(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

会長メッセージ

親愛なる皆様へ

本年もまた、異例とも言える1年が過ぎました。我々は皆、世界共通の重要課題に直面しており、それはサイバーセキュリティに限ったことではありませんが、現代の「常時接続社会」の安全を確保するため、依然として取り組むべきことが山積しています。

この場をお借りして、「(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」をご紹介させていただきます。本報告書は、我々の戦略的提携パートナーであるKPMGの多大なご尽力によって実現したもので、心から感謝いたします。また、調査から最終報告に至るまで重要な貢献をしてくださったFortinet社、Waterfall Security Solutions社、その他多くのスポンサー企業様（57ページを参照）、年次報告書運営委員会（54～55ページ）にも謝意を表します。この共同プロジェクトを支援している企業や個人は、「制御システムサイバーセキュリティ担当者が抱える課題を解決する」というミッションに貢献し続けています。

本報告書は、580人以上の業界関係者、および(CS)^{2}AIの世界各国の会員（約25,000人）を対象に、制御システムのセキュリティインシデント、サイバー攻撃や防御対策の傾向、この課題を対処するために組織が優先して取り組んでいることに関する質問を行った結果に基づくものです。

我々の多くは「すべてを実施する」ことはできず、どこに重点を置くか、賢明な判断が必要となります。本報告書を、同業他社の活動をより明確に把握し、難しい決断を下す際のツールとして活用いただけましたら幸いです。

Derek Harp氏
Founder & Chairman
(CS)^{2}AI

序文

産業界におけるサイバーセキュリティには引き続き大きな課題があります。脅威の頻度と精巧さが増すにつれ、企業はリソースと専門知識を動員し、大胆かつ斬新な方法で組織を保護する必要があります。

「コロニアル・パイプライン」、「オールズマーの水道施設」、「JBSフーズのランサムウェア事件」など、新聞の見出しをにぎわすようなインシデントが各国で相次ぎ、運用技術（OT）サイバーセキュリティにとって憂慮すべき状況が続いています。

このような状況を受け、多くの企業が重要な事業運営と俊敏性を維持しながら、必要な投資、人材、技術を最重要課題に充てるため、OT環境の見直しを急いでいます。OTセキュリティの強化においては特に、機密性の高いOT環境や、産業界のターゲットを混乱させる可能性があるランサムウェアの脅威に焦点を当てる必要があります。

ランサムウェアなどのサイバー脅威が勢いを増す一方、企業は「国家」による事件や脅威の可能性にも目を向けています。本調査の回答者は、制御システムのセキュリティ侵害において最も一般的な脅威要因として「内部関係者の過失」を挙げていますが、国家による攻撃も重要な懸念事項と言えるでしょう。

こうした不穏な動向を受け、より多くの企業が、執拗かつ攻撃的な昨今の敵対者に対抗するため、OTサイバーセキュリティへの新たな投資を検討するようになりました。ただ、往々にして、OTインフラ保護のための投資には予算の制約があることも事実です。

制御システムのセキュリティ予算については、2020年は「30%以上増加」との回答が最も多かったことに比べ、2021年は「10%以上の増加」が最多となり、増加率は低下しています。一方、約10%の企業で実際に予算が減少しており、前年度の約1%から、その割合は増えています。

また、制御システムサイバーセキュリティの確たる進展にあたり、ハードルとなっているのは、専門知識の不足であることが、今回の調査で明らかになりました。回答者の約半数（49.1%）が、制御システムへのサイバー攻撃を防ぐうえでの最大のハードルとして「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」を挙げ、さらに3分の1超が「人材不足」を挙げています。

サードパーティアウトソーシングの傾向が強まるなか、トレーニングへの十分な投資も不足しています。新型コロナウイルス感染症（COVID-19）の世界的なパンデミックによる労働力不足の影響で、サービス企業が人材・スキル不足に苦慮していることもあり、解決策は限定的です。企業は、限られた社内の専門知識とアウトソーシングされた人材を組み合わせて対応していますが、たとえば現在のOTサイバーセキュリティのニーズの複雑さに適切に対応したSOCサービス（セキュリティ監視サービス）はほとんどなく、OT分野ではマネージドサービスがまだ確実ではないことに注意が必要です。

こうした状況において、社内トレーニングの必要性が大幅に高まっています。この分野への投資が全体的に不足するなか、一部の企業は実際に成果を上げており、さまざまなトレーニング法が採用されていることは朗報と言えるでしょう。制御システムのセキュリティに対する成熟度が低い組織（以降、低成熟度組織）は、依然として従来のコンピュータベースやインストラクター主導のプログラムに依存していますが、成熟度の高い組織（以降、高成熟度組織）は、「ライブ」のテーブルトップインシデントシミュレーション演習に注目しています。これにより、OTセキュリティを理解できるようになるだけでなく、脅威が拡大する昨今の状況に対応するための準備がどの程度整っているかを把握できます。

この傾向は、「セキュリティ意識向上トレーニング」の重要性を物語っています。これはセキュリティ担当者のスキルや能力を開発するセキュリティ研修とは異なり、組織全体のセキュリティ文化の醸成を目的とするもので、理想を言えば、すべての従業員がセキュリティリスクの軽減における自らの役割を認識できるようになることを目指します。ただ、進展がみられる一方、依然として、約2割（17.4%）の組織で制御システムセキュリティ意識向上トレーニングが実施されていません。これは知識のない従業員が危険な電子メールのリンクをクリックするという、単純なミスにつながりかねず、「内部関係者の過失」によるインシデントの脅威が増している状況を考慮すると憂慮すべきことです。

セキュリティ計画の現状については、約85%の組織が「管理／対応計画を何らかの段階まで進めている」と回答していることは心強い結果です。「計画を実行もしくはテスト済み」との回答は依然として低いものの、18～27%が計画すら立てていなかった2020年と比較すると、大幅な改善と言えます。

最新の包括的な調査が示すように、脅威が拡大し、変化のスピードが加速している今日の危険な環境では、まだ多くの課題が残っています。このような状況下では「危機意識」を高めることが不可欠で、高度なスキルを持つOTセキュリティ担当者の重要性は強調してもしきれないほどです。確たる進展には、コスト、システムの可用性、増大する脅威に立ち向かうための最新の対策を管理する戦略的なバランスが肝要で、時間を無駄にする猶予は残されていません。

Walter Risi
Global Cyber IoT Leader
KPMGアルゼンチン

目次

エグゼクティブサマリー

本報告書は、Control System Cyber Security Association International ((CS)^{2}AI) とその会員および、戦略的提携パートナー (SAPs) のコミュニティによる継続的な調査から得られた、年次プロジェクトシリーズの最新版です。(CS)^{2}AI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氏が主導する、数十年にわたる制御システム (CS) セキュリティ調査の開発、調査、分析に基づいて、約25,000人の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約600人が回答し、さらにその他多くの方々から定期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。

組織内の政治力学やベンダーの影響を排除するために匿名による調査を行い、CS/OTの運用と資産に関与する個人と組織が直面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。

プロジェクトの目的

(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の運営委員会は、エンドユーザーやベンダー、リーダーや運用担当者など、この仕事に関与するすべての人に有益な判断材料を毎年展開することを目的とし、2021年第1四半期にプロジェクトを開始しました。

データ収集のため、制御システムサイバーセキュリティに積極的に関与している関係者を対象に、幅広いネットワークおよびダイレクトチャネルを通じ、調査への参加を呼びかけました。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、さまざまな組織レベルの関係者が含まれています。

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)」としています。CSまたは (CS) 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、労働力を指します。

主なハイライト

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が高い（「高成熟度」）と認識する組織は、「低成熟度」と認識する組織と比べ、多くの点で勝っていました。特に注目すべき回答は以下のとおりです。

- 制御システム製品／サービスの導入前リスクアセスメントにIEC62443-4-1の準拠を確認するとの回答が2倍近い（高成熟度組織：**34.8%**、低成熟度組織：**17.6%**）。
- 制御システムサイバーセキュリティサービスはCISO/CSO/CTO配下の社内セキュリティチームから提供されているとの回答が2倍以上（高成熟度組織：**49.3%**、低成熟度組織：**21.4%**）。
- 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との回答が4倍近い（高成熟度組織：**44.3%**、低成熟度組織：**12.8%**）。
- すべての制御システムのネットワーク稼働状況の監視をすでに実施しているとの回答（高成熟度組織：**35.7%**、低成熟度組織：**13.0%**）、および今後18 ヵ月以内に監視の頻度を増やす予定との回答（高成熟度組織：**17.1%**、低成熟度組織：**6.5%**）が3倍近い。
- ネットワーク上のすべてのデバイス、アプリケーション、ユーザーを継続的に監視しているとの回答が2倍以上（高成熟度組織：**27.5%**、低成熟度組織：**12.5%**）。

＊「高成熟度組織」「低成熟度組織」の定義についてはp8を参照

調査方法

(CS)²AI-KPMG 制御システムサイバーセキュリティ調査と報告書の作成は、以下の団体の協力で実施されました。

- **(CS)²AI**：プロジェクトの発案者として、成果物である本報告書の執筆・作成をはじめ、プロジェクトの開発、指導、実施において主要な役割を担う。
- **KPMG**：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、人材、組織の面で主要なサポートを提供。
- **その他スポンサー**：可能な限り追加の資金や人的・組織面でのリソースを提供。（付録D：スポンサー企業を参照）

(CS)²AIとプロジェクトスポンサーは、前章のプロジェクト目的に従って、2021年の第2四半期と第3四半期に、現場で働くCS/OTのメンバーを対象に複数の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[1]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、さまざまなソーシャルメディアチャネルを通じた調査票の配布や、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検討することが、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。組織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の成熟度が最も重要な要素であるという観点から、調査項目の1つとして、自組織に当てはまるレベルを選択するよう依頼しました。

＊本報告書は、2022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「Control System Cyber Security Annual Report 2022」を翻訳したものです。

＊本報告書では、少数点第2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。

1 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。

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、「プログラム」で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＞

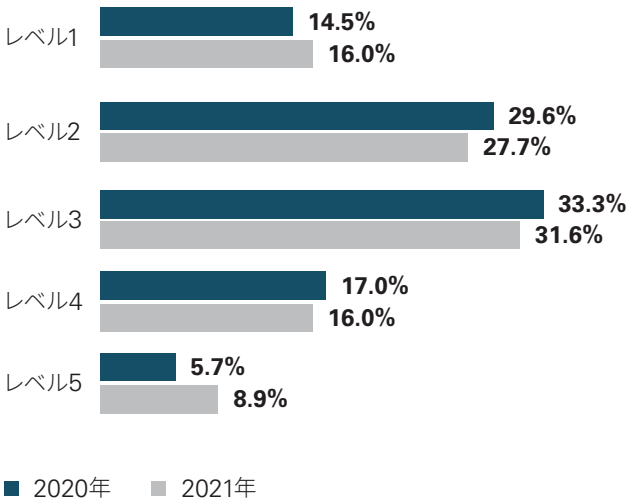
レベル2 ― サイバーセキュリティの実装において、基本的なプロジェクトマネジメントが実施されています。知識体系が構築されつつあり、ベストプラクティスが実行されているものの、アドホックの可能性があります。＜消極的なディフェンス＞

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でリードされ、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。＜積極的なディフェンス：最適化、自動化、統合化、予測可能＞

自組織の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



レベル1、レベル2の組織を「低成熟度組織」、レベル4、レベル5の組織を「高成熟度組織」と定義します。これら2つの組織の回答は、すべての質問で大きな差がみられたわけではありませんが、違いが表れた質問についてはグラフで示しています。

また、調査を毎年実施することで年ごとの傾向や変化を調べることができ、データの縦断的な検証が可能となります。質問の修正・改良をすると、直接的な比較が難しくなることもありますが、年ごとのデータセット間に興味深い差異がみつかった場合には特記しています。

“サイバーセキュリティプログラムの成熟度に関するデータセットの回答分布は、Industrial Defender社の認識と一致しています。取引先の社内規定や業界規制によって標準規格を選択した業界は、サイバーセキュリティプログラムのレベル3に分類される傾向があります。残念ながら、水やガス産業は、資金や規制監督が不十分なため、一般的にレベル1やレベル2に分類されがちです。”

George Kalavantis氏
COO
Industrial Defender

調査結果

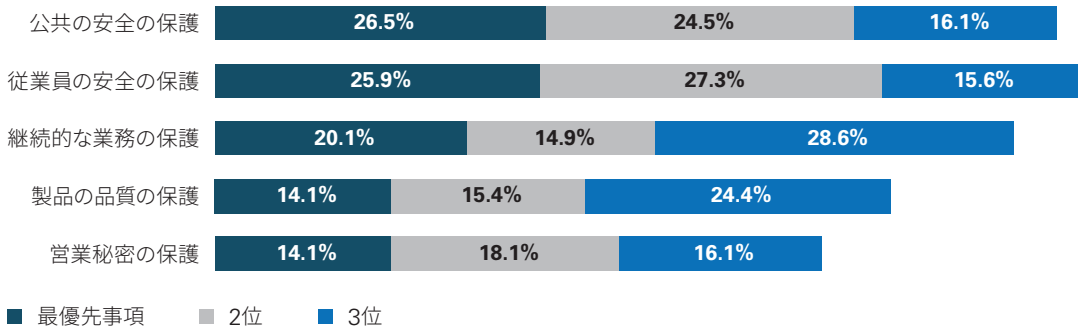
最優先事項

本調査の意思決定ツールとしての有用性を高めるため、前回調査より多肢選択質問を多く組み込みました。また、特にエンドユーザーからの回答は、セキュリティ技術やサービスのベンダーからの回答とは別に分析しました。多くの質問で、両者の回答は非常に類似していることがわかりましたが、大きな相違がみられた質問については、エンドユーザーの回答を具体的に紹介しています。

制御システムサイバーセキュリティに関する組織の最優先事項が、その1つです。下記のすべての選択肢が、さまざまなエンドユーザーから選ばれており、従業員と公共の安全保護を重視していることは明らかです。

OTセキュリティの検討において、安全性は常に重要な位置を占めているため、年次報告書運営委員会のメンバーのなかには、安全性がはるかに高い順位にならなかったことに驚きを示す人もいました。よくあることですが、なぜ回答者がこのような回答をしたのかという根本的な疑問は完全には明らかにされません。多くの安全計装システムがサイバー脅威にさらされているという十分な証拠や、サイバー攻撃の有名な事例[2]があるにもかかわらず、多くの人が自組織がサイバー脅威にさらされているとは考えていないことが原因かもしれません。

制御システムサイバーセキュリティに関して、自組織が重視している事項を順位付けしてください（エンドユーザーの回答）



> 重要なインフラが日々ハッキングされるなか、安全かつ継続的な運用に関する懸念がIT関係者の間で高まっているのは当然のことです。ファイアウォールの追加など、過去に有効だったネットワークソリューションが、もはや効果がないことがわかります。ゼロトラストやセキュアリモートアクセスなどのサイバーセキュリティソリューションにより、サイバー攻撃を受ける対象資産を減らし、組織への財務的な悪影響を軽減する必要性が高まっています。

Keith Beeman氏
CEO
Tempered Networks

2 https://www.technologyreview.com/2019/03/05/103328/cybersecurity-critical-infrastructure-triton-malware/

重要業績評価指標（KPI）

組織がサイバーセキュリティプログラムのパフォーマンスをモニタリングするために使用する指標には、組織の優先事項、成熟度、過去のインシデント経験、現在のセキュリティ体制に関する重要な情報が含まれていることがあります。たとえば、右のグラフをみると、高成熟度組織は低成熟度組織よりも多くの重要業績評価指標（KPI）を設定しており、約2倍の頻度でKPIをモニタリングしています（例：「セキュリティインシデント数の削減」をKPIとして設定しているとの回答が、高成熟度組織：50.7%、低成熟度組織：25.6%）。また、「KPIをまったく設定していない」との回答が、低成熟度組織は2倍以上も高い結果となりました（高成熟度組織：4.2%、低成熟度組織：10.4%）。さらに、高成熟度組織は、セキュリティ情勢をよく見据えたうえで、より意味のある指標を算出しKPIを設定しているため、一貫したモニタリングが可能となっています。

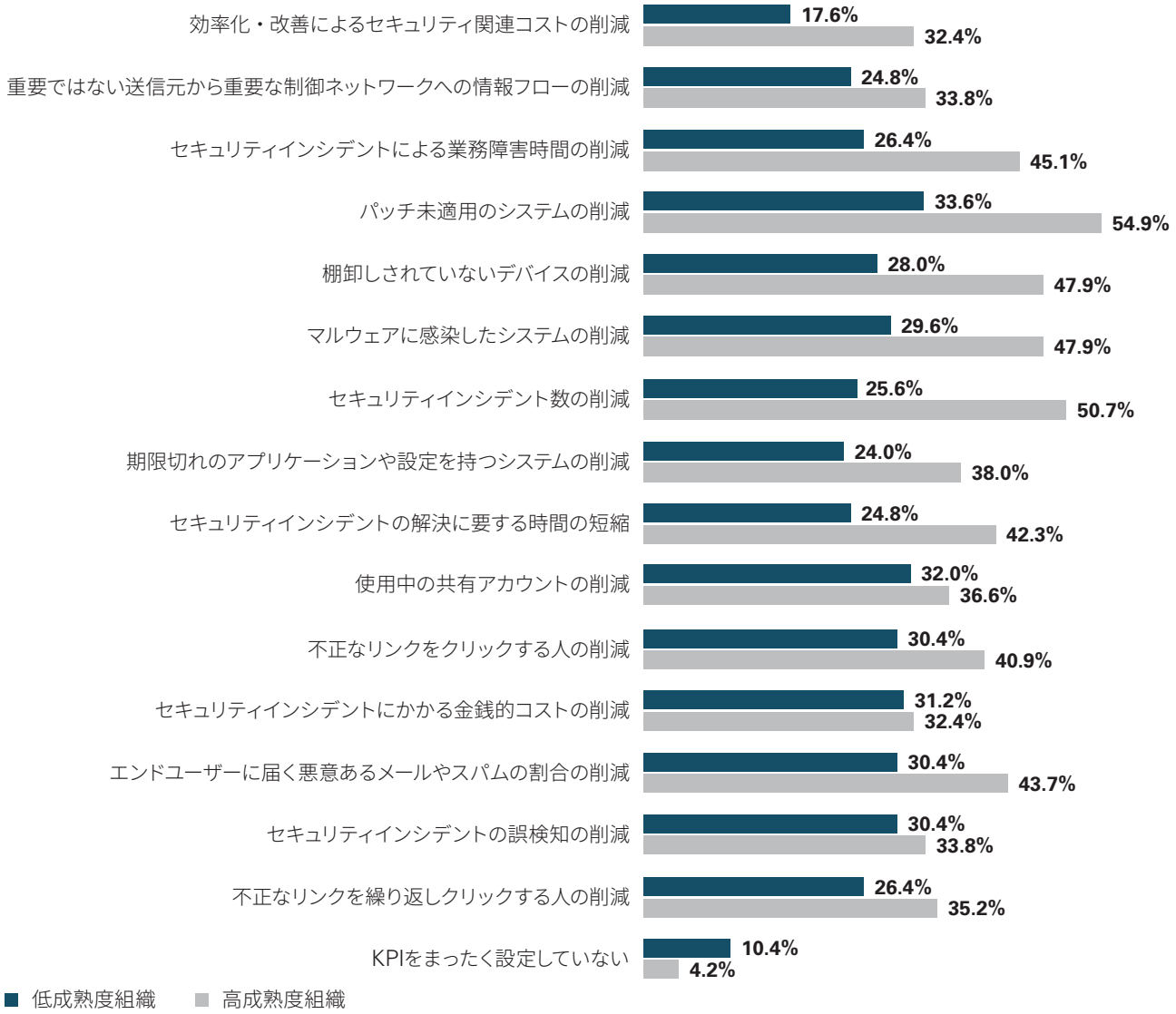
高成熟度、低成熟度の両グループが同じレベルに達しているのは、「使用中の共有アカウントの削減」、「セキュリティインシデントにかかる金銭的コストの削減」、「セキュリティインシデントの誤検知の削減」の3指標のみです。セキュリティプログラムの成熟度は、回答組織の規模に関係なく均等に分布していますが、次ページのグラフに示されるように、大規模組織は小規模組織よりも多くのKPIを設定していることがわかりました。KPIの設定状況について、16の選択肢のうち11の項目に組織規模の違いによる明確な差がみられます。

本調査では、いくつかの質問において、回答者の分類（成熟度別／組織規模別）によって結果に差があるかどうかを調べました。

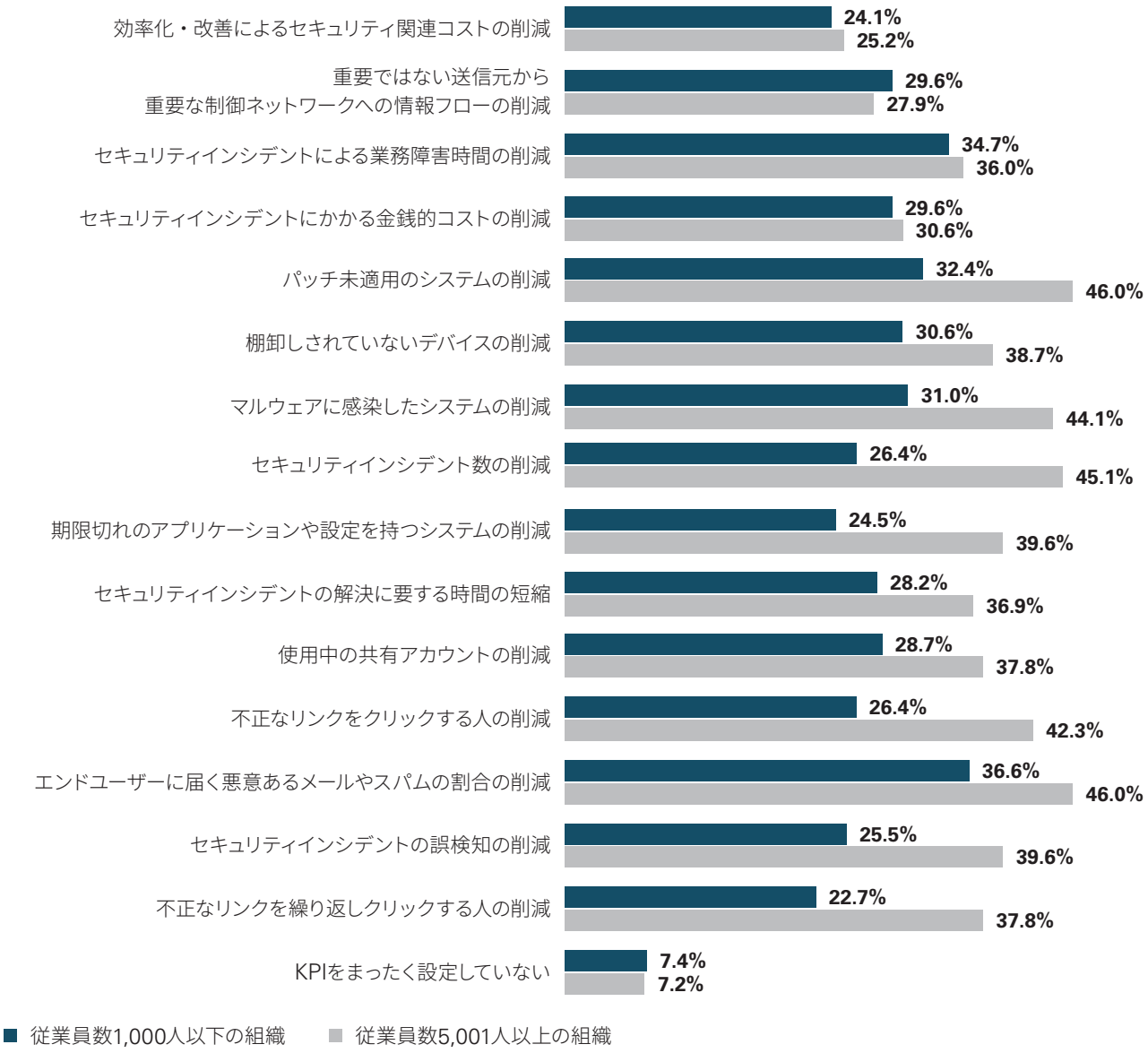
統計的に有用な相関性がみられた場合は、グラフに「ρ」という記号をつけています。

ρ

自組織で設定しているセキュリティプログラムのKPIをすべて教えてください（高成熟度組織と低成熟度組織の比較）



自組織で設定しているセキュリティプログラムのKPIをすべて教えてください（大規模組織と小規模組織の比較）



これらの指標の多くは、互いに影響し合い、好循環を生み出します。パッチ未適用のシステムや期限切れのアプリケーションなどの削減に積極的な組織は、ランサムウェア攻撃の発生を抑制し、より迅速に解決することができます。

