2. セキュリティへの取り組み状況

2. セキュリティへの取り組み状況

2.1 セキュリティ対策実施状況、セキュリティ要請状況

- セキュリティ対策は、会員顧客企業で 8 割、中規模一般企業で 7 割、小規模一般企業で 6 割の実施済みの状況
- セキュリティに関する要請元は、「要請元なし」の割合が高い
- セキュリティ要請がある企業の方が、セキュリティ対策実施率が高い

2.1.1 セキュリティ対策実施状況

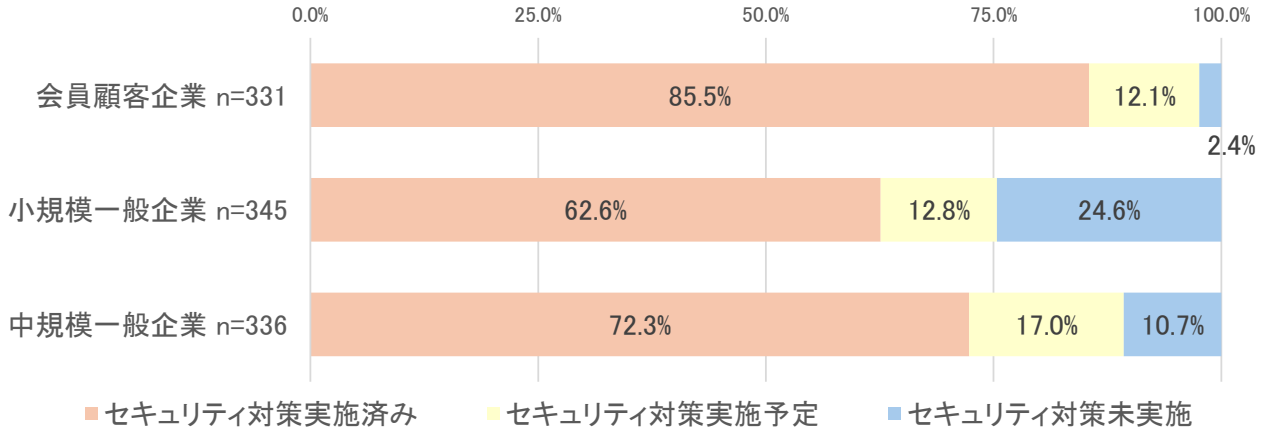

図 2.1-1 セキュリティ対策の実施状況

企業群別でみたセキュリティ対策の実施状況は図 2.1-1 の通りである。

会員顧客企業では、「セキュリティ対策実施済み」（85.5％）、「セキュリティ対策実施予定」（12.1％）、「セキュリティ対策未実施」（2.4％）であった。

「セキュリティ対策実施済み」を企業群別でみると、小規模一般企業（62.6％）、中規模一般企業（72.3％）となっており、会員顧客企業のセキュリティ対策実施済みはいずれも高い結果であった。

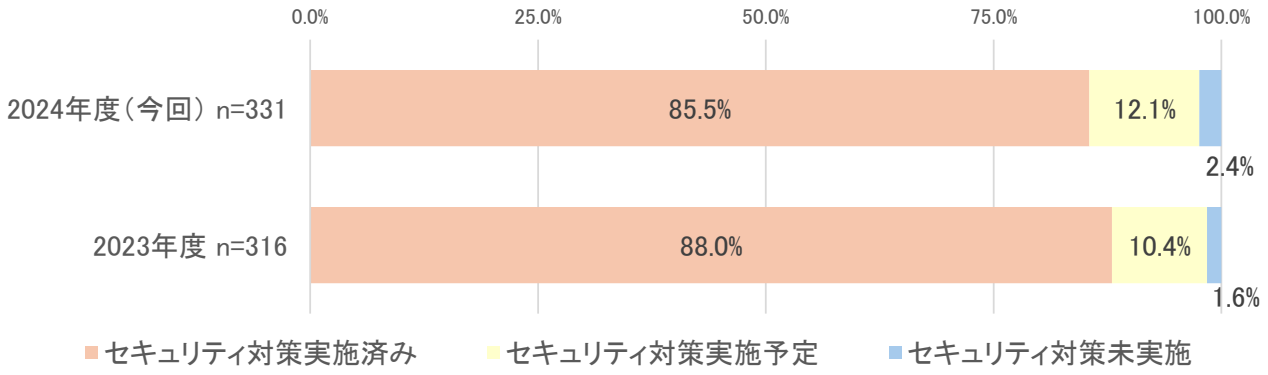

図 2.1-2　会員顧客企業のセキュリティ対策の実施状況変化

会員顧客企業のセキュリティ対策の実施状況について前年度結果と比べると、「セキュリティ対策実施済み」が 2.5 ポイント低く、「セキュリティ対策未実施」が 0.8 ポイント高い結果であった（図 2.1-2）。

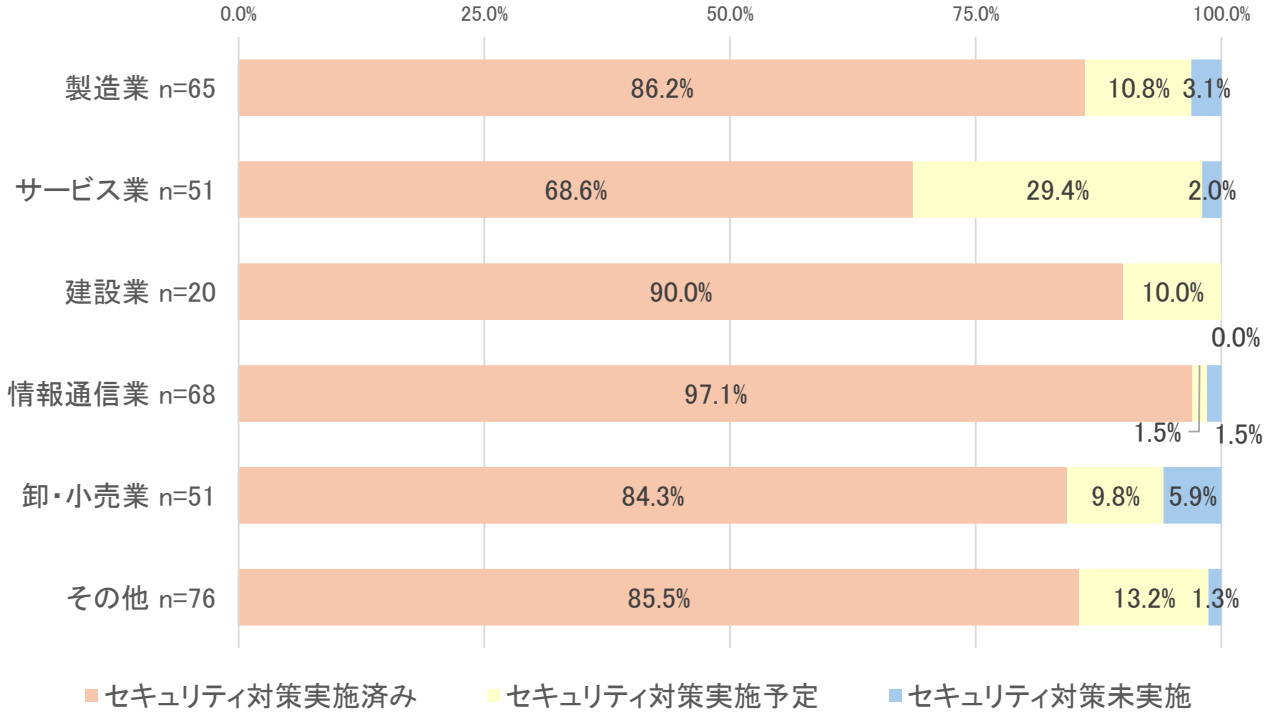

図 2.1-3　会員顧客企業（業種別）のセキュリティ対策の実施状況

会員顧客企業のセキュリティ対策の実施状況を業種別でみると、情報通信業（97.1%）、建設業（90.0%）が高い実施状況にあり、サービス業を除き 8 割を超える実施状況にある。他方で、サービス業だけが「セキュリティ対策実施済み」が 7 割を割っていた（68.6%）。「セキュリティ対策未実施」でみると、卸・小売業が 5.9%と高くなっていた（図 2.1-3）。

