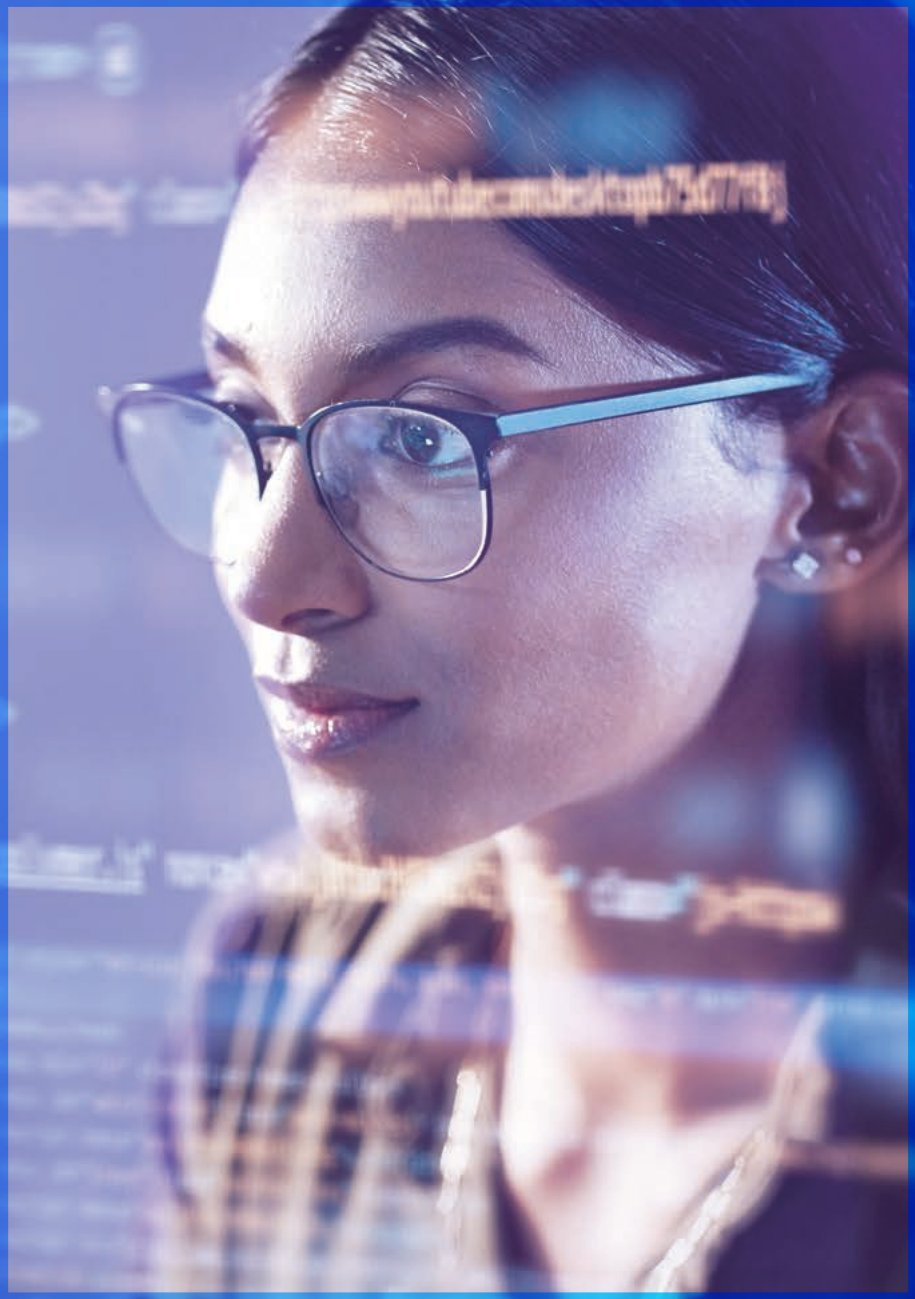
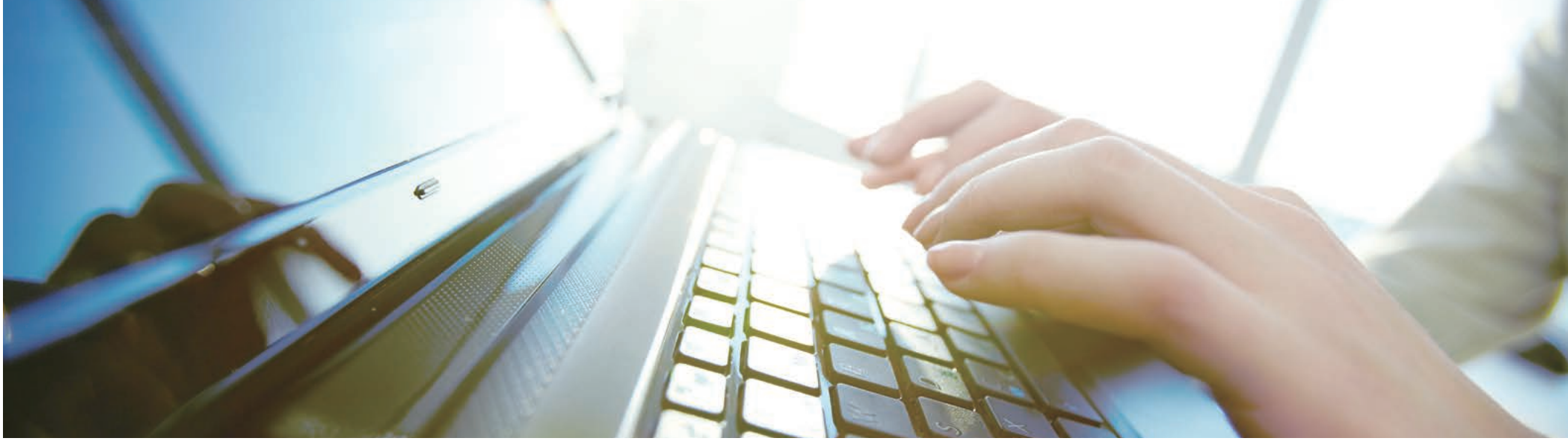
KPMG

サイバーセキュリティサーベイ 2023



Contents



ご挨拶

コロナ禍を経て社会のデジタル化が一段と進んだことに伴い、サイバー攻撃もより高度に、より巧妙になりました。代表例がランサムウェアによる攻撃で、新型コロナ前は個人への無差別攻撃で数十万円規模の支払いを求めるタイプが主流でしたが、現在は、脆弱性対策が不十分な企業を攻撃し、バックアップデータの暗号化、機密データの持ち出しによる二重脅迫など数千万円規模の身代金支払いを要求する攻撃が目立ち、産業界に喫緊の課題を突きつけています。

本調査においても、業務上の被害があったサイバーインシデントとしてランサムウェア攻撃を挙げた企業が最も多いという結果になりました。また、過去1年間に1,000万円以上の被害額が発生した企業が30%を占め、1億円以上の被害が発生した企業もサイバーセキュリティサーベイ2022（以降、「前回（2022年）の調査」という）の1.1%から6.7%に増加しています。

被害が大幅に拡大している半面、CISOの設置、SOCの整備、CSIRTの整備といったインシデント対応に備えた体制整備は進んでおらず、日本企業の対応の遅れが浮き彫りになりました。多くの企業がサイバーセキュリティ予算や人材の確保に苦労している状況も続いています。

海外子会社がサイバー攻撃を受ける事例が増えており、本調査では、海外子会社管理についての設問を設けました。結果は、海外子会社のセキュリティ対策について、40%程度の企業が子会社任せで親会社が十分に関与していない実態が明らかになりました。

さらに、今後、導入が加速するとされるAIに関する設問では、プライバシー、サイバーセキュリティ、ハルシネーションなどのリスクへの懸念が高いことがわかりました。

今回で6回目となる当社の「サイバーセキュリティサーベイ」は、サイバーセキュリティ促進のための有益な情報提供を目的に実施しており、皆様の組織のサイバーセキュリティ対策にお役立ていただけますと幸甚に存じます。

最後になりましたが、本調査の実施にあたり、回答にご協力いただいた皆様に心から御礼申し上げます。

2024年2月

KPMGコンサルティング株式会社
執行役員　パートナー
澤田 智輝

調査概要

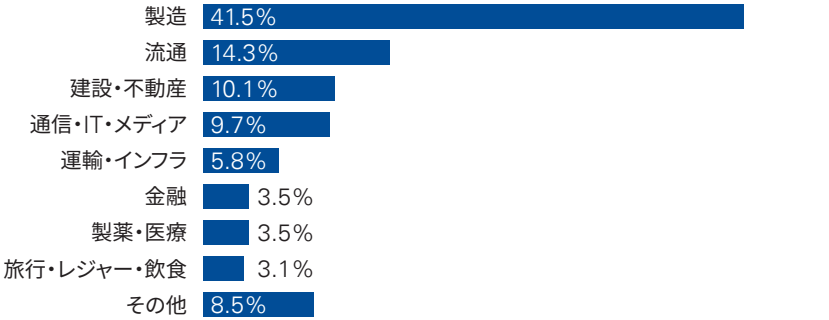
サーベイの概要

名称	企業のサイバーセキュリティに関する調査
対象	国内上場企業、および売上高400億円以上の未上場企業の サイバーセキュリティ責任者
調査期間	2023年6月9日～7月3日 ※7月7日着分までを集計対象として分析
調査方法	郵送によるアンケート票の送付・回収、 ウェブによるアンケートの回収
発送数	4,000件
有効回答数	258社（回収率6.5%）

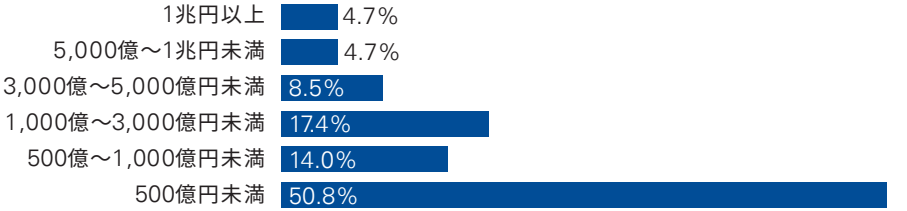
回答企業の属性

従業員数（連結）

業種



売上高（2022年度連結）



表記数値は小数点以下第2位を四捨五入しているため、パーセンテージ合計は100%とならない場合があります。

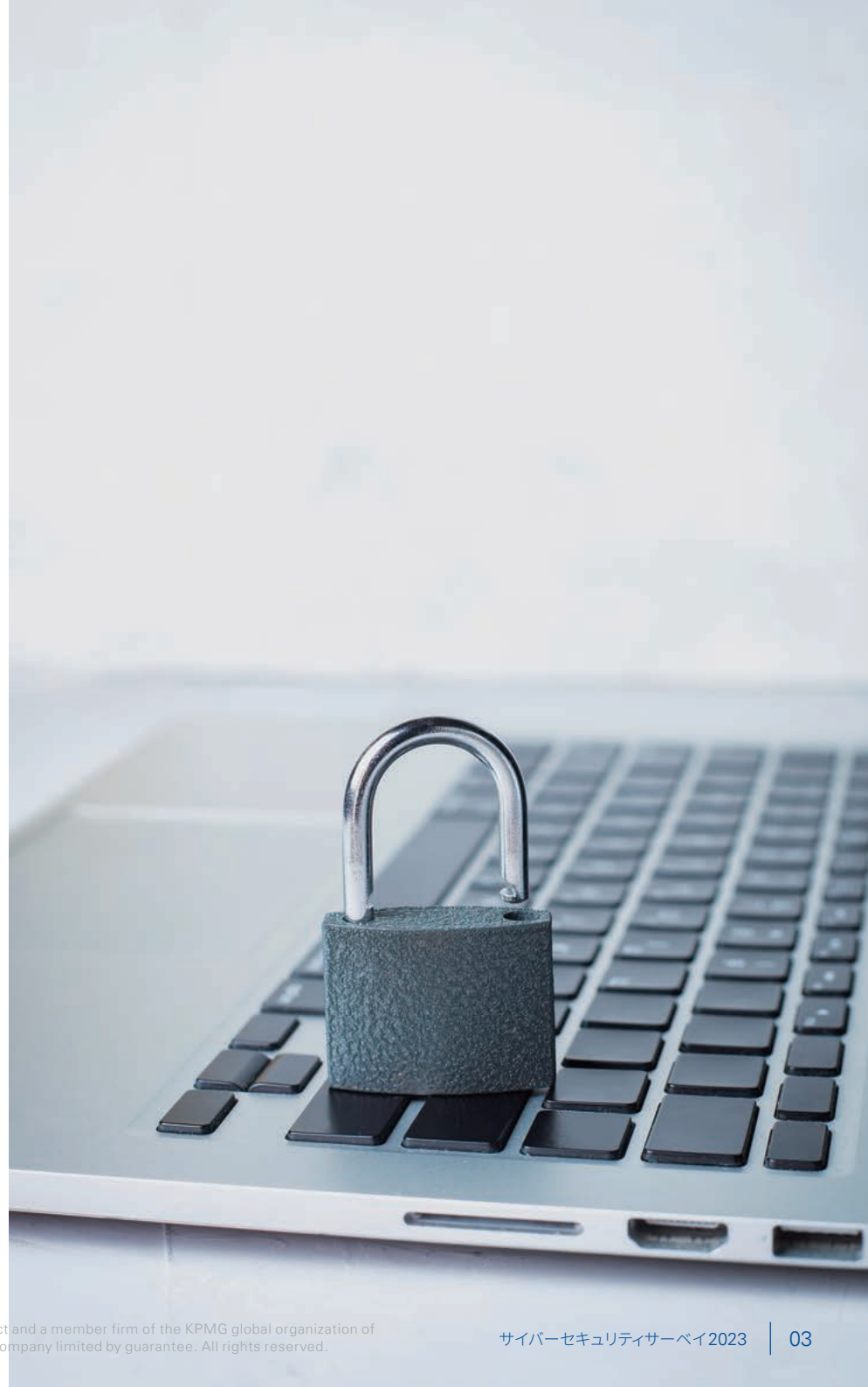
イントロダクション

本調査にて、過去1年間で10社に1社はサイバー攻撃の被害に遭ったことがあるとの回答を得ました。このような状況下において、サイバーセキュリティに関するリスクについて理解を深め、適時適切に対策を講じていくことは企業を「守る」うえで非常に重要な活動です。この“守り”を実践するためには、現状を把握し、どこにリスクが潜んでいるか理解することが重要です。

本調査では、従業員「1～499人」規模の企業から「1万人以上」の規模の企業まで、「製造」業や「金融」業など多種多様な企業258社から回答をいただきました。その結果を「1. サイバー攻撃の実態」「2. セキュリティ管理態勢と対策」「3. 海外子会社管理」「4. 制御システムセキュリティ」「5. AI導入およびAI導入に係るリスク管理」の5つにまとめています。200社を超える企業の回答から現状を俯瞰し、リスクが高まっている領域を知ることができます。

たとえば、本調査により、前回（2022年）の調査からサイバー攻撃被害額が増加していることや、子会社・委託先のシステムを経由したサイバー攻撃の手口、制御システムにおけるサイバーセキュリティ対策の遅れなど、現状のさまざまな事実がわかりました。

さらに、本調査では新たにAIの業務利用に関するリスクについても調査しています。昨今話題になっている生成AIの活用など、AIを業務に取り込む企業も増えてきました。「5. AI導入およびAI導入に係るリスク管理」では、AIの導入状況やリスク対策状況についてまとめています。セキュリティ監視やデータ分析、マーケティング活動にAIを導入済み、または導入を検討される企業が増えています。一方で、AIリスク管理について体系的に実施している企業は多くなく、今後の課題となることが予想されます。



エグゼクティブサマリー

テーマ 01
サイバー攻撃の実態

11.6%の企業が過去1年間にサイバー攻撃で何らかの業務上の被害があったと回答しています。また、1億円以上の被害があったと回答した企業の割合が前回（2022年）の調査と比べて大幅に増加するなど高額化の傾向にあり、サイバー攻撃への備えがより一層求められています。サイバー攻撃の侵入経路としては、子会社や委託先を経由したサイバー攻撃が直接的な攻撃の約2倍となっており、サプライチェーンでのセキュリティ強化にも目を向ける必要があります。

テーマ 02
セキュリティ管理態勢と対策

テーマ1（サイバー攻撃の実態）のとおり、サイバー攻撃の被害が拡大しており、企業には十分な対策が求められています。多くの企業がCISOもしくはサイバーセキュリティ責任者を設置し、セキュリティ組織体制を構築していますが、一方で、人員・予算の確保に苦慮していることがわかりました。また、SOCを導入していない企業は55.0%、CSIRTを設置していない企業は72.7%となるなど、セキュリティインシデント発生に備えた体制の整備としては改善の余地が残っています。

テーマ 03
海外子会社管理

昨今、海外子会社がサイバー攻撃の被害に遭うケースが増えており、セキュリティ対策強化を検討する必要があります。現状は、40%程度の企業において、海外子会社のセキュリティ対策状況を確認していないと回答しており、早急に実態把握から進める必要があります。また、高度なエンドポイントセキュリティ対策は、32.7%の企業がすべての海外子会社に実施を要請していますが、本社にて十分な対策ができているという企業は27.5%にとどまるなど、海外子会社への要請と、本社での取組みに整合性が取れていない対策があることもわかりました。

テーマ 04
制御システムセキュリティ

制御システムを利用している企業の40%強で、「成熟度レベル1：サイバーセキュリティのプロセスは未整理で文書化されておらず、活動も整理されていない」と回答しています。海外で行ったサーベイでは、成熟度レベル1は16.0%にとどまっており、日本の活動が海外と比べ大幅に遅れていることがうかがえます。ITセキュリティと同様に、制御システムにおいても知見・人的リソースの不足が最も大きな課題となっています。ただし、前回（2022年）の調査の結果と比較して、セキュリティ対策が全体的に進んでいることが見受けられます。

テーマ 05
AI導入およびAI導入に係るリスク管理

AI導入について、導入済み・計画ありと回答した企業は70%程度でした。特に「質問・問合せへのアシスト」、「データ分析」では多くの企業が導入・前向きに検討しています。一方で「採用活動」、「人事評価」では前向きな回答は10%程度にとどまり、プライバシー情報の取扱いに十分な配慮が必要であったり、人間の判断要素が大きいと考えられている分野ではAI導入に抵抗感があったりすることがことがうかがえます。AI導入に係るリスクについて、約30%の企業において「プライバシー侵害」、「アウトプットの正確性」、「不正もしくは有害な利用」を非常に懸念していると回答していますが、AIリスク管理について「整備済み」と回答した企業は4.3%にとどまり、AIリスク管理の整備が遅れている状況がうかがえます。

テーマ 01

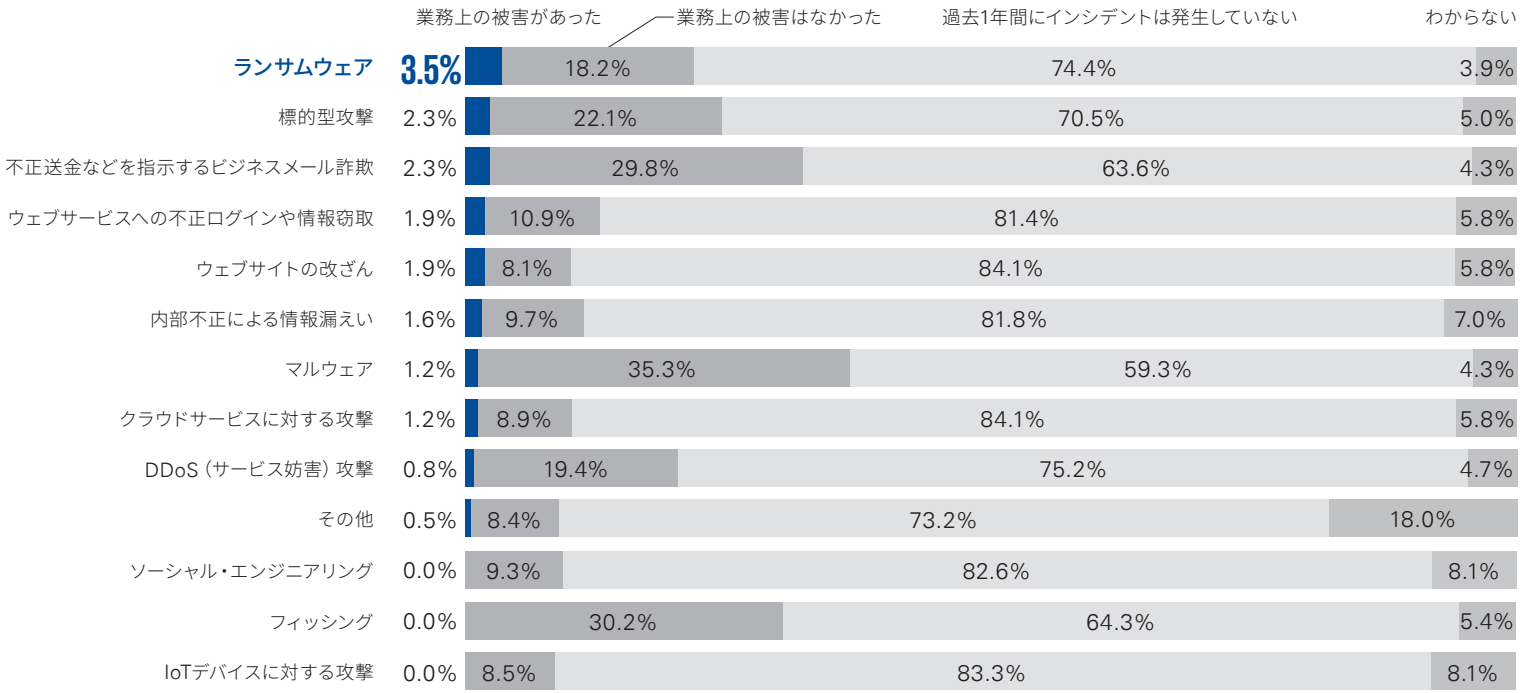
サイバー攻撃の実態

サイバー攻撃の発生状況と攻撃手法

過去1年間でサイバー攻撃により業務上の被害があった企業は30社あり、回答企業258社の11.6%にのぼります。攻撃手法としては「ランサムウェア」が3.5%と最も多く、「ランサムウェア」による攻撃を受けた企業56社のうち業務上の被害があった企業は9社で16.1%にのぼることから、ランサムウェアは実被害を与える攻撃手法として比較的効果が高く、今後も継続してインシデント発生に備える必要があります。
また、「不正送金などを指示するビジネスメール詐欺」、「マルウェア」、「フィッシング」は、業務上の被害に遭った割合は高くはないものの、これらのサイバー攻撃を回答企業の30%以上が受けていることがわかります。技術的な対策のみで防御することは限界があるため、教育・訓練によりセキュリティ意識を高めるなど、ヒューマンリスクを少なくする活動が不可欠です。

