

2026年4月23日

「サイバーセキュリティ対策に関する企業調査（2026年）」について

常陽銀行（頭取 秋野 哲也）の子会社である常陽産業研究所（代表取締役社長 大森 範久）は、このたび、「サイバーセキュリティ対策に関する企業調査（2026年）」をとりまとめましたので、その結果を下記のとおりお知らせいたします。

当社は、地域のシンクタンクとして各種調査研究および総合金融サービスの提供を通じ、今後とも、地域の課題解決のためのさまざまな情報発信および取り組みを展開し、地域の成長と活性化に貢献してまいります。

常陽銀行グループでは、同じく常陽銀行の子会社である常陽コンピューターサービス（代表取締役社長 五來 雄二）とも連携し、本調査で明らかとなった課題を踏まえ、今後も地域企業のサイバーリスク低減に貢献してまいります。

記

1. 調査結果

近年、国内企業へのサイバー攻撃の被害が相次いでおり、企業規模に関わらず、サプライチェーン全体での対策が不可欠となっています。政府においても、経済産業省などを中心にサイバーセキュリティ対策をさらに推し進めていく見通しにあります。対策の必要性が高まっている背景から、当社では、2026年3月、茨城県内企業を対象に、サイバーセキュリティ対策の実施状況を調査しました。

調査によると、サイバーセキュリティへの対策について、全産業で77.2%が「取り組んでいる」と回答しました。ウイルス対策ソフト導入などの基本的な対策が進む一方、企業からは、コストや専門人員などのリソース不足により対応が困難であるといった声も聞かれています。なお、調査結果の詳細は別紙を参照してください。

2. 調査の特徴

本調査は、2026年3月2日～23日に茨城県内の企業を対象に実施したものです。有効回答数は193社（製造業86社、非製造業107社）でした。なお、従業員数300人以上の大企業から30人未満の企業まで、茨城県内企業を幅広く調査対象としています。

3. 地域企業のサイバーセキュリティ対策の実態

常陽コンピューターサービスでは、地域企業様へITソリューションサービスの提供を行う中で、本調査結果と同様のサイバーセキュリティ対策への課題を実感しています。地域企業ではウイルス対策などの初期対応は浸透しつつありますが、専門的な知見を要する最新の脅威への対策などについては、資金や人材の不足を理由に足踏みされている傾向にあります。今後は、こうした各社のリソース不足を補い、地域全体の実力を底上げする伴走型の支援がより一層求められると考えております。

【常陽銀行グループのサイバーリスク低減の取り組み】

常陽コンピューターサービスでは、以下のような地域企業のサイバーリスク低減に向けた取り組みを行っております。

特に、IT 専門人材の不足等により対策が進みにくい事業者さまに対し、分かりやすく実行可能な対策に重点をおいた支援に取り組んでおります。

主な取組内容

■サイバーセキュリティ現状診断・リスク可視化

事業者さまのIT環境や運用状況を整理し、潜在的なサイバーリスクを可視化するとともに、優先的に対応すべき課題の明確化を支援しております。

■ランサムウェア※¹対策支援

バックアップ対策、EDR※²導入、メールセキュリティ対策等を通じ、被害の未然防止および早期検知・迅速な復旧に向けた体制整備を支援しております。

※¹：近年被害が拡大しているサイバー攻撃のひとつ。悪意あるソフトウェアの一種で、悪意を持った第三者により、端末やサーバー内のデータを無断で暗号化し、そのデータの復元の条件として身代金などを要求するものを言います。

※²：EDR（Endpoint Detection and Response）は、サイバー攻撃による侵入を前提に“その後”の対応を強化するサイバーセキュリティ対策です。

■セキュリティ対策の段階的導入支援

企業規模や業種、予算に応じた無理のない段階的な対策導入を提案し、継続的なセキュリティ強化を支援しております。

以 上

本件に対するご照会は、下記までお願いいたします
常陽産業研究所 地域研究センター（中橋・荒澤） 029-233-6735
常陽コンピューターサービス 営業部（宮田・堀口）029-253-4419