2.1.2 セキュリティ要請状況

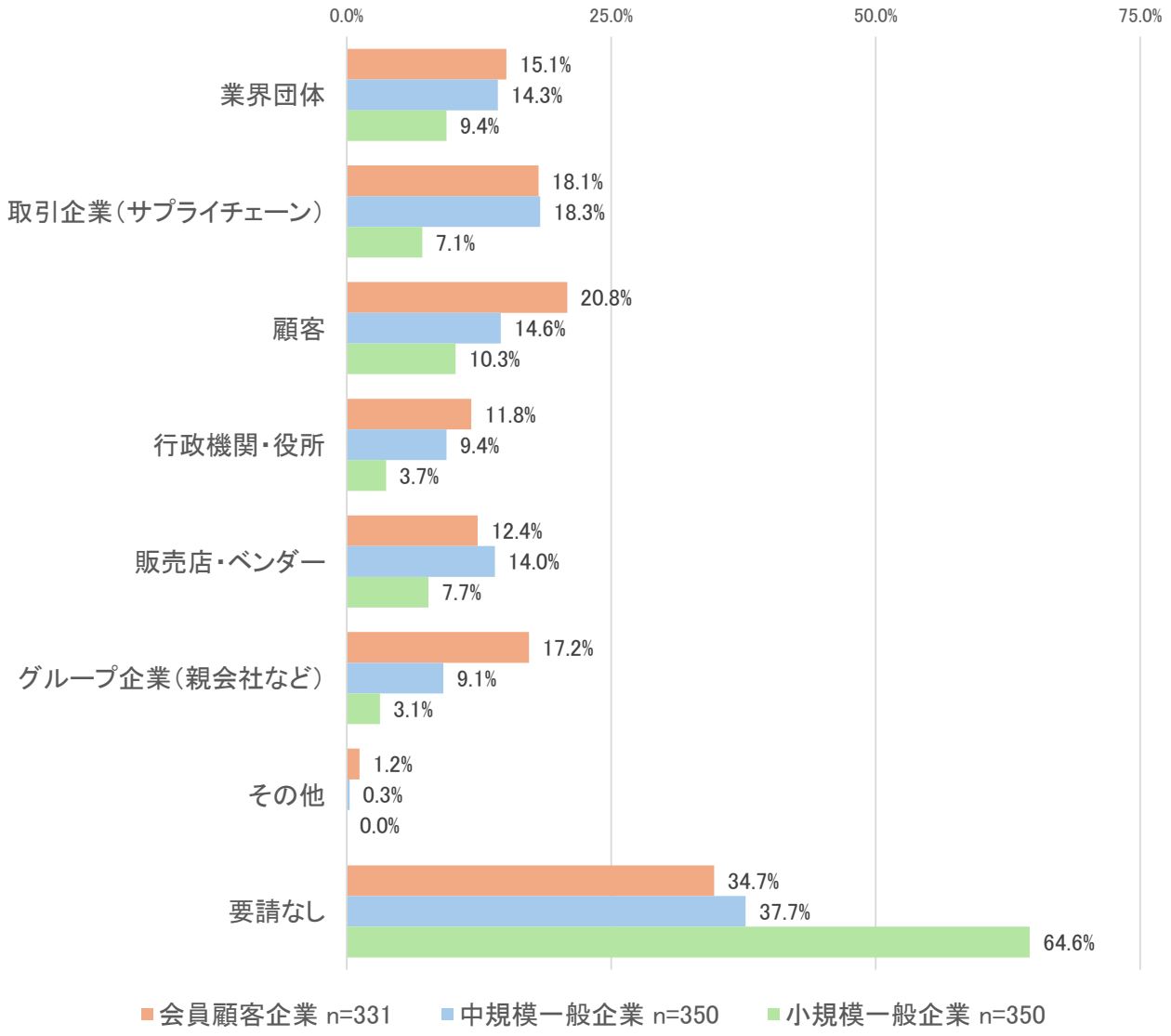

図 2.1-4　セキュリティに関する要請元

セキュリティに関する要請（決められたセキュリティ基準への対応依頼）元をみると、会員顧客企業では、「要請なし」（34.7%）、「顧客」（20.8%）、「取引企業（サプライチェーン）」（18.1%）であった。中規模一般企業では、「要請なし」（37.7%）、「取引企業（サプライチェーン）」（18.3%）、「顧客」（14.6%）であった。小規模一般企業では、「要請なし」（64.6%）、「顧客」（10.3%）、「業界団体」（9.4%）であった（図 2.1-4）。

2.1.3 セキュリティ対策とセキュリティ要請の関係

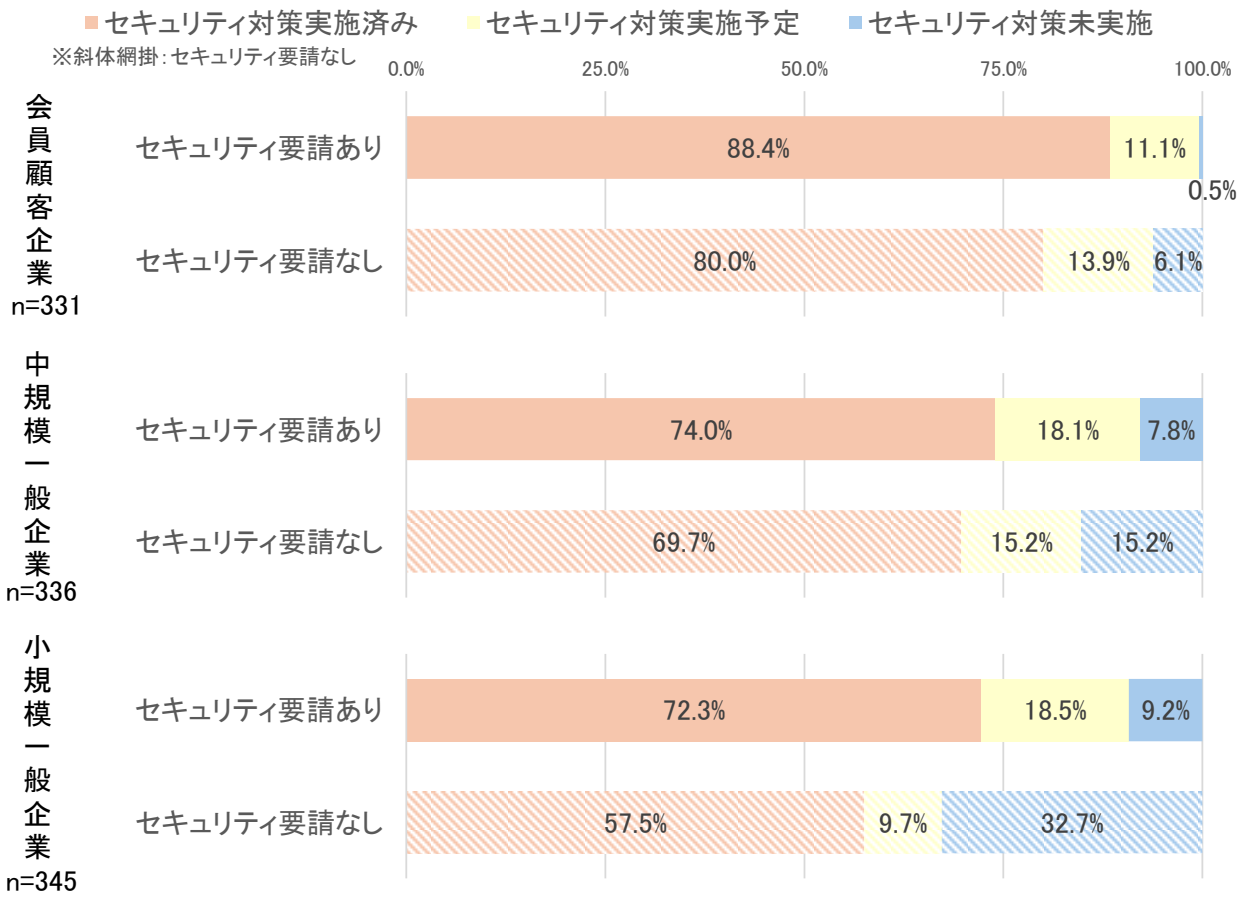

図 2.1-5　セキュリティ要請の有無別でみたセキュリティ対策の実施状況

セキュリティ要請の有無別でみた対策の実施状況は図 2.1-5 の通りであった。会員顧客企業（+8.4 ポイント）、中規模一般企業（+4.3 ポイント）、小規模一般企業（+14.8 ポイント）のいずれでもセキュリティ要請がある企業の対策実施率が高くなっている。小規模一般企業においては、セキュリティ要請がないと回答した企業の 32.7%がセキュリティ対策未実施の結果であった。

2.2 セキュリティ対策実施のきっかけ

■ セキュリティ対策実施のきっかけは、会員顧客企業では「自社で必要性を感じた」の割合が高い

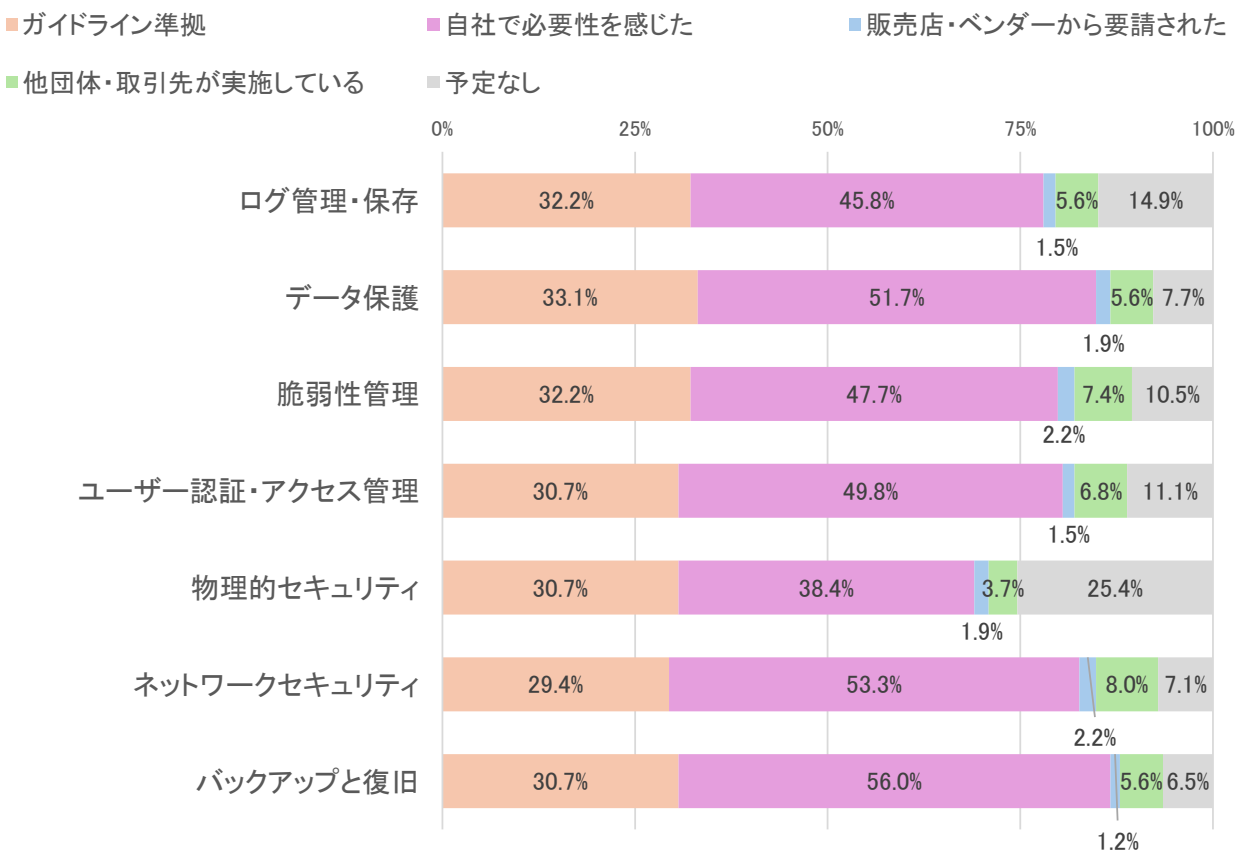

図 2.2-1 セキュリティ対策のきっかけ（会員顧客企業 n=323）

会員顧客企業がセキュリティ対策実施のきっかけについて、実施項目別でみた結果が図 2.2-1 である。「データ保護」、「ネットワークセキュリティ」、「バックアップと復旧」では＜自社で必要性を感じた＞の回答が 5 割を超えている。他方、「物理的セキュリティ」では＜予定なし＞が 25.4%と他の項目に比べ高い結果であった。

