2021年度中小企業における
情報セキュリティ対策に関する実態調査
― 調査報告書 ―

2022年3月31日

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

目 次

第１章　本調査研究の背景・目的

１．背景・目的

近年、中小企業においてもIT化が進み、業務の効率化、サービスレベルの向上等が図られている。その一方で、機密情報を狙ったサイバー攻撃は日々発生し、その被害も確認されている。中小企業を取り巻く環境においては、サプライチェーンの関係性を悪用し、セキュリティ対策の強固な大企業を直接攻撃するのではなく、その目的企業が構成するサプライチェーンにある、セキュリティが脆弱な中小企業等の取引先を経由し、最終目的である企業を攻撃するケースも発生している。

中小企業においては、自社が直接攻撃され、保有する取引先企業の機密情報が漏えいする、あるいは、サイバー攻撃の足掛かりとされる可能性があることを念頭に置き、IT技術、特にインターネットの安全な利用をするために情報セキュリティ対策の必要性を認識し、適切な対策を実施することが重要である。

独立行政法人情報処理推進機構（以下「IPA」という。）では、中小企業における情報セキュリティに関する実態把握を目的として、2016年度に「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「前回調査」という。）や2018年度に「SECURITY ACTION 宣言事業者における情報セキュリティ対策に関する実態調査」を実施したところである。また今般、IPAが事務局を務めるサプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）において「発注元企業として取り組むべき課題」等についての議論も行われている。加えて、中小企業においても、2020年以降、急速に普及しつつあるテレワーク等によって、働き方も大きく変化しつつある。

こうした状況に鑑み、前回調査から5年経過した2021年度に中小企業における情報セキュリティ対策の実情を把握するため、「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」を実施した。

本調査報告書は、調査結果を取りまとめたものである。加えて、個別のインタビュー調査に基づく61件の取組事例を事例集として取りまとめた。報告書と併せて、中小企業における情報セキュリティ対策の実態や取組事例等について参考としていただき、今後の中小企業向けセキュリティ対策の強化につなげる一助となれば幸いである。

２．調査実施内容

（１）業務概要

中小企業における情報セキュリティ対策の実態や対策実施時の課題、経営層の認識等を把握し、必要な対策を促すため、以下の調査を行い、その結果を調査報告書等に取りまとめる。

・ 中小企業を対象としたアンケート調査（以下「アンケート調査」という。）

・ アンケート調査結果に基づく個別ヒアリング調査（以下「個別調査」という。）

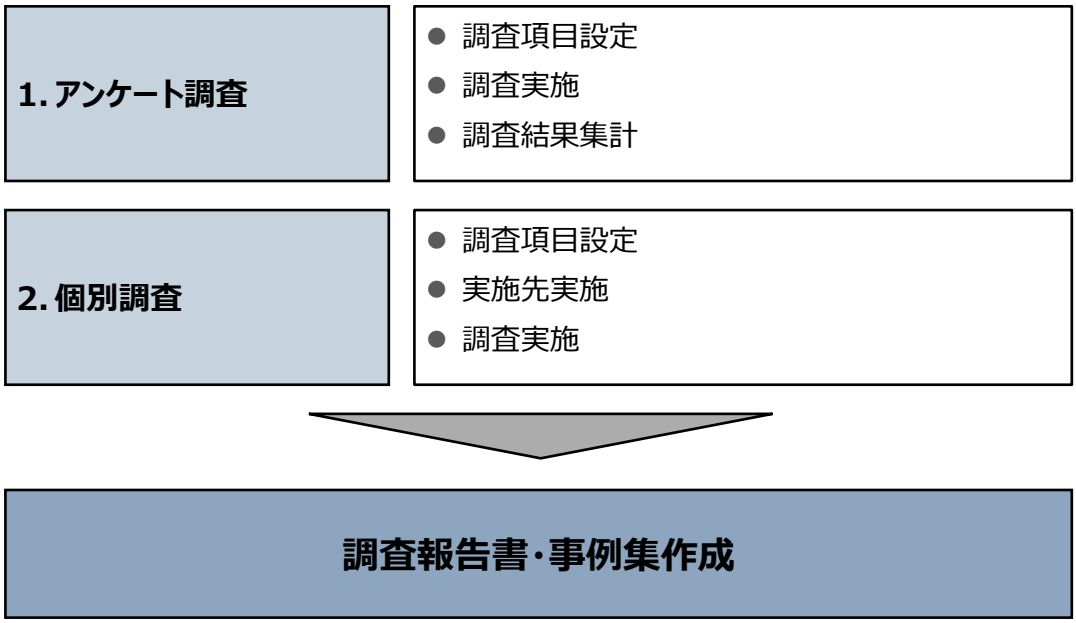
上記の両調査から得られた結果を基に、中小企業における情報セキュリティ対策の啓発・促進に資する事例（情報セキュリティに関する被害の実態、情報セキュリティ対策の実践により経営にプラスの効果を発揮した事例等）を事例集として取りまとめる。

（２）調査内容・方法

本調査では、中小企業における情報セキュリティ対策の実態や実施時の課題、経営層の認識、今後求められる対策等を把握ため、中小企業を対象としたアンケート調査と個別調査を実施した。

アンケート調査、個別調査を実施のうえ、調査結果を取りまとめた調査報告書と、個別調査実施により得られた中小企業の情報セキュリティ対策の取組例を取りまとめた事例集を作成した。

図表 1 調査フロー



①中小企業を対象としたアンケート調査

１)調査手法・回答方法

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

アンケート調査手法は、ウェブサイトによる回答システム（以下「ウェブ回答システム」という。）を構築して実施した。回答の回収は、ウェブ回答システムを通じ回収することを前提とし、電子ファイルの添付によるメール回答と併用して実施した。

２)調査項目

アンケート調査票は、以下の項目を中心に設問した。調査票の詳細は、別添に示す。

図表 2 調査項目

- 企業概要
- ITの導入状況
- 情報セキュリティに関する意識・状況
- 情報セキュリティ被害
- 取引先を含む情報セキュリティ対策

３)調査対象企業

「前回調査」の送付数内訳を参考として、以下の内訳で、アンケートを送付した。アンケートの総送付数は40,000件である。アンケート送付先リストは、企業信用調査会社の企業データベースからランダムに抽出した。

図表 3 アンケート送付数内訳

業種名	中小企業数	小規模企業者数	業種別合計数
農業・林業・漁業	746	1,049	1,795
建設業	1,353	3,160	4,513
製造業、鉱業・採石業・砂利採取業、電気・ガス・熱供給・水道業	1,337	3,123	4,460
情報通信業	529	1,229	1,758
運輸業・郵便業	529	1,229	1,758
卸売業・小売業	2,530	6,074	8,604
金融業・保険業	528	1,231	1,759
不動産業・物品賃貸業	1,115	2,599	3,714
サービス業・その他	3,495	8,144	11,639
合計	12,162	27,838	40,000

中小企業と小規模企業者の定義は、中小企業基本法第２条及び同法第２条第５項の定義を基準に、常時使用する従業員の数と資本金の額で判断した。

図表 4 中小企業の定義[1]

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

図表 5 小規模企業者の定義[2]

業種分類	中小企業基本法の定義
製造業その他	従業員20人以下
商業・サービス業	従業員 5人以下

[1] 中小企業庁 「中小企業・小規模企業者の定義」
https://www.chusho.meti.go.jp/soshiki/teigi.html
[2] 中小企業庁 「中小企業・小規模企業者の定義」
https://www.chusho.meti.go.jp/soshiki/teigi.html

②個別調査

１)調査手法

アンケート調査の有効回答数4,074件のうち、以下の観点を極力すべて満たすように対象企業をサンプリングした。調査にあたっては、オンライン会議ツールを使用したウェブ会議、もしくは先方の都合に配慮し、電話での聞き取りのいずれかの方法により実施した。

図表 6 対象企業選定の観点

- 地域（経済産業省の各経済産業局が所管する地域ごとに一定数の事例が含まれること）
- アンケート調査の回答により、情報セキュリティに関する被害実態等があり、情報セキュリティ対策の実践により経営面を中心にプラスの効果を発揮している事例（下記、３つの観点から抽出）
  - 情報セキュリティに関する実施対策が多い、もしくは情報セキュリティ対策投資が多い事例
  - 情報セキュリティに関する被害実態等のある事例
  - サプライチェーン上での情報セキュリティ対策の要請の多い事例
- 業種・従業員（各業種分類において中小企業基本法で定義される「中小企業」と「小規模企業者」を従業員数の観点で極力それぞれ含むこと）

２)調査項目

個別調査は、以下の項目を中心に質問を行い、アンケート調査の回答内容の詳細やアンケート調査では把握の難しい実態や問題認識等を深掘りした。

図表 7 調査項目

- 情報セキュリティ対策の取り組みについて
- 情報セキュリティ対策による効果について
- 情報セキュリティ被害について
- 取引先との関連について
- その他

第２章　アンケート調査

１．調査概要

（１）実施概要

実施概要は、下表のとおりである。

図表 8　アンケート調査実施概要

調査手法	・ウェブによるアンケート調査
調査対象	・全国の中小企業を対象とし、業種別（10区分）、企業規模別（3区分）、で中小企業基本法の定義に基づいて割付を行い、サンプルを回収。
調査期間	2021年10月～2021年12月
有効回答数	4,074人（内訳：経営層2,819人、ITや情報セキュリティの社内担当者561人、一般社員、役職無回答・不明：694人）

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。

２．調査結果（サマリー）

1.単純集計

- 過去3期におけるIT投資の状況について、「投資を行っていない」と回答している中小企業が30%となっている。また、過去3期の情報セキュリティ対策投資の状況について投資を行っていないと回答している中小企業が33.1%となっている。情報セキュリティ対策投資を行わなかった理由としては、「必要性を感じていない」の割合が最も多く、「費用対効果が見えない」、「コストがかかりすぎる」という結果となっている。
- コンピュータウイルスや不正アクセス、DoS・DDoS攻撃等の情報セキュリティに関する事象に対する脅威の認識については、すべての事象において、「非常に大きな脅威である」、「どちらかといえば脅威である」を合わせた割合が5割を超えている。
- 2020年度の1年間に、何らかしらの情報セキュリティ被害に遭った企業は5.7%となっており、最も多い回答は、「コンピュータウイルスに感染」となっている。コンピュータウイルスの侵入経路としては、「電子メール」や「インターネット接続」、「自らダウンロードしたファイル」との回答が多い。
- 取引先との間における情報セキュリティに関する条項・取引上の義務・要請の有無については、63.2%の企業が「義務・要請はない」と回答している。販売先（委託元）からの情報セキュリティ対策要請を受けた際の課題については、「特になし」との回答が最も多かったものの、「対策費用（具体的な対策と費用）の用意、費用負担の検討」に回答が32.5%、「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）」、「専門人材の確保・育成」の回答が25.8%となっている。

２.企業規模によるクロス集計

- 企業規模が大きいほど組織体制、教育、情報セキュリティ関連製品やサービスの導入等、様々な観点で情報セキュリティに関して積極的に実施する傾向にある。
- ただし、セキュリティパッチの適用やウイルス対策ソフト・サービスの導入等については、企業規模によらず実施をしている傾向にある。
- 活用したい情報セキュリティ対策に関するサービスについては、中小企業（100人以下）や中小企業（101人以上）は「業界ごとのセキュリティガイドライン」や「中小企業向けセキュリティ対策に関する定期的な情報発信」等の情報に関する項目に回答が集まっているのに対し、小規模企業者については「オンライン・電話での窓口相談サービス」が最も高く、相談先を必要としている。
- 情報セキュリティ対策を実施して感じられたメリットについては、企業規模が大きいほど何らかのメリットを享受しているとの回答が多くなる。

３.セキュリティ体制によるクロス集計

- 専門部署がある・兼務だが担当者が任命されている企業は、情報セキュリティ関連製品やサ

ービスの導入状況、セキュリティパッチの適用、スマートフォンやタブレット端末に対して実施している対策、各種保険加入等において、全体の水準以上に実施している傾向にある。

- 活用したい情報セキュリティ対策に関するサービスについては、専門部署がある・兼務だが担当者が任命されている企業は情報やガイドラインを望んでいるのに対し、組織的には行っていない企業は窓口相談サービスを望んでいる。
- 情報セキュリティ対策を実施して感じられたメリットについては、専門部署がある・兼務だが担当者が任命されている企業ほど何らかのメリットを享受しているとの回答が多くなる。特に、「従業員の情報セキュリティへの意識向上」、「取引先からの信頼獲得」、「対処すべきリスクの特定」は全体に比べ大きく高い結果である。

4.取引上の立場によるクロス集計

- 取引先との間における情報セキュリティに関する条項・取引上の義務・要請については、サプライチェーンの上流（元請・一次請）から下流（三次請け・それ以降）にいくにつれ、「義務・要請がある」との回答の割合が増加している。

5.前回調査との比較

前回調査から変化が小さい結果が多い。

- コロナ禍による影響で、情報セキュリティ関連製品やサービスのうち、「VPN」の導入が増加している。一方で、情報セキュリティ対策の必要性を感じたきっかけについては、「マイナンバー制度の開始」が減少している。

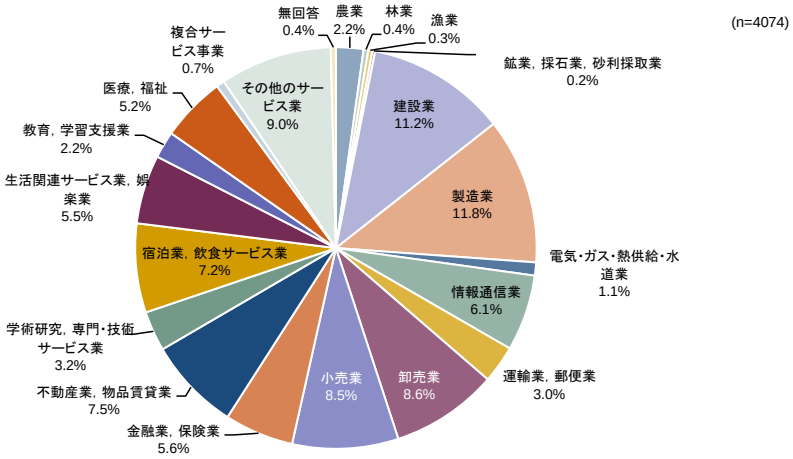
3．調査結果（単純集計）

（1）回答企業の属性

①業種

「製造業」の割合が最も高く11.8%となっている。次いで、「建設業（11.2%）」、「その他のサービス業（9.0%）」となっている。

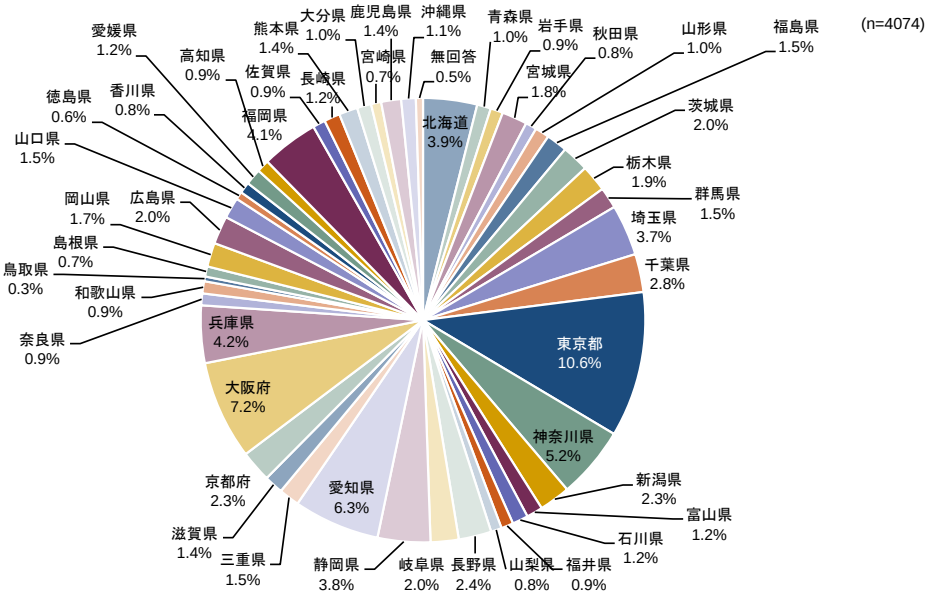
図表 2-9 業種（SA）



②所在地

「東京都」の割合が最も高く10.6%となっている。次いで、「大阪府（7.2%）」、「愛知県（6.3%）」となっている。

図表 2-10 所在地（SA）

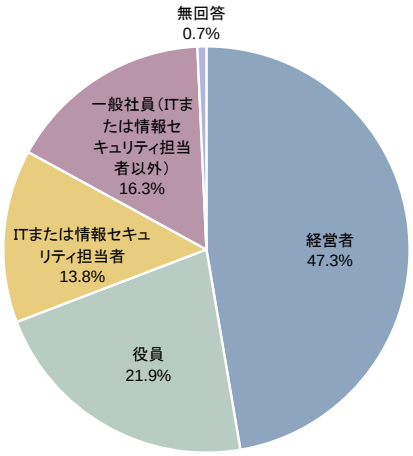


③回答者の役職・担当

「経営者」の割合が最も高く47.3%となっている。次いで、「役員（21.9%）」、「一般社員（ITまたは情報セキュリティ担当者以外）（16.3%）」となっている。

図表 2-11 回答者の役職・担当（SA）

(n=4074)

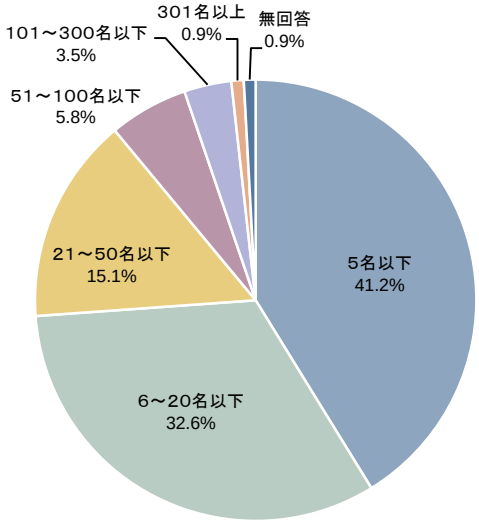


④従業員規模

「５名以下」の割合が最も高く41.2%となっている。次いで、「６～２０名以下（32.6%）」、「２１～５０名以下（15.1%）」となっている。

図表 2-12 従業員規模（SA）

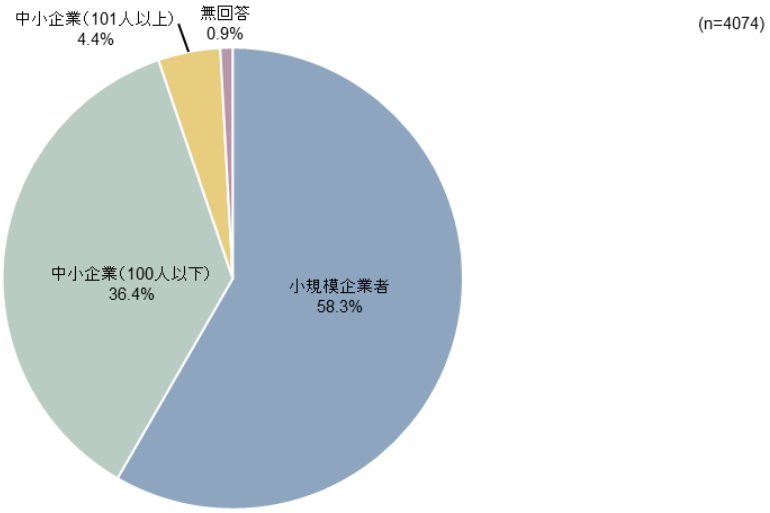
(n=4074)



⑤企業規模

「小規模企業者」の割合が最も高く58.3%となっている。次いで、「中小企業（100人以下）（36.4%）」、「中小企業（101人以上）（4.4%）」となっている。

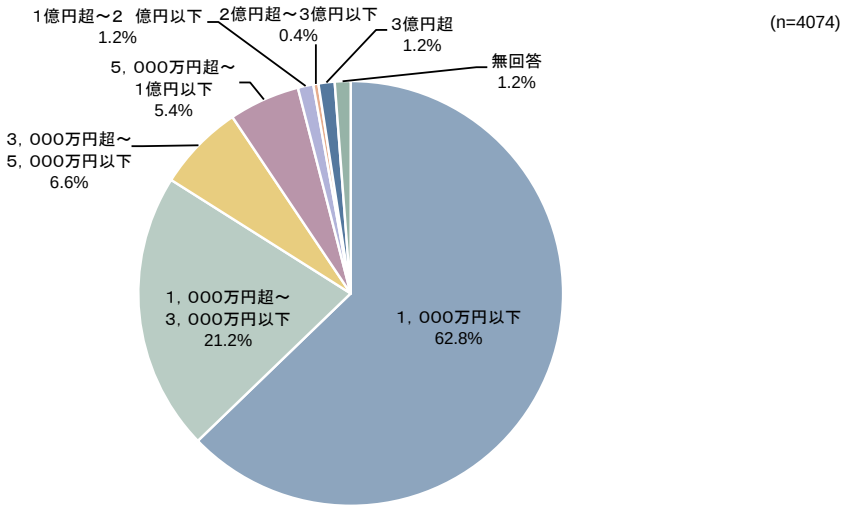
図表 2-13 企業規模（SA）



⑥直近会計年度の資本金

「1,000万円以下」の割合が最も高く62.8%となっている。次いで、「1,000万円超～3,000万円以下（21.2%）」、「3,000万円超～5,000万円以下（6.6%）」となっている。

図表 2-14 直近会計年度の資本金（SA）

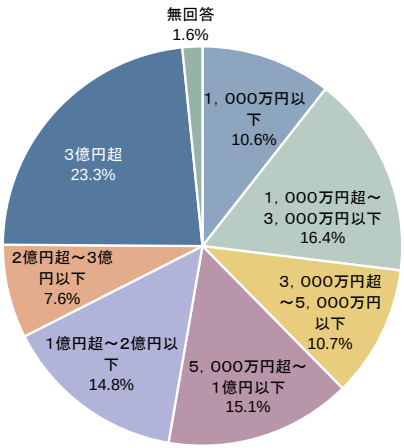


⑦直近会計年度の売上高

「３億円超」の割合が最も高く23.3%となっている。次いで、「1,000万円超～3,000万円以下（16.4%）」、「5,000万円超～１億円以下（15.1%）」となっている。

図表　2-15　直近会計年度の売上高（SA）

(n=4074)

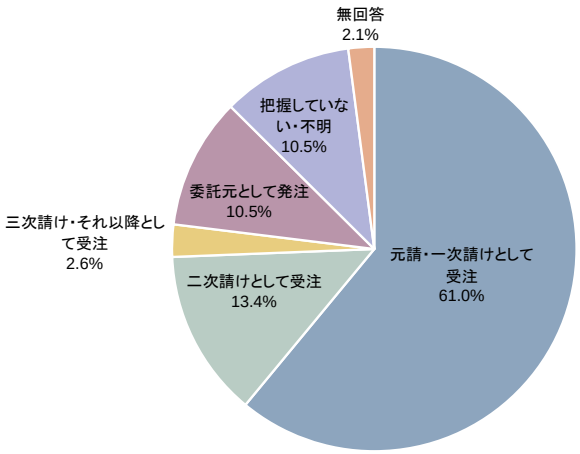


⑧取引の立場

「元請・一次請けとして受注」の割合が最も高く61.0%となっている。次いで、「二次請けとして受注（13.4%）」、「委託元として発注（10.5%）」、「把握していない・不明（10.5%）」となっている。

図表　2-16　取引の立場（SA）

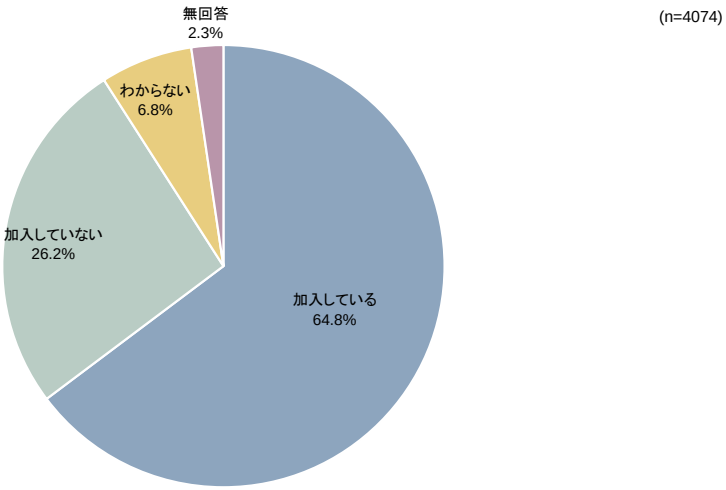
(n=4074)



⑨業界団体への加入状況

「加入している」の割合が64.8%となっており、「加入していない」の割合が26.2%となっている。

図表　2-17　業界団体への加入状況（SA）

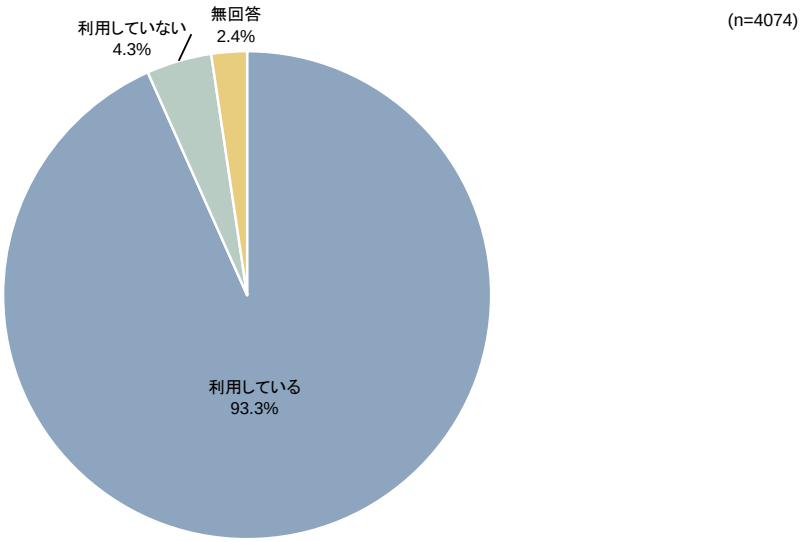


（2）ITの導入状況

①業務用パソコン・タブレット端末・スマートフォンの利用状況

「利用している」の割合が93.3%となっている。

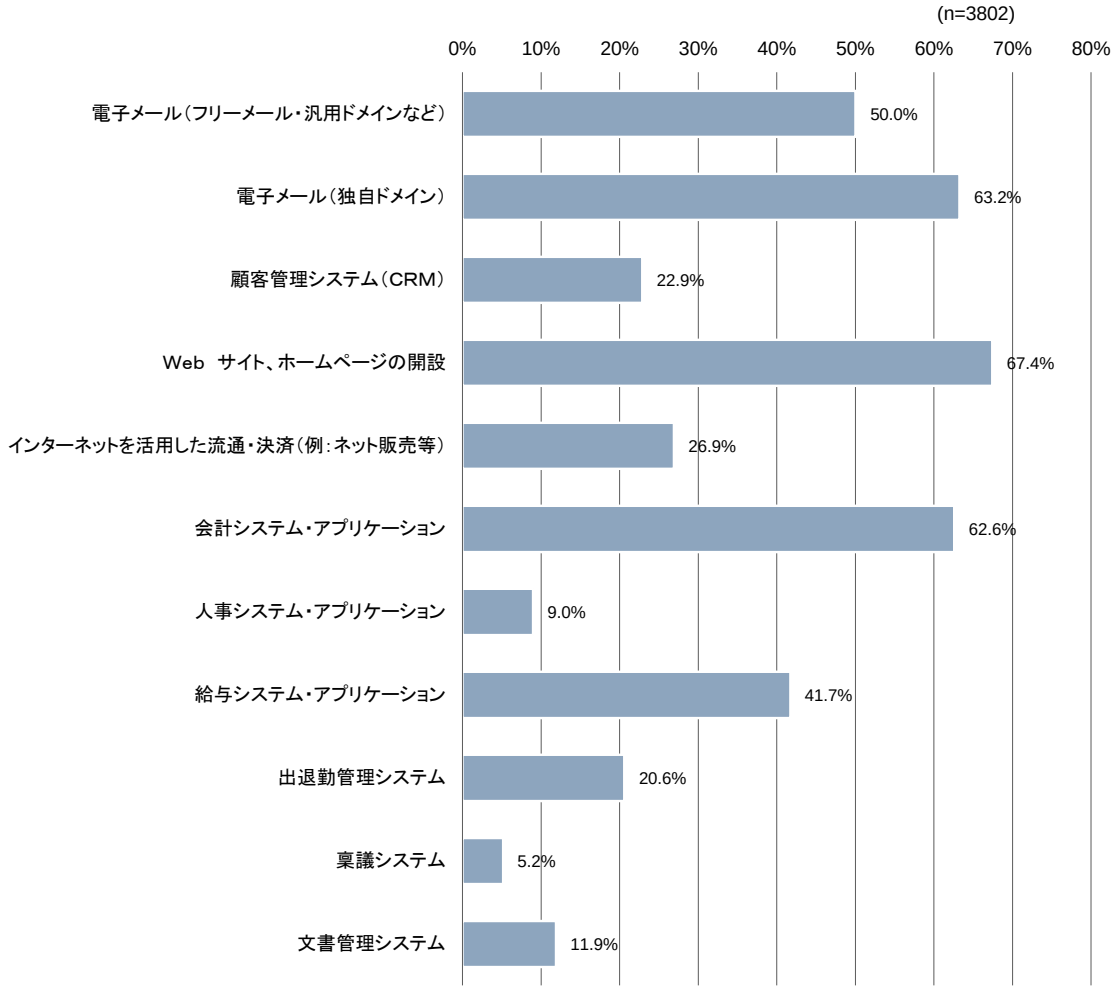
図表　2-18　業務用パソコン・タブレット端末・スマートフォンの利用状況（SA）



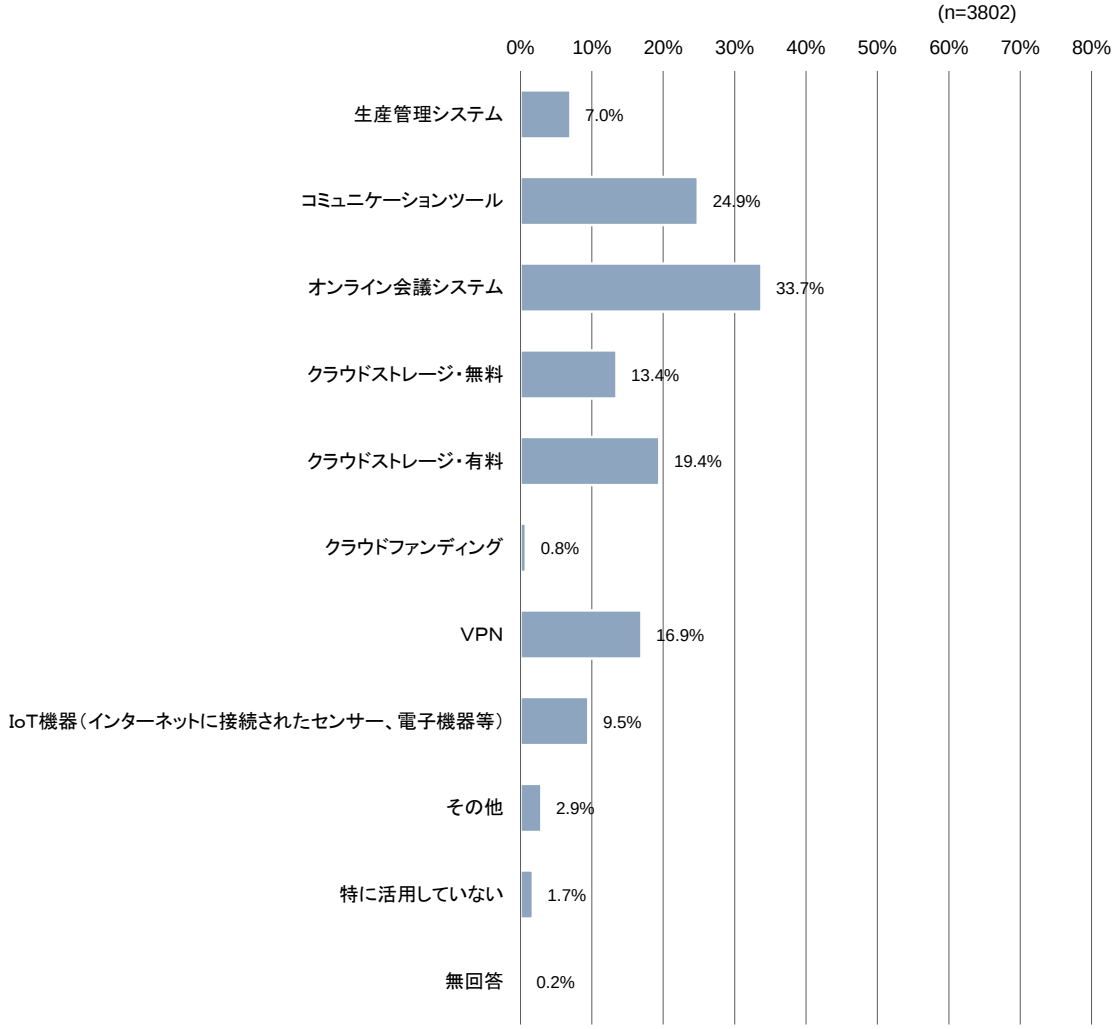
②利用・導入しているサービスやシステム

「Webサイト、ホームページの開設」の割合が最も高く67.4%となっている。次いで、「電子メール（独自ドメイン）（63.2%）」、「会計システム・アプリケーション（62.6%）」となっている。

図表 2-19 利用・導入しているサービスやシステム①（MA）



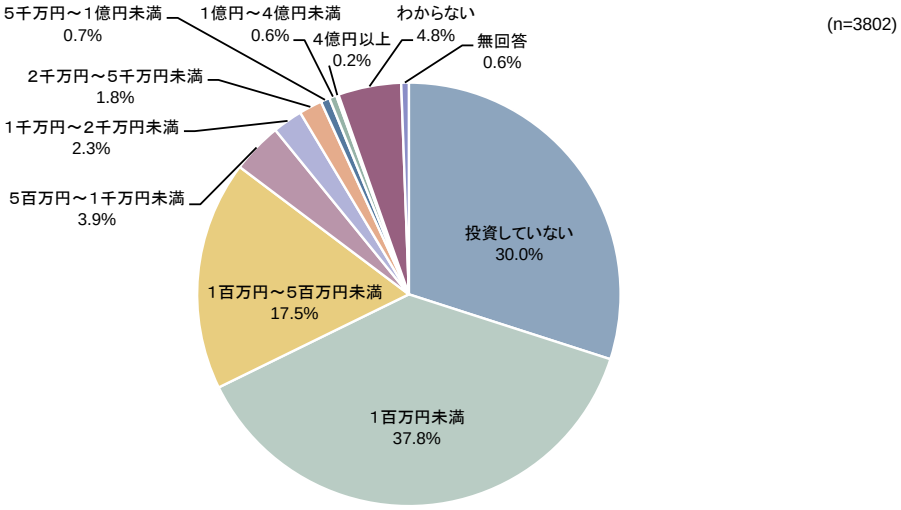
図表 2-20 利用・導入しているサービスやシステム②（MA）



③直近過去３期のIT投資額

「１百万円未満」の割合が最も高く37.8%となっている。次いで、「投資していない（30.0%）」、「１百万円～５百万円未満（17.5%）」となっている。

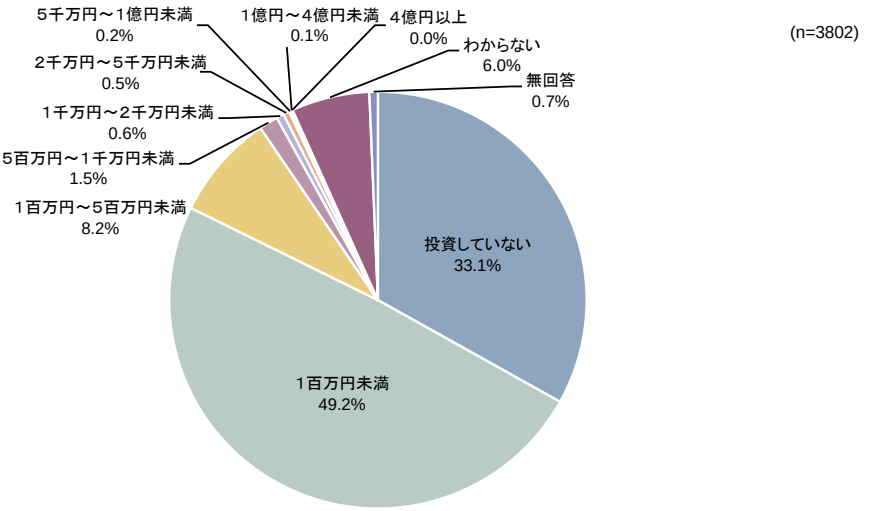
図表　2-21　直近過去３期のIT投資額（SA）



④直近過去３期の情報セキュリティ対策投資額

「１百万円未満」の割合が最も高く49.2%となっている。次いで、「投資していない（33.1%）」、「１百万円～５百万円未満（8.2%）」となっている。

図表　2-22　直近過去３期の情報セキュリティ対策投資額（SA）

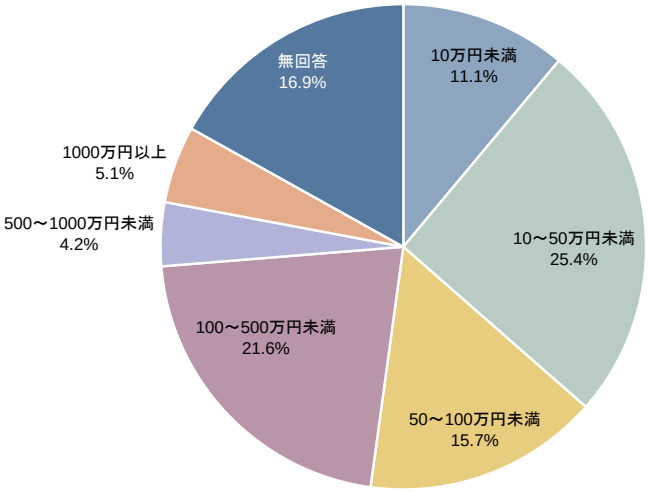


⑤直近過去１期のIT投資額

「10～50万円未満」の割合が最も高く25.4%となっている。次いで、「100～500万円未満（21.6%）」、「50～100万円未満（15.7%）」となっている。（平均値：360万円、中央値：50万円）

図表　2-23　直近過去１期のIT投資額（NA）

(n=2663)

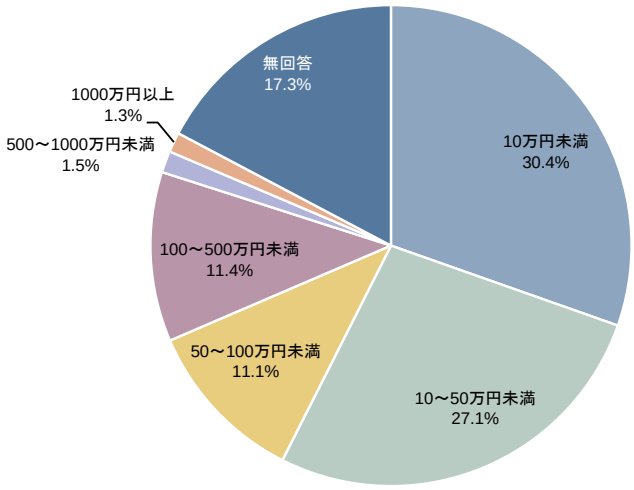


⑥直近過去１期の情報セキュリティ対策投資額

「10万円未満」の割合が最も高く30.4%となっている。次いで、「10～50万円未満（27.1%）」、「100～500万円未満（11.4%）」となっている。（平均値：113万円、中央値：12万円）

図表　2-24　直近過去１期の情報セキュリティ対策投資額（NA）

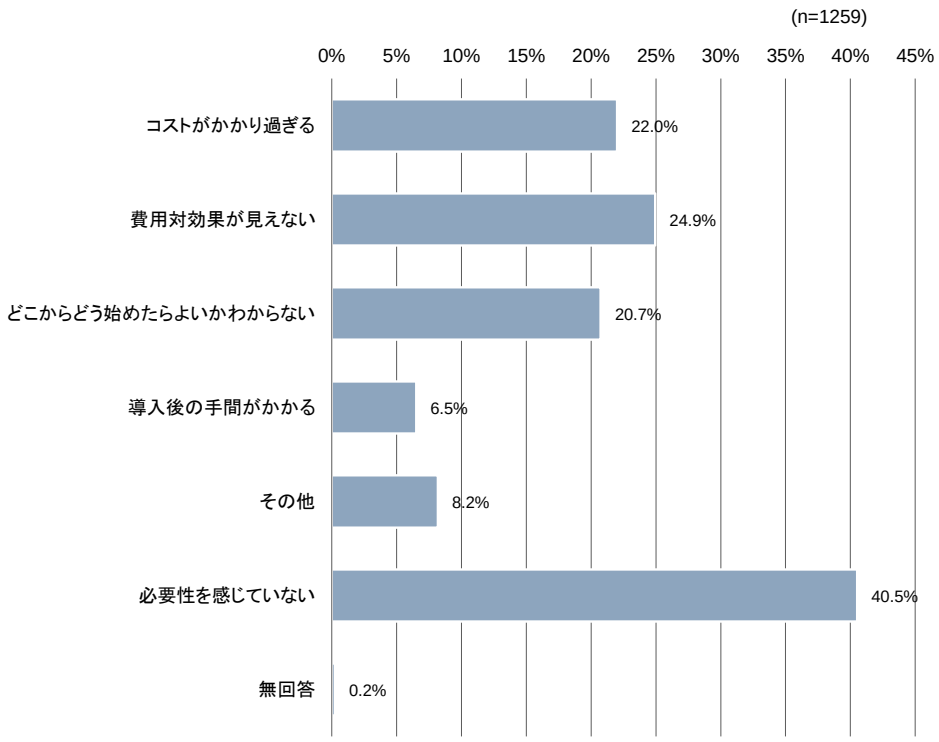
(n=2543)



⑦情報セキュリティ対策投資を行わなかった理由

「必要性を感じていない」の割合が最も高く40.5%となっている。次いで、「費用対効果が見えない（24.9%）」、「コストがかかり過ぎる（22.0%）」となっている。

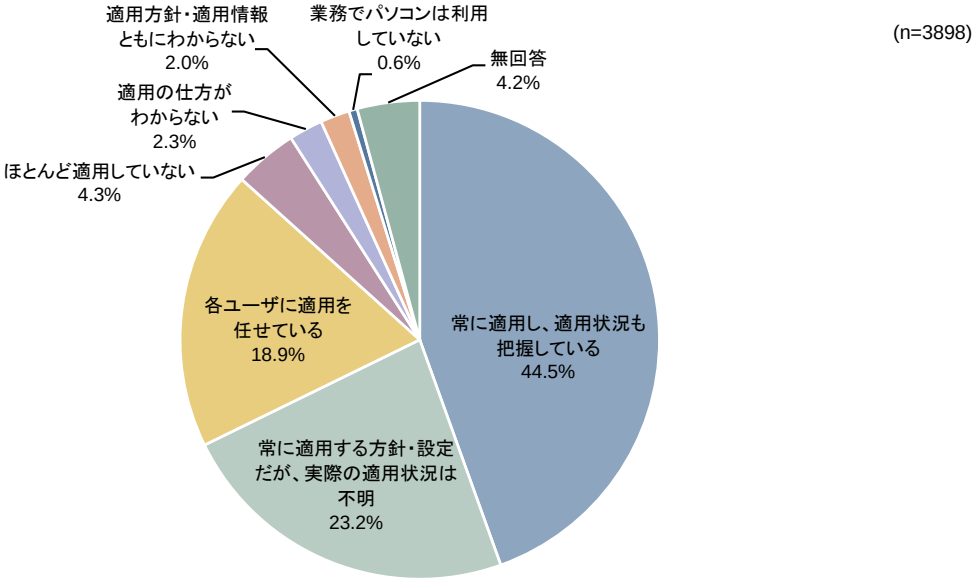
図表　2-25　情報セキュリティ対策投資を行わなかった理由（MA）



⑧パソコンへのWindows Updateなどによるセキュリティパッチの適用状況

「常に適用し、適用状況も把握している」の割合が最も高く44.5%となっている。次いで、「常に適用する方針・設定だが、実際の適用状況は不明（23.2%）」、「各ユーザに適用を任せている（18.9%）」となっている。

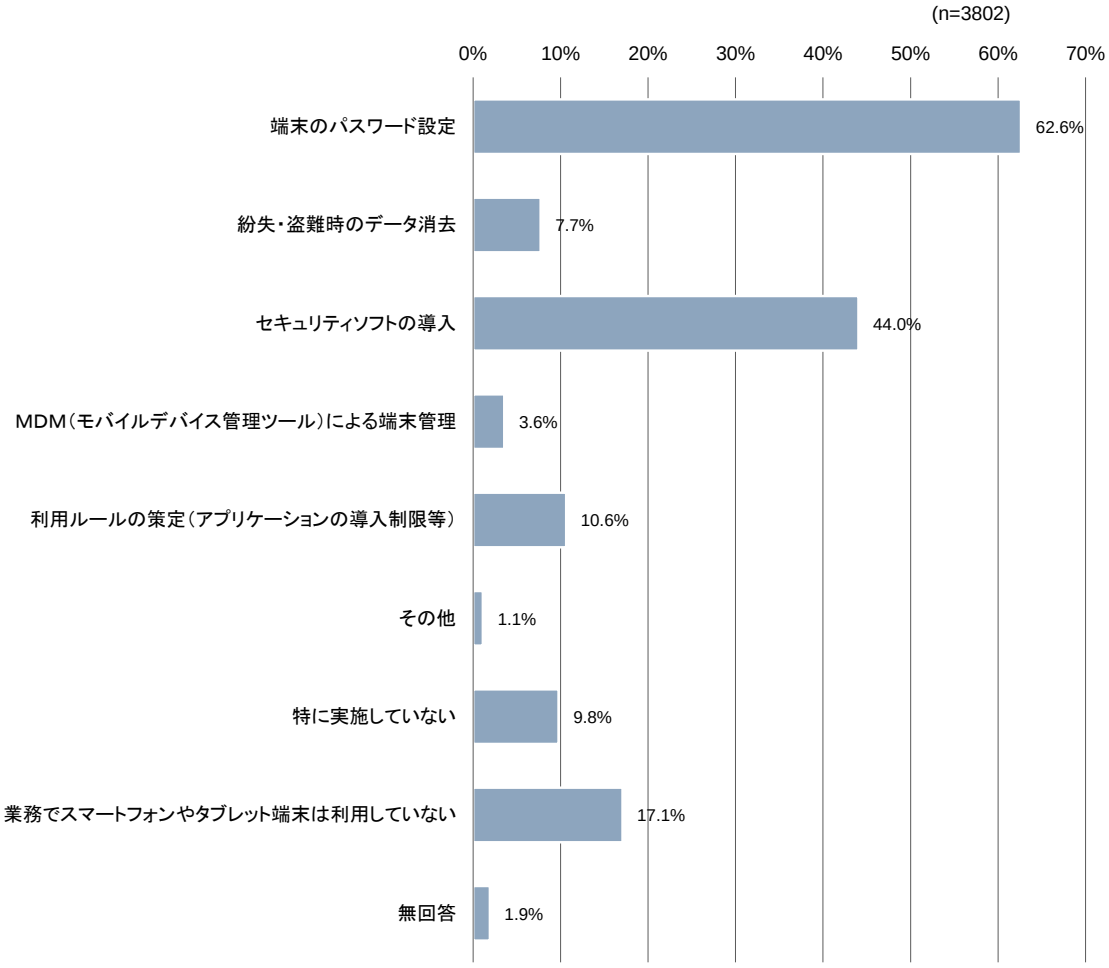
図表 2-26 パソコンへのWindows Updateなどによるセキュリティパッチの適用状況（SA）



⑨スマートフォンやタブレット端末に対して実施している対策

「端末のパスワード設定」の割合が最も高く62.6%となっている。次いで、「セキュリティソフトの導入（44.0%）」、「業務でスマートフォンやタブレット端末は利用していない（17.1%）」となっている。

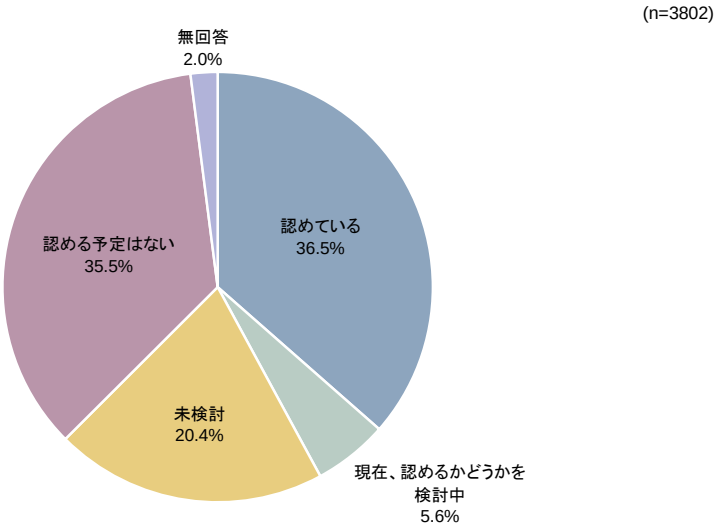
図表　2-27　スマートフォンやタブレット端末に対して実施している対策（MA）



⑩社員の私有端末の業務利用（BYOD：Bring Your Own Device）

「認めている」の割合が最も高く36.5%となっている。次いで、「認める予定はない（35.5%）」、「未検討（20.4%）」となっている。

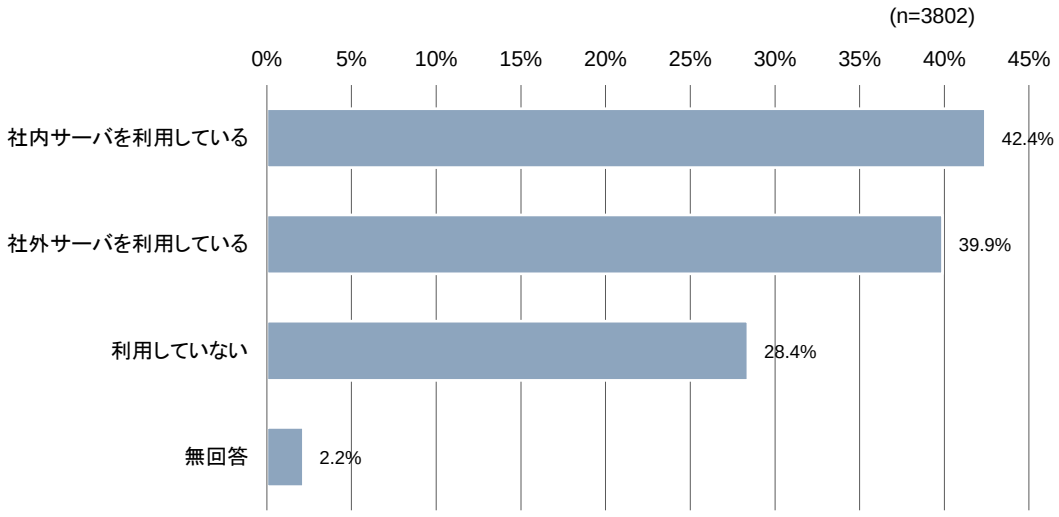
図表　2-28　社員の私有端末の業務利用（SA）



⑪サーバの利用

「社内サーバを利用している」の割合が最も高く42.4%となっている。次いで、「社外サーバを利用している（39.9%）」、「利用していない（28.4%）」となっている。

