セキュリティ成熟度と被害の実態 2023

～CIO Lounge×トレンドマイクロ共同調査～

詳細版

2024年1月
トレンドマイクロ株式会社

目次

はじめに 03

01 エグゼクティブサマリー 05

02 セキュリティ成熟度 06

・全体傾向
・「経営層の関わり」と「セキュリティ成熟度」の関係
・「従業員規模」と「セキュリティ成熟度」の関係
・海外拠点の「セキュリティ成熟度」
・「セキュリティ成熟度」向上に向けた課題
・被害組織が「強化しておくべきだった」と感じた機能
・「セキュリティ成熟度」向上のきっかけ

03 サイバー攻撃被害の実態 12

・サイバー攻撃による被害額の累計
・「最も被害コストの大きかったサイバー攻撃」
・「最も被害コストの大きかったサイバー攻撃」の種類別被害コスト
・「最も被害コストの大きかったサイバー攻撃」のコスト内訳
・「最も被害コストの大きかったサイバー攻撃」で生じた業務停止期間
・大きな被害をもたらす「ランサムウェア攻撃」
・国内組織も無視できない「BEC」の脅威

04 サイバー攻撃被害に遭いやすい組織の特徴.....22

・「従業員規模」と「被害コスト」の関係
・「セキュリティ成熟度」と「業務停止期間」の関係
・「インシデントの発生地点」と「業務停止期間」の関係
・「侵入から検知までにかかった時間」と「業務停止期間」の関係

まとめ.....25

発行
特定非営利活動法人 CIO Lounge
Trend Micro 株式会社

執筆者
Trend Micro Research

はじめに

事業の安定稼働のため、ひいては顧客との信頼関係醸成のためにも、サイバーセキュリティ対策は企業にとって欠かせない活動のひとつです。サイバーセキュリティ運用の現場は、日々高度化するサイバー攻撃と戦っています。組織のセキュリティ責任者にとって「自社のセキュリティレベルが十分な水準にあるのか」を見極めることは、今まで以上に重要な課題となっています。そこで2023年6月、トレンドマイクロ株式会社は特定非営利法人CIO Loungeの監修のもと、国内の法人組織を対象とした「セキュリティ成熟度と被害の実態調査 2023」を実施しました。本調査では、実際にサイバー被害に遭った組織における「被害規模」と「セキュリティ成熟度」の関係を読み解きます。「被害規模」と「セキュリティ成熟度」を相関的に分析することで、組織の特徴やセキュリティ対策状況の統計的な傾向を明らかにします。その傾向から、組織にとって有効なサイバー被害低減策を提示します。

本レポートは、2023年10月に発行したレポート「セキュリティ成熟度と被害の実態 2023 ～CIO Lounge×トレンドマイクロ共同調査～ サマリー版」に、より詳細なサイバー攻撃被害の分析結果を追記したものです。追記項目には、ランサムウェアやビジネスメール詐欺などの個別の脅威に関する被害の分析や、海外拠点の「セキュリティ成熟度」の分析などが含まれています。本レポートにより、組織のセキュリティ責任者はサイバー被害の詳細を把握することができ、自組織のセキュリティ戦略の立案を行う上での参考値を得ることができます。

調査概要

- 調査名：セキュリティ成熟度と被害の実態調査 2023
- 調査対象：305名（以下の条件をすべて満たす個人を抽出）
  - I. 過去3年以内にサイバー攻撃による被害を受けた法人組織に所属
  - II. 従業員500名以上の法人組織に所属
  - III. 経営管理・BCP策定・DX推進・情報資産管理・セキュリティ関連業務に携わる、部長職以上の責任者
- 役職別内訳：経営者:3、役員級:58、本部長級:45、部長級:199
- 組織規模別内訳：500~999人:48、1,000~2,999人:74、3,000~4,999人:40、5,000~9,999人:39、10,000~19,999人:34、20,000人以上:70
- 調査時期：2023年6月
- 調査方法：インターネット調査

本レポート記載の主要用語

- **セキュリティ成熟度**：アメリカ国立標準技術研究所(NIST)の提唱するサイバーセキュリティフレームワーク v1.1(以下NIST CSF)[1]に規定される5つの機能「識別」「防御」「検知」「対応」「復旧」について、それぞれ5つの設問を設定し、全25問から各社の対策状況に応じてスコアを算出したもの。対策状況は0:「全くできていない」、1:「会社が定める正式手順はなく、個人の裁量で取り組んでいる」、2:「会社が定める正式手順に沿って、部分的に取り組みが行われている」、3:「会社が定める正式手順に沿って、包括的に取り組みが行われている」、4:「会社が定める正式手順に沿って、包括的に取り組みが行われており、定期的な改善を図っている」の5段階でスコアを測定。

- **最も被害コストの大きかったサイバー攻撃**：過去3年間に回答者組織が受けたサイバー攻撃の内、最も直接、復旧、再発防止などのコストがかかったインシデント。

- **直接・復旧・再発防止コスト**：サイバー攻撃被害によりもたらされるコストの内、身代金支払いや業務停止期間の売り上げなど、攻撃そのものによってもたらされる、主には金銭的なコストを”直接コスト”、攻撃を受けてからの調査・封じ込めなどの対応、システム復旧などに必要な、主には人的コストを”復旧コスト”、被害を受けた後の今後の再発防止や被害低減に向けた様々な施策・活動・投資などの中長期的コストを”再発防止コスト”として設定

- **経営層の関わり**：セキュリティに対する経営層の業務上の関与状況を示す。関与の具体的な事項として「セキュリティ業務に関する報告」、「セキュリティ対策へのリーダーシップの主導」、「経営会議でのセキュリティリスクの取扱い」、「セキュリティに関する予算等分配指示」の4つの実施状況を設定し、調査の中ではそれぞれ0:「全く実施されていない」、1:「必要に応じて実施されている」、2:「定期的に実施されている」の3段階でスコアを測定している。

- **経営層の関わり大・中・小**：経営層の関わりの4つの実施状況スコアの平均値を取得し、小＝0～1.49(119サンプル)、中＝1.5～1.99(53サンプル)、大＝2(131サンプル)で分類したもの。相関分析の際の分類条件として使用。

[1] https://www.ipa.go.jp/security/reports/oversea/nist/ug65p90000019cp4-att/000071204.pdf

特定非営利活動法人 CIO Loungeについて

急速に変化・進展しているIoTやAI等に代表されるICT技術をいかに経営に取込み、企業活動を伸長させるかが企業の課題となっています。この課題に対し、経営幹部層・CIO及びIT部門責任者は、どう対応していくかの悩みをかかえているのが現状です。

そこで、大手企業でCIO及びIT部門責任者としてこれら課題に先進的に対応してきたメンバーが集い、各人の経験・知識を利用することで、悩みを抱える企業の経営幹部層・CIO及びIT部門責任者の相談相手となり、解決への糸口を見出し、情報化社会の発展を図る活動に寄与すること及び最新のICT技術活用普及促進による科学技術の振興を図る活動、更には各企業へのコンサルティング活動・各種セミナー開催・次世代CIO育成等を通じた経済活動の活性化を図る活動を目的としてCIO Loungeを立ち上げました。

任意団体では企業に対する信頼性が低いこと、その設立趣旨から、広く支援を受けつつ中立的な団体であり続けることから、特定非営利活動法人を設立し活動しています。「企業の経営者と情報システム部門の架け橋」、「企業とベンダーとの架け橋」を進め、企業の効率的な成長を支援させていただきます。

https://www.ciolounge.org/

理事長　矢島孝應

1. エグゼクティブサマリー

本章では、今回の調査結果での特筆すべき点や推奨事項を取り上げます。法人組織は、本調査結果をもとに自組織に合ったセキュリティ強化を検討することをお勧めします。また、本レポートの数値結果をベンチマークとして、自社の「セキュリティ成熟度」を定期的に計測することも有効です。

調査から見られた5つのポイント

調査から様々なサイバー攻撃被害の傾向、攻撃の特徴、被害企業のセキュリティ対策状況などの情報が得られました。中でも特筆すべき点は以下の5点です：

I. 被害低減に向けた指標として「定期的なセキュリティ成熟度の計測」が有用。

「セキュリティ成熟度」が高いほど「サイバー攻撃による業務停止期間」が短いという統計的な傾向が見られました。これは、言葉だけ聞けば一見当たり前の結果ではあるものの、NIST CSFなどを基準とした「セキュリティ成熟度」の計測が被害低減に向けた確かな指標であるということが、再現性を持つデータとして示されたことが重要な点です。継続的な「セキュリティ成熟度」の計測が、成果の見えにくいセキュリティ対策の有意性を数値として確認できることが示されました。

II. 「資産の棚卸やリスク管理」「インシデント時の対応計画準備」の優先的な実行が有効。

多種多様なセキュリティ対策の中から、まず何に手を付けるべきかの優先度の決定が難しいということも、多くの企業が抱える課題のひとつです。被害の大きかった組織と小さかった組織では、特にNIST CSFの「識別」（資産の棚卸やリスク管理）や「対応」（インシデント時の対応計画準備）における成熟度の差が大きかったことから、まずはそれらの対策を組織的に実施することが重要です。

III. 経営層がセキュリティリスクとその対策方法に関して説明責任を負うことがセキュリティ成熟度向上のカギ。

「セキュリティ成熟度」と「経営層の関わり」の間に強い相関が見られました。セキュリティは組織包括的な対応を継続的に実施する必要があるため、組織横断的な指示や長期的取り組みを実現しやすい「経営層の関わり」の影響が大きかったことが考えられます。これは経営層がサイバーセキュリティを経営リスクとして認識し、対策を主導することが、「セキュリティ成熟度」向上に向けて必須の事項であることを示しています。

IV. 「自社で行うセキュリティ業務の整理」と「必要な人材像とスキルセットの特定」が喫緊の課題。

「セキュリティ成熟度」を向上させる上での課題として「スキルある人材の不足」が最も回答を集めました。人口減少や人材不足が叫ばれる現状では、こうした傾向はますます深刻化する可能性があります。そうした中で自社に最適な人材を見極め採用していくことや効率的に外部委託などのリソースを使用することがセキュリティチームにはより求められます。そのためにも、自社で担当する範囲の業務の棚卸と不足しているスキル領域を特定することが、最適化の第一歩となります。

V. 「取引先や海外拠点を経由して自社に侵入されるシナリオ」を想定した訓練の実施が重要。

調査からは①「10,000人以上の組織における金銭的被害コストが大きい」②「500-999人の組織における『セキュリティ成熟度』が最も低い」③「長期的な業務停止被害が海外拠点で起こりやすい」などがわかりました。より大きな利益を狙うサイバー攻撃者は大規模組織を標的とする可能性があります。しかし、大規模組織は「セキュリティ成熟度」が相対的に高い傾向があるため、サイバー攻撃者にとっても直接侵入は困難です。したがって、サイバー攻撃者は「セキュリティ成熟度」の低い中規模組織や海外拠点を侵入口として利用し、それらを経由して大規模組織を侵害する攻撃（サプライチェーン攻撃）を採用する可能性が高まると予想されます。

2. セキュリティ成熟度

本調査では、NIST CSFに沿ったオリジナルの設問を用いて、国内組織のセキュリティ対策状況を調査しました。**本章では、本調査結果をもとに国内組織の「セキュリティ成熟度」について考察します。具体的には、各組織の「セキュリティ成熟度」スコアと他の変数の相関関係を分析し、持続的なセキュリティ対策を取り続けていくために必要な組織的特徴を特定します。**なお、レポート末尾に「セキュリティ成熟度調査の設問表」を添付しています。設問表に回答し他社の結果と比較することで、相対的に自社のセキュリティ対策状況を確認することができます。

