Biz Clip調査レポート（第29回）

企業の情報セキュリティ対策意識調査2021

2021.12.27



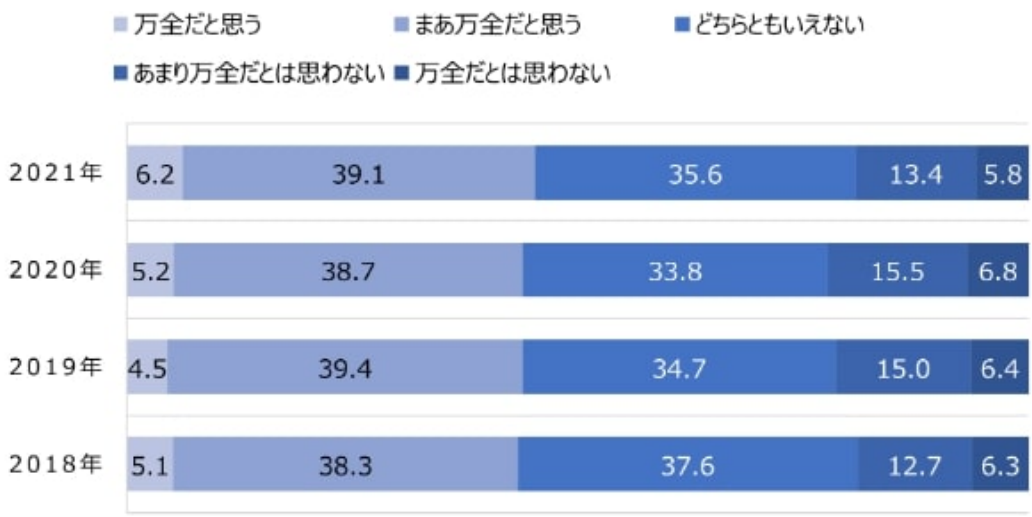
サイバー攻撃が後を絶たない。企業における情報セキュリティ対策はどうなっているか。対策の度合い、脅威に感じるもの、対策をするうえでの課題など最新動向について2021年12月に調査を行った。調査は日経BPコンサルティングのアンケートシステムにて、同社保有の調査モニター3098人を対象に実施した。

情報セキュリティ対策が万全だと45%が認識

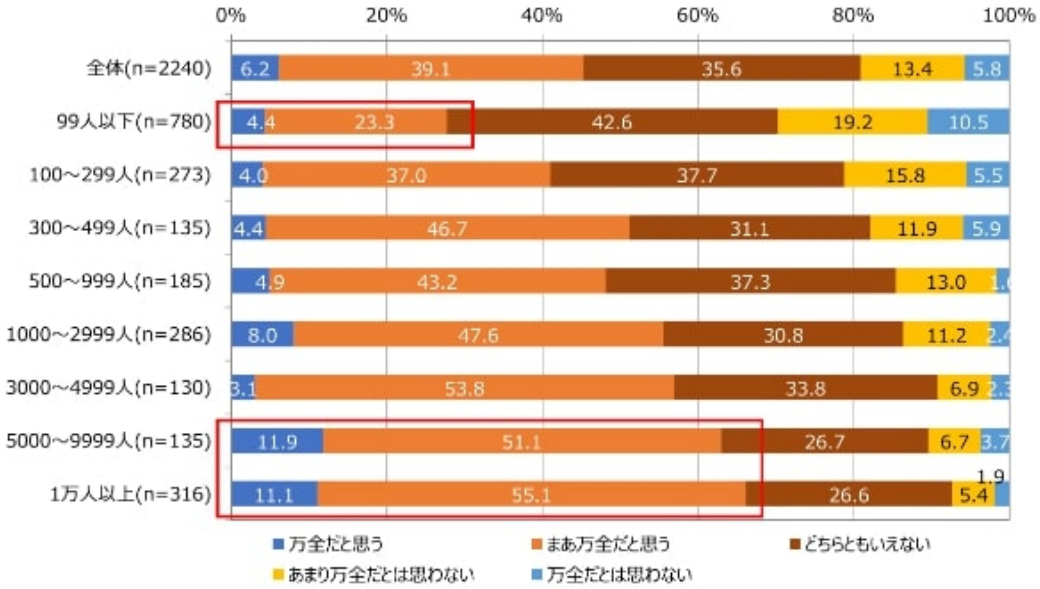
社内の情報セキュリティ対策が「万全だと思う」との回答は6.2%。「まあ万全だと思う」と合わせると45.3%が自社のセキュリティ対策について信頼感を示した。「あまり万全だとは思わない」は13.4%で前回比2.1ポイント、「万全だとは思わない」は5.8%で前回比1ポイント減。3.1ポイントとわずかながらも、前回調査より対策への不安感は減少した（図1-1）。

