KPMG

サイバーセキュリティサーベイ 2022

ご挨拶

2020年に新型コロナウイルス感染症（COVID-19）のパンデミックが起きたことにより、我々の働き方は一変しました。これまでリモートワークは限定的な働き方として整備されてきましたが、国や都道府県による外出自粛要請等により、リモートワークは広く普及しはじめています。

リモートワークやコミュニケーションツールの利用が浸透するなかで、サイバー攻撃は新たな局面を迎えており、二重脅迫型ランサムウェアなどによる被害がさらに拡がりを見せています。働き方の変化がサイバー攻撃をより複雑化させ、新たなリスクが生み出されています。

本調査によると、在宅勤務を少なからず導入している企業は全体の約75%を占めている一方で、リモートワークに関するサイバーセキュリティの対策方針を策定している企業は半分に満たない状況です。

このような情勢において「ゼロトラスト」という考え方が提唱されています。ゼロトラストとは、社内外すべてを「信用できない領域」としてセキュリティ対策を行うことです。リモートワークによって働く場所（ワークプレイス）がオフィスのみにとどまらず、社外と社内の区別が曖昧になっていることから、従前のセキュリティ対策で見られた、いわゆる「境界」で防御するという考え方が破綻しようとしています。

さまざまな問題を提起することになったCOVID-19は、サイバーセキュリティにおいても大きな影響を与えています。それが企業や組織の施策・計画に対してどのように影響したのかを知るために、本調査では新しい取組みとして、NISTのサイバーセキュリティフレームワーク（CSF）を意識した設問を構成して分析しました。

今年で5回目となる「サイバーセキュリティサーベイ」は、KPMGコンサルティングとKPMG FASが、デジタル化におけるサイバーセキュリティ推進のための有益な情報提供を目的として、調査を実施したものです。

本調査が少しでも皆さまのお役に立つことができれば幸いです。

最後になりましたが、本調査の実施にあたり、ご回答にご協力いただいた多くの皆さまに心から御礼申し上げます。

2022年1月

KPMGコンサルティング株式会社
執行役員パートナー
田口　篤

株式会社KPMG FAS
パートナー
上原 豊史

サイバーセキュリティサーベイ2022

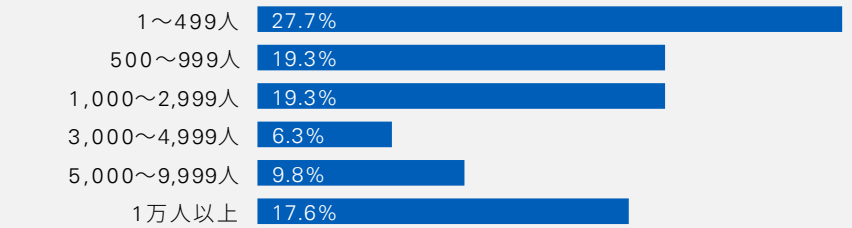
CONTENTS

調査概要

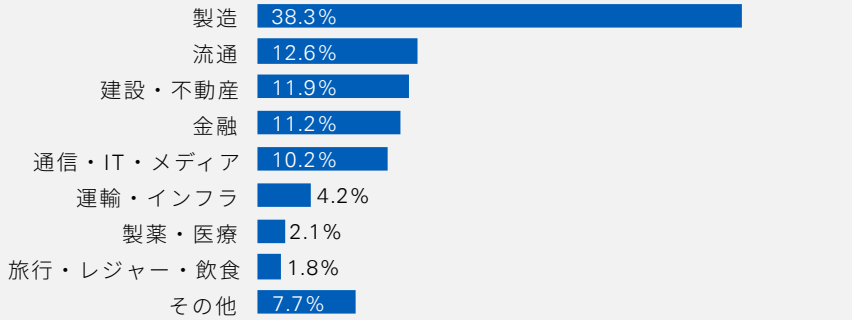
名称	企業のサイバーセキュリティに関する調査
対象	国内上場企業、および売上高400億円以上の 未上場企業のサイバーセキュリティ責任者
調査期間	2021年6月1日～7月31日
調査方法	郵送によるアンケート票の送付・回収、 ウェブによるアンケートの回収
発送数	3,960件
有効回答数	285 件（回収率 7.2%）

回答企業の属性

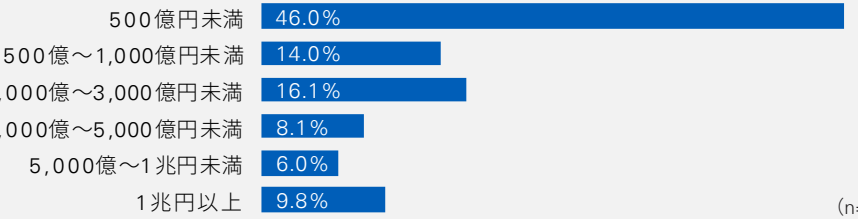
従業員数（連結）



業種



売上高（**2020年度**連結）



（n=285）

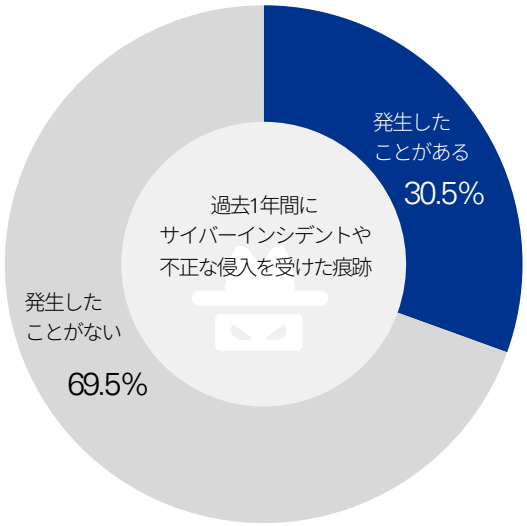
Executive Summary

テーマ 01

サイバーセキュリティ

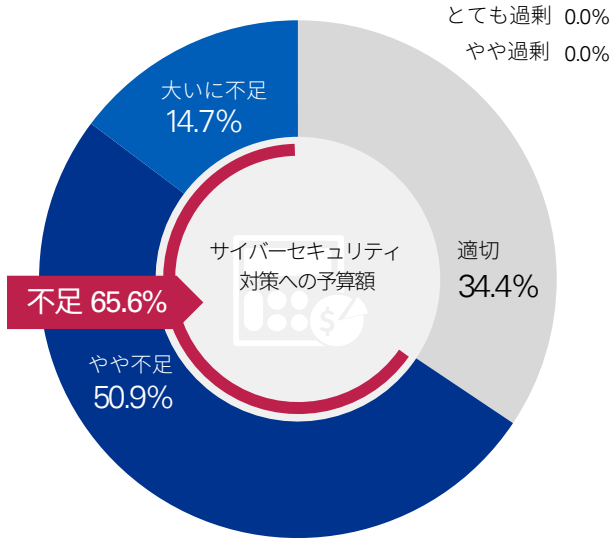
回答企業の30.5%がサイバーインシデントや不正侵入の痕跡を発見しており、サイバー攻撃が対岸の火事ではなくなってきています。一方、予算不足（65.6%）や情報セキュリティ人材不足（79.0%）が原因で、サイバーセキュリティ対策の導入がなかなか進まず、日々、高度化・複雑化し続けるサイバー攻撃への対応に苦慮している様子がうかがえます。

30.5% の企業が
サイバーインシデントや不正侵入の痕跡を発見



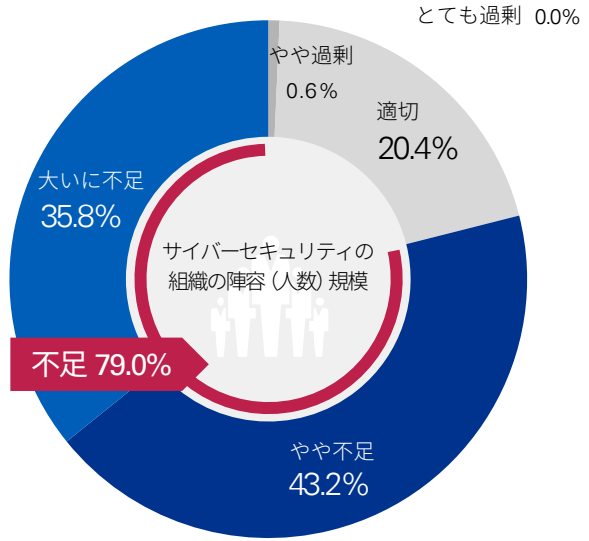
（n=285）

65.6% の企業が
サイバーセキュリティ対策への予算不足



（n=285）

79.0% の企業が
情報セキュリティ人材不足



（n=285）

Executive Summary

テーマ 01

サイバーセキュリティ

NISTのサイバーセキュリティフレームワーク（CSF）の5つの機能に沿って、回答の傾向を整理しました。

識別

回答企業の57.9%がサイバーセキュリティ対策の現状分析および対応計画の策定を、60.7%がセキュリティ監査を定期的に実施しておらず、サイバーセキュリティ管理におけるPDCAサイクルにおいて計画（Plan）と監査（Check）に改善の余地があります。

また、52.7%が業務委託先へのセキュリティ対策の要請を未実施または未把握でした。近年、サプライチェーンの脆弱性を突いて侵入するサイバー攻撃が発生しているため、委託先・提携先等の**サプライチェーンを含めたサイバーセキュリティ管理**の仕組みづくりが必要です。

防御

回答企業の注目領域は、**高度なエンドポイントセキュリティ対策**（積極的に導入を検討35.4%、導入済み55.1%）と、**クラウドセキュリティ対策**（同35.1%、26.7%）です。リモートワークの浸透とクラウドサービス利用の拡大により、境界型セキュリティからゼロトラストセキュリティへの転換が喫緊の課題になっていると考えられます。

検知

回答企業の約半数（54.4%）がSOC(Security Operation Center)を導入していません。防御系のセキュリティ対策製品の導入状況と比較して、ユーザー／エンティティの行動分析（UEBAなど、10.9%）の導入率が低く、**セキュリティ監視機能の高度化**の余地が見込まれます。

対応

回答企業の34.4%がCSIRT（サイバー攻撃による情報漏えいや障害などに対処するための組織やチーム）を設置しており、47.4%が初動対応手順を準備しています。しかし、セキュリティ運用の自動化（SOARなど、8.1%）の導入率は低くなっています。**セキュリティ運用の自動化**は、情報セキュリティ人材不足への対応として、今後の浸透が期待される領域です。

復旧

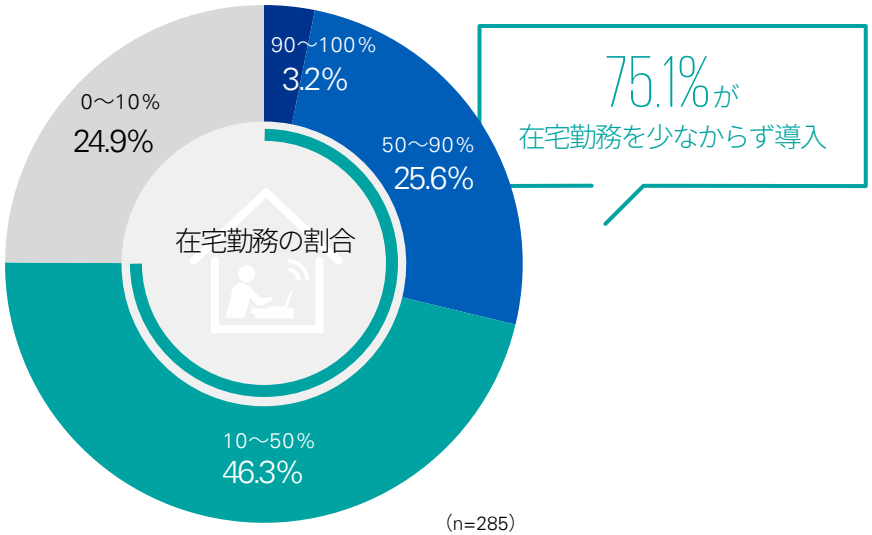
回答企業の42.5%が復旧手順を準備しており、32.6%がメディアへの連絡や広報の手順を準備しています。復旧対応については、51.7%が約1週間程度で対応が完了していますが、数日間遮断した場合の業務継続の対応をあらかじめ定めている企業は約23%にとどまっています。

復旧手順に加えて、**事業継続や業務継続の対応計画の策定**が求められています。

テーマ
02

リモートワークセキュリティ

COVID-19によるリモートワークを中心とした働き方の変化によって、回答企業のうち75.1%が在宅勤務を少なからず導入しています。また、50.5%が従業員による内部不正を懸念しており、在宅勤務率が高いほど、内部不正を懸念する企業が多い傾向が見られました。過半数の企業でハードディスクの暗号化、USB接続の制限・禁止、モバイルデバイス管理（MDM）によるスマートフォン等のリモート消去など、端末からの物理的な情報漏えいへの対策が講じられている一方で、メール・ウェブ・クラウド経由の情報漏えい対策（DLP）は17.3%にとどまり、あまり普及していない状況が見受けられます。

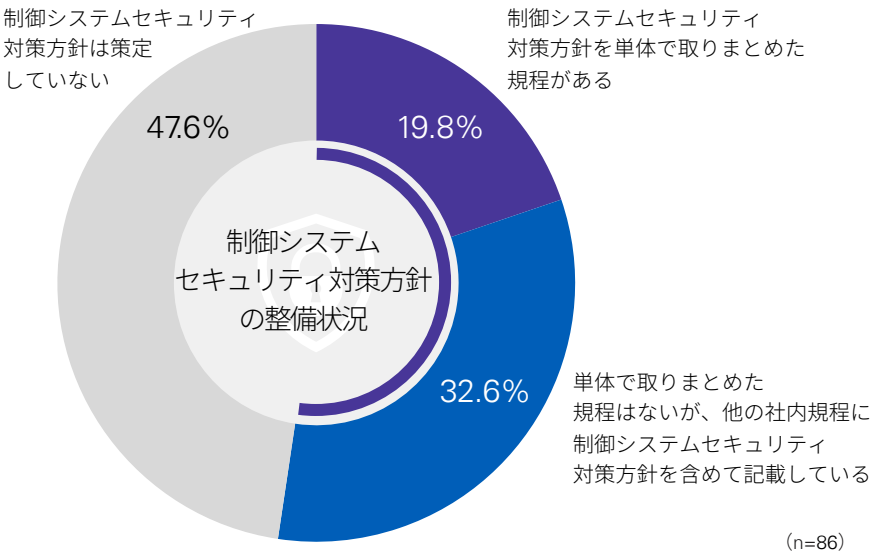


（n=285）

テーマ
03

制御システムセキュリティ

日本の製造業が抱える課題の解決策として、スマートファクトリーへの取組みはますます加速しています。一方、工場のスマート化によるサイバー攻撃のリスク増大への懸念もあり、制御システムセキュリティ対策の導入について苦慮する企業も増えています。方針の策定や具体的な対策の導入が求められています。



（n=86）

テーマ

01

サイバーセキュリティ

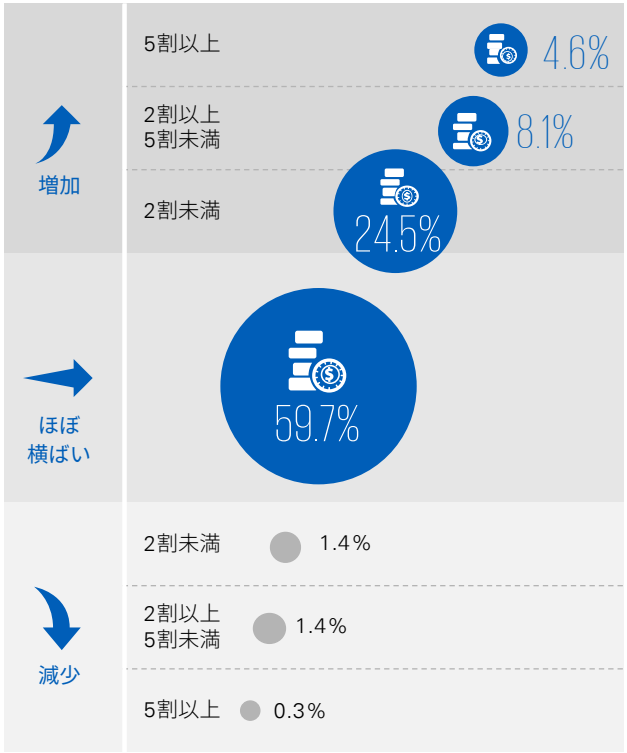
サイバーセキュリティ対策への年間投資額

識別 防御 検知 対応 復旧

2021年度のサイバーセキュリティ対策への投資額は、2020年度に比べて横ばい、もしくは増加と答えた企業が96.9%に上り、全体としては増加傾向にあります。しかし、IT予算におけるサイバーセキュリティ対策予算の比率が10%未満の企業は62.1%で、65.6%の企業が投資額が十分ではないと回答しています。

2021年度と2020年度の投資額比較

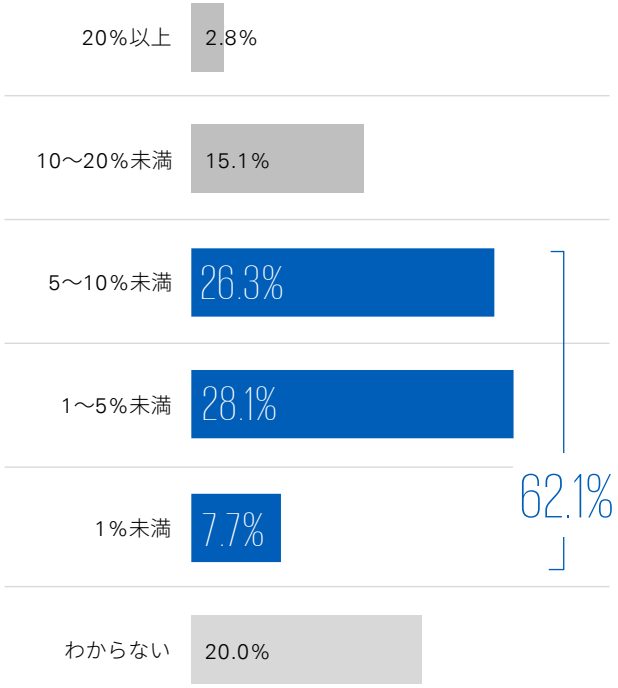
サイバーセキュリティ対策への投資額は増加傾向



(n=285)

