KPMG

サイバーセキュリティ サーベイ 2017

はじめに

全世界的に被害を及ぼす、大規模なサイバー攻撃が数多く報告されています。これらのサイバー攻撃の中には、重要インフラに対するものも含まれ、経済活動に大きな被害を与えています。IoT（Internet of Things）の拡大により、現代社会はインターネットへの依存度を高めています。この来たるべきIoT社会を安心・安全に迎えるために、サイバーセキュリティの重要度は一層高まっています。

日本でも、2015年12月に「サイバーセキュリティ経営ガイドライン」が経済産業省より公開されました。同ガイドラインでは、企業はサイバーセキュリティの確保を経営課題として位置づけ、CISO（最高情報セキュリティ責任者）を中心とした管理体制を構築することが求められています。本サーベイは、CISOまたは情報セキュリティ責任者を中心とした「サイバーセキュリティ経営」の推進の実態を明らかにすることを目的として実施しました。

多くの企業が「サイバーセキュリティ経営」を推進している一方で、課題も明らかとなってきました。サイバー攻撃がピークとなると見込まれる2020年の東京オリンピック・パラリンピックに向け、それほど時間は残されていません。サイバーセキュリティの推進は、より一層、経営者がリーダーシップをとって進めていかなければなりません。

KPMGサイバーセキュリティアドバイザリーは、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、少しでも皆様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、今回のサイバーセキュリティサーベイ実施にあたり、ご回答いただきました多くの皆様に心から御礼を申し上げます。

2017年6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

目次

エグゼクティブサマリー

セキュリティ被害の実態と対策の実情

企業の4社に1社は過去1年間に不正な侵入を受けています。しかし、進化を続けるサイバー攻撃の脅威に対して継続的に対策を更新するとともに、緊急時の即応体制を訓練するなど、実効性のある対策と態勢を整えてある企業は、全体の2〜3割程度しかありません。

情報セキュリティはITによる対策の域を超えていない

企業の情報セキュリティ対策は、事業の継続や訴訟リスクへの配慮が不足している懸念があります。サイバー攻撃が発生した際には、技術面の対応に追われ、経営を揺るがす問題に発展するのをくい止められないかもしれません。経営層とセキュリティ担当部門の連携をより一層強化し、マネジメント・テクノロジー・オペレーションの機能を高度化させる必要があります。

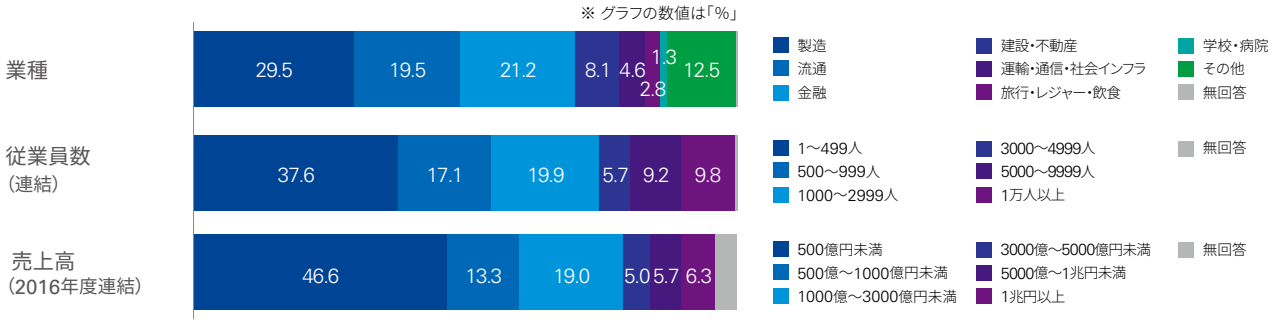
サイバーセキュリティ経営を実践するために

サイバーセキュリティリスクを適切に管理するためには、まず経営層が対策の現状を的確に理解できていなければなりません。そのためには、経営層にCISO（最高情報セキュリティ責任者）を置き、トップダウンでセキュリティの推進を主導する必要があります。同時に、セキュリティ部門の強化や全社員の意識向上など、全社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500億円以上の未上場企業の情報セキュリティ責任者
調査期間	：	2017年4月17日〜5月15日
調査方法	：	郵送によるアンケート票の送付・回収
発送数	：	6159件
有効回答数	：	457件（回収率7.4%）

回答企業の属性



実態
セキュリティ被害の実態と対策の実情

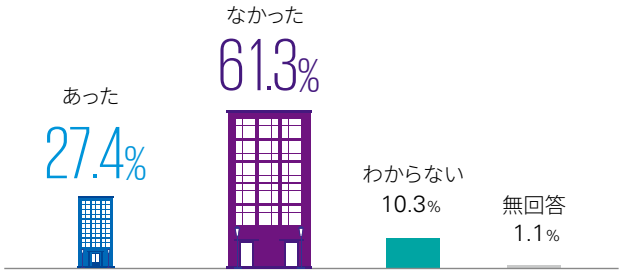
過去1年間に実被害の有無を問わず、サイバー攻撃による不正な侵入を受けた痕跡が見つかった企業は27.4%、およそ4社に1社に上ります。

国内外で猛威を振るうランサムウェアでも、22.3%の企業に業務上の被害が発生。金銭詐取や顧客への補償、対応人件費・機会損失費用など、過去1年間の合計損失額をわからないと回答した企業は2割でした。