【サイバーセキュリティ対策に関する企業調査（2026年）】

サイバーセキュリティ対策に「取り組んでいる」企業は約8割 —ウイルス対策ソフト等の導入が進むものの、専門人材育成やコスト面に課題—

今回調査の概要

サイバーセキュリティ対策に77.2%の企業が「取り組んでいる」と回答

サイバーセキュリティへの対策について「取り組んでいる」（「全社的に取り組んでいる」または「一部部署で取り組んでいる」）と回答した企業は77.2%であった（図表1）。

業種別にみると、「取り組んでいる」と回答した企業は、製造業で77.9%、非製造業で76.6%とほぼ同じであった。従業員規模別にみると、30人未満の企業で「取り組んでいない」（32.7%）の割合が、他の従業員規模を大きく上回った。

対策を開始したきっかけは、「他社のサイバー攻撃事例を見て」（59.0%）が最も多く、「DX化・IoT機器の導入」（35.3%）、「取引先からの依頼」（28.1%）と続いた（図表2-1）。「その他」（10.1%）と回答した企業の中には「自社が攻撃された経験がある」とコメントした企業もあり、サイバー攻撃は県内企業にとっても身近な脅威となっている。

ウイルス対策ソフト等の導入は84.5%、セキュリティ対策に係る人材育成は34.5%

実施している具体的な対策内容は、「ウイルス侵入防御ソフトの導入」（84.5%）が最も多く、「ファイアーウォールの設置」（54.2%）、「従業員向けのセキュリティ研修や訓練」（34.5%）と続いた（図表3-1）。ウイルス対策ソフト導入などの基本的な対策は多くの企業で取り組んでいる一方、セキュリティ対策に係る人材育成は約3割にとどまった。また、多要素認証^{※1}の導入など、より高度なセキュリティ対策は、総じて約1割と低い結果であった。

人材育成やコスト面・体制面に課題

対策に取り組んでいない企業の理由は、「専門人材の不足」（46.7%）が最も多く、「（対策ソフト等の）導入コストが高い」（43.3%）、「運用コストが高い」（26.7%）と続いた（図表4-1）。

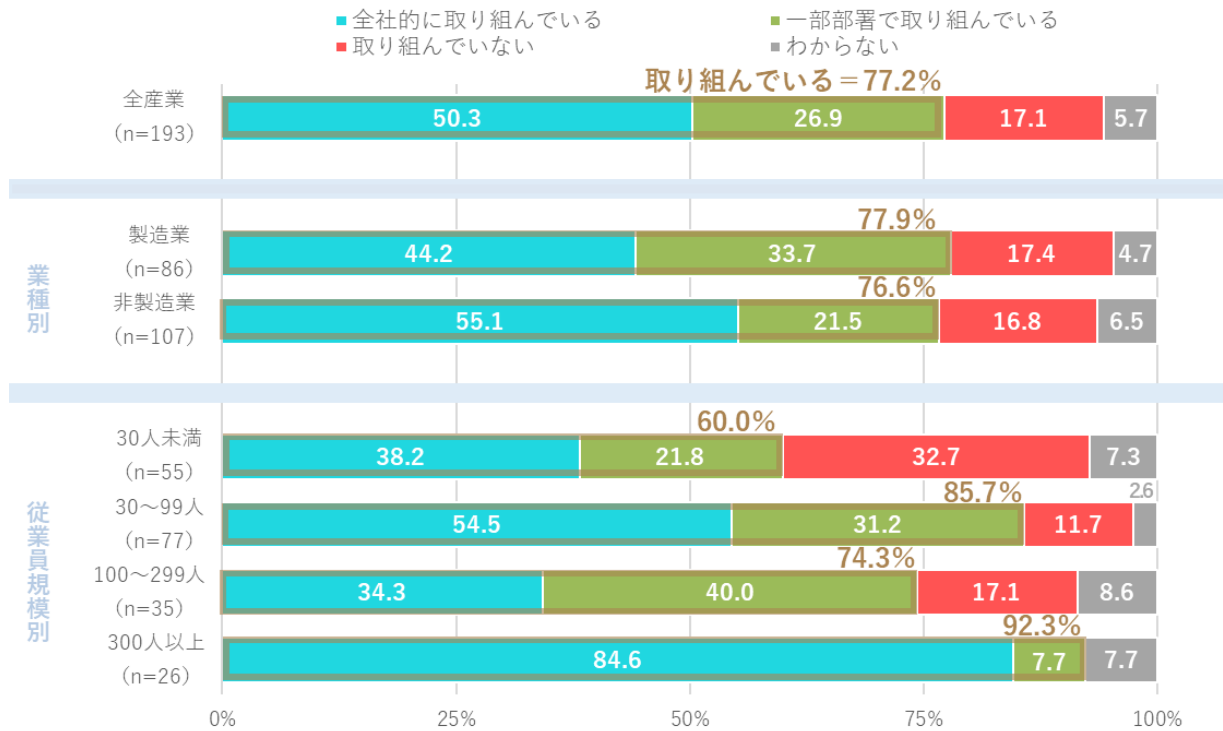
企業からは、「社内に教育に時間を割く余裕がない」（はん用機械製造業）、「社員向けの研修や訓練が不足している状況」（卸売業）など、人材育成の面での懸念を指摘する声が複数聞かれた。小規模企業からは「中小零細企業にセキュリティ強化を求めるのはコスト面・体制面から無理がある」（その他の製造業）など、リソース不足により対応が困難であるといった声が聞かれた。一方で、「セキュリティ対策評価制度^{※2}も意識した取り組みを実施している」（卸売業）など、経済産業省が開始を予定する新たな評価制度を見据えて動く企業もみられた。

