Press Release

2024 年 12 月 10 日

過去3年間で70.9%がサイバー攻撃を経験、3年間の累計被害額は平均1.7億円、ランサムウェア被害経験企業では平均2.2億円

～セキュリティ成熟度と被害の実態調査 2024～

トレンドマイクロ株式会社（本社：東京都新宿区、代表取締役社長 兼 CEO：エバ・チェン　東証プライム：4704）と特定非営利活動法人 CIO Lounge（所在地：大阪府大阪市北区、理事長：矢島孝應）は、過去 3 年間でサイバー攻撃を経験している、国内の法人組織（従業員 500 名以上）の経営者、セキュリティやリスクマネジメントの責任者（部長以上）300 人を対象に「セキュリティ成熟度と被害の実態調査 2024」を実施しました※1。

※1 調査結果のパーセンテージは、小数点以下第二位を四捨五入した数値です。合計が 100%にならない場合があります。

サイバー攻撃による法人組織の被害状況調査レポート全文はこちら

■調査結果トピックス

- 過去 3 年間で 70.9%がサイバー攻撃を経験、最も被害コストが大きかったサイバー攻撃はビジネスメール詐欺（BEC）が 18.3%で最多、ランサムウェア攻撃が 13.0%で次点
- 過去 3 年間のサイバー攻撃の累計被害額は平均約 1 億 7 千 1 百万円、ランサムウェア被害を経験した法人組織の累計被害額は平均約 2 億 2 千万円
- サイバー攻撃による業務停止期間は平均 6.1 日、ランサムウェア攻撃による業務停止期間は平均 10.2 日
- サイバー攻撃対策の強化を重要視しているが、阻害要因により 33.3%の組織が実施できず

● 過去 3 年間で 70.9%がサイバー攻撃を経験、被害コストが最も大きかったサイバー攻撃はビジネスメール詐欺

過去 3 年間におけるサイバー攻撃の経験有無を聞いたところ（n=556）※2、経験したと回答した割合は 70.9%でした。サイバー攻撃を経験した回答者から本調査の対象である経営者、セキュリティやリスクマネジメントの責任者（部長以上）（n=300）に対して被害コストが最も大きかったサイバー攻撃を聞いたところ、ビジネスメール詐欺が 18.3%で最多、ランサムウェア攻撃が 13.0%で次点となっています。また、全体では 61.6%がサイバー攻撃によって何らかの実被害を受けています。

この結果から、組織においては、サイバー攻撃は「もし起きたら」ではなく起きる前提での対策を進めていく必要性が高まっていると言えます。経営層は、サイバーリスクがビジネスに実被害をもたらすビジネスリスクであることを再認識したうえで、サイバー攻撃への対策が求められます。

※2 本設問のみスクリーニング時点での集計結果であり、セキュリティやリスクマネジメント責任者（部長職以上）でない回答者を含みます。

図1：サイバー攻撃の被害有無（n=556）
質問「お勤め先の会社が過去3年間に外部から受けたサイバー攻撃のうち
該当するものを全てお答えください。」
（複数回答：「外部からサイバー攻撃は受けていない・わからない」と他の選択肢は排他）

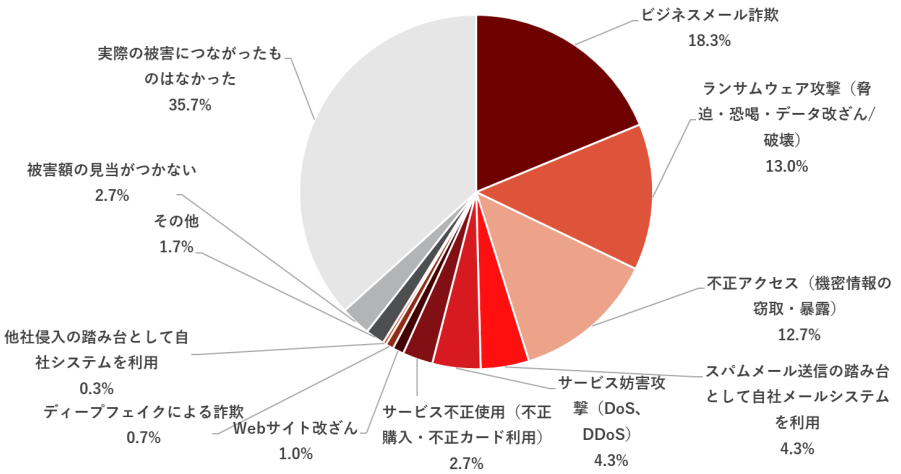

図2：最も被害コストが大きかったサイバー攻撃（n=300）
質問「過去3年間に外部から受けたサイバー攻撃の中で
最も被害コストが大きかったものをお答えください」（単一回答）

