プレスリリース資料

CISO/CSO 相当の設置率は約 7 割、自社サプライチェーンに「サイバー攻撃を受けた」は約 4 割

―サイバーセキュリティに関する調査―

2022 年 7 月 1 日
株式会社日経リサーチ
トレンドマイクロ株式会社

株式会社日経リサーチ（本社：東京都千代田区、代表取締役社長：新藤政史）と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　東証プライム：4704）は、国内の大企業（従業員 1,000 名以上）に勤めるセキュリティ責任者・DX 責任者（経営層～部長級）を対象に「サイバーセキュリティに関する調査」を実施し、調査結果を発表しました。

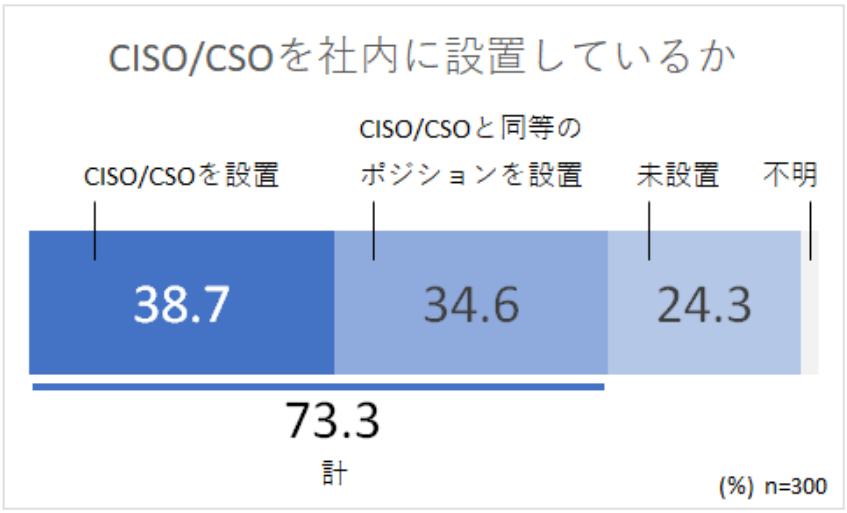
■調査結果トピックス

- **国内大企業の CISO/CSO 設置率は 38.7%（同等ポジションを含むと 73.3%）、未設置は 24.3%**
- **自社サプライチェーンに「サイバー攻撃を受けたことがある」43.3%**
- **今のセキュリティ投資額は自社の防衛に対して「不足」41.3%**

国内大企業の CISO/CSO 設置率は 38.7%（同等ポジションを含むと 73.3%）、未設置は 24.3%

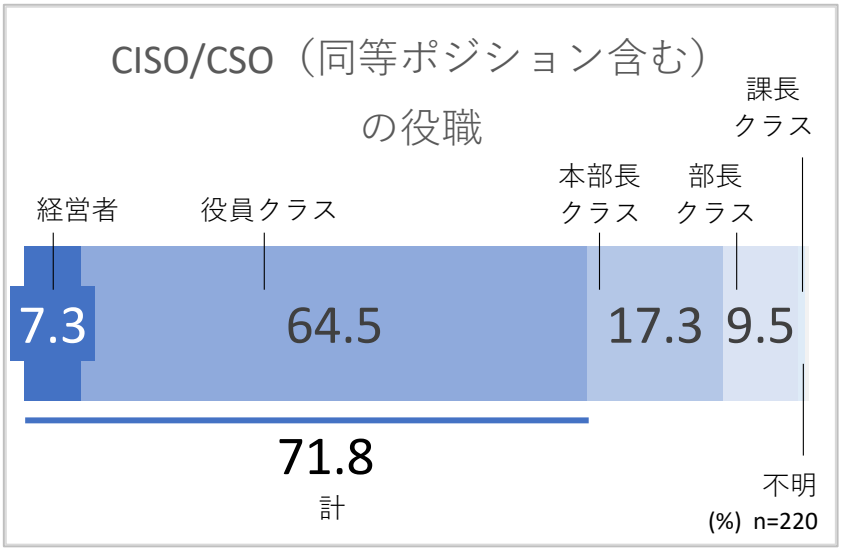
CISO（Chief Information Security Officer、最高情報セキュリティ責任者）または CSO（Chief Security Officer、最高セキュリティ責任者）を社内に設置しているかを聞いたところ、設置していると回答した割合は 38.7%でした。CISO/CSO という呼称とは異なるセキュリティトップのポジション設置を含めると 73.3%にのぼりました。一方で、いずれも設置していないという回答は 24.3%ありました。