リソース不足という課題はあるものの、こうした制度化の動きや、サイバー攻撃の増加・多様化を背景に、企業は規模を問わず対策を進めざるを得ない状況となるだろう。コストや専門人材不足に悩む中小企業が置き去りにならないよう、行政や支援機関等による実効性のある支援体制づくりが求められる。

※1：知識（パスワード）、所持（スマートフォン・カード）、生体（指紋・顔）の3つの要素から2つ以上を組み合わせる本人確認するセキュリティ手法。

※2：企業のサイバーセキュリティ対策状況を客観的に評価・可視化するための新しい仕組み。対策の熟練度に応じて星の数で格付け（5段階評価）。サプライチェーンに関わるほぼすべての企業が対象範囲に想定されている。

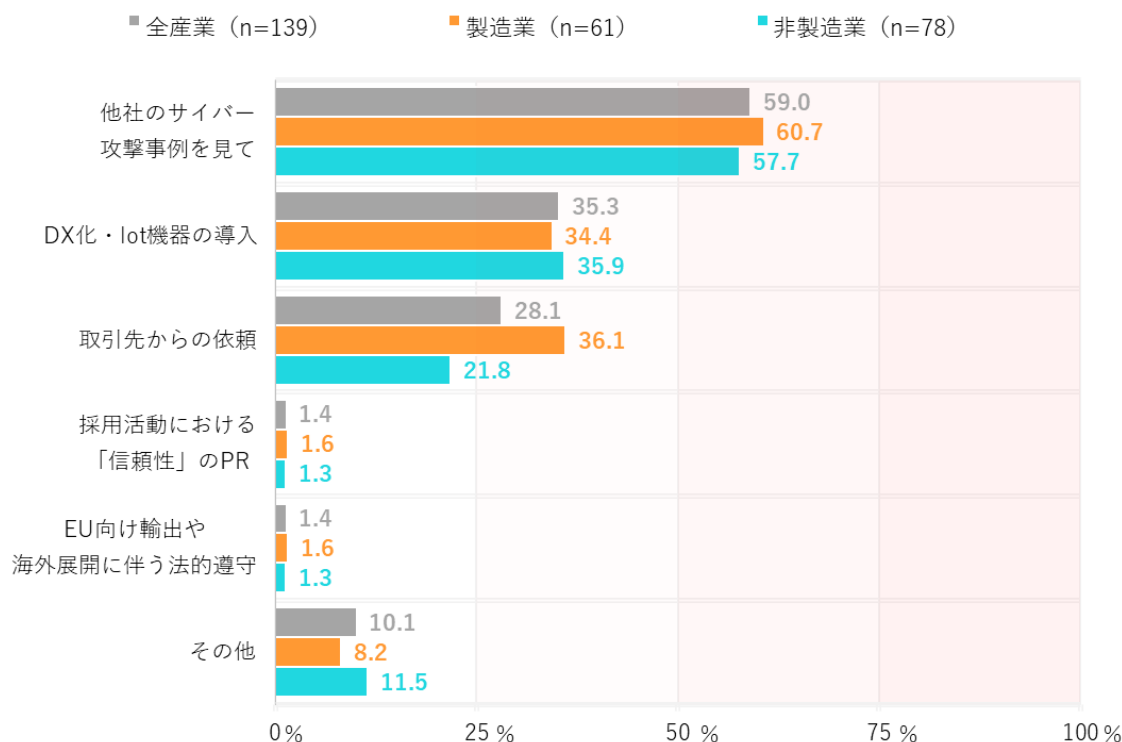
図表1 企業のサイバーセキュリティ対策への取り組み状況
(業種・従業員規模別)



