Information-technology
Promotion
Agency, Japan

2024 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 －

2025 年 5 月
独立行政法人情報処理推進機構

Information-technology
Promotion
Agency, Japan

目次

1. 本調査研究の背景・目的

1.1 調査背景・目的

近年、サプライチェーン上の弱点を狙って、攻撃対象への侵入を図るサイバー攻撃が顕在化・高度化している。サプライチェーンを構成する中小企業等がサイバー攻撃に対する対策が不十分である場合、当該中小企業等の事業活動に支障が生じ得ることに加えて、取引先が提供した重要な情報が流出してしまうおそれや、当該企業を踏み台にして取引先が攻撃されるおそれ等がある。

情報処理推進機構（以下、IPA）では、「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」（以下、「2021 年度調査」という）を実施し、中小企業等における情報セキュリティ対策の実態を明らかにした。2023 年度に「SECURITY ACTION 宣言事業者における情報セキュリティ対策の実態調査」（以下「2023 年度調査」という。）を実施した。その結果、SECURITY ACTION 宣言により取引先からの信頼性が高まる等の期待に反して十分な効果が得られていないこと、二つ星の宣言事業者の中には現状の取組より一層高度化させたい意向があること等を明らかにした。

本調査は、「2021 年度調査」からの経年変化の把握、および「2023 年度調査」の結果を踏まえ、中小企業等におけるサイバーセキュリティ対策の実態及び課題等を明らかにし、中小企業等における規模・業種等に応じた効果の高いサイバーセキュリティ対策の分析・整理することで、サプライチェーン全体のサイバーセキュリティ強化に資することを目的とする。また、SECURITY ACTION 一つ星及び二つ星に求められる基準について分析・調査し、SECURITY ACTION 宣言及びサイバーセキュリティお助け隊サービスを導入する中小企業が、中小企業全体の割合に対して低い水準となっている理由を分析・調査する。

1.2 調査実施内容

本調査では、「2021 年度調査」からの経年変化の把握、中小企業等における規模・業種等に応じた効果の高いサイバーセキュリティ対策の分析・整理を実施した。なお、本調査報告書では、文献調査、アンケート調査、インタビュー調査及びその分析の結果について報告を行う。

- 文献調査
- アンケート調査
- インタビュー調査

1.2.1 調査内容・方法

全体調査フローは次図の通りである。また次項以降に各調査の概要を示す。

1. 文献調査	● 調査項目設定 ● 調査対象選定 ● 調査実施 ● 調査結果整理

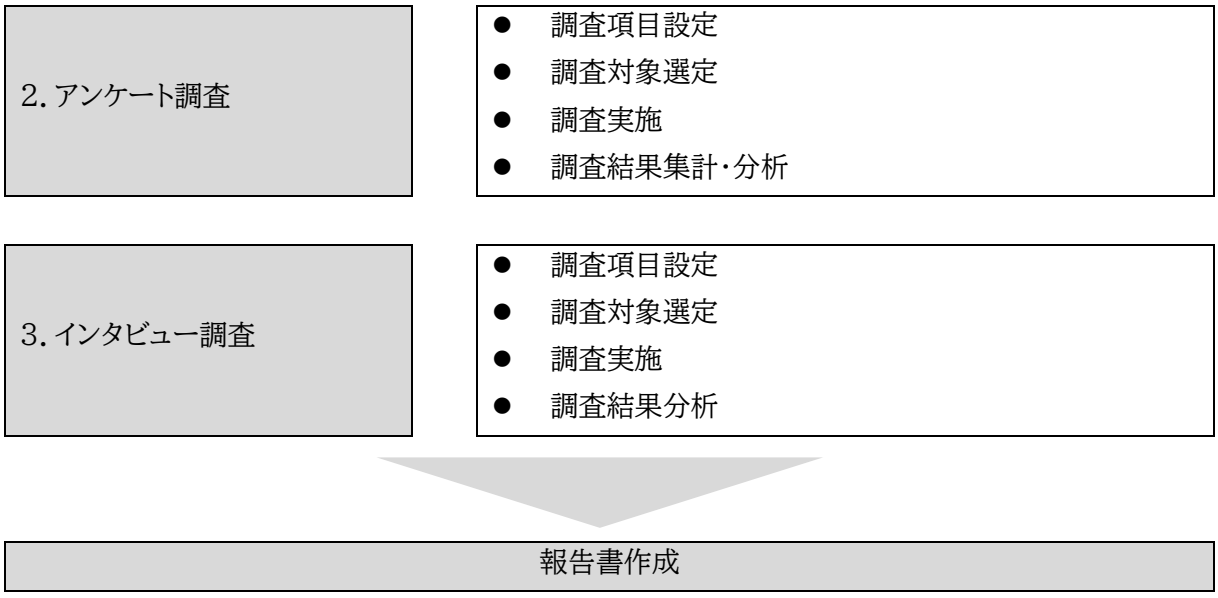
2. アンケート調査
● 調査項目設定
● 調査対象選定
● 調査実施
● 調査結果集計・分析
3. インタビュー調査
● 調査項目設定
● 調査対象選定
● 調査実施
● 調査結果分析
報告書作成

図 1-1 全体調査フロー

2. 文献調査

「2021 年度調査」からの経年変化の把握、中小企業等における規模・業種等に応じた効果の高いサイバーセキュリティ対策の分析・整理を行うにあたり、関連する文献調査を行った。

2.1 調査対象文献

以下を調査観点として設定し、文献調査を実施した。

- 中小企業の実態（経営状況）と支払意思（経営状況と支払意思）
- 中小企業が被るサイバーインシデント被害と被害額の動向（サイバーインシデント被害の動向）
- 自社が行っているサイバーセキュリティ対策に関する認識（自社のセキュリティ対策の認識）
- 中小企業向けサイバーセキュリティ対策ソリューションの動向とコスト感（セキュリティ対策ソリューションの動向とコスト）
- 業界に限らず中小企業等が実施すべきサイバーセキュリティ対策等の観点（実施すべきサイバーセキュリティ対策）
- サプライチェーンの一員としてセキュリティ対策の必要性に関する認識（サプライチェーンにおけるセキュリティ対策の必要性に関する認識）
- サプライチェーンセキュリティにおける評価取得のメリット等の観点（サプライチェーンセキュリティにおける評価取得のメリット）

調査対象文献の一覧と各文献の調査観点を以下に示す。

表 2-1 調査文献対象一覧

No.	文献名	発行者	調査の観点						
			経営状況と支払意思	サイバーインシデント被害の動向	自社のセキュリティ対策の認識	セキュリティ対策ソリューションの動向とコスト	実施すべきサイバーセキュリティ対策	サプライチェーンにおけるセキュリティ対策の必要性に関する認識	サプライチェーンセキュリティにおける評価取得のメリット
1	企業の CISO 等やセキュリティ対策推進に関する実態調査 調査報告書	IPA	○						
2	国内企業のサイバーリスク意識・対策実態調査 2020	日本損害保険協会	○	○	○				
3	中小企業の経営者のサイバーリスク意識調査 2019	日本損害保険協会	○	○	○				

No.	文献名	発行者	調査の観点						
			経営状況と支払意思	サイバーインシデント被害の動向	自社のセキュリティ対策の認識	セキュリティ対策ソリューションの動向とコスト	実施すべきサイバーセキュリティ対策	サプライチェーンにおけるセキュリティ対策の必要性に関する認識	サプライチェーンセキュリティにおける評価取得のメリット
4	インシデント損害額調査レポート 第 2 版	日本ネットワークセキュリティ協会		○					
5	インシデント損害額調査レポート 別紙「被害組織調査」	日本ネットワークセキュリティ協会		○					
6	2023 年国内情報セキュリティ市場調査報告書	日本ネットワークセキュリティ協会				○			
7	データ侵害のコストに関する調査 2024	IBM		○					
8	会員企業の災害・リスク対策に関するアンケート 2024 年調査結果	東京商工会議所	○	○		○			
9	テレワークセキュリティに係る実態調査 結果報告書(2024 年 3 月)	総務省	○	○		○			
10	情報セキュリティ 10 大脅威「2024」・「2025」	情報処理推進機構					○		
11	インシデント報告対応レポート	JPCERT コーディネーションセンター					○		
12	NRI Secure Insight 2023	NRI セキュアテクノロジーズ						○	
13	セキュリティ対策の基本と共通対策_情報セキュリティ 10 大脅威 2024 版	情報処理推進機構					○		
14	自工会/部工会・サイ	日本自							○

No.	文献名	発行者	調査の観点						
			経営状況と支払意思	サイバーインシデント被害の動向	自社のセキュリティ対策の認識	セキュリティ対策ソリューションの動向とコスト	実施すべきサイバーセキュリティ対策	サプライチェーンにおけるセキュリティ対策の必要性に関する認識	サプライチェーンセキュリティにおける評価取得のメリット
	バーセキュリティガイドライン（2023 年度）	動 車 工業会							
15	技術情報管理認証制度	経 済 産業省							○
16	ISMS 適合性評価制度	情 報 マネジメントシステム 認 定センター							○
17	プライバシーマーク制度	日 本 情報 経 済社 会 推進協会							○
18	英 CS/CS+	英国							○
19	米 CMMC	米国							○
20	濠エッセンシャルエイト	オーストラリア							○

2.2 文献調査結果

2.2.1 文献1：IPA「企業の CISO 等やセキュリティ対策推進に関する実態調査 調査報告書」

（1） 概要

本文献[1]は、企業のセキュリティ対策の実態や経営層・CISO 等のセキュリティへの取組みの状況を把握することを目的として文献調査やインタビュー、アンケート調査を実施し、結果と得られた知見をまとめたものである。

表 2-2 アンケート概要[2]

調査対象	従業員数 301 人以上かつ、CISO 等を任命している国内企業
対象期間	2019 年 10 月 1 日～2019 年 10 月 21 日
調査方法	ウェブアンケート調査およびアンケート票調査
回収結果	有効回答数 534 件
調査項目	回答企業の基本属性（業種、従業員数、CISO 等の任命状況等） セキュリティに関する会議体の実施状況やテーマ 経営層が必要とするサイバーセキュリティに関する情報 経営層が CISO 等に求める・重視する役割 CISO 等に求められる重要なスキル・経験 サイバーセキュリティマネジメントの PDCA サイクル サプライチェーンに関する実践事例 インシデントレスポンスに関する実践事例 等 全 34 項目
データ精査方法	回答データに関して、下記の方針で精査し、該当したデータは、回答内容に不備や矛盾があり、信頼性に問題があると判断し、除外 回答時間が 180 秒未満の回答 10 問以上連続して同じ記号の選択肢を回答する不正な回答 設問 34 まで回答がなされていない回答 設問間で矛盾がある回答 同一企業による重複回答

[1] IPA「企業の CISO 等やセキュリティ対策推進に関する実態調査 調査報告書」（2020 年 3 月）
[2] 出所）IPA「企業の CISO 等やセキュリティ対策推進に関する実態調査 調査報告書」（2020 年 3 月）、P17、表 3-1 より

（2） 調査結果

「サプライチェーンの一員としてのセキュリティ対策に関する認識」について、「Q26 サプライチェーンセキュリティへの対策」の回答傾向から、以下が読み取れる。

- 従業員数 301 人以上かつ、CISO 等を任命している国内企業において、サプライチェーンセキュリティへの対策として実施されているのは「契約条項へのセキュリティ要求事項の追加」が主である（60.5%）。
- 「いずれの対策も実施していない」「わからない」と回答した企業はあわせて 13.3%に留まる。
- 中小企業が取り組むべきサイバーセキュリティ対策を検討する際、大企業の認識も踏まえて検討することが考えられる。

「サプライチェーンの一員としてのセキュリティ対策に関する認識」について、「Q31 CSIRT の人員配置状況」の回答傾向から、以下が読み取れる。

- 従業員数 301 人以上かつ、CISO 等を任命している国内企業であっても、CSIRT に 1 名以上の専任のメンバーを配置しているのは約 30%に留まっている。人材不足が課題となっている中小企業では、さらにその割合は小さいと推測できる。

2.2.2 文献2：日本損害保険協会「国内企業のサイバーリスク意識・対策実態調査 2020」

（1） 概要

本文献 [3]は、「新しい生活様式」における企業のサイバーリスクに対する意識や最新の対策状況を把握するため 2020 年 10 月に実施された、日本国内の企業の経営者、管理部門担当者を対象としたインターネット・リサーチ法による、アンケート調査結果である。

表 2-3 アンケート概要 [4]

対象組織	調査実施機関の企業モニタ調査の登録企業（4,000 社）
対象期間	2020 年 10 月 1 日～2020 年 10 月 19 日
調査方法	インターネット調査
回収結果	回答率 1,535 件/4000 件（38.4%） ※回答企業の内訳： 大企業 520 社（33.9%）、中小企業 1,015 社（66.1%）
データ精査方法	不明、回答拒否など回答を得られなかった場合、無回答として設問ごとの集計から除外

[3] 一般社団法人日本損害保険協会「国内企業のサイバーリスク意識・対策実態調査 2020 集計報告書」（2020 年 12 月）
[4] 出所）一般社団法人日本損害保険協会「国内企業のサイバーリスク意識・対策実態調査 2020 集計報告書」を元に株式会社三菱総合研究所が作成

（2）調査結果

「自社が行っているサイバーセキュリティ対策に関する認識」について、「Q6 行っているサイバーリスク対策」の回答傾向から、以下が読み取れる。

- サイバーリスク対策を行っていない企業は企業規模にかかわらず少なく、ほとんどの企業で何かしらの対策が行われている。
- 「ソフトウェア等の脆弱性管理・ウイルス対策ソフトの導入」は企業規模にかかわらず多くの企業で行われている。

「サプライチェーンの一員としてセキュリティ対策の必要性に関する認識」について、「Q10 取引先や委託先のサイバーリスク対策の管理状況」の回答傾向から、以下が読み取れる。

- 取引先や委託先のサイバーリスク対策の管理を行っていない企業は、大企業でも中小企業でも40％以上にのぼる。ただし、従業員数が少ない企業ほど比率が高くなる傾向にある。

「サイバー保険の動向」について、「Q13 サイバーリスク保険の加入状況」の回答傾向から、以下が読み取れる。

- 取引先や委託先のサイバーリスク対策の管理を行っていない企業は、大企業でも中小企業でも40％以上にのぼる。ただし、従業員数が少ない企業ほど比率が高くなる傾向にある。

「中小企業が被るサイバーインシデント被害と被害額の動向」について、「Q17 サイバー被害状況」の回答傾向から、以下が読み取れる。

- 13.4％の企業がこれまでにサイバー被害を受けたことがあると回答しており、中小企業でも11.4％が経験している。

「中小企業が被るサイバーインシデント被害と被害額の動向」について、「Q18-2 サイバー被害を受けた際の攻撃の種類」の回答傾向から、以下が読み取れる。

- 攻撃の種類としては、「マルウェア」や「ランサムウェア」が最も多く、次点で「不正送金を促すビジネスメール詐欺やフィッシングサイト」が多い。
- 企業規模による傾向の違いは見られない。

「中小企業が被るサイバーインシデント被害と被害額の動向」について、「Q18-5 サイバー被害を受けた際の被害総額」の回答傾向から、以下が読み取れる。

- 被害額としては、大企業・中小企業ともに 50 万円未満が最も多いが、中小企業でも 1000 万～1 億円未満の被害を受けたと回答したところもあり、中小企業の 1 企業あたりの売上高は 2.1 億円（経済産業省 令和 5 年中小企業実態基本調査）であることを考えると、経営に多大な影響を及ぼすことが考えられる。（サイバー攻撃による被害によって倒産してしまった企業は回答していないことにも留意が必要である）

2.2.3 文献3：日本損害保険協会「中小企業の経営者のサイバーリスク意識調査 2019」

（1） 概要

本文献 [5]は、中小企業のサイバーリスクに対する危機意識および対策実態を明らかにする目的で2019 年 11 月に実施された、中小企業の経営者・役員（825 社）、大企業の経営者・役員（207 社）を対象としたインターネット・リサーチ法による、サイバーリスク意識調査結果である。

調査項目は経営課題、サイバー攻撃のリスク認知および被害と対策状況、サイバー保険などに関して、簡潔な設問内容（合計28問）で構成されており、分析結果は大企業と中小企業との対比、業種別（製造業と非製造業）の割合などがわかるように整理されている。

（2） 調査結果

「中小企業の実態（経営状況）と支払意思」について、「Q1 経営課題の優先度」および「Q2 サイバーリスクの認知度」の回答傾向から、以下が読み取れる。

- 本資料の分析サマリにも記載があるが、経営課題における「サイバーリスクへの対応」の優先順位は中小企業、大企業ともに「その他」に次いで低い状況にある。 Q2 のサイバーリスクの認知度の結果（大企業の方がリスク認知度が高い）と合わせると、経営課題に係る投資項目としてのサイバーリスクへの対応（支払意思）は、リスク認知度によらず経営課題に挙がっていないことが推察される。
- 一方で「収益性の向上」、「人材の育成」は中小企業、大企業ともに共通する優先課題であり、「サイバーリスクへの対応」が「収益性の向上」とほとんど結びついていないことが推察される。

「中小企業が被るサイバーインシデント被害と被害額の動向」について、「Q16 サイバー攻撃の被害経験」の回答傾向から、以下が読み取れる。

- 何らかのサイバー攻撃の被害にあったと回答した中小企業の経営者は825 人中155 人（18.8%）
- 不正送金を促すビジネスメール詐欺やフィッシングサイトの被害にあった割合は大企業・中小企業共に高く、対策が求められると考えられる。

「中小企業が被るサイバーインシデント被害と被害額の動向」について、「Q17 サイバー攻撃による被害額」の回答傾向から、以下が読み取れる。なお、「金銭的被害」の捉え方によっては、「費用損害」「賠償損害」「利益損害」「行政損害」「無形損害」が別にかかっている可能性があることに留意が必要である。

- 金銭的被害まで発生したと回答した中小企業の経営者は 825 人中 27 人（3.3%）
- 被害額としては、50 万円未満が最も多いが、1000 万～1 億円未満の被害を受けた事例も発生しており、中小企業の 1 企業あたりの売上高は 2.1 億円（経済産業省 令和 5 年中小企業実態基本調査）であることを考えると、経営に多大な影響を及ぼすことが考えられる。（サイバー攻撃による被害によって倒産してしまった企業は回答していないことにも留意が必要である）

「中小企業が被るサイバーインシデント被害と被害額の動向」について、「Q19 サイバー攻撃の被害に遭った際の影響」の回答傾向から、以下が読み取れる。

- 中小企業では、「原因の調査・復旧対応にかかる費用の捻出」と回答する企業が多かった。

[5] 一般社団法人日本損害保険協会「中小企業の経営者のサイバーリスク意識調査 2019」（2020 年 1 月）

- 特に「社会的評価の低下」については、企業規模による差異が大きい。

「自社が行っているサイバーセキュリティ対策に関する認識」について、「Q8 攻撃への対策内容」の回答傾向から、以下が読み取れる。

- 中小企業は大企業と比較して、OS やソフトウェアの脆弱性管理、ウイルス対策ソフトの導入以外の対策が行われていない傾向にある。また、対策を行っていないと回答した中小企業の経営者は 24.0%に及んでおり、自社状況を踏まえた適切な対策(≒効果の高い対策)が取れていない可能性がある。
- 大企業と中小企業の差が一番大きいのは「社員の教育・研修・訓練の実施」となっており、標的型攻撃や不注意による情報漏えい、ビジネスメール詐欺といった従業員のリテラシーが問われる脅威に対して脆弱である可能性がある。

「自社が行っているサイバーセキュリティ対策に関する認識」について、「Q15 サイバーセキュリティについて今後打つべき対策」の回答傾向から、以下が読み取れる。

- 中小企業は大企業と比較して、教育や人材より具体的なセキュリティ対策(脆弱性管理、ウイルス対策、データ暗号化)を選択しているも、一方で、リスクアセスメントの実施を選択した割合は少なく、また特になし、わからないを選択した割合の多さからも自社状況を踏まえた適切な対策(≒効果の高い対策)が取れていない可能性がある。
- 専門部署の設置や人材の雇用・育成を選択する割合は低いが、社員教育・訓練は3番目に多い回答となっており、現有の人材のセキュリティリテラシーを高めることの意識が高いものと推察できる。
- 取引先や委託先への対策依頼・義務化は、中小企業、大企業ともに低い傾向がある。
- セキュリティ認証の取得は中小企業においても 10%弱であるが必要性を認識している。

「サイバー保険の動向」について、「Q23 サイバー保険の認知度」および「Q24 サイバー保険の加入有無【保険認知者ベース】」の回答傾向から、以下が読み取れる。

- サイバー保険を認知している中小企業の経営者は 33.5%に留まっており、特に中小企業ではサイバー保険の認知が進んでいない状況にある。
- サイバー保険を認知している経営者であっても、85.5%がこれまでに加入したことがないと回答しており、普及は進んでいない状況にある。

2.2.4 文献4:日本ネットワークセキュリティ協会「インシデント損害額調査レポート 第２版」

(1) 概要

本文献[6]は、インシデント発生時の具体的な対応、アウトソーシング先、実際に生じるコスト(損害額・損失額)を各事業者への調査によりまとめたもの。インシデント発生時において生じる損害を６つに区分

[6] 特定非営利活動法人日本ネットワークセキュリティ協会「インシデント損害額調査レポート 第２版」(2023 年２月)

したうえで、それぞれの対応およびそのコストがまとめられている。

表 2-4 インシデント発生時において生じる損害の 6 つの区分[7]

損害の種類	説明
費用損害 （事故対応損害）	被害発生から収束に向けた各種事故対応（「初動対応および調査」「対外的対応」「復旧および再発防止」等）に関してアウトソーシング先への支払を含め、自組織で直接、費用を負担することにより被る損害
賠償損害	情報漏えいなどにより、第三者（被害者個人ほか、委託契約における委託元、クレジットカード会社、取引先等の法人）から損害賠償請求がなされた場合の損害賠償金や弁護士報酬等を負担することにより被る損害
利益損害	ネットワークの停止などにより、事業が中断した場合の利益喪失や、事業中断時における人件費などの固定費支出による損害
金銭損害	ランサムウェアをはじめとするマルウェア感染、ビジネスメール詐欺、インターネットバンキングでのなりすまし等による直接的な、金銭（自組織の資金）の支払いによる損害
行政損害	個人情報保護法において命令違反等により科される罰金、GDPR（EU 一般データ保護規則。日本における個人情報保護法に相当）等において課される課徴金等の損害
無形損害	風評被害、ブランドイメージの低下、株価下落など、無形資産等の価値の下落による損害、金銭の換算が困難な損害

（2）調査結果

中小企業における損害額のイメージ（参考値）が見積もられている。「中小企業が被るサイバーインシデント被害と被害額の動向」について、ケースバイケースではあるものの、中小企業で数千万円単位、場合によっては数億円単位の損失もあり得るとのことだが、中小企業の 1 企業あたりの売上高は 2.1 億円（経済産業省 令和 5 年中小企業実態基本調査）であることを考えると、サイバーインシデントが生じた場合、経営に多大な影響を及ぼすことが考えられる。

表 2-5 中小企業における損害額のイメージ（参考値）[8]

損害の種類		中小企業における損害額のイメージ（参考値）
大区分	小区分	
費用損害	事故原因・被害範囲調査費用	300～400 万円

[7] 出所）特定非営利活動法人日本ネットワークセキュリティ協会「インシデント損害額調査レポート 第 2 版」（2023 年 2 月）を元に株式会社三菱総合研究所が作成
[8] 出所）特定非営利活動法人日本ネットワークセキュリティ協会「インシデント損害額調査レポート 第 2 版」（2023 年 2 月）、P3 より

損害の種類		中小企業における損害額のイメージ（参考値）
大区分	小区分	
（事故対応損害）	コンサルティング費用	10～100 万円
	法律相談費用	30～100 万円
	広告・宣伝活動費用	1 万人に DM 送付した場合、約 130 万円 地方紙への新聞広告を出稿した場合約 50 万円
	コールセンター費用	3 ヶ月の対応で 700～1,000 万円
	見舞金・見舞品購入費用	1 万人へのプリペイドカード送付で 650 万円
	ネット炎上防止費用	対応内容によって大きく異なるが 300～900 万円のケースも
	ダークウェブ調査費用	調査内容によって大きく異なるが数百万円以上の額となるケースも
	クレジット情報モニタリング費用	1 ヶ月あたり 100～500 万円
	システム復旧費用	対応規模等によって大きく異なるが、数百～数千万円のケースも
	再発防止費用	対応規模等によって大きく異なるが、数百～数千万円のケースも
	超過人件費	対応規模等によって大きく異なるが、多くの従業員等が対応に追われるケースも
賠償損害	損害賠償金	委託先から預かった情報漏えい事案の場合、上記費用損害の合計額が委託先から求償されることも。EC サイトのクレジットカード情報漏えい事案の場合、不正利用の規模によるが数千万円以上の額の求償がなされるケースも
	弁護士費用等	損害賠償金に比例して高額に
利益損害		数ヶ月の売上高の減少（利益喪失に加え、回避できない固定費の支払い）
金銭損害	ランサムウェアによる身代金	支払いは慎むべきだが、数千万円以上の額の要求がなされるケースも
行政損害		個人情報保護法上の罰金は最大 1 億円
無形損害		顧客離れ、株価下落など換算不能な損失が
合計		ケースバイケースではあるものの、中小企業で数千万円単位、場合によっては数億円単位の損失も。経営に多大な影響が・・・。

2.2.5 文献5：日本ネットワークセキュリティ協会「インシデント損害額調査レポート 別紙「被害組織調査」」

（1） 概要

本文献[9]は、実際にサイバーインシデント被害に遭った組織について、組織の規模、業種、サイバー攻撃の種別ごとに集計した統計情報、アンケート調査によって判明したサイバー攻撃の被害組織が被った損害額、そしてアンケート調査に回答いただいた被害組織へのインタビューにより、被害の実態を明らかにしたものである。

表 2-6 調査概要[10]

対象組織	サイバー攻撃に関する被害の公表または報道等がなされた国内の約1,300 組織
対象期間	2017 年 1 月～2022 年 6 月
収集方法	情報の収集にあたっては次のような情報ソースを参照 ① セキュリティ情報サイト Security NEXT：https://www.security-next.com/ ScanNetSecurit：https://scan.netsecurity.ne.jp/ サイバーセキュリティ.com：https://cybersecurity-jp.com/ ② サイバー攻撃による被害等を公表した組織のページ ③ セキュリティベンダーやセキュリティ研究者が公開している国内外のサイト、ブログなど

（2） 調査結果

「中小企業が被るサイバーインシデント被害と被害額の動向」について、「被害組織（全体）の規模別割合」、「被害組織業種別割合」、「国内企業全体の業種別割合」から、以下が読み取れる。

- そもそもの企業数の差はあるが、被害組織の規模別件数・割合は中小企業が最も多く、大企業だけが被害にあうわけではないことが分かる。
- 国内企業全体の業種別割合を踏まえると、製造業や情報通信業では被害組織の割合が高い。被害公表がされづらい業種があることも留意する必要があるが、業種によって傾向が異なる可能性が示唆されるため、業種別の検討が求められることが分かる。

[9] 特定非営利活動法人日本ネットワークセキュリティ協会「インシデント損害額調査レポート 別紙「被害組織調査」」（2024 年 2 月）
[10] 出所）特定非営利活動法人日本ネットワークセキュリティ協会「インシデント損害額調査レポート 別紙「被害組織調査」」を元に株式会社三菱総合研究所が作成

「中小企業が被るサイバーインシデント被害と被害額の動向」について、「ランサムウェア感染被害組織の被害金額」、「エモテット感染組織の被害金額」、「ウェブサイトからの情報漏えい被害組織の被害金額」から、以下が読み取れる。

- 被害額の平均値は被害の種類によって異なっている。対策を検討する際はどの被害を防ぐためのものなのかについて意識する必要があると思われる。
  ※上記の結果は中小企業だけでなく大企業や団体等の回答も含まれたものであることに留意が必要である。

表 2-7 被害の種類ごとの被害額(平均値)とアンケート回答傾向 [11]

被害の種類		被害額の平均値	備考
ランサムウェア		2,386 万円	• ほとんどの被害組織が被害金額を 1,000 万円超と回答 • 事故対応に要した内部工数(人月)は平均 27.7 人月 • ランサムウェア感染によって引き起こされたシステムの停止、データの消失による利益の喪失、機会損失などによる損害額、組織内部の従業員や職員による対応に要したコストが被害金額に計上されていないケースが多数 • すべての被害組織がランサムウェア攻撃者に対して身代金は支払っていないと回答
エモテット		1,030 万円	• 被害金額を 2,000 万円以上と回答した組織がある一方で、被害金額が極端に低い組織(数 10 万円以下や対応工数のみなど)も存在 • 事故対応に要した内部工数(人月)は、平均が2.9 人月 • 組織内部の従業員や職員による対応に要したコストが被害金額に計上されていないケースが多数
ウェブサイトからの情報漏えい	個人情報のみが漏えい	2,955 万円	• 事故対応に要した内部工数(人月)は、平均が 13.3 人月 • 組織内部の従業員や職員による対応に要したコストが被害金額に計上されていないケースが多数
	クレジットカード情報も漏えい	3,843 万円	• 事故対応に要した内部工数(人月)は、平均が 13.5 人月 • 組織内部の従業員や職員による対応に要したコストが被害金額に計上されていないケースが多数

2.2.6 文献6:日本ネットワークセキュリティ協会「2023 年度 国内情報セキュリティ市場

[11] 特定非営利活動法人日本ネットワークセキュリティ協会「インシデント損害額調査レポート 別紙「被害組織調査」」(2024 年 2 月)を元に株式会社三菱総合研究所が作成

調査報告書」

（1） 概要

本文献[12]は、国内における情報セキュリティに関するツール、サービスの提供を行う事業者を対象とし、市場規模データの算出、集計、調査、分析を行った報告書である。

調査対象となる事業者の事業は、ツール（ハード・ソフトウェア等のプロダクト）やサービス（役務提供、ノウハウ知的事業活動）の 2 種類に分類。調査対象となる事業者は、セキュリティツールのメーカー、販売店、コンサルティング企業等の 8 区分。なお、事業者の規模に関する言及は無い。

有効回答数は 680 社（調査対象：1,033 社）。調査結果は、事業者の売上高を基に、様々な軸（情報セキュリティ市場全体規模、ツールの市場規模、ツールごとの市場規模、サービスの市場規模、サービスごとの市場規模）で市場規模の推移が整理されている。

（2） 調査結果

「情報セキュリティ 市場規模の推移」について、以下が読み取れる。

- 日本国内において、情報セキュリティ市場規模全体として、増加傾向にある。ツール及びサービスについても、それぞれ市場規模は増加傾向にある。
- 情報セキュリティ市場は、ツールとサービスを比較すると、ツールの方が市場規模は高い。

「情報セキュリティ ツール市場推移」について、以下が読み取れる。

- すべてのツールにおいて、市場規模は増加傾向にある。

「情報セキュリティ サービス市場推移」について、以下が読み取れる。

- すべてのサービスにおいて、市場規模は増加傾向にある。

2.2.7 文献7：IBM「データ侵害のコストに関する調査 2024」

（1） 概要

本文献[13]は、2023 年 3 月から 2024 年 2 月の間に、データ侵害の影響を受けた 604 社を対象として、2,100 件～11 万 3,000 件の侵害状況に関する調査結果をまとめたものである。

調査対象は、16 の国（日本を含む）や地域における、17 の業種の組織である。なお、調査対象企業の規模に関する言及は無く、プライバシーの観点で組織の情報は収集していない。

- 国と地域
  ASEAN、オーストラリア、ベルネクス、ブラジル、カナダ、フランス、ドイツ、インド、イタリア、日本、ラテンアメリカ、中東、南アフリカ共和国、韓国、イギリス、アメリカ合衆国

[12] 特定非営利活動法人日本ネットワークセキュリティ協会「2023 年 国内情報セキュリティ市場調査報告書」（2024 年 6 月）
[13] IBM「2024 年データ侵害のコストに関する調査」、https://www.ibm.com/jp-ja/reports/data-breach

- 業種
  金融業、製造業、プロフェッショナル・サービス（法律、会計等）、テクノロジー、官公庁・政府機関、エネルギー、小売、メディア（新聞、出版等）、消費財、運輸、製薬、ホスピタリティー（ホテル、レストラン等）、マスコミ、教育、エンターテイメント、医療、研究

本文献において、データ侵害とは、企業、官公庁・政府機関、金融関連の機密情報または個人を特定する情報が漏洩するイベントを意味している。また、コストとは、業務中断による被害や侵害に対応するための費用等を意味している。

（2）調査結果

「データ侵害のグローバルな平均総コスト」より、以下が読み取れる。

- グローバル全体でみたときに、データ侵害によるコストは増加傾向ある。
- なお、この傾向は、日本の中小企業全体でみたときは、概ね同様であるかは不明である。

「業界別データ侵害コスト」より、以下が読み取れる。

- 業種別にみたときに、「医療」業界のデータ侵害コストが最も大きい。
- 業界によって、データ侵害に対する脆弱性リスクの高さが異なる場合がある。

「侵害を受けたデータの種類（割合別）」より、以下が読み取れる。

- 盗難または侵害に遭ったデータの種類で最も多かったのは、顧客の個人情報（PII）で、46％であった。
  ※個人情報には、納税者番号やＥメール、自宅の住所等が含まれる
- 組織が持つデータの種類によって、脆弱性リスクの高さが異なる場合がある。

「AIと自動化の使用レベル別のデータ侵害のコスト」より、以下が読み取れる。

- AIと自動化を利用している組織ほど、平均侵害コストが低くなっている。
- セキュリティ対策を実行することで、効果が得られることが定量的なデータとして表れている。

「法執行機関との連携によるコスト削減」より、以下が読み取れる。

- 法執行機関との連携を通じてランサムウェア攻撃に対する侵害コストを大幅に削減できる。法執行機関の支援を受けて交渉を進めることで、困難な状況でも 100 万ドルもの資金を節約でき、組織はさらなる損失を未然に防ぐための迅速な手段を確保することができる。これによりコスト削減だけでなく、リスクマネジメント能力の向上も期待できる。

「セキュリティ運用と AI の連動効果」より、以下が読み取れる。

- AI 技術を組み込んだセキュリティ運用は、攻撃予防から事後対応にわたる全段階で業務の効率化を可能にし、コスト削減につながっている。特に、予防領域における AI の活用が最も大きな効果をもたらし、攻撃発生以前の潜在的脅威を効果的に排除することで、コストを 222 万ドルまで抑えることができると報告されている。

「業務中断と投資のバランス」より、以下が読み取れる。

- 中小企業は、業務中断に敏感で、経費削減圧力との間で、サイバーセキュリティへの投資のバランスを取る意思が求められている。特にサイバー攻撃による業務中断は、企業の財務基盤に即時かつ多大な影響を与える可能性があるため、わずかなセキュリティ投資の決定も経営上の大きな課題として捉えられている。

「侵害コストの増加と PII の影響」より、以下が読み取れる。

- データ侵害の被害額が前年比で大幅に増加し、2024 年には世界での侵害コストが平均して 488 万ドルに達している。特に中小企業では顧客の PII が関与した侵害が頻発し、その対応に苦慮している。これにより事業停止や顧客離れといった深刻な影響が発生しており、これが企業存続に影を落としている。なお、PII には納税者番号や E メール、自宅の住所などが含まれており、なりすましやクレジットカード詐欺に利用されることがある。

シャドー・データ関連の増加傾向について以下が読み取れる。

- 中小企業のセキュリティリスクは特に、シャドー・データの扱いに起因する場合が多く、この影響により、データ侵害が生じると一般的なコストが増加することが報告されている。この影響を軽減し、業績に与える深刻な影響を抑制するため、データ管理の透明性向上や適切な監視体制が求められている。

2.2.8 文献8：東京商工会議所「会員企業の災害・リスク対策に関するアンケート 2024 年調査結果」

（1） 概要

本文献[14]は、東京商工会議所が、災害・リスク対策委員会において、会員企業における BCP 策定状況や、帰宅困難者対策、行政に望む災害・リスク対策施策等を把握するため、アンケートを実施し、調査結果をとりまとめたものである。なお、情報セキュリティ上のリスクに対する備えについても調査対象としている。

表 2-8 アンケート概要[15]

調査対象	東京商工会議所会員企業 17,472 件
回答件数	1,157 件（回答率 6.6%）

[14] 東京商工会議所「会員企業の災害・リスク対策に関するアンケート2024年調査結果」（2024 年 8 月）
[15] 出所）東京商工会議所「会員企業の災害・リスク対策に関するアンケート2024年調査結果」を元に株式会社三菱総合研究所が

調査期間	2024 年 6 月 3 日～6 月 19日
調査方法	• FAX・メールによる調査票の送付 • オンライン・FAX・メールによる回答

（2） 調査結果

「中小企業の実態（経営状況）と支払意欲」について、情報セキュリティ上のリスクに対して、備えが必要だと感じている企業は 8 割となっている。一方で、BCP で情報セキュリティ上のリスクを想定している企業は 4 割となっている。この結果から、以下が読み取れる。

- 情報セキュリティ上のリスクに対する備えが必要と感じていながらも、BCP でリスクとして想定していない企業が多い傾向がある。

「中小企業の実態（経営状況）と支払意欲」について、情報セキュリティ対策への年間投資額にて、投資をしていない中小企業が 14.5%、50 万円未満の中小企業が 36.6%となっている。大手企業と比べると、いずれの割合も下回っている。この結果から、以下が読み取れる。

- 中小企業は情報セキュリティ対策への年間投資額は少なく、費用面の課題を解消することが必要である

「サプライチェーンの一員としてのセキュリティ対策に関する認識」について、BCP 策定済みの企業のうち、社内周知・見直しを実施している企業は約 7 割、訓練を実施している企業は 5 割であった。また、受注時に、BCP の有無の確認や策定の要請を受けていない企業は約 7 割であった。この結果から、以下が読み取れる。

- BCP 策定後の社内周知・見直し・訓練が十分に取り組まれていないこと、取引先からの BCP 策定の要請を受ける企業が少ない。

2.2.9 文献9：総務省「テレワークセキュリティに係る実態調査 結果報告書（2024 年 3 月）」

（1） 概要

本文献[16]は、企業等におけるテレワークに関するセキュリティ等の実態を把握するための調査を Web アンケートにより実施し、調査結果をとりまとめたものである。

表 2-9 アンケート概要[17]

[16] 総務省「テレワークセキュリティに係る実態調査 調査報告書」（2024 年 3 月）
[17] 出所）総務省「テレワークセキュリティに係る実態調査 調査報告書」を元に株式会社三菱総合研究所が作成

調査地域	日本全国
対象企業	31,200（従業員等が 10 名以上）
回答件数	9,587（うちテレワーク実施企業 2,548）
調査期間	2024 年 1 月 31 日～2 月 22 日
調査方法	はがきにより調査案内を郵送し、専用ウェブサイトにて回答
アンケート項目の観点	・ スクリーニング調査 ・ テレワーク導入状況 ・ テレワーク実施における各種対策 ・ テレワーク端末 ・ その他のテレワーク利用製品 ・ 情報セキュリティ対策 ・ テレワーク時のセキュリティ対策を推進するに当たって ・ 総務省が作成するガイドライン

（2） 調査結果

「自社が行っているサイバーセキュリティ対策に関する認識」について、情報セキュリティ対策に関する取組の実施状況について、マルウェア対策は 6 割半ばが十分に実施、教育・脅威インテリジェンスは7割近くが不十分か未実施となっている。また、多くの企業で情報セキュリティ対策の組織体制整備ができていない状況であった。この結果より、以下が読み取れる。

- 情報セキュリティ対策の実施事項のうち、組織体制整備や教育が十分に実施されていない傾向がある。

「業界に寄らず中小企業等が実施すべきサイバーセキュリティ対策等」について、一部の企業では、サポート期限切れ OS の使用が続けられている。また、サポート期限切れ OS が危険という認識を持っていない企業も存在する。この結果より、以下が読み取れる。

- サポート期限切れ OS を使用することに関するリスクが認知されていないこと、サポート期限切れ OS の使用が続けられている企業が存在する。

2.2.10 文献10：IPA「情報セキュリティ 10 大脅威「2024」・「2025」」

（1） 概要

「情報セキュリティ 10 大脅威」[18]は、前年に発生した社会的に影響が大きかったと考えられる情報セ

[18] IPA「情報セキュリティ 10 大脅威」、https://www.ipa.go.jp/security/10threats/index.html

キュリティにおける事案から、IPA が脅威候補を選出し、情報セキュリティ分野の研究者、企業の実務担当者などのメンバーからなる「10 大脅威選考会」が脅威候補に対して審議・投票を行い、決定したものである。また、脅威ごとの説明や対策についてまとめた解説書も併せて発行されている。

※本文献の調査では、2024 年版、2025 年版を対象としている

※本調査時点（2025 年 2 月 28 日）では、2025 年版の解説書は未発行である

（2）調査結果

2024 年版（2023 年）、2025 年版（2024 年版）の情報セキュリティ 10 大脅威[組織]は下表のとおり。上位に挙げられている脅威は、継続して脅威として取り扱われている。

表 2-10 情報セキュリティ 10 大脅威 2024[組織][19]

順 位	「組織」向け脅威
1	ランサムウェアによる被害
2	サプライチェーンの弱点を悪用した攻撃
3	内部不正による情報漏えい等の被害
4	標的型攻撃による機密情報の窃取
5	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）
6	不注意による情報漏えい等の被害
7	脆弱性対策情報の公開に伴う悪用増加
8	ビジネスメール詐欺による金銭被害
9	テレワーク等のニューノーマルな働き方を狙った攻撃
10	犯罪のビジネス化（アンダーグラウンドサービス）

表 2-11 情報セキュリティ 10 大脅威 2025[組織][20]

順位	「組織」向け脅威	10 大脅威での取り扱い（2016 年以降）
1	ランサムウェアによる被害	10 年連続 10 回目
2	サプライチェーンの弱点を悪用した攻撃	7 年連続 7 回目
3	内部不正による情報漏えい等の被害	5 年連続 8 回目
4	標的型攻撃による機密情報の窃取	10 年連続 10 回目

[19] IPA「情報セキュリティ 10 大脅威 2024」、https://www.ipa.go.jp/security/10threats/10threats2024.html
[20] IPA「情報セキュリティ 10 大脅威 2025」、https://www.ipa.go.jp/security/10threats/10threats2025.html

5	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	10 年連続 10 回目
6	不注意による情報漏えい等の被害	5 年連続 5 回目
7	脆弱性対策情報の公開に伴う悪用増加	初選出
8	ビジネスメール詐欺による金銭被害	5 年ぶり 6 回目
9	テレワーク等のニューノーマルな働き方を狙った攻撃	8 年連続 8 回目
10	犯罪のビジネス化（アンダーグラウンドサービス）	7 年連続 8 回目

また、2024 年版（2023 年）の情報セキュリティ 10 大脅威[組織]の各脅威に対する対策と対応（一部抜粋）は以下のとおり。特に、上位に挙げられている脅威に対する対策は、効果の高いセキュリティ対策の一つとして考えられる。

表 2-12 情報セキュリティ 10 大脅威 2024[組織]に対する対策と対応（一部抜粋）[21]

情報セキュリティ 10 大脅威 2024[組織]		対策と対応
順位	「組織」向け脅威	
1	ランサムウェアによる被害	■組織（経営者層） • 組織としての体制の確立 ➢ 組織としての体制の確立 ■組織（システム管理者、従業員） • 被害の予防 ➢ インシデント対応体制を整備し対応する ➢ 情報セキュリティ対策の基本（ソフトウェアの更新、セキュリティソフトの利用、パスワードの管理・認証の強化、設定の見直し、脅威・手口を知る）を実施 ➢ メールの添付ファイル開封や、メールや SMS のリンク、URL のクリックを安易にしない • 被害を受けた後の対応 ➢ 適切な報告／連絡／相談を行う ➢ 適切なバックアップ運用を行う
2	サプライチェーンの弱点を悪用した攻撃	■組織（経営者層） • 被害の予防 ➢ インシデント対応体制を整備し対応する

[21] 出所）IPA「情報セキュリティ 10 大脅威 2024」を元に株式会社三菱総合研究所が作成

情報セキュリティ 10 大脅威 2024[組織]		対策と対応
順位	「組織」向け脅威	
		■組織（自組織で実施） • 被害の予防 ➢ 情報管理規則の徹底 ➢ セキュリティ評価サービス（SRS）を用いた自組織のセキュリティ対策状況の把握 ➢ 信頼できる委託先、取引先、サービスの選定 ➢ 商流に関わる組織、サービスの信頼性評価（ISMAP など）、品質基準を検討し、複数候補を検討する。 ➢ 契約内容の確認 • 被害を受けた後の対応 ➢ インシデント対応体制を整備し対応する ➢ 被害への補償 ■組織（自組織に関わる組織と共に実施） • 被害の予防 ➢ 取引先や委託先との連絡プロセスの確立 ➢ 取引先や委託先の情報セキュリティ対応の確認、監査 ➢ 情報セキュリティの認証取得 • 被害を受けた後の対応 ➢ 適切な報告／連絡／相談を行う
3	内部不正による情報漏えい等の被害	■組織（システム管理者） • 被害の予防 ➢ 基本方針の策定 ➢ 資産の把握、対応体制の整備 ➢ 重要情報の管理、保護 ➢ 物理的管理の実施 • 被害の早期検知 ➢ システム操作履歴の監視 • 被害を受けた後の対応 ➢ 適切な報告／連絡／相談を行う ➢ インシデント対応体制を整備し対応する
4	標的型攻撃による機密情報の窃取	■組織（経営者層） • 組織としての体制の確立

情報セキュリティ 10 大脅威 2024[組織]		対策と対応
順位	「組織」向け脅威	
		➢ インシデント対応体制を整備し対応する ■組織（セキュリティ担当者、システム管理者） • 被害の予防／対応力の向上 ➢ 情報の管理と運用規則策定 ➢ サイバー攻撃に関する継続的な情報収集 • 被害の早期検知 ➢ サーバやクライアント、ネットワークに適切なセキュリティ対策を行う • 被害を受けた後の対応 ➢ インシデント対応体制を整備し対応する ■組織（従業員、職員） • 被害の予防（通常、組織全体で実施） ➢ 情報セキュリティ対策の基本（ソフトウェアの更新、セキュリティソフトの利用、パスワードの管理・認証の強化、設定の見直し、脅威・手口を知る）を実施 ➢ メールの添付ファイル開封や、メールや SMS のリンク、URL のクリックを安易にしない • 被害を受けた後の対応 ➢ インシデント対応体制を整備し対応する
5	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	■組織（経営者層） • 被害の予防 ➢ インシデント対応体制を整備し対応する ■組織（ソフトウェアの利用者、システム管理者） • 被害の予防 ➢ 情報セキュリティ対策の基本（ソフトウェアの更新、セキュリティソフトの利用、パスワードの管理・認証の強化、設定の見直し、脅威・手口を知る）を実施 ➢ 資産の把握、対応体制の整備 ➢ セキュリティのサポートが充実しているソフトウェアやバージョンを使う • 被害の早期検知 ➢ サーバやクライアント、ネットワークに適切なセキュリティ対策を行う • 修正プログラムのリリース前の対応

情報セキュリティ 10 大脅威 2024[組織]		対策と対応
順位	「組織」向け脅威	
		➢ 回避策や緩和策の適用 ➢ 当該ソフトウェアの一時的な使用停止 • 修正プログラムリリース後の対応 ➢ 修正プログラムの適用 • 被害を受けた後の対応 ➢ 影響調査および原因の追究、対策の強化
6	不注意による情報漏えい等の被害	■組織（当事者） • 被害の予防（被害に備えた対策含む） ➢ 情報リテラシー、モラルを向上させる ➢ 確認プロセスに基づく運用 ➢ 特定の担当者に業務が集中しない体制の構築 • 被害の早期検知 ➢ 問題発生時の内部報告体制の整備 ➢ 外部からの連絡窓口の設置 • 被害を受けた後の対応 ➢ 適切な報告／連絡／相談を行う ■個人/組織（被害者） • 被害を受けた後の対応 ➢ クレジットカードの停止 ➢ 適切な報告／連絡／相談を行う
7	脆弱性対策情報の公開に伴う悪用増加	■組織（経営者層） • 被害の予防 ➢ インシデント対応体制を整備し対応する ■個人、組織（システム管理者／ソフトウェア利用者） • 被害の予防 ➢ 情報セキュリティ対策の基本（ソフトウェアの更新、セキュリティソフトの利用、パスワードの管理・認証の強化、設定の見直し、脅威・手口を知る）を実施 ➢ サーバやクライアント、ネットワークに適切なセキュリティ対策を行う ➢ 脆弱性関連情報の収集と対応 • 被害の早期検知 ➢ サーバやクライアント、ネットワークに適切なセキュリティ対策を行う • 被害を受けた後の対応 ➢ 適切な報告／連絡／相談を行う

情報セキュリティ 10 大脅威 2024[組織]		対策と対応
順位	「組織」向け脅威	
		➢ インシデント対応体制を整備し対応する ■組織（開発ベンダー） • 製品セキュリティの管理、対応体制の整備 ➢ 製品に組み込まれているソフトウェアの把握、管理の徹底 ➢ サーバやクライアント、ネットワークに適切なセキュリティ対策を行う ➢ 脆弱性発見時の対応手順の作成
8	ビジネスメール詐欺による金銭被害	• 被害の予防（被害に備えた対策含む） ➢ 情報セキュリティ対策の基本（ソフトウェアの更新、セキュリティソフトの利用、パスワードの管理・認証の強化、設定の見直し、脅威・手口を知る）を実施 ➢ BEC（ビジネスメール詐欺）への認識を深める ➢ ガバナンスが機能する業務フローの構築 ➢ メールに依存しない業務フローの構築 ➢ メールの電子署名の付与（S/MIME や PGP） ➢ MARC の導入 ➢ パスワードを適切に運用する • 被害を受けた後の対応 ➢ 適切な報告／連絡／相談を行う ➢ インシデント対応体制を整備し対応する ➢ メールアカウントの設定を確認する
9	テレワーク等のニューノーマルな働き方を狙った攻撃	■個人（テレワーカー） • 被害の予防（被害に備えた対策含む） ➢ 情報セキュリティ対策の基本（ソフトウェアの更新、セキュリティソフトの利用、パスワードの管理・認証の強化、設定の見直し、脅威・手口を知る）を実施 ➢ 組織のテレワークの規則を遵守（使用する端末、ネットワーク環境、作業場所等） • 被害を受けた後の対応 ➢ 適切な報告／連絡／相談を行う ■組織（経営者層） • 組織としての体制の確立 ➢ インシデント対応体制を整備し対応する ■組織（セキュリティ担当者、システム管理者） • 被害の予防（被害に備えた対策含む）

情報セキュリティ 10 大脅威 2024[組織]		対策と対応
順位	「組織」向け脅威	
		➢ シンクライアント、VDI、VPN、ZTNA/SDP 等のセキュリティに強いテレワーク環境の採用 ➢ テレワークの規程や運用規則の整備 • 被害の早期検知 ➢ サーバやクライアント、ネットワークに適切なセキュリティ対策を行う • 被害を受けた後の対応 ➢ インシデント対応体制を整備し対応する
10	犯罪のビジネス化（アンダーグラウンドサービス）	■組織（経営者層） • 組織としての体制の確立 ➢ インシデント対応体制を整備し対応する ■組織（システム管理者） • 被害の予防 ➢ DDoS 攻撃の影響を緩和する ISP（インターネットサービスプロバイダー）や CDN（コンテンツデリバリーネットワーク）等を利用する ➢ システムの冗長化等の軽減策 • 被害の早期検知 ➢ ダークウェブの監視 • 被害を受けた後の対応 ➢ 適切な報告／連絡／相談を行う ➢ 通信制御（DDoS 攻撃元をブロック等） ➢ Web サイト停止時の代替サーバの用意と告知手段の整備 ■組織（PC 利用者） • 被害の予防 ➢ 情報リテラシー、モラルを向上させる ➢ メールの添付ファイル開封や、メールや SMS のリンク、URL のクリックを安易にしない • 被害の早期検知 ➢ 不審なログイン履歴の確認 • 被害を受けた後の対策 ➢ インシデント対応体制を整備し対応する

2.2.11 文献11：JPCERT コーディネーションセンター「インシデント報告対応レポート」

（1） 概要

JPCERT/CC（JPCERT コーディネーションセンター）では、国内外で発生するコンピューターセキュリティインシデント（インシデント）の報告を受け付けている。本レポート[22]では、特定の期間に受け付けたインシデント報告について、統計など定量的な観点と、特筆すべき事例など定性的な観点から紹介されている。

なお、本文献調査では、以下の期間のレポートを対象としている。

- 2024 年 4 月 1 日から 2024 年 6 月 30 日
- 2024 年 7 月 1 日から 2024 年 9 月 30 日
- 2024 年 10 月 1 日から 2024 年 12 月 31 日

（2） 調査結果

2024 年 4 月 1 日から 12 月 31 日におけるインシデント報告関連件数は以下のとおり。

表 2-13 インシデント報告関連件数（2024 年 4 月 1 日から 12 月 31 日）[23]

	4 月	5 月	6 月	7 月	8 月	9 月	10 月	11 月	12 月
報告件数	4,277	6,148	4,971	4,627	3,095	3,075	3,465	3,339	2,939
インシデント件数	2,280	2,398	1,926	1,821	1,779	1,547	1,889	1,713	1,959
調整件数	1,541	1,375	1,260	1,071	1,167	1,093	1,286	1,119	1,192

また、2024 年 4 月 1 日から 12 月 31 日におけるインシデント報告関連のカテゴリ別件数は以下のとおり。フィッシングサイトに分類されるインシデントが最も割合が高い。

表 2-14 インシデント報告関連のカテゴリ別件数（2024 年 4 月 1 日から 12 月 31 日）[24]

インシデント	4 月	5 月	6 月	7 月	8 月	9 月	10 月	11 月	12 月
フィッシングサイト	1,685	1,733	1,607	1,490	1,423	1,320	1,619	1,476	1,685
Web サイト改ざん	8	20	15	61	25	7	8	21	24
マルウェアサイト	28	12	5	9	10	6	11	11	14
スキャン	252	285	152	154	127	93	74	77	82
DoS/DDoS	0	1	2	0	5	4	0	3	1

[22] 一般社団法人 JPCERT コーディネーションセンター「インシデント報告対応レポート」、https://www.jpcert.or.jp/ir/report.html
[23] 出所）JPCERT/CC「インシデント報告対応レポート」を元に、株式会社三菱総合研究所が作成
[24] 出所）JPCERT/CC「インシデント報告対応レポート」を元に、株式会社三菱総合研究所が作成

制御システム関連	0	0	0	0	0	0	0	0	0
標的型攻撃	2	0	0	0	1	5	0	2	0
その他	305	347	145	107	188	112	177	123	153

2.2.12 文献12：NRI セキュアテクノロジーズ株式会社「NRI Secure Insight 2023」

（1） 概要

本文献 [25]は、企業における情報セキュリティの現状と課題を把握し、対策を提案することを目的に実態調査された調査結果である。

表 2-15 調査期間と調査対象 [26]

調査期間	2023 年 8 月から 9 月
調査対象	• 日本・アメリカ・オーストラリア 計 2,783 社 • 企業の情報システム・情報セキュリティ担当者

（2） 調査結果

「EDR 導入の普及と運用負荷」について、以下が読み取れる。

- “Emotet の流行やランサムウェアによる攻撃の増加、テレワークを前提にしたセキュリティ対策を背景に、日本の EDR 導入率が上昇している。” ソリューションの導入状況では、62%が「導入済み、検証中または検討中」との回答を示している。一方で、EDR と NDR の機能を併せ持った XDR の導入も増加している。XDR の導入によって各機能を一元的に管理し、運法負荷を下げる狙いがある。

「サプライチェーンの統制」について、以下が読み取れる。

- サプライチェーンにおける統制状況として、取引先へのセキュリティ要件の明確化や、定期的な監査の実施状況が報告されている。特に、重要な取引先に対するセキュリティ対策の要求事項の明確化や、契約への反映が進んでいる。一方で、取引先の統制状況の確認や監査の実施については、まだ十分な取り組みが行われていない企業も存在しており、今後はそういった取引先のセキュリティ対策状況を効率的に統制することが求められている。

[25] NRI セキュアテクノロジーズ株式会社「NRI Secure Insight 2023」、https://www.nri-secure.co.jp/download/insight2023-report
[26] 出所）NRI セキュアテクノロジーズ株式会社「NRI Secure Insight 2023」を元に株式会社三菱総合研究所が作成

「サプライチェーンの全体像把握」について、以下が読み取れる。

- サプライチェーンに対するセキュリティ対応における課題として、「サプライチェーンで管理すべき対象の全体像が把握できていない」が最も多く挙げられている。委託関係含めた状況把握はサプライチェーンのセキュリティ対策を行う上で非常に重要であるが、中小企業にとっては対応する予算や人材不足などもあり、対応が難しい状況である。

「SBOM の導入状況」について、以下が読み取れる。

- 2021 年 5 月の米国大統領令によって、SBOM の普及が急速に進んでいる。SBOM を活用することでサプライチェーンのリスク管理や脆弱性管理を効率的に行うことができ、今後日本でも普及が期待されている。

2.2.13 文献13：IPA「セキュリティ対策の基本と共通対策 情報セキュリティ 10 大脅威 2024 版」

（1） 概要

本文献 [27]は、情報セキュリティの基本的な対策と、複数の脅威に共通して有効な対策を解説した資料であり、中小企業等が情報セキュリティの基本的な対策を理解し、実践するための手引きとなる。

（2） 調査結果

本文献で示されている「複数の脅威に有効な対策」から、以下の点が読み取れる。

- 複数の脅威に有効な対策として示されている対策は、多岐に亘る脅威の種類に対して共通して有効であり、複数の脅威に対して同時に行えることから効率的な対策であると示されており、「効果の高いサイバーセキュリティ対策」であると考えられる。
- 共通対策を実施すれば完全な対策となるものではないと記載されているが、中小企業等が実施すべきサイバーセキュリティ対策等としては最優先とすべきものと考えられる。
- 対策項目は以下の点とされており、中小企業実態調査において企業の対策状況を評価する指標になると考えられる。
  - パスワード管理
  - 情報リテラシー、モラル
  - フィッシング対策
  - 報告／連絡／相談
  - インシデント対応体制の整備
  - IT 機器の適切なセキュリティ対策の実施
  - バックアップ運用

[27] IPA「セキュリティ対策の基本と共通対策 情報セキュリティ 10 大脅威 2024 版」（2024 年 2 月）

2.2.14 文献14：日本自動車工業会・日本自動車部品工業会「2023 年度自動車産業サプライチェーンへのサイバーセキュリティ推進活動集計データ最終結果」

（1） 概要

本文献[28]は、日本自動車工業会（自工会）及び日本自動車部品工業会（部工会）が共同で作成・公開した「自動車産業サイバーセキュリティガイドライン（V2.1）」におけるセキュリティチェックシートに基づき、自動車産業の企業によるセルフチェックの結果をとりまとめたものである（2024 年 3 月発表）。

「自動車産業サイバーセキュリティガイドライン（V2.1）」のチェックシートの評価結果算出方法は以下のとおり。

- 達成条件は全 153 項目あり、難易度によってレベル 1～3 に分けられる
- 評価はそれぞれの達成条件に対し、「対策完了（2 点）」、「該当なし（2 点）」、「対策中（1 点）」、「未実施（0 点）」の 4 つからの選択式

（2） 調査結果

「自社が行っているサイバーセキュリティ対策に関する認識」について、本ガイドラインでは、すべての企業が目標レベル 2 を標準的に目指すべきと位置付けているのに対し、目標レベル 1（最低限実装すべき項目）に留まっている企業が 659 社（約 20%）であった。この結果より、以下が読み取れる。

- 自動車業界が求める目標レベル 2 の取組を開始していない企業が多く存在する。

また、本ガイドラインでは、目標レベル 2 を取り組んでいる企業に対しては、目標レベル 1、2 のすべての項目を達成すべきと位置づけているのに対し、平均点は目標レベル 1 が約 85%、目標レベル 2 が約 79%であった。この結果より、以下が読み取れる。

- 目標レベル 2 の取組を開始している企業のうち、目標レベル 1、2 のすべての項目を達成している企業はすべてとなっていない。

「サプライチェーンセキュリティにおける評価取得のメリット等」について、2022 年度と比較し、2023 年度ではすべてのレベルにおいて平均点が向上した。この結果より、以下が読み取れる。

- ガイドラインの目的に記載されているとおり、「セキュリティリスクを考慮した対策フレームワークや業界共通の自己評価基準を明示することで、自動車産業全体のサイバーセキュリティ対策のレベルアップや対策レベルの効率的な点検を推進する」ことに寄与している。

[28] 一般社団法人日本自動車工業会、一般社団法人日本自動車部品工業会「2023 年度自動車産業サプライチェーンへのサイバーセキュリティ推進活動集計データ最終結果公表」、
https://www.jama.or.jp/operation/it/cyb_sec/cyb_sec_supply_chain.html

2.2.15 文献15：経済産業省「技術情報管理認証制度」

（1）概要

本制度は、企業の情報セキュリティ対策を、国の認定を受けた認証機関が、国によって策定された基準に基づいて審査・認証する制度である。

組織の「強み」となる情報に絞った管理方法を認証している。組織の強みとなる情報の一例は以下のとおり。

- 金型・試作品
- 製造装置、製造プロセス情報
- 研究情報
- 製造設計図・CAD
- 顧客情報・仕入先情報
- 業務マニュアル、製造／業務ノウハウ

なお、「電子情報」だけではなく、製造設備や図面など「ノウハウが詰まった完成品等の物自体」や「紙」も管理対象に含まれる。また、対象企業は、全ての法人である。（中小企業・製造業系企業が多い）

認証の取得には第三者の審査が必要となり、ハードルが高いと考える組織は、自組織内で完結する自己チェックリストによって手軽にセキュリティチェックが可能となっている。

（2）調査結果

取得するメリットの一例は以下のとおり。

- 国が主導する認証制度のため、お客さまや取引先の信頼につながる。
- 情報セキュリティの取組をマークで対外的（パンフレット、ウェブサイト、封筒、名刺等）に示せる。
- 国の一部の補助事業の審査の際に加点が受けられる。
  - ➢ 加点が受けられる例
    - ✧ ものづくり補助金の採択審査時の優遇
    - ✧ 事業再構築補助金の採択審査時の優遇
    - ✧ Go-Tech 事業採択審査時の加点と認証取得経費補助
- 日本政策金融公庫が実施する中小企業向けのIT関連設備等の導入資金や長期運転資金の融資（IT活用促進資金）を特別利率で受けられる。
- 社内の情報セキュリティ意識の向上につながる。

費用については、事業者の規模や情報セキュリティの取組状況、認証機関によるが、費用は数十万円程度必要である。（詳細は認証取得を希望する認証機関に問い合わせが必要）

評価スキーム（認証取得）については、以下のとおり。

- 認証取得を希望する事業者は、認証機関に審査を申込む。
  - 必要に応じて認証機関の指導・助言を受け、技術情報（研究成果など、技術に関する事業活動に有用な情報）のセキュリティ対策を整備、実施。
- 認証機関は、必要に応じて指導・助言しつつ、事業者の情報セキュリティ対策が基準を満たしているかを審査し、適合していれば認証。
- 申込から認証取得まで早い場合で1～2ヶ月。

評価スキーム（認証機関）については、以下のとおり。

- 認証機関の業務を行う者は、認証業務の範囲等を記載・申請し、国の認定を受けなければならない。
- 申請を受けた国は、その申請内容が「技術等情報漏えい防止措置の実施の促進に関する指針（促進指針告示）」に適合しているかどうか、また「技術等情報漏えい防止措置認証業務の実施の方法（実施方法告示）」に則した認証業務を行えるかどうかを審査し認定を行う。

制度導入促進策については、以下のとおり。

- 専門家派遣事業
  - 認証取得を検討する事業者等への支援として、情報セキュリティの専門家を無償で派遣し、守るべき情報の見極めや具体的な情報セキュリティ手法のアドバイスを行う
  - 派遣する専門家の例
    - ✧ IT コーディネータ、中小企業診断士（情報管理方法のためのアドバイスを実施）
    - ✧ 情報セキュリティ監査人（認証取得のための内部監査を実施）
- 認証制度の活用が見込まれる業界団体に対する制度の説明
  - 対象団体に対して、制度概要や業界における制度の活用可能性の説明を実施
- セミナー開催による制度の周知
  - 不特定向けのオンラインセミナーを開催し、外部弁護士による情報管理の必要性・ 経済産業省による制度概要やインセンティブの説明を実施
- メールマガジンによる制度の周知
  - 技術情報管理認証制度に係る検討会に参加する中小企業関連の団体において、メールマガジンでの配信・HP への掲載を実施

2.2.16 文献16：情報マネジメントシステム認定センター「ISMS 適合性評価制度」

（1） 概要

本制度は、情報セキュリティマネジメントシステム（ISMS）適合性評価制度は、国際的に整合性のとれた情報セキュリティマネジメントシステムに対する第三者適合性評価制度である。

ISMS の認証基準 JIS Q 27001（ISO/IEC 27001）は、ISMS 適合性評価制度において、第三者である認証機関が本制度の認証を希望する組織の適合性を評価するための基準となっている。

認証の有効期限は 3 年であり、初回審査の後も年に 1 回以上の中間的な審査（サーベイランス審査）がある。なお、3 年ごとに認証の有効期限を更新するための全面的な審査（再認証審査）が必要となっている。

認証範囲は、取得企業の必要に応じて定めることが可能であり、必ずしも全社を範囲とする必要はない。

また、ISMS を取得した組織を対象とした、特定の分野/技術の認証がある。具体的には以下のとおり。

- ISMS クラウドセキュリティ認証
  クラウドサービス固有の管理策（ISO/IEC 27017）が 適切に導入、実施されていることを認証
- ISMS-PIMS 認証
  ISO/IEC 27701 に基づくプライバシー情報マネジメントシステム（PIMS）が適切に導入、実施されていることを認証

（2） 調査結果

取得するメリットの一例は以下のとおり。

- 取得組織内に対する効果
  - 社員の情報セキュリティに関する意識向上につながる
  - 組織の情報セキュリティ管理体制、情報セキュリティ対策を強化できる
  - 経営者の情報セキュリティに対する関与が深まる
  - 組織の情報セキュリティレベルを向上し、期待レベルを維持できる
- 対外的な効果
  - 顧客からの信頼確保につながる
  - 企業イメージの向上につながる

費用については、主に審査費用、更新審査費用に分けられる。また、費用は、認証機関によって異なる。さらには、同じ認証機関であっても、申請した組織の従業員人数、拠点数、業種等の規模によっても異なる。

評価スキームは下図のとおり。

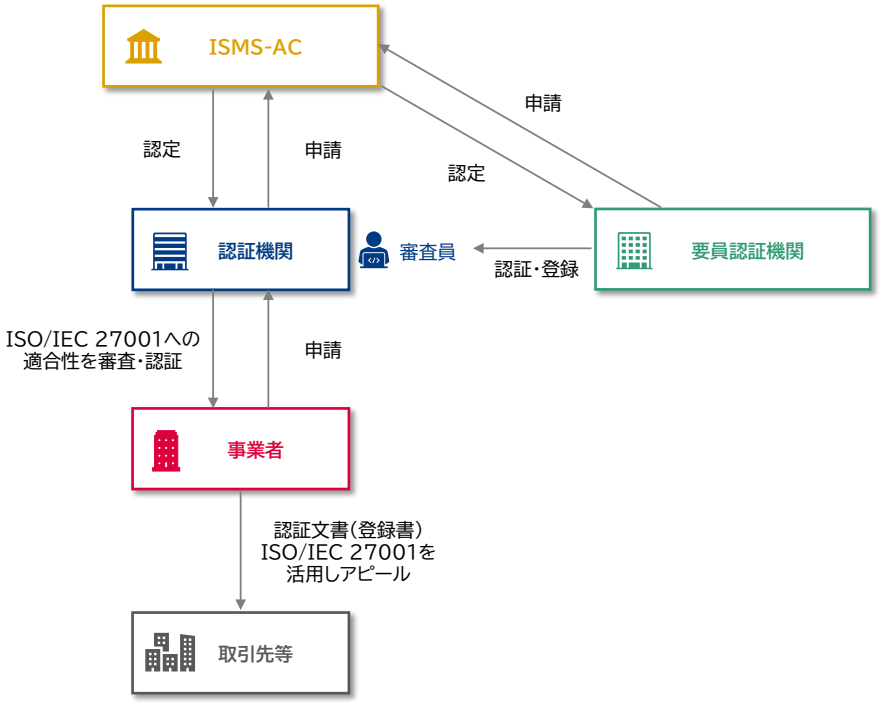

図 2-1 「ISMS 適合性評価制度」の評価スキーム

2.2.17 文献17：日本情報経済社会推進協会「プライバシーマーク制度」

(1) 概要

本制度は、日本産業規格「JIS Q 15001 個人情報保護マネジメントシステム－要求事項」に準拠した「プライバシーマークにおける個人情報保護マネジメントシステム構築・運用指針」に基づいている。個人情報について適切な保護措置を講ずる体制を整備している事業者等を評価して、その旨を示すプライバシーマークを付与し、事業活動に関してプライバシーマークの使用を認める制度である。

プライバシーマーク付与の対象は、国内に活動拠点を持つ事業者である。また、プライバシーマーク付与は、法人単位（医療法人等、および学校法人等については一部例外がある）である。

本制度を取得するためには、少なくとも以下の条件を満たしている事業者であって、実際の事業活動の場で個人情報の保護を推進している必要がある。

- JIS Q 15001「個人情報保護マネジメントシステム－要求事項」に基づいた「プライバシーマークにおける個人情報保護マネジメントシステム構築・運用指針」に即し、個人情報保護マネジメントシステム（PMS：Personal information protection Management System）を定めていること。
- PMS に基づき実施可能な体制が整備されて個人情報の適切な取扱いが行われていること。
- 「プライバシーマーク付与に関する規約（PMK500）」に定める欠格事項に該当しない事業者であること。

プライバシーマーク付与の有効期間は、2 年間である。ただし、以降は、2 年ごとに更新を行うことが

可能である。

（2）調査結果

取得するメリットの一例は以下のとおり。

- 取得企業
  - 顧客からの信頼度アップ
  - ビジネスチャンスの拡大
  - 社員の個人情報保護意識の向上
- 取得企業のサービスや製品を利用する消費者
  - 個人情報をあずけても安心
  - 個人情報を適切に取り扱っていることがひとめでわかる
  - 個人情報について安心・安全な社会へ

費用については、新規/更新、事業者規模（小/中/大）によって費用の区分は異なる。事業者規模の区分は、登記された資本金の額または出資の総額、従業者数、業種を基準に判定される。

申請時、審査時、登録時それぞれで費用が設定されている。

- 申請料：P マーク付与適格性審査の申請料
  ※審査の結果に係わらず必要
- 審査料：P マーク付与適格性審査の審査料
- 付与登録料：P マーク付与登録料（有効期間（2 年間）分）

評価スキームは下図のとおり。

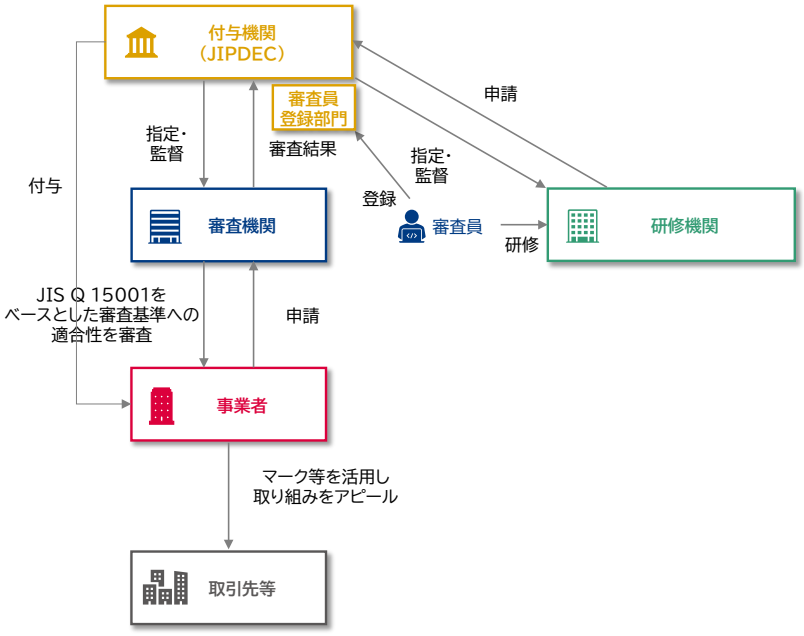

図 2-2 「P マーク制度」の評価スキーム

2.2.18 文献18：英国「Cyber Essentials/Cyber Essentials Plus」

（1） 概要

Cyber Essentials[29]は、英国政府が英国内のあらゆる規模の組織にサイバーセキュリティの最低限の基準を定めたものである。最も一般的なインターネットベースのサイバーセキュリティの脅威を防ぐために設計された 5 つの技術管理に準拠している。

Cyber Essentials 認証は、組織が最も重要なサイバーセキュリティコントロールを実装し、自らを保護していることを証明する。専門家チームが定期的にこのスキームをレビューし、常に進化する脅威の下、スキームが効果的であることを確認する。

Cyber Essentials 認証には、年間売上高が 2,000 万ポンド未満の英国の組織に対する自動サイバー賠償責任保険が含まれる。

全ての自己評価の質問は、事前に無料でダウンロード可能。Cyber Essentials に合格すると、システムの実践的な監査が含まれる Cyber Essentials Plus に申し込むことができる。

表 2-16 Cyber Essentials/Cyber Essentials Plus の評価概要 [30]

	評価の概要
Cyber Essentials	• 自己評価アンケートの形式で評価。組織は、評価の範囲、従業員、デバイス、作業場所に関する一連の質問に回答する。 • ユーザーアクセス制御、安全な構成、セキュリティ更新管理、ファイアウォールとルーター、マルウェア保護を含む 5 つのコア制御に関する質問にも回答する。 • 回答は取締役会メンバーまたは同等の人物によって承認され、その後、独立した評価者によって採点される。
Cyber Essentials Plus	• Cyber Essentials の検証済み自己評価アンケートが前提となる。 • 同じ技術要件に基づくが、制御が適切に行われていることを確認するための IT システムの技術監査が含まれる。これにより、スキームに準拠していることがより確実となる。 • 監査は、代表的なユーザーデバイスのセット、全てのインターネットゲートウェイ、及びインターネットにアクセス可能なサービスを備えたすべてのサーバを対象とする。

（2） 調査結果

取得するメリットの一例は以下のとおり。

- Cyber Essentials 認証のメリット

[29] National Cyber Security Centre「Cyber Essentials」、https://www.ncsc.gov.uk/cyberessentials/
[30] 出所）IPA 調査資料を元に株式会社三菱総合研究所が作成

- サイバーセキュリティが組織にとって優先事項であることを顧客に証明することができる。
- 毎年、フレームワークに照らしてシステムを評価すると、新たなサイバーセキュリティリスクに先手を打つことができる。
- 認証取得により、サプライチェーンのセキュリティに対応する契約増につながる。

• 支援の仕組み
- 技術的な IT のバックグラウンドがない場合や、企業構造が複雑な場合は、Cyber Essentials の自己評価の質問の一部を理解するのが難しい場合がある。その場合、サイバーアドバイザーが支援可能である。
- サイバーアドバーザー派、国立サイバー セキュリティセンター保証サービスプロバイダーに勤務し、中小企業に信頼性が高くコスト効率の高いサイバーセキュリティのアドバイスと実践的なサポートを提供する。アドバイザーは、技術的な知識を活用し、個々の企業の特定のニーズを念頭に置いた実践的なサポートを提供し、推奨されるアクションの実行を支援する。
- Cyber Essentials 評価者は、認証機関に勤務する。評価者は、組織が Cyber Essentials 認証に必要な基準を満たしているかどうかを評価し、その認証を発行できるように、IASME によってトレーニングとライセンスを受けている。また、アセスメントの質問を理解し、それが企業にどのように関係するかについてサポートすることもできる。

費用については、以下のとおり。

表 2-17 Cyber Essentials/Cyber Essentials Plus の費用 [31]

	従業員数 0～9 名	従業員数 10～49 名	従業員数 50～249 名	従業員数 250 名以上
Cyber Essentials	420$	570$	650$	780$
Cyber Essentials Plus	ネットワークの規模と複雑さに応じて価格が決定			

評価スキームについては、Cyber Essentials は DSIT が生産を管轄担当し、NCSC により運用責任・管理を担い、IASME とのパートナーシップ契約により、運用を推進している。

[31] 出所）IPA 調査資料を元に株式会社三菱総合研究所が作成

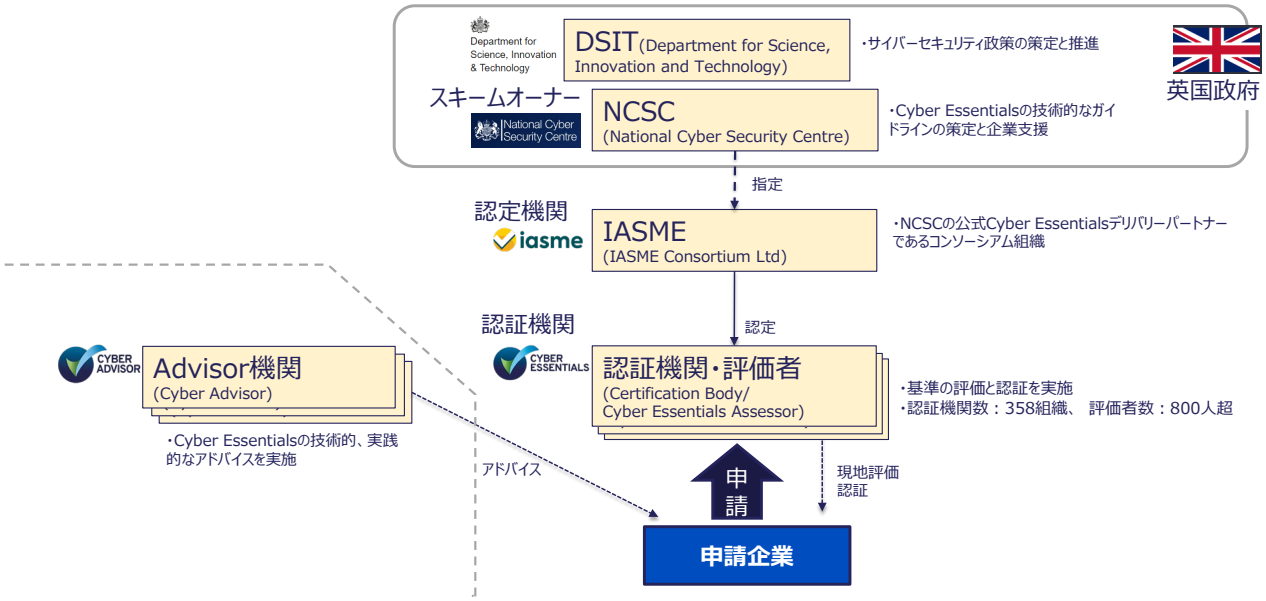

図 2-3 英国「Cyber Essentials/Cyber Essentials Plus」の評価スキーム [32]

2.2.19 文献19：米国「CMMC」

（1） 概要

サイバーセキュリティは国防総省（DoD）にとって最優先事項である。防衛産業基盤（DIB）は、ますます頻繁かつ複雑なサイバー攻撃に直面している。DIB のサイバーセキュリティを強化し、DOD の情報をより適切に保護するために、DOD は、既存の DOD のサイバーセキュリティ要件を評価するサイバーセキュリティ成熟度モデル認証（CMMC）プログラム [33]を開発した。

CMMC プログラムは DIB に関する既存の情報セキュリティ要件と一致している。このプログラムは、DOD が請負業者や下請け業者と共有する機密扱いでない機密情報の保護を強化するように設計されている。このプログラムにより、DOD は、請負業者や下請け業者が管理されている機密扱いでない情報を処理する非連邦システムのサイバーセキュリティ要件を満たしていることを確認できる。

CMMC プログラムの主な特徴は以下のとおり。

- 階層モデル: CMMC では、機密扱いされていない国防総省の機密情報を委託された企業に対し、情報の種類と機密性に応じて、段階的に高度なレベルのサイバーセキュリティ標準を実装することを義務付けている。このプログラムでは、下請け業者に流される情報の保護を要求するプロセスも概説している。
- 評価要件: CMMC 評価により、DOD は DIB による既存のサイバーセキュリティ標準の実装を検証できる。

[32] IPA 調査資料より
[33] U.S. Department of Defense「CMMC」、https://dodcio.defense.gov/CMMC/

- 契約による実装: 機密扱いではない機密扱いの国防総省情報を扱う DOD の請負業者と下請業者は、契約締結の条件として特定の CMMC レベルを達成する必要がある。

CMMC モデルは、契約履行中に防衛請負業者および下請業者と共有される連邦契約情報（FCI）及び管理された非機密情報（CUI）を保護するように設計されている。

- 連邦契約情報（FCI）: 連邦調達規則（FAR）のセクション 4.1901 で定義されているように、FCI とは政府向けの製品またはサービスを開発または提供する契約に基づいて政府によって提供されるか政府のために生成される、一般公開を意図しない情報であり、政府が一般に提供する情報（公開 Web サイト上の情報など）や、支払い処理に必要な情報などの単純な取引情報は除く。
- 管理された非機密情報（CUI）: Title 32 CFR 2002.4(h) に概説されているように、CUI とは「政府が作成または保有する情報、または政府に代わって組織が作成または保有する情報で、法律、規制、または政府全体のポリシーにより、機関が保護または配布管理を使用して処理することが要求または許可されている情報」である。特定の CUI カテゴリとサブカテゴリの詳細については、DoD CUI レジストリの Web サイトを参照のこと。

CMMC プログラムは、既存の規制とガイドラインのセキュリティ要件をそれぞれ組み込んだ 3 つのレベルで評価を提供する。

- レベル 1: FCI の基本的な保護
- レベル 2: CUI の広範な保護
- レベル 3: 高度な持続的脅威に対する CUI の高度な保護

（2）調査結果

機密扱いではない機密扱いの DOD 情報を扱う請負業者と下請業者は、契約締結の条件として特定の CMMC レベルを達成する必要がある。

費用については、下表のとおり。

表 2-18 費用一覧 [34]

項目	レベル 1 自己評価	レベル 2 自己評価	レベル 2 第三者認証	レベル 3 DoD 認証
費用	• DoD 報告における認証に要する費用の推計は以下の通り。ただし企業により差異は大きい。 費用には要件の実装費用、保守費用は含まない。			

[34] 出所）IPA 調査資料を元に株式会社三菱総合研究所が作成

項目	レベル 1 自己評価	レベル 2 自己評価	レベル 2 第三者認証	レベル 3 DoD 認証
	• Level3 取得の実装には、別途$2,700,000(420,000 千円)が必要と推計されている。			
① 評価の計画と準備	$1,803 (約 280,000 円)	$14,426 (約 2,240,000 円)	$20,699 (約 3,210,000 円)	$1,905 (約 300,000 円)
② 評価の実施	$2,705 (約 420,000 円)	$15,542 (約 2,410,000 円)	$76,743 (約 11,900,000 円)	$1,524 (約 236,000 円)
③ 評価結果の報告	$909 (約 140,000 円)	$2,851 (約 442,000 円)	$2,851 (約 442,000 円)	$1,876 (約 290,000 円)
④ 確認	$560 (約 87,000 円)	$4,377 (約 680,000 円)	$4,377 (約 680,000 円)	$5,628 (約 872,000 円)
⑤ 行動計画の作成	$0	$0	$0	$1,869 (約 290,000 円)
合計	$5,977 (936 千円)	$37,196 (5,765 千円)	$104,670 (16,220 千円)	$12,802 (1,980 千円)

評価スキームについては、スキームオーナーである DOD が認定機関である CyberAB と契約し、認証機関である C3PAOs を認定。評価者は CAICO により認定される。

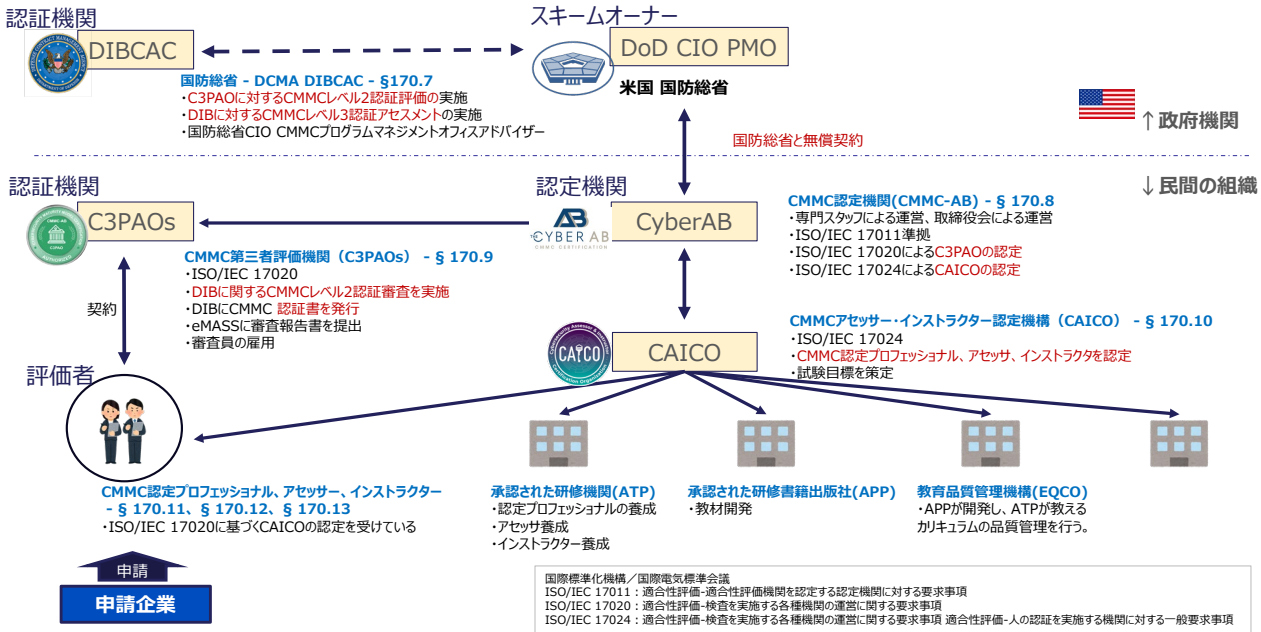

図 2-4 米国「CMMC」の評価スキーム [35]

2.2.20 文献20：オーストラリア「Essential Eight」

(1) 概要

Essential Eight[36]は、オーストラリア通信電子局（ASD）が定義している「サイバーセキュリティインシデントを緩和する 8 つの主要な対策」である。オーストラリア通信電子局（ASD）が公開しているサイバーセキュリティインシデントを緩和する戦略は、企業が自社のコンピューターのセキュリティをさらに強化するために優先して実行すべき実用的な対策のリストである。本ガイダンスには、リスクプロファイルや最も懸念している脅威に基づいて各企業が自社の状況に合わせてカスタマイズできるというメリットがある。

オーストラリア通信電子局（ASD）が公開している「サイバーセキュリティインシデントを緩和する 8 つの主要な対策」を効果的に導入することは、サイバーセキュリティの基準を満たすことに役立つ。サイバーセキュリティの基準とは、WannaCry や NotPetya など最新の攻撃の成功を阻止できる水準を指している。

「サイバーセキュリティインシデントを緩和する 8 つの主要な対策」は 2 つのセクションに分類できる。

- マルウェアの実行を阻止するための 4 つの対策
- インシデントの範囲を制限しデータを復元するための 4 つの対策

[35] IPA 調査資料より
[36] The Australian Signals Directorate's Australian Cyber Security Centre「Essential Eight」、https://www.cyber.gov.au/resources-business-and-government/essential-cybersecurity/essential-eight

（2）調査結果

取得メリットの一例は以下のとおり。

- Essential Eight を積極的に実装すると、大規模なサイバーセキュリティインシデントに対応するよりも、時間、費用、労力の面でコスト効率が高くなる。
- 一般的に、成熟度レベル 1 は中小企業、成熟度レベル 2 は大企業、成熟度レベル 3 は重要なインフラストラクチャプロバイダーや脅威の高い環境で活動するその他の組織に適している。
- Essential Eight の要件を実装する場合、組織は、自社の環境に適した目標成熟度レベルを特定し、計画を立てる必要がある。その後、組織は、その目標が達成されるまで、各成熟度レベルを段階的に実装する必要がある。
- トレーニング：
  - ASD は Essential Eight 評価コースを開発し、TAFEcyber と提携してオーストラリア全土のサイバーセキュリティ専門家にこのコースを提供している。
  - Essential Eight アセスメントコースは、専門知識、知識、実践的な技術トレーニングを組み合わせた対面式の 3 日間のコースである。

2.3 文献調査サマリ

調査観点ごとに、文献調査から得られた概要を示す。

a. 中小企業の実態（経営状況）と支払意思

中小企業や経営者に対するセキュリティ対策の実態に関する報告書を調査した結果、サプライチェーンセキュリティへの対策、経営課題におけるサイバーリスクへの対応の優先順位等の実態が得られた。

b. 中小企業が被るサイバーインシデント被害と被害額の動向

サイバーインシデント被害に関する報告書を調査した結果、中小企業が被るサイバーインシデント被害と被害額、グローバルでのサイバーインシデント被害等の動向が得られた。

c. 自社が行っているサイバーセキュリティ対策に関する認識

サイバーセキュリティのリスクの意識や対策の実態に関する報告書を調査した結果、企業規模別（中小企業と大企業）で行っているサイバーセキュリティ対策等の動向が得られた。

d. 中小企業向けサイバーセキュリティ対策ソリューションの動向とコスト感

国内の情報セキュリティ市場に関する報告書を調査した結果、情報セキュリティ市場規模、情報セキュリティ対策への投資額等の動向が得られた。

e. 業界に限らず中小企業等が実施すべきサイバーセキュリティ対策等の観点

国内の情報セキュリティの事案や事案から導出した脅威に関する報告書を調査した結果、企業への影響が大きいと考えられる脅威と脅威に対するセキュリティ対策が得られた。

f. サプライチェーンの一員としてセキュリティ対策の必要性に関する認識

サプライチェーンにおける企業のセキュリティ対策に関する報告書を調査した結果、取引先へのセキュリティ要件の明確化や、定期的な監査の実施状況が得られた。また、サプライチェーンのセキュリティ対応における課題が得られた。

g. サプライチェーンセキュリティにおける評価取得のメリット等の観点

国内外問わず、サプライチェーンセキュリティにおける評価制度を調査した結果、企業が評価制度を取得するメリット、費用感等が得られた。

3. アンケート調査

「2021 年度調査」からの経年変化の把握、中小企業等におけるサイバーセキュリティ対策の実態及び課題等についての分析・整理、中小企業等における規模・業種等に応じた効果の高いサイバーセキュリティ対策の分析・整理、SECURITY ACTION 一つ星及び二つ星に求められる基準についての分析・調査、SECURITY ACTION 宣言及びサイバーセキュリティお助け隊サービスを導入する中小企業が、中小企業全体の割合に対して低い水準となっている理由の分析・調査を目的として、アンケート調査を行った。

アンケート調査の対象者は、中小企業等における経営層を第一とし、IT や情報セキュリティの社内担当者、一般社員による代理回答も可としたが、回答者の役割（経営層、IT や情報セキュリティの社内担当者、一般社員の別）を含めてデータを収集した。

3.1 調査概要

（1） 実施概要

実施概要は、下表の通りである。調査項目としては、中小企業等における情報セキュリティ対策の実態及び課題の把握および SECURITY ACTION 一つ星及び二つ星に求められる基準についての分析・調査、SECURITY ACTION 宣言及びサイバーセキュリティお助け隊サービスを導入する中小企業が、中小企業全体の割合に対して低い水準となっている理由の分析・調査を行う目的で、以下の分析が行えるように設定した。

- サイバーセキュリティ対策への取組状況
- サイバーセキュリティ対策実施への経営層の関与の状況
- サイバーセキュリティに関する被害の状況
- サプライチェーンにおけるサイバーセキュリティの状況
- SECURITY ACTION の認知度・宣言状況・宣言の効果・宣言の理由／宣言しない理由
- サイバーセキュリティお助け隊サービスの利用状況、利用の効果、利用の理由／利用しない理由

表 3-1 アンケート調査実施概要

調査対象	一般企業の経営層及び情報システム／情報セキュリティの担当マネージャ
調査期間	2024 年 10 月 25 日（金）～11 月6日（水）
調査項目数	概要設問 8 問、本設問 104 問 ※概要設問（業種、回答者の役職等）においてスクリーニングを実施し、有効回答を得られると判断した回答者が本設問へ進む
調査項目	1. 回答者の属性 2. 回答企業の属性 3. IT の導入状況 4. 情報セキュリティに関する意識・状況 5. 情報セキュリティ教育の状況

	6. サイバーインシデント被害の状況 7. 取引先を含む情報セキュリティ対策 8. 「SECURITY ACTION」の宣言状況 9. 「サイバーセキュリティお助け隊サービス」の導入状況 10. 情報セキュリティ対策の状況（25項目）
調査手法	・ Web アンケーケートモニタ調査（NTT コム リサーチ） ・ Web モニタに対してアンケートを実施
有効回答数	4,191件

数値については、小数点第2位を四捨五入され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。

有効回答を得るにあたり、全ての回答サンプルから、以下の観点でスクリーニングおよびデータクリーニングを実施した。

- 中小企業庁の定義に基づく中小企業および小規模企業者に所属している回答者に絞込み。
- 自社の情報セキュリティ対策状況を把握、情報セキュリティ対策投資の判断に関与している回答者に絞込み。
- 短時間での回答、無意味な文字の羅列、質問とは無関係な内容の回答、数値入力のはずれ値がある回答サンプルの排除。
- 同一企業の回答者が違う回答結果となる可能性が少ない設問（業種、従業員数、資本金、本社所在地）の回答結果をもとにした同一企業からの複数回答の排除。

3.2 調査結果(単純集計)

設問文における SC はアンケート回答者(企業)の属性に関する概要設問、Q はアンケートの本設問を表す。また、(SA)は単一回答、(MA)は複数回答を表す。

3.2.1 回答者の属性

アンケート回答者の属性に関する設問と調査結果を記載する。

a. 回答者の役職・担当

SC4. あなたがお勤め・経営されている企業において、あなたご自身の役職・担当業務をお教えください。(SA)

経営者(2,720 件)が 64.9%で最も多く、次いで役員(827 件)が 19.7%であり、回答者全体の約 9 割は経営層である。

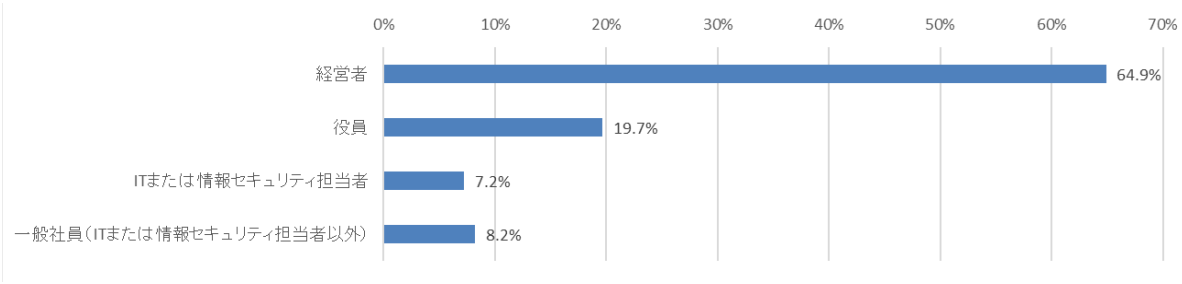

図 3-1 回答者の役職・担当(n=4191)

SC5. あなたがお勤め・経営されている企業において、あなたは自社のサイバーセキュリティ対策の投資にどのように関与しているか教えてください。(SA)

経営者として意思決定する立場(2,852 件)が 68.1%で最も多く、次いで経営層に提案・助言・判断を支援する立場(536 件)が 12.8%であり、これらの回答者で全体の約 8 割を占めている。

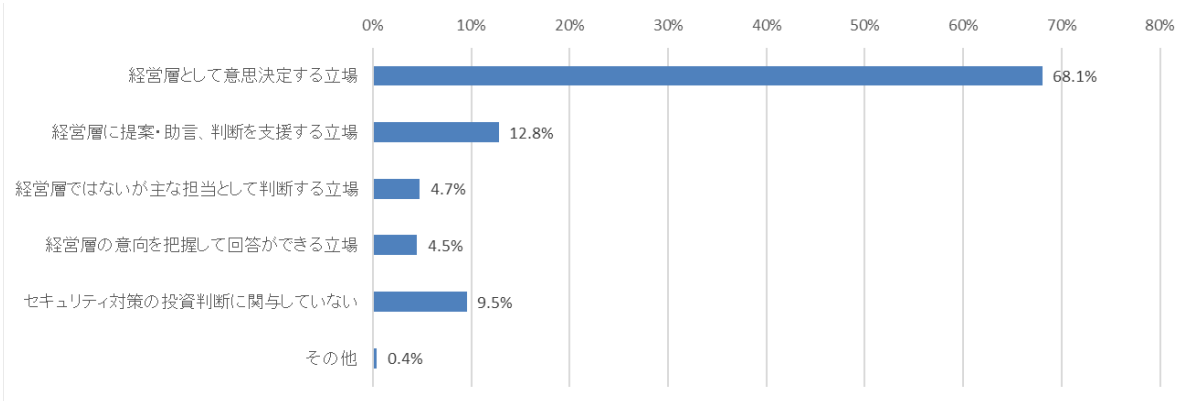

図 3-2 自社のサイバーセキュリティ対策の投資への関与(n=4191)

3.2.2 回答企業の属性

アンケート回答者が勤務または経営する企業の属性に関する設問と回答結果を記載する。

a. 業種

SC1. あなたがお勤め・経営されている企業の業種を教えてください。（SA）

回答者の業種は建設業（566 件）が 13.5%で最も多く、その他のサービス業（553 件）が 13.2%、製造業（504 件）が 12.0%、不動産業・物品賃貸業（410 件）が 9.8%、小売業（327 件）が 8.9%、情報通信業（317 件）が 7.6%と続いており、これらの業種の合計で全体の約 7 割を占めている。

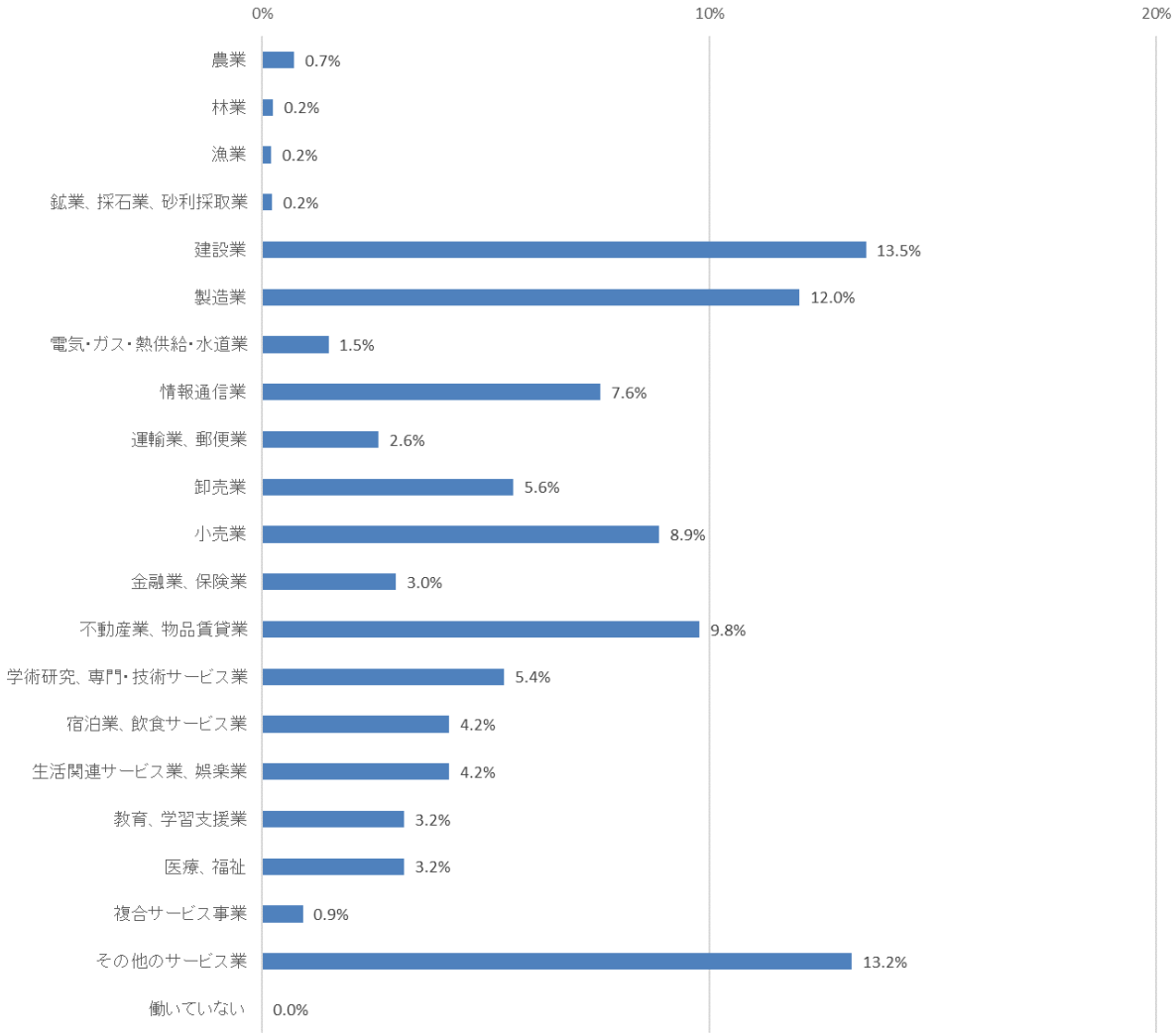

図 3-3 業種(n=4191)

b. 所在地

Q1. 貴社の所在地（本社所在地）を教えてください。（SA）

東京都（820 件） 19.6%、大阪府（400 件）9.5%、愛知県（276 件）6.6%、神奈川県（243 件）5.8%、北海道（194 件）4.6%、兵庫（176 件）4.2%、埼玉県（155 件）3.7%、千葉県（149 件）3.6%、福岡県（147 件）3.5%という順である。

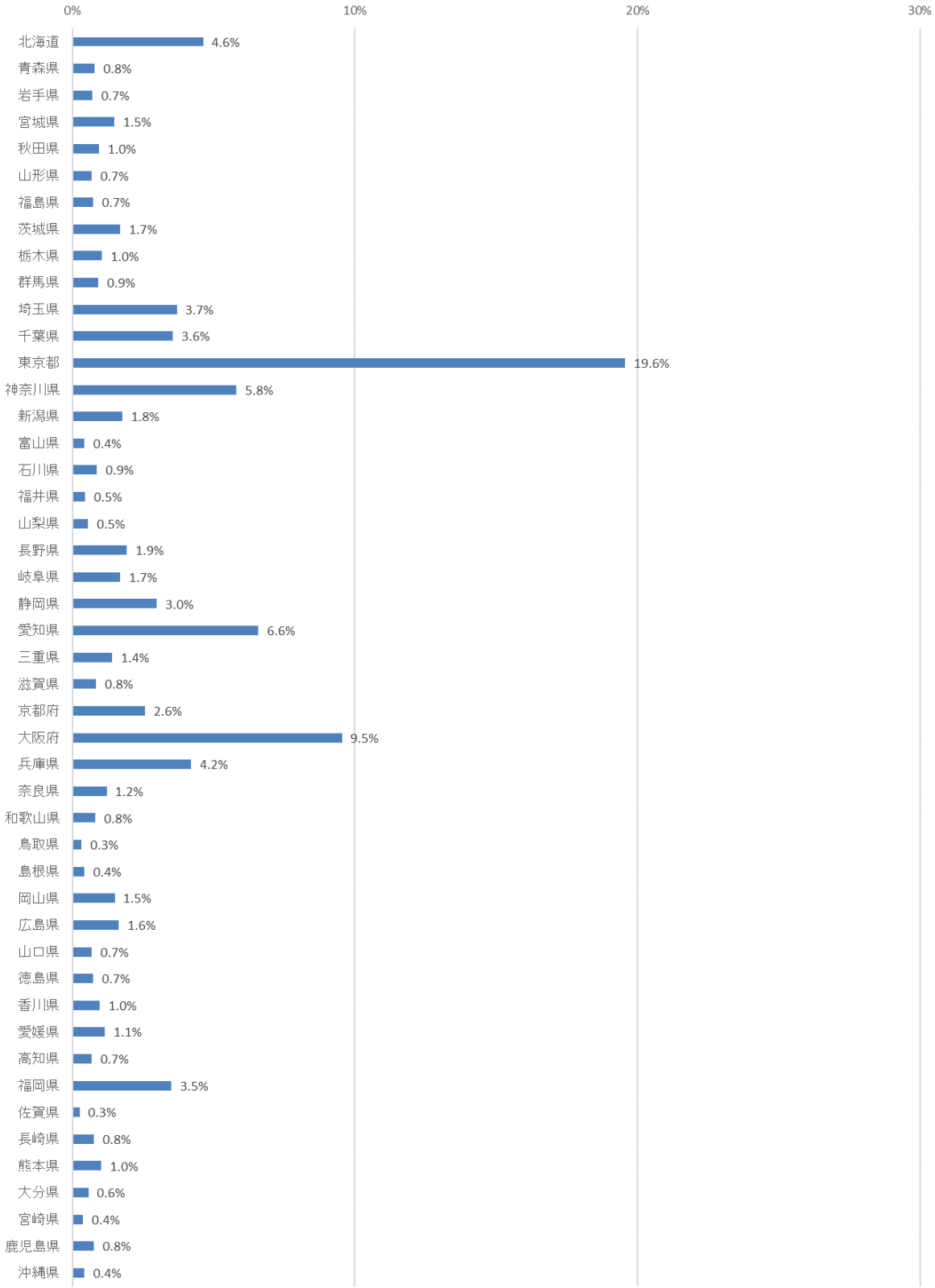

図 3-4 所在地(n=4191)

c. 従業員規模

SC2. あなたがお勤め・経営されている企業の総従業員数を教えてください。（SA）

従業員数は 5 名以下(2,442 件)が 58.2%と半数以上を占め、次いで 6～20 名以下(770 件)が 18.4%、21～50 名以下(410 件)の 9.8%と続いており、これらの合計で全体の約 9 割を占めている。

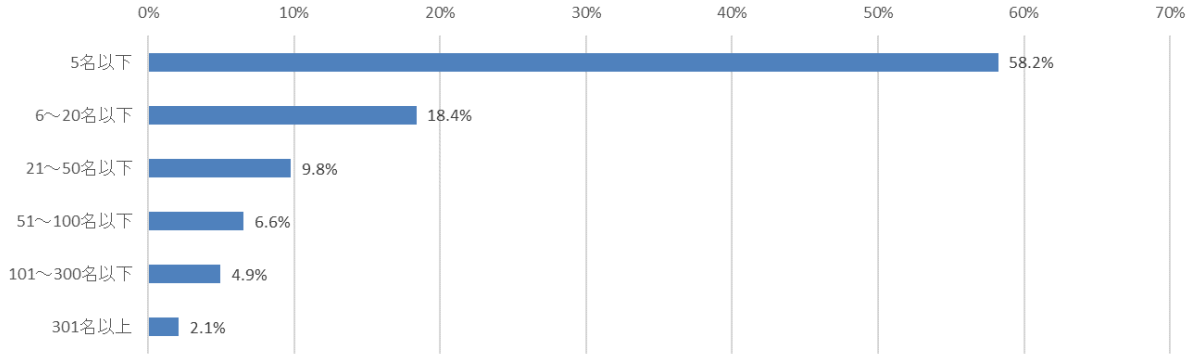

図 3-5 従業員規模(n=4191)

d. 直近会計年度の資本金

SC3. 貴社の資本金について教えてください。(SA)

資本金は,000 万円以下(2,478 件)が 59.1%と 6 割近くを占め、次いで 1,000 万円超～3,000 万円以下(671 件)が 16.5%である。さらに、3,000 万円超～5,000 万円以下(282 件)6.7%、5,000 万円超～1 億円以下(272 件)6.5%とほぼ並んでいる。これらの合計で全体の 9 割近くを占めている。

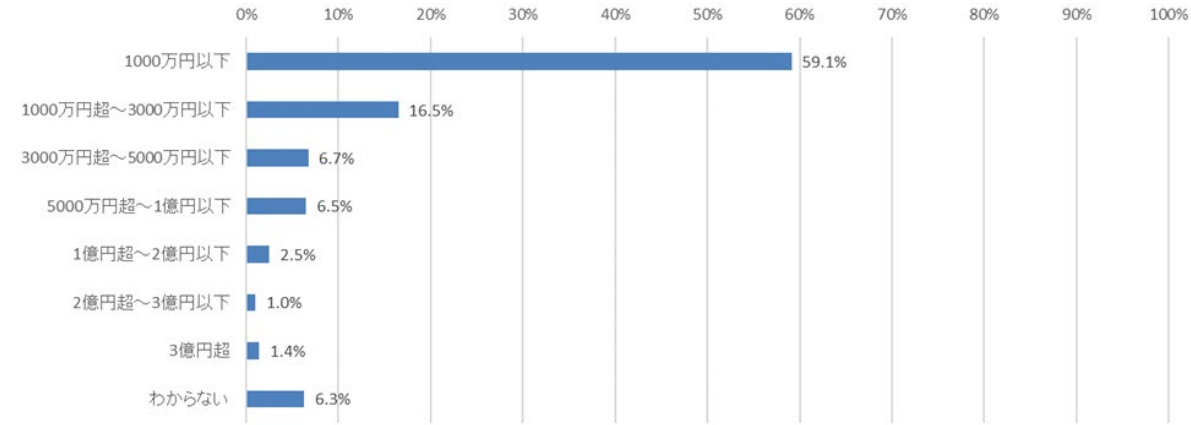

図 3-6 資本金(n=4191)

e. 直近会計年度の売上高

Q2. 貴社の総売上高(単体)について教えください。(SA)

総売上高は 1,000 万円以下が 31.9%と最も多い。次いで、3億円超が 18.2%、1,000 万円超～3,000 万円以下が 16.1%となっている。

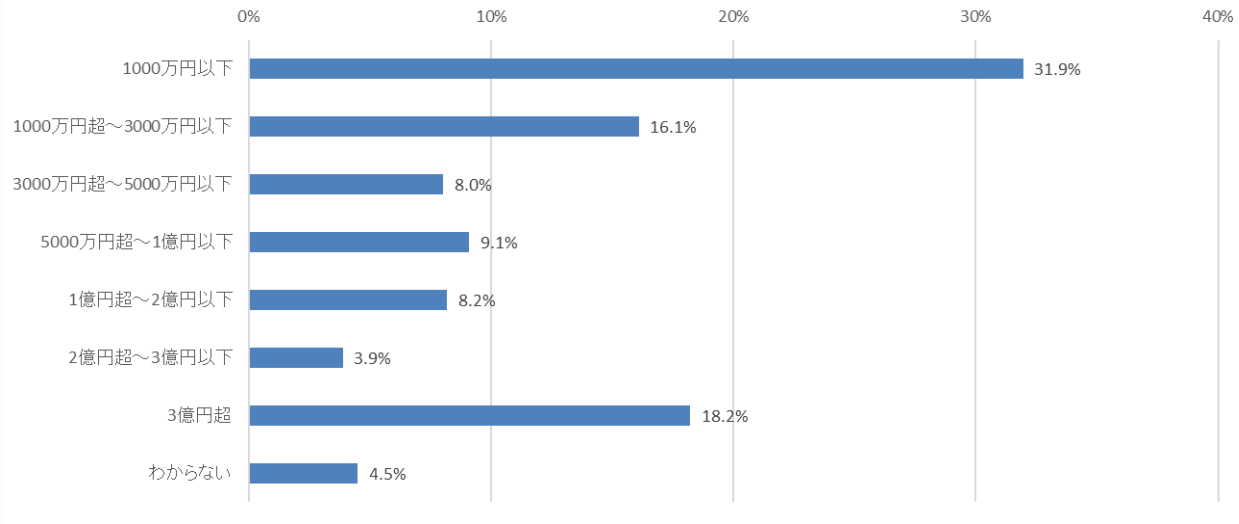

図 3-7 売上高(n=4191)

f. 業界団体への加入状況

Q3. 貴社は業界団体(貴社の業種に関連する業界団体、商工会議所、商工会・中小企業団体中央会等)に加入していますか。(SA)

業界団体に加入している企業(872 件)は 20.8%にとどまっている。

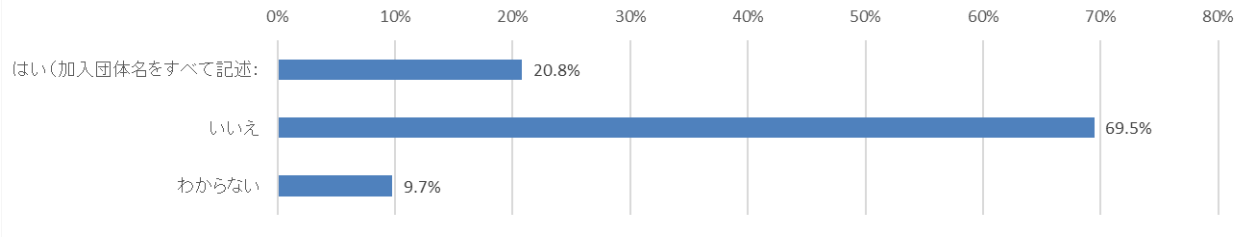

図 3-8 業界団体への加入状況(n=4191)

g. グループ会社

Q4. 貴社がグループ会社の場合、親会社のセキュリティ方針に沿った対応を行っていますか。(SA)

グループ会社(回答が「グループ会社ではない」以外)の場合、親会社が決めている(307 件)7.3%と自社でも一部のセキュリティ方針を決めている(340 件)8.1%は同程度の割合である。

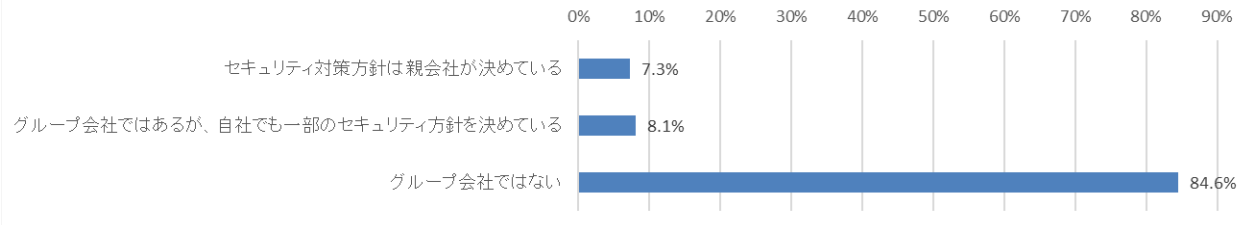

図 3-9 グループ会社(n=4191)

3.2.3 IT の導入状況

回答企業の IT の利用・導入状況について調査結果を記載する。

a. 利用・導入しているサービスやシステム

Q5. 貴社では経営資源の確保や業務の効率化に IT を活用されていますか。情報セキュリティ対策サービス以外で利用・導入されているサービスやシステムについて教えてください。 あてはまるものを下記よりすべてお選びください。（MA）

電子メール(フリーメール・汎用ドメイン等)(1941 件)が 46.3%と最も高くなっている。次いで、電子メール(独自ドメイン)(1520 件)が 36.3%と、全体の約8割が電子メールを導入している。また Web サイト(1,383 件)も 33.0%と全体の 1/3 が導入している。社内システムに関しては、会計システム・アプリケーション(1,263 件)が 30.1%、オンライン会議システム(777 件)が 18.5%、給与システム・アプリケーション(1,263 件)が 17.6%と社内の IT 化は全体として十分ではない。さらに、特に活用していない(954 件)も 22.8%と全体の約 1/5 に上っている。

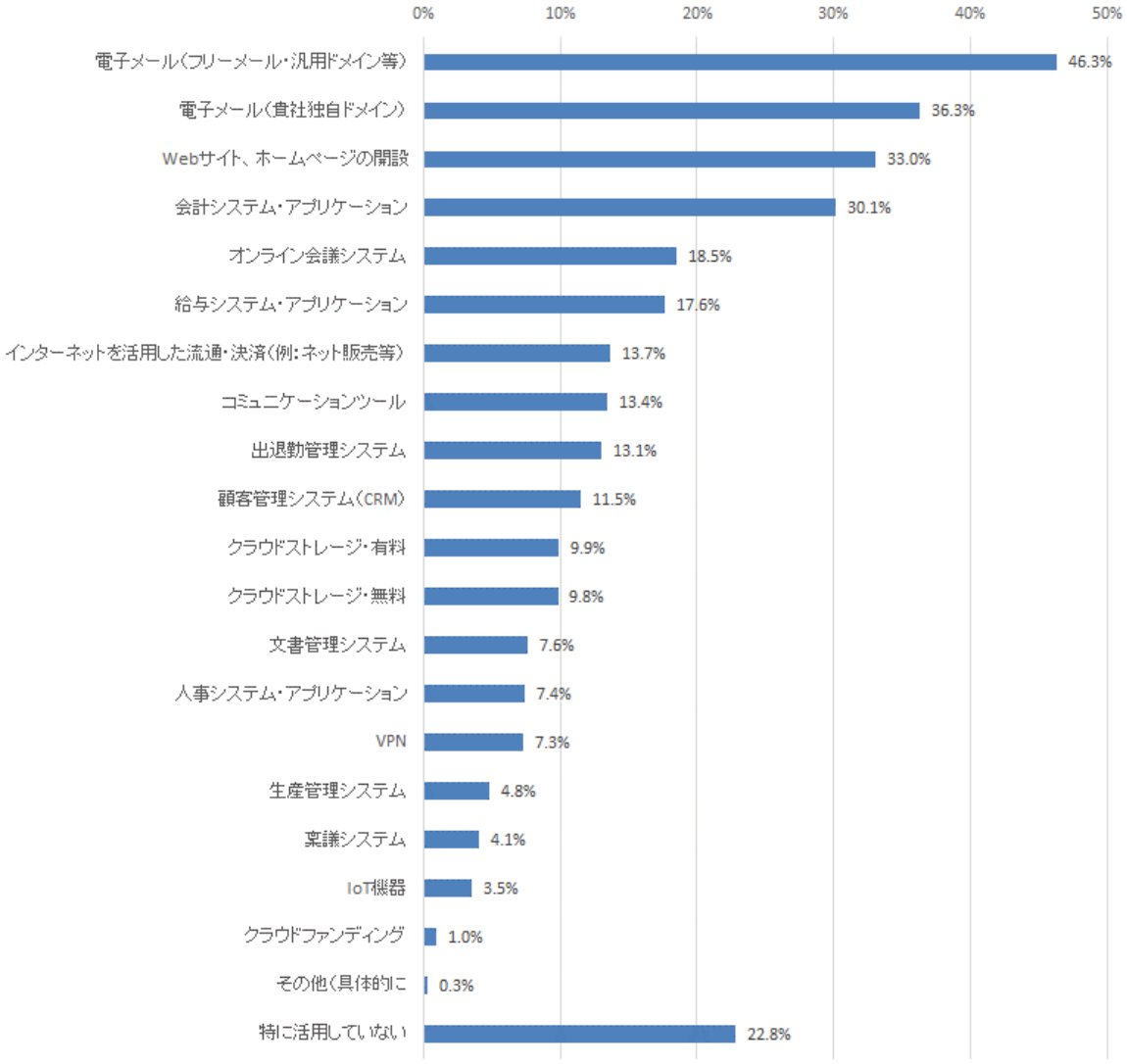

図 3-10 情報セキュリティ対策サービス以外で利用・導入されているサービスやシステム(n=4191)

