KPMG
cutting through complexity

サイバーセキュリティ サーベイ2013

KPMGジャパン

ご挨拶

サイバー攻撃による被害が、連日のようにメディアで取り上げられています。攻撃手法は高度化の一途をたどり、高い技術力を有する第三者が、明確な目的を持って特定企業をターゲットに仕掛けるサイバー攻撃の脅威が急速に増大しています。

これに対し、多くの企業では攻撃を受けてから初めて対策が取られているのが現状です。事後対応よりも予防措置の方がより費用対効果が高いにもかかわらず、サイバー攻撃の予兆の検出やその防御に必要な能力を備えている企業はほとんどありません。急速に変わりゆく外部環境にあわせて、企業はこれまでの情報セキュリティ、機密管理の取組みを、サイバーセキュリティ防御態勢へと変革し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グループでは、サイバーセキュリティに関する問題解決の支援とともに、有益な情報を広く社会に提供することも重要な役割として認識しております。今回実施した本サーベイの結果が、少しでもサイバーセキュリティ対策に取り組む皆様のお役に立てれば幸いです。

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、ご回答いただいた多くの皆様に心から感謝を申し上げます。

2014年1月
KPMGサイバーセキュリティアドバイザリーグループ

目 次

はじめに

1）サーベイ実施の背景および目的

昨今、グローバルな活動を展開する企業や政府において、サイバーセキュリティへの関心が高まっています。狙いを定めた企業に対して、高度なIT技術を駆使し集中的に仕掛けられるサイバー攻撃は、従来の不特定多数の企業を対象にした腕試しや愉快犯的なハッキングとは一線を画すものです。サイバー攻撃は、営業秘密や個人情報の搾取、漏えい、基幹システムの停止、社会インフラや工場の制御系システムの破壊など、企業の事業継続上、深刻なダメージを引き起こすリスクであるため、その対応については社会的に喫緊の課題となっています。

このような状況を受けて、KPMGジャパンでは、企業のサイバーセキュリティへの対応状況に関する調査を実施しました。

本報告書では、今回の調査結果のとりまとめに加え、海外の調査結果[1]との比較を行い、国内外におけるサイバーセキュリティに対する意識や対策実施状況の差異を分析しました。

本報告書は、サイバーセキュリティに関わる動向ならびに課題を明らかにし、各企業において、より効果的かつ効率的にサイバーセキュリティ対策に取り組むための情報を提供することを目的としています。

2）サーベイの方法

本サーベイでは、2013年10月に、国内の上場企業と売上高500億円以上の未上場企業の情報システム部門責任者を中心に、郵送、メールなどの手段を用いて質問票を6,509通発信しました。

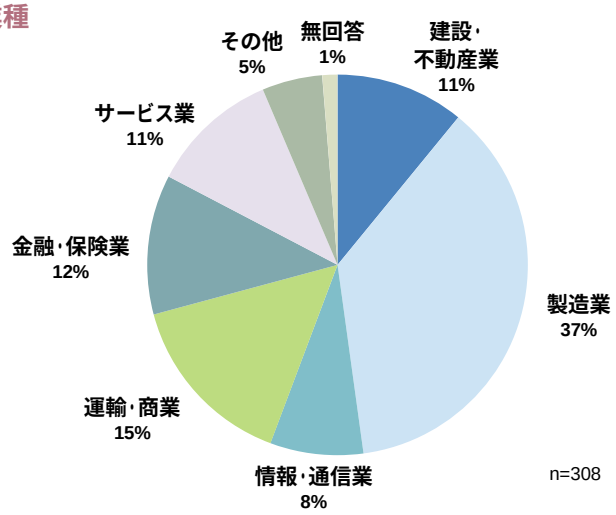
本報告書は、2013年11月中旬までにご回答いただいた308社（回答率4.7%）について、集計および分析を行った結果を記載しています。

1. 海外の調査結果は、KPMG Advisory N.V.が実施した「KPMG Cybercrime Survey 2011」を参照しました。

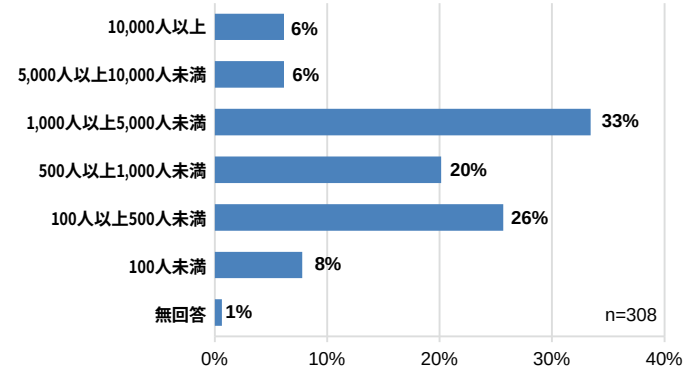
3) 回答企業の概要

回答企業の概要は下図のとおりです。

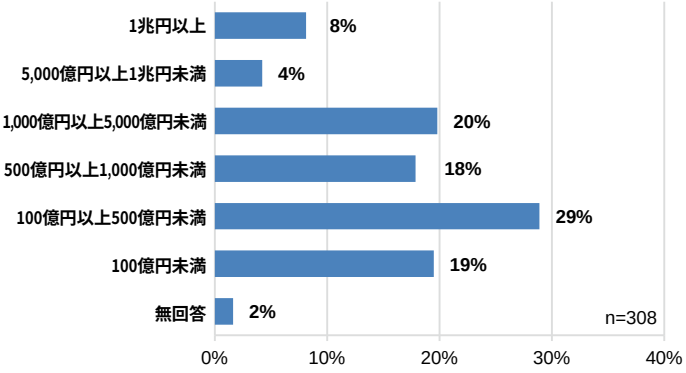
業種



従業員数



年間売上高



4) 用語定義

本報告書で使用している用語について、その定義を説明します。

用語	定義
サイバー攻撃	コンピュータシステムやインターネットなどを利用して、標的のコンピュータやネットワークに不正に侵入してデータの詐取や改ざん・破壊などを行なったり、標的のシステムを機能不全に陥らせること
クラッキング	悪意をもって他人のコンピュータのデータやプログラムを盗み見たり、改ざん・破壊などを行うこと
ERPシステム	企業全体を経営資源の有効活用の観点から統合的に管理し、経営の効率化を図るための手法・概念、およびこれを実現するITシステムやソフトウェアのこと
フォレンジック	不正アクセスや機密情報漏洩など、コンピュータに関する犯罪や法的紛争が生じた際に、原因究明や捜査に必要な機器やデータ、電子的記録を収集・分析し、その法的な証拠性を明らかにする手段や技術の総称
ソーシャル・エンジニアリング	人間の心理的な隙や、行動のミスにつけ込んで個人が持つ秘密情報を入手する方法
フィッシング	金融機関（銀行やクレジットカード会社）などを装った電子メールを送り、住所、氏名、銀行口座番号、クレジットカード番号などの個人情報を詐取する行為。電子メールのリンクから偽サイト（フィッシングサイト）に誘導し、そこで個人情報を入力させる手口が一般的に使われる
マルウェア	ウイルス、ワーム、トロイの木馬を含む悪質なコードの総称

1 エグゼクティブサマリー

情報セキュリティを取り巻く環境は常に進化しています。自らは標的にならないと考えている企業は、その考えを改めなければなりません。標的となり、攻撃される可能性が十分にあることを認識したうえで、サイバーセキュリティへの取組みを、有効に機能し続けるサイバー攻撃防御態勢へと変革させる必要があります。

対岸の火事ではない

本サーベイ回答企業のうち、情報・通信業の35%、製造業の29%、全体では24%が、過去1年間にサイバー攻撃の試みを受けており（2.1参照）、そのうちの46%で実際の被害が生じています（2.3参照）。被害内容として最も多く挙げられたのは、「業務プロセスの中断（53%）」であり（2.4参照）、事業活動の阻害を狙った攻撃が現実のものとなっています。海外では、「財務的な損失（41%）」や「情報の漏えい（個人情報24%、顧客の機密情報22%）」も主要な被害として報告されています（2.4参照）。

また、自社にサイバー攻撃を発見する能力があると考えている企業は31%にすぎません（3.7参照）。このことは、本サーベイで明らかにされたサイバー攻撃は氷山の一角にすぎず、「過去1年間にサイバー攻撃の試みを受けたことがない」と回答した75%の企業[2]も、検知されていないサイバー攻撃を受けていた可能性があることを示唆しています。

回答企業の88%が「サイバー攻撃は一時的なものとは思わない」と考えており（5.1参照）、サイバー攻撃は一過性の問題ではなく、今後も大きな課題であり続けるという認識が広まっています。

一方で、過去1年間にサイバー攻撃を受けた企業の22%は、「自社はサイバー攻撃のターゲットとして魅力的だと思わない」と考えており（3.3参照）、自社の価値に対する企業の認識が、必ずしも攻撃者の認識とは一致していない状況がうかがえます。

システムから人へ

国内では、過去1年間にサイバー攻撃を受けた企業の約半数がマルウェア感染やウェブアプリケーションへの攻撃を経験しています。一方、海外ではソーシャル・エンジニアリングやフィッシングといった、人の錯誤を利用した攻撃も主流になっています（2.2参照）。

国内では、過去1年間にサイバー攻撃の被害が発生した企業の91%が被害金額は1,000万円未満であったと回答しています。一方、海外では、16%の企業が75万ユーロ（約1億500万円[3]）以上の損失を被っています（2.5参照）。

ITや情報セキュリティは、海外のトレンドが数年遅れで日本に到来する事例が多いことから、今後、サイバー攻撃の標的がシステムから人へとシフトしながら、損失金額も増大していくことが懸念されます。

2. 1%の企業は無回答
3. 1ユーロ＝140円で計算

テクノロジーの限界

国内では48%が「サイバー攻撃は防ぐことができない」と考えている一方（3.1参照）、「自社にはサイバー攻撃に効率的に対処する能力がある」と考えている企業は23%にすぎず（3.8参照）、回答企業の96%は「サイバー攻撃への新たな対策が必要」と考えています（5.3参照）。海外では35%が「サイバー攻撃は防ぐことができない」と考えています（3.1参照）。

サイバー攻撃の予防をテクノロジーに依存すべきと考える企業は国内で46%、海外では26%にすぎません（5.5参照）。しかしながら、国内の回答企業の94%はサイバー攻撃予防のための年間予算のほとんどをシステム関連に使用しています（4.6参照）。一連の回答から、サイバー攻撃への対処はシステム対応だけでは不十分と認識しながらも、システム対応に終始してしまう企業のジレンマを感じます。

情報セキュリティ対策は、防御側である企業と攻撃者のいたちごっこの繰り返しであり、100%完全な防御策はありません。粘り強く攻撃されれば、いかなる防御の壁もいずれは打ち破られてしまいます。そこで、組織的対策、物理的対策、技術的対策をバランスよく取り入れながら、サイバー攻撃を早期に検知し、拡大を食い止め、重要な資産を保護し、迅速かつ有効的な事故対応メカニズムを確保することが重要になります。

マネジメントの責務

サイバー攻撃の予防を取締役レベルで議論すべきと考える企業は国内で52%、海外では88%にのぼります（5.6参照）。過去1年間にサイバー攻撃を受けた企業の23%が「非常にそう思う」と回答しており、サイバー攻撃対策を円滑に推進するために、取締役レベルの強い関与が求められている状況がうかがえます。

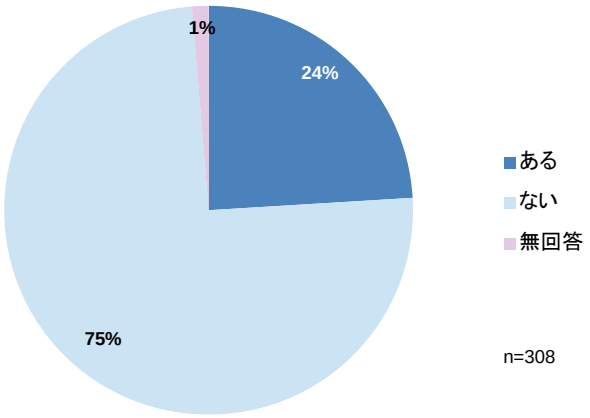
2 サイバー攻撃の発生状況

本章では、過去1年間に発生したサイバー攻撃の有無、攻撃手法や被害状況など、サイバー攻撃の発生状況について報告します。

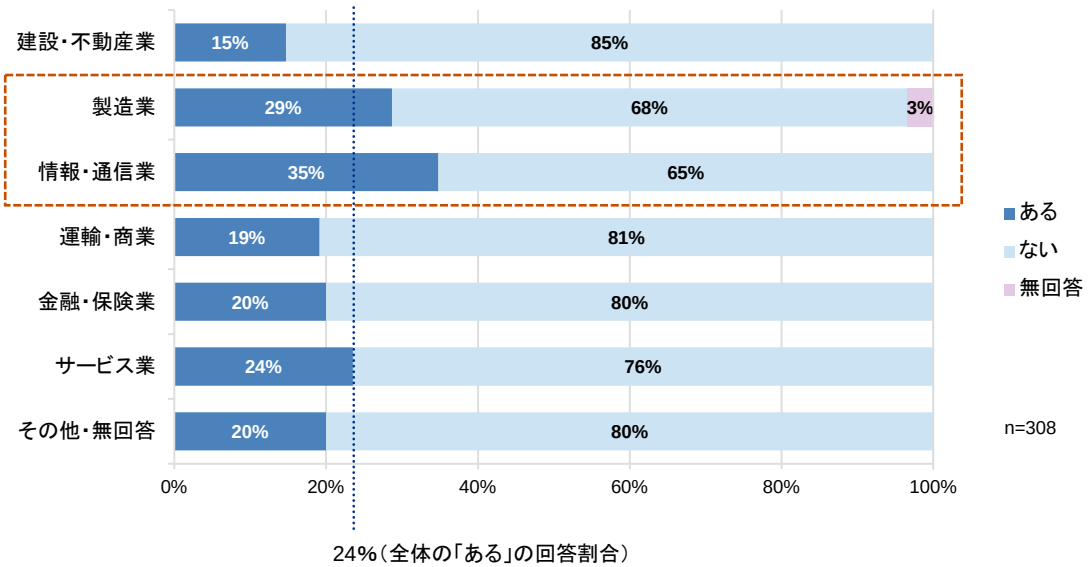
2.1. サイバー攻撃の試みを受けた経験

回答企業の24%が過去1年間にサイバー攻撃の試みを受けています。
業種別では製造業および情報・通信業が標的にされやすく、また、年間売上高が大きい企業ほど標的にされやすい傾向がうかがえます。