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。

サイバー攻撃による業務被害は企業の3割で発生

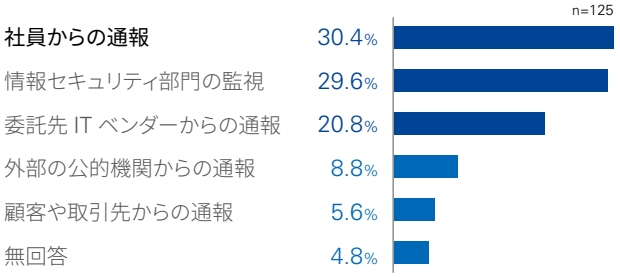
不正侵入の痕跡の有無
3割弱の企業が痕跡を発見



n=457

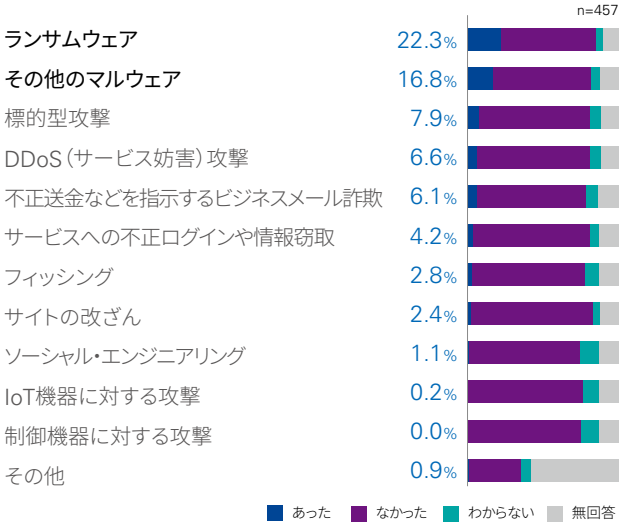
不正侵入に気づいたきっかけ
社員からの通報が最多

n=125



業務上の被害の有無
ランサムウェアでは
2割の企業に業務上の被害が発生

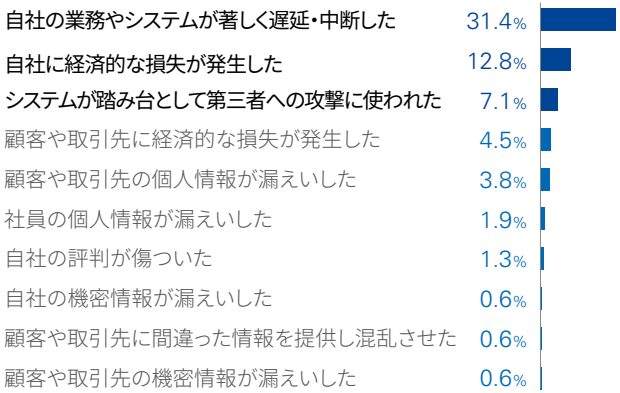
n=457



警察への届け出
ランサムウェア被害で届け出たのは2%

n=102

過去1年間の被害内容



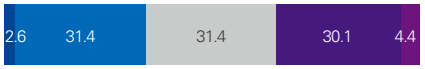
過去1年間の合計損失額 n=156

対策の実効性を高める取組みが不十分

最新情報を自社の対策に取り込む

34.1%

n=455



十分できている / ある程度できている / どちらとも言えない / あまりできていない / まったくできていない

攻撃時の初動対応マニュアルを整備する

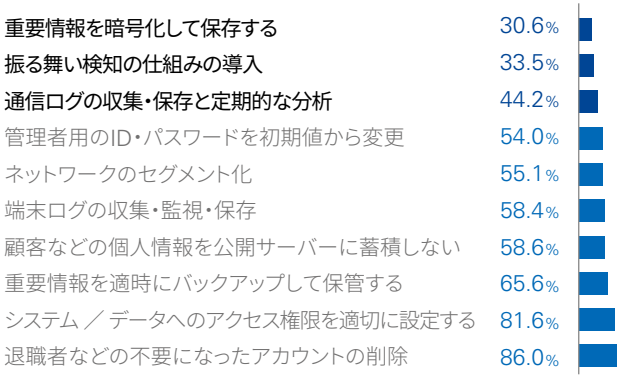
36.6%

n=456

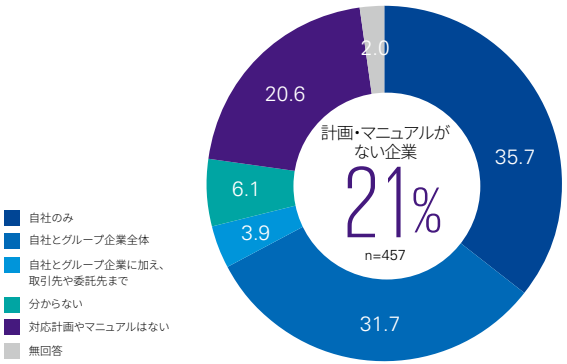
十分できている / ある程度できている / どちらとも言えない / あまりできていない / まったくできていない

■ 不正侵入等を前提とした技術的対策の実施状況

n=457



■ 対応計画やマニュアルの対象範囲



攻撃への定期的かつ実践的な演習・訓練を行う

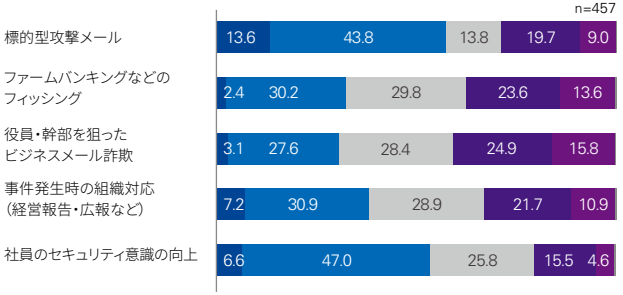
25.2%

n=456

十分できている / ある程度できている / どちらとも言えない / あまりできていない / まったくできていない

■ 教育・訓練・演習の実施状況

n=457



十分できている / ある程度できている / どちらとも言えない / あまりできていない / まったくできていない / 無回答

サイバーセキュリティ保険への加入状況

23.9%

n=457

加入している / 加入を現在検討中 / 加入予定はない / 分からない / 無回答

■ サイバーセキュリティ保険の補償範囲

n=56

セキュリティ上の脅威が現実のリスクとなりつつある中、不正侵入等を前提とした技術的対策と、攻撃時の初動対応マニュアルの整備や演習・訓練ができている企業は、全体の2～3割に留まります。

また、サイバーセキュリティ保険への加入については、検討中の企業も含めて調査企業の4分の1に留まりました。しかし、昨今の大規模なサイバー攻撃による被害の増加により、侵入されることを前提とした対策の一環として、今後加入が増加していく可能性があります。

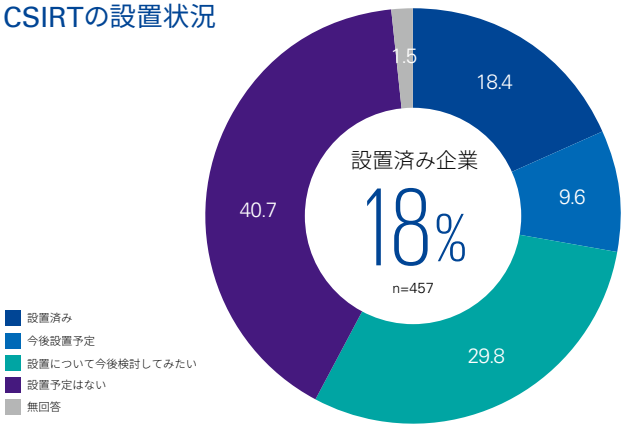
CSIRTを設置済みの企業は2割に満たない

サイバー攻撃などのインシデントに対応する組織である「CSIRT（Computer Security Incident Response Team）」を設置済みの企業は2割弱に留まります。設置予定がない企業は、4割にも達しています。設置済み企業が多い業種は金融業で3割強。設置予定がない企業は、「従業員999人以下」（50.8%）、「売上高1000億円未満」（50.4%）に多い傾向があります。

