2024 年 5 月 16 日

レポート

中小企業における情報セキュリティ対策の最新動向

～脅威の認識が難しい中でも、対策を普及させるため必要な施策とは～

産業創発部　副主任研究員　山本洋平
研究開発第 2 部（大阪）　研究員　小島雄祐

1. はじめに

近年、中小企業においても IT 化が進み、業務の効率化、サービスレベルの向上等が図られている一方で、機密情報を狙ったサイバー攻撃は日々発生し、その被害も確認されている。

独立行政法人情報処理推進機構（以下、「IPA」）では、中小企業における情報セキュリティに関する実態把握を目的として、「2021 年度中小企業における情報セキュリティ対策に関する実態調査[1]」（以下、「2021 年度調査」）等の調査を実施している。しかし、2021 年度調査後も中小企業における情報セキュリティ対策の重要性は高まり続けているものの、中小企業の意識は高まっておらず、対策が進んでいない懸念がある。

本レポートは、2021 年度調査の調査項目を参考として当社が 2023 年度に実施した調査（以下、「当社調査」）の結果を報告するものである。調査結果を踏まえ、中小企業における情報セキュリティ対策の最新動向について整理するとともに、より多くの中小企業に情報セキュリティ対策に取り組んでもらうために必要な取組・支援について、取引先からの要請の状況に触れながら考察を行った。

[1]「2021 年度 中小企業における情報セキュリティ対策に関する実態調査」は IPA から委託を受け、三菱 UFJ リサーチ&コンサルティングが実施した。

2. 調査概要

(1) 調査方法・対象

中小企業の情報セキュリティ対策への取組や被害の状況、対策実施における課題、経営層の関与や認識に関する実態を把握するため、2023 年 8 月、アンケート調査を実施した。

調査は、クロス・マーケティング社が保有する企業パネル[2]のうち、中小企業基本法に基づいた中小企業の経営者・役員を対象として実施した。サンプル数は 2,000 件である。

2021 年度調査は、全国の中小企業を対象に、企業信用調査会社の企業データベースから 40,000 件を抽出・アンケート送付し、経営者・役員、IT・情報セキュリティ担当者、および一般社員から回答を得ており、今回の当社調査とは調査方法が異なることに留意されたい。

図表 1 中小企業の定義

業種分類	中小企業基本法の定義
製造業その他	資本金の額又は出資の総額が 3 億円以下の会社又は 常時使用する従業員の数が 300 人以下の会社及び個人
卸売業	資本金の額又は出資の総額が 1 億円以下の会社又は 常時使用する従業員の数が 100 人以下の会社及び個人
小売業	資本金の額又は出資の総額が 5 千万円以下の会社又は 常時使用する従業員の数が 50 人以下の会社及び個人
サービス業	資本金の額又は出資の総額が 5 千万円以下の会社又は 常時使用する従業員の数が 100 人以下の会社及び個人

数値については、小数点第2位を四捨五入した値をグラフ上に掲載しているため、合計値が 100.0%とならない場合があることに留意されたい。なお、図表の説明に記載されている「SA」は単一回答の設問、「MA」は複数回答の設問、「NA」は数値回答の設問を示す。

[2] 株式会社クロス・マーケティング 「企業パネル」
https://www.cross-m.co.jp/monitor/specialmonitor/business/

(2) 回答企業属性

回答企業の属性は以下のとおりである。経営者・役員（経営層）からの回答を収集しており、2021 年度調査において回答に含まれていた IT・情報セキュリティ担当者及び一般社員からの回答は含まれていない。

[1] 役職

図表 2 役職

合計	経営者	役員	その他
2,000	1,183	817	0
100.0%	59.1%	40.8%	0.0%

[2] 業種

図表 3 業種

合計	製造業その他	卸売業	小売業	サービス業
2,000	838	266	197	699
100.0%	41.9%	13.3%	9.9%	35.0%

[3] 従業員規模

図表 4 従業員規模

合計	5名以下	6～20名以下	21～50名以下	51～100名以下	101～300名以下	301名以上
2,000	877	496	234	163	129	101
100.0%	43.8%	24.8%	11.7%	8.2%	6.4%	5.1%

[4] 地域ブロック[3]

図表 5 地域ブロック

合計	北海道	東北	関東	中部	近畿	中国	四国	九州・沖縄
2,000	103	117	994	160	339	103	56	128
100.0%	5.2%	5.8%	49.7%	8.0%	17.0%	5.1%	2.8%	6.4%

[5] 資本金

図表 6 資本金

合計	1,000万円以下	1,000万円超～3,000万円以下	3,000万円超～5,000万円以下	5,000万円超～1億円以下	1億円超～2億円以下	2億円超～3億円以下	3億円超
2,000	881	502	217	206	93	39	62
100.0%	44.0%	25.1%	10.8%	10.3%	4.7%	2.0%	3.1%

[3] 地域ブロックごとの都道府県の内訳は、経済産業局の管轄区域に基づいて設定した。
https://www.meti.go.jp/policy/economy/consumer/credit/renrakusaki.pdf

[6] 総売上高（直近会計年度）

図表 7 総売上高

合計	1,000 万円以下	1,000 万円超～3,000 万円以下	3,000 万円超～5,000 万円以下	5,000 万円超～１億円以下	１億円超～２億円以下	２億円超～３億円以下	３億円超
2,000	286	316	175	288	241	115	579
100.0%	14.3%	15.8%	8.8%	14.4%	12.1%	5.8%	29.0%

[7] 業務を受注する際に多い立場

図表 8 業務を受注する際に多い立場

合計	元請・一次請けとして受注	二次請けとして受注	三次請け・それ以降として受注	委託元として発注	把握していない・不明
2,000	1,179	290	67	224	240
100.0%	59.0%	14.5%	3.4%	11.2%	12.0%