●過去 3 年間のサイバー攻撃の累計被害額は平均約 1 億 7 千 1 百万円、ランサムウェア被害を経験した法人組織の累計被害額は平均約 2 億 2 千万円

過去3年間でのサイバー攻撃の被害を経験した法人組織の累計被害額は平均約1億7千1百万円となっています。2023年時点の調査における同被害額は平均約1億2千5百万円であり、前回よりも約4千6百万円増えています。また、被害の公表が日本でも相次いでいるランサムウェア攻撃では、一度でも被害を経験した法人組織の累計被害額は平均2億2千万円となっています。2023年時点の調査における同被害額は平均1億7千6百万円であり、前回よりも約4千4百万円増えています。

昨年度の調査と比較して、被害額が大幅に増加していることから、国内の法人組織においてサイバーリスクが短期間で急激に増大していると考えられます。さらに、本調査は、個別企業における被害額を算出していますが、ランサムウェアによる業務停止や情報流出は、サプライチェーン上の関係組織にも大きな影響を与えます。そのためサプライチェーン全体での被害額は、より大きなものになっていると考えられます。サプライチェーンを狙ったサイバー攻撃によって自社が被害を受けないためにも、脆弱性対応やインシデント発生時におけるセキュリティに関する契約の見直しやアクセス権限やリスク評価などのセキュリティ監査の重要性は高まっています。

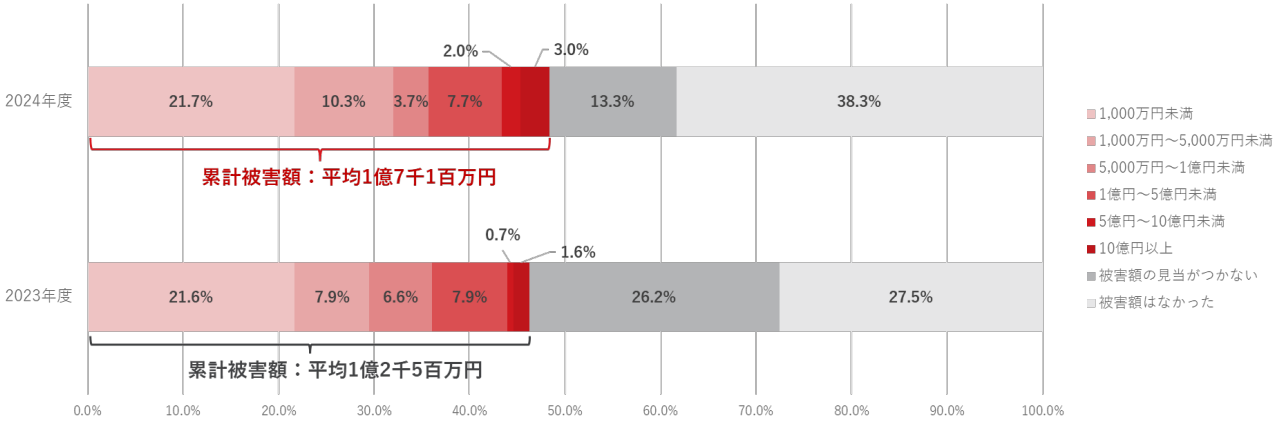

図3：過去3年間の累計被害額
※回答のレンジに一定額をあてはめ平均額を算出
サイバー攻撃の被害経験（2024年度 n=300，2023年度 n=305）
質問「サイバー攻撃によって発生した被害への対応コスト※3の合計金額について
最も近いものをお答えください」（単一回答）

