正アクセスによる業務情報の漏えい、改ざんまたは削除。
C) 業務メールの誤送信によるクレームの発生。
D) 悪意のメールを開いたことによるウィルス感染。

確認テスト 3 設問 2

悪意の攻撃メールを見分けるポイントについての説明として正しいものを、以下から 1 つ選びなさい。

A) 攻撃メールは件名や文面が不自然なので、内容をよく読めば不正なものと気付ける。
B) 実在の大手企業の名称と正しい連絡先が書かれていれば、正当なメールと判断できる。
C) 自分が実際に送信したメールへの返信の形で攻撃メールが送られて来ることがある。
D) 攻撃メールの被害は 1 件では大きな金額にならないので、あまり神経質に警戒するべきではない。

確認テスト 4 設問 1

情報セキュリティの 3 要素に関して正しい情報を、以下から 1 つ選びなさい。

A) 機密性 ＝ 必要な時に情報を利用できること。
B) 完全性 ＝ 外部に情報を漏らさないこと。
C) 可用性 ＝ 正しい情報が全て揃っていること。
D) 情報セキュリティの CIA のうち C : Confidentiality は機密性のこと。

総合テスト設問 1

「顧客の個人情報や新製品のアイディアがふくまれていないので、常識から考えてこれは会社にとって重要な機密情報に該当しない」という判断は、なぜ間違っているのでしょうか。理由の説明として正しいものを以下からすべて選びなさい。

A) 業務で取り扱う情報は全て重要機密情報と見なす必要がある。
B) 会社固有の事情により、個人情報や新製品情報の他にも重要な情報が存在することが考えられる。
C) 同じ情報であっても重要度や機密度は部門によって大きく異なるので、都度部門の責任者に確認する必要がある。
D) 会社にとっての重要度は一般常識や個人判断でなく会社組織のルールとして判断する必要がある。

総合テスト設問 2

標的型メール攻撃に関する説明として正しいものを、以下からすべて選びなさい。 A) 特定の相手専用に偽物のメールを作り、ビジネス上の詐欺などを目的として送りつけて来る。 B) 何億円という巨額の被害が発生した事例もある。 C) メールに添付されたファイルを開かなければ被害を防ぐことができる。 D) D.文面や形式をよく気をつけて確認すれば、偽物を見破ることができる。

コースの修了時に、修了者にコースの学習の満足度と難易度について確認した。

「情報セキュリティの基礎」の満足度については、全員から満足しているとの回答が得られた。具体的に図 32 のとおり、とても満足しているが約 3 割、どちらかといえば満足しているが約 7 割という結果であった。

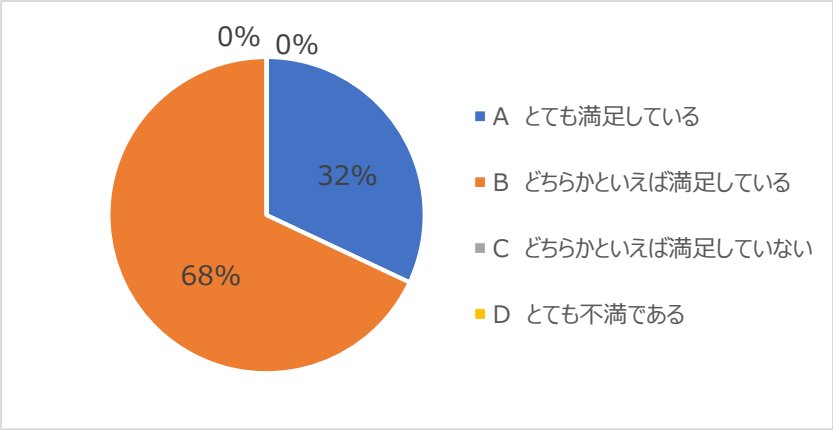


図 32 「情報セキュリティの基礎」の満足度

「情報セキュリティの基礎」の難易度については、コースの難易度として適切とされる「どちらかといえば難しかった」と「ちょうどよかった」の合計が 80%と大半を占める結果であった（図 33）。

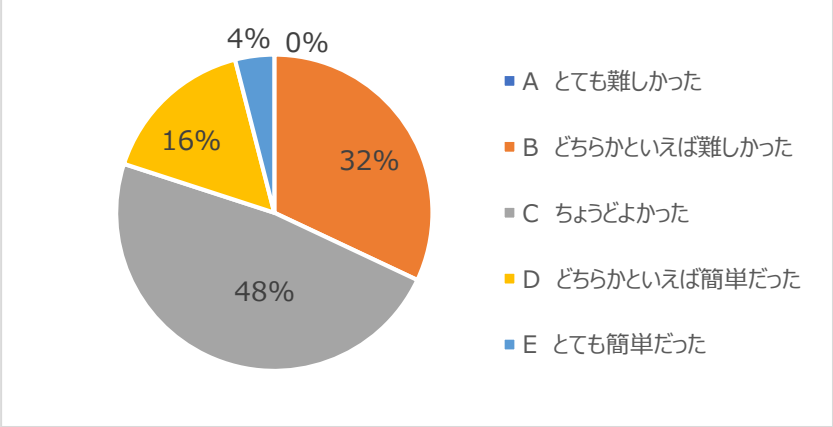


図 33 「情報セキュリティの基礎」の難易度

「情報セキュリティの基礎」を受講した感想として、次のようなコメントが得られ、受講者にとっては勘違いしていた内容を正す機会として、また、改めてセキュリティやウイルス、情報漏えいについて考える機会としての意義があったといえる。

- ✓ 自分自身のいる職場と想定の職場のイメージが違うので、若干戸惑った。
- ✓ 興味深く取り組めた。既知の内容も多かったが、当然だが勘違いしていた内容もあり、勉強になった。
- ✓ 普段、何気なく使用している PC ですが、改めてセキュリティやウイルス・情報漏洩について考えるよい機会になりました。

「ケースで学ぶ！情報セキュリティの最新脅威 2020-2021 年版（標的型メール対応）」の満足度については、ほぼ全員から満足しているとの回答が得られた。具体的に図 34 のとおり、とても満足しているが約 3 割、どちらかといえば満足しているが約 7 割という結果で、「情報セキュリティの基礎」と概ね同様の結果といえる。

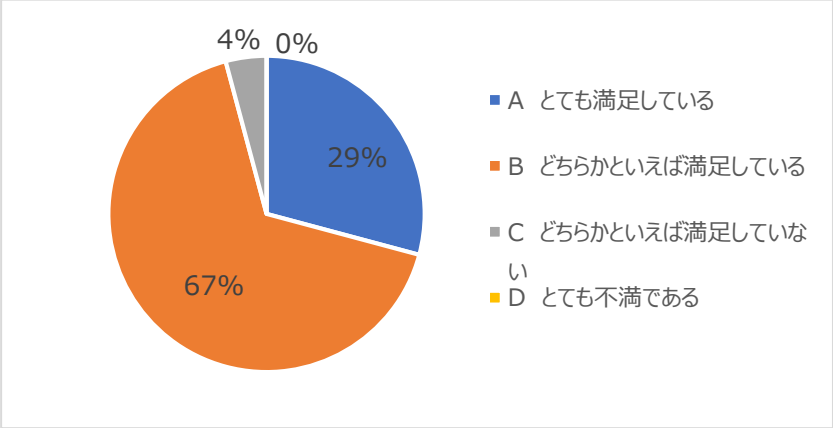


図 34 「ケースで学ぶ！情報セキュリティの最新脅威 2020-2021 年版（標的型メール対応）」の満足度

「ケースで学ぶ！情報セキュリティの最新脅威 2020-2021 年版（標的型メール対応）」の難易度については、コースの難易度として適切とされる「どちらかといえば難しかった」と「ちょうどよかった」の合計が 9 割弱と、こちらも「情報セキュリティの基礎」と同様に、難易度として適切であることが示される結果となった（図 35）。

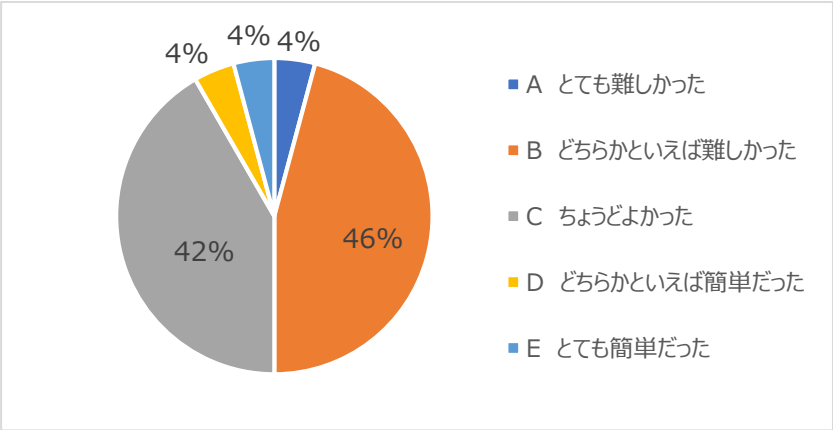


図 35 「ケースで学ぶ！情報セキュリティの最新脅威 2020-2021 年版（標的型メール対応）」の難易度

「ケースで学ぶ！情報セキュリティの最新脅威 2020-2021 年版（標的型メール対応）」を受講した感想として、次のようなコメントが得られた。特に、情報セキュリティ上の脅威に関して自己の認識が甘いことに気づいたとのコメントにあるとおり、攻撃者が様々な攻撃を仕掛けてくる可能性が身近に存在する現在、受講者に新たな知識・情報を継続的に伝えていく意義があると考える。

- ✓ ビデオなどで学習することも効果があると思う。
- ✓ 読むのは苦手であるので、聞き取りの方が理解し易い。
- ✓ 情報セキュリティ・・・自分の認識の甘さに気が付きました。今後は、もう少し気を付けていきたいと思います。

4. 実証期間中のサイバーセキュリティ脅威の状況と対策支援状況

4.1 UTM のログから見える脅威のアタックとブロック状況

UTM で検知した事象は、以下表 5 の種別のとおりログとして把握できる。

表 5 UTM で検知する事象の種別およびその内容

種別	内容
①不正プログラム／スパイウェア	不正プログラム検索機能により、不正プログラム（マルウェア）、スパイウェアであることを検知
②不正侵入検知（IPS）	通信が IPS 機能で定義されたルールにマッチしたかを検知
③不正サイト	Web レピュテーション機能により、危険とされる URL への HTTP リクエストまたは TLS ネゴシエーション等を検知
④スパムメール	メールセキュリティ機能により、スパムメールを検知
⑤ランサムウェア	不正プログラム検索機能により、ランサムウェアであることを検知
⑥CnC コールバック	C&C コールバックとされる URL への HTTP リクエストを検知
【参考 1】禁止アプリケーション	ポリシー設定で禁止したアプリケーションからの通信要求を検知
【参考 2】URL カテゴリフィルタ	トレンドマイクロがカテゴライズした URL カテゴリに該当した HTTP リクエストまたは TLS ネゴシエーションを検知

以下では事象の種別ごとにその検知数や特徴を見ていく。

4.1.1　不正プログラム／スパイウェア

「不正プログラム／スパイウェア」は、コンピューターに害悪を及ぼすプログラムであり、コンピューターが不正に操作され、社内の情報をインターネットに対して送り出してしまう脅威がある。

UTM により、不正な通信、プログラムによる攻撃を検知し、どんな通信が行われているかを判別し、内部感染を早期に発見できる。

2020 年 10 月から 12 月の間に「不正プログラム／スパイウェア」を検知した件数は、表 6 のとおり、10 月は 0 件、11 月は 50 件、12 月は 26 件であった。月別の変化を 1 社あたり検知件数でみると顕著な差はない。

表 6 不正プログラム／スパイウェアの検知件数（月別）

	2020 年 10 月	2020 年 11 月	2020 年 12 月
社数[3]	35（22）	134（131）	95（87）
検知件数	0	50	26
1 社あたり検知件数	0	0.38	0.30

[3] 括弧内は UTM 設置企業のうちデータ送受信のあった企業数を示す。以降の検知件数を示す表においても同じ。

「不正プログラム／スパイウェア」について、プログラム名称別の件数内訳でみると、表 7 のとおり、11 月は「load-scripts.php」が 34 件と全体の 7 割弱を占めた。次いで「COMPANY PROFILE.doc」が 9 件と続く。この不正プログラム「COMPANY PROFILE.doc」は、同時期に検知した社数が 4 社あり該当社数が複数存在したのが特徴的で、本実証参加以外の企業も含め広く流通した可能性がある。

12 月では、件数が突出している不正プログラムはないが、11 月の「COMPANY PROFILE.doc」に類似した「COMPANY PROFILE.doc,RFQ.exe」が検知されているほか、名称は異なるものの「Fattura_」で始まる表計算関連ファイル（拡張子が.xls や.xlsm）が複数検知された。表計算関連ファイルのように業務上利用頻度が高いと思われるファイルに不正プログラムが含まれるのは特徴の一つといえる。

表 7 不正プログラム／スパイウェアの名称別累計検知件数および該当社数

（2020 年 10 月）

不正プログラム名	累計件数	該当社数
なし	0	0 社
合計	0	-

（2020 年 11 月）

不正プログラム名	累計件数	該当社数
load-scripts.php	34	1 社
COMPANY PROFILE.doc	9	4 社
采购查询-SFD9751CS # .iso	2	1 社
--	2	1 社
five days trip.doc	2	1 社
Fattura_13397.xlsm	1	1 社
合計	50	-

（2020 年 12 月）

不正プログラム名	累計件数	該当社数
Urgent Request.doc	4	2 社
--	3	1 社
Shipping document PL and BL0076,pdf.iso	3	1 社
Mwasiti Mnindy CV.exe	3	1 社
変化 10 月 02.doc	1	1 社
Fattura_13397.xlsm	1	1 社
COMPANY PROFILE.doc,RFQ.exe	1	1 社
payment slip.exe	1	1 社
RF-008055.exe	1	1 社
111737454985.xls	1	1 社
711340022881.xlsm	1	1 社
Fattura_16509.xlsm	1	1 社
Fattura_75038.xlsm	1	1 社
Fattura_94762.xlsm	1	1 社
12_09_2020_1.xls	1	1 社
Fattura_74362.xlsm	1	1 社
n.485884_12/02/2020.xls	1	1 社
printouts of outstanding as of 87607_12_07_2020.xlsm	1	1 社
合計	26	--

4.1.2　不正侵入検知（IPS）

「不正侵入検知（IPS)」は、ソフトウェアやネットワークの脆弱性を利用してシステムが乗っ取られ、その結果機密情報が漏えいしてしまう脅威がある。

UTM により、ソフトウェアやネットワークの脆弱性をついた攻撃と疑われる通信を検知しブロックできる。

2020 年 10 月から 12 月の間に「不正侵入検知（IPS)」を検知したマッチ回数は、表 8 の通り、10 月は 539 件、11 月は 18,328 件、12 月は 783 件であった。月別の変化を 1 社あたりマッチ件数でみると、2020 年 11 月の多さが際立っている。

表 8 不正侵入検知（IPS）のマッチ回数（月別）

	2020 年 10 月	2020 年 11 月	2020 年 12 月
社数	35（22）	134（131）	95（87）
マッチ件数	539	18,328	783
1 社あたりマッチ件数	24.5	139.9	9.0

「不正侵入検知（IPS)」について、ルール名称別の件数内訳を表 9 に示した。10 月に該当社数は 1 社ながら累計マッチ回数が 309 件と最も多かった「1059125」は、11 月には該当社数が 6 社で累計マッチ回数が 12,412 回に及んでいる。また、10 月に該当社数が 18 社で累計マッチ回数が 130 件と第 2 位だった「1133679」は、11 月に第 4 位（74 社、905 件)、12 月に第 8 位（3 社、59 件）に位置し、ルールによってはこれらのように複数月に跨りマッチ回数として検知されるルールもある。

12 月に第 1 位や第 2 位に位置しているルールは初出ではあるが、2021 年 1 月以降にも継続して検知される可能性もある。

表 9 不正侵入検知（IPS）のルール名別累計マッチ回数および該当社数（累計マッチ回数上位 10 ルール）

（2020 年 10 月）

	IPS ルール名	累計 マッチ回数	該当社数
1	1059125:INVALID HTTP VERSION:MISC:RFC 2616;	309	1 社
2	1133679:SSL OpenSSL ChaCha20-Poly1305 and RC4-MD5 Integer Underflow -2 （CVE-2017-3731）:CVE-2017-3731	130	18 社
3	1054753	40	1 社
4	1056952:TCP Paws Elimination:MISC:RFC 1323	32	1 社
5	1130226	10	5 社
6	1050015:WEB Cross-site Scripting -34:CVE-2011-2133; CVE-2014-4116; CVE-2017-7309	6	2 社
7	1055299	5	2 社
8	4043309087:Bad TCP Flag:MISC:RFC 791	2	1 社
9	1133401:NTP ntp.org Network Time Protocol Windows Daemon getEndptFromIoCtx Denial of Service （CVE-2016-9312）:CVE-2016-9312	2	1 社
10	1059756	1	1 社