3.2.4 情報セキュリティに関する意識・状況

回答企業の情報セキュリティに関する意識・状況として、IT 投資額や情報セキュリティ対策を必要としたきっかけなどに関する設問と回答結果を記載する。

a. 直近過去3期の IT 投資額

Q6-1. 貴社における、直近過去 3 期の IT 投資額(情報セキュリティ対策投資額を含む)と、情報セキュリティ対策投資額(IT 機器や社員への教育等も含む)の概算について教えてください。(SA)
-IT 投資額(情報セキュリティ対策投資額を含む)

投資をしていないという回答が最も多く 59.7%と約 6 割に上る。投資をしている場合でも投資額が増えるほど件数は少なくなり、最も多いものが 100 万円未満で 20.7%という状況である。

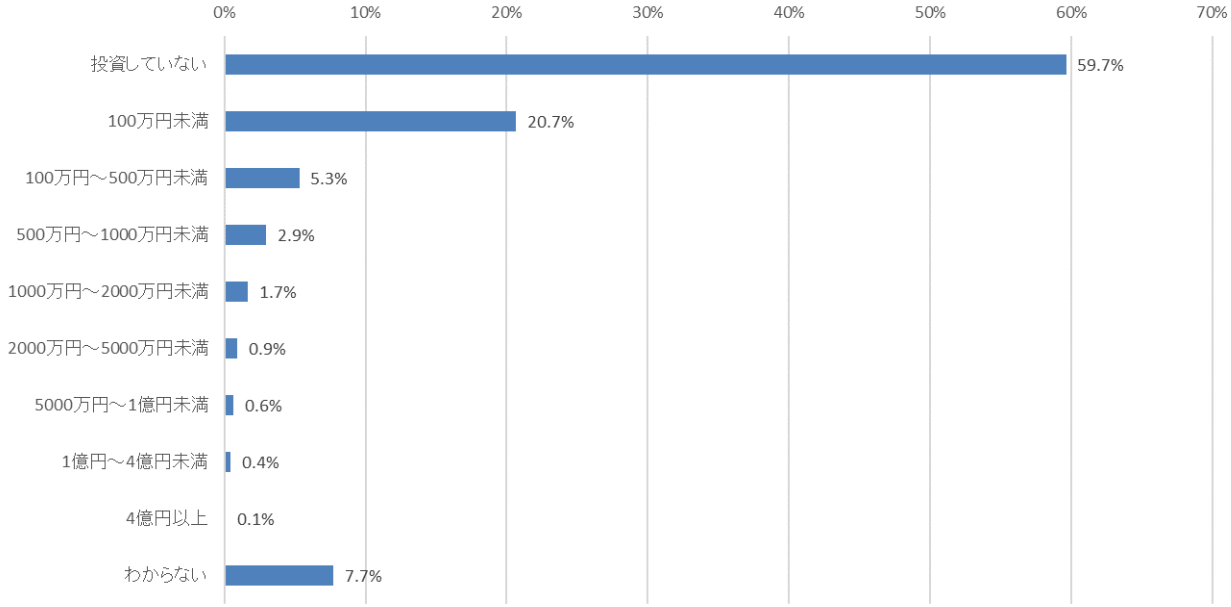

図 3-11 直近過去 3 期の IT 投資額(情報セキュリティ対策投資額を含む)(n=4191)

b. 直近過去3期の情報セキュリティ対策投資額

Q6-2. 貴社における、直近過去 3 期の IT 投資額(情報セキュリティ対策投資額を含む)と、情報セキュリティ対策投資額(IT 機器や社員への教育等も含む)の概算について教えてください。(SA)
-情報セキュリティ対策投資額(IT 機器や社員への教育等も含む)

傾向は IT 投資額とほぼ同じで、投資をしていないという回答が最も多く(2,623 件)62.6%と 6 割を超えている。投資をしている場合でも投資額が増えるほど件数は少なくなり、最も多いものが 100 万円未満(856 件)で 20.4%という状況である。

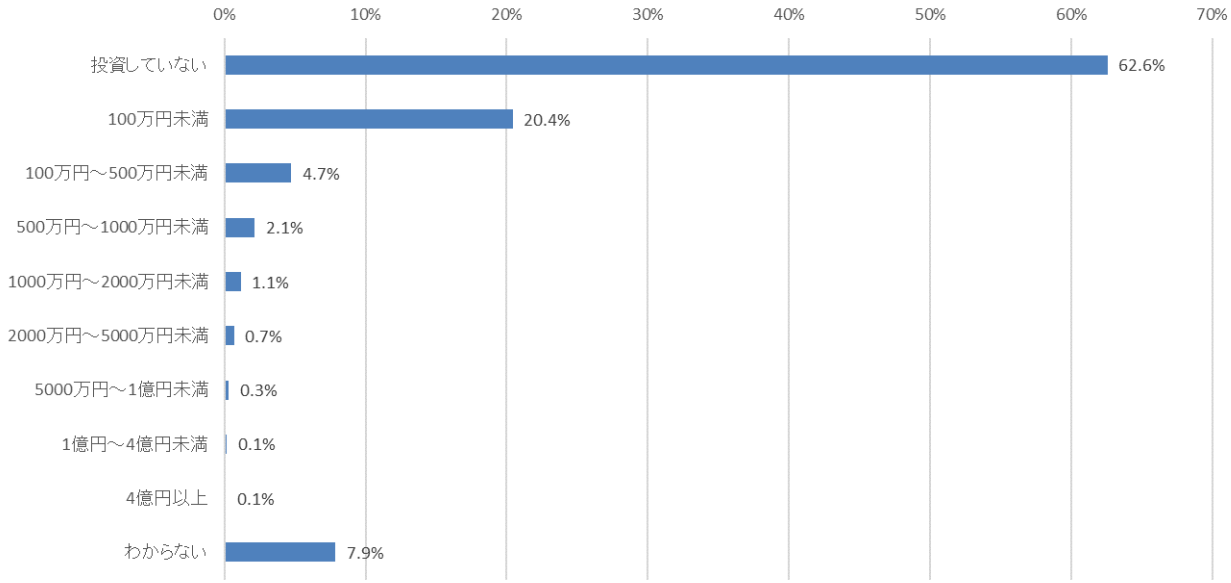

図 3-12 直近過去 3 期の情報セキュリティ対策投資額(IT 機器や社員への教育等も含む)(n=4191)

Q7. (Q6-2.で「投資していない」と回答された方について)前問で情報セキュリティ対策投資額について「投資をしていない」とお答えになった一番の理由について教えてください。(SA)

情報セキュリティ対策投資をしていない理由としては、必要性を感じていない(1,162 件)が 44.3%と最も多く、費用対効果が見えない(634 件)24.2%、コストがかかりすぎる(570 件)21.7%という回答が続いている。

回答者は小規模企業者が多いため、情報セキュリティ対策の必要性が十分に理解されていないことや、コストに見合う投資なのか確信が持てずに投資が躊躇されている実態が分かる。

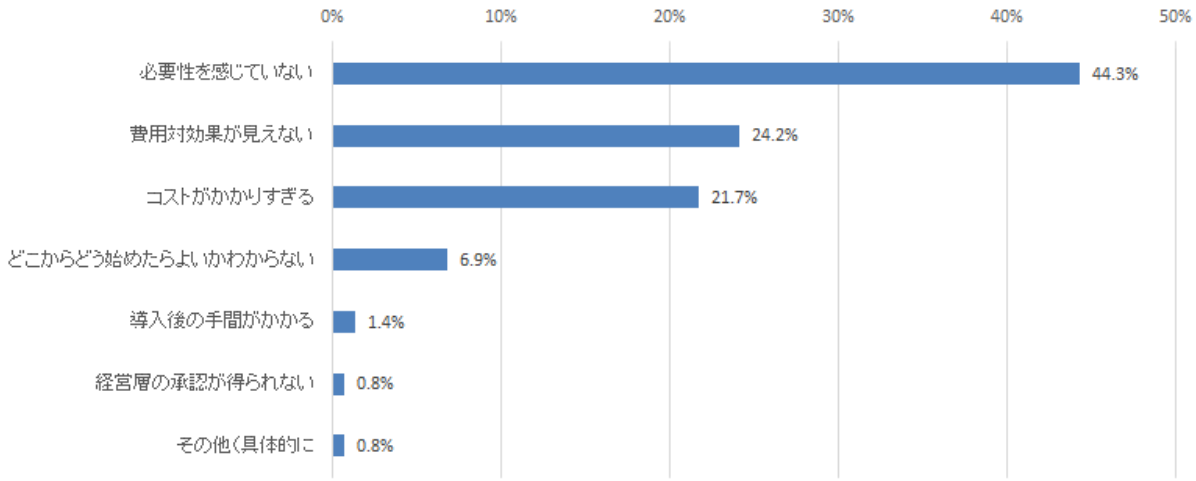

図 3-13 情報セキュリティ対策投資額について「投資をしていない」と回答した一番の理由(n=2623)

Q8. (Q7.で「必要性を感じていない」と回答された方について)前問で情報セキュリティ対策投資について「必要性を感じていない」とお答えになった理由について教えてください。 あてはまるものを下記よりすべてお選びください。(MA)

情報セキュリティ対策投資の必要性を感じていない理由として主なものは、重要情報を保有していない(424 件)36.5%、他社とのネットワーク接続がない(367 件)31.6%、事業の継続に大きな影響がな

い(301件)25.9%、サイバーセキュリティ被害にあうと思わない(279 件)24.0%である。

Q5 では全体の 8 割以上が電子メールを導入し、1/3 が Web サイトを利用、2 割近くが様々な社内 IT システムを利用しているという回答となっており、自社がサイバー攻撃に合う可能性やその際の事業への影響を過小評価している可能性がうかがえる。

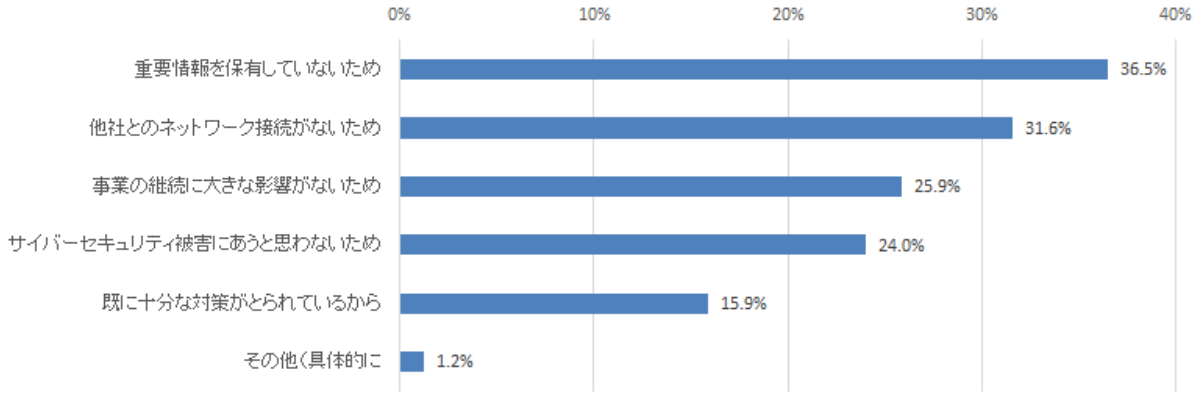

図 3-14 情報セキュリティ対策投資について「必要性を感じていない」と回答した理由(n=1162)

c. 情報セキュリティ対策の必要性を感じたきっかけ

Q9. 貴社で情報セキュリティ対策を実施(強化)するきっかけとなった理由について教えてください。(MA)

対策強化を実施していると思われる事業者においては、法令の制定や改訂への対応(838 件)20.0%が最も多く、重要情報の保持(596 件)14.2%、取引先からの要請(498 件)11.9%、業界基準の制定・業界団体の呼びかけ(387 件)9.2%と続いている。

自ら重要情報を保持しているとの認識をもって対策強化するケースもみられるが、外的要因(何らかの外的基準の制定や取引先からの要請)をきっかけとするケースも多いことがうかがえる。

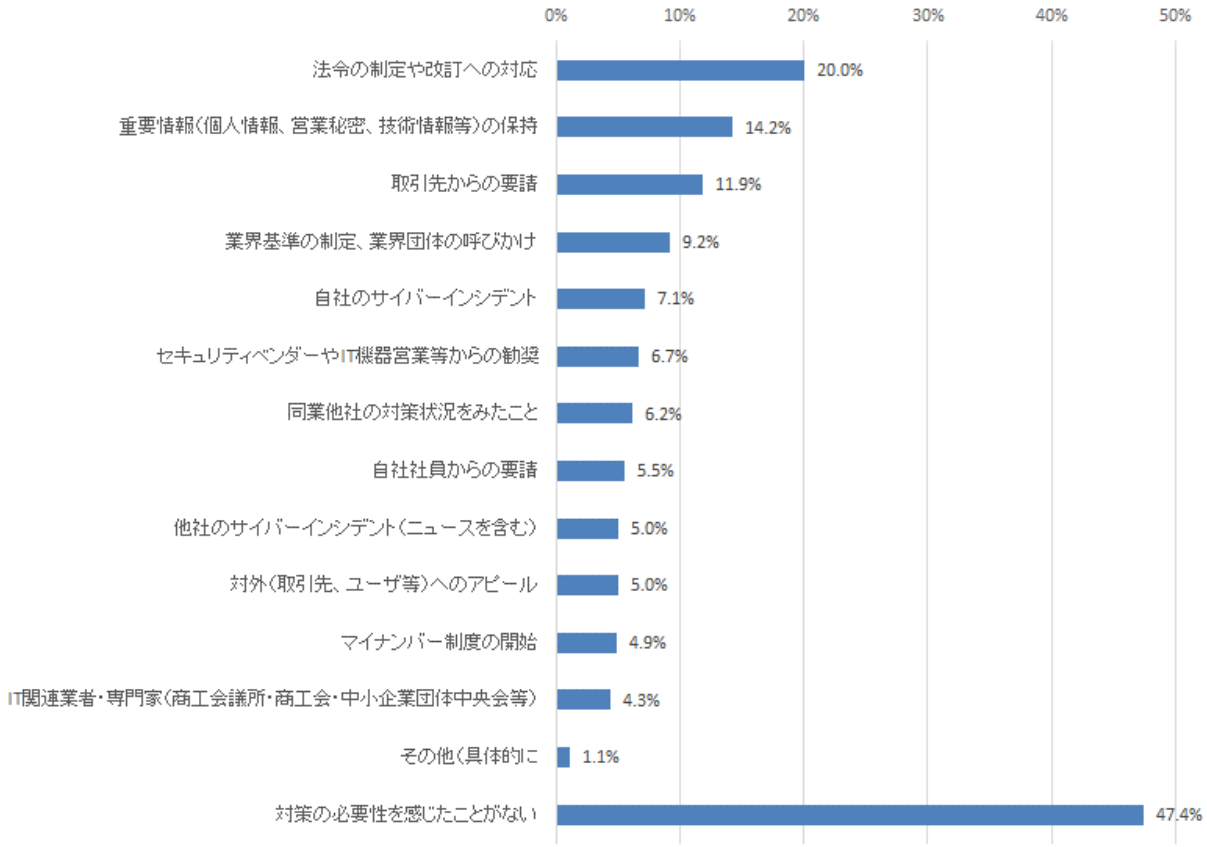

図 3-15 情報セキュリティ対策を実施(強化)するきっかけとなった理由(n=4191)

Q10.(Q9 で「対策の必要性を感じたことがない」以外の回答をされた方について)貴社が情報セキュリティ対策に期待する効果について教えてください。(MA)

情報セキュリティ対策に期待する効果としては、従業員の情報セキュリティへの意識向上(1,065 件)48.3%が最も多く、対処すべきリスクの特定(784 件)35.6%がこれに続いている。取引先からの信頼獲得(494 件)22.4%、サイバーインシデントで発生するコスト削減(401 件)18.2%、データ利活用の推進(402 件)18.2%、データ棚卸し等による業務効率化の実現(326 件)14.8%などの回答も多く、実利的な効果への期待も一定数、見受けられる。

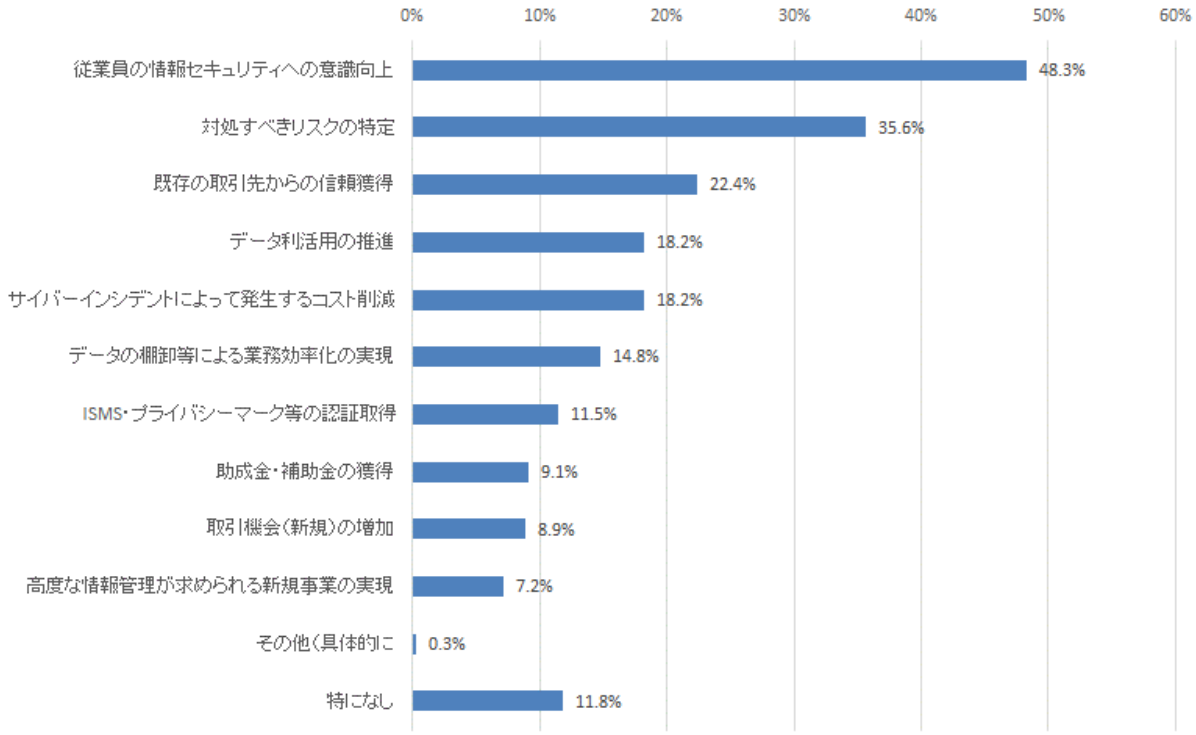

図 3-16 情報セキュリティ対策に期待する効果(n=2203)

Q11.（Q9 で「対策の必要性を感じたことがない」以外の回答をされた方について）貴社で情報セキュリティ対策を実施して感じられた具体的なメリットについて教えてください。（FA）

全ての自由回答内容の内、キーワードとして「安心」が 238 件、「信頼」が 95 件、「信用」が 41 件含まれている。（n=4191）

ア）「安心」が含まれる回答例

以下のような、情報セキュリティ対策により安心感が生まれたという回答が見られた（一部抜粋）。

- 顧客情報の漏洩を防ぐことができるという安心感を得られたこと
- 安心してインターネットを利用できる
- 取引先の安心感獲得

イ）「信頼」が含まれる回答例

以下のような、情報セキュリティ対策により信頼感が生まれたという回答が見られた（一部抜粋）。

- 取引先との信頼関係が高まったことで、より多くの取引を行うことが出来ている
- 大手企業からの信頼が得られ受注数が増えた
- ステークホルダーからの信頼の獲得
- 若い社員の信頼が増した
- WEB サイトで、発表して、 顧客の信頼を勝ち得たと思います
- 顧客との信頼を得る上で、情報漏洩等を問われることが多いので 会社として対策マニュアルを

用意していると説得力があり、有効と思われる

ウ）「信用」が含まれる回答例

以下のような、情報セキュリティ対策により信用が生まれたという回答が見られた（一部抜粋）

- 社員、顧客からの信用・信頼増加
- 取引先の信用度が高まる
- 万が一の時に何もしていなければ、取引先から信用を失う。逆に言い訳が出来る
- 目に見える形では現れていないが、顧客からの信用を失うことを防ぐことはできていると考える

図 3-17 情報セキュリティ対策を実施して感じられた具体的なメリット

Q12.（Q9 で「対策の必要性を感じたことがない」以外の回答をされた方について）貴社では情報セキュリティ関連製品やソフトウェアを導入していますか。導入している情報セキュリティ関連製品やソフトウェアを教えてください。あてはまるものを下記よりすべてお選びください。（MA）

導入している情報セキュリティ関連製品やソフトウェアとしてはウイルス対策ソフト・サービスの導入（1,762 件）80.0%が最も高く、幅広く利用されていることが読み取れる。次いで、ファイアウォール（821 件）37.3%、ウェブ閲覧のフィルタリングソフトウェア（494 件）22.4%が 20%を超える回答となる。

その他の項目についてはいずれも 10%程度であり、多くの中小企業では採用が進んでいないことが分かる。

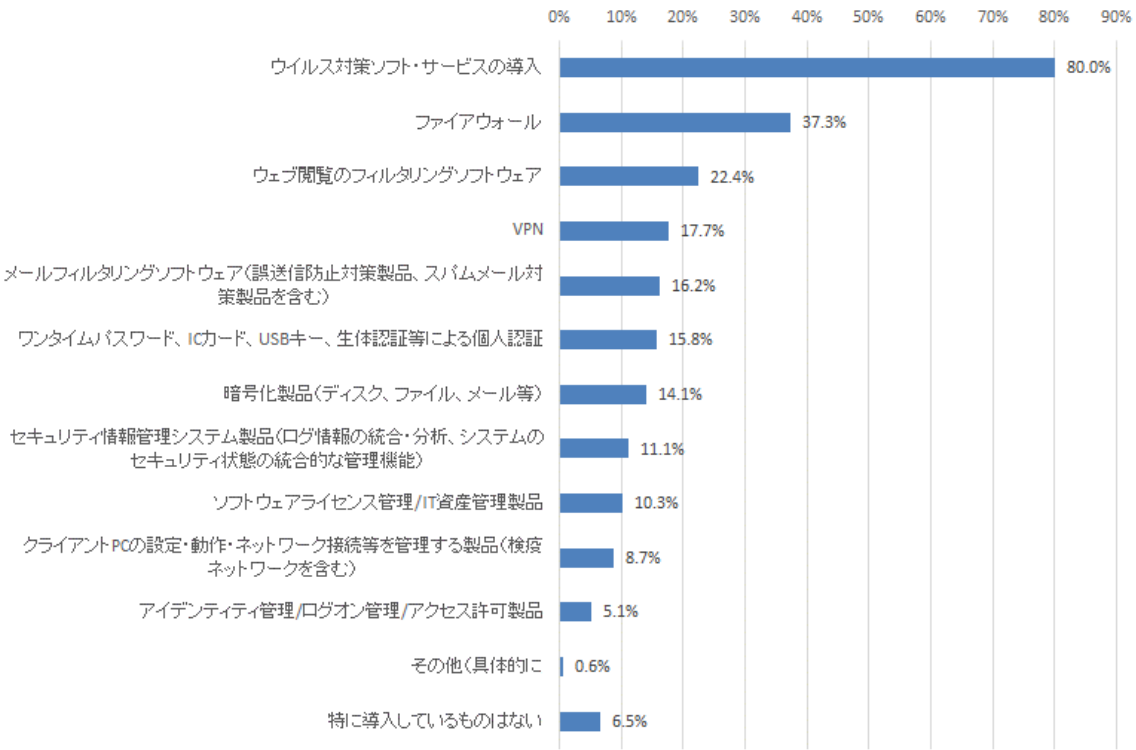

図 3-18 情報セキュリティ関連製品やソフトウェアの導入状況(n=2203)

Q13.（Q9 で「対策の必要性を感じたことがない」以外の回答をされた方について）貴社が利用している又は利用したいと考えている情報セキュリティ関連製品やサービスの内、費用対効果が高いと考えているものを教えてください。あてはまるものを下記よりすべてお選びください。（MA）

費用対効果が高いと選択した情報セキュリティ関連製品やサービスは、Q12 で導入済みと回答した製品やサービスとほぼ同じ構成となっていることが読み取れるが、ウイルス対策ソフト・サービスの導入（1,346 件）は 61.6%と Q12 の回答割合より低い

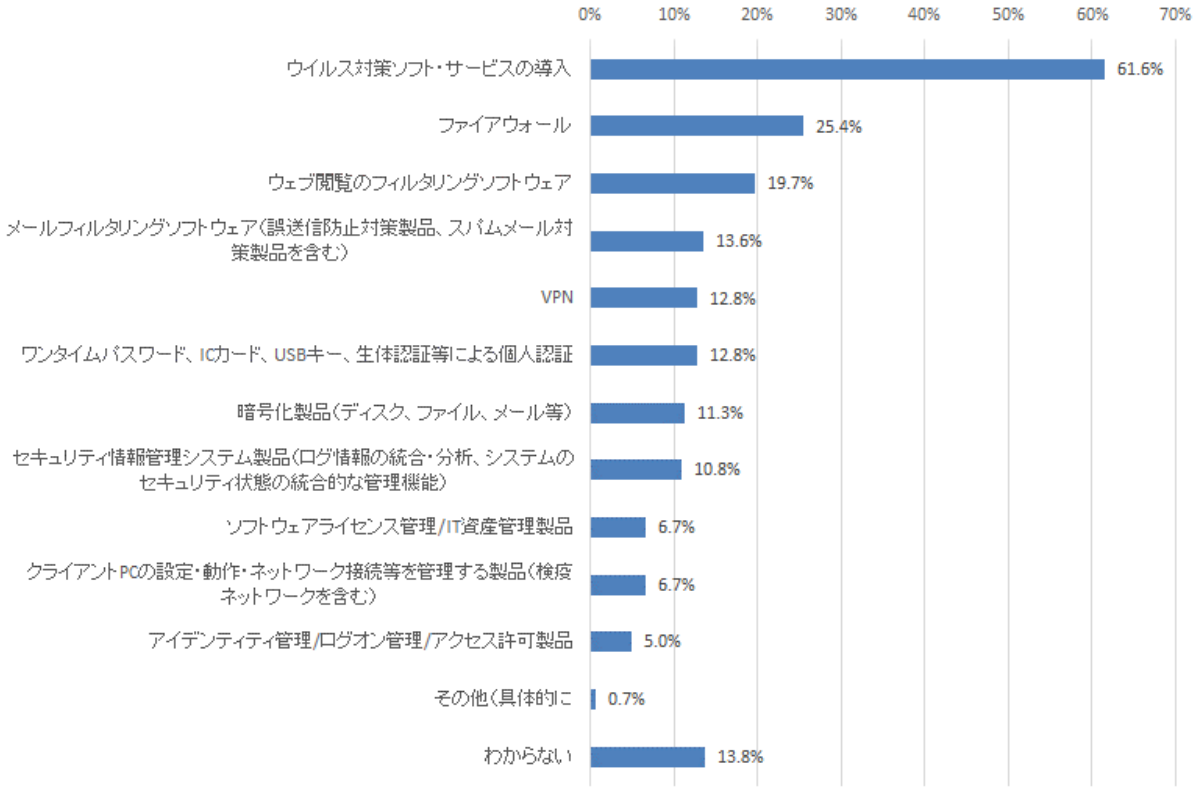

図 3-19 情報セキュリティ関連製品やサービスの内、費用対効果が高いと考えているもの(n=2203)

Q14.（Q9 で「対策の必要性を感じたことがない」以外の回答をされた方について）貴社ではサーバ等にセキュリティパッチを適用していますか。パッチを適用していない場合は理由について教えてください。あてはまるものを下記よりすべてお選びください。（MA）

サーバ等にセキュリティパッチを適用している（689 件）31.3%と、全体の 3 割に留まっており、パッチの適用が一般的な運用として浸透していないことが読み取れる。

パッチを適用しない理由としては、パッチの評価や運用に多大なコストがかかる（552 件）25.1%、パッチを適用しなくても問題ないと判断した（534 件）24.2%が高く、コスト上の課題と、リスク認識の甘さがあることが読み取れる。

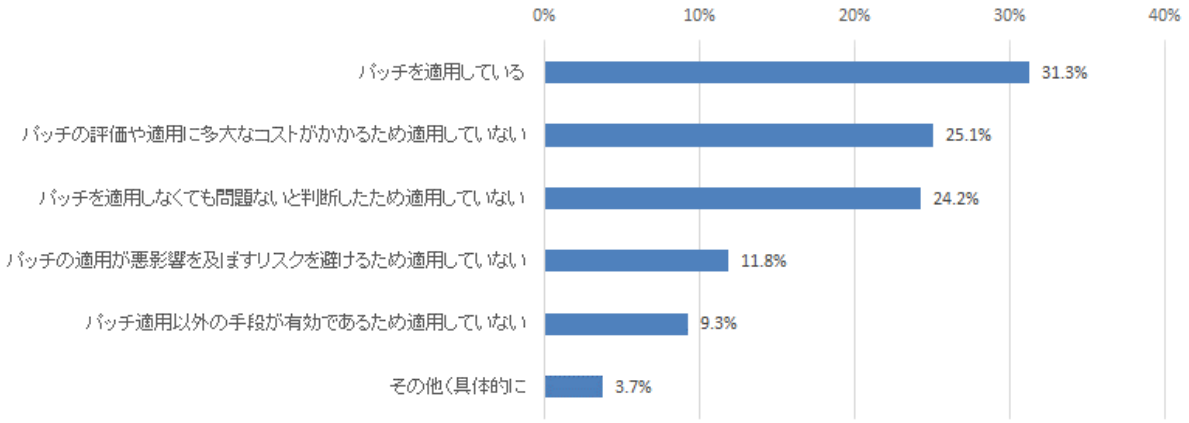

図 3-20 セキュリティパッチの適用状況(n=2203)

d. 情報漏えい等のインシデント又はその兆候を発見した場合の報告先

Q15. 貴社で情報漏洩等のインシデント又はその兆候を発見した場合に、規定されている報告先は何ですか。あてはまるものを下記よりすべてお選びください。（MA）

報告先として、経営者への報告(1,629 件)38.9%が最も多く、次いで報告先として多いのは、責任者への報告(1,025 件)24.5%、本人、関係者、取引先への連絡(954 件)22.8%となっている。一方で報告先が決まっていないは(1,338件)31.9%であり、インシデントが発生した際の対応における規定が中小企業では整備されていない実態が読み取れる。

業界団体への報告(215 件)5.1%、官公庁への報告(178 件)4.2%の割合は低いものの中小企業においては一定程度の業界団体および官公庁への報告を行われていることが読み取れる。

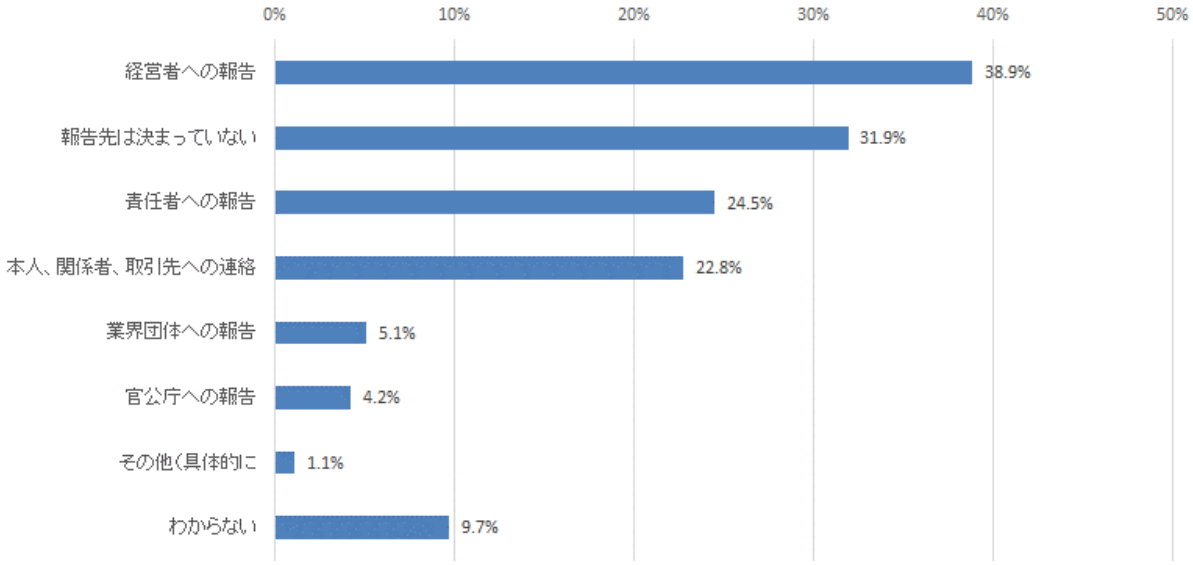

図 3-21 情報漏えい等のインシデント又はその兆候を発見した場合の報告先(n=4191)

e. 情報漏えい等のインシデント又はその兆候を発見した場合の対応方法

Q16. 貴社で情報漏洩等のサイバーインシデント又はその兆候を発見した場合の対応方法として規定されているものは何ですか。あてはまるものを下記よりすべてお選びください。（MA）
※サイバーインシデント: サイバーセキュリティの事故。例えば、不正アクセスやデータ漏洩など。

インシデントが発生した場合の対応方法について、対応方法が決まっていない(1,564 件)37.3%と4 割近くとなっており、中小企業においてはサイバーインシデントへの対応方法が曖昧な状態となっていることが読み取れる。

具体的な対応方法としては、情報の隔離(1,227 件)29.3%、ネットワーク診断(1,023 件)24.4%、原因の究明(868 件)20.7%、サービスの停止(839 件)20.0%となっており、サイバーインシデントが発生した際の対応方法については一定程度の認識されていることが読み取れる。

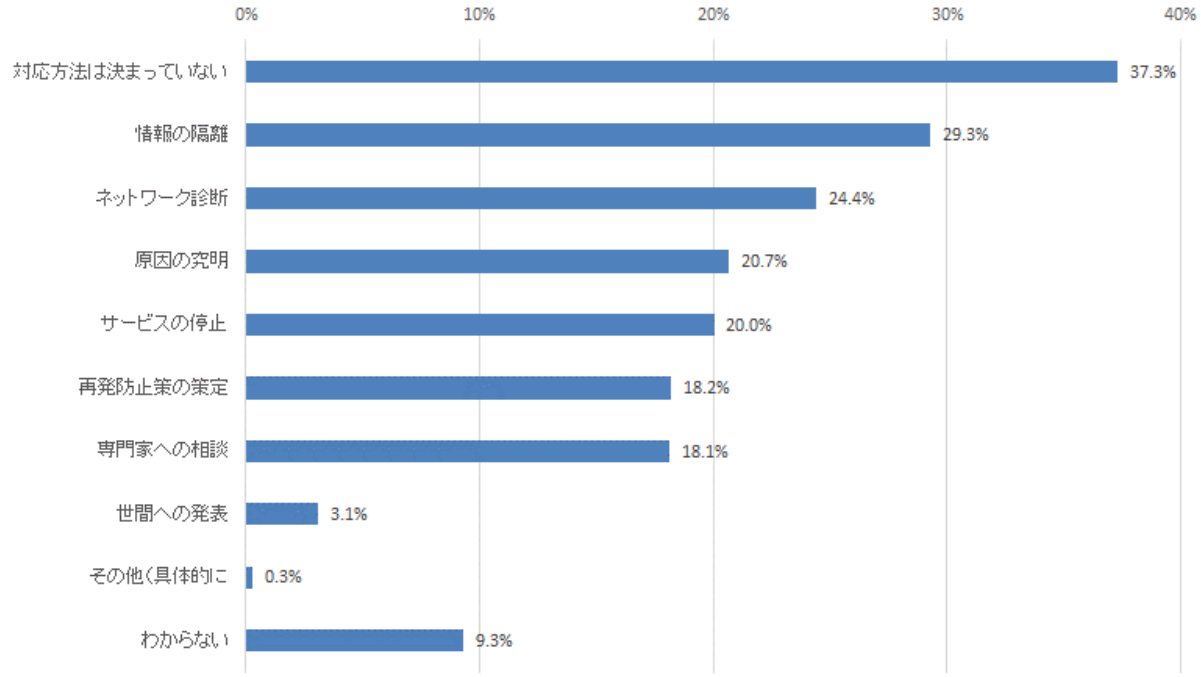

図 3-22 サイバーインシデント又はその兆候を発見した場合の対応方法(n=4191)

f. 情報セキュリティ業務の外部委託の状況・内容

Q17. 貴社は情報セキュリティ業務の外部委託(システム子会社への委託を含む)を行っていますか。行っている場合は、外部委託しているサービスについて教えてください。あてはまるものを下記よりすべてお選びください。（MA）

情報セキュリティ業務の外部委託は、委託していない(2,951 件)70.4%が最も多く、中小企業において外部委託が一般的でないことが読み取れる。

外部委託をしているサービスについて各々数パーセント台となっており突出しているものはないが、情報セキュリティ/BCP コンサルティングサービス(283 件)6.8%、ウイルス監視サービス(249 件)5.9%が比較的高い傾向にある。

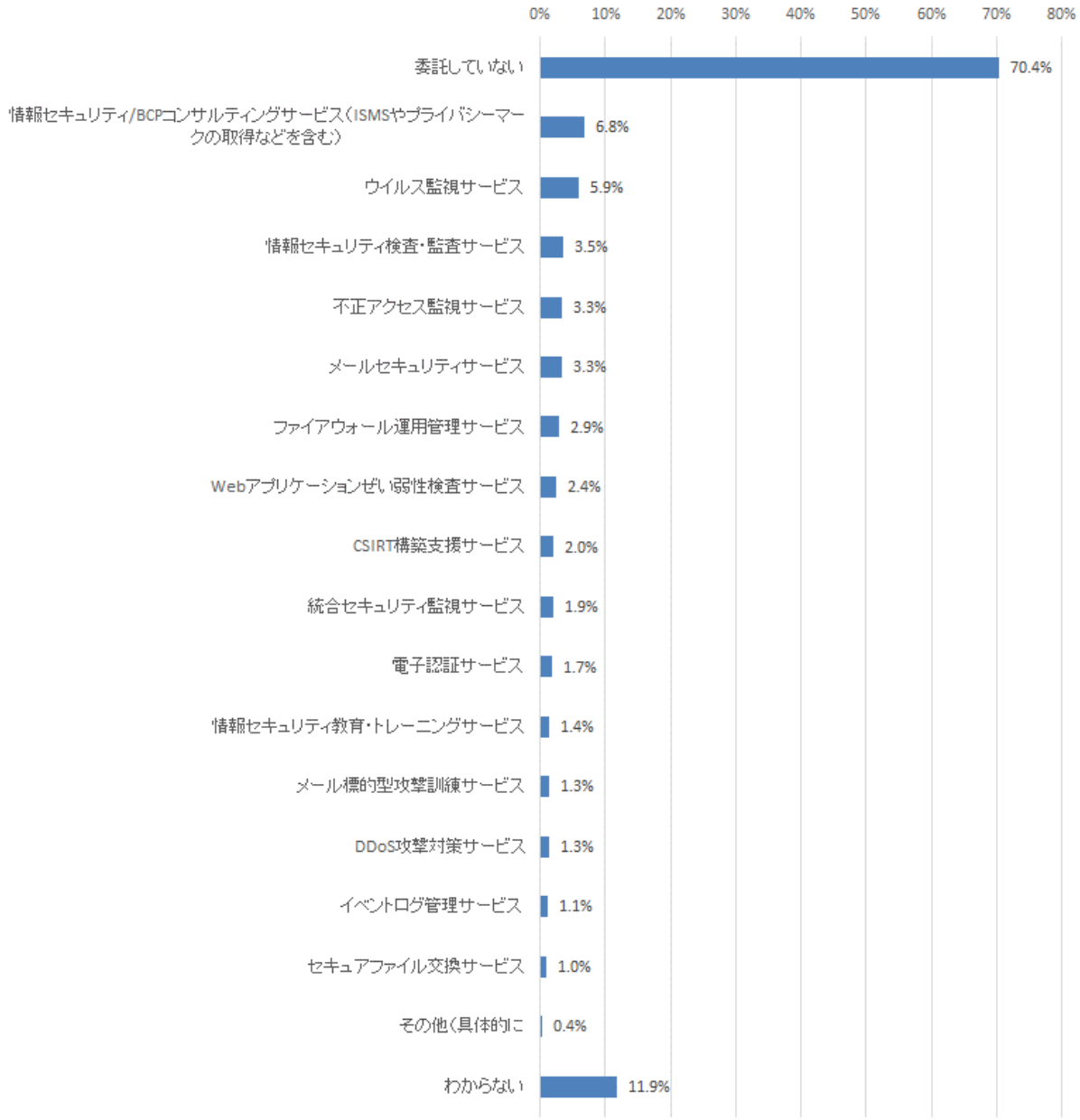

図 3-23 情報セキュリティ業務の外部委託状況(n=4191)

g. 情報セキュリティ業務の外部委託(システム子会社への委託を含む)をしている又はしたいと考えているものの内、費用対効果の高いもの

Q18. 情報セキュリティ業務の外部委託(システム子会社への委託を含む)をしている又はしたいと考えているものの内、費用対効果の高いものを教えてください。あてはまるものを下記よりすべてお選びください。(MA)

外部委託をしている又はしたいと考えているものの内、費用対効果が高いと認識されているサービスとしては、ウイルス監視サービス(635 件)15.2%、情報セキュリティ/BCP コンサルティングサービス(477 件)11.4%が高い傾向にある。

その他のサービスについて、実際に導入している割合より高い傾向にあり、外部委託への期待が一定程度あることが読み取れる。一方で、わからない(2,475 件)59.1%があるため、外部委託についての

費用対効果が認知されている可能性もある。

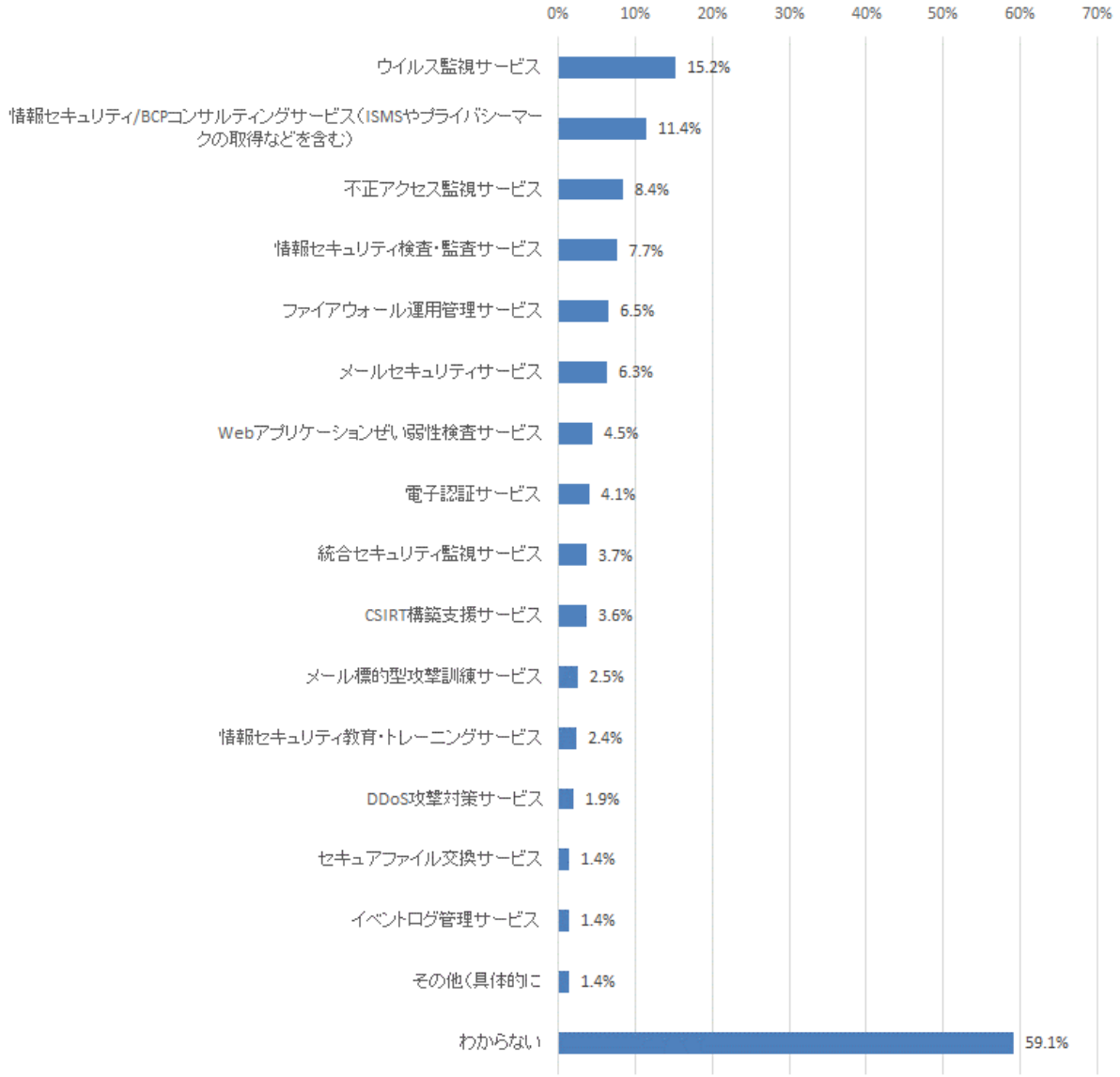

図 3-24 費用対効果の高い、情報セキュリティ業務の外部委託内容(n=4191)

h. どのような効果が期待できれば現状以上の情報セキュリティ対策を実施するか

Q19. 貴社で現状以上の情報セキュリティ対策を実施するためには、どのような効果が期待できれば対策を行うと思いますか。あてはまるものを下記よりすべてお選びください。
(MA)

現状以上の情報セキュリティ対策を行うために期待する効果としては、従業員の情報セキュリティへの意識向上(1,569 件)37.4%が最も高く、教育などへの期待が読み取れる。

次いで対処すべきリスクの特定(1,283 件)30.6%とリスク分析の実施が必要であると認識されていることが読み取れる。

一方で助成金・補助金の獲得(886 件)21.2%と、情報セキュリティ対策を必要な投資と捉えるよりむしろ、助成金・補助金を獲得するための手段としてとらえている実態も読み取れる。

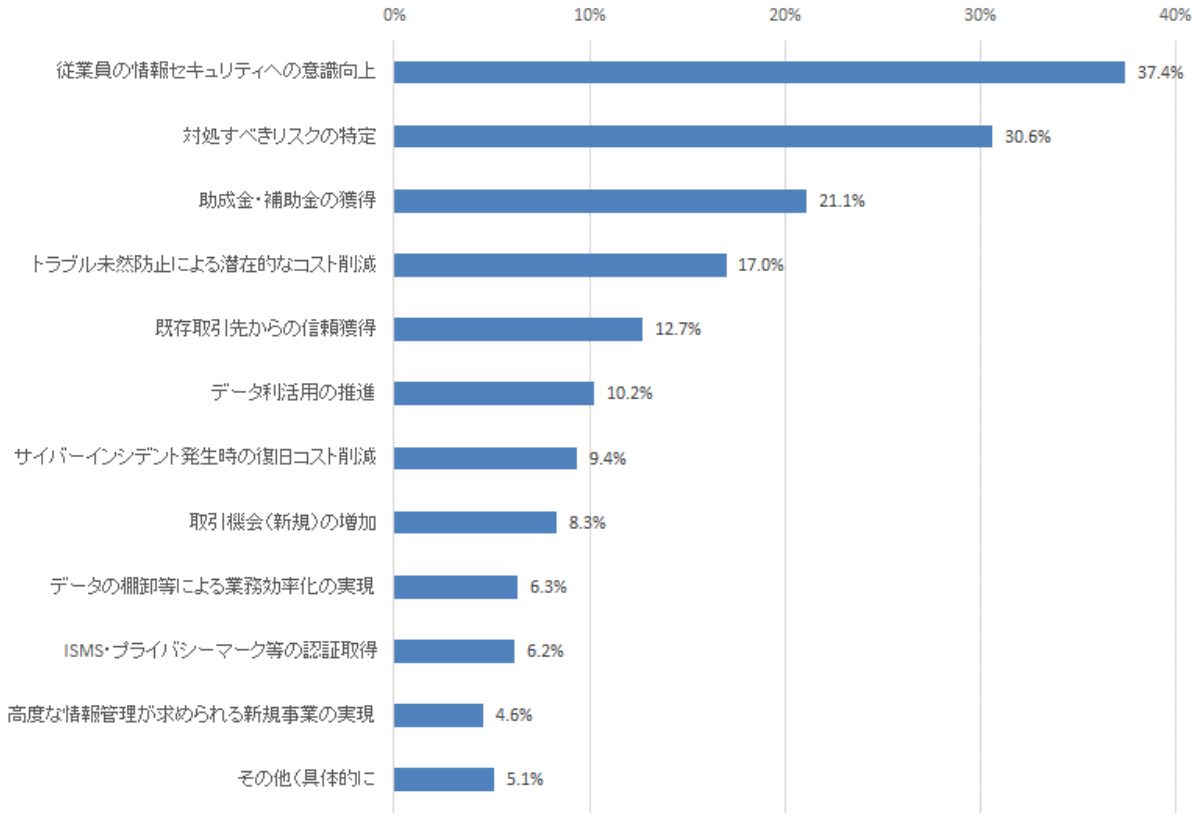

図 3-25 どのような効果が期待できれば現状以上の情報セキュリティ対策を実施するか(n=4191)

i. 情報セキュリティ対策をさらに向上させるために必要と思われること

Q20. 貴社の情報セキュリティ対策を、さらに向上させるために必要と思うことは何ですか。(MA)

情報セキュリティ対策を向上させるために必要なものとして、経営者のサイバーセキュリティリスク意識向上(1,365 件)32.6%が最も高く、次いで従業員の情報セキュリティ意識向上(1,124 件)26.8%と続く。

一方で特にない(1,629 件)38.9%の回答が最も高いことから、中小企業において情報セキュリティ対策をさらに向上させる意思が低い可能性も推察される。

地域での支援者育成や確保、サポートセンターの充実(213 件)5.1%などと地域の支援体制に一定程度の期待があることが読み取れる。

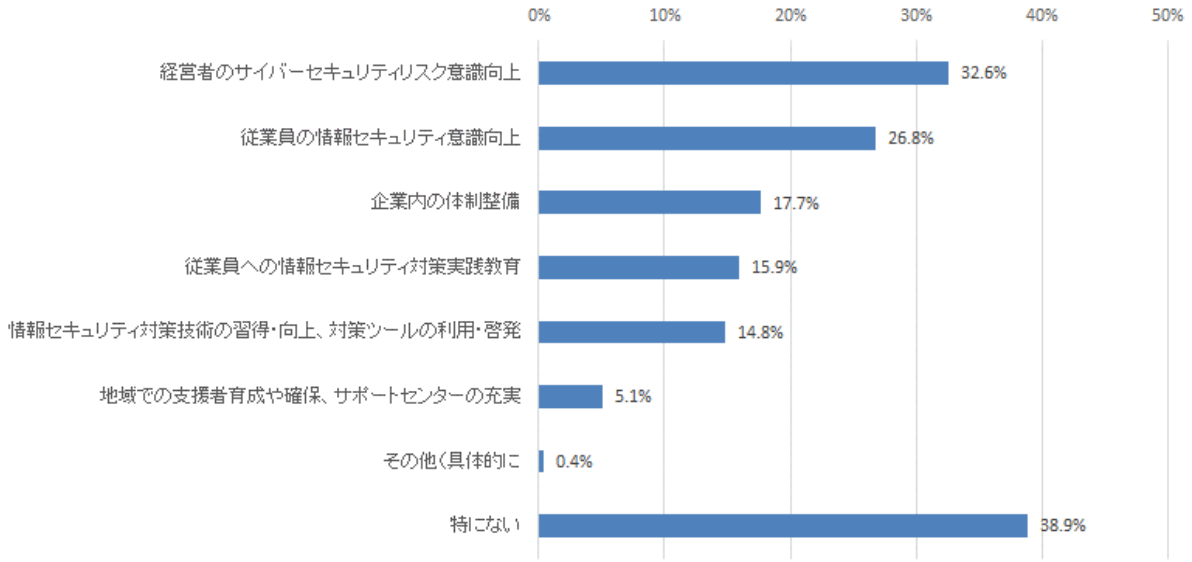

図 3-26 情報セキュリティ対策を、さらに向上させるために必要と思うこと(n=4191)

j. 活用したい情報セキュリティ対策に関するサービス

Q21. どのような情報セキュリティ対策に関するサービスがあれば活用したいと思いますか。あてはまるものを下記よりすべてお選びください。(MA)

活用したい情報セキュリティ対策に関するサービスとしては、経営層向けの手引書(1,210件)28.9%が最も高く、次いで経営層への教育(セキュリティ対策の重要性の理解)(926 件)22.1%となっている。その他の項目についても概ね 10%以上となっており、中小企業にとって各サービスへの期待が一定程度あることが読み取れる。

企業専属のセキュリティコンサルティングサービス(234 件)5.6%は最も低いが、一方で中小企業のセキュリティ対策の可視化サービス(780 件)18.6%とリスクと対策の可視化についての期待は高い傾向にある。

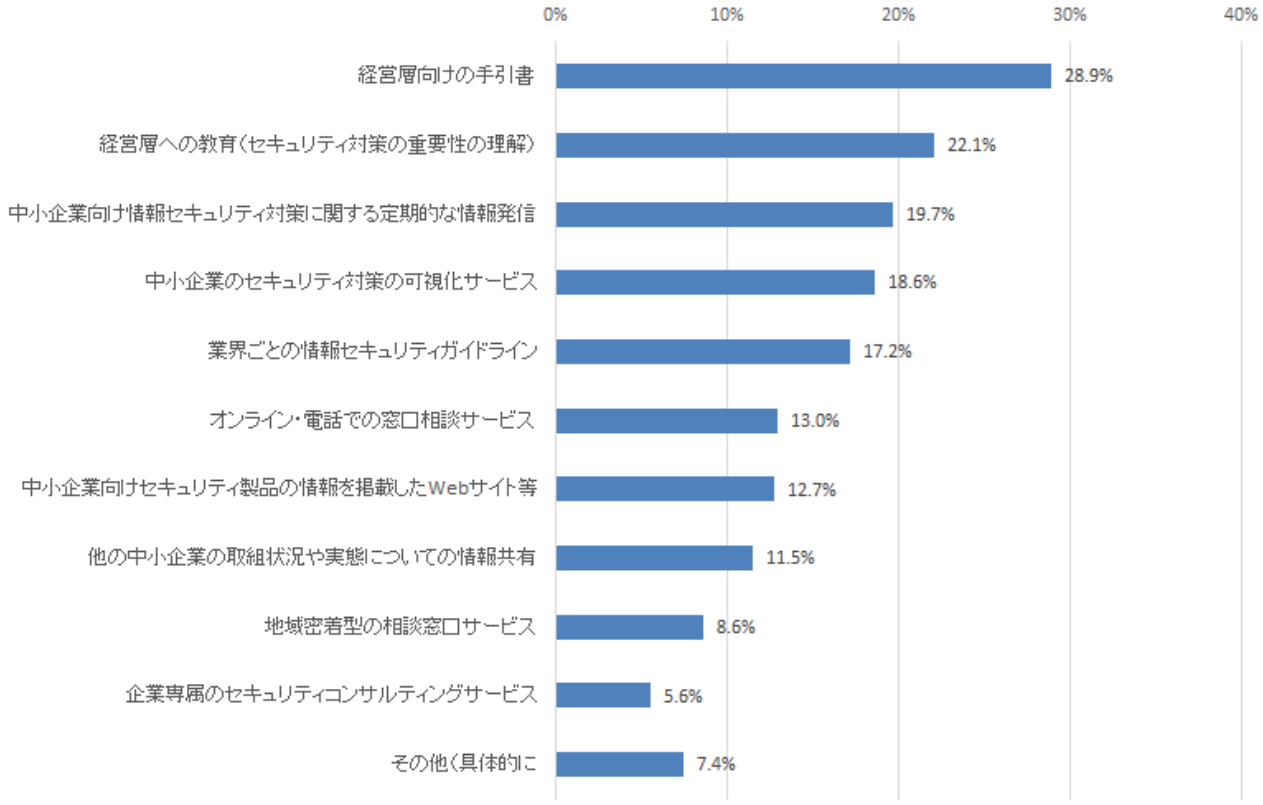

図 3-27 活用したい情報セキュリティ対策に関するサービス(n=4191)

k. 組織体制

Q22. 貴社の情報セキュリティ対策はどのような体制で行われていますか。(SA)

中小企業における情報セキュリティ対策の体制としては、組織的には行っていない(各自の対応)(2,920 件)69.7%が最も高く、7 割近くの中小企業において体制が整備されていない実態が読み取れる。

一方で専門部署(担当者)がある(390 件)9.3%と、兼務だが、担当者が任命されている(881 件)21.0%を合わせると 3 割近くの企業において何らかの情報セキュリティ対策体制が整備されていることが読み取れる。

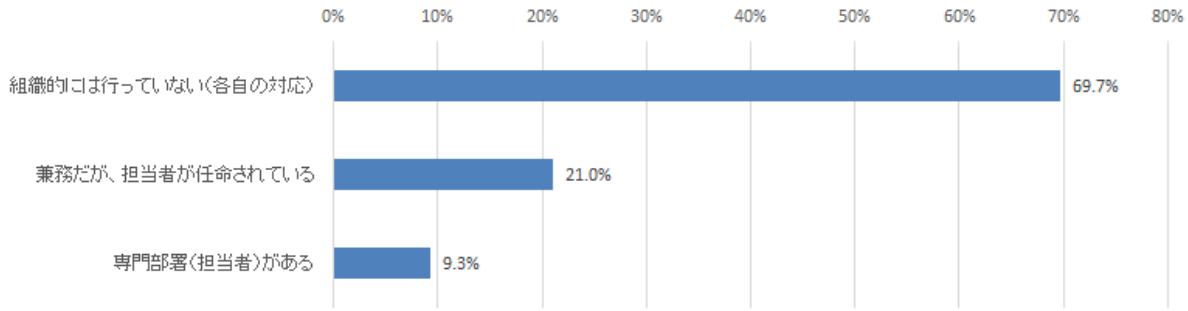

図 3-28 情報セキュリティ対策の体制(n=4191)

l. 認証取得や自己宣言の実施状況

Q77. 貴社の認証取得や自己宣言の実施状況について教えてください。

ISMS またはＰマーク取得済みの中小企業は全体の1割程度となっている。

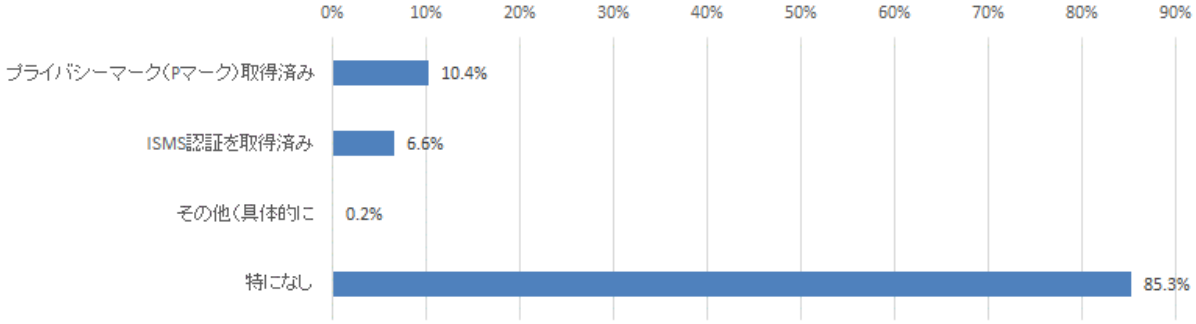

図 3-29 認証取得や自己宣言の実施状況(n=4191)

Q78. 認証取得や自己宣言にあたり、実施した具体的な取り組み・工夫などについて教えてください。

認証取得や自己宣言にあたり実施した取り組みとしては、情報セキュリティポリシーの策定と更新（362 件）58.9%が最も多く、次いで従業員のセキュリティ教育と訓練（323 件）52.5%である。

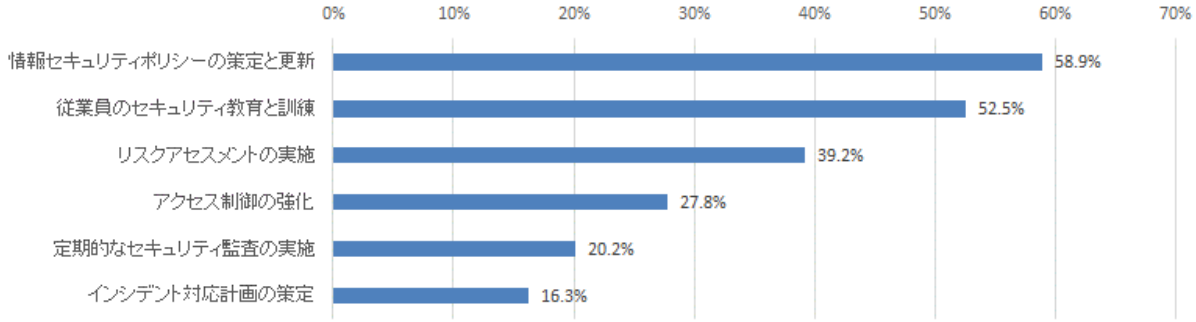

図 3-30 認証取得や自己宣言にあたり、実施した具体的な取り組み・工夫(n=615)

m. 情報セキュリティ対策を実施する上で参考にしたガイドライン

Q79. 貴社において、情報セキュリティ対策を実施する上で、参考にしたガイドライン等はありますか。

セキュリティ対策を実施する上で参考にしたガイドラインのうち、中小企業の情報セキュリティ対策ガイドラインを挙げた割合は全体の 5 割に達する。

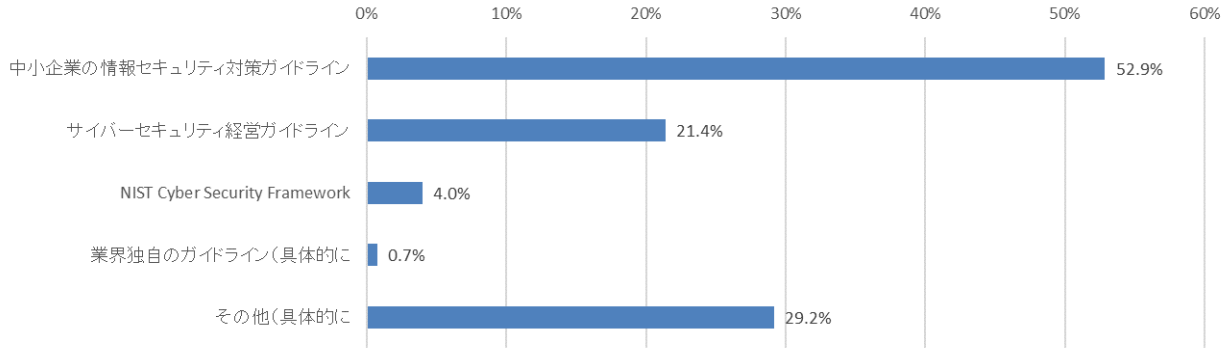

図 3-31 情報セキュリティ対策を実施する上で参考にしたガイドライン(n=4191)

n. 困ったことがあった際の相談先

Q23. 貴社の情報セキュリティ対策に関して困ったことがあった際の相談先を教えてください。あてはまるものを下記よりすべてお選びください。（SA/MA）

中小企業における情報セキュリティ対策の相談先としては、社内の担当者（1,162 件）27.7%が最も多く、次いで社外の IT 関連業者・営業（762 件）18.2%となっており、登録セキスペ等の外部人材を活用できていない実態が読み取れる。

一方で特にない（2,127 件）50.8%と 5 割近くの企業が困った先の相談先が無いと回答している。

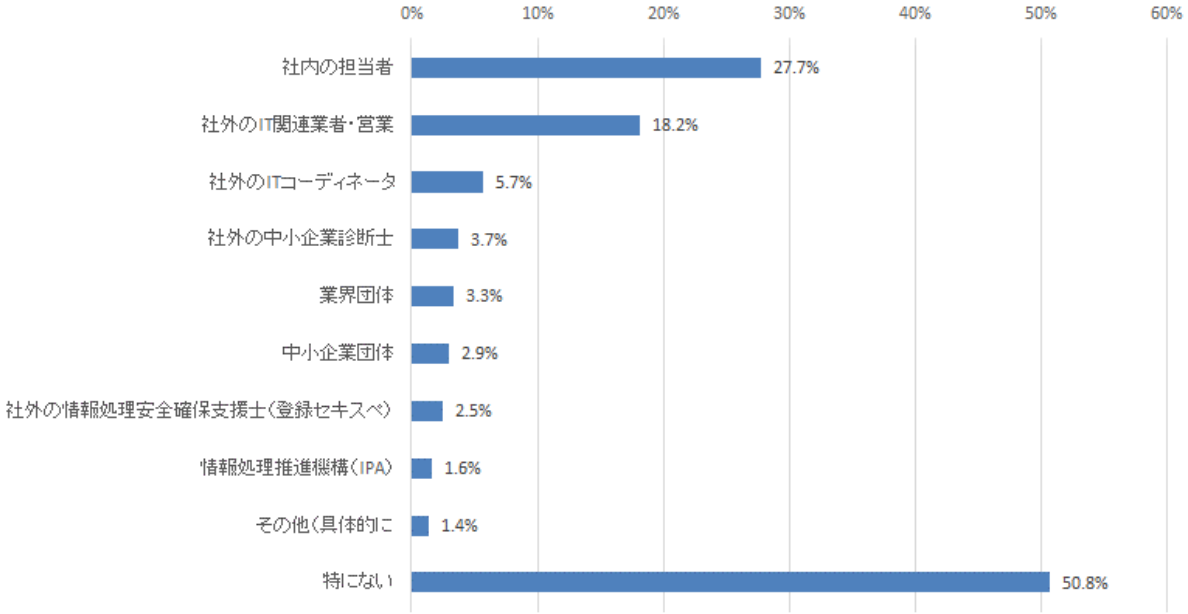

図 3-32 情報セキュリティ対策に関して困ったことがあった際の相談先(n=4191)

o. 情報セキュリティに関する情報収集先

Q24. 貴社の情報セキュリティ対策に関する情報収集先を教えてください。あてはまるものを下記よりすべてお選びください。（MA）

中小企業における情報セキュリティ対策に関する情報収集先としては、社内の担当者（1,122

件)26.8%、次いでインターネット(884 件)21.1%となっており、インターネットにおける情報の重要性が読み取れる。

社外の IT 関連業者(687 件)16.4%と、中小企業にとって情報セキュリティ対策に関する情報を収集する対象として IT 関連業者の割合が比較的高い実態が読み取れる。一方で、社外の登録セキスペを活用している回答企業は 2.4%に留まる。

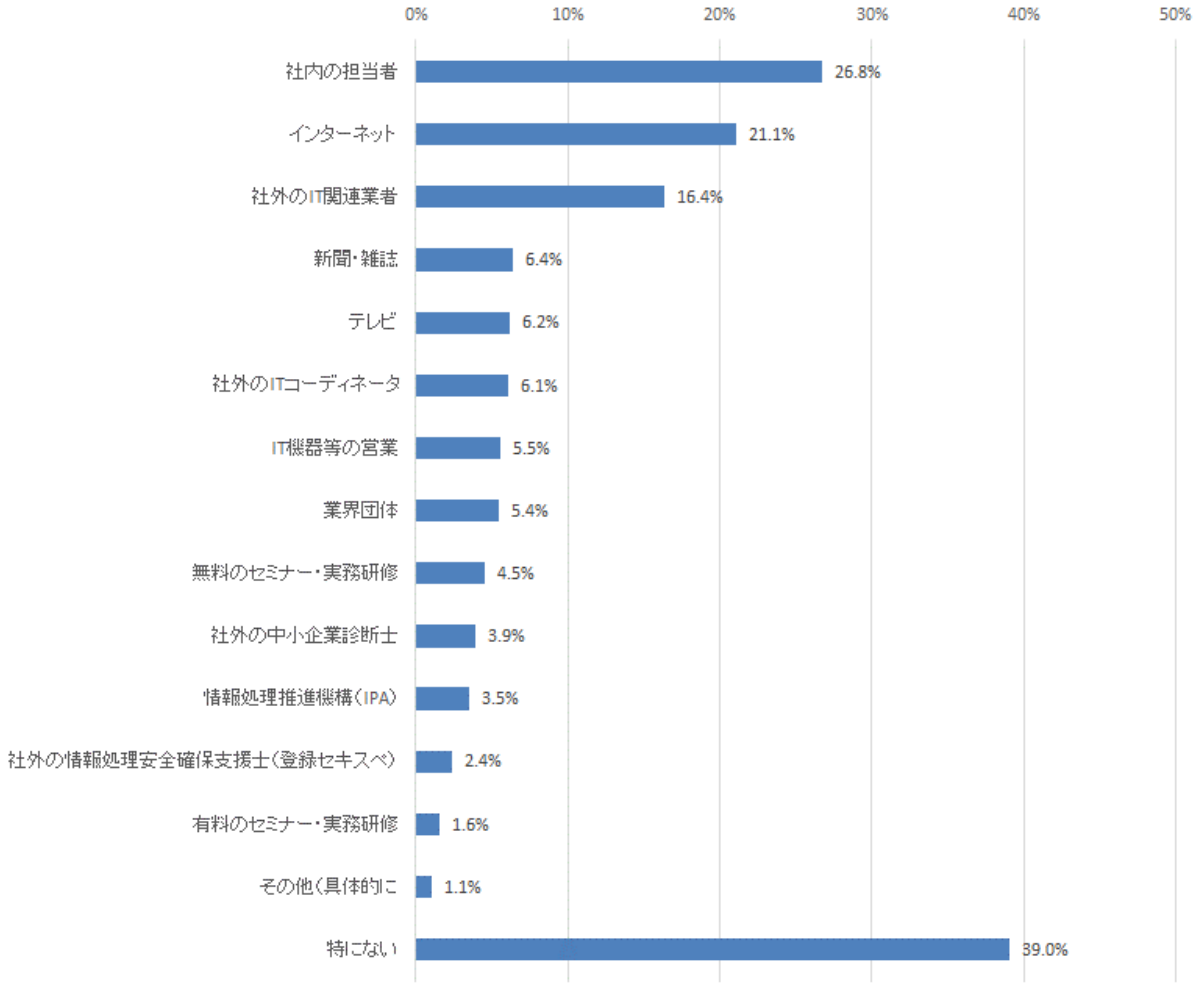

図 3-33 情報セキュリティ対策に関する情報収集先(n=4191)

3.2.5 情報セキュリティ教育の状況

回答企業の情報セキュリティ教育の関する状況や外部研修の活用状況などに関する設問と回答結果を記載する。

a. 従業員に対する情報セキュリティ教育の実施状況

Q25. 貴社では従業員に対する情報セキュリティ教育をどのように実施していますか。(MA)

情報セキュリティ教育について、特に実施していない(2,667 件)63.6%となっており、6 割強の企業において情報セキュリティ教育が実施されていない実態が読み取れる。

実施されている情報セキュリティ教育の中では、関連情報の周知(890 件)21.2%が最も高く、次いで e ラーニング(460 件)11.0%、社内の研修や勉強会(436 件)10.4%となっている。

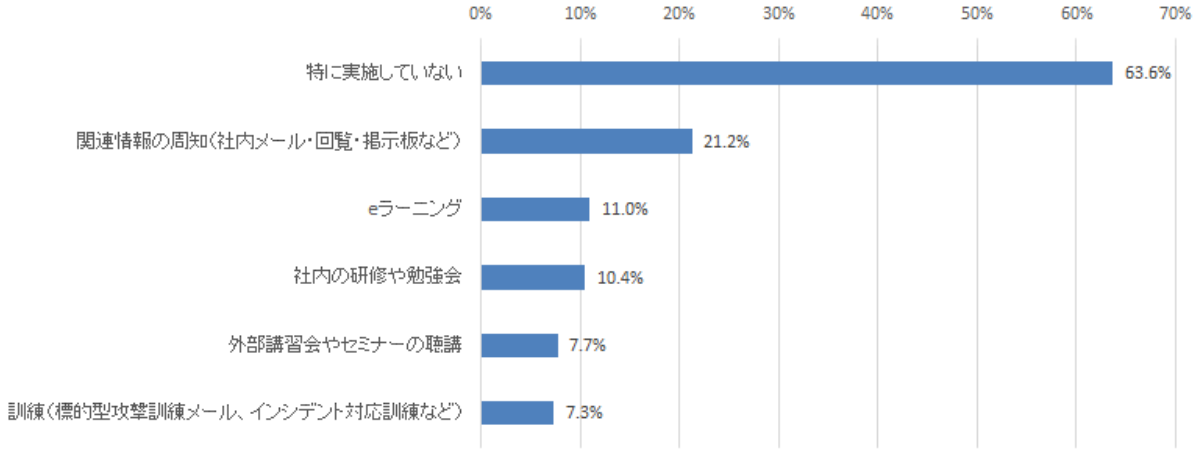

図 3-34 従業員に対する情報セキュリティ教育の実施状況(n=4191)

Q26. (Q25.で「特に実施していない」以外を回答した方について)貴社で行われている情報セキュリティ教育の内容はどのようなものですか。あてはまるものを下記よりすべてお選びください。(MA)

情報セキュリティ教育を実施している中小企業において、その内容としては情報セキュリティの基礎知識(1,046 件)68.6%が最も高く、7 割近い中小企業において情報セキュリティの基礎知識から教育を実施している実態が読み取れる。

会社のセキュリティポリシーと遵守事項(728 件)47.8%、メール利用時の注意点(790 件)51.8%、情報漏洩防止(686 件)45.0%と 5 割近くの企業が情報セキュリティに関するルールおよび被害に遭わないための注意点について教育を行っていることが読み取れる。

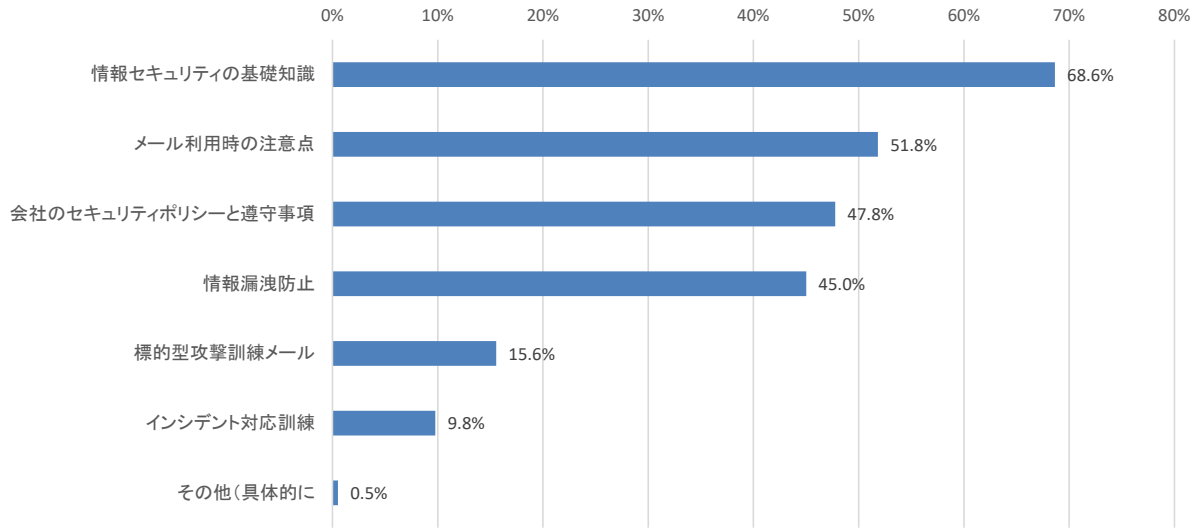

図 3-35 情報セキュリティ教育の内容(n=1524)

b. 情報セキュリティ人材を育成するための外部研修の活用状況

Q27. 貴社は情報セキュリティ人材を育成するために外部研修を活用している、または活用する意向がありますか。（SA）

中小企業における情報セキュリティ人材の育成において、外部研修を活用している企業は 2 割程度である。

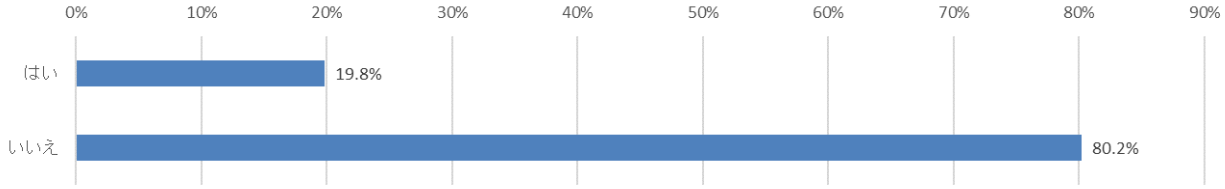

図 3-36 外部研修の活用状況(n=4191)

Q28.（Q27.で「はい」と回答された方について）貴社では情報セキュリティ人材育成のための外部研修に年間どの程度の期間をかけていますか。（SA）

情報セキュリティ人材の育成のために外部研修を使っている企業において、1 日～5 日（293 件）35.3%が最も多く、最長でも 2 週間程度までの期間をかけている企業が全体の 7 割程度になる。

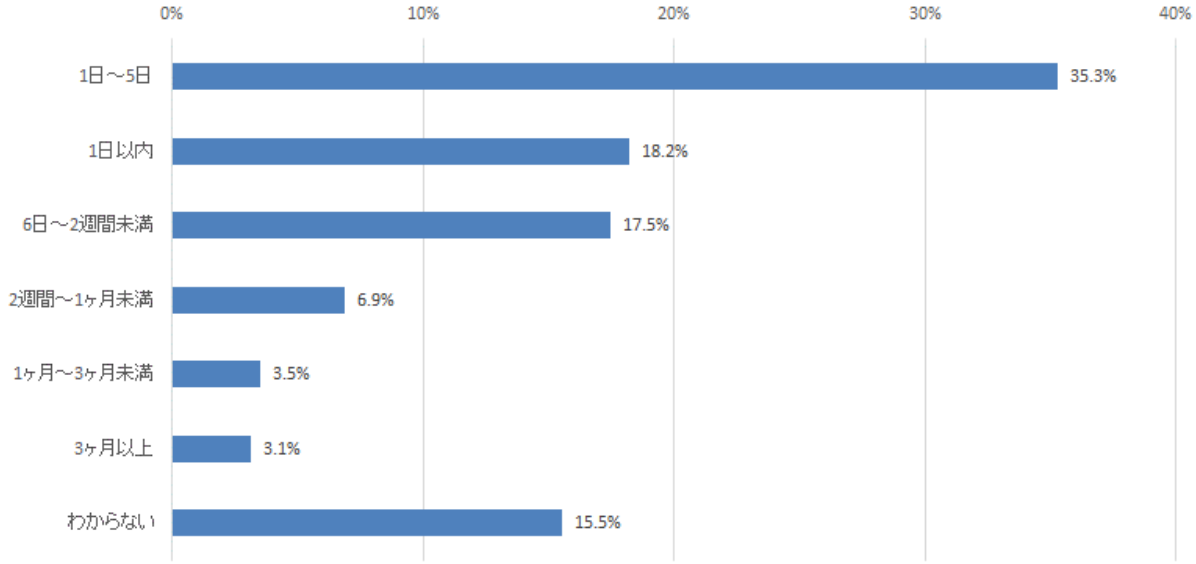

図 3-37 外部研修に年間どの程度の期間をかけているか(n=830)

Q29.（Q27.で「はい」と回答された方について）貴社では情報セキュリティ人材育成のための外部研修に年間どの程度の費用をかけていますか。（SA）

情報セキュリティ人材育成のための外部研修にかける費用としては、1 万円以上～10 万円未満（288 件）34.7%が最も多く、50 万円未満までの費用をかけている企業が全体の 7 割程度である。

一部の企業においては 100 万円以上の費用をかけている企業があることも読み取れる。

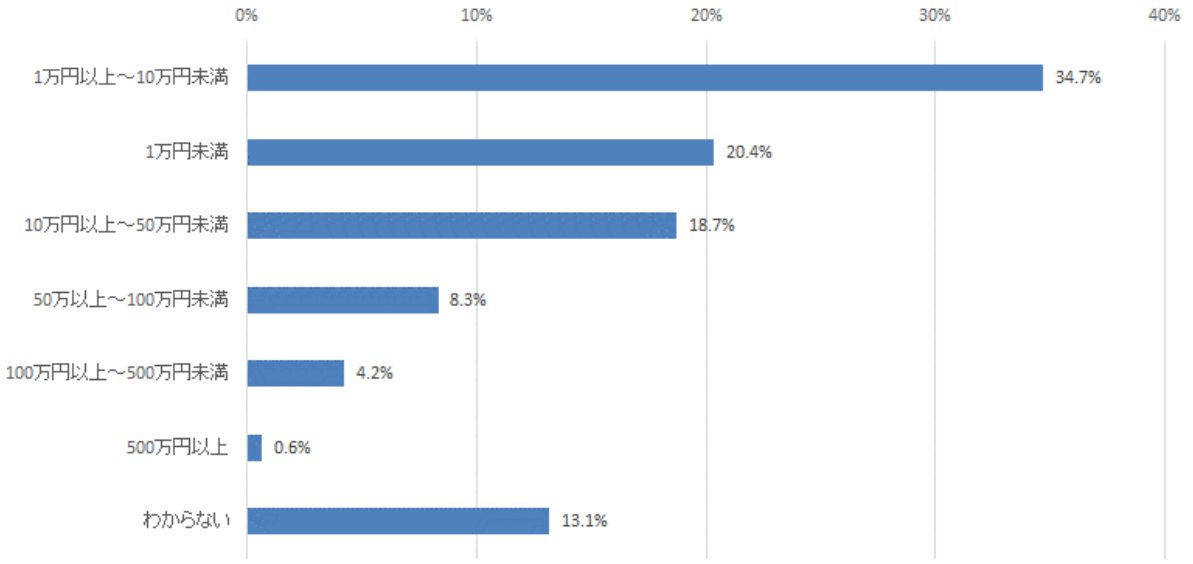

図 3-38 外部研修に年間どの程度の費用をかけているか(n=830)

Q30.（Q27.で「はい」と回答された方について）貴社では情報セキュリティ人材育成のための外部研修を活用する場合、どのような実施形態が望ましいと思いますか。あてはまるものを下記よりすべてお選びください。（MA）

セキュリティ人材育成のための外部研修の実施形態として望ましいと考えられているものは、オンラインと対面が5割程度と同等になっている。

外部研修の期間としては週 5 日の集中的な演習が 16.3%と最も多くなっている。

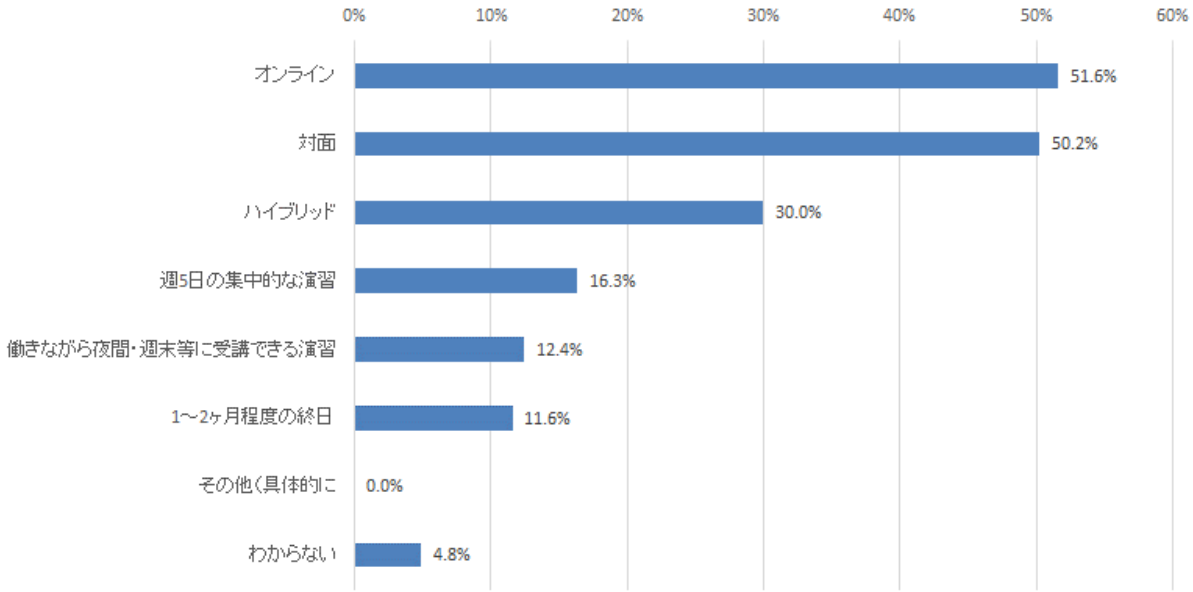

図 3-39 外部研修の実施形態(n=830)

Q31.（Q27.で「はい」と回答された方について）貴社では外部研修を年間どの程度の期間をかけることが望ましいと思いますか。（SA）

情報セキュリティ教育に関する外部研修の期間としては、年間 1 日～5 日（347 件）41.8%が最も多く、2 週間未満と回答した企業が全体の 7 割強になる。

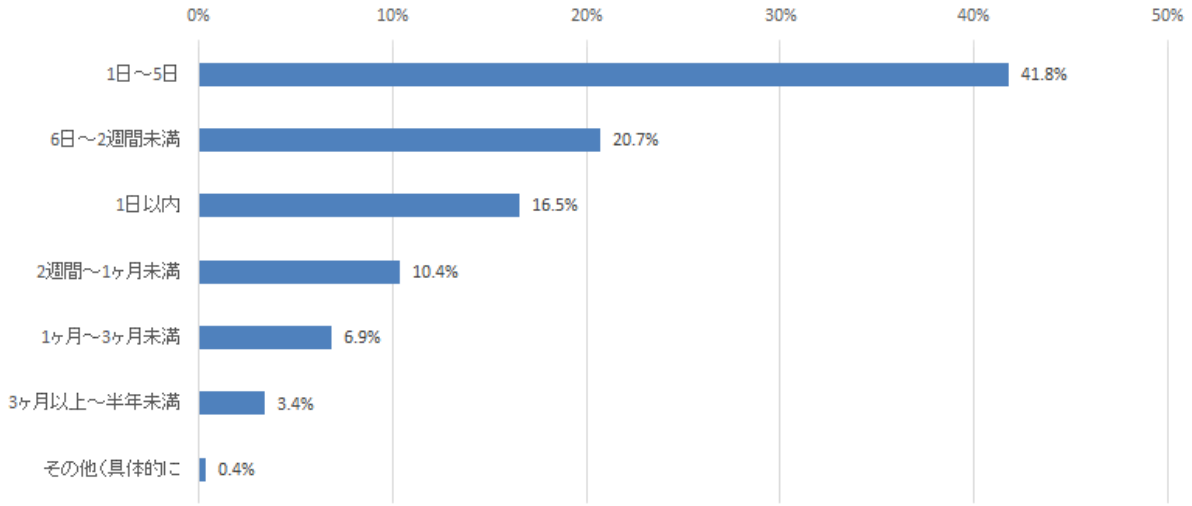

図 3-40 外部研修にかける期間(n=830)

Q32.（Q27.で「はい」と回答された方について）貴社では情報セキュリティ人材育成のための外部研修に年間どの程度の費用をかけることが望ましいと思いますか。（SA）

情報セキュリティ教育に関する外部研修の費用としては、年間で 5 万円未満と回答した企業が 4 割となっており、30 万円未満までの選択肢を回答した企業が全体の 8 割強になっている。

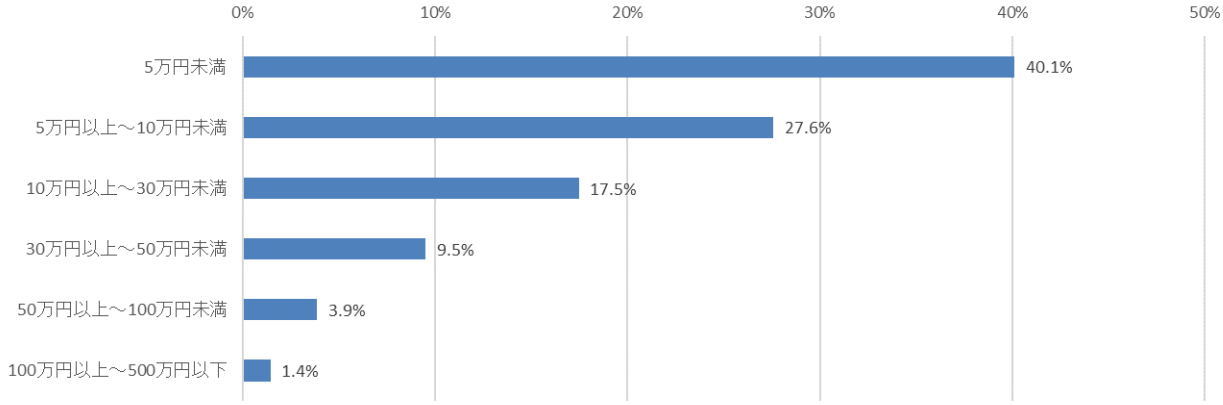

図 3-41 外部研修にかける費用(n=830)

Q33.（Q27.で「いいえ」と回答された方について）貴社で情報セキュリティ人材育成のための外部研修を活用していない又は活用する意向がない理由を教えてください。あてはまるものを下記よりすべてお選びください。（MA）

情報セキュリティ人材育成において外部研修を活用していない理由として、費用が高い(1,627 件)48.4%が最も高く、コストが外部研修の障壁となっている実態が読み取れる。

一方で適切な演習がない・わからない(1,366 件)40.6%と、4 割近くの中小企業が適切な演習を見つけられていない実態が読み取れる。

また、人的リソースが割けないと回答している企業が 3 割近くあり、人材不足が読み取れる。

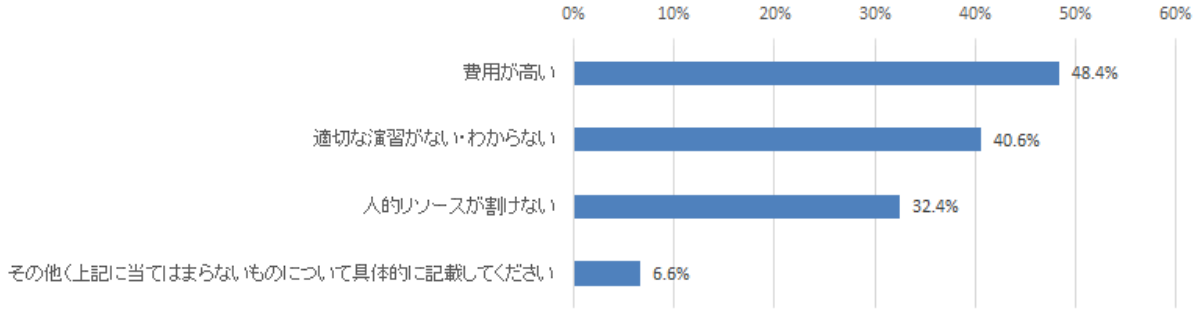

図 3-42 外部研修を活用していない又は活用する意向がない理由(n=3361)

3.2.6 サイバーインシデント被害の状況

回答企業が 2023 年度に受けたサイバーインシデント被害の状況、および影響に関する設問と回答結果を記載する。

Q34. 貴社では 2023 年度（2023 年4月～2024 年3月）にサイバーインシデントの発生、もしくは発生があった可能性が高い経験はありましたか。これらにあった場合は、その内容を教えてください。あてはまるものを下記よりすべてお選びください。（MA）

被害にあっていない（3,216 件）76.7%が最も多く、中小企業におけるサイバーインシデントの被害実態としては約2割が被害に遭っていると回答している。

被害の内容としては、コンピュータウイルス感染（619 件）14.8%、不正アクセス（419 件）10.0%、ランサムウェア感染（349 件）8.3%の順で多い。

内部者の不正に起因する情報漏洩は全体の 2.4%にとどまっている。

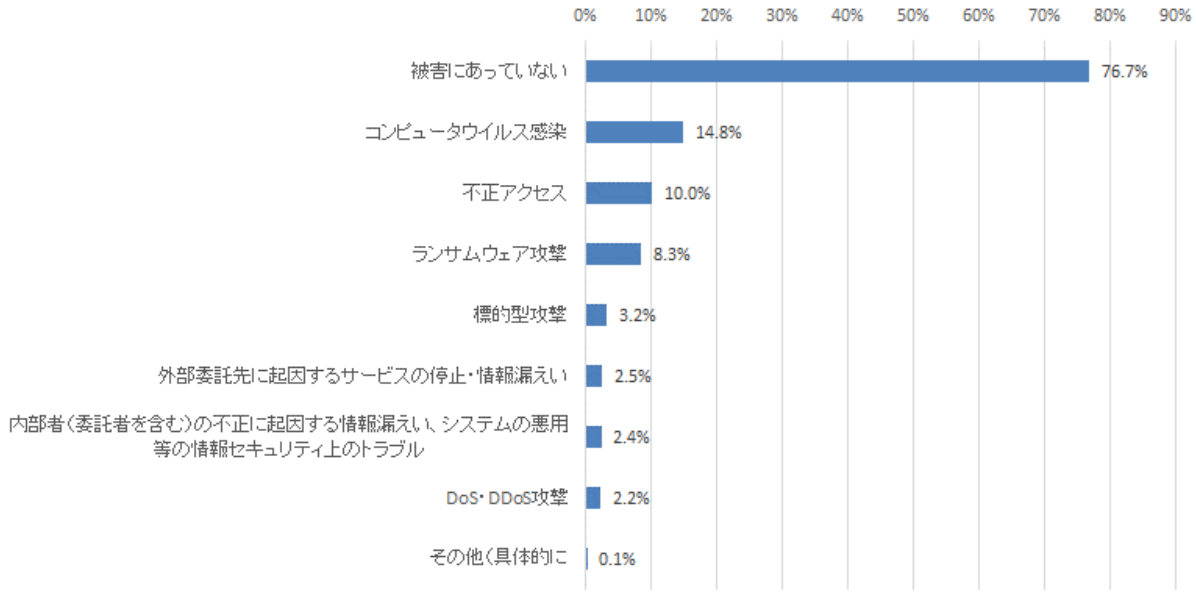

図 3-43 2023 年度にサイバーインシデントの発生もしくは発生があった可能性が高い経験(n=4191)

Q35.（Q34.で「被害にあっていない」以外のいずれかと回答された方について）貴社でサイバーインシデントによる影響で、生じた被害について教えてください。（MA）

サイバーインシデントによる影響としては、データの破壊(346 件)35.7%、個人情報の漏洩(342 件)35.1%が多く、次いで教務情報(営業秘密を除く)の漏洩(208 件)21.3%、ウイルスメール等の発信(147 件)21.5%となっている。

取引先への感染拡大(31 件)3.2%があることからサプライチェーン上のサイバーセキュリティリスクが顕在化していることが読み取れる。

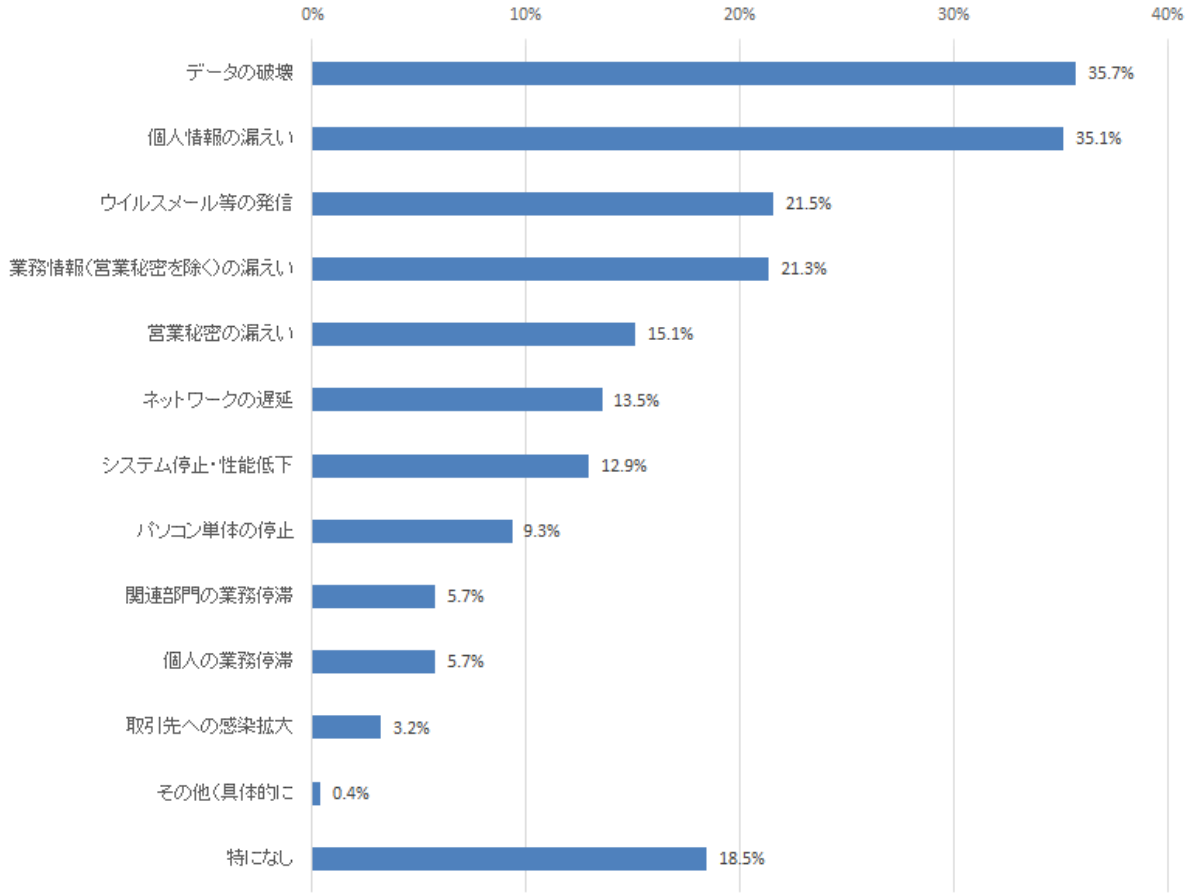

図 3-44 サイバーインシデントによる影響で生じた被害(n=975)

Q36. (Q34.で「被害にあっていない」以外のいずれかと回答された方について)サイバーインシデントにより貴社の取引先(サプライチェーン)に影響はありましたか。影響が及んだ場合はその内容について教えてください。あてはまるものを下記よりすべてお選びください。(MA)

サイバーインシデントにより取引先への影響があったと回答している企業は約 7 割に上り、その内容についてはサービスの障害遅延停止による逸失利益(352 件)36.1%、個人顧客への賠償や法人取引への補償負担(316 件)32.4%が多い。

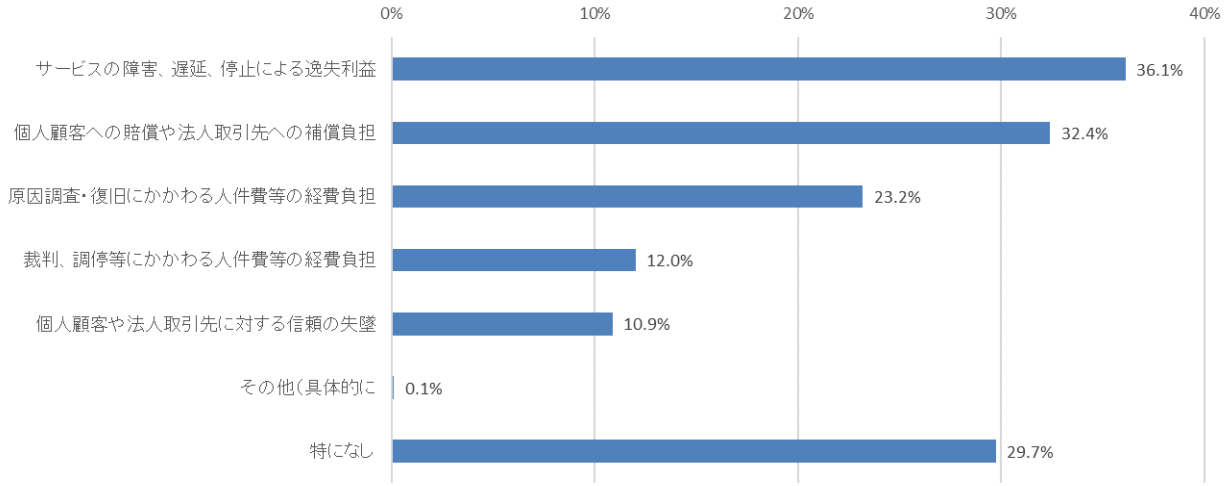

図 3-45 自社のサイバーインシデントによる取引先への影響(n=975)

Q37.（Q34.で「不正アクセス」と回答された方について）貴社が受けたサイバー攻撃の手口について教えてください。あてはまるものを下記よりすべてお選びください。（MA）

不正アクセスを受けたケースでのサイバー攻撃の手口としては、脆弱性（201 件）48.0%が最も多く、5 割近くがセキュリティパッチの未適用等に起因するよみ脆弱性を突かれたものであることが読み取れる。

次いで、ID・パスワードをだまし取られたケースが 3 割強となっており、フィッシング被害などによる ID・パスワードの漏洩のケースも含めて、ID とパスワード管理の重要性が示唆される。

サプライチェーン上のセキュリティリスクとしては、取引先やグループ会社等を経由して侵入（83 件）19.8%と 2 割程度あることが読み取れる。

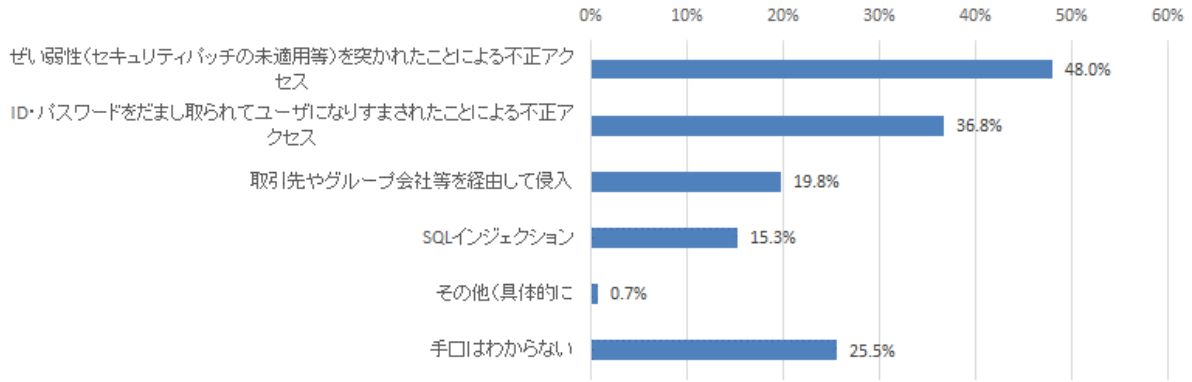

図 3-46 不正アクセスの手口(n=419)

Q38.（Q34.で「不正アクセス」と回答された方について）貴社が受けたサイバー攻撃の被害について教えてください。あてはまるものを下記よりすべてお選びください。（MA）

不正アクセスによる被害の内容としては自社 Web サイトに関する被害として、改ざん（69 件）16.5%、サービス停止（96 件）22.9%がある。同様に、業務サーバに関する被害としても、改ざん（85 件）15.5%、サービス停止（85 件）20.3%と特定のシステムに限らず被害を受けている状況が読み取れる。

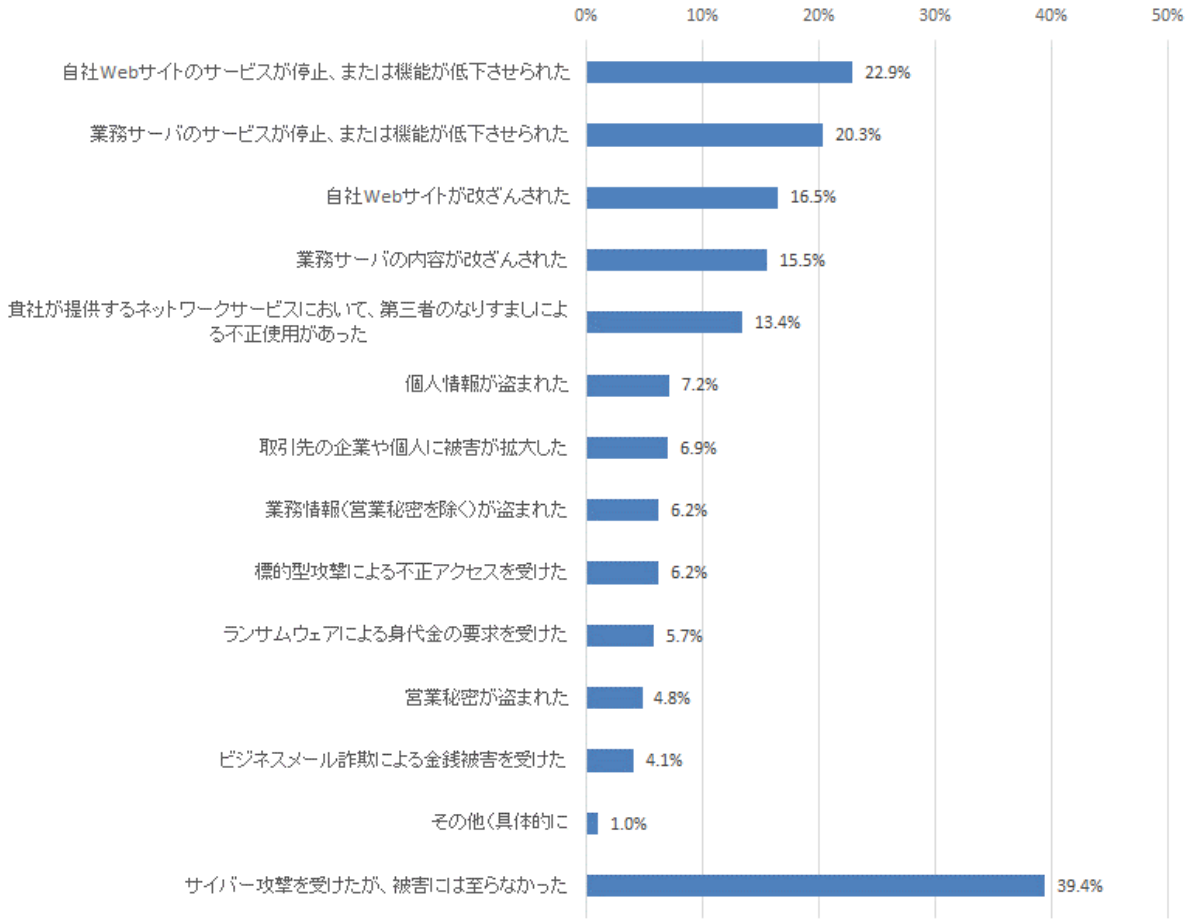

図 3-47 不正アクセスによる被害(n=419)

Q39.（Q34.で「被害にあっていない」以外のいずれかと回答された方について）過去 3 期、サイバーインシデントの発生で生じた被害額の総額、サイバーインシデントの発生回数、復旧するまでに要した最大の期間について教えてください。（0 以上の半角数字で入力してください。）（FA）

過去 3 期に発生したサイバーインシデントで生じた被害額の平均は 73 万円であり、100 万円以上の被害額であった企業は 9.4%（最大で1億円）、過去3期内で 10 回以上のサイバーインシデント被害に遭った企業が 1.7%（最大で 40 回）、復旧までに要した期間の平均は 5.8 日であり、50 日以上を要した企業が 2.1%（最大で 360 日）であった。中小企業においても実際に甚大な被害が起きていることが伺える。

表 3-2 被害額、発生回数、期間の平均値と最大値

項目	平均値	最大値
被害総額(円)	約 73 万	1 億
発生回数(回)	1.1	40
復旧期間(日)	5.8	360

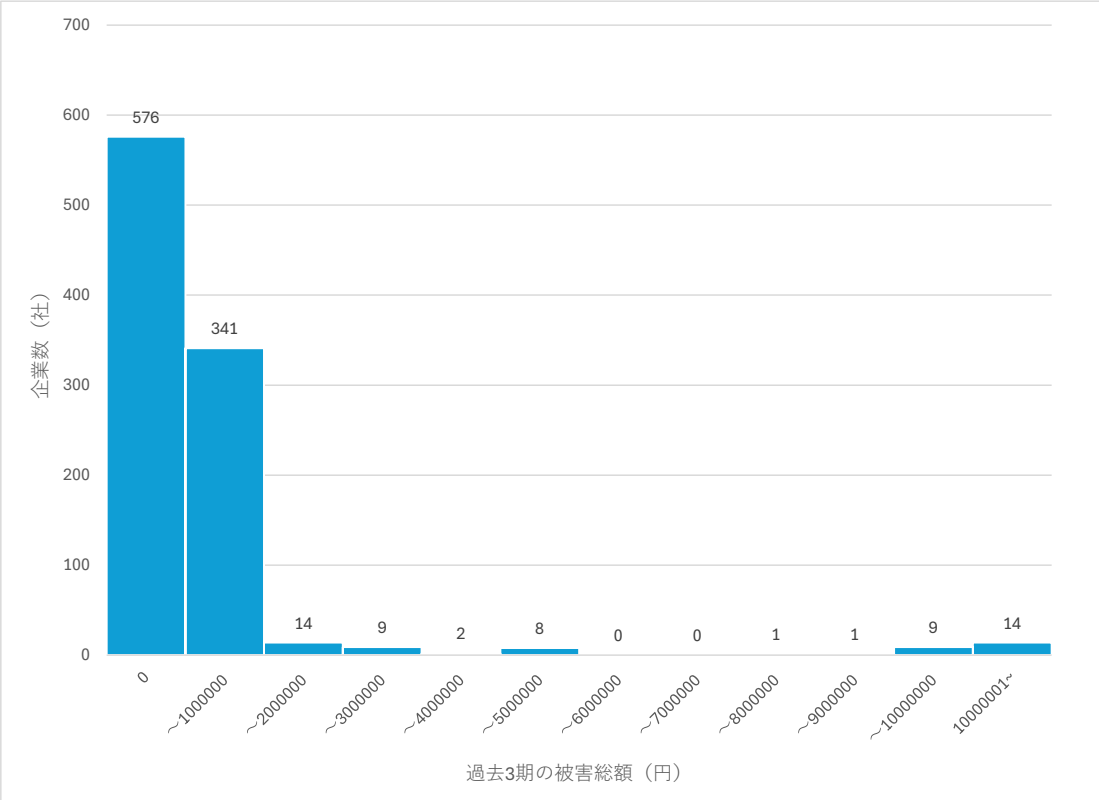

図 3-48 被害総額の分布（n=975）

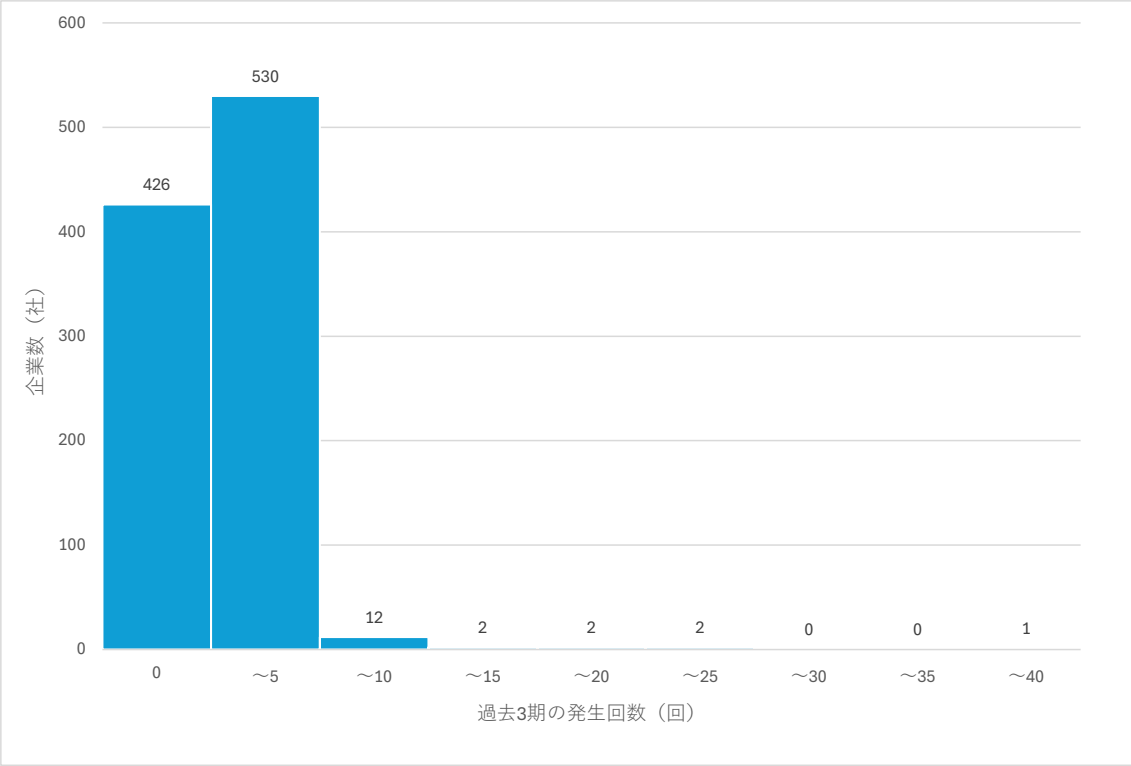

図 3-49 発生回数の分布（n=975）

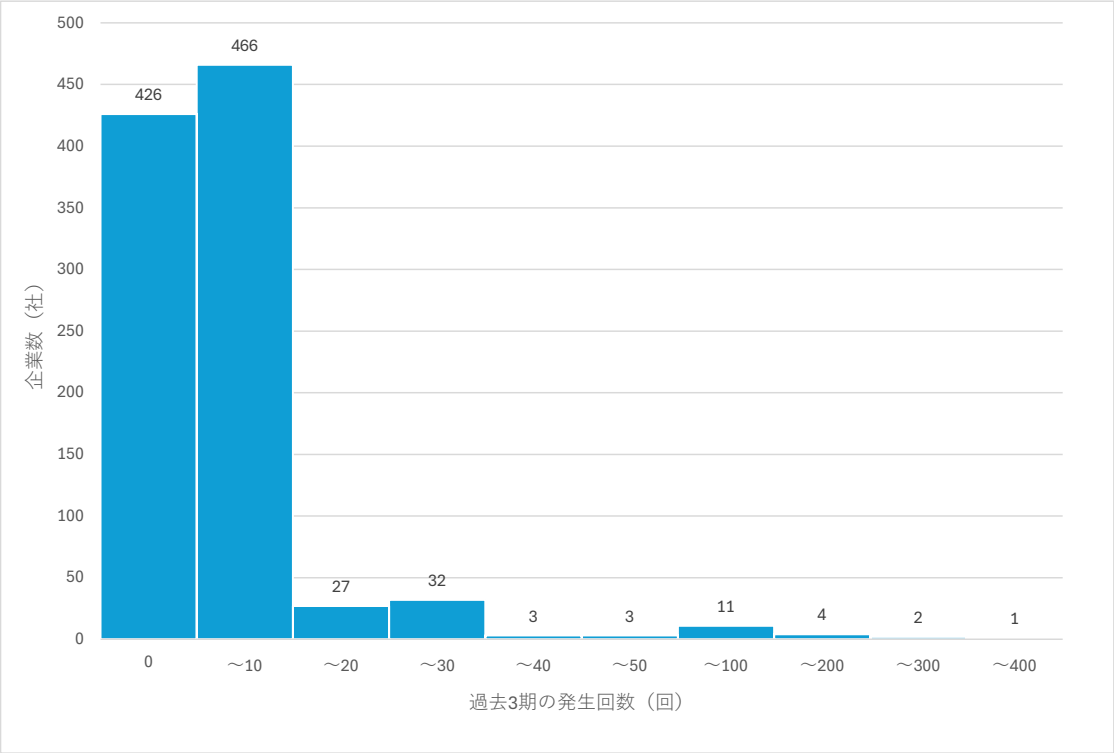

図 3-50 復旧期間の分布(n=975)

Q40.（Q34.で「被害にあっていない」以外のいずれかと回答された方について）サイバーインシデントの経験を踏まえて、情報セキュリティ対策を強化しましたか（当該被害経験は、対策を強化するきっかけとなりましたか）。（SA）

サイバーインシデントの経験を踏まえて、1 割強が情報セキュリティ対策を強化すると回答している。一方で 8 割強の企業は強化しないと回答しており、サイバーインシデントの経験が一時的な対応に留まっている実態が読み取れる。

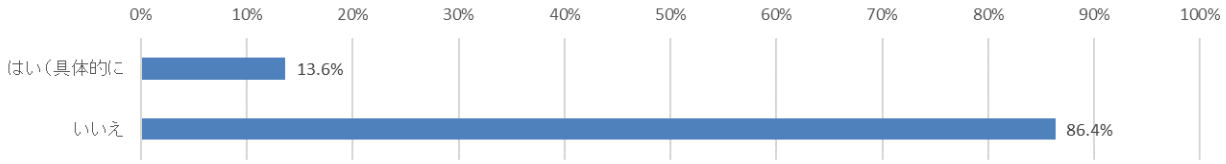

図 3-51 サイバーインシデントの経験を踏まえて、情報セキュリティ対策を強化したか(n=975)

3.2.7 取引先を含む情報セキュリティ対策

取引先との関係における情報セキュリティ上のリスクに関する設問と回答結果を記載する。

a. 他社との取引において、貴社の主要な事業に最も大きいリスクと考えていること

Q41. 他社との取引において、貴社の主要な事業に最も大きいリスクと考えていることを教えてください。（SA）

他社との取引において主要な事業に最も大きいリスクと考えていることとしては、機密性の高い情報（個人情報・設計図面等）（1,614 件）38.5%が最も多い。一方で、わからない（1,608 件）38.4%があるため、事業のリスクを認識できていない可能性もある。

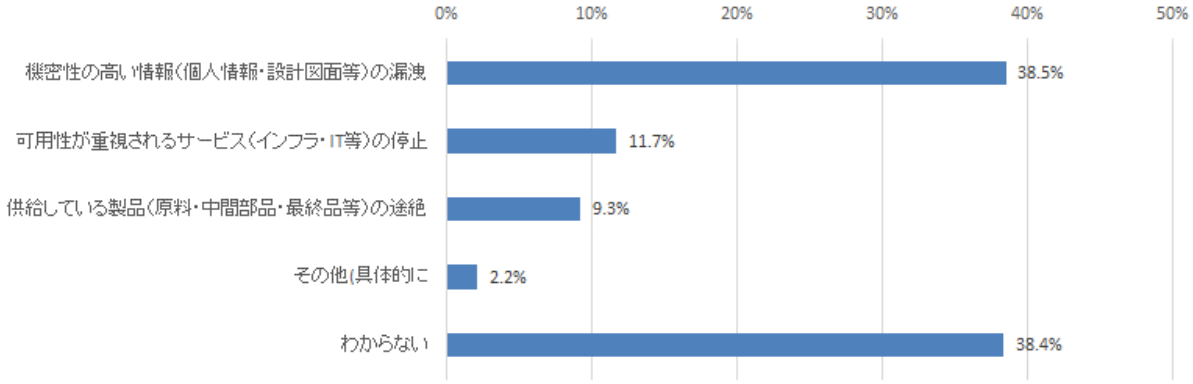

図 3-52 他社との取引で自社の主要な事業に最も大きいリスクと考えていること(n=4191)

b. 取引先でサイバーインシデントが発生した場合の、自社への影響

Q42. サイバーインシデントの影響により、Q41 で想定する事態が取引先で発生した場合、ビジネス的な観点で、貴社の主要な事業にどれほど影響がありますか。（SA）