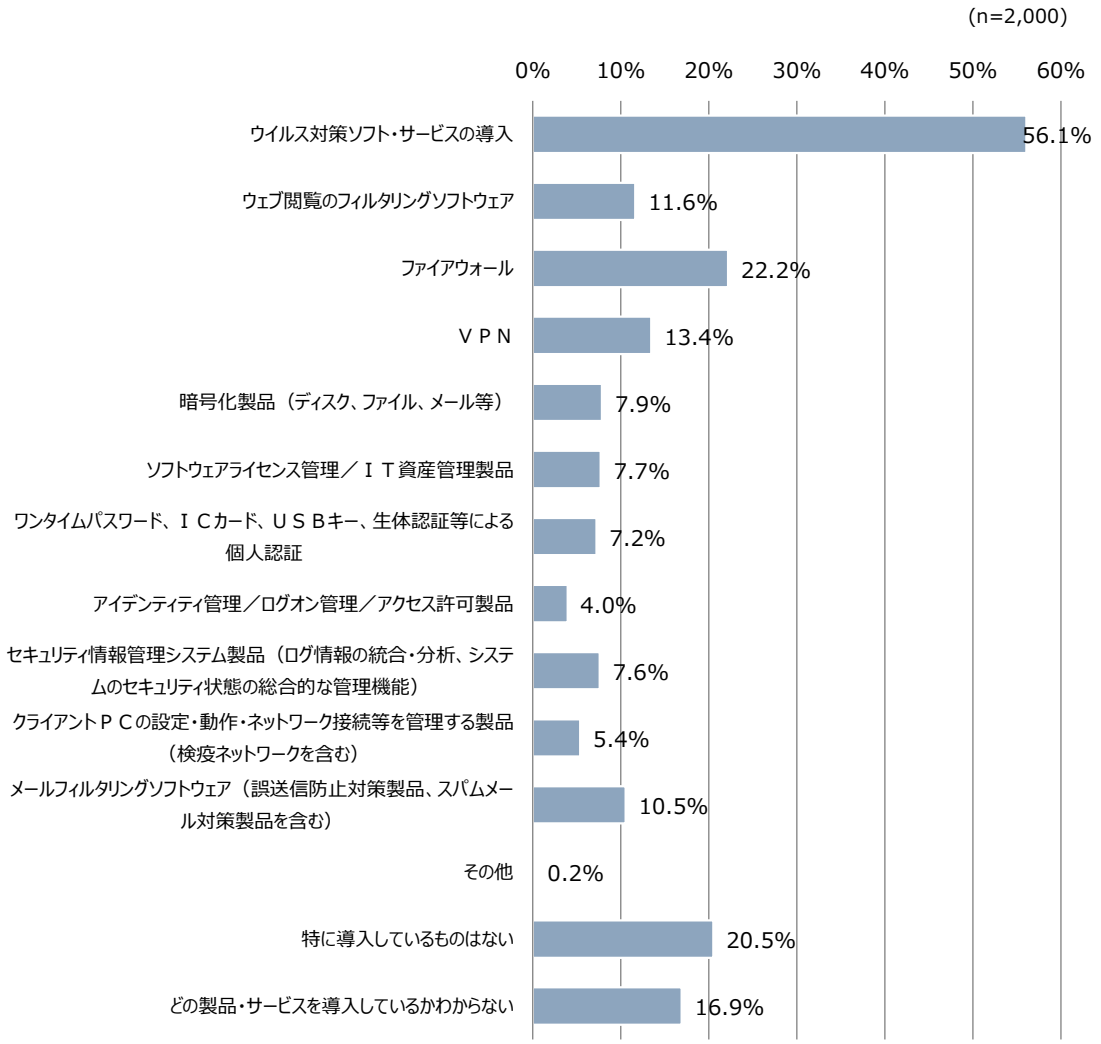
3. 中小企業における情報セキュリティ対策の最新動向（脅威の認識は十分か）

2021 年度調査報告書においても、情報セキュリティ上の脅威の認識が十分でない可能性が指摘されており、2021 年度調査から数年経過したものの、脅威の認識が浸透したとはいえないおそれもある。そこで今回、当社調査では、中小企業における情報セキュリティ上の脅威の認識について、中小企業の経営者・役員を対象とした調査を行った[4]。

(1) 情報セキュリティ製品・サービスの導入状況

情報セキュリティ製品・サービスの導入状況について、「ウイルス対策ソフト・サービスの導入」が最も多く、56.1%となっている。次いで、「ファイアウォール（22.2%）」となっている。一方で、「特に導入しているものはない」が 20.5%、「どの製品・サービスを導入しているかわからない」が 16.9%となっており、導入していないもしくは導入状況を経営者・役員が把握できていない企業が 37.4%を占めている。

図表 9 情報セキュリティ製品・サービスの導入状況（MA）

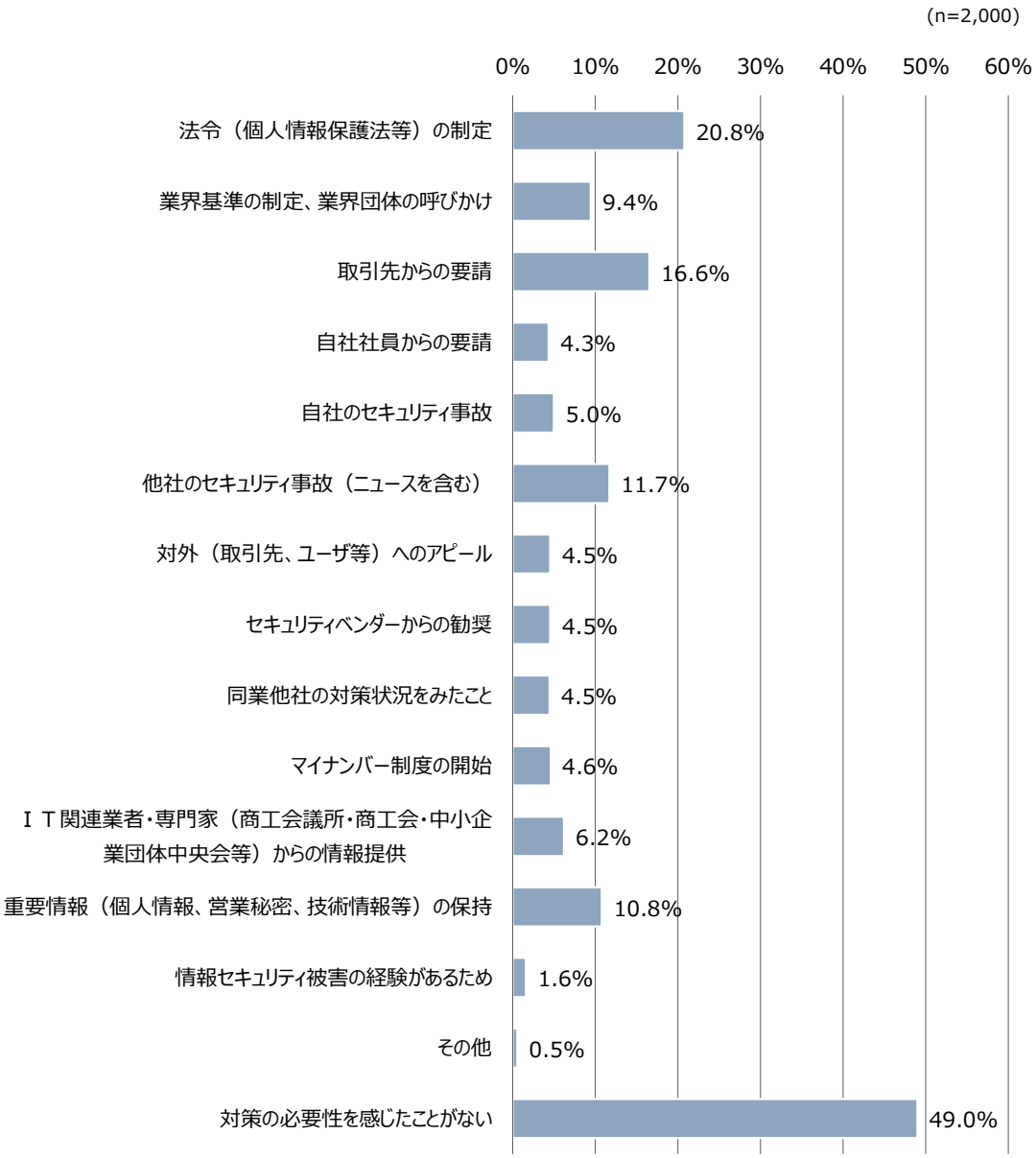


[4] 当調査では、経営者・役員を対象としているが、「2021 年度 中小企業における情報セキュリティ対策に関する実態調査」におけるアンケート調査では、IT・情報セキュリティ担当者及び一般社員も回答者に含まれる。

