Biz Clip調査レポート（第40回）

企業の情報セキュリティ対策意識調査2023

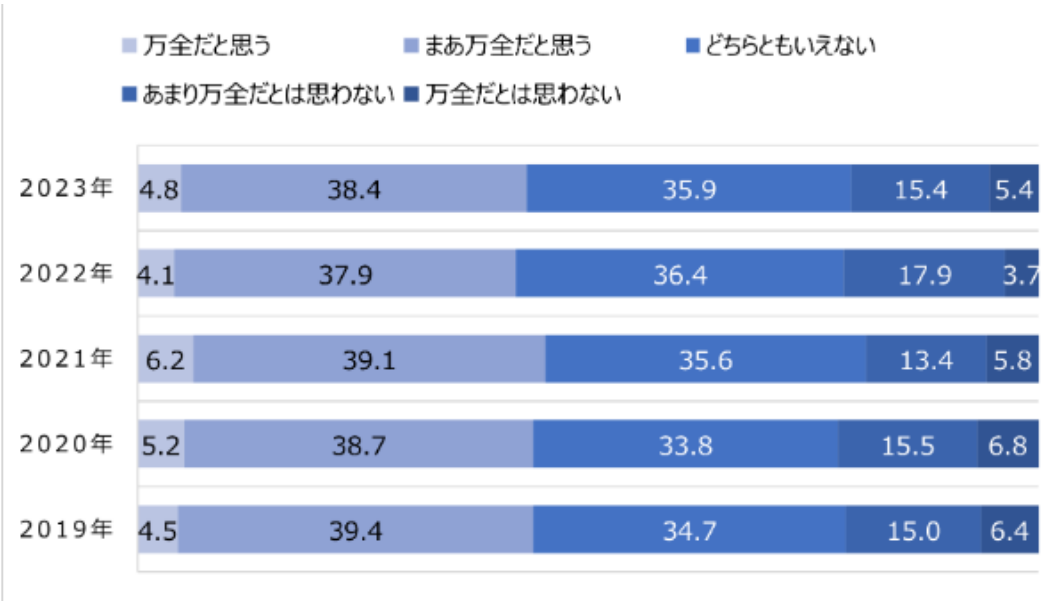
2023.09.06

サイバー攻撃が複雑化・多様化し続けている。AIやRPAなどのテクノロジーや、社内外のコミュニケーションを円滑化するクラウドストレージ活用が進む中、企業における情報セキュリティ対策はどうなっているのだろうか。対策度合いや、脅威に感じるもの、対策上の課題などについて2023年8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を用い、同社保有の調査モニター3246人を対象に調査を実施した。

約4割が「情報セキュリティ対策が万全」と認識

社内の情報セキュリティ対策について「万全だと思う」との回答は4.8%、「まあ万全だと思う」の38.4%と合わせると全体の約4割が自社セキュリティ対策への信頼感を示した。「あまり万全だとは思わない」（15.4%）、「万全だとは思わない」（5.4%）は合計で20.8%。前回比でも大きな変化は見られなかった（図1-1）。