過去1年間に発生したサイバーインシデントをもたらした直接的な要因（攻撃手法）

過去1年間で業務上の被害をもたらしたサイバー攻撃は「ランサムウェア」が最も多い。



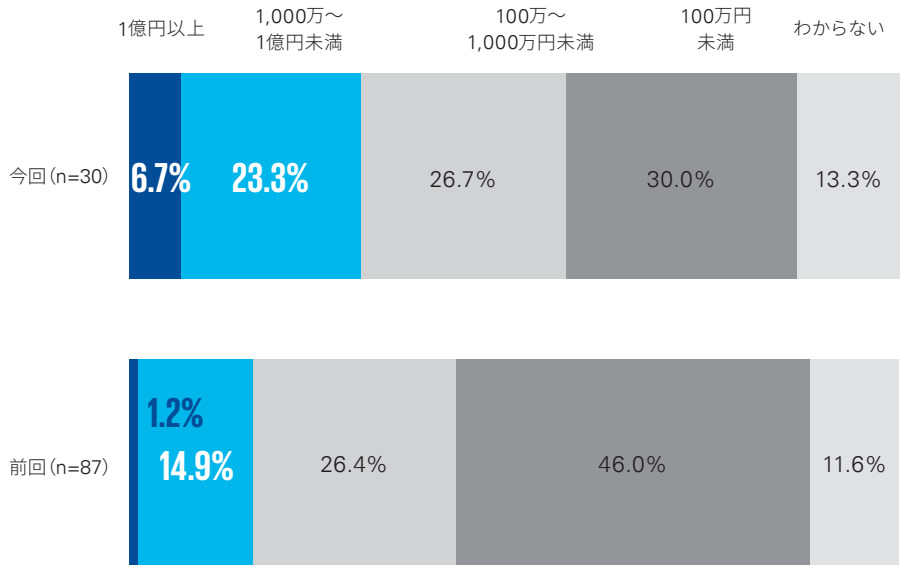
n=258

サイバーインシデントによる被害

サイバーインシデントによる被害額は、前回（2022年）の調査と比較して「1億円以上」が1.2%から6.7%、「1,000万円～1億円未満」が14.9%から23.3%と急激に高額化しています。
過去1年間に発生したサイバーインシデントの被害の特徴としては、「自社の業務やシステムが著しく遅延・中断した」（40.0%）、「自社に経済的な損失が発生した」（33.3%）と回答した企業の割合が高いことに加え、機密情報が漏えいしたという回答が急激に増加していることが特徴的です。機密情報の搾取などサイバー攻撃のビジネス化が加速し、企業のビジネスに大きな被害を及ぼしていることがうかがえます。

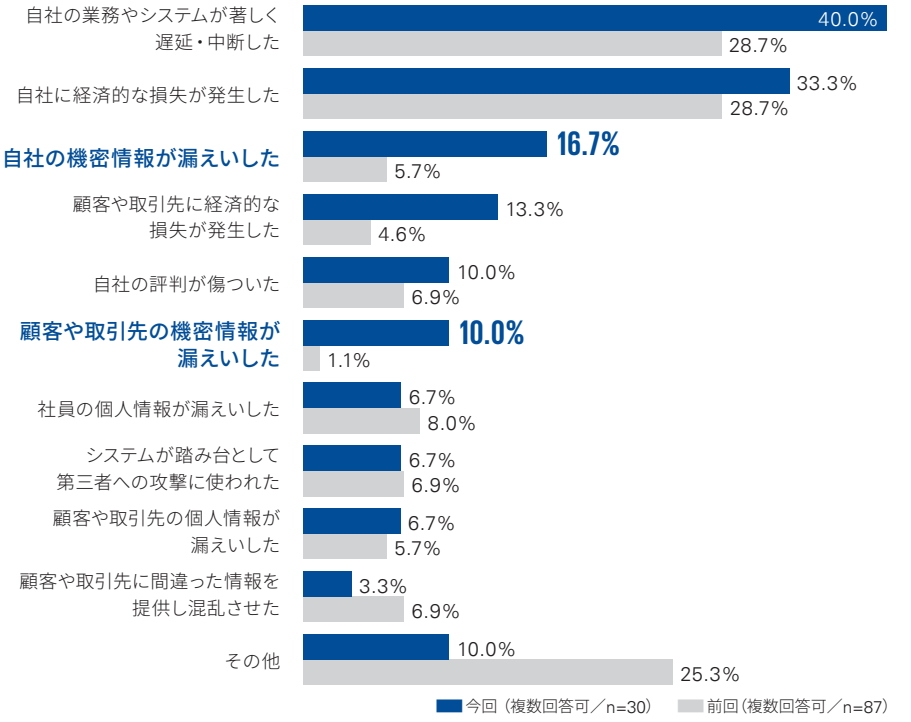
過去1年間に発生したサイバーインシデントの合計被害額

1,000万円以上の被害に遭ったと回答する企業が30.0%を占め、被害額は前回（2022年）の調査と比較して増加している傾向にある。



過去1年間に発生したサイバーインシデントによる被害内容

「自社の機密情報が漏えいした」、「顧客や取引先の機密情報が漏えいした」という回答が急激に増加している。

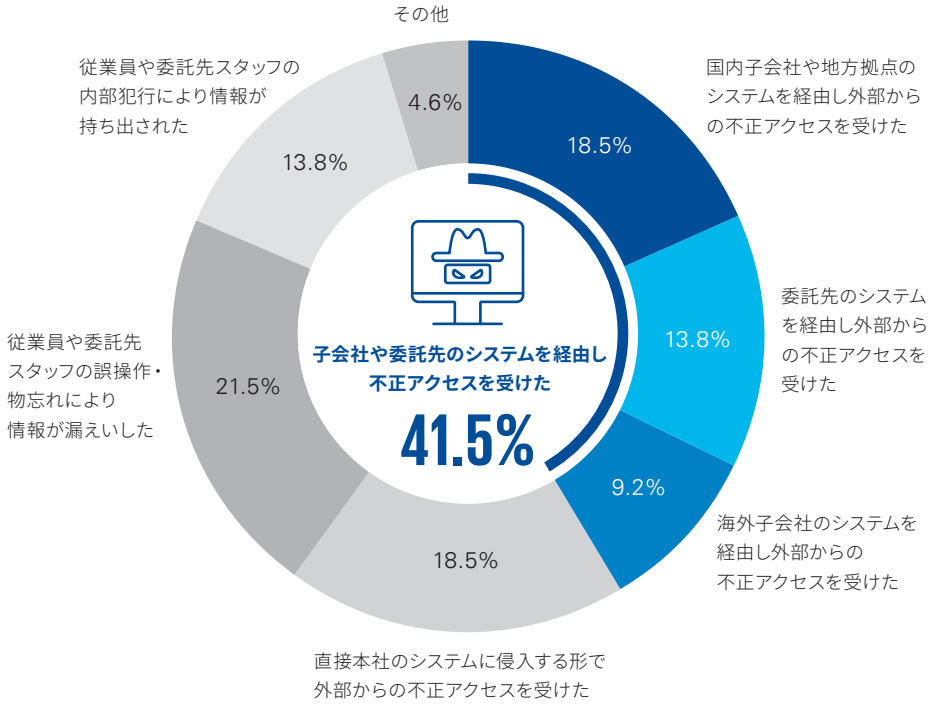


サイバー攻撃の侵入経路

過去1年間に発生したサイバー攻撃では、子会社や委託先のシステムを経由した攻撃が41.5%を占めており、直接本社のシステムを攻撃する経路の約2倍になっています。本社における対策のみならず、子会社や委託先を含めたサプライチェーンにまで目を向け、侵入経路の抜け道ができないようにセキュリティ対策を強化する必要があります。

過去1年間に発生したサイバー攻撃の侵入経路

子会社や委託先のシステムを経由しての攻撃が41.5%を占めている。



n=65

テーマ 02

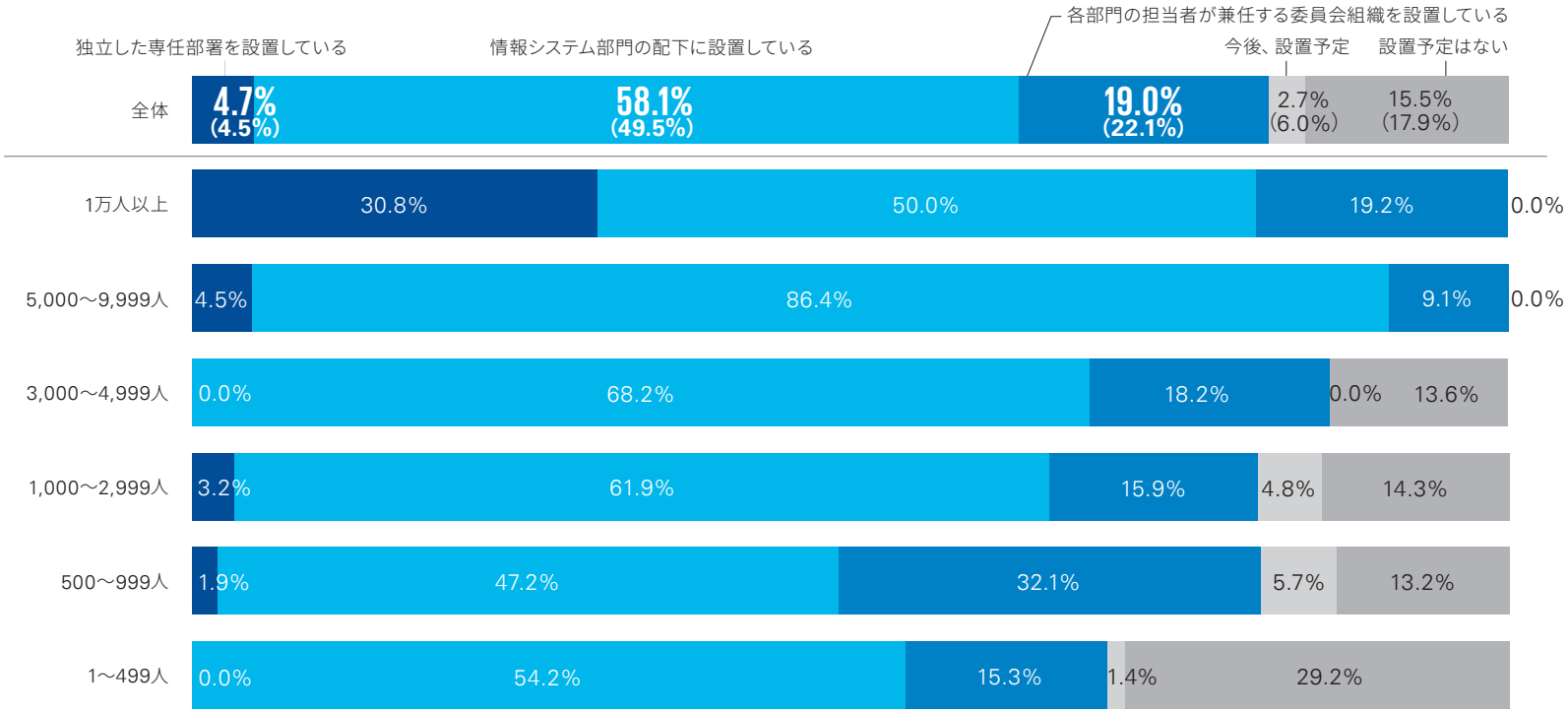
セキュリティ管理態勢と対策

サイバーセキュリティ組織体制

サイバーセキュリティ組織を設置している企業の割合は81.8%にのぼります。従業員数が多いほど設置している割合は高くなる傾向にあり、5,000人以上の企業ではすべての企業でサイバーセキュリティ組織を設置しており、1万人以上の企業では30.8%が独立した専任部署を設置しています。一方で1～499人の企業では29.2%が「設置する予定はない」と回答しています。従業員数が多い企業ではセキュリティ対策に投じる予算やリソースに余裕があること、業界規制への対応が求められるなどの理由から組織整備が進んでいる一方で、従業員数が少ない企業ではリソースや投資対効果などの理由から組織整備が進んでいない現状がうかがえます。

サイバーセキュリティ組織の設置状況

回答企業の81.8%がセキュリティ組織を整備しており、前回（2022年）の調査結果（76.1%）よりも組織整備が進んでいる。



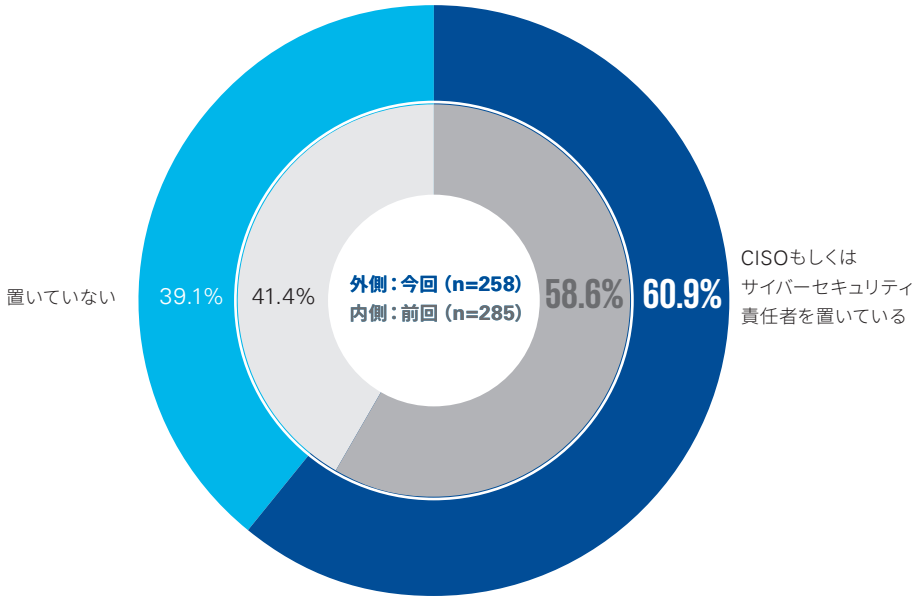
今回（n=258）／（）内は前回（2022年）の調査数値（n=285）

CISOの設置

回答企業の60.9%が最高情報セキュリティ責任者（CISO）もしくはサイバーセキュリティ責任者を設置しています。
1万人以上の企業では、84.7%が最高情報セキュリティ責任者（CISO）もしくはサイバーセキュリティ責任者を設置していますが、それ以下の企業では50%から60%にとどまります。

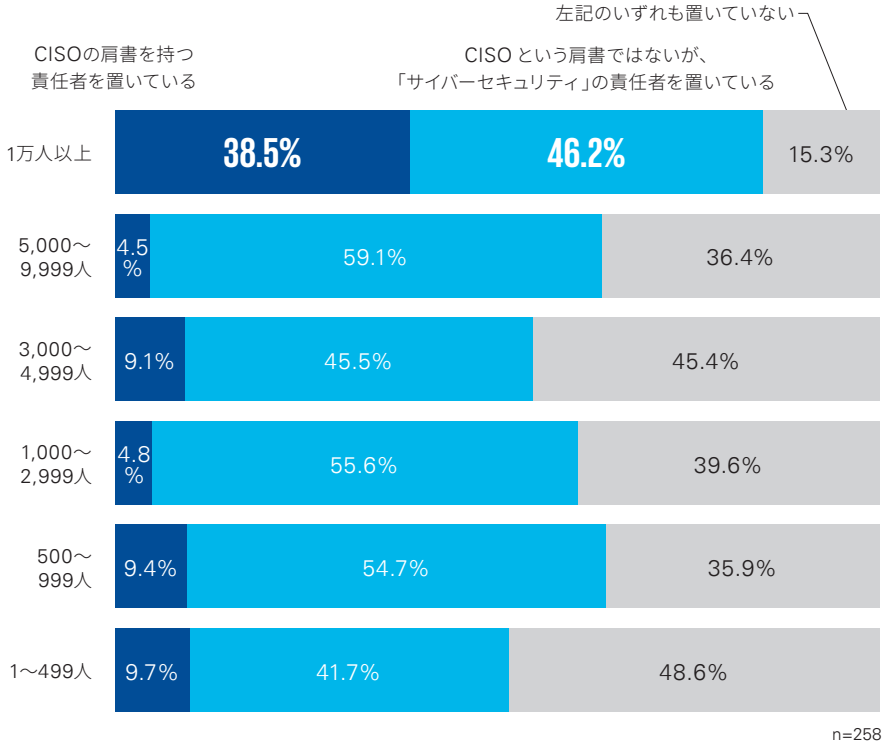
CISOもしくはサイバーセキュリティ責任者の設置状況（全体）

前回（2022年）の調査と同様に回答企業の60%程度がCISOもしくはサイバーセキュリティ責任者を設置している。



CISOもしくはサイバーセキュリティ責任者の設置状況（従業員数別）

1万人以上の企業では84.7%がCISOもしくはサイバーセキュリティ責任者を設置している。



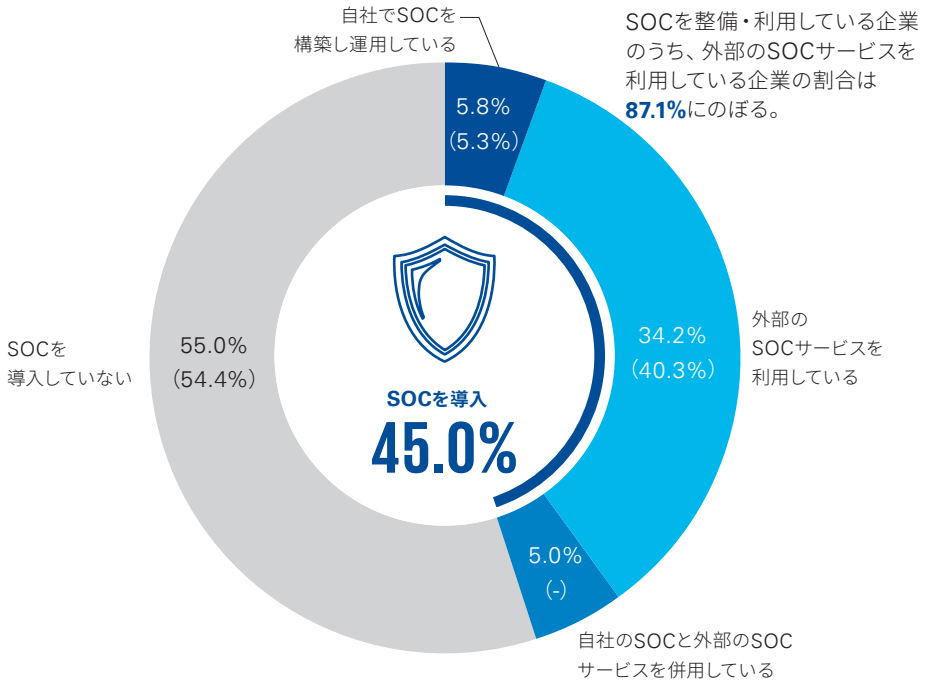
n=258

SOCの整備

回答企業の45.0%が何らかの形でSOC（Security Operation Center）を導入しており、そのうち外部のSOCサービスを利用している割合は87.1%にのぼります。SOCの整備には機材や施設、専門人材の確保を要するため、積極的に外部サービスを活用していることがうかがえます。
監視している攻撃としては、「不審なウェブサイトへのアクセス・閲覧」、「EDR製品によるマルウェアの挙動」、「インターネットからの攻撃性の高いアクセス」といった従前からよく監視されている事項が並びます。また、前回（2022年）の調査と同様にクラウドサービスに対する監視は少数にとどまります。
クラウドサービスに対する監視を強化するためにクラウドサービスやシステム特性を踏まえたうえで、CSPM（Cloud Security Posture Management）やCWPP（Cloud Workload Protection Platform）などのソリューションを検討することが望まれます。

