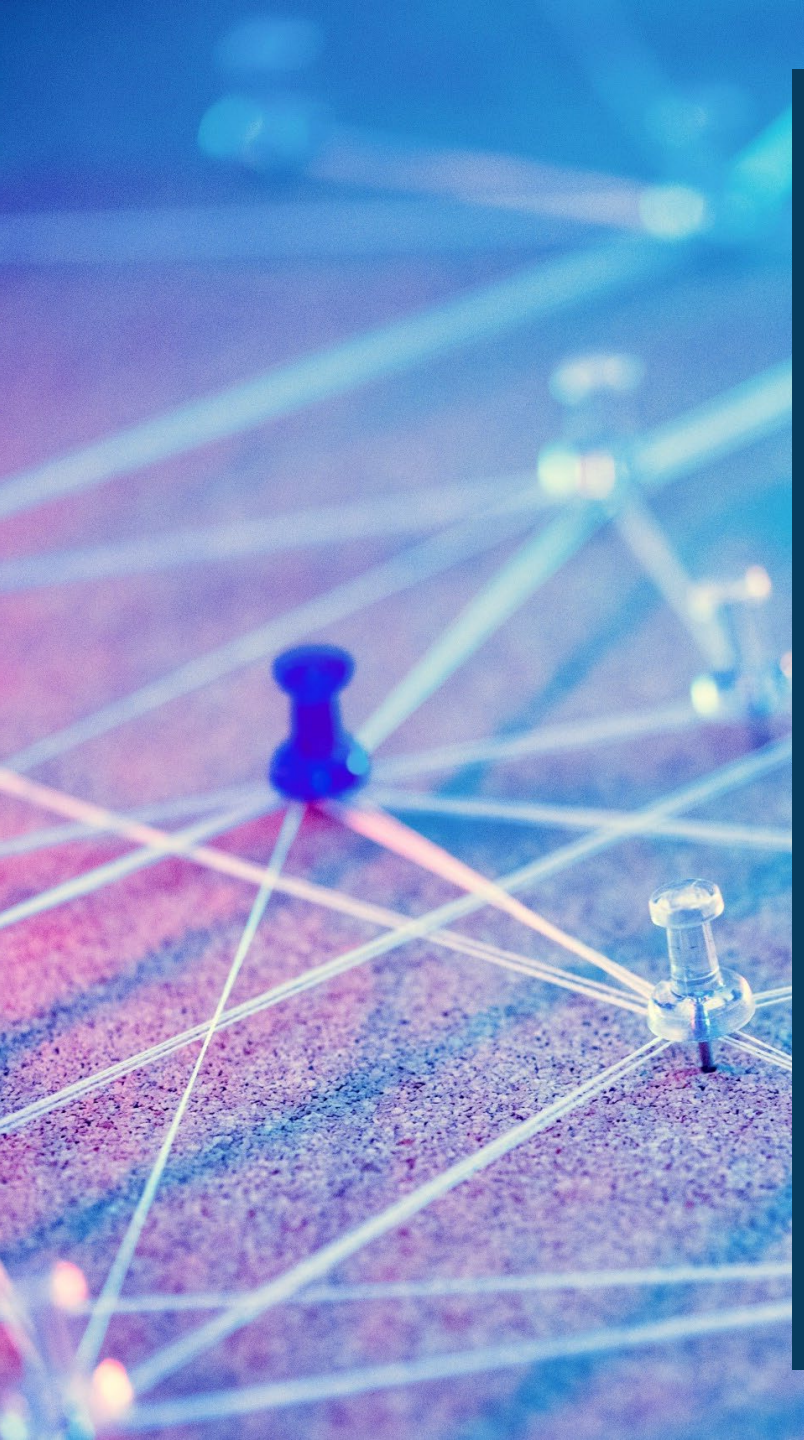
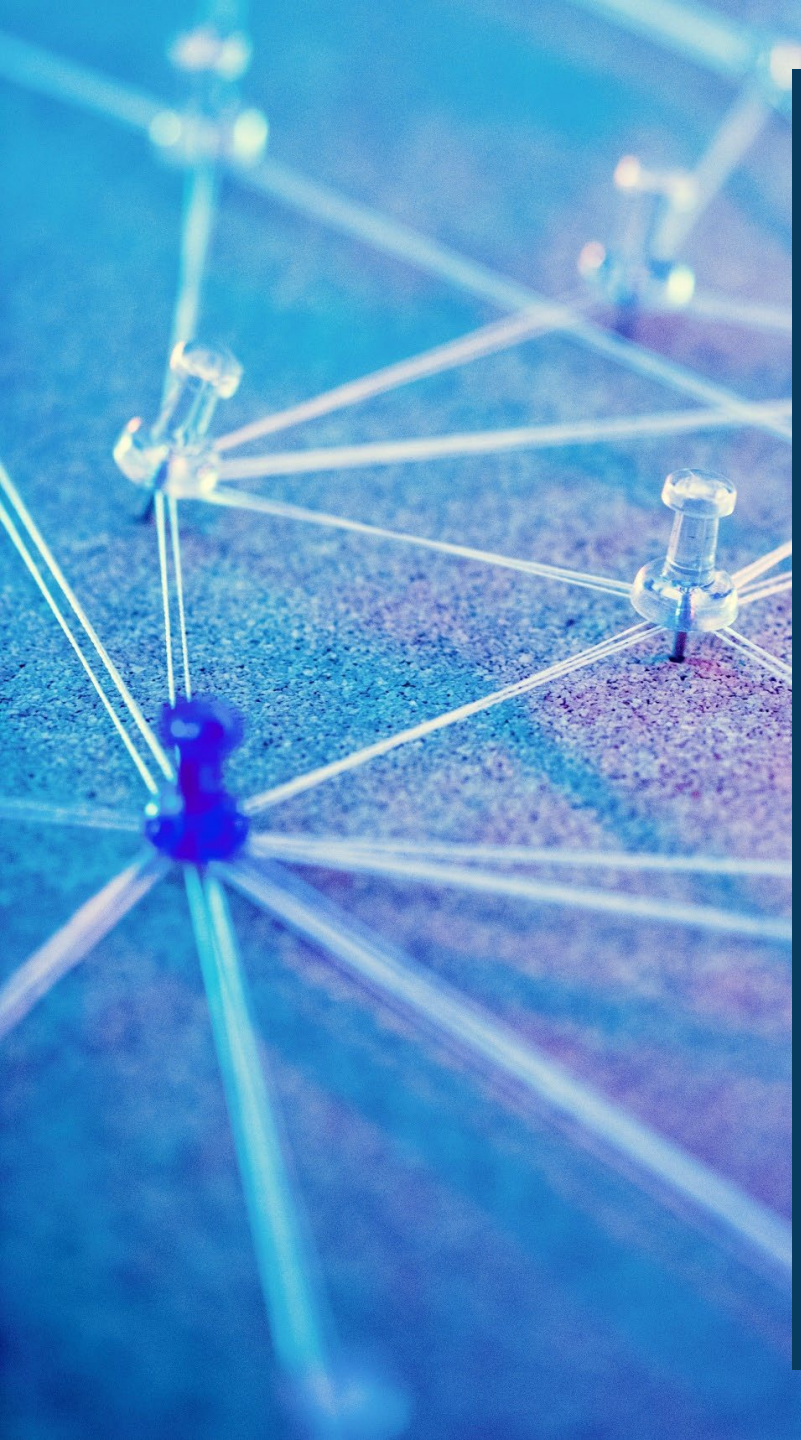
(CS)²AI-KPMG 制御システム サイバーセキュリティ 年次報告書 2024



目次



(CS)²AIより

親愛なる皆様へ

新年を迎えるにあたり、制御システムセキュリティの分野で我々が達成した進歩と引き続き直面している課題について振り返る必要があります。私は根本的に楽観主義者ですが、何百人もの方と個人的に交流した2023年の1年間で得たことは、進歩という長い道のりを確かに歩んでいるという感覚です。ただ1つ変わらないのは、現代の生活様式を可能にするシステムの安全性確保に向けて、依然として取り組むべきことが山積しているということです。

この度、第3版となる「(CS)²AI-KPMG制御システムサイバーセキュリティ年次報告書2024」を発表できることを嬉しく思います。本報告書は、(CS)²AIのアナリストや研究者だけでなく、年々規模を拡大している年次報告書運営委員会の皆様のご尽力によって作成されています。

本報告書は、630人以上の業界関係者、および(CS)²AIの世界各国の会員（約34,000人）を対象に、制御システムのセキュリティインシデント、サイバー攻撃の傾向、重要なシステムや資産を守るために組織が重点的に資金を投じている分野について質問を行った結果に基づくものです。

今回の調査では、制御システムセキュリティ業界における複数の重要な傾向と課題が浮き彫りになりました。サイバー攻撃の増加が懸念される一方で、組織はサイバーセキュリティに対する予算の確保に一段と積極的になり、予防策に重点的に取り組み、サプライチェーンへの攻撃の脅威を認識するようになっています。本報告書で明らかになった重要な課題の1つは、サイバーセキュリティ分野のスキルを持つ人材の不足です。サイバー脅威の高まりに伴い、サイバーセキュリティの専門家に対する需要はかつてないほど高まっています。調査では有能な人材の確保がより困難になったとの回答が寄せられ、既存の従業員のサイバーセキュリティに関するスキルの向上とトレーニングへの投資の必要性が示されています。

本報告書は、多数の皆様のご尽力により作成されました。本報告書のタイトルスポンサーであるKPMGインターナショナルには、数年前の本プロジェクト立上げ以降、報告書の作成に継続的にご協力いただき心から感謝いたします。また、第1版よりともに取り組み、リソースと専門知識を提供してくださるWaterfall Security Solutions社およびFortinet社、価値ある意思決定をサポートいただき、本報告書の作成に毎年ご支援とご指導をいただいているその他のパートナー企業様にも敬意を表します（付録Dを参照）。もちろん、年次報告書運営委員会のメンバーに加わってくださった皆様にも感謝申し上げます（付録Bを参照）。

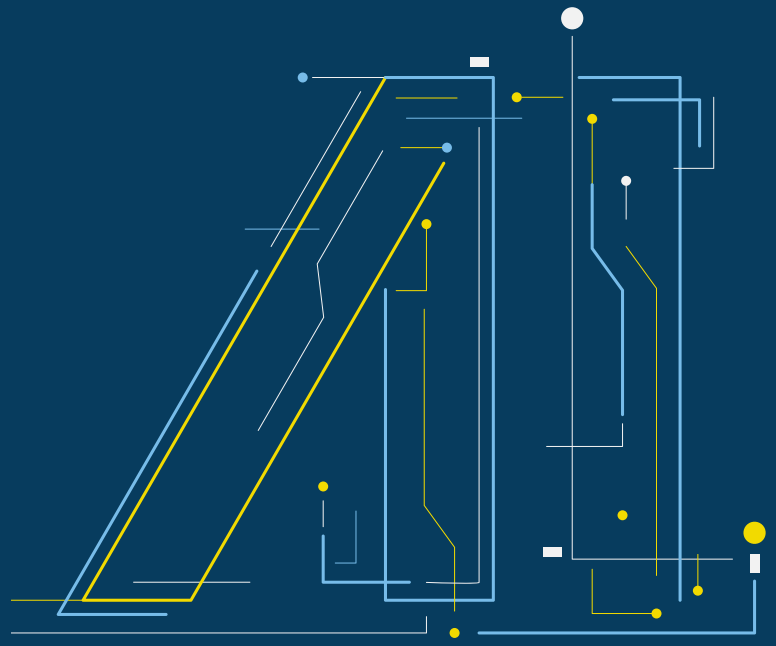
我々の目的は、同業他社の活動に関する有益な洞察を提供し、本報告書を日々の難しい決断を下す際のツールとして活用していただくことです。本報告書の調査結果を活用することにより、十分な情報に基づく意思決定を行い、制御システムセキュリティの投資対効果が最も高い分野に優先的に投資することが重要です。我々は、現代の生活様式を可能にするシステムの安全性を確保するため、コミュニティの取組みを引き続き支援していきます。

Derek R. Harp

Derek Harp氏

Founder & Chairman, (CS)²AI

序文



Walter Risi

Global OT Cybersecurity Leader
KPMGインターナショナル
Partner and Head of Consulting
KPMGアルゼンチン

Pablo Almada

Global OT Cybersecurity Deputy Leader
KPMGインターナショナル
Partner and Head of OT Cybersecurity
KPMGアルゼンチン

運用技術（OT）サイバーセキュリティは、最高情報セキュリティ責任者（CISO）の間で重要な議題として浸透していますが、多くの場合、より広範なサイバーセキュリティ環境のなかでは十分な取組みが行われず引き続き課題となっています。近年、数多くの企業が大きな発展を遂げたにもかかわらず、この分野における成熟度の向上と統合はまだ道半ばの状況です。今回の(CS)²AIとKPMGインターナショナルによる共同調査の結果からは、我々が達成した進歩と引き続き直面している課題の両方が明らかになりました。

制御システムサイバーセキュリティプログラムの成熟度については、レベル1とレベル2に分類された組織の合計が約半数（49%）という結果でした。レベル1はその場しのぎの対応策、レベル2は基本的なマネジメントが実施されているレベルです。OTサイバーセキュリティプログラム確立の必要性はもはや新しい概念ではなくなり、技術的解決策が利用しやすくなっているにもかかわらず、調査結果では成熟度に大きな変化はみられませんでした。特に進歩を妨げている要因は、この分野が何年も悩まされている課題、すなわちスキルを持つ人材の不足です。

このような課題を抱え、発展のペースも比較的緩やかではあるものの、経営層との議論では、OTサイバーセキュリティに関連したリスクに対する認識は高まっていることが明らかになっています。理解を得にくかった過去数年間に比べて、サイバーセキュリティに関する経営層との議論はOTサイバーセキュリティを中心に展開するようになっています。これは、このテーマの重要性に対する理解や認識が深まっていることを示しています。経営層がOTサイバーセキュリティに重点を置いたクライシスシミュレーションや机上訓練により積極的に取り組んでいることは驚くにはあたりません。

KPMGインターナショナルと(CS)²AIが作成した本報告書は、経営層の意識の向上にきわめて重要な役割を果たすと考えます。本報告書は、世界中の担当者やリーダーからもたらされた実社会の洞察に基づき、この分野の世界的な進化に関する中立的な視点を提供します。これにより十分な情報に基づく投資判断を支援すると同時に、この分野への関心の高まりを明らかにします。本報告書は、OTサイバーセキュリティの担当者、リーダー、そして経営層にとって有益な資料になると考えています。今回の第3版では、OTサイバーセキュリティをめぐり、この分野のグローバルリーダーが主な課題と認識しているものについて公平な視点を提供するという我々のミッションを再確認しました。

読者の皆様には、本報告書の洞察を深く掘り下げていただき、担当者、リーダー、経営層を問わず、より詳細な情報に基づく意思決定と投資ができるようになることを願っています。OTサイバーセキュリティに終わりはありません。本調査、そしてサイバーセキュリティ自体が、この終わりのない道のりにおいて不可欠であり、我々は毎年この重要な分野により優れた洞察を届けるべく注力しています。

エグゼクティブサマリー

本報告書は、Control System Cyber Security Association International （(CS)²AI）と約34,000人の会員および、数十もの戦略的提携パートナーのコミュニティによる調査から得られた、年次発行シリーズの最新版です。(CS)²AIチームは、創設者兼会長のDerek Harp氏と共同創設者兼社長のBengt Gregory-Brown氏が主導してきた数十年にわたるサイバーセキュリティ調査の開発、調査、分析に基づいて、世界各国の会員と数千人に及ぶコミュニティに参加を呼びかけました。同調査では、数百万から数十億米ドルの設備投資がかかるOTシステムと資産の運用・保護・防御の最前線での経験や、売上に影響を与えるようなインシデント被害、世界中の企業活動や人々の日常生活への被害の有無などについて、カギとなる質問をしました。また、我々の一次調査には630人を超える方々が回答し、さらにその他多くの方々から、(CS)²教育プログラムを通じて継続的に実施している二次データ収集にご協力いただきました。

参加者の回答に影響を与える可能性のある要素を排除するために匿名による調査を行い、CSの運用と資産に関与する個人と組織が直面し経験する現実について深い洞察を得ることができました。本報告書の詳細な情報が、皆様の組織の意思決定に役立つことを願っています。

主な調査結果

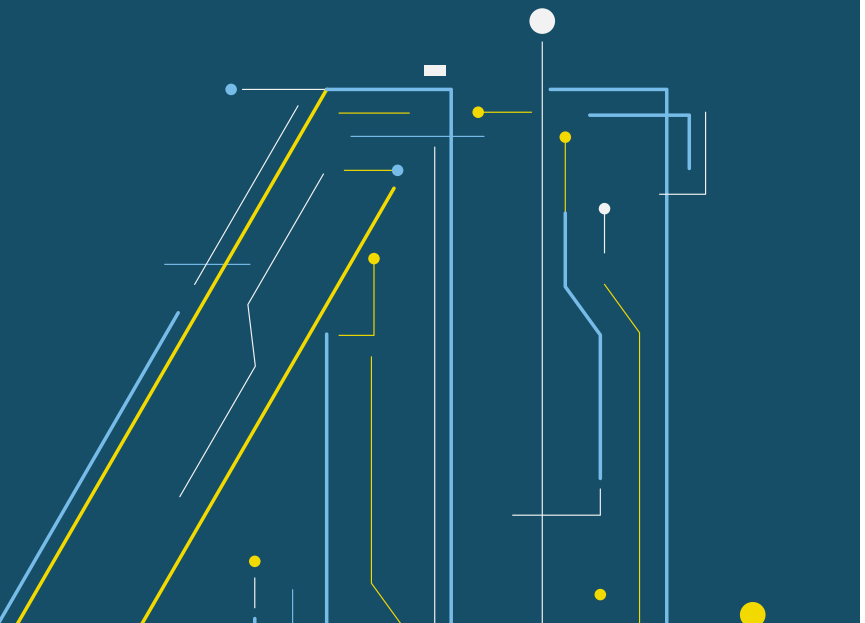
- 約半数（49%）の組織は、依然として産業用制御システム（ICS）／OTサイバーセキュリティプログラムを利用していないか、基本的なプログラムのみを利用しています。このような組織では、計画、手順、能力向上プロセスなどが確立されていません。
- 役職クラスによって、それぞれが裁量権を持つ追加資金の配分の優先順位が大きく異なることが明らかになりました。このことは、組織内のインセンティブに整合性があるのか、なぜ役職クラスによって目標が異なるのかという問題を提起しています。
- 制御システムのネットワーク稼働状況の監視を完全に実施している組織が増加し、前回から8割増となりました。
- 各制御システム要素（PLC[1]、IED[2]、RTU[3]、HMI[4]、サーバ、ワークステーション、ヒストリアン機能）について、ビジネスネットワーク、インターネット、クラウドおよび、ベンダー／インテグレーターによるアクセシビリティを評価しました。この分野では、高成熟度組織と低成熟度組織の間でそれほど大きな違いはみられませんでした。ただし、高成熟度組織の要素は、多くの場合で低成熟度組織よりもアクセシビリティが高い結果となりました。
- 「高成熟度組織」と「低成熟度組織」の定義については8ページをご参照ください。

1 プログラマブルロジックコントローラ
2 高性能電子装置
3 遠方監視制御装置
4 ヒューマンマシンインターフェース

調査の目的と方法

本報告書では、物理的な装置やプロセスを管理、監視、制御するあらゆるシステムを「制御システム（CS）」および「運用技術（OT）」としています。CSまたは（CS）、OTには、産業用制御システム（ICS）、監視制御およびデータ収集（SCADA）、プロセス制御システム（PCS）、プロセス制御領域（PCD）、建物／設備制御、自動化および管理システム（BACS/BAMS/FRCS等）、ネットワーク接続型医療機器などが含まれます。

また、(CS)²という用語は、制御システムサイバーセキュリティの分野、専門職、プログラム、労働力を指します。



(CS)²AI-KPMG制御システムサイバーセキュリティ年次報告書の作成は、エンドユーザー、ベンダー、経営層、マネージャー、運用担当者など、セキュリティ制御システムの資産および運用にかかわる世界中のすべての関係者を対象に、十分な情報に基づく意思決定を支援するツールの作成を目的として、2019年に始まりました。

本報告書は、以下の団体の協力により作成されました。

- (CS)²AI：プロジェクトの発案者として、データの収集・分析、本報告書の執筆・作成など、プロジェクトの企画、指導、実施において主要な役割を担う。
- KPMGインターナショナル：プロジェクトのタイトルスポンサーとして、(CS)²AIの機能強化のため、資金面および組織面で主要なサポートを提供。
- その他のスポンサー：Fortinet社、Waterfall Security Solutions社、Opscura社といったスポンサー企業が、追加の資金やその他のリソースを提供（付録D：スポンサー企業を参照）。

(CS)²AIとスポンサー企業は、前述の調査目的に従って、現場で働くCS/OTサイバーセキュリティコミュニティのメンバーを対象にオンライン調査を実施し、CSに係る事象、活動、技術、および脅威の全体像[5]の変化への組織の対応に関して主要なデータを収集しました。

(CS)²AIは、できるだけ多くのサンプルを収集するため、関連メンバーやOTセキュリティの担当者・研究者に参加を呼びかけ、直接またはさまざまな放送メディアチャネルを通じて調査票を配布し、CSサイバーセキュリティ担当者向けのサイトでの展開を実施しました。回答者は、現在または最近、(CS)²の分野に関与しているとの認識に基づき自発的に調査に参加しています。また、回答者には、サイバーセキュリティの専門家や内容領域専門家（SME）、制御システムのセキュリティと保護の専任ではなくそれ以外の業務も兼任している人など、さまざまな役職クラスの関係者が含まれています。

回答者をさまざまなグループに分け、そのグループの関連性に照らして回答を比較することが、この年次調査プロジェクトから得られる洞察のカギとなります。我々は、組織における(CS)²AIプログラムの成熟度が最も重要な要素であると同時に、役職クラス、地域、(CS)²資産との関係性（ベンダー、ユーザー、オーナー、オペレーター）も重要であると考えています。もちろん、縦断的な分析も実施しました。これにより興味深い傾向がみられた場合には本報告書内で示しています。

5 脅威の全体像：CS/OTの運用と資産に対して起こり得るすべての脅威。脅威の状況は動的であり、脆弱性が発見され、その悪用に対抗するための保護策が開発されるにつれて絶えず変化する。

* 本報告書は、2024年4月にKPMGインターナショナルと(CS)²AIが共同で発行した「The (CS)²AI - KPMG Control System Cybersecurity Annual Report 2024」を翻訳したものです。
* 本報告書では、少数点第1位で四捨五入しているため、合計値が100%にならない場合があります。
* 本報告書内のグラフは、小数点以下も含めたデータを基に作成しているため、表記数値とは必ずしも一致しません。

(CS)²プログラム

組織が利用する(CS)²プログラムの成熟度の測定は本調査のカギであり、その他の多くのデータを評価する際の指標となります。より成熟度の高いプログラム[6]を利用する組織は、他の組織と何が異なっているのでしょうか。また、利用頻度がどれほど高いのでしょうか。こうした高成熟度組織と低成熟度組織の間に大きな差異がみつかった場合には特記しています。各参加者に、自組織に当てはまるレベルを回答してもらいました。

制御システムサイバーセキュリティプログラムの成熟度

レベル5

サイバーセキュリティプロセスは、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ます。プロセスを実行する担当者は、十分なスキルと知識を保有しています。また、プロセスは最適化・自動化・統合化されており、予測可能な状態です。

＜積極的なディフェンス：最適化、自動化、統合化、予測可能＞

レベル4

組織のサイバーセキュリティプログラムは、成果を向上させるためにデータの収集と分析を実施しています。活動は文書化された組織の指示により行われ、標準規格とガイドラインの両方またはその一方の遵守要件が方針に含まれます。制御システムセキュリティの担当者は、訓練と経験を積んでいます。また、プログラムは一部が自動化され、指標の追跡や事前検知に対応しています。

＜積極的なディフェンス：セキュリティ情報とイベント管理（SIEM）、異常検知、侵害検知等を実施＞

レベル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ます。主要なステークホルダーは特定され、サイバーセキュリティに関与し、プロセスを支援するための適切なリソース（人、資金、ツール）が提供されています。また、実装するための規格やガイドラインも特定されています。

＜消極的なディフェンス＞

レベル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ます。知識体系が構築されつつあり、ベストプラクティスが実行されているものの、アドホックの可能性があります。

＜消極的なディフェンス＞

レベル1

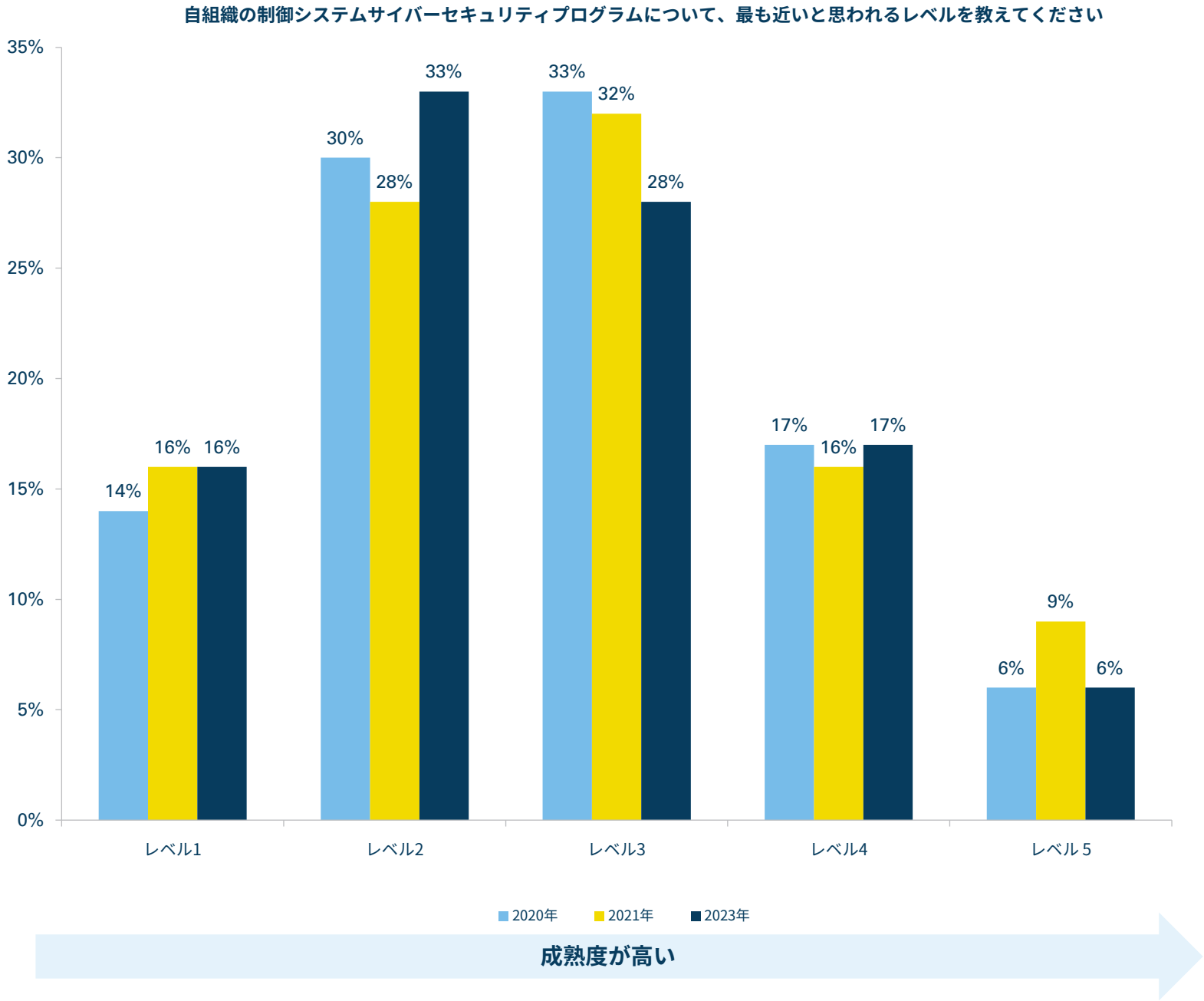
その場しのぎの対応策が取られています。サイバーセキュリティのプロセスは未整理で文書化されておらず、「プログラム」において整理されてもいません。プロセスが十分に定義・文書化されていないため、再現性や拡張性はなく、セキュリティ対策の成功は個人の努力に依存しています。

＜消極的なディフェンス＞

6 レベル4、レベル5の組織を「高成熟度組織」、レベル1、レベル2の組織を「低成熟度組織」と定義します。

(CS)²プログラムの成熟度：縦断的分析

各レベルに分類された回答者の数には変動がみられ、特にレベル2の回答者が増加しました。しかし、高成熟度組織と低成熟組織の各グループの総計はほとんど変化していません。回答者は、自組織の(CS)²プログラムについて一貫性を持った評価を続けています。我々は、この自己評価は妥当であると考えています。このデータは、提言のベースとなるものとして、高成熟度組織（レベル4およびレベル5）と低成熟度組織（レベル1およびレベル2）の差異および類似点の分析に幅広く活用されています。



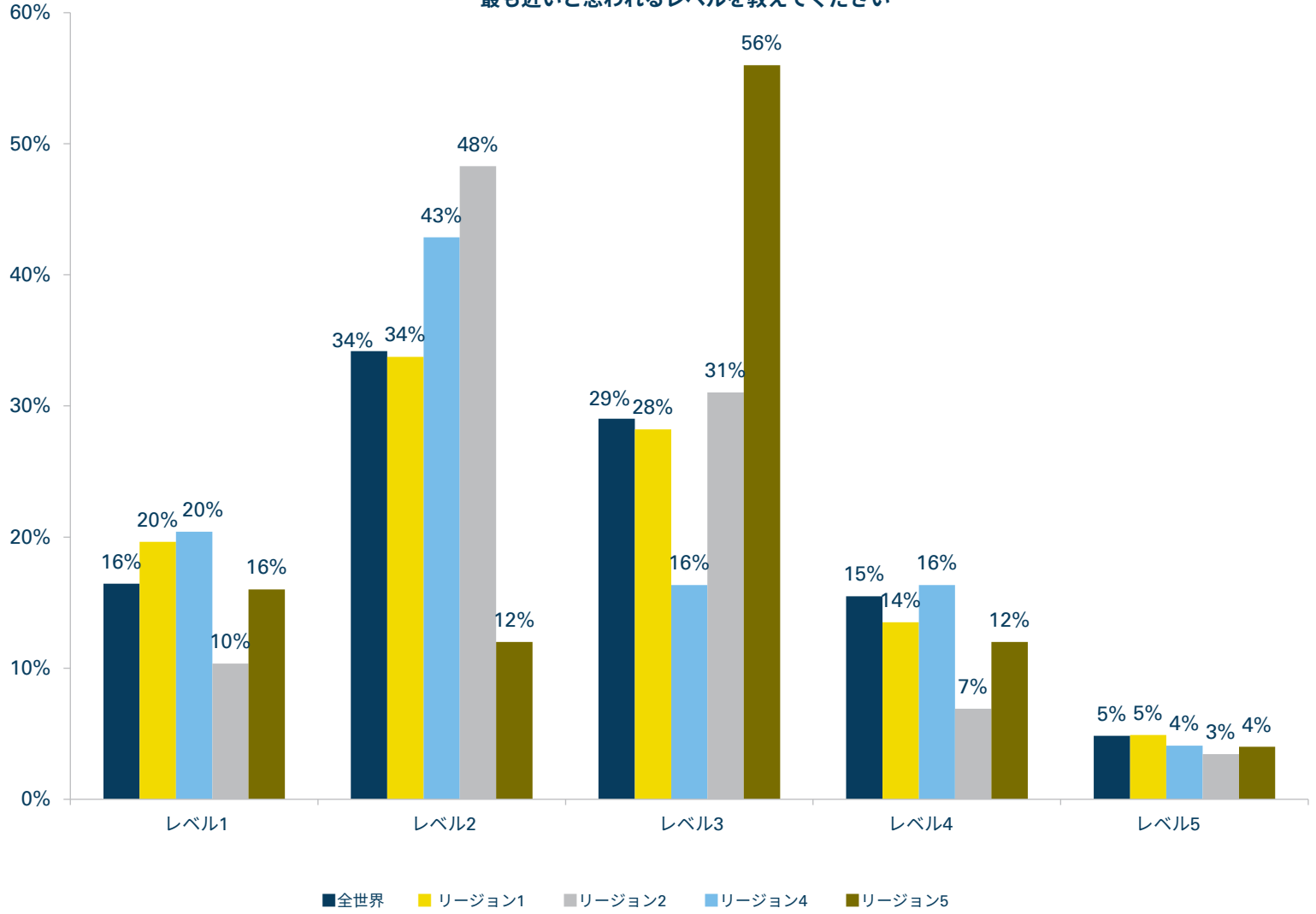
顧客企業の(CS)²プログラムの成熟度：地域別[7]

世界各地のコンサルタント（ベンダー、サービスプロバイダー、インテグレーター）は、顧客企業の(CS)²プログラムの成熟度について異なる見解を持っています。地域によっても成熟度に関する考え方は異なります。リージョン2は自己評価が低く、レベル1およびレベル2が63%を占めています。リージョン4はレベル2の割合が多く（48%）、リージョン5はレベル3に集中しています（56%）。リージョン3、リージョン6、リージョン7では、分析を行うための十分な回答数を得られませんでした（脚注7を参照）。

7 (CS)2AIは回答者を7つの地域に分類しました。

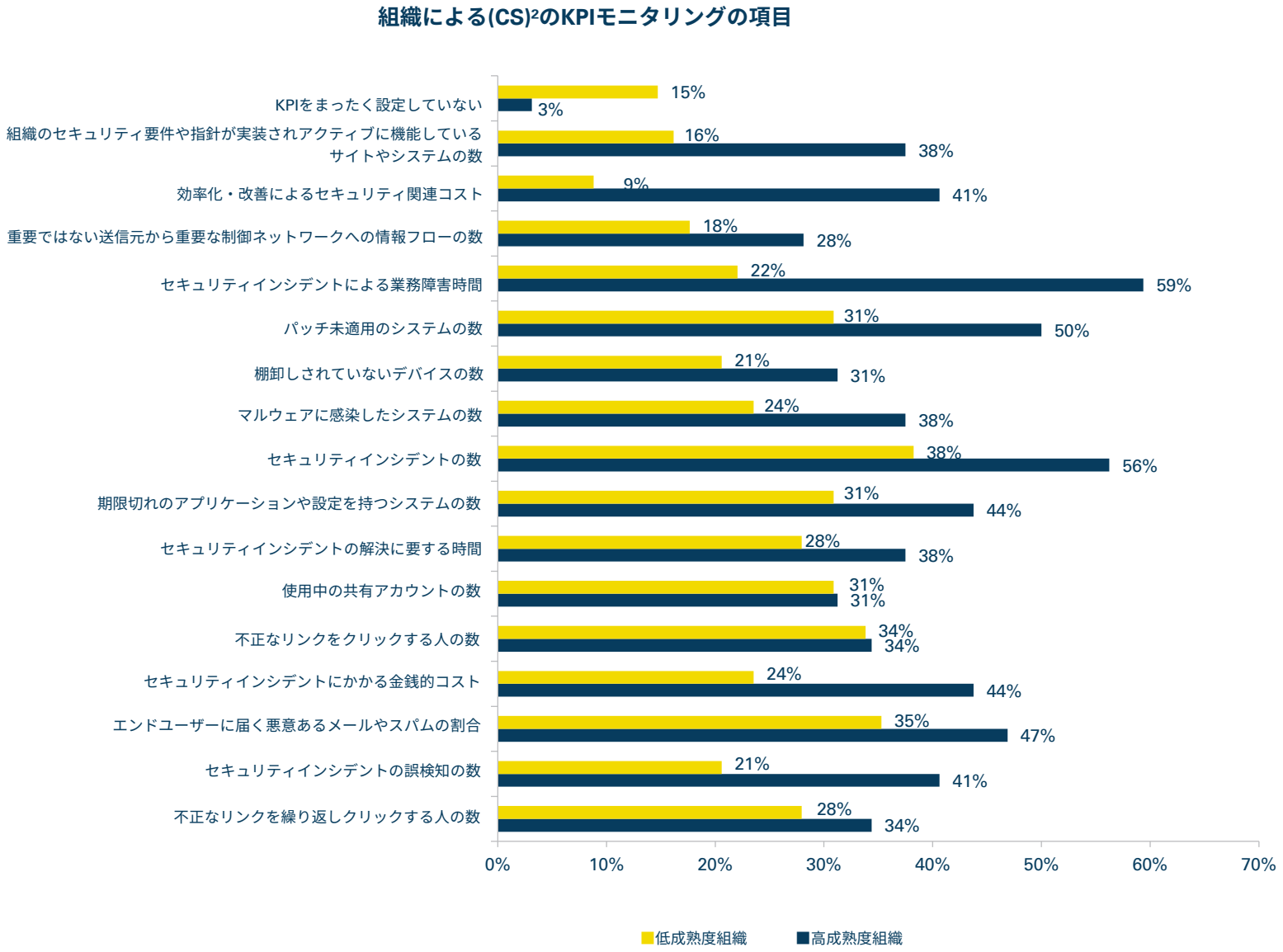
1) 北米
2) 欧州（中欧、西欧、北欧、南欧）
3) ユーラシア大陸
4) インド太平洋
5) 中東・北アフリカ
6) 南アフリカ
7) ラテンアメリカ・カリブ海地域