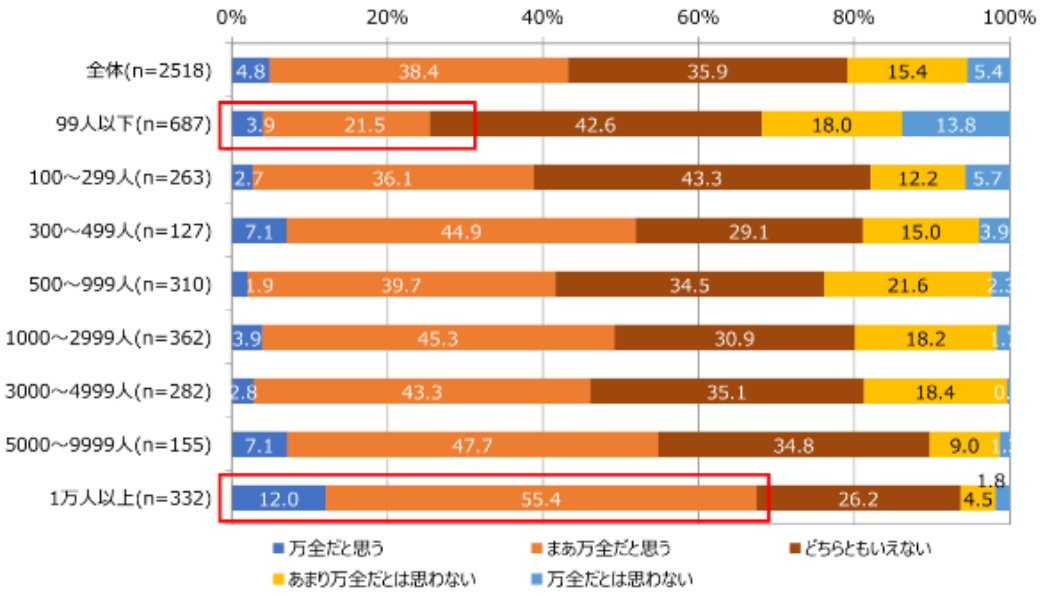
【図1-1 社内の情報セキュリティ対策は万全か（2019～2023年比較）】



社内の情報セキュリティ対策について従業員規模で捉えると、従業員数と対策度合いで相関性が浮かび上がる。例えば、99人以下の企業で「万全だと思う」「まあ万全だと思う」とする割合は合計25.4%となり、3割を下回る。この一方、1万人以上の

規模の企業では同項目の合計で67.4%となり、大きな開きがある(図1-2)。

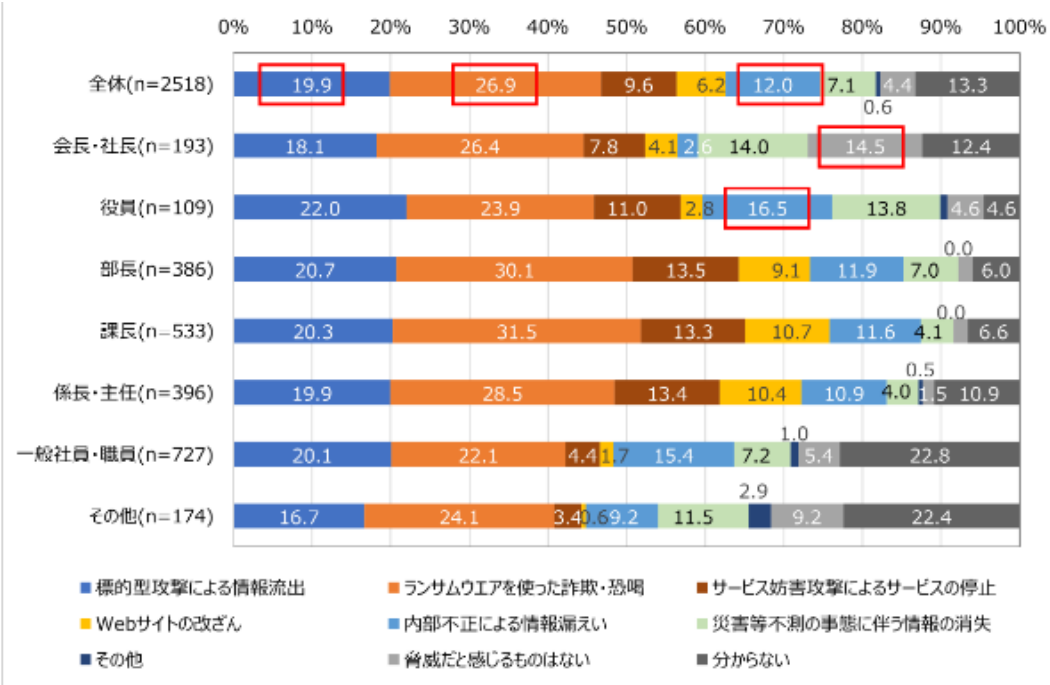
【図1-2 社内の情報セキュリティ対策は万全か(従業員数別)】



社内ネットワークへの不正侵入やUSBなど、企業規模で対策に濃淡も

社内の情報資産管理における脅威は、全体で見ると、1位「ランサムウエアを使った詐欺・恐喝」(26.9%)、2位「標的型攻撃による情報流出」(19.9%)、3位に「内部不正による情報漏えい」(12.0%)という結果となった(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)】

