今、中小企業が狙われている!

中小企業情報セキュリティ・アンケート調査結果

～回答企業の 17%が「被害経験あり」～

令和５年２月

横須賀商工会議所

監 修/株式会社ワールドスカイ
協 力/日本マイクロソフト株式会社

「横須賀市の中小企業セキュリティ対策調査」に関する結果報告を発表
～中小企業が直面するサイバーセキュリティ対策の脆弱性と課題～

（はじめに）

高度情報化社会においては、企業規模を問わず様々なサイバー攻撃によるセキュリティ被害が増加しております。

特に近年、攻撃者の新たなターゲットとして、セキュリティ対策予算や人員が不足しがちな中小企業に向けられており、その企業と取引のある大手企業を攻撃する「入り口」（サプライチェーン攻撃）として狙う手口も散見されます。

このような背景から、横須賀商工会議所では傘下の会員企業向けにセキュリティ問題についてどのように考え、且つ対策を講じようとしているか情報セキュリティソリューション事業を展開している株式会社ワールドスカイ（本社：東京都中央区、代表取締役社長：柳沢　智幸）と日本マイクロソフト株式会社（本社：東京都港区、代表取締役社長：津坂　美樹）と共同で、アンケート調査とヒアリングを実施いたしました。

(調査概要)

本調査では、中小企業のセキュリティ対策への取組み状況および意識調査を行うため、アンケート調査を行いました。アンケート調査結果については、「セキュリティに対する意識調査」「対策状況（技術・組織・人）」の観点でまとめております。また、アンケート調査結果からは得られない諸課題や各企業の考え方などについては個別のヒアリング内容を通じて、関連する項目に記載しております。

○調査方法

アンケート調査は横須賀市の中小企業に対して、情報セキュリティに対する取組み及び状況の把握および意識調査を行う為に実施しました。（実施時期：2022 年 10 月）

アンケート調査のみでは得られない諸課題や各企業の考え方などを把握する目的で現地ヒアリングを実施しました。（実施時期：2023 年 1 月）

○アンケート調査

調査期間　　令和４年１０月１１日～１０月２５日
調査方式　　FAX 同報による無記名方式
調査対象　　当所会員企業
回答者数　　２０９件

○ヒアリング調査

調査期間　　令和５年１月１６日～１月２６日
調査方式　　個別訪問による
調査対象　　当所会員企業１０社
調査業種　　塗装工事業、医薬品製造業、建築工事業、医療福祉業、工業製品製造業、パン製造販売業、衣服小売業、印刷業、衣料卸販売業

○回答企業概要

横須賀市の中小企業に対して調査を実施しました。業種及び回答者の役職比率は下記図の通りとなります。

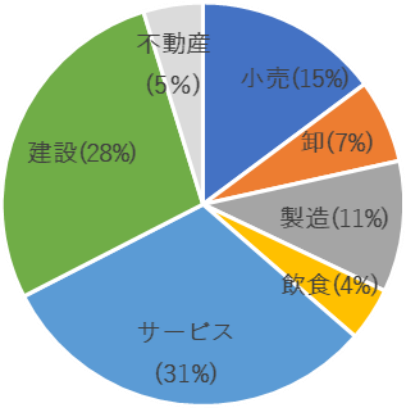

図 1：回答企業の業種について

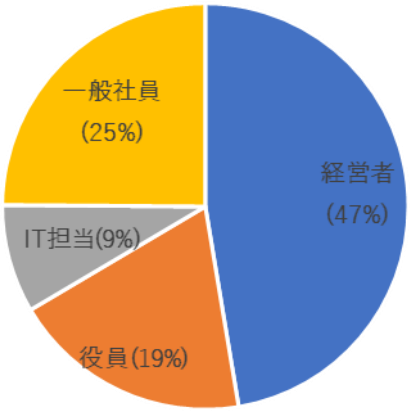

図 2：回答者の役職について

1) 横須賀市中小企業におけるセキュリティ被害実態

1)-①アンケート結果の 17%がセキュリティ被害経験あり

【サイバーセキュリティ被害を受けたことがありますか】への質問において、「被害経験あり」と回答した企業は、全体の 17%(36 社)となり被害経験として比較的高い数値の回答結果になりました。※図 3 参照

