KPMG

サイバーセキュリティ サーベイ 2018

ご挨拶

サイバーセキュリティサーベイ 2018の調査結果をご報告します。本サーベイは今年で3年目の取り組みとなりました。
調査結果を紐解くと、この3年間、セキュリティ侵害の数は減っておらず、企業のセキュリティ投資は年々増加傾向にあります。終わりのない戦いを強いられている企業の姿が浮かび上がってきます。また、我が国全体が働き手不足の事態に直面していますが、セキュリティ人材も圧倒的に不足しており、深刻な問題化していることも窺い知ることができます。これらの傾向は今後も続くのではないかと思われます。

世の中の動きに目を移すと、働き方改革、Inclusion & Diversityをキーワードに多種多様なユーザがいつでもどこからでも会社のアセットにアクセスできる環境が整いつつあります。人手不足の解消、業務効率化を目的にRPAやAIの導入も急速な広がりを見せています。ビジネスフロントでは破壊的テクノロジーを活用した新しいビジネスモデルが日々創出されています。

これらの動きはセキュリティの観点で考えると、重要情報を含む数多くの会社のアセットがファイアウォールの外側に保管され、多種多様なユーザから常にアクセスされていることが常態化していることを意味します。また、ロボットやAI、IoTデバイスに対する内部統制やアクセス制御など、新しいタイプのセキュリティのテーマが発生していることを意味します。そして、何よりもこうした変化がすさまじいスピードで現場主導で起こっているために、セキュリティのゲートキーパーであるIT部門が従来の管理手法ではそのペースに対応しきれなくなってきていることを示唆しています。我々は今こそセキュリティのトランスフォーメーションを実現しなくてはならないのです。

我々KPMGのサイバーセキュリティアドバイザリーグループでは、アドバイザリー業務を通じたサイバーセキュリティに関する問題解決の支援に留まらず、有益な情報を広く社会に提供することも自らの重要な役割であると考えています。本サーベイ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、本サーベイの実施にあたり、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。

2018年9月

KPMGコンサルティング
サイバーセキュリティアドバイザリーグループ
パートナー
田口 篤

Contents

Executive Summary

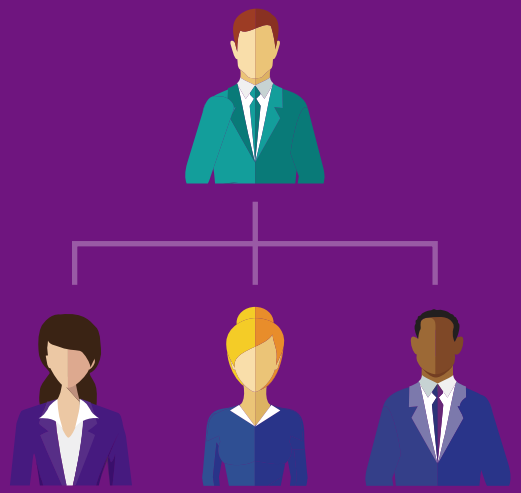
セキュリティ被害の実態と対策の実情

過去3年間の継続調査において、企業ネットワークへの不正侵入の発生状況はほぼ横ばいで、3割程度の企業が攻撃を受けていました。また、不法侵入の多くのケースにおいて、外部からの通報・指摘ではなく、自組織内部での認知に至っています。

見えない対策のゴールとセキュリティ人材の不足

メール／Webセキュリティ、エンドポイントセキュリティといった一般的な対策は回答企業の8割を超える企業で実施済みであり、一定水準のセキュリティ対策が広く普及していることが伺えます。こうした自組織のセキュリティデバイスを活用することで、多くの不正侵入・サイバー攻撃を把握し、対応につなげることができていると思われます。

しかし、日々高度化するサイバー攻撃に対し、さまざまなセキュリティ対策製品が登場する中、自組織がいったいどこまでの対策を行えば十分といえるのか、見えにくくなっている実態があります。また、企業のセキュリティ対策を真に有効なものとするためには、こうしたテクノロジーだけではなく「人・組織」との両輪で対策を推進していくことが重要ですが、多くの企業で、知見を持ったセキュリティ技術者の不足といった人的リソースに関する悩みを抱えています。



専門組織の設置と実践的訓練

こうした状況に対応するためには、経営層にCISO（最高情報セキュリティ責任者）を設置し、トップダウンでセキュリティ対策の推進を主導することが重要です。同時に、CSIRTに代表されるセキュリティ組織の強化や、従業員の意識向上といった全社としての体制整備も欠かせません。

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	2018年4月1日～5月22日
調査方法	株式会社ラックの協力のもと、 郵送によるアンケート票の送付・回収、Webによるアンケートの回収
発送数	8,192件
有効回答数	329件（回収率 4.0%）

回答企業の属性

従業員数（連結）	
1～499人	21.6%
500～999人	21.3%
1,000～2,999人	23.4%
3,000～4,999人	8.2%
5,000～9,999人	7.6%
1万人以上	17.6%
無回答	0.3%
売上高（2017年度連結）	
500億円未満	45.6%
500～1,000億円未満	13.1%
1,000～3,000億円未満	16.7%
3,000～5,000億円未満	5.8%
5,000～1兆円未満	7.6%
1兆円以上	10.3%
無回答	0.9%
業種	
流通	14.6%
製造	36.8%
金融	11.2%
建設・不動産	9.7%
通信・IT・メディア	14.3%
旅行・レジャー・飲食	1.5%
学校	0.9%
運輸・インフラ	5.2%
その他	5.8%

実 態

セキュリティ被害の実態と対策の実情

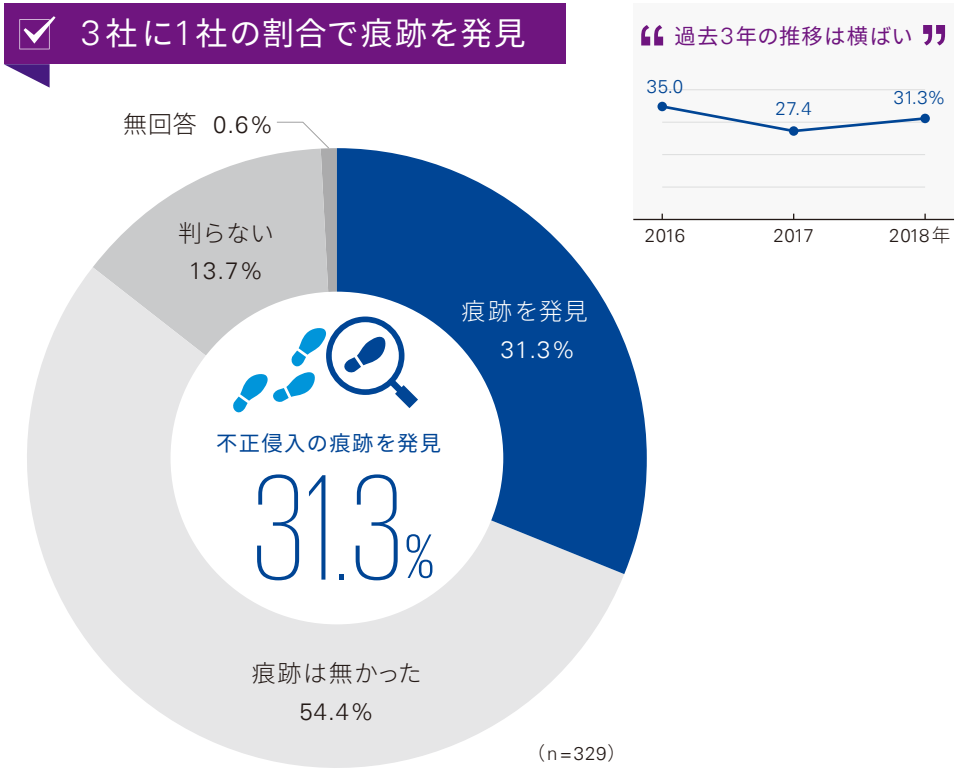
回答企業のうち、3社に1社の割合で、過去1年間に不正な侵入を受けています。8割以上の企業が自社または契約している委託先からの通知により、不正侵入に気付くことができている状態で、近年の防御対策に対するセキュリティ投資が功を奏していると考えられます。

