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

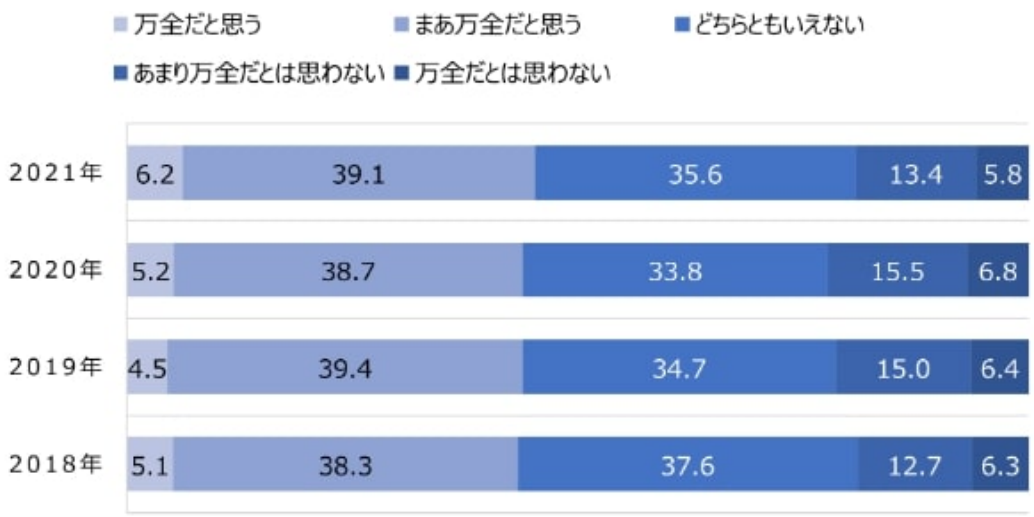
サイバー攻撃が後を絶たない。企業における情報セキュリティ対策はどうなっているか。対策の度合い、脅威に感じるもの、対策をするうえでの課題など最新動向について2021年12月に調査を行った。調査は日経BPコンサルティングのアンケートシステムにて、同社保有の調査モニター3098人を対象に実施した。

情報セキュリティ対策が万全だと45%が認識

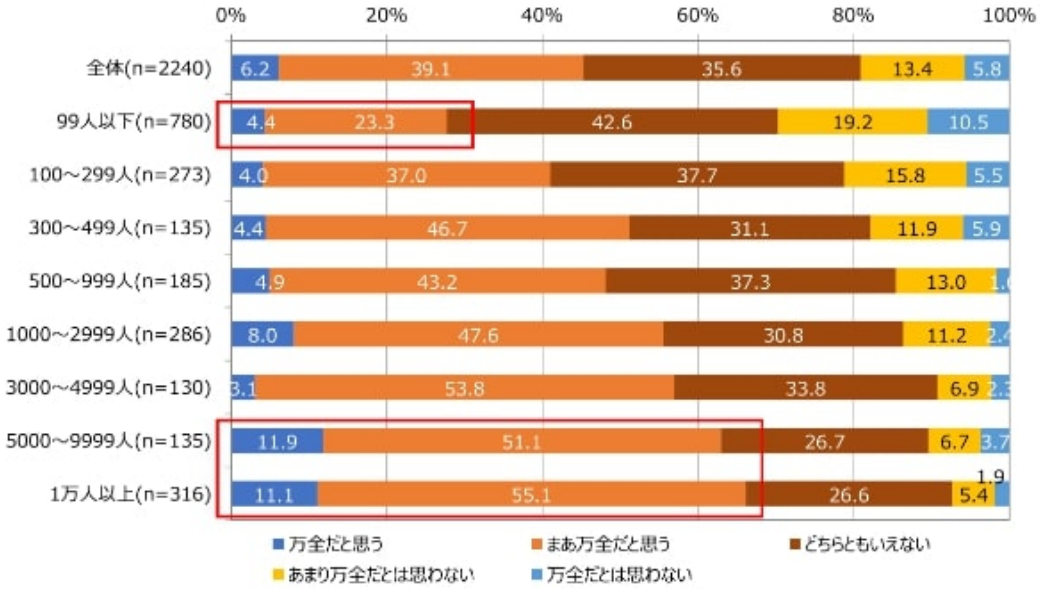
社内の情報セキュリティ対策が「万全だと思う」との回答は6.2%。「まあ万全だと思う」と合わせると45.3%が自社のセキュリティ対策について信頼感を示した。「あまり万全だとは思わない」は13.4%で前回比2.1ポイント、「万全だとは思わない」は5.8%で前回比1ポイント減。3.1ポイントとわずかながらも、前回調査より対策への不安感は減少した（図1-1）。