IT予算におけるサイバーセキュリティ対策予算

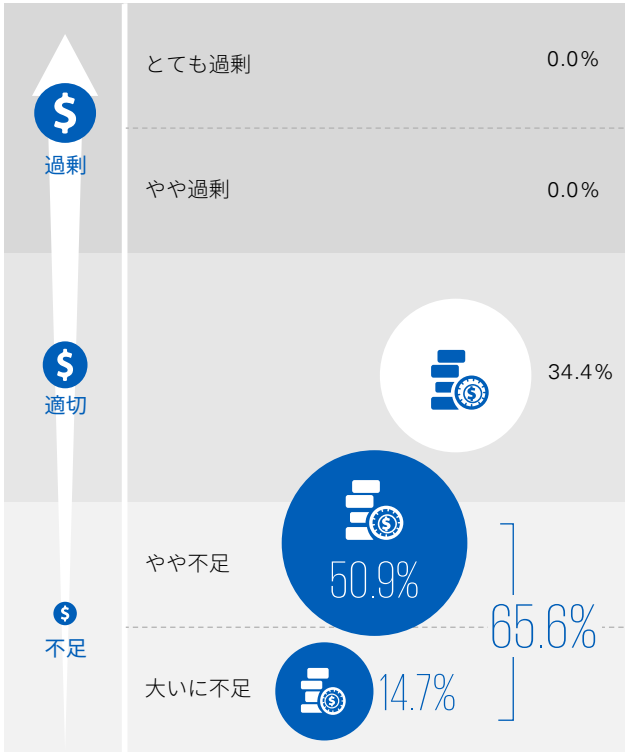
62.1%がIT予算の10%未満



(n=285)

2021年度の投資規模

65.6%が投資額の不足を感じている



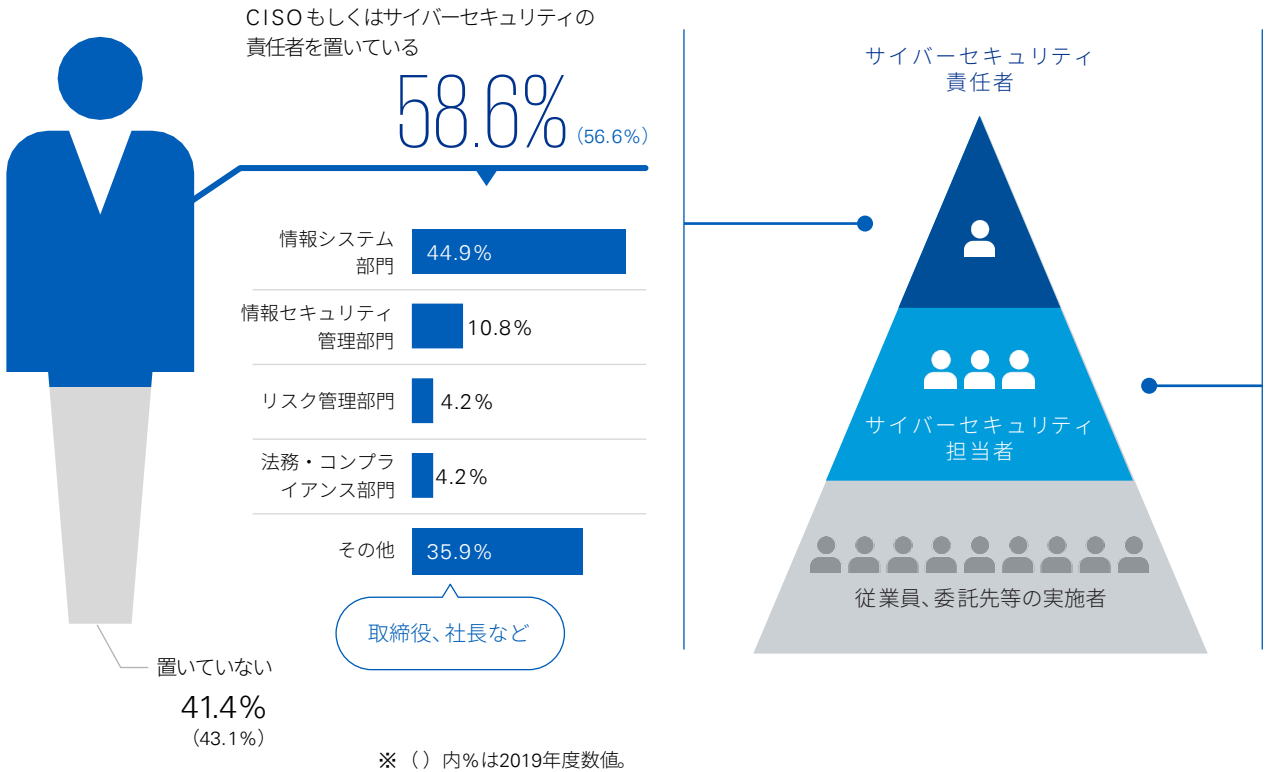
(n=285)

サイバーセキュリティの責任者・担当者

識別　防御　検知　対応　復旧

回答企業の58.6%が最高情報セキュリティ責任者（CISO）もしくはサイバーセキュリティの責任者を設置し、
76.1%がサイバーセキュリティ対策の担当者を設置しています。
前回（2019年）の調査と比較して、責任者の設置は2.0%増加、担当者の設置は21.3%増加しています。

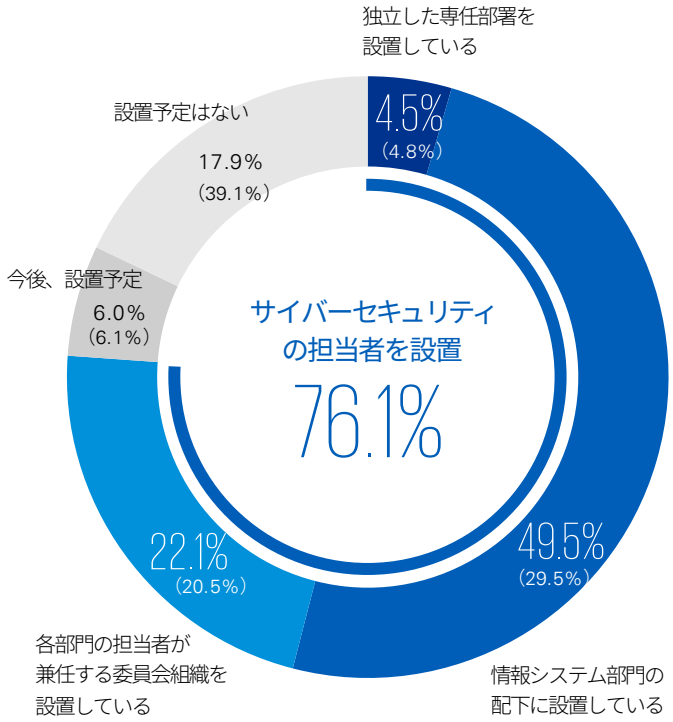
CISOもしくはサイバーセキュリティの責任者の設置



※（）内%は2019年度数値。
2019年は0.3%が無回答

（n=285）　（n=313）

サイバーセキュリティの担当者の設置



※（）内%は2019年度数値

（n=285）

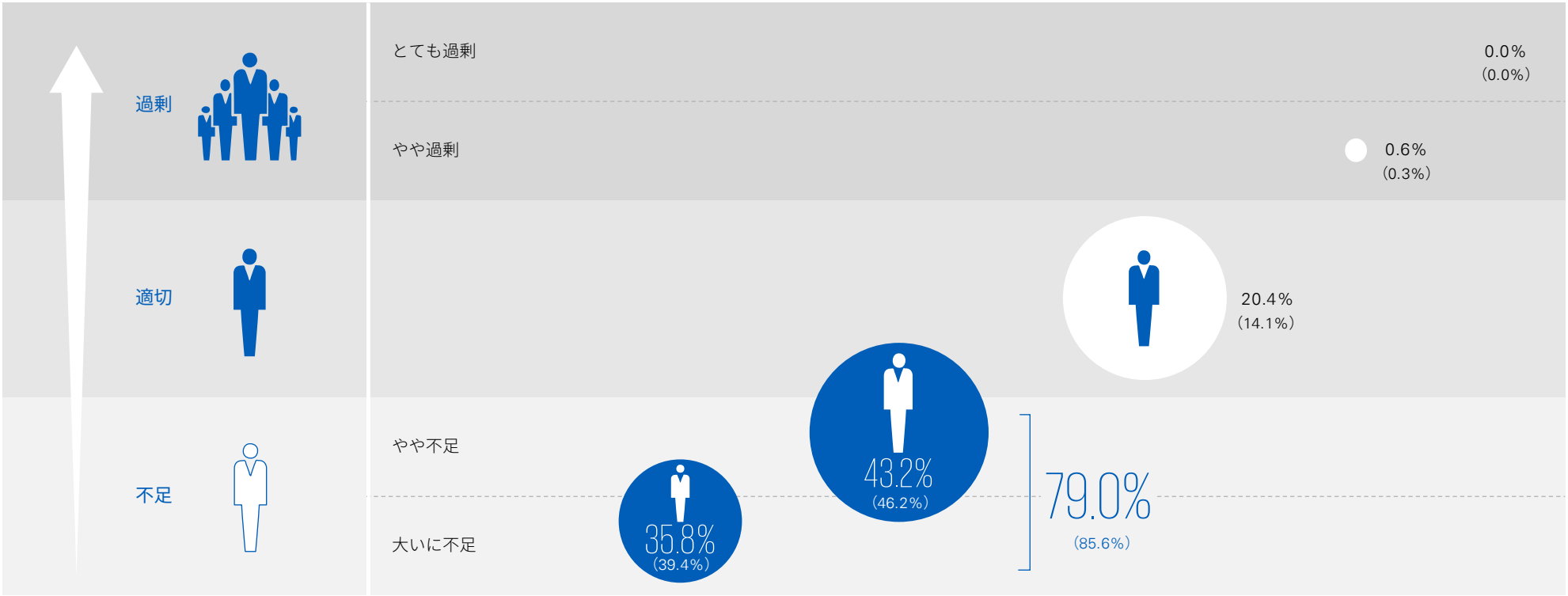
情報セキュリティ人材

識別 防御 検知 対応 復旧

サイバーセキュリティ対策のための体制はあるものの、79.0%の企業が人材不足と回答しています。
前回（2019年）調査と比較して6.6%の改善が見られるものの、依然として情報セキュリティ人材不足の状況が続いています。

サイバーセキュリティ対策組織の陣容（人数）規模

79.0%が人材不足を感じている

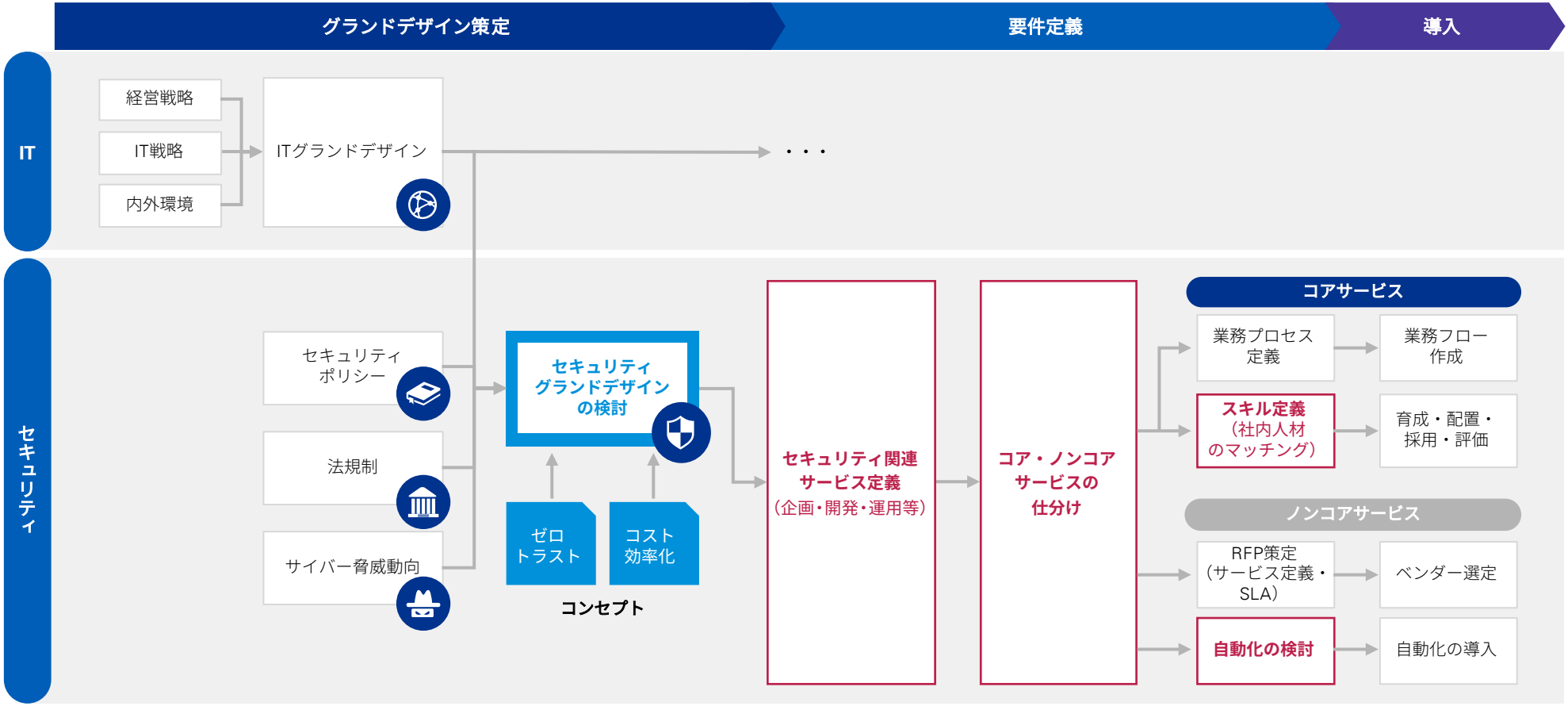


※（）内%は2019年度数値。2019年は0.4%が無回答　(n=285)

COLUMN

セキュリティ業務・要員配置の最適化

情報セキュリティ人材の不足が続くなか、限られたリソースで最大限の成果を発揮するためには、選択と集中が欠かせない。
セキュリティグランドデザインを描き、その実現に求められるサービス（＝業務）を定義。これらを、将来的にコアコンピタンスとして伸ばしていくコアサービスと、積極的にアウトソースしていくノンコアサービスに仕分け、コアサービスは社内人材の活用を、ノンコアサービスはアウトソースの活用を検討することが考えられる。



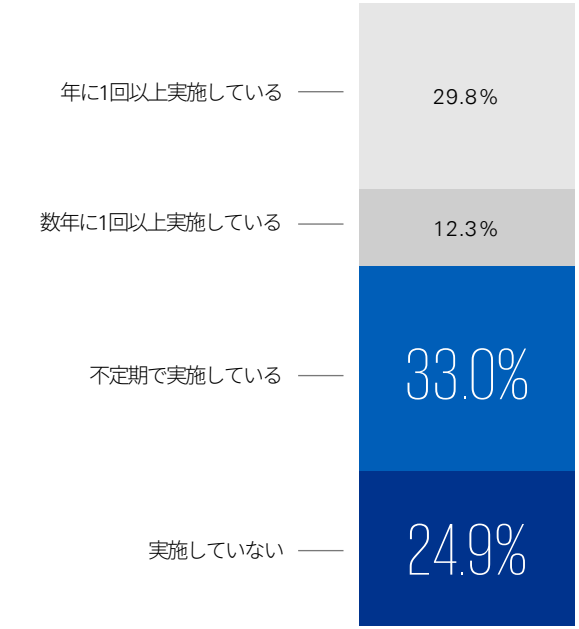
サイバーセキュリティ対策の継続

識別 防御 検知 対応 復旧

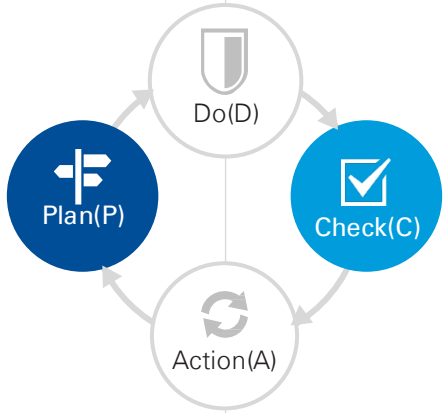
サイバーセキュリティ対策の現状分析および対応計画の策定（Plan）で57.9%、監査（Check）で60.7%の企業が「不定期に実施」もしくは「実施していない」と回答しており、サイバーセキュリティ管理におけるPDCAサイクルに改善の余地があります。

サイバーセキュリティ対策の現状分析および対応計画の策定（Plan）

33.0%が不定期に実施し、24.9%が実施していない

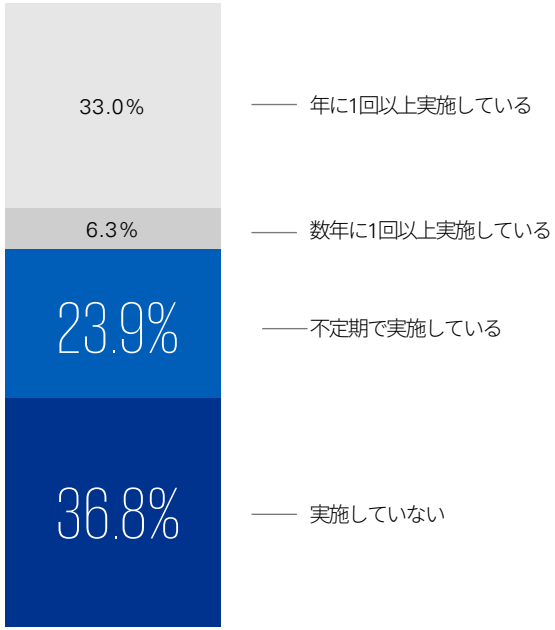


（n=285）



サイバーセキュリティ対策状況に関する監査の実施（Check）

23.9%が不定期に実施し、36.8%が実施していない



（n=285）

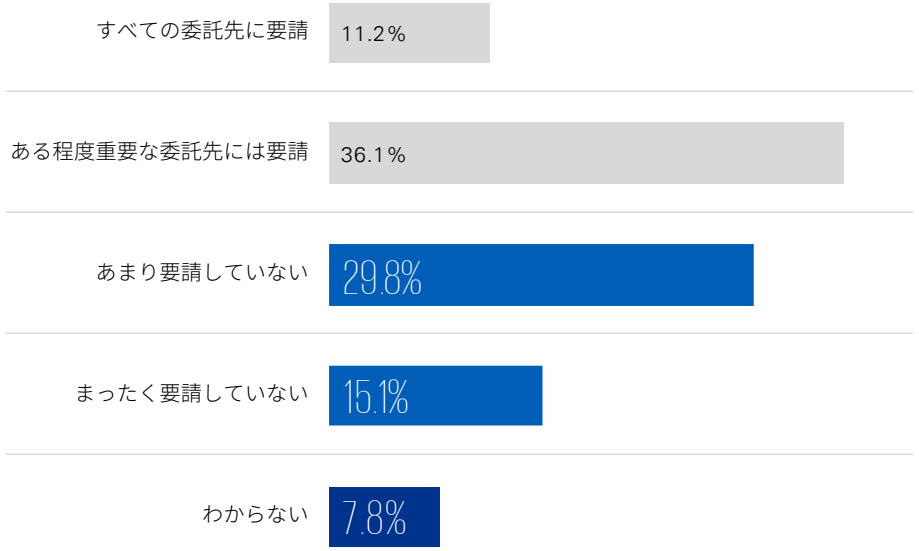
業務委託先の管理

識別 防御 検知 対応 復旧

未把握を含めると、52.7%の企業が業務委託先へのセキュリティ対策を要請できていません。
委託先におけるセキュリティ対策状況の確認方法は、76.3%が調査票（紙、Excel、PDF等）を使用している一方、サードパーティリスク評価サービスを利用している企業は4.4%にとどまり、GRC（ガバナンス・リスク・コンプライアンス）のツールは使用されていません。