しかしながら、サイバー攻撃の被害については、ランサムウェアなど、業務への被害だけでなく、経済的な損失、委託先・取引先を巻き込んだ被害も出ており、セキュリティ上の脅威は、企業経営にとって、想定上のリスクではなく、現実のリスクです。

不正侵入の痕跡の有無

本年の調査においても、過去1年間で、約3割の企業が不正侵入があったことを確認しています。これは、KPMGコンサルティングが調査を開始した2016年からほぼ横ばいで、約3社に1社の割合で攻撃を受けており、かつその痕跡を発見できていることになります。

不正侵入の痕跡を発見した企業

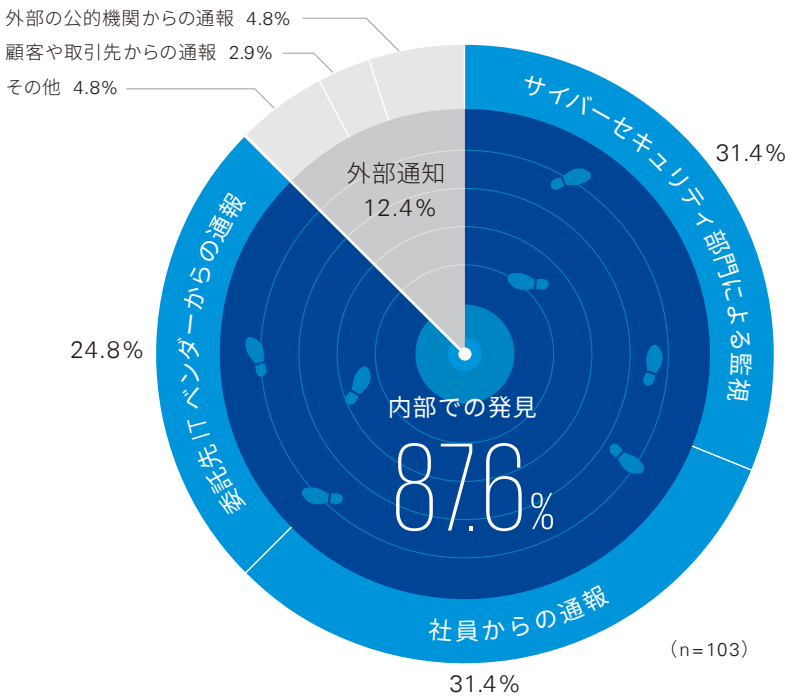


不正侵入に気付いたきっかけ

不正侵入に気付いたきっかけは、社員からの通報と、サイバーセキュリティ部門による監視が同率となり、近年のセキュリティ監視強化の傾向が、自組織内での侵入検知率の向上に貢献していることが伺えます。

不正侵入に気付いたきっかけ

約87%は内部での発見



業務上の被害の有無

ランサムウェアはファイルを暗号化し復合不能とするその攻撃の特徴から、被害が表面化しやすく昨年に続き被害のトップに位置づけられました。
過去1年間の被害内容を見ると、自社の業務やシステムへの影響が多くを占めますが、顧客や取引先を巻き込んだ被害も出ています。

サイバー攻撃による被害

(n=263)

ランサムウェア	16.1%
マルウェア	14.9
ビジネスメール詐欺	9.4
DDoS(サービス妨害)攻撃	7.9
標的型攻撃	5.8
不正ログイン	4.6
フィッシング	4.6
Web サイト改ざん	2.1
ソーシャル・エンジニアリング	1.8
制御システムに対する攻撃	0.9
IoTデバイスに対する攻撃	0.6
その他	1.2

業務上の被害内容(過去1年間)

(n=137)

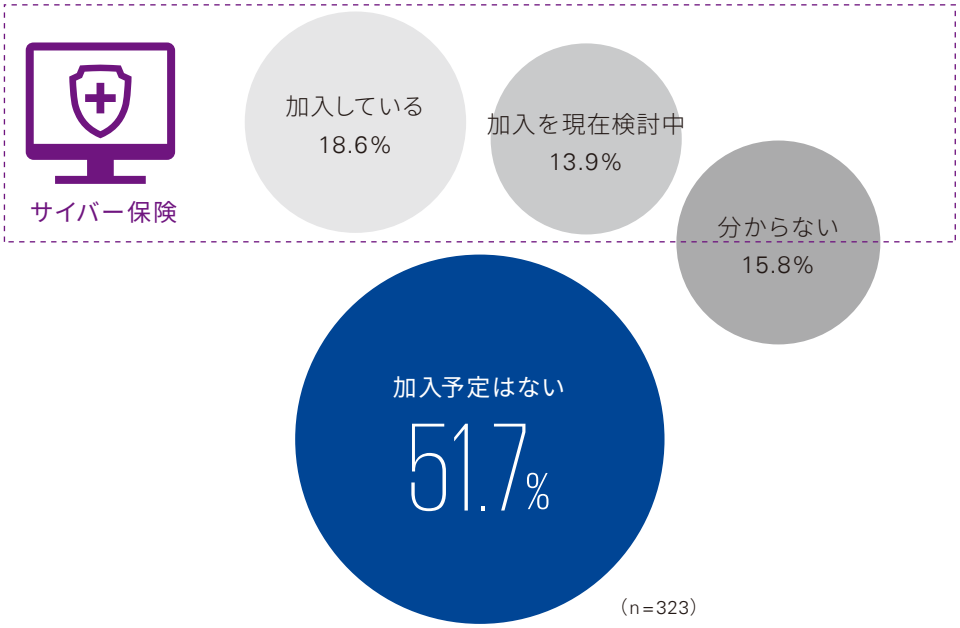
自社の業務やシステムが著しく遅延・中断した	41.3%
自社に経済的な損失が発生した	22.5
システムが踏み台として第三者への攻撃に使われた	10.0
自社の評判が傷ついた	7.5
顧客や取引先に経済的な損失が発生した	7.5
自社の機密情報が漏えいした	3.8
顧客や取引先に間違った情報を提供し混乱させた	3.8
社員の個人情報が漏えいした	1.3
顧客や取引先の機密情報が漏えいした	1.3
顧客や取引先の個人情報が漏えいした	1.3

サイバー保険

欧米では導入が進みつつあるサイバー保険ですが、回答企業の約半数が加入予定はないと回答しています。
日本では、組織構築、技術的対策の導入といったセキュリティ対策に投資する組織が大多数を占めているため、限られたセキュリティ予算をサイバー保険へ回すという判断をする組織はまだ少数派と言えるでしょう。

サイバー保険への加入

約半数が加入予定はない



COLUMN

サイバー保険の現在

セキュリティリスクマネジメントにおける対策には「低減」「保有」「回避」「移転」の考え方があるが、サイバー保険はこのうちの「リスクの移転」(リスクを他社等に移す対策)に相当する対策である。平成29年11月に経済産業省が公開した「サイバーセキュリティ経営ガイドライン Ver 2.0」においても、リスク移転策の例として、「クラウドサービスの利用」と併せて「サイバー保険の加入」が挙げられている。

一般的な保険と同じように、セキュリティインシデントが発生した際に金銭的な補償を受け取ることができる点が加入のメリットである。その補償範囲も、サービス停止による収益減少、営業継続費用、事故調査費用や損害賠償費用といった幅広い損害に対応する商品も少なくない。また、セキュリティ専門ベンダと協業して、インシデントの初動対応から収束までの支援を付帯サービスとして提供する商品もある。

サイバー保険の検討にあたっては、自社において想定されるインシデントやその予想被害額をあらかじめ算定するなどしたうえで、実際の補償範囲や各種条件を比較し、被害低減に有効な商品を選択することが重要といえる。

サイバー脅威動向収集のための活動

業態や組織規模を問わないランサムウェアのような無差別攻撃、ビジネスメール詐欺のような標的型攻撃等、自組織が直接被害にあっていない場合でも、サイバー脅威の動向を収集することにより、攻撃内容を事前に把握し、攻撃の検知・対応・復旧への準備に役立てることが可能になるため、サイバー脅威動向を収集することは非常に重要です。