全体傾向

調査では、各社で実施している様々なセキュリティ対策の成熟度を網羅的に図るために、NISTの提唱するCSFを採用しました。具体的にはNISTが”Core”として設定するセキュリティ機能「識別」「防御」「検知」「対応」「復旧」それぞれについて、5問ずつ合計25問の設問を用意しました。さらに設問の中で各対策を組織的かつ継続的に実施しているか、5段階の選択肢で計測しました。なお選択肢は、NIST CSFにて定義される”implementation tier”(実装状況を測る指標)の指標ルールを参考に作成しています。

図：「セキュリティ成熟度」の算出方法

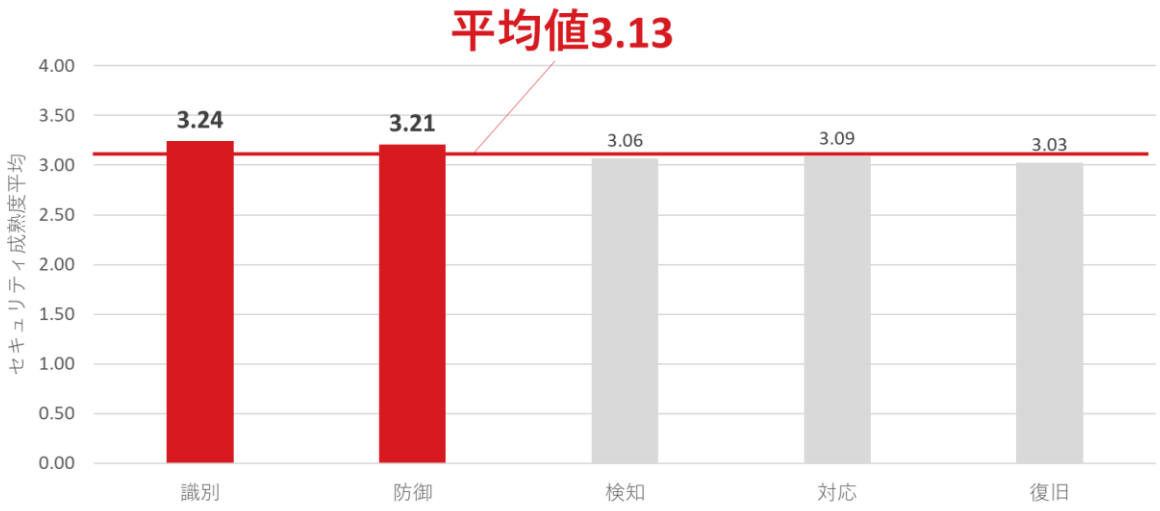
各カテゴリにおける「セキュリティ成熟度」の回答集計は下記表の通りです。

機能	カテゴリ	0を選択	1を選択	2を選択	3を選択	4を選択
識別	資産管理	4	3	39	103	147
	ビジネス優先度に応じたリスク管理	4	4	59	92	140
	ガバナンス	3	2	43	101	153
	リスクアセスメント	4	2	52	103	139
	リスクマネジメント	8	7	57	86	136
防御	ID管理・アクセス制御	3	5	43	108	138
	トレーニング	7	9	41	106	140
	データセキュリティ	4	5	41	112	139
	脆弱性対応	6	9	41	113	129
	保護技術	4	9	58	93	135
検知	検知対象	6	8	44	100	127
	異常とイベント	6	13	51	99	111
	相関分析	8	18	55	75	109
	継続的なモニタリング	7	10	52	102	119
	プロセステスト	9	11	54	93	111
対応	対応計画	6	14	52	100	122
	役割の明確化	6	10	49	108	123
	コミュニケーション	5	14	44	110	123
	分析	5	13	46	108	119
	計画改善	13	10	62	84	121
復旧	復旧プロセス	9	12	51	98	118
	復旧目標	13	13	54	89	113
	役割の明確化	10	14	52	100	114
	対外コミュニケーション	13	11	52	103	110
	計画の合意	9	10	48	98	122

図：「セキュリティ成熟度」を調査した25の設問の回答数集計(N=304,全機能”わからない”を選択した人を除く)

カラーマップで濃い赤色に表現される通り、全ての設問で7割以上の回答者が3:「会社が定める正式手順に沿って、包括的に取り組みが行われている」以上を選択しました。0や1を選択した数が1割以下であることを鑑みても、全てのセキュリティ対策において、9割以上の組織で正式な手順が確立されていることがわかります。

各機能における「セキュリティ成熟度」スコアを平均した結果は、下記グラフの通りです。

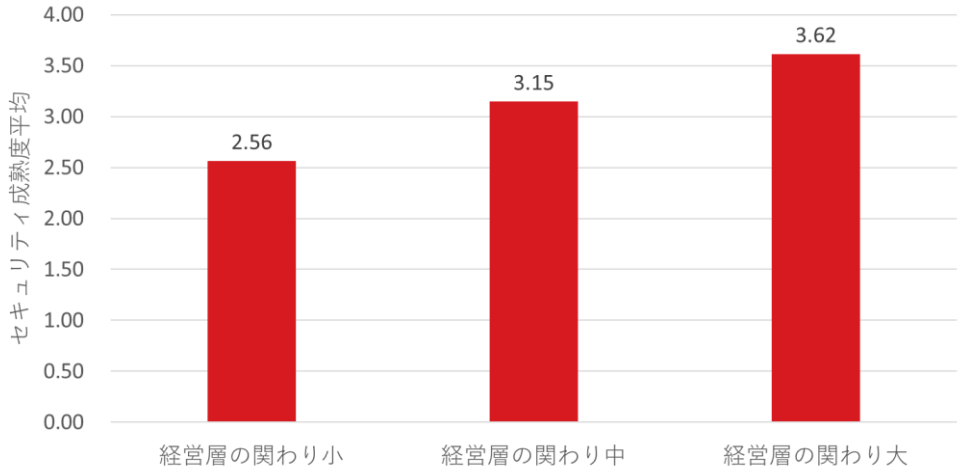


図：「セキュリティ成熟度」の機能別平均値(N=304,全機能”わからない”を選択した人を除く)

全ての機能の平均値が3を超える中、特に攻撃が行われる前の事前対策である「識別」「防御」の平均値が高い傾向にあります。「識別」「防御」の段階で、守るべき資産の特定や事前の対策整備ができていなければ、後に続く「検知」「対応」等も機能しません。そのため、各組織においてまずは「識別」「防御」の対策が優先的に実施されていると考えられます。

「経営層の関わり」と「セキュリティ成熟度」の関係

「経営層の関わり」の大きさを、「セキュリティ業務やリスクに関する報告」「セキュリティ対策へのリーダーシップの主導」「経営会議でのセキュリティリスクの取扱い」「セキュリティに関する資源分配指示」の4つの実施状況から調査しました。結果として、「経営層の関わり」と「セキュリティ成熟度」には強い相関関係が見られました。

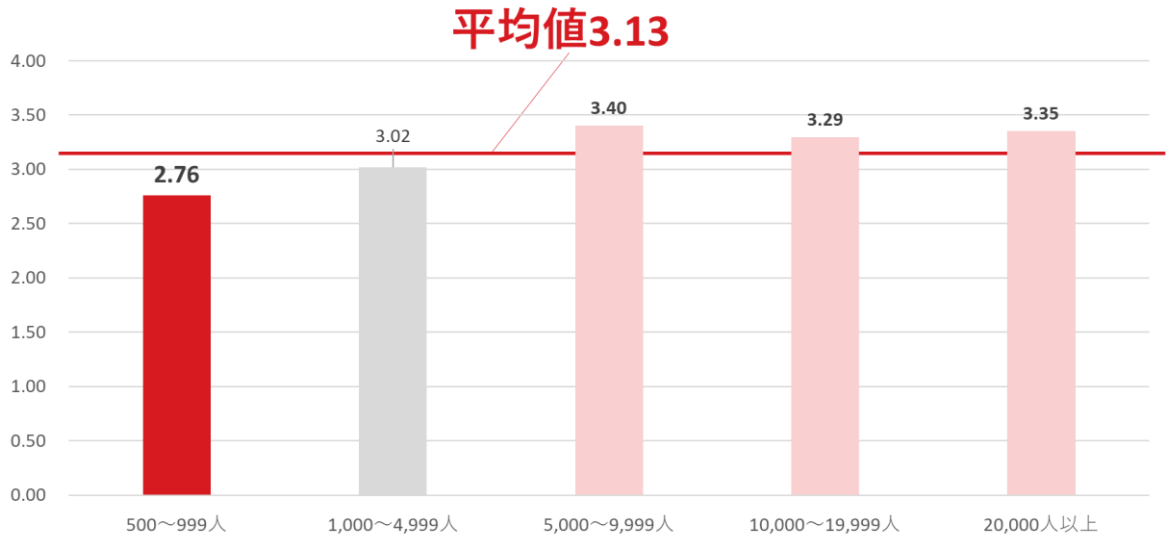


図：「セキュリティ成熟度」と「経営層の関わり」の相関関係(N=304,全機能”わからない”を選択した人を除く)

グラフに示される通り、「経営層の関わり」の大きい組織ほど「セキュリティ成熟度」も高いという傾向が見られました。今回の調査は25のセキュリティ対策事項に対し、いかに組織的かつ継続的に取り組んでいるかによって「セキュリティ成熟度」が評価されます。そのため、部門横断的かつ長期的な取り組みを実現しやすい「経営層の指示や主導」といった「ガバナンス」の要素がスコアに大きく影響したと考えられます。この結果は「セキュリティ成熟度」の向上に、「経営会議でのセキュリティに関する議論」や「予算配分まで含めた経営層の指示」が重要な役割を担っていることを示しています。

「従業員規模」と「セキュリティ成熟度」の関係

調査を行う前に立てた仮説のひとつに、「従業員規模の大きな組織は、守るべき資産や取り扱うビジネスの規模も大きいため、リスクも大きい。そのため『セキュリティ成熟度』が高い傾向にある」というものがありました。この仮説に対する結果が下記グラフです。

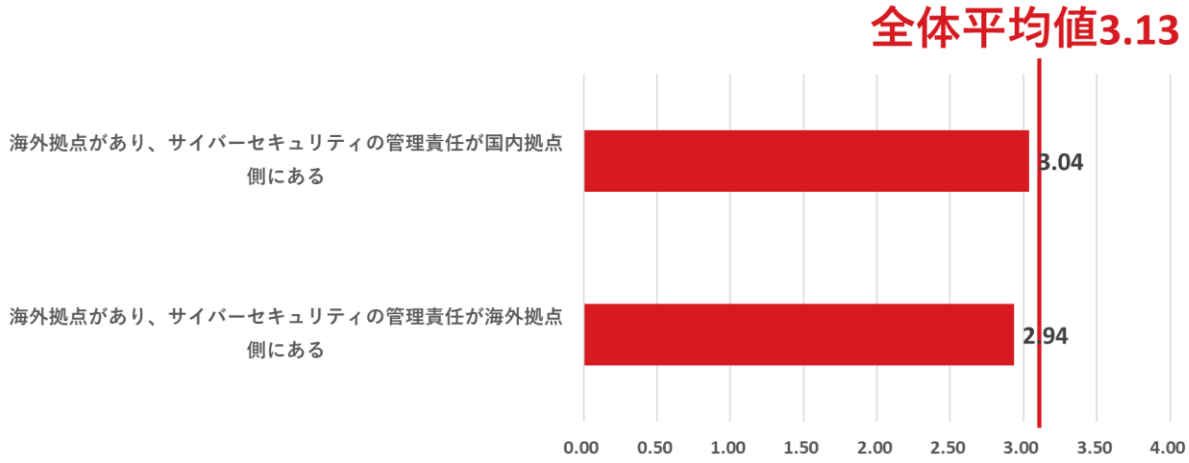


図：「セキュリティ成熟度」と「従業員規模」の相関関係(N=304,全機能”わからない”を選択した人を除く)

特に5,000人以上の組織における「セキュリティ成熟度」が相対的に高水準となりました。一方で、500～999人の組織における「セキュリティ成熟度」が最も低い結果となりました。セキュリティの樽の考え方に則れば、サプライチェーンを構成する組織の内、「サプライチェーン内で最も低いセキュリティレベルの組織」＝「サプライチェーン全体のセキュリティレベル」となります。本結果から中規模以下の組織が大規模組織侵害に向けた侵入口として狙われる可能性が懸念されます。