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）】

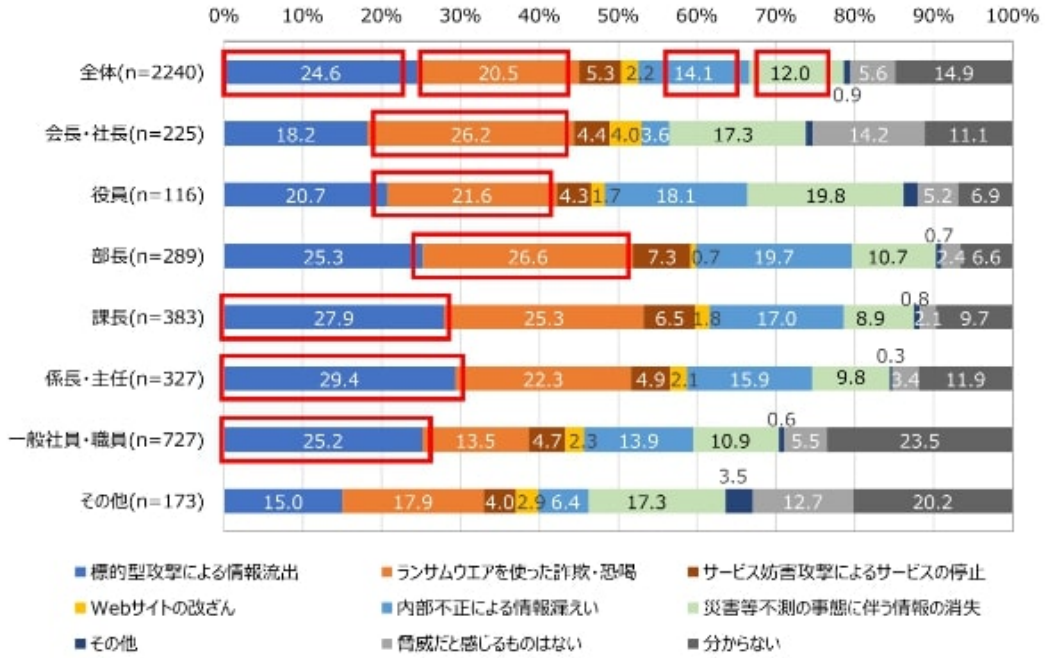


最も脅威なのは標的型攻撃。会社上層部はランサムウエアを警戒

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）。

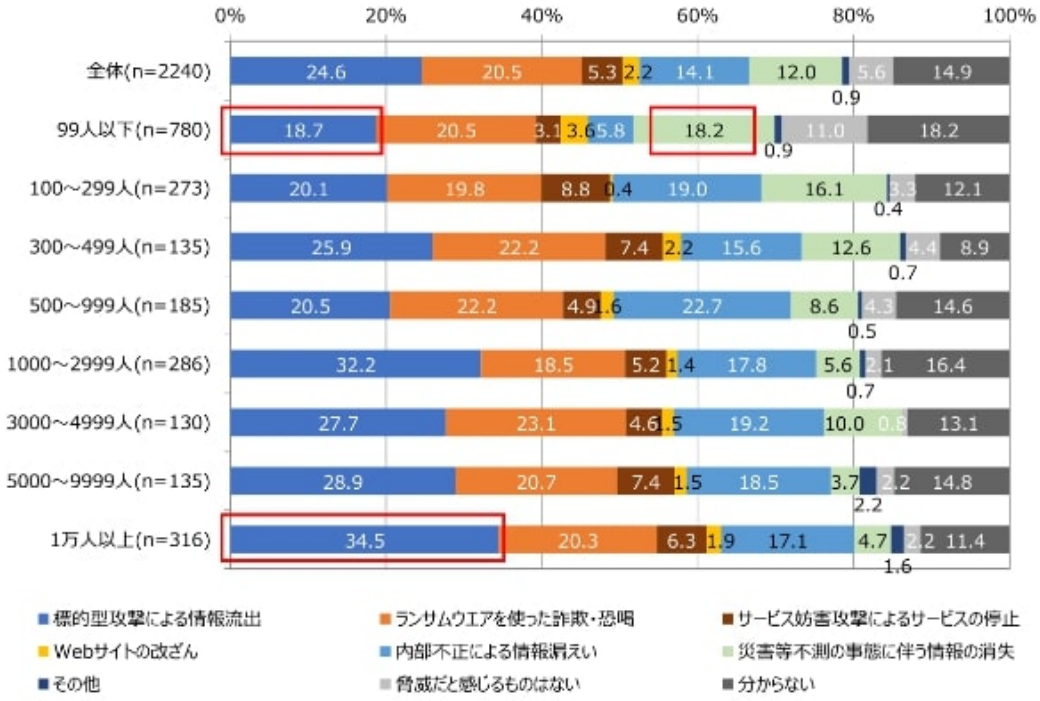
【図2-1 社内の情報資産管理で最も脅威と感じること（役職別）】



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)】

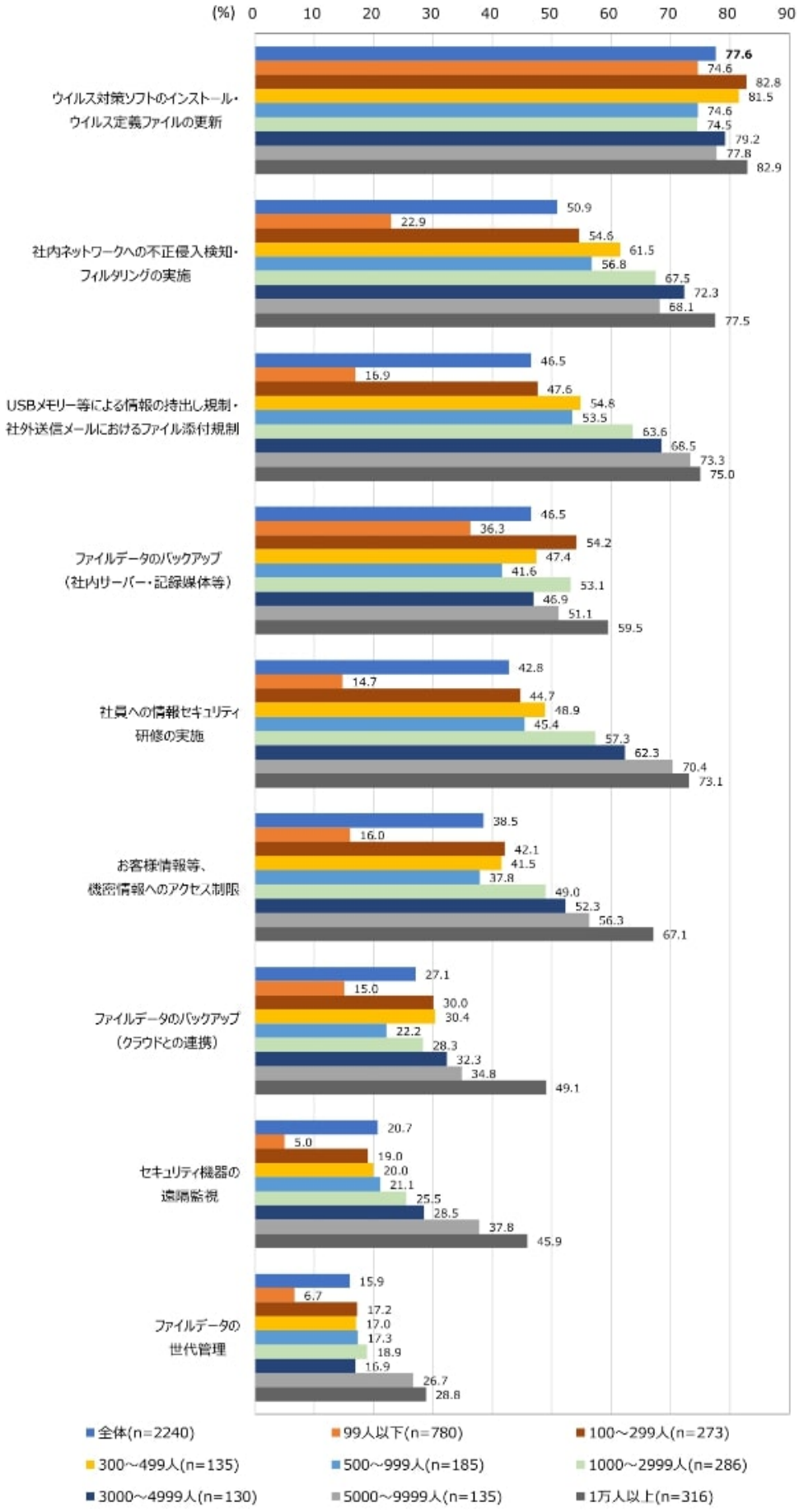


「ウイルス対策」は事業規模に差はなし。それ以外は小規模企業の対応遅れ

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77.6%。他の対策よりも圧倒的に導入が進み、かつ従業員規模別に見てもほとんど差が見られない。しかし、それ以外の項目では総じて中小企業の導入率は低く、大企業は導入率が高い結果が顕著となった。

例えば、「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」では99人以下の企業と1万人以上の企業では54.6ポイント差、「USBメモリー等による情報の持出し規制・社外送信メールにおけるファイル添付規制」では58.1ポイントの差がついた。「社員への情報セキュリティ研修の実施」においては58.4ポイントの差となった(図3)。

