Biz Clip調査レポート（第34回）

企業の情報セキュリティ対策意識調査2022

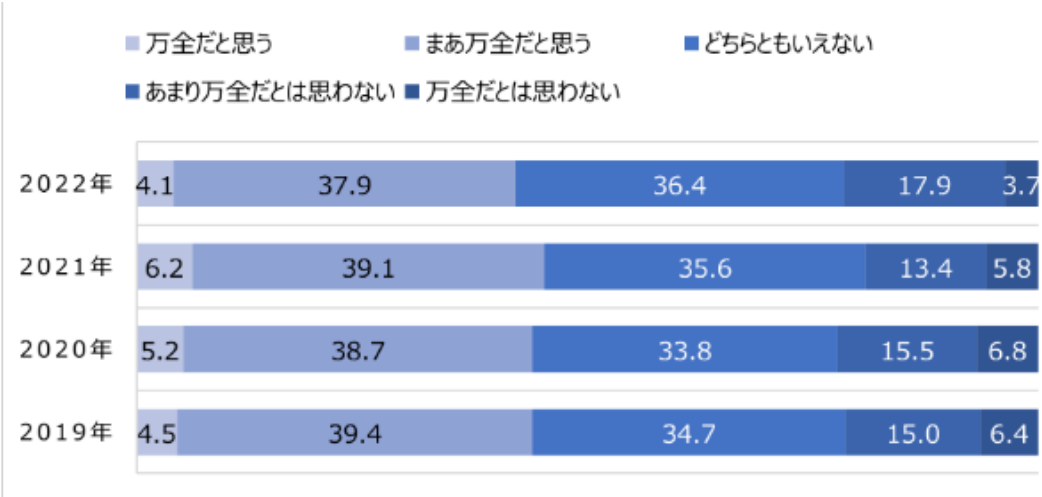
2022.11.28

DX推進が企業にとって成長のドライバーとなる中、サイバー攻撃も多様化・複雑化の一途をたどっている。AIやRPAなど各種のICT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現在、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、対策をするうえでの課題などの最新動向について2022年10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3680人を対象に調査を実施した。

42.0%が「情報セキュリティ対策が万全」と認識

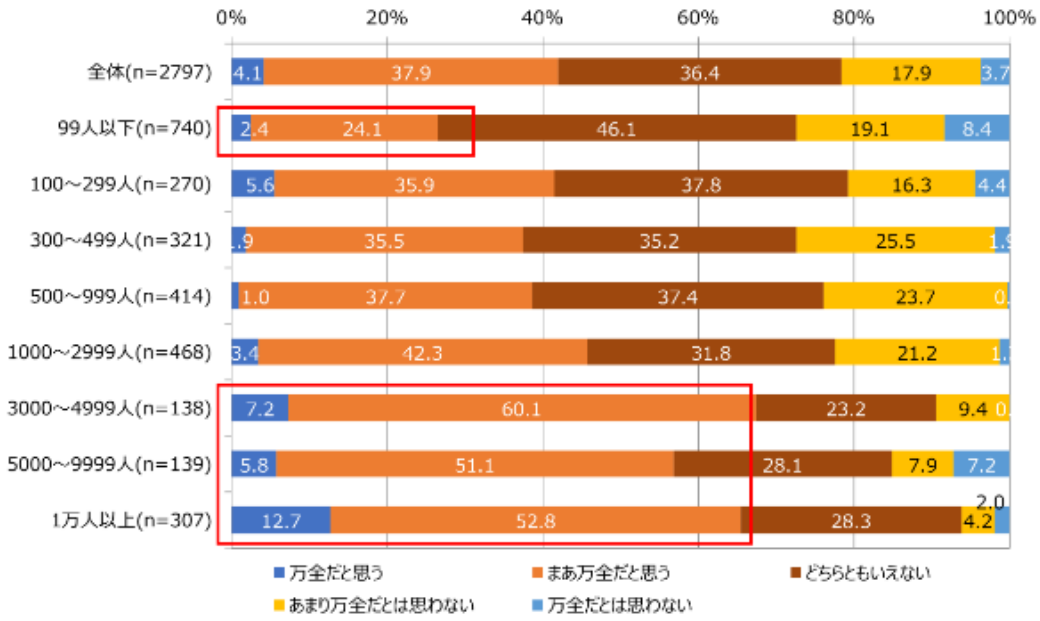
社内の情報セキュリティ対策が「万全だと思う」との回答は4.1%、「まあ万全だと思う」の37.9%と合わせると全体の42.0%が自社セキュリティ対策への信頼感を示し、前回調査とほぼ同様の形となった。「あまり万全だとは思わない」（17.9%）、「万全だとは思わない」（3.7%）は合計で21.6%、前回比で2.4ポイント増とほぼ横ばいとなった（図1-1）。