自組織の顧客企業における制御システムサイバーセキュリティプログラムについて、最も近いと思われるレベルを教えてください



(CS)²の重要業績評価指標（KPI）：高成熟度組織と低成熟度組織の比較

高成熟度組織が低成熟度組織よりも多くの重要業績評価指標（KPI）を設定していることは驚くにはあたりませんが、KPIを設定していると回答した低成熟度組織の割合が少ないことが懸念されます。「効率化・改善によるセキュリティ関連コスト」をKPIとして設定しているとの回答は低成熟度組織の9%に対し、高成熟度組織は41%と約5倍に上りました。この項目はあらゆるプログラムを改善するために長期的かつ重点的に取り組むもののため、予想の範囲内の結果でした。今回の調査では、低成熟度組織に分類された組織は高成熟度組織の約2倍となりました。低成熟度組織の85%が何らかのKPIを設定していることは心強い結果ですが、ほとんどの低成熟度組織はごくわずかしかモニタリングを行っていません。こうした組織は、より優れた可視性を獲得するための指標をセキュリティプログラムの有効性にまで拡大することが強く推奨されます。

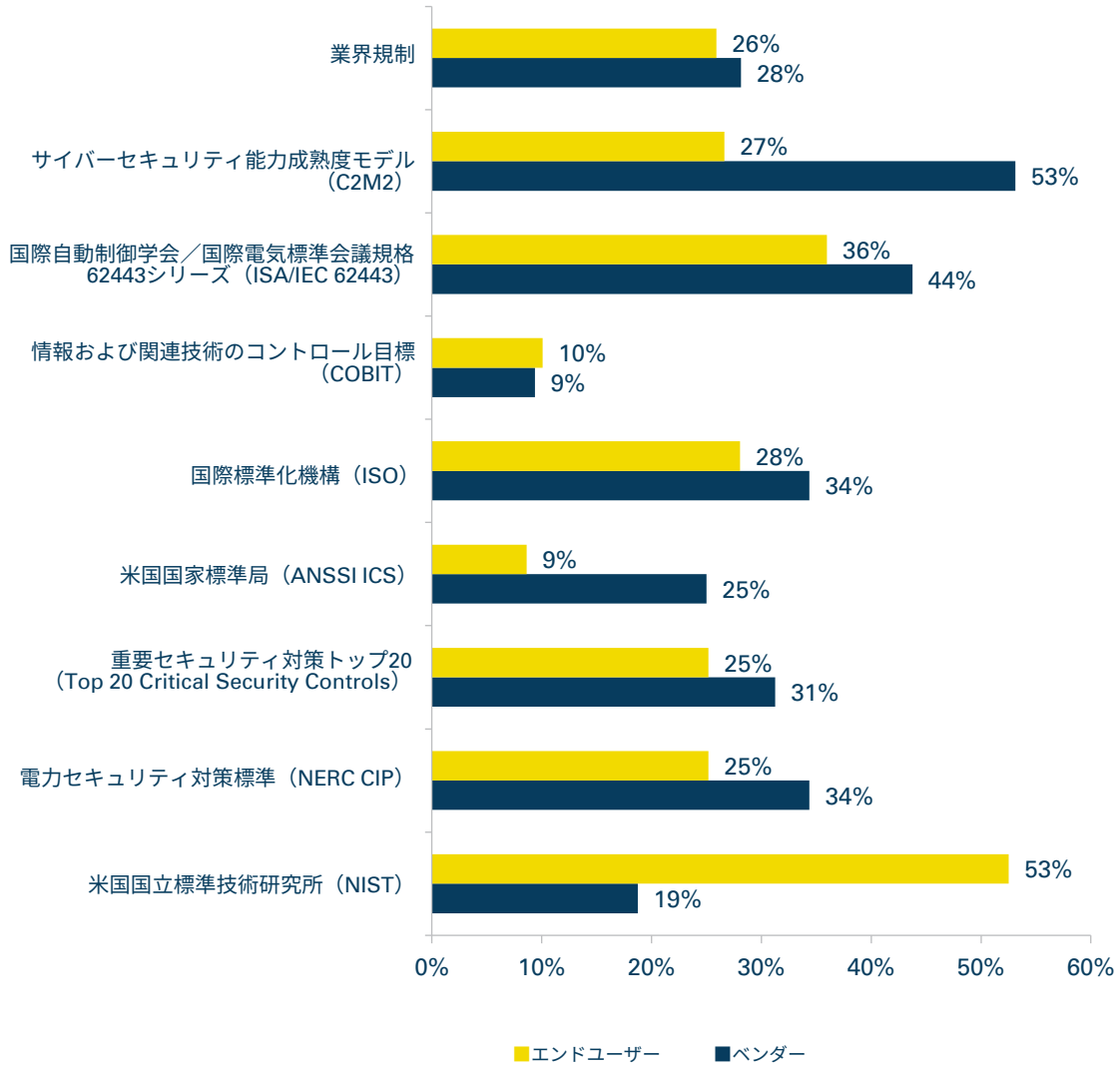


利用されているセキュリティフレームワーク：エンドユーザーとベンダーの比較

性質の異なるグループの回答を比較することには否定的な意見もありますが、制御システムのセキュリティに責任を持つ2つの回答を並べて比較することは有益であると我々は考えています。調査結果によると、利用されているフレームワークではC2M2とNISTが突出しており、前者はベンダー向け、後者はエンドユーザー向けであることがわかります。エンドユーザーがC2M2を利用している割合は、前回の全回答者の結果（26.2%）とおおむね一致していますが、前回の調査ではエンドユーザーとベンダーの回答を区別していませんでした。

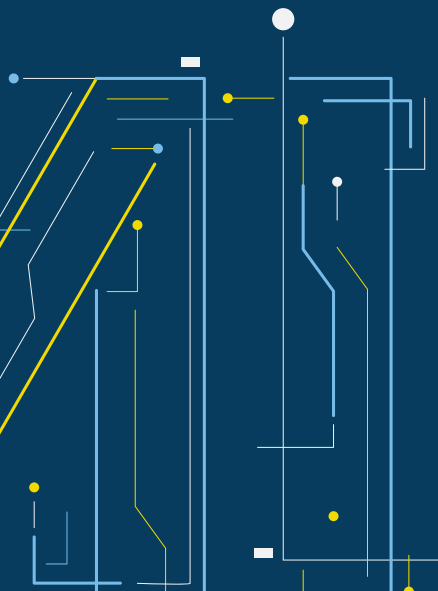
今回の調査では、エンドユーザーとベンダーから別々に回答を得た結果、ベンダーがC2M2を利用する割合はエンドユーザーの約2倍でした（エンドユーザー：27%、ベンダー：53%）。NISTの利用状況に大きな変化はみられず、前回（2021年）の結果45.7%に対して、今回は2つのグループの平均が45%以内に収まっています。

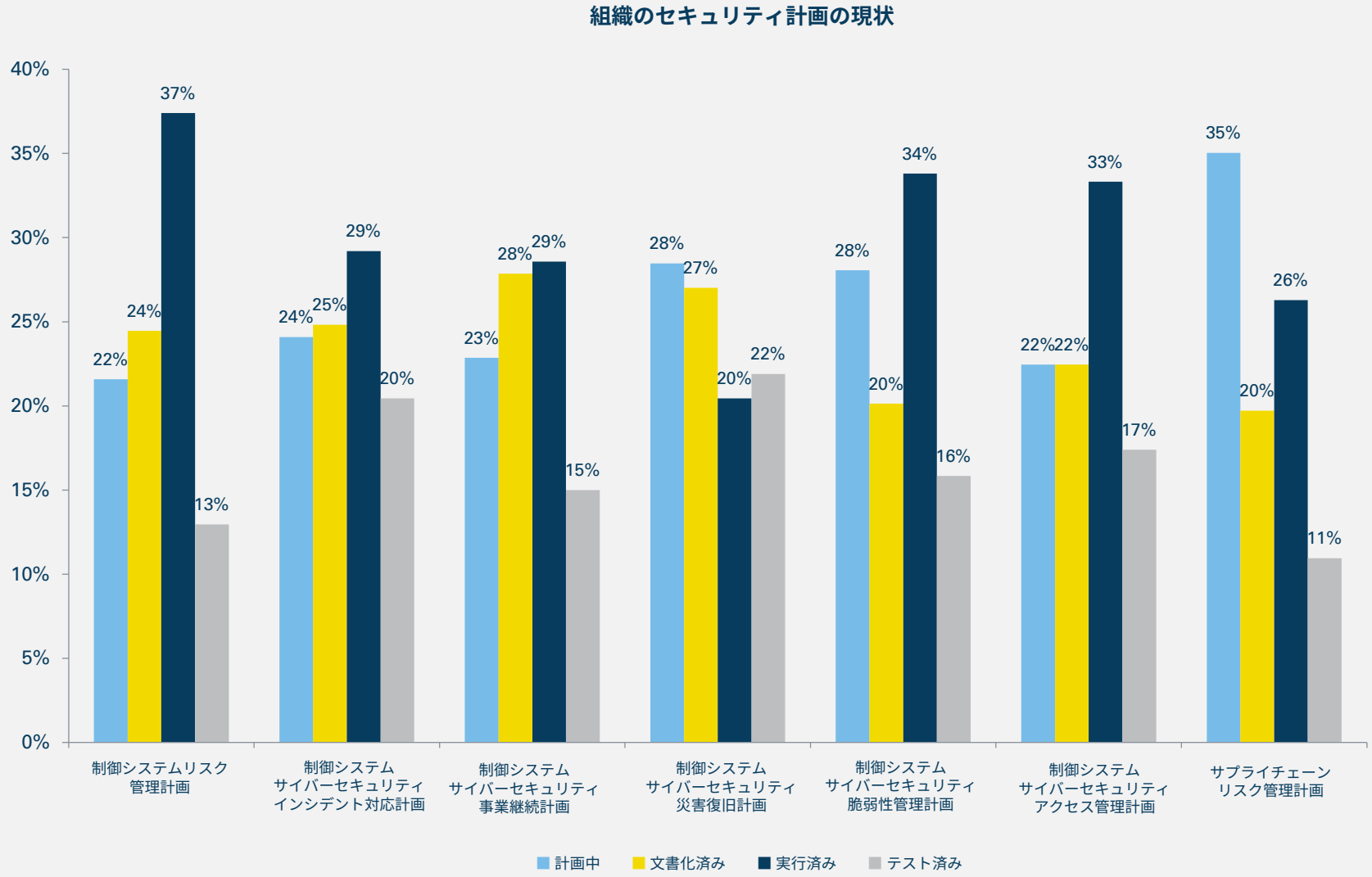
制御システムのセキュリティチームが利用しているフレームワーク



組織のセキュリティ計画：エンドユーザーの回答

(CS)²に責任を持つあらゆる組織は、インシデントを減らし、企業・従業員・顧客への影響を最小限に抑えられるよう、文書化・実行・テスト済みの計画や手順を用いてリスクを包括的に管理する必要があります。計画が完全に「実行済み」かつ「テスト済み」の状況をゴールドスタンダード（絶対的な基準）とすれば、回答した多くの組織では計画状況の大半が「文書化済み」または「計画中」の段階にとどまっており、これらの計画で想定されるインシデントの管理と対応に必要な手続き上の準備が整っていない点が懸念されます。





(CS)²のサービス：エンドユーザーの回答

組織は(CS)²関連の資産・人材・運用を保護するうえで必要な支援をどこから得ているのでしょうか。回答によると、サービスの提供元はさまざまです。「社内ITセキュリティリソース」（56%）の回答が突出して多いことから、多くの組織ではIT部門がOTサイバーセキュリティを推進していることが示されており、ITセキュリティの手段やテクノロジーはこうした環境で利用されている可能性があります。

多くのCISOはOTセキュリティプロジェクトを恐れています。なぜなら、工場のサイバーセキュリティを治療することは病気の治療よりも大変だからです。私もCISOの経験があるため、その気持ちは理解できます。ITがダウンタイムよりセキュリティを優先するのに対して、OTではプロセスを優先させる必要があります。

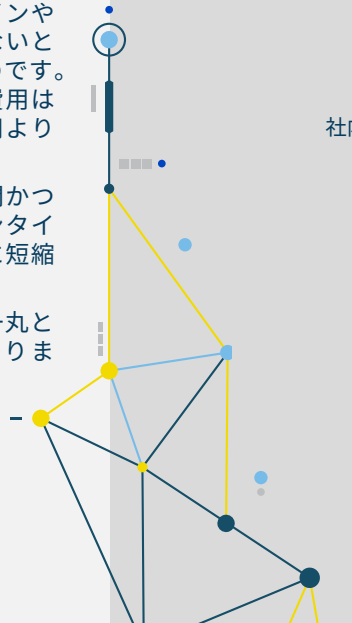
私たちがサイバー攻撃者との戦いに負けているのは、何もしていないことが大きな要因です。従来のITツールを利用してOTを保護するには費用がかかります。その原因は、コンサルティング、計画策定、設備導入、そして何よりもダウンタイムによる影響が大きいです。

運用担当者は、ネットワークを再構成し、稼働中の（しかし寿命の近い）資産を入れ替え、セキュリティチームを配置するという、痛みを伴う決断を下さなければなりません。また、これらすべてを行うために、数週間とはいかないまでも、数日間は工場を閉鎖する必要があります。生産ラインや設備のサイバーセキュリティを進めないという厳しい決断を彼らに強いているのです。多くの場合、ダウンタイムにかかる費用はセキュリティプロジェクト自体の費用よりも高くつきます。

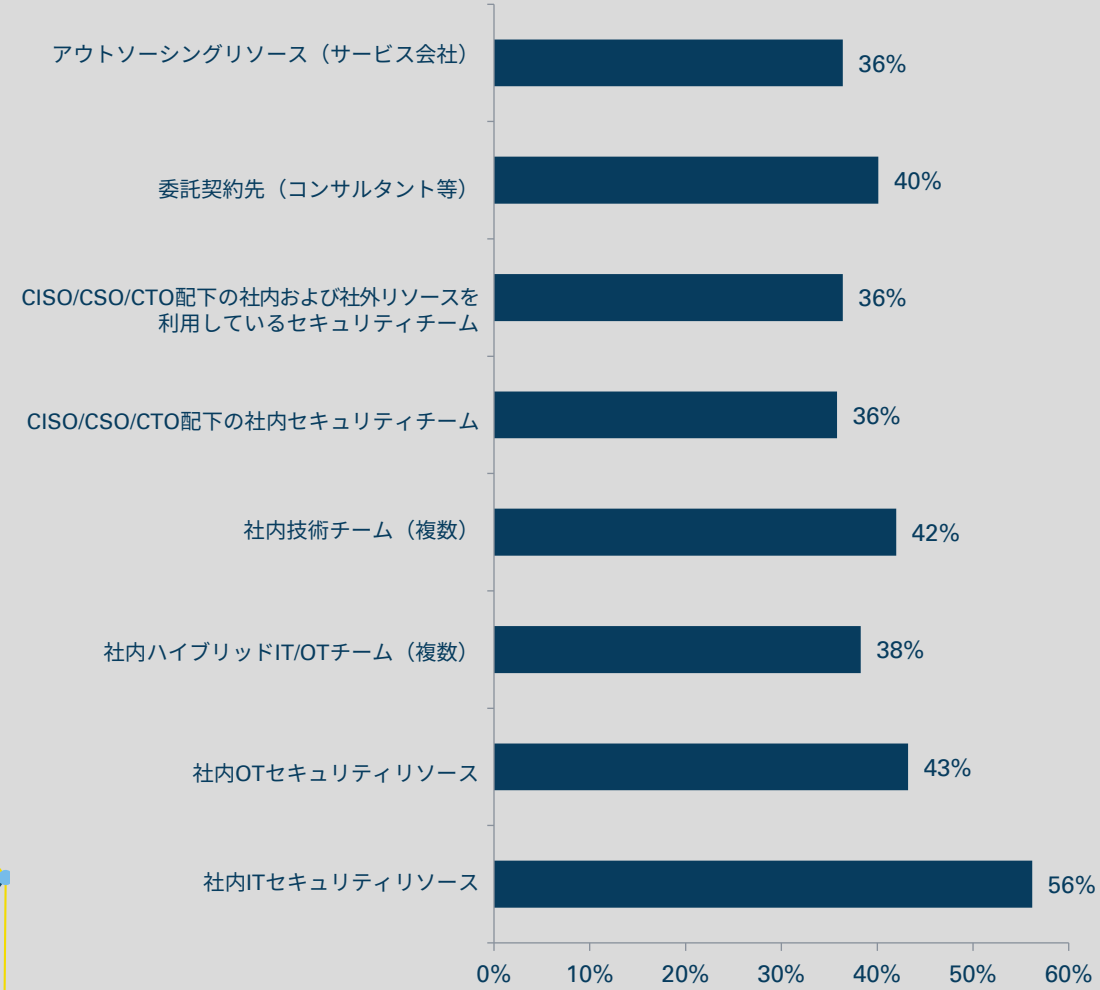
工場や設備の保護と維持をより短時間かつ低コストで行い、また何よりもダウンタイムを（ゼロではないにしても）大幅に短縮する必要があります。

ともに従来のITの障壁を取り払い、一丸となって私たちの世界のインフラを守りましょう。

Brian Brammeier氏
CEO
Opscura社

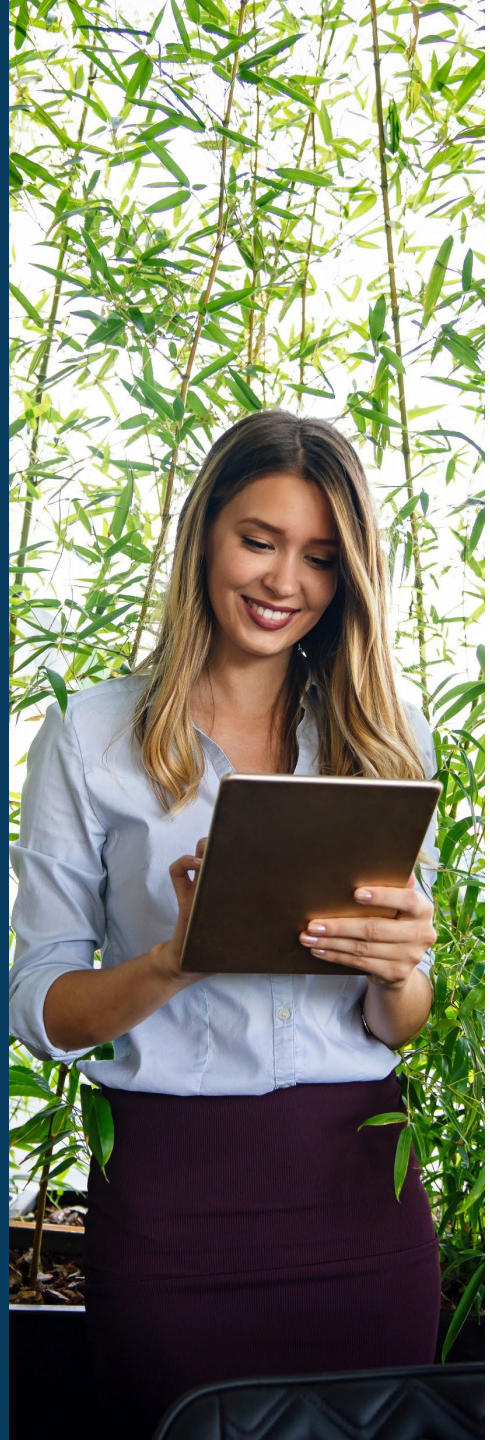


組織が利用している制御システムセキュリティサービスの提供元

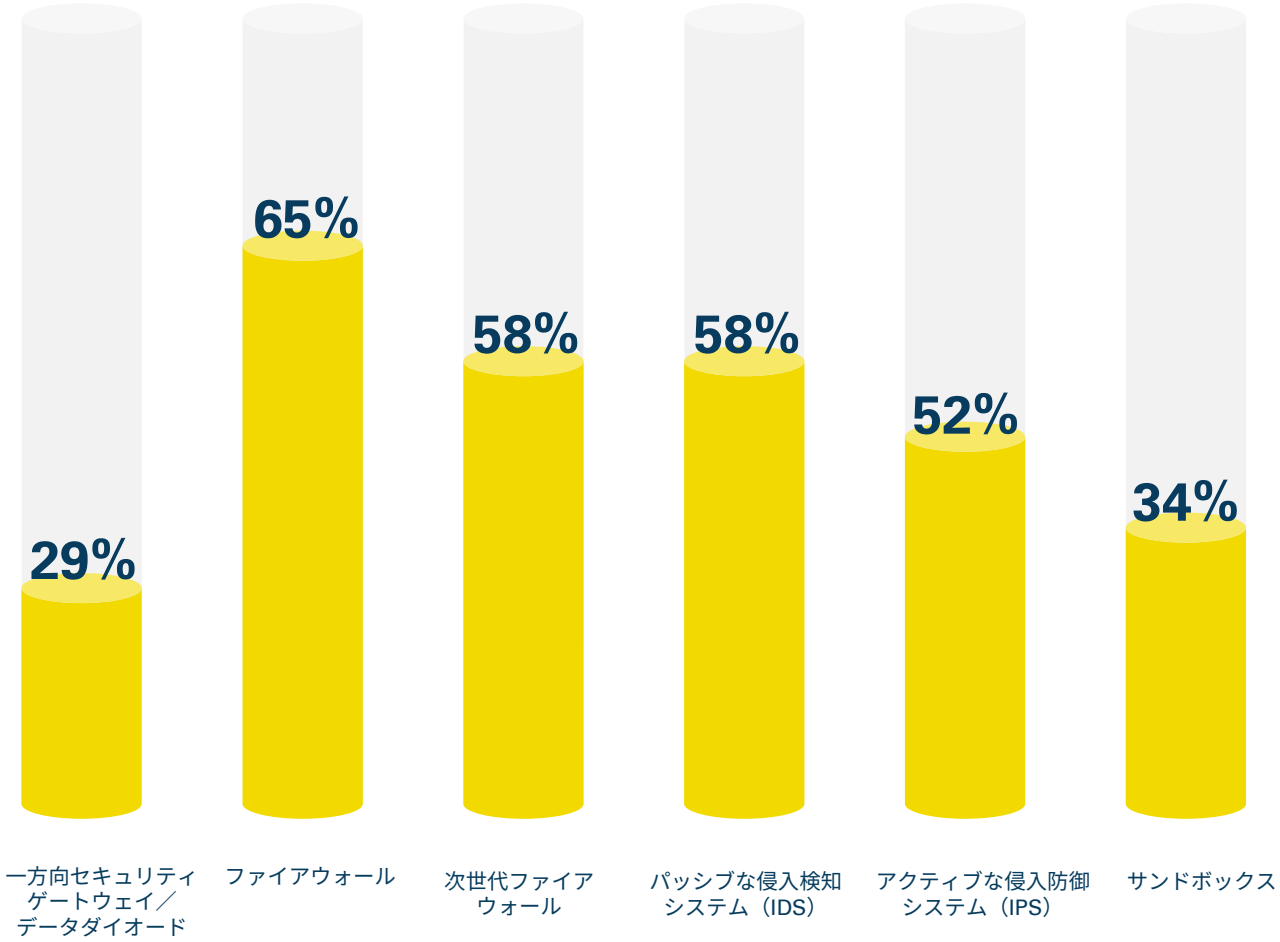


(CS)²テクノロジー：エンドユーザーの回答

すべてのテクノロジーがすべての環境のニーズや要件に適合するわけではありません。とはいえ、「パッシブな侵入検知システム（IDS）」（58%）を有利用していると回答したICS/OT資産を保有または運用している組織が、「アクティブな侵入防御システム（IPS）」を導入した場合にもシステムが十分に機能するものと考えられます。「次世代ファイアウォール」も同様に幅広い有用性を持ち、自社や外部ネットワークに起因する脅威からより多くのICS環境を保護しています。「一方向セキュリティゲートウェイ／データダイオード」は主に最高レベルのセキュリティ環境（原子力発電所など）で使用されることから複雑で高コストであるとの評価でしたが、我々は最近ではこれらの2つの要因はどちらも縮小しているとみており、将来的には導入が進むことを予想しています。



制御システム資産をサイバー脅威から保護するために組織が利用しているセキュリティ技術

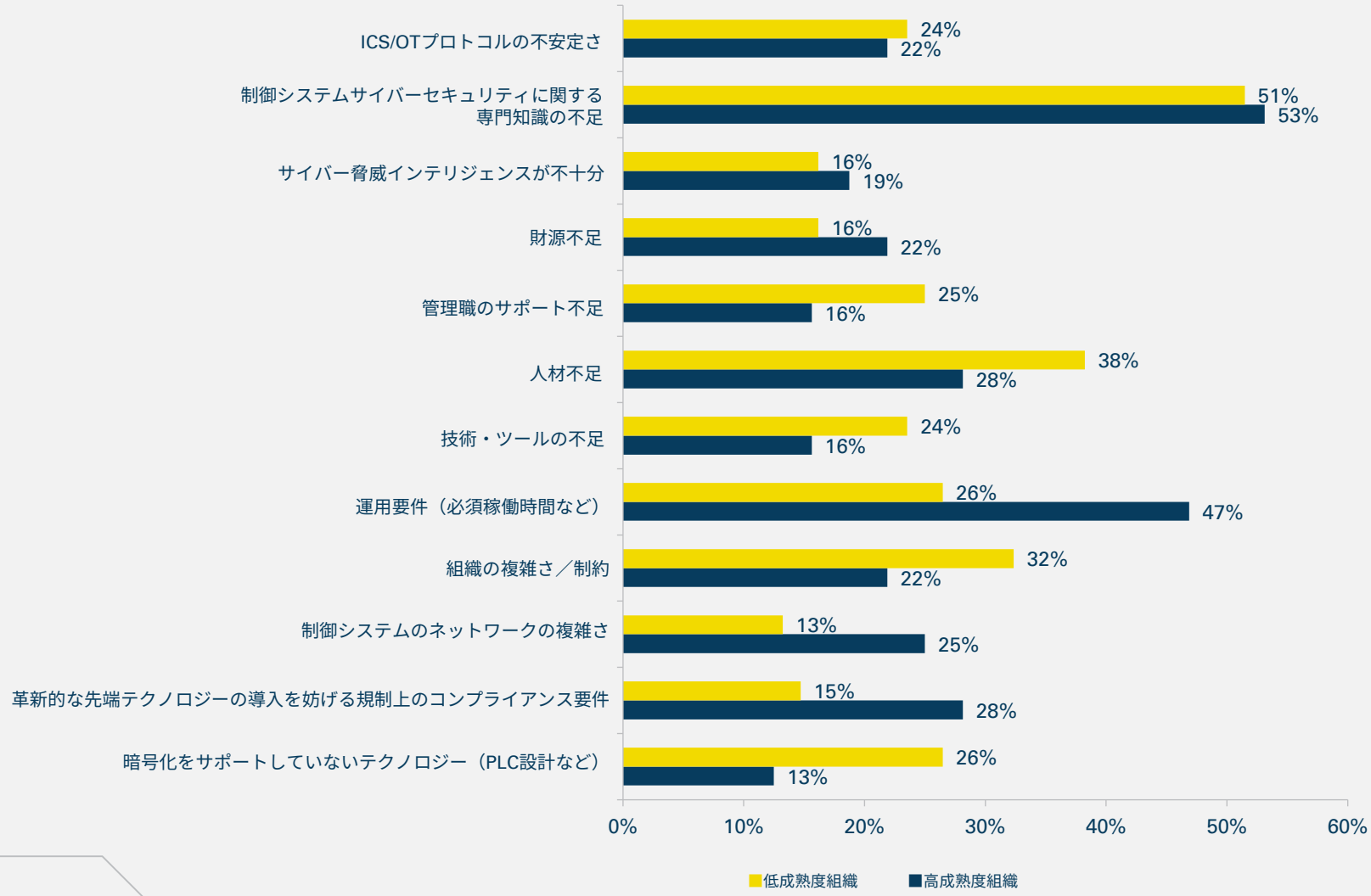


(CS)²への攻撃を防ぐうえでのハードル

(CS)²のハードル：高成熟度組織と低成熟度組織の比較

我々は年に一度、異なるグループ間の状況や回答の違いを比較しています。本章では、組織が何を最大のハードルと考えているかについて、高成熟度組織と低成熟度組織の制御システムサイバーセキュリティプログラムを比較しながら考察します。これにより、何がうまくいっていて何がうまくいっていないのか、また、組織がセキュリティ向上の取組みを進めるにつれてどのように物事が変化しているのかを確認します。右のグラフでは、「ICS/OTプロトコルの不安定さ」（低成熟度組織：24%、高成熟度組織：22%）、「制御システムサイバーセキュリティに関する専門知識の不足」（低成熟度組織：51%、高成熟度組織：53%）など、いくつかのハードルではどちらの組織も同程度の回答であることがわかります。一方で、「管理職のサポート不足」（低成熟度組織：25%、高成熟度組織：16%）、「暗号化をサポートしていないテクノロジー（PLC設計など）」（低成熟度組織：26%、高成熟度組織：13%）といった項目では組織ごとで回答に差があります。これは、より成熟度の高い組織は、成熟度の低い組織が取組み中であるハードルの一部をすでに克服していることを示しています。

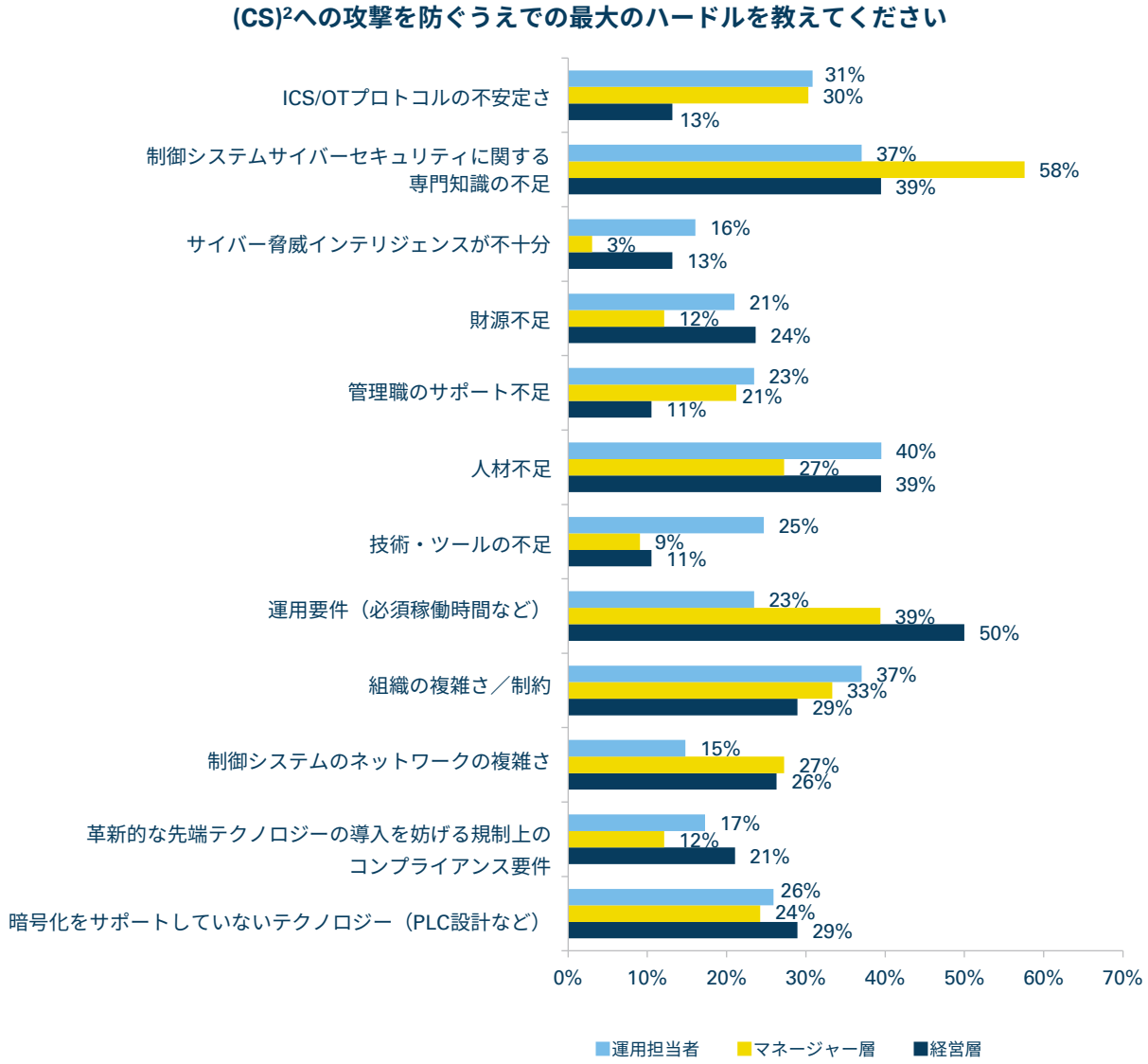
(CS)²への攻撃を防ぐうえでの最大のハードルを教えてください



(CS)²のハードル：役職クラス別[8]

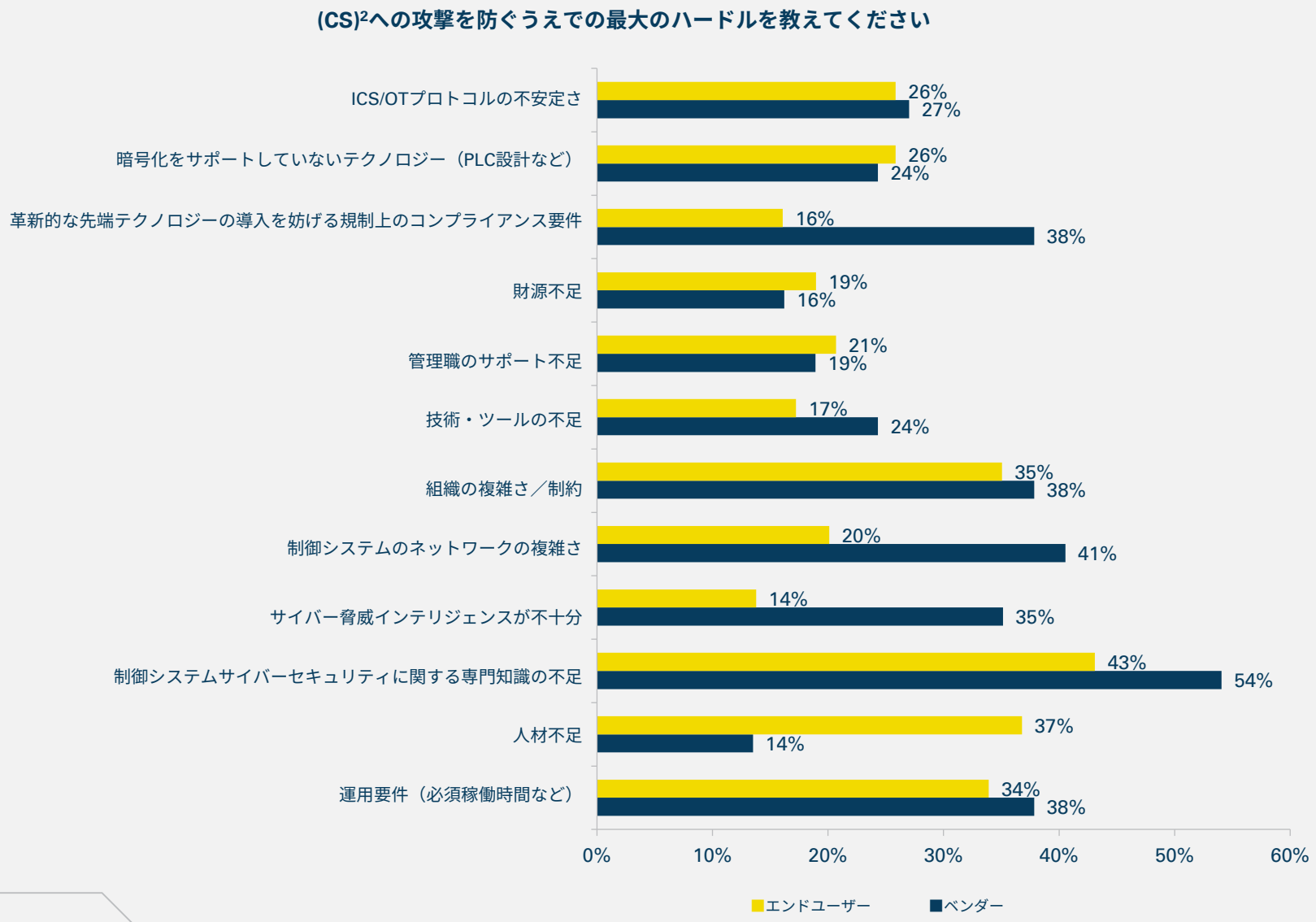
現代の制御システム環境について、その全体像と細部を一個人が完全に把握することは非常に難しいと思われます。各個人の見解に差があることにより、成すべきことの認識にも必然的に差が生じます。調査によると、経営層は「運用要件（必須稼働時間など）」（50%）、「人材不足」（39%）、「制御システムサイバーセキュリティに関する専門知識の不足」（39%）が最大のハードルであると考えています。これは、運用担当者の回答結果と一致している部分もありますが（運用担当者が最も高いハードルと考えているのは40%の「人材不足」と、37%の「制御システムサイバーセキュリティに関する専門知識の不足」）、運用担当者の間では「運用要件（必須稼働時間など）」（23%）は6番目に多い回答であり、それほど高いハードルではないと考えられています。マネージャー層は片方または両方のグループと大きく回答が異なっており、マネージャー層の課題解決を支援する際には、組織内エンドユーザーの役割の把握が重要であることが明らかになりました。

8 本調査の各質問における回答者数にはばらつきがあるため、特定の分類において、有効な統計分析のために必要な回答数が不十分な場合があります。異なる役職クラスの回答者より得られたデータを分析した際、リーダーシップレベルの回答者が非常に少なかったため、一部のグラフに含めることができませんでした。