【a】取引先が販売先（発注元企業）の場合

わからないと回答した企業を除くと、販売先（発注元企業）のサイバー攻撃により、自社の事業に多大な影響に及ぶと回答した企業が 20.9%存在して、最も大きな割合を占めた。

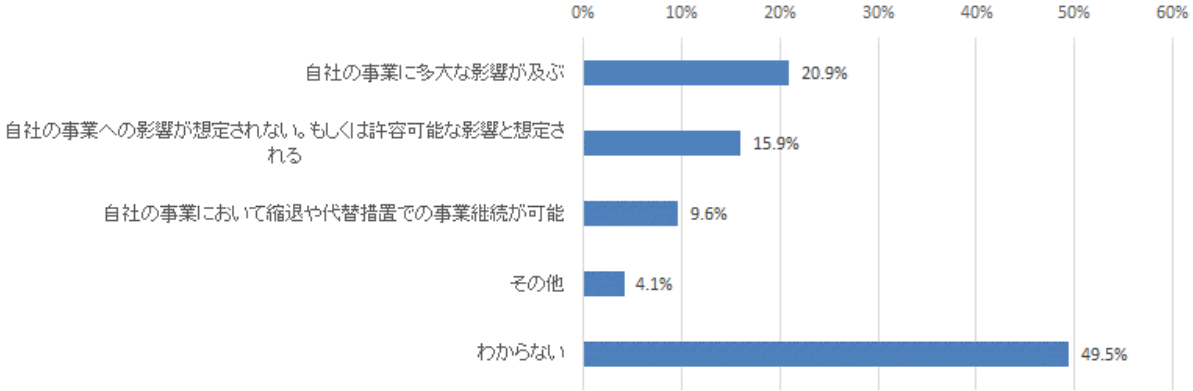

図 3-53 販売先（発注元企業）のサイバーインシデントが自社に及ぼす影響(n=4191)

【b】取引先が仕入先（委託・協力企業）の場合

わからないと回答した企業を除くと、仕入先（委託・協力企業）のサイバー攻撃により、自社の事業に多大な影響に及ぶと回答した企業が 17.8%存在して、最も大きな割合を占めた。

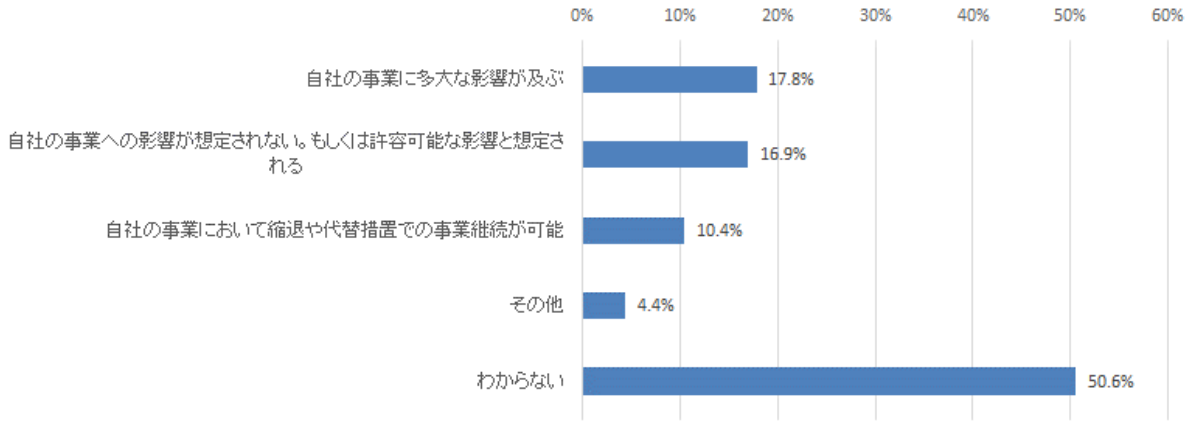

図 3-54 仕入先(委託・協力企業)のサイバーインシデントが自社に及ぼす影響(n=4191)

c. 自社でサイバーインシデントが発生した場合の、取引先への影響

Q43. サイバーインシデントの影響により、貴社で Q41 で想定する事態が発生した場合、ビジネス的な観点で、取引先の主要な事業にどれほど影響があると考えられますか。(SA)

【a】取引先が販売先(発注元企業)の場合

わからないと回答した企業を除くと、自社のサイバーインシデントにより、販売先(発注元企業)の事業に多大な影響に及ぶと回答した企業が 19.7%存在して、最も大きな割合を占めた。

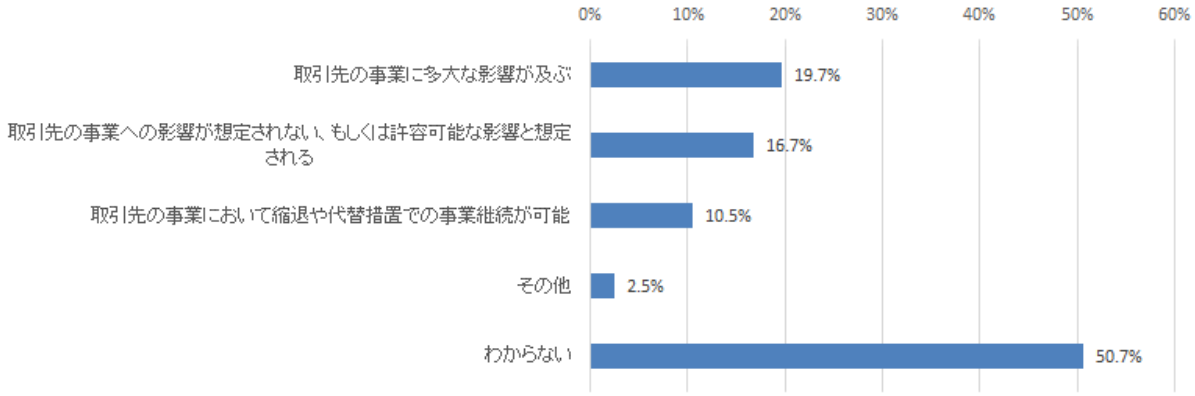

図 3-55 自社のサイバーインシデントが販売先(発注元企業)に及ぼす影響(n=4191)

【b】取引先が仕入先(委託・協力企業)の場合

わからないと回答した企業を除くと、自社のサイバーインシデントにより、仕入先(委託・協力企業)の事業への影響が想定されないと回答した企業が 18.5%存在して、最も大きな割合を占めた。

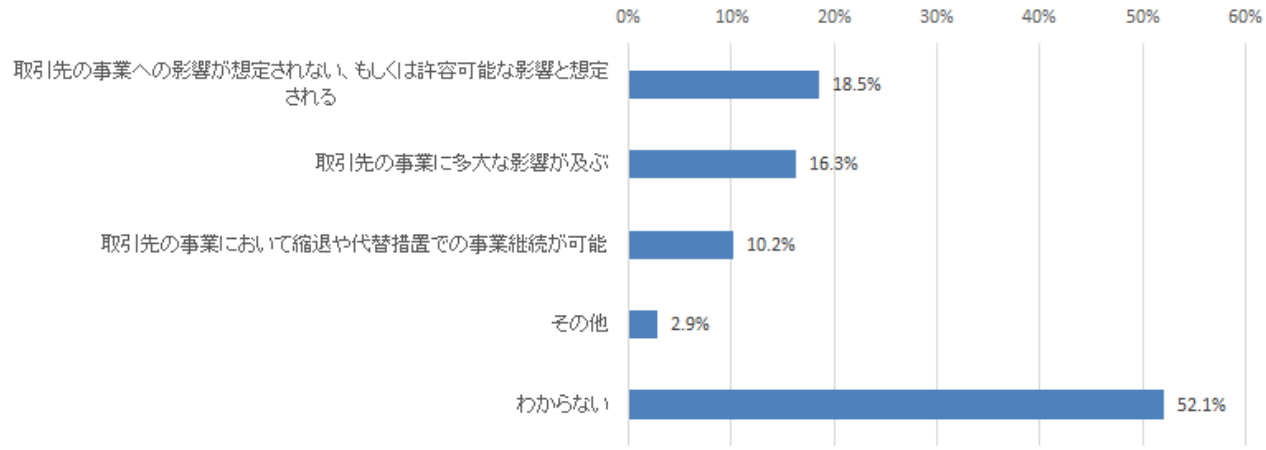

図 3-56 自社のサイバーインシデントが仕入先(委託・協力企業)に及ぼす影響(n=4191)

d. 取引先とのネットワーク接続状況

Q44. 貴社の社内ネットワークは販売先(発注元企業)や仕入先(委託・協力企業)のネットワークと接続していますか。(SA)
※ネットワーク接続の例:自社システムと取引先システムを連携するため WAN を経由したネットワーク接続など。

経営者や仕入先とネットワークを接続している企業はわずか 14.8%であり、サプライチェーン全体でのデジタルネットワーク連携が割合としては少ない。

取引先とのネットワーク接続について、約 8 割が「接続していない」と回答している。

取引先とのネットワーク接続の状況を「わからない」とする企業が 8.1%存在する。これは、ネットワークインフラの管理や情報セキュリティに関する情報が社内で十分に伝達されていない可能性がある。

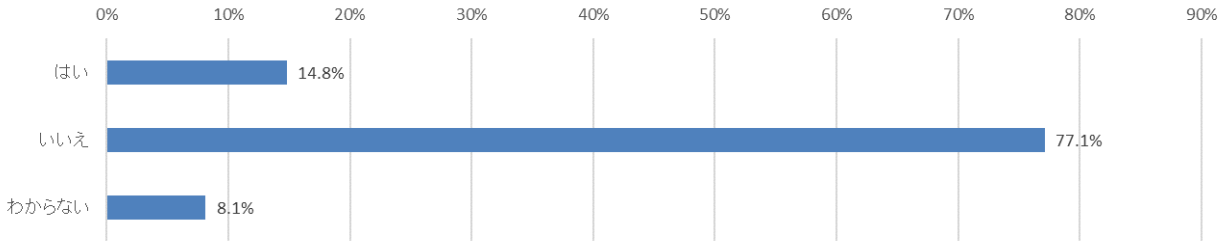

図 3-57 社内ネットワークは取引先のネットワークと接続しているか(n=4191)

Q45. (Q44.で「はい」と回答された方について)貴社は販売先(発注元企業)や仕入先(委託・協力企業)とのネットワーク接続がある場合、アクセス権限や範囲を適切に設定していますか。(SA)
※アクセス権限の例:取引先が貴社の社内ネットワークに接続するためのアカウントを付与してる場合など。

「はい(アカウントも付与している)」の回答が(406 件)65.5%と一番高く、次いで「はい(アカウントは付与していない)」が(121 件)19.5%となっている。なお、アカウントを付与している場合は、取引先のシステムが侵害された場合にネットワーク経由(付与しているアカウント経由)での社内ネットワーク侵害があり得るため、アクセス権限を適切に管理する必要がある。

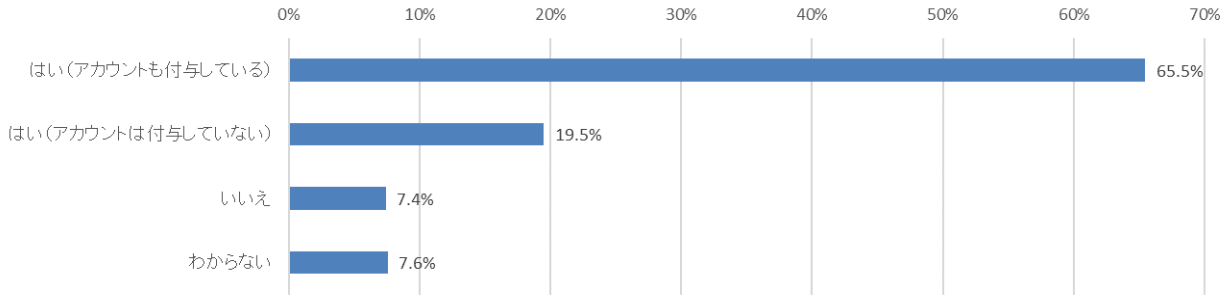

図 3-58 取引先とのネットワーク接続がある場合、アクセス権限や範囲を適切に設定しているか(n=620)

e. 販売先（発注元企業）からの情報セキュリティに関する要請と対応状況

Q46. 貴社は販売先（発注元企業）から貴社への情報セキュリティに関する要請を受けた経験はありますか。（SA）

全体の 1 割強が発注元企業から情報セキュリティに関する要請を受けた経験があると回答している。

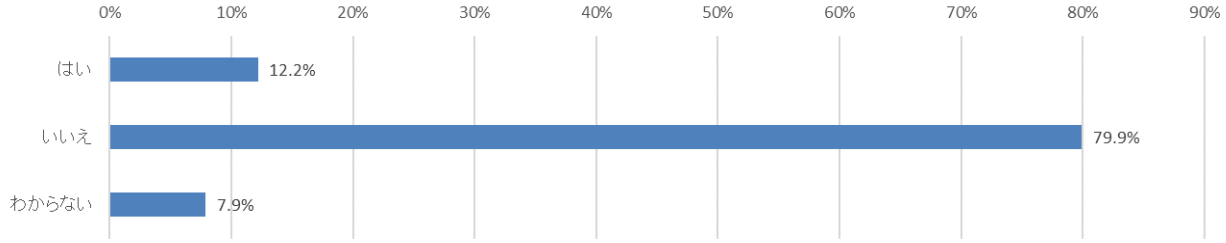

図 3-59 販売先（発注元企業）から情報セキュリティに関する要請を受けた経験(n=4191)

Q47. （Q46.で「はい」と回答された方について）販売先（発注元企業）から貴社への情報セキュリティに関する要請の具体的な内容について教えてください。あてはまるものを下記よりすべてお選びください。（MA）

情報セキュリティに関する要請の具体的な内容として、8 割近くが秘密保持を上げている。

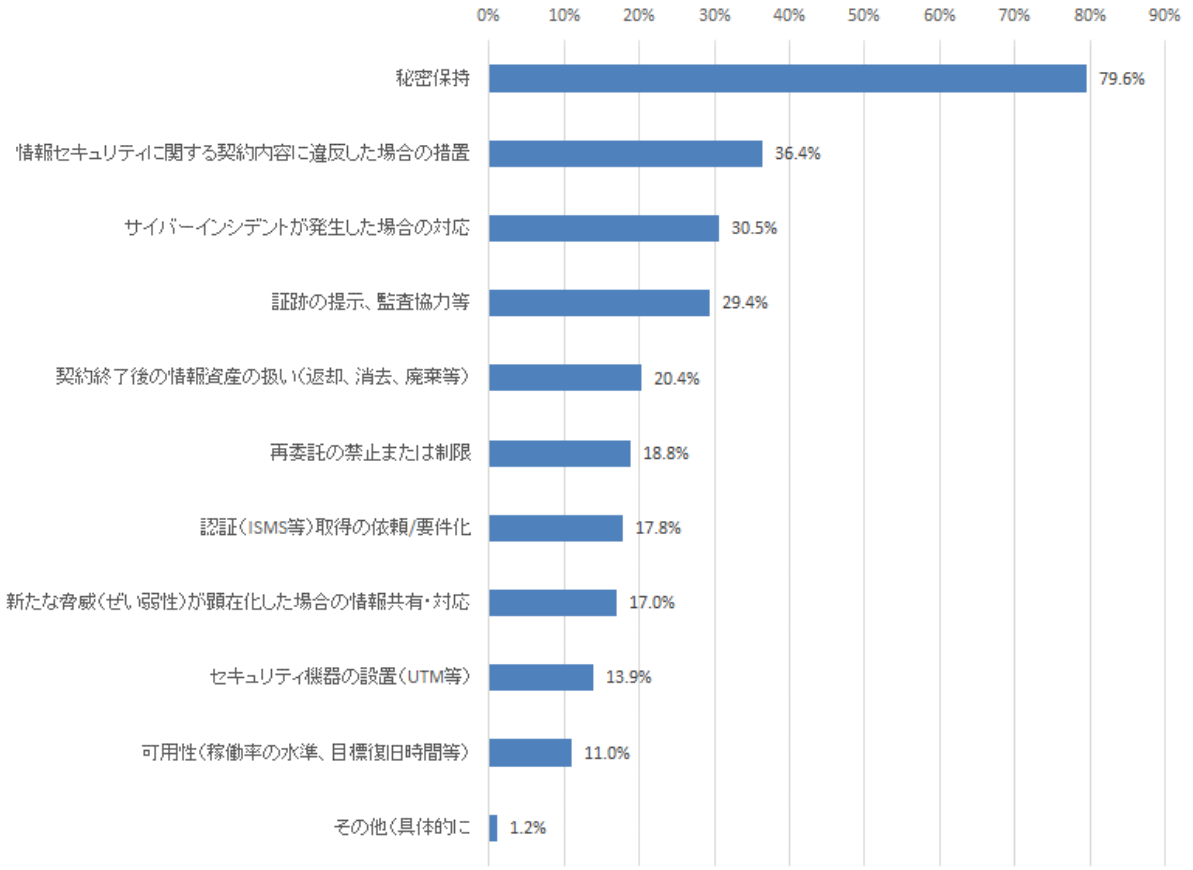

図 3-60 販売先(発注元企業)からの情報セキュリティに関する要請の具体的な内容(n=511)

Q48.(Q46.で「はい」と回答された方について)販売先(発注元企業)から貴社への情報セキュリティに関する要請に対して、貴社の行ったセキュリティ対策の具体的な内容について教えてください。またどの程度の費用が掛かりましたか。(SA)

情報セキュリティに関する要請に対して、セキュリティ対策を行ったとの回答が 2 割を超えている。費用が発生したものとしてはウイルス対策ソフト(約 20 万円)や UTM の導入(約 60 万円)、P マーク取得(約 120 万円)、社内研修の実施などが挙げられた。一方で、費用が発生しなかったものとしては、従業員への注意喚起、誓約書の提出、発注元負担での情報セキュリティに関する講座の受講などが挙げられた。

また、要請に対して、対策を行っていない企業が約55%みられた。サプライチェーン上での情報セキュリティの重要性が浸透していないと考えられる。

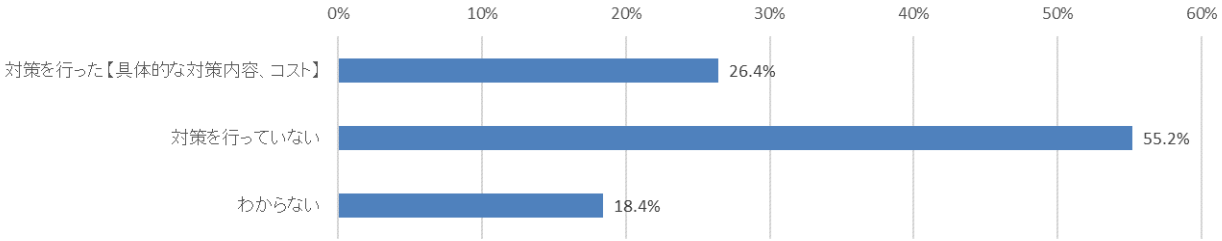

図 3-61 販売先(発注元企業)からの情報セキュリティに関する要請に対して行ったセキュリティ対策 (n=511)

Q49.（Q46.で「はい」と回答された方について）貴社は販売先（発注元企業）から要請された情報セキュリティ対策を行ったことが取引先との取引につながった大きな要因だと思いますか。（SA）

要請に基づき、情報セキュリティ対策を行ったことが取引に繋がった大きな要因だと考える企業は全体の 4 割強に上る。

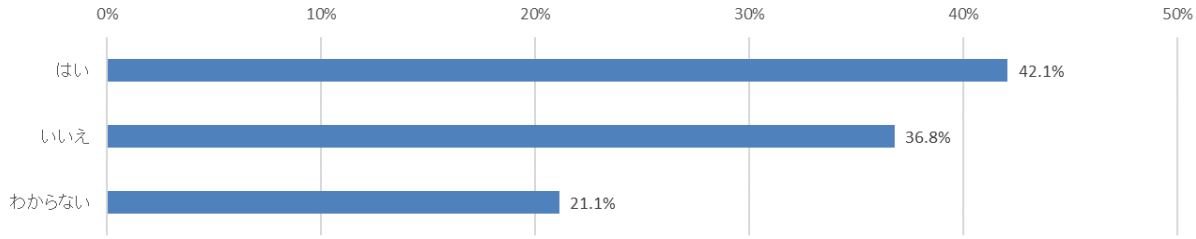

図 3-62 販売先（発注元企業）の要請に応じたことが取引につながった大きな要因か(n=511)

Q50.（Q46.で「はい」と回答された方について）貴社で販売先（発注元企業）から情報セキュリティ対策の要請を受けた場合に、対策の実施に向けての課題となることについて教えてください。（MA）

情報セキュリティ対策の要請を受けた場合に対策の実施に向けて課題となることとしては対策費用が 5 割強と多く、次いで契約の明確化（240 件）47.0%となっている。

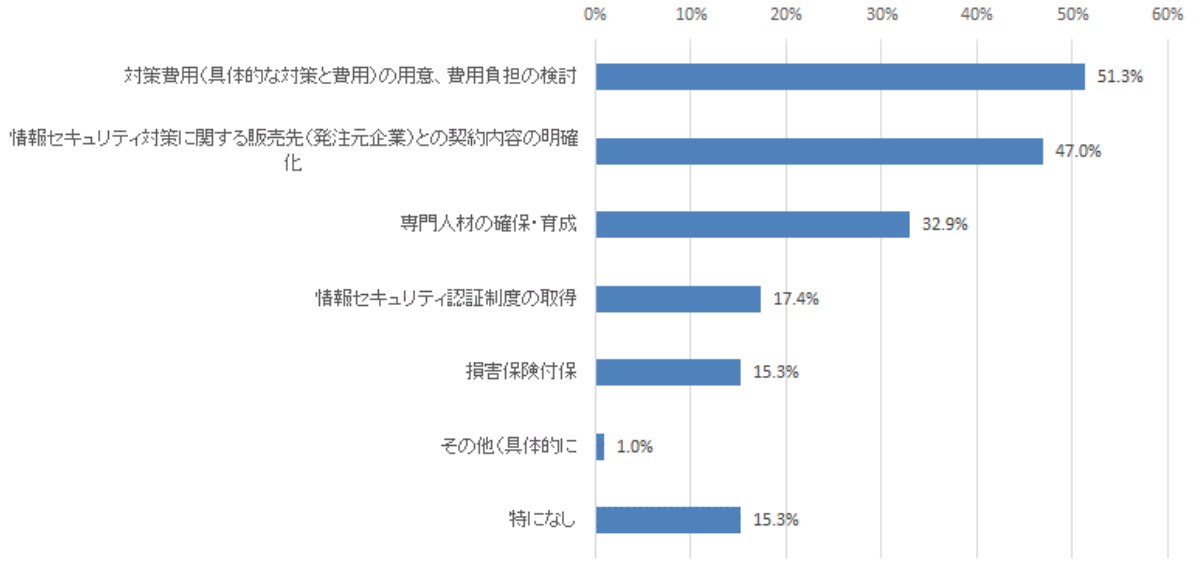

図 3-63 販売先（発注元企業）からの要請を受けた場合に、セキュリティ対策の実施に向けての課題 (n=511)

Q51.（Q46.で「はい」と回答された方について）販売先（発注元企業）からの情報セキュリティに関する要請・推奨に対応するための、貴社の費用負担について教えてください。（SA）

情報セキュリティに関する要請・推奨に対応するための費用負担としては、全額自社で負担しているとの回答が 6 割強に上る。

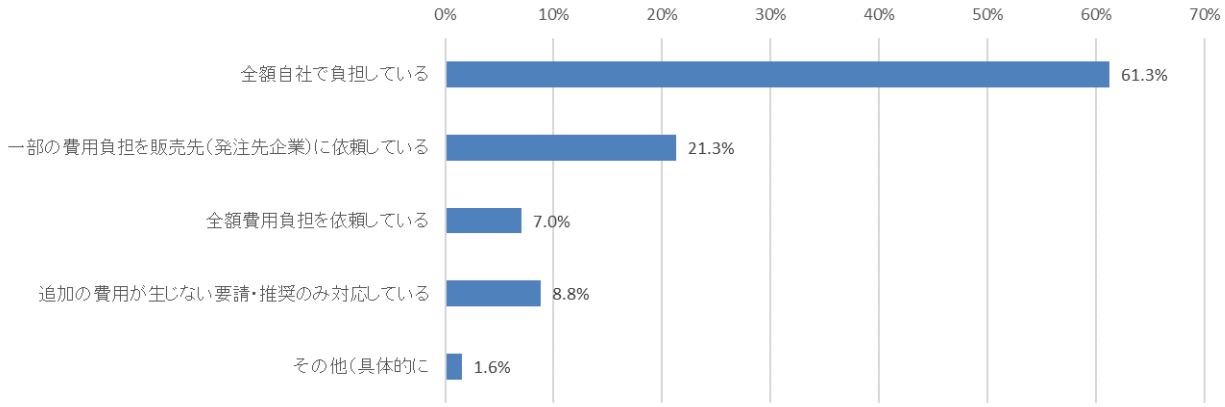

図 3-64 販売先(発注元企業)からの情報セキュリティに関する要請・推奨に対応する費用の負担(n=511)

Q52. (Q46.で「いいえ」と回答された方について)貴社では販売先(発注元企業)から情報セキュリティ対策の要請を受けたら対策を行いますか。(SA)

情報セキュリティ対策の要請を受けて対策を実施する際に、費用によると回答した企業は 4 割強に上る。一方で、いいえ(1098 件)が 32.8%があるため、費用に関わらず情報セキュリティ対策が行われない可能性もある。

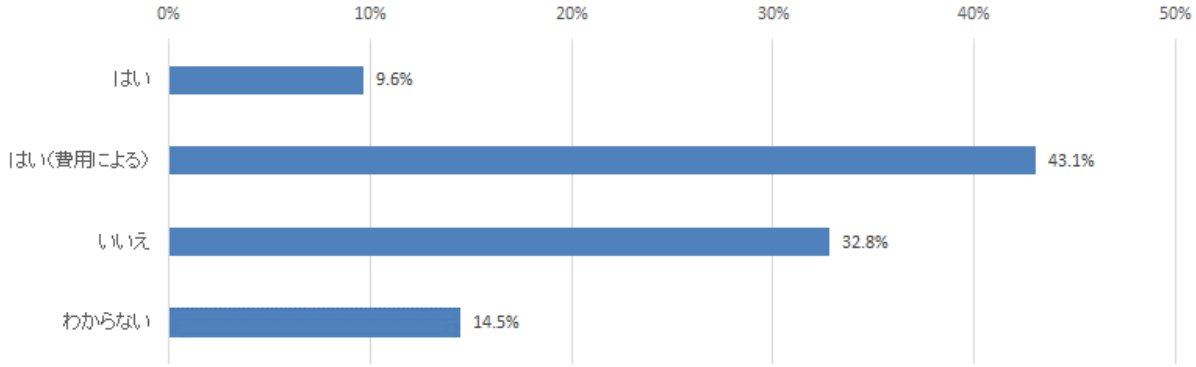

図 3-65 販売先(発注元企業)から情報セキュリティ対策の要請を受けたら対策を行うか(n=3350)

Q53. (Q46.で「いいえ」と回答された方について)貴社では販売先(発注元企業)から要請された情報セキュリティ対策を行わなかったことにより取引先との取引につながらなかったことがあると思いますか。(SA)

要請された情報セキュリティ対策を行わなかったことで取引につながらなかったと回答している企業は全体の 3%程度に留まる。

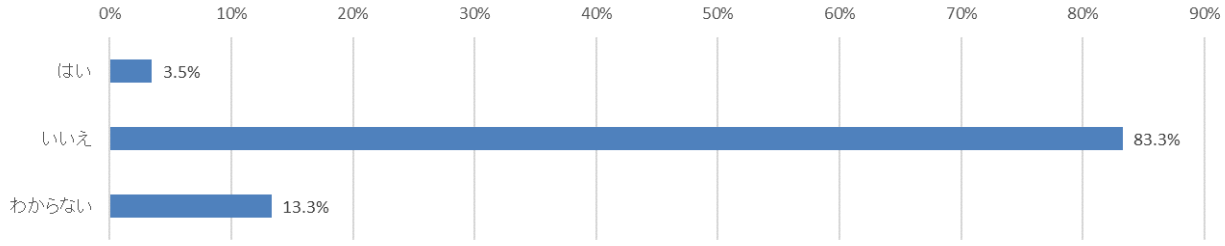

図 3-66 販売先(発注元企業)からの要請に応じなかったことで取引につながらなかったか(n=3350)

Q54.（Q46.で「いいえ」と回答された方について）貴社では販売先（発注元企業）から「情報セキュリティ対策を行わない企業とは取引できない」と言われた場合、対策を行うと思いますか。（SA）

情報セキュリティ対策が取引の前提となる場合に対策を行うと回答した企業は全体の 3 割強に上る。一方で対策を行わないと回答した企業は 4 割になる。

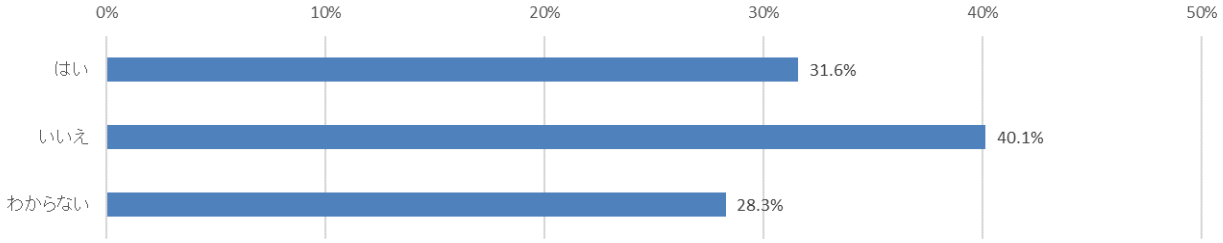

図 3-67 「情報セキュリティ対策を行わない企業とは取引できない」と言われた場合の対応(n=3350)

f. 仕入先（委託・協力企業）に対する情報セキュリティに関する要請と対応状況

Q55. 貴社は仕入先（委託・協力企業）に対してセキュリティ対策の要請をしたことがありますか。（SA）

仕入先に対してセキュリティ対策の要請をしたことがある企業は全体の 1 割未満である。

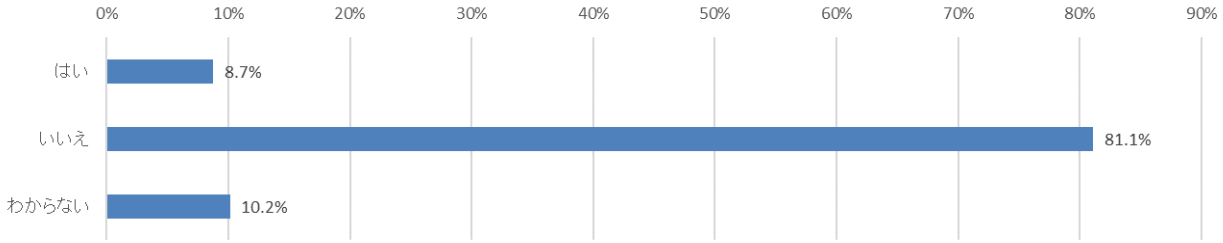

図 3-68 仕入先（委託・協力企業）に対してセキュリティ対策の要請をしたことがあるか(n=4191)

Q56.（Q55.で「はい」と回答された方について）仕入先（委託・協力企業）は要請に応じましたか。（SA）

要請したセキュリティ対策に仕入れ先が応じたと回答した企業は全体の 8 割強に上る。

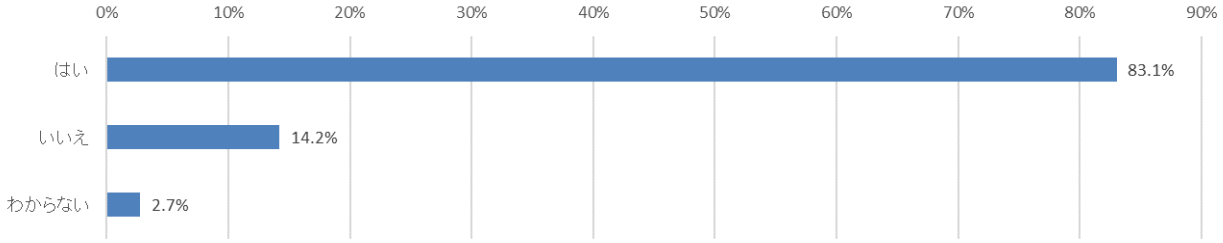

図 3-69 仕入先（委託・協力企業）は要請に応じたか(n=366)

Q57.（Q56.で「はい」と回答された方について）前問で仕入先（委託・協力企業）は要請に応じたかの設問に「はい」とお答えになった方にお伺いします。貴社では要請した情報セキュリティ対策を取引先が行ったことが取引先との取引につながった大きな要因だったと思いますか。（SA）

仕入れ先が情報セキュリティ対策に応じたことが取引に繋がった大きな要因だったと思う企業は全体

の 7 割に上る。

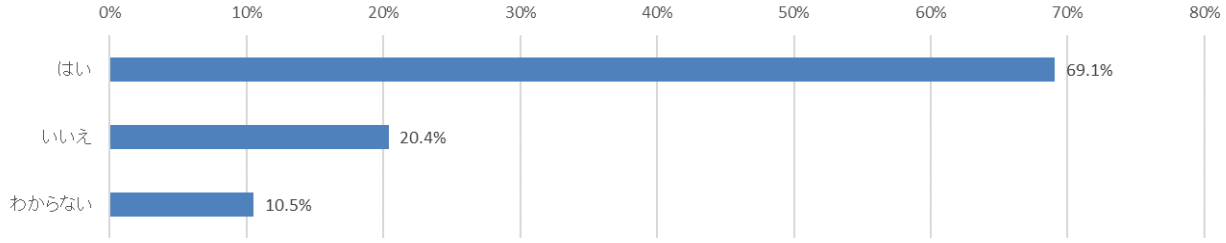

図 3-70 仕入先(委託・協力企業)が要請に応じたことが取引につながらなかった大きな要因か(n=304)

Q58.(Q56.で「いいえ」と回答された方について)前問で仕入先(委託・協力企業)は要請に応じたかの設問に「いいえ」とお答えになった方にお伺いします。貴社では要請した情報セキュリティ対策を取引先が行わなかったことが取引先との取引につながらなかった大きな要因と思うことがありましたか。(SA)

仕入先が要請した情報セキュリティ対策を行わなかったことにより取引が成立しなかったと回答している企業は全体の 5 割に上る。

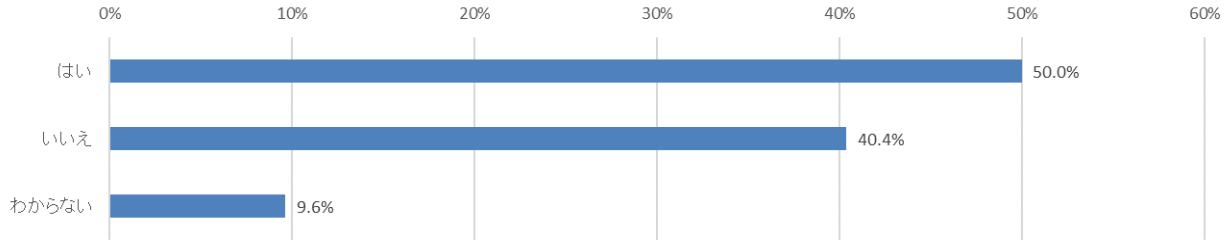

図 3-71 仕入先(委託・協力企業)が要請に応じなかったことは取引につながらなかった大きな要因か (n=52)

Q59.(Q55.で「はい」と回答された方について)貴社では仕入先(委託・協力企業)への情報セキュリティ対策を要請するための貴社のガイドライン等はありますか。(SA)

仕入先への情報セキュリティ対策を要請するためのガイドラインがあると回答している企業は全体の 6 割強に上る。

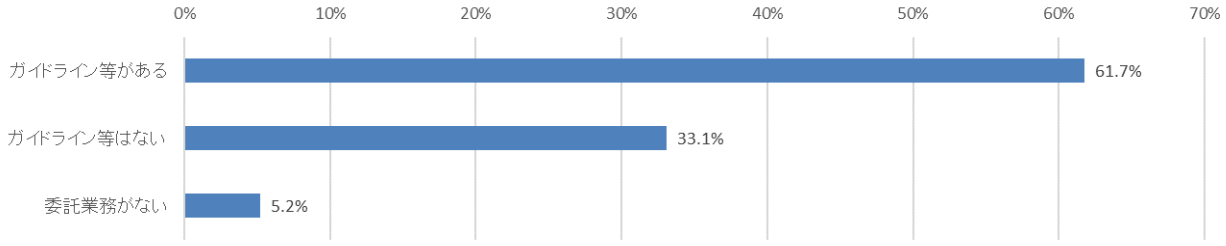

図 3-72 仕入先(委託・協力企業)への情報セキュリティ対策を要請するためのガイドライン等(n=366)

3.2.8 「SECURITY ACTION」の宣言状況

回答企業の「SECURITY ACTION」に関する認識と宣言状況に関する設問と回答結果を記載する。

Q60. 貴社は IPA の施策である「SECURITY ACTION」という制度を知っていますか。
「SECURITY ACTION」は中小企業自らが、情報セキュリティ対策に取組むことを自己宣言する制度です。（SA）
参照：https://www.ipa.go.jp/security/SECURITY ACTION/

「SECURITY ACTION」を認知している企業は全体の 1 割程度に留まる。

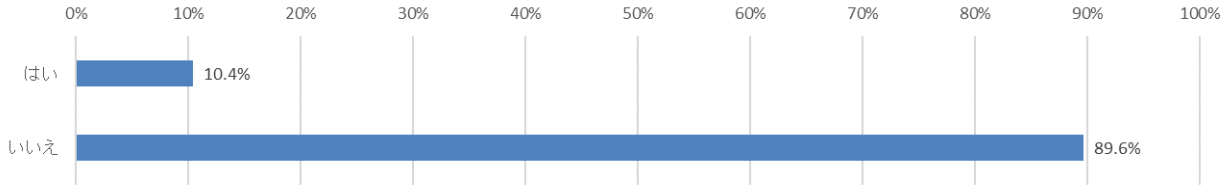

図 3-73 「SECURITY ACTION」制度の認知状況(n=4191)

Q61.（Q60.で「はい」と回答した方について）貴社は「SECURITY ACTION」の一つ星（または二つ星）を宣言していますか。（SA）

「SECURITY ACTION」を認知している企業の内、一つ星または二つ星を宣言している企業は 6 割弱に上る。

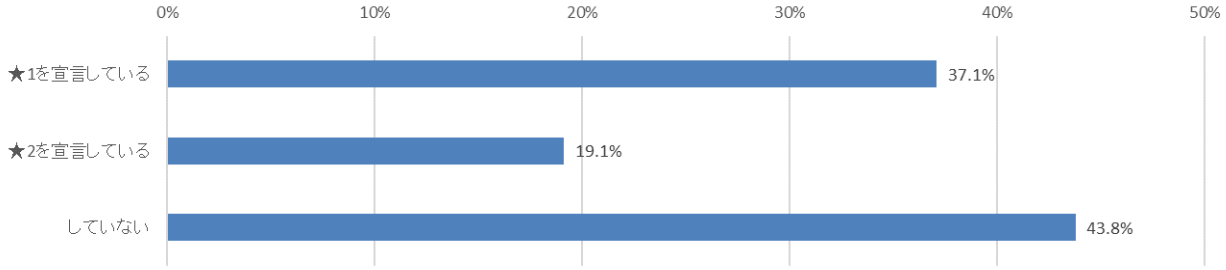

図 3-74 「SECURITY ACTION」の宣言状況(n=434)

Q62.（Q61.で「★1 を宣言している」あるいは「★2 を宣言している」と回答された方について）貴社が「SECURITY ACTION」の宣言を行ったきっかけを教えてください。あてはまるものを下記よりすべてお選びください。（MA）

「SECURITY ACTION」の宣言を行ったきっかけとして、補助金や助成金の申請要件（134 件）54.9%がもっと多く、次いで顧客や取引先からの要求（118 件）48.4%となる。

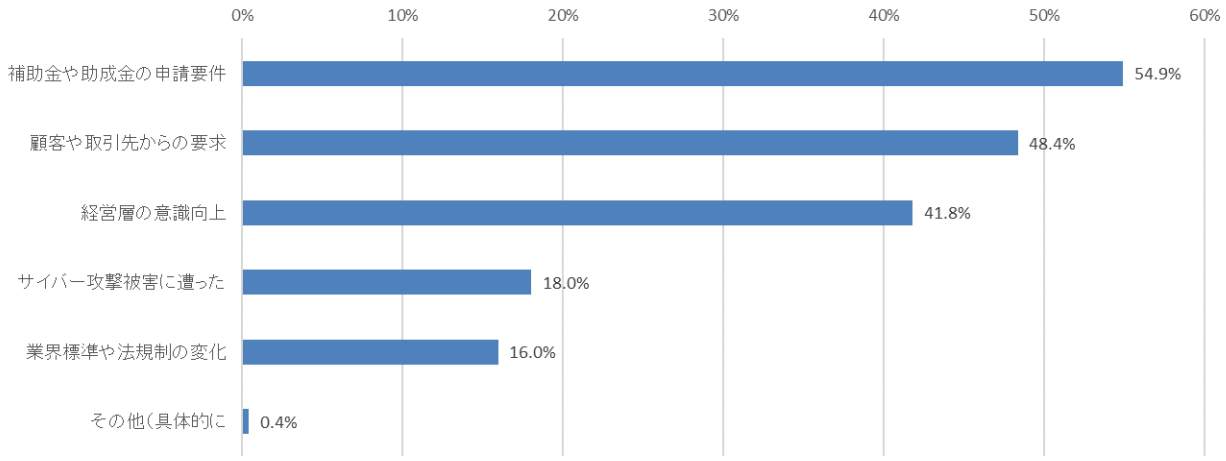

図 3-75 「SECURITY ACTION」の宣言を行ったきっかけ(n=244)

Q63.（Q61.で「★1 を宣言している」あるいは「★2 を宣言している」と回答された方について）「SECURITY ACTION」の宣言に関して、貴社の現在の状況を教えてください。（SA）

「SECURITY ACTION」を宣言した企業が、宣言した状態を維持できていると回答した割合は全体の 9 割近くに上る。

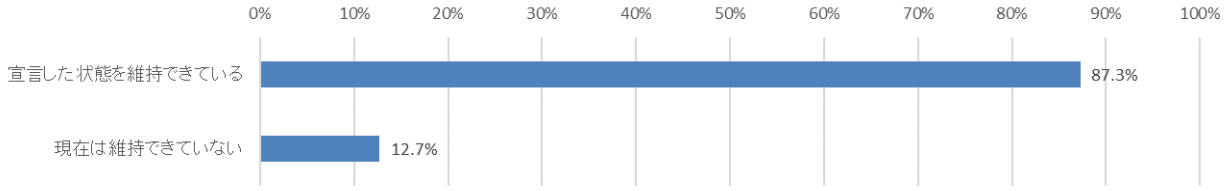

図 3-76 「SECURITY ACTION」を宣言した後、現在の状況(n=244)

Q64.（Q61.で「★1 を宣言している」あるいは「★2 を宣言している」と回答された方について）「SECURITY ACTION」の宣言に関して、各項目を維持してくために貴社で必要となることを教えてください。あてはまるものを下記よりすべてお選びください。（MA）

「SECURITY ACTION」の宣言を維持していくために必要であることとして、予算の確保（137 件）56.1%、専門知識を持った人材の確保（136 件）55.7%が多く、次いで経営層の関与（98 件）40.2%となる。

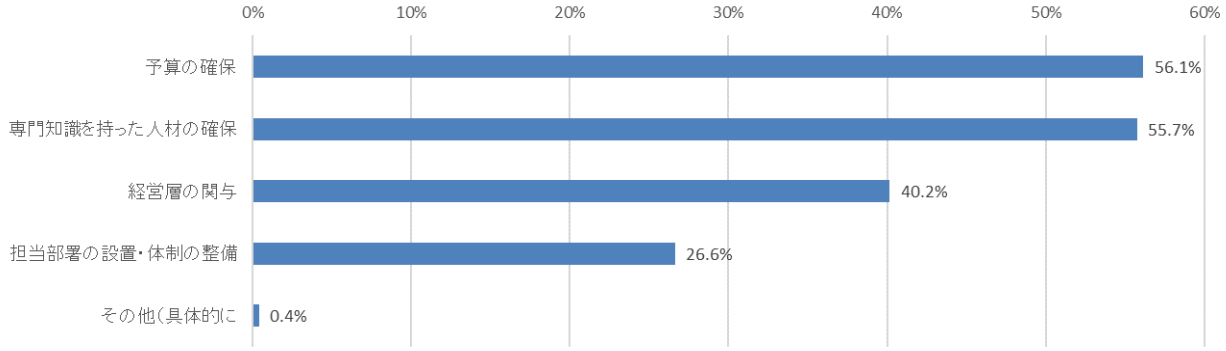

図 3-77 「SECURITY ACTION」の宣言を維持していくために必要となること(n=244)

Q65.（Q63.で「現在は維持できていない」と回答された方について）貴社が「SECURITY ACTION」の宣言を維持できなかった理由を教えてください。あてはまるものを下記よりすべてお選びください。（MA）

「SECURITY ACTION」の宣言を維持できなかった理由として、専門知識の不足（17 件）54.8%、コストが高い（14 件）45.2%、情報セキュリティへの意識が低い（10 件）32.3%の順で多い。

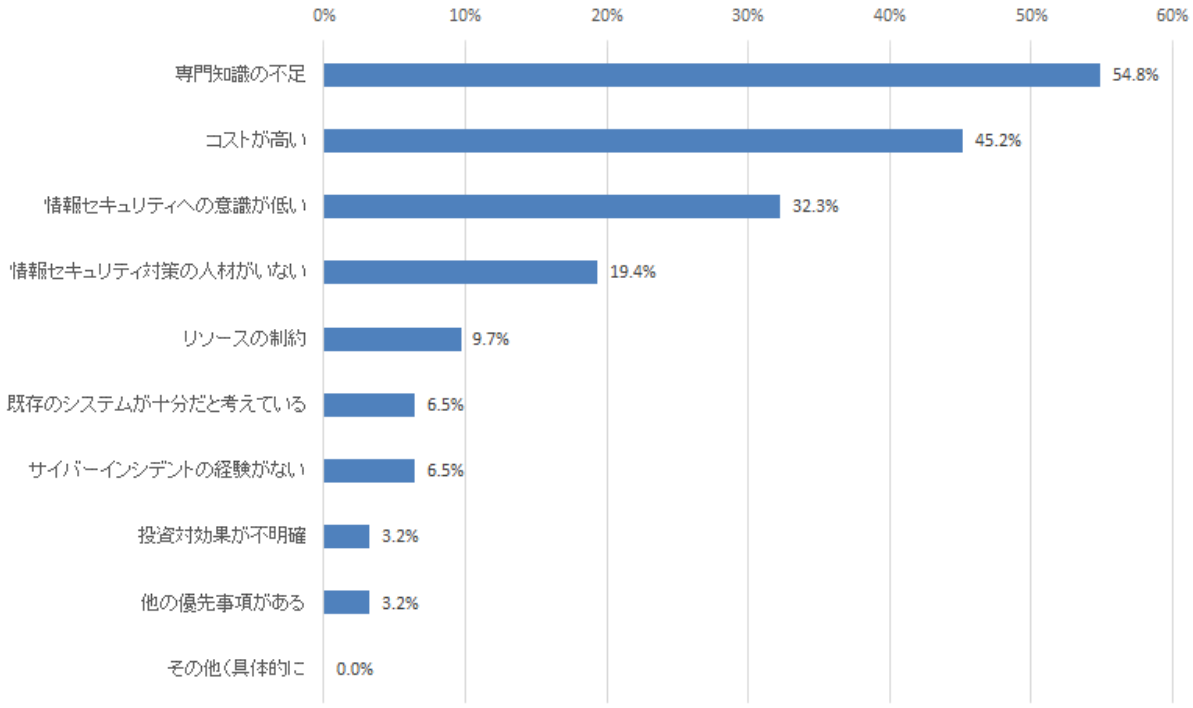

図 3-78 「SECURITY ACTION」の宣言を維持できなかった理由(n=31)

Q66.（Q61.で「★1 を宣言している」あるいは「★2 を宣言している」と回答された方について）貴社の職員から「SECURITY ACTION」の取組状況は確認できますか。（SA）

「SECURITY ACTION」の取り組み状況が確認できると回答した企業の割合は、7 割弱となる。

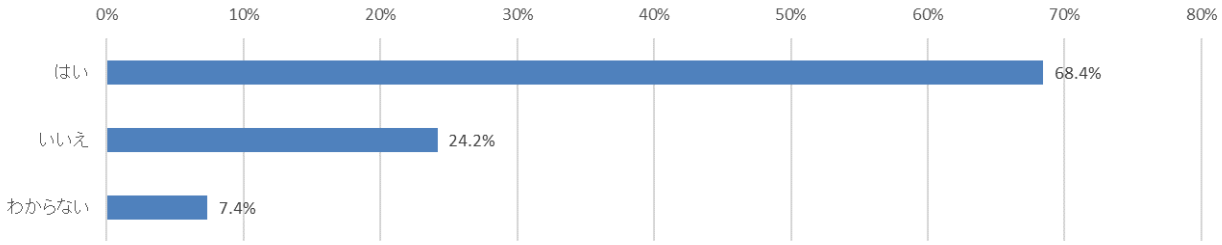

図 3-79 職員から「SECURITY ACTION」の取組状況は確認できますか(n=244)

Q67.（Q66.で「いいえ」と回答された方について）貴社の職員から「SECURITY ACTION」の取組状況を確認できない理由は教えてください。（MA）

「SECURITY ACTION」の取り組み状況を確認できない理由として共有するためのシステムがないと回答した割合が全体の 7 割強に上る。

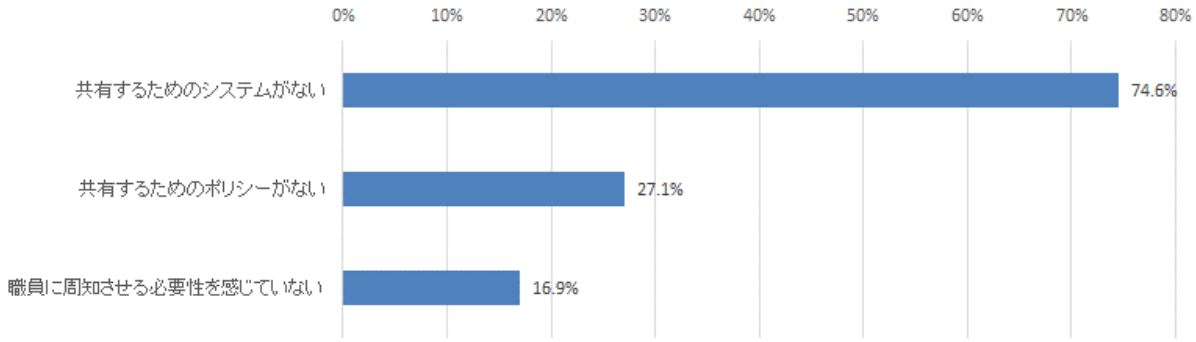

図 3-80 職員から「SECURITY ACTION」の取組状況を確認できない理由(n=59)

Q68.（Q60.で「いいえ」または Q66.で「わからない」と回答された方について）貴社が「SECURITY ACTION」の宣言を実施していない理由を教えてください。あてはまるものを下記よりすべてお選びください。（MA）

「SECURITY ACTION」の宣言を実施していない理由として、知らなかった（1,523 件）38.6%が最も多い。これにより、制度自体の認知度が低く、多くの企業がその存在を知らないために導入を考えていないことが示唆されている。

28.5%の企業が「必要性を感じられない」と回答しており、サイバーセキュリティに対する重要性の認識が不足している可能性がある。企業におけるセキュリティ意識の向上が求められる。

「リソース不足」および「情報セキュリティ対策を実施できる人材がいない」とする企業がそれぞれ 14.0%と 14.1%であり、人的リソースの制約が大きな課題として認識されていることがわかる。

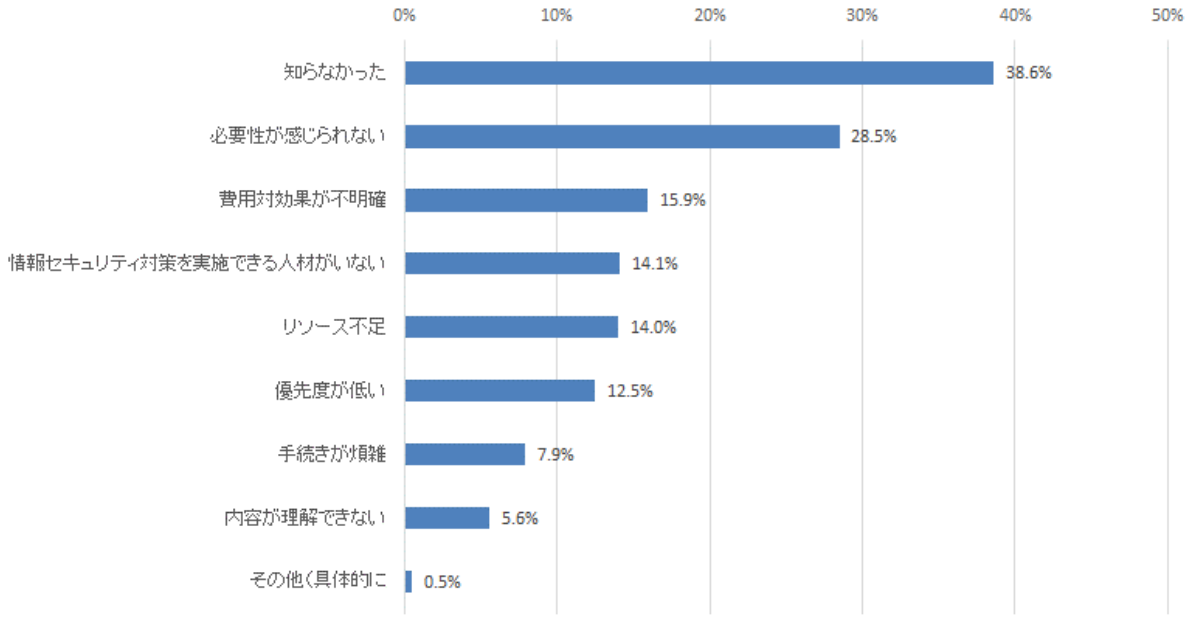

図 3-81 「SECURITY ACTION」の宣言を実施していない理由(n=3947)

Q69.（Q60.で「いいえ」または Q66.で「わからない」と回答された方について）「SECURITY ACTION」は中小企業自らが、情報セキュリティ対策に取組むことを自己宣言する制度です。貴社はどのようなきっかけがあれば宣言を行うか教えてください。あてはまるものを下記よりすべてお選びください。（MA）

「SECURITY ACTION」を宣言するきっかけとなり得るものとして、顧客や取引先からの要求

(1,392 件)35.3%が最も高く、次いで対応できる人材がいれば実施できる(1,062 件)26.9%となっている。

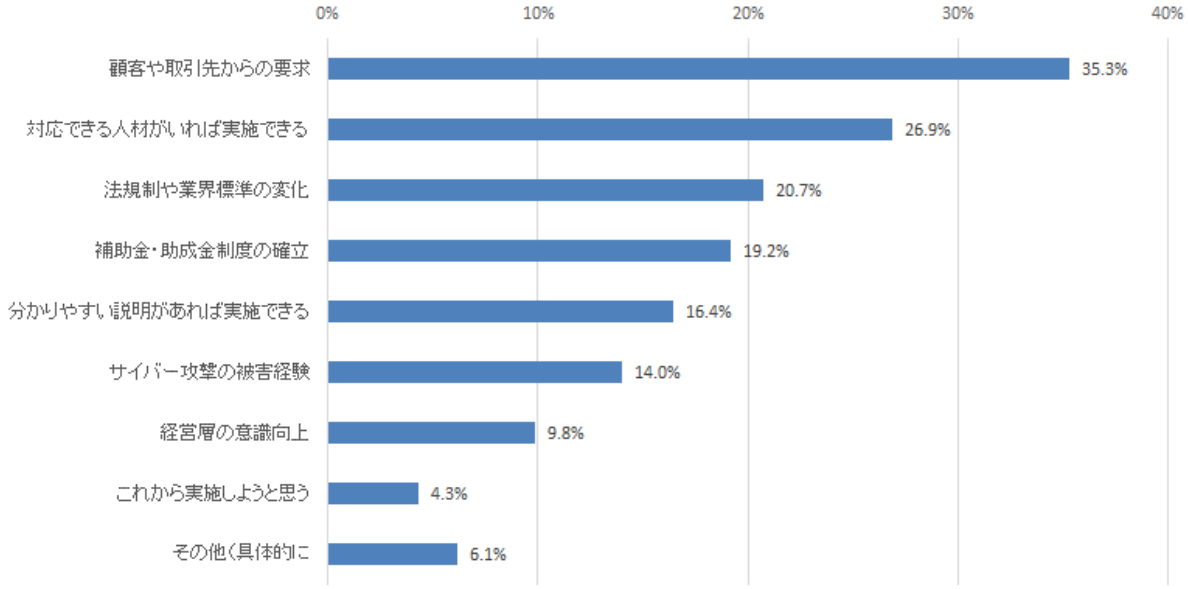

図 3-82 どのようなきっかけがあれば「SECURITY ACTION」の宣言を行うか(n=3947)

3.2.9 「サイバーセキュリティお助け隊サービス」の導入状況

回答企業の「サイバーセキュリティお助け隊サービス」に関する知識と導入状況に関する設問と回答を記載する。

Q70. 独立行政法人情報処理推進機構(IPA)が実施している「サイバーセキュリティお助け隊サービス制度」をご存じですか。(SA)
参照:https://www.ipa.go.jp/security/otasuketai-pr/

「サイバーセキュリティお助け隊サービス制度」を知っていると回答した企業の割合は 1 割弱に留まる。

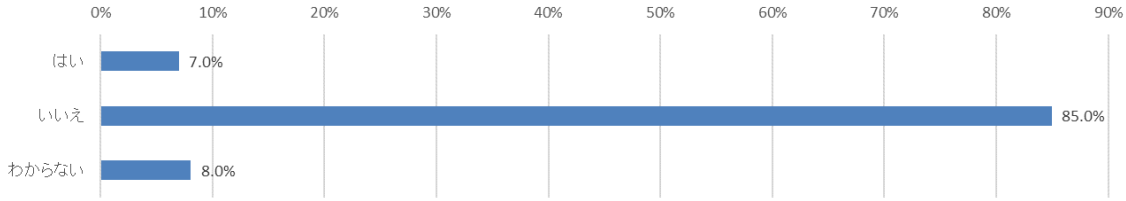

図 3-83 「サイバーセキュリティお助け隊サービス制度」をご存じですか(n=4191)

Q71. (Q70.で「はい」と回答された方について)貴社は「サイバーセキュリティお助け隊サービス」を導入されていますか。(SA)

「サイバーセキュリティお助け隊サービス制度」を知っていると回答した企業の内、導入していると回答した企業の割合は 3 割強に留まる。

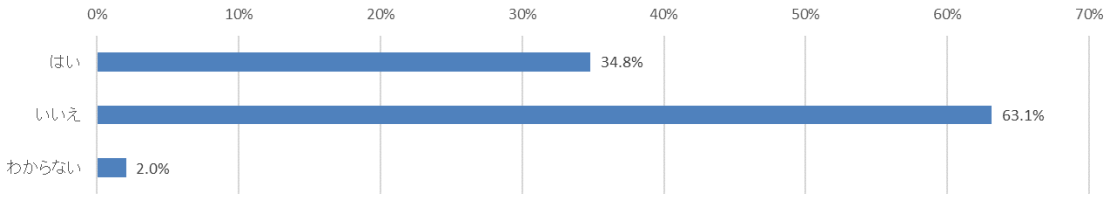

図 3-84 「サイバーセキュリティお助け隊サービス」を導入されていますか(n=293)

Q72.（Q71.で「はい」と回答された方について）貴社が「サイバーセキュリティお助け隊サービス」を導入したきっかけについて教えてください。あてはまるものを下記よりすべてお選びください。（MA）

「サイバーセキュリティお助け隊サービス制度」を知っていると回答した企業の内、導入したきっかけとして補助金や助成金の申請要件との回答が 6 割強に上る。次いで、顧客や取引先からの要求が 5 割強となっている。

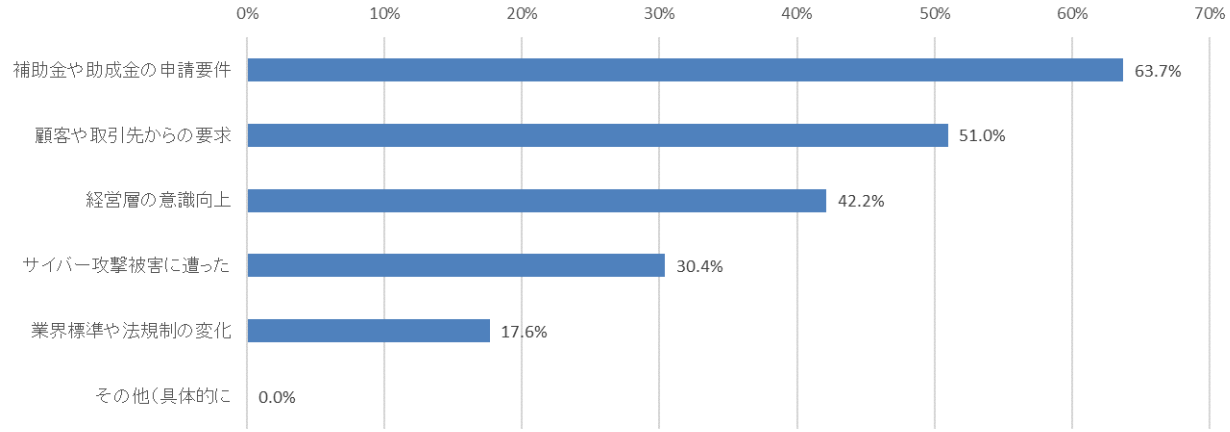

図 3-85 「サイバーセキュリティお助け隊サービス」を導入したきっかけ(n=102)

Q73.（Q71.で「はい」と回答された方について）貴社が「サイバーセキュリティお助け隊サービス」を導入して良かった点を教えてください。あてはまるものを下記よりすべてお選びください。（MA）

「サイバーセキュリティお助け隊サービス制度」導入してよかった点としては、ワンパッケージでの情報セキュリティ対策（58 件）56.9%、導入が容易（57 件）55.9%が多い。

一方でコストの削減（37 件）36.3%との回答があり、サービスの導入によりコスト削減となっているケースがあることが読み取れる。

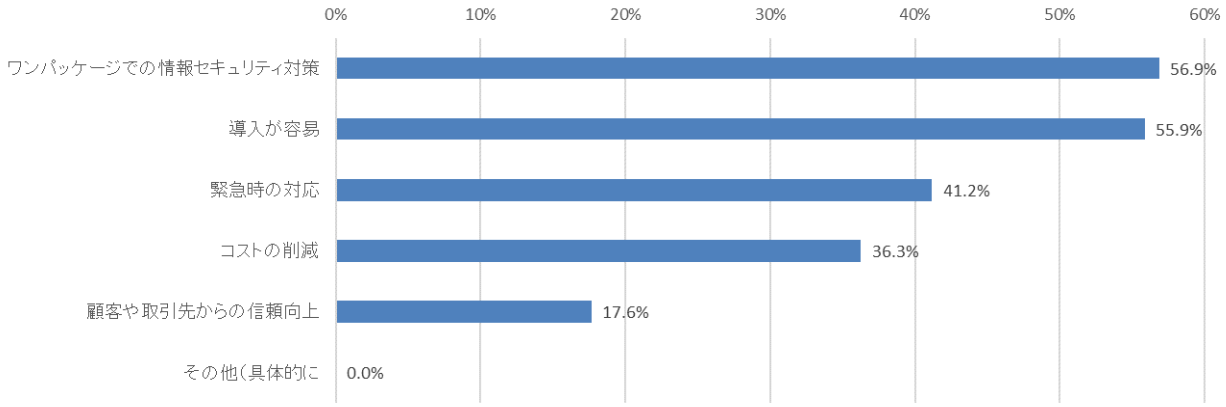

図 3-86 「サイバーセキュリティお助け隊サービス」を導入して良かった点(n=102)

Q74.（Q71.で「いいえ」と回答された方について）貴社が「サイバーセキュリティお助け隊サービス」を導入しない理由を教えてください。あてはまるものを下記よりすべてお選びください。（MA）

「サイバーセキュリティお助け隊サービス制度」を導入していないと回答した企業の内、その理由として費用対効果が不明確（61 件）33.0%が最も多く、次いでリソース不足（55 件）29.7%となっている。

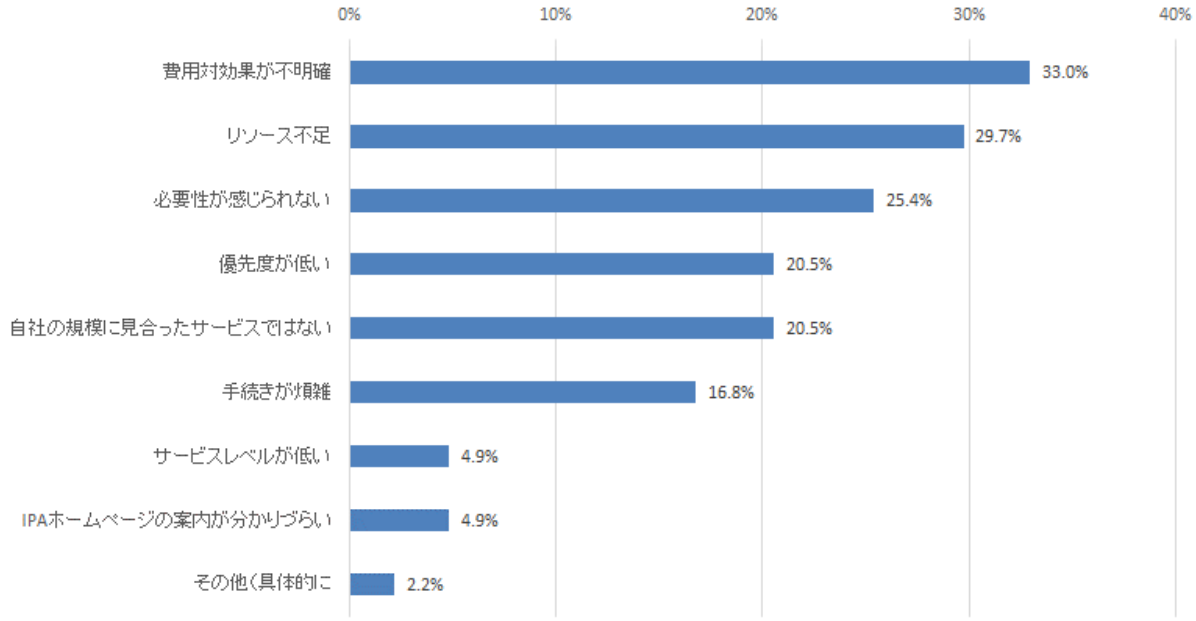

図 3-87 「サイバーセキュリティお助け隊サービス」を導入しない理由(n=185)

Q75.（Q70.で「いいえ」と回答された方について）「サイバーセキュリティお助け隊サービス」は、中小企業の情報セキュリティ対策に不可欠な各種サービス（相談窓口、システムの異常監視、緊急時の対応支援、簡易サイバー保険など）をワンパッケージで安価に提供するサービスです。「サイバーセキュリティお助け隊サービス」を導入したいと思いますか？（SA）

「サイバーセキュリティお助け隊サービス制度」を知らないと回答した企業について、サービス内容を知っても導入する意思がある企業は 1 割未満となっている。一方で分からないと回答した企業は全体の

3 割強であり、サービス内容のより丁寧な説明が必要と考えられる。

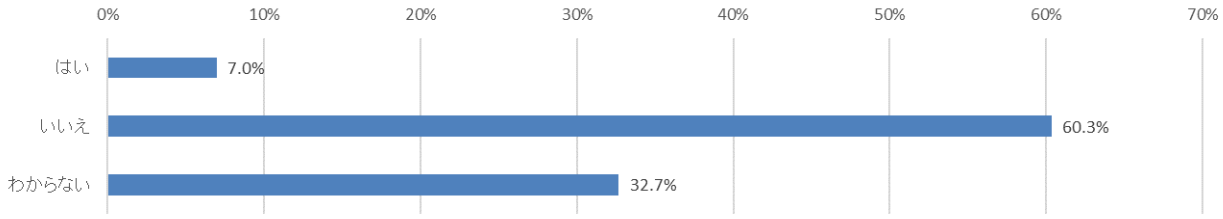

図 3-88 「サイバーセキュリティお助け隊サービス」を導入したいと思いますか(n=3561)

Q76.（Q75.で「いいえ」と回答された方について）貴社が「サイバーセキュリティお助け隊サービス」を導入したいと思わない理由は何ですか。あてはまるものを下記よりすべてお選びください。（MA）

サイバーセキュリティお助け隊サービスを導入したいと思わない理由として、必要性が感じられない企業が 46.9%と最も多く、セキュリティリスクの認識が十分でないことが示唆される。企業にとってこのサービスの価値をより明確化する必要がある。

費用対効果が不明確であるとの理由で導入を躊躇する企業が 27.2%に上る。これは、サービスの具体的な効果やコストの明示が不足していることを意味し、より透明性のある情報提供が求められる。

優先度が低いとする企業が 19.8%に達しており、緊急性や必要性が十分に認識されていないことがうかがえる。セキュリティの重要性とその企業運営への影響を強調する教育が不可欠である。

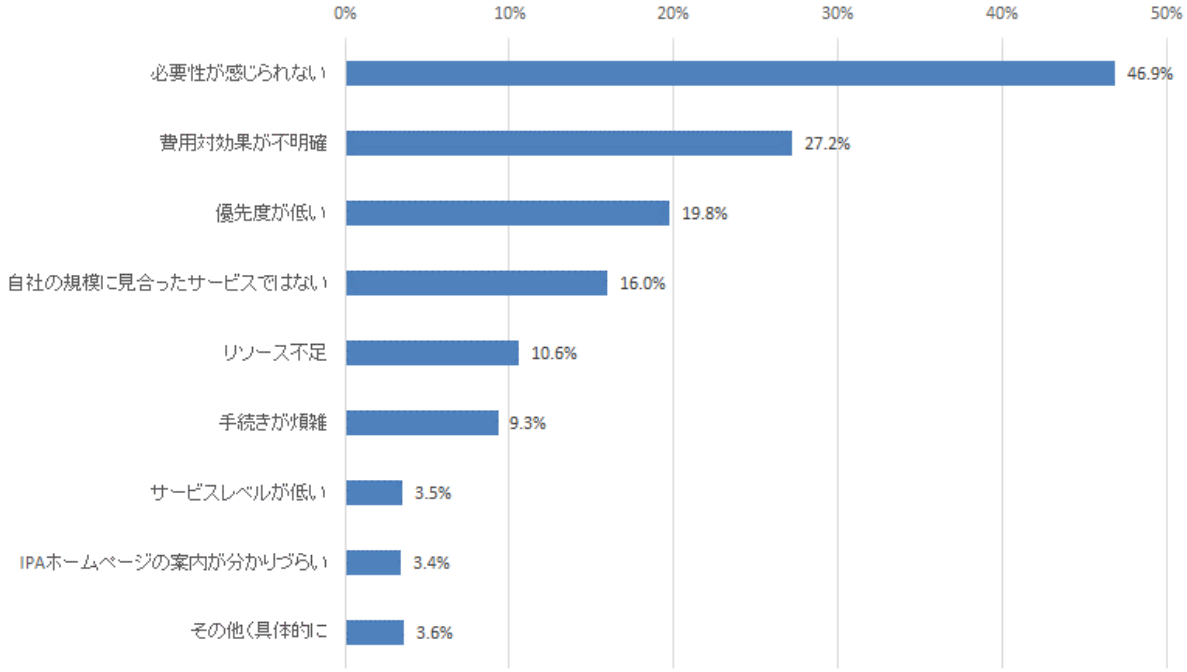

図 3-89 「サイバーセキュリティお助け隊サービス」を導入したいと思わない理由(n=2149)

3.2.10 情報セキュリティ対策の状況（25項目）

回答企業のセキュリティ対策状況について、「SECURITY ACTION」の二つ星に該当するチェック

項目の回答結果を記載する。

Q80-1. パソコンやスマホなど情報機器の OS やソフトウェアは常に最新の状態にしていますか？(SA)

回答者全体の 5 割強かパソコンやスマホなど情報機器の OS やソフトウェアを常に最新の状態にしていると回答している。

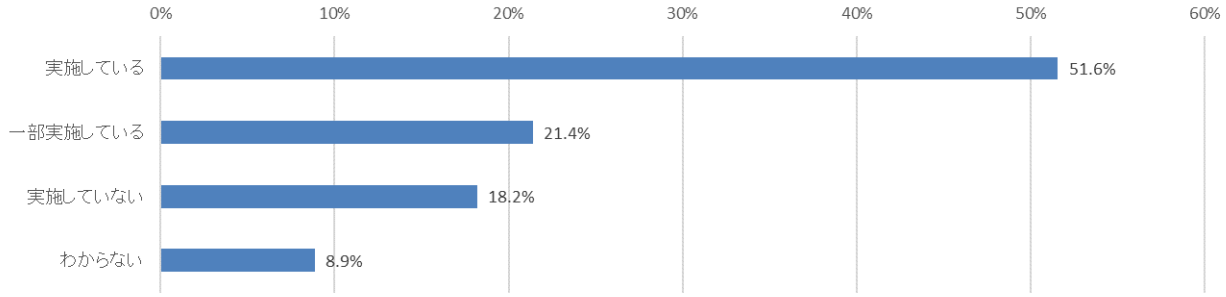

図 3-90 情報セキュリティ対策の状況(1)(n=4191)

Q80-2. パソコンやスマホなどにはウイルス対策ソフトを導入し、ウイルス定義ファイルは最新の状態にしていますか？(SA)

ウイルス対策ソフトを導入し、定義ファイルを最新の状態にしていると回答した割合は 5 割に上る。

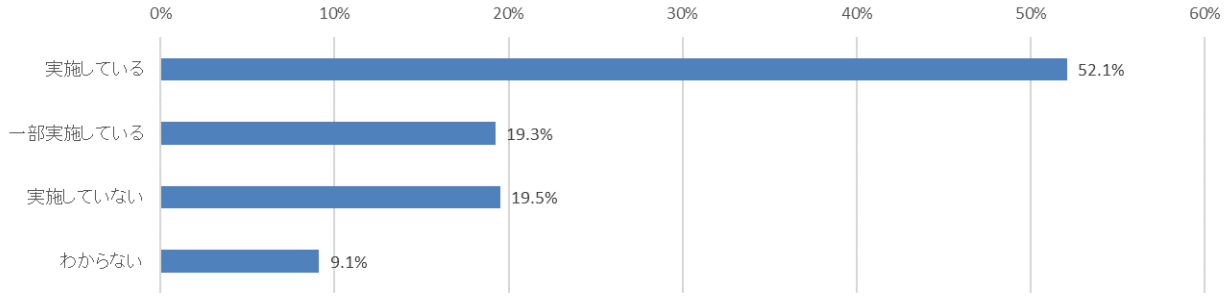

図 3-91 情報セキュリティ対策の状況(2)(n=4191)

Q80-3. パスワードは破られにくい「長く」「複雑な」パスワードを設定していますか？(SA)

パスワードを破られにくいものにしている割合は全体の 3 割強に留まる。

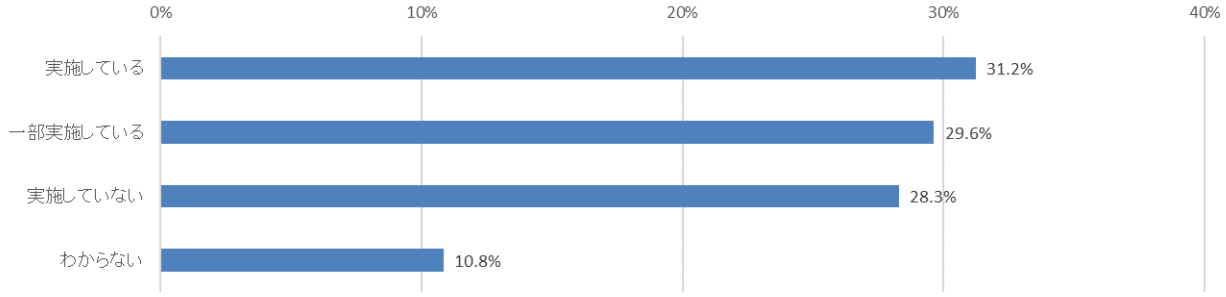

図 3-92 情報セキュリティ対策の状況(3)(n=4191)

Q80-4. 重要情報に対する適切なアクセス制限を行っていますか？(SA)

重要情報に対する適切なアクセス制限を行っていると回答した企業は全体の 2 割強に留まる。

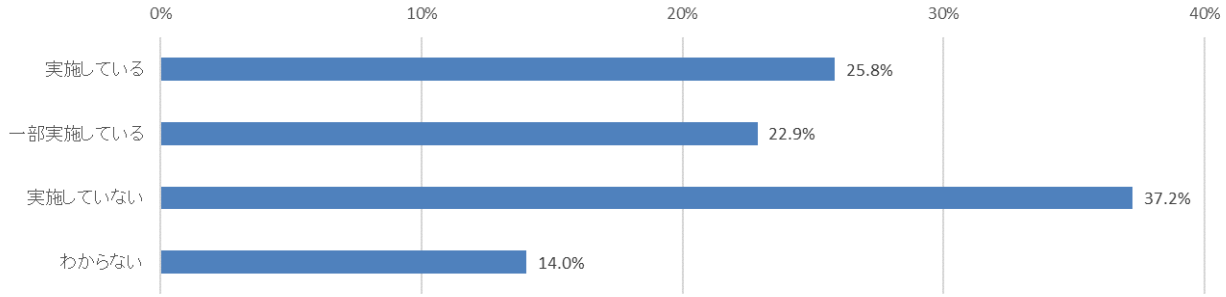

図 3-93 情報セキュリティ対策の状況(4)(n=4191)

Q80-5. 新たな脅威や攻撃の手口を知り対策を社内共有する仕組みはできていますか？（SA）

サイバー攻撃の新たな脅威や手口を知り社内共有する仕組みができていると回答している企業は全体の 2 割弱になる。

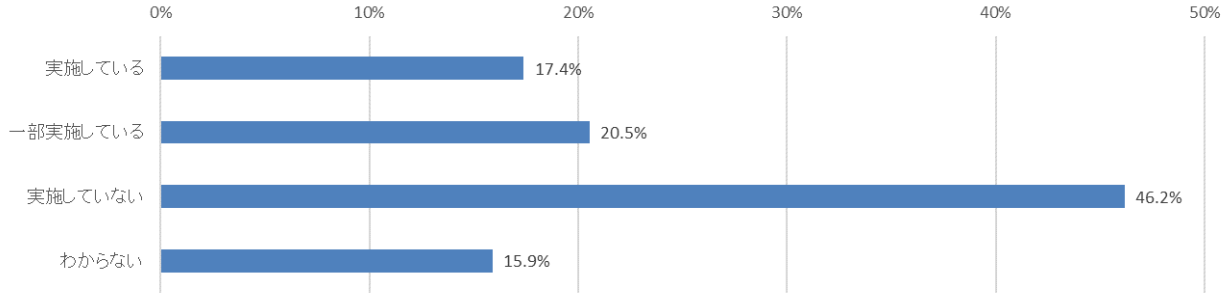

図 3-94 情報セキュリティ対策の状況(5)(n=4191)

Q80-6. 電子メールの添付ファイルや本文中の URL リンクを介したウイルス感染に気を付けていますか？(SA)

電子メールを経由したウイルス感染に気をつけていると回答した企業は全体の 4 割強に上る。

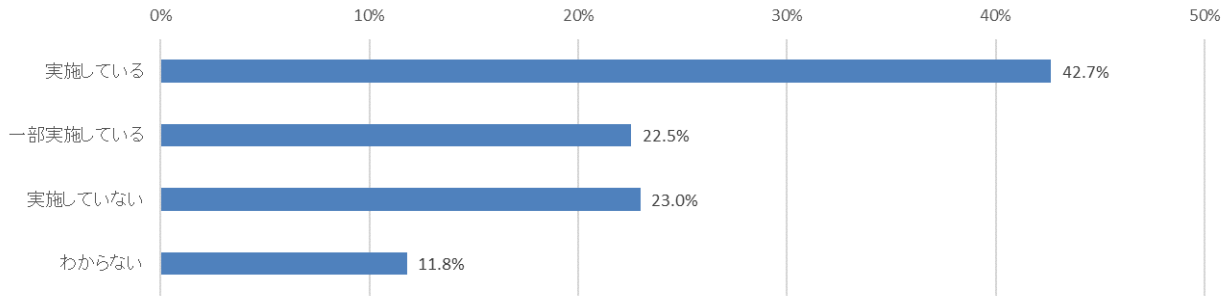

図 3-95 情報セキュリティ対策の状況(6)(n=4191)

Q80-7. 電子メールや FAX の宛先の送信ミスを防ぐ取り組みを実施していますか？(SA)

電子メールや FAX の宛先送信ミスを防ぐ取り組みを実施していると回答した企業は全体の 3 割弱になる。

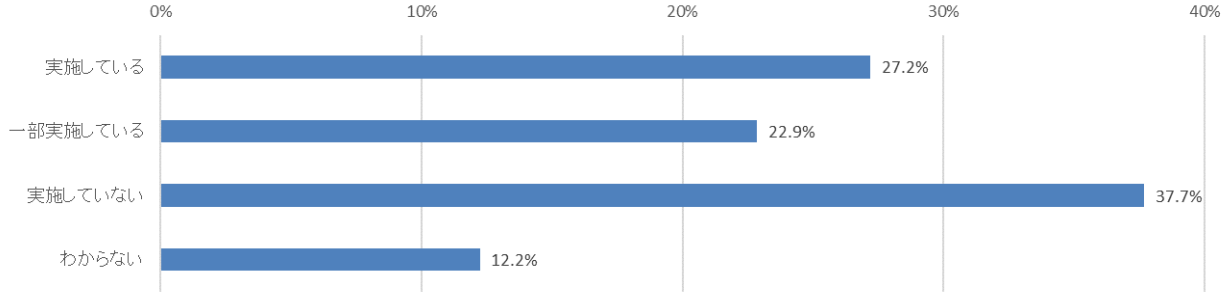

図 3-96 情報セキュリティ対策の状況(7)(n=4191)

Q80-8. 重要情報は電子メール本文に書くのではなく、添付するファイルに書いてパスワードなどで保護していますか？(SA)

重要情報を電子メール本文に書くのではなく、添付するファイルに書いてパスワードなどで保護すると回答した企業は全体の 2 割程度に留まる。

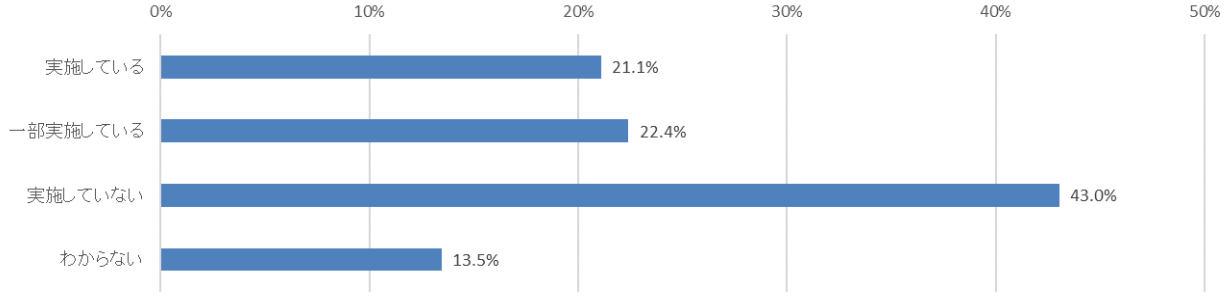

図 3-97 情報セキュリティ対策の状況(8)(n=4191)

Q80-9. 無線 LAN を安全に使うために適切な暗号化方式を設定するなどの対策をしていますか？(SA)

適切な暗号化方式を設定していると回答した企業は全体の 3 割弱である。

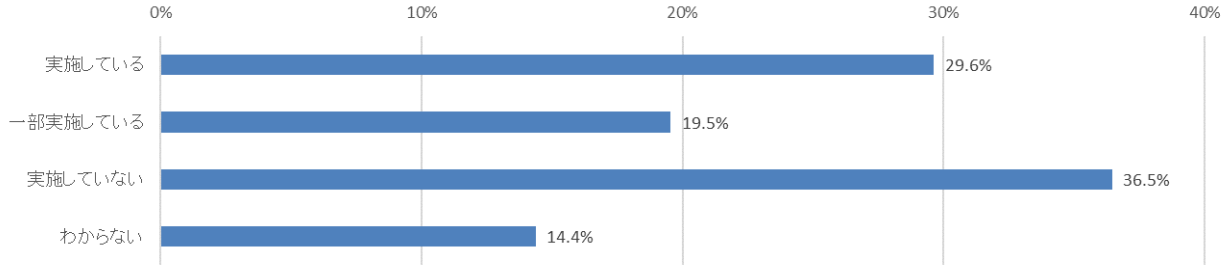

図 3-98 情報セキュリティ対策の状況(9)(n=4191)

Q80-10. インターネットを介したウイルス感染や SNS への書き込みなどのトラブルへの対策をしていますか？(SA)

インターネットを介したウイルス感染や SNS への書き込みなどのトラブルへの対策をしていると回答した企業は全体の 3 割弱である。

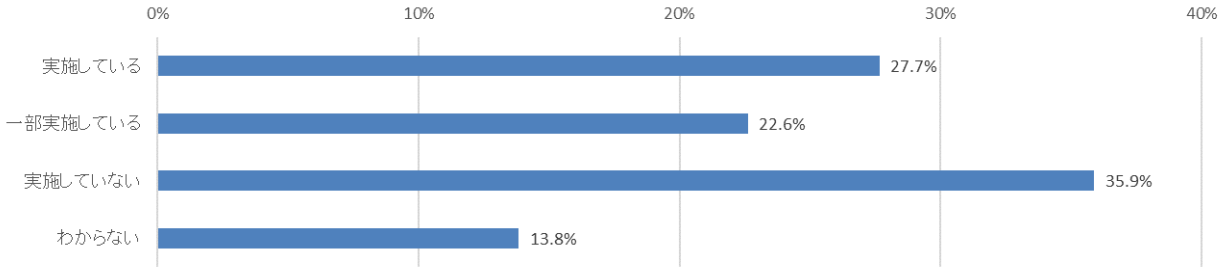

図 3-99 情報セキュリティ対策の状況(10)(n=4191)

Q80-11. パソコンやサーバのウイルス感染、故障や誤操作による重要情報の消失に備えてバックアップを取得していますか？(SA)

重要情報の消失に備えてバックアップをしていると回答した企業は全体の 3 割強である。

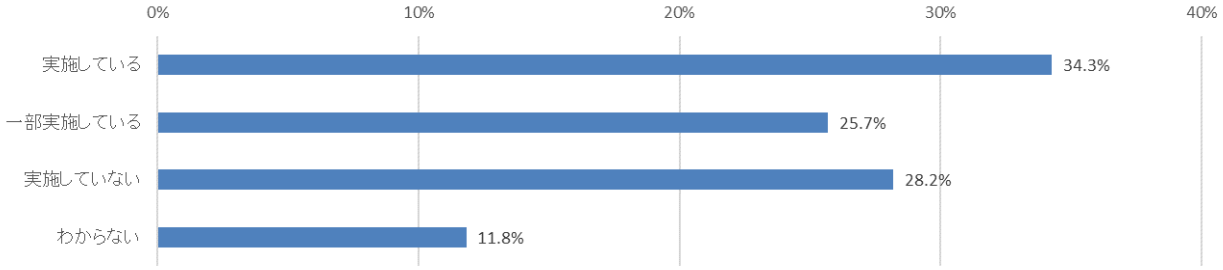

図 3-100 情報セキュリティ対策の状況(11)(n=4191)

Q80-12. 紛失や盗難を防止するため、重要情報が記載された書類や電子媒体は机上に放置せず、書庫などに安全に保管していますか？(SA)

紛失や盗難に備えて重要情報を書庫などの安全な場所に保管していると回答した企業は全体の 3 割弱になる。

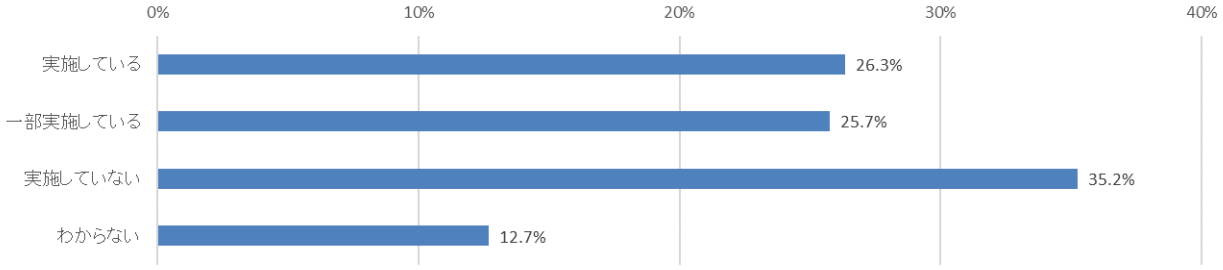

図 3-101 情報セキュリティ対策の状況(12)(n=4191)

Q80-13. 重要情報が記載された書類や電子媒体を持ち出す時は、盗難や紛失の対策をしていますか？(SA)

重要情報が記載された書類や電子媒体を持ち出すときに、盗難や紛失の対策をしていると回答した企業は全体の 3 割弱に留まる。

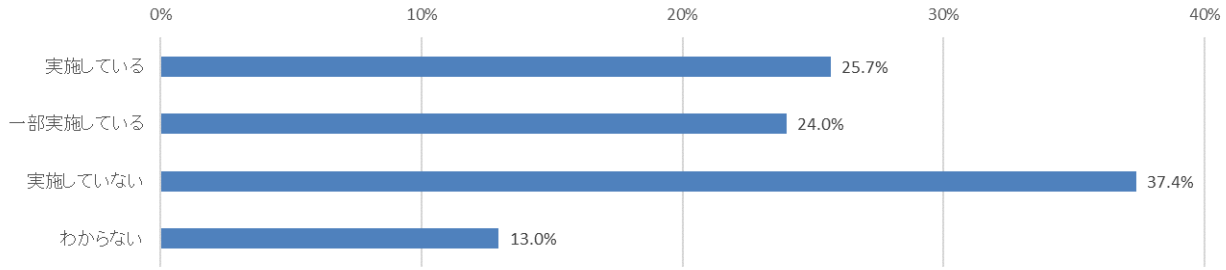

図 3-102 情報セキュリティ対策の状況(13)(n=4191)

Q80-14. 離席時にパソコン画面の覗き見や勝手な操作ができないようにしていますか？(SA)

離席時にパソコンの画面をロックするなど、覗き見や勝手な操作ができないようにすると回答した企業は全体の 2 割強である。

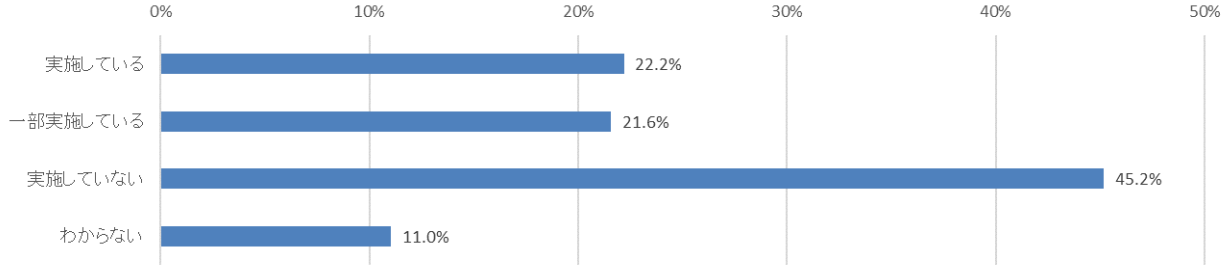

図 3-103 情報セキュリティ対策の状況(14)(n=4191)

Q80-15. 関係者以外の事務所への立ち入りを制限していますか？(SA)

関係者以外の事務所への立ち入りを制限していると回答している企業は全体の 3 割である。

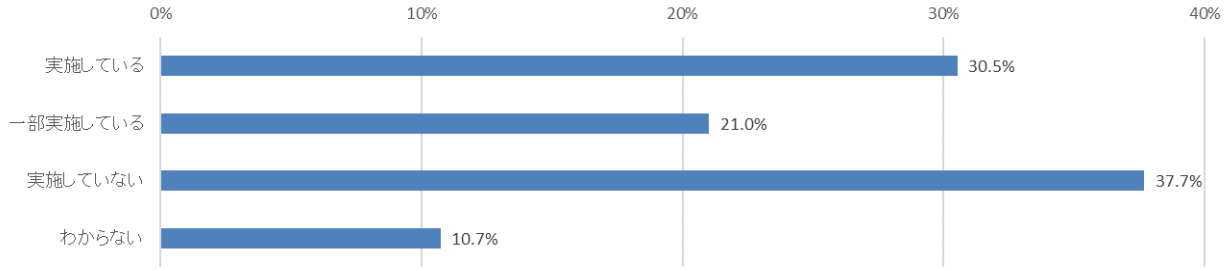

図 3-104 情報セキュリティ対策の状況(15)(n=4191)

Q80-16. 退社時にノートパソコンや備品を施錠保管するなど盗難防止対策をしていますか？(SA)

退社時にノートパソコンや備品を施錠、保管するなど盗難防止対策を行っていると回答した企業は全体の 2 割強である。

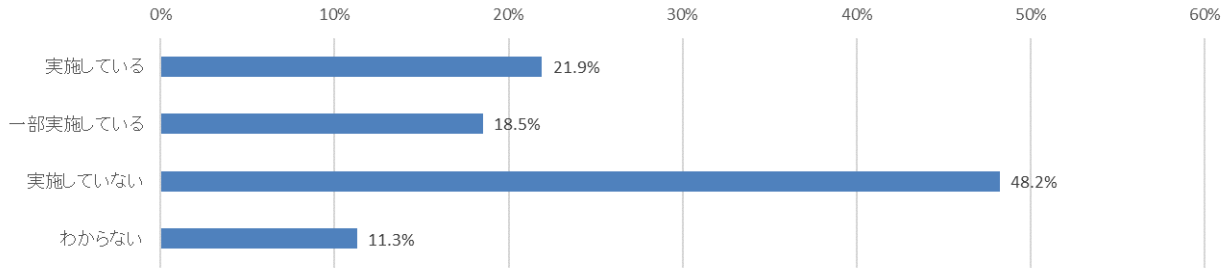

図 3-105 情報セキュリティ対策の状況(16)(n=4191)

Q80-17. 事務所が無人になるときの施錠忘れ対策を実施していますか？(SA)

事務所が無人になるときの施錠忘れ対策を実施していると回答した企業は全体の 3 割強である。

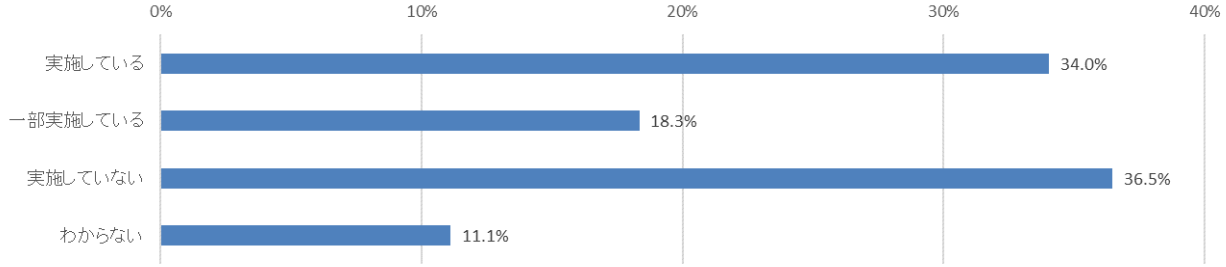

図 3-106 情報セキュリティ対策の状況(17)(n=4191)

Q80-18. 重要情報が記載された書類や重要なデータが保存された媒体を破棄する時は、復元できないようにしていますか？(SA)

重要情報が記載された書類や重要データが保存された媒体を破棄する時に復元できないようにしていると回答した企業は全体の 3 割弱である。

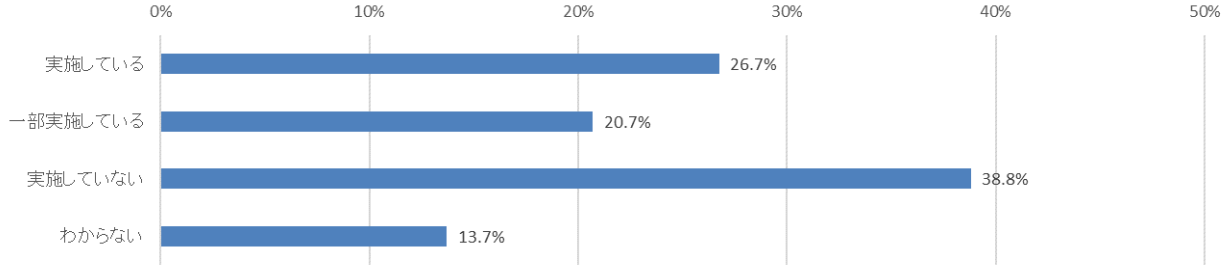

図 3-107 情報セキュリティ対策の状況(18)(n=4191)

Q80-19. 従業員に守秘義務を理解してもらい、業務上知り得た情報を外部に漏らさないなどのルールを守らせていますか？(SA)

従業員に守秘義務を理解させ、業務上知り得た情報を外部に漏らさないなどのルールを明確にし、守らせていると回答した企業は、全体の 3 割強である。

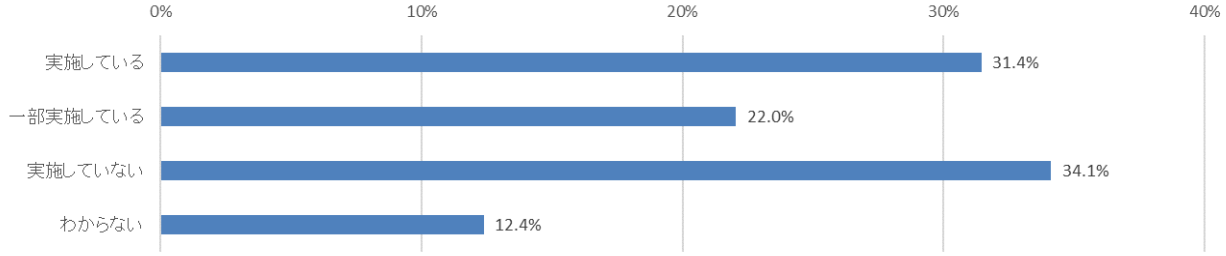

図 3-108 情報セキュリティ対策の状況(19)(n=4191)

Q80-20. 従業員にセキュリティに関する教育や注意喚起を行っていますか？(SA)

従業員に対するセキュリティ教育や注意喚起を行っていると回答した企業は全体の 2 割強である。

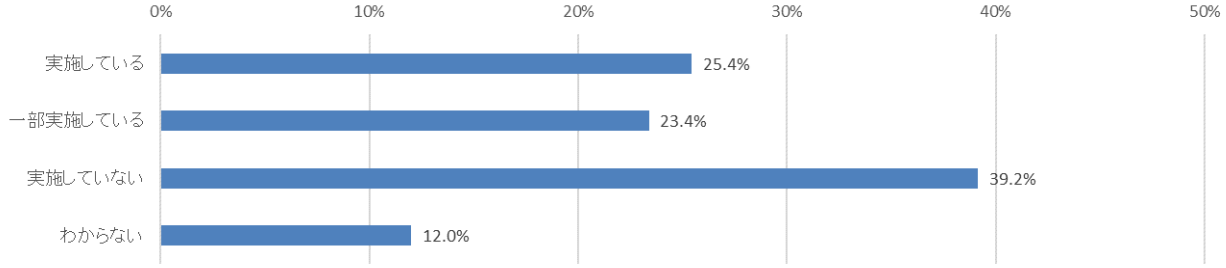

図 3-109 情報セキュリティ対策の状況(20)(n=4191)

Q80-21. 個人所有の情報機器を業務で利用する場合のセキュリティ対策を明確にしていますか？(SA)

所有の情報機器を業務で利用する場合のセキュリティ対策を明確にしていると回答した企業は全体の 2 割強である。

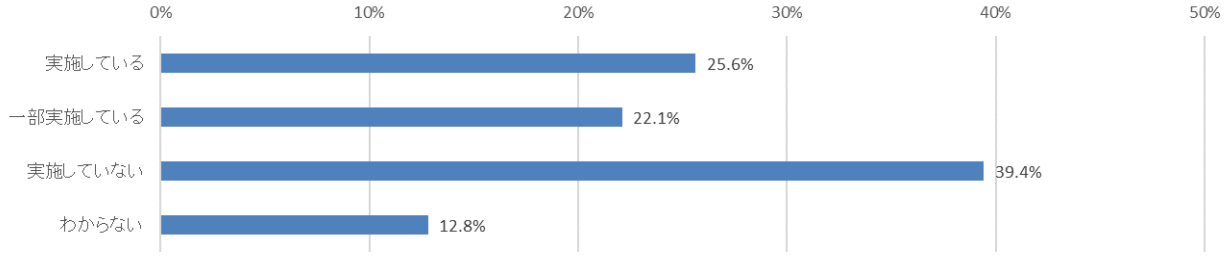

図 3-110 情報セキュリティ対策の状況(21)(n=4191)

Q80-22. 重要情報の授受を伴う取引先との契約書には、秘密保持条項を規程していますか？(SA)

重要情報の授受を伴う取引先との契約書に秘密保持情報を規程していると回答した企業は全体の 2 割強である。

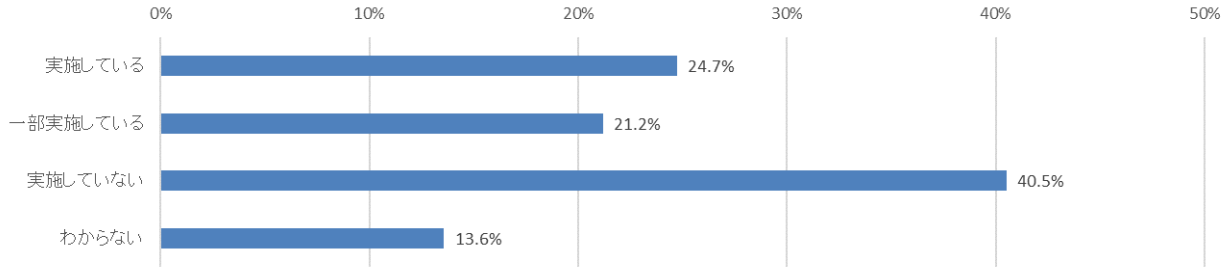

図 3-111 情報セキュリティ対策の状況(22)(n=4191)

Q80-23. クラウドサービスやウェブサイトの運用等で利用する外部サービスは、安全・信頼性を把握して選定していますか？(SA)

サービスやウェブサイトの運用等で利用する外部サービスの選定において、安全や信頼性を把握して選定していると回答した企業は全体の 2 割強である。

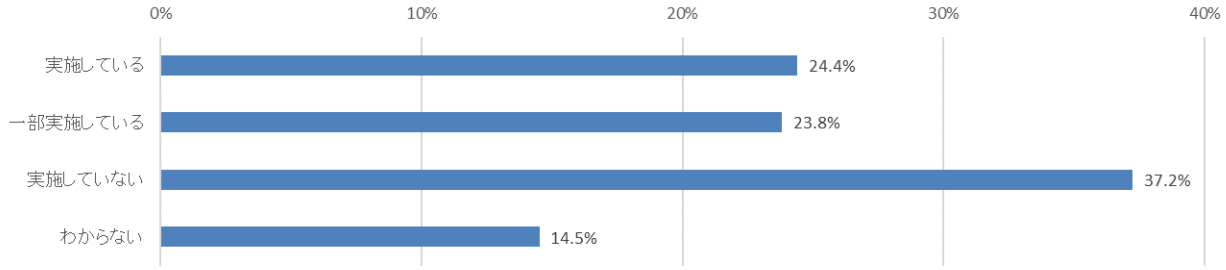

図 3-112 情報セキュリティ対策の状況(23)(n=4191)

Q80-24. セキュリティ事故が発生した場合に備え、緊急時の体制整備や対応手順を作成するなど準備をしていますか？(SA)

セキュリティ事故が発生した場合に備え、緊急時の対応体制を整備していると回答した企業は全体の 2 割弱である。

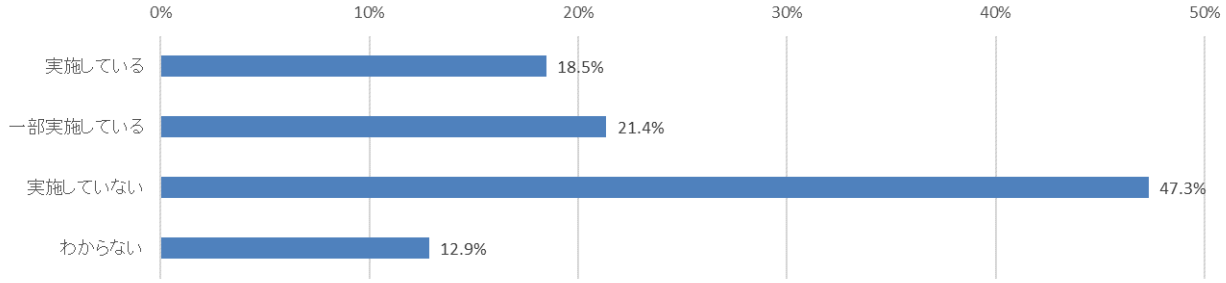

図 3-113 情報セキュリティ対策の状況(24)(n=4191)

Q80-25. 情報セキュリティ対策(上記 1～24 など)をルール化し、従業員に明示していますか？(SA)

情報セキュリティ対策をルール化し、従業員に明示していると回答した企業は全体の 2 割弱である。

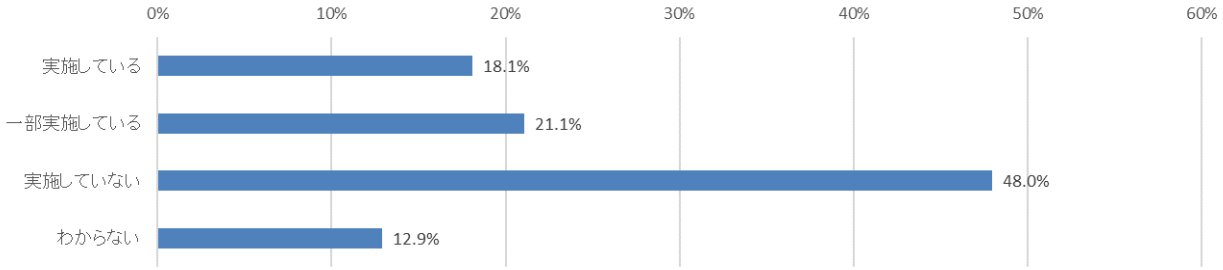

図 3-114 情報セキュリティ対策の状況(25)(n=4191)

3.3 調査結果(クロス集計)

ここからは、クロス集計結果の一部について示す。なお、本調査でクロス集計の軸として設定したのは以下の項目である。

- 企業規模
- 業種
- 情報セキュリティ対策投資
- 情報セキュリティ体制

企業規模については、中小企業及び小規模企業者の定義に従い分類した上で、中小企業については100 名以下と 101 名以上に二分した。

表 3-3 企業規模の区分

区分	業種	従業員規模	アンケート回答数
小規模企業者	商業・サービス業	1～5名	2,775
	製造業その他	1～20 名	
中小企業 (100 名以下)	商業・サービス業	6～100 名	1,121
	製造業その他	21～100 名	
中小企業 (101 名以上)	全業種	101 名以上	295

3.3.1 企業規模によるクロス集計結果

表 3-3 企業規模の区分に示す企業規模と各設問のクロス集計を行うことにより、企業規模に応じたセキュリティ対策の実態と課題を分析する。

小規模企業者では、直近過去 3 期の情報セキュリティ対策投資について「投資していない」との回答が 7 割強となっており、その理由として中小企業（100 名以下）、中小企業（101 名以上）と比較して、「重要情報を保有していないため」との回答割合多く、事業における情報セキュリティ上のリスクに対する認識が不足している可能性が示唆される。また情報セキュリティ体制も、専門部署の設置または兼務も含めた担当者が任命されている割合は低く 1 割強であり、困ったことがあった時の相談先として「特にない」を上げる割合が 7 割弱と高く、限られた人員の中で情報セキュリティ関連業務に十分な対応ができていない実態が浮き彫りとなっている。

企業規模が大きくなるにつれ、情報セキュリティ対策投資額は増え、社内体制は整備されている傾向が見て取れるが、中小企業（100 名）以下では約 4 割が「投資していない」との回答であり、また、社内体制の整備状況も「組織的に行っていない」が 5 割弱であることから、中小企業（100 名以下）におけるサイバーセキュリティに対する投資や組織的な取り組みが依然として不十分であることが示唆されます。この状況は、限られたリソースやサイバーセキュリティの優先度の低さが背景にあり、潜在的な脅威に対する脆弱性を抱えている可能性があります。従って、中小企業に対しては、サイバーセキュリティの重要性を喚起し、そのための効果的かつ手頃なソリューションの提供と企業への認識向上が急務であると考えられます。

中小企業（101 名以上）となると、情報セキュリティ体制において「組織的には行っていない」との回答は 1 割強と少なくなり、情報セキュリティ対策投資を行っていないとの回答も 2 割弱となることから、この規模の企業では、情報セキュリティ対策について、比較的積極的に取り組んでいることが伺えます。組織の規模が大きくなるにつれて、サイバー脅威の影響範囲やリスクに対する認識もされるようになり、これらの企業はその対策に対する意識が高く、必要なリソースを確保しやすいと考えられ、より体系的なセキュリティ戦略の実施が進んでいると見受けられます。ただし、未だ一定数の企業が投資を行っていない実態を踏まえ、さらなる意識改革や効果的な対策事例の共有が求められます。

a. 利用・導入しているサービスやシステム

Q5. 貴社では経営資源の確保や業務の効率化に IT を活用されていますか。情報セキュリティ対策サービス以外で利用・導入されているサービスやシステムについて教えてください。 あてはまるものを下記よりすべてお選びください。（MA）

電子メール（フリーメール・汎用ドメイン等）の利用は小規模企業者で 50%と多く、逆に電子メール（独自ドメイン）は中小企業（101 名）以上が 71.5%と多くなっている。小規模企業でも 2 割強が Web サイト、ホームページを開設しているなど IT 利用が進んでおり、たとえ小規模企業者であってもフィッシングメールへの対応や、Web サイトへの攻撃対策などサイバーセキュリティ対策が重要な状況となっていることが分かる。

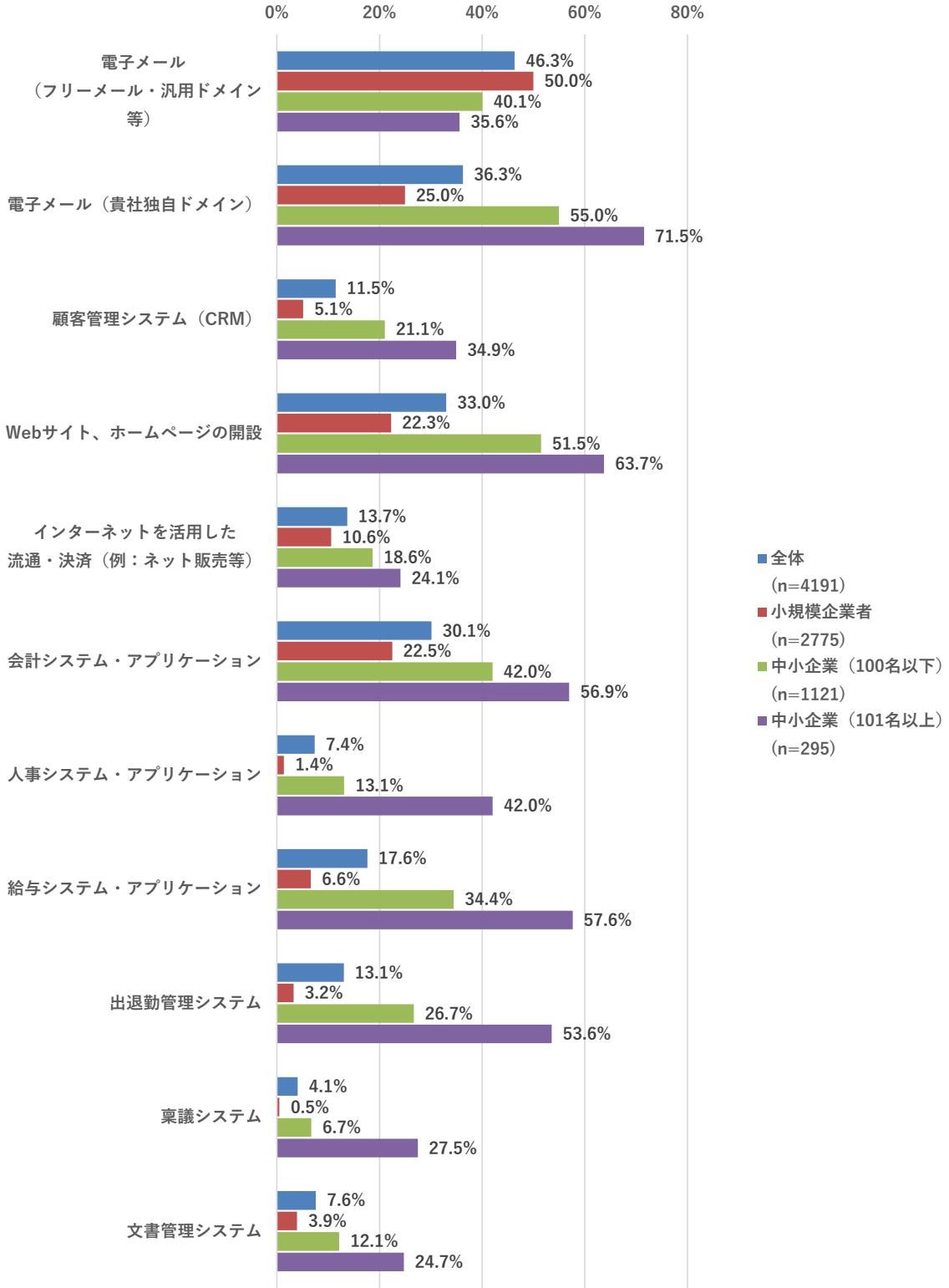

図 3-115 利用･導入しているサービスやシステム(企業規模別)①(n=4191)

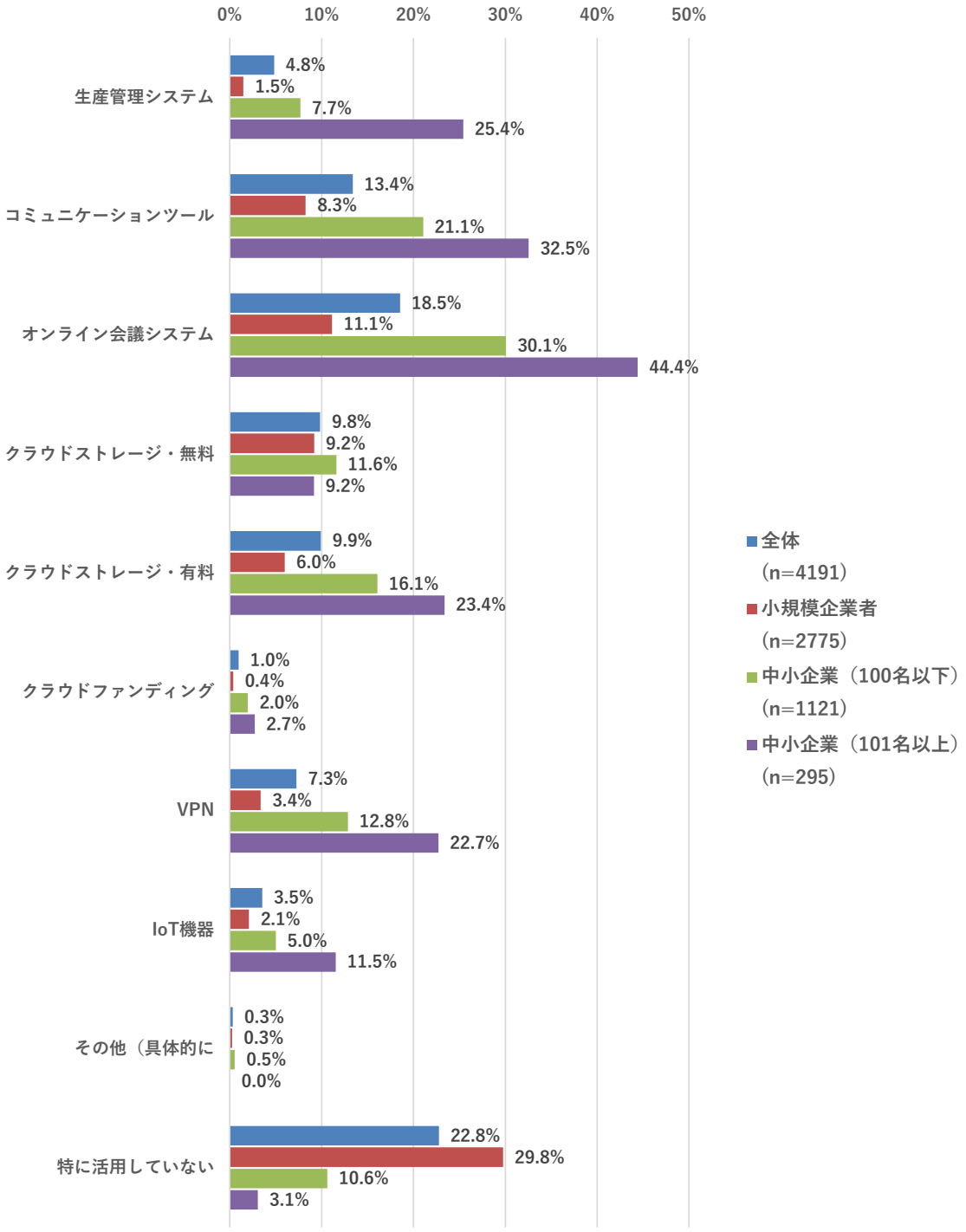

図 3-116 利用･導入しているサービスやシステム(企業規模別)②(n=4191)

b. 直近過去3期の情報セキュリティ対策投資額

Q6 項目 2. 貴社における、直近過去 3 期の IT 投資額(情報セキュリティ投資額を含む)と、情報セキュリティ対策投資額(IT 機器や社員への教育等も含む)の概算について教えてください。-情報セキュリティ対策投資額(IT 機器や社員への教育等も含む)(SA)