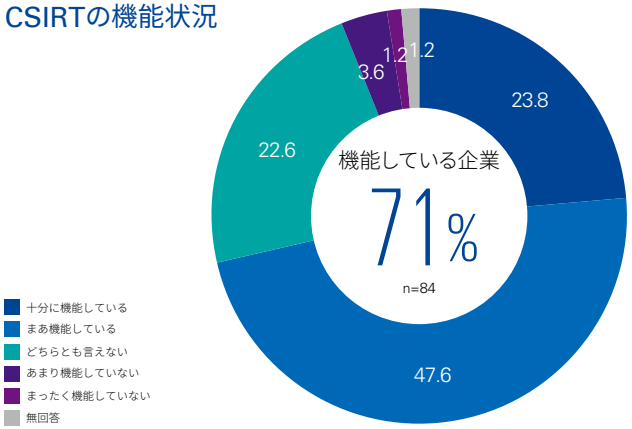
9割の企業は、CSIRT（設置予定を含む）の構成員として情報システム部門のセキュリティ担当者を配置しています。情報システム部門以外では、それぞれ3割前後の企業が個人情報保護・広報・経営企画の担当者を配置しています。法務担当者を配置しているのは全体の4分の1程度。役員をメンバーとしている企業は28.1%です。

7割超の企業は、自社のCSIRTが「機能している」と評価しています。ただし「十分に機能している」と評価した企業は4社に1社程度に留まります。

CSIRTの設置状況



CSIRTの機能状況



CSIRTの陣容

専任者平均	全体平均	
1.4人	9.3人	n=128

業種別のCSIRT設置状況

製造業 n=135 **16.3%**

流通業 n=89 **7.9%**

金融業 n=97 **33.0%**

CSIRTの設置予定がない企業

従業員数別

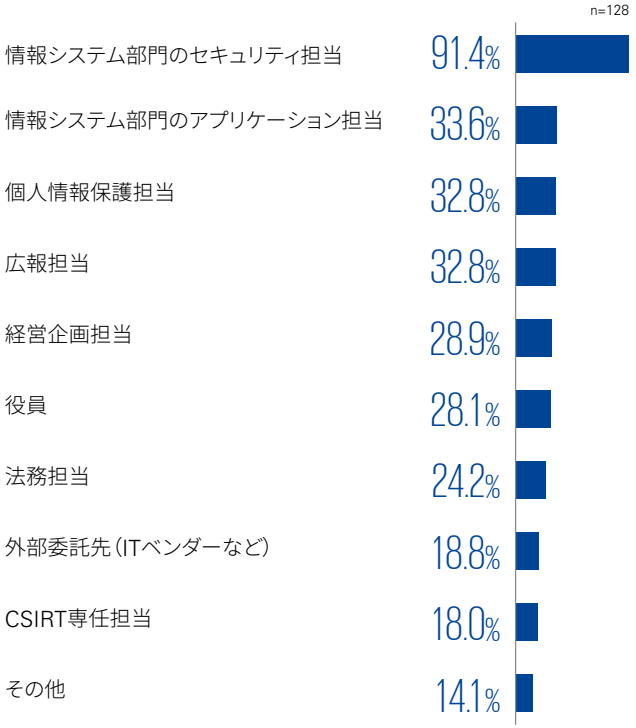
999人以下 n=250	50.8%
1000人～2999人以下 n=91	40.7%
3000人以上 n=113	18.6%

売上高別

1000億円未満 n=274	50.4%
3000億円未満 n=87	37.9%
5000億円未満 n=23	13.0%
5000億円以上 n=55	12.7%

CSIRTの構成員

n=128

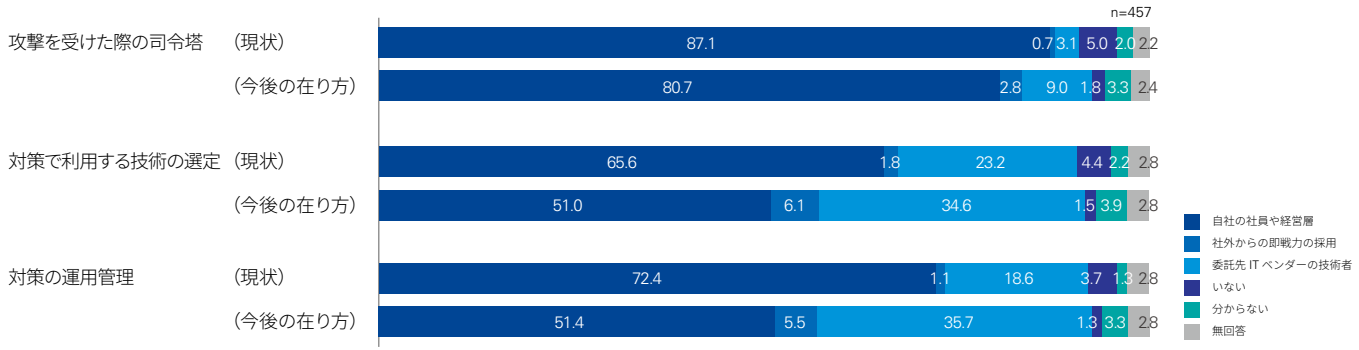


技術選定と運用管理の外部委託を3割の企業が指向

セキュリティ対策の「技術選定」と「運用管理」の担当者については、現状でも2割前後の企業がITベンダーに委託しています。さらに、今後の在り方としてITベンダーへの委託を指向する企業は全体の3分の1強に上ります。