(CS)²のハードル：エンドユーザーとベンダーの比較

エンドユーザーとベンダーの回答には、興味深い違いがみられました。この違いは、制御システムを所有し運用しているエンドユーザーと、OT資産を製造し監視しているベンダーの性質の違いから生まれるのでしょうか。あるいは、利用できるリソースの違い、財務的な責任の違いなどの複合的な要因によるものでしょうか。注目すべきは、ベンダーでは「革新的な先端テクノロジーの導入を妨げる規制上のコンプライアンス要件」、「制御システムのネットワークの複雑さ」、「サイバー脅威インテリジェンスが不十分」が最大のハードルであるとの回答が多く、これらの項目はエンドユーザーの2〜3倍になったことです。エンドユーザーの回答がベンダーよりも大幅に高くなった項目は「人材不足」のみでした（エンドユーザー：37%、ベンダー：14%）。ベンダーは、エンドユーザーである顧客が何を最大のハードルとして認識しているかに留意し、顧客がそれを乗り越えられるよう最大限の支援を行う必要があるでしょう。



(CS)²のハードル：
地域別[9] [10]

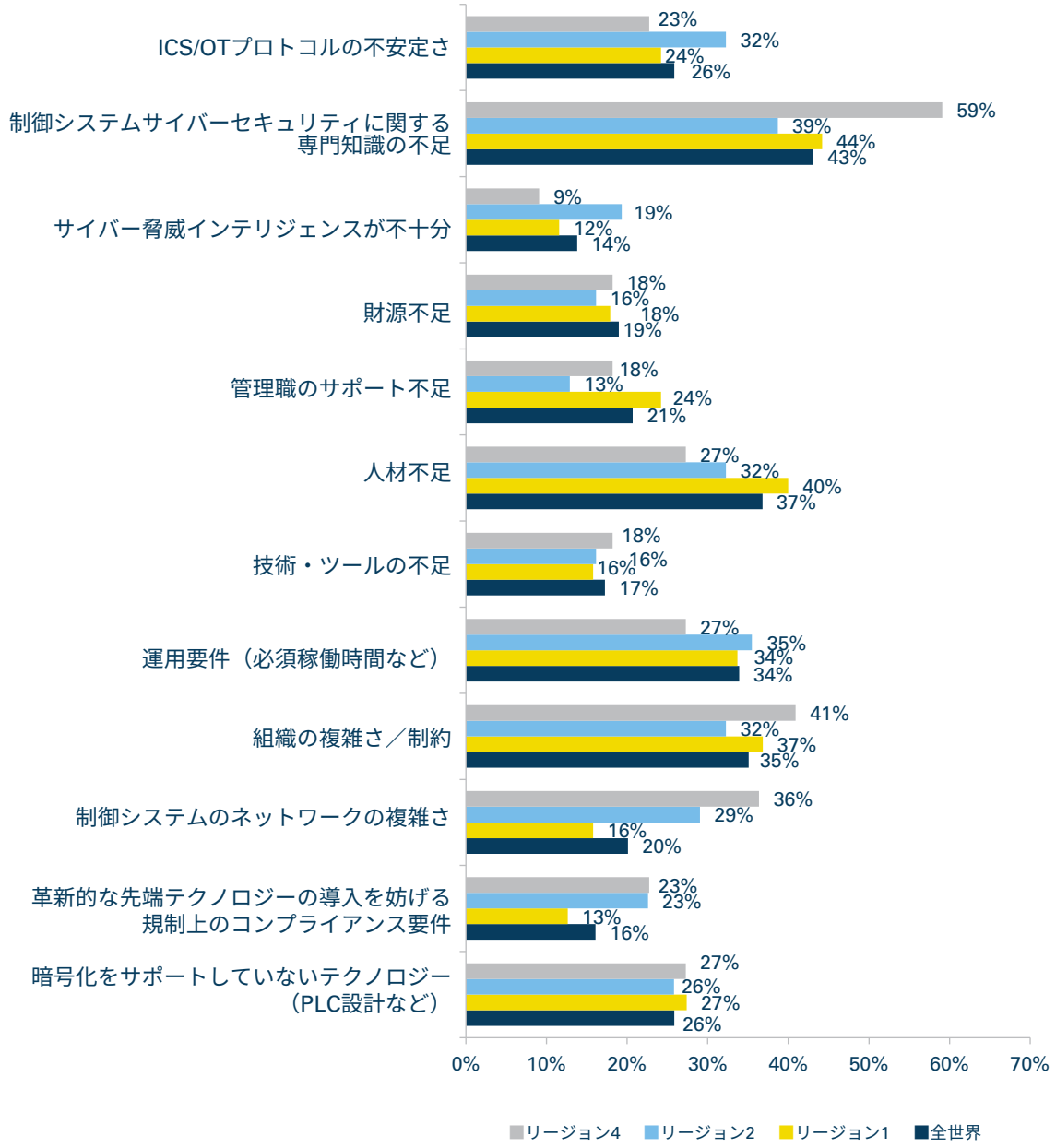
セキュリティのハードルに関する最後の考察として、世界の各地域別にどのような違いがみられるかについて分析しました。世界の制御システムは大部分が共通のテクノロジーに基づいて構築されています。そのため、この質問に対する回答には地理的場所に関係なくある程度の統一性がみられることが予想されており、実際にこのグラフでは、本報告書の他の多くのグラフと比べて違いが少ないことが示されています。注目すべき差が表れたのはリージョン4（インド太平洋）の「制御システムサイバーセキュリティに関する専門知識の不足」の回答割合（59%）で、リージョン2、リージョン1、全世界の回答割合と比べると、15ポイント以上高い結果となりました。また、リージョン2（欧州（中欧、西欧、北欧、南欧））およびリージョン4（インド太平洋）の回答者は、「制御システムのネットワークの複雑さ」について他の地域の回答者よりも懸念を抱いています（リージョン4：36%、リージョン2：29%、全世界：20%）。

9 役職クラス別の回答の分析と同様に、一部の地域では有効な分析を行うための十分な回答数を確保できませんでした。右のグラフでは、分析に十分な回答が得られた地域のみを表示しています。また、比較しやすいよう全世界（全回答者）の回答も併記しました。

10 (CS)2AIは回答者を7つの地域に分類しました。

1) 北米、2) 欧州（中欧、西欧、北欧、南欧）、3) ユーラシア大陸、4) インド太平洋、5) 中東・北アフリカ、6) 南アフリカ、7) ラテンアメリカ・カリブ海地域

(CS)²への攻撃を防ぐうえでの最大のハードルを教えてください




SERVER ROOM ASSISTANT
12-8976-3457-567
1 ACCESS CATEGORY
FG12558BKLSPPP166161

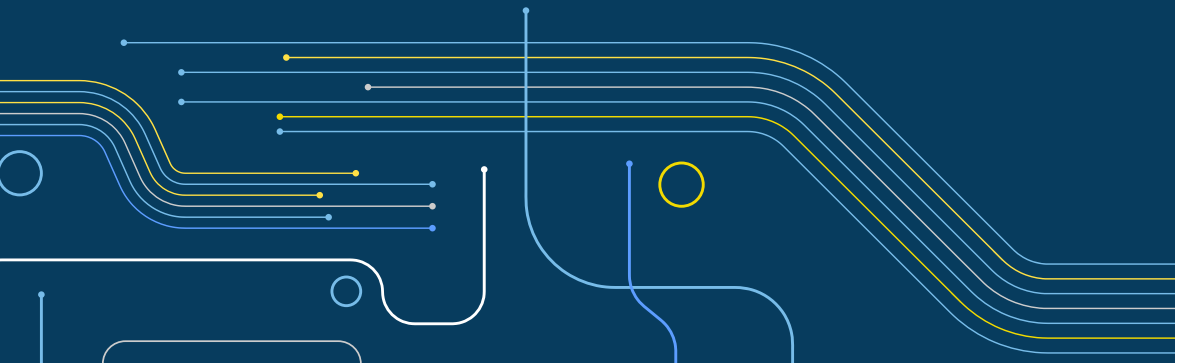
(CS)²の支出と予算

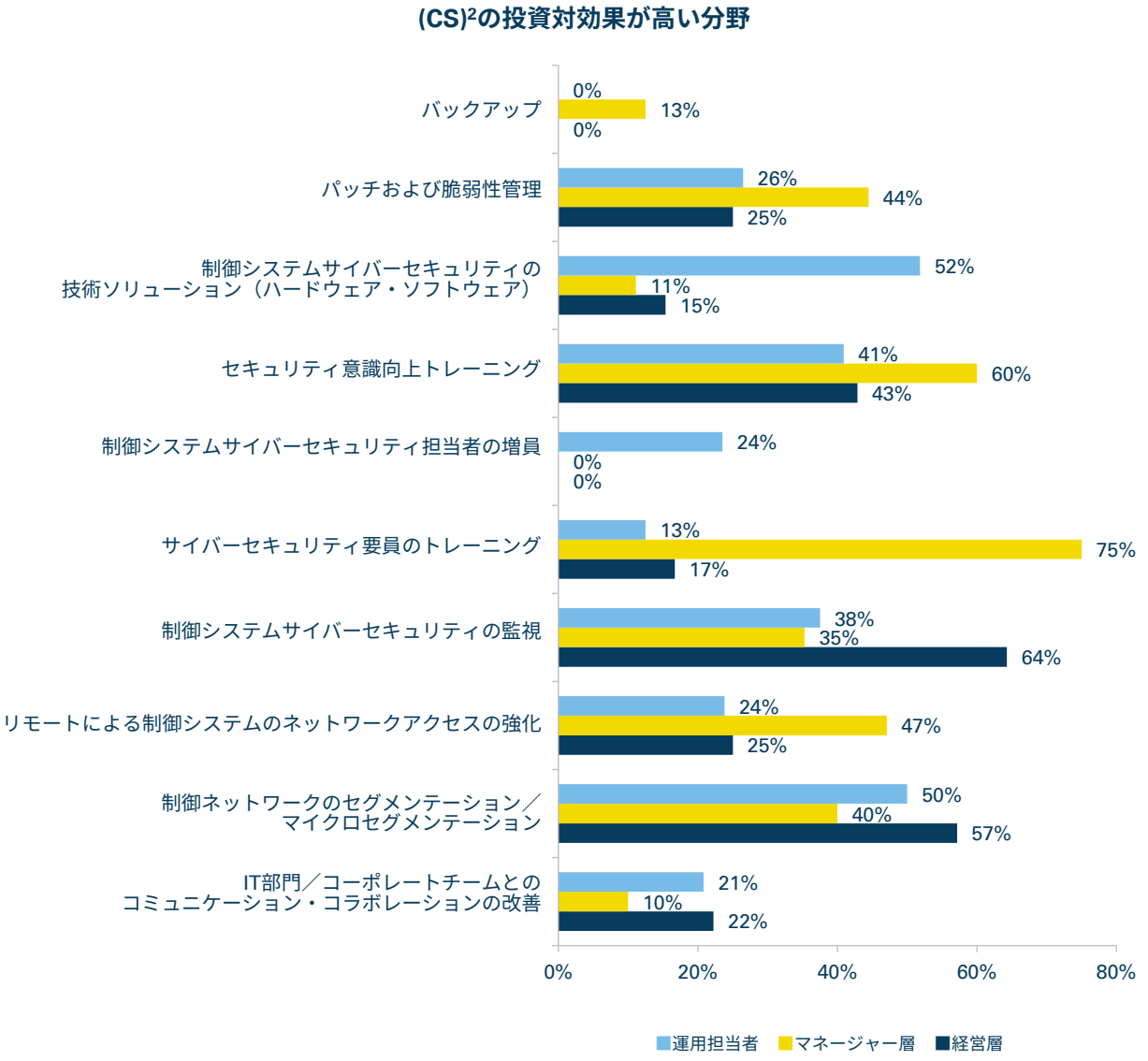
(CS)²の投資対効果が高い分野：役職クラス別[11]

(CS)²AIのチームと多くの回答者は、セキュリティの必要性に対して経営層の支援をどのように獲得すればよいかという問題を熟知しています。特にセグメンテーションでは、インパクト分析や、場合によっては重要なネットワークの再設計が必要になるため、調査に回答した経営層の多く（57%）がセグメンテーションの実施における投資対効果（ROI）を理解しているのは心強いことであり、セキュリティおよびレジリエンスの両面で重要です。「可視性はあらゆるセキュリティ改善プログラムにおける第一のステップである」との内容領域専門家（SME）による長年の議論を踏まえ、「制御システムサイバーセキュリティの監視」（64%）が経営層の回答で最も多い点を前向きに捉えています。一方、マネージャー層の回答者はトレーニングのROIが最も高いと考えており、「セキュリティ意識向上トレーニング」（60%）および「サイバーセキュリティ要員のトレーニング」（75%）がいずれも上位となりました。

経営層の39%、マネージャー層の27%が組織の(CS)²をめぐる状況を改善するためには「人材不足」が最大のハードルであると認識しているにもかかわらず（「(CS)²のハードル：役職クラス別」（18ページ）のグラフを参照）、「制御システムサイバーセキュリティ担当者の増員」におけるROIが高いと考える回答者がいない（両グループとも0%）という事実に注意を向けることが重要です。

11 十分な回答数を確保できなかったため、リーダーシッププレベルは本分析には含めていません。





(CS)²の投資対効果：
高成熟度組織と低成熟度組織の比較

克服すべきセキュリティのハードルに関する高成熟度組織と低成熟度組織の回答を比較すると、(CS)²への支出で最も投資対効果（ROI）が高いと考える分野において意見の一致が多くみられます。一方で、いくつかの項目で注目すべき明確な差が表れています。特に、「IT部門／コーポレートチームとのコミュニケーション・コラボレーションの改善」では、低成熟度組織の回答割合が高く（低成熟度組織：17%、高成熟度組織：0%）、反対に「バックアップ」では低い結果（低成熟度組織：0%、高成熟度組織：50%）となっています[12]。

このことが示す1つの可能性は、最も成熟度の高い組織はすでにチームを統合し、当然、堅固なバックアップシステムや手順を実装しているということです。両グループで「制御ネットワークのセグメンテーション／マイクロセグメンテーション」のROIが最も高いと考えていることがわかりました。意見の一致がみられたことは、数年間に及ぶ調査と、セキュリティ全体の改善およびサイバーインシデントによる影響減少のためにこれを導入すべきとの提言に沿っています。

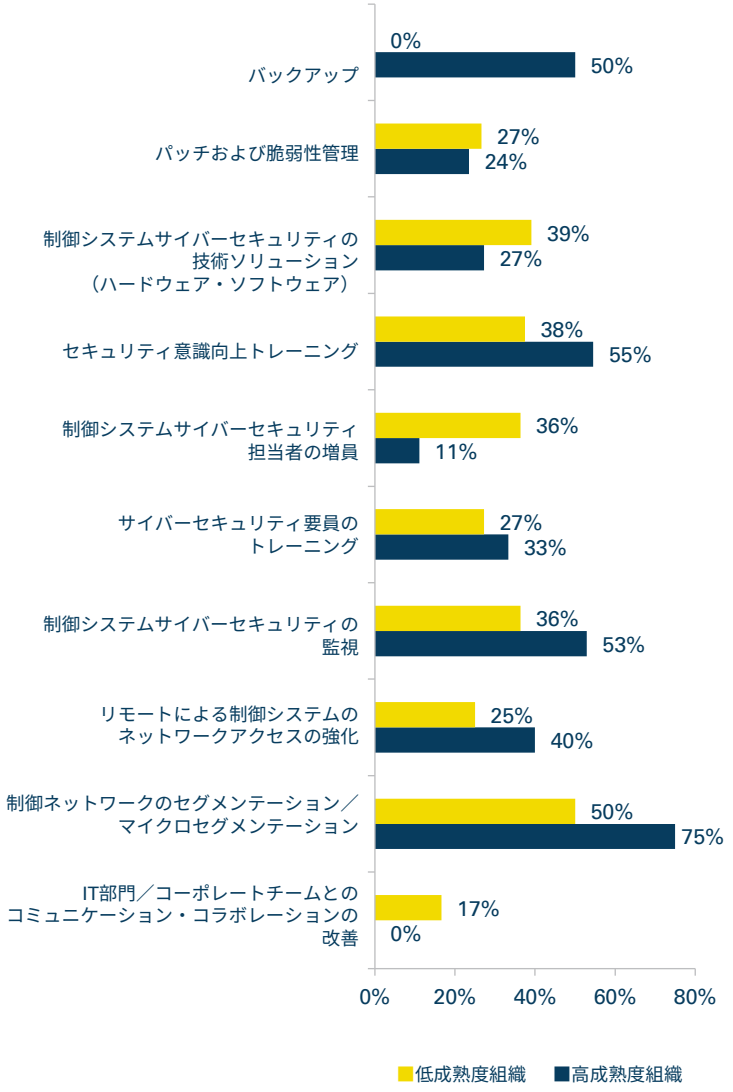
12 これは、最近ランサムウェア攻撃が増加しているなかで、高成熟度組織はその被害経験から、この結果になったと推察されます。

低成熟度組織の50%は、「制御ネットワークのセグメンテーション」がサイバーセキュリティプログラムのROIが最も高い分野であると考えています。ネットワークエンジニアリングに関する最新の考え方では、ネットワーク境界において、いくつかのエンジニアリングレベルにネットワークセグメンテーションのアプローチを展開することが最も効果的であるとされています。ネットワーク境界には、ITとOTのインターフェース、OTとインターネットのインターフェース、およびセキュリティ侵害による最悪の結果が大きく異なるネットワーク間のその他の接続を含みます。攻撃ツリー分析の結果は、こうした境界におけるエンジニアリングレベルに応じたセグメンテーションによって、重要なネットワークの攻撃対象領域の数が最大3桁減少することを示しています。

Andrew Ginter氏

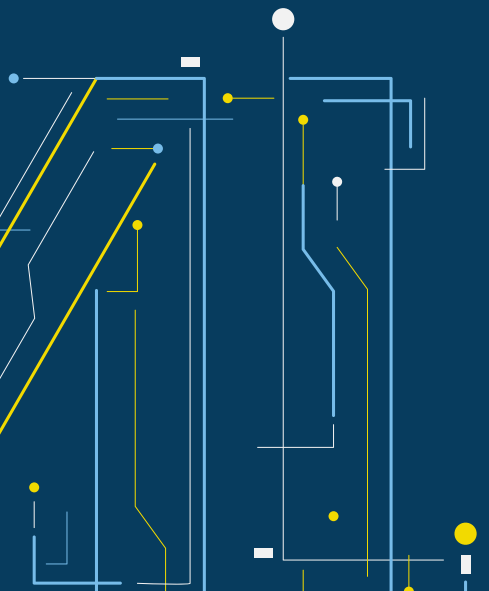
VP Industrial Security
Waterfall Security Solutions社

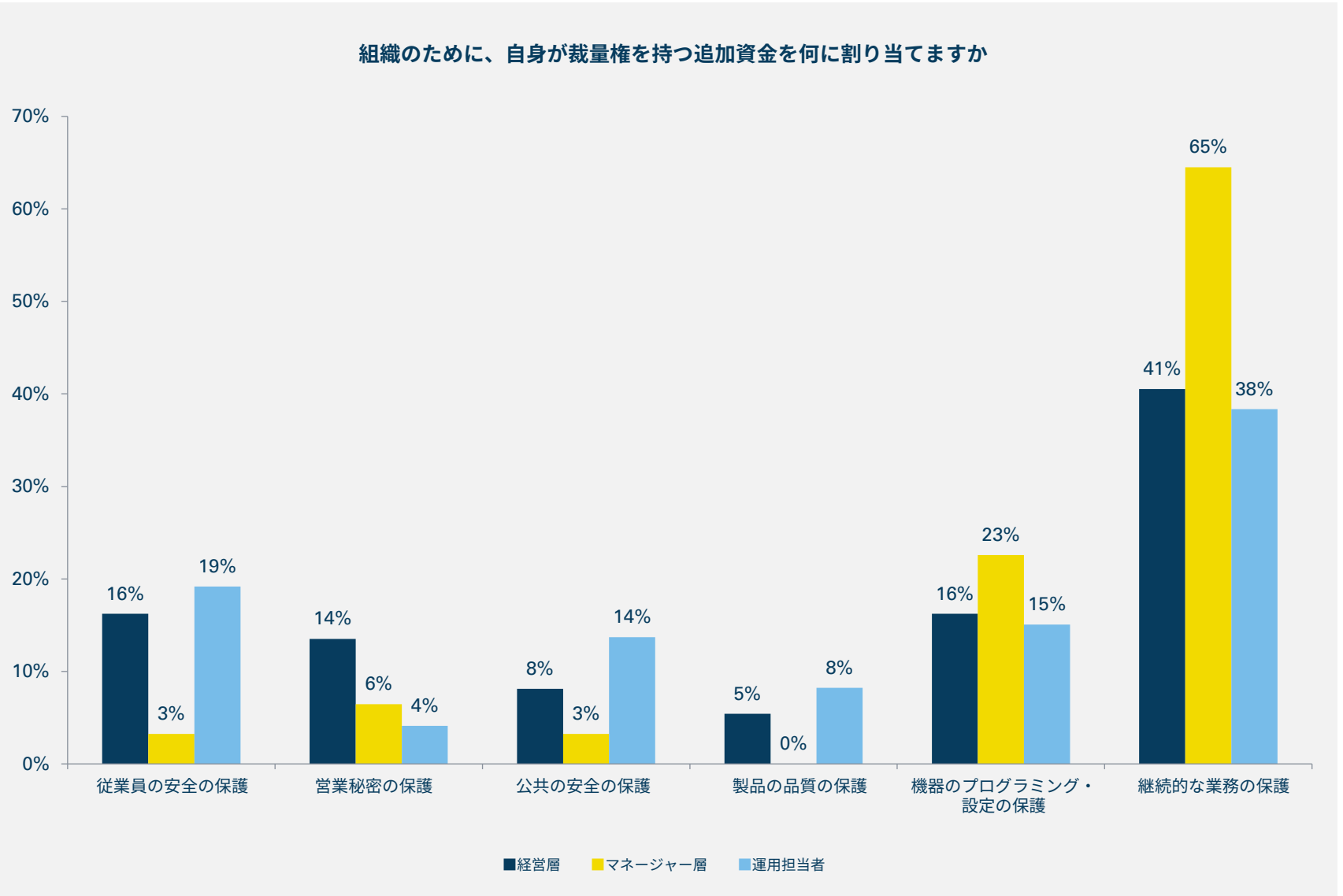
(CS)²の投資対効果が高い分野：
高成熟度組織と低成熟度組織の比較



支出の優先順位：役職クラス別

今回の調査で新たに行った質問では、興味深い回答が得られました。すべての回答者グループで「継続的な業務の保護」に追加資金を割り当てるとの回答が多くみられたが、その他の項目では回答者の職位ごとに明確な差が表れています。留意すべきは、マネージャー層は「従業員の安全の保護」と「公共の安全の保護」を重要と考える人が非常に少なく（どちらも3%）、「製品の品質の保護」を選んだ回答者はいない点です。こうした違いを踏まえ、組織には事業の優先順位の調整に関する議論を進めることが推奨されます。

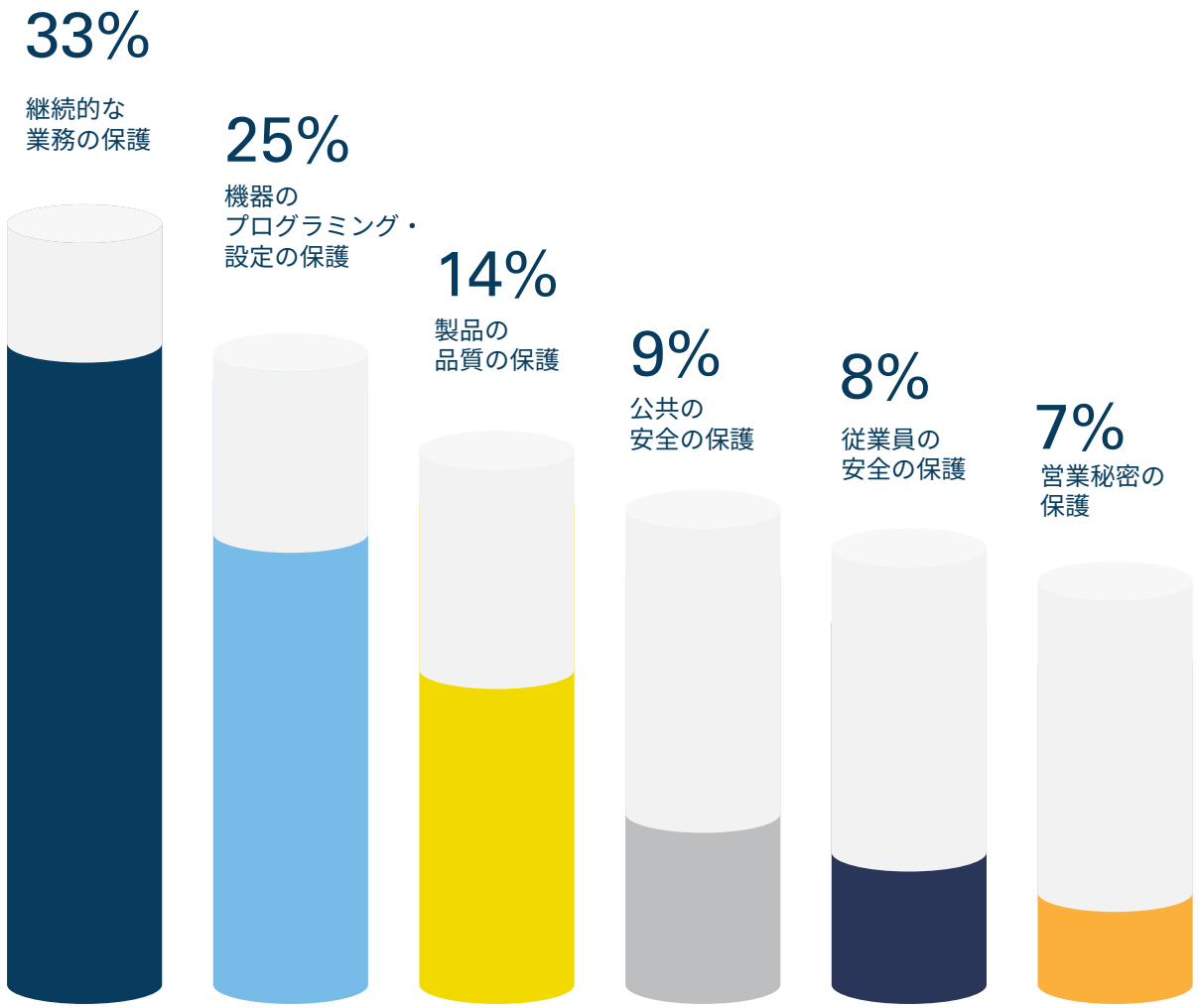




予算に関する顧客企業へのアドバイス：ベンダーの回答

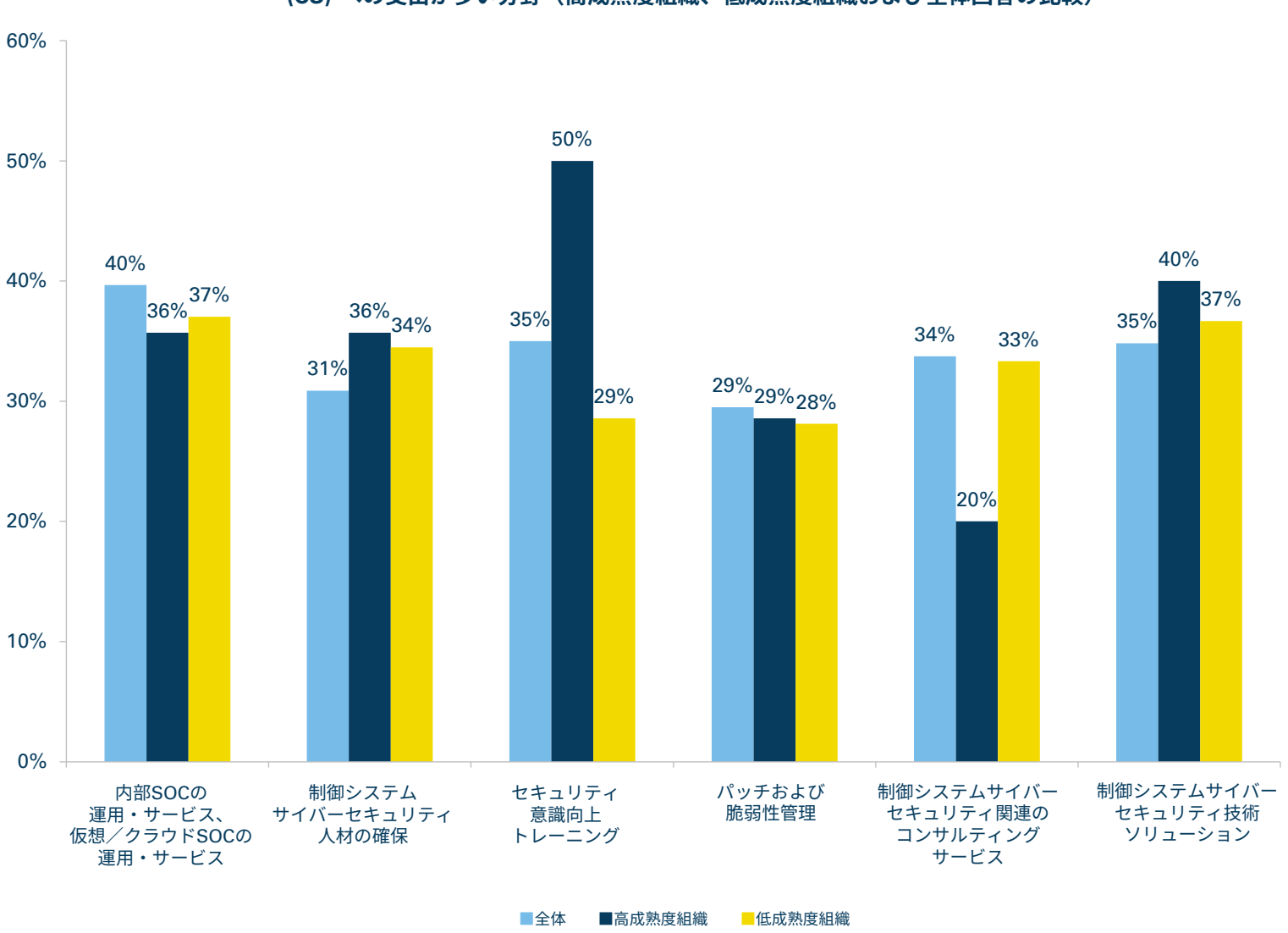
多くのアセットオーナーや運用担当者は、信頼するベンダーの内容領域専門家（SME）のアドバイスに頼っています。そこで、今回はリソースの配分に関するベンダーのアドバイスについて調査しました。この調査結果と前のページのグラフを比較すると、やはり「継続的な業務の保護」が最も重要視されていることがわかります。

顧客企業に対して、次年度は何により多くのリソースを投資するようにアドバイスしますか



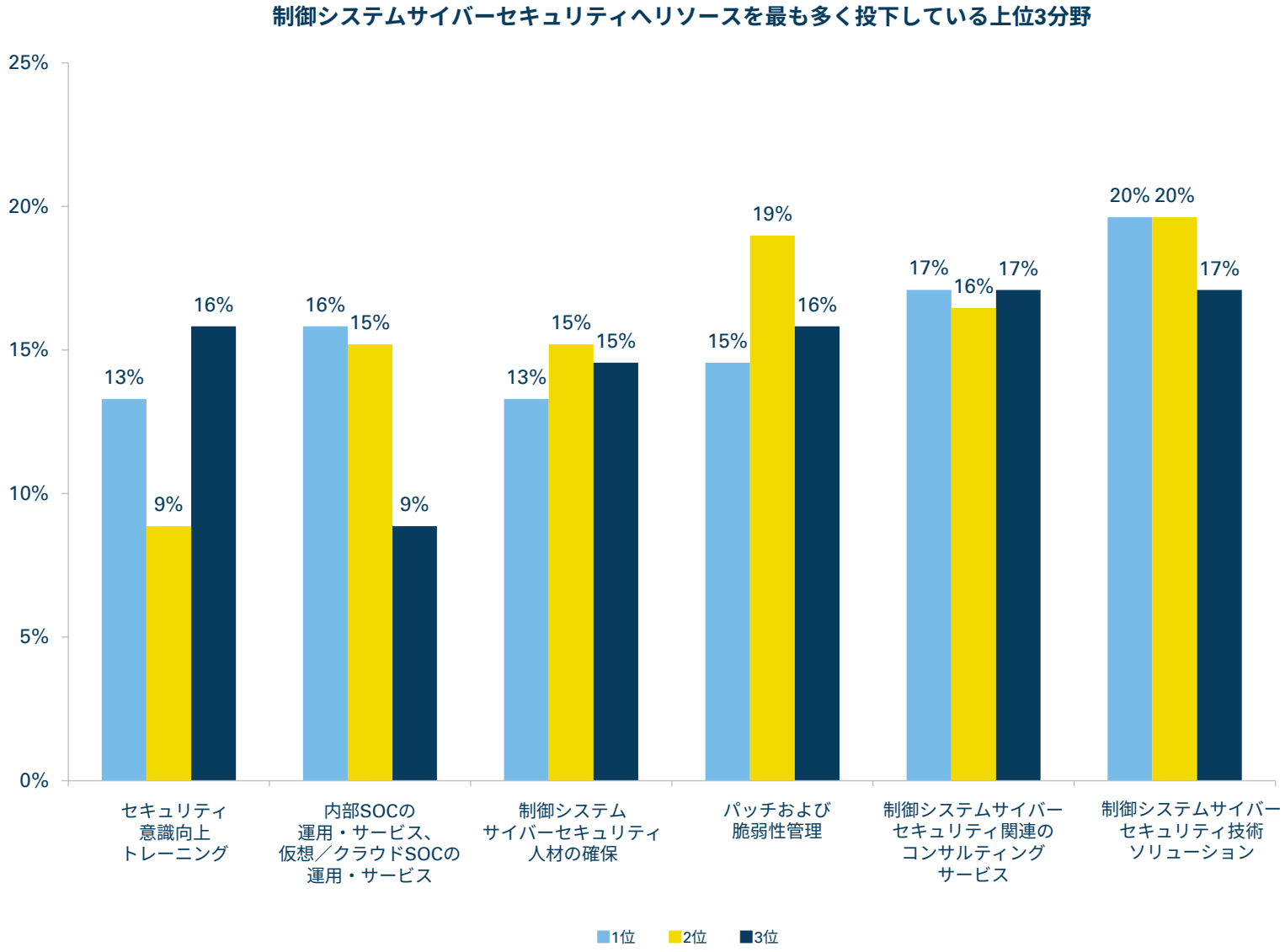
(CS)²への支出が多い分野：高成熟度組織、低成熟度組織および全体回答の比較

比較しやすいよう、このグラフでは全回答者の結果を掲載しました。このグラフから、高成熟度組織は「セキュリティ意識向上トレーニング」に非常に多く投資しており（高成熟度組織：50%、低成熟度組織：29%、全体：35%）、一方で、「制御システムサイバーセキュリティ関連のコンサルティングサービス」を重視している高成熟度組織の回答者は比較的少数（高成熟度組織：20%、低成熟度組織：33%、全体：34%）であることがわかります。



(CS)²への支出が多い分野：エンドユーザーの回答

高成熟度組織と低成熟度組織の支出が多い分野に加えて、(CS)²予算の優先順位をさらに詳しく調査するため、エンドユーザーにも組織がリソースを投じている上位3分野を選択してもらいました。その結果、「制御システムサイバーセキュリティ関連のコンサルティングサービス」（50%）、「制御システムサイバーセキュリティ技術ソリューション」（57%）が予算の最も大きな割合を占めています（それぞれ1〜3位の合計）。我々は、「制御システムサイバーセキュリティ人材の確保」への投資が比較的少ないことが、この分野で人材の需要が供給を上回っている現状の要因であるかどうか、調査する価値があると考えています。



(CS)²予算の変化：縦断的分析

過半数をわずかに上回る組織（53％）が(CS)²予算を継続的に増加させており、この回答割合は数年間にわたり50％前後で推移しています（2021年：46％、2020年：51％）。(CS)²予算の増加率が30％未満のグループは一定の割合で増加しており、2020年の20％から今回の調査では34％に上昇しました。増加率が30％以上と高いグループは、相応して2020年の31％から今回は19％に減少しました。本調査の分析チームのメンバーは、(CS)²のベンダーやソリューションプロバイダーのセクターにおける明らかな減速を指摘しています。これは競争激化や過度な市場の欲求に対応したものである可能性があります。

