KPMG Insight

KPMG Newsletter
July 2014

日本におけるサイバー攻撃の状況と課題
―サイバーセキュリティサーベイ2013から―

KPMG
cutting through complexity

Volume 7

日本におけるサイバー攻撃の状況と課題
―サイバーセキュリティサーベイ2013から―

KPMGサイバーセキュリティアドバイザリーグループ
株式会社KPMG FAS　フォレンジック部門
ディレクター　**伊藤　益光**

伊藤（いとう）　益光（ますみつ）
KPMGサイバーセキュリティ
アドバイザリーグループ
リーダー
株式会社KPMG FAS
フォレンジック部門
ディレクター

昨今、グローバルに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、漏洩、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喫緊の課題となっています。
このような状況を踏まえ、KPMGジャパンでは、サイバーセキュリティにかか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に、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。
本稿では、本調査結果から判明した日本におけるサイバー攻撃の状況と、欧米企業との比較から浮き彫りになった課題について解説します。

【ポイント】

- サイバー攻撃は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、そのうちの46%に実際の被害が生じている。
  - サイバー攻撃による実際の被害内容として「業務プロセスの中断」が最も多く（53%）挙げられている。
- サイバー攻撃の標的はシステムから人へ
  - 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。一方、海外では、58%が1,000万円未満、16%の企業が7,500万円以上の損失を被っている。
  - ITや情報セキュリティは、海外のトレンド（ソーシャル・エンジニアリングやフィッシング）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る。
- サイバー攻撃の防御におけるテクノロジーの限界
  - 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%にすぎない。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る。
  - 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が感じられる。

● サイバー攻撃の防御に取締役の関与が求められる
- 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%にのぼっている。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る。

I サイバー攻撃の発生状況

1. サイバー攻撃の試みを受けた経験

国内企業の24%が過去1年間にサイバー攻撃の試みを受けています（**図表1**参照）。業種別では情報・通信業および製造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（**図表2、図表3**参照）。

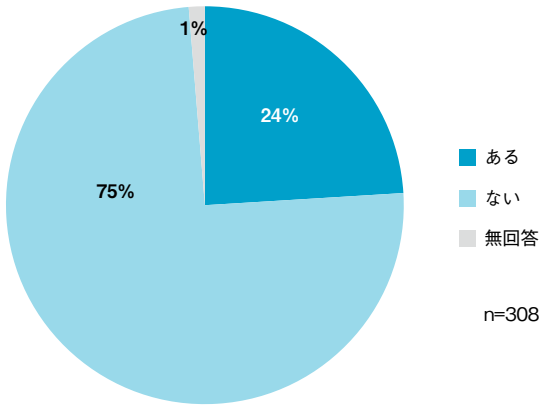
2. 攻撃手法（海外比較）

国内では、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が多く見受けられますが、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。いずれ日本も同じ傾向に進むことが予想されます（**図表4**参照）。

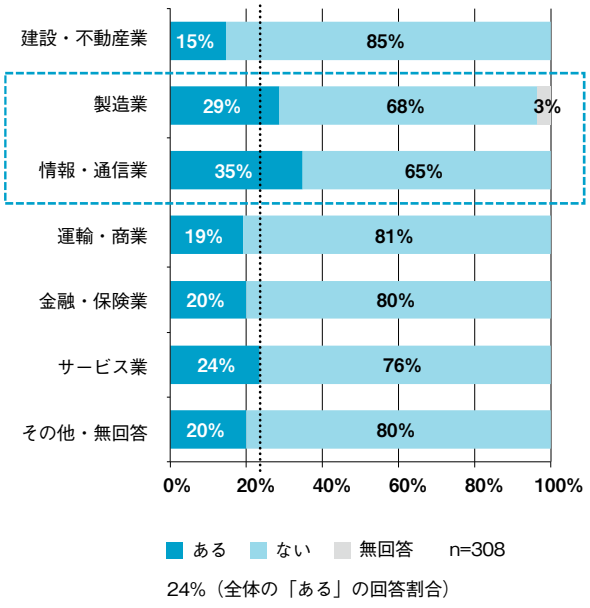
3. 被害発生回数

サイバー攻撃の試みを受けた国内企業のうち、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（**図表5**参照）。