攻撃に遭ったことのある割合としてはかなり多い結果となり、且つサイバー攻撃を受けていることを気づかないケースが多いため、調査結果以上に攻撃に遭っていることが推測されます。また、被害に遭った企業の業種割合ではサービス業が 31%と最も高くなりました。但し、すべての業種において被害経験ありとの回答があったため、業種を問わずセキュリティ被害に遭う可能性があることが言えます。

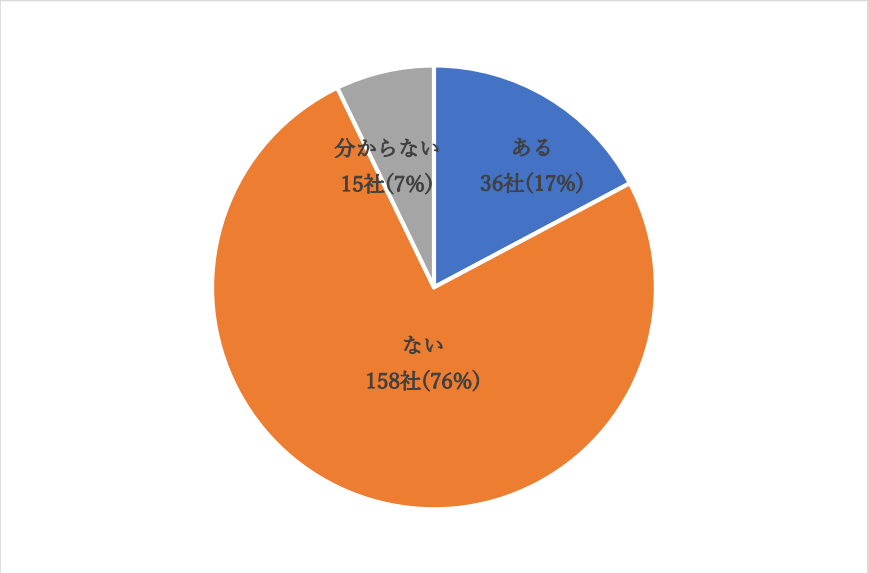

図 3：サイバー攻撃の被害経験について(全体)
質問「サイバー攻撃の被害を受けたことがありますか」

2）セキュリティに対する意識調査

2)-①　サプライチェーン攻撃への危機管理から、製造業の対策意識が高い

【セキュリティ被害に遭った際のサイバーセキュリティ対策への取組み】への質問において、「とてもできている・ある程度できている」と回答した企業は、全体の 44%となり、半数弱の企業はセキュリティ対策を考え、取り組んでいるという回答結果になりました。　※図 4 参照

また、この質問を業種別でみると、「とてもできている・ある程度できている」の割合が高い業種は、「製造業（55%）」、「サービス業（54%）」、「小売業（48%）」となりました。一方で、「不動産業（20%）」,「卸売業（29%）」は低い割合となりました。製造業においては、昨今の大手企業が不正アクセスといったサイバー攻撃の被害を受けたことを発表したこともあり、経営的課題としてのセキュリティ意識が向上したことが推測されます。一方で、不動産業、EC 等を行う卸売業は、個人情報を多く保有する業態ではありますが、対策検討を行っている企業は少なく、セキュリティ意識の低さが懸念されます。　※図 5 参照