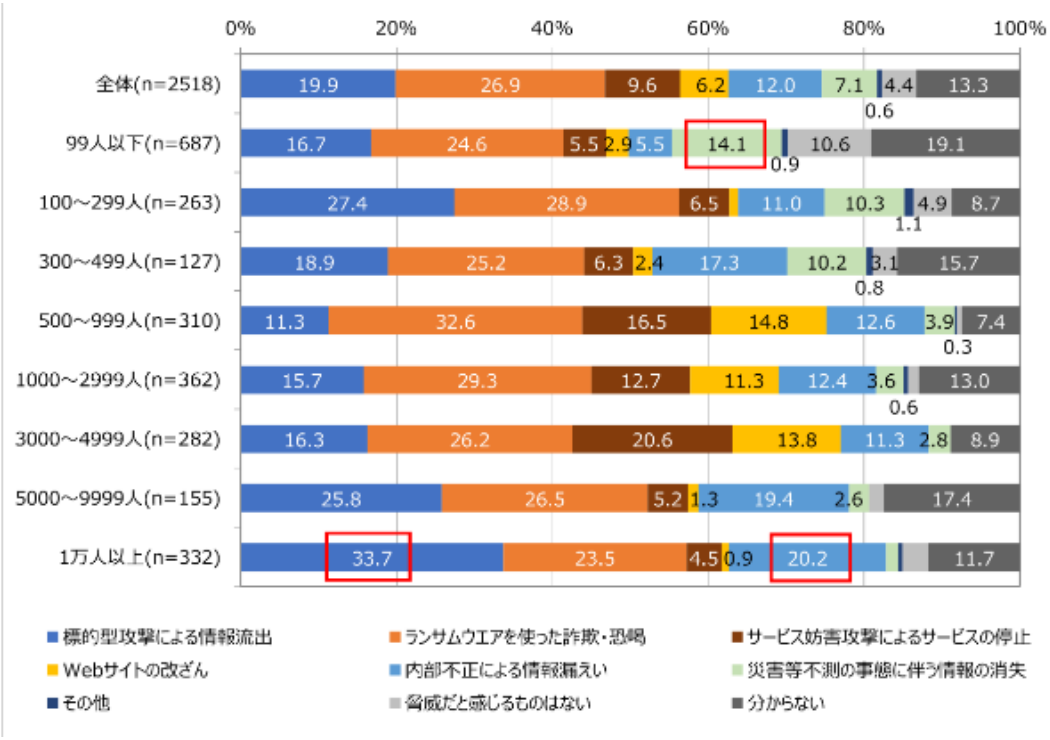


ランサムウエアのインシデントは、経営判断に関わる問題に発展しがちである点から、一般社員から経営層まで影響を与え

たものと思われる。また、役員の回答からは内部不正に懸念を置いている姿も見て取れる（全体12.0%のところ16.5%）。一方、「脅威だと感じるものはない」を最も多く選択したのは会長・社長（14.5%）との気になる結果もある。経営幹部層のセキュリティ対策意識の希薄さは、今後の焦点の1つとなりそうだ。