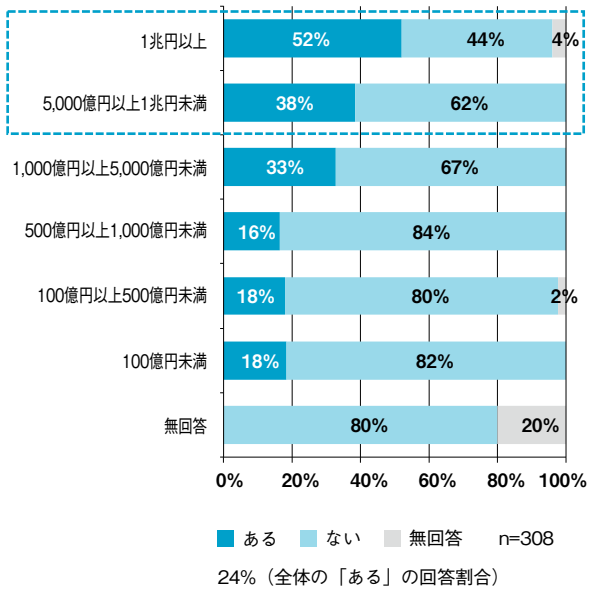
図表1　過去1年間にサイバー攻撃の試みを受けたことがあるか



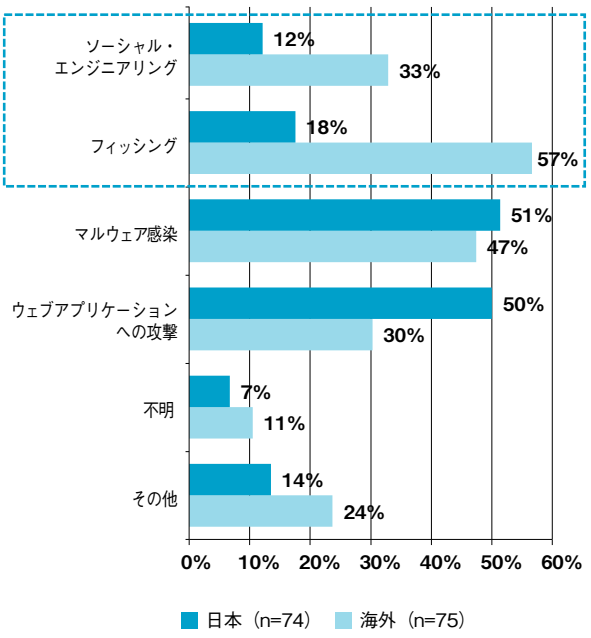
図表2　過去1年間にサイバー攻撃の試みを受けたことがあるか（業種別）



図表3　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）

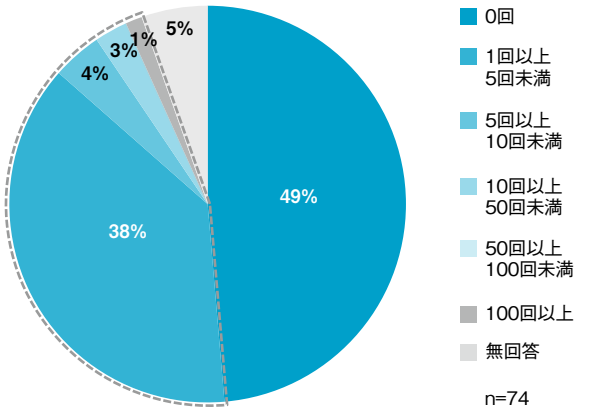


図表4　攻撃手法の海外との比較（複数回答）



※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。

図表5　被害が発生したのは何回くらいか

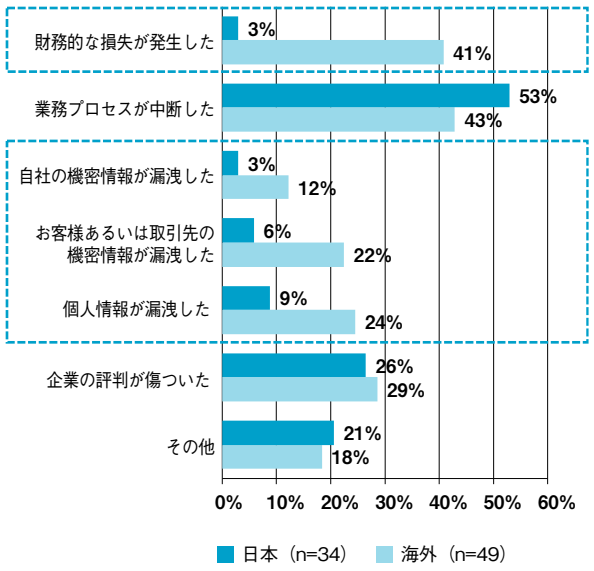


※サイバー攻撃の試みを受けたことがあると回答した企業が対象です。

4. 被害内容（海外比較）

過去1年間にサイバー攻撃の被害を受けた国内企業の58%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。一方、海外では、財務的な損失および情報の漏洩を挙げた企業の割合が日本を大きく上回っています（**図表6**参照）。