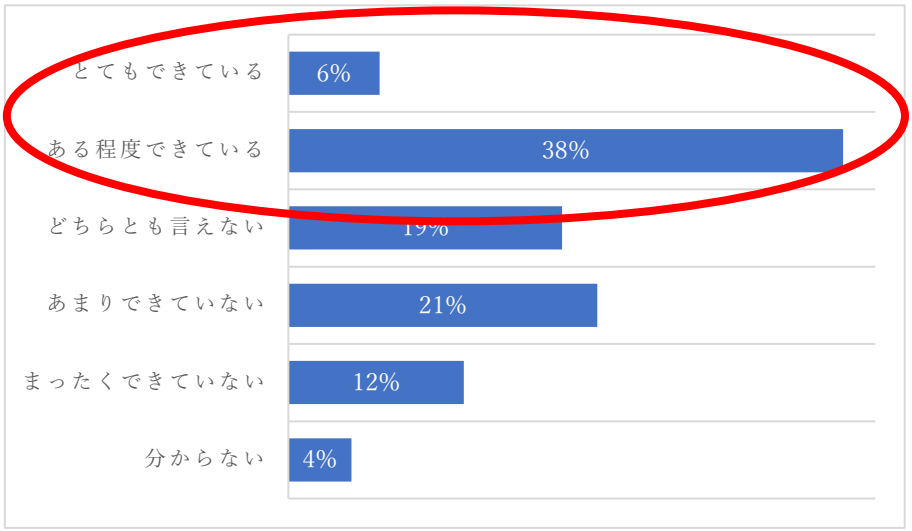

図 4：サイバー被害に遭った際のサイバーセキュリティ対策への取組み（全体）
質問「セキュリティ被害にあった際のサイバーセキュリティ対策がどの程度できていると思いますか」

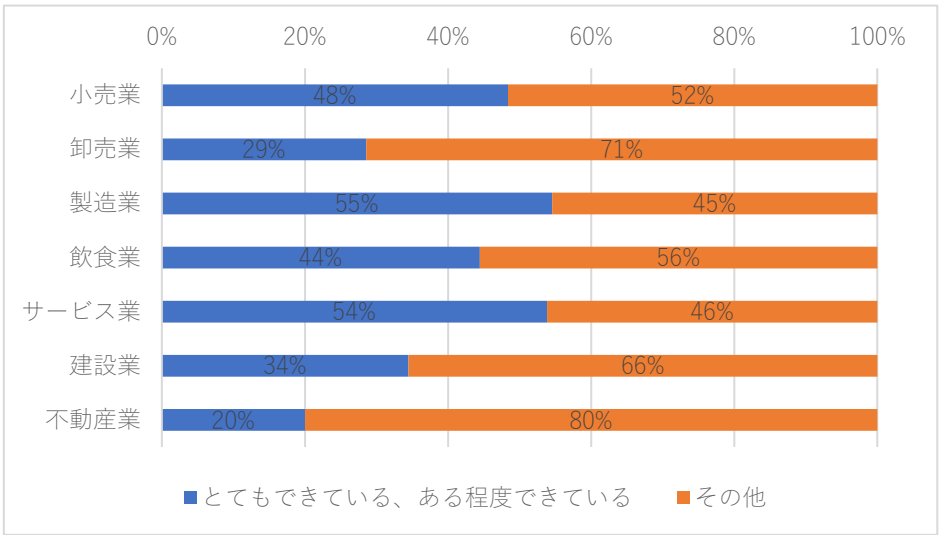

図 5：サイバー被害に遭った際のサイバーセキュリティ対策への取組み（業種別）

2)-②　経営層における意識改革が課題

【社内システムへのサイバー攻撃・被害への懸念】の質問においては、「とても感じている・ある程度感じている」と回答した企業は全体の 63%となりました。　※図 6 参照

経営者・役員のみで回答者を絞った結果では、「とても感じている・ある程度感じている」の割合は 61%となりましたが、残りの 39%の経営層はサイバー攻撃に対しての危機意識を持っていないことが調査結果から窺えます。IT に対する投資やセキュリティに対する投資等をどの程度行うかなど、経営者による判断が必要となるため、中小企業におけるセキュリティ強化を推進するには、経営層における意識改革が課題だと考えられます。

現地ヒアリングでは、懸念を感じていない理由についてヒアリングを行いました。懸念がない理由としては、「ウィルス対策ソフト、UTM [*1] を導入しているため安全」「PC 以外の IT ツールを利用していない」等があがりました。この「ウィルス対策ソフト、UTM 等を導入しているため安全」と回答した企業について更に詳細な稼働状況を聞いてみたところ、セキュリティ機器を導入しているが、運用（パターンファイル [*2] の更新・監視）、製品機能理解まではできていない、それ以外の対策（社内規程の整備等）は取り組んでいないことがわかりました。

