KPMG
cutting through complexity

2014年4月

新たなITリスクに立ち向かう　連載シリーズ　第3回

サイバーセキュリティ

ー攻撃者に隙を見せない態勢づくりー

サイバー攻撃に端を発する被害のニュースが後を絶たない。ITは多くの企業活動において重要な位置を占めており、サイバー攻撃を受けた場合は、顧客や企業内に提供しているサービスの停止、機密情報の漏えい、風評被害等の大きな打撃を受けるであろう。しかしながら、サイバー攻撃に対して明確な対策を打っている企業は多くはない。

本稿では、「新たなITリスクに立ち向かう」の第3回目テーマとして、サイバーセキュリティについて述べていきたい。

1. サイバーセキュリティとは

サイバー攻撃は、標的のコンピュータやネットワークに不正に侵入し、機密情報を搾取、改ざん、破壊する。あるいは、標的のシステムに大量にデータを送りつけ機能不全に陥らせる。このような攻撃に対応するための防御態勢の維持が、サイバーセキュリティといえる。

どのようなリスクであっても、現状把握、必要な対策の導入、対策実施やモニタリング等の態勢整備と維持が必要であり、サイバー攻撃についても同様である。セキュリティにかかるリスクについては、すでにCISO（Chief Information Security Officer）を任命し、情報システム部門を主導とした管理態勢を整備している企業もあることだろう。ただし情報システム部門の管理外のシステム、たとえば、生産システム、プラントシステム、運行システム等の制御系システムについては、他のシステムとの接続がなく利用者が限定されるため、攻撃の対象とならずリスクが低い等の理由で、管理態勢の対象外となっている場合がある。

しかしながら、企業のシステム環境は変化しており、上記の前提が覆っている可能性がある。企業活動において重要な全てのシステムを対象に、サイバー攻撃のリスクを正しく把握し対策を打つ態勢を取らなければ、サイバーセキュリティは実現できない。また、技術や環境の変化に従い攻撃も変化していく。この変化をいち早くとらえ、早期に対応していかなければならない。

2. サイバー攻撃の実態

KPMGでは、2013年10月、国内の上場企業と売上高500億円以上の未上場企業を対象に、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た。この調査結果[1]と、各省庁の公表資料等からうかがえる、昨今のサイバー攻撃の実態を一部紹介する。

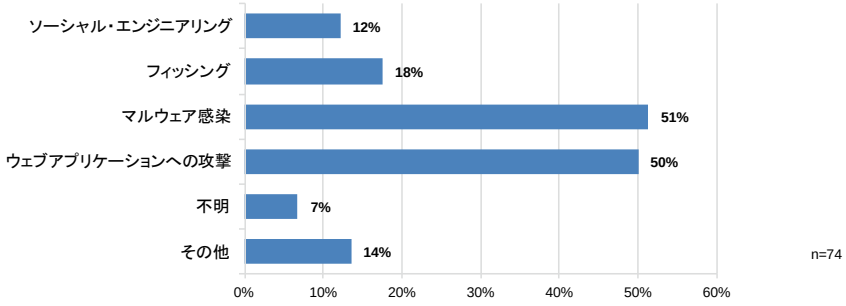
(1) 攻撃手法

攻撃の手法は、より巧妙なものに変化している。警察庁の広報資料「平成25年中のサイバー攻撃の情勢及び対策の推進状況について」(平成26年2月27日)[2]によると、企業を対象とした標的型メール攻撃の手法は、同様の文面を多数の攻撃対象に送付する「ばらまき型」から、対象企業や人を特定し、メールを数度やりとりして信用させたうえで不正プログラムを送付する「やりとり型」に移行している。さらに、送付される不正プログラムは、何重もの暗号化やファイルサイズの縮小等を組み合わせ、ウイルス対策ソフトによる検知や動作解析を困難にしたものが増えている。標的型メール攻撃以外にも、対象企業の従業員が頻繁に閲覧するウェブサイトを改ざんし、閲覧したコンピュータに不正プログラムを自動的に感染させる「水飲み場型攻撃」が、平成25年に国内で初めて確認された。

