

令和7年度テレワーク推進リーダーアンケート分析資料 (第2回目)

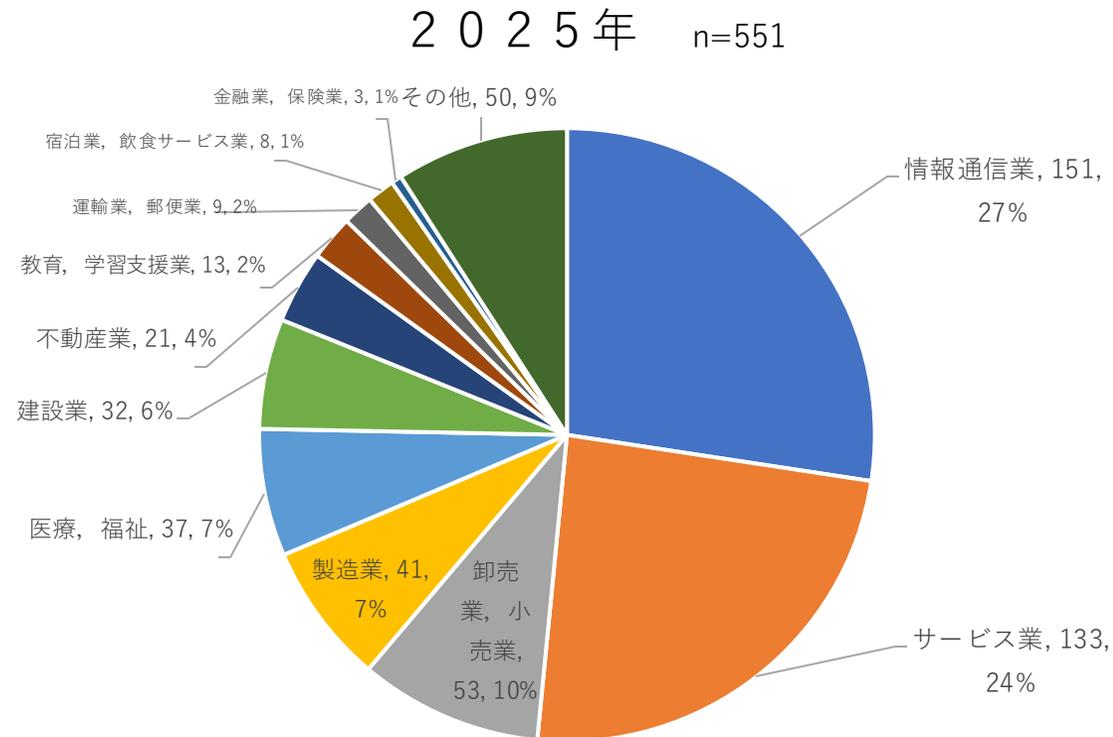
2026年1月

一般社団法人 日本テレワーク協会

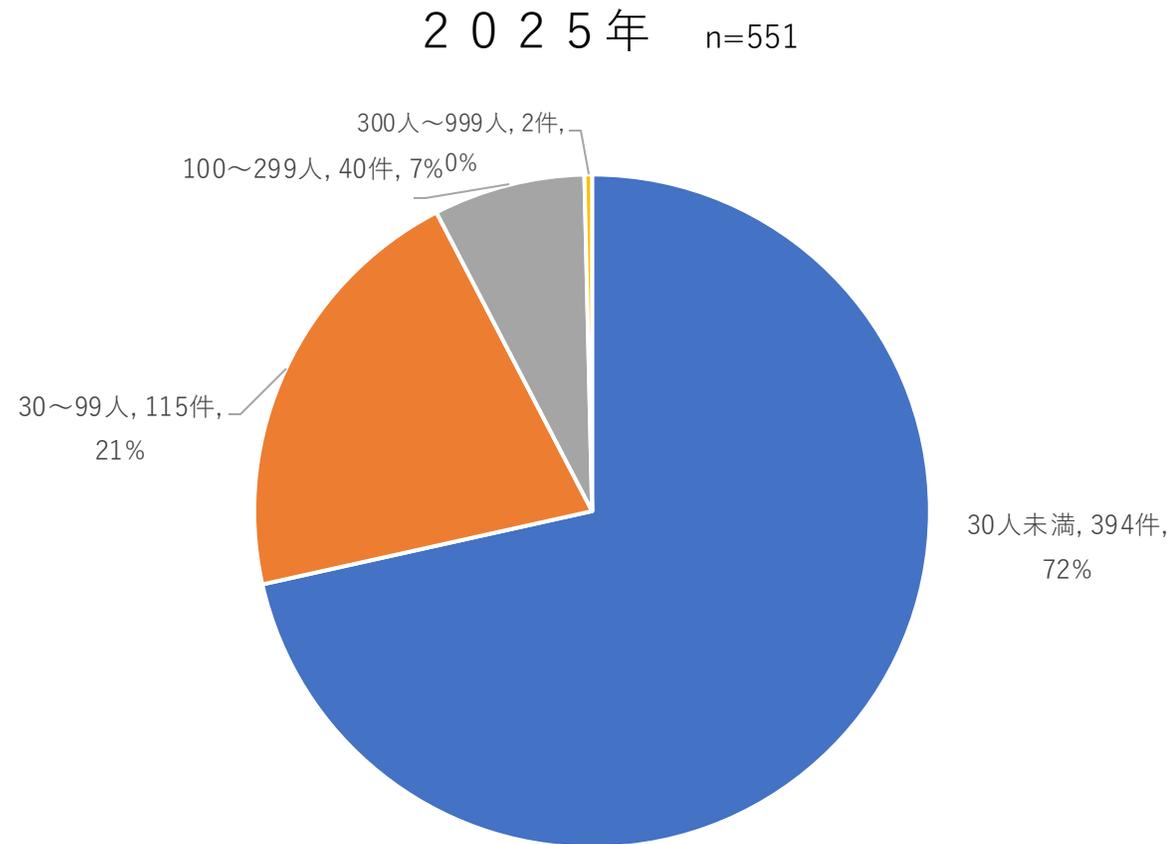