業務委託先に対するセキュリティ対策の取組みの要請状況

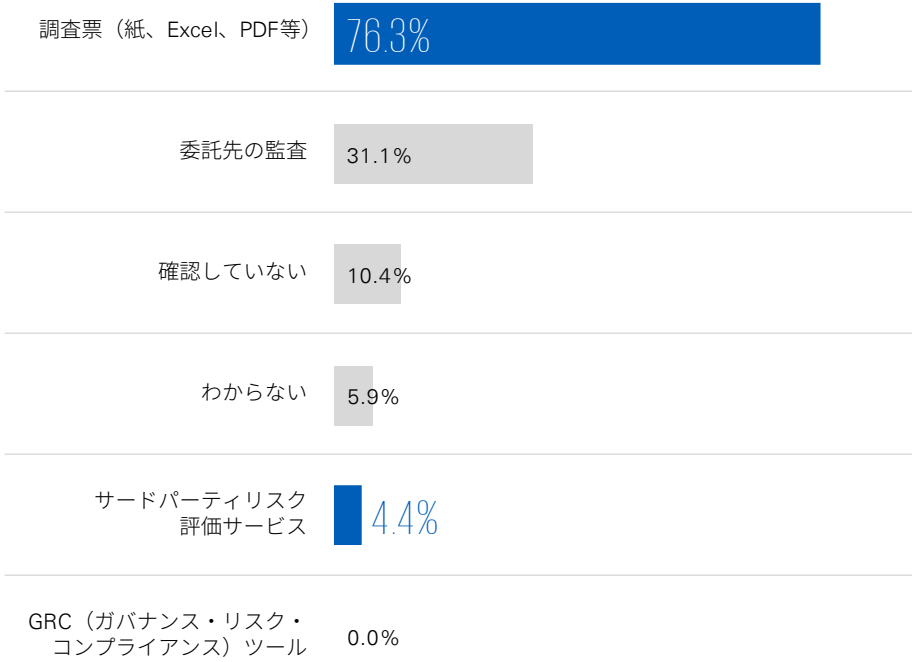
29.8%があまり要請しておらず、15.1%が未要請、7.8%が把握していない



（n=285）

業務委託先におけるセキュリティ対策状況の確認方法

76.3%が調査票を、4.4%が外部サービスを利用、GRCツールは使用されていない



（複数選択可／n=135）

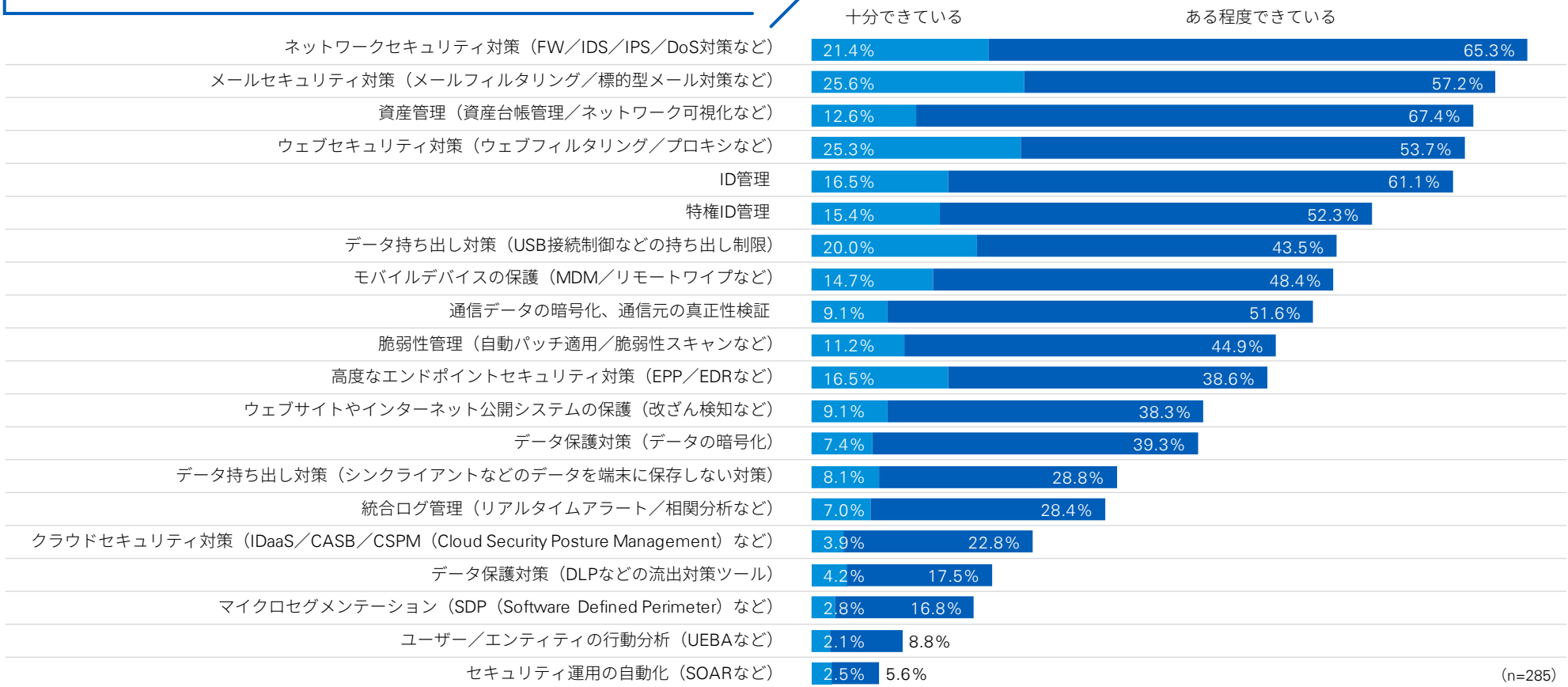
サイバーセキュリティ対策の実施状況

識別 防御 検知 対応 復旧

ネットワークセキュリティ、ウェブセキュリティ、メールセキュリティなど、従来からある対策に比べて、
ユーザー／エンティティの行動分析（UEBA）、セキュリティ運用の自動化（SOAR）など新しい領域の対策が進んでいない傾向が見られます。

サイバーセキュリティ対策の実施状況

UEBA、SOARなどの新しい領域に取り組んでいる企業は1割程度となっている



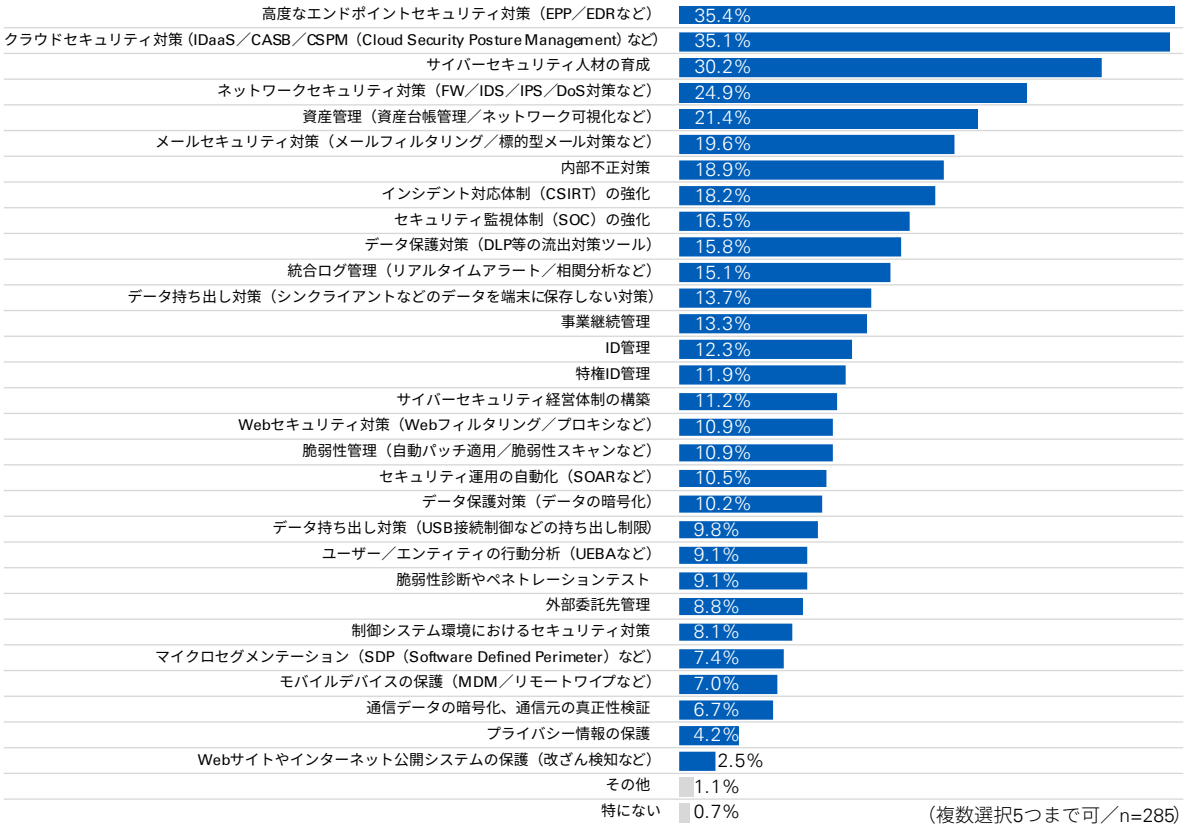
今後の投資を要するサイバーセキュリティ対策領域

識別 防御 検知 対応 復旧

約35%の企業が高度なエンドポイントセキュリティ対策やクラウドセキュリティ対策を急務ととらえています。
72.6%の企業が、サイバーセキュリティ対策に取り組むうえでの課題として、サイバーセキュリティ人材の不足を問題視しています。

今後、より積極的に取り組みたいと考えているサイバーセキュリティ対策領域

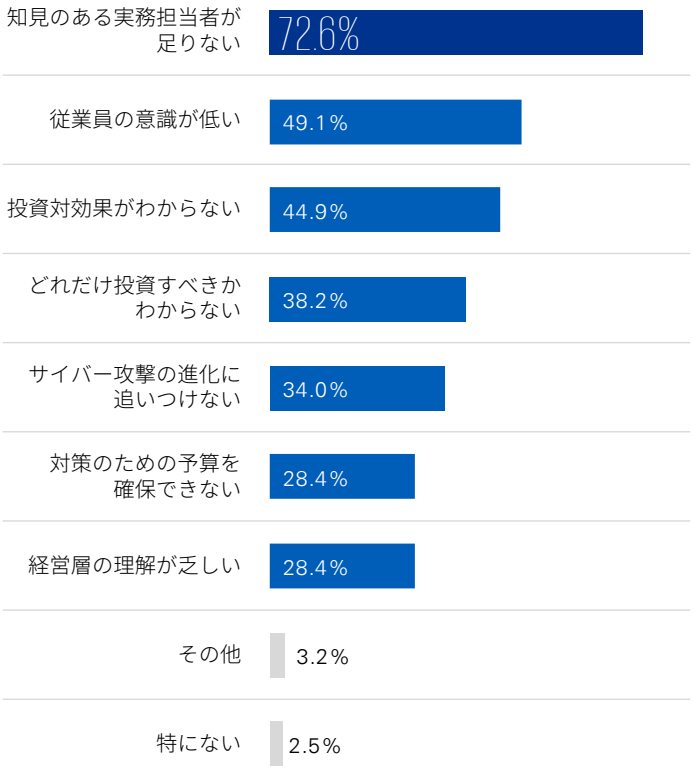
高度なエンドポイントセキュリティ対策、クラウドセキュリティ対策が最優先の課題となっている



（複数選択5つまで可／n=285）

サイバーセキュリティ対策に取り組むうえでの課題

サイバーセキュリティ人材の不足が課題となっている



（複数選択可／n= 285）

COLUMN

ゼロトラストセキュリティの現実解

リモートワークの浸透とクラウドサービス利用の拡大により、境界型セキュリティからゼロトラストセキュリティへの転換が必要となってきているが、導入が進んでいない対策も多い。

- 原則は多層防御（Defense in Depth）
- ネットワークだけでなく、認証・認可、監視等の対策を多層で取り込むことで、防御・検知のポイントを増やすことが肝要
- 増大する運用管理を効率的に回す仕組みの構築と運用が課題

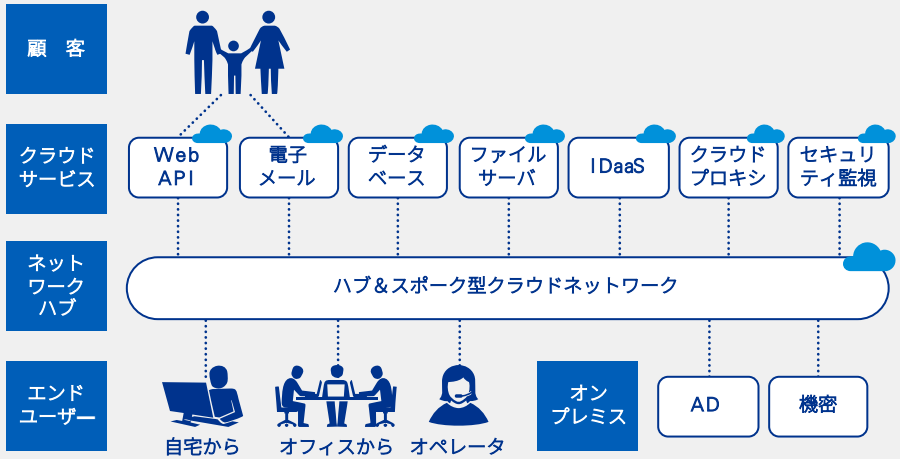
セキュリティ対策の原則は多層防御（Defense in Depth）にあることは変わりはない。エンドポイントでの対策が鍵。

マイクロセグメンテーションに始まるネットワークアーキテクチャの見直しから、認証・認可の仕組み、データ保護、監視といった多層での防御・検知の仕組みの整備が「ゼロトラスト」におけるセキュリティの維持に必要。
通信内容に基づく防御・検知策はTLS／SSL等による暗号化通信の増大に伴い効果が薄れてきているため、エンドポイントやサービスエンド（サーバやクラウド等）での対策の増強が求められる（プロキシによる暗号通信の復号はボトルネックとなりやすい）。

考慮点	ゼロトラストセキュリティの考え方	セキュリティ対策例
デバイス	• デバイスは内部に限らず、どこにでも存在する • デバイスの認証を常に実施する • すべてのデバイスの保護を徹底する	• EDR・EPP • MDM
ID・ユーザー	• 内部・外部を問わずID・ユーザーを必ず検証する • ユーザーIDを多要素認証で検証する	• IAM • PAM
アプリケーション	• 内部・外部を問わずアプリケーションへのアクセスを制限し、不正操作を監視する	• CASB • 標的型メール対策
通信	• 内部の通信も厳密に制限する • 内部・外部を問わず、送信元の検証、通信の真正性を確保する	• マイクロセグメンテーション • SDP（Software Defined Perimeter） • 通信の認証、暗号化
データ	• 情報資産はクラウドなどの外部にも存在する • データが改ざんされないように保護する • データが漏えいしないように保護する	• データの暗号化 • DLP
監視・ログ	• 内部・外部を問わず脅威に対する監視・ログ分析によって可視化する • セキュリティ対応を自動化する	• CASB • SIEM・UEBA • SOAR

防御策や検知策の運用管理の煩雑化による障壁でつまずくことが多い。自動化やアウトソースの利用が解決策として浮上。

プロキシによるボトルネックを回避するためにローカルブレイクアウトを検討する組織が増えている実感あり。しかし、必要な回線帯域の見極めや、ローカルブレイクアウトの統合管理（SD-WAN）、端末やマルチクラウドの統合監視などの障壁を乗り越えられずにいる組織が多く見受けられる。
セキュリティアーキテクチャ全体を見直すにあたっては、システム・ネットワークの利用実態の把握、クラウドとオンプレミスのバランスを考慮したグランドデザインの策定、最適なコストでの製品選定など、企業特性に合わせた姿を描く必要がある。



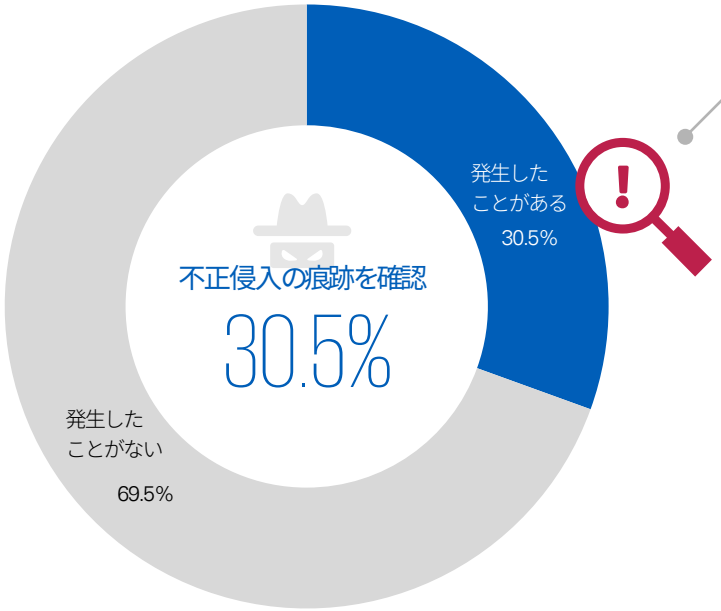
サイバー攻撃の発生状況と攻撃の種類

識別　防御　検知　対応　復旧

30.5%の企業において、サイバー攻撃の痕跡が確認されています。
被害を受けた攻撃としては、ランサムウェアがトップで26.4%の企業が被害を受けています。

サイバーインシデントや不正な侵入の痕跡

30.5%がサイバーインシデントや不正な侵入の痕跡を確認している



（n=285）

サイバー攻撃による被害

26.4%でランサムウェアによる実被害が発生している

ランサムウェア	26.4%
マルウェア	25.3%
ウェブサイトの改ざん	20.7%
ウェブサービスへの不正ログインや情報窃取	20.7%
フィッシング詐欺	19.5%
DDoS（サービス妨害）攻撃	19.5%
標的型攻撃	18.4%
不正送金などを指示するビジネスメール詐欺	17.2%
ソーシャルエンジニアリング	17.2%
クラウドサービスに対する攻撃	17.2%
内部不正による情報漏えい	16.1%
IoTデバイスに対する攻撃	13.8%
その他	8.0%