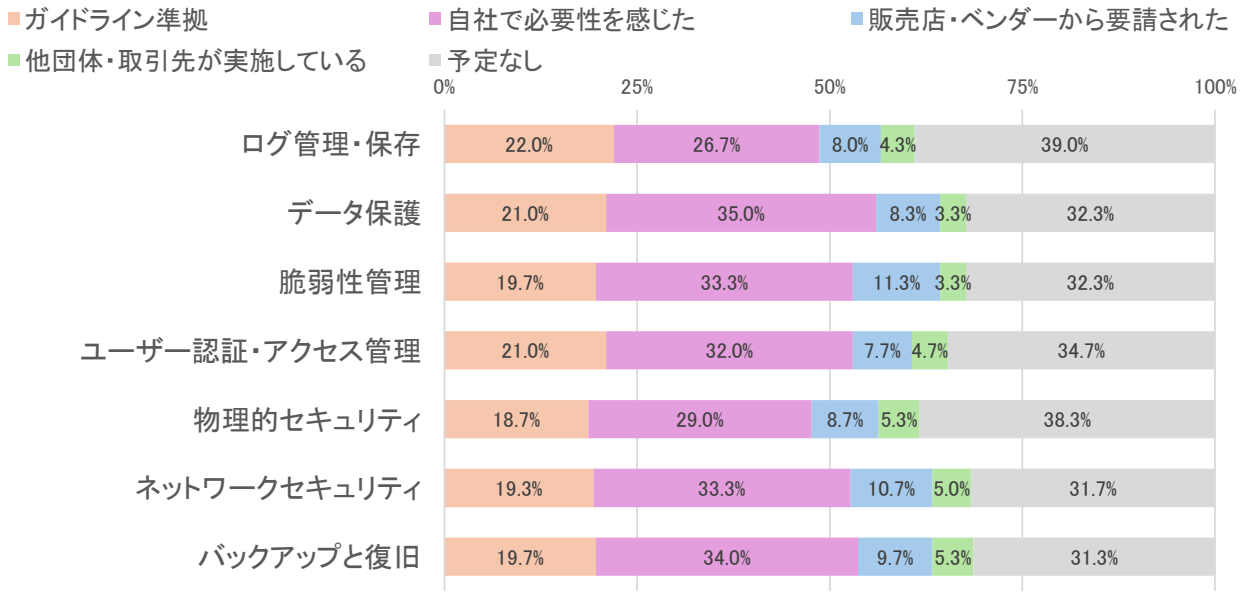

図 2.2-2　セキュリティ対策のきっかけ（中規模一般企業　n=300）

中規模一般企業の結果が図　2.2-2 である。割合が高いものは、「ログ管理・保存」＜予定なし＞（39.0%）、「物理セキュリティ」＜予定なし＞（38.3%）、「データ保護」＜自社で必要性を感じた＞（35.0%）の順であった。

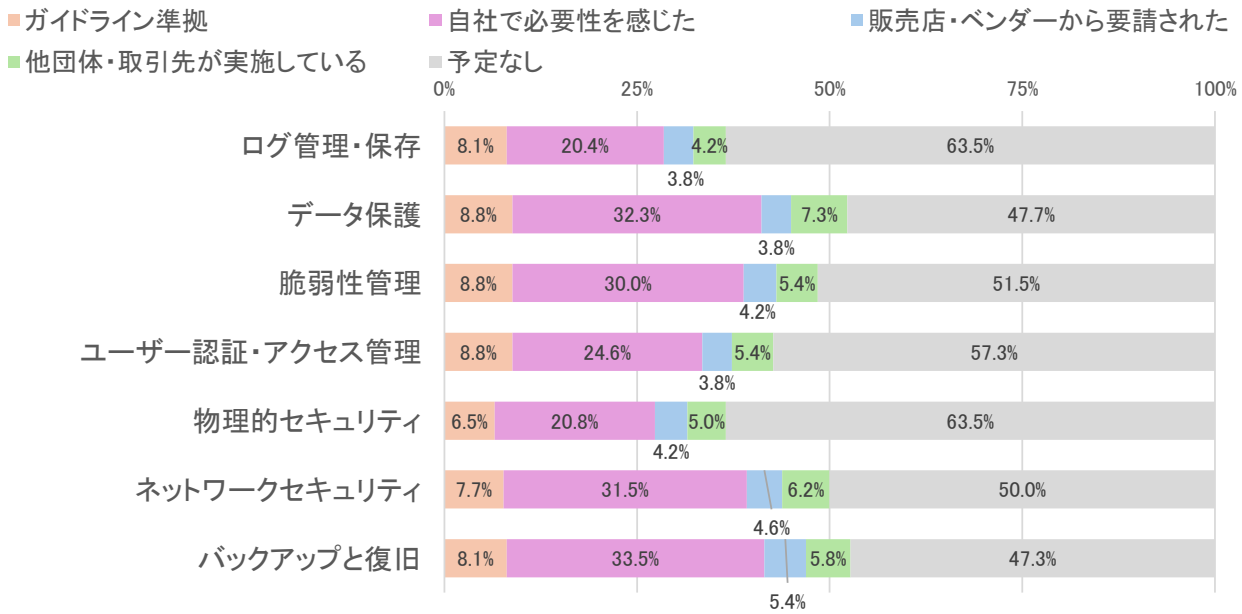

図 2.2-3 セキュリティ対策のきっかけ（小規模一般企業　n=260）

小規模一般企業の結果が図　2.2-3 である。小規模一般企業では、セキュリティ対策項目としてあげられている 7 項目すべてにおいて、＜予定なし＞と回答した割合が 4 割を超える水準にある。

割合が高いものは、「ログ管理・保存」＜予定なし＞（63.5%）、「物理セキュリティ」＜予定なし＞（63.5%）、「ユーザー認証・アクセス管理」＜予定なし＞（57.3%）の順であった。

2.3 導入済み、または導入予定のセキュリティ製品・サービス

■ 社内データ保護のために導入されている製品では、会員顧客企業では「バックアップ製品」、「Active Directory」、中規模一般企業では「Active Directory」、「ネットワークアクセス制限製品」、小規模一般企業では「バックアップ製品」の割合が高い
■ インターネット上のデータ保護のために導入されている製品では、「ウイルス対策」、「スパムメール対策」の割合が高い

2.3.1 社内データ保護

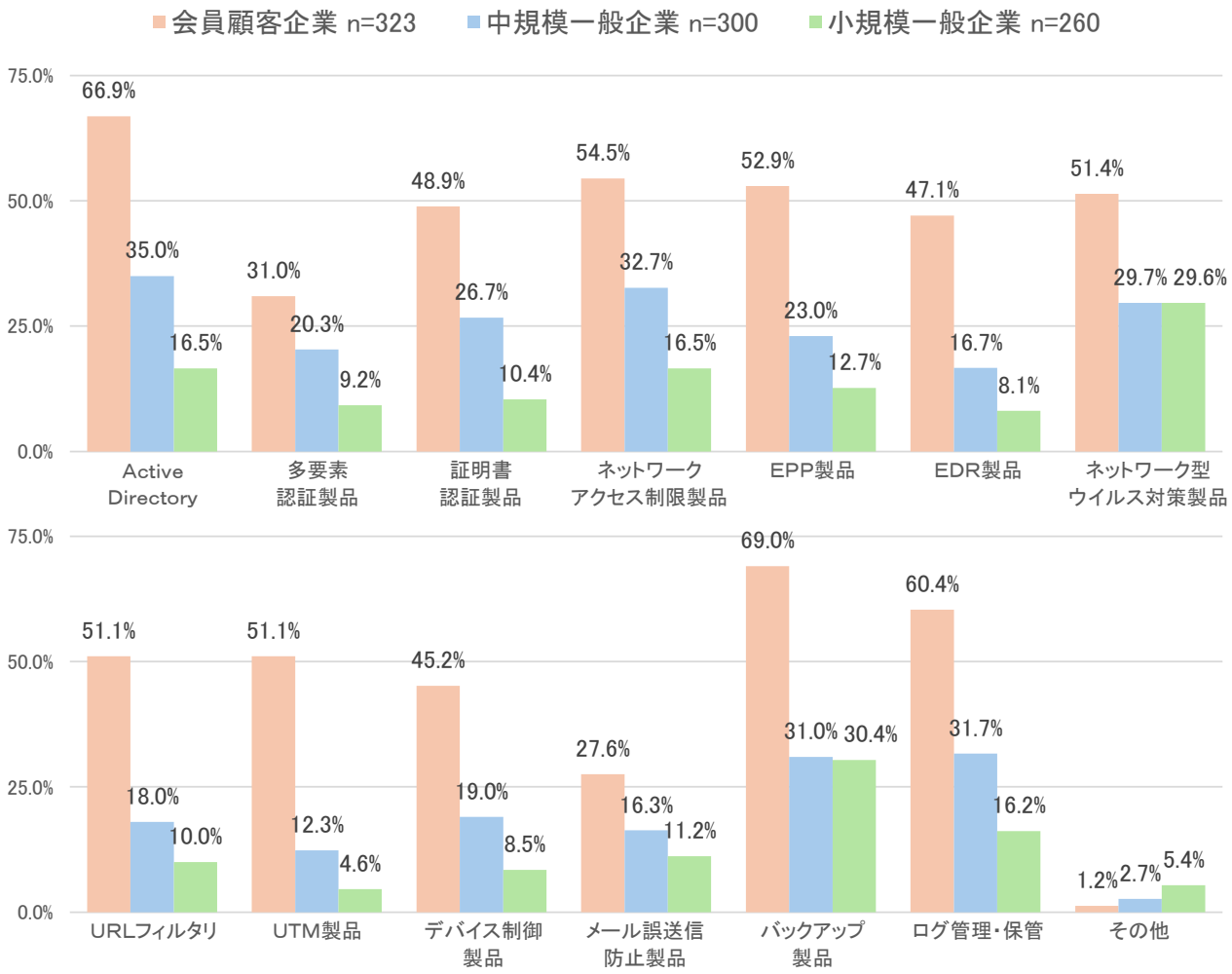

図 2.3-1 社内データ保護のために導入済み（導入予定）のセキュリティ製品・サービス

社内データ保護のためのセキュリティ製品・サービスの導入状況は図 2.3-1 であった。

会員顧客企業では、「バックアップ製品」（69.0%）、「Active Directory」（66.9%）、「ログ管理・保管」（60.4%）、「ネットワークアクセス制限製品」（54.5%）、「EPP 製品」（52.9%）の順であった。