図表6　被害内容の海外との比較（複数回答）

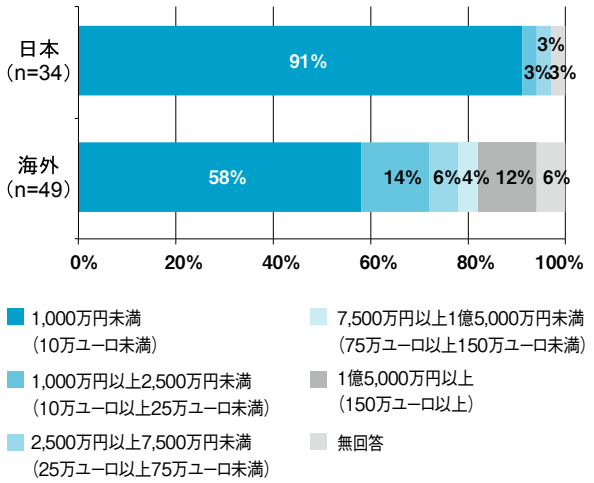


※サイバー攻撃の被害が1回以上発生したことがあると回答した企業が対象です。

5. 損失金額（海外比較）

過去1年間にサイバー攻撃の被害を受けた国内企業の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）以上の損失が発生したと回答しています（**図表7**参照）。

図表7　損失金額の海外との比較（複数回答）



1ユーロ＝140円で計算

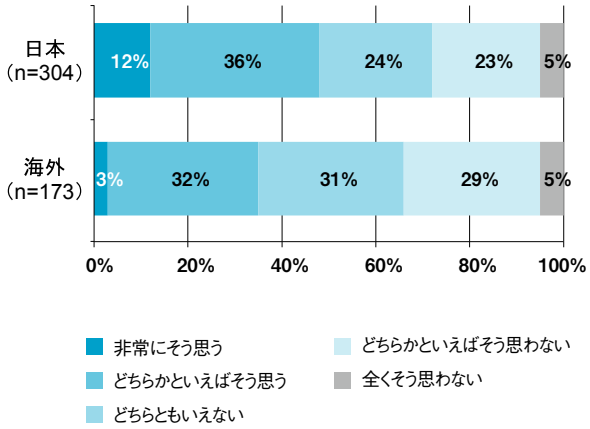
※サイバー攻撃の被害が1回以上発生したことがあると回答した企業が対象です。

Ⅱ サイバー攻撃に対する認識

1. サイバー攻撃の防御（海外比較）

国内企業では、48%がサイバー攻撃を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」）と考えています。一方、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（「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（**図表8**参照）。