■アンケート実施内容

- ・ 期間：2025年12月4日～12月26日
- ・ 回答数：551件（2024年は438件）

1 御社の業種を選択ください。

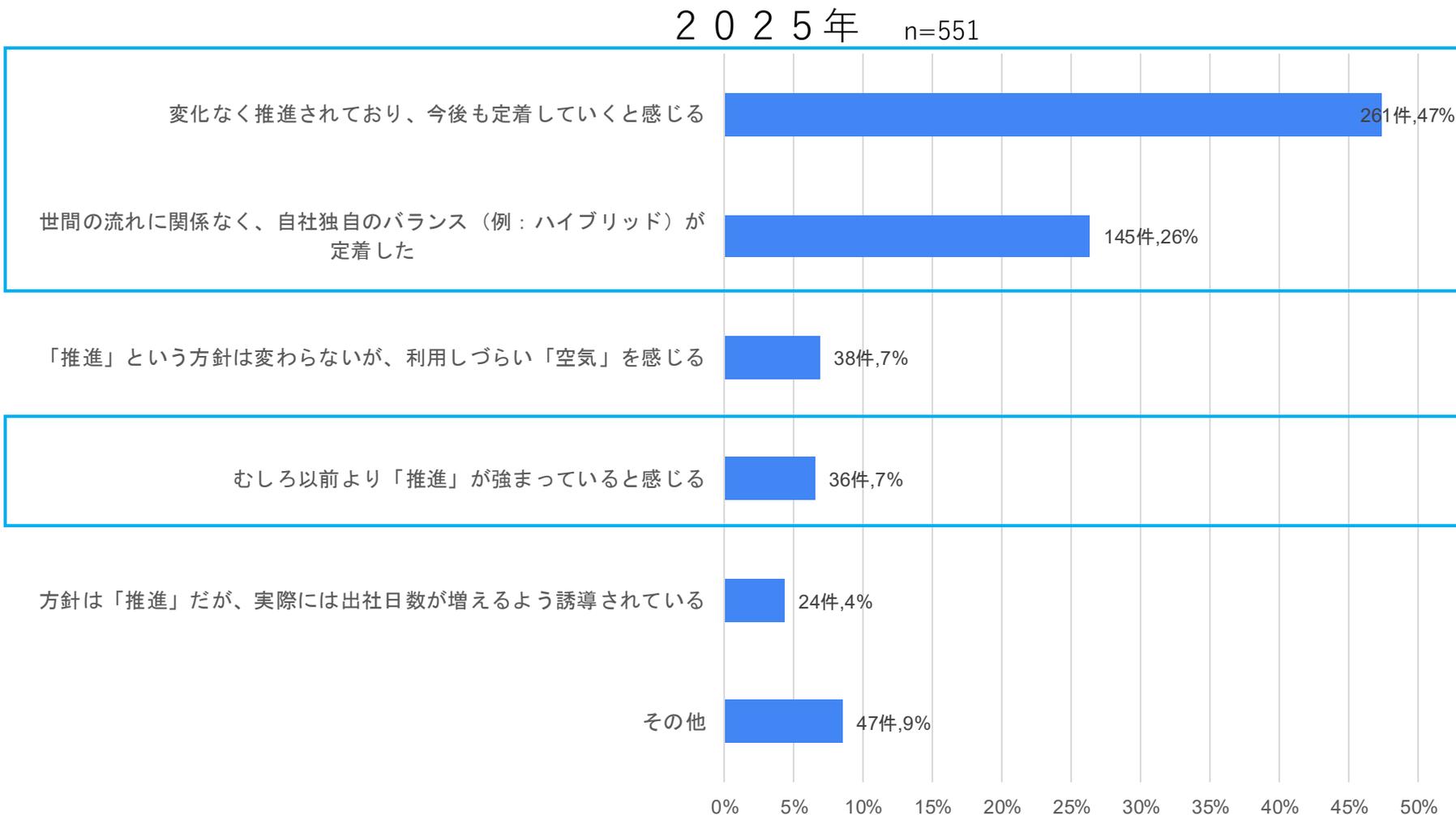


2 御社の企業規模を選択ください。



3 世間では「出社回帰」の動きも報道されていますが、御社（または部署）におけるテレワークの「位置付け」は、この1年間でどのように変化したと感じますか？ 最も近いものを選んでください。