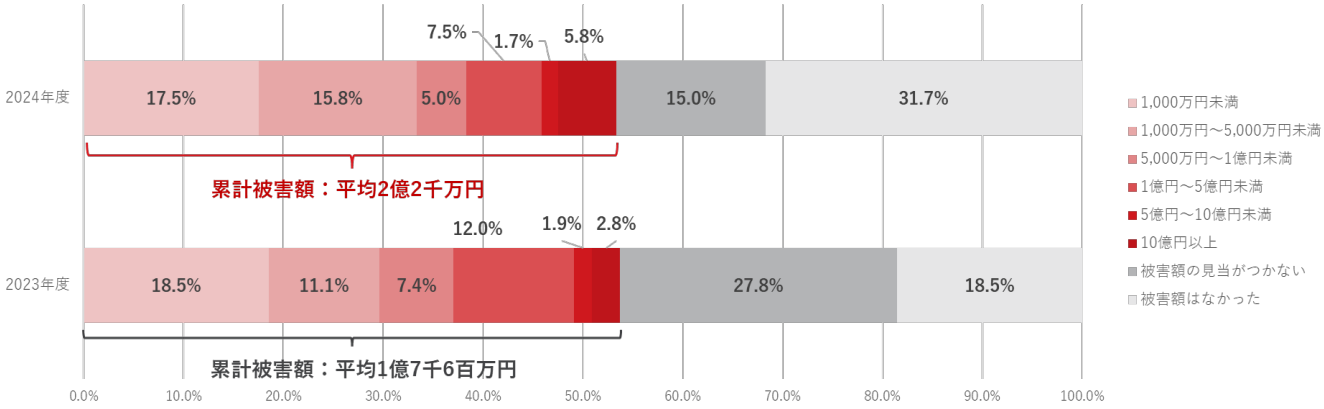

図4：過去3年間の累計被害額
※回答のレンジに一定額をあてはめ平均額を算出
ランサムウェア攻撃の被害経験組織（2024年度 n=120，2023年度 n=108）
質問「サイバー攻撃によって発生した被害への対応コスト※3の合計金額について
最も近いものをお答えください」（単一回答）

※3 本調査における対応コストは以下の合計と定義しています。
①直接コスト（例：不正送金、身代金支払い、業務停止期間の売上、コンサル料、補償金）
②復旧コスト（例：被害範囲の特定、データやシステムの復旧人件費）
③再発防止コスト（例：セキュリティ対策強化、追加投資）

●サイバー攻撃による業務停止期間は平均 6.1 日、ランサムウェア攻撃による業務停止期間は平均 10.2 日

過去3年間で、最も対応コストが大きかったサイバー攻撃からの復旧に要した時間を聞いたところ、平均で6.1日であることがわかりました。また、最も対応コストが大きかったサイバー攻撃がランサムウェア攻撃の場合、復旧に要した時間は、平均で10.2日となっています。

2024年においても、ランサムウェア攻撃等によって、長期的な業務停止を強いられている事例が複数発生している状況です。業務停止の影響は直接的な経済的損失だけでなく、顧客や取引先との信

頼関係を損なうリスクも伴います。特に長期間の業務停止は、ブランドイメージの低下や顧客の流出につながる可能性があるため、企業はサイバーレジリエンス（復旧力）を意識した体制を構築することが求められます。

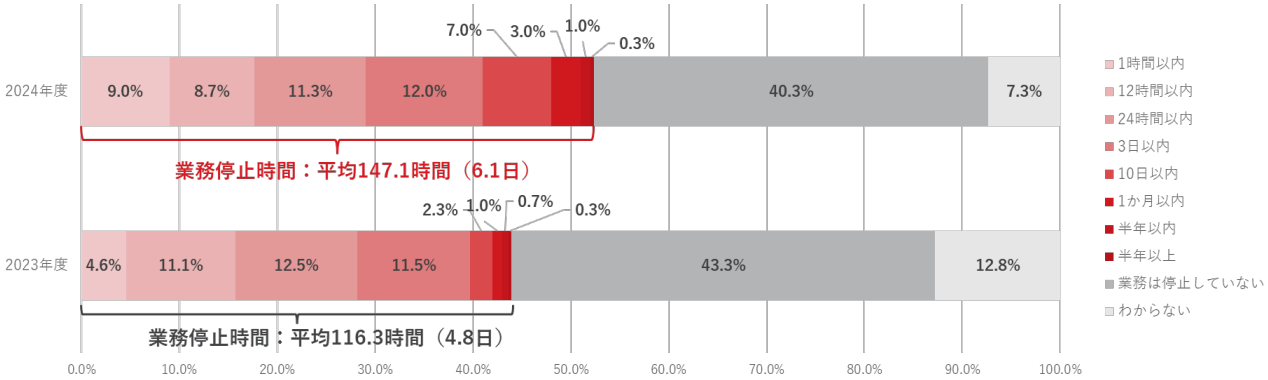

図5：サイバー攻撃の被害による業務停止期間
※回答のレンジに一定時間をあてはめ業務停止時間の平均を算出
業務停止期間（2024年度 n=300，2023年度 n=305）
質問「最も被害額が大きかったサイバー攻撃について、
それぞれどれくらいの時間がかかりましたか。最も近いものをお答えください」（単一回答）