図表　2-29　サーバの利用（MA）

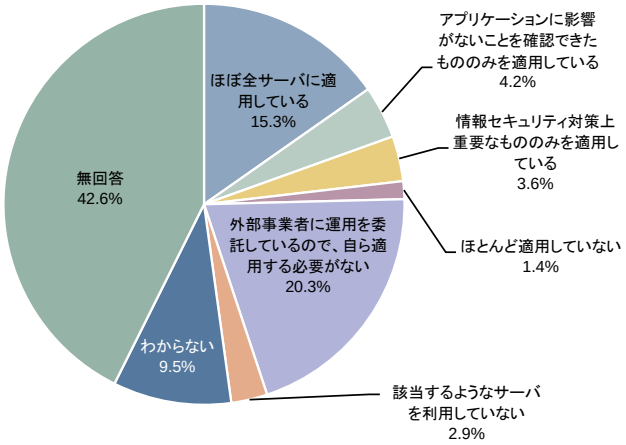


⑫セキュリティパッチの適用状況（外部に公開しているネットワークサーバ）

「外部事業者に運用を委託しているので、自ら適用する必要がない」の割合が最も高く20.3%となっている。次いで、「ほぼ全サーバに適用している（15.3%）」、「わからない（9.5%）」となっている。

図表　2-30　セキュリティパッチの適用状況（外部に公開しているネットワークサーバ）（SA）

(n=2639)

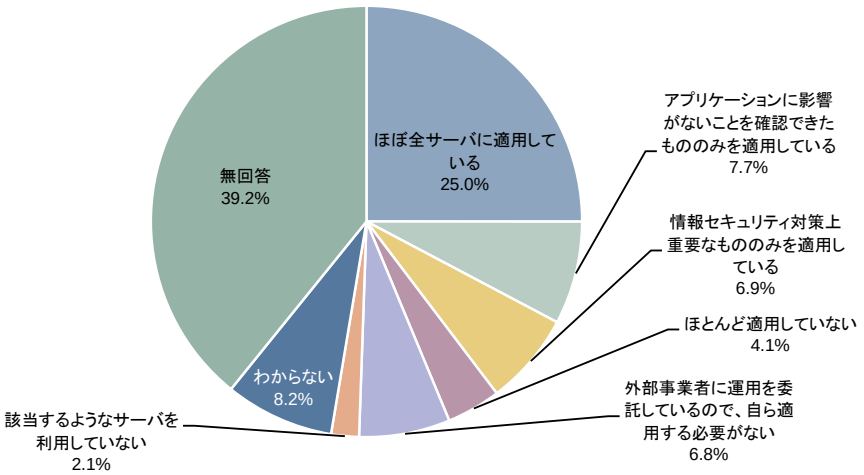


⑬セキュリティパッチの適用状況（内部で利用しているローカルサーバ）

「ほぼ全サーバに適用している」の割合が最も高く25.0%となっている。次いで、「わからない（8.2%）」、「アプリケーションに影響がないことを確認できたもののみを適用している（7.7%）」となっている。

図表　2-31　セキュリティパッチの適用状況（内部で利用しているローカルサーバ）（SA）

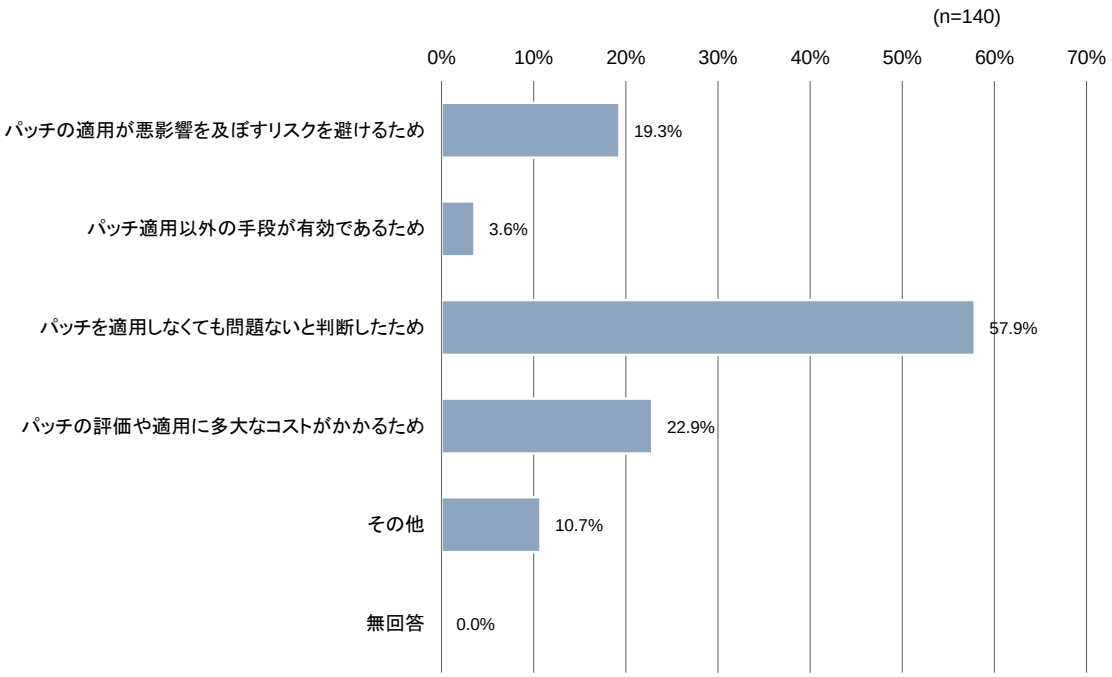
(n=2639)



⑭セキュリティパッチを適用しない理由

「パッチを適用しなくても問題ないと判断したため」の割合が最も高く57.9%となっている。次いで、「パッチの評価や適用に多大なコストがかかるため（22.9%）」、「パッチの適用が悪影響を及ぼすリスクを避けるため（19.3%）」となっている。

図表 2-32 セキュリティパッチを適用しない理由（MA）

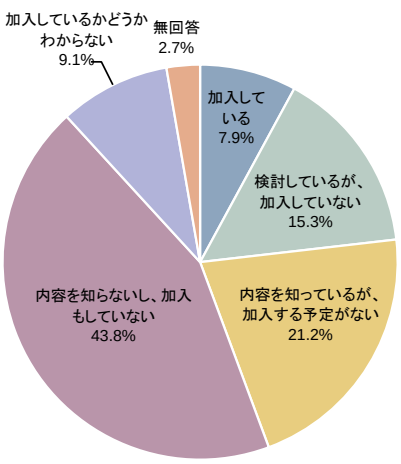


⑮保険への加入（サイバー保険）

「内容を知らないし、加入もしていない」の割合が最も高く43.8%となっている。次いで、「内容を知っているが、加入する予定がない（21.2%）」、「検討しているが、加入していない（15.3%）」となっている。

図表　2-33　保険への加入（サイバー保険）（SA）

(n=3802)

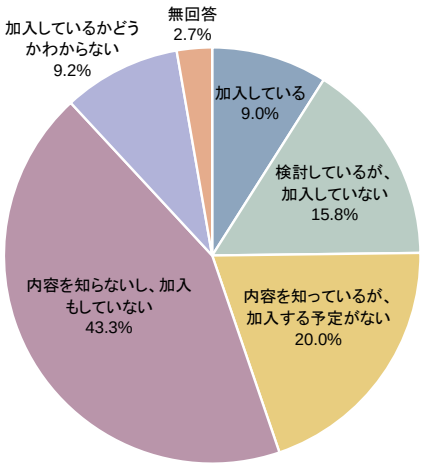


⑯保険への加入（情報漏えい賠償責任保険）

「内容を知らないし、加入もしていない」の割合が最も高く43.3%となっている。次いで、「内容を知っているが、加入する予定がない（20.0%）」、「検討しているが、加入していない（15.8%）」となっている。

図表　2-34　保険への加入（情報漏えい賠償責任保険）（SA）

(n=3802)



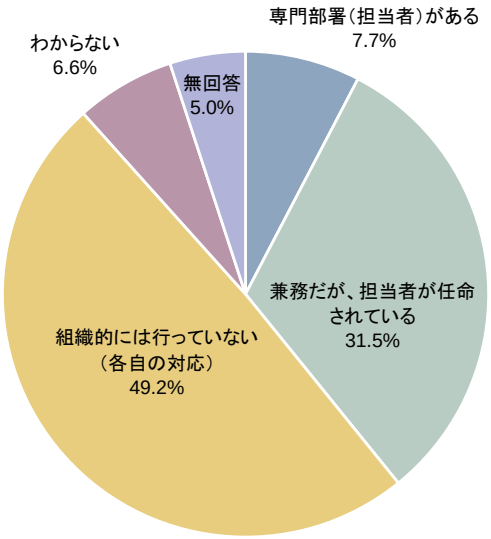
（３）情報セキュリティに関する意識・状況

①組織体制

「組織的には行っていない（各自の対応）」の割合が最も高く49.2%となっている。次いで、「兼務だが、担当者が任命されている（31.5%）」、「専門部署（担当者）がある（7.7%）」となっている。

図表 2-35 組織体制（SA）

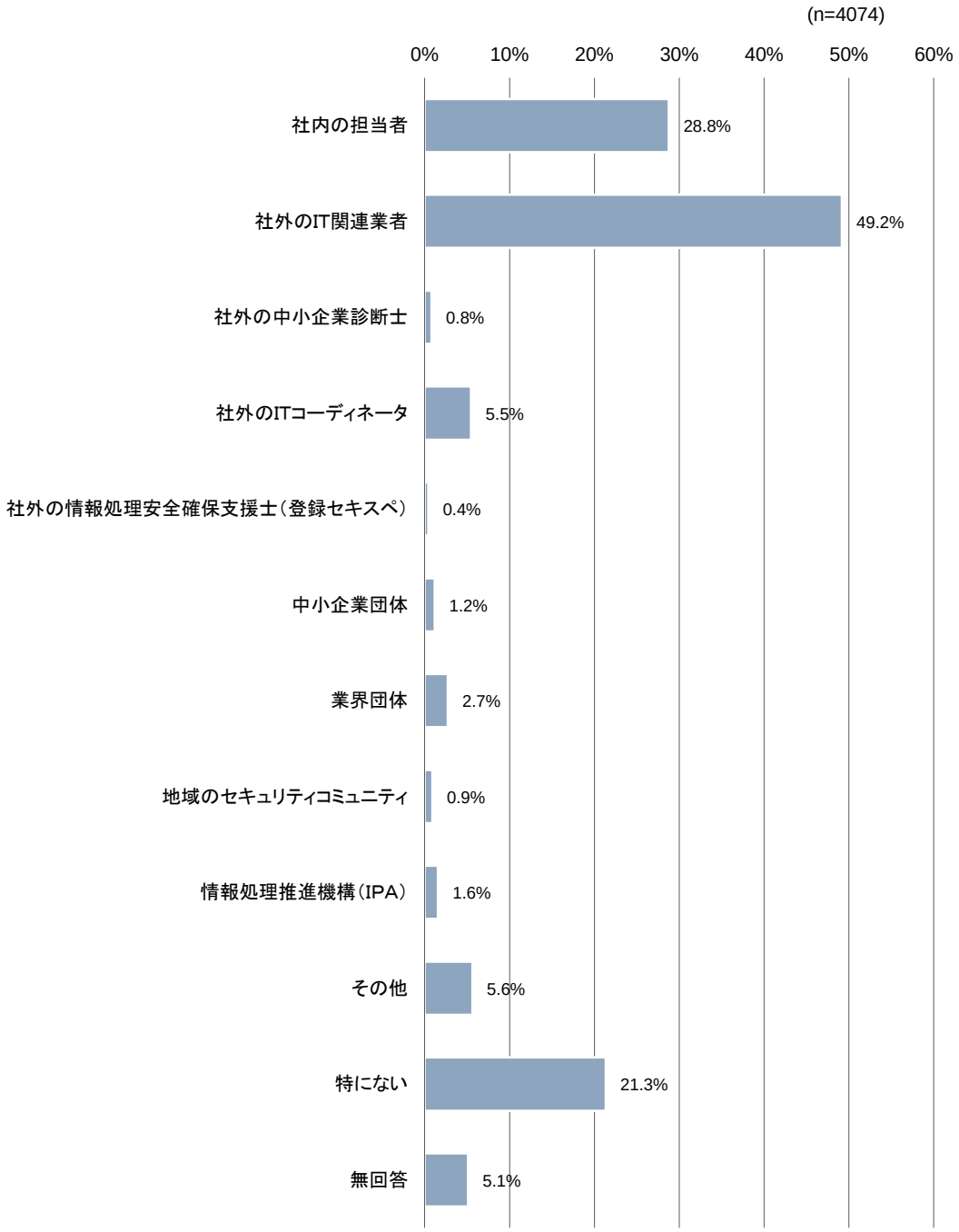
(n=4074)



②困ったことがあった際の相談先

「社外のIT関連業者」の割合が最も高く49.2%となっている。次いで、「社内の担当者（28.8%）」、「特にない（21.3%）」となっている。

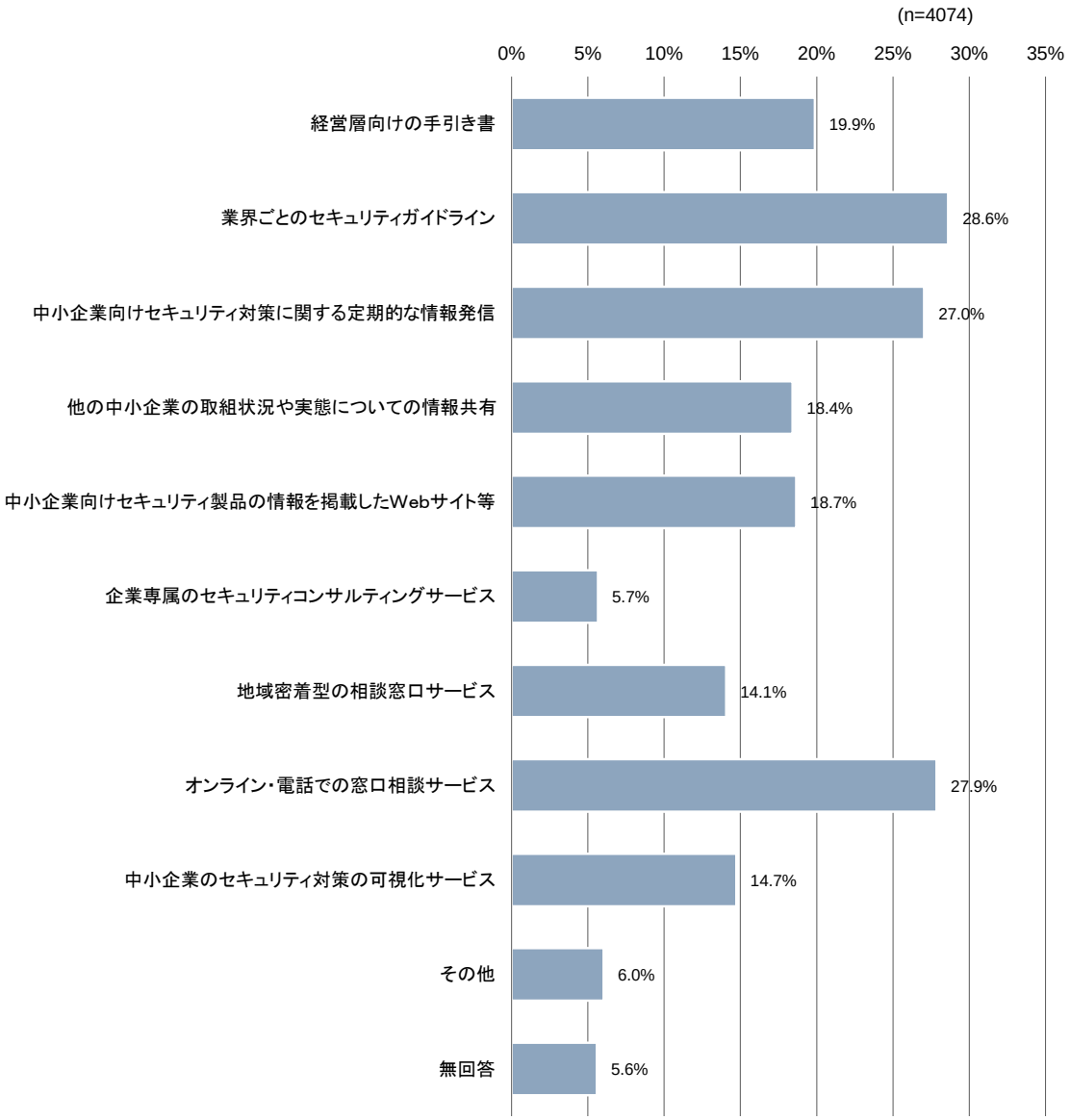
図表 2-36 困ったことがあった際の相談先（MA）



③活用したい情報セキュリティ対策に関するサービス

「業界ごとのセキュリティガイドライン」の割合が最も高く28.6%となっている。次いで、「オンライン・電話での窓口相談サービス（27.9%）」、「中小企業向けセキュリティ対策に関する定期的な情報発信（27.0%）」となっている。

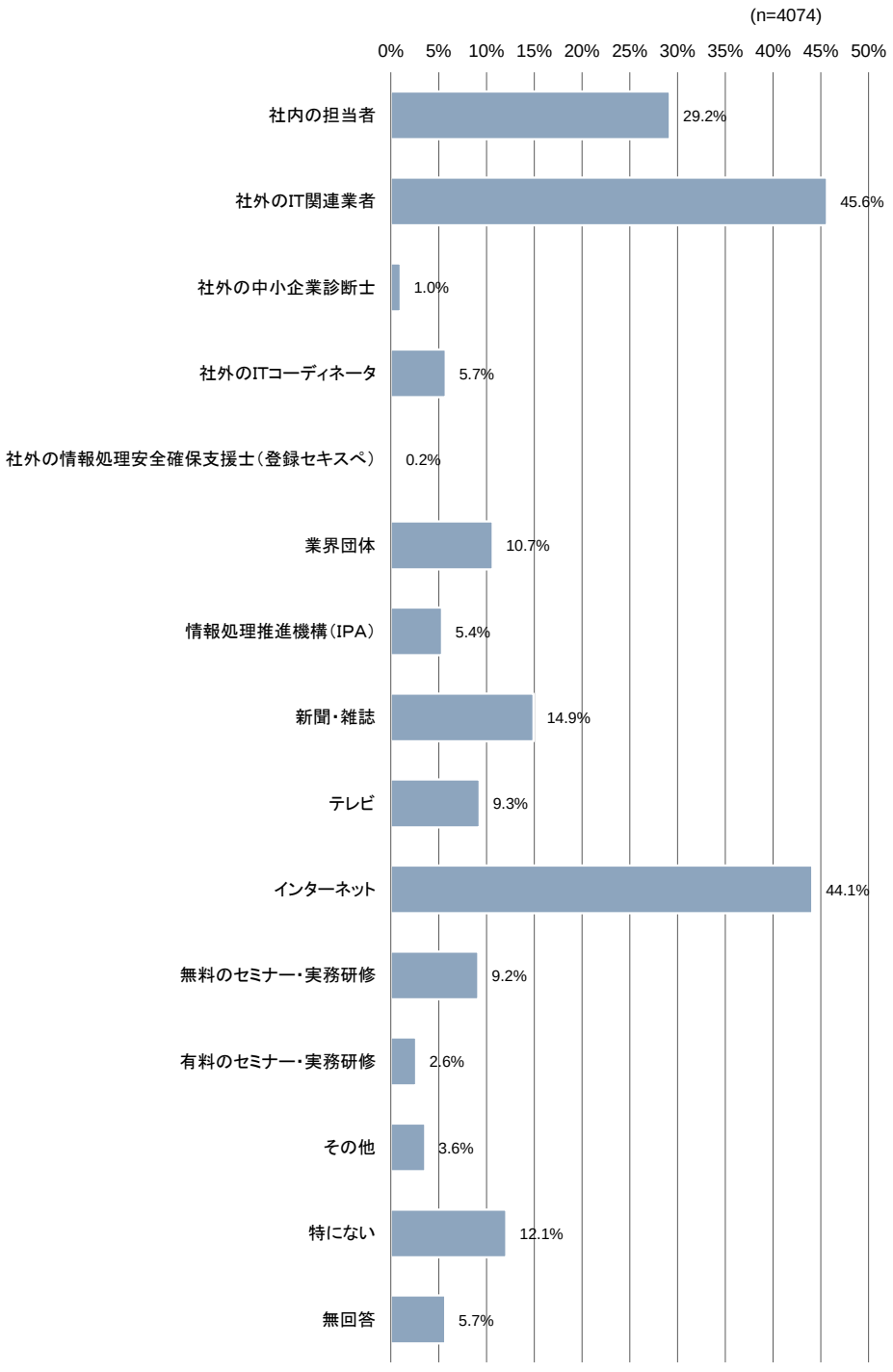
図表　2-37　活用したい情報セキュリティ対策に関するサービス（MA）



④情報セキュリティに関する情報収集先

「社外のIT関連業者」の割合が最も高く45.6%となっている。次いで、「インターネット（44.1%）」、「社内の担当者（29.2%）」となっている。

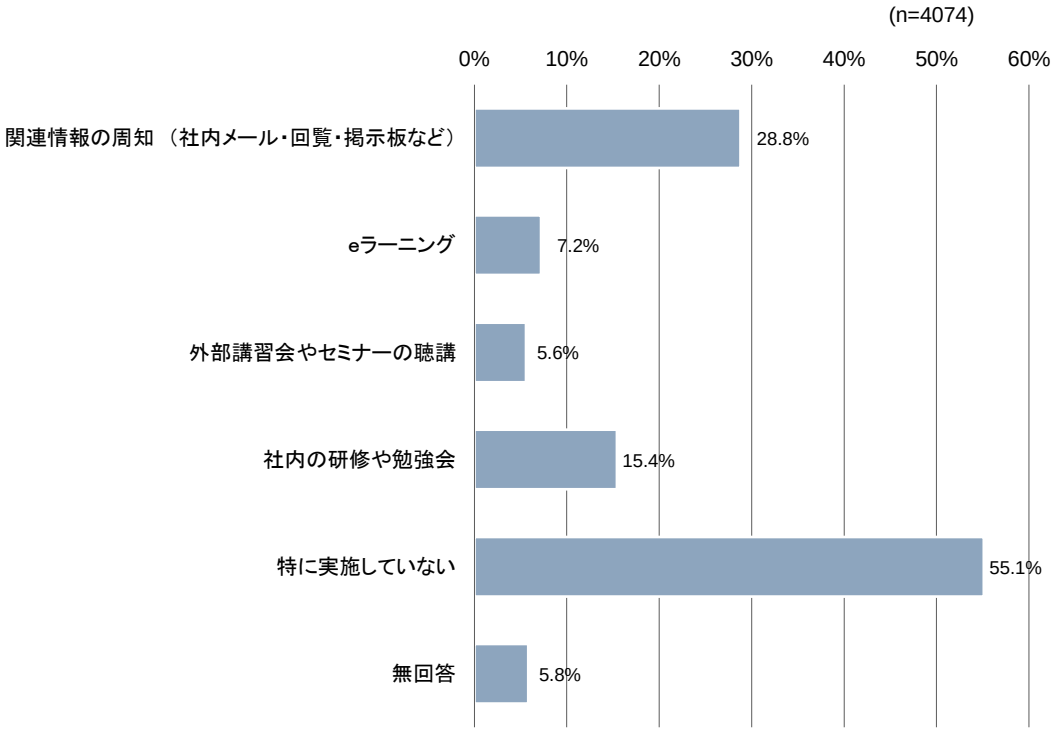
図表 2-38 情報セキュリティに関する情報収集先（MA）



⑤従業員に対する情報セキュリティ教育の実施状況

「特に実施していない」の割合が最も高く55.1%となっている。次いで、「関連情報の周知　（社内メール・回覧・掲示板など）（28.8%）」、「社内の研修や勉強会（15.4%）」となっている。

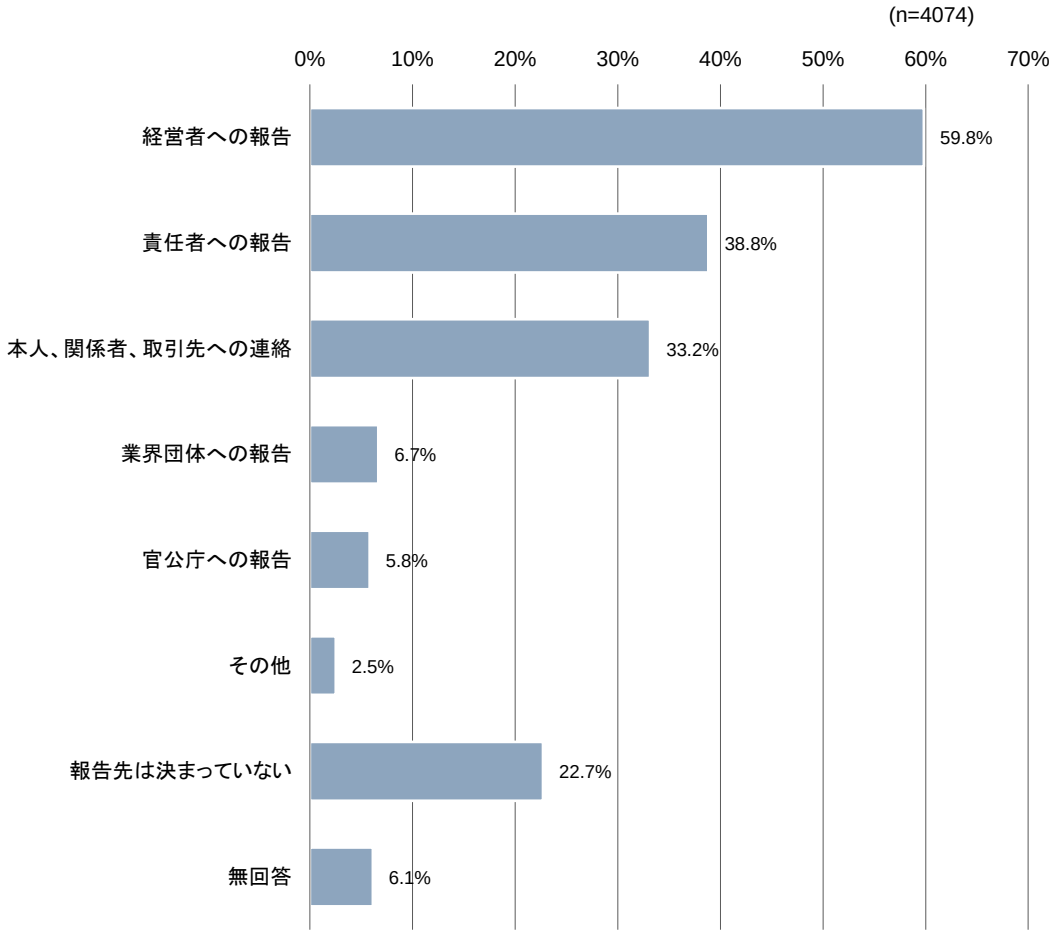
図表　2-39　従業員に対する情報セキュリティ教育の実施状況（MA）



⑥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

「経営者への報告」の割合が最も高く59.8%となっている。次いで、「責任者への報告（38.8%）」、「本人、関係者、取引先への連絡（33.2%）」となっている。

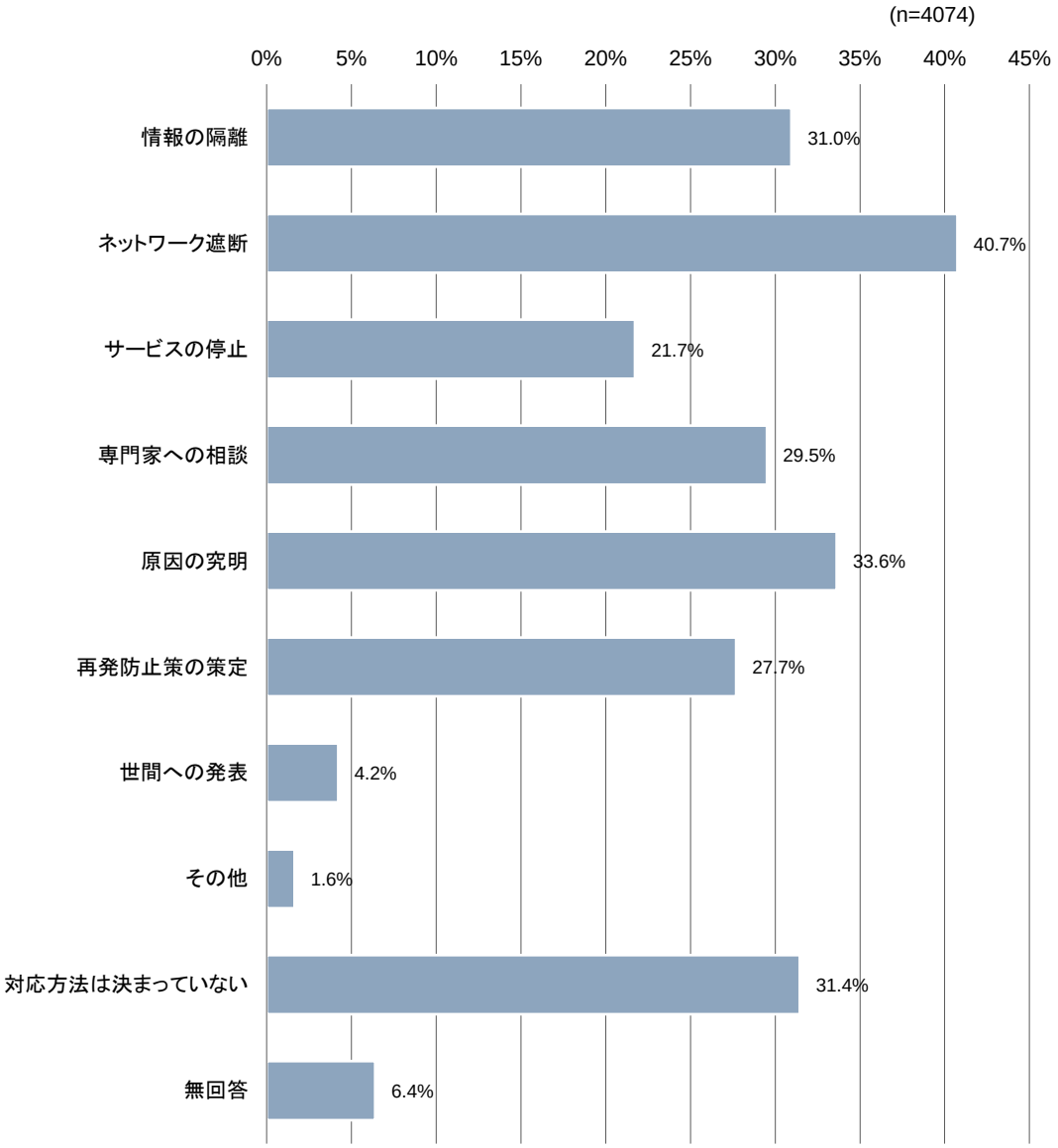
図表　2-40　情報漏えい等のインシデント又はその兆候を発見した場合の報告先（MA）



⑦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

「ネットワーク遮断」の割合が最も高く40.7%となっている。次いで、「原因の究明（33.6%）」、「対応方法は決まっていない（31.4%）」となっている。

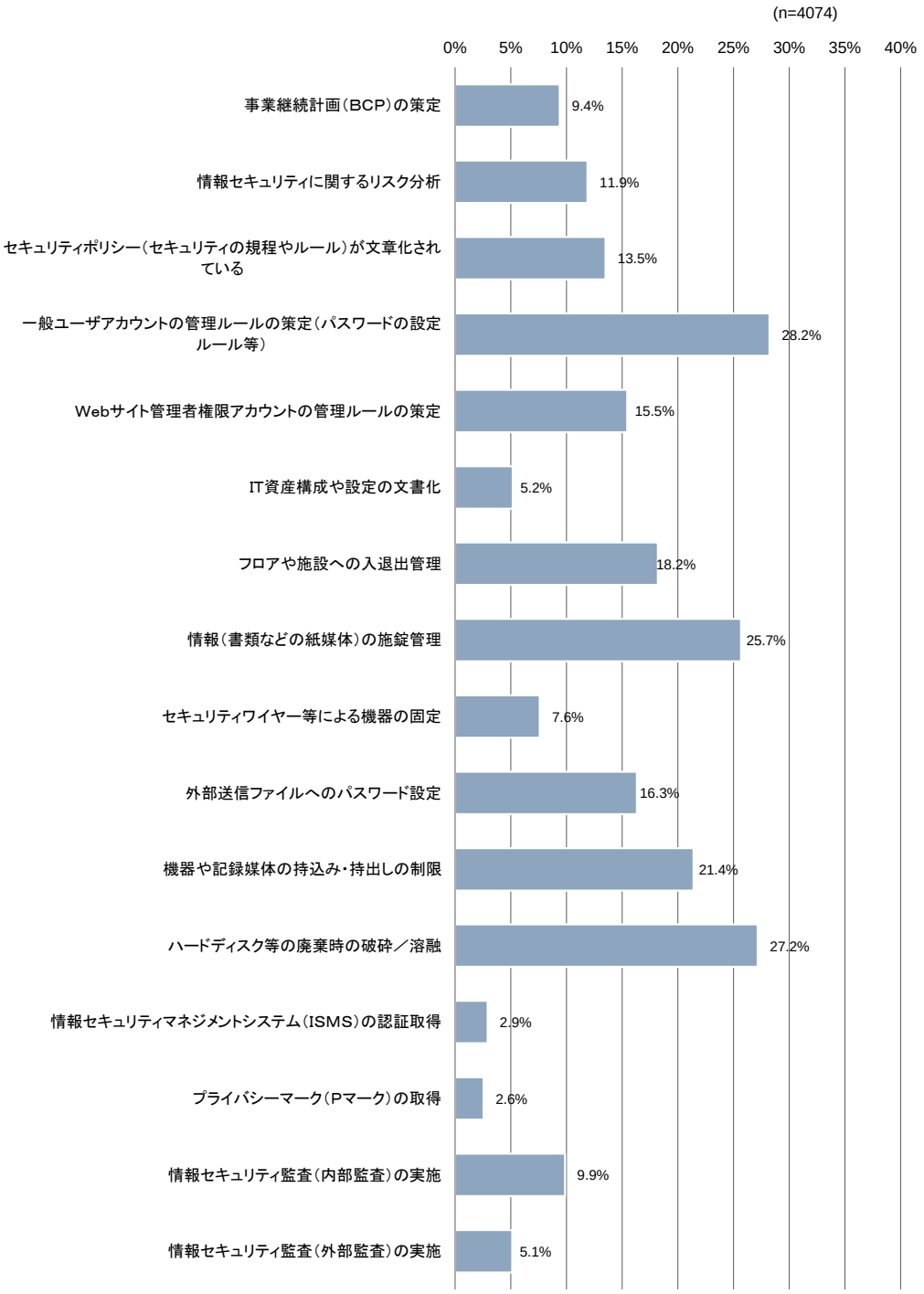
図表 2-41 情報漏えい等のインシデント又はその兆候を発見した場合の対応方法（MA）



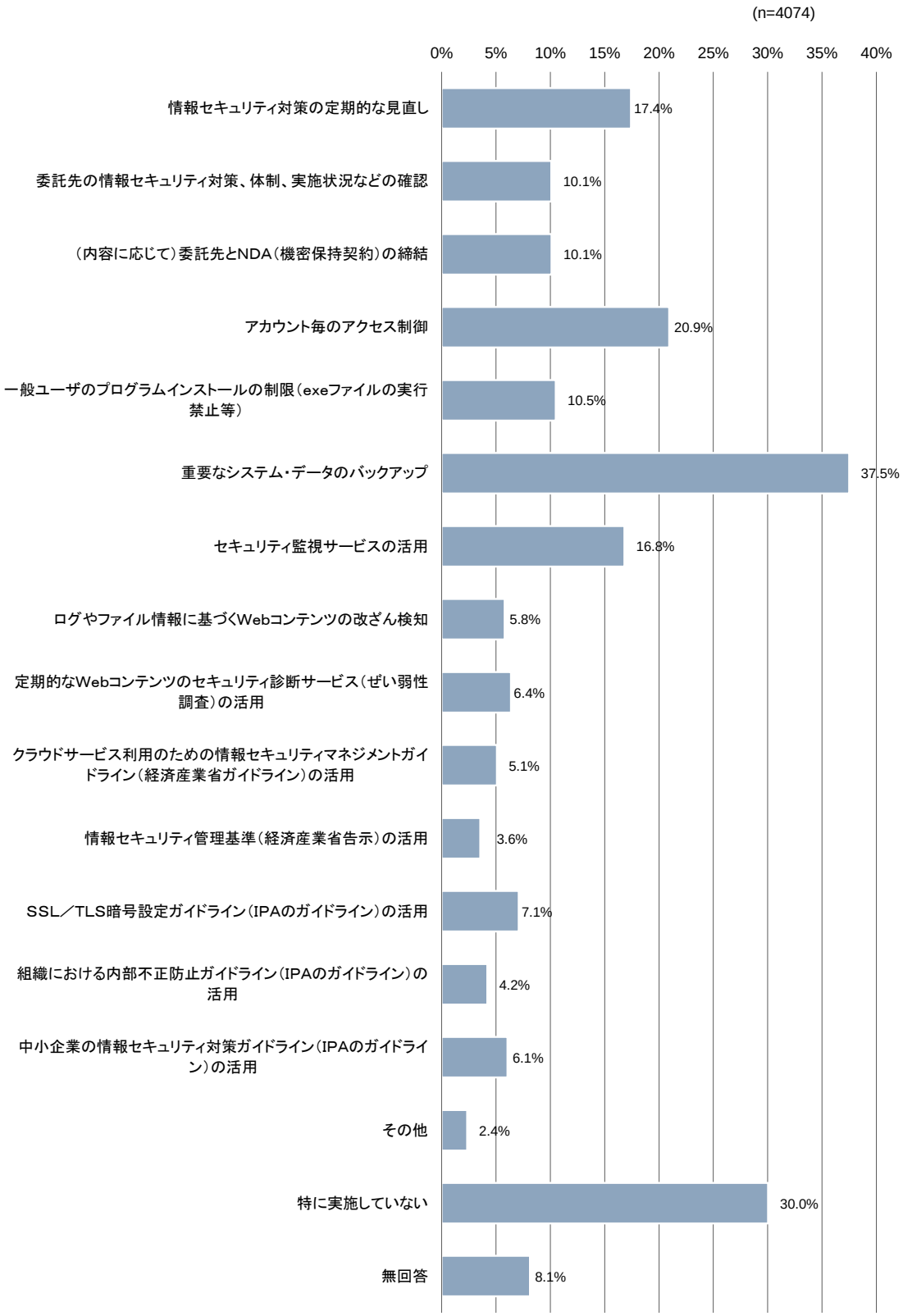
⑧被害防止のための組織面・運用面の対策

「重要なシステム・データのバックアップ」の割合が最も高く37.5%となっている。次いで、「特に実施していない（30.0%）」、「一般ユーザアカウントの管理ルールの策定（パスワードの設定ルール等）（28.2%）」となっている。

図表 2-42 被害防止のための組織面・運用面の対策①（MA）



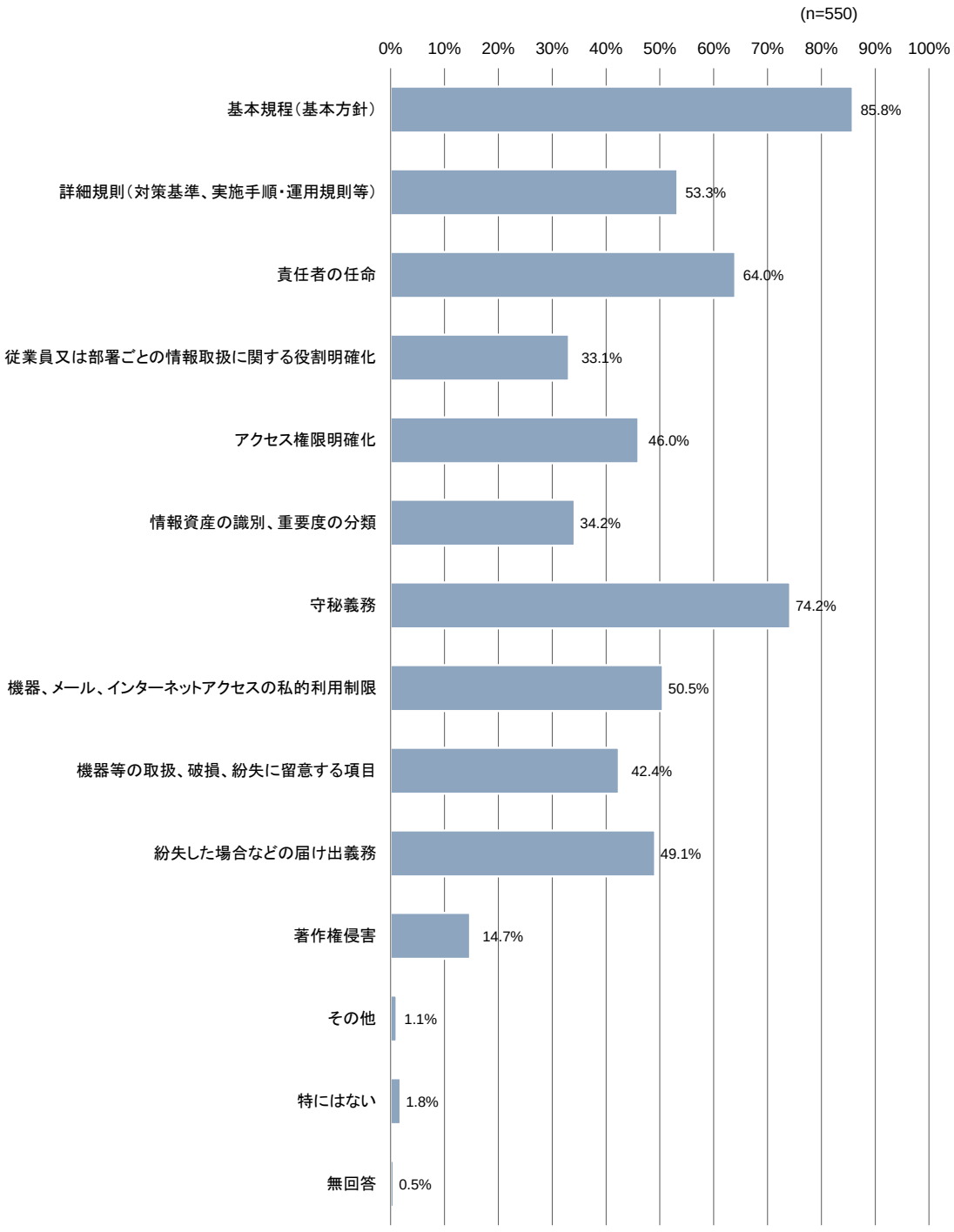
図表　2-43　被害防止のための組織面・運用面の対策②（MA）



⑨社内のセキュリティポリシー規定

「基本規程（基本方針）」の割合が最も高く85.8%となっている。次いで、「守秘義務（74.2%）」、「責任者の任命（64.0%）」となっている。

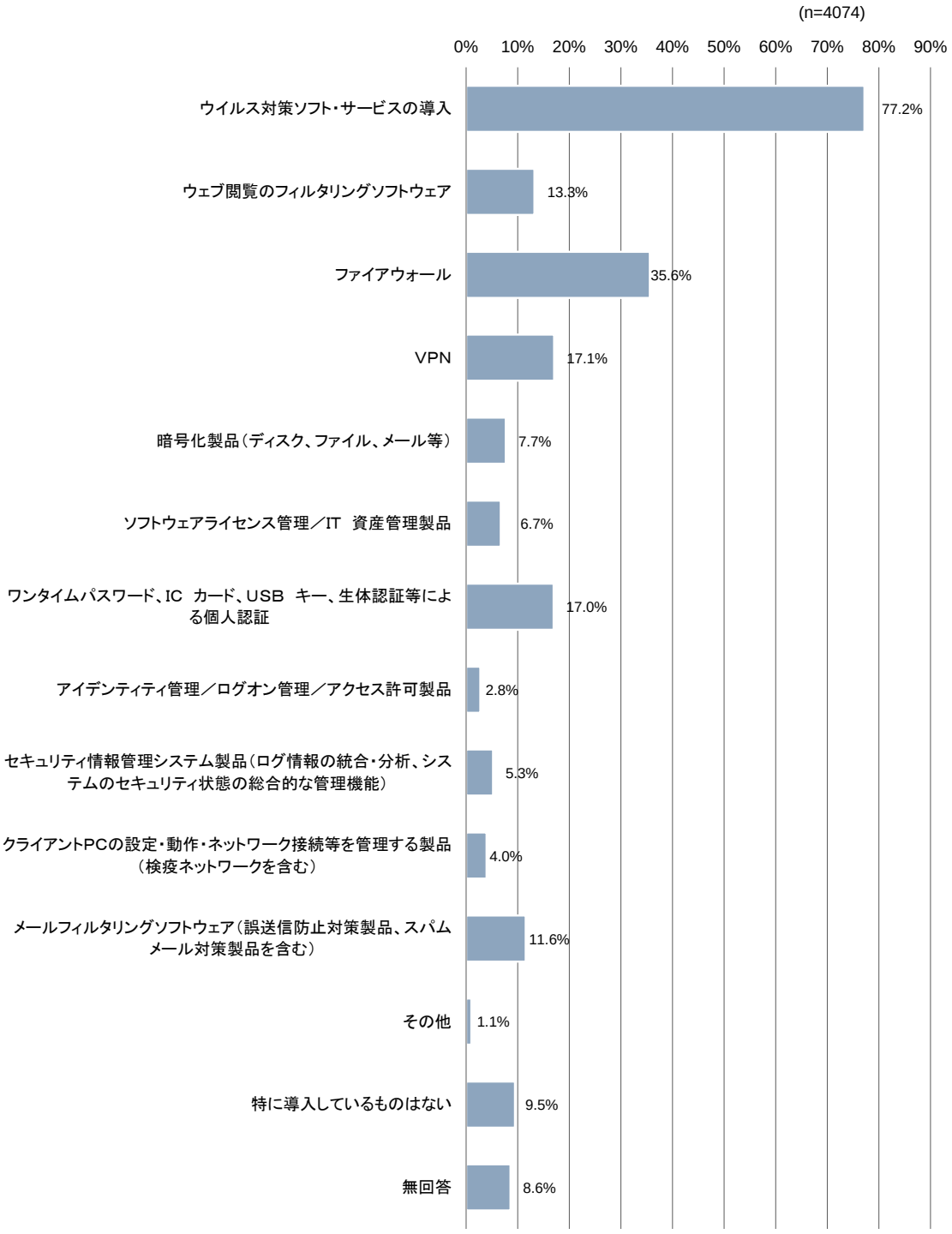
図表　2-44　社内のセキュリティポリシー規定（MA）



⑩情報セキュリティ関連製品やサービスの導入状況

「ウイルス対策ソフト・サービスの導入」の割合が最も高く77.2%となっている。次いで、「ファイアウォール（35.6%）」、「VPN（17.1%）」となっている。

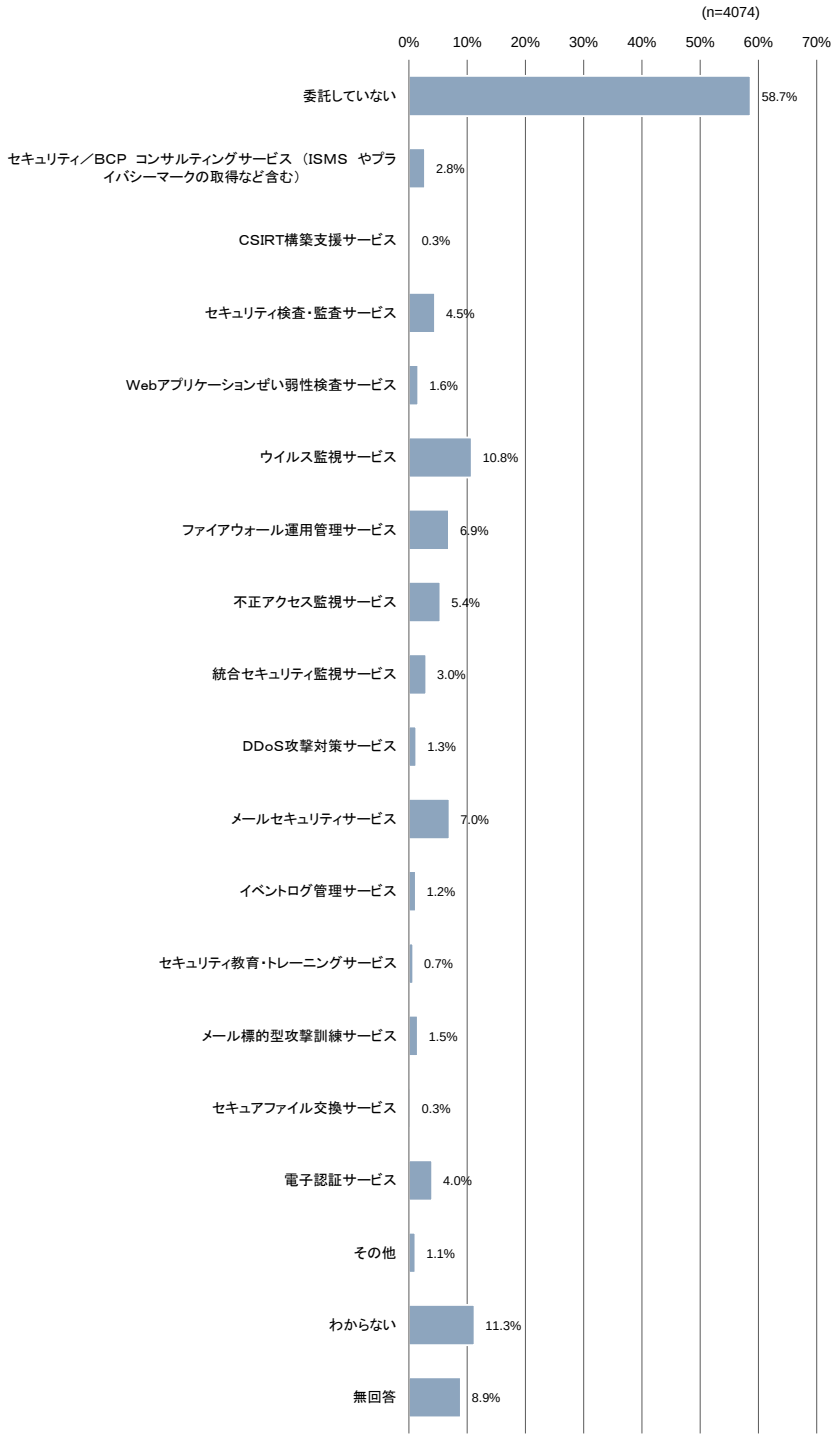
図表　2-45　情報セキュリティ関連製品やサービスの導入状況（MA）



⑪情報セキュリティ業務の外部委託の状況・内容

「委託していない」の割合が最も高く58.7%となっている。次いで、「わからない（11.3%）」、「ウイルス監視サービス（10.8%）」となっている。

図表 2-46 情報セキュリティ業務の外部委託の状況・内容（MA）

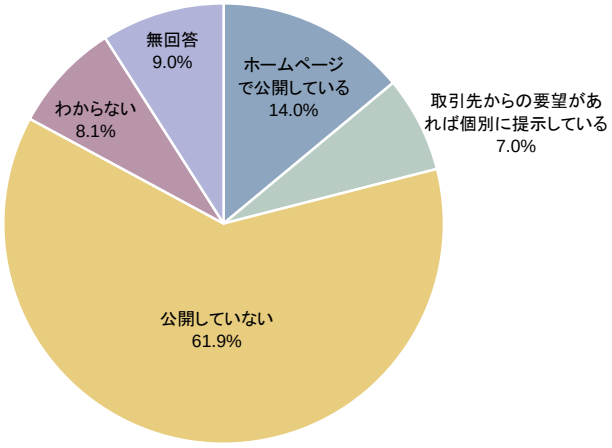


⑫情報セキュリティ対策の実施内容についての外部への公開状況

「公開していない」の割合が最も高く61.9%となっている。次いで、「ホームページで公開している（14.0%）」、「わからない（8.1%）」となっている。

図表　2-47　情報セキュリティ対策の実施内容についての外部への公開状況（SA）

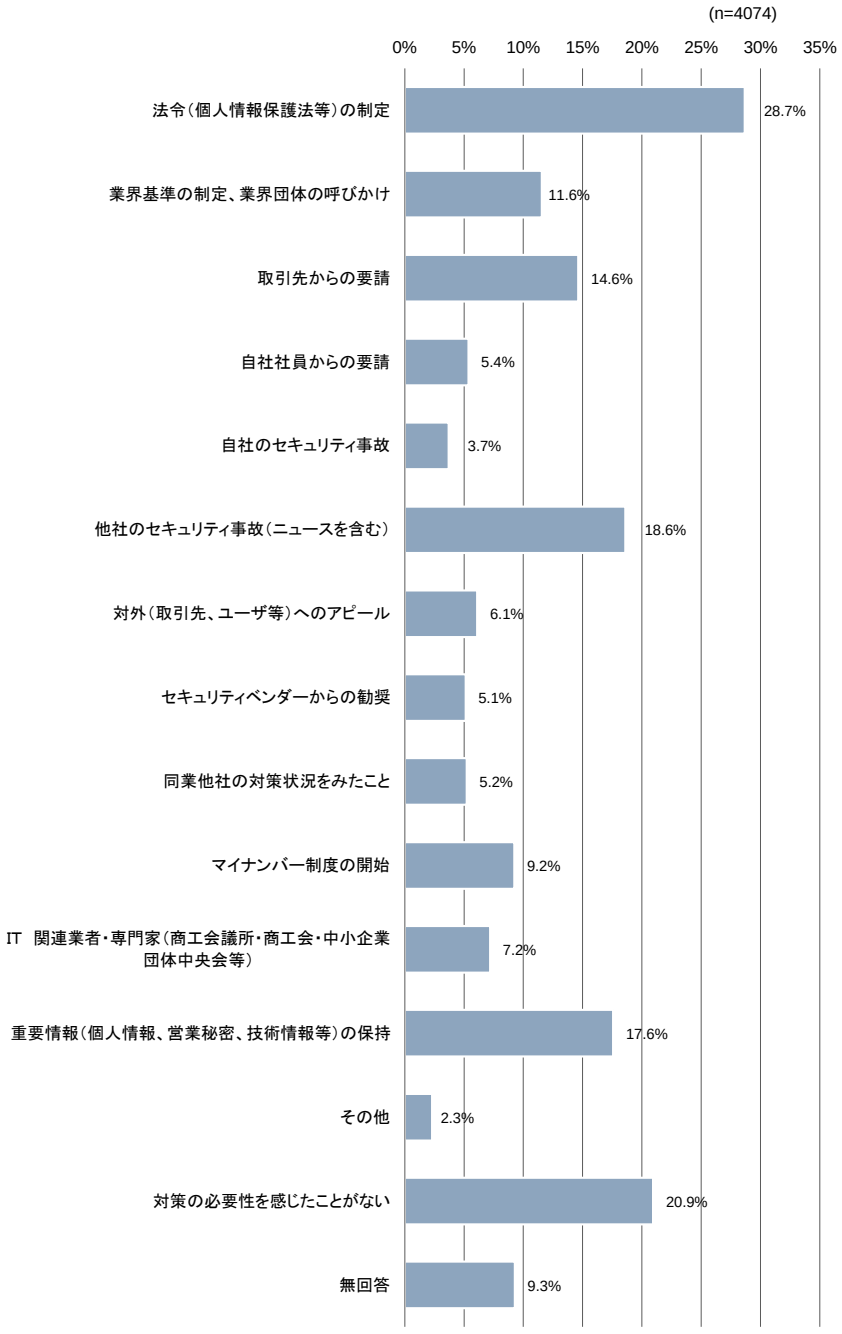
(n=4074)



