

Biz Clip調査レポート(第36回)

企業の情報セキュリティリスク認知調査2023

2023.01.17



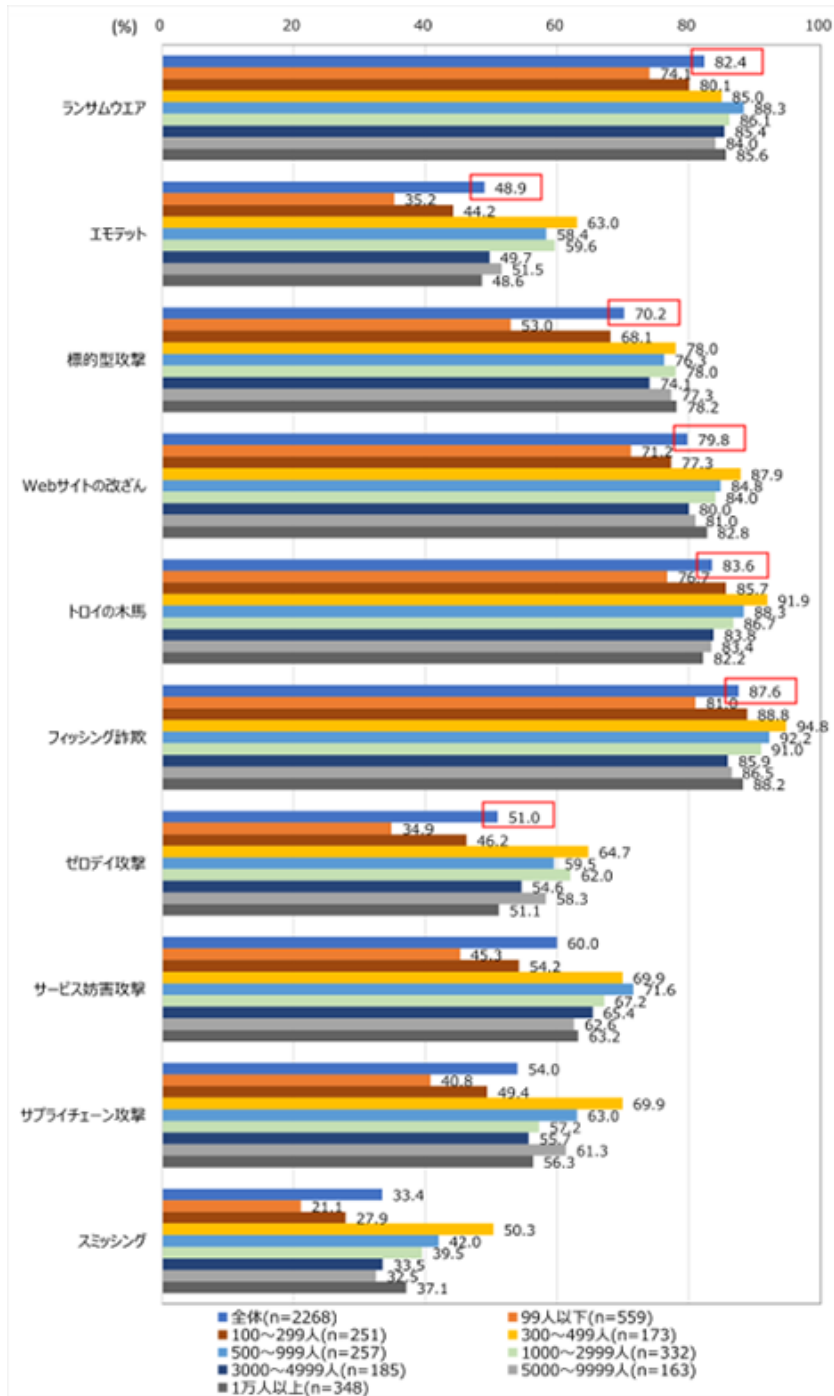
テクノロジーの進化によって、生産性の向上や多様な働き方の実現などの恩恵がもたらされる一方、サイバー攻撃も多様化・複雑化の一途をたどっている。こうした中、攻撃手法などの情報セキュリティリスクをどれくらい認知しているのだろうか。その最新動向について2023年1月に調査を行った(日経BPコンサルティングのアンケートシステムを用い、同社保有の調査モニター2566人を対象に調査を実施)。