※小数点以下第2位を四捨五入しているため、構成比の合計は必ずしも100とはならない

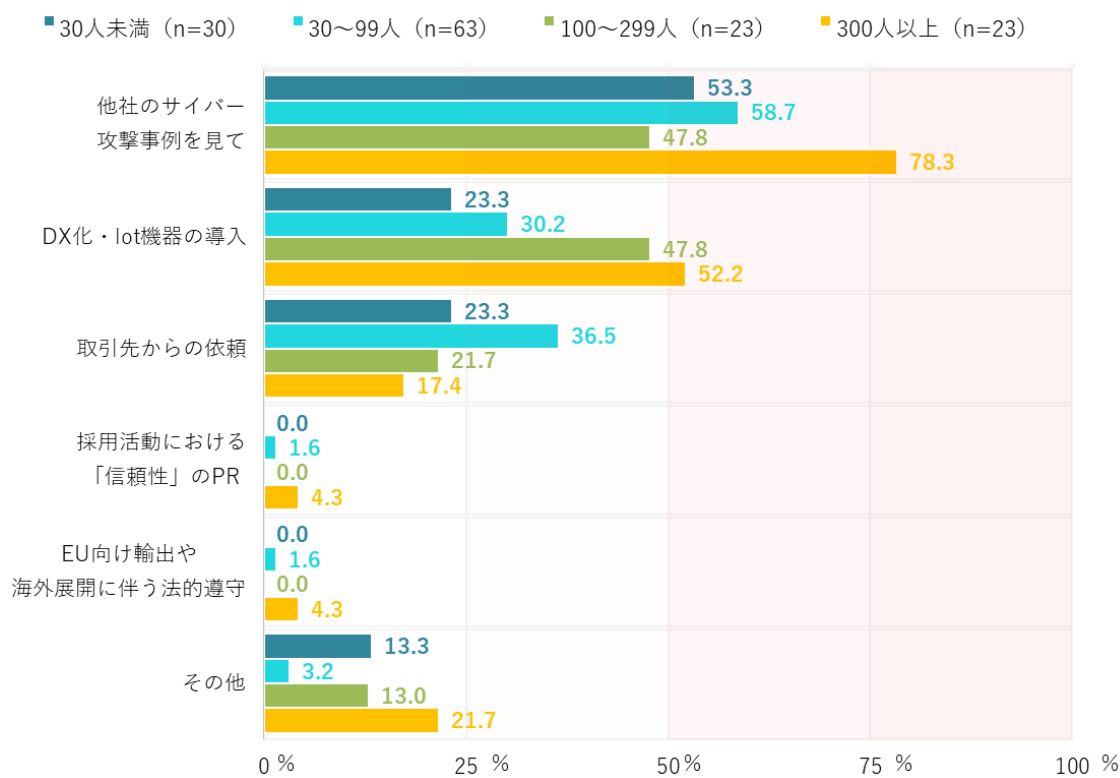
出所：常陽産業研究所「サイバーセキュリティ対策に関する企業調査（2026年）」