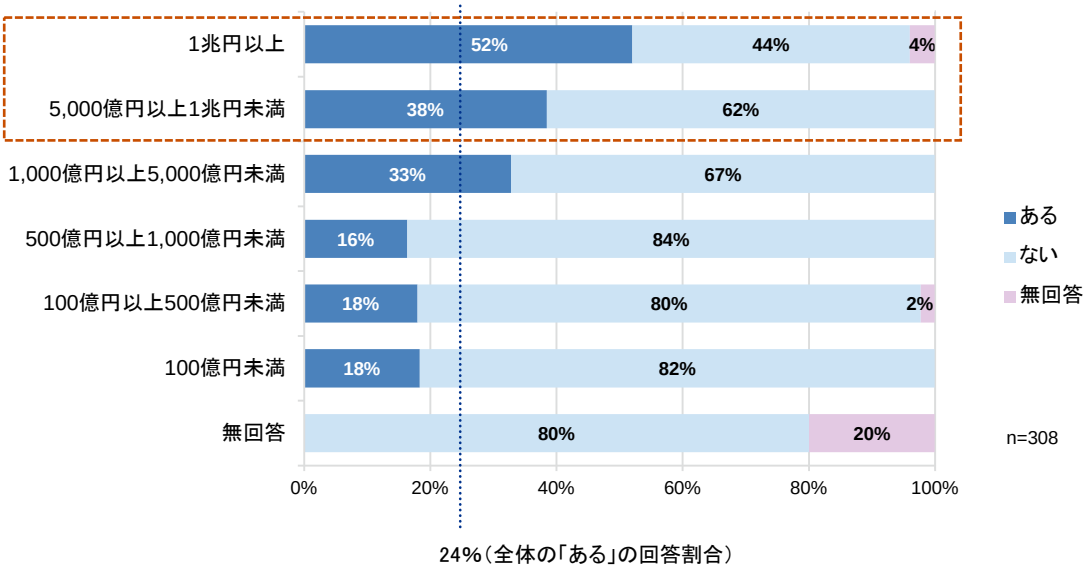
過去1年間にサイバー攻撃の試みを受けたことがあるか



過去1年間にサイバー攻撃の試みを受けたことがあるか（業種別）



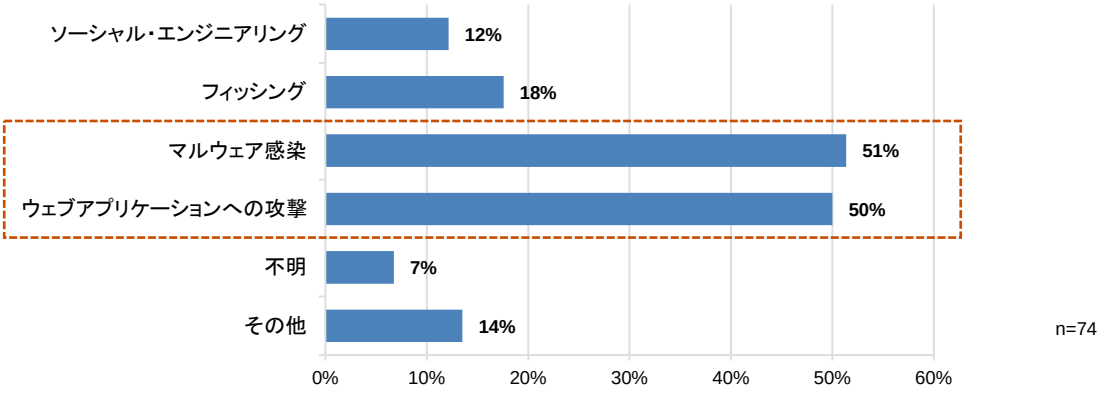
過去1年間にサイバー攻撃の試みを受けたことがあるか（年間売上高別）



2.2. 攻撃手法

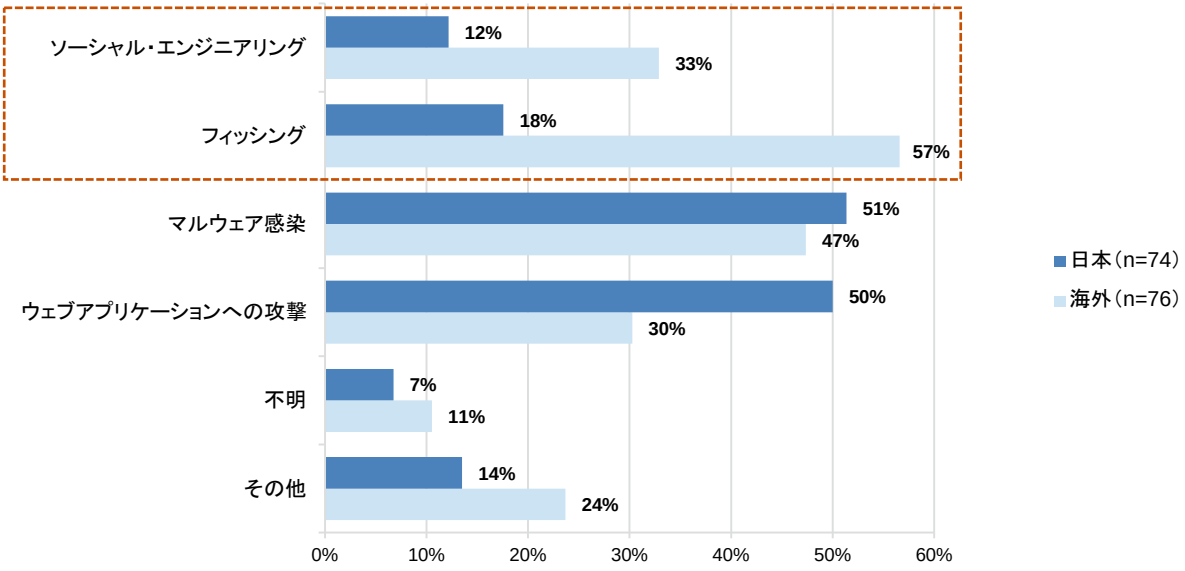
過去1年間にサイバー攻撃の試みを受けた企業の約半数が、マルウェア感染やウェブアプリケーションへの攻撃といった、システムに対する攻撃を経験しています。
一方、海外ではソーシャル・エンジニアリングやフィッシングなどの「人」を対象とした攻撃手段も主流になっています。

攻撃手法はどのようなものであったか（複数回答）



＊2.1の設問で「過去1年間にサイバー攻撃の試みを受けたことがある」と回答した企業が対象です。

攻撃手法の海外との比較（複数回答）

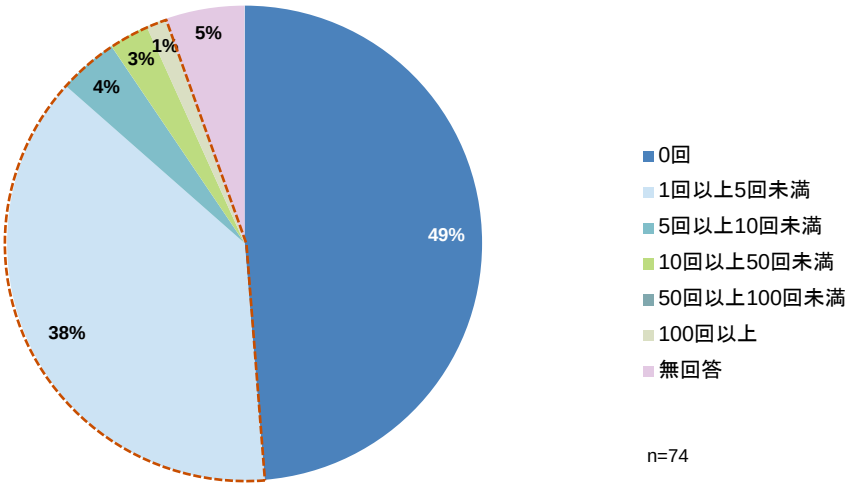


＊2.1の設問で「過去1年間にサイバー攻撃の試みを受けたことがある」と回答した企業が対象です。

2.3. 被害発生回数

サイバー攻撃の試みを受けた企業のうち、実際に被害が発生した企業は46%です。8%の企業は5回以上の被害を受けています。

被害が発生したのは何回くらいか

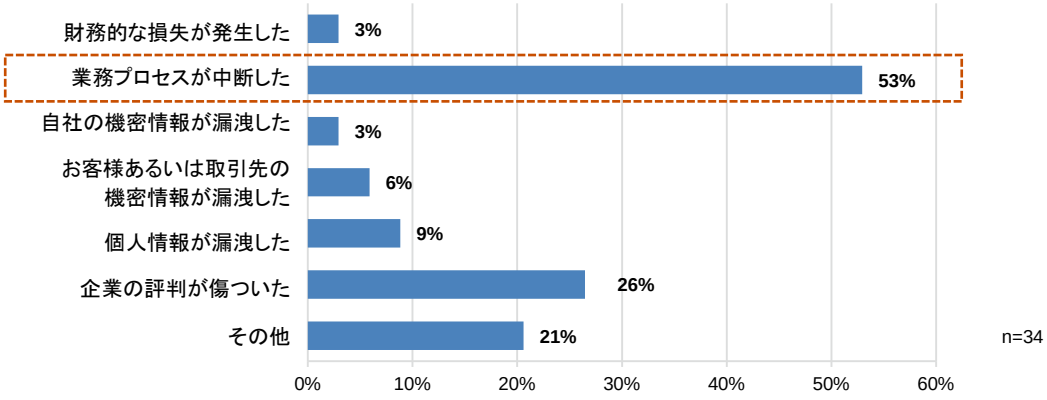


＊2.1の設問で「過去1年間にサイバー攻撃の試みを受けたことがある」と回答した企業が対象です。

2.4. 被害内容

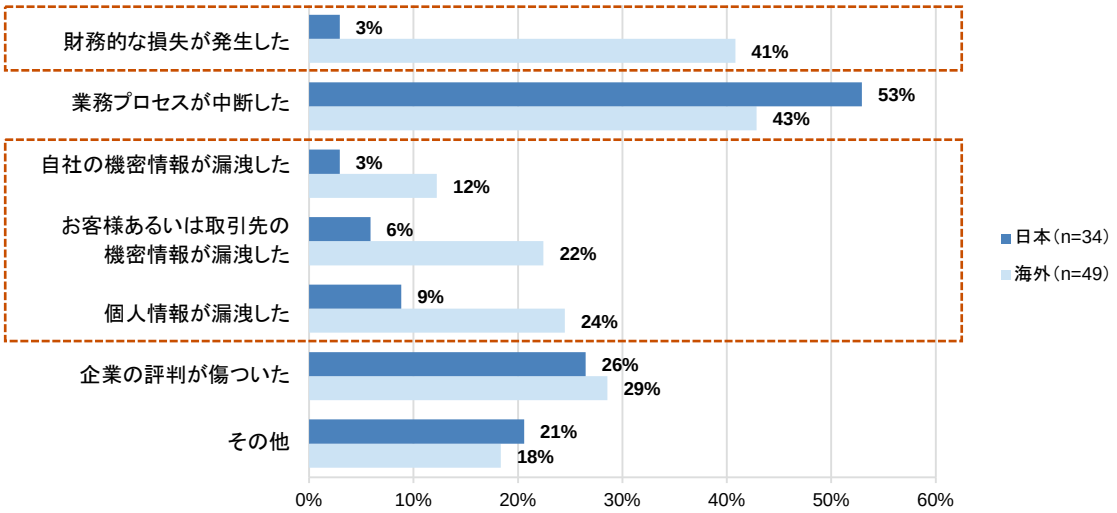
過去1年間にサイバー攻撃の被害を受けた企業の53%が、サイバー攻撃により業務プロセスが中断したと回答しています。海外では、財務的な損失および情報の漏えいを挙げた企業の割合が日本を大きく上回っています。

どのような被害が発生したか（複数回答）



＊2.3の設問でサイバー攻撃の被害が1回以上発生したことがあると回答した企業が対象です。

被害内容の海外との比較（複数回答）

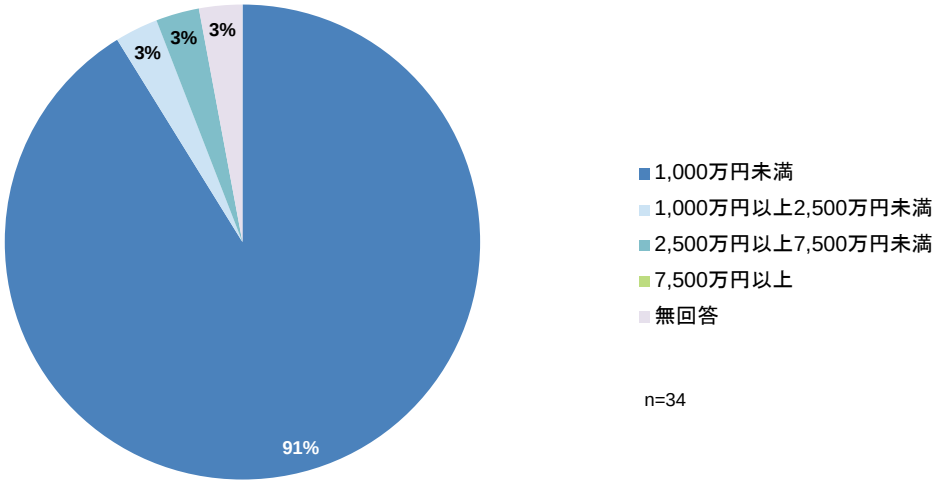


＊2.3の設問でサイバー攻撃の被害が1回以上発生したことがあると回答した企業が対象です。

2.5. 損失金額

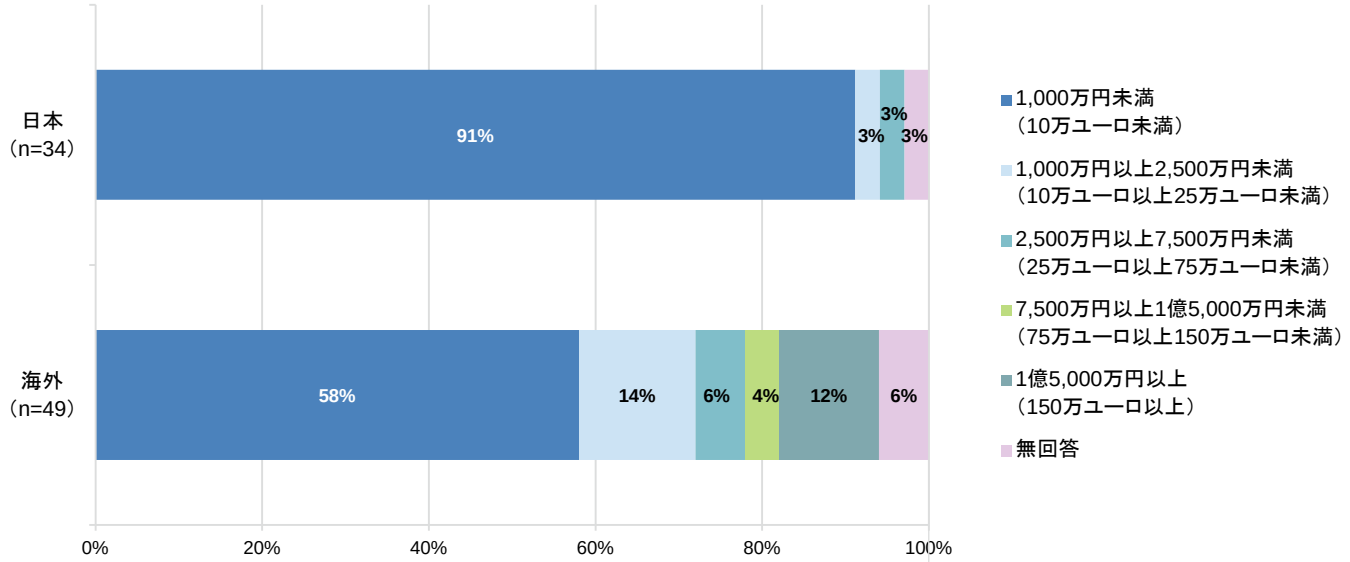
過去1年間にサイバー攻撃の被害を受けた企業の91%が、サイバー攻撃による累計損失金額は1,000万円未満であったと回答しており、7,500万円以上と回答した企業は0%でした。一方、海外では16%の企業が75万ユーロ（約1億500万円[4]）以上の損失が発生したと回答しています。

過去1年間のサイバー攻撃による損失はどのくらいであったか



＊2.3の設問でサイバー攻撃の被害が1回以上発生したことがあると回答した企業が対象です。

損失金額の海外との比較（複数回答）



＊2.3の設問でサイバー攻撃の被害が1回以上発生したことがあると回答した企業が対象です。

4. 1ユーロ＝140円で計算

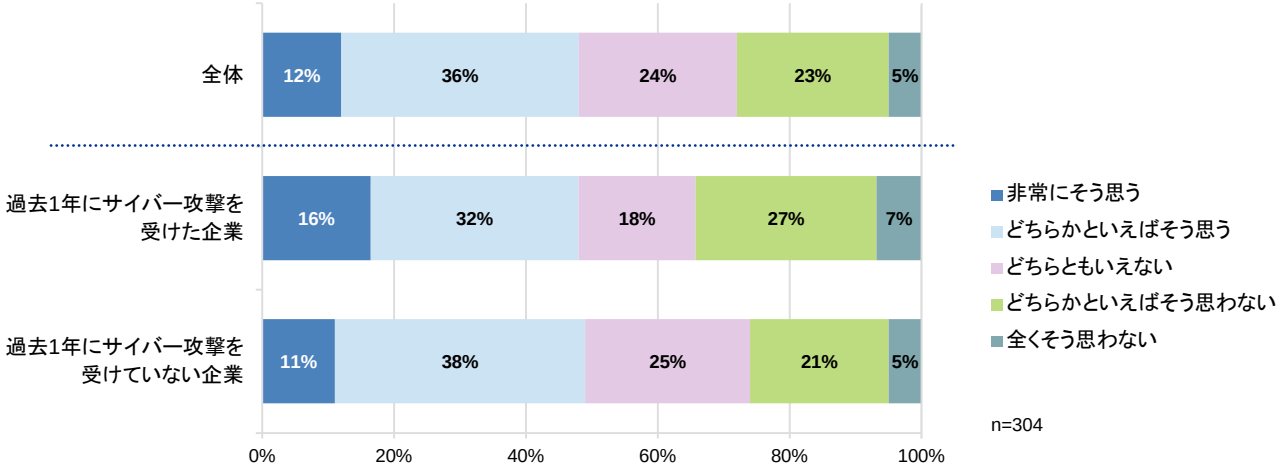
3 サイバー攻撃に対する認識

本章では、サイバー攻撃の防御や動機、サイバー攻撃のターゲットとしての自社の魅力、サイバー攻撃への対応能力など、サイバー攻撃に対する企業の認識について報告します。

3.1. サイバー攻撃の防御

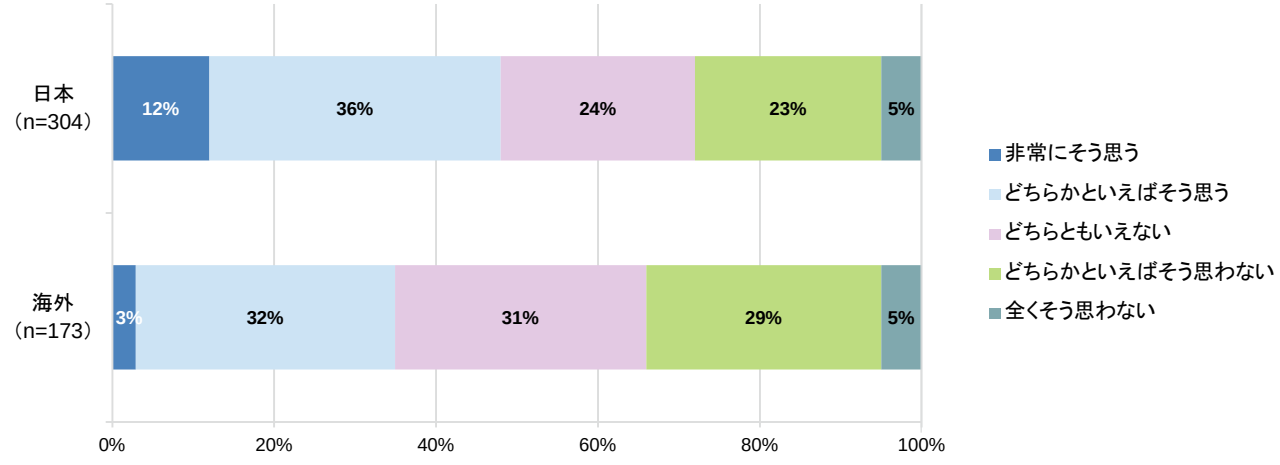
過去1年間にサイバー攻撃を受けた企業の48%、受けていない企業の49%がサイバー攻撃は防ぐことができない(「非常にそう思う」、「どちらかといえばそう思う」、以下同じ)と考えています。海外では35%の企業がサイバー攻撃は防ぐことができないと回答しています。