【図1-1 社内の情報セキュリティ対策は万全か（2019～2022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分析すると、従業員数と対策の度合いの相関関係が見て取れる。例えば、万全と感じる割合は3000人規模以上の企業で高く、「万全だと思う」と「まあ万全だと思う」を合わせると共に約6割となる。一方、99人以下の企業の同項目選択率が3割を下回り、大きく開きを見せている。この結果からは、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浮かび上がってくる（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）】



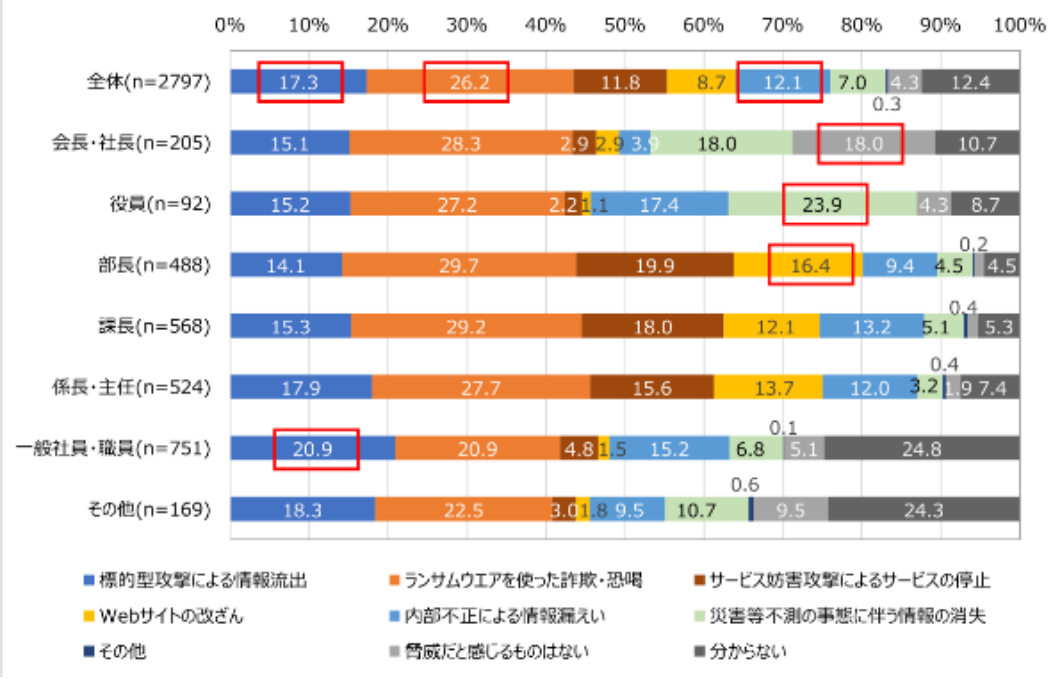
脅威の“多様化”。適切なリスクマネジメントを

社内の情報資産管理における脅威として、1位に「ランサムウエアを使った詐欺・恐喝」（26.2%）が、2位の「標的型攻撃による情報流出」（17.3%）に入り、この2項目だけで4割超の企業が選択した。3位には「内部不正による情報漏えい」（12.1%）が入った。

役職別の結果について、全役職で最も多く選択されたのは「ランサムウエアを使った詐欺・恐喝」であった。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、「災害等不測の事態に伴う情報消失」を最も選択したのは役員（23.9%）で、「Webサイトの改ざん」を最も選択したのは部長（16.4%）などの結果も得られた。この一方で、「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（18.0%）という気になる結果もある。経営幹部層へのセキュリティインシデントに対する適切なリスクマネジメントへの意識付けも、今後の1つの焦点となりそうだ（図2-1）。