(2) 情報セキュリティ対策の必要性の認識

情報セキュリティ対策の必要性を感じたきっかけについて、「対策の必要性を感じたことがない」との回答が最も多く、49.0%となっている。2021 年度調査においては、「対策の必要性を感じたことがない」との回答は 20.9%となっており、情報セキュリティ対策の必要性の認識については大きく悪化している結果となった[5]。調査方法の違いによる影響も考えられるが、情報セキュリティ対策の必要性について 2021 年度調査と比較して、認識が高まったとは考えづらい。

図表 10 情報セキュリティ対策の必要性を感じたきっかけ（MA）

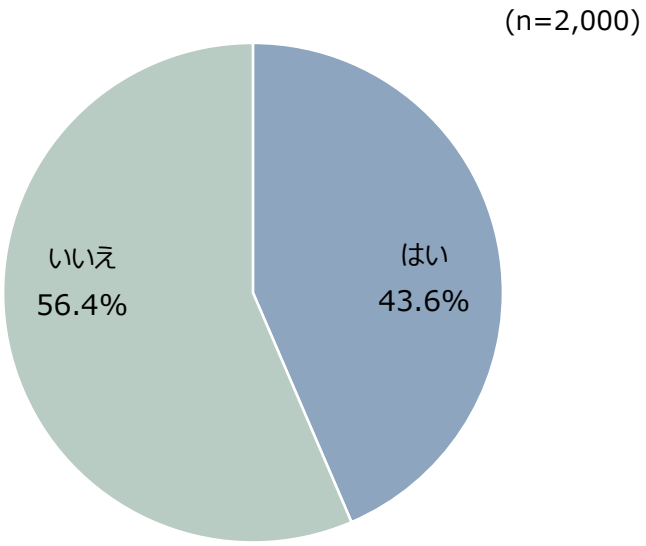


[5] 独立行政法人情報処理推進機構 「2021 年度中小企業における情報セキュリティ対策に関する実態調査― 調査報告書 ―」(p.38)
https://www.ipa.go.jp/security/reports/sme/ug65p90000019djm-att/000097060.pdf

(3) 情報セキュリティ被害に遭う可能性の認識

情報セキュリティ被害に遭う可能性の認識を聴取した設問について、「いいえ」との回答が 56.4%となっており、半数以上の中小企業が被害に遭う可能性を認識していない結果となっている。