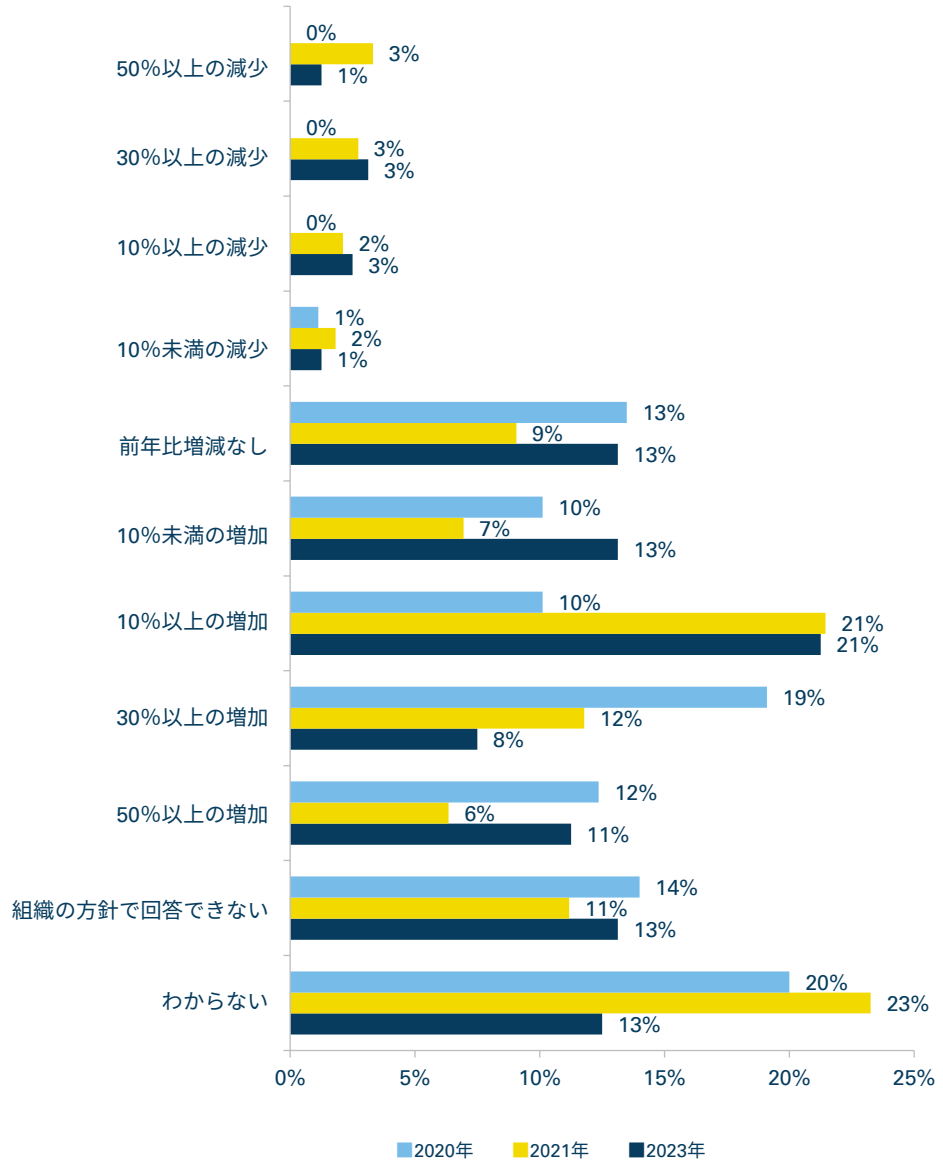
前年比投資を増加させるという継続的なコミットメントは、組織が事業における脅威の状況や、直面しているエクスポージャーの程度について理解を深めつつあることを示しています。近年の(CS)サイバーインシデントのニュースにより、存在するサイバーリスクと、同様のインシデントの発生を防ぐために必要な行動への意識が高まっています。

Brad Raiford

Director, National IoT & OT Cyber Services

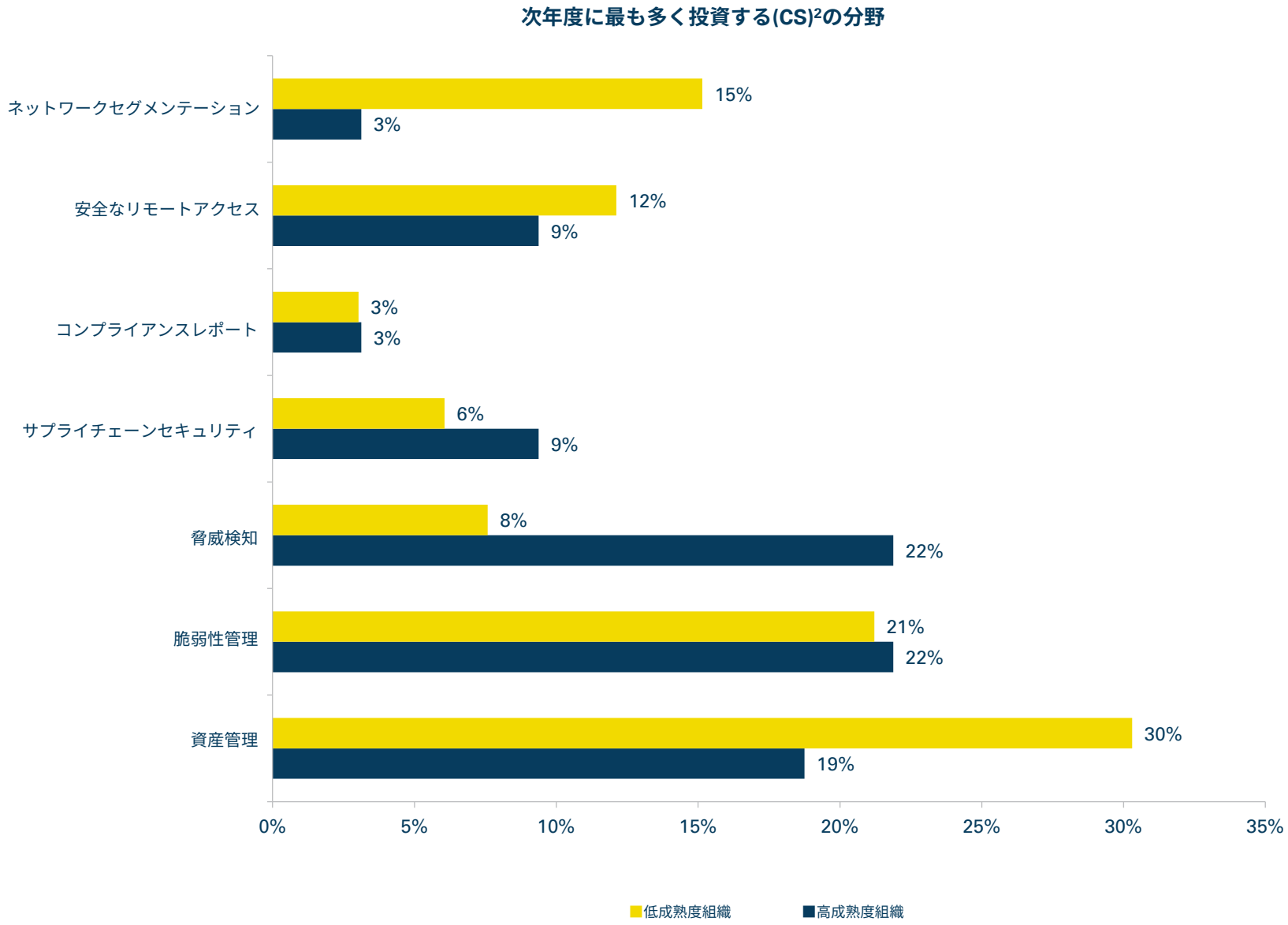
KPMG米国

2023年の制御システムサイバーセキュリティ予算は前年と比べてどのように変化すると思いますか



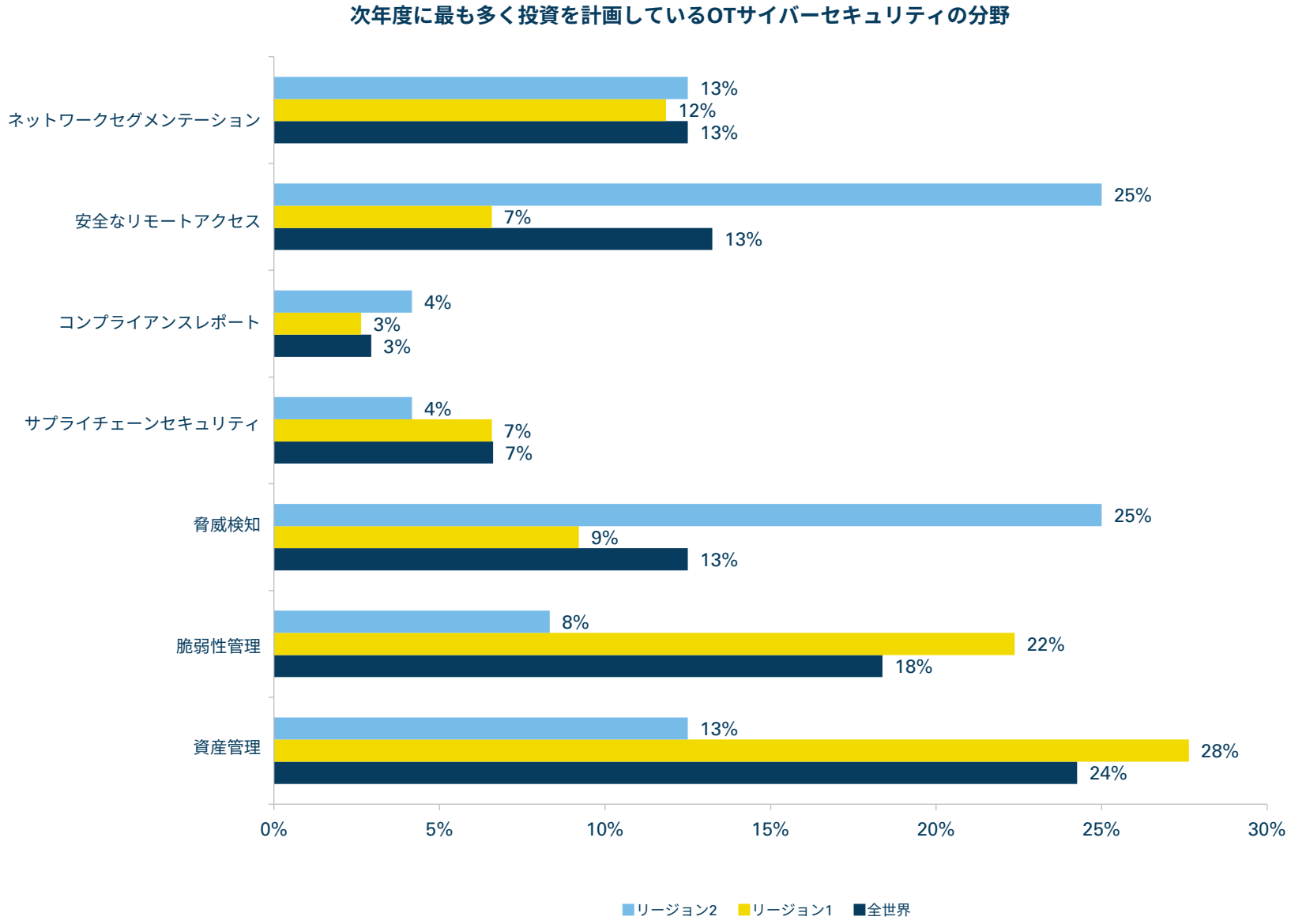
今後の(CS)²への投資計画：高成熟度組織と低成熟度組織の比較

「ネットワークセグメンテーション」の価値が非常に高いことを考えると（「(CS)²の投資対効果が高い分野」（23ページ）のグラフを参照）、次年度のセキュリティ投資でこの分野への投資を計画している組織が少ないことは注目に値します。これは、高成熟度組織はすでに十分なネットワークセグメンテーションを実施済みであるために、現在は低成熟度組織（15%）よりも少ない（3%）支出にとどまっていることを示している可能性があります。また、「脅威検知」および「資産管理」に関する投資計画の違いも、同様の要因と考えられます。



今後の(CS)²への投資計画：地域別

この質問について、リージョン3〜7[13]では分析のための十分な回答数を確保できませんでしたが、リージョン1とリージョン2では計画が大きく異なる結果となりました。リージョン2の回答者は「安全なリモートアクセス」と「脅威検知[14]」を重視しています（どちらも25%）が、リージョン1の回答者は「脆弱性管理」と「資産管理」をより緊急性の高い問題であると考えていることがわかります（脆弱性管理：22%、資産管理：28%）。1つの可能性として、リージョン2の組織は、これらの「管理」についての懸念事項をリージョン1の組織が到達していない水準まで、すでに解決しているものと考えられます。



13 (CS)2AIは回答者を7つの地域に分類しました。
1) 北米、2) 欧州（中欧、西欧、北欧、南欧）、3) ユーラシア大陸、4) インド太平洋、5) 中東・北アフリカ、6) 南アフリカ、7) ラテンアメリカ・カリブ海地域

14 リージョン2で「脅威検知」が重視されている要因の1つは、欧州の規制機関（国内外）が、複数の業界やインフラセクターで脅威検知を義務付ける法律を推進・発行していることです。

(CS)²予算：
高成熟度組織と低成熟度組織の比較

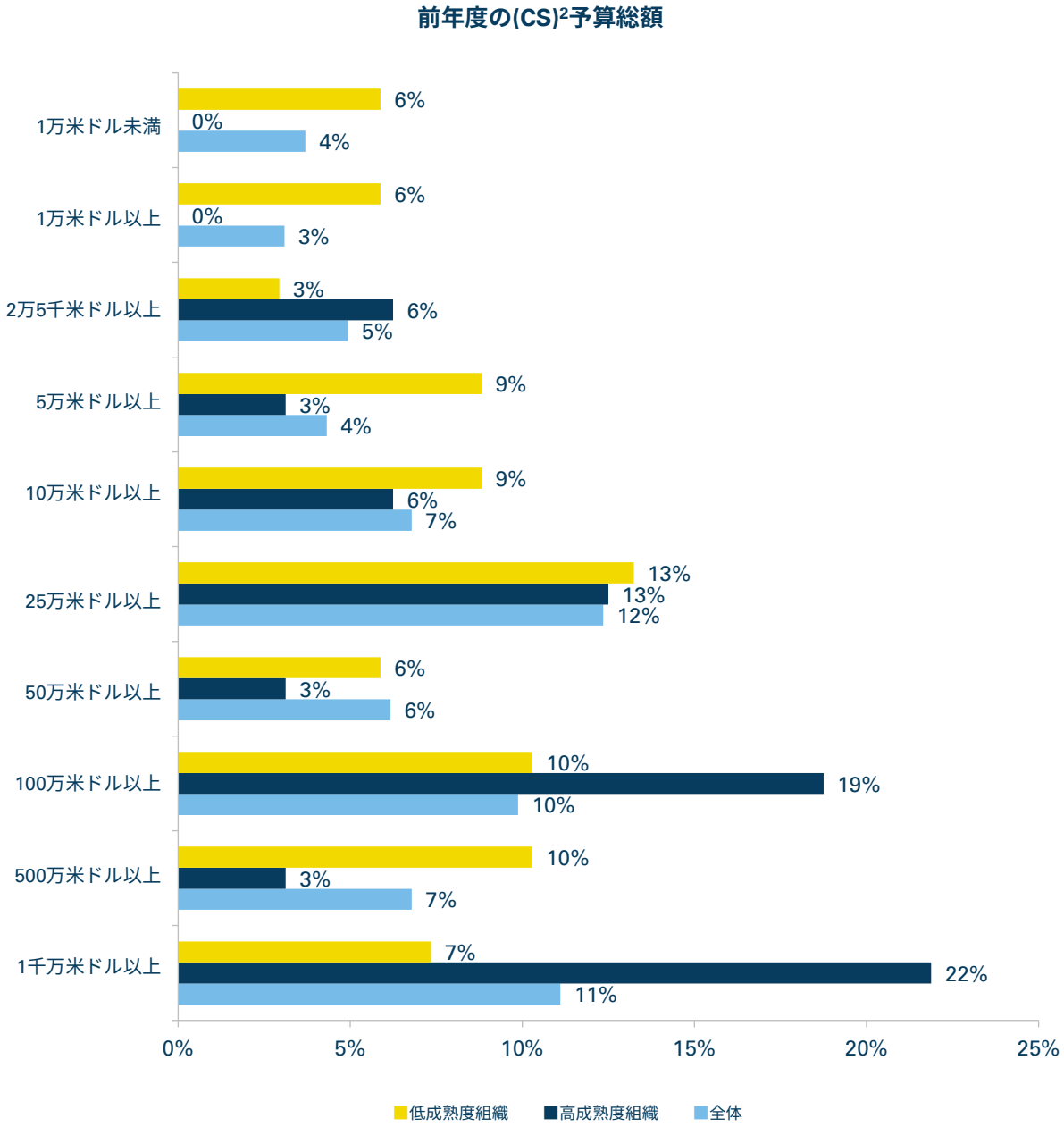
高成熟度組織は、制御システムサイバーセキュリティ予算を非常に多く確保していたことがわかっています。一説では、規模の大きい（より多くのリソースを保有している）組織は、規模の小さい組織よりもセキュリティへの取組みが進んでいると言われています。規模の小さい企業では、多くの場合、財務的な問題からセキュリティの改善に十分なリソースを配分することが難しい状況であると思われます。また、財務面に限界があるということは、サイバーインシデントの被害を乗り越え、回復する能力が低いことを意味する可能性があります。サイバー攻撃の脅威によって長期間にわたり業務の中断を余儀なくされることは、企業の存亡にかかわる問題となる恐れがあり、これを考慮してリスクマネジメントのプロセスを策定する必要があります。

この相関関係から、(CS)²業界には、規模の小さい顧客企業が予算を縮小できるようにするためのソリューションやサービスを提供する余地があることも浮き彫りになっています。

Rod Locke氏

Director of Product Management

Fortinet社

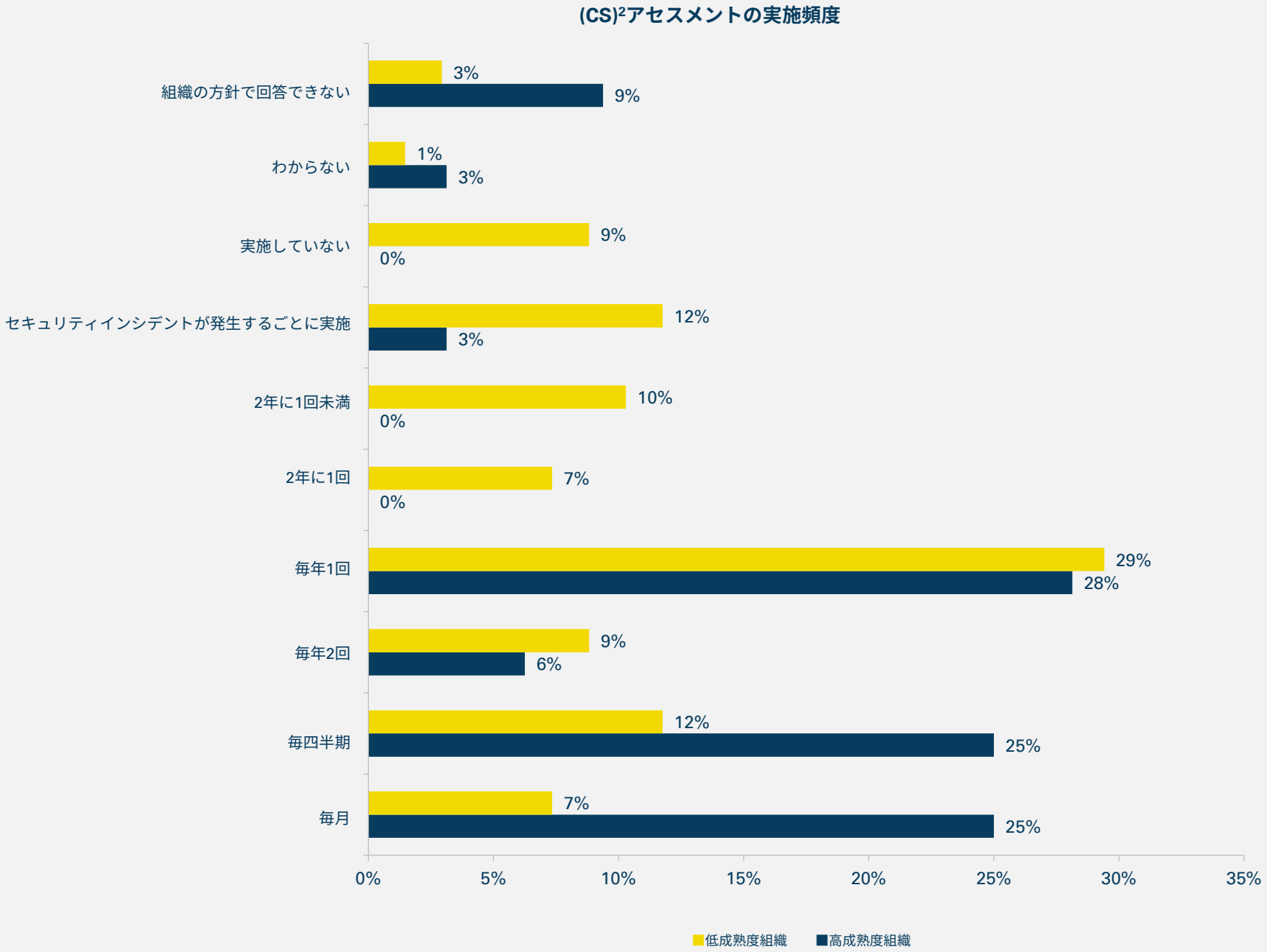



SERVER ROOM ASSISTANT
12-8976-3457-567
1 ACCESS CATEGORY
FG12558BKLSPPP166161

(CS)²アセスメント

(CS)²アセスメントの実施頻度：高成熟度組織と低成熟度組織の比較

高成熟度組織と低成熟度組織の差が明確に表れた調査結果の1つは、制御システムサイバーセキュリティアセスメントの実施頻度です。高成熟度組織の半数が少なくとも四半期に1回アセスメントを実施している一方、低成熟度組織の半数以上は毎年1回以下の実施にとどまっています。低成熟度組織の9%がセキュリティアセスメントを実施していないと回答していることからも、両組織の差は明らかです。

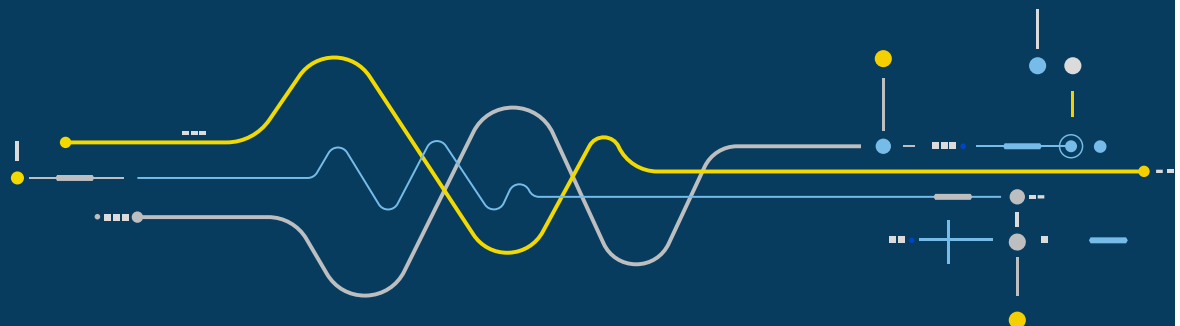


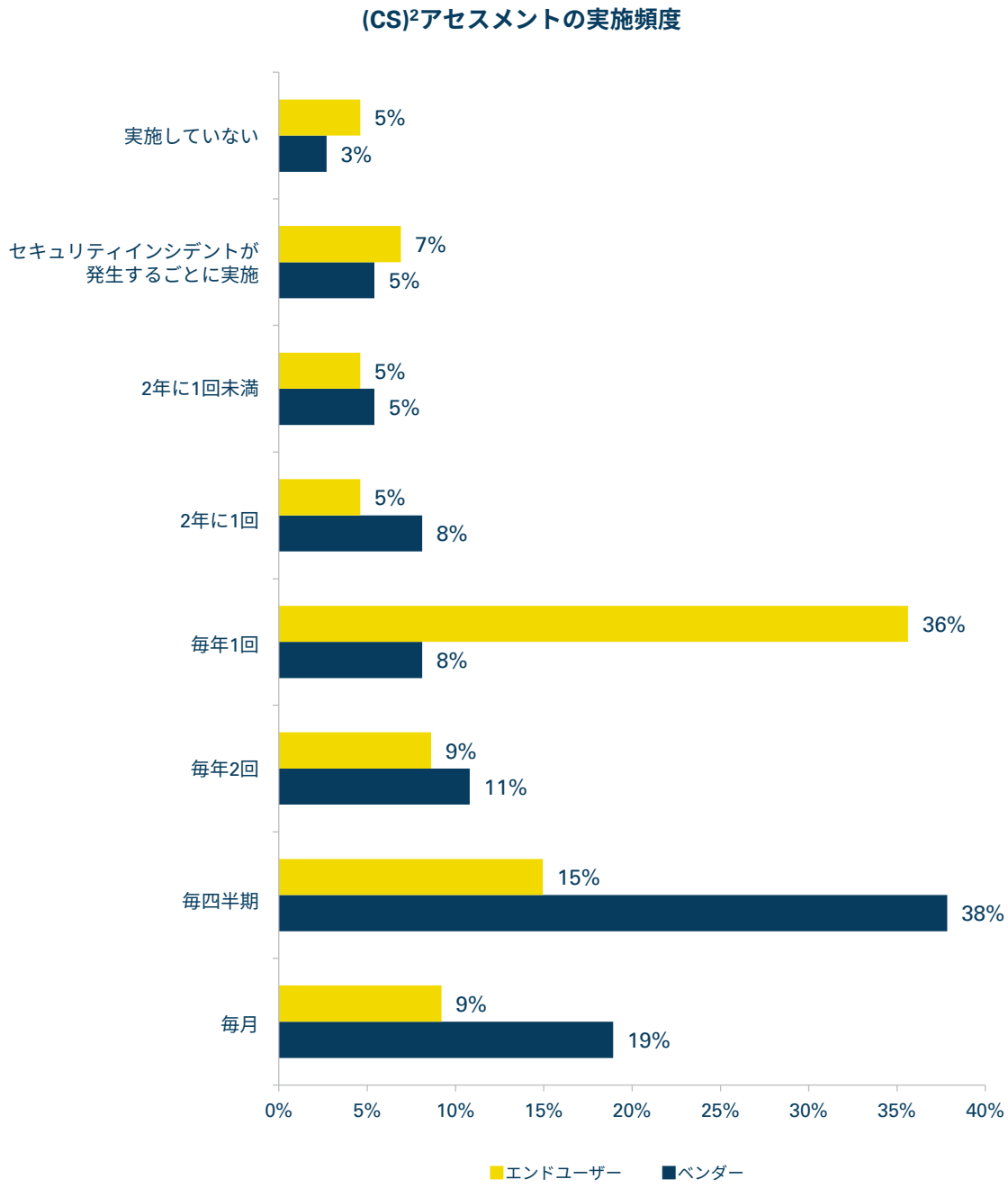
(CS)²アセスメントの実施頻度：エンドユーザーとベンダーの比較

多くの場合、ベンダーは顧客から継続的な監視・メンテナンス・更新のための特権的アクセス権を付与されます。そのためベンダーは、自社だけでなく顧客を保護する必要があり、エンドユーザーのセキュリティに対してさまざまな責任を負っています。ベンダーの3分の2以上（68%）が少なくとも毎年2回(CS)²アセスメントを実施しており、実施頻度が非常に高いことはよい傾向と言えるでしょう。ベンダーは、エンドユーザーのサプライチェーンを攻撃から守る盾として、非常に有益な役割を果たしています[15]。エンドユーザーによるアセスメントの実施頻度は、毎年1回の回答が最も多く（36%）、実施頻度が非常に低いことは、好ましいとは言えません。

テクノロジー、特権的アクセス権を持つ人員、攻撃手法や機能など、あらゆる要素が常に変化し続けているため、侵入防御・検知システム（IPS/IDS）を利用しても不正アクセスを発見できない場合があります。なかには、アセスメントの実施中に発覚することもあります。より頻繁にアセスメントを実施することで、不正な侵入者の滞留時間を大幅に短縮し、あらゆる損害を受ける可能性を減らすことができます。エンドユーザー、ベンダーを問わず、あらゆる組織では、少なくとも四半期に1回(CS)²ネットワークや資産のアセスメントを実施することが推奨されます。

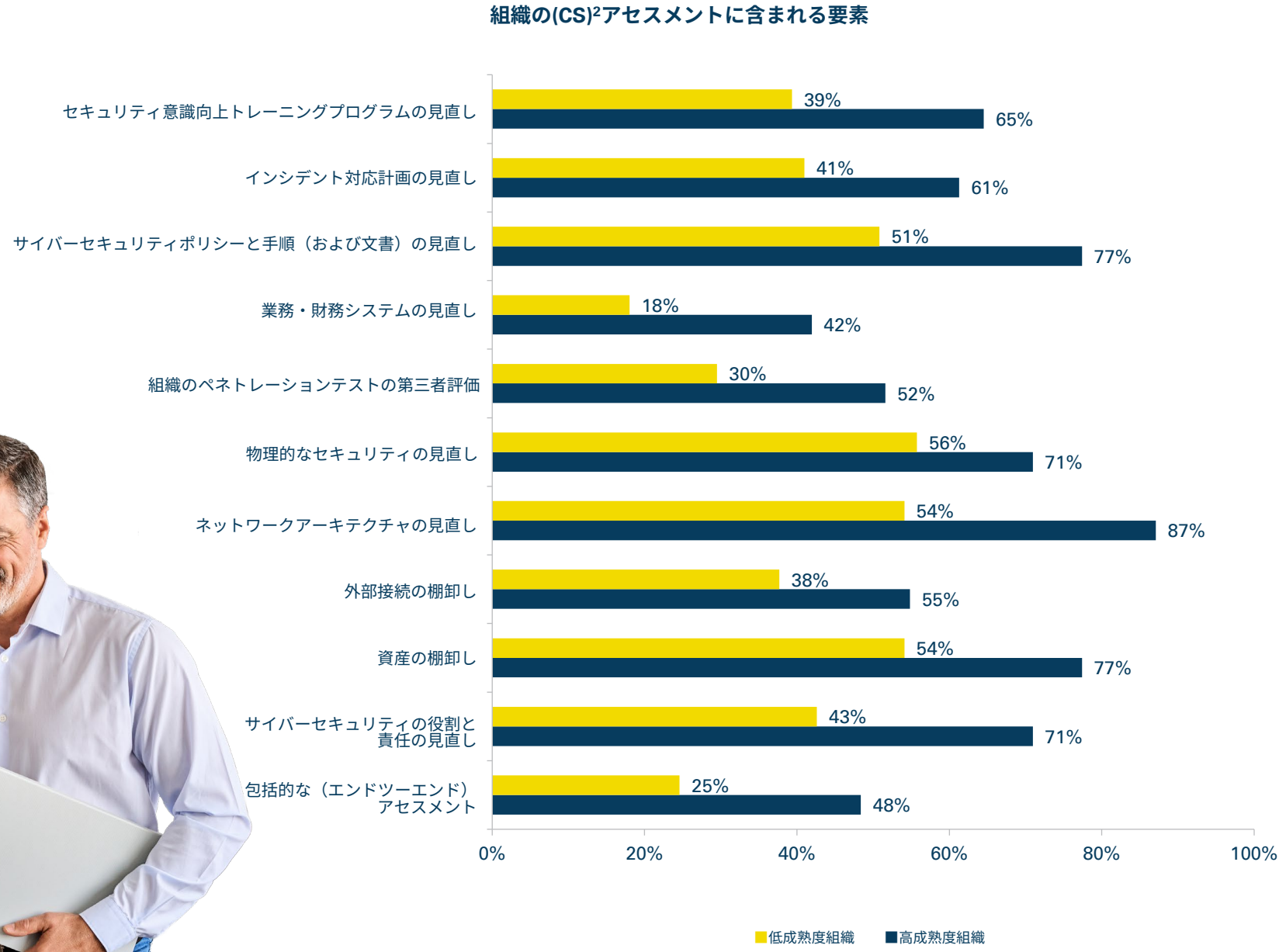
15 2020年のSolarWinds社製品を悪用したサプライチェーン攻撃に関する複数の記事を参照。





(CS)²アセスメントの包括性：高成熟度組織と低成熟度組織の比較

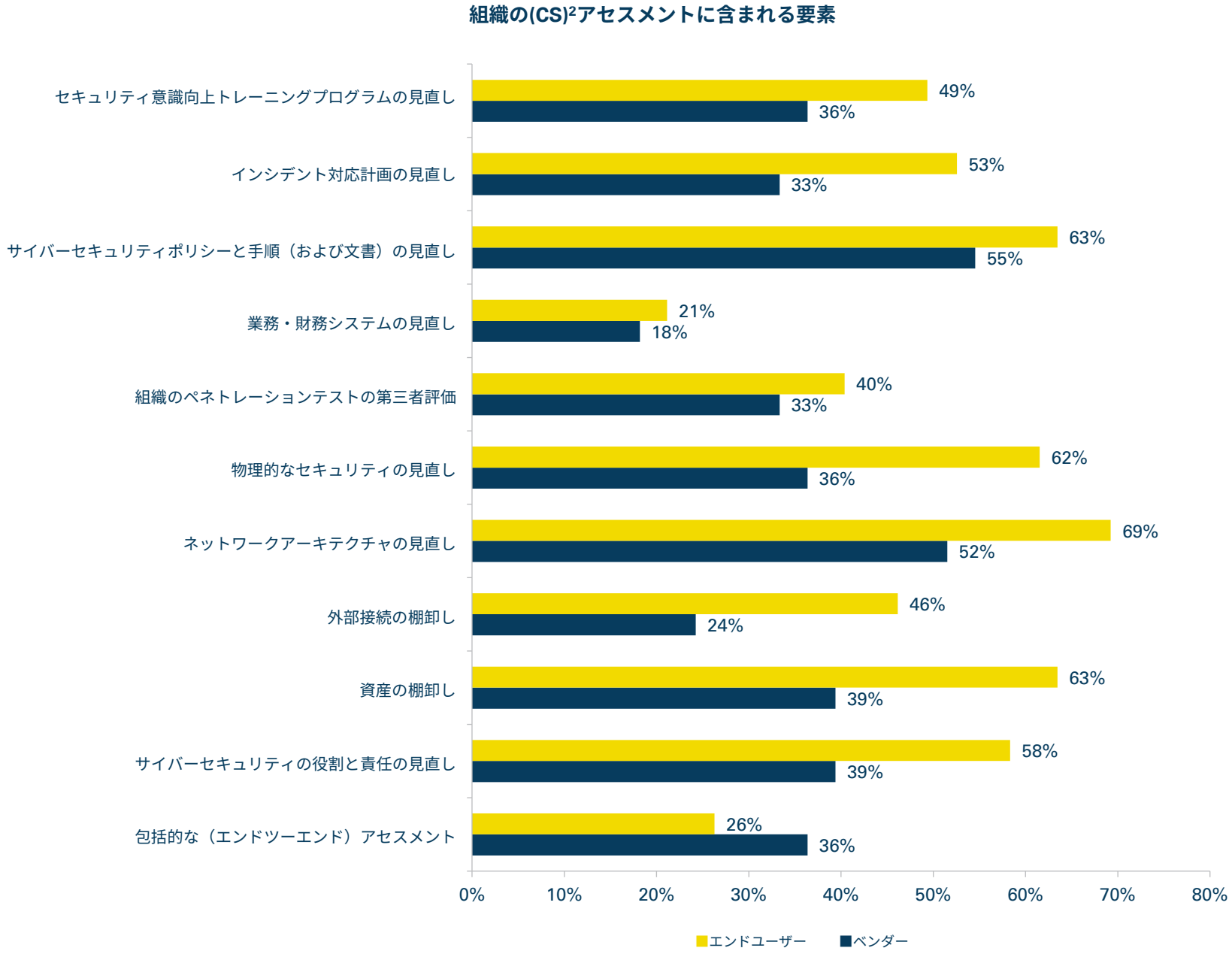
徹底したセキュリティアセスメントを実施しているかどうかは、実施頻度と同様に重要です。このグラフでは、高成熟度組織の回答がほぼすべての項目で50%以上となっており、低成熟度組織よりもアセスメント実施を徹底していることがわかります。



(CS)²アセスメントの包括性：エンドユーザーとベンダーの比較

「包括的な（エンドツーエンド）アセスメント」（エンドユーザー：26%、ベンダー：36%）を除くすべての項目において、エンドユーザーのセキュリティアセスメント実施率がベンダーを上回るという興味深い結果となりました。このことから、エンドユーザーのアセスメントには複数の重要な活動（物理的なセキュリティの見直し：62%、ネットワークアーキテクチャの見直し：69%、資産の棚卸し：63%）が含まれているものの、ベンダーやベンダーの顧客によるアセスメントと比較すると、エンドツーエンドではない場合が多いことが示されています。エンドユーザーの組織では、エンドツーエンドの可視化が必要な水準まで到達していない可能性があります。また、ベンダーは中間的な立場にあり、顧客に提供するサービスだけでなく、自社のサプライチェーンやアプリケーションのセキュリティについても考慮しなければならないことに留意する必要があります。

このグラフに記載された項目はすべて、進化するサイバー攻撃をキルチェーンに沿って防止（または検知）するための重要なポイントです。各要素をすべて盛り込んだ計画を策定し、それぞれにアセスメントと改善のサイクルを定めることを推奨します。



(CS)²アセスメント後の対応：高成熟度組織と低成熟度組織の比較

(CS)²アセスメントに関する3つの調査結果の最後は、アセスメント後の組織の対応について分析しました。ここでも、高成熟度組織はすべての項目で低成熟度組織よりもアセスメントの結果に徹底して対応していることがわかります。特に、「脆弱な制御システムのハードウェア、ソフトウェアまたはデバイス等の交換」（低成熟度組織：30%、高成熟度組織：61%）および「改善計画の策定と実行」（低成熟度組織：41%、高成熟度組織：68%）で明らかな違いがみられます。