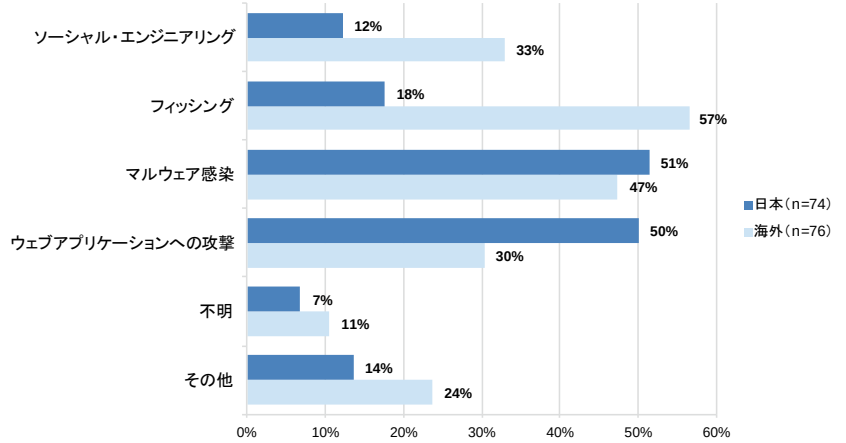
また、国内外の攻撃手法に違いがみられる。KPMGの調査によれば、国内では、サイバー攻撃の試みを受けた企業の半数は、マルウェア感染やウェブアプリケーションへの攻撃といった、システムに対する攻撃を主に受けている。一方、国外においては、ソーシャル・エンジニアリングやフィッシング等の、人にアプローチする攻撃が主流となっている。ITについては海外のトレンドが数年遅れで日本に到来する事例も多いことから、今後、日本においても攻撃の標的がシステムから人へシフトしていくことが懸念される。

【図表1】攻撃手法について

攻撃手法はどのようなものであったか(複数回答)



攻撃手法の海外との比較(複数回答)



*「過去1年間にサイバー攻撃の試みを受けたことがある」と回答した企業を対象にアンケートを行った結果

1 「サイバーセキュリティサーベイ2013」(KPMGサイバーセキュリティ アドバイザリーグループ)
http://www.kpmg.com/jp/ja/knowledge/article/research-report/Pages/cyber-security-survey-2013.aspx

2 平成25年中のサイバー攻撃の情勢及び対策の推進状況について(平成26年2月27日、警察庁)
https://www.npa.go.jp/keibi/biki3/260227kouhou.pdf

（2） 被害内容

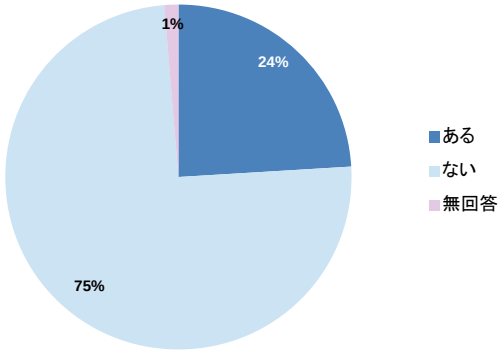
KPMGの調査によれば、過去1年間にサイバー攻撃の試みを受けたことがある企業は、全体の24%であった。業種別では、情報・通信業および製造業が多い。国内では、被害金額が1,000万円以下であった企業が9割以上であり、7,500万円以上の損失が発生したと回答した企業はなかった。しかし、海外においては、7,500万円以上の損失があった企業が16%であった。

国内における被害は、「業務プロセスの中断」が1番多く、5割超の企業で発生しているが、「お客様あるいは取引先の機密情報漏えい」「個人情報漏えい」が発生した企業はそれぞれ1割以下である。一方で、自社が攻撃される目的として何が認識されているかの調査結果では、国内では7割以上の企業で「お客様あるいは取引先の機密情報の入手」が認識されている。この結果から、機密情報保護への認識は高く対策が打たれているものの、業務継続に対する対策は比較的甘いことがうかがえる。