中規模一般企業では、「Active Directory」（35.0%）、「ネットワークアクセス制限製品」（32.7%）、「ログ管理・保管」（31.7%）、「バックアップ製品」（31.0%）、「ネットワーク型ウイルス対策製品」（29.7%）の順であった。

小規模一般企業では、「バックアップ製品」（30.4%）、「ネットワーク型ウイルス対策製品」（29.6%）、「Active Directory」/「ネットワークアクセス制限製品」（ともに 16.5%）、「ログ管理・保管」（16.2%）の順であった。

2.3.2 インターネット上のデータ保護

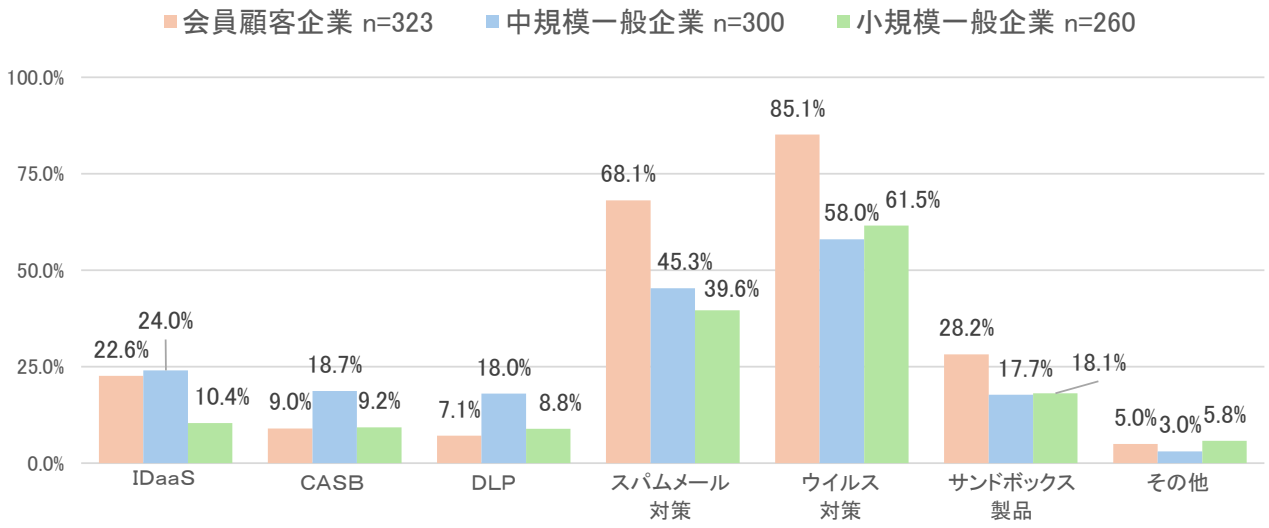

図 2.3-2　インターネット上のデータ保護のために導入済み（導入予定）のセキュリティ製品・サービス

インターネット上のデータ保護のためのセキュリティ製品・サービスの導入状況は図 2.3-2 であった。

会員顧客企業では、「ウイルス対策」（85.1%）、「スパムメール対策」（68.1%）、「サンドボックス製品」（28.2%）の順であった。

中規模一般企業では、「ウイルス対策」（58.0%）、「スパムメール対策」（45.3%）、「IDaaS」（24.0%）の順であった。

小規模一般企業では、「ウイルス対策」（61.5%）、「スパムメール対策」（39.6%）、「サンドボックス製品」（18.1%）の順であった。

2.4 セキュリティ対策の運用

- セキュリティ対策として＜正しく運用されており機能している＞ものは「セキュリティルールやポリシーの整備」が 8 割弱
- 会員顧客企業ならびに中規模一般企業では、「生成 AI のガイドライン整備」は 4 割前後の運用状況

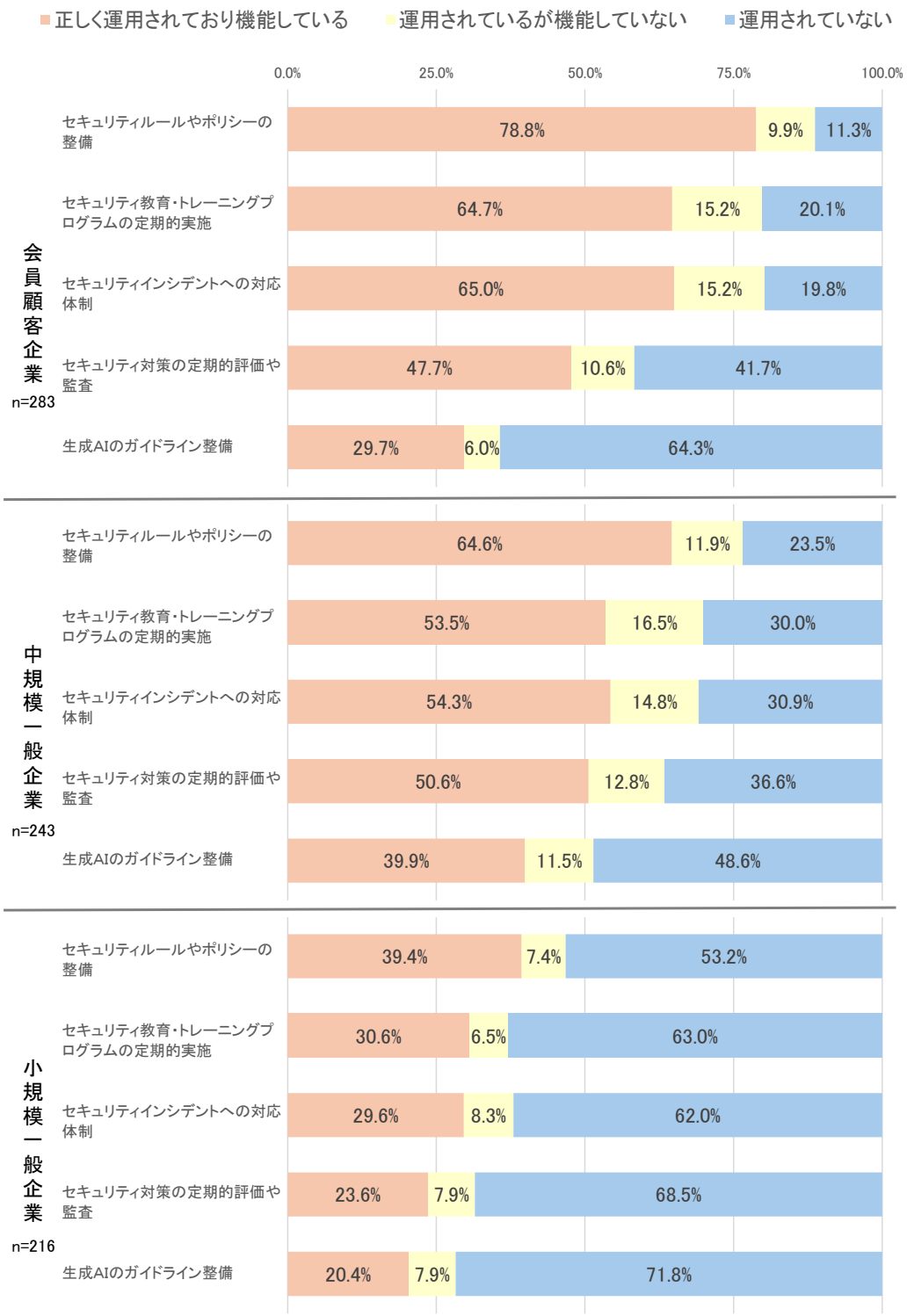

図 2.4-1　セキュリティ対策の運用状況

セキュリティ対策の 5 つの項目について、運用状況を聞いた結果が図 2.4-1 である。

会員顧客企業では、「セキュリティルールやポリシーの整備」について＜正しく運用されており機能している＞との回答が 78.8%と高い結果であり、「セキュリティインシデントへの対応体制」＜正しく運用されており機能している＞65.0%の順で機能していた。

中規模一般企業では、「セキュリティルールやポリシーの整備」について＜正しく運用されており機能している＞との回答が 64.6%と高い結果であり、「セキュリティインシデントへの対応体制」＜正しく運用されており機能している＞54.3%の順で機能していた。

小規模一般企業では、会員顧客企業ならびに中規模一般企業と比べると割合は低いものの、「セキュリティルールやポリシーの整備」について＜正しく運用されており機能している＞との回答が 39.4%と高く、「セキュリティ教育・トレーニングプログラムの定期的実施」＜正しく運用されており機能している＞30.6%の順で機能していた。