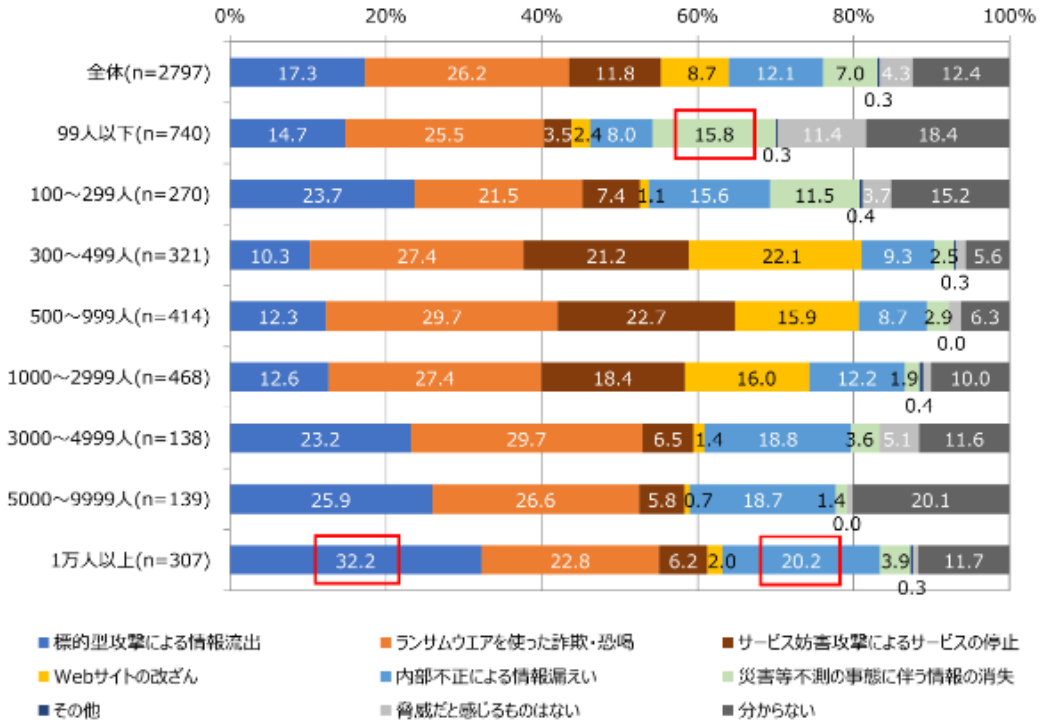
【図2-1 社内の情報資産管理で最も脅威と感じること（役職別）】



次に、同項目を従業員規模別で見てみよう。今回の調査では、1万人以上の企業で「標的型攻撃による情報流出」32.2%、「内部不正による情報漏えい」も20.2%と高い選択比率となった。リモートワーク・テレワークの浸透などによって、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。

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15.8%が選択し、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)。