今後の在り方として、社外からの即戦力の採用を指向する企業もありますが、比率は5〜6%とごく一部に限られています。

セキュリティ対策の主な役割の担当者（現状と今後）

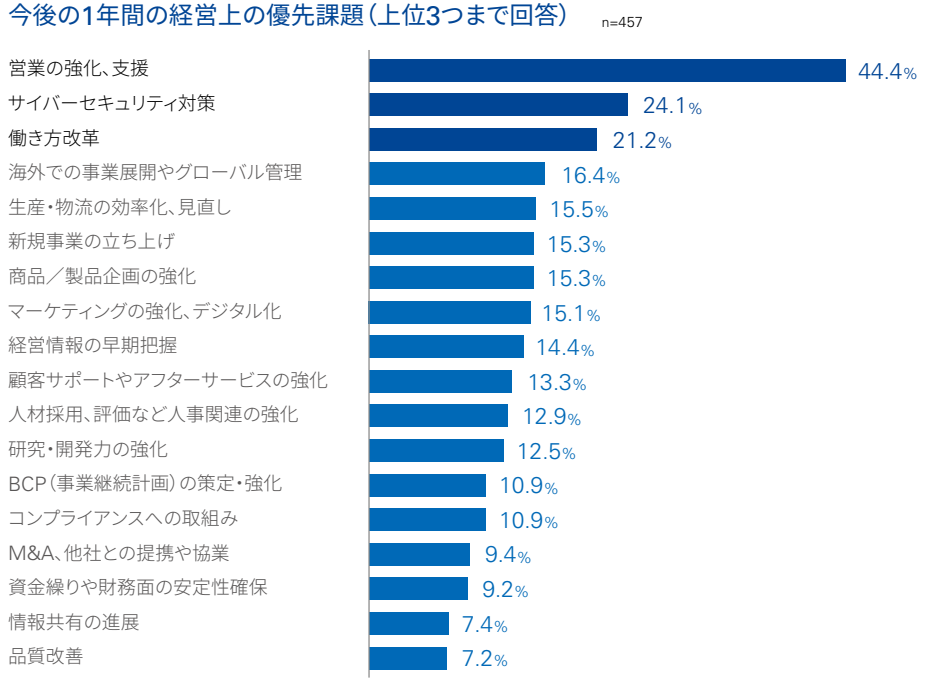


セキュリティは「働き方改革」を上回る第2位の優先課題

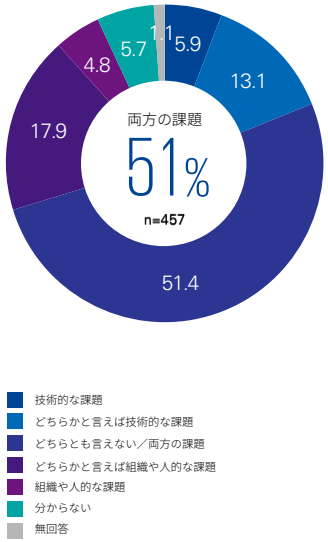
回答者が情報セキュリティ責任者であるためバイアスを考慮する必要がありますが、今後1年間の経営上の課題として「サイバーセキュリティ対策」は「働き方改革」を上回る第2位の優先度に位置付けられています。

セキュリティ対策を「技術面」と「組織・人的な面」のどちらの課題に位置付けるかについては、「両方の課題」とする企業がほぼ半数を占めます。

今後の1年間の経営上の優先課題（上位3つまで回答）



セキュリティ対策は技術課題か組織・人的課題か



課題

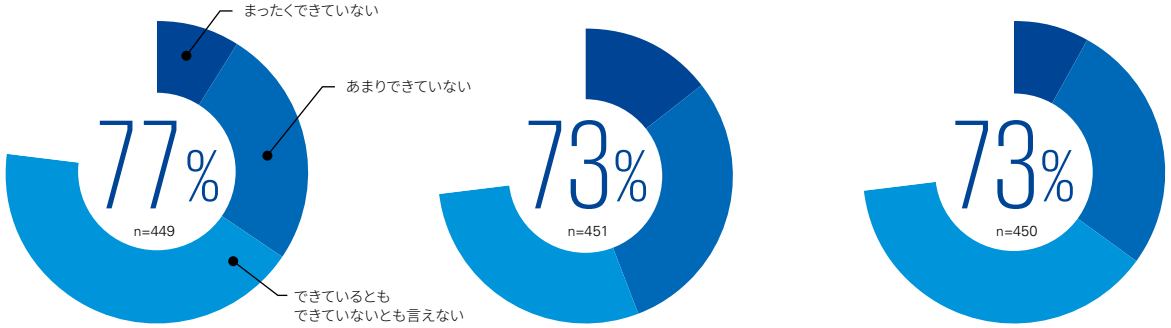
情報セキュリティはITによる対策の域を超えていない

※「%」数値は「まったくできていない」「あまりできていない」「できているともできていないとも言えない」の回答の和

CSR（企業の社会的責任）

8割の企業では外部への説明責任や攻撃による社会への影響を考慮できていません

約8割の企業は、取締役の善管注意義務違反や株主代表訴訟などを考慮したセキュリティ対策が実施できていません。情報漏洩事件などが発生した際には、経営陣が法的な責任を問われる恐れがあります。また、自社が攻撃を受けることによって直接・間接に顧客や社会に与える影響を考慮し、セキュリティ対策を行っていかなければいけません。



善管注意義務違反など法的リスクを考慮した対策

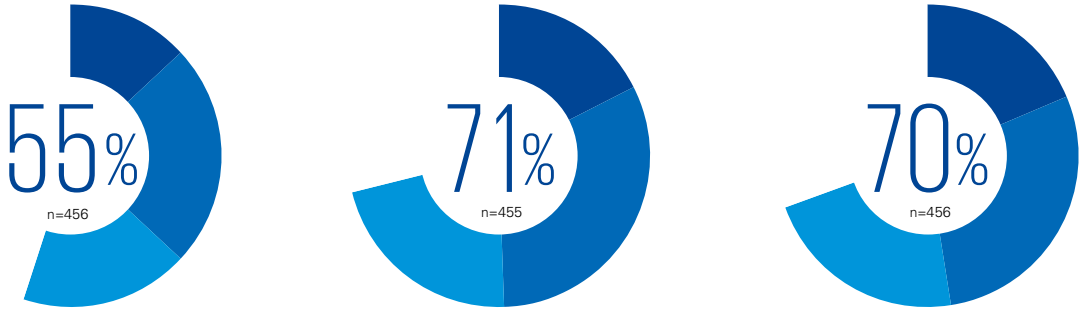
対策・リスクの四半期ごとの報告

顧客利便性や社員生産性を損ねないための事業部門との調整

BCP（事業継続計画）

7割の企業は攻撃による数日間のネット遮断に事業が耐えられません

サイバー攻撃を受けると、被害の拡大をくい止めるためにインターネット接続を遮断しなければならない場合があります。約5割の企業は、遮断時の判断基準や意思決定の手順を策定していません。約7割の企業では遮断が数日間に及んだ際の事業への影響や損害規模を把握できていません。事業を維持する手段も確保されていません。



遮断時の判断基準や意思決定の手順策定

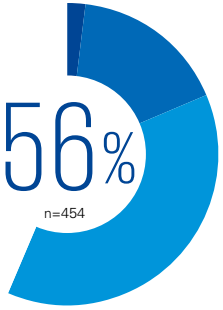
数日間のネット遮断時の事業上の影響範囲や損害規模の把握

数日間のネット遮断時の事業の維持・縮退のための手段の確保

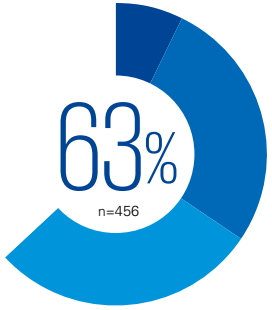
被害の予防・軽減策

3社に2社は定期的な監査と報告に基づく改善活動が行えていません

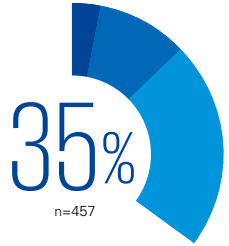
セキュリティ被害の予防・軽減の対策は、半数以上の企業が同業種・同規模の企業と比べ遅れています。進化を続けるセキュリティの脅威に対し、定期的な監査と報告に基づく改善活動を行えていない企業は、6割を超えます。不審メールの開封など危険な行為の報告の奨励は、いまだ3分の1の企業において徹底できていません。



