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

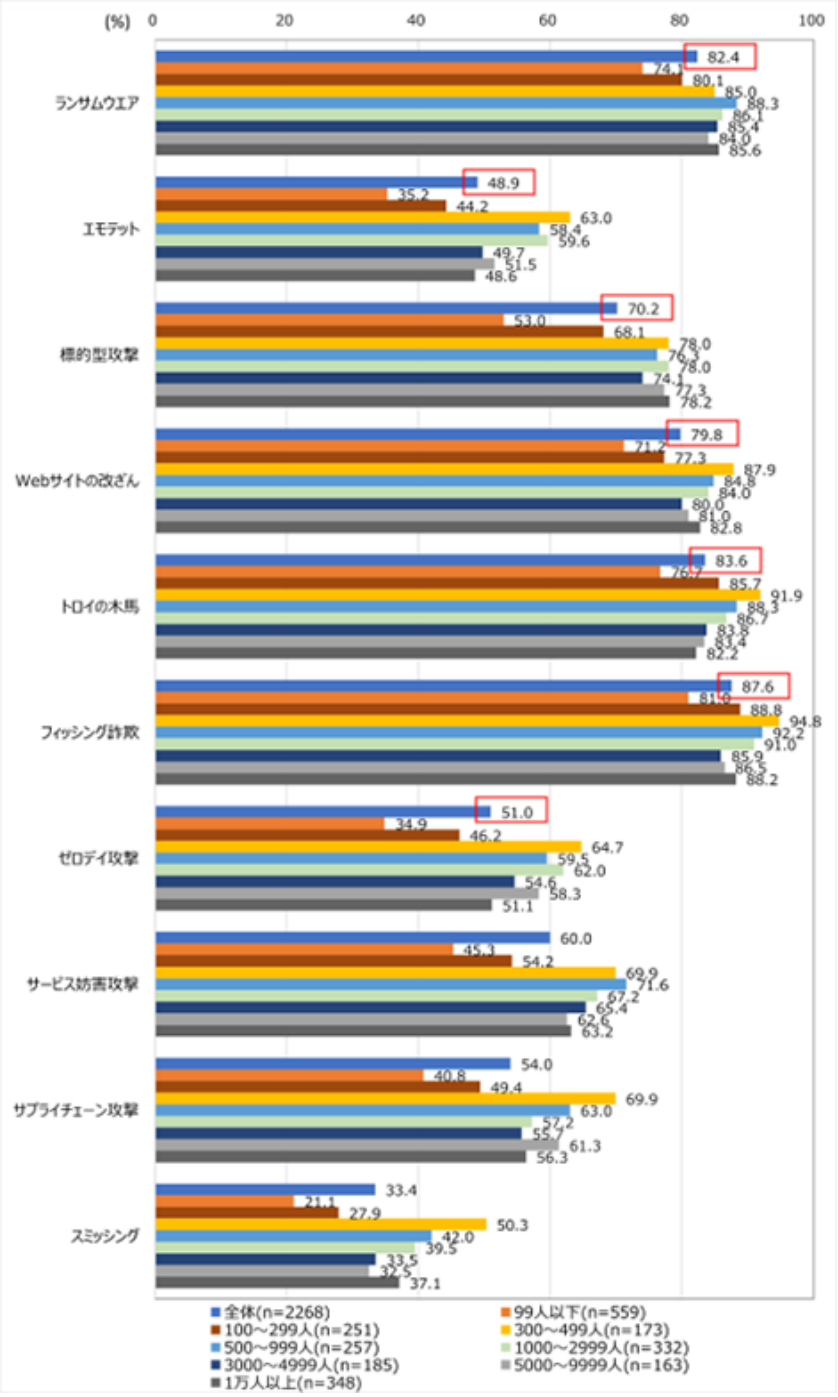
テクノロジーの進化によって、生産性の向上や多様な働き方の実現などの恩恵がもたらされる一方、サイバー攻撃も多様化・複雑化の一途をたどっている。こうした中、攻撃手法などの情報セキュリティリスクをどれくらい認知しているのだろうか。その最新動向について2023年1月に調査を行った（日経BPコンサルティングのアンケートシステムを用い、同社保有の調査モニター2566人を対象に調査を実施）。