企業規模に応じて投資額が大きく異なる傾向がみられる。小規模企業者では 7 割強、中小企業(101 名以下)の 40 %、中小企業(101 名以上)の 17 %が投資をしないと回答している。

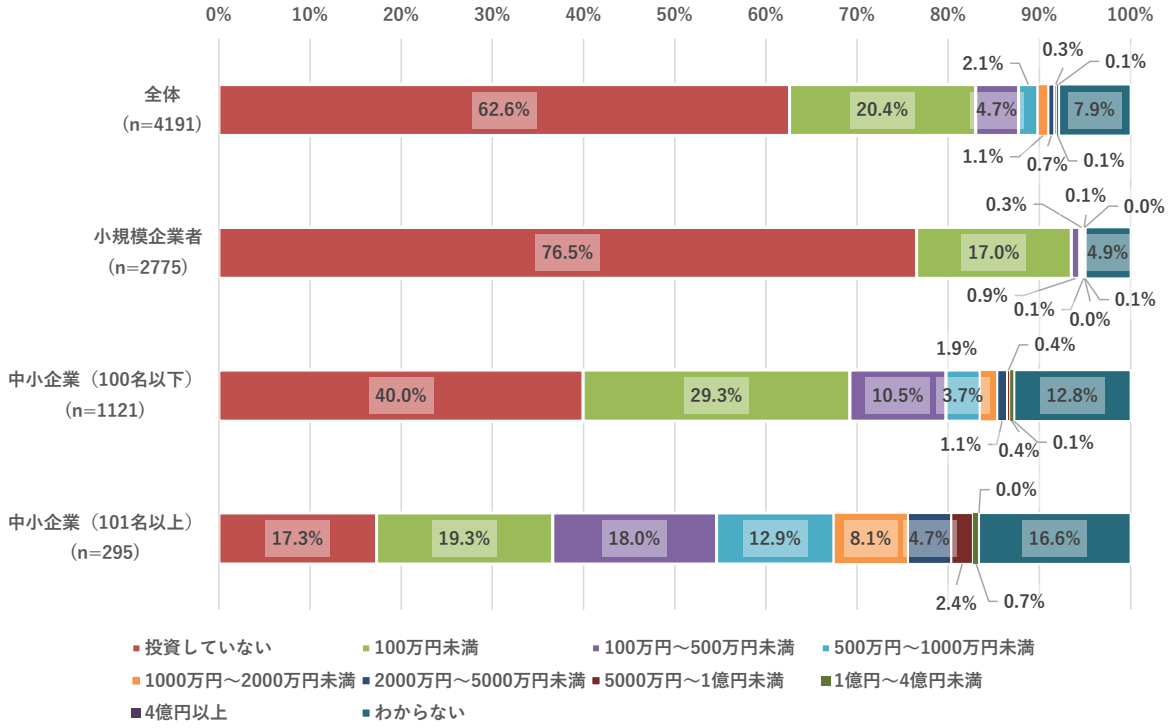

図 3-117 直近過去3期の情報セキュリティ対策投資額(企業規模別)(n=4191)

c. 情報セキュリティ対策投資を行わなかった理由

Q7. (Q6-2.で「投資していない」と回答された方について)前問で情報セキュリティ対策投資額について「投資をしていない」とお答えになった一番の理由について教えてください。(SA)

企業規模別にみると最も多い回答が小規模企業者では必要性を感じていないが 48%、中小企業(101 名以下)では費用対効果が見えないが 34%、中小企業(101 名以上)ではコストがかかりすぎると費用対効果が見えないが同じ 33%となっており、企業規模別の傾向が見て取れる。

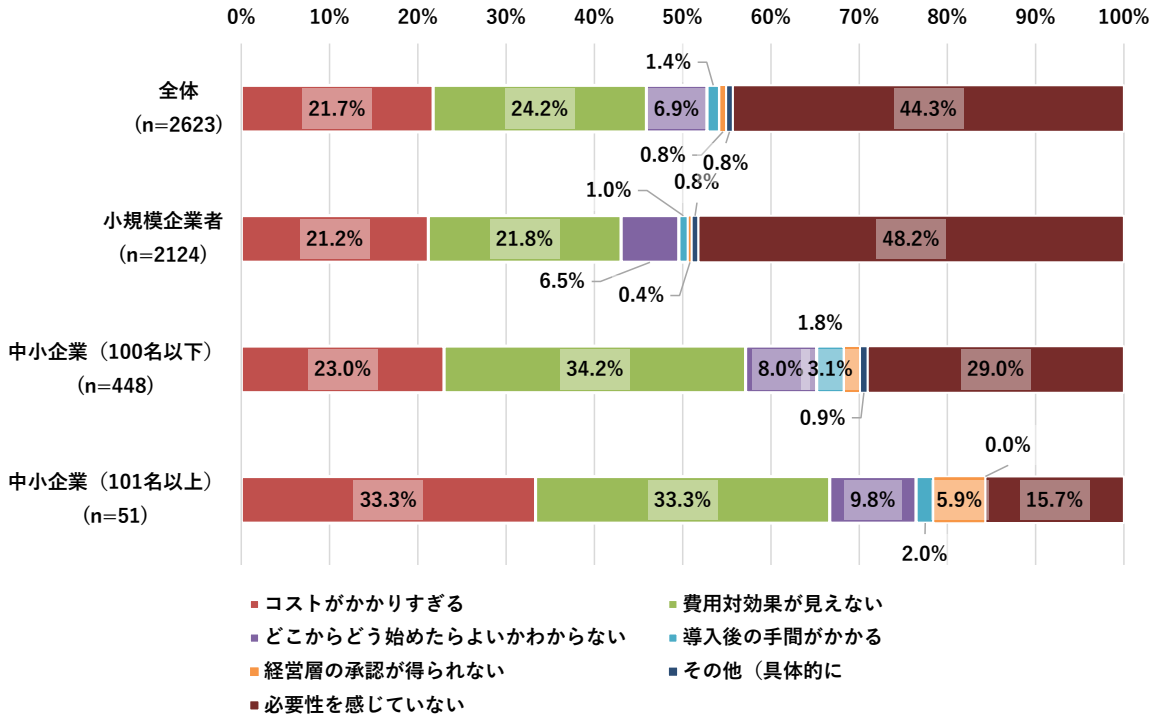

図 3-118 情報セキュリティ対策投資を行わなかった理由(企業規模別)(n=2623)

Q8.(Q7.で「必要性を感じていない」と回答された方について)前問で情報セキュリティ対策投資について「必要性を感じていない」とお答えになった理由について教えてください。 あてはまるものを下記よりすべてお選びください。(MA)

「必要性を感じていない」理由として中小企業(101 名以上)では既に十分な対策がとられているからが最も多く 62%となっている。小規模企業者では重要情報を保有していないためが 38%と最も多く、次いで他社とのネットワーク接続が無いためが 32%である。中小企業(101 名以下)は、どの回答も20%強となっている。

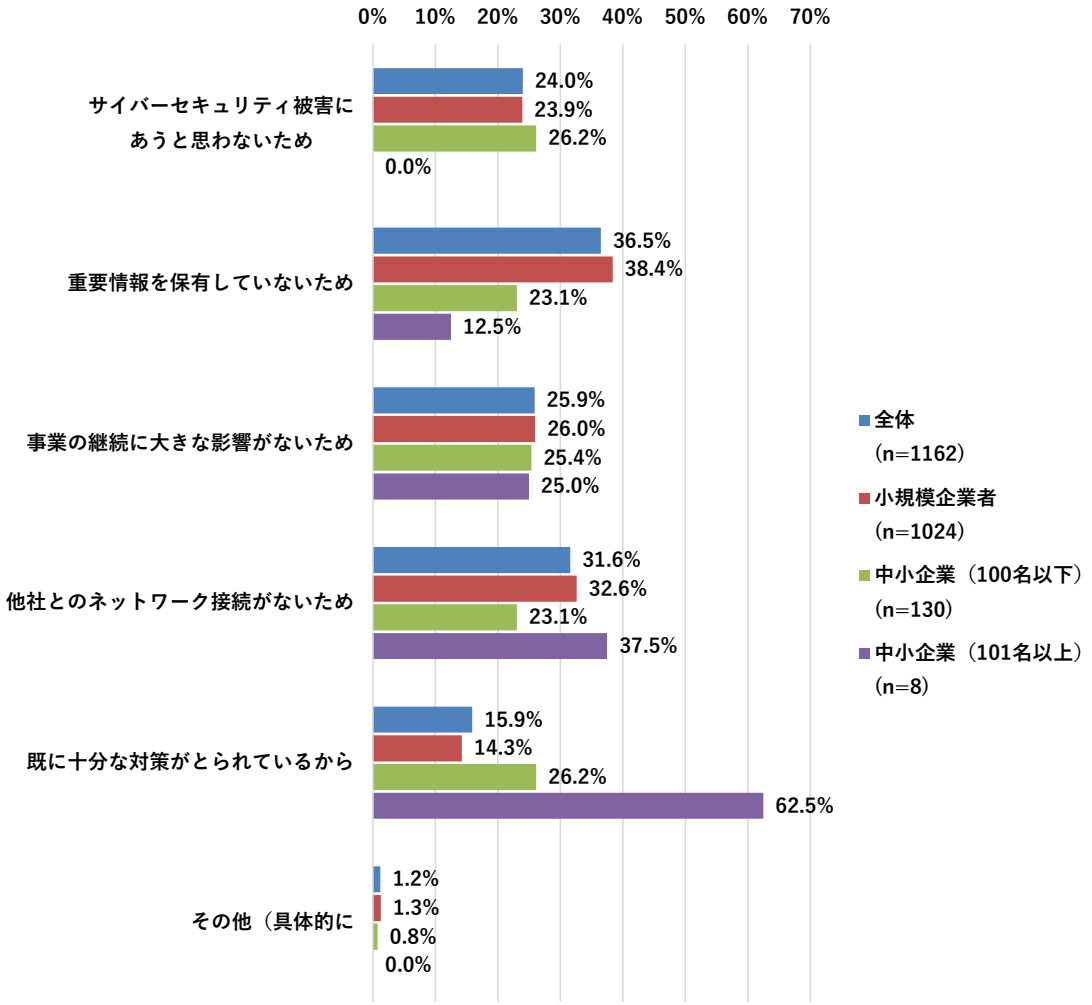

図 3-119 情報セキュリティ対策投資について「必要性を感じていない」と回答した理由（企業規模別）（n=1162）

d. セキュリティパッチの適用状況

Q14.（Q9 で「対策の必要性を感じたことがない」以外の回答をされた方について）貴社ではサーバ等にセキュリティパッチを適用していますか。パッチを適用していない場合は理由について教えてください。 あてはまるものを下記よりすべてお選びください。（MA）

企業規模が大きくなるにつれてパッチを提供していると回答する割合が増えている。小規模企業者がパッチを適用していない最も大きな理由としては、パッチの適用に多大なコストがかかること、パッチを適用しなくても問題無いと判断したが、それぞれ 3 割程度となっている。

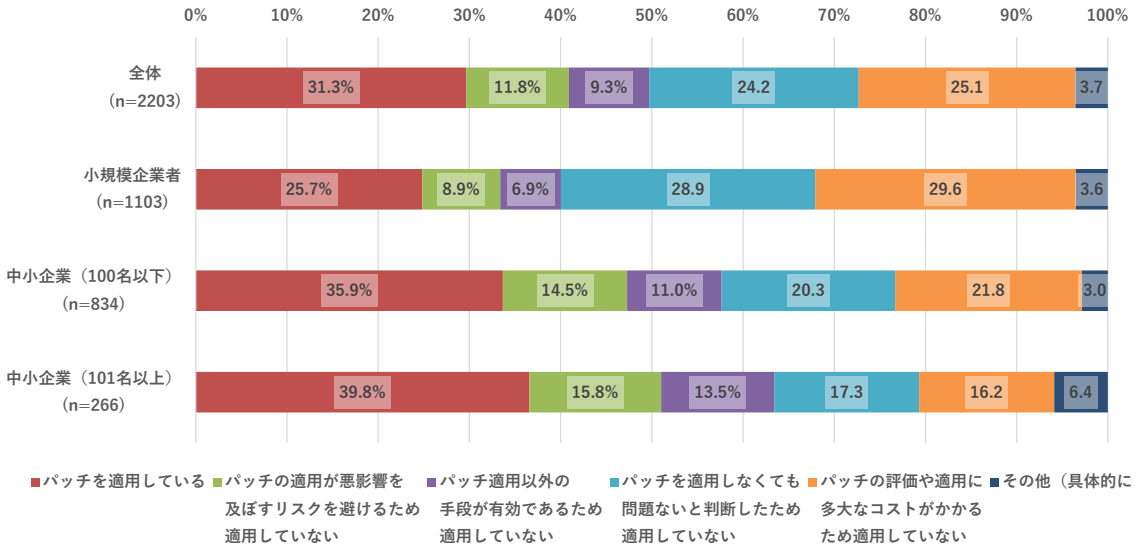

図 3-120 セキュリティパッチの適用状況（企業規模別）(n=2203)

e. 組織体制

Q22. 貴社の情報セキュリティ対策はどのような体制で行われていますか。（SA）

「専門部署（担当者）がある」、「兼務だが、担当者が任命されている」と回答した企業は、企業規模が大きいほど割合が高い。

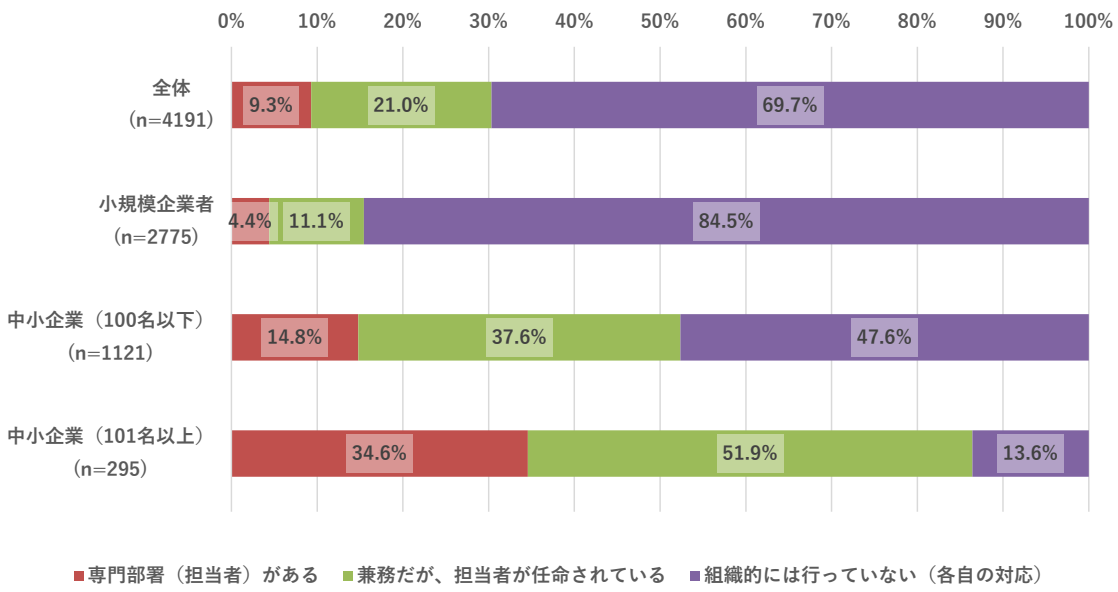

図 3-121　貴社の情報セキュリティ対策はどのような体制(企業規模別)(n=4191)

f. 困ったことがあった際の相談先

Q23. 貴社の情報セキュリティ対策に関して困ったことがあった際の相談先を教えてください。あてはまるものを下記よりすべてお選びください。(MA)

困ったことがあった際の相談先として、企業規模が大きいほど、社内の担当者を上げる割合が大きくなる。相談先として次に多いのは「社外の IT 関連業者・営業」である。小規模企業者では、社内の担当者、社外の IT 関連業者・営業はどちらも 1 割～2 割弱であり、相談先に乏しいことが想定される。

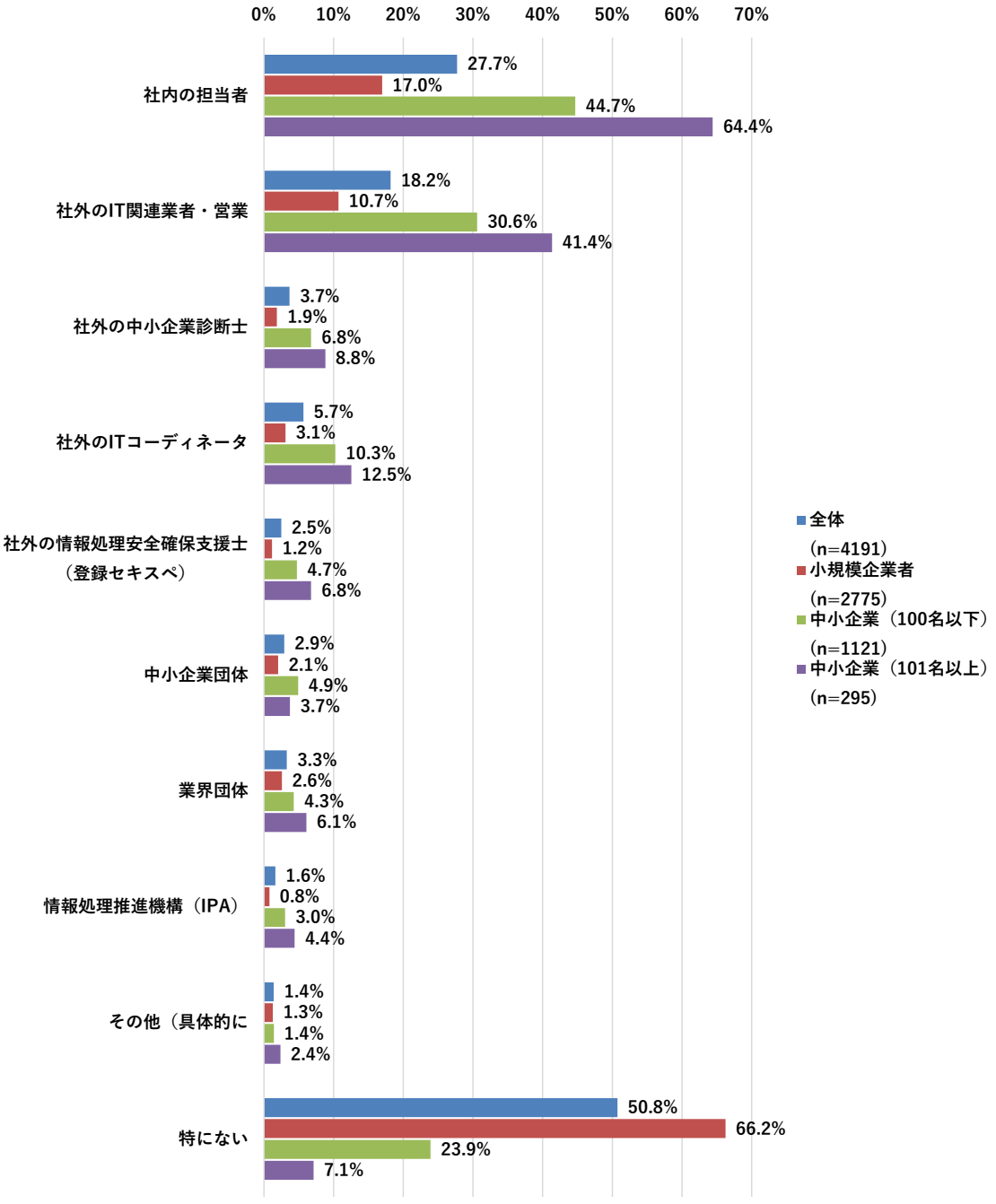

図 3-122 情報セキュリティ対策に関して困ったことがあった際の相談先(企業規模別)(n=4191)

g. 活用したい情報セキュリティ対策に関するサービス

Q21. どのような情報セキュリティ対策に関するサービスがあれば活用したいと思いますか。あてはまるものを下記よりすべてお選びください。(MA)

企業規模別に回答が多かったサービスを見ると、小規模企業者では「経営層向けの手引書」が最も多く、中小企業(101 名以下)と中小企業(101 名以上)では経営層への教育(セキュリティ対策の重要性の理解)となっており、何れも経営層に係るものであることが分かる。

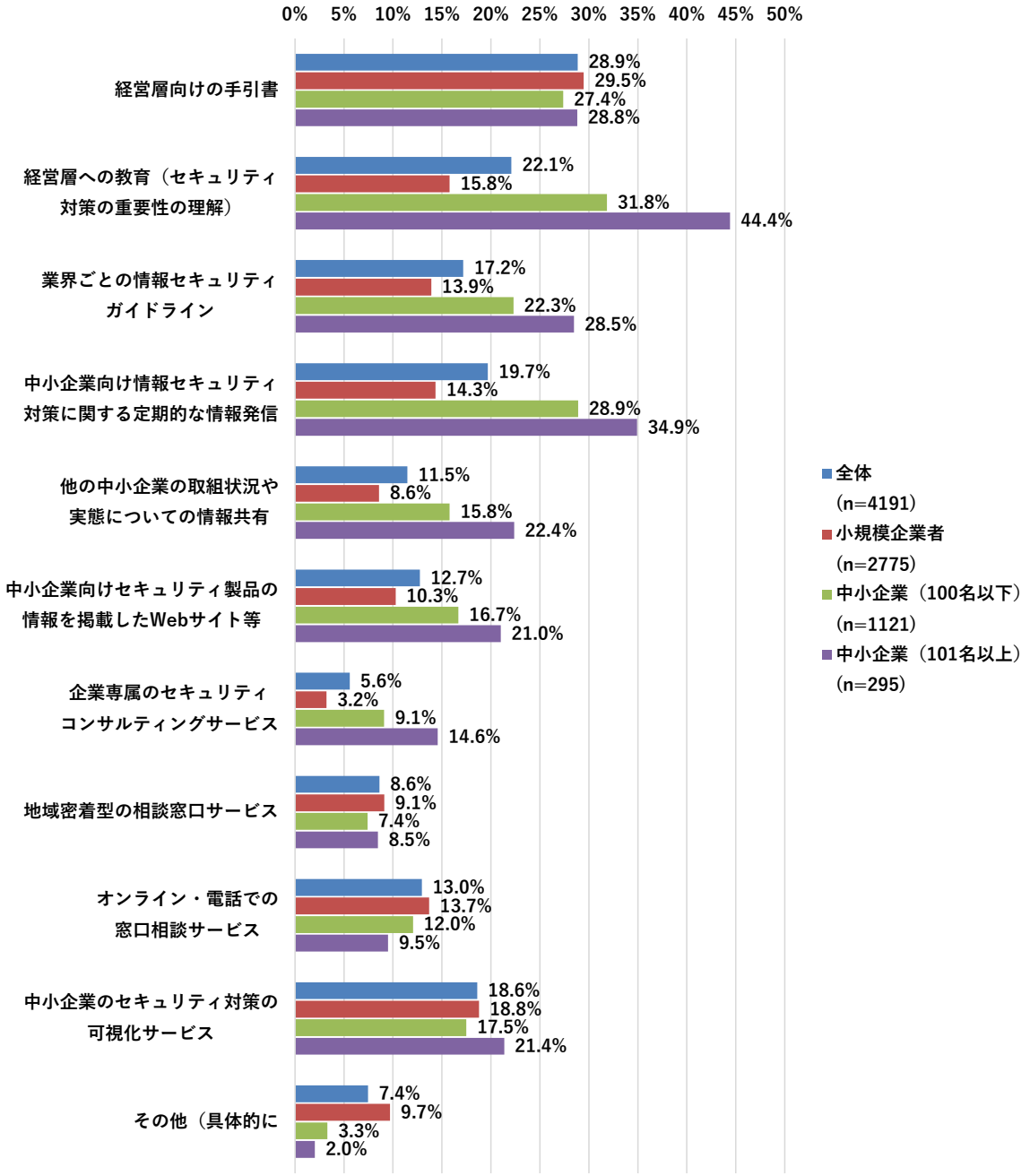

図 3-123 活用したい情報セキュリティ対策に関するサービス(企業規模別)(n=4191)

h. 情報セキュリティに関する情報収集先

Q24. 貴社の情報セキュリティ対策に関する情報収集先を教えてください。 あてはまるものを下記よりすべてお選びください。(MA)

規模の大きい企業は社内担当者、または社外の IT 関連業者から情報を入手している。小規模企業者では特にないとの回答を除き、インターネットが最も多くなっている。

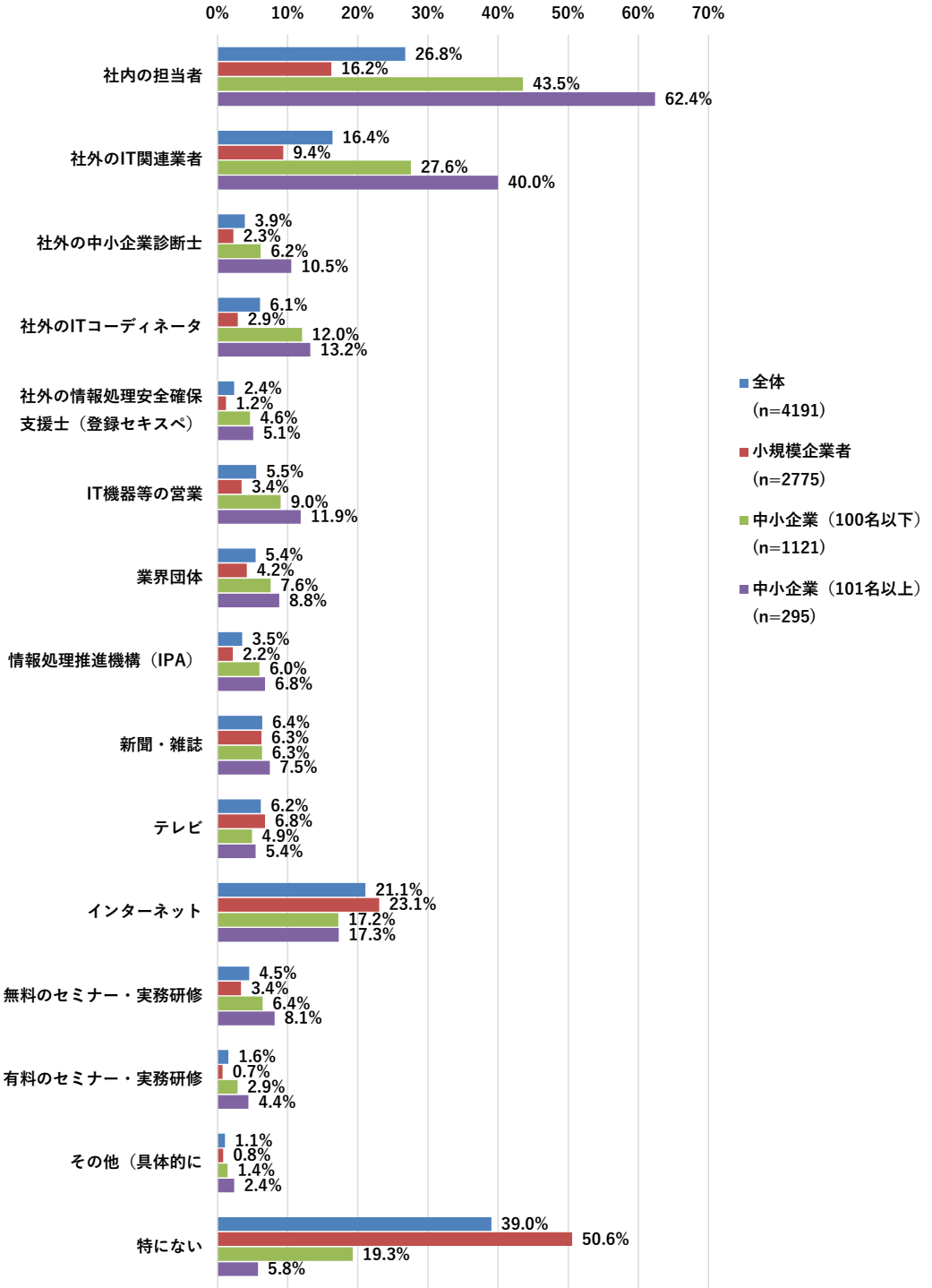

図 3-124 情報セキュリティ対策に関する情報収集先(企業規模別)(n=4191)

i. 従業員に対する情報セキュリティ教育の実施状況

Q25. 貴社では従業員に対する情報セキュリティ教育をどのように実施していますか。(MA)

従業員への情報セキュリティ教育については、全ての教育内容に関して中小企業(101 名以上)が最も実施している。一方で特に実施していないとの回答は、小規模企業者が最も多く 8 割弱、中小企業(101 名以下)でも 4 割となっている。

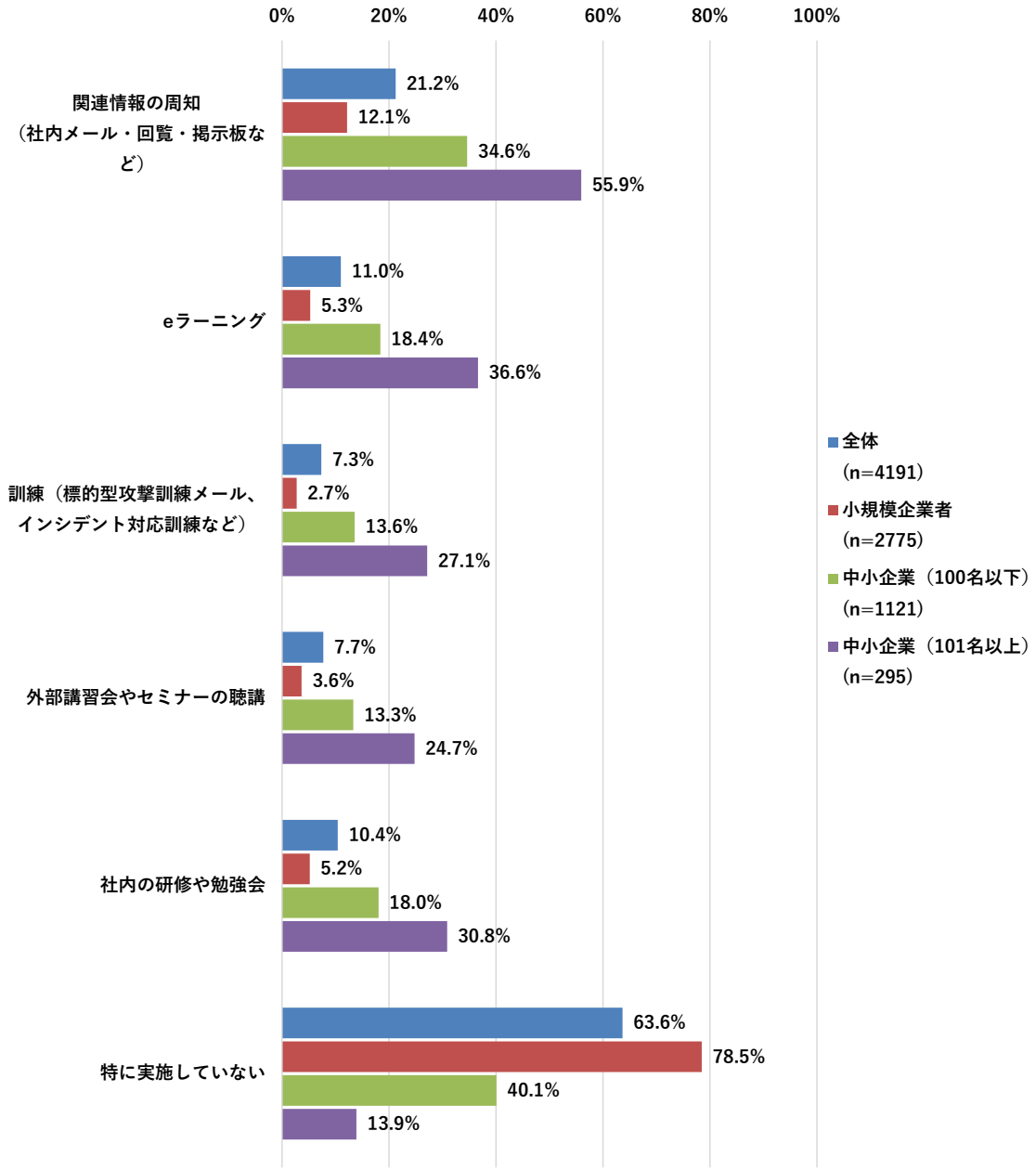

図 3-125 従業員に対する情報セキュリティ教育の実施状況(企業規模別)(n=4191)

j. 情報漏えい等のインシデント又はその兆候を発見した場合の報告先

Q15. 貴社で情報漏洩等のインシデント又はその兆候を発見した場合に、規定されている報告先は何ですか。 あてはまるものを下記よりすべてお選びください。(MA)

中小企業(101 名以下)と中小企業(101 名以上)で最も多い回答は「経営者への報告」となっており、報告先が決まっていることが分かるが、小規模企業者では 4 割強が報告先は決まっていないと回答している。

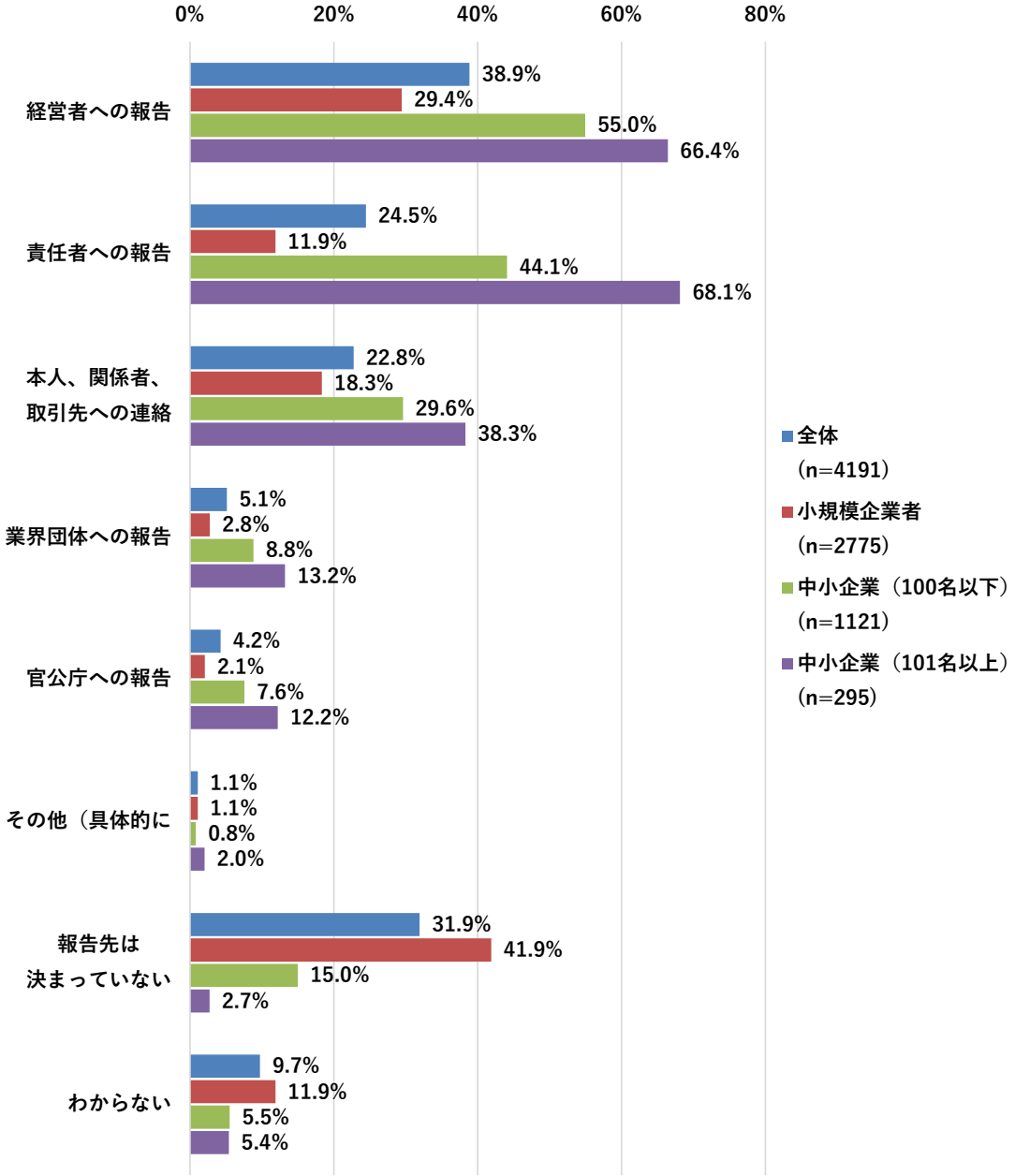

図 3-126 情報漏えい等のインシデント又はその兆候を発見した場合の報告先(企業規模別)(n=4191)

k. 情報漏えい等のインシデント又はその兆候を発見した場合の対応方法

Q16. 貴社で情報漏洩等のサイバーインシデント又はその兆候を発見した場合の対応方法として規定されているものは何ですか。 あてはまるものを下記よりすべてお選びください。(MA)

小規模企業者では対応が決まっていないが最も多く、5 割弱となっている。一方で中小企業(101 名以上)では 4 割～5 割の企業が対応方法を決めていることが分かる。

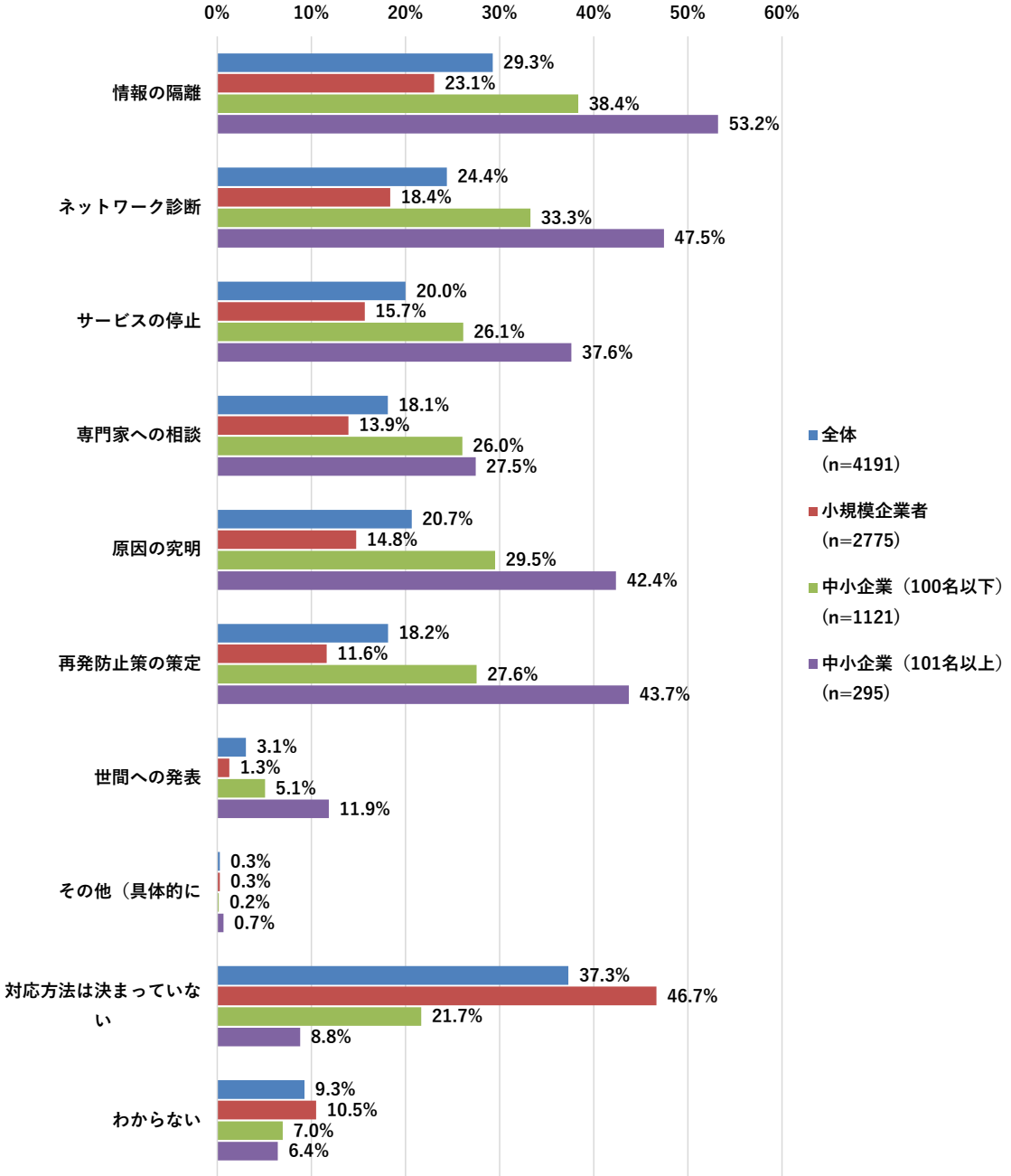

図 3-127 サイバーインシデント又はその兆候を発見した場合の対応方法(企業規模別)(n=4191)

I. 情報セキュリティ関連製品やサービスの導入状況

Q12.（Q9 で「対策の必要性を感じたことがない」以外の回答をされた方について）貴社では情報セキュリティ関連製品やソフトウェアを導入していますか。 導入している情報セキュリティ関連製品やソフトウェアを教えてください。 あてはまるものを下記よりすべてお選びください。（MA）

どの企業規模でもウイルス対策ソフトの導入は 8 割程度となっており、基本的なセキュリティ対策は進んでいる。次いでファイアウォールの導入割合が高い。

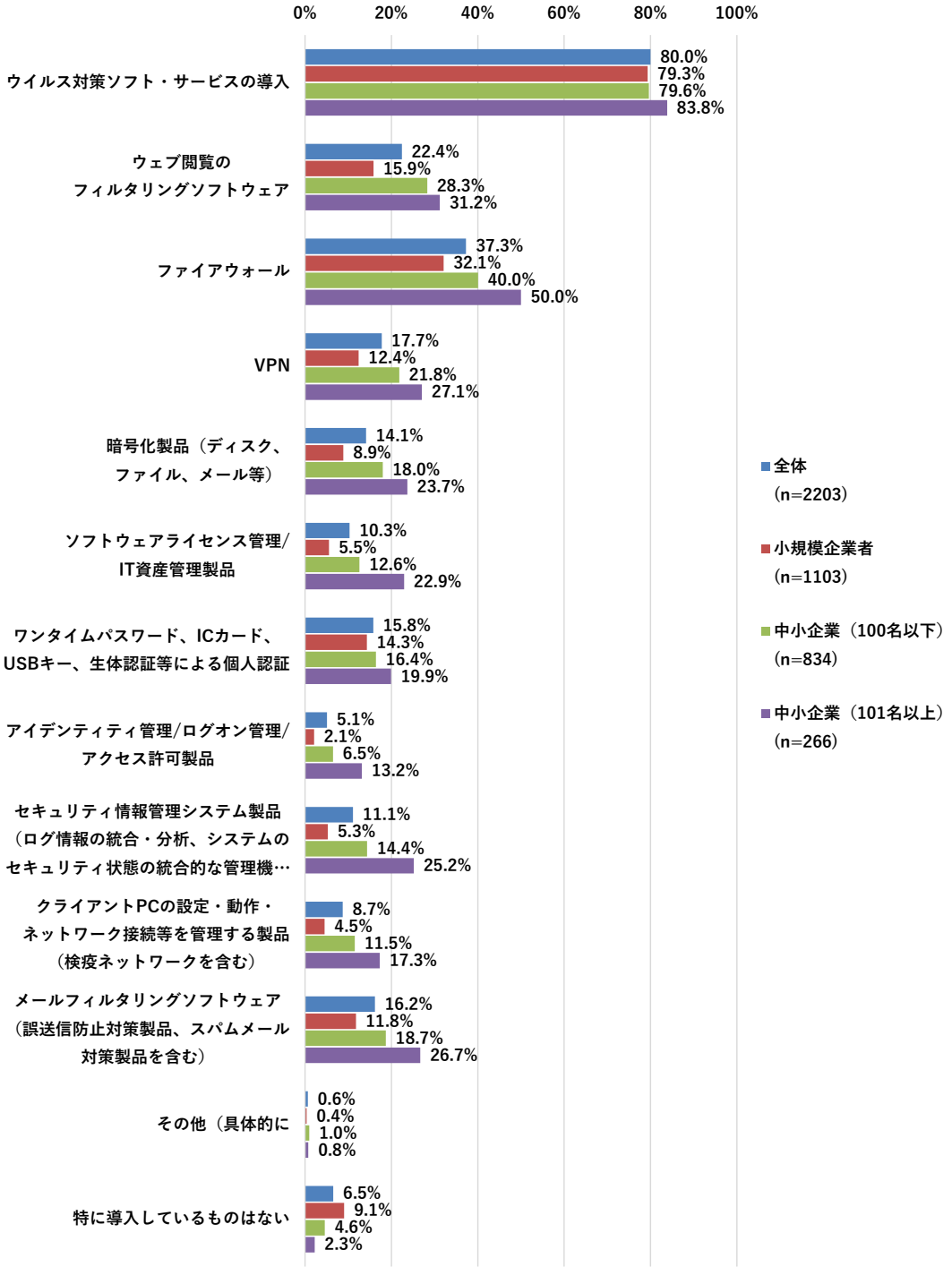

図 3-128 情報セキュリティ関連製品やサービスの導入状況（企業規模別）（n=2203）

m. 情報セキュリティ対策に期待する効果

Q19. 貴社で現状以上の情報セキュリティ対策を実施するためには、どのような効果が期待できれば対策を行うと思いますか。あてはまるものを下記よりすべてお選びください。
（MA）

どの企業規模でももっと多い回答は「従業員の情報セキュリティへの意識向上」である。次いで対処すべきリスクの特定が上がっている。

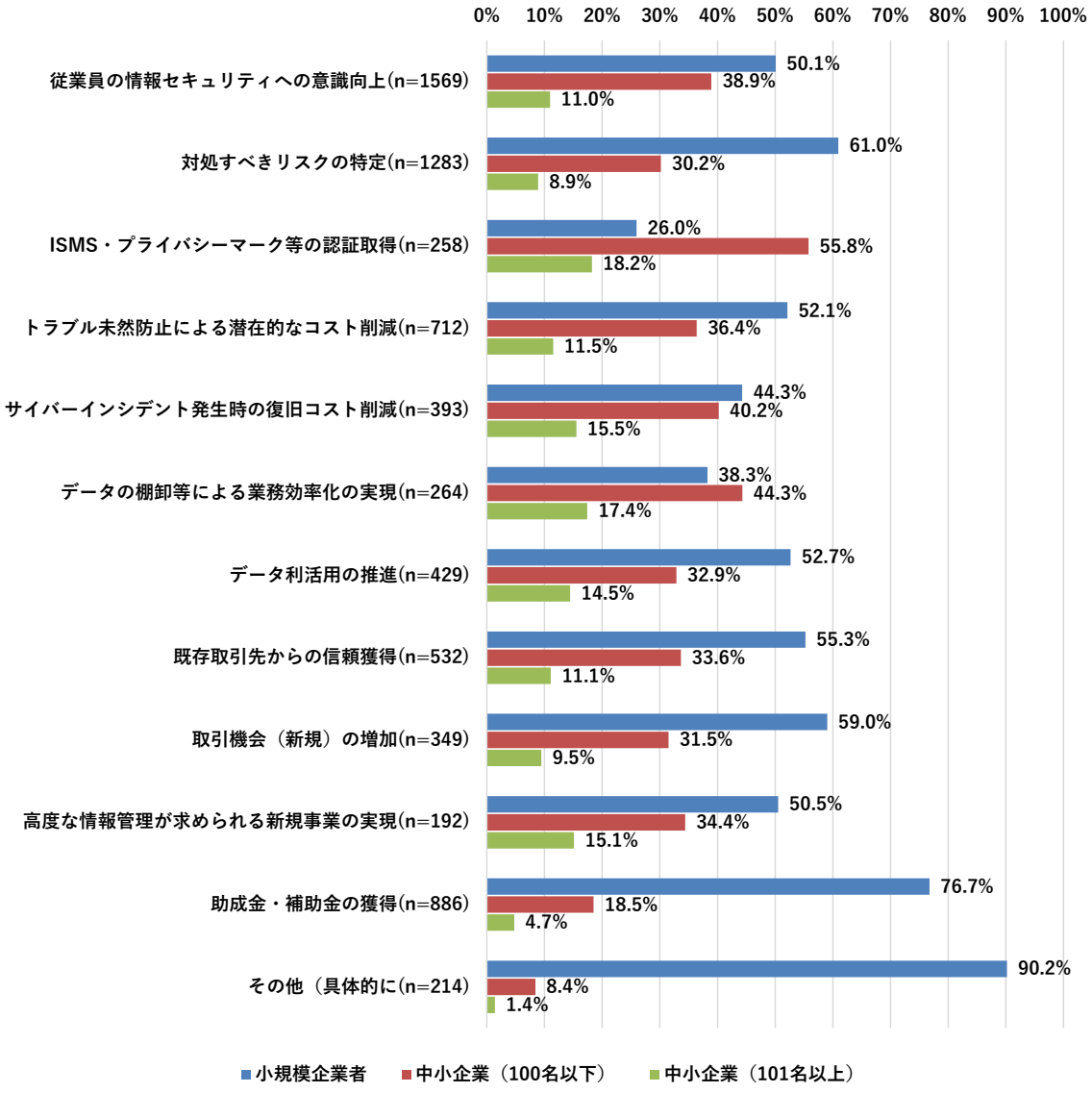

図 3-129 情報セキュリティ対策に期待する効果(企業規模別)(n=4191)

n. 情報セキュリティ対策をさらに向上させるために必要と思われること

Q20. 貴社の情報セキュリティ対策を、さらに向上させるために必要と思うことは何ですか。（MA）

小規模企業者では特にないが 5 割弱と最も多く、次いで経営者のサイバーセキュリティリスク意識向上となっている。中小企業（101 名以上）では従業員の情報セキュリティ意識向上が最も多くなっている。

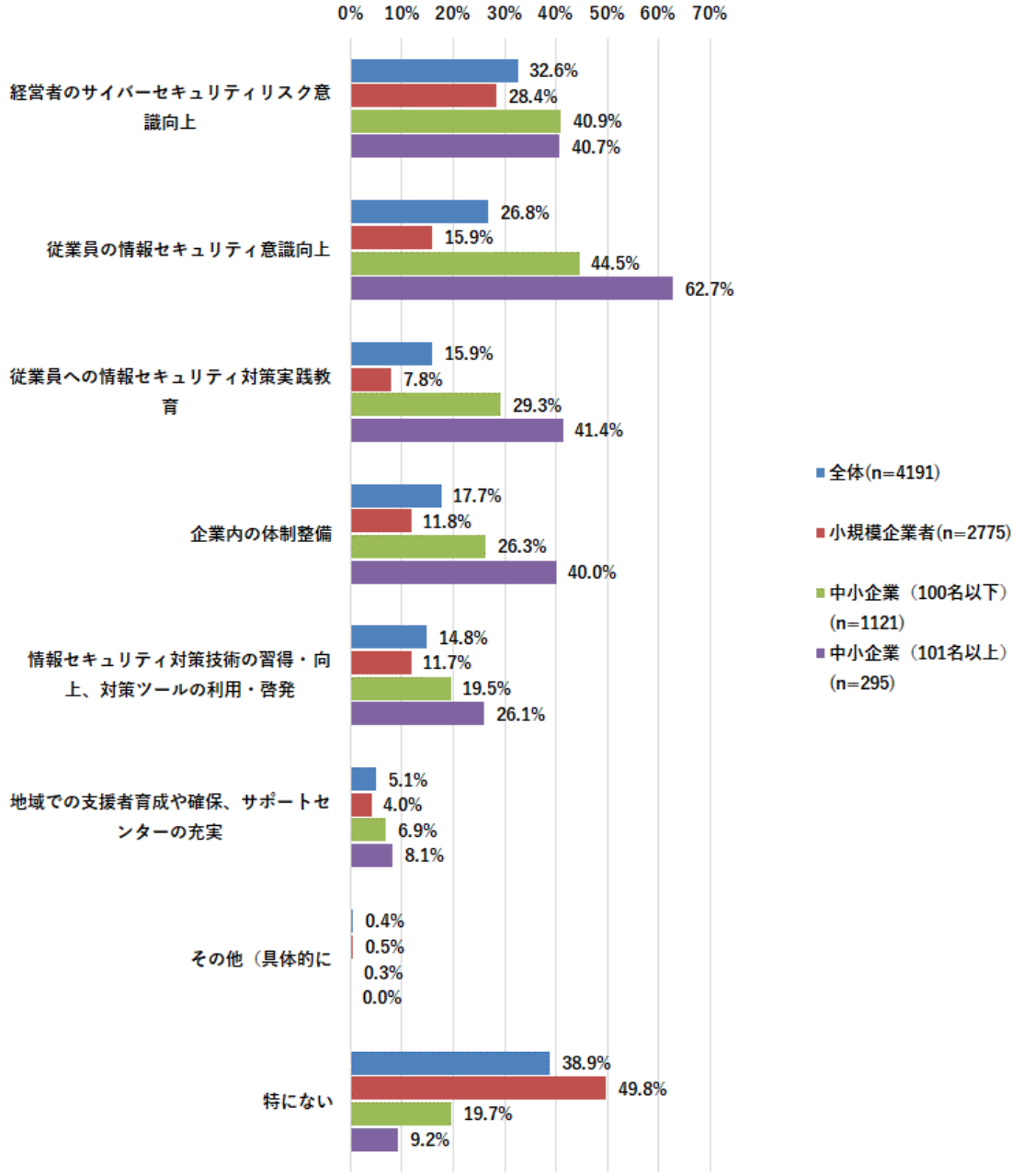

図 3-130 情報セキュリティ対策を、さらに向上させるために必要と思うこと（企業規模別）（n=4191）

3.3.2 業種によるクロス集計結果

概要設問 SC1 の回答選択肢の業種についてクロス集計を行った。具体的には以下の通りである。

- 農業
- 林業
- 漁業
- 鉱業、採石業、砂利採取業
- 建設業
- 製造業
- 電気・ガス・熱供給・水道業
- 情報通信業
- 運輸業、郵便業
- 卸売業
- 小売業
- 金融業、保険業
- 不動産業、物品賃貸業
- 学術研究、専門・技術サービス業
- 宿泊業、飲食サービス業
- 生活関連サービス業、娯楽業
- 教育、学習支援業
- 医療、福祉
- 複合サービス事業
- その他のサービス業

a. 利用・導入しているサービスやシステム

Q5. 貴社では経営資源の確保や業務の効率化に IT を活用されていますか。情報セキュリティ対策サービス以外で利用・導入されているサービスやシステムについて教えてください。 あてはまるものを下記よりすべてお選びください。(MA)

業界ごとに各システムの導入状況を可視化した。多くの業種で電子メール(独自ドメイン)が多く、次いで Web サイト、ホームページの開設となっている。

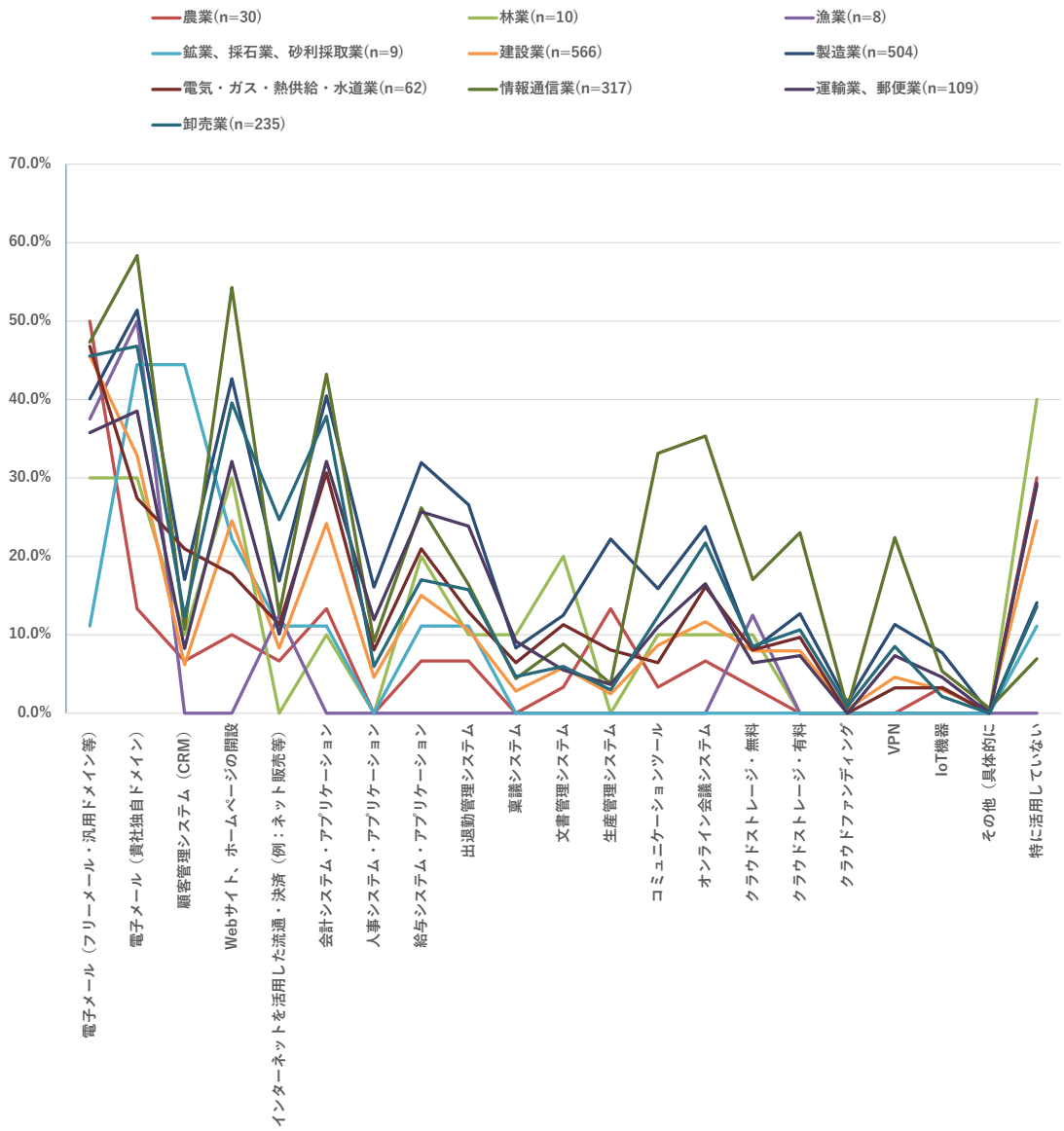

図 3-131 情報セキュリティ対策サービス以外で利用・導入されているサービスやシステム(業種別)①
(n=4191)

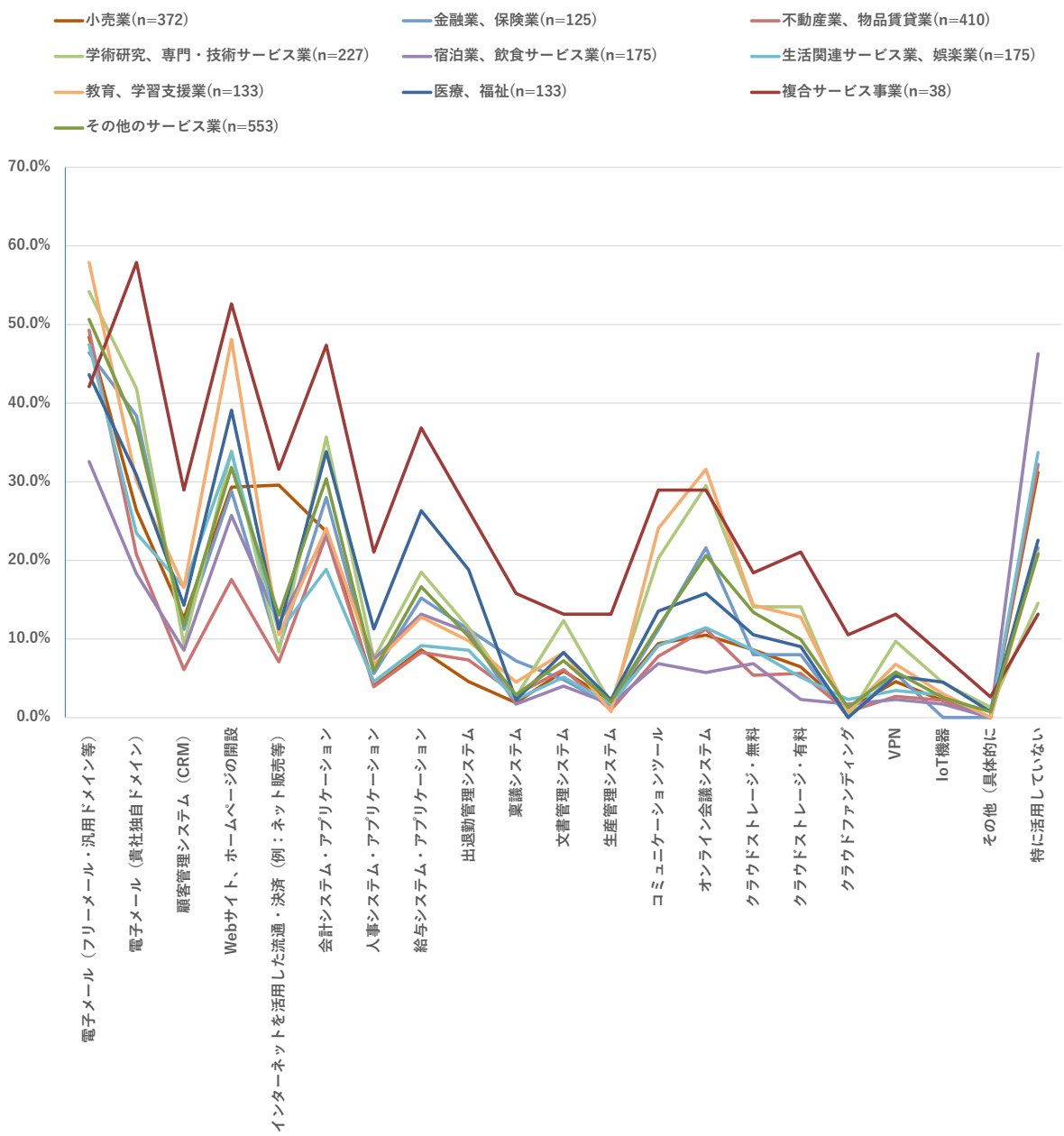

図 3-132 情報セキュリティ対策サービス以外で利用・導入されているサービスやシステム(業種別)②
(n=4191)

同様に、業種別での利用システムの傾向を可視化した。多くの業種で電子メール、WEB サイト、ホームページの利用が多くなっている。学術研究、専門・技術サービス業および教育、学習支援業で利用割合が 5 割を超えている。

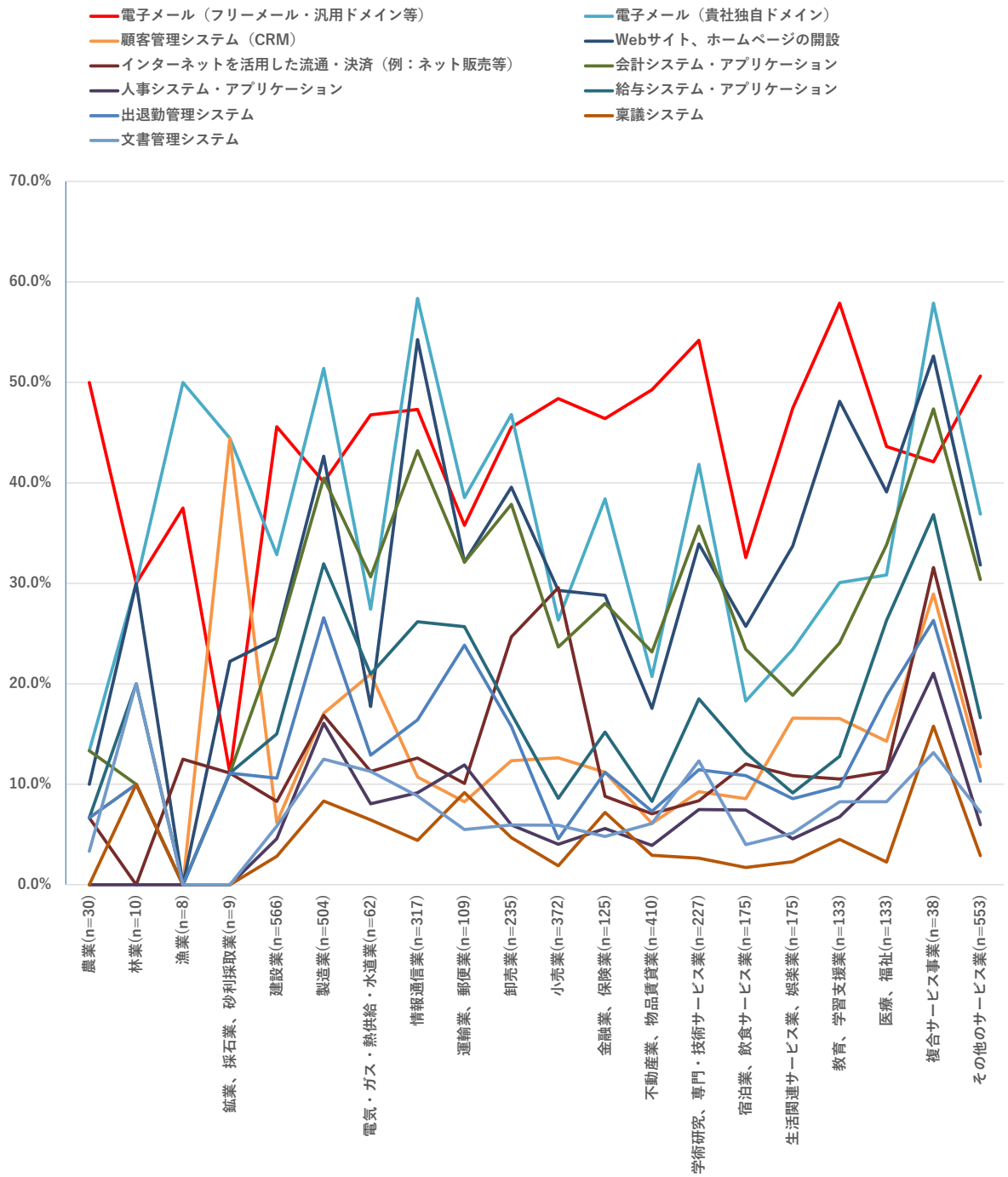

図 3-133 情報セキュリティ対策サービス以外で利用・導入されているサービスやシステム(業種別)③
(n=4191)

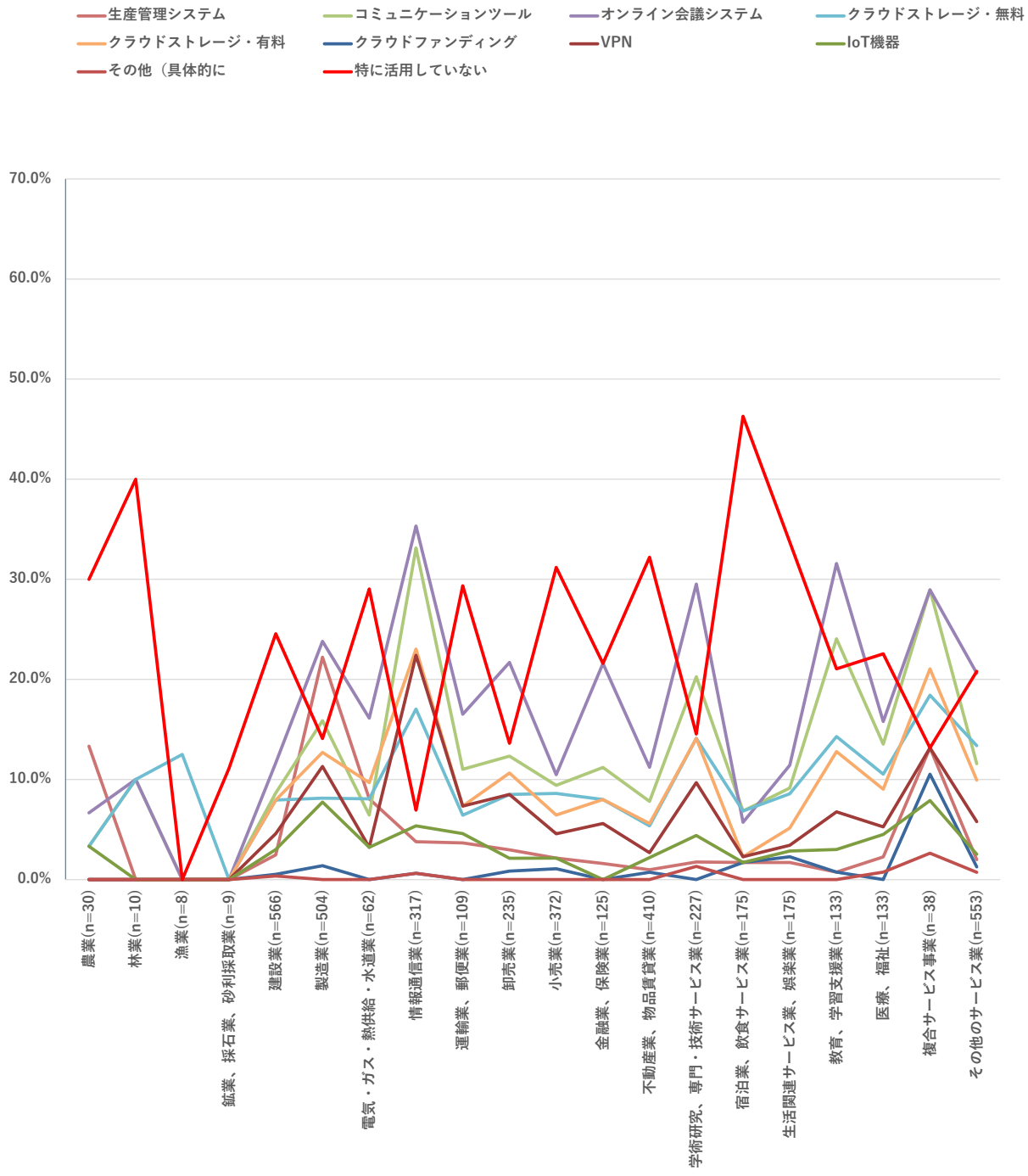

図 3-134 情報セキュリティ対策サービス以外で利用・導入されているサービスやシステム(業種別)④
(n=4191)

b. 直近過去3期の情報セキュリティ対策投資額

Q6 項目 2. 貴社における、直近過去 3 期の IT 投資額(情報セキュリティ投資額を含む)と、情報セキュリティ対策投資額(IT 機器や社員への教育等も含む)の概算について教えてください。
-情報セキュリティ対策投資額(IT 機器や社員への教育等も含む)(SA)

業種ごとの情報セキュリティ投資額の傾向を可視化した。投資していないとの回答の割合が最も多いのは小売業、宿泊業、飲食サービス業で 75%程度である。

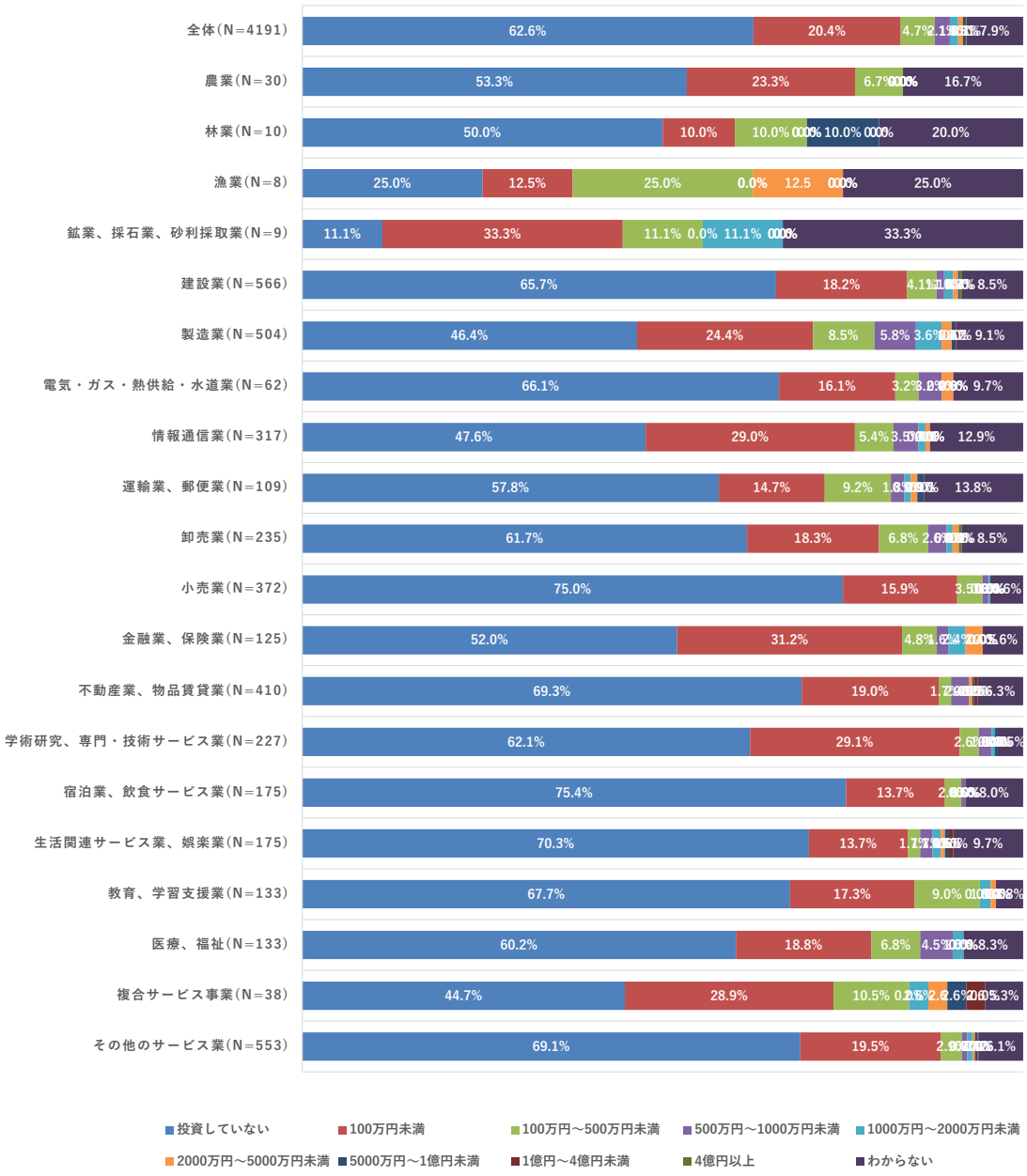

図 3-135 直近過去 3 期の情報セキュリティ対策投資額(業種別)(n=4191)

c. 情報セキュリティ対策投資を行わなかった理由

Q7.（Q6-2.で「1.投資していない」と回答された方について）前問で情報セキュリティ対策投資額について「投資をしていない」とお答えになった一番の理由について教えてください。（SA）

情報セキュリティ投資の必要性を感じていないと回答した割合が最も高い業種は、回答数が 1 件の業種を除き不動産業、物品賃貸であり、6 割が必要性を感じていないと回答している。

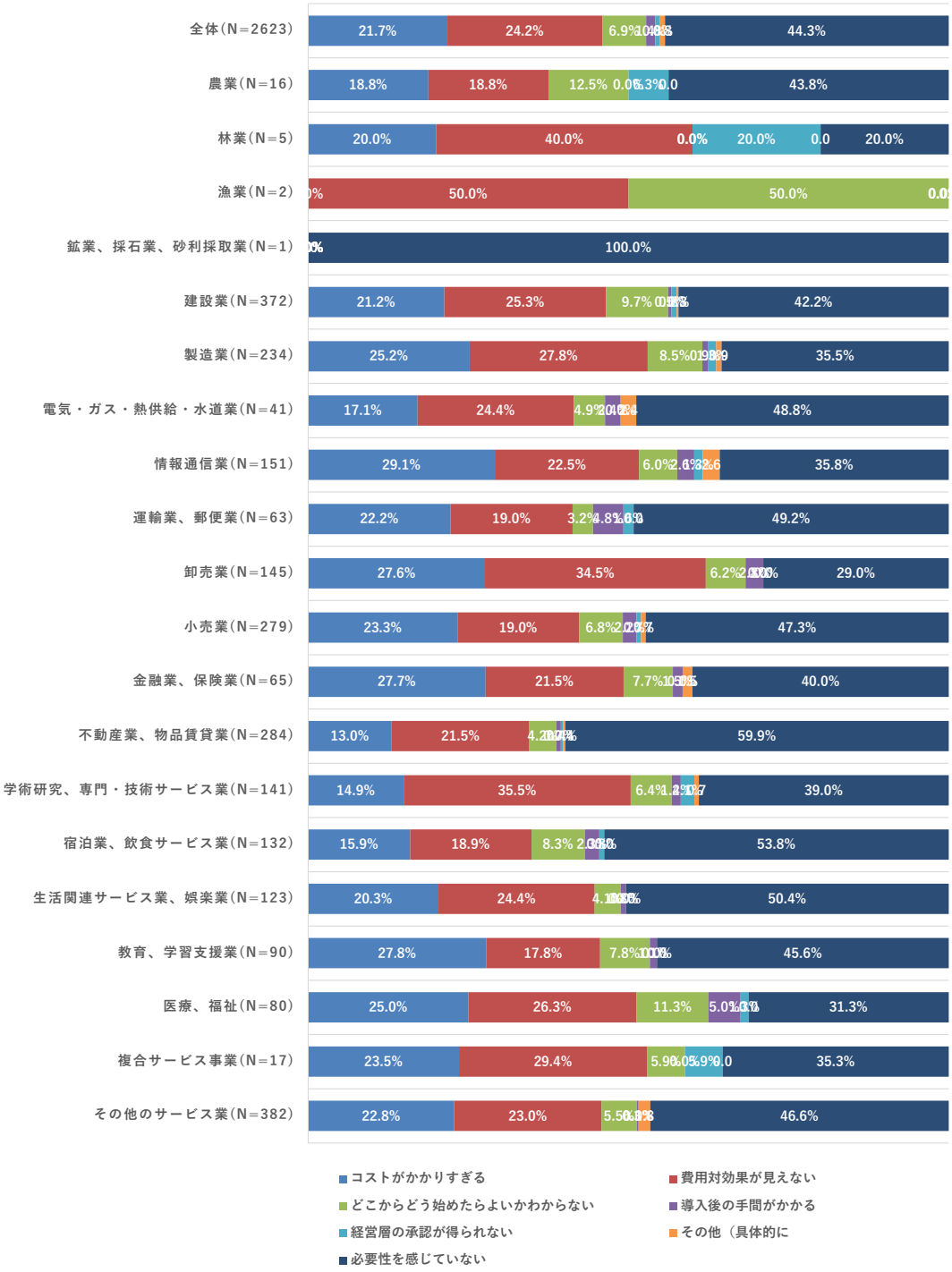

図 3-136 情報セキュリティ対策投資額について「投資をしていない」と回答した一番の理由（業種別）（n=2623）

Q8.（Q7.で「必要性を感じていない」と回答された方について）前問で情報セキュリティ対策投資について「必要性を感じていない」とお答えになった理由について教えてください。 あてはまるものを下記よりすべてお選びください。（MA）

必要性を感じていない理由として多くの業種で、重要情報を保有していないためとの回答が多い。

特徴が見られた業種について以下に示す。

- 電気、ガス、熱供給、水道業は、重要情報を保有していないと考えている割合が高い。
- 金融、保険業は、既に十分な対策がとられている割合が高い。
- 宿泊業、飲食サービス業は、他社との NW 接続がない割合が高い。
- 教育、学習支援業は、重要情報を保有していないと考えている割合が高い。
- 複合サービス業は、事業継続に大きな影響がないと考えている割合が高い。

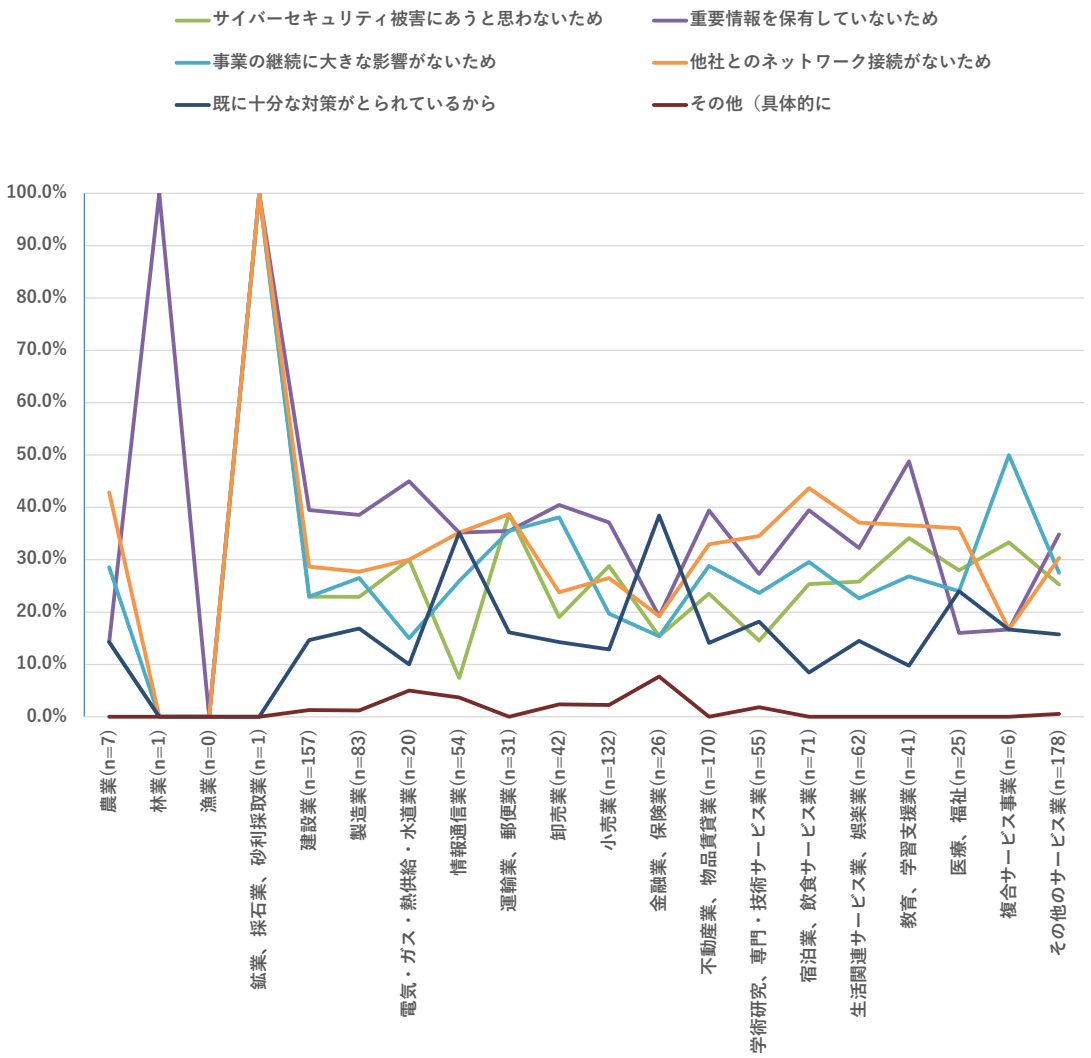

図 3-137 情報セキュリティ対策投資について「必要性を感じていない」と回答した理由（業種別）
（n=1162）

d. セキュリティパッチの適用状況

Q14.（Q9 で「対策の必要性を感じたことがない」以外の回答をされた方について）貴社ではサーバ等にセキュリティパッチを適用していますか。パッチを適用していない場合は理由について教えてください。 あてはまるものを下記よりすべてお選びください。（MA）

情報通信業ではパッチを提供している割合が 6 割を超えて多い、一報で生活関連サービス業、娯楽業ではパッチの適用に多大なコストがかかるため適用していないとの回答が多い。

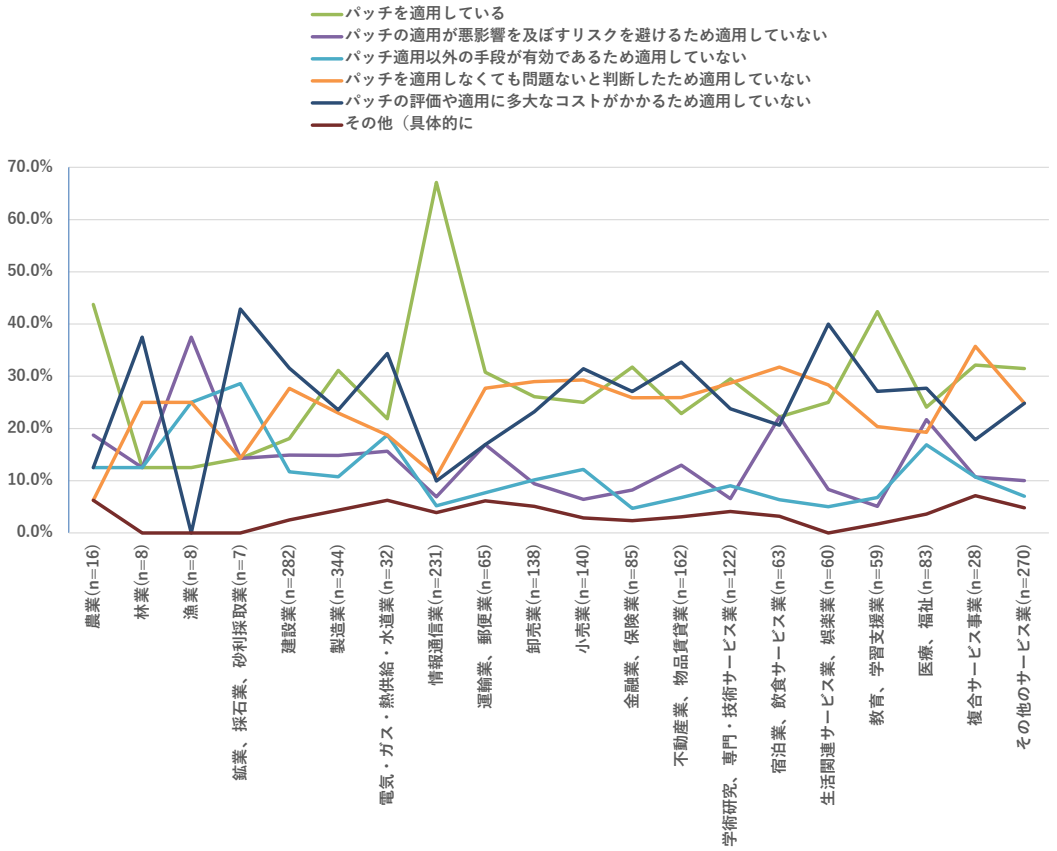

図 3-138 セキュリティパッチの適用状況（業種別）（n=2203）

e. 組織体制

Q22. 貴社の情報セキュリティ対策はどのような体制で行われていますか。(SA)

業種別にみると、製造業、情報通信業、運輸業、郵便業、複合サービス事業、医療、福祉において、専門部署の設置や担当者の任命(兼務も含む)が実施されていることが分かる。

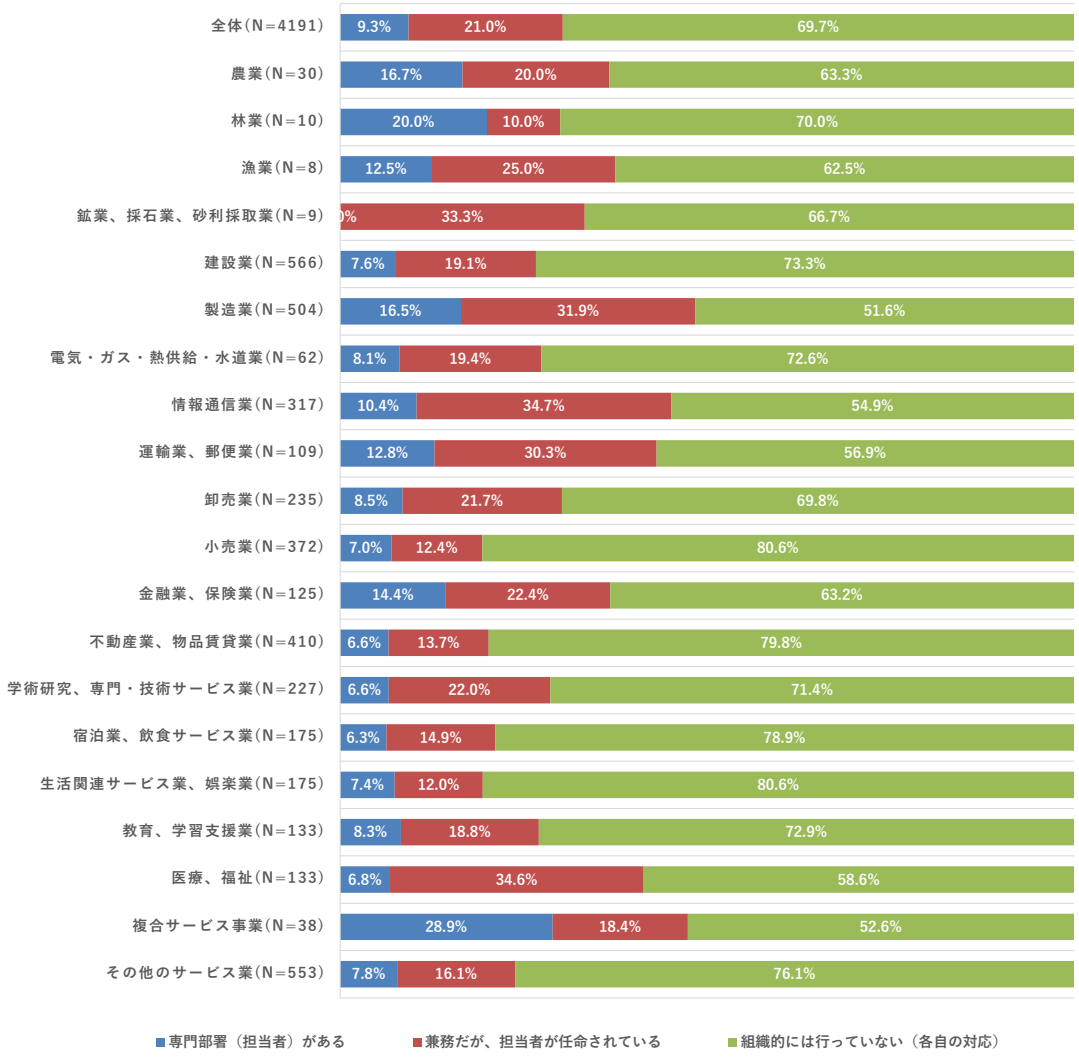

図 3-139 情報セキュリティ対策の体制(業種別)(n=4191)

f. 困ったことがあった際の相談先

Q23. 貴社の情報セキュリティ対策に関して困ったことがあった際の相談先を教えてください。あてはまるものを下記よりすべてお選びください。(MA)

多くの業種で相談先が特にないとの回答が多い。複合サービス事業と製造業では逆に社内の担当者の割合が最も多い。

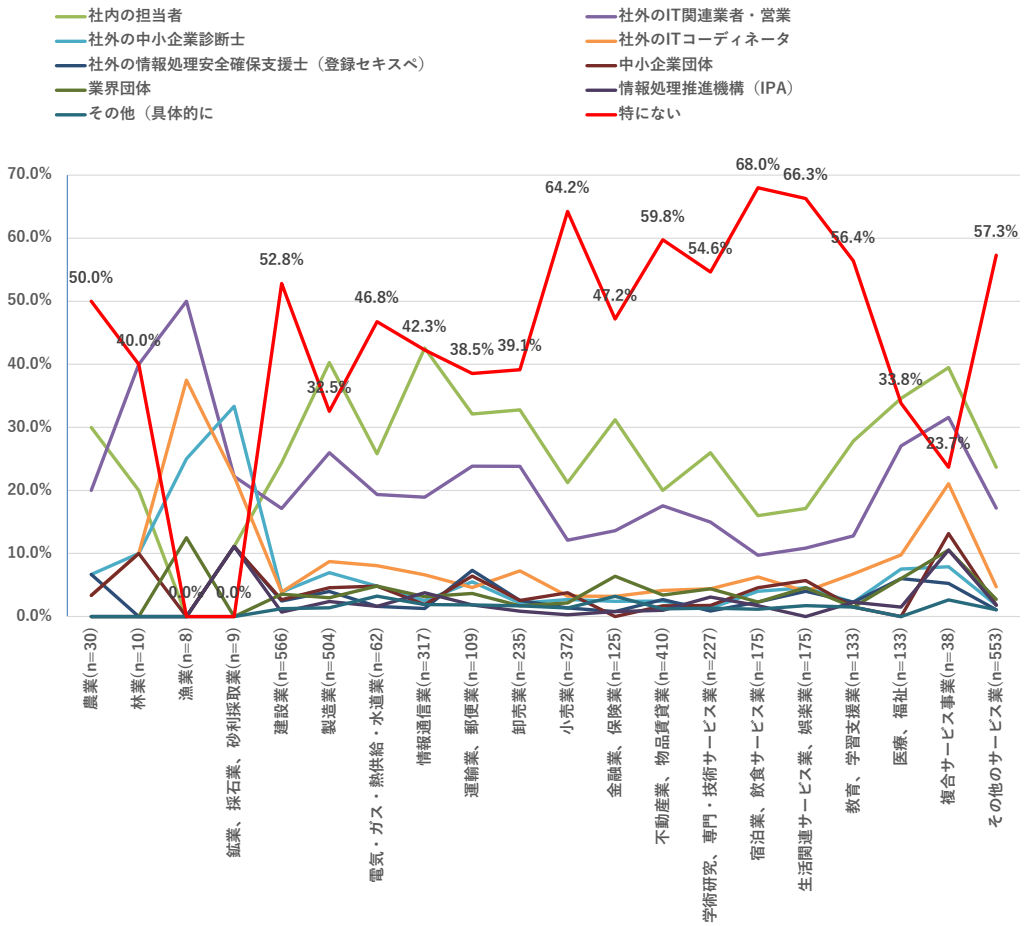

図 3-140 情報セキュリティ対策に関して困ったことがあった際の相談先(業種別)(n=4191)

g. 活用したい情報セキュリティ対策に関するサービス

Q21. どのような情報セキュリティ対策に関するサービスがあれば活用したいと思いますか。 あてはまるものを下記よりすべてお選びください。(MA)

業種を通じて経営層向けの手引書が最も多い。

特徴が見られた業種について以下に示す。

- 運送業、郵便業は、経営層への教育が多い傾向にある。
- 不動産業、物品賃貸業、宿泊業、飲食サービス業は、経営層へ手引書が多い傾向にある。
- 複合サービス事業は、中小企業向け情報セキュリティ対策に関する定期的な情報発信が多い傾向にある。

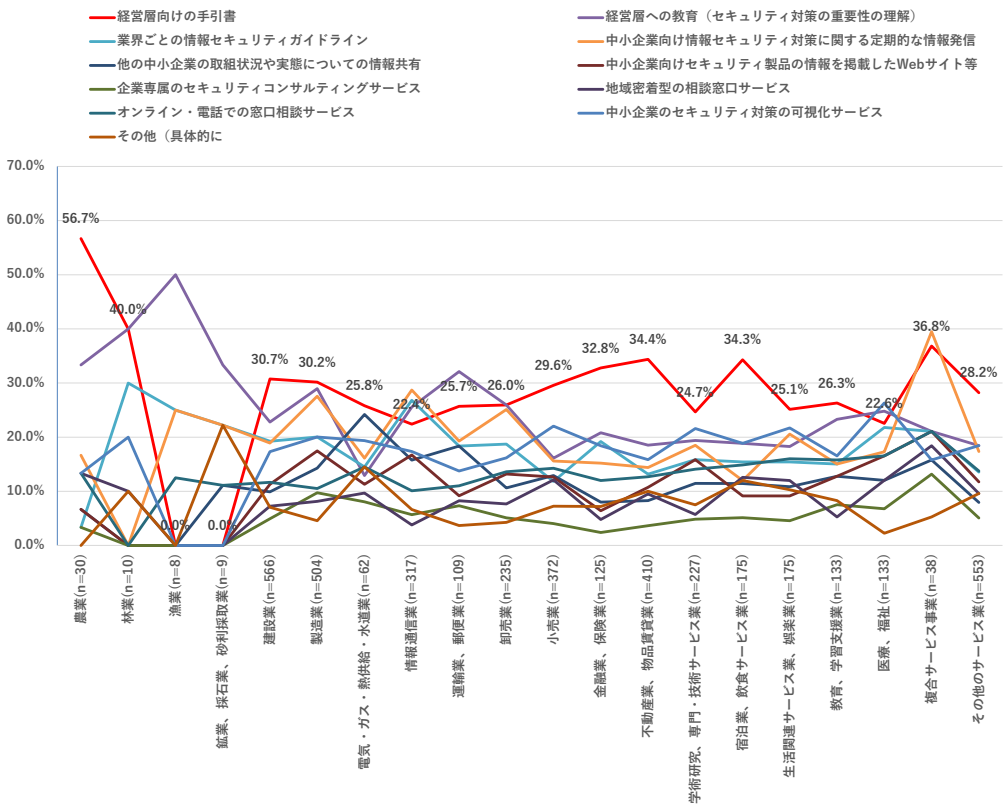

図 3-141 活用したい情報セキュリティ対策に関するサービス(業種別)(n=4191)

h. 情報セキュリティに関する情報収集先

Q24. 貴社の情報セキュリティ対策に関する情報収集先を教えてください。 あてはまるものを下記よりすべてお選びください。(MA)

業種を通じて特に無いが多い。製造業、情報通信業では社内の担当者がもっと多くなっている。

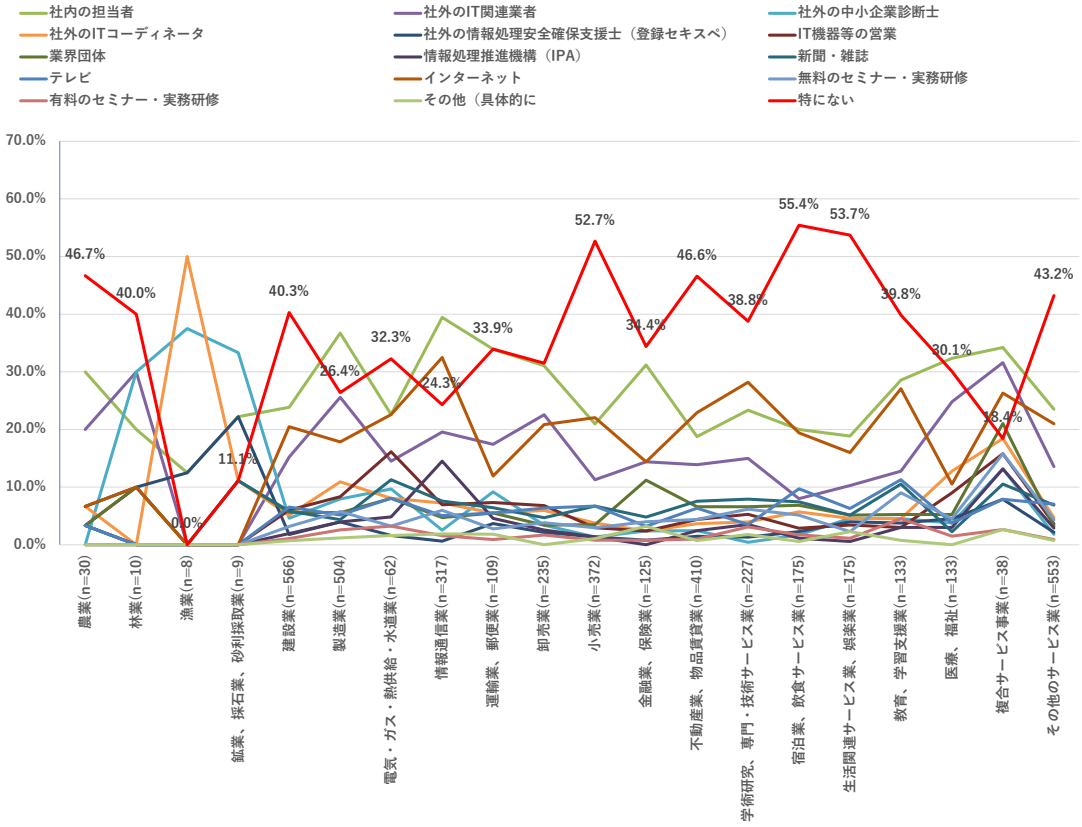

図 3-142 情報セキュリティ対策に関する情報収集先(業種別)(n=4191)

i. 従業員に対する情報セキュリティ教育の実施状況

Q25. 貴社では従業員に対する情報セキュリティ教育をどのように実施していますか。(MA)

業種を通じて特に実施していないが最も多い。金融業、保険業では e ラーニングが多くなっている。

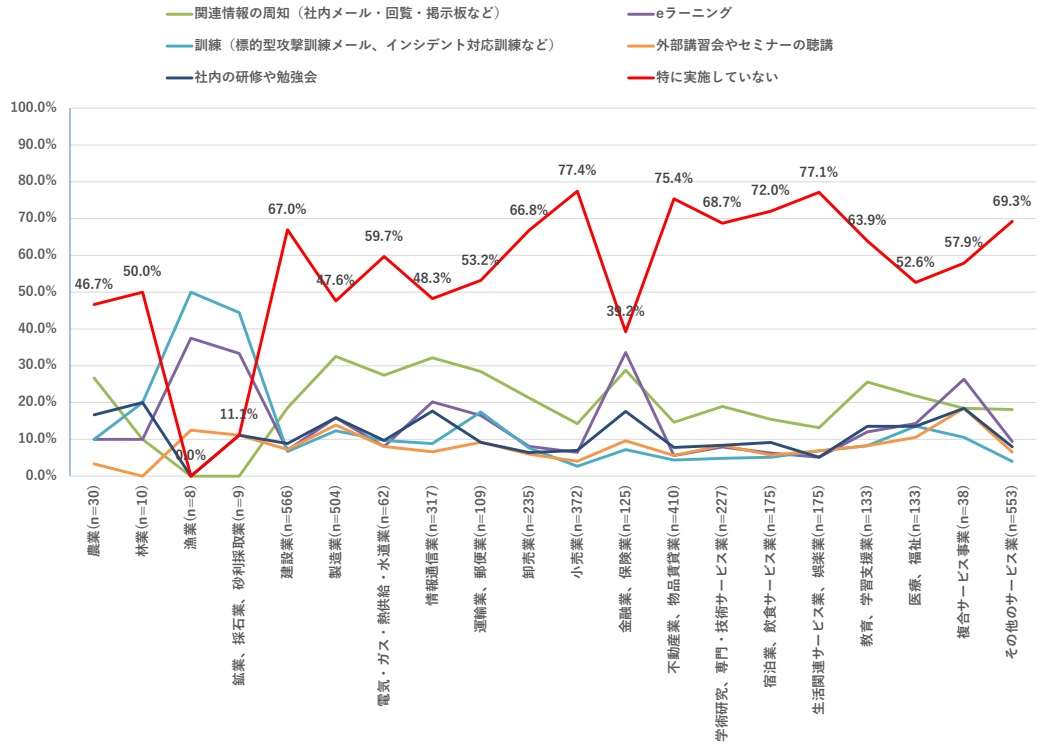

図 3-143 従業員に対する情報セキュリティ教育の実施状況(業種別)(n=4191)

j. 情報漏えい等のインシデント又はその兆候を発見した場合の報告先

Q15. 貴社で情報漏洩等のインシデント又はその兆候を発見した場合に、規定されている報告先は何ですか。 あてはまるものを下記よりすべてお選びください。(MA)

業種を通じて経営者への報告が多い傾向にある。業種を通じて経営層向けの手引書が最も多い。特徴が見られた業種について以下に示す。

・ 小売業、不動産、物品賃貸業、宿泊業、飲食サービス業、生活関連サービス業、娯楽業、教育、学習支援業は、報告先が決まっていない傾向が多い傾向にある。

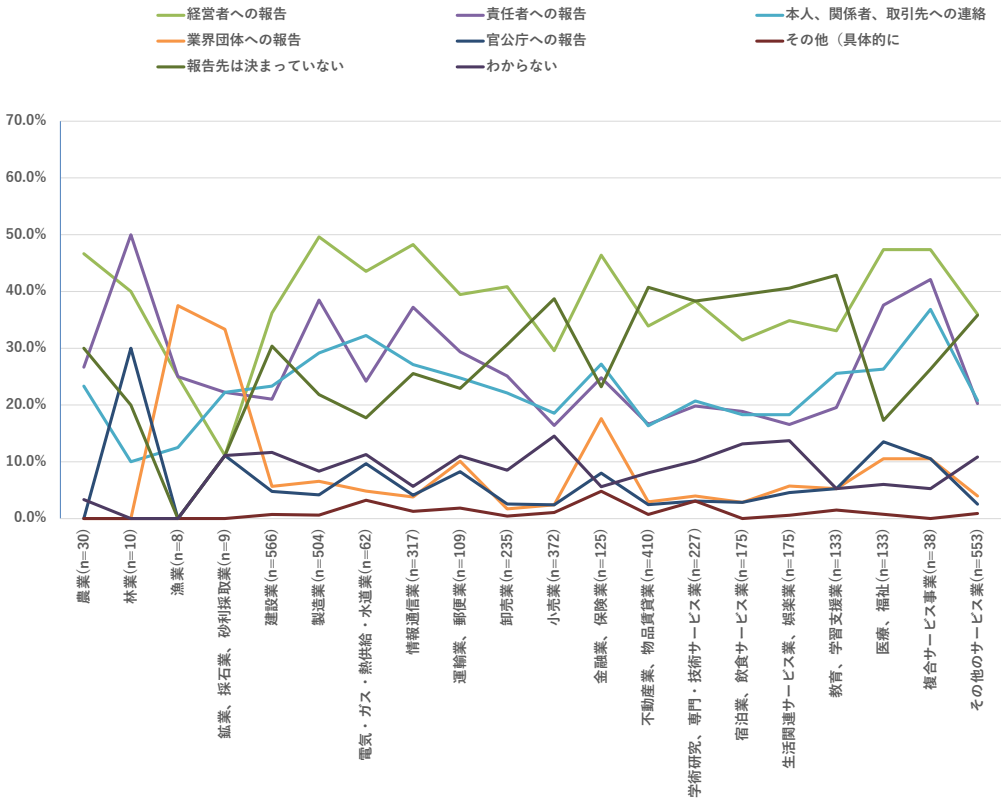

図 3-144 情報漏えい等のインシデント又はその兆候を発見した場合の報告先(業種別)(n=4191)

k. 情報漏えい等のインシデント又はその兆候を発見した場合の対応方法

Q16. 貴社で情報漏洩等のサイバーインシデント又はその兆候を発見した場合の対応方法として規定されているものは何ですか。 あてはまるものを下記よりすべてお選びください。(MA)

対応方法が特に決まっていないと回答する割合が多い業種は、宿泊業、飲食サービス業、不動産業、物品賃貸業、小売業で 5 割程度となっている。

特徴が見られた業種について以下に示す。

・ 情報通信業、金融業、保険業、複合サービス事業は、情報の隔離が多い傾向にある。

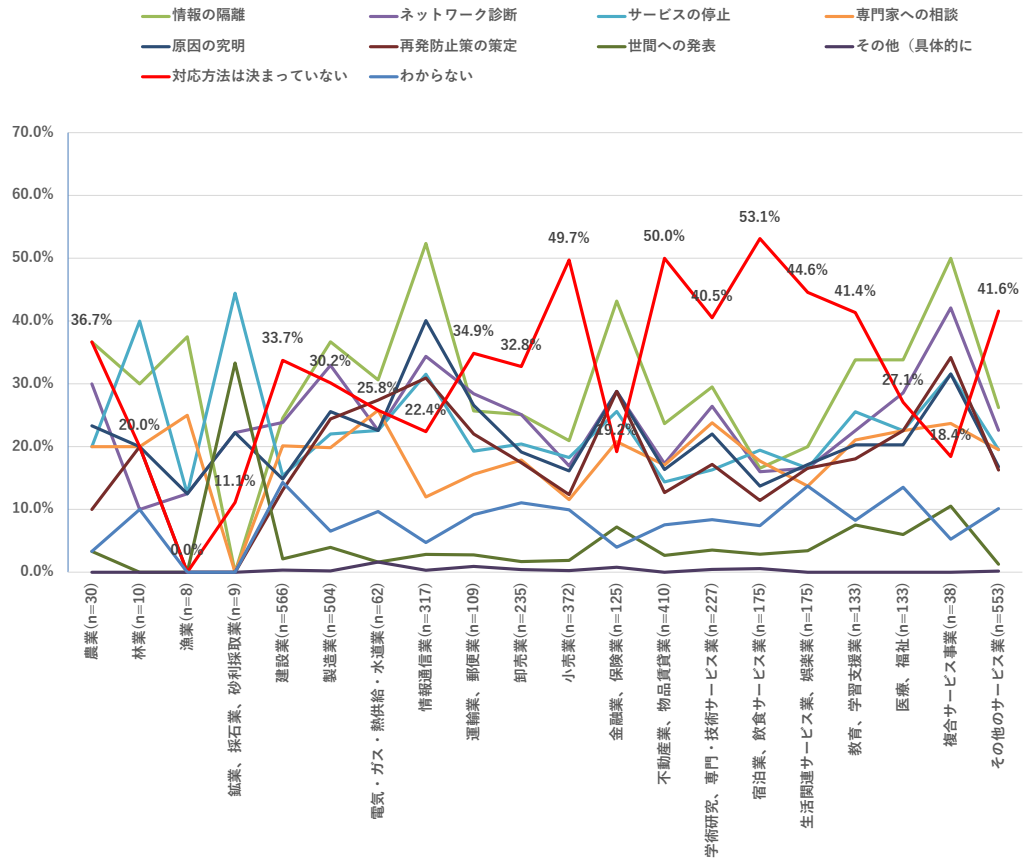

図 3-145 サイバーインシデント又はその兆候を発見した場合の対応方法(業種別)(n=4191)

l. 情報セキュリティ関連製品やサービスの導入状況

Q12.（Q9 で「対策の必要性を感じたことがない」以外の回答をされた方について）貴社では情報セキュリティ関連製品やソフトウェアを導入していますか。 導入している情報セキュリティ関連製品やソフトウェアを教えてください。 あてはまるものを下記よりすべてお選びください。（MA）

業種を通じてウイルス対策ソフトは導入されている。次いでファイアウォールの導入が多い。

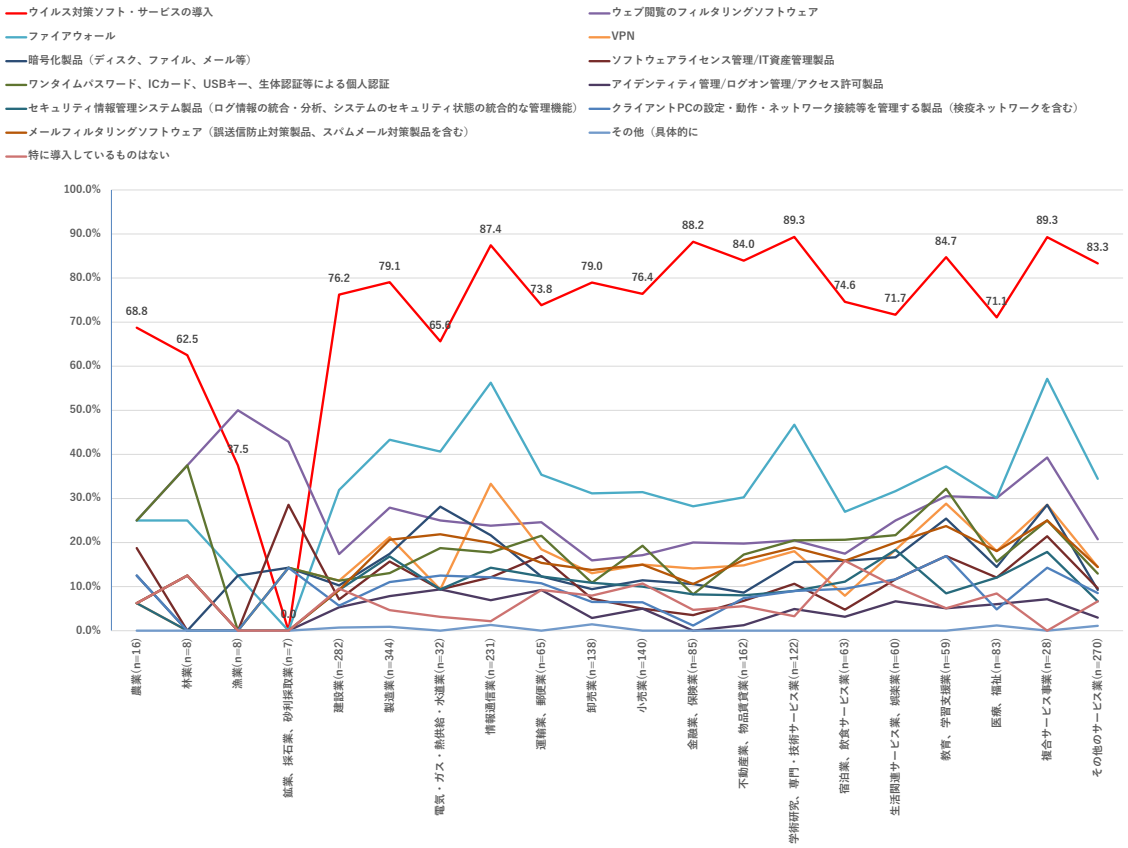

図 3-146 情報セキュリティ関連製品やソフトウェアの導入状況（業種別）（n=2203）

m. 情報セキュリティ対策に期待する効果

Q19. 貴社で現状以上の情報セキュリティ対策を実施するためには、どのような効果が期待できれば対策を行うと思いますか。あてはまるものを下記よりすべてお選びください。
（MA）

業種　を通じて、従業員の情報セキュリティへの意識向上と回答する割合が高く、次いで対応すべきリスクの特定となっている。

特徴が見られた業種について以下に示す。

・電気・ガス・熱供給・水道業は、トラブル未然防止による潜在的なコスト削減が多い傾向にある。

・宿泊業、飲食サービス業は、助成金・補助金の獲得が多い傾向にある。

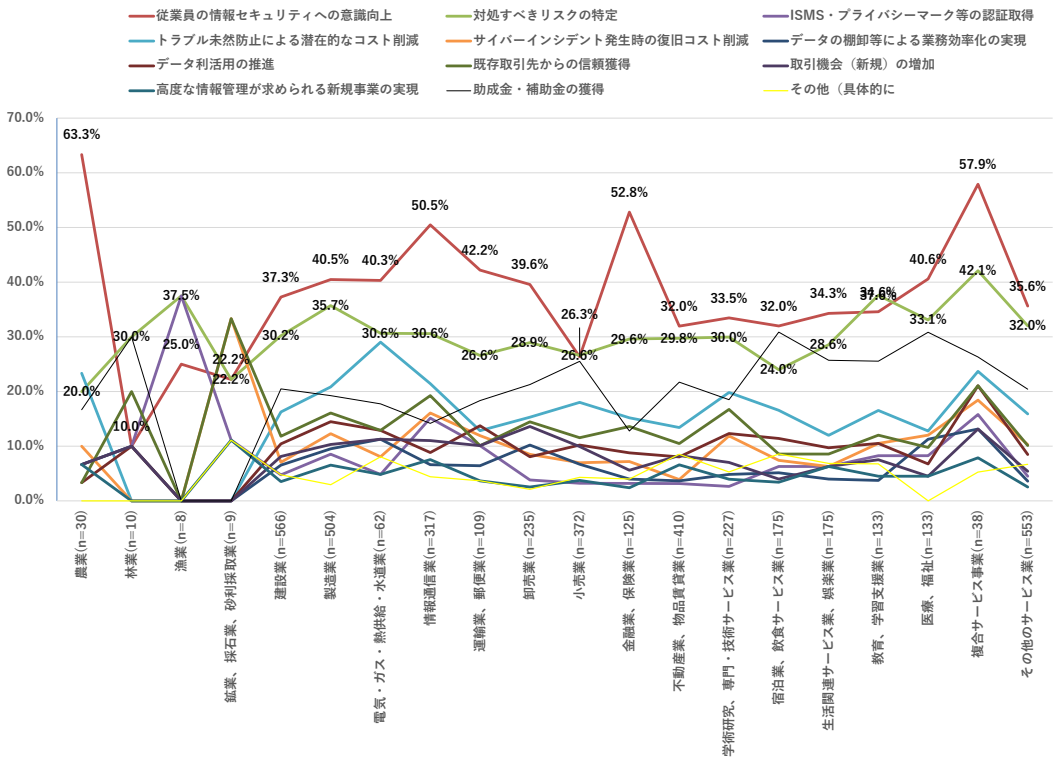

図 3-147　情報セキュリティ対策に期待する効果（業種別）（n=2203）

n. 情報セキュリティ対策をさらに向上させるために必要と思われること

Q20. 貴社の情報セキュリティ対策を、さらに向上させるために必要と思うことは何ですか（MA）

宿泊業、飲食サービス業、生活関連サービス業、娯楽業では特にないの回答割合が高い。金融保険業、複合サービス業では、経営層のサイバーセキュリティリスク意識向上が多い。

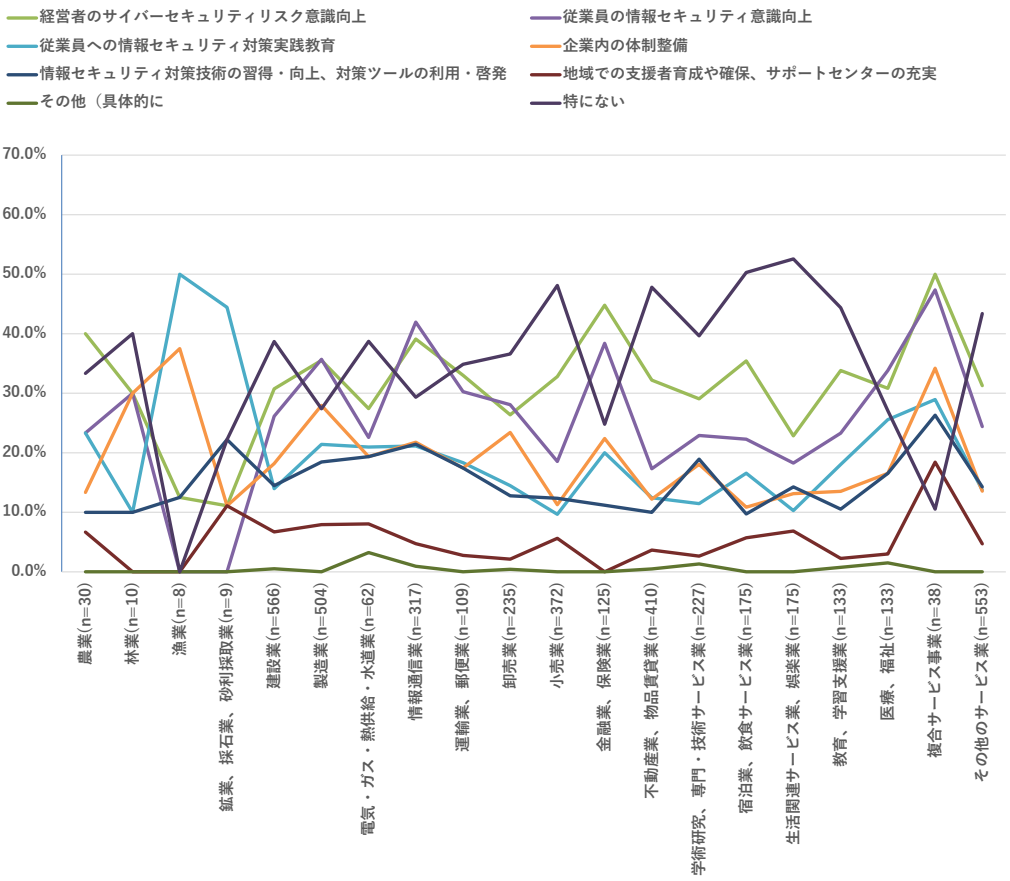

図 3-148 情報セキュリティ対策を、さらに向上させるために必要と思うこと（業種別）（n=4191）

o. 情報セキュリティ対策投資額と売上高に占める割合

業種別の情報セキュリティ対策投資額の平均値および売上高（直近会計年度）に占める割合を分析しした。投資額と売上高の平均値は、回答企業全ての平均と、投資していると回答した企業のみの平均をそれぞれ算出した。