ユーザーの行動についても同様のことが言えます。トレーニングやサイバー演習（フィッシングなど）の結果を追跡している組織は、おそらく不正なリンクをクリック（1回または複数回）する人の数やソーシャルエンジニアリングの攻撃ベクトルに起因するインシデントの発生頻度が低い傾向がみられるでしょう。

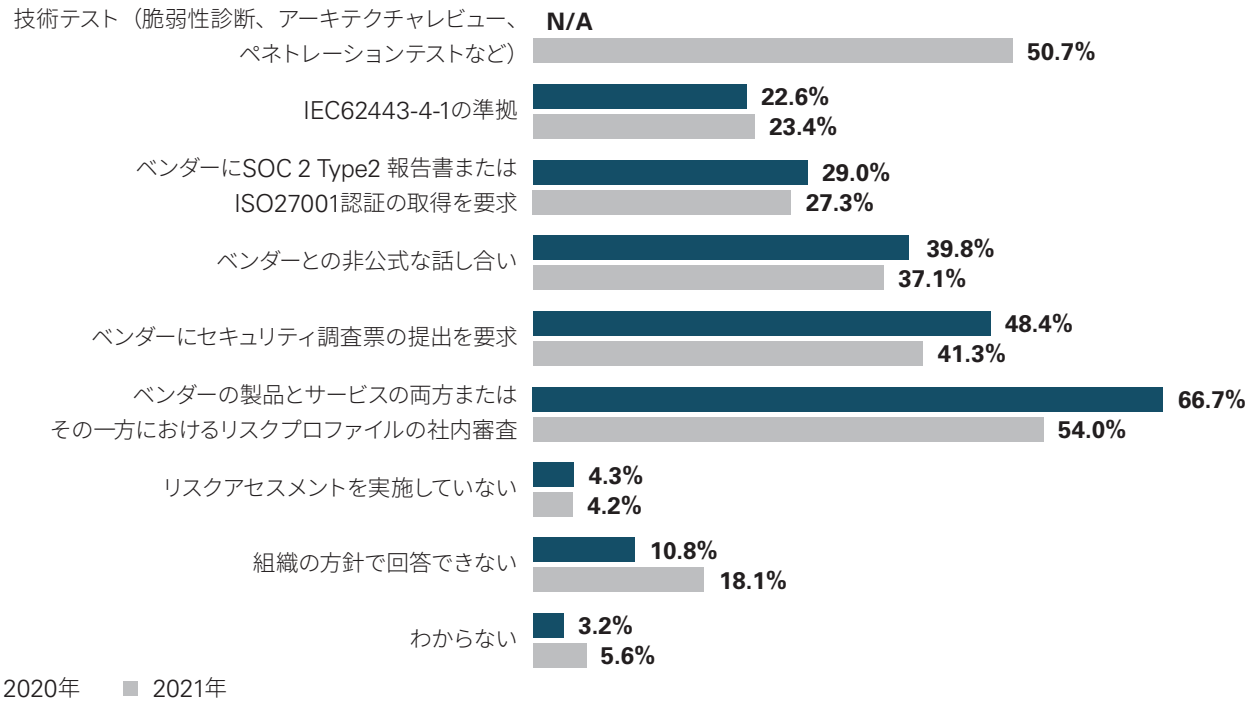
Brad Raiford
Director, Cyber Security
KPMG米国

導入前のリスクアセスメント

「ベンダーの製品とサービスの両方または一方におけるリスクプロファイルの社内審査」は、依然として制御システム所有者のためのリスクアセスメントとして最も利用されています（2021年：54.0%、2020年：66.7%）。今回の調査では、「技術テスト」を新たな選択肢として追加しましたが、回答組織の少なくとも半数（50.7%）が実施していると回答したことは心強い結果です。このうち、約7割の組織（69.2%）は、ベンダーの製品とサービスの両方またはその一方におけるリスクプロファイルの社内審査も実施しており、50.6%は、ベンダーにセキュリティ調査票の提出を求めています。多くの制御システムで潜在的な影響があるため、リスクを測定し管理するために複数のアプローチを使用することが推奨されます。

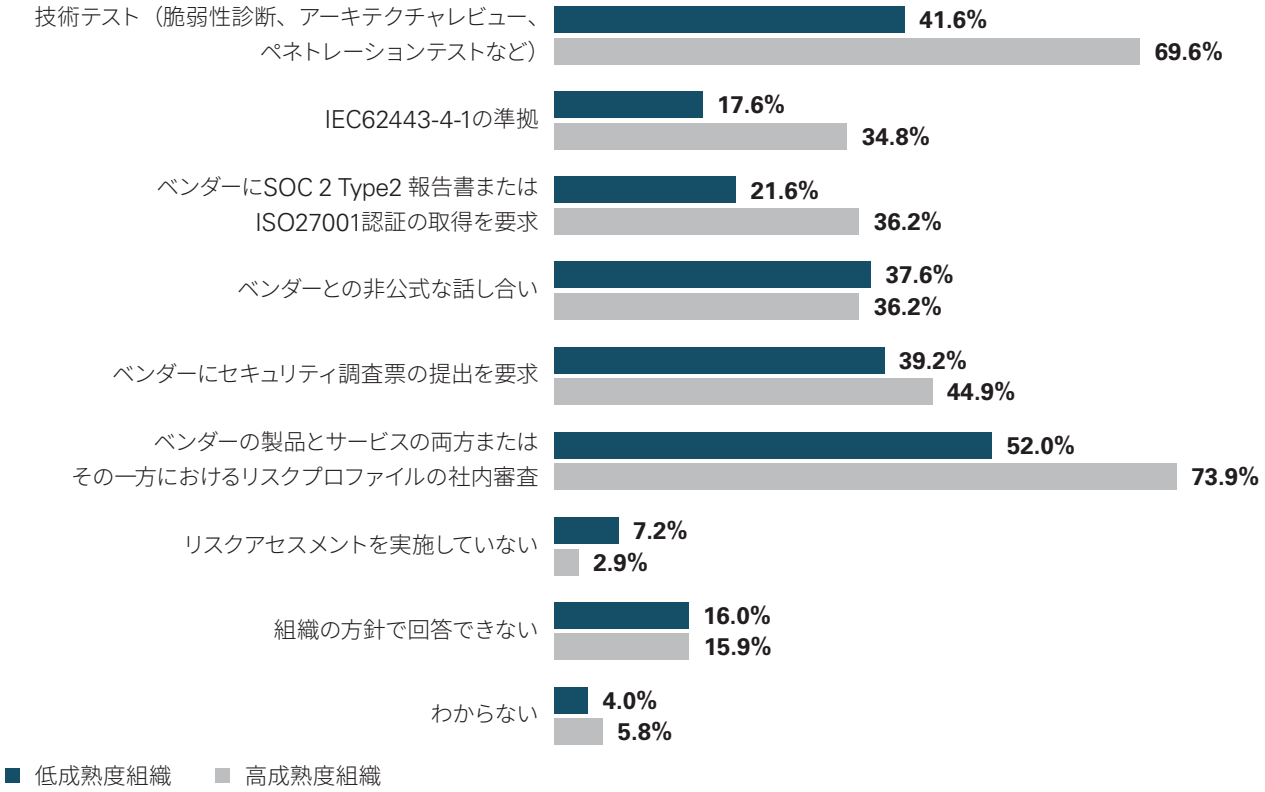
高成熟度組織と低成熟度組織の比較で特に注目すべきは、技術テスト（高成熟度組織：69.6%、低成熟度組織：41.6%）」と、「IEC62443-4-1の準拠（高成熟度組織：34.8%、低成熟度組織：17.6%）に大きな違いがみられる点です。また、「ベンダーの製品とサービスの両方またはその一方におけるリスクプロファイルの社内審査」の実施についても大幅な差が表れています（高成熟度組織：73.9%、低成熟度組織：52.0%）。

制御システム製品またはサービスを導入する前に、自組織で実施しているリスクアセスメントをすべて教えてください（2020年と2021年の比較）



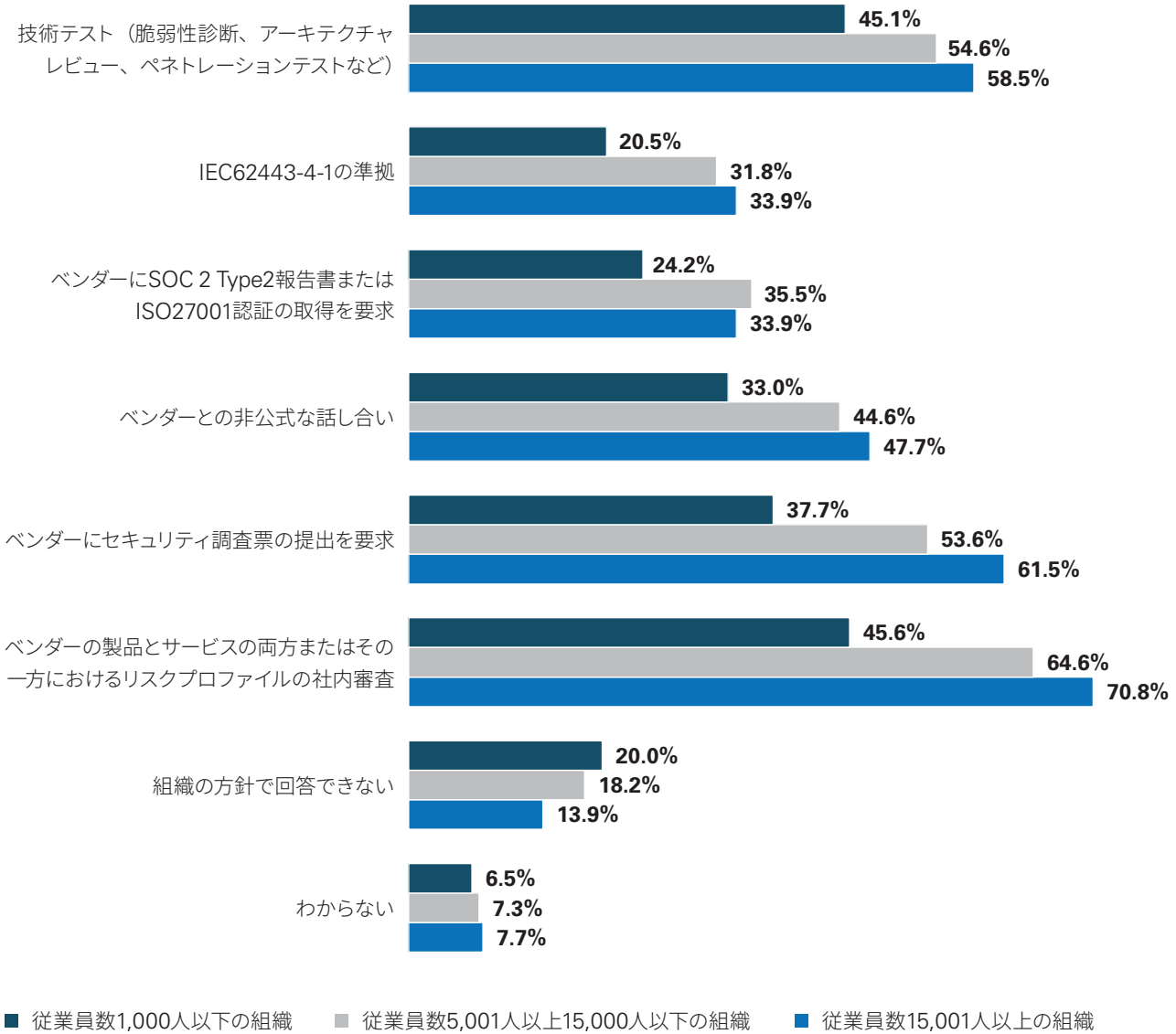
回答組織の規模の違い（従業員数で定義）も、制御システム製品またはサービスを導入する前に実施するリスクアセスメントに明らかな影響を及ぼしています。サイバーセキュリティプログラムの成熟度を考慮しても、大規模組織ほど、あらゆる種類のリスクアセスメントを実施していることがわかります。おそらく、より多くのリソースを持つ大規模組織は、リスク管理の側面において徹底した方法を選択でき、実行していると考えられます。

制御システム製品またはサービスを導入する前に、自組織で実施しているリスクアセスメントをすべて教えてください（高成熟度組織と低成熟度組織の比較）

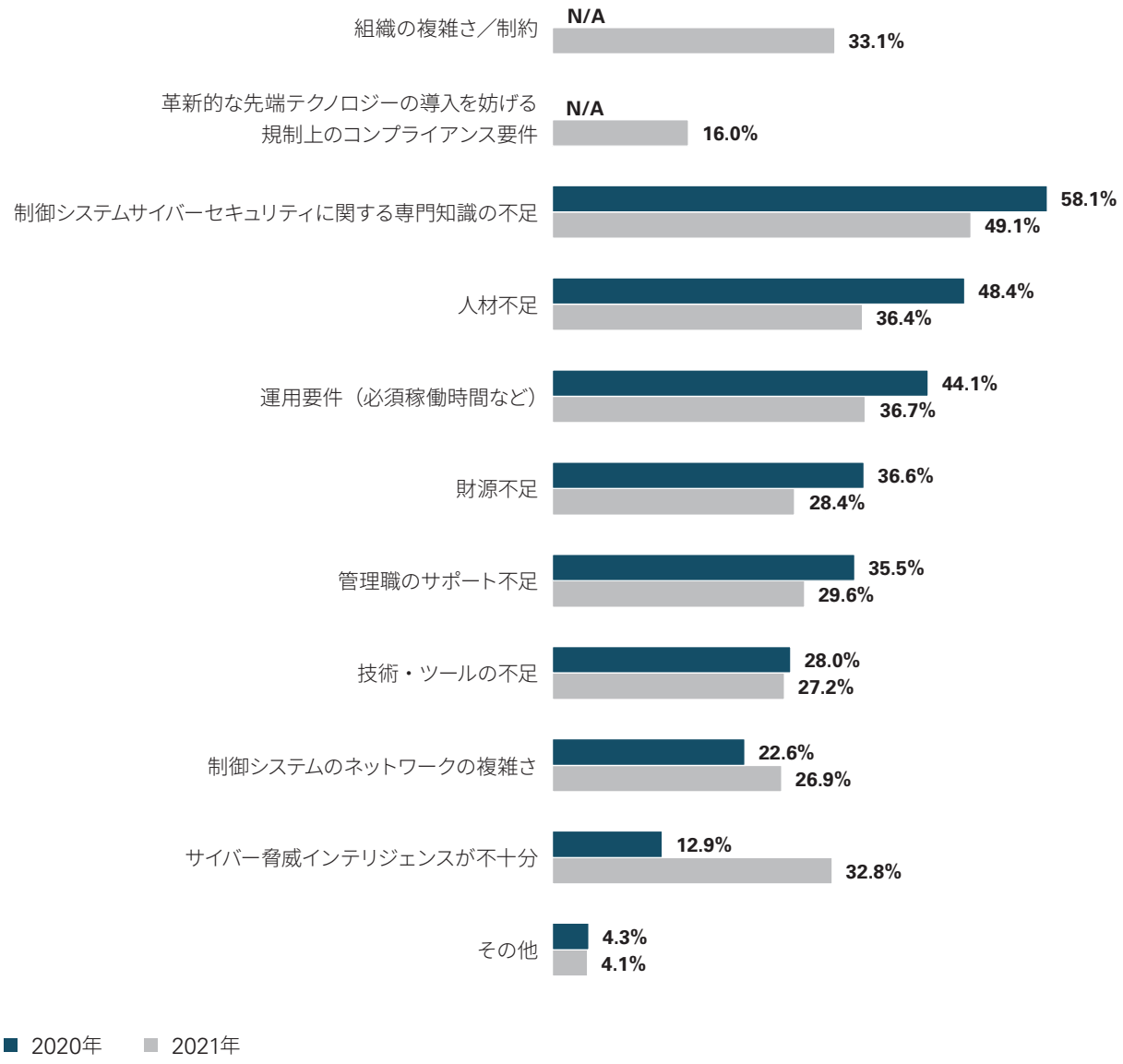


組織の規模が大きくなるにつれて、ベンダーポートフォリオの規模が確実に増え、リスクに対する最新の認識を維持することが難しくなります。買収時のリスクアセスメントは一度で済みますが、買収後には、ベンダーとその機器、ソフトウェア、サービスが時間とともに膨れ上がり、定期的なリスクアセスメントが何千回、何万回と必要になります。

制御システム製品またはサービスを導入する前に、自組織で実施しているリスクアセスメントをすべて教えてください（組織規模別）



制御システム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（2020年と2021年の比較）

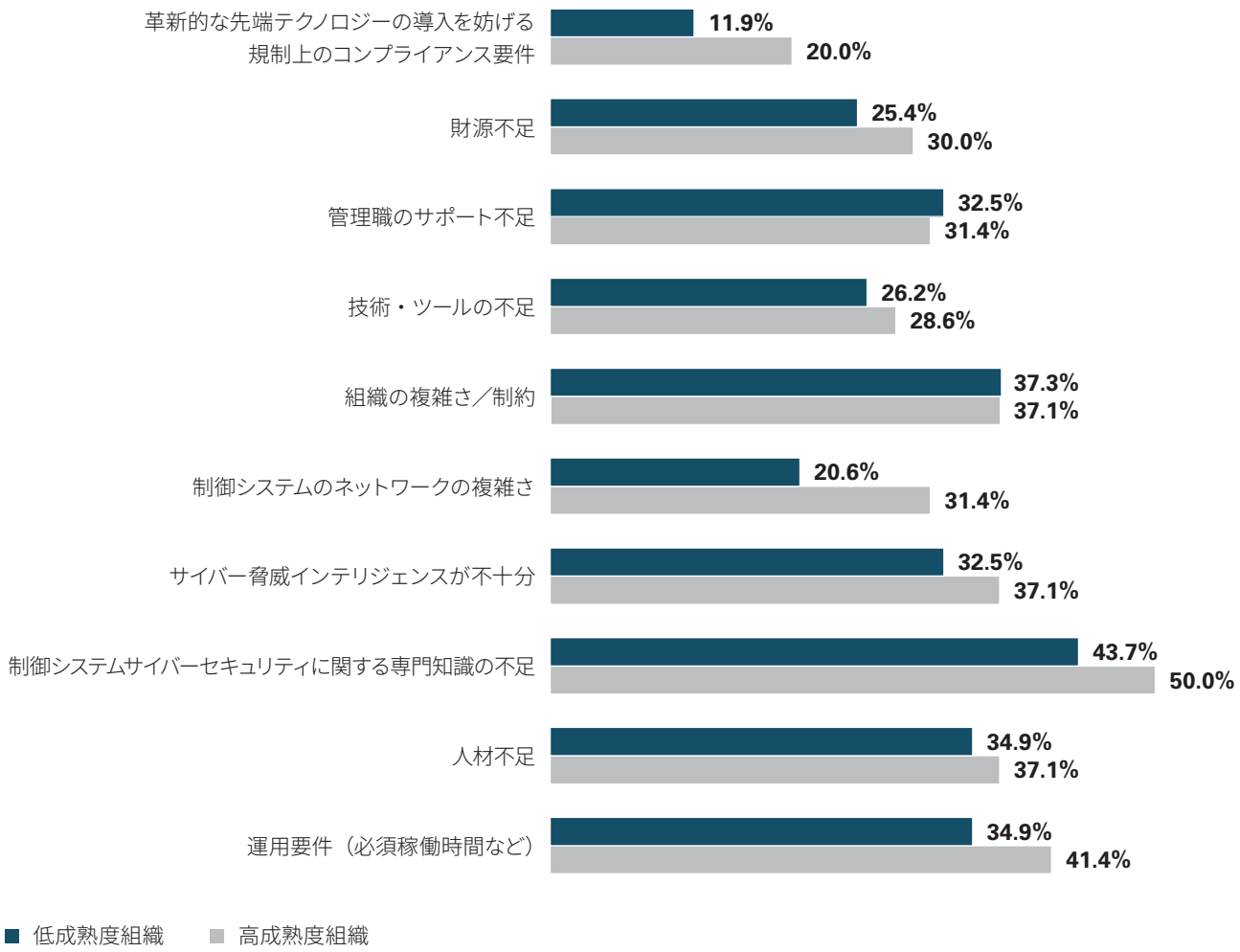


(CS)²への攻撃を防ぐうえでの最大のハードル

「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」が、最大のハードルであると考えている組織が多いことが見受けられます。

縦断的な分析では、ほぼすべての項目で2020年よりも回答比率が低くなっていますが、これは今回の調査で2つの新しい選択肢を追加したことによる影響と言えます。注目すべきは、「技術・ツールの不足」がほぼ横ばいだったこと（2021年：27.2%、2020年：28.0%）と、「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」の2つの項目を選択している組織の割合が前回より増えていることです。「制御システムのネットワークの複雑さ」は、22.6%（2020年）から26.9%（2021年）へとわずかに上昇し、「サイバー脅威インテリジェンスが不十分」との回答は、12.9%（2020年）から32.8%（2021年）に急増しました。当然ながら、より高度なネットワークセグメンテーションを実施すると、管理の複雑さやネットワークの可視性に対する新たな課題が発生するため、多くの組織がストレスを感じています。

