過去 3 年間で 56.8%がサイバー攻撃の被害を経験、3 年間の累計被害額は平均 1.3 億円、

ランサムウェア被害経験企業では平均 1.8 億円

―サイバー攻撃による法人組織の被害状況調査―

2023 年 11 月 1 日
トレンドマイクロ株式会社
特定非営利活動法人 CIO Lounge

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、国内の法人組織（従業員 500 名以上）に勤めるセキュリティやリスクマネジメントの責任者（部長職以上）305 人を対象に「サイバー攻撃による法人組織の被害状況調査」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
https://resources.trendmicro.com/jp-docdownload-form-m624-web-security-maturity-damage-2023.html

■調査結果トピックス

- **過去 3 年間で 56.8%がサイバー攻撃の被害を経験、**
  被害コストが最も大きかったサイバー攻撃はランサムウェア
- **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、**
  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 1 億 7689 万円
- **サイバー攻撃による業務停止期間、国内拠点では平均 4.5 日、海外拠点では平均 7.0 日**
- **セキュリティ対策の阻害要因は「スキル人材の不足」が最多で 74.4%**

- **過去 3 年間で 56.8%がサイバー攻撃の被害を経験、**
  被害コストが最も大きかったサイバー攻撃はランサムウェア

過去 3 年間におけるサイバー攻撃の被害経験有無を聞いたところ※2、経験したと回答した割合は 56.8%でした。サイバー攻撃の被害を経験した回答者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、ランサムウェアが 17.4%で最多となっています。

世界各国で被害が確認されているランサムウェアですが、その特性上、被害が深刻化しやすくなっています。近年、国内においても、組織の事業継続に大きな影響が出るランサムウェア被害も多数報告されているため、より一層注意と対策が必要になっています。経営層は、サイバーリスクが事業継続に関わるビジネスリスクであることを再認識したうえで、ランサムウェアを始めとするサイバー攻撃への対策が求められます。