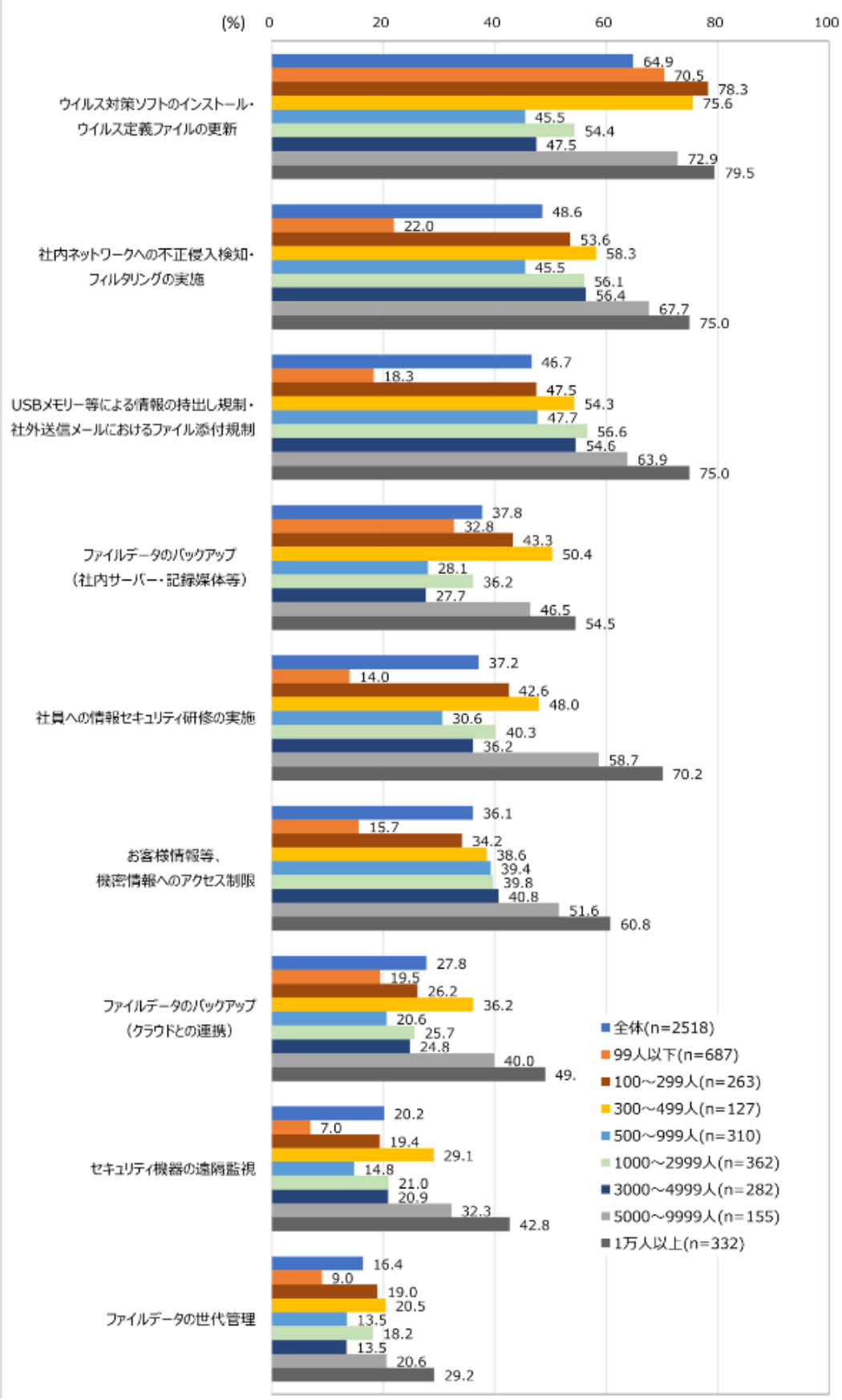
次に、同項目を従業員規模別で見てみよう。1万人以上の企業では「標的型攻撃による情報流出」が33.7%、「内部不正による情報漏えい」が20.2%と全体より高い選択率となっている。働き方の多様化によって、社内外を問わず情報のやり取りが複雑化・多様化したことが背景にあると考えられる。この一方、従業員規模が小さい企業で選択率の高い項目は、「災害等不測の事態に伴う情報の消失」。99人以下の企業では14.1%が選択した。本項目は従業員規模が大きくなるにつれて選択率が低くなる傾向が表出している（図2-2）。

【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）】



続いて、すでに導入されている情報セキュリティ対策について見ていこう。全体を通じて最多は、「ウイルス対策ソフトのインストール・ウイルス定義ファイルの更新」（64.9%）。2位に「社内ネットワークへの不正侵入検知・フィルタリングの実施」（48.6%）、3位には「USBメモリー等への情報持ち出し規制・社外送信メールにおけるファイル添付規制」（46.7%）となった。この結果に関し、「社内ネットワーク」「USB」の選択率について99人以下の企業が突出して他より低い結果となった点は、注目すべきポイントと言えそうだ。