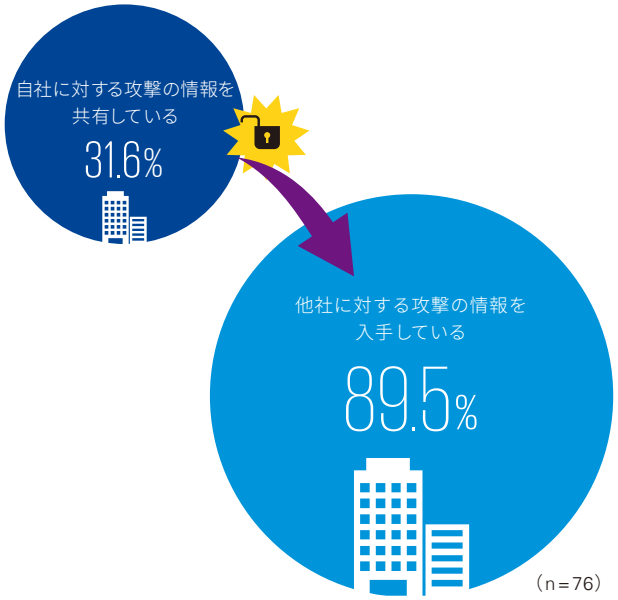
情報共有を行うコミュニティに所属している企業では、9割近い企業が他社に対する攻撃情報の取得を行っているものの、自社に対する攻撃情報を共有している企業は3割程度に留まっております。社会インフラを担う企業では、個々の企業への攻撃が社会への影響を与える可能性も高く、また昨今の攻撃動向では業界全体を狙った標的型攻撃も横行しているため、自社の脅威情報共有という形での社会貢献ととらえた積極的な共有を推奨します。

サイバー脅威動向収集のための活動

News 75.9%	日常業務の一環としてオープンソースの情報（Webサイト／ニュースなど）を収集している
46.0%	政府機関や非営利団体からの情報配信を受けている
22.8%	業界内の**情報共有コミュニティ（ISACなど）**に加入している
21.9%	民間事業者による有償サービスの提供を受けている
9.6%	何もしていない

（n=325）

サイバー攻撃の情報共有（情報共有コミュニティに参加している企業）



（n=76）

COLUMN

情報セキュリティ共有組織（ISAC）とは

ISAC（Information Sharing and Analysis Center）とは、同業界の事業者間でサイバーセキュリティに関する情報を共有し、セキュリティインシデントへの対応力や攻撃への防御力の向上を目指すための組織である。

米国においては1999年から2000年にかけて金融、通信、電力、緊急時対応の4分野においてISACが設立され、その後、化学、エネルギーなどさまざまな分野におけるISACが設立された。日本国内においても、金融分野における金融ISAC、電力分野における電力ISAC、電気通信事業者を中心に放送事業者やセキュリティベンダー等が参加するICT-ISACなどがある。

課題1

見えない対策のゴール

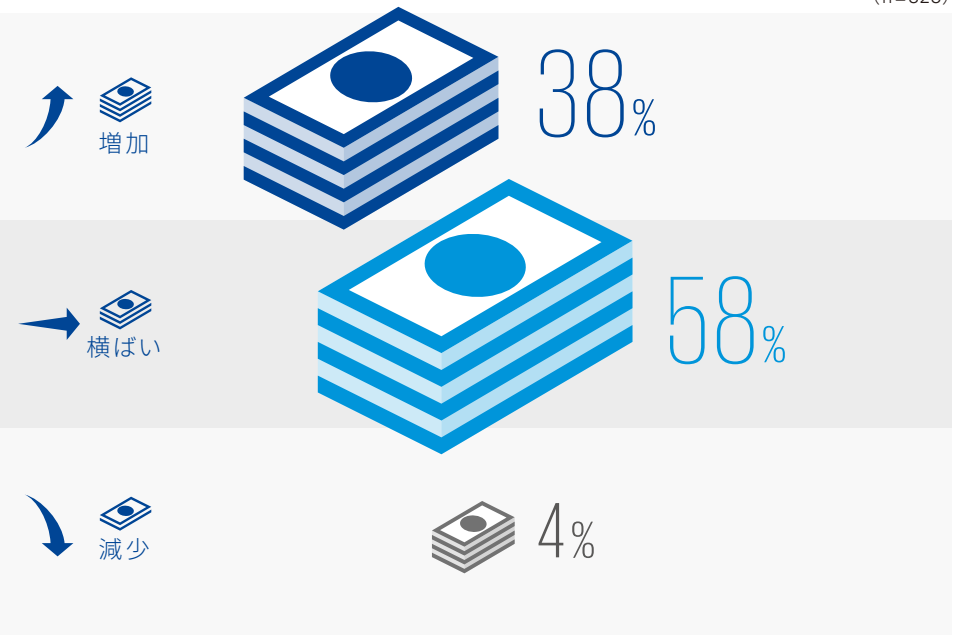
今後のサイバーセキュリティ対策への投資額

2018年度のサイバーセキュリティ対策への投資額は、2017年度に比べて横ばい、もしくは増加と答えた企業が94.5%に上り、全体としては増加傾向にあります。

2018年度と2017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にある

（n=323）



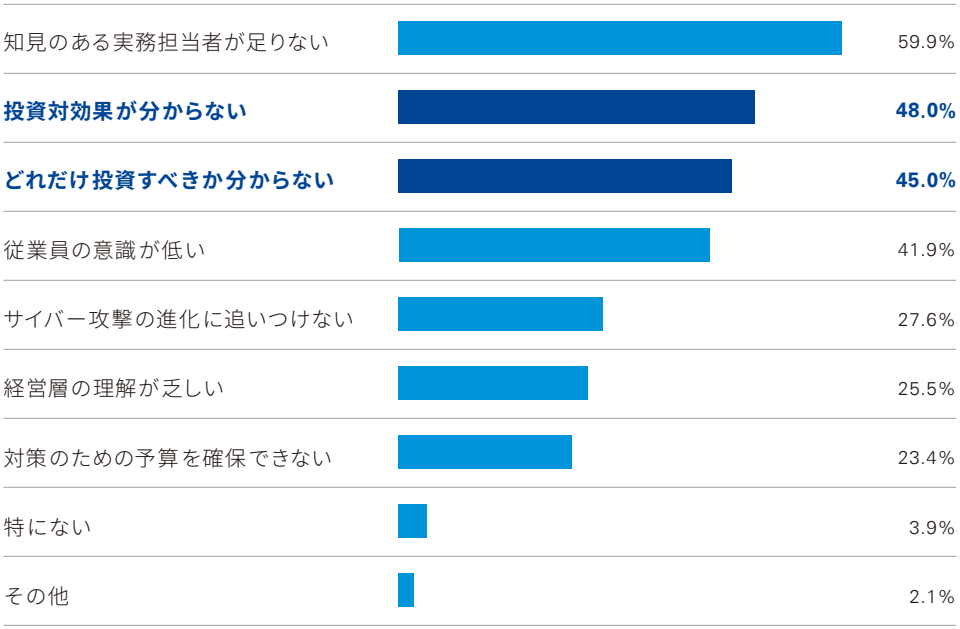
しかし、「サイバーセキュリティ対策に取り組むうえでの課題」として、「知見のある実務担当者が足りない」とともに、「投資対効果がわからない」「どれだけ投資すべきか分からない」が上位に挙がっており、サイバーセキュリティ対策への投資が不足していることは把握しているものの、実際にどれだけの投資をすれば十分な対策を行っていると言えるのか、悩んでいる実態が伺えます。

65%の企業が自社のサイバーセキュリティ対策への投資額が「大いに不足している」あるいは「やや不足している」と回答しています。一方、自社のサイバーセキュリティ対策への投資額が適切であると評価している企業は回答企業全体のおよそ3分の1に留まります。