デジタルがビジネスの基盤となる現在、サイバーセキュリティの重要性は高まっています。企業の経営層やそれに準ずる役職者はその重要性を認識し、リーダーシップを発揮することが求められます。しかし、情報システム部の設置やセキュリティ担当を配置するだけでは権限が不足し、経営レベルでサイバーセキュリティ戦略を検討することが困難になることが推察できます。そのため、権限と責任を持った CISO や CSO といったポジションを設置し、適切なサイバーセキュリティ戦略を立案、推進する必要があります。

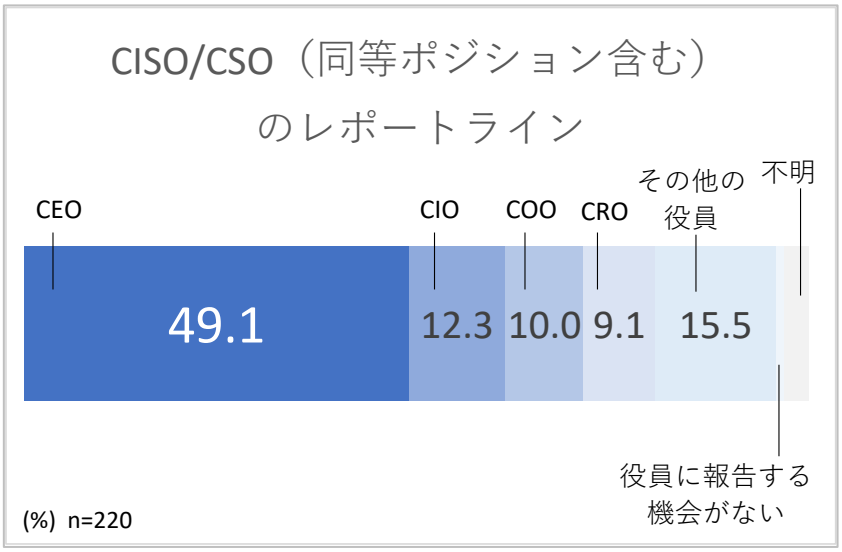


（数字は小数点第二位を四捨五入した数値です。合計 100%とならない場合があります）

CISO/CSO（呼称の異なる同等ポジションを含む）を設置していると回答した人に、CISO/CSO 自身の役職を聞いたところ、「経営者」が 7.3%、「役員クラス」が 64.5%で、合わせて 7 割以上が経営に関与するポジションを担っていることが分かりました。直接のレポートライン（指揮命令系統）は「CEO（最高経営責任者）」が 49.1%で、「CIO（最高情報責任者）」が 12.3%、「COO（最高執行責任者）」が 10.0%、「CRO（最高リスク管理責任者）」が 9.1%と続きました。



（社内に CISO/CSO を設置、CISO/CSO と同等のポジションを設置と答えた人のみ回答）



（社内に CISO/CSO を設置、CISO/CSO と同等のポジションを設置と答えた人のみ回答）

自社サプライチェーンに「サイバー攻撃を受けたことがある」43.3%

自社の委託先、グループ会社、グローバル拠点いずれかに対して、サプライチェーン（供給網）へサイバー攻撃を受けたことがあるかを聞いたところ、あるという回答が 43.3%を占めました。委託先へのサイバー攻撃は 16.7%、グループ会社へは 30.7%、グローバル拠点へは 28.3%が攻撃を受けたことがあると回答しており、多くの企業が自社のサプライチェーンにサイバー攻撃を受けている実態が明らかになりました。