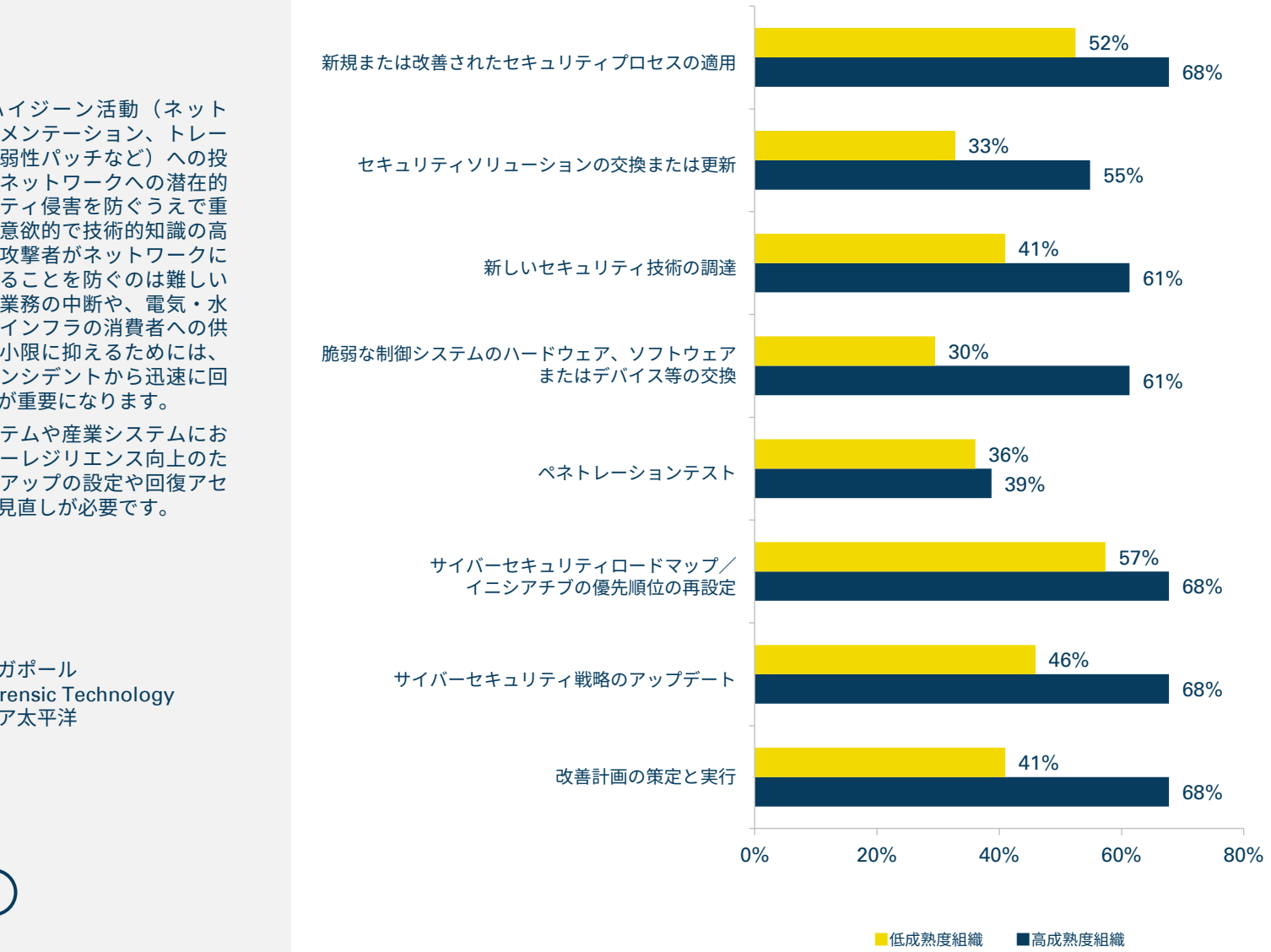
サイバーハイジーン活動（ネットワークセグメンテーション、トレーニング、脆弱性パッチなど）への投資は、産業ネットワークへの潜在的なセキュリティ侵害を防ぐうえで重要ですが、意欲的で技術的知識の高いサイバー攻撃者がネットワークにアクセスすることを防ぐのは難しいでしょう。業務の中断や、電気・水道といったインフラの消費者への供給停止を最小限に抑えるためには、サイバーインシデントから迅速に回復する能力が重要になります。

重要なシステムや産業システムにおけるサイバーレジリエンス向上のため、バックアップの設定や回復アセスメントの見直しが必要です。

Eddie Toh

Partner
KPMGシンガポール
Head of Forensic Technology
KPMGアジア太平洋

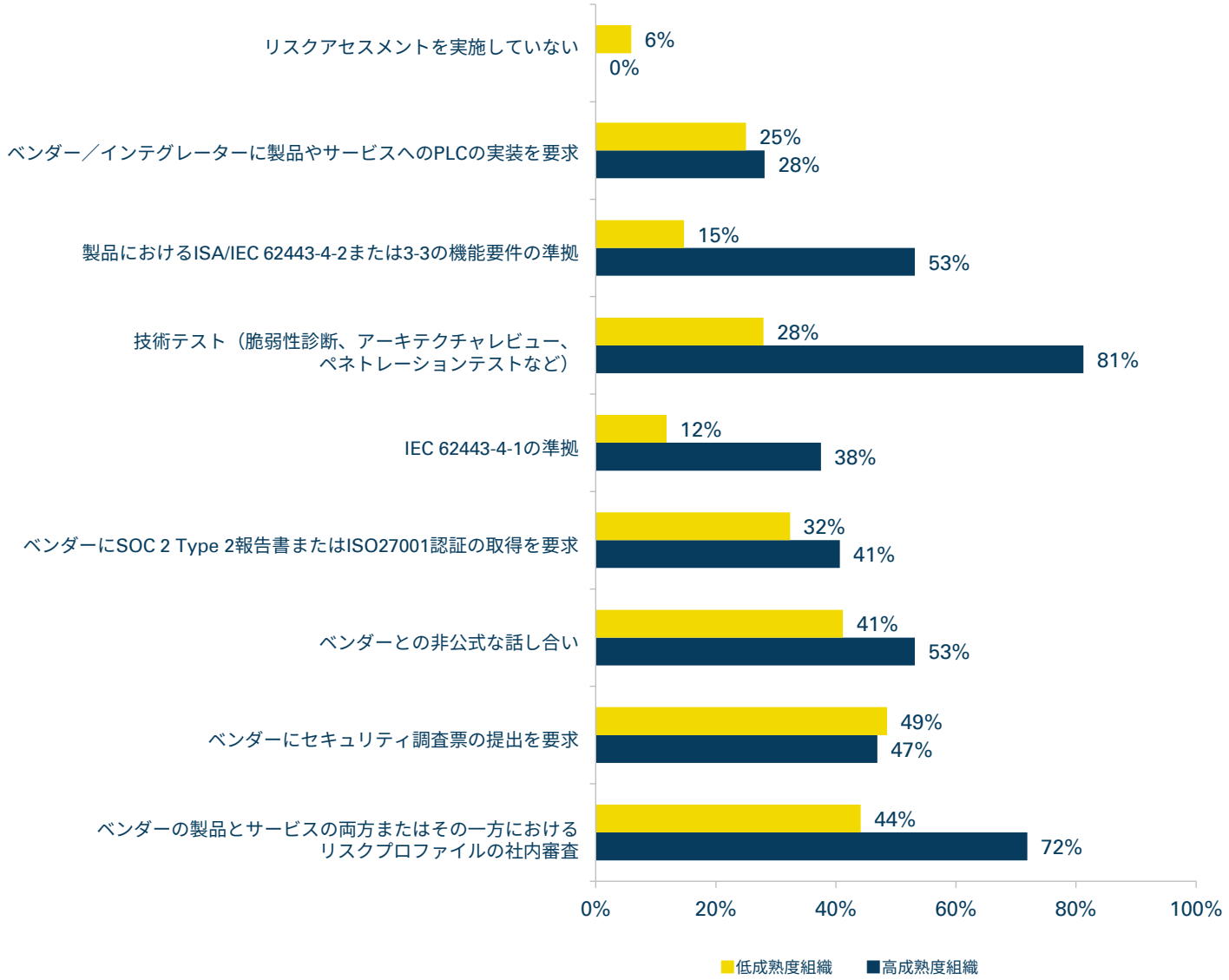
過去12ヵ月以内に実施された(CS)²アセスメントの結果に応じて、組織が取り組んだ（または計画している）活動



(CS)²導入前のリスクアセスメント：高成熟度組織と低成熟度組織の比較

新しいデバイスやソフトウェアのリスク評価は、定期的なセキュリティアセスメントとは区別して考える必要があります。高成熟度組織は、セキュリティアセスメントの実施頻度が全体的に高い結果となりましたが、導入前リスクアセスメントについてもほぼすべての項目で低成熟度組織より高い実施率であることがわかりました（「ベンダーにセキュリティ調査票の提出を要求」を除く）。規格の準拠について回答割合に差がみられた点については、米国の規制活動の高まりが回答に大きく影響していると思われます。一方、高成熟度組織による「技術テスト（脆弱性診断、アーキテクチャレビュー、ペネトレーションテストなど）」の実施率が高いことは（低成熟度組織：28%、高成熟度組織：81%）よい傾向です。技術テストはスナップショットのみを採取するため、定期的なセキュリティアセスメントを補完することができます。

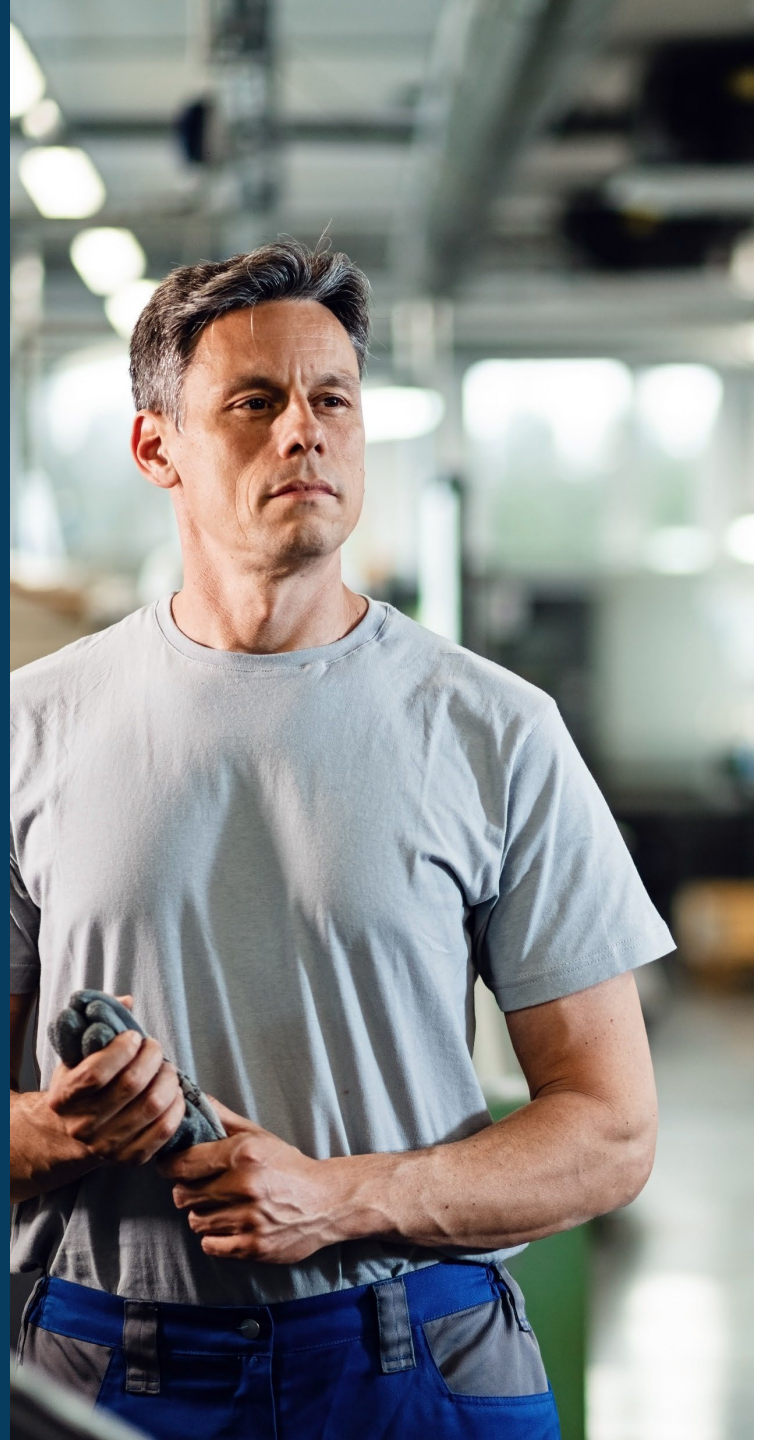
制御システム製品またはサービスを導入する前に、組織が実施しているリスクアセスメント



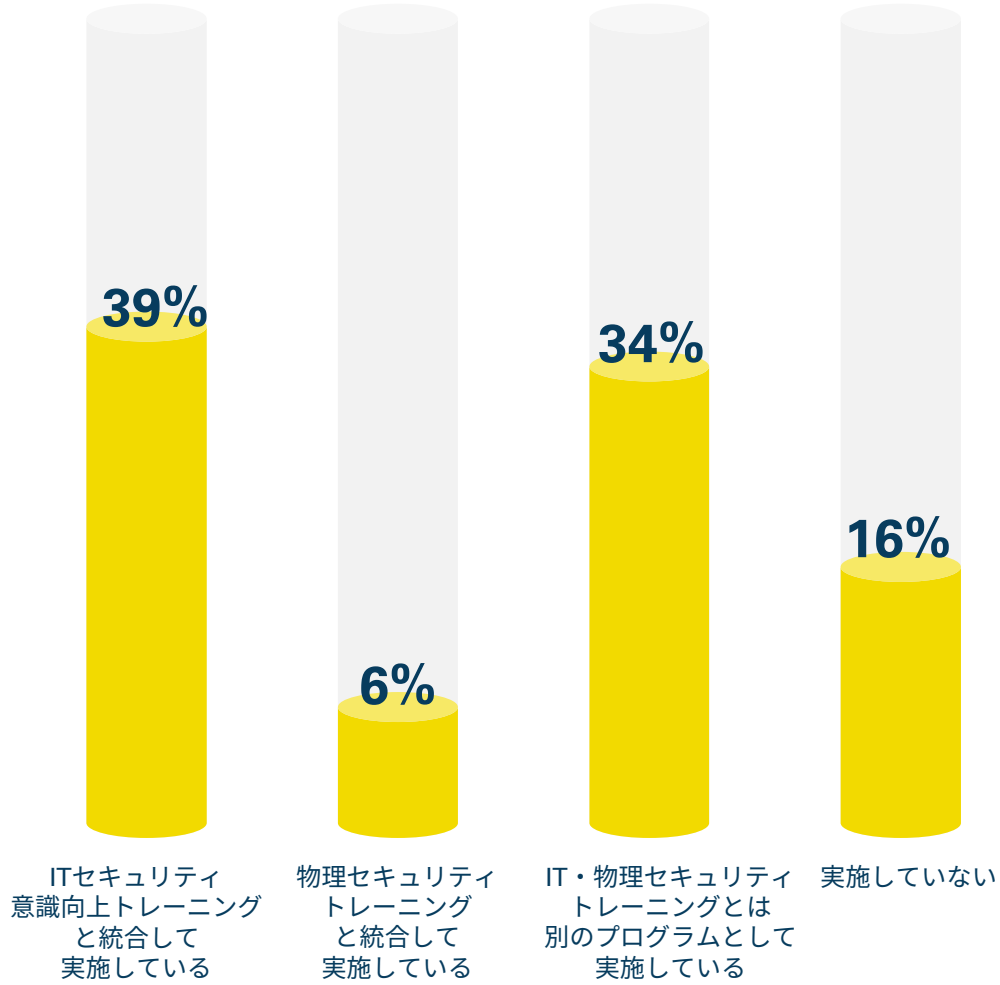
セキュリティトレーニング

(CS)²意識向上トレーニングの統合：エンドユーザーの回答

非常に多くのエンドユーザー組織でセキュリティ意識向上トレーニングへの取組みが不十分であることは深刻な問題です（実施していない：16%）。制御システムサイバーセキュリティの運用またはその他の設計においては、それを担うのがIT部門かリスクマネジメント部門かにかかわらず、あらゆるICS/OTの運用環境に内在するリスクを管理するため、サイバー脅威、攻撃手法、脆弱性、手順についての意識を全体として高く持ち、これを維持することが必要不可欠です。(CS)²資産または運用に責任を持つすべての組織には、セキュリティ意識向上トレーニングを導入することを強く推奨します。



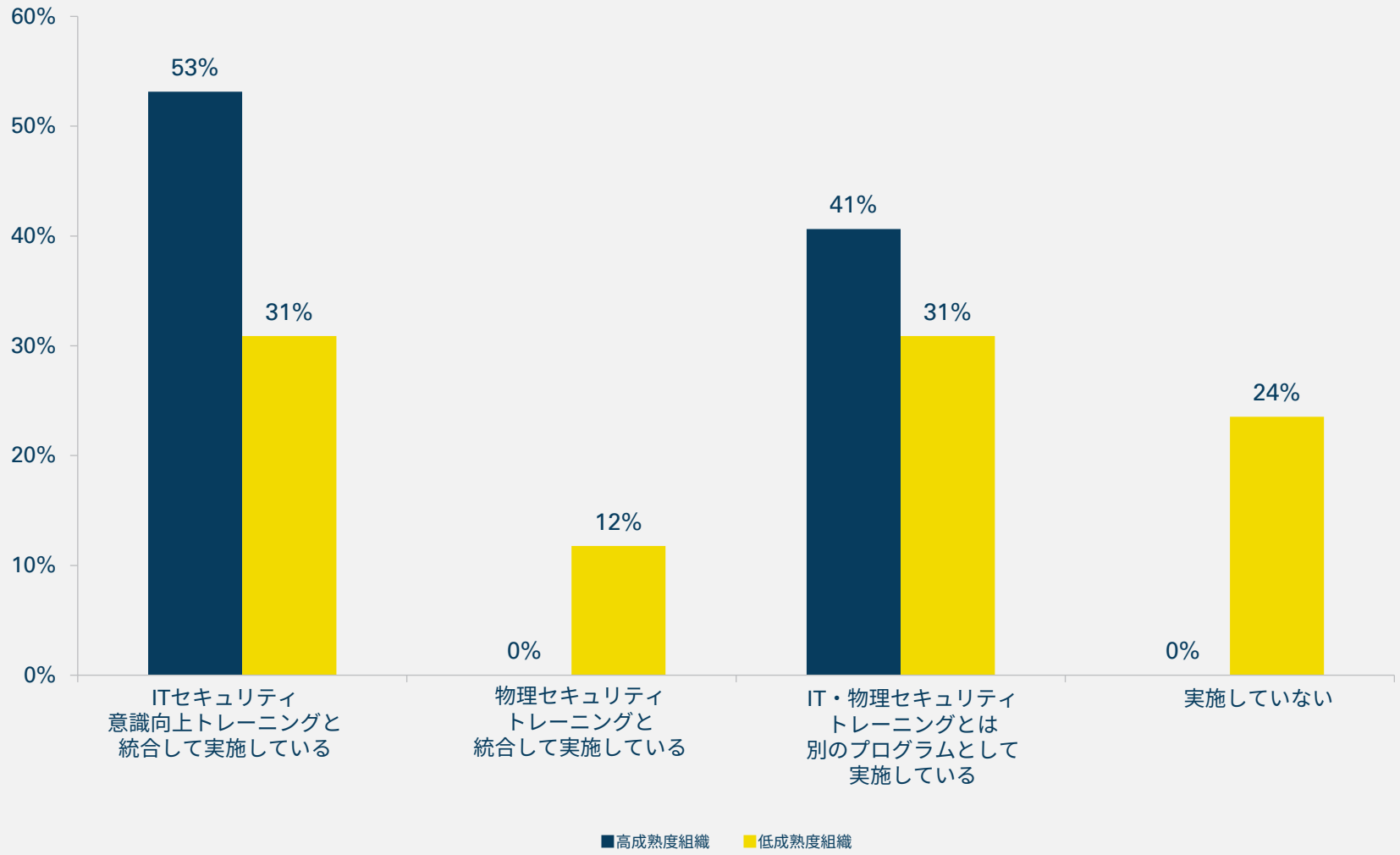
制御システムセキュリティ意識向上トレーニングの実施状況



(CS)²意識向上トレーニングの統合：高成熟度組織と低成熟度組織の比較

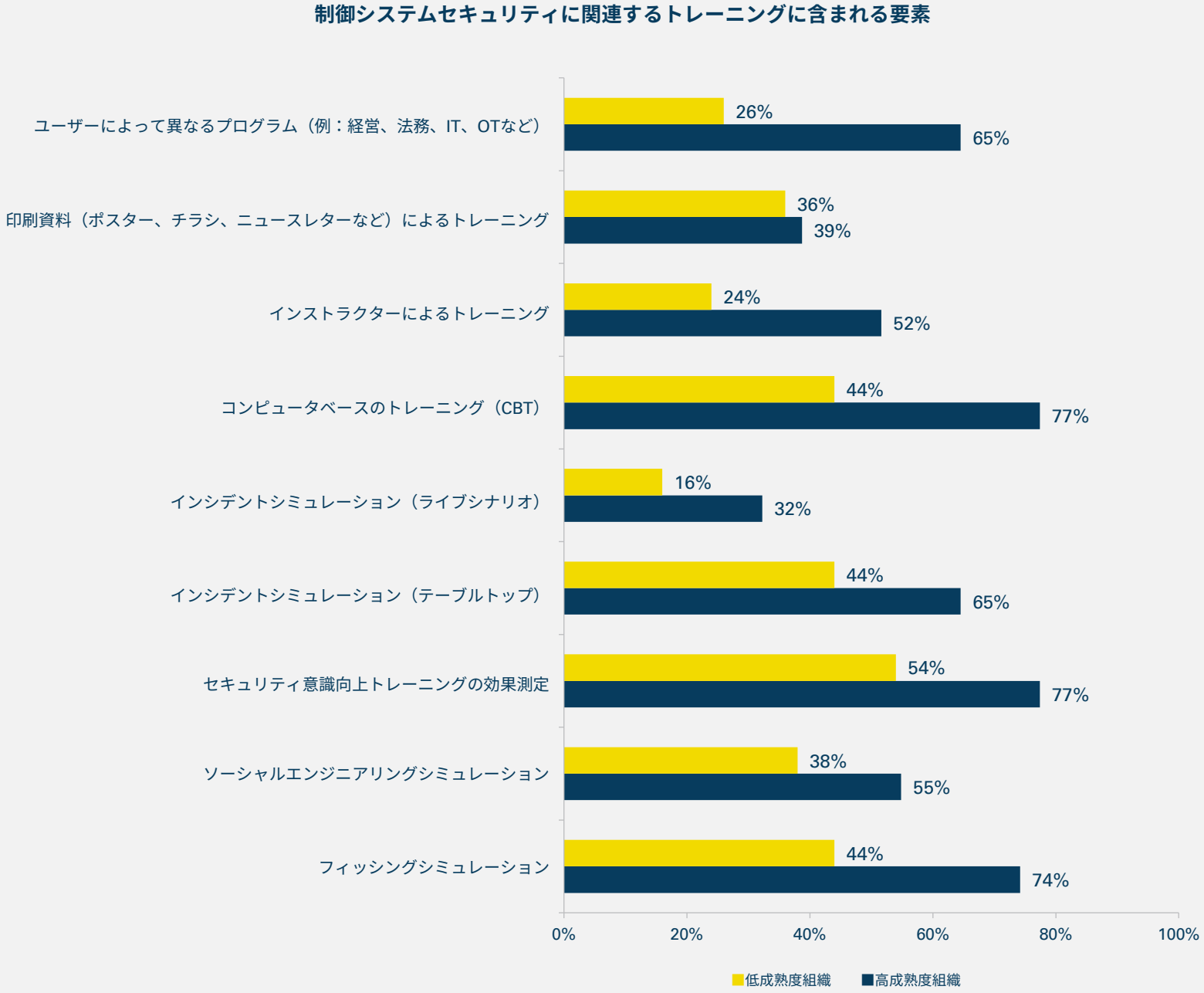
高成熟度組織と低成熟度組織の回答結果を比較すると、低成熟度組織の(CS)²セキュリティプログラムでは「意識向上トレーニング」関連の取組みが不足していることがわかります（「実施していない」と回答した割合は高成熟度組織：0%、低成熟度組織：24%）。一方、高成熟度組織では半数以上の回答者が「ITセキュリティ意識向上トレーニングと統合して実施している」と回答しました。

制御システムセキュリティ意識向上トレーニングの実施状況



(CS)²トレーニングの包括性：高成熟度組織と低成熟度組織の比較

さまざまなセキュリティプログラムの成熟度に関する説明ではセキュリティトレーニングに触れませんでしたが、このグラフから、高成熟度組織が従業員にトレーニングを受けさせることにより多く投資していることは明らかです。両グループの回答率が比較的近い値となった要素は「印刷資料によるトレーニング」のみでしたが、これは多くの場合、その他の項目に比べて有効性が低いと考えられています。実際に、さまざまなシミュレーションやトレーニングなどの非常に有効性が高い分野では、両グループの差が大きくなっているものがあります。また、「セキュリティ意識向上トレーニングの効果測定」（低成熟度組織：54%、高成熟度組織：77%）の実施割合が高い企業ほど、トレーニングの効果を重視し、トレーニングプログラムを継続的に改善できていると言えます。




SERVER ROOM ASSISTANT
12-8976-3457-567
1 ACCESS CATEGORY
FG12558BKLSPPP166161

(CS)²のネットワーク

制御システム要素のアクセシビリティ

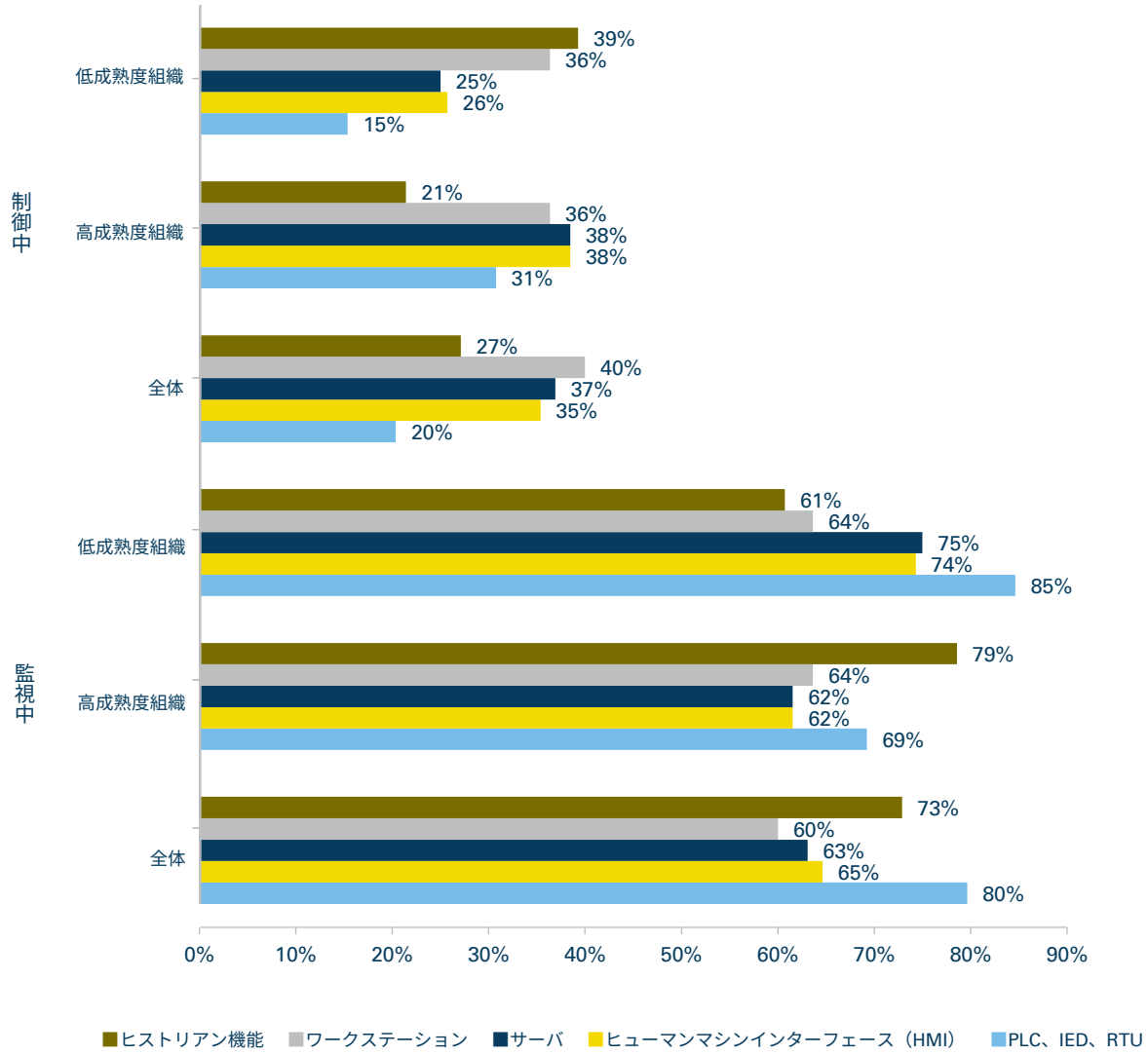
全体として、このグラフとそれに続く一連のグラフの内容は、非常に気がかりなものとなっています。制御システムへのインターネットからのアクセシビリティは、制御中の要素でもばらつきが大きく（低成熟度組織では「PLC、IED、RTU」：15%、「ヒストリアン機能」：39%）、攻撃者にとっての攻撃対象領域が広範で、企業は大きな影響を受ける可能性があることがわかります。

本調査の回答者である内容領域専門家（SME）のなかには、「アクセス可能であること」はアクセシビリティの「制御」または「方法」をさらけ出すことでもある点に留意すべきと指摘する人もいます。これらは、インターネットにオープンなポートを備えたシステム（ヒューマンマシンインターフェース（HMI）のログイン画面など）、インターネットからリモートアクセス可能なシステム（仮想プライベートネットワーク（VPN）、リモートデスクトッププロトコル（RDP）など）、インターネットに接続しているその他の機器から到達可能なシステム（ジャンプホストなど）、もしくはジャンプホストにアクセス可能なネットワーク上のシステムである可能性があります。各アクセシビリティおよびアクセシビリティを保護する制御の詳細は、企業のリスクレベルの評価における重要な検討事項です。

多くの項目で、高成熟度組織がインターネットを通じて要素を制御している割合が低成熟度組織と同程度であることは、興味深い点と言えます。実際は、「サーバ」、「ヒューマンマシンインターフェース（HMI）」、「PLC、IED、RTU」の項目では、高成熟度組織の回答が多い結果となっています[16]。また、ビジネスネットワーク、ベンダー／インテグレーター、クラウドからの要素へのアクセシビリティを示した次ページ以降のグラフでも同様の傾向がみられます。

16 高成熟度組織の回答でネットワークセグメンテーションにおけるROIが最も高い結果であったこと（75%、「(CS)²の投資対効果が高い分野：高成熟度組織と低成熟度組織の比較」（23ページ）のグラフを参照）が影響している可能性があります。

制御システム要素へのインターネットからのアクセシビリティ



制御システム要素のアクセシビリティ（続き）

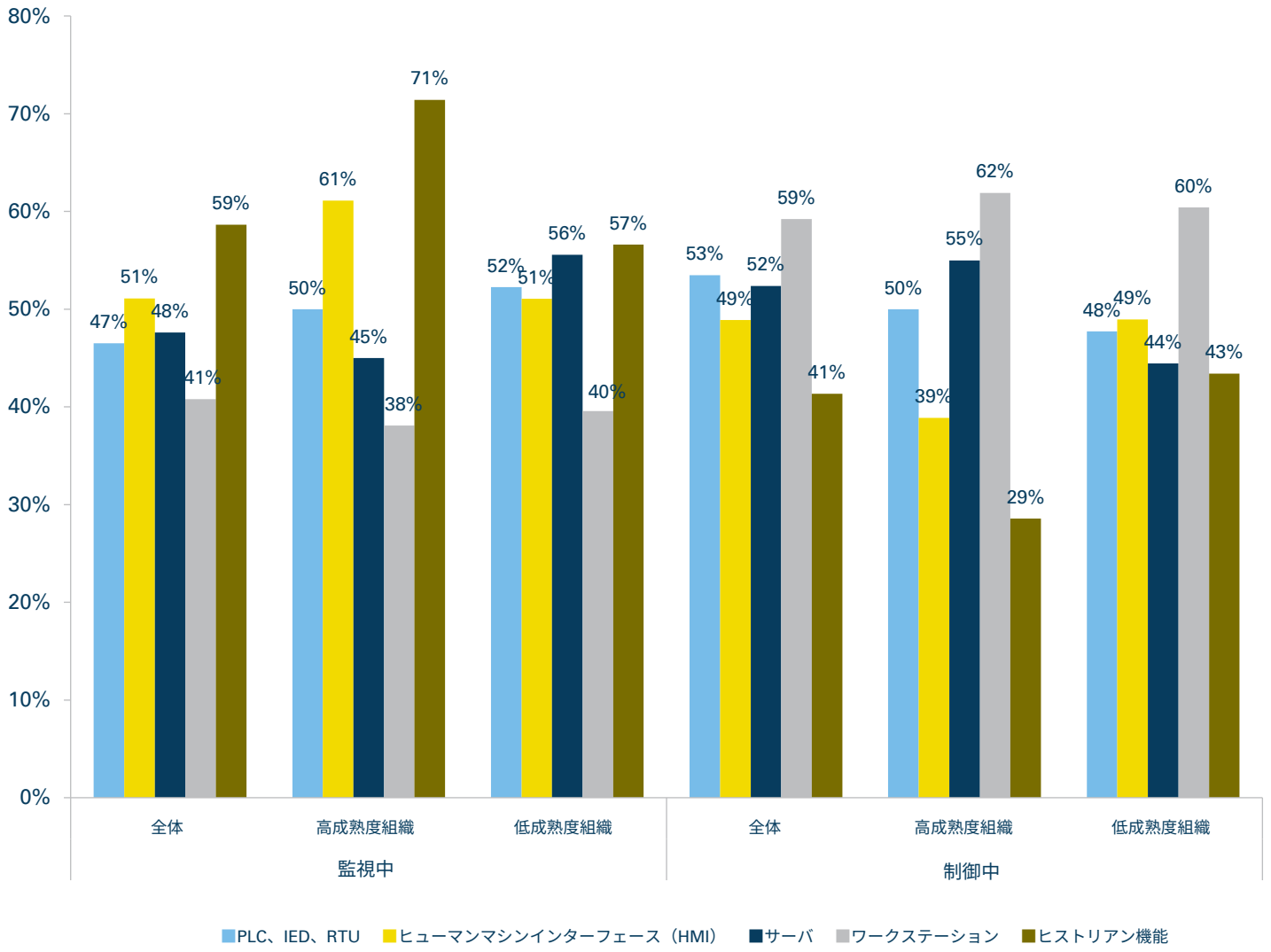
これらの対応は現在、ビジネスネットワーク、ベンダー、クラウドを含め、制御システムに対する外部からのアクセスが広く普及していることを示しています。このIT/OTコンバージェンスの拡大により、組織は制御システムセキュリティを別の領域としてではなく、全体的なセキュリティプログラムの一部として考えることが必要不可欠となっています。これは、セキュリティマネジメントプログラム（IEC 62443やISO 27001などの規格に準拠）と、こうしたシステムを保護・監視するための制御の両方にあてはまります。

Fortinet社の「2023年OTサイバーセキュリティに関する現状レポート」によると、ほぼすべての組織でOTセキュリティはCISOの担当業務の一部と考えられていることが示されています。IT/OTコンバージェンスの現実は、サイバー脅威の状況に関する組織の見方にも反映されています。大多数の組織が、ランサムウェアをOT環境に対するその他の脅威よりも深刻な問題と考えています。

Rod Locke氏

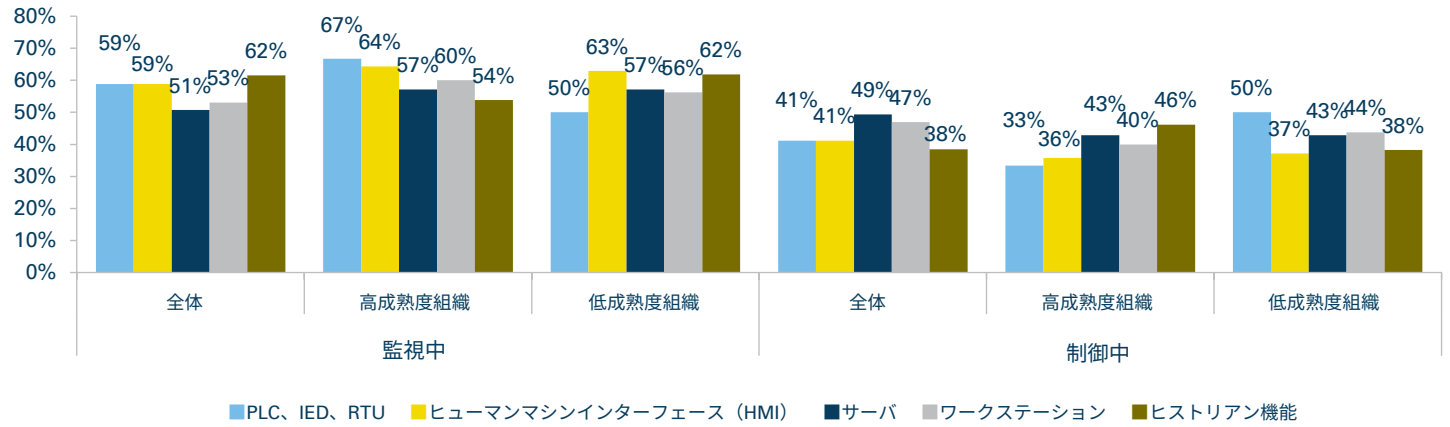
Director of Product Management
Fortinet社