サイバーセキュリティ対策に取り組むうえでの課題（複数選択可）

投資対効果や適切な投資額が分からないという悩みも

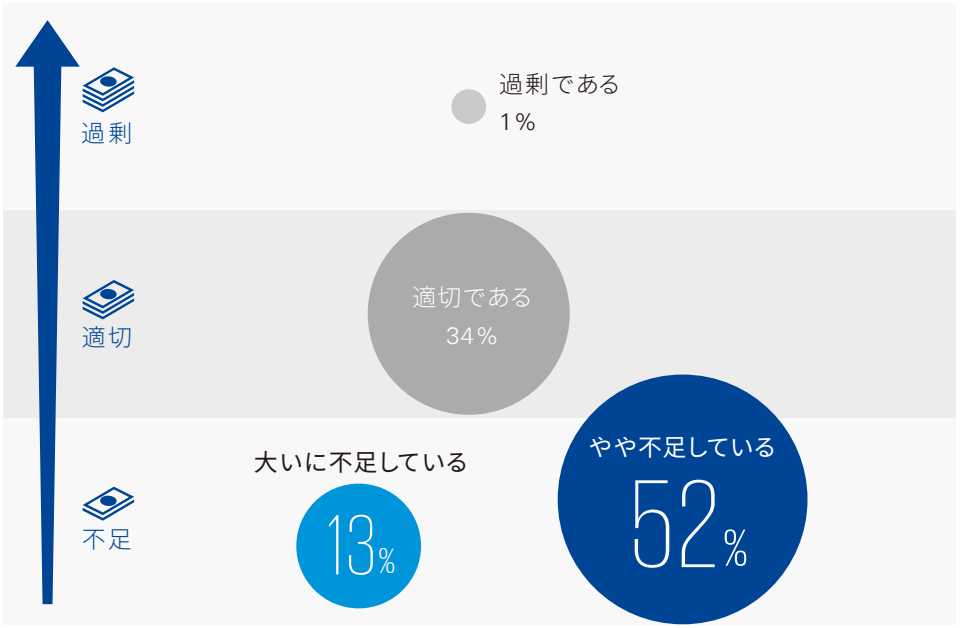
（n=327）



現状のサイバーセキュリティ対策への投資額

65%が「不足している」と回答

（n=323）



課 題 2

セキュリティ人材の不足

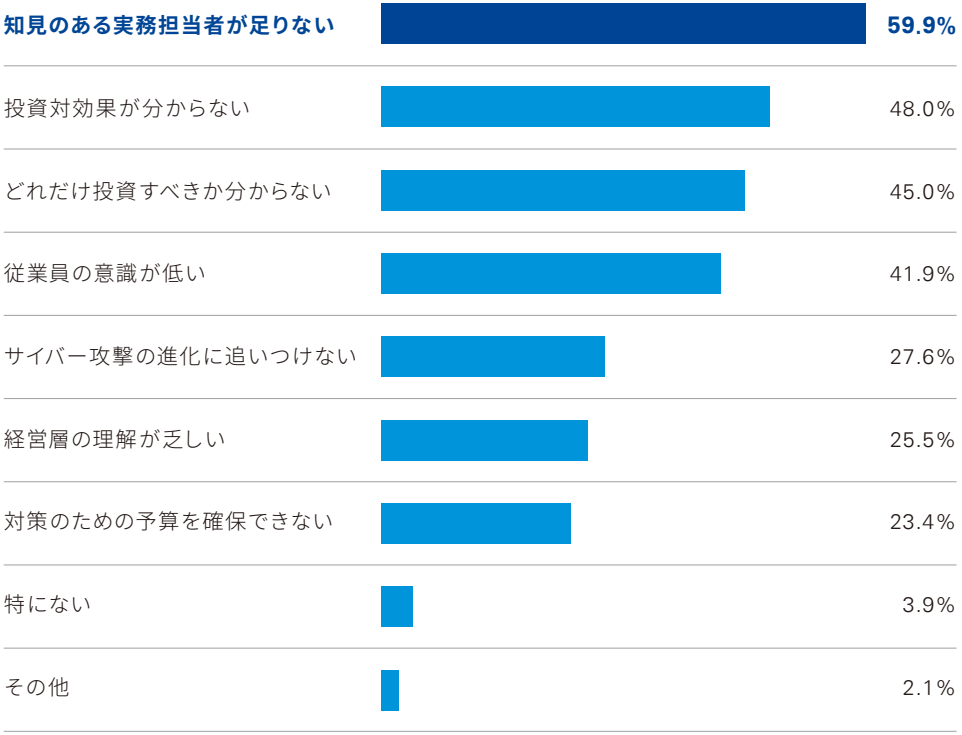
セキュリティ人材不足

さまざまな課題の中「知見のある実務担当者が足りない」を挙げた企業が最も多かったです。

サイバーセキュリティ対策に取り組むうえでの課題（複数選択可）

セキュリティ人材の不足が最も大きな課題としてあがっている

（n＝327）

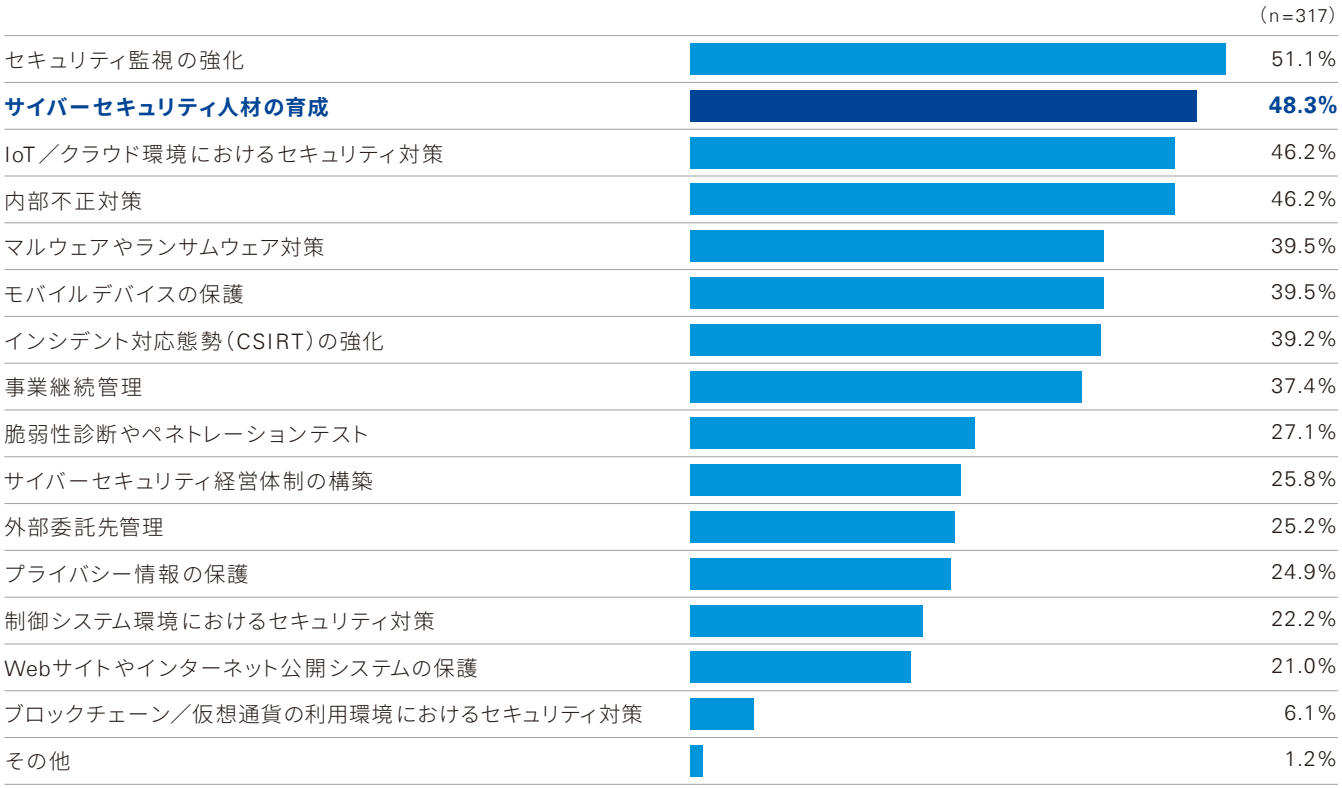


今後積極的に取り組むサイバーセキュリティ対策領域

さまざまな技術領域への対策について取り組む中、やはりサイバーセキュリティ人材育成の必要性が強く認識されていることが伺えます。

今後積極的に取り組む対策領域（複数選択可）

☑ サイバーセキュリティ人材の育成を急務ととらえる企業が多数



課題3

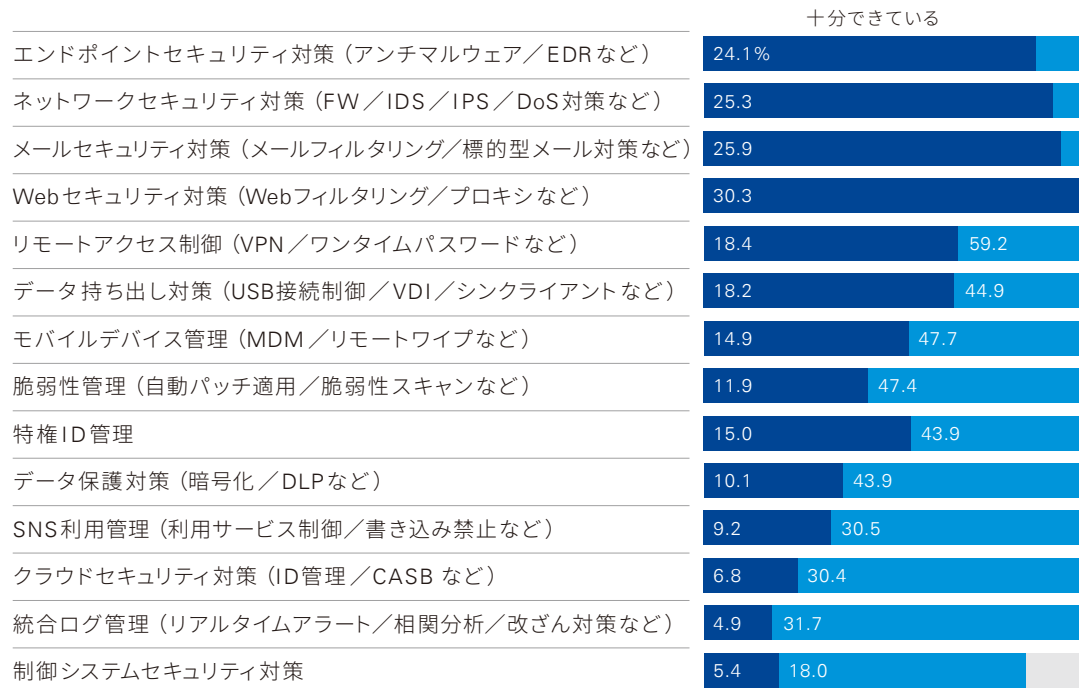
制御セキュリティ・クラウドへの取組み

サイバーセキュリティ対策の実施状況