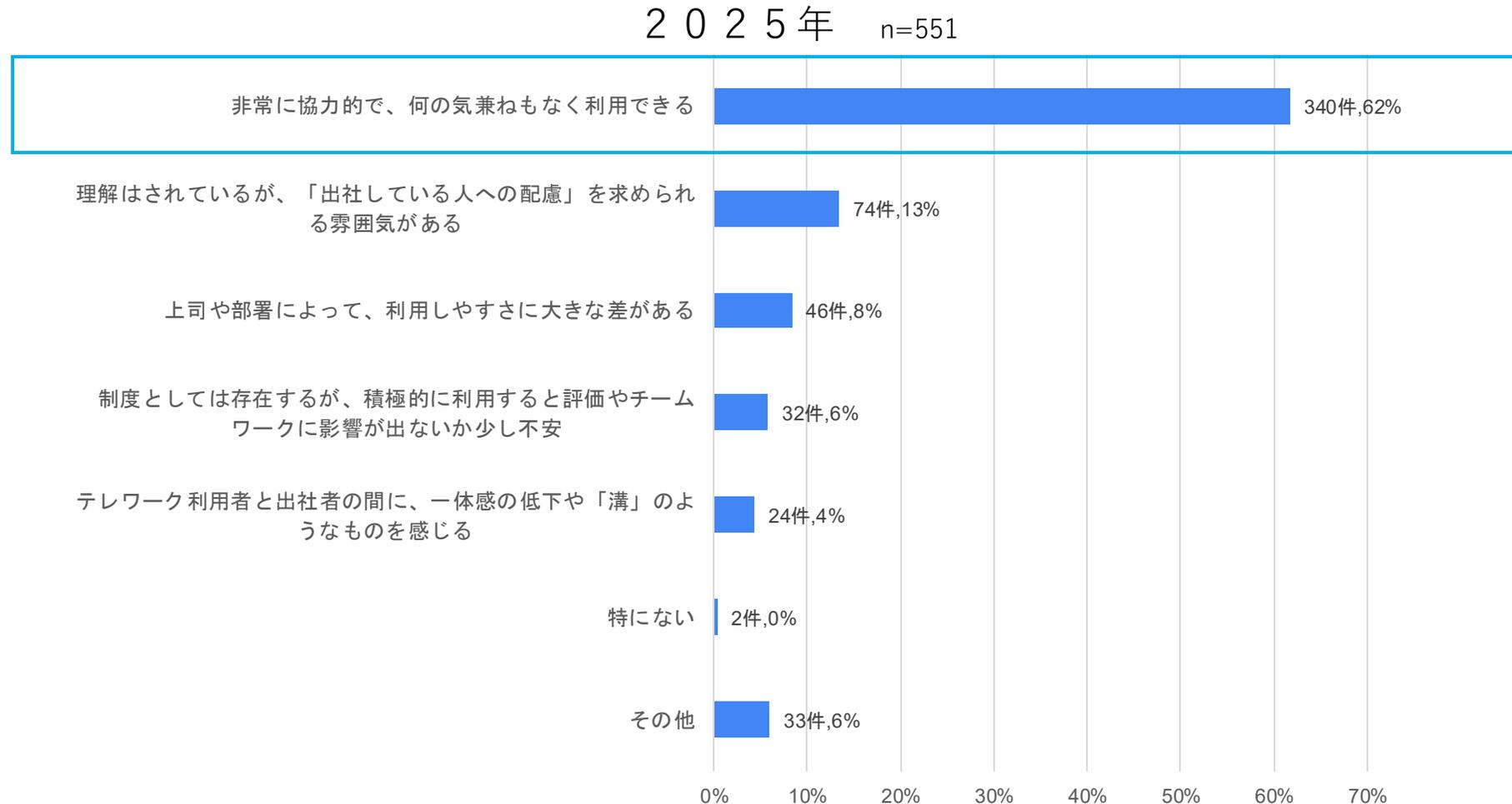
パワーアップリーダー各社が外部環境に流されず、テレワーク定着へ向けて自社の業務特性に合わせた出社とテレワークのバランス検討やテレワークの位置づけ見直しを行っていることが伺えます。



変わらず推進、定着が8割。

4 社員がテレワークを利用する際、上司や同僚、職場の「雰囲気（空気感）」について、どのように感じますか？ 最も近いものを選んでください。

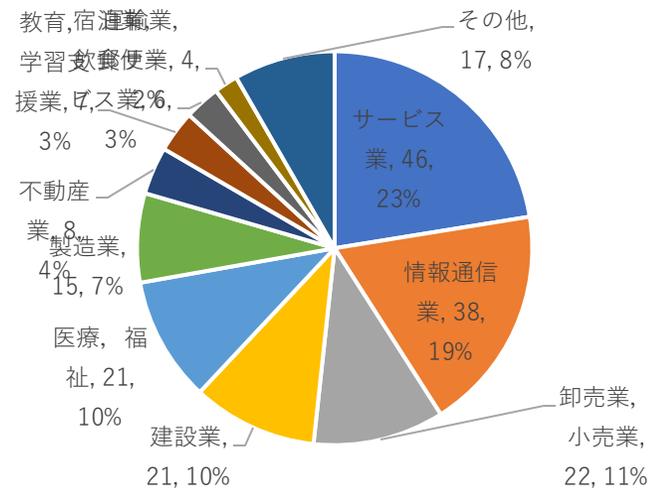
テレワーク利用にあたって、上司や同僚の雰囲気（空気感）が良好で心理的安全性が確保された環境である企業が約6割である一方利用しづらい企業が約3割あり、次のページでこちらの3割を深堀分析します。