図表 2-1 サイバーセキュリティ対策を開始したきっかけ（業種別）



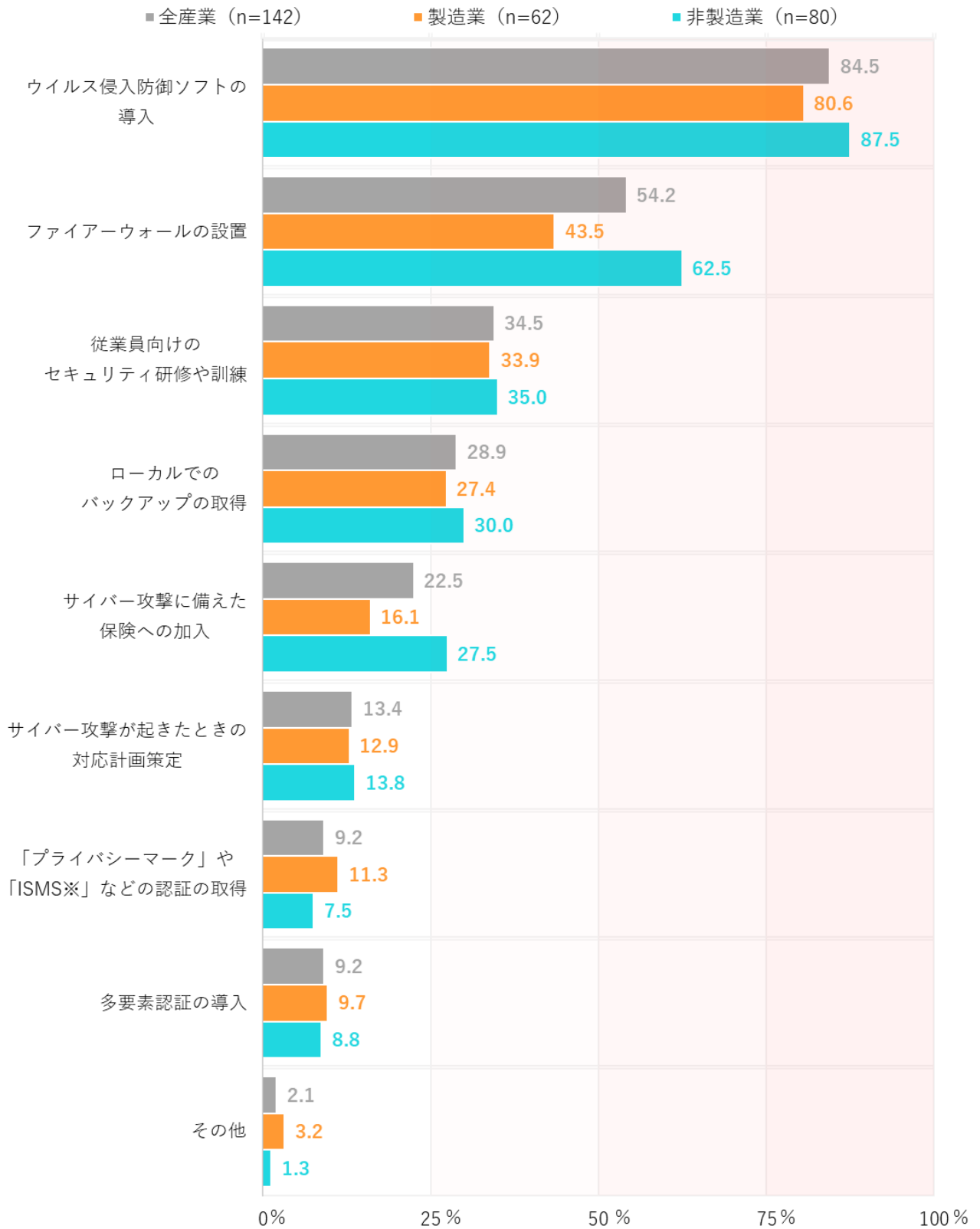
※複数回答（回答数制限なし） 出所：常陽産業研究所「サイバーセキュリティ対策に関する企業調査（2026年）」