制御システム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（高成熟度組織と低成熟度組織の比較）



この質問で回答者がその他に記入した内容には、「サプライチェーンの問題」、「安全なOT製品の不足」、「組織の管理職以下のサポートが不十分」などがありました。

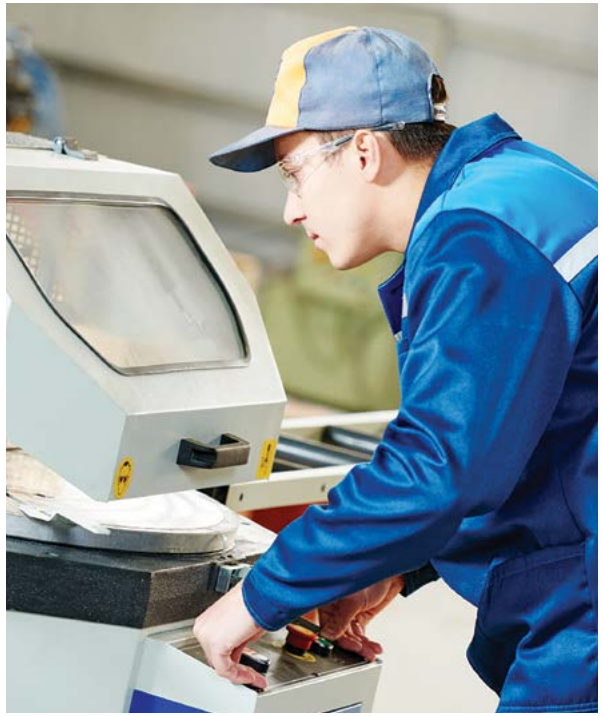
この調査結果からわかるとおり、ITとOTのネットワーク化が進むにつれ、OTセキュリティに関連する組織の複雑さは、産業用制御システム（ICS）のサイバーセキュリティ担当者の不足とともに、大きなハードルとなっています。

敵はITやOT環境に関係なく攻撃してくるため、組織をサイロ化していてはリスクの全体像が掴めません。IT/OT資産を保有している組織は、ICSサイバーセキュリティの専門知識を向上させるとともに、それをITセキュリティの専門知識と組み合わせる必要があります。ITとOTにまたがる状況を把握する能力は、弾力性のある重要なオペレーションを確保するために不可欠です。ITとOTのテレメトリを統合して可視化するセキュリティプラットフォームは、重要インフラの保護、検知、対応能力を効果的に強化することができます。

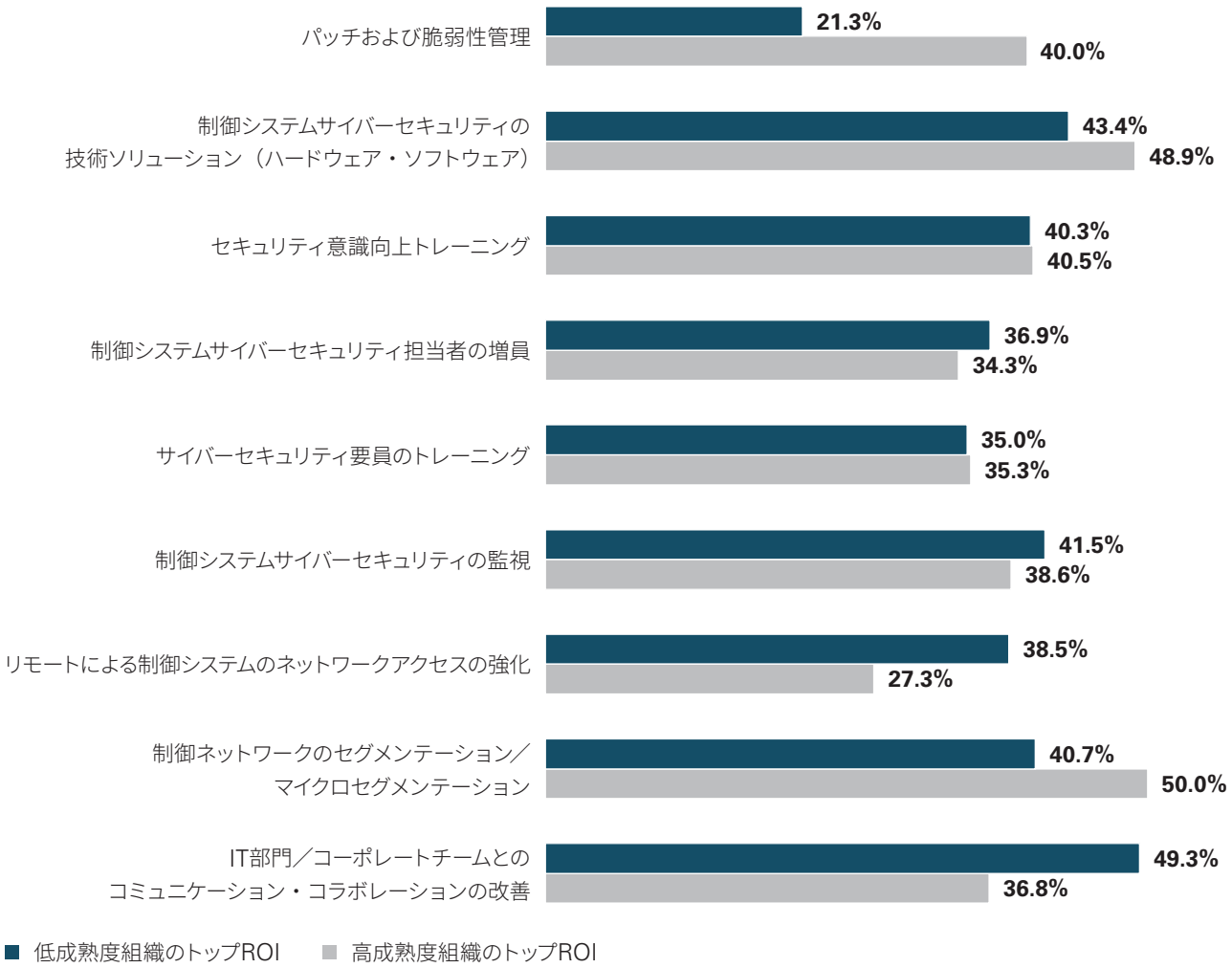
William Malik氏
Vice President of Infrastructure Strategies
Trend Micro

(CS)²の投資対効果が高い上位3分野

サイバーセキュリティに費やすべき分野については、制御システムサイバーセキュリティプログラムの相対的な成熟度によって、大きな違いがあることがわかりました。両グループの回答は「セキュリティ意識向上トレーニング」、「制御システムサイバーセキュリティ担当者の増員」、「サイバーセキュリティ要員のトレーニング」の3つにおいては、非常に近い割合となりましたが、これら以外では、3ポイントから20ポイント近い差がみられます。(「パッチおよび脆弱性管理」高成熟度組織：40.0%、低成熟度組織：21.3%／「制御システムサイバーセキュリティの監視」高成熟度組織：38.6%、低成熟度組織：41.5%)



制御システムサイバーセキュリティ対策で投資対効果が高い分野を教えてください（高成熟度組織と低成熟度組織の比較）



高成熟度組織は、「パッチおよび脆弱性管理への投資が、高いROIをもたらす」と考える傾向が低成熟度組織の2倍近くあります。

“

OT部門とIT部門間のコミュニケーションとコラボレーションの改善について、ROIの期待値が低いかどうかを判断するために、さらなる精査が必要です。Fortinet社の調査レポートである「2021 The State of Operational Technology and Cybersecurity」では、ITとOTの融合はCOVID-19の感染拡大以前から進んでおり、パンデミックはあくまでデジタル変革を加速させ、接続の必要性を高めただけであることが示されています。

また、本報告書では、侵入がなかったと回答した少数の組織は、いくつかのベストプラクティスに倣っている可能性が高いことが明らかになりました。それらの組織の特徴は以下のとおりです。

— オーケストレーションと自動化を活用し、セキュリティの追跡と報告を実施している

— セキュリティオペレーションセンターで完全かつ集中的に可視化されている

— パンデミック時の在宅勤務に対応するため、より早い段階から準備を進めていた

セキュリティ上の脆弱性が財務に与える影響については、大手企業の74%が追跡および報告をしています。また、発見された、あるいはパッチ適用された脆弱性については74%が、具体的なリスクマネジメントの成果については60%が追跡を実施しています。”

William Noto氏
Global Product Marketing Leader for Operational Technology
Fortinet

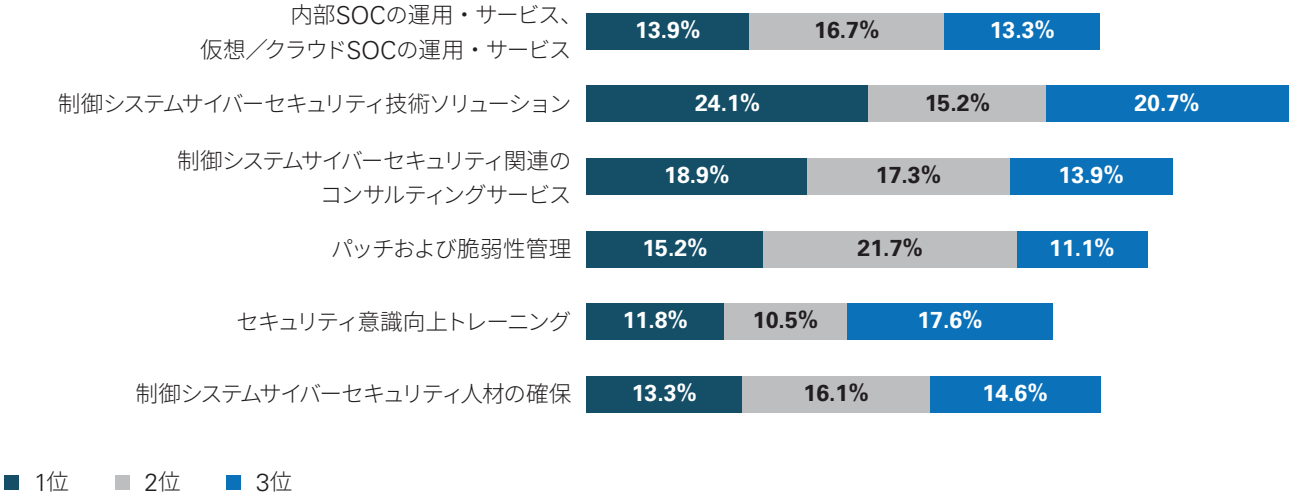
成熟度の差によってどのようにセキュリティ対策が異なるかを確認するだけでなく、その理由を考えることも重要です。低成熟度組織では、リモート接続やアウトソーシングされたセキュリティへの依存が問題となっているため、リモート接続におけるセキュリティ対策に重点的に取り組んでいるのでしょうか。また、高成熟度組織が「IT部門／コーポレートチームとのコミュニケーション・コラボレーションの改善」はROIが低いと考えているのは、この活動に関する課題を克服するプロトコルやプロセスを確立し次に進んでいる、あるいはこの分野での過去の取組みが期待外れの結果であったことなどが理由でしょうか。これらの疑問に答えるためには、根本的な理由を調査し、さらなる研究が必要と思われます。

(CS)²への支出が多い上位3分野

「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」は、制御システムサイバーセキュリティのリソースを最も多く投下している分野として引き続き報告されています。しかし、これに「最も多くリソースを投下している」を選択する回答者の割合は大幅に減少しています（2021年：24.1%、2020年：48.3%）。「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」、「パッチおよび脆弱性管理」は、2020年と同じ順位でした。

「セキュリティ意識向上トレーニング」は最下位に、「制御システムサイバーセキュリティ人材の確保」は最下位から2番目に、それぞれ入れ替わりました。全体として、2021年から「内部SOCの運用・サービス、仮想／クラウドSOCの運用・サービス」が新たな選択肢として加わったことによる希薄化の影響は認めざるを得ません。また、プロセスの改善やテクノロジーの導入により、セキュリティ機能の実行に必要な人手が減少している影響も考えられます。この点については、今後さらに調査を進めるべき興味深い分野であると考えています。

自組織で制御システムサイバーセキュリティのリソースを最も多く投下している上位3分野を教えてください



予算

予算データを提供した回答者の約43%が、2020会計年度の制御システムサイバーセキュリティ予算は100万米ドルを超えると報告しており、これは前回の調査結果と同程度です。

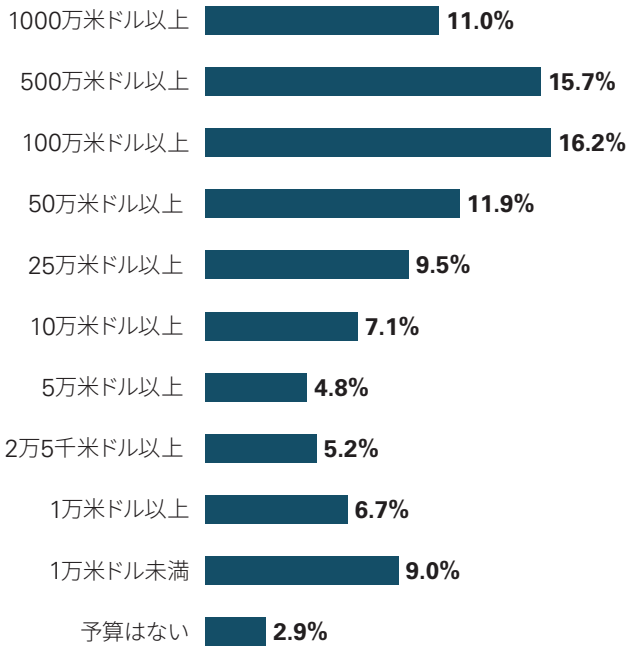
一方で、予算の制約を裏付ける回答がいくつか見受けられました。ほとんどの回答者が「過去1年間に制御システムサイバーセキュリティ予算は増加した」と回答しましたが、全体の約10%が「2020年より減少見込み」としており、これは2019年予算との比較を聞いた前回調査の1.7%を大きく上回りました。さらに、予算の伸び率は前回調査の30〜50%から10〜30%に低下しており、これは少なくとも、部分的にはパンデミックが影響していると思われます。

全体的には予算増の傾向は続くとみられ、全体の約3分の2（60.4%）が「2021年の予算は2020年より少なくとも10%以上増加する見込み」と回答しています。多くの組織において、予算面での制約よりCOVID-19の感染拡大によるリモートワーカーのアクセス需要の急増が勝り、ネットワークセグメンテーションとIDアクセス管理への支出増加を招きました。

> 「銀の弾丸などない」というメッセージは、ようやく浸透しつつあるように思います。多くのベンダーが、サイバー全体あるいは特定の機能を向上させるための「ソリューション」を持ち、それは大きな効果があると主張してきました。しかし、組織が解決すべき問題領域の本質については深く理解されていませんでした。テクノロジーは、人が実行・管理・監督するプロセスを可能にしますが、プロセスのギャップや未熟性を解決するものではなく、人やスキルのギャップ・不足を本質的に解決することはできません。

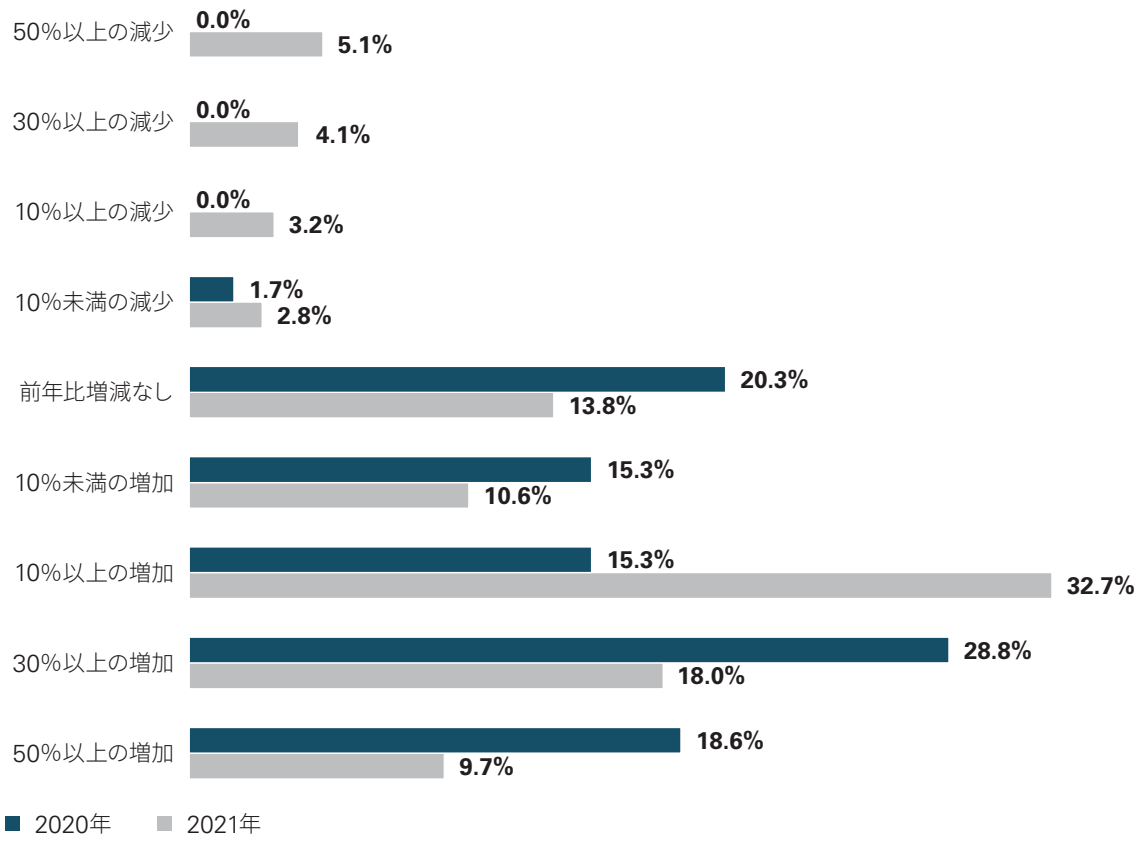
Brad Raiford
Director, Cyber Security
KPMG米国

自組織の制御システムサイバーセキュリティ予算総額（年間）を教えてください



さまざまな組織に与える相対的な影響について、データをさらに詳しく調べてみると、組織の規模によって予算の差にいくつかの明確なパターンがあることがわかりました。50%以上という最大規模の予算減少との回答は、従業員数1,000人以下の中小企業がほぼ独占しました。一方で、予算増10%以上と30%以上との回答も多く、予算のスタンスについて非常に多様性があることも明らかです。従業員数15,001人以上の大手企業も景気の逆風を免れませんでしたが、このグループの12.9%が50%以上の予算増を見込んでおり、最大の予算増加を示しました。

2021年の制御システムセキュリティ予算は前年と比べどのように変化すると思いますか（2020年と2021年の比較）

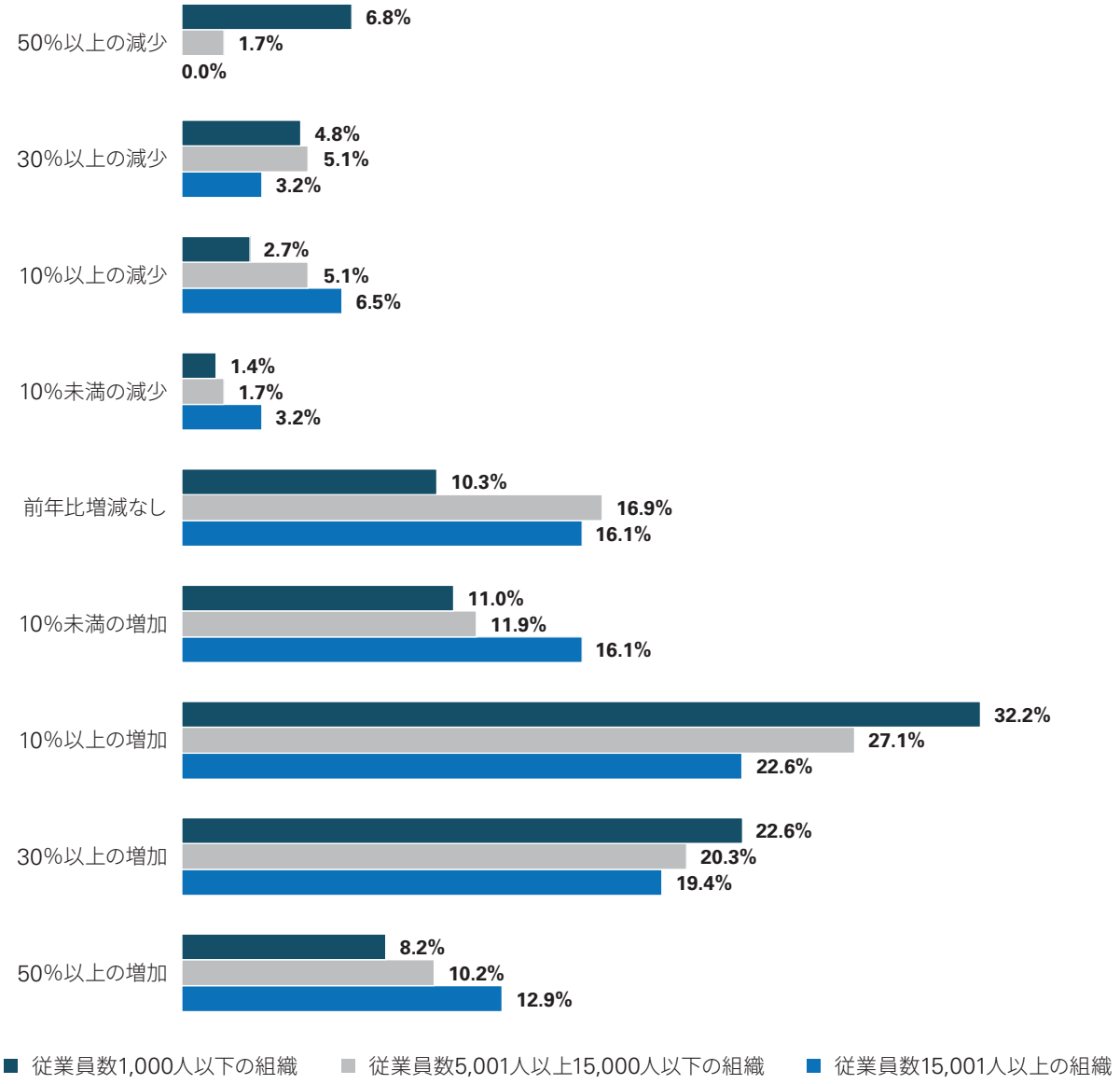


重要インフラを保護する責任を持つすべての組織がセキュリティに真剣に取り組む必要があります。今年度の(CS)²AIの調査データは、予算の制約、専門知識の不足、制御システムを24時間365日稼働させる必要性が、強力なサイバーセキュリティを実現するための大きなハードルになり得ることを示しています。しかし、実際に阻まれることはありません。