（複数選択可／n=87）

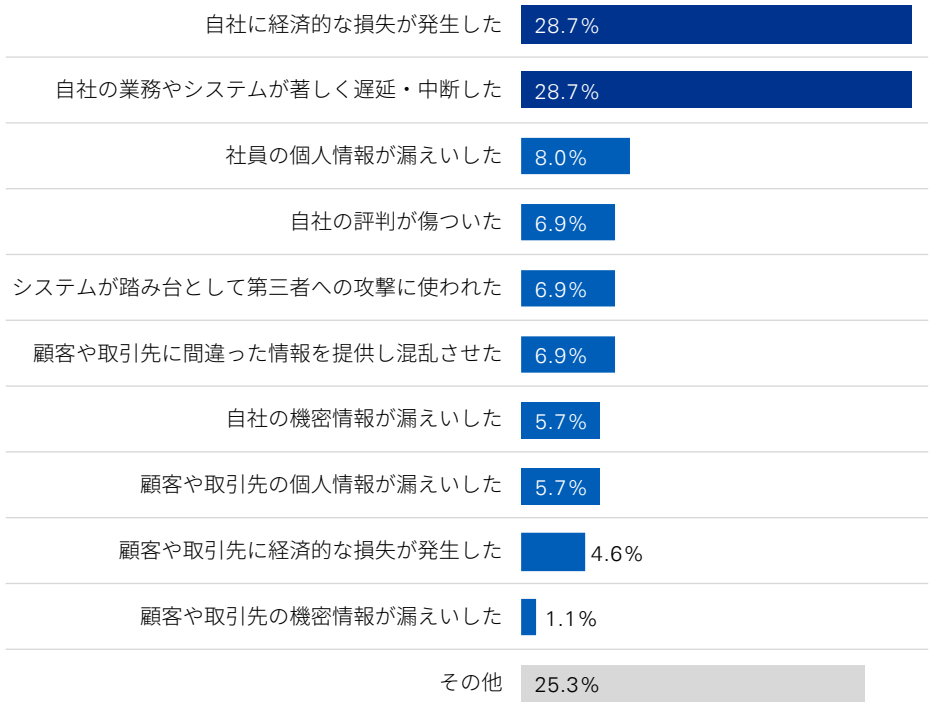
サイバーインシデントの被害状況

識別 防御 検知 対応 復旧

サイバーインシデントにより、「自社に経済的な損失が発生した」、「自社の業務やシステムが著しく遅延・中断した」という回答が多く、企業のビジネスに実害を及ぼしている様子がうかがえます。また、損失費用が発生した企業における損失合計額としては、100万～1,000万円未満が最も多いものの、1億円以上の損失被害も発生しています。

サイバーインシデントの被害状況

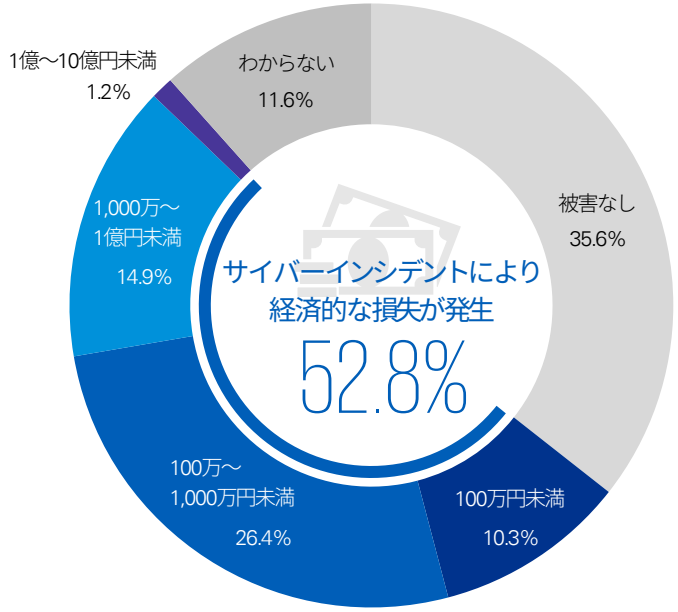
約3割で経済的な損失やシステム遅延・中断が発生している



（複数選択可／n=87）

合計損失額

サイバーインシデントにより経済的な損失が発生している



（n=87）

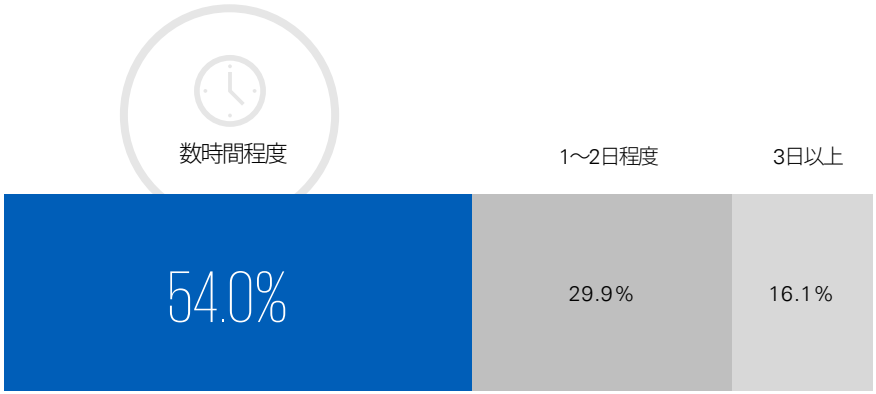
サイバーインシデントの対応時間

識別 防御 検知 対応 復旧

サイバーインシデントに対する初動対応は、54.0％が数時間程度と回答していますが、一方で3日以上かかったと回答した企業も少なくありません。また、復旧対応については、51.7％が1週間程度で対応が完了していますが、数週間以上、場合によっては3ヵ月以上かかるケースも見られます。

初動対応にかかった時間

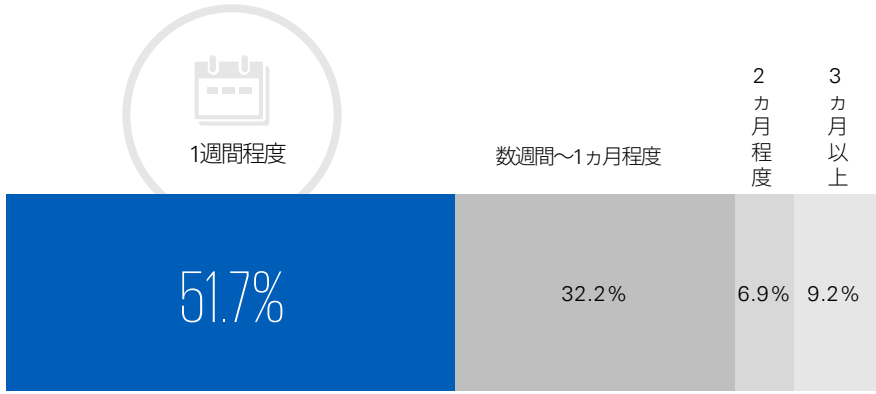
54.0%が初動対応を数時間程度で実施している



（n=87）

復旧までにかかった時間

51.7%が1週間程度で復旧している



（n=87）

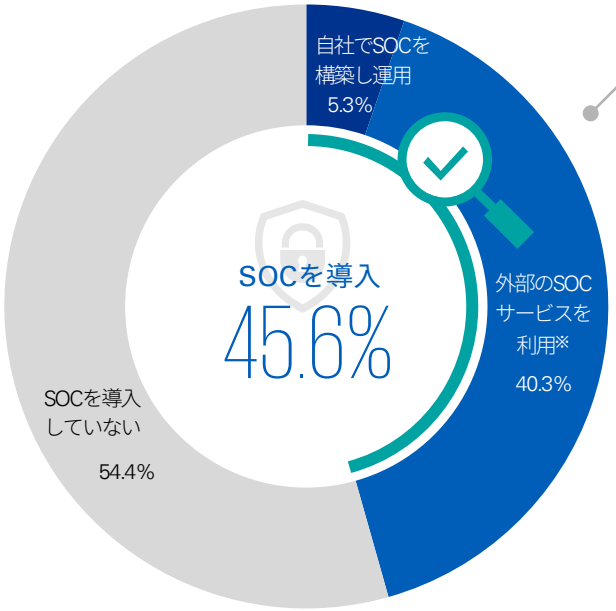
SOCの導入状況

識別 防御 検知 対応 復旧

回答企業のうち、45.6%がSOC（Security Operation Center）を導入しており、そのうち40.3%が外部のSOCサービスを利用しています。監視している攻撃としては、不審なウェブサイトへのアクセス・閲覧やインターネットからの攻撃性の高いアクセス、DoS／DDoS攻撃といった従前からよく見られる監視対象が並びます。クラウドサービスに対する監視は少数にとどまっています。

SOC導入状況

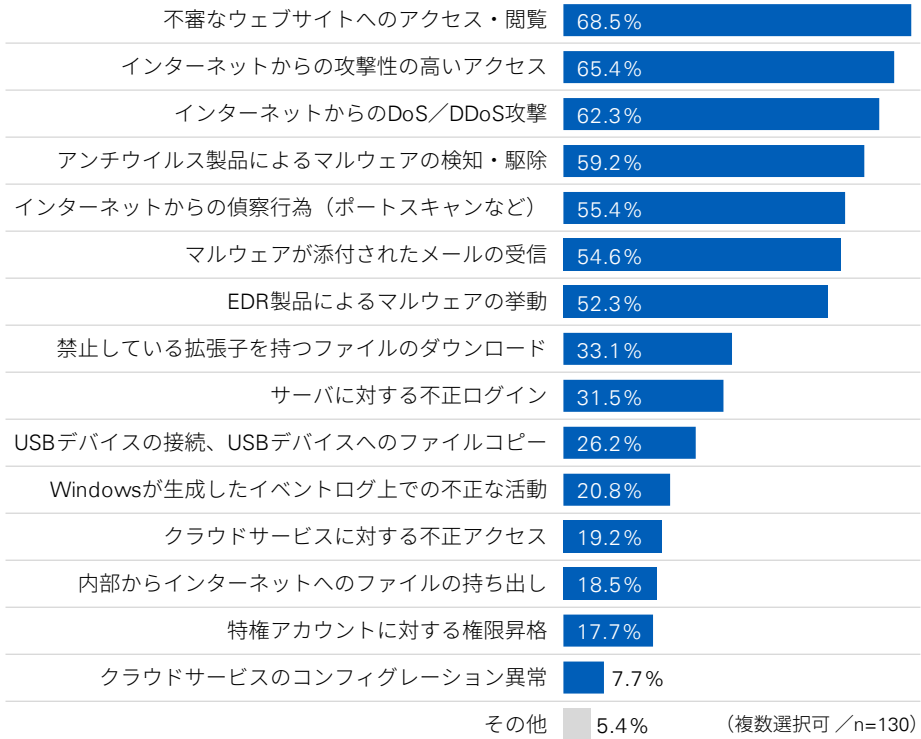
45.6%がSOCを導入し、40.3%が外部SOCを利用



※自社のSOCと外部のSOCサービスの併用を含む
（n=285）

SOCで検知しているセキュリティイベント

クラウドサービスに対する監視は少数にとどまる



（複数選択可／n=130）

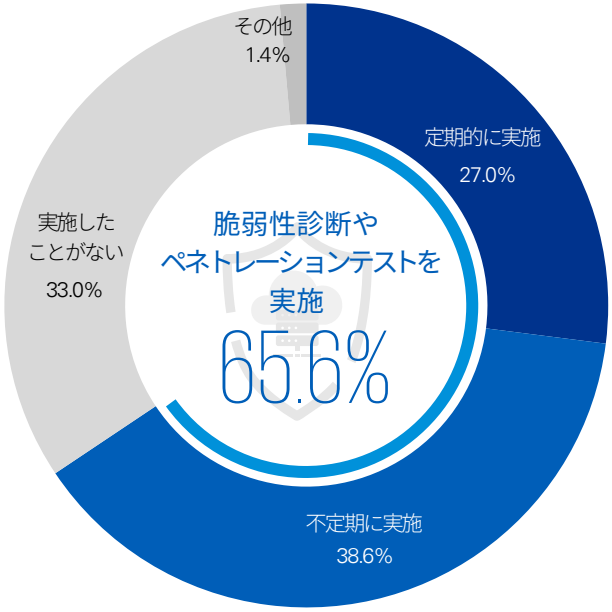
脆弱性診断やペネトレーションテストの実施状況

識別 防御 検知 対応 復旧

回答企業のうち、65.6%が脆弱性診断やペネトレーションテストを実施していると回答しています。

脆弱性診断やペネトレーションテストの実施状況

65.6%が脆弱性診断やペネトレーションテストを実施している



(n=285)

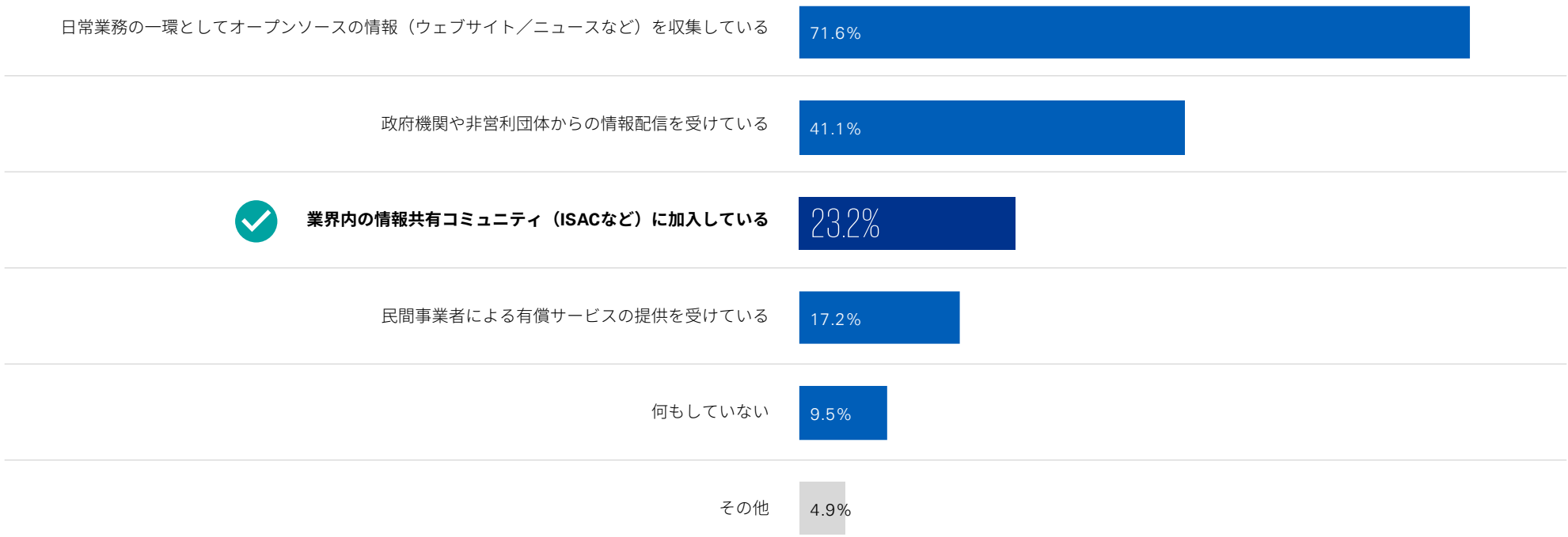
サイバー脅威動向の情報収集・共有

識別 防御 検知 対応 復旧

大半の企業が、何らかの社外リソースを活用して情報収集をしています。回答企業のうち23.2%は、
ISAC（Information Sharing and Analysis Center）等の情報共有コミュニティを活用して他社と攻撃情報を共有しています。

サイバー脅威動向を収集するための活動

23.2%がISAC等の情報共有コミュニティを活用して他社と攻撃情報を共有している



（複数選択可 ／n=285）

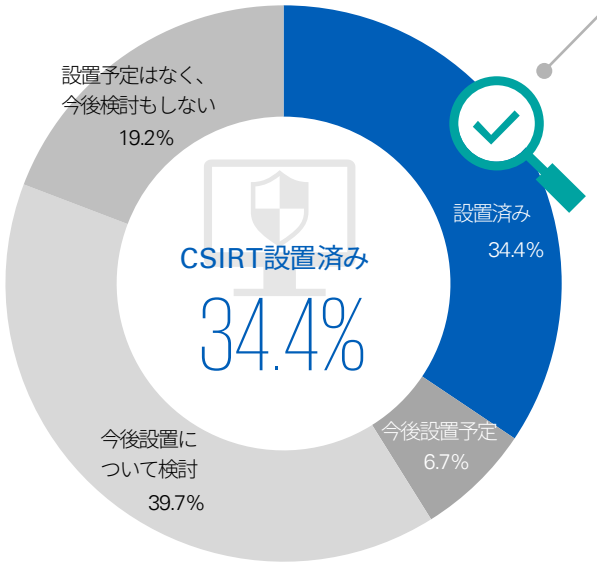
CSIRTの設置

識別　防御　検知　対応　復旧

回答企業のうち、34.4%がCSIRT（サイバー攻撃による情報漏えいや障害などに対処するための組織やチーム）を設置しており、そのうち75.5%ではCSIRTが機能していると回答しています。CSIRTの対象範囲に含まれるシステムとしては、自社の共通基盤や事業部門が構築したシステムが多い一方、設置済み企業の28.6%が海外の子会社や関連会社のシステムも含んでいます。