回答企業全てについて、情報セキュリティ対策投資額（単年度換算）の平均値は 60 万円であり、平均値が高い業種は、「製造業」が最も高く 102 万円、次いで「卸売業」で 95 万円、「生活関連サービス業、娯楽業」で 91 万円、「建設業」で 83 万円であった。また、低い業種は、「宿泊業、飲食サービス業」が最も低く 7 万円、次いで「小売業」で 10 万円、「教育、学習支援業」で 29 万円、「医療、福祉」で 31 万円であった。

情報セキュリティ対策投資を行っている企業のみについて、情報セキュリティ対策投資額（単年度換算）の平均値は 188 万円であり、平均値が高い業種は、「生活関連サービス業、娯楽業」が最も高く 413 万円、次いで「建設業」と「卸売業」が 293 万円、「不動産業、物品賃貸業」で 260 万円、「製造業」で 208 万円であった。また、低い業種は、「宿泊業、飲食サービス業」が最も低く 36 万円、次いで「小売業」で 46 万円、「学術研究、専門・技術サービス業」で 73 万円、「情報通信業」で 79 万円であった。

なお、回答数が 100 件より少ない農業、林業、漁業、鉱業、採石業、砂利採取業、複合サービス事業は除外している。

表 3-4 情報セキュリティ対策投資額と売上高に占める割合(回答企業全て)

業種	回答数 ※1	情報セキュリティ対策投資額(単年度換算) ※2	売上高 ※3	割合
全体	3862 件	60 万円	9,587 万円	0.6%
農業	25 件	13 万円	4,696 万円	0.3%
林業	8 件	327 万円	8,450 万円	3.9%
漁業	6 件	231 万円	6,375 万円	3.6%
鉱業、採石業、砂利採取業	6 件	108 万円	10,722 万円	1.0%
建設業	518 件	83 万円	10,495 万円	0.8%
製造業	458 件	102 万円	16,545 万円	0.6%
電気・ガス・熱供給・水道業	56 件	36 万円	8,741 万円	0.4%
情報通信業	276 件	36 万円	10,047 万円	0.4%
運輸業、郵便業	94 件	63 万円	14,620 万円	0.4%
卸売業	215 件	95 万円	14,779 万円	0.6%
小売業	355 件	10 万円	6,355 万円	0.2%
金融業、保険業	118 件	57 万円	10,093 万円	0.6%
不動産業、物品賃貸業	384 件	68 万円	7,711 万円	0.9%
学術研究、専門・技術サービス業	219 件	26 万円	6,403 万円	0.4%
宿泊業、飲食サービス業	161 件	7 万円	5,423 万円	0.1%
生活関連サービス業、娯楽業	158 件	91 万円	5,477 万円	1.7%
教育、学習支援業	128 件	29 万円	5,968 万円	0.5%
医療、福祉	122 件	31 万円	9,492 万円	0.3%
複合サービス事業	36 件	363 万円	11,711 万円	3.1%
その他のサービス業	519 件	43 万円	7,240 万円	0.6%

※1 回答数は情報セキュリティ対策投資額に対する質問(Q6 項目 2)に対して「わからない」と回答した企業を除いた値

※2 情報セキュリティ対策投資額に対する質問(Q6 項目 2)に「わからない」と回答した企業を除き、同質問の回答選択肢ごとに階級値を設定して平均値を算出

※3 情報セキュリティ対策投資額に対する質問(Q6 項目 2)に「わからない」と回答した企業を除き、売上高に対する質問(Q2)の回答選択肢ごとに階級値を設定して平均値を算出

表 3-5 情報セキュリティ対策投資額と売上高に占める割合(情報セキュリティ対策投資を行っている企業のみ)

業種	投資していると回答した企業数 ※4	情報セキュリティ対策投資額(単年度換算) ※5	売上高 ※6	割合
全体	1217 件	188 万円	15,336 万円	1.2%
農業	9 件	35 万円	4,722 万円	0.7%
林業	3 件	872 万円	13,833 万円	6.3%
漁業	4 件	346 万円	10,500 万円	3.3%
鉱業、採石業、砂利採取業	5 件	130 万円	5,000 万円	2.6%
建設業	144 件	293 万円	16,361 万円	1.8%
製造業	222 件	208 万円	20,601 万円	1.0%
電気・ガス・熱供給・水道業	14 件	136 万円	12,393 万円	1.1%
情報通信業	124 件	79 万円	12,859 万円	0.6%
運輸業、郵便業	31 件	191 万円	20,629 万円	0.9%
卸売業	70 件	293 万円	22,414 万円	1.3%
小売業	73 件	46 万円	12,630 万円	0.4%
金融業、保険業	53 件	127 万円	14,028 万円	0.9%
不動産業、物品賃貸業	98 件	260 万円	13,689 万円	1.9%
学術研究、専門・技術サービス業	76 件	73 万円	10,079 万円	0.7%
宿泊業、飲食サービス業	28 件	36 万円	13,607 万円	0.3%
生活関連サービス業、娯楽業	35 件	413 万円	12,114 万円	3.4%
教育、学習支援業	36 件	99 万円	11,917 万円	0.8%
医療、福祉	41 件	91 万円	13,598 万円	0.7%
複合サービス事業	19 件	689 万円	15,184 万円	4.5%
その他のサービス業	132 件	161 万円	13,292 万円	1.2%

※4 情報セキュリティ対策投資額に対する質問(Q6 項目 2)に対して「投資していない」および「わからない」と回答した企業を除いた値

※5 情報セキュリティ対策投資額に対する質問(Q6 項目 2)に「投資していない」および「わからない」と回答した企業を除き、同質問の回答選択肢ごとに階級値を設定して平均値を算出

※6 情報セキュリティ対策投資額に対する質問(Q6 項目 2)に「投資していない」および「わからない」と回答した企業を除き、売上高に対する質問(Q2)の回答選択肢ごとに階級値を設定して平均値を算出

3.3.3 情報セキュリティ対策投資によるクロス集計

過去 1 期、情報セキュリティ投資を行った企業群と行っていない企業群を比較することで、情報セキュリティへの投資の有効性などの効果の分析を行った。

a. 情報セキュリティ対策投資が取引につながったか

情報セキュリティ対策投資別に見てみると、過去に情報セキュリティ対策投資を行っている企業の 49.8%が、発注元からの要請でサイバーセキュリティ対策を行ったことが取引につながったと回答しているのに対し、そうでない企業は 27.4%に留まっています。

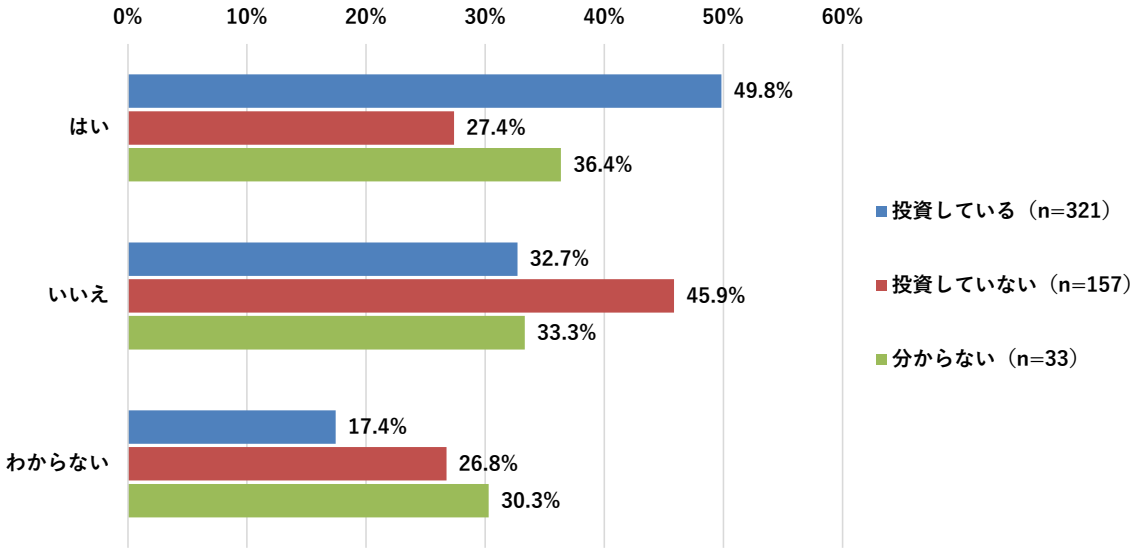

図 3-149 情報セキュリティ対策投資が取引につながったか（n=511）

3.3.4 情報セキュリティ体制によるクロス集計

本設問 Q22.の選択肢とのクロス集計を行うことで、情報セキュリティ体制の整備状況による違いを明らかにした。

セキュリティ体制の整備状況について、「専門部署（担当者）がある」、「兼務だが、担当者が任命されている」を体制が整備されている企業、「組織的には行っている（独自の対応）」を体制が整備されていない企業として区分した場合、体制が整備されていない企業の多くが IT の導入割合が低く、また関連して情報セキュリティ対策投資も少ない状況にある。それらの企業は、「重要情報を保持していない」ことを投資しない理由に挙げており、情報セキュリティ上のリスクに関する認識が低いことが明らかになっている。一方でこれらの企業は困ったことがあった際の連絡先が無いとの回答が多く、サイバーセキュリティに関する問い合わせ先の充実が必要と考えられる。

a. 利用・導入しているサービスやシステム

Q5. 貴社では経営資源の確保や業務の効率化に IT を活用されていますか。情報セキュリティ対策サービス以外で利用・導入されているサービスやシステムについて教えてください。 あてはまるものを下記よりすべてお選びください。（MA）

「電子メール（フリーメール・汎用ドメイン等）」については、情報セキュリティ体制の整備状況よる差異は見られないが、「電子メール（会社独自ドメイン）」、「Web サイト、ホームページの開設」など組織的な管理が必要となるサービスやシステムの利用は、体制が整備されていない企業の方が少ない傾向が読み取れる。また、体制が整備されていない企業は「特に活用していない」の割合が高く、3 割となっている。

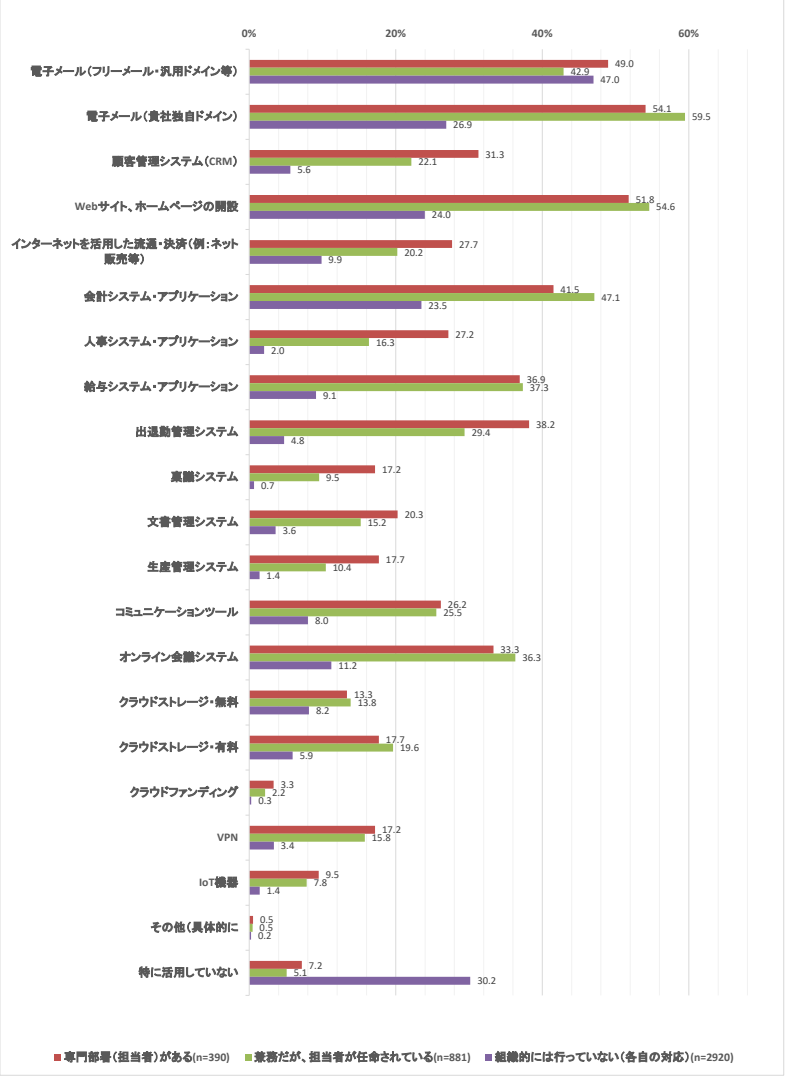

図 3-150 情報セキュリティ対策サービス以外で利用・導入されているサービスやシステム（セキュリティ体制の整備状況別）（n=4191）

b. 直近過去3期の情報セキュリティ対策投資額

Q6 項目 2. 貴社における、直近過去 3 期の IT 投資額（情報セキュリティ投資額を含む）と、情報セキュリティ対策投資額（IT 機器や社員への教育等も含む）の概算について教えてください。
-情報セキュリティ対策投資額（IT 機器や社員への教育等も含む）（SA）

情報セキュリティ体制が整備されてない企業ほど、「投資していない」の割合が高くなり 8 割弱である。一方で専門部署（担当者）があると回答している企業においても、「投資していない」の割合は 3 割となっており、これは「兼務だが、担当者が任命されている」場合においても同様の傾向である。

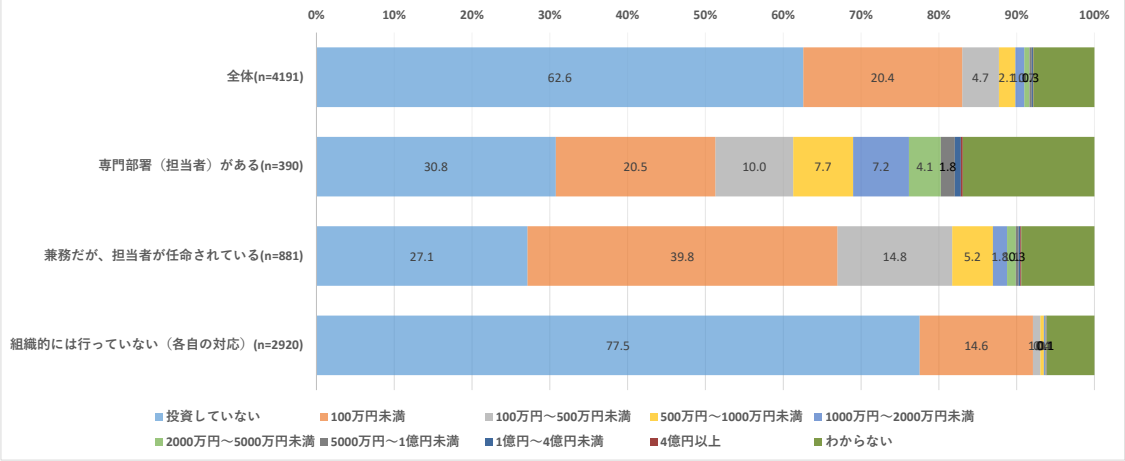

図 3-151 直近過去 3 期の情報セキュリティ対策投資額(IT 機器や社員への教育等も含む)(セキュリティ体制の整備状況別)（n=4191）

c. 情報セキュリティ対策投資を行わなかった理由

Q7.（Q6-2.で「投資していない」と回答された方について）前問で情報セキュリティ対策投資額について「投資をしていない」とお答えになった一番の理由について教えてください。（SA）

体制が整備されていない企業では、「必要性を感じていない」が 5 割弱ともっと多く、専門部署がある企業では 2 割強にとどまる。

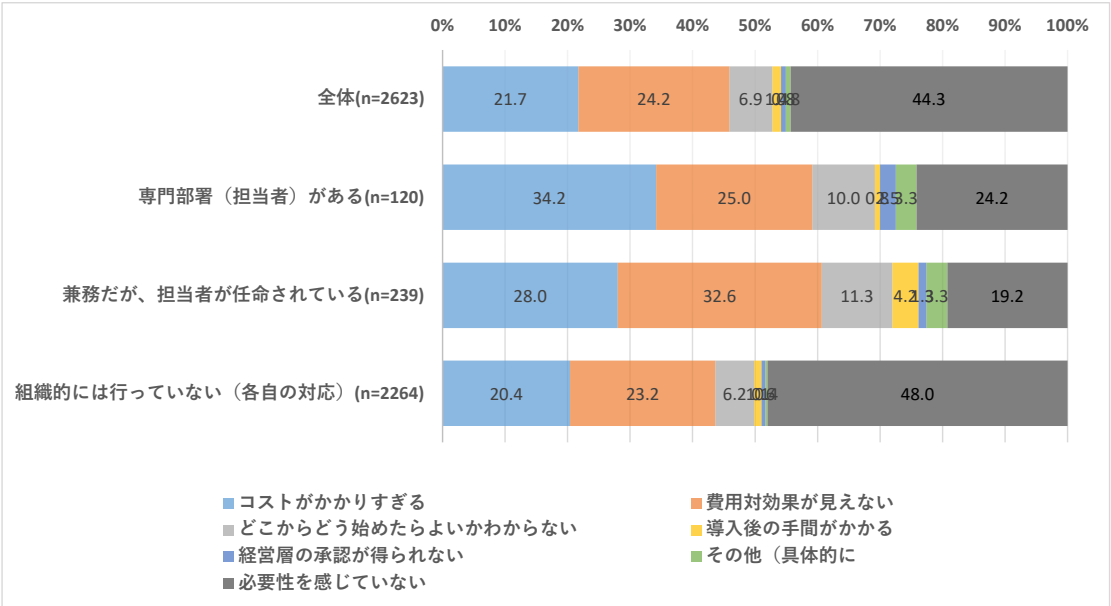

図 3-152 情報セキュリティ対策投資額について「投資をしていない」と回答した一番の理由(セキュリティ体制の整備状況別)（n=2623）

Q8.（Q7.で「必要性を感じていない」と回答された方について）前問で情報セキュリティ対策投資について「必要性を感じていない」とお答えになった理由について教えてください。 あてはまるものを下記よりすべてお選びください。（MA）

体制が整備されていない企業では、「重要除法を保有していないため」との回答が最も多く 4 割弱である。一方で、体制が整備されている企業では「既に十分な対策がとられているから」との回答が多く、4

割強である。

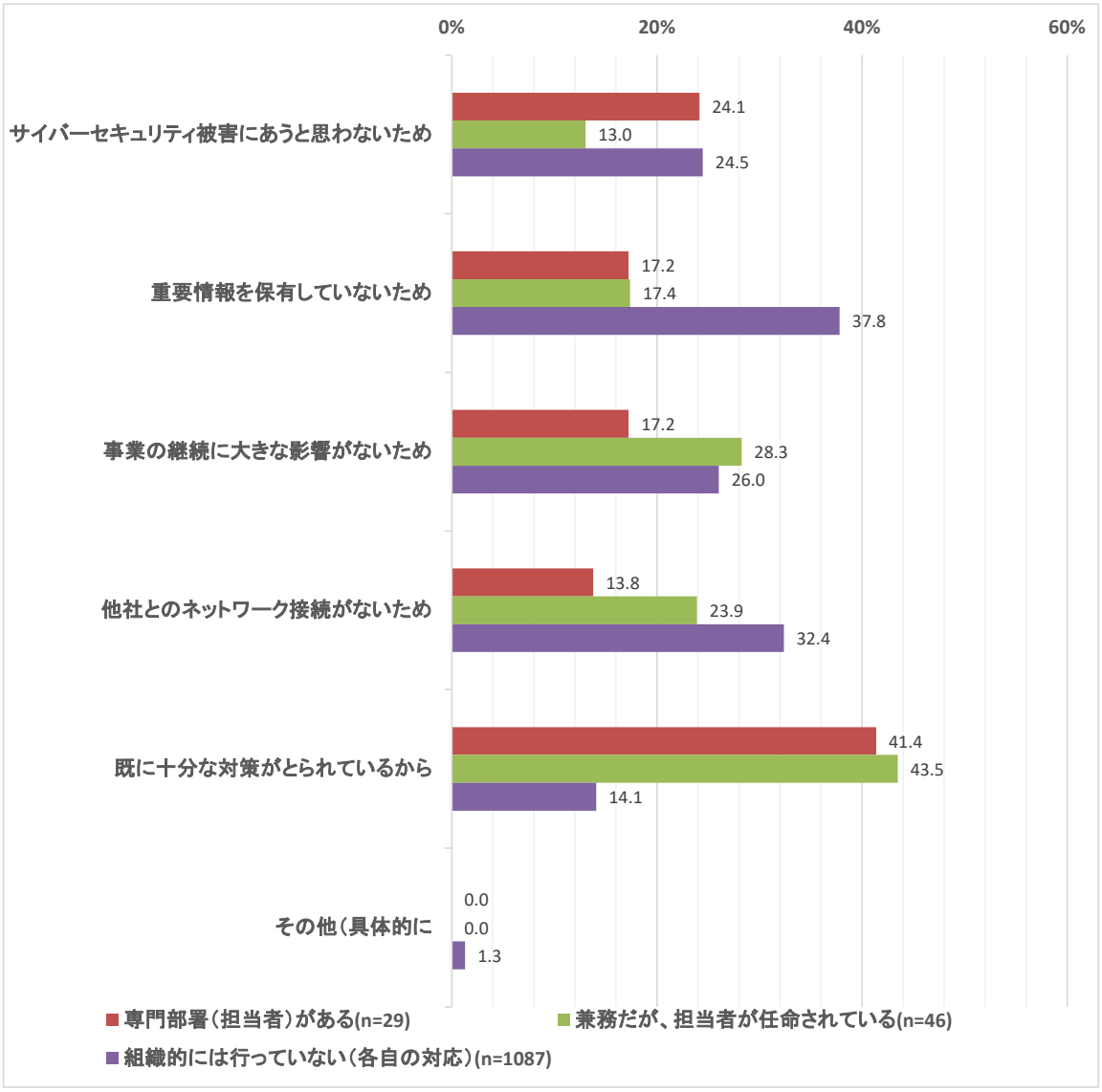

図 3-153 情報セキュリティ対策投資について「必要性を感じていない」と回答した理由（セキュリティ体制の整備状況別）（n=1162）

d. セキュリティパッチの適用状況

Q14.（Q9 で「対策の必要性を感じたことがない」以外の回答をされた方について）貴社ではサーバ等にセキュリティパッチを適用していますか。パッチを適用していない場合は理由について教えてください。 あてはまるものを下記よりすべてお選びください。（MA）

体制の整備がされるとともに、パッチを適用している割合が上がる傾向が読み取れる。

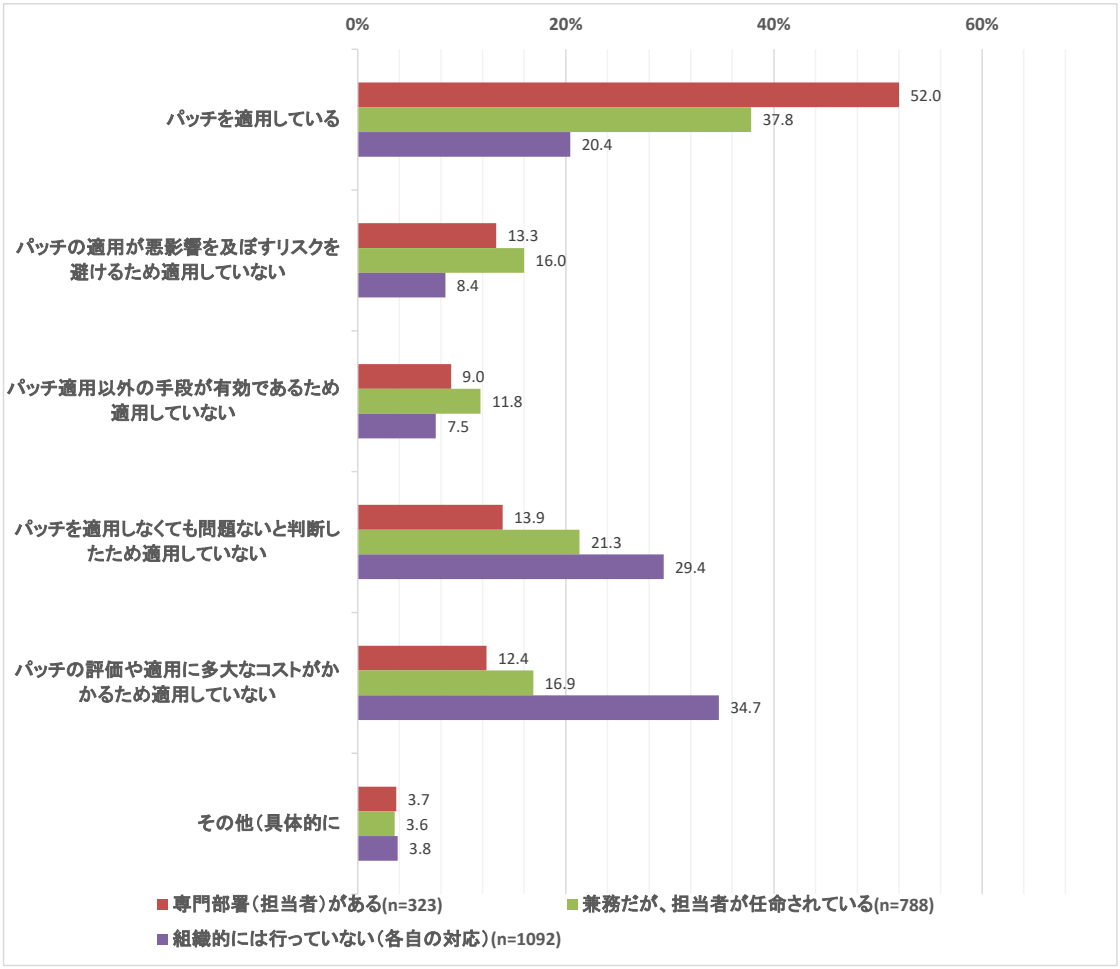

図 3-154 セキュリティパッチの適用状況（セキュリティ体制の整備状況別）(n=2203)

e. 困ったことがあった際の相談先

Q23. 貴社の情報セキュリティ対策に関して困ったことがあった際の相談先を教えてください。あてはまるものを下記よりすべてお選びください。(MA)

体制が整備されてない企業においては、「特にない」が 7 割近く、困ったことがあった際の相談先が極端に少ない実態が読み取れる。

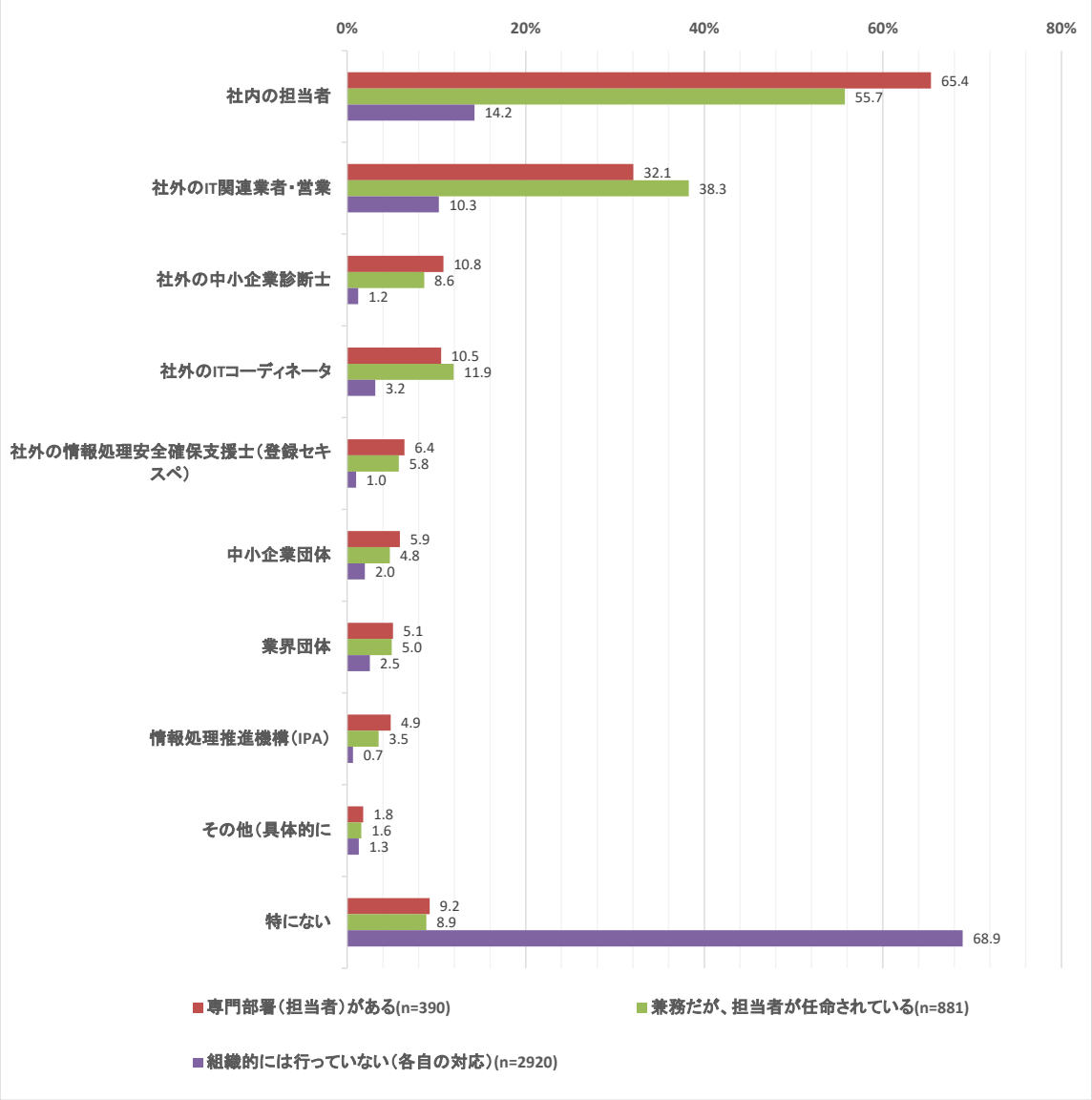

図 3-155 情報セキュリティ対策に関して困ったことがあった際の相談先（セキュリティ体制の整備状況別）（n=4191）

f. 活用したい情報セキュリティ対策に関するサービス

Q21. どのような情報セキュリティ対策に関するサービスがあれば活用したいと思いますか。あてはまるものを下記よりすべてお選びください。（MA）

体制が整っていない企業ほど、中小企業のセキュリティ対策の可視化サービスと回答する割合が増えており、担当者不在のため自社の対策状況を把握できていない実態が読み取れる。

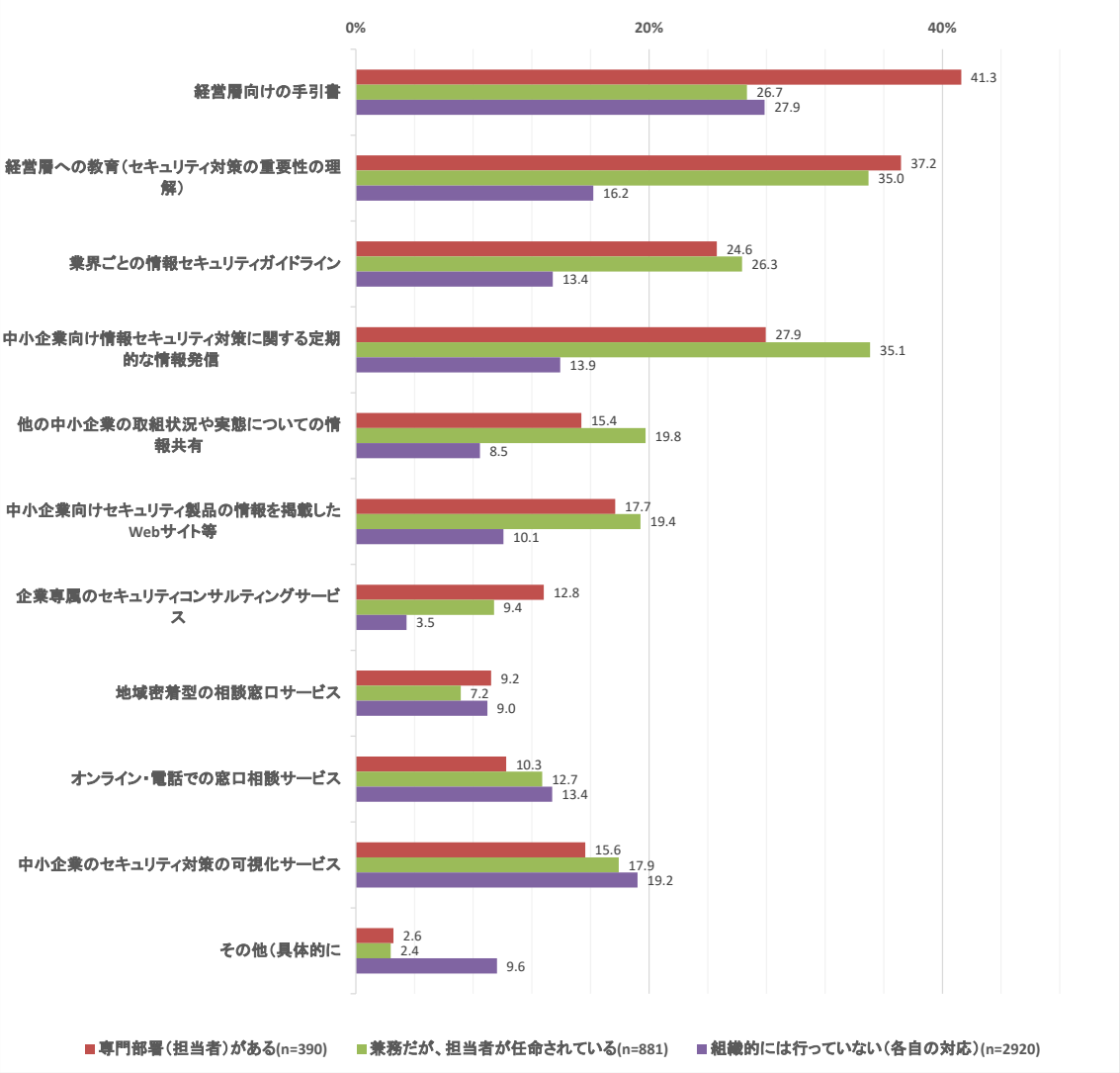

図 3-156 活用したい情報セキュリティ対策に関するサービス（セキュリティ体制の整備状況別）（n=4191）

g. 情報セキュリティに関する情報収集先

Q24. 貴社の情報セキュリティ対策に関する情報収集先を教えてください。 あてはまるものを下記よりすべてお選びください。（MA）

体制が整備されていない企業では「特にない」との回答が最も多く、5 割強であり、次いで「インターネット」が 2 割となっており、これらの企業についてはインターネット上での情報が重要な情報源となっていることが読み取れる。

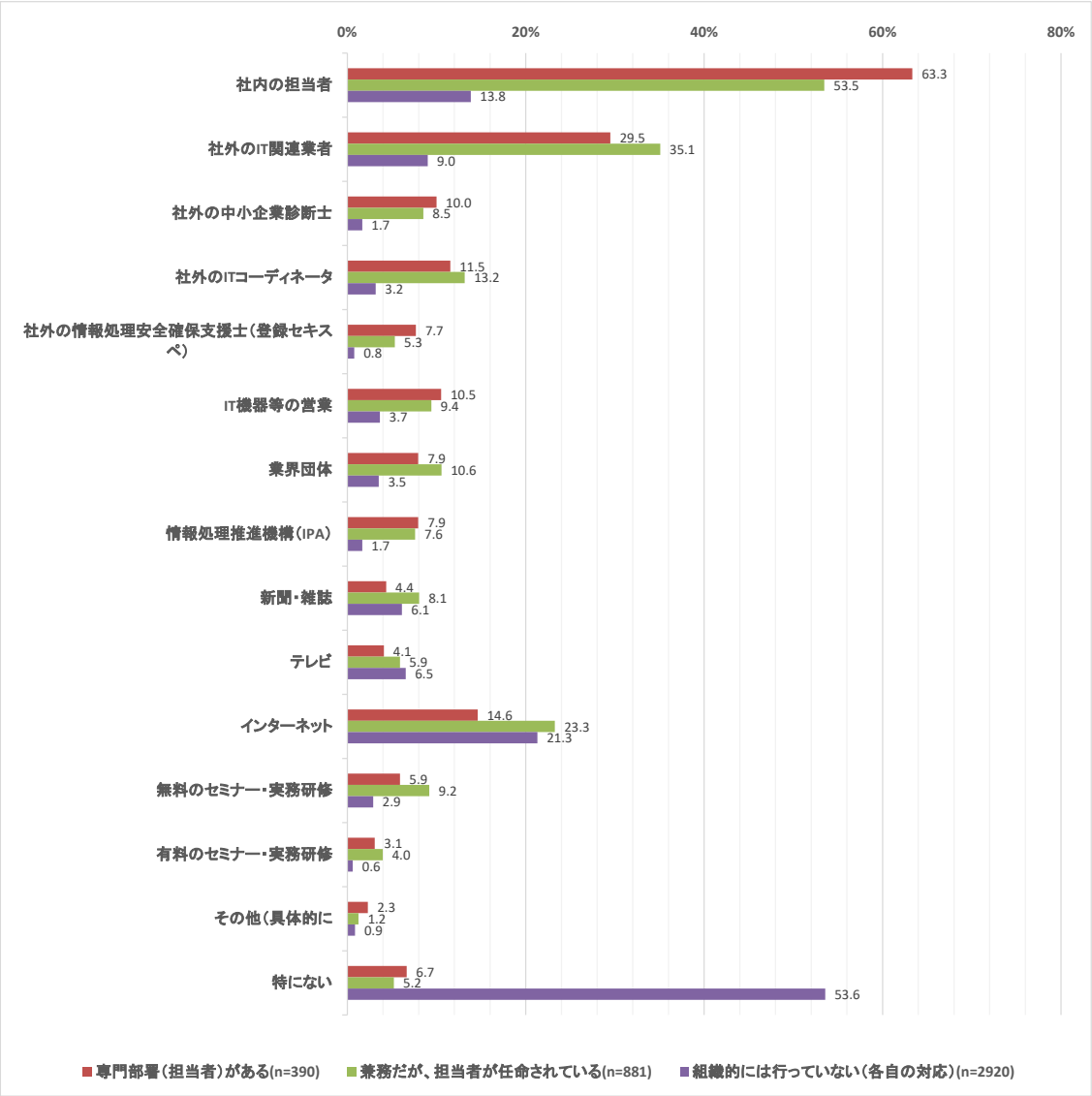

図 3-157 情報セキュリティ対策に関する情報収集先（セキュリティ体制の整備状況別）（n=4191）

h. 従業員に対する情報セキュリティ教育の実施状況

Q25. 貴社では従業員に対する情報セキュリティ教育をどのように実施していますか。（MA）

セキュリティ体制が整備されてない企業では、「特にない」が 8 割と、情報セキュリティ教育がほとんど行われていないことが読み取れる。体制が整備されている企業は「関連情報の通知（社内メール・回覧・掲示板など）」の割合が高い。

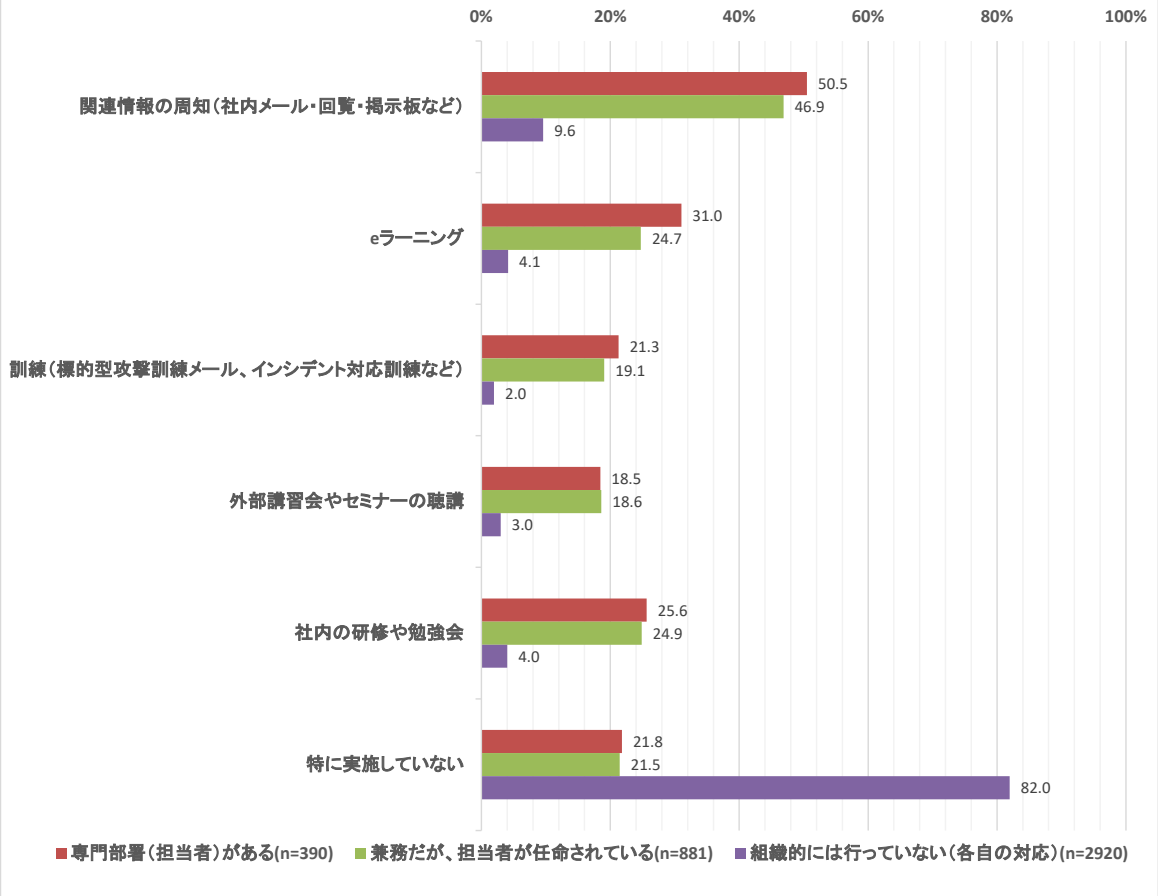

図 3-158 従業員に対する情報セキュリティ教育の実施状況（セキュリティ体制の整備状況別）
（n=4191）

i. 情報漏えい等のインシデント又はその兆候を発見した場合の報告先

Q15. 貴社で情報漏洩等のインシデント又はその兆候を発見した場合に、規定されている報告先は何ですか。 あてはまるものを下記よりすべてお選びください。（MA）

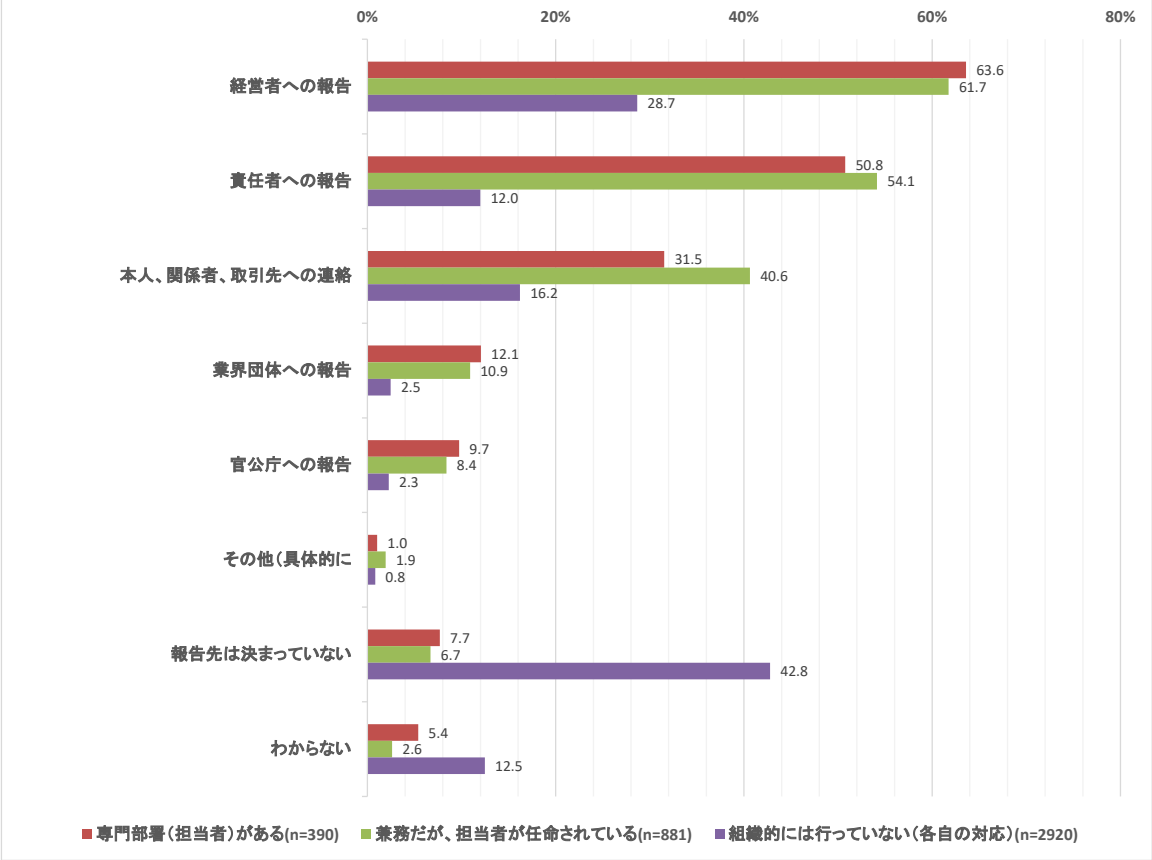

図 3-159 情報漏えい等のインシデント又はその兆候を発見した場合の報告先（セキュリティ体制の整備状況別）（n=4191）

j. 情報漏えい等のインシデント又はその兆候を発見した場合の対応方法

Q16. 貴社で情報漏洩等のサイバーインシデント又はその兆候を発見した場合の対応方法として規定されているものは何ですか。 あてはまるものを下記よりすべてお選びください。（MA）

体制が整理されている企業では、情報の隔離が最も多く、次いでネットワーク診断である。体制が整備されてない企業では「対応方法が決まっていない」が最も多く 5 割弱となっている。

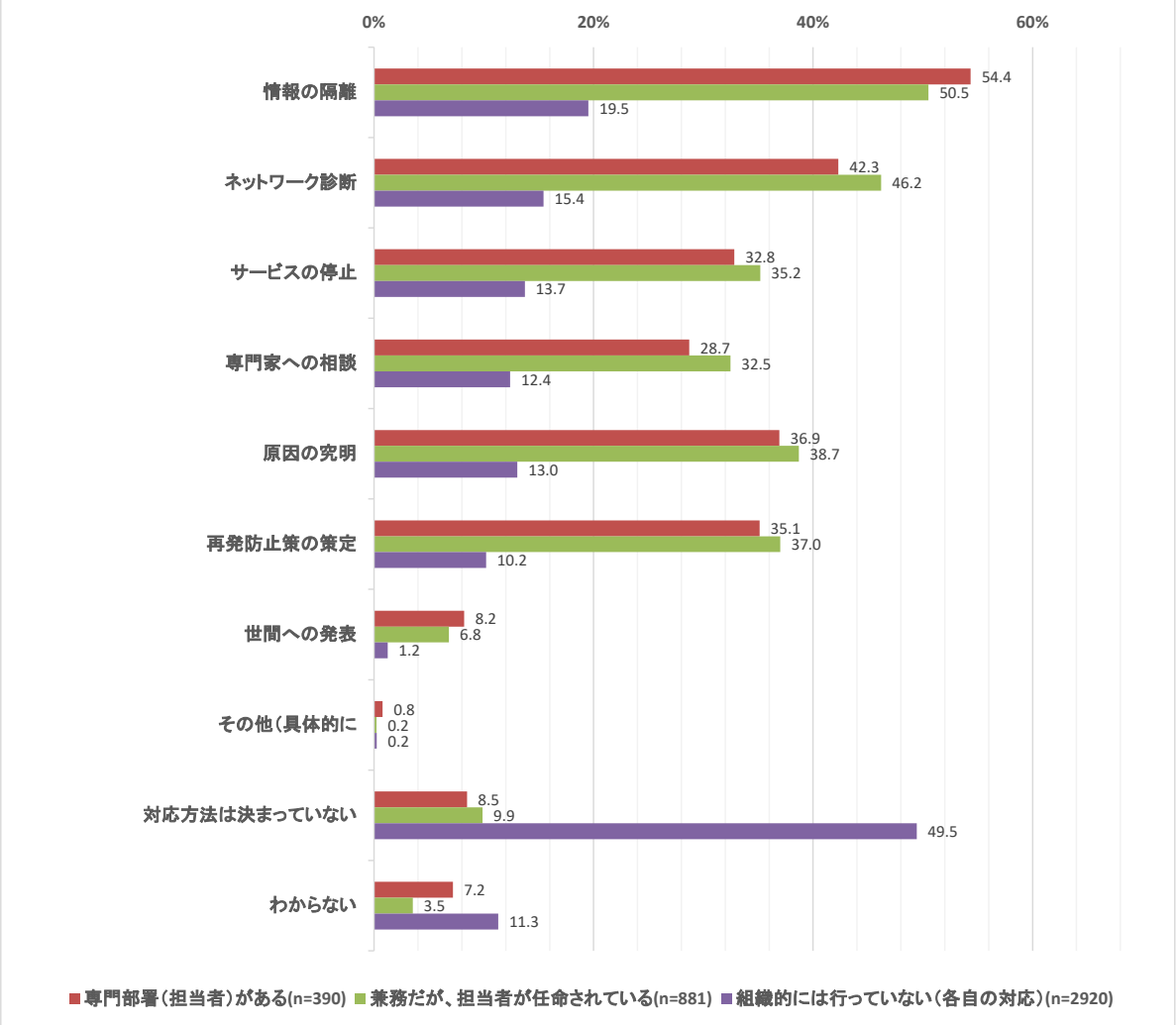

図 3-160 サイバーインシデント又はその兆候を発見した場合の対応方法（セキュリティ体制の整備状況別）（n=4191）

k. 情報セキュリティ関連製品やサービスの導入状況

Q12.（Q9 で「対策の必要性を感じたことがない」以外の回答をされた方について）貴社では情報セキュリティ関連製品やソフトウェアを導入していますか。 導入している情報セキュリティ関連製品やソフトウェアを教えてください。 あてはまるものを下記よりすべてお選びください。（MA）

ウイルス対策ソフト・サービスの導入は、情報セキュリティ体制の整備状況に関わらず、7 割を超えて高く、ほとんどの企業で浸透していることが分かる。一方、その他のサービスやソフトウェアは体制が整備されてない企業と整備されている企業での導入割合に大きな違いが出ており、また、体制が整備されてない企業では「特に導入しているものはない」が 1 割程度あるなど、体制の整備がセキュリティ対策の充実度に強く影響していることが読み取れる。

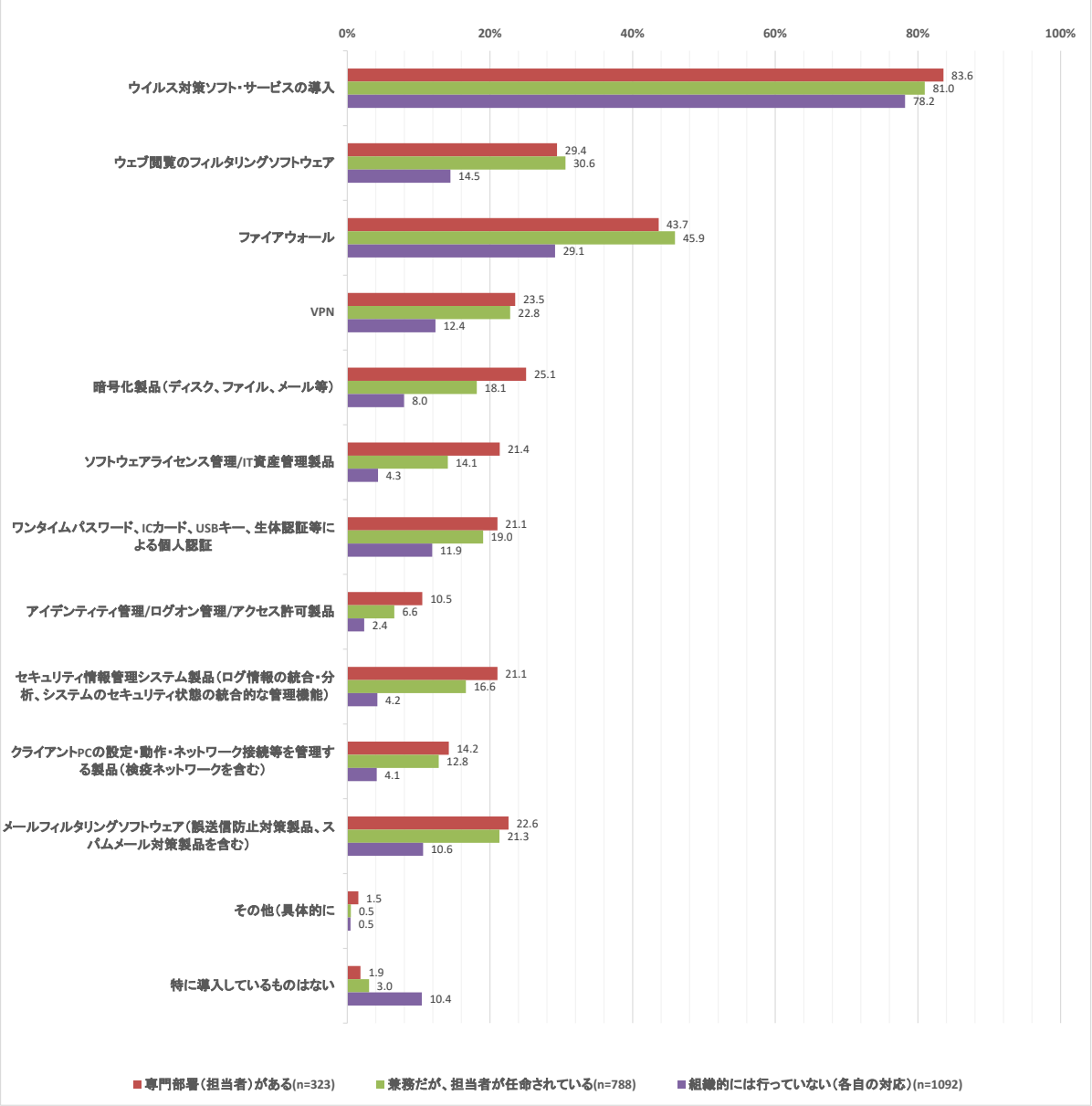

図 3-161 情報セキュリティ関連製品やソフトウェアの導入状況（セキュリティ体制の整備状況別）（n=2203）

l. 情報セキュリティ対策に期待する効果

Q19. 貴社で現状以上の情報セキュリティ対策を実施するためには、どのような効果が期待できれば対策を行うと思いますか。あてはまるものを下記よりすべてお選びください。（MA）

体制が整備されている企業ほど「従業員の情報セキュリティへの意識向上」との回答が高い傾向にある。対処すべきリスクの特定は、兼務だが、担当者が任命されている企業で最も多く、専門部署がない兼務担当者にとってリスクの特定ができていない実態が明らかになった。

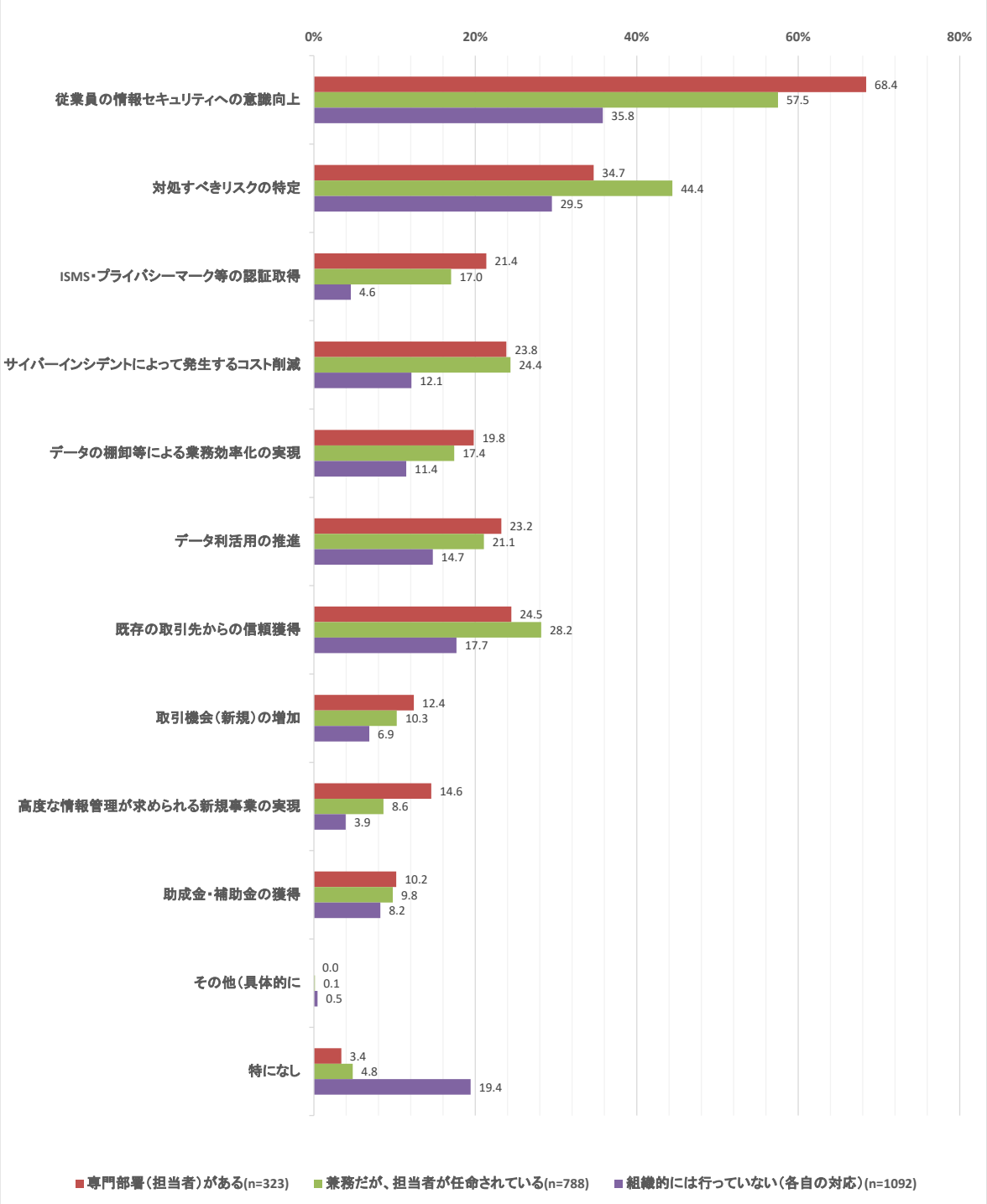

図 3-162 情報セキュリティ対策に期待する効果（セキュリティ体制の整備状況別）（n=2203）

m. 情報セキュリティ対策をさらに向上させるために必要と思われること

Q20. 貴社の情報セキュリティ対策を、さらに向上させるために必要と思うことは何ですか。（MA）

経営者のサイバーセキュリティリスク意識向上が、特にないを除き、情報セキュリティ体制の整備状況によらず回答割合が高い傾向にある。

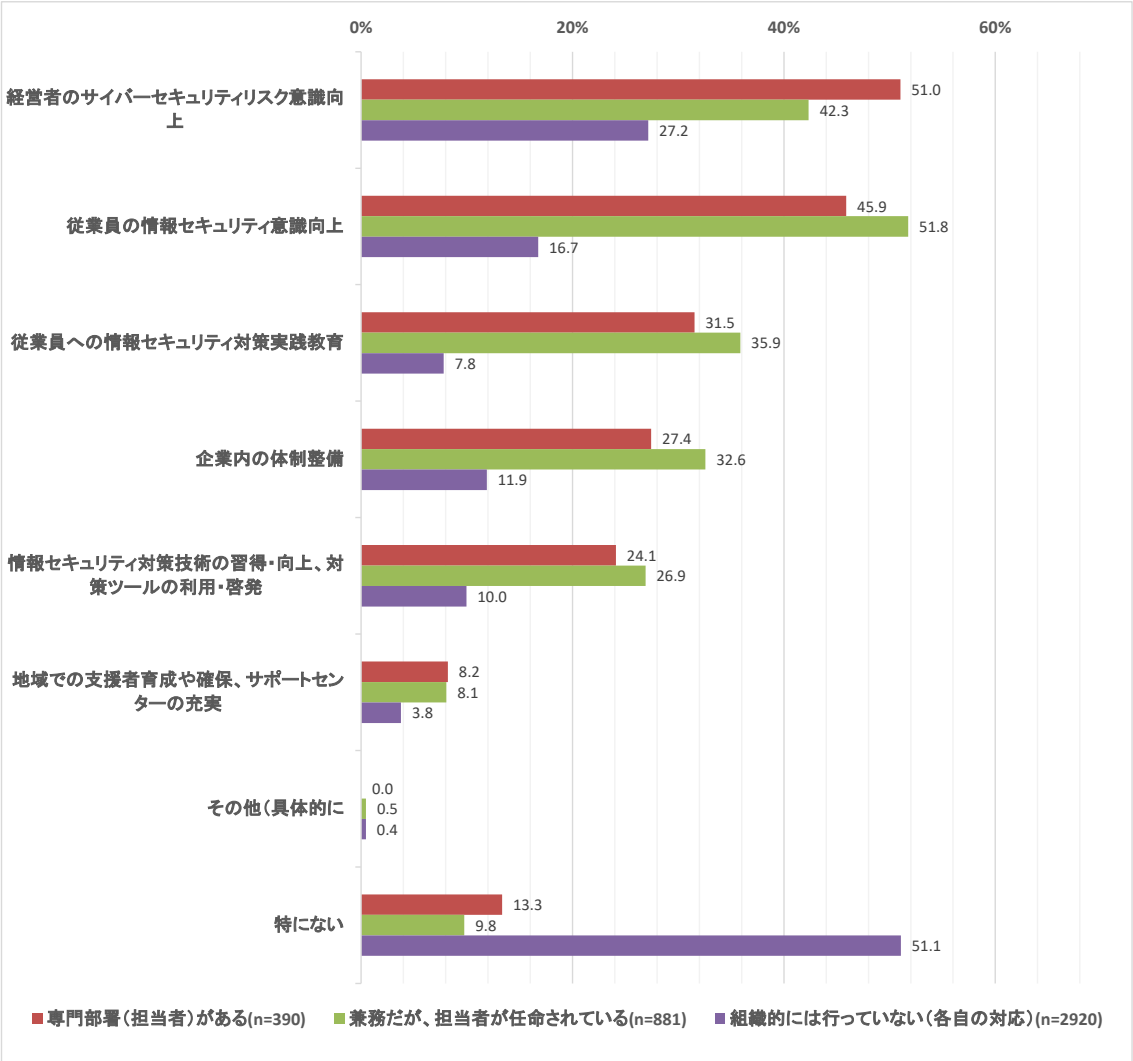

図 3-163 情報セキュリティ対策をさらに向上させるために必要と思うこと（セキュリティ体制の整備状況別）（n=4191）

3.3.5 所在地によるクロス集計

設問 Q1.所在地（本社所在地）の回答結果を軸としてクロス集計を行った。なお、地方分類は以下とした。

地方分類	回答数	都道府県名
北海道	194	北海道
東北	225	青森県・岩手県・秋田県・宮城県・山形県・福島県
北関東	258	茨城県・栃木県・群馬県・山梨県・長野県
南関東	1367	埼玉県・千葉県・東京都・神奈川県
東海	531	静岡県・岐阜県・愛知県・三重県
北陸	147	新潟県・富山県・石川県・福井県
近畿	804	滋賀県・京都府・奈良県・和歌山県・大阪府・兵庫県
中国	193	鳥取県・島根県・岡山県・広島県・山口県
四国	149	徳島県・香川県・愛媛県・高知県
九州・沖縄	323	福岡県・佐賀県・長崎県・大分県・熊本県・宮崎県・鹿児島県・沖縄県

a. 利用・導入しているサービスやシステム

Q5. 貴社では経営資源の確保や業務の効率化に IT を活用されていますか。情報セキュリティ対策サービス以外で利用・導入されているサービスやシステムについて教えてください。 あてはまるものを下記よりすべてお選びください。（MA）

サービスやシステムの利用状況を地方別に整理した。サービスやシステムごとの利用割合は、地方分類に関わらずほぼ同様の傾向が見られた。具体的には、最も多くの企業が利用しているのは電子メール（フリーメール・汎用ドメイン等）であり、次いで電子メール（貴社独自ドメイン）、Web サイト・ホームページの開設、会計システム・アプリケーションと続く。

個々のサービスやシステムで見た場合、電子メール（貴社独自ドメイン）、Web サイト・ホームページの開設、オンライン会議システム、コミュニケーションツール、クラウドストレージ有料、VPN では南関東が最も利用している割合が高く、このことから、南関東ではインターネットを活用したサービス利用が特に進んでいることが読み取れる。

四国はサービスやシステムの利用割合が低く、特に活用していないと回答している割合が最も高くなっている。

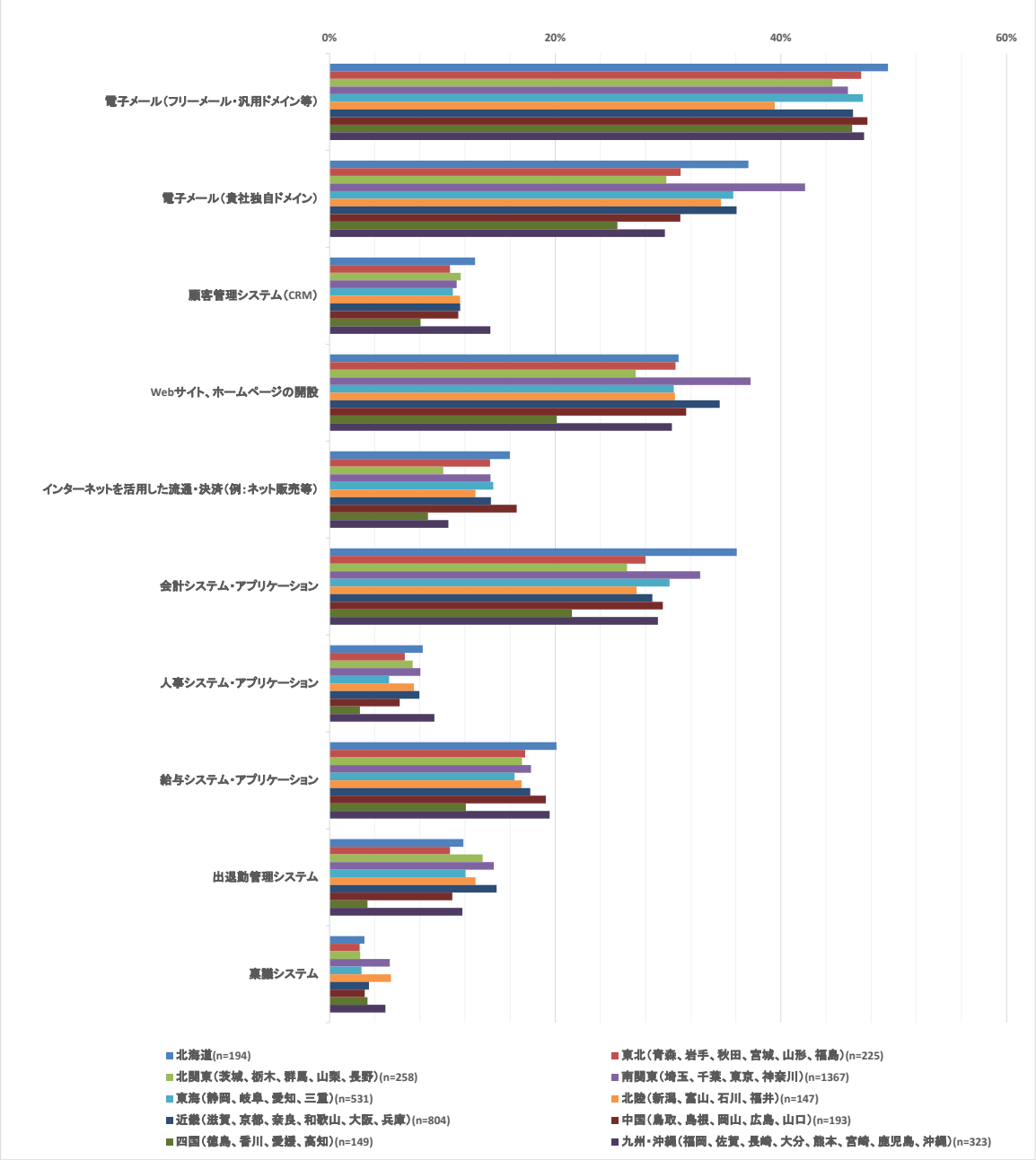

図 3-164 所在地別のサービスやシステムの利用状況①（n=4191）

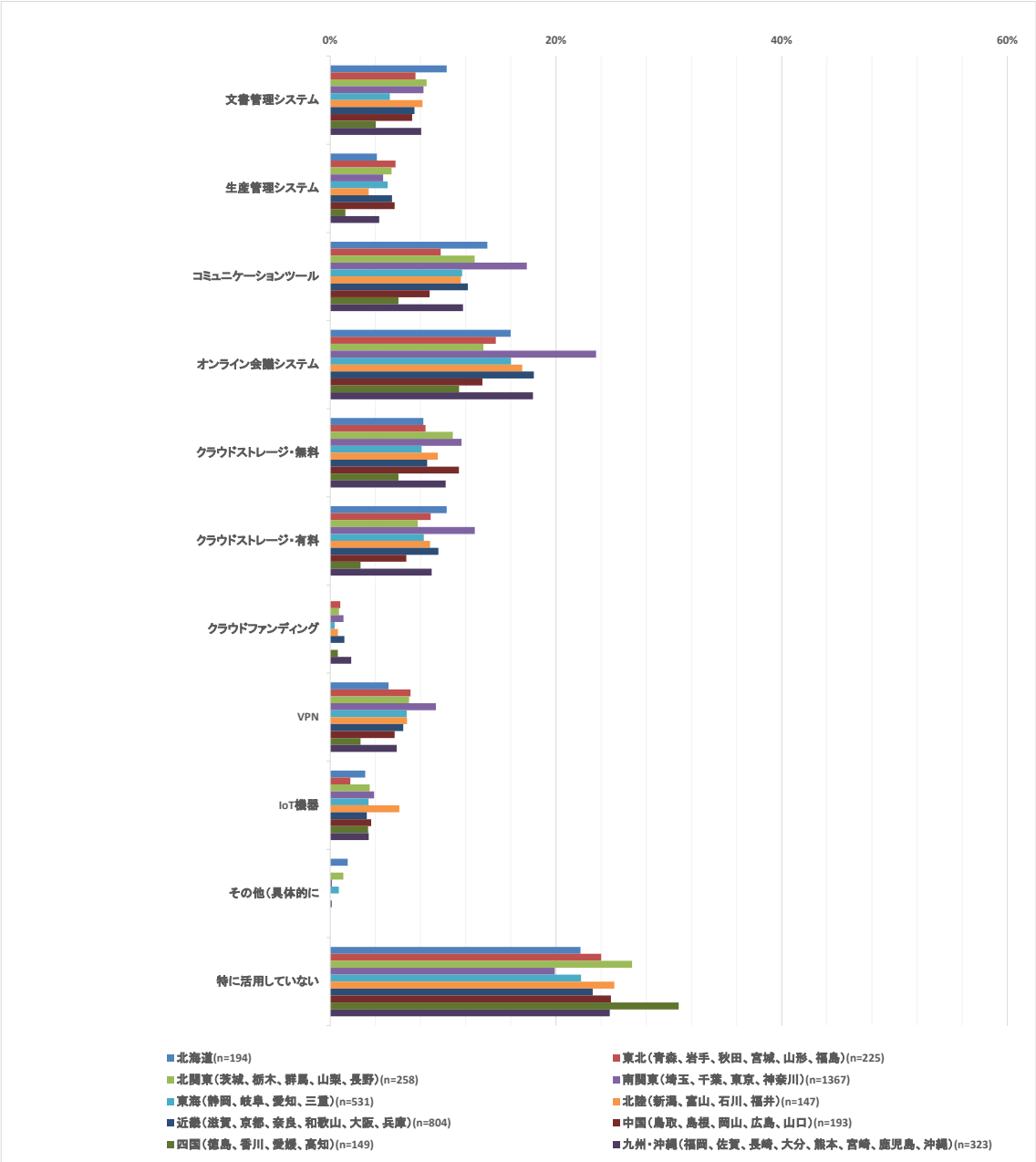

図 3-165 所在地別のサービスやシステムの利用状況②（n=4191）

b. 直近過去3期の情報セキュリティ対策投資額

Q6 項目 2. 貴社における、直近過去 3 期の IT 投資額（情報セキュリティ投資額を含む）と、情報セキュリティ対策投資額（IT 機器や社員への教育等も含む）の概算について教えてください。
-情報セキュリティ対策投資額（IT 機器や社員への教育等も含む）（SA）

直近過去 3 期の情報セキュリティ対策投資額について、地方分類による大きな差はない。投資していないの回答割合は南関東で最も低く、四国が最も高い。

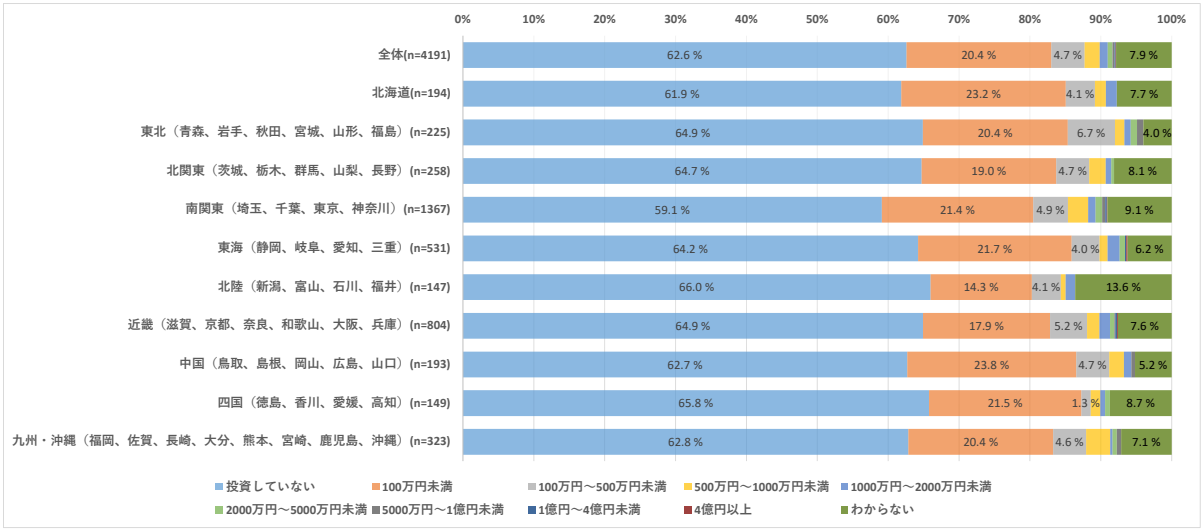

図 3-166 所在地別の情報セキュリティ対策投資状況(n=4191)

c. 情報セキュリティ対策投資を行わなかった理由

Q7.（Q6-2.で「投資していない」と回答された方について）前問で情報セキュリティ対策投資額について「投資をしていない」とお答えになった一番の理由について教えてください。（SA）

投資をしていない理由として、コストがかかりすぎる及び費用対効果が見えないなど費用に関する理由を挙げた割合は最も高いのは近畿であり、次いで東北、九州・沖縄である。四国では必要性を感じていないが最も多い。

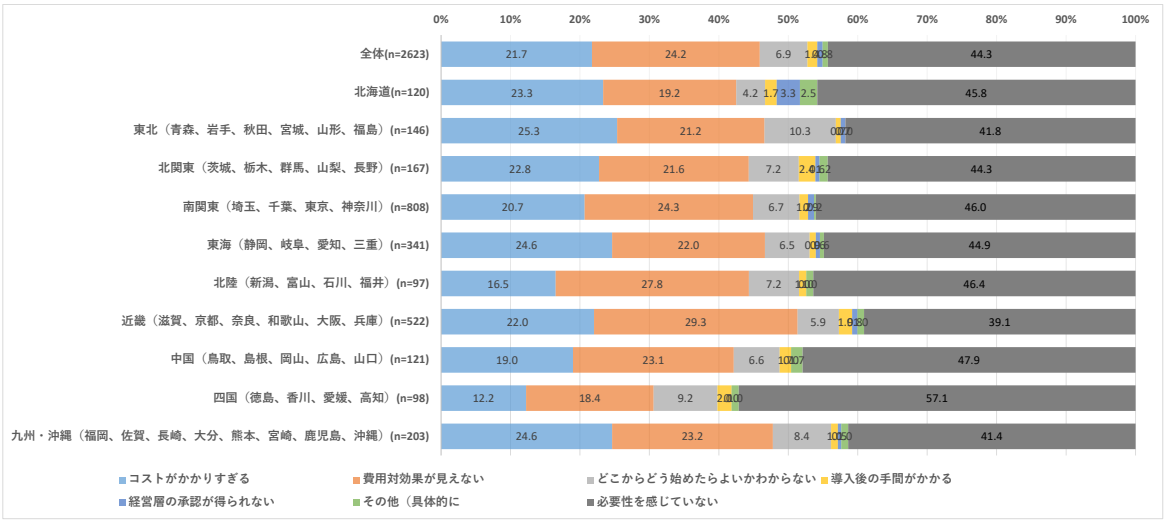

図 3-167 所在地別の情報セキュリティ対策投資を行わなかった理由(n=2623)

d. セキュリティパッチの適用状況

Q14.（Q9 で「対策の必要性を感じたことがない」以外の回答をされた方について）貴社ではサーバ等にセキュリティパッチを適用していますか。パッチを適用していない場合は理由について教えてください。 あてはまるものを下記よりすべてお選びください。(MA)

パッチを提供している割合が最も高いのは、南関東(36.7%)であり、次いで中国(35.0%)であるなど、パッチ適用を行っている企業が少ない実態が明らかになった。

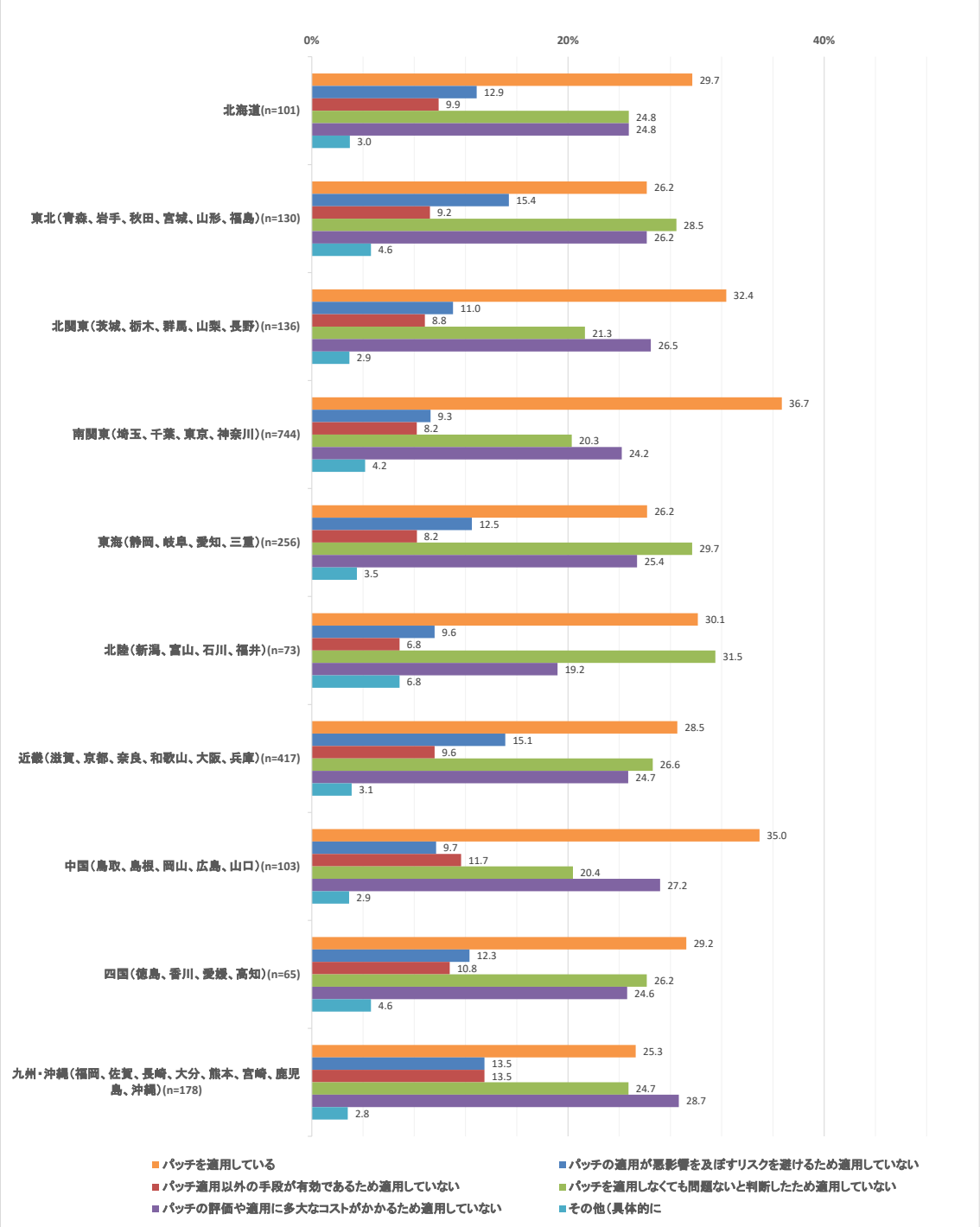

図 3-168 所在地別のセキュリティパッチの適用状況(n=2203)

e. 組織体制

Q22. 貴社の情報セキュリティ対策はどのような体制で行われていますか。(SA)

専門部署(担当者)がある及び兼務だが担当者が任命されていると回答した、なんらか情報セキュリティ対策の体制がとられている企業の割合が高い傾向にあるのは南関東、中国であり、逆に低い傾向にあるのは東海、四国であるなど、地方分類による差が読み取れる。

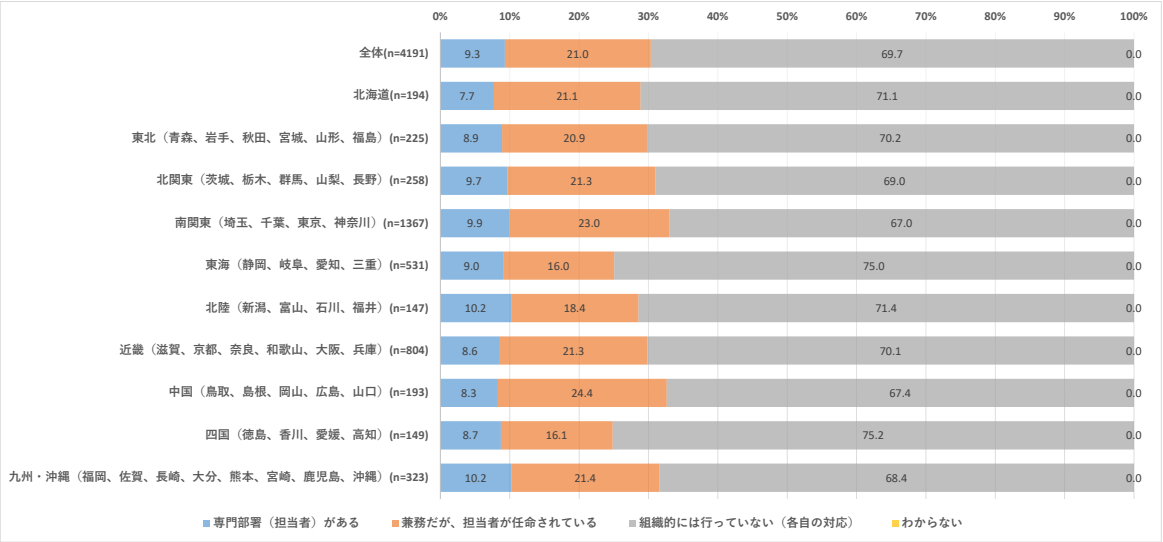

図 3-169 所在地別の組織体制(n=4191)

f. 困ったことがあった際の相談先

Q23. 貴社の情報セキュリティ対策に関して困ったことがあった際の相談先を教えてください。あてはまるものを下記よりすべてお選びください。(MA)

地方分類に関わらず、特に無いが最も多く、次いで社内の担当者となっている。特にないとの回答割合が多いのは東海、北陸、四国であり、これらの地方では社内の担当者の割合も低いことから情報セキュリティ対策の知識を持った人材が不足していることが推察される。

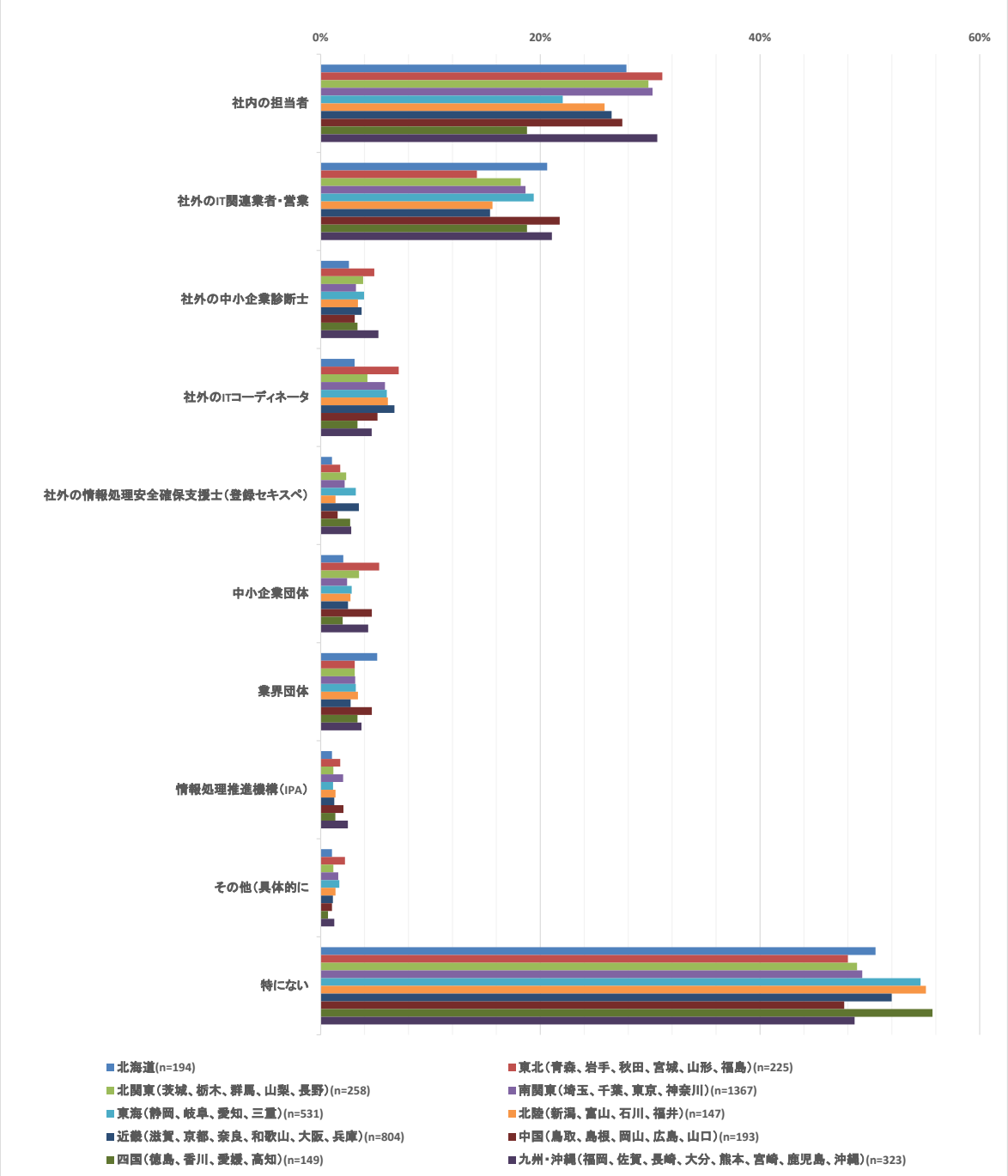

図 3-170 所在地別の困ったことがあった際の相談先（n=4191）

g. 活用したい情報セキュリティ対策に関するサービス

Q21. どのような情報セキュリティ対策に関するサービスがあれば活用したいと思いますか。 あてはまるものを下記よりすべてお選びください。（MA）

地方分類に関わらず、経営層向けの手引書が最も多い。中小企業のセキュリティ対策の可視化サービスの回答割合が高いのは四国、東北、北陸であり、四国、北陸では前項目の結果を踏まえると情報セキュリティ対策の問合せ先が少ない地方で要望が高いことが考えられる。

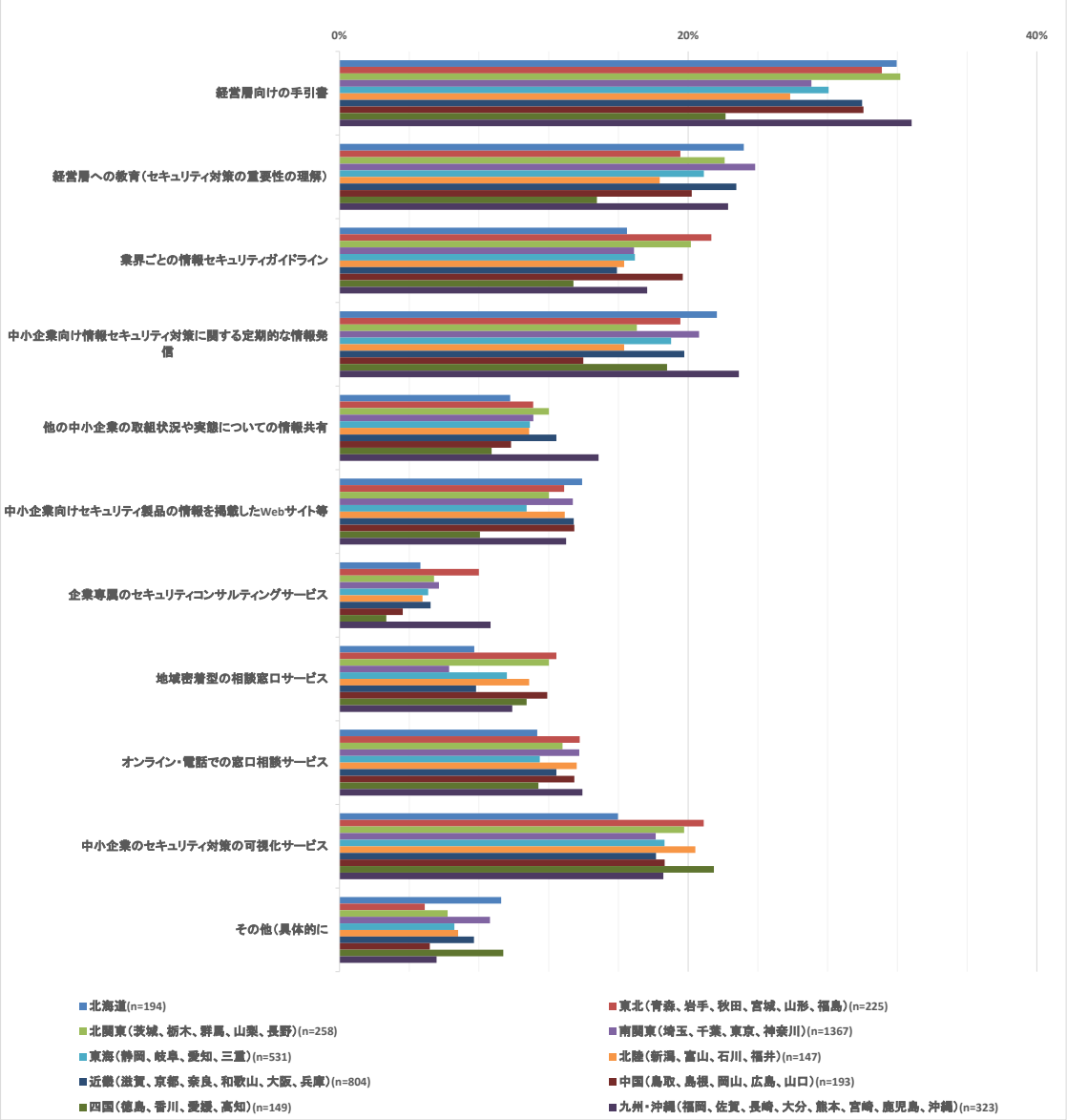

図 3-171 所在地別の活用したい情報セキュリティ対策に関するサービス（n=4191）

h. 情報セキュリティに関する情報収集先

Q24. 貴社の情報セキュリティ対策に関する情報収集先を教えてください。 あてはまるものを下記よりすべてお選びください。（MA）

地方分類に寄らず、特にないとの回答が最も多く、次いで社内の担当者となる。どの地方でもインターネットによる情報収集は行われており、社外の IT 関連業者よりも割合が高く、中小企業向けの情報セキュリティに関する情報提供手段としてインターネットの重要性が読み取れる。社外の IT 担当者の割合が低いのは東北、北陸、近畿、四国であり、情報セキュリティ対策に関して中小企業とつながりを持った IT 関連業者が少ないことが理由の一つとして考えられる。

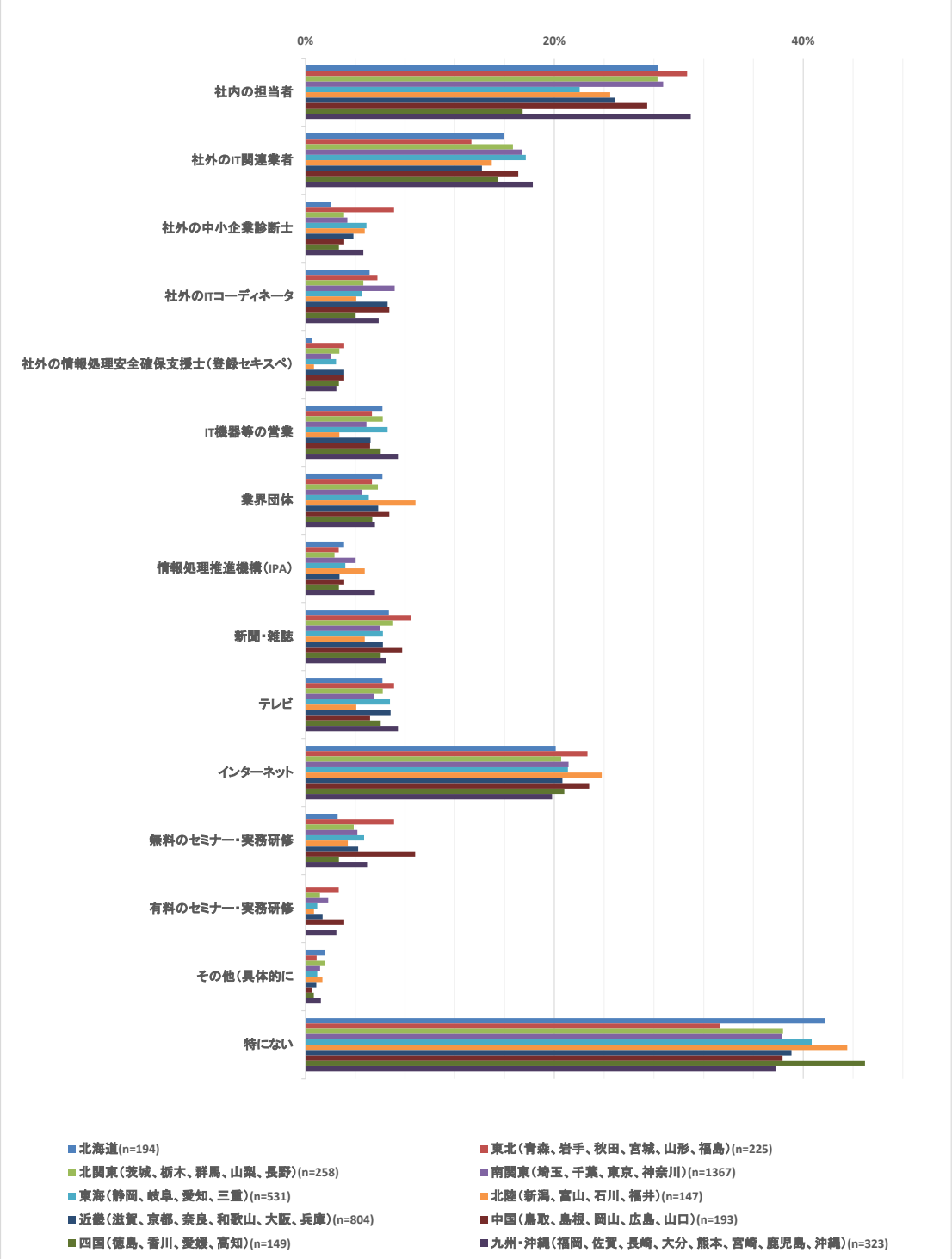

図 3-172 所在地別の情報セキュリティに関する情報収集先（n=4191）

i. 従業員に対する情報セキュリティ教育の実施状況

Q25. 貴社では従業員に対する情報セキュリティ教育をどのように実施していますか。（MA）

地方分類に関わらず、特に実施していないと回答した割合が最も高く、次いで関連情報の周知（社内メール・回覧・掲示板など）となる。特に実施していない割合が最も高いのは東海であり、次いで北陸、四国となる。

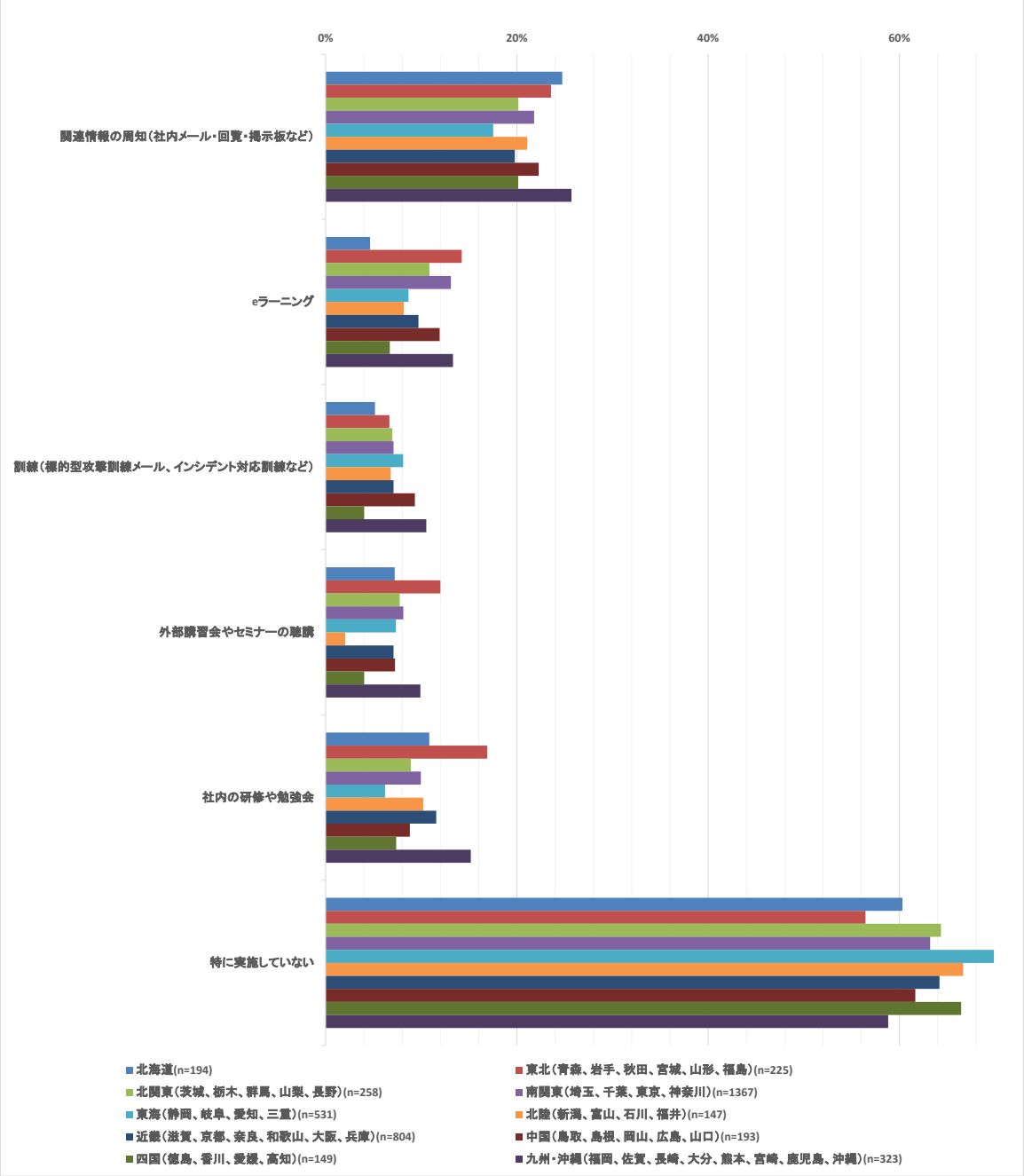

図 3-173 所在地別の従業員に対する情報セキュリティ教育の実施状況（n=4191）

j. 情報漏えい等のインシデント又はその兆候を発見した場合の報告先

Q15. 貴社で情報漏洩等のインシデント又はその兆候を発見した場合に、規定されている報告先は何ですか。 あてはまるものを下記よりすべてお選びください。（MA）

地方分類ごとに僅かであるが回答傾向に差がみられる。報告先が決まっていないと回答した割合は北海道が最も低く、北陸が最も高い。経営者への報告が最も高いのは東北、最も低いのは北陸となっている。

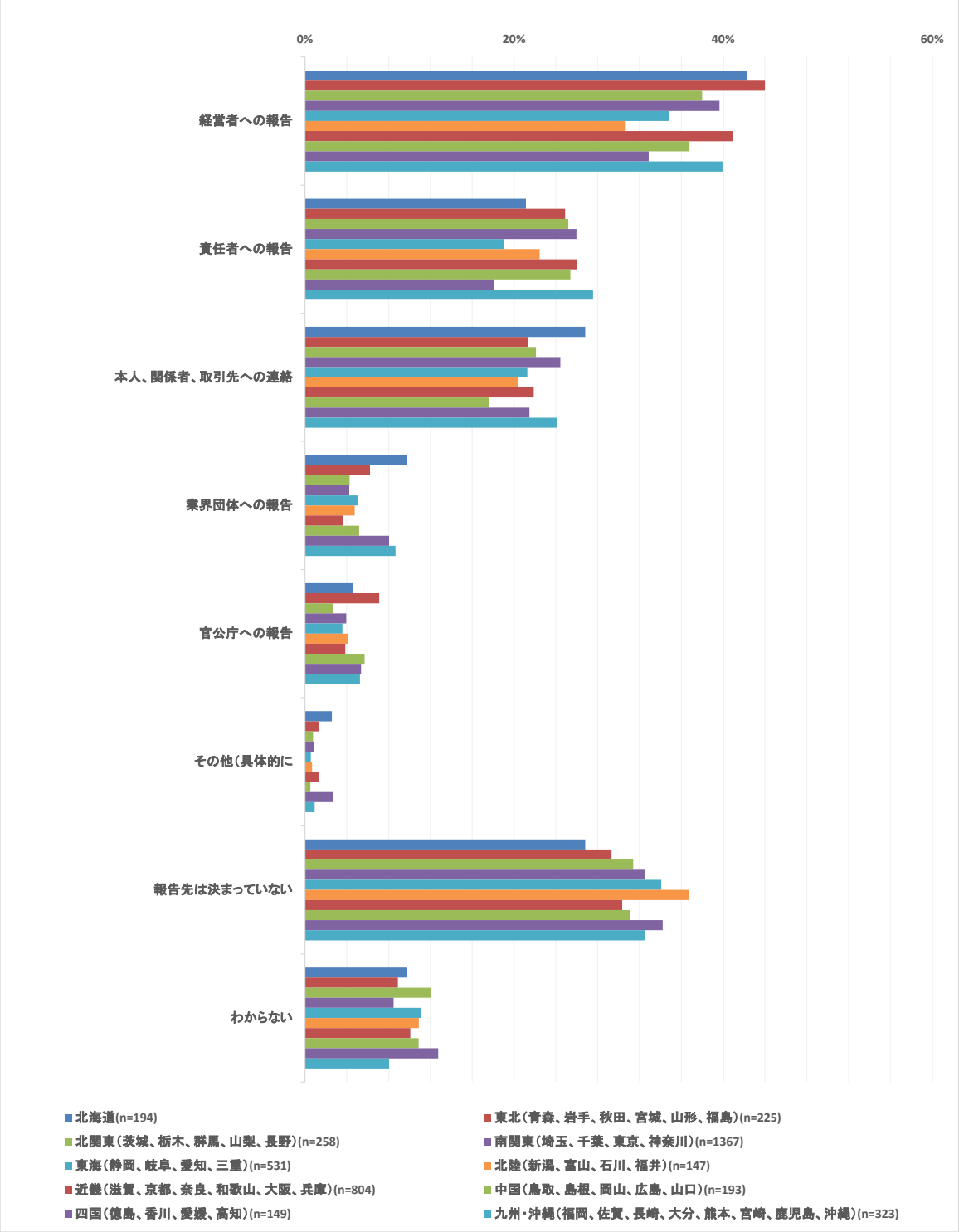

図 3-174 所在地別のインシデント又はその兆候を発見した場合の報告先（n=4191）

k. 情報漏えい等のインシデント又はその兆候を発見した場合の対応方法

Q16. 貴社で情報漏洩等のサイバーインシデント又はその兆候を発見した場合の対応方法として規定されているものは何ですか。 あてはまるものを下記よりすべてお選びください。(MA)

地方分類に関わらず、対応方法が決まっていないが最も高く、次いで情報の隔離となる。地方分類ごとに回答傾向に差が見られ、対応方法が決まっていないとの回答が最も高いのは四国である。また専門家への相談の割合が最も高いのは東北である。

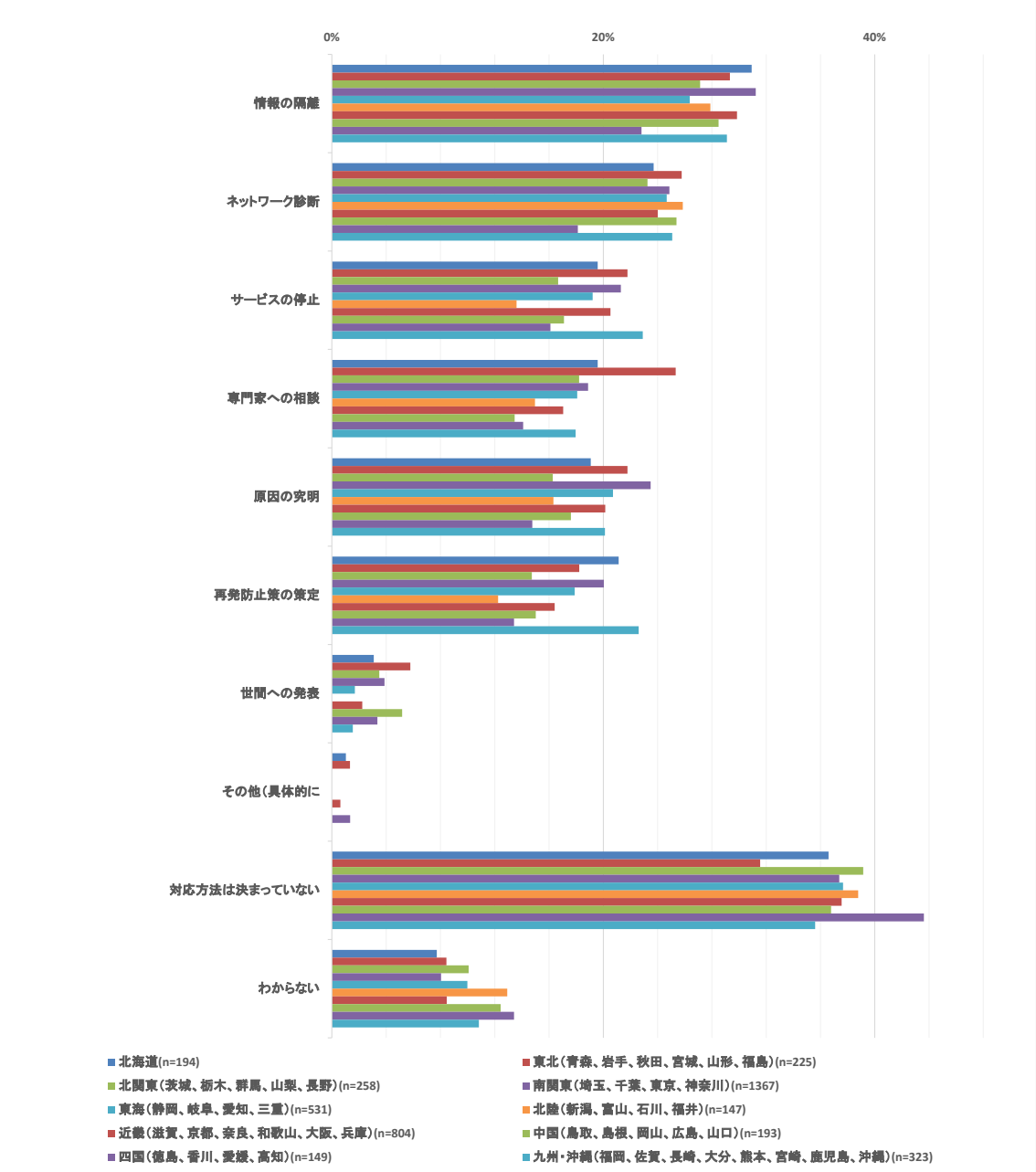

図 3-175 所在地別のインシデント又はその兆候を発見した場合の対応方法(n=4191)

l. 情報セキュリティ関連製品やサービスの導入状況

Q12.（Q9 で「対策の必要性を感じたことがない」以外の回答をされた方について）貴社では情報セキュリティ関連製品やソフトウェアを導入していますか。 導入している情報セキュリティ関連製品やソフトウェアを教えてください。 あてはまるものを下記よりすべてお選びください。（MA）

地方分類で傾向の差は無く、ウイルス対策ソフト・サービスの導入との回答の割合が最も高い。ファイアウォールの導入と回答した割合が最も高いのは、南関東である。

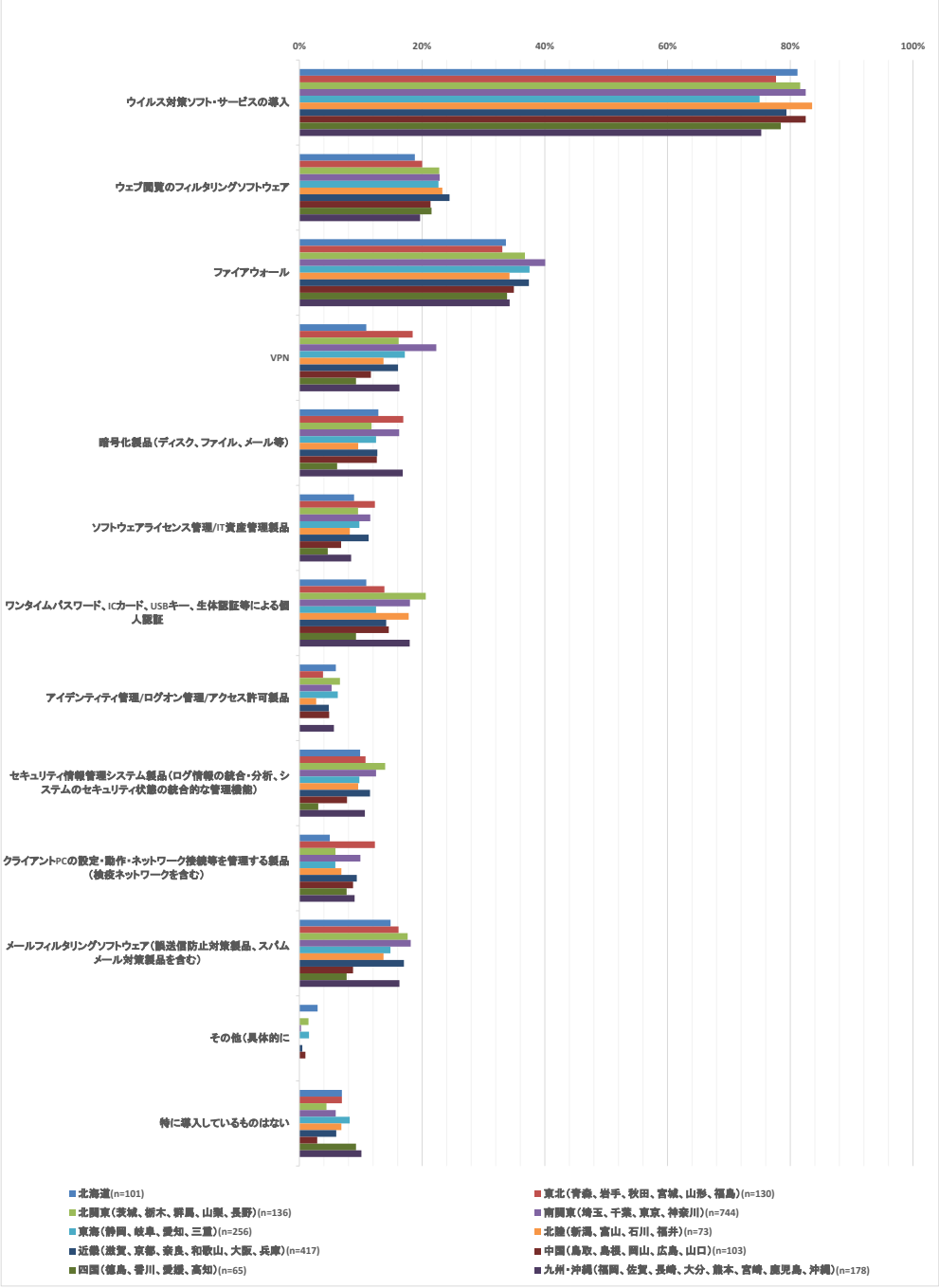

図 3-176 所在地別の情報セキュリティ関連製品やサービスの導入状況（n=2203）

m. 情報セキュリティ対策に期待する効果

Q19. 貴社で現状以上の情報セキュリティ対策を実施するためには、どのような効果が期待できれば対策を行うと思いますか。あてはまるものを下記よりすべてお選びください。
（MA）

従業員の情報セキュリティへの意識向上と回答した割合は九州・沖縄、中国、北海道の順で高く、四国が最も低い。

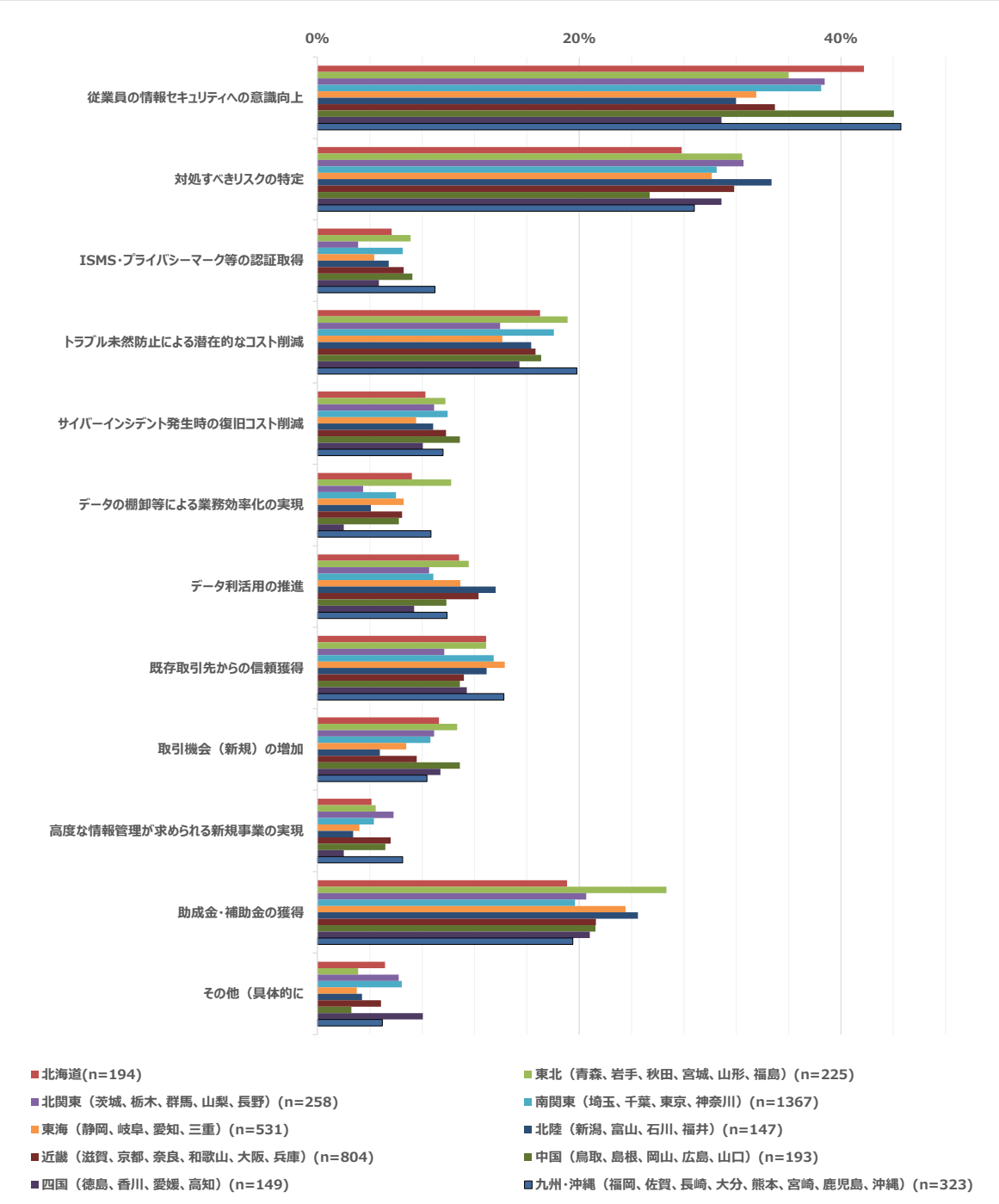

図 3-177 所在地別の情報セキュリティ対策に期待する効果(n=4191)

n. 情報セキュリティ対策をさらに向上させるために必要と思われること

Q20. 貴社の情報セキュリティ対策を、さらに向上させるために必要と思うことは何ですか。（MA）

地方分類ごとに若干傾向に差が見られる。従業員の情報セキュリティへの意識向上は北海道、九州・沖縄、南関東の順で高く、四国、東海、北陸で低い。対処すべきリスクの特定と回答した割合は北海道で最も高く、四国が最も低い。ISMS・プライバシーマーク等の認証取得は東北で最も高く、次いで南関東である。