海外拠点の「セキュリティ成熟度」

サイバーセキュリティにおけるグローバル規模での連携には、地域ごとの法的制約や言語的障壁などを理由に課題を持つ組織が多いと考えられます。調査ではセキュリティの管理責任が海外拠点にあるかどうかについて質問を行うことで、国内側・海外側それぞれでどの程度「セキュリティ成熟度」に差が生じるかを分析し、その課題を明らかにすることを試みました。

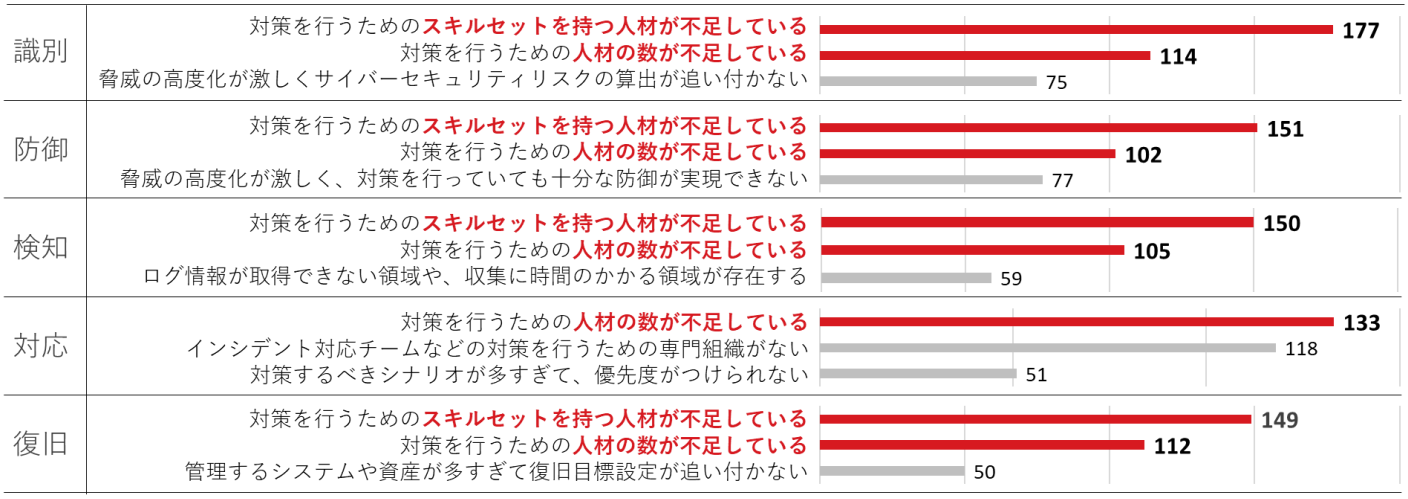


図：国内または海外にセキュリティの管理責任を持つ組織のセキュリティ成熟度平均値

結果は上図の通りです。サイバーセキュリティの管理責任の所在にかかわらず、セキュリティ成熟度に大きな差は見られませんでした。一方、今回の回答者全体の「セキュリティ成熟度」平均が3.13であることから、海外拠点を持っている組織のセキュリティ成熟度が全体の中で低い傾向にあることがわかります。サプライチェーン攻撃では、サプライチェーンを構成する拠点や組織の中でセキュリティレベルが低い部分が侵入口として侵害されます。海外拠点起因のサプライチェーン攻撃が多数確認されている状況も考慮すると、海外拠点も含めた組織全体のセキュリティレベルの測定と向上を行う必要性が高まっていることが伺えます。

「セキュリティ成熟度」向上に向けた課題

もちろんどの企業もセキュリティのレベルを向上させるために様々な対策を試みています。しかし実際のところ「セキュリティ成熟度」が不十分であることが明らかであっても、改善できていない状況が多く見られます。こうした状況の原因を探るためにセキュリティ対策を行う上での阻害要因についても調査しました。

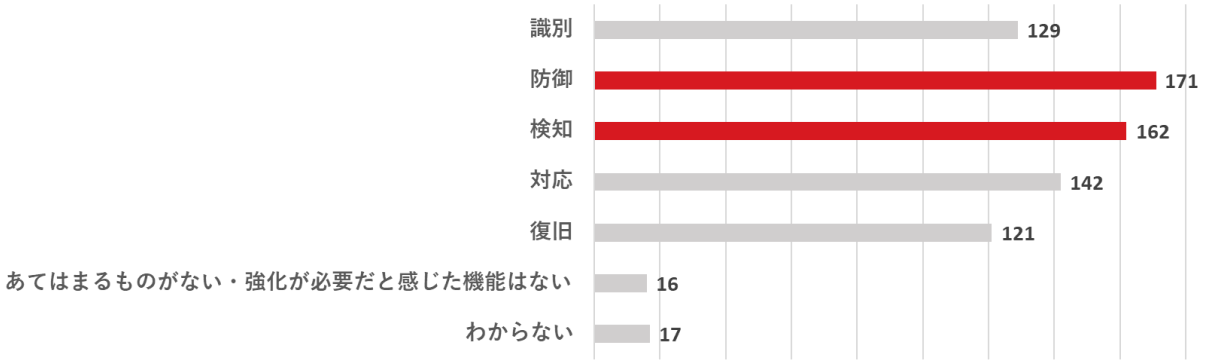


セキュリティ対策を行う上での機能別阻害要因　回答数上位3つのみ表示 (N=305,複数回答)

調査実施前の私たちの予想では、「予算不足」や「セキュリティ以外の部門からの協力不足」などの選択肢にも票が集まると見ていました。しかし、最も選択率の高かった課題は「スキルセットを持つ人材の不足」でした。同時に「人材の数の不足」への回答も集まったことから、セキュリティ対策上の最も大きな課題は「人材」であり、その量も質も不足しているということが分かります。現在の人口変動予測を踏まえた場合に、今後人材が現在よりも拡充していく可能性は少ないことから、セキュリティ業界においてより効率的な運用や外注、もしくは最適な人材選定のニーズが高まっていくことが予想できます。

被害組織が「強化しておくべきだった」と感じた機能

サイバー攻撃を受けた被害組織に共通する「不足しがちな機能」を特定するために、「サイバー攻撃被害発生後に強化しておくべきだったと感じた機能」に関して尋ねました。

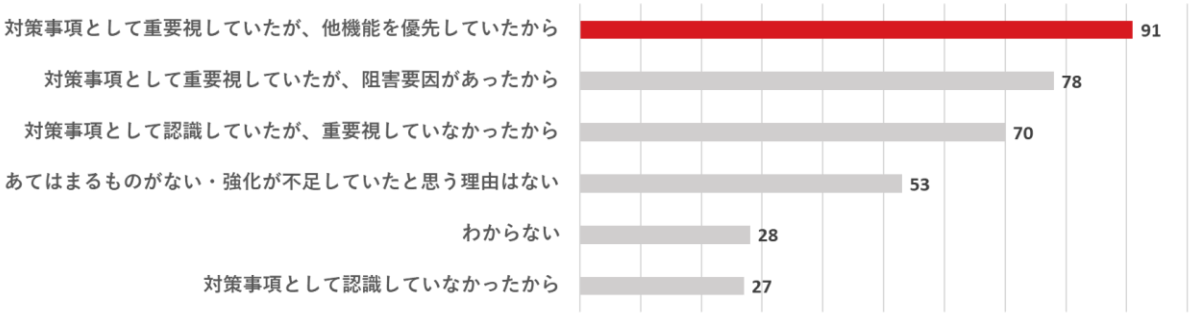


図：サイバー攻撃被害発生後に強化しておくべきだったと感じた機能(N=305,複数選択)

5機能の内、最も回答が集まったのは「防御」の機能でした。「防御」のセキュリティ成熟度は3.21であり全体平均3.13よりも高かったことから、防御に関してサイバー攻撃発生前の時点で組織包括的な対応ができている組織が多かったことが予想されます。しかしそれでも「強化しておくべきだった」と感じた回答者が多かったことは、一通りの「防御」対策は実施または実装されていたものの、それらを実際に取り扱う際の「運用」や体制構築後の「定期的な改善」などに課題があった可能性があります。構築した防御体制の有効性を、訓練などを通して定期的に評価することも被害低減に向けた必要事項の1つであることがここから読み取れます。

次に、「検知」の機能にも回答が多く集まりました。現在のサイバー攻撃の代表とも言える標的型ランサムウェア攻撃や標的型攻撃では、被害組織に気づかれないよう組織内へ侵入・潜伏する手口が多数確認されています。こうした手口に対する「検知」機能のセンサー範囲の網羅性やより迅速にアラートを上げる即時性がサイバー攻撃被害の大きさに影響することは明らかです。サイバー攻撃被害を経験した組織において「検知」を起点とした事後対策に関しても重要性が見直されているということは、未だ被害の発生したことのない組織においても留意しておくべき点と言えるでしょう。

また、強化しておくべきだった機能に関して、強化を行っていなかった理由についても尋ねました。

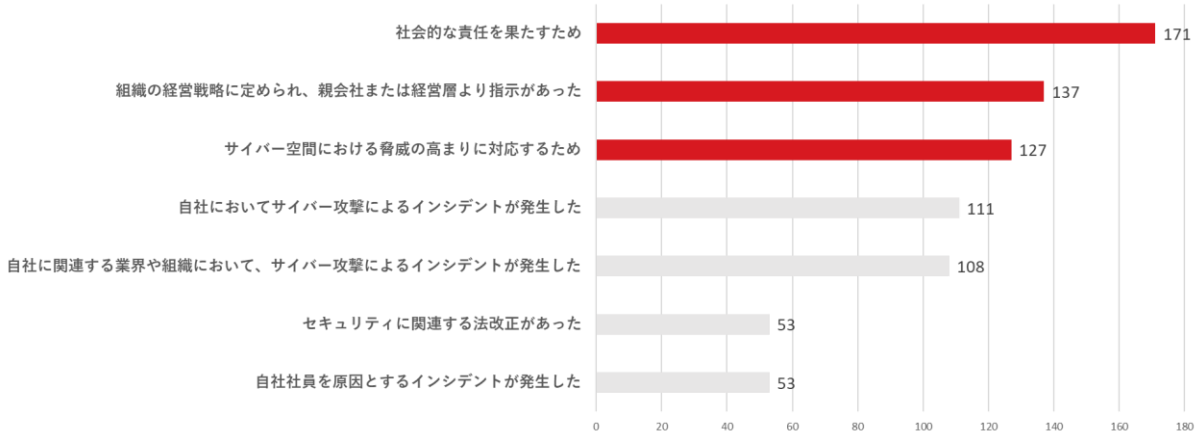


図：強化しておくべきだった機能を、強化できていなかった理由(N=305, 複数回答)

最も回答の集まった理由は「対策事項として重要視していたが、他機能を優先していたから」でした。この結果はセキュリティ対策の優先順位づけが非常に難しいことを表しています。各組織でビジネスの状況が異なる上、セキュリティにかけられる予算と人員が限られるため、自組織にとって最も優先度の高い機能の判断が難しい状況であるとも言えます。今回の調査で行った自組織の「セキュリティ成熟度」を数値的に計測し把握する取り組みは、全体を俯瞰したときの判断材料として有効なものとなるでしょう。

「セキュリティ成熟度」向上のきっかけ

組織が「セキュリティ成熟度」の向上を図るきっかけは何でしょうか。複数の組織で共通するセキュリティ対策強化のきっかけを把握することで、自組織でも対策強化を行う際の推進材料とできるでしょう。そこで調査では、どのようなきっかけでセキュリティ対策を強化したか、に関しても尋ねています。



図：セキュリティ対策を強化したきっかけ (N=305, 複数回答)