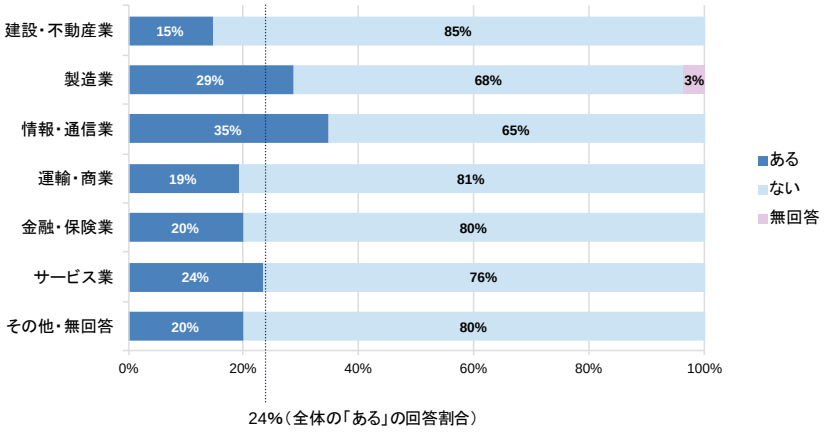
海外における被害は、「業務プロセスの中断」「財務的な損失発生」と回答した企業がそれぞれ4割以上であった。他に、「お客様あるいは取引先の機密情報漏えい」「個人情報漏えい」と回答した企業がそれぞれ2割以上であり、国内より大きくなっている。海外では、攻撃の目的を「業務プロセスの中断」であると考えている企業が多く、「お客様あるいは取引先の機密情報の入手」を挙げる企業は国内に比べ少ない。

