2018 年 8 月 28 日

損害保険ジャパン日本興亜株式会社
ＳＯＭＰＯリスケアマネジメント株式会社
トレンドマイクロ株式会社

「セキュリティインシデントに関する被害コスト調査」を発表

～社外からの通報で発覚したインシデントの場合、対外的な対応コストがかさむ傾向に～

損害保険ジャパン日本興亜株式会社（本社：東京都新宿区、社長：西澤　敬二、以下「損保ジャパン日本興亜」）とＳＯＭＰＯリスケアマネジメント株式会社（本社：東京都新宿区、社長：布施　康、以下「ＳＯＭＰＯリスケア」）、トレンドマイクロ株式会社（本社：東京都渋谷区、代表取締役社長 兼 CEO：エバ・チェン、東証一部：4704、以下「トレンドマイクロ」）は、民間企業における情報システム・セキュリティに関する意思決定者を対象に、事業継続を脅かすサイバー攻撃および内部犯行による対応コストへの影響を明らかにする「セキュリティインシデント※に関する被害コスト調査」を実施しました。

※セキュリティインシデントとは、サイバー攻撃や内部犯行によって発生する事故のことです。

１．背景

セキュリティインシデントに対する被害が年々深刻化するなかで、高額の対応コストが発生するサイバー攻撃や内部犯行といったセキュリティインシデントが顕在化しています。このような背景をふまえ、セキュリティインシデントにおける具体的な対応コストの実態を把握する目的で、損保ジャパン日本興亜とＳＯＭＰＯリスケア、トレンドマイクロの３社は「セキュリティインシデントに関する被害コスト調査」を実施しました。

２．調査結果

今回の調査では民間企業における情報システム・セキュリティに関する意思決定者、意思決定関与者 1,745 名を対象に調査を実施しました。その結果、全体の 43.9%を占める 766 名が、2017 年 1 年間に被害額の発生する何かしらのセキュリティインシデントを経験していることが分かりました。

・セキュリティインシデントの発覚が「社外からの通報」の場合、対外的な対応コストが増加

セキュリティインシデントにおける対応コストを「対外的コスト」と「対内的コスト」に分類して見てみると（図 1）、外部機関や顧客といった「社外からの通報」によりインシデントが発覚した場合、事業継続に必要な機器の調達や社告、コールセンター開設・増設などの対外的コストが全体の 59.0%を占めることがわかりました（図 2）。一方、社内のセキュリティ業務や社員からの連絡といった「社内からの通報」で発覚した場合には、対応コスト全体に占める対外的コストの割合は 44.7%にとどまっており 14.3 ポイントの大幅なひらきがあることが分かりました。

「対外的コスト」の中で全体コストに占める割合が最も大きくひらいたのは「謝罪文作成・送付費用」であり、「社外からの通報」の場合には 9.4%、「社内からの通報」の場合には 5.0%と約 2 倍近いひらきがありました。

社外からの通報で発覚するセキュリティインシデントは、個人情報漏洩などの深刻かつ顧客や取引先への直接的な影響が高いものと考えられることから、企業の説明責任やブランド・信頼の回復といったような企業存続に向けたコストがかさむものと推測されます。セキュリティリスク自体や対外的コストを低減するためにも、サイバー攻撃や内部犯行の兆候を早期に特定できるセキュリティ対策が重要であると考えられます。

対外的コスト	対内的コスト
•営業継続費用	•外部調査機関への調査依頼費用
•社告費用	•システム復旧費用
•コールセンター開設・増設・増員費用	•データ復旧費用
•謝罪文作成・送付費用	•再発防止案策定費用
•お詫び品・金券調達・送付費用	•再発防止策導入費用
•争訟費用	•利益損害
•損害賠償金	•その他