【図3 すでに導入されている対策(MA)】

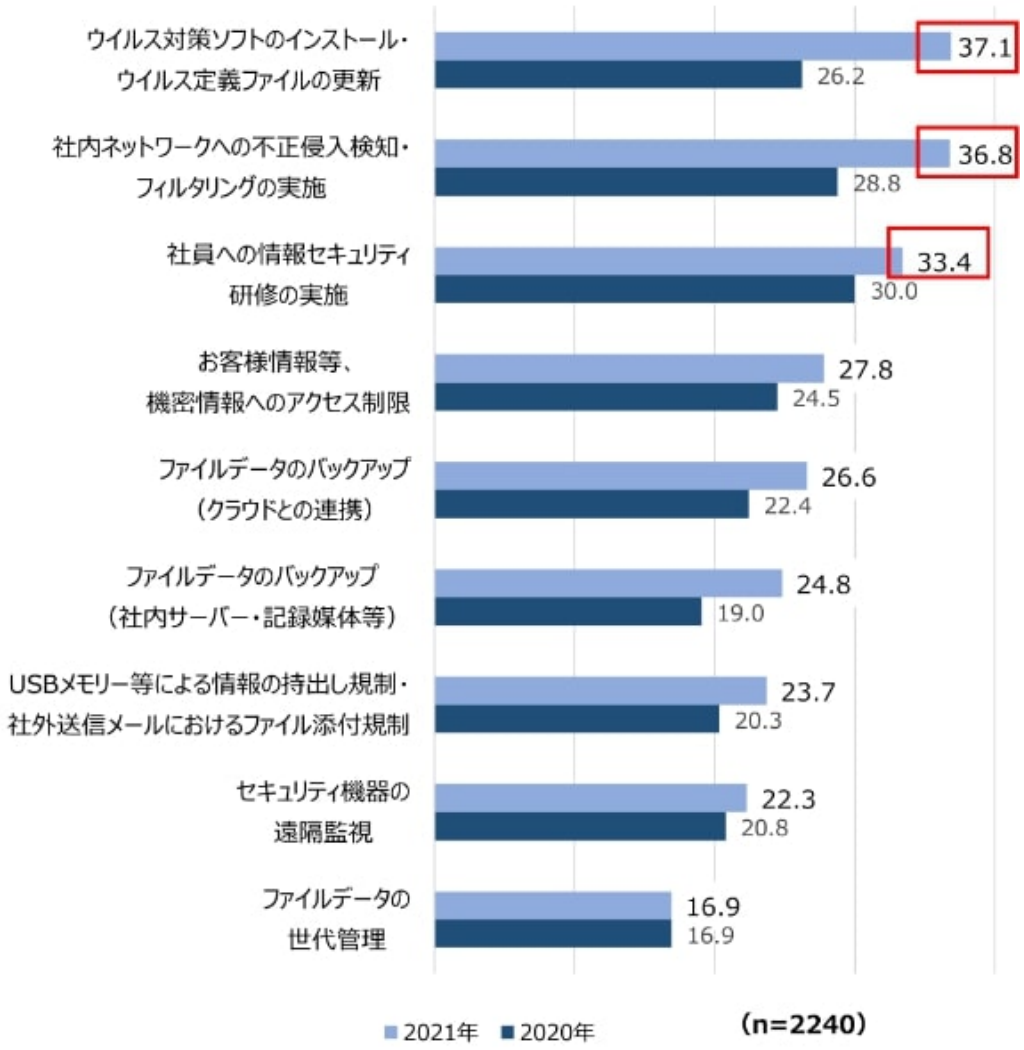

(%) 0 10 20 30 40 50 60 70 80 90
ウイルス対策ソフトのインストール・ウイルス定義ファイルの更新
77.6 74.6 82.8 81.5 74.6 74.5 79.2 77.8 82.9
社内ネットワークへの不正侵入検知・フィルタリングの実施
50.9 22.9 54.6 61.5 56.8 67.5 72.3 68.1 77.5
USBメモリー等による情報の持出し規制・社外送信メールにおけるファイル添付規制
46.5 16.9 47.6 54.8 53.5 63.6 68.5 73.3 75.0
ファイルデータのバックアップ（社内サーバー・記録媒体等）
46.5 36.3 54.2 47.4 41.6 53.1 46.9 51.1 59.5
社員への情報セキュリティ研修の実施
42.8 14.7 44.7 48.9 45.4 57.3 62.3 70.4 73.1
お客様情報等、機密情報へのアクセス制限
38.5 16.0 42.1 41.5 37.8 49.0 52.3 56.3 67.1
ファイルデータのバックアップ（クラウドとの連携）
27.1 15.0 30.0 30.4 22.2 28.3 32.3 34.8 49.1
セキュリティ機器の遠隔監視
20.7 5.0 19.0 20.0 21.1 25.5 28.5 37.8 45.9
ファイルデータの世代管理
15.9 6.7 17.2 17.0 17.3 18.9 16.9 26.7 28.8
全体(n=2240)
99人以下(n=780)
100～299人(n=273)
300～499人(n=135)
500～999人(n=185)
1000～2999人(n=286)
3000～4999人(n=130)
5000～9999人(n=135)
1万人以上(n=316)

今後重視する項目で「ウイルス対策」がトップ

情報セキュリティにおいて、今後さらに必要・重要と思われる対策は、2020年の結果と比較すると上位3つにエントリーした項目は同じだが、順位は入れ替わった。今回一番多かったのは、「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」(37.1%)で、前回3位から順位を上げ、ポイントも10.9増となった。2番目が「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」(36.8%)で8.0ポイント増。