図表 2-2 サイバーセキュリティ対策を開始したきっかけ（従業員規模別）



※複数回答（回答数制限なし） 出所：常陽産業研究所「サイバーセキュリティ対策に関する企業調査（2026年）」

図表 3-1 サイバーセキュリティで取り組んでいる内容（業種別）

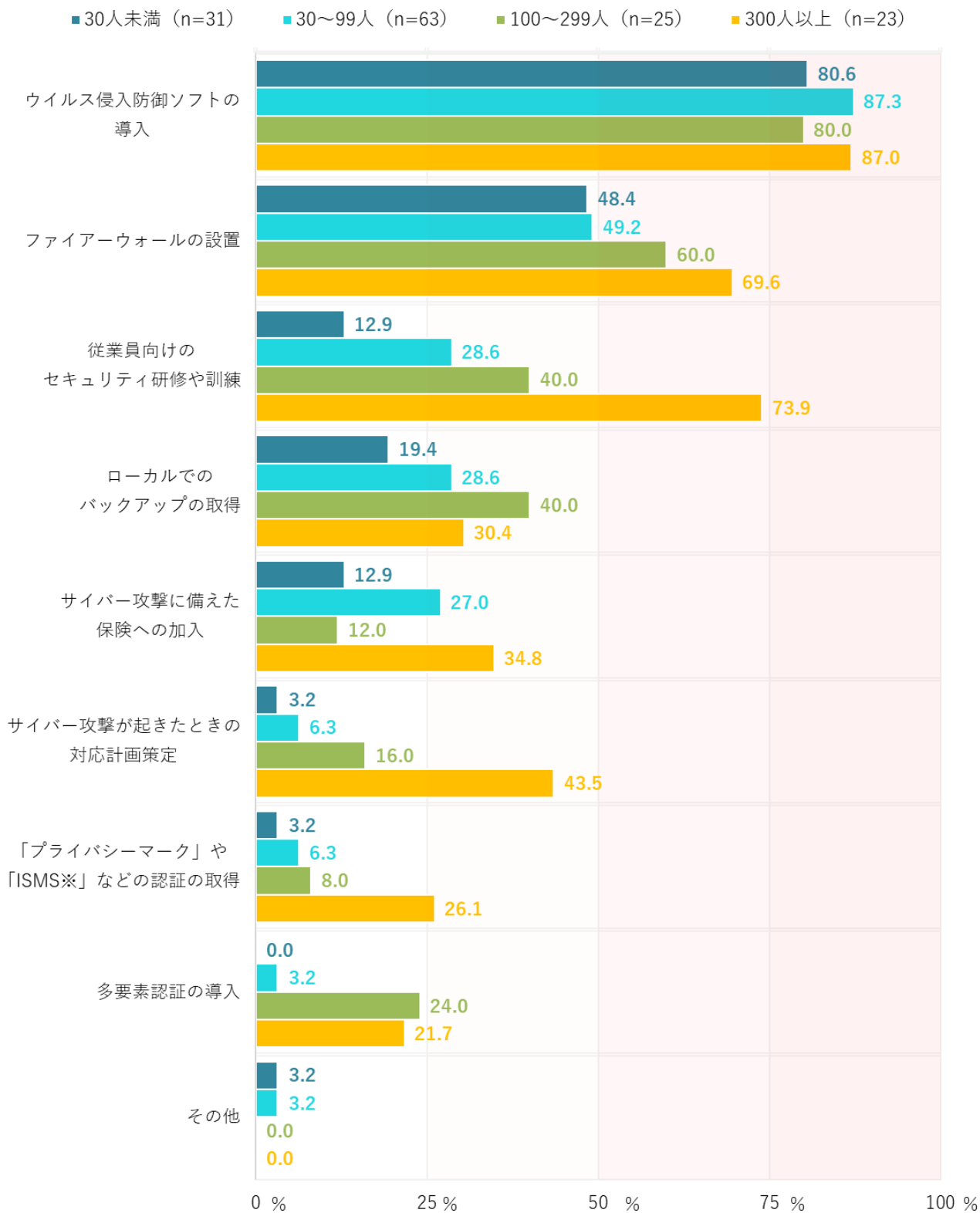


※「情報マネジメントシステム」の略

複数回答（回答数制限なし）