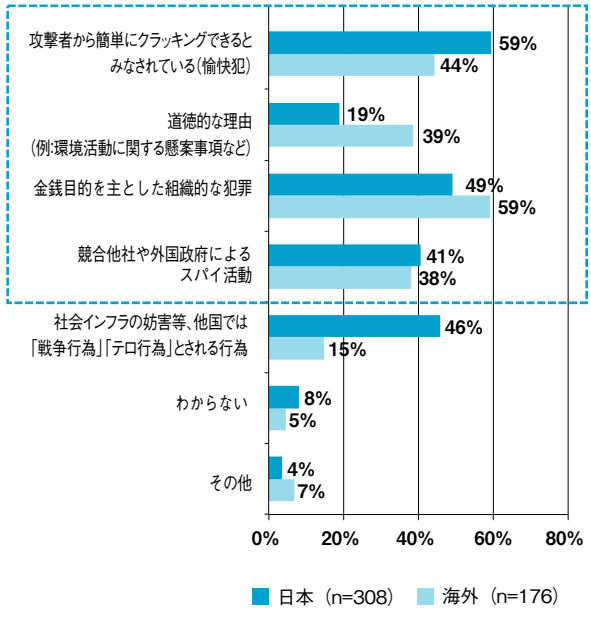
図表8　サイバー攻撃は防ぐことができない（海外との比較）



2. サイバー攻撃の動機（海外比較）

国内では、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。一方、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。ハクティビストと組織犯罪の活動が活発であることがうかがえます（**図表9**参照）。

図表9　サイバー攻撃の動機の海外との比較（複数回答）

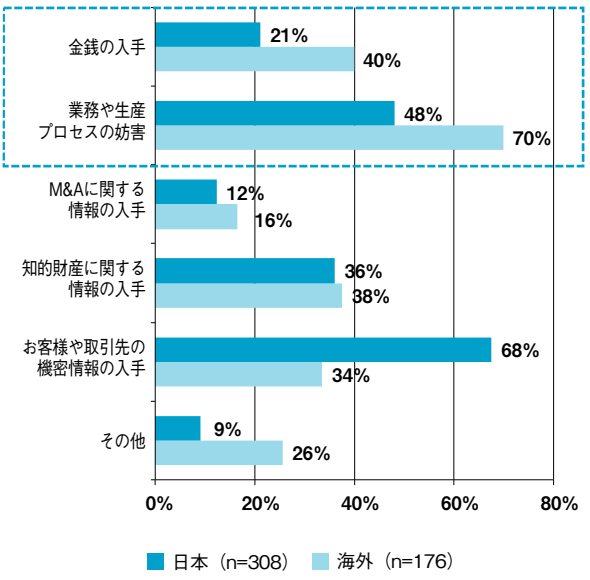


3. 自社が攻撃される理由（海外比較）

国内において、攻撃される理由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、「情報（知的財産、機密情報）の入手」を自社が攻撃される理由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」が主要な理由として挙げられています（**図表10**参照）。

図表10　自社が攻撃される目的の海外との比較（複数回答）



Ⅲ サイバー攻撃への対応状況

1. サイバー攻撃の予防

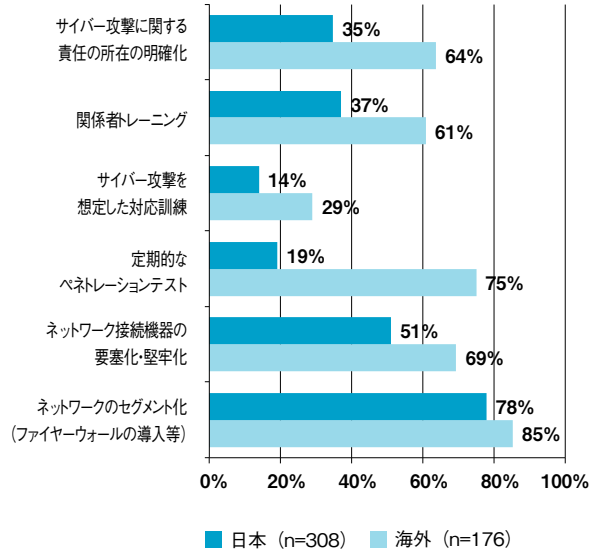
サイバー攻撃を予防するために、国内企業の78%が「ネットワークのセグメント化」を実施しています。「ネットワーク機器の要塞化・堅牢化」を行っている日本企業も51%近くに上ります。