「ゼロデイ攻撃」や「エモテット」の認知度はやや低調に

まず情報セキュリティリスクについて、代表的な攻撃手法としてどのようなものを知っているかについて従業員規模別にその認知度を聞いた。最も認知度(「よく知っている(対処法も含め)」「どのようなものか知っている」「なんとなく知っている」と回答した合計値)が高かったのが「フィッシング詐欺」(87.6%)。2位が「トロイの木馬」(83.6%)、3位が「ランサムウェア」(82.4%)となった。そして、4位に「Webサイトの改ざん」(79.8%)、5位に「標的型攻撃」(70.2%)が続いた。

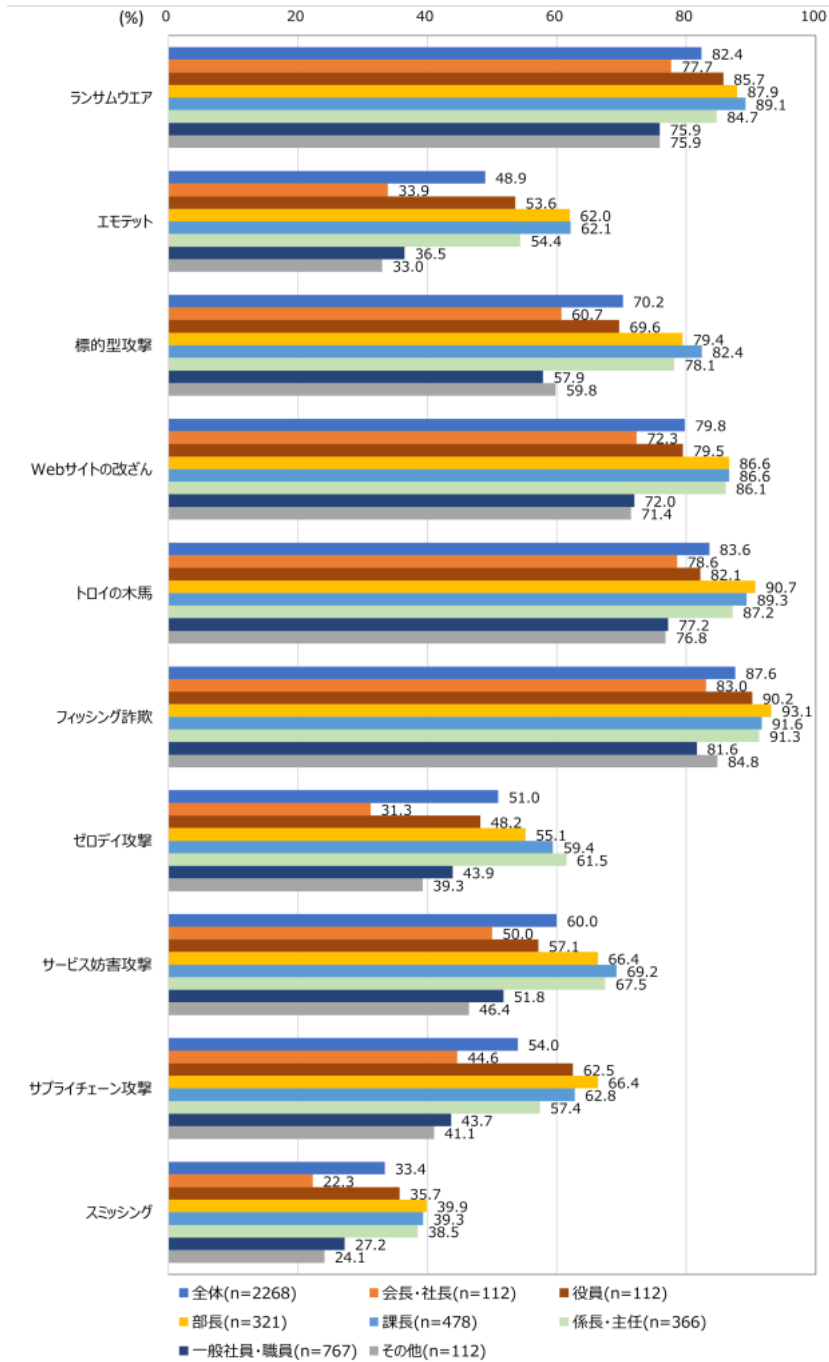
この一方、ソフトウェアのセキュリティホール対策前を狙う「ゼロデイ攻撃」(51.0%)や近年大きな脅威として話題を集めた「エモテット」は48.9%という結果となった。特に300人未満の中小企業において、各脅威について認知度が低い傾向が顕著に表れた(図1-1)。