⑬情報セキュリティ対策の必要性を感じたきっかけ

「法令（個人情報保護法等）の制定」の割合が最も高く28.7%となっている。次いで、「対策の必要性を感じたことがない（20.9%）」、「他社のセキュリティ事故（ニュースを含む）（18.6%）」となっている。

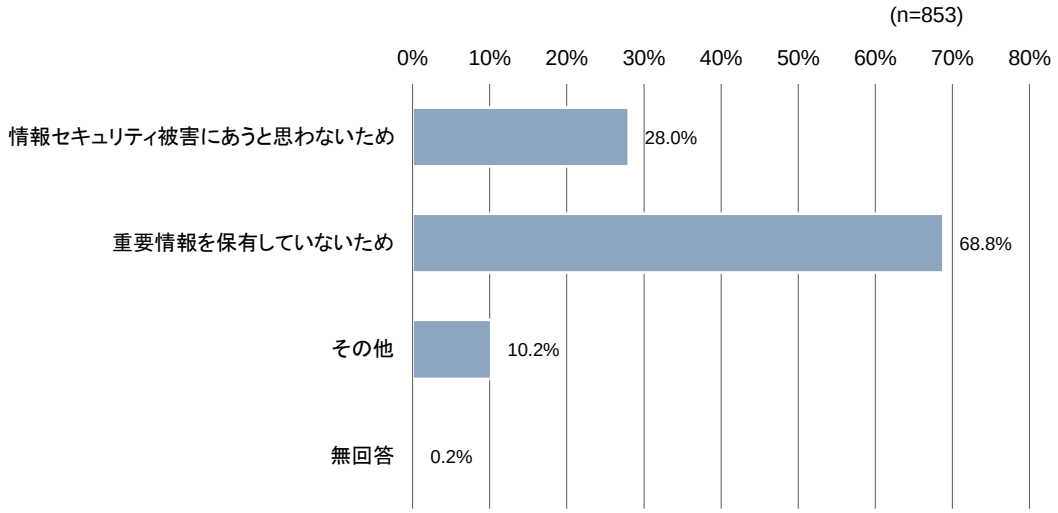
図表 2-48 情報セキュリティ対策の必要性を感じたきっかけ（MA）



⑭情報セキュリティ対策の必要性を感じない理由

「重要情報を保有していないため」の割合が最も高く68.8%となっている。次いで、「情報セキュリティ被害にあうと思わないため（28.0%）」、「その他（10.2%）」となっている。

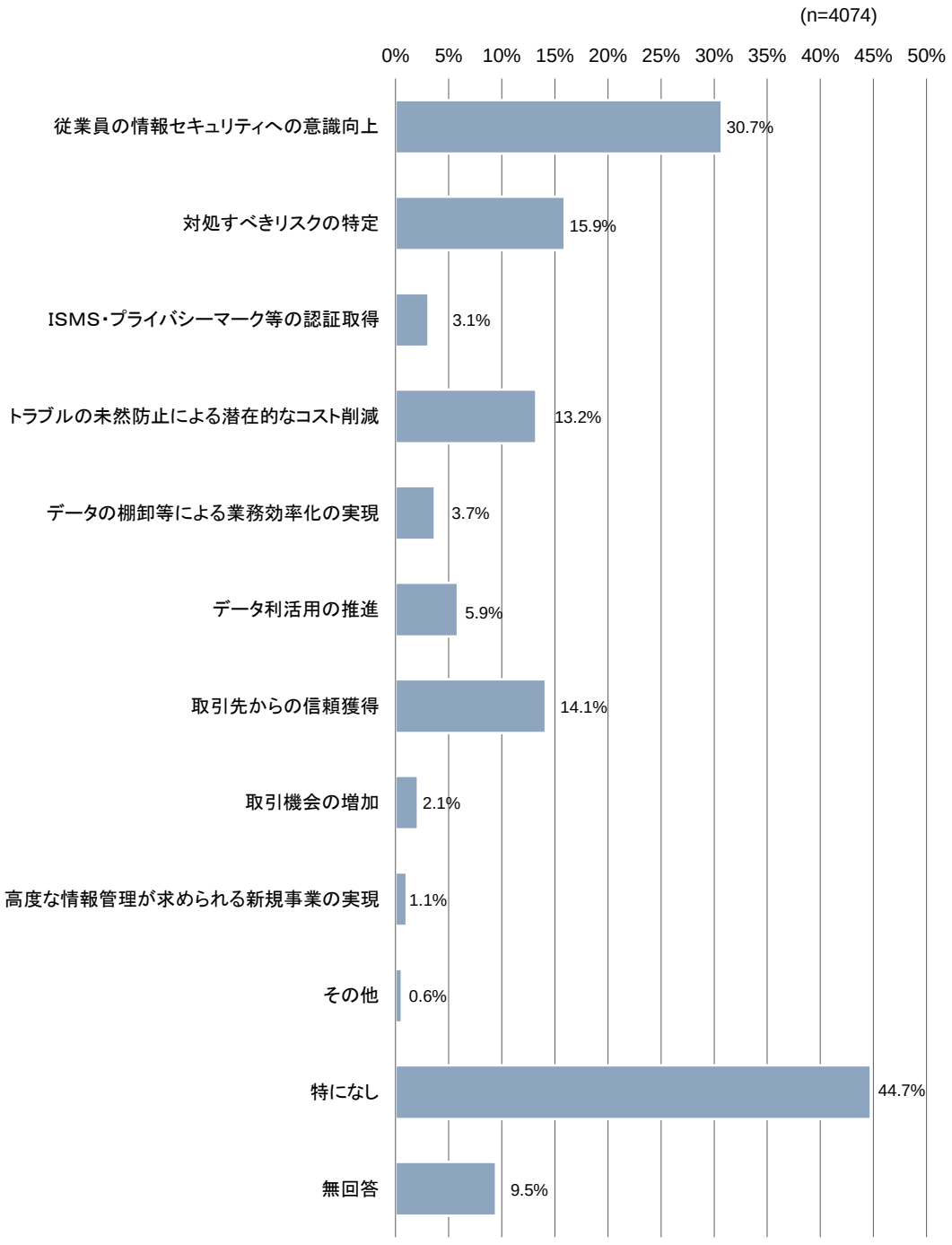
図表 2-49 情報セキュリティ対策の必要性を感じない理由（MA）



⑮情報セキュリティ対策を実施して感じられたメリット

「特になし」の割合が最も高く44.7%となっている。次いで、「従業員の情報セキュリティへの意識向上（30.7%）」、「対処すべきリスクの特定（15.9%）」となっている。

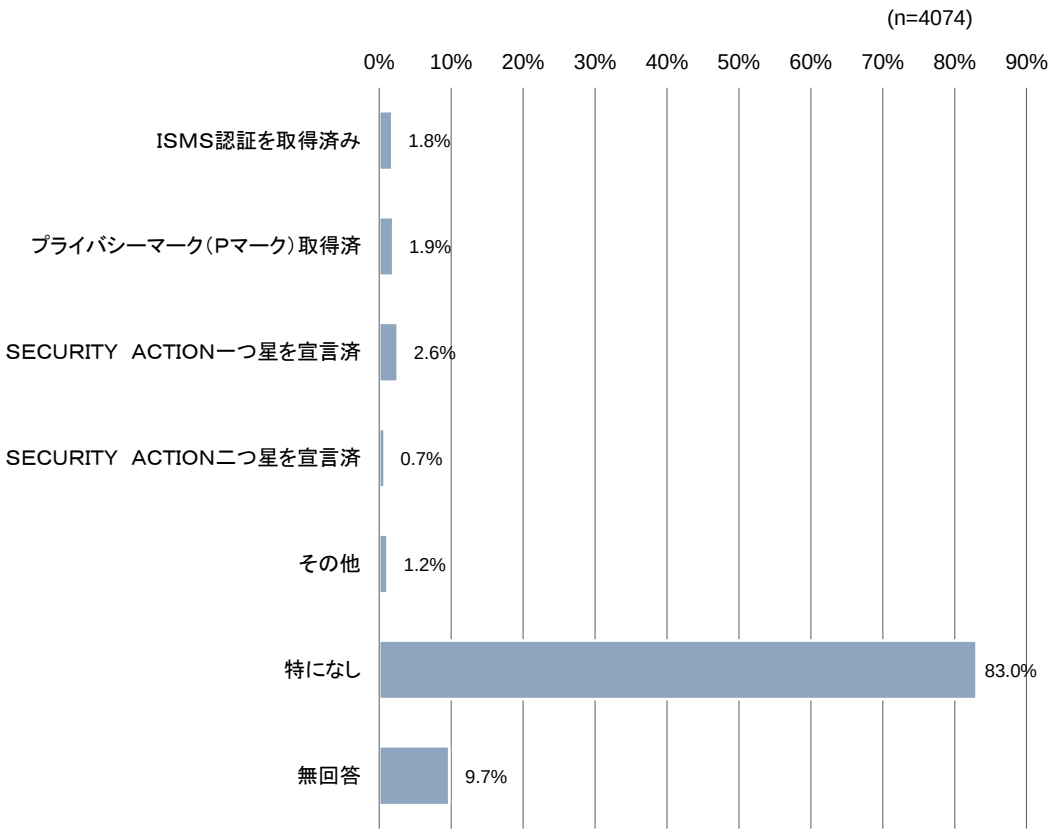
図表 2-50 情報セキュリティ対策を実施して感じられたメリット（MA）



⑯認証取得や自己宣言の実施状況

「特になし」の割合が最も高く83.0%となっている。次いで「SECURITY ACTION一つ星を宣言済（2.6%）」、「プライバシーマーク（Ｐマーク）取得済（1.9%）」となっている。

図表 2-51 認証取得や自己宣言の実施状況（MA）



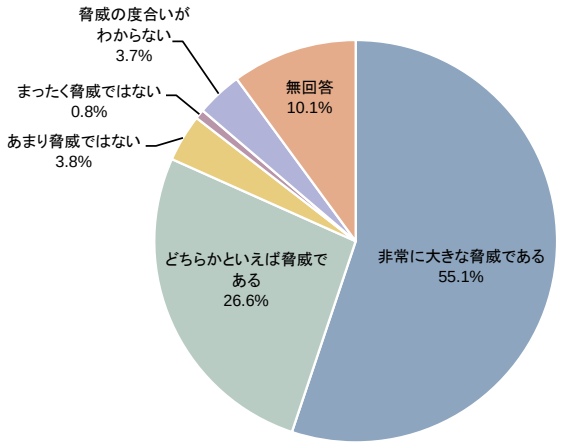
⑰情報セキュリティに関する脅威

1)コンピュータウイルス

「非常に大きな脅威である」の割合が最も高く55.1%となっている。次いで、「どちらかといえば脅威である（26.6%）」、「あまり脅威ではない（3.8%）」となっている。

図表 2-52 コンピュータウイルス（SA）

(n=4074)

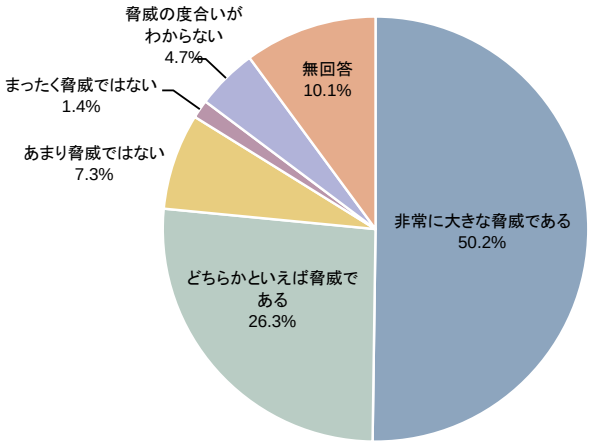


2)不正アクセス

「非常に大きな脅威である」の割合が最も高く50.2%となっている。次いで、「どちらかといえば脅威である（26.3%）」、「あまり脅威ではない（7.3%）」となっている。

図表 2-53 不正アクセス（SA）

(n=4074)

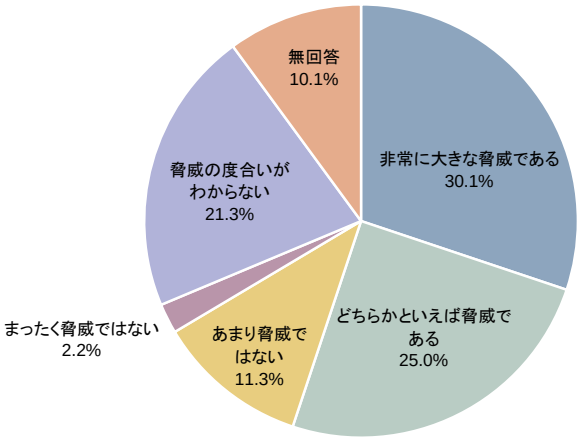


３)DoS攻撃・DDoS攻撃

「非常に大きな脅威である」の割合が最も高く30.1%となっている。次いで、「どちらかといえば脅威である（25.0%）」、「脅威の度合いがわからない（21.3%）」となっている。

図表　2-54　DoS攻撃･DDoS攻撃（SA）

(n=4074)

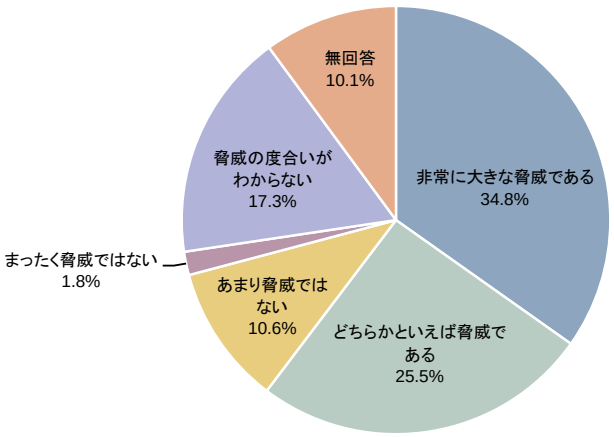


４)標的型攻撃

「非常に大きな脅威である」の割合が最も高く34.8%となっている。次いで、「どちらかといえば脅威である（25.5%）」、「脅威の度合いがわからない（17.3%）」となっている。

図表　2-55　標的型攻撃（SA）

(n=4074)

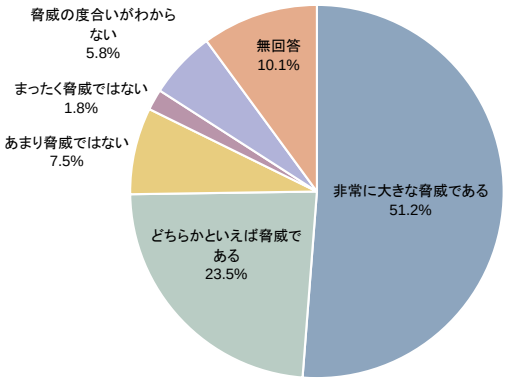


5)情報漏えい

「非常に大きな脅威である」の割合が最も高く51.2%となっている。次いで、「どちらかといえば脅威である（23.5%）」、「あまり脅威ではない（7.5%）」となっている。

図表　2-56　情報漏えい（SA）

(n=4074)

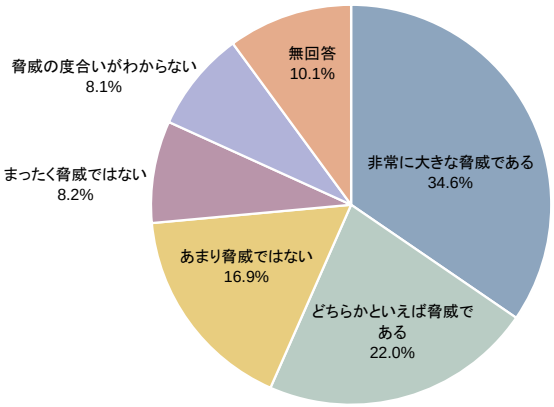


6)内部犯行（内部不正）

「非常に大きな脅威である」の割合が最も高く34.6%となっている。次いで、「どちらかといえば脅威である（22.0%）」、「あまり脅威ではない（16.9%）」となっている。

図表　2-57　内部犯行（内部不正）（SA）

(n=4074)

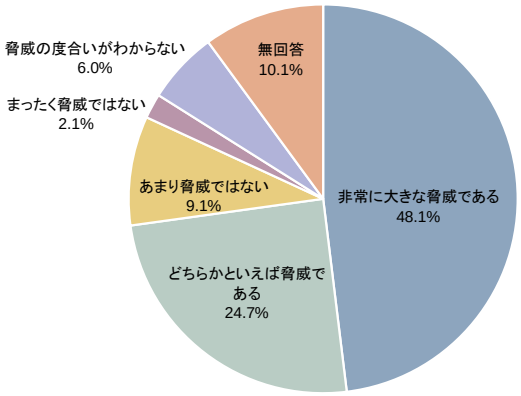


7)システム機能不全

「非常に大きな脅威である」の割合が最も高く48.1%となっている。次いで、「どちらかといえば脅威である（24.7%）」、「あまり脅威ではない（9.1%）」となっている。

図表 2-58 システム機能不全（SA）

(n=4074)

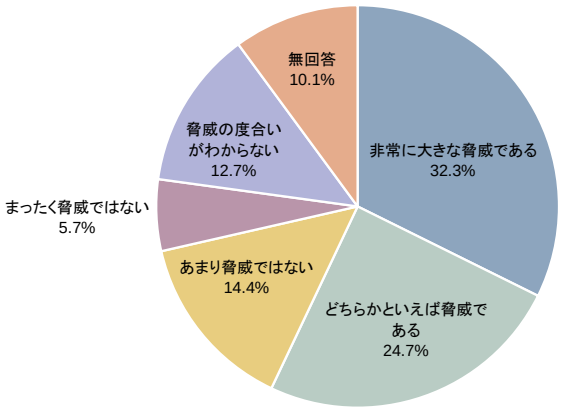


8)外部委託先のサービス停止

「非常に大きな脅威である」の割合が最も高く32.3%となっている。次いで、「どちらかといえば脅威である（24.7%）」、「あまり脅威ではない（14.4%）」となっている。

図表 2-59 外部委託先のサービス停止（SA）

(n=4074)

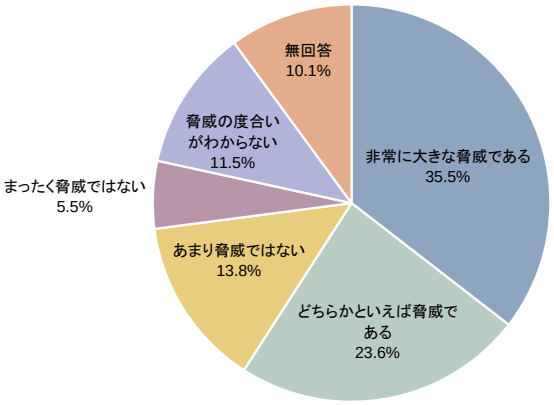


９)外部委託先からの情報漏えい

「非常に大きな脅威である」の割合が最も高く35.5%となっている。次いで、「どちらかといえば脅威である（23.6%）」、「あまり脅威ではない（13.8%）」となっている。

図表　2-60　外部委託先からの情報漏えい（SA）

(n=4074)



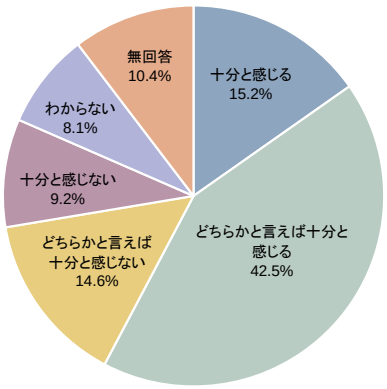
⑱脅威対策の満足度

１)コンピュータウイルス

「どちらかと言えば十分と感じる」の割合が最も高く42.5%となっている。次いで、「十分と感じる（15.2%）」、「どちらかと言えば十分と感じない（14.6%）」となっている。

図表　2-61　コンピュータウイルス（SA）

(n=4074)

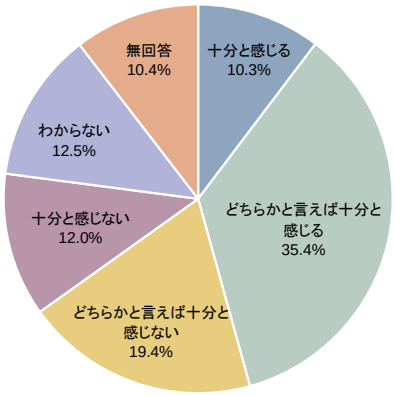


2)不正アクセス

「どちらかと言えば十分と感じる」の割合が最も高く35.4%となっている。次いで、「どちらかと言えば十分と感じない（19.4%）」、「わからない（12.5%）」となっている。

図表 2-62 不正アクセス（SA）

(n=4074)

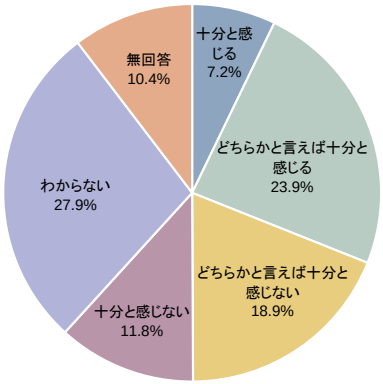


3)DoS攻撃・DDoS攻撃

「わからない」の割合が最も高く27.9%となっている。次いで、「どちらかと言えば十分と感じる（23.9%）」、「どちらかと言えば十分と感じない（18.9%）」となっている。

図表 2-63 DoS攻撃・DDoS攻撃（SA）

(n=4074)

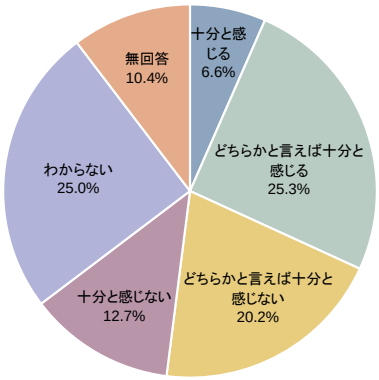


４)標的型攻撃

「どちらかと言えば十分と感じる」の割合が最も高く25.3%となっている。次いで、「わからない（25.0%）」、「どちらかと言えば十分と感じない（20.2%）」となっている。

図表　2-64　標的型攻撃（SA）

(n=4074)

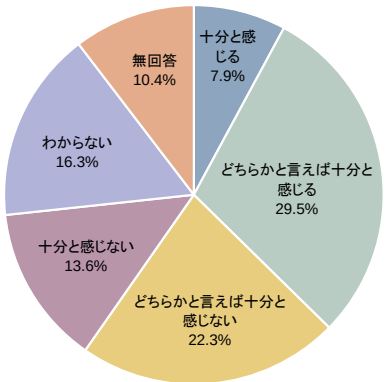


５)情報漏えい

「どちらかと言えば十分と感じる」の割合が最も高く29.5%となっている。次いで、「どちらかと言えば十分と感じない（22.3%）」、「わからない（16.3%）」となっている。

図表　2-65　情報漏えい（SA）

(n=4074)

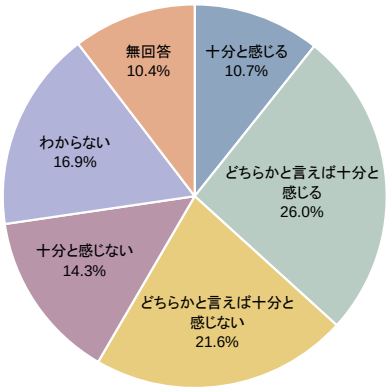


6)内部犯行（内部不正）

「どちらかと言えば十分と感じる」の割合が最も高く26.0%となっている。次いで、「どちらかと言えば十分と感じない（21.6%）」、「わからない（16.9%）」となっている。

図表 2-66 内部犯行（内部不正）（SA）

(n=4074)

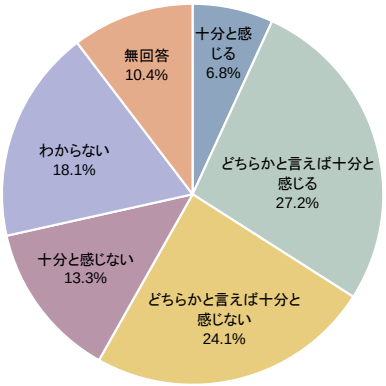


7)システム機能不全

「どちらかと言えば十分と感じる」の割合が最も高く27.2%となっている。次いで、「どちらかと言えば十分と感じない（24.1%）」、「わからない（18.1%）」となっている。

図表 2-67 システム機能不全（SA）

(n=4074)

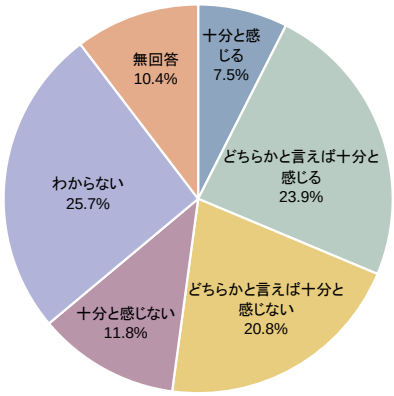


8)**外部委託先のサービス停止**

「わからない」の割合が最も高く25.7%となっている。次いで、「どちらかと言えば十分と感じる（23.9%）」、「どちらかと言えば十分と感じない（20.8%）」となっている。

図表　2-68　外部委託先のサービス停止（SA）

(n=4074)

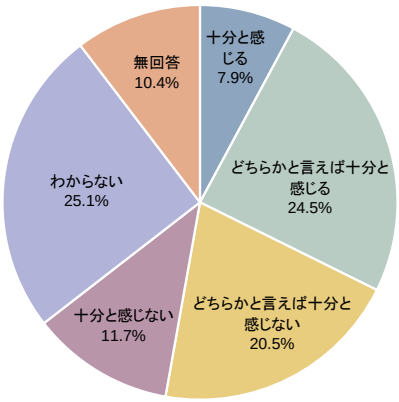


9)**外部委託先からの情報漏えい**

「わからない」の割合が最も高く25.1%となっている。次いで、「どちらかと言えば十分と感じる（24.5%）」、「どちらかと言えば十分と感じない（20.5%）」となっている。

図表　2-69　外部委託先からの情報漏えい（SA）

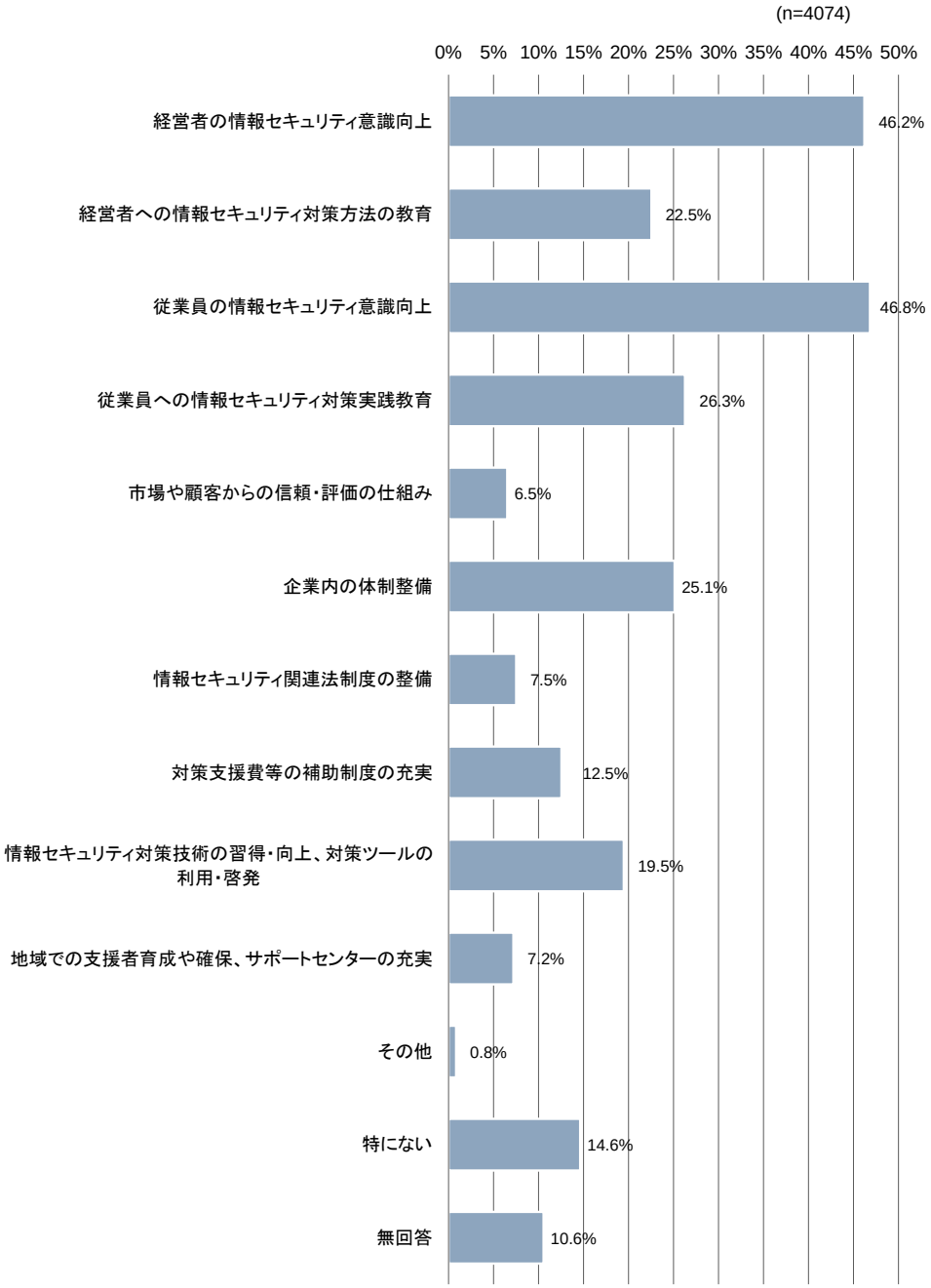
(n=4074)



⑲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

「従業員の情報セキュリティ意識向上」の割合が最も高く46.8%となっている。次いで、「経営者の情報セキュリティ意識向上（46.2%）」、「従業員への情報セキュリティ対策実践教育（26.3%）」となっている。

図表 2-70 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（MA）

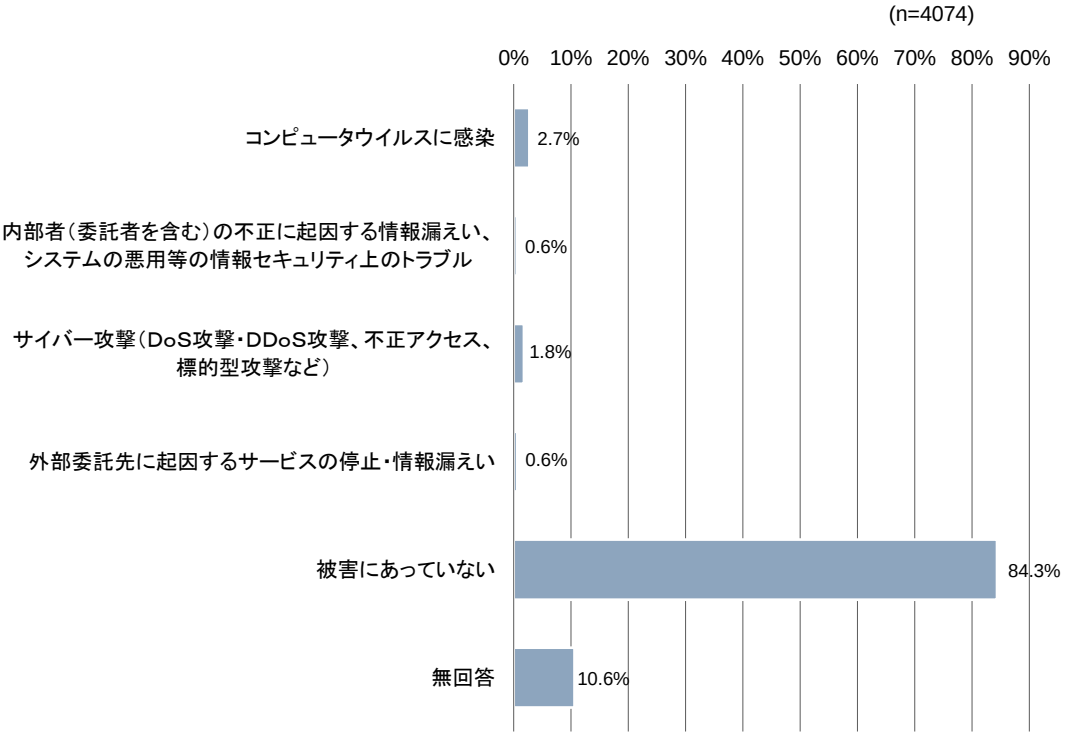


（４）情報セキュリティ被害の状況

①2020年度（2020年４月～2021年３月）における情報セキュリティ被害の有無

「被害にあっていない」の割合が最も高く84.3%となっている。次いで、「コンピュータウイルスに感染（2.7%）」、「サイバー攻撃（DoS攻撃・DDoS攻撃、不正アクセス、標的型攻撃など）（1.8%）」となっている。

図表 2-71 2020年度における情報セキュリティ被害の有無（MA）

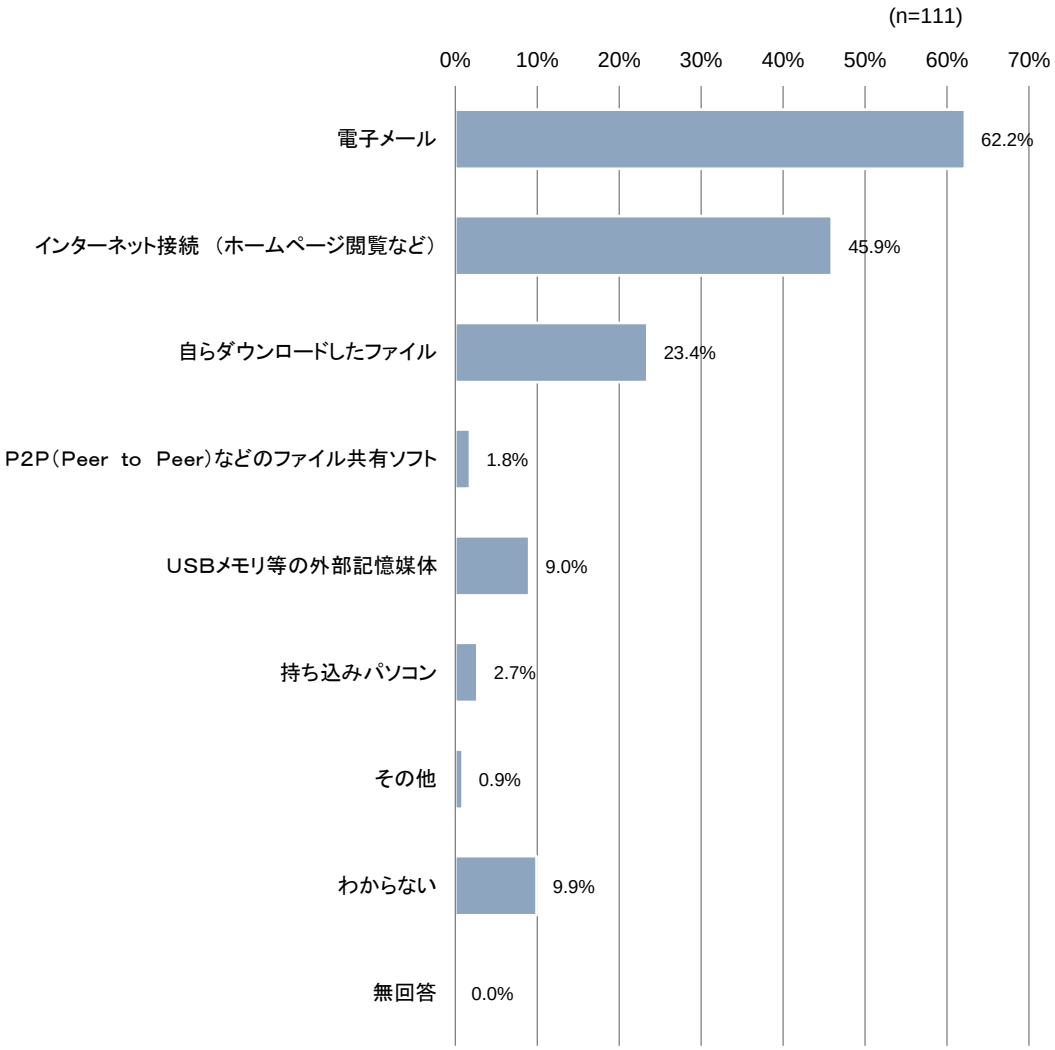


②コンピュータウイルスの被害状況

１)感染あるいは発見したコンピュータウイルスの想定される侵入経路

「電子メール」の割合が最も高く62.2%となっている。次いで、「インターネット接続　（ホームページ閲覧など）（45.9%）」、「自らダウンロードしたファイル（23.4%）」となっている。

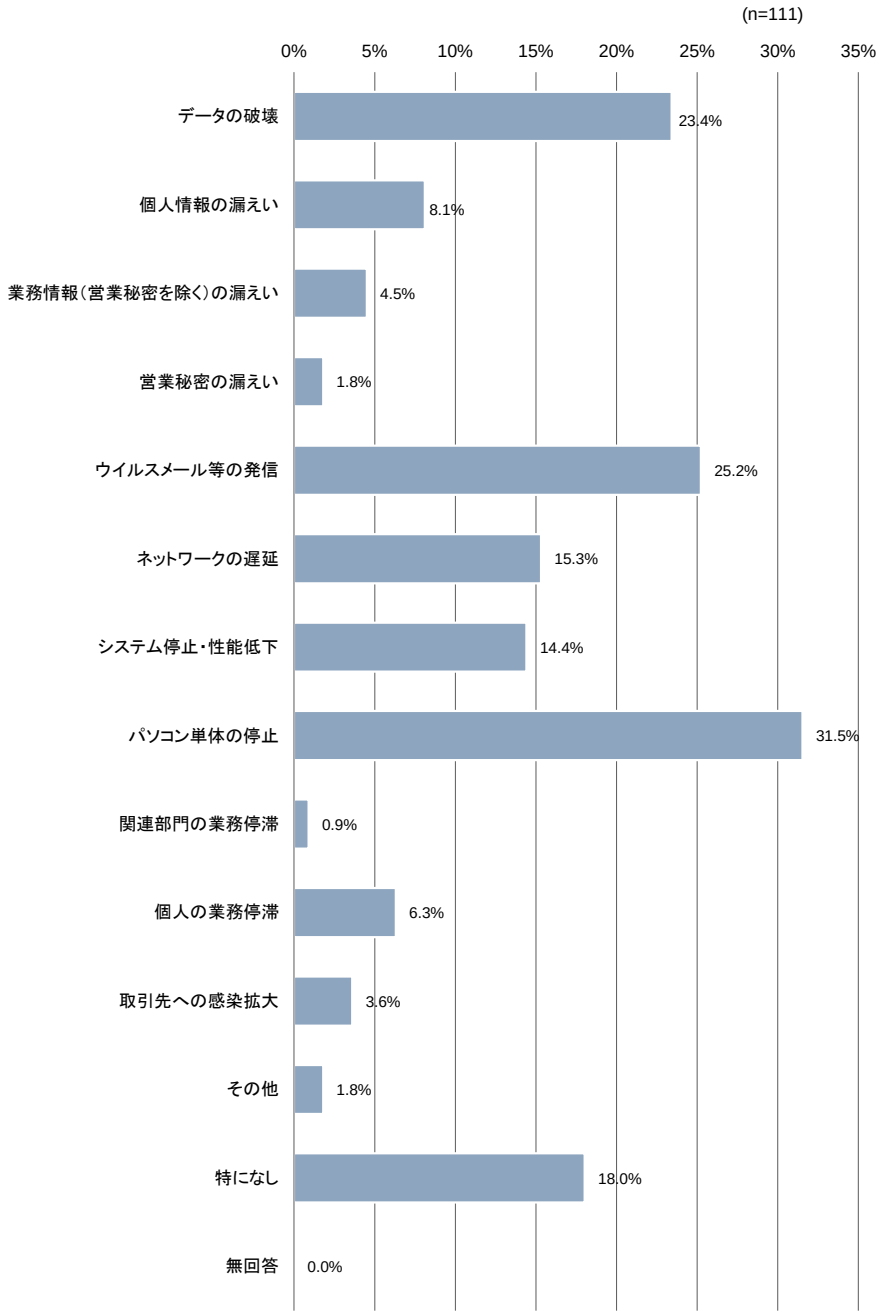
図表　2-72　感染あるいは発見したコンピュータウイルスの想定される侵入経路（MA）



2)コンピュータウイルスに感染した影響で生じた被害

「パソコン単体の停止」の割合が最も高く31.5%となっている。次いで、「ウイルスメール等の発信（25.2%）」、「データの破壊（23.4%）」となっている。

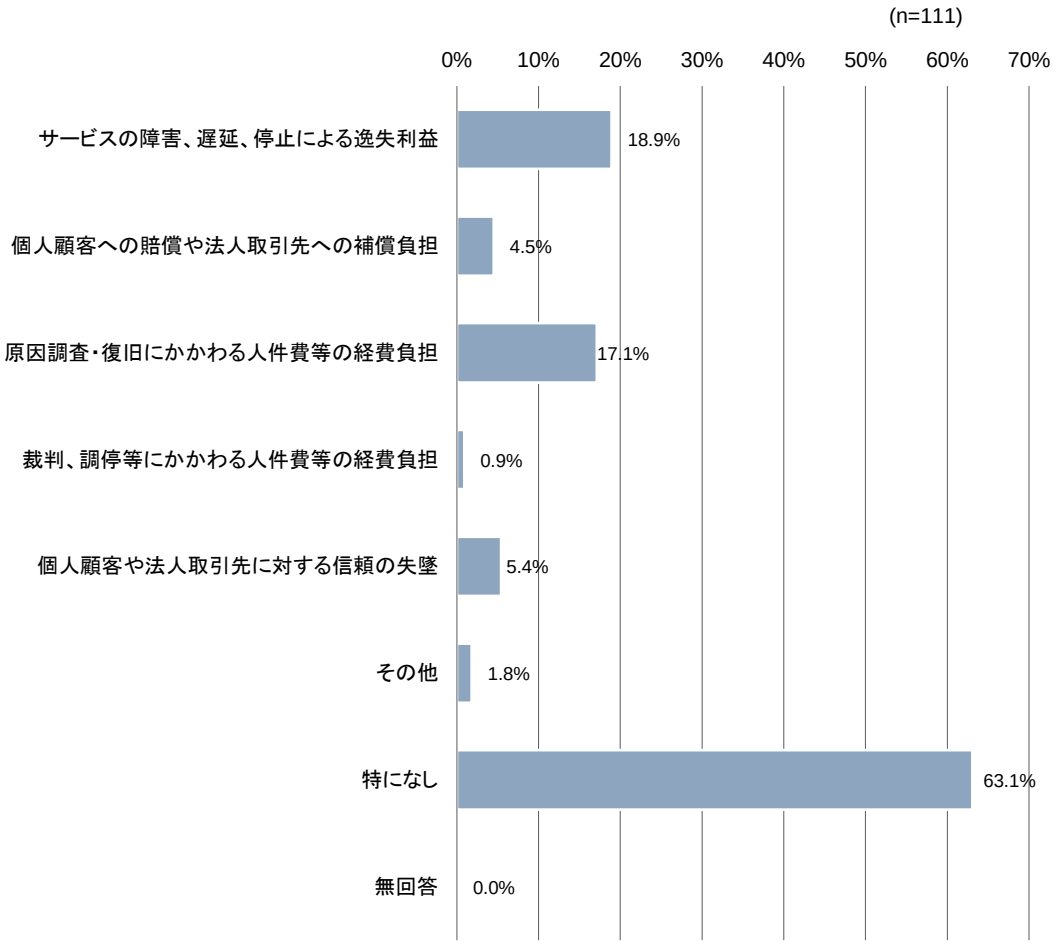
図表 2-73 コンピュータウイルスに感染した影響で生じた被害（MA）



3)コンピュータウイルスに感染した影響で、取引先に影響が及んだ内容

「特になし」の割合が最も高く63.1%となっている。次いで、「サービスの障害、遅延、停止による逸失利益（18.9%）」、「原因調査・復旧にかかわる人件費等の経費負担（17.1%）」となっている。

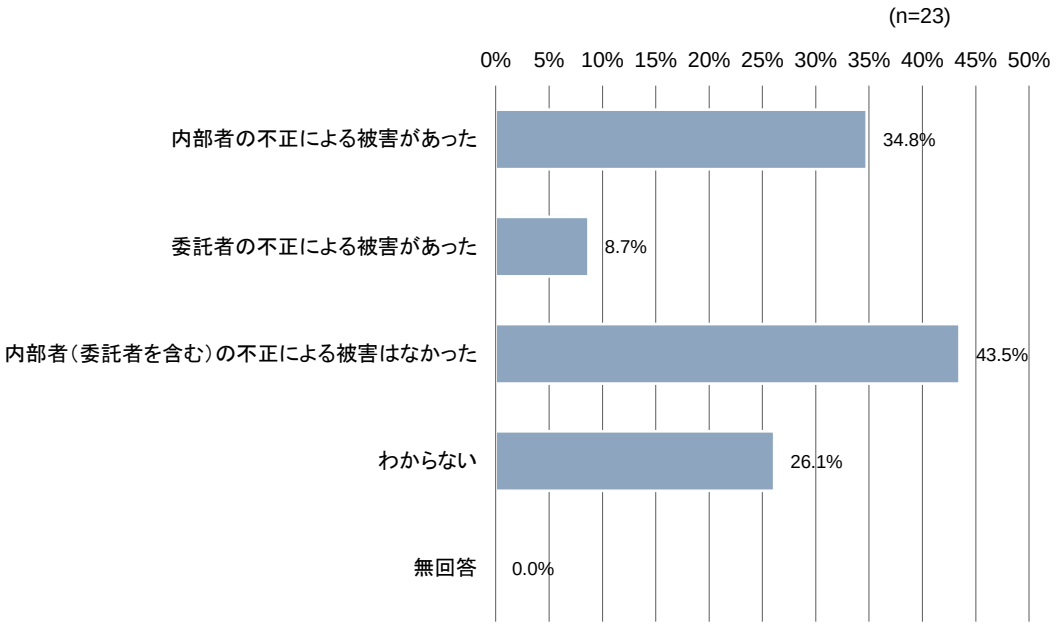
図表 2-74 コンピュータウイルスに感染した影響で、取引先に影響が及んだ内容（MA）



③内部者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の内容

「内部者（委託者を含む）の不正による被害はなかった」の割合が最も高く43.5%となっている。次いで、「内部者の不正による被害があった（34.8%）」、「わからない（26.1%）」となっている。