回答の結果は「社会的な責任を果たすため」、「組織の経営戦略に定められた」、「サイバー空間における脅威の高まりに対応するため」に回答が集まりました。「自社や関係組織におけるインシデント」よりも票が集まったことから、インシデントが起因でなくともセキュリティ対策を強化するきっかけとなり得ることが本結果からわかります。特に「社会的な責任を果たすため」が最も回答を集めていることから、サイバー攻撃による影響範囲が各社だけでなく社会にまで広がっており、多くの組織が一定のセキュリティレベルを確保する必要に駆られている現状が読み取れます。セキュリティに問題があることを知っていながら対策を施さないことによって善管注意義務違反に問われるケースもある為、組織にはセキュリティへの適切な投資判断が今後も求められます。

3. サイバー攻撃被害の実態

調査では、サイバー攻撃による被害の金額や攻撃の具体的な内容、また使用された手法などからサイバー攻撃被害の実態を把握することを目的としました。**本章では「多くの組織で発生している攻撃の種類」や「被害の大きいサイバー攻撃の内容」に関する調査結果から、組織が優先的に備えるべき脅威を考察します。**

サイバー攻撃による被害額の累計

調査では、過去3年間で発生したサイバー攻撃による被害コストの総額やその攻撃内容について尋ねました。
過去3年間のサイバー攻撃の累計被害額は、平均1億2528万円でした。中には10億円以上の被害が生じた組織も存在しています。

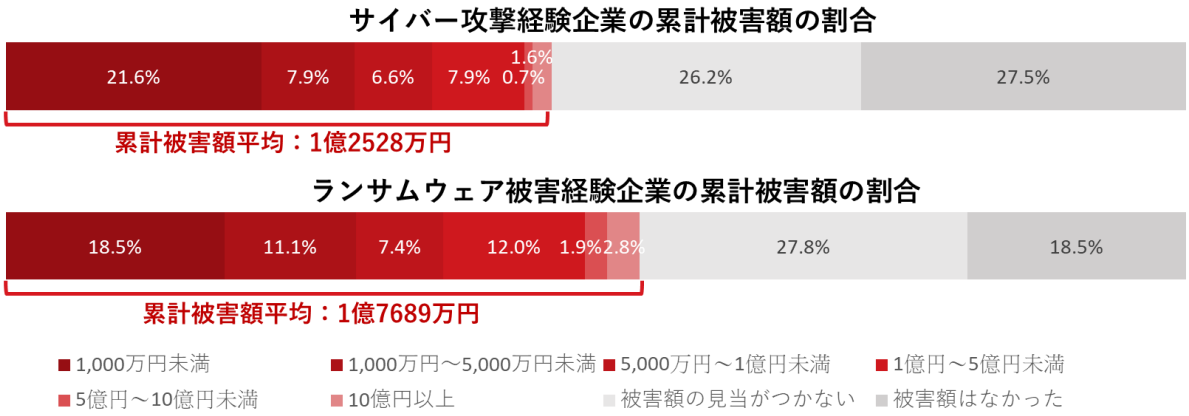
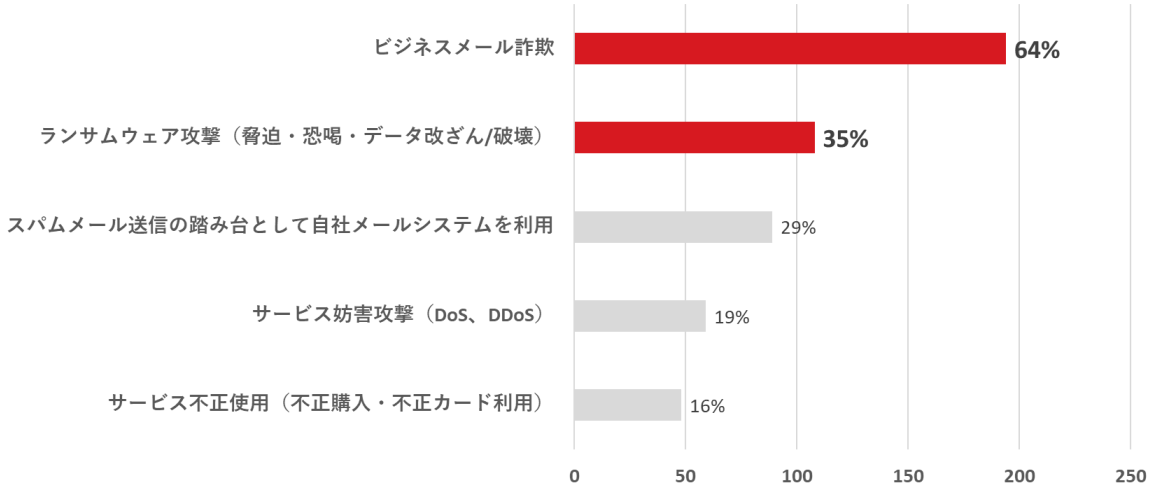


図3：過去3年間の累計被害額（サイバー攻撃経験企業：N=305、ランサムウェア被害経験企業：N=108）

またランサムウェア攻撃を受けた企業に限定した場合、平均被害額はさらに5千万円ほど大きくなります。すでに多くの組織が警戒を強めていると思われますが、やはりランサムウェア攻撃への対策を実施することは大きな被害を防ぐ観点で重要です。

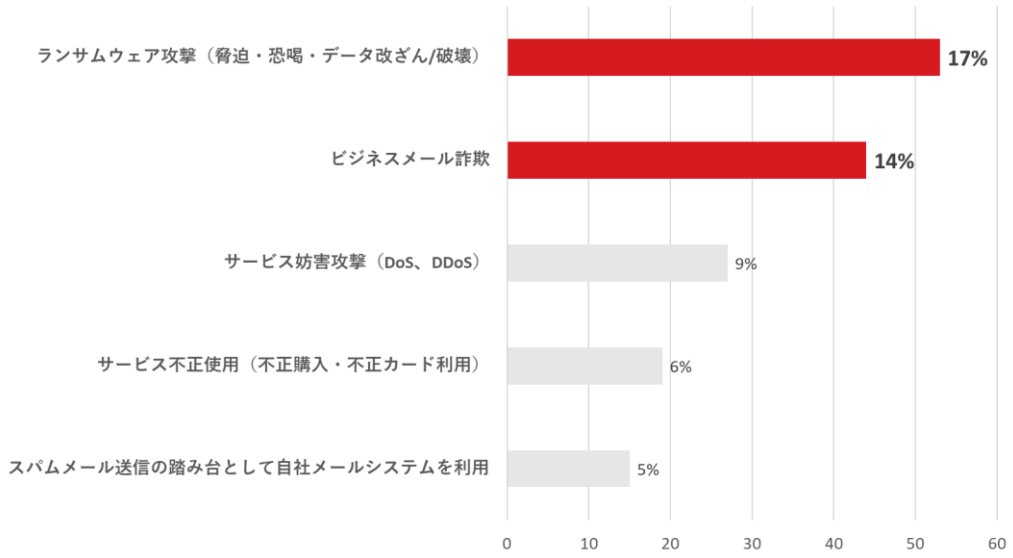


過去3年間で受けたことのある攻撃内容　回答率上位5種類(N=305,複数回答)

過去3年間で受けた攻撃を全て選択する設問では、ビジネスメール詐欺（以下BEC）が最多の回答で65%、約3社に2社が被害経験ありと回答しました。メールを使った攻撃は、ビジネスを行う上でメールを利用しているユーザが大多数であるため、頻繁に攻撃が試みられていると考えられます。またここでもランサムウェアは2番目に多い攻撃として位置しており、3社に1社以上の回答者が攻撃を受けています。

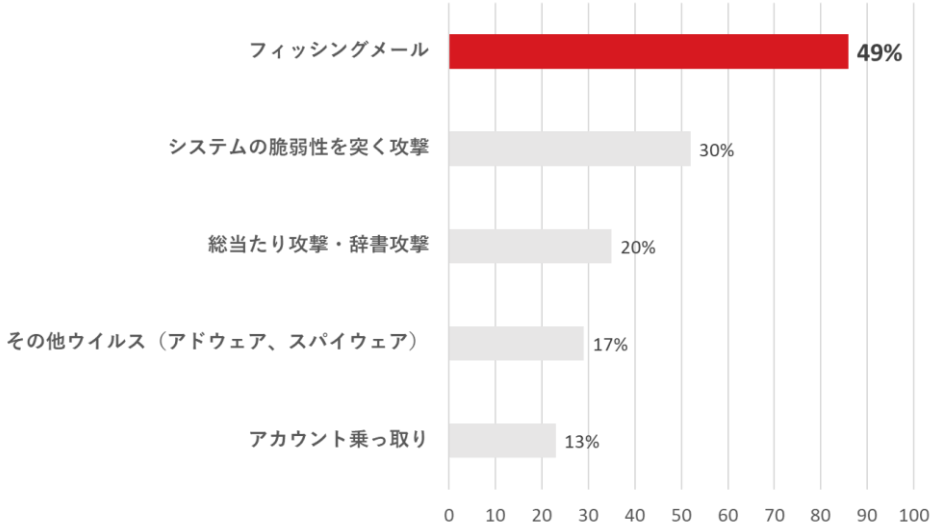
「最も被害コストの大きかったサイバー攻撃」

過去3年間で受けた攻撃の内「最も被害コストの大きかったサイバー攻撃」についても攻撃内容や使われた手法を調査しています。



図：過去3年間で「最も被害コストの大きかったサイバー攻撃」の種類　回答率上位5種類(N=305,単一回答)

「最も被害コストの大きかったサイバー攻撃」の種類はランサムウェア攻撃でした。ランサムウェア攻撃を受けた人のみの平均被害額が大きかったことがこちらの結果にも表れています。次点でBECによる被害も大きく、攻撃の頻度はBECの方が高いことを踏まえると、ランサムウェアに比べて被害に繋がりにくいものの、同等レベルの脅威であることが示されています。



図：過去3年間で「最も被害コストの大きかったサイバー攻撃」に使用された攻撃手法
回答率上位5手法(N=174, 「最も被害コストの大きかったサイバー攻撃」の種類を回答した人のみ)

「最も被害コストの大きかったサイバー攻撃」で、最も使用された手法としては約半数の組織がフィッシングメールと回答しました。BECもランサムウェアも事前に標的組織に関する十分な情報が必要となることから、フィッシングメールを使用して窃取した情報を悪用し、攻撃を成功させている可能性があります。このことはメールを起点とした侵入型攻撃が被害に繋がりやすい傾向にあることを示していると考えられます。

「最も被害コストの大きかったサイバー攻撃」の種類別被害コスト

「最も被害コストの大きかったサイバー攻撃」で、選択された攻撃それぞれでどの程度コストが発生したかの分析も行いました。

順位	攻撃の種類	平均被害コスト	サンプル数
1	機密情報の窃取・暴露	¥385,227,273	6
2	ランサムウェア攻撃（脅迫・恐喝・データ改ざん/破壊）	¥121,809,524	53
3	サービス不正使用（不正購入・不正カード利用）	¥121,428,571	19
4	ビジネスメール詐欺	¥54,841,772	44
5	スパムメール送信の踏み台として自社メールシステムを利用	¥35,833,333	15
6	サービス妨害攻撃（DoS、DDoS）	¥32,163,462	27
7	Webサイト改ざん	¥13,125,000	4
8	他社侵入の踏み台として自社システムを利用	¥7,500,000	2