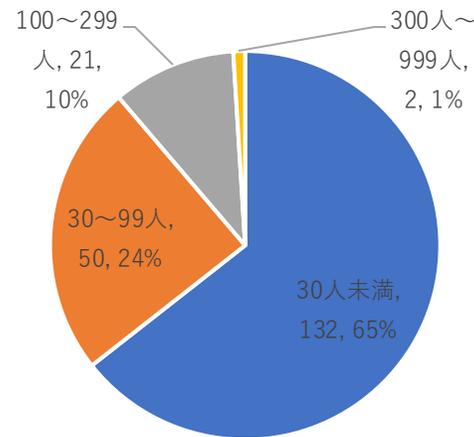
4-1 社員がテレワークを利用する際、上司や同僚、職場の「雰囲気（空気感）」について、どのように感じますか？最も近いものを選んでください。

テレワークを利用しづらい企業3割を深堀分析しましたが、業種、社員数に特徴は見られなかったです。テレワークの位置づけの変化においては、ハイブリッドとテレワーク推進の1位と2位が逆転しハイブリッドが定着している企業が多い状況です。

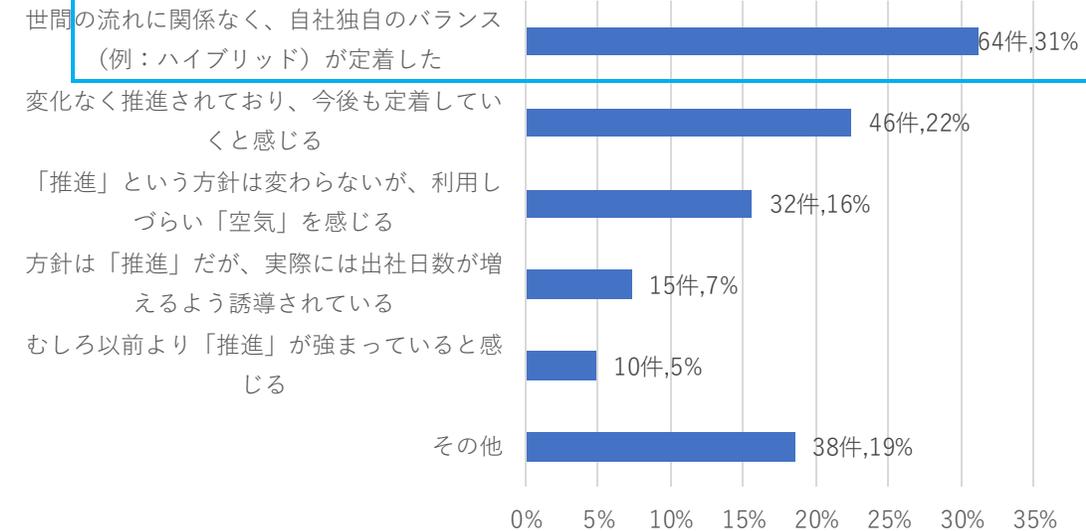
1. テレワークが利用しづらい企業
業種 n=205



2. テレワークが利用しづらい企業
社員数 n=205

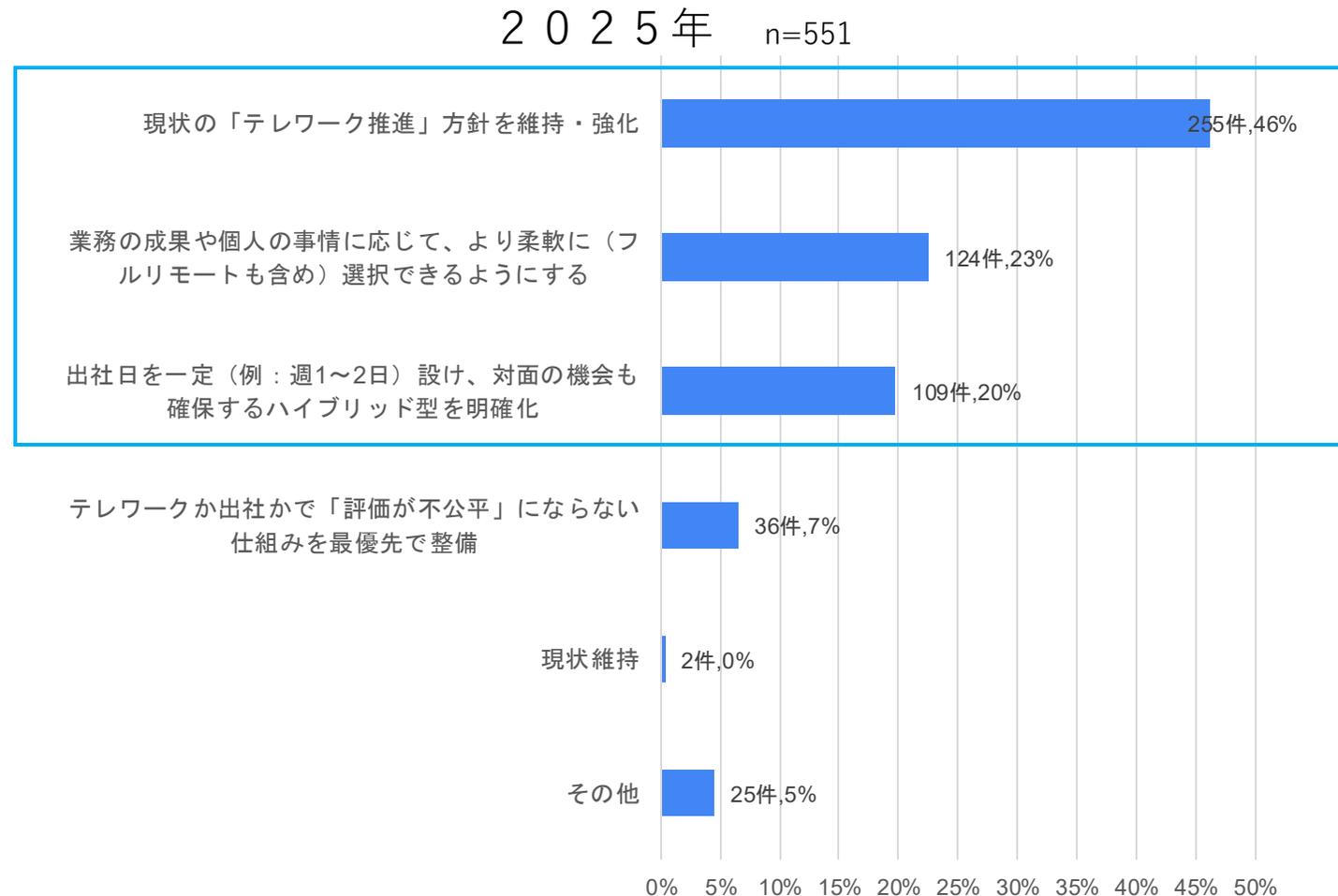


3. テレワークが利用しづらい企業
テレワークの位置づけ変化 n=205



5 御社が生産性の向上と働きやすさ（満足度）を両立させるために、今後テレワークと出社のバランスについてどのような方針ですか？