サイバー攻撃は防ぐことができない



＊本設問に無回答の企業は集計に含めていません。

サイバー攻撃は防ぐことができない(海外との比較)

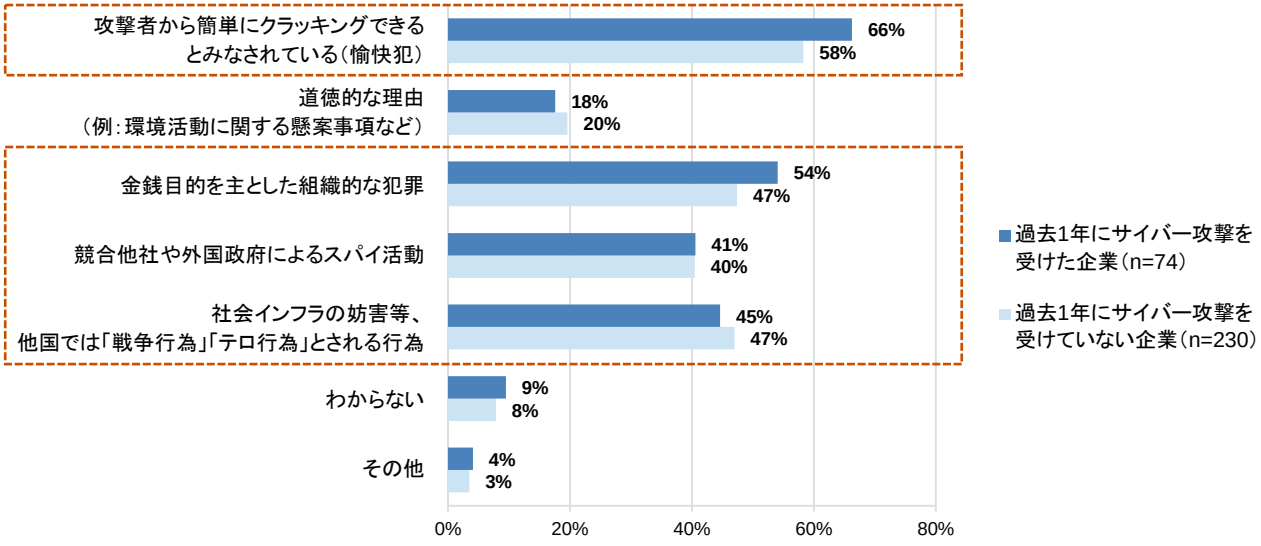


＊本設問に無回答の企業は集計に含めていません。

3.2. サイバー攻撃の動機

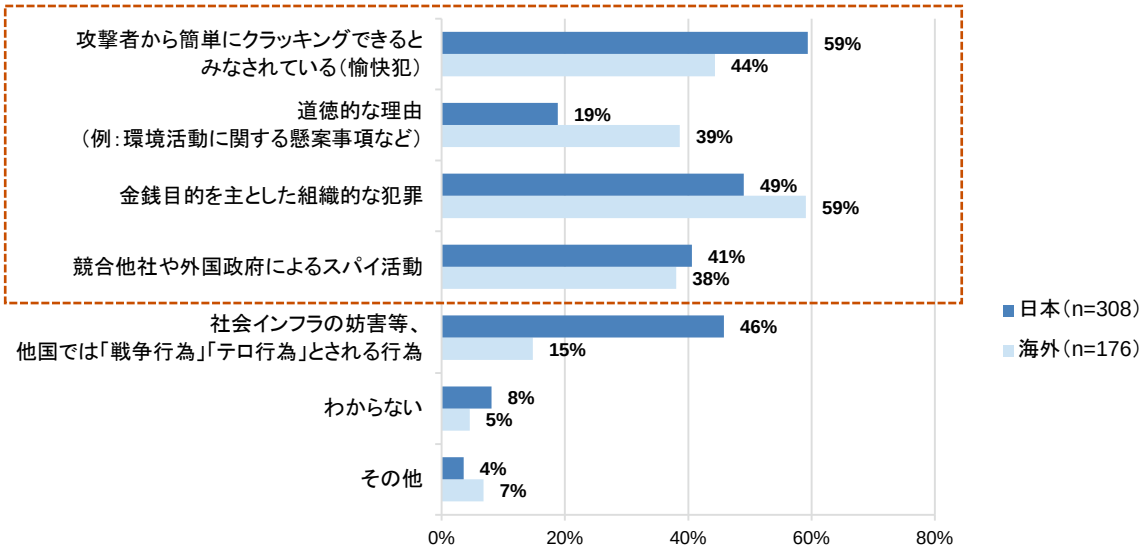
サイバー攻撃の動機として考えられる理由で最も多かったのは「愉快犯」、続いて「金銭目的」、「社会インフラの妨害等」、「スパイ活動」となりました。海外では「金銭目的」を挙げる企業が最も多く、続いて「愉快犯」、「道徳的な理由」、「スパイ活動」となっています。

サイバー攻撃の動機は何だと考えるか（複数回答）



＊2.1.「過去１年にサイバー攻撃の試みを受けたことがあるか」の設問に回答した企業（304社）が対象です。

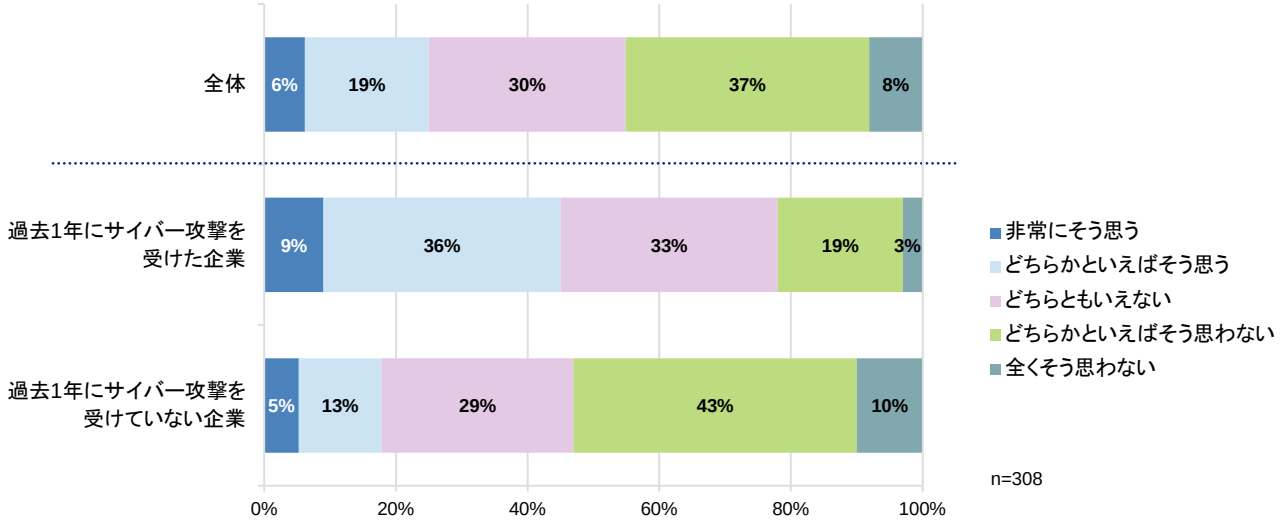
サイバー攻撃の動機の海外との比較（複数回答）



3.3. サイバー攻撃のターゲットとしての魅力

過去1年間にサイバー攻撃を受けた企業の45%が、自社はサイバー攻撃のターゲットとして魅力的だと思う(「非常にそう思う」、「どちらかといえばそう思う」)と回答しています。一方、過去1年間にサイバー攻撃を受けていない企業のうち、自社がサイバー攻撃のターゲットとして魅力的だと考えている企業は18%でした。

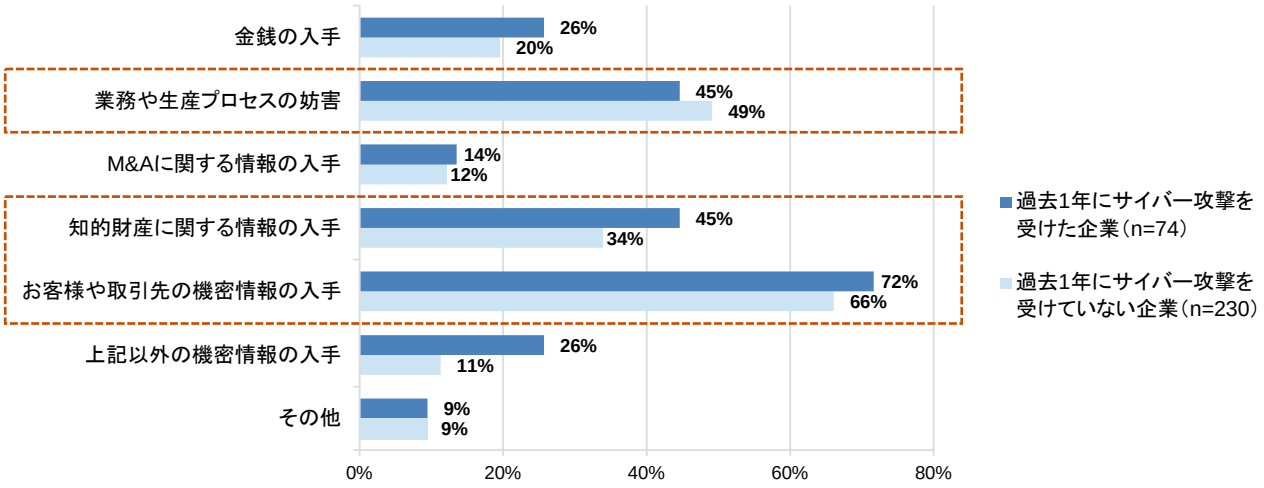
自社はサイバー攻撃のターゲットとして魅力的か



3.4. 自社が攻撃される目的

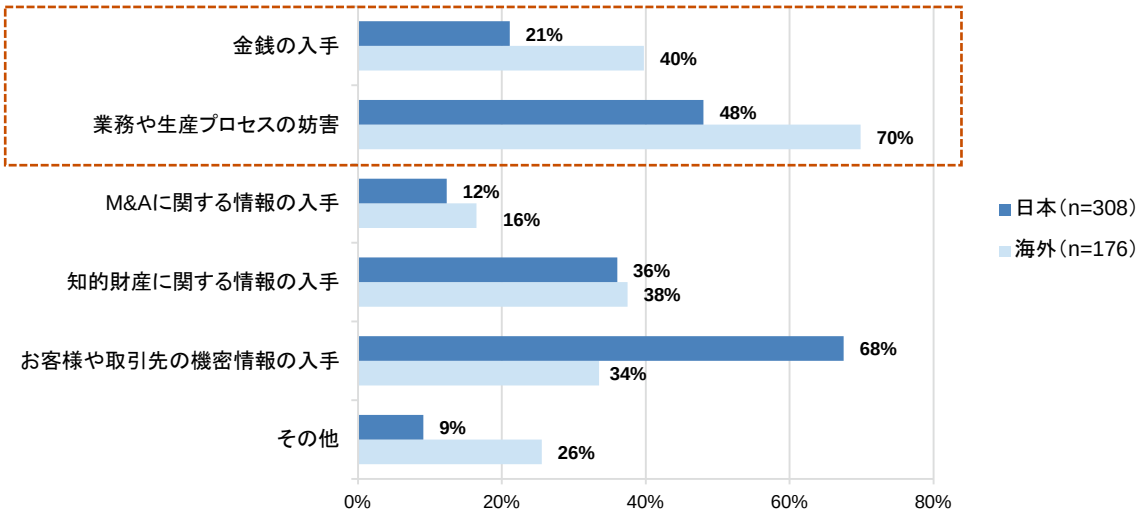
自社が攻撃される目的として最も多く考えられているのは「お客様や取引先の機密情報の入手」、続いて「業務や生産プロセスの妨害」、「知的財産に関する情報の入手」となりました。過去1年間にサイバー攻撃を受けた企業は、受けていない企業よりも、「重要情報（知的財産、機密情報）の入手」を自社が攻撃される目的として考えていることが多いという傾向が見られます。
一方、海外では「業務や生産プロセスの妨害」や「金銭の入手」が主要な目的として挙げられています。

自社が攻撃される目的（複数回答）



＊2.1.「過去１年にサイバー攻撃の試みを受けたことがあるか」の設問に回答した企業（304社）が対象です。

自社が攻撃される目的の海外との比較（複数回答）

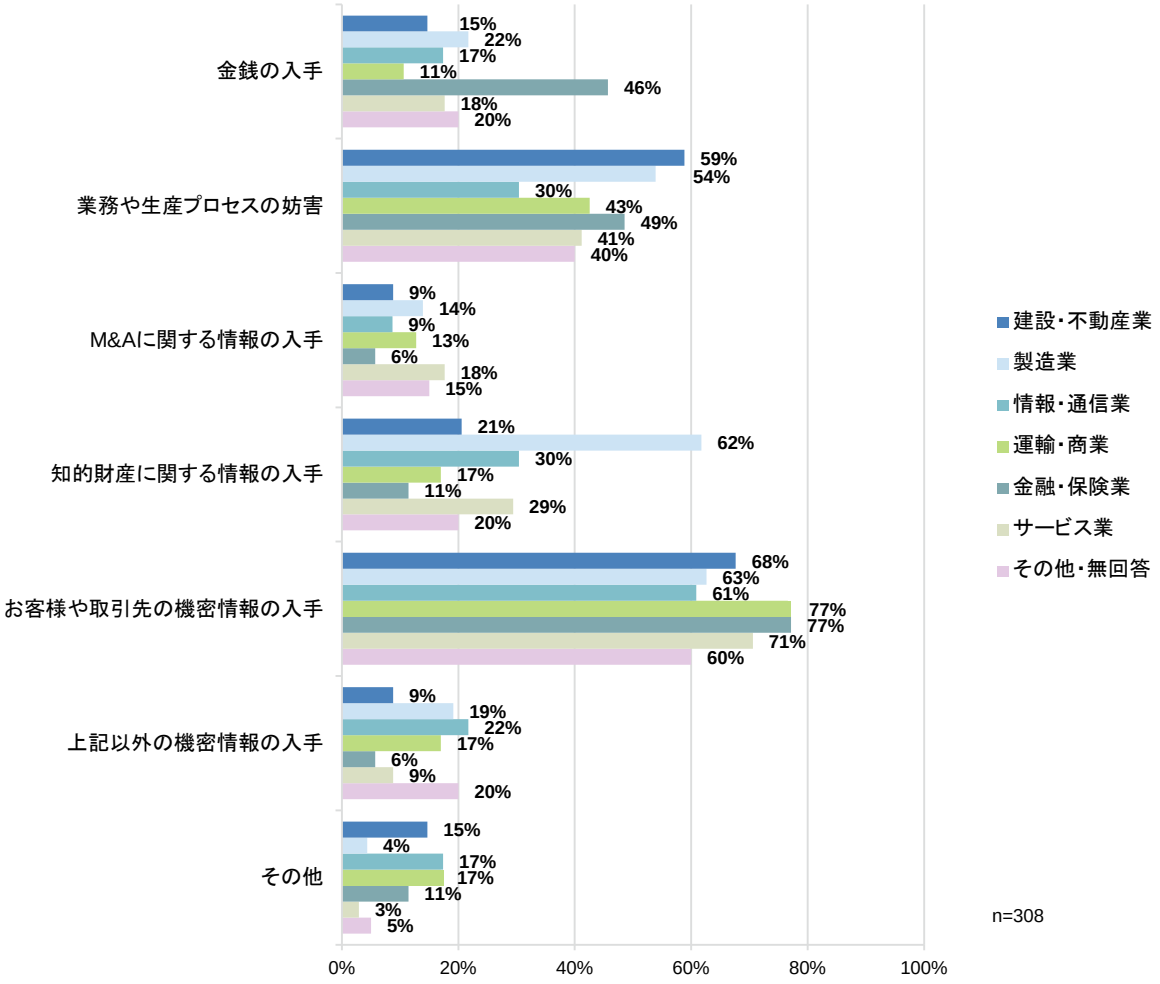


＊回答項目「上記以外の機密情報の入手」は海外の調査設問になかったため、除外しています。

自社が攻撃される目的を業種別にみると、以下のような傾向がうかがえます。

- 「金銭の入手」を挙げた企業は、金融・保険業が突出して多く、運輸・商業には少ない
- 「業務や生産プロセスの妨害」を懸念する企業は、建設・不動産業、製造業に多く、情報・通信業には少ない
- 「知的財産に関する情報の入手」を挙げた企業は、製造業が突出して多く、金融・保険業には少ない
- 「お客様や取引先の機密情報の入手」はどの業種も60%以上の企業が選択しており、業種を問わず共通の標的と考えられている