2.5 セキュリティ脅威への対応

- 会員顧客企業のセキュリティ脅威の理解（把握）は中規模・小規模一般企業よりも高く、対策も進んでおり、前回調査結果よりも理解が高まった
- インシデントが発生した際の相談先としては「販売店・ベンダー」が最も多い

2.5.1 セキュリティ脅威の理解度と対応状況

セキュリティの脅威に対し、理解度と対策状況を調査した結果が図 2.5-1、図 2.5-2、図 2.5-3 である。

最新としては、「情報セキュリティ 10 大脅威 2024」が独立行政法人 情報処理推進機構より公表されているが、前年度調査との比較の観点から「情報セキュリティ 10 大脅威 2023」を使っている。脅威の種類・内容（要約）は表 2.5-1 の通り。

表 2.5-1 情報セキュリティ 10 大脅威[2]

順位	脅威	内容
1	ランサムウェア	ランサムウェアと呼ばれるウイルスにPCやサーバーが感染すると、端末のロックや、データの暗号化が行われ、その復旧と引き換えに金銭を要求される。さらに、暗号化だけで はなく、重要な情報を窃取されることもあり、その情報を公開すると脅す。このように複数の脅しを組み合わせる（四重脅迫等）ことで、ランサムウェアに感染した組織が金銭を支払わざるを得ない状況を作り出そうとする。
2	サプライチェーンの弱点を悪用した攻撃	商品の企画・開発から、調達、製造、在庫管理、物流、販売までの一連のプロセス、およびこの商流に関わる組織群をサプライチェーンと呼ぶ。攻撃者はそのサプライチェーンを悪用し、セキュリティ対策の強固な関連企業・サービス・ソフトウェア等は直接攻撃せずに、それ以外のセキュリティ対策が脆弱なプロセスを最初の標的とし、そこを踏み台として顧客や上流プ ロセスの関連企業等 、本命の標的を攻撃する。また、もう1つのサプライチェーンとして「ソフトウェアサプライチェーン」もある。これはソフトウェア開発のライフサイクルに関与する全てのモノ（コード、ライブラリ、プラグイン、各種ツール等）や人（開発者、運用者等）の繋がりであり、ここを狙った攻撃も行われている。
3	標的型攻撃による機密情報の窃取	標的型攻撃とは、特定の組織（官公庁、民間団体、企業等）を狙う攻撃のことであり、機密情報等を窃取することや業務妨害を目的としている。攻撃者は社会の変化や、働き方の変化に便乗し、状況に応じた巧みな攻撃手法で機密情報等を窃取しようとする。
4	内部不正による情報漏えい	組織に勤務する従業員や元従業員等の組織関係者による機密情報の持ち出しや悪用等の不正行為が発生している。また、組織内の情報管理の 規則 を守らずに情報を持ち出し、紛失や情報漏えいにつながるケースもある。組織関係者による不正行為は、組織の社会的信用の失墜、損害賠償による経済的損失を与える。また、不正に取得した情報を他組織に持ち込んだ場合、その組織も損害賠償等の対象になるおそれがある。
5	テレワーク等のニューノーマルな働き方を狙った攻撃	2020年以降、新型コロナウイルス感染症（ COVID-19）の世界的な 蔓延に伴い、感染症対策の一環として政府機関がニューノーマルな働き方の 1つであるテレワークを推奨している。勤労形態としてテレワークが活用され、ウェブ会議サービスや VPN等の本格的な活用がされる中、それらを狙った攻撃が行われている。
6	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	OSやソフトウェアに脆弱性が存在することが判明し、脆弱性の修正プログラム（パッチ）や回避策がベンダーから提供される前に、その脆弱性を悪用してサイバー攻撃が行われることがある。これをゼロデイ攻撃という。 多くのシステムで利用されているソフトウェアに対してゼロデイ攻撃が行われると、社会が混乱に陥るおそれがある。
7	ビジネスメール詐欺による金銭被害	ビジネスメール詐欺（Business E-mail Compromise BEC）は、悪意のある第三者が取引先等になりすまして偽のメールを送ったり、組織間のメールのやり取りを乗っ取ったりした上で、最終的に偽の銀行口座に送金させるサイバー攻撃である。組織間取引の送金であることから被害額は大きくなる。
8	脆弱性対策情報の公開に伴う悪用増加	ソフトウェアやハードウェア（機器類）の脆弱性対策情報の公開は、脆弱性の脅威や対策情報を製品の利用者に広く呼び掛けられるメリットがある。一方で、攻撃者はその情報を悪用し、当該製品への脆弱性対策を講じていないシステムを狙って攻撃を行うことができる。近年では脆弱性関連情報の公開後に攻撃コードが流通し、攻撃が本格化するまでの時間 もますます短くなっている。
9	不注意による情報漏えい等の被害	メールの誤送信や記録端末や記録媒体の紛失等の不注意による個人情報等の漏えいが発生している。漏えいした情報が第三者に売買されるとさらなる悪用につながるおそれもある。情報漏えいした組織は社会的信頼の失墜や経済的な損失につながるおそれもあり、組織はデータに対して慎重な扱いが求められる。
10	犯罪のビジネス化（アンダーグラウンドサービス）	犯罪に使用するためのサービスやツール、IDやパスワードの情報等がアンダーグラウンド市場で取り引きされ、これらを悪用した攻撃が行われている。攻撃に対する専門知識が無い者でもサービスやツールを利用することで、容易に攻撃を行えるため、サービスやツールが公開されると被害が広がるおそれがある。

[2] 『セキュリティーとデジタルトランスフォーメーションへの取り組み状況に関する調査研究 2023 年度版』, 一般社団法人 日本コンピュータシステム販売店協会,2024/2

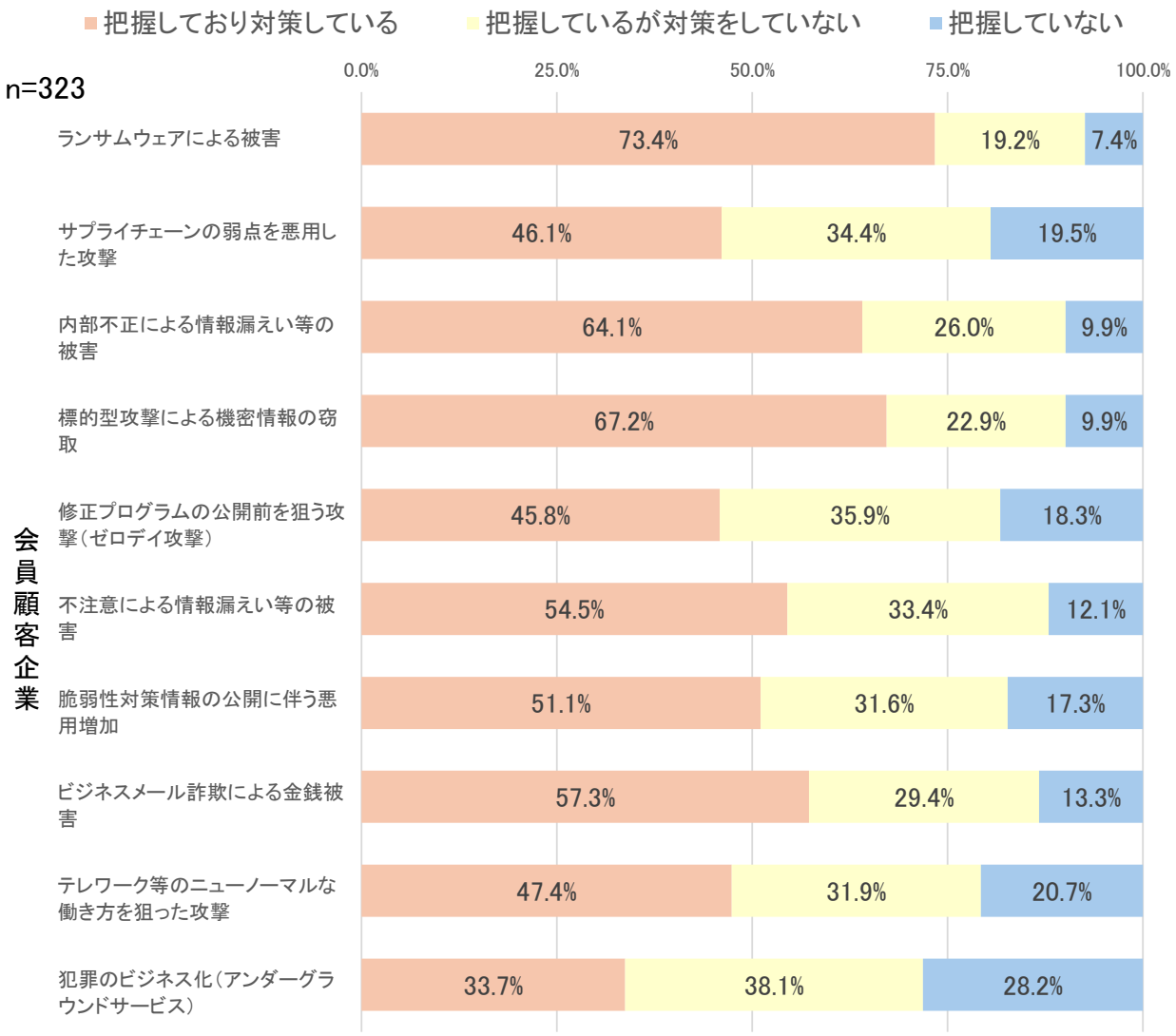

図 2.5-1　会員顧客企業のセキュリティ脅威の理解度と対応状況

会員顧客企業におけるセキュリティ脅威の理解度として把握しており対策されているものとしては、「ランサムウェアによる被害」（73.4%）、「標的型攻撃による機密情報の窃取」（67.2%）、「内部不正による情報漏えい等の被害」（64.1%）であった。他方、把握されていないものは、「犯罪のビジネス化（アンダーグラウンドサービス）」（28.2%）と「テレワーク等のニューノーマルな働き方を狙った攻撃」（20.7%）が 2 割を超えていた。