企業の従業員規模で見ると、従業員数と情報セキュリティ対策度合いには相関関係があるのが分かる。情報セキュリティ対策が万全と感じる比率は5000人以上の企業で高く、5000～9999人で11.9%、1万人以上で11.1%と、共に1割を超えた。「万全だと思う」と「まあ万全だと思う」を合わせると、99人以下の企業の選択率が3割を下回るのに対し、5000人以上、1万人以上の企業では共に6割超えとなる。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ている（図1-2）。

【図1-1 社内の情報セキュリティ対策は万全か（2018～2021年比較）】



【図1-2 社内の情報セキュリティ対策は万全か（従業員数別）】

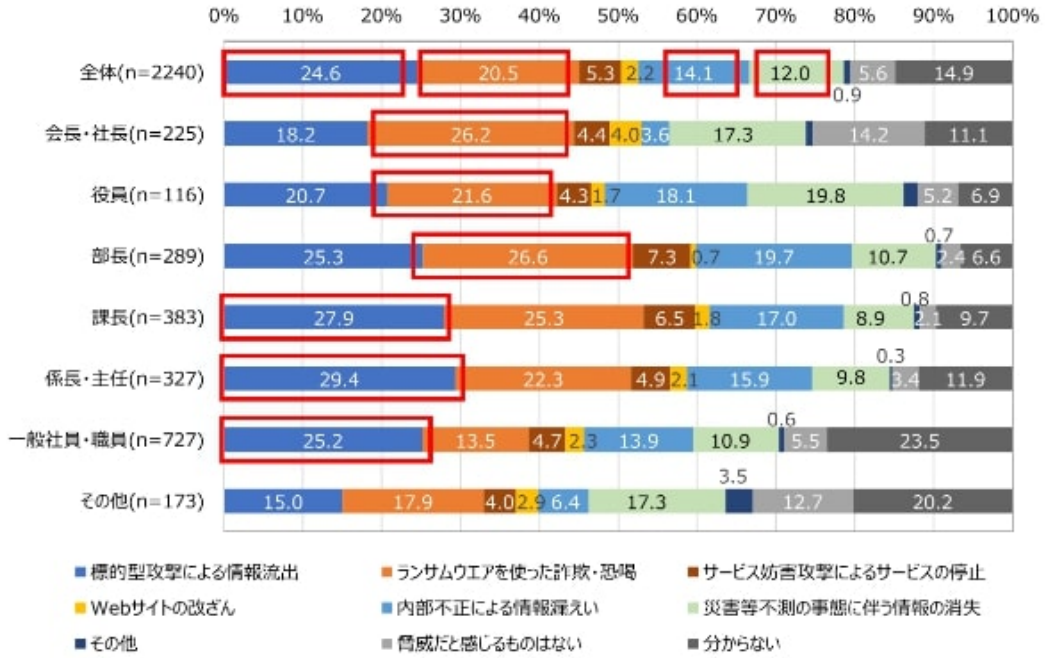


最も脅威なのは標的型攻撃。会社上層部はランサムウエアを警戒

社内の情報資産管理で最も脅威なのは、「標的型攻撃による情報流出」で、全体の24.6%が選択した。それに続くのが「ランサムウエアを使った詐欺・恐喝」（20.5%）で、前回調査で2位だった「内部不正による情報漏えい」は、前回比7ポイントダウンの14.1%となった。2018年調査から上昇していた「災害等不測の事態に伴う情報の消失」は12.0%。前回比1.1ポイントマイナスで今回は横ばいとなった。