同業種・同規模企業の平均水準以上の対策



定期的な監査と報告に基づく改善

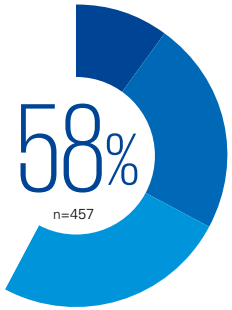


不審メールの開封など危険な行為の報告の奨励

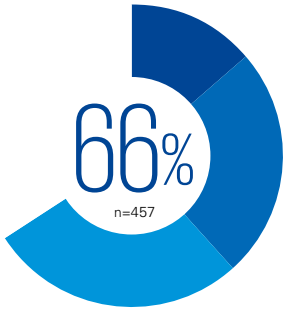
クライシス・コミュニケーション

7割の企業は被害発生時に適切な情報発信・提供ができません

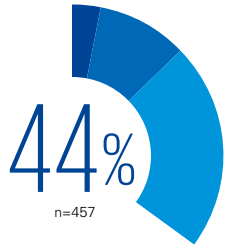
セキュリティインシデントが発生した際には、被害の拡大防止や早期復旧のために、関係者に迅速に情報を伝える必要があります。半数強の企業は、委託先ITベンダーとの連携手順を整えてあるものの、6〜7割の企業は顧客・取引先・メディアへの連絡手順が未整備です。セキュリティ侵害が発生した際に問い合わせや苦情が殺到する恐れがあります。



顧客・取引先への連絡手順



メディアへの連絡や広報の手順



委託先ITベンダーとの連携手順

セキュリティ対策は、単なるITのリスク対策に留まるものではなく、事業継続や法的責任など、企業経営の全般にわたって行われるべきものです。

インシデントが発生した際には、たとえCSIRTが整備してあったとしても、技術面の対応に終始してしまい、自社やステークホルダーに与える影響を俯瞰した適切な行動を行えず、経営を揺るがす問題に発展するのをくい止められないかもしれません。

被害の影響を考慮し、企業として適切な行動を取るためには、サイバーセキュリティをITや情報システム部門だけによる課題とせず、経営全体が取り組むべき課題とし、経営者が自らリーダーシップを取っていくことが必要です。

それはまさに「サイバーセキュリティ経営ガイドライン」の重要なメッセージでもあります。

サイバーセキュリティ対策の実施状況

CSR（企業の社会的責任）

「ある程度できている」「十分できている」
「どちらとも言えない」「あまりできていない」「まったくできていない」

01 善管注意義務違反、株主代表訴訟などの法的リスクを考慮した対策
n=449
22.9% / 77.1%

02 対策の現状とリスクの頻繁な（3ヵ月に1回以上の）経営層への報告
n=451
26.8% / 73.2%

03 顧客の利便性や社員の生産性を損ねないための事業部門との調整
n=450
26.9% / 73.1%

サイバー攻撃発生時のBCP（事業継続計画）

04 ネット接続を遮断する際の判断基準や意思決定の手順の策定
n=456
45.0% / 55.0%

05 ネット接続を数日間遮断した場合の事業上の影響範囲や損害規模の把握
n=455
28.8% / 71.2%

06 ネット接続を数日間遮断した場合の、事業の継続・縮退のための手段の確保
n=456
30.5% / 69.5%

被害の予防策／軽減策

07 同業種・同規模の企業の平均以上の水準の対策
n=454
43.6% / 56.4%

08 対策状況についての定期的な監査と報告を受けての改善
n=456
36.8% / 63.2%

09 社内システムに侵入されても情報の漏えいや破壊を免れる対策
n=453
50.3% / 49.7%

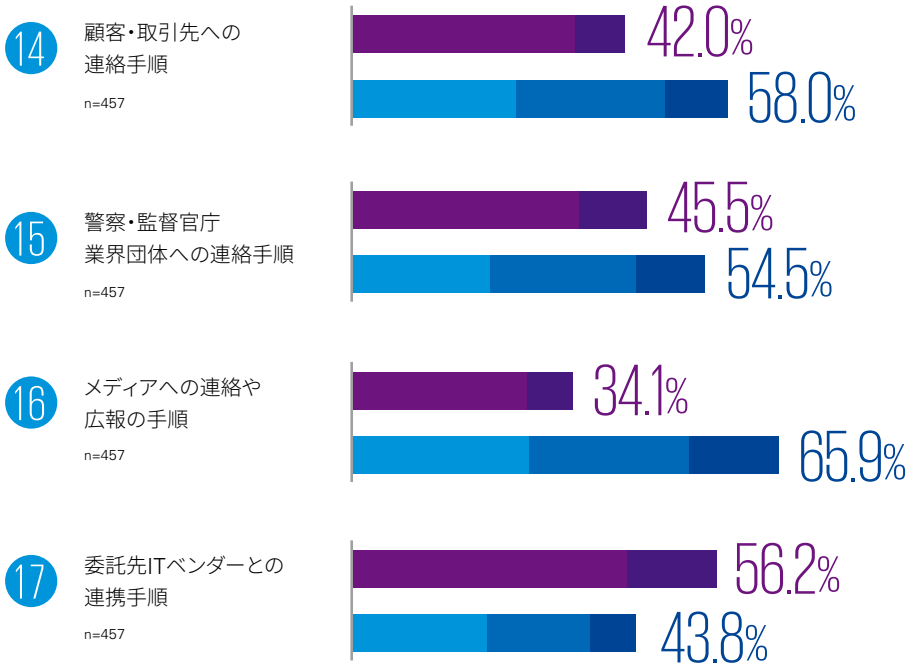
10 標的型攻撃メールの開封など危険行為を隠さず報告することの奨励
n=457
64.8% / 35.2%

11 情報資産をすべて洗い出し、その重要度に応じた保護対策
n=457
38.1% / 61.9%

12 インターネットにつながっていないシステム（工場、POSなど）への対策
n=449
30.1% / 69.9%

13 系列企業や取引先企業の対策状況の把握と改善要望の提示
n=449
26.5% / 73.5%

クライシス・コミュニケーション



サイバーセキュリティ対策の実施状況に関して17の設問を設け確認しました。

全17設問のうち、「危険行為の報告の奨励」「委託先ITベンダーとの連携」「侵入されても情報の漏えいや破壊を免れる対策」の3つを除くと、「できていない」(「どちらとも言えない」を含む)という回答が過半を占めています。