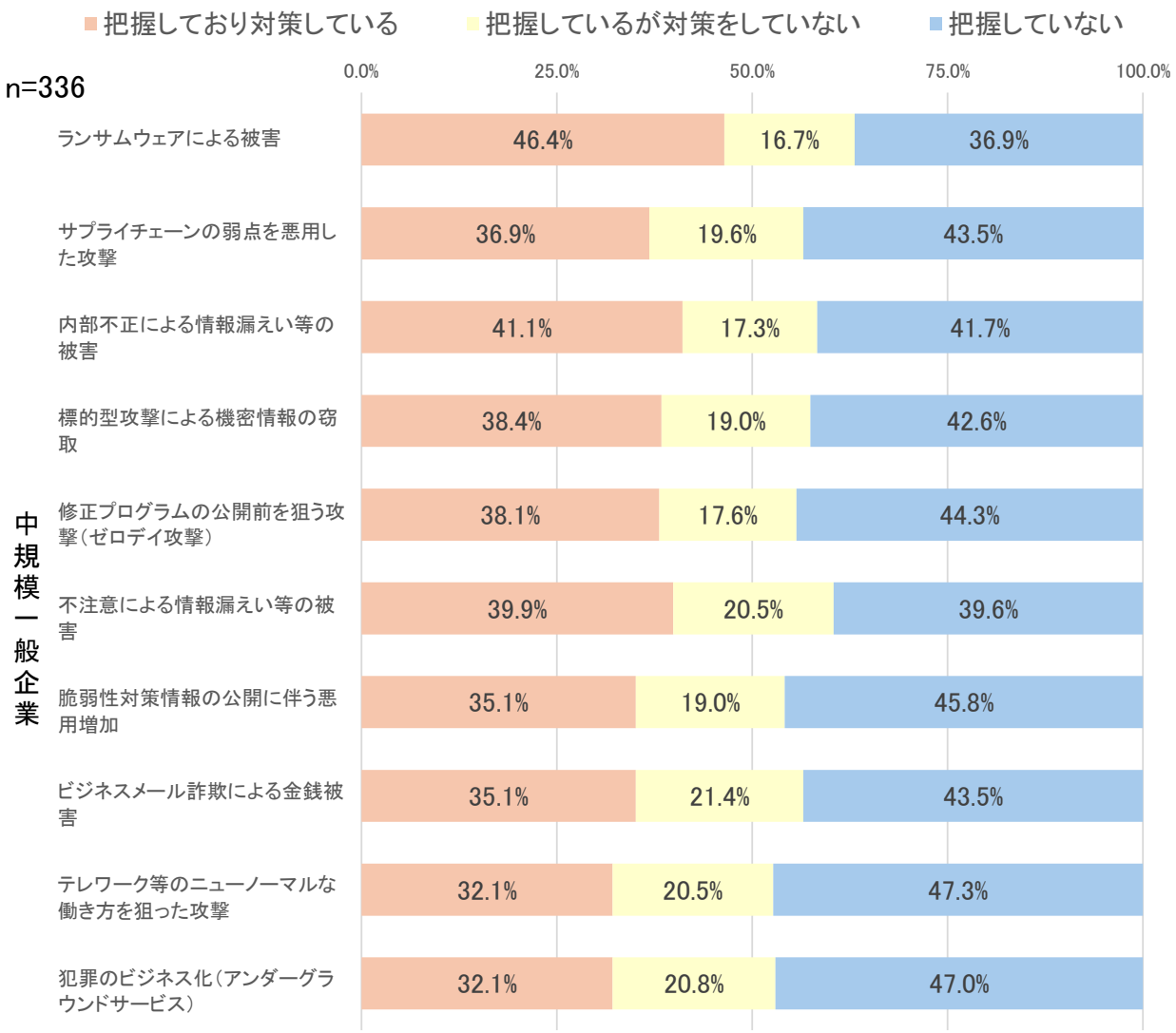

図 2.5-2　中規模一般企業のセキュリティ脅威の理解度と対応状況

中規模一般企業におけるセキュリティ脅威の理解度として把握しており対策されているものとしては、「ランサムウェアによる被害」（46.4%）、「内部不正による情報漏えい等の被害」（41.1%）、「不注意による情報漏えい等の被害」（39.9%）であった。他方、把握されていないものは、「テレワーク等のニューノーマルな働き方を狙った攻撃」（47.3%）、「犯罪のビジネス化（アンダーグラウンドサービス）」（47.0%）、「脆弱性対策情報の公開に伴う悪用増加」（45.8%）の 3 つが 45%を超えていた。

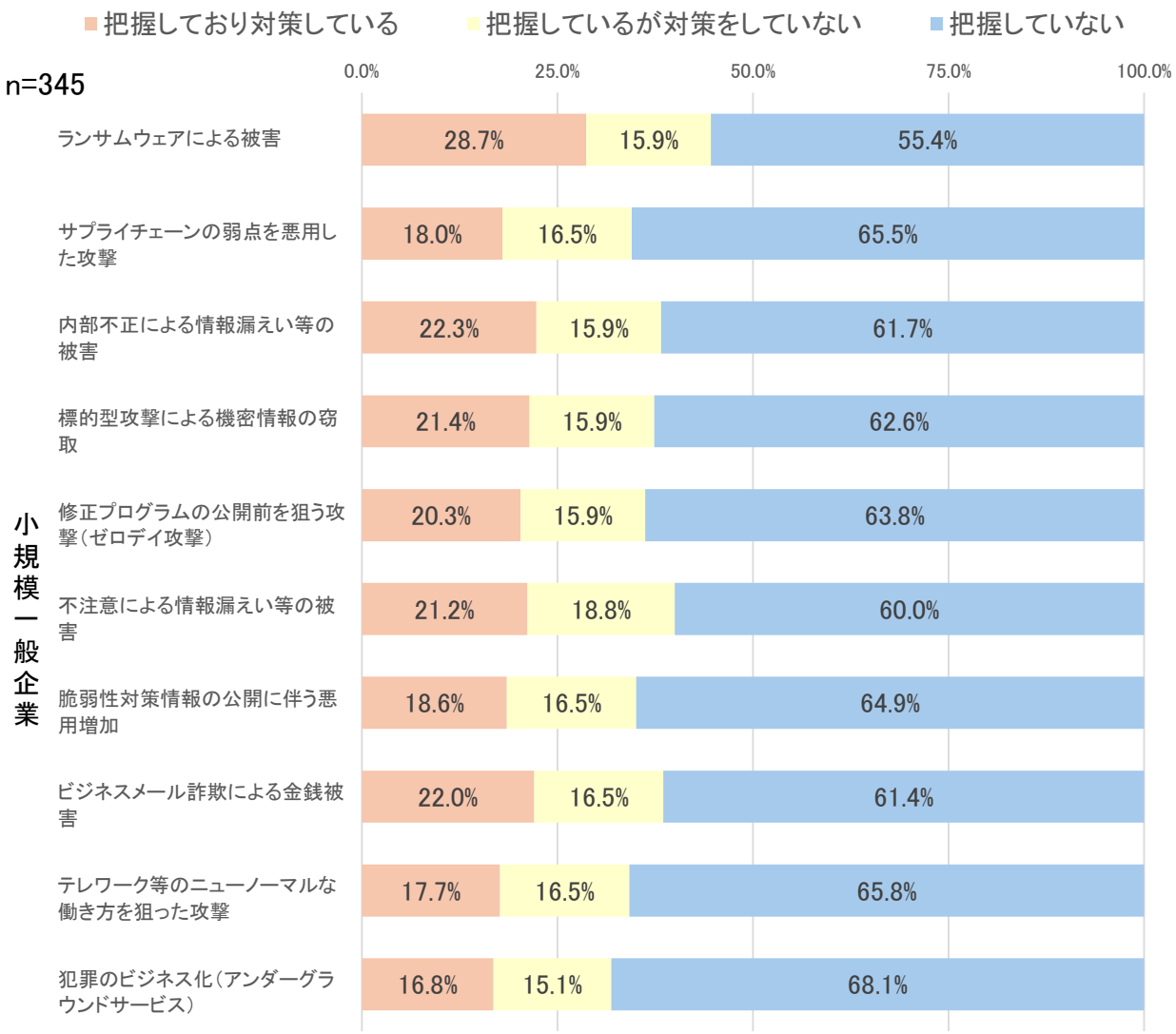

図 2.5-3　小規模一般企業のセキュリティ脅威の理解度と対応状況

小規模一般企業におけるセキュリティ脅威の理解度として把握しており対策されているものとしては、「ランサムウェアによる被害」（28.7%）、「内部不正による情報漏えい等の被害」（22.3%）、「ビジネスメール詐欺による金銭被害」（22.0%）となっており、2 割を超える水準であった。他方、把握されていないものは、「犯罪のビジネス化（アンダーグラウンドサービス）」（68.1%）、「テレワーク等のニューノーマルな働き方を狙った攻撃」（65.8%）、「サプライチェーンの弱点を悪用した攻撃」（65.5%）の 3 つが 65%を超えていた。