制御システム要素へのビジネスネットワークからのアクセシビリティ

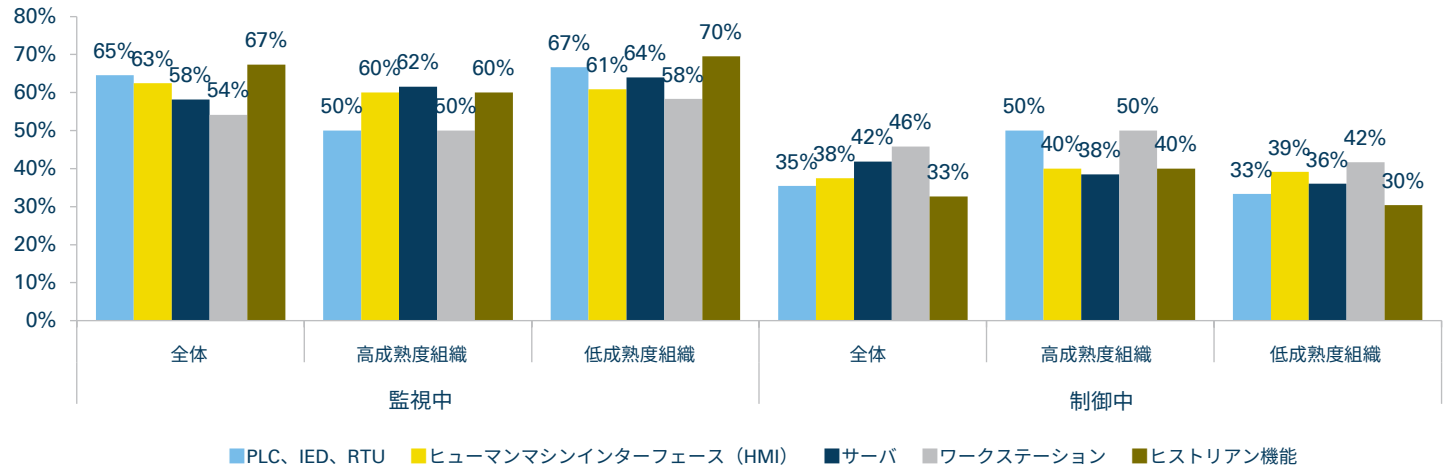


制御システム要素のアクセシビリティ（続き）

ベンダー／インテグレーターによる制御システム要素へのリモートでのアクセシビリティ

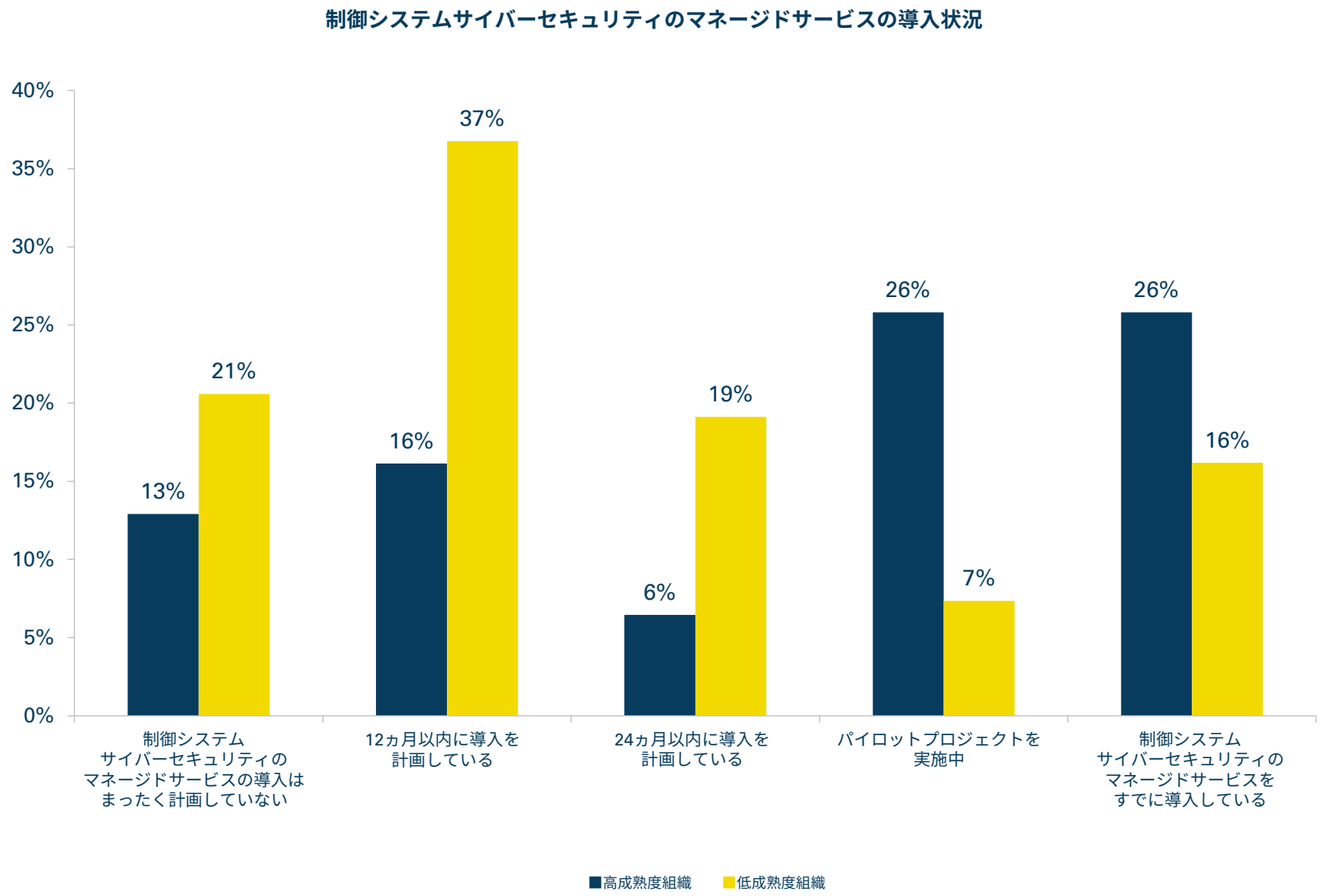


制御システム要素へのクラウドからのアクセシビリティ



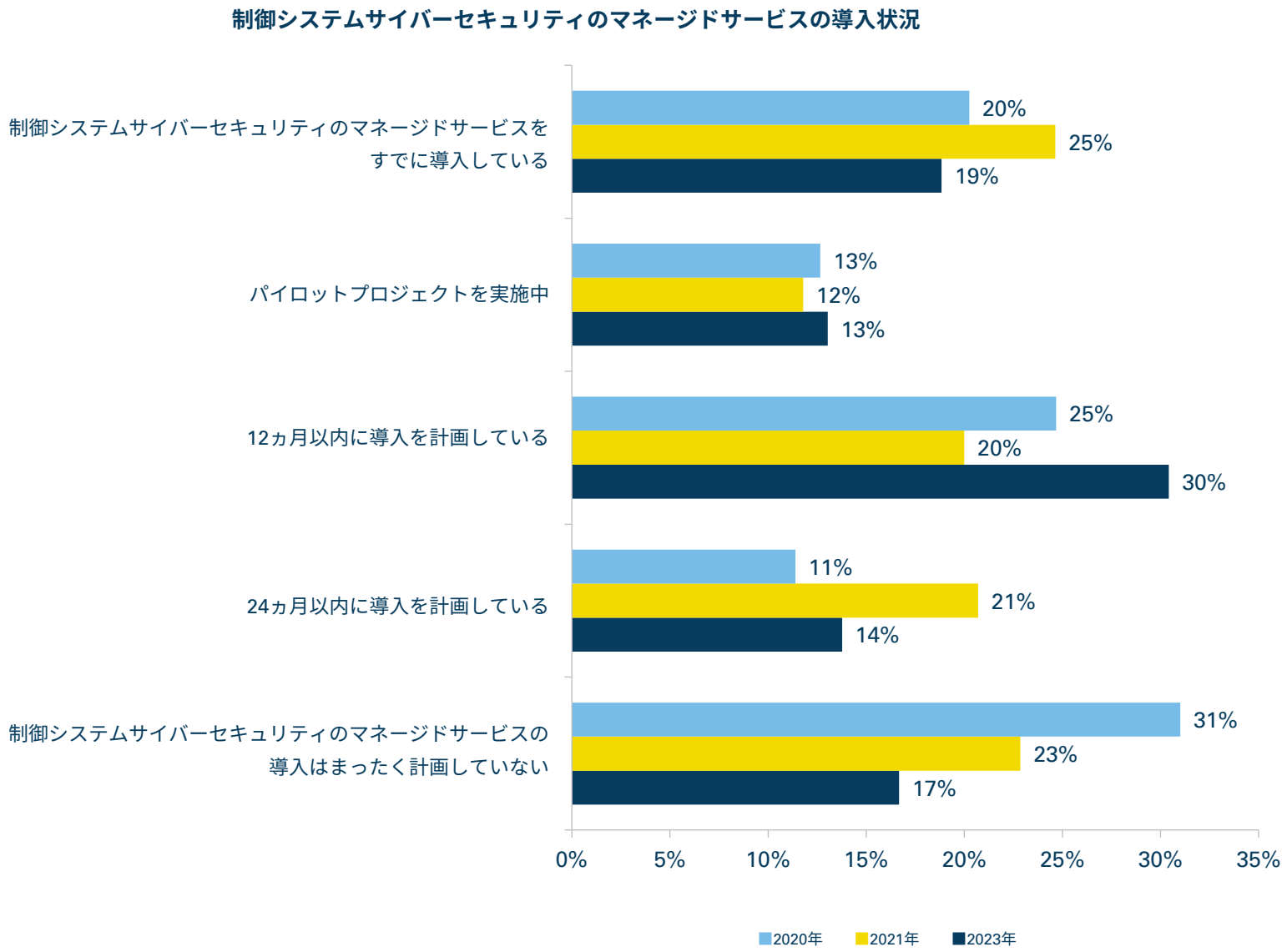
(CS)²のマネージドサービスの導入状況：高成熟度組織と低成熟度組織の比較

今回の調査では、前回に引き続き「制御システムサイバーセキュリティのマネージドサービスをすでに導入している」（高成熟度組織：26%、低成熟度組織：16%）、「パイロットプロジェクトを実施中」（高成熟度組織：26%、低成熟度組織：7%）のいずれにおいても高成熟度組織の回答割合が高い結果となりました。



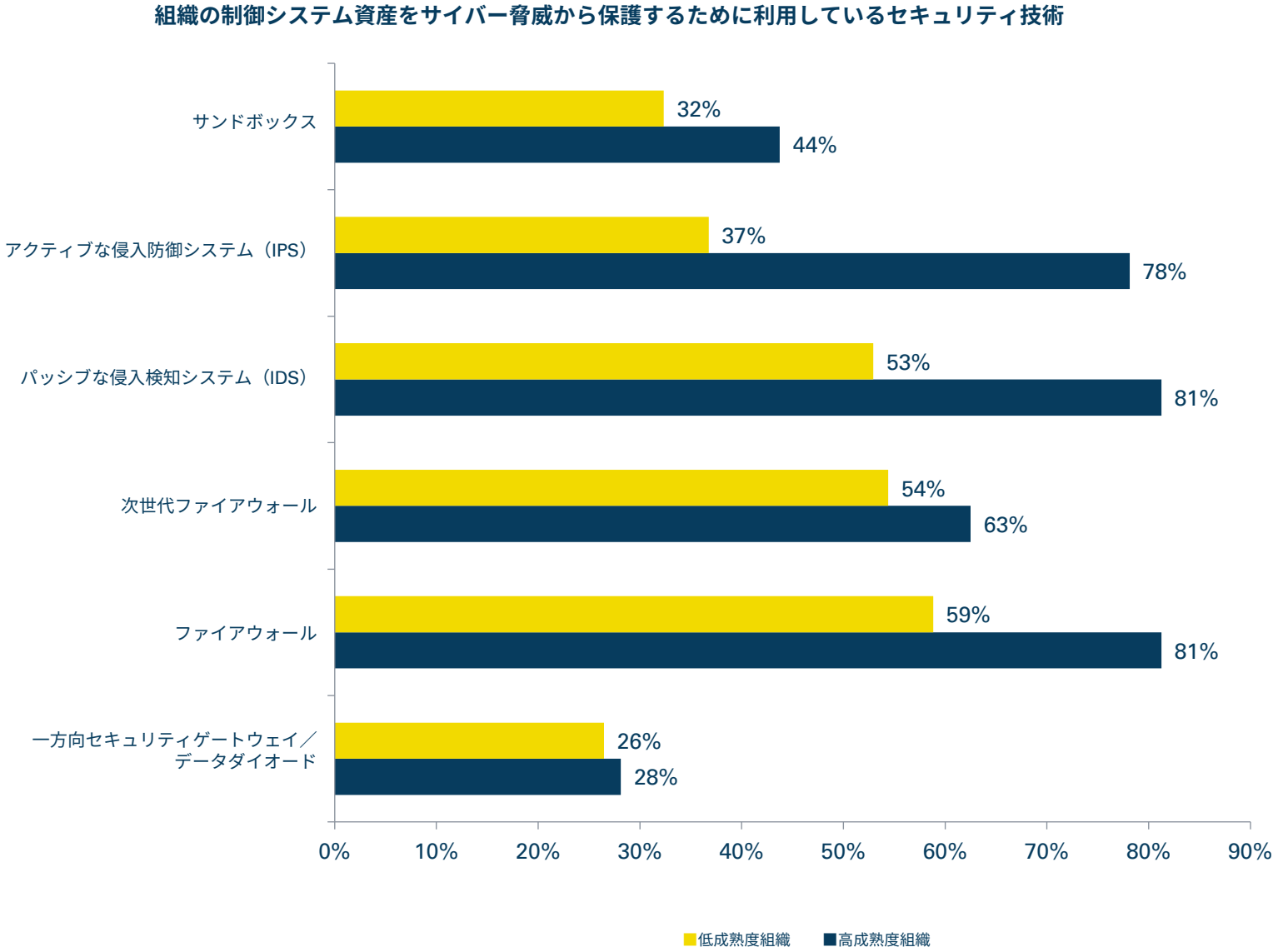
(CS)²のマネージドサービスの導入状況：縦断的分析

(CS)²のマネージドサービスへの移行は、我々が長年読者にアドバイスしている内容に即しています。社内人材のトレーニングや教育は言うまでもありませんが、短期では確実性が低下する可能性があるため、より長期的な投資が必要になっています。技術や慣行が急速に変化し、制御システムデバイスの接続性が高度に拡大するなか、(CS)²に精通した経験豊富な人材は、長い間供給不足に陥っています。したがって、(CS)²サービスの市場が拡大することは当然と言えます。十分なリソースを有する企業には、社内人材の開発プログラムを進めるとともに、資産と運用の保護という差し迫ったニーズに対処するために外部の専門知識を利用することを推奨します。これは組織の長期的な見通しの改善に最も有効なアプローチであると考えられます。



(CS)²技術の利用状況：高成熟度組織と低成熟度組織の比較

全体として、高成熟度組織はあらゆるセキュリティ技術を低成熟度組織よりも高い頻度で使用している傾向にあります。また、「アクティブな侵入防御システム（IPS）」（低成熟度組織：37%、高成熟度組織：78%）および「パッシブな侵入検知システム（IDS）」（低成熟度組織：53%、高成熟度組織：81%）の利用状況には大きな差が表れました。これは、高成熟度組織はより短時間で侵入を特定・遮断することにより、システムへの潜在的な影響を軽減できる可能性がはるかに高いことを示しています。



(CS)²のネットワークの監視：縦断的分析

制御システムネットワークの可視化は、ネットワークや接続された資産を保護するうえできわめて重要です。OT特有の文化は、歴史的にOT環境へのネットワーク監視技術の導入に消極的でしたが（当然ながら、導入により運用が中断されるケースがあるため）、この洞察を提供するツールと手法は成熟と改善を続けており、リスク対ベネフィットの比率が受け入れられつつあります。(CS)²ネットワークの監視と強化を予定している組織が前年比で増加したことは心強い結果です。「監視を実施中、さらに今後18ヵ月以内に頻度を増やす予定」と回答した組織の割合は、2020年には0%でしたが、2023年は18%に増加しています。ネットワーク稼働状況の監視を計画していない組織の割合は、初めて一桁台（9%）に減少しました。調査結果は組織が今後もネットワーク稼働状況の監視を展開し強化し続けることを示しています。監視を計画していない組織が2021年に急増（19%）したことは、当初、多くの組織が「すべての監視を実施中」の状態に移行していることを示していると考えられていました。しかし、今回の結果を鑑みれば、この考えには疑問が生じます。我々は、この点について今後も継続的に注視していきます。

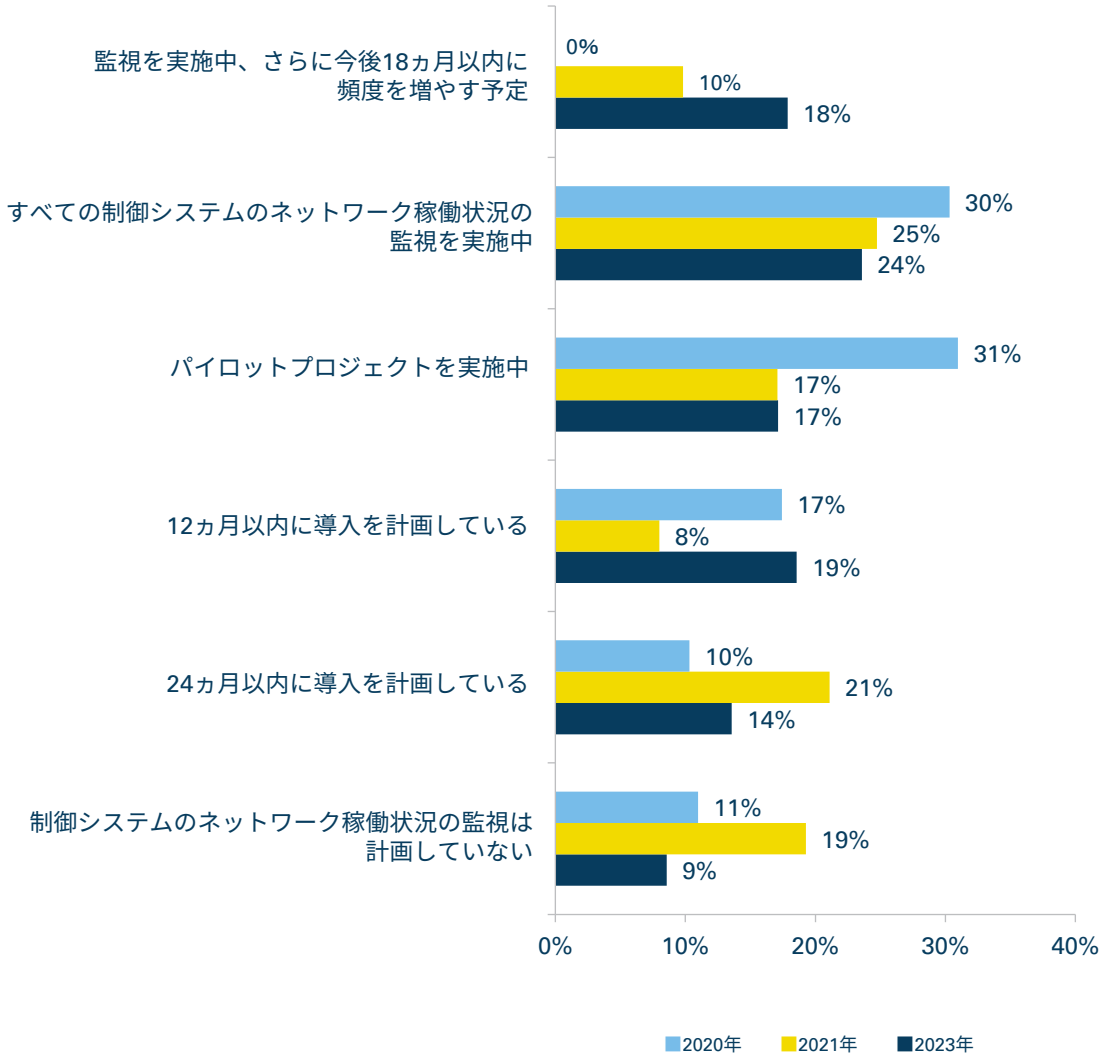
OTが現代化され、OTシステムとITシステムの接続性が高まるなか、攻撃対象領域は拡大し続けています。脅威アクターは非常に高度な「戦術・技術・手順」を用いて脆弱な部分を攻撃し、システムに被害を与え続けるでしょう。たとえば機能性に着目すると、きわめて高度化した機能により産業システムを混乱させる脅威アクターの例としてPipedreamが挙げられます。

悪意のある活動を検知し、こうしたインシデントに適切なタイミングで対処するには、OT/IT/IIOT（産業用IoT）ネットワークの可視化と継続的な監視が必要不可欠になるでしょう。

Eddie Toh

Partner
KPMGシンガポール
Head of Forensic Technology
KPMGアジア太平洋

制御システムのネットワーク稼働監視状況



(CS)²の可視性：エンドユーザーの回答

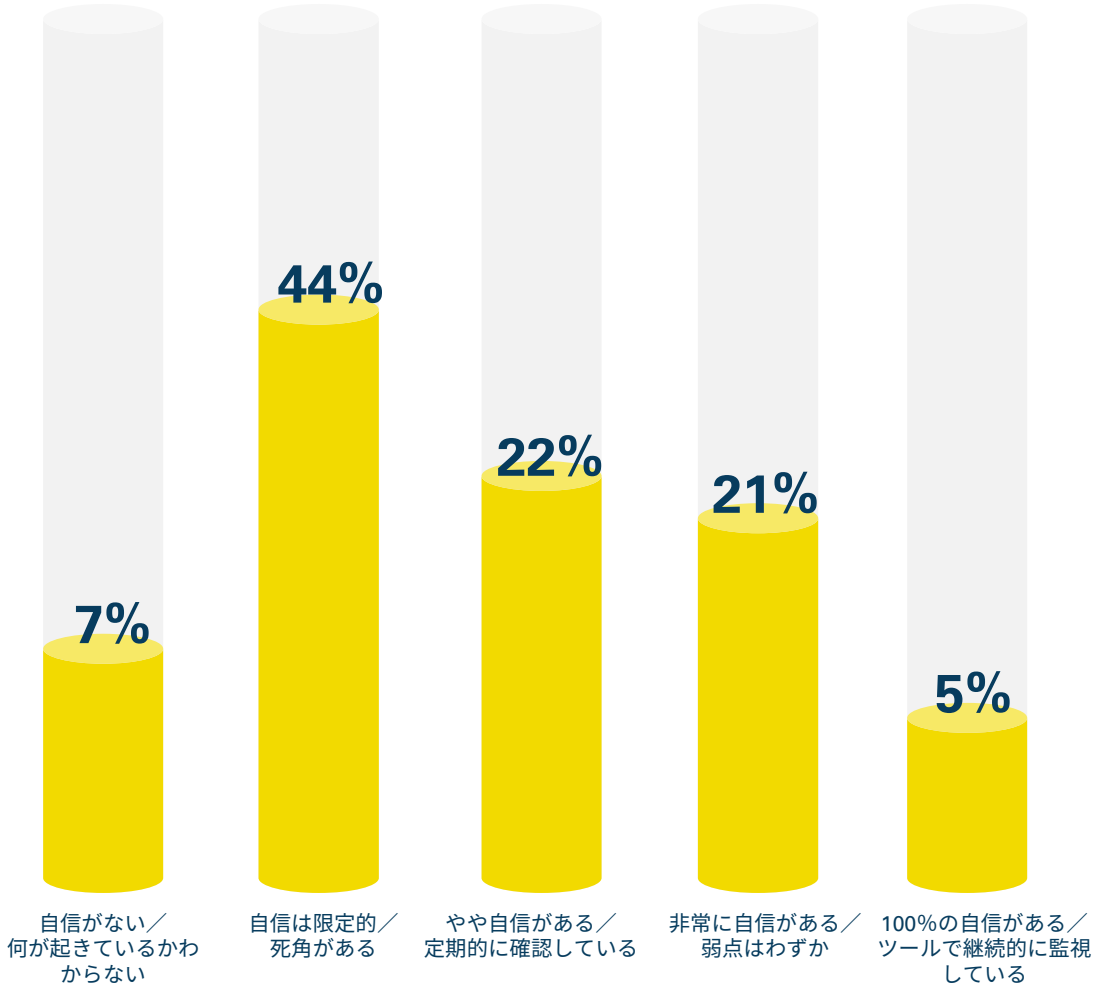
エンドユーザーの回答割合が最も高い結果であった項目（「自信は限定的／死角がある」：44%）は、非常に現実に即していると思われます。制御システムネットワークの可視化は恒常的な課題となっていますが、この重要な機能を備えたツールが普及してきたのはここ数年のことです。読者の皆様がまだ対応していない場合は、死角をなくし、(CS)²セキュリティ担当者に対して業務の遂行に必要不可欠な知識を提供するため、これらのツールを利用することを推奨します。

オフラインのネットワークモデリングは、非侵入型で包括的なネットワークの可視性を提供する最も迅速で効果的な方法です。これは、私たちが業務を中断することなく保護しようと努めているネットワーク環境について正確な理解を深めるのに役立ちます。ネットワークの構成、トポロジー、セキュリティ方針をオフライン環境で分析することにより、オンラインのネットワーク分析セッションでは発見されない可能性のある、重要な通信経路やカバレッジギャップに関する深い洞察を得ることができます。この方法では、ネットワークの整合性と性能を維持しながら可視化が不十分な領域を迅速に特定し対処することで、潜在的なサイバー脅威に対するネットワークの防御を強化します。

Robin Berthier氏

CEO and Co-Founder
Network Perception社

組織のネットワーク上のデバイス、ユーザー、アプリケーションの可視化に対する自信



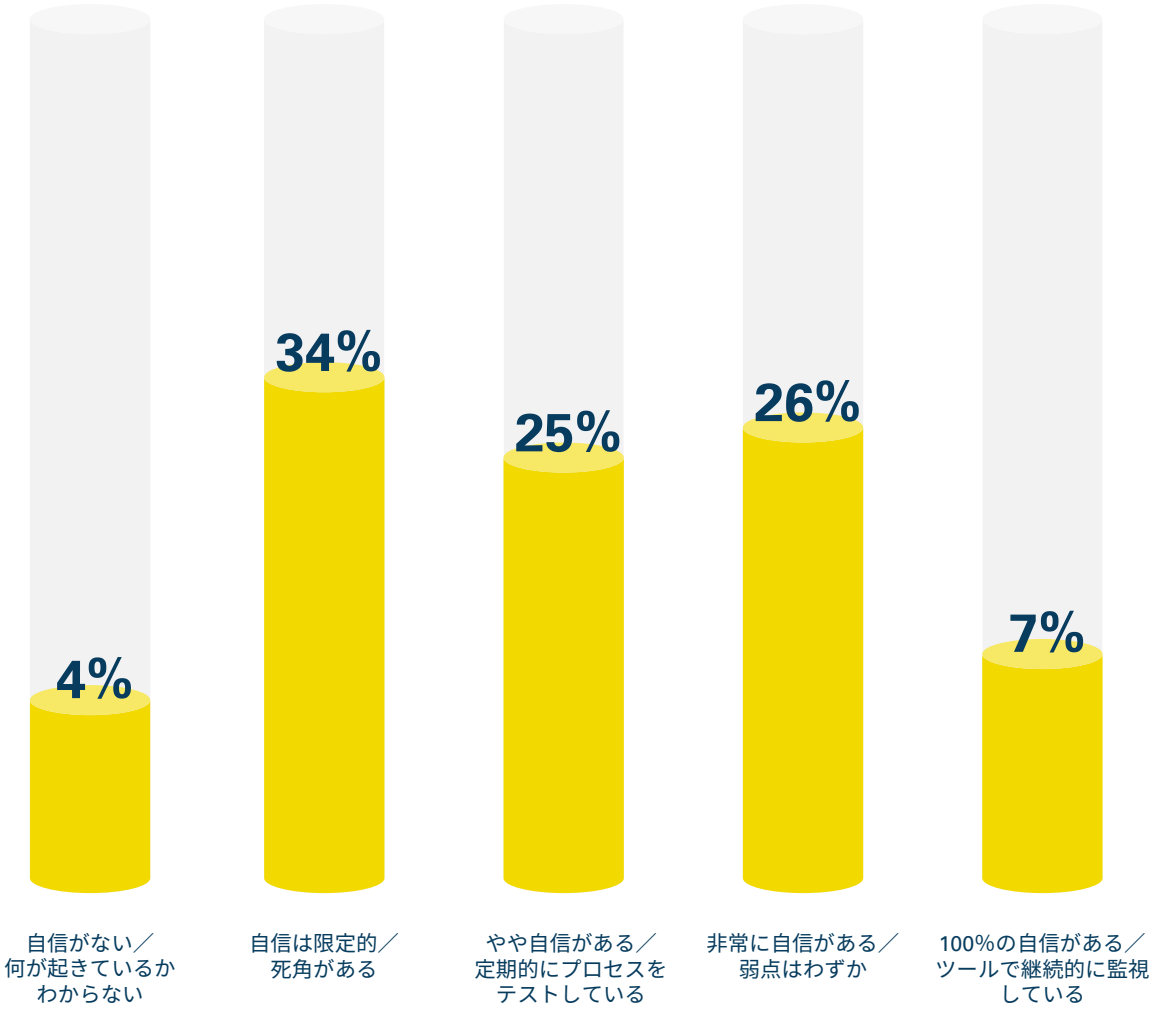

SERVER ROOM ASSISTANT
12-8976-3457-567
1 ACCESS CATEGORY
FG12558BKLSPPP166161

(CS)²インシデント

(CS)²攻撃への対応：エンドユーザーの回答

サイバー攻撃インシデントへの対応プロセスについて、(CS)²資産保有者および運用者（エンドユーザー）の58%が「やや自信がある」以上の回答を選択し、その大半が「非常に自信がある」または「100%の自信がある」と回答したことは喜ばしい結果です。これは、エンドユーザーのネットワークの可視化に対する自信を上回る結果となりました（「組織のネットワーク上のデバイス、ユーザー、アプリケーションの可視化に対する自信」（51ページ）のグラフを参照）。

サイバー攻撃を受けた場合の対応プロセスへの自信



昨今の(CS)²インシデント：縦断的分析

過去12ヵ月以内に発生した(CS)²インシデントが「50件以上」との回答はわずかに増加しました（前回の5%に対して今回は6%）。前回調査時からの顕著な変化としては、「発生していない」との回答が大幅に増加し（2021年：15%、2023年：25%）、一方で、「25件以上50件未満」との回答が大きく減少しました（2021年：19%、2023年：10%）。この結果が無知や誤りによるものではなく、保護とレジリエンスへの継続的な取組みの成果であることを願います。

サイバー攻撃は増加の一途をたどると思われます。これは工業生産のデジタル化における負の側面です。組織内だけでなく、外部パートナーのインターフェースも増えつつあり、残念ながら攻撃ベクトルは増加しています。

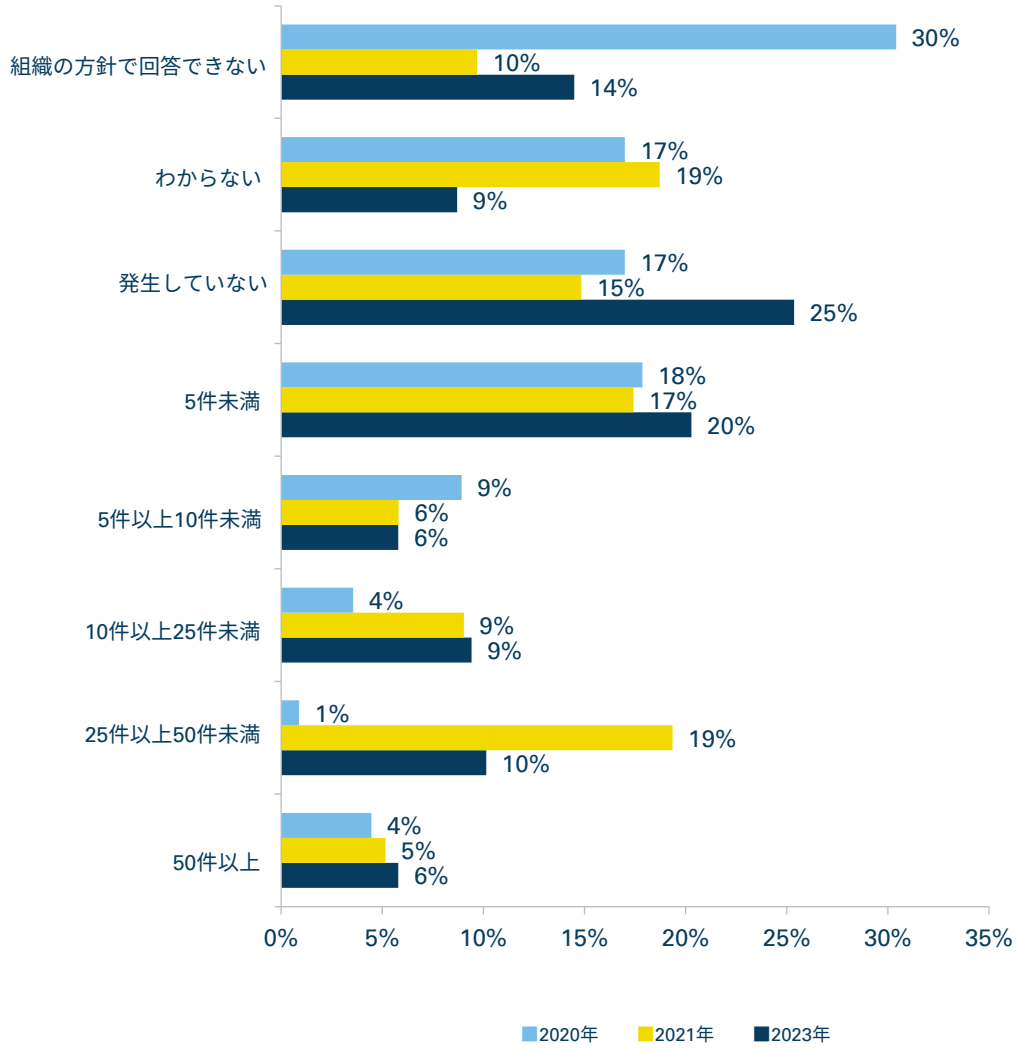
したがって、生産システムとプロセスを保護するためには優先順位を付け、的を絞ったアプローチを取ることが重要です。堅固なOTセキュリティアプローチは技術的側面だけでなく、セキュリティのプロセス、ガバナンス、人的要因をカバーすることができます。

防止・検知・防御においては、最新の状態に保つことがカギとなります。なぜなら、OTサイバーセキュリティには「変化」と「スピード」という2つのきわめて重要な特徴があるからです。

Marko Vogel

Partner and Head of OT Cybersecurity
KPMGドイツ

過去12ヵ月以内に組織内で発生した制御システムサイバーセキュリティインシデントのおおよその件数



顧客企業の(CS)²インシデント攻撃ベクトル：地域別[17]

今回の調査では、「電子メール（フィッシングメールなど）」（全世界：35%）および「ユーザーアカウントへの侵害」（全世界：31%）が攻撃ベクトルの1位と2位を占めました。ただし、これらの攻撃ベクトルは重複の可能性があります。「感染したリムーバブルメディア」の割合も前回より上昇しましたが、わずかな差で3位となりました（前回：24%、今回：26%）。リージョン5（中東・北アフリカ）では、「組織のウェブサイトへの侵害」がリージョン4（インド太平洋）とほぼ同水準（リージョン5：28%、リージョン4：31%）となった一方、「ベンダーのアップデートによる脆弱性」（36%）が他の地域よりも非常に高い結果となりました。リージョン4では、特に「Wi-Fiへの侵害」（24%）と「感染または破損したモバイルデバイスや携帯電話」（28%）の割合がその他のベクトルを大きく上回りました。