「PC 以外の IT ツールを利用していない」については、PC 経由でウィルス感染した際のサイバーセキュリティリスクの詳しい情報が不足している状況がわかりました。

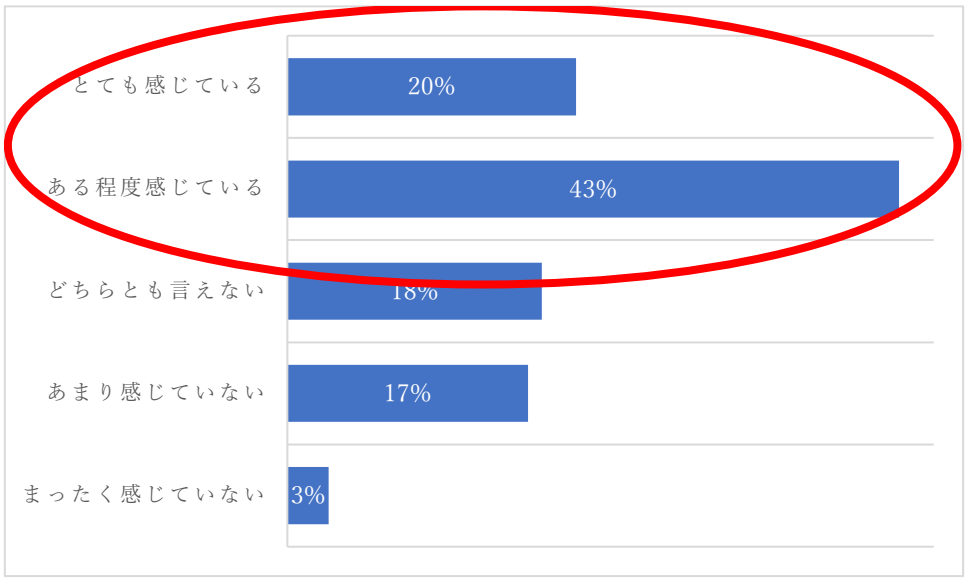

図 6：サイバー攻撃・被害への懸念（全体）

質問「社内システムへのサイバー攻撃やその被害について、どの程度懸念を感じていますか」

【用語解説】

※1　UTM：Unified Threat Management の略で日本語にすると「統合脅威管理」となります。
不正な通信の遮断や悪意のあるメールの受信拒否、ウイルス対策機能等が 1 つに統合されたセキュリティ対策製品を指す。

※2 パターンファイル：既知のウイルスの特徴を記録したファイルを指す。従来からある、一般的なウィルス対策ソフトに実装される方式。

2)-③　どう対策すればいいのか分からない

【必要と感じるサイバーセキュリティ対策】の質問においては、「1 位：サイバー攻撃への適切な防御策の導入」、「2 位：経営者による危機意識」、「3 位：従業員教育」となりました。他の選択肢である、「セキュリティ規程の策定」や「リスクの洗い出し、評価」・「管理体制の構築」と云ったような事前の根本的な施策については一定の選択数はあったものの、上位項目とはなりませんでした。　※図 7 参照

一方で、現地ヒアリングでは、どのようなセキュリティ対策を講じるべきかわからない（相談相手がいない）ことと、社内規程への取組みを必要と感じている企業が多数おりました。中小企業としてどのような対策を行うべきか把握し、社内規程に取り込み、規程に沿った運用と従業員への教育が必要と考えているが、最初の「どのような対策を行うべきかが不明なこと」がサイバーセキュリティ対策の阻害要因であるとことが考えられます。