情報セキュリティ対策を実施する上での責任者となる担当幹部(CISO等)に経営者が指示すべき「重要10項目」

サイバーセキュリティリスクへの対応について、組織の内外に示すための方針(セキュリティポリシー)を策定すること。

方針に基づく対応策を実装できるよう、経営者とセキュリティ担当、両者をつなぐ仲介者としてのCISO等からなる適切な管理体制を構築すること。その中で、責任を明確化すること。

経営戦略を踏まえて守るべき資産を特定し、セキュリティリスクを洗い出すとともに、そのリスクへの対処に向けた計画を策定すること。

計画が確実に実施され、改善が図られるよう、PDCAを実施すること。また、対策状況については、CISO等が定期的に経営者に対して報告をするとともに、ステークホルダーからの信頼性を高めるべく適切に開示すること。

系列企業やサプライチェーンのビジネスパートナーを含め、自社同様にPDCAの運用を含むサイバーセキュリティ対策を行わせること。

PDCAの運用を含むサイバーセキュリティ対策の着実な実施に備え、必要な予算の確保や人材育成など資源の確保について検討すること。

ITシステムの運用について、自社の技術力や効率性などの観点から自組織で対応する部分と他組織に委託する部分の適切な切り分けをすること。また、他組織に委託する場合においても、委託先への攻撃を想定したサイバーセキュリティの確保を確認すること。

攻撃側のレベルは常に向上することから、情報共有活動に参加し、最新の状況を自社の対策に反映すること。また、可能な限り、自社への攻撃情報を公的な情報共有活動に提供するなどにより、同様の被害が社会全体に広がることの未然防止に貢献すること。

サイバー攻撃を受けた場合、迅速な初動対応により被害拡大を防ぐため、CSIRT(サイバー攻撃による情報漏えいや障害など、コンピュータセキュリティにかかるインシデントに対処するための組織)の整備や、初動対応マニュアルの策定など緊急時の対応体制を整備すること。また、定期的かつ実践的な演習を実施すること。

サイバー攻撃を受けた場合に備え、被害発覚後の通知先や開示が必要な情報項目の整理をするとともに、組織の内外に対し、経営者がスムーズに必要な説明ができるよう準備しておくこと。

出所:「サイバーセキュリティ経営ガイドライン」経済産業省・情報処理推進機構

戦略
サイバーセキュリティ経営を実践するために

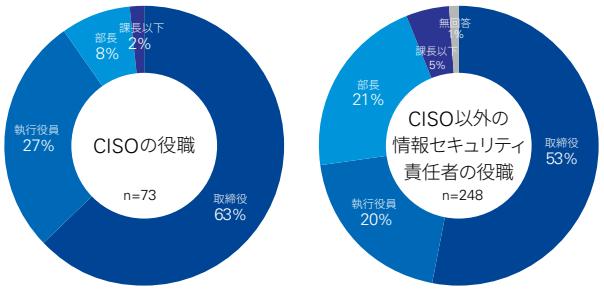
企業がサイバーセキュリティリスクを適切に管理できるようにするためには、経営層がセキュリティ対策の現状等を的確に理解できていなければなりません。そのためには、経営層にCISO（最高情報セキュリティ責任者）を置き、トップダウンでセキュリティの推進を主導し、情報セキュリティ部門との間で、正確・適時に情報を交換・共有できる管理体制を整えることが重要です。

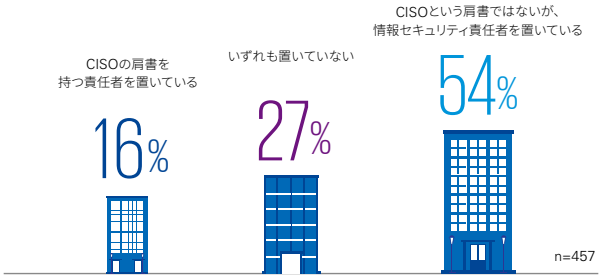
CISO／情報セキュリティ責任者により経営層と情報セキュリティ部門を連携させる

経営層がサイバーセキュリティをリードするために重要な役割を果たすのがCISO（最高情報セキュリティ責任者）です。

CISOを含む情報セキュリティ責任者を設けている企業は7割に達しています。その55%は取締役であり、業務執行の意思決定体である取締役会の場で情報セキュリティを経営課題として直接議論できる立場にあります。全体では39%の企業で取締役が情報セキュリティの責任者を務めています。

一方で、全体で3割の企業は、セキュリティ責任者を置いていないか回答がありませんでした。



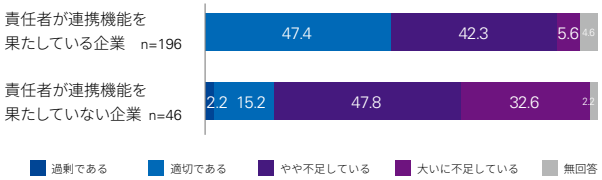


責任者が経営層と情報セキュリティ部門とを密接に連携させる機能を果たしている企業では、経営層が対策の現状を理解できており、両者には明らかな相関関係が見られました。

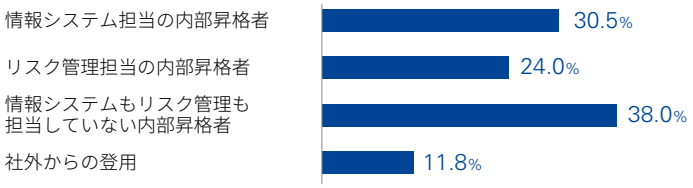
また、情報セキュリティ責任者が機能している企業は、ほぼ半数がセキュリティ対策の投資額が適切と答えています。責任者が経営層と現場を連携させる機能を果たすことは投資額の適正化に寄与すると考えられます。