SOCの整備状況

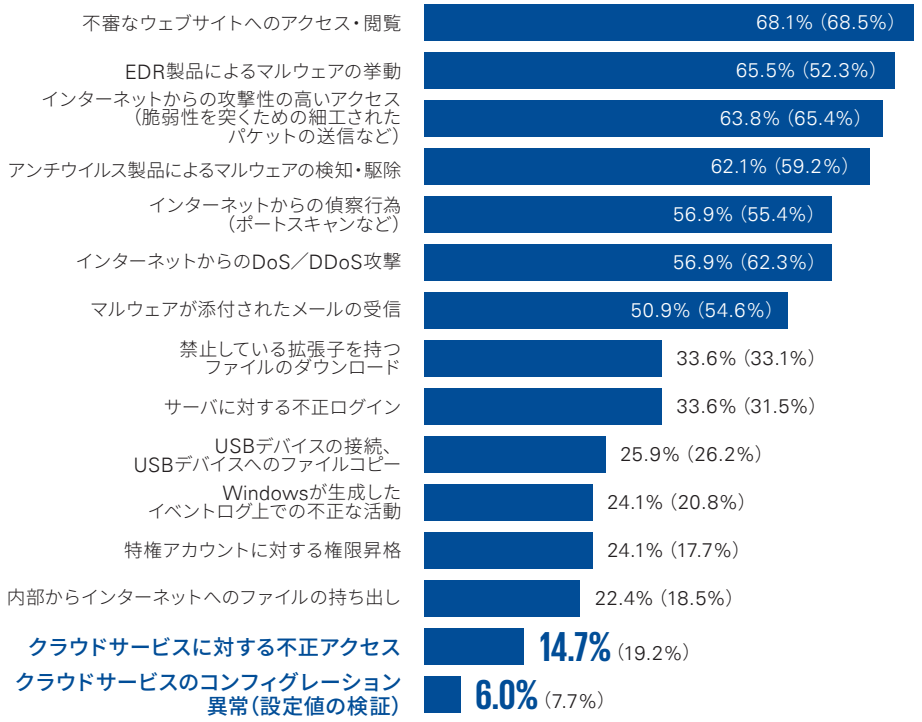
回答企業の45.0%がSOCを導入しており、そのうち87.1%が外部サービスを利用している。



今回（n=258）／（）内は前回（2022年）の調査数値（n=285）

SOCで検知しているセキュリティイベント

「クラウドサービスに対する不正アクセス」、「クラウドサービスのコンフィグレーション異常（設定値の検証）」の検知は15.0%に満たない。



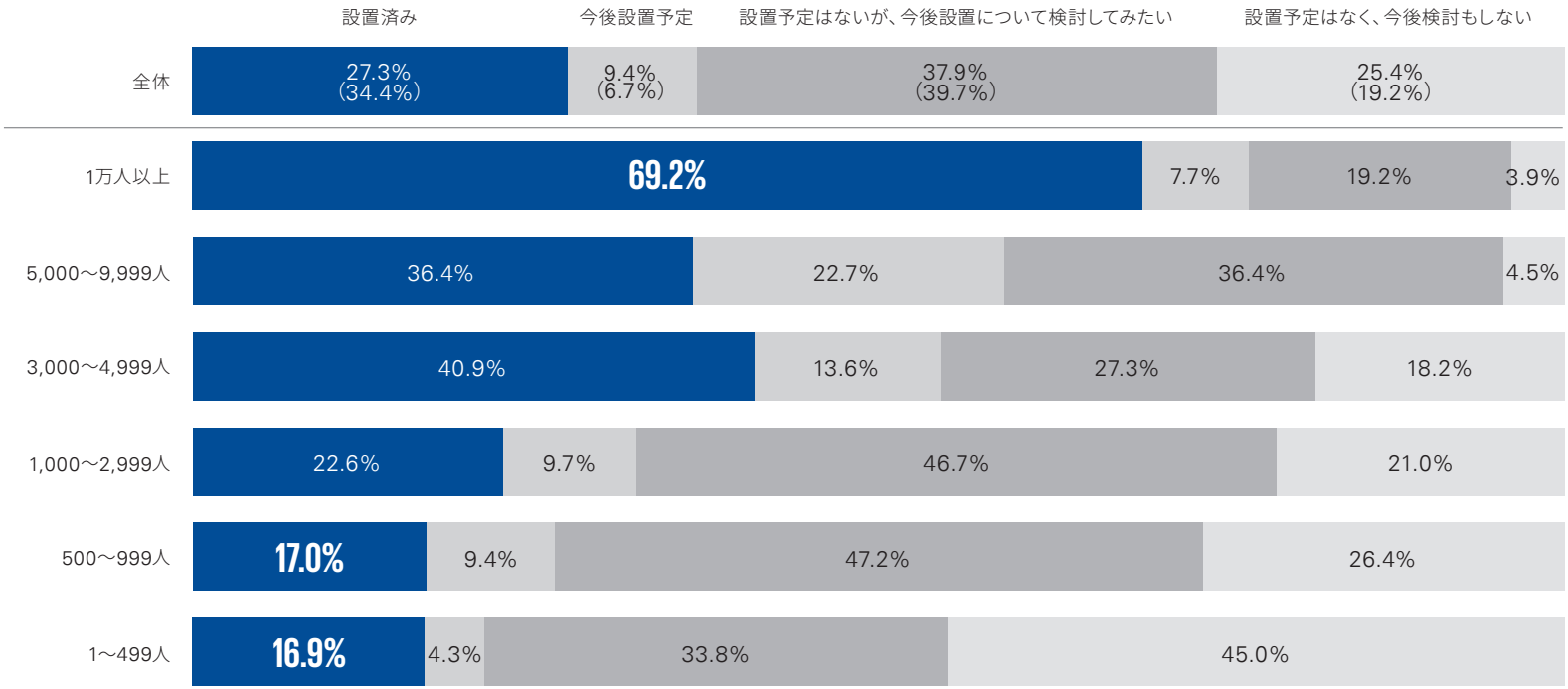
Windowsは、マイクロソフト グループの企業の商標です。
今回（複数回答可／n=116）／（）内は前回（は2022年）の調査数値（複数回答可／n=130）

CSIRTの整備

74.6%の企業がCSIRT（Computer Security Incident Response Team）を「設置済み」、「今後設置予定」、または「設置予定はないが、今後設置について検討してみたい」と積極的な回答をしており、前回（2022年）の調査と比較してもこの傾向に大きな差はありません。また、「設置予定はないが、今後設置について検討してみたい」と回答している企業の割合が高いことから、今後さらにCSIRTの整備が進むことが期待されます。
従業員数別でみると、従業員数が多い企業ほど積極的に取り組む傾向にあり、特に1万人以上の企業では69.2%もの企業がすでにCSIRTを設置している一方で、1,000人未満の企業では17%程度にとどまります。

CSIRTの整備状況

1万人以上の企業では69.2%がすでにCSIRTを設置している一方で、1,000人未満の企業では17%程度にとどまる。



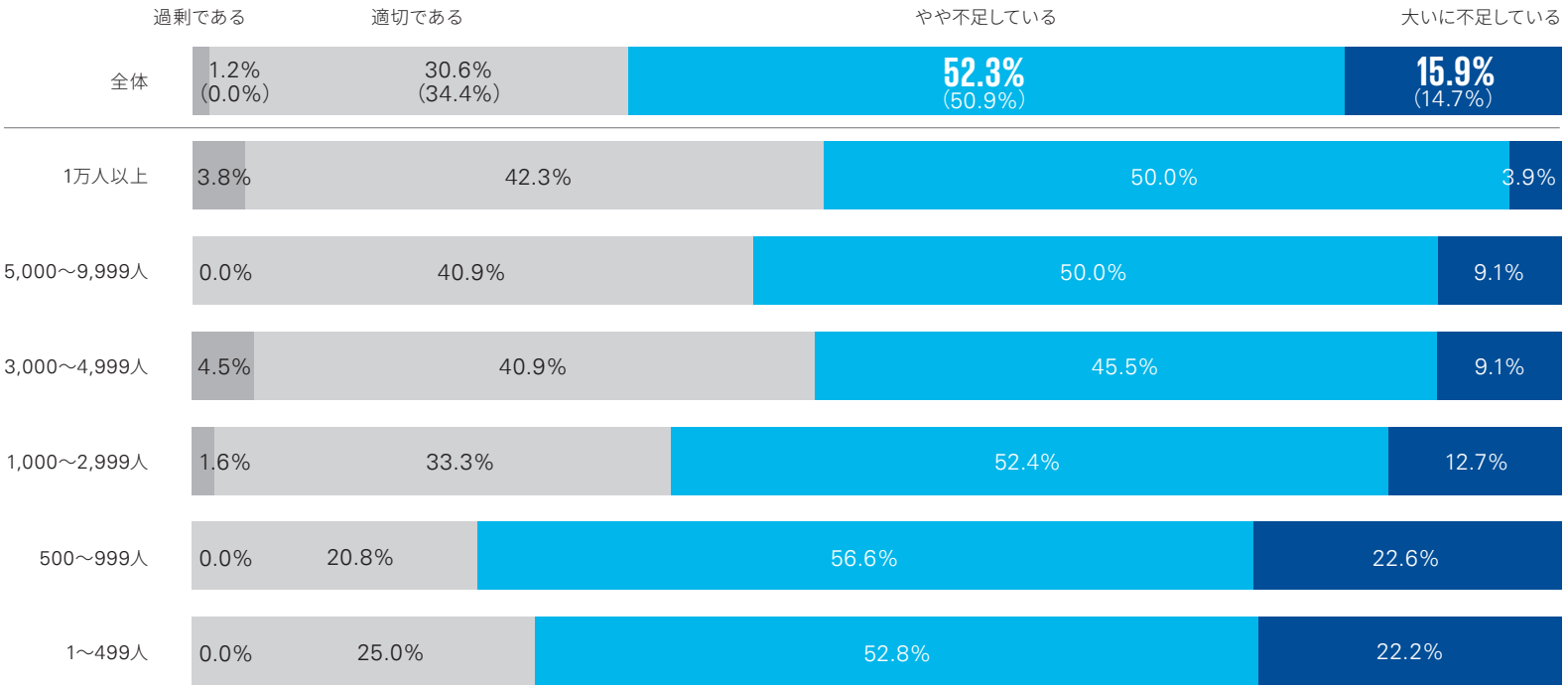
今回（n=258）／（）内は前回（2022年）の調査数値（n=285）

サイバーセキュリティ予算

サイバーセキュリティ予算について、68.2%の企業が不足していると回答しています。
従業員数別にみると、1,000人未満の企業では不足している傾向が強くなり、予算をサイバーセキュリティにまでまわすことが困難であることがうかがえます。昨今ではサイバーセキュリティ対策が強固な大企業ではなく、同一のサプライチェーンを構成する中小企業などの取引先を経由してサイバー攻撃が行われる事例も多いことから、優先度を上げて適切にセキュリティ対策を行うことが求められます。

サイバーセキュリティ予算の状況

68.2%の企業でサイバーセキュリティ予算が不足している。



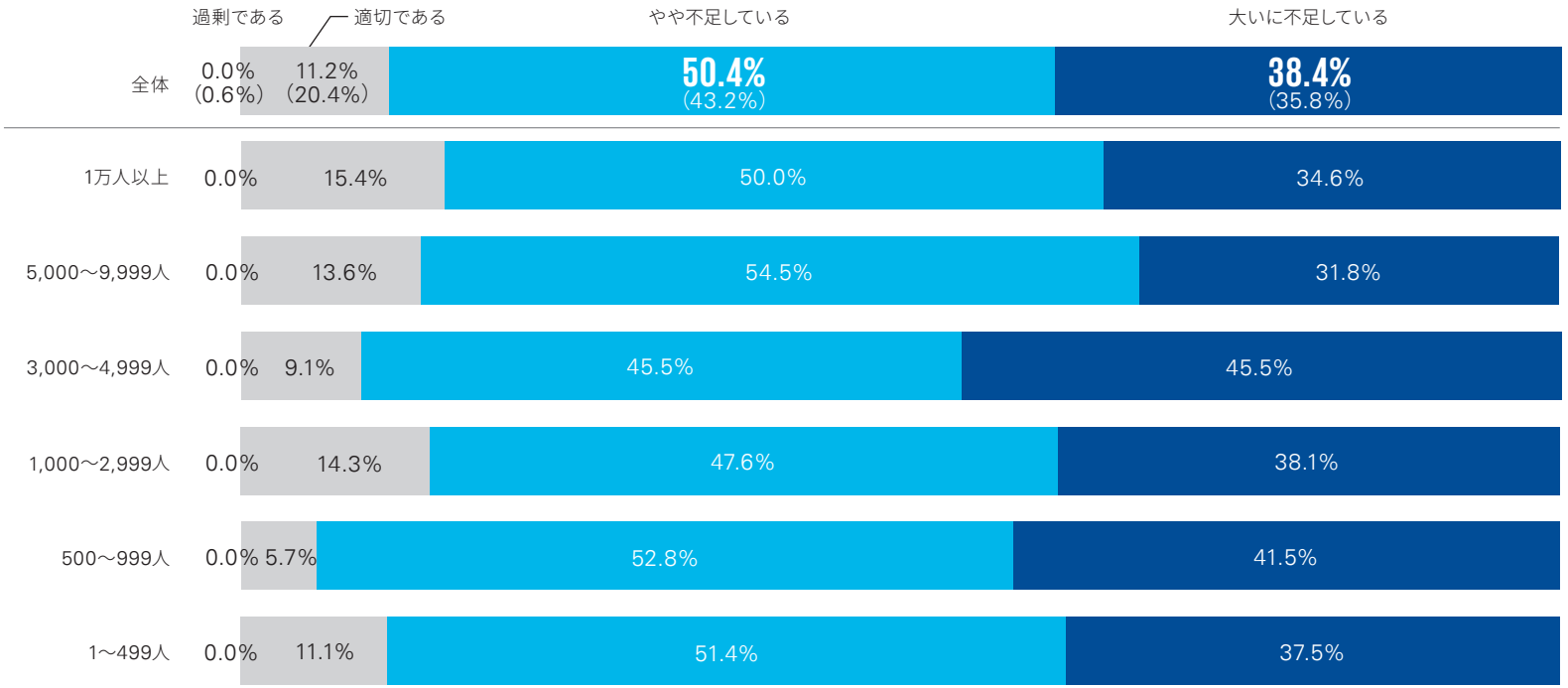
今回（n=258）／（）内は前回（2022年）の調査数値（n=285）

サイバーセキュリティ人材

サイバーセキュリティ体制は多くの企業で整備が進んでいますが、規則整備や現場対応を行うサイバーセキュリティ人材については、88.8%もの企業で不足していると回答しており、この傾向は従業員規模にかかわらず、前回（2022年）の調査よりも増加しています。
近年の高度化・巧妙化されたサイバー攻撃に対処するためには、自社で人材育成することは引き続き重要であるものの、外部の専門家やサービスを活用する、自動化ツールを導入して効率化を図るなど、さまざまな対策を組み合わせて組織のセキュリティ態勢を強化し、人材不足に対処する必要があります。

サイバーセキュリティ人材の状況

88.8%の企業でサイバーセキュリティ人材が不足している。



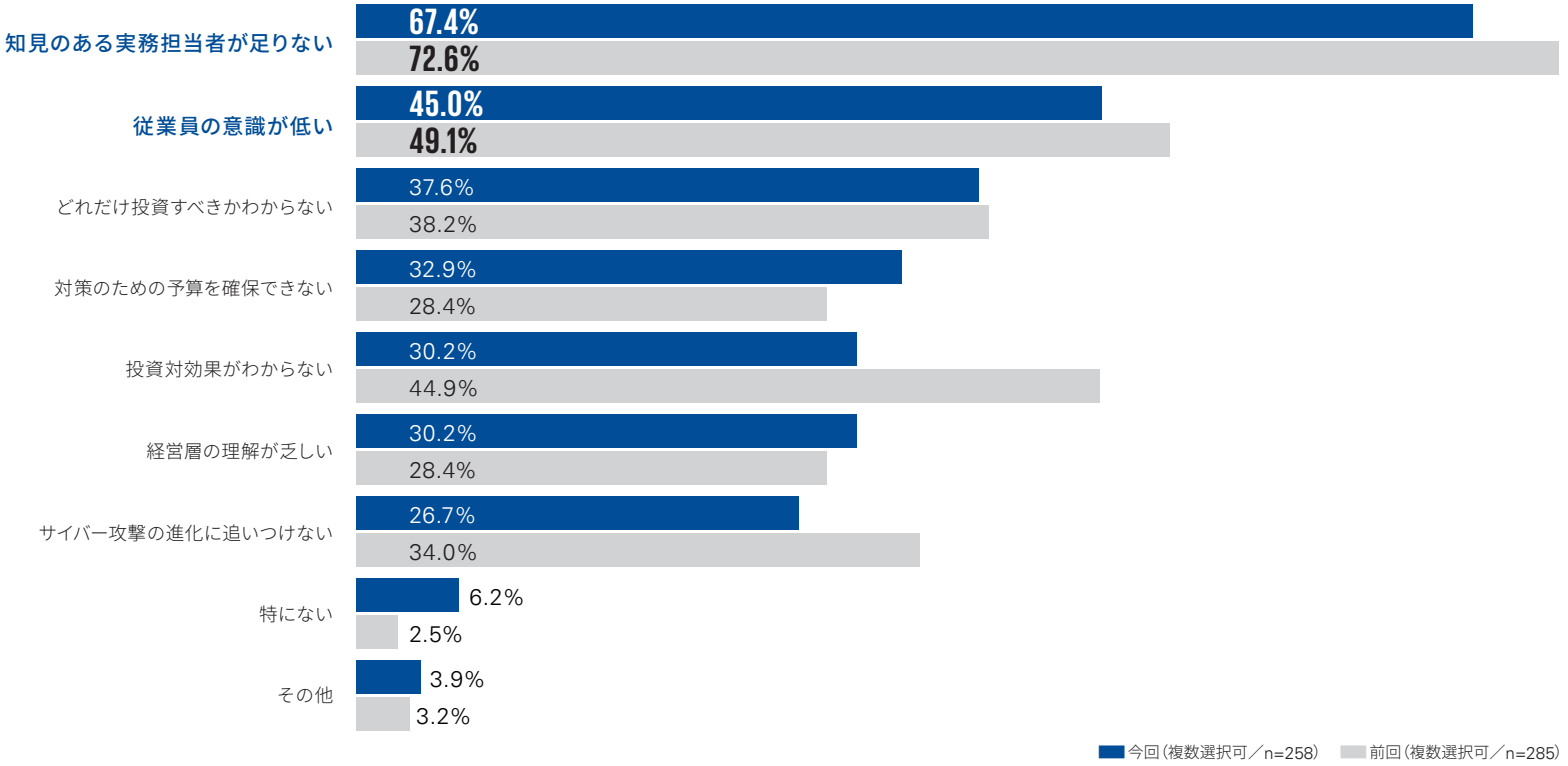
今回（n=258）／（）内は前回（2022年）の調査数値（n=285）

サイバーセキュリティ対策の課題

前回（2022年）の調査と同様に「知見ある実務担当者が足りない」、「従業員の意識が低い」といった人材に関する事項が大きなセキュリティ課題として認識されています。
一方で「投資対効果がわからない」は大幅に減少していることから、サイバーセキュリティ対策の重要性と投資対効果について理解が進んでいる傾向にあることがうかがえます。