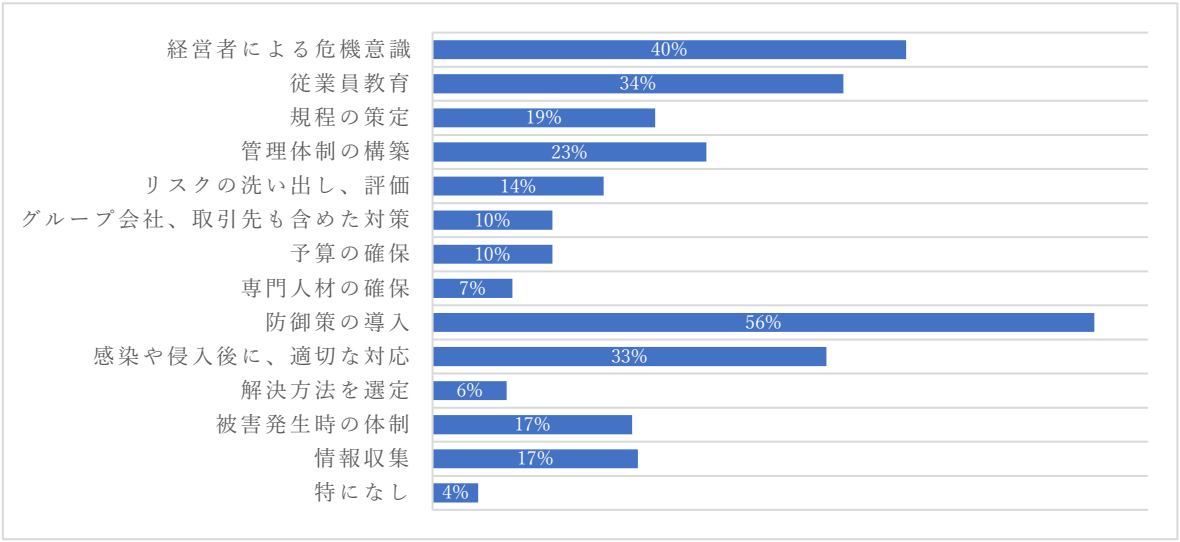

図 7：必要と感じるサイバーセキュリティ対策
質問「サイバーセキュリティ対策について、必要と考えること」（複数回答可）

2)-④　対策を外部に依存する傾向が強い

また、【セキュリティに関する相談相手の有無】の質問においては、「いる」と回答した企業は全体の 73%と比較的高い結果となりました。中でも、その相談相手が「社内」なのか「社外」なのかを合わせて聞いたところ、企業規模を問わず「社外」と回答した企業が全体の 57%を占めていました。　※図 8 参照

「いる」の詳細について現地ヒアリングした結果、相談相手の多くは、製品導入・ネットワーク敷設等を行った「取引先のベンダー」でした。そのため、セキュリティを相談した結果、製品の提案等に流れるため、コスト増およびセキュリティ対策の全体像が把握できていないとの懸念もあがりました。

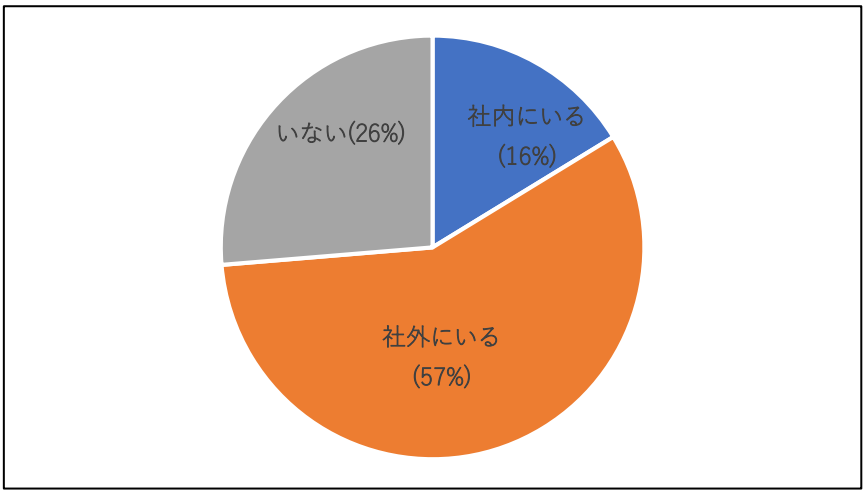

図 8：セキュリティに関する相談相手の有無
質問「セキュリティに関する相談相手はいますか」

2)-⑤　社内教育など予算をかけず自社で取り組むことからスタート

【自社の課題と考えているセキュリティ対策】の質問においては、「1 位：セキュリティ担当者が少ない／いない」、「2 位：適切な対策方法が分からない」、「3 位：投資余力が少ない」となりました。調査結果から、人材・予算の確保と有用な方法論の入手が喫緊の課題であることが窺えます。　※図 9 参照