図表 2-75 内部者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の内容（MA）

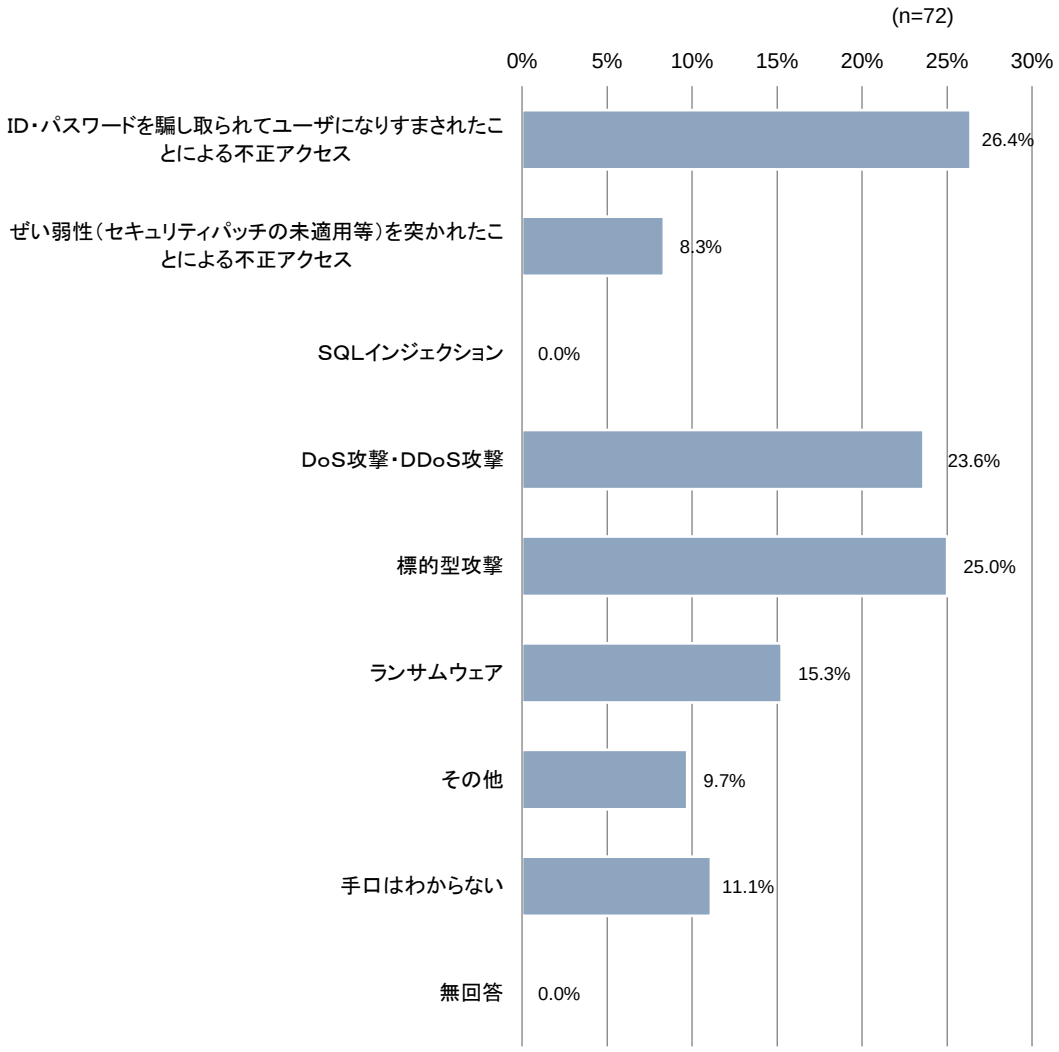


④サイバー攻撃の被害状況

１)サイバー攻撃の手口

「ID・パスワードを騙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」の割合が最も高く26.4%となっている。次いで、「標的型攻撃（25.0%）」、「DoS攻撃・DDoS攻撃（23.6%）」となっている。

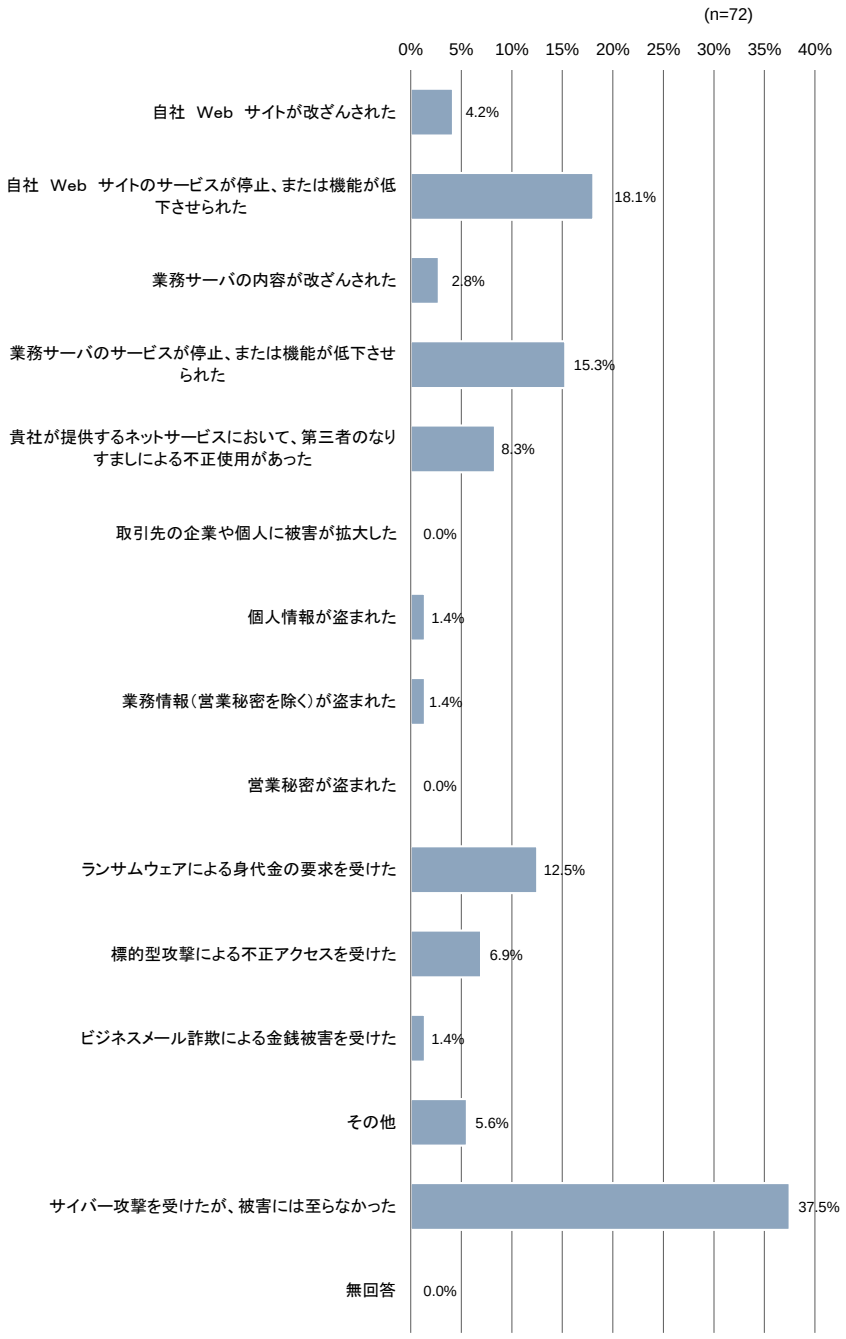
図表 2-76 サイバー攻撃の手口（MA）



２)サイバー攻撃の被害内容

「サイバー攻撃を受けたが、被害には至らなかった」の割合が最も高く、37.5%となっている。次いで、「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（18.1%）」、「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（15.3%）」となっている。

図表 2-77 サイバー攻撃の被害内容（MA）

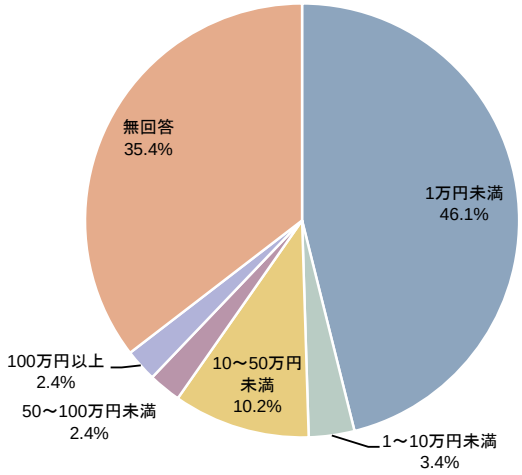


⑤情報セキュリティ被害で生じた被害額

「1万円未満」の割合が最も高く46.1%となっている。次いで、「10～50万円未満（10.2%）」、「1～10万円未満（3.4%）」となっている。

図表　2-78　情報セキュリティ被害で生じた被害額（SA）

(n=206)

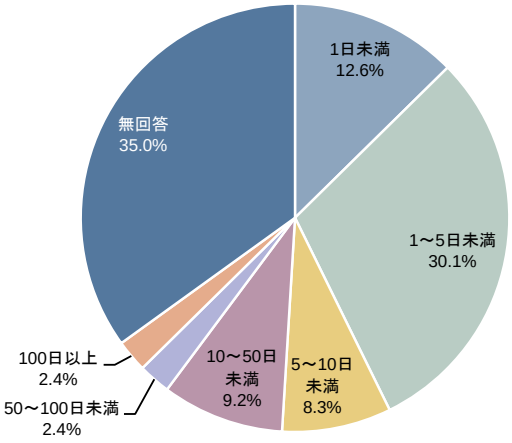


⑥情報セキュリティ被害から復旧に要した期間

「1～5日未満」の割合が最も高く30.1%となっている。次いで、「1日未満（12.6%）」、「10～50日未満（9.2%）」となっている。

図表　2-79　情報セキュリティ被害から復旧に要した期間（SA）

(n=206)



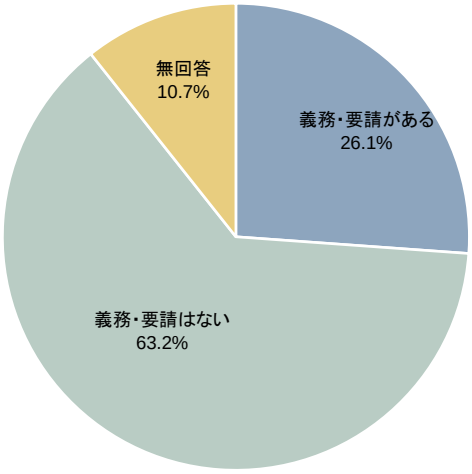
（５）取引先を含む情報セキュリティ対策

①販売先・仕入先との契約締結時における情報セキュリティに関する条項・取引上の義務・要請

「義務・要請はない」の割合が高く63.2%となっている。「義務・要請がある」の割合は26.1%となっている。

図表　2-80　販売先・仕入先との契約締結時における情報セキュリティに関する条項・取引上の義務・要請（SA）

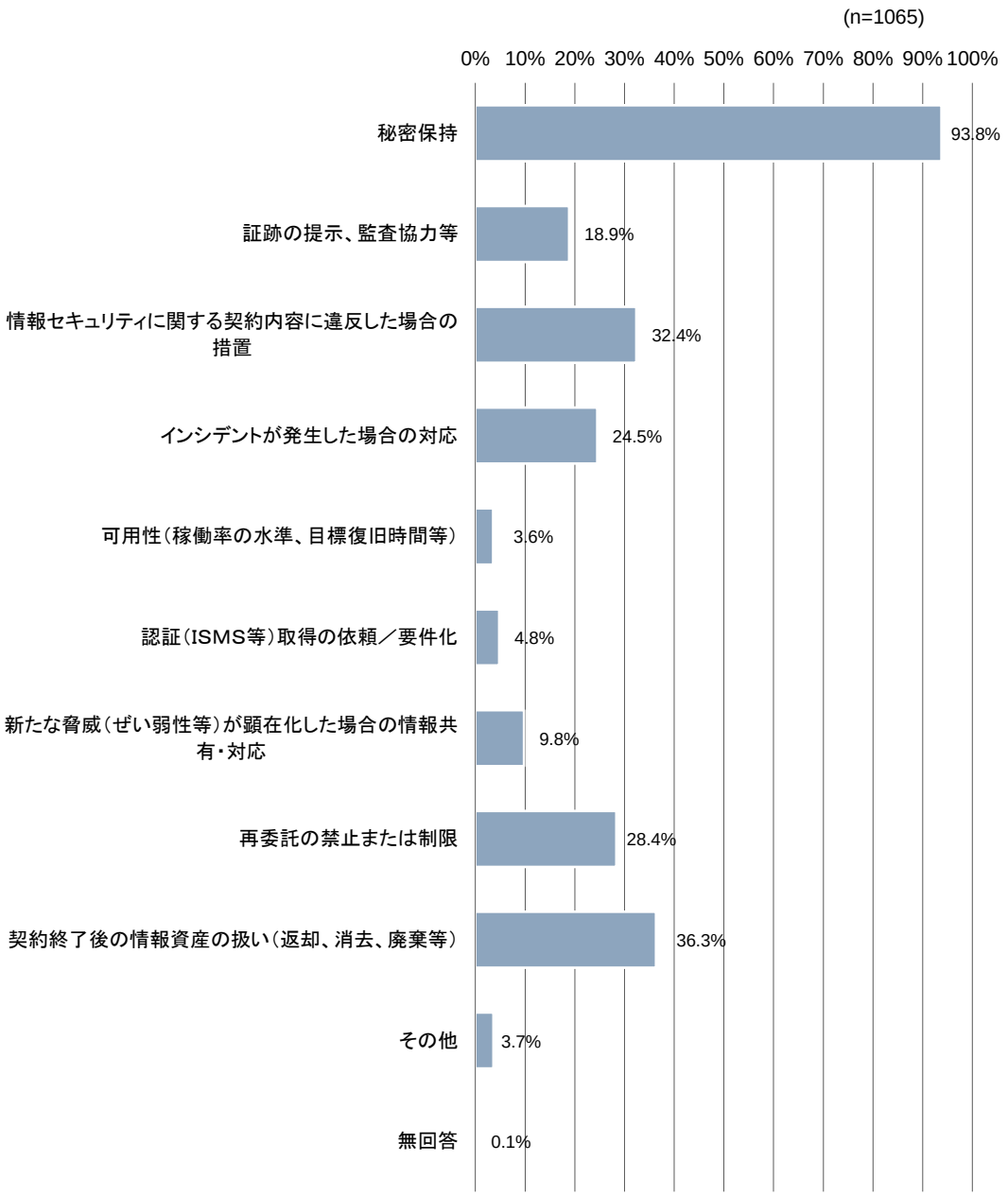
(n=4074)



②契約時における情報セキュリティに関する要請（販売先(発注元企業)との契約時）

「秘密保持」の割合が最も高く93.8%となっている。次いで、「契約終了後の情報資産の扱い（返却、消去、廃棄等）（36.3%）」、「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（32.4%）」となっている。

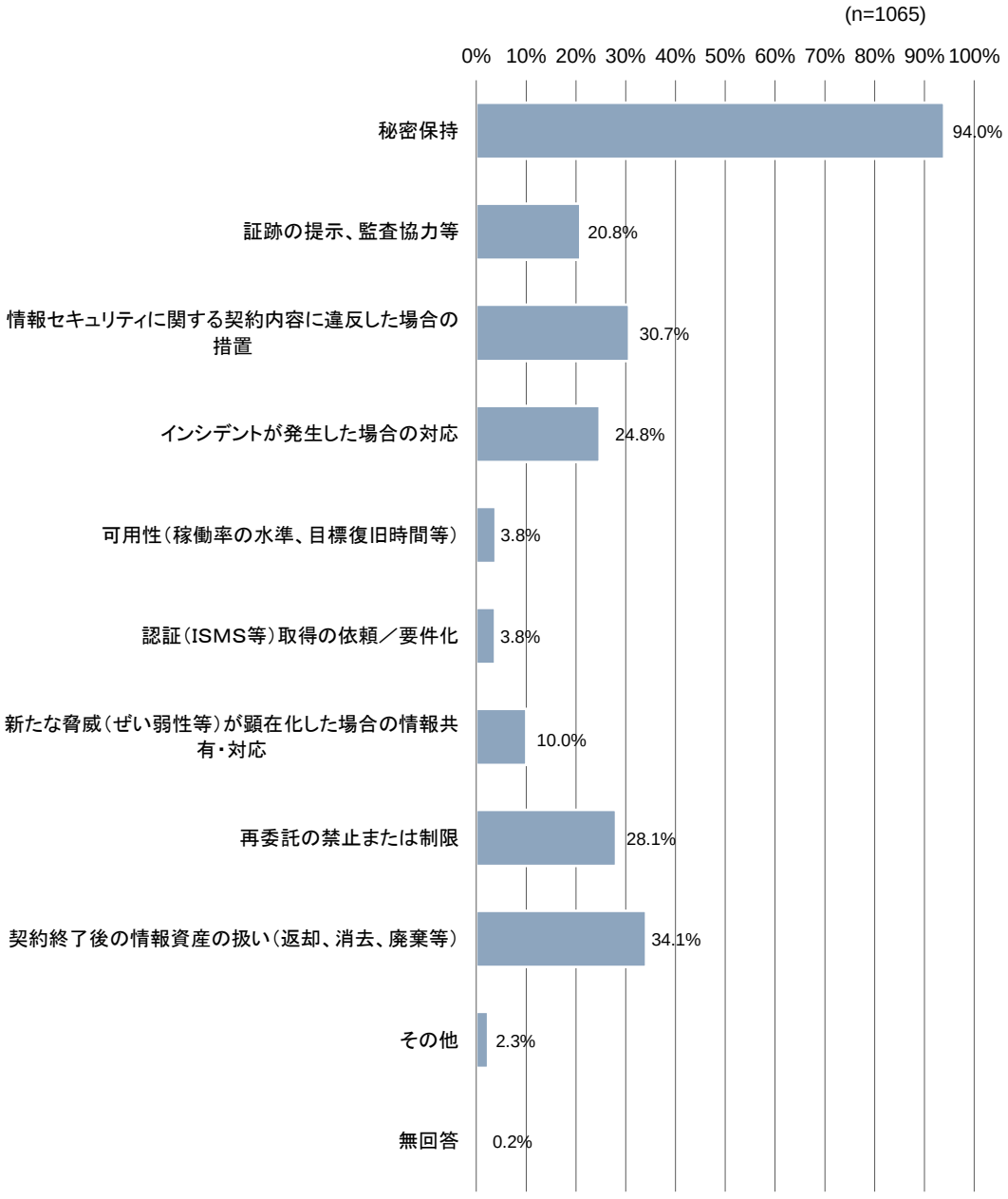
図表　2-81　契約時における情報セキュリティに関する要請（販売先（発注元企業）との契約時）　（MA）



③契約時における情報セキュリティに関する要請（仕入先(委託・協力企業)との契約時）

「秘密保持」の割合が最も高く94.0%となっている。次いで、「契約終了後の情報資産の扱い（返却、消去、廃棄等）（34.1%）」、「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（30.7%）」となっている。

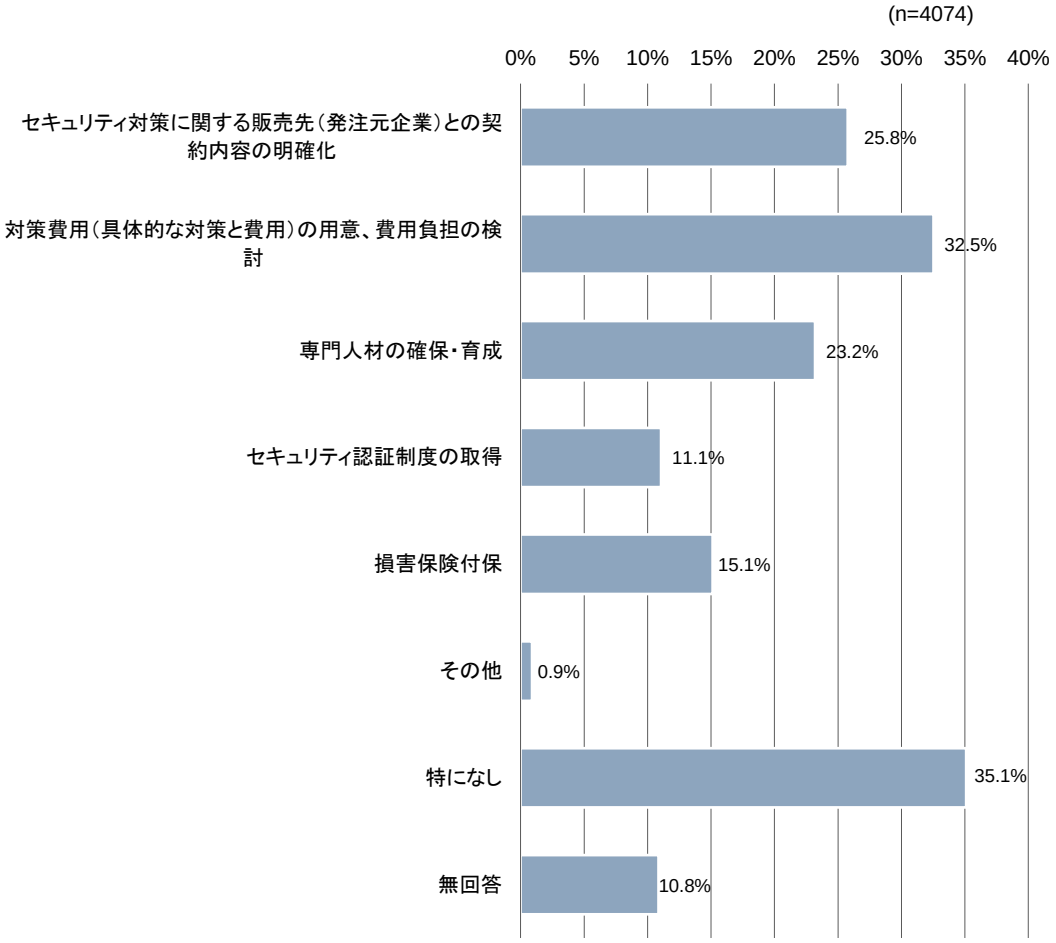
図表 2-82 契約時における情報セキュリティに関する要請
（仕入先(委託・協力企業)との契約）（MA）



④販売先から情報セキュリティ対策の要請を受けた場合、対策実施に向けての課題

「特になし」の割合が最も高く35.1%である。課題の中で最も高いのは、「対策費用（具体的な対策と費用）の用意、費用負担の検討」で32.5%であり、次いで「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（25.8%）」となっている。

図表 2-83 販売先から情報セキュリティ対策の要請を受けた場合、対策実施に向けての課題（MA）

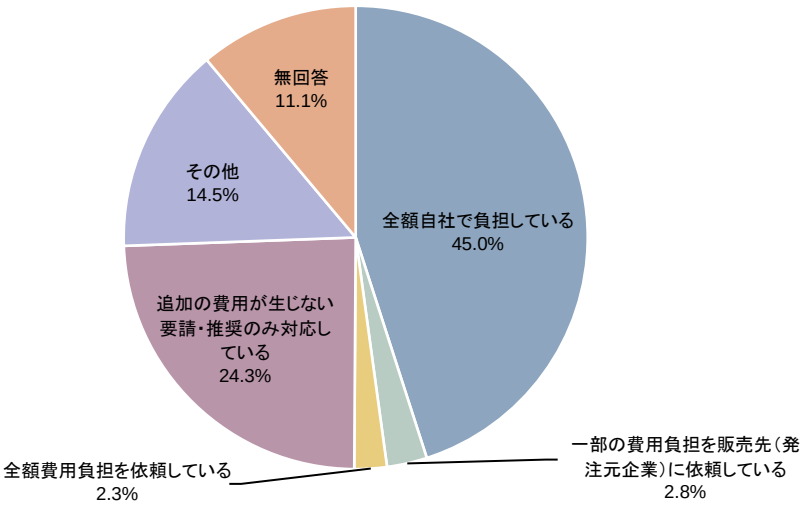


⑤販売先からの情報セキュリティに関する要請・推奨に対応するための費用負担

「全額自社で負担している」の割合が最も高く45.0%となっている。次いで、「追加の費用が生じない要請・推奨のみ対応している（24.3%）」、「その他（14.5%）」となっている。

図表 2-84 販売先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費用負担（SA）

(n=4074)

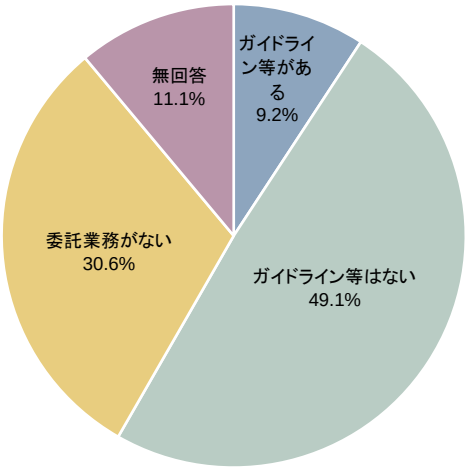


⑥仕入先への情報セキュリティ対策を行うためのガイドライン

「ガイドライン等はない」の割合が最も高く49.1%となっている。次いで、「委託業務がない（30.6%）」、「ガイドライン等がある（9.2%）」となっている。

図表　2-85　仕入先への情報セキュリティ対策を行うためのガイドライン（SA）

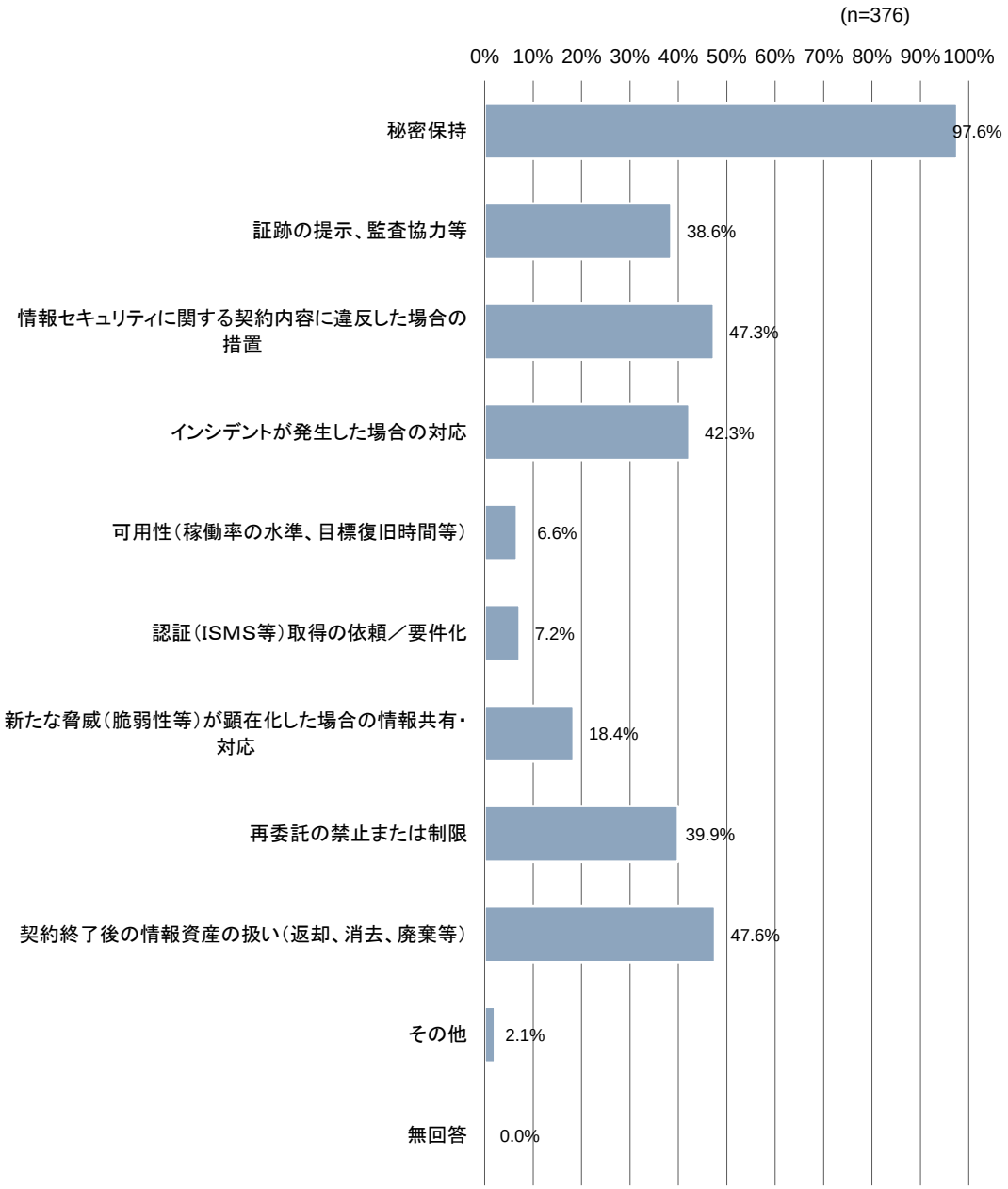
(n=4074)



⑦仕入先の情報セキュリティ対策等で規定していること

「秘密保持」の割合が最も高く97.6%となっている。次いで、「契約終了後の情報資産の扱い（返却、消去、廃棄等）（47.6%）」、「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（47.3%）」となっている。

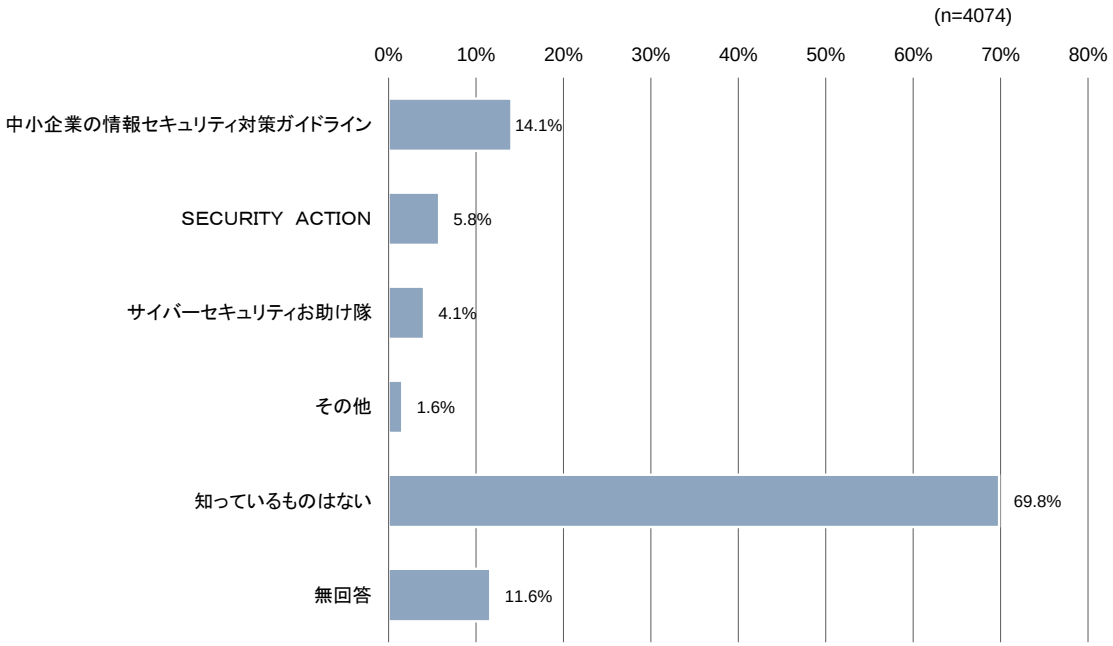
図表 2-86 仕入先の情報セキュリティ対策等で規定していること（MA）



（６）IPAが実施する活動の認知度

「知っているものはない」の割合が最も高く69.8%となっている。次いで、「中小企業の情報セキュリティ対策ガイドライン（14.1%）」、「SECURITY ACTION（5.8%）」となっている。

図表 2-87 IPAが実施する活動の認知度（MA）



４．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
- セキュリティ体制
- 取引上の立場

企業規模については、図表 2-88に示すように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。

図表 2-88 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	2,377
	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	1,484
	製造業その他	21～100名	
中小企業（101名以上）	全業種	101名以上	178

取引上の立場については、取引先や顧客から、情報セキュリティに関する要請が近年増加していることから、実態を把握するために調査を行ったものである。図表 2-89に委託元から三次請けまでの４段階のいずれに当てはまるかの回答を基に、クロス集計を試みた。

図表 2-89 取引上の立場の区分

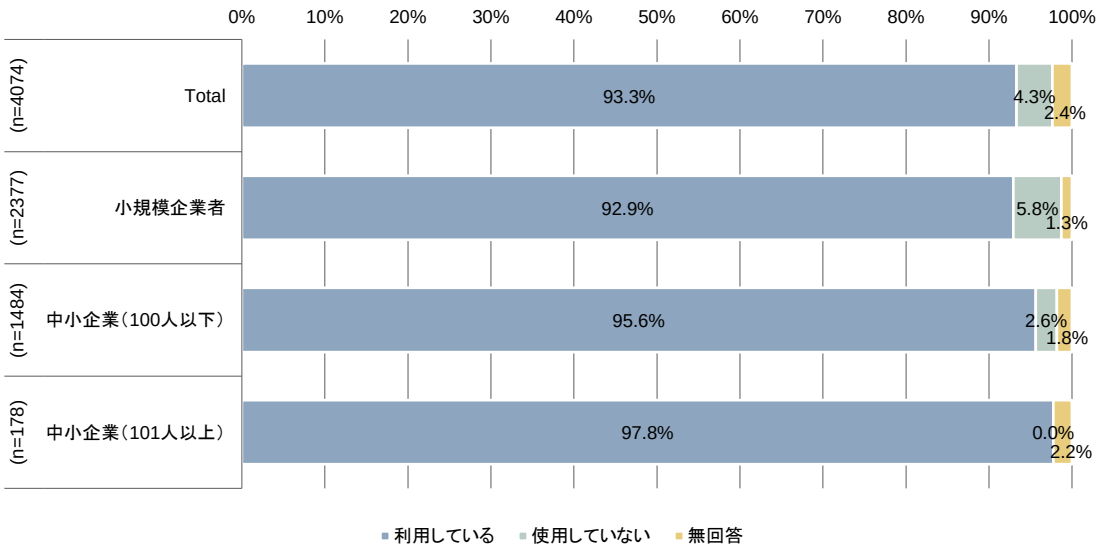
（例）	委託元→	下請事業者 A→（元請・一次）	下請事業者 B→（二次）	下請事業者 C（三次）

（１）企業規模によるクロス集計結果

①業務用パソコン・タブレット端末・スマートフォンの利用状況

企業規模での差はほとんどない結果である。

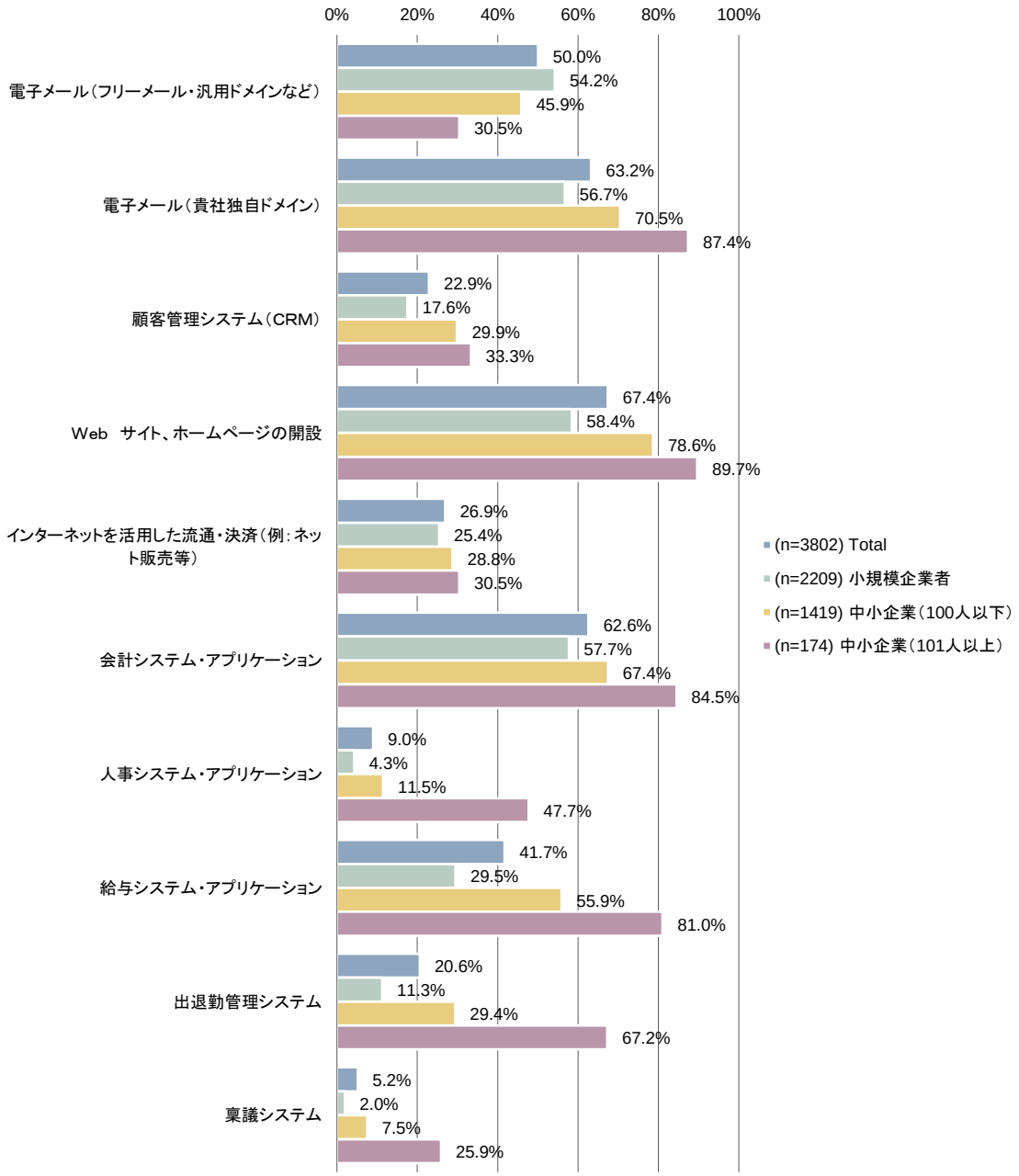
図表　2-90　業務用パソコン･タブレット端末･スマートフォンの利用状況（企業規模別）（SA）



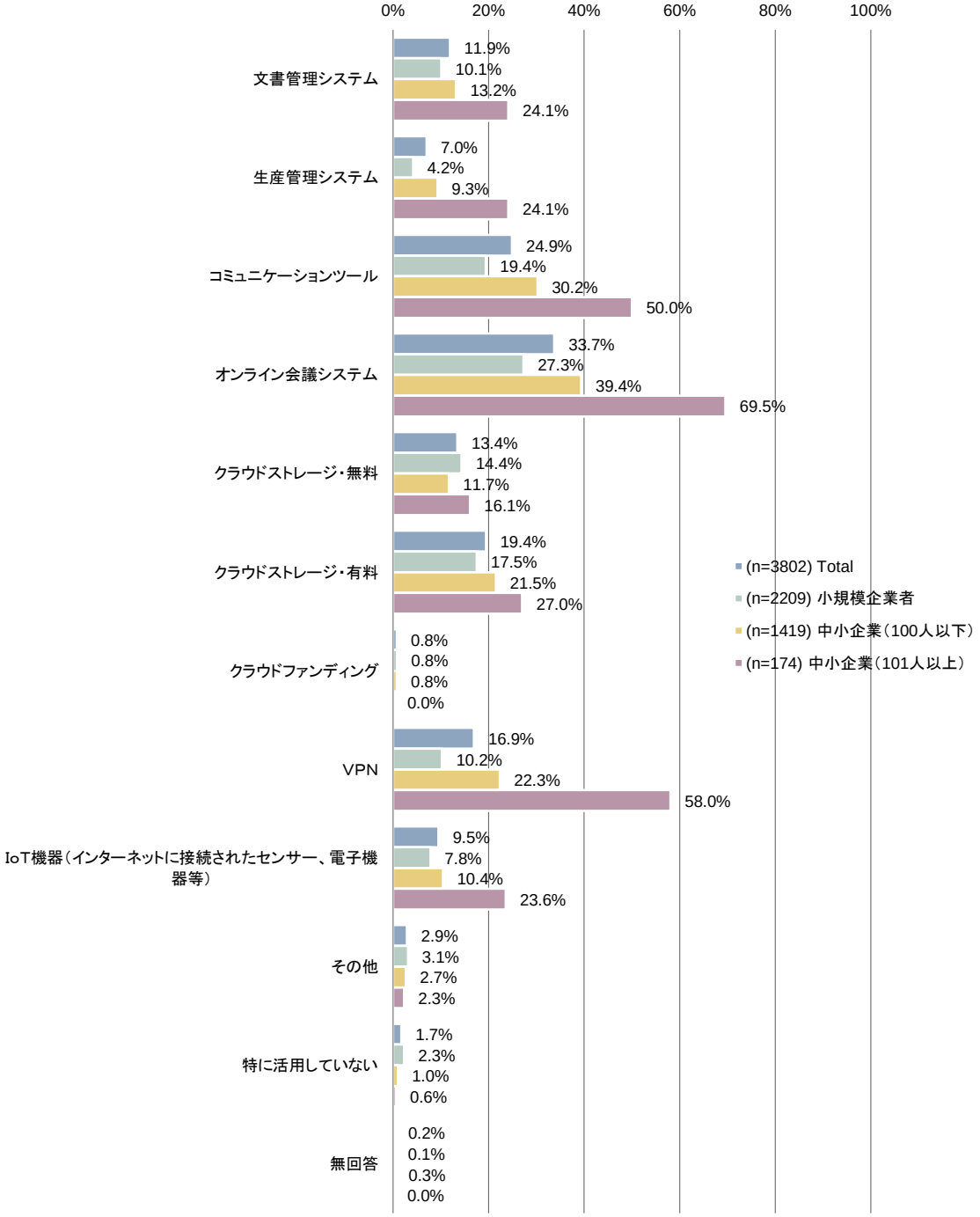
②利用・導入しているサービスやシステム

規模の大きい中小企業（101人以上）の利用率が高い傾向がある。コロナ禍におけるテレワーク・在宅勤務等の増加にも関連性が高いと考えられる、出退勤管理システム、コミュニケーションツール、オンライン会議システム、VPN等についても、規模による利用率に違いが見られる。

図表　2-91　利用・導入しているサービスやシステム①（企業規模別）（MA）



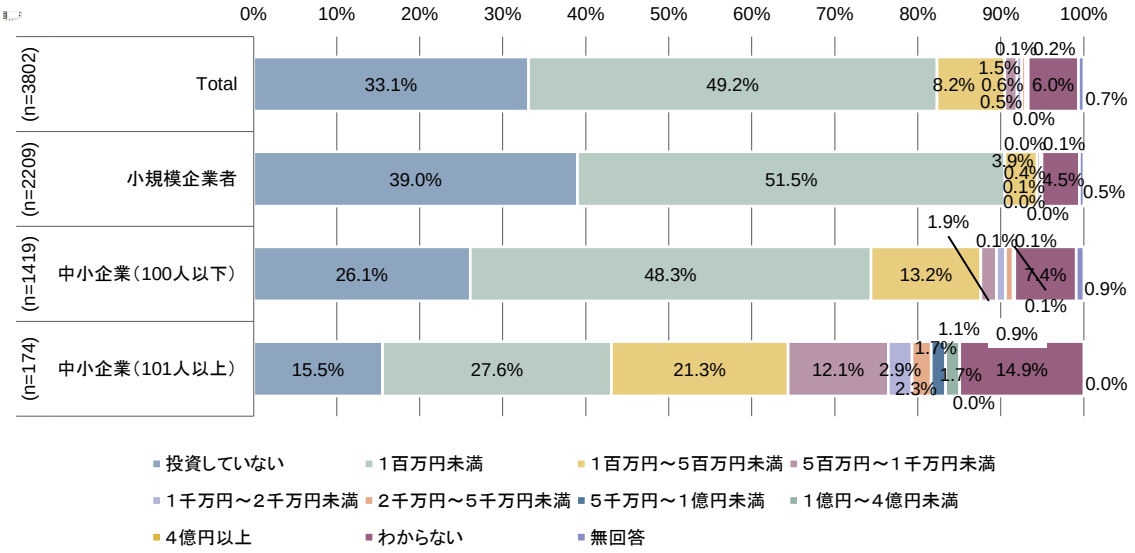
図表　2-92　利用・導入しているサービスやシステム②（企業規模別）（MA）



③直近過去３期の情報セキュリティ対策投資額

企業規模に応じて投資額が大きくなる傾向がみられる。また、小規模企業者の約40%、中小企業（100人以下）の約26%、中小企業（101人以上）の約16%は投資をしていないと回答している。

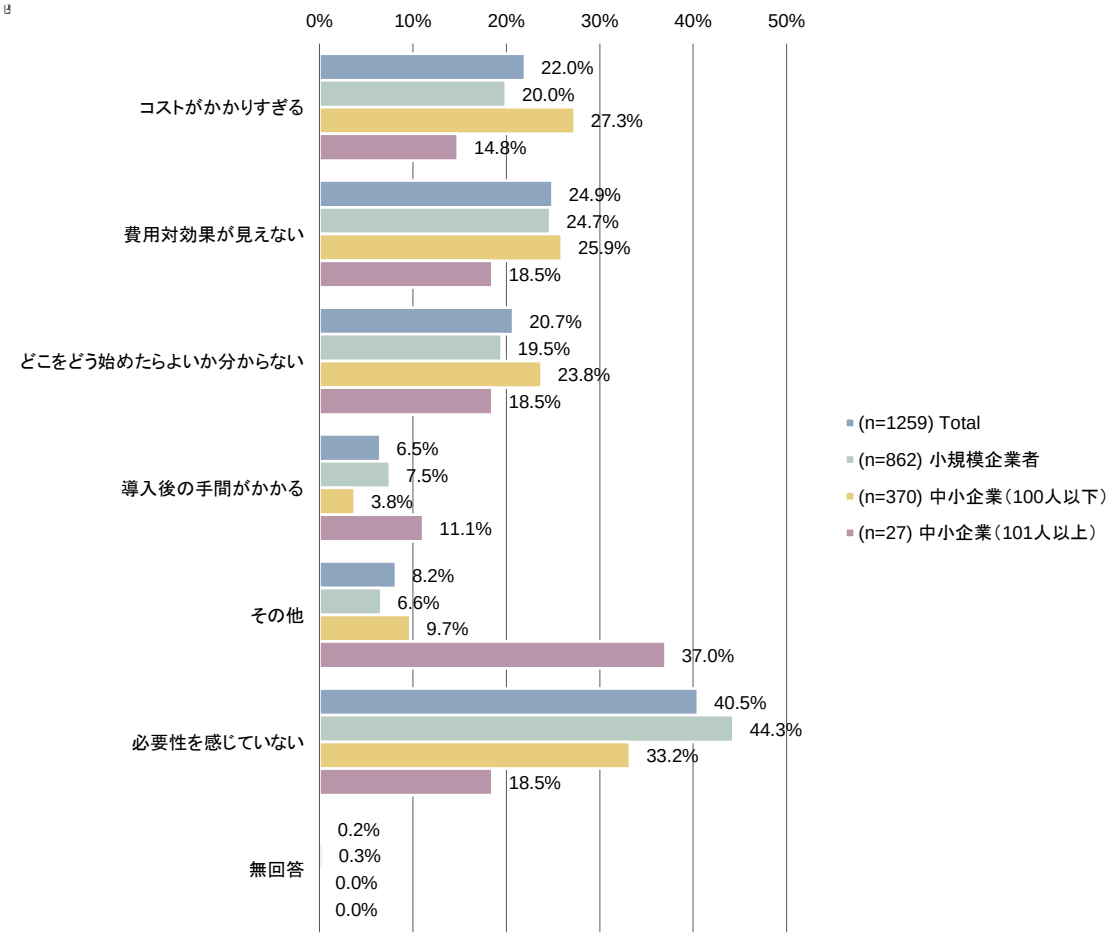
図表　2-93　直近過去３期の情報セキュリティ対策投資額（企業規模別）（SA）



④情報セキュリティ対策投資を行わなかった理由

企業規模に関わらず、「必要を感じていない」という回答が最も多く、特に小規模企業者や中小企業（100人以下）において回答の割合が高い。コストや費用対効果、どう始めたらよいか分からないという回答については企業規模間での差はやや小さい。

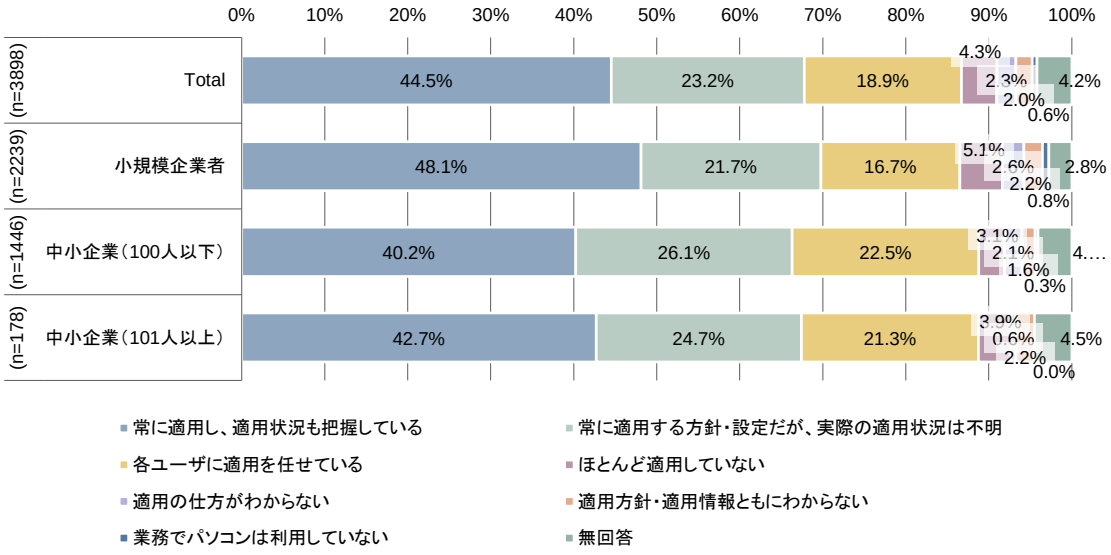
図表　2-94　情報セキュリティ対策投資を行わなかった理由（企業規模別）（MA）