一般的なネットワークセキュリティや、メール／Webセキュリティ、エンドポイントセキュリティといった対策は8割を超える企業で一巡していると考えられます。しかし、クラウドセキュリティ対策などの新しい技術領域の対策はあまり進んでいるとはいえず、特に制御システムセキュリティ対策の実施状況は低い水準にあります。

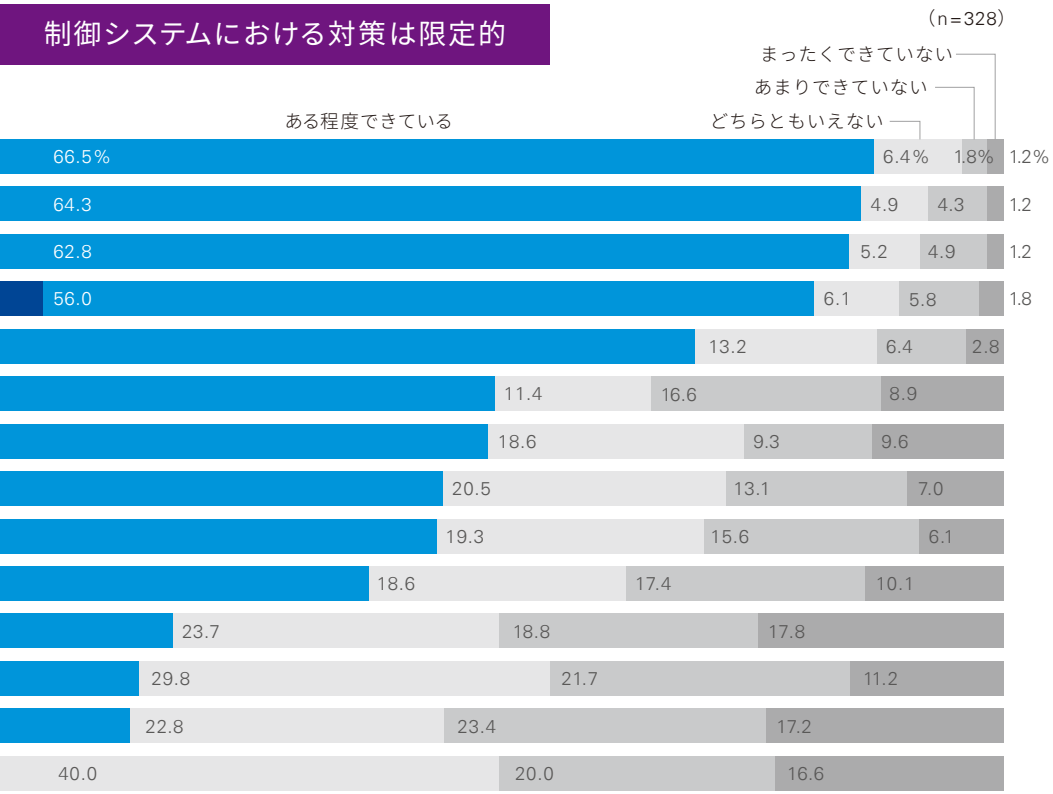
サイバーセキュリティ対策の実施状況

OA環境における一般的な対策はほとんどの企業で実施済みである一方、



今日の制御システムは、必ずしもインターネットから隔離された安全なネットワーク上ではなく、OA環境を含む情報系ネットワークと接続されるケースも増加しており、制御システムに対するサイバー攻撃対策の充実は急務といえます。

制御システムにおける対策は限定的

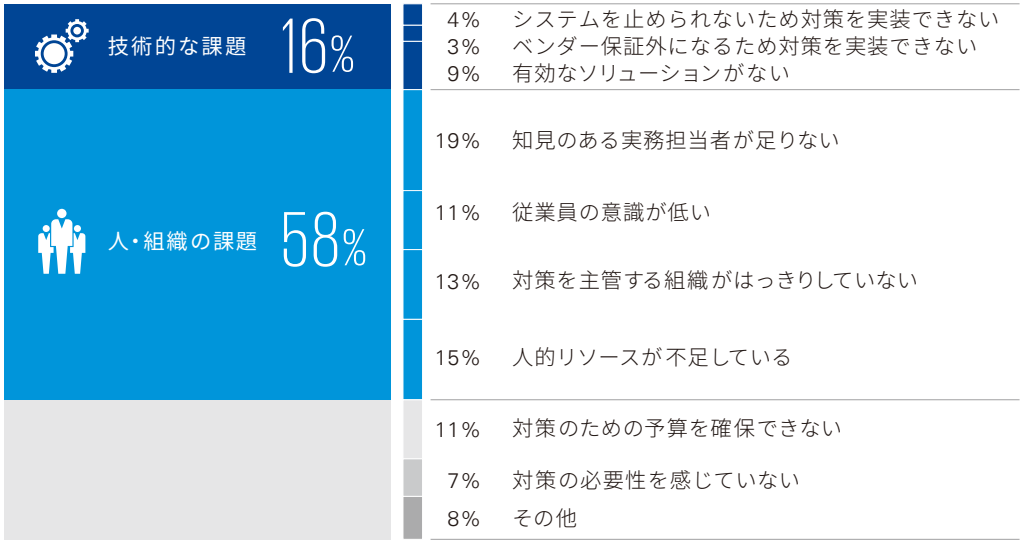


制御系システムセキュリティ対策における課題

「システムを止められないため対策を実装できない」「ベンダー保証外になるため対策を実装できない」「有効なソリューションがない」といった、技術的な課題は10%程度に留まり、「知見のある実務担当者がいない」「従業員の意識が低い」「対策を主管する組織がはっきりしていない」「人的リソースが不足している」といった、人・組織に関する課題が大勢を占めることがわかりました。既存のセキュリティ対策組織との所掌整理を含めた組織体制の整備と、限られた人員でサイバーセキュリティ対策を推進するための仕組みづくりが必要といえます。