経営層が対策の現状を理解できている企業の割合

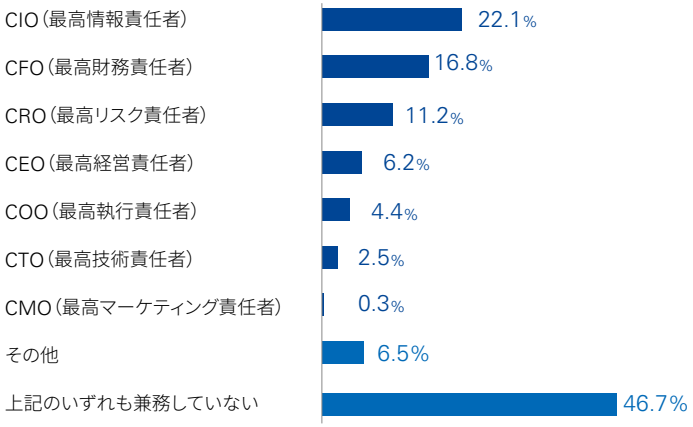
セキュリティ対策投資額の適正さ



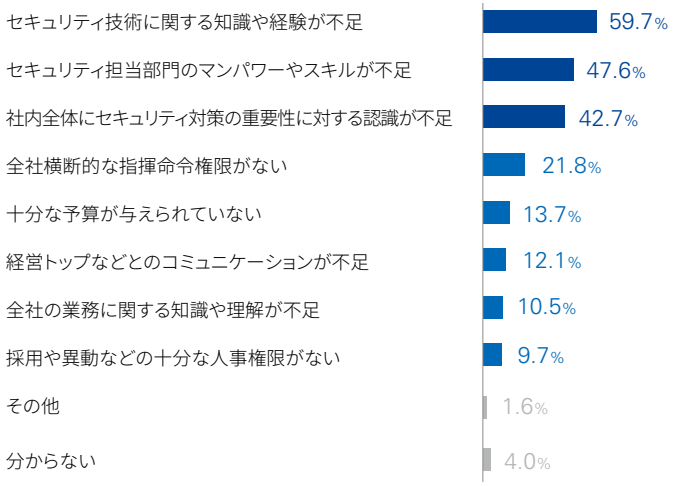
CISO／責任者の経歴 n=321



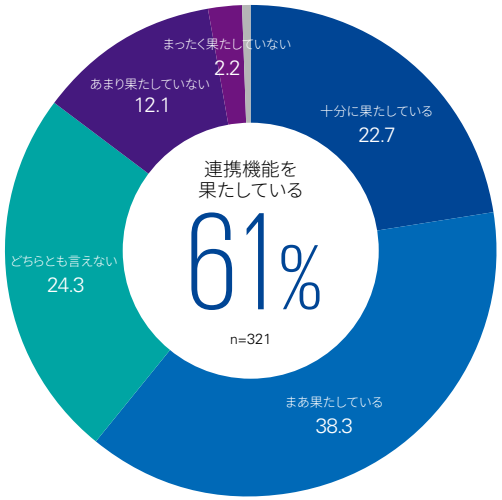
CISO／責任者のCxO兼務状況 n=321



CISO／責任者が連携機能を果たせない理由 n=124



責任者は連携機能を果たしているか



CISO／情報セキュリティ責任者を設置している企業の6割は、責任者が連携機能を果たしていると回答しました。一方、連携機能を果たせていない企業に理由を尋ねると、責任者の知識や経験の不足を挙げた回答が6割と最多でした。

責任者の4割は、情報システムやリスク管理の担当経験がありません。

CISO／情報セキュリティ責任者のほぼ半数は、CxOを兼務しています。最も多いのはCIOとの兼務で22%でした。

知識や経験の不足は一朝一夕で解決するものではありません。教育・訓練などの長期的視野の施策とともに、外部の専門家の活用等の短期的な施策も検討すべきでしょう。

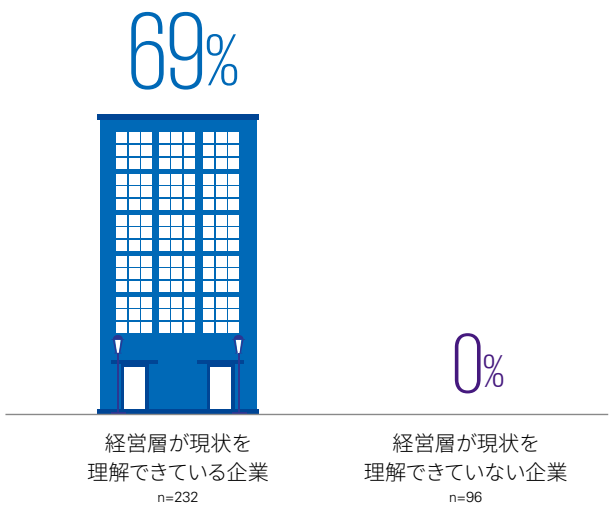
また、CIOがCISOを兼務する組織は、両者の分離が必要になるかもしれません。AI・IoT等の新たなテクノロジーによる変革の波が押し寄せる中、新たなサービスや製品を生み出し、顧客を獲得することに創造力を発揮する「攻めの活動」と、経営者の最大の関心事となりつつあるサイバーリスクを軽減する「守りの活動」の双方の比重が高まるためです。両者ともに企業活動における重要性が高まるなか、組織を守る牽制機能を充実させる必要性はさらに高まっていくでしょう。

セキュリティ対策の「あるべき姿」を描く

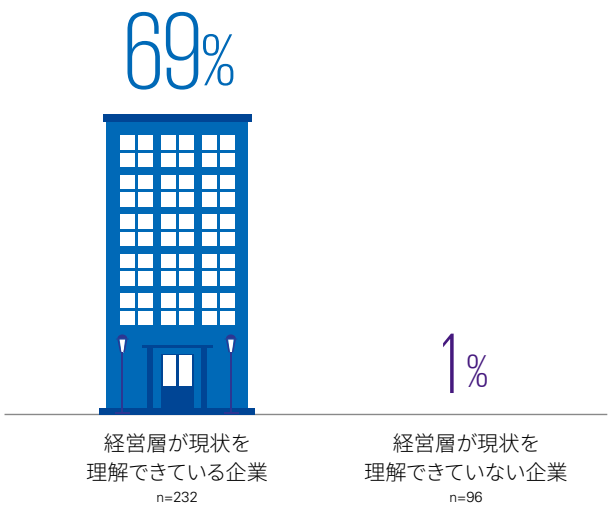
経営層が現状を理解している企業の7割は、セキュリティ対策の「あるべき姿」を経営層が持ち、同じく7割の企業はセキュリティ担当部門との間で「あるべき姿」について共通の認識を持つことができています。逆に、経営層が現状を理解できていない企業は、経営層が「あるべき姿」を持つことも、それをセキュリティ部門と共有することも、まったくできていません。

対策の現状を理解し、強化すべき改善事項などの「あるべき姿」を描くことができたら、その実現に向けて経営資源の適時・適切な配分を決定することが、経営層の役割です。予算・人材の配分を経営層が自ら判断・決定し、適切に管理していくことが重要です。