今後12ヵ月の間に、セキュリティリーダーがメンテナンスやパッチ適用を必要としない強力な保護を求めるようになり、ハードウェアベースのセキュリティが好まれる傾向になるでしょう。あらゆる種類の遠隔攻撃から重要なインフラを守ることができる、洗練されたソリューションが求められているのです。

Ron Indeck博士
CEO
Q-Net Security

2021年の制御システムセキュリティ予算は前年と比べどのように変化すると思いますか（組織規模別）



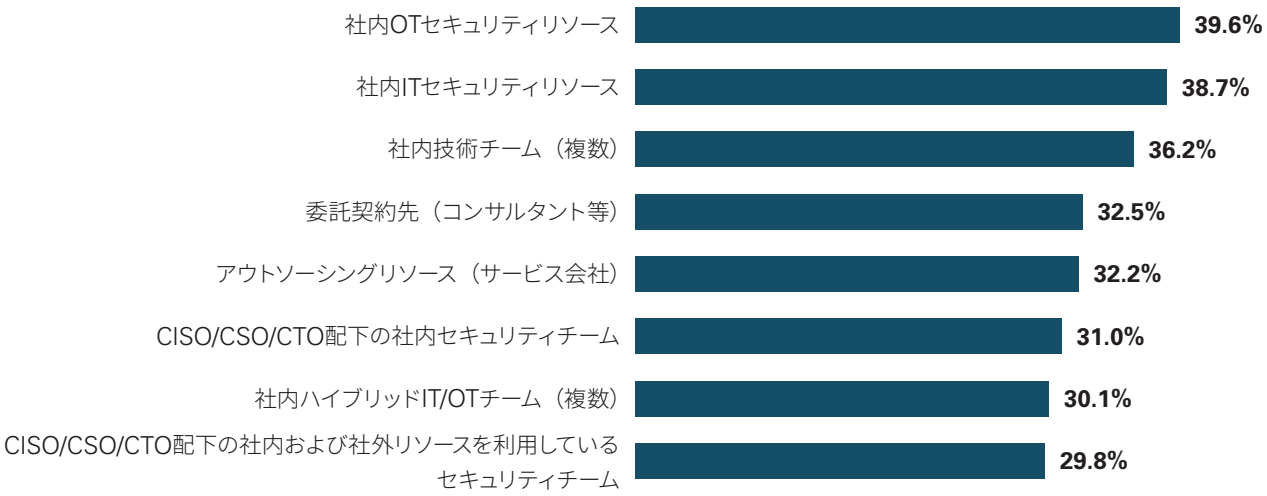
利用サービス

「制御システムサイバーセキュリティサービスを利用しているか」という質問については、2020年の調査結果と大きな変化はありませんでした。組織は、制御システムサイバーセキュリティサービスの提供元として社内リソースに大きく依存しており、最も多い回答は「社内OTセキュリティリソース」の39.6%、次いで「社内ITセキュリティリソース」の38.7%となりました。

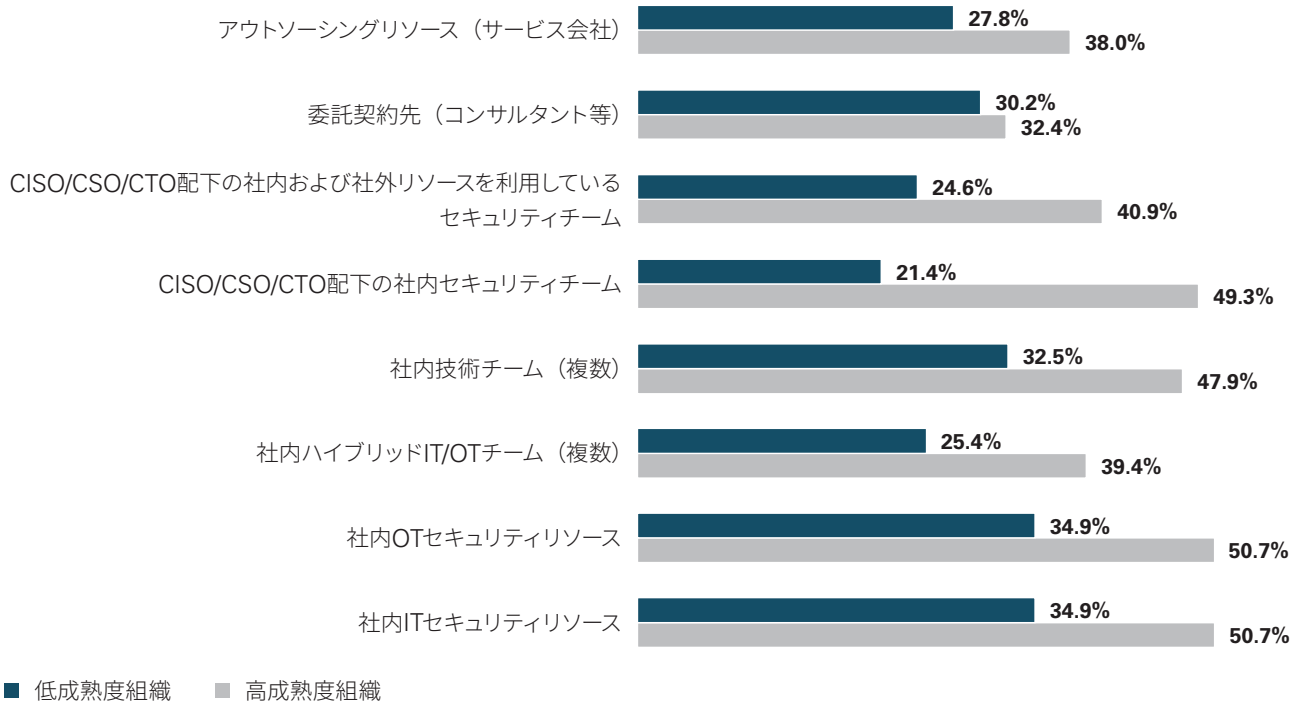
今回の調査結果によると、組織は平均して2〜3種類のサービスを組み合わせて利用していることがわかりました。

成熟度別に分類したところ、高成熟度組織は、低成熟度組織よりもすべてのサービスを頻繁に利用し、より包括的なアプローチをとっていることが明らかです。

自組織で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をすべて教えてください



自組織で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をすべて教えてください（高成熟度組織と低成熟度組織の比較）



高成熟度組織は、低成熟度組織に比べて、CISO/CSO/CTO配下の社内セキュリティチームから提供されるサービスを利用している割合が2倍以上高いことがわかります。

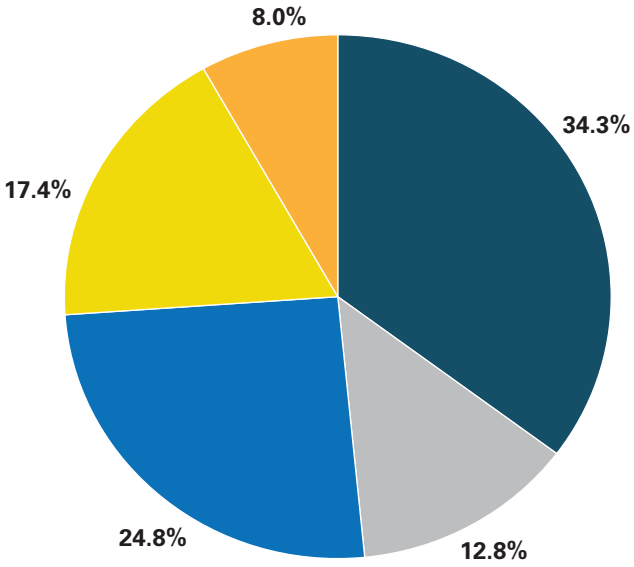
セキュリティ意識向上トレーニング

組織や資産、リソースを守るセキュリティ担当者のスキルや能力の開発を目的としたセキュリティ研修だけでなく、組織のセキュリティ文化を醸成し、セキュリティリスクを減らすための役割を全従業員に認識させる「セキュリティ意識向上トレーニング」の活用が、制御システムの現場で発展しつつあります。ただ、日々進化するサイバー攻撃の手口に対してトレーニングの発展・浸透が追い付かず、各セキュリティ事象の危険性に対する認知度・理解度には差があるのが実態です。

たとえば、不明なリンクをクリックする前に電子メールの送信元を確認するといったITセキュリティ意識の概念については、その理由と重要性が広く知られ、理解されています。一方で、制御システムとITシステムを接続する際に生じる危険性については、よく理解されていません。このような認識不足を解消するためには、すべての組織が制御システムサイバーセキュリティに関する意識向上トレーニングを全従業員に実施することが重要です。このトレーニングを広範なプログラムに統合して実施するか、単独で実施するかは問いません。

主な懸念は、回答者の約2割（17.4%）が、制御システムセキュリティ意識向上トレーニングをまったく実施していないということです。ごくわずかな改善がみられるものの（2020年の調査結果では20.6%）、制御システムを安全に保つための責任について、すべての担当者に認識させる重要性を強調しなければなりません。

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を教えてください



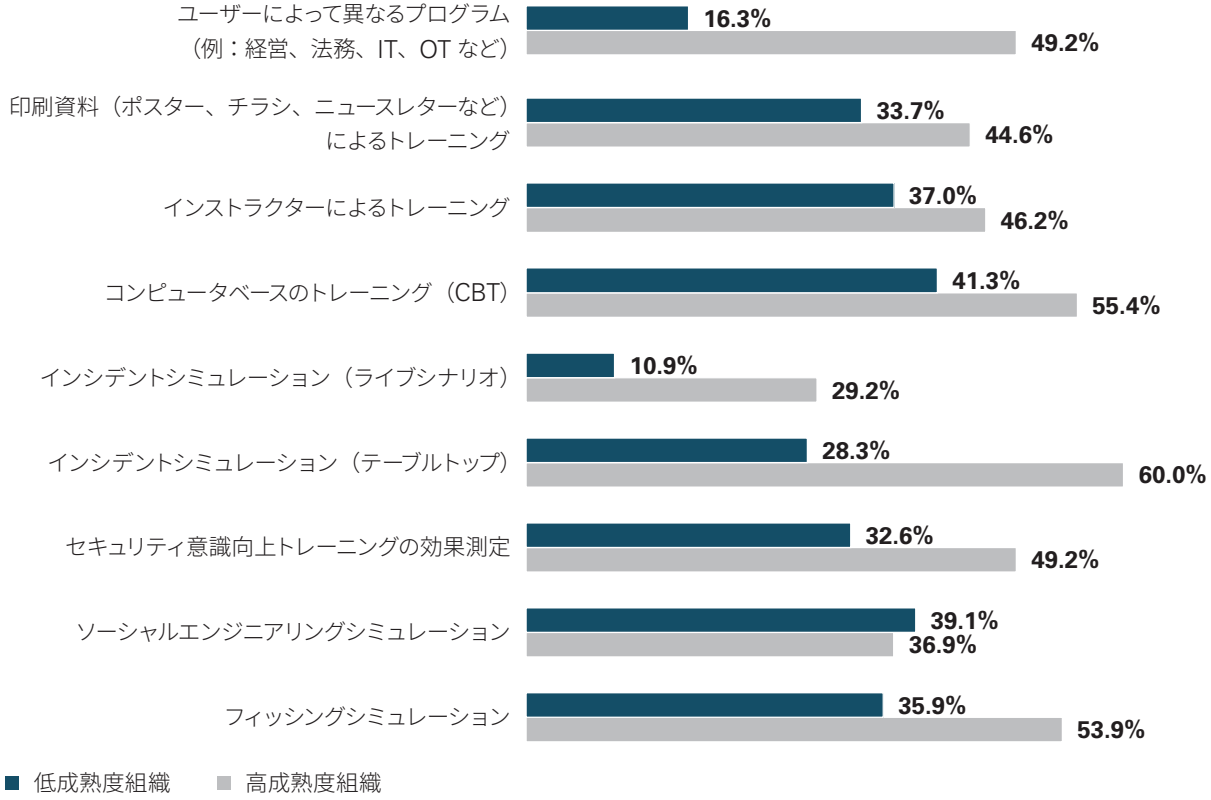
トレーニング

回答結果から、平均して3つ以上の要素が各トレーニングプログラムに含まれていることがわかります。多様なトレーニング手法の有用性は組織によって異なりますが、各トレーニングの要素を組み合わせ、内容やメッセージを統一したうえで複数のチャネルで配信することで、研修プログラムの効果を期待できます。

「インシデントシミュレーション（ライブシナリオ）」は、低成熟度組織において、最も低い回答となりました。これは非常に複雑で費用のかかる訓練であることは確かですが、特にインシデント対応計画と事業継続計画のギャップを発見するうえで、ほかの訓練よりもはるかに効果的です。

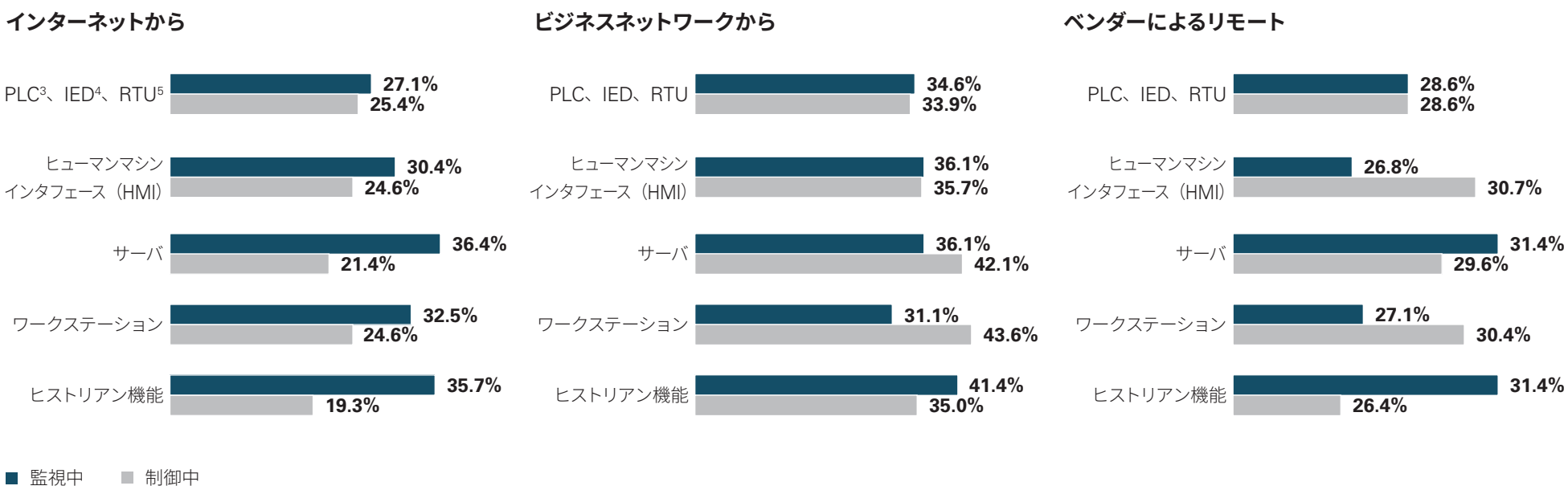
高成熟度組織がインシデントシミュレーションを実施する傾向が高い明確な理由は、これをゼロから始めるのが容易ではないためです。まず前段階として、テーブルトップシミュレーションを始める前に、関連する計画（災害復旧（DR）／事業継続（BC）／インシデント対応（IR）等）を策定し、文書化を早期に進め、すべての人が自身の役割を理解していなければなりません。また、運用システムを含むライブシナリオに進む前に、複数回にわたる練習が必要です（その都度、学んだ教訓と改善は計画に反映しなければなりません）。

制御システムセキュリティに関連するトレーニングに含まれる要素をすべて教えてください（高成熟度組織と低成熟度組織の比較）



制御システムコンポーネントのアクセシビリティ

大半の環境では、制御ネットワークの外部から少なくとも何らかのアクセシビリティがすでに確立されているため、
制御システムの各コンポーネントをリモートで監視または制御できているかを質問しました。



3　プログラマブルロジックコントローラ
4　高性能電子装置
5　遠方監視制御装置

制御システムで最も侵害されやすいコンポーネント

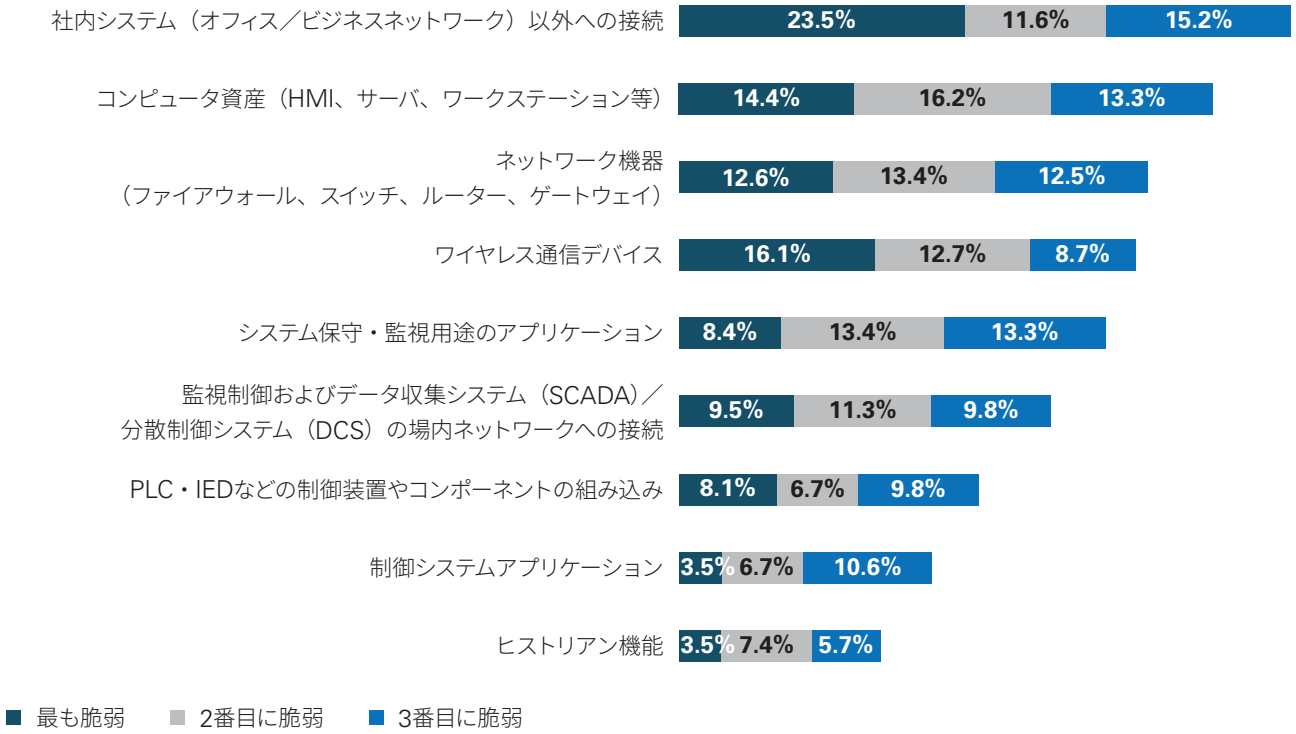
システムの安全性確保が進んできたとはいえ、引き続き、「社内システム（オフィス／ビジネスネットワーク）以外への接続」と「コンピュータ資産（HMI、サーバ、ワークステーション等）」が最大の弱点となっています。「ワイヤレス通信デバイス」については、2020年と比較して注目度が50%近く上がっており、安全性またはセキュリティが脆弱なワイヤレスデバイスの普及に対する認識が高まったことがうかがえます。

組織のセキュリティ計画の現状

約85%の組織がすべての計画において、テストまたは実行、文書化済み、計画中といった何らかの段階に進んでいます。そのうち、約20%が文書化済み、約26～30%が実行済みの状況です。これは、18～27%がそれぞれの管理・対応計画すら持っていなかった2020年と比べ、大幅な改善と言えます。

注目すべきは「計画を実際にテスト済み」との回答が少ないことで、特に「サプライチェーンリスク管理計画」と「脆弱性管理計画」のテスト実施率が低い結果でした。計画を実際にテストすることは、インシデント発生時に失敗しないよう、ギャップを発見して埋めるために不可欠です。

現在の保護と設定状況を踏まえ、どの制御システムコンポーネントが最も侵害されやすいと考えていますか



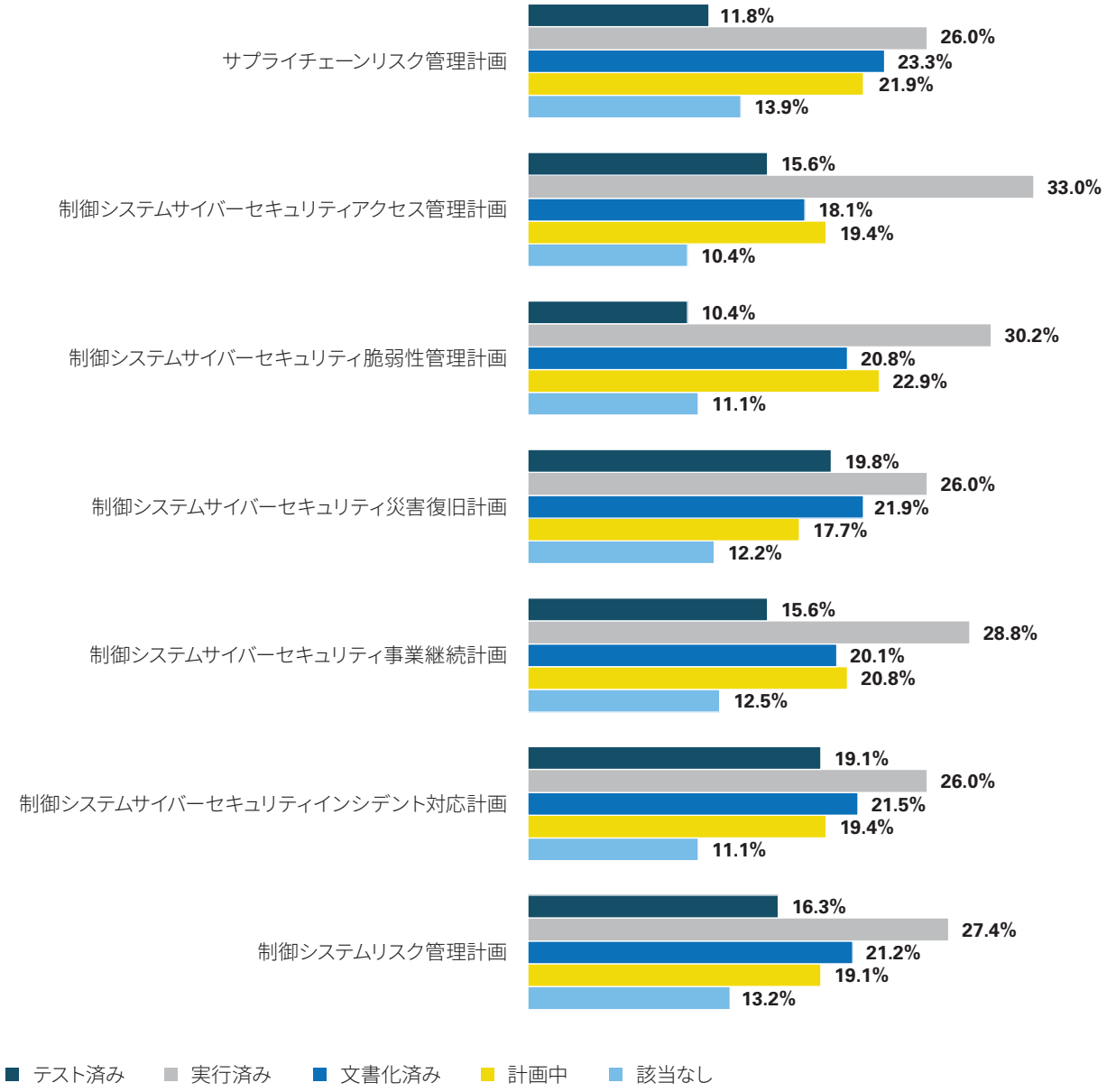
> 最も侵害されやすいコンポーネントとして、「社内システム以外への接続」が最多の回答を得たことは、私の2019年の著書「Secure Operations Technology」の前提を裏付けています。すべての接続や情報の流れは、攻撃対象となります。安全な産業現場は、重要度の低いネットワークから制御システムに入る情報フローの数と種類を最小限に抑えるよう努力しています。そして、制御クリティカルなネットワークとビジネスクリティカルなネットワークの間に、アウトバウンド専用の一方向セキュリティゲートウェイを広く配備しています。