役職別の結果は次の通り。「会長・社長」「役員」「部長」で最も選択されたのは「ランサムウエアを使った詐欺・恐喝」なのに対し、「課長」「係長・主任」「一般社員・職員」で最も脅威と感じられたのは、「標的型攻撃による情報流出」だった。世間をにぎわすランサムウエアのニュースが身代金の支払いをすべきか否かなど、経営判断に関わる問題に発展しがちなのが理由の1つと考えられる（図2-1）。

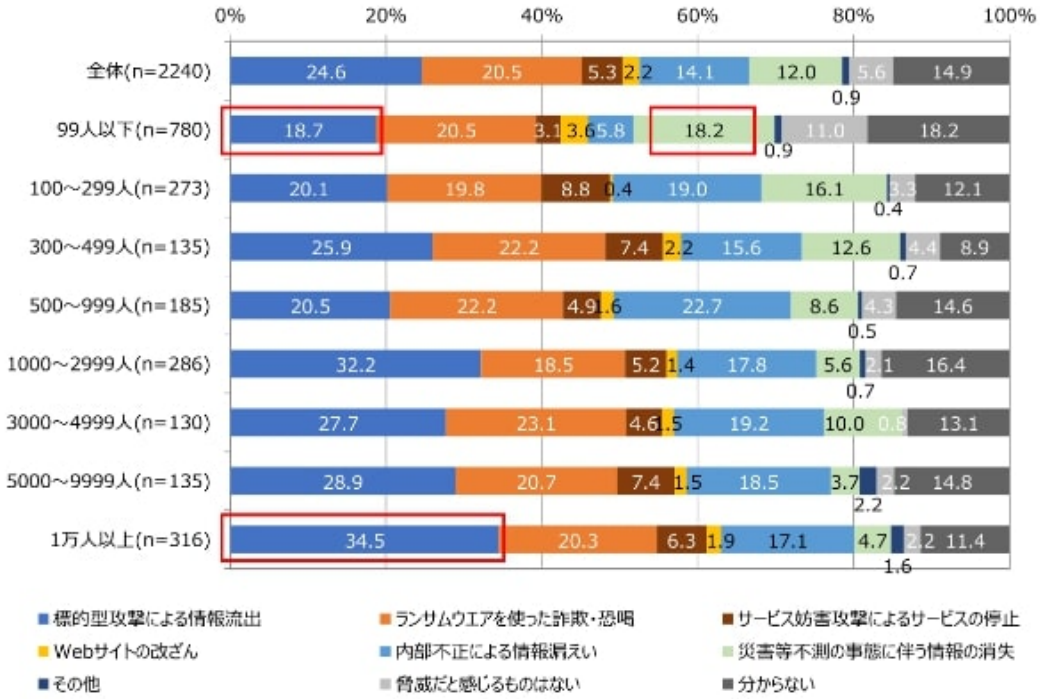
【図2-1 社内の情報資産管理で最も脅威と感じること（役職別）】



従業員規模別の結果では、トップの「標的型攻撃による情報流出」が、99人以下の企業で18.7%なのに対し、1万人以上の企業では34.5%と15.8ポイントもの差がついた。標的型攻撃に関しては、従業員規模が大きい方が脅威を感じる傾向が表れている。

一方、従業員規模が小さい企業で選択率の高い項目は、「災害等不測の事態に伴う情報の消失」となった。99人以下の企業では18.2%が選択した。この項目は従業員規模が大きくなるにつれて選択率が低くなる傾向が出た(図2-2)。

【図2-2 社内の情報資産管理で最も脅威と感じること(従業員数別)】



「ウイルス対策」は事業規模に差はなし。それ以外は小規模企業の対応遅れ… 続きを読む