【図1-1 サイバー攻撃の種類について(従業員規模別)】



続いて、役職別に見た場合ほぼ全ての項目において「経営者(会長・社長)」と「一般社員・職員」の情報セキュリティリスクの認知度の低調が目立つ形となった(図1-2)。

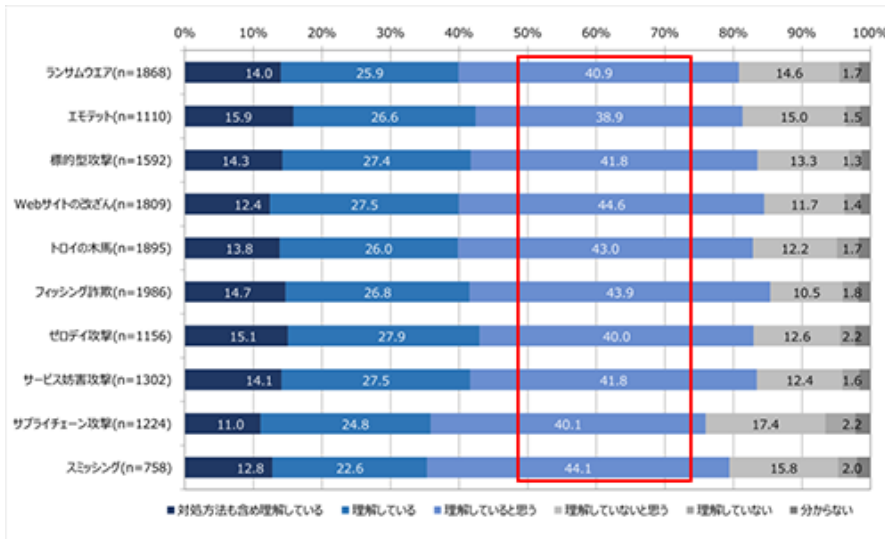
【図1-2 サイバー攻撃の種類について(役職別)】



多様化する攻撃の中、約4割がリスクを「理解していると思う」と回答

ここでは、一歩踏み込んで各攻撃手法の内容について、その理解度を聞いた。「対処方法も含め理解している」という回答について、最も高い値となったのが「エモテット」で15.9%。ここにゼロデイ攻撃が続いた(15.1%)。しかし、全ての項目において約4割が「理解していると思う」と回答しており、多様化・巧妙化するサイバー攻撃への備えの中で、多くの企業が不安を抱えつつも試行錯誤の中で対策を進めている姿が浮かび上がる(図2)。