Andrew Ginter氏
VP Industrial Security
Waterfall Security Solutions

“IT（OSベースのサーバ）と純粋な産業用OTデバイスの両方があるため、OTはITに比べ、より複雑なセキュリティ環境が存在しています。デバイスを分離することで、ITチームとOTチームの間で所有権、スキルセット、予算の境界線が生まれます。ITとOTのギャップがあることは事実ですが、このギャップを埋めようとしている先進的な企業もあります。IT部門が産業用デバイスに触れることで、OT現場では未成熟な基本制御を対応でき、産業部門は追加人員、確立したセキュリティ手法、必要な予算確保につなげられます。サイバーリスクと生産リスクは混在しているため、ITとOTのギャップを迅速に解消し、両方のリスクに対処することが企業にとって重要です。”

Richard Springer氏
Director of Business Development, Industrial
Tripwire

自組織における各計画の実施状況について教えてください

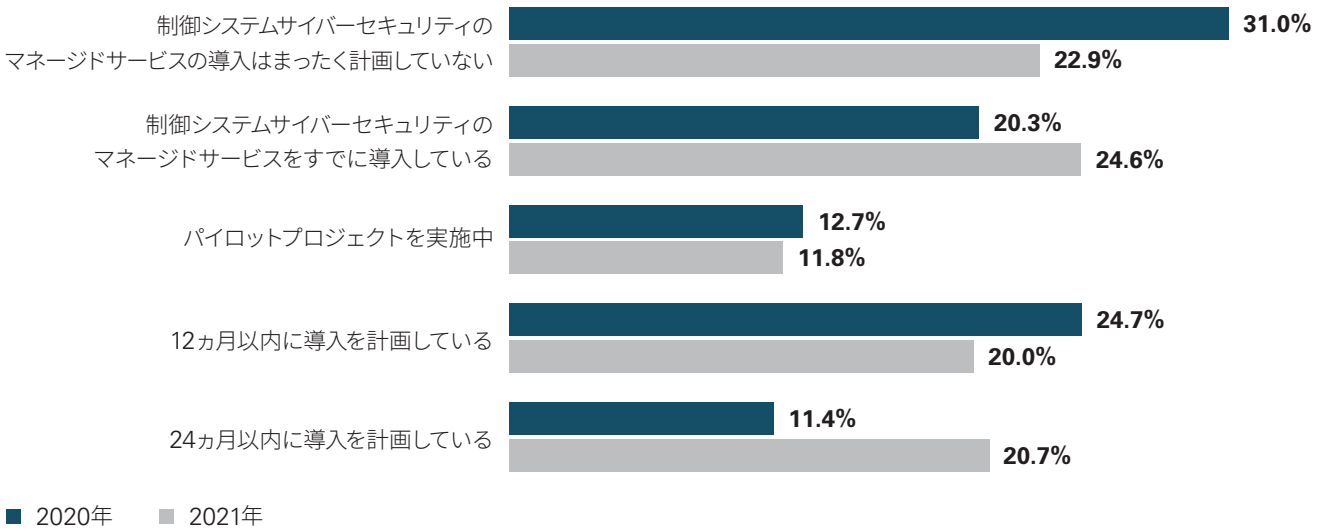


マネージドサービス

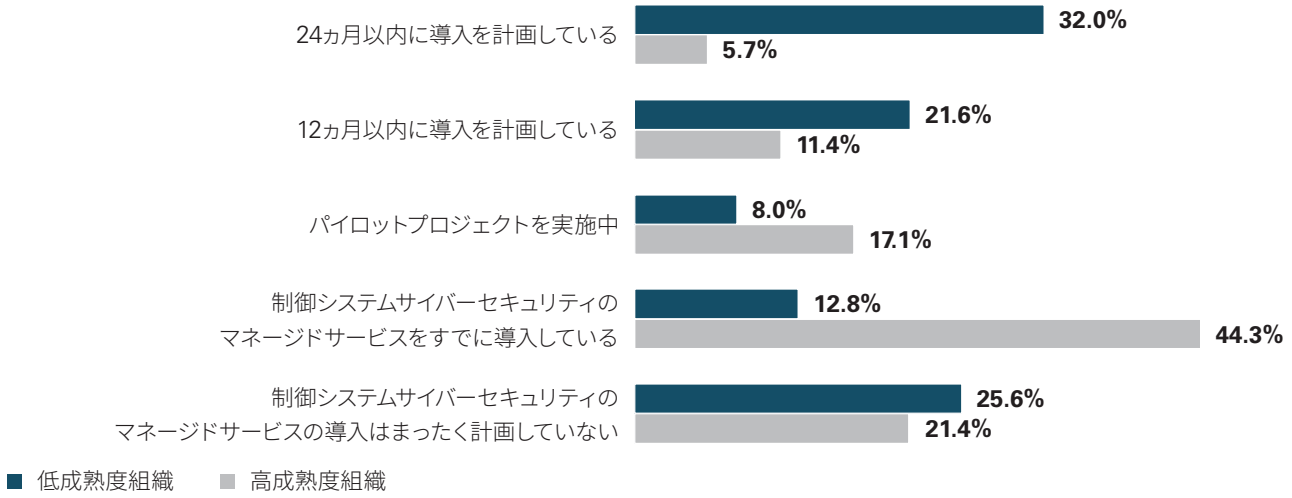
2020年と比較すると、制御システムサイバーセキュリティのマネージドサービスをすでに導入している割合が若干増加し（約5%増）、「まったく計画していない」とする回答が減少しています。高成熟度組織と低成熟度組織とではいくつかの差がみられましたが、従業員規模に基づく組織間の明確な傾向はみられませんでした。

「十分なトレーニングがされ専門知識を備えた内部リソースの不足」は、前回に引き続き、組織が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導入する主な動機となっています。約44%がこの要因のみを単独で選択し、両方選択した割合も含めると全体で約68%となっています。データを縦断的に比較すると、2020年よりも多くの組織が唯一の明確な要因でマネージドサービスを支持しているように見受けられます。このことは、2020年の報告書で「その他」を選択した際に、マネージドサービスを導入するための明確なビジネスケースを持っていないと明記した回答者の数からも裏付けられています。

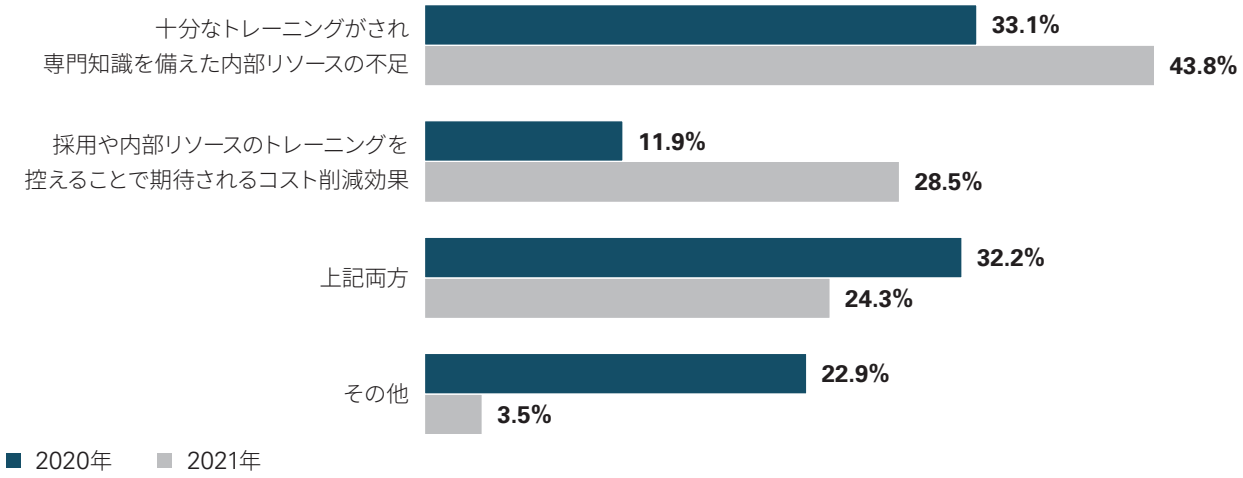
自組織における制御システムサイバーセキュリティのマネージドサービスの導入状況を教えてください



自組織における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の導入状況を教えてください（高成熟度組織と低成熟度組織の比較）



自組織で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導入している（または導入を計画している）理由を教えてください



現在の制御システムのネットワーク稼働状況の監視

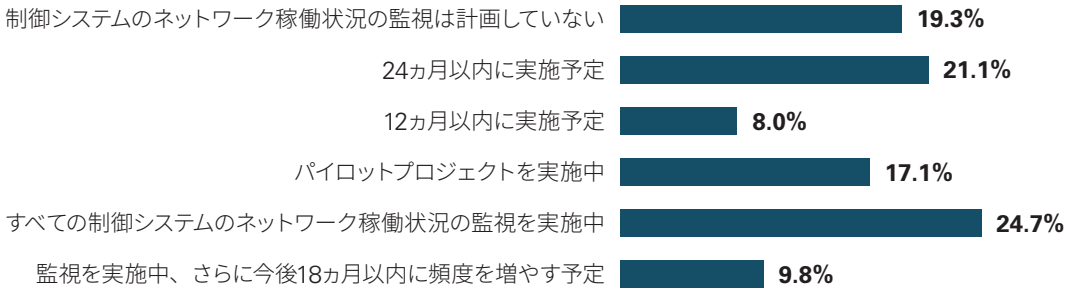
半数以上が、制御システムのネットワーク稼働状況の監視を実施しており（51.6%）、約3割（29.1%）が「監視の実施予定」と回答しています。残念ながら、約5分の1（19.3%）は監視の計画すらしていません。

制御システムのネットワークを監視できていないということは、組織が侵害された際の最初の兆候として認識するのは運用の中断であり、その時点で脅威者に対して、制御ネットワーク環境へ侵入し偵察するための無期限的なシステム内での滞留を許していることになります。多くのケーススタディによると、まさにこれが要因で、脅威者が気付かれずに自由に行動できる時間が長くなるため、被害の程度や排除の難易度ははるかに高くなります。

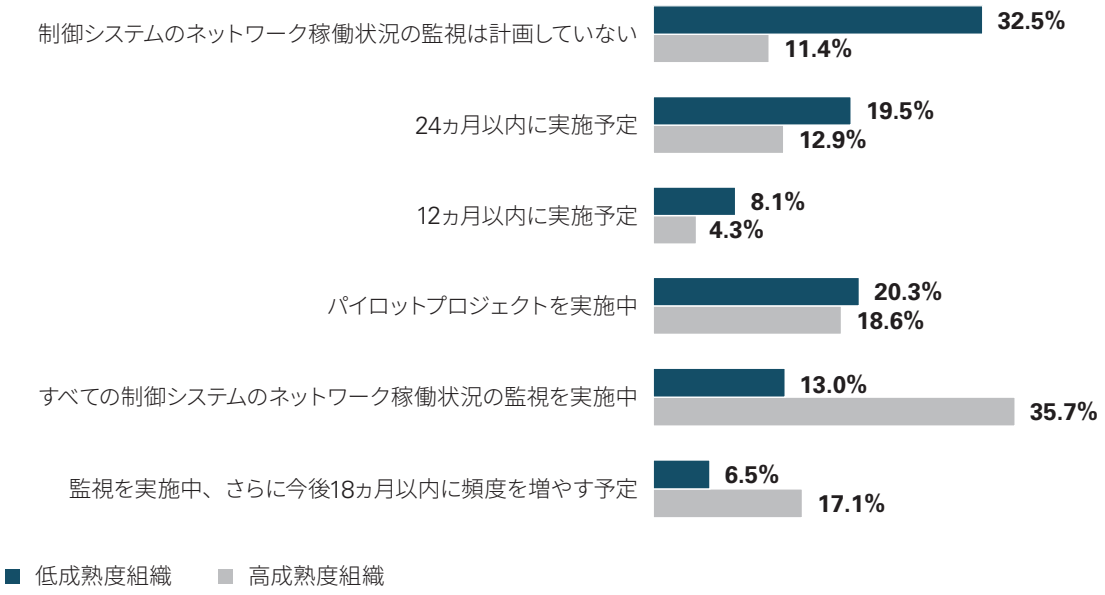
さらに興味深いのは、低成熟度組織と高成熟度組織の回答に明確な違いがあることで、後者では制御システムのネットワーク稼働状況の監視を実施しているだけでなく、さらに頻度を増やす傾向が顕著にみられます。

経験豊富な制御システムの担当者の多くは、監視ソリューションに対し依然として警戒心を抱いており、大抵の場合、IT由来のスキャンツールをOT環境に適用していた過去の問題点に起因しています。ただ、制御システム特有の侵入検知・防御ツール（IDS/IPS）は、近年大きな進歩を遂げ、知識のある担当者が関与すれば、かつてのようなリスクはほとんどないことを認識しなければなりません。IDS/IPSは、制御システムの資産と運用を保護するための必須要素と考えられつつあります。

自組織における制御システムのネットワーク稼働状況の監視について、現状を教えてください



自組織における制御システムのネットワーク稼働状況の監視について、現状を教えてください（高成熟度組織と低成熟度組織の比較）



アセスメント

頻度

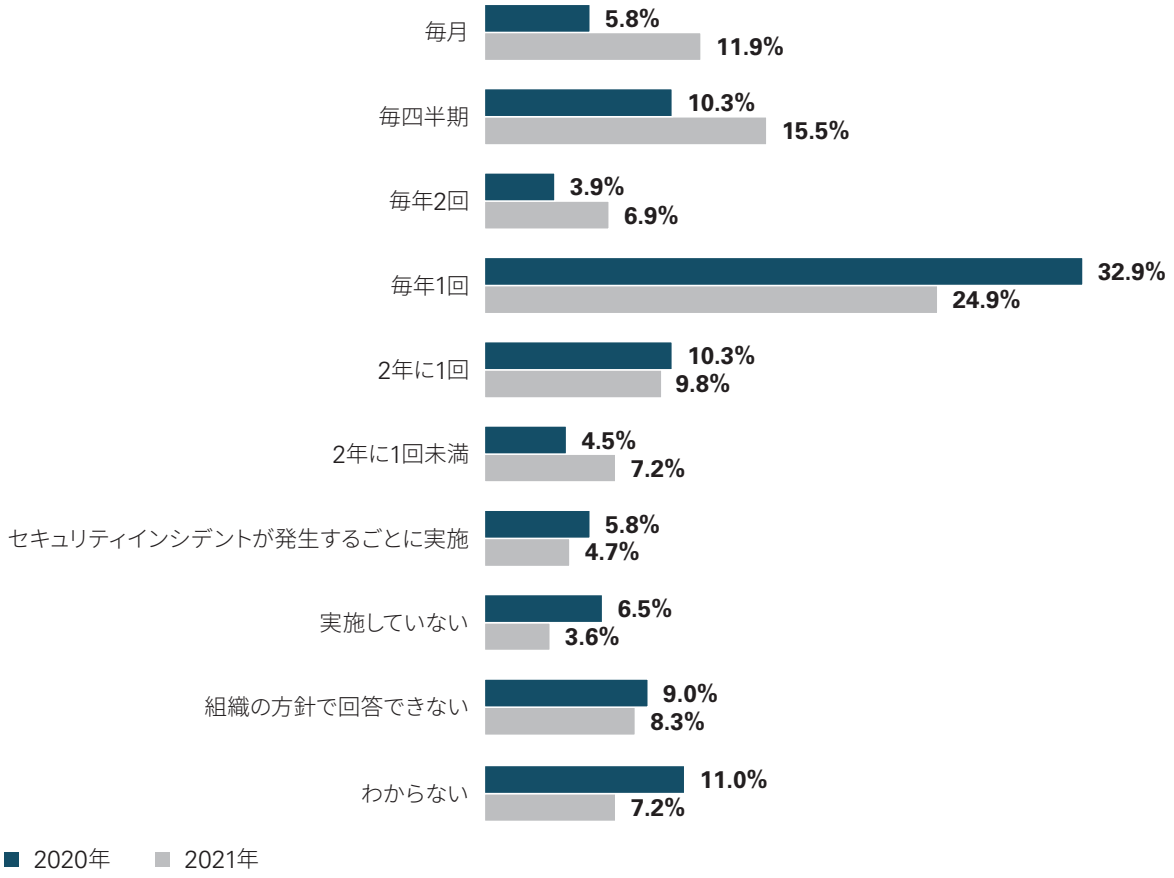
制御システムサイバーセキュリティアセスメントの実施頻度では、前回に引き続き「毎年1回（24.9%）」との回答が最も多い結果でしたが、実施頻度が高い項目においても全体的に回答割合が増えていることは良い傾向と言えるでしょう。「毎月」と回答した割合は前回の約2倍（11.9%）、「毎四半期」は約1.5倍（15.5%）となりました。

高成熟度組織によるアセスメントの実施頻度は、低成熟度組織と比較して大きな違いはなかったものの、アセスメントの実施内容については、明らかな違いがみられました。

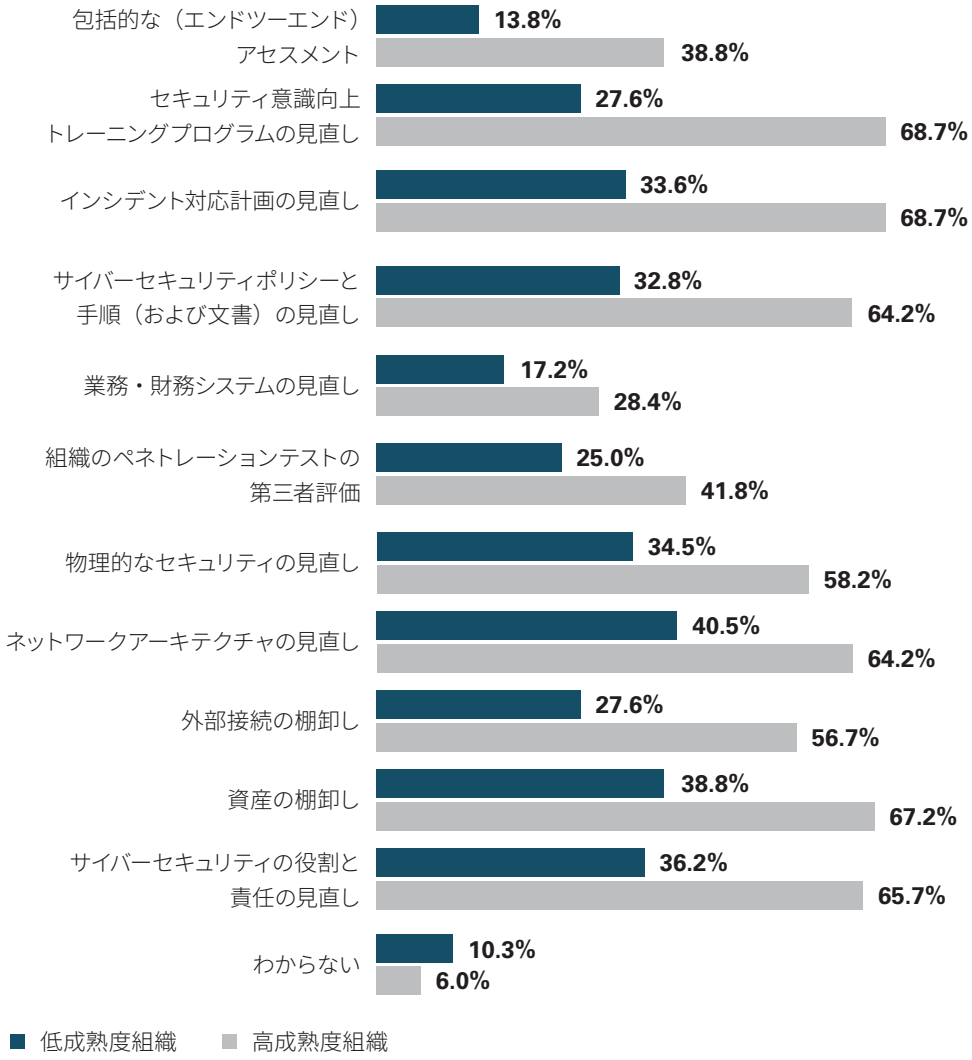
包括性

高成熟度組織は、徹底したサイバーセキュリティアセスメントを実施しており、すべてのコンポーネントにおいて、低成熟度組織に大差をつけて回答割合が多いだけでなく、「包括的な（エンドツーエンド）アセスメント」の実施においては、3倍近くの差（高成熟度組織：38.8%、低成熟度組織：13.8%）がありました。