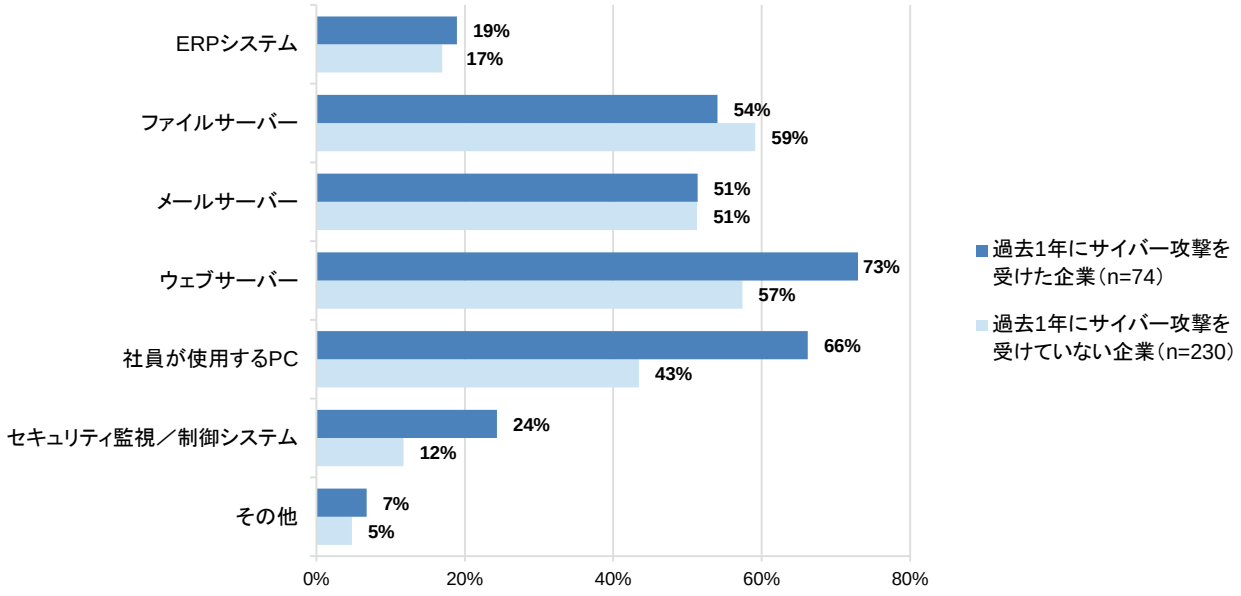
自社が攻撃される目的（業種別・複数回答）



3.5. 自社の攻撃対象

過去1年間にサイバー攻撃を受けた企業の73%がウェブサーバーを、66%が社員が使用するPCを、自社で攻撃対象となるものだと回答しています。また、50%を超える企業がファイルサーバーやメールサーバーも攻撃対象となりうると考えています。

自社で攻撃対象になるものは何か（複数回答）

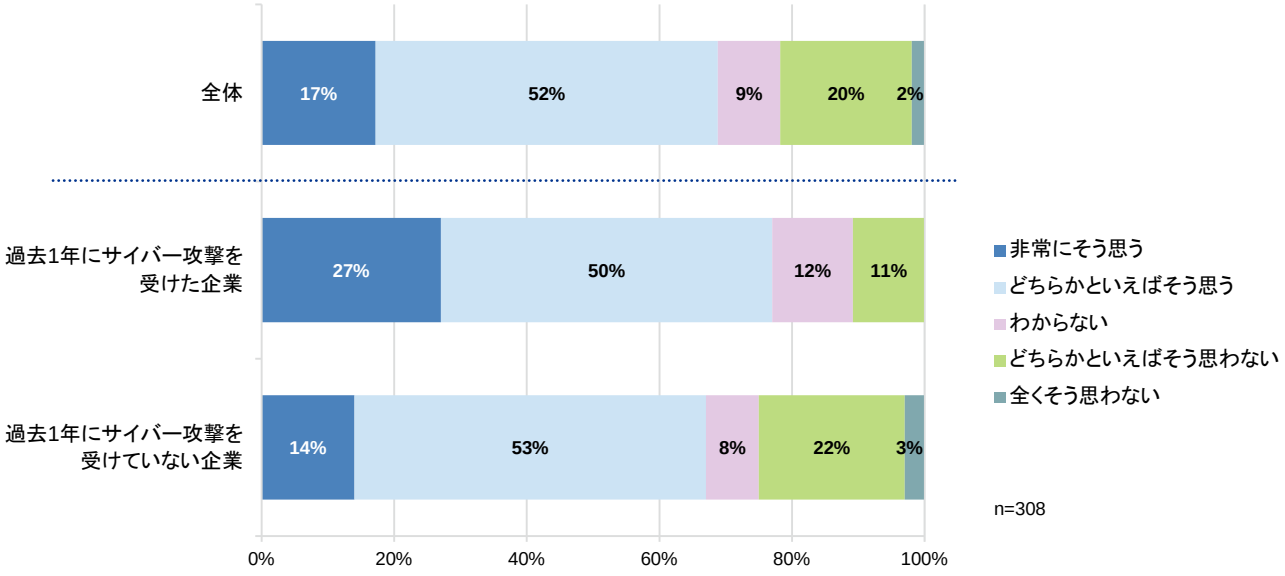


＊2.1.「過去1年にサイバー攻撃の試みを受けたことがあるか」の設問に回答した企業（304社）が対象です。

3.6. サイバー攻撃のリスク認識

過去1年間にサイバー攻撃を受けた企業の77%、受けていない企業の67%が、自社ではサイバー攻撃のリスクを認識している(「非常にそう思う」、「どちらかといえばそう思う」)と回答しています。

自社ではサイバー攻撃のリスクを十分に認識しているか



3.7. サイバー攻撃の発見能力

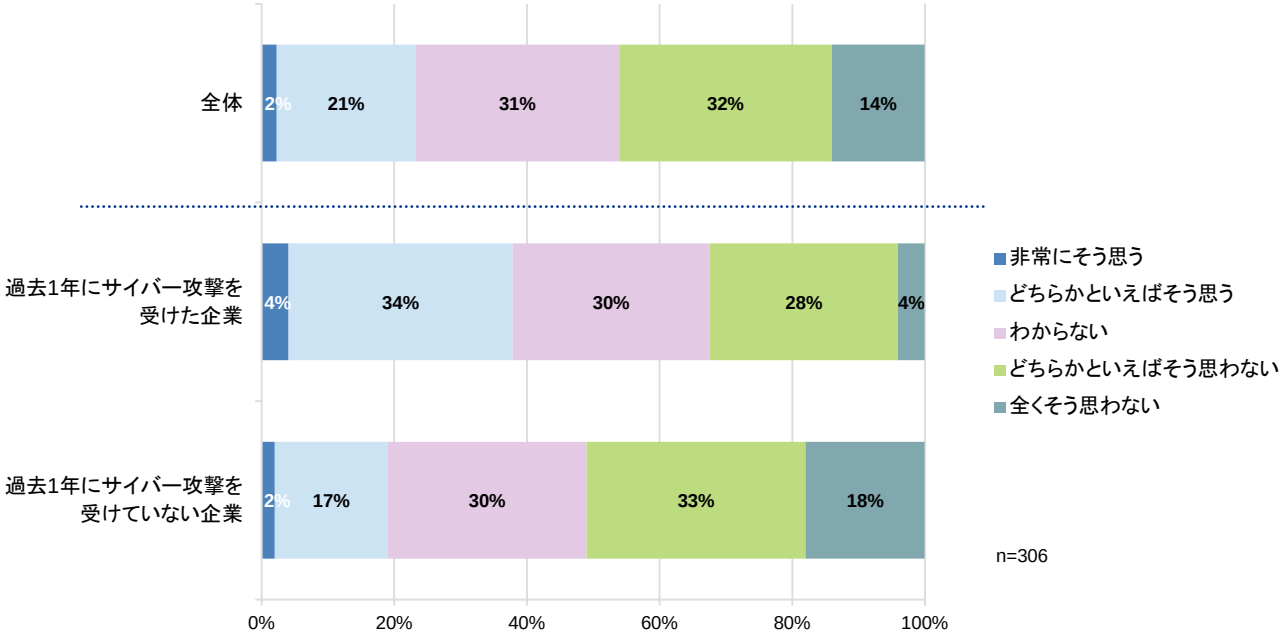
過去1年間にサイバー攻撃を受けた企業の49%、受けていない企業の25%が、自社にはサイバー攻撃を発見する能力がある(「非常にそう思う」、「どちらかといえばそう思う」)と回答しています。過去1年間にサイバー攻撃を受けていない企業において、サイバー攻撃を発見する能力の整備が遅れている現状がうかがえます。

自社にはサイバー攻撃を発見する能力があるか

3.8. サイバー攻撃への対処能力

自社にはサイバー攻撃に効率的に対処する能力がある（「非常にそう思う」、「どちらかといえばそう思う」）と回答した企業は、過去1年間にサイバー攻撃を受けた企業の38%、受けていない企業の19%にすぎません。

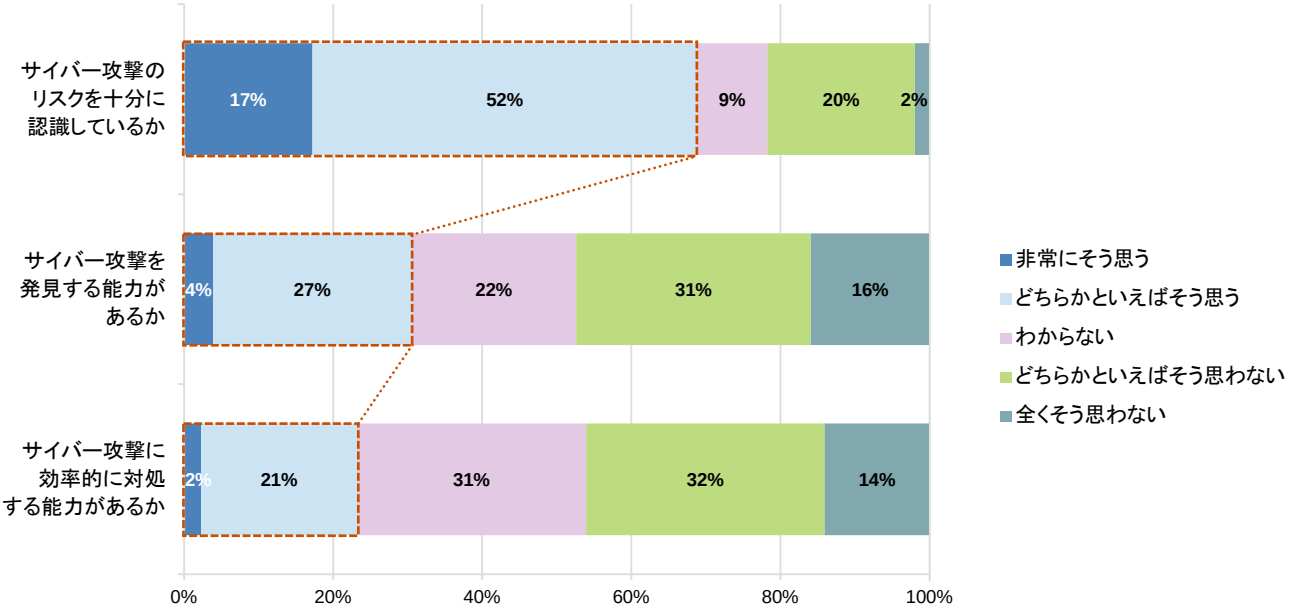
自社にはサイバー攻撃に効率的に対処する能力があるか



＊本設問に無回答の企業は集計に含めていません。

3.6～3.8の一連の回答を比較すると、サイバー攻撃のリスクを認識しながらも、サイバー攻撃を発見し、効率的に対処するための備えが追い付いていないという状況がうかがえます。