⑤パソコンへのWindows Updateなどによるセキュリティパッチの適用状況

企業規模による回答傾向の差はあまりない。「常に適用し、適用状況も把握している」という回答に限定すると、最も割合が高いのは小規模企業者で48.1%となっている。

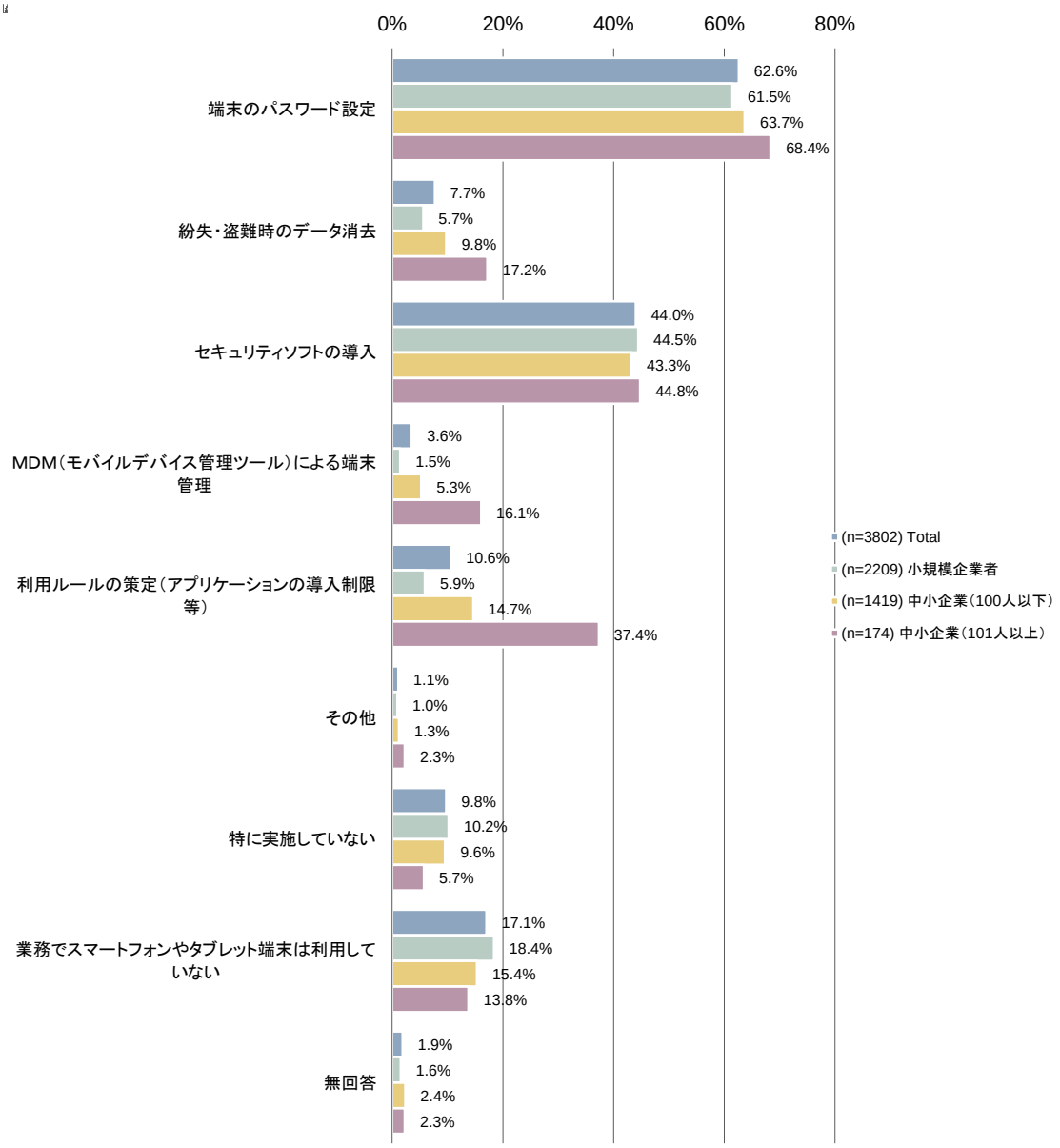
図表 2-95 パソコンへのWindows Updateなどによるセキュリティパッチの適用状況（企業規模別）（SA）



⑥スマートフォンやタブレット端末に対して実施している対策

企業規模による回答傾向の差はあまり見られない。利用ルールの策定やMDM（モバイルデバイス管理ツール）による端末管理の実施については、中小企業（101人以上）の割合が高い。

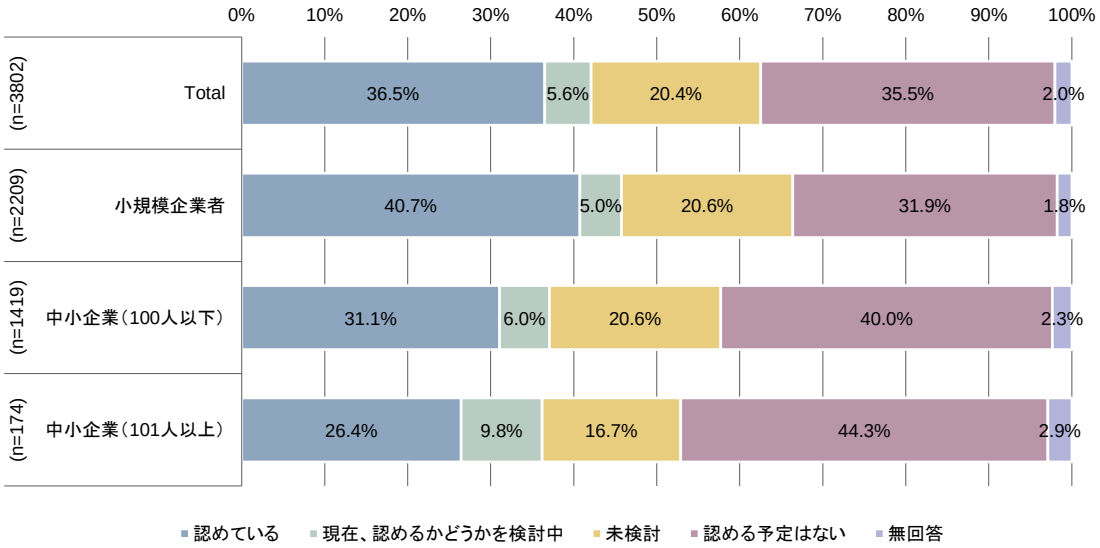
図表 2-96 スマートフォンやタブレット端末に対して実施している対策（企業規模別）（MA）



⑦社員の私有端末の業務利用（BYOD：Bring Your Own Device）

小規模企業者の方が「認めている」という割合が高く、40.7%となっている。一方、中小企業（101人以上）では、26.4%となっている。

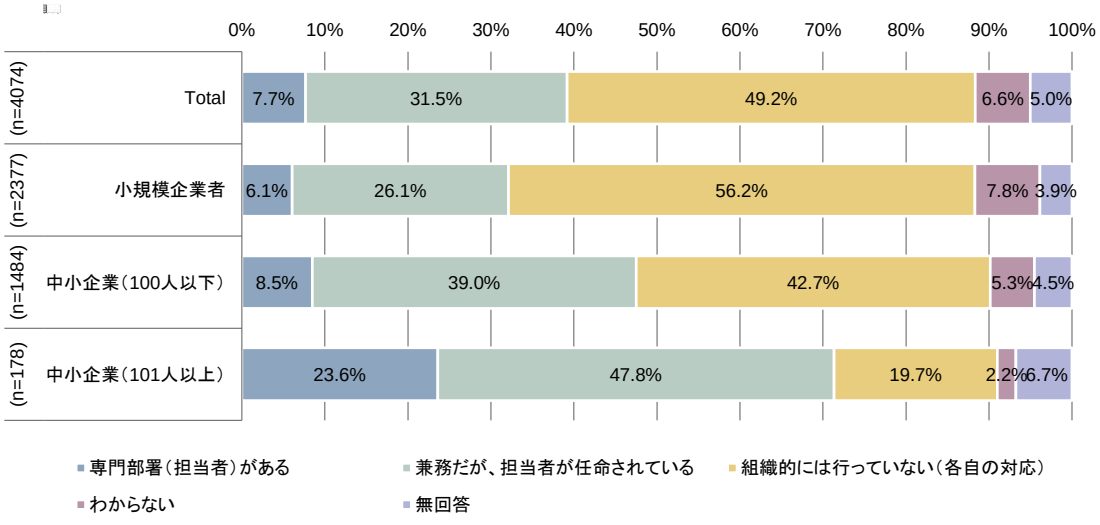
図表　2-97　社員の私有端末の業務利用（企業規模別）（SA）



⑧組織体制

「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」の回答はいずれも企業規模が大きいほど割合が高く、回答の合計は小規模企業者では32.2%、中小企業（100人以下）では47.5%、中小企業（101人以上）では71.4%となっている。

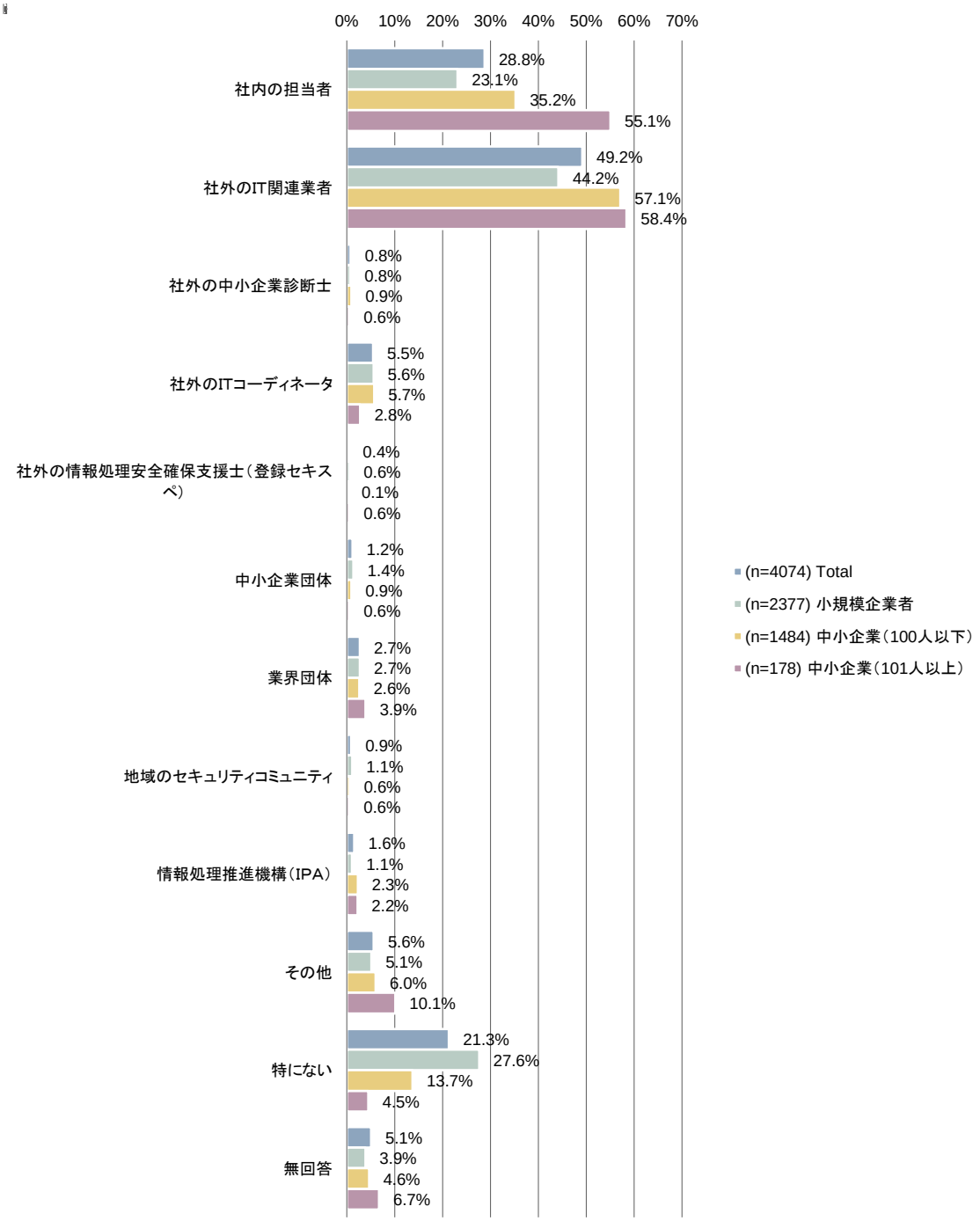
図表　2-98　組織体制（企業規模別）（SA）



⑨困ったことがあった際の相談先

「社内の担当者」や「社外のIT関連事業者」の回答が多いものの、いずれも小規模企業者の回答が少ない。逆に「特にない」という回答は小規模企業者が最も多く、27.6%となっている。

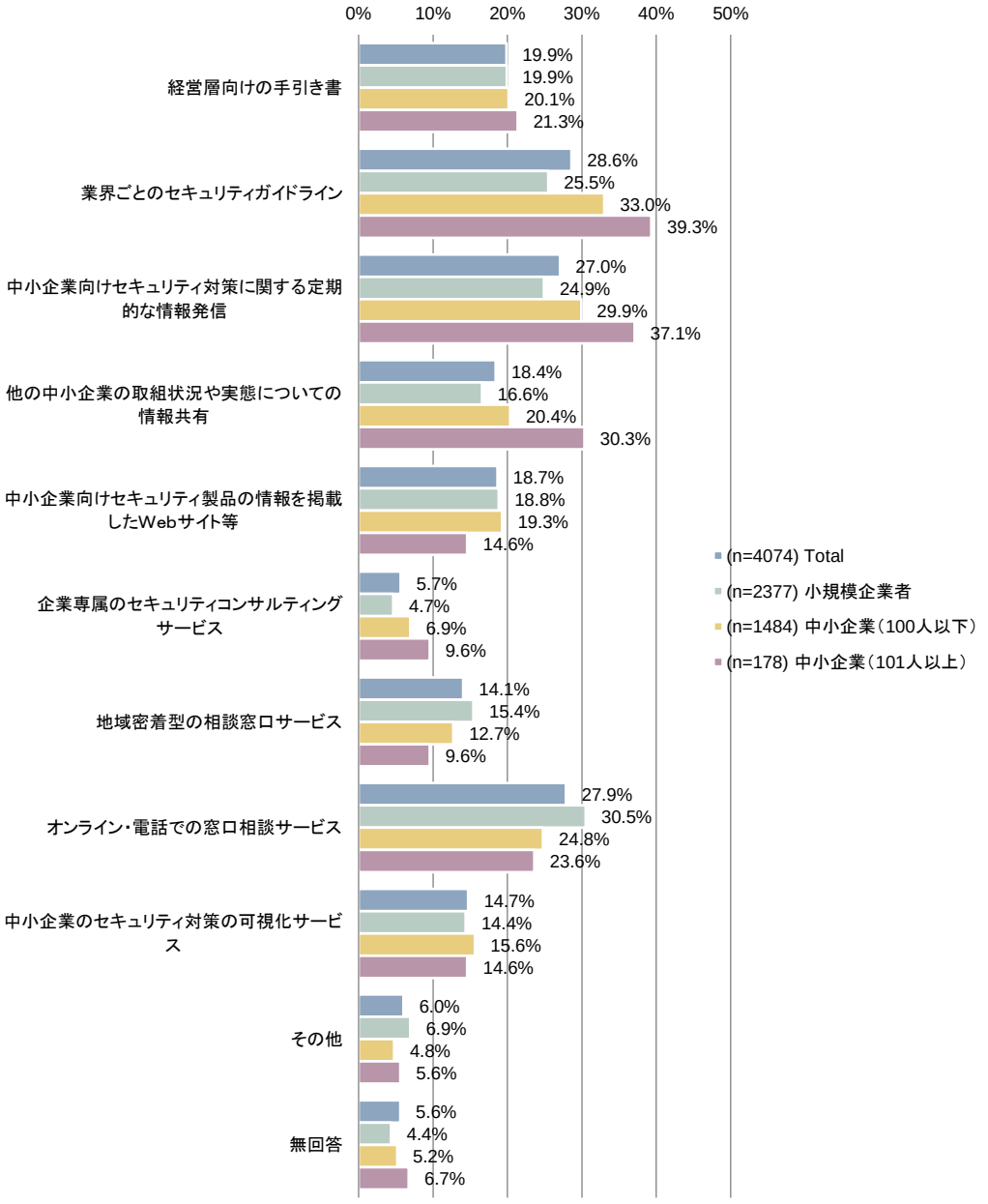
図表 2-99 困ったことがあった際の相談先（企業規模別）（MA）



⑩活用したい情報セキュリティ対策に関するサービス

企業規模別に回答が多かったサービスをみると、小規模企業者については「オンライン・電話での窓口相談サービス」が30.5%となっているのに対し、中小企業（100人以下）や中小企業（101人以上）は「業界ごとのセキュリティガイドライン」がそれぞれ33.0%、39.3%、次いで「中小企業向けセキュリティ対策に関する定期的な情報発信」が29.9%、37.1%となっており、求めているサービスが異なっている。

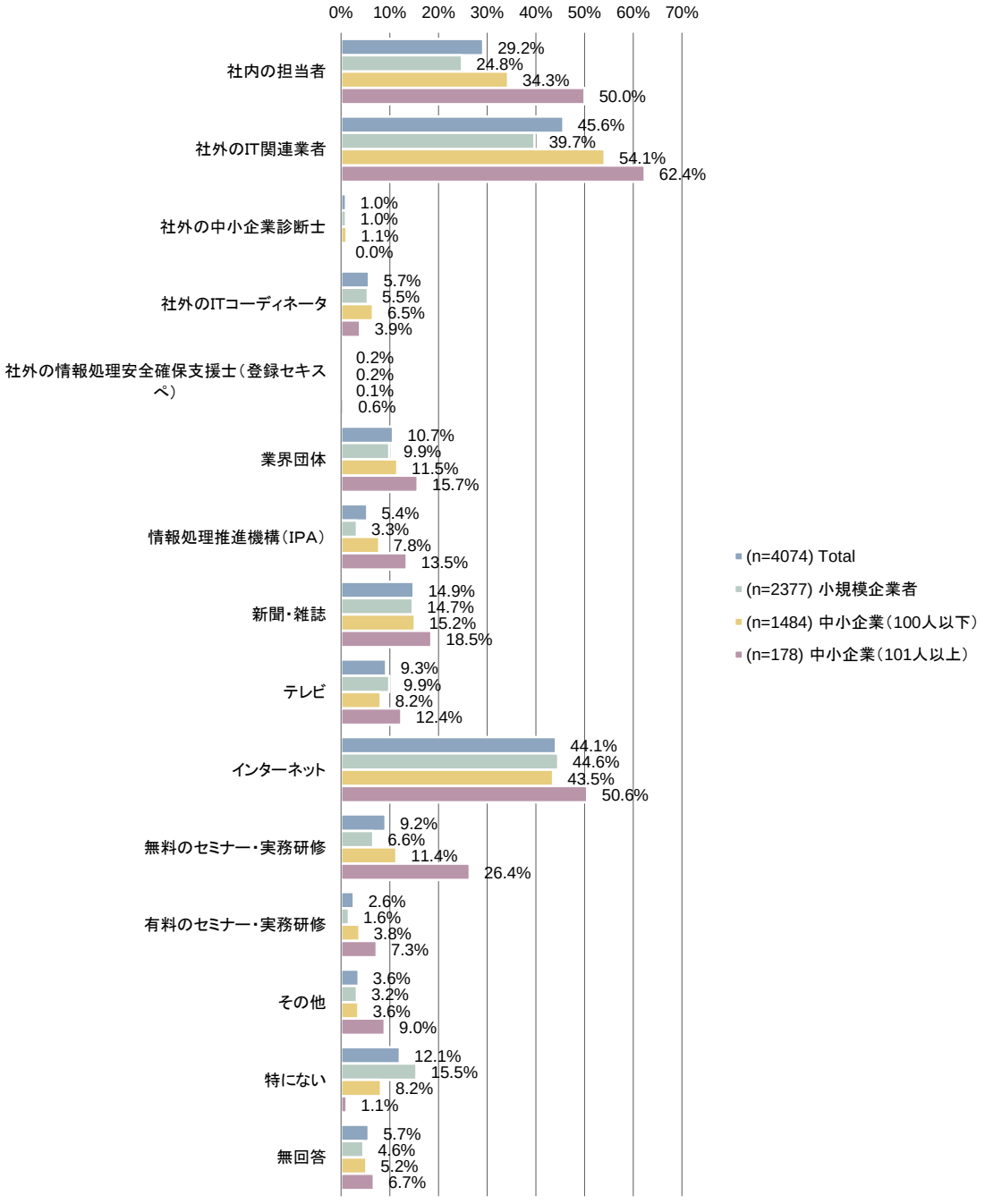
図表　2-100　活用したい情報セキュリティ対策に関するサービス（企業規模別）（MA）



⑪情報セキュリティに関する情報収集先

大半の選択肢において、中小企業（101人以上）の割合が最も高い結果となっており、相対的に規模の大きい中小企業の方が複数の情報収集先から情報を収集している傾向がある。

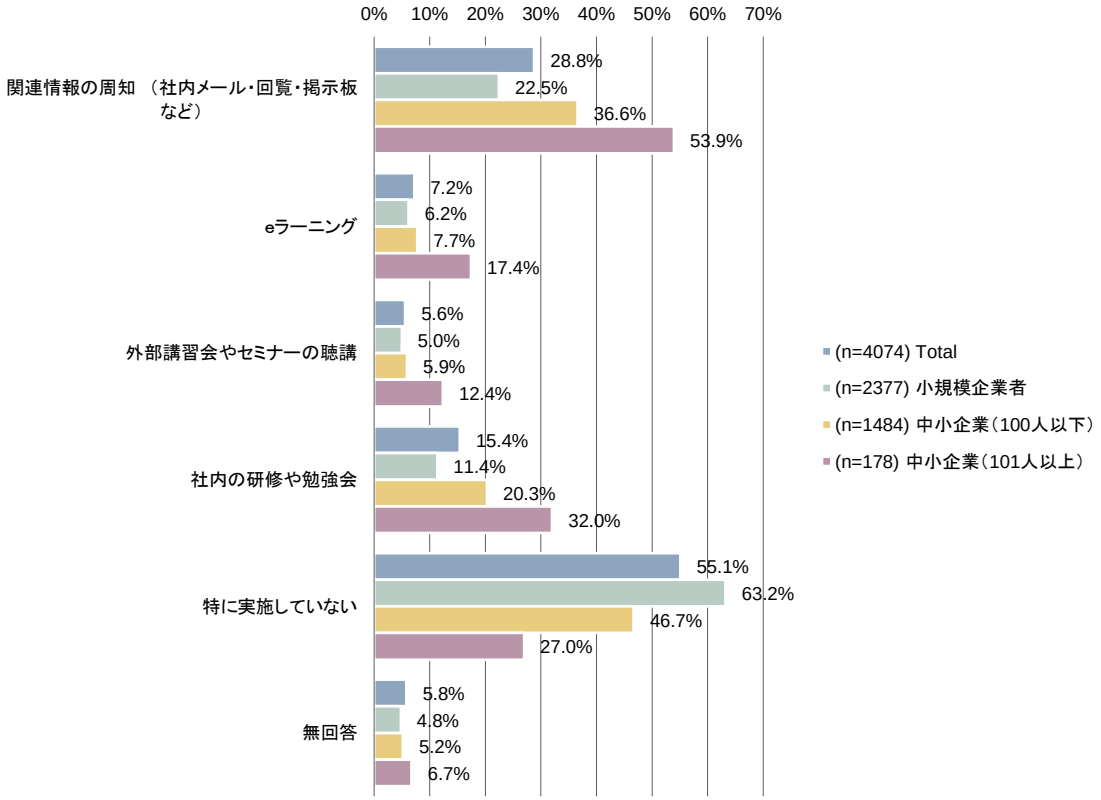
図表　2-101　情報セキュリティに関する情報収集先（企業規模別）（MA）



⑫従業員に対する情報セキュリティ教育の実施状況

従業員への情報セキュリティ教育については、すべての教育内容に関して中小企業（101人以上）が最も実施している。「特に実施していない」の割合については、小規模企業者が63.2%、中小企業（100人以下）は46.7%、中小企業（101 人以上）は27.0%となっている。

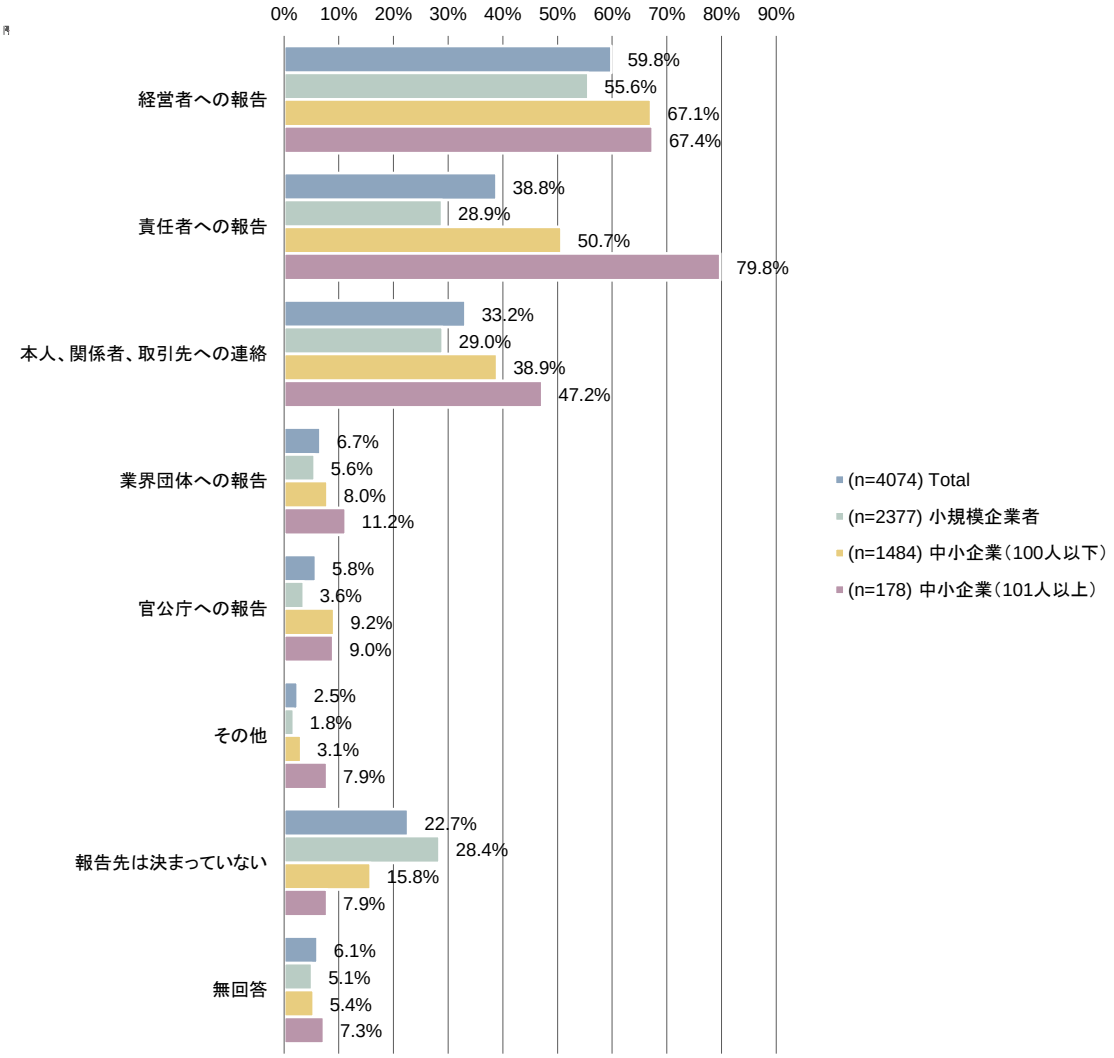
図表 2-102 従業員に対する情報セキュリティ教育の実施状況（企業規模別）（MA）



⑬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

「経営者への報告」については企業規模によらず規定されている。「責任者への報告」については、中小企業（101人以上）で特に高く、79.8%となっている。

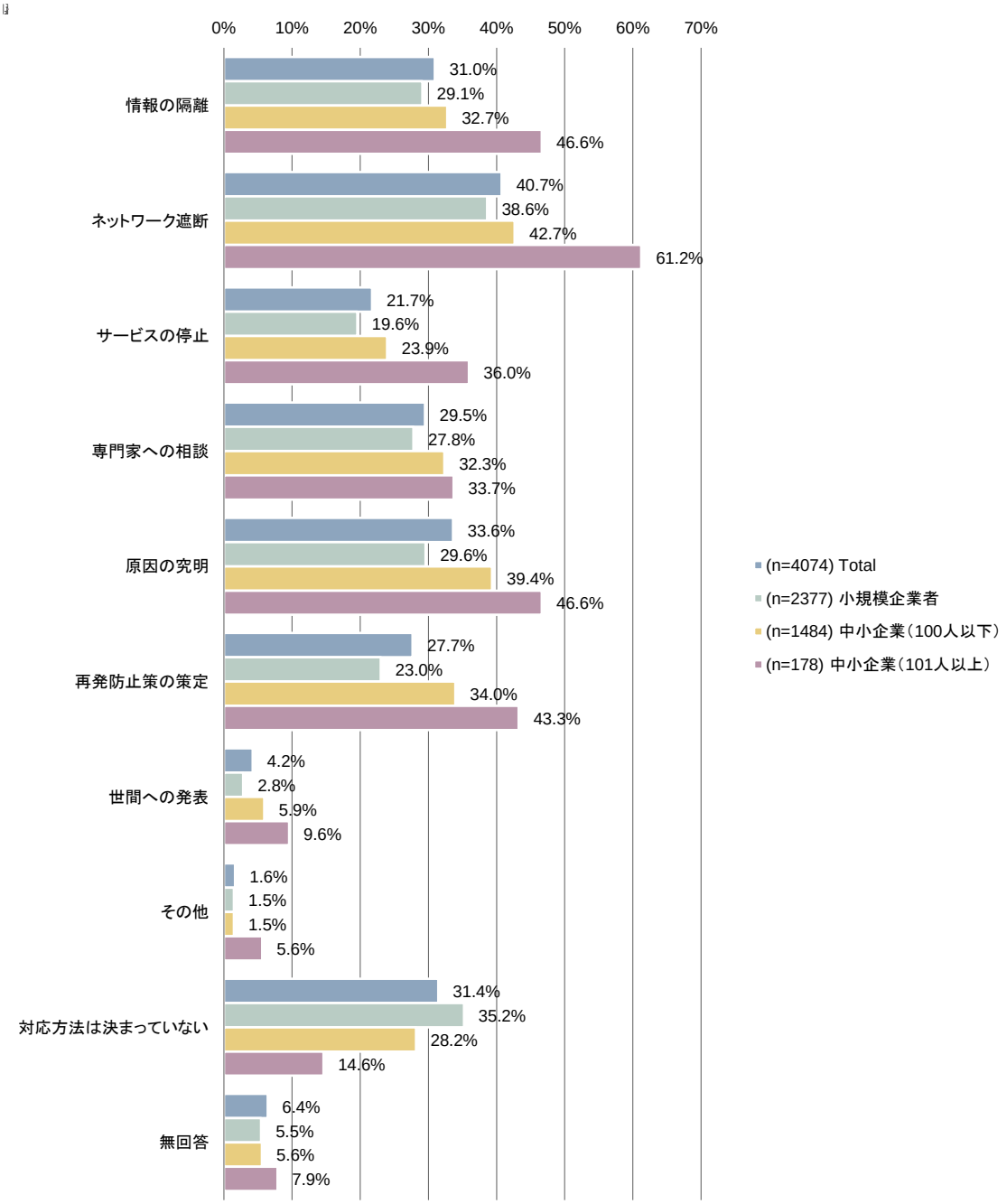
図表　2-103　情報漏えい等のインシデント又はその兆候を発見した場合の報告先（企業規模別）（MA）



⑭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

全ての選択肢において、中小企業（101人以上）の割合が最も高い結果となっている。

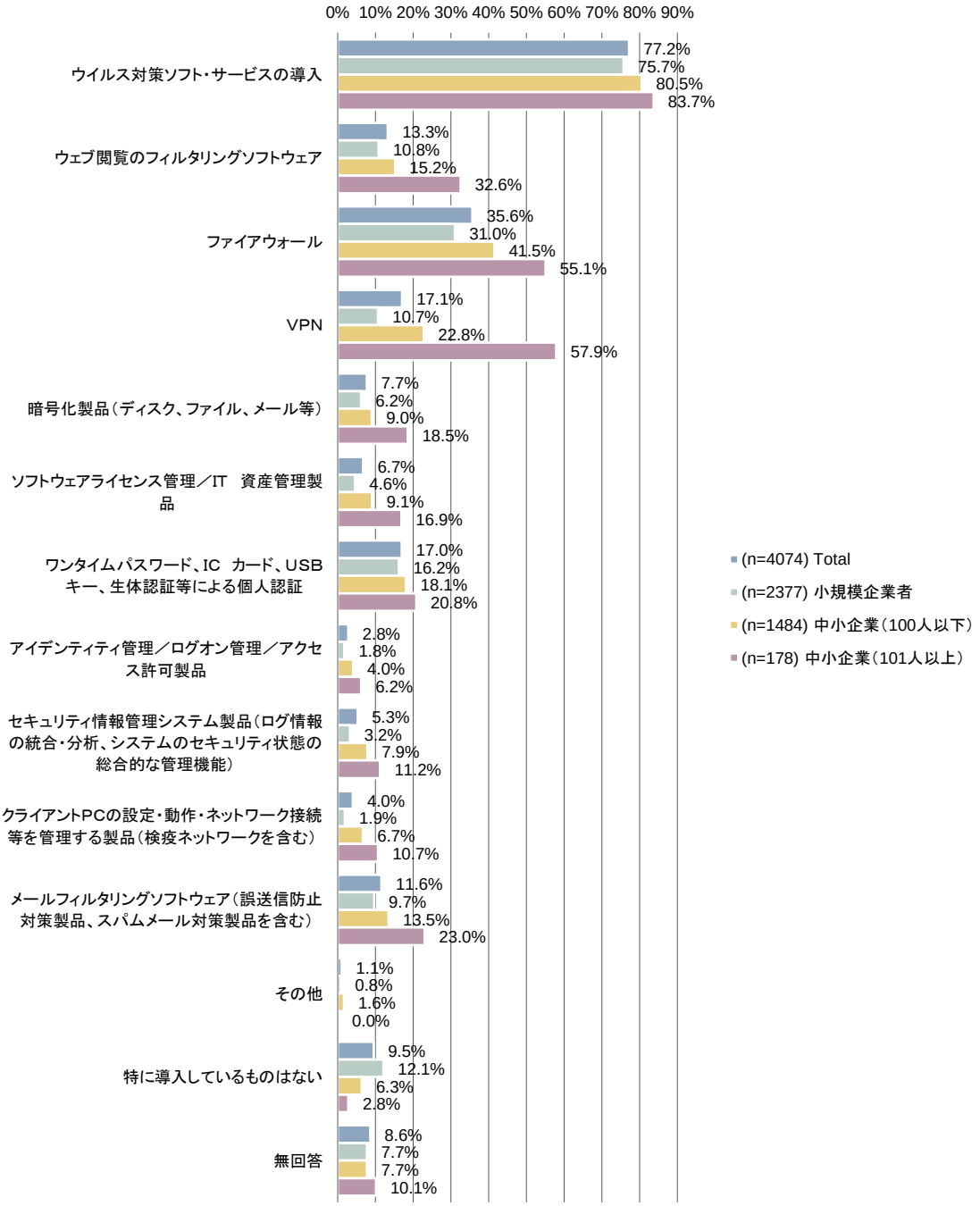
図表　2-104　情報漏えい等のインシデント又はその兆候を発見した場合の対応方法（企業規模別）（MA）



⑮情報セキュリティ関連製品やサービスの導入状況

中小企業（101人以上）において、「ウェブ閲覧のフィルタリングソフトウェア（32.6%）」、「ファイアウォール（55.1%）」、「VPN（57.9%）」と、中小企業全体と比較すると高い割合で導入されている。また、「ウイルス対策ソフト・サービスの導入」については、企業規模に関わらず導入割合が高い。

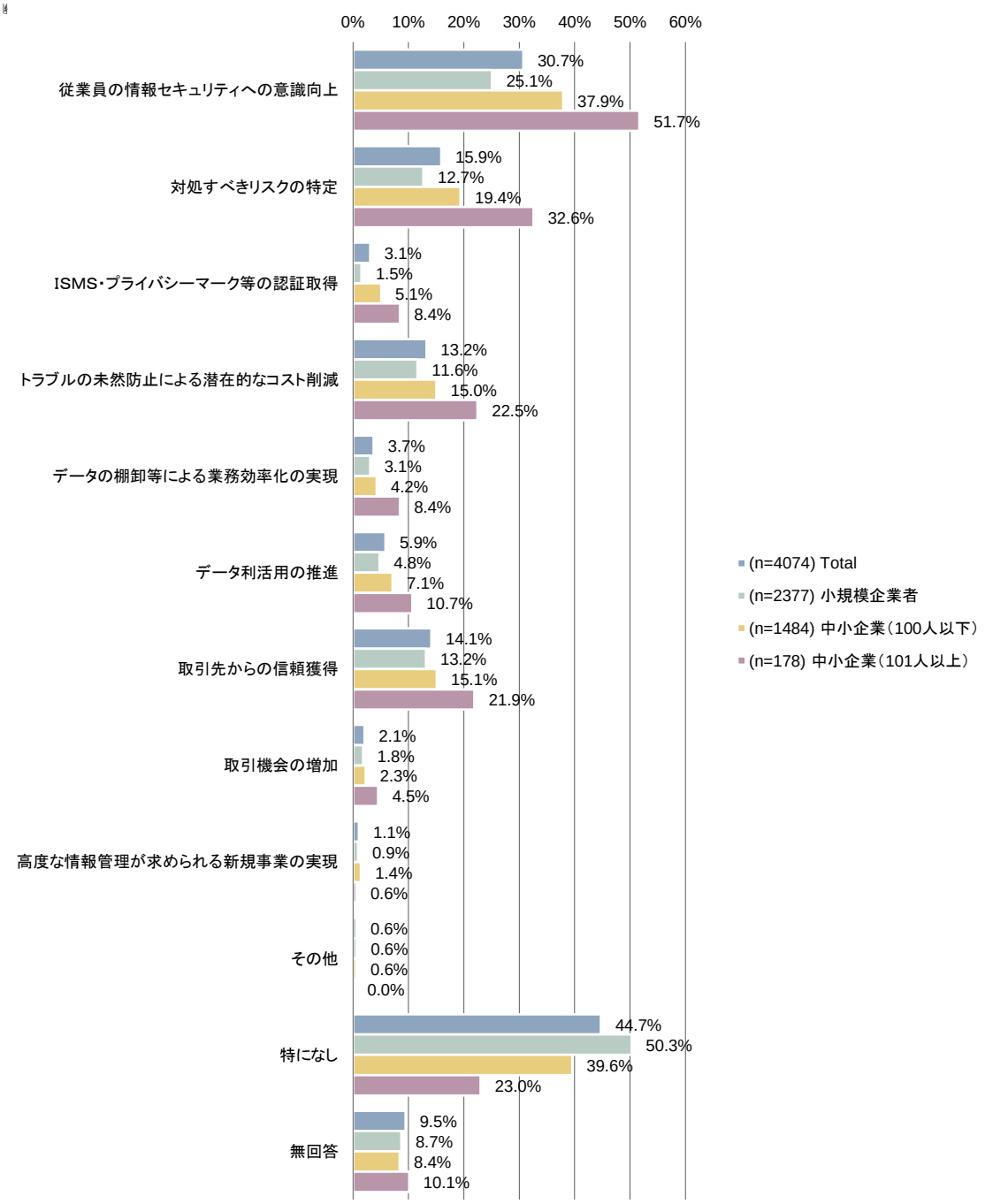
図表　2-105　情報セキュリティ関連製品やサービスの導入状況（企業規模別）（MA）



⑯情報セキュリティ対策を実施して感じられたメリット

「従業員の情報セキュリティへの意識向上」を回答している中小企業（101人以上）が51.7%と最も高い。「特になし」を回答した中小企業（101人以上）が23.0%に対し、小規模企業者は50.3%となっており、企業規模が大きいほどメリットを感じている。

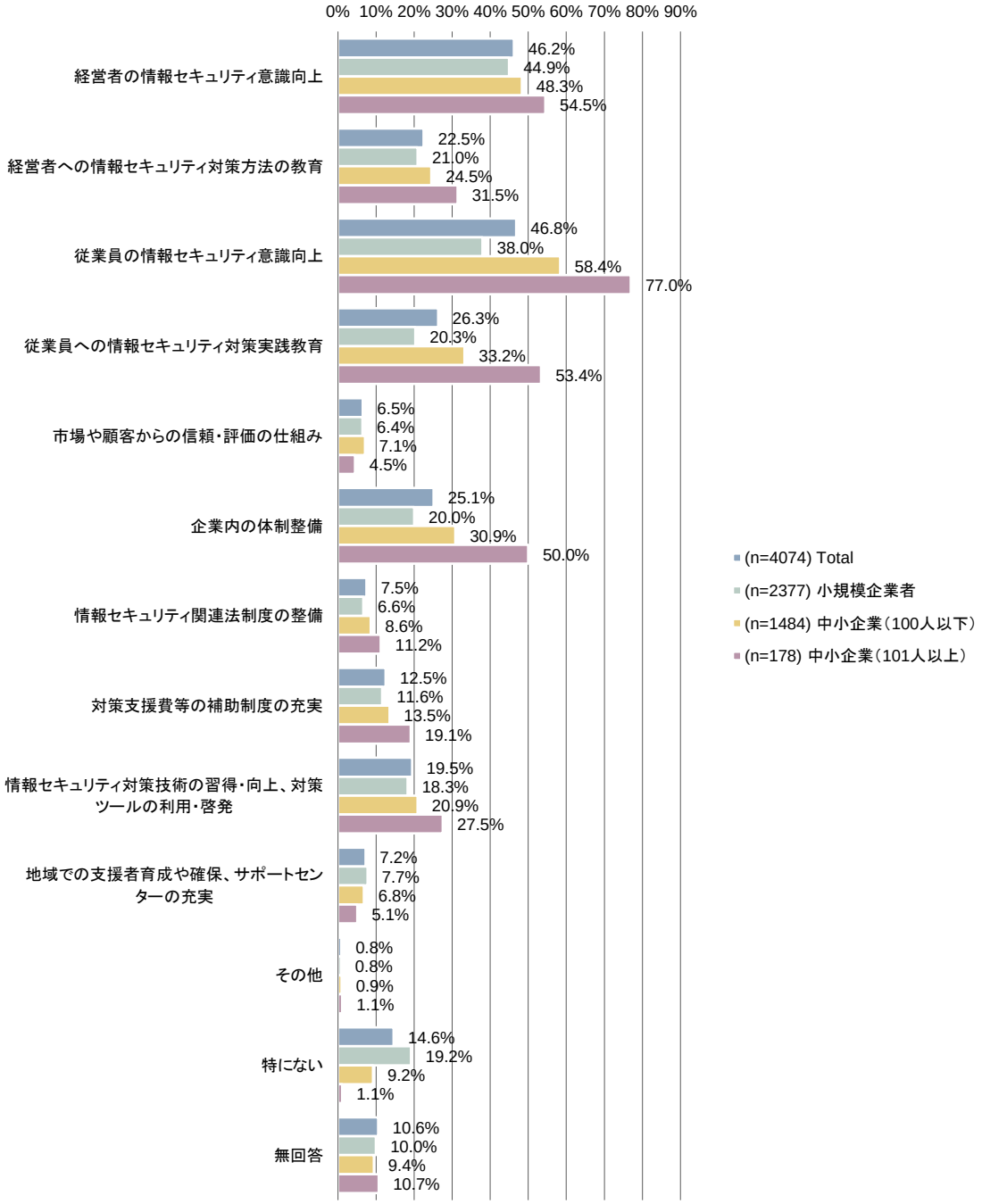
図表　2-106　情報セキュリティ対策を実施して感じられたメリット（企業規模別）（MA）



⑰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

中小企業（101人以上）は、「従業員の情報セキュリティ意識向上（77.0%）」、「従業員への情報セキュリティ対策実践教育（53.4%）」と従業員に関する項目の割合が全体の平均に比べ特に高い。

図表　2-107　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（企業規模別）（MA）

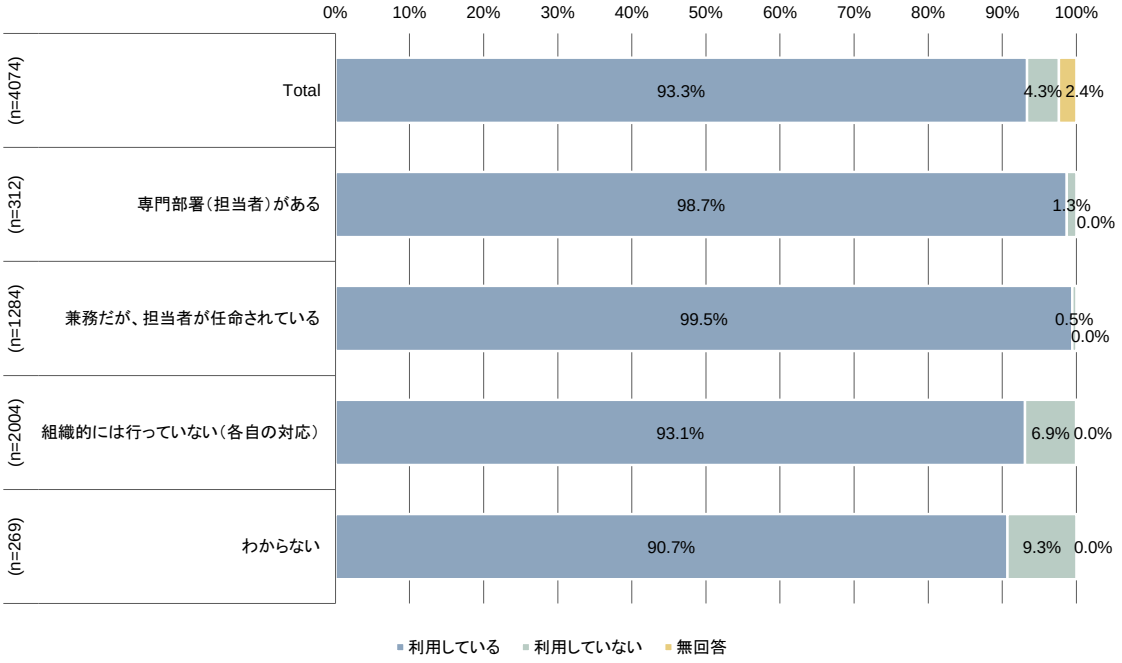


（２）セキュリティ体制によるクロス集計結果

①業務用パソコン・タブレット端末・スマートフォンの利用状況

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企業での利用されている割合が多少高い。

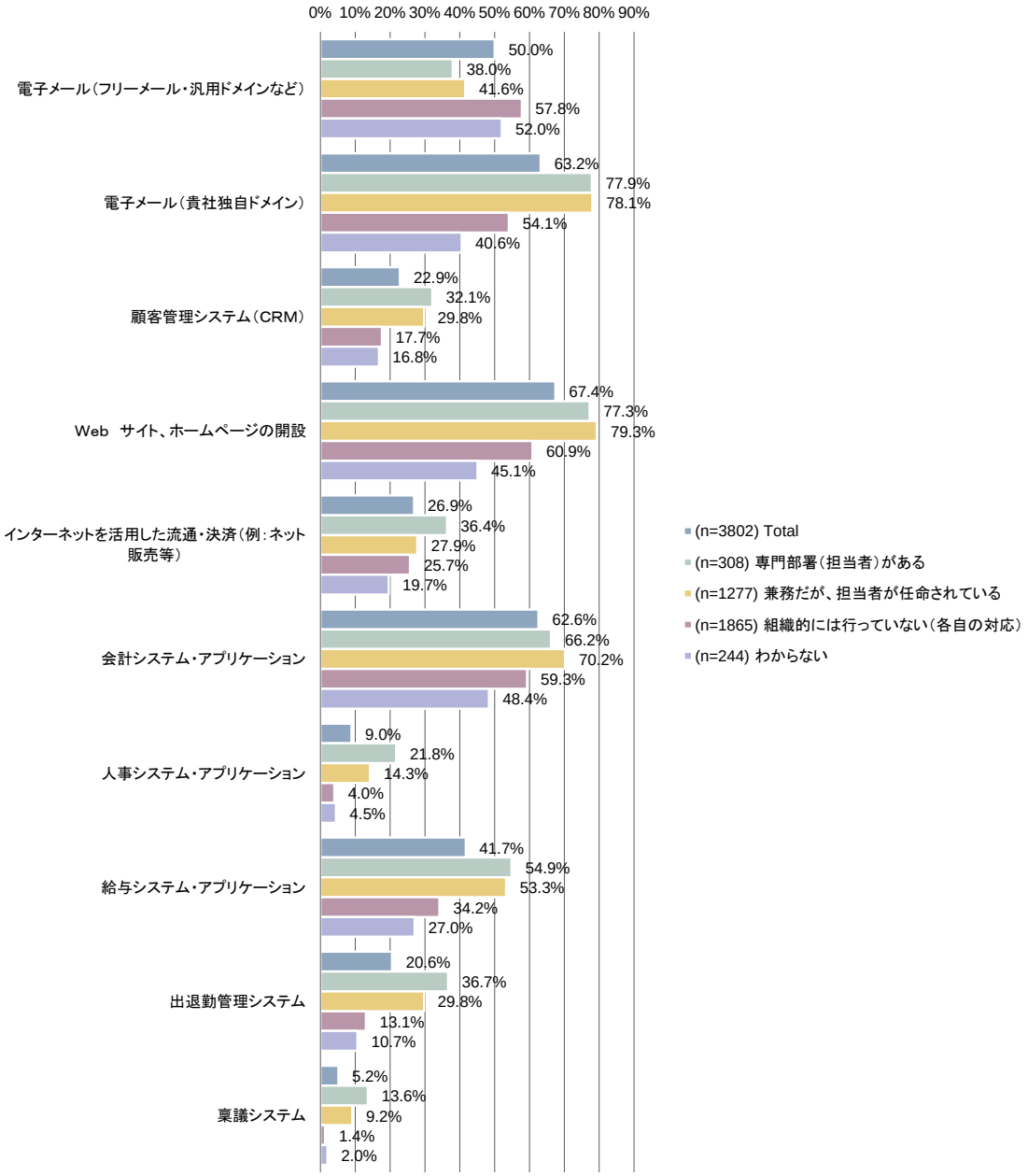
図表　２-108　業務用パソコン・タブレット端末・スマートフォンの利用状況（セキュリティ体制別）（SA）



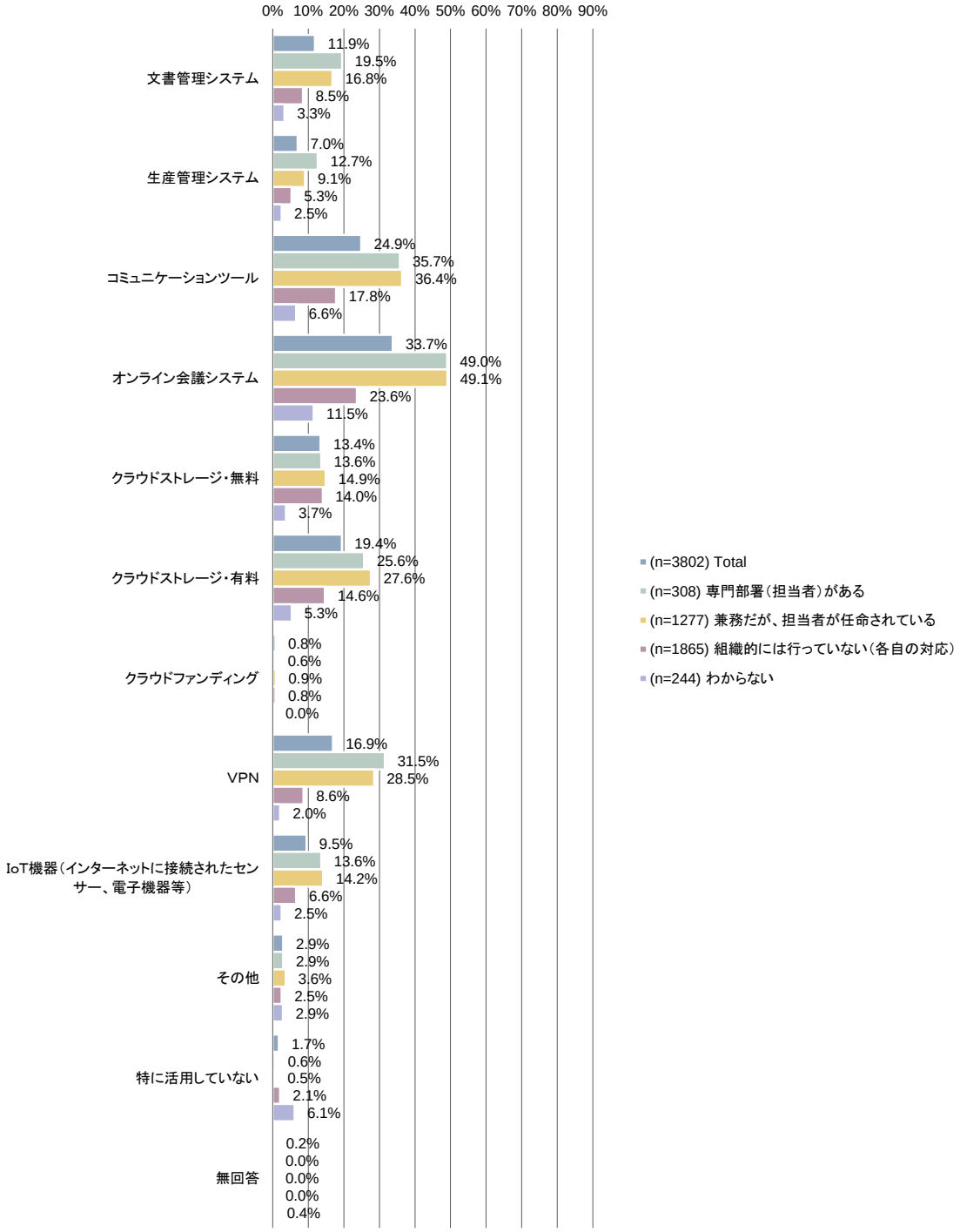
②利用・導入しているサービスやシステム

大半のサービスにおいて、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企業で使用されている割合が多少高い。