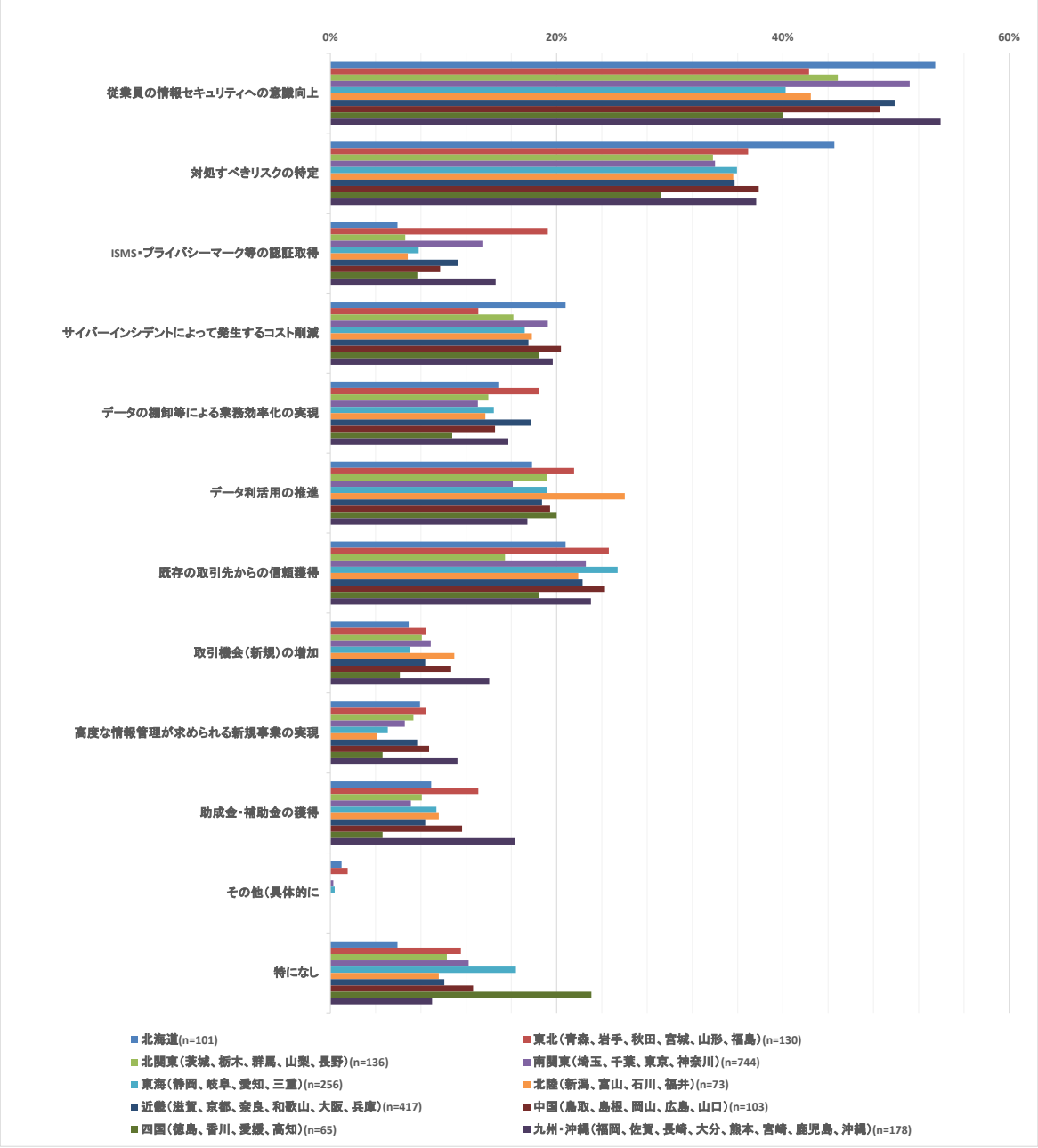

図 3-178 所在地別の情報セキュリティ対策をさらに向上させるために必要と思われること（n=4191）

3.4 調査結果(前回調査との比較)

3.4.1 前回調査結果との比較

a. IT 投資額

Q6 項目 1. 貴社における、直近過去 3 期の IT 投資額(情報セキュリティ投資額を含む) の概算について教えてください。(SA)

投資をしていない企業の割合は 59.7%であり、2021 年度の 30.0%から大幅に増加している。特に 100 万円未満の投資割合が減少していることが影響している。2016 年度の 47.3%から投資していない割合が増えている。中規模の投資も減少しており、資金不足がうかがえる。

中小企業の IT 投資は、2016 年から 2021 年にかけて一時増加したものの、今回の調査で大幅に減少している。

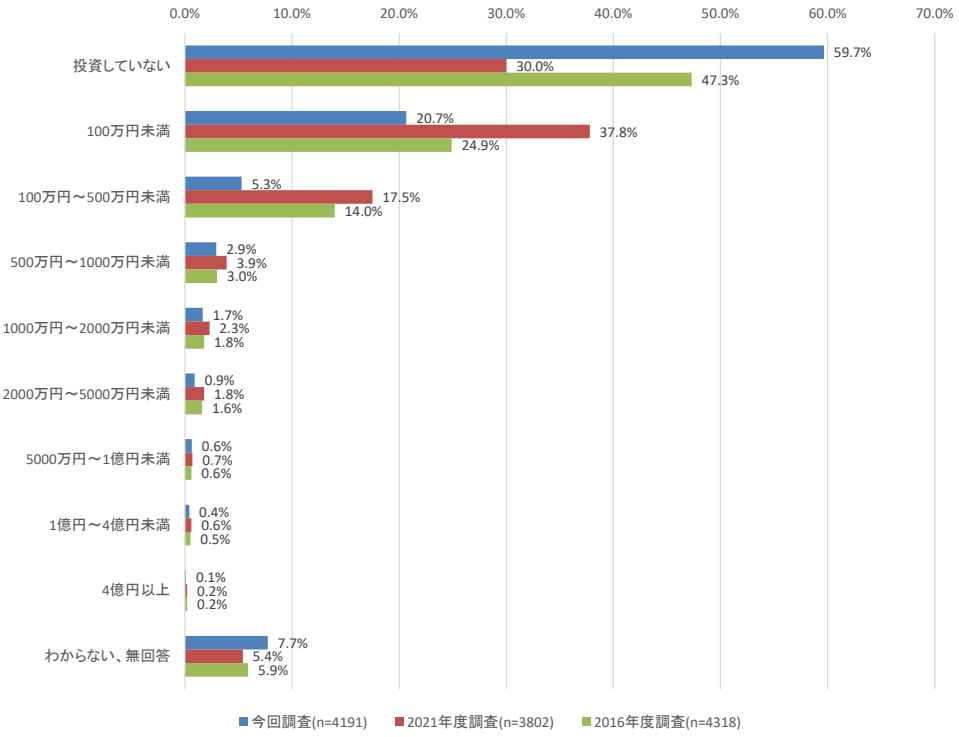

図 3-179　IT 投資額(前回調査との比較)(n=4191)

b. 情報セキュリティ投資額

Q6 項目 2. 貴社における、直近過去 3 期の情報セキュリティ対策投資額(IT 機器や社員への教育等も含む)の概算について教えてください。(SA)

情報セキュリティ投資をしていない企業の割合が 62.6%に増加している。2016 年度の 55.2%からさらに増加している。IT 投資と同様に、セキュリティ投資も控えられている企業が多く見受けられる。

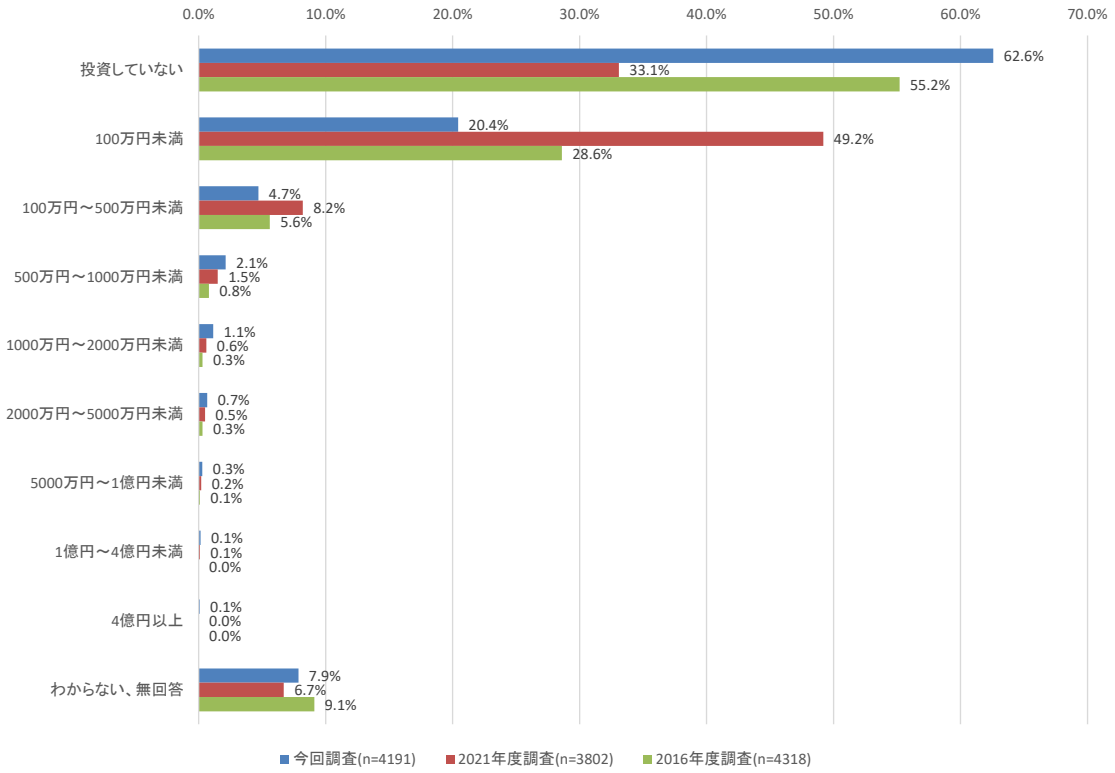

図 3-180 情報セキュリティ投資額(前回調査との比較)(n=4191)

c. 組織体制

Q22. 貴社の情報セキュリティ対策はどのような体制で行われていますか。(SA)

専門部署がある企業は 9.3%とわずかに増えている一方で、兼務で対応せざるを得ない企業は減少し、組織的対策を行っていない企業は増加している。兼務担当者が任命されている割合が減少し、各自が対応するケースが増えている。

専門部署の必要性は認識されつつあるが、組織としての対応は不十分である。各自の取り組みに頼っている企業が増えているのが懸念材料である。

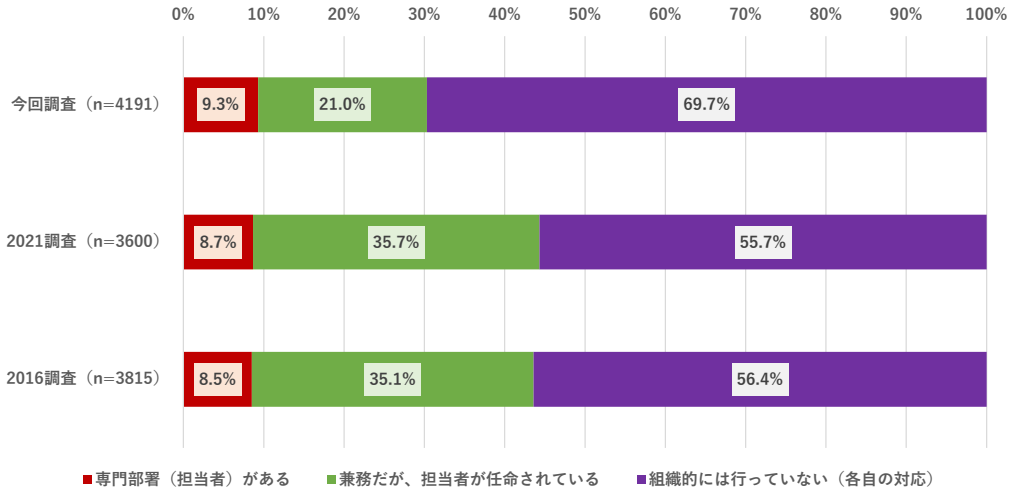

図 3-181 組織体制(前回調査との比較)

d. 従業員に対する情報セキュリティ教育の実施状況

Q25. 貴社では従業員に対する情報セキュリティ教育をどのように実施していますか。(MA)

e ラーニングを通じた情報セキュリティ教育の割合は 11.0%となり、2016 年度の 5.1%、2021 年度の 7.2%を上回っている。テクノロジーを活用したデジタル教育が進展していることが示されている。

社内の研修や勉強会を行っている割合は減少し、2016 年度の 17.9%から 10.4%に低下している。これは内部での教育活動が弱まっていることを示している。

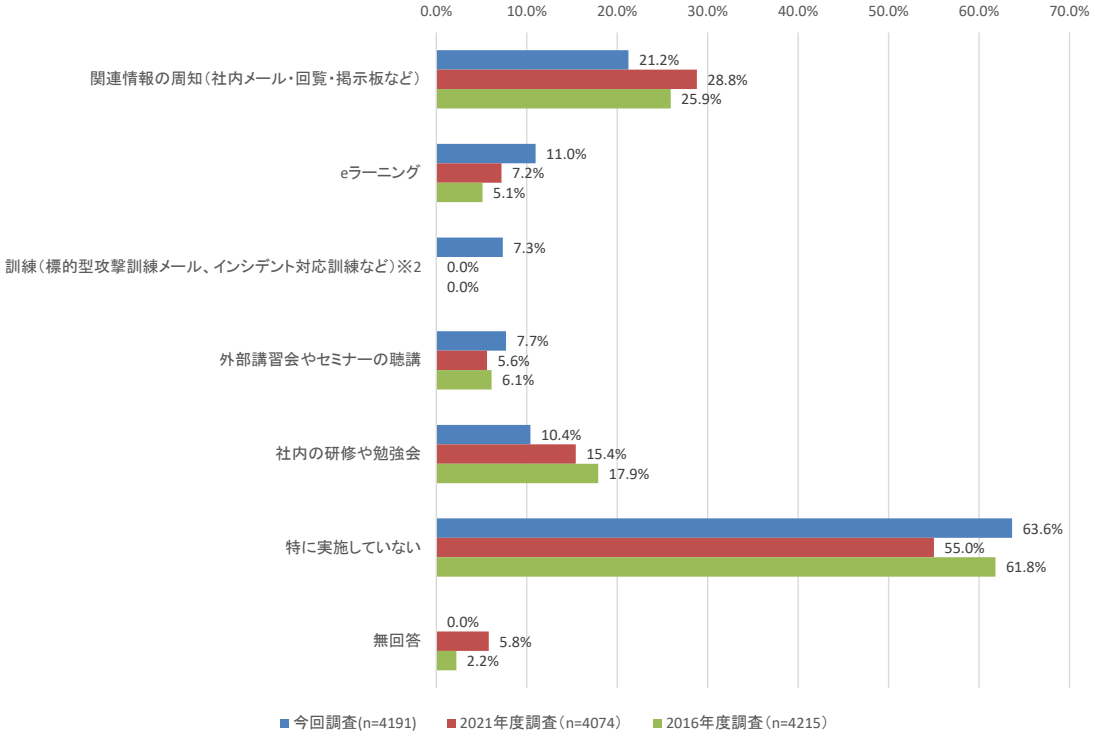

図 3-182 従業員に対する情報セキュリティ教育の実施状況(前回調査との比較)(n=4191)

e. 情報セキュリティ関連製品やサービスの導入状況

Q12. (Q9 で「対策の必要性を感じたことがない」以外の回答をされた方について)貴社では情報セキュリティ関連製品やソフトウェアを導入していますか。導入している情報セキュリティ関連製品やソフトウェアを教えてください。(MA)

ウイルス対策ソフトの導入率は 80.0%であり、2021 年度の 77.2%と比較して微増している。基本的なセキュリティ対策の導入は進んでいる。ウイルス対策ソフトの導入は一定の安定を見せる一方、フィルタリングや資産管理製品の導入拡大は新たなセキュリティニーズを反映したものである。

クライアント PC の設定管理製品の導入も増えており、2016 年度の 4.1%から 8.7%に増加している。ネットワーク管理の重要性が認識されてきている。

データ保護への関心と投資が顕著に高まっており、それに伴い様々なセキュリティ製品が導入されつつあることが伺える。

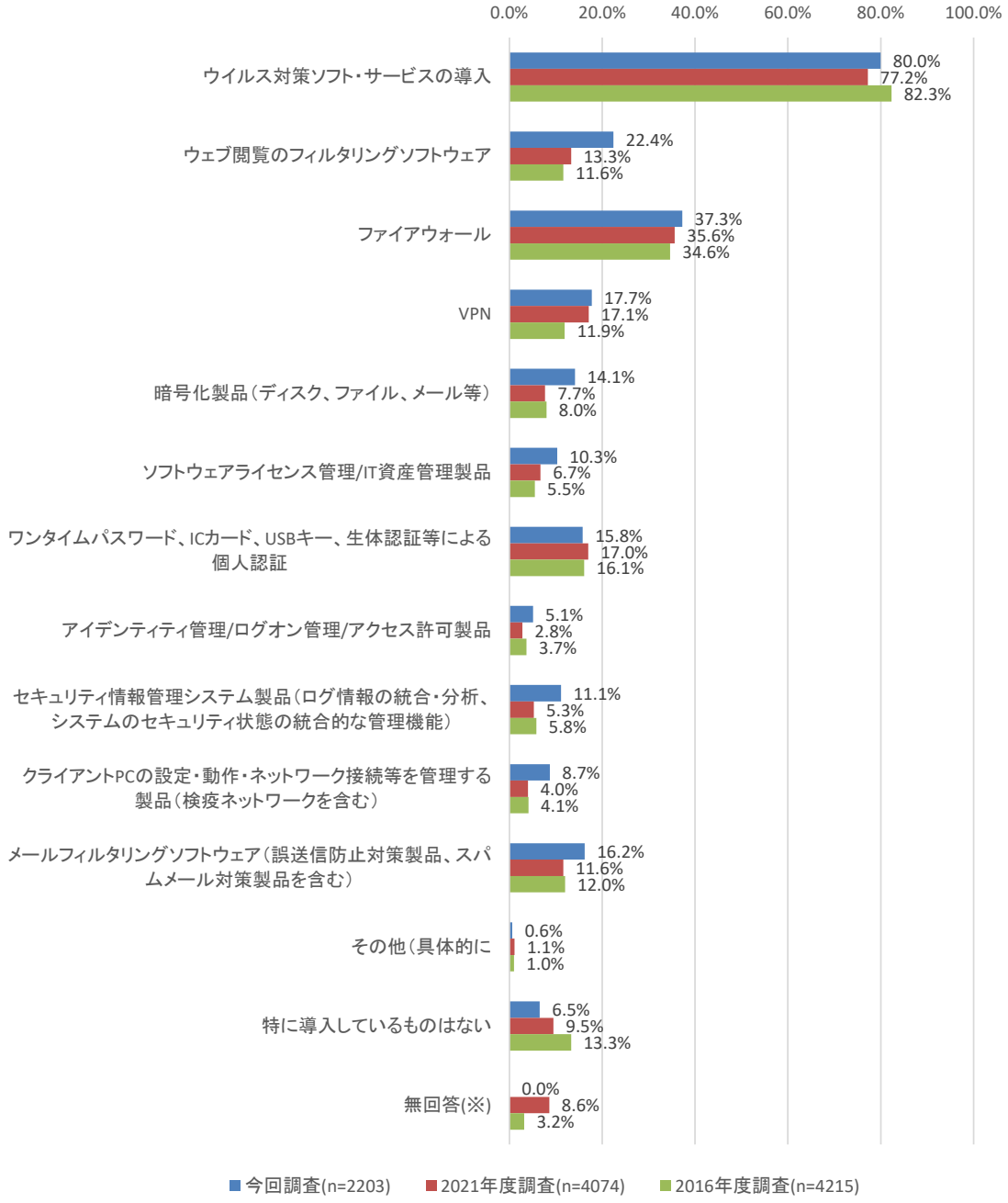

図 3-183 情報セキュリティ関連製品やサービスの導入状況（前回調査との比較）（n=2203）

f. 情報セキュリティ対策の必要性を感じたきっかけ

Q9. 貴社で情報セキュリティ対策を実施（強化）するきっかけとなった理由について教えてください。

法令の制定や改訂への対応として情報セキュリティ対策を実施する企業は 20.0%であり、2021 年度の 28.7%から減少している。法令遵守の動機が少し弱まっている傾向が見られる。2015 年のマイナンバー制度の開始をきっかけに対策を強化した企業の割合は 4.9%であり、2016 年度の 25.5%から著しく減少している。制度開始直後の影響が落ち着いている。

自社のサイバーインシデントをきっかけに対策を実施する企業が 7.1%となり、2021 年度の 3.7%か

ら増加している。具体的なリスク経験が対策強化の推進要因となっている。

対策の必要性を感じない企業の増加は、情報セキュリティの重要性が十分に浸透していないことを示しており、教育や意識改革の必要性が増している。

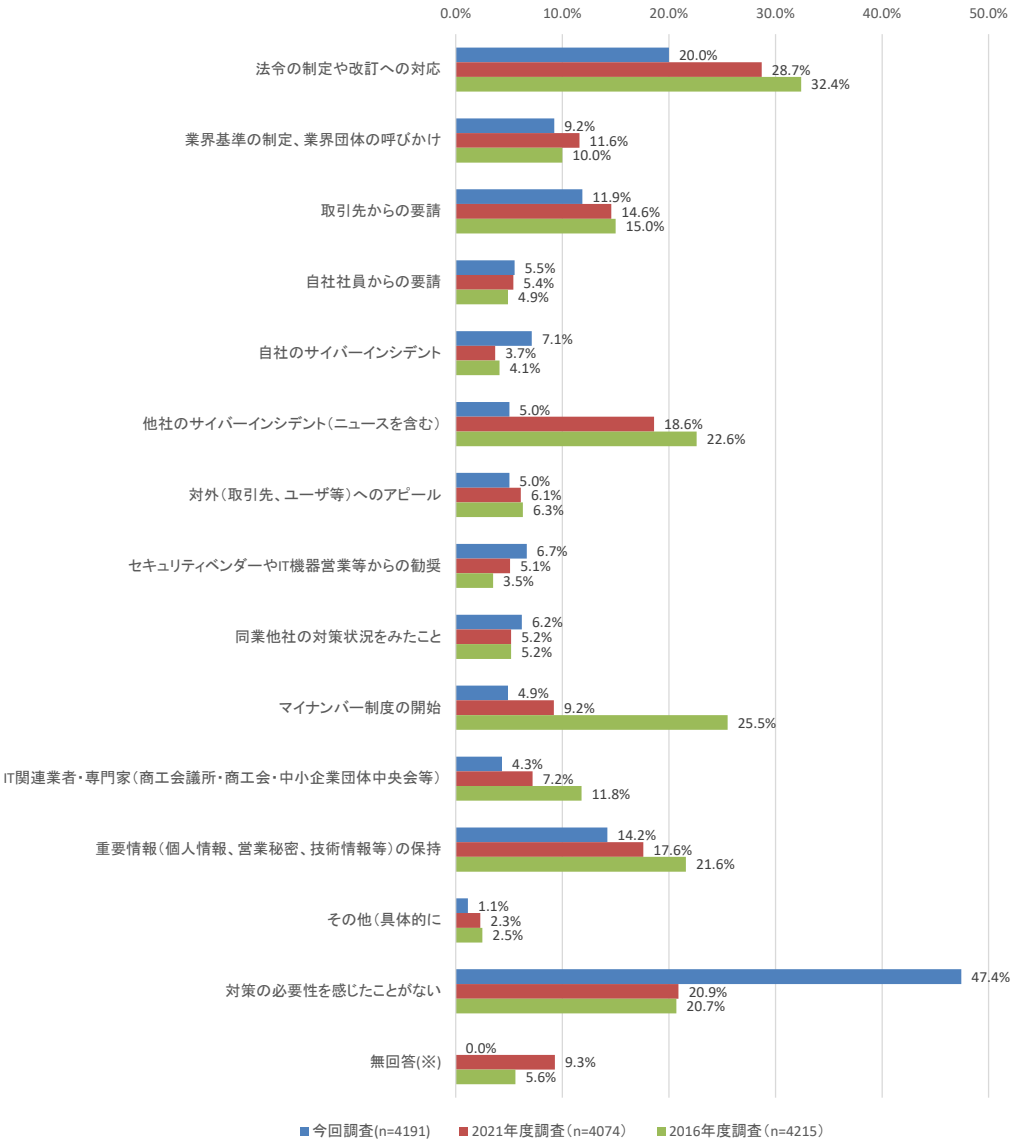

図 3-184 情報セキュリティ対策の必要性を感じたきっかけ（前回調査との比較）（n=4191）

g. 情報セキュリティ対策をさらに向上させるために必要と思われること

Q20. 貴社の情報セキュリティ対策を、さらに向上させるために必要と思うことは何ですか。

経営者および従業員の意識向上に対する必要性がいずれも低下しており、教育や意識改革に対する関心がやや薄れていることを示している。

企業での体制整備に対する需要も低下傾向にあり、2021 年度および 2016 年度から示されていた組織改革への意識が後退している。

特に必要なことがないとする企業が増加しており、意識改革や具体的な対策強化が進んでいない現状が見える。

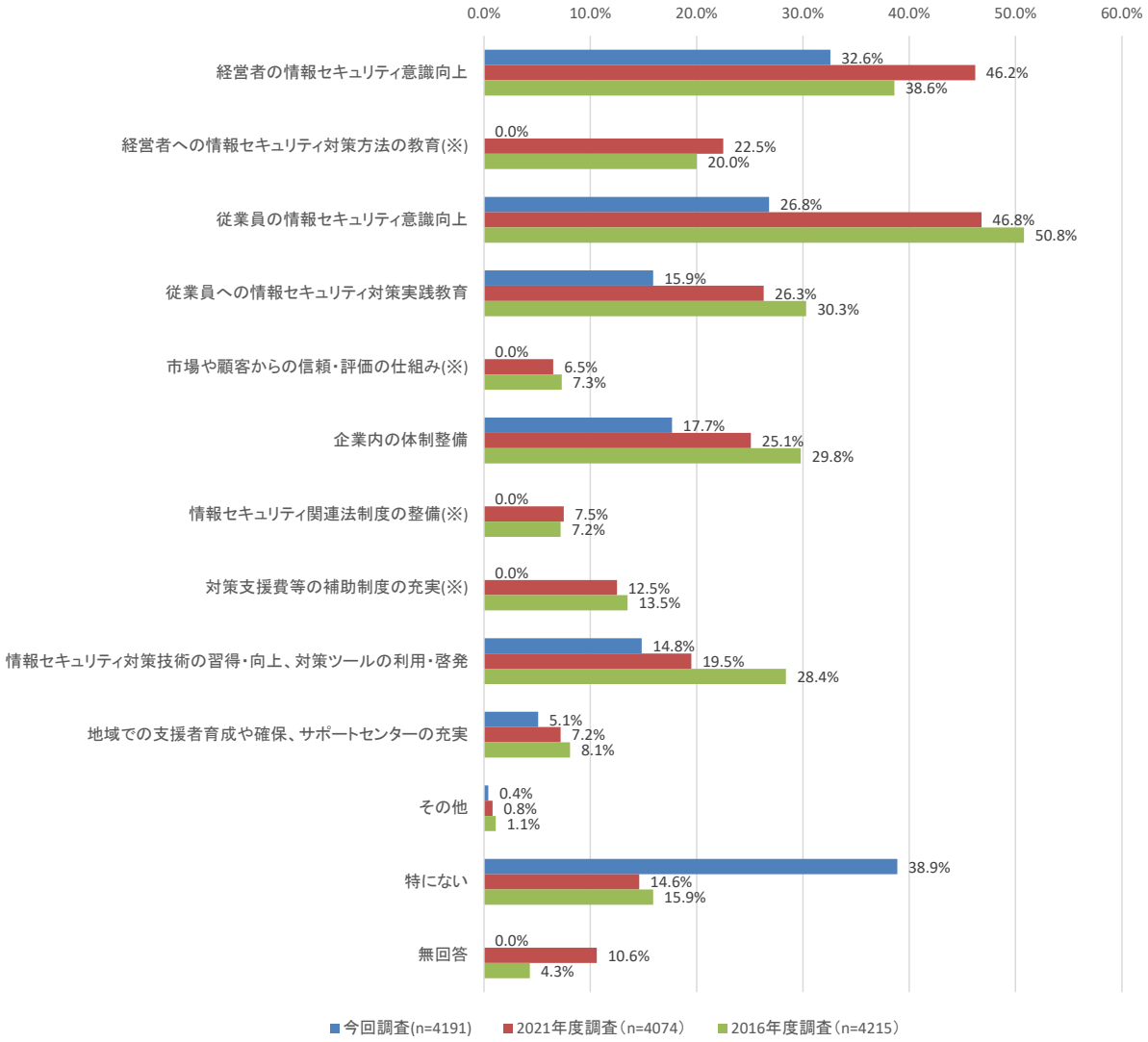

図 3-185 情報セキュリティ対策をさらに向上させるために必要と思われること（前回調査との比較）（n=4191）

3.5 分析

アンケート調査結果を元に、中小企業等における情報セキュリティ対策の実態及び課題の把握として、以下の観点で分析を行った。

- サイバーセキュリティ対策への取組状況
- サイバーセキュリティ対策実施への経営層の関与の状況
- サイバーセキュリティに関する被害の状況
- サプライチェーンにおけるサイバーセキュリティの状況

また、SECURITY ACTION 一つ星及び二つ星に求められる基準についての分析・調査、SECURITY ACTION 宣言及びサイバーセキュリティお助け隊サービスを導入する中小企業が、中小企業全体の割合に対して低い水準となっている理由の分析・調査として、以下の分析を行った。

- SECURITY ACTION の認知度・宣言状況・宣言の効果・宣言の理由／宣言しない理由
- サイバーセキュリティお助け隊サービスの利用状況、利用の効果、利用の理由／利用しない理由

3.5.1 サイバーセキュリティ対策への取組状況

サイバーセキュリティ対策へ積極的な企業と消極的な企業の二極化が見て取れた。対策を行っている企業では、ウイルス対策やファイアウォールなどの基本的な対策の導入率が過年度と比較しても上がっている。その一方で、中小企業の多くは情報セキュリティ対策に十分な投資をしておらず、投資していても多くが 100 万円未満であった。なお、投資していない多くの理由は、情報セキュリティに対する意識の低さや資金面であった。また、約半数が「対策の必要性を感じたことがない」と答えており、被害を受けていない企業が多いことも、対策が進まない一因と考えられる。

- ウイルス対策ソフトの導入率は 80.0%であり、2021 年度の 77.2%と比較して微増している。また、ファイアウォールや VPN 等の導入率もわずかではあるが増加傾向にある。(Q12)
- サイバーセキュリティ対策への取組状況として、情報セキュリティ対策投資の状況を見ると、全体の約 7 割が「投資していない」または「わからない」という回答である。投資を行っていても、約 2 割は「100 万円未満」であり、中小企業等においては情報セキュリティ対策への投資を行うケースは限られている。(Q6-2)
- また「投資していない」理由としては、「必要性を感じていない」が約 44%であり半数近くが情報セキュリティへの意識がそもそも低いという結果が出ている。さらに「費用対効果が見えない」と「コストがかかりすぎる」を合わせると 45%を超えており、中小企業として資金が限られる中で情報セキュリティ投資に踏み出せない状況がうかがえる。(Q7)
- 情報セキュリティ対策実施のきっかけについては、全体の 5 割近くが「対策の必要性を感じたことがない」と回答しており、経済活動の範囲が限られる中小企業においてサイバーセキュリティ対策を必要とする事態に直面する機会が限られるという現実を反映していると思われる。これは、サイバーインシデント被害について「被害にあっていない」が全体の約 3/4 ということにも表れている。(Q9、Q34)

3.5.2 サイバーセキュリティ対策実施への経営層の関与の状況

中小企業における情報セキュリティ対策の向上には、経営層の関与と意識の向上が重要であると多くの回答者が認識している。実際、「経営者のリスク意識の向上」や「経営層向け手引書・教育」のニーズが高く、経営層自身が知識不足を自覚している傾向が見られた。一方で、インシデント対応計画やセキュリティ事故発生時の体制や対応手順対策体制の整備が進んでいない現状が見られた。また、セキュリティ教育を実施していない企業、外部研修を利用する意向がない企業が多く、人材育成も大きな課題であることがわかった。

- 情報セキュリティ対策をさらに向上させるために必要と思うこととして、「経営者のサイバーセキュリティリスク意識の向上」との回答が 32.6%と最も大きく、回答者の 84.6%が経営層（経営者・役員）であることを考慮すると、経営層自身が情報セキュリティ対策に関与することの重要性を認知していることが推察される。（Q20、SC5）
- また、利用したいサービスとして「経営層向けの手引書」を選択する回答が 28.9%ともっと多く、次いで「経営層向けの教育」との回答が 22.1%と、多くの中小企業で経営層自身が情報セキュリティ対策の知識不足を不安視している実態が読み取れる。（Q21）
- 経営層の大切な役割として、情報セキュリティ対策のルール化とインシデント発生時の対応計画の整備があげられるが、サイバーインシデント発生時の対応方法が「決まっていない」との回答が 37.3%も存在し、対応計画の策定が進んでいない現状が読み取れる。（Q16）
- また、セキュリティ事故発生を想定した緊急時の体制整備や対応手順の整備を実施していないとの回答が 47.3%であり、体制や対応手順の整備が多くの中小企業にとって共通の課題であることが示されており、経営層の積極的な関与が期待される。（Q80 項目 24）
- 経営層の情報セキュリティ対策への関与で最も重要な点の一つとして情報セキュリティ対策投資を行うことがあげられるが、投資をしていない理由として「必要性を感じていない」との回答が 44.3%である。情報セキュリティ対策を実施（強化）するきっかけについて尋ねた設問では、「対策の必要性を感じたことがない」とする回答が 47.4%となっており、企業全体でセキュリティ対策の必要性がまだ十分に理解されていないことを示している。（Q7、Q8、Q9）
- 経営層が積極的に従業員に対する情報セキュリティ教育を実施することは、組織全体としての情報セキュリティ人材育成に向けた重要課題であるが、情報セキュリティ教育として特に実施していないと回答した企業が 63.6%である。この高い割合は、経営層を含めた全社的なセキュリティ意識向上の機会が不足していることを示唆している。（Q25）
- 情報セキュリティ人材育成のために外部研修を活用する意向がない企業は 80.2%に及び、多くの企業において、経営層を含む情報セキュリティ教育やトレーニングの機会が乏しいことが示されている。経営層が主体的に学ぶ場を設け、具体的な事例を通じてリスクの現実を理解することが推奨される。（Q27）

3.5.3 サイバーセキュリティに関する被害の状況

2023 年度、中小企業におけるサイバーインシデントの被害は最も多いのはコンピュータウイルス感染、次いで不正アクセスが挙げられた。また、被害によって、データ破壊や個人情報漏えい等の問題が

発生している。また、被害を受けた多くの企業では、取引先に何らかの影響を及ぼしており、サービス遅延や停止、補償負担など、サプライチェーン全体に悪影響が及ぶ実態が明らかになった。不正アクセス被害では、脆弱性の悪用や ID・パスワードの不正利用が多く、システム更新の遅れや認証管理の甘さがリスク要因となっている。また、ウェブサービスの停止も発生しており、事業継続に直接的な影響を及ぼすため、迅速な対策が急務である。

- 2023 年度において、サイバーインシデントの被害を受けた企業はコンピュータウイルスの感染が 14.8%と最も多く、その次に不正アクセスの影響を 10.0%の企業が受けている。これらの被害は中小企業にとって現実的な脅威であることが示されている。またサイバーインシデントによる影響として、データの破壊(35.7%)や個人情報の漏えい(35.1%)が最も多く発生している。これによって企業の信頼性や業務運営に直結する深刻な問題が発生している状況が分かる。(Q34、Q35)
- 2023 年度にサイバーインシデントの被害を受けたと回答した企業(975 件)のうち、取引先にサービスの停止や遅延による影響が出たとの回答は 36.1%であり、また個人顧客への賠償や法人取引先への補償負担の影響が出たとの回答は 32.4%、続いて原因調査・復旧に関わる人件費等の経費負担で 23.2%と高い割合で取引先に影響が出ていることが読み取れる。(Q36)
- 「特に無し」を除くと全体の 70%程度がサイバーインシデントにより取引先に影響があったと回答しており、サプライチェーン全体でのサイバーセキュリティの不備は、企業を取り巻く環境だけでなく取引先にも深刻な影響を及ぼし、事業の継続性を脅かす実情を浮き彫りにしている。(Q36)
- 2023 年度にサイバーインシデント(不正アクセス)に遭ったと回答した企業(419 件)のうち、48.0%の企業がぜい弱性を突かれた不正アクセスを経験しており、企業のシステム更新の遅延が深刻なリスクを招いていることを示し、ぜい弱性管理の重要性が再認識されている。また、ID・パスワードの不正利用によるなりすましが 36.8%と報告され、この形式の攻撃が依然として効果的であることが読み取れる。認証情報の管理不備が重大な侵入の引き金となるため、多要素認証などの強化策が推奨される。(Q37)
- また、22.9%の企業がウェブサイトのサービス停止または機能低下を経験しており、ウェブサービスの可用性が脅かされている現状が示されている。これらは企業のオンライン事業活動に直接響くため、迅速な復旧と再発防止策が急務であることを示している。(Q38)

3.5.4 サプライチェーンにおけるサイバーセキュリティの状況

販売先(発注元企業)から情報セキュリティに関する要請を受けた企業限定的であり、要請内容の多くは秘密保持に関する内容であった。また、契約違反時の措置を講じている企業は一定数存在し、契約面での対応も進んでいる。一方で、仕入先(発注先企業)に対してセキュリティ対策を要請した企業はわずかであり、仕入先(発注先企業)への働きかけは消極的であった。しかし、要請を受けた企業の多くは、要請に対応しており、対応意欲が高いことがわかる。さらに、要請への対応が取引につながったとする企業は多く、セキュリティ対策がビジネスの信頼性向上に寄与していることが示された結果となった。

- 販売先(発注元企業)から情報セキュリティに関する要請を受けたとの回答(511 件)は全体の

12.2%に留まる。販売先(発注元企業)から情報セキュリティに関する要請を受けた企業の内では、取引先からの要求で最も多いのが秘密保持で 79.6%である。また、情報セキュリティに関する契約違反時の措置を導入する企業が 36.4%と高い割合であり、契約面での対応にも注力している状況を示唆している。(Q46、Q47)

- 情報セキュリティ対策の要請を仕入先に行ったことがある企業は 8.7%しかなく、依然として多くの企業が自らのサプライヤーに対し、積極的なセキュリティ要求をしていないことが浮き彫りになっている。(Q55)
- 要請に対して仕入先が応じたケースは 83.1%となっている。この結果は、実際に要請があれば、企業はセキュリティ対策を実施する意欲があることを示している。また、要請した情報セキュリティ対策を取引先が実施したことが取引につながった大きな要因であると認識している企業は 69.1%と高く、サプライチェーン全体で求められるセキュリティの標準とその実装がビジネスの信頼性確保に重要であることを示唆している。(Q56、Q57)

3.5.5 SECURITY ACTION の認知度・宣言状況・宣言の効果・宣言の理由／宣言しない理由

SECURITY ACTION を宣言している企業は全体の半数以下であった。宣言の主な理由は、補助金・助成金の申請要件や取引先からの要請であり、外部からの動機が大きい。宣言しない理由は、知らなかった、必要性を感じない、費用対効果が不明であること等が挙げられ、認知度の向上とメリットの周知が課題となっている。一方で、宣言の維持率は高く、継続実施に一定の効果があることが示されており、制度が企業のセキュリティ意識や体制に良い影響を与えていると考えられる。

- SECURITY ACTION を認知している企業は全体の 10.4%に留まった。SECURITY ACTION を知っていると回答した者の内、「★1 を宣言している」企業が 37.1%、「★2 を宣言している」企業が 19.1%である。「していない」企業は 43.8%に上る。「SECURITY ACTION の宣言を行った主な理由」には、補助金や助成金の申請要件が 54.9%、顧客や取引先からの要求が 48.4%である。企業の戦略的な選択として、外部からの要請や利益に対する動機が大きい。(Q60、Q61、Q62)
- 「SECURITY ACTION を宣言しない理由」には、「知らなかった」(38.6%)に次いで「必要性を感じられない」が 28.5%、「費用対効果が不明確」が 15.9%である。認知度の向上と SECURITY ACTION を宣言することの効果に関する訴求が必要であることが示唆されている。(Q68)
- SECURITY ACTION の宣言を維持できている企業は 87.3%で、継続的な実施が比較的安定していることがわかる。これは、宣言後の変化としての意義やメリットを認識している企業が多い可能性を示しており、制度的枠組みが組織体制に一定の影響を与えていると考えられる。(Q63)

3.5.6 サイバーセキュリティお助け隊サービスの利用状況、利用の効果、利用の理由／利用しない理由

「サイバーセキュリティお助け隊サービス」は、中小企業向けに 24 時間の異常監視や緊急時の駆け付け支援、相談窓口の設置、簡易的なサイバー保険などをワンパッケージで提供し、低価格で安心のサポートを実現しています。しかしながら、このサービスの認知度はわずか 7.0%にとどまり、実際に導入している企業は非常に限られている。認知度や普及率の低さが導入の伸び悩みの一因となっており、サービスの普及や情報提供が課題である。また、導入を見送る理由としては「リソース不足」や「費用対効果が不明確」といった点が挙げられ、特にセキュリティ人材の不足や導入のメリットが十分に理解されていないことが障壁となっている。

- サイバーセキュリティお助け隊サービスは、中小企業向けに 24 時間の異常監視、緊急時の駆け付け支援、相談窓口の設置、簡易的サイバー保険などをワンパッケージで提供し、低価格で安心のサポートを行っている。サービスを利用した企業が「ワンパッケージでの情報セキュリティ対策」を 56.9%で最も評価し、続いて「導入が容易」(55.9%)を挙げている。これは、サービスの実装のしやすさが企業にとって重要な魅力となっていることを示すもの考えられる。(Q73)
- 「サイバーセキュリティお助け隊サービス」を知っている企業は 7.0%にとどまり、多くの企業がこのサービスを認識していないことが示されている。また、知っていると回答した企業(293 件)の内、実際にサービスを導入している企業は34.8%であり、利用企業は限定的となっている。この低い認知度や普及率は、サービスの利用状況が伸び悩んでいる理由の一つである可能性が高く、サービスの普及や情報提供を行うことでサービスの普及につながることが推察される。(Q70、Q71)
- サイバーセキュリティお助け隊サービスを知っているが導入しない企業(185 件)の内、サービス導入を見送る理由として「リソース不足」が 29.7%、「費用対効果が不明確」が 33.0%であった。一方でサイバーセキュリティお助け隊サービスを知らない企業(2,149 件)の内、利用しない理由として「必要性が感じられない」と答える企業が 46.9%に達している。このことはお助け隊サービスの導入の障壁となっている点として、セキュリティ人材の不足に加え、導入のメリットを十分に理解されていないことが示唆される。(Q74、Q76)

4. インタビュー調査

アンケート調査の結果を踏まえ、アンケート調査では捉えきれない実態等を把握するため、中小企業等へのインタビュー調査を実施した。インタビュー調査の対象者は、中小企業等における経営層を対象とし、やむを得ず代理回答となる場合でも、経営層からの回答を収集するように努めた。企業へのインタビューにあたっては、以下の条件を満たすよう実施した。

- インタビュー調査の対象企業は、アンケート調査の回答企業のうち、IPA と協議の上、国内企業 20 社を選定した。
- 調査項目は、アンケート調査の内容を深掘りするため以下を聞いた。
  a. サイバーセキュリティの管理体制
  b. サイバーセキュリティ対策への取り組みを行う上での課題や重要と考える事項
  c. 取引先からの要請状況
  d. サイバーセキュリティ対策の費用と効果の捉え方
  e. サイバーセキュリティ対策の第三者評価の利用状況

具体的なインタビュー調査の概要、調査項目、調査結果について以下に記す。

4.1 調査概要

アンケートの回答結果から、有効な対策を実施していると想定される企業を抽出し、アンケート調査では捉えきれない実態等を把握し、有効な対策や効果を明らかにすることを目的にインタビュー調査を実施した。そのうえ、インタビュー調査結果をもとに、他社の模範となる取組や、他社にとって参考になる取組について、グッドプラクティスを整理した。

4.2 調査項目

調査項目は以下のとおりである。設問番号1～15番（赤色）を中心にインタビューを行った。設問番号16～26番はインタビュー時間に余裕があった場合に問うようにした。

表 4-1 インタビュー調査項目

インタビュー調査項目		番号	質問
セキュリティ管理	管理体制の確保状況	1	経営者として、貴社におけるセキュリティ対策にはどのように関わっていますか。
		2	セキュリティに関する組織全体の対応方針について、具体的にどのように意思決定を行っていますか。また、意思決定の過程で苦労されることがあれば教えていただけますか。

インタビュー調査項目		番号	質問
		3	貴社の管理体制や実施しているサイバーセキュリティ対策において、取り組み内容や水準の改善に向けたプロセスが含まれていますか。もし含まれている場合、具体的にどのようなものが含まれているか教えていただけますか。
		4	貴社が認識しているセキュリティ上のリスクについて教えていただけますか。可能であれば、認識している全てのリスクとそれぞれのリスクの大きさも併せて教えていただけると幸いです。
		5	貴社では、インシデント発生時の対応や復旧のための体制（BCP：事業継続計画）を整備していますか。また、その体制を整備する際に参照した情報があれば教えていただけますか。
	セキュリティ対策を行う上で重視していること	6	セキュリティ対策を行う上で、最も重要だと考えていることは何ですか。
対策コスト感	セキュリティ対策にかかるコストの相場観	7	セキュリティ対策の導入コストおよび運用コストについて、どの程度のコストをかけ、具体的に何を実施していますか。また、「お助け隊サービス」の導入の有無も教えてください。さらに、セキュリティ対策への投資の妥当性については、どのように考えていますか（例：毎年10万円をサイバーセキュリティに投資する場合、なぜその額が適当だと判断するのか）。また、月額の予算額はおおよそいくらですか。
	コストをかけずに実施した対策	8	費用をかけずに実施したセキュリティ対策はありますか。もしある場合は、具体的にどのような対策をコストをかけずに実施できたか教えていただけますか。
	対策によるメリット	9	セキュリティ対策を実施して良かったと思うことはありますか。また、今後も継続して実施していきたいとお考えですか。具体的なエピソードがあれば、ぜひ教えてください。
	必要としている対策とその実現性	10	貴社では、守るべき情報に応じて必要となるセキュリティ対策を検討していますか。また、その際にどのような判断基準を設けていますか。さらに、実施状況や対策にかけているコストについても教えていただけますか。
		11	必要としているセキュリティ対策が実現できていない場合、その主な課題は何ですか（例：コストなど）。具体的に教えていただけますか。
	費用対効果の悪い対策	12	実施してみたものの、結果として必要がなかったセキュリティ対策はありますか。もしある場合、その理由について教えてください。また、そのセキュリティ対策にかかった費用や、必要がないと判断した後の改善方法についても教えていただけますか。
サプライチェーン対応	セキュリティ対策の要請とコストの考え方	13	貴社のサプライチェーン上の位置付けや、属する業界について教えてください。特に、取引先としてどのような業種の企業が何社程度あるかもお伺いします。また、取引先からセキュリティ対策の要請を受ける頻度についても教えていただけますか。

インタビュー調査項目		番号	質問
		14	貴社においてセキュリティ対策を実施した結果、そのコストを一般管理費の増加分として商品価格やサービス価格に転嫁し、値上げしたことはありますか。もし値上げした場合、取引先の反応はいかがでしたか。
		15	取引先企業から、ランサムウェア攻撃による貴社のシステム停止が自社の業務にも影響を及ぼすため、セキュリティを強化し安定した取引関係を築く観点から、セキュリティ機器やツールの導入（例：サイバーセキュリティお助け隊サービスの導入）や、ISMSやPマークなどの認証取得といったコストを要するセキュリティ対策を要請された場合、どのように対応しますか。また、発注者側から「対策をしない場合には今後取引には応じない」と言われた場合、どのように応じますか。 さらに、応じる場合、セキュリティ対策に要したコストを発注者側に（一部）負担してもらうための価格交渉を行いますか。その際、どのような説明をして相手方に価格転嫁に対する理解を求めますか。それ以外に、価格交渉に際してどのような要求を行うかについても教えてください。
インシデント対応	インシデントによってどの程度、事後対応にコストがかかるのか	16	貴社で発生した具体的なインシデントの内容について、被害状況、復旧にかかったコスト、および復旧までに要した期間について教えていただけますか。
	インシデントをきっかけとしたセキュリティ対策	17	インシデント発生の前後で、貴社のセキュリティ対策を見直しましたか。見直した場合、具体的にどのような対策を行い、どのくらいのコストをかけましたか。見直しを行っていない場合、その理由について教えてください。また、今後、見直しを行う予定はありますか。
人材育成	セキュリティ対策と社内の人材状況	18	貴社で実施しているセキュリティ対策について教えてください。また、その実施のための社内セキュリティ人材の配置状況についても教えていただけますか（兼任の場合は、どの程度セキュリティ対策に従事しているかもお知らせください）。 注：ここでいう社内セキュリティ人材とは、企業のサイバーセキュリティ対策を統括する業務を主に行う者を指します。具体的には、企業の個別の事業を遂行する中で対策を行う者ではなく、社内のセキュリティ規定の策定やセキュリティ対策ツールの導入などの日常的な対策や、インシデント時の対応を、外部の専門家への相談を含めて社内で主導する者です。
	人材育成に関する取組	19	社内人材の確保・育成のために、貴社として実施している取り組みはありますか。特に、大きなコストをかけずに始められる具体的な取り組みについて教えてください（例：経験者の中途採用、特定曜日の非常勤活用、社内公募、無料の教材・コンテンツの活用など）。

インタビュー調査項目		番号	質問
	人材不足の課題と必要な支援	20	セキュリティ人材を増やすためには、どのような課題があると考えていますか（例：自社内に適切な人材がいない、中途採用への応募がない、条件面で折り合えない、外部の専門人材を活用しようにも適切な相談先が見つからないなど）。また、これらの課題を解決するために、国や第三者機関からどのような支援が必要だと考えていますか。
外部委託	相談先への相談状況	21	セキュリティ対策を進めるにあたり、具体的に相談している先について教えてください。また、その相談先に対して具体的にどのような相談を行っているか、どのくらいのコストを支払っているかについても教えてください。さらに、相談先の方はセキュリティを高める観点から適切な助言をしてくれていると感じますか。
	日常的な相談先とのコミュニケーション	22	貴社では、商工会議所、よろず支援拠点、IT コーディネーター、銀行、地域の IT ベンダー企業、税理士や行政書士といった資格者など、普段からコミュニケーションを取っている相談先はありますか。そういった相談先と、DX（デジタルトランスフォーメーション）やセキュリティに関する取り組みについて、どのような相談を行っているか教えてください。
	相談していない場合の対策	23	反対に、外部の相談先には相談せずに自社内でセキュリティ対策を考え実施している場合、どのような情報を参照してセキュリティ対策を実施していますか。また、参照した情報に基づいて行った対策は効果がありましたか。その際にかかった費用についても教えてください。
第三者評価制度や支援策	第三者評価制度の取得状況と、第三者評価制度の取得に要したコスト・取得によるメリット	24	貴社は、ISMS、P マーク、技術情報管理認証制度などの認証を取得していますか。取得している場合、どの認証を取得しているか、それを取得したきっかけ、取得に要した費用、および具体的なメリットについて教えてください。取得していない場合、どのようなきっかけがあれば取得する考えがありますか。また、コストの負担以外で、第三者評価を取得するに当たってのハードルがあれば教えてください。
	SECURITY ACTION 達成状況について	25	貴社は、「SECURITY ACTION 宣言」の 25 項目を達成できていますか。
	グッドプラクティス	26-1	貴社は「SECURITY ACTION 宣言」の 25 項目を達成できていますか。達成できている場合、それを実現するためにかかったコストや期間について教えてください。また、現在も継続できていますか。継続できていない場合には、継続的に達成できない項目、その理由や課題、どのようにしたら継続して達成できるかについても教えてください。
	バッドプラクティス	26-2	貴社が「SECURITY ACTION 宣言」の 25 項目を達成できていない場合、その理由や課題について教えてください。達成できていない具体的な項目や、どのようにしたら継続して達成できるか、またその達成を持続できるかについてもお聞かせください。

4.3 調査結果

アンケート回答者からサイバーセキュリティ対策に力を入れている企業を抽出し、インタビューを実施した。インタビュー調査の結果から得られた中小企業等における実態と課題を整理する。

取引先からのセキュリティ要請はほぼ全ての企業が経験しており、対応は取引関係や内容によって様々であるが、断りづらい風潮との声もあった。

サイバーセキュリティ対策を行うことにより新たな取引につながっている例も見られた。

4.3.1 セキュリティ管理について

中小企業等におけるセキュリティ管理状況について整理した。

（1） 管理体制の確保状況

a. 経営者としての関与

- 経営層が、サイバーセキュリティ対策の内容にまで関わる事例と、コスト面だけに関わる事例とがあった。具体的な関わり方は、自身に決定権がある、役員会議への付議を行う、その他（最終決定は関与するが内容はセキュリティ担当者に一任する、回答者が担当者等）であった。

b. 意思決定の過程で苦労すること

- 課題を感じている回答のうち、約半数は金銭的コストに関する課題であった。

c. サイバーセキュリティ対策の取組内容改善のプロセス

- 改善プロセスがあるとの回答より、改善プロセスがないとの回答が多くあった。
- 改善プロセスがあるとの回答では、ISMS による見直し、親会社からの指示に従って行う見直し、独自のプロセスによる見直しが行われているとの回答があった。

d. 認識しているセキュリティ上のリスク

- 認識しているセキュリティ上のリスクに関しては、顧客情報や自社内の機微な情報などの漏洩に対する回答が最も多かった。他には、マルウェア感染、社員のリテラシー不足、事業の継続、デバイス管理、有事の体制の欠如、サイバー攻撃であった。

e. インシデント発生時の体制整備

- インシデント発生時の体制について、整備されていないとの回答が最も多くあった。整備されているとの回答において、参考とした情報については、社内担当者、社外の相談相手や所属協会など、自社関係者によるものが多かった。

f. セキュリティ対策を行う上で重視していること

- セキュリティ対策を行う上で最も重要だと感じていることについては、業務の継続性、情報漏洩対策に関する回答があった。
- 「d. 認識しているセキュリティ上のリスク」の回答との関係性では、業務の継続に関するリスクを感じている回答者は、セキュリティ対策についても業務の継続性を重要だと感じているなど、関係性が見えた。

4.3.2 セキュリティ対策のコスト感

中小企業等のセキュリティ対策コストについて調査した。

a. セキュリティ対策にかかるコストの相場観

- セキュリティ対策にかけるコスト(IT 導入含む)について、最も低い金額は月に数千円程度、最も高い金額は年に 2～3 億円との回答であった。
- 回答者の売上に着目した場合、最も低い金額を回答した企業の売上は 1000 万円以下、最も高い金額を回答した企業の売上は 3 億円超であることから、売上によってセキュリティ対策に割ける金額が異なることがわかる。他方で、売上が 3 億円超の企業であっても、セキュリティ対策にかけるコストは年に 10 万円という企業もあり、単純に売上が高い場合にセキュリティ対策にかけるコストが高いとは限らない結果となった。
- セキュリティ対策の内容としては、ウイルス対策ソフトに関する回答が最も多く、他には、サイバー保険の加入、独自システムの構築、UTM の導入であった。

b. コストをかけずに実施した対策

- 費用をかけずに実施したセキュリティ対策としては、社員教育に関する回答が多く、他には無料のウイルス対策ソフトの導入、業務終了時におけるオフィスのネットワーク遮断、クリアデスクの実施、取引先のシステムエンジニアとの情報交換、不要なソフトの見直し、社内ルールの設定であった。

c. 対策によるメリット

- セキュリティ対策を実施したことによるメリットとしては、取引につながった又は顧客からの信頼度が上がった、安心感など精神面に関する回答があった。他には、リスクの可視化による運用性の向上、ISMS 取得による税制優遇に関する回答があった。

d. 必要としている対策とその実現性

- 守るべき情報に応じたセキュリティ対策の検討としては、検討しているとの回答が多くあった。その内、顧客データや重要データなどの情報資産によって判断している、親会社からの要請に対応するとの回答があった。コストに関しては年間で数十万円から 1000 万円まで様々であった。
- 親会社からの要請に対応している企業では、最低限の要請の内容はコスト的な負担はないが、

理想的な（最高レベル）の要請の内容はコスト的な負担が大きいという課題が挙げられた。

e. 必要としている対策が実現できない場合の原因

- 実現できていないセキュリティ対策に対する課題として、社員教育等の人的要素に関する回答、金銭的コストに関する回答であった。他には、回答者（役員）自身の知識不足、情報漏洩リスクへの対策・体制の不備、セキュリティ対策の範囲の不明確に関する課題が得られた。
- セキュリティ対策が実現するための課題として、そもそも課題が整理されていないという回答があった。

f. 費用対効果の悪い対策

- 不必要と感じたセキュリティ対策としては、無償のウイルス対策ソフトに関するものであった。その他、ISO 等のセキュリティ対策関連の認証は不要との回答があったが、回答者の業種においてはセキュリティ対策が集客力の向上に直結しないことを理由としていた。

4.3.3 サプライチェーン対応

中小企業が取引先から受けるセキュリティ対策要請への対応について調査した。

a. セキュリティ対策の要請とコストの考え方

- サプライチェーン上の位置付けについて、特定の発注元がなく直接エンドユーザーと取引しているとの回答が 11 件であり、また、親会社や不明といった回答を除くと、事業者からの発注を受けている旨の回答は 7 件であった。また、取引先数については数社から数十社であった。
- 委託先に関しては、何らかの委託を行っているとの回答が 10 件あり、数は 10 社以内であった。
- セキュリティ要請の内容に関しては、秘密保持契約、チェックシート、要請元の自社への訪問、監査、データ送信時の取扱い（パスワード付与、アップローダー利用等）が挙げられた。

b. セキュリティ対策に関する価格転嫁

- セキュリティ対策に関する価格転嫁の経験について、ありとの回答が 6 件、なしとの回答が 15 件となった。ありと回答した意見の具体的内容としては、取引先と自社との折半（自社または取引先いずれかの負担割合増を含む）、あらかじめ製品価格に転嫁済み、工事費に転嫁、内部的に上乗せが挙げられた。
- 価格転嫁の経験が無い企業では、価格転嫁によって価格構造を変更することは取引先からは受け入れられない懸念が挙げられた。

c. 取引先企業からのセキュリティ対策要請

- セキュリティ要請があった場合の対応の有無について、対応するとの回答が 15 件、対応しないとの回答が 6 件であった。対応するとの回答としては、取引先との関係性を考慮する意見や、自社へのメリットがある場合に限り対応するとの意見があった。

- また、要請された場合の価格交渉の有無に関しては、行うとの回答が 10 件、行わないとの回答が 11 件であった。価格交渉を行うとの回答としては、取引先との関係性に左右されるとの意見が多かった。
- 取引先から ISMS やＰマークの取得を要請された場合、対応が困難と感じる企業がいる結果となった。
- 要請された場合に価格交渉を行わないと回答した企業では、価格競争のため現実的ではないという課題が挙げられた。

4.4 分析

インタビュー結果から、効果が高い対策として低コストで実施することができるものや、企業価値を上げることで取引増に役立つものといった他社にとって参考になる取組を抽出・整理し、「グッドプラクティス」の事例として 10 社を選出した。

4.4.1 グッドプラクティス事例

選出した事例は、ISMS やサイバーお助け隊サービスといった制度を活用した取組と、自社の工夫による独自の取組の 2 種類に大別可能であるため、それぞれの分類で分析・整理を実施した。

独自の取組のうち、特に低コストで実施できるものについて、中小企業という枠内で考えたときに他社でのフィージビリティの観点から有用であると考え、それらが分かるように印付けを実施した。

（1） 認証制度およびサイバーセキュリティお助け隊サービスを活用した取組み

グッドプラクティスのうち制度を活用した取組は以下の通りである。

表 4-2 グッドプラクティス

項目	プラクティスの内容
認証制度の取得	（情報通信業） 今後の取得費用増額の可能性を考え、先んじてＰマークと ISMS を取得 （個人向け学習塾） 大手の塾で発生した情報漏洩の事案を受けて情報管理の必要性を認識し、ISMS を取得 （情報サービス業） ISMS の取得をはじめとしたセキュリティ対策によって全社的なセキュリティ意識が全社的に向上した他、取引のきっかけにもなり、顧客の評価も向上 （製造業） 納入先から ISMS 取得の要請があり、その取得が取引において大きなアドバンテージとなった。 （クラウドサービス提供等の IT 関連事業者） ISMS を取得したことで、顧客との契約締結に発展。また、セキュリティ対策に取り組んだことでパソコンの電

項目	プラクティスの内容
	車内への置忘れや、私物 USB メモリを使用しない等のセキュリティ意識が醸成
お助け隊サービスの活用	（製造業）「サイバーセキュリティお助け隊サービス」の利用により、社員の過失による情報漏洩が防げるといった安心感を享受。導入に際しては、社内の知的財産を守ってくれることや、万が一の時の助け舟となることを社長に説明

（2）自社独自の取組み

グッドプラクティスのうち自社独自の取組は以下の通りである。また特に費用をかけずに実施できる対策については〇印で示す。

表 4-3 グッドプラクティス（自社の取組み）

項目	プラクティスの内容	低コスト
パソコン以外へのバックアップ	（製造業） 事業継続の観点から、CAD のデータをクラウドにバックアップ。また、複数の機能を有する点で費用対効果が高いと考え、UTM を導入	
NW 遮断による不正アクセス防止対策	（その他サービス業） 業務終了時にネットワークを遮断することで、夜間における不正アクセスを防止	〇
サプライチェーンでの情報共有	（製造業） 費用をかけないセキュリティ対策の一環として、社内 SE と取引先 SE とで情報共有を行い、互換性のあるセキュリティ対策を実施	〇
情報漏洩対策	（その他サービス業） 機密情報は別々のデバイスで管理することで、漏洩リスクを軽減 （保険代理店 I） 内部からの情報漏洩防止の観点による社員からの誓約書の徴集、メモ紙や記録文書の持出に対する意識付けの実施、情報漏洩時のエスカレーションを規定、サイバー保険に加入	
セキュリティ対策の見直し	（情報通信業）年に一度の頻度で全体的な見直しを行うことで、セキュリティ対策の更新や改善を実施している他、社会的なトレンドや大規模なサイバー事件が発生した時にも、再評価を実施	〇
	（製造業） 商工会議所が実施する無料の情報セキュリティに関する講習会に参加し、新しい情報を入手	〇
	（情報サービス業） 費用をかけずに行ったセキュリティ対策とし	〇

項目	プラクティスの内容	低コスト
	て、不要なソフトの見直しと削除を実施	
無料のセキュリティセミナーの活用	インターネット上やセキュリティコンサルタントが提供する無料のセキュリティセミナー等を社員向けトレーニングに活用	○
インシデントの早期発見の取組	（製造業）インシデントの早期発見を目的として、気づいた問題点をすぐに共有できるイントラネットの掲示板を設置	

（3）企業規模別の整理

グッドプラクティスとして選出した事例について、他社において活用する際に、社の規模に応じて参照しやすくするという観点から、事業者規模に応じた分類を行った。

分類の基準は、アンケート回答における売上とし、抽出された 10 社をなるべく均等になるよう分類した結果、次の 3 種類に分類することとした。

- 5000 万円以下
- 5000 万円超 1 億円以下
- 3 億円超

※ 回答は選択制のため、同分類となっている事業者については、さらに資本金、総従業員数の順で並べ替えを実施。

売上による事業者規模別の分類整理の結果は次の通りである。

表 4-4 グッドプラクティス（事業者規模別）

売上	グッドプラクティス
5000万円以下	• 「お助け隊サービス」を活用している事例がある。 • 一方で、同分野の他事業者による情報漏洩事案を受けて ISMS を取得している事業者もある。
5000 万円超 1 億円以下	• 情報漏洩を意識した対策を行っている事業者の他、P マークや ISMS を取得している事業者もある。
3 億円超	• クラウドサービスの利用、UTM の導入、イントラネットの掲示板の設置、ISMS の取得といった費用をかけたセキュリティ対策を実施している事例が比較的多い。 • 一方で、無料のセキュリティセミナーの活用や、自社ネットワークの夜間の遮断といった工夫点も見られる。

（参考）事業者規模別事例分類（売上 5000 万円以下）

表 4-5 事業者規模別事例分類（売上 5000 万円以下）

売上	資本金	従業員数	業種	プラクティス事例
3000 万円超～5000 万円以下	1000 万円以下	5 名以下	個人向け学習塾	大手の塾で発生した情報漏洩の事案を受けて情報管理の必要性を認識し、ISMS を取得
3000 万円超～5000 万円以下	5000 万円超～1 億円以下	21 名～50 名以下	製造業（防犯カメラやレーザー加工装置の製造）	「お助け隊サービス」の利用により、社員の過失による情報漏洩が防げるといった安心感を享受 導入に際しては、社内の知的財産を守ってくれることや、万が一の時の助け舟となることを社長に説明

（参考）事業者規模別事例分類（売上 1 億円以下）

表 4-6 事業者規模別事例分類（売上 1 億円以下）

売上	資本金	従業員数	業種	プラクティス事例
5000 万円超～1 億円以下	1000 万円以下	6 名～20 名以下	保険代理店	内部からの情報漏洩防止の観点による社員からの誓約書の徴集、メモ紙や記録文書の持出に対する意識付けの実施、情報漏洩時のエスカレーションを規定、サイバー保険に加入
5000 万円超～1 億円以下	5000 万円超～1 億円以下	21 名～50 名以下	情報通信業（スマホアプリ開発）	• 今後の取得費用増額の可能性を考え、先んじて P マークと ISMS を取得 • 年に一度の頻度で全体的な見直しを行うことで、セキュリティ対策の更新や改善を実施している他、社会的なトレンドや大規模なサイバー事件が発生した時にも、再評価を実施

（参考）事業者規模別事例分類（売上 3 億円超）

表 4-7 事業者規模別事例分類(売上 3 億円超)

売上	資本金	従業員数	業種	プラクティス事例
3 億円超	1000 万円以下	6 名～20 名以下	製造業(建築用金属製品、建物骨組み鉄骨の製造)	• 事業継続の観点から、CAD のデータをクラウドにバックアップ • 複数の機能を有する点で費用対効果が高いと考え、UTM を導入 • 商工会議所が実施する情報セキュリティに関する講習会に参加し、新しい情報を入手
3 億円超	1000 万円以下	21 名～50 名以下	情報サービス業(エンタープライズ系の個別受注型ソフトウェア開発)	• ISMS の取得をはじめとしたセキュリティ対策によって全社的なセキュリティ意識が全社的に向上した他、取引のきっかけにもなり、顧客の評価も向上 • 費用をかけずに行ったセキュリティ対策として、不要なソフトの見直しと削除を実施 • インターネット上で提供されたり、セキュリティコンサルタントが提供する無料のセキュリティセミナー等を社員向けトレーニングに活用
3 億円超	3000 万円超～5000 万円以下	51 名～100 名以下	その他サービス業(政治関係の出版物、セミナーの運営、結婚相談所、冠婚葬祭業(献花等))	• 業務終了時にネットワークを遮断することで、夜間における不正アクセスを防止 • 機密情報は別々のデバイスで管理することで、漏洩リスクを軽減
3 億円超	3000 万円超～5000 万円以下	101 名～300 名以下	製造業(電子部品の開発設計)	• 納入先から ISMS 取得の要請があり、その取得が取引において大きなアドバンテージとなった。 • 費用をかけないセキュリティ対策の一環として、社内 SE と取引先 SE とで情報共有を行い、互換性のあるセキュリティ対策を実施
3 億円超	2 億円超～3 億円以下	301 名以上	製造業(太陽発電装置、蓄電池の開発・製造)	インシデントの早期発見を目的として、気づいた問題点をすぐに共有できるイントラネットの掲示板を設置

売上	資本金	従業員数	業種	プラクティス事例
3 億円超	3 億円超	51 名～100 名以下	IT 関連（情報通信業、情報サービス業、クラウドサービスの提供）	ISMS を取得したことで、顧客との契約締結に発展 また、セキュリティ対策に取り組んだことでパソコンの電車内への置忘れや、私物 USB メモリを使用しない等のセキュリティ意識が醸成

5. 考察

本章では、文献調査、アンケート調査、インタビュー調査の結果を踏まえて、以下の点について考察を行う。

- 中小企業等におけるサイバーセキュリティ対策の実態及び課題等
- 中小企業等における規模・業種等に応じた効果の高いサイバーセキュリティ対策
- SECURITY ACTION 一つ星及び二つ星に求められる基準
- SECURITY ACTION 宣言及びサイバーセキュリティお助け隊サービスを導入する中小企業が、中小企業全体の割合に対して低い水準となっている理由

5.1 中小企業等におけるサイバーセキュリティ対策の実態及び課題等

調査結果を踏まえて、中小企業等におけるサイバーセキュリティ対策の実態及び課題等について分析・整理を行った。

5.1.1 情報セキュリティ対策投資

アンケート調査の結果、中小企業の約6割が過去 3 年間で情報セキュリティ対策投資を実施していないと回答しており、また投資をしていない理由として必要性を感じないことを挙げた割合は小規模企業者では約 5 割となっているなど、中小企業では情報セキュリティ対策投資に踏み出せていない実態が明らかになった。これは東京商工会議所が実施した「会員企業の災害・リスク対策に関するアンケート 2024 年調査結果 [37]」においても中小企業の情報セキュリティ対策の年間投資額について「投資していない、または 50 万円未満の企業が約 5 割を占める」ことが示されており、同様の結果となっている。

中小企業におけるサイバーセキュリティ対策の導入では、対策の費用対効果が見えないことが課題のとして挙がっており、本調査では効果の高いサイバーセキュリティ対策として分析した結果を次項（5.2）に記載している。

5.1.2 中小企業等で求められるサイバーセキュリティ対策

中小企業等に求められる情報セキュリティ対策としては、IPA［中小企業の情報セキュリティガイドライン］で示された人的・組織的対策、技術的対策、物理的対策の実施が推奨される。一方で、サプライチェーン上のサイバーセキュリティリスクが増大していることも踏まえ、業界ごとに対策ガイドラインが整備され、「自動車産業サイバーセキュリティガイドライン（V2.1）」は技術情報管理認証制度における認証基準の改正 [38]において参照されるなど自動車業界以外でも注目されている。

5.1.3 SECURITY ACTION 宣言

[37] 東京商工会議所 https://www.tokyo-cci.or.jp/page.jsp?id=1203944
[38] 経済産業省「技術情報管理認証制（TICS）について」（2024 年 8 月）
https://www.meti.go.jp/policy/mono_info_service/mono/technology_management/pdf/outline.pdf

中小企業等におけるサイバーセキュリティ対策の推進に向けて、独立行政法人情報処理推進機構（IPA）が提供する「SECURITY ACTION」制度が存在する。本制度は、中小企業が自らのサイバーセキュリティ対策への取組状況を可視化し、段階的に対策を強化していくことを目的としている。SECURITY ACTION には「一つ星」「二つ星」の 2 段階が設けられており、企業は自社の状況に応じていずれかを宣言し、必要な対策を実施していく仕組みである。宣言を行った企業は、ロゴマークを用いた対外的なアピールが可能となり、取引先や顧客からの信頼向上にもつながることが期待されている。

このように、中小企業のセキュリティ対策を促進する制度が整備されつつあり、今後はそれらの活用と連携が重要となる。一方で SECURITY ACTION 宣言に関する認知度は非常に低い状況にあり、IPA が提供しているサイバーセキュリティお助け隊サービスと共に、その認知度を上げる取組みが必要である。

5.2 中小企業等における規模・業種等に応じた効果の高いサイバーセキュリティ対策

中小企業等における規模・業種等に応じた効果の高いサイバーセキュリティ対策について分析・整理を行った。

分析のアプローチとして、アンケート調査の結果に基づき、回答企業のサイバーセキュリティ対策の内容及びサイバーセキュリティ対策投資に関する設問を分析軸として、サイバーセキュリティ対策の効果を示すと考えられる設問とのクロス集計分析を実施した。この分析を通じて、各設問における回答結果間との関係性を明らかにし、サイバーセキュリティ対策と期待される効果との関連性を評価した。

回答企業のサイバーセキュリティ対策内容及び関連する投資に関する設問としては、サイバーセキュリティ対策の製品導入状況やセキュリティ体制の整備状況などを選定した。また、Q80 の 25 項目の設問内容は、IPA が提供する「5 分でできる！情報セキュリティ自社診断」[39]の「診断編」に掲載されている 25 個の診断項目と同じ内容になっているため、Q80 の回答結果を「5 分でできる！情報セキュリティ自社診断」で示された基準に沿って点数化し、25 項目の合計点を算出することで回答企業におけるサイバーセキュリティ対策のレベルが数値化される。それらの合計点を自社診断の総合的な指標（以下、“自社診断の合計点”と記載する）として、分析に活用した。なお点数化と合計点の算出方法は下図の通りである。

診断項目	No	診断内容	チェック			
			実施している	一部実施している	実施していない	わからない
Part 1 基本的対策	1	パソコンやスマホなど情報機器の OS やソフトウェアは常に最新の状態にしていますか？	4	2	0	−1
	2	パソコンやスマホなどにはウイルス対策ソフトを導入し、ウイルス定義ファイル※1 は最新の状態にしていますか？	4	2	0	−1
	3	パスワードは破られにくい「長く」「複雑な」パスワードを設定していますか？	4	2	0	−1
	4	重要情報※2 に対する適切なアクセス制限を行っていますか？	4	2	0	−1
	5	新たな脅威や攻撃の手口を知り対策を社内共有する仕組みはできていますか？	4	2	0	−1
Part 2 従業員としての対策	6	電子メールの添付ファイルや本文中の URL リンクを介したウイルス感染に気をつけていますか？	4	2	0	−1
	7	電子メールや FAX の宛先の送信ミスを防ぐ取り組みを実施していますか？	4	2	0	−1
	8	重要情報は電子メール本文に書くのではなく、添付するファイルに書いてパスワードなどで保護していますか？	4	2	0	−1
	9	無線 LAN を安全に使うために適切な暗号化方式を設定するなどの対策をしていますか？	4	2	0	−1
	10	インターネットを介したウイルス感染やSNSへの書き込みなどのトラブルへの対策をしていますか？	4	2	0	−1
	11	パソコンやサーバーのウイルス感染、故障や誤操作による重要情報の消失に備えてバックアップを取得していますか？	4	2	0	−1
	12	紛失や盗難を防止するため、重要情報が記載された書類や電子媒体は机上に放置せず、書庫などに安全に保管していますか？	4	2	0	−1
	13	重要情報が記載された書類や電子媒体を持ち出す時は、盗難や紛失の対策をしていますか？	4	2	0	−1
	14	離席時にパソコン画面の覗き見や勝手な操作ができないようにしていますか？	4	2	0	−1
	15	関係者以外の事務所への立ち入りを制限していますか？	4	2	0	−1
	16	退社時にノートパソコンや備品を施錠保管するなど盗難防止対策をしていますか？	4	2	0	−1
	17	事務所が無人になる時の施錠忘れ対策を実施していますか？	4	2	0	−1
	18	重要情報が記載された書類や重要なデータが保存された媒体を破棄する時は、復元できないようにしていますか？	4	2	0	−1
Part 3 組織としての対策	19	従業員に守秘義務を理解してもらい、業務上知り得た情報を外部に漏らさないなどのルールを守らせていますか？	4	2	0	−1
	20	従業員にセキュリティに関する教育や注意喚起を行なっていますか？	4	2	0	−1
	21	個人所有の情報機器を業務で利用する場合のセキュリティ対策を明確にしていますか？	4	2	0	−1
	22	重要情報の授受を伴う取引先との契約書には、秘密保持条項を規定していますか？	4	2	0	−1
	23	クラウドサービスやウェブサイトの運用等で利用する外部サービスは、安全・信頼性を把握して選定していますか？	4	2	0	−1
	24	セキュリティ事故が発生した場合に備え、緊急時の体制整備や対応手順を作成するなど準備をしていますか？	4	2	0	−1
	25	情報セキュリティ対策（上記 1～24 など）をルール化し、従業員に明示していますか？	4	2	0	−1

※1 コンピュータウイルスを検出するためのデータベースファイル「パターンファイル」とも呼ばれます。
※2 重要情報とは営業秘密など事業に必要で組織にとって価値のある情報や顧客や、従業員の個人情報など管理責任を伴う情報のことです。

A 実施しているの合計点	B 一部実施しているの合計点	C わからないの合計点
点	点	マイナス(−) 点

診断の後は次ページ以降を読んで対策を検討してください。

A+B+C 合計 点

図 5-1 「5 分でできる！情報セキュリティ自社診断」の点数化と合計点の算出

[39] 独立行政法人 情報処理推進機構,「5 分でできる！情報セキュリティ自社診断」

自社診断の合計点は回答企業のサイバーセキュリティ対策のレベルを数値で示すものであり、また SECURITY ACTION 二つ星宣言に必要な診断項目である。合計点ごとのサイバーセキュリティ対策状況の評価は下図の通りである。

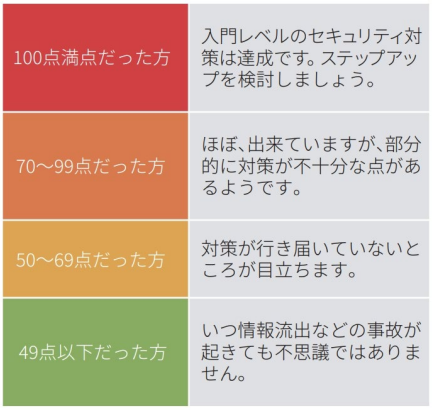

図 5-2 自社診断の合計点ごとのサイバーセキュリティ対策状況の評価

サイバーセキュリティ対策による効果と考えられる設問としては、サイバーインシデントによる被害状況に関する設問のほか、サイバーセキュリティ対策を行ったことにより得られる効果として、取引上におけるメリット（信頼の獲得）を示す設問や、セキュリティ体制整備や第三者認証の取得により社内のセキュリティ意識向上につながった（事業基盤の強化）を示す設問も選択した。

具体的にはサイバーインシデントによる被害状況に関しては、サイバーインシデントの発生有無（Q34）、サイバーインシデントによる被害（Q35）、サイバーインシデントによるサプライチェーンへの影響（Q36）、直近 3 期でのサイバーインシデントの被害額（Q39）とのクロス集計を行った。取引上におけるメリットについては、取引先からのセキュリティ要請応じたことが取引につながったか（Q49）とのクロス集計を行った。

5.2.1 「5 分でできる！情報セキュリティ自社診断」の合計点を軸とした効果の分析

Q80 の 25 項の回答結果を「5 分でできる！情報セキュリティ自社診断」で示された基準に沿って点数化し、それらの合計点を自社診断の総合的な指標として、各設問との関係性を分析した。分析は 3.3 で示す企業規模の定義に基づき、小規模企業者と中小企業（100 名以下）及び中小企業（101 名以上）に分けて行った。

分析の結果、企業の規模に関わらず、自社診断の合計点の高さと、サイバーインシデント被害の有無や影響の軽微さとの間に、一貫した関連性があることが分かった。このことから Q80 の 25 項目の設問、すなわち「5 分でできる！情報セキュリティ自社診断」の診断項目に示されたサイバーセキュリティ対策の実施はサイバーインシデント被害の低減に効果のある対策であると考えられる。

また、中小企業（100 名以下）及び中小企業（101 名以上）においては自社診断の合計点の高さが、取引先からのセキュリティ要請への対応状況や、それを取引上のメリットとして認識する度合いは、一貫して関連していることが読み取れたが、小規模企業者においては取引上のメリットとして認識する度合いについては同様の関連は読み取れなかった。このことから、企業規模が中小企業（100 名以下）及び中小企業（101 名以上）については、「5 分でできる！情報セキュリティ自社診断」の診断項目に示されたサイバーセキュリティ対策の実施が取引上におけるメリットに効果のある対策であると考えられる。

（1） 企業規模が中小企業（100 名以下）及び中小企業（101 名以上）の分析

ここでは企業規模が中小企業（100 名以下）及び中小企業（101 名以上）の分析結果を示す。

アンケート回答企業における中小企業（100 名以下）及び中小企業（101 名以上）の合計（1,416 件）の内、合計点が 70 点以上の企業は約 3 割（429 件）、69 点以下の企業は約 7 割（987 件）であった。

1） 自社診断の合計点とサイバーインシデントによる被害の関係

自社診断の合計点とサイバーインシデントの被害状況を示す設問（Q34、Q35、Q36、Q39）の回答結果との関連性を分析した。

分析の結果、2023 年度中の被害経験（Q34）では、自社診断の合計点が高いほど「被害にあっていない」との回答割合が高かった。同様に、インシデントによる影響（Q35）やサプライチェーンへの影響（Q36）においても、自社診断の合計点が高い企業ほど「特に無し」と回答する割合が高い傾向が見られた（サプライチェーンへの影響は、特に合計点 70 点以上と 69 点以下を分けた場合に顕著である）。さらに、インシデントによる被害額（Q39）の最高額と自社診断の合計点の間にも関連性が認められた。

これらの分析結果は、自社診断の合計点の高さと、サイバーインシデント被害の有無や影響の軽微さとの間に、一貫した関連性があることを示していると考えられる。

a. サイバーインシデントの被害経験

> Q34 貴社では 2023 年度（2023 年 4 月～2024 年 3 月）にサイバーインシデントの発生、もしくは発生が遭った可能性が高い経験はありましたか。 これらに遭った場合は、その内容を教えてください。 あてはまるものを下記よりすべてお選びください。（MA）

Q34 において「被害にあっていない」と回答した企業の割合は、自社診断の合計点が高いほど高くなる傾向が見られる。特に、自社診断の合計点が 70 点以上の企業群と 69 点以下の企業群とでは、その割合に約 10 ポイントの差が認められる。この結果は、自社診断の合計点の高さとサイバーインシデント被害経験の有無との間に関連性があることを示唆している。

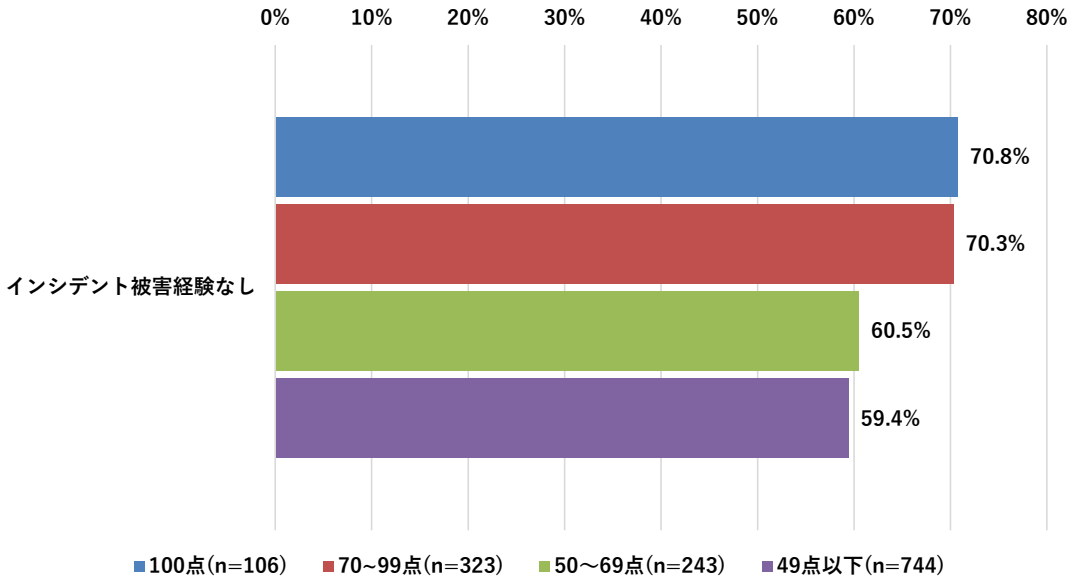

図 5-3 自社診断の合計点とサイバーインシデント被害経験の関係（中小企業（100 名以下）及び中小企業

（101 名以上））（n=1416）

b. サイバーインシデントによる影響

Q35.（Q34.で「被害にあっていない」以外のいずれかと回答された方について）貴社でサイバーインシデントによる影響で、生じた被害について教えてください。（MA）

Q34 で「被害にあっていない」以外の回答を選択した中小企業（100 名以下）及び中小企業（101 名以上）を対象とした分析では、自社診断の合計点が高い企業ほど、サイバーインシデントによる影響を「特になし」と回答する割合が高い傾向が認められた。これは、自社診断の合計点の高さとインシデントによる影響の有無（または軽微さ）との間に関連性があることを示す結果である。

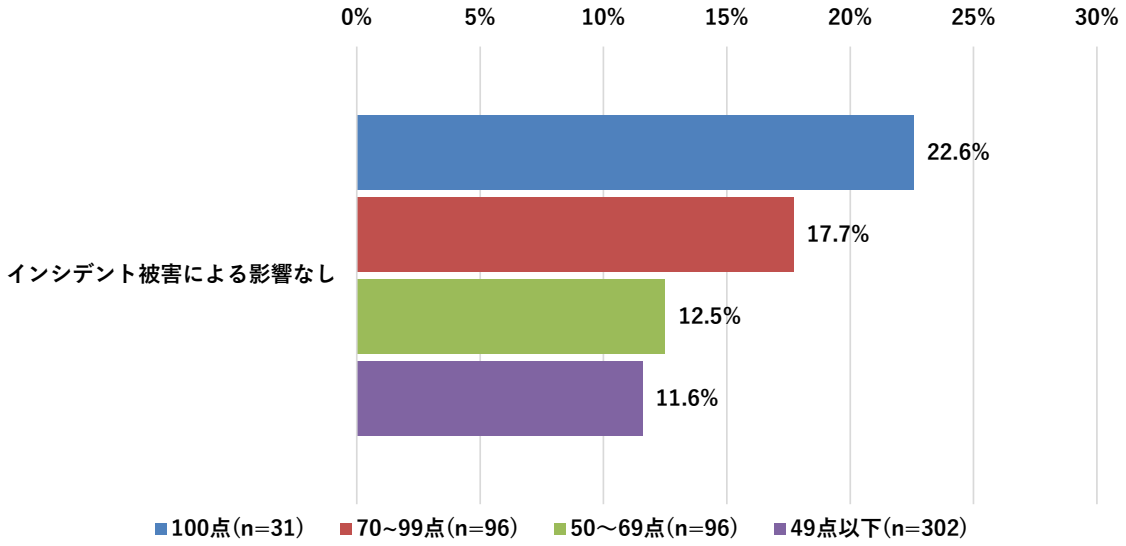

図 5-4 自社診断の合計点とサイバーインシデントによる影響の関係（中小企業（100 名以下）及び中小企業（101 名以上））(n=525)

c. インシデントによる被害額

Q39.（Q34.で「被害にあっていない」以外のいずれかと回答された方について）過去 3 期、サイバーインシデントの発生で生じた被害額の総額、サイバーインシデントの発生回数、復旧するまでに要した最大の期間について教えてください。（0 以上の半角数字で入力してください。）（FA）

自社診断の合計点が高いほど、インシデントの被害額の最大値が下がっていることが確認できる。

表 5-1 自社診断の合計点とインシデントによる被害額の関係中小企業（100 名以下）及び中小企業（101 名以上）（n=575）

自社診断の合計点	回答企業数	平均	最大値
100 点	31	約 39 万円	500 万円
70～99 点	96	約 162 万円	3000 万円
50～69 点	96	約 180 万円	8000万円
49 点以下	302	約 96 万円	1 億円

d. サプライチェーンへの影響

Q36.（Q34.で「被害にあっていない」以外のいずれかと回答された方について）サイバーインシデントにより貴社の取引先（サプライチェーン）に影響はありましたか。影響が及んだ場合はその内容について教えてください。あてはまるものを下記よりすべてお選びください。（MA）

自社診断の合計点が高いほど、サプライチェーンへの影響について特になしと回答している企業の割合が高くなっていることが分かる。特に合計点 70 点以上と 69 点以下を分けた場合、その違いは顕著に読み取れる。

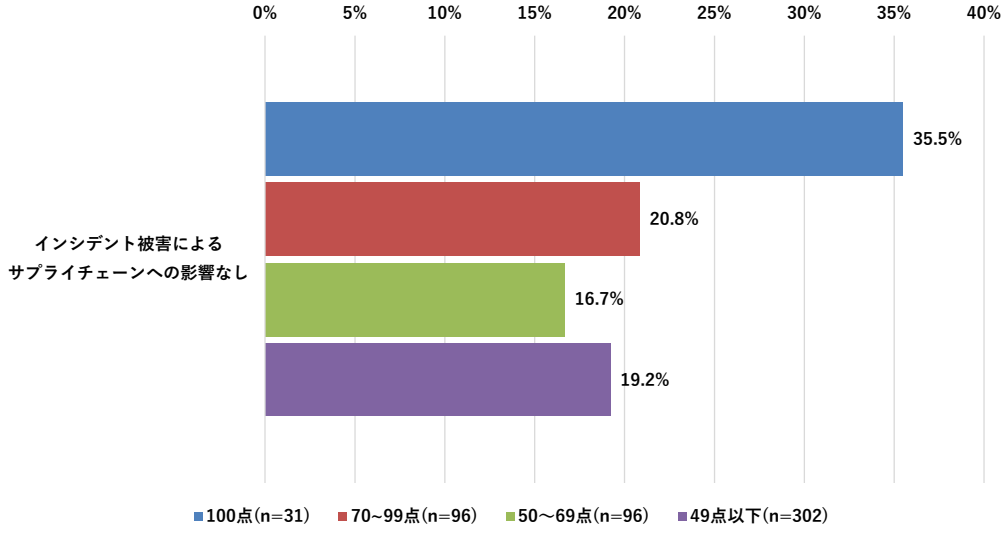

図 5-5 自社診断の合計点とサプライチェーンへの影響の関係中小企業（100 名以下）及び中小企業（101 名以上）（n=1416）

2）自社診断の合計点と取引上におけるメリットの関係

自社診断の合計点と取引上におけるメリットを示す設問（Q46、Q48、Q49）の回答結果との関連性を分析した。

分析の結果、自社診断の合計点と、取引先（発注元）からのサイバーセキュリティ対策要請への対応状況、およびその取引への影響認識との間に関連が見られた。まず、合計点が高い企業ほど、取引先（発注元）から対策要請を受けた経験が多く、かつその要請に応じたと回答する割合が高い傾向が認められた。さらに、合計点が高い企業ほど、要請された対策の実施が取引継続または獲得の要因となったと認識している割合も高いことが示された。

これらの結果は、自社診断の合計点の高さが、取引先からのセキュリティ要請への対応状況や、それを取引上のメリットとして認識する度合いと、一貫して関連していることを示唆するものである。

a. 取引におけるセキュリティ要請

Q46. 貴社は販売先（発注元企業）から貴社への情報セキュリティに関する要請を受けた経験はありますか。（SA）

自社診断の合計点が 70 点以上の企業はセキュリティ要請経験があると回答している割合が高いことが分かる。

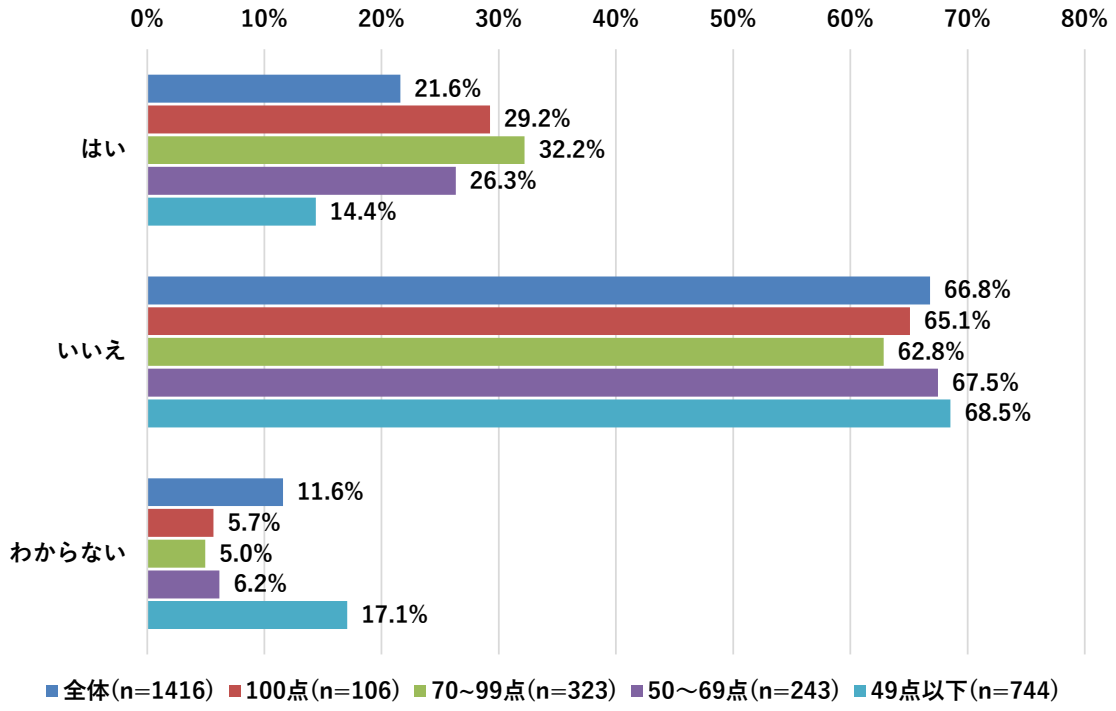

図 5-6 自社診断の合計点とセキュリティ要請経験の有無の関係中小企業(100 名以下)及び中小企業(101 名以上)(n=1416)

Q48.(Q46.で「はい」と回答された方について)販売先(発注元企業)から貴社への情報セキュリティに関する要請に対して、貴社の行ったセキュリティ対策の具体的な内容について教えてください。またどの程度の費用が掛かりましたか。(SA)

また、セキュリティ要請に応じたと回答している割合は自社診断の合計点が高い方が多いことが分かる。

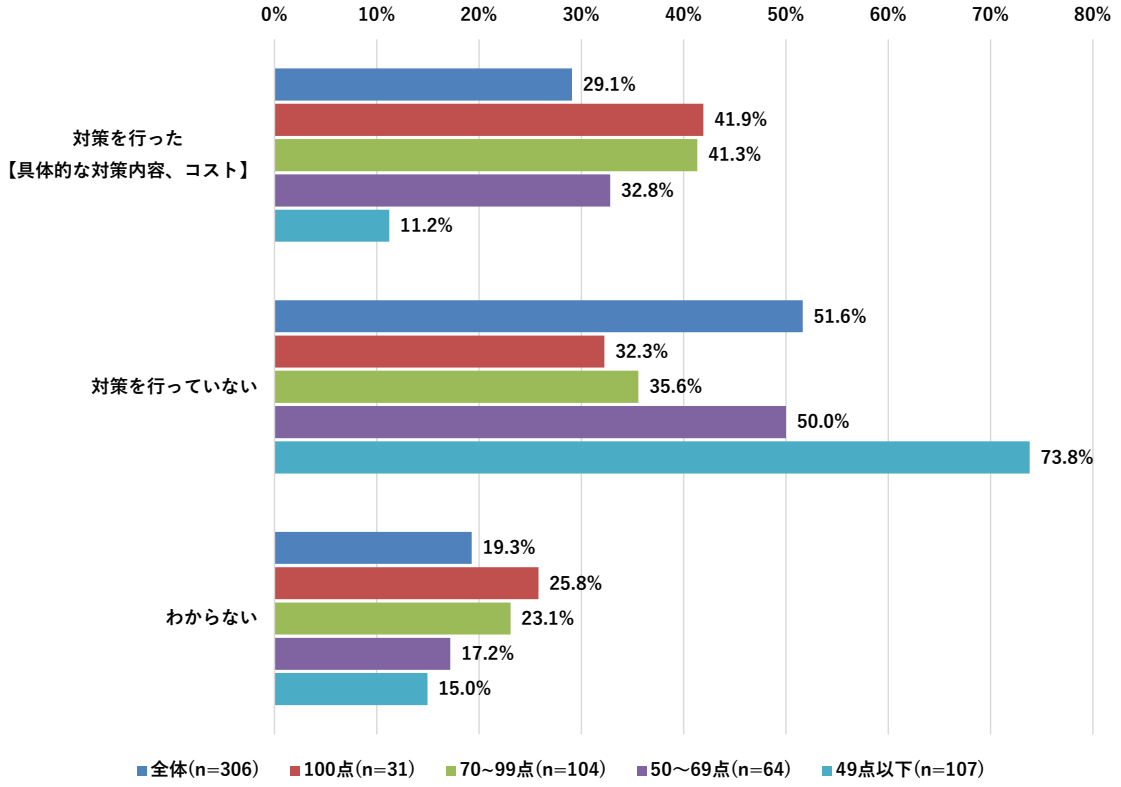

図 5-7 自社診断の合計点とセキュリティ要請への対応の関係中小企業(100 名以下)及び中小企業(101 名以上)(n=306)

b. セキュリティ要請応じたことが取引につながったか

Q49.(Q46.で「はい」と回答された方について)貴社は販売先(発注元企業)から要請された情報セキュリティ対策を行ったことが取引先との取引につながった大きな要因だと思いますか。(SA)

自社診断の合計点が高い企業ほど、はい(取引につながった)と回答している割合が高い傾向が読み取れる。

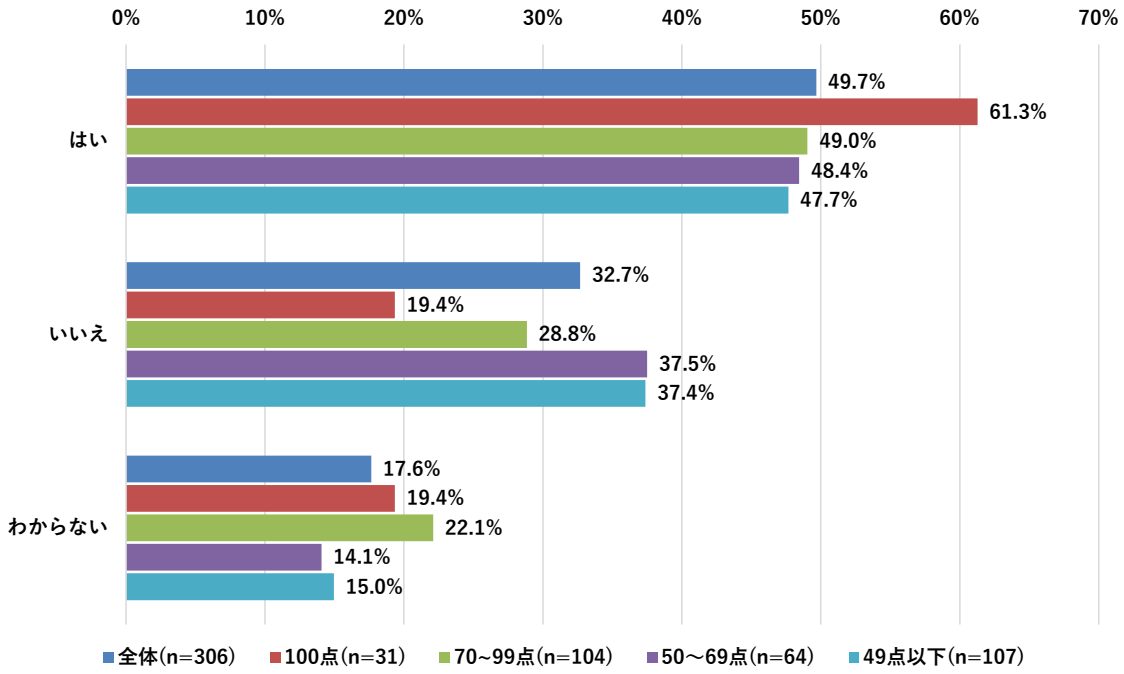

図 5-8 自社診断の合計点とセキュリティ要請に応じたことが取引につながったかの関係中小企業(100名以下)及び中小企業(101 名以上)(n=306)

（2） 企業規模が小規模企業者の分析

ここでは小規模企業者についての分析結果を示す。

アンケート回答企業における小規模企業者（2,775 件）の内、70 点以上の企業は約 2 割弱（485 件）、69 点以下の企業は約 8 割強（2,290 件）であった。中小企業（100 名以下）及び中小企業（101 名以上）の企業群と比べ、70 点以上の企業の割合が少ないため自社診断の得点分布を 70 点以上と 69 点以下の2つの企業群に分けてクロス集計を行っている。

1） 自社診断の合計点とサイバーインシデントによる被害の関係

自社診断の合計点とサイバーインシデントの被害状況を示す設問（Q34、Q35、Q36、Q39）の回答結果との関連性を分析した。

分析の結果、2023 年度中の被害経験（Q34）では、自社診断の合計点が高いほど「被害にあっていない」との回答割合が高かった。同様に、インシデントによる影響（Q35）やサプライチェーンへの影響（Q36）においても、自社診断の合計点が高い企業ほど「特に無し」と回答する割合が高い傾向が見られた。さらに、インシデントによる被害額（Q39）の最高額と自社診断の自社診断の合計点の間にも関連性が認められた。

これらの分析結果は、自社診断の合計点の高さと、サイバーインシデント被害の有無や影響の軽微さとの間に、一貫した関連性があることを示していると考えられる。

a. サイバーインシデント被害経験

> Q34 貴社では 2023 年度（2023 年 4 月～2024 年 3 月）にサイバーインシデントの発生、もしくは発生が遭った可能性が高い経験はありましたか。 これらに遭った場合は、その内容を教えてください。 あてはまるものを下記よりすべてお選びください。（MA）

Q34 において「被害にあっていない」と回答した企業の割合は、自社診断の合計点が高いほど高くなる傾向が見られる。インシデントの発生経験について、被害に遭っていない割合が 70 点以上の企業が 87.8%に対して、69 点以下では 82.9%と少なくなっている。

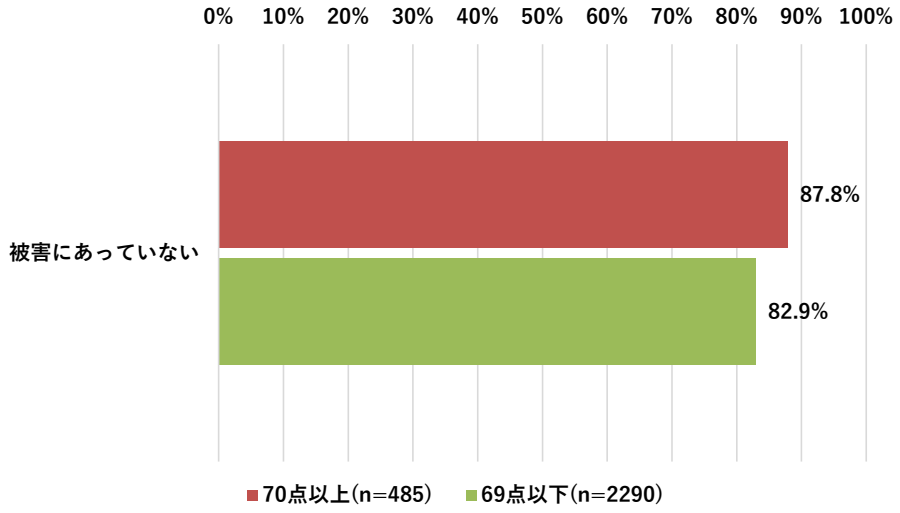

図 5-9 自社診断の合計点とサイバーインシデント被害経験の関係（小規模企業者）（n=2775）

b. サイバーインシデントによる影響

Q35.（Q34.で「被害にあっていない」以外のいずれかと回答された方について）貴社でサイバーインシデントによる影響で、生じた被害について教えてください。（MA）

Q34 で「被害にあっていない」以外の回答を選択した小規模企業者を対象とした分析では、サイバーインシデントによる被害に遭った小規模企業者（450 件）の内、影響で「特になし」と回答している割合が 70 点以上で 32.2%に対して、69 点以下では 23%と少なくなっており、自社診断の合計点の高さとインシデントによる影響の有無（または軽微さ）との間に関連性があることを示す結果である。

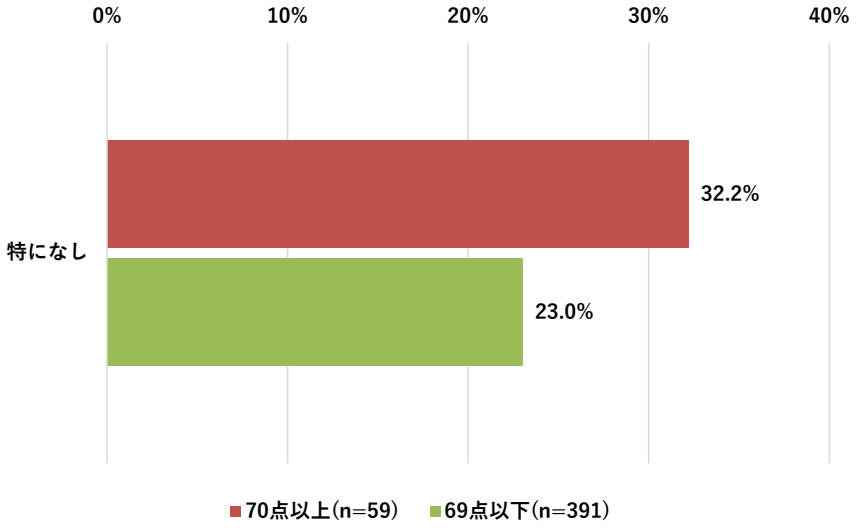

図 5-10 自社診断の合計点とサイバーインシデントによる影響の関係（小規模企業者）(n=450)

c. インシデントによる被害額

Q39.（Q34.で「被害にあっていない」以外のいずれかと回答された方について）過去 3 期、サイバーインシデントの発生で生じた被害額の総額、サイバーインシデントの発生回数、復旧するまでに要した最大の期間について教えてください。（0 以上の半角数字で入力してください。）（FA）

自社診断の合計点とインシデントによる被害額の関係を下表に示す。被害額も 70 点以上は平均が約 10 万円に対して、69 点以下は約 20 万円と高くなっている。

表 5-2 自社診断の合計点とインシデントによる被害の関係（n=450）

自社診断の合計点	回答企業数	平均	最大値
70 点以上	59	約 10 万円	100 万円
69 点以下	391	約 20 万円	5000万円

d. サプライチェーンへの影響

Q36.（Q34.で「被害にあっていない」以外のいずれかと回答された方について）サイバーインシデントにより貴社の取引先（サプライチェーン）に影響はありましたか。影響が及んだ場合はその内容について教えてください。あてはまるものを下記よりすべてお選びください。（MA）

自社診断の合計点が高いほど、サプライチェーンへの影響が「特になし」と回答している企業の割合が

高くなっていることが分かる。具体的には、70 点以上で 54.2%に対して、69 点以下では 39.1%と少なくなっている。

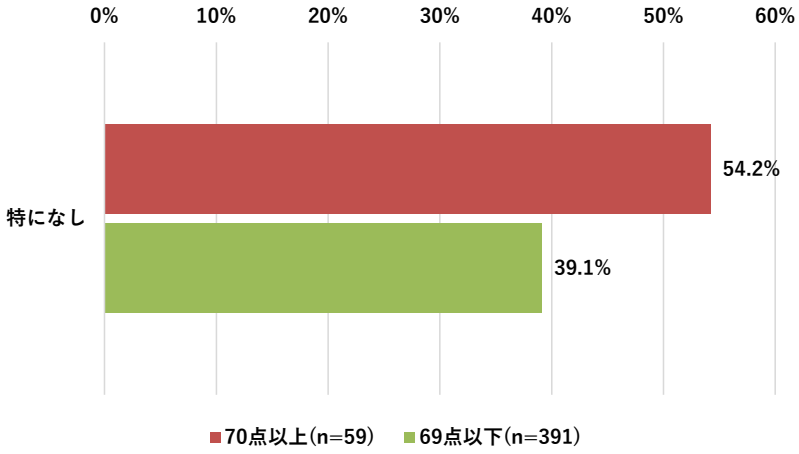

図 5-11 自社診断の合計点とサプライチェーンへの影響の関係(小規模企業者)(n=450)

2) 自社診断の合計点と取引上におけるメリットとの関係

自社診断の合計点と取引上におけるメリットを示す設問(Q46、Q48、Q49)の回答結果との関連性を分析した。

分析の結果、自社診断の合計点と、取引先(発注元)からのサイバーセキュリティ対策要請への対応状況、およびその取引への影響認識との間に関連は、中小企業(100 名以下)及び中小企業(101 名以上)と異なる傾向が見られた。まず、合計点が高い企業ほど、取引先(発注元)から対策要請を受けた経験が多く、かつその要請に応じたと回答する割合が高い傾向が認められた。一方で、合計点が高い企業ほど、要請された対策の実施が取引継続または獲得の要因となったと認識している割合も低いことが示された。

a. 取引におけるセキュリティ要請

Q46. 貴社は販売先(発注元企業)から貴社への情報セキュリティに関する要請を受けた経験はありますか。(SA)

自社診断の合計点が 70 点以上の企業では約 17%、69 点以下の企業では約 5%の企業がセキュリティ対策の要請を受けた。

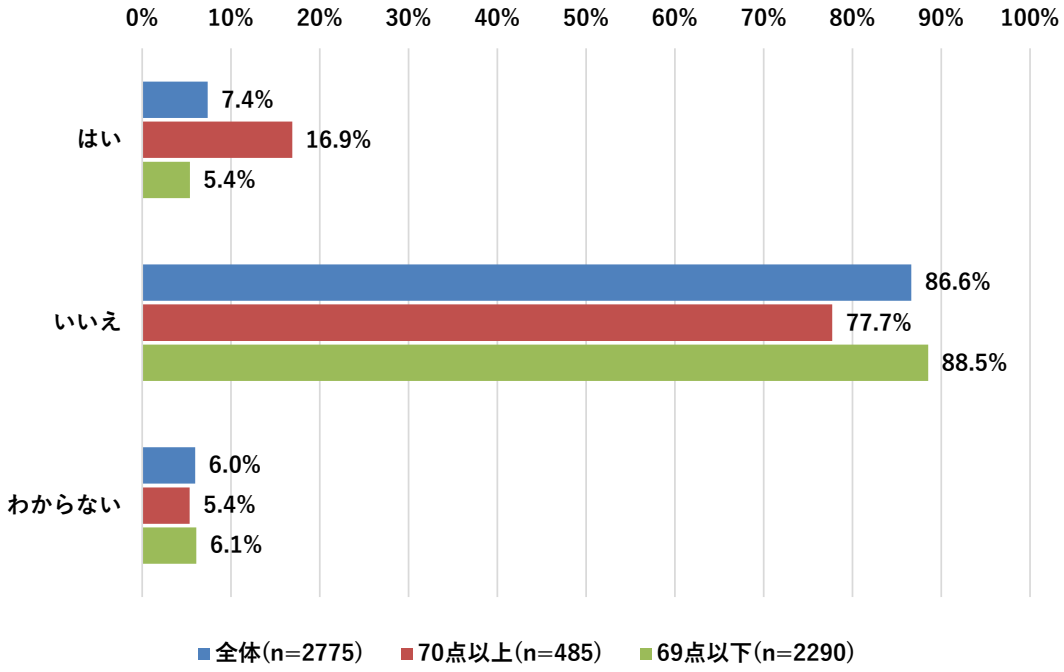

図 5-12 自社診断の合計点とセキュリティ要請経験の有無の関係(小規模企業者)(n=2775)

Q48.(Q46.で「はい」と回答された方について)販売先(発注元企業)から貴社への情報セキュリティに関する要請に対して、貴社の行ったセキュリティ対策の具体的な内容について教えてください。またどの程度の費用が掛かりましたか。(SA)

70 点以上の企業では約30%以上がセキュリティ要請に応じた。69 点以下の企業では約17%となった。

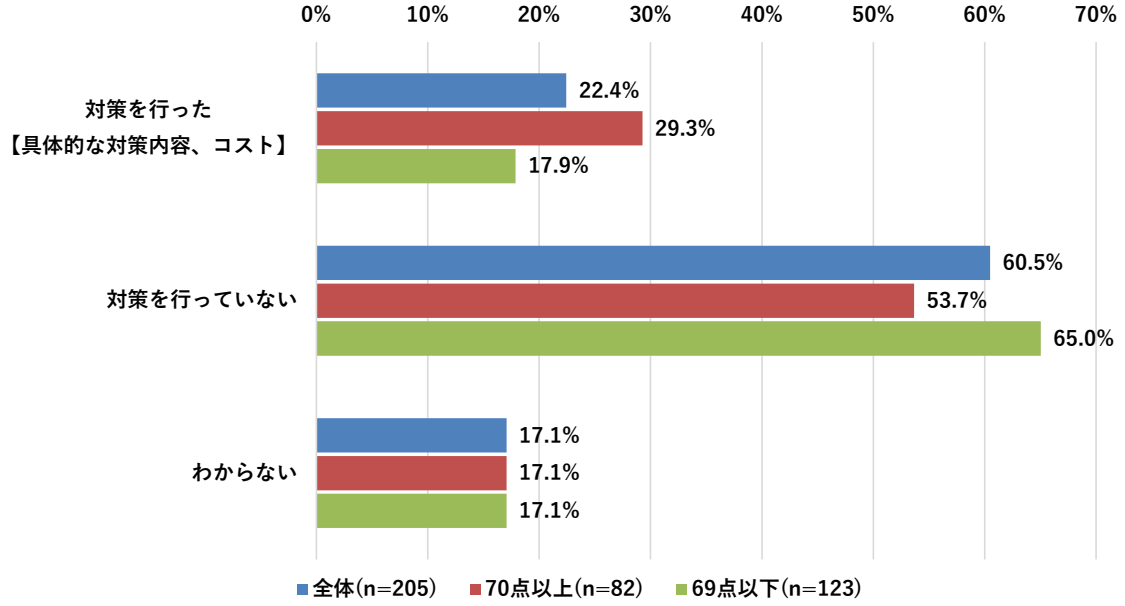

図 5-13 自社診断の合計点とセキュリティ要請への対応の関係(小規模企業者)(n=205)

b. セキュリティ要請応じたことが取引につながったか

Q49.（Q46.で「はい」と回答された方について）貴社は販売先（発注元企業）から要請された情報セキュリティ対策を行ったことが取引先との取引につながった大きな要因だと思いますか。（SA）

自社診断の合計点が高いほど、セキュリティ要請に応じたことが取引につながったとの回答割合が低くなっていることが分かった。

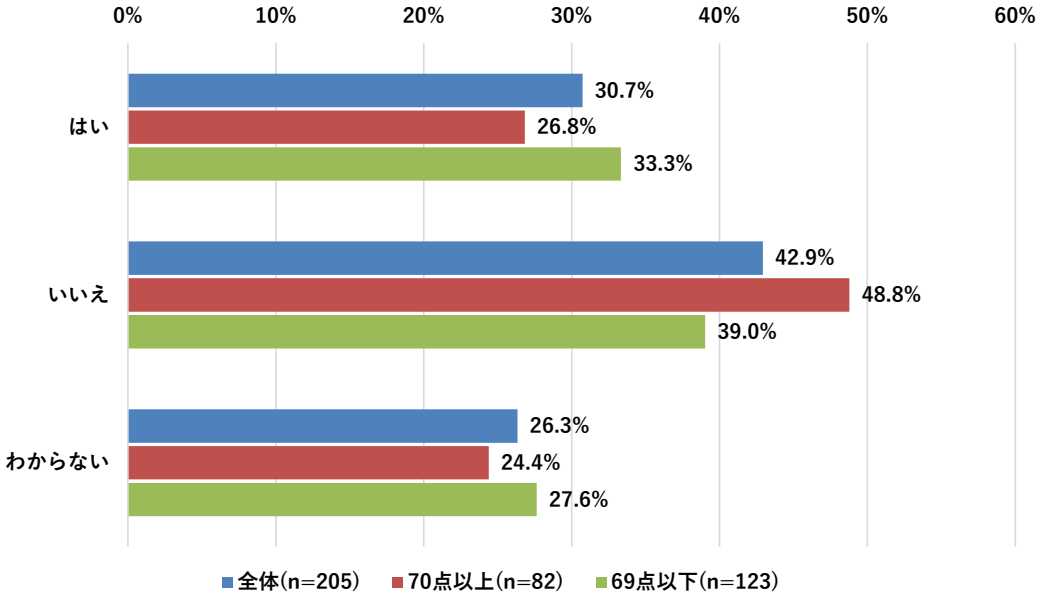

図 5-14 自社診断の合計点とセキュリティ要請応じたことが取引につながったかの関係（小規模企業者）（n=205）

5.2.2 第三者評価制度の取得状況を軸とした効果の分析

アンケート調査結果を元に、ISMS 評価制度および P マーク取得による効果について分析を行った。分析は ISMS 評価制度取得および P マーク取得に関する設問（Q77）と企業規模、業種、セキュリティ対策に期待する効果、サイバーインシデントの発生などの設問とのクロス集計を行い、各評価制度を取得している企業群（導入済）と取得していない企業群（導入無）の傾向の違いおよび関係性の有無を評価することで行った。

分析の結果、第三者評価制度の取得有無によりサイバーインシデントの被害経験、被害の大きさ（内容、被害額）、サプライチェーンへの影響の低減に関して関係性が見られなかった。第三者評価制度を取得していない企業ではセキュリティ体制が整っておらず、サイバーインシデントとして認識される機会が少ないことが考えられる。

一方、第三者評価制度の取得により取引上におけるメリットが見られた。ISMS を取得している企業では約 5 倍の割合で取引先からサイバーセキュリティに関する要請経験があり、要請に応じた割合が約 1.5 倍、要請に応じたことで取引につながったと感じた企業が約 2.5 倍存在した。P マークを取得している企業では約 3 倍の割合でサイバーセキュリティ要請経験があり、要請に応じた割合が約 1.2 倍、要請に応じたことで取引につながったと感じた企業が約 2 倍存在した。

これらのことから、サイバーセキュリティ対策に関する第三者評価制度の取得は、企業の規模・業種に関わらず、取引上におけるメリットに効果のある対策であると考えられる。

（1） ISMS 評価制度の取得による効果の分析

アンケート調査結果を元に、ISMS 取得による効果について分析を行った。分析は ISMS 取得に関する設問（Q77）と企業規模、業種、取引におけるリスク認識および取引上のメリットに関する設問とのクロス集計を行い、 ISMS を取得している企業と取得していない企業の傾向の違いおよび関係性の有無を評価することで行った。