サイバーセキュリティ対策における課題

前回（2022年）の調査と同様に人材に関する事項がセキュリティ対策において大きな課題になっている。

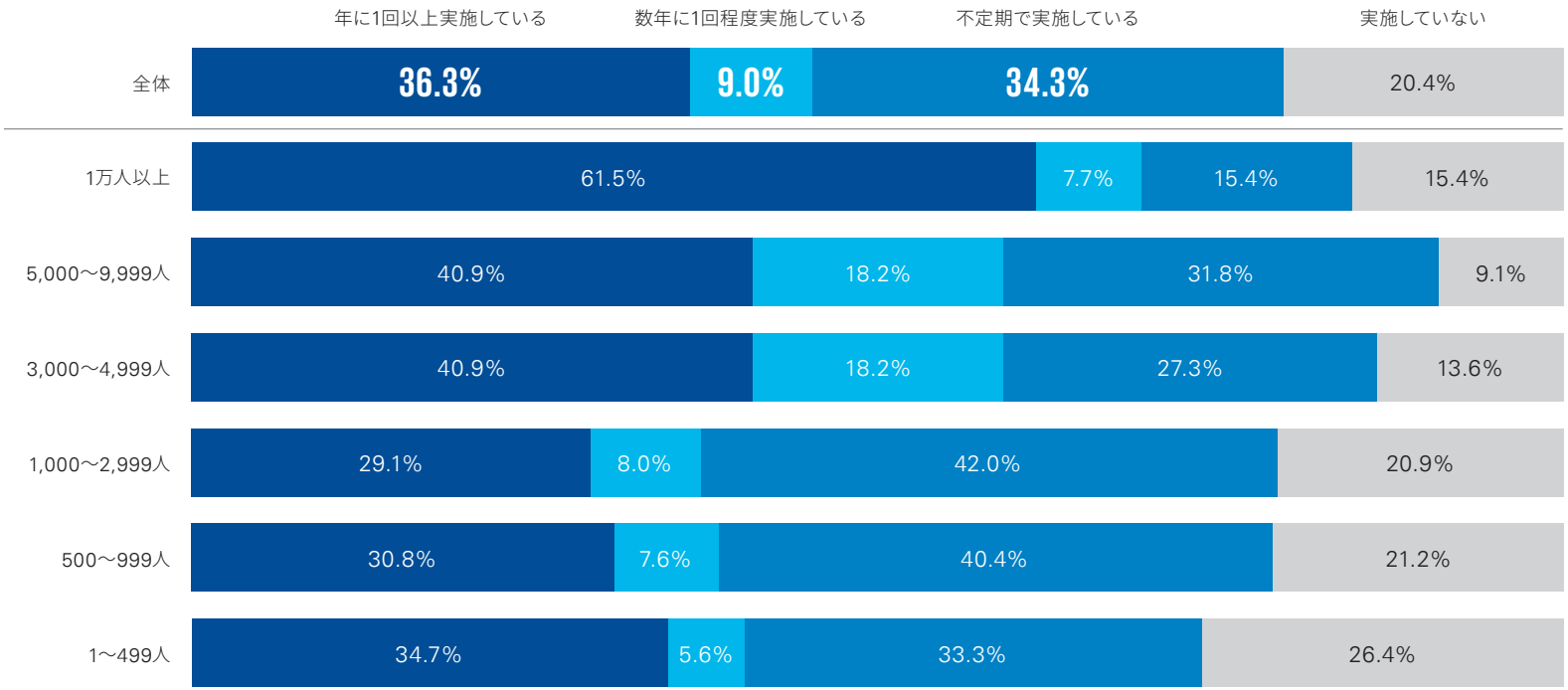


リスクアセスメントの実施状況

サイバーセキュリティ対策のリスクアセスメントについて、不定期での実施を含めて79.6%の企業が実施しています。
従業員数別にみると、従業員が多い企業ほどリスクアセスメントを実施する傾向にあり、1万人以上の企業では61.5%が「年に1回以上実施している」と回答しているのが特徴的です。

リスクアセスメントの実施状況

回答企業の79.6%がリスクアセスメントを実施している。



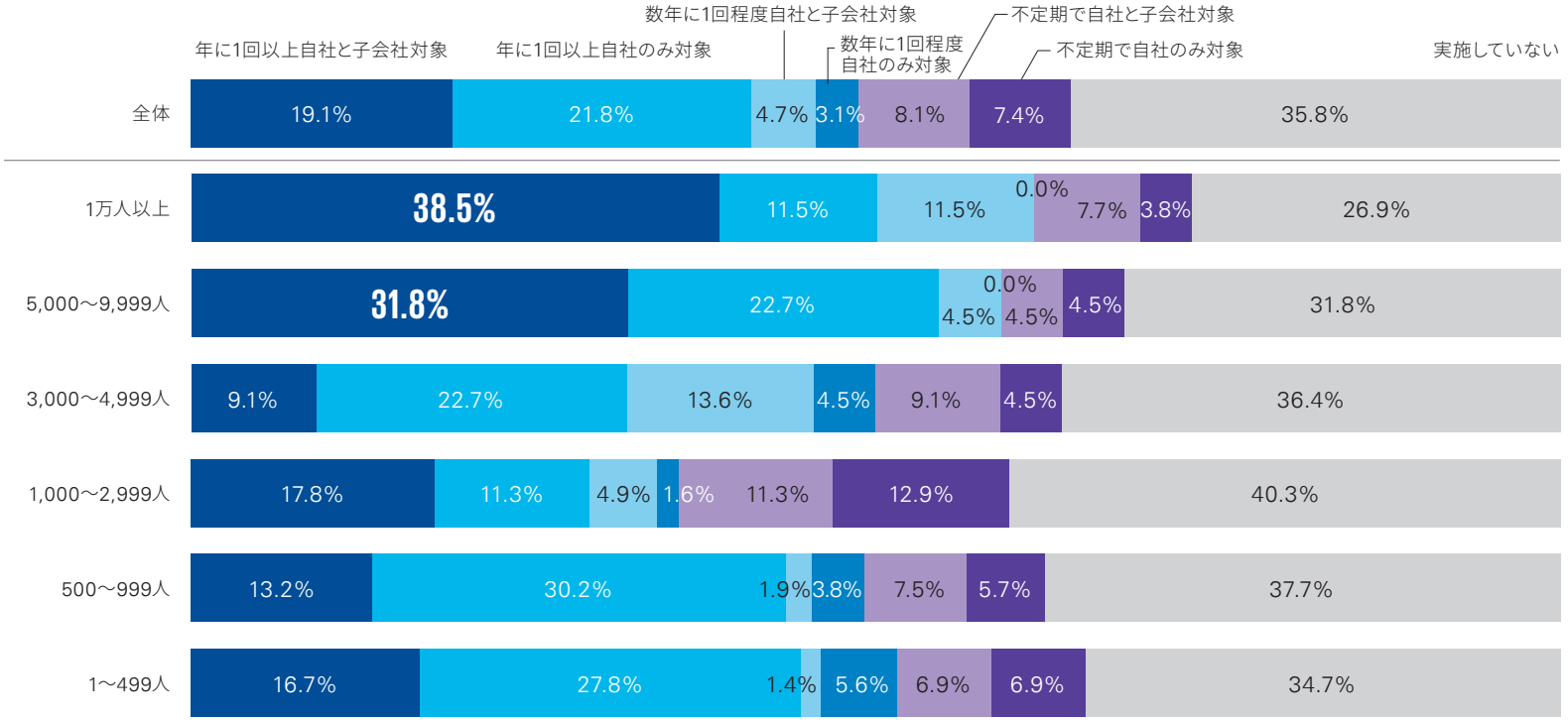
n=258

サイバーセキュリティ監査の実施状況

サイバーセキュリティ対策状況の監査について、64.2%の企業が不定期を含めて監査を実施していると回答しています。
従業員数別にみると、5,000人以上の企業では30%以上の企業が子会社も含めて年1回以上監査を実施しており、業界規制への対応やセキュリティガバナンスを強く求められていると推察されます。なお、全体的な傾向として、従業員数にかかわらず、30%程度の企業でセキュリティ監査を実施していないと回答しています。

サイバーセキュリティ監査の実施状況

5,000人以上の企業では30%以上の企業が子会社も含めて年1回以上監査を実施している。



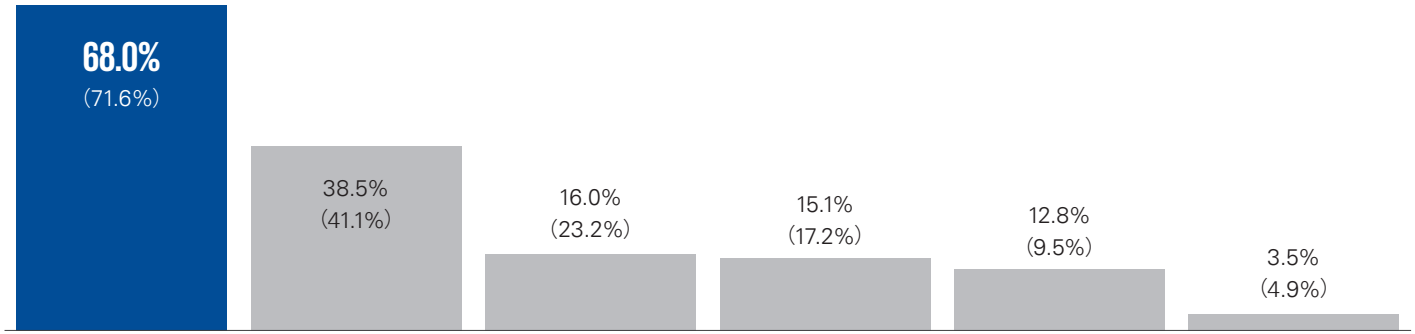
n=258

サイバー脅威動向の情報収集

サイバー脅威動向の情報収集について、68.0%の企業が日常業務の一環としてオープンソースから情報収集しており、38.5%が「政府機関や非営利団体からの情報配信を受けている」と回答しています。
従業員数別にみると、3,000人以上の企業ではISAC（Information Sharing and Analysis Center）等の情報共有コミュニティや民間事業者の有償サービスも活用している割合が高くなります。業界内の情報共有コミュニティを活用して同業他社の情報を収集するなど、サイバー脅威動向の情報収集においては多角的な観点で情報収集することが求められ、従業員の多い企業ほど実践している企業が多くなっています。

サイバー脅威動向の収集方法

多くの企業がオープンソースから情報収集する傾向にあるが、1万人以上の企業では複数のチャネルから情報収集する傾向が高くなる。



	日常業務の一環としてオープンソースの情報（ウェブサイト／ニュースなど）を収集している	政府機関や非営利団体からの情報配信を受けている	業界内の情報共有コミュニティ（ISACなど）に加入している	民間事業者による有償サービスの提供を受けている	何もしていない	その他
1万人以上	73.1%	**53.8%**	**46.2%**	**26.9%**	0.0%	3.8%
5,000～9,999人	59.1%	50.0%	27.3%	31.8%	4.5%	4.5%
3,000～4,999人	63.6%	54.5%	22.7%	18.2%	4.5%	9.1%
1,000～2,999人	69.0%	40.1%	9.6%	11.2%	14.5%	4.9%
500～999人	75.5%	37.7%	9.4%	15.1%	15.1%	0.0%
1～499人	63.9%	23.6%	9.7%	8.3%	19.4%	2.8%

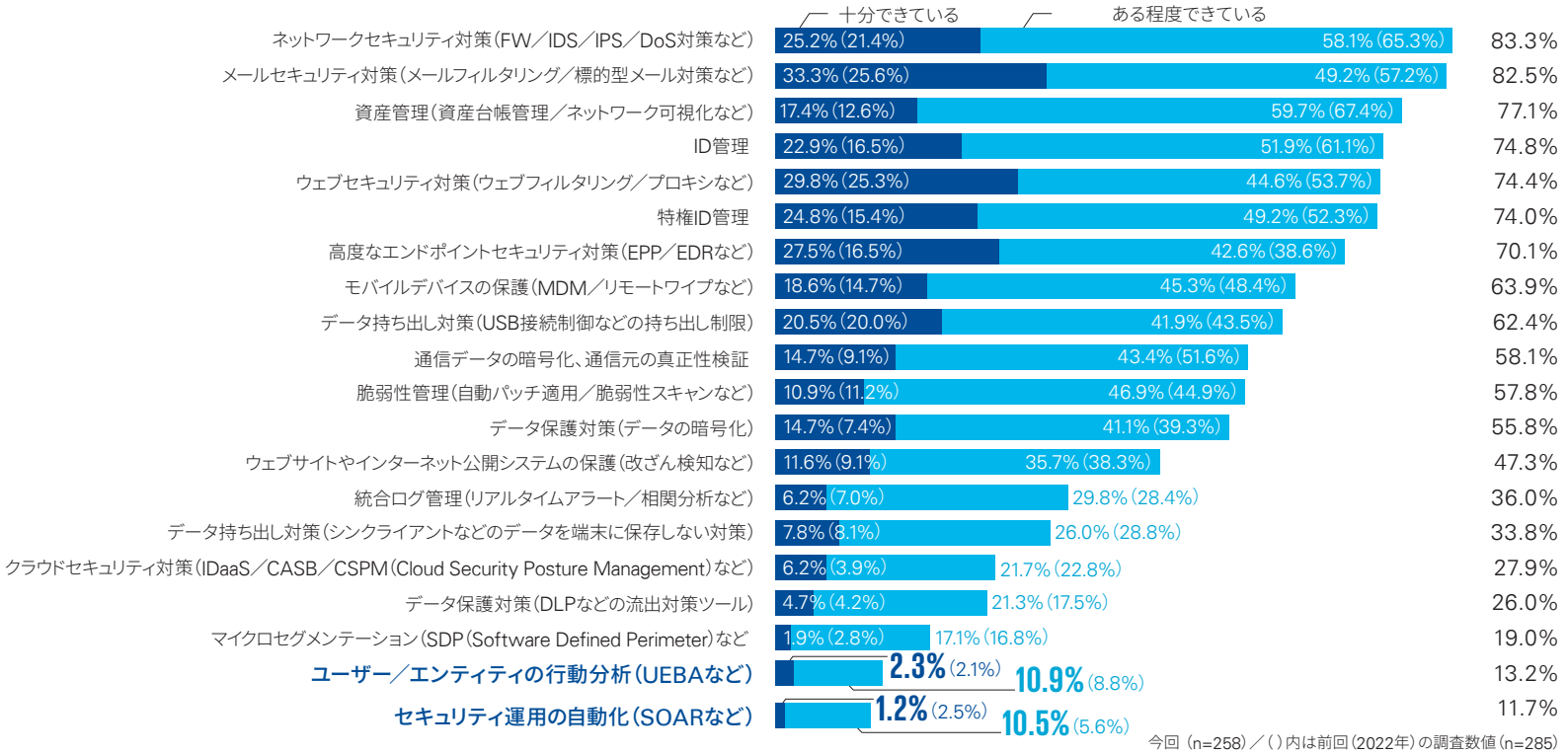
全体スコアから5ポイント以上　全体スコアから5ポイント以下
今回（複数回答可／n=258）／（）内は前回（2022年）の調査数値（複数回答可／n=285）

サイバーセキュリティ対策の実施状況

ネットワークセキュリティ、メールセキュリティ、エンドポイントセキュリティなどの従来からある対策に比べて、「ユーザー／エンティティの行動分析」、「セキュリティ運用の自動化」などの新しい領域の対策は12～13%程度にとどまっています。高度化・巧妙化するサイバー攻撃へ対応するため、UEBAやSOAR等の導入によるセキュリティ監視・運用のOODA（Observe・Orient・Decide・Act）ループを実現し、運用負荷の軽減や品質向上などを図ることが重要です。

サイバーセキュリティ対策の実施状況

「ユーザー／エンティティの行動分析（UEBAなど）」、「セキュリティ運用の自動化（SOARなど）」など高度なサイバーセキュリティ対策を「十分できている」、「ある程度できている」と回答した企業は12～13%程度にとどまる。

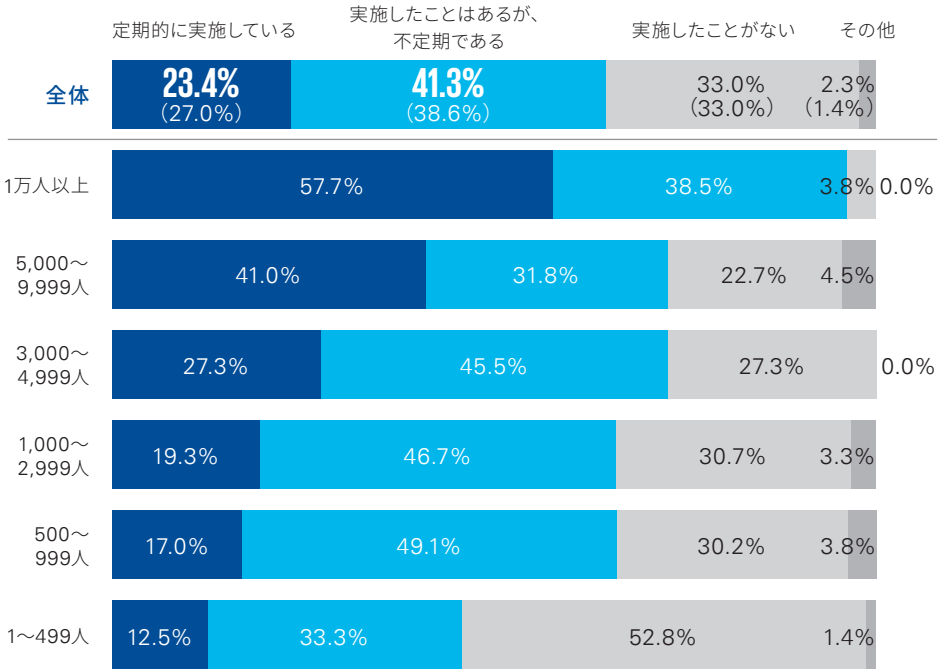


脆弱性診断・ペネトレーションテスト実施状況

回答企業の64.7%が脆弱性診断やペネトレーションテストを実施していると回答しており、従業員数が多いほど実施している割合が高い傾向にあります。
業種別でみた場合は、金融では44.4%の企業が定期的に実施しており、不定期も含めると100%の企業が実施していると回答しています。一方で建設・不動産は56.0%の企業が「実施したことがない」と回答しており、業種により実施割合に差があることがうかがえます。
DXが加速していくなかで、脆弱性診断やペネトレーションテストの未実施は企業リスクを高める可能性があるため、定期的に実施して脆弱性を可能な限り排除することが重要です。

脆弱性診断・ペネトレーションテストの実施状況（従業員数別）

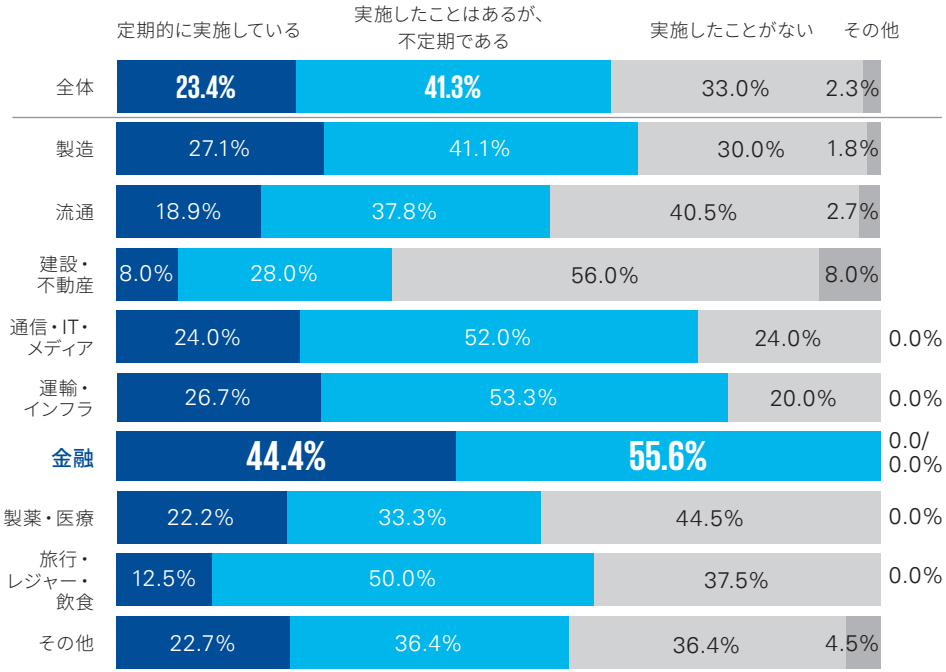
回答企業の64.7%が脆弱性診断・ペネトレーションテストを実施しており、従業員数に比例して実施している割合が高い。