CSIRT設置状況

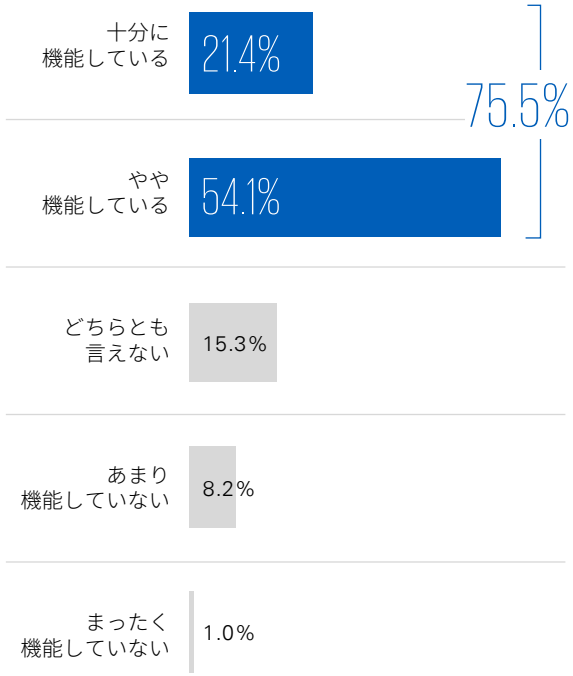
34.4%がCSIRTを設置している



（n=285）

CSIRTは機能しているか

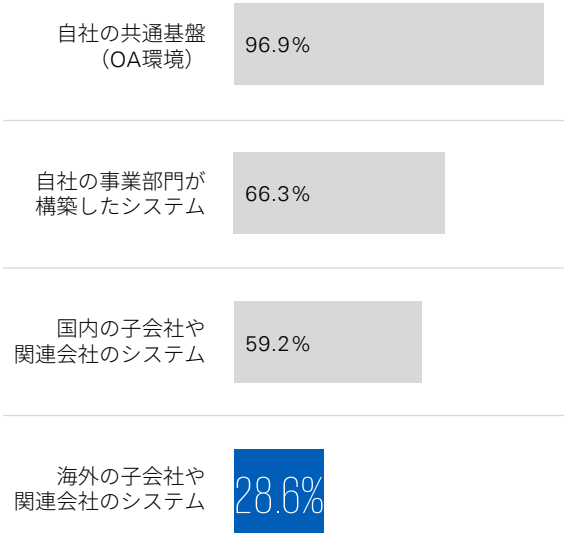
設置済み企業の75.5%が機能していると回答



（n=98）

CSIRTの対象範囲

設置済み企業の28.6%が海外の子会社や関連会社のシステムも対象に含む



（複数選択可／n=98）

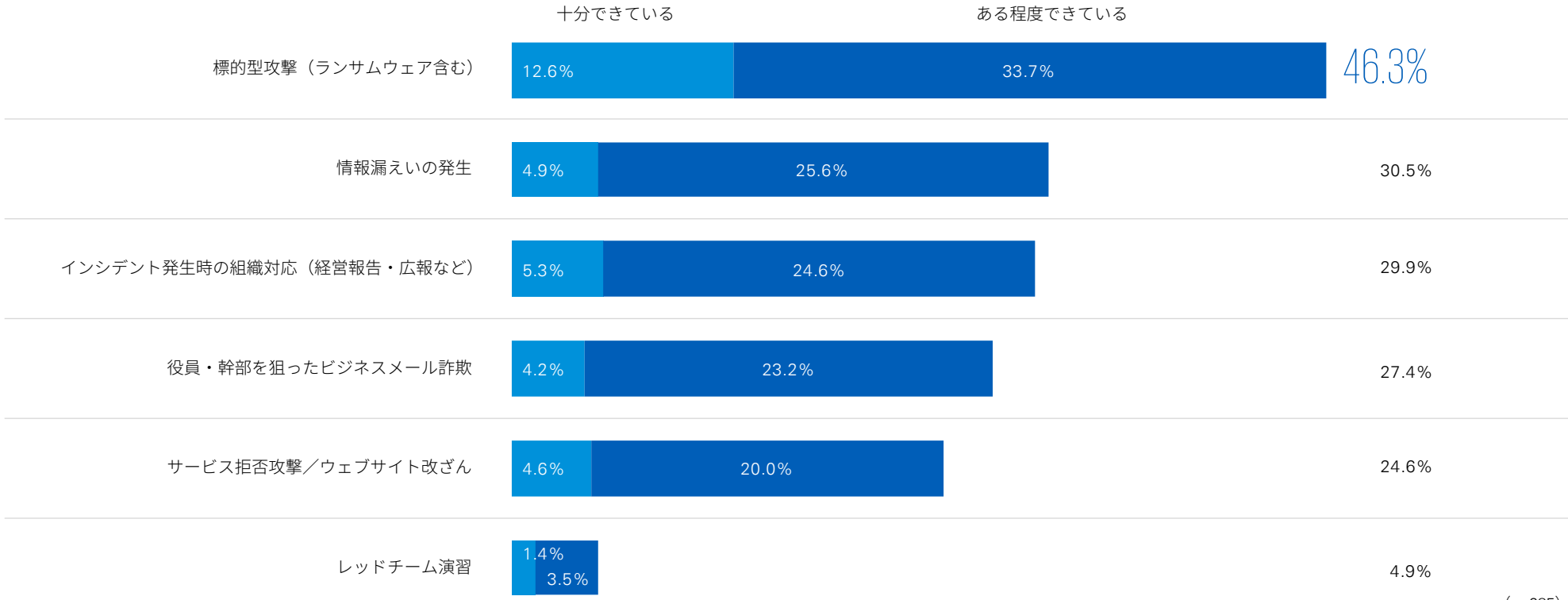
サイバー攻撃対策の訓練・演習

識別 防御 検知 対応 復旧

訓練・演習を「十分できている」と回答する企業は少なく、特にレッドチーム演習（セキュリティ専門家で構成する攻撃チームが攻撃を仕掛け、攻撃される企業のセキュリティ対策状況を検証）はほとんど実施されていません。

サイバー攻撃対策の訓練・演習の実施状況

46.3%が標的型攻撃訓練を実施しているが、レッドチーム演習の実施はわずか4.9%にとどまる



（n=285）

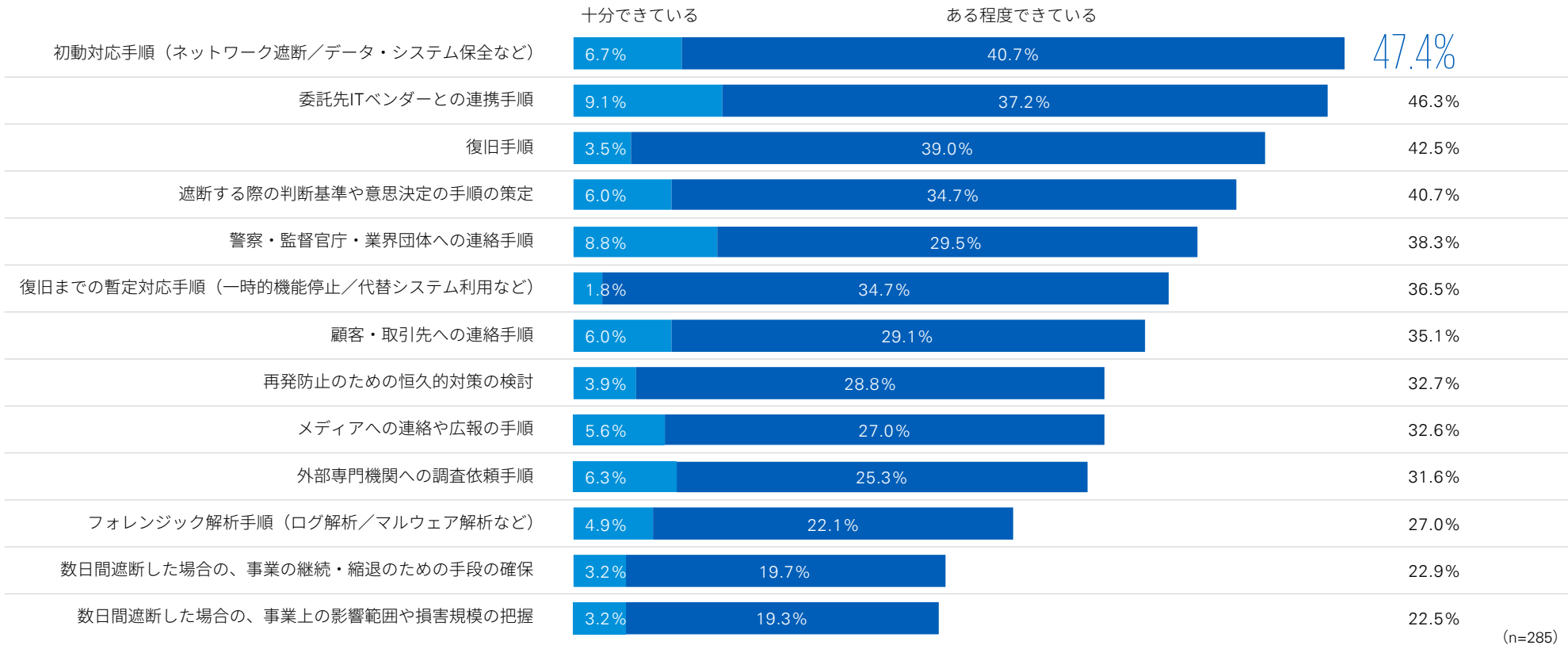
サイバーインシデントに備えた具体的な準備や対策

識別 防御 検知 対応 復旧

サイバーインシデントに対して、具体的な準備や対策を「十分できている」と回答する企業は少ないものの、「ある程度できている」とする企業も合わせると、47.4%が初動対応手順を準備しています。また、約23%が数日間遮断した場合の対応をあらかじめ定めています。

サイバーインシデントへの備え

47.4%が初動対応手順を、約23%が数日間遮断した場合の手順を準備している



（n=285）

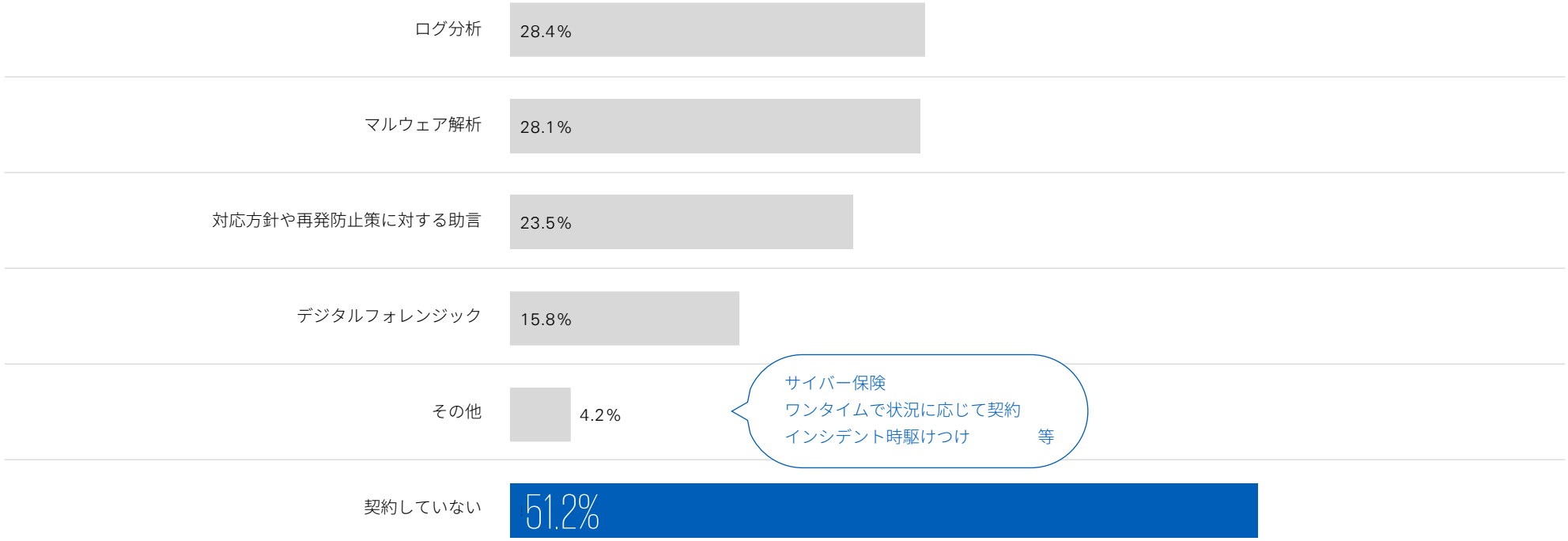
インシデント対応を支援するための外部サービス契約状況

識別 防御 検知 対応 復旧

回答企業の51.2%がインシデント対応を支援するための外部サービスを契約していません。
また、3割弱がログ分析やマルウェア解析の外部サービスを利用しています。

インシデント対応支援の外部サービス契約状況

51.2%が外部サービスを契約していない



（複数選択可／n=285）

COLUMN

二重脅迫型ランサムウェアへの対応

業務上重要なデータを暗号化するだけでなく、これらのデータを窃取して外部に公開することで身代金の回収率を高める犯行パターンである「二重脅迫型ランサムウェア」の被害が急増している。ランサムウェアへの対応については、各国において法令や規制が制定されており、その動きについては注視しておくことが重要である。これらの規制等を踏まえて、各国で発生したランサムウェア被害への対応方針を定めておくことが喫緊の課題となっている。

犯行グループとの戦略的な交渉のための行動指針

I 被害企業の顧客、従業員および関係者の安全確保

- 犯行グループとの通信によって被害企業やすべての関係者への二次攻撃のリスクが発生しないようにする。
- 交渉人の素性（所属組織や経歴等）がわからないようにする。

II データ主体のリスクの最小化

- プライバシーデータの公開リスクを軽減すべく、対象となるデータ主体（個人）と危険にさらされているデータを特定するため、取り得る対応を検討する。
- 犯行グループによるデータの公開に対する被害を軽減するためのあらゆる努力を図る。

III 漏えいデータ等の事実確認

- 漏えいの可能性のあるデータサンプルを入手して、犯行グループの犯行声明の内容を検証する。
- 確認された事実をもとに、被害企業が効果的なインシデントレスポンスを実施できるように調整を図る。

IV 証拠収集機会の最大化

- 法的な手続きを円滑に行うため、犯行グループとのコミュニケーションを通じて、情報／証拠を入手する。
  - 犯行グループの正体
  - 物理的な所在地
  - 通信手段
  - 口座や資金の流れ

V 法令遵守の徹底と重要な意思決定

- 被害企業は、交渉プロセスにおいてすべての法律および規制を遵守する必要がある。
- 交渉人は重要な戦略や意思決定については被害企業に確認しながら進めていく。

テーマ

02

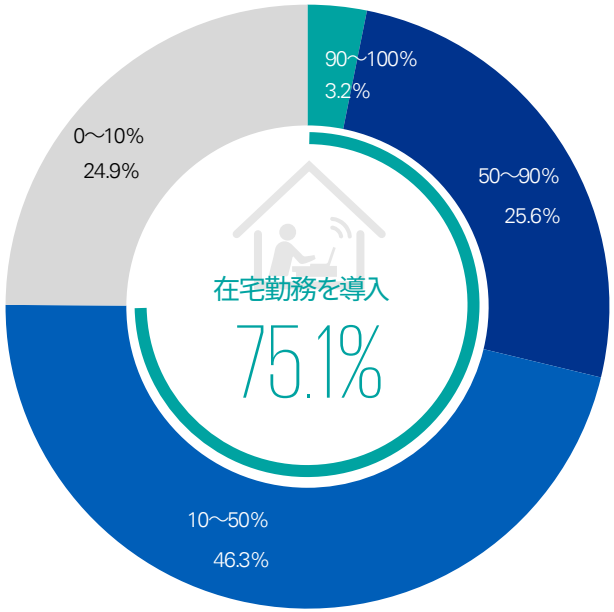
リモートワークセキュリティ

在宅勤務の割合とリモートワークにおけるサイバーセキュリティ対策方針

回答企業の75.1%が何らかの形で在宅勤務を導入している一方で、リモートワークにおけるサイバーセキュリティの対策方針を策定している企業は47.7%と半分に満たない状況です。既存の事業継続計画の流用を含めると、在宅勤務率の高い企業ほど対策方針を明確にしている割合が高く、在宅勤務率90～100%の企業の88.8%が対策方針を策定している、もしくは既存の事業継続計画を流用していると回答しています。

在宅勤務の割合

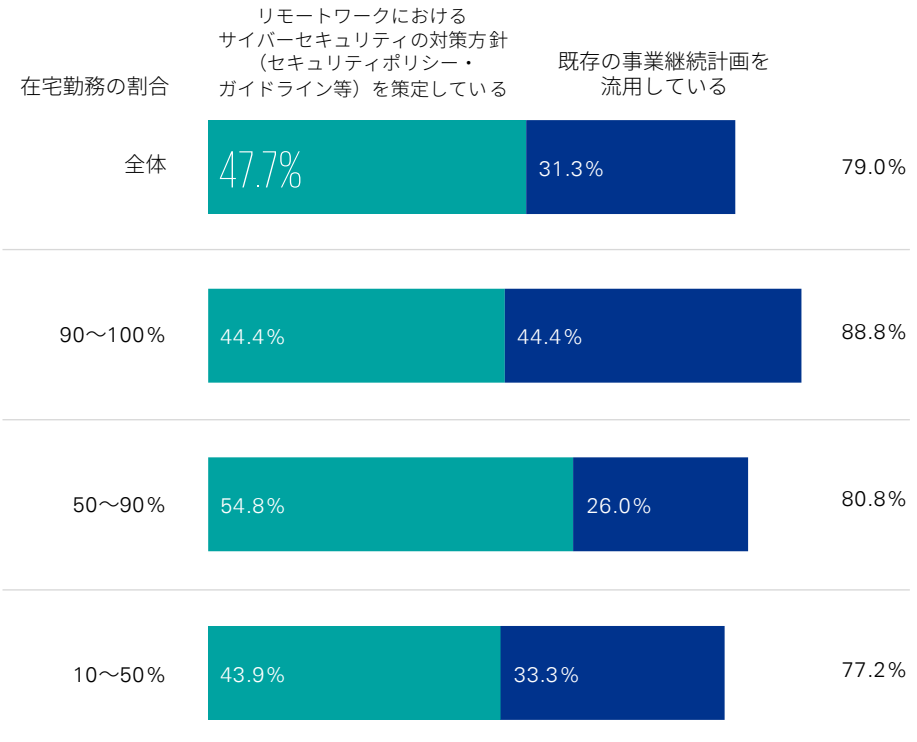
75.1%が在宅勤務を導入している



（n=285）

リモートワークにおけるサイバーセキュリティの対策方針の策定状況

47.7%がリモートワークにおけるサイバーセキュリティの対策方針を策定している。在宅勤務の割合が高いほど、対策方針が明確に示されている



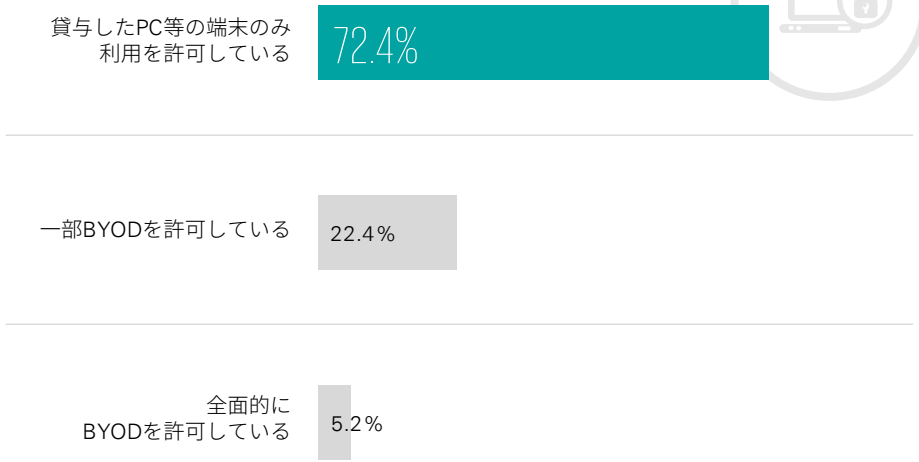
（n=214）

在宅勤務で利用するPC等の端末と業務システムへのアクセス方法

回答企業の72.4%が貸与端末のみ在宅勤務での利用を許可しています。一方27.6%は何らかの形で私物端末の業務利用（BYOD）を許可しています。業務システムへのアクセス方法は、84.1%がVPN（Virtual Private Network）接続を利用しています。その他のアクセス方法としてキャリア閉域網を利用しているという回答が複数寄せられました。