自組織における制御システムセキュリティアセスメントの実施頻度を教えてください



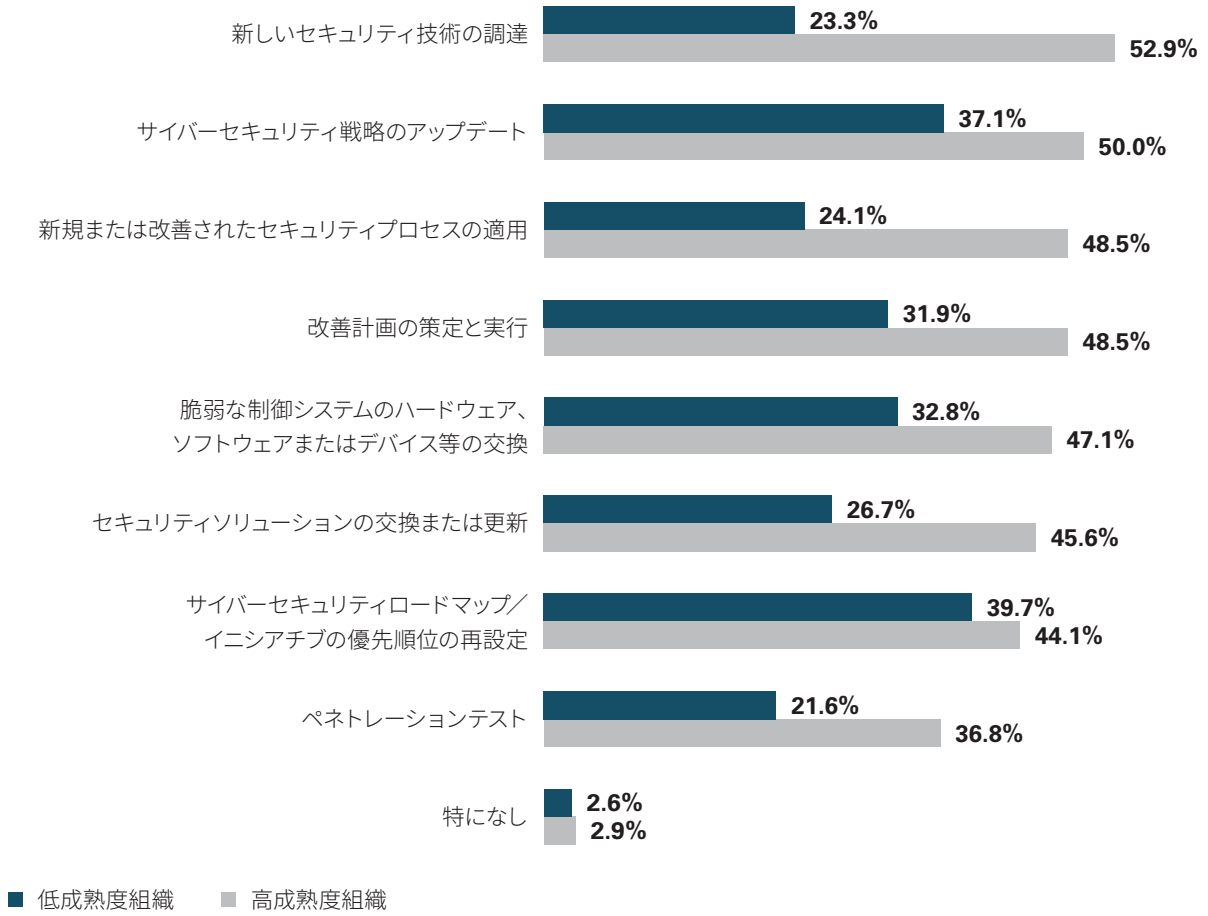
自組織における制御システムセキュリティアセスメントに含まれるコンポーネントをすべて教えてください（高成熟度組織と低成熟度組織の比較）



フォローアップ活動

前項と同様、高成熟度組織は、セキュリティアセスメントの結果に応じて幅広いフォローアップ活動を実施する傾向があります。

過去12ヵ月以内に実施されたセキュリティアセスメントの結果に応じて、自組織で取り組んだ（または計画している）活動をすべて教えてください（高成熟度組織と低成熟度組織の比較）



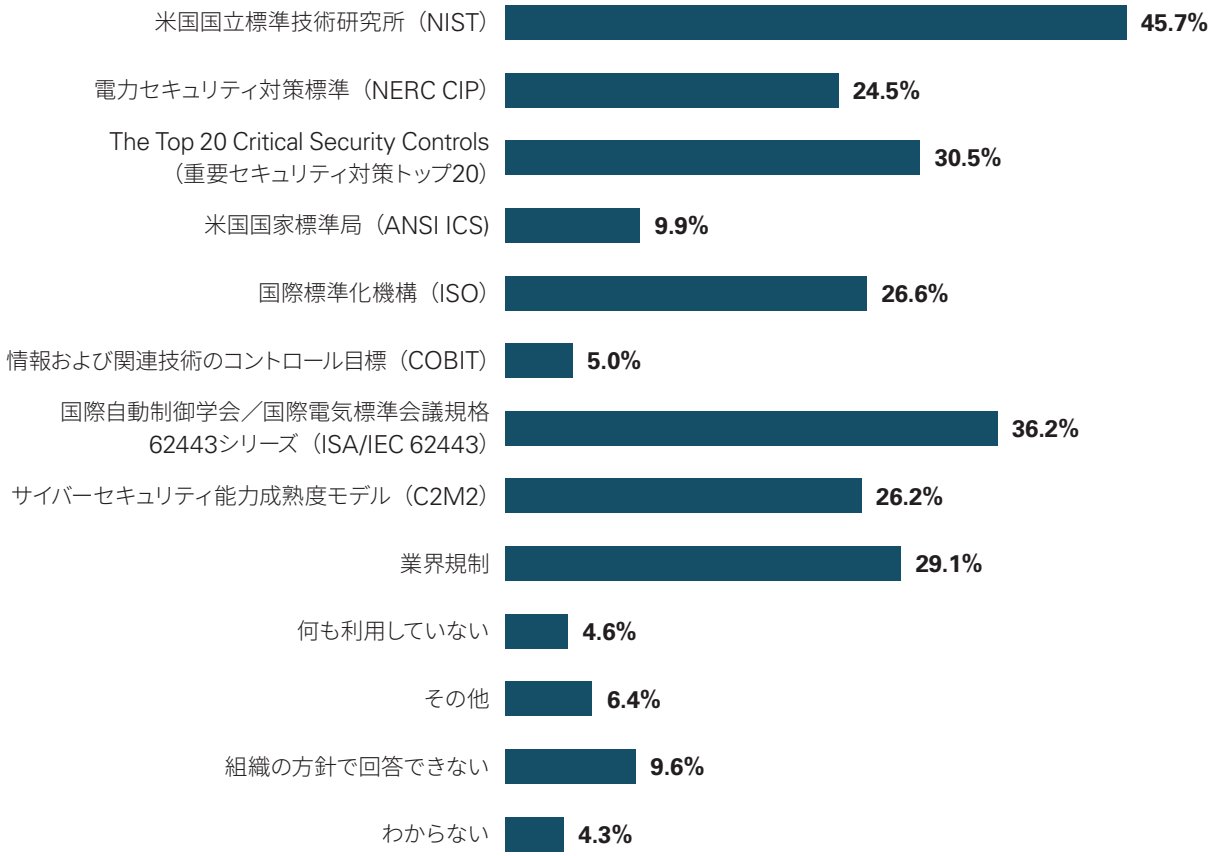
利用されているフレームワーク

米国国立標準技術研究所（NIST）のサイバーセキュリティフレームワークが、引き続き最も利用されています。この質問は前回から変更したため単純な比較はできませんが、前回の調査では提示されなかった2つの選択肢、「ISA/IEC 62443」と「サイバーセキュリティ能力成熟度モデル（C2M2）」が、広く利用されていることは注目に値します（それぞれ36.2%と26.2%）。

「The Top 20 Critical Security Controls（重要セキュリティ対策トップ20）」は、低成熟度組織が高成熟度組織よりも多く利用している唯一のフレームワークです（高成熟度組織：28.6%、低成熟度組織：30.1%）。それ以外のフレームワークについては、高成熟度組織の利用割合が高く、低成熟度組織よりも頻繁に複数の専門知識の情報源を利用していることがよくわかります。

このことが示すのは、「特定のフレームワークを採用しセキュリティ体制を改善すべき」ということではなく、低成熟度組織にとって、より多くの専門知識の情報源をベストプラクティスとプロセスに取り入れることの重要性です。

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をすべて教えてください



利用されている技術

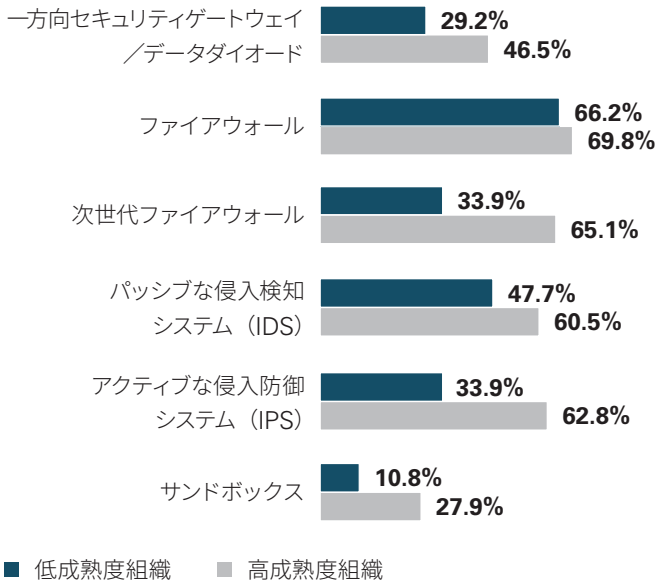
高成熟度組織におけるセキュリティ技術の利用には、いくつかの顕著な傾向があることがわかりました。利用率はそれぞれ、「一方向セキュリティゲートウェイ／データダイオード」は、低成熟度組織の約1.5倍（高成熟度組織：46.5%、低成熟度組織：29.2%）であり、「次世代ファイアウォール」は、同約2倍（高成熟度組織：65.1%、低成熟度組織：33.9%）、「アクティブな侵入防御システム（IPS）」は、同約2倍（高成熟度組織：62.8%、低成熟度組織：33.9%）、「サンドボックス」は同約2倍以上（高成熟度組織：27.9%、低成熟度組織：10.8%）との結果でした。

昨今のサイバーセキュリティインシデント

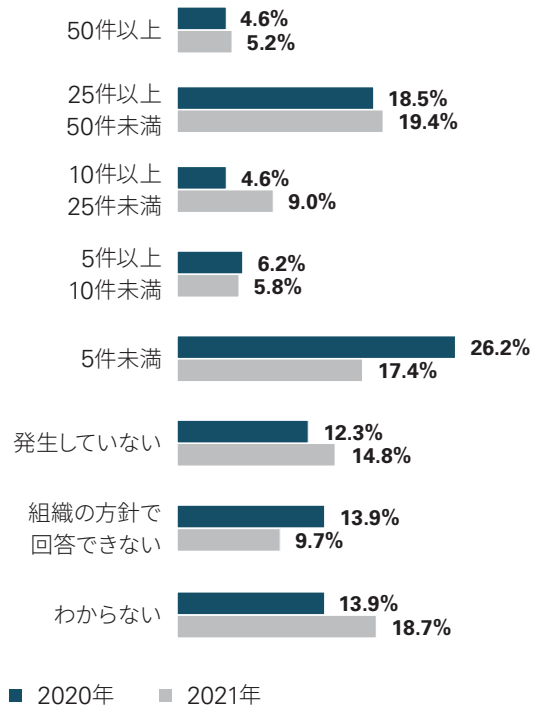
縦断的な分析により、過去12ヵ月以内に制御システムサイバーセキュリティインシデントが「10件以上25件未満」発生した組織は統計的に大幅に増え（2020年：4.6%、2021年：9.0%）、「5件未満」との回答が減少していることがわかりました（2020年：26.2%、2021年：17.4%）。

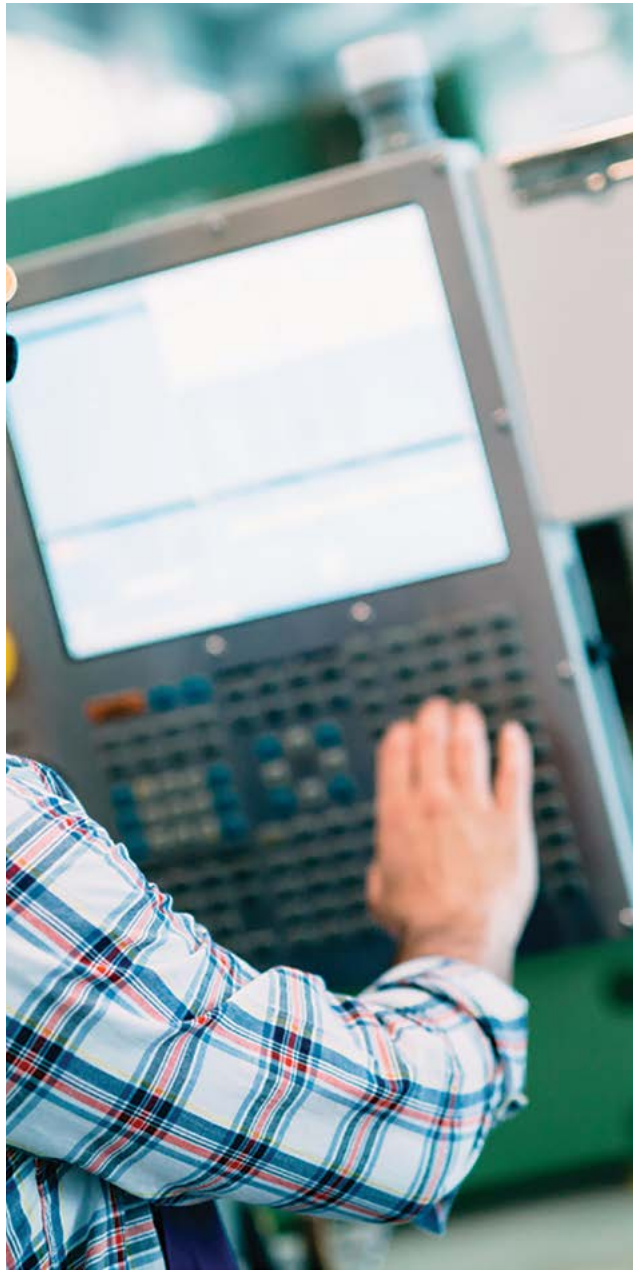
組織規模別でみると、顕著な違いが明らかになりました。従業員数501～1,000人の組織では、過去12ヵ月以内に「25件以上50件未満」の制御システムサイバーセキュリティインシデントが発生したとの回答が多く（40.9%）、100～500人と1,001～5,000人の組織ではほぼ同レベル（それぞれ28.6%と28.0%）にとどまりました。この3つの規模以外の組織では大幅に低いことから、悪質なサイバー犯罪業者はこれらの規模の組織をターゲットにしている可能性を示唆しています。

自組織の制御システム資産をサイバー脅威から保護するために利用しているセキュリティ技術をすべて教えてください（高成熟度組織と低成熟度組織の比較）

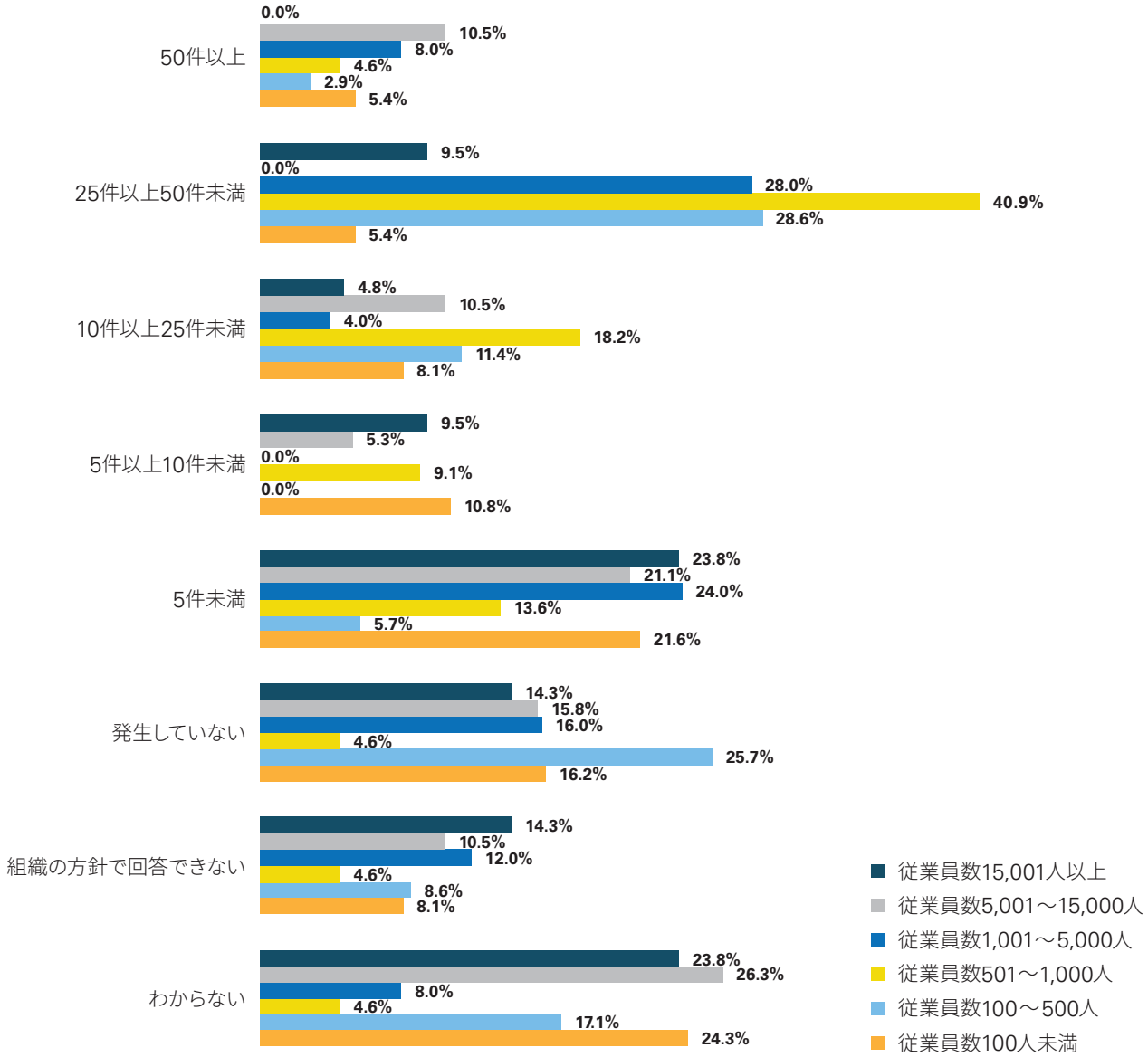


過去12ヵ月以内に自組織で発生した制御システムサイバーセキュリティインシデントのおおよその件数を教えてください





過去12ヵ月以内に自組織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を教えてください（組織規模別）

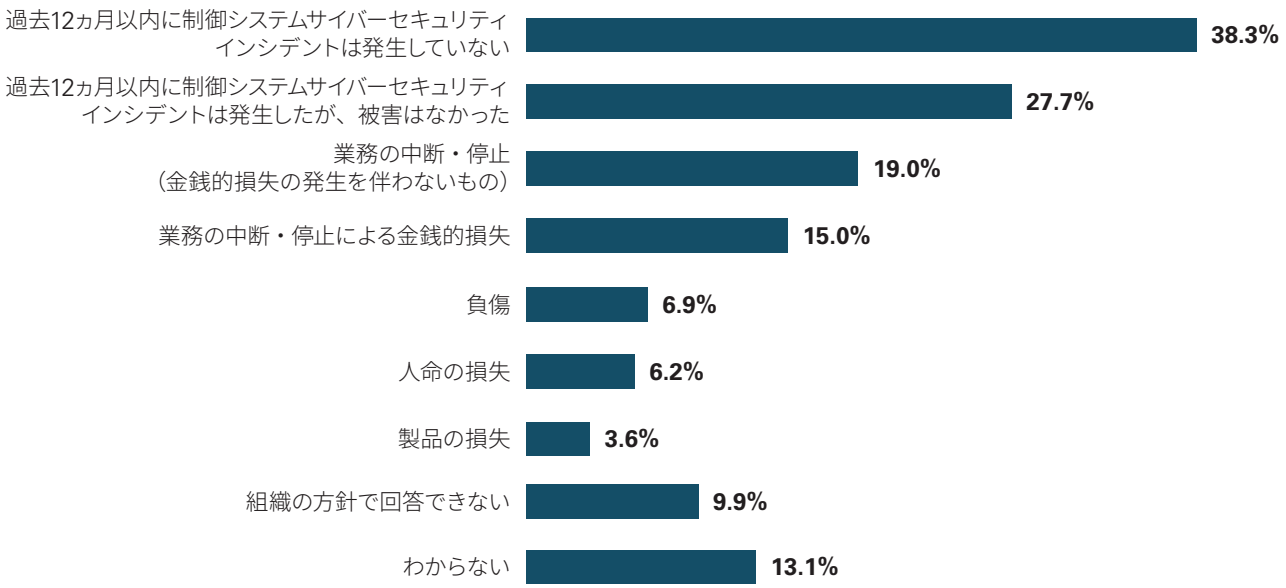


昨今のセキュリティインシデントによる被害

2021年と2020年の報告書を直接比較することは、調査方法の変更により不可能ですが、過去12ヵ月以内に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として、「負傷」が1.3%から6.9%に、「人命の損失」が1.3%から6.2%と明らかに増えています。この理由として考えられるのは、医療関係者の割合が高いこと（2021年の調査回答者の12%以上が医療にかかわる仕事をしている）、医療システムに対するランサムウェア攻撃[6]が急増していることがあります。

その他の傾向として、「組織の方針で回答できない」や「わからない」を理由に回答を控える割合が減少した（それぞれ30.9%から9.9%と34.9%から13.1%）ことが挙げられます。この調査に情報を提供する人が増えていることを非常にポジティブに捉えています。

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をすべて教えてください



> 2021年7月、アメリカ合衆国運輸保安庁（TSA）は米国のパイプライン事業者に対し、ITネットワークが侵害されても、パイプラインの輸送が継続可能となるようセキュリティの向上を命じました。結局のところ、『用心に用心を重ねて停止する』とは、OTセキュリティプログラムの強度を信用しないことを意味します。OT/ICSのセキュリティ設計に、ハードウェアで強化された一方向セキュリティゲートウェイのレイヤーを追加する時代になりました。