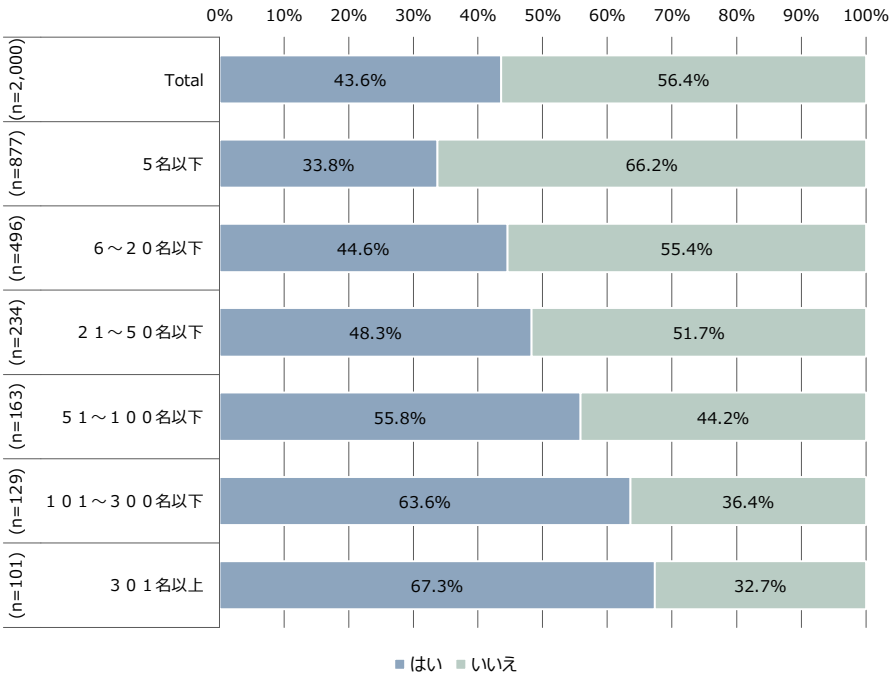
図表 11 情報セキュリティ被害に遭う可能性を感じるか（SA）



[1] 情報セキュリティ被害に遭う可能性の認識（従業員規模別）

情報セキュリティ被害に遭う可能性の認識を聴取した設問について従業員規模別にみると、従業員規模が小さいほど被害に遭う可能性の認識が低い傾向にある。

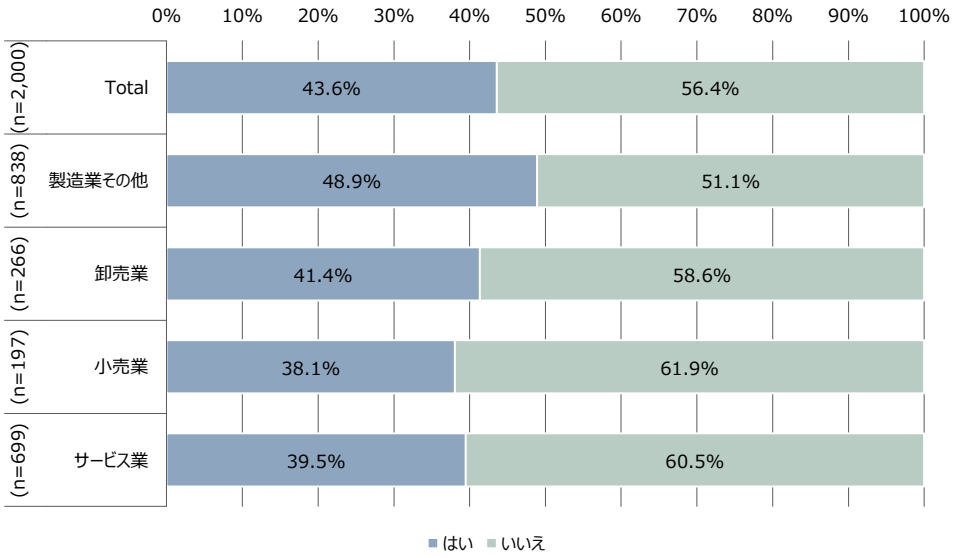
図表 12 情報セキュリティ被害に遭う可能性を感じるか（従業員規模別）（SA）



[2] 情報セキュリティ被害に遭う可能性の認識（業種別）

情報セキュリティ被害に遭う可能性の認識を聴取した設問について業種別にみると、「製造業その他」の企業の方が、被害に遭う可能性の認識が高い傾向にある。

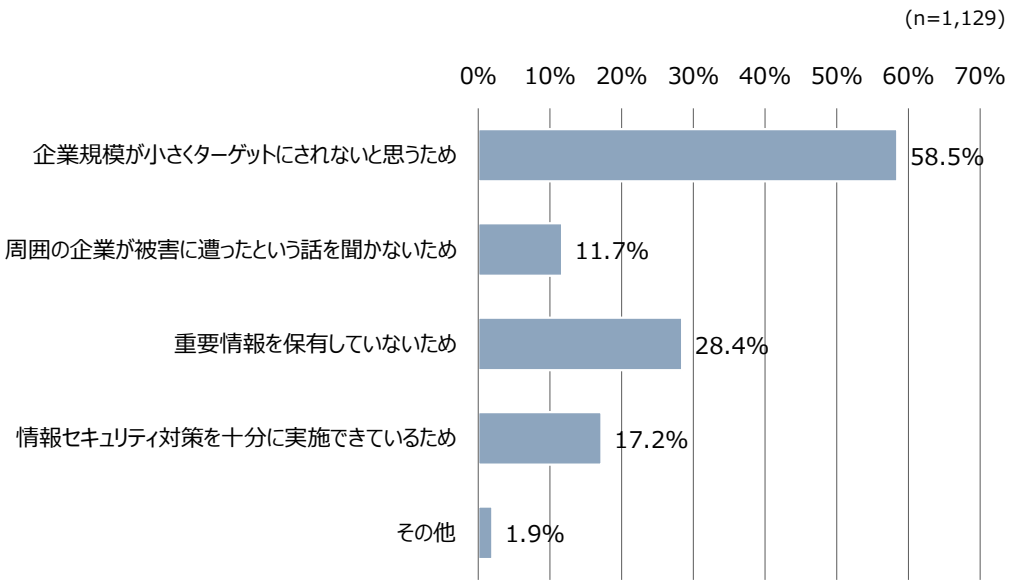
図表 13 情報セキュリティ被害に遭う可能性を感じるか（業種別）（SA）



(4) 情報被害に遭わないと考える理由

情報セキュリティ被害に遭う可能性の認識を聴取した設問に「いいえ」と回答された回答者に対し、情報セキュリティ被害に遭わないと感じる理由について聴取したところ、「企業規模が小さくターゲットにされないと思うため」が最も多く、58.5%となっている。次いで、「重要情報を保有していないため（28.4%）」となっている。

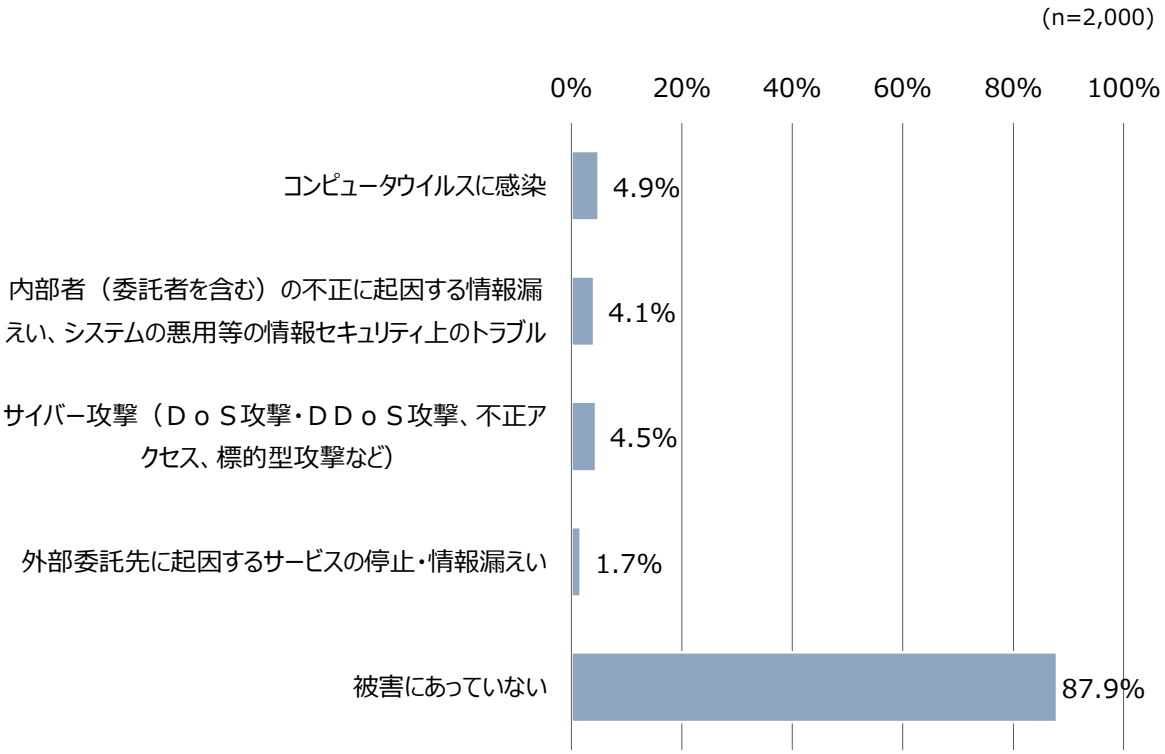
図表 14 情報セキュリティ被害に遭わないと感じる理由（MA）



(5) 情報セキュリティ被害の有無・認知について

2022 年度の 1 年間において、情報セキュリティ被害に 1 度でも遭ったかどうか聴取したところ、「被害にあっていない」との回答が最も多く 87.9%となっている。2021 年度調査においては、「被害にあっていない」との回答が 84.3%となっており、情報セキュリティ被害の有無・認知について大きな変化は確認できなかった。ただし、2021 年度調査においても指摘されているとおり、情報セキュリティ対策の実施状況を踏まえると、回答企業においてサイバー攻撃を認識できておらず、被害の認知が進んでいない可能性も否定できない[6]。