在宅勤務で利用するPC等の端末

72.4%が貸与端末のみ利用許可している



（n=285）

業務システムへのアクセス方法

84.1%がVPNを利用している

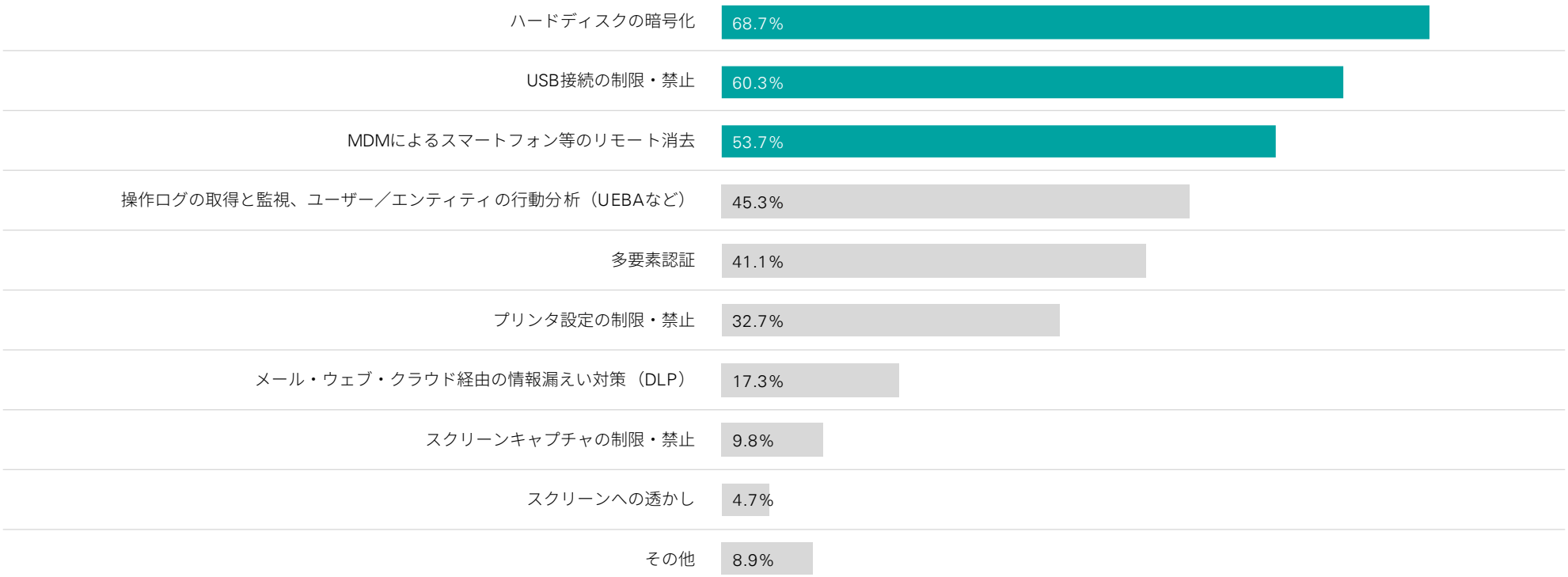
（複数選択可／n=214）

在宅勤務で利用するPC等の端末にて講じられているセキュリティ対策

回答企業の半数以上がハードディスクの暗号化、USB接続の制限・禁止、モバイルデバイス管理（MDM）によるスマートフォン等のリモート消去を導入しています。一方で、メール・ウェブ・クラウド経由の情報漏えい対策（DLP）は17.3%でした。このことから、端末からの物理的な情報漏えい対策が講じられている反面、ネットワーク経由における対策はあまり普及していない様子がうかがえます。

在宅勤務用端末のセキュリティ対策導入状況

半数以上が物理的な漏えい対策を導入している



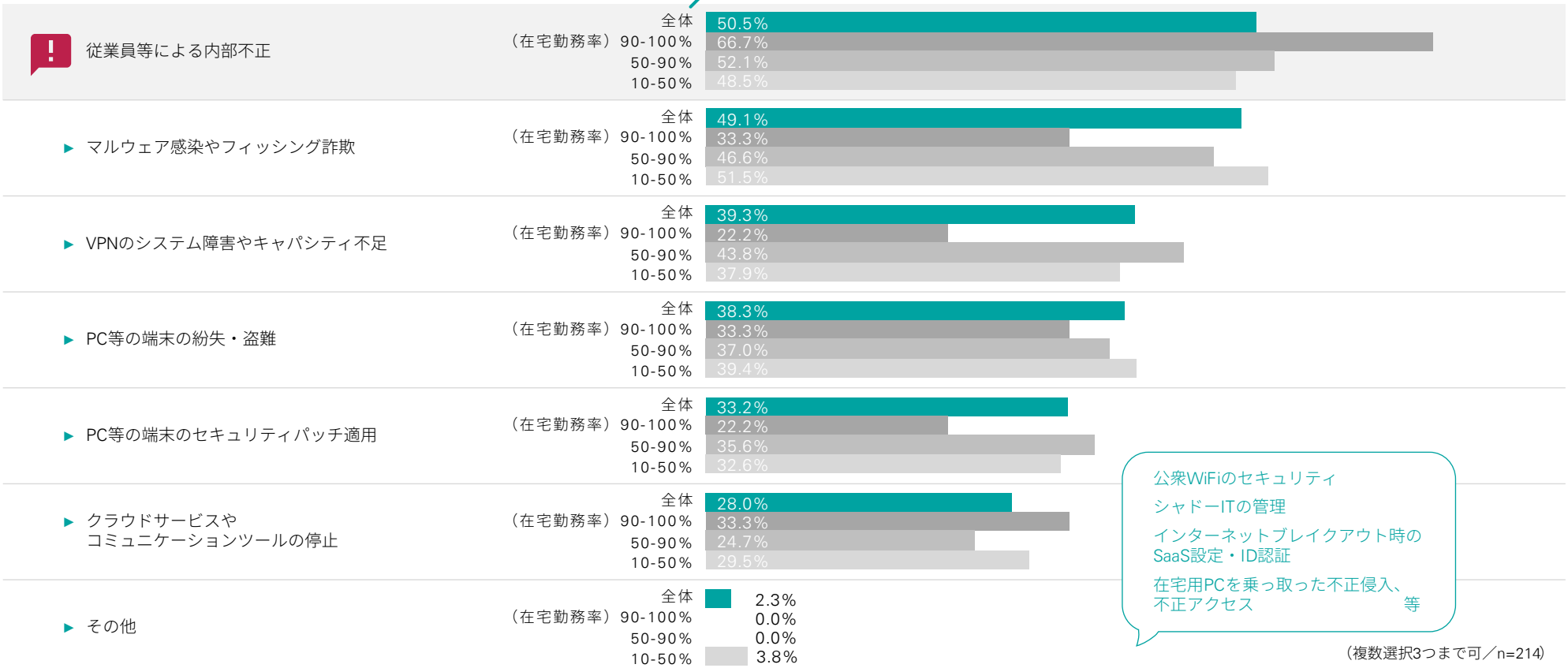
（複数選択可／n=214）

在宅勤務におけるセキュリティ面での問題として特に関心が高いもの

回答企業の50.5%が従業員等による内部不正を懸念しています。在宅勤務率が高いほど、内部不正に対して危機感を持つ企業が多く見られます。一方、マルウェア感染やフィッシング詐欺、端末のセキュリティパッチ適用や紛失・盗難は、在宅勤務率が低いほど問題点として挙げる企業が多い傾向にあります。

在宅勤務におけるセキュリティ面での問題

50.5%が従業員等による内部不正を懸念している

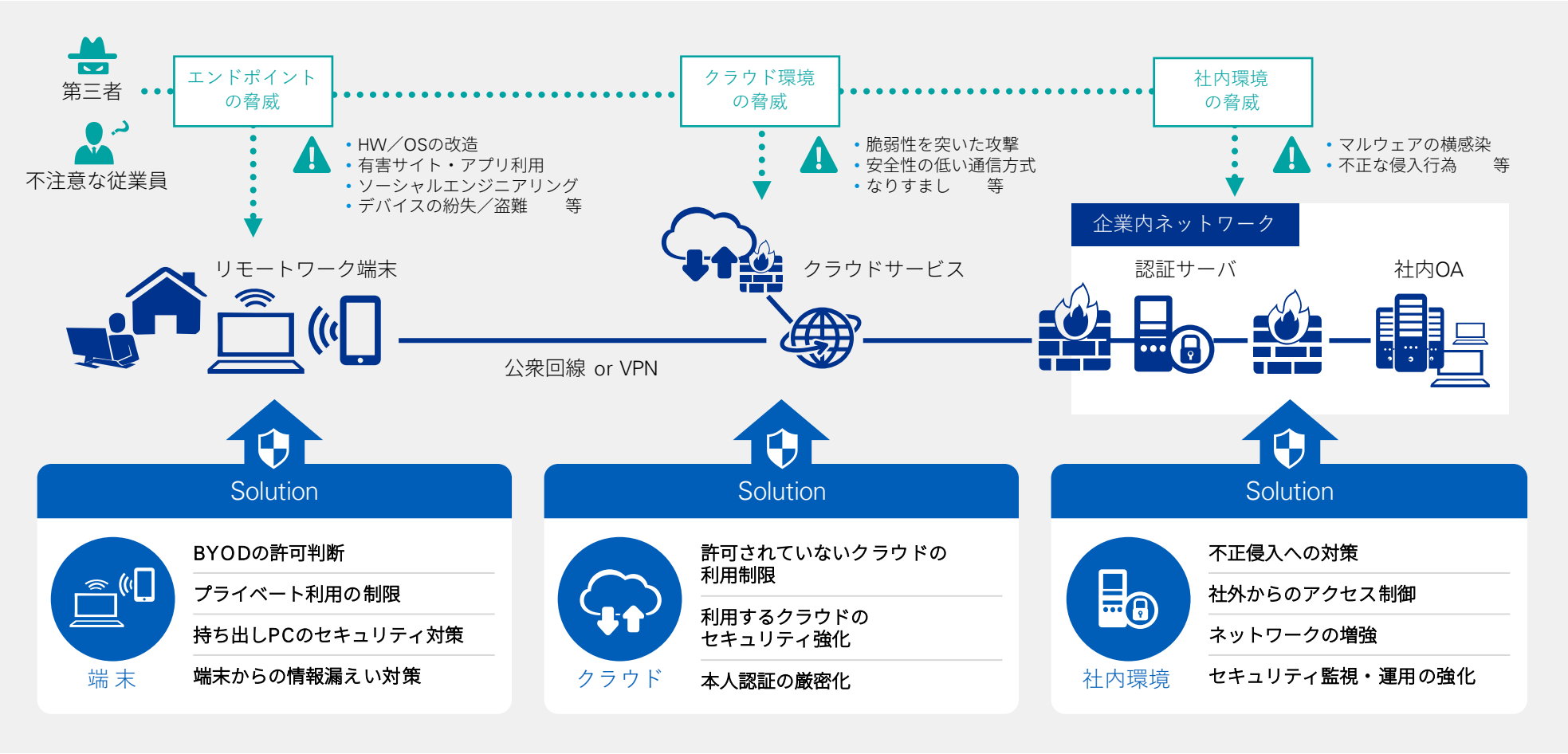


（複数選択3つまで可／n=214）

COLUMN

リモートワーク環境のセキュリティリスク

リモートワーク環境においては、社内環境だけでなく、クラウド等の社外環境やPC・スマートフォンなどのエンドポイントへの攻撃も想定され、対応が求められる。



テーマ

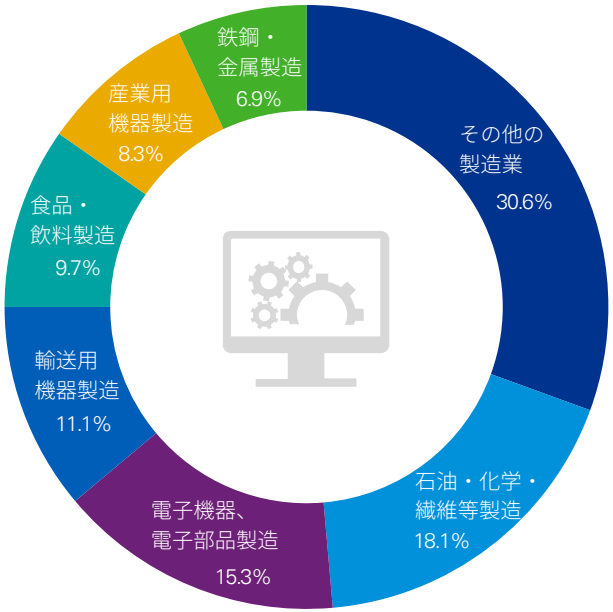
03

制御システムセキュリティ

制御システムに関する事業への取組み

回答企業の約3割が、工場・プラントにおける制御システムに関する事業に取り組んでいます。そのなかで海外工場が存在する企業において、統制管理ができていないとの回答は68.7%に達しており、前回（2019年）の調査と同じ傾向が見られます。

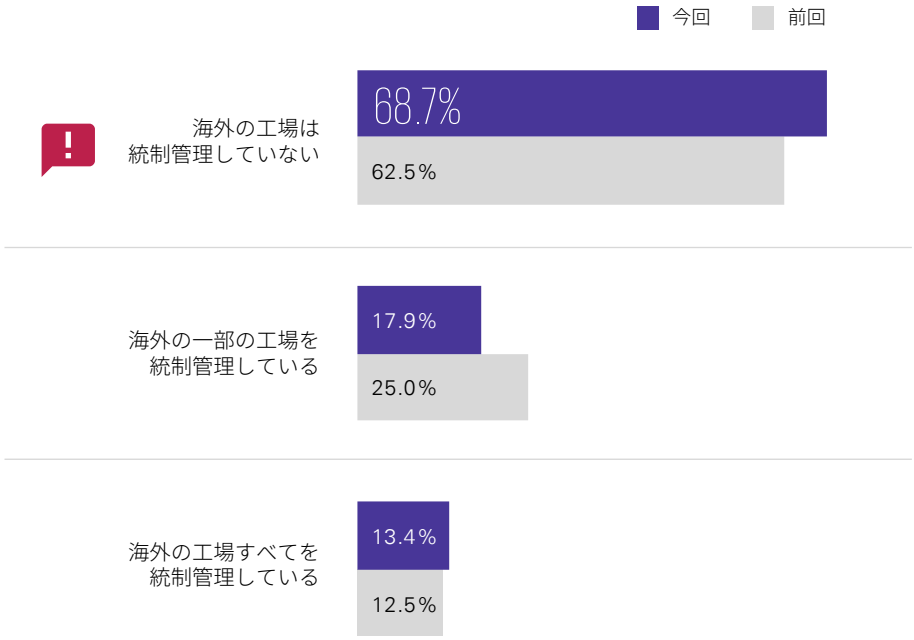
制御システムに関する事業に取り組んでいる企業（回答企業の業種別内訳）



（n=86）

海外工場の統制管理の状況

海外工場の統制管理は前回調査時から進んでいない



（n=86）

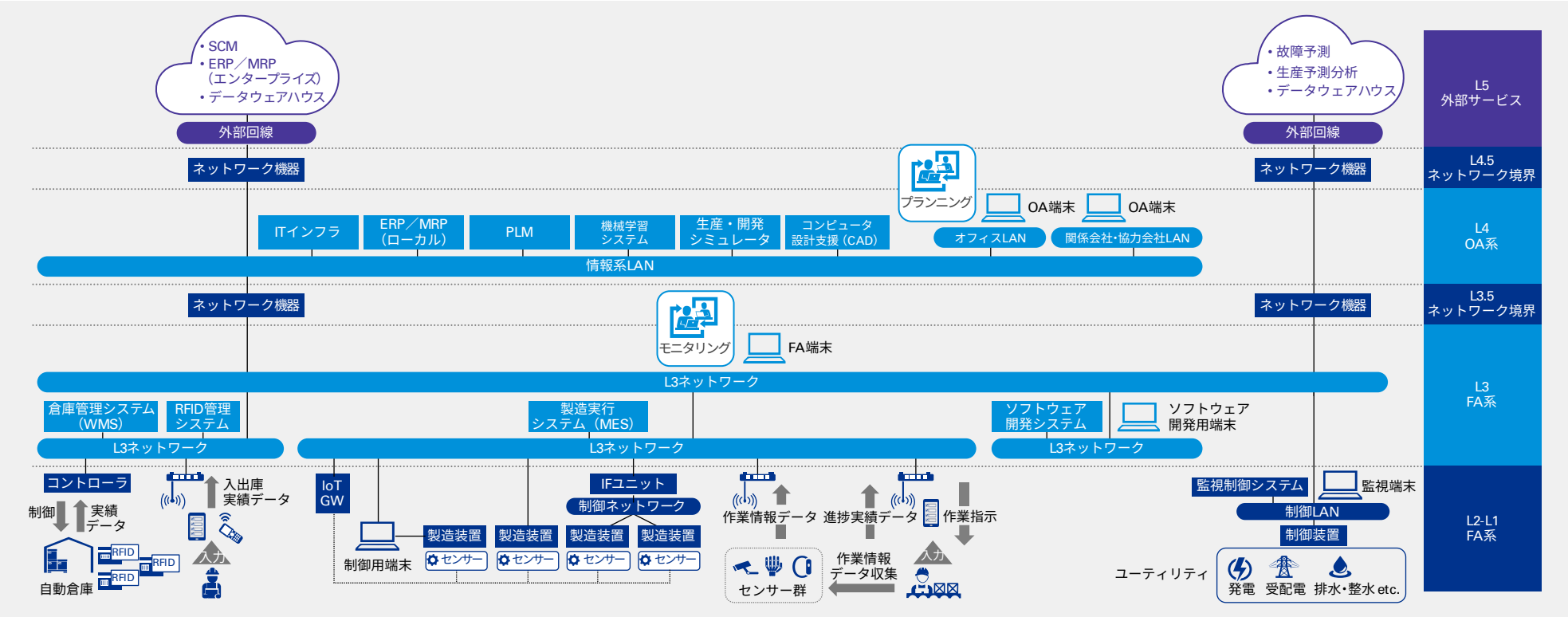
COLUMN

スマートファクトリー化で懸念されるサイバーセキュリティリスク

スマートファクトリーは、ドイツが提唱したIndustry 4.0で謳われた技術コンセプトであり、ビッグデータ、ロボット、AIによる生産や流通工程のオートメーション化、データ利活用による生産コストや流通コストの最適化を主眼としている。日本においても、Society 5.0で提唱する概念として取り上げられており、停滞した日本の製造業が抱える技術継承、生産性向上などの課題解決策として注目され、各企業で取組みが加速している。

スマートファクトリー化が進んだ工場では、さまざまなデバイスをネットワークに接続し、蓄積したデータを分析することでクラウド、AI、ロボットなどの最新テクノロジーを活用する。従来の工場と比較して、ERP、SCMなど情報系との通信、クラウド、リモートなど外部との通信等、ネットワークの接続が多岐にわたるためサイバー攻撃の標的になりやすく、かつさまざまなデバイスがネットワークに接続するために、被害を受けた場合は操業に直接的なインパクトを与える。多くの企業において、サイバー攻撃を懸念しているものの、スマート化された工場におけるリスクをどのように評価し、どのようなセキュリティ対策を導入するかが課題となっている。

課題解決のアプローチとしては、スマートファクトリー化の目的（品質の安定化、生産リソースの低減、製品の開発・設計の自動化など）と、最新テクノロジー（AI、クラウド、IoT、ロボティクスなど）の活用事例を組み合せてスマートファクトリーの工場モデルを作成し、そのモデルごとにリスクとセキュリティ対策を検討するアプローチがある。工場モデル化により海外も含めた工場展開も期待できる。