出所：常陽産業研究所「サイバーセキュリティ対策に関する企業調査（2026年）」

図表3-2 サイバーセキュリティで取り組んでいる内容（従業員規模別）

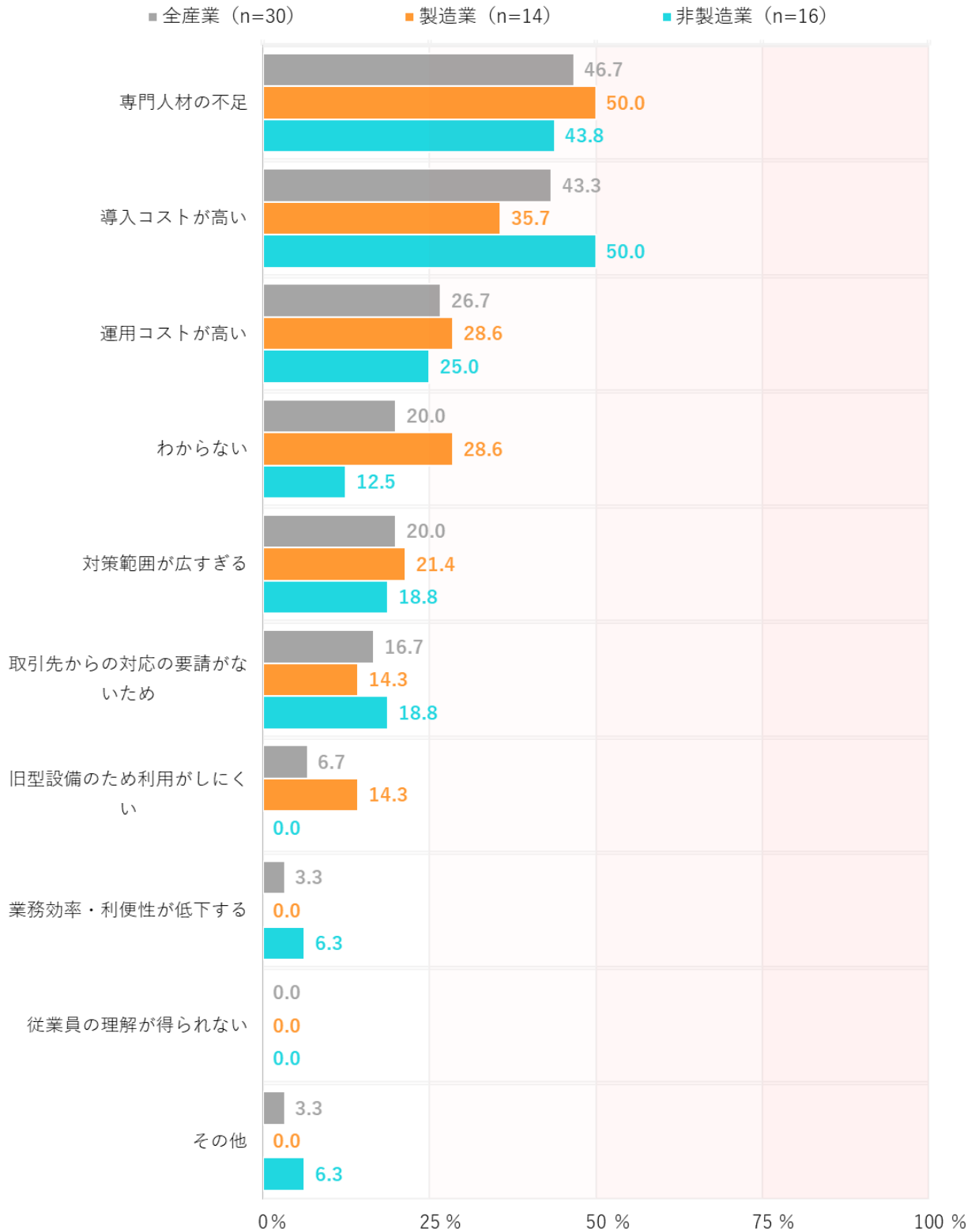


※「情報マネジメントシステム」の略

複数回答（回答数制限なし）

出所：常陽産業研究所「サイバーセキュリティ対策に関する企業調査（2026年）」

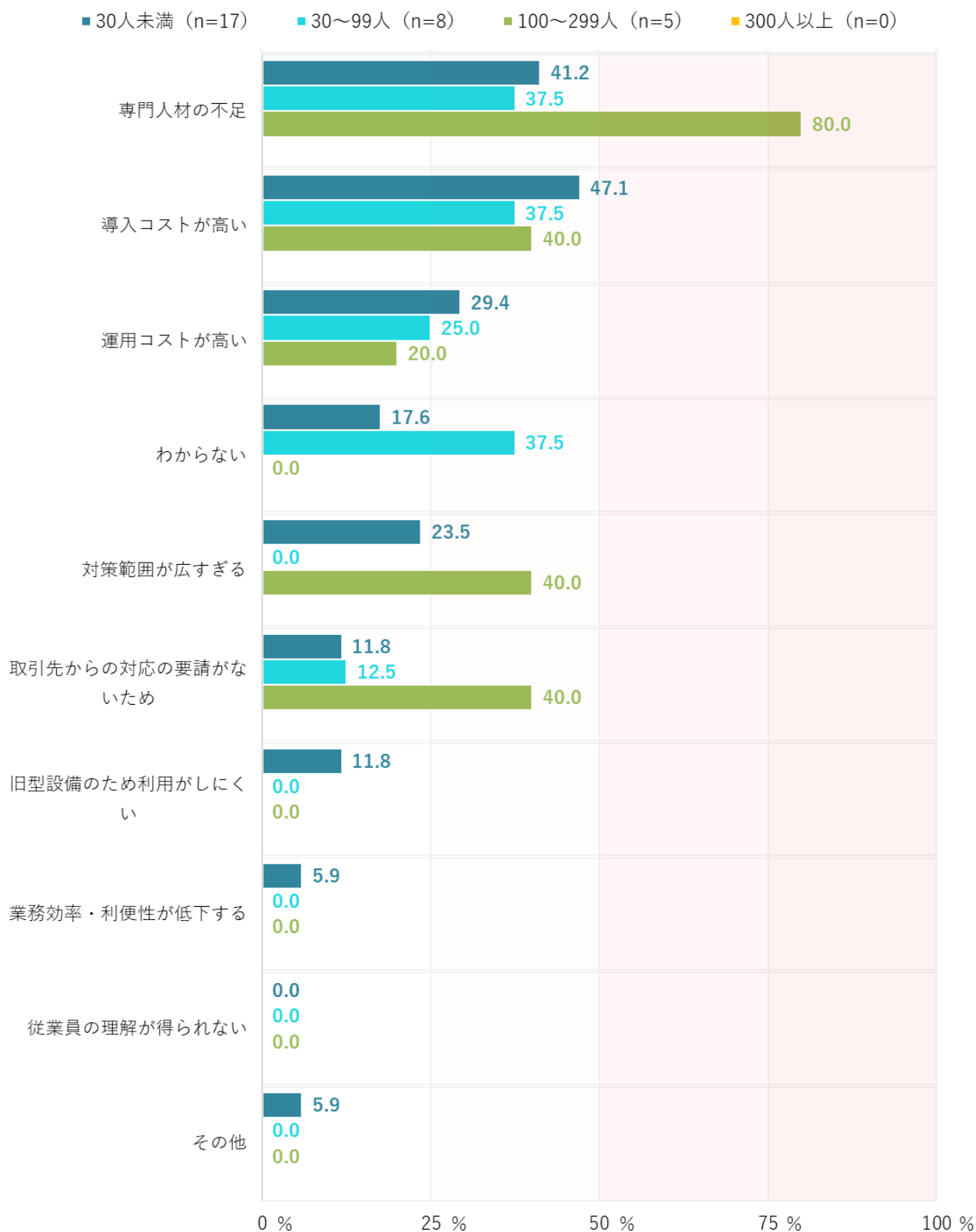
図表 4-1 サイバーセキュリティ対策に取り組んでいない理由（業種別）



※複数回答（回答数制限なし）

出所：常陽産業研究所「サイバーセキュリティ対策に関する企業調査（2026年）」

図表 4-2 サイバーセキュリティ対策に取り組んでいない理由（従業員規模別）



※複数回答（回答数制限なし）

出所：常陽産業研究所「サイバーセキュリティ対策に関する企業調査（2026年）」