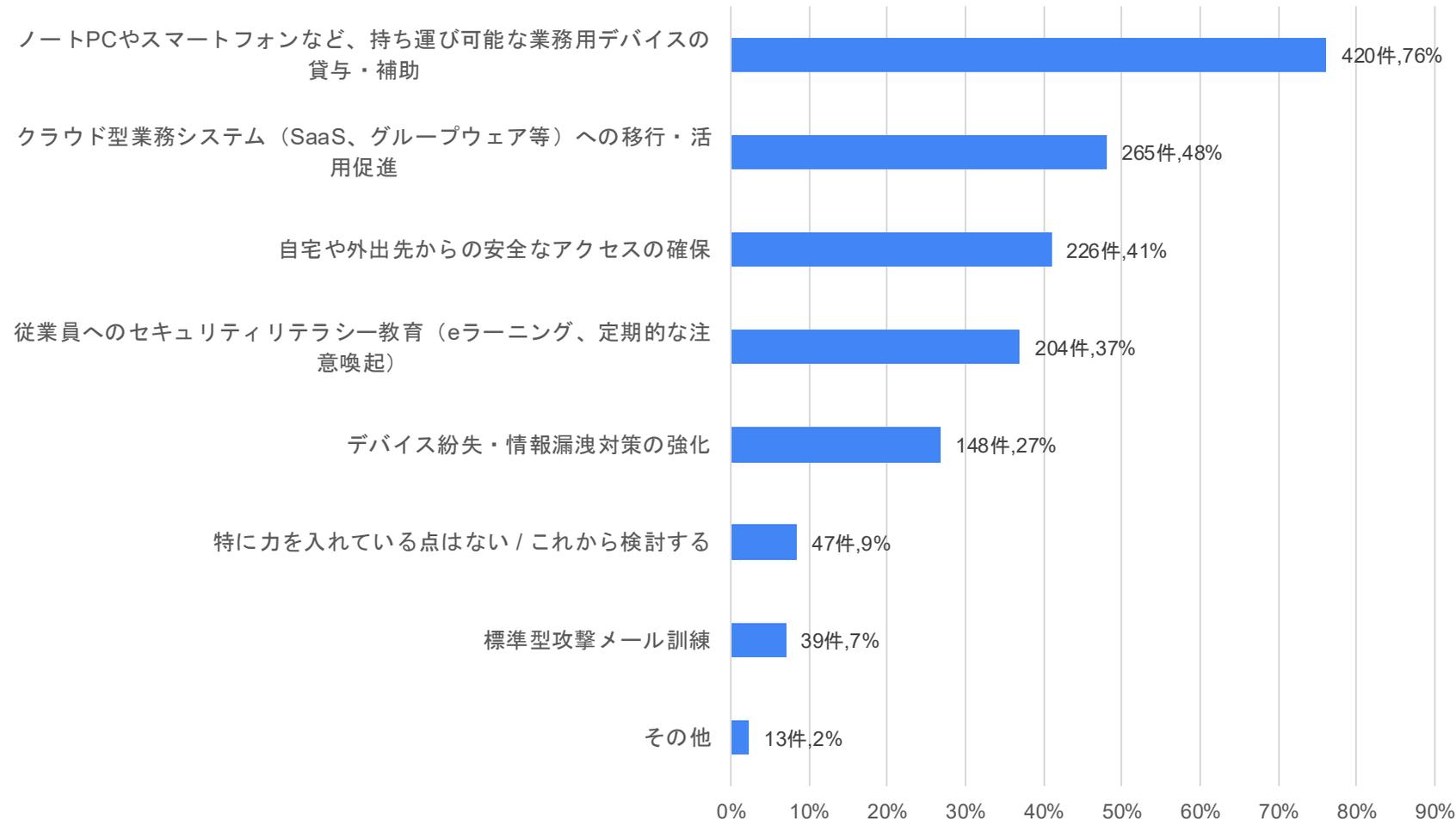
現状のテレワーク推進方針を維持・強化が最も多い一方、生産性向上と社員満足度の両立に向けて業務の成果や個人の事情から出社とテレワークの最適解を模索する企業の姿勢が伺えます。



6 御社では、従業員がモバイルワークなどの場所を問わず安全かつ効率的に働ける環境を推進するため、IT環境やセキュリティ面でどのような工夫や投資を行っていますか？（複数選択可）