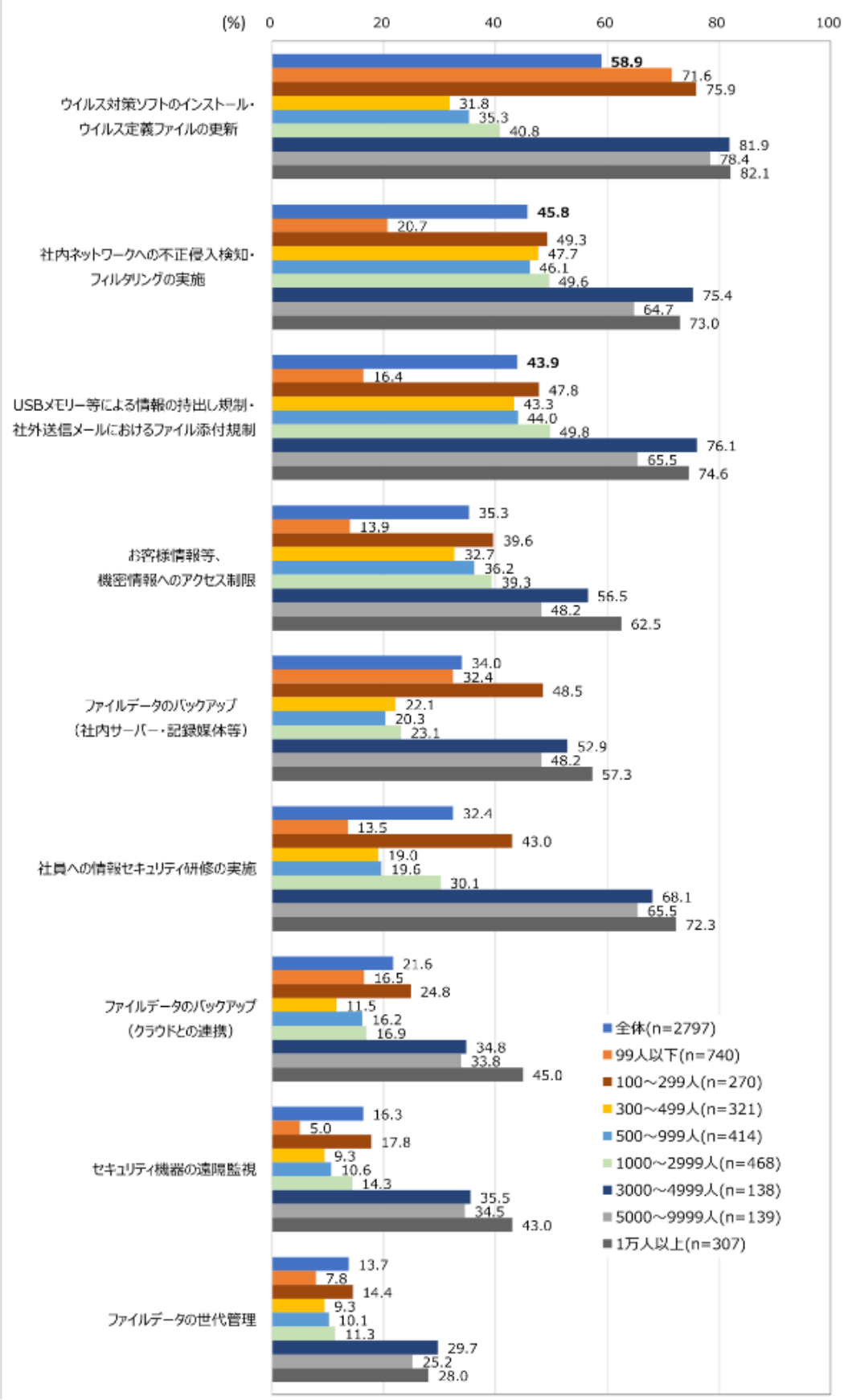
【図2-2 社内の情報資産管理で最も脅威と感じること(従業員数別)】



「ウイルス対策」は、事業規模に関係なく重要な関心事

すでに導入されている情報セキュリティ対策のうち最も多いのは、「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」で1位となった（58.9%）。2位には「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」（45.8%）、3位に「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」（43.9%）となった。ただし、社内ネットワーク、USBについては99人以下の企業のみ、選択率が突出して他より低い結果となった。