【図3 すでに導入されている対策】

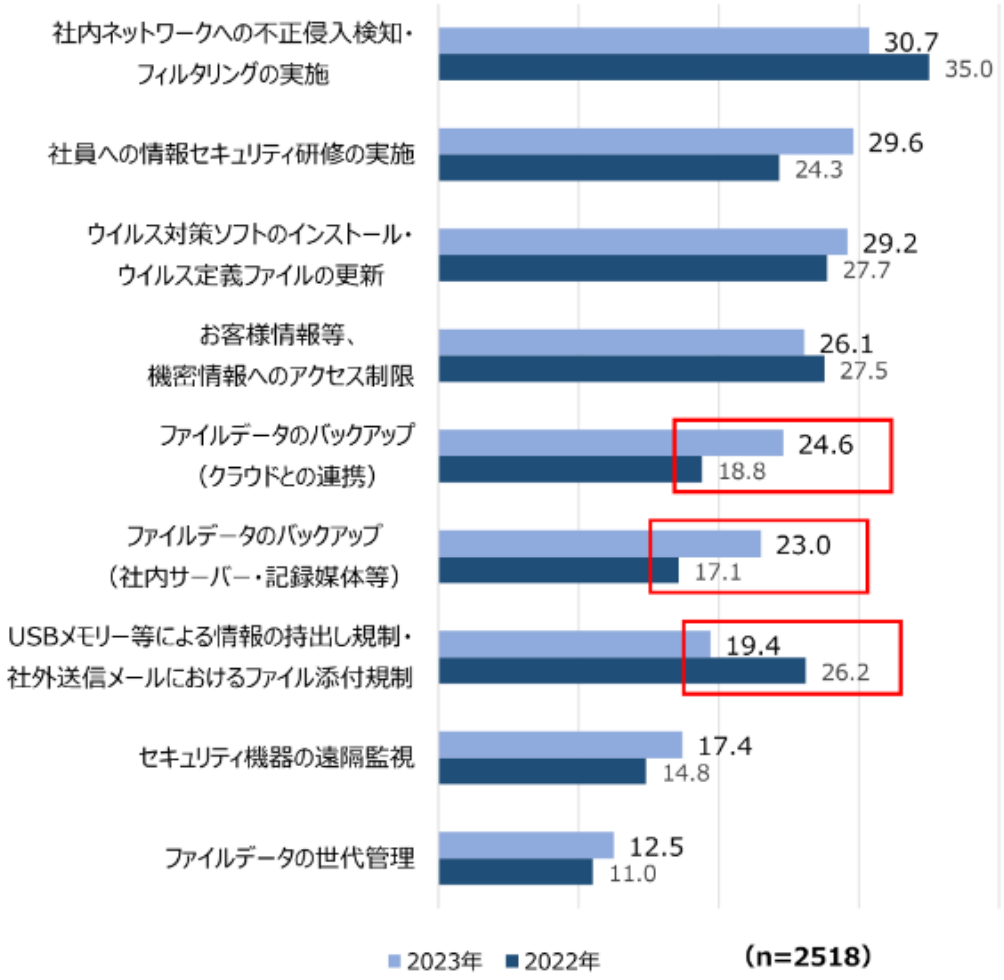


社員の情報セキュリティ意識の向上やクラウド活用関連の割合が増加

今後さらに必要・重要と思われる対策についても聞いた。1位が「社内ネットワークへの不正侵入検知・フィルタリングの実施」(30.7%)、2位に「社員への情報セキュリティ研修の実施」(29.6%)が続く。情報セキュリティ研修の項目は、前回比5.3ポイント増となり(前回5位)、社員教育に対する意識の高まりがその背景にあると考えられる。3位には「ウイルス対策ソフトのインストール・ウイルス定義ファイルの更新」(29.2%)が続いた(図4-1)。