（2020 年 11 月）

	IPS ルール名	累計 マッチ回数	該当社数
1	1059125:INVALID HTTP VERSION:MISC:RFC 2616;	12,412	6 社
2	1054217:EXPLOIT iSCSI target Multiple Implementations iSNS Stack overflow （CVE-2010-2221）:CVE-2010-2221,	1,863	1 社
3	4043309058:UDP Land:MISC:RFC 768	1,529	3 社
4	1133679:SSL OpenSSL ChaCha20-Poly1305 and RC4-MD5 Integer Underflow -2 （CVE-2017-3731）:CVE-2017-3731	905	74 社
5	1054742:EXPLOIT Microsoft Client Service for NetWare Memory Corruption （CVE-2006-4688）:CVE-2006-4688	527	3 社
6	1130226	198	26 社
7	1131496	86	2 社
8	4043309087:Bad TCP Flag:MISC:RFC 791	78	14 社
9	1055299	64	6 社
10	1136723:SMB Microsoft Windows SMB Server SMBv3 Buffer Overflow -1 （CVE-2020-0796） :CVE-2020-0796; https://portal.msrc.microsoft.com/en-US/security-guid	61	1 社

（2020 年 12 月）

	IPS ルール名	累計 マッチ回数	該当社数
1	1055397:DNS Microsoft DNS Server NAPTR Record Sign Extension Memory Corruption （CVE-2011-1966）:CVE-2011-1966; MS11-058	113	2 社
2	1049407:WEB Linux /etc/shadow File Download:CVE-2002-unknown	100	4 社
3	4043309087:Bad TCP Flag:MISC:RFC 791	86	6 社
4	1050015:WEB Cross-site Scripting -34:CVE-2011-2133; CVE-2014-4116; CVE-2017-7309	68	13 社
5	1133480:EXPLOIT Remote Command Execution via Shell Script -2:CVE-2017-unknown	68	2 社
6	1056153:WEB SQL injection select from attempt -3.u:CVE-2015-7297; CVE-2015-7857; CVE-2015-7858; CVE-2017-8917	65	2 社
7	1054837:WEB Remote File Inclusion /etc/passwd:BID:65874; CVE-1999-0262; CVE-2007-1277; CVE-2011-0405; CVE-2011-0518; CVE-2011-4716; CVE-2012-5192; CVE	61	8 社
8	1133679:SSL OpenSSL ChaCha20-Poly1305 and RC4-MD5 Integer Underflow -2 （CVE-2017-3731）:CVE-2017-3731	59	3 社
9	1055299:ICMP Microsoft Windows TCP-IP Stack ICMP Sequence Denial of Service （CVE-2011-1871）:CVE-2011-1871;CVE-2011-2013	51	1 社
10	1052848:NETBIOS SMB username brute force attempt	13	1 社

4.1.3　不正サイト

「不正サイト」は、不正な Web サイトへのアクセスによる不正プログラムへの感染や実行、フィッシング詐欺被害等の発生につながる脅威がある。

UTM により、IP アドレスの情報から、どのユーザーが不正サイトへのアクセスを試みているかを把握することが可能で、不正サイトへの接続を検知しブロックできる。

2020 年 10 月から 12 月の間の「不正サイト」を検知した件数は、表 10 のとおり、10 月は 18 件、11 月は 441 件、12 月は 251 件であった。月別の変化を 1 社あたりマッチ件数でみると、2020 年 11

月の多さが際立っている。月別の変化を 1 社あたり検知件数でみると、11 月が僅かに多いが、顕著な差ではない。

表 10 不正サイトの検知件数（月別）

	2020 年 10 月	2020 年 11 月	2020 年 12 月
社数	35（22）	134（131）	95（87）
検知件数	18	441	251
1 社あたり検知件数	0.8	3.4	2.9

「不正サイト」について、不正サイト名称別の件数内訳を表 11 に示した。10 月に検知された「m.hcloset.com」は、11 月（第 6 位）、12 月（第 1 位）にも継続的に検知されている。同様に 11 月に第 3 位（該当社数 4 社、累計件数 52 件）に位置する「api.bdisl.com」は、12 月に第 4 位の位置で、11 月に第 8 位（該当社数 2 社、累計件数 11 件）に位置する「survey-smiles.com」は、12 月に第 7 位の位置でそれぞれ検知されている。

表 11 不正サイトのサイト名称別累計検知件数および該当社数（累計件数上位 10 サイト）

（2020 年 10 月）

	不正サイト名称	累計件数	該当社数
1	m.hcloset.com	18	1 社
	合計	18	-

（2020 年 11 月）上位 10 サイトが累計件数全体に占める割合：75.7%

	不正サイト名称	累計件数	該当社数
1	www.masksjp.xyz	88	1 社
2	jafuq.com	60	1 社
3	api.bdisl.com	52	4 社
4	jagee.xyz	44	1 社
5	www.yarex.xyz	36	1 社
6	m.hcloset.com	15	2 社
7	qaloqum.com	12	1 社
8	survey-smiles.com	11	2 社
9	www.specopy.com	8	1 社
10	www.staytokei.com	8	1 社
	小計（上位 10 サイト）	334	-
	合計	441	-

（2020 年 12 月）上位 10 サイトが累計件数全体に占める割合：69.3%

	不正サイト名称	累計件数	該当社数
1	m.hcloset.com	36	1 社
2	track2.highseas.xyz	31	4 社
3	link.hcloset.com	30	1 社
4	api.bdisl.com	25	1 社
5	click.mnmnck.com	15	1 社
6	goescar.top	12	1 社
7	survey-smiles.com	11	1 社
8	manuqas.com	6	3 社
9	kzclip.com	4	1 社
10	clicks.mnmnck.com	4	1 社
	小計（上位 10 サイト）	174	
	合計	251	-

4.1.4　スパムメール

「スパムメール」は、宣伝広告目的で、ユーザーの同意なしに勝手に送られてくる迷惑メールで、アクセスのみで感染に至る URL が記されている場合は誤ってアクセスすることで情報漏えい等につながる脅威がある。

UTM により、スパムメールを判定して、件名に「スパムメール」と付与する処理を行いユーザーが誤って URL にアクセスしないよう注意を喚起できる。

2020 年 10 月から 12 月の間の「スパムメール」を検知した件数は、表 12 のとおり、10 月は 516 件、11 月は 36,903 件、12 月は 21,763 件であった。月別の変化を 1 社あたり検知件数でみると、2020 年 11 月の多さが目立つ結果となった。

表 12 スパムメールの検知件数（月別）

	2020 年 10 月	2020 年 11 月	2020 年 12 月
社数	35（22）	134（131）	95（87）
検知件数	516	36,903	21,763
1 社あたり検知件数	23.5	281.7	250.1

4.1.5　ランサムウェア

「ランサムウェア」は、PC 内のファイルの暗号化やロックにより、それを元に戻すことと引き換えに「身代金」（Ransom）を要求する不正プログラムで、業務で使っている PC 等が使用できない状況に追いこまれる脅威がある。

UTM により、ランサムウェアの侵入を検出しブロックした件数と、宛て先となっていたユーザーを把握できる。

2020 年 10 月から 12 月の間の「ランサムウェア」を検知した件数は、表 13 のとおり、10 月は 6 件、11 月は 67 件、12 月は 150 件であった。月別の変化を 1 社あたり検知件数で比較すると、2020 年 12 月は前月比 3 倍以上となっており、その多さが目立つ結果となった。

表 13 ランサムウェアの検知件数（月別）

	2020 年 10 月	2020 年 11 月	2020 年 12 月
社数	35（22）	134（131）	95（87）
検知件数	6	67	150
1 社あたり検知件数	0.3	0.5	1.7

4.1.6　CnC コールバック

「CnC コールバック」は、ボットネットや感染コンピューターのネットワークに対し、不正なコマンドを遠隔で頻繁に送信するために利用される C&C サーバーに通信が発生した場合、特定の Web サイトへ負荷を与える DDoS 攻撃や、サーバーから重要な機密情報を抜き取りなどの被害が発生する脅威がある。

UTM により、C&C サーバー接続を検知・ブロックし、IP アドレスにより、どのユーザーが C&C サーバーへの通信を実施しているか把握できる。

2020 年 10 月から 12 月の間の「CnC コールバック」を検知した件数は、表 14 のとおり、10 月および 12 月の検知件数はゼロで、609 件（1 社あたり 4.6 件）を検知した 11 月が目立つ結果となった。

表 14 CnC コールバックの検知件数（月別）

	2020 年 10 月	2020 年 11 月	2020 年 12 月
社数	35（22）	134（131）	95（87）
検知件数	0	609	0
1 社あたり検知件数	0	4.6	0

以降では、参考情報として UTM で検知した「禁止アプリケーション」の検知件数と「URL カテゴリフィルタ」の検知件数を示す。

【参考 1】禁止アプリケーション

「禁止アプリケーション」の検知件数は、ポリシー設定で禁止したアプリケーションからの通信要求が検知された件数を示す（以下表 15）。

表 15 禁止アプリケーションの検知件数（月別）

	2020 年 10 月	2020 年 11 月	2020 年 12 月
社数	35（22）	134（131）	95（87）
検知件数	2,578	12,431	3,375
1 社あたり検知件数	117.2	94.9	38.8

【参考 2】URL カテゴリフィルタ

「URL カテゴリフィルタ」の検知件数は、HTTP リクエストまたは TLS ネゴシエーションをもとにトレンドマイクロがカテゴライズした URL カテゴリに該当した場合、そのアクセス件数（HTTP リクエストまたは TLS ネゴシエーション試行単位）を示す（以下表 16）。

表 16 URL カテゴリフィルタの検知件数（月別）

	2020 年 10 月	2020 年 11 月	2020 年 12 月
社数	35（22）	134（131）	95（87）
検知件数	439,392	19,111,133	25,464,619
1 社あたり検知件数	19,972.4	145,886.5	292,696.8

4.2 標的型攻撃メール訓練開封率（実証前後比較）

標的型攻撃メール訓練は以下のとおり、あえて異なる内容の訓練を 2 回実施した。第 1 回訓練は添付ファイルのあるメールを、第 2 回訓練では添付ファイルはなく URL が含まれるメールをそれぞれ送信した。訓練対象は第 1 回も第 2 回も 140 社の 418 ユーザーである。

訓練メールの具体的な内容は表 17 に示す。なお訓練期間中、訓練についての事前および事後の通知は行っていない。

表 17 訓練メールの内容

（第 1 回）2020 年 11 月 20 日 11 時～2020 年 12 月 24 日 17 時に実施

送信元	kyoyu-groupmail@infomaton.com
差出人名	総務
メール件名	テレワークの助成制度について
本文	各位 総務より連絡です。 テレワークの導入に伴ない、自宅での通信費（インターネット利用費） の一部を会社が助成する制度が開始されます。 申請方法は部署により異なりますので、 添付の手順に従い実施願います。 また、本件についての問い合わせ先も添付に記載 しておりますのでご確認願います。 宜しくお願い致します。
添付ファイル	助成制度の申請方法.pdf（圧縮無し、パスワード無し）

（第 2 回）2020 年 12 月 17 日 16 時～2020 年 12 月 24 日 17 時に実施

送信元	kenkan@infomaton.com
差出人名	健康管理センター
メール件名	【緊急依頼】新型コロナウイルス健康調査について
本文	社員の皆様へ 健康管理センターです。 いつもお世話になっております。 このたび、社員皆様の健康状態を把握するために、 アンケートを実施させていただきます。 大変申し訳ございませんが、 本日中に以下の URL にアクセスいただき、健康状態についてご報告願います。 URL お手数をおかけしますが、

	ご対応よろしくお願いいたします。
添付ファイル	無し

まず、ユーザー単位でその結果を見ると、第 1 回は検知率（開封率）5.0%（対象者数は計 418、検知数（開封数）は計 21 件）、第 2 回は検知率 7.7%（対象者数は 418、検知数は 32 件）と、第 2 回の検知率が約 3 ポイント高い結果となった（以下表 18）。

送付した指定された URL をクリックする行為が添付ファイルを開くよりも手軽で、警戒の度合いが小さく、そのため第 2 回訓練での検知率の高さに結びついたものと想定する。

表 18 標的型攻撃メール訓練の実施概要および結果概要（ユーザー単位）

	訓練期間	対象数	検知数	検知率
第 1 回	2020 年 11 月 20 日 11 時-2020 年 12 月 24 日 17 時 （以下は内訳）	418	21	5.0%
	2020 年 11 月 20 日 11 時-2020 年 12 月 01 日 17 時	32	1	3.1%
	2020 年 11 月 26 日 13 時-2020 年 12 月 01 日 17 時	381	20	5.2%
	2020 年 12 月 03 日 11 時-2020 年 12 月 09 日 17 時	5	0	0%
第 2 回	2020 年 12 月 17 日 16 時-2020 年 12 月 24 日 17 時 （第 2 回は上記期間に一斉に実施）	418	32	7.7%

次に、企業単位の結果として、その企業に所属するユーザーの少なくとも 1 人が検知された企業の割合は、第 1 回が 11.4%、第 2 回が 17.9%であった。ユーザー単位での結果と同様に第 2 回の割合が高い結果となっている（以下表 19）。

標的型攻撃メールを開いてしまった場合、その被害を受けるのはメールを開いてしまった本人に留まらず、社内のネットワークを通じる等で会社全体に被害が拡がる可能性がある。標的型攻撃メールの受信および開封に伴いその被害を受ける可能性のある企業は潜在的には約 1~2 割存在することを示しており、メールの利用においては一人ひとりが安易に添付ファイルを開いたり、リンクをクリックしたりしないよう留意しておくことが強く求められることを改めて示した結果と考える。

表 19 標的型攻撃メール訓練の実施概要および結果概要（企業単位）

	訓練期間	対象社数	検知数 （社数）	割合
第 1 回	2020 年 11 月 20 日 11 時-2020 年 12 月 24 日 17 時 （以下は内訳）	140	16	11.4%
	2020 年 11 月 20 日 11 時-2020 年 12 月 01 日 17 時	17	1	5.9%
	2020 年 11 月 26 日 13 時-2020 年 12 月 01 日 17 時	122	15	12.3%
	2020 年 12 月 03 日 11 時-2020 年 12 月 09 日 17 時	1	0	0%
第 2 回	2020 年 12 月 17 日 16 時-2020 年 12 月 24 日 17 時 （第 2 回は上記期間に一斉に実施）	140	25	17.9%

4.3 企業ホームページ上の脅威や脆弱性に関する診断

Web サイトの改ざん検出と脆弱性診断から成る Web セキュリティ診断は、以下のとおり実施した（表 20）。

表 20 Web セキュリティ診断の実施概要

実施期間	2020 年 11 月 30 日～2020 年 12 月 31 日 （計 32 日間）
診断対象	107 契約（なお、上記実施期間中に URL 変更が行われた契約があるため、サイト数ベースでは 108URL）
診断項目	● 改ざん検出 ● 脆弱性診断 ➢ クロスサイトスクリプティング ➢ SQL インジェクション ➢ OS コマンドインジェクション ➢ ディレクトリトラバーサル ➢ ディレクトリインデックス