経営層が対策の「あるべき姿」を持っている企業の割合



経営層と担当部門が「あるべき姿」を共有できている企業の割合

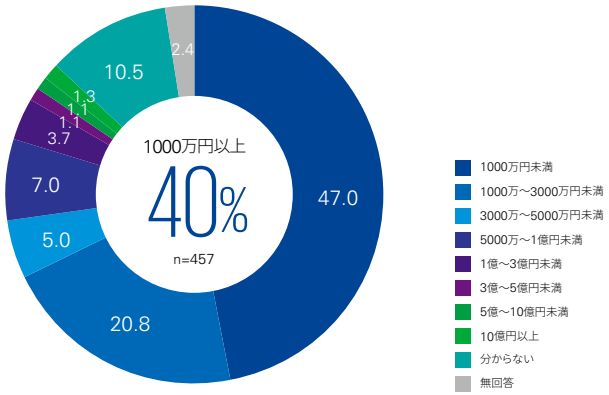


経営資源を適切に配分する　(1) 予算

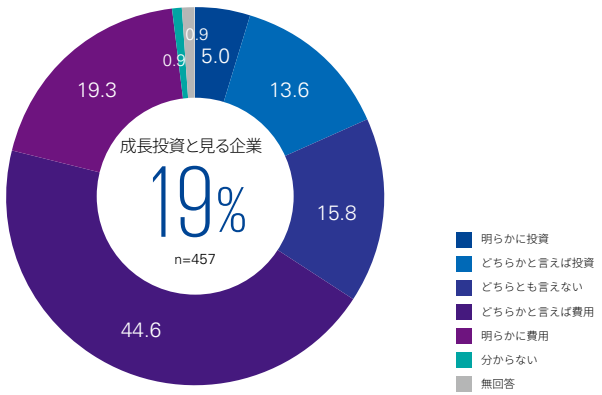
セキュリティ対策の支出を、「成長のための投資」と見るのか、「やむを得ない費用」と見るのか――。成長投資と見る企業は、全体の18.6%、2割弱に留まっています。圧倒的な多数派は、「やむを得ない費用」と見る企業です。ほぼ3社に2社は「やむを得ない費用」に位置付けています。

しかし、セキュリティ対策の支出を「投資」と見る企業と、「費用」と見る企業では、予算の充足状況や増減計画に明確な違いがあります。「投資」と見る企業では、7割超が必要な予算を確保できており、4割弱が投資額を増やす計画です。一方、「費用」と見る企業では、それぞれ4割強、3割弱に留まります。

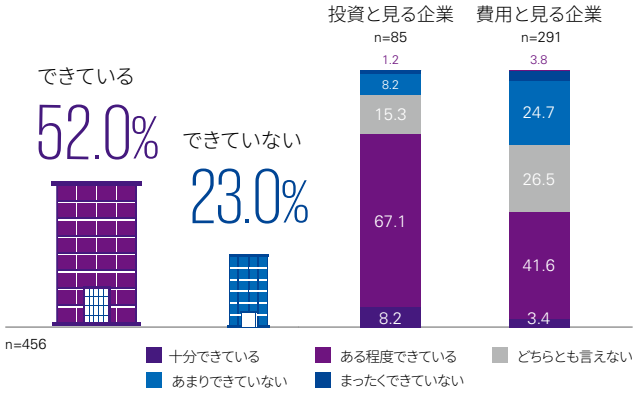
年間投資額



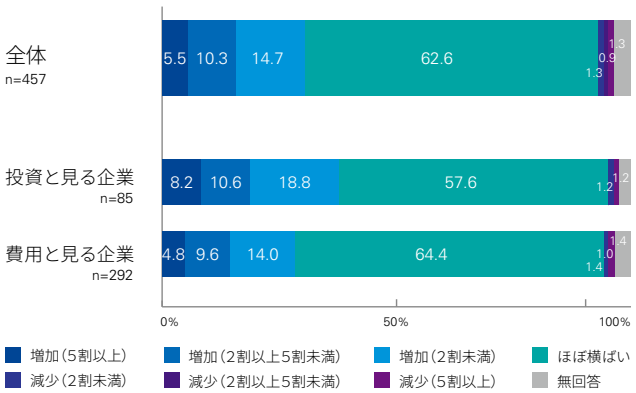
投資か費用か



必要なセキュリティ予算の確保



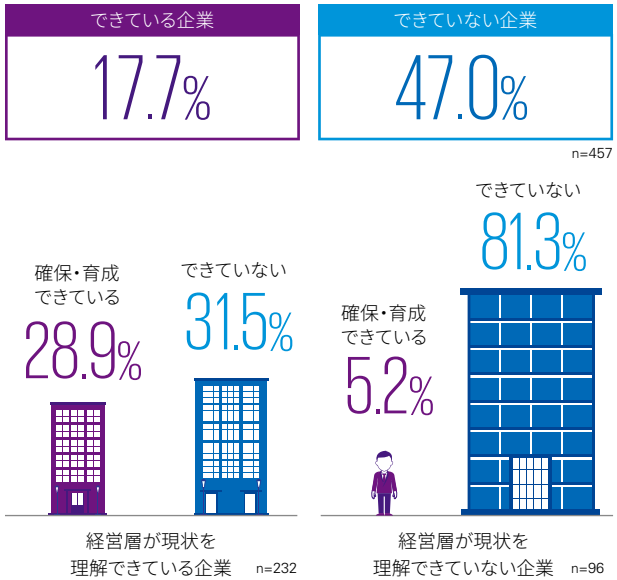
2017年度のセキュリティ投資額の増減



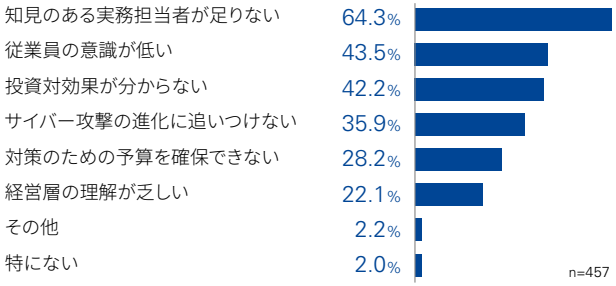
経営資源を適切に配分する　(2) 人材

セキュリティ対策に取り組む上での最大の課題として最も多く挙げられたのは、知見のある実務担当者が足りないという、人材の確保・育成に関する事項でした。ただし、欠乏感は企業によって大きな差があります。経営層が対策の現状を理解している企業では、3割弱が確保できているのに対し、経営層が現状を理解できていない企業では、確保できていない企業が8割に上ります。

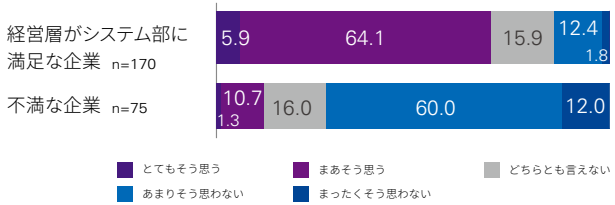
必要な人材の確保・育成の状況



対策に取り組む上での課題



システム部門は対策に対する経営層の理解に満足しているか



経営層がシステム部門の取組みや技術力に満足していない企業では、7割超がシステム部門も経営層の対策への理解に満足していません（グラフ「システム部門は対策に対する経営層の理解に満足しているか」を参照）。一方に不満があると、他方も不満を抱いています。

経営層が現状を理解した上で対策のあるべき姿を持ち、システム部門と密接に意見や情報を交換できる関係を築くことが重要です。

お問い合わせ先

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