制御系システムセキュリティ対策が進まない原因

「技術」よりも「人と組織」に関する課題が大勢を占める

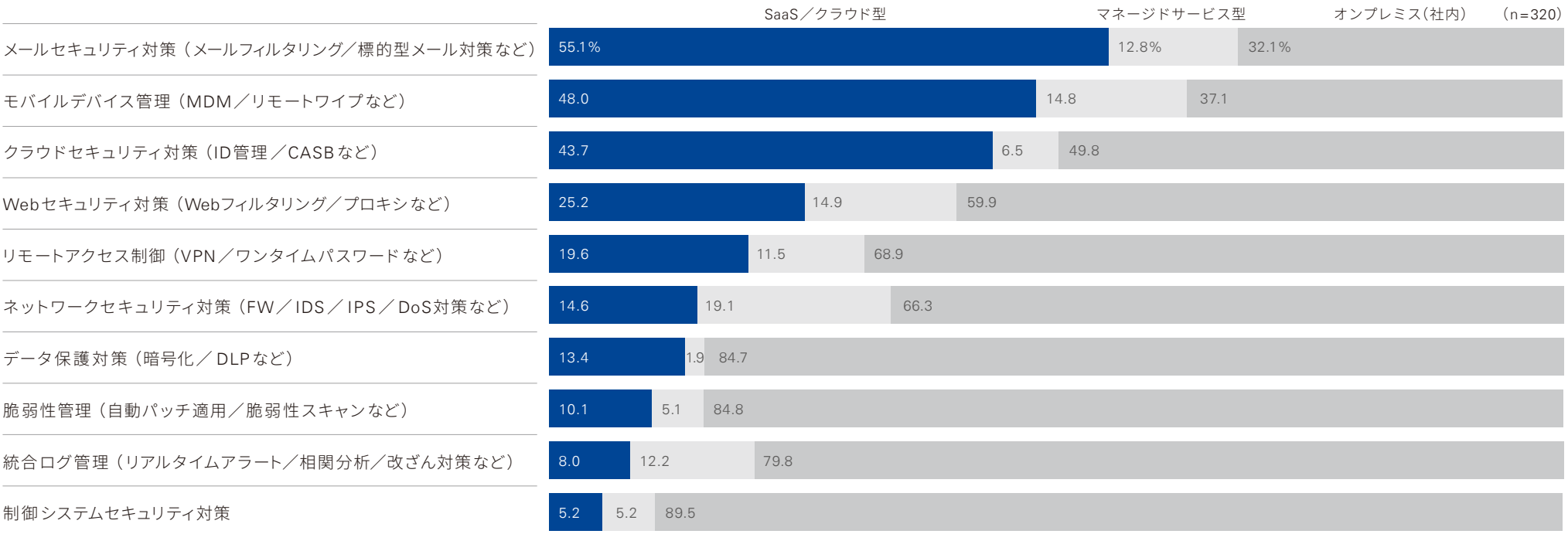


セキュリティ機能のクラウド活用状況

「モバイルデバイス管理」や「メールセキュリティ対策」といった、クラウドと相性がよいと思われるセキュリティ機能は比較的クラウド化が進んでいますが、それ以外の領域においてはオンプレミス型の比率が高いです。業務システムのクラウド化に応じて今後さまざまなセキュリティ機能がクラウドに移行すると思われます。

セキュリティ機能のクラウド活用状況

☑ クラウドを活用したセキュリティ機能の実装はまだ部分的

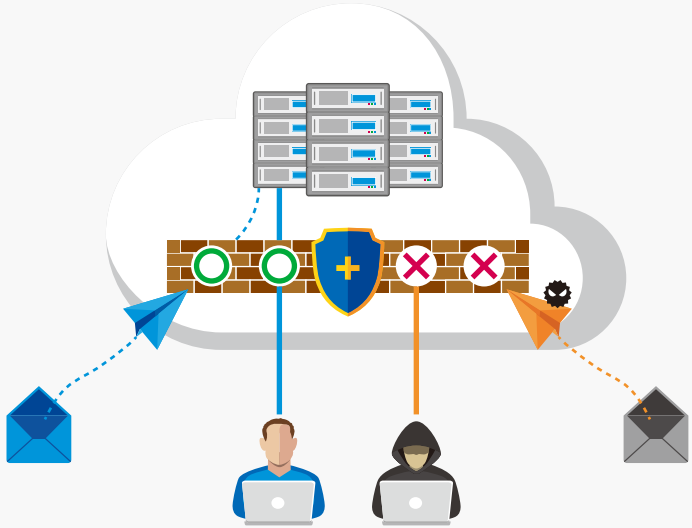


COLUMN

セキュリティ機能のクラウド化

アンチスパムやアンチウイルスといったメールセキュリティ対策は、コモディティ化が進んで久しく、内部ネットワークに配置する必要も無いため、クラウドの活用が進んだのは自然な流れといえる。

一方、今回の調査結果からWebセキュリティ対策の状況を見ると、メールセキュリティ対策の半分程度しかクラウド化が進んでいない点は興味深い。昨今のHTTPS通信の増加や、将来の通信料変動などに対し、オンプレミスに比べてリソース面で柔軟に対応できるクラウドサービスの活用はメリットが多いと思われるため、今後、より一層の成長が見込まれるのではないだろうか。



課題4

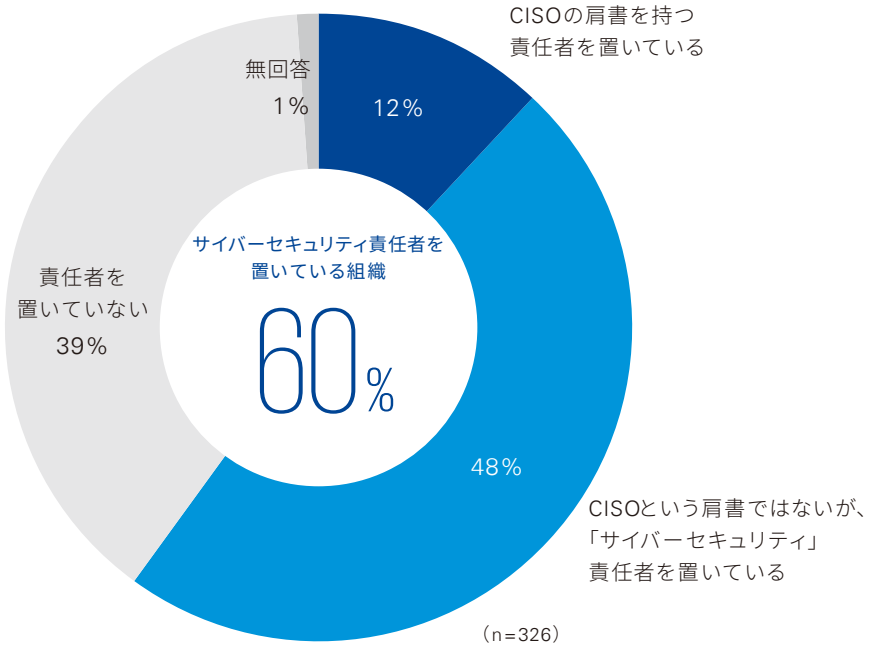
専門組織の設置と実践的訓練

CISOの設置

インシデント発生に備えた具体的な対策の整備にあたり、重要な役割を担う、CISO（最高情報セキュリティ責任者）及びCSIRTの整備状況を見ると、CISOという肩書ではないが、「サイバーセキュリティ」責任者を置く組織は、回答企業のうち約半数近くあり、CISOの肩書を持つ責任者を置いている12%と合わせると60%となり、企業でのCISO設置の重要性の理解は年々進んでいると言えます。

CISOの設置有無

「サイバーセキュリティ」責任者を置く組織は60%

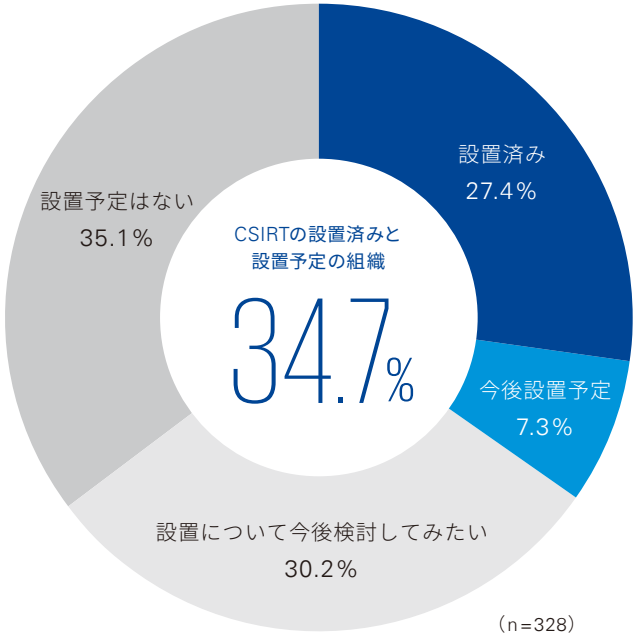


CSIRTの設置

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であるCSIRTの設置に関しては、設置済みと今後設置予定を合わせて35%に満たず、多くの組織では、サイバー攻撃対応への専門組織やチームの設置が遅れていることを示しています。