各診断項目の概要について、以下に記す。

- 「改ざん検出」とは、Web サイトの改ざんが行われていないか否かを検出する。Web サイトの改ざんとは、攻撃者やコンピューターウイルス等により、Web サイトのコンテンツ（HTML データ等）が不正に書き換えられることを指す。改ざんされた Web サイトを閲覧した利用者が、悪意のある外部の Web サイトへ誘導され、ウイルス感染等の被害にあう恐れがあるほか、改ざんによって Web サイトが正常に機能しなくなったり、Web サイト内の機密情報が漏えいしたりする恐れもある。
- 「クロスサイトスクリプティング」とは、Web サイト利用者のブラウザに悪意のあるスクリプト（簡易プログラム）を送り込み、実行させることを許してしまう脆弱性を指す。攻撃者によって利用者の Web ブラウザが不正に操作された場合、Web サイト利用者を識別・認証している Cookie 情報が盗まれたり、偽 Web ページが表示されたりしてしまう恐れがある。Cookie 情報が攻撃者に奪われると、攻撃者は正当な利用者になりすまして Web サイトを不正に利用することが可能となる。また、偽 Web ページの表示によって、Web サイト利用者がフィッシング等の被害にあう恐れがある。
- 「SQL インジェクション」とは、ホームページと連携しているデータベースにおいて、悪意のある SQL 文（データベースへの命令）により、意図しないデータベースの操作が実行されてしまう脆弱性を指す。この脆弱性が存在すると、攻撃者によって、データベース内に格納されたデータの奪取や改ざんが行われる恐れがある。
- 「OS コマンドインジェクション」とは、悪意のあるリクエスト（OS への命令）により、不正に操作されてしまう脆弱性を指す。Web サイトにこの脆弱性が存在する場合、攻撃者が任意の OS コマンドを実行可能であるため Web サーバー内の情報漏えい、改ざん、削除または、不正にシステム操作されてしまう恐れがある。
- 「ディレクトリトラバーサル」とは、公開されているトップディレクトリを遡り、非公開のディレクトリへとアクセスできてしまう脆弱性を指す。この脆弱性が存在すると、非公開の

ファイルやフォルダ内の情報を不正に閲覧、または改ざんなどが行われる恐れがある。

・ 「ディレクトリインデックス」とは、Web コンテンツを格納するディレクトリ（フォルダ）配下のファイルが一覧表示されてしまう脆弱性を指す。この脆弱性が存在すると、表示されたファイル一覧上に存在するファイルにアクセスすることによって、公開を意図していないファイルの閲覧や実行が可能となる恐れがある。

診断の結果、Web サイトの改ざんが行われた件数は 0 であったが、何らかの脆弱性が 1 件以上検出されたサイト数は、11 月 30 日で 18URL、12 月 30 日で 16URL だった。診断項目別にみた内訳は以下表 21 のとおりである。

診断項目別にみると、11 月、12 月ともクロスサイトスクリプティングへの該当が 11 月で 10URL・216 件、12 月で 9URL・217 件と最も多く、ディレクトリインデックスがそれに次ぐ多さとなった。

表 21 Web セキュリティ診断の実施結果

診断項目		11 月 30 日		12 月 1 日～31 日	
		検出サイト数	検出件数	検出サイト数	検出件数
改ざん検出		0URL	0 件	0 URL	0 件
脆弱性診断	クロスサイトスクリプティング	10 URL	216 件	9 URL	217 件
	SQL インジェクション	2 URL	3 件	2 URL	3 件
	OS コマンドインジェクション	1 URL	2 件	1 URL	2 件
	ディレクトリトラバーサル	0 URL	0 件	0 URL	0 件
	ディレクトリインデックス	7 URL	104 件	6 URL	94 件
	全体[4]	18URL	-	16URL	-

[4] 複数の診断項目に該当する URL が複数存在するため、検出サイト数の合計 URL 数とは一致しない。

4.4 セキュリティサポートデスクへの問合せ内容、頻度・傾向

実証期間中、一元対応窓口（サポートデスク）には実証参加企業より以下の問合せがあり対応を行った。なお、サイバーセキュリティのインシデント事項に関する問合せは 0 件であり、駆け付け対応も発生しなかった。

表 22 一元対応窓口（サポートデスク）への問合せ内容

問合せ内容	件数	問合せ内容
①セキュリティ機器設置の問合せ	2 件	・設置機器の取り扱い方法について詳しく教えてほしい ・実証事業終了後の設置機器の取り扱いについて教えてほしい
②セキュリティ対応相談	1 件	・あるサイトにアクセスしたいがブロックされるため、ブロックを解除したい
③その他	2 件	・事前アンケートの内容について詳細を教えてほしい ・実証事業実施期間について教えてほしい
合計	5 件	

4.5 全体的なサイバーセキュリティ上のトピックス

UTM のログで検知した事象や Web セキュリティ診断の結果から、日常的に様々なサイバーセキュリティ上の脅威が身近に存在することを改めて確認した。期間中、駆けつけ対応等が必要な重大インシデントの発生には至らなかったものの、脆弱性の存在は攻撃者に攻撃機会を与え、企業自体やその顧客は予期せぬ被害を受けてしまう契機となるため、継続的なログの確認およびセキュリティ診断、その結果を踏まえた脆弱性の除去等、速やかな対応が必要といえる。

5. 実証後の企業・社員の意識の変化

5.1 定期的な標的型メール訓練実施とサイバーセキュリティ脅威状況のフィードバックによる意識変化

中小企業のサイバーセキュリティ対策の現状把握、実証開始時の中小企業における社員のサイバーセキュリティに対する意識調査を目的に実証開始時にアンケートを実施した。（実証前後の比較を行うため実証後にも同種のアンケートを実施する）

5.1.1　アンケート内容

＜対象者＞　実証参加企業
＜回答数＞　43 社
＜実施日＞　2021 年 1 月に実施
＜実証開始時アンケート内容＞

Q1.実証事業期間終了後もサイバーセキュリティ対策に関心をお持ちですか

1. すぐにでも、検討しようと思った
2. とても関心があり、いずれ検討しようと思った
3. 関心はあるが、検討するかはわからない
4. 関心はない

Q2.ご存知のセキュリティ脅威がございましたらお答え願います。（いくつでも）

1. 標的型攻撃による機密情報の窃取
2. 内部不正による情報漏えい
3. ビジネスメール詐欺による金銭被害
4. サプライチェーンの弱点を悪用した攻撃
5. ランサムウェアによる被害
6. 予期せぬ IT 基盤の障害に伴う業務停止
7. 不注意による情報漏洩
8. IoT 機器の不正利用
9. サービス妨害攻撃によるサービスの停止
10. インターネット上のサービスからの個人情報の窃取
11. その他

Q3.貴社で今後導入を検討しているサイバーセキュリティ対策をお教えください。（いくつでも）

1. ウイルス対策ソフト
2. 出入口対策
3. 社員教育
4. セキュリティ管理者の設置
5. セキュアな無線環境
6. セキュアな拠点間通信
7. 重要なファイルのバックアップ
8. サイバーリスク保険加入
9. セキュリティポリシーの策定

Q4.現在サイバーセキュリティ対策にかかっている月額費用はいくらぐらいですか。

1. 3,000 円以下
2. 3,000 円～5,000 円
3. 5,000 円～10,000 円
4. 10,000～20,000 円
5. 20,000 円～

Q5.今後サイバーセキュリティ対策にかける月額費用はいくらぐらいを見込んでいますか。

1. 3,000 円以下
2. 3,000 円～5,000 円
3. 5,000 円～10,000 円
4. 10,000～20,000 円
5. 20,000 円～
6. 現状の月額費用と変わらない

Q6.サイバーセキュリティ対策に関して、貴社の課題を教えてください

1. セキュリティポリシーの策定
2. 管理体制の構築
3. リスクの洗い出し、評価
4. グループ会社、取引先も含めた対策の実施
5. セキュリティ対策費予算の確保
6. セキュリティ対策専門人材の確保
7. インシデント発生時の体制の構築
8. 情報収集（最新技術動向や事故事例）
9. なし

Q7.セキュリティ対策機器の設置により、総合的なサーバーセキュリティの脅威について意識の変化はありましたか

1. 脅威を感じ、意識に変化があった
2. 脅威は感じたが、意識に変化はない
3. 特に何も感じない

Q8.お客様ホームページの脆弱性診断の実施（一部のお客様）により、Web サイト上の脅威について意識の変化はありましたか

1. 脅威を感じ、意識に変化があった
2. 脅威は感じたが、意識に変化はない
3. 特に何も感じない

Q9.標的型攻撃メールの疑似訓練の実施により、なりすましメールの脅威について意識の変化はありましたか

1. 脅威を感じ、意識に変化があった
2. 脅威は感じたが、意識に変化はない
3. 特に何も感じない

Q10.情報セキュリティ対策 e ラーニングの内容は、現状の動向の把握や今後のセキュリティ対策を検討する上で役に立つ内容でしたか

1. とても役に立つ内容だった
2. まあまあ役に立つ内容だった
3. あまり役に立たない内容だった
4. 全く役に立たない内容だった
5. 受講していない

Q11.Q10 で＜受講していない＞とお答えいただいた方にお聞きします。受講されなかった理由についておしえてください（いくつでも）

1. 受講する時間を確保できなかった
2. あまり必要のない内容だと思った
3. 受講する環境の確保が難しかった
4. その他

Q12.本実証事業の参加を通じて、サイバーセキュリティに関する意識は変わりましたか

1. 大きく意識が向上した
2. 少し意識が向上した
3. 特に変わらない

Q13.情報漏えいやシステム停止などのインシデントが発生した場合の対応方針（手順・連携先など）を決めていますか

1. 決めている
2. 現在検討している
3. 決めていない

Q14.情報漏えいやシステム停止などのインシデントが発生した場合に発生する費用の予算を確保していますか

1. 予算を確保している
2. 保険に加入し予算を確保している
3. 今後予算を確保する予定
4. 予算を確保していない

Q15.外部からの不正アクセスや情報漏えいに備える保険（サイバーリスク保険）があることを知っていましたか

1. 知っていた
2. 知らなかった

Q16.サイバーセキュリティ対策としてサイバーリスク保険を活用したいと思いますか

1. 活用を検討したい
2. 活用は難しい（費用面要因）
3. 活用は難しい（保険は不要）

Q17.サイバーリスク保険についての詳細説明を希望されますか ※希望しない以外をご回答いただいた方には、東京海上日動火災保険株式会社よりご案内のご連絡をさせていただきます

1. 商品内容について知りたい
2. 保険料イメージについて知りたい
3. 希望しない

Q18.SECURITY ACTION（セキュリティ対策自己宣言）についてご存知ですか

1. 知っており、一つ星登録済
2. 知っており、二つ星登録済
3. 知っているが、宣言していない
4. 知らない

Q19.Q18 で＜知っているが、宣言していない／知らない＞とお答えいただいた方にお聞きします。
今後宣言される予定はありますか

1. 一つ星登録まで実施したい
2. 二つ星登録まで実施したい
3. 登録しない

Q20.ご意見・ご要望等を自由にご記入ください。（自由回答・任意）

5.1.2 アンケート回答企業の属性

アンケート回答企業 42 社の規模は以下のとおり。

表 3-1 企業規模ごとの回答企業数

企業規模	回答企業数（社）
~20 名	21
21 名~100 名	16
101 名~	5

5.1.3　個別回答結果

① Q1.サイバーセキュリティ対策に関心をお持ちですか

すぐにでも検討しようと考えるのは、規模が小さい企業の方が高くなるという傾向がみられた。これは、規模が小さい企業の方が、サイバーセキュリティ対策を行っていない割合が高いことに起因すると考えられる。一方で、20 名以下の企業のうち、2 社はサイバーセキュリティ対策に興味なしと回答しており、企業による温度差があることが確認された。

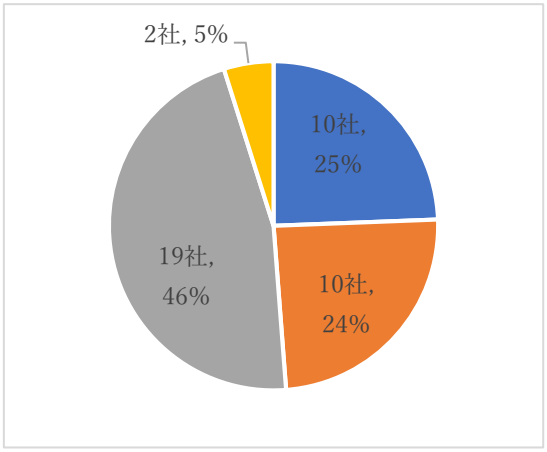


図 36 Q1 への回答（全体）

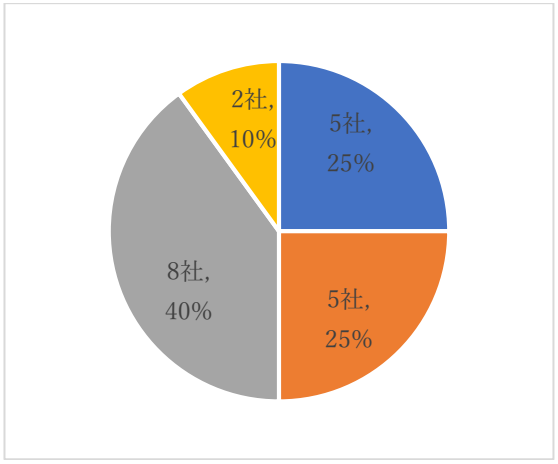


図 37 Q1 への回答（~20 名）

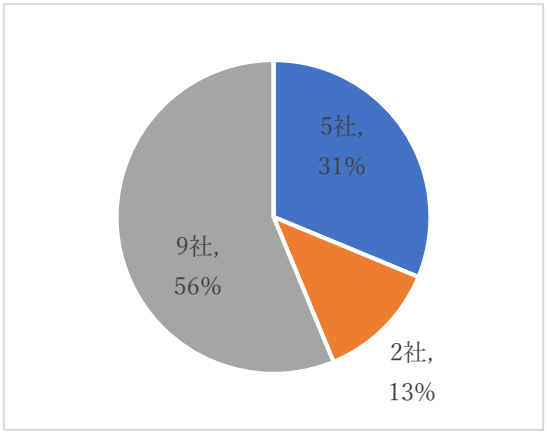


図 38 Q1 への回答（~100 名）

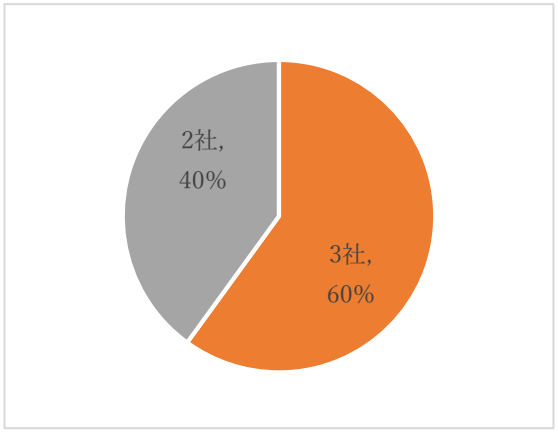
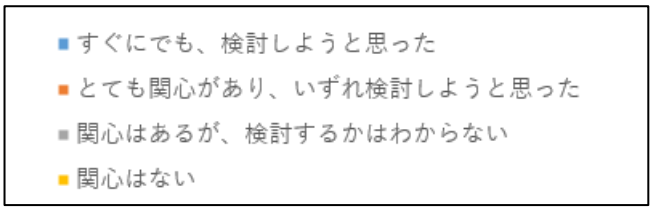


図 39 Q1 への回答（~100 名）

＜凡例＞



② Q2.貴社で脅威に感じているサイバーセキュリティ事項についてお答え願います。（いくつでも）

事前調査で認知度が高かったサイバーセキュリティ事項に対して、脅威を感じている企業が多いという結果となった。「ランサムウェアによる被害」、「不注意による情報漏洩」、「標的型攻撃による機密情報の窃取」等は、事前の認知度よりも今回脅威を感じる企業が多く、実証に参加することで、より脅威を体感したものと考えられる。

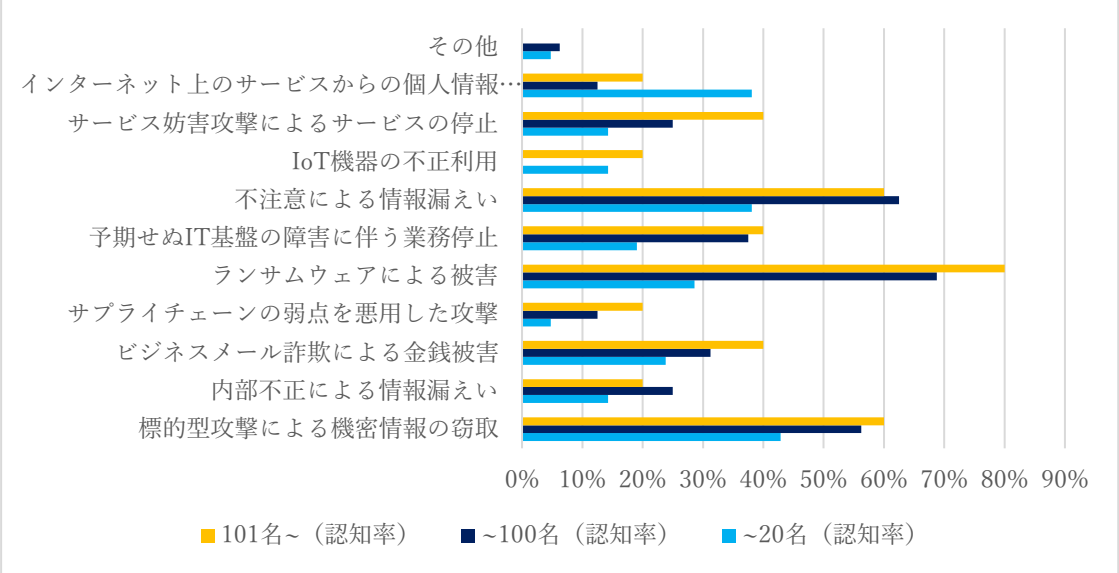


図 40 Q2 への回答

「その他」のコメントは以下の通り。

- ✓ 社員の IT 教育不足
- ✓ ウイルス感染に起因する迷惑メールの拡散での信用の毀損

③　Q3.貴社で今後導入を検討しているサイバーセキュリティ対策をお教えください。（いくつでも）

企業規模を問わず、ほとんどの企業が導入済のウイルス対策ソフトが最も高い割合となった。これは、アンケートの意図を「ウイルスソフトの最新バージョン適用を続けること」と捉えた企業による回答と推察される。企業規模が大きくなるほど、社員教育やセキュリティ管理者の設置のような組織的な対策に注力している。セキュアな拠点間通信、セキュアな無線環境のようなインフラの整備については関心が薄いという結果となった。