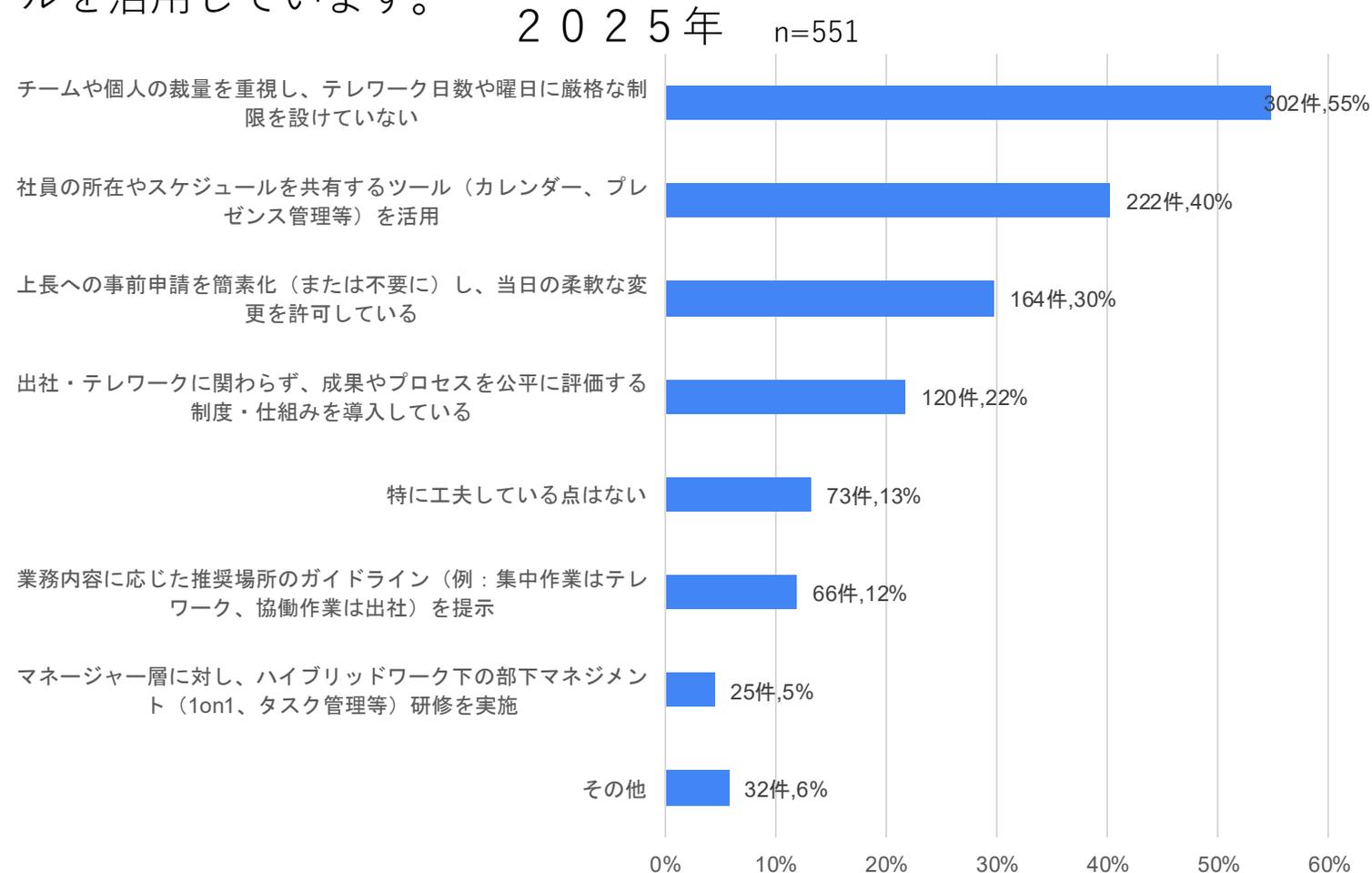
場所を問わず「安全かつ効率的」に働くため、ハード面（デバイス等）とソフト面（クラウド等）の両方で様々な工夫や投資を行っています。

2025年 n=551



7 従業員が「今日は出勤する」「今日はテレワークにする」といった働き方を自律的に選択できる環境を整えるため、御社が導入している制度や、運用上（マネジメント面・コミュニケーション面）で工夫している点は何ですか？（複数選択可）