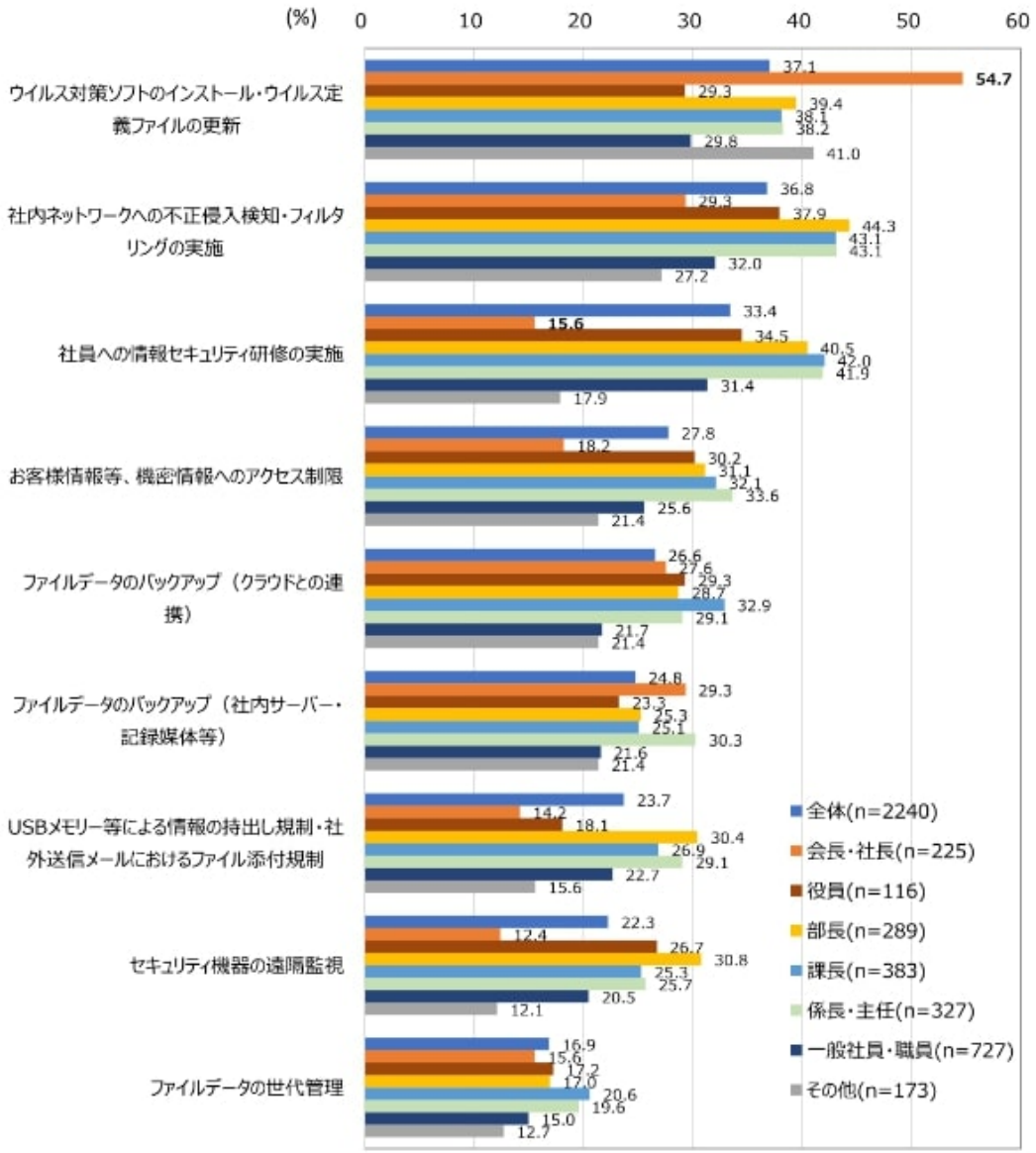
3番目の「社員への情報セキュリティ研修の実施」(33.4%)は前回トップから順位を下げたものの、3.4ポイントアップとなった。「ファイルデータの世代管理」だけは前回と選択率は変わらなかったが、それ以外の項目はすべて前回の数字を上回る結果となった(図4-1)。

【図4-1 今後さらに必要(重要)と思われる対策】



役職別で特徴的なのは、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54.7%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33.4%なのに対してこの層は15.6%。どの役職にも属さない「その他」17.9%と共に、他の役職より大幅に低い選択率となった(図4-2)。