17 (CS)2AIは回答者を7つの地域に分類しました。

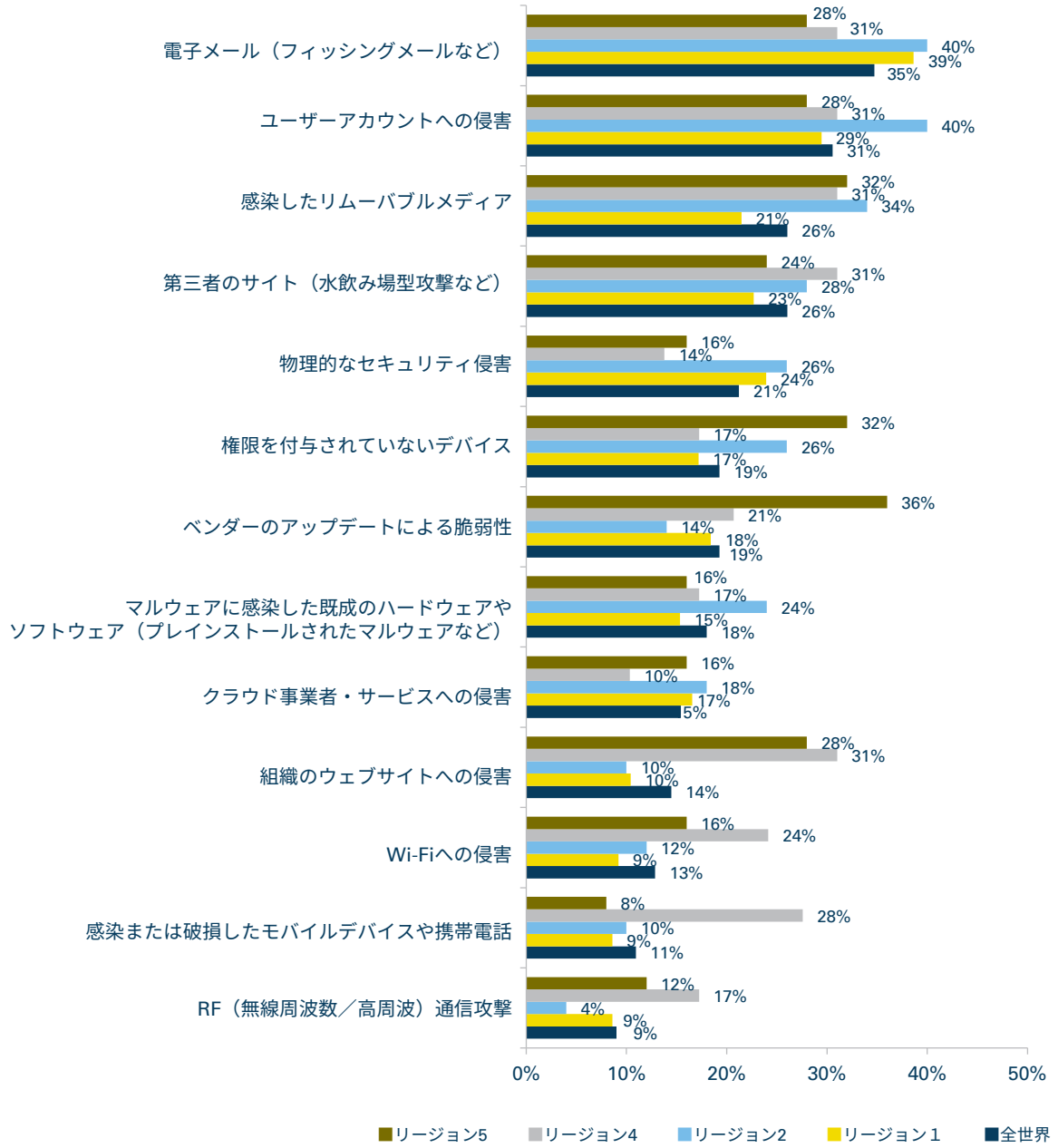
1) 北米、2) 欧州（中欧、西欧、北欧、南欧）、3) ユーラシア大陸、4) インド太平洋、5) 中東・北アフリカ、6) 南アフリカ、7) ラテンアメリカ・カリブ海地域

多くの組織では、さまざまな理由から、ITセキュリティの成熟度がOTセキュリティの成熟度よりも高くなっています。しかし、組織がIT/OTサイバーコンバージェンスを適用すれば、OTセキュリティの成熟度を向上させ、セキュリティ運用の効率を高め、企業のイノベーションを促進する絶好の機会を手にすることができます。IT/OTサイバーコンバージェンスは、多くの企業におけるセキュリティ体制の統合、攻撃対象領域の縮小、IIoTを活用したデジタルトランスフォーメーションの促進、先進技術による意思決定能力の向上に寄与します。

Hossain Alshedoki

Cybersecurity & Privacy Energy and Natural Resources Lead
KPMGサウジアラビア

過去12ヵ月以内に対応した顧客企業の(CS)²インシデントで悪用された攻撃ベクトル



(CS)²インシデントによる被害：縦断的分析

この質問は過去数年間の調査で変更があり、調査分析の精度向上を目的として回答の選択肢を追加したため、2020年にはなかった回答が複数あります。

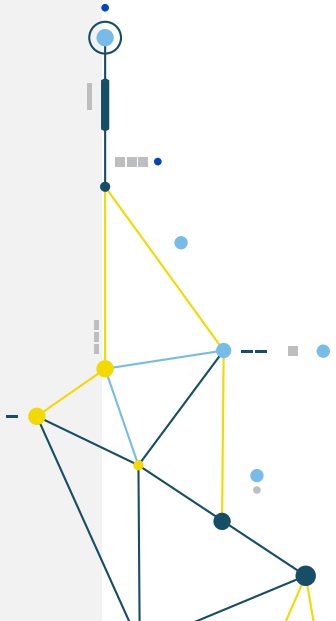
「業務の中断・停止による金銭的損失」、「負傷」、「製品の損失」の割合が前回より増加したことは、重要なポイントです。前述の調査結果と同様に、ここでも業務の継続が重要視されています（「支出の優先順位：役職クラス別」（24ページ）、「予算に関する顧客企業へのアドバイス：ベンダーの回答」（25ページ）のグラフを参照）。

「人命の損失」の回答結果については、ここ数年間にわたり疑問視し続けています。おそらく、悪意のあるサイバー攻撃によって人命が失われた場合にはトップニュースとして報道されると思われます。企業や政府が報告を公表していない事件があるとしても、こうしたインシデントに関する報道が1件もないにもかかわらず、この数年間の調査で「サイバーインシデントによる人命の損失」が発生したとの回答が5〜6%となった理由は説明がつきません。調査回答者には、システムの中断が直接的または間接的に人命の損失につながる病院や医療センターなどの保護を担当する個人が含まれていますが、この結果を説明できるほど多くはありません。これらの「インシデント」は、意図的な攻撃を受けたことによるものと思い違いをされており、実際はコンピュータのエラーに起因している可能性があります。

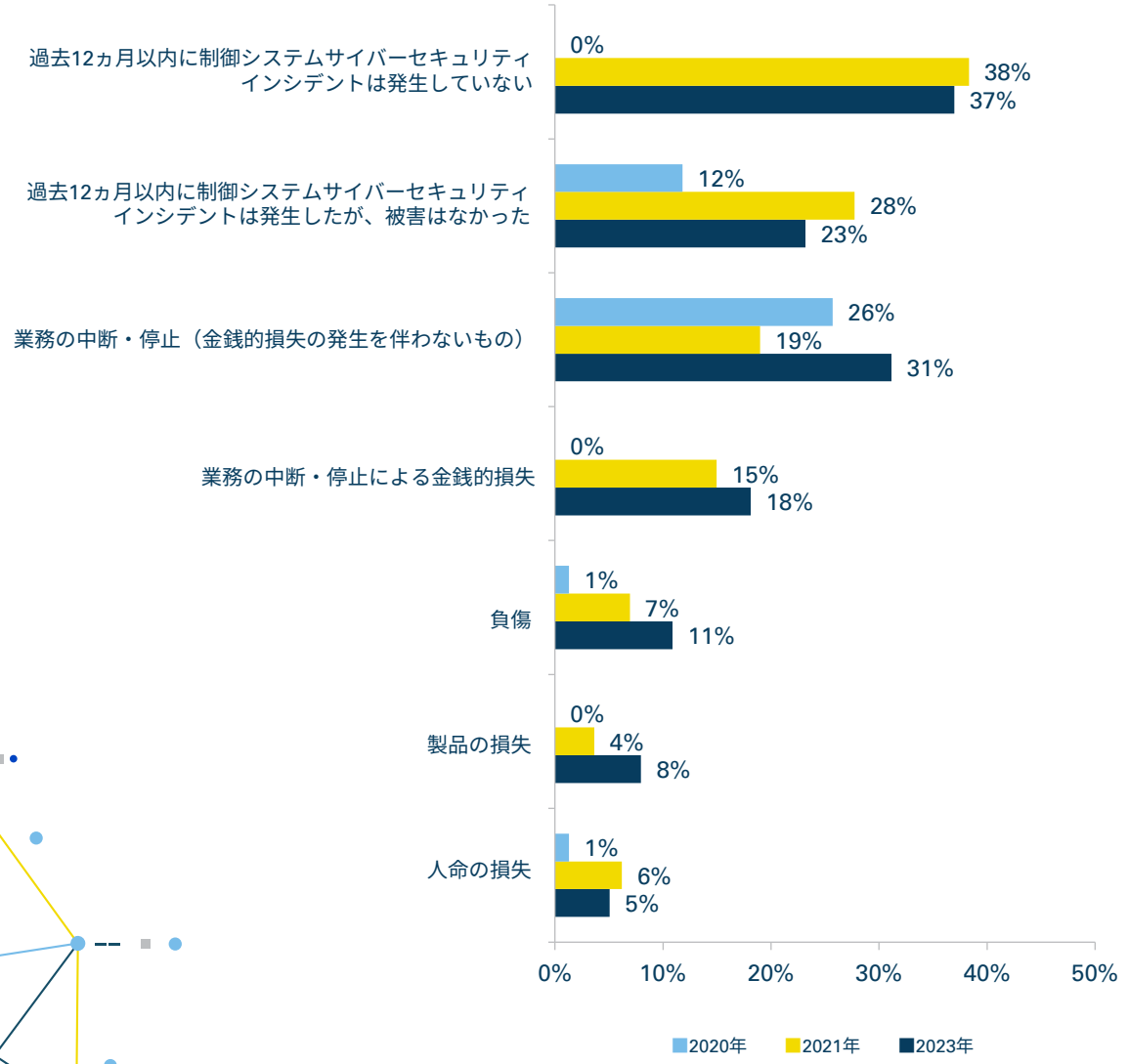
(CS)²の侵害に関する調査データは、セキュリティインシデントによる業務の中断が頻発していること、またそれに伴う被害が深刻化していることを示しています。Fortinet社の「2023年OTサイバーセキュリティに関する現状レポート」でも、業務環境に何らかの影響を受けたと回答した組織は49%で、本調査の結果に近い割合となっています。同レポートでは、高成熟度組織ほど、ネットワークへの侵害と業務への影響がより少ないことが明らかになっています。また、高成熟度組織は、経営層や取締役会に提出するリスク報告書において、OTサイバーセキュリティ体制を重要な要素として盛り込んでいる傾向が強まっています。

Rod Locke氏

Director of Product Management
Fortinet社



過去12ヵ月以内に発生した制御システムセキュリティインシデントに起因する被害



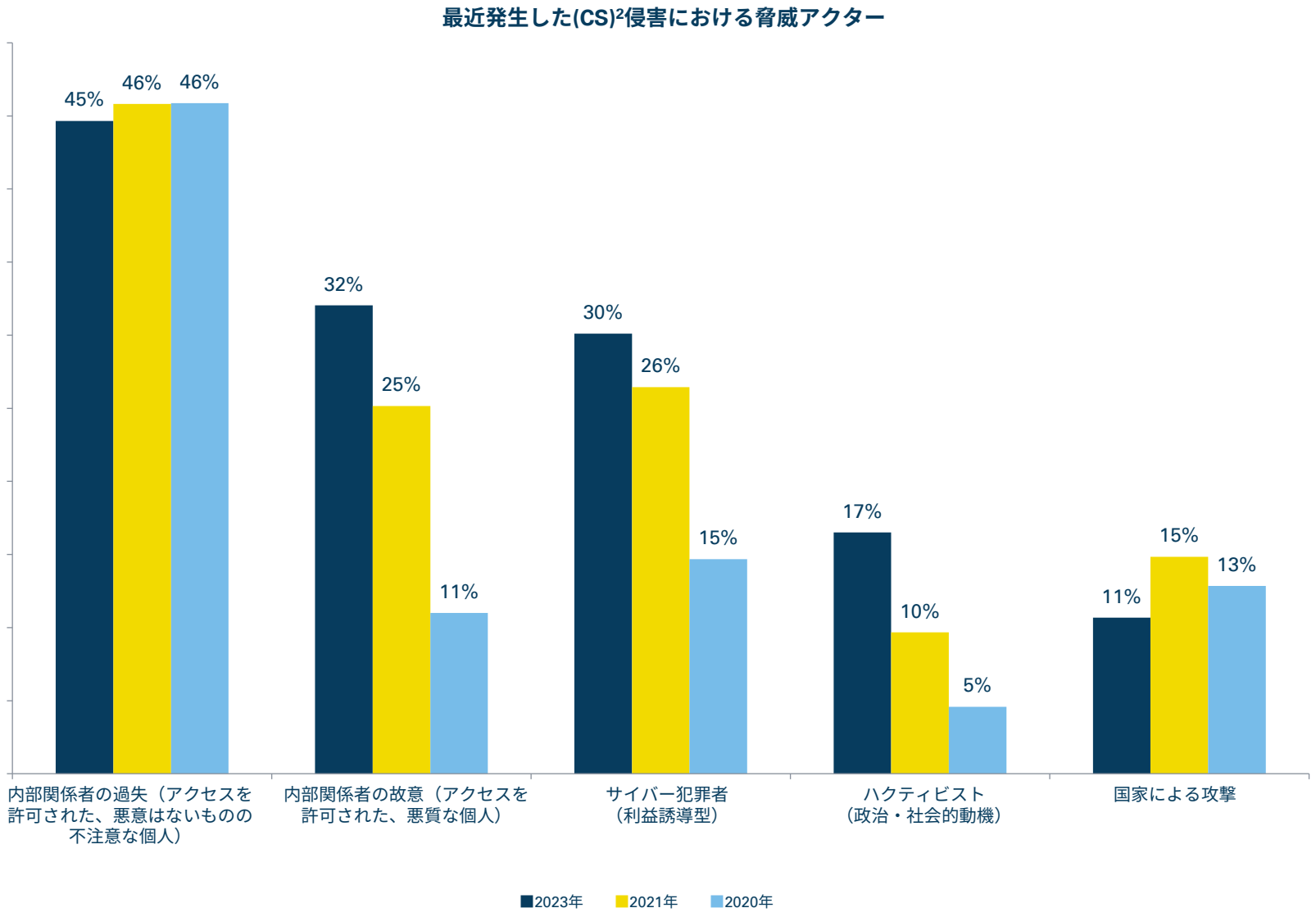
昨今の(CS)²攻撃ベクトル：縦断的分析

全世界における各攻撃ベクトルの頻度について分析しました。前回までの結果と比較すると、複数の項目で明確な増加がみられました。「クラウド事業者・サービスへの侵害」（2020年：6%、2023年：25%）、「組織のウェブサイトへの侵害」（2020年：6%、2023年：17%）および「Wi-Fiへの侵害」（2020年：3%、2023年：17%）の回答割合が継続して増加していることは注目に値します。また、攻撃者はフィッシングにとどまらず、標的とする攻撃対象領域以外の部分にも拡大しているとの脅威に関する調査報告を裏付けています。「クラウド事業者・サービスへの侵害」および「Wi-Fiへの侵害」は、少なくとも部分的には、近年の(CS)²環境においてこれらのソリューションの利用が増加していることが原因である可能性があります。「ユーザーアカウントへの侵害」および「権限を付与されていないデバイス」は今回新たに追加された項目であり、2020年と2021年の結果は含まれていない点にご留意ください。「ベンダーのアップデートによる脆弱性」は2021年に追加されました。

過去12ヵ月以内に組織内で発生した(CS)²インシデントで悪用された攻撃ベクトル

(CS)²の脅威アクター：縦断的分析

「国家による攻撃」と「内部関係者の過失」は比較的変化が少なく、後者は引き続き最も多い回答割合となりました。「内部関係者の故意」、「サイバー犯罪者」および「ハクティビスト」が前年より増加したことは注目に値します。なお、地域間で大きな差はみられませんでした。報道機関と国家情報機関は、利益誘導型サイバー犯罪者の活動がこの数年で急増していると考えており、本調査結果もこれに一致しています。一方で、「内部関係者の故意」による(CS)²侵害の増加は、表立って明らかになっていません。これは、社会的な分断と緊張の高まりによる副産物なのかもしれません。



ベンダーによるアドバイス

顧客企業が重視すべきKPIに関するアドバイス：ベンダーの回答

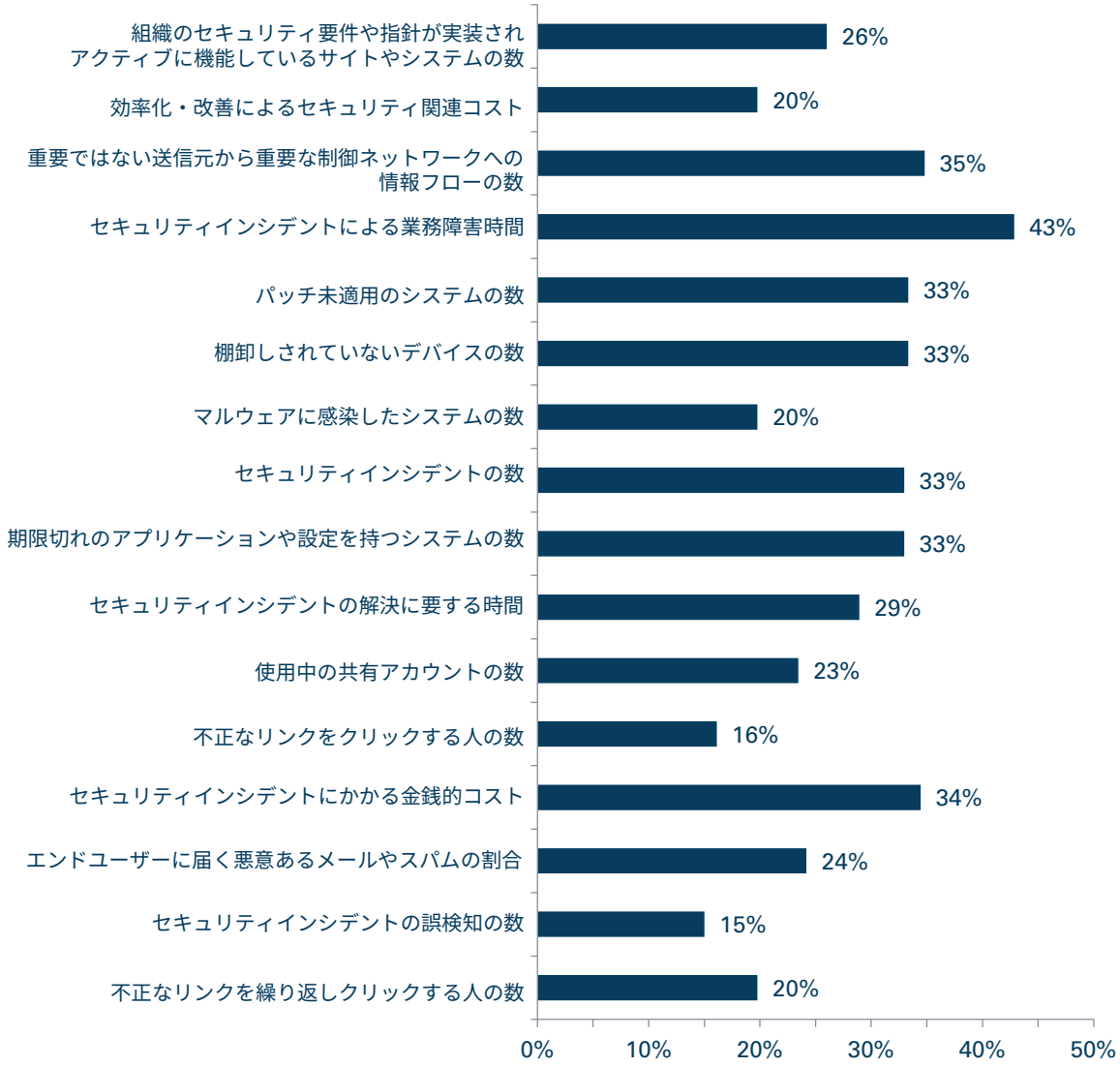
Waterfall Security Solutions社およびICSStriveによる「2023 Threat Report」では、OT被害をもたらす攻撃は過去4年間で急増していることが示されています。本調査では、重視すべきKPIの上位3項目は「重要ではない送信元から重要な制御ネットワークへの情報フローの数」、「セキュリティインシデントによる業務障害時間」、「セキュリティインシデントにかかる金銭的コスト」となりました。

これらのKPIは、被害の軽減と堅固なソリューションの展開に対する強い意欲を示しています。アイダホ国立研究所が主導する新たな戦略「Cyber-Informed Engineering」の一環として、物理的な被害を軽減し、情報フローを確定的に制御する強力なエンジニアリングレベルのソリューションは、こうした取組みをサポートするものです。

Andrew Ginter氏

VP Industrial Security
Waterfall Security Solutions社

セキュリティプログラムのKPIにおいて、次年度に顧客企業が重点的に取り組むべき項目

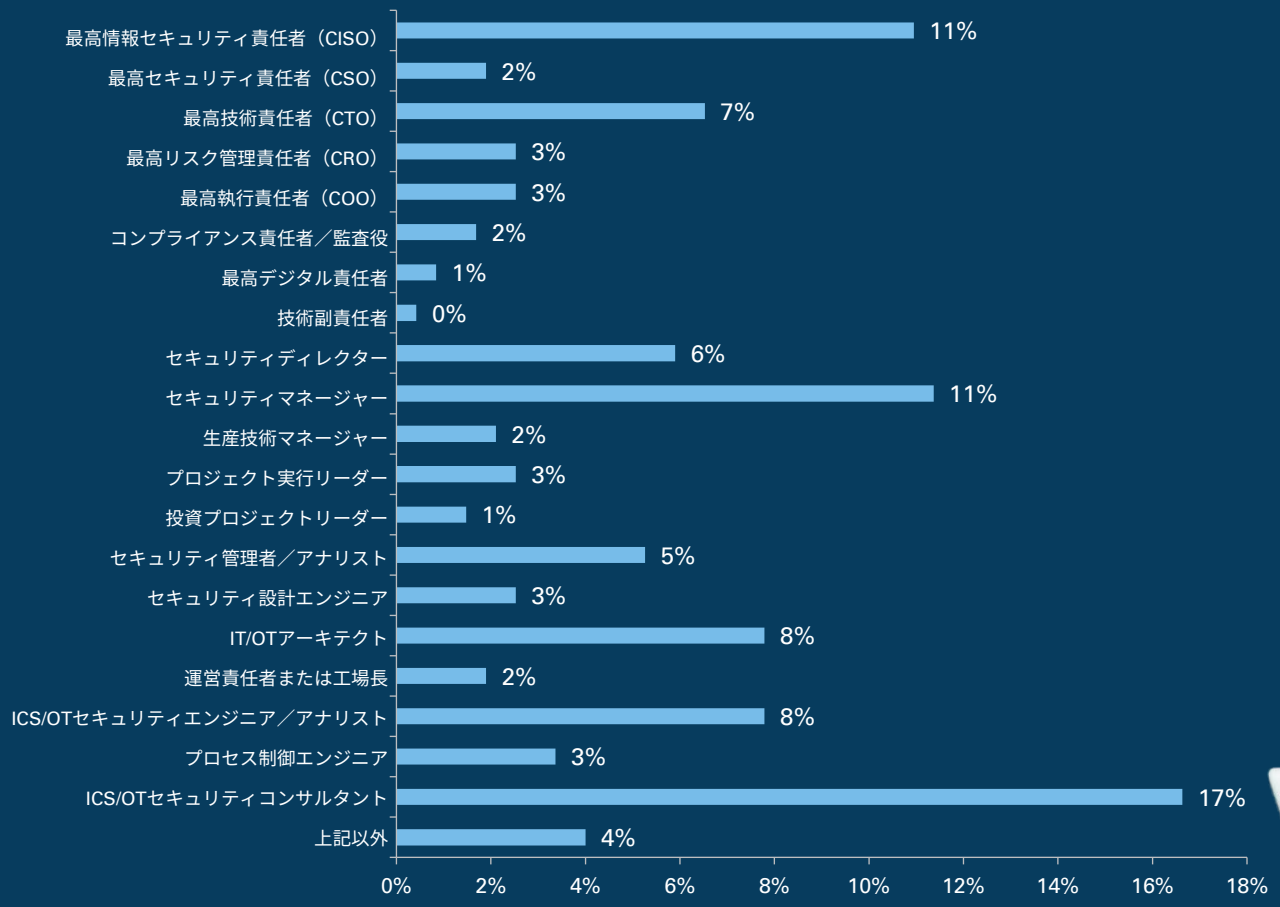



SERVER ROOM ASSISTANT
12-8976-3457-567
1 ACCESS CATEGORY
FG12558RKLSPPP166161

付録A：回答者属性

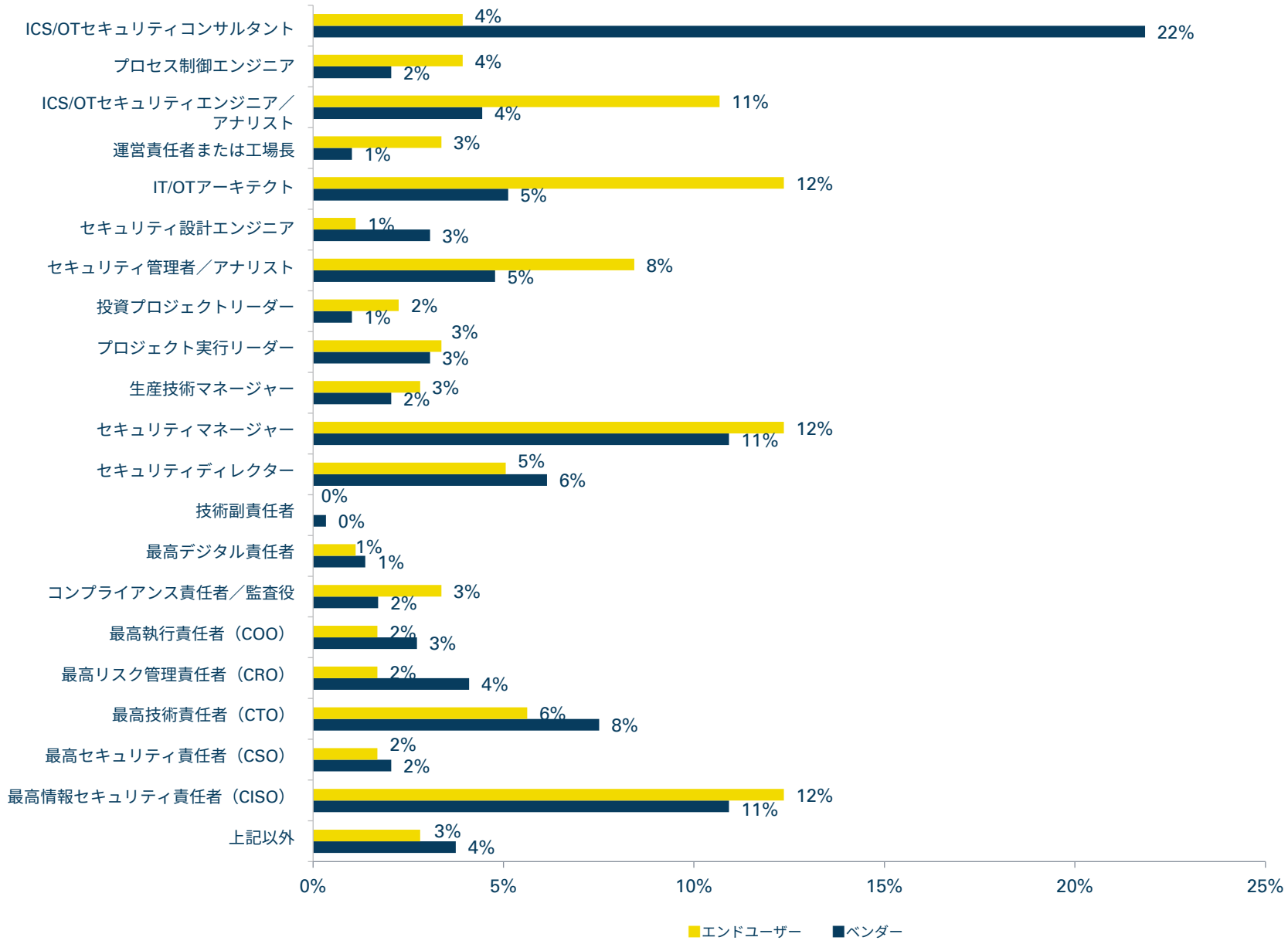
役職

制御システムセキュリティ関連業務における回答者の役職

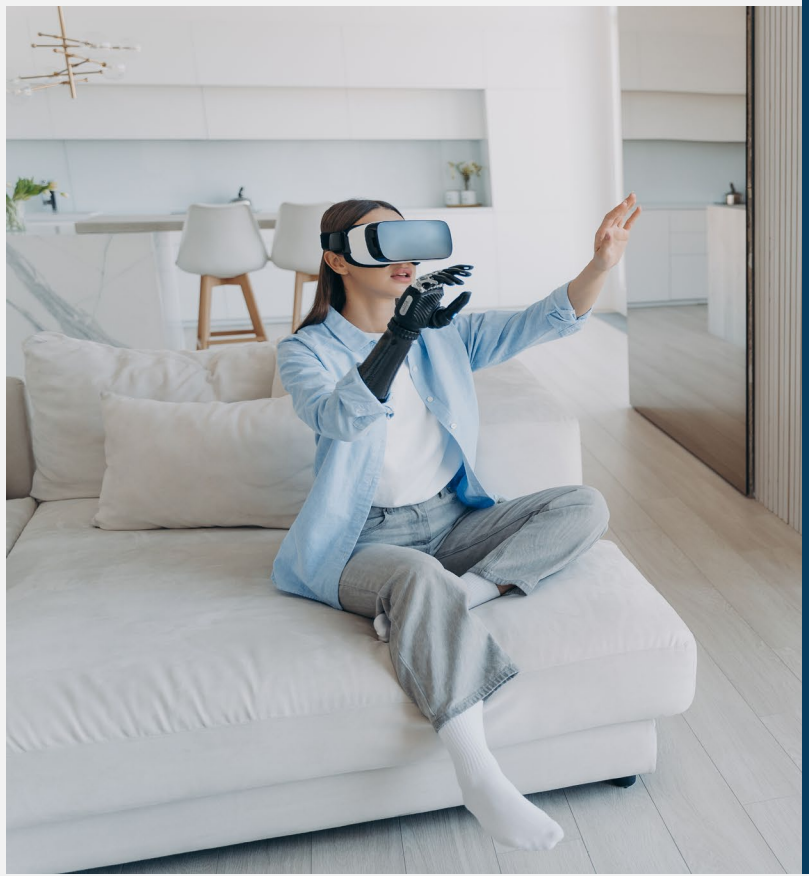


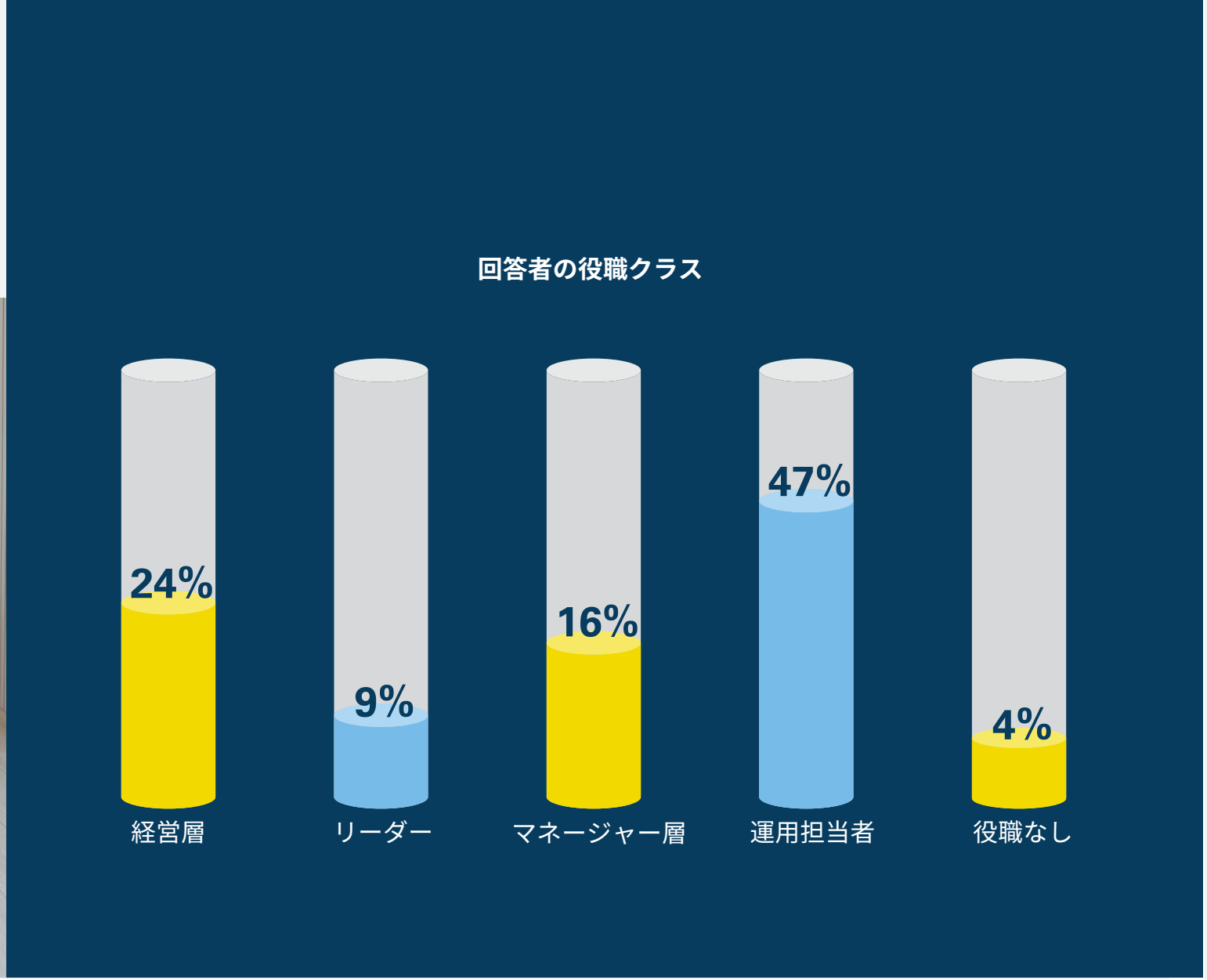
役職：
エンドユーザーとベンター

制御システムセキュリティ関連業務における回答者の役職



役職クラス



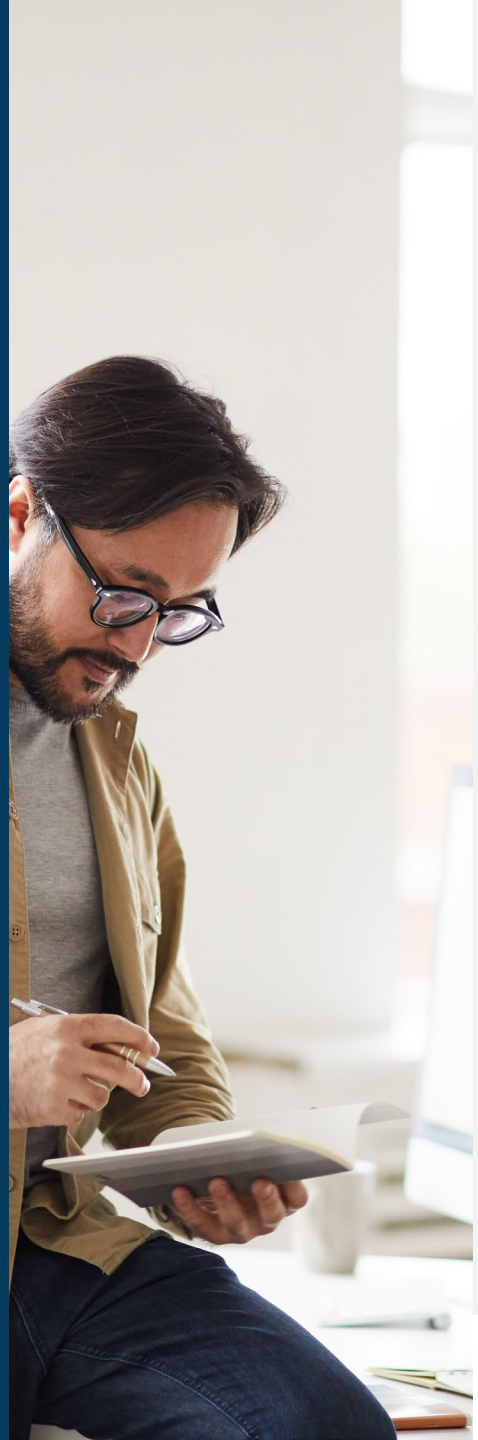


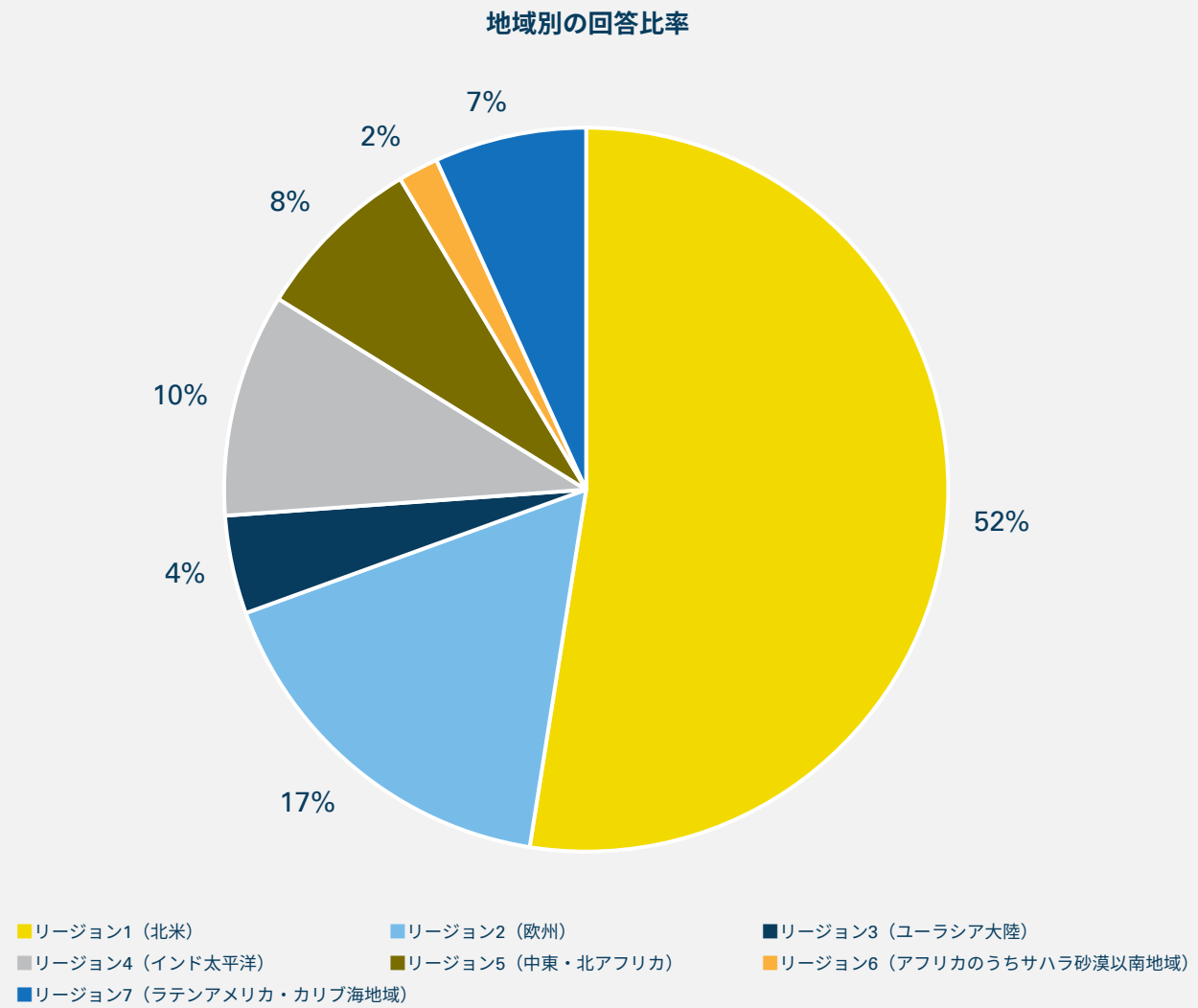
地域別の回答比率

(CS)2AIは回答者を7つの地域に分類しました。

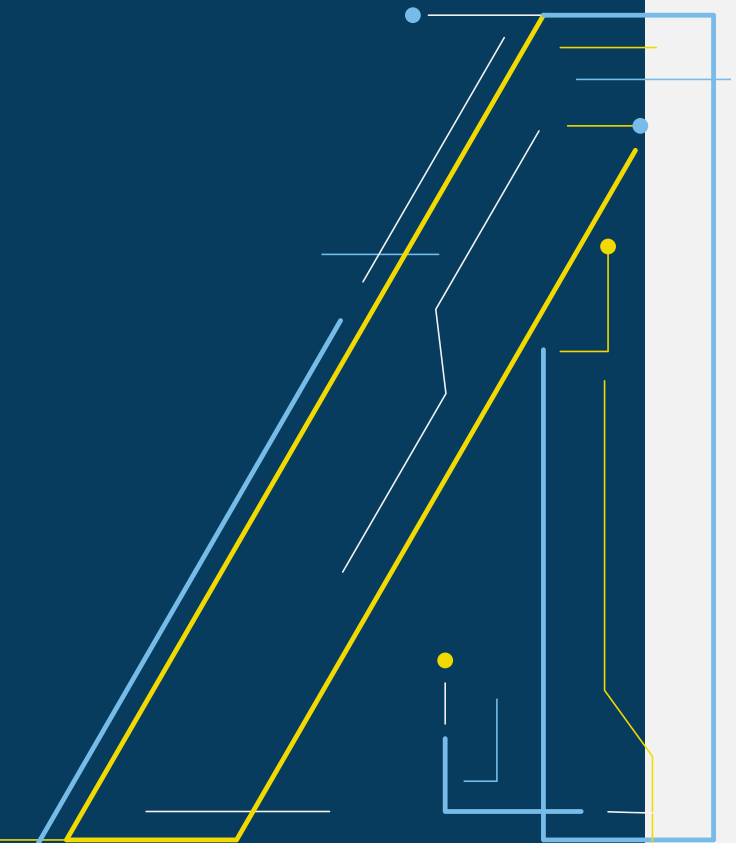
1. 北米
2. 欧州（中欧、西欧、北欧、南欧）
3. ユーラシア大陸
4. インド太平洋
5. 中東・北アフリカ
6. アフリカのうちサハラ砂漠以南地域
7. ラテンアメリカ・カリブ海地域