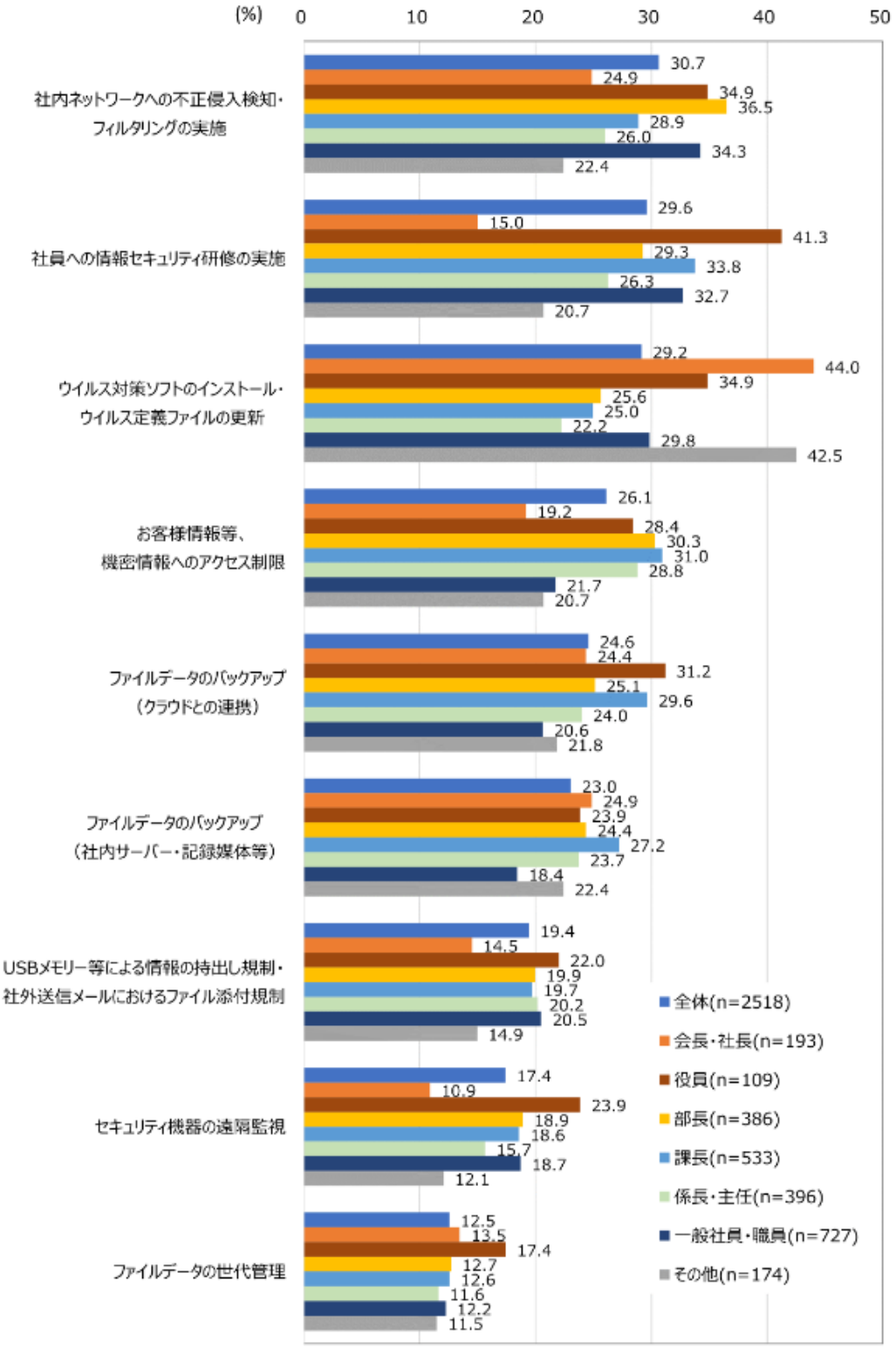
その他、注目すべき項目としては、「ファイルデータのバックアップ(クラウドとの連携)」「ファイルデータのバックアップ(社内サーバー・記録媒体等)」の項目で前回比約5ポイント増加する一方で、「USBメモリー等による情報の持ち出し規制・社外送信メールにおけるファイル添付規制」が約7ポイント減となった点だ。企業のクラウド活用の進展が伺える。

【図4-1 今後さらに必要(重要)と思われる対策】



役職別に捉えた際に特徴的なのは、前回と同様に会長・社長が最も必要・重要と考える項目として、「ウイルス対策ソフトのインストール・ウイルス定義ファイルの更新」が44.0%と突出しつつも、「社員への情報セキュリティ研修の実施」の選択率は15.0%と他の役職より大幅に低い選択率となっていることだ(図4-2)。この点からも会社の意思決定層の情報セキュリティ意識をいかに高めていくのかが今後、企業にとって大きなポイントとなりそうだ。