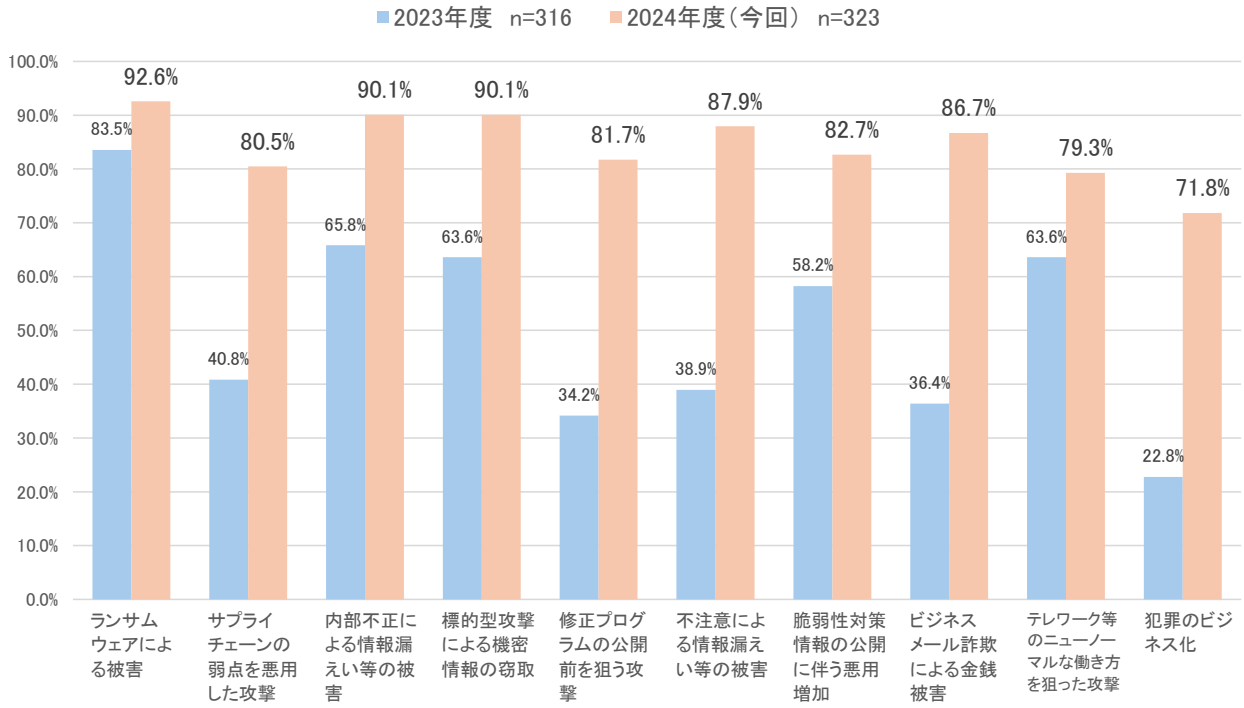

図 2.5-4　会員顧客企業におけるセキュリティ脅威の理解の変化

会員顧客企業における「情報セキュリティ 10 大脅威」の理解について、前年度調査結果と比較したのが図 2.5-4 である。※今回調査結果では「把握しており対策している」と「把握しているが対策をしていない」を合計し「把握している」として集計した。

今年度の調査では、すべての項目の理解が 7 割を超えており、すべての項目で理解度は上昇していた。なかでも、前年度から大きく理解度が上がっていたのは、「ビジネスメール詐欺による金銭被害」（プラス 50.3 ポイント）、「不注意による情報漏えい等の被害」および「犯罪のビジネス化（アンダーグラウンドサービス）」（ともにプラス 49.0 ポイント）であった。

2.5.2 インシデントが発生した際の想定される相談先

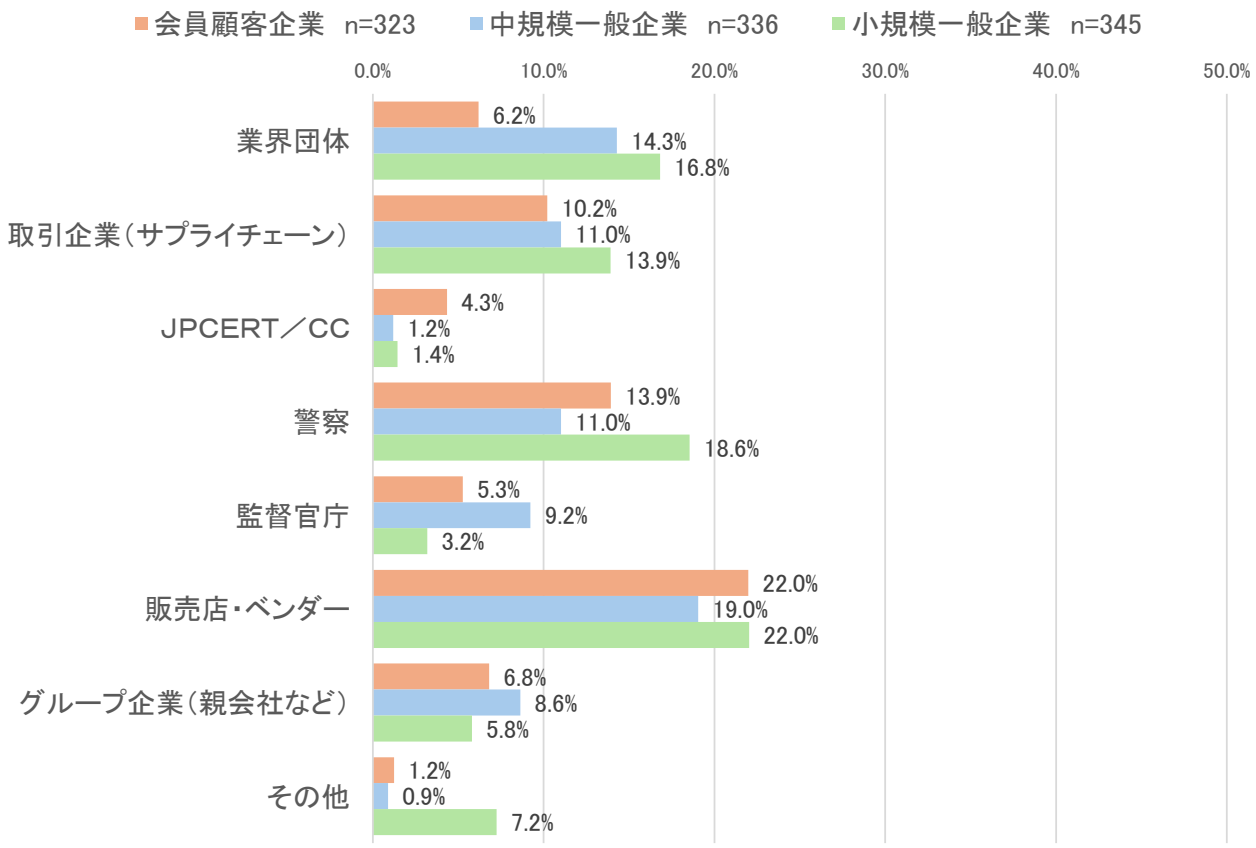

図 2.5-5　インシデントが発生した際の想定される相談先

前節の「情報セキュリティ 10 大脅威」に関するインシデントが発生した際に想定される相談先を聞いた結果が図 2.5-5 である。

会員顧客企業では、「販売店・ベンダー」（22.0%）、「警察」（13.9%）、「取引企業（サプライチェーン）」（10.2%）の順で相談先としてあげられていた。

中規模一般企業では、「販売店・ベンダー」（19.0%）、「業界団体」（14.3%）、「取引企業（サプライチェーン）」・「警察」（11.0%）の順であった。

小規模一般企業では、「販売店・ベンダー」（22.0%）、「警察」（18.6%）、「業界団体」（16.8%）の順であった。

2.6 セキュリティ対策への課題、投資状況

- セキュリティ対策未実施企業の課題としては、会員顧客企業では「リソース不足」、一般企業では「コスト、経済的な制約」・「経営陣のセキュリティへの関心や意識」の割合が高い
- セキュリティ投資額は、会員顧客企業・中規模一般企業では「100 万円以上､300 万円未満」、小規模一般企業では「10 万円未満」の割合が高い
- セキュリティ投資額が多い業種は、会員顧客企業では「建設業」、中規模一般企業では「情報通信業」

2.6.1 セキュリティ対策未実施企業における課題

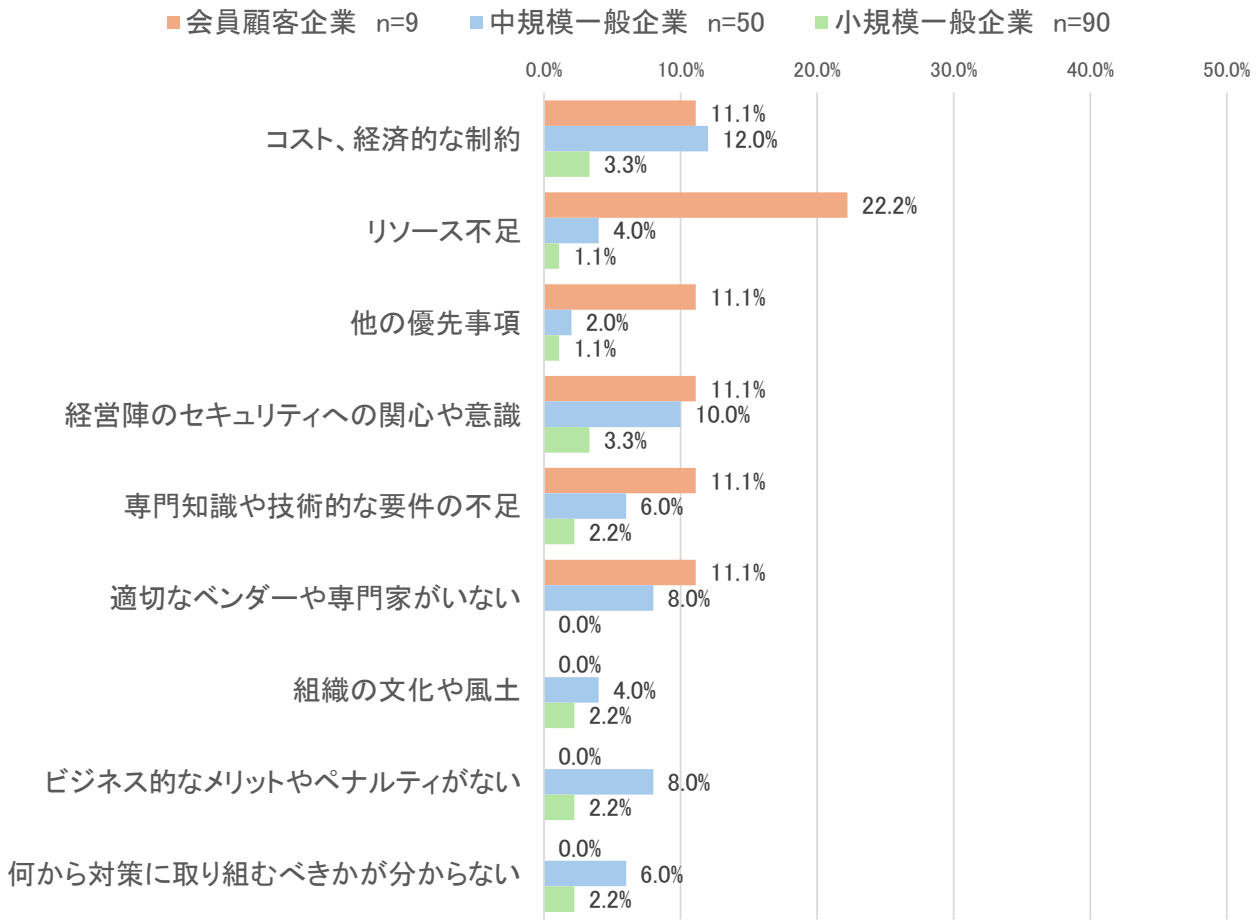

図 2.6-1 セキュリティ対策未実施企業における課題

セキュリティ対策未実施企業において、妨げとなっている課題を聞いた結果が図 2.6-1 である。

会員顧客企業では、「リソース不足」(22.2%) を 2 社があげていた。他には、「コスト、経済的な制約」・「他の優先事項」・「経営陣のセキュリティへの関心や意識」・「専門知識や技術的な要件の不足」・「適切なベンダーや専門家がいない」があげられている。