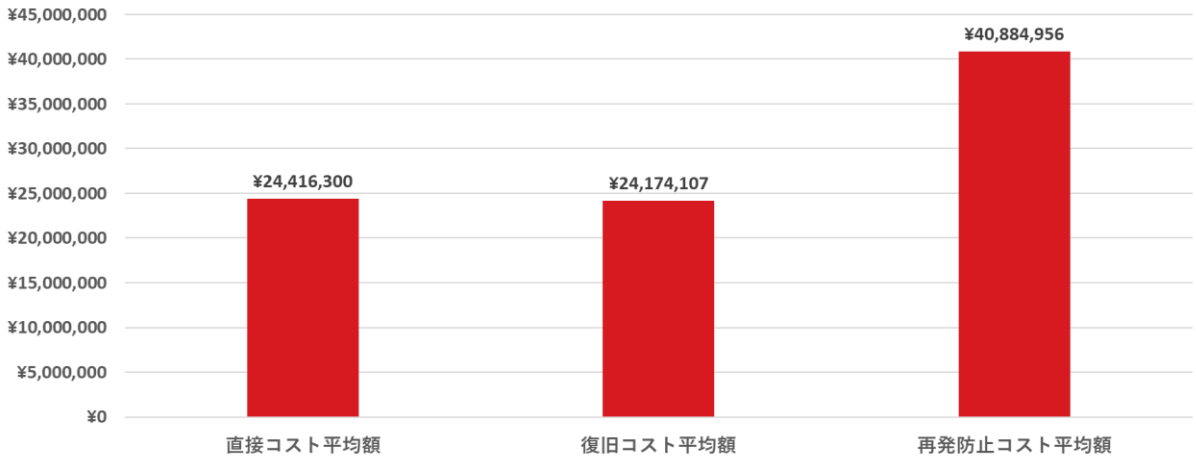
表：過去3年間で「最も被害コストの大きかったサイバー攻撃」の種類別平均被害額（その他やわからないを除く）とサンプル数（上位8種）

平均の被害額という観点で見れば、「機密情報の窃取・暴露」がサンプル数は少ないものの最も被害コストの大きい攻撃となりました。調査ではランサムウェア攻撃はあくまで「脅迫・データ改ざん/破壊」のみを攻撃の中身として定義しています。しかし、暴露型ランサムウェア攻撃の場合、「脅迫・データ改ざん/破壊」に「機密情報の窃取・暴露」の要素が加わるため、被害コストがより高まることに注意が必要です。今回の調査では被害コストとして、補償金や被害発生後の対応コストも含めた金額を算出しているので、より多くの対外対応が必須となる情報窃取に関して大きな被害コストとなりやすかったと考えられます。また同様に「サービス不正使用」の平均被害コストが高く、こちらもクレジットカード会社や不正利用の被害者への対応・説明など人的コストの影響が顕著に出たことが想定されます。

上位7種のサイバー攻撃被害についてもし自社に発生する確率の高い、または対策優先度の高い攻撃が上記に含まれる場合には、該当する平均被害額をリスク規模算出のひとつの基準として使用することも可能です。

「最も被害コストの大きかったサイバー攻撃」のコスト内訳

被害により生じたコストの内訳として、調査の中で設定した「直接コスト」「復旧コスト」「再発防止コスト」の3点に関して、どのコストに最も費用が掛かったかを明らかにするべく、それぞれのコストの平均金額を調査しました。

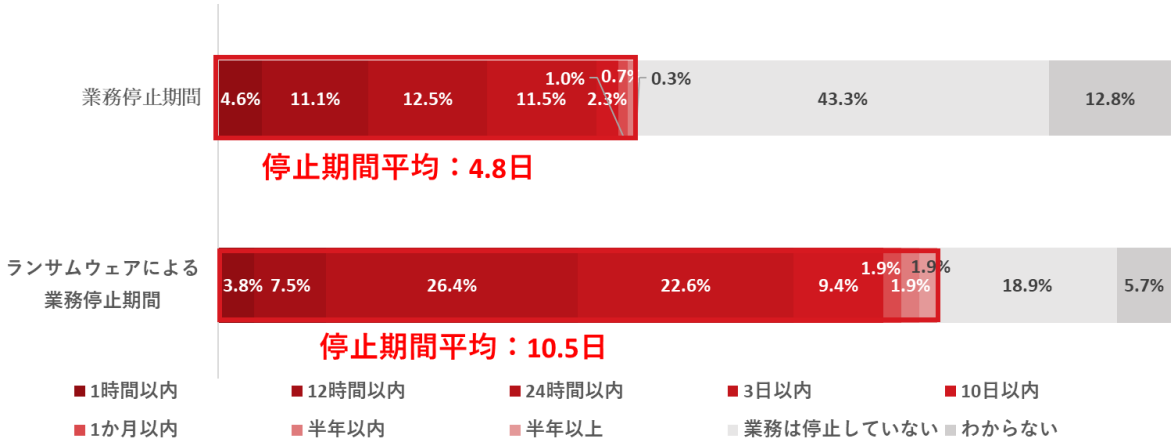


図：「最も被害コストの大きかったサイバー攻撃」によって生じた被害コストの種類別平均額

被害コストの内、平均金額が最も大きかったのは「再発防止コスト」でした。身代金支払いや売上停止による「直接コスト」、調査・封じ込めや通常業務に戻るための人的対応による「復旧コスト」はそれぞれ、あくまで一時的なコストであるため、長期的な対策を含む「再発防止コスト」が大きくなること自体は調査前の予想通りでした。自社内で保有しているリスクに対する対応方法を検討する際には、被害発生後に「再発防止コスト」が生じ、かつ最も大きな投資が必要となることを前提に組み込んだ上で、方針を定める必要性があるでしょう。

「最も被害コストの大きかったサイバー攻撃」で生じた「業務停止期間」

ここまで、主に金額を軸にサイバー攻撃被害の度合いを分析してきました。金額もサイバー攻撃被害を測る有効な指標のひとつではあるものの、サイバー攻撃によってもたらされる損害はそれだけではありません。そこで調査では、もうひとつの被害度合いを測る軸として「業務停止期間」を設定し質問しました。「最も被害コストの大きかったサイバー攻撃」で発生した「業務停止期間」は下記の通りでした。

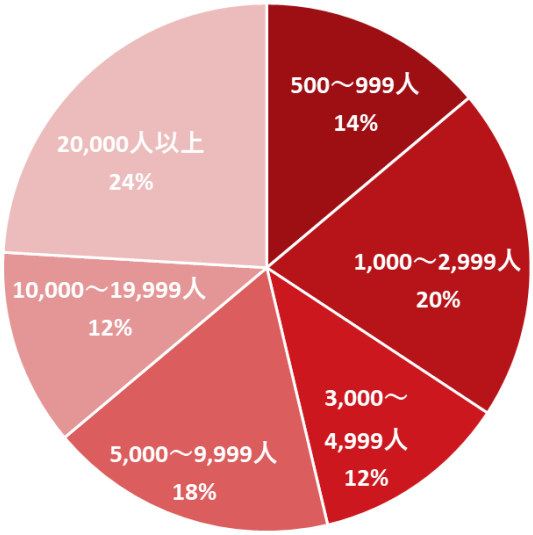


図：「最も被害コストの大きかったサイバー攻撃」で発生した「業務停止期間」（上段N=172, 下段N=38）

調査回答者全体でサイバー攻撃により「業務停止期間」が発生したとする回答者は約4割でした。またその平均期間は4.8日でした。業種・業態によるものの一週間の営業日が5日間であると仮定すれば、サイバー攻撃1回あたり平均約1週間業務が停止する可能性があると言えます。しかしこれはあくまでも平均値であり、上図の通り被害が発生した人43.9%のうち3日以内に復旧した人が39.7%であり、被害があった場合でも9割は3日以内に復旧が完了しています。さらに今回「最も被害コストの大きかったサイバー攻撃」を対象とし、「業務停止期間」を尋ねていることからも、サイバー攻撃により3日以上の業務停止被害が発生する確率は比較的低いことが本結果からわかります。この事実を踏まえると、特定のシステムへのセキュリティ投資の優先度を検討する際に、可用性を重視するのであれば、保護対象が数時間～3日でも停止すると事業リスクが高い、あるいはそれ以上に社会的な損失に繋がる可能性が高いシステム（医療機関などライフライン関連）かどうかが優先度を判断する際の検討項目のひとつとなるでしょう。
今回、ランサムウェア攻撃の被害を受けた場合、さらに「業務停止期間」が長期化する傾向も確認されました。図中では「最も被害コストの大きかったサイバー攻撃」に限定されますが、全体平均としては10.5日で全体の平均期間の約2.5倍の期間となりました。データの暗号化を主な手段とするランサムウェア攻撃は被害組織にとっての事業継続性を脅迫材料として金銭を要求する手口であるため、全体と比較して業務停止の長期化が顕著に表れたと考えられます。12～24時間以内、24時間～3日以内、3日～10日以内の割合が増加していることから、ランサムウェアへのリスクシナリオを検討する際にはある程度被害が長期間に渡る事を踏まえる必要があることが本結果からわかります。

大きな被害をもたらす「ランサムウェア攻撃」

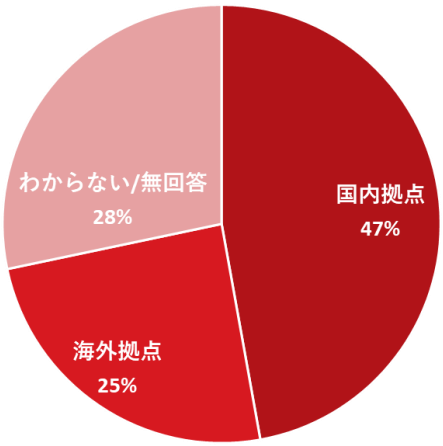
金銭的被害、業務停止被害の双方で最も被害の大きかったランサムウェア攻撃に関しても、よりその傾向を分析するために相関分析を行いました。最初に、組織規模による分析です。



図：「最も被害コストの大きかった攻撃」でランサムウェアを選択した組織の規模内訳(N=53,単一回答)

結果として特定の規模の組織が目立って被害にあっているという、統計的な傾向は見られませんでした。ランサムウェア攻撃では、標的組織を入念に調査した上で攻撃を行う「標的型ランサムウェア攻撃」が主流となっていることから、攻撃者は特定の規模の会社を標的に定めて侵害を行っているというよりは、脆弱性を抱えているなどネットワークから直接侵入可能な組織を優先的に攻撃している傾向が強いと考えられます。これは当社の別のリサーチでも明らかになっている傾向です。[2]

さらに、今回の被害発生拠点が国内であったか、海外であったかに分けて分析を行いました。

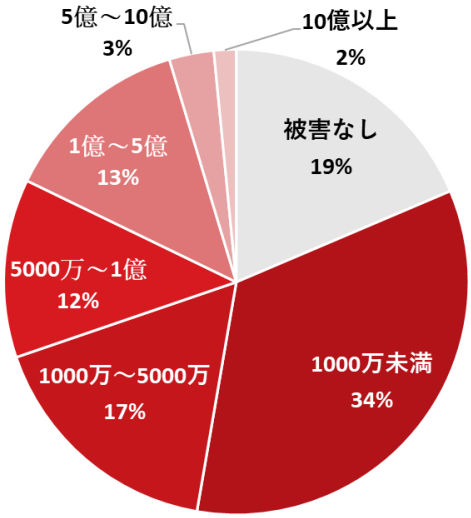


図：ランサムウェア攻撃による被害が発生した拠点の内訳(N=53,単一回答)

[2] https://www.trendmicro.com/ja_jp/jp-security/23/b/securitytrend-20230220-01.html

ランサムウェア攻撃では海外拠点での被害発生割合が25%でした。今回の調査の回答者の内、海外拠点を持つ組織の割合は7割程度でしたが、今回の調査の対象が国内組織であり、またそれらの組織規模の内訳を考慮しても国内拠点の数の方が多い組織が多数であると考えられます。それでも25%の被害が海外拠点にて発生しているという事実は注意を払うべき内容と言えます。海外拠点を持つ組織の「セキュリティ成熟度」が平均よりも低かったことからも、グローバル全体でのセキュリティ向上の必要性が高まっていることが読み取られます。