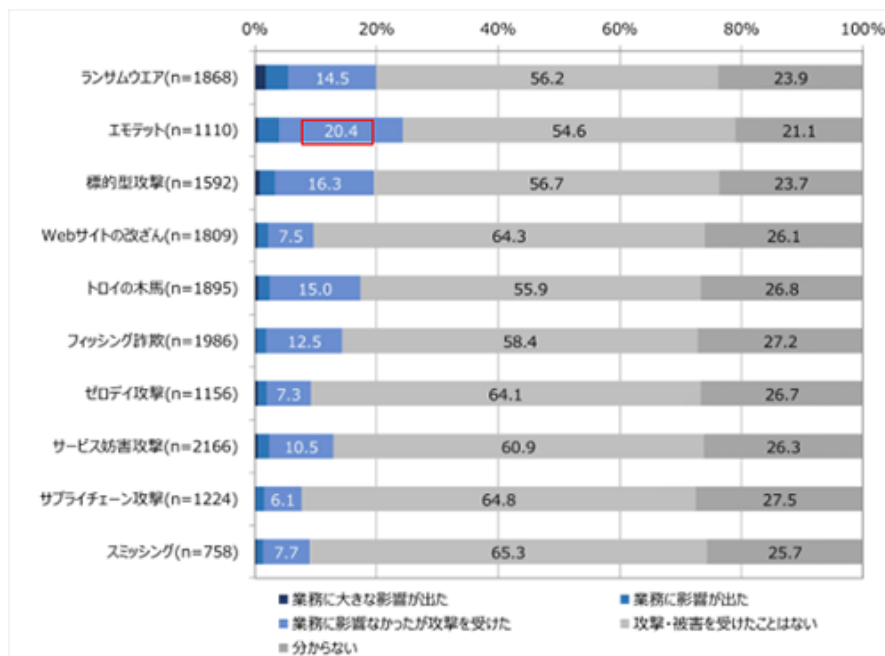
【図2 サイバー攻撃のリスクとその対処への理解】



企業が受けた攻撃・被害は「エモテット」がトップ

ここでは、勤務先がどのようなサイバー攻撃を受けたことがあるのかについて聞いた。「業務に影響なかったが攻撃を受けた」という点で、1位はエモテット(20.4%)、2位は標的型攻撃(16.3%)、3位はトロイの木馬(15.0%)という結果となった。エモテットによる攻撃は、業務に影響はなかったものも含めると実に5社に1社以上が攻撃を受けたことになる(図3)。だが、前項で示したようにエモテット自体の認知度はやや低い傾向にある。こうした企業のセキュリティ意識の“ギャップ”も攻撃者にとつての狙い目になっていると思われる。