図表 15 情報セキュリティ被害の有無（SA）



(6) 情報セキュリティ上の脅威の認識に関する考察

今回の当社調査や過去の調査の結果を踏まえると、中小企業の情報セキュリティ対策の重要性や情報セキュリティ上の脅威の認識に、ここ数年でポジティブな変化が生じているとは考えづらい状況にある。また、従業員規模が小さい企業ほど、情報セキュリティ対策の重要性や情報セキュリティ上の脅威の認識が低い傾向も継続している。

今後、中小企業に情報セキュリティ対策に取り組んでもらうことを考えると、なぜ中小企業が情報セキュリティ対策に自分事としてとらえる必要があるのか、自分事としてとらえてもらうために必要な取組・支援は何か、といった情報セキュリティ対策の普及に係る課題に対処する必要がある。

[6] 独立行政法人情報処理推進機構 「「2021 年度 中小企業における情報セキュリティ対策に関する実態調査」報告書について」
https://www.ipa.go.jp/security/reports/sme/about.html

4. なぜ中小企業が情報セキュリティ対策に取り組む必要があるのか

(1) なぜ情報セキュリティ対策の必要性を認識することが難しいのか

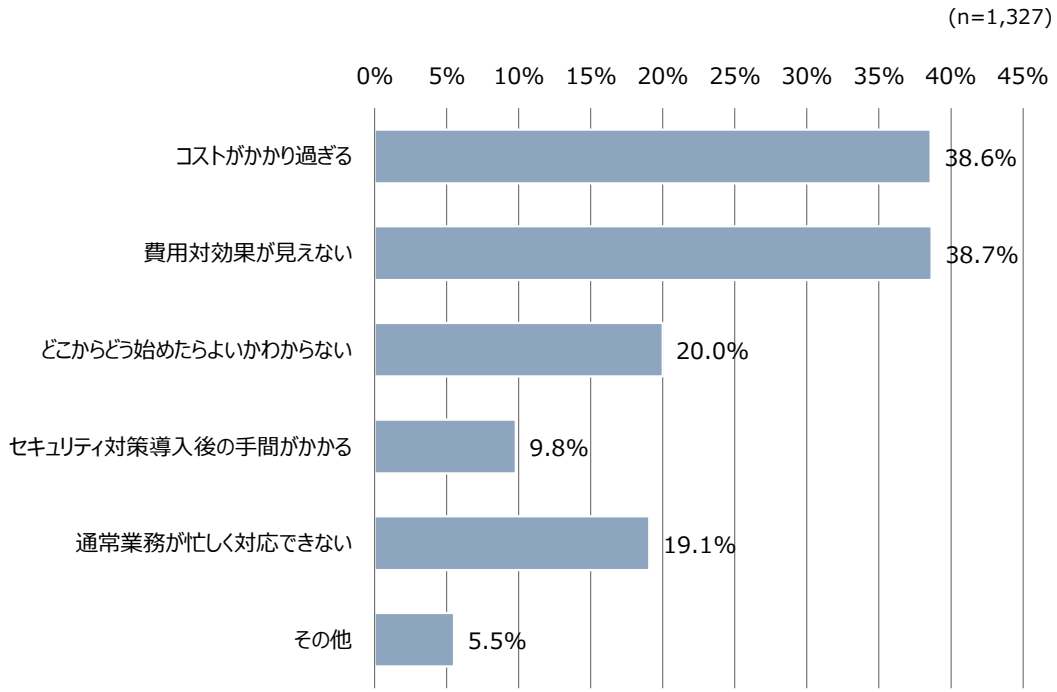
中小企業における情報セキュリティをテーマとした調査において、なぜ取組が進まないのかという点については、過去にも検討されており、以下のような理由が挙げられてきた。

図表 16 中小企業が情報セキュリティ対策に取り組むことが難しい理由として多く挙げられてきた例

- 中小企業にとって、被害に遭うことが想定できないのではないか。
- 中小企業にとって、セキュリティ対策を実施するメリットがわからないのではないか。
- 中小企業にとって、どういった対策から実施したらよいかわからないのではないか。
- 中小企業にとって、情報セキュリティ対策を担う人材が不足/組織的な対応が難しいのではないか。
- 中小企業にとって、情報セキュリティ対策を実施するための費用が用意できないのではないか。

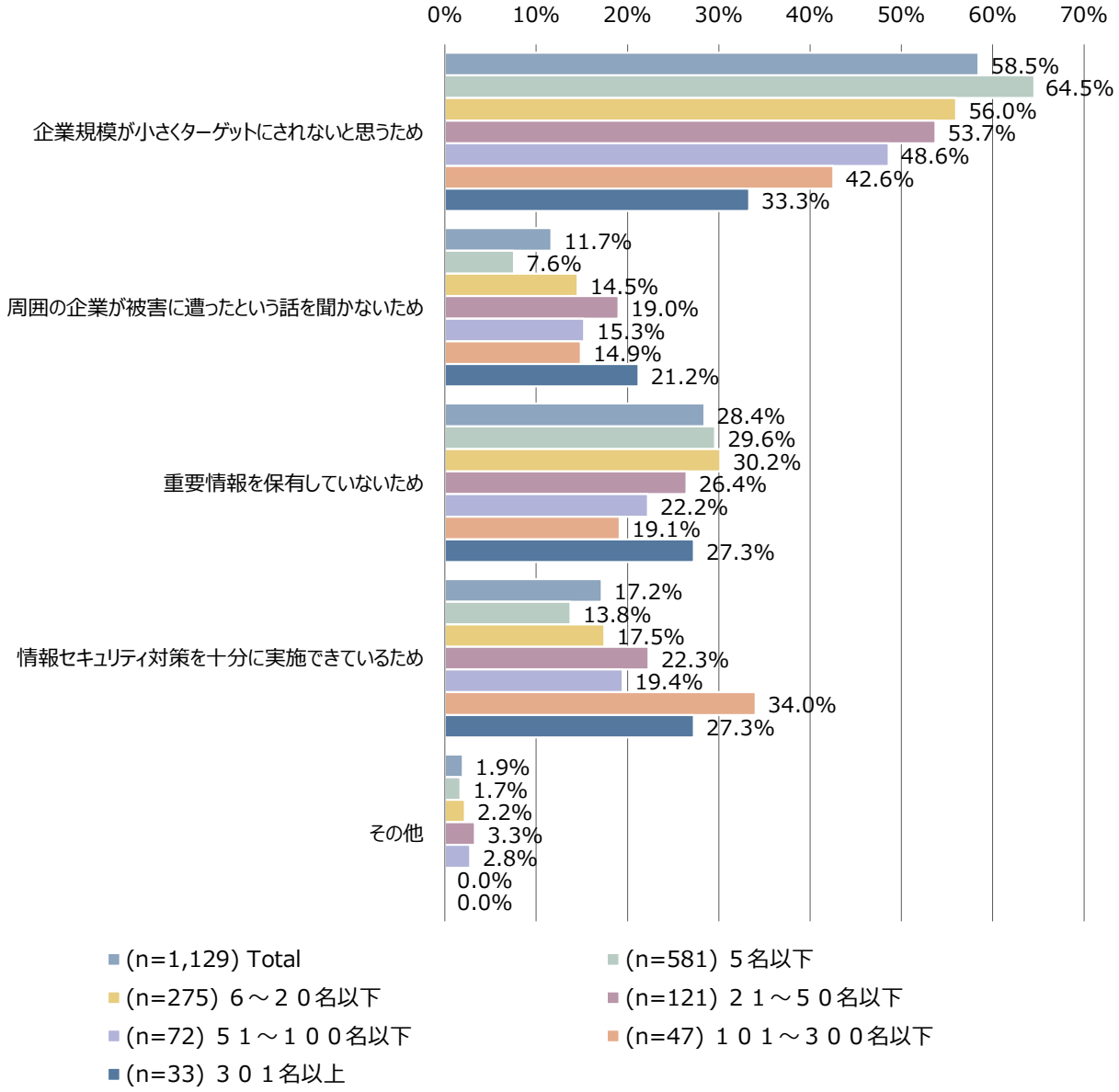
当社調査においても、2022 年度に情報セキュリティ投資を行わなかった理由について聴取したところ、「費用対効果が見えない」が最も多く 38.7%となっており、「コストがかかり過ぎる(38.6%)」、「どこからどう始めればいいかわからない(20.0%)」の順となっている。この結果をみると、費用対効果・コストを理由に挙げる企業が多く、情報セキュリティ対策に取り組まないリスク・取り組むメリットを多くの中小企業が十分に認識できていないことが示唆される。