1） ISMS 取得状況

a. ISMS 取得状況と企業規模の関係

全体としての導入率は約 7%となっている。企業規模の大きさに応じて取得率が増えていることが明らかになった。

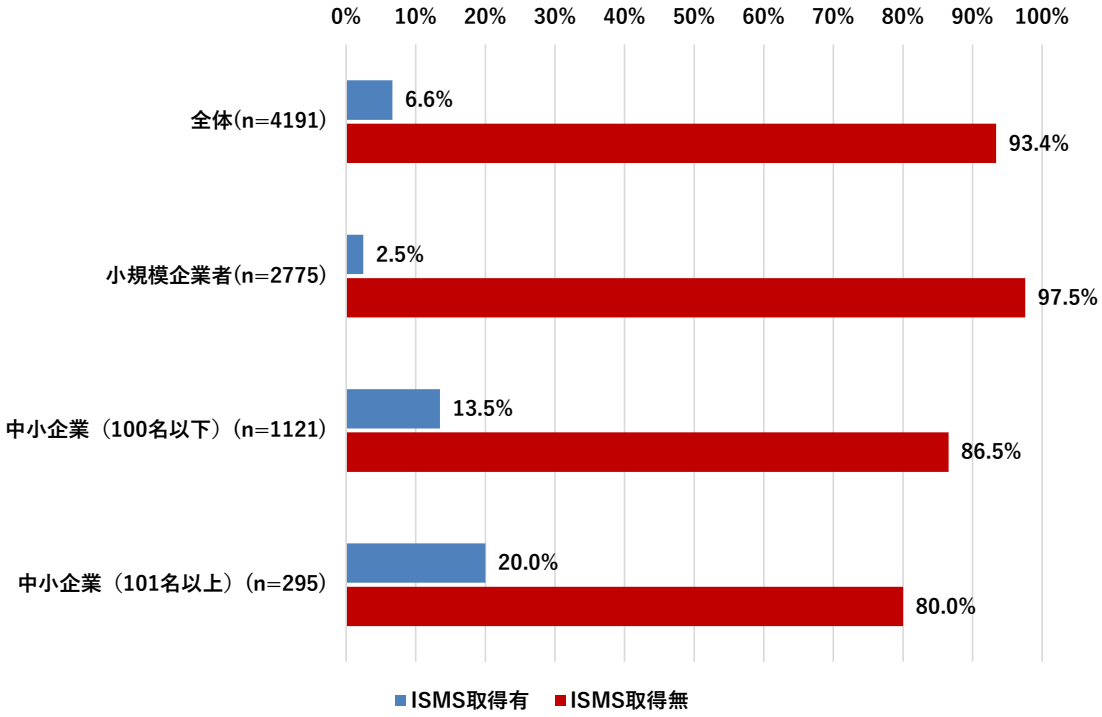

図 5-15 企業規模別の ISMS 取得状況(n=4191)

b. ISMS 取得状況と業種の関係性

業種では製造業、情報通信業、複合サービス業が取得している割合が高く、10-15%となった。

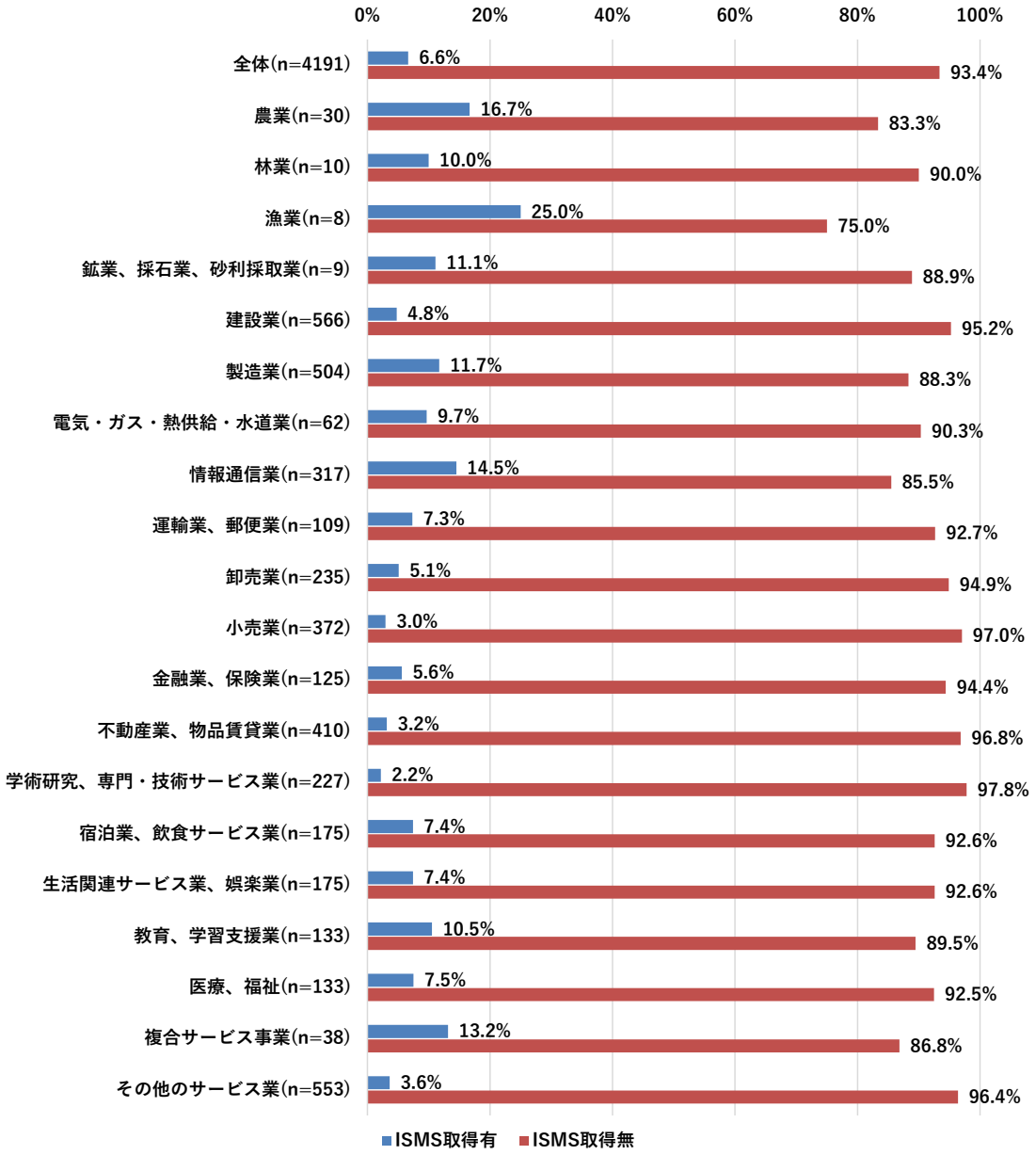

図 5-16 業種別の ISMS 取得状況(n=4191)

c. ISMS 取得状況とセキュリティ対策に期待する効果

セキュリティ対策に期待する効果として、ISMS を取得している企業では「ISMS・プライバシーマーク等の認証取得」が最も多く、次いで「高度な情報管理が求められる新規事業の実現」、「データの棚卸等による業務効率化の実現」である。ISMS を取得していない企業では「その他」を除き、「助成金・補助金の獲得」が最も多い。

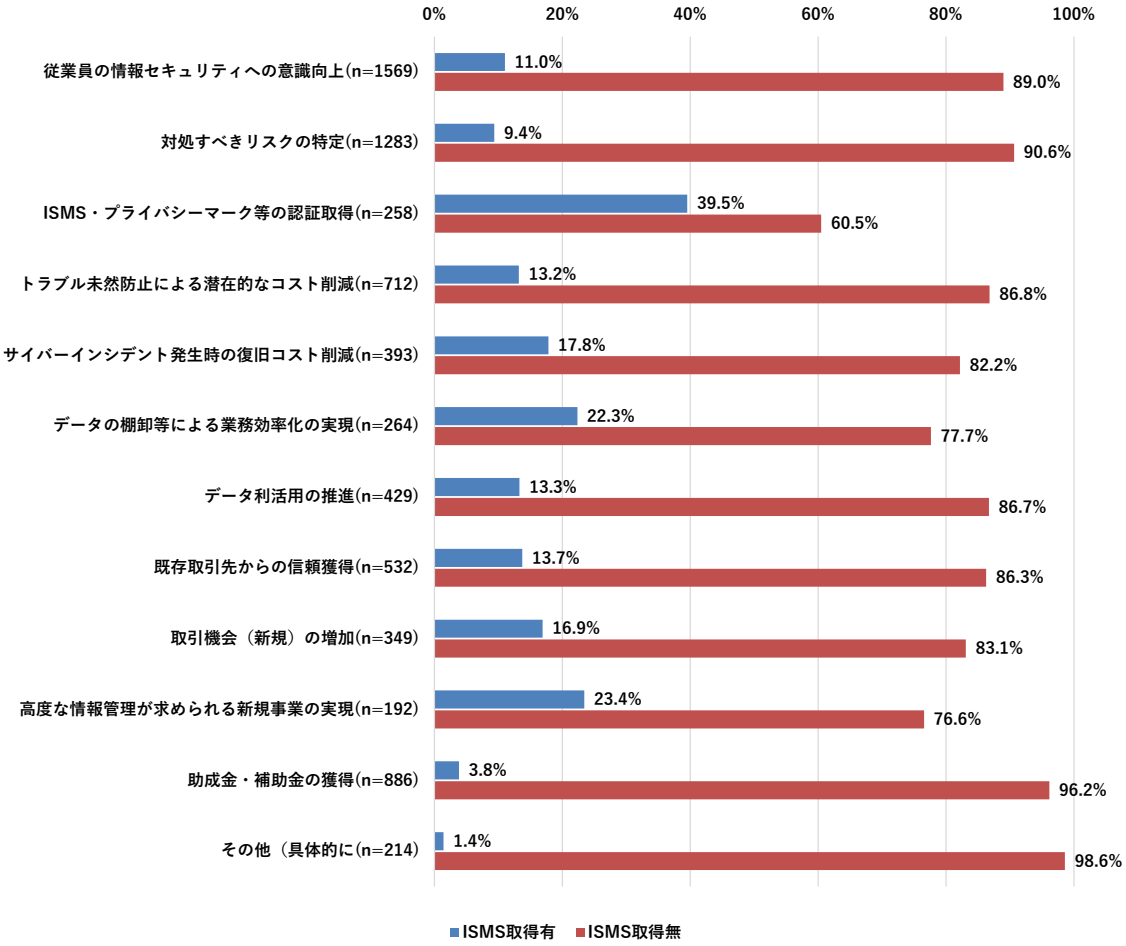

図 5-17 ISMS 取得状況とセキュリティ対策に期待する効果(n=4191)

d. ISMS 取得状況と取引上のリスク認識

ISMS を取得している企業では約 90%の企業、ISMS を取得していない企業では約60%の企業で取引上におけるリスク認識がなされている。

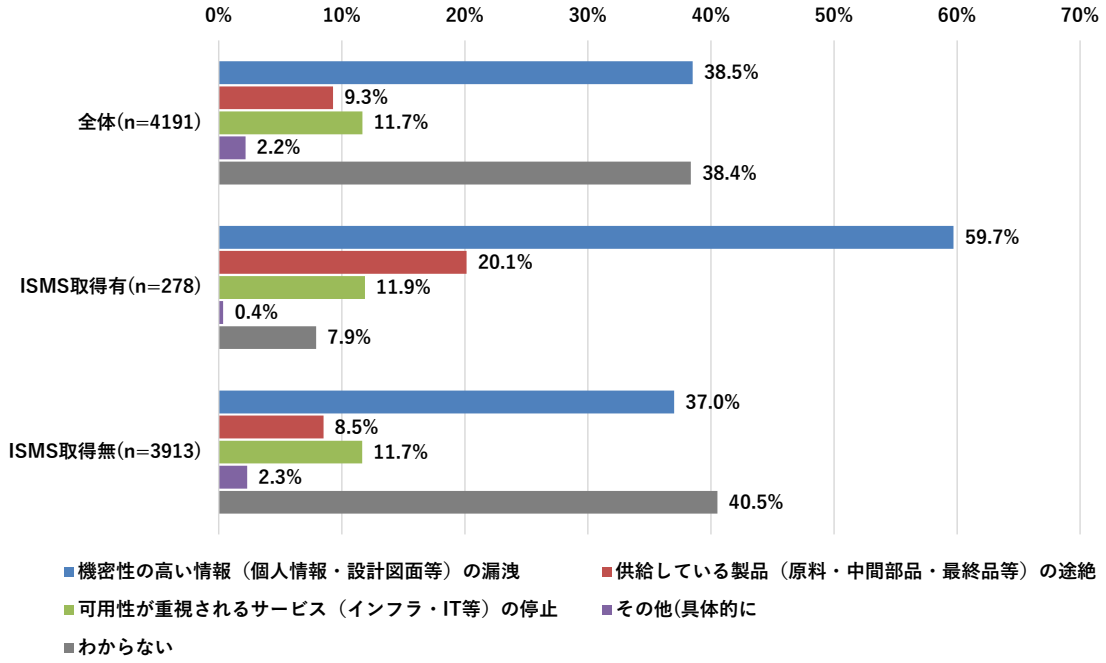

図 5-18 ISMS 取得状況と取引上のリスク認識(n=4191)

2）取引上におけるメリットに関する分析

a. ISMS 取得状況と取引におけるセキュリティ要請

ISMS 取得している企業では 50%の企業、ISMS 取得していない企業では約 10%の企業でセキュリティ対策の要請を受けた。(取得有無で約 5 倍)セキュリティ要請に応じた割合に関しては ISMS 取得を行っている企業の方が約 1.5 倍高かった。(取得有無で約 1.5 倍)

セキュリティ要請に応じたことが取引につながったと回答した企業が ISMS 取得している企業の方が約 2.5 倍高かった(取得有無で約 2.5 倍)

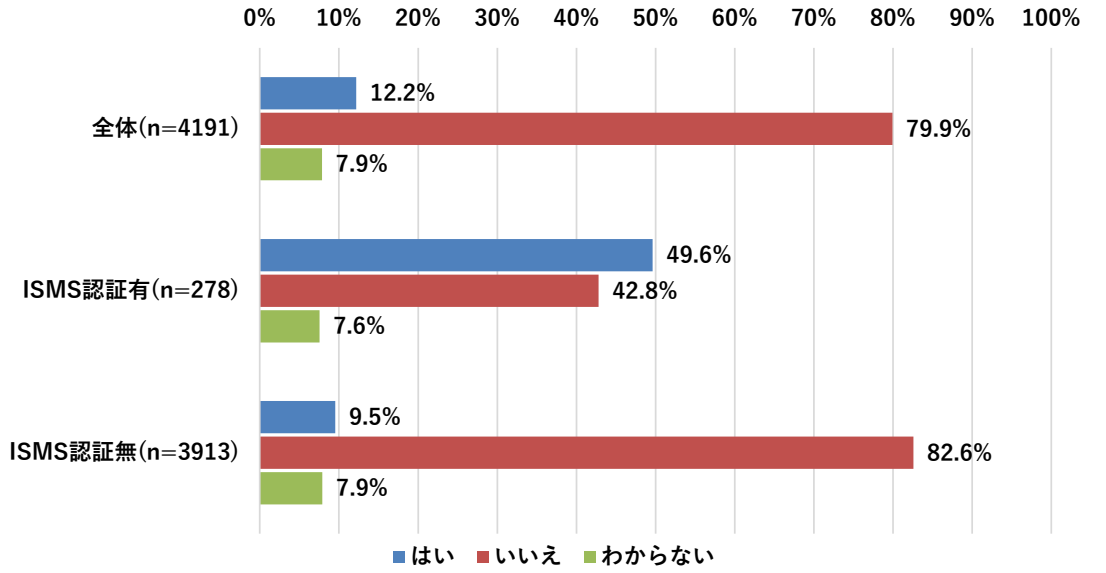

図 5-19 ISMS 取得状況とセキュリティ要請の有無の関係(n=4191)

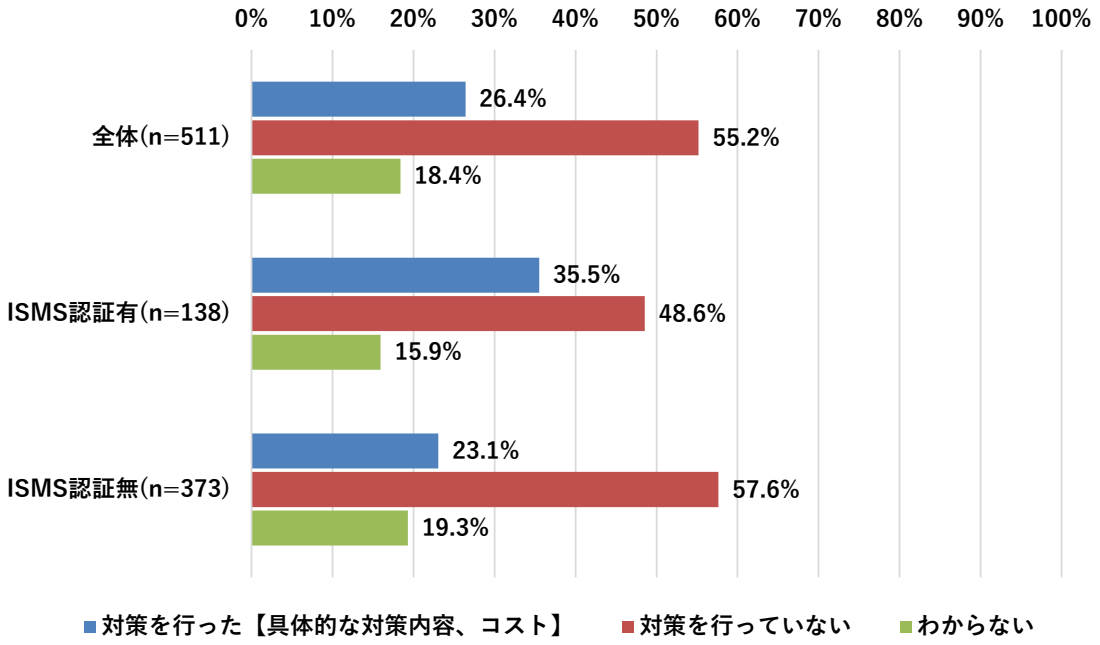

図 5-20 ISMS 取得状況とセキュリティ要請への対応の関係(n=511)

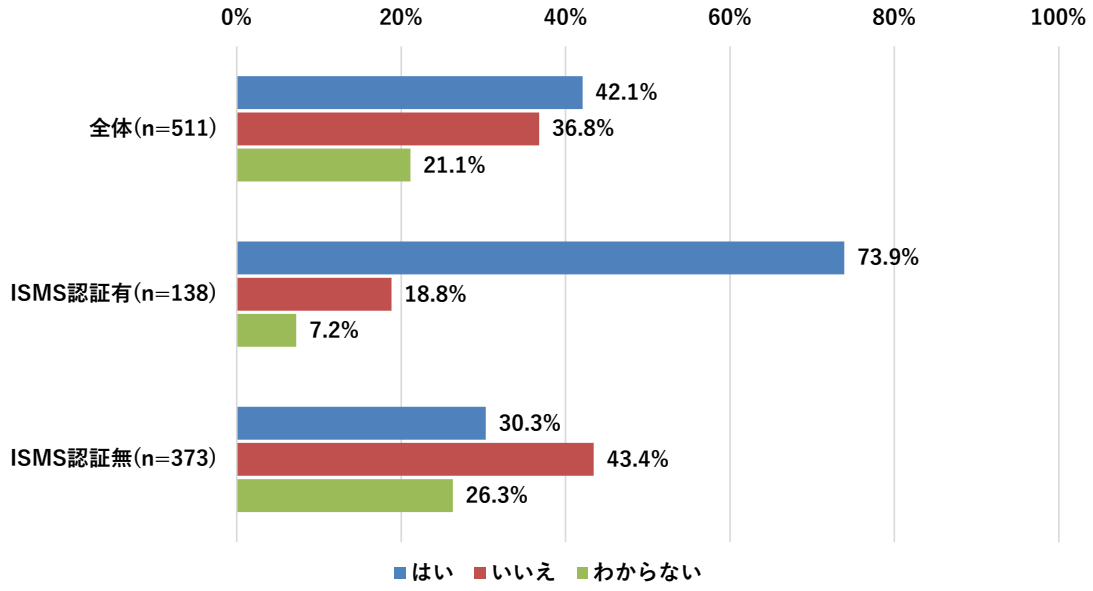

図 5-21 ISMS 取得状況セキュリティ要請応じたことが取引につながったかの関係(n=511)

(2) P マーク取得による効果の分析

アンケート調査結果を元に、P マーク取得による効果について分析を行った。分析は P マーク取得に関する設問(Q77)と企業規模、業種、取引におけるリスク認識および取引上のメリットに関する設問とのクロス集計を行い、P マークを取得している企業と取得していない企業の傾向の違いおよび関係性の有無を評価することで行った。

1) P マーク取得状況

a. P マーク取得状況と企業規模の関係性

全体としての導入率は約 10%となっている。企業規模の大きさに応じて取得率が増えている。

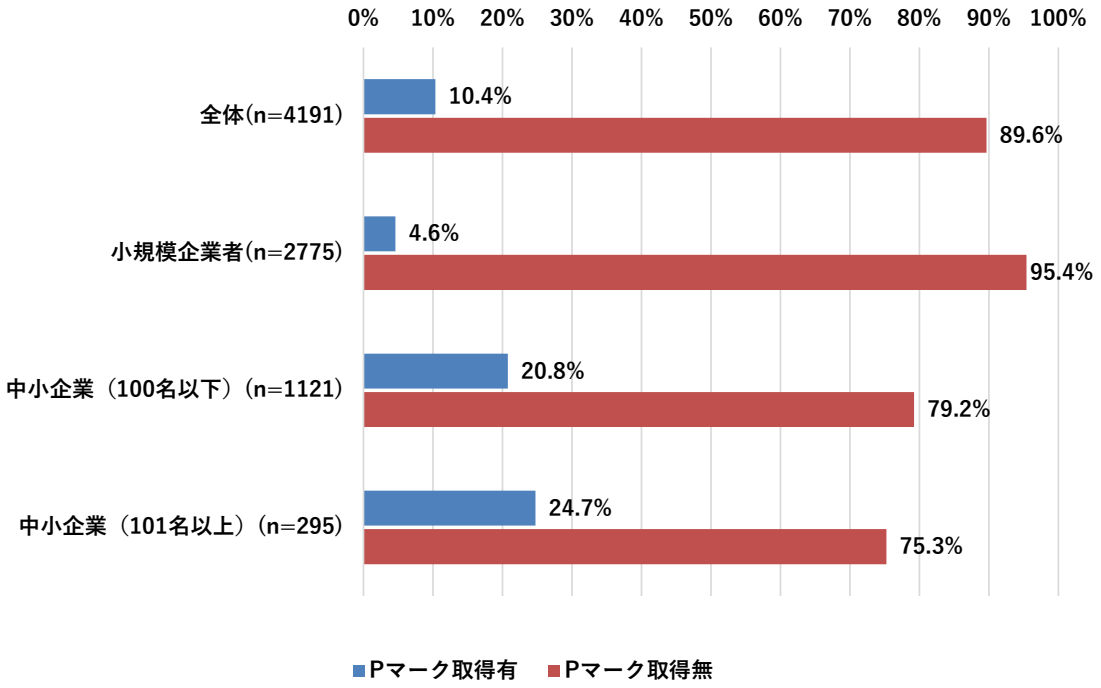

図 5-22 企業規模別の P マーク取得状況(n=4191)

b. P マークの導入状況と業種の関係性

P マークを取得している業種では農業、製造業、情報通信業、運輸業、郵便業、医療、福祉で多く、15-20%程度となった。なお、「林業」、「漁業」、「鉱業、採石業、砂利採取業」は回答企業数が少ないため分析から除外している。

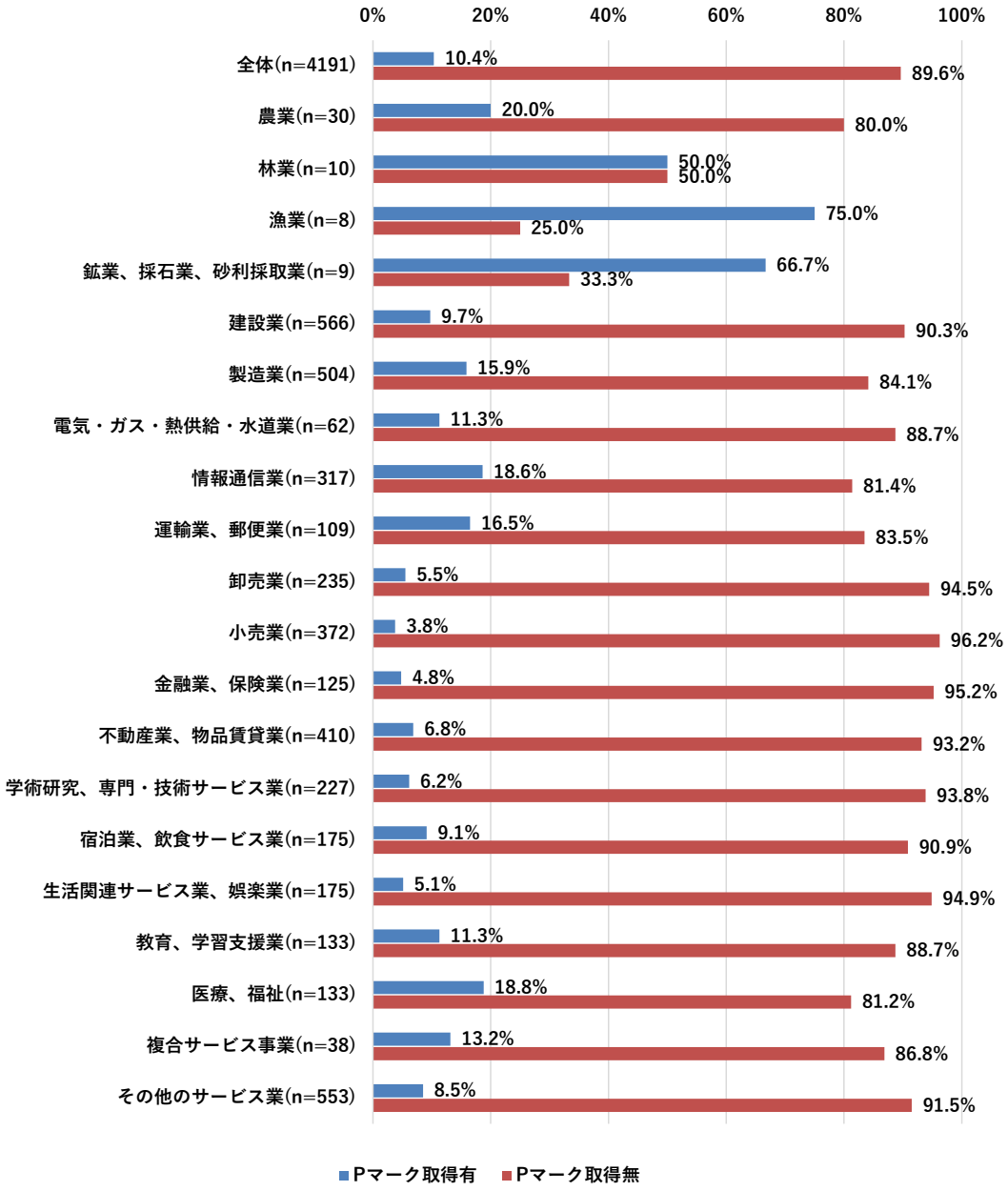

図 5-23 業種別の P マーク取得状況(n=4191)

c. P マーク取得状況と取引上のリスク認識

P マークを取得している企業では約 90%の企業、P マーク取得していない企業では約60%の企業で取引上におけるリスク認識がある。

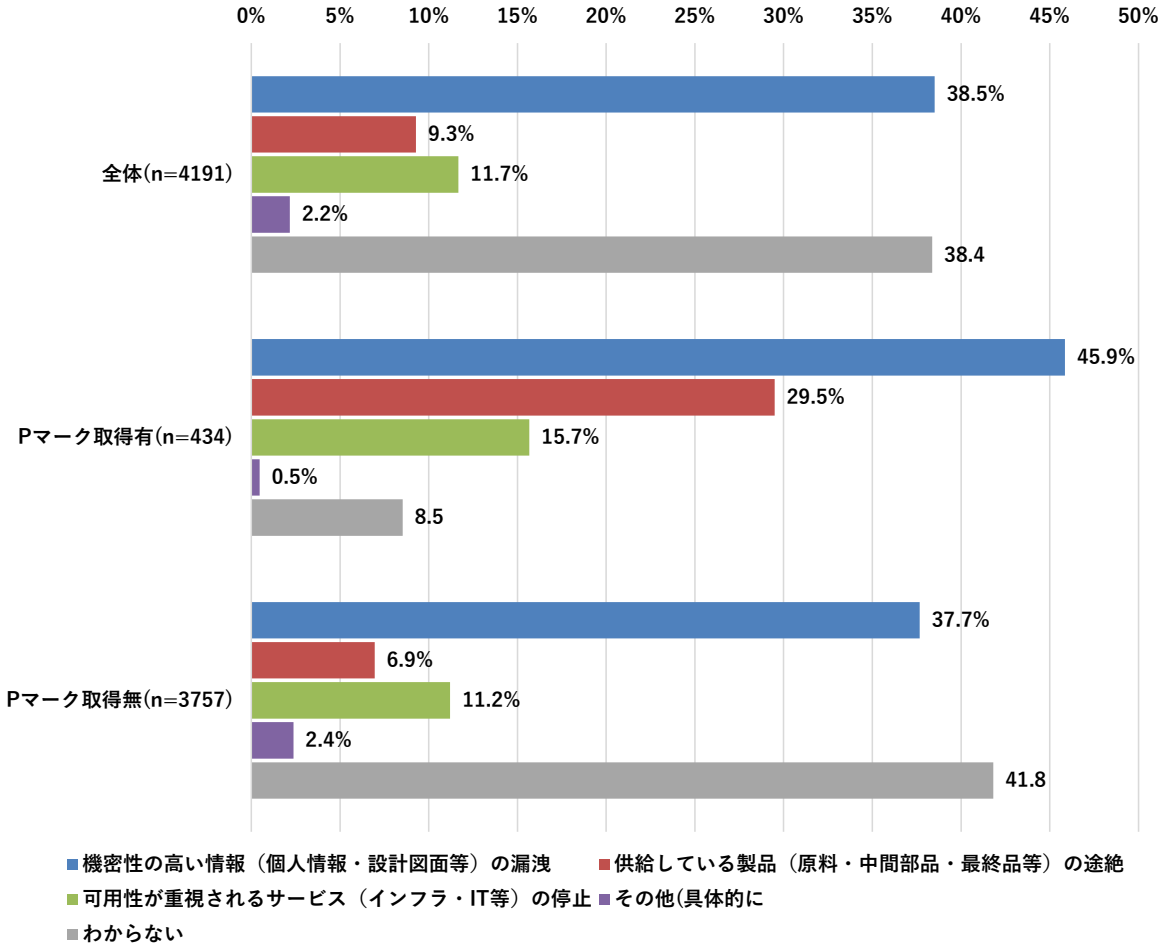

図 5-24 P マーク取得状況と取引上のリスク認識(n=4191)

2）取引上のメリットに関する分析

a. P マーク取得状況と取引におけるセキュリティ要請

P マーク取得している企業では 30%の企業、P マーク取得していない企業では約 10%の企業でセキュリティ対策の要請を受けた。セキュリティ要請に応じた割合に関しては P マーク取得を行っている企業の方が約 1.2 倍高かった。(取得有無で約 1.2 倍)セキュリティ要請に応じたことが取引につながったと回答した企業の割合は P マーク取得している企業の方が約 2 倍高かった(取得有無で約 2 倍)

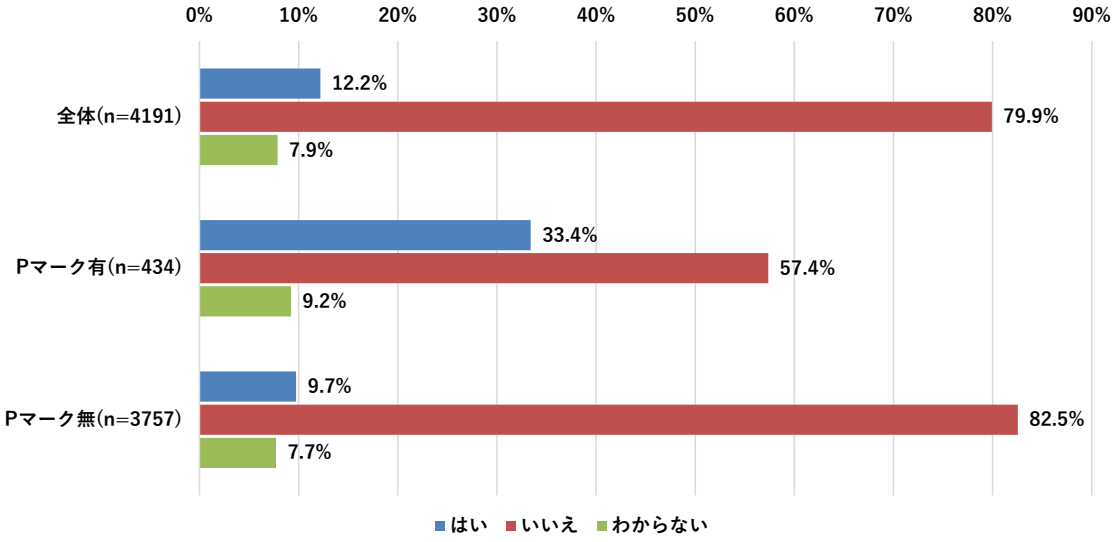

図 5-25 P マーク取得状況とセキュリティ要請経験の有無の関係(n=4191)

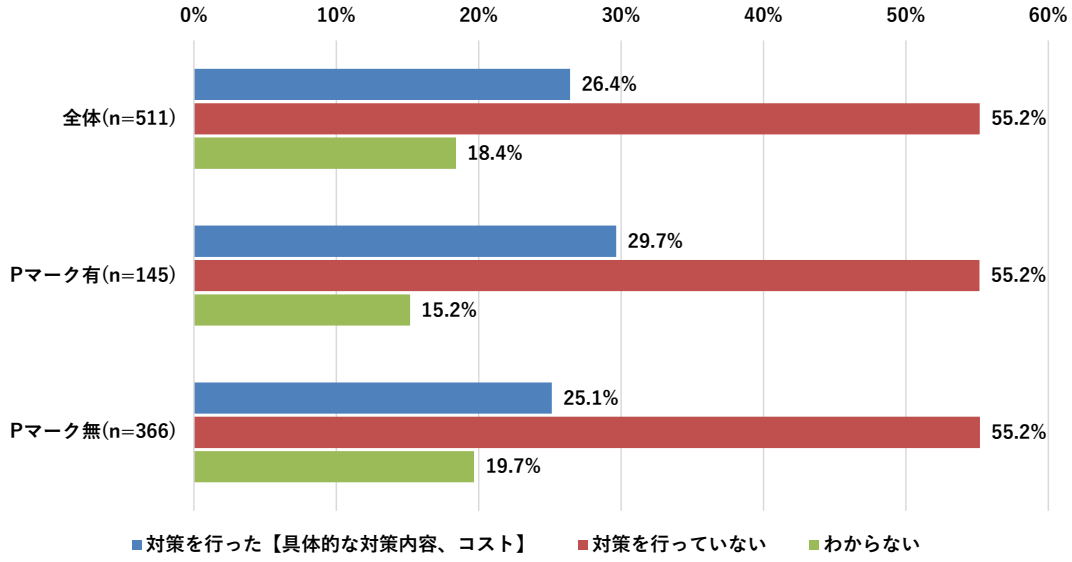

図 5-26 P マーク取得状況とセキュリティ要請への対応の関係 (n=511)

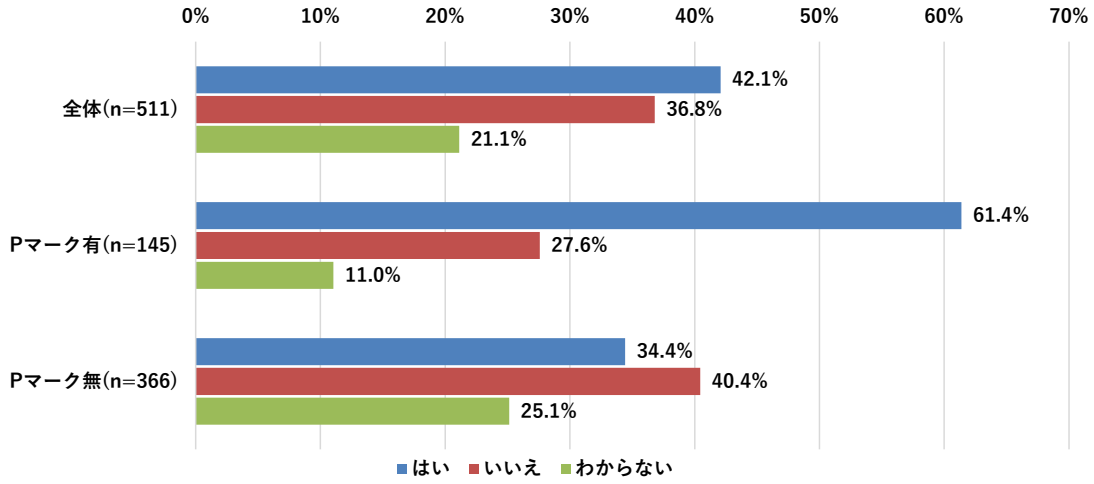

図 5-27 P マーク取得状況とセキュリティ要請応じたことが取引につながったかの関係(n=511)

5.2.3 セキュリティ体制整備による効果の分析

アンケート調査結果を元に、セキュリティ体制整備による効果について分析を行った。設問 Q22 の回答が「1. 専門部署(担当者)がある」と「2. 兼務だが、担当者が任命されている」である企業をセキュリティ体制が整備されている企業とした。

分析の結果、セキュリティ体制整備有無によりインシデントの被害経験、被害の大きさ(内容、被害額)、サプライチェーンへの影響の低減に関しては、効果が見られなかった。セキュリティ体制が整っておらず、インシデントとして認識される機会が少ないことが考えられる。

一方で、セキュリティ体制の整備により取引におけるメリットが見られた。セキュリティ体制整備を行っている企業では約 5～6 倍の割合でセキュリティ要請経験があり、要請に応じた割合が約 2 倍、要請に応じたことで取引につながったと感じた企業が約 2 倍存在した。セキュリティ体制の整備により、取引においてのセキュリティ要請に関して一定のメリットが得られると考えられる。

1) セキュリティ体制の整備状況

a. セキュリティ体制整備状況と企業規模の関係性

企業規模が大きくなるにつれ、セキュリティ体制の整備がなされている。

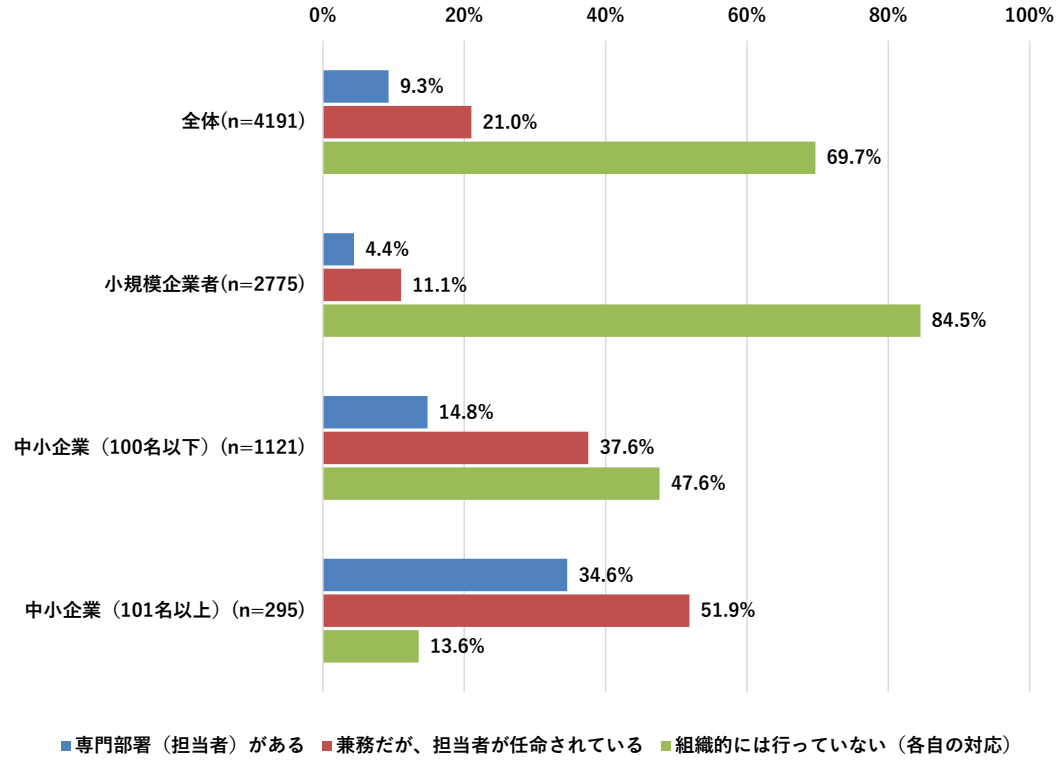

図 5-28 企業規模別のセキュリティ体制整備状況(n=4191)

b. セキュリティ体制整備と業種の関係性

セキュリティ体制を整備している企業の割合が高い業種は製造業、複合サービス業、情報通信業となり、体制を整備している割合が約 45-50%となった。これらの業種は小規模企業者の割合が約 50-55%となり、比較的低い。

セキュリティ体制を整備している企業の割合が低い業種は小売業、生活関連サービス業、娯楽業、不動産業、物品賃貸業となり、体制を整備している割合が約 20%となった。これらの業種は小規模企業者の割合が約 75-90%となり、比較的高い。

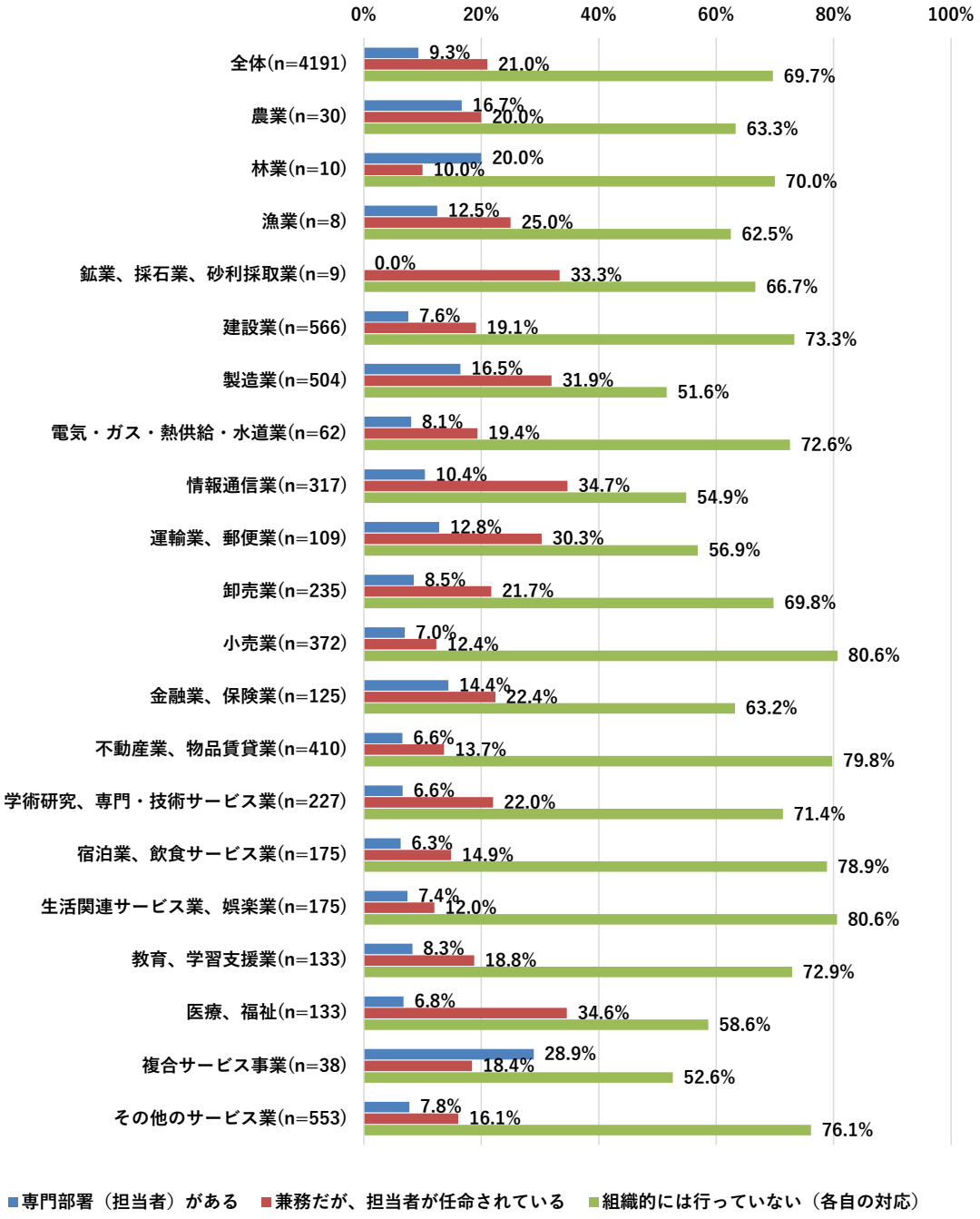

図 5-29 業種別のセキュリティ体制整備状況(n=4191)

表 5-3 業種別の企業規模の割合

業種	小規模企業者	中小企業 (100 名以下)	中小企業 (101 名以上)
全体(n=4191)	66.2%	26.7%	7.0%
農業(n=30)	73.3%	26.7%	0.0%
林業(n=10)	80.0%	20.0%	0.0%

業種	小規模企業者	中小企業 （100 名以下）	中小企業 （101 名以上）
漁業(n=8)	12.5%	87.5%	0.0%
鉱業、採石業、砂利採取業(n=9)	11.1%	77.8%	11.1%
建設業(n=566)	77.9%	16.4%	5.7%
製造業(n=504)	49.4%	28.0%	22.6%
電気・ガス・熱供給・水道業(n=62)	72.6%	21.0%	6.5%
情報通信業(n=317)	56.2%	40.7%	3.2%
運輸業、郵便業(n=109)	51.4%	29.4%	19.3%
卸売業(n=235)	52.3%	39.6%	8.1%
小売業(n=372)	75.0%	22.3%	2.7%
金融業、保険業(n=125)	80.0%	8.0%	12.0%
不動産業、物品賃貸業(n=410)	87.6%	8.8%	3.7%
学術研究、専門・技術サービス業(n=227)	70.9%	26.9%	2.2%
宿泊業、飲食サービス業(n=175)	59.4%	37.1%	3.4%
生活関連サービス業、娯楽業(n=175)	73.1%	26.3%	0.6%
教育、学習支援業(n=133)	63.2%	32.3%	4.5%
医療、福祉(n=133)	30.8%	63.2%	6.0%
複合サービス事業(n=38)	47.4%	47.4%	5.3%
その他のサービス業(n=553)	68.2%	27.1%	4.7%
働いていない(n=0)	0.0%	0.0%	0.0%

c. セキュリティ体制整備とセキュリティ対策に期待する効果

セキュリティ対策に期待する効果として、セキュリティ体制の整備を行っている企業ではISMS・プライバシーマーク等の認証取得が最も多く、セキュリティ体制の整備を行っていない企業では助成金・補助金の取得が最も多い。

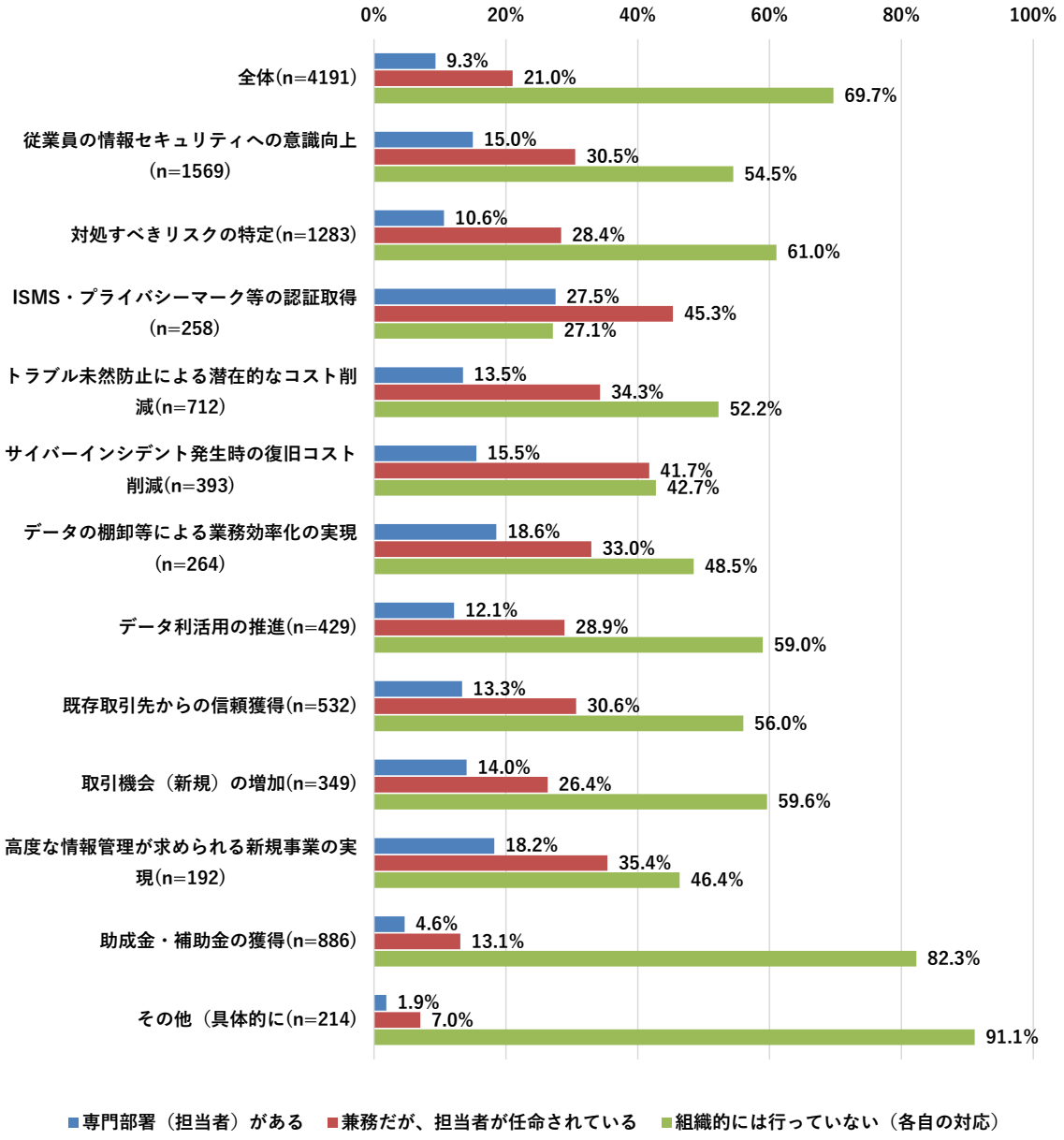

図 5-30 セキュリティ体制整備状況とセキュリティ対策に期待する効果(n=4191)

d. セキュリティ体制整備と取引上のリスク認識

セキュリティ体制の整備が行われている企業では約 80-85%の企業、セキュリティ体制の整備が行われていない企業では約 50%の企業で取引上におけるリスク認識がなされている。

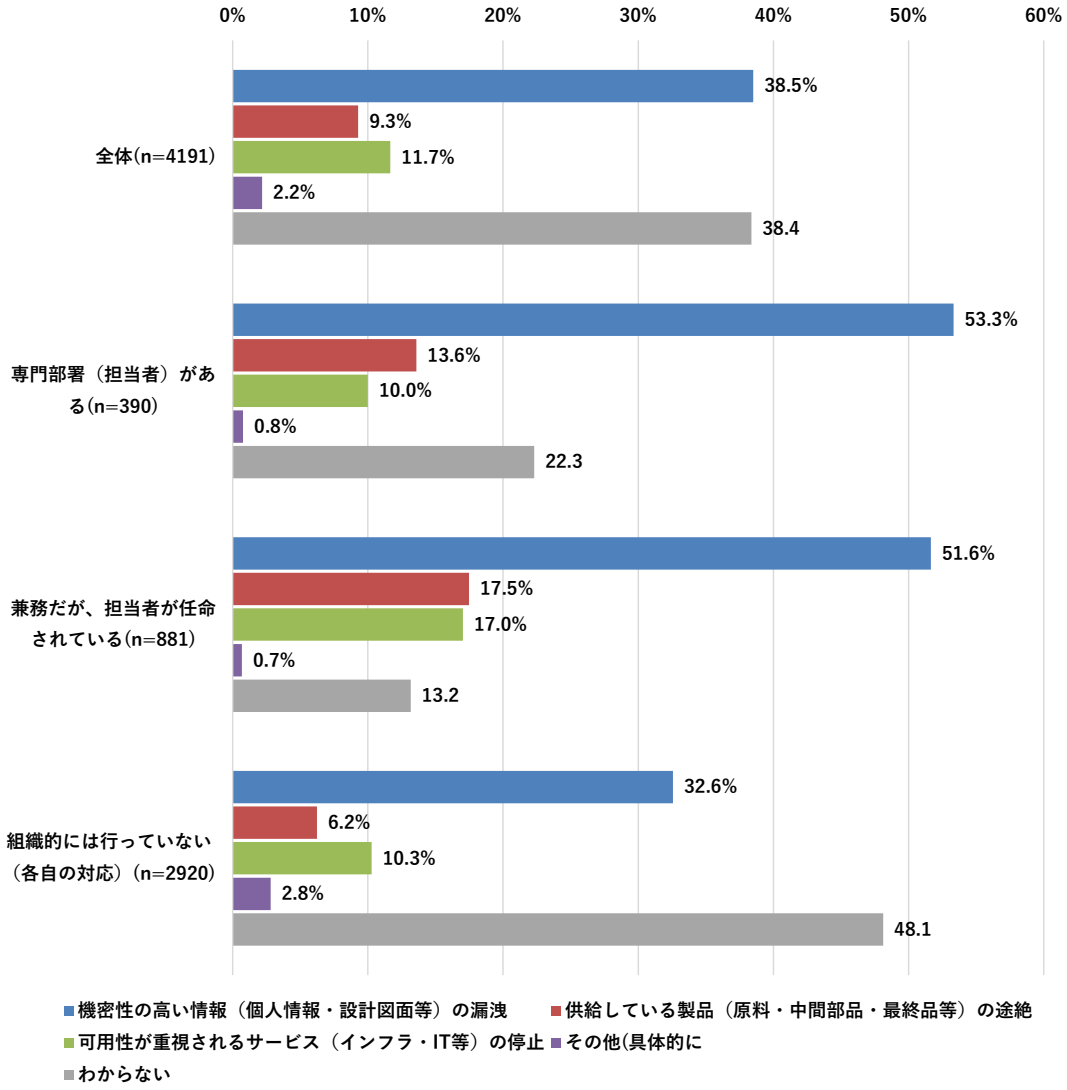

図 5-31 セキュリティ体制整備状況と取引上のリスク認識(n=4191)

2）取引上のメリットに関する分析

a. セキュリティ体制整備状況と取引におけるセキュリティ要請

セキュリティ要請を受けた割合に関してはセキュリティ体制を行っている企業の方が約 5～6 倍高かった。セキュリティ要請に応じた割合に関してはセキュリティ体制を行っている企業の方が約 2 倍高かった。

セキュリティ要請に応じたことが取引につながったと回答した企業の割合はセキュリティ体制を行っている企業の方が約 2 倍高かった.

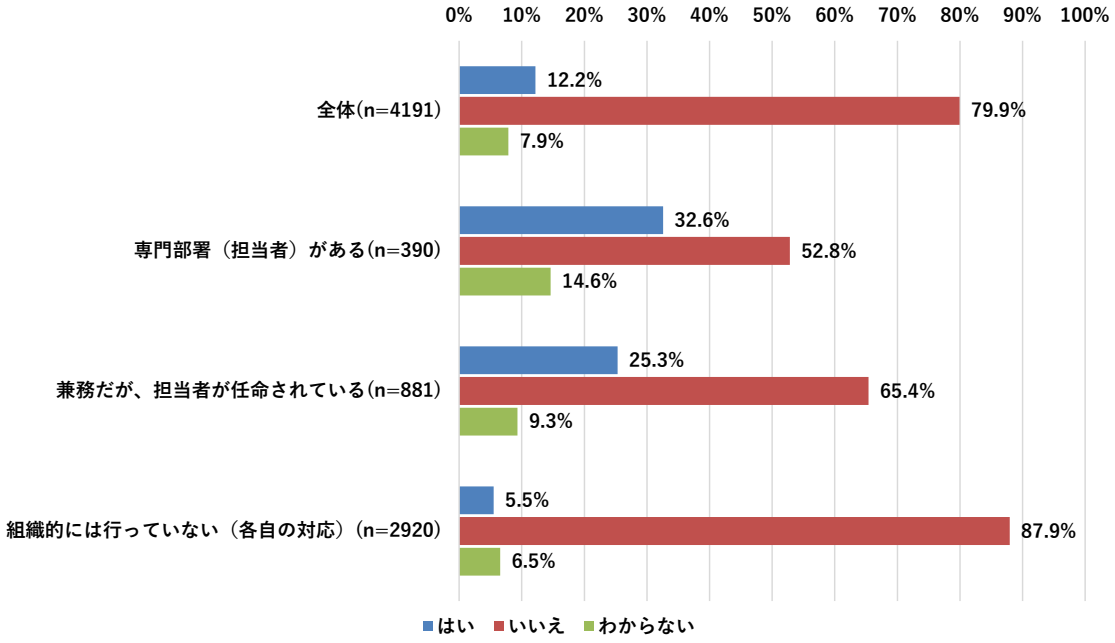

図 5-32 セキュリティ体制整備状況とセキュリティ要請経験の有無の関係(n=4191)

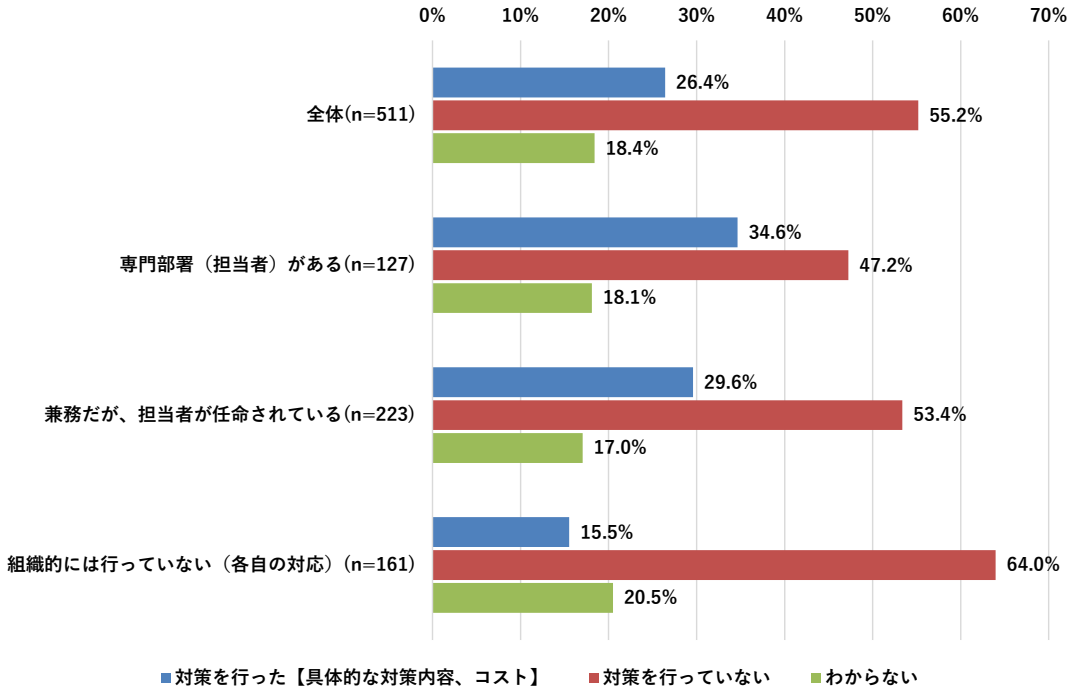

図 5-33 セキュリティ体制整備状況とセキュリティ要請への対応の関係(n=511)

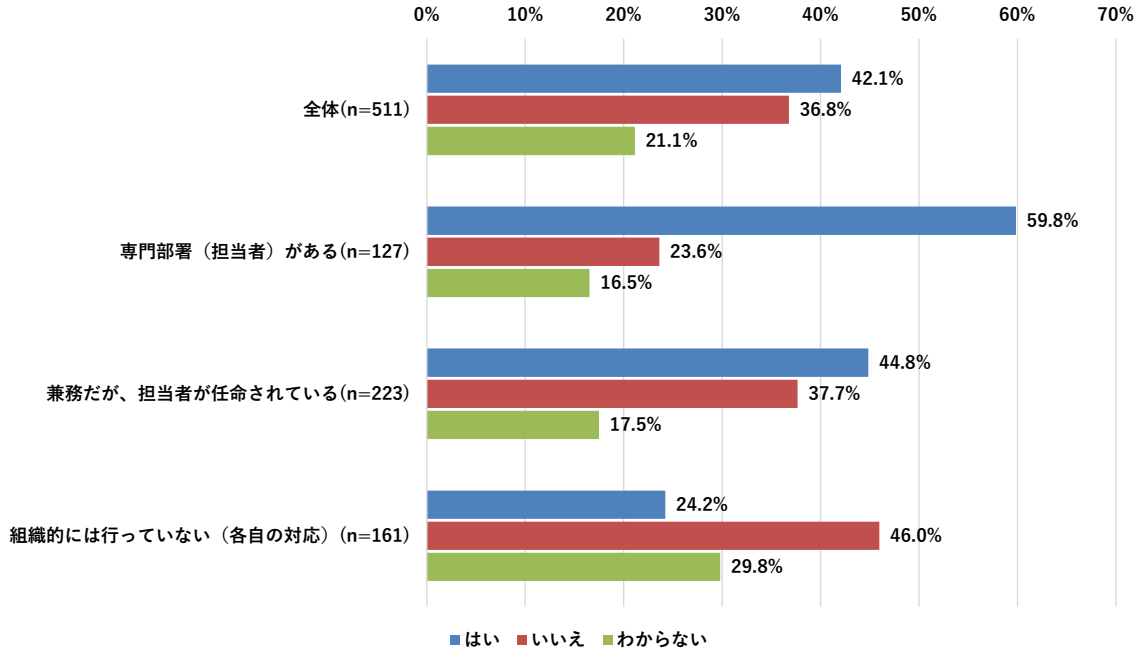

図 5-34 セキュリティ体制整備状況とセキュリティ要請に応じたことが取引につながったかの関係（n=511）

5.2.4 取引におけるリスク認識有無の効果

アンケート調査結果を元に、取引におけるリスク認識による効果について分析を行った。設問 Q41 では他社との取引において自社の主要な事業に最も大きいリスクと考えていることを質問している。その回答として「わからない」を選択した企業(1,608 件)は取引におけるリスクを認識していないものとして「リスク認識なし」、また「わからない」及び「その他」以外を選択した企業(2,492 件)はリスクを認識しているものとして「リスク認識あり」として統合し、各設問とのクロス集計を行った。なお、「その他」は自由回答であるため集計から除外しており集計の全体回答数は n=4,100 となっている。

分析の結果、取引におけるリスク認識の有無によりインシデントの被害経験、被害の大きさ(内容、被害額)、サプライチェーンへの影響の低減については関係性が見られなかった。一方で、取引におけるリスク認識がある方が取引上におけるメリットが見られた。取引におけるリスク認識がある企業では取引におけるリスク認識がない企業に比べて約 9 倍の割合でセキュリティ要請経験があり、要請に応じた割合が約 9 倍、要請に応じたことで取引につながったと感じた企業が約 2 倍存在した。

これらのことから、取引におけるリスク認識があることは、企業の規模・業種に関わらず、取引上におけるメリットに効果のある対策であると考えられる。

1） 取引におけるリスク認識状況

a. 取引におけるリスク認識状況と企業規模の関係性

企業規模が大きくなるにつれ、取引におけるリスク認識がなされている。

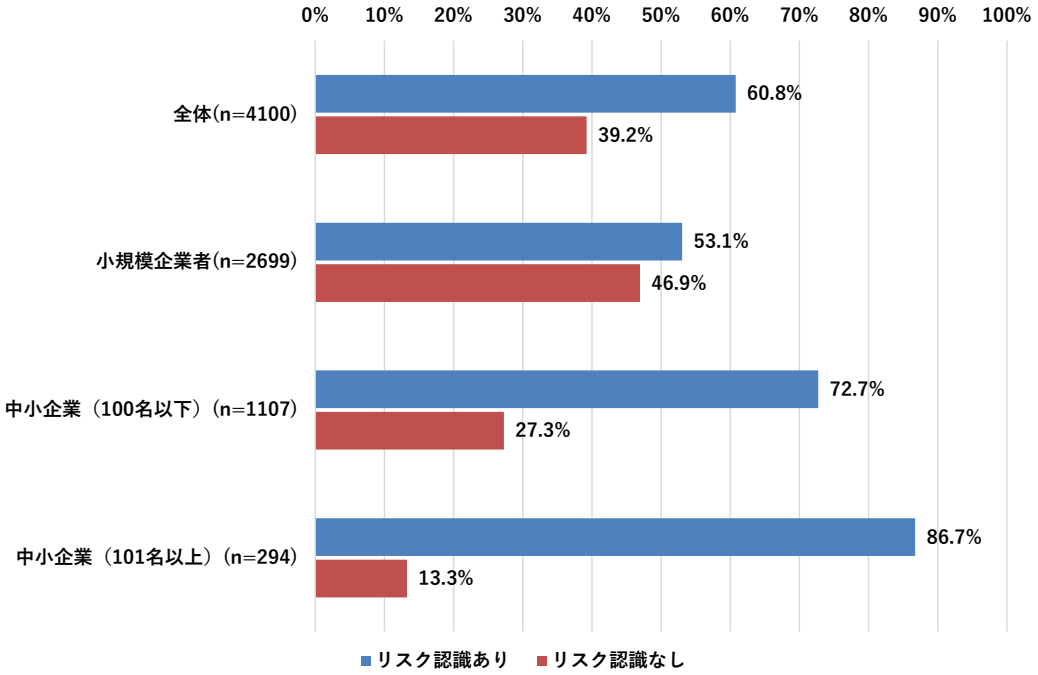

図 5-35 企業規模別の取引におけるリスク認識有無(n=4100)

b. 取引におけるリスク認識状況と業種の関係性

取引におけるリスク認識のある企業の割合が高い業種は製造業、情報通信業、金融業、保険業、複合サービス業となり、約 70-80%となっている。

取引におけるリスク認識のある企業の割合が低い業種は小売業、宿泊業、飲食サービス業となり、約50%となっている。

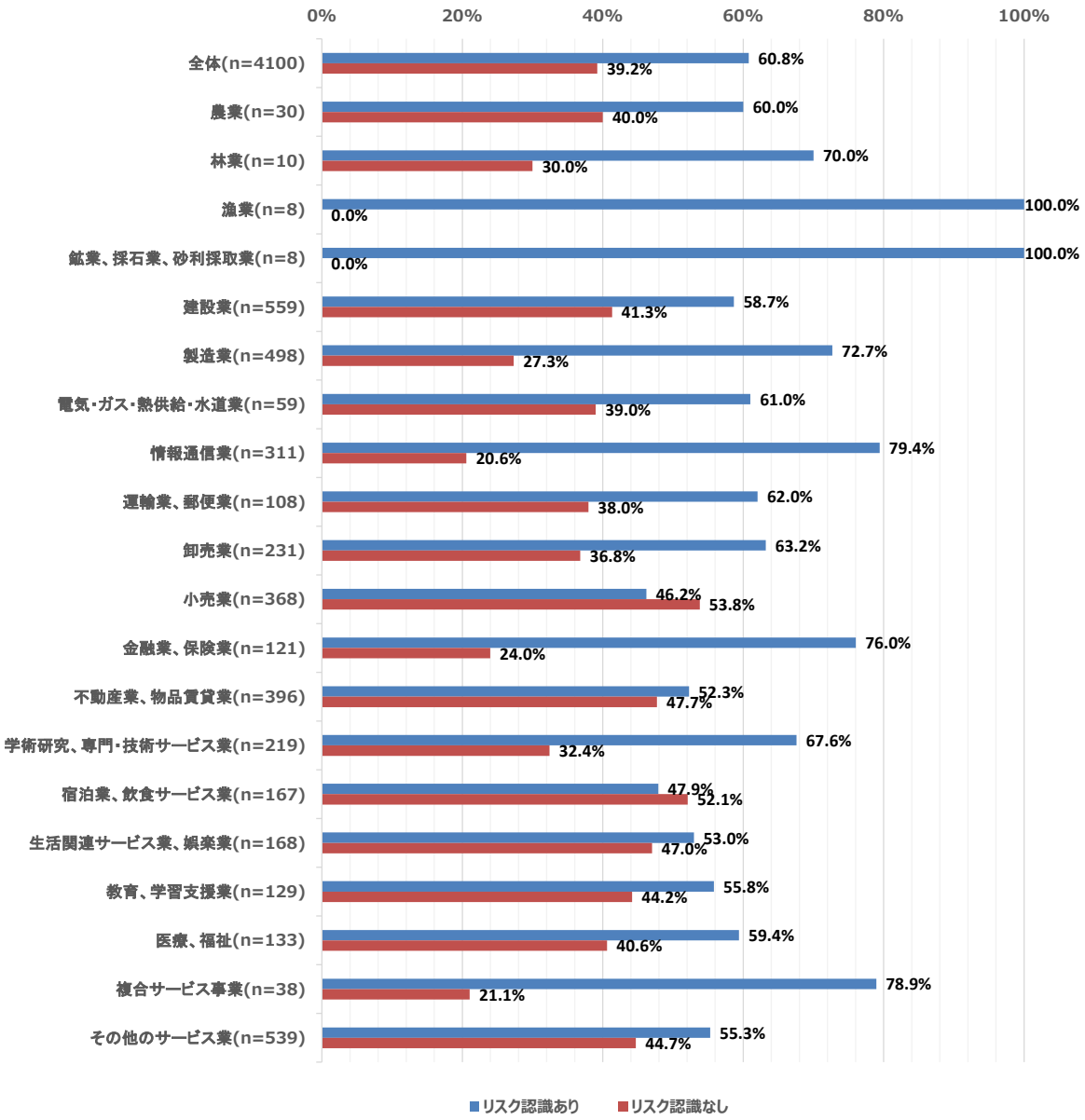

図 5-36 業種別の取引におけるリスク認識有無(n=4100)

c. 取引におけるリスク認識とセキュリティ対策に期待する効果

Q19 とのクロス集計の結果、取引におけるリスク認識がある企業では、ISMS・プライバーマーク等の認証取得が最も高く、次いでサイバーインシデント発生時の復旧コスト削減であることが分かった。

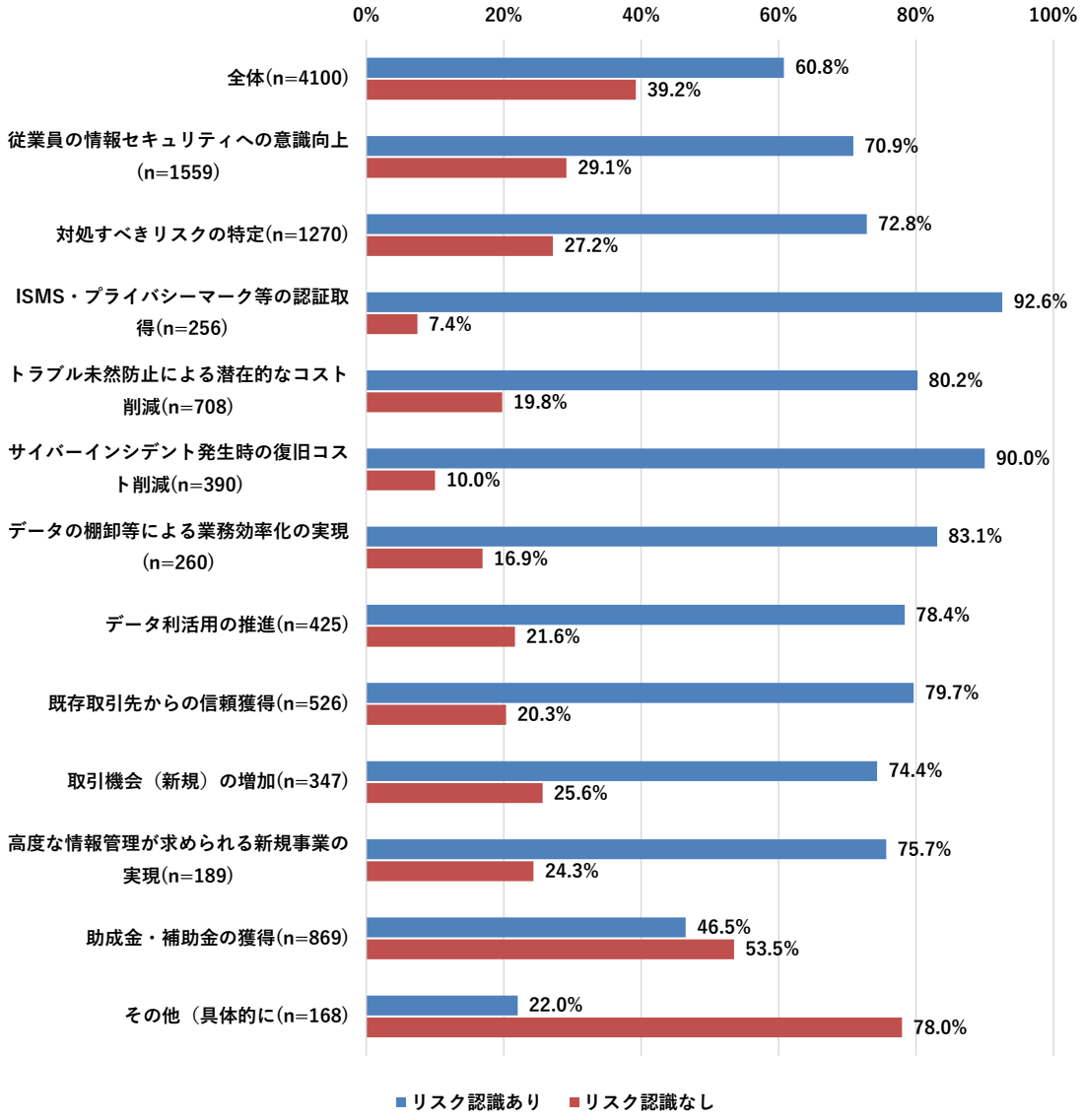

図 5-37 取引におけるリスク認識状況とセキュリティ対策に期待する効果(n=4100)

2）取引上のメリットに関する分析

a. 取引におけるリスク認識状況と取引におけるセキュリティ要請

セキュリティ要請を受けた割合は取引におけるリスク認識のある企業の方が約 9 倍高かった。また、セキュリティ要請に応じた割合は取引におけるリスク認識のある企業の方が約 9 倍高かった。

セキュリティ要請に応じたことが取引につながったと回答した企業の割合は取引におけるリスク認識のある企業の方が約 2 倍高かった。

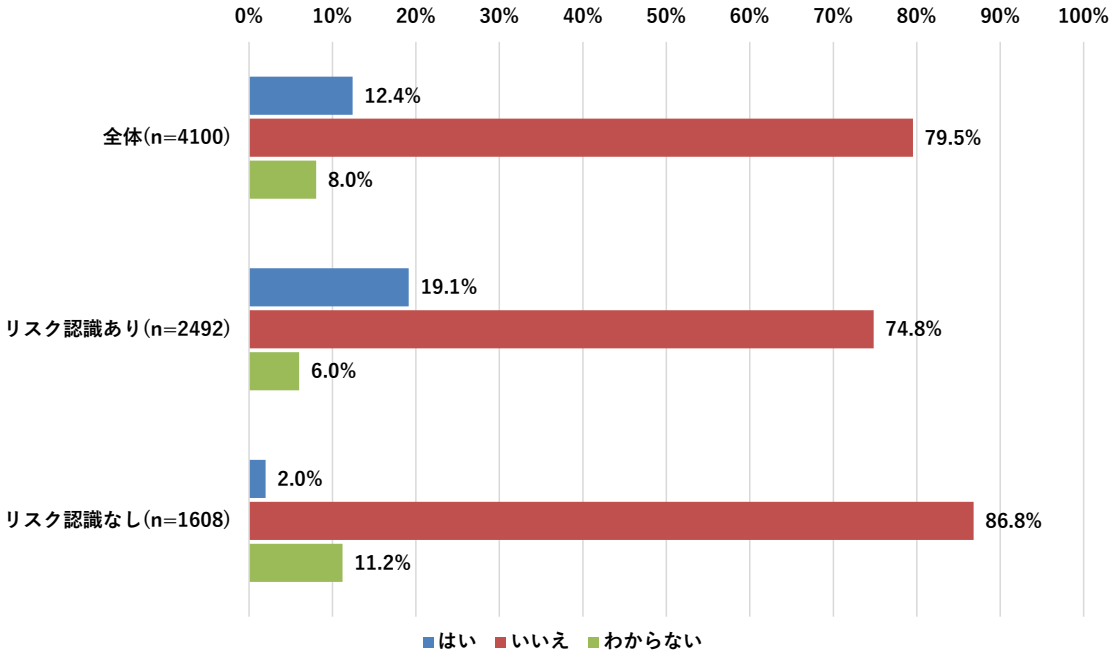

図 5-38 取引におけるリスク認識状況とセキュリティ要請経験の有無の関係(n=4100)

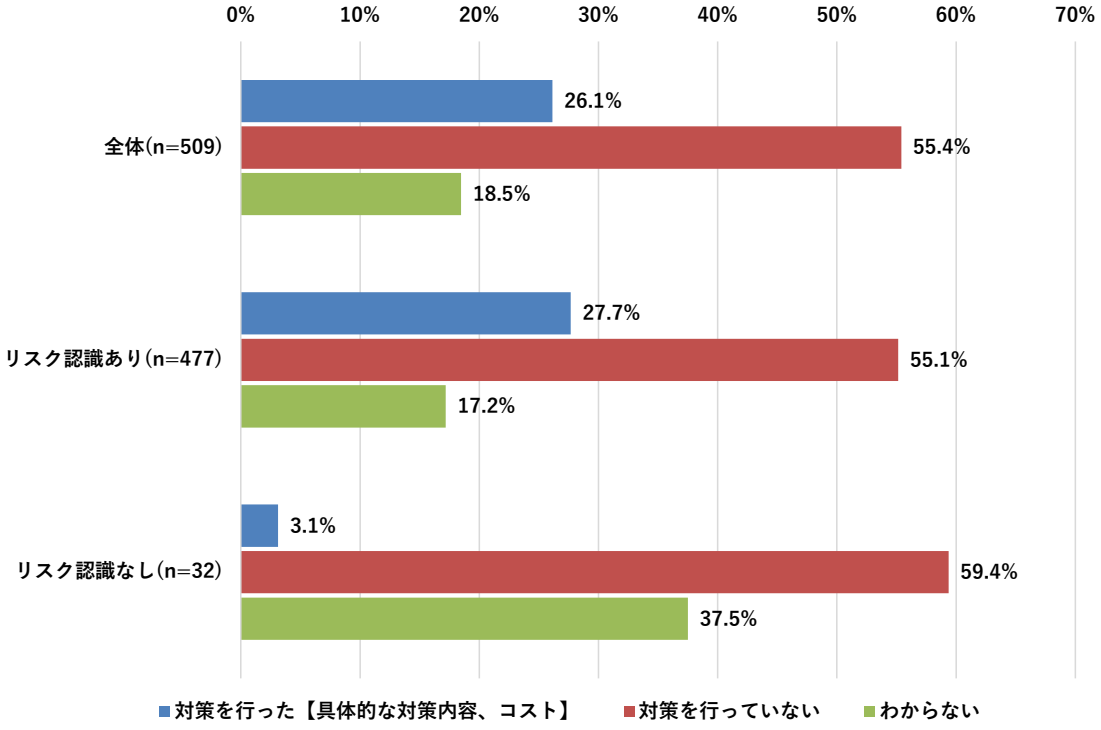

図 5-39 取引におけるリスク認識状況とセキュリティ要請への対応の関係(n=509)

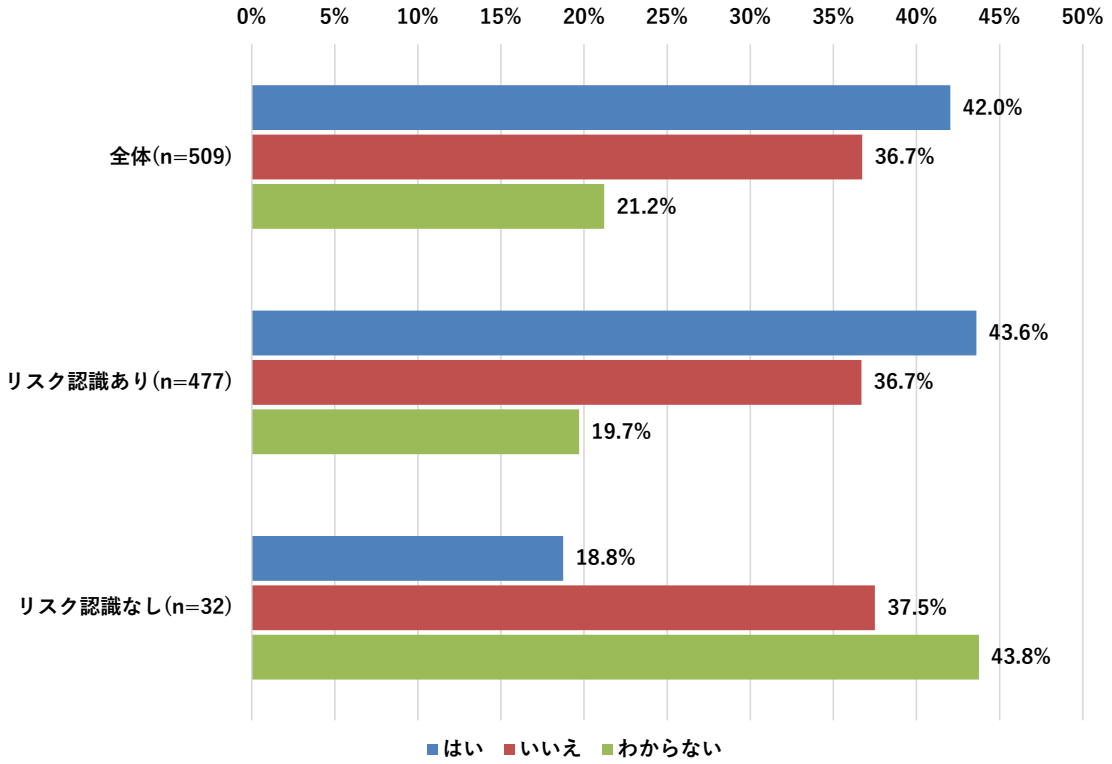

図 5-40 取引におけるリスク認識状況とセキュリティ要請応じたことが取引につながったかの関係（n=509）

5.3 SECURITY ACTION 一つ星及び二つ星に求められる基準

ここでは IPA の中小企業向けの施策である、SECURITY ACTION 一つ星、二つ星に求められるサイバーセキュリティ対策に関して分析を行う。

5.2 で説明の通り、アンケート設問 Q80 の 25 項目は、IPA が提供する「5 分でできる！情報セキュリティ自社診断」の「診断編」に掲載されている 25 項目の診断項目と同じであり、またこれらの項目は、SECURITY ACTION 二つ星の自己宣言を行う上で診断項目として活用される。また、「Part1 基本的対策」の 5 項目は、SECURITY ACTION 一つ星に該当している。従って、Q80 の回答を分析することで、回答した中小企業が SECURITY ACTION 一つ星、および二つ星の診断項目をどの程度満たしているかを確認できる。

5.3.1 SECURITY ACTION 一つ星に求められる基準

ここでは IPA の中小企業向けの施策である、SECURITY ACTION 一つ星に求められるサイバーセキュリティ対策に関して分析を行う。

分析のアプローチは、アンケート調査結果から SECURITY ACTION 一つ星の診断項目に該当する設問の回答結果を集計し、中小企業における SECURITY ACTION 一つ星の診断項目の実施度合いを分析する。その結果から SECURITY ACTION 一つ星に該当するサイバーセキュリティ対策を中小企業が行うにあたっての課題や、中小企業が必要となる支援策の検討を行った。

分析の結果、SECURITY ACTION 一つ星の診断項目を実施している企業は約 30%であることが分かった。また、特に重要情報へのアクセスコントロールとサイバー攻撃に関する情報の周知の実施率が低いことが分かった。中小企業は自社の管理責任が伴うような重要情報を特定し、重要情報の管理体制を構築することが望ましい。また、IPA や内閣サイバーセキュリティセンター（以下、NISC）といった公的機関の情報を参照することや、知り合いやコミュニティへの参加で情報交換を積極的に行うことが望ましい。

(1) SECURITY ACTION 一つ星の診断項目の実施状況

分析に用いる設問と選択肢を以下に示す。

表 5-4 SECURITY ACTION 一つ星に関する設問と選択肢

設問	各設問の選択肢
項目 1. パソコンやスマホなど情報機器の OS やソフトウェアは常に最新の状態にしていますか？	1. 実施している 2. 一部実施している 3. 実施していない 4. 分からない
項目 2. パソコンやスマホなどにはウイルス対策ソフトを導入し、ウイルス定義ファイルは最新の状態にしていますか？	
項目 3. パスワードは破られにくい「長く」「複雑な」パスワードを設定していますか？	

設問	各設問の選択肢
項目 4. 重要情報に対する適切なアクセス制限を行っていますか？	
項目 5. 新たな脅威や攻撃の手口を知り対策を社内共有する仕組みはできていますか？	

本分析では上記に掲載した 5 項目すべてが「1. 実施している」「2. 一部実施している」のいずれかを回答している場合に「一つ星実施」とし、それ以外の場合を「一つ星未実施」としてアンケート回答企業の実施状況を表記する。

表 5-5 SECURITY ACTION の診断項目に関して実施、未実施とする条件

「一つ星実施」に該当する条件	「一つ星未実施」に該当する条件
表 5-4 で提示される 5 つの設問すべてにおいて、「1. 実施している」「2. 一部実施している」のいずれかを回答している。	表 5-4 で提示される 5 つの設問のいずれかに、「3. 実施していない」「4. 分からない」を回答している。

以下に SECURITY ACTION 一つ星の診断項目についてアンケート回答企業における実施状況の割合、および企業規模別、業種別の分析結果を示す。

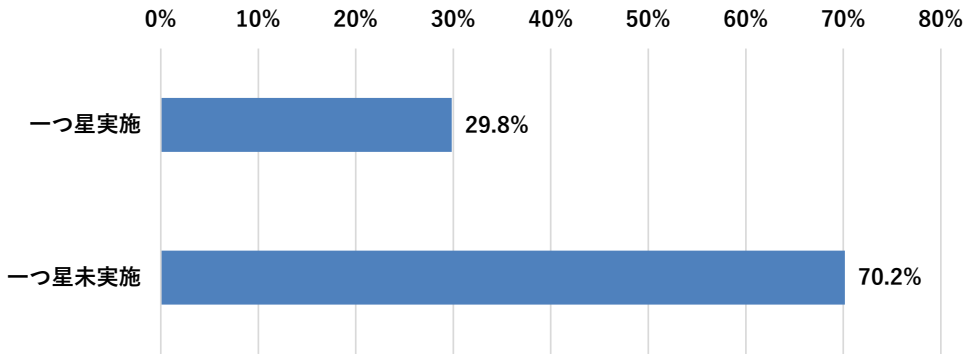

図 5-41 SECURITY ACTION 一つ星の実施状況（n=4191）

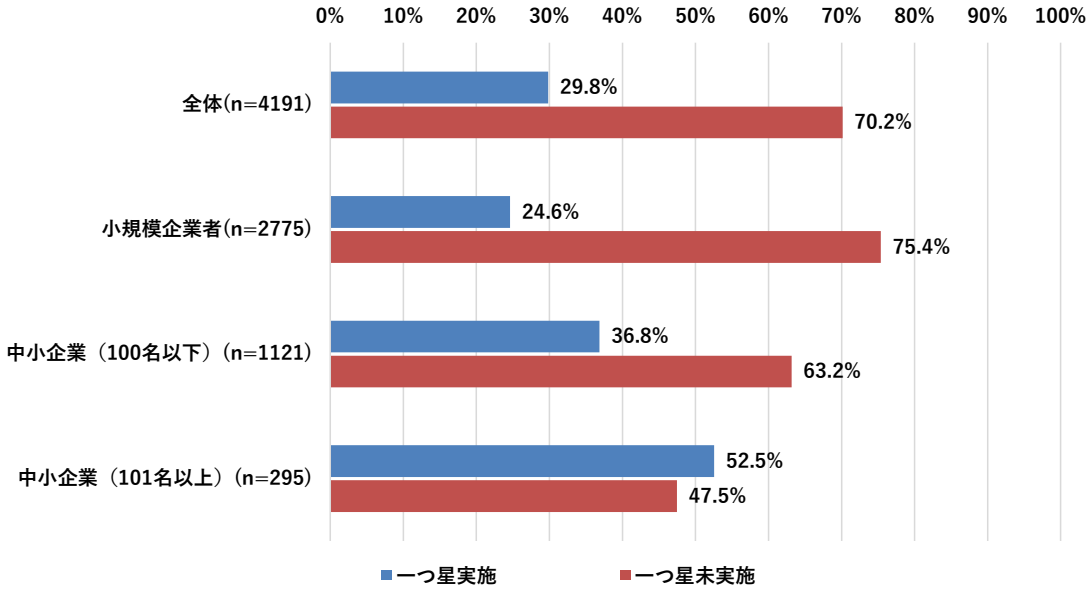

図 5-42 SECURITY ACTION 一つ星の実施状況と企業規模の関係(n=4191)

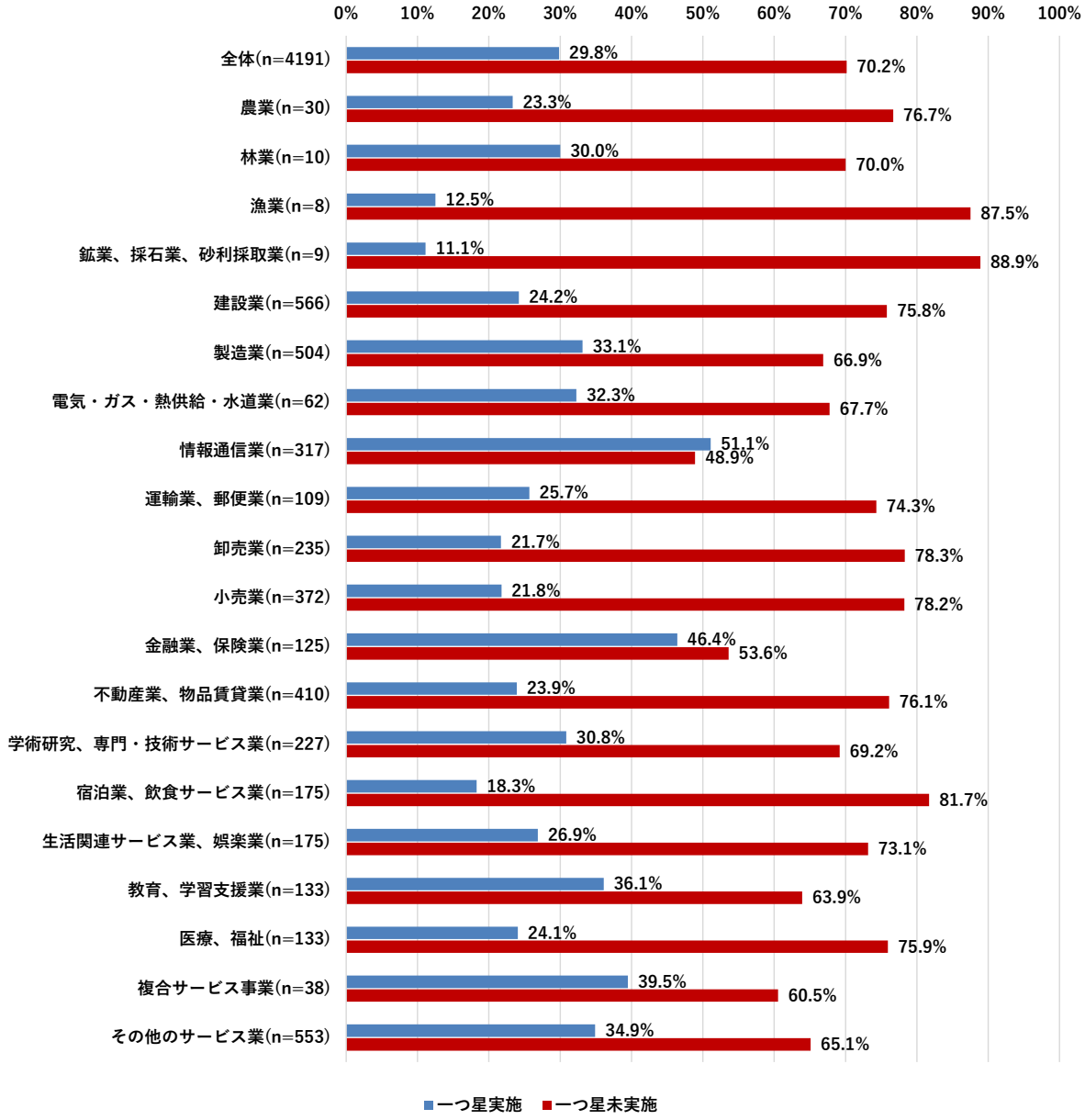

図 5-43 SECURITY ACTION 一つ星の実施状況と業種の関係(n=4191)

SECURITY ACTION 一つ星の診断項目を実施している企業(「一つ星実施」)は約 30%となった。

企業規模別では、企業規模が大きくなるにつれて実施している企業の割合が増えており、特に中小企業(101 名以上)では約 50%となっている。

業種別では SECURITY ACTION 一つ星の診断項目を実施している企業の割合が高い業種は情報通信業、金融業、保険業であり、割合として約 50%となり、基礎的なサイバーセキュリティ対策が行えている割合が高いことが分かる。また、SECURITY ACTION 一つ星の診断項目を実施している企業の割合が低い業種は宿泊業、飲食サービス業、卸売業、小売業であり、割合として約 20%となり、基礎的なサイバーセキュリティ対策が行えている割合が低いことが分かった。なお、業種別の回答数が少ない農業、林業、漁業、工業、採石業、砂利採取業は除外している。

図 5-44 は上記の業種についてサイバーセキュリティ対策実施のきっかけを示したものである。

SECURITY ACTION 一つ星の診断項目を実施している企業の割合が高い業種（情報通信業、金融業、保険業）では、法令の制定や改訂への対応、業界基準の制定、業界団体の呼びかけをきっかけにサイバーセキュリティ対策を実施する割合が高い。一方、SECURITY ACTION 一つ星の診断項目を実施している割合が低い業種（宿泊業、飲食サービス業、卸売業、小売業）では、対策の必要性を感じたことがないと回答した企業が多い。

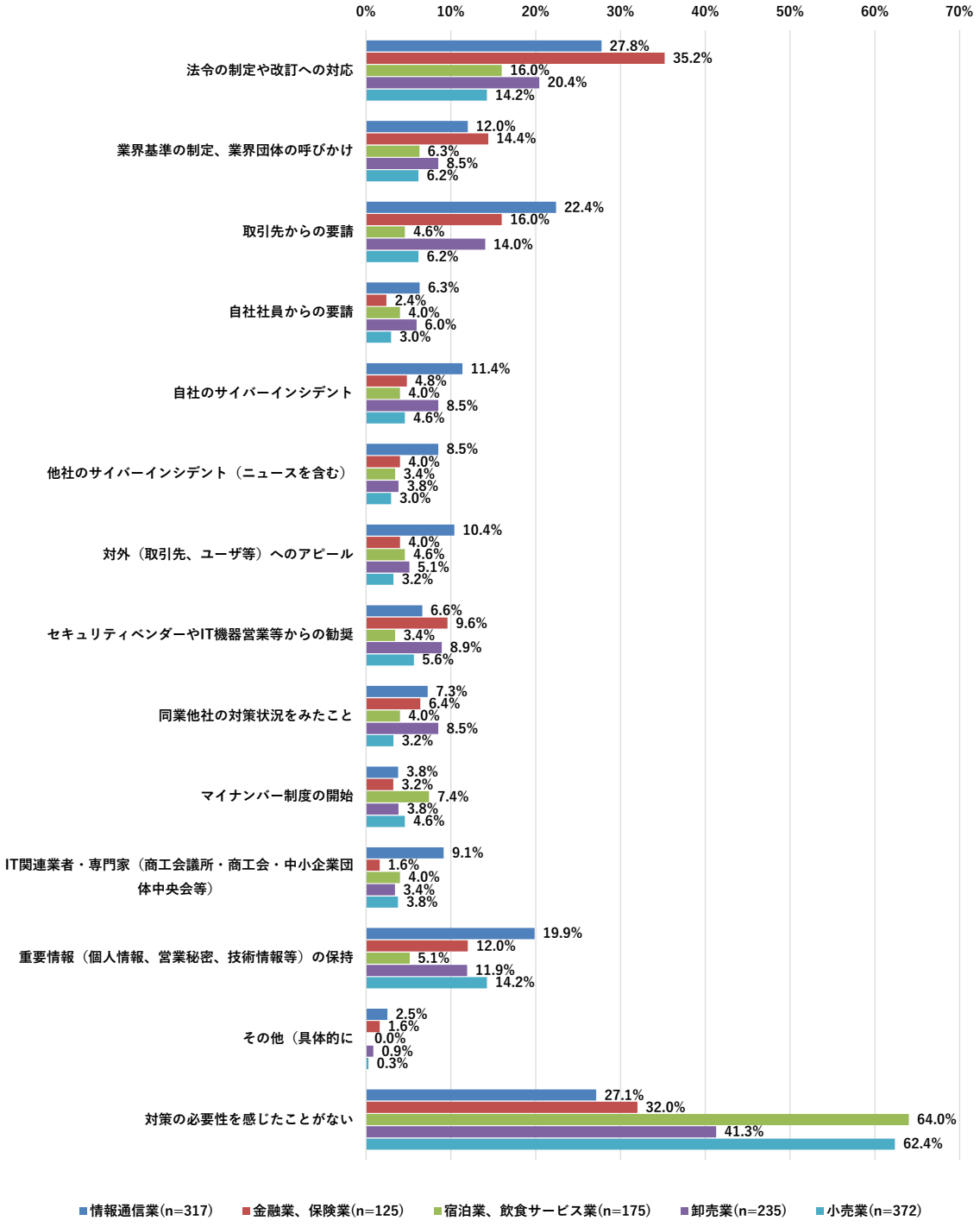

図 5-44 SECURITY ACTION 一つ星の診断項目を実施している企業の割合が高い業種（情報通信業、金融業、保険業）と SECURITY ACTION 一つ星の診断項目を実施している企業の割合が低い業種（宿泊業、飲食サービス業、卸売業、小売業）のサイバーセキュリティ対策実施のきっかけ（n=1224）

SECURITY ACTION 一つ星の診断項目を実施していない企業(「一つ星未実施」)における各項目の実施状況を以下に示す。

表 5-6 「一つ星未実施」の企業における診断項目の実施率(n=2940)

診断項目	実施率
項目1. パソコンやスマホなど情報機器のOSやソフトウェアは常に最新の状態にしていますか?	61.5%
項目2. パソコンやスマホなどにはウイルス対策ソフトを導入し、ウイルス定義ファイルは最新の状態にしていますか?	59.2%
項目3. パスワードは破られにくい「長く」「複雑な」パスワードを設定していますか?	44.2%
項目4. 重要情報に対する適切なアクセス制限を行っていますか?	26.9%
項目5. 新たな脅威や攻撃の手口を知り対策を社内共有する仕組みはできていますか?	11.5%

(2) 実施率の低い診断項目

SECURITY ACTION 一つ星の診断項目を実施していない企業(「一つ星未実施」)において、実施率が低い項目は以下であった。

- 項目 4. 重要情報に対する適切なアクセス制限を行っていますか?
  - 重要情報に対するアクセスコントロールを行っていない、実施状況が分からないとした企業の割合が約 70%となった。情報資産を一覧化した上で、どの従業員がアクセスする必要があるのかを把握する必要がある。情報資産について、その重要性、漏えいした場合のリスクを評価し、管理体制を構築することが望ましい。

- 項目 5. 新たな脅威や攻撃の手口を知り対策を社内共有する仕組みはできていますか?
  - サイバー攻撃や脅威に関する情報の周知を行っていない、実施状況が分からないとした企業の割合が約 90%となった。サイバーインシデントがどういった場面で発生するのか、どういった被害があるのかを実例等を交えて身近に感じる必要がある。中小企業は IPA や NISC といった公的機関の情報を参照することや、知り合いやコミュニティへの参加で情報交換を積極的に行うことが望ましい。

5.3.2 SECURITY ACTION 二つ星に求められる基準

ここでは SECURITY ACTION 二つ星宣言に求められるサイバーセキュリティ対策に関して分析を行う。

本分析ではアンケート回答企業における SECURITY ACTION 二つ星の診断項目の実施状況を

調査し、実施率が低い診断項目や、逆に実施率が高い診断項目を明らかにした。実施率が低い診断項目については、それらに関する促進策などを検討した。

分析の結果、SECURITY ACTION 二つ星の診断項目の多くを実施している企業（自社診断の合計点が 70 点以上の企業）は、全体の約 2 割であることが分かった。また、実施率が高い対策項目としては、サイバーセキュリティ対策として広く周知されているものや、PC やソフトウェアに標準機能として組み込まれているため利用者が受動的に対策実施のタイミングを知ることができる機能を持つものなどの特徴が見られた。一方で実施率が低い診断項目として、特にサイバー攻撃に関する情報の周知、インシデント対応計画の策定、サイバーセキュリティ対策のルール化と周知があり、中小企業ではこれらの実施に課題があることが分かった。中小企業はIPAやNISCといった公的機関の情報を参照することや、知り合いやコミュニティへの参加で情報交換を積極的に行うことが望ましい。また、IPA の提供する「中小企業の情報セキュリティ対策ガイドライン」を活用することで、自社に合わせたサイバーセキュリティ対策のルール作成及び従業員への周知やサイバーインシデントへの対応計画を策定することが望ましい。

（1） SECURITY ACTION 二つ星宣言に必要な自社診断項目の実施状況

アンケート回答企業における Q80 の 25 項目の回答結果を「5 分でできる！情報セキュリティ対策自社診断」の基準に沿って得点化して算出した自社診断の合計点の分布を分析した。

100 点の企業が全体の 6%、70 点～99 点の企業が 15.8%となっており、このことから、SECURITY ACTION 二つ星宣言に必要な診断項目を多く実施している企業（自社診断の合計点が 70 点以上）は、全体の約 2 割であることが分かった。また、自社診断の合計点が 70 点に満たない企業は、50 点～69 点が 15.6%、49 点以下が 62.6%と全体の約 8 割であった。

企業規模別の分析結果から、企業規模が大きくなるほど自社診断の合計点が高い企業の割合が多くなっていることが明らかになった。特に中小企業（101 名以上）では約 4 割の企業が 70 点以上であり、SECURITY ACTION 二つ星宣言に必要な自社診断項目の実施状況が高いレベルにあることが分かった。

また業種別でみると、情報通信業、金融業、保険業は 70 点以上を取得している企業の割合が高く、一方で 49 点以下の割合が高い業種としては、宿泊業、飲食サービス業、卸売業、小売業が挙げられる。これらの業種は 5.3.1 で行った一つ星に関する分析で得られた結果と同じであった。

1） 自社診断の合計点の分布

自社診断の合計点の分布状況は以下の通りである。

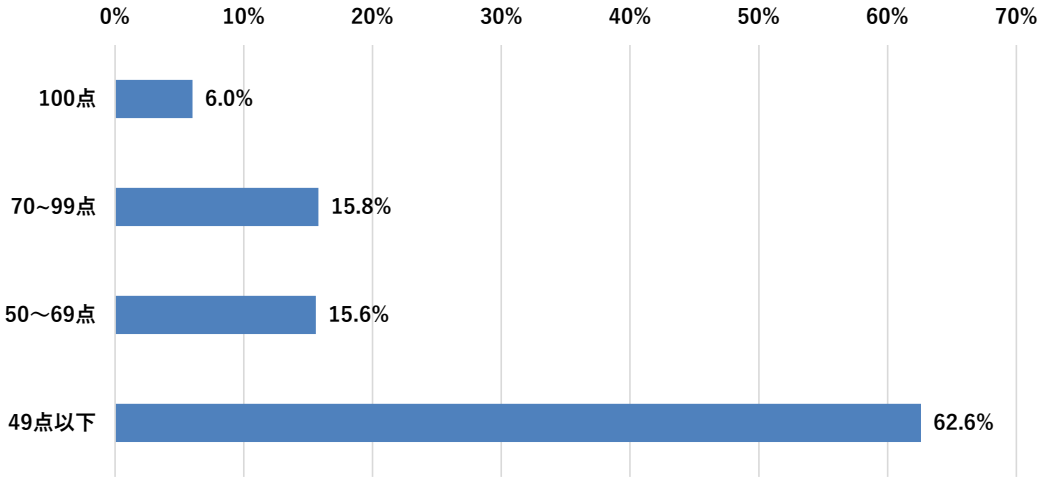

図 5-45 自社診断の合計点の分布(n=4191)

2）度数分布と平均点

アンケート回答企業における平均は 36.6 点であり、度数分布は下図の通りであった。

表 5-7 自社診断の合計点の平均

アンケート回答企業数	平均点	最大値	最小値
4,191	36.6	100	-25

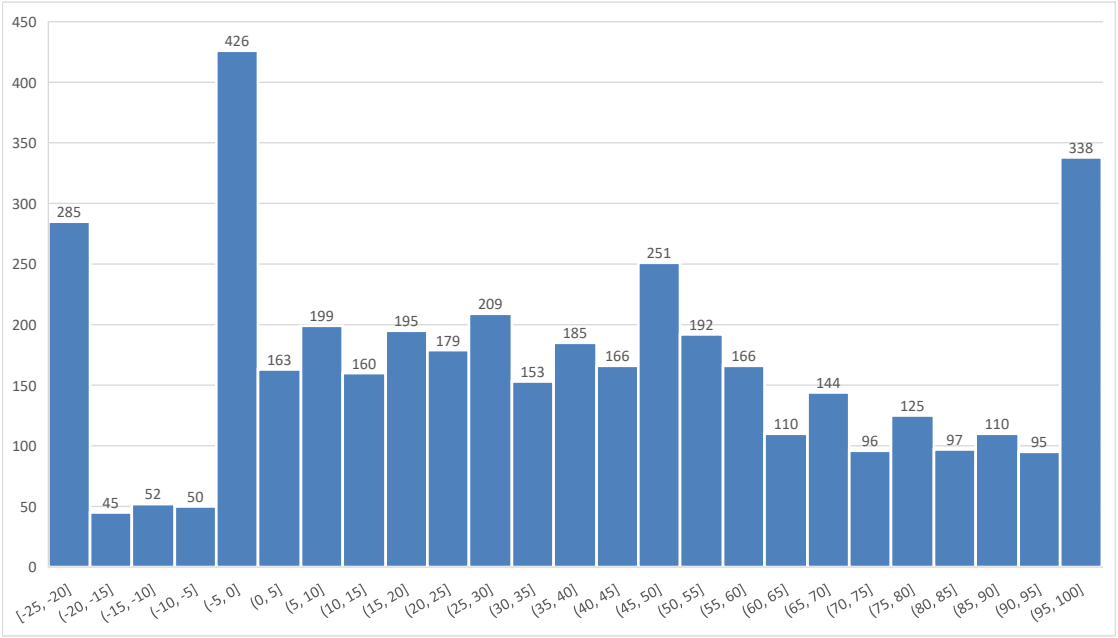

図 5-46 自社診断の合計点の度数分布図(n=4191)

3）企業規模別の自社診断の合計点

企業規模別の自社診断の合計点の状況は以下の通りである。

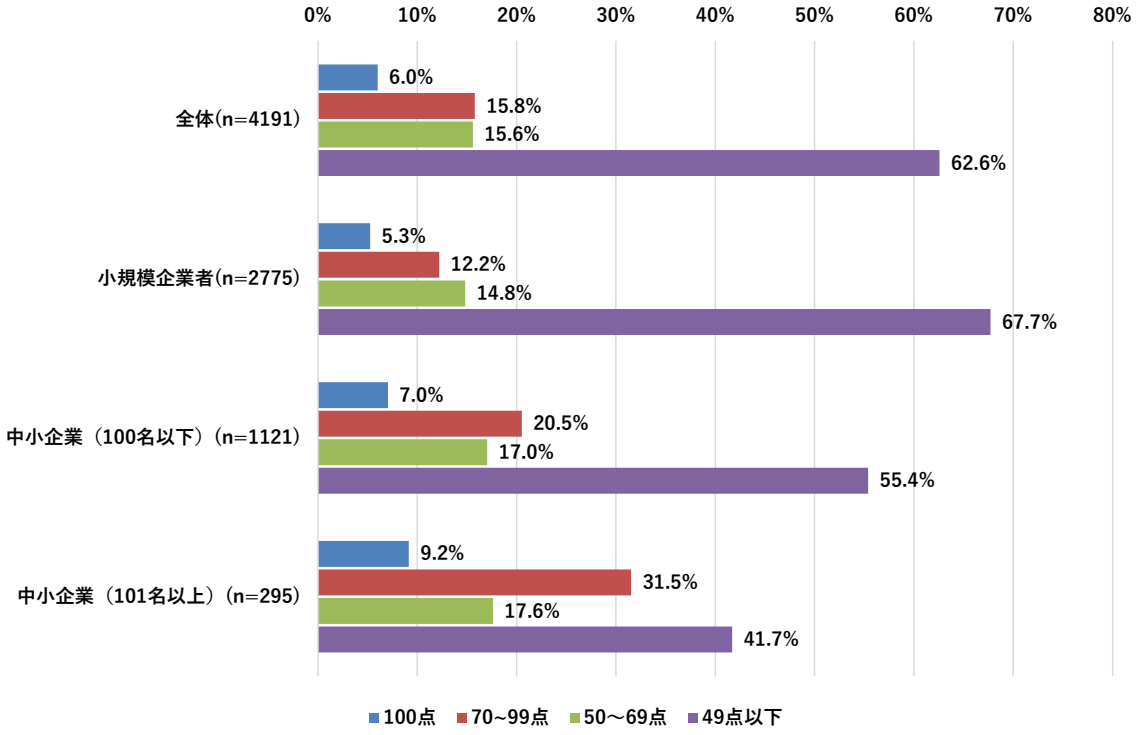

図 5-47 企業規模別の自社診断の合計点(n=4191)

4）業種別の自社診断の合計点

業界別の自社診断の合計点は以下の通りである。

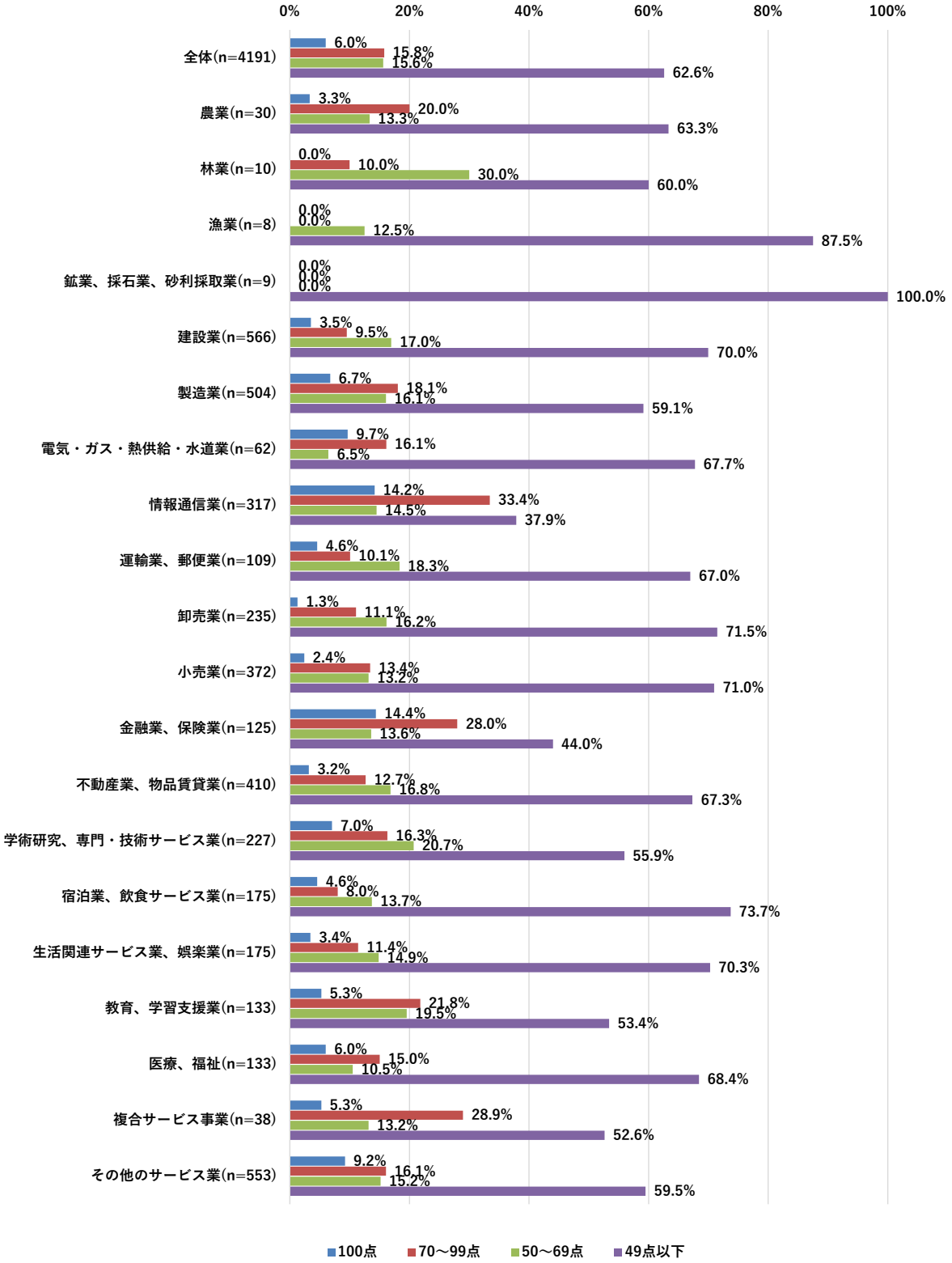

図 5-48 業種別の自社診断の合計点(n=4191)

（2）診断項目ごとの実施率

SECURITY ACTION 二つ星の診断項目について、自社診断 25 項目の実施状況を図 5-49 に、自社診断の合計点ごとの実施状況を表 5-8 に示す。実施の有無に関しては、表 5-5 SECURITY ACTION の診断項目に関して実施、未実施とする条件と同様の条件とする。実施率が高い項目および低い項目について分析を行う。

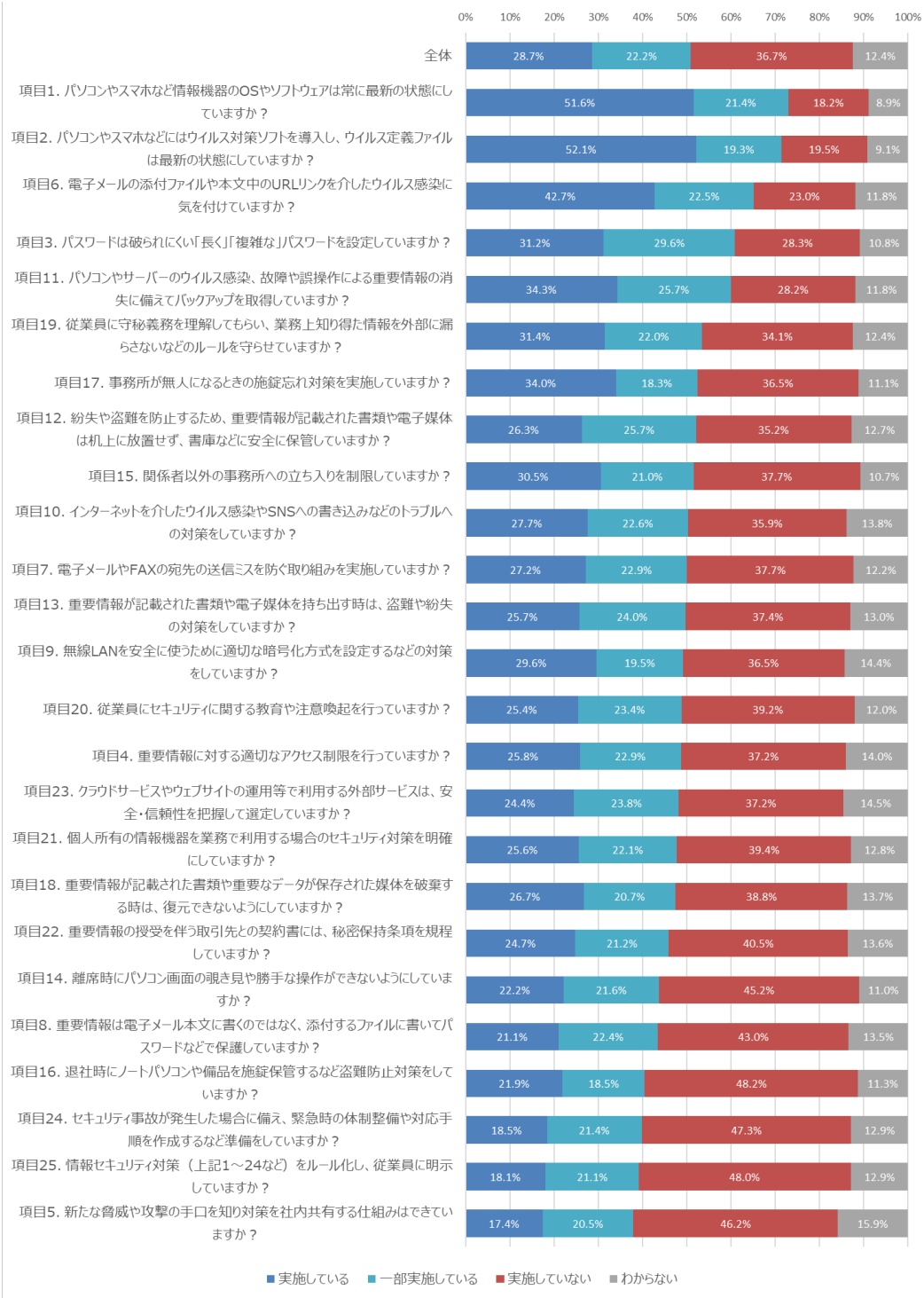

図 5-49 自社診断 25 項目の実施状況（n=4191）

表 5-8 SECURITY ACTION 二つ星の診断項目ごとの実施率（自社診断の合計点別）

	診断項目	70点～99点（n=662）	50点～69点（n=654）	49点以下（n=2623）
基本的対策	項目1. パソコンやスマホなど情報機器のOSやソフトウェアは常に最新の状態にしていますか？	98.9%	97.1%	57.8%
	項目2. パソコンやスマホなどにはウイルス対策ソフトを導入し、ウイルス定義ファイルは最新の状態にしていますか？	98.3%	96.6%	55.5%
	項目3. パスワードは破られにくい「長く」「複雑な」パスワードを設定していますか？	95.8%	92.2%	40.5%
	項目4. 重要情報に対する適切なアクセス制限を行っていますか？	93.7%	80.0%	24.7%
	項目5. 新たな脅威や攻撃の手口を知り対策を社内共有する仕組みはできていますか？	83.5%	62.4%	14.4%
従業員としての対策	項目6. 電子メールの添付ファイルや本文中のURLリンクを介したウイルス感染に気を付けていますか？	99.2%	95.7%	45.7%
	項目7. 電子メールやFAXの宛先の送信ミスを防ぐ取り組みを実施していますか？	95.2%	78.0%	26.9%
	項目8. 重要情報は電子メール本文に書くのではなく、添付するファイルに書いてパスワードなどで保護していますか？	87.6%	71.1%	20.1%
	項目9. 無線LANを安全に使うために適切な暗号化方式を設定するなどの対策をしていますか？	91.7%	79.2%	26.1%
	項目10. インターネットを介したウイルス感染やSNSへの書き込みなどのトラブルへの対策をしていますか？	95.8%	83.0%	25.8%
	項目11. パソコンやサーバーのウイルス感染、故障や誤操作による重要情報の消失に備えてバックアップを取得していますか？	98.2%	93.7%	38.0%
	項目12. 紛失や盗難を防止するため、重要情報が記載された書類や電子媒体は机上に放置せず、書庫などに安全に保管していますか？	97.0%	86.1%	27.7%
	項目13. 重要情報が記載された書類や電子媒体を持ち出す時は、盗難や紛失の対策をしていますか？	97.6%	85.6%	23.8%
	項目14. 離席時にパソコン画面の覗き見や勝手な操作ができないようにしていますか？	88.8%	71.1%	20.2%
	項目15. 関係者以外の事務所への立ち入りを制限していますか？	93.1%	82.1%	28.8%
	項目16. 退社時にノートパソコンや備品を施錠保管するなど盗難防止対策をしていますか？	85.5%	66.5%	16.9%
	項目17. 事務所が無人になるときの施錠忘れ対策を実施していますか？	95.3%	83.8%	29.2%
組織としての対策	項目18. 重要情報が記載された書類や重要なデータが保存された媒体を破棄する時は、復元できないようにしていますか？	93.5%	79.2%	22.9%
	項目19. 従業員に守秘義務を理解してもらい、業務上知り得た情報を外部に漏らさないなどのルールを守らせていますか？	98.5%	90.2%	28.5%
	項目20. 従業員にセキュリティに関する教育や注意喚起を行っていますか？	94.9%	85.6%	23.1%
	項目21. 個人所有の情報機器を業務で利用する場合のセキュリティ対策を明確にしていますか？	98.2%	82.3%	21.4%
	項目22. 重要情報の授受を伴う取引先との契約書には、秘密保持条項を規程していますか？	93.5%	79.4%	20.4%
	項目23. クラウドサービスやウェブサイトの運用等で利用する外部サービスは、安全・信頼性を把握して選定していますか？	94.7%	81.5%	23.2%
	項目24. セキュリティ事故が発生した場合に備え、緊急時の体制整備や対応手順を作成するなど準備をしていますか？	91.1%	65.9%	14.6%
	項目25. 情報セキュリティ対策（上記1～24など）をルール化し、従業員に明示していますか？	89.3%	63.3%	14.6%