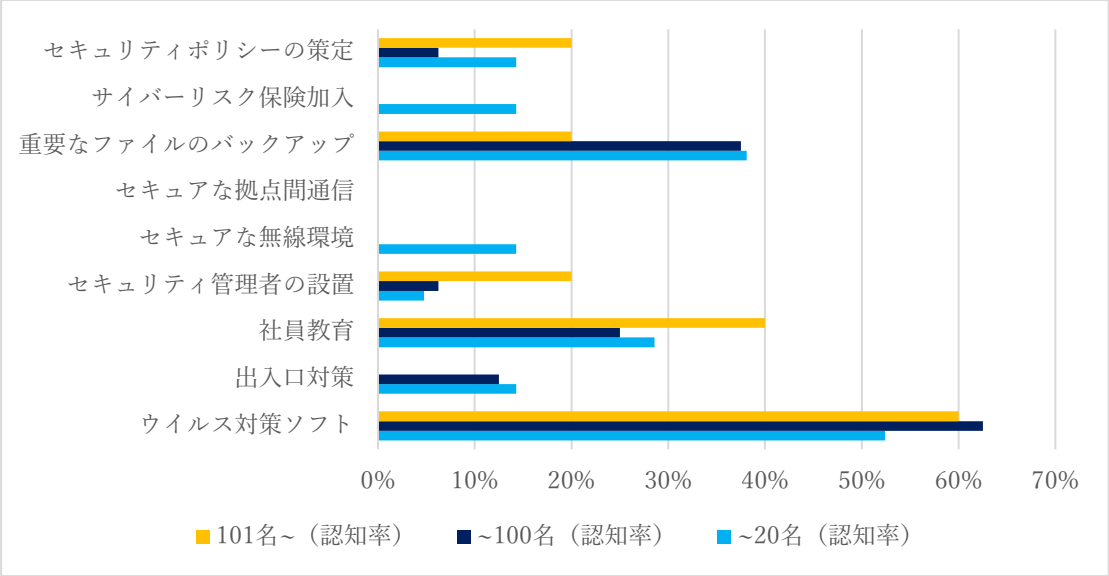


図 41 Q3 への回答

④　Q4.現在サイバーセキュリティ対策にかかっている月額費用はいくらぐらいですか。

事前アンケート回答に比べると、サイバーセキュリティ対策にかけている月額費用は 20 名以下の企業では高め、21 名～100 名の企業は同等、101 名以上の企業では低めという結果となった。実証後アンケートに回答した企業は、規模が小さいほど、もともと意識が高く、規模が大きいほど、もともと意識が低かったという傾向が現れた。

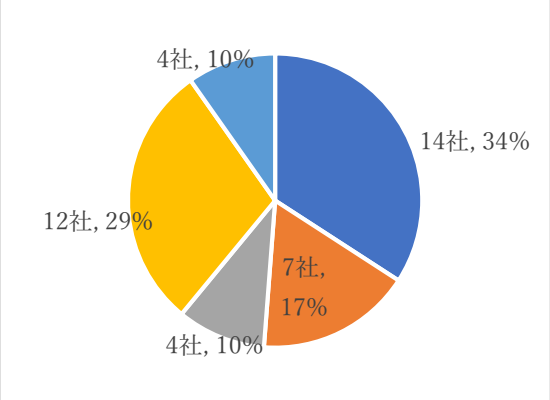


図　42 Q4 への回答（全体）

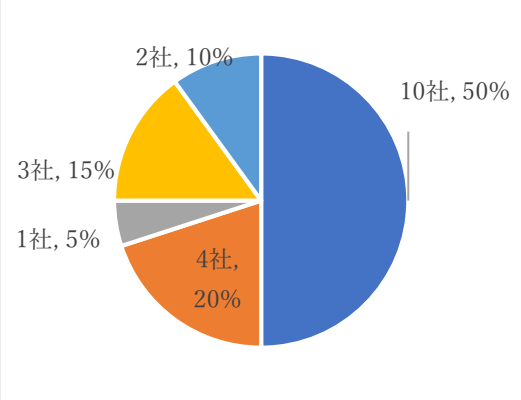


図　43 Q4 への回答（～20 社）

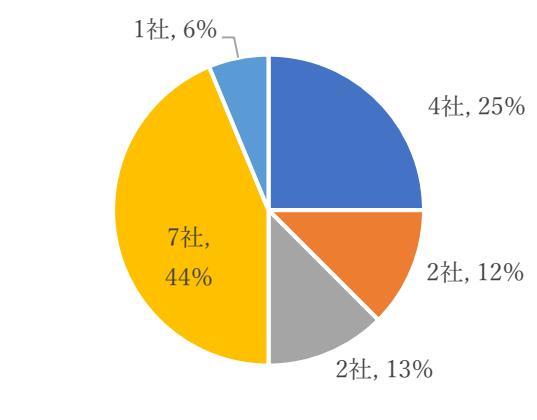


図　44 Q4 への回答（21～100 社）

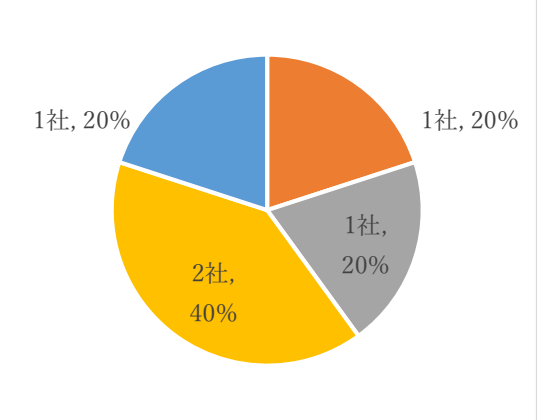
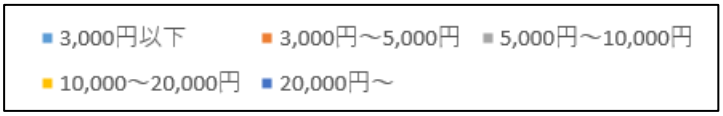


図　45 Q4 への回答（101 社～）

＜凡例＞



⑤　Q5.今後サイバーセキュリティ対策にかける月額費用はいくらぐらいを見込んでいますか。

サイバーセキュリティ対策にかける費用は現状維持が 40%～50%で、どの企業規模でも最も大きな割合を占めた。サイバーセキュリティ対策に関心は示しつつも、コストをかけられないという、中小企業の実情が推察される。

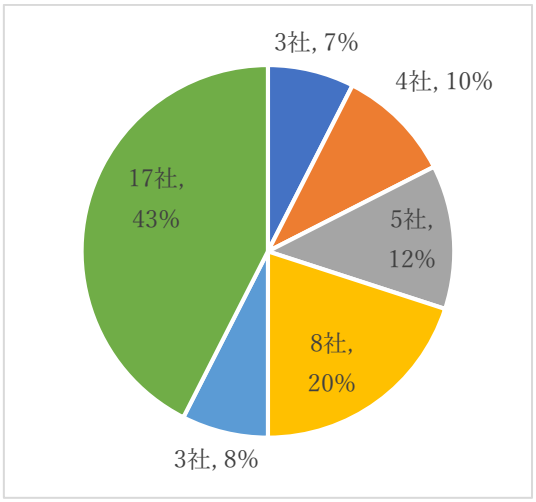


図 46 Q5 への回答（全社）

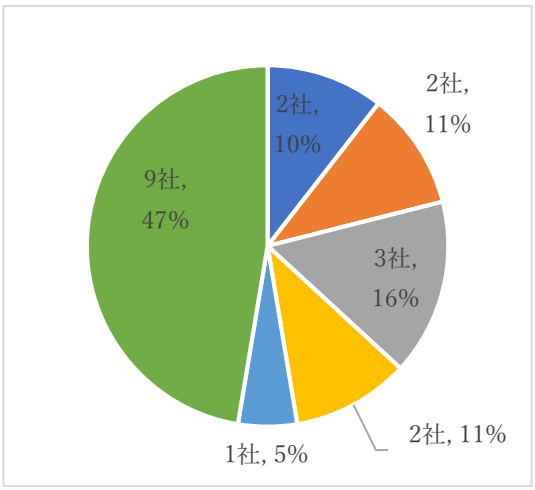


図 47 Q5 への回答（～20 社）

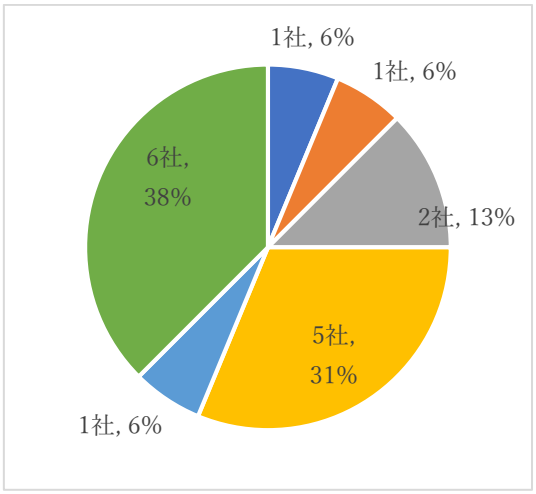


図 48 Q5 への回答（21～100 社）

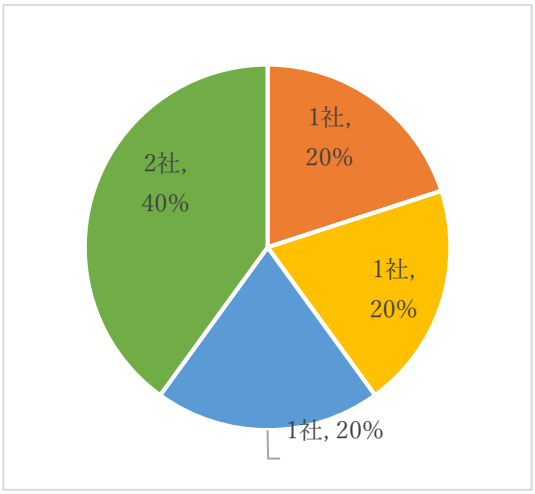


図 49 Q5 への回答（101 社～）

＜凡例＞

⑥　Q6.サイバーセキュリティ対策に関して、貴社の課題を教えてください

各社とも、課題認識を持っていることがうかがえる結果となった。その中でも、セキュリティ対策予算の確保は 101 名以上の企業で突出している。他の規模の企業でも 35%程度が課題と認識しており、サイバーセキュリティ対策の予算化の難しさが表出した。

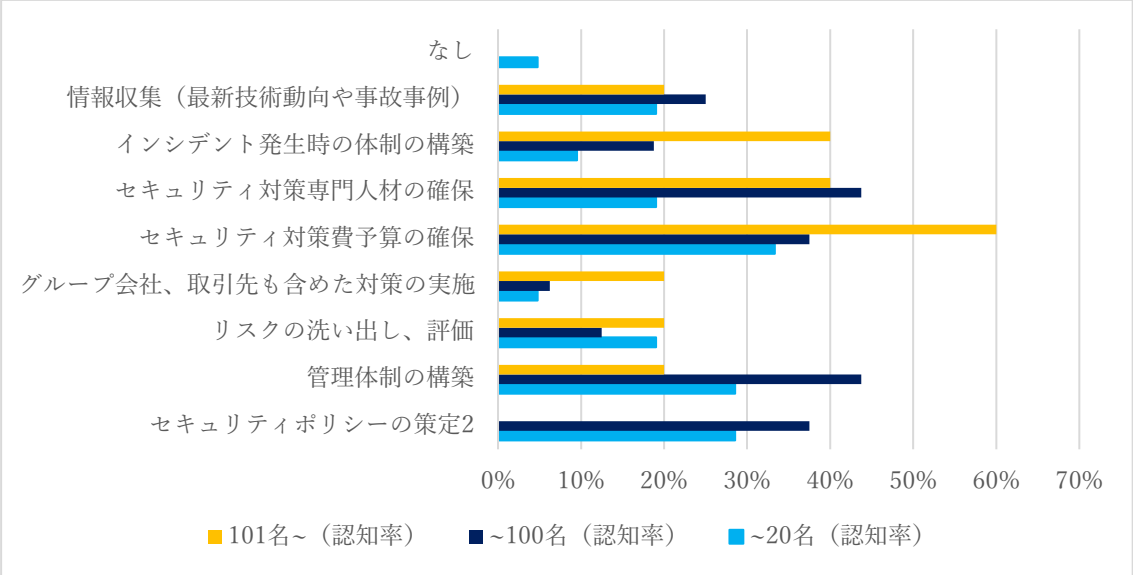


図 50 Q6 への回答

⑦　Q7.セキュリティ対策機器の設置により、総合的なサーバーセキュリティの脅威について意識の変化はありましたか

意識の変化は規模の小さい企業の方が高い割合となった。脅威の認識自体は規模の大きい企業の方が高い割合となった。

100 名以下の会社では実証後も特に意識が変わらない企業の割合が 30%を占めており、脅威に対する温度差が見受けられる。

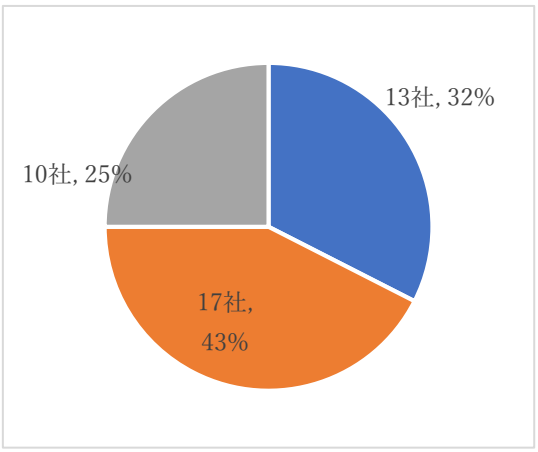


図 51 Q7 への回答（全社）

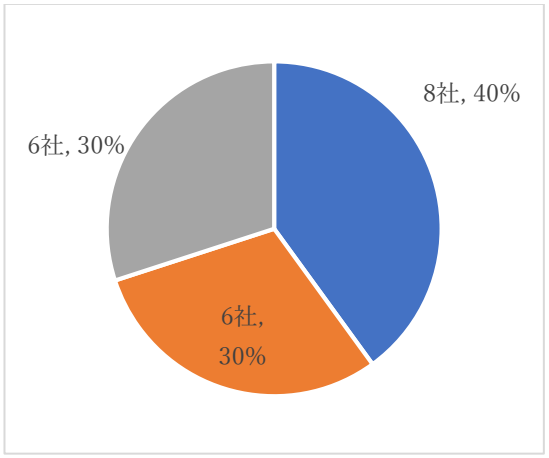


図 52 Q7 への回答（~20 社）

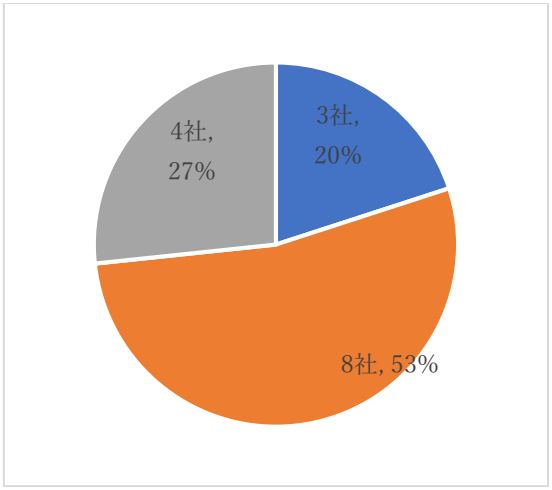


図 53 Q7 への回答（21~100 社）

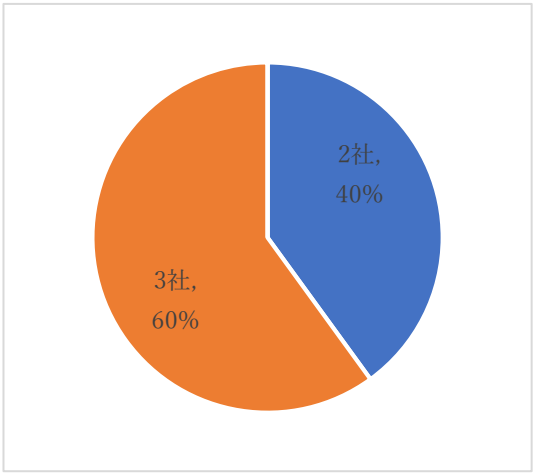


図 54 Q7 への回答（101 社~）

＜凡例＞

⑧　Q8.お客様ホームページの脆弱性診断の実施（一部のお客様）により、Web サイト上の脅威について意識の変化はありましたか

ホームページの脆弱性に対する脅威の実感や、意識の変化はサイバーセキュリティ対策全般に比べると低いという結果となった。サイバーセキュリティ対策の必要性は認識しているものの、自社の具体的な要件としての意識には差がある。