※2 本調査において、本設問のみ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

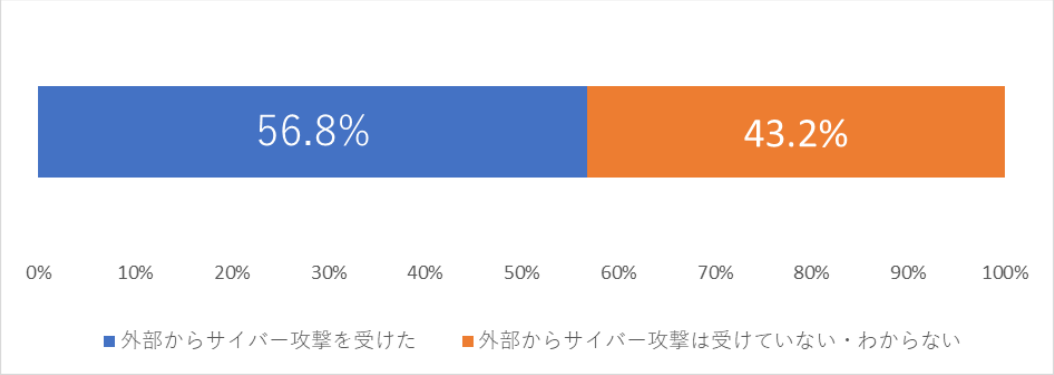

図 1：サイバー攻撃の被害有無（n=628）
質問「お勤め先の会社が過去 3 年間に外部からサイバー攻撃を受けましたか」

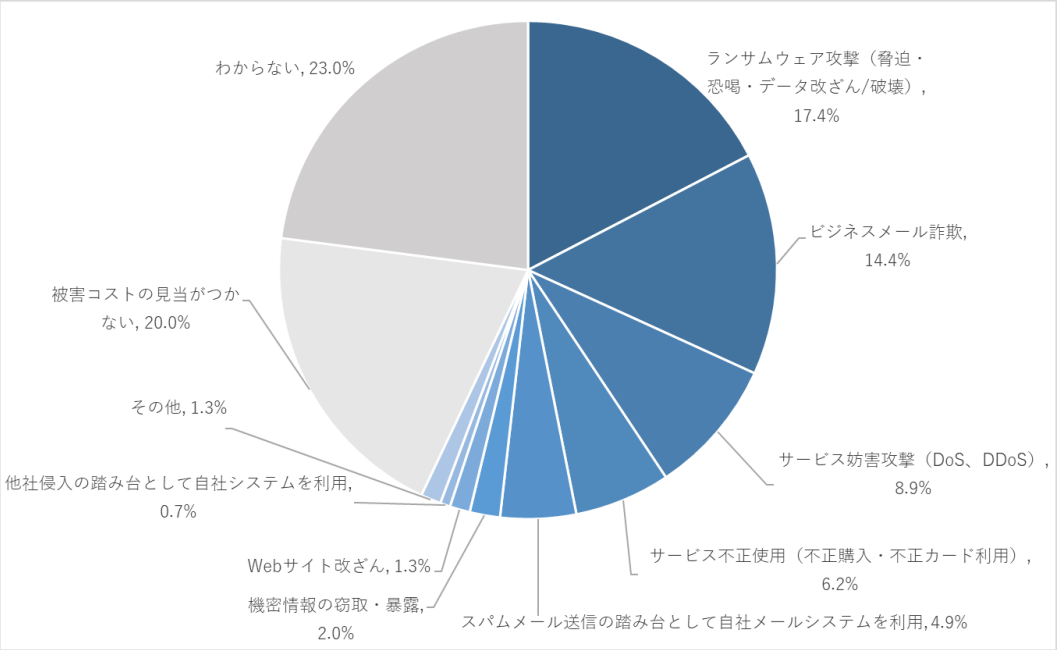

図 2：最も被害コストが大きかったサイバー攻撃（n=305）
質問「過去 3 年間に外部から受けたサイバー攻撃の中で
最も被害コストが大きかったものをお答えください」

● **過去 3 年間でのサイバー攻撃の累計被害額は平均 1 億 2528 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 1 億 7689 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 1 億 2528 万円となっています。また、一度でも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 1 億 7689 万円となっており、被害規模の観点においてランサムウェアが大きな脅威となっていることが明らかになりました。

本調査では、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、ビジネスサプライチェーンの関係組織にも影響することから、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ると考えられます。ランサムウェアの被害リスクを低減していくために、自社のセキュリティ強化だけではなく、サプライチェーン全体でのセキュリティレベルの向上が求められます。

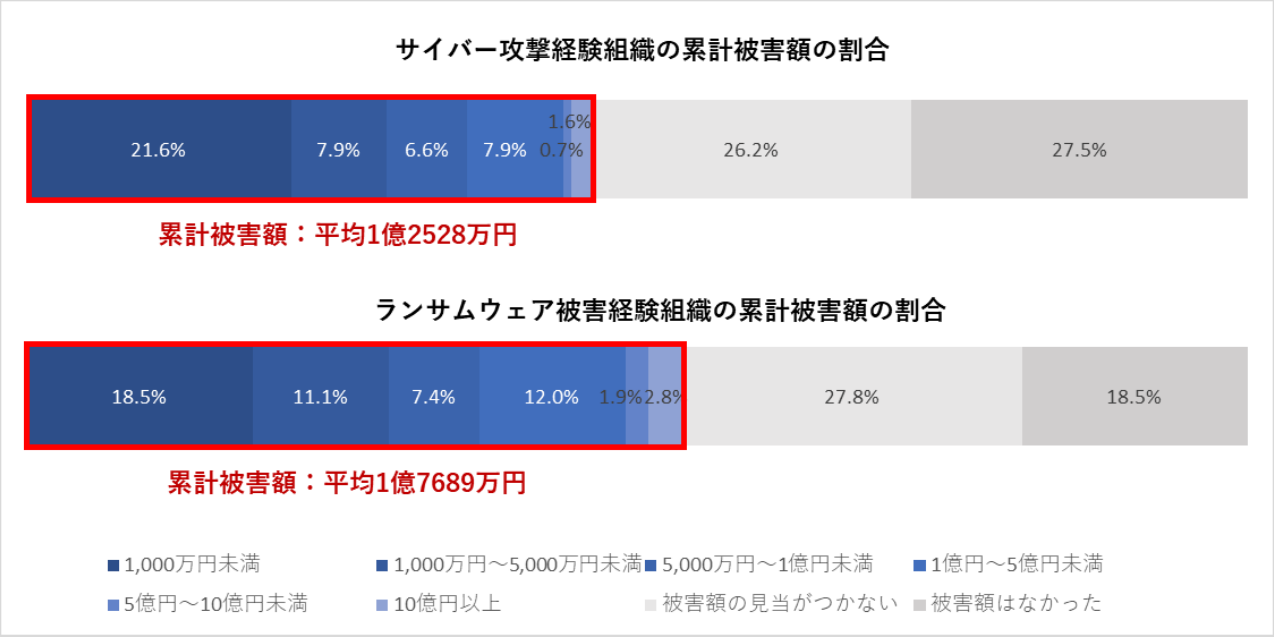

図 3：過去 3 年間の累計被害額
サイバー攻撃の被害経験（n=305）、ランサムウェア被害経験（n=108）
質問：「サイバー攻撃によって発生した被害への対応コスト※3 の合計金額について、
最も近いものをお答えください」