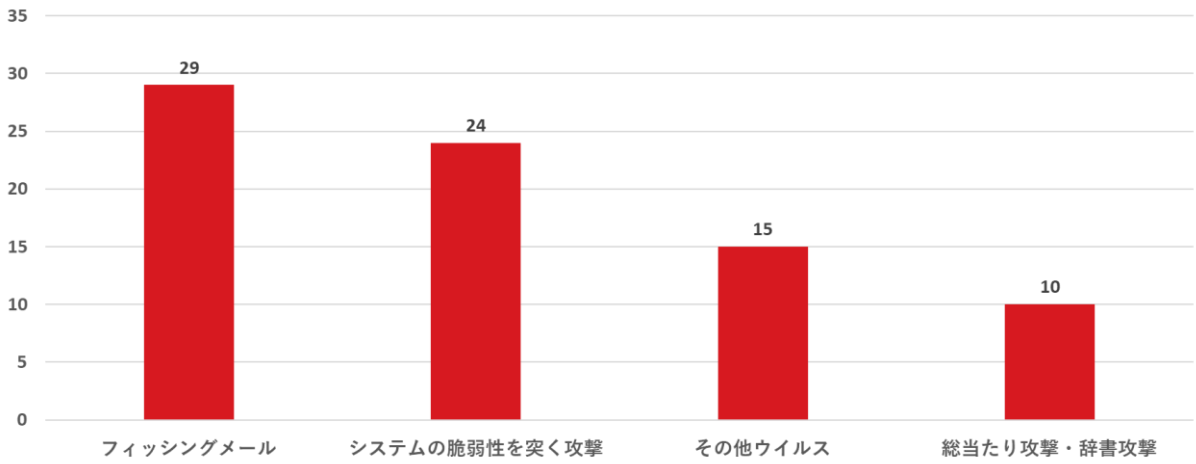
ランサムウェア攻撃による被害額はどの程度か、「最も被害コストの大きかったサイバー攻撃」においてランサムウェアを選択した回答者の被害額内訳が以下の図です。



図：ランサムウェア攻撃により生じた対応コストの内訳(「被害の見当がつかない」を除く)(単位：円)

上記図の通り、47%の回答者が所属する組織において、ランサムウェア攻撃により1,000万円以上の被害が発生しています。5,000万円以上に絞った場合でも、約30%の回答者の組織で被害が発生しています。また、これらの被害の1件あたりの被害金額は121,809,524円であり、万が一攻撃の被害に遭った場合大きなビジネスリスクとなる可能性が伺えました。すでにその脅威は十分に認識されているランサムウェア攻撃ですが、数千万～数億円単位の大きな損失を引き起こす脅威であることを前提に、そのリスク対応指針を決定する必要性があります。

ランサムウェア攻撃に使用された攻撃手段は下記の内訳となりました。

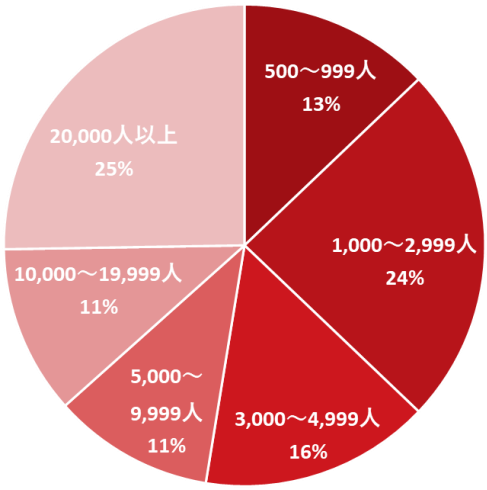


図：ランサムウェアで使用された攻撃手段　選択数上位4種類
(N=53, 複数回答, その他ウイルスはアドウェア/スパイウェアなどを指す)

ランサムウェアではフィッシングメールが攻撃のための手段として多用されていました。組織で使用しているアカウントの認証情報を奪うことで組織内への侵入を行ったり、侵入の契機となる不正ツールをダウンロードさせるWebサイトなどに誘導したりしている可能性があります。ランサムウェアそのものへの対策に加えて、不正サイト対策やアカウント情報の堅牢性を高く保つ運用を徹底することもまた必要な対策のひとつであると言えます。またシステムの脆弱性を突く攻撃についても回答数が多いことから、脆弱性対策も優先度の高い項目となります。前述した通り、ランサムウェア攻撃の被害は組織規模に依らないという点からも、侵入できる組織には手当たり次第に攻撃を試みています。特に外部と接するシステムに関する脆弱性の検査・管理は被害発生率に直結する要素となるため優先的な対策が必要です。

国内組織も無視できない「BEC」の脅威

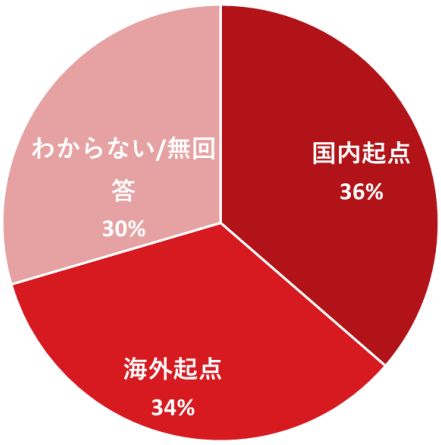
BEC（ビジネスメール詐欺：Business E-mail Compromise、以下、BEC）は世界規模で大きな金銭的被害をもたらすサイバー犯罪です。英語圏での攻撃や被害がその大半を占めているとされていることから、調査前時点では今回の国内を対象とした調査においてBECによる被害が多数または大規模であるという予想はしていませんでした。しかし、今回の調査では過去3年間で受けたサイバー攻撃で最もBECの選択率が高く、また最も被害コストの大きかった攻撃でも2番目に選択数の多い攻撃であったことから、よりその傾向を分析するために被害組織の特徴に関する分析を行いました。そのひとつが組織規模による分析です。



図：「最も被害コストの大きかった攻撃」でBECを選択した組織の規模内訳(N=44,単一回答)

結果として比較的規模の小さいまたは大きい組織においてBEC被害に遭う可能性が高い、などといった有意な傾向は特にみられませんでした。これはBECが組織規模によらずそのターゲットとなる可能性があることを示しています。組織にとっては「従業員規模」を理由にBECのリスクを小さく/または大きく見積もることは実態と異なる可能性があることに留意しておくべきでしょう。

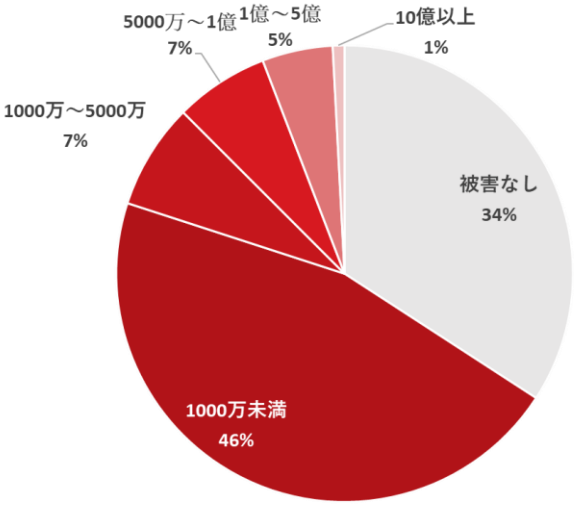
また、当社のSPNのデータ上では英語圏での攻撃が盛んであることから、あくまで海外拠点などを中心としてBECの被害が発生している可能性を鑑み、国内、海外拠点のどちらで、BECの被害が発生したかについても分析を行いました。



図：BEC被害が発生した拠点の内訳(N=44,単一回答)

結果として、国内拠点、海外拠点どちらにおいても同数程度被害が発生していたことが分かりました。今回の調査では、メールの内容が日本語であったか英語であったかなどの区分までは調査していませんが、海外組織とのやりとりが頻繁にある組織でなくとも、ある程度BECの脅威に晒される可能性を考慮し対策を行っておく必要があります。

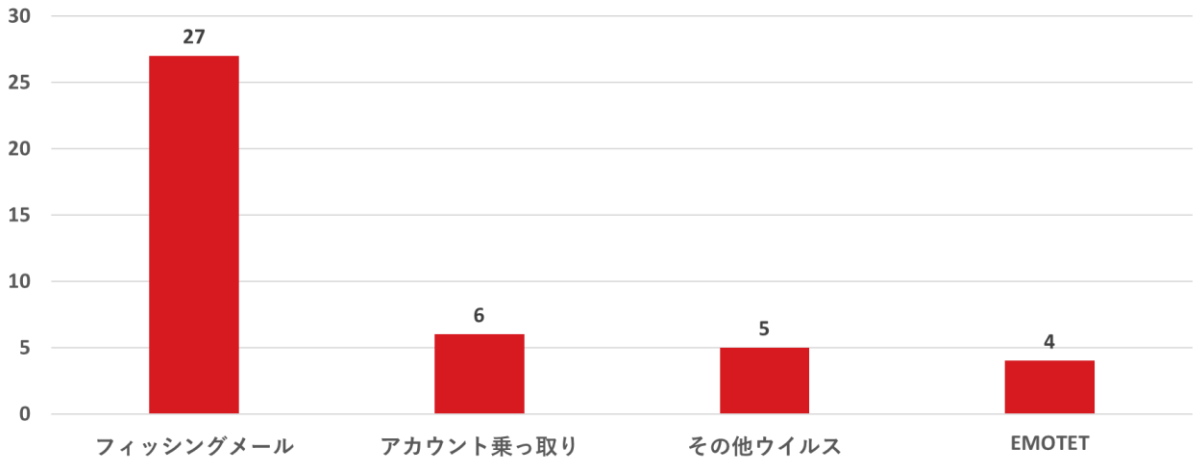
BECによってどの程度の被害がでているかも分析を行いました。下記は、「最も被害コストの大きかったサイバー攻撃」において、BECを選択した回答者の被害金額の内訳を集計したものです。



図： BECにより生じた対応コストの内訳(「被害の見当がつかない」を除く)(単位：円)

こちらの結果からはBECの被害があったとした回答者のうち、約3割で1,000万円以上の被害を受けていることが示されています。また、これらの被害の1件あたりの平均金額は54,841,772円であり、BEC攻撃が一度でも被害に繋がってしまうと数千万円単位の大きなコストを被る可能性があることも読み取れます。本章冒頭で記載した通り、今回の調査においてBECによる攻撃を受けた経験のある組織が65%であったことを踏まえると、BECは国内においても十分に警戒すべき脅威のひとつであると捉えられます。

BECへの警戒を強める際の強化ポイントを明確にするために、BECにおいて使用された攻撃手段を確認しました。



図：BECで使用された攻撃手段　選択数上位4種類
(N=44, 複数回答, その他ウイルスはアドウェア/スパイウェアなどを指す)

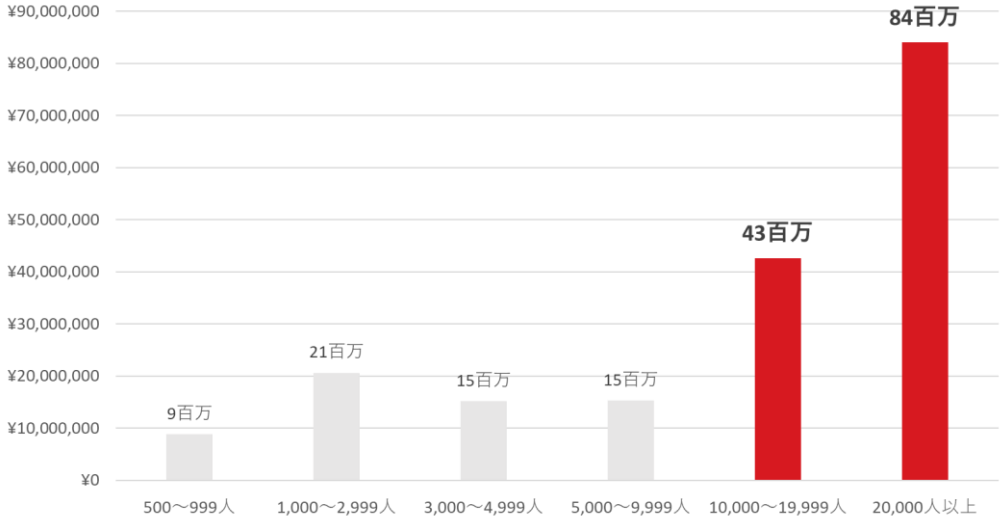
被害に繋がったBECの攻撃で最も使用された手段はフィッシングメールでした。また次点でアカウント乗っ取りが続くことからもアカウント情報の窃取が手段として事前に多用されていることが分かります。攻撃が成功してしまう主な要因として、そのメール内容の巧妙さが挙げられますが、その準備段階として攻撃者は情報の窃取や盗み見を行っています。被害に遭わないためにはBECそのものへの対策だけでなく、本結果に示されるようなフィッシングやアカウント乗っ取りなどの情報収集段階に対する対策も漏れなく実施しておくことが重要と言えます。