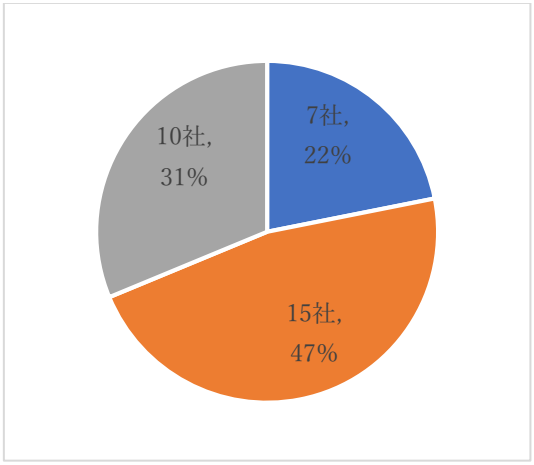


図 55 Q8 への回答（全社）

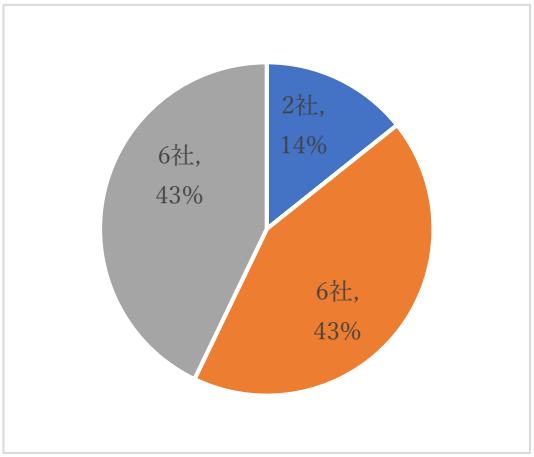


図 56 Q8 への回答（~20 社）

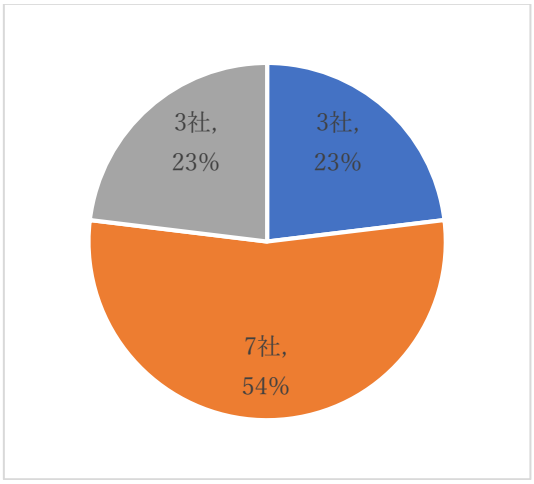


図 57 Q8 への回答（21~100 社）

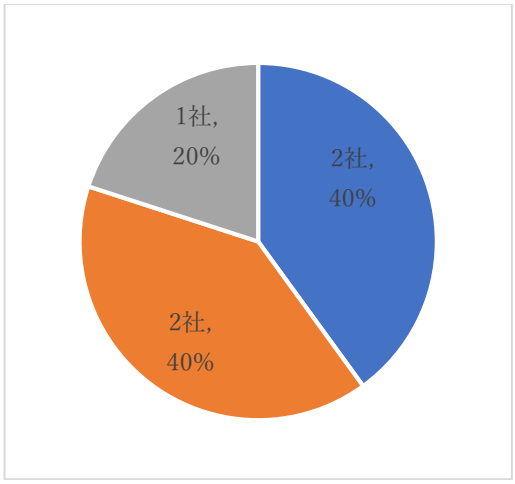


図 58 Q8 への回答（101 社～）

＜凡例＞

⑨　Q9.標的型攻撃メールの疑似訓練の実施により、なりすましメールの脅威について意識の変化はありましたか

21 名以上の企業は、Q8 とほぼ同一の割合となった。20 名以下の企業では、Q8 に比べて脅威を実感する割合が高かった。日常利用するツールに対する脅威への気づきとなったと考えられる。

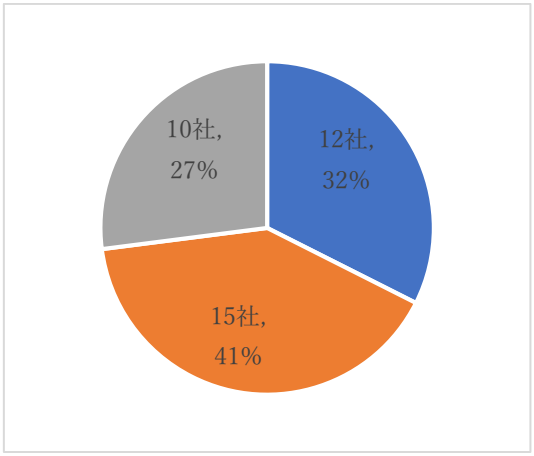


図 59 Q9 への回答（全社）

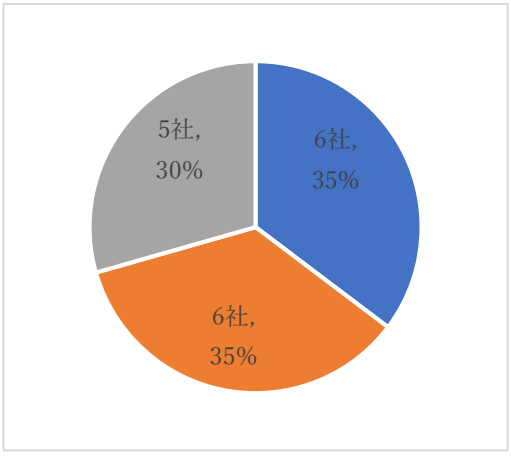


図 60 Q9 への回答（～20 社）

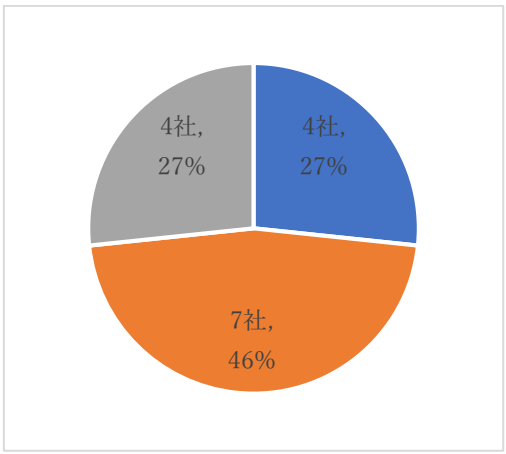


図 61 Q9 への回答（21～100 社）

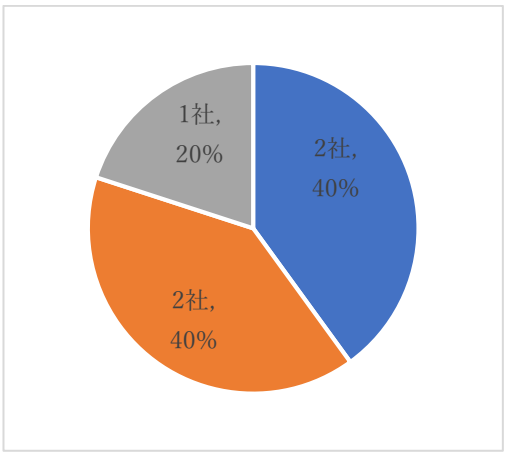


図 62 Q9 への回答（101 社～）

＜凡例＞

⑩　Q10.情報セキュリティ対策 e ラーニングの内容は、現状の動向の把握や今後のセキュリティ対策を検討する上で役に立つ内容でしたか

受講した方はほとんどが有益であったと回答している。非受講者が 50%を占めており、情報セキュリティ対策に対する知識習得の機会を逃す結果となった。

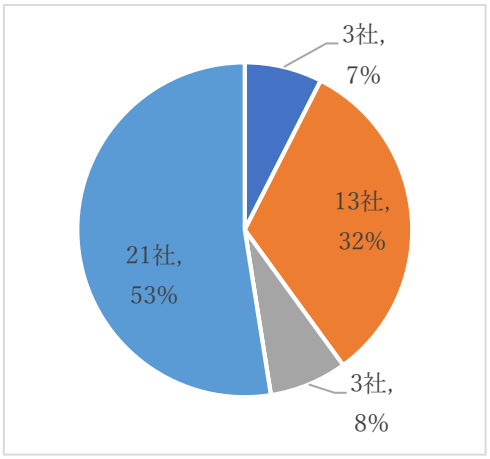


図 63 Q10 への回答（全社）

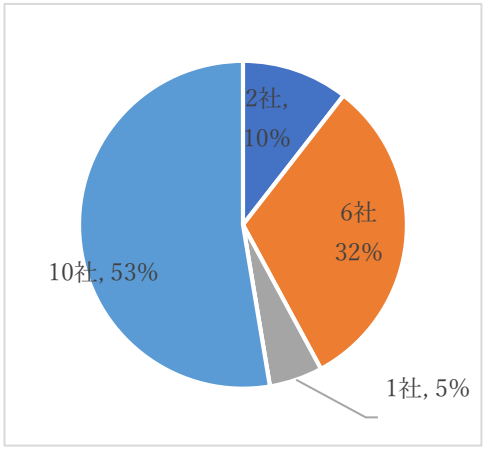


図 64 Q10 への回答（～20 社）

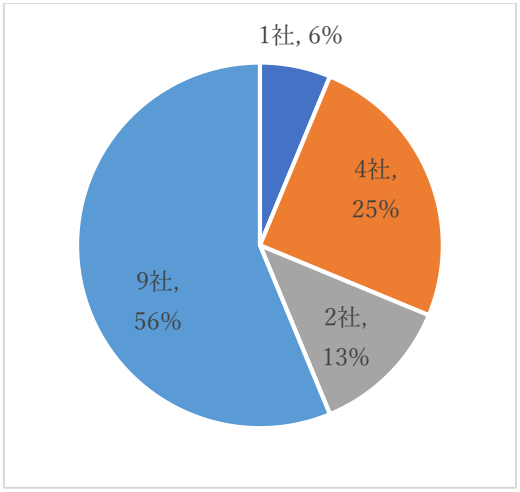


図 65 Q10 への回答（21～100 社）

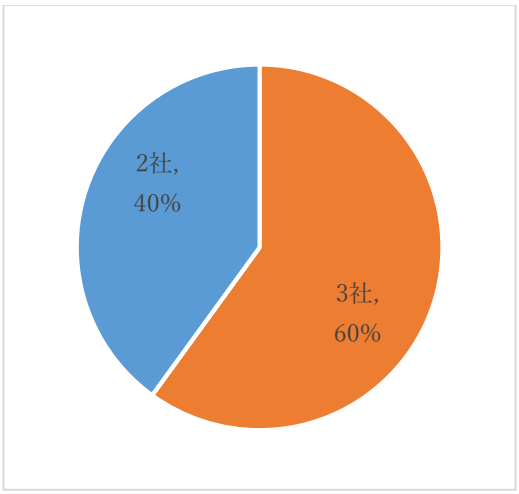
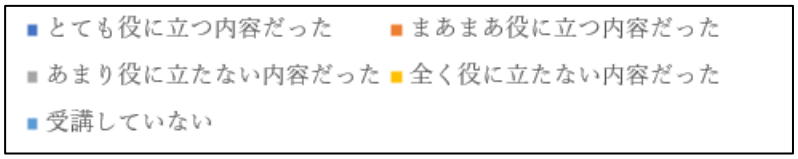


図 66 Q10 への回答（101 社～）

＜凡例＞



⑪　Q11.Q10 で＜受講していない＞とお答えいただいた方にお聞きします。受講されなかった理由について教えてください（いくつでも）

どの企業規模においても、受講できなかった理由の大半は時間を確保できなかったとのことである。中小企業には、物理的に時間が確保できない実情があることが確認できる。これは、社員教育を実施できない理由とも考えられる。

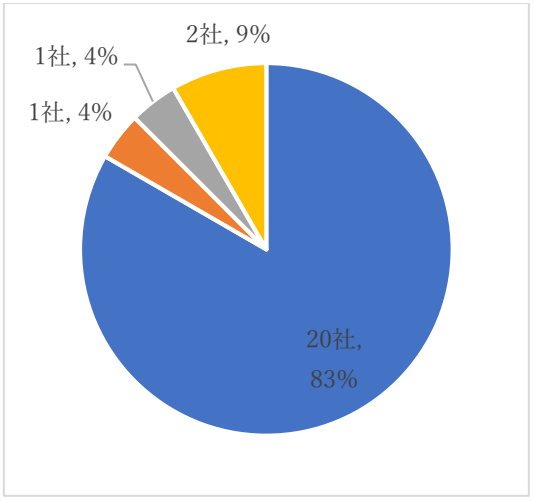


図　67 Q11 への回答（全社）

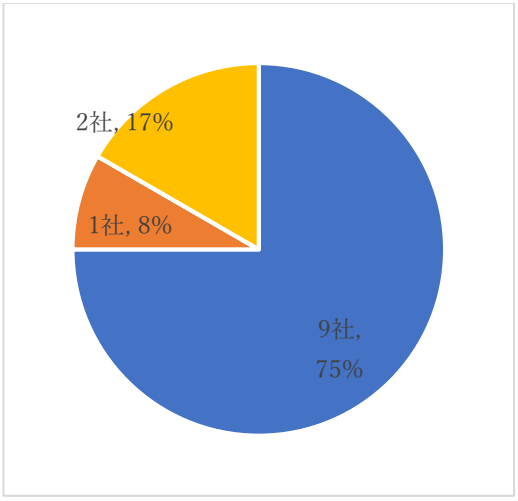


図　68 Q11 への回答（~20 社）

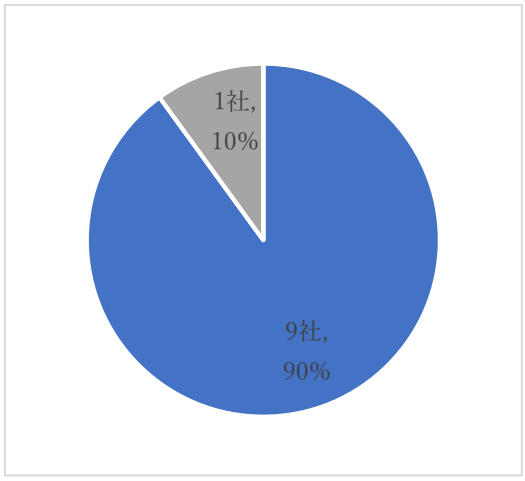


図　69 Q11 への回答（21~100 社）

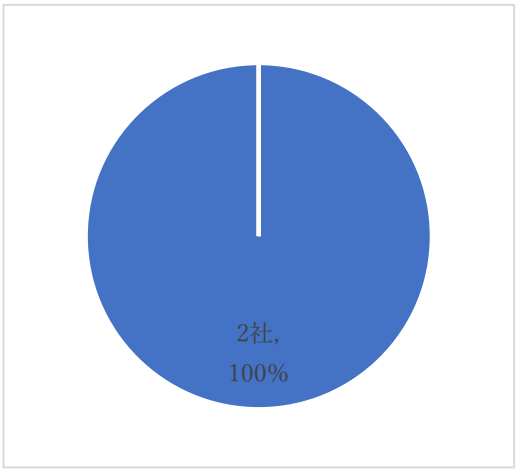
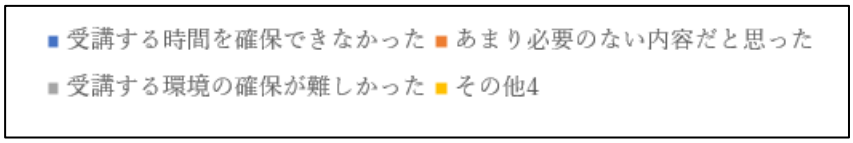