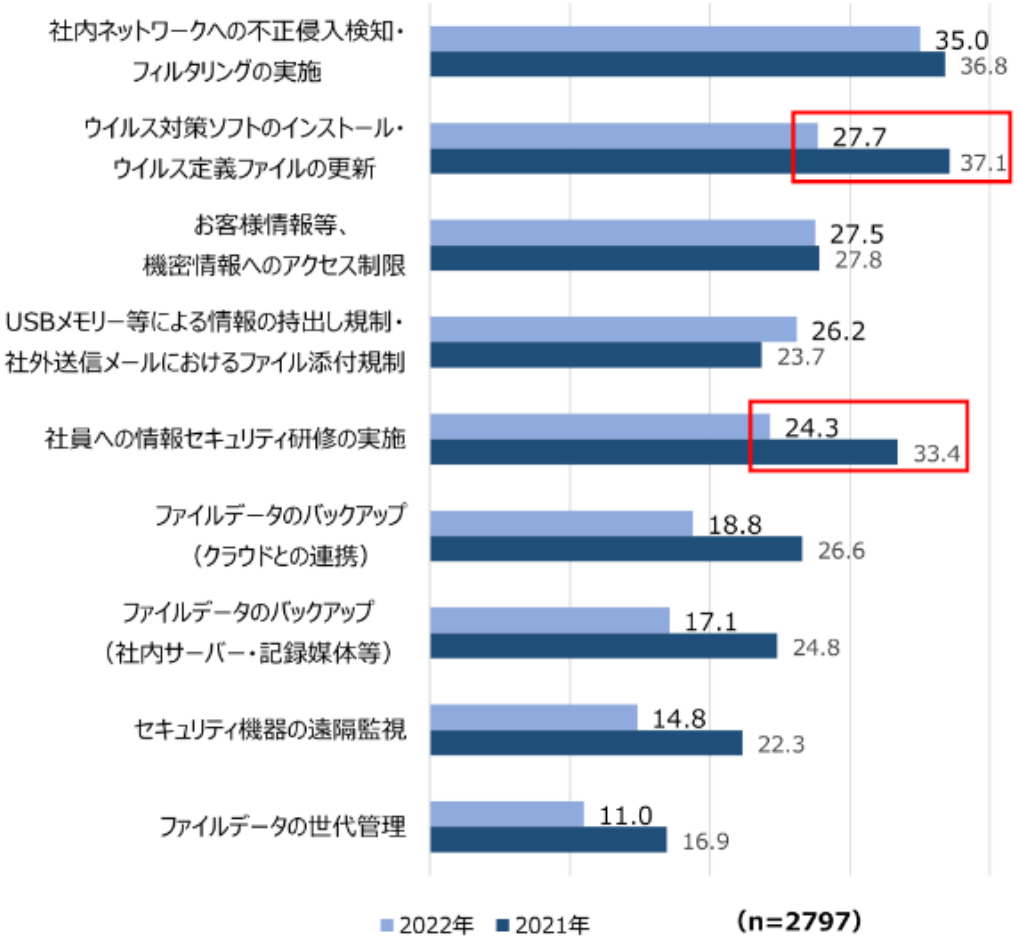
【図3 すでに導入されている対策（MA）】



「情報セキュリティ研修の実施」等が割合低下。対策に迷う企業像を反映か？

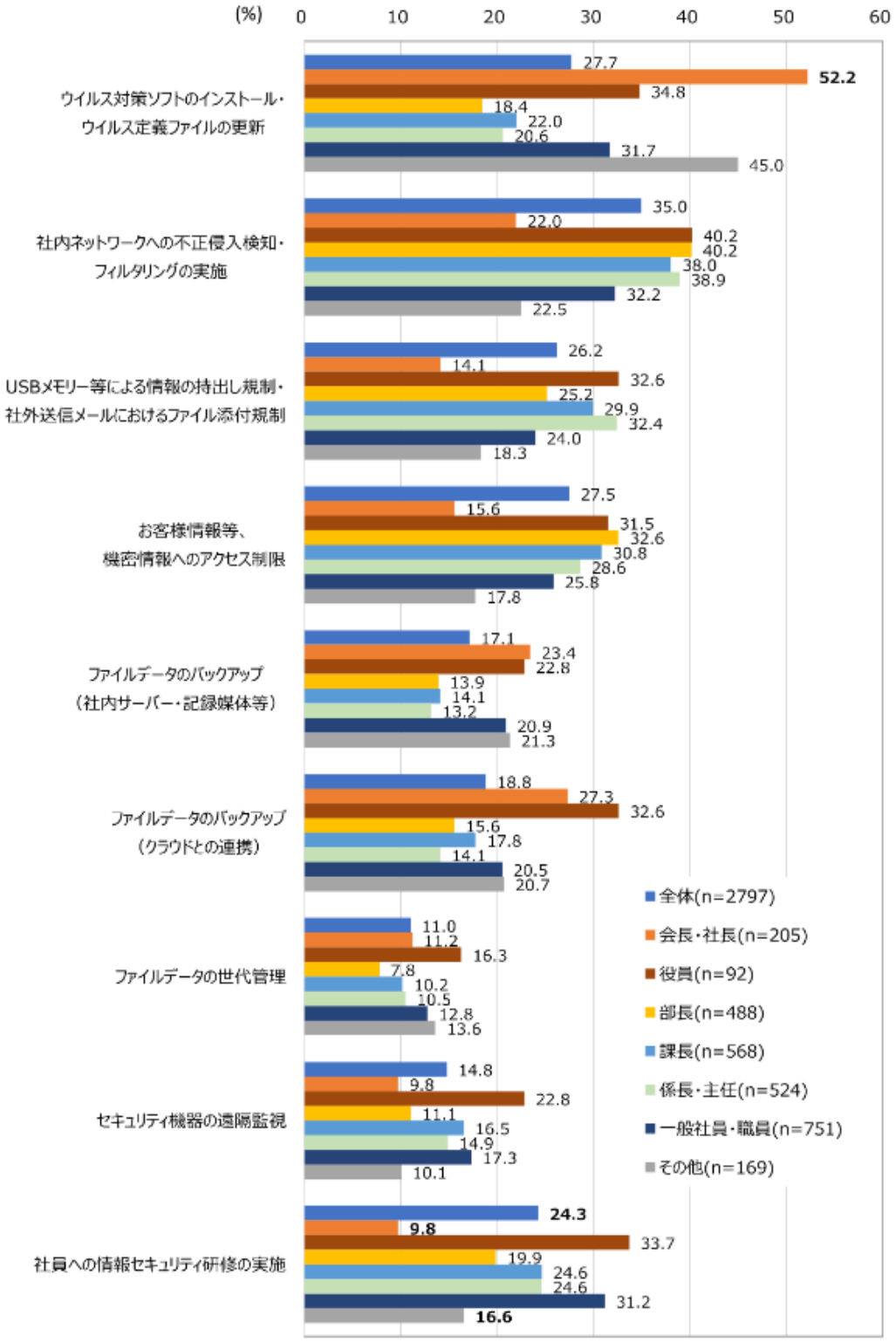
今後さらに必要・重要と思われる対策は、1位が「社内ネットワークへの不正侵入検知・フィルタリングの実施」(35.0%)、2位が「ウイルス対策ソフトのインストール・ウイルス定義ファイルの更新」(27.7%)、そして3位が「お客様情報等、機密情報へのアクセス制限」(27.5%)という結果が得られた(図4-1)。前年結果と比較すると特に、2位の「ウイルス対策ソフト」5位の「社員への情報セキュリティ研修の実施」がそれぞれ、10ポイント程度の低下を見せている。

【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、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52.2%と突出している点だ。一方「社員への情報セキュリティ研修の実施」は、全体が24.3%なのに対してこの層は9.8%。どの役職にも属さない「その他」16.6%と共に、他の役職より大幅に低い選択率となっている(図4-2)。