今回（n=258）／（）内は前回（2022年）の調査数値（n=285）

脆弱性診断・ペネトレーションテストの実施状況（業種別）

金融業界ではすべての企業が脆弱性診断・ペネトレーションテストを実施している。



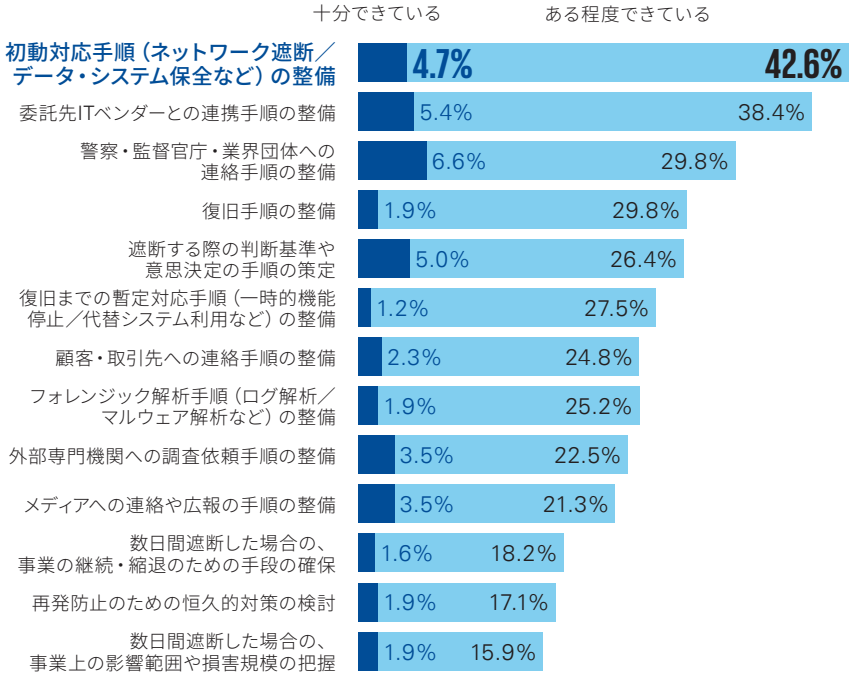
n=258

サイバーインシデントに備えた具体的な準備や対策

サイバーインシデントに関する対応手順等の整備については、初動対応手順、委託先ITベンダーや関係各所への連携・連絡手順がある程度整備できていると回答する企業が多くあります。一方で障害等の発生時の影響分析や詳細な対応手順は十分に整備できていない企業が多いことから、まずはサイバー演習などを通じて現状を認識し、対応手順の見直し・整備を行うことが重要になります。
サイバーインシデント対応演習においては、「標的型攻撃ランサムウェア等を想定したインシデント対応演習」を42.2%の企業で実施していると回答しており、標的型攻撃メール対応訓練などが広く行われている傾向にあります。「レッドチーム演習」を実施している企業は5.1%にとどまりますが、セキュリティ対策の実効性を検証するうえで有効な手段であるため実施することが望まれています。

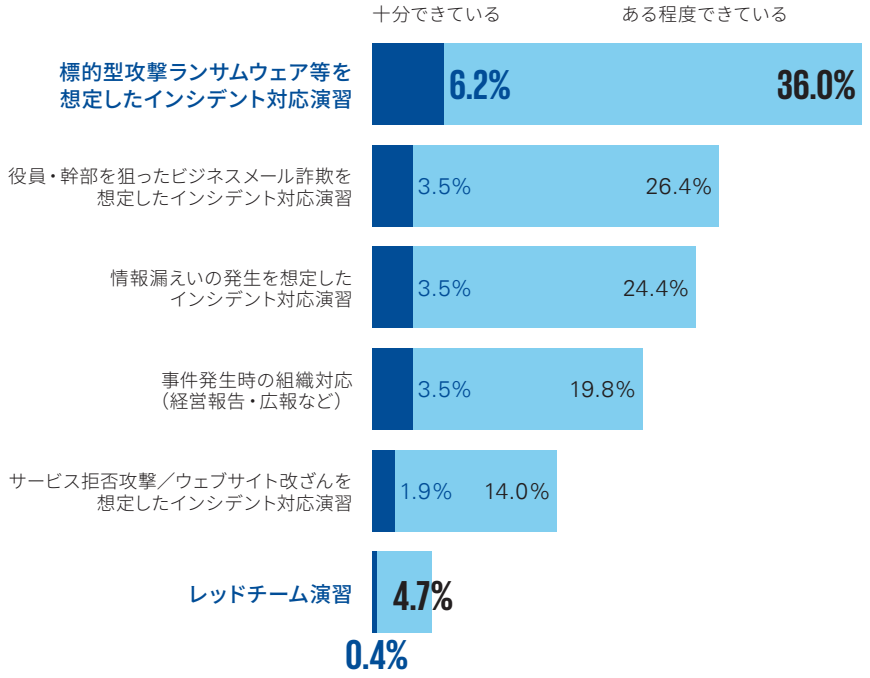
サイバーインシデント対応手順等の整備状況

初動対応手順の整備は47.3%の企業で実施されている。



サイバーインシデント対応演習の実施状況

「標的型攻撃ランサムウェア等を想定したインシデント対応演習」は42.2%の企業で実施されているが、「レッドチーム演習」の実施はわずか5.1%にとどまる。

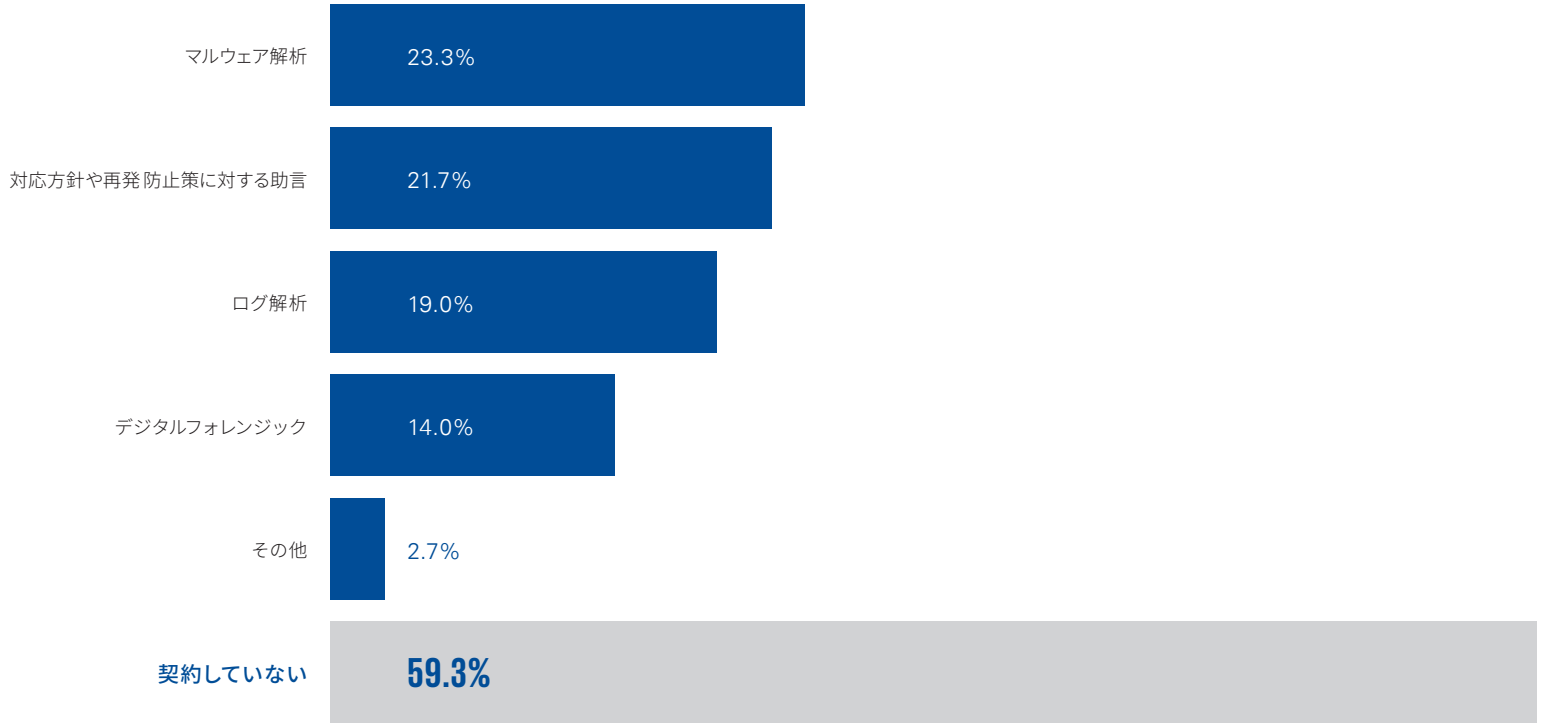


インシデント対応時の外部サービス利用状況

「マルウェア解析」、「対応方針や再発防止策に対する助言」、「ログ解析」、「デジタルフォレンジック」の順にインシデント対応時に外部サービスを利用していると回答しています。一方で回答企業の59.3%は外部サービスを「契約していない」と回答しています。インシデントの原因究明は専門的な知見・スキルを要する場合があるため、適宜これらの外部サービスを活用することをおすすめします。

インシデント対応時における外部サービス利用状況

回答企業の59.3%が外部サービスを契約していない。



複数選択可／n=258

テーマ 03

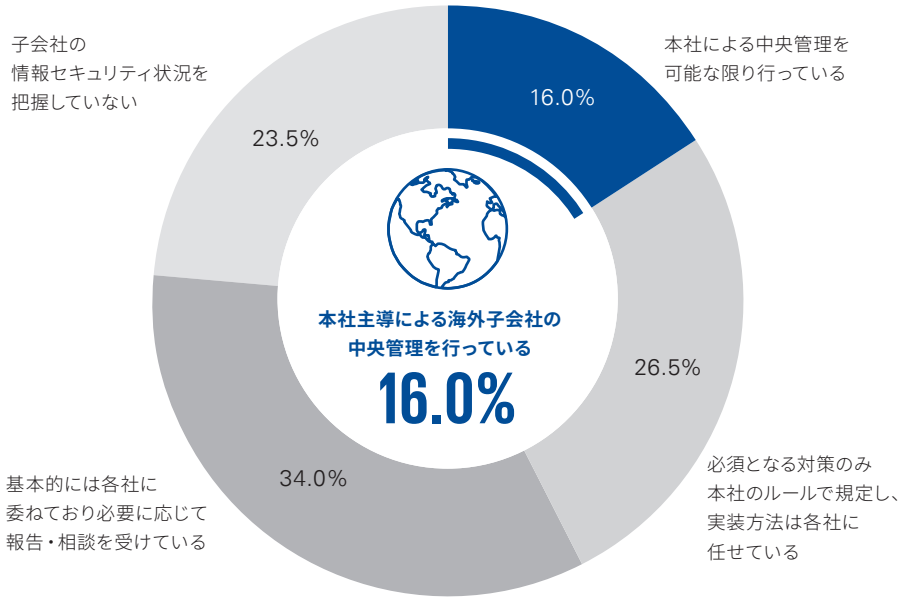
海外子会社管理

海外子会社に対するセキュリティ管理

海外子会社のセキュリティ対策については、「基本的には各社に委ねており必要に応じて報告・相談を受けている」という回答が34.0%、「子会社の情報セキュリティ状況を把握していない」という回答が23.5%にのぼります。しかし、海外子会社がそれぞれ場当たり的に対策を講じるのではなく、本社主導で海外子会社（拠点）のセキュリティリスクを正確に把握し、グループ全体で整合性の取れたセキュリティ施策を計画し、導入することが望まれます。

海外子会社における情報セキュリティレベルの管理状況

本社主導による海外子会社の中央管理を行っている企業は16.0%にとどまる。



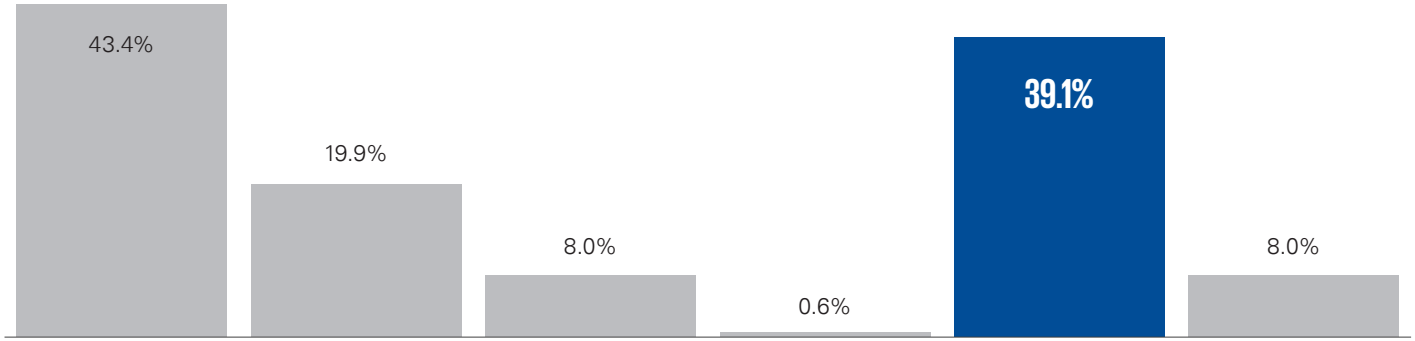
n=162

海外子会社における取組み状況の把握

回答企業の39.1%が「海外子会社の取組みを把握していない」と回答していますが、海外を含めた子会社を経由してサイバー攻撃が行われる事例も多いことから、まずは実施状況の確認の徹底を進める必要があります。
海外子会社のセキュリティ対策状況の把握方法については、43.4%が「調査票（紙、表計算ソフト、PDFなど）」を使用している一方、監査は19.9%、「外部のリスク評価サービス」の利用は8.0%にとどまります。1万人以上の企業でも86.4%が調査票を用いて確認している状況ですが、外部サービスの活用やGRC（ガバナンス・リスク・コンプライアンス）ツールを活用することにより、正確かつ詳細に把握・管理していくことが望ましいです。

サイバーセキュリティ対策状況の把握方法

39.1%の企業で海外子会社の取組みを把握できていない。



	調査票（紙、表計算ソフト、PDFなど）	海外子会社の監査	外部のリスク評価サービス	GRC（ガバナンス・リスク・コンプライアンス）ツール	海外子会社の取組みを把握していない	わからない
1万人以上	86.4%	27.3%	13.6%	0.0%	13.6%	0.0%
5,000～9,999人	47.6%	19.0%	9.5%	4.8%	23.8%	14.3%
3,000～4,999人	57.9%	26.3%	15.8%	0.0%	31.6%	5.3%
1,000～2,999人	34.9%	11.6%	7.0%	0.0%	46.5%	9.3%
500～999人	39.4%	24.2%	6.1%	0.0%	42.4%	3.0%
1～499人	8.3%	16.7%	0.0%	0.0%	62.5%	16.7%

全体スコアから5ポイント以上　全体スコアから5ポイント以下

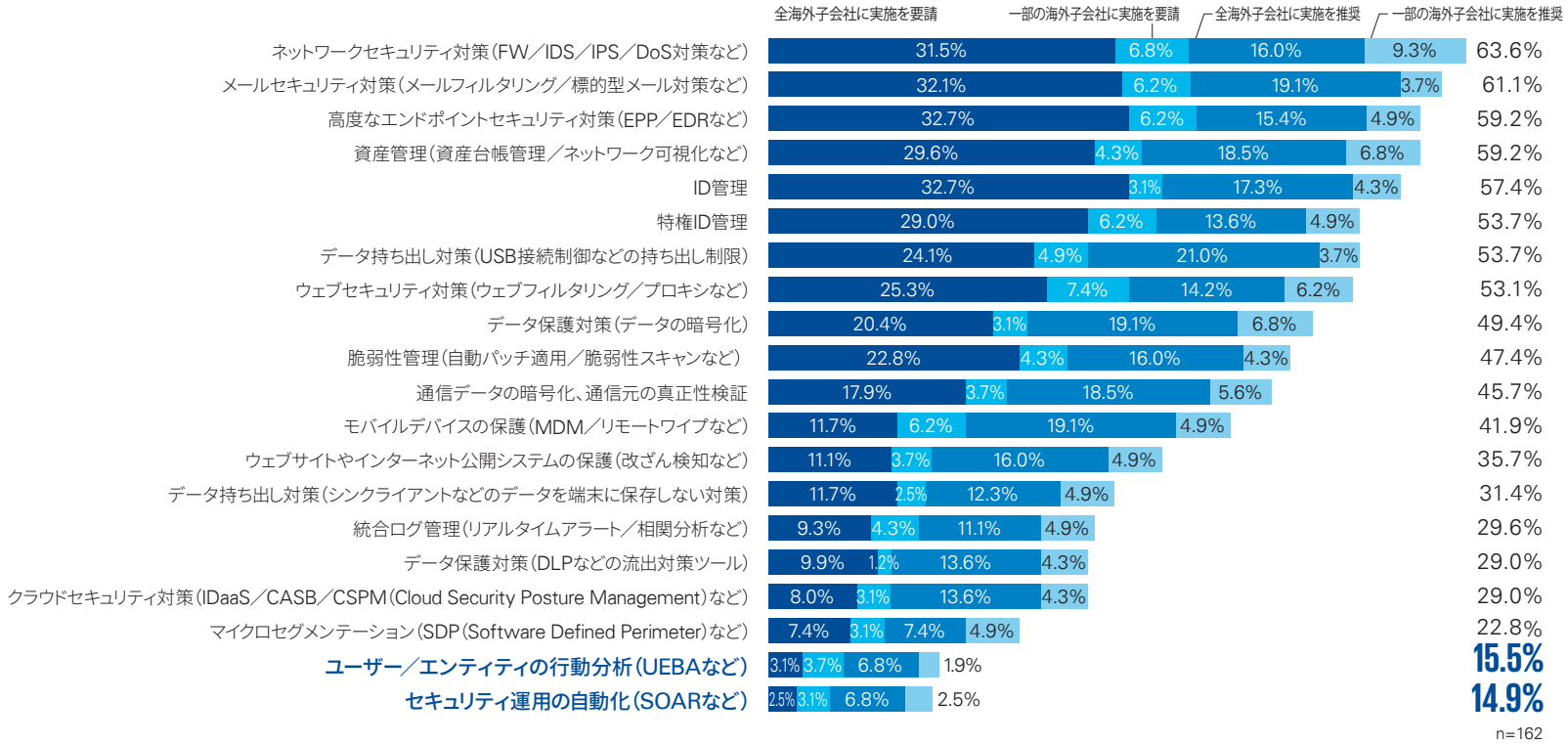
複数回答可／n=162

海外子会社への対策要請

海外子会社へのサイバーセキュリティ対策の要請状況は、国内におけるサイバーセキュリティ対策実施状況と同様の傾向にあります。
しかし、ネットワークセキュリティ、メールセキュリティ、エンドポイントセキュリティなどの従来からある対策に比べて、「ユーザー／エンティティの行動分析」、「セキュリティ運用の自動化」などの新しい領域の対策を要請・推奨する企業は15%程度にとどまります。高度化・巧妙化するサイバー攻撃へ対応するため、UEBAやSOARの導入によるセキュリティ監視・運用のOODA（Observe・Orient・Decide・Act）ループを実現し、運用負荷の軽減や品質向上などを図ることが求められています。

海外子会社に要請・推奨しているセキュリティ対策

海外子会社管理においても、UEBA、SOARなどの新しい領域の対策を要請・推奨している企業は15%程度にとどまる。

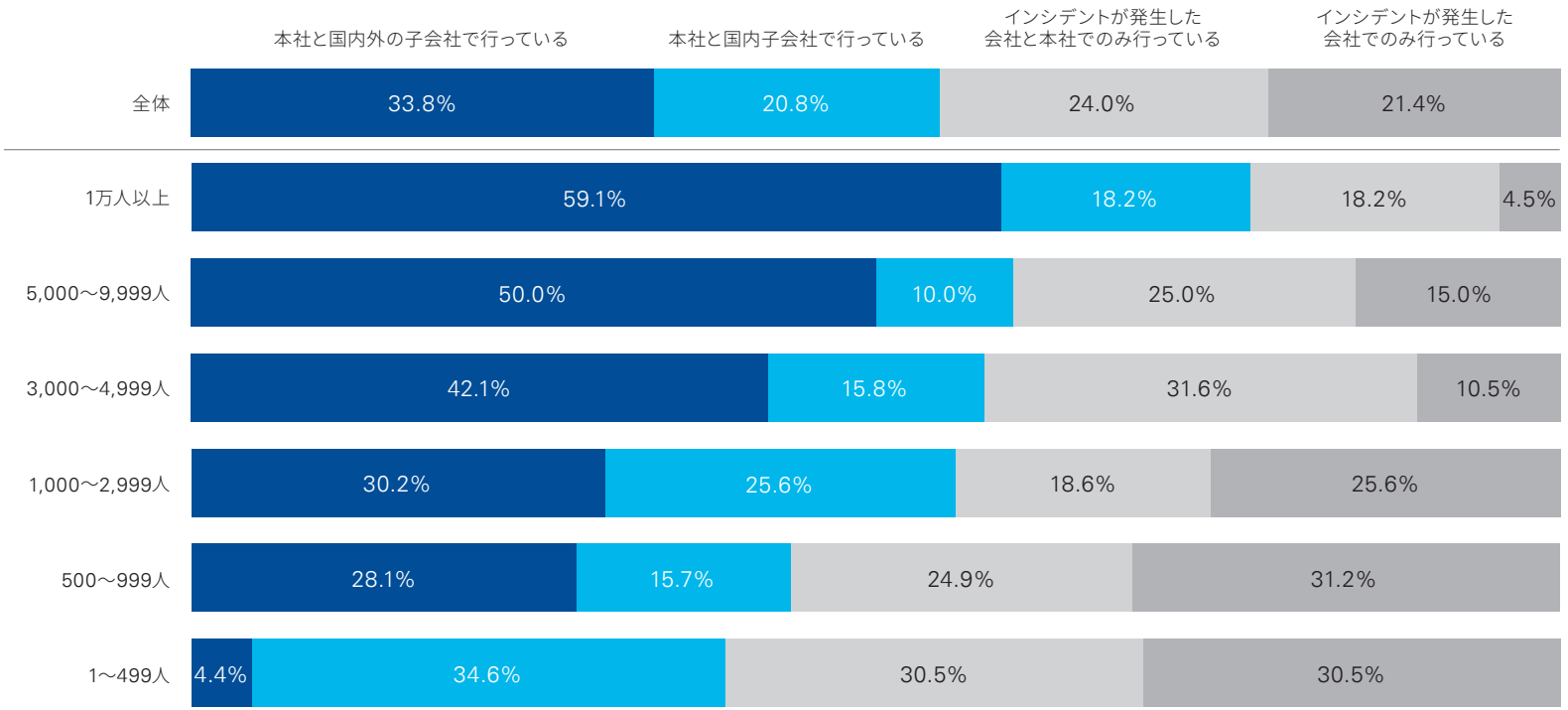


再発防止策の展開範囲

サイバーインシデントが発生した際の再発防止策の展開範囲は、従業員数が多いほど本社と国内外の子会社に展開されている割合が高くなる傾向にあります。再発防止策を国内外の子会社へ幅広く展開することは、過去に経験した事象だけでなく将来的なサイバー攻撃に対しても適切かつ迅速に対応することが可能になり、組織全体のセキュリティ意識を高めるなど、グループ全体として包括的にリスクを軽減することにつながります。