4. サイバー攻撃被害に遭いやすい組織の特徴

調査では、サイバー攻撃被害の大小とその他の要素の相関関係を把握することで、被害に遭いやすい企業の特徴を突き止めることを主目的として設定しました。

「従業員規模」と「被害コスト」の関係

現在、侵入型のサイバー攻撃が多発している状況を踏まえると、「従業員規模」の大きな組織は守るべきデジタル資産やビジネスの規模が大きいため、大きな組織ほど被害が大きくなる傾向にあるという仮説を立てていました。

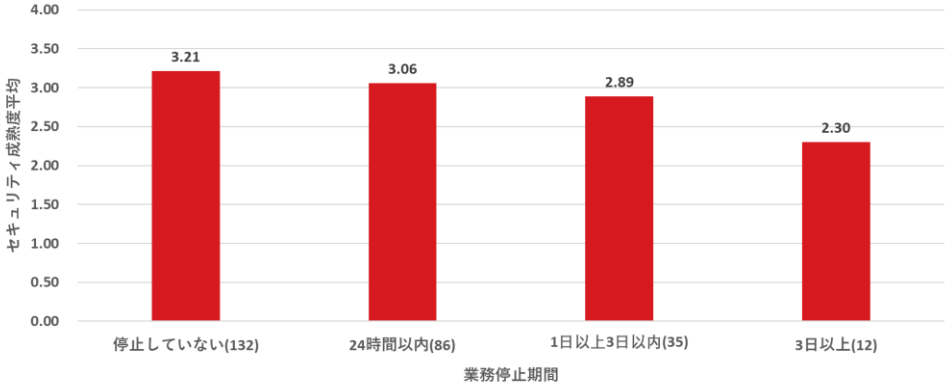


図：「従業員規模」と「最も被害コストの大きかったサイバー攻撃により生じた被害コスト」の相関関係

調査の結果として1万人以上の組織における「最も被害コストの大きかったサイバー攻撃」によって生じた平均被害額が大きいことがわかりました。本結果から、攻撃者がより大きな利益を得ることを意図している場合、1万人以上の組織が標的となる可能性が高いことが予想されます。

「セキュリティ成熟度」と「業務停止期間」の関係

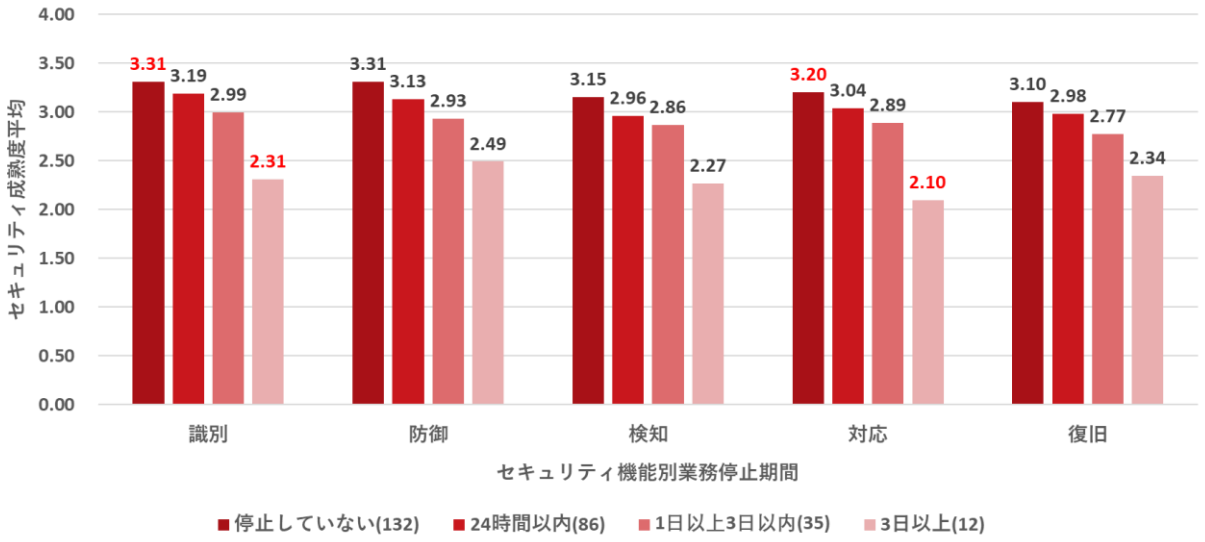
「セキュリティ成熟度」が高いほど、被害が小さいという仮説に基づき「セキュリティ成熟度」平均値と「業務停止期間」の相関を分析しました。



図：「セキュリティ成熟度」と「業務停止期間」の相関

上図の通り、「セキュリティ成熟度」の平均値が高い組織ほど「業務停止期間」が短いことがわかりました。これは一見当たり前のことのように思われます。しかし様々な対策を行っていても、その有効性を検証することが難しいセキュリティの世界においては重要な結果であると捉えられます。業務停止被害を低減するという目的では、「停止していない」の回答者の平均値にあたる3.21をベンチマークとして自社の「セキュリティ成熟度」を向上させていくことを推奨いたします。

なお上図は今回「識別」「防御」などをはじめとする5つの機能の「セキュリティ成熟度」を合算した平均値となります。さらなる分析として各セキュリティ機能の内どれが最も影響しているかを把握するため、5つの機能別で「業務停止期間」に応じた平均値を計算しました。

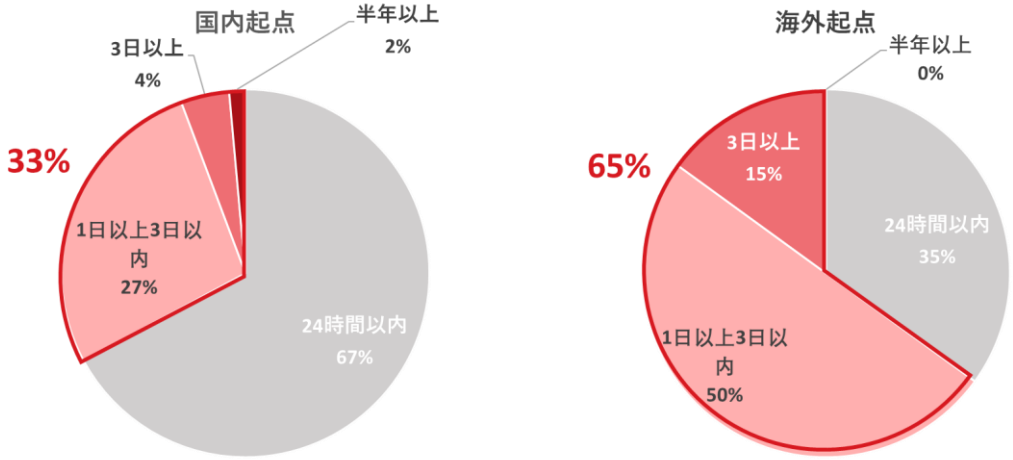


機能別の「セキュリティ成熟度」と「業務停止期間」の相関関係(n=265, “わからない”及び外れ値“半年以上“の回答者を除外)

機能別で見た際には、「識別」「防御」「検知」「対応」「復旧」の全ての機能が「業務停止期間」と負の相関を持つことがわかりました。これは、どの機能の「セキュリティ成熟度」においても、業務停止被害軽減に一定の効果を持つことを示していると考えられます。さらに、中でも赤字でハイライトした「識別」「対応」における「停止していない」と「3日以上(停止)」の「セキュリティ成熟度」平均値が1ポイント以上差をつけていることから、「識別」「対応」の「セキュリティ成熟度」向上による被害低減の効果が大きいことが伺えます。

「インシデントの発生地点」と「業務停止期間」の関係

サイバー攻撃による被害の大小に影響を与える要因の一つとして、その攻撃が国内で発生したものか海外で発生したものか、という点が挙げられると予想しました。

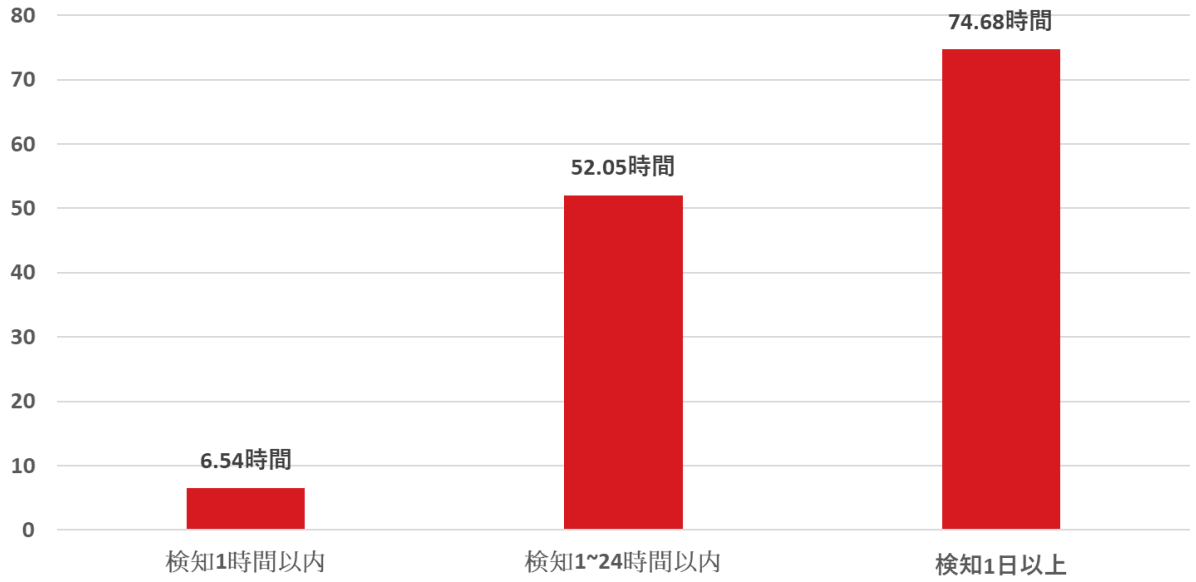


国内起点と海外起点のインシデントによる「業務停止期間」の比較(国内n=70,海外n=20 業務停止が発生した人のみ)

国内でサイバー攻撃が発生した回答者の内、3人に1人が1日以上の業務停止を経験したと回答しましたが、国外で発生したケースでは3人に2人が1日以上の業務停止被害を受けたと回答しています。これは海外拠点で発生したサイバー攻撃の方がより被害が大きくなる傾向にあることを示しています。海外拠点に対するセキュリティの統制や管理が国内に比べると機能しづらい状況にあることが予想されます。海外に拠点を持つ組織は、海外拠点を発端とするセキュリティインシデントに伴うリスクの特定や管理方針の決定を優先的に行うことで被害低減につながる可能性があります。また、もしインシデントが起こってしまった場合の訓練を、拠点横断で行っておくことも効果的であると考えられます。