※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、国内拠点では平均 4.5 日、海外拠点では平均 7.0 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、国

内拠点で発生した場合は平均 4.5 日であることがわかりました。また、海外拠点で発生した場合は平均で 7.0 日となりました。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であった場合、復旧に要した時間は、国内拠点では平均 13.0 日、海外拠点では平均 15.1 日となり、海外拠点においては、復旧までの期間が長期化しやすくなることが明らかになりました。

海外拠点におけるセキュリティリスクの問題は国内のグローバル企業の多くが抱えています。「セキュリティ対策が行き届かない」「セキュリティガバナンスが浸透しにくい」などの理由により、海外拠点はサプライチェーン上の弱点になりやすくなっています。また、今回の調査から、国内拠点と比べて、サイバーレジリエンス（復旧力・回復力）の観点においても、問題点があることが明らかになりました。サイバー攻撃の被害に遭った際の対応や復旧を見越したインシデント訓練など、被害発生を前提とした対策を、海外拠点を含めた組織全体で行っていくことが求められます。

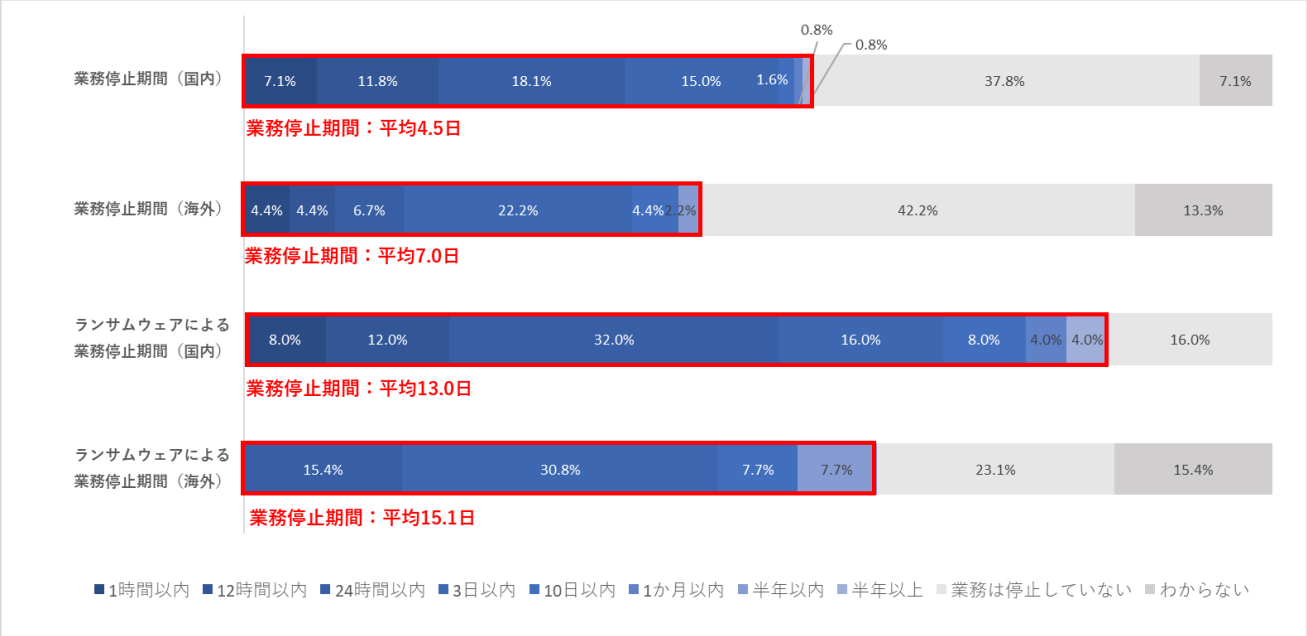

図 4：サイバー攻撃の被害による業務停止期間
業務停止期間（国内）（n=127）、業務停止期間（海外）（n=45）
ランサムウェアによる業務停止期間（国内）（n=25）、ランサムウェアによる業務停止期間（海外）（n=13）
質問「最も対応コストが大きかったサイバー攻撃について、それぞれどれくらいの時間がかかりましたか」

- **セキュリティ対策の阻害要因は「スキル人材の不足」が最多で 74.4%**

セキュリティ対策の阻害要因について聞いたところ「対策を行うためのスキルセットを持つ人材や専門組織が不足」が 74.4%、続いて「対策を行うための人材の数が不足」が 63.3%となりました。