サイバーインシデントが発生した際における再発防止策の展開範囲

従業員数が多いほど本社と国内外の子会社に再発防止策が展開されている割合が高い。



n=162

テーマ 04

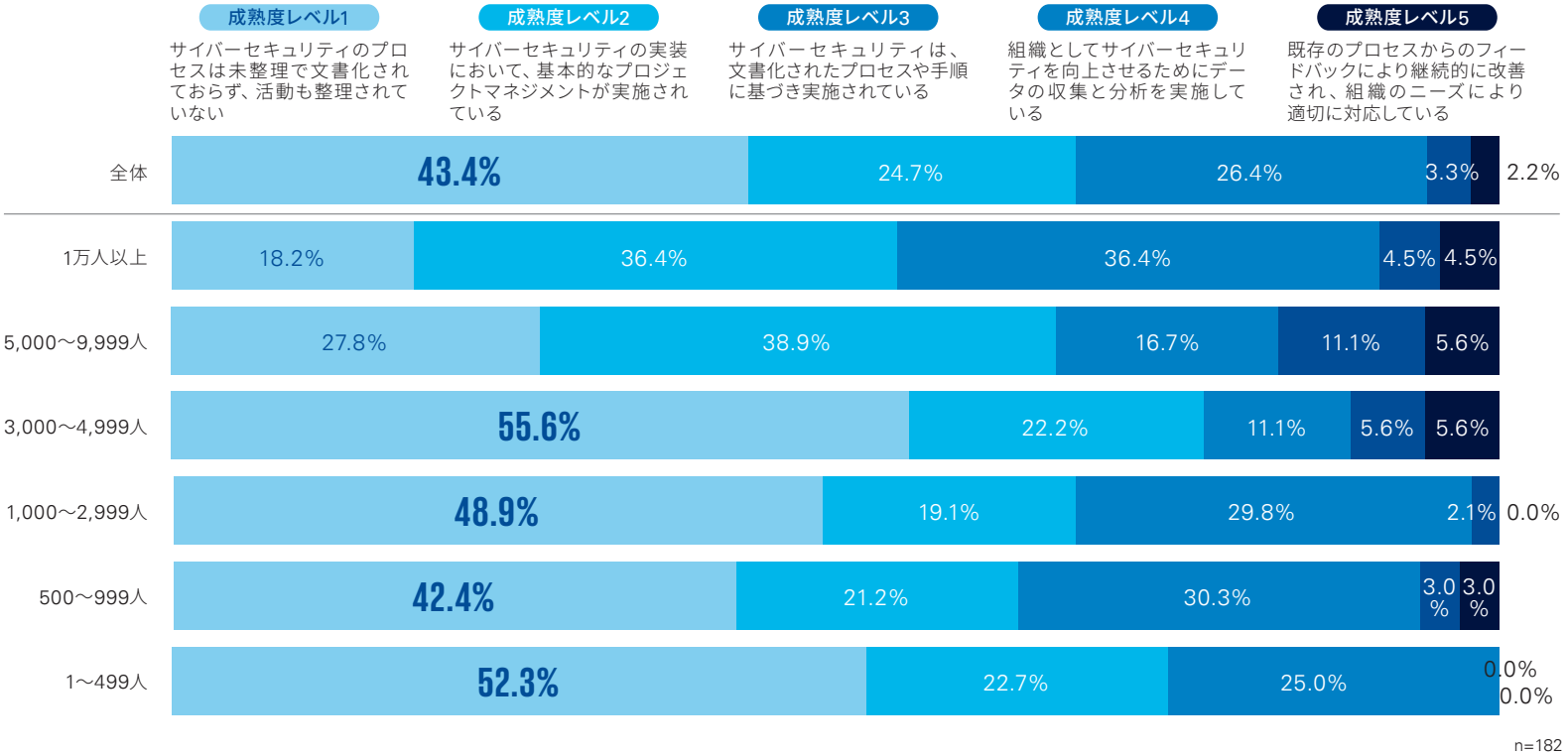
制御システムセキュリティ

制御システムセキュリティレベル

制御システムセキュリティレベルの分布は、「成熟度レベル1」が43.4%で最も多く、サイバーセキュリティのプロセスは未整理で文書化されておらず、活動も整理されていない企業が多数を占めています。続いて、「成熟度レベル2」、「成熟度レベル3」がそれぞれ24.7%、26.4%となり、「成熟度レベル4」、「成熟度レベル5」の企業は合計で5.5%にとどまる状況です。
従業員数別で成熟度レベルをみると、従業員数が少ない回答企業ほど成熟度レベルが低いことがわかります。ただし、従業員数が比較的多い企業であっても、「成熟度レベル1」にとどまる企業もあるため、制御システムセキュリティへの取組みは全体的な課題だと言えます。

制御システムのセキュリティ成熟度

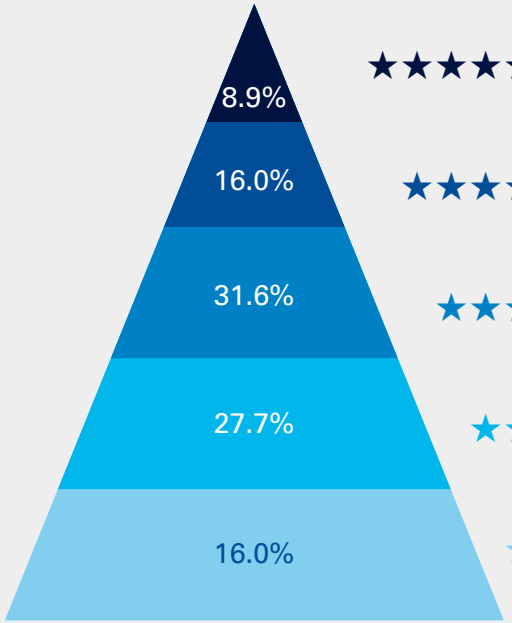
制御システムセキュリティレベルは「成熟度レベル1」が最も多く43.4%を占めており、従業員数が5,000人未満の企業で割合が高い。



[参考] 制御システムセキュリティの成熟度

2023年1月30日に公開した「(CS)²AI- KPMG 制御システムサイバーセキュリティ年次報告書 2022」* において調査した結果、グローバルにおいては、制御システムセキュリティ成熟度は以下のような分布になります。制御システム分野においては、グローバルと比較して日本ではまだ成熟度が低い傾向にあります。

積極的なディフェンス
高成熟度組織
24.9%



消極的なディフェンス
低成熟度組織
43.7%

★★★★★	Level 5	既存のプロセスからのフィードバックにより継続的に改善され、組織のニーズにより適切に対応している。
★★★★	Level 4	組織としてサイバーセキュリティを向上させるためにデータの収集と分析を実施している。
★★★	Level 3	サイバーセキュリティは、文書化されたプロセスや手順に基づき実施されている。
★★	Level 2	サイバーセキュリティの実装において、基本的なプロジェクトマネジメントが実施されている。
★	Level 1	サイバーセキュリティのプロセスは未整理で文書化されておらず、活動も整理されていない。

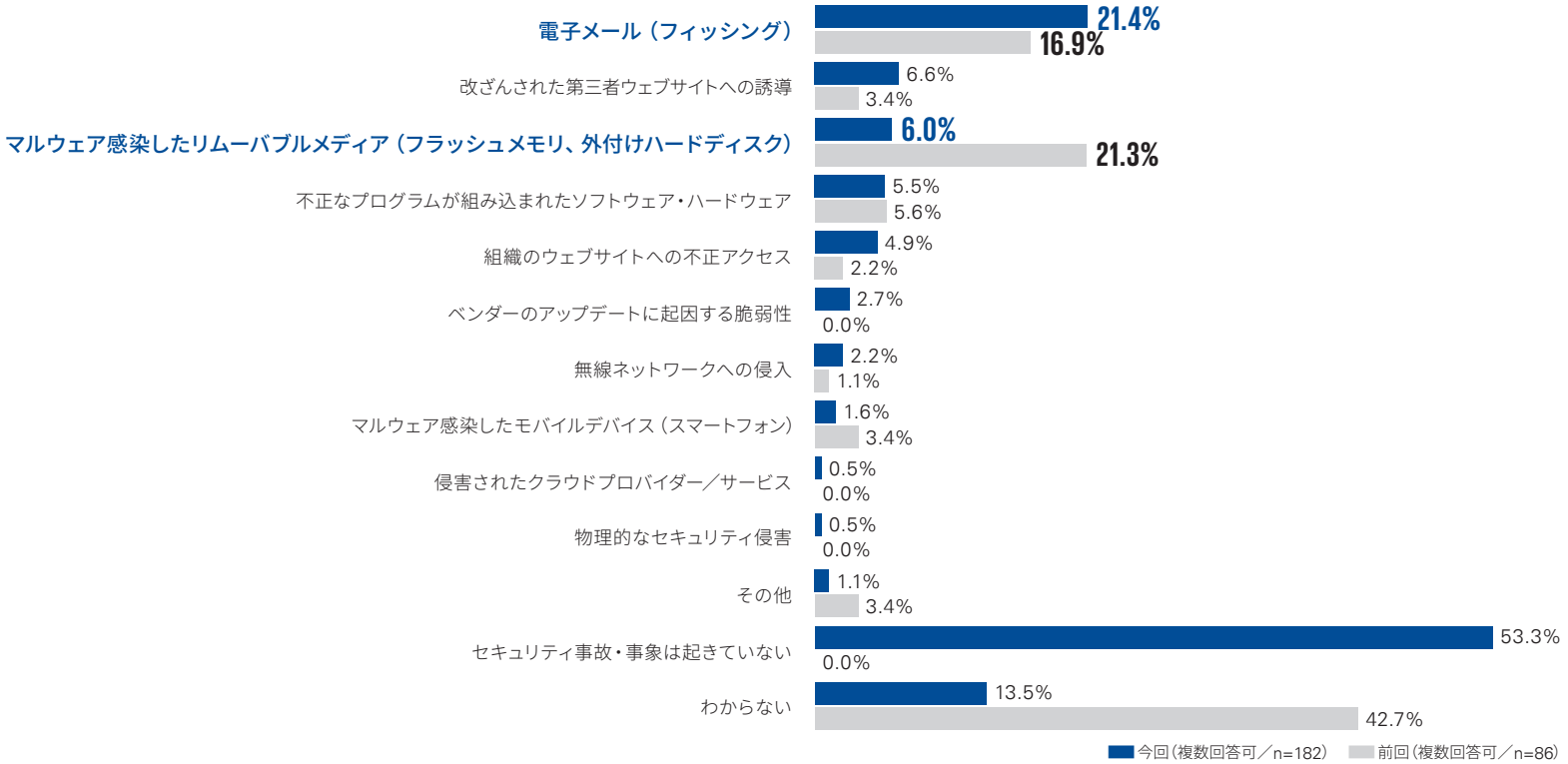
*出所：(CS)² AI-KPMG 制御システムサイバーセキュリティ年次報告書 2022
https://assets.kpmg.com/content/dam/kpmg/jp/pdf/2023/jp-cyber-controlsystem-report2022.pdf

制御システムへのサイバー攻撃実態

制御システムへのサイバー攻撃（未然に防がれたものを含む）の経路で最も多かったものは「電子メール（フィッシング）」で21.4%を占めています。他の経路についてはいずれも7%未満にとどまり、「セキュリティ事故・事象は起きていない」が半数を超えています。「電子メール（フィッシング）」が増加する一方で、「マルウェア感染したリムーバブルメディア（フラッシュメモリ、外付けハードディスク）」が減少していることから、リムーバブルメディアによる接続ではなく、他システムとのネットワーク接続の増加がうかがえ、ネットワーク接続での攻撃の可能性が高まっていると言えます。

制御システムに関するセキュリティ事故・事象（未然に防がれたものを含む）の攻撃経路

前回（2022年）の調査と比較して電子メール（フィッシング）による攻撃が増加し、リムーバブルメディアによる攻撃が大きく減少している。

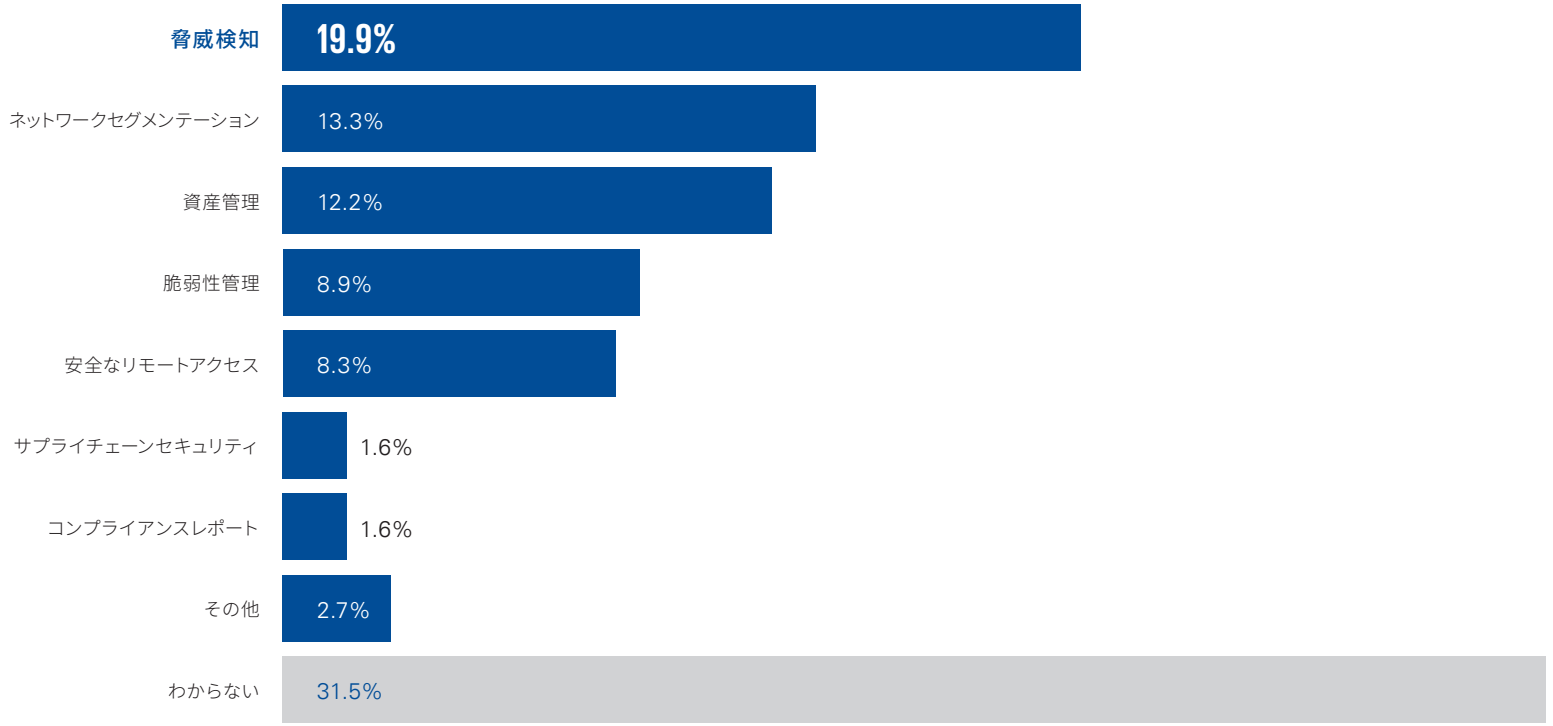


今後1年間の投資方針

制御システムセキュリティに対する今後1年間の投資方針として、最も多く投資する施策は「脅威検知」（19.9%）となっています。続いて「ネットワークセグメンテーション」（13.3%）、「資産管理」（12.2%）の順で多くなっており、現時点ではまだ基礎的なセキュリティ対策に投資を予定している段階と言えます。

今後1年間に最も多く投資する制御システムセキュリティ対策

「脅威検知」に対して投資する企業の割合が高い。



n=182

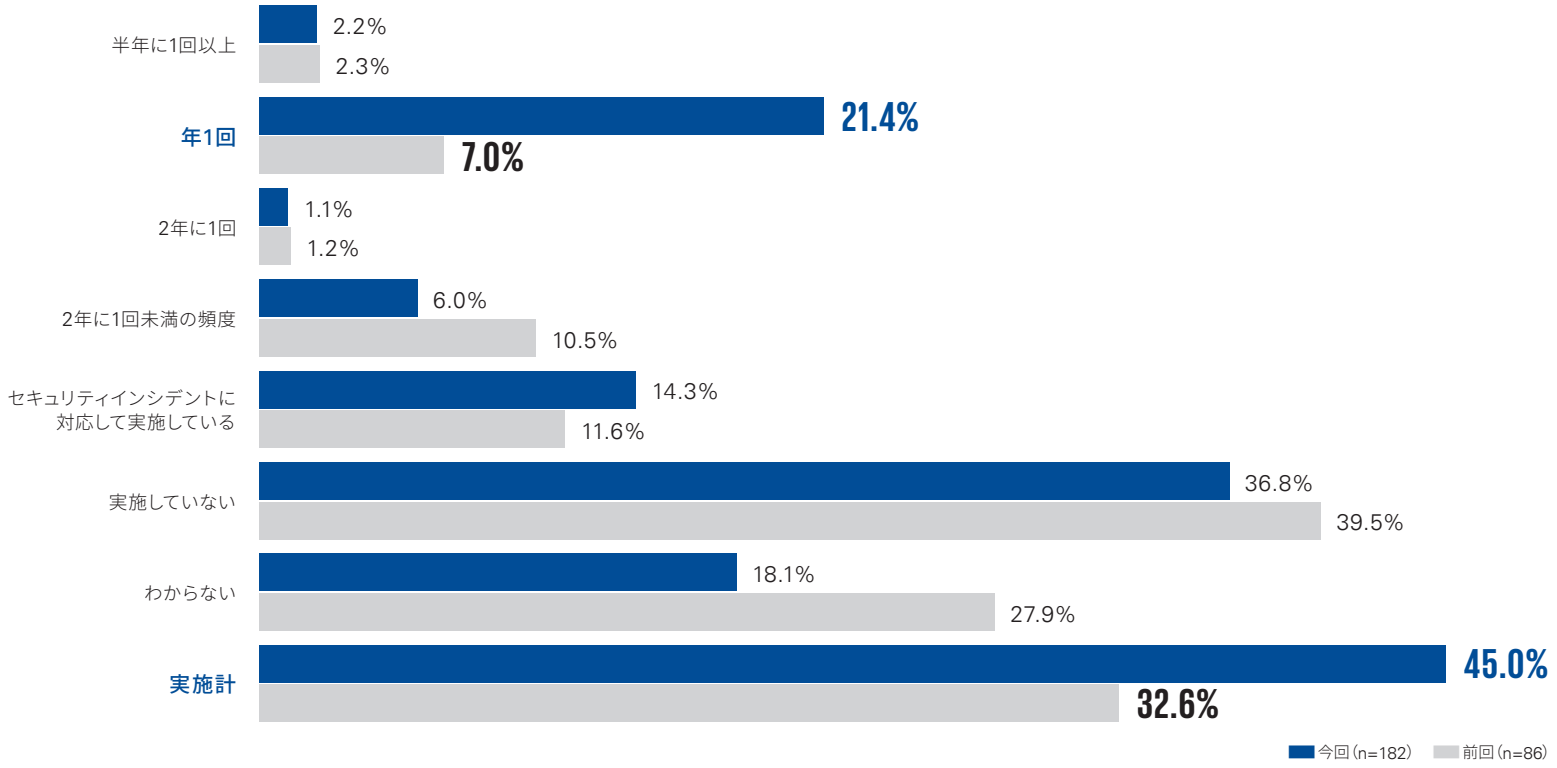
制御システムセキュリティアセスメント

制御システムセキュリティアセスメントの実施頻度は、「年1回」(21.4%) と、「セキュリティインシデントに対応して実施している」(14.3%) の順であり、セキュリティアセスメントを実施する企業は前回 (2022年) の調査と比較して増加しています。特に年1回の頻度で実施する企業が増加しており、成熟度レベルが向上してきていることが推察されます。しかし、海外におけるリスクアセスメント実施状況としては年1回以上実施している企業が52.3%であるため*、改善の余地が大きいと言えます。
また、「わからない」という回答も大幅に減少しており、セキュリティアセスメントに対する認識が醸成されつつあります。