図 1：インシデント対応コスト一覧

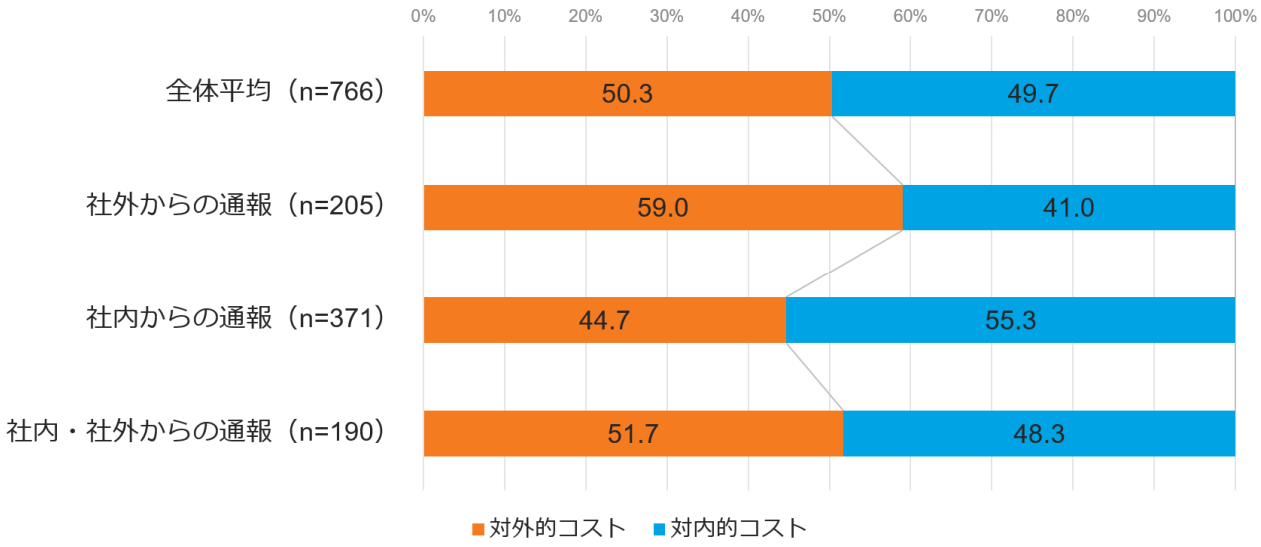

図 2：発覚事由別被害コスト割合　（N=766）

・サイバー攻撃はシステム関連コスト、内部犯行は情報漏洩・消失関連コストに影響

セキュリティインシデントを「サイバー攻撃」と「内部犯行」に分類し、それぞれにかかった対応コストを調べたところ、サイバー攻撃の場合には内部犯行に比べて「営業継続費用」が+9.1 ポイント、「システム復旧費用」が+3.9 ポイントと大きな差が出ていました。サイバー攻撃の場合には、システムの調達や復旧に関連した費用割合が大きくなる傾向が分かりました。

一方で内部犯行の場合には、サイバー攻撃に比べて「お詫び品・金券調達・送付費用」で+4.3 ポイント、「データ復旧費用」で+2.2 ポイントと、情報漏洩や情報消失に関連した対応コストの割合が膨らむ傾向にあることが分かりました。

最悪な事態が発生した際には、様々な対応コストを計上する必要性が出てくることから、企業はサイバー攻撃や内部犯行といったリスクによってもたらされる損害を想定し、対策を強化する必要があります。

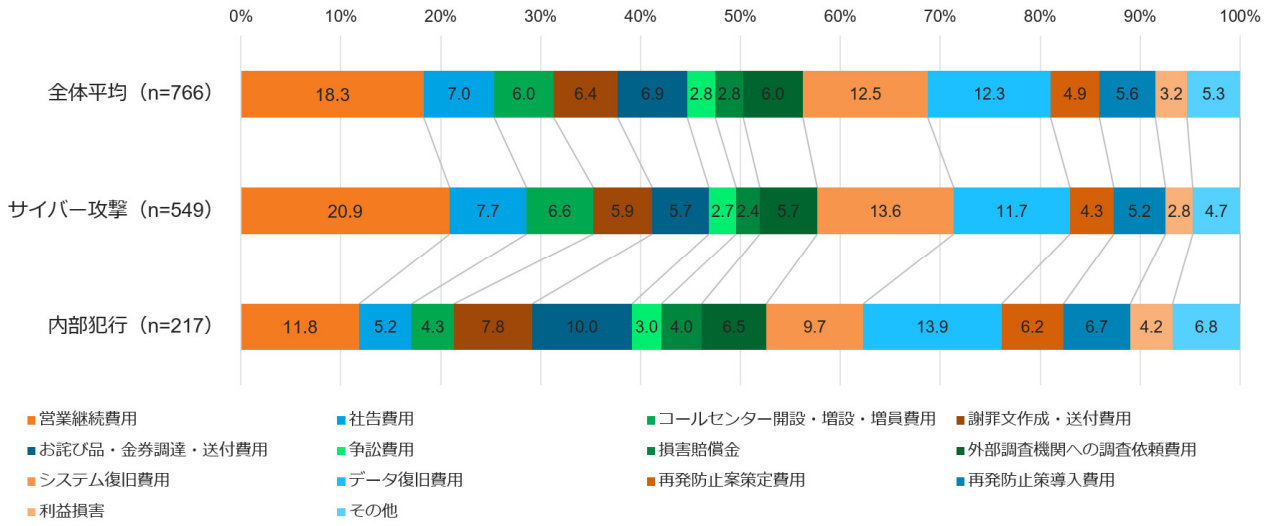

図 3：インシデント別被害コスト内訳　（N=766）

・依然として進まないセキュリティ対策

ネットワーク、エンドポイントといった領域での技術的対策や、経営リスクとしての認識・体制整備といった組織的対策を含め、組織のセキュリティ対策を25項目・5段階の対策レベルで調査しました。これらの設問は、サイバー保険加入時にお客様へ記入いただく告知書の確認事項をベースに作成したものです。