図　70 Q11 への回答（101 社~）

＜凡例＞



「その他」と回答した企業のコメントは以下のとおり。

- ✓　情報がなかった
- ✓　Windows を使用していない

⑫　Q12.本実証事業の参加を通じて、サイバーセキュリティに関する意識は変わりましたか

多くの企業が意識を変えるきっかけとなったと回答している。21 名~100 名規模の企業では 6 社（38%）が特に意識は変わらないと回答しており、高い割合を占めている。もともと意識が高かったため、意識が変化しなかったのか、サイバーセキュリティに対する関心が低いのか、あいまいな結果となった。

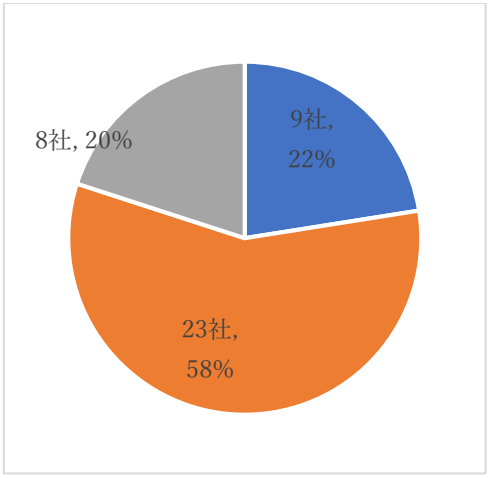


図 71 Q12 への回答（全社）

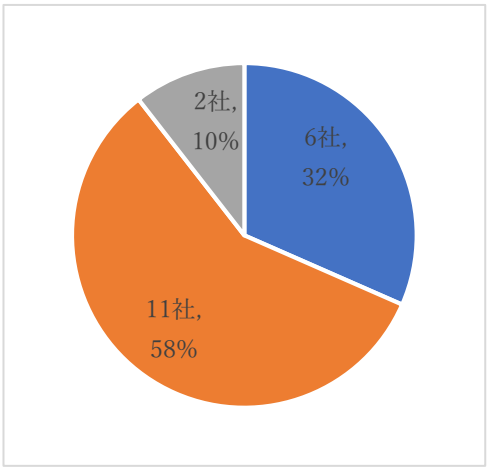


図 72 Q12 への回答（~20 名）

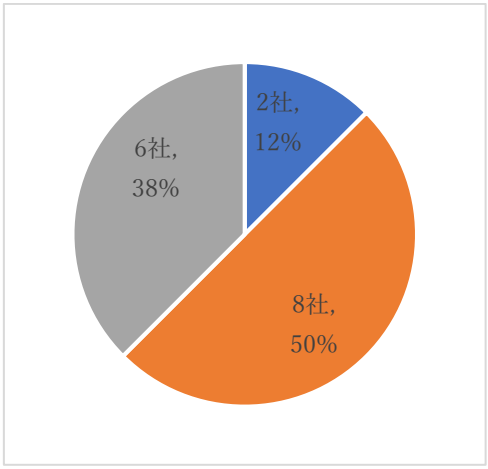


図 73 Q12 への回答（21~100 名）

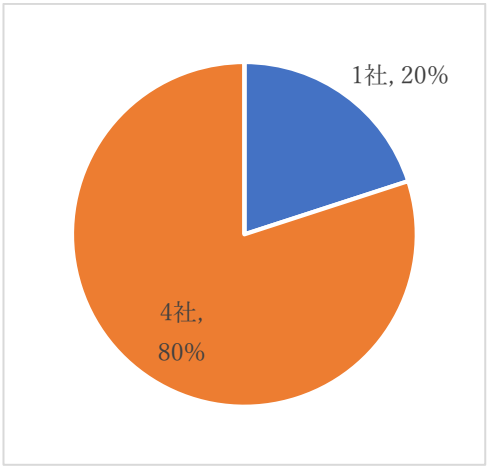


図 74 Q12 への回答（101 名~）

＜凡例＞

⑬　Q13.情報漏えいやシステム停止などのインシデントが発生した場合の対応方針（手順・連携先など）を決めていますか

インシデント発生時の対応方針を決めているのは 3 社（全体の 7%）と極めて低い。検討している企業を含めると半数以上、101 名以上の企業では 100%となったが、時間捻出が厳しい中小企業は、対応方針の整備は今後も検討状態が続くことが懸念される。

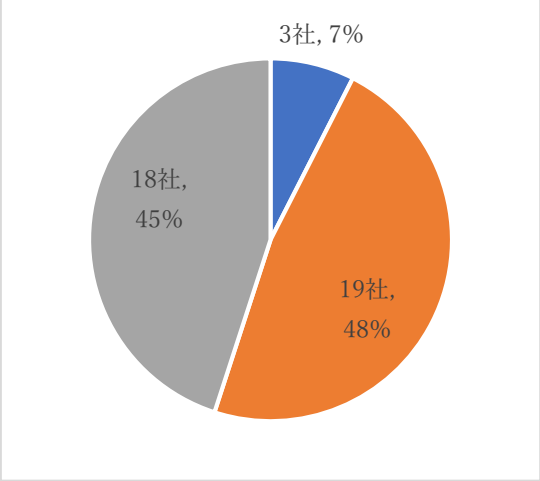


図 75 Q13 への回答（全社）

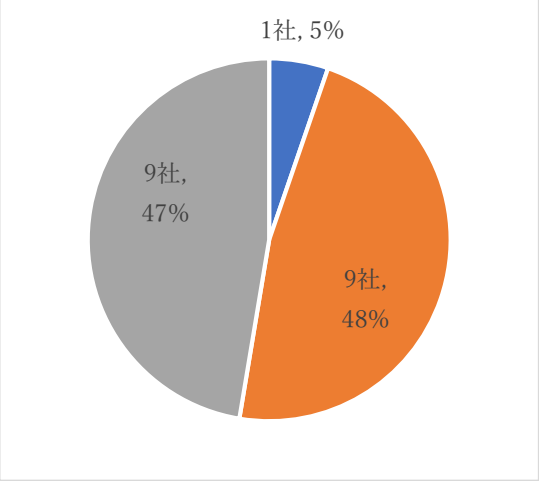


図 76 Q13 への回答（~20 名）

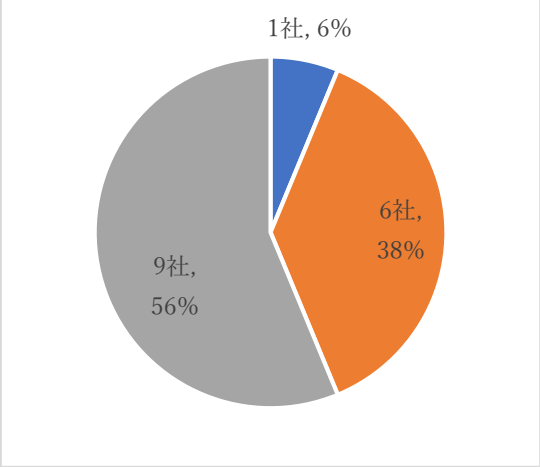


図 77 Q13 への回答（21~100 名）

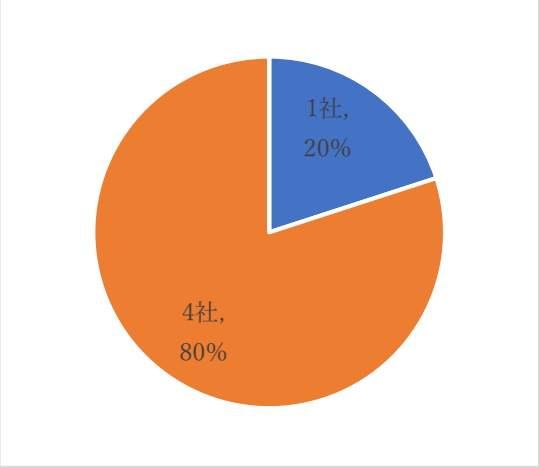
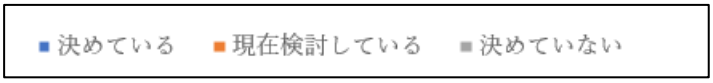


図 78 Q13 への回答（101 名~）

＜凡例＞



⑭　Q14.情報漏えいやシステム停止などのインシデントが発生した場合に発生する費用の予算を確保していますか

現在、予算を確保している企業は 20 名以下の 1 社（全体の 3%）であった。サイバーセキュリティ対策に対する経営面での支援は非常に厳しい状況であると推察される。

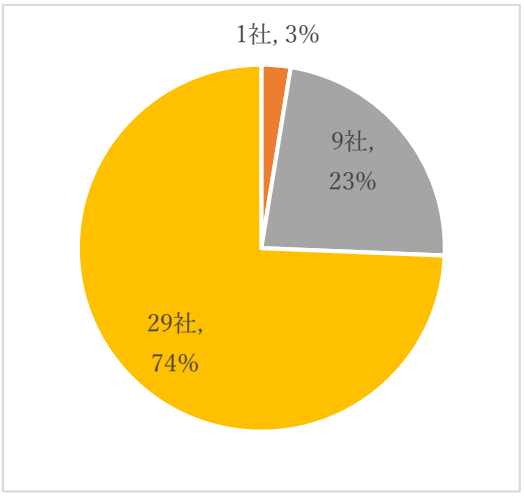


図 79 Q14 への回答（全社）

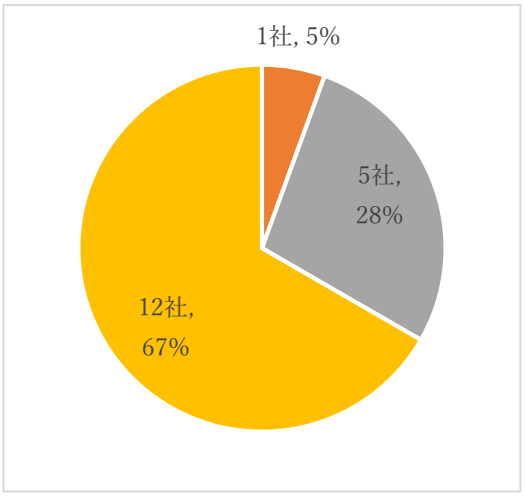


図 80 Q14 への回答（~20 社）

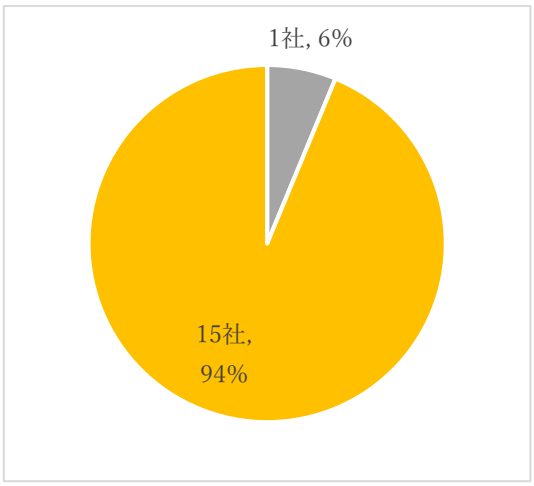


図 81 Q14 への回答（21~100 社）

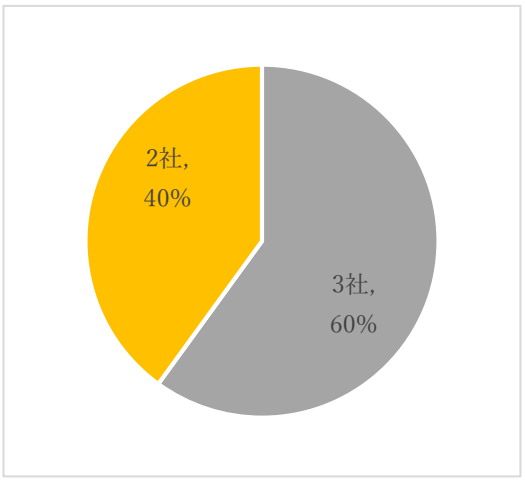


図 82 Q14 への回答（101 社~）

＜凡例＞

⑮　Q15.外部からの不正アクセスや情報漏えいに備える保険（サイバーリスク保険）があることを知っていましたか

保険に関しては、企業規模を問わず 40%（16 社）が知っているという結果となった。

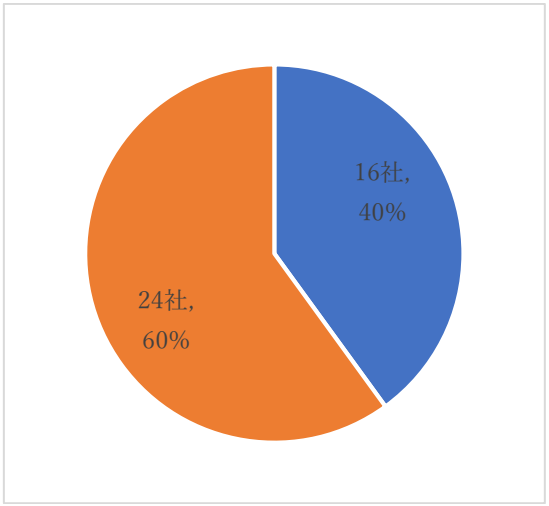


図 83 Q15 への回答（全社）

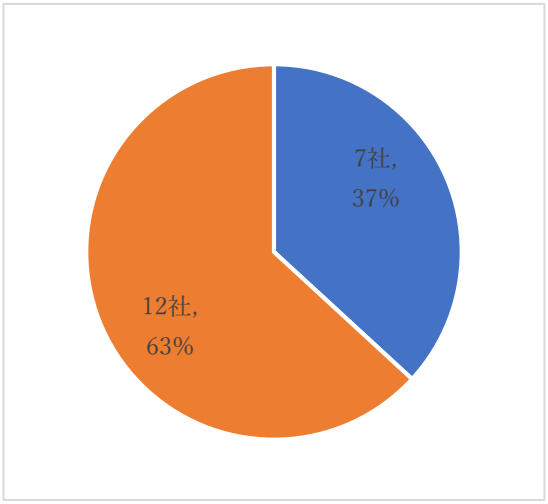


図 84 Q15 への回答（~20 社）

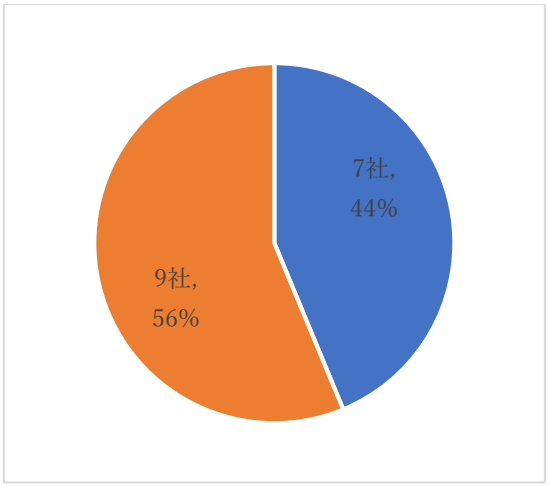


図 85 Q15 への回答（21~100 社）

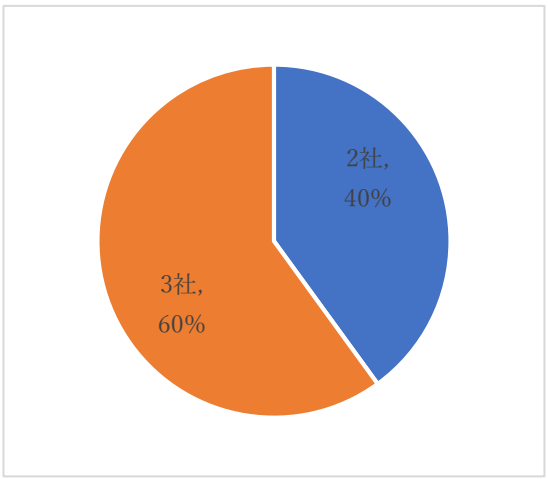
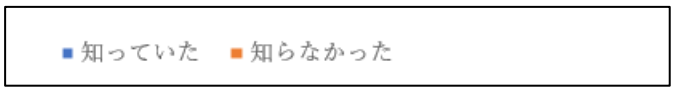