図表 17 情報セキュリティ投資を行わなかった理由(MA)



確かに、情報セキュリティ被害に遭わないと感じる理由について従業員規模別にみると、企業規模が小さいほどターゲットにされないと感じている傾向が強く、特に規模の小さい企業においては被害に遭うことのイメージを持つことが難しく、費用対効果が見えないと感じることも理解しうる。

図表 18 情報セキュリティ投資を行わなかった理由（従業員規模別）（MA）



また、情報セキュリティ投資の費用対効果は、投資による利益が得られる性質のものではなく、明確に認識することは難しい。情報セキュリティ投資の費用対効果を、対策に係る費用と被害に遭った際の被害額から判断することを考えると、被害に遭う可能性を認識していない企業が費用対効果を認識することは困難であると考えられる。

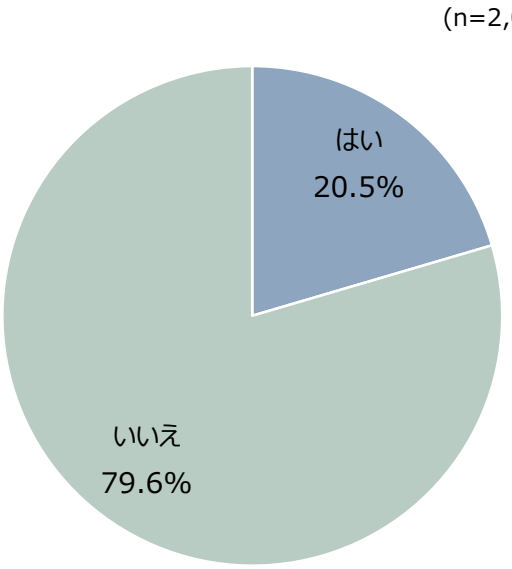
(2) 費用対効果が感じられなくとも自分事として取り組む必要があるのはなぜか

前項において、中小企業にとっては情報セキュリティ対策投資の費用対効果の認識が難しいと考えられることを述べたが、そうであっても中小企業が情報セキュリティ対策投資を行う必要性が高まっている理由として、情報セキュリティ対策の実施が、企業間の取引の前提条件として認識されつつあることが挙げられる。

近年、サプライチェーンの弱点を悪用した攻撃が重大な脅威となっており、サプライチェーン全体でセキュリティレベルの向上を目指す動きが強まる中、中小企業に対しても取組が求められるようになってきている。

当社調査においても、取引先からの情報セキュリティに係る要請の有無について、20.5%が「義務・要請を受けたことがある」と回答している。2021 年度調査においても、取引先からの情報セキュリティ対策上の義務・要請を受けたことがあるとする回答が 26.1%を占めている[7]。そのため、既に、中小企業のうち2～3割程度は、取引先からの情報セキュリティ対策実施が求められる状況となっているといえる[8]。

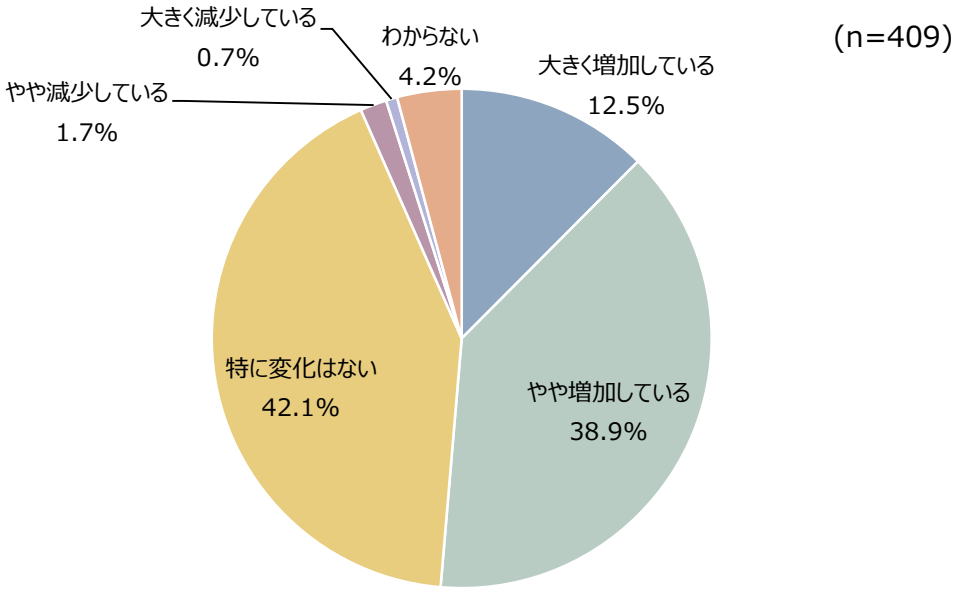
図表 19 販売先（発注元企業）との契約締結時の情報セキュリティに関する条項・取引上の義務・要請の有無（SA）



また、取引先からの要請があると回答した方に発注元企業から情報セキュリティに関する要請・推奨を受ける機会の動向について聴取したところ、「大きく増加している（12.5%）」、「やや増加している（38.9%）」となっている。既に取引時に情報セキュリティ上の要請を受けている企業のうち半数以上については、要請を受ける機会が増加傾向にある。