サイバー攻撃に対する自社の認識（3.6、3.7、3.8より）



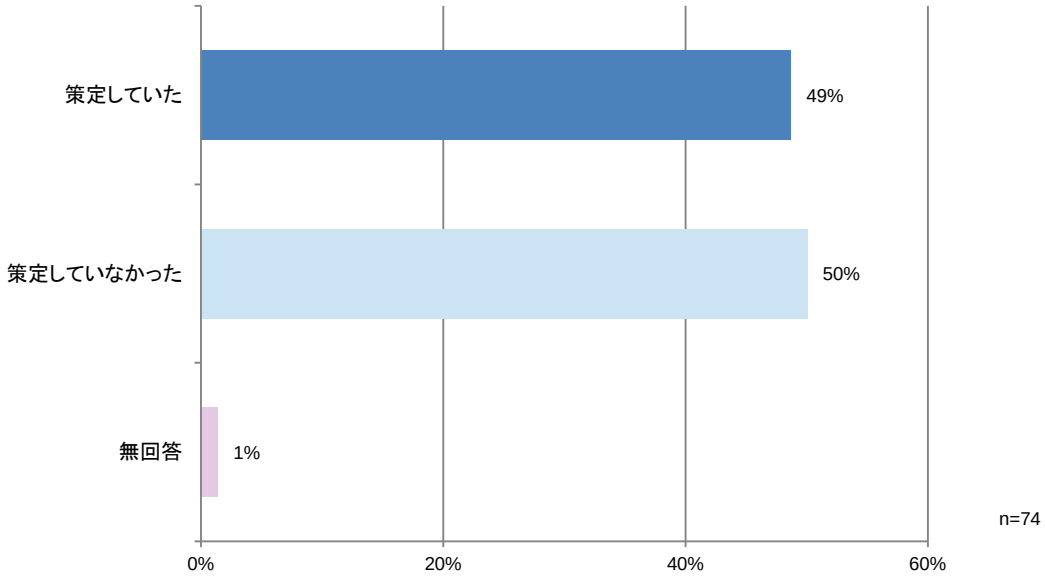
4 サイバー攻撃への対策状況

本章では、対応計画の策定状況、サイバー攻撃を予防・発見・対処するための方策、年間予算など、サイバー攻撃への対策状況について報告します。

4.1. 対応計画の策定状況

過去1年間にサイバー攻撃を受けた企業のうち、サイバー攻撃を受ける前に対応計画を策定していた企業は49%でした。

サイバー攻撃を受ける前に対応計画を策定していたか

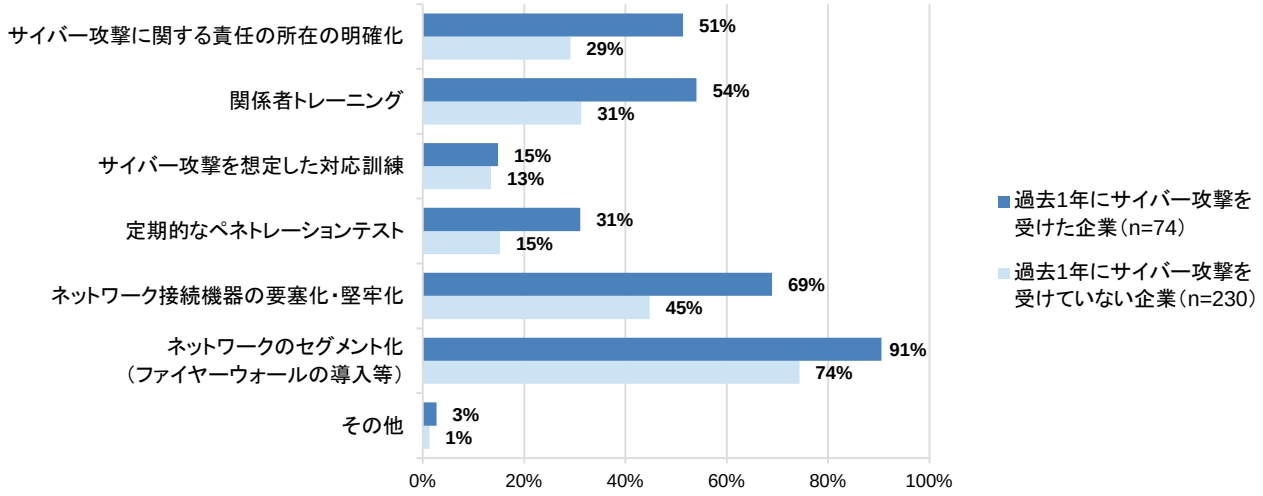


＊2.1の設問で「過去1年間にサイバー攻撃の試みを受けたことがある」と回答した企業が対象です。

4.2. サイバー攻撃の予防

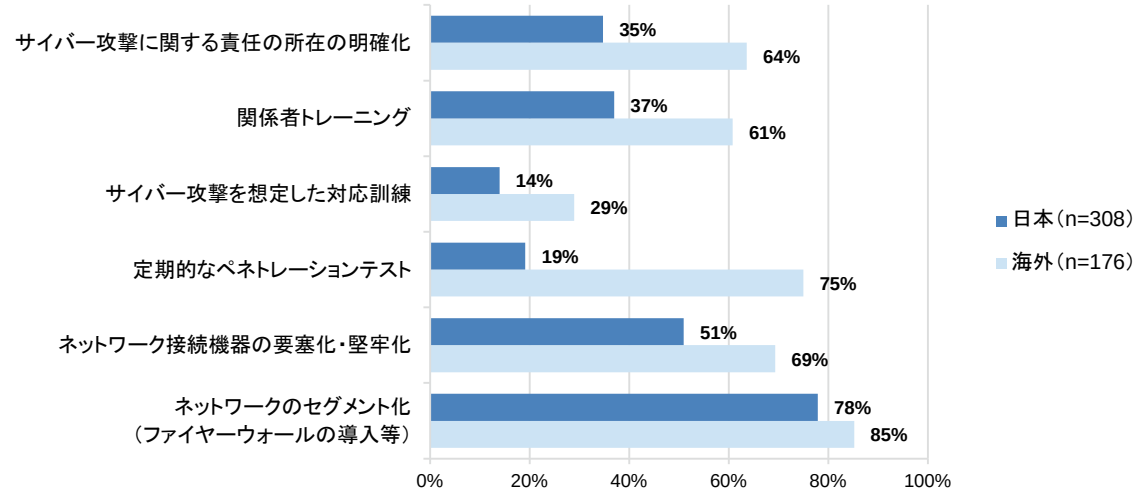
サイバー攻撃を予防するために、過去1年間にサイバー攻撃を受けた企業の91%、受けていない企業の74%が「ネットワークのセグメント化」を実施しています。「ネットワーク機器の要塞化・堅牢化」を行っている企業も過去1年間にサイバー攻撃を受けた企業の69%にのぼります。海外では、これらの対策に加えて、「定期的なペネトレーションテスト」を75%、「サイバー攻撃に関する責任の所在の明確化」および「関係者トレーニング」を60%を超える企業が実施しています。いずれの方策においても、過去1年間にサイバー攻撃を受けた企業の方が、受けていない企業よりも対策が進んでおり、また、海外の方が対策が進んでいるという状況がうかがえます。

サイバー攻撃をどのように予防しているか（複数回答）



＊2.1.「過去1年にサイバー攻撃の試みを受けたことがあるか」の設問に回答した企業（304社）が対象です。

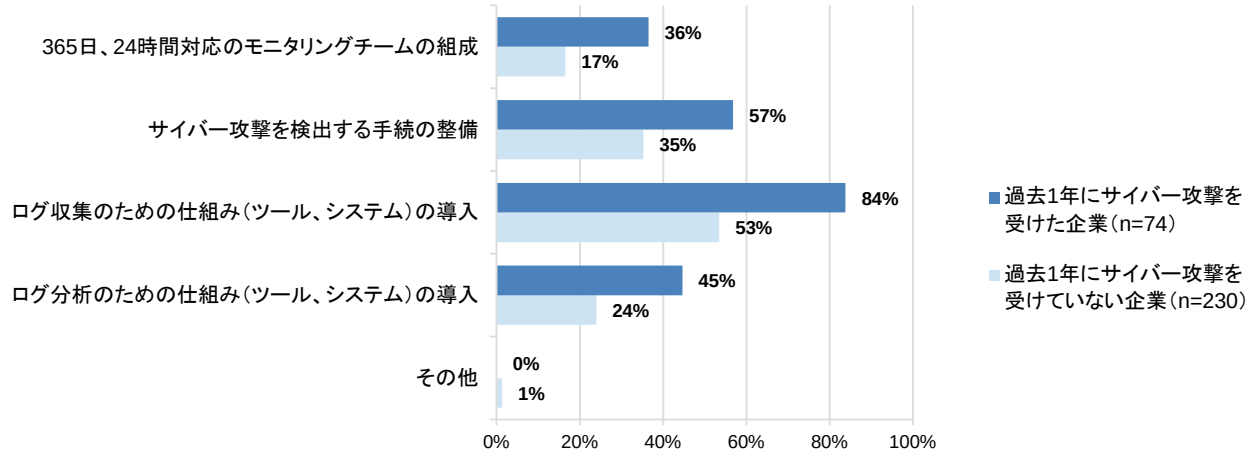
サイバー攻撃予防策の海外との比較（複数回答）



4.3. サイバー攻撃の発見

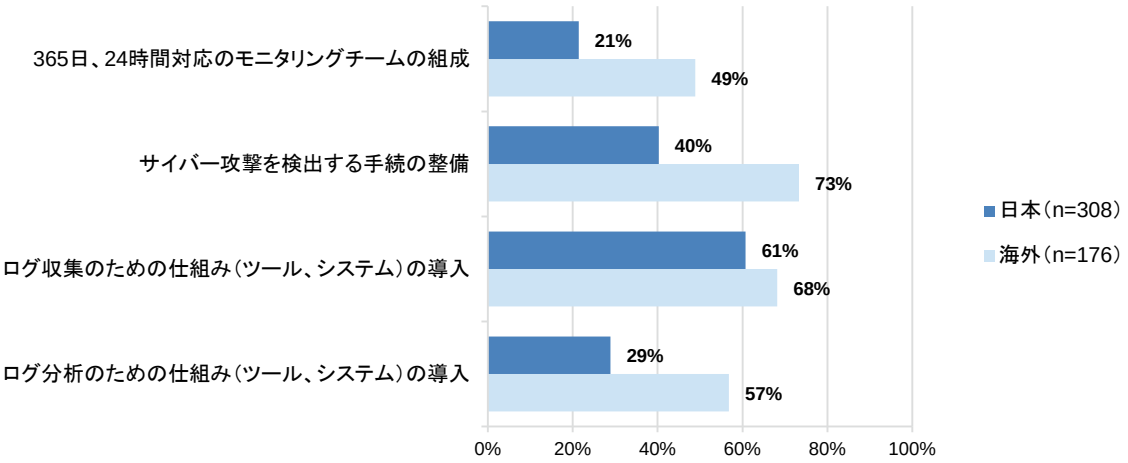
サイバー攻撃を発見するために、過去1年間にサイバー攻撃を受けた企業の84%、受けていない企業の53%がログ収集のための仕組みを導入しています。しかし、収集したログを分析するための仕組みを導入している企業はその半数程度にとどまります。海外では68%の企業がログ収集のための仕組みを導入し、57%の企業がログ分析のための仕組みを導入しています。
また、海外では、「サイバー攻撃を検出する手続の整備」に最も多い回答が寄せられており、組織的対応が重視されていると考えられます。
いずれの方策においても、過去1年間にサイバー攻撃を受けた企業の方が、受けていない企業よりも対策が進んでおり、また、海外の方が対策が進んでいるという状況がうかがえます。

サイバー攻撃をどのように発見するか（複数回答）



＊2.1.「過去1年にサイバー攻撃の試みを受けたことがあるか」の設問に回答した企業（304社）が対象です。

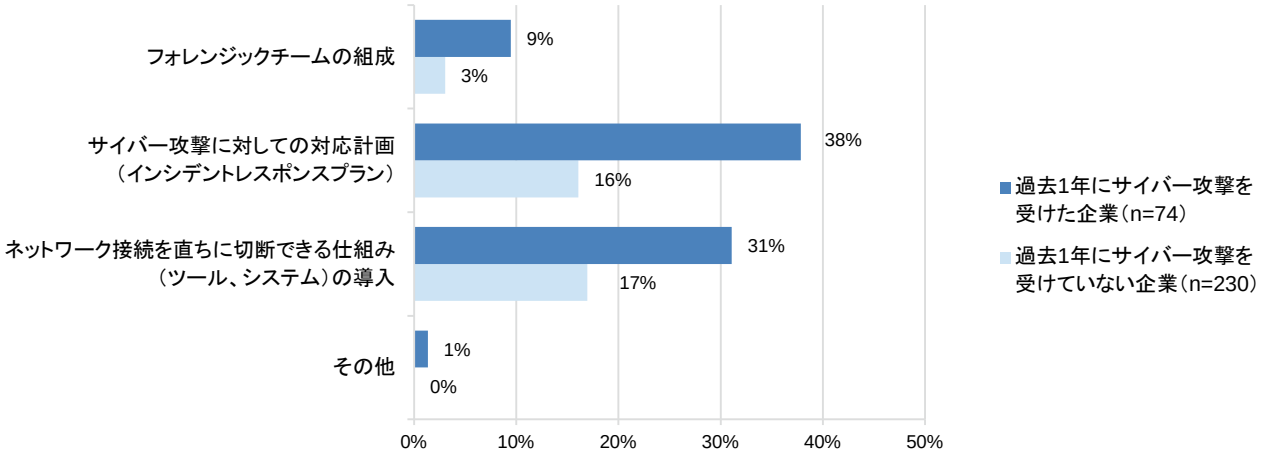
サイバー攻撃発見策の海外との比較（複数回答）



4.4. サイバー攻撃発見時の対処

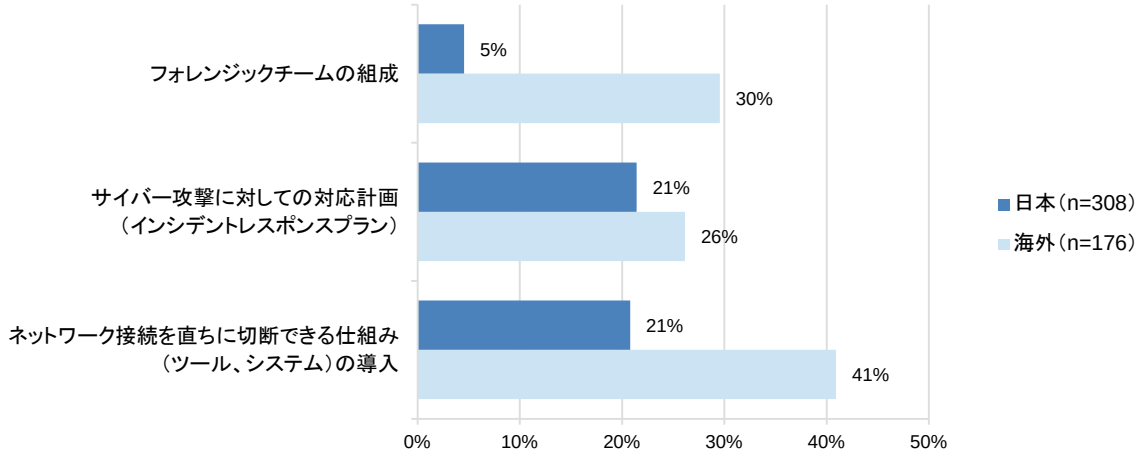
サイバー攻撃への対処として最も多かったのは「サイバー攻撃に対しての対応計画（インシデントレスポンスプラン）」ですが、この回答を選択したのは、過去1年間にサイバー攻撃を受けた企業の38%、受けていない企業の16%にすぎません。海外では41%の企業がネットワーク機器をただちに切断できる仕組みを導入しています。
いずれの方策においても、過去1年間にサイバー攻撃を受けた企業の方が、受けていない企業よりも対策が進んでおり、また、海外の方が対策が進んでいるという状況がうかがえます。
また、サイバー攻撃に対処するための対策は、サイバー攻撃を予防・発見するための対策と比較して導入が進んでいない状況がうかがえます。

サイバー攻撃にどのように対処するか（複数回答）



＊2.1.「過去1年にサイバー攻撃の試みを受けたことがあるか」の設問に回答した企業（304社）が対象です。

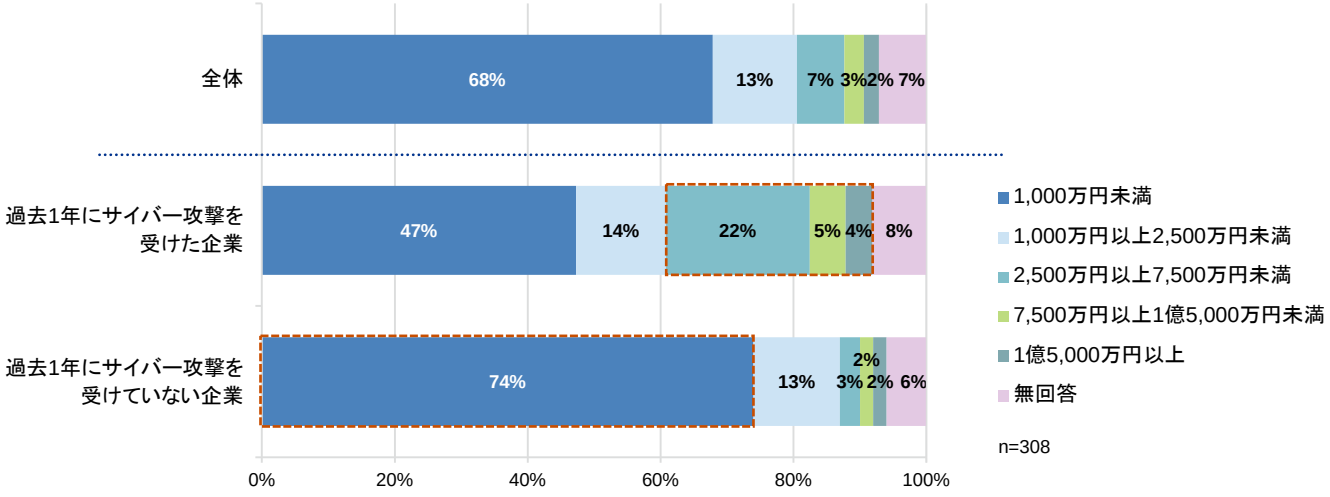
サイバー攻撃対処策の海外との比較（複数回答）



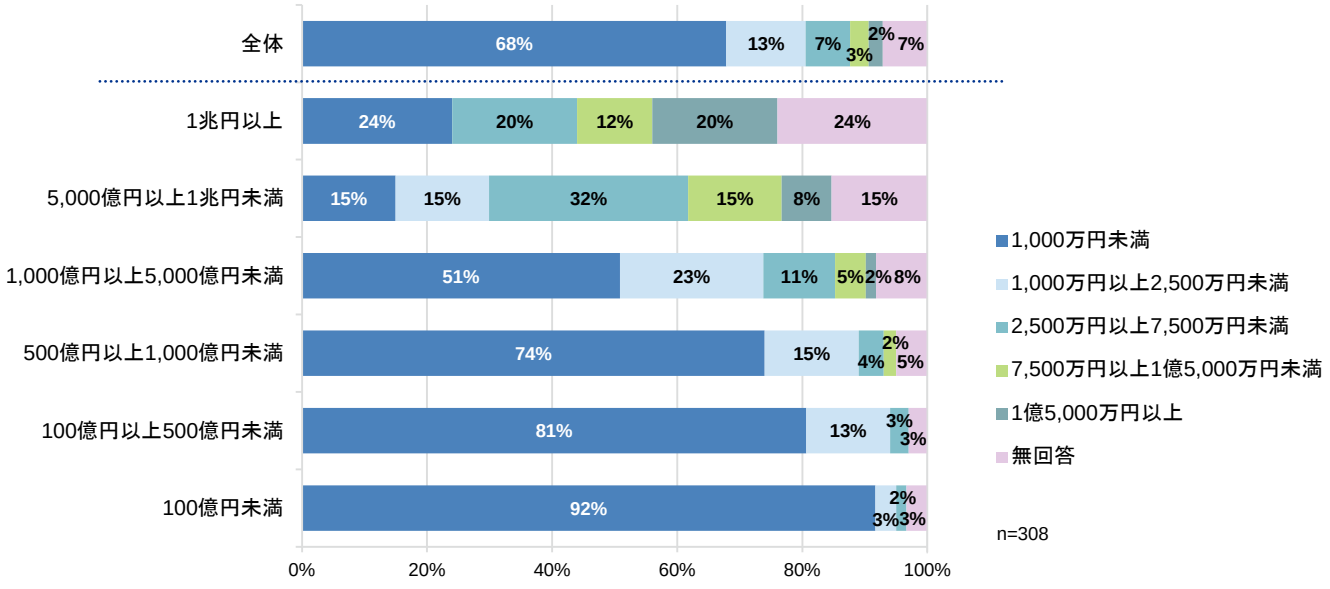
4.5. サイバー攻撃予防のための年間予算

サイバー攻撃の予防のための年間予算については、過去1年間にサイバー攻撃を受けた企業の31%が2,500万円以上と回答しており、1億5,000万円以上と回答した企業も4%ありました。
一方、受けていない企業の74%は1,000万円未満と回答しています。
また、年間売上高が大きい企業ほど、サイバー攻撃の予防に使っている年間予算も大きい傾向がうかがえます。