図 86 Q15 への回答（101 社~）

＜凡例＞



⑯　Q16.サイバーセキュリティ対策としてサイバーリスク保険を活用したいと思いますか

保険を検討したい企業は 4 社（10%）と少ない。101 名以上規模の企業では 40%が保険を検討したいと考えている。これは、企業規模に比例して取り扱う情報量も多いことが要因と想定される。

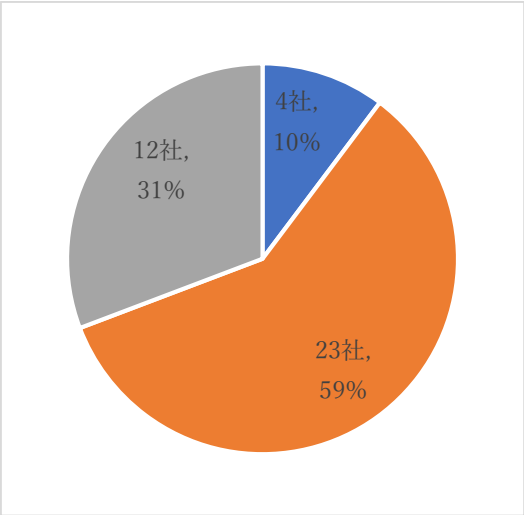


図 87 Q16 への回答（全社）

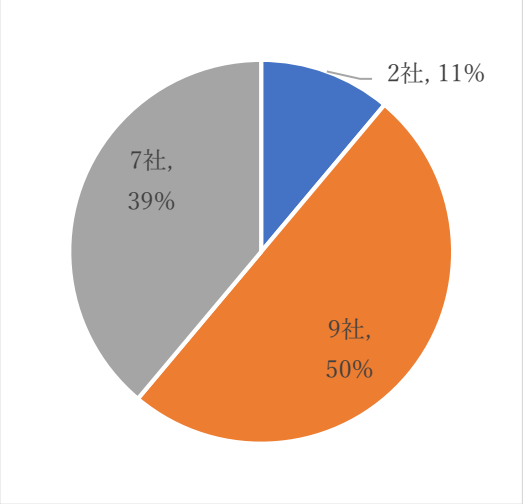


図 88 Q16 への回答（~20 社）

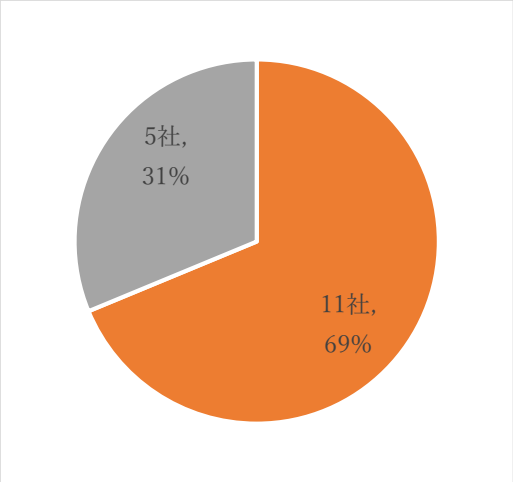


図 89 Q16 への回答（21~100 社）

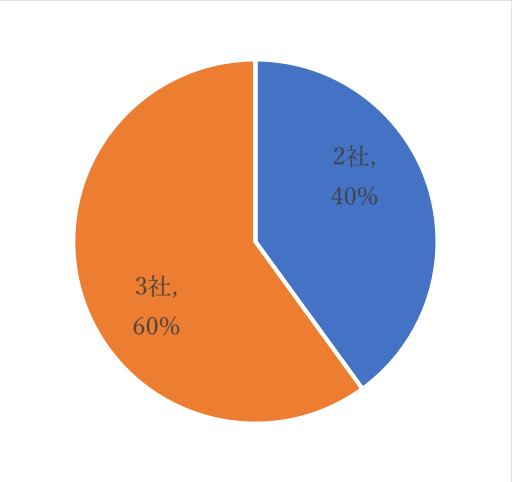


図 90 Q16 への回答（101 社~）

＜凡例＞

⑰　Q17.サイバーリスク保険についての詳細説明を希望されますか

※希望しない以外をご回答いただいた方には、東京海上日動火災保険株式会社よりご案内のご連絡をさせていただきます

保険を検討はするものの、具体的なプラン作成や情報収集を希望する企業は少ない。今回情報収集を希望しなかった企業は、自社と取引のある損害保険会社に相談するのが先決と判断したのではないかと考えられる。

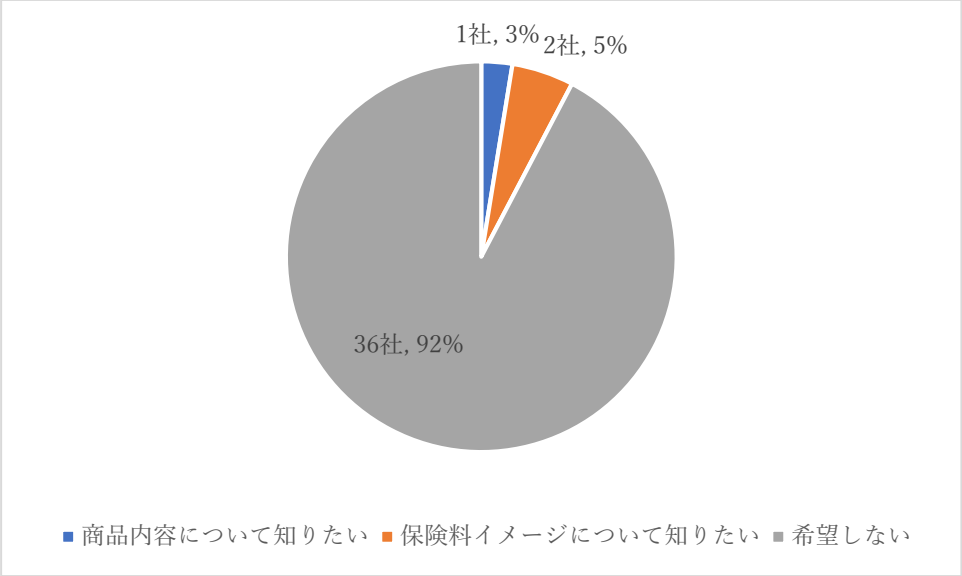


図 91 Q17 への回答（全社）

⑱　Q18.SECURITY ACTION（セキュリティ対策自己宣言）についてご存知ですか

SECURITY ACTION の認知度は低く、33 社（83%）が知らないと回答している。101 名以上の企業では 40%（2 社）が登録している。登録の経緯は不明だが、企業規模が大きい方が高い登録率となった。

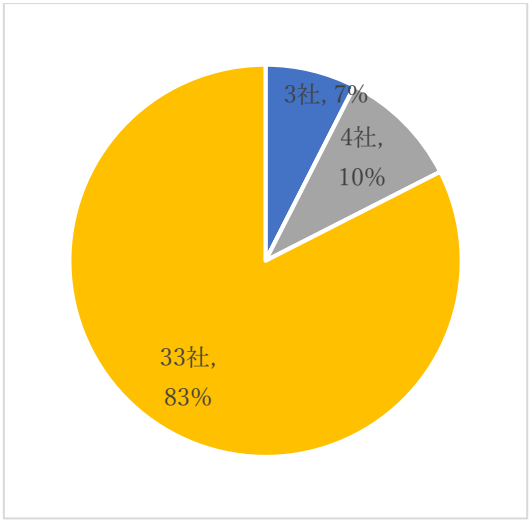


図 92 Q18 への回答（全社）

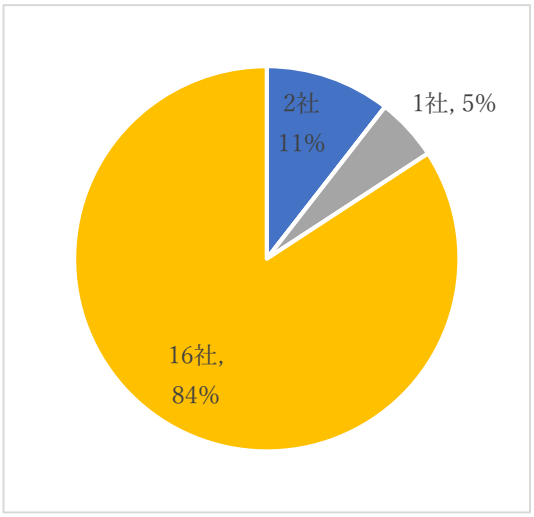


図 93 Q18 への回答（~20 名）

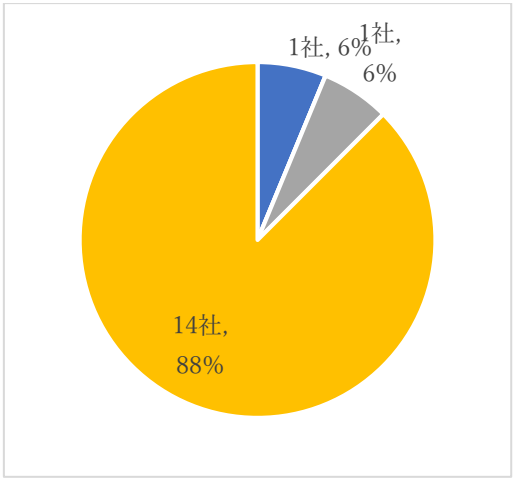


図 94 Q18 への回答（21~100 名）

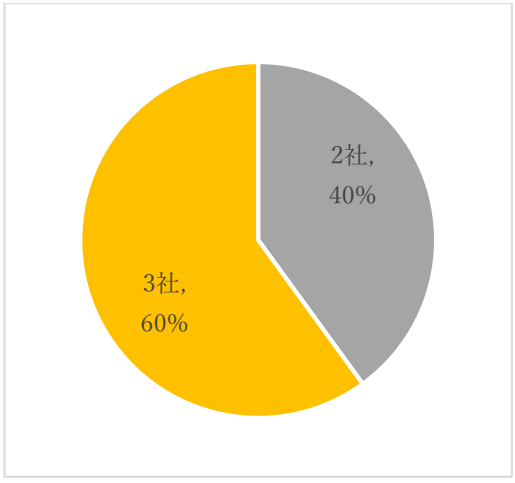


図 95 Q18 への回答（101 名~）

＜凡例＞

⑲　Q19.Q18 で＜知っているが、宣言していない／知らない＞とお答えいただいた方にお聞きします。今後宣言される予定はありますか

SECURITY ACTION 未登録の企業は、登録の意思はほぼない。101 名以上規模の企業が、1 社のみ登録を希望するという結果となった。今回の回答企業は多忙につき、情報セキュリティ対策 e ラーニングも受講が滞っている状態であるため、SECURITY ACTION 登録の実効性やメリットが把握しづらいものと思われる。

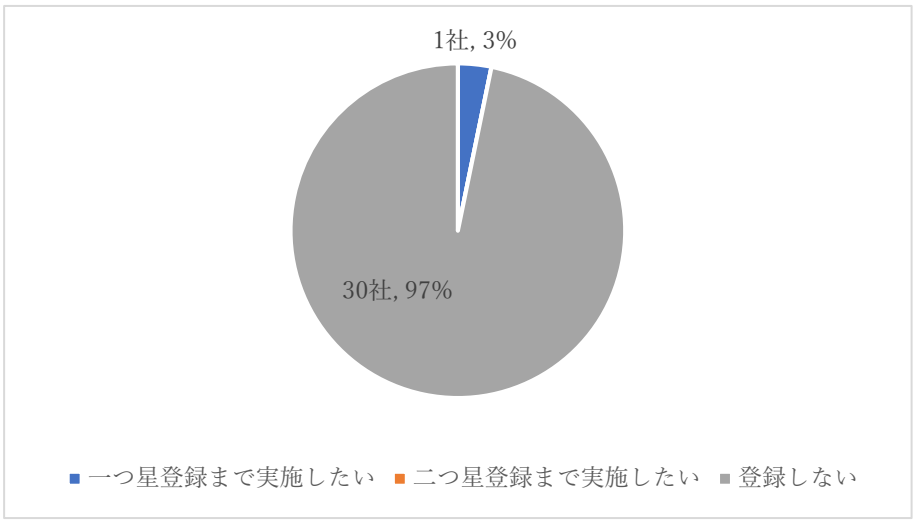


図 96 Q19 への回答（全社）

⑳　Q20.ご意見・ご要望等を自由にご記入ください。（自由回答・任意）

挙がった意見を以下に記載する。ただし、実証に対する要望は割愛する。

- ✓ 実際に UTM のデータを見るとセキュリティ上の不足している所が分かった。全体を管理することは難しいので出入り口である程度防いでくれると安心感が強い。現在は釧路だけに導入したが、札幌支社についても検討したい。

5.2 事前の出入り口対策や事後の措置、保険による補償に対する必要性についての意識変化

今回のアンケートにより、中小企業のサイバーセキュリティに関する意識は高まったことが確認できた。特に現在サイバーセキュリティ対策を十分に行えてない 20 名以下の企業において、対策の必要性に関する意識付けとなった。21 名以上の企業も脅威を感じており、101 名以上の企業に至っては、全企業が脅威を認識する結果となった。Web サイトに対する攻撃の実態、なりすましメールによる実施訓練から、脅威を感じる企業が 60%程度となっており、今後サイバーセキュリティ対策を検討するきっかけになったと考えられる。

一方で、e-ラーニングは 50%を超える企業が未受講と回答している。未受講の理由は受講時間が確保できないが大部分を占める。受講した企業の大半が e-ラーニング受講が役に立ったと回答していることを考えると、今後中小企業がサイバーセキュリティ対策を検討、実施するためには、それなりの体制、時間を投入するという経営判断が重要と考えられる。

予算確保が課題であると回答した企業の多さにも着目したい。出入り口対策や事後の措置について、関心を持ちつつも対応できないのは、時間的制約に加え、予算を確保できていない実情が障壁となっている。今回の実証において意識変化した企業が、投資対効果を考慮してサイバーセキュリティ対策の予算を確保し、導入の機運を高めることが中小企業のサイバーセキュリティ対策を次のステップに進めるために重要となる。

6. 本実証における普及啓発活動の実施報告

6.1 企業向けセキュリティセミナーの実施報告

6.1.1　北海道地域情報セキュリティセミナー

（1） 開催概要

① 開催日程　：　令和 2 年 12 月 1 日（火）13 時 15 分～16 時 20 分

② 開催手法　：　ライブ配信（YouTube チャンネルにて Web オンライン開催）

③ 主催　　：　北海道地域情報セキュリティ連絡会（以下、HAISL）

④ プログラム：

- 情報提供【HAISL 事務局・会員から】
- DX with CyberSecurity【グローバルセキュリティエキスパート株式会社】
- サイバーセキュリティお助け隊（北海道）中間報告【NTT 東日本】
- サイバー攻撃演習～ゲームで学ぶ対処手順～【NTT 東日本】

（2） 開催結果

① 参加者数（対象：企業の経営者・サイバーセキュリティ担当者、支援機関、学生等）

- 最大接続数　90 人

② サイバー攻撃演習のアンケート結果（回答数 21 件）

- ゲーム形式の内容は評価が高く事故対応（インシデント対応）を学ぶ効果がある。実機やソフトウェア等のよりテクニカルなリアリティを求めるニーズもある。
- Q１：難易度とその理由

難易度	理由	回答数
非常に簡単	講師の説明がわかりやすかった	1
普通	（内訳） ・自身の保有する知識を活用して答えが出せたため ・本日のセミナー参加等で得た知識を活用して答えが出せたため ・自分の知識では答えが出せなかったため ・未回答	7 (4) (1) (1) (1)
難しい	（内訳） ・未回答 ・本日のセミナー参加等で得た知識を活用して答えが出せたため ・自分の知識では答えが出せなかったため	5 (3) (1) (1)

・　Q２：サイバー攻撃演習の良かった点

ゲーム形式で楽しかった	7
ゲーム形式で受け入れやすかった	6
各ステップがつながっていてトラブルの相関性を理解できた	5
ストーリーやシナリオに納得感があった	4
ゲームの流れ・仕組みがわかりやすかった	3
実際に体験しているように学べた	3
損害額により正解との乖離がわかりやすかった	3