一方、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（**図表11**参照）。

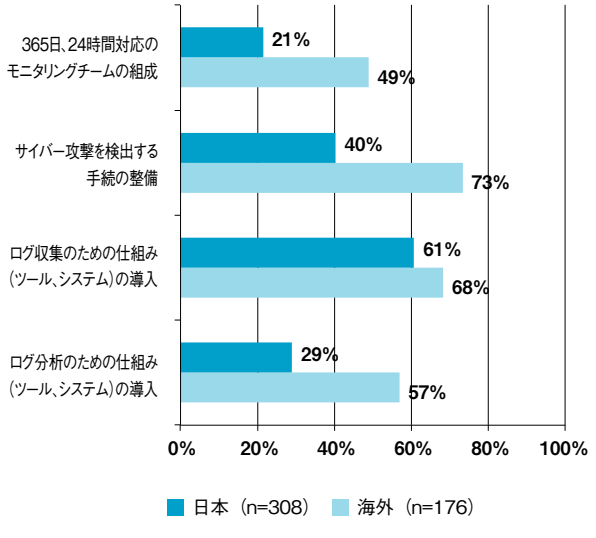
図表11　サイバー攻撃予防策の海外との比較（複数回答）



2. サイバー攻撃の発見

サイバー攻撃を発見するために、国内企業の61%がログ収集のための仕組みを導入していますが、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。

図表12　サイバー攻撃発見策の海外との比較（複数回答）



一方、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、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（**図表12**参照）。

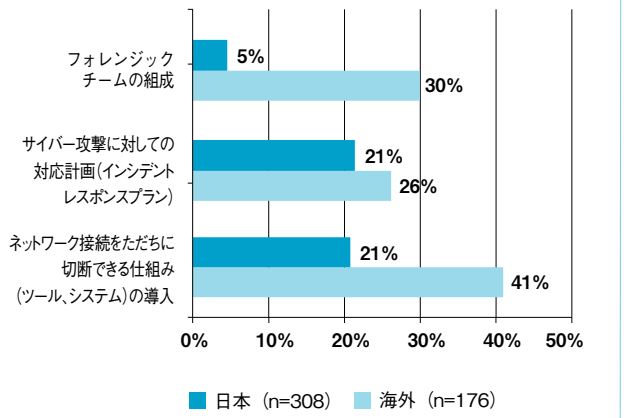
3. サイバー攻撃発見時の対処

国内企業において、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書（インシデントレスポンスプラン）」と「ネットワーク接続をただちに切断できる仕組み（ツール、システム）の導入」です。

一方、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。さらには海外では30%の企業が攻撃を受けた後の保全と分析のためのフォレンジックチームを組成しています。

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、その導入が進んでいない状況がうかがえます（**図表13**参照）。