CSIRT設置の現状

CSIRTの設置済みと設置予定を合わせて35%に満たない

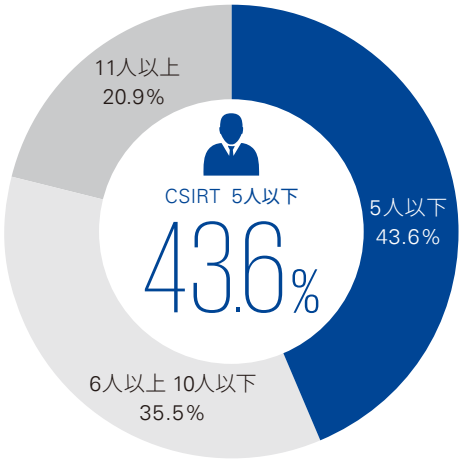


（n=328）

CSIRTの適切な要員配置とは(1/2)

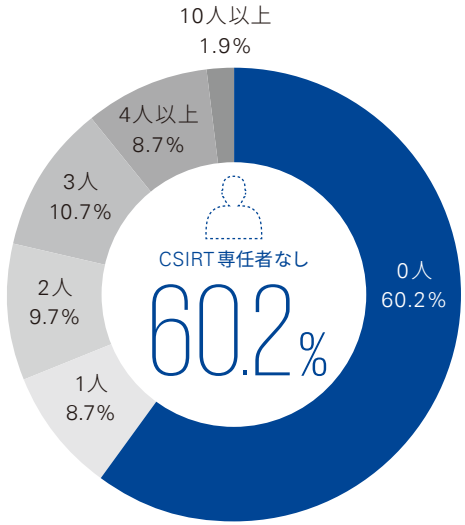
CSIRT設置済み、今後設置予定と回答した組織では、CSIRT要員が5人以下の組織が、約半数の43%を占めていました。また、CSIRT要員の専任者についての質問では、専任者なしと回答した組織が最も多く6割を占めていました。CSIRTは設置しているが、専任者はおいておらず、他業務を行うメンバーが兼務するといった形が多いと考えられます。

CSIRT人数



（n=112）

CSIRT専任者数



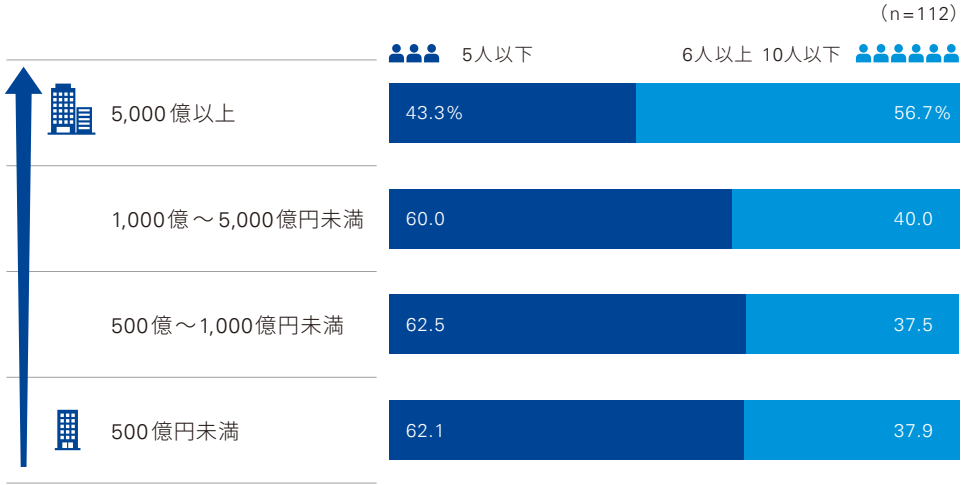
（n=105）

CSIRTの適切な要員配置とは(2/2)

また組織の売り上げ規模別に、CSIRT要員の人数を見ていくと、500億円未満の小規模な組織では、5人以下のCSIRTが大多数を占めており、5,000億円以上の大規模組織では、CSIRT要員も6人以上の組織が半数以上を占めています。組織の規模とCSIRT要員の人数は比例関係にあります。

企業規模に見るCSIRT人数

☑ 組織規模に応じたCSIRT要員の人数の配置が一般的



COLUMN

CSIRTは専任であるべきか

2012年に内閣サイバーセキュリティセンターが発行した「政府機関の情報セキュリティ対策のための統一基準群」にCSIRTが明記されて以来、民間企業においてもCSIRTの設置が進んでいる。しかしながら、自社にCSIRTを設置するにあたって、そのメンバーは専任であるべきか、最適サイズは何人なのか、多くの企業担当者が頭を悩ませている。

多くの企業で陥る失敗例としては、CSIRTに求められる業務量の把握が不十分であるため、他業務との兼任として配置されたメンバーの業務量がひっ迫し、CSIRTが機能しなくなってしまうケースである。

これを解決するには、まず、CSIRTの基本的な役割である、連絡窓口、インシデント対応、情報収集、脆弱性分析、インシデント詳細解析（フォレンジック）の各タスクについて、平時・インシデント時の業務量を見積り、可視化することが重要である。次に、業務量が可視化されたタスクにメンバー候補の現時点での空き業務時間を当てはめ、兼任での活動が可能かを見極める。すると、専任にすべき役割またはメンバーとその規模が見えてくる。

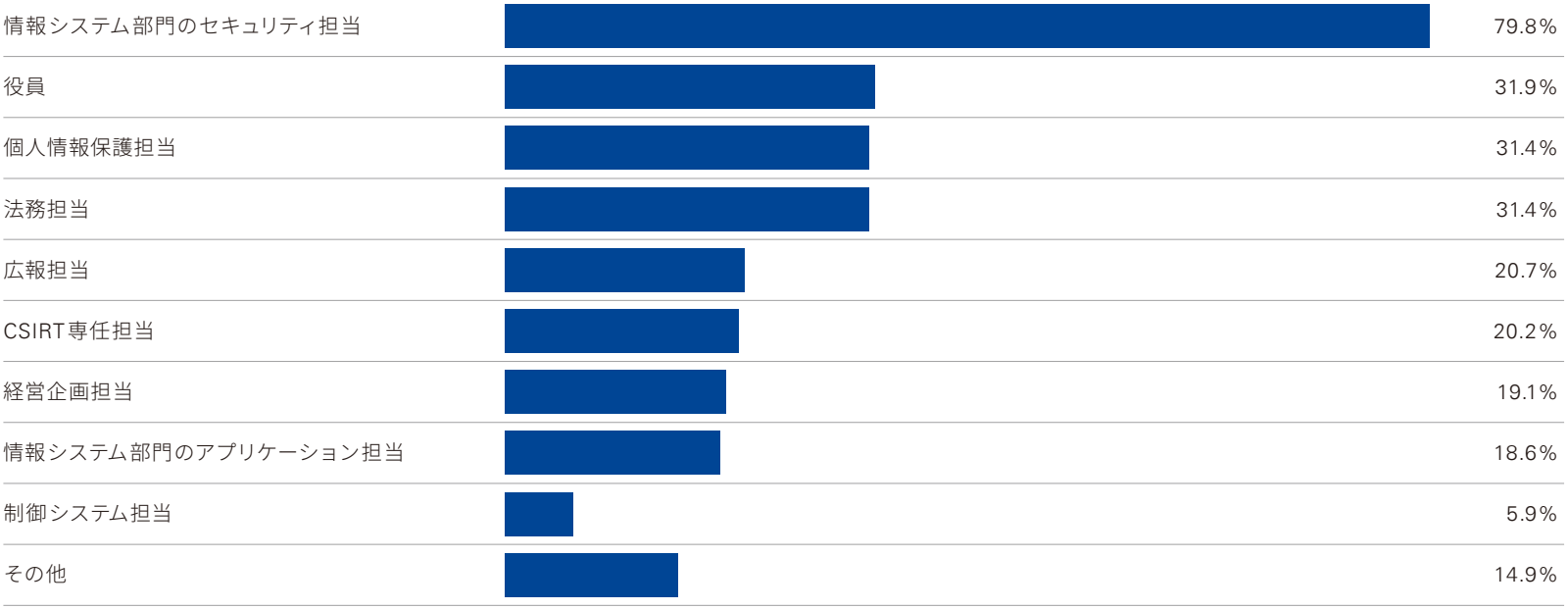
CSIRTに含む担当メンバー

CSIRTにはどのような役割の担当メンバーを含めるべきでしょうか。CSIRT設置済みまたは今後設置予定と回答した組織では、以下のような役割のメンバーが含まれています。インシデント発生時に、被害拡大の防止を図るための、技術的な対応と、組織内外の関係者との情報連携、情報開示を担うために、組織内のさまざまな部署から適切な役割を持った担当者を配置しておく必要があります。インシデントが発生してから適切な担当者探しに奔走しないためにも、緊急時の対応体制を整備し、その有効性検証、および担当メンバーへの対応レベル向上のための研修を兼ねた実践的な演習を行うことが望ましいです。