【図3 勤務先が受けたサイバー攻撃】

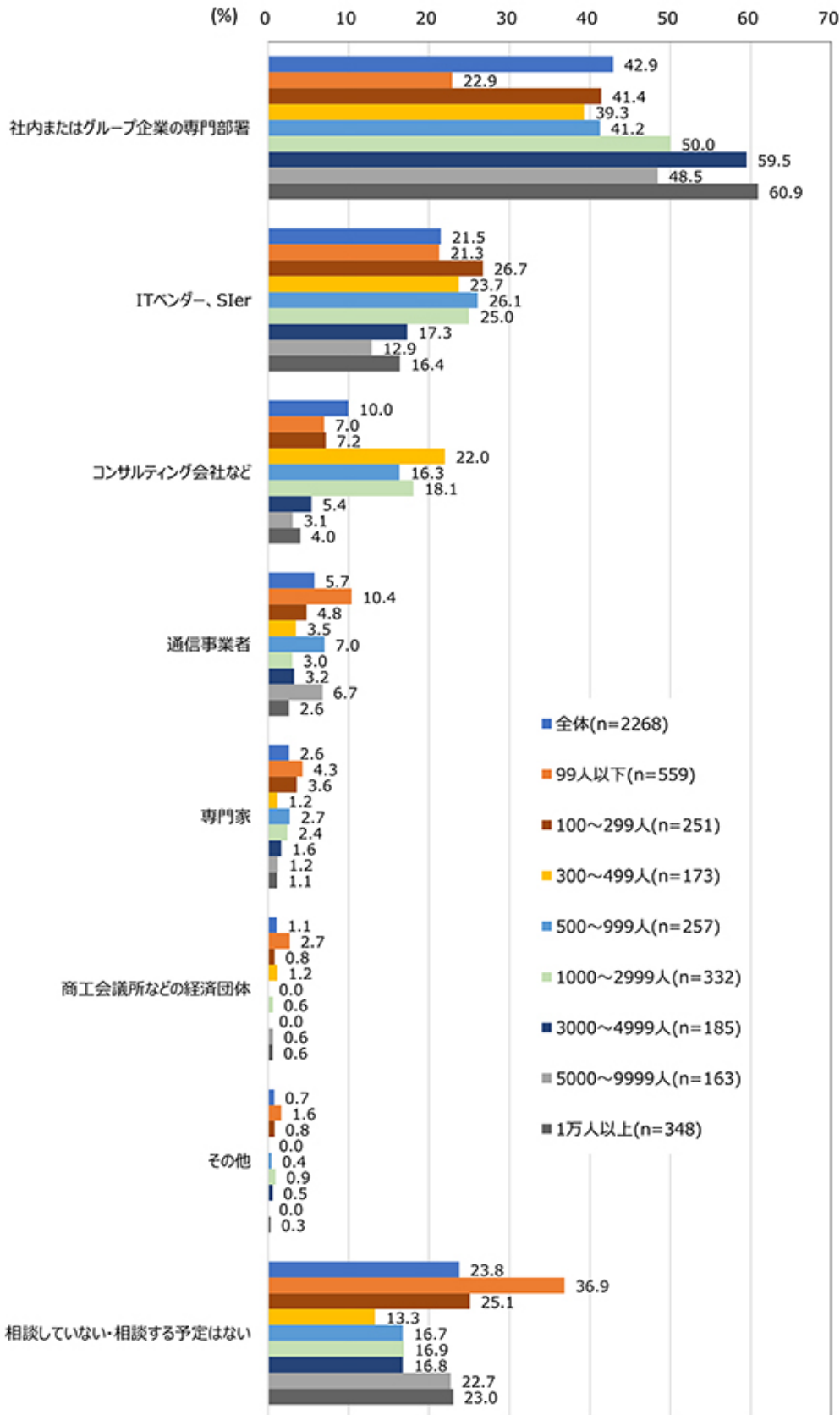


セキュリティ対策拡充は「社内の専門部署」がカギを握る

最後に、今後のセキュリティ対策拡充に向けての相談先について聞いた。従業員規模を問わず「社内またはグループ企業の専門部署」に回答が集中した。例えば、全体では42.9%となり、1万人以上企業では60.9%となっている。一方、99人以下企業では同様の傾向は見られつつも、「相談していない・相談する予定はない」が36.9%に、100~299人以下企業でも2

5.1%との結果になった(図4)。「企業の情報セキュリティ対策意識調査2022」では、従業員規模が小さいほど情報セキュリティ対策は十分ではないと感じる姿があるのではないかと触れた。図1での結果も踏まえ、今回の結果からも同様の姿が浮かび上がってくる。

【図4 セキュリティ対策拡充に際しての相談先】



テレワーク・リモートワークの広がりや社員一人ひとりに合った働き方の実現、より効率的な電子商取引の推進などビジネス

のあらゆる場面でITの導入が進む。企業環境の変化とともに攻撃者の手法も次々に新たなものが生まれ続けている。一度、サイバー攻撃によって情報の流出や改ざんなどの被害が起きれば、自社の信用失墜はもちろん、場合によっては損害賠償問題にまで発展することもあり得る。

図2で紹介した、情報セキュリティリスクについて「対処法も含めてよく知っている」という回答は2割以下にとどまる。確かなセキュリティ意識の醸成と各種対策強化のため、その攻撃手法を正しく知り、十全に備えるためにも外部専門家知見の活用なども有効な選択肢として幅広く取り組みを進めていきたい。

<本調査について>

日経BPコンサルティングのアンケートシステムにて、同社モニター2566人を対象に2023年1月に調査