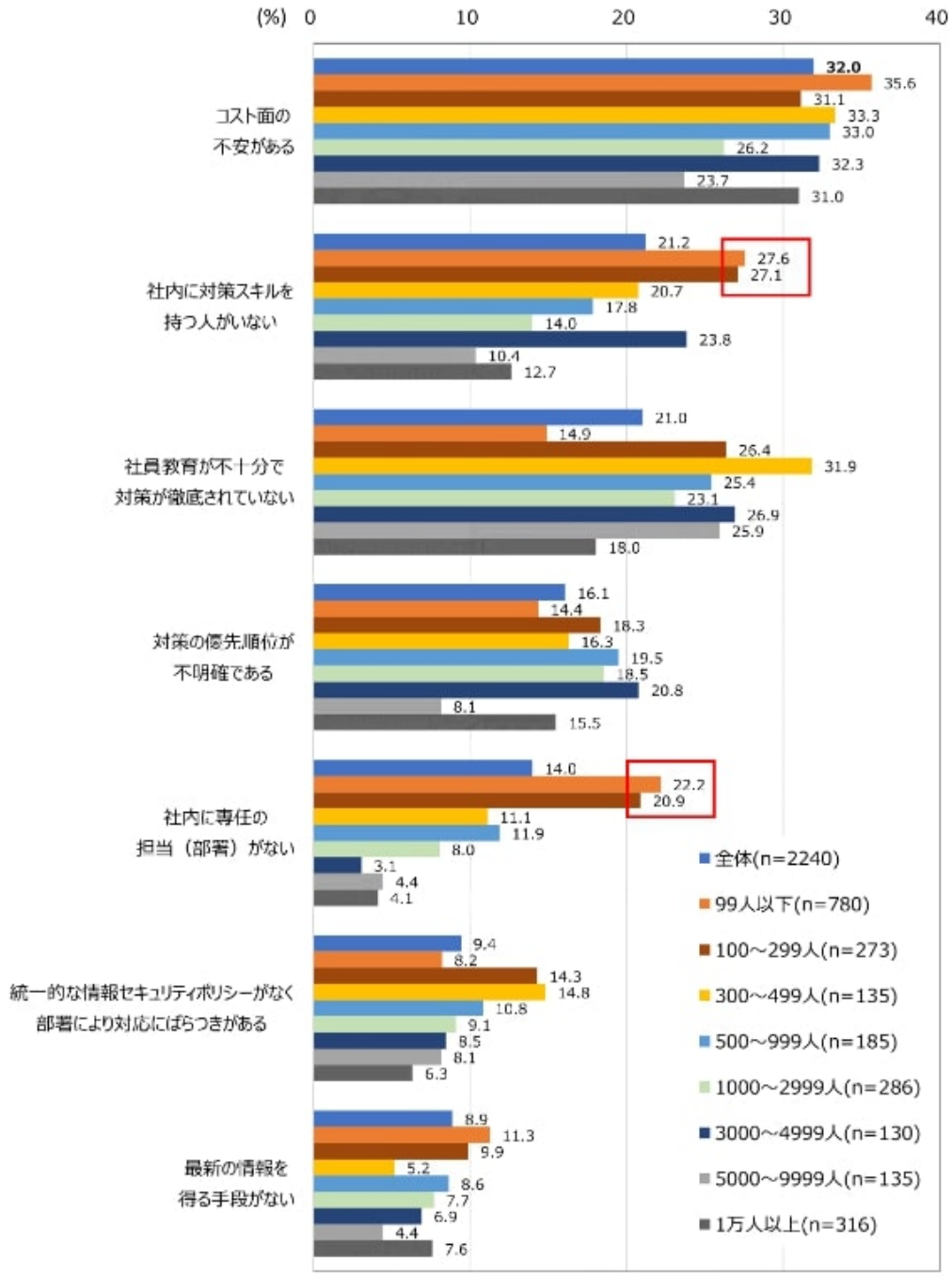
【図4-2 今後さらに必要（重要）と思われる対策（役職別）】



実施のうえでの課題はコストがトップ。中小では人材不足も顕著

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32.0%が選択した。企業規模による違いが明確だったのは、「社内に対策スキルを持つ人がいない」と「社内に専任の担当（部署）がない」という人材系の項目で、299人以下の企業でこの項目が突出して選ばれた。中小企業のIT人材不足は依然、根強い状況が見て取れる（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）】



＜企業の情報セキュリティ対策意識まとめ＞

・情報セキュリティ対策が「万全だと思う」「まあ万全だと思う」は45.3%

・従業員規模が大きくなるに従い、導入比率が高まる傾向

・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」の24.6%

・部長以上の役職では「ランサムウエアを使った詐欺・恐喝」の選択率がトップ

・最も導入率の高い対策は「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77.6%

・上記ウイルス以外の対策で中小企業の導入率は低く、大企業は導入率が高い傾向

・今後重視する対策のトップは「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」（37.1%）

・セキュリティ対策実施上の課題のトップは「コスト面の不安がある」（32.0%）

情報セキュリティへの意識の高まりは感じられつつも、特に中小規模の企業に関してはなかなか対策強化に結びついてないのが現状といえる。対策遅れの原因にはコスト面や人材面が挙げられるが、万が一の状況に陥ったときのリスクや損害を考えれば、それらを言い訳にして先延ばしにはできない。教育の徹底はもちろんのこと、IT人材を抱える余裕はなくてもアウトソーシングを検討してみるなどの対策を講じたい。

＜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3098人を対象に2021年12月に調査