現地ヒアリングでは、セキュリティに明るい人材を自社で抱えている企業はなく、基本的には外部ベンダーへの相談が中心となっていることがわかりました。また、セキュリティ対策には製品導入コストがかかることを前提と考えており、中小企業としてどの程度のコストを費やし、どのような対策を行うべきかの情報が収集できていないことが窺えました。

そのため、セキュリティ予算の検討を進めると同時に、セキュリティ対策の情報を収集、製品導入以外の対策（運用・教育面で回避できる内容等）を理解し、取組める内容からセキュリティ対策を推進していくことが課題であると考えられます。

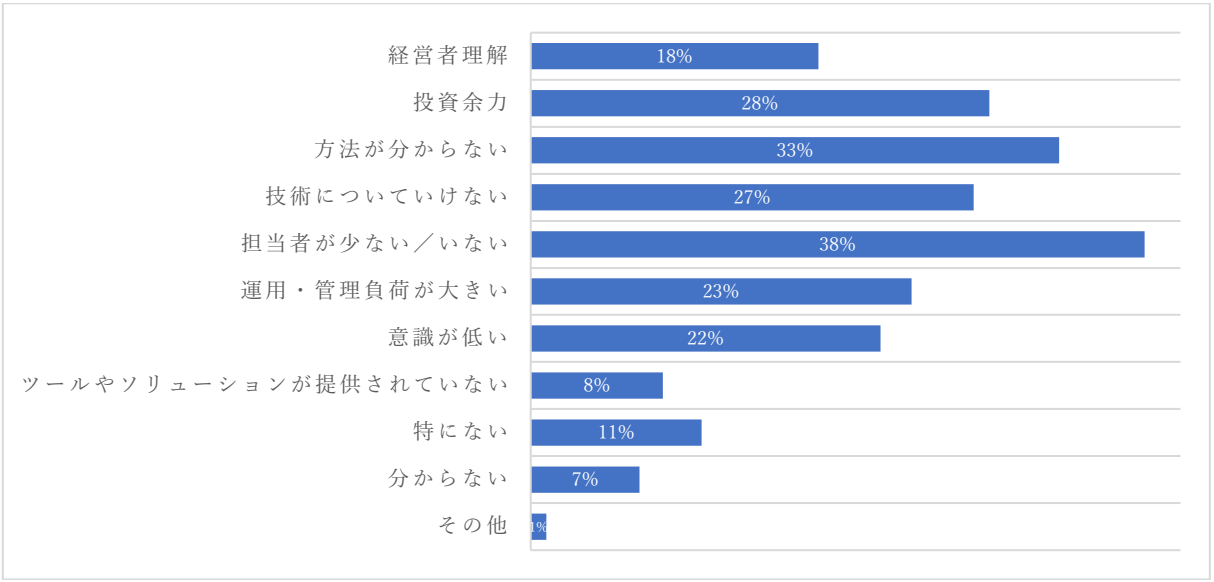

図 9：自社の課題と考えているセキュリティ対策

質問「セキュリティ対策における自社の課題と考えるものを選んでください」（複数回答可）

3）対策状況（技術・組織・人）

3)-①　セキュリティ対策標語などで常に目に留まる工夫

【セキュリティに関する社内規程の有無】についての質問においては、「ない」と回答した企業は全体の 63%となりました。※図 10 参照

従業員 50 人以下の企業で「ない」と回答した割合は 68%を占めており、企業規模が小さいほど、社内規程が整備できていないという傾向が窺えました。また、セキュリティに関する社内規程がないと回答した企業のうち、【サイバー被害に遭った際のサイバーセキュリティ対策への取組み】の質問で、「あまりできていない・まったくできていない」と回答した企業が 46%を占めており、社内規程がない企業は同時にサイバーセキュリティ対策への取組みも行えていない現状が伺えます。