※サプライチェーンとは、特定の製品・サービスが生産され消費されるまでの一連のプロセスおよびネットワークを指します。

※本調査では、サプライチェーンのステークホルダーを下記のように分類して質問を行っています。

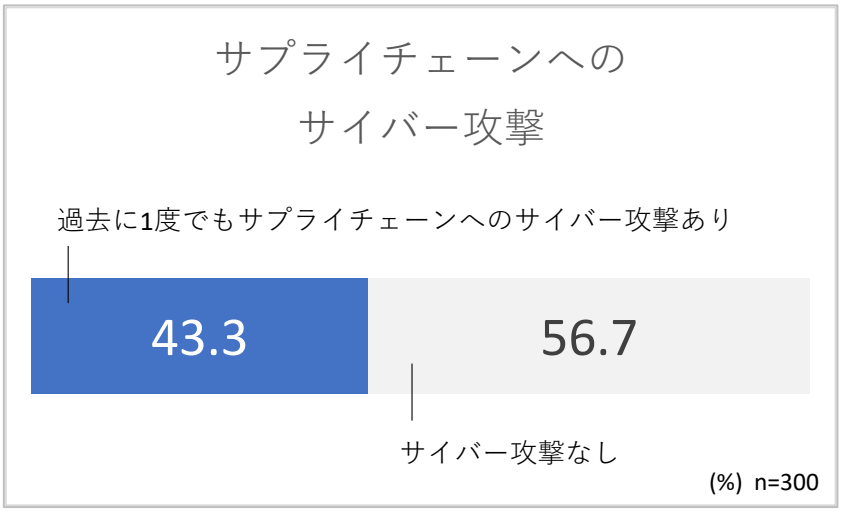
「自社」：本調査への回答者が所属する企業

「取引先」：自社製品・サービスの販売先企業

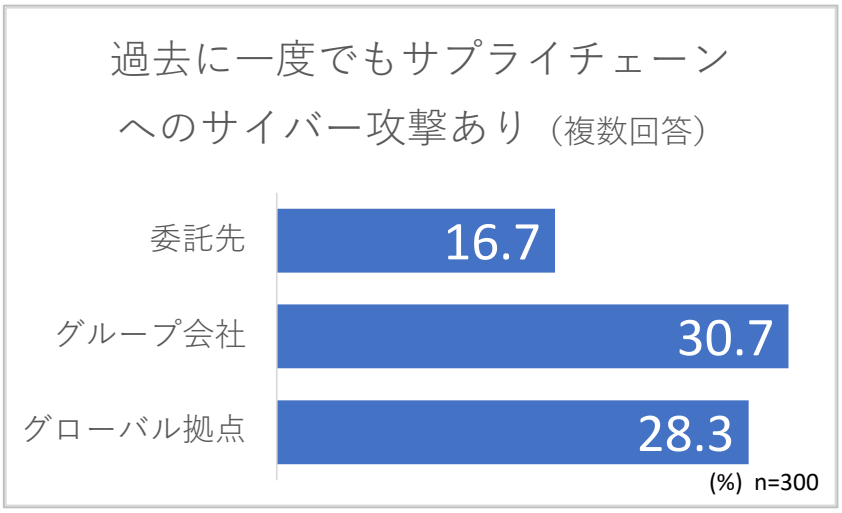
「委託先」：自社にとってのサプライヤー企業

「グループ会社」：自社と資本関係にある企業

「グローバル拠点」：自社の海外拠点

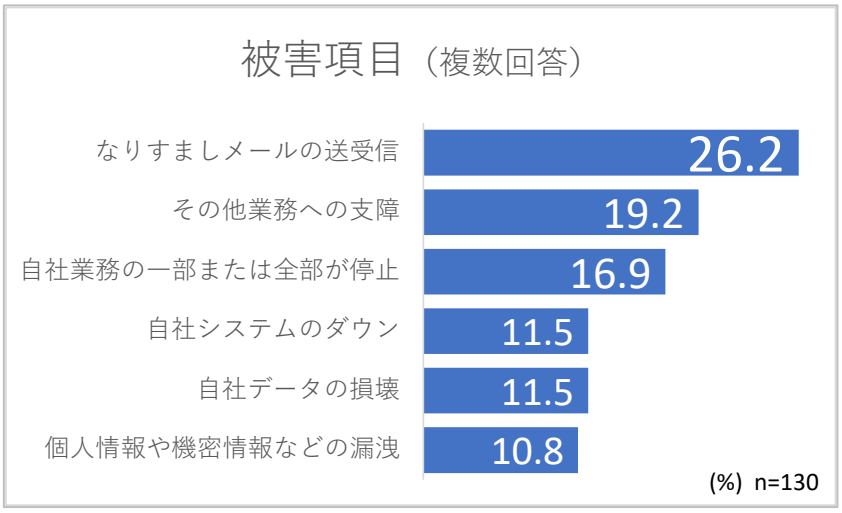


（委託先、グループ会社、グローバル拠点それぞれで聴取し、集計時に統合）

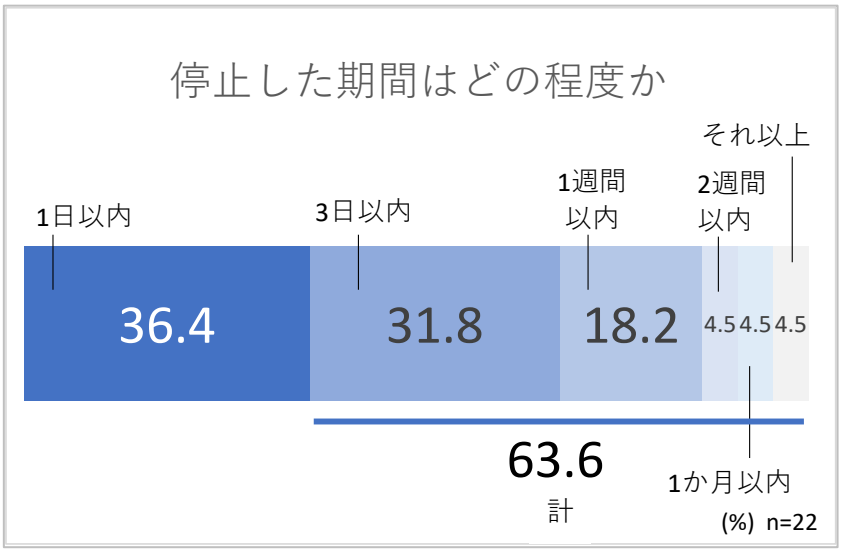


サプライチェーンへサイバー攻撃があった人に、その被害内容を聞いたところ「なりすましメールの送受信」が 26.2%で最も高く「その他業務への支障」が 19.2%、「自社業務の一部または全部が停止」が 16.9%と続きました。業務に支障が出たり停止したりするほどの被害は事業ダメージが大きく、2 割近い数字は無視できない割合です。

また、自社業務の一部または全部が停止したという人に、業務が停止した期間を聞いたところ、復旧に 1 日以上かかった割合は 6 割を超えました（回答者数が 22 人と少ないため、参考値）。一度被害を受け事業が停止すると、復旧までに時間がかかる様子がうかがえます。



（過去に一度でもサプライチェーンへサイバー攻撃があった人のみ回答）
（委託先、グループ会社、グローバル拠点それぞれで聴取し、集計時に統合）



（自社業務の一部/全部が停止した人のみ回答。参考値）

多くの大企業がサプライチェーンに対するサイバー攻撃を受けており、かつ大企業自身もサイバー攻撃による影響を受けていることが今回の調査で明らかになりました。特にランサムウェアなどは、事業や生産活動の停止に至る可能性があります。サプライチェーンへのサイバー攻撃は、自社のセキュリティレベルを向上するだけでは防ぐことが困難なため、委託先、グループ会社、グローバル拠点などサプライチェーン全体でセキュリティレベルを向上していく必要があります。