【図表2】サイバー攻撃の試みを受けた経験

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

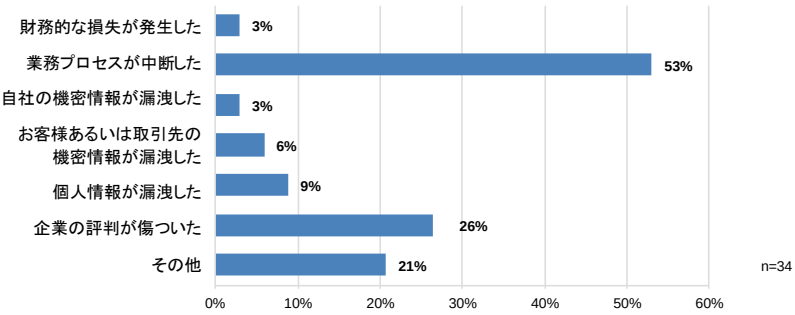


過去1年間にサイバー攻撃の試みを受けたことがあるか（業種別）

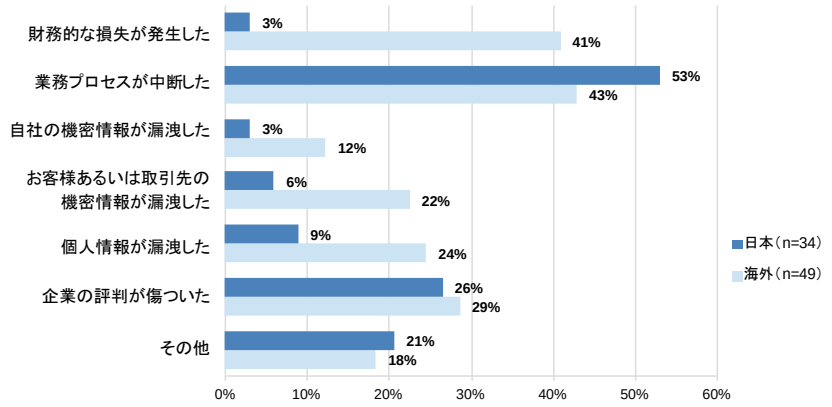


【図表3】被害内容

どのような被害が発生したか（複数回答）



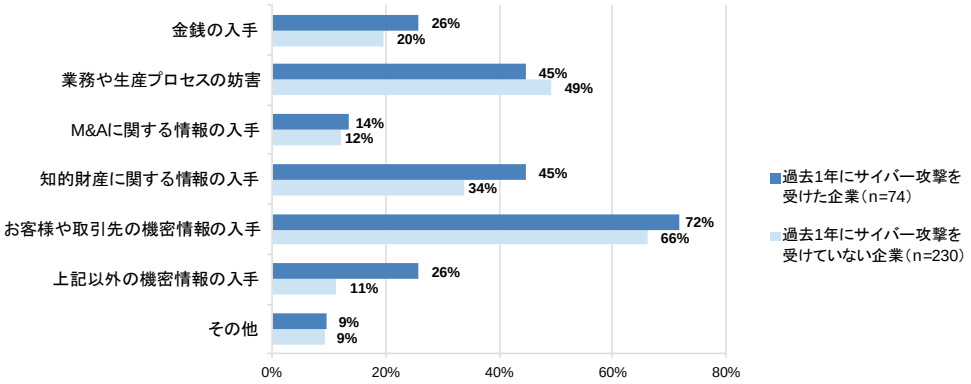
被害内容の海外との比較（複数回答）



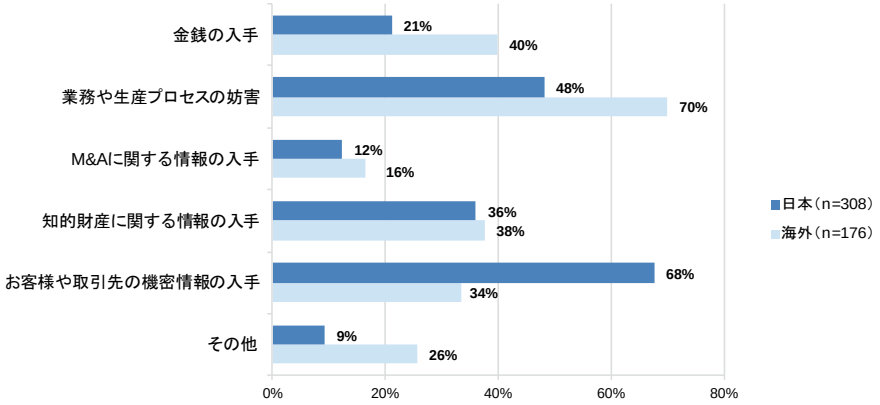
*「過去１年間にサイバー攻撃の試みを受けたことがある」「サイバー攻撃の被害が1回以上発生したことがある」と回答した企業を対象にアンケートを行った結果

【図表4】自社が攻撃される目的

自社が攻撃される目的（複数回答）



自社が攻撃される目的の海外との比較（複数回答）



*「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」の設問に回答した企業を対象にアンケートを行った結果

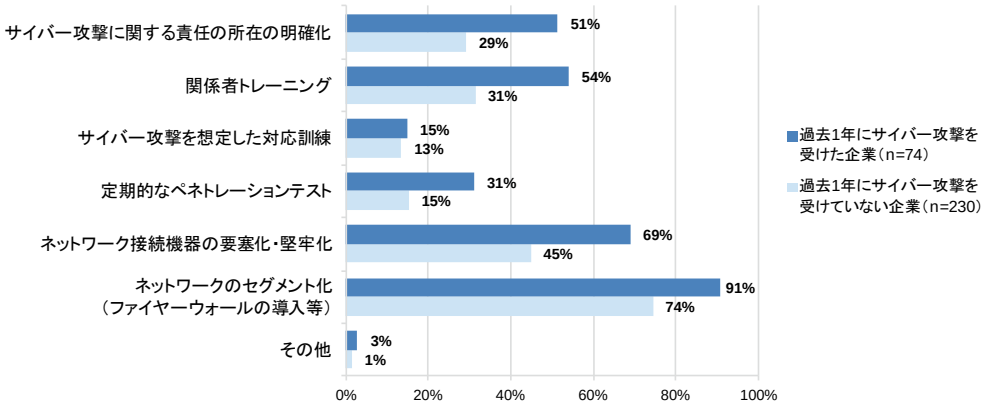
（3） 企業が実施している対策

KPMGの調査は、現在実施している体制面および技術面の対策を、複数の選択肢から選んでいただく方法をとった。この結果、ネットワークのセグメント化やネットワーク機器の堅牢化を挙げている企業が多かった。国内外ともに、体制面よりも技術面の対策がやや優先されている。

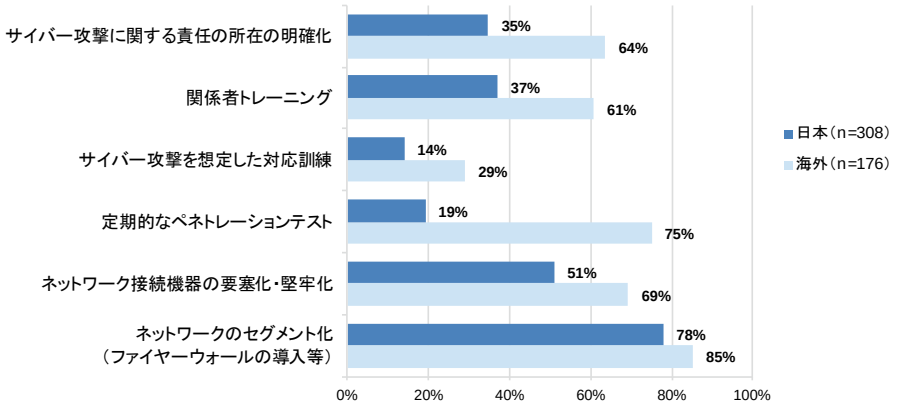
攻撃手法が人の錯誤を利用したものに変わってきている昨今、技術面の対策は必須であるものの、それだけに留まらない対策が必要であることがうかがえる。