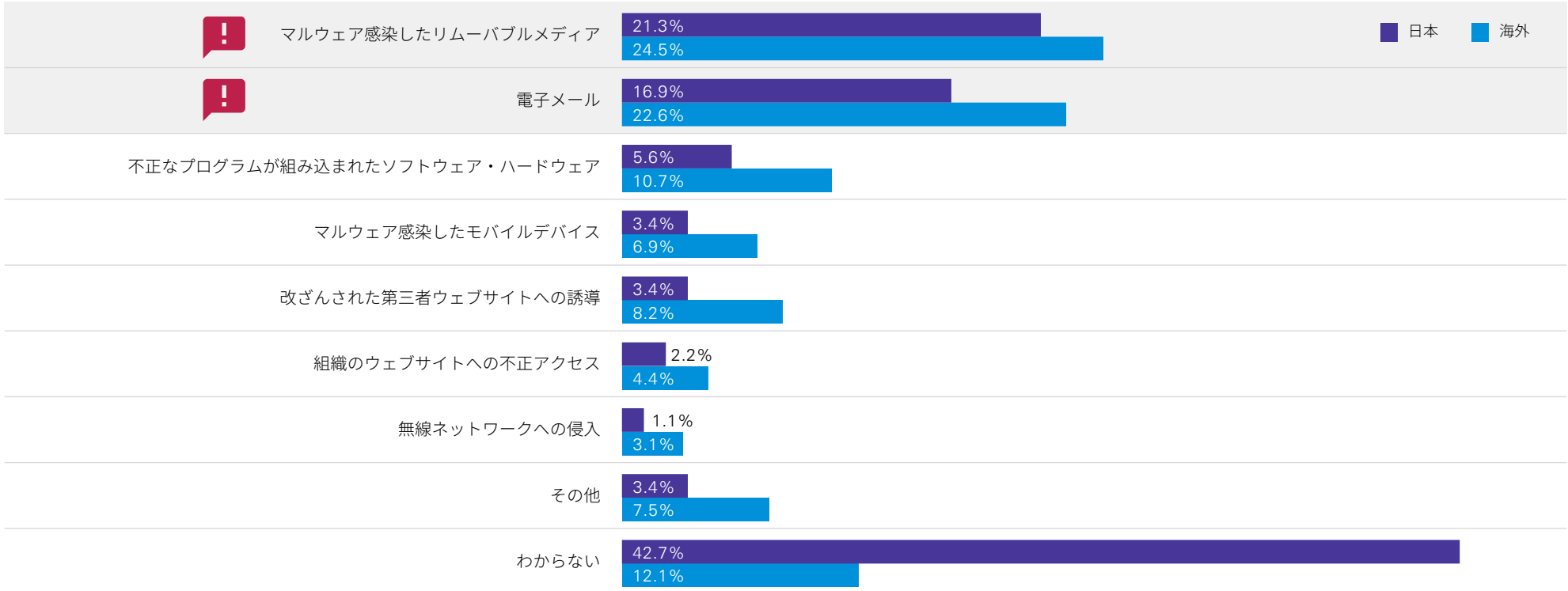


制御システムへのサイバー攻撃実態

制御システムへの攻撃は、従来から存在するマルウェア感染したリムーバブルメディアからの感染拡大に加えて、悪意のある第三者からの電子メール（フィッシング）による攻撃が多くなっています。これは海外も同じ傾向であり、工場・プラントの物理的なセキュリティ対策だけでは防ぐことが困難になってきていることがわかります。また、攻撃経路がわからないというユーザーが多いことも大きな課題です。

過去に発生した制御システムに関するセキュリティ事象（未然に防がれたものを含む）の攻撃経路・場所

マルウェア感染したリムーバブルメディアと、電子メール（フィッシング）による攻撃が多い



出所：海外は「(CS)2 AI-KPMG Control System Cyber Security Annual Report 2020」の調査データをもとに分析
https://assets.kpmg/content/dam/kpmg/xx/pdf/2020/10/kpmg-control-system-cyber-security-annual-report.pdf

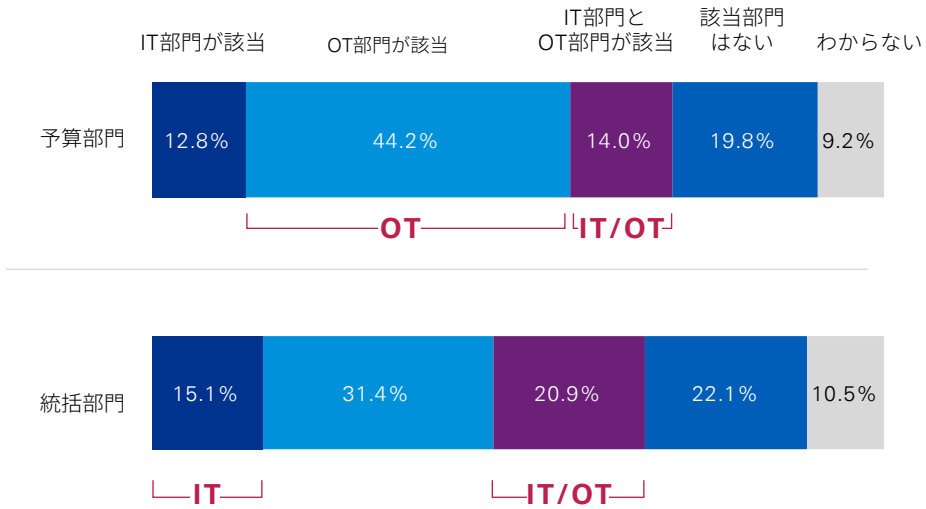
（日本：複数選択可／n=86）

制御システムセキュリティの予算と統括管理

制御システムのセキュリティに関する予算部門については、制御システム（OT）部門の関与が58.2%と半数以上を占めています。統括部門については、情報システム（IT）部門の関与が36.0%ですが、32.6%が「統括部門がない」、または「わからない」と回答しています。また、業務の委託先に対してセキュリティ対策を要請できている企業は、わずか17.5%です。

制御システムの統括部門と予算部門

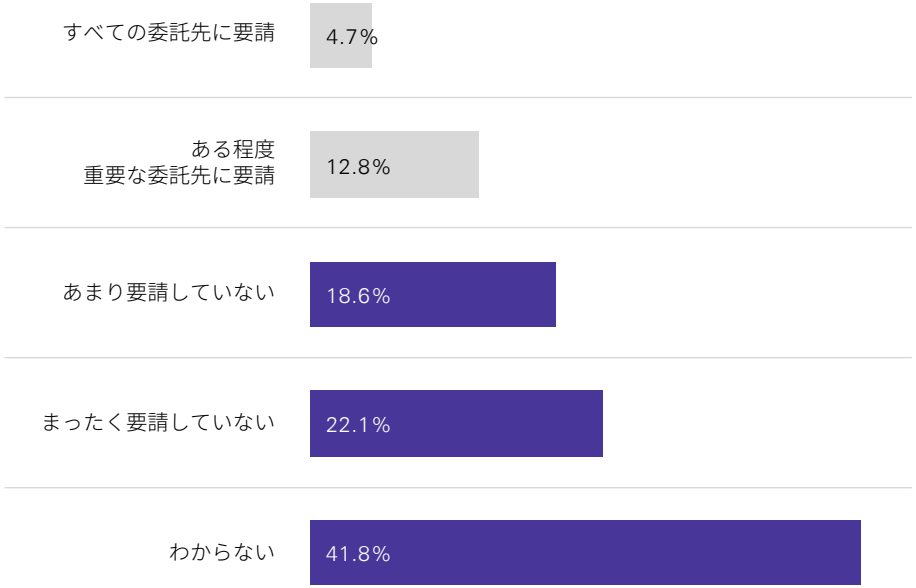
予算はOT部門、統括はIT部門が関与していることが多い



（n=86）

業務の委託先に対するセキュリティ対策の取組みの要請状況

委託先に対してセキュリティ対策を要請できていない



（n=86）

COLUMN

サプライチェーンに対するサイバーセキュリティ監査

DXに代表されるテクノロジーの進化、脱炭素社会を目指した水素・再生可能エネルギーインフラの整備などの外部環境や、グローバルに張り巡らされたサプライチェーン構造の複雑さにより、企業経営の難易度は飛躍的に高まっている。サプライチェーンの拡がりにおいてサイバーセキュリティは大きな課題であり、セキュリティレベルが低い取引先がサイバー攻撃を受けると、サプライチェーン全体に影響を及ぼす可能性がある。エネルギー業界においてはサプライチェーンのサイバーセキュリティ監査の取組みが加速しており、NIST CSFをベースとしたサイバーセキュリティ監査が取引先に求められている。

SACS-002　Third Party Cybersecurity Standard			
NIST CSF機能	NIST CSFカテゴリー	コントロール	要 件
識 別	Asset Management (AM)	1	情報資産の管理
	Governance (GV)	3	サイバーセキュリティに関する方針や体制
	Risk Assessment (RA)	2	リスクアセスメントのペネトレーションテスト
	Risk Management Strategy (RM)	1	サイバーセキュリティリスク評価
防 御	Access Control (AC)	19	システム・ネットワークおよび物理的なアクセス制御
	Awareness and Training (AT)	3	サイバーセキュリティに係る従業員への通知、トレーニング
	Data Security (DS)	20	データの保護
	Information Protection Processes and Procedures (IP)	13	情報保護のプロセスと手順
	Protective Technology (PT)	10	FW・IPSなどの境界防御や物理的な保護
検 知	Anomalies and Events (AE)	2	不正なイベントの監視
	Continuous Monitoring (CM)	6	アカウント、デバイス、アクセスなどの継続的なモニタリング
対 応	Communications (CO)	4	インシデント管理
	Mitigation (MI)	2	脆弱性対応、DDoS攻撃に対する軽減策

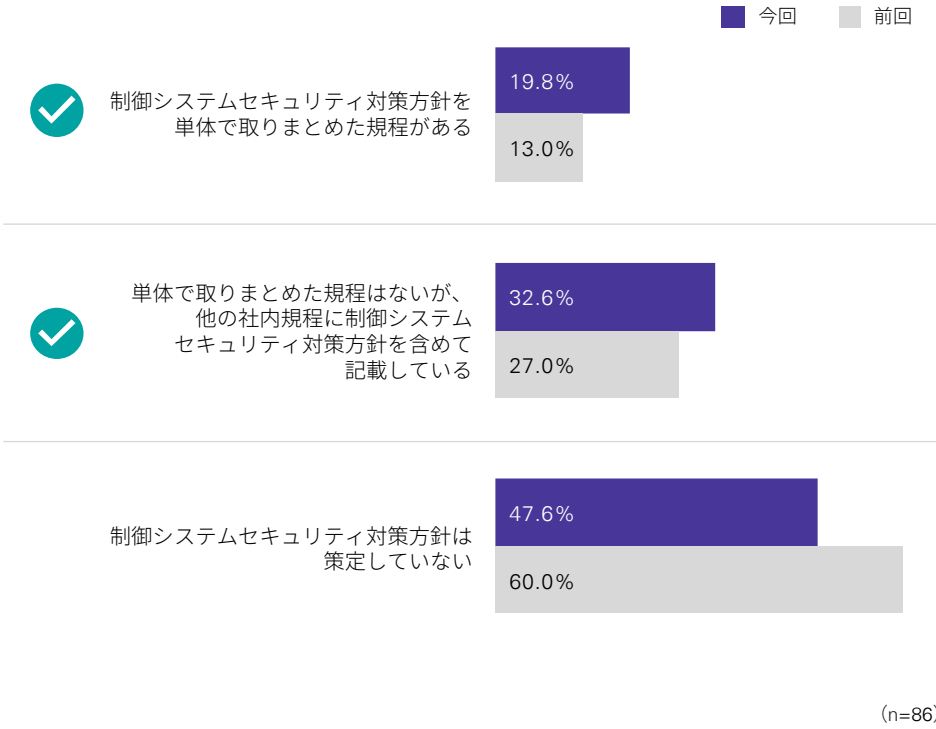
出所：「SACS-002 Third Party Cybersecurity Standard」をもとにKPMGが資料作成
https://www.aramco.com/-/media/downloads/working-with-us/ccc/sacs-002-third-party-cybersecurity-standard.pdf?la=en&hash=BF094FB8D0EC073102DED6F6BCAB5B7879B1D2BB

制御システムセキュリティ対策方針の整備

47.6%が制御システムセキュリティに係る対策方針が整備できていない状況ですが、前回（2019年）調査の60.0%と比べると、改善傾向にあります。なお、海外においては制御システムセキュリティ対策方針を整備するため、NIST CSF等のサイバーセキュリティのフレームワーク・ガイドラインが参照されています。

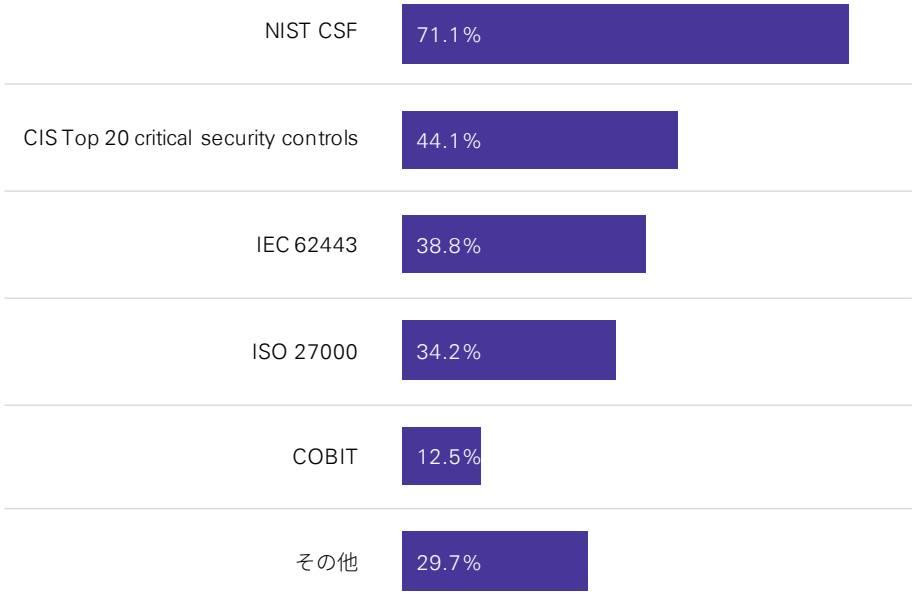
制御システムセキュリティ対策方針の整備状況

制御システムセキュリティ対策方針を整備する企業が増えている



（n=86）

海外で参照される制御システムセキュリティフレームワーク



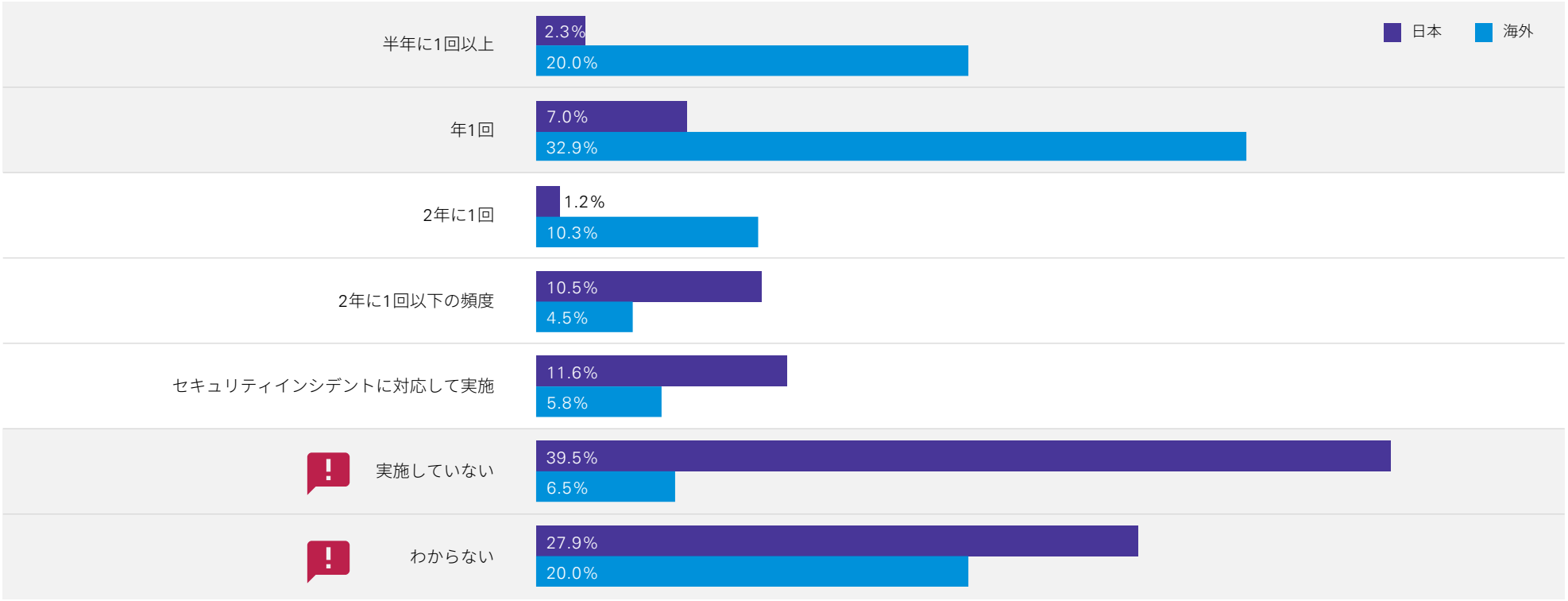
出所：海外は「(CS)² AI-KPMG Control System Cyber Security Annual Report 2020」をもとに集計
https://assets.kpmg/content/dam/kpmg/xx/pdf/2020/10/kpmg-control-system-cyber-security-annual-report.pdf

制御システムのセキュリティアセスメント

日本では制御システムに対するセキュリティアセスメントは浸透しておらず、39.5%が実施していない状況です。一方、海外では52.9%が少なくとも年に1回以上実施していると回答しています。海外と比べると、日本はセキュリティアセスメントの実施において大きく遅れていると言えるでしょう。