CSIRTに含む担当メンバー（CSIRT設置済みまたは今後設置予定企業の回答）

☑ 技術的な担当者と、組織内外との情報連携・情報開示を担うための担当者を配置しておく必要がある

（n=188）



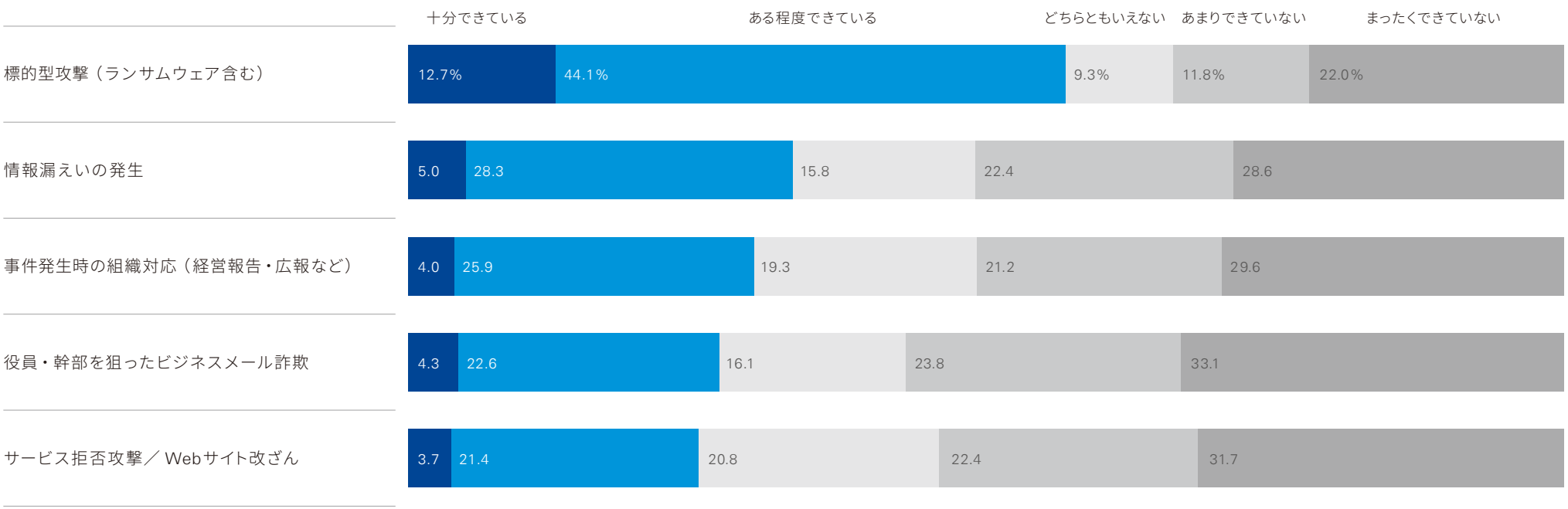
インシデント発生に備えた訓練や演習の実施

メールによる標的型攻撃の横行から、「訓練用標的型メールを配信し、受信者の開封率を測る」標的型メール訓練は半数以上の組織である程度は実施されており、普及してきているといえるでしょう。
一方で、サイバーセキュリティ経営ガイドラインVer 2.0で言及されているのは、業務停止等に至った場合の企業経営への影響を考慮したより広範囲かつ多くの対象者を巻き込んだ実践的な演習です。
事件発生時の組織対応（経営報告・広報など）の訓練・演習については、ある程度できているとしているのが、30％弱の企業にとどまっており、2018年5月に施行された欧州一般データ保護規則（GDPR）の72時間以内報告と相まって、取り組むべき課題としての重要度が増しています。

インシデント発生に備えた訓練や演習の実施

☑ 事件発生時の組織対応（経営報告・広報など）については、取り組むべき課題として重要度が増している

（n=323）



インシデント発生に備えた具体的な対策整備の実情

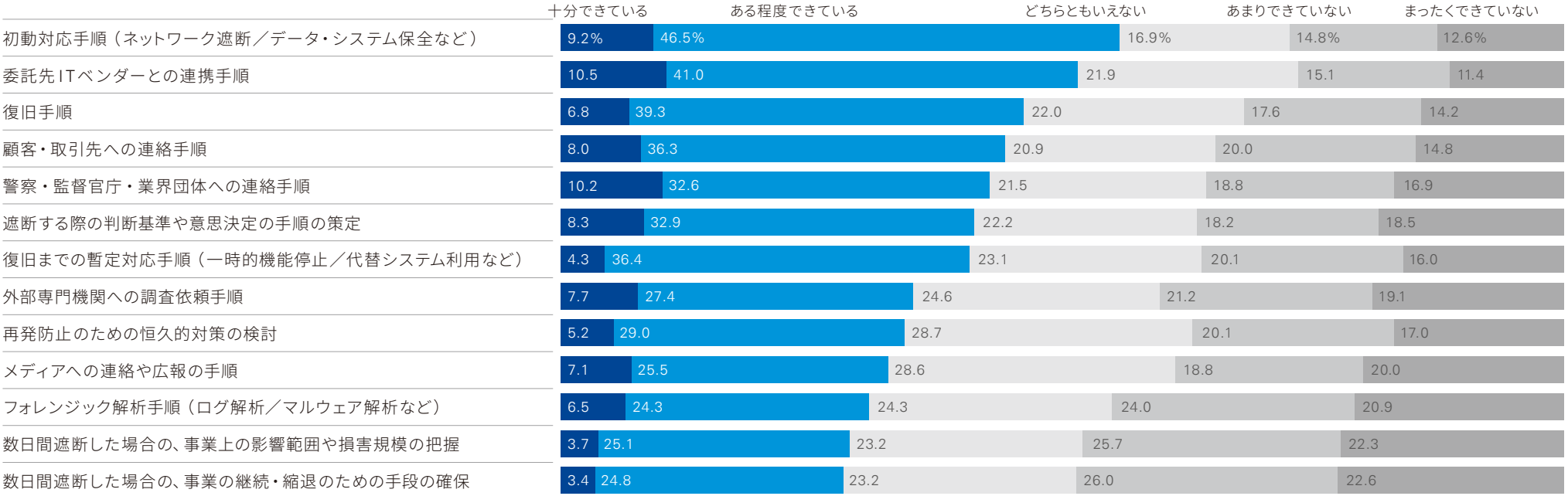
インシデント発生に備えた具体的な準備や対策整備の状況では、初動対応手順など、検知・隔離に関わる対策について十分にできている、ある程度できているとする企業が半数を超えていますが、第三者への情報連携に関わる準備については、半数以上の企業は十分な緊急連絡体制が整っていない状況であることが伺えます。

組織内での緊急連絡体制の整備とともに、第三者への連携、支援要請、報告についても、事前に整備、実践的な演習を通して、その有効性を検証しておく必要があるでしょう。

インシデント発生に備えた具体的な対策整備の状況

☑ 第三者への情報連携に関わる準備については、半数以上の企業が十分な緊急連絡体制が整っていない状況

（n=325）



Contact us

KPMGコンサルティング株式会社
サイバーセキュリティアドバイザリー

TEL：03-3548-5111
kc-cybersecurity@jp.kpmg.com

www.kpmg.com/jp/cyber-security