図表 2-109 利用・導入しているサービスやシステム①（セキュリティ体制別）（MA）



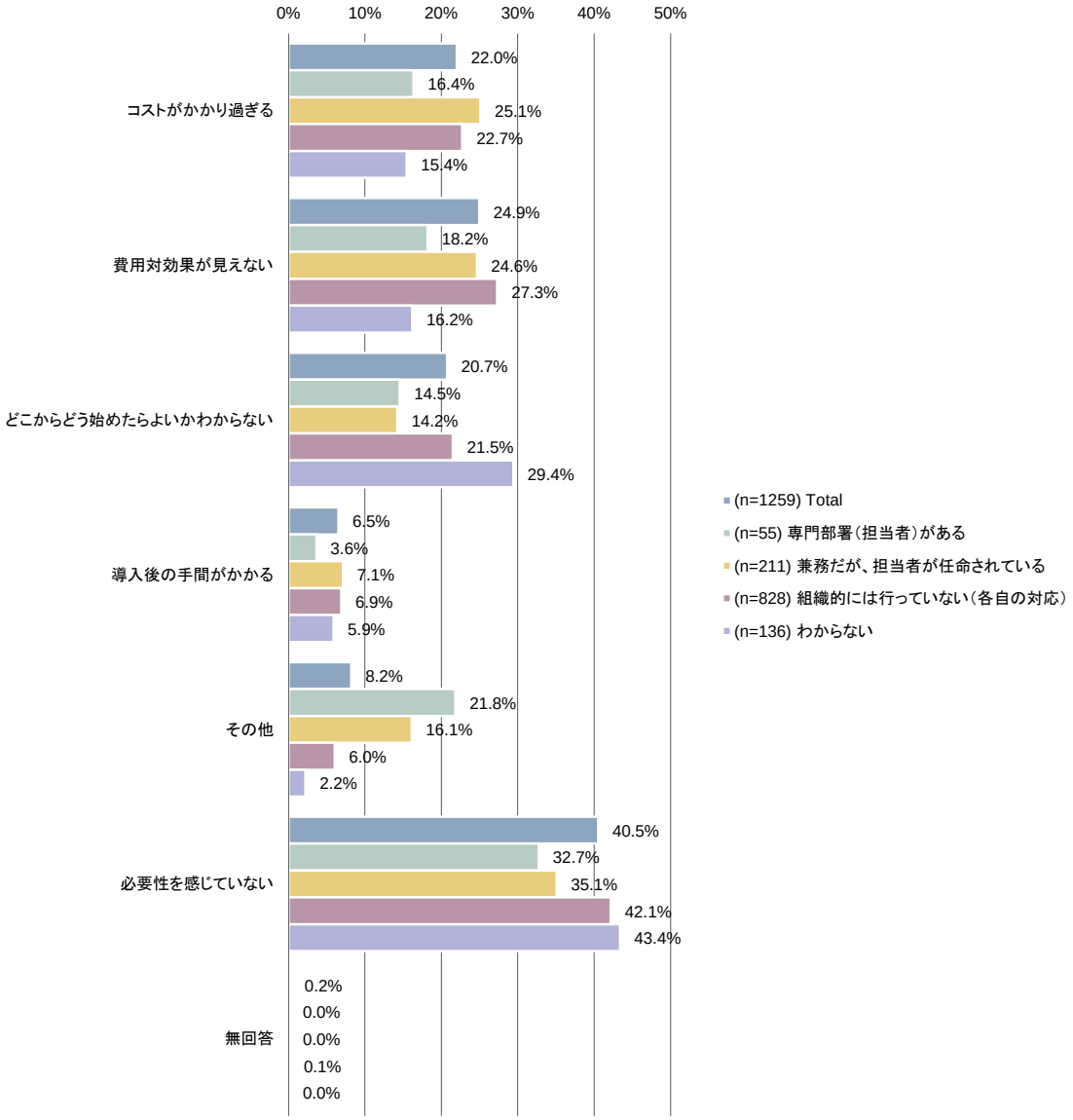
図表　2-110　利用・導入しているサービスやシステム②（セキュリティ体制別）（MA）



③情報セキュリティ対策投資を行わなかった理由

「どこをどう始めたらよいか分からない」、「必要性を感じていない」という回答は、組織的に対応していない企業での割合が高い。「コストがかかりすぎる」、「費用対効果が見えない」という回答は、担当者が任命されている企業においても一定の割合がある。

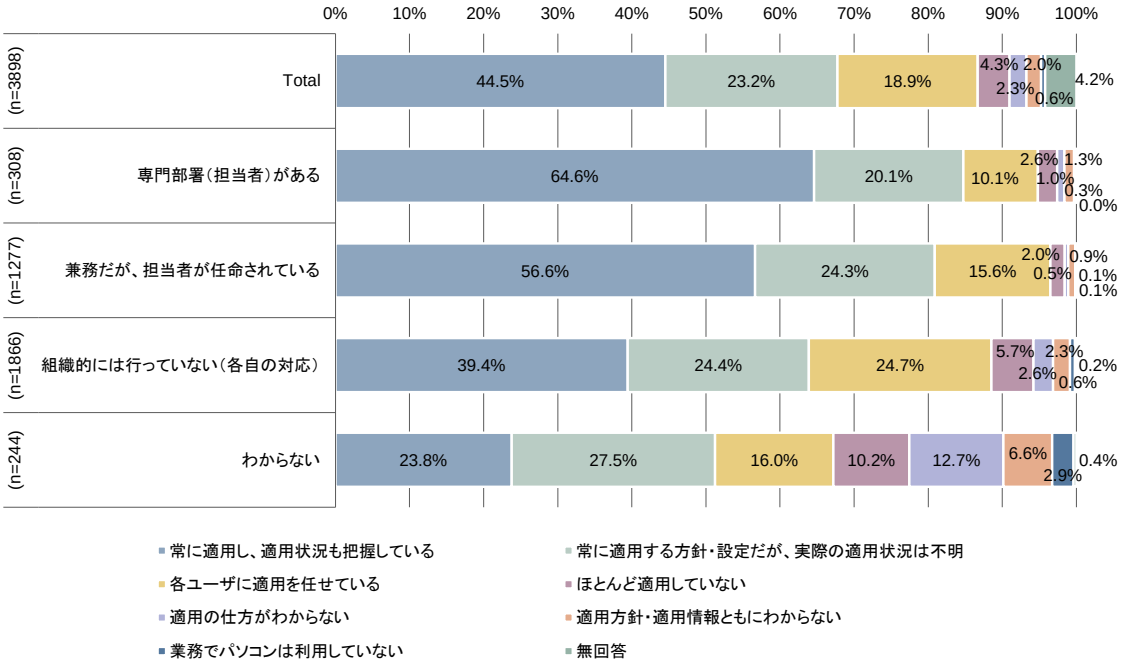
図表　2-111　情報セキュリティ対策投資を行わなかった理由（セキュリティ体制別）（MA）



④パソコンへのWindows Updateなどによるセキュリティパッチの適用状況

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企業ほど常に適用する方針とされており、適用状況も把握されている結果である。

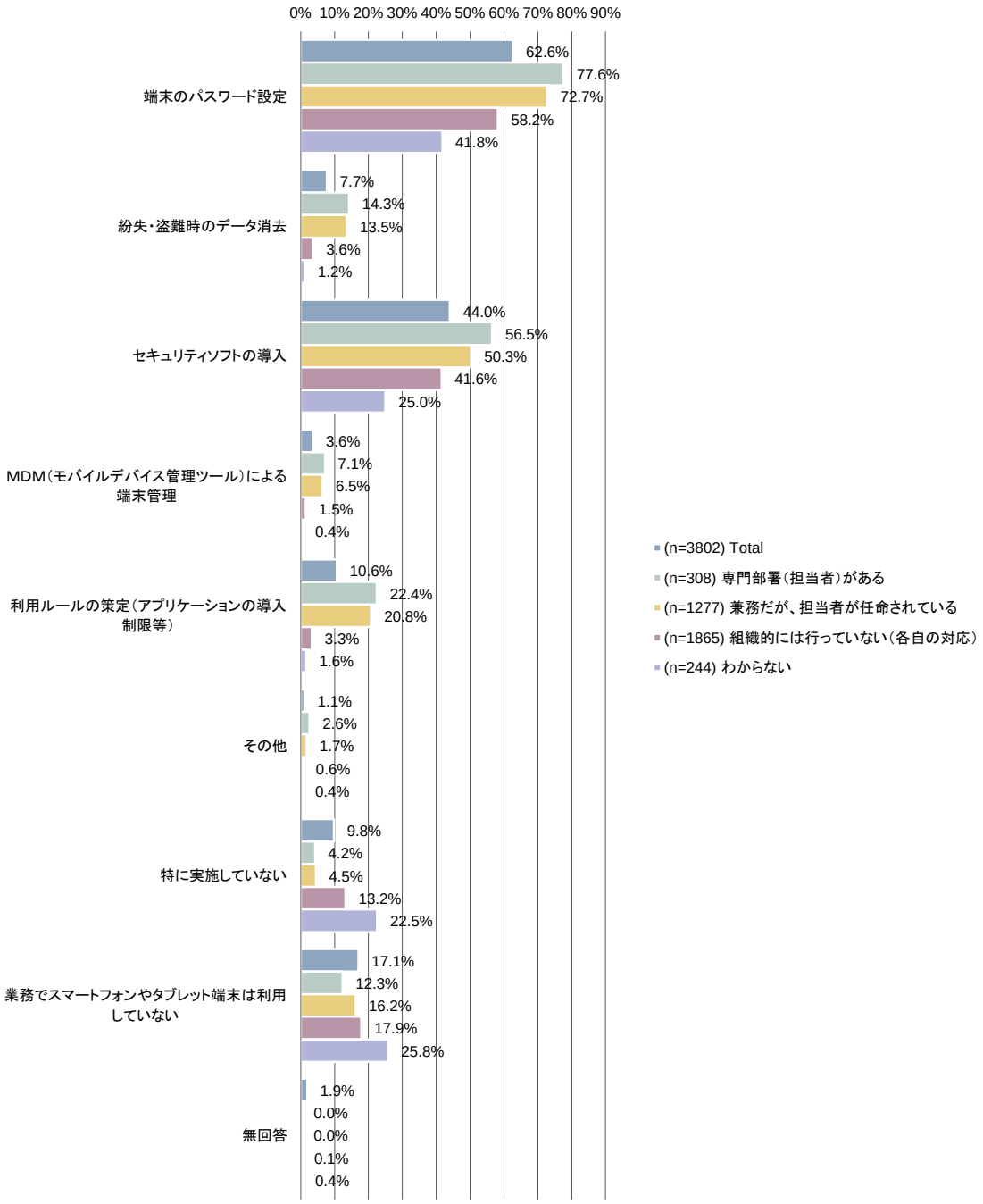
図表 2-112 パソコンへのWindows Updateなどによるセキュリティパッチの適用状況（セキュリティ体制別）（SA）



⑤スマートフォンやタブレット端末に対して実施している対策

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企業ほど、あらゆる対策を積極的に実施している。特に「利用ルールの策定（アプリケーションの導入制限等）」の回答については、実施している企業の多くは専門部署（担当者）がある、兼務だが担当者が任命されている企業となっている。

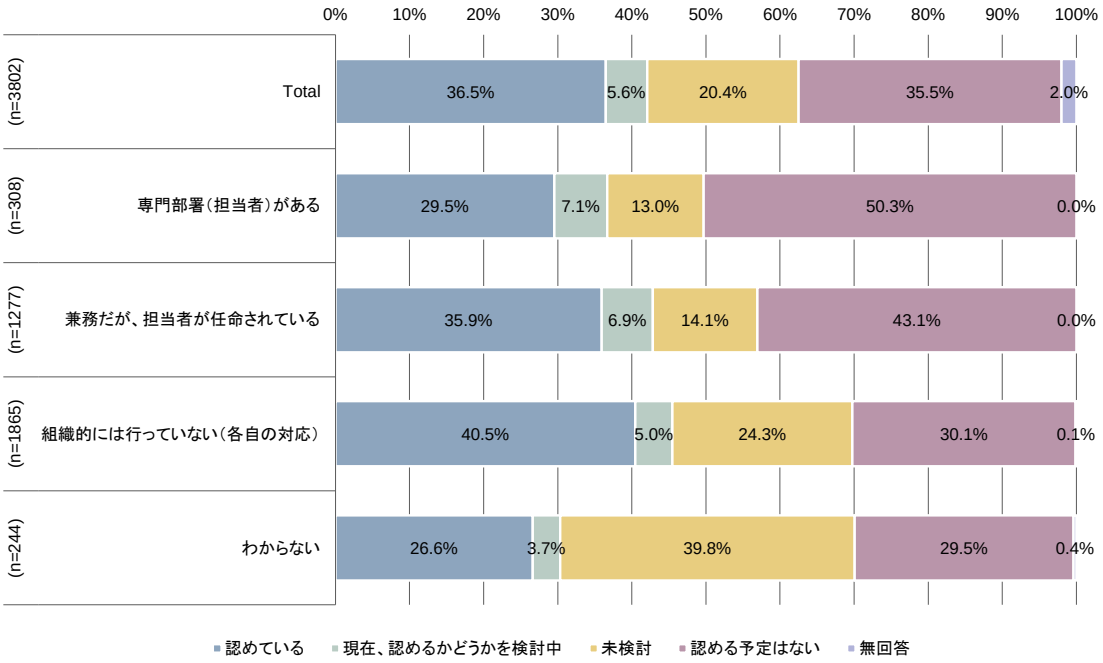
図表 2-113 スマートフォンやタブレット端末に対して実施している対策（セキュリティ体制別）（MA）



⑥社員の私有端末の業務利用（BYOD：Bring Your Own Device）

組織的に対応していない企業の方が「認めている」という割合が高く、40.5%となっている。

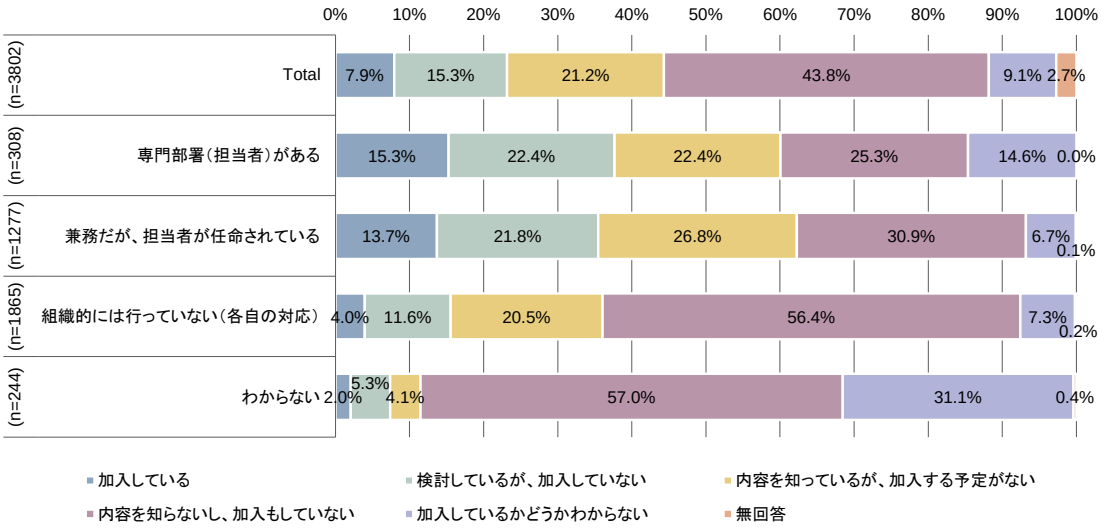
図表　2-114　社員の私有端末の業務利用（セキュリティ体制別）（SA）



⑦保険への加入（サイバー保険）

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企業では、「保険に加入している」のがそれぞれ15.3%、13.7%となっている。

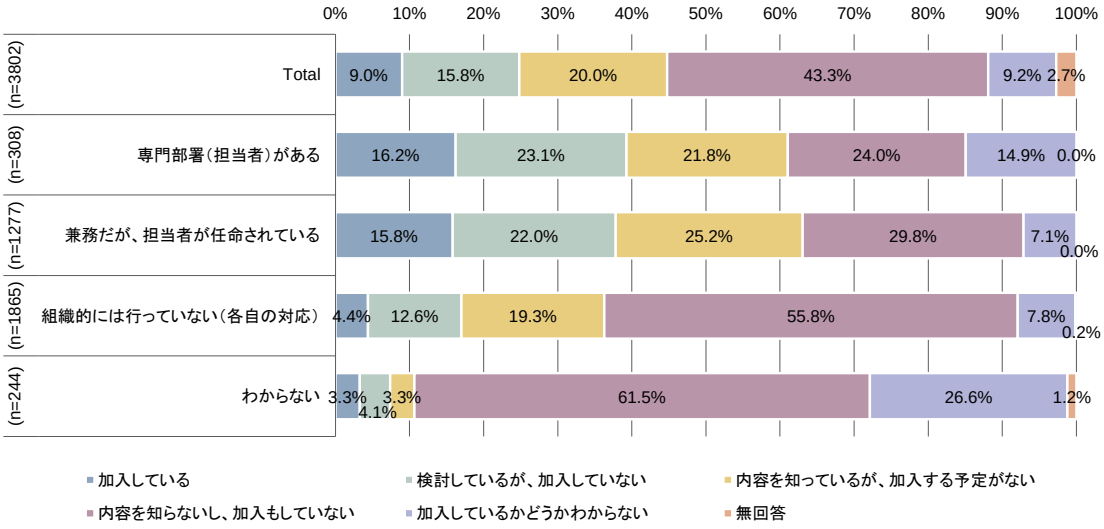
図表 2-115 保険への加入（サイバー保険）（セキュリティ体制別）（SA）



⑧保険への加入（情報漏えい賠償責任保険）

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企業では、「保険に加入している」のがそれぞれ16.2%、15.8%となっている。

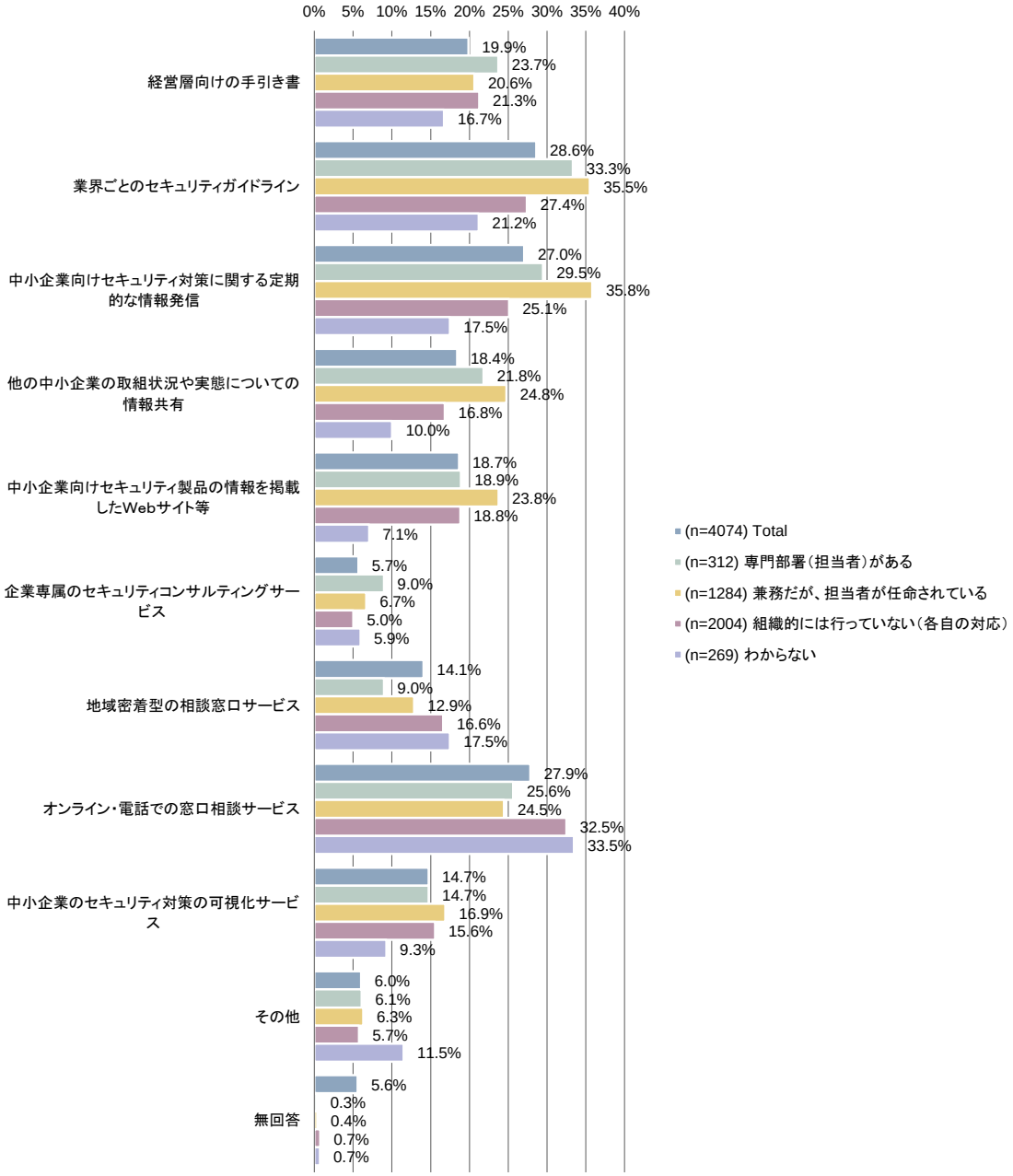
図表 2-116 保険への加入（情報漏えい賠償責任保険）（セキュリティ体制別）（SA）



⑨活用したい情報セキュリティ対策に関するサービス

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企業と、組織的に対応していない企業において結果の差が目立つ選択肢として、「業界ごとのセキュリティガイドライン」、「中小企業向けセキュリティ対策に関する定期的な情報発信」、「他の中小企業の取組状況や実態についての情報共有」、「オンライン・電話での窓口相談サービス」がある。前者３つについては、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企業のニーズが高く、窓口相談サービスについては組織的に対応していない企業のニーズが高い。

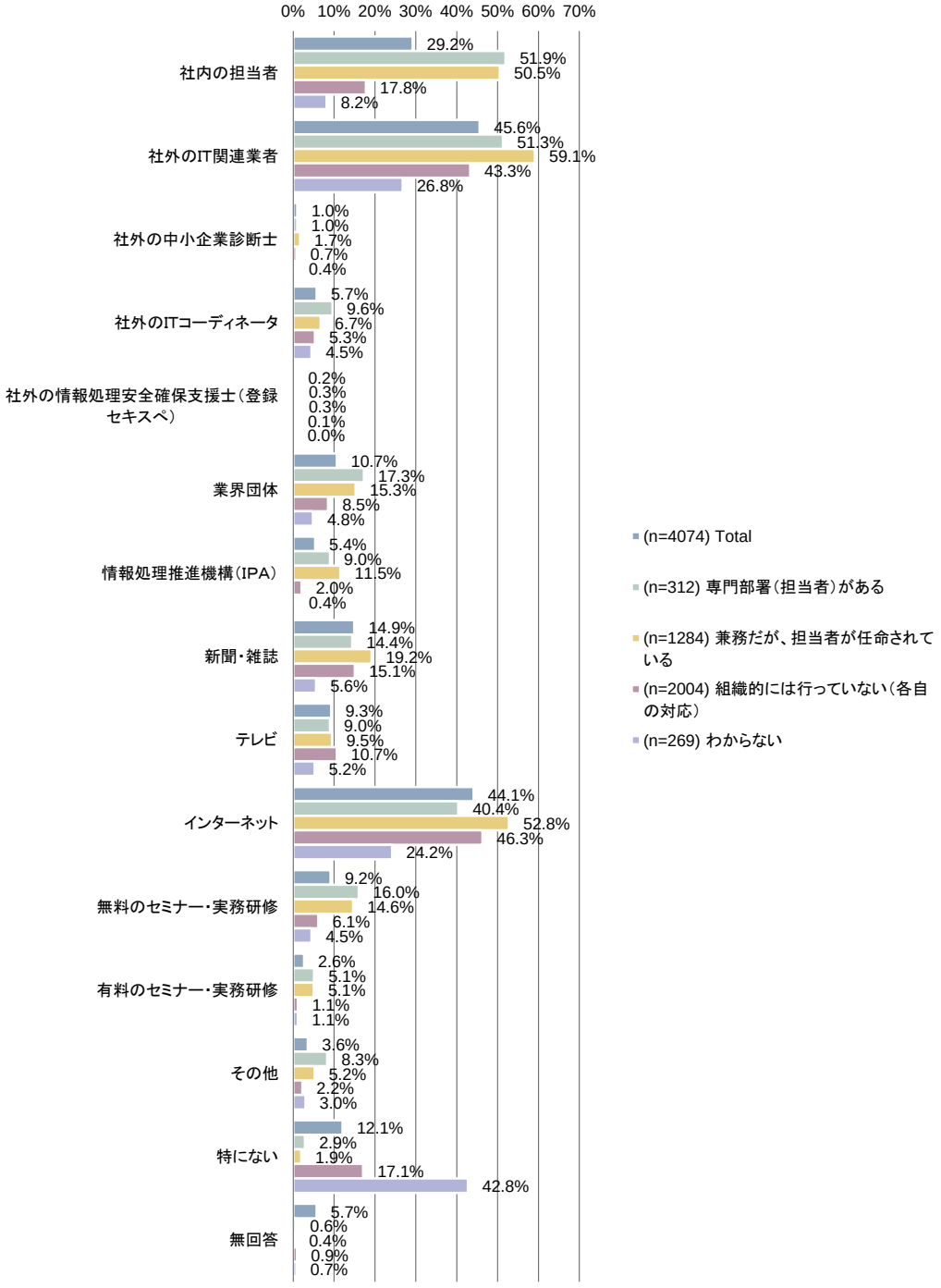
図表　2-117　活用したい情報セキュリティ対策に関するサービス（セキュリティ体制別）（MA）



⑩情報セキュリティに関する情報収集先

セキュリティ体制によらず「社外のIT関連事業者」、「インターネット」の割合が高い。「社内の担当者」の割合は、専門部署がある・担当者が任命されている企業においては50%を超えている。

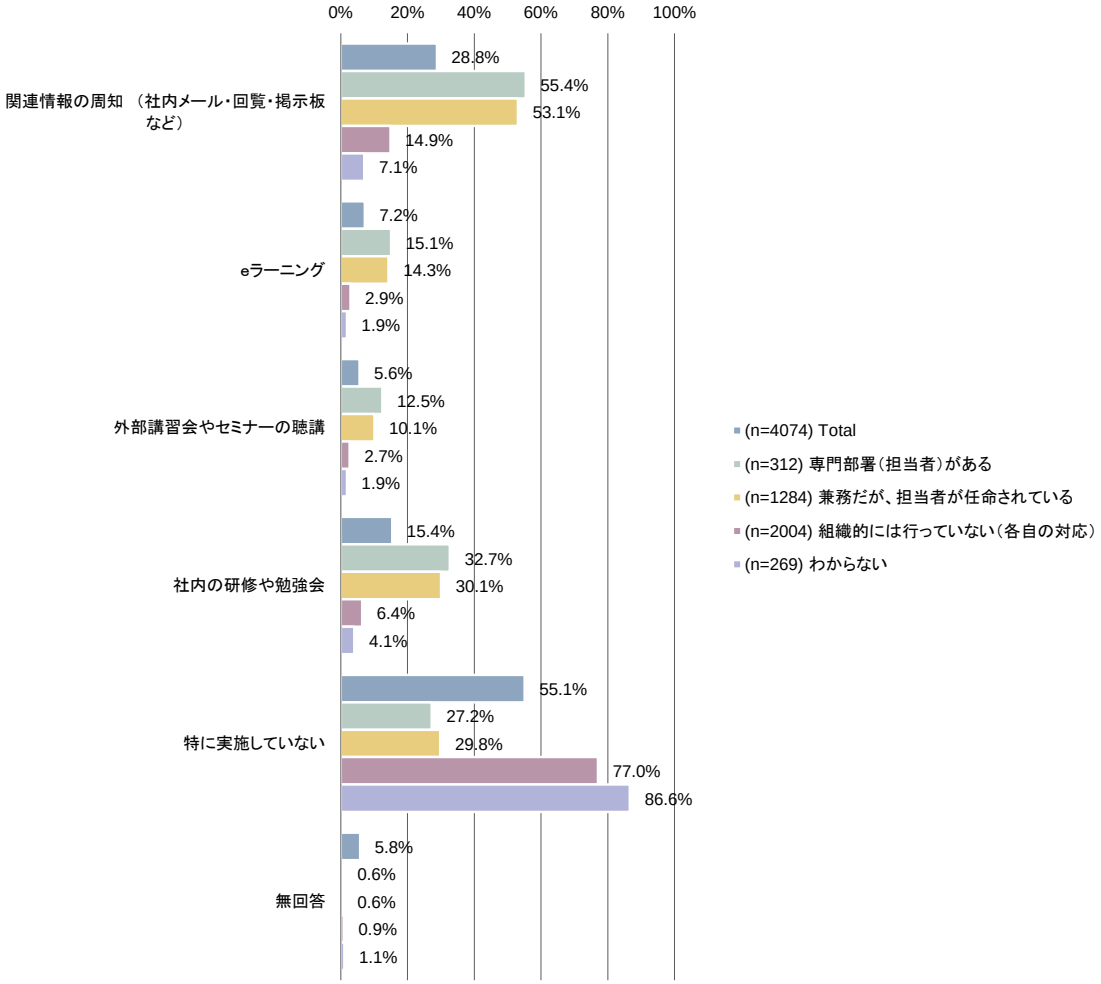
図表 2-118 情報セキュリティに関する情報収集先（セキュリティ体制別）（MA）



⑪従業員に対する情報セキュリティ教育の実施状況

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企業において、「関連情報の周知（社内メール・回覧・掲示板など）」、「社内の研修や勉強会」の割合が高い。組織的に対応していない企業は、「特に実施していない」の割合が70%を超えている。

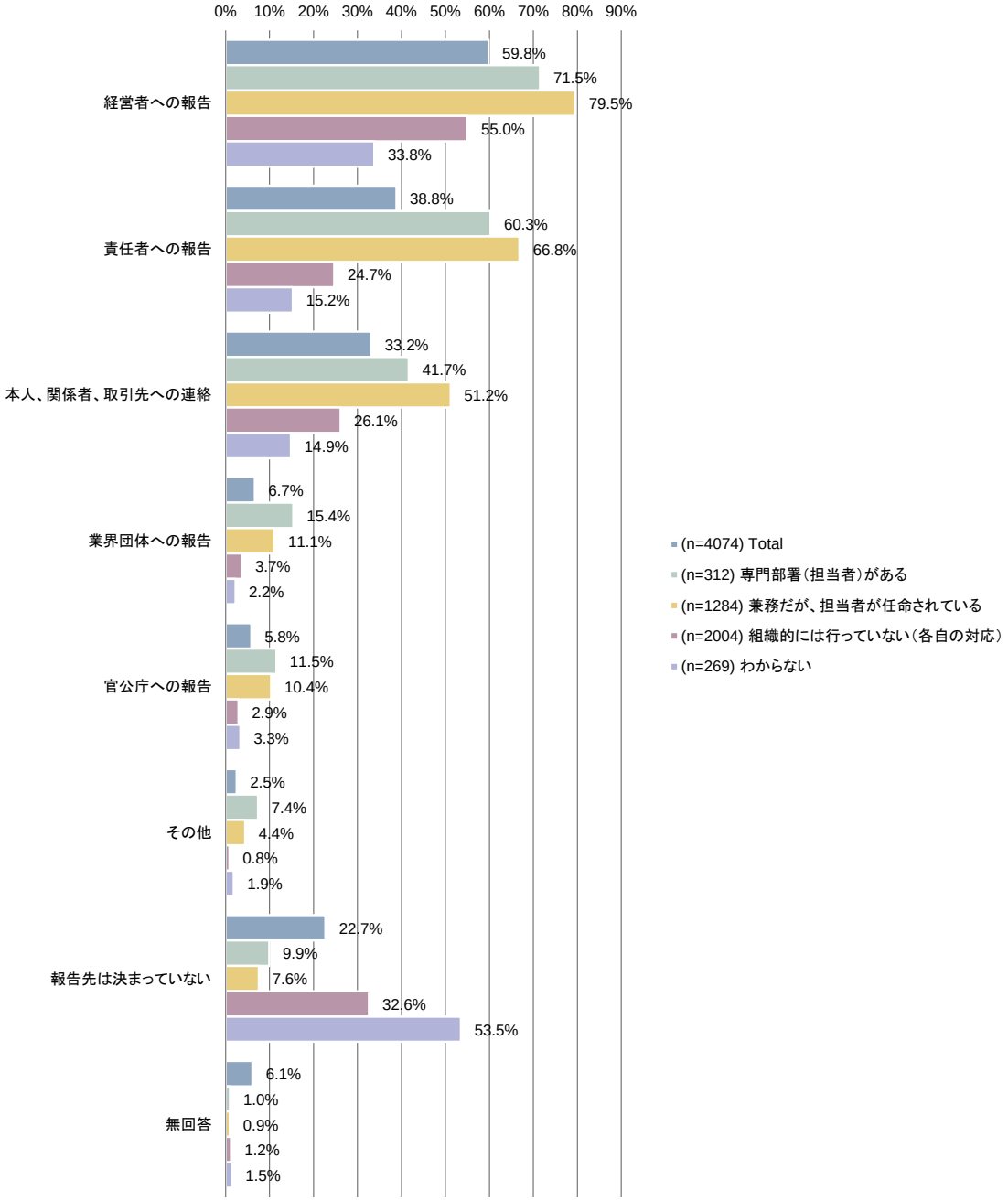
図表　2-119　従業員に対する情報セキュリティ教育の実施状況（セキュリティ体制別）（MA）



⑫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

「経営者への報告」「責任者への報告」への回答は、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企業における割合が高く、特に「責任者への報告」については、60%を超えている。

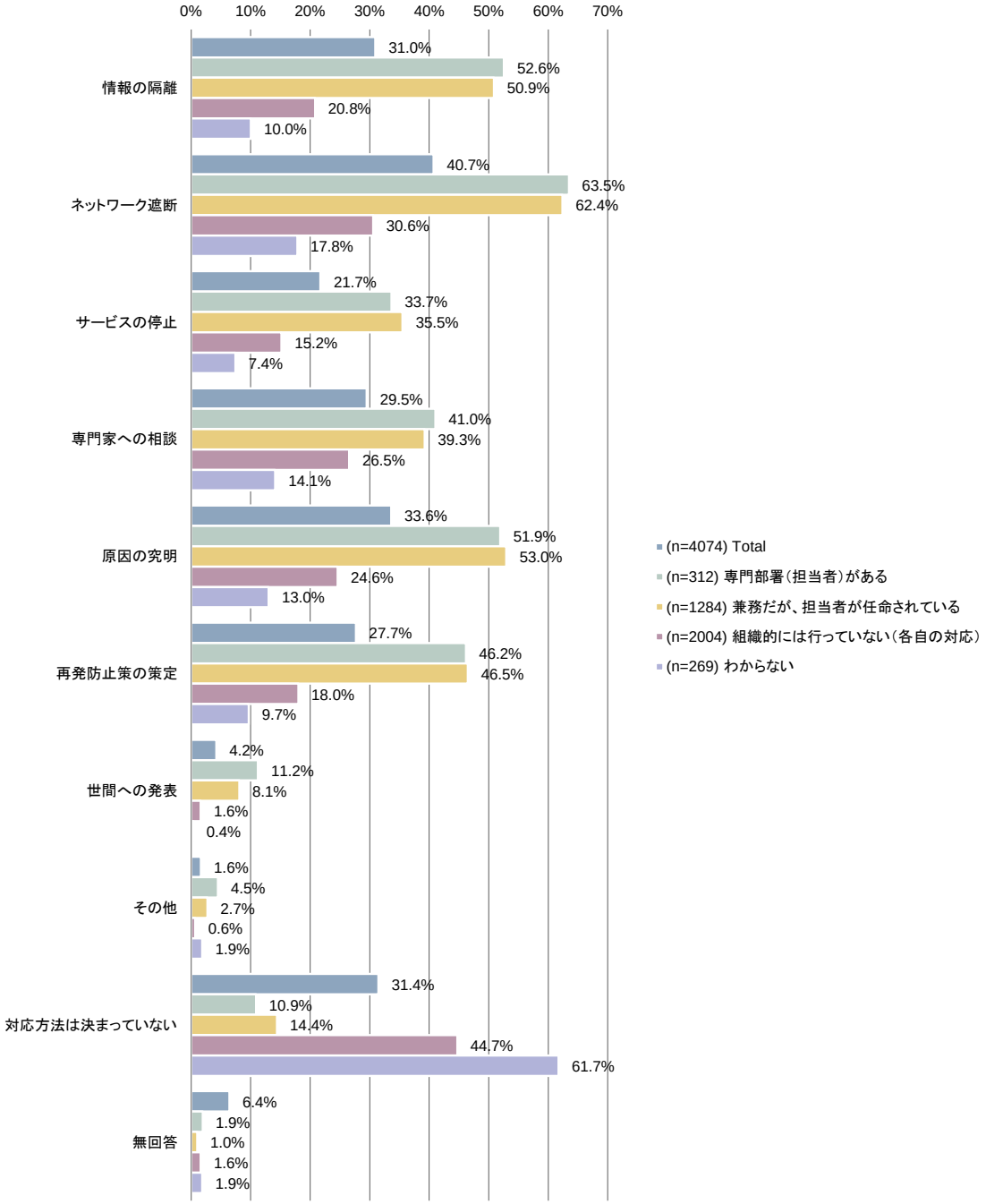
図表　2-120　情報漏えい等のインシデント又はその兆候を発見した場合の報告先（セキュリティ体制別）（MA）



⑬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

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については、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企業が、あらゆる方法において回答の割合が高い。

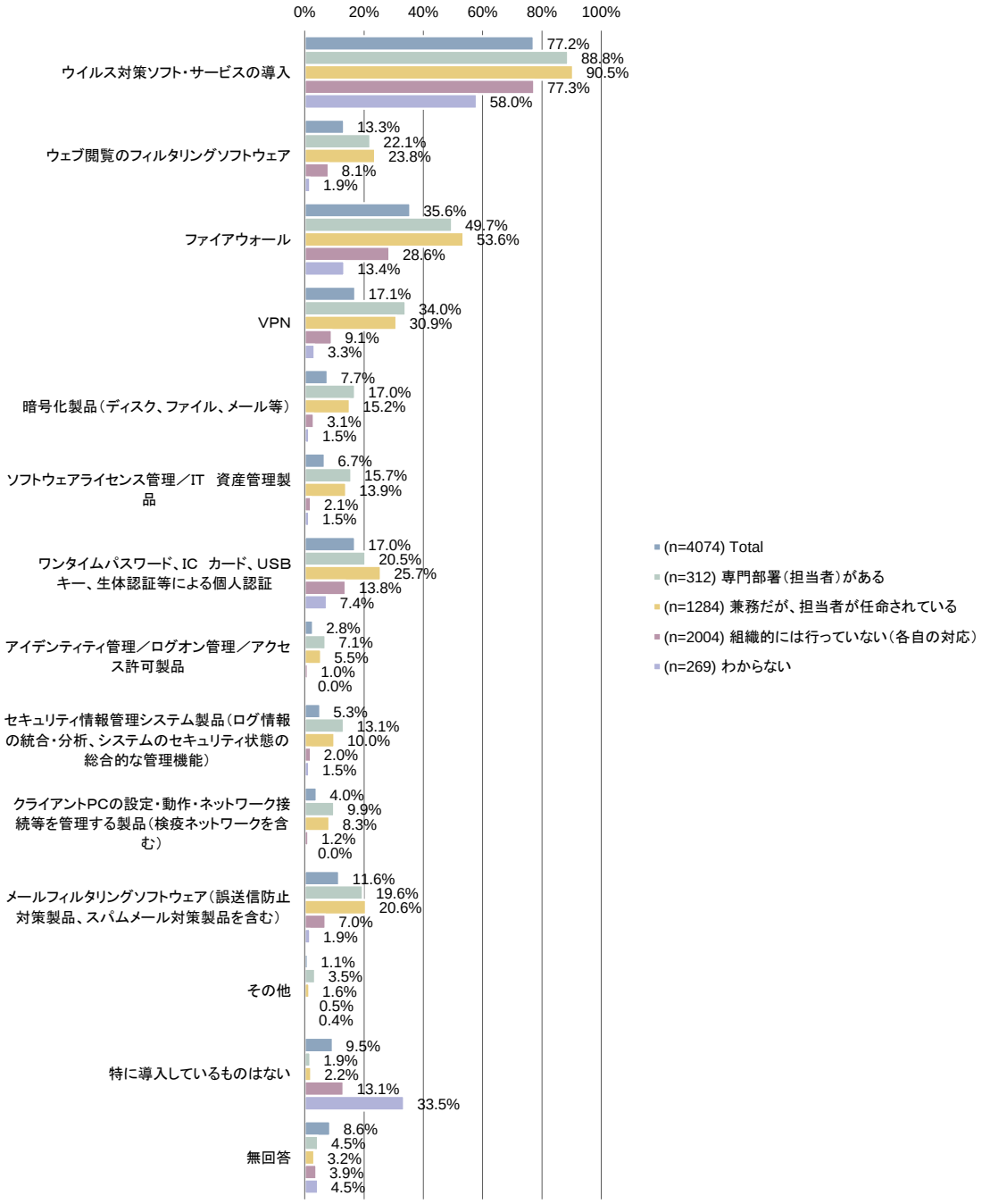
図表　2-121　情報漏えい等のインシデント又はその兆候を発見した場合の対応方法（セキュリティ体制別）（MA）



⑭情報セキュリティ関連製品やサービスの導入状況

「ウイルス対策ソフト・サービスの導入」については、セキュリティ体制に関わらず高い割合で導入されているが、「ファイアウォール」や「VPN」等は専門部署（担当者）がある、兼務だが担当者が任命されている企業が高い割合となっている。

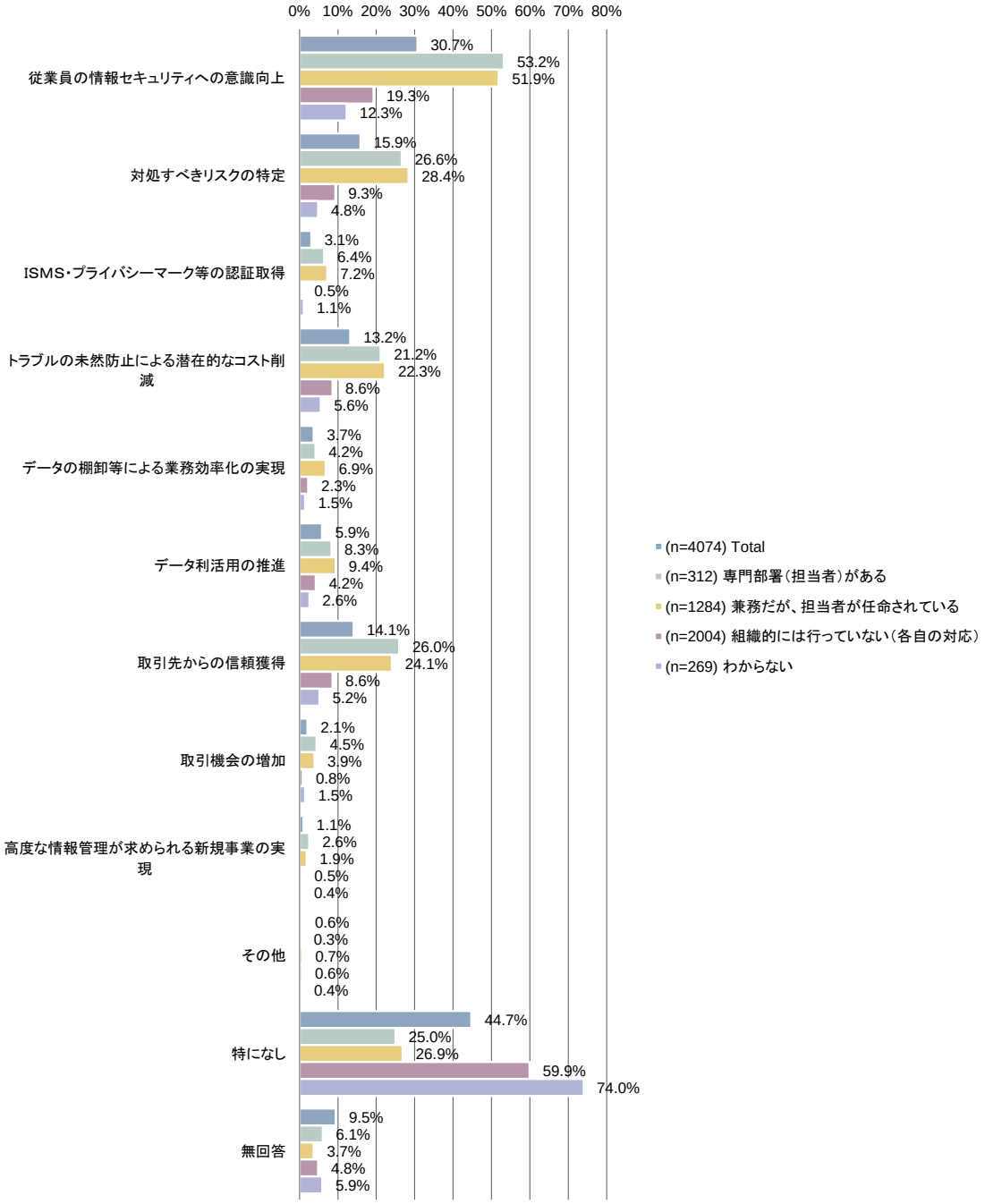
図表　2-122　情報セキュリティ関連製品やサービスの導入状況（セキュリティ体制別）（MA）



⑮情報セキュリティ対策を実施して感じられたメリット

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企業は「従業員の情報セキュリティへの意識向上」をそれぞれ53.2%、51.9%となっており、全体より高い。また、「取引先からの信頼獲得」や「対処すべきリスクの特定」においても同様の結果である。

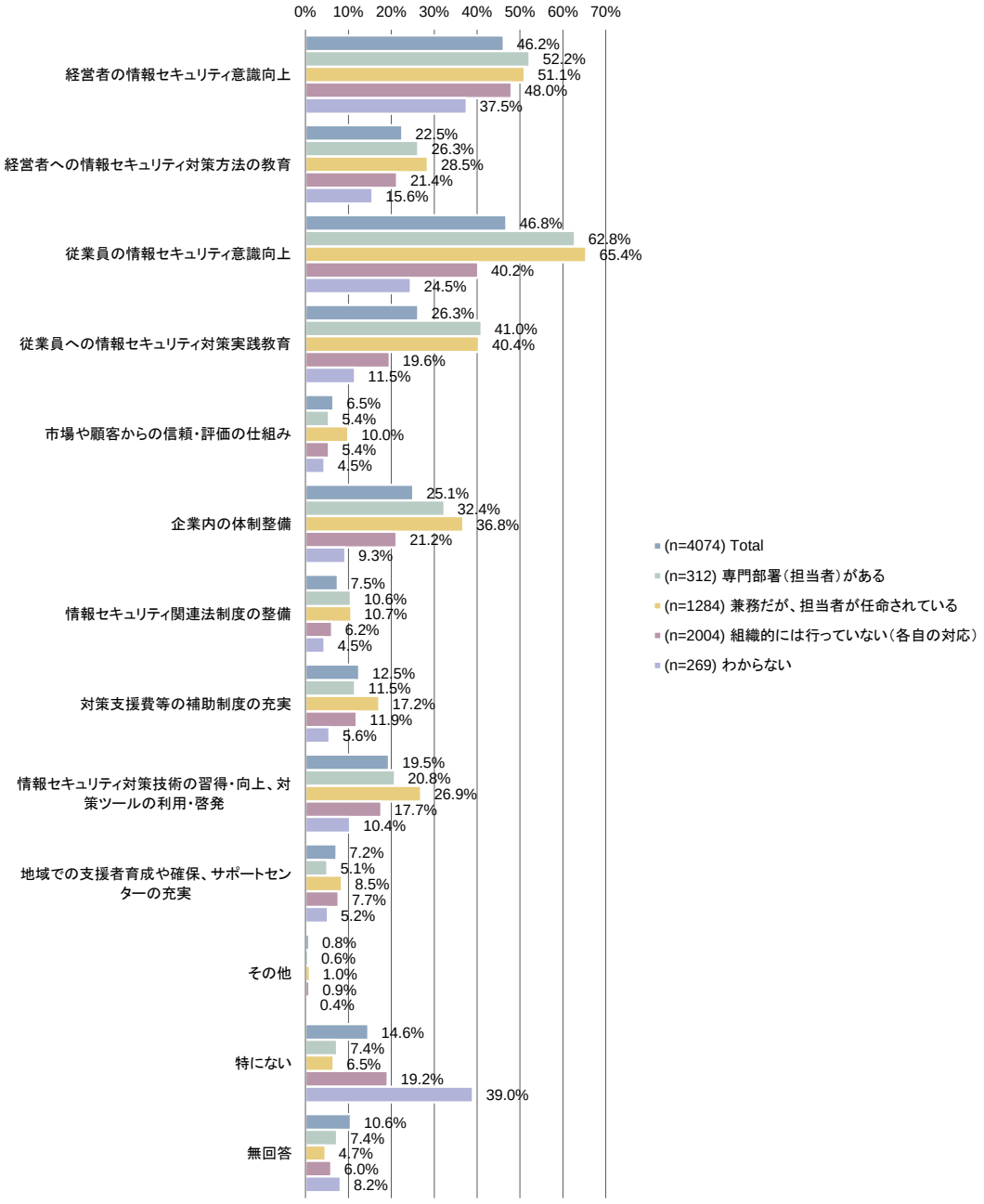
図表　2-123　情報セキュリティ対策を実施して感じられたメリット（セキュリティ体制別）（MA）



⑯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

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企業は「従業員の情報セキュリティ意識向上（62.8%、65.4%）」、「従業員への情報セキュリティ対策実践教育（41.0%、40.4%）」と従業員に関する項目の割合が全体の平均より高く、「企業内の体制整備（32.4%、36.8%）」も平均より高くなっている。