サイバー攻撃の予防のための年間予算はどれくらいか

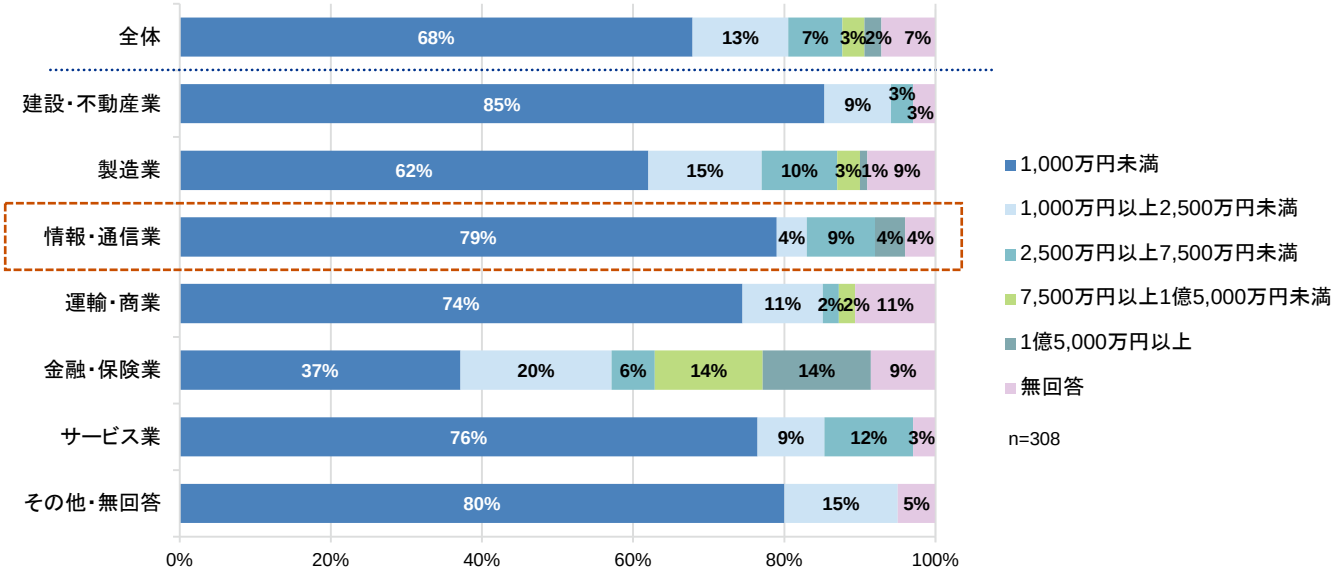


サイバー攻撃の予防のための年間予算はどれくらいか（年間売上高別）

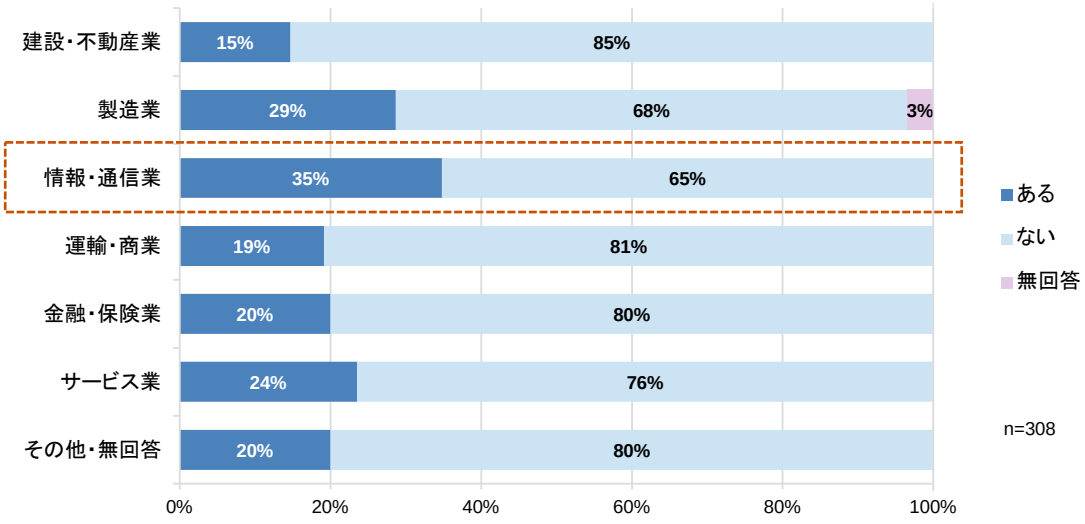


業種別にみると、金融・保険業、製造業の順に、サイバー攻撃予防のための年間予算が多い傾向がうかがえます。35%の企業が過去1年間にサイバー攻撃の試みを受けたと回答している情報・通信業では、年間予算1,000万円未満の企業が79%を占めている一方、1億5,000万円以上の回答が4%あり、対応の二極化が進んでいる可能性が考えられます。

サイバー攻撃の予防のための年間予算はどれくらいか（業種別）



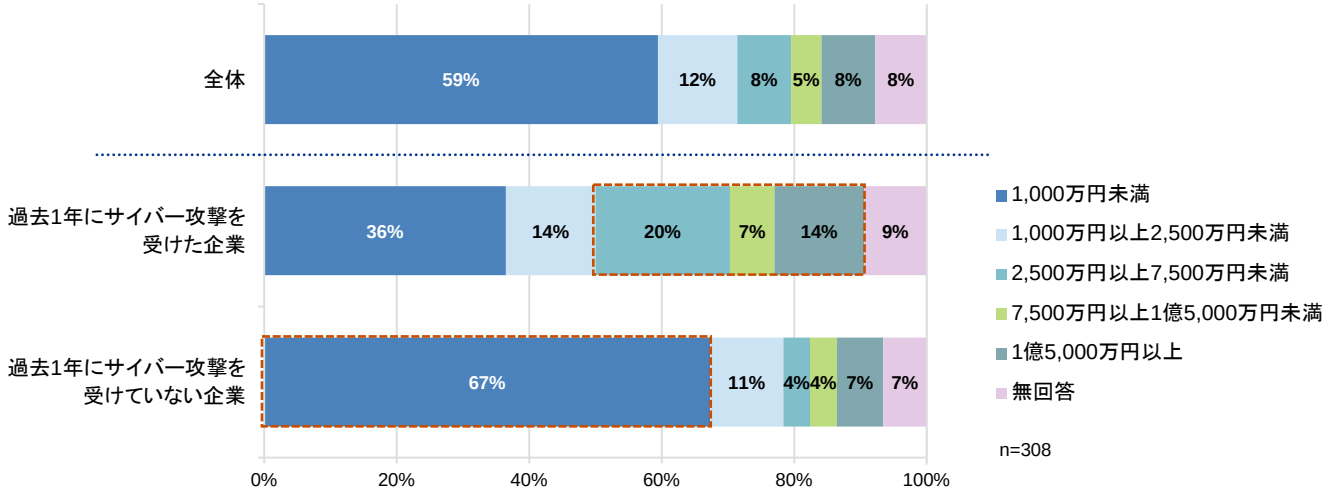
過去1年間にサイバー攻撃の試みを受けたことがあるか（業種別） [2.1.再掲]



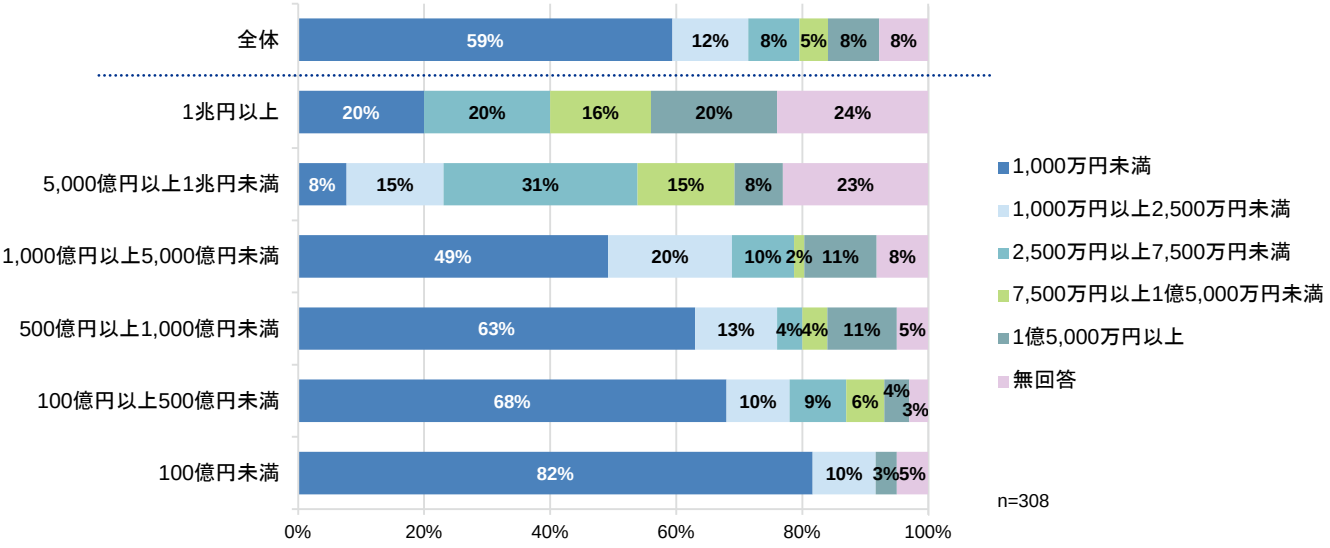
4.6. サイバー攻撃予防のための年間予算（システム関連）

サイバー攻撃の予防のための年間予算のうちシステム関連に使用している金額については、過去1年間にサイバー攻撃を受けた企業の41%が2,500万円以上と回答しており、1億5,000万円以上と回答した企業も14%ありました。一方、受けていない企業の67%は1,000万円未満と回答しています。
また、年間売上高が大きい企業ほど、サイバー攻撃の予防に使っている年間予算も大きい傾向がうかがえます。

年間予算のうちどれくらいをシステム関連に使用しているか

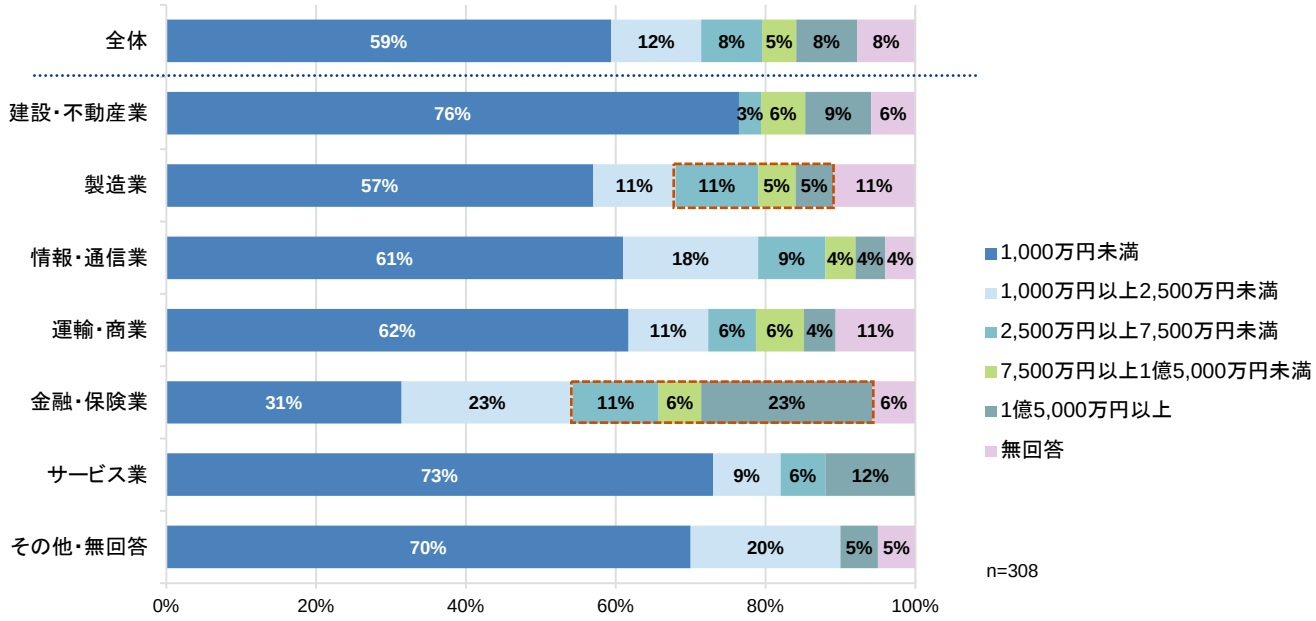


年間予算のうちどれくらいをシステム関連に使用しているか（年間売上高別）



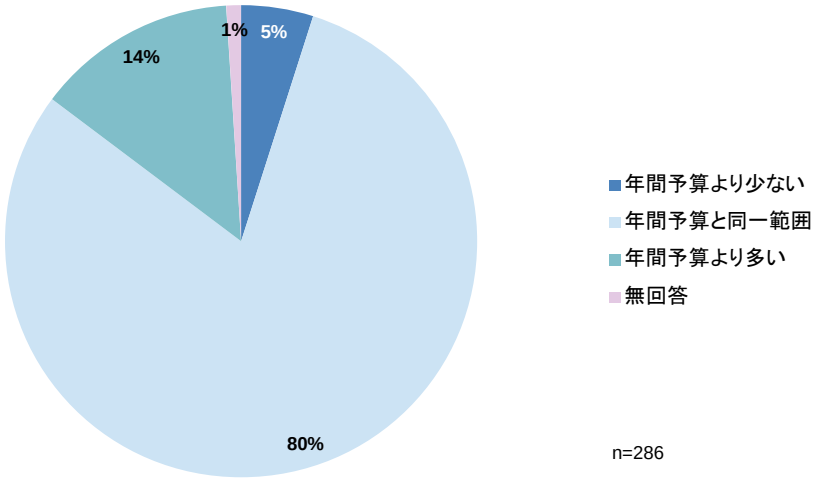
業種別にみると、金融・保険業、製造業の順に、サイバー攻撃予防のためのシステム関連予算が多い傾向がうかがえます。

年間予算のうちどれくらいをシステム関連に使用しているか（業種別）



この設問では80%の企業が前項(4.5)で回答した年間予算と同一範囲の選択肢を選択していることから、サイバー攻撃予防のための年間予算の大半がシステム関連に割り当てられている状況がうかがえます。
また、14%の企業が年間予算を超える金額を選択しており、いずれの業界においても、システム関連予算をサイバー攻撃予防とそれ以外に切り分けることが難しいという状況がうかがえます。

サイバー攻撃予防のための年間予算とシステム関連予算の関係



n=286

＊設問4.5.に無回答の企業は集計に含めていません。

年間予算のうちどれくらいをシステム関連に使用しているか(年間予算別)