社内規程については、過去に作成したものはあるが更新されず形骸化していると回答した企業もいました。そのため、規程はあるものの運用されず、実態と乖離した状態であることが懸念されます。規程整備に加えて日常的に目に触れる場所に、セキュリティ対策標語などを掲出することも効果があると思われます。

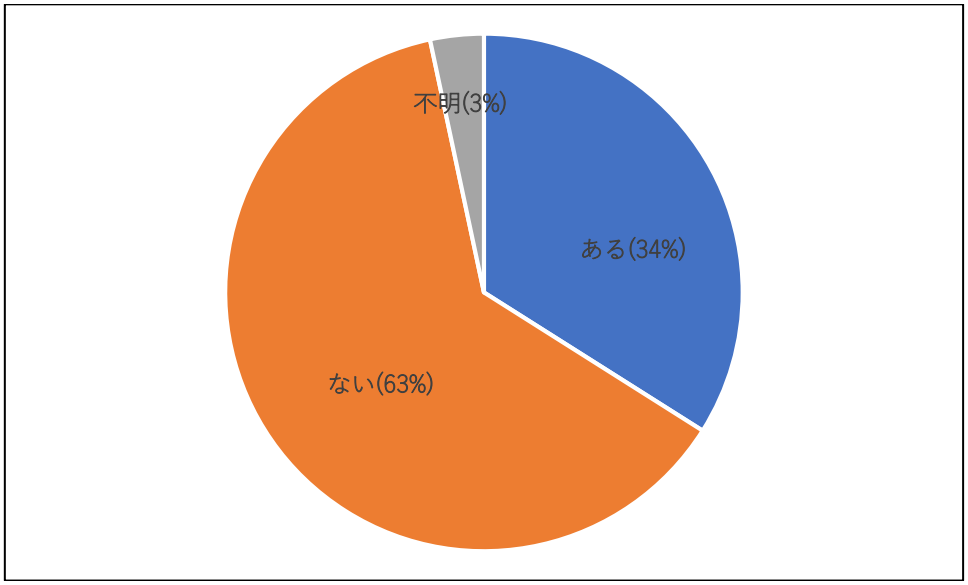

図 10：セキュリティに関する社内規程の有無
質問「セキュリティに関する社内規程はありますか」

3)-②　ウイルス対策ソフトは企業規模問わず普及

【自社で実施しているセキュリティ対策】の質問においては、「1 位：ウィルス対策ソフト」、「2 位：データバックアップ」、「3 位：ファイアウォール、ふるまい検知サービス [*3] など」となりました。