Andrew Ginter氏
VP Industrial Security
Waterfall Security Solutions

6 https://thecrimereport.org/2021/08/18/hospitals-cyberattacks/

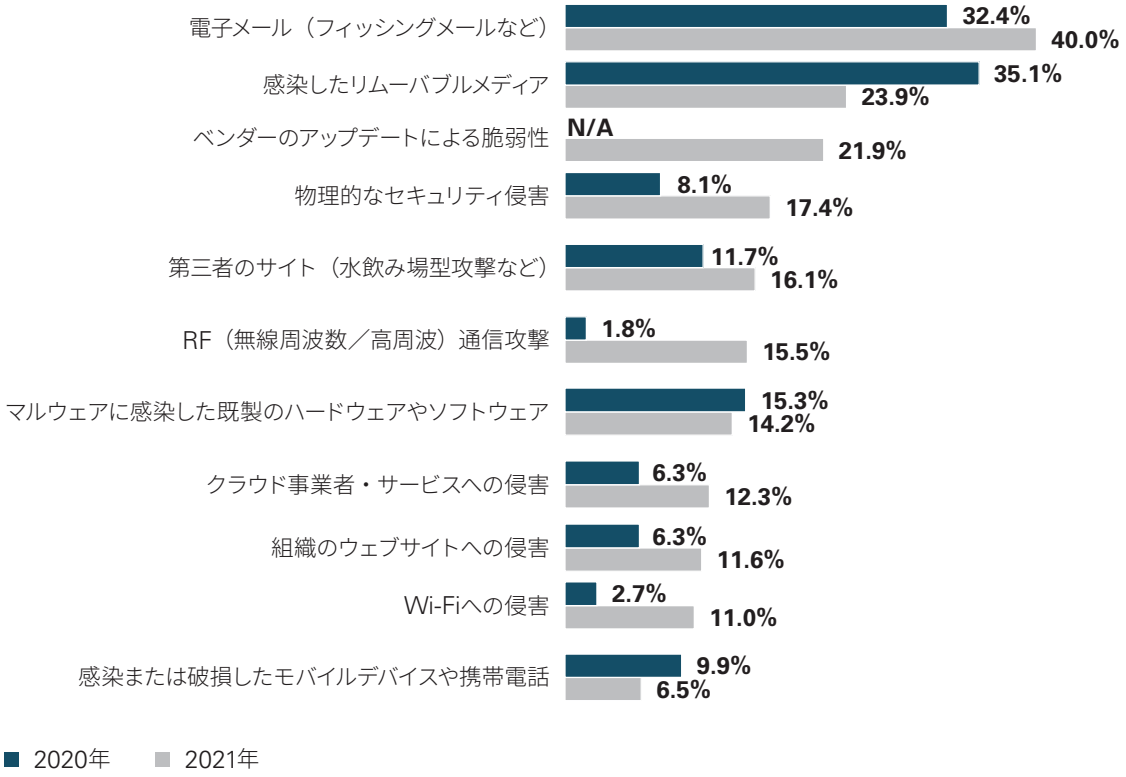
“成功している組織は、指標、目標、詳細な手順、および毎時間、毎日、毎週の監視による計算結果に基づき事業を運営しています。サイバーセキュリティの目標は、脆弱性の削減、潜在的なマルウェアの特定、攻撃者の特定、インシデント対応の改善など、細かなものや野心的なものになりがちです。OTサイバーセキュリティの成功に向けたアプローチは、これらの目標を、単純な色分けなどで明確に示された計画的な目標と指標に変換することです。”

Rick Kaun氏
VP Solutions
Verve Industrial Protection

昨今の攻撃ベクトル

2021年の調査で新たに追加されたベクトルである「ベンダーのアップデートによる脆弱性」は、21.9%と予想以上に高い結果となりました。選択肢を増やしたことで希釈効果が出たベクトルもありますが、おおむね2020年より上昇しました。特に、「物理的なセキュリティ侵害（2020年：8.1%、2021年：17.4%）」、「RF（無線周波数／高周波）通信攻撃（2020年：1.8%、2021年：15.5%）」、「クラウド事業者・サービスへの侵害（2020年：6.3%、2021年：12.3%）」、「Wi-Fiへの侵害（2020年：2.7%、2021年：11.0%）」などが顕著でした。

過去12ヵ月以内に自組織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で悪用された攻撃ベクトルをすべて教えてください



“

COVID-19のパンデミックは、物理世界とデジタル世界の境界線をさらにあいまいにし、サイバーセキュリティインフラの断層を露呈させ、多くの新たな課題を明らかにしました。パンデミック後の状況における、現場での労働力不足もその1つです。COVID-19関連の制約があるなかで、企業におけるハイブリッド勤務の採用やチームの分割が、現場の人員不足の主な要因となっています。そのため、メンテナンスサイクルの延長や、請負業者の遠隔サービスサポートなどの回避策が必要になることがしばしばあり、その結果、サプライチェーンのリスクも高まっています。

ワイヤレス通信は、攻撃者がICSネットワークに侵入するための1つの手段です。5Gのような無線周波数は、モバイル機器や長距離に配置された機器間の通信を容易にするために導入されています。その他の無線周波数は、日常的な手動制御やトラブルシューティングのために使用されることがあります。通信に無線周波数を使用するリスクは、安全性や生産に影響を与えるような方法で、記録、リバースエンジニアリング、操作、再生される可能性があることです。ホームネットワークでよく使われるWi-FiアクセスポイントをICSネットワークに導入すると、エアギャップの確立を目的としたデータダイオードの利用を損なう可能性があります。ICSネットワークにどのような技術が導入されているかを知り、それらがビジネスにどのようなリスクをもたらすかを理解することが重要です。”

Eddie Toh
Partner, Head of Forensic Technology, Asia Pacific, Advisory, Cyber, Advisory
KPMGシンガポール

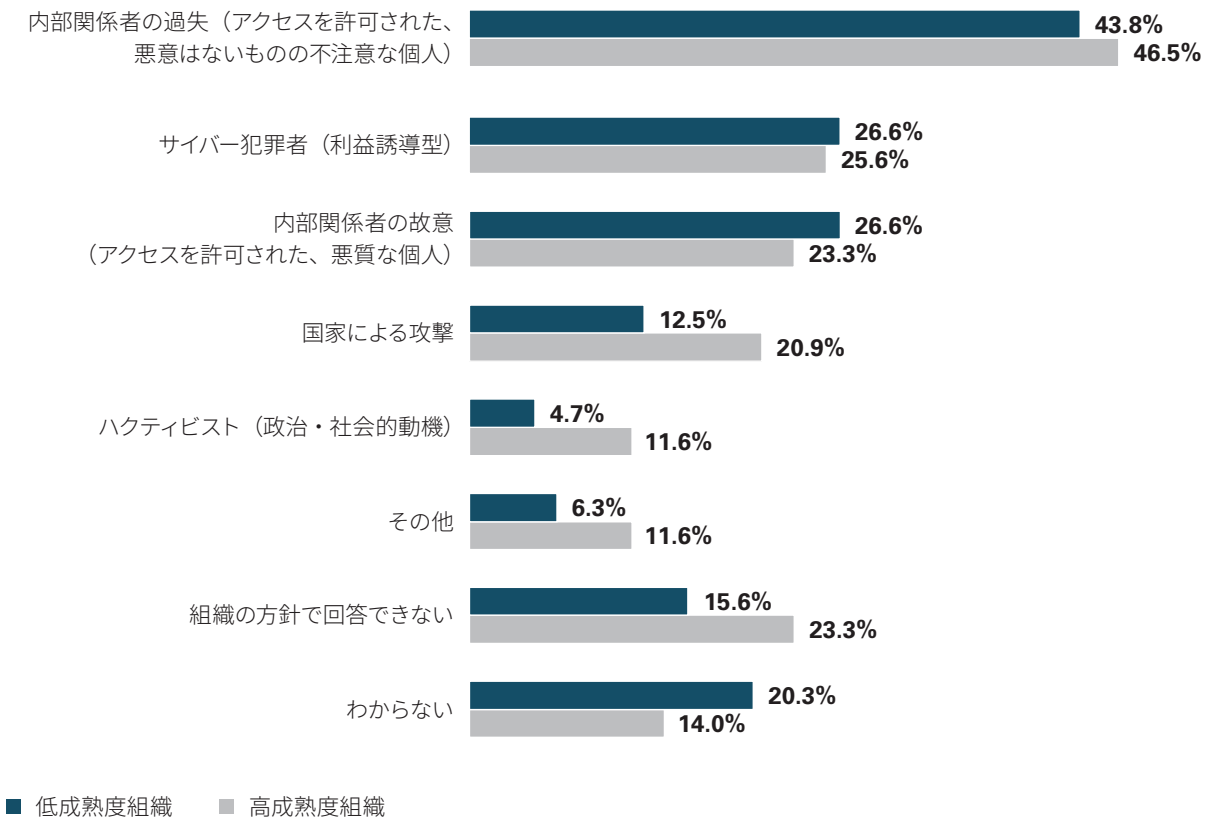
脅威アクター

「内部関係者の過失」は、制御システムセキュリティ侵害において、最も一般的に認識されている脅威要因の1つです。アクセスを許可された、悪意がないものの不注意な個人が、その性質上、システムやプロセスに混乱を引き起こすケースは往々にして発生しています。その可能性を減らすには、以下の2つのアプローチが必要です。

— 可能であれば、混乱を招く可能性のある行為をさせないためのセーフガードを導入する。状況や環境によっては、パラメータ制限、物理的な制御、または実行に移す際の第三者承認のチェックなどを行う。

— 技術的な運用とセキュリティ意識のコンポーネントを含むトレーニングにより、アクセスを許可された個人が、混乱を招くことなく自身の仕事を務める方法と、ミスをした場合に起こり得る被害の両方を確実に理解する。

最近発生した制御システムサイバーセキュリティ侵害における脅威アクターについて、すべて教えてください（高成熟度組織と低成熟度組織の比較）

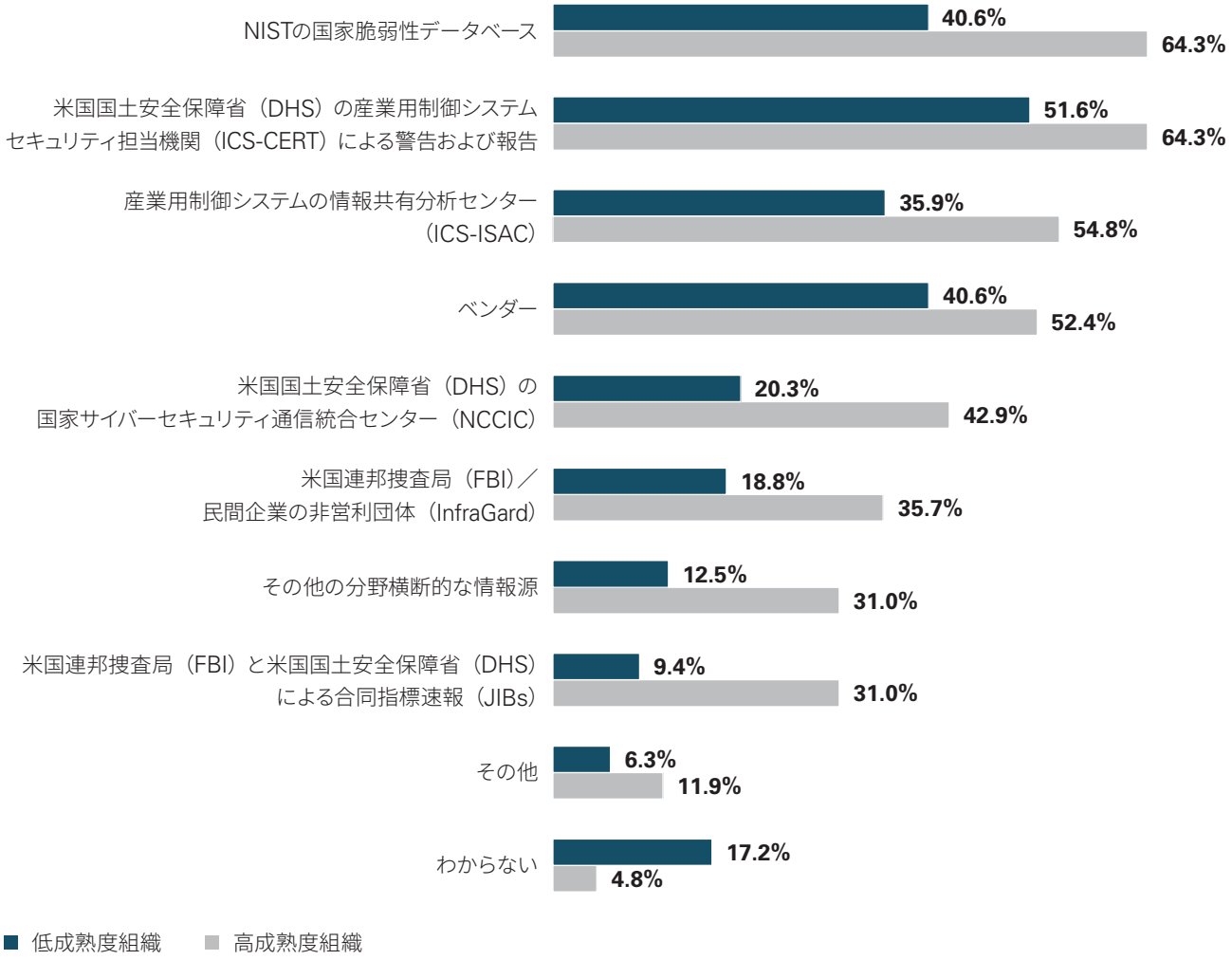


サイバー脅威に関する情報源

高成熟度組織は低成熟度組織と比べて「わからない」との回答が低く（高成熟度組織：4.8%、低成熟度組織：17.2%）、さらに選択肢以外の情報源（その他）の利用が約2倍近くあり（高成熟度組織：11.9%、低成熟度組織：6.3%）、より多くの情報源を把握し活用していることが明らかです。

高成熟度組織は、さまざまな情報源から得られる脅威インテリジェンスを有効活用することで、脅威の状況を見通すことができていると思われます。

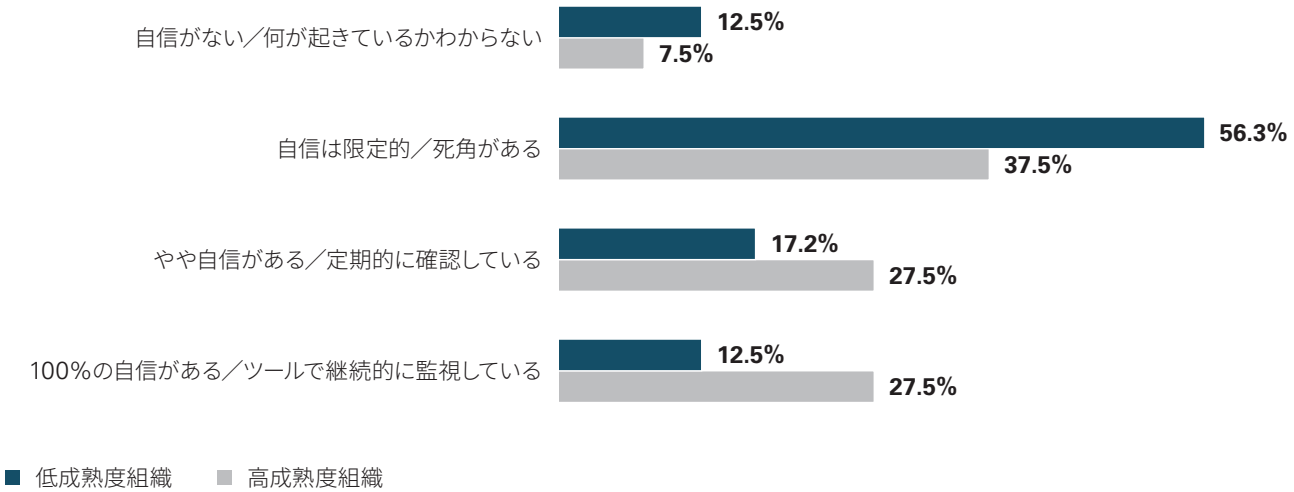
自組織が制御システムサイバーセキュリティ脅威に関する情報源として利用しているものを教えてください（高成熟度組織と低成熟度組織の比較）



ネットワーク可視化に対する自信

回答者の多くは、デバイス、アプリケーション、ユーザーのいずれについても、自組織のネットワークに何らかの死角があると認識しています。高成熟度組織は、自らが責任を負うべき領域で何が起きているかをより高いレベルで認識していますが、それでも約3分の2が「まだ確認すべきものがある」と考えています（高成熟度組織の合計65.0%が「自信は限定的／死角がある」「やや自信がある／定期的に確認している」のいずれかを回答）。昨今の中小企業のインシデントや現場に対するアセスメントから推測すると、100%の自信を持つ組織も、注意が必要です。

自組織のネットワーク上のデバイス、アプリケーション、ユーザーの可視化について、どの程度自信がありますか（高成熟度組織と低成熟度組織の比較）

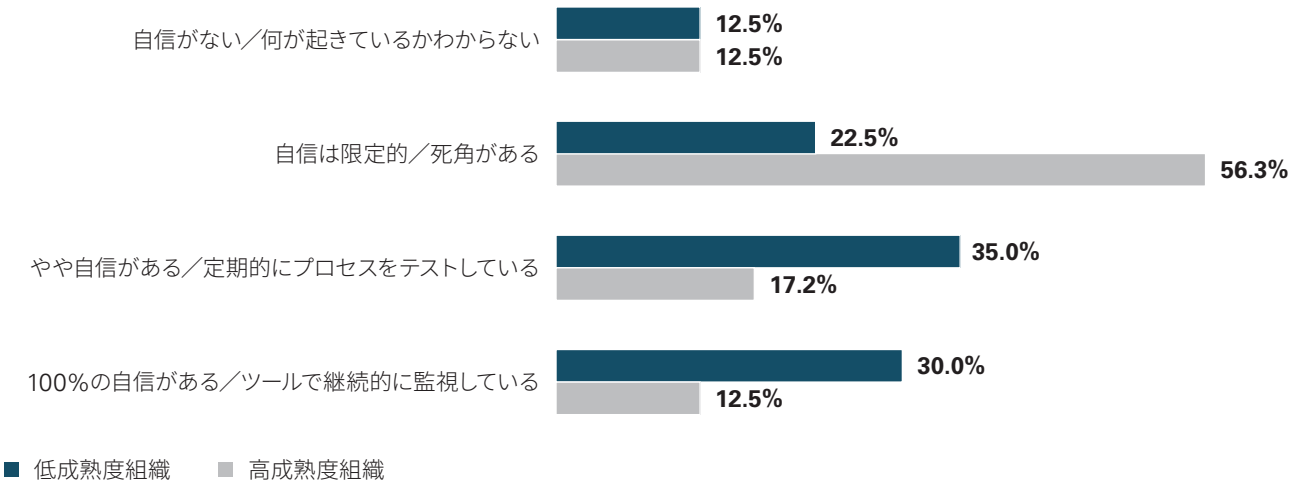


> ほとんどの組織で環境の複雑さが増し、規模が拡大しているため、ネットワークと資産の可視化には限界があり、完全に自信があるわけではありません。ネットワークの可視化には、アクティブなトラフィックモニタリングと独立したアーキテクチャレビューの2種類があると理解することが重要です。前者は、現場へのセンサーの配置が必要となり、数年かかることがよくあります。後者は、ファイアウォールやルーターの設定ファイルのみを必要とするセンサーレスネットワークモデリングソリューションを用いて実現できます。つまり、組織は後者を活用することで、ネットワークアーキテクチャをより迅速に、低コストで可視化できるのです。

Robin Berthier氏
CEO
Network Perception

サイバー攻撃対応プロセスへの自信

自組織がサイバー攻撃を受けた場合、その対応プロセスにどの程度自信がありますか（高成熟度組織と低成熟度組織の比較）



次年度の投資

多くの組織にとって特に重要なポイントである、OTサイバーセキュリティへの投資計画に対する回答を調べました。昨今、サプライチェーンに関する衝撃的な事件が数多く発生していることを考えると、この分野にリソースを集中させるという回答が少ないことが、最大の驚きと言えるでしょう。

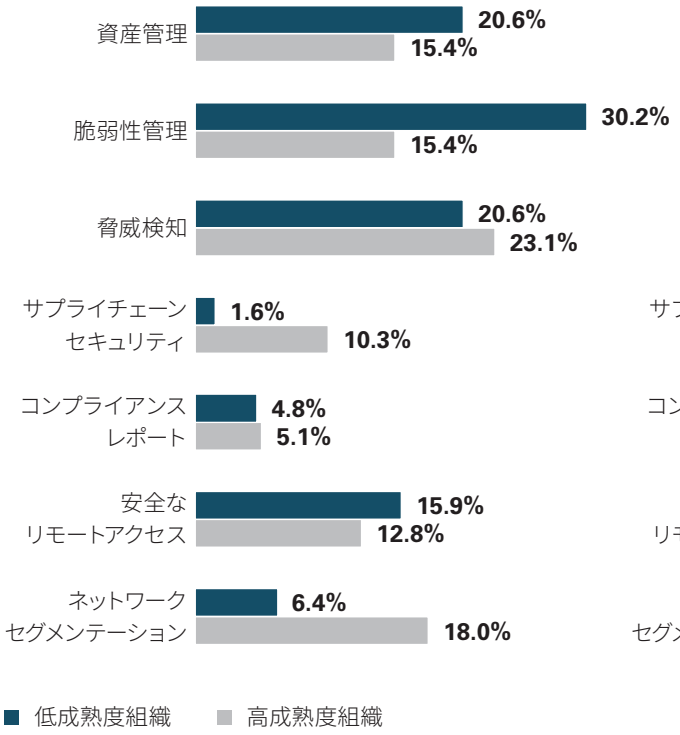
成熟度別でみると、低成熟度組織は基本的な「資産管理（20.6%）」および「脆弱性管理（30.2%）」については、高成熟度組織（それぞれ15.4%、15.4%）より必要性を認識していることが明らかです。また、両グループとも「脅威検知」の弱点に対処する予定で（高成熟度組織：23.1%、低成熟度組織：20.6%）、高成熟度組織は「ネットワークセグメンテーション」の実装にも重点を置いています（高成熟度組織：18.0%、低成熟度組織：6.4%）。

“脅威の増大や社会的圧力の高まりにもかかわらず、組織は準備不足のままです。その対応として、サイバーセキュリティ業界には無数のサービスがありますが、大多数が比較的新しく、未検証のものもあります。多くの組織は選択に迷い、結局は無防備の状態となっています。したがって、OT分野のセキュリティ確保に投資することは将来の産業ビジネスのための必須条件であり、文化、プロセス、人、技術における準備体制を構築することが重要です。既存システムの脅威を評価し、将来にわたって継続的に監視するために、サイバーセキュリティ機能を導入する必要があります。”

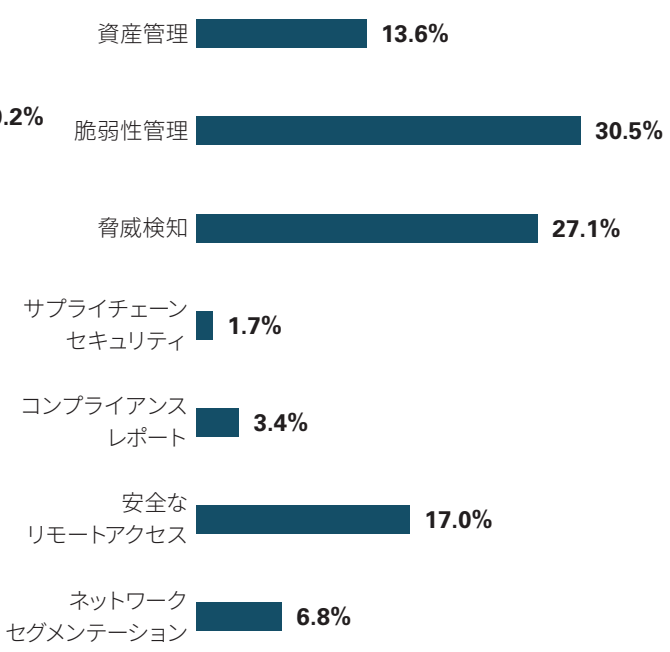
Hossain Alshedoki
Associate Director, IT/OT Cybersecurity & Data Privacy ENR Lead
KPMGサウジアラビア