今のセキュリティ投資額は自社の防衛に対して「不足」41.3%

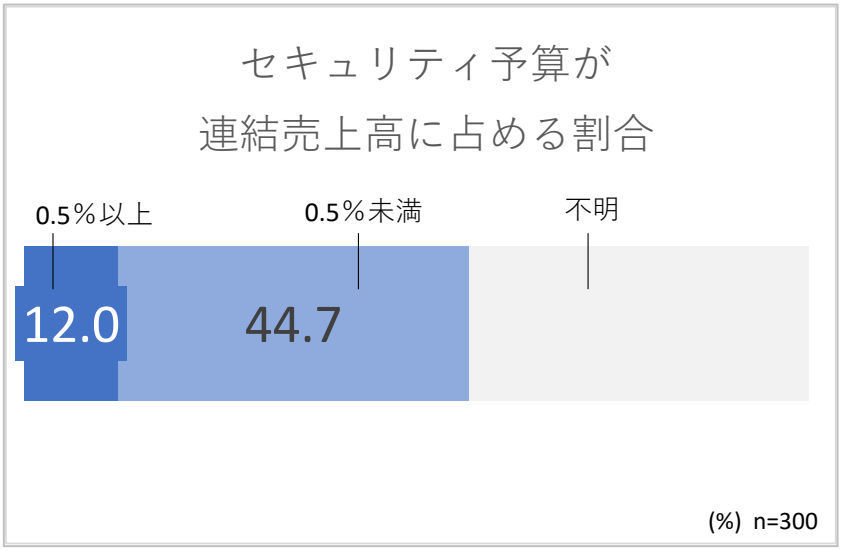
一般財団法人日本サイバーセキュリティ・イノベーション委員会（JCIC）は、企業のセキュリティ投資額は連結売上高の「0.5%以上」を投資すべきとの基準を示しています*。本調査で「お勤め先のセキュリ

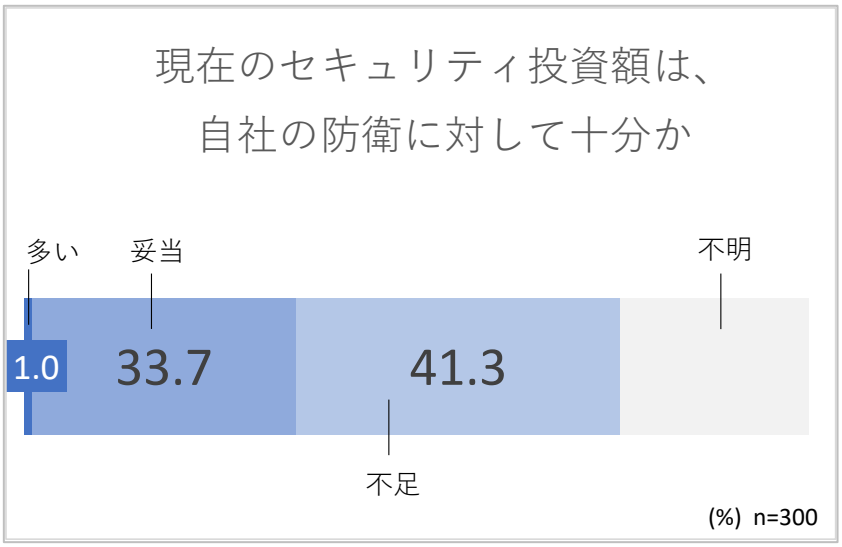
ティ予算が連結売上高に占める割合」を聞いたところ、JCIC が示す 0.5%という基準未満という回答が44.7%で、基準以上という回答（12.0%）を上回っていました。