・　Q３：サイバー攻撃演習の悪かった点

ツールの文字等が見えづらく操作しにくい	3
実際の機器やソフトウェア等が無いと、リアル感が無い	3
ツールが動作しない、動作が不安定	1
ストーリーやシナリオに納得感が無い	1
制限時間が短い、事前のヒントが多すぎる	1
特に無し	1

・　Q４：演習で得た事・感じた事

セキュリティ事故発生後の行動が大切だということ	9
セキュリティ事故への対応イメージが湧いたこと	5
より難易度の高いサイバー攻撃演習を行いたいと感じたこと	4
セキュリティ分野に興味をもったこと	3

6.1.2　お助け隊事業（北海道）成果報告会　兼　セキュリティ対策セミナー

（1） 開催概要

① 集合・Web オンライン同時開催

・開催日程　：令和 3 年 1 月 19 日（火）13 時 30 分～15 時 30 分

・集合場所　：札幌市中央区北 1 西 2 北海道経済センター

・Web 開催手法：ライブ配信（Microsoft Teams にて Web オンライン開催）

② Web オンライン開催のみ

・開催日程　：令和 3 年 1 月 20 日（水）10 時 00 分～15 時 30 分

令和 3 年 1 月 20 日（水）13 時 30 分～15 時 30 分

・Web 開催手法：ライブ配信（Microsoft Teams にて Web オンライン開催）

③ 主催　　：　NTT 東日本

④ プログラム ：

- 中小企業向けサイバーセキュリティ対策支援体制構築事業（サイバーセキュリティお助け隊事業）成果報告【NTT 東日本・東京海上日動火災保険（株）】
- セキュリティ対策セミナー「最新のサイバー脅威動向とセキュリティ対策の強化」【トレンドマイクロ（株）】
- SECURITY ACTION 制度等のご紹介「中小企業向け情報セキュリティ対策支援事業について」【IPA・IPA セキュリティプレゼンター（NTT 東日本）】
- 採用活動におけるセキュリティ対策「オンライン面接ルームのご紹介」【NTT 東日本】

（2） 開催結果

① 参加者数（対象：お助け隊事業（北海道）実証参加企業、一般企業・団体等）

- 集合　：　3 社（4 名）
- Web オンライン：　最大接続数　16 社（42 名）

② アンケート結果（回答数 7 件、令和 3 年 1 月 22 日時点）

- 「お助け隊事業（北海道）成果報告」だけでなく、セキュリティベンダーによる講演や、コロナ禍での新たなセキュリティ活用ソリューションへの関心度が高い。
- IPA や地域協力団体等からも情報発信することにより、幅広い募集効果が見込める。
- Q１：参加のきっかけ

お助け隊事業者（NTT 東日本）	2
IPA	1
地域協力団体（札幌商工会議所・中小企業診断協会北海道）	4

・　Q２：成果報告会兼セキュリティ対策セミナーの満足度

満足	1
まあまあ満足	2
普通	4

・　Q３：成果報告会兼セキュリティ対策セミナーの時間

やや長い	4
適切	3

・　Q４：特に参考になった・印象に残ったプログラム

セキュリティ対策セミナー	5
サイバーセキュリティお助け隊事業（成果報告）	3
採用活動におけるセキュリティ対策（オンライン面接ルーム）	3
SECURITY ACTION 制度等のご紹介	1

7. 企業活動継続リスクについて

7.1 脅威が顕在化した場合の企業活動継続への影響のシナリオ

必要十分なサイバーセキュリティ対策を講じていないことにより脅威が顕在化した場合、組織の存立さえも脅かされる可能性がある。脅威を早期に取り除き復旧できない場合、事業継続も困難になる。

サイバー攻撃を受けてしまうことで企業が被る可能性のある不利益は、金銭の喪失（損害賠償、不正送金による直接的損失等）や顧客の喪失（社会的評価の低下、顧客離れ等)、業務の喪失（システム停止に伴う営業機会の喪失、社内業務の停滞等）がある。顕在化した脅威の内容によっては、経営者等が法的責任を問われ、損害賠償責任を負うこともある。

これらは企業活動継続に大きなダメージとなる。そのため、事前の防御としてのサイバーセキュリティ対策を必要十分に講じ、万一の際に早期の復旧を可能とするために整備した初動対応マニュアル等に基づく対応により原因特定や応急処置を行い、企業として社会に対する責任を果たすことが求められる

8. まとめ・提言

8.1 企業におけるサイバーセキュリティ対策のあるべき姿

業務効率化や生産性向上のため既に多くの企業が IT を活用している。その際、サイバーセキュリティの必要性や重要性を強く意識し、対策を講じたうえで IT を活用することが求められる。サイバーセキュリティ対策が不十分なまま万一サイバー攻撃を受けてしまった場合、その企業は様々な不利益を被る可能性や、法的責任が問われる可能性があるためだ。

サイバー攻撃に対するセキュリティ対策には物理的対策や技術的対策に加え、組織的対策、人的対策が含まれる。これらの対策には費用を要するため、サイバーセキュリティ対策の費用対効果を踏まえて必要な投資を行うことが企業のあるべき姿といえる。

では、それらのサイバーセキュリティ対策にどの程度の費用をかけるのが望ましいのだろうか。サイバーセキュリティガイドブック『中小企業向けサイバーセキュリティ対策の極意』（東京都産業労働局）[5]よれば、サイバー攻撃による想定被害額を上回る水準のセキュリティ対策費を費やすことは現実的ではなく、セキュリティ対策費が、セキュリティ侵害による想定被害額を上回っている場合は対策費を削減すべきとしている。

加えて、様々なセキュリティ対策を講じてもリスクは残るため、この残留リスクをどこまで許容するかには経営判断が求められる。残留リスクによって発生した被害の想定被害額が、セキュリティ侵害発生時に支出可能な対策費に収まるよう残留リスクを下げる対策を講じることが求められる。

表 22 企業におけるサイバーセキュリティ対策費の考え方

IT 化による想定利益＞IT 化投資額（IT 導入、運用、セキュリティ対策費）
セキュリティ侵害による想定被害額（経済的損失、社会的信用）＞セキュリティ対策費
セキュリティ侵害発生時に支出可能な対策費＞残留リスクによる想定被害額

[5] 東京都産業労働局：サイバーセキュリティ、https://www.sangyo-rodo.metro.tokyo.lg.jp/chushou/shoko/cyber/（2021/1/18 参照）。なおガイドブック本文は以下で公開されている。https://www.sangyo-rodo.metro.tokyo.lg.jp/chushou/guidebook_full.pdf

8.2 サイバー保険のあるべき姿

中小企業が継続して利用可能な保険商品の検討にあたり、本実証において「対策の実態と課題の把握」と「仮説に基づく具体的サービスの検討」を実施した。

実証の内容を踏まえ、中小企業が考えるセキュリティ対策と現状のギャップとそれを踏まえた具体的なサービス内容を考察する。

8.2.1　実証を踏まえた中小企業のセキュリティ対策の実態

実証参加企業のうち「サイバーセキュリティ対策に関心がある」と回答した企業は約 95%と非常に高い水準であり、多くの企業がセキュリティ対策に関心を抱いている。

また実証参加企業のうちサイバーセキュリティの課題として、「インシデント発生時の体制の構築」「最新動向や事故事例などの情報収集」を挙げている企業は約 38%である。

これらの高いニーズや課題感の一方で、導入している対策に「サイバーリスク保険」を挙げた企業は約 5%であり、中小企業が課題としている領域に適切に対処できていない状況が顕在化した。

加えて、今後導入を検討する対策に「サイバーリスク保険」を挙げた企業は約 7%であった。

8.2.2　実証を踏まえた中小企業のセキュリティ対策の課題

上記のとおり、サイバーセキュリティに関心がある企業がほとんどであり、インシデント発生時の体制構築を課題に挙げている企業も一定数存在するにも関わらず、サイバーリスク保険の普及が進まない要因は、以下の 2 点であると考察する。

① 対策の優先順位における課題

アンケートにおいてセキュリティ対策導入を検討できる価格帯は 10,000 円未満が全体の約 65%を占め、そのうち過半数は 5,000 円未満と回答する等、限られたコストでセキュリティ対策全般を検討せざるを得ない実態がある。

事後の対策であるサイバーリスク保険までコストが配分されず、優先順位が後位となっていると考察する。

② サイバーリスク保険の認知度における課題

上記のとおり、限られたコストでセキュリティ対策を講じなければいけない状況下において、インシデント発生時のファイナンス機能の重要性をより一層訴求していく必要がある。現時点では、「ウイルス対策ソフト」や「社員教育の実施」といったマーケットに浸透している入口の対策が中心となっており、サイバーセキュリティ対策というキーワードでサイバーリスク保険を連想しづらい状況下にあると考察する。

8.2.3　具体的なサービス内容の検討

セキュリティ対策は予防としての事前の対策とインシデント発生後の事後の対策を総合的に検討、導入する必要がある。実証参加企業のセキュリティ対策の実態や課題を踏まえ、サイバーリスク保険の具体的なサービス内容を以下のとおり考察する。

① 見舞金サービスの提供

不正アクセス等のインシデントが確定した場合、一律 10 万円を見舞金としてユーザーに提供する。ユーザーは見舞金を初期対応費用等に充当することができる。一方で、10 万円の見舞金は重大なインシデント発生時の対応費用としては過少である。また、見舞金サービスを提供する場合は、単体では販売できず、ウイルス対策ソフトや UTM 等に付随するサービスとして販売する必要がある。

② 復旧サービス等の実質無償提供

インシデント発生時のパソコン環境復旧作業等のサービスを利用するための費用を補償する。これまで有料で提供していたサービスの料金を平準化して既存サービスに組み込むことで、ユーザーにとっては追加料金がなく、有事の際にサービスを享受できる仕組みとなる。各種復旧サービスや駆けつけ費用を組み合わせ一つのパッケージとして販売することで、中小企業のインシデント発生時の対応を一元的に補償することができる。

③ 再発防止コンサルティング等の実質無償提供

インシデント発生時の再発防止にかかわる費用や社員教育を実施するための費用を補償する。インシデント発生時には損害賠償や顧客対応で再発防止にまで十分に費用や時間がかけられないことが想定される。本サービスでは、十分な再発防止策を立案するコンサルティングや実行のための各種費用を補償することで、サイバーリスクに強い体制構築を実現する。

また、サイバーリスク保険の費用については、アンケートにおいてセキュリティ対策導入を検討できる価格帯は 10,000 円未満と回答した実証参加企業が全体の約 60%を占めている状況から、年間保険料 1,000 円前後での提供が望ましいと考える。

8.2.4 サイバーリスク保険の販売体制について

実証実験の結果および、各種サービス設計を考慮し、中小企業に対するサイバーリスク保険の販売は、以下の方法で実現可能であると考察する。

① セキュリティ対策サービスに保険を自動付帯する

導入ニーズが高いウイルス対策ソフトや UTM 等のセキュリティ商材に保険を付帯することで、ユーザーはセキュリティ商材を導入することで自動的に補償を得ることができ、セキュリティ対策を一気通貫に手配することができる。

② セキュリティ対策サービス提供時の保険代理店との連携

ユーザーがセキュリティ対策サービスを導入時に、サービス販売主体が保険代理店と連携し、カスタマイズしたサイバーリスク保険を販売する。セキュリティ、保険の両軸で協働しリスクコンサルティングを行うことで、ユーザーのニーズに的確に応えることができる。

8.2.5　今後の検討の方針

上記を踏まえ、中小企業を取り巻くサイバーリスクに対する認知度の向上およびインシデント発生時の補償の確保を推進すべく、サービスの検討を継続する。8.2.3 で示したとおり、3 種類の補償制度を検討しているが、実証参加企業のニーズやコストの観点で、現時点では②復旧サービス等の実質無償提供、③再発防止コンサルティング等の実質無償提供の優先順位が高いと考える。最適な補償内容や提供方法でユーザーにセキュリティ対策を届けられる体制を構築していく。

8.3 推奨する企業のサイバーセキュリティ対策と支援体制

企業におけるサイバーセキュリティ対策として、同ガイドブックに示されている具体的な項目を表 23 に示す。同ガイドブックでは技術的対策や物理的対策にどれだけ投資してもリスクは残ることから(残留リスク)、人的対策や組織的対策を優先する方が効果的であるとの考え方が示されている。

表 23 サイバーセキュリティ対策の具体的項目

分類	具体的な項目の例
人的対策	・　セキュリティポリシーの策定 ・　各種社内規定、マニュアルの整備 ・　社員教育・訓練 ・　アクセス管理
組織的対策	・　管理組織の設置・運用 ・　情報資産の分類・持ち出し管理 ・　サイバー攻撃対応マニュアルの整備 ・　事業継続管理
物理的対策	・　コンピューターや通信装置の保護 ・　重要情報の一元管理、入退室管理 ・　アクセスできる区域の制限 ・　クリアデスク、クリアスクリーン
技術的対策	・　本人認証・アクセス制御、権限管理 ・　ウイルス対策 ・　脆弱性対策 ・　暗号技術や認証技術の利用 ・　ファイアーウォールやコンテンツフィルターの設定

企業により IT の利用範囲や内容が異なるため、一様に推奨されるサイバーセキュリティ対策は存在しない。自社の業務内容に適したサイバーセキュリティ対策を講じることが求められる。

その際、情報セキュリティ対策診断（例:IPA の「情報セキュリティ対策ベンチマーク」等）を行うことが有益となる。その結果を参考に、取り組むべきセキュリティ対策や強化すべき対策を把握し、費用対効果を見極めながら対策を講じていくことが推奨される。

上記のようなサイバーセキュリティ対策を講じることが推奨されるが、本実証事業の事前アンケートの結果から現状サイバーセキュリティ対策にかける費用が 10,000 円以下の企業が全体の 77%となっており、対策を講じたいものの予算の確保が難しい状況であることが想定される。そのような中でも、本実証事業での UTM のログからも見て取れるように身近に様々なサイバーセキュリティ脅威が存在していることから、UTM 等の設置による最低限の技術的対策を講じることが推奨される。今

回の実証事業で提供した UTM、標的型攻撃メール訓練、Web セキュリティ診断、e ラーニングの各種サービスは現時点でも多くの企業に利用されているサービスであり、NTT 東日本のサービス以外にも費用対効果が優れているサービスが多数提供されているため、お助け隊事業者側がサイバーセキュリティ対策の重要性を中小企業に訴求することで積極的にサイバーセキュリティ対策に費用を投資するよう促すことが重要となる。また、お助け隊事業者側も新たなサービス開発の際は費用面を考慮し、より多くのユーザーに活用してもらうことを意識することが必要となる。

NTT 東日本では、万が一インシデントが発生した場合の電話一元窓口を設けており、各都道県の主要拠点にインシデント発生時の駆けつけ対応を実施する組織を設けている。また、各地域のニーズや傾向調査のためのマーケティング機能も各都道県の主要拠点に配置しており、エリア特有のニーズのキャッチアップにも注力している。本実証事業では駆けつけ対応が必要となる重大なインシデントは発生しなかったものの、いつ重大なインシデントが発生してもおかしくない状況であることから、現状の体制を維持することが必要となる。

8.4 新たなサービス・支援体制モデル等に関する提言

企業の働き方はテレワークを代表しますます多様化が進み、様々な場所から様々な NW やデバイスを利用し企業の機密情報にアクセスしているのが現状。
実証参加企業のセキュリティ対策の実態や課題を踏まえ、推奨する企業のサイバーセキュリティ対策について以下のとおり考察する。

① クラウドアプリケーション向けのセキュリティ対策

社内やテレワーク先で利用するためのツールとして手軽に導入・運用できる Microsoft 365 や Google Workspace に代表される SaaS サービスを活用し、メール、ストレージ、コミュニケーションツールを利用する企業が増加。

SaaS 型サービスはその構成上、元々企業が用意している社内防御機能（UTM、FW 等）が働かないケースが増えるため、SaaS 型サービスに特化したセキュリティ対策が必要。

② エンドポイントセキュリティ対策の強化（EDR）

Emotet や IcedID 等に代表される新種、亜種マルウェアを活用した未知脅威の攻撃が拡大。セキュリティ対策のベースとなる GW 型セキュリティ、エンドポイント型セキュリティ対策といった基本となる多層防御だけでは防ぎきれず、実際に取引先がマルウェア感染したという事例も散見。

EDR、MDR 等の技術やサービスを活用した未知脅威検知や早期発見、対処を実現するセキュリティ対策の強化が必要。

以上