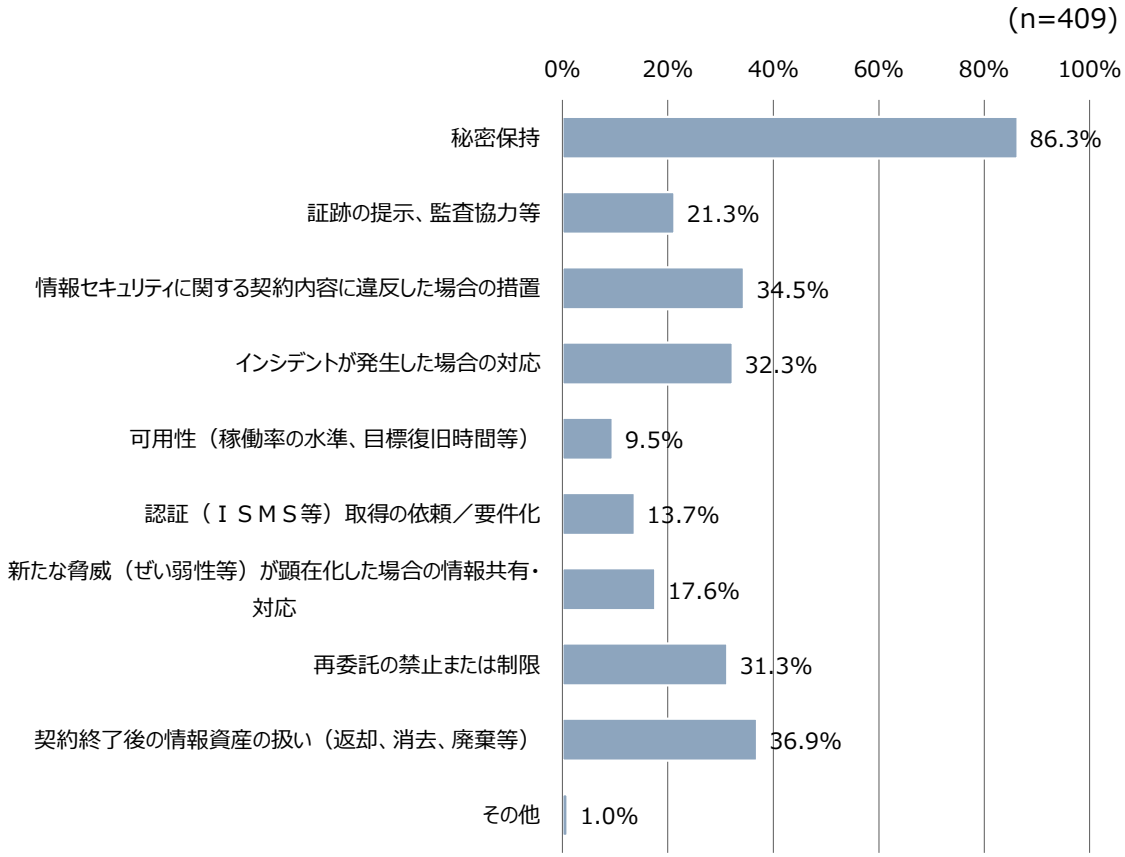
[7] 独立行政法人情報処理推進機構 「「2021 年度 中小企業における情報セキュリティ対策に関する実態調査」報告書について」 https://www.ipa.go.jp/security/reports/sme/about.html
[8] 独立行政法人情報処理推進機構 「「2021 年度 中小企業における情報セキュリティ対策に関する実態調査」報告書について」 https://www.ipa.go.jp/security/reports/sme/about.html

図表 20 販売先（発注元企業）との契約締結時の情報セキュリティに関する条項・取引上の義務・要請の頻度（SA）



契約時に具体的に求められる要請としては、「秘密保持」が最も多く 86.3%となっており、「契約終了後の情報資産の扱い（返却、消去、廃棄等）（36.9%）」、「情報セキュリティに関する契約内容に違反した場合の措置（34.5%）」と続く。

図表 21 販売先（発注元企業）との契約締結時の情報セキュリティに関する条項・取引上の義務・要請の内容（SA）



上記に示すような取組が、取引の際の前提として求められるようになっていることを考慮すると、情報セキュリティ対策には一定のコストがかかるものの、中小企業においても、通常業務を継続するための取組の一環としての情報セキュリティ対策をとらえる必要が出てきているといえるだろう。