次年度の投資について回答をみると、2つの分野（脆弱性管理：30.5%、脅威検知：27.1%）が特出しており、承認される投資領域は限られていることがわかります。

今後1年間に最も多く投資するOTサイバーセキュリティ施策を教えてください（高成熟度組織と低成熟度組織の比較）



今後1年間に最も多く投資するOTサイバーセキュリティの施策を教えてください（財務意思決定者／承認者の回答）



提言

CS 環境を保護するために推奨されるアプローチには、いくつかの重要なコンセプトがあります。まず、セキュリティは目的地ではなく、継続的に追求するものです。確実に安全であるという理想的な状態は、あくまでも仮説であり、現在の世界では達成できない可能性が高いと言えるでしょう。そこから派生して、セキュリティの中核的なミッションは、リスクを管理すること、すなわち許容レベルまで低減することであると考えます。このミッションのパラメータは、組織のリーダーによって確立されます。リーダーはリスク許容レベルを定義し、そのレベルと一致させるために必要なリソースを備えなければなりません。

万能な解決策はなく、組織のリーダーを導くための提言にも限界があります。しかし我々は、組織が可能な限り目標達成に向けて努力し続けることを推奨します。

— トレーニング、教育、組織内のセキュリティ文化の醸成と改善を通じて、従業員を育成する。これにより、インシデントの発生リスク、被害、復旧時間を削減できる。

— 資産管理とネットワークトラフィックの監視を改善することで、制御システム環境に対する洞察力を向上する。これにより、障害の発生する可能性と期間を削減できる。

— 制御システムのネットワークは非OTネットワークから隔離する。可能な場合は、OTネットワークをマイクロセグメンテーションする。これにより、インシデントの広がりを抑え、被害の範囲を縮小できる。

— サプライチェーンのセキュリティを調査し、システムへの侵入経路を制御する。これにより、サプライヤーへの攻撃が自組織に影響を及ぼす可能性を低減できる。

付録A：回答者属性

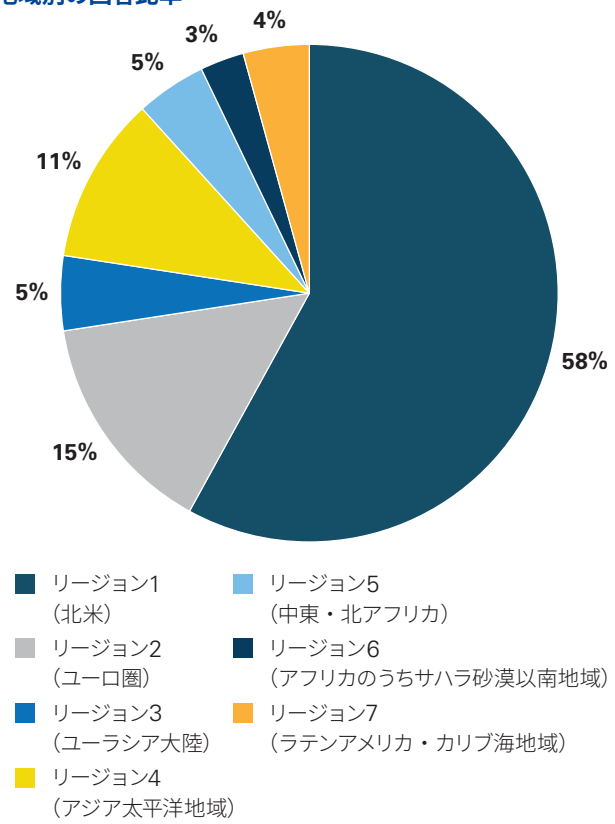
属性

所在地

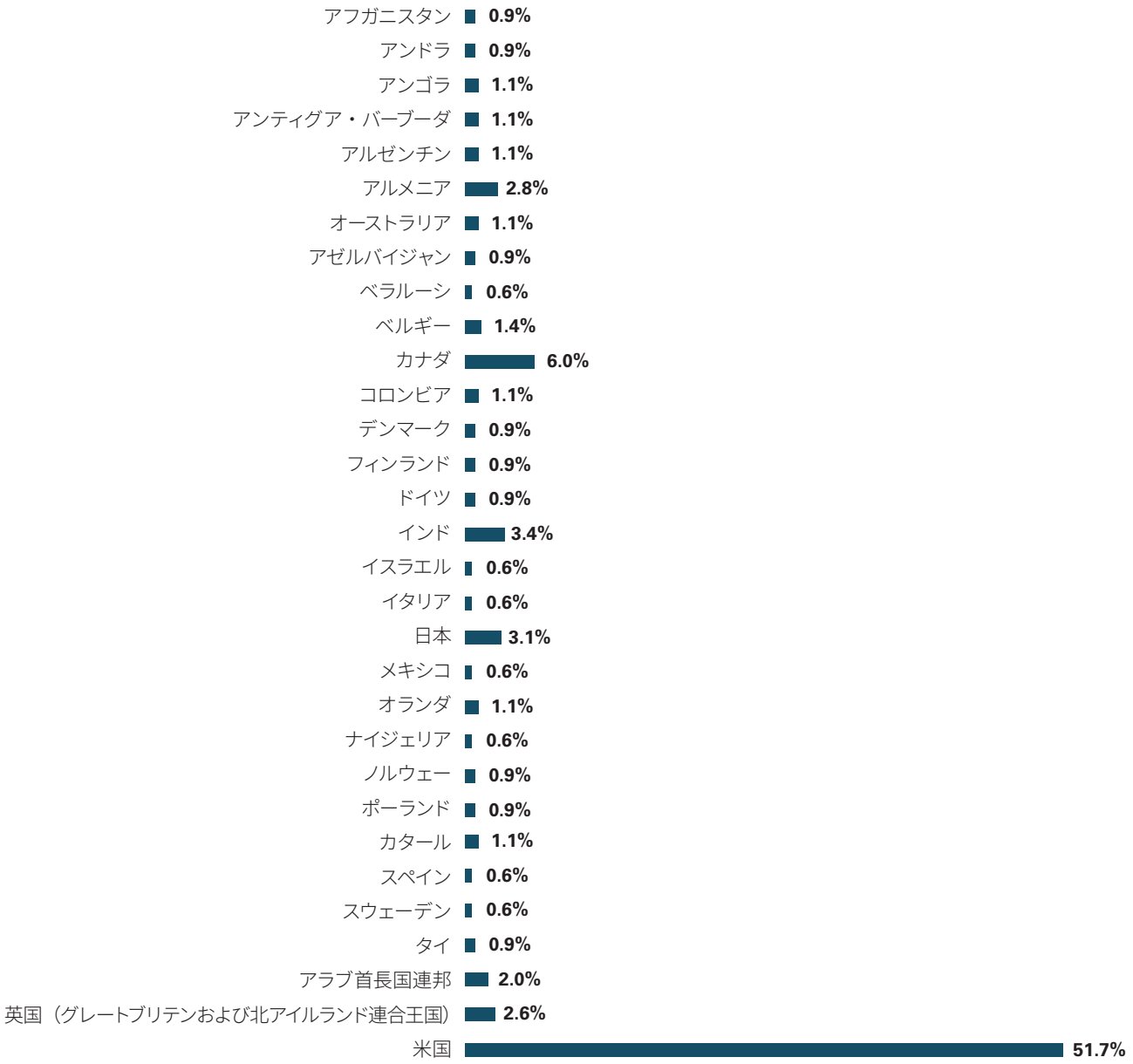
(CS)²AIでは、この1年間で会員数が20%以上増加しましたが、研究プロジェクトに参加する回答者の層はそれ以上に広がっており、北米で最も急速に拡大しています。絶対数では、私たちの目標であった、北米以外の国々からの回答が大幅に増加しました。しかし、米国とカナダからの回答がさらに増えたため、割合的にはこの地域が半分以上を占める結果となりました。

リストに記載している国名は、全回答の一部となります。

地域別の回答比率



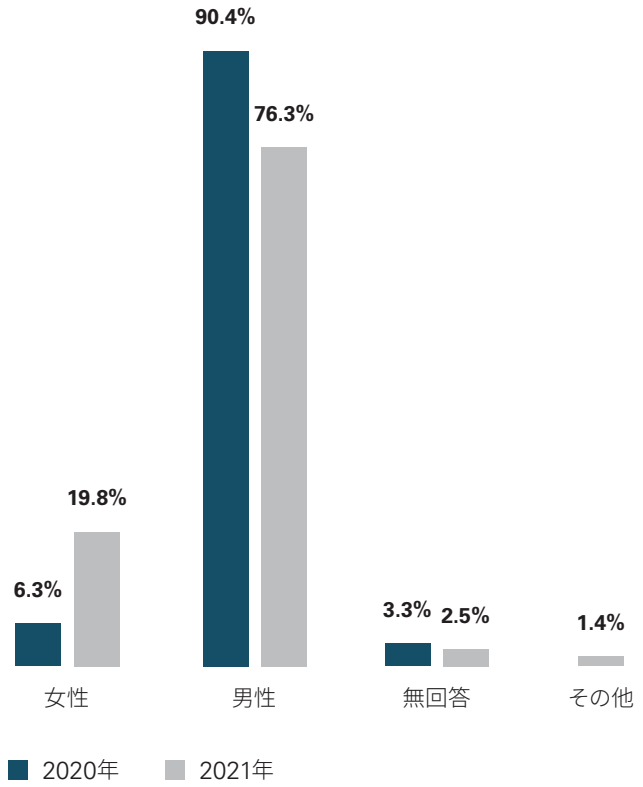
主な所在地を教えてください



性別

労働力不足に対応するためには、あらゆる層からの人材確保が必要であることは当然と言えます。2021年は、CSサイバーセキュリティの分野で働く女性の数が大幅に増え、前回調査よりも多くの方に参加していただけたことを嬉しく思います。これにより、性別間の視点の違いについて考察することができました。興味深い結果を挙げると、従業員規模が100～1,000人の組織で働く女性の割合が、およそ50%まで増加したことがわかりました。

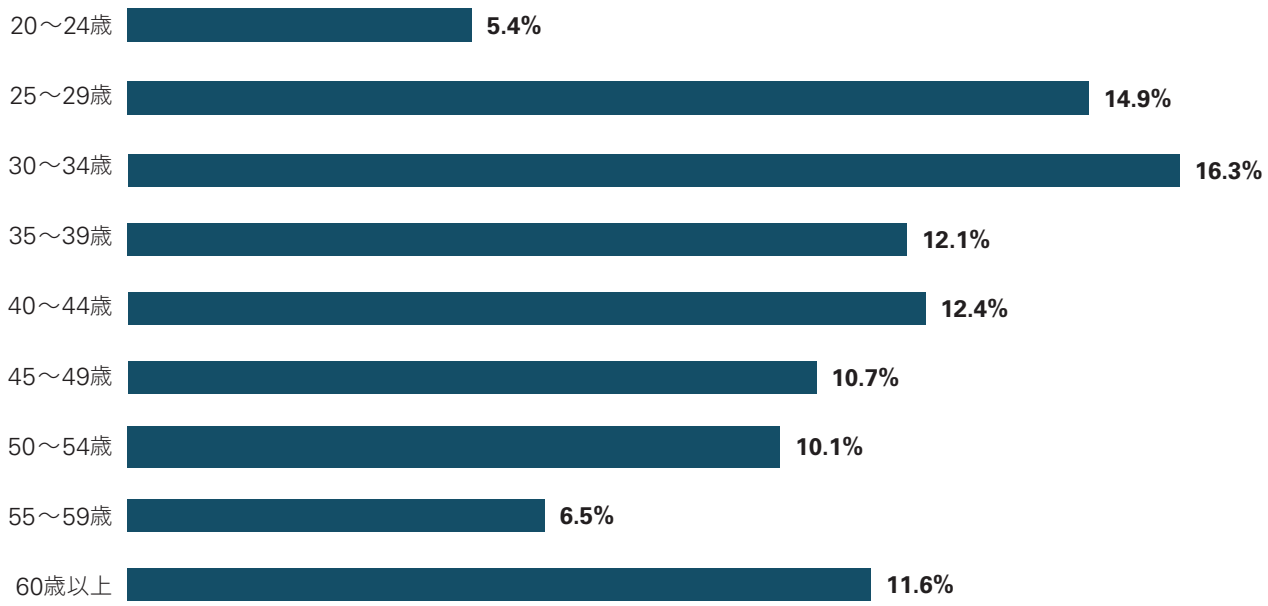
性別を教えてください

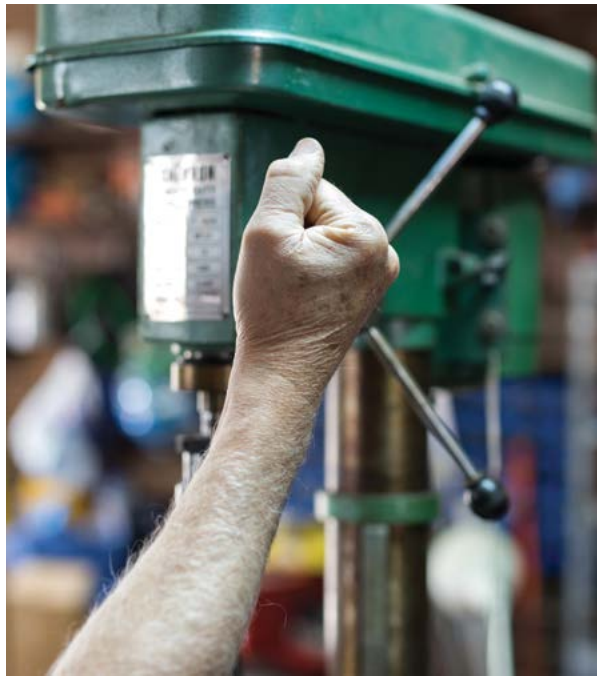


年齢分布

今回、若年層の回答者が大幅に増加したことは、ポジティブな兆候です。サイバーセキュリティの担当者が属する理工系人材の高齢化は頻繁に報告されており、組織的な知識の喪失と、需要の増加による人材の不足が懸念されています。特に米国のような先進国では、インフラやサプライチェーンの相互接続が急速に進んでいることに加え、技術者の世代交代が進んでいるため、その影響は顕著に表れています。このような背景のなか、今回の回答者の大半（61.1%）がキャリアの前半に位置し、残り数十年のキャリアにおいて、我々のミッションをともに果たしてくれることを大変嬉しく思います。

年齢を教えてください





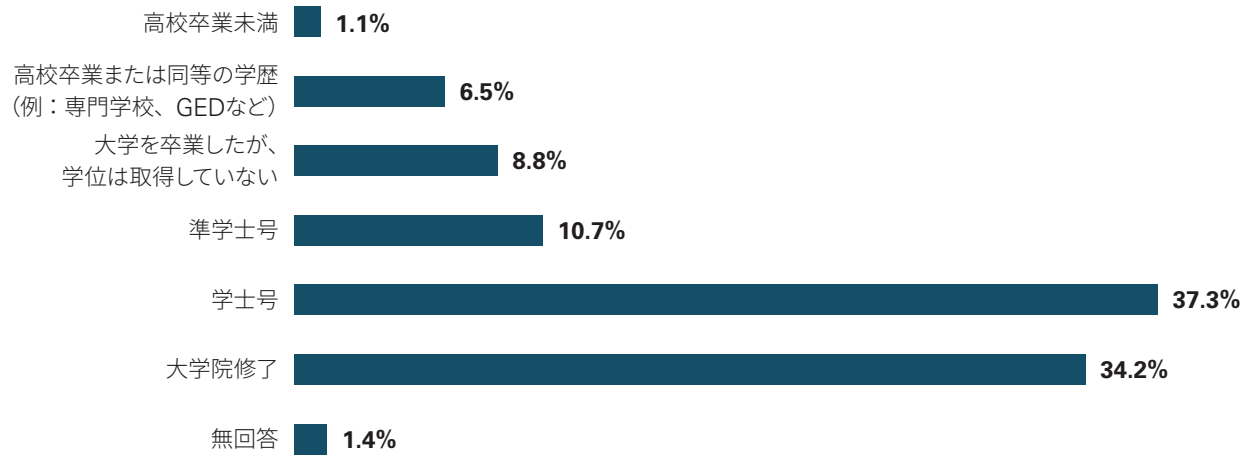
雇用形態

高価なOTシステムを使用しての学習には制約があり、技術トレーニングのコストも高いため、担当者の多くは雇用主を通じて学習機会を得ており、また雇用主にとってはこれが事業運営コストの一部となっています。回答者の大多数（59.8%）は、サイバーセキュリティの職責を果たしている組織の従業員として働いています。

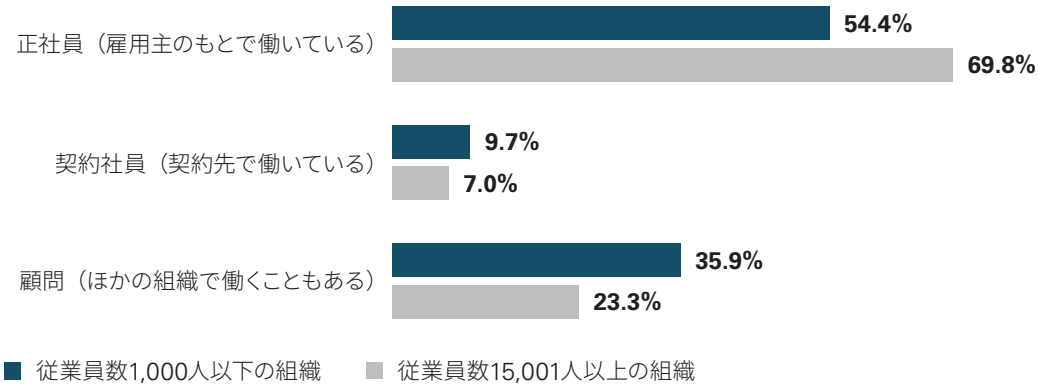
ただ、組織の規模によって多少の違いはみられ、従業員数が1,000人以下の組織では、顧問や契約社員の活用が増加していることがわかりました。このことから、これらの組織は財務的な制約が厳しく、サイバーセキュリティ業務に恒常的なリソースを割く余力が低下していると思われます。

学歴

最終学歴、または取得した最高学位を教えてください



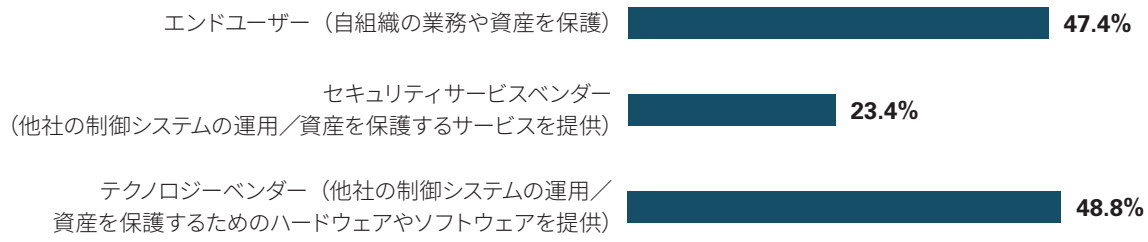
最も近い雇用形態を教えてください



組織カテゴリー

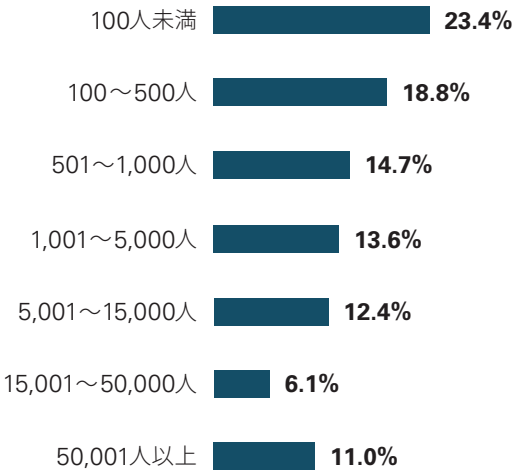
複数回答可の質問であるため、このグラフの回答合計は100%を超えています。

制御システムサイバーセキュリティに関して自組織のカテゴリーを教えてください



従業員規模

自組織の従業員数の規模を教えてください



付録B：年次報告書運営委員会

Derek Harp

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

Bengt Gregory-Brown

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

John Merkel

(CS)²AI Lead Data Analyst, Annual Survey & Report Lead Data Scientist

Walter Risi

(CS)²AI Strategic Alliance Partner Liaison, Survey Design and Report Analysis Teams Global Cyber IoT Leader KPMGアルゼンチン

コミュニティ全体を代表して、(CS)²AIより、2022年度年次報告書運営委員会の皆様に心から感謝申し上げます。質問項目の検討、調査ツールの発行支援、結果の分析、報告内容の準備・編集、そして最終報告書の配布に至るまで、右記のプロフェッショナル集団の尽力により、毎年の取組みが可能となっています。このことは、(CS)²AIの会員同士が支援し合う最も良い例の1つです。

Brad Raiford
Survey Design and Report Analysis Teams
KPMG米国

Hossain Alshedoki
Report Analysis Team
KPMGサウジアラビア

Eddie Toh
Report Analysis Team
KPMGシンガポール

Jaco Benadie
Report Analysis Team
KPMGマレーシア

Sandra Cusato
Report Production Lead
KPMGインターナショナル

Andrew Ginter
(CS)²AI Strategic Alliance Partner Liaison, Survey Design and Report Analysis Teams
Waterfall Security Solutions

Bryan Singer
Report Analysis Team
Accenture

William Noto
Report Analysis Team
Fortinet

George Kalavantis
Report Analysis Team
Industrial Defender

Robin Berthier
Report Analysis Team
Network Perception

William Malik
Report Analysis Team
Trend Micro

Ron Indeck
Report Analysis Team
Q-Net Security

Keith Beeman
Report Analysis Team
Tempered

Rick Kaun
Report Analysis Team
Verve Industrial

Richard Springer
Report Analysis Team
Tripwire

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

(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25,000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世界随一の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。

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

(CS)²AIは、この年次報告書の作成に継続的な貢献をいただいている戦略的アライアンスパートナーと、そして最も重要で欠かすことのできない、システムの保護に尽力いただいている世界中のサイバーセキュリティ担当者に、心からの感謝を申し上げます。

タイトルスポンサー

KPMG

編集スポンサー

Fortinet

Waterfall Security

Sable Lion Cyber

スポンサー

Applied Risk

Network Perception

Trend Micro

GBQ Partners

Q-Net Security

Tripwire

Industrial Defender

Tempered

Verve Industrial

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

home.kpmg/jp/kc

home.kpmg/jp/socialmedia

Designed by Evalueserve.
Publication name: (CS)²AI ― KPMG Control System Cyber Security Annual Report 2022
Publication number: 137866-G
Publication date: April 2022