その結果、最も対策が進んでいる「対策レベル5」に属する企業は全体のわずか16.0%に留まることが分かりました。一方で対策の進んでいない「対策レベル2」と「対策レベル1」に属する企業は全体の56.7%となっており、過半数を占める企業においてサイバー攻撃や内部犯行といったリスクを低減させる対策が不十分であることが分かりました。今回の調査から、セキュリティ対策が最も進んでいる対策レベル5に属する組織においても、セキュリティインシデントの平均対応コストは約1億7,600万円になることが明らかになっており、被害を見据えた上での対策も重要なポイントになります。

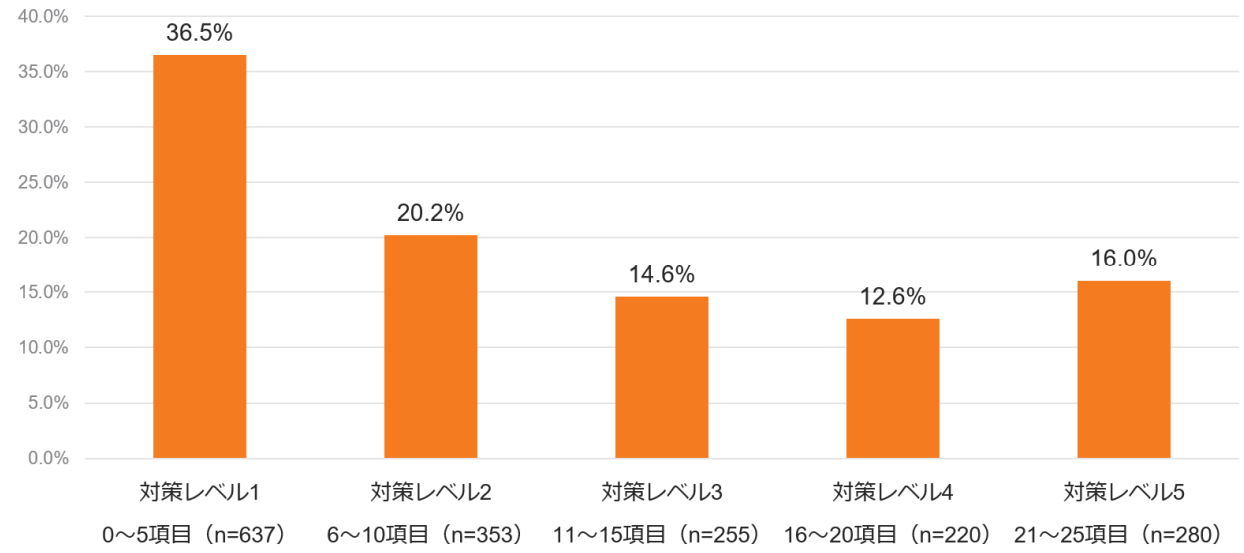

図 4：セキュリティ対策項目実施割合（N =1,745）

技術・組織の両面で包括的にセキュリティ対策を実施することは、サイバー攻撃や内部犯行のリスクを緩和させると同時に、有事の際に発生するコストをリスク移転する上での手段となるサイバー保険契約の締結においても重要なポイントになります。脅威によるリスクを緩和し、対応コストにともなうダメージを最小限に止めるためにも、企業としての全方位的なセキュリティ対策は不可欠となります。

３．今後について

損保ジャパン日本興亜、ＳＯＭＰＯリスケア並びにトレンドマイクロは、これまで培ってきたセキュリティ分野における様々な独自のデータや知見を活用して、今後のサービス開発・拡充を実施することで、顧客の課題解決に向けて取り組んでまいります。

＜調査概要＞

■調査名：「セキュリティインシデントに関する被害コスト調査」
■調査実施期間：2018 年 4 月
■回答者：日本在住で民間企業における情報システム・セキュリティに関する意思決定者、
意思決定関与者 1,745 名
■調査方法：インターネット調査

以上