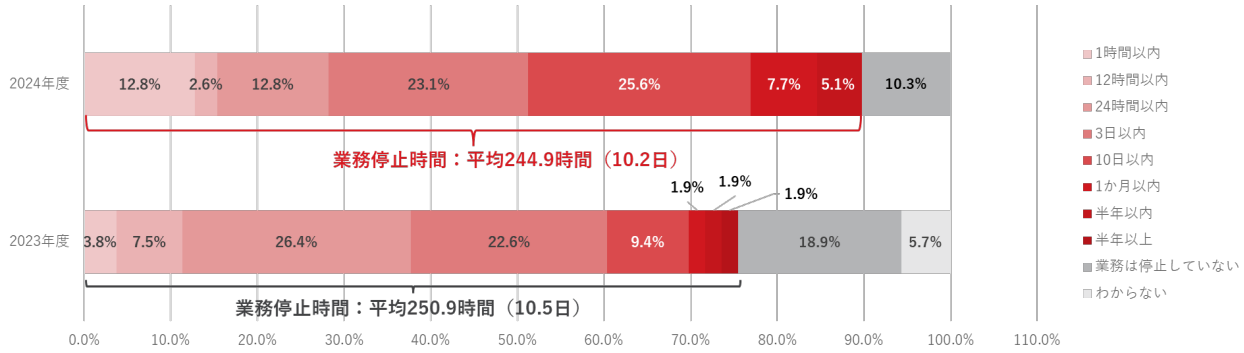

図6：ランサムウェアによる業務停止期間
※回答のレンジに一定時間をあてはめ業務停止時間の平均を算出
業務停止期間（2024年度 n=35，2023年度 n=40）
質問「最も被害額が大きかったサイバー攻撃について、
それぞれどれくらいの時間がかかりましたか。最も近いものをお答えください」（単一回答）

●サイバー攻撃対策の強化を重要視しているが、阻害要因により 33.3%の組織が実施できず

サイバー攻撃のインデント対応後に強化が必要だと感じた機能について、「NIST サイバーセキュリティフレームワーク 2.0」の各機能の中では、防御が 42.0%で最多でした。さらに、強化が不足していた理由を聞いたところ「対策事項として重要視していたが、阻害要因があった」が 33.3%、「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」が 32.7%と、一定以上の割合が対策事項を重要視していたにも関わらず、それを強化できなかった事情があることがわかりました。

この結果は、組織内でセキュリティ対策の重要性は認識されているものの、実装に至る過程で様々な課題に直面していることを示唆しています。単なる技術的な課題ではなく、人的リソースの制約、さらには組織としての優先順位付けに関する問題が背景にあると考えられます。このような状況を改善するためには、セキュリティ部署が「技術的な必要性」だけでなく、「ビジネスインパクト」の観点から説明できることが重要だと考えられます。経営層が理解しやすい形でセキュリテ