【図4-2 今後さらに必要(重要)と思われる対策(役職別)】

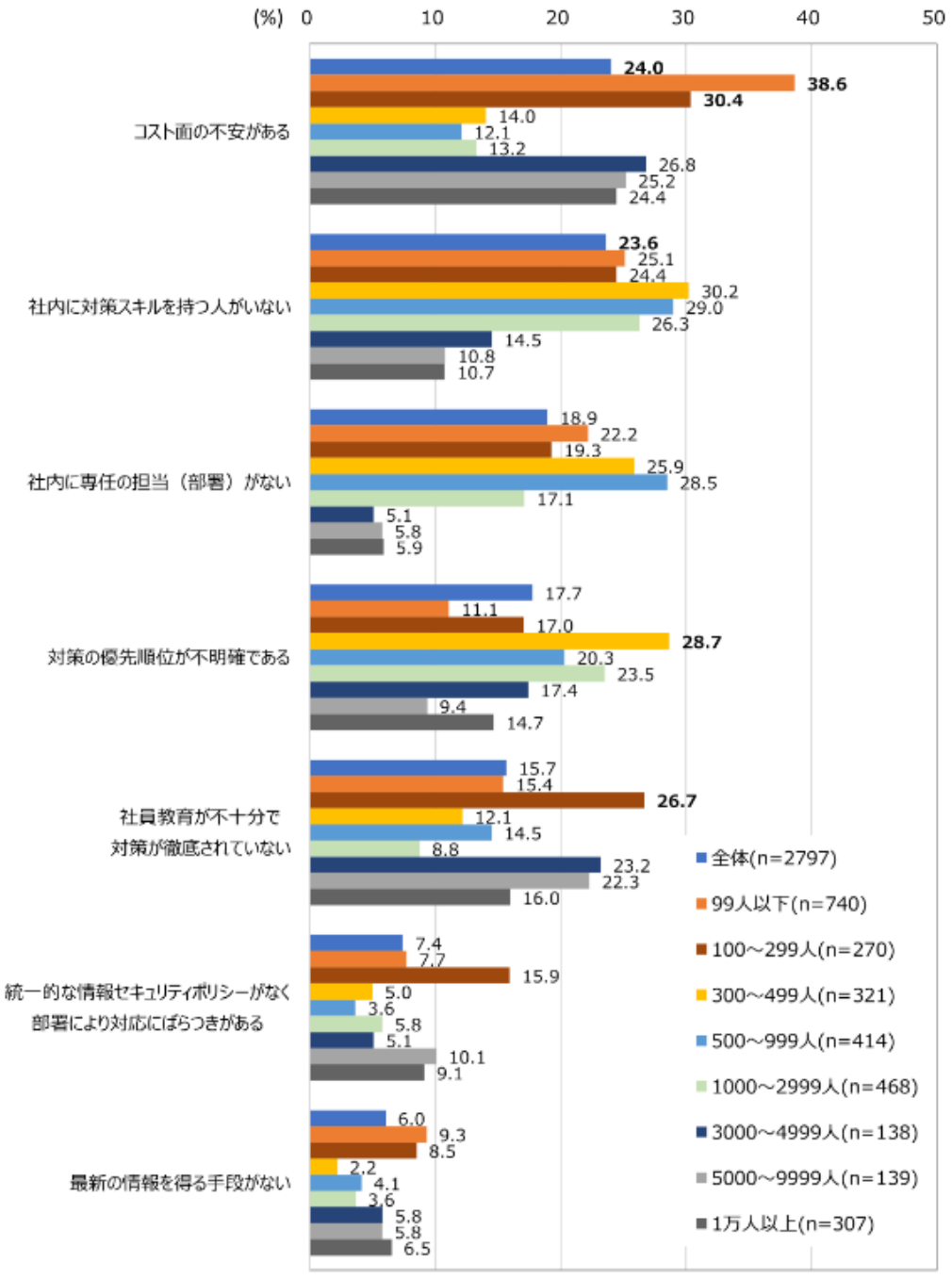


前述の「社内の情報資産管理で最も脅威と感じること（役職別）」の結果で、会長・社長層の特徴として「脅威だと感じるものはない」（18.0%）の選択率の高さには言及した。この結果と照らし合わせると、経営幹部層の情報セキュリティ意識をいかに高めていくのかは企業にとって大きな課題・ポイントとなってきそうだ。

実施課題は「コスト面の不安」が依然トップに

情報セキュリティ対策を実施するうえでの課題のトップは、「コスト面の不安がある」で全体の24.0%が選択した。特に、99人以下企業では38.6%、100～299以下人企業で30.4%が選択した。2位の「社内に対策スキルを持つ人がいない」(23.6%)は、3000人以上の大企業では選択率が極端に低く、3000人未満の企業では総じて選択率が高い。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課題(従業員数別)】



多様化する働き方や、日々変化し続けるセキュリティリスクへの対応。今回の調査からは、標的型攻撃への対応はもちろん、内部不正による情報漏えいといった新たな情報セキュリティへの意識の高まりは感じられつつも、具体的な対策強化に結びついてない企業の姿が見えてきた。企業環境が大きく変化する昨今、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対策強化のため、外部専門家知見の活用など幅広く取り組みを進めて

行きたいところだ。

＜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3680人を対象に2022年10月に調査