【図4-2 今後さらに必要(重要)と思われる対策(役職別)】

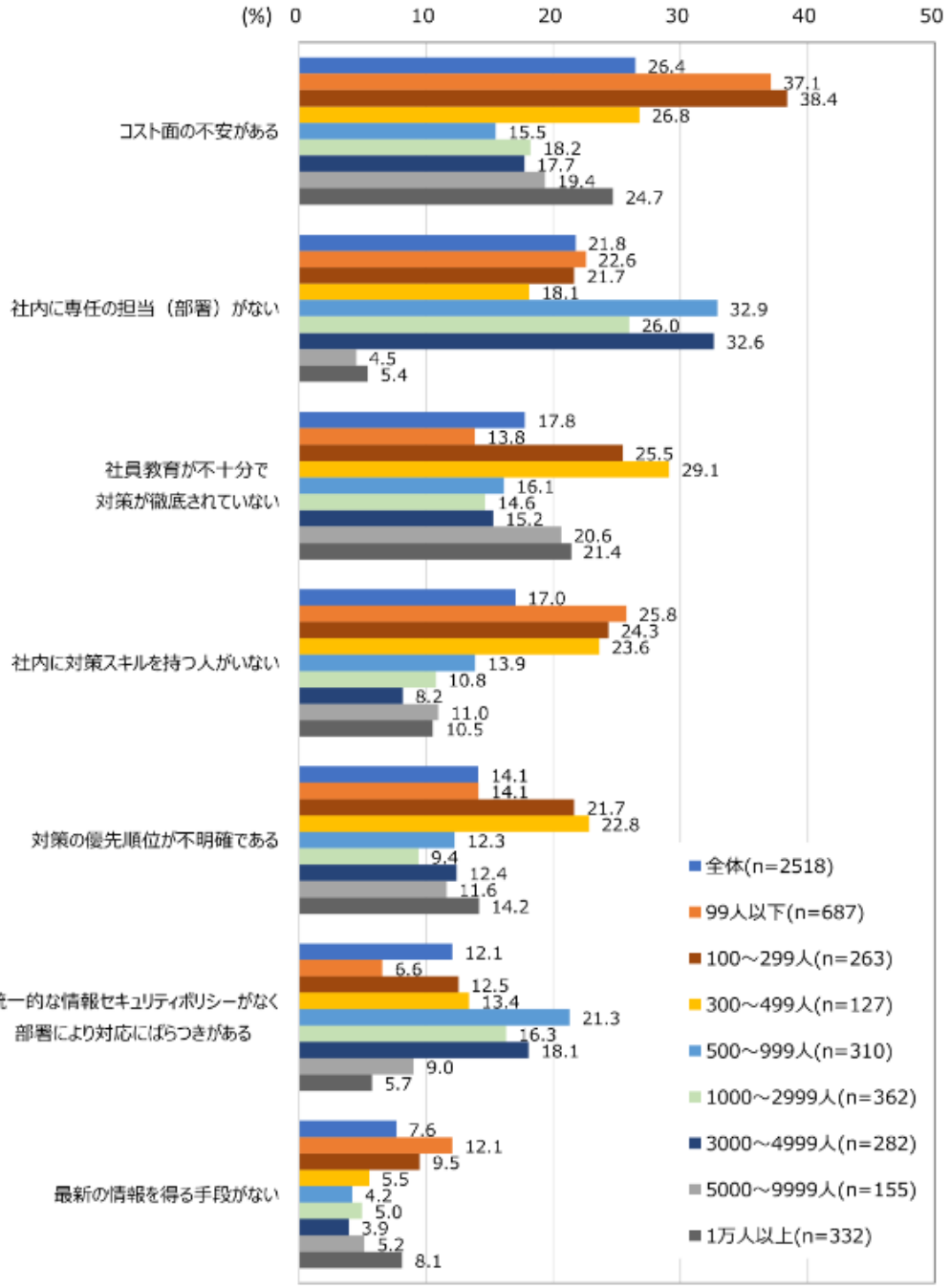


企業規模問わず、実施課題は「コスト面の不安」

対策実施に際しての課題トップは、「コスト面の不安がある」（全体で26.4%が選択）。特に、99人以下の企業では37.1%、100～299以下人企業で38.4%と高い選択率となった。2位には、「社内に専任の担当（部署）がない」（21.8%）が続いた。ただ5

000人以上の大企業では選択率が極端に低く、5000人未満の企業でのIT人材不足が顕著となっている姿が浮かび上がる（図5）。

【図5 情報セキュリティ対策を実施するうえでの課題（従業員数別）】



日々変化し、多様化・複雑化を続けるセキュリティリスク。さまざまな情報セキュリティへの意識変容は感じられつつも、特に中小企業経営者における意識の希薄さは依然否めず、具体的な対策に結びつけにくい実情が見える。万が一のサイバーインシデントへの対策強化は一刻を争う。より確かなセキュリティ意識の醸成と各種の対策強化を急ぎたいところだ。

＜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3246人を対象に2023年8月に調査