* 出所:「(CS)² AI-KPMG 制御システムサイバーセキュリティ年次報告書 2022」
https://assets.kpmg.com/content/dam/kpmg/jp/pdf/2023/jp-cyber-controlsystem-report2022.pdf

制御システムセキュリティのセキュリティアセスメント実施状況

前回(2022年)の調査と比較して、「年1回」セキュリティアセスメントを実施している企業が約3倍に増加しており、実施している企業の合計(実施計)が約1.4倍に増加している。

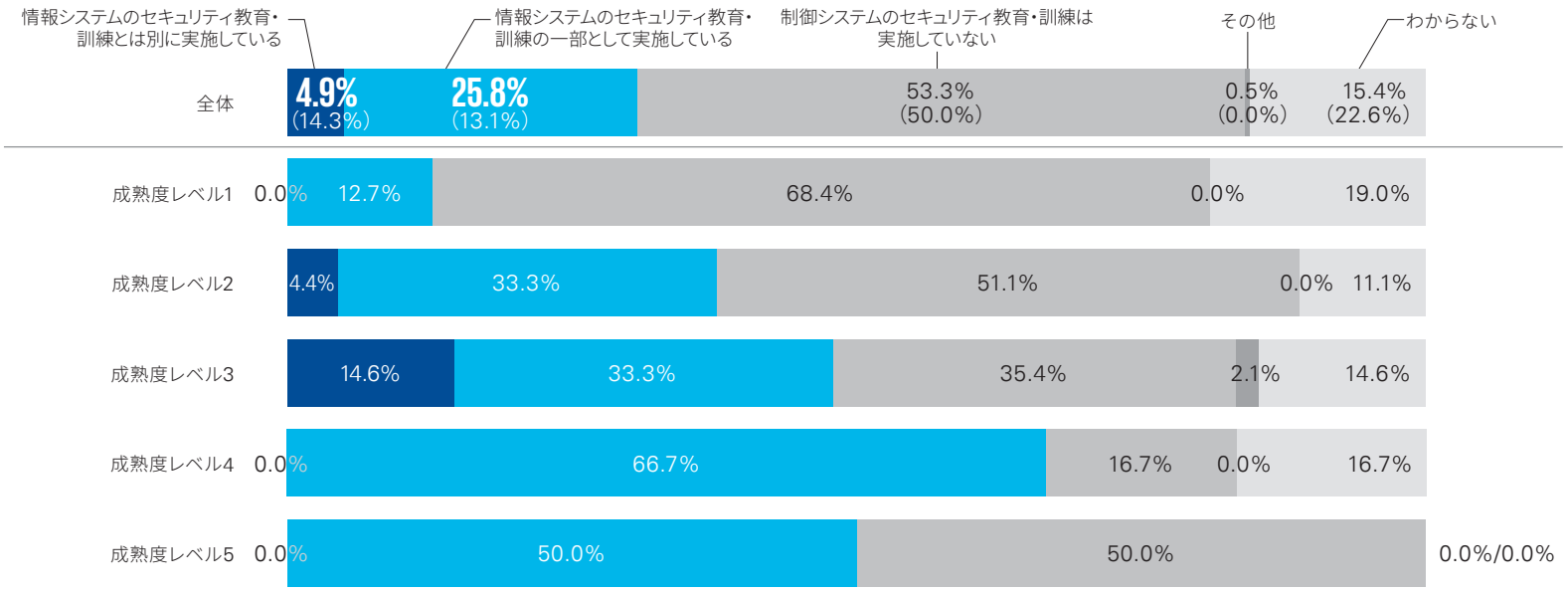


制御システムセキュリティの教育・訓練

「制御システムのセキュリティ教育・訓練は実施していない」企業は53.3%にのぼります。制御システムセキュリティの教育・訓練状況は、「情報システムのセキュリティ教育・訓練とは別に実施している」が4.9%、「情報システムのセキュリティ教育・訓練の一部として実施している」が25.8%で、合計で30.7%になります。「情報システムのセキュリティ教育・訓練の一部として実施している」企業は前回（2022年）の調査時の13.1%から25.8%に増加しており、制御システムセキュリティの教育・訓練が情報システムと連携して実施されるようになっている傾向がうかがえます。
成熟度レベル別でみると、成熟度が上がるにつれて教育・訓練を実施しているという回答が増え、情報システムとの連携が強まる傾向がうかがえます。

制御システムセキュリティの教育・訓練状況

制御システムセキュリティの教育・訓練の実施は全体では30.7%にとどまる。



凡例
成熟度レベル1 ー サイバーセキュリティのプロセスは未整理で文書化されておらず、活動も整理されていない
成熟度レベル2 ー サイバーセキュリティの実装において、基本的なプロジェクトマネジメントが実施されている
成熟度レベル3 ー サイバーセキュリティは、文書化されたプロセスや手順に基づき実施されている
成熟度レベル4 ー 組織としてサイバーセキュリティを向上させるためにデータの収集と分析を実施している
成熟度レベル5 ー 既存のプロセスからのフィードバックにより継続的に改善され、組織のニーズにより適切に対応している

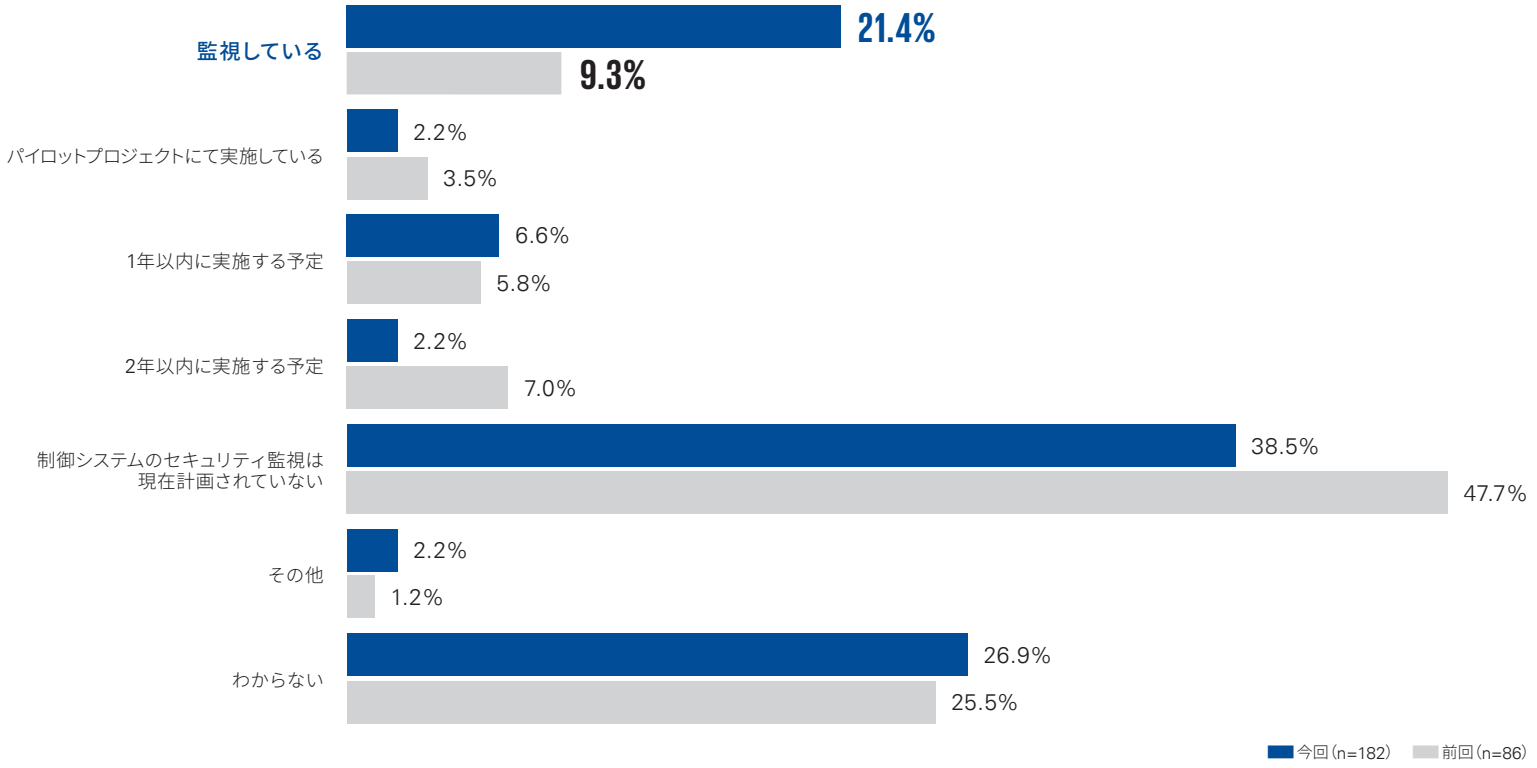
今回（n=182）／（）内は前回（2022年）の調査数値（n=86）

制御システムセキュリティの監視

制御システムセキュリティの監視状況としては、「監視している」が前回（2022年）の調査では9.3%であったのに対して、21.4%に増加しています。制御システムに対する監視の必要性が認識され、着実に監視する傾向にあることがうかがえます。
ただし、全体としては「監視している」、「パイロットプロジェクトにて実施している」と回答した企業は合計23.6%にとどまっているため、さらなる改善が必要です。

制御システムセキュリティの監視状況

制御システムセキュリティの監視状況としては、「監視している」が前回（2022年）の調査では9.3%であったのに対して、21.4%と増加している。

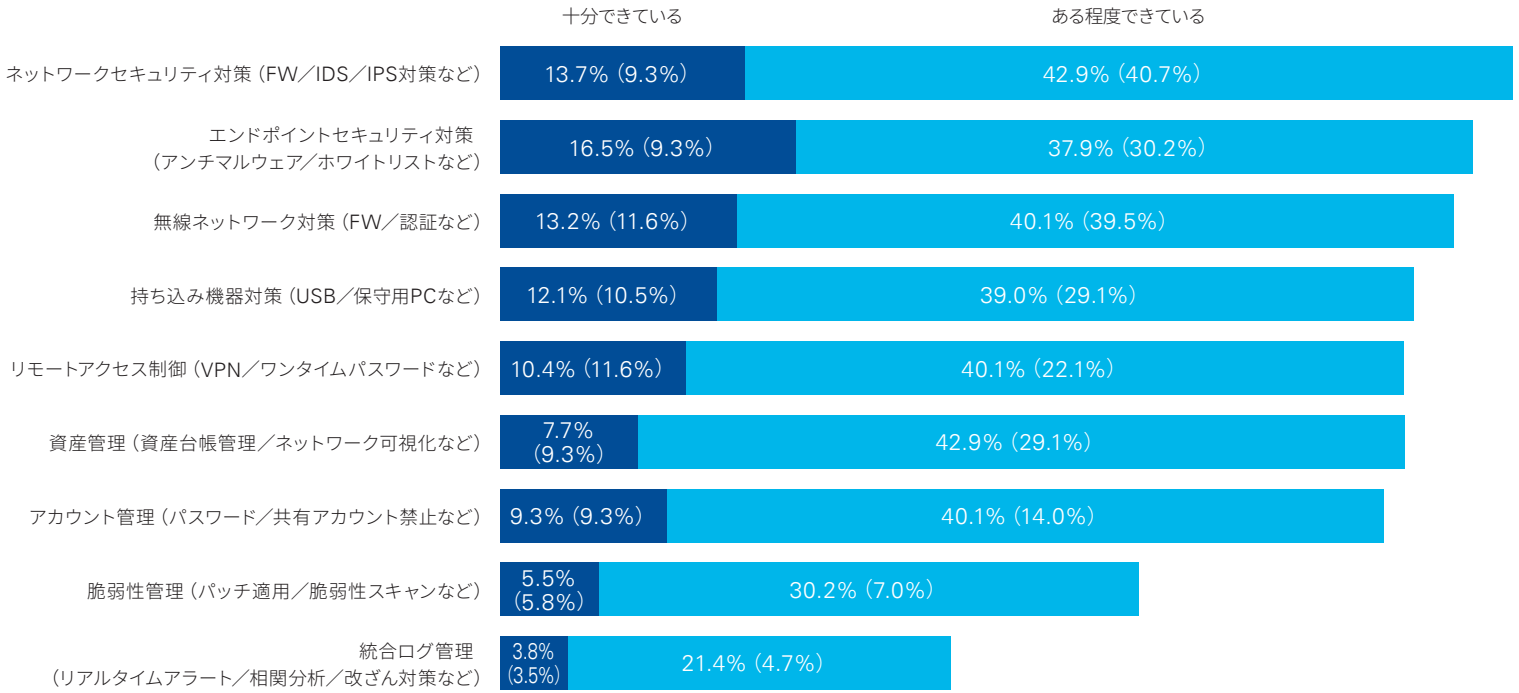


制御システムセキュリティの対策

制御システムセキュリティの対策状況として、「ネットワークセキュリティ対策」、「エンドポイントセキュリティ対策」、「無線ネットワーク対策」などの対策は進んでいますが、「脆弱性管理」や「統合ログ管理」のような制御システムでは対応が難しいと考えられる領域の対策までは十分に進んでいない傾向にあります。ただし、前回（2022年）の調査と比較すると全体的に「ある程度できている」と回答している企業数が増えていることから、セキュリティ対策が着実に進んでいる傾向にあります。

制御システムセキュリティの対策状況

前回（2022年）の調査と比較して、全体的なセキュリティ対策は進んでいる。



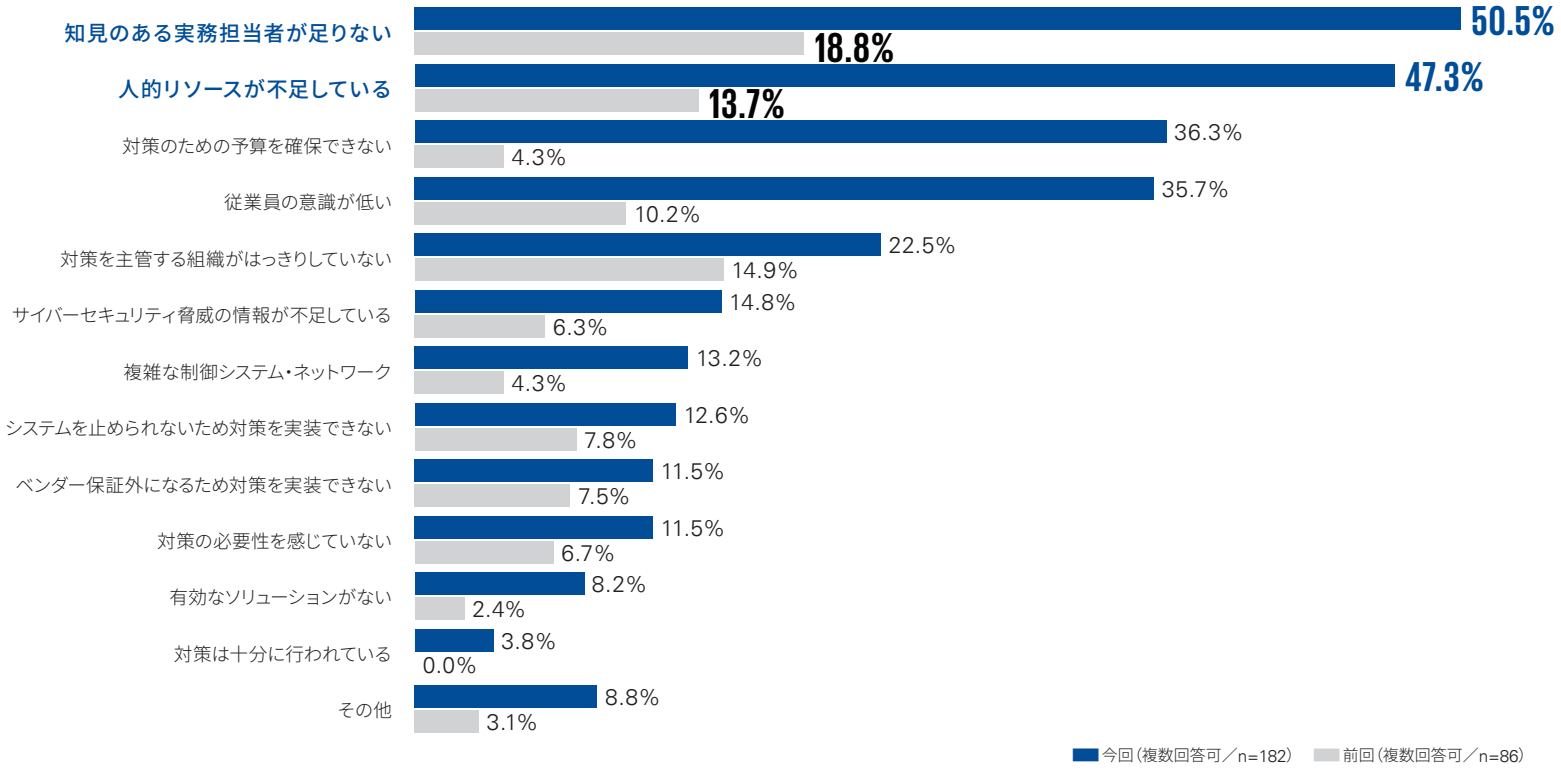
今回（n=182）／（）内は前回（2022年）の調査数値（n=86）

制御システムセキュリティ対策の課題

前回（2022年）の調査と比較して、各項目の回答割合が全体的に大幅に増加していることから、制御システムセキュリティに対する取組みが進んでおり、その過程で課題が明確になってきていることがうかがえます。そのなかでも特に、前回（2022年）の調査と同様に制御システムセキュリティに関する知見や人的リソースの不足、予算の確保が大きな課題であると回答しています。また、制御システムについて「対策を主管する組織がはっきりしていない」ことから、「対策のための予算を確保できない」という回答が急激に増えたのではないかと推察されます。
全体として、前回（2022年）の調査と同様に知見や人的リソースの問題は非常に大きいものの、対策推進にあたっての課題が明確になってきたことにより責任範囲や予算確保といった事項が重要課題に移行している傾向にあります。

制御システムセキュリティ対策が進んでいない課題

前回（2022年）の調査と同様に「知見のある実務担当者が足りない」（50.5%）と「人的リソースが不足している」（47.3%）が大きな課題として認識されている。



テーマ 05

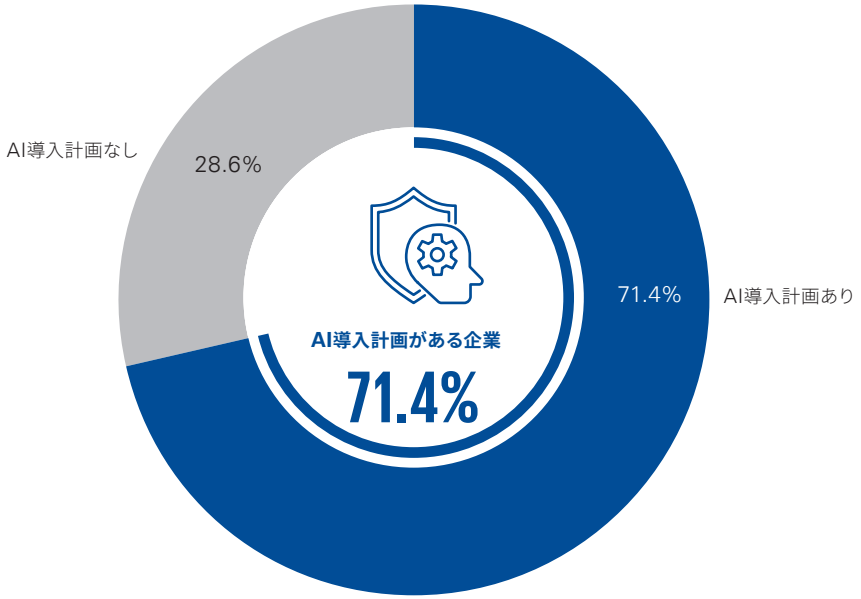
AI導入および AI導入に係るリスク管理

AI導入計画

回答企業のうち、71.4%が「AI導入計画あり」と回答しており、多くの企業がAI導入に積極的であることがわかります。
従業員数別でみると、500人以上の層では70%を超える企業が「AI導入計画あり」と回答しており、また規模が大きい企業ほどAI導入に積極的な傾向にあります。業種別では、建設・不動産、製薬・医療以外は70%を超える企業が「AI導入計画あり」と回答しています。