1） 実施率の高い項目に関する分析

アンケート回答企業の半数以上を占める、69 点以下の企業群において、実施率の高い項目は以下となった。これらの項目は中小企業においてサイバーセキュリティ対策として深く浸透している、もしくは中小企業にとって実施しやすい項目であることが考えられる。

- 項目 1. パソコンやスマホなど情報機器の OS やソフトウェアは常に最新の状態にしていますか？
  - OS やソフトウェアの更新に関しては、49 点以下の企業群であっても、約60%となった。最近のPCやスマートフォンなどではソフトウェアを利用する際に更新の通知が行われるなど、利用者が受動的にOSやソフトウェア更新の必要性を把握しやすいことなどから、中小企業にも広く認知されていると考えられる。

- 項目 2. パソコンやスマホなどにはウイルス対策ソフトを導入し、ウイルス定義ファイルは最新の状態にしていますか？
  - ウイルス対策ソフトの導入に関しては、49 点以下の企業群であっても、約 55%となった。PC を購入する時点で組み込まれていることも多く、また、インタビュー調査から最低限のサイバーセキュリティ対策として認知されていることが明らかになっており、中小企業にも広く認知されていることが読み取れる。

- 項目 6. 電子メールの添付ファイルや本文中の URL リンクを介したウイルス感染に気を付けていますか？
  - ウイルスメールへの警戒に関しては、49 点以下の企業群であっても、約 45%となった。メールアプリにデフォルトで迷惑メールフォルダが実装されているほか、ウイルスメールがサイバー攻撃の手段として被害事例を含めて中小企業にも広く認知されていることが考えられる。

2）実施率の低い項目に関する分析

アンケート回答企業の半数以上を占める、69 点以下の企業群において、実施率の低い項目は以下となった。

- 項目 5. 新たな脅威や攻撃の手口を知り、対策を社内共有する仕組みはできていますか？
  - サイバー攻撃や脅威に関する情報の周知を行っていない、実施状況が分からないとした企業の割合が 49 点以下の企業群では約 85%、50～69 点の企業群では約 40%となった。サイバーインシデントがどういった場面で発生するのか、どういった被害があるのかを実例等を交えて身近に感じる必要があると考えられる。中小企業は IPA や NISC といった公的機関の情報を参照することや、知り合いや関連するコミュニティへ参加すること通じて情報交換を積極的に行うことが望ましい。また、対策を社内共有する仕組みは、経営層を交えて検討をしたうえで構築することが望ましい。

- 項目 24. セキュリティ事故が発生した場合に備え、緊急時の体制整備や対応手順を作成するなど準備をしていますか？
  - サイバーインシデント発生後の対応計画等の準備を行っていない、実施状況が分からないとした企業の割合が 49 点以下の企業群では約 85%、50～69 点の企業群では約 35%となった。中小企業自身がサイバーインシデントの被害に関するリスクを把握し、インシデン

ト発生時の体制整備や対応手順を検討することが求められる。IPA では「中小企業の情報セキュリティ対策ガイドライン 付録 8：中小企業のためのセキュリティインシデント対応の手引き」において、サイバーインシデント対応の基本的なステップを把握することができる。また、インシデント発生時の駆け付け支援やサイバー保険等がワンパッケージで提供されるサイバーセキュリティお助け隊サービスの活用により、復旧工数の削減などが期待できる。こういった IPA の施策を中小企業が活用するために、業界団体や地域コミュニティとの連携による普及促進などが重要となる。

- 項目 25. 情報セキュリティ対策（上記 1～24 など）をルール化し、従業員に明示していますか？
  - 情報セキュリティ対策のルール化及び従業員への明示を行っていない、または実施状況が分からないと回答した企業の割合が 49 点以下の企業群では約 85%、50～69 点の企業群では約 35%となった。中小企業がサイバーセキュリティ対策を適切にルール化し、従業員へ周知するためには、IPA「中小企業の情報セキュリティ対策ガイドライン 付録 4：情報セキュリティハンドブック（ひな形）」をテンプレートとして活用することが効果的である。これにより、中小企業が自社の状況に合わせたサイバーセキュリティ対策の社内ルールを策定し、従業員への周知に活用することができる。また、これらの取り組みには経営層の関与が重要である。

5.4 SECURITY ACTION 宣言及びサイバーセキュリティお助け隊サービスを導入する中小企業が、中小企業全体の割合に対して低い水準となっている理由

本アンケート結果を元に、中小企業全体の割合に対して SECURITY ACTION 宣言とサイバーセキュリティお助け隊サービスの普及が進んでいない理由について分析を行った。

5.4.1 SECURITY ACTION 宣言について

ここでは、SECURITY ACTION 宣言を行う中小企業の割合が低い理由に関する分析を行う。

本分析では、SECURITY ACTION の宣言状況および認知度を明らかにし、また宣言したきっかけや、宣言によるメリットに関する認識、宣言しない理由などについて調査結果を分析し、普及が進んでいない理由と対応策を検討する。

分析の結果、SECURITY ACTION の認知度は約 10%であり、SECURITY ACTION 宣言をしている企業の割合は約 6%であった。SECURITY ACTION を宣言する中小企業の割合が低いことが改めて明らかになり、その理由として中小企業における SECURITY ACTION の認知度が低いことが大きな課題であることが分かった。また、認知度以外の課題としては小規模企業者では SECURITY ACTION の必要性を感じない企業が多く、小規模企業者以外の中小企業ではセキュリティ人材の不足や費用対効果の不明瞭が挙げられている。

一方で設問 Q63 のアンケート結果から、SECURITY ACTION の宣言を維持できている企業は 87.3%で、継続的にサイバーセキュリティ対策が実施されており、宣言後の変化としての意義やメリットを認識している企業が多い可能性を示しており、宣言を行うことが企業のサイバーセキュリティ対策に一定の影響を与えていると考えられる。

SECURITY ACTION という制度が中小企業に基本的なセキュリティ対策を促すための施策であることを踏まえると、経営層を対象として、引き続き広報活動に力を入れ、SECURITY ACTION 取得を行うことによるメリットを明確に示すことが望ましい。

(1) SECURITY ACTION 宣言の認知度の分析

アンケート回答結果から SECURITY ACTION 宣言の認知度について、企業規模および業種ごとに分析を行った。

分析の結果、SECURITY ACTION 宣言の認知度は約 10%となった。企業規模別では、企業規模が大きくなるほど認知度が上がっていることが明らかになった。従業員数の増加による認知機会の増加や、サイバーセキュリティ担当部署等の設置が理由として考えられる。

業種別にみると、認知度が高い業種は運輸業、郵便業、情報通信業、複合サービス業であり、約 20%となった。これらの業種は情報セキュリティが業務の重要な要素であるため、セキュリティ対策に関する情報へのアンテナが高く、制度の認知度が高まっていると考えられる。一方で認知度が低い業種は小売業、生活関連サービス、娯楽業、不動産業、物品賃貸業となっており、約 5%となった。これらの業種は直接的なセキュリティリスクを感じにくい業務特性や、規制の関与が少ないことが、制度に対する認知の優先順位を下げていると考えられる。なお、業種別の回答数が少ない農業、林業、漁業、工業、採石業、砂利採取業は除外している。

1）企業規模別の認知度

企業規模別の SECURITY ACTION の認知度は以下の通りである。

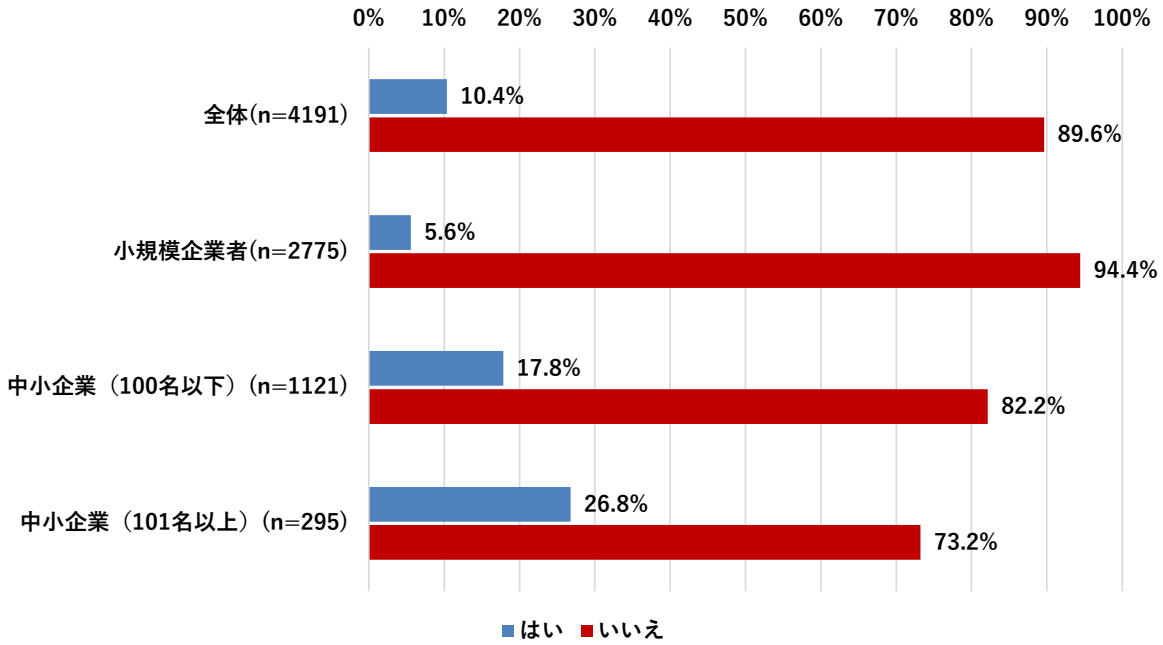

図 5-50 企業規模別の SCURITY ACTION の認知度(n=4191)

2）業種別の認知度

業種別の SECURITY ACTION の認知度は以下の通りである。

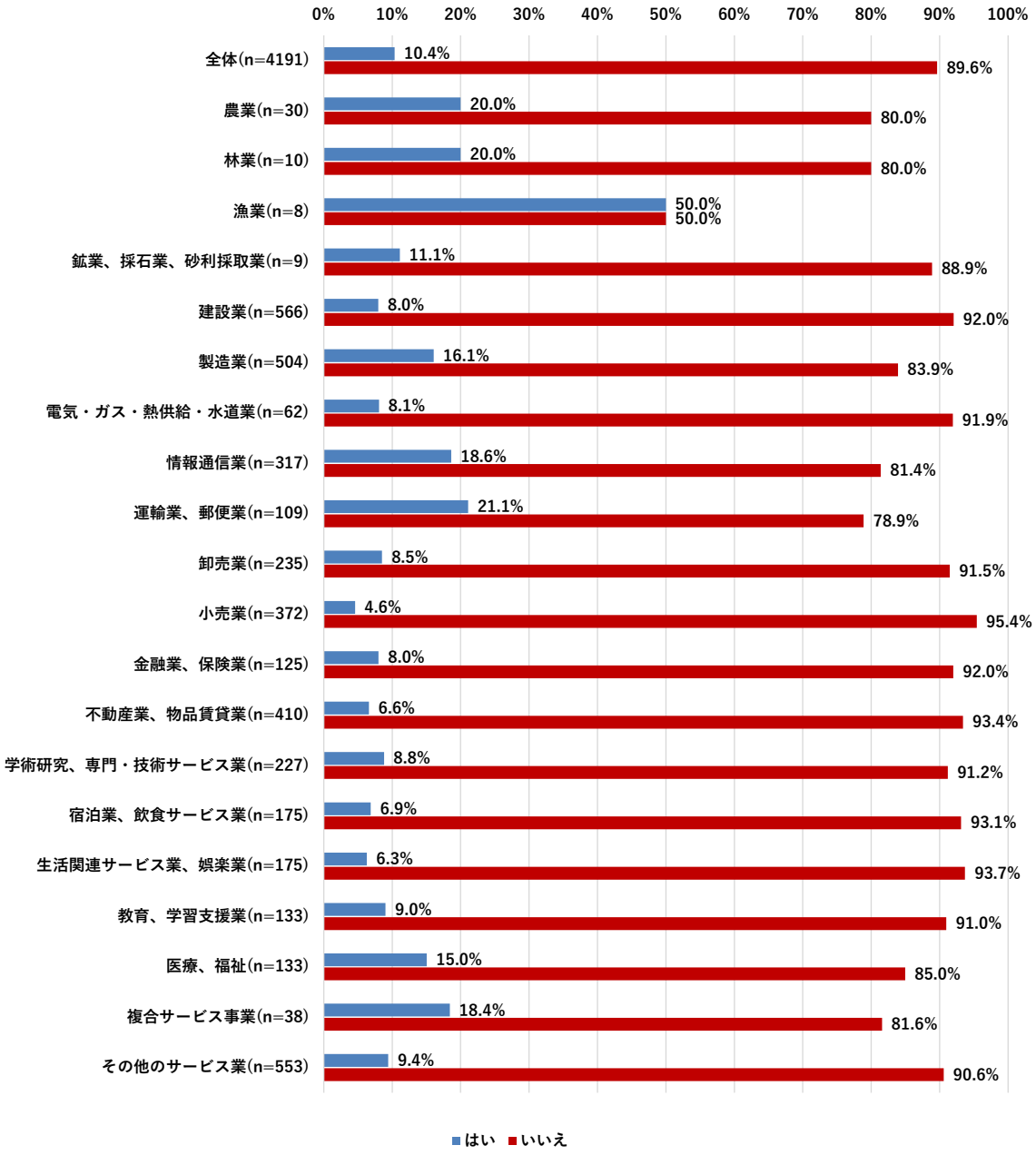

図 5-51 業種別の SECURITY ACTION の認知度(n=4191)

(2) SECURITY ACTION の宣言状況の分析

アンケート結果から SECURITY ACTION の宣言状況を企業規模および業種ごとに分析した。

分析の結果、SECURITY ACTION 一つ星または二つ星を宣言している割合は、全体の約 6%に留まっている。企業規模別にみると、企業規模が大きくなるほど宣言割合が上がっていることが明らかになった。

業種別にみると、宣言割合が高い業種として製造業、運輸業、郵便業、医療、福祉が挙げられ、約10%となった。一方で宣言割合が低い業種として、金融業、保険業小売業、不動産業、物品賃貸業となっていて約 3%となった。なお、業種別の回答数が少ない農業、林業、漁業、工業、採石業、砂利採取業は除外している。

宣言したきっかけでは、SECURITY ACTION 一つ星においては、補助金や助成金の申請要件を挙げた企業が最も多く、約 60%となった。また、次に多かったきっかけとしては、顧客や取引先からの要求であり約 45%となった。一つ星に求められる対策項目はサイバーセキュリティ対策において基本的な内容となっているため、補助金や助成金の申請をきっかけとした宣言が多いものと考えられる。また、SECURITY ACTION 二つ星においては、顧客や取引先からの要求をきっかけとして宣言した企業が最も多く、約 55%となった。また、次に多かったきっかけとして、経営層の意識向上が挙げられ、約 50%となった。二つ星は、一つ星と比較して求められる対策項目数も増えていることから、サイバーセキュリティ対策の実施による取引先へのアピールや自社への安心感を期待していることが考えられる。

SECURITY ACTION の宣言を維持するために必要な要素としては予算の確保と専門知識を持った人材の確保が挙げられ、各々約 55%となった。また SECURITY ACTION 二つ星に関しては経営層の関与が重要であることが示されている。

SECURITY ACTION を実施しない理由として最も大きな割合を示したのが認知度であり、「知らなかった」の回答が最も多かった。その他の理由として、小規模企業者においてはセキュリティ対策の必要性、それ以外の中小企業では、費用対効果の不明瞭、セキュリティ人材の不足、リソース不足等が挙げられた。

1） 企業規模別の宣言状況

企業規模別の SECURITY ACTION 宣言状況は以下の通りである。

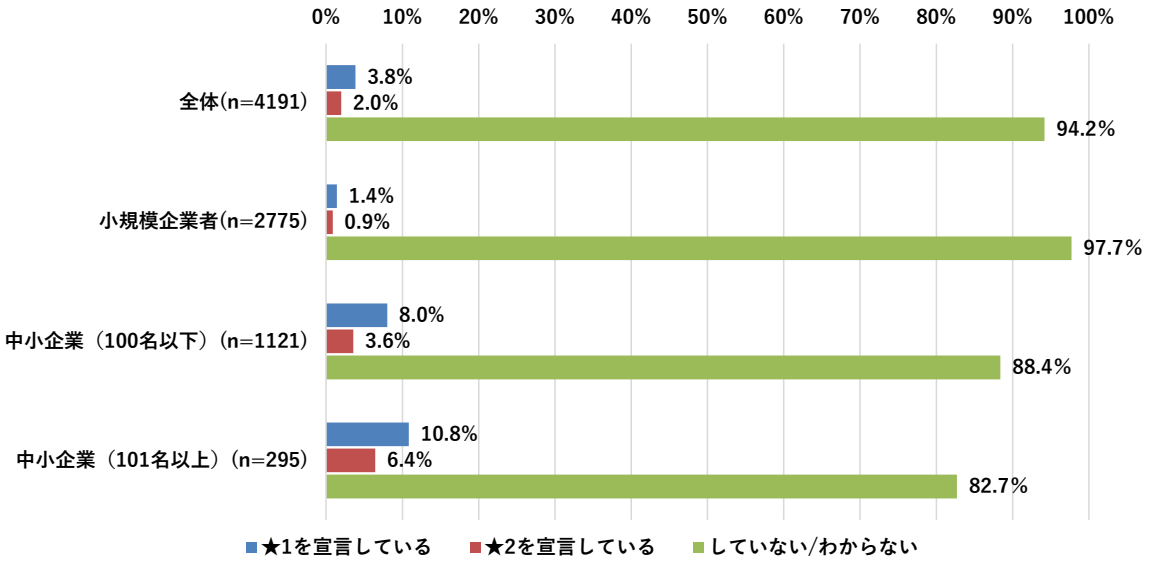

図 5-52 企業規模と SECURITY ACTION の実施の関係(n=4191)

2） 業種別の宣言状況

業種別の SECURITY ACTION 宣言状況は以下の通りである。

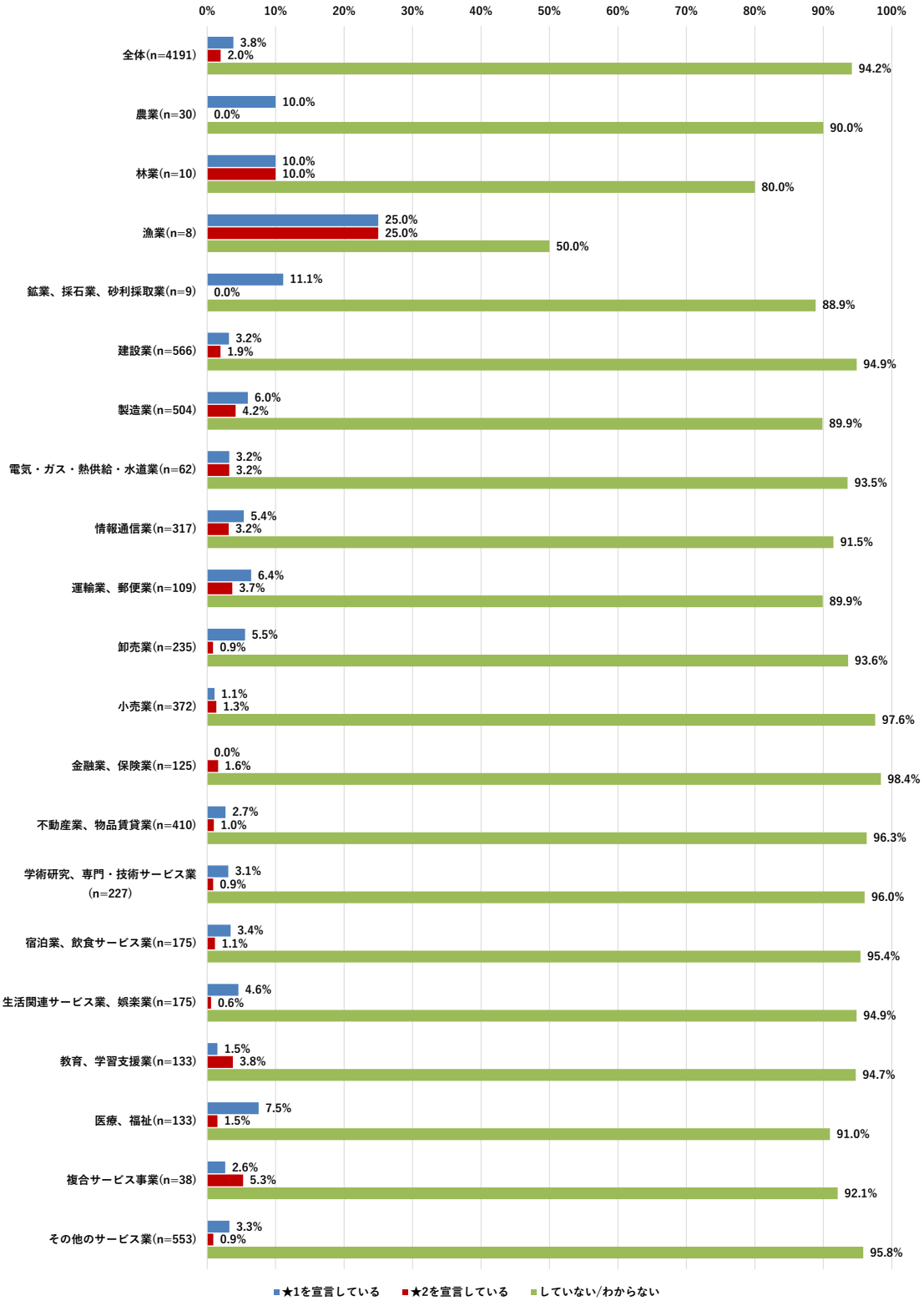

図 5-53 業種と SECURITY ACTION の実施の関係(n=4191)

3) SECURITY ACTION 宣言したきっかけ

SECURITY ACTION 宣言を行ったきっかけは以下の通りである。

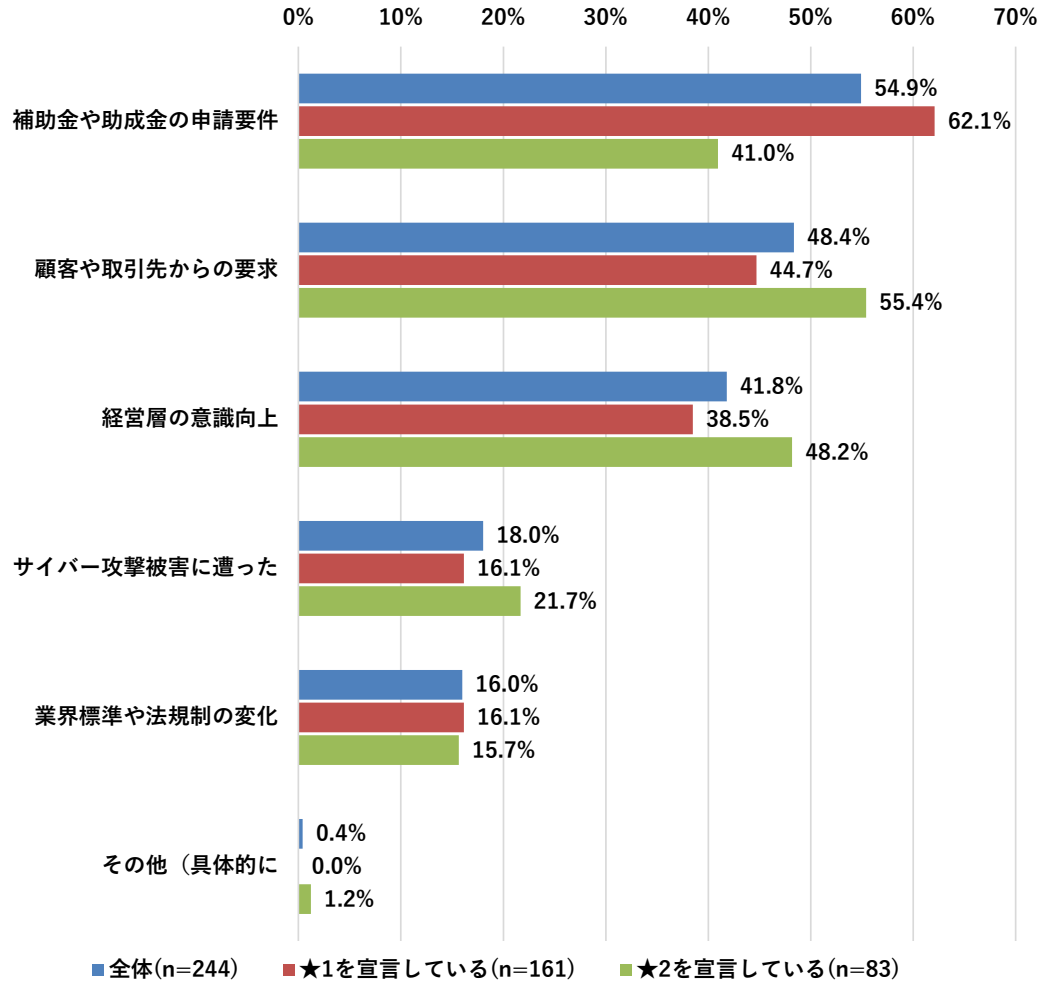

図 5-54 SECURITY ACTION 宣言状況と SECURITY ACTION を宣言したきっかけの関係(n=244)

4）SECURITY ACTION 宣言状況と自社診断の合計点

a. 一つ星宣言

SECURITY ACTION 一つ星の宣言状況と、アンケート設問 Q80 の項目のうち一つ星宣言に必要な 5 項目について「1. 実施している」または「2. 一部実施している」と回答している企業(一つ星実施と称する)との関係を分析した結果は以下の通りである。

SECURITY ACTION 宣言をしていないまたはわからないと回答した企業のうち約28%は、設問 Q80 の結果からは一つ星の宣言に値するセキュリティ対策を実施していると考えられる企業であった。

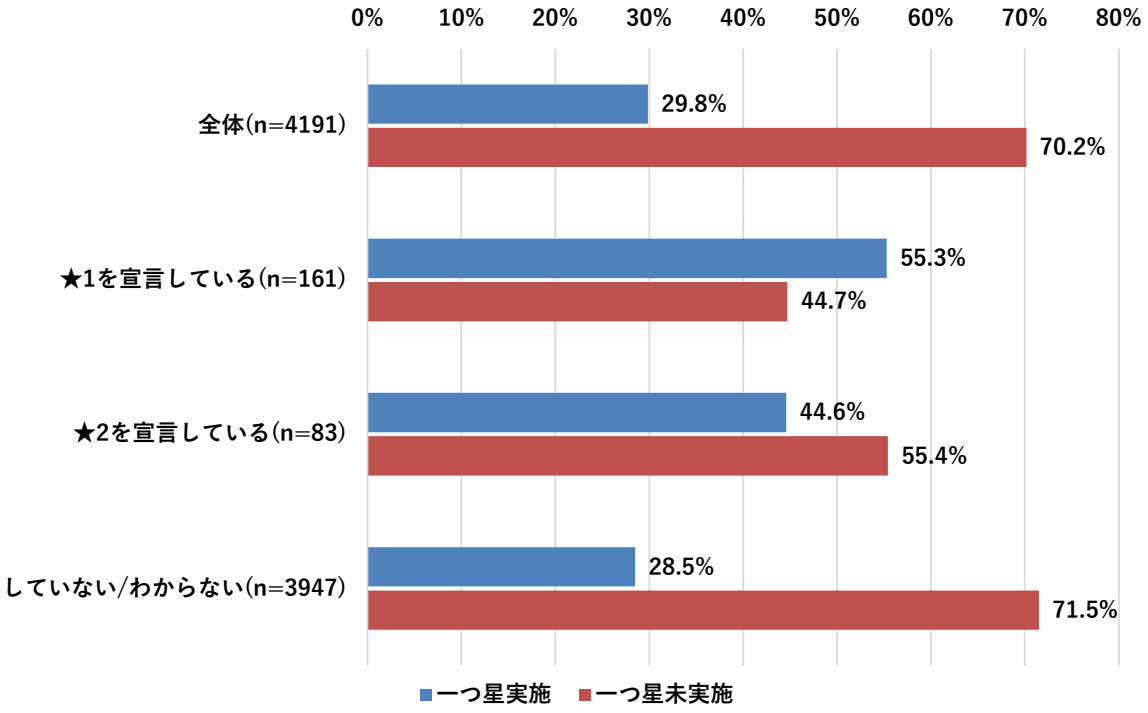

図 5-55 SECURITY ACTION の宣言状況と採点結果による SECURITY ACTION 一つ星の各項目の実施状況(n=4191)

b. 二つ星宣言

SECURITY ACTION 二つ星の宣言状況と設問 Q80 の結果を IPA「5 分でできる！情報セキュリティ自社診断」の基準に基づいて得点化した自社診断の合計点との関係性を分析した結果は以下の通りである。

SECURITY ACTION 宣言をしていないまたはわからないと回答した企業のうち約 2 割は、設問 80 の結果得られた自社診断の合計点に照らすと、SECURITY ACTION 二つ星に求められる対策項目を実施している企業(自社診断の合計点が 70 点以上の企業)であると考えられる。

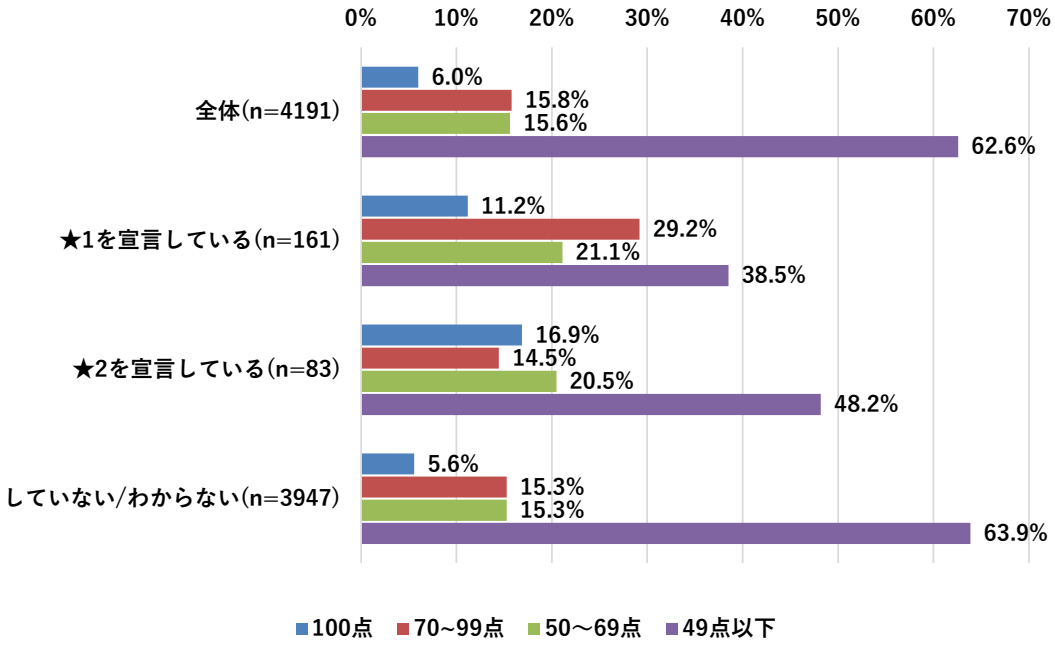

図 5-56 SECURITY ACTION の宣言状況と自社診断の合計点の関係(n=4191)

5) SECURITY ACTION 宣言を維持するために必要なこと

SCURITY ACTION 宣言をしている企業について、宣言を維持するために必要だと感じる要素の分析結果は以下の通りである。

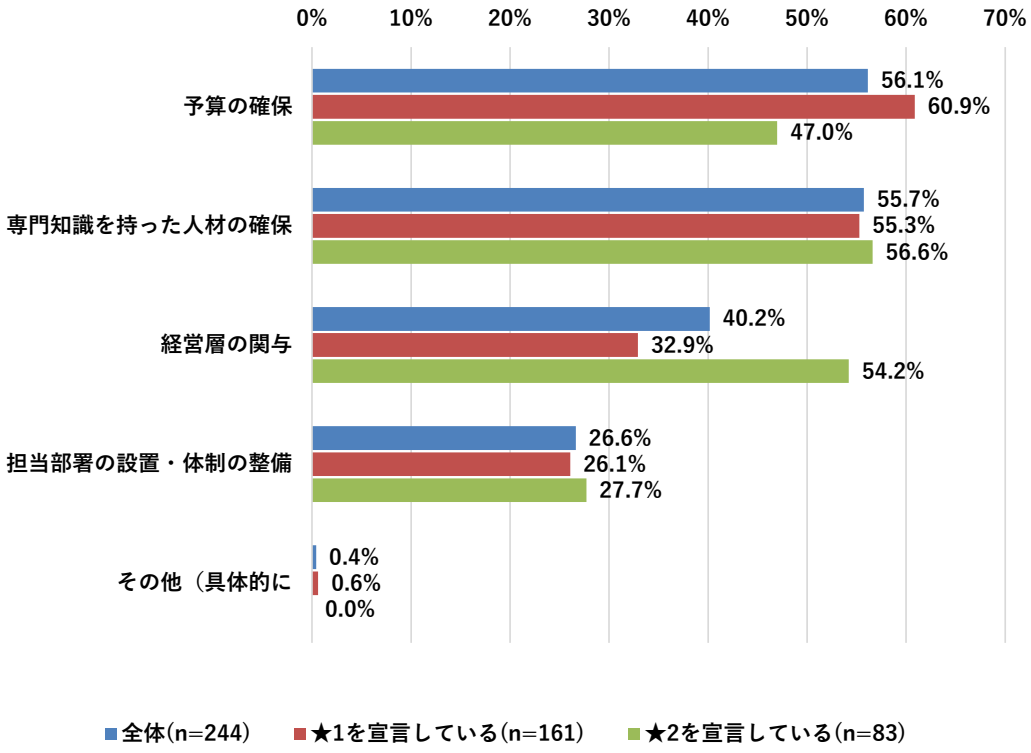

図 5-57 SECURITY ACTION の宣言状況と SECURITY ACTION の維持に必要な要素の関係(n=244)

6）SECURITY ACTION 宣言を行わない理由

SECURITY ACTION の宣言を行っていない企業について、SECURITY ACTION の宣言を行わない理由を企業規模別に分析した結果は以下の通り。

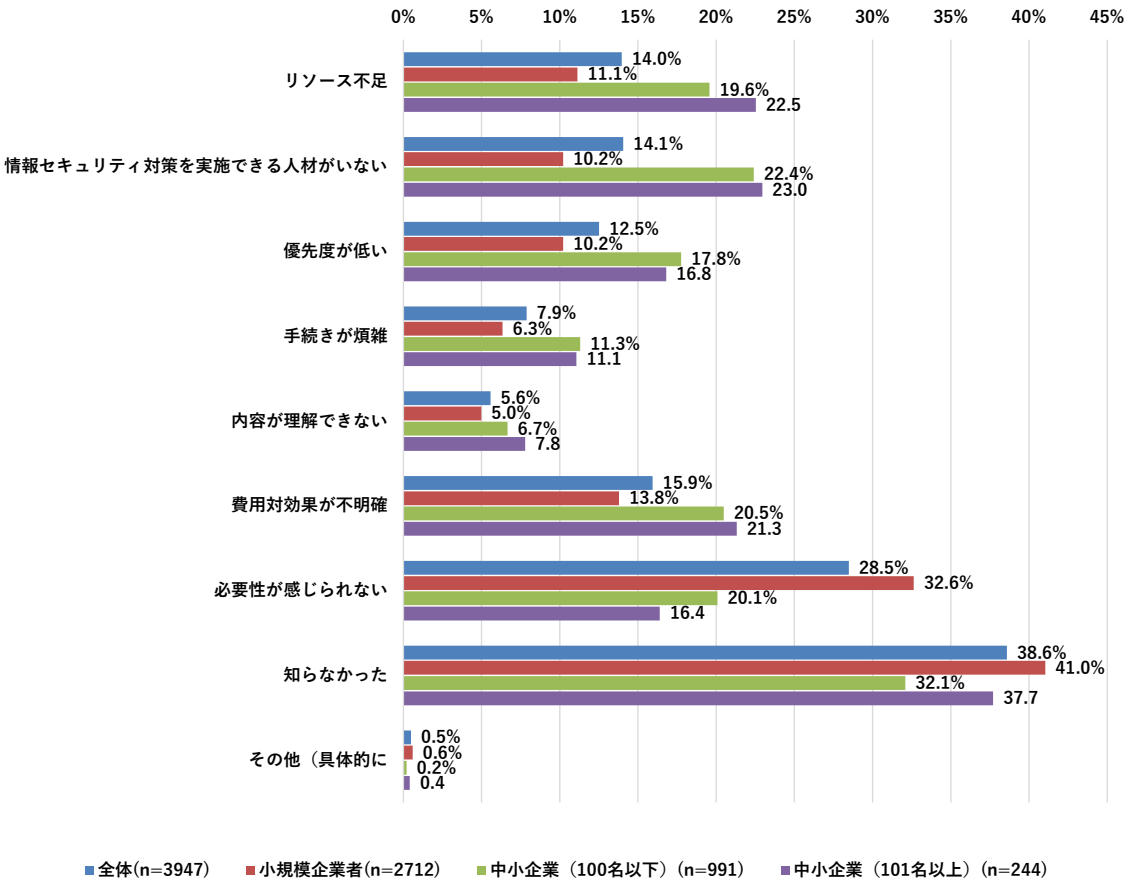

図 5-58 企業規模別の SECURITY ACTION を実施しない理由(n=3947)

（3）SECURITY ACTION の普及促進策の検討

SECURITY ACTION の普及促進策としては、広報活動で制度そのものを知ってもらうことが求められる。図 5-59 に示す通り、経営層(経営者、役員)の認知度が低いことが分かり、認知度向上のため、経営層へのアプローチが有効であると考えられる。また、中小企業が SECURITY ACTION の宣言を行う際、経営層が最終的な決断を行うことから、経営層の認知度向上が、SECURITY ACTION の普及促進の観点からも有効だと考えられる。

広報活動においては、図 5-60 に示されるように、セキュリティ対策を行っていることを対外的にアピールすることによる効果として、SECURITY ACTION の宣言状況と取引上のメリットとの関係性も示すことで、制度の普及促進が期待される。

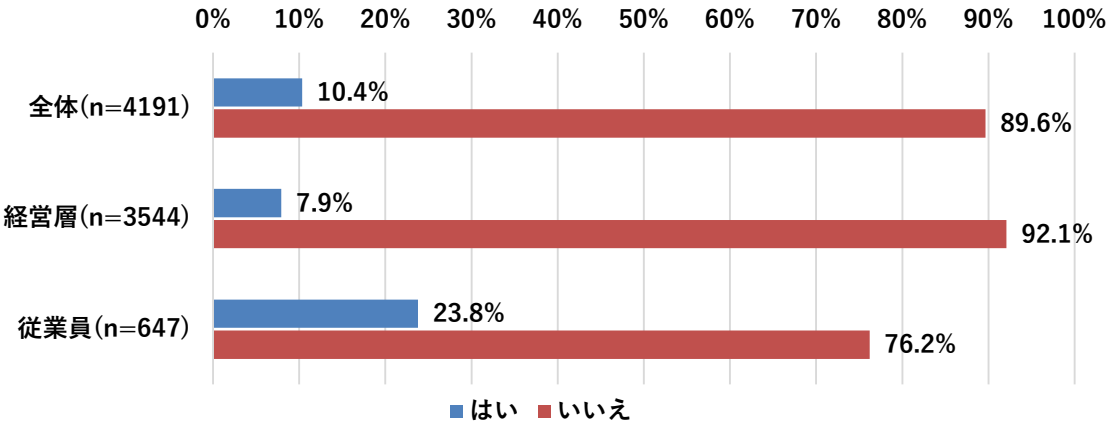

図 5-59 役職ごとの SECURITY ACTION を認知している割合(n=4191)

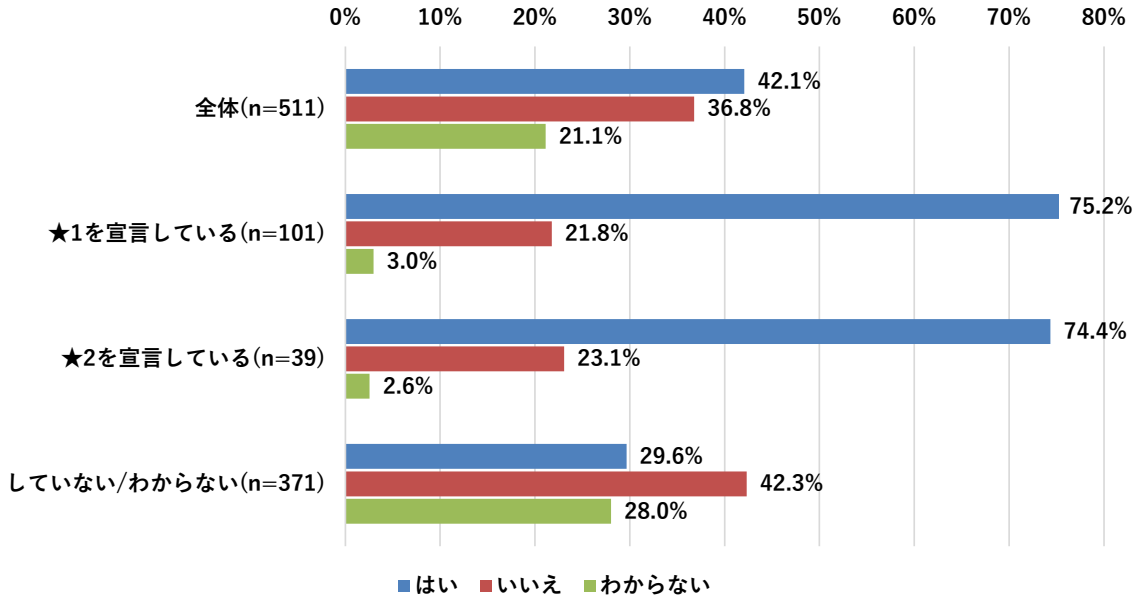

図 5-60 SECURITY ACTION 宣言の有無とセキュリティ要請に応じたことが取引につながったかの関係(n=511)

5.4.2 サイバーセキュリティお助け隊サービスについて

ここでは、サイバーセキュリティお助け隊サービスを導入する中小企業の割合が低い理由に関する分析を行う。

本分析では、サイバーセキュリティお助け隊サービスの導入状況および認知度を明らかにし、また導入のきっかけや導入によるメリットに関する認識、導入しない理由などについてアンケート調査およびインタビュー調査から得られた結果を分析し、導入割合が低い理由と対応策を検討する。

分析の結果、本サービスを導入している企業が非常に限られていることが改めて明らかになり、この要因として中小企業の認知度の低さが大きな課題であることが分かった。一方で、導入している企業からは本サービスの特徴となるワンパッケージでの導入の容易性、低コストなどのメリットを感じていることも明らかになっており、導入をしない理由として挙がっている「リソース不足」や「費用対効果が不明確」といった点を考慮すると、サービス内容および導入によって得られる効果が中小企業に理解されていない点も大きな課題であると考えられる。

これらの課題解決には、経営層を対象として、サイバーセキュリティお助け隊サービスの内容と費用および導入によって得られる効果をより明確に示した上で、広報に引き続き力を入れていくことが有効であると考えられる。

(1) サイバーセキュリティお助け隊サービスの認知度の分析

アンケート回答結果からサイバーセキュリティお助け隊サービスの認知度について、企業規模および業種ごとに分析を行った。

分析の結果、サイバーセキュリティお助け隊サービスの認知度はアンケート回答企業のうち約 7%に留まり、さらにサービスを導入している企業の割合はわずか約 2%であった。サイバーセキュリティお助け隊サービスが中小企業向けの施策であることを踏まえると、認知度は低く、広報活動に力を入れることが望ましいと考えられる。

企業規模別にみると、企業規模が大きくなるほど認知度が上がっていることが明らかになった。従業員数の増加による認知機会の増加や、サイバーセキュリティ体制の整備、担当部署等の設置により認知度が向上していることが考えられる。

業種別にみると、運輸業、郵便業、医療、福祉、製造業では業種別の認知度が 10%を超えているなど、全体の認知度に比べて高い傾向にあることが分かった。これらの業種ではサイバーセキュリティ対策が直接的に業務の安全性や信頼性に影響を与えるため、サイバーセキュリティ対策への関心が高まっていると考えられる。一方で全体に比べて認知度が低い業種は、小売業、宿泊業、飲食サービス業、不動産業、物品賃貸業であり、2～4%程度であった。これらの業種はセキュリティ対策への意識が業務に直結しづらい場合があり、その結果として対策に対する認知度が低いと考えられる。なお、業種別の回答数が少ない農業、林業、漁業、工業、採石業、砂利採取業は除外している。

1) 企業規模別の認知度

企業規模別のサービスの認知度は以下の通りである。

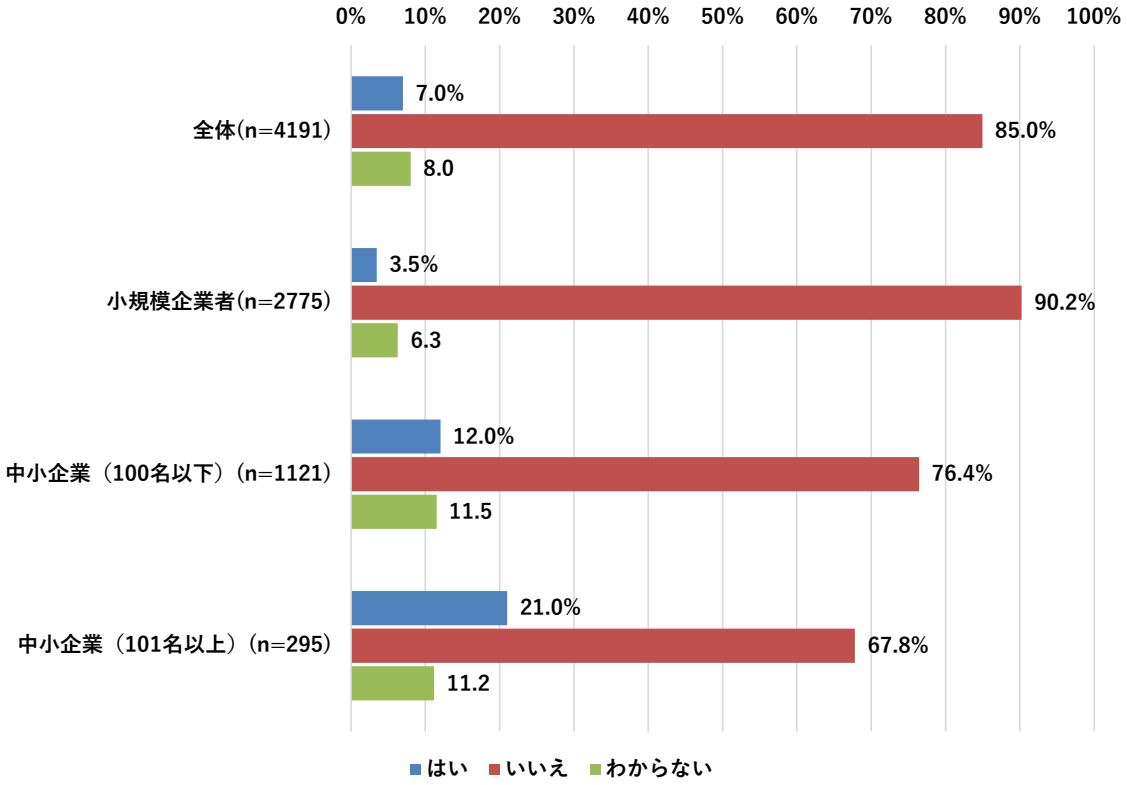

図 5-61 企業規模別のサイバーセキュリティお助け隊サービスの認知度(n=4191)

2）業種別の認知度

業種別のサービスの認知度は以下の通りである。

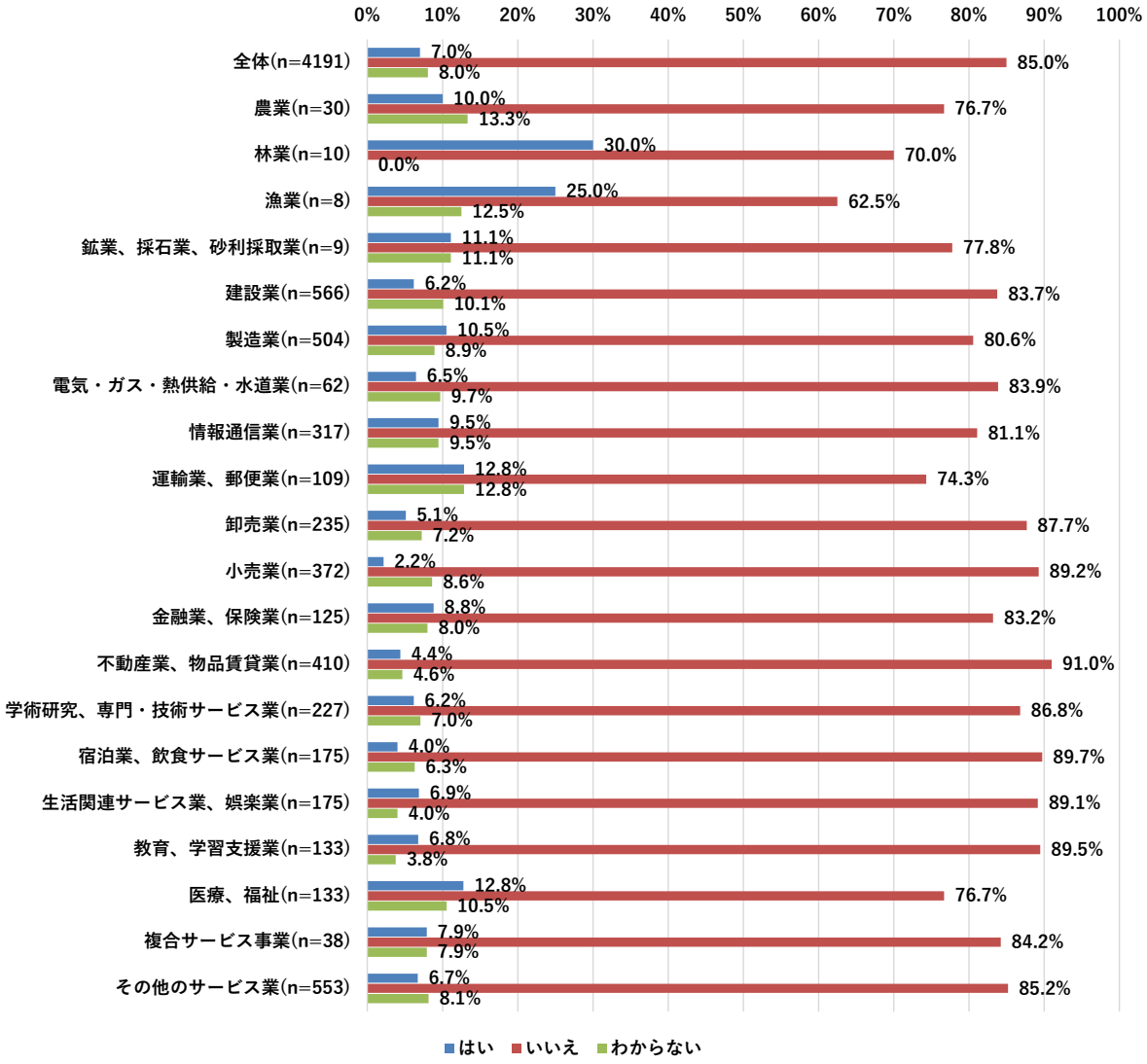

図 5-62 業種とサイバーセキュリティお助け隊サービスの認知度の関係(n=4191)

(2) サイバーセキュリティお助け隊サービスの導入状況の分析

アンケート結果からサイバーセキュリティお助け隊サービスの導入状況について企業規模および業種ごとに分析した。

分析の結果、全体的な導入割合はアンケート回答企業の約 2%であった。企業規模別にみると、企業規模が大きくなるほど導入割合が上がっていることが明らかになった。中小企業(101 名以上)では導入割合が 8.8%であるが、一方で小規模企業者では 1%未満であり、小規模企業者にはほとんど普及していない実態が明らかになった。

業種別にみると、導入割合が高い業種は運輸業、郵便業、医療、福祉、製造業であり、約 5%であった。一方で導入割合が低い業種は小売業、金融業、保険業、不動産業、物品賃貸業であり約 1%と低い状況であった。なお業種別の分析では回答数が少ない農業、林業、漁業、工業、採石業、砂利採取業は除外している。

サイバーセキュリティお助け隊サービスを導入している企業における導入のきっかけを分析した結果、補助金や助成金の申請要件との回答が最も多く、特に小規模企業者では約 75%であり、補助金や助

成金が中小企業のサービス導入判断に大きく影響していることが明らかになった。また、中小企業（100名以下）では顧客や取引先からの要求の割合が高く、補助金や助成金の申請要件との回答と同程度の割合（約 57%）であった。中小企業（101 名以上）では経営層の意識向上が 53.8%となっており、この規模の企業群では顧客や取引先からの要求、経営者の意向がサービス導入につながることが分かった。

導入をしていない理由としては、必要性が感じられないと回答した割合が最も高く、企業規模別でみると、特に小規模企業者の約 50%が回答している。小規模企業者以外では、費用対効果が不明確や優先度が低いといった回答が見られた。また、業種別ではどの業種においても、必要性が感じられない、費用対効果の不明瞭が挙げられていた。サイバーセキュリティお助け隊サービスの導入よる効果を明示的に示すことが望ましいと考えられる。

サイバーセキュリティお助け隊サービスを導入してよかった点としては、ワンパッケージでの情報セキュリティ対策、導入が容易であることがそれぞれ約 5 割と最も多く挙げられており、またコストの削減が約 3 割となっていることから、サービスの導入により中小企業の人的リソース不足の課題解決やコスト削減による費用対効果の改善などにつながっているケースがあることが読み取れる。

1） 企業規模別の導入状況

企業規模別の導入状況は以下の通りであった。

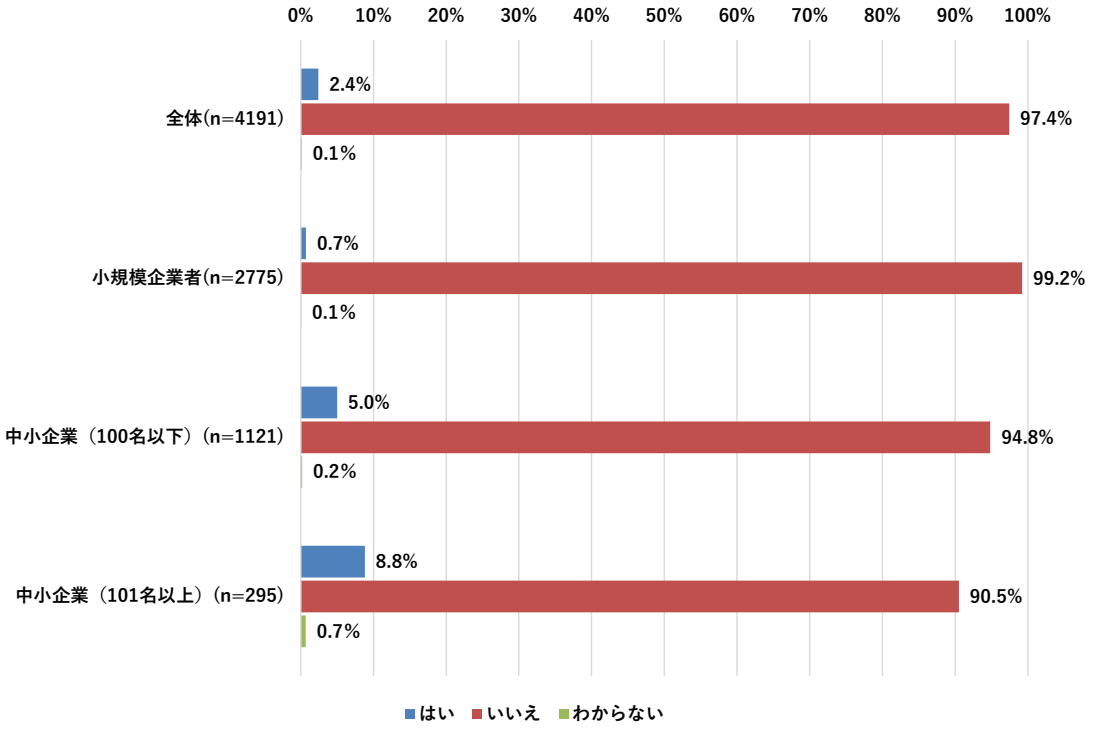

図 5-63 企業規模別のサイバーセキュリティお助け隊サービスの導入率（n=4191）

2） 業種別の導入状況

業種別の導入状況は以下の通りであった。

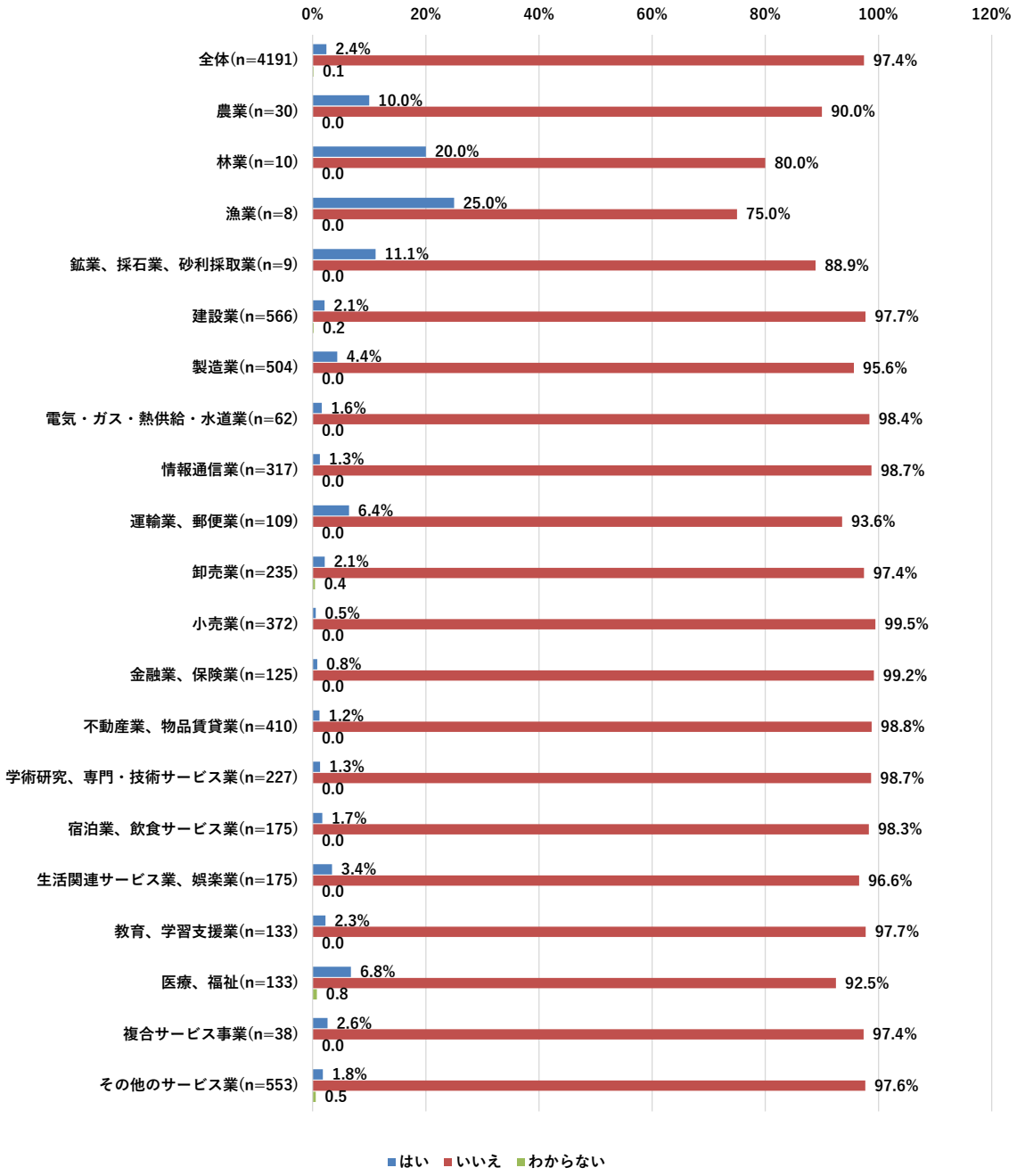

図 5-64 業種別のサイバーセキュリティお助け隊サービスの導入率(n=4191)

3）導入したきっかけ

サイバーセキュリティお助け隊サービスを認知している企業について、企業規模別に導入したきっかけを分析した結果は以下の通りであった。

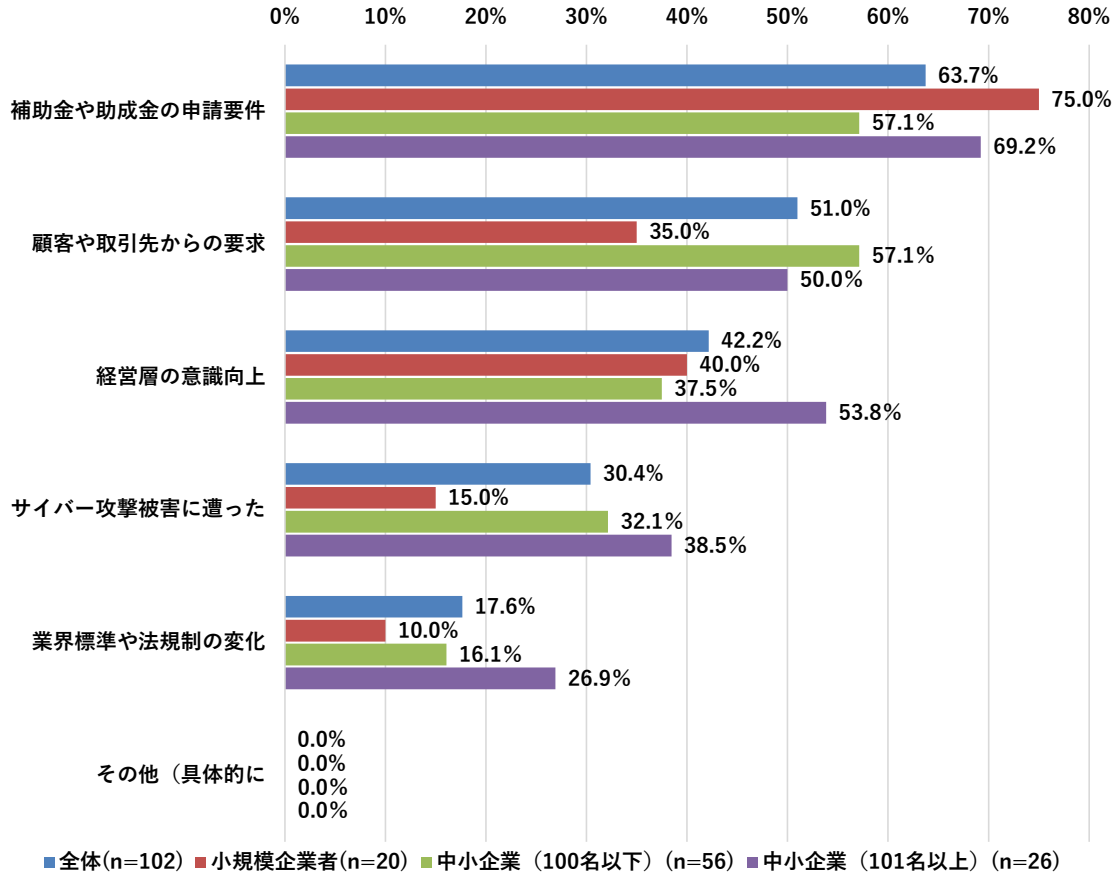

図 5-65 企業規模別のサイバーセキュリティお助け隊サービスを導入したきっかけ(n=102)

4）導入していない理由

サイバーセキュリティお助け隊サービスの導入を行っていない企業に対してサイバーセキュリティお助け隊サービスの導入を行わない理由を企業規模および業種ごとに分析した結果は以下の通りである。

a. 企業規模別の導入していない理由

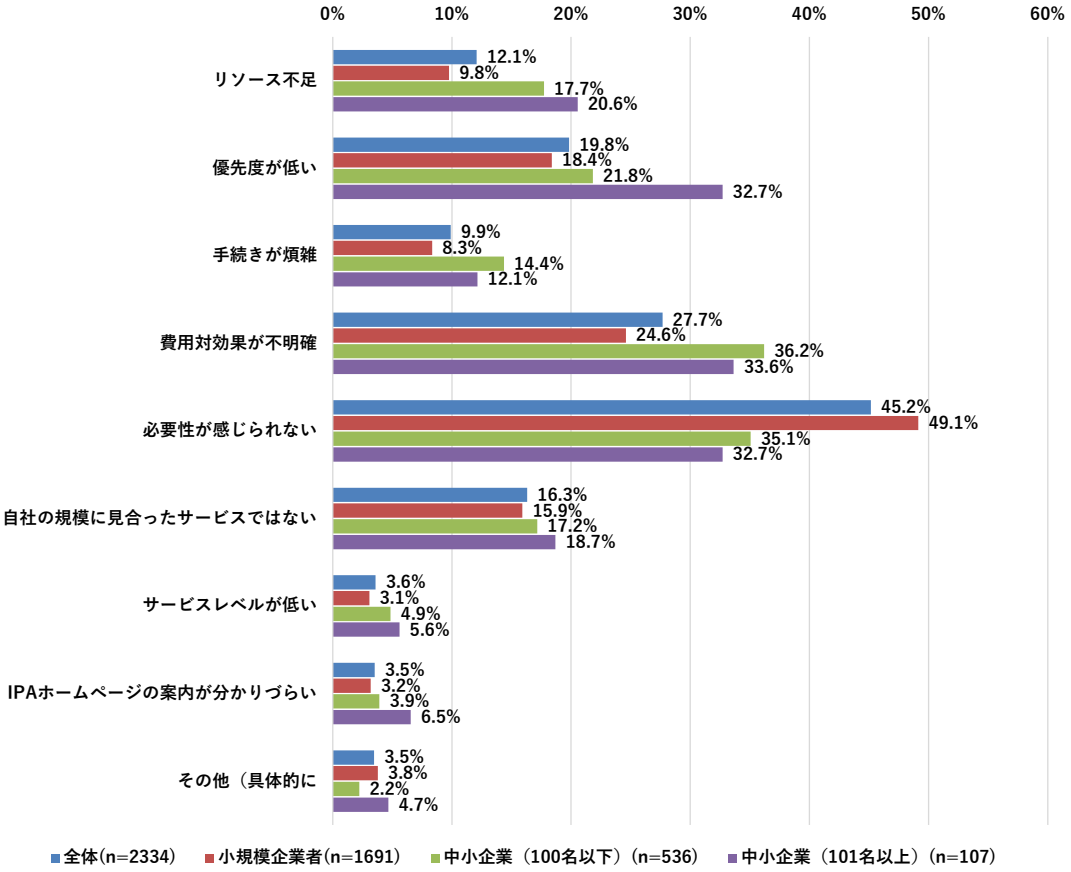

図 5-66 企業規模とサイバーセキュリティお助け隊サービスを導入しない理由の関係(n=2334)

b. 業種別の導入していない理由

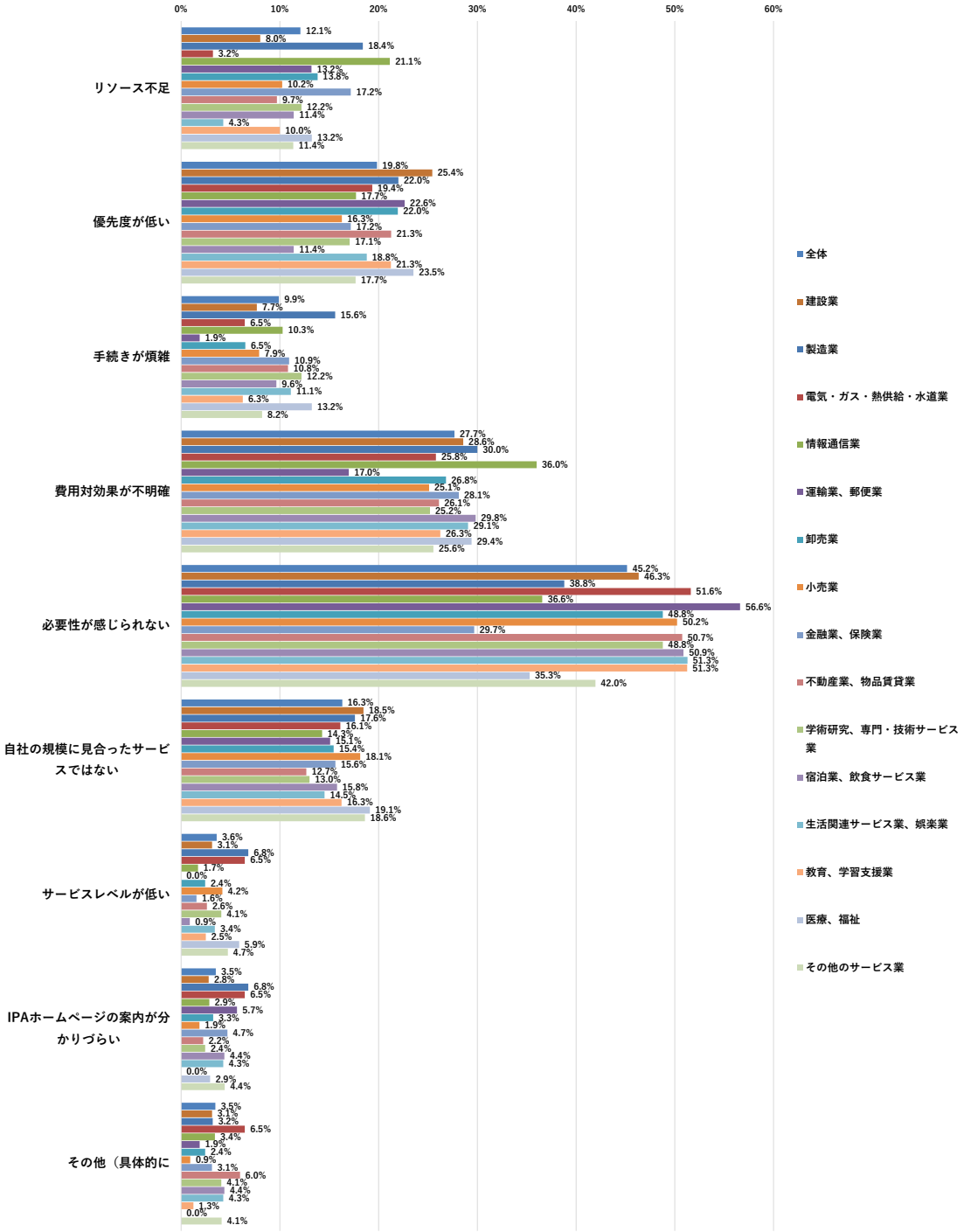

図 5-67 業種別のサイバーセキュリティお助け隊サービスを導入しない理由(n=2334)

5）導入してよかった点

サイバーセキュリティお助け隊サービスを導入している企業に対して、導入してよかった点を問うQ73 の回答結果は以下の通りである。(3.2.9 の結果を再掲)

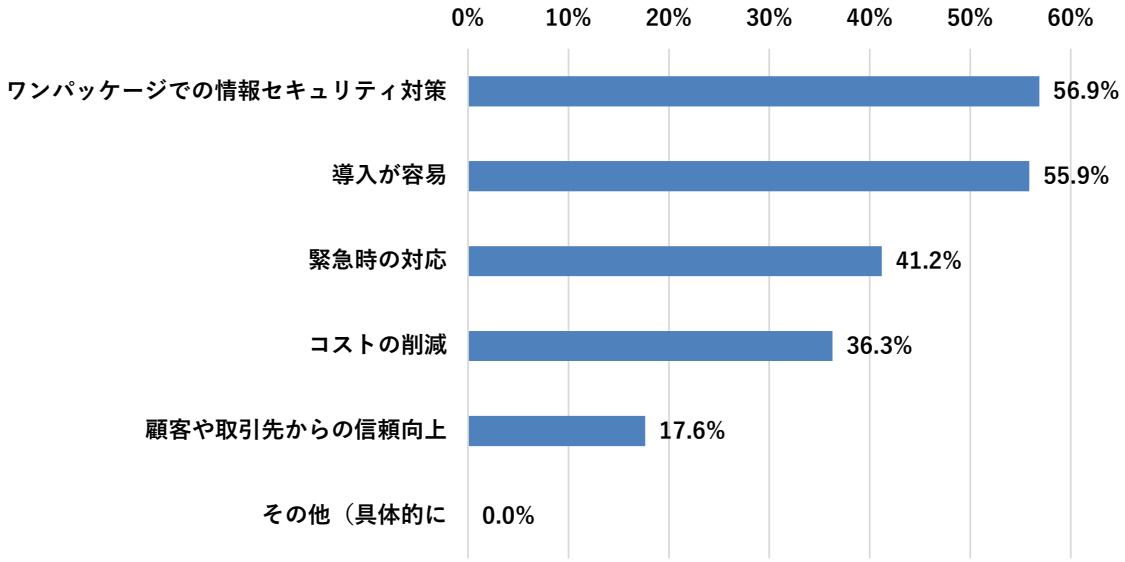

図 5-68 「サイバーセキュリティお助け隊サービス」を導入して良かった点(n=102)

（3）サイバーセキュリティお助け隊サービス隊の普及促進策の検討

サイバーセキュリティお助け隊サービスの普及促進策としては、広報活動で制度そのものを知ってもらうことが求められるが、図 5-69 役職ごとのサイバーセキュリティお助け隊サービス隊を認知している割合（n=4191）に示す通り、経営層（経営者、役員）の認知度が低いことが明らかになっており、経営層へのアプローチがサイバーセキュリティお助け隊サービス隊の普及促進の観点からも有効であると考えられる。

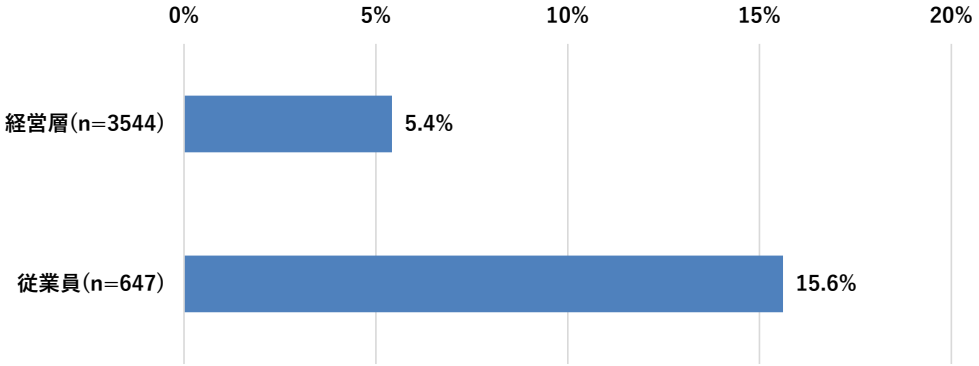

図 5-69 役職ごとのサイバーセキュリティお助け隊サービス隊を認知している割合（n=4191）

6. 参考資料(アンケート調査項目)

＜概要設問＞

【SC1】 あなたがお勤め・経営されている企業の業種を教えてください。(SA)

1. 農業	2. 林業	3. 漁業
4. 鉱業、採石業、砂利採取業	5. 建設業	6. 製造業
7. 電気・ガス・熱供給・水道業	8. 情報通信業	9. 運輸業、郵便業
10. 卸売業	11. 小売業	12. 金融業、保険業
13. 不動産業、物品賃貸業	14. 学術研究、専門・技術サービス業	15. 宿泊業、飲食サービス業
16. 生活関連サービス業、娯楽業	17. 教育、学習支援業	18. 医療、福祉
19. 複合サービス事業	20. その他のサービス業	21. 働いていない

【SC1sq】 あなたがお勤め・経営されている企業の業種(分類)を教えてください。(SA)

1. 電気小売業	2. ガス小売業
3. 上記以外の電気・ガス・熱供給・水道業	4. 宿泊
5. 飲食店	6. 持ち帰り・配達飲食サービス業
7. 放送業	8. 情報サービス業
9. 映像情報制作・配給業	10. 音声情報制作業
11. 広告制作業	12. 映像・音声・文字情報制作に附帯するサービス業
13. 上記以外の情報通信業	14 .レッカー・ロードサービス業
15. 上記以外の運輸業、郵便業	16. 駐車場業
17 .物品賃貸業	18. 上記以外の不動産業、物品賃貸業
19. 旅行業	20. 上記以外の生活関連サービス業、娯楽業

【SC2】 あなたがお勤め・経営されている企業の総従業員数を教えてください。※2024 年度当初の人数 (SA)

1. 5 名以下	2. 6～20 名以下	3. 21～50 名以下
4. 51～100 名以下	5. 101～300 名以下	6. 301 名以上

【SC3】 貴社の資本金について教えください。※直近会計年度の金額 (SA)

1. 1000 万円以下	2. 1000 万円超～3000 万円以下
3. 3000 万円超～5000 万円以下	4. 5000 万円超～1 億円以下
5. 1 億円超～2 億円以下	6. 2 億円超～3 億円以下
7. 3 億円超	8. わからない

【SC4】 あなたがお勤め・経営されている企業において、あなたご自身の役職・担当業務をお教えください。(SA)

1. 経営者	2. 役員
3. IT または情報セキュリティ担当者	4. 一般社員(IT または情報セキュリティ担当者以外)

【SC5】 あなたがお勤め・経営されている企業において、あなたは自社のサイバーセキュリティ対策の投資にどのように関与しているか教えてください。(SA)

1. 経営層として意思決定する立場	2. 経営層に提案・助言、判断を支援する立場
3. 経営層ではないが主な担当として判断する立場	4. 経営層の意向を把握して回答ができる立場
5. セキュリティ対策の投資判断に関与していない	6. その他

＜本設問＞

【Q1】 貴社の所在地(本社所在地)を教えてください。(SA)

1. 北海道	2. 東北(青森、岩手、秋田、宮城、山形、福島)
3. 北関東(茨城、栃木、群馬、山梨、長野)	4. 南関東(埼玉、千葉、東京、神奈川)
5. 東海(静岡、岐阜、愛知、三重)	6. 北陸(新潟、富山、石川、福井)
7. 近畿(滋賀、京都、奈良、和歌山、大阪、兵庫)	8. 中国(鳥取、島根、岡山、広島、山口)
9. 四国(徳島、香川、愛媛、高知)	10. 九州・沖縄(福岡、佐賀、長崎、大分、熊本、宮崎、鹿児島、沖縄)

【Q2】 貴社の総売上高(単体)について教えください。※直近会計年度の金額 (SA)

1. 1000 万円以下	2. 1000 万円超～3000 万円以下
3. 3000 万円超～5000 万円以下	4. 5000 万円超～1 億円以下
5. 1 億円超～2 億円以下	6. 2 億円超～3 億円以下
7. 3 億円超	8. わからない

【Q3】 貴社は業界団体（貴社の業種に関連する業界団体、商工会議所、商工会・中小企業団体中央会等）に加入していますか。（SA）

1. はい（加入団体名をすべて記述：　）	2. いいえ	3. わからない

【Q4】 貴社がグループ会社の場合、親会社のセキュリティ方針に沿った対応を行っていますか。（SA）

1. セキュリティ対策方針は親会社が決めている
2. グループ会社ではあるが、自社でも一部のセキュリティ方針を決めている
3. グループ会社ではない

【Q5】 貴社では経営資源の確保や業務の効率化に IT を活用されていますか。情報セキュリティ対策サービス以外で利用・導入されているサービスやシステムについて教えてください。 あてはまるものを下記よりすべてお選びください。（MA）

1. 電子メール（フリーメール・汎用ドメイン等）	2. 電子メール（貴社独自ドメイン）
3. 顧客管理システム（CRM）	4. Web サイト、ホームページの開設
5. インターネットを活用した流通・決済（例：ネット販売等）	6. 会計システム・アプリケーション
7. 人事システム・アプリケーション	8. 給与システム・アプリケーション
9. 出退勤管理システム	10. 稟議システム
11. 文書管理システム	12. 生産管理システム
13. コミュニケーションツール	14. オンライン会議システム
15. クラウドストレージ・無料	16. クラウドストレージ・有料
17. クラウドファンディング	18. VPN
19. IoT 機器	20. その他（具体的に
21. 特に活用していない	

【Q6】 貴社における、直近過去 3 期の IT 投資額（情報セキュリティ投資額を含む）と、情報セキュリティ対策投資額（IT 機器や社員への教育等も含む）の概算について教えてください。（SA）

［Q6 項目 1］ IT 投資額（情報セキュリティ対策投資額を含む）

1. 投資していない	2. 100 万円未満
3. 100 万円～500 万円未満	4. 500 万円～1000 万円未満
5. 1000 万円～2000 万円未満	6. 2000 万円～5000 万円未満
7. 5000 万円～1 億円未満	8. 1 億円～4 億円未満
9. 4 億円以上	10. わからない

［Q6 項目 2］ 情報セキュリティ対策投資額（IT 機器や社員への教育等も含む）

1. 投資していない	2. 100 万円未満
3. 100 万円～500 万円未満	4. 500 万円～1000 万円未満
5. 1000 万円～2000 万円未満	6. 2000 万円～5000 万円未満
7. 5000 万円～1 億円未満	8. 1 億円～4 億円未満
9. 4 億円以上	10. わからない

【Q7】 前問で情報セキュリティ対策投資額について「投資をしていない」とお答えになった一番の理由について教えてください。（SA）

1. コストがかかりすぎる	2. 費用対効果が見えない
3. どこからどう始めたらよいかわからない	4. 導入後の手間がかかる
5. 経営層の承認が得られない	6. その他（具体的に
7. 必要性を感じていない	

【Q8】 前問で情報セキュリティ対策投資について「必要性を感じていない」とお答えになった理由について教えてください。あてはまるものを下記よりすべてお選びください。（MA）

1. サイバーセキュリティ被害にあうと思わないため	2. 重要情報を保有していないため
3. 事業の継続に大きな影響がないため	4. 他社とのネットワーク接続がないため
5. 既に十分な対策がとられているから	6. その他（具体的に

【Q9】 貴社で情報セキュリティ対策を実施(強化)するきっかけとなった理由について教えてください。(MA)

1. 法令の制定や改訂への対応
2. 業界基準の制定、業界団体の呼びかけ
3. 取引先からの要請
4. 自社社員からの要請
5. 自社のサイバーインシデント
6. 他社のサイバーインシデント(ニュースを含む)
7. 対外(取引先、ユーザ等)へのアピール
8. セキュリティベンダーや IT 機器営業等からの勧奨
9. 同業他社の対策状況をみたこと
10. マイナンバー制度の開始
11. IT 関連業者・専門家(商工会議所・商工会・中小企業団体中央会等)
12. 重要情報(個人情報、営業秘密、技術情報等)の保持
13. その他(具体的に
14. 対策の必要性を感じたことがない

【Q10】 貴社が情報セキュリティ対策に期待する効果について教えてください。(MA)

1. 従業員の情報セキュリティへの意識向上
2. 対処すべきリスクの特定
3. ISMS・プライバシーマーク等の認証取得
4. サイバーインシデントによって発生するコスト削減
5. データの棚卸等による業務効率化の実現
6. データ利活用の推進
7. 既存の取引先からの信頼獲得
8. 取引機会(新規)の増加
9. 高度な情報管理が求められる新規事業の実現
10. 助成金・補助金の獲得
11. その他(具体的に
12. 特になし

【Q11】 貴社で情報セキュリティ対策を実施して感じられた具体的なメリットについて教えてください。(FA)

【Q12】 貴社では情報セキュリティ関連製品やソフトウェアを導入していますか。 導入している情報セキュリティ関連製品やソフトウェアを教えてください。 あてはまるものを下記よりすべてお選びください。(MA)

1. ウイルス対策ソフト・サービスの導入
2. ウェブ閲覧のフィルタリングソフトウェア
3. ファイアウォール
4. VPN
5. 暗号化製品(ディスク、ファイル、メール等)
6. ソフトウェアライセンス管理/IT 資産管理製品
7. ワンタイムパスワード、IC カード、USB キー、生体認証等による個人認証
8. アイデンティティ管理/ログオン管理/アクセス許可製品
9. セキュリティ情報管理システム製品(ログ情報の統合・分析、システムのセキュリティ状態の統合的な管理機能)
10. クライアント PC の設定・動作・ネットワーク接続等を管理する製品(検疫ネットワークを含む)
11. メールフィルタリングソフトウェア(誤送信防止対策製品、スパムメール対策製品を含む)
12. その他(具体的に
13. 特に導入しているものはない

【Q13】 貴社が利用している又は利用したいと考えている情報セキュリティ関連製品やサービスの内、費用対効果が高いと考えているものを教えてください。 あてはまるものを下記よりすべてお選びください。(MA)

1. ウイルス対策ソフト・サービスの導入
2. ウェブ閲覧のフィルタリングソフトウェア
3. ファイアウォール
4. VPN
5. 暗号化製品(ディスク、ファイル、メール等)
6. ソフトウェアライセンス管理/IT 資産管理製品
7. ワンタイムパスワード、IC カード、USB キー、生体認証等による個人認証
8. アイデンティティ管理/ログオン管理/アクセス許可製品
9. セキュリティ情報管理システム製品(ログ情報の統合・分析、システムのセキュリティ状態の統合的な管理機能)
10. クライアント PC の設定・動作・ネットワーク接続等を管理する製品(検疫ネットワークを含む)
11. メールフィルタリングソフトウェア(誤送信防止対策製品、スパムメール対策製品を含む)
12. その他(具体的に
13. わからない

【Q14】 貴社ではサーバ等にセキュリティパッチを適用していますか。パッチを適用していない場合は理由について教えてください。 あてはまるものを下記よりすべてお選びください。（MA）

1. パッチを適用している
2. パッチの適用が悪影響を及ぼすリスクを避けるため適用していない
3. パッチ適用以外の手段が有効であるため適用していない
4. パッチを適用しなくても問題ないと判断したため適用していない
5. パッチの評価や適用に多大なコストがかかるため適用していない
6. その他（具体的に

【Q15】 貴社で情報漏洩等のインシデント又はその兆候を発見した場合に、規定されている報告先は何ですか。 あてはまるものを下記よりすべてお選びください。（MA）

1. 経営者への報告
2. 責任者への報告
3. 本人、関係者、取引先への連絡
4. 業界団体への報告
5. 官公庁への報告
6. その他（具体的に
7. 報告先は決まっていない
8. わからない

【Q16】 貴社で情報漏洩等のサイバーインシデント又はその兆候を発見した場合の対応方法として規定されているものは何ですか。 あてはまるものを下記よりすべてお選びください。（MA）

1. 情報の隔離
2. ネットワーク診断
3. サービスの停止
4. 専門家への相談
5. 原因の究明
6. 再発防止策の策定
7. 世間への発表
8. その他（具体的に
9. 対応方法は決まっていない
10. わからない

【Q17】 貴社は情報セキュリティ業務の外部委託（システム子会社への委託を含む）を行っていますか。行っている場合は、外部委託しているサービスについて教えてください。 あてはまるものを下記よりすべてお選びください。（MA）

1. 委託していない
2. 情報セキュリティ/BCP コンサルティングサービス（ISMS やプライバシーマークの取得などを含む）
3. CSIRT 構築支援サービス
4. 情報セキュリティ検査・監査サービス
5. Web アプリケーションぜい弱性検査サービス
6. ウイルス監視サービス
7. ファイアウォール運用管理サービス
8. 不正アクセス監視サービス
9. 統合セキュリティ監視サービス
10. DDoS 攻撃対策サービス
11. メールセキュリティサービス
12. イベントログ管理サービス
13. 情報セキュリティ教育・トレーニングサービス
14. メール標的型攻撃訓練サービス
15. セキュアファイル交換サービス
16. 電子認証サービス
17. その他（具体的に
18. わからない

【Q18】 情報セキュリティ業務の外部委託（システム子会社への委託を含む）をしている又はしたいと考えているものの内、費用対効果の高いものを教えてください。 あてはまるものを下記よりすべてお選びください。（MA）

1. 情報セキュリティ/BCP コンサルティングサービス（ISMS やプライバシーマークの取得などを含む）
2. CSIRT 構築支援サービス
3. 情報セキュリティ検査・監査サービス
4. Web アプリケーションぜい弱性検査サービス
5. ウイルス監視サービス
6. ファイアウォール運用管理サービス
7. 不正アクセス監視サービス
8. 統合セキュリティ監視サービス
9. DDoS 攻撃対策サービス
10. メールセキュリティサービス
11. イベントログ管理サービス
12. 情報セキュリティ教育・トレーニングサービス
13. メール標的型攻撃訓練サービス
14. セキュアファイル交換サービス
15. 電子認証サービス
16. その他（具体的に
17. わからない

【Q19】 貴社で現状以上の情報セキュリティ対策を実施するためには、どのような効果が期待できれば対策を行うと思いますか。あてはまるものを下記よりすべてお選びください。（MA）

1. 従業員の情報セキュリティへの意識向上	2. 対処すべきリスクの特定
3. ISMS・プライバシーマーク等の認証取得	4. トラブル未然防止による潜在的なコスト削減
5. サイバーインシデント発生時の復旧コスト削減	6. データの棚卸等による業務効率化の実現
7. データ利活用の推進	8. 既存取引先からの信頼獲得
9. 取引機会（新規）の増加	10. 高度な情報管理が求められる新規事業の実現
11. 助成金・補助金の獲得	12. その他（具体的に

【Q20】 貴社の情報セキュリティ対策を、さらに向上させるために必要と思うことは何ですか。 （MA）

1. 経営者のサイバーセキュリティリスク意識向上
2. 従業員の情報セキュリティ意識向上
3. 従業員への情報セキュリティ対策実践教育
4. 企業内の体制整備
5. 情報セキュリティ対策技術の習得・向上、対策ツールの利用・啓発
6. 地域での支援者育成や確保、サポートセンターの充実
7. その他（具体的に
8. 特にない

【Q21】 どのような情報セキュリティ対策に関するサービスがあれば活用したいと思いますか。 あてはまるものを下記よりすべてお選びください。（MA）

1, 経営層向けの手引書
2. 経営層への教育（セキュリティ対策の重要性の理解）
3. 業界ごとの情報セキュリティガイドライン
4. 中小企業向け情報セキュリティ対策に関する定期的な情報発信
5. 他の中小企業の取組状況や実態についての情報共有
6. 中小企業向けセキュリティ製品の情報を掲載した Web サイト等
7. 企業専属のセキュリティコンサルティングサービス
8. 地域密着型の相談窓口サービス
9. オンライン・電話での窓口相談サービス
10. 中小企業のセキュリティ対策の可視化サービス
11. その他（具体的に

【Q22】 貴社の情報セキュリティ対策はどのような体制で行われていますか。（SA）

1. 専門部署（担当者）がある	2. 兼務だが、担当者が任命されている
3. 組織的には行っていない（各自の対応）	4. わからない

【Q23】 貴社の情報セキュリティ対策に関して困ったことがあった際の相談先を教えてください。 あてはまるものを下記よりすべてお選びください。 （MA）

1. 社内の担当者	2. 社外の IT 関連業者・営業
3. 社外の中小企業診断士	4. 社外の IT コーディネータ
5. 社外の情報処理安全確保支援士（登録セキスペ）	6. 中小企業団体
7. 業界団体	8. 情報処理推進機構（IPA）
9. その他（具体的に	10. 特にない

【Q24】 貴社の情報セキュリティ対策に関する情報収集先を教えてください。 あてはまるものを下記よりすべてお選びください。（MA）

1. 社内の担当者	2. 社外の IT 関連業者
3. 社外の中小企業診断士	4. 社外の IT コーディネータ
5. 社外の情報処理安全確保支援士（登録セキスペ）	6. IT 機器等の営業
7. 業界団体	8. 情報処理推進機構（IPA）
9. 新聞・雑誌	10. テレビ
11. インターネット	12. 無料のセミナー・実務研修
13. 有料のセミナー・実務研修	14. その他（具体的に
15. 特にない	

【Q25】 貴社では従業員に対する情報セキュリティ教育をどのように実施していますか。 （MA）

1. 関連情報の周知（社内メール・回覧・掲示板など）
2. e ラーニング
3. 訓練（標的型攻撃訓練メール、インシデント対応訓練など）
4. 外部講習会やセミナーの聴講
5. 社内の研修や勉強会
6. 特に実施していない

【Q26】 貴社で行われている情報セキュリティ教育の内容はどのようなものですか。 あてはまるものを下記よりすべてお選びください。（MA）

1. 情報セキュリティの基礎知識	2. 会社のセキュリティポリシーと遵守事項
3. メール利用時の注意点	4. 情報漏洩防止
5. 標的型攻撃訓練メール	6. インシデント対応訓練
7. その他（具体的に	

【Q27】 貴社は情報セキュリティ人材を育成するために外部研修を活用している、または活用する意向がありますか。（SA）

1. はい	2. いいえ

【Q28】 貴社では情報セキュリティ人材育成のための外部研修に年間どの程度の期間をかけていますか。（SA）

1. 1 日以内	2. 1 日～5 日
3. 6 日～2 週間未満	4. 2 週間～1 ヶ月未満
5. 1 ヶ月～3 ヶ月未満	6. 3 ヶ月以上
7. わからない	

【Q29】 貴社では情報セキュリティ人材育成のための外部研修に年間どの程度の費用をかけていますか。（SA）

1. 1 万円未満	2. 1 万円以上～10 万円未満
3. 10 万円以上～50 万円未満	4. 50 万以上～100 万円未満
5. 100 万円以上～500 万円未満	6. 500 万円以上
7. わからない	

【Q30】 貴社では情報セキュリティ人材育成のための外部研修を活用する場合、どのような実施形態が望ましいと思いますか。あてはまるものを下記よりすべてお選びください。（MA）

1. オンライン	2. 対面
3. ハイブリッド	4. 1～2 ヶ月程度の終日
5. 週 5 日の集中的な演習	6. 働きながら夜間・週末等に受講できる演習
7. その他（具体的に	8. わからない

【Q31】 貴社では外部研修を年間どの程度の期間をかけることが望ましいと思いますか。（SA）

1. 1 日以内	2. 1 日～5 日
3. 6 日～2 週間未満	4. 2 週間～1 ヶ月未満
5. 1 ヶ月～3 ヶ月未満	6. 3 ヶ月以上
7. わからない	

【Q32】 貴社では情報セキュリティ人材育成のための外部研修に年間どの程度の費用をかけることが望ましいと思いますか。（SA）

1. 5 万円未満	2. 5 万円以上～10 万円未満
3. 10 万円以上～30 万円未満	4. 30 万円以上～50 万円未満
5. 50 万円以上～100 万円未満	6. 100 万円以上～500 万円以下

【Q33】 貴社で情報セキュリティ人材育成のための外部研修を活用していない又は活用する意向がない理由を教えてください。あてはまるものを下記よりすべてお選びください。（MA）

1. 適切な演習がない・わからない
2. 費用が高い
3. 人的リソースが割けない
4. その他（上記に当てはまらないものについて具体的に記載してください

【Q34】 貴社では 2023 年度（2023 年 4 月～2024 年 3 月）にサイバーインシデントの発生、もしくは発生が遭った可能性が高い経験はありましたか。 これらに遭った場合は、その内容を教えてください。 あてはまるものを下記よりすべてお選びください。（MA）

1. コンピュータウイルス感染
2. ランサムウェア攻撃
3. 不正アクセス
4. 標的型攻撃
5. DoS・DDoS 攻撃
6. 外部委託先に起因するサービスの停止・情報漏えい
7. 内部者（委託者を含む）の不正に起因する情報漏えい、システムの悪用等の情報セキュリティ上のトラブル
8. 被害にあっていない
9. その他（具体的に

【Q35】 貴社でサイバーインシデントによる影響で、生じた被害について教えてください。 （MA）

1. データの破壊	2. 個人情報の漏えい	3. 業務情報（営業秘密を除く）の漏えい
4. 営業秘密の漏えい	5. ウイルスメール等の発信	6. ネットワークの遅延
7. システム停止・性能低下	8. パソコン単体の停止	9. 関連部門の業務停滞
10. 個人の業務停滞	11. 取引先への感染拡大	12. その他（具体的に
13. 特になし		

【Q36】 サイバーインシデントにより貴社の取引先（サプライチェーン）に影響はありましたか。影響が及んだ場合はその内容について教えてください。 あてはまるものを下記よりすべてお選びください。（MA）

1. サービスの障害、遅延、停止による逸失利益	2. 個人顧客への賠償や法人取引先への補償負担
3. 原因調査・復旧にかかわる人件費等の経費負担	4. 裁判、調停等にかかわる人件費等の経費負担
5. 個人顧客や法人取引先に対する信頼の失墜	6. その他（具体的に
7. 特になし	

【Q37】 貴社が受けたサイバー攻撃の手口について教えてください。 あてはまるものを下記よりすべてお選びください。（MA）

1. ID・パスワードをだまし取られてユーザになりすまされたことによる不正アクセス
2. ぜい弱性（セキュリティパッチの未適用等）を突かれたことによる不正アクセス
3. SQL インジェクション
4. 取引先やグループ会社等を経由して侵入
5. その他（具体的に
6. 手口はわからない

【Q38】 貴社が受けたサイバー攻撃の被害について教えてください。 あてはまるものを下記よりすべてお選びください。（MA）

1. 自社 Web サイトが改ざんされた
2. 自社 Web サイトのサービスが停止、または機能が低下させられた
3. 業務サーバの内容が改ざんされた
4. 業務サーバのサービスが停止、または機能が低下させられた
5. 貴社が提供するネットワークサービスにおいて、第三者のなりすましによる不正使用があった
6. 取引先の企業や個人に被害が拡大した
7. 個人情報が盗まれた
8. 業務情報（営業秘密を除く）が盗まれた
9. 営業秘密が盗まれた
10. ランサムウェアによる身代金の要求を受けた
11. 標的型攻撃による不正アクセスを受けた
12. ビジネスメール詐欺による金銭被害を受けた
13. その他（具体的に
14. サイバー攻撃を受けたが、被害には至らなかった

【Q39_1】 過去 3 期、サイバーインシデントの発生で生じた被害額の総額、サイバーインシデントの発生回数、復旧するまでに要した最大の期間について教えてください。（0 以上の半角数字で入力してください。） - 被害総額 （FA）

［Q39_2］ 過去 3 期、サイバーインシデントの発生で生じた被害額の総額、サイバーインシデントの発生回数、復旧するまでに要した最大の期間について教えてください。（0 以上の半角数字で入力してください。） - 発生回数 （FA）

［Q39_3］ 過去 3 期、サイバーインシデントの発生で生じた被害額の総額、サイバーインシデントの発生回数、復旧するまでに要した最大の期間について教えてください。（0 以上の半角数字で入力してください。） - 期間 （FA）

【Q40】 サイバーインシデントの経験を踏まえて、情報セキュリティ対策を強化しましたか（当該被害経験は、対策を強化するきっかけとなりましたか）。（SA）

1. はい（具体的に 2. いいえ

【Q41】 他社との取引において、貴社の主要な事業に最も大きいリスクと考えていることを教えてください。（SA）

1. 機密性の高い情報（個人情報・設計図面等）の漏洩
2. 供給している製品（原料・中間部品・最終品等）の途絶
3. 可用性が重視されるサービス（インフラ・IT 等）の停止
4. その他（具体的に
5. わからない

【Q42】 サイバーインシデントの影響により、前問で想定する事態が取引先で発生した場合、ビジネス的な観点で、貴社の主要な事業にどれほど影響がありますか。（SA）

［Q42 項目 1］【a】取引先が販売先（発注元企業）の場合

1. 自社の事業に多大な影響が及ぶ
2. 自社の事業において縮退や代替措置での事業継続が可能
3. 自社の事業への影響が想定されない、もしくは許容可能な影響と想定される
4. その他
5. わからない

［Q42 項目 2］【b】取引先が仕入先（委託・協力企業）の場合

1. 自社の事業に多大な影響が及ぶ
2. 自社の事業において縮退や代替措置での事業継続が可能
3. 自社の事業への影響が想定されない、もしくは許容可能な影響と想定される
4. その他
5. わからない

【Q43】 サイバーインシデントの影響により、貴社で前問で想定する事態が発生した場合、ビジネス的な観点で、取引先の主要な事業にどれほど影響があると考えられますか。（SA）

［Q43 項目 1］【a】取引先が販売先（発注元企業）の場合

1. 取引先の事業に多大な影響が及ぶ
2. 取引先の事業において縮退や代替措置での事業継続が可能
3. 取引先の事業への影響が想定されない、もしくは許容可能な影響と想定される
4. その他
5. わからない

［Q43 項目 2］【b】取引先が仕入先（委託・協力企業）の場合

1. 取引先の事業に多大な影響が及ぶ
2. 取引先の事業において縮退や代替措置での事業継続が可能
3. 取引先の事業への影響が想定されない、もしくは許容可能な影響と想定される
4. その他
5. わからない

【Q44】 貴社の社内ネットワークは販売先（発注元企業）や仕入先（委託・協力企業）のネットワークと接続していますか。（SA）

1. はい　　2. いいえ　　3. わからない

【Q45】 貴社は販売先（発注元企業）や仕入先（委託・協力企業）とのネットワーク接続がある場合、アクセス権限や範囲を適切に設定していますか。（SA）

1. はい（アカウントも付与している）　　2. はい（アカウントは付与していない）
3. いいえ　　4. わからない

【Q46】 貴社は販売先（発注元企業）から貴社への情報セキュリティに関する要請を受けた経験はありますか。（SA）

1. はい　　2. いいえ　　3. わからない

【Q47】 販売先（発注元企業）から貴社への情報セキュリティに関する要請の具体的な内容について教えてください。あてはまるものを下記よりすべてお選びください。（MA）

1. 秘密保持
2. 証跡の提示、監査協力等
3. 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
4. サイバーインシデントが発生した場合の対応
5. 可用性（稼働率の水準、目標復旧時間等）
6. 認証（ISMS 等）取得の依頼/要件化
7. 新たな脅威（ぜい弱性）が顕在化した場合の情報共有・対応
8. 再委託の禁止または制限
9. 契約終了後の情報資産の扱い（返却、消去、廃棄等）
10. セキュリティ機器の設置（UTM 等）
11. その他（具体的に

【Q48】 販売先（発注元企業）から貴社への情報セキュリティに関する要請に対して、貴社の行ったセキュリティ対策の具体的な内容について教えてください。またどの程度の費用が掛かりましたか。（SA）

1. 対策を行った【具体的な対策内容、コスト】　　2. 対策を行っていない　　3. わからない

【Q49】 貴社は販売先（発注元企業）から要請された情報セキュリティ対策を行ったことが取引先との取引につながった大きな要因だと思いますか。 （SA）

1. はい	2. いいえ	3. わからない

【Q50】 貴社で販売先（発注元企業）から情報セキュリティ対策の要請を受けた場合に、対策の実施に向けての課題となることについて教えてください。（MA）

1. 情報セキュリティ対策に関する販売先（発注元企業）との契約内容の明確化
2. 対策費用（具体的な対策と費用）の用意、費用負担の検討
3. 専門人材の確保・育成
4. 情報セキュリティ認証制度の取得
5. 損害保険付保
6. その他（具体的に
7. 特になし

【Q51】 販売先（発注元企業）からの情報セキュリティに関する要請・推奨に対応するための、貴社の費用負担について教えてください。（SA）

1. 全額自社で負担している
2. 一部の費用負担を販売先（発注先企業）に依頼している
3. 全額費用負担を依頼している
4. 追加の費用が生じない要請・推奨のみ対応している
5. その他（具体的に

【Q52】 貴社では販売先（発注元企業）から情報セキュリティ対策の要請を受けたら対策を行いますか。 （SA）

1. はい	2. 費用による	3. いいえ	4. わからない

【Q53】 貴社では販売先（発注元企業）から要請された情報セキュリティ対策を行わなかったことにより取引先との取引につながらなかったことがあると思いますか。（SA）

1. はい	2. いいえ	3. わからない

【Q54】 貴社では販売先（発注元企業）から「情報セキュリティ対策を行わない企業とは取引できない」と言われた場合、対策を行うと思いますか。（SA）

1. はい	2. いいえ	3. わからない

【Q55】 貴社は仕入先（委託・協力企業）に対して情報セキュリティ対策の要請をしたことがありますか。（SA）

1. はい	2. いいえ	3. わからない

【Q56】 仕入先（委託・協力企業）は要請に応じましたか。（SA）

1. はい	2. いいえ	3. わからない

【Q57】 貴社では要請した情報セキュリティ対策を取引先が行ったことが取引先との取引につながった大きな要因だったと思いますか。（SA）

1. はい	2. いいえ	3. わからない

【Q58】 貴社では要請した情報セキュリティ対策を取引先が行わなかったことが取引先との取引につながらなかった大きな要因と思うことがありましたか。（SA）

1. はい	2. いいえ	3. わからない

【Q59】 貴社では仕入先（委託・協力企業）への情報セキュリティ対策を要請するための貴社のガイドライン等はありますか。（SA）

1. ガイドライン等がある	2. ガイドライン等はない	3. 委託業務がない

【Q60】 貴社は独立行政法人情報処理推進機構（IPA）の施策である「SECURITY ACTION」という制度を知っていますか。（SA）

1. はい	2. いいえ

【Q61】 貴社は「SECURITY ACTION」の一つ星（または二つ星）を宣言していますか。（SA）

1. ★1 を宣言している	2. ★2 を宣言している	3. していない

【Q62】 貴社が「SECURITY ACTION」の宣言を行ったきっかけを教えてください。 あてはまるものを下記よりすべてお選びください。（MA）

1. 補助金や助成金の申請要件	2. 顧客や取引先からの要求
3. 経営層の意識向上	4. サイバー攻撃被害に遭った
5. 業界標準や法規制の変化	6. その他（具体的に

【Q63】「SECURITY ACTION」の宣言に関して、貴社の現在の状況を教えてください。（SA）

1. 宣言した状態を維持できている	2. 現在は維持できていない

【Q64】「SECURITY ACTION」の宣言に関して、各項目を維持してくために貴社で必要となることを教えてください。 あてはまるものを下記よりすべてお選びください。（MA）

1. 予算の確保	2. 専門知識を持った人材の確保
3. 経営層の関与	4. 担当部署の設置・体制の整備
5. その他（具体的に	

【Q65】 貴社が「SECURITY ACTION」の宣言を維持できなかった理由を教えてください。 あてはまるものを下記よりすべてお選びください。（MA）

1. コストが高い	2. 専門知識の不足
3. 情報セキュリティ対策の人材がいない	4. 情報セキュリティへの意識が低い
5. リソースの制約	6. 既存のシステムが十分だと考えている
7. サイバーインシデントの経験がない	8. 投資対効果が不明確
9. 他の優先事項がある	10. その他（具体的に

【Q66】 貴社の職員から「SECURITY ACTION」の取組状況は確認できますか。（SA）

1. はい	2. いいえ	3. わからない

【Q67】 貴社の職員から「SECURITY ACTION」の取組状況を確認できない理由は教えてください。（MA）

1. 共有するためのポリシーがない	2. 共有するためのシステムがない
3. 職員に周知させる必要性を感じていない	4. その他（具体的に

【Q68】 貴社が「SECURITY ACTION」の宣言を実施していない理由を教えてください。 あてはまるものを下記よりすべてお選びください。（MA）

1. リソース不足	2. 情報セキュリティ対策を実施できる人材がいない
3. 優先度が低い	4. 手続きが煩雑
5. 内容が理解できない	6. 費用対効果が不明確
7. 必要性が感じられない	8. 知らなかった
9. その他（具体的に	

【Q69】「SECURITY ACTION」は中小企業自らが、情報セキュリティ対策に取組むことを自己宣言する制度です。貴社はどのようなきっかけがあれば宣言を行うか教えてください。 あてはまるものを下記よりすべてお選びください。（MA）

1. 顧客や取引先からの要求	2. 法規制や業界標準の変化
3. サイバー攻撃の被害経験	4. 補助金・助成金制度の確立
5. 経営層の意識向上	6. これから実施しようと思う
7. 分かりやすい説明があれば実施できる	8. 対応できる人材がいれば実施できる
9. その他（具体的に	

【Q70】 独立行政法人情報処理推進機構（IPA）が実施している「サイバーセキュリティお助け隊サービス制度」をご存じですか。（SA）

1. はい	2. いいえ	3. わからない

【Q71】 貴社は「サイバーセキュリティお助け隊サービス」を導入されていますか。（SA）

1. はい	2. いいえ	3. わからない

【Q72】 貴社が「サイバーセキュリティお助け隊サービス」を導入したきっかけについて教えてください。 あてはまるものを下記よりすべてお選びください。（MA）

1. 補助金や助成金の申請要件	2. 顧客や取引先からの要求
3. 経営層の意識向上	4. サイバー攻撃被害に遭った
5. 業界標準や法規制の変化	6. その他（具体的に

【Q73】 貴社が「サイバーセキュリティお助け隊サービス」を導入して良かった点を教えてください。 あてはまるものを下記よりすべてお選びください。（MA）

1. ワンパッケージでの情報セキュリティ対策	2. 導入が容易
3. 緊急時の対応	4. コストの削減
5. 顧客や取引先からの信頼向上	6. その他（具体的に

【Q74】 貴社が「サイバーセキュリティお助け隊サービス」を導入しない理由を教えてください。 あてはまるものを下記よりすべてお選びください。（MA）

1. リソース不足	2. 優先度が低い
3. 手続きが煩雑	4. 費用対効果が不明確
5. 必要性が感じられない	6. 自社の規模に見合ったサービスではない
7. サービスレベルが低い	8. IPA ホームページの案内が分かりづらい
9. その他（具体的に	

【Q75】「サイバーセキュリティお助け隊サービス」を導入したいと思いますか？（SA）

1. はい　　2. いいえ　　3. わからない

【Q76】 貴社が「サイバーセキュリティお助け隊サービス」を導入したいと思わない理由は何ですか。 あてはまるものを下記よりすべてお選びください。（MA）

1. リソース不足	2. 優先度が低い
3. 手続きが煩雑	4. 費用対効果が不明確
5. 必要性が感じられない	6. 自社の規模に見合ったサービスではない
7. サービスレベルが低い	8. IPA ホームページの案内が分かりづらい
9. その他（具体的に	

【Q77】 貴社の認証取得や自己宣言の実施状況について教えてください。（MA）

1. ISMS 認証を取得済み	2. プライバシーマーク（P マーク）取得済み
3. その他（具体的に	4. 特になし

【Q78】 認証取得や自己宣言にあたり、実施した具体的な取り組み・工夫などについて教えてください。（MA）

1. リスクアセスメントの実施	2. 情報セキュリティポリシーの策定と更新
3. 従業員のセキュリティ教育と訓練	4. アクセス制御の強化
5. インシデント対応計画の策定	6. 定期的なセキュリティ監査の実施

【Q79】 貴社において、情報セキュリティ対策を実施する上で、参考にしたガイドライン等はありますか。（MA）

1. 中小企業の情報セキュリティ対策ガイドライン	2. サイバーセキュリティ経営ガイドライン
3. NIST Cyber Security Framework	4. 業界独自のガイドライン（具体的に
5. その他（具体的に	

【Q80】 貴社では下記にあげる項目について、どの程度、実施していますか。 （SA）

［Q80 項目 1］ パソコンやスマホなど情報機器の OS やソフトウェアは常に最新の状態にしていますか？

1. 実施している　　2. 一部実施している　　3. 実施していない　　4. わからない

［Q80 項目 2］ パソコンやスマホなどにはウイルス対策ソフトを導入し、ウイルス定義ファイルは最新の状態にしていますか？

1. 実施している　　2. 一部実施している　　3. 実施していない　　4. わからない

［Q80 項目 3］ パスワードは破られにくい「長く」「複雑な」パスワードを設定していますか？

1. 実施している　　2. 一部実施している　　3. 実施していない　　4. わからない

［Q80 項目 4］ 重要情報に対する適切なアクセス制限を行っていますか？

1. 実施している　　2. 一部実施している　　3. 実施していない　　4. わからない

［Q80 項目 5］ 新たな脅威や攻撃の手口を知り対策を社内共有する仕組みはできていますか？

1. 実施している　　2. 一部実施している　　3. 実施していない　　4. わからない

［Q80 項目 6］ 電子メールの添付ファイルや本文中の URL リンクを介したウイルス感染に気を付けていますか？

1. 実施している　　2. 一部実施している　　3. 実施していない　　4. わからない

［Q80 項目 7］ 電子メールや（FA）X の宛先の送信ミスを防ぐ取り組みを実施していますか？

1. 実施している　　2. 一部実施している　　3. 実施していない　　4. わからない

［Q80 項目 8］重要情報は電子メール本文に書くのではなく、添付するファイルに書いてパスワードなどで保護していますか？

1. 実施している	2. 一部実施している	3. 実施していない	4. わからない

［Q80 項目 9］無線 LAN を安全に使うために適切な暗号化方式を設定するなどの対策をしていますか？

1. 実施している	2. 一部実施している	3. 実施していない	4. わからない

［Q80 項目 10］インターネットを介したウイルス感染や SNS への書き込みなどのトラブルへの対策をしていますか？

1. 実施している	2. 一部実施している	3. 実施していない	4. わからない

［Q80 項目 11］パソコンやサーバのウイルス感染、故障や誤操作による重要情報の消失に備えてバックアップを取得していますか？

1. 実施している	2. 一部実施している	3. 実施していない	4. わからない

［Q80 項目 12］紛失や盗難を防止するため、重要情報が記載された書類や電子媒体は机上に放置せず、書庫などに安全に保管していますか？

1. 実施している	2. 一部実施している	3. 実施していない	4. わからない

［Q80 項目 13］重要情報が記載された書類や電子媒体を持ち出す時は、盗難や紛失の対策をしていますか？

1. 実施している	2. 一部実施している	3. 実施していない	4. わからない

［Q80 項目 14］離席時にパソコン画面の覗き見や勝手な操作ができないようにしていますか？

1. 実施している	2. 一部実施している	3. 実施していない	4. わからない

［Q80 項目 15］関係者以外の事務所への立ち入りを制限していますか？

1. 実施している	2. 一部実施している	3. 実施していない	4. わからない

［Q80 項目 16］退社時にノートパソコンや備品を施錠保管するなど盗難防止対策をしていますか？

1. 実施している	2. 一部実施している	3. 実施していない	4. わからない

［Q80 項目 17］事務所が無人になるときの施錠忘れ対策を実施していますか？

1. 実施している	2. 一部実施している	3. 実施していない	4. わからない

［Q80 項目 18］重要情報が記載された書類や重要なデータが保存された媒体を破棄する時は、復元できないようにしていますか？

1. 実施している	2. 一部実施している	3. 実施していない	4. わからない

［Q80 項目 19］従業員に守秘義務を理解してもらい、業務上知り得た情報を外部に漏らさないなどのルールを守らせていますか？

1. 実施している	2. 一部実施している	3. 実施していない	4. わからない

［Q80 項目 20］従業員にセキュリティに関する教育や注意喚起を行っていますか？

1. 実施している	2. 一部実施している	3. 実施していない	4. わからない

［Q80 項目 21］個人所有の情報機器を業務で利用する場合のセキュリティ対策を明確にしていますか？

1. 実施している	2. 一部実施している	3. 実施していない	4. わからない

［Q80 項目 22］重要情報の授受を伴う取引先との契約書には、秘密保持条項を規程していますか？

1. 実施している	2. 一部実施している	3. 実施していない	4. わからない

［Q80 項目 23］クラウドサービスやウェブサイトの運用等で利用する外部サービスは、安全・信頼性を把握して選定していますか？

1. 実施している	2. 一部実施している	3. 実施していない	4. わからない

［Q80 項目 24］セキュリティ事故が発生した場合に備え、緊急時の体制整備や対応手順を作成するなど準備をしていますか？

1. 実施している	2. 一部実施している	3. 実施していない	4. わからない

［Q80 項目 25］情報セキュリティ対策（上記 1～24 など）をルール化し、従業員に明示していますか？

1. 実施している　2. 一部実施している　3. 実施していない　4. わからない

2024 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－
https://www.ipa.go.jp/security/reports/sme/sme-survey2024.html

2025 年 5 月
独立行政法人情報処理推進機構

https://www.ipa.go.jp/