【図表5】サイバー攻撃の予防

サイバー攻撃をどのように予防しているか（複数回答）



サイバー攻撃予防策の海外との比較（複数回答）



*「過去1年間にサイバー攻撃の試みを受けたことがある」と回答した企業を対象にアンケートを行った結果

3. サイバーセキュリティを実現するために

ここまでで述べてきたように、攻撃手法の変化やリスクと対策のずれなどに継続的に対応していくために、企業は以下を実施しなければならない。

（1） セキュリティマネジメント態勢の見直し

これまで、情報システム部門を主導とした情報セキュリティ管理態勢を構築してきた国内企業は、顧客や取引先情報の機密性や完全性に着目し、情報系や基幹系等と分類されるシステムに保管される情報の保護を行い、一定の効果をあげてきていることがうかがえる。しかし、可用性が求められる情報・通信業や製造業における制御監視や生産システムについてはどうだろうか。これらのシステムは、企業の情報システム部門の管理下にないことが多く、十分なリスク評価や対策検討ができていないケースもある。

また、海外展開している企業では、国によるリスクの違いを考慮した現状把握ができていない可能性がある。

企業にとって保護すべきシステムは何か、直面しているリスクは何かを再度見直し、漏れのない対策をとるセキュリティ態勢を整備することが重要である。

制御監視や生産システムのセキュリティについては、管理体制やセキュリティ技術に関するさまざまな基準が策定されている。また、日本においては、制御システムを利用する事業者に対するセキュリティマネジメントの要求事項を規定した国際規格IEC62443-2-1をもとにしたCSMS（Cyber Security Management System）認証スキームの確立を目指している[3]。制御監視や生産システムをもつ企業は、このような基準を参考にして態勢整備をしていくことも考えられる。

（2） 継続的な従業員教育および関係者のセキュリティ意識向上

刻々と変化しているサイバー攻撃に対応できる人材を育成することが必要である。システムの脆弱性をついてくる攻撃に対応するためには、システムの企画開発を行う技術者への教育が必要であり、人の錯誤を利用した攻撃に対応するためには、システム利用者の意識付け教育が必要になる。システム利用者には、顧客や業務委託先等、企業が管理するシステムにアクセスする従業員以外の関係者が含まれるかもしれない。セキュリティホールになりうる関係者がどこにいるのかを明確にし、セキュリティの意識付けをする必要がある。

（3） トップのコミットメント

サーバー攻撃に関するリスク評価や対策、および人材育成に関する投資は、トップによるリスクの理解と意思決定をなくしては実現できない。また、トップのコミットメントがなければ、サイバーセキュリティに対する各部門の意欲や重要性の理解が損なわれ、態勢の維持はできない。経営層は、企業が直面しているリスクとしてサイバー攻撃を認識し、サイバーセキュリティに関与することが必要である。

KPMGビジネスアドバイザリー株式会社
シニア　小寺　くれは

3 制御システムセキュリティの認証スキーム確立に向けたパイロットプロジェクトに着手（2013年3月6日、独立行政法人情報処理推進機構　技術本部セキュリティセンター）https://www.ipa.go.jp/security/fy24/reports/ics_sec/index.html

*掲載の図表は全て「KPMGサイバーセキュリティサーベイ2013」（KPMGサイバーセキュリティアドバイザリーグループ）より引用

KPMGビジネスアドバイザリー株式会社

東京本社
〒100-0004
東京都千代田区大手町1丁目9番7号
大手町フィナンシャルシティ　サウスタワー
TEL ： 03-3548-5305
FAX ： 03-3548-5306

名古屋事務所
〒451-6031
名古屋市西区牛島町6番1号　名古屋ルーセントタワー
TEL ： 052-571-5485

www.kpmg.com/jp/ba