図表　2-124　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（セキュリティ体制別）（MA）

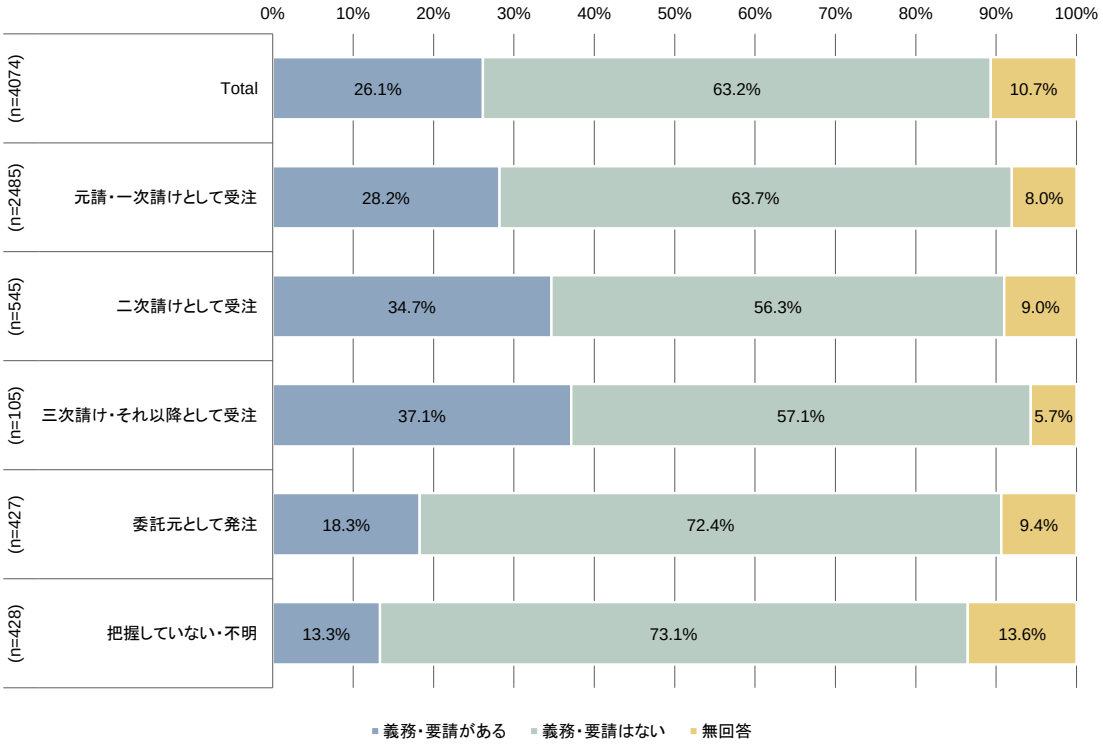


（３）取引上の立場によるクロス集計結果

①販売先・仕入先との契約締結時における情報セキュリティに関する条項・取引上の義務・要請

サプライチェーンの上流（元請・一次請）から下流（三次請け・それ以降）にいくにつれ、「義務・要請がある」の割合が増加している。

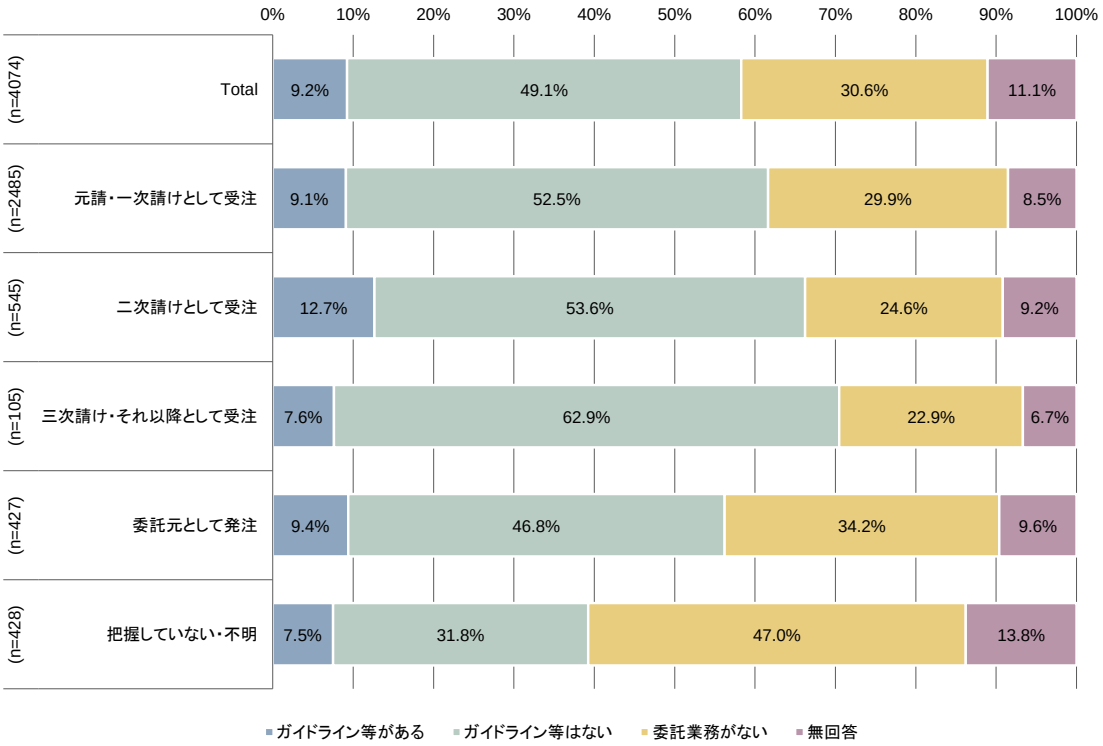
図表　2-125　販売先・仕入先との契約締結時における情報セキュリティに関する条項・取引上の義務・要請（取引上の立場）（SA）



②仕入先への情報セキュリティ対策を行うためのガイドライン

取引上の立場に関わらず「ガイドライン等がある」の割合が10%前後である。

図表　2-126　仕入先への情報セキュリティ対策を行うためのガイドライン（取引上の立場）（SA）



５．調査結果（前回調査との比較）

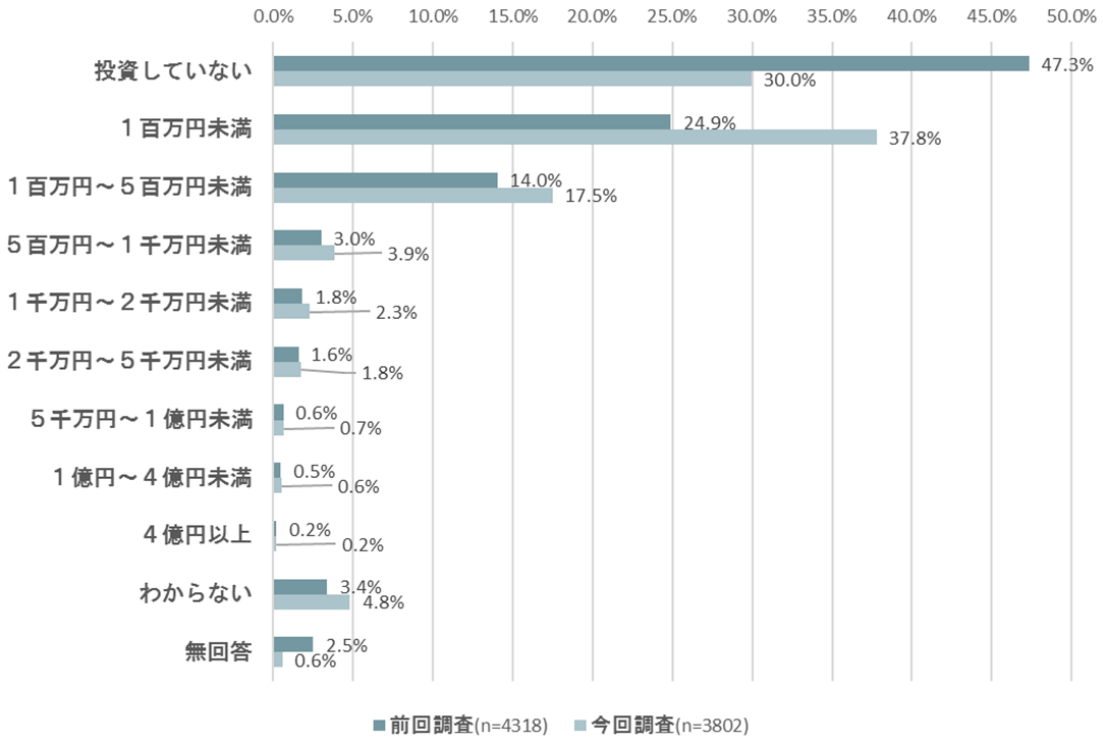
ここからは、前回調査（『2016年度 中小企業における情報セキュリティ対策に関する実態調査』）から継続的に調査を行った設問に関して、結果の比較を実施する。

（１）前回調査結果との比較

①IT投資額

前回調査に比べ、「投資していない」の割合が47.3%から30.0%に減少した。「1百万円未満」の割合が24.9%から37.8%に増加した。

図表 2-127 IT投資額（前回比較）（SA）[3]

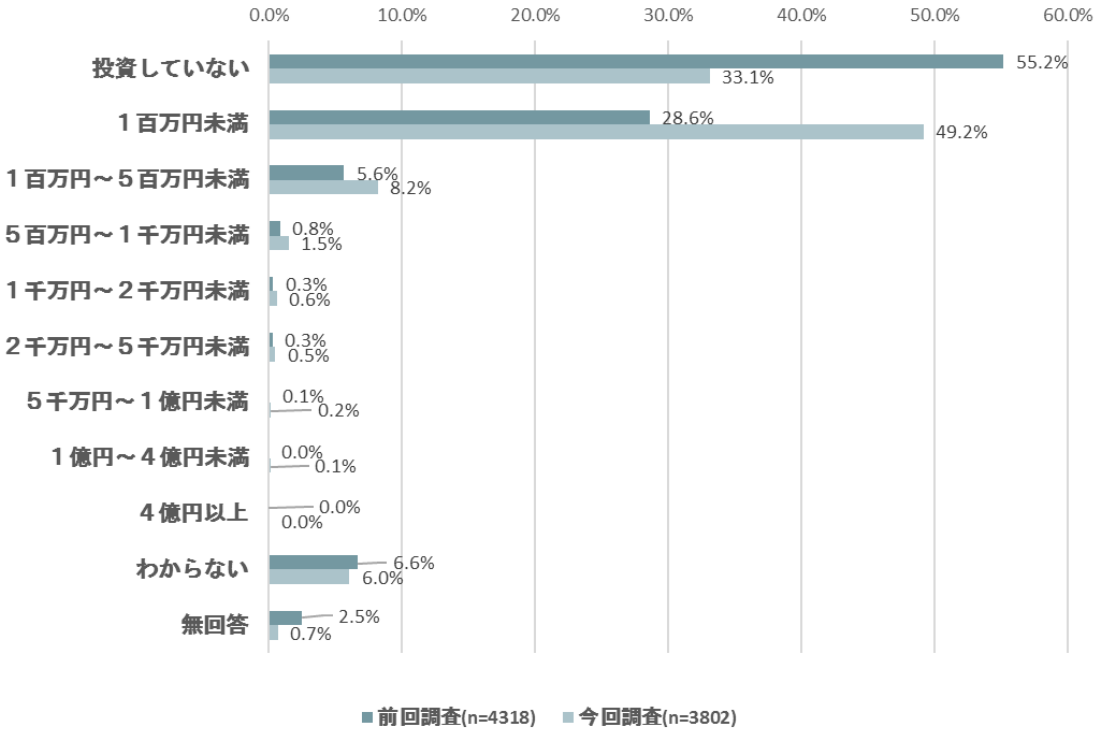


[3] 前回調査の設問設定が異なるので再集計

②情報セキュリティ投資額

前回調査に比べ、「投資していない」の割合が55.2%から33.1%に減少した。「1百万円未満」の割合が28.6%から49.2%に増加した。

図表 2-128 情報セキュリティ投資額（前回比較）（SA）[4]

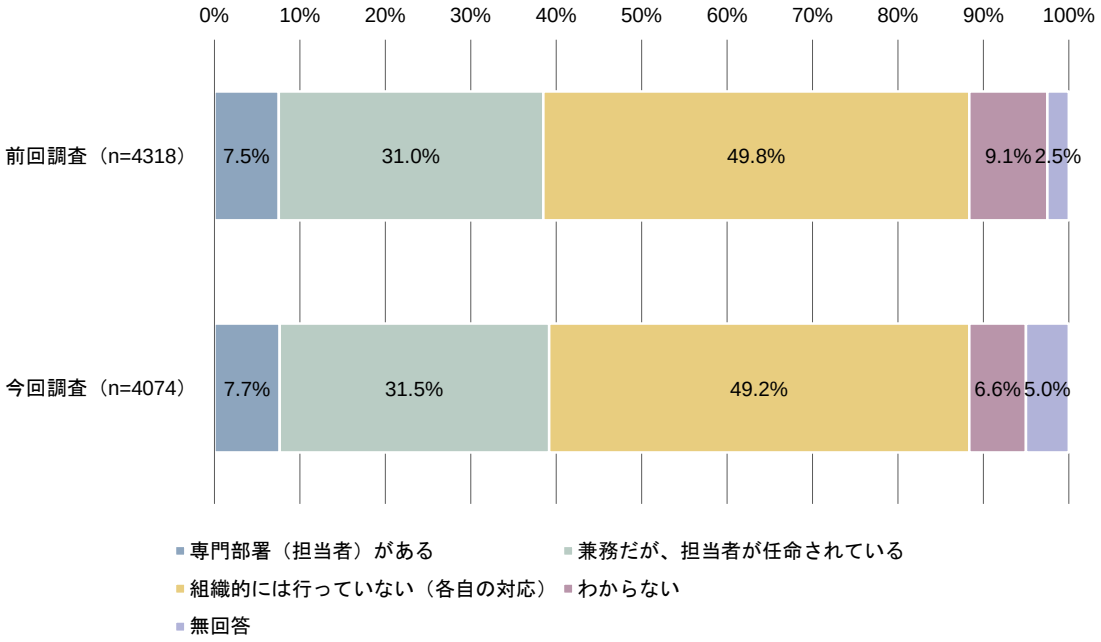


[4] 前回調査の設問設定が異なるので再集計

③組織体制

前回調査から組織体制に大きな変化はない。

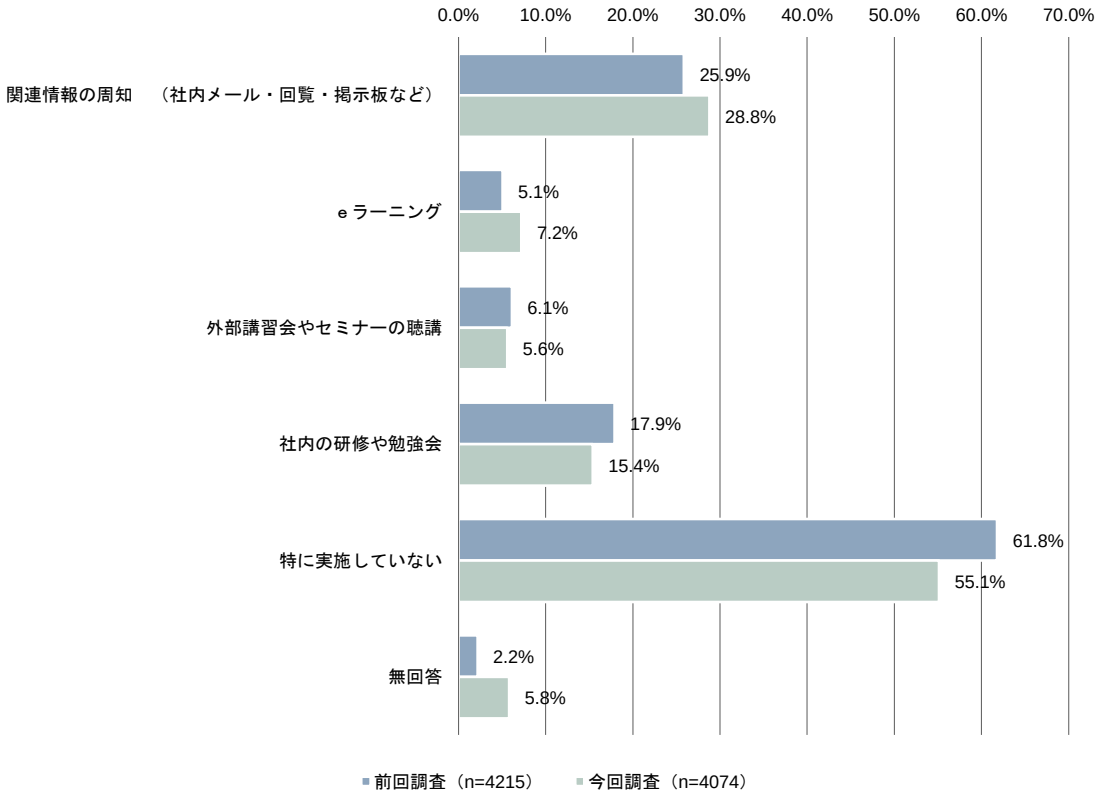
図表 2-129 組織体制（前回比較）（SA）



④従業員に対する情報セキュリティ教育の実施状況

前回調査に比べ、「関連情報の周知（社内メール・回覧・掲示板など）」の割合が若干増えており、「特に実施していない」の割合が61.8%から55.1%に減少した。

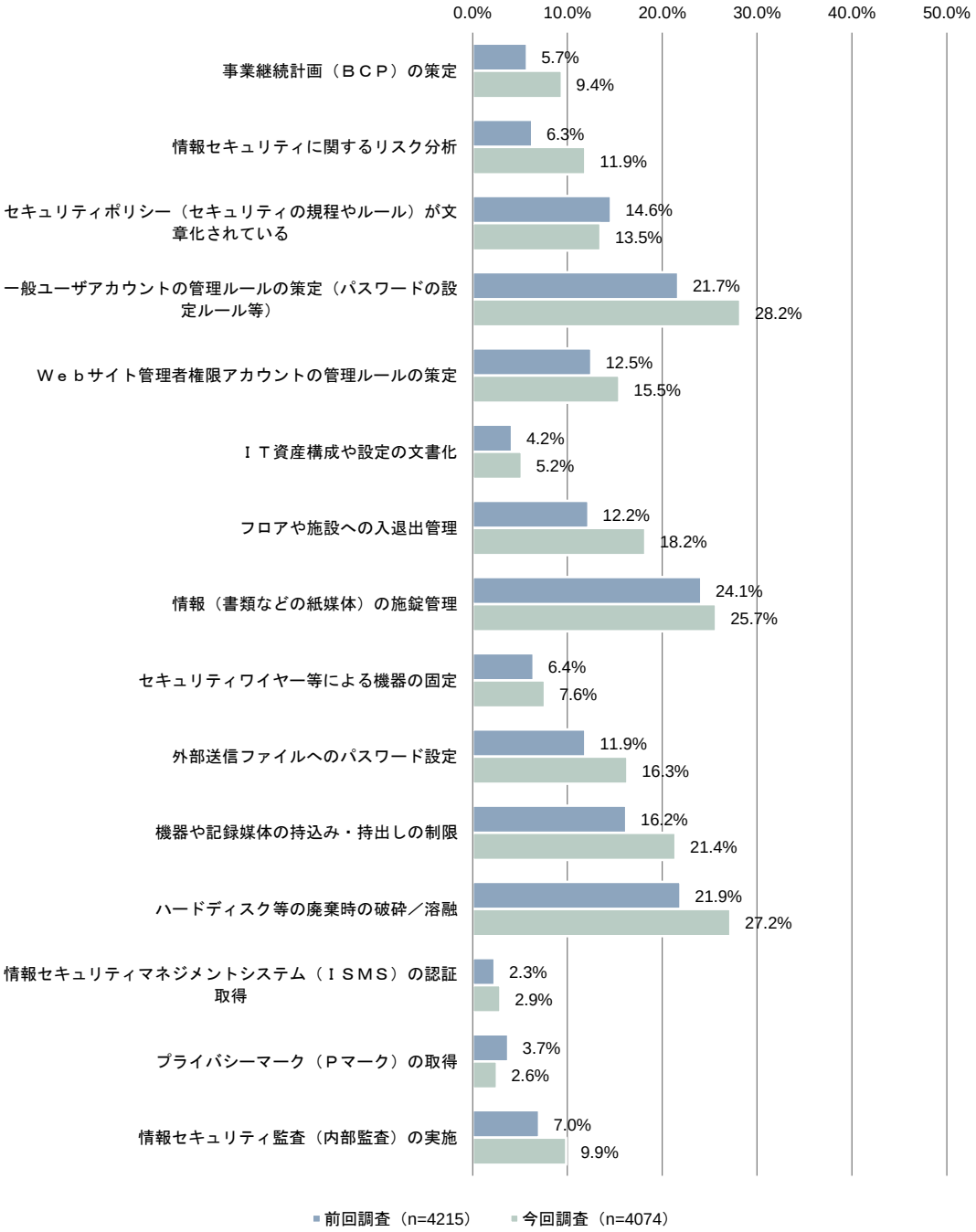
図表 2-130 従業員に対する情報セキュリティ教育の実施状況（前回比較）（MA）



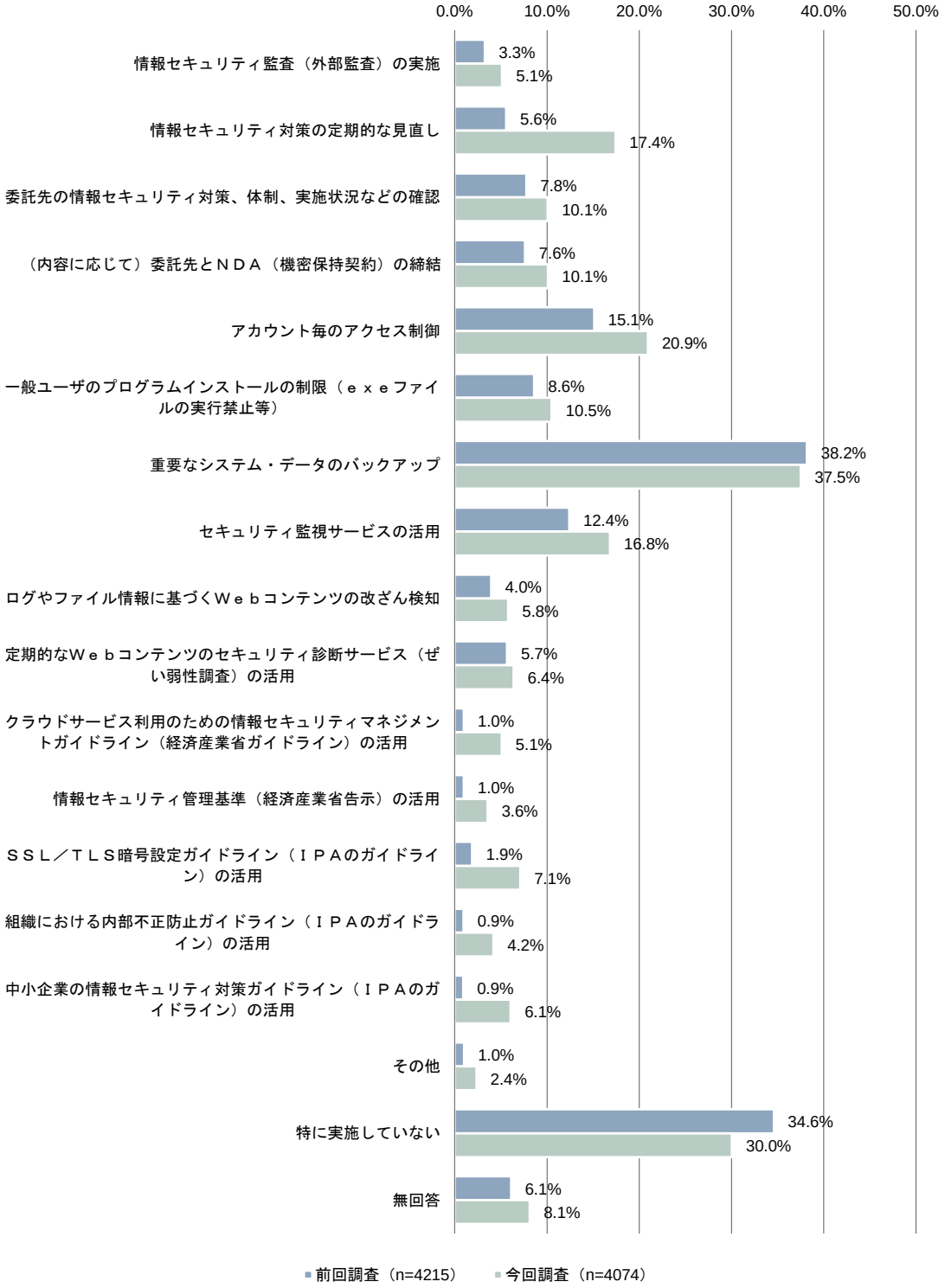
⑤被害防止のための組織面・運用面の対策

「セキュリティポリシー（セキュリティの規程やルール）が文章化されている」、「プライバシーマーク（Ｐマーク）の取得」、「重要なシステム・データのバックアップ」については、若干前回調査を下回っているものの、その他の項目では前回調査から割合が増加している。「情報セキュリティ対策の定期的な見直し」については10%以上増加している。

図表　2-131　被害防止のための組織面・運用面の対策①（前回比較）（MA）



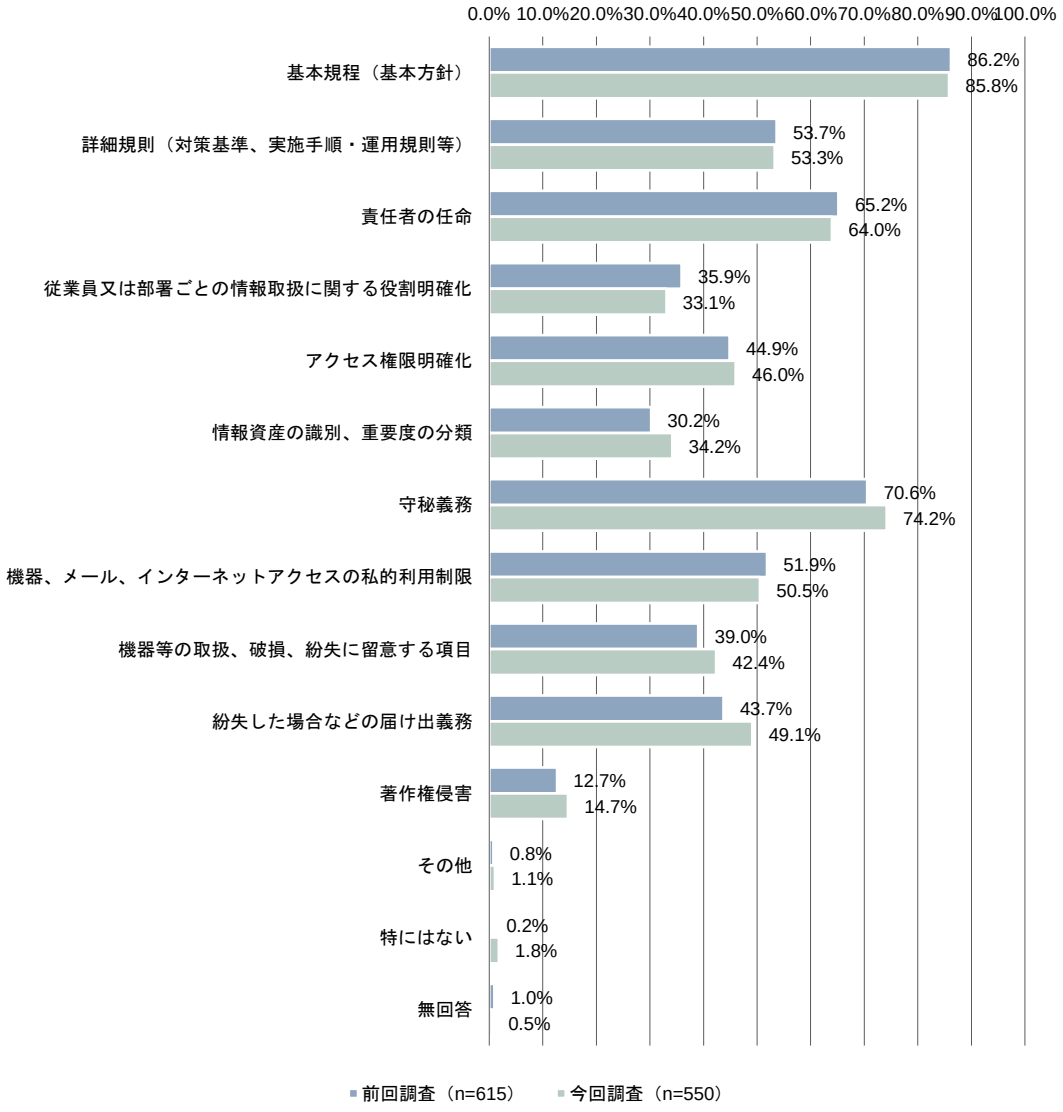
図表 2-132 被害防止のための組織面・運用面の対策②（前回比較）（MA）



⑥社内のセキュリティポリシー規定

選択肢によって多少の増減はあったものの、セキュリティポリシーに規定されている内容に大きな変化はない。

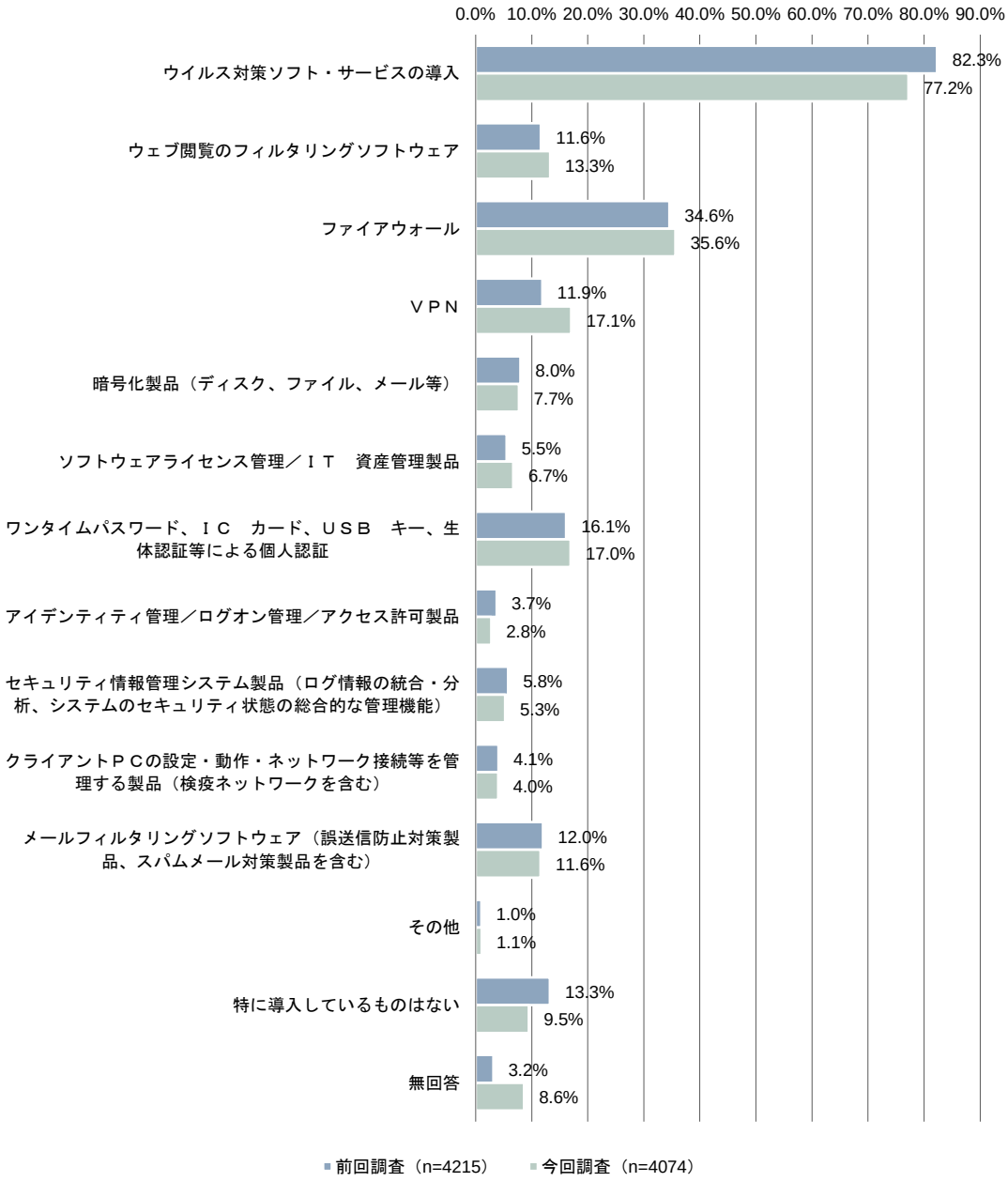
図表 2-133 社内のセキュリティポリシー規定（前回比較）（MA）



⑦情報セキュリティ関連製品やサービスの導入状況

「VPN」の導入が11.9%から17.1%に増加しているものの、その他の選択肢については前回調査と大きな差はない。

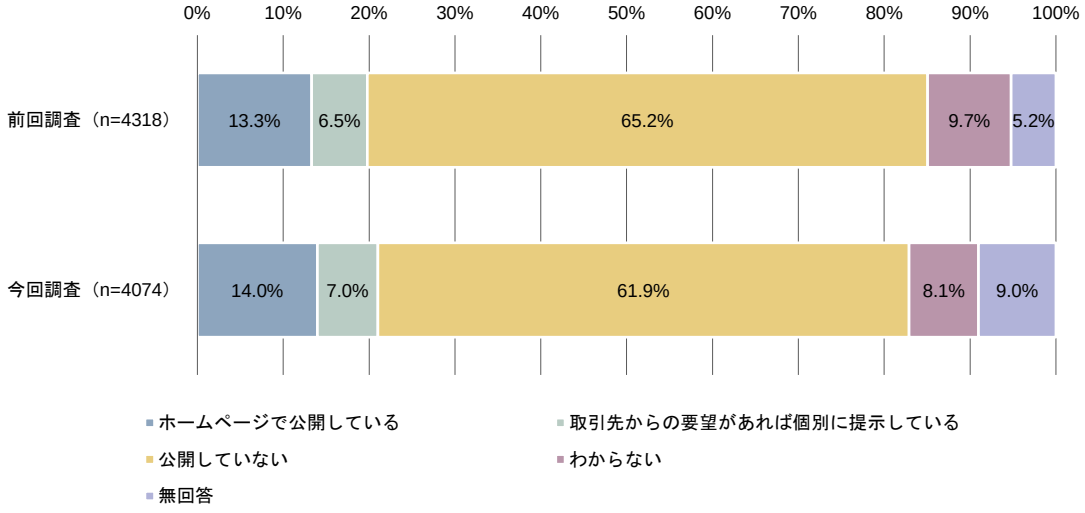
図表 2-134 情報セキュリティ関連製品やサービスの導入状況（前回比較）（MA）



⑧情報セキュリティ対策の実施内容についての外部への公開状況

前回調査と大きな差はない。

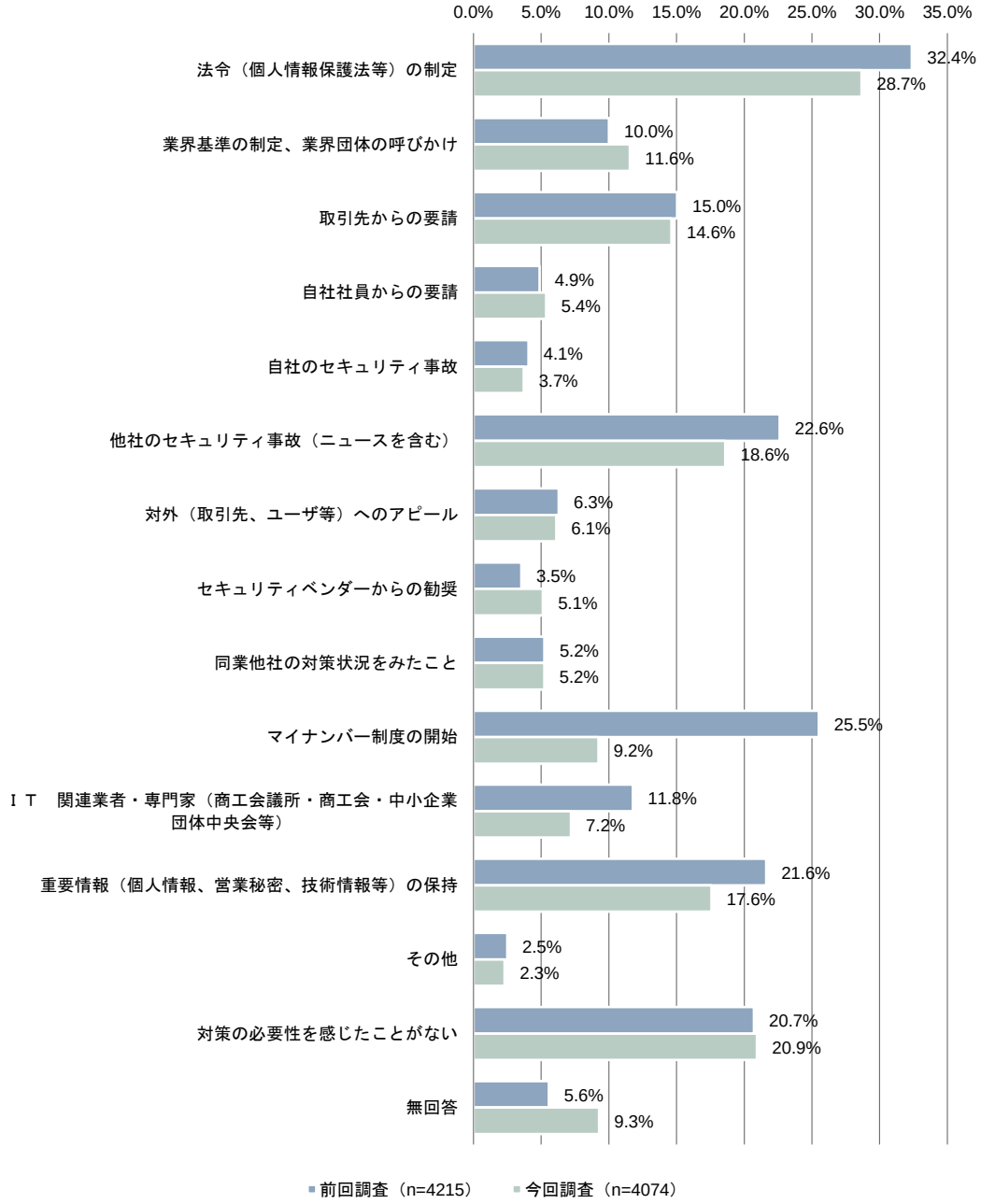
図表　2-135　情報セキュリティ対策の実施内容についての外部への公開状況（前回比較）（SA）



⑨情報セキュリティ対策の必要性を感じたきっかけ

「マイナンバー制度の開始」が25.5%から9.2%に減少している。また、他の選択肢についても減少しているものが多い。

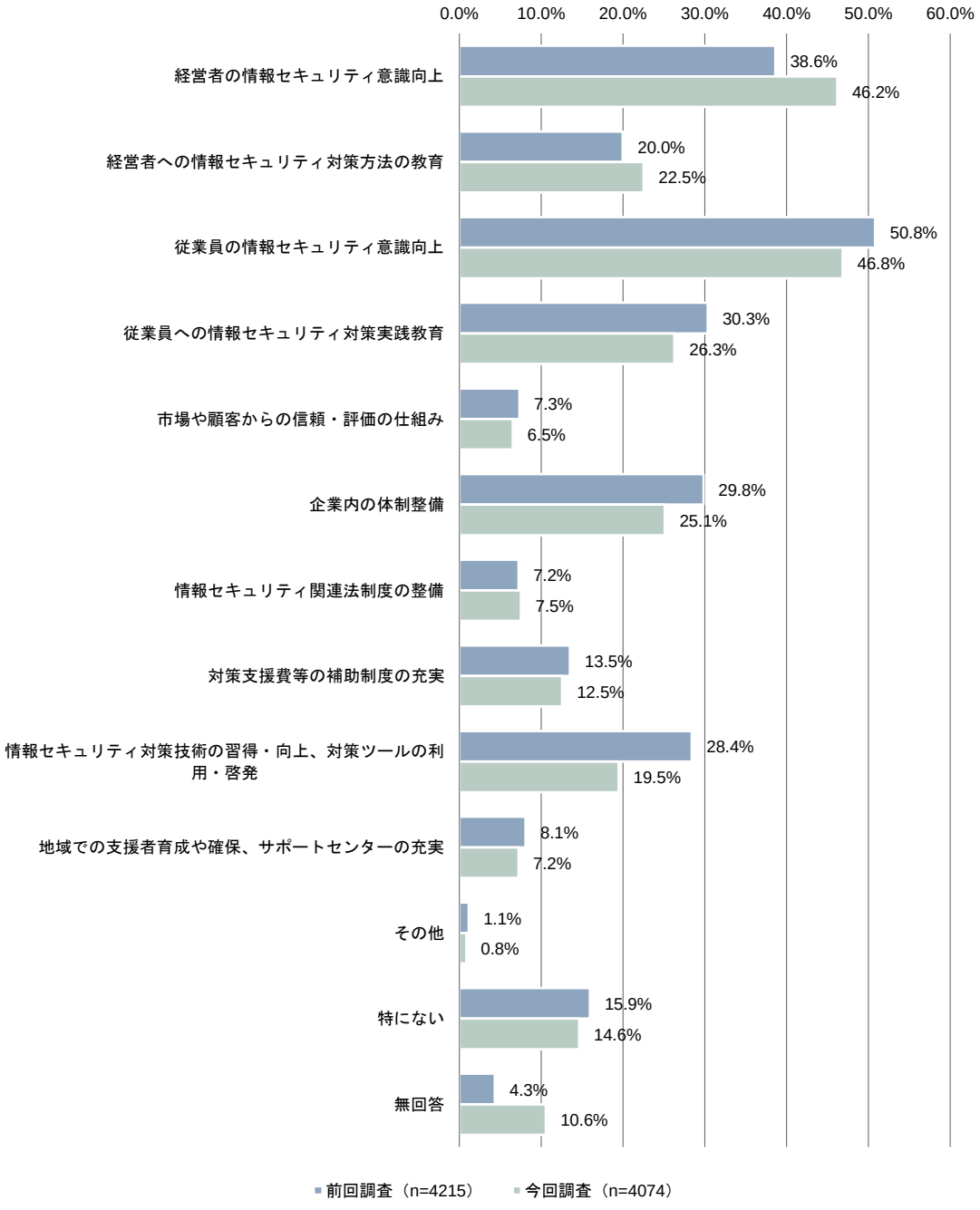
図表　2-136　情報セキュリティ対策の必要性を感じたきっかけ（前回比較）（MA）



⑩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

「経営者の情報セキュリティ意識向上」については、38.6%から46.2%に増加している。一方で、他の選択肢は前回と同程度か減少している。

図表　2-137　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（前回比較）（MA）



第３章　個別調査

１．調査概要

アンケート調査の有効回答数 4,074 件のうち、以下の観点を極力すべて満たすように対象企業をサンプリングした。調査にあたっては、コロナ禍の影響や先方の都合等にも配慮し、オンライン会議ツールを使用したウェブ会議、もしくは、電話での聞き取りのいずれかの方法により実施した。

図表 3-1　対象企業選定の観点

- 地域（経済産業省の各経済産業局が所管する地域ごとに一定数の事例が含まれること）
- アンケート調査の回答により、情報セキュリティに関する被害実態等があり、情報セキュリティ対策の実践により経営面を中心にプラスの効果を発揮している事例（下記、３つの観点から抽出）
  - 情報セキュリティに関する実施対策が多い・もしくは情報セキュリティ対策投資が多い事例
  - 情報セキュリティに関する被害実態等のある事例
  - サプライチェーン上での情報セキュリティ対策の要請の多い事例
- 業種・従業員（各業種分類において中小企業基本法で定義される「中小企業」と「小規模企業者」を従業員数の観点で極力それぞれ含むこと）

選定の結果、個別調査は、地域ブロック別に以下の企業数に対して実施した。

図表 3-2 地域ブロック別実施企業

地域ブロック	実施件数
北海道経済産業局	5
東北経済産業局	6
関東経済産業局	17
中部経済産業局	8
近畿経済産業局	10
中国経済産業局	5
四国経済産業局	5
九州経済産業局	6
内閣府沖縄総合事務局	2
合計	64

図表 3-3 業種別実施企業

業種	事例件数
農業・林業・漁業	2
建設業	8
製造業、鉱業・採石業・砂利採取業、電気・ガス・熱供給・水道業	8
情報通信業	9
運輸業・郵便業	1
卸売業	6
小売業	3
金融・保険業	10
不動産業・物品賃貸業	4
サービス業	13
合計	64

2．調査項目

個別調査は、以下の項目を中心に質問を行い、アンケート調査の回答内容の詳細やアンケート調査では把握の難しい実態や問題認識等を深掘りした。

図表 3-4 調査項目

- 情報セキュリティ対策の取り組みについて
- 情報セキュリティ対策による効果について
- 情報セキュリティ被害について
- 取引先との関連について
- その他

第４章　考察

１．ITの導入状況

- 中小企業を対象とした本調査で、業務用パソコン・タブレット端末・スマートフォンの利用があると回答している企業は 93.3%となっており、中小企業にとっても必須のツールとなっている（図表 2－18）。一方で、利用・導入しているサービスやシステムについて、利用率は相当にバラツキがあり、6割を超える利用率が確認されたのは「Web サイト、ホームページの開設（67.4%）」、「電子メール（独自ドメイン）（63.2%）」、「会計システム・アプリケーション（62.6%）」に限られる。テレワークやコロナ禍における非対面のコミュニケーションに有用な「オンライン会議システム（33.7%）」「コミュニケーションツール（24.9%）」は必ずしも中小企業全般に浸透しているとは言えない実態が改めて確認された（図表 2－19、図表 2－20）。この点、規模別にクロス集計をしても傾向は同じだが、特徴としてやはり規模の大きい中小企業ほど利用率が高い傾向が確認された他、「オンライン会議システム」「コミュニケーションツール」等については、特に規模の大きい中小企業での導入率が高い傾向が確認された（図表 2－91、図表 2－92）。
- 直近過去 3 期における IT 投資の状況について投資を行っていないと回答している中小企業が 30.0%（図表 2－21）、同じく直近過去 3 期の情報セキュリティ対策投資の状況について投資を行っていないと回答している中小企業が 33.1%となっている（図表 2－22）。情報セキュリティ対策投資を行わなかった理由としては、「必要性を感じていない」の割合が最も高く 40.5%となっている。次いで、「費用対効果が見えない（24.9%）」、「コストがかかり過ぎる（22.0%）」という結果となっている（図表 2－25）。一方、情報セキュリティに関する脅威認識について、例えばコンピュータウイルスについては、「非常に大きな脅威である（55.1%）」「どちらかといえば脅威である（26.6%）」と脅威と捉えている中小企業は 8 割を超えている（図表 2－52）。同様に不正アクセスについては、「非常に大きな脅威である（50.2%）」「どちらかといえば脅威である（26.3%）」と脅威と捉えている中小企業は 7 割を超えている（図表 2－53）。これらの結果から、情報セキュリティに関する脅威認識はあるものの、自社は情報セキュリティ被害にあわないと考えている中小企業や、必要性を感じつつも金銭的リソース配分の優先順位を高めるまでに至っていない中小企業が多いと考察される。
- スマートフォンやタブレット端末等、携帯の利便性が高い端末について、実施している対策を質問したところ、「端末のパスワード設定（62.6%）」や「セキュリティソフトの導入（44.0%）」といった技術的な対策が取られていることは多い傾向にある。一方で、「利用ルールの策定（アプリケーションの導入制限等（10.6%）」といった対策が取られている中小企業の割合は 1 割程度に留まっており、組織的な対策にまで至っていない中小企業が多いことが確認された（図表 2－27）。
- パソコンへの Windows Update などによるセキュリティパッチの適用状況については、「常に適用し、適用状況も把握している」の割合が最も高く 44.5%となっている。一方で、「各ユーザに適用を任せている（18.9%）」という回答も 2 割、「ほとんど適用していない（4.3%）」、「適用の仕方が分からない（2.3%）」「適用方針・適用情報ともにわからない（2.0%）」という回答も合わせて

１割となっている等、対応が 2 極化している（図表 2－26）。また、「セキュリティパッチの適用状況（外部に公開しているネットワークサーバ）」や「セキュリティパッチの適用状況（内部で利用しているローカルサーバ）」に関する設問への回答は、いずれも無回答であった中小企業が 4 割前後となっており、「ほぼすべてのサーバに適用している」という中小企業は前者の設問で 15.3%、後者の設問で 25.0%に留まっている（図表 2－30、図表 2－31）。傾向として、セキュリティパッチの必要性に対する理解が必ずしも浸透していないことを示唆する結果であった。

- サイバー保険や情報漏えい賠償責任保険に関する設問への回答は、いずれも「内容を知らないし、加入もしていない」の割合が最も多く４割となっている（図表 2－33、図表 2－34）。保険によるリスクファイナンスは、財務的なインパクトが発生した際の資金調達に関わる対応策の１つであるが、情報セキュリティ対策投資（リスク低減・回避）を行ったとしても効果が十分に期待できないリスクについて、保険（リスク移転）によるリスクヘッジを行うことの有効性自体の周知もまだ途上であると考えられる。

２．情報セキュリティに関する意識・状況

- 情報セキュリティに係る組織体制は、「組織的には行っていない（各自の対応）」の割合が最も高く 49.2%となっている（図表 2－35）。アンケート調査の回答企業の属性を見ると 4 割が 5 名以下の事業者である（図表 2－12）ことを考えれば、妥当な結果であると考えられる。また、困ったことがあった際の相談先が「特にない」と回答している中小企業が 21.3%となっている（図表 2－36）。社内に相談できる担当者を配置できていない場合でも、社外の IT 関連事業者を含めて相談できる先を持つことは、情報セキュリティ対策を行う上で重要であり、組織的な対応が出来ていない中小企業であっても身近に相談できる相手を持つことが望まれる。この点、企業規模別にクロス集計を行うと、相対的に規模の大きい中小企業では、組織的な体制を整備していない企業や、困ったことがあった際の相談先が無いと回答している割合が低いことが確認できる（図表 2－98、図表 2－99）
- 従業員に対する情報セキュリティ教育の実施状況について、5 割を超える中小企業が「特に実施していない」と回答している（図表 2－39）。この傾向は小規模企業者においてはより顕著で、63.2%が「特に実施していない」と回答している（図表 2－102）。一方で、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について質問したところ、「従業員の情報セキュリティ意識向上」をあげた割合が最も高く 46.8%となっている（図表 2－70）。情報セキュリティリスクを軽減する上で、従業員のリテラシー向上が重要となることに加え、リスク顕在化時には迅速な初動対応が被害の拡大・拡散を防ぐうえでも重要であることが知られている中、懸念が残る結果であった。また、情報漏えい等を発見した場合の報告先について、「報告先が決まっていない」と回答している中小企業が 22.7%存在していること（図表 2－40）や、情報漏えい等を発見した場合の対処方法について、「ネットワーク遮断」という基本動作を規定している企業が 40.7%に留まり、「対応方法は決まっていない」と回答している企業が 31.4%存在している（図表 2－41）ことも併せて