AI導入計画の有無

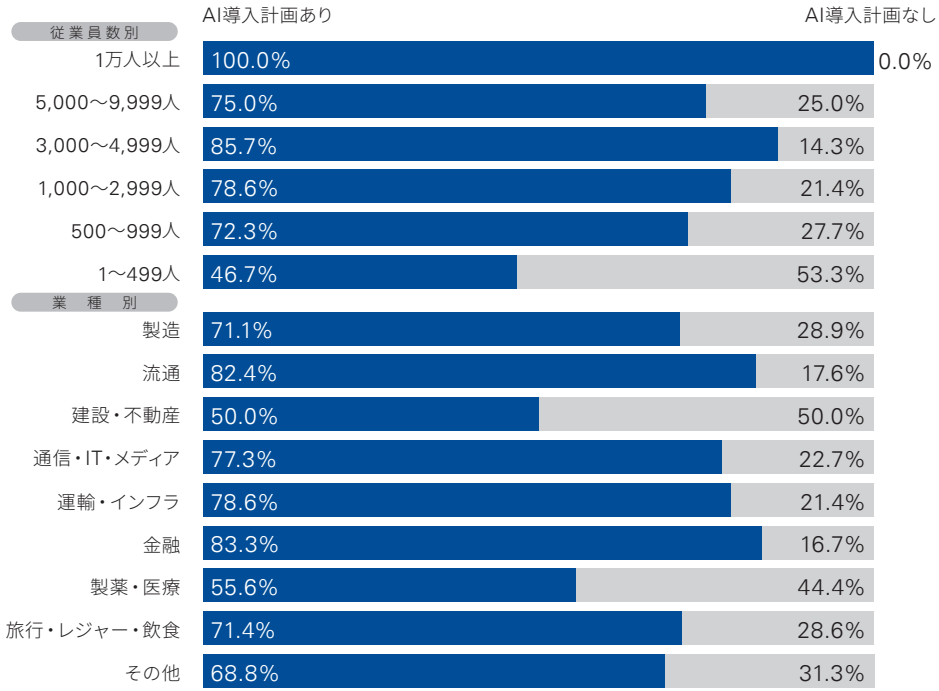
「AI導入計画あり」と回答した企業は70%にのぼる。



n=227

AI導入計画の有無（従業員数別、業種別）

従業員数が多いほどAI導入に積極的である。



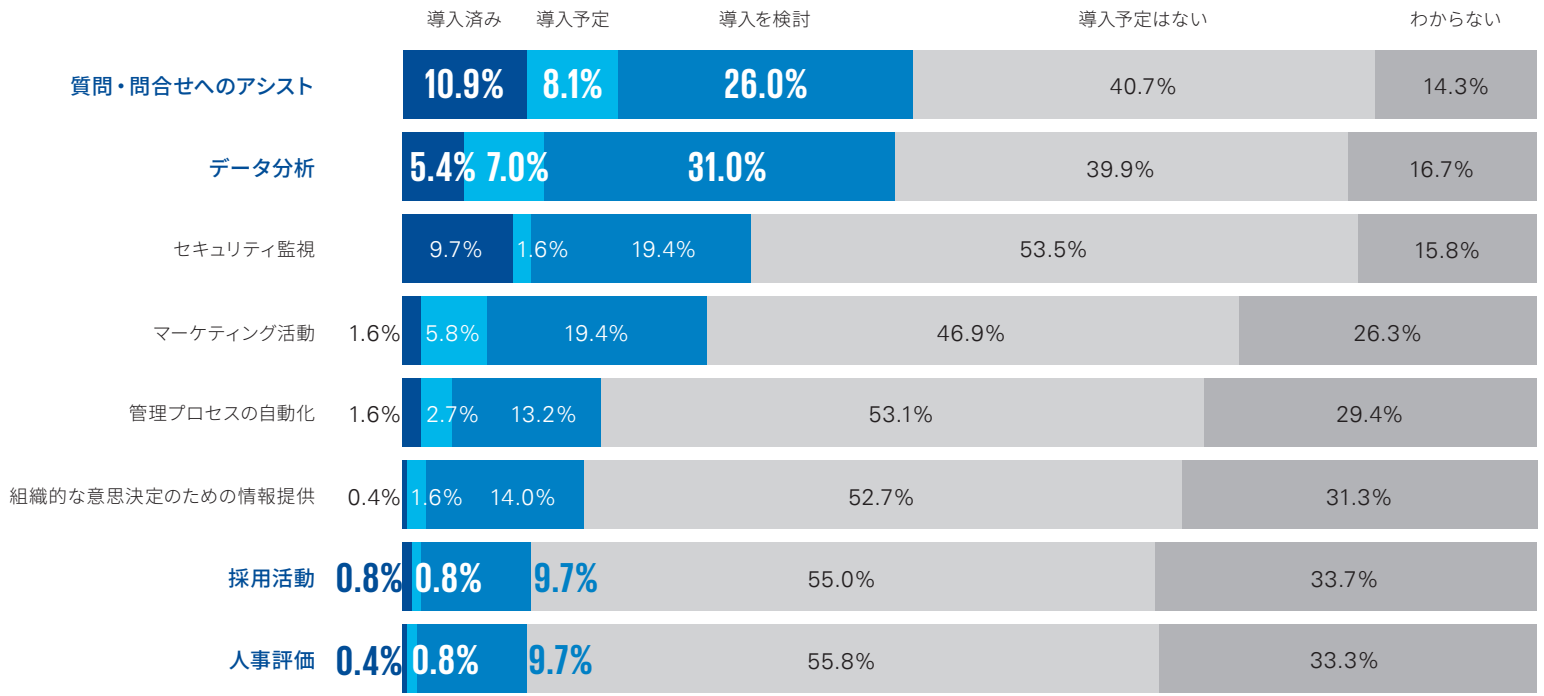
n=227

AI導入状況

AI導入について、「導入済み」、「導入予定」、「導入を検討」を合計すると「質問・問合せへのアシスト」（合計45.0%）、「データ分析」（合計43.4%）で多くの企業が前向きな回答をしています。このようにAIが得意と言われており、かつソリューションの選択肢が比較的多い分野から導入が進む傾向にあります。一方で「採用活動」や「人事評価」では前向きな回答は10%程度にとどまります。このようなプライバシー情報の取扱いに十分な配慮が必要であったり、人間の判断要素が大きいと考えられている分野では、AI導入に抵抗感があることがうかがえます。

AI導入予定分野

AI導入について「質問・問合せへのアシスト」や「データ分析」は積極的、「採用活動」や「人事評価」は消極的な傾向にある。



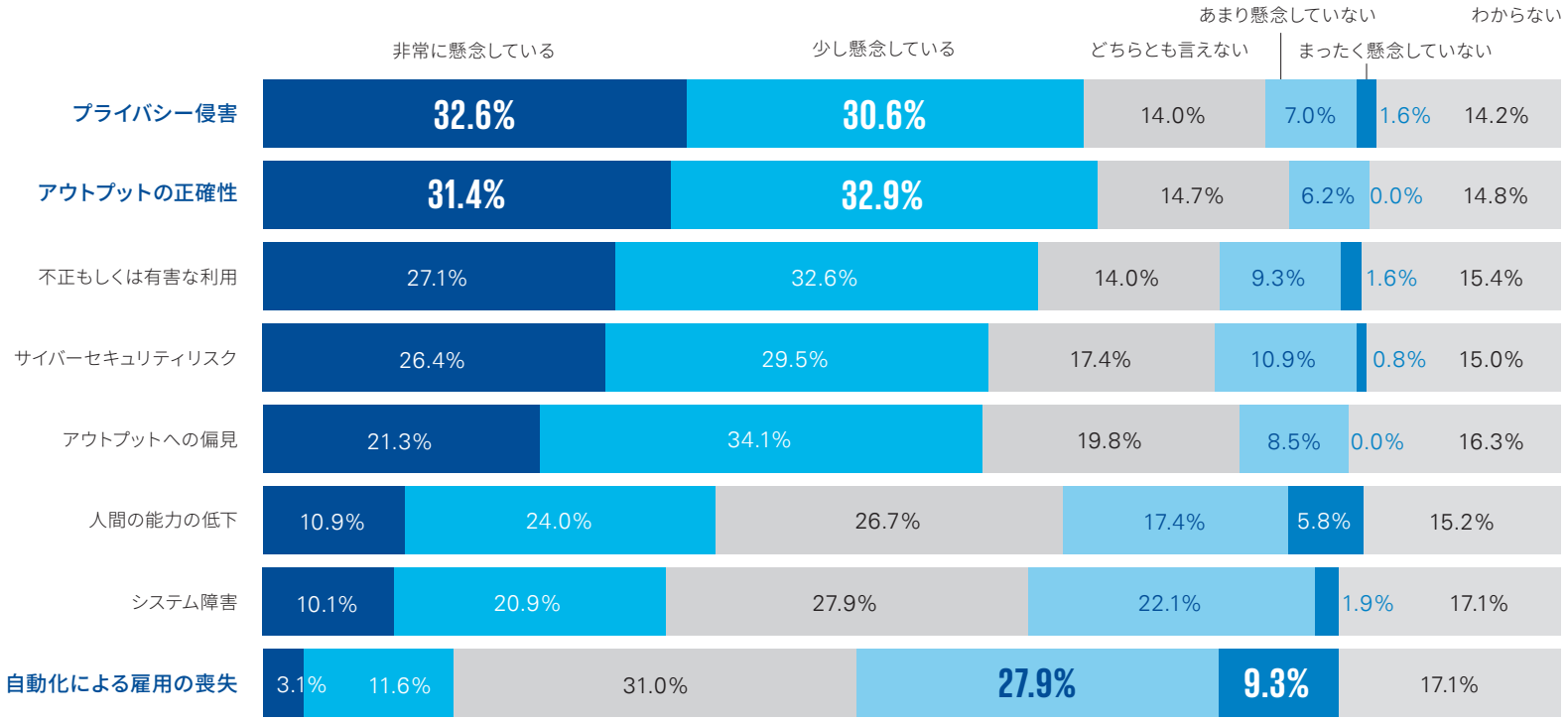
n=258

AI導入リスク

AI導入のリスクでは、「プライバシー侵害」、「アウトプットの正確性」について「非常に懸念している」が30%を超え、「少し懸念している」を含めると60%強が懸念していると回答しています。一方で、「自動化による雇用の喪失」については、回答企業の合計37.2%が「あまり懸念していない」、「まったく懸念していない」と回答しています。
AIのメリットを享受するためには、プライバシー、サイバーセキュリティ、ハルシネーションといったリスクへの対応検討が必要であることがうかがえます。

AI導入リスク

「プライバシー侵害」、「アウトプットの正確性」の順で非常に懸念されており、「自動化による雇用の喪失」は懸念されていない。



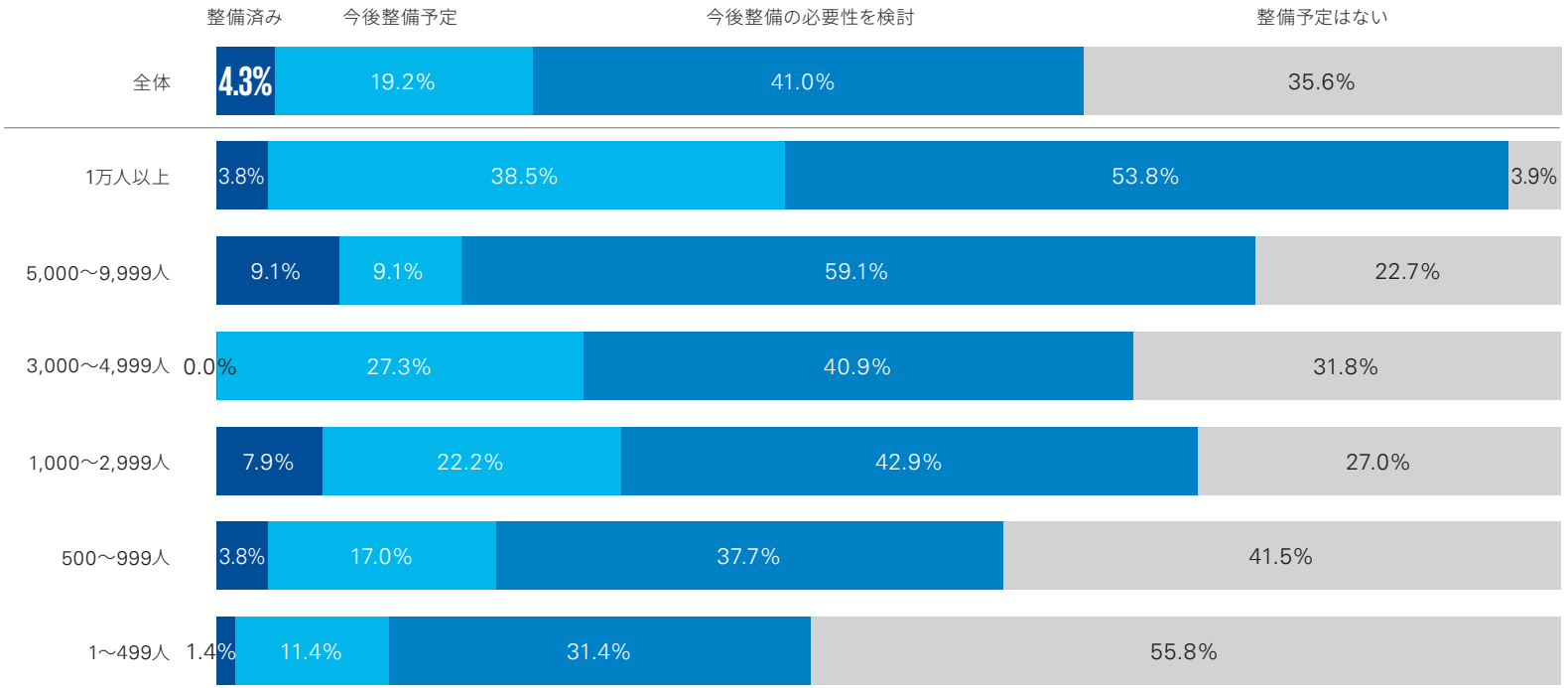
n=258

AIリスク管理（従業員数別）

AIリスクを管理する組織、ルール、プロセスについて、「整備済み」は4.3%にとどまりますが、「今後整備予定」が19.2%、「今後整備の必要性を検討」が41.0%と合計60%強の企業がAIリスク管理への対応を前向きに考えており、今後整備されていくことが期待されます。
従業員数別でみると、「今後整備の必要性を検討」まで含めると、従業員数が多いほどAIリスク管理への対応について前向きに検討される傾向にあります。

AIリスクを管理する組織、ルール、プロセスの整備状況（従業員数別）

AIリスクを管理する組織、ルール、プロセスを整備済みの企業は、現時点では4.3%にとどまる。



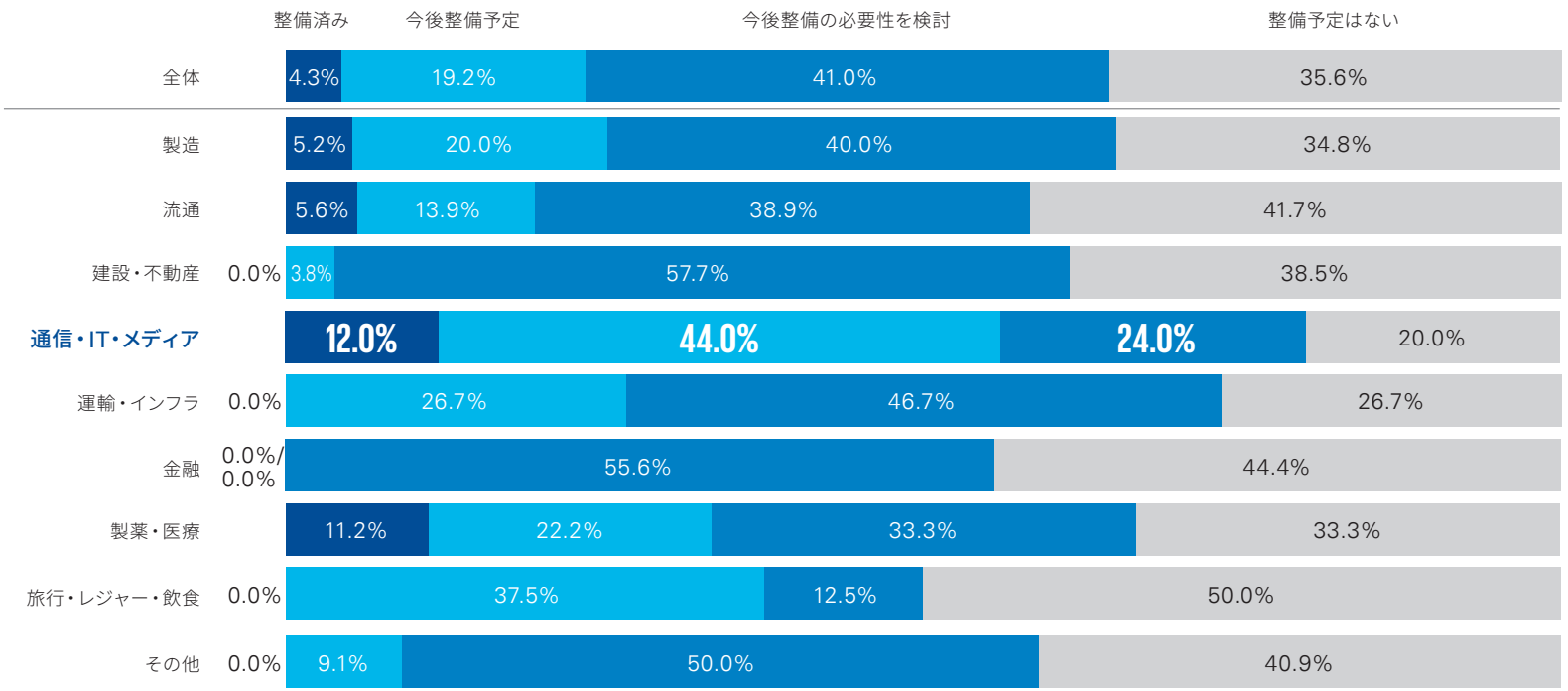
n=258

AIリスク管理（業種別）

AIリスクを管理する組織、ルール、プロセスについて、「今後整備の必要性を検討」まで含めると、通信・IT・メディア（合計80.0%）、運輸・インフラ（合計73.4%）の企業で積極的に導入・検討が進められています。AIと業務の親和性が高く、AIを活用できる人材が比較的多い業種からAIの導入が進められており、AIリスク管理が現実的な課題として顕在化しつつあることがうかがえます。

AIリスクを管理する組織、ルール、プロセスの整備状況（業種別）

AIリスク管理の整備状況について、業種別では「通信・IT・メディア」で最も整備が進んでいる。



n=258

KPMGジャパンのサイバーセキュリティサービス

KPMGジャパンでは、以下のサービスを中心にサイバーセキュリティに関連する
さまざまな支援を実施しています。支援内容はホームページからもご確認いただけます。

kpmg.com/jp/cyber-security

サイバーストラテジー＆ガバナンス

新たなセキュリティリスクに対応するための管理態勢の構築・強化、戦略・方針策定、各種公的認証基準への準拠・維持・審査を支援します。

制御システム／IoTセキュリティ

スマート化する産業用制御システム、IoTサービスのシステムに求められるサイバーセキュリティ対策を支援します。

サイバーインシデントレスポンス

サイバーインシデントの発生時に、初動対応のサポート、侵入経路や原因・被害範囲の特定を目的としたフォレンジック調査、広報支援などのサービスを提供します。

サイバーディフェンス

サイバーセキュリティリスクに対し、テクノロジーの導入やアセスメント、アーキテクチャデザインなど技術的な視点から包括的に支援します。

オートモーティブサイバーセキュリティ

IT／OA、車両／製品、工場／FAの3領域にわたり、オートモーティブに関するサイバーセキュリティ全般を支援します。

サイバーフォレンジック

サイバーインシデントが発生した際の重要なプロセスである証拠保全、および被害内容の特定などの詳細分析について支援します。

プライバシー＆データ規制

グローバル企業における世界各国のデータ保護規制対応に関するサービスをはじめ、プライバシーに関するさまざまなサービスを提供します。

防衛・宇宙

宇宙・防衛に精通したプロフェッショナルが、KPMGの海外組織とも連携し、経営課題の解決を支援し、産業の成長に貢献します。

サイバーデューデリジェンス

ITデューデリジェンスのみならず、サイバーセキュリティやプライバシーリスクも交えた支援を行います。

ISMAP監査支援

ISMAPクラウドサービスリストへ登録された、もしくはこれから登録を目指す企業に、ISMAP監査基準に基づく監査を提供し、ガバナンス・マネジメント・セキュリティ対策状況を確認します。

Powered Enterprise Cyber

KPMGのソリューションである「Powered Enterprise Cyber」を活用し、デジタル時代のサイバーセキュリティ対策を支援します。

お問合せ先

KPMGコンサルティング株式会社

T：03-3548-5111
E：kc@jp.kpmg.com

kpmg.com/jp/cyber-security

本レポートで紹介するサービスは、公認会計士法、独立性規則および利益相反等の観点から、提供できる企業や提供できる業務の範囲等に一定の制限がかかる場合があります。詳しくはKPMGコンサルティング株式会社までお問い合わせください。