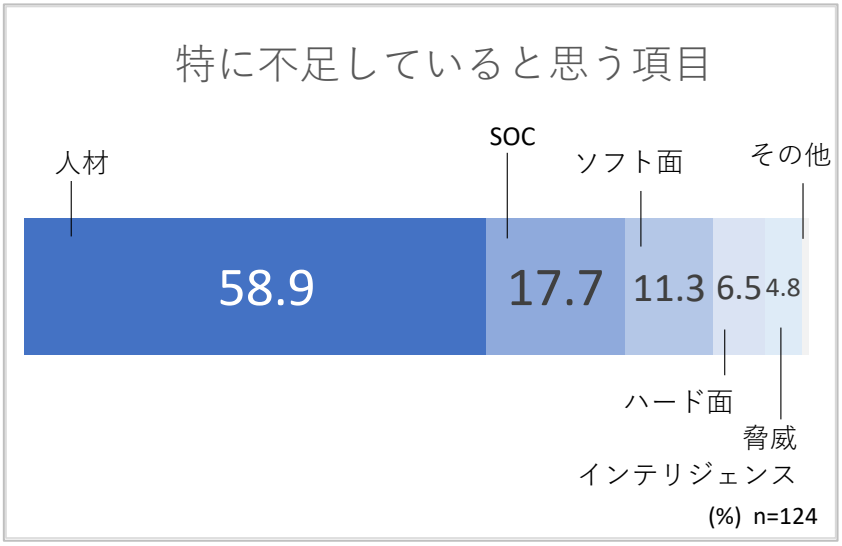
* https://www.j-cic.com/pdf/report/Security-Resources-Report.pdf

現在のセキュリティ投資額が自社の防衛に対して十分だと思うかについては「不足」が 41.3%と「妥当」の 33.7%よりも高く、今の投資額では不足しているという認識が多くあることも分かりました。

自社の防衛に対してセキュリティ投資額が不足していると回答した人に対し、特に不足していると思う項目について聞いたところ「人材」という回答が 58.9%で最も高く、「SOC（サイバー攻撃の検知や分析などを行い、対応策を示す専門組織）」が 17.7%と続きました。







（自社の防衛に対してセキュリティ投資額が「不足」しているとした人のみ回答）

今回の調査では、セキュリティの投資について、最も不足している項目が「人材」となりましたが、企業が DX を推進していく上では、セキュリティの専門人材だけではなく、ビジネスをけん引するビジネス部門がサイバーセキュリティを踏まえて業務を推進していけるプラスセキュリティ人材を確保、育成することが重要です。

■調査概要

調査手法（サンプリング）	インターネット調査（日経リサーチのビジネスパーソン調査サービスを利用）
調査地域	日本国内
調査対象者	従業員規模 1,000 名以上の企業にお勤めのセキュリティ責任者・DX 責任者（経営層～部長級）
回収数	300
調査時期	2022 年 6 月 2 日（木）～8 日（水）
調査主体	株式会社日経リサーチ、トレンドマイクロ株式会社

■会社概要

会 社 名：株式会社 日経リサーチ
住　　所：東京都千代田区内神田 2 丁目 2 番 1 号　鎌倉河岸ビル
代 表 者：代表取締役社長 新藤 政史
事業内容：顧客満足度（CS）調査や、ブランド調査、デジタルマーケティングなど各種市場調査を国内外で幅広く展開しています。また、定期的に実施する世論調査や企業調査の結果は日本経済新聞などの媒体に多く掲載されています。
U R L：https://www.nikkei-r.co.jp/

会 社 名：トレンドマイクロ株式会社
住　　所：東京都渋谷区代々木 2-1-1　新宿マインズタワー
代 表 者：代表取締役社長 兼 CEO エバ・チェン
事業内容：コンピュータ及びインターネット用セキュリティ関連製品・サービスの開発・販売
U　R　L：https://www.trendmicro.com/

【本件に関するお問い合わせ先】　株式会社日経リサーチ　ソリューション本部
担当：持木、大澤
TEL：03-5296-5151（平日 10:00～12:30、13:30～17:30）
メール：nid_survey@nikkei-r.co.jp

※本リリースは、2022 年 7 月 1 日現在の情報をもとに作成されたものです。