システム予算 / 年間予算	1,000万円未満	1,000万円以上2,500万円未満	2,500万円以上7,500万円未満	7,500万円以上1億5,000万円未満	1億5,000万円以上	無回答	計
1,000万円未満	85%	3%	3%	3%	5%	1%	100%
1,000万円以上2,500万円未満	15%	67%	0%	0%	15%	3%	100%
2,500万円以上7,500万円未満	4%	14%	64%	0%	14%	4%	100%
7,500万円以上1億5,000万円未満	0%	0%	33%	67%	0%	0%	100%
1億5,000万円以上	0%	0%	14%	0%	86%	0%	100%

n=286

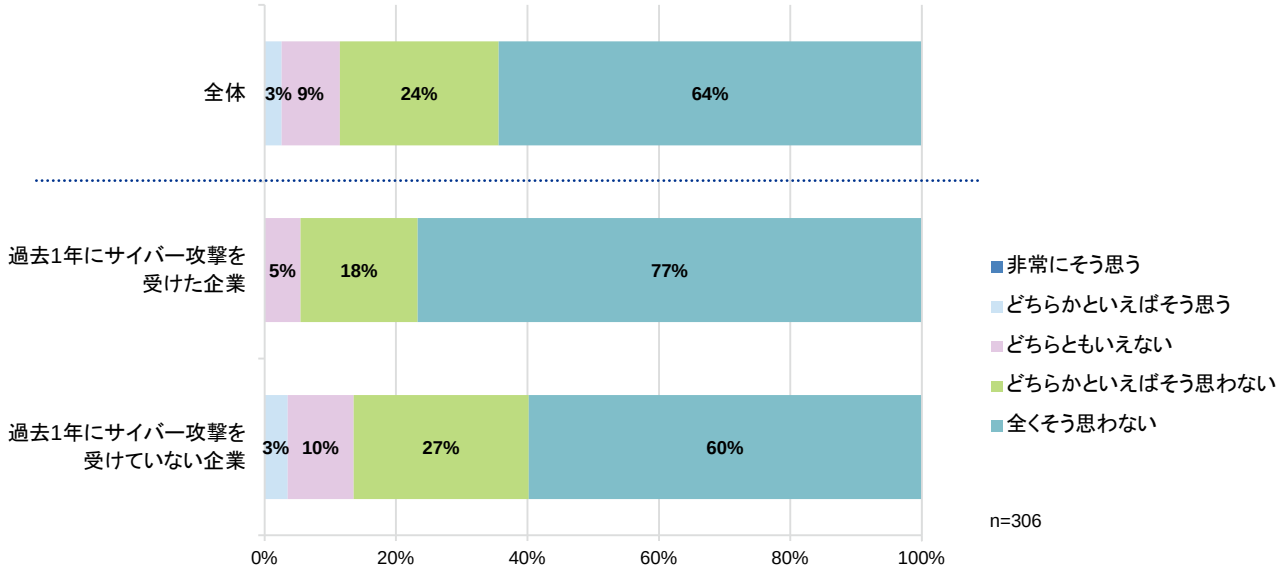
5 サイバー攻撃への今後の取組みに対する考え

本章では、対応計画の策定状況、サイバー攻撃を受けた場合の対応や、サイバー攻撃への新たな対策など、サイバー攻撃への今後の取組みに対する考えについて報告します。

5.1. サイバー攻撃は一時的なものと思うか

過去1年間にサイバー攻撃を受けた企業の95%、受けていない企業の87%が、サイバー攻撃は一時的なものとは思わない(「全くそう思わない」、「どちらかといえばそう思わない」)と回答しています。なお、この設問に「非常にそう思う」と回答した企業はありませんでした。

サイバー攻撃は一時的なものと思うか

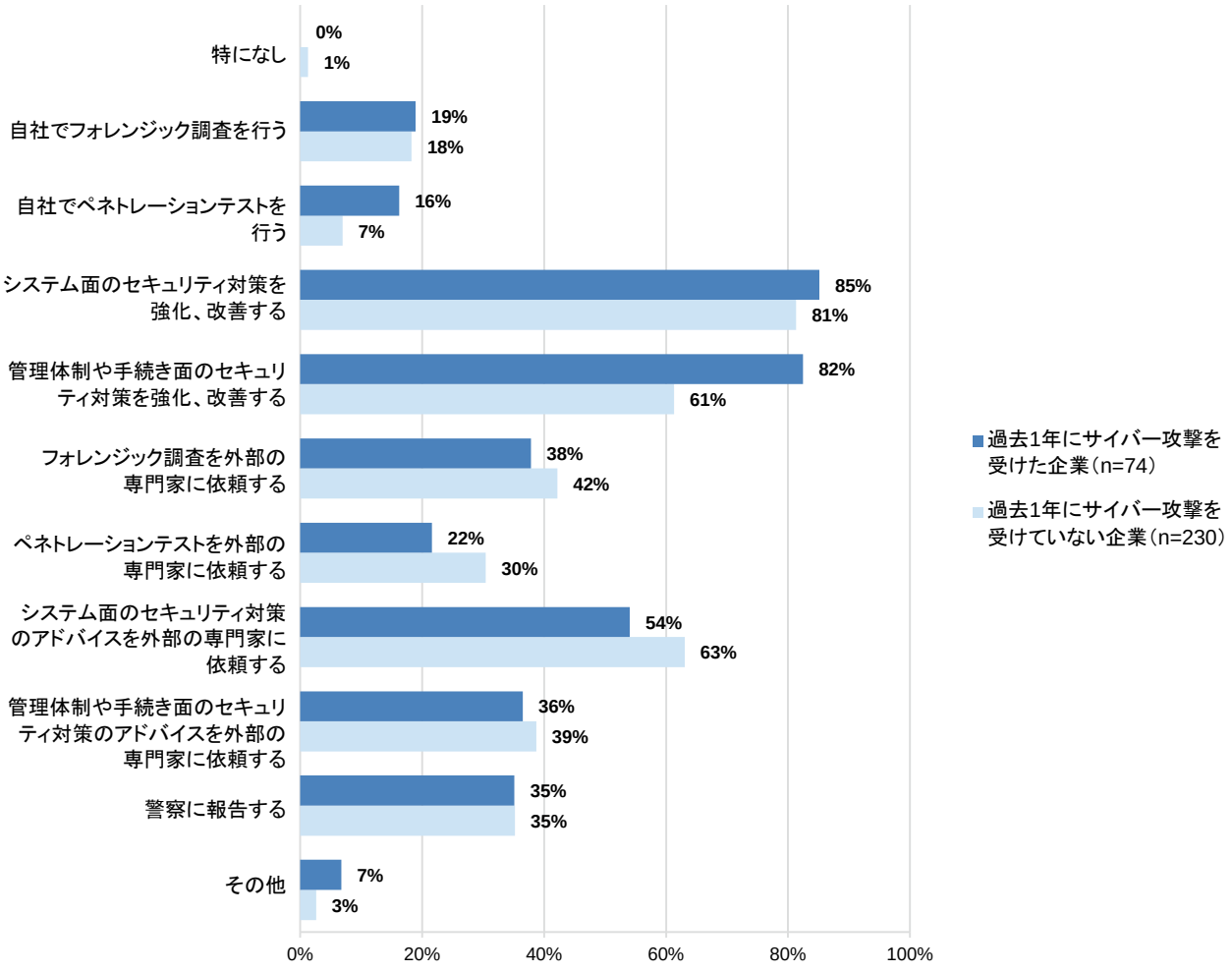


＊本設問に無回答の企業は集計に含めていません。

5.2. サイバー攻撃を受けた場合の対応

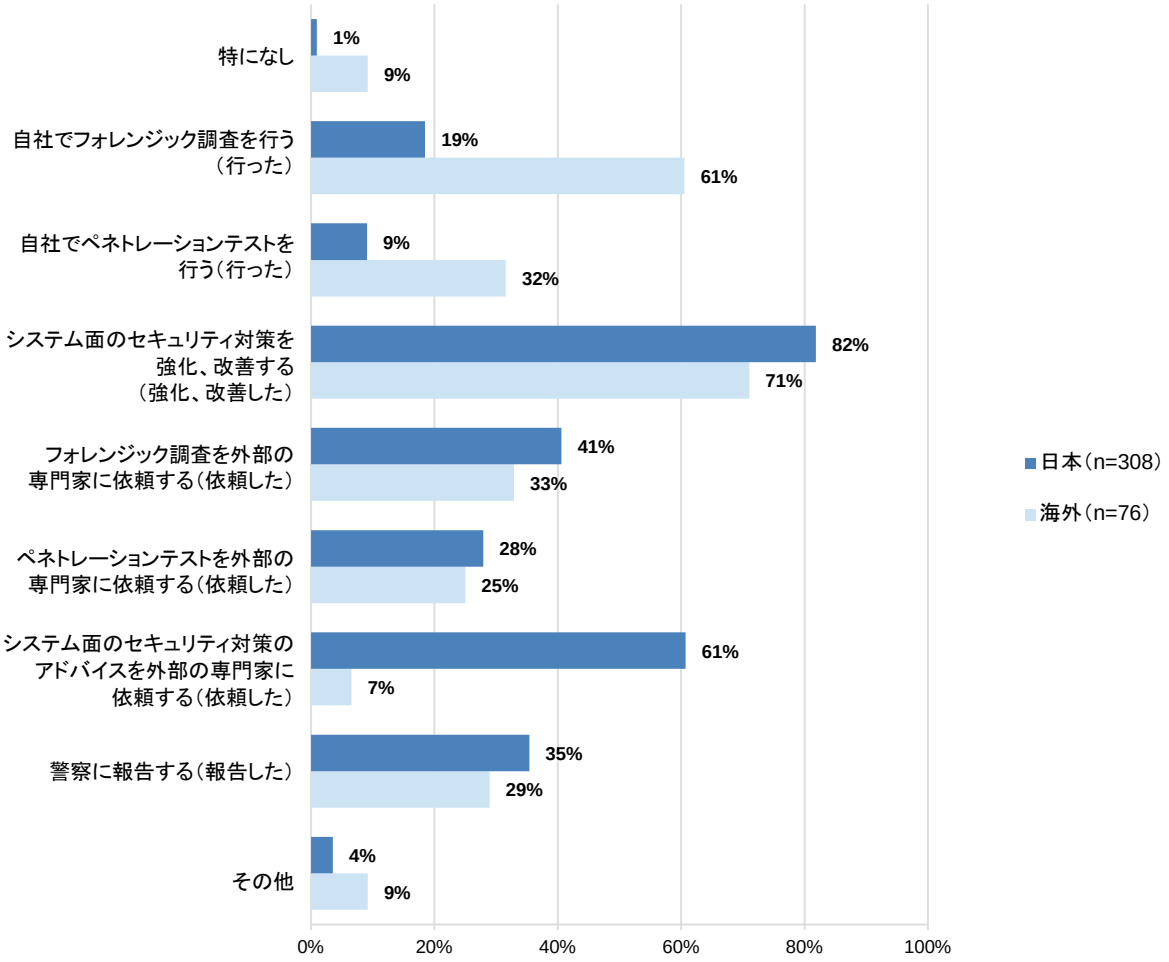
サイバー攻撃を受けた場合の対応として最も多かったのは、「システム面のセキュリティ対策を強化、改善する」、続いて「管理体制や手続き面のセキュリティ対策を強化、改善する」、「システム面のセキュリティ対策のアドバイスを外部の専門家に依頼する」となりました。海外では、国内と比較して、「自社でフォレンジック調査を行う」、「自社でペネトレーションテストを行う」といった、自社で対応するという回答が多く寄せられています。

サイバー攻撃を受けた場合はどのように対応するか（複数回答）



＊ 2.1.「過去1年にサイバー攻撃の試みを受けたことがあるか」の設問に回答した企業（304社）が対象です。

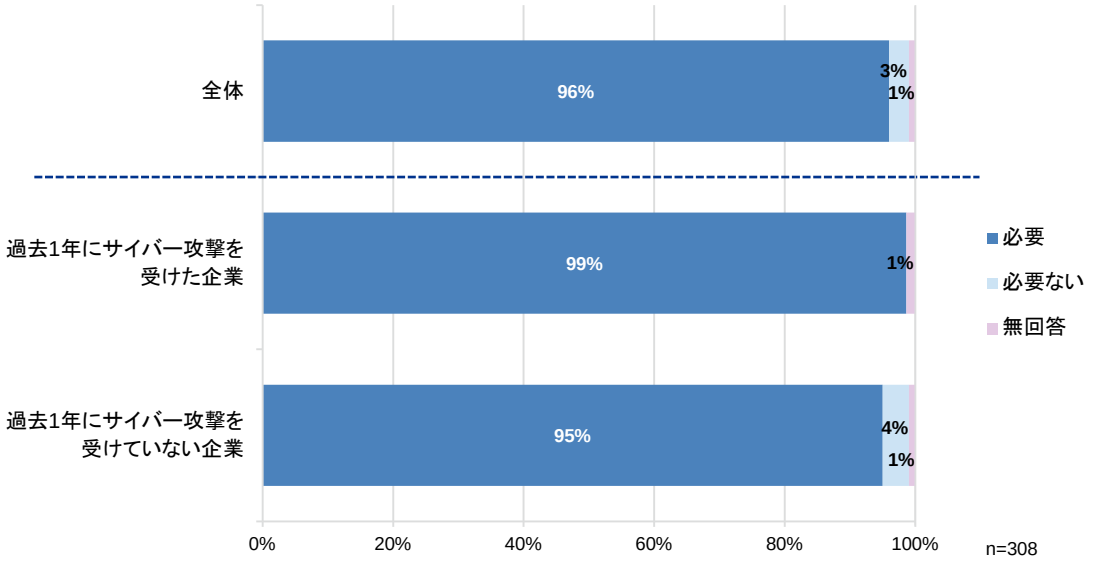
サイバー攻撃を受けた場合の対応の海外との比較（複数回答）



5.3. サイバー攻撃への新たな対策の必要性

過去1年間にサイバー攻撃を受けた企業の99%、受けていない企業の95%が、「サイバー攻撃への新たな対策が必要」と回答しています。

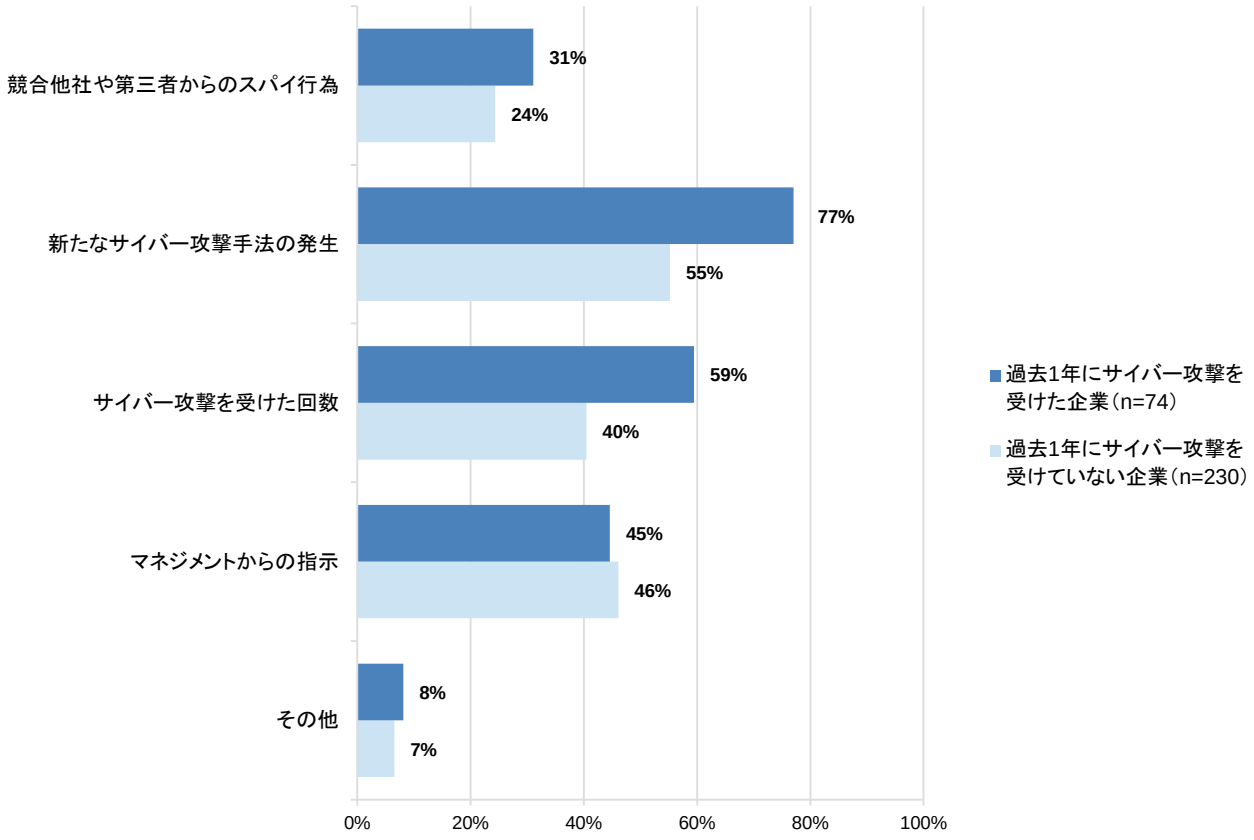
サイバー攻撃への新たな対策は必要か



5.4. サイバー攻撃への新たな対策を導入するきっかけ

新たな対策を導入するきっかけとして最も多かったのは、「新たなサイバー攻撃手法の発生」、続いて「サイバー攻撃を受けた回数」、「マネジメントからの指示」となりました。