考えると、従業員の情報セキュリティ意識向上が必要であると認識しつつ、教育を実施できていないギャップを少しでも埋める支援や施策の必要性が示唆される。

- 活用したい情報セキュリティ対策に関するサービスについて質問したところ、いずれの選択肢についても一定のニーズが確認され、「業界ごとのセキュリティガイドライン（28.6%）」、「オンライン・電話での窓口相談サービス（27.9%）」、「中小企業向けセキュリティ対策に関する定期的な情報発信（27.0%）」等について、相対的にニーズが高い傾向が見られた（図表 2－37）。また、情報セキュリティに関する情報収集先は、「社外の IT 関連業者（45.6%）」、「インターネット（44.1%）」の比率が高くなっている（図表 2－38）。情報セキュリティに関するサービスや情報発信自体は、国や公的機関、業界団体、情報セキュリティや IT 関連事業者等から提供されているが、中小企業にその情報が届いていないことも少なくはない。中小企業に対する認知の向上にあたっては IT 関連事業者を通じた情報発信が有効であると同時に、インターネット上で閲覧可能な情報や各種コンテンツの充実と、その存在の認知を促していくことが必要である。
- 情報セキュリティ対策の必要性を感じたきっかけについて質問したところ、「法令（個人情報保護法等）の制定（28.7%）」をあげる中小企業が最も多かったが、その他、「他社のセキュリティ事故（ニュースを含む）（18.6%）」、「取引先からの要請（14.6%）」、「業界基準の制定、業界団体の呼びかけ（11.6%）」をあげる中小企業も相対的に多い傾向が確認出来た（図表 2－48）。このことはサプライチェーン全体で情報セキュリティ対策に取り組むことの有用性や、業界内での取り組みの有用性を示唆しており、引き続き業界団体を通じた情報発信や啓発が重要となると考えられる。
- 情報セキュリティ対策を実施して感じられたメリットについて質問したところ、「特になし」と回答した中小企業が 44.7%となっており、メリットを実感できていない中小企業が少なくないことが確認された（図表 2－50）。一方で、具体的なメリットを感じている中小企業も相当数存在しており、個別調査においても具体的なメリットがあったという声も聞いていることも事実である。特に、規模の大きい中小企業（101 人以上）においてはメリットがあったと回答する中小企業の比率が高い傾向にある（図表 2－106）。また、セキュリティ体制のある企業ほどメリットを実感している傾向がある（図表 2－123）。情報セキュリティ対策を実施するのには金銭的リソースや人的リソースの投入が必要となることは事実であるが、いずれのクロス集計の結果からも対策を実施している中小企業ほどメリットを感じているという傾向があることもうかがえることから、対策実施の必要性とメリットの両面について継続的に発信していくことが重要である。

3．情報セキュリティ被害の状況

- 2020 年度（2020 年４月～2021 年３月）における情報セキュリティ被害の有無を質問したところ、「被害にあっていない」という回答が 84.3%となっている。被害の認識があったものとしては、「コンピュータウイルスに感染（2.7%）」、「サイバー攻撃（DoS 攻撃・DDoS 攻撃、不正アクセス、標的型攻撃など）（1.8%）」をあげる中小企業が相対的に多いことが明らかとなった（図表２－

71）。本調査の回答企業の属性として、経営者が 47.3%、役員が 21.9%となっていること（図表 2－11）、社員の私有端末の業務利用（BYOD）を認めている中小企業が 36.5%となっていること（図表 2－28）、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について「報告先は決まっていない」としている中小企業が 22.7%となっていること（図表 2－40）等を併せて考えると、軽微な被害であれば、中小企業が認識できていないケースも相当数存在している可能性はあると考えられる。なお、被害認識のあった中小企業に対して、情報セキュリティ被害で生じた被害額を質問しているが、「1 万円未満」と回答した中小企業が 46.1%と最も多い結果となっている。しかし、同設問の回答も「無回答」が 35.4%と高い比率となっており（図表 2－78）、被害を受けた事実を認識出来ていても、その影響の程度や損害の程度まで把握できていない中小企業も少なくないものと考えられる。

- 被害を認識している中小企業に対して、感染あるいは発見したコンピュータウイルスの想定される侵入経路を質問したところ、「電子メール（62.2%）」、「インターネット接続（ホームページ閲覧など）（45.9%）」、「自らダウンロードしたファイル（23.4%）」等をあげる中小企業が多かった（図表 2－72）。基本的な対策の実施・徹底が有効であることの重要性を示唆している。
- また、被害を認識している中小企業に具体的な被害の内容を質問したところ、コンピュータウイルスに感染した影響で生じた被害については、「パソコン単体の停止」という回答が 31.5%と高い結果であったが、「ウイルスメール等の発信（25.2%）」、「データの破壊（23.4%）」等、組織全体や取引先への影響も懸念される項目についても高い比率の回答があった（図表 2－73）。コンピュータウイルスに感染した影響で、取引先に影響が及んだ内容については、「サービスの障害、遅延、停止による逸失利益（18.9%）」、「原因調査・復旧にかかわる人件費等の経費負担（17.1%）」等を上げる中小企業が多く（図表2－74）、中小企業に対する情報セキュリティの意識啓発に際しては、こうした被害事例が相当程度存在することも発信することも有用であると考えられる。

４．取引先を含む情報セキュリティ対策

- 本調査ではサプライチェーンにおける情報セキュリティの重要性に鑑みて、関連する質問を行った。販売先・仕入先との契約締結時における情報セキュリティに関する条項・取引上の義務・要請の有無について質問したところ、「義務・要請がある」と回答したのは 26.1%となっている（図表 2－80）。この点、サプライチェーンの川上に位置する企業よりも、川下に位置する企業の方が「義務・要請がある」と認識している比率が高いことも確認された（図表 2－125）。
- 「義務・要請がある」と回答した中小企業にその内容を質問したところ、販売先(発注元企業)との契約時の要請としては、93.8%の中小企業が「秘密保持」が明確に義務付けられていると回答している。その他、「契約終了後の情報資産の扱い（返却、消去、廃棄等）（36.3%）」、「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（32.4%）」等をあげる中小企業も多い結果となった（図表 2－81）。仕入先(委託・協力企業) との契約時の要請としても、94%の中小

企業が「秘密保持」が明確に義務付けられていると回答している他、「契約終了後の情報資産の扱い（返却、消去、廃棄等）（34.1%）」、「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（30.7%）」をあげる中小企業が多いという結果であった（図表 2－82）。取引先に対して契約上の秘密保持義務を要請することが定着してきており、中小企業においても契約上の義務を履行するために情報セキュリティ対策を実施する必要性が高まっていると考えられる。

- 情報セキュリティ対策の要請に対して、対策を実施する際の費用の負担や人材の確保等の面で課題があると認識している企業も少なくない（図表 2－83）。また、要請に対応するために追加的な費用の負担が発生する場合であっても、「全額自社で負担している」と回答している企業が45.0%で最も高い比率となっている（図表 2－84）。基本的な情報セキュリティ対策は中小企業であっても必要であるが、情報セキュリティ対策投資を行わなかった理由として、「必要性を感じていない」の割合が最も高く 40.5%となっており、次いで、「費用対効果が見えない（24.9%）」、「コストがかかり過ぎる（22.0%）」という結果となっている（図表 2－25）事実も念頭に置く必要がある。特定の業界や特殊な業務の発注にあたり一般的な中小企業にとって高度な情報セキュリティを求める場面や、サプライチェーン全体としての情報セキュリティを高めなければならない場面において、情報セキュリティの必要性を訴えたり、取引上の立場を利用して要請をしたりするだけでは、十分な対策とはならない可能性がある。

５．調査結果を踏まえた示唆、課題の整理

①前回調査との比較から得られる示唆

- IT投資額やセキュリティ対策投資額について、2016年度に実施した前回調査において、過去3年間でのIT分野の投資を「行っていない」と回答した企業は47.3%[5]となっていた。この点、今回の調査においては、直近過去3期におけるIT投資額について、「投資していない」と回答した企業は30.0%となっている（図表２－127）。前回調査と比較して、IT投資を行っていない企業の割合が17.3%の改善と考えることができ、ITの導入・活用が中小企業においても一定程度、進んでいる様子がうかがえる。
- 一方で、情報セキュリティ対策を推進する組織体制に着目すると、前回調査の結果と比較して、大きな変化はみられない。「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」との回答が、前回調査ではあわせて38.5%であり、今回の調査においては、あわせて39.2%となっている（図表２－129）。IT投資を行う企業は増加傾向にあるものの、情報セキュリティ対策を推進する担当者を配置するといった組織体制の整備については、あまり進んでいないと見られる。前回調査以降も、中小企業における人手不足は依然として続いており、情報セキュリティ対策を推進する担当者を任命するまで手が回らない状況であった可能性も推察される[6]。
- 情報セキュリティ教育の実施状況については、前回調査と比較して「特に実施していない」企業の割合が6.7%減少したものの、55.1%と依然高い状況にある（図表２－130）。しかし、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について、前回調査と同様に、「従業員の情報セキュリティ意識向上」と「経営者の情報セキュリティ意識向上」を挙げた企業が多い（図表２－135）。この点、個別調査において、同様の問題意識をもつ企業がIPAの提供するコンテンツを活用した情報セキュリティ教育・意識啓発を実施している事例が複数確認されている。今後、事例集等の他社の取り組みも参考にして、情報セキュリティ教育・意識啓発のさらなる実施が望まれる。
- 上述の通り、情報セキュリティ対策を実施する組織体制に大きな変化はみられなかったものの、被害防止のための組織面・運用面の対策実施状況については、多くの項目で増加傾向にある。特に、「情報セキュリティ体制の定期的な見直し」については、実施している企業が、前回調査と比較して10%以上増加している（図表2－131，図表2－132）。しかし、前回調査と比較して大きく増加した項目は少なく、今後、さらなる対策の実施が望まれる。
- 「情報セキュリティ対策」の必要性を感じたきっかけについて、前回調査と比較して微減傾向にある項目が多い（図表２-136）。大きな変化のあった項目として、「マイナンバー制度の開始」があり、前回調査は25.5%だったのに対し、今回の調査では9.2%にまで下落している。これは、

[5] 前回調査の設問設定が異なるため再集計

[6] 中小企業庁 「2020年度版 小規模企業白書（HTML版）」
https://www.chusho.meti.go.jp/pamflet/hakusyo/2020/shokibo/b1_1_3.html

前回調査が、マイナンバー制度が開始された2016年に実施された影響もあると考えられる。しかし、「マイナンバー制度の開始」以外の項目に大きな変化がないことは、大きな社会情勢の変化があれば、中小企業に情報セキュリティ対策の必要性を感じてもらうことができるものの、そうではない場合、その必要性を感じてもらうことは難しい、ということも考えられる。そうした中、前回調査と比較して増加した項目の中に、「業界基準の制定・呼びかけ」も含まれていることは注目される。今後、国や公的機関から中小企業に対する情報セキュリティ対策水準の向上に向けた施策の継続的な実施という「公助」に加え、業界団体や地域社会による「共助」の取り組みが増加することによって、中小企業が情報セキュリティ対策の必要性を感じ、対策水準を向上していくことが望まれる。

②情報セキュリティに係る普及啓発

- 情報セキュリティリスクは、中小企業にとっても見過ごすことのできない経営リスクであり、本報告書の冒頭の「背景・目的」にも記載した通り、サプライチェーンの関係性を悪用した攻撃はサプライチェーンを構成するすべての企業において重大なリスクである。
- 中小企業が情報セキュリティ対策に取り組むためには、まず「リスク認識」が必要である。経営資源が乏しい中小企業の場合、情報セキュリティリスクに限らず、あらゆるリスクについて、幅広く予防的対策を講じることは出来ない。そのため、経営上の影響度の高いリスクから優先的に取り組まざるを得ないため、まずは情報セキュリティ上の被害のリスクについて、正しく認識をすることが重要となる。本調査の結果から、コンピュータウイルスや不正アクセスを脅威として認識している中小企業の比較的多いことが確認できた（図表2-52から図表2-60）。
- 上記のような脅威の認識が、情報セキュリティ対策につながっているかというと、本調査の結果を見る限り、具体的な情報セキュリティ対策の実施に結びつかないケースが多いことが明らかである。また、「重要情報を保有していない」、「必要性を感じていない」という認識を持っている中小企業が少なくない傾向がある（図表2-49）。業種や事業内容によって、保有する情報の内容や量には当然差異があるものの、取引先の情報や顧客の情報（個人情報を含む）については多かれ少なかれ、保有せざるを得ず、中小企業であっても事業を営む上で、こうした情報を適正に管理し、情報漏えいを防ぐことは取引における信頼の基盤である。また、多くの中小企業が脅威として認識しているコンピュータウイルスや不正アクセスは、単に情報漏えいの原因となるだけでなく、業務・操業の一時停止等の原因にもなりうる。そのため、「重要情報を保有していない」、「必要性を感じていない」という回答をしている中小企業の中には、脅威を認識しつつも、自社への影響を評価出来ていない中小企業や、脅威を正しく認識できていない中小企業も多く含まれている可能性が高い[7]。

[7] 独立行政法人情報処理推進機構が2021年12月に公表した『【レポート】中小企業従業員アンケート』においても、「かくれサイバートラブル」が相当数発生している可能性があることが指摘されている。
https://www.ipa.go.jp/security/otasuketai-pr/assets/pdf/enq20211208.pdf?v=202202

情報セキュリティ対策を十分に実施していない中小企業の比率	主な要因
直近過去３期の情報セキュリティ対策投資額（図表2－22） 「投資していない」＝33.1% 「1百万円未満」＝49.2%	情報セキュリティ対策投資を行わなかった理由（図表2－25） 「必要性を感じていない」＝40.5% 「費用対効果が見えない」＝24.9% 「コストがかかりすぎる」＝22.0% 「どこからどう始めたらよいかわからない」＝20.7%
従業員に対する情報セキュリティ教育の実施状況（図表2－39） 「特に実施していない」＝55.1%	情報セキュリティ対策の必要性を感じない理由（図表2－49） 「重要情報を保有していないため」＝68.8% 「情報セキュリティ被害にあうと思わないため」＝28.0%
被害防止のための組織面・運用面の対策（図表2－43、2－44） 「特に実施していない」＝30.0%	

- こうした調査結果及び考察を踏まえると、今後の普及啓発に係る力点として、どのような業態や規模の企業であっても個人情報の漏えいや営業情報の漏えい、サイバー攻撃を受ける、といった事態が発生すれば、取引先や顧客の信頼を失ったり、業務が一部停止したりするリスクがあることについて、強調した発信を検討する余地があるものと思われる。
- この点については、発信した情報を、中小企業が自分のこととして受け止め、「気づき」を得る必要があることから、キャッチコピーやチラシ・ポスターのような伝達手段では限界がある。また、情報セキュリティ対策投資を行っていない者の回答として、「費用対効果が見えない（24.9%）」、「コストがかかりすぎる（22.0%）」、「どこからどう始めたらよいかわからない（20.7%）」といった回答が目立つことからも、必ずしも情報セキュリティの専門家でなくても、相談相手がいれば取り組みにより着手しやすくなる可能性はある。
- この点、IPAでは既に中小企業支援機関や業界団体との連携を進めているが、より連携を深化させる観点から、中小企業支援機関や業界団体への発信機会を増やすことや、協働機会を増やすことも検討に値する。その際、中小企業支援機関や業界団体の職員が中小企業とコミュニケーションをする際に活用可能なツールを提供することや、中小企業支援機関や業界団体が行う情報発信の機会にIPAからも情報発信を行ったり、セミナーや相談会等を協働して開催したりするといったことも検討に値する。

③サプライチェーンを意識した情報セキュリティ対策

- 本調査では、サプライチェーンに着目した調査も行った。情報セキュリティ対策の必要性を感じたき

っかけとして、「業界基準の制定、業界団体の呼びかけ（11.6%）」をあげる中小企業が一定数存在することから、業界内における意識が高まっているケースも増えているものと考えられる。また、販売先・仕入先との契約締結時における情報セキュリティに関する条項・取引上の義務・要請の有無について質問したところ、「義務・要請がある」と回答したのは26.1%となっている（図表2－80）。「義務・要請がある」と回答した中小企業にその内容を質問したところ、販売先(発注元企業)との契約時の要請としては、93.8%の中小企業が「秘密保持」が明確に義務付けられていると回答している。その他、「契約終了後の情報資産の扱い（返却、消去、廃棄等）（36.3%）」、「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（32.4%）」等をあげる中小企業も多い結果となった（図表2－81）。

- 契約上、情報セキュリティに関する義務・要請があれば何らかの対応が必要となり、サプライチェーン全体の情報セキュリティ水準の向上に資する一方、取引上の立場を利用して過度な対応を求めることは公正取引の観点からの懸念を生じさせる可能性もあり、バランスが求められる。現状、契約上の義務・要請について、その内容の大半が、秘密保持義務となっている。秘密保持義務を負わせることは、結果責任のみを求めており、その結果を実現するための手段、つまりどのような情報セキュリティ対策を講じるかについては義務を負う者に委ねることになる。実施を促したい情報セキュリティ対策がある場合には、契約書にその内容を明記するか、契約の外で「要請」「お願い」という形で依頼をするしかないが、現実的には、そうした条件を依頼できるのは取引上において優位な立場にある者であることが多いため、公正取引の観点にも留意が必要となる。
- 業界によっては、既に業界独自のガイドラインを設けているケースもあり、発注側にとっても、受注側にとっても１つの目安となっている。業界内でコンセンサスがとれたガイドラインが存在するのであれば、こうしたガイドラインに準拠することを契約書に求めることも可能であり、両当事者が安心して情報セキュリティ対策を実施するのに資するものと考えられる。業界独自のガイドラインは、民間事業者や業界団体の積極的な活動に委ねられることとなるが、業界団体等の組織の規模や推進するセキュリティ人材の有無には差があり、自発的な取り組みを直ちに進めていくことが容易ではない業界も存在することから、SC3の活動において、ガイドラインの策定を支援するような取り組みが期待される。また、経済産業省やIPA等が主導する形で、特に大企業が懸念する不公正な取引にならない形での情報セキュリティ強化の要請に係るガイドライン等を作成することが出来れば、業界内での検討を後押しすることにもつながるものと期待される。
- 業界独自のガイドラインを策定する際、ガイドラインの遵守を前提としたマネジメントシステムの導入・実践を促すことが出来れば、より効果的に情報セキュリティ対策の実施を促すことが出来る。高度な情報セキュリティ対策が求められてきた業界であれば、ISMSやPマークの取得を促すという方法もあるかもしれないが、一般論として、業界で広くこれをスタンダードに出来る業界は限られていると考えられる。現在、中小企業も含めた情報セキュリティ対策の普及を目指し「SECURITY ACTION」の取り組みも開始されているため、必要最低限の対応として「SECURITY ACTION」で言及されている対策の実施を求めるよう、各業界が策定するガイドラインに盛り込むことを促すといった対応も考えられる。

- 一方で、「SECURITY ACTION」の1つ星の宣言を実施している企業は、2.6%にとどまる結果となった（図表2-51）。今後、他の認証制度も参考としつつ、「企業に対して求めるセキュリティ対策の水準」、「宣言内容の確実な実施の促し方」、「宣言企業へのインセンティブの内容・程度」、「自己宣言の是非」、といった点について、検討・改善を行うことが求められる。

参考資料（アンケート調査票）

2021 年度 中小企業における情報セキュリティ対策の実態調査(アンケート調査)

アンケートの回答手順

①アンケート回答用ウェブサイトに接続してください。

URL か QR コードからアクセス

- 以下の URL か右記の QR コードからアクセスしてください。
  https://rsch.jp/eqt4/?sme2021
- 同封されている紙の調査票は設問や選択肢を事前に確認していただくための参考資料です。この紙の調査票を返送していただくことはできません。
- ウェブ回答が難しい場合は、電子データ(Word 形式)をお送りしますので、回答記入の上ご返信ください。

https://rsch.jp/eqt4/?sme2021

②表示された質問事項にご回答ください。

- 質問事項は同封されている紙の調査票と同じです。
- ご回答は 2021 年 12 月 10 日(金)までにお願いいたします。

（調査の趣旨に関するお問い合わせ）
独立行政法人 情報処理推進機構
セキュリティセンター 企画部 中小企業支援グループ
担当：白川、鈴木、佐藤(み)
Email: isec-renkei@ipa.go.jp
※お問い合わせは、電子メールにてお願いいたします。
【参考】「2021 年度中小企業における情報セキュリティ対策の実態調査」について
https://www.ipa.go.jp/security/fy28/reports/isec-survey/sme2021.html

（調査の内容・回答方法に関する連絡先）
三菱 UFJ ﾘｻｰﾁ&ｺﾝｻﾙﾃｨﾝｸﾞ 株式会社
担当：青木、山田、柴田、山本
Email: sec@murc.jp
※新型コロナウイルスの影響にともない、電子メールでのお問い合わせにご協力を頂けますと幸いです。
TEL ：03-6733-3400
※お問い合わせ電話の受付時間
月～金曜日 10:30～12:00、13:00～16:30
（祝日は除きます）

貴社名	
役職・お名前	
郵便番号	
E-mail	@
お電話番号	（ ）

2021 年度 中小企業における情報セキュリティ対策の実態調査票

◎独立行政法人情報処理推進機構（以下、IPA）では、中小企業における情報セキュリティ対策への取り組みや被害の状況、対策実施における課題等を捉えることを目的としたアンケートを実施しております。今回の調査結果は、2022 年 3 月以降、IPA のホームページにて公開する予定です。

◎ご回答の内容については、すべて統計数値として集計いたしますので、会社名や個人名、個別のご回答内容などが公表されることは一切ございません。

◎本調査は、IPA より委託を受け、三菱 UFJ リサーチ&コンサルティング株式会社が実施しております。なお、アンケート回答用のウェブページにつきましては、同社からの再委託のもと、株式会社クロス・マーケティングが提供するアンケートシステムを利用いたします。

◎IT をほとんど利用していないという企業も、今回の調査の対象となっております。IT の依存度、セキュリティ対策、被害の実態を広く捉え、統計的に有意な結果を得るために、ご回答へのご協力を何卒よろしくお願い申し上げます。

◎回答期限は、2021 年 12 月 10 日（金）まで、とさせて頂きます。

◎原則、貴社の経営層（経営者、役員）の方がご回答ください。質問によっては、貴社の IT や情報セキュリティの担当者等、より詳しい方が回答して頂いても構いません。

◎より詳細に情報セキュリティ対策へのお取り組みや被害の状況、対策実施における課題等を捉え、企業の皆様の情報セキュリティ対策に資する調査報告書や、企業様の取組事例集を作成するため、一部の企業様には追加的なインタビュー調査のお願いをさせて頂く場合があります。インタビュー調査の依頼については、アンケートシステムを提供する株式会社クロス・マーケティングより実施させて頂きます。インタビュー調査にてお聞かせ頂いた実態やご意見についても、調査報告書や事例集として取りまとめ、今後の対策実施に向けた基礎資料として活用させて頂きます。

◎本アンケート調査は、株式会社クロス・マーケティングのアンケートシステムを用いて回答結果の収集を行います。冊子の表紙に記載の URL・QR コードよりアンケートサイトにアクセスいただき、ご回答をお願いいたします。次ページ以降に、お伺いさせて頂きたい調査項目を記載しております。同封しております用語集とともに、アンケートシステムへの入力の際に参照頂けますと幸いです。

◎なお、アンケートシステムによる回答が難しい場合には、アンケート調査票の電子データ版（Word 形式）を、アンケート用ウェブサイトＵＲＬからダウンロード頂くか、次のメールアドレス（sec@murc.jp）まで御連絡を頂ければ、電子データ版（Word 形式）をお送り致します。電子データ版のアンケート調査票に回答を頂いた場合、添付ファイルの形式で、調査担当のメールアドレス宛（sec@murc.jp）にお送りください。

1．貴社の概要についてお尋ねします。

問1-1 貴社の主な業種をお答えください。（最も当てはまるものに１つだけ☑）

□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

問1-2 貴社の所在地（本社所在地）を教えてください。（当てはまるものに１つだけ☑）

□1. 北海道	□2. 青森県	□3. 岩手県	□4. 宮城県	□5. 秋田県	□6. 山形県	□7. 福島県	□8. 茨城県
□9. 栃木県	□10. 群馬県	□11. 埼玉県	□12. 千葉県	□13. 東京都	□14. 神奈川県	□15. 新潟県	□16. 富山県
□17. 石川県	□18. 福井県	□19. 山梨県	□20. 長野県	□21. 岐阜県	□22. 静岡県	□23. 愛知県	□24. 三重県
□25. 滋賀県	□26. 京都府	□27. 大阪府	□28. 兵庫県	□29. 奈良県	□30. 和歌山県	□31. 鳥取県	□32. 島根県
□33. 岡山県	□34. 広島県	□35. 山口県	□36. 徳島県	□37. 香川県	□38. 愛媛県	□39. 高知県	□40. 福岡県
□41. 佐賀県	□42. 長崎県	□43. 熊本県	□44. 大分県	□45. 宮崎県	□46. 鹿児島県	□47. 沖縄県	

問1-3 あなたの主な役職・担当を教えてください。（最も当てはまるものに１つだけ☑）

□ 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）

問1-4 貴社の総従業員数について、2020 年度（2020 年 4 月～2021 年 3 月）の人数を教えてください。
（当てはまるものに１つだけ☑）
※常時従業者の総数をお答えください。また、常時従業者数は有給役員及び常時雇用者（正社員・正職員、準社員・準職員、アルバイト等、１ヶ月を超える雇用契約者）の合計とし、人材派遣業者からの派遣従業者は含めません。

□ 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

問1-5 貴社の資本金について、直近会計年度の金額を教えてください。（当てはまるものに１つだけ☑）

□ 1. 1,000 万円以下	□ 2. 1,000 万円超～3,000 万円以下	□ 3. 3,000 万円超～5,000 万円以下
□ 4. 5,000 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		

問1-6 貴社の総売上高（単体）について、直近会計年度の金額を教えてください。（当てはまるものに１つだけ☑）

□ 1. 1,000 万円以下	□ 2. 1,000 万円超～3,000 万円以下	□ 3. 3,000 万円超～5,000 万円以下
□ 4. 5,000 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		

問1-7 貴社が業務を受注する際、どのお立場での取引が多いですか。（最も当てはまるものに１つだけ☑）

□ 1. 元請・一次請けとして受注
□ 2. 二次請けとして受注
□ 3. 三次請け・それ以降として受注
□ 4. 委託元として発注
□ 5. 把握していない・不明

（例） 委託元→ 下請事業者 A→（元請・一次） 下請事業者 B→（二次） 下請事業者 C（三次）

問1-8 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。また、加入している場合、加入している団体名をすべてご記入ください。
（当てはまるものに１つだけ☑）

□ 1. はい【加入団体名： 】
□ 2. いいえ
□ 3. わからない

2. 貴社の IT の導入状況についてお尋ねします。

問2-1 貴社において、業務で業務用パソコン・業務用タブレット端末・業務用スマートフォンを利用していますか。（当てはまるものに１つだけ☑）

□ 1. はい
□ 2. いいえ　**→p.5 の問 3-1 へお進みください。**

問2-2 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。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。（当てはまるものすべてに☑）

□ 1. 電子メール(フリーメール・汎用ドメインなど)
□ 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（インターネットに接続されたセンサー、電子機器等）
□ 20. その他
（具体的に【　　】）
□ 21. 特に活用していない

問2-3 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の概算について教えてください。（次の【a】【b】それぞれの項目について、当てはまるものに１つだけ☑）

【a】 IT 投資額	【b】 情報セキュリティ投資額
□ 1. 投資していない	□ 1. 投資していない　**→問 2-5 へお進みください**
□ 2. １百万円未満　□ 3. １百万円~５百万円未満	□ 2. １百万円未満　□ 3. １百万円~５百万円未満
□ 4. ５百万円~１千万円未満　□ 5. １千万円~２千万円未満	□ 4. ５百万円~１千万円未満　□ 5. １千万円~２千万円未満
□ 6. ２千万円~５千万円未満　□ 7. ５千万円~１億円未満	□ 6. ２千万円~５千万円未満　□ 7. ５千万円~１億円未満
□ 8. １億円~４億円未満　□ 9. ４億円以上	□ 8. １億円~４億円未満　□ 9. ４億円以上
□ 10. わからない	□ 10. わからない

問2-4 貴社における、過去１期の IT 投資額、情報セキュリティ対策投資額の概算について教えてください。

IT 投資額	情報セキュリティ投資額
【　　】円	【　　】円

問2-5 【問 2-3「情報セキュリティ投資額」で「1」と回答された方】にのみお伺いします。
情報セキュリティ対策投資を行わなかった理由について教えてください。（当てはまるものすべてに☑）

□ 1. コストがかかり過ぎる
□ 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. その他
（具体的に【　　】）
□ 6. 必要性を感じていない

問2-6 貴社では、業務で使用するパソコンへの Windows Update などによるセキュリティパッチの適用をどのように実施していますか。（最も当てはまるものに１つだけ☑）

□ 1. 常に適用し、適用状況も把握している
□ 2. 常に適用する方針・設定だが、実際の適用状況は不明
□ 3. 各ユーザに適用を任せている
□ 4. ほとんど適用していない
□ 5. 適用の仕方がわからない
□ 6. 適用方針・適用情報ともにわからない
□ 7. 業務でパソコンは利用していない

問2-7 業務で利用されているスマートフォンやタブレット端末について、実施されている対策について教えてください。（当てはまるものすべてに☑）

□1. 端末のパスワード設定	□2. 紛失・盗難時のデータ消去
□3. セキュリティソフトの導入	□4. MDM（モバイルデバイス管理ツール）による端末管理
□5. 利用ルールの策定（アプリケーションの導入制限等）	□6. その他（具体的に：【　　】）
□7. 特に実施していない	□8. 業務でスマートフォンやタブレット端末は利用していない

問2-8 業務で利用するパソコン、スマートフォンやタブレット端末について、社員の私有端末の業務利用（BYOD: Bring Your Own Device）を認めていますか。（当てはまるものに１つだけ☑）

□ 1. 認めている	□ 2. 現在、認めるかどうかを検討中
□ 3. 未検討	□ 4. 認める予定はない

問2-9 貴社では、業務でサーバ（メールサーバ、Web サーバ、ファイルサーバ、プリントサーバなど）を利用していますか。（当てはまるものすべてに☑）

□ 1. 社内サーバを利用している	**→次の問 2-10 へお進みください**
□ 2. 社外サーバを利用している	**→次の問 2-10 へお進みください**
□ 3. 利用していない	**→問 2-12 へお進みください**

問2-10 【問 2-9 で「1」あるいは「2」と回答された方】にお伺いします。
貴社ではサーバにセキュリティパッチ（ぜい弱性の修正）を適用していますか。（次の【a】【b】それぞれの項目について、当てはまるものに１つだけ☑）

【a】 外部に公開しているネットワークサーバ（メールサーバ、Web サーバなど）	【b】 内部で利用しているローカルサーバ（ファイルサーバ、プリントサーバなど）
□ 1. ほぼ全サーバに適用している **→問 2-12 へ**	□ 1. ほぼ全サーバに適用している **→問 2-12 へ**
□ 2. アプリケーションに影響がないことを確認できたもののみを適用している **→問 2-12 へ**	□ 2. アプリケーションに影響がないことを確認できたもののみを適用している **→問 2-12 へ**
□ 3. 情報セキュリティ対策上重要なもののみを適用している **→問 2-12 へ**	□ 3. 情報セキュリティ対策上重要なもののみを適用している **→問 2-12 へ**
□ 4. ほとんど適用していない **→次の問 2-11 へ**	□ 4. ほとんど適用していない **→次の問 2-11 へ**
□ 5. 外部事業者に運用を委託しているので、自ら適用する必要がない **→問 2-12 へ**	□ 5. 外部事業者に運用を委託しているので、自ら適用する必要がない **→問 2-12 へ**
□ 6. 該当するようなサーバを利用していない **→問 2-12 へ**	□ 6. 該当するようなサーバを利用していない **→問 2-12 へ**
□ 7. わからない **→問 2-12 へ**	□ 7. わからない **→問 2-12 へ**

問2-11 【問 2-10 の【a】あるいは【b】で「4」と回答された方】にお伺いします。
セキュリティパッチを適用しない理由について教えてください。（当てはまるものすべてに☑）

□1. パッチの適用が悪影響を及ぼすリスクを避けるため	□2. パッチ適用以外の手段が有効であるため
□3. パッチを適用しなくても問題ないと判断したため	□4. パッチの評価や適用に多大なコストがかかるため
□5. その他（具体的に：【　　】）	

問2-12 貴社はサイバー保険（サイバー攻撃の被害にあったときの補償に特化した保険）や情報漏えい賠償責任保険（商工会議所保険制度）に加入されていますか。（次の【a】【b】それぞれの項目について、当てはまるものに１つだけ☑）

【a】 サイバー保険	【b】 情報漏えい賠償責任保険
□ 1. 加入している	□ 1. 加入している
□ 2. 検討しているが、加入していない	□ 2. 検討しているが、加入していない
□ 3. 内容を知っているが、加入する予定がない	□ 3. 内容を知っているが、加入する予定がない
□ 4. 内容を知らないし、加入もしていない	□ 4. 内容を知らないし、加入もしていない
□ 5. 加入しているかどうかわからない	□ 5. 加入しているかどうかわからない

3. 貴社の情報セキュリティに関する意識・状況についてお伺いします。

問3-1 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。（当てはまるものに１つだけ☑）

- □ 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

問3-2 情報セキュリティに関して困ったことがあった際にどこに相談しますか。（当てはまるものすべてに☑）

- □ 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. 中小企業団体
- □ 7. 業界団体
- □ 8. 地域のセキュリティコミュニティ
- □ 9. 情報処理推進機構（IPA）
- □ 10. その他 （具体的に：【 】）
- □ 11. 特にない

問3-3 どのような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ですか。（当てはまるものすべてに☑）

- □ 1. 経営層向けの手引き書
- □ 2. 業界ごとのセキュリティガイドライン
- □ 3. 中小企業向けセキュリティ対策に関する定期的な情報発信
- □ 4. 他の中小企業の取組状況や実態についての情報共有
- □ 5. 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
- □ 6. 企業専属のセキュリティコンサルティングサービス
- □ 7. 地域密着型の相談窓口サービス
- □ 8. オンライン・電話での窓口相談サービス
- □ 9. 中小企業のセキュリティ対策の可視化サービス
- □ 10. その他【 】

問3-4 貴社の情報セキュリティに関する情報収集先を教えてください。（当てはまるものすべてに☑）

- □ 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. 業界団体
- □ 7. 情報処理推進機構（IPA）
- □ 8. 新聞・雑誌
- □ 9. テレビ
- □ 10. インターネット
- □ 11. 無料のセミナー・実務研修
- □ 12. 有料のセミナー・実務研修
- □ 13. その他
  （具体的に：【 】）
- □ 14. 特にない

問3-5 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。
（当てはまるものすべてに☑）

□ 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. 外部講習会やセミナーの聴講	□ 4. 社内の研修や勉強会
□ 5. 特に実施していない	

問3-6 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に、規定されている報告先を下記よりすべてお選びください。（当てはまるものすべてに☑）

□ 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	

問3-7 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として規定されているものは何ですか。該当するものを下記よりすべてお選びください。（当てはまるものすべてに☑）

□ 1. 情報の隔離	□ 2. ネットワーク遮断
□ 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	

問3-8 貴社では情報セキュリティ関連の被害を防止するために、どのような組織面・運用面の対策を実施していますか。（当てはまるものすべてに☑）

（人的対策）
□ 1. 事業継続計画（BCP）の策定
□ 2. 情報セキュリティに関するリスク分析
□ 3. セキュリティポリシー（セキュリティの規程やルール）が文章化されている **→次のページの問 3-9 へ**
□ 4. 一般ユーザアカウントの管理ルールの策定（パスワードの設定ルール等）
□ 5. Web サイト管理者権限アカウントの管理ルールの策定
□ 6. IT 資産構成や設定の文書化
（物理的対策）
□ 7. フロアや施設への入退出管理
□ 8. 情報（書類などの紙媒体）の施錠管理
□ 9. セキュリティワイヤー等による機器の固定
□ 10. 外部送信ファイルへのパスワード設定
□ 11. 機器や記録媒体の持込み・持出しの制限
□ 12. ハードディスク等の廃棄時の破砕／溶融
（組織的対策）
□ 13. 情報セキュリティマネジメントシステム（ISMS）の認証取得
□ 14. プライバシーマーク（P マーク）の取得
□ 15. 情報セキュリティ監査（内部監査）の実施
□ 16. 情報セキュリティ監査（外部監査）の実施
□ 17. 情報セキュリティ対策の定期的な見直し
□ 18. 委託先の情報セキュリティ対策、体制、実施状況などの確認
□ 19. （内容に応じて）委託先とNDA（機密保持契約）の締結

次ページへ続く

（技術的対策）
□ 20. アカウント毎のアクセス制御
□ 21. 一般ユーザのプログラムインストールの制限（exe ファイルの実行禁止等）
□ 22. 重要なシステム・データのバックアップ
□ 23. セキュリティ監視サービスの活用
□ 24. ログやファイル情報に基づく Web コンテンツの改ざん検知
□ 25. 定期的な Web コンテンツのセキュリティ診断サービス（ぜい弱性調査）の活用
（その他の対策）
□ 26. クラウドサービス利用のための情報セキュリティマネジメントガイドライン（経済産業省ガイドライン）の活用
□ 27. 情報セキュリティ管理基準（経済産業省告示）の活用
□ 28. SSL/TLS 暗号設定ガイドライン（IPA のガイドライン）の活用
□ 29. 組織における内部不正防止ガイドライン（IPA のガイドライン）の活用
□ 30. 中小企業の情報セキュリティ対策ガイドライン（IPA のガイドライン）の活用
□ 31. その他 （具体的に：【 】）
□ 32. 特に実施していない

問3-9 【問 3-8 で「3」と回答された方】にお伺いします。
社内のセキュリティポリシーで規定していることについて教えてください。（当てはまるものすべてに☑）

□ 1. 基本規程（基本方針）	□ 2. 詳細規則（対策基準、実施手順・運用規則等）
□ 3. 責任者の任命	□ 4. 従業員又は部署ごとの情報取扱に関する役割明確化
□ 5. アクセス権限明確化	□ 6. 情報資産の識別、重要度の分類
□ 7. 守秘義務	□ 8. 機器、メール、インターネットアクセスの私的利用制限
□ 9. 機器等の取扱、破損、紛失に留意する項目	□ 10. 紛失した場合などの届け出義務
□ 11. 著作権侵害	□ 12. その他 （具体的に：【 】）
□ 13. 特にはない	

問3-10 貴社では情報セキュリティ関連製品やサービスを導入していますか。（当てはまるものすべてに☑）

□ 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総合的な管理機能）
□ 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

問3-11 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）の状況・内容について教えてください。（当てはまるものすべてに☑）

□ 1. 委託していない	□ 2. 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含む）
□ 3. CSIRT 構築支援サービス	□ 4. 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. 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

問3-12 貴社では情報セキュリティ対策の実施内容（プライバシーポリシーや業務情報の取り扱い基準等）を外部に公開していますか。（最も当てはまるものに１つだけ☑）

□ 1. ホームページで公開している	□ 2. 取引先からの要望があれば個別に提示している
□ 3. 公開していない	□ 4. わからない

問3-13 情報セキュリティ対策の必要性を感じたきっかけについて教えてください。（当てはまるものすべてに☑）

□ 1. 法令（個人情報保護法等）の制定	□ 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. 自社のセキュリティ事故	□ 6. 他社のセキュリティ事故（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 →問3-14へ

問3-14 【問 3-13 で「14」と回答された方】にお伺いします。
情報セキュリティ対策の必要性を感じない理由について教えてください。（当てはまるものすべてに☑）

□ 1. 情報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. その他（具体的に：【　　】）

問3-15 情報セキュリティ対策を実施して感じられたメリットについて教えてください。
（当てはまるものすべてに☑））

□ 1. 従業員の情報セキュリティへの意識向上 →問3-16へ	□ 2. 対処すべきリスクの特定 →問3-16へ
□ 3. ISMS・プライバシーマーク等の認証取得 →問3-16へ	□ 4. トラブルの未然防止による潜在的なコスト削減→問3-16へ
□ 5. データの棚卸等による業務効率化の実現 →問3-16へ	□ 6. データ利活用の推進 →問3-16へ
□ 7. 取引先からの信頼獲得 →問3-16へ	□ 8. 取引機会の増加 →問3-16へ
□ 9. 高度な情報管理が求められる新規事業の実現 →問3-16へ	□ 10. その他【　　】→問3-16へ
□ 11. 特になし →問3-17へ	

問3-16 【問 3-15 で「1」～「10」と回答された方】にのみお伺いします。
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。

【具体的な事例等】

問3-17 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。（当てはまるものすべてに☑）

□ 1. ISMS 認証を取得済み →問3-18へ	□ 2. プライバシーマーク（P マーク）取得済→問3-18へ
□ 3. SECURITY ACTION 一つ星を宣言済→問3-18へ	□ 4. SECURITY ACTION 二つ星を宣言済→問3-18へ
□ 5. その他【 】→問3-18へ	□ 6. 特になし →問3-19へ

問3-18 認証取得や自己宣言にあたり、実施した具体的な取組・工夫などについて教えてください。

【具体的な事例等】

問3-19 次の情報セキュリティに関する事象に対して、どの程度脅威を感じていますか。（【a】～【i】のそれぞれの項目について、当てはまるものに１つだけ☑）

項目	脅威の認識	
【a】コンピュータウイルス	□ 1. 非常に大きな脅威である	□ 2. どちらかといえば脅威である
	□ 3. あまり脅威ではない	□ 4. まったく脅威ではない
	□ 5. 脅威の度合いがわからない	
【b】不正アクセス	□ 1. 非常に大きな脅威である	□ 2. どちらかといえば脅威である
	□ 3. あまり脅威ではない	□ 4. まったく脅威ではない
	□ 5. 脅威の度合いがわからない	
【c】DoS 攻撃・DDoS 攻撃	□ 1. 非常に大きな脅威である	□ 2. どちらかといえば脅威である
	□ 3. あまり脅威ではない	□ 4. まったく脅威ではない
	□ 5. 脅威の度合いがわからない	
【d】標的型攻撃	□ 1. 非常に大きな脅威である	□ 2. どちらかといえば脅威である
	□ 3. あまり脅威ではない	□ 4. まったく脅威ではない
	□ 5. 脅威の度合いがわからない	
【e】情報漏えい	□ 1. 非常に大きな脅威である	□ 2. どちらかといえば脅威である
	□ 3. あまり脅威ではない	□ 4. まったく脅威ではない
	□ 5. 脅威の度合いがわからない	
【f】内部犯行（内部不正）	□ 1. 非常に大きな脅威である	□ 2. どちらかといえば脅威である
	□ 3. あまり脅威ではない	□ 4. まったく脅威ではない
	□ 5. 脅威の度合いがわからない	
【g】システム機能不全	□ 1. 非常に大きな脅威である	□ 2. どちらかといえば脅威である
	□ 3. あまり脅威ではない	□ 4. まったく脅威ではない
	□ 5. 脅威の度合いがわからない	
【h】外部委託先のサービス停止	□ 1. 非常に大きな脅威である	□ 2. どちらかといえば脅威である
	□ 3. あまり脅威ではない	□ 4. まったく脅威ではない
	□ 5. 脅威の度合いがわからない	
【i】外部委託先からの情報漏えい	□ 1. 非常に大きな脅威である	□ 2. どちらかといえば脅威である
	□ 3. あまり脅威ではない	□ 4. まったく脅威ではない
	□ 5. 脅威の度合いがわからない	

問3-20 前問の脅威に対して実施している対策は十分だと感じますか。(【a】～【i】のそれぞれの項目について、当てはまるものに１つだけ☑)

項目	対策について	
【a】コンピュータウイルス	□ 1. 十分と感じる	□ 2. どちらかと言えば十分と感じる
	□ 3. どちらかと言えば十分と感じない	□ 4. 十分と感じない
	□ 5. わからない	
【b】不正アクセス	□ 1. 十分と感じる	□ 2. どちらかと言えば十分と感じる
	□ 3. どちらかと言えば十分と感じない	□ 4. 十分と感じない
	□ 5. わからない	
【c】DoS 攻撃・DDoS 攻撃	□ 1. 十分と感じる	□ 2. どちらかと言えば十分と感じる
	□ 3. どちらかと言えば十分と感じない	□ 4. 十分と感じない
	□ 5. わからない	
【d】標的型攻撃	□1. 十分と感じる	□ 2. どちらかと言えば十分と感じる
	□ 3. どちらかと言えば十分と感じない	□ 4. 十分と感じない
	□ 5. わからない	
【e】情報漏えい	□ 1. 十分と感じる	□ 2. どちらかと言えば十分と感じる
	□ 3. どちらかと言えば十分と感じない	□ 4. 十分と感じない
	□ 5. わからない	
【f】内部犯行（内部不正）	□ 1. 十分と感じる	□ 2. どちらかと言えば十分と感じる
	□ 3. どちらかと言えば十分と感じない	□ 4. 十分と感じない
	□ 5. わからない	
【g】システム機能不全	□ 1. 十分と感じる	□ 2. どちらかと言えば十分と感じる
	□ 3. どちらかと言えば十分と感じない	□ 4. 十分と感じない
	□ 5. わからない	
【h】外部委託先のサービス停止	□ 1. 十分と感じる	□ 2. どちらかと言えば十分と感じる
	□ 3. どちらかと言えば十分と感じない	□ 4. 十分と感じない
	□ 5. わからない	
【i】外部委託先からの情報漏えい	□ 1. 十分と感じる	□ 2. どちらかと言えば十分と感じる
	□ 3. どちらかと言えば十分と感じない	□ 4. 十分と感じない
	□ 5. わからない	

問3-21 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われることについて教えてください。(当てはまるものすべてに☑)

□ 1. 経営者の情報セキュリティ意識向上	□ 2. 経営者への情報セキュリティ対策方法の教育
□ 3. 従業員の情報セキュリティ意識向上	□ 4. 従業員への情報セキュリティ対策実践教育
□ 5. 市場や顧客からの信頼・評価の仕組み	□ 6. 企業内の体制整備
□ 7. 情報セキュリティ関連法制度の整備	□ 8. 対策支援費等の補助制度の充実
□ 9. 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	□ 10. 地域での支援者育成や確保、サポートセンターの充実
□ 11. その他 （具体的に：【 】）	□ 12. 特にない

4. 貴社の情報セキュリティ被害についてお伺いします。

問4-1 貴社では 2020 年度 1 年間（2020 年 4 月～2021 年 3 月）に、情報セキュリティ被害にあったことがありましたか。一度でもあればお答えください。（当てはまるものすべてに☑）

□ 1. コンピュータウイルスに感染	→次の問 4-2 へ
□ 2. 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	→問 4-5 へ
□ 3. サイバー攻撃（DoS 攻撃・DDoS 攻撃、不正アクセス、標的型攻撃など）	→問 4-6 へ
□ 4. 外部委託先に起因するサービスの停止・情報漏えい	→問 4-8 へ
□ 5. 被害にあっていない	→問 5-1 へ

問4-2 【問 4-1 で「1」と回答された方】にお伺いします。
感染あるいは発見したコンピュータウイルスの想定される侵入経路について教えてください。（当てはまるものすべてに☑）

□ 1. 電子メール	□ 2. インターネット接続 （ホームページ閲覧など）
□ 3. 自らダウンロードしたファイル	□ 4. P2P（Peer to Peer）などのファイル共有ソフト
□ 5. USB メモリ等の外部記憶媒体	□ 6. 持ち込みパソコン
□ 7. その他（具体的に：【 】）	□ 8. わからない

問4-3 【問 4-1 で「1」と回答された方】にお伺いします。
コンピュータウイルスに感染した影響で生じた被害について教えてください。（当てはまるものすべてに☑）

□ 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	

問4-4 【問 4-1 で「1」と回答された方】にお伺いします。
コンピュータウイルスに感染した影響で、取引先（サプライチェーン）に影響が及んだ内容について教えてください。（当てはまるものすべてに☑）

□ 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	

問4-5 【問 4-1 で「2」と回答された方】にお伺いします。
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の内容について教えてください。（当てはまるものすべてに☑）

□ 1. 内部者の不正による被害があった	□ 2. 委託者の不正による被害があった
□ 3. 内部者（委託者を含む）の不正による被害はなかった	□ 4. わからない

問4-6【問 4-1 で「3」と回答された方】にお伺いします。
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。（当てはまるものすべてに☑）

- □ 1. ID・パスワードを騙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. DoS 攻撃・DDoS 攻撃
- □ 5. 標的型攻撃
- □ 6. ランサムウェア
- □ 7. その他（具体的に：【　　】）
- □ 8. 手口はわからない

問4-7【前頁の問 4-1 で「3」と回答された方】にお伺いします。
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。（当てはまるものすべてに☑）

- □ 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

問4-8【前頁の問 4-1 で「1」～「4」のいずれかと回答された方】にお伺いします。
昨年度、情報セキュリティ被害で生じた被害額、復旧するまでに要した期間について教えてください。

被害額	【　　】円
期間	【　　】日

5. 取引先を含む情報セキュリティ対策についてお尋ねします。

問5-1 販売先（発注元企業）や、仕入先（委託・協力企業）との契約締結時に、情報セキュリティに関する条項・取引上の義務・要請はありますか。（当てはまるものに１つだけ☑）

- □1. はい　　**→次の問 5-2 へお進みください**
- □2. いいえ　　**→次頁の問 5-4 へお進みください**

問5-2【問 5-1 で「1」と回答された方】契約時における情報セキュリティに関する要請について当てはまるものすべてをお答えください。（次の【a】【b】それぞれの項目について、当てはまるものすべてに☑）

【a】 販売先（発注元企業）との契約時	【b】 仕入先（委託・協力企業）との契約時
□ 1. 秘密保持	□ 1. 秘密保持
□ 2. 証跡の提示、監査協力等	□ 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	□ 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. インシデントが発生した場合の対応	□ 4. 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）	□ 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	□ 6. 認証（ISMS 等）取得の依頼/要件化
□ 7. 新たな脅威（ぜい弱性等）が顕在化した場合の情報共有・対応	□ 7. 新たな脅威（ぜい弱性等）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	□ 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）	□ 9. 契約終了後の情報資産の扱い（返却、消去、廃棄等）
□ 10. その他【　　】	□ 10. その他【　　】

問5-3 【問 5-1 で「1」と回答された方】にのみお伺いします。
前問【a】でご回答頂いた販売先（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。

問5-4 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課題となることについて教えてください。（当てはまるものすべてに☑）

□ 1. 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. セキュリティ認証制度の取得
□ 5. 損害保険付保
□ 6. その他【 】
□ 7. 特になし

問5-5 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。（最も当てはまるものに１つだけ☑）

□ 1. 全額自社で負担している	□ 2. 一部の費用負担を販売先（発注元企業）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【 】	

問5-6 仕入先（委託・協力企業）への情報セキュリティ対策を行うための貴社のガイドライン等はありますか。（当てはまるものに１つだけ☑）

□ 1. ガイドライン等がある**→問 5-7 へ**
□ 2. ガイドライン等はない **→問 6-1 へ**
□ 3. 委託業務がない **→問 6-1 へ**

問5-7 【問 5-6 で「1」と回答された方】にのみお伺いします。
貴社のガイドラインにおいて、仕入先（委託・協力企業）の情報セキュリティ対策等で規定していることを教えてください。（当てはまるものすべてに☑）

□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．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（脆弱性等）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．その他【 】

6. IPAが実施する活動につきまして。

問6-1 独立行政法人情報処理推進機構（IPA）が実施する活動についてご存じのものをお答えください。
（当てはまるものすべてに☑）

□ 1. 中小企業の情報セキュリティ対策ガイドライン	□ 2. SECURITY ACTION
□ 3. サイバーセキュリティお助け隊	□ 4. その他
□ 5. 知っているものはない	