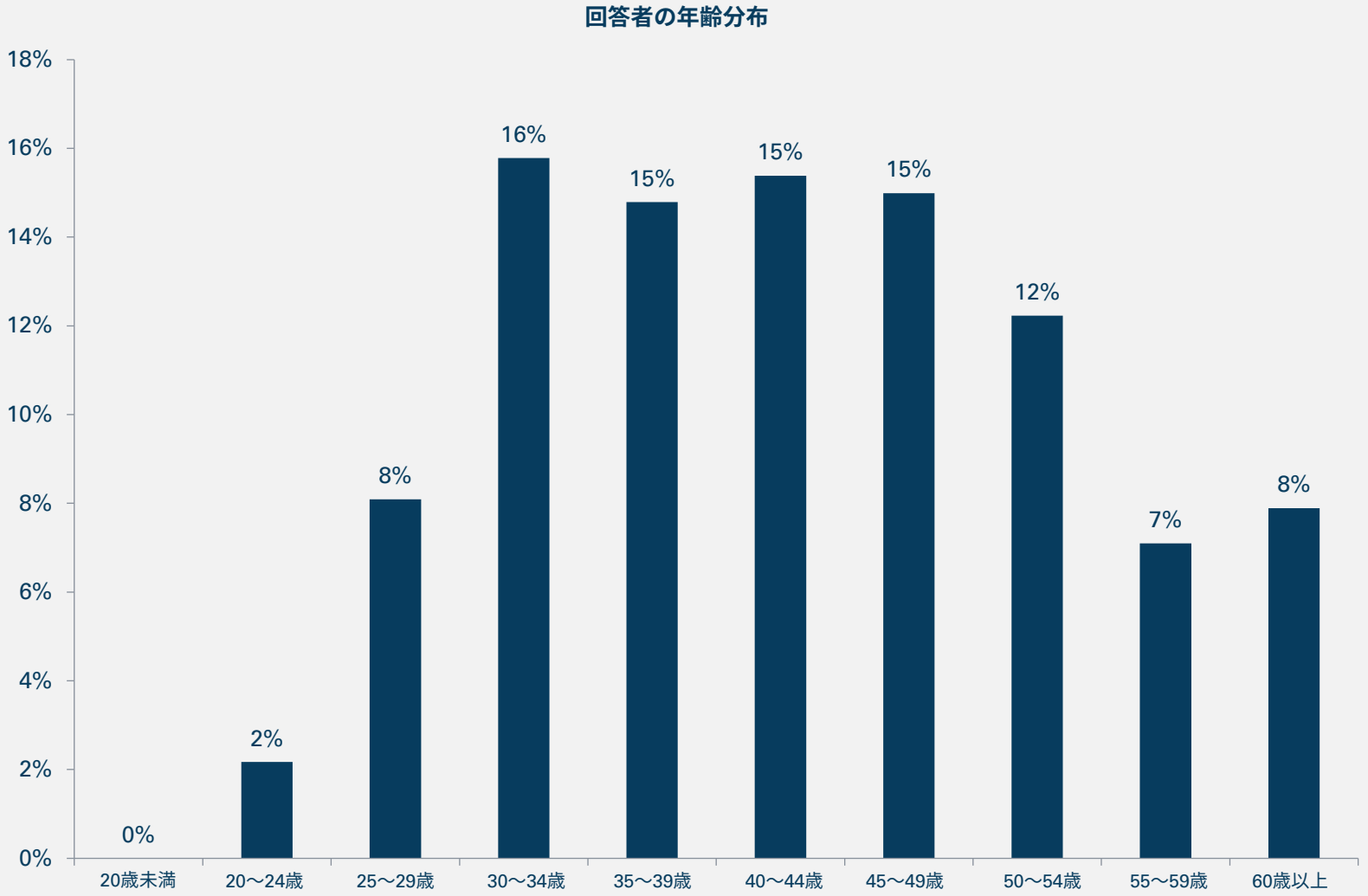
今回はリージョン2、5、7からの回答が増加しました。本調査では、すべての質問で統計的分析に十分な回答数を確保し、担当者、マネージャー、経営層、学生にかかわらずより多くの関係者から(CS)²に関する情報を収集するため、全地域における回答者数の拡大を目指しています。





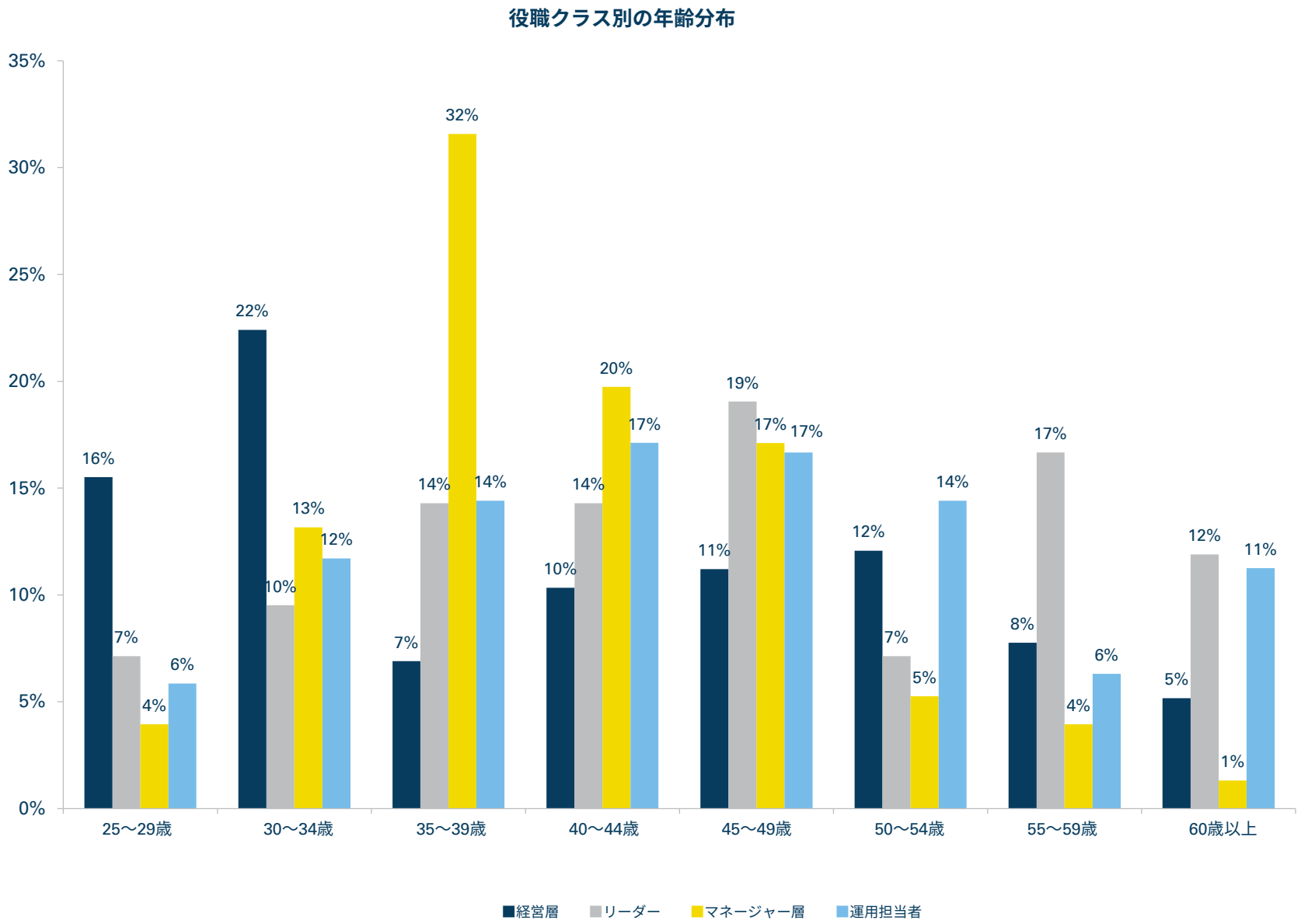
年齢




回答者の年齢分布
18%
16%
14%
12%
10%
8%
6%
4%
2%
0%
0%
2%
8%
16%
15%
15%
15%
12%
7%
8%
20歳未満
20〜24歳
25〜29歳
30〜34歳
35〜39歳
40〜44歳
45〜49歳
50〜54歳
55〜59歳
60歳以上

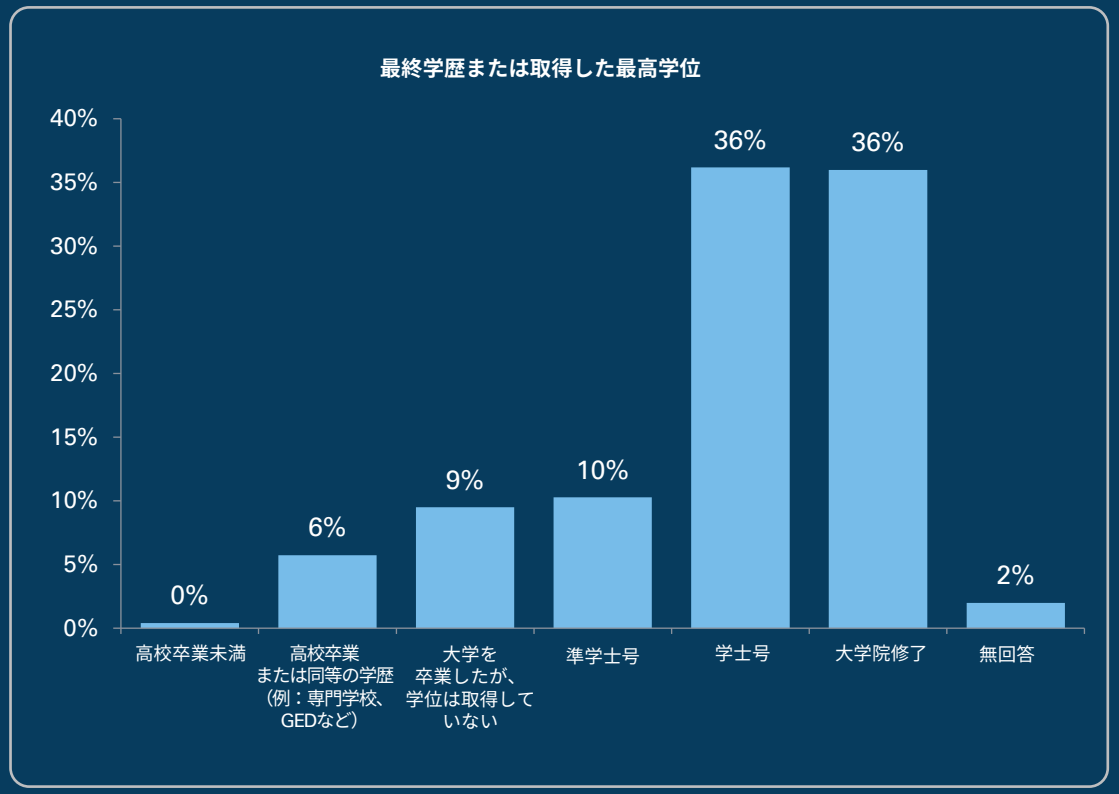
役職クラス別の年齢分布

回答者の大半（60%超）が30〜50歳に位置しています。本調査では運用担当者のグループに重点を置いています。運用担当者は、最も直接的に資産やシステムを利用し、退職すればともに失われてしまう重要な技術的知識や専門性を蓄積しているためです。進化する開発に関する最新の情報を取り入れながら、従業員が蓄積した知識を保持することは、制御システムの維持と改善にとってきわめて重要です。そのため、キャリアの中間地点や前半に位置し、より熟練した人材から学んでいる段階にある回答者の割合が多いことをポジティブに捉えています。



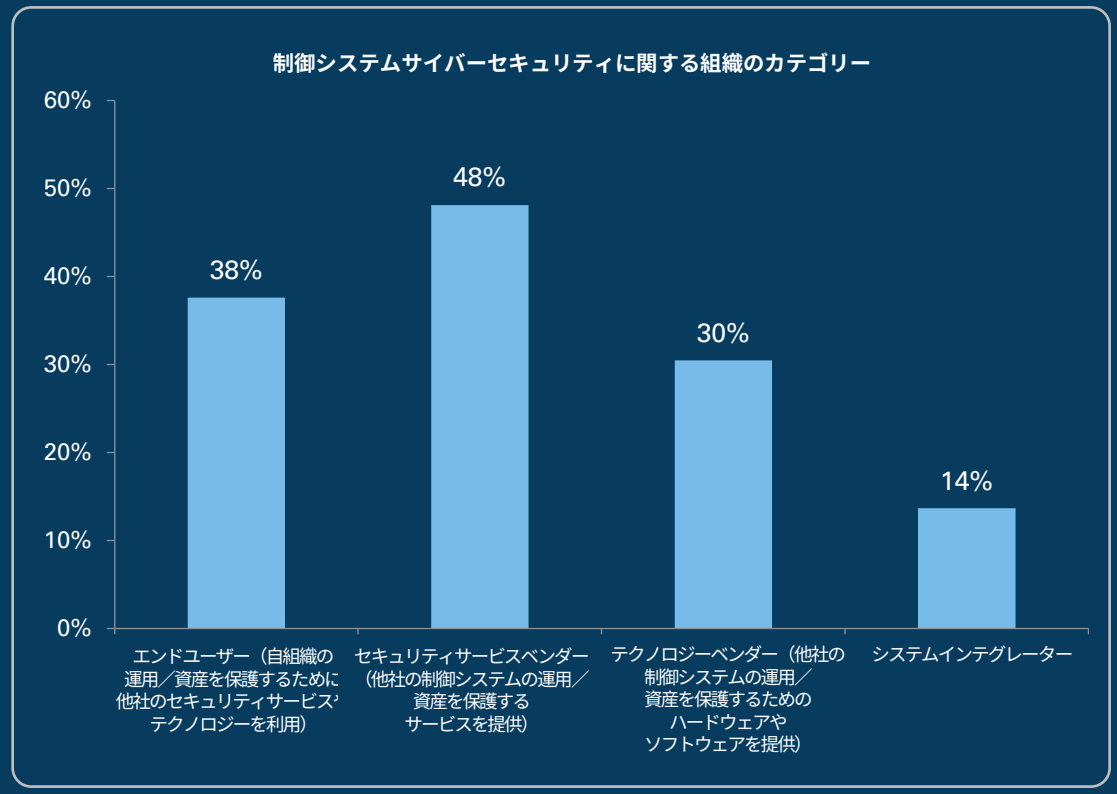
学歴

回答者の学歴は前回と非常に近い水準となっています。



組織カテゴリー

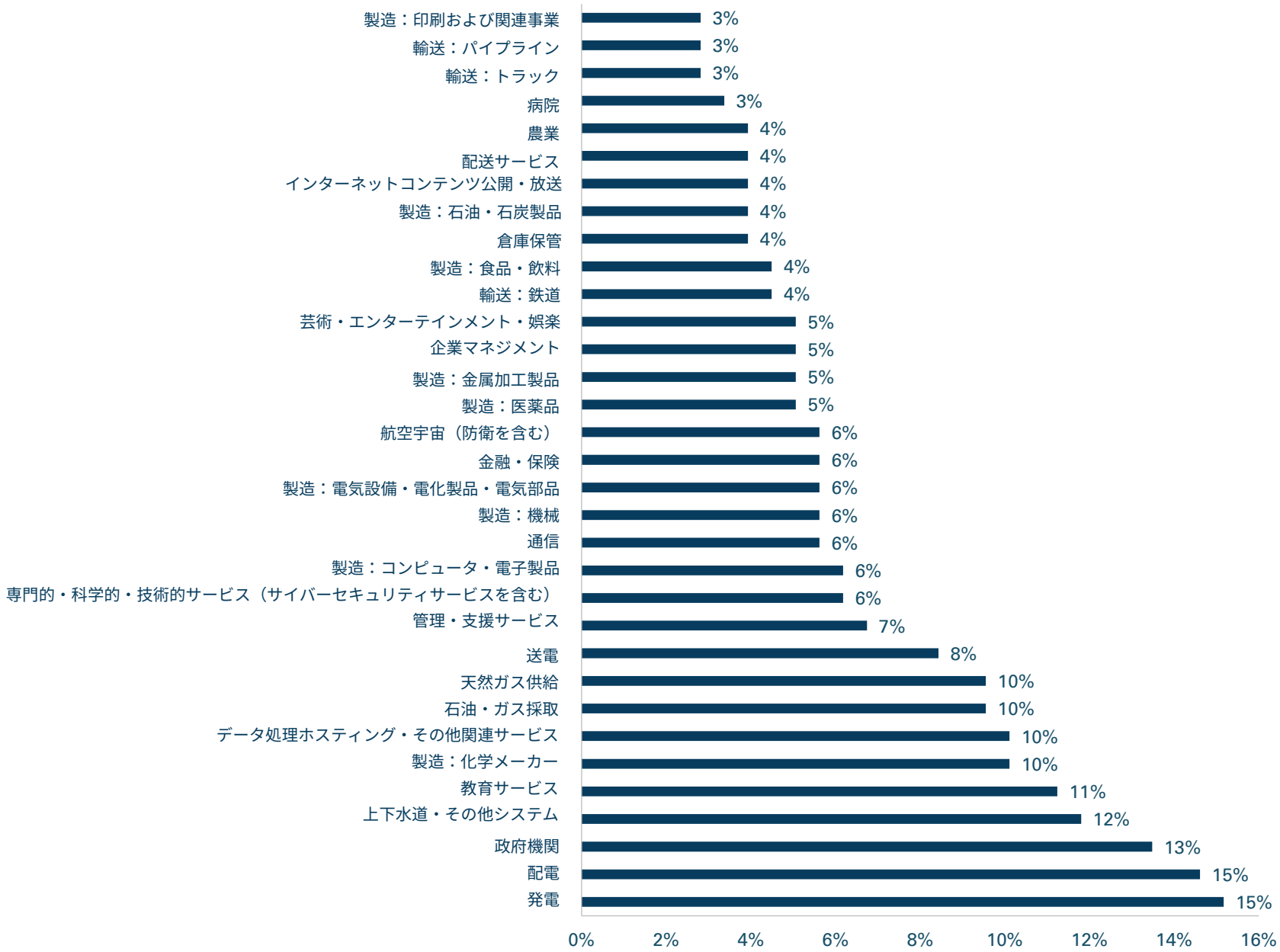
エンドユーザーとテクノロジーベンダーは、ほぼ同様の割合で増減しました（エンドユーザー：10ポイント減、テクノロジーベンダー：19ポイント減。システムインテグレーターは今回新たに追加されたカテゴリーです。複数回答可の質問であるため、回答合計は100%を大きく上回っています。また、今回はその他のカテゴリーを追加し、回答割合は5%でした。



業界別の回答比率（エンドユーザーのみ）

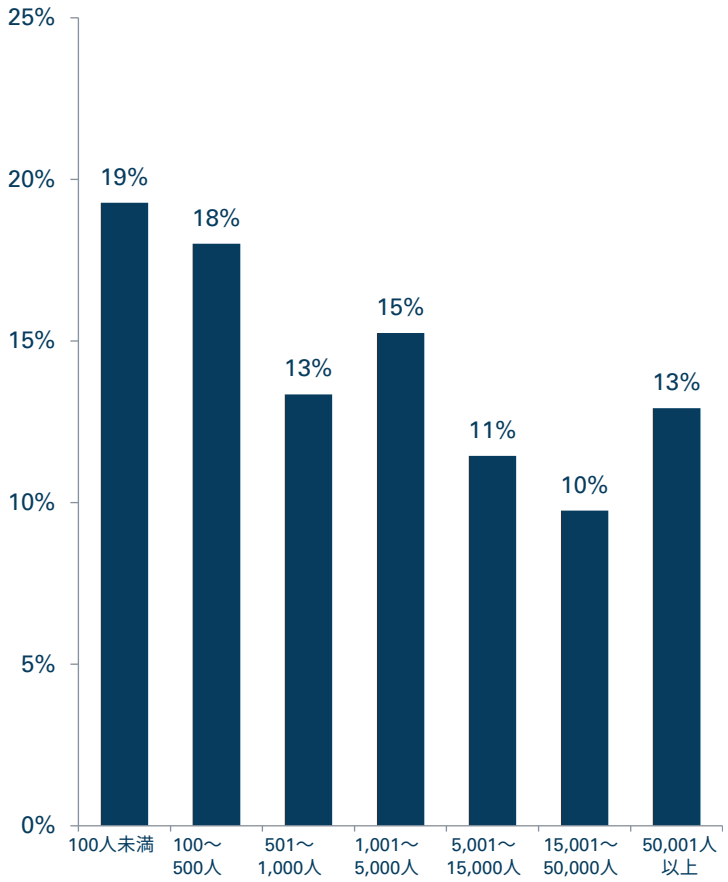
多くの回答者は関連する組織として複数の業界セクターを選択しています。また、可読性のため回答率が3%未満の業界はこの表から削除しています。

回答組織の業界分布



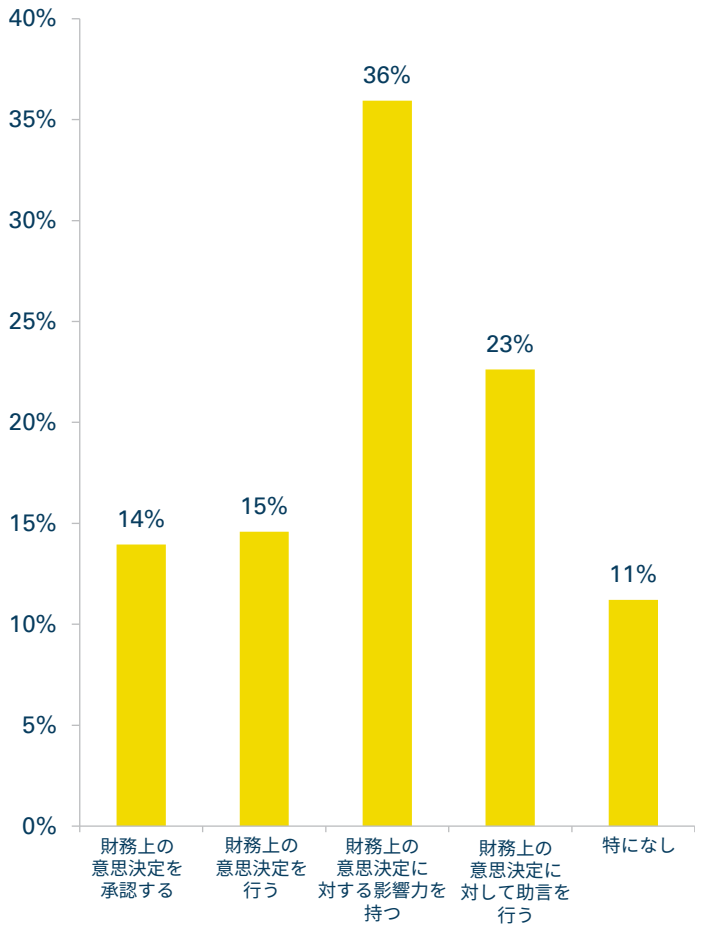
従業員規模

組織の従業員数の規模



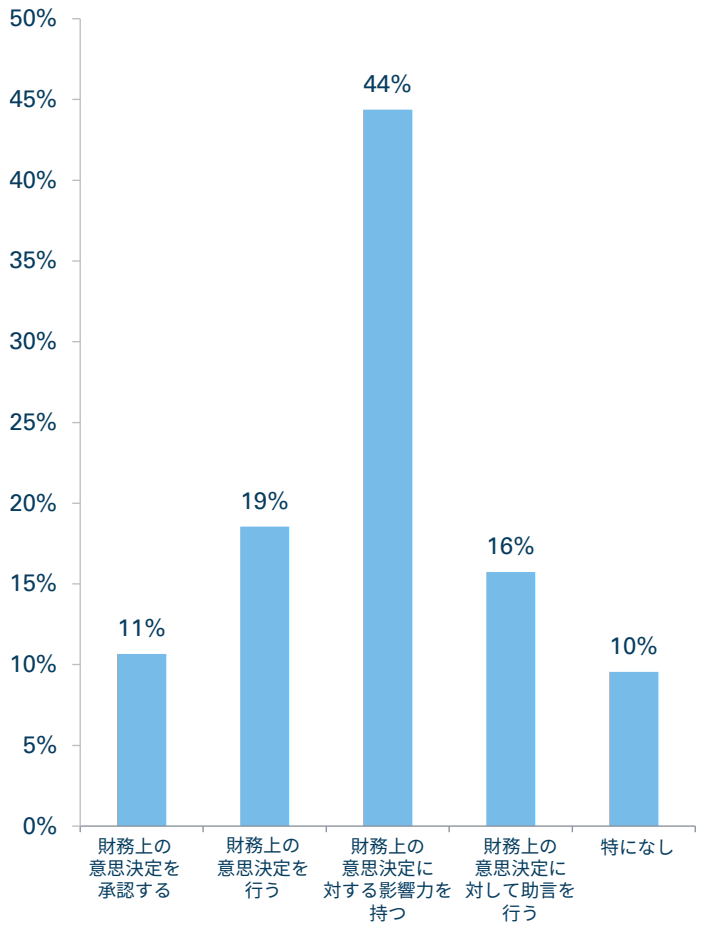
意思決定における役割

制御システムセキュリティ関連支出の意思決定における回答者の役割



意思決定における役割：エンドユーザーのみ

制御システムセキュリティ関連支出の意思決定における回答者の役割（エンドユーザーのみ）



付録B：年次報告書編集委員

Derek Harp氏

(CS)²AI Founder and Chairman
Annual Survey & Report Chair,
Co-Author

Bengt Gregory-Brown氏

(CS)²AI Co-Founder and President
Annual Survey & Report Director,
Lead Designer & Analyst, Co-Author

Walter Risi

(CS)²AI Strategic Alliance Partner Liaison

Survey Design and Report Analysis Teams

Global OT Cybersecurity Leader
KPMGインターナショナル

Partner and Head of Consulting
KPMGアルゼンチン

Andrew Ginter氏

Survey Design and Report Analysis
Teams (CS)²AI Founding Fellow

Author and Lecturer
VP Industrial Security
Waterfall Security Solutions

協力

Ana Girdner VP of Security, Cognite

Brent Huston CEO, MicroSolved

Daryl Haegley Technical Director, Control Systems Cyber Resiliency, US DoD

Mark Bristow Director, CIPIC MITRE

Michael Chipley President, The PMC Group

Rees Machtemes Director of Industrial Security, Waterfall Security Solutions

Rod Locke Director of Product Management, Fortinet

Steve Mustard President & CEO, National Automation

Vivek Ponnada Technology Solutions Director, Nozomi Networks

Anish Mitra, Director, KPMGインド

Hossain Alshedoki, Director, KPMGサウジアラビア

Jayne Goble, Director, KPMG英国

Craig Morris, Director, KPMGオーストラリア

Joshua Turner, Consultant, KPMGジャパン

Brad Raiford, Director, KPMG米国

Pablo Almada, Partner, KPMGアルゼンチン

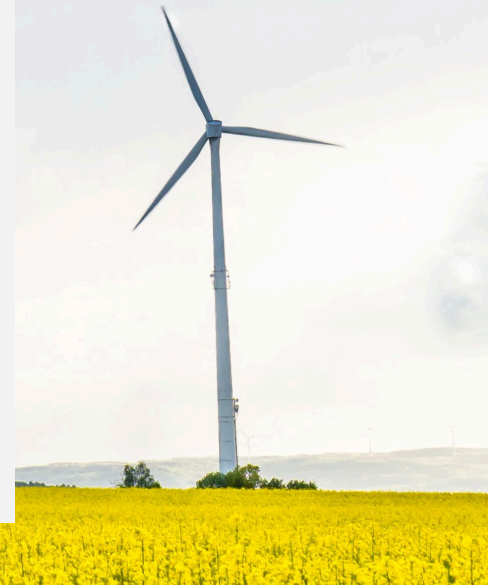
Thomas Gronenwald, Senior Manager, KPMGドイツ

Marko Vogel, Partner, KPMGドイツ

Eddie Toh, Partner, KPMGシンガポール

Sarah Puziewicz Senior Associate, KPMGドイツ

Valentin Steinforth Cybersecurity Consultant, KPMGドイツ



付録C：(CS)²AIについて

ビジョン

制御システムサイバーセキュリティのピアツーピアのネットワーク形成と発展を促進することにより、グローバル規模で重要インフラを強化する。

ミッション

国際組織としてピアツーピア組織を支え、その草の根活動を支援する。

目標

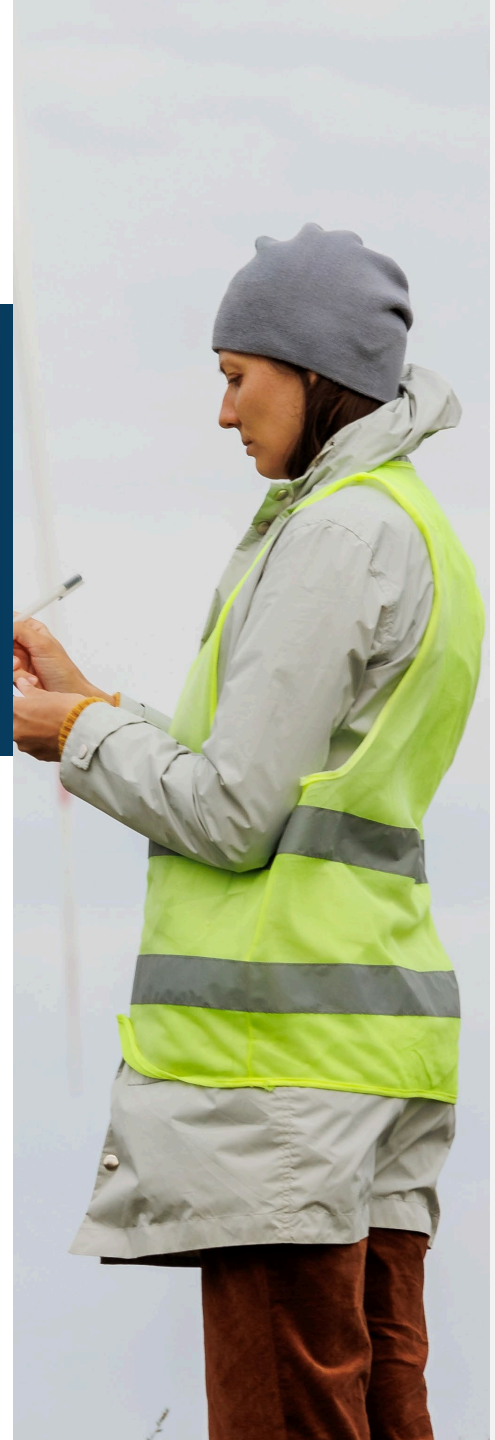
- プロフェッショナルネットワーキング
- コミュニティへの貢献
- グローバルアライアンス
- 主導的役割につく
- プロフェッショナルの育成

(CS)²AIは、急速に成長しているグローバルな非営利団体で、世界中に約34,000人の会員を有し、制御システムの安全確保を担うあらゆるレベルの担当者を支援する非営利人材開発組織です。会員同士が支援し合うためのプラットフォームを提供し、有意義なピアツーピアの交流を促進しています。また、専門的な教育を継続して実施し、あらゆる方法でサイバーセキュリティ担当者の育成を直接的に支援しています。

https://www.cs2ai.org

グローバル規模でのピアツーピアネットワークの形成

(CS)²AIの会員になることで、非常に重要な分野における個人および専門的な能力向上を目指す制御システムサイバーセキュリティ担当者が属する、グローバルコミュニティに参加する機会が得られます。(CS)²AIが提供する、ピアツーピアのつながり、業界をリードする専門家との小グループでの交流、経験・課題・ベストプラクティスの共有、および発達と成長に必要なリソースの活用により、キャリアアップに役立てることができます。



付録D：スポンサー企業

Tier 1 Sponsor

KPMG

Tier 3 Sponsor

Fortinet
Waterfall Security Solutions

Tier 5 Sponsor

Opscura
Network Perception

Tier 6 Sponsor

Bridewell

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/kc

本報告書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。

本報告書は、KPMGインターナショナルと(CS)²AIが2024年4月に共同で発行した「The (CS)²AI - KPMG Control System Cybersecurity Annual Report 2024」を、KPMGインターナショナルおよび(CS)²AIの許可を得て翻訳したものです。
翻訳と英語原文間に齟齬がある場合は、当該英語原文が優先するものとします。

文中の社名、商品名等は各社の商標または登録商標である場合があります。本文中では、Copyright、TM、Rマーク等は省略しています。

ここに記載されている情報はあくまで一般的なものであり、特定の個人や組織が置かれている状況に対応するものではありません。私たちは、的確な情報をタイムリーに提供するよう努 めておりますが、情報を受け取られた時点及びそれ以降においての正確さは保証の限りではありません。何らかの行動を取られる場合は、ここにある情報のみを根拠とせず、プロフェッ ショナルが特定の状況を綿密に調査した上で提案する適切なアドバイスをもとにご判断ください。

KPMGは、グローバル組織、またはKPMG International Limited（「KPMGインターナショナル」）の1つ以上のメンバーファームを指し、それぞれが別個の法人です。 KPMG International Limitedは英国の保証有限責任会社（private English company limited by guarantee）です。KPMG International Limitedおよびその関連事業体は、クライアントに対していかなるサービスも提供していません。KPMGの組織体制の詳細については、kpmg.com/governanceをご覧ください。

© 2024 Control System Cybersecurity Association International, a.k.a. (CS)²AI. (CS)²AI is a 501(c)6 nonprofit organization registered in the United States of America

© 2024 KPMG Consulting Co., Ltd., a company established under the Japan Companies Act and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. C24-1038

The Control System Cybersecurity Association International, a.k.a. (CS)²AI names and logo are registered trademarks.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

CREATE: CRT152075