「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「ランサムウエア」（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。

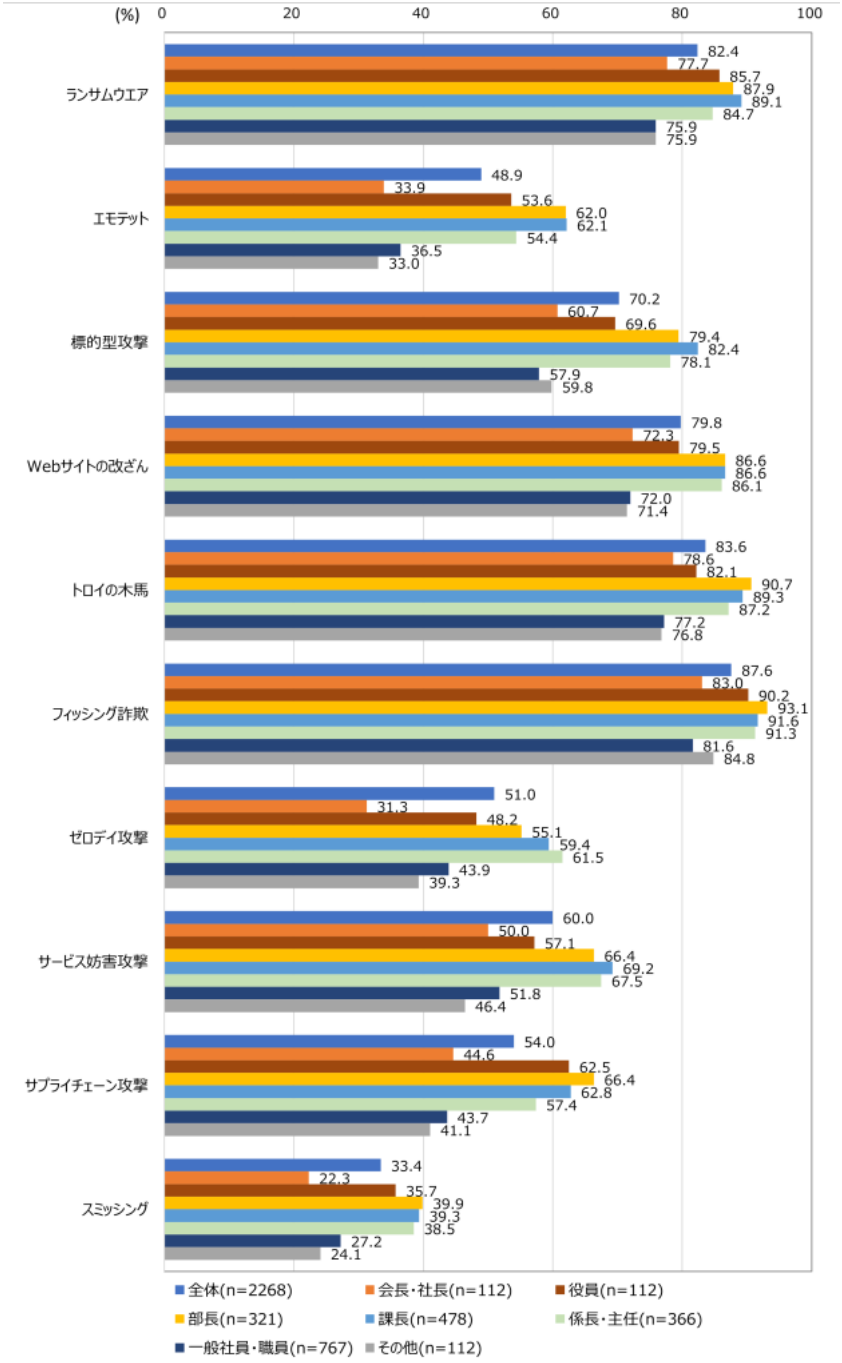
この一方、ソフトウエアのセキュリティホールの対策前を狙う「ゼロデイ攻撃」（51.0％）や近年大きな脅威として話題を集めた「エモテット」は48.9％という結果となった。特に300人未満の中小企業において、各脅威について認知度が低い傾向が顕著に表れた（図1-1）。

【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… 続きを読む