「侵入から検知までにかかった時間」と「業務停止期間」の関係

調査では、「最も被害コストの大きかった攻撃」を検知したタイミングに関しても尋ねています。特に組織内への侵入を伴う攻撃の場合、いかに素早く侵入を検知できるかによって被害の大きさが異なるであろうという仮説の元、検知タイミングごとの平均の「業務停止期間」を計算しました。



図：「侵入から検知までにかかった時間」と「業務停止期間」の関係性を算出したグラフ

攻撃を検知した時間が遅くなればなるほど、「業務停止期間」も長引くことが本結果から示されています。つまり組織が受けた攻撃をいかにすばやく検知するかが、その後の被害の大きさを決めることになります。また、「検知1時間以内」に対して「検知1～24時間以内」の「業務停止期間」が8倍強であることから、同じ一日以内でもその被害度が急速に拡大していることも注意すべき点と言えます。しかし組織内において使用するIT資産やそのログの量も膨大であることから、検知業務を人力で実現することは現実的に難しい状況にあります。実際に当社が提供するインシデント対応サービスにおける、被害組織への侵入の際に使用されたアタックサーフェス（攻撃対象領域）は、VPN等ネットワーク機器、クラウド、Webブラウザ経由など多岐にわたりました。これらを踏まえると、サイバー攻撃被害を低減するためには検知時間の短縮が必須であり、そのためには組織の幅広い領域にまたがったセキュリティソリューションの導入が重要と言えます。これによって検知に使用可能なテレメトリを集めるためのDetection & Responseの体制を整えることが効果的なセキュリティ投資のひとつとなるでしょう。

まとめ

今回の調査では、国内組織の「セキュリティ成熟度」をはじめとする様々な特徴と共に、サイバー攻撃被害の実態を調査することで、サイバー被害に遭いやすい組織の特徴を特定しました。これにより、被害低減に向けて実施すべき対策事項が明らかになりました。

今回の「セキュリティ成熟度」に関する調査では、さまざまなセキュリティ対策全般を網羅しつつ、多くの業種で汎用的に使用できるフレームワークとして、NIST CSFを採用しました。ただし、「セキュリティ成熟度」を測るために最適なフレームワークは、業界や業務内容に応じて異なる可能性があることに注意してください。またNIST CSFも2024年にバージョン改定が予定されていることからも、「セキュリティ成熟度」測定の指標も時代と共に変化する可能性があります。重要なことは自社のセキュリティ対策が組織的に実施されていること、また継続的に改善が施されていることです。さらに定期的な確認を通して、改善のための課題や阻害要因を特定していくことも求められます。

ランサムウェアやビジネスメール詐欺による被害が、企業規模に依らず発生していたことも注目すべき点です。攻撃者がセキュリティ体制に弱点を持つ組織を手当たり次第に攻撃している状況を踏まえると、どのような組織も例外なく「セキュリティ成熟度」の向上に取り組む必要性があります。上述の通り、何よりも自社の「セキュリティ成熟度」を把握し、セキュリティ対策の優先度を決定することが推奨されます。その上で実際の対策にあたっては、

・自社内の資産の業務停止などのリスクを評価し、それら資産の保護優先度を設定する

・定期的な防御体制全体の見直しを行う

・自社内の攻撃の検知に必要となる時間を計測し短縮を図る

・実際に攻撃が発生した場合のシナリオに基づいた訓練を実施する

・資産のリスクに応じた復旧目標と計画を定める

など、今回のNIST CSFに規定される5つの機能それぞれの「セキュリティ成熟度」向上に向けた最適な準備が必要です。

なお、今回より重要性が明らかになった点として、サイバー攻撃被害発生後の「検知」「対応」「復旧」の機能が挙げられます。実際にインシデント発生後に強化しておくべきだったと感じた機能でも事前対応の「防御」に迫る形で「検知」が2番目に回答を集めました。また検知期間が業務停止期間に有意に影響していることも確認されました。さらにセキュリティ成熟度の被害への影響の大きな点として「対応」が挙げられました。これらの事実は国内で ISO/ICE 27001 / 27002 など事前防御の部分に関わるガイドラインが主流な状況において重要な点と言えます。エンドポイントなど従来のIT環境にセキュリティ製品を導入することだけで安心するのではなく、より踏み込んだ一歩として、被害後の「検知」「対応」「復旧」手順を整備し、訓練しておくことや、それらの事後対応を円滑にサポートするソリューションプラットフォームを選択することを優先的な投資対象とすることを推奨いたします。

最後に付録として「セキュリティ成熟度」を調査した設問票を下記に掲載します。自社の対策状況の測定や他社平均と比べた際の相対的な「セキュリティ成熟度」の把握にお役立ていただければ幸いです。

(付録)セキュリティ成熟度調査の設問表

■成熟度
4: 会社が定める正式手順に従って、包括的な取り組みが行われており、定期的な改善を図っている
3: 会社が定める正式手順に沿って、包括的な取り組みが行われている
2: 会社が定める正式手順に沿って、部分的に取り組みが行われている
1: 会社が定める正式手順はなく、個人の裁量で取り組んでいる
0: 全くしていない

設問			成熟度
機能	カテゴリ	あるべき状態	
識別	資産管理	データ、デバイス、システム、アプリケーションなどの情報資産を、重要度に応じて管理している	
	ビジネス管理	自組織のサービスや事業などの優先順位付けを行い、リスクマネジメントの意思決定に利用している	
	ガバナンス	サイバーセキュリティ上の役割と責任を、経営層と共に明確化している	
	リスクアセスメント	ビジネスおよび資産が保有するサイバーリスク（脆弱性および内外の脅威）を特定している	
	リスクマネジメント戦略	サイバーリスクの許容度を、組織の利害関係者の間で合意を取って決めている	
防御	ID管理・アクセス制御	資産へのアクセスは、アクセスのリスクレベルに応じた追加の認証（多要素など）をもって制限している	
	トレーニング	自組織の社員に対して、セキュリティポリシーを遵守してもらうための教育やトレーニングをしている	
	データセキュリティ	情報資産に対する管理策（バックアップや暗号化など）を情報の重要度に応じて設定している	
	脆弱性対応	自組織が利用するシステムで脆弱性が発覚した際に、自組織のリスク許容度に応じた対応判断をしている	
	保護技術	リスクの高いファイルやアクティビティ（マクロ実行など）は、ポリシーやセキュリティソリューションによって制限している	
検知	検知対象	ログやテレメトリの記録対象をセキュリティポリシーに則って決めている	
	異常とイベント	ネットワークの正常な通信、ユーザごとに想定される正常なふるまいのベースライン（閾値）を決めている	
	相関分析	複数のセキュリティレイヤーからセキュリティイベント情報が収集され、相互に分析している	
	ユーザ監視	ユーザやアカウントのふるまい、およびネットワーク通信の不審な動作を検知できるようモニタリングしている	
	プロセステスト	セキュリティイベントの検知プロセスが正常に動作するかどうか、何らかの方法でテストしている	
対応	対応計画	インシデントが発生した際に、タイムリーかつ確実に対応できるよう、複数のシナリオを設定し、対応プロセスを決めている	
	役割の明確化	タイムリーに対応できるよう、対応計画に関わる各社内関係者の役割を決めている	
	コミュニケーション	インシデントに関する情報を、定められた対応計画にしたがって社内に報告・共有している	
	分析	発生したインシデントの影響範囲を特定している	
	対応計画改善	インシデント対応計画の有効性を訓練などを行うことで、検証している	
復旧	復旧プロセス	影響をうけたシステムや資産の重要度に応じた復旧プロセスを決めている	
	復旧目標の策定	影響をうけたシステムや資産の重要度に応じた復旧目標（ＲＴＯ／ＲＰＯ／ＭＴＤ）を決めている	
	役割の明確化	迅速にプロセスが実行されるよう、復旧計画に関わる各社内関係者の役割を決めている	
	対外コミュニケーション	インシデント発生時の対外的なコミュニケーション活動方針を定めている	
	計画の合意	復旧計画の方針を、社内関係者だけでなく経営陣や役員と合意を取って決めている	

本書に記載されている各社の社名、製品名、およびサービス名は、各社の商標または登録商標です。TRENDMICROは、記載内容は2023年MM月現在のものです。内容は予告なく変更になる場合があります。

TRENDMICRO、TREND MICRO、ウイルスバスター、InterScan、INTERSCAN VIRUSWALL、InterScanWebManager、InterScan Web Security Suite、PortalProtect、Trend Micro Control Manager、Trend Micro MobileSecurity、VSAPI、Trend Park、Trend Labs、Network VirusWall Enforcer、Trend Micro USB Security、InterScan Web Security Virtual Appliance、InterScan Messaging Security Virtual Appliance、Trend Micro Reliable Security License、TRSL、Trend Micro Smart Protection Network、SPN、SMARTSCAN、Trend Micro Kids Safety、Trend Micro Web Security、Trend Micro Portable Security、Trend Micro Standard Web Security、Trend Micro Hosted Email Security、Trend Micro Deep Security、ウイルスバスタークラウド、スマートスキャン、Trend Micro Enterprise Security for Gateways、Enterprise Security for Gateways、Smart Protection Server、Deep Security、ウイルスバスター ビジネスセキュリティサービス、SafeSync、Trend Micro NAS Security、Trend Micro Data Loss Prevention、Trend Micro オンラインスキャン、Trend Micro Deep Security Anti Virus for VDI、Trend Micro Deep Security Virtual Patch、SECURE CLOUD、Trend Micro VDIオプション、おまかせ不正請求クリーンナップサービス、Deep Discovery、TCSE、おまかせインストール・バージョンアップ、Trend Micro Safe Lock、Deep Discovery Inspector、Trend Micro Mobile App Reputation、Jewelry Box、InterScan Messaging Security Suite Plus、おもいでバックアップサービス、おまかせ！スマホお探しサポート、保険&デジタルライフサポート、おまかせ！迷惑ソフトクリーンナップサービス、InterScan Web Security as a Service、Client/Server Suite Premium、Cloud Edge、Trend Micro Remote Manager、Threat Defense Expert、Next Generation Threat Defense、Trend Micro Smart Home Network、Retro Scan、is702、デジタルライフサポート プレミアム、Airサポート、Connected Threat Defense、ライトクリーナー、Trend Micro Policy Manager、フォルダシールド、トレンドマイクロ認定プロフェッショナルトレーニング、Trend Micro Certified Professional、TMCP、XGen、InterScan Messaging Security、InterScan Web Security、Trend Micro Policy-based Security Orchestration、Writing Style DNA、Securing Your Connected World、Apex One、Apex Central、MSPL、TMOL、TSSL、ZERO DAY INITIATIVE、Edge Fire、Smart Check、Trend Micro XDR、Trend Micro Managed XDR、OT Defense Console、Edge IPS、Trend Micro Cloud One、スマスキャ、Cloud One、Cloud One - Workload Security、Cloud One - Conformity、ウイルスバスター チェック！、Trend Micro Security Master、Trend Micro Service One、Worry-Free XDR、Worry-Free Managed XDR、Network One、Trend Micro Network One、らくらくサポート、Service One、超早得、先得、Trend Micro One、Workforce One、Security Go、Dock 365、およびTrendConnectは、トレンドマイクロ株式会社の登録商標です。 BR-REPO-092

トレンドマイクロ株式会社

www.trendmicro.com

東京本社
〒160-0022
東京都新宿区新宿4-1-6　JR新宿ミライナタワー
TEL：03-4330-7600
FAX：03-4330-7592

大阪営業所
〒532-0003
大阪府大阪市淀川区宮原 3-4-30 ニッセイ新大阪ビル 13 階
TEL：06-6350-0330
FAX：06-6350-0591

名古屋営業所
〒460-0002
愛知県名古屋市中区丸の内 3-22-24 名古屋桜通ビル 7 階
TEL：052-955-1221
FAX：052-963-6332

福岡営業所
〒812-0011
福岡県福岡市博多区博多駅前 2-3-7 シティ 21 ビル 7 階
TEL：092-471-0562
FAX：092-471-0563