ウィルス対策ソフトの導入については企業規模を問わず広く普及しているツールとなるため大半の企業が導入済みの回答結果となったことが窺えます。　※図 11 参照

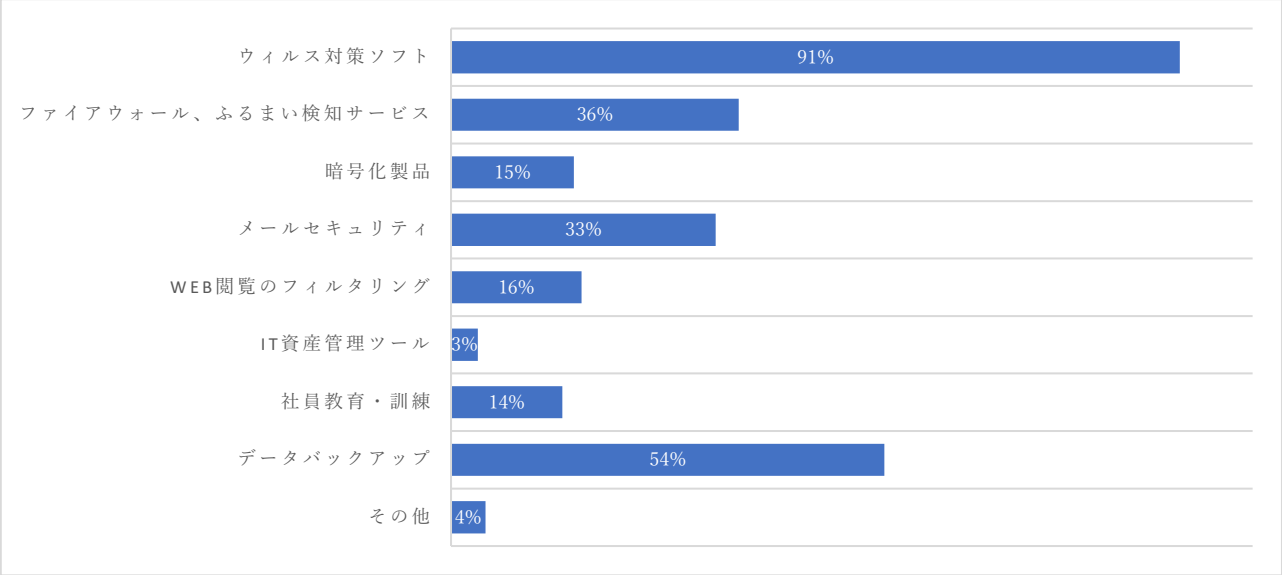

図 11：自社で実施しているセキュリティ対策

質問「自社で実施しているセキュリティ対策を教えてください」(複数回答可)

【用語解説】

※3 ふるまい検知：コンピューター内での不正な動作を検出する機能を指す。

4）調査結果の総括

経営層と社員が一体となった情報セキュリティへの意識づけが必要

セキュリティ被害に遭う企業件数は増加する一方で、中小企業においてはセキュリティ体制が整っていない傾向にあり、且つ、セキュリティ人材が十分に確保できない実態が顕著となっています。このような実態の中、サイバー攻撃の被害に遭うリスクを少しでも低減するためにも、以下のような観点で経営層を中心としたセキュリティ強化を推進していく必要が喫緊の課題であるといえます。

■セキュリティに関する社内規程策定の重要性の再認識

まずはセキュリティポリシーの策定及び社内教育の推進を実施したうえで、段階的に技術的対策を講じながら強化していくことが求められます。

■自社のセキュリティ対策は経営者と社員が一丸となって進めていく

特にセキュリティ予算の確保や人材の育成については、経営者の理解が欠かせません。且つ、日ごろの運用においては全社員の協力体制を構築していくことが求められます。

■自社のセキュリティリスクを考慮したセキュリティ対策

技術的対策としての IT ツールの導入については、自社のセキュリティリスクを十分考慮した上で効果があがる製品を選定し、優先的に導入することが重要となります。

4. 今後の中小企業へのセキュリティ対策について

会員中小企業へのアンケートとヒアリングの結果、社内規程策定、従業員教育、情報資産運用・管理、技術・物理対策等の課題が多く見受けられました。これらの課題を解決するため、各企業のセキュリティ強化を目的とし、令和 5 年度に関係機関と連携した「YOKOSUKA 情報セキュリティ・プロジェクト(仮称)」を立ち上げ、地域全体のサイバーセキュリティ対策を推進していく予定です。

＜横須賀商工会所　団体概要＞
設立：1928 年 11 月
会頭：平松　廣司
所在地：神奈川県横須賀市平成町 2-14-4
事業内容：政策提言活動、中小企業振興、地域振興、産業振興、共済事業、情報化推進
URL：https://yokosukacci.com/

＜株式会社ワールドスカイ　会社概要＞
設立：2004 年 6 月
代表取締役社長：柳沢　智幸
所在地：東京都中央区新川 1-3-3　グリーンオーク茅場町 7 階
事業内容：セキュリティソリューション、製品ソリューション、保守サービス
URL: https://www.worldskyjp.com/

＜日本マイクロソフト株式会社　会社概要＞
設立：1986 年 2 月
代表取締役社長：津坂　美樹
所在地：東京都港区港南 2-16-3　品川グランドセントラルタワー
事業内容：ソフトウェアおよびクラウドサービス、デバイスの営業・マーケティング
URL:https:www.microsoft.com