こうした状況を踏まえ、より多くの中小企業に情報セキュリティ対策に取り組んでもらうためにどのような取組・支援が必要か考察する。

5. 中小企業にセキュリティ対策を自分事としてとらえてもらうために必要な取組・支援とは

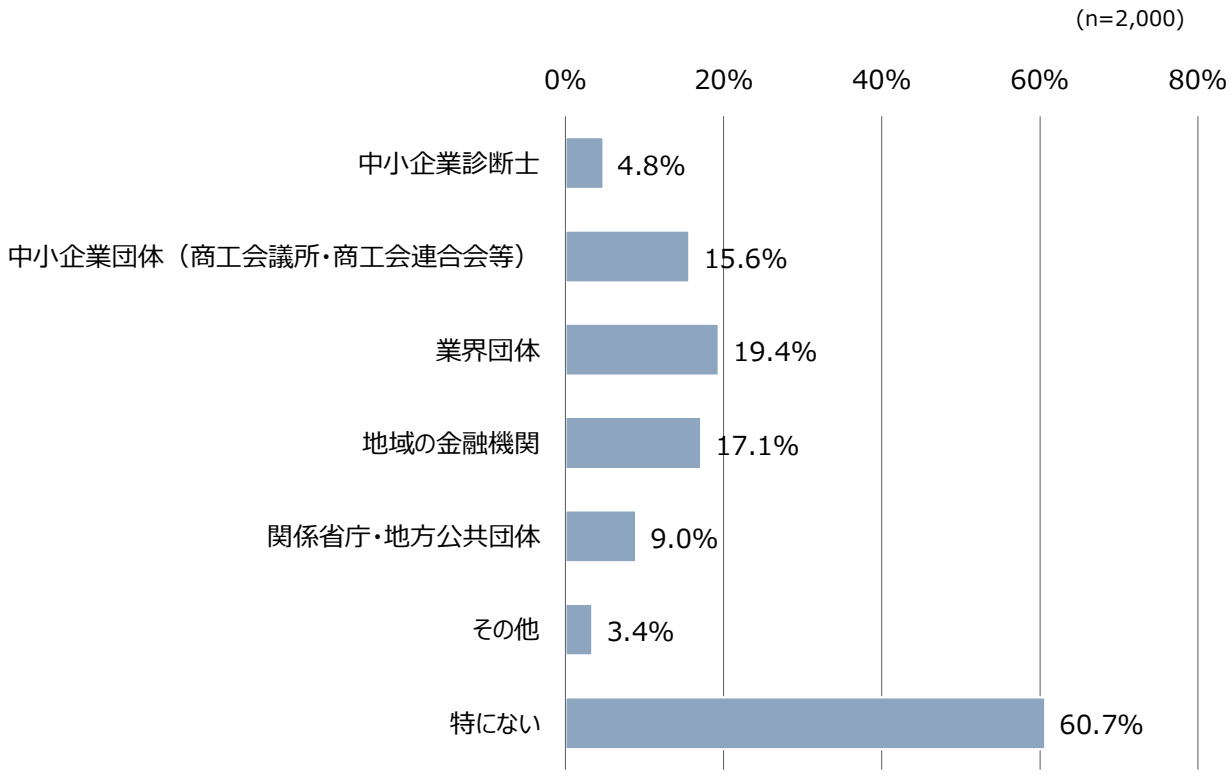
(1) どのようなルートで情報セキュリティ対策の重要性を伝えていくべきか

これまで指摘してきたように、現状では、中小企業において、経営層が情報セキュリティ被害の有無や被害に遭う可能性、被害に遭った際の影響といった情報セキュリティリスクを正しく認識できていないおそれがある。そのため、中小企業に対し、情報セキュリティリスクを正しく見積り、対処することが重要であるという啓発を行うだけでは、中小企業に情報セキュリティ対策を強化してもらうことは難しい。ゆえに、中小企業であっても情報セキュリティ被害に遭う可能性やリスクが大きいということ、取引先との関係、既存の業務、サプライチェーンを維持するために必要な取組になりつつあることを理解してもらう必要がある。取引先が多い企業においては、情報セキュリティ対策実施の要請を受ける可能性も増えるものの、取引先が限定的な企業においては、取引先との関係維持のために将来的に求められる取組であることを認識してもらうことは難しいと考えられる。そうした企業に対しては、取引先以外の接点として、普段経営に関する情報を収集する先となる組織を活用することも求められるだろう。

当社調査で、普段経営に関する情報を収集する先について聴取したところ、「業界団体」が最も多く 19.4%であり、「地域の金融機関(17.1%)」、「中小企業団体(商工会議所・商工会連合会等)(15.6%)」と続いている。このような中小企業との接点も多く有していると考えられる組織を通じた情報発信・経営支援が求められる。

一方で、経営に関する情報を収集する先が「特にない」との回答も 60.7%となっており、情報収集先のない中小企業に対して、どのように情報を届けるかという点に課題があるといえる。

図表 22 経営に関する情報を収集する先(MA)



(2) 行政の施策は認知されているのか

業界団体等の組織を通じた情報収集を行っていない企業に対しては、行政から直接情報を届けることも必要となる。そこで、現状の行政施策の認知度について聴取したところ、IPA が実施する代表的な施策である「SECURITY ACTION」、「サイバーセキュリティお助け隊」、「中小企業の情報セキュリティ対策ガイドライン」、「5分でできる！情報セキュリティ自社診断」についてみると、全ての施策・ツールについて「全く知らない/今回初めて知った」、との回答が 50%を越えている。

図表 23 行政が実施する施策の認知度（SA、n=2,000）

	非常に よく知っている	よく知っている	どちらでもない	あまり知らない	全く知らない／ 今回初めて知った
SECURITY ACTION	2.6%	5.8%	21.3%	16.6%	53.8%
サイバーセキュリティお助け隊	1.8%	6.1%	21.1%	17.7%	53.3%
中小企業の情報セキュリティ対策ガイドライン	2.1%	6.6%	23.4%	16.5%	51.4%
5分でできる！情報セキュリティ自社診断	1.8%	4.9%	21.6%	17.4%	54.3%

特に、「SECURITY ACTION」については、行政が実施する補助金の申請要件等に採用されているケースもある[9]。また、「SECURITY ACTION」は、中小企業が情報セキュリティ対策に取り組むことを自己宣言する制度であるが、中小企業による自己宣言だけでなく、「SECURITY ACTION」の趣旨に賛同し、当制度の普及促進に積極的に取り組む普及賛同企業の一覧も公開されている[10]。

「サイバーセキュリティお助け隊サービス」についても、本制度を活用することで、セキュリティ対策を安価に実施することも可能であり、より多くの企業に認知してもらうことが望ましい。このように、企業に対して取組を促すための金銭的な支援やインセンティブ付与が行政の施策でも実施されるようになっている。情報セキュリティ対策の重要性や脅威の認識を高めるため、引き続き行政が実施する施策の認知度を高めることも重要となるだろう。

[9] 独立行政法人情報処理推進機構 「SECURITY ACTION 自己宣言を申請要件等に採用している補助金・助成金 一覧」
https://www.ipa.go.jp/security/security-action/requirement/requirement.html
[10] 独立行政法人情報処理推進機構 「SECURITY ACTION「普及賛同企業等」一覧」
https://www.ipa.go.jp/security/security-action/download/pr-assist.pdf

6. おわりに

これまで述べてきたように、情報セキュリティ対策は、対策を実施する企業にとって費用対効果をイメージすることが難しい取組である。一方で、これまで防災・減災の事前対策に係る取組として実施されてきた「事業継続力強化計画認定制度」において、サイバー攻撃への対策を追加した計画策定も求められるようになっており、情報セキュリティ対策は、情報セキュリティ上のリスクマネジメントとして取り組む必要があるだけでなく事業継続上の対策として取り組むことが求められている[11]。

こうした状況を踏まえ、行政機関においては、情報セキュリティ対策を実施しなければ情報セキュリティ被害に遭う可能性が高まるだけでなく、取引機会を損失するおそれがあることを中小企業にも認識してもらう取組や、既に用意されている情報セキュリティ対策に取り組んだ企業が得られる補助金等のメリットの周知といった取組を早急に進めていくことが強く求められる。

[11] 中小企業庁 「- 中小企業等経営強化法 - 事業継続力強化計画　策定の手引き（令和6年4月1日版）」
https://www.chusho.meti.go.jp/keiei/antei/bousai/download/keizokuryoku/tebiki_tandoku.pdf

参考文献

独立行政法人情報処理推進機構（2022）「2021 年度中小企業における情報セキュリティ対策に関する実態調査― 調査報告書 ―」

独立行政法人情報処理推進機構（2023）中小企業の情報セキュリティ対策ガイドライン第 3.1 版

独立行政法人情報処理推進機構（2024）「情報セキュリティ 10 大脅威 2024～脅威に呑まれる前に十分なセキュリティ対策を～」

竹内 英二（2022）「中小企業におけるサイバーセキュリティ対策の現状と課題」、日本政策金融公庫『調査月報 中小企業の今とこれから』No.161

菅野泰子、島田裕次（2010）「情報セキュリティ対策における阻害要因の構造に関する企業規模別比較研究」、日本情報経営学会誌 Vol.30, No.3