図表13　サイバー攻撃対処策の海外との比較（複数回答）



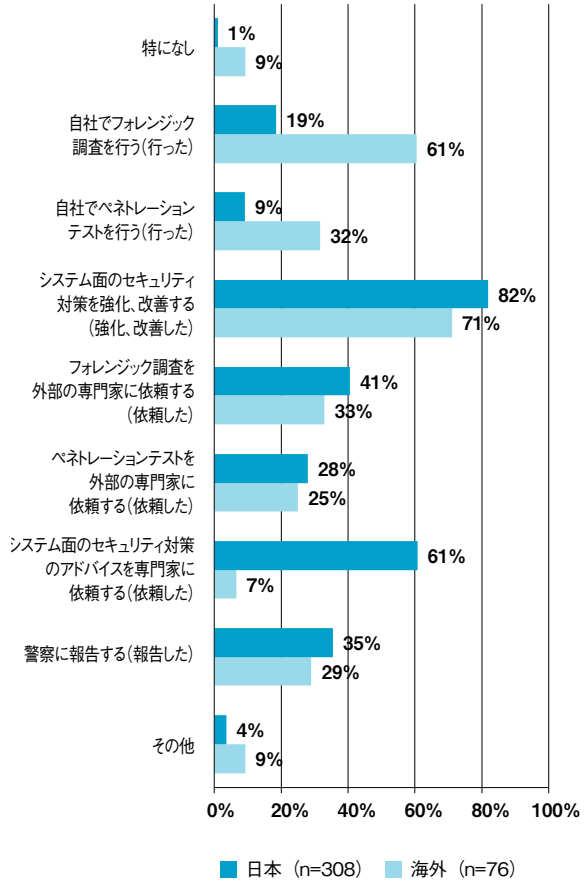
Ⅳ サイバー攻撃への今後の取組みに対する考え

1. サイバー攻撃を受けた場合の対応

国内企業において、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。

一方、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（**図表14**参照）。

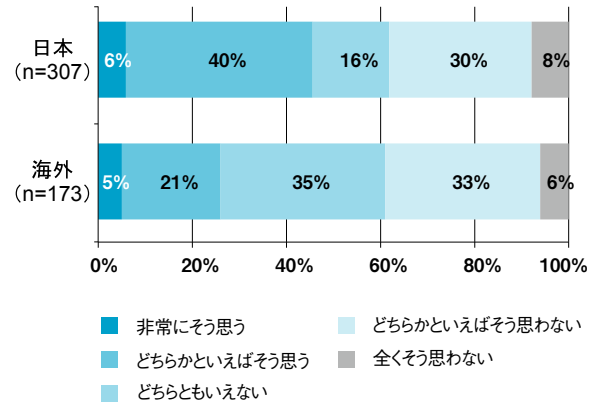
図表14　サイバー攻撃を受けた場合の対応の海外との比較（複数回答）



2. 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、国内企業の46%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、38%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。

図表15　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）



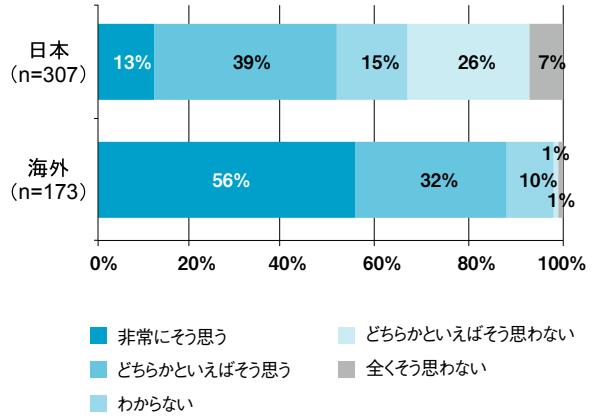
一方、海外で「そう思う」と回答した企業は26%にすぎず、テクノロジーによる防御の限界を感じている企業が国内より多い状況がうかがえます（**図表15**参照）。

3. サイバー攻撃の予防への取締役の関与

サイバー攻撃の予防への取締役レベルの関与について、国内企業の52%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。

さらに、国内企業の13%が「非常にそう思う」と回答いるのに対し、海外では56%の企業が「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（**図表16**参照）。

図表16　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）



V　おわりに

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。

本調査により、日本企業が欧米企業に比べ、注力している

分野、手法が異なることが判明しました。欧米で発生しているサイバー攻撃が遅れて日本にやってくる傾向があります。本調査を参考に自社のサイバーセキュリティ防御態勢を一度見直されると良いでしょう。

また、サイバーセキュリティ防御態勢の変革には、トップマネジメントの関与は必須です。これを機に、サイバーセキュリティは単にIT部門だけの問題ではなく、全社的な問題であるという認識をもっていただければ幸いです。

サイバーセキュリティサーベイ2013の全文をご希望の方は、下記の資料請求ページからお申込みくださいますようお願いいたします。
http://www.kpmg.com/jp/ja/knowledge/article/research-report/pages/cyber-security-survey-2013.aspx

KPMGサイバーセキュリティアドバイザリーグループ

サイバーセキュリティに関する防御態勢の診断からサイバー攻撃防御態勢の改善計画立案・高度化支援、グローバルな防御態勢への変革支援まで、業種に特有の課題に対応したサービスを提供いたします。
cybersecurity@jp.kpmg.com

【バックナンバー】
「サイバー犯罪の見通し ①」
（AZ Insight Vol.56 ／ Mar 2013）
「サイバー犯罪の見通し ②」
（AZ Insight Vol.57 ／ May 2013）

本稿に関するご質問等は、以下の者までご連絡くださいますようお願い致します。

株式会社 KPMG FAS
フォレンジック部門
ディレクター　伊藤　益光
TEL：03-5218-8837
masumitsu.ito@jp.kpmg.com

KPMGジャパン

marketing@jp.kpmg.com
www.kpmg.com/jp