ィリスクと対策の重要性を示していくことが求められています。

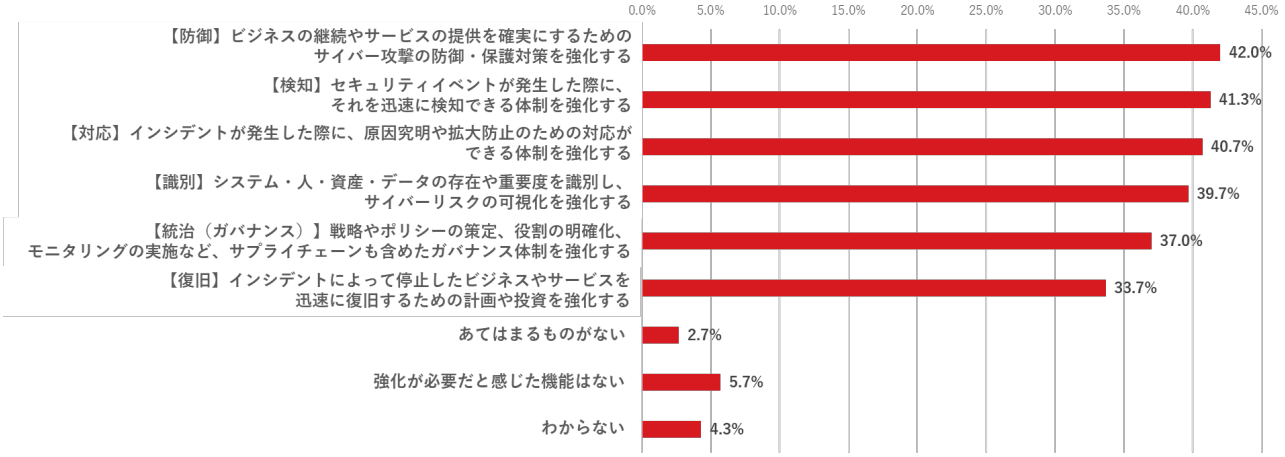

図7：インシデント対応後に強化が必要だと感じた機能（n=300）
質問「最も被害額が大きかったサイバー攻撃へのインシデント対応後に
強化が必要だと感じた機能をお答えください。」（複数回答）

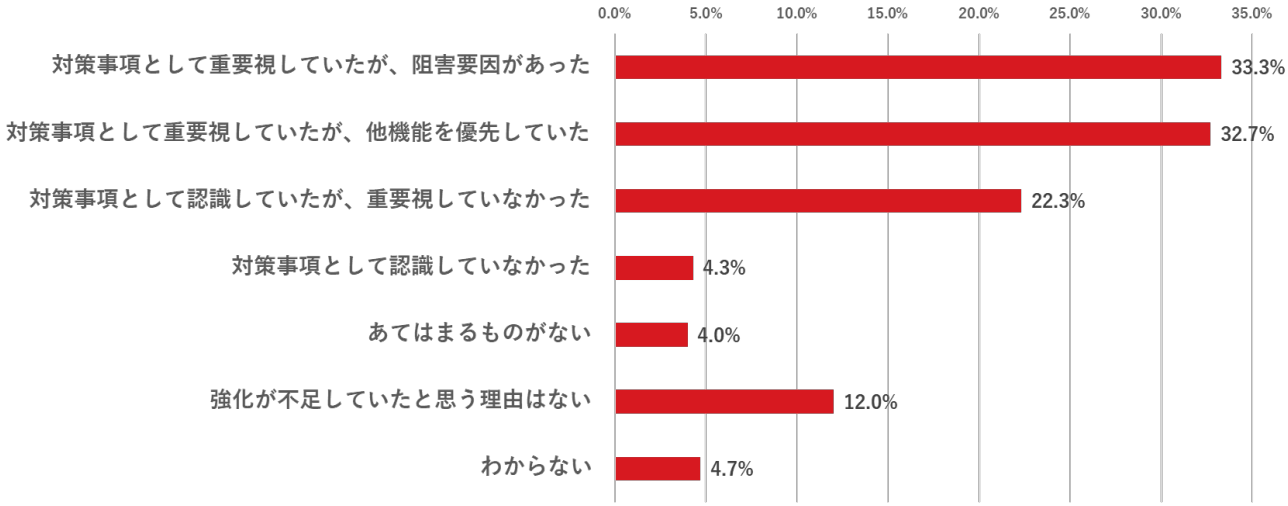

図8：インシデント対応後に強化が不足していた要因（n=300）
質問「インシデント対応後に強化が必要だと感じた機能に関して
なぜ強化が不足していたと思いますか」（複数回答）

■調査概要

調査手法（サンプリング）	インターネット調査
調査地域	日本国内
調査対象者	過去3年間でサイバー攻撃を経験している、従業員規模500名以上の法人組織の経営者、セキュリティやリスクマネジメントの責任者（部長以上）
回答者数	300
調査時期	2024年9月
調査主体	トレンドマイクロ株式会社、特定非営利活動法人 CIO Lounge

※ 2024年12月10日現在の情報をもとに作成したものです。今後、内容の全部もしくは一部に変更が生じる可能性があります。

本件に関するお問合せ先
マーケティング本部 広報グループ
成田・高橋・中村・牧野
e-mail：pressweb@trendmicro.com
Web ページ:https://www.trendmicro.co.jp

商品に関するお問合せ先
営業 TEL　　：03－4330－7601
紙誌面掲載用 TEL：03－4330－7601