中規模一般企業においては、「コスト、経済的な制約」（12.0%）、「経営陣のセキュリティへの関心や意識」（10.0%）、「適切なベンダーや専門家がいない」・「ビジネス的なメリットやペナルティがない」（ともに 8.0%）があげられている。

小規模一般企業においては、「コスト、経済的な制約」・「経営陣のセキュリティへの関心や意識」（ともに 3.3%）、「専門知識や技術的な要件の不足」・「組織の文化や風土」・「ビジネス的なメリットやペナルティがない」・「何から対策に取り組むべきかが分からない」（ともに 2.2%）があげられている。

2.6.2 セキュリティ投資額

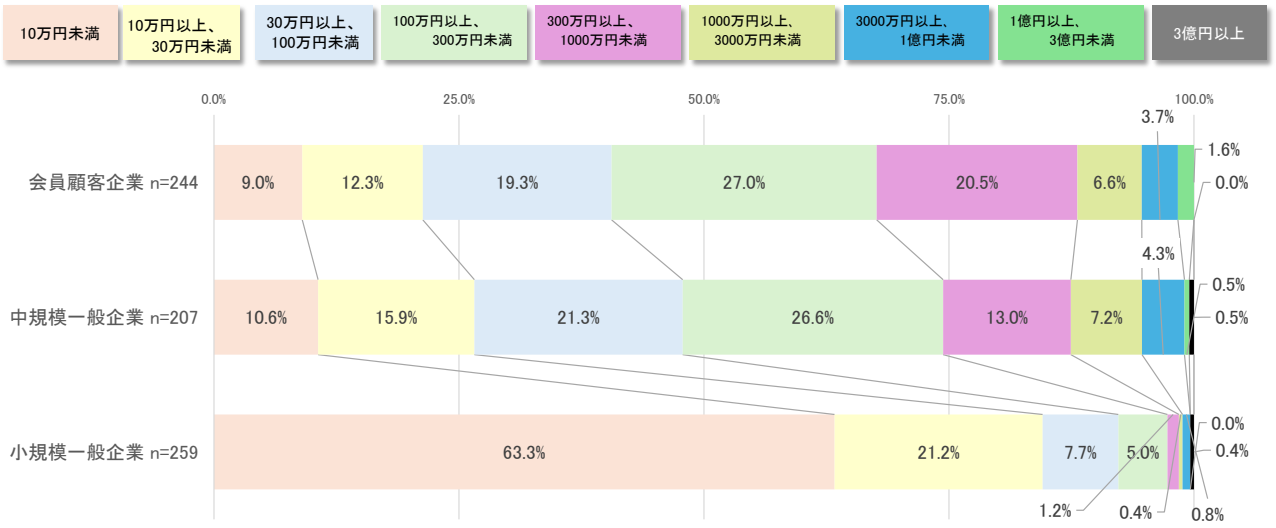

図 2.6-2　今年度のセキュリティ投資額

今年度のセキュリティに対する投資額を聞いた結果が図 2.6-2 である。

会員顧客企業では、「100 万円以上、300 万円未満」（27.0%）、「300 万円以上、1000 万円未満」（20.5%）、「30 万円以上、100 万円未満」（19.3%）であった。

中規模一般企業では、「100 万円以上、300 万円未満」（26.6%）、「30 万円以上、100 万円未満」（21.3%）、「10 万円以上、30 万円未満」（15.9%）であった。

小規模一般企業では、「10 万円未満」（63.3%）、「10 万円以上、30 万円未満」（21.2%）、「30 万円以上、100 万円未満」（7.7%）であった。

次に、セキュリティ投資額を業種別でみてみる。投資額については、「1000 万円未満」、「1000 万円-1 億円未満」、「1 億円以上」の 3 分類とする。

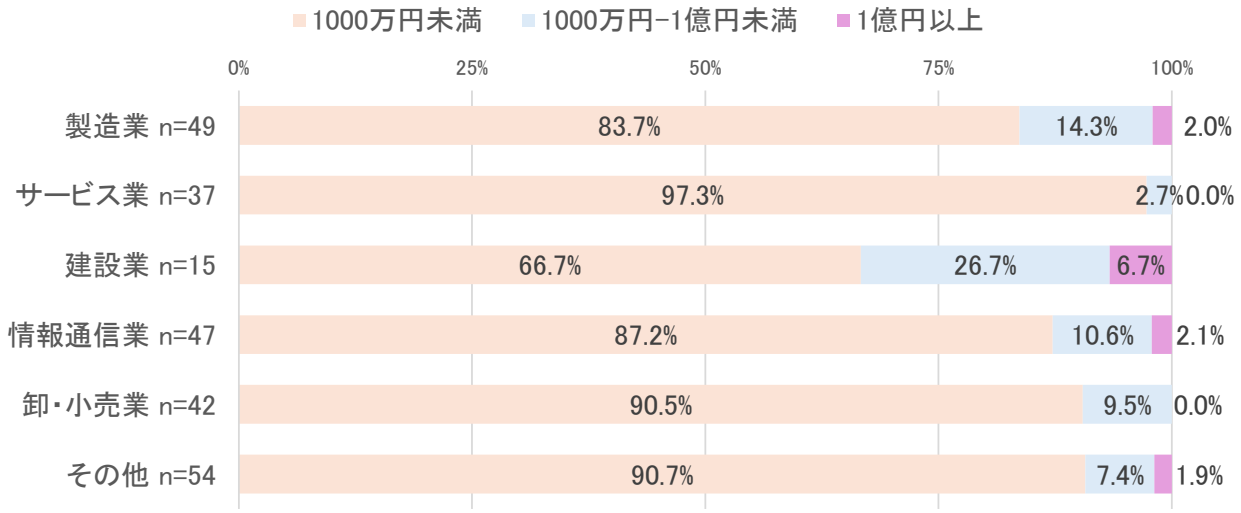

図 2.6-3　会員顧客企業（n=244）の業種別セキュリティ投資額

会員顧客企業（図　2.6-3）では、建設業でのセキュリティ投資額が多く、1000 万円以上（33.3%）の結果であった。

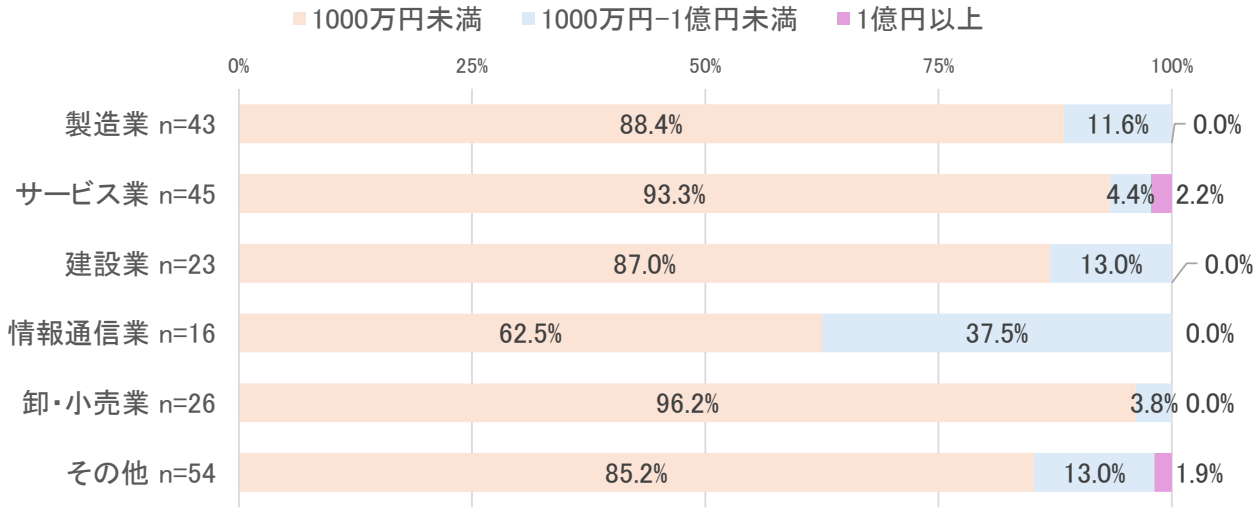

図 2.6-4　中規模一般企業（n=207）の業種別セキュリティ投資額

中規模一般企業（図　2.6-4）では、情報通信業でのセキュリティ投資額が多く、1000 万円以上（37.5%）の結果であった。

図 2.6-5　小規模一般企業（n=259）の業種別セキュリティ投資額

小規模一般企業（図 2.6-5）では、「サービス業」、「その他」を除き投資額は 1000 万円未満であった。