人材については質・数ともに足りていない状況となっており、深刻なセキュリティ人材不足が法人組織の共通の阻害要因となっていることが伺えます。セキュリティ人材の確保を進めるのであれば、専門人材の採用や人材の育成などに取り組む必要がありますが、そのような投資は法人組織にとっては簡単で

はありません。場合によっては、経済産業省が主導するサイバーセキュリティ支援制度を活用するなど、外部委託等も視野に入れていくべきでしょう。

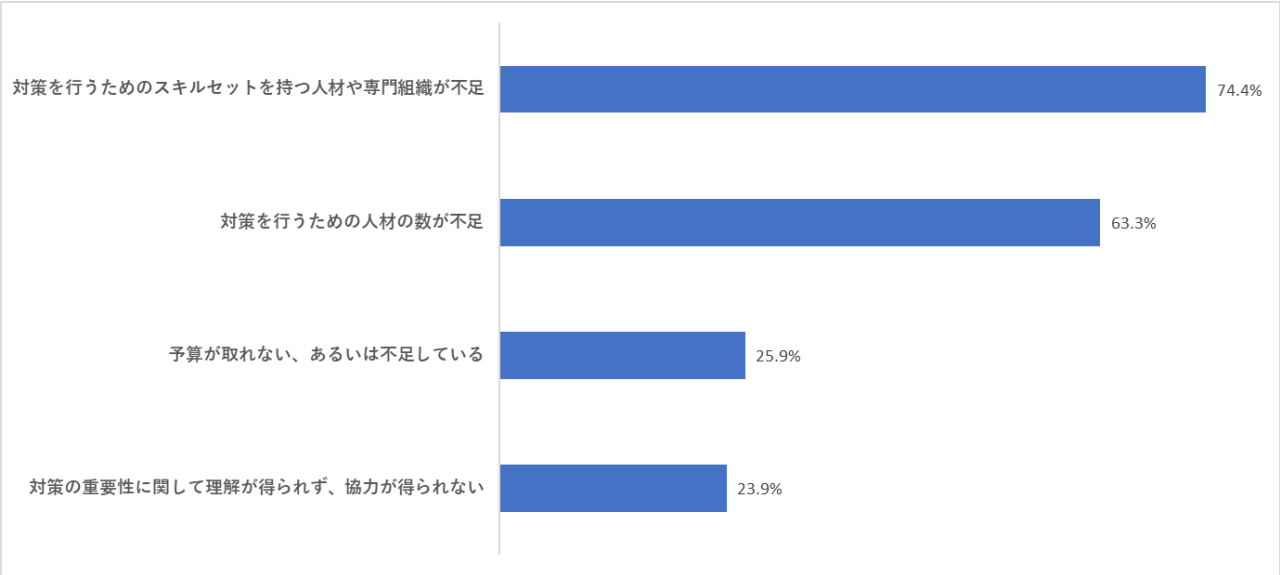

図 5：セキュリティ対策の阻害要因（n=305）
質問「識別」「防御」「検知」「対応」「復旧」のそれぞれの項目において
「対策を行うにあたり、阻害要因と感じることは何ですか」
関連した回答に一度でも選択した回答者数の割合を算出

■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	従業員規模 500 名以上の法人組織にお勤めのセキュリティや リスクマネジメントの責任者（経営層～部長級）
回答者数	305
調査時期	2023 年 6 月
調査主体	トレンドマイクロ株式会社、CIO Lounge

■会社概要

会社名：トレンドマイクロ株式会社
住所：東京都新宿区新宿 4-1-6　JR 新宿ミライナタワー
代表者：代表取締役社長 兼 CEO エバ・チェン
URL：https://www.trendmicro.com/

法人名：特定非営利活動法人 CIO Lounge
住所：大阪市北区大深町 3 番 1 号　グランフロント大阪北館
代表者：理事長　矢島 孝應

URL：https://www.ciolounge.org/

本件に関するお問合せ先
広報グループ
成田・高橋・牧野
e-mail：pressweb@trendmicro.com
TEL：０３－５３３４－３６５８
ホームページ：https://www.trendmicro.com/ja_jp/business.html
※現在、当社はハイブリッドワークを主としているため、電話がつながらない場合は、メールでご一報いただけますと幸いです。

商品に関するお問合せ先
営業　　TEL：０３－５３３４－３６０１
紙誌面掲載用 TEL：０３－５３３４－３６０１

※本リリースは、2023 年 11 月 1 日現在の情報をもとに作成されたものです。