制御システムに対するセキュリティアセスメントの実施状況

海外と比べてセキュリティアセスメントの実施は大きく遅れている



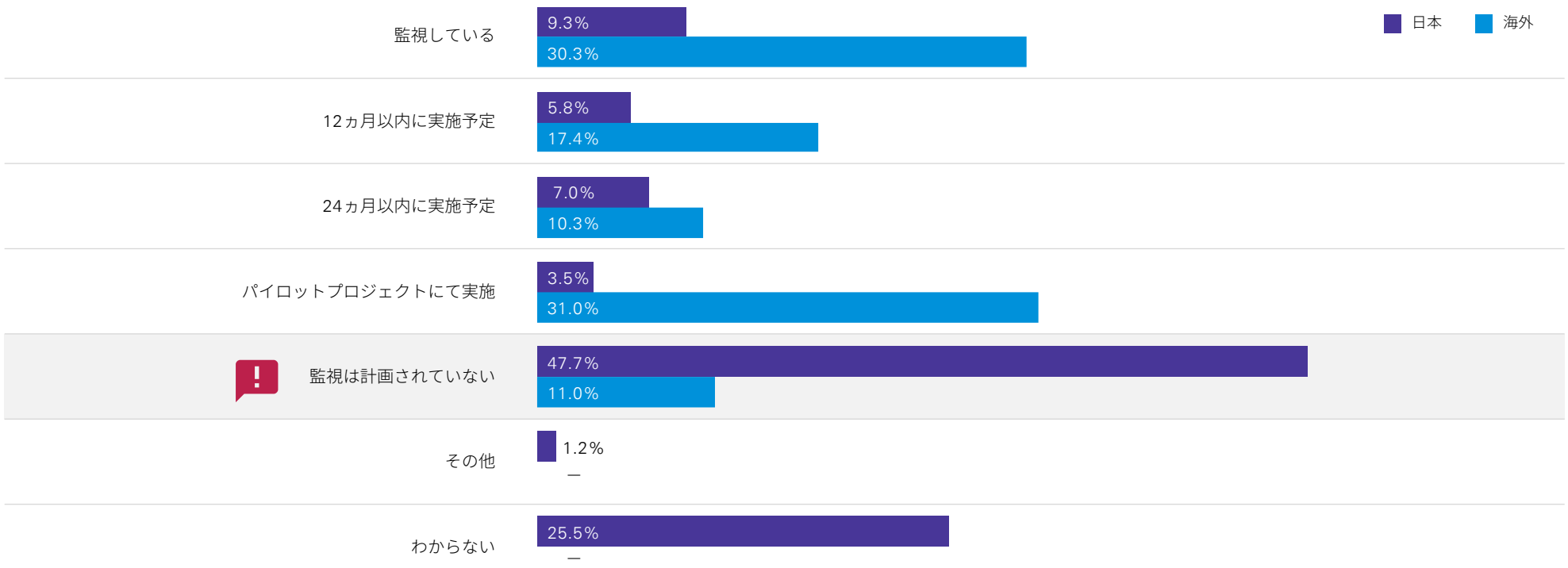
出所：海外は「(CS)² AI-KPMG Control System Cyber Security Annual Report 2020」をもとに集計　（日本：複数選択可／n=86）
https://assets.kpmg/content/dam/kpmg/xx/pdf/2020/10/kpmg-control-system-cyber-security-annual-report.pdf

制御システムのセキュリティ監視

日本では、制御システムのセキュリティ監視を実施している企業はわずか9.3%にとどまり、また計画されていない企業が47.7%と、ほとんど実施されていない状況です。一方、海外では監視を実施している企業は30.3%に上り、パイロットや実施予定も含めると9割近くとなっており、日本と海外とでは大きく開きがあります。

制御システムのセキュリティ監視

日本では制御システムのセキュリティ監視が遅れている



出所：海外は「(CS)² AI-KPMG Control System Cyber Security Annual Report 2020」をもとに集計
https://assets.kpmg/content/dam/kpmg/xx/pdf/2020/10/kpmg-control-system-cyber-security-annual-report.pdf

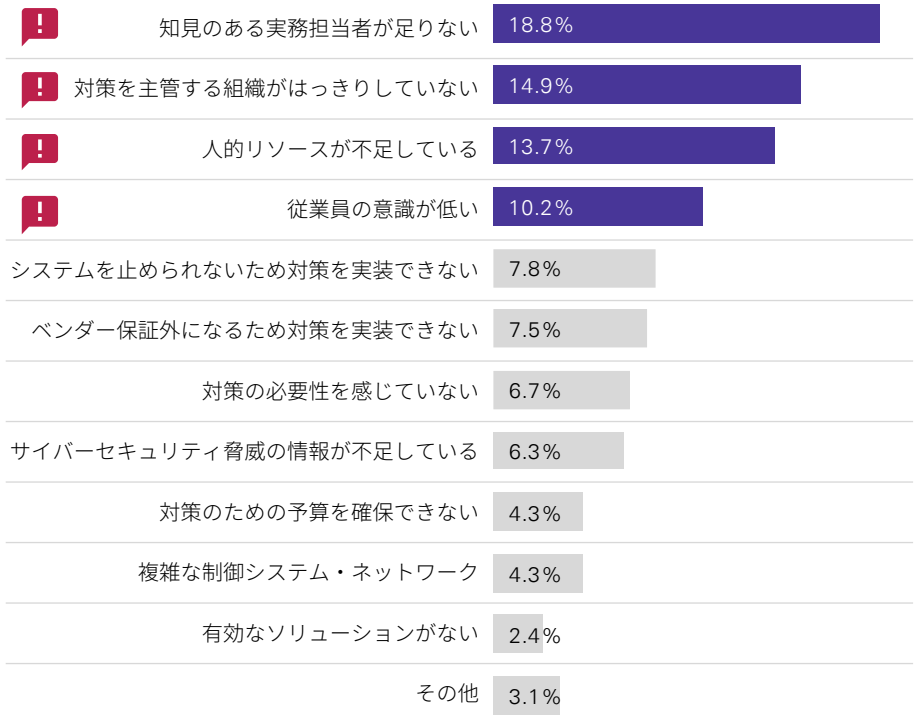
（日本：複数選択可／n=86）

制御システムセキュリティ対策が進んでいない原因

制御システムセキュリティ対策が進んでいない原因としては、知見・人的リソースの不足、主管組織の欠如であることがうかがえます。こうした状況においても、50％の企業が制御システムのセキュリティ教育・訓練を実施できておらず、企業にとってセキュリティ人材の確保・育成は大きな課題です。

制御システムセキュリティ対策が進んでいない原因

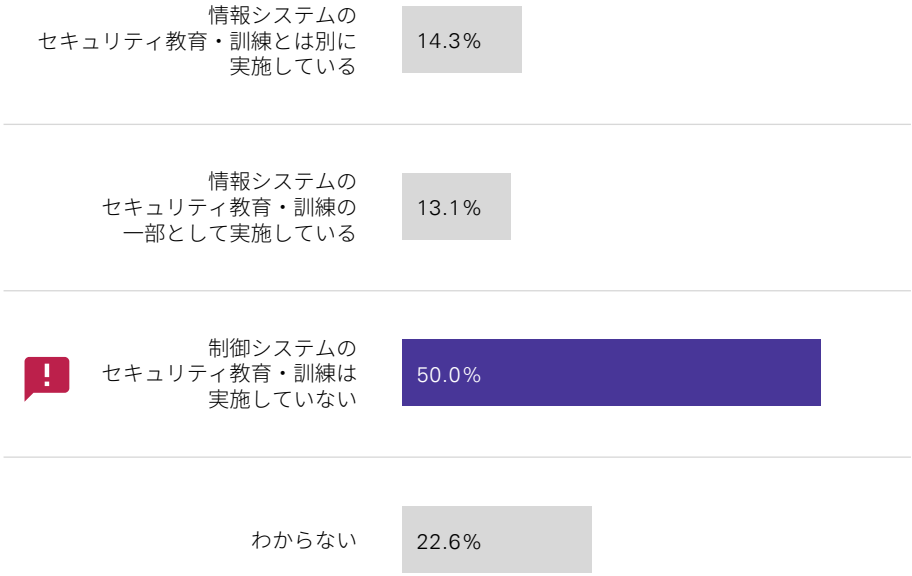
知見・人的リソースの不足、主管組織が曖昧であることが主な原因となっている



（複数選択可／n=86）

制御システムのセキュリティ教育・訓練の実施状況

制御システムのセキュリティ教育・訓練は実施できていない



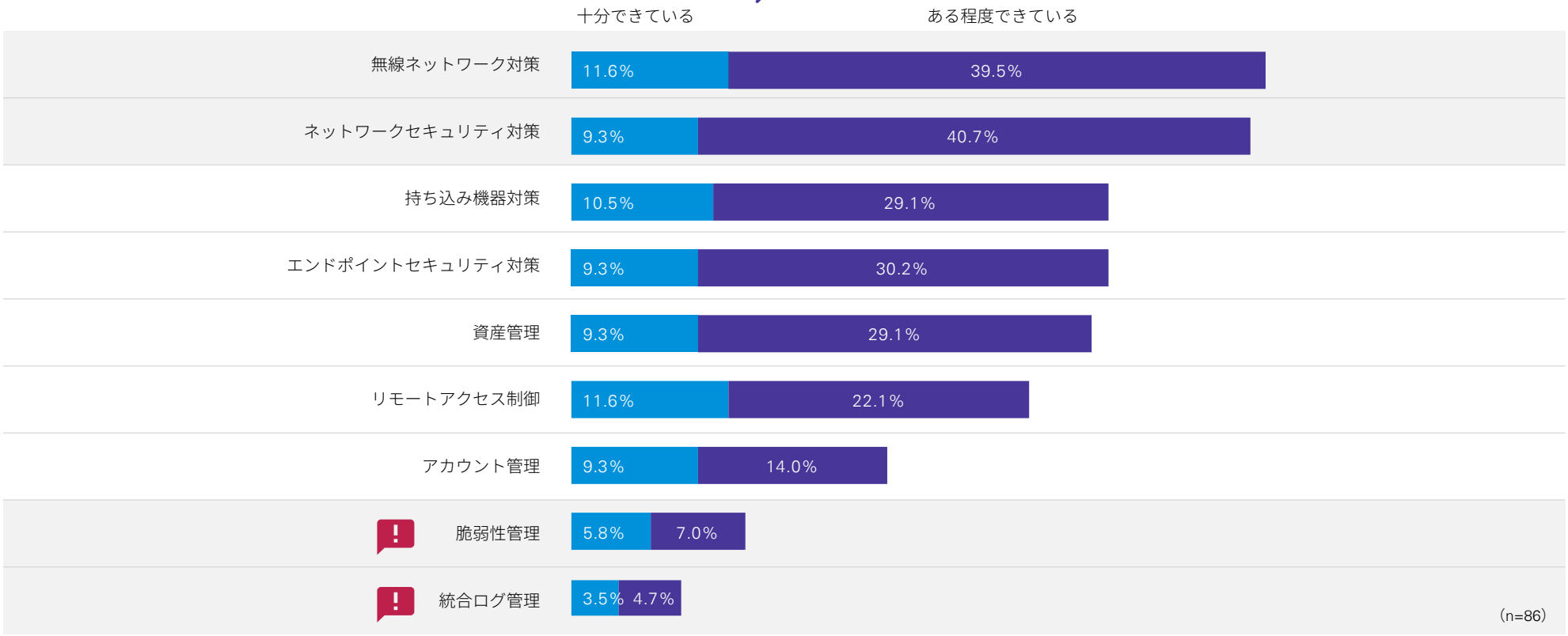
（n=86）

制御システムセキュリティ対策の実施状況

制御システムのセキュリティ対策は、ネットワーク対策に重点が置かれている傾向が見られますが、これは制御システムの設備機器そのものに対策を実施することが難しいことが要因の1つと考えられます。今後の課題としては、設備機器の脆弱性管理や統合ログといったセキュリティ運用面の対策が挙げられます。

制御システムセキュリティ対策の実施状況

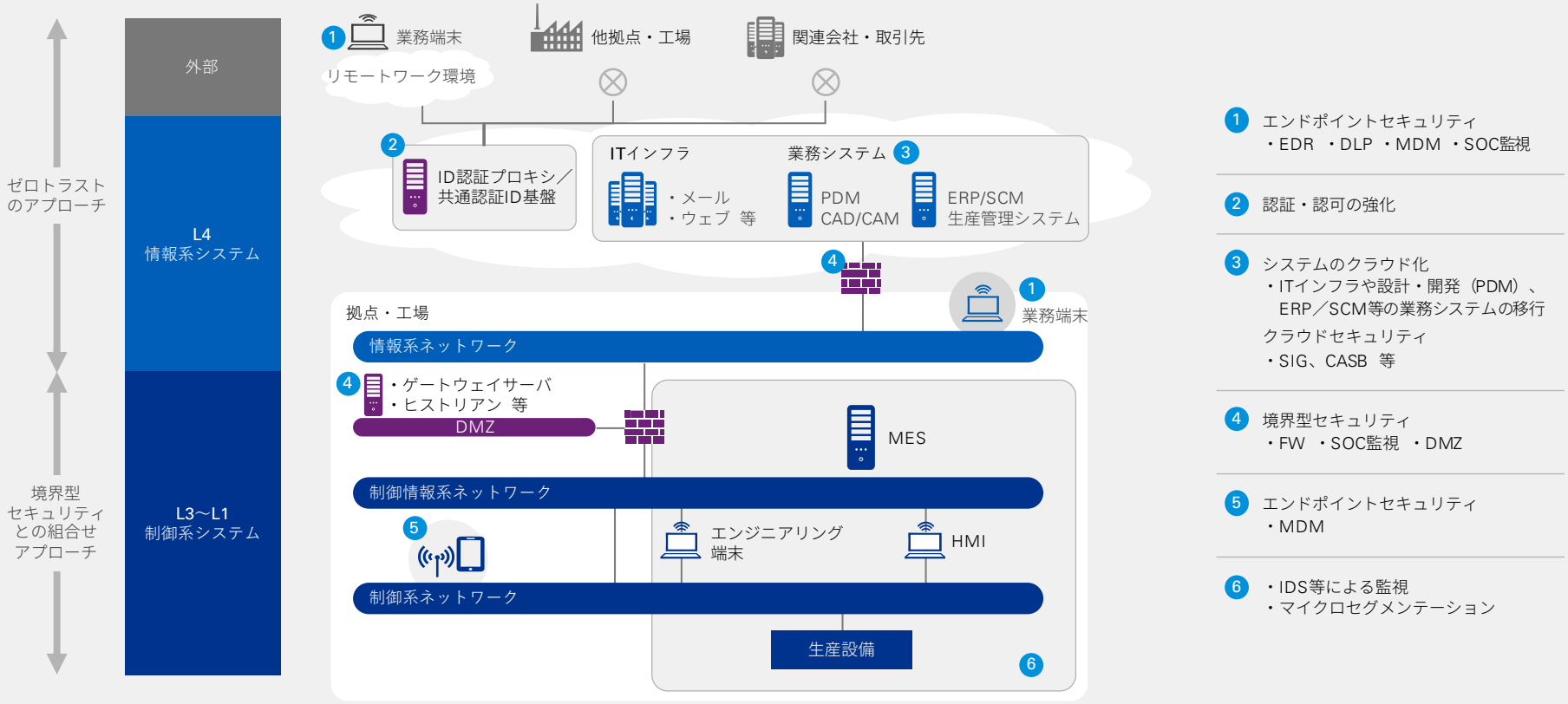
脆弱性管理、統合ログ管理などのセキュリティ運用面の対策が遅れている

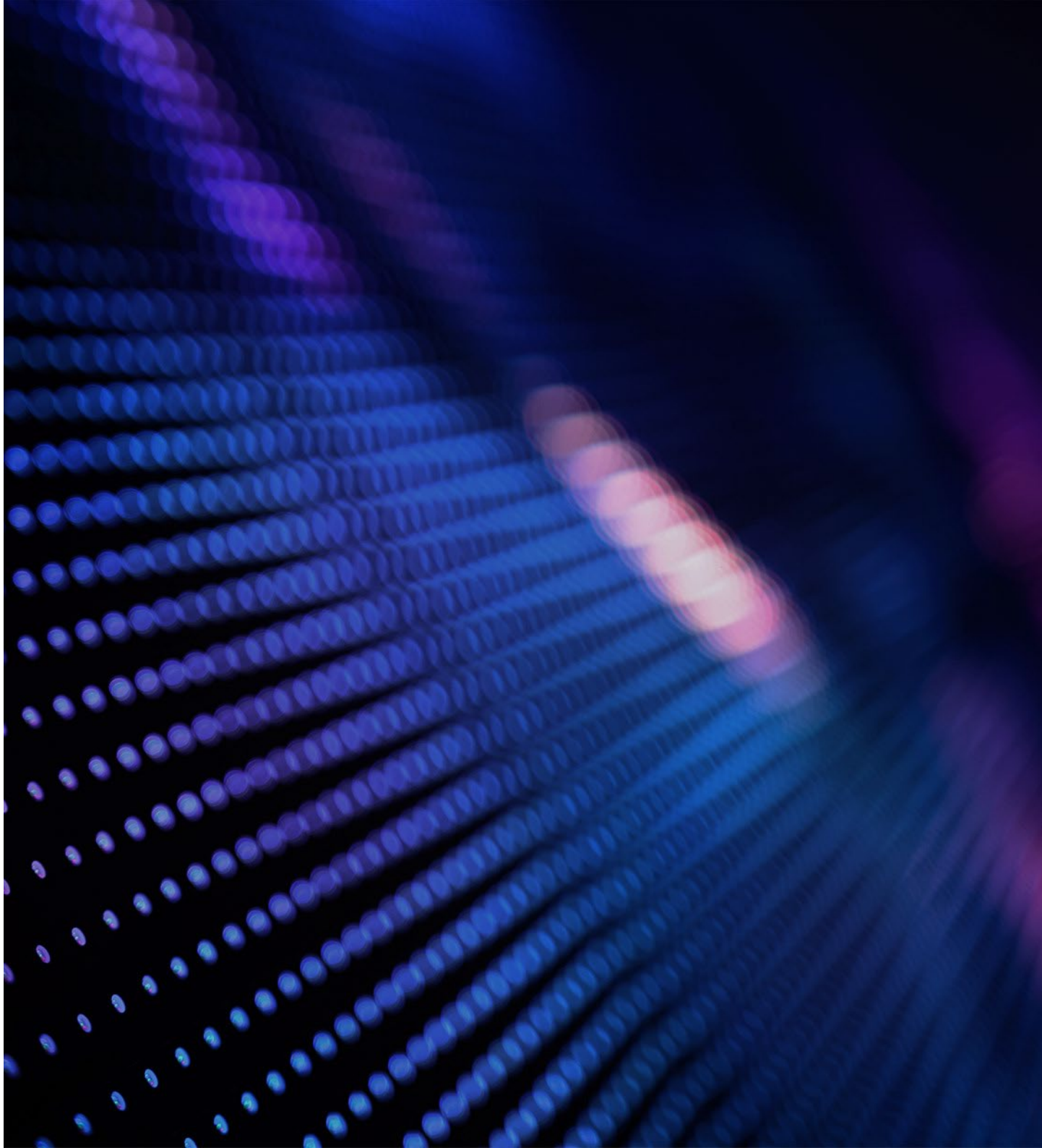


COLUMN

工場におけるゼロ・トラストアーキテクチャとは？

昨今IT環境においてゼロ・トラストアーキテクチャの導入が検討されているが、従来の制御システムは大規模かつ平坦なネットワークとして実装されていることが多く、ネットワーク境界対策も不十分だったため、容易に侵入可能な状態になっていた。また、工場ネットワーク内部の設備機器は古いものが多くエンドポイントのセキュリティ対策が難しいため、物理的な保護に頼らざるを得ない。そのため、工場においてはゼロトラストと他の標準ベースのアプローチ（例：IEC 62443 Zones and Conduits）を組み合せることで、工場のセキュリティ強化を図っていくべきである。





発行元

KPMGコンサルティング株式会社
株式会社 KPMG FAS

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/cyber-security