サイバー攻撃への新たな対策を導入するきっかけは何か（複数回答）

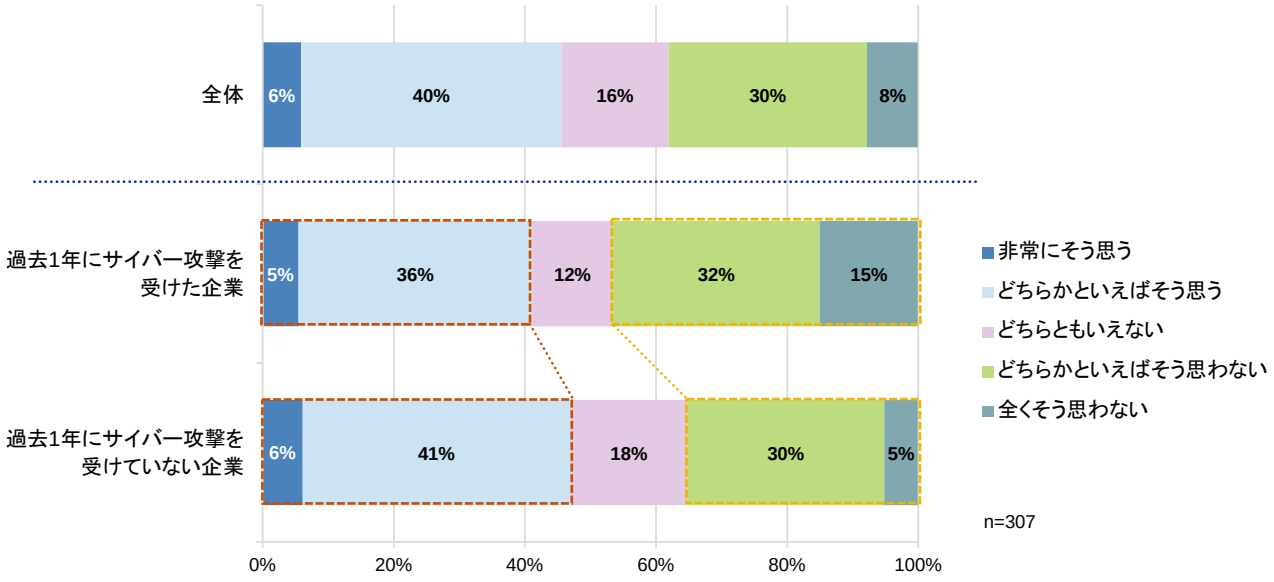


＊ 2.1.「過去1年にサイバー攻撃の試みを受けたことがあるか」の設問に回答した企業（304社）が対象です。

5.5. サイバー攻撃の予防のテクノロジーへの依存

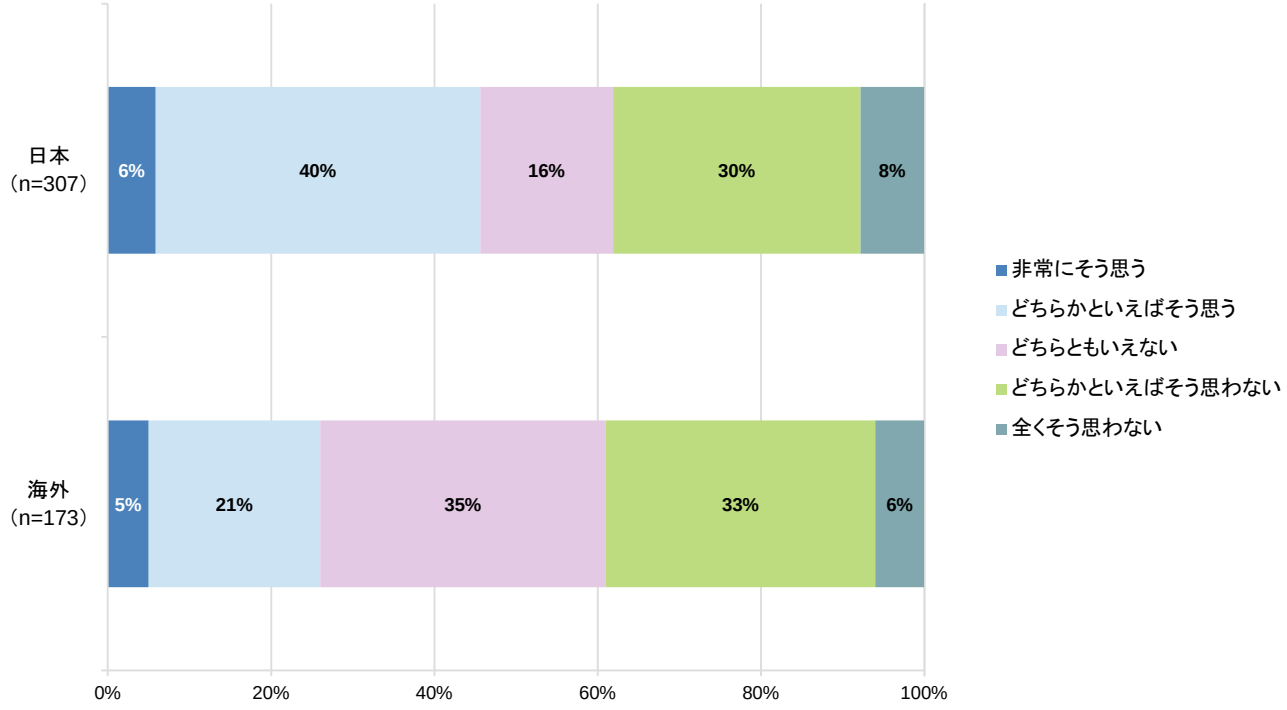
サイバー攻撃の予防をテクノロジーに依存すべきかについて、過去1年間にサイバー攻撃を受けた企業の41%が「そう思う(「非常にそう思う」、「どちらかといえばそう思う」、以下同じ)」と回答し、47%が「そう思わない(「全くそう思わない」、「どちらかといえばそう思わない」、以下同じ)」と回答しています。受けていない企業では47%が「そう思う」と回答し、35%が「そう思わない」と回答しています。サイバー攻撃を受けた経験の有無により、「そう思う」と「そう思わない」の比率が逆転していることから、実際にサイバー攻撃を受けることによってテクノロジーだけでは防ぎきれないと認識を深めている可能性が考えられます。また、海外で「そう思う」と回答した企業は26%にすぎず、テクノロジーによる防御の限界を感じている企業が国内より多い状況がうかがえます。

サイバー攻撃の予防はテクノロジーに依存すべきか



＊本設問に無回答の企業は集計に含めていません。

サイバー攻撃の予防はテクノロジーに依存すべきか（海外との比較）

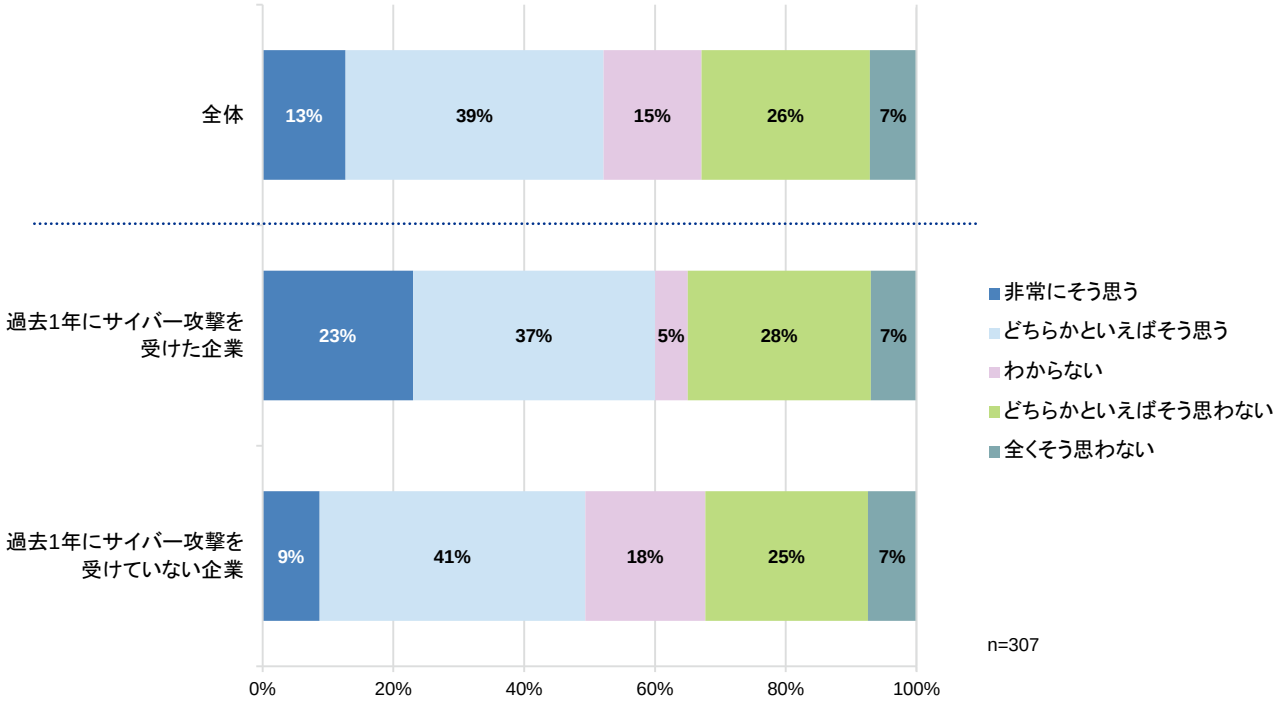


＊本設問に無回答の企業は集計に含めていません。

5.6. サイバー攻撃の予防への取締役の関与

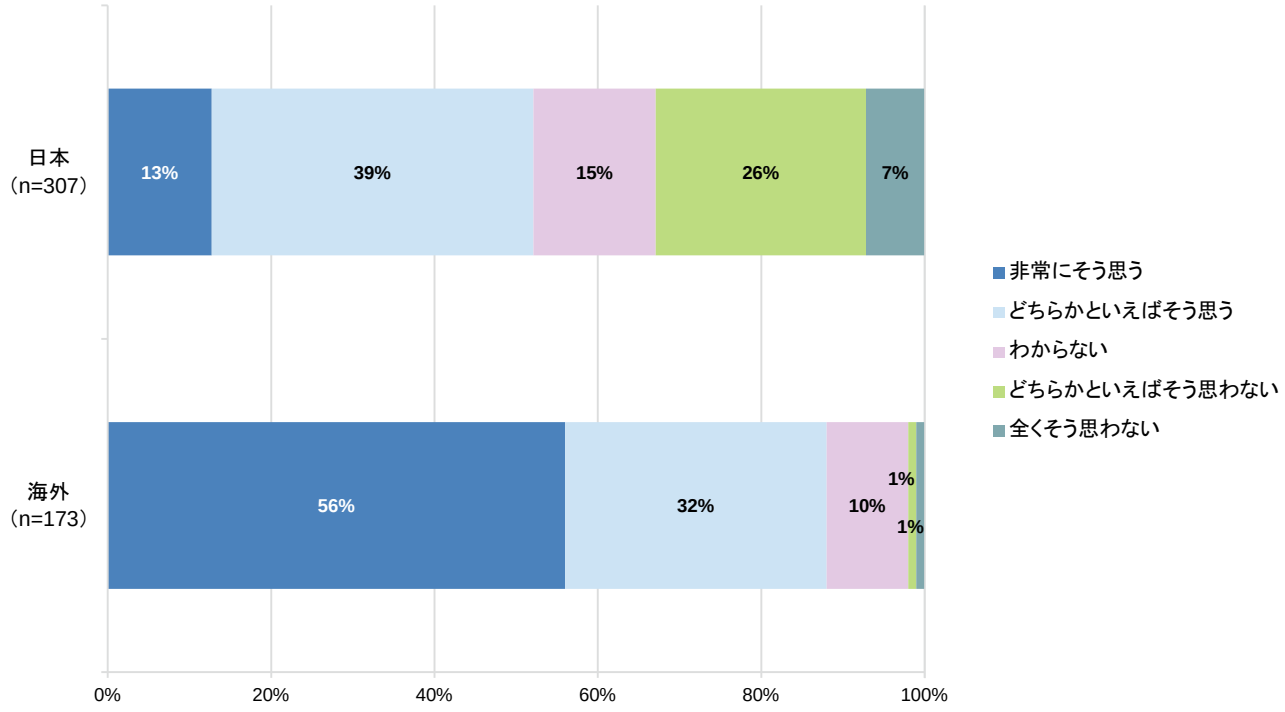
過去1年間にサイバー攻撃を受けた企業の60%、受けていない企業の50%がサイバー攻撃の予防は取締役レベルで議論すべき(「非常にそう思う」、「どちらかといえばそう思う」、以下同じ)と考えています。海外では88%の企業が取締役の関与が必要だと回答しています。
過去1年間にサイバー攻撃を受けた企業の23%が「非常にそう思う」と回答しており、サイバー攻撃対策を円滑に推進するために、取締役レベルの強い関与が求められている状況がうかがえます。

サイバー攻撃の予防は取締役レベルで議論すべきか



＊本設問に無回答の企業は集計に含めていません。

サイバー攻撃の予防は取締役レベルで議論すべきか（海外との比較）



＊本設問に無回答の企業は集計に含めていません。

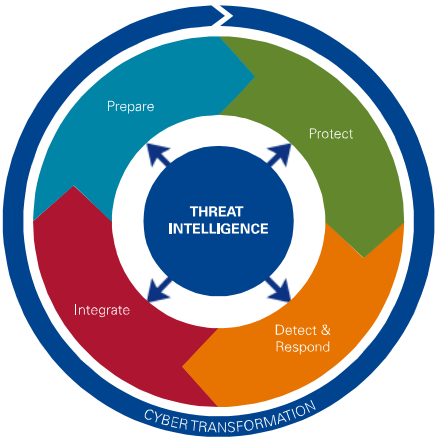
KPMGとサイバーセキュリティ

KPMGのメンバーファームは、政府機関や諜報機関の情報収集・分析活動の設計、実行を支援してきました。また、世界トップクラスの企業におけるサイバーセキュリティプログラムの策定にも複数参画しています。

こうして得られた知見に基づき、KPMGでは、効果的なサイバーセキュリティに関する脅威情報の収集・分析機能の構成要素を独自の視点から整理しています。

KPMGは脅威情報の収集・分析を、効果的なサイバーセキュリティ対策の中核を成す構成要素としてとらえています。KPMGのメンバーファームは、顧客が適切な情報収集・分析モデルを設計し、自社組織に組み込むための支援をしており、こうした活動を通じて顧客の持続可能なサイバーセキュリティ管理態勢構築に貢献することを目指しています。

KPMGのサイバーセキュリティサービスは、情報セキュリティ、事業継続、リスクマネジメント、プライバシー管理、フォレンジックの専門家を結集して提供するサービスです。これらのスキルを統合し活用することで、それぞれのクライアントが直面するサイバー攻撃の脅威に適合した戦略を策定できます。



KPMGのメンバーファームには以下の強みがあります。

●グローバル

KPMGは世界156ヵ国のメンバーファームに、計15万2000人を超える専門家を擁しています。世界中に、より深い専門知識を提供します。

●受賞歴

英国のKPMGは、2011年と2012年の2年連続で、SC Magazine Awards Europeの「最優秀情報セキュリティコンサルタント会社（Information Security Consultancy of the Year）」賞を受賞しています。また、「最優秀情報セキュリティプロジェクト（Information Security Project of the Year）」 部門でも、国際情報インテグリティ機構（International Information Integrity Institute [I-4]）に関し、高い評価を得ました。I-4は、世界各国の大企業で構成される世界屈指の情報セキュリティフォーラムです。

●サイバーセキュリティの課題を特定

KPMGのサイバーセキュリティサービス部門はI-4を通じて、世界の主要企業が現在あるいは将来的に直面するサイバーセキュリティ上の課題を共同で解決する支援を行っています。

●顧客に対する献身

KPMGのメンバーファームとクライアントとの関係は、効果的、効率的な解決策の提供のために長きにわたる努力と相互信頼の上に築かれたものです。KPMGの専門家は他では実現できないサービスを提供すべく、常に全力を尽くしています。

KPMGサイバーセキュリティアドバイザリーグループ

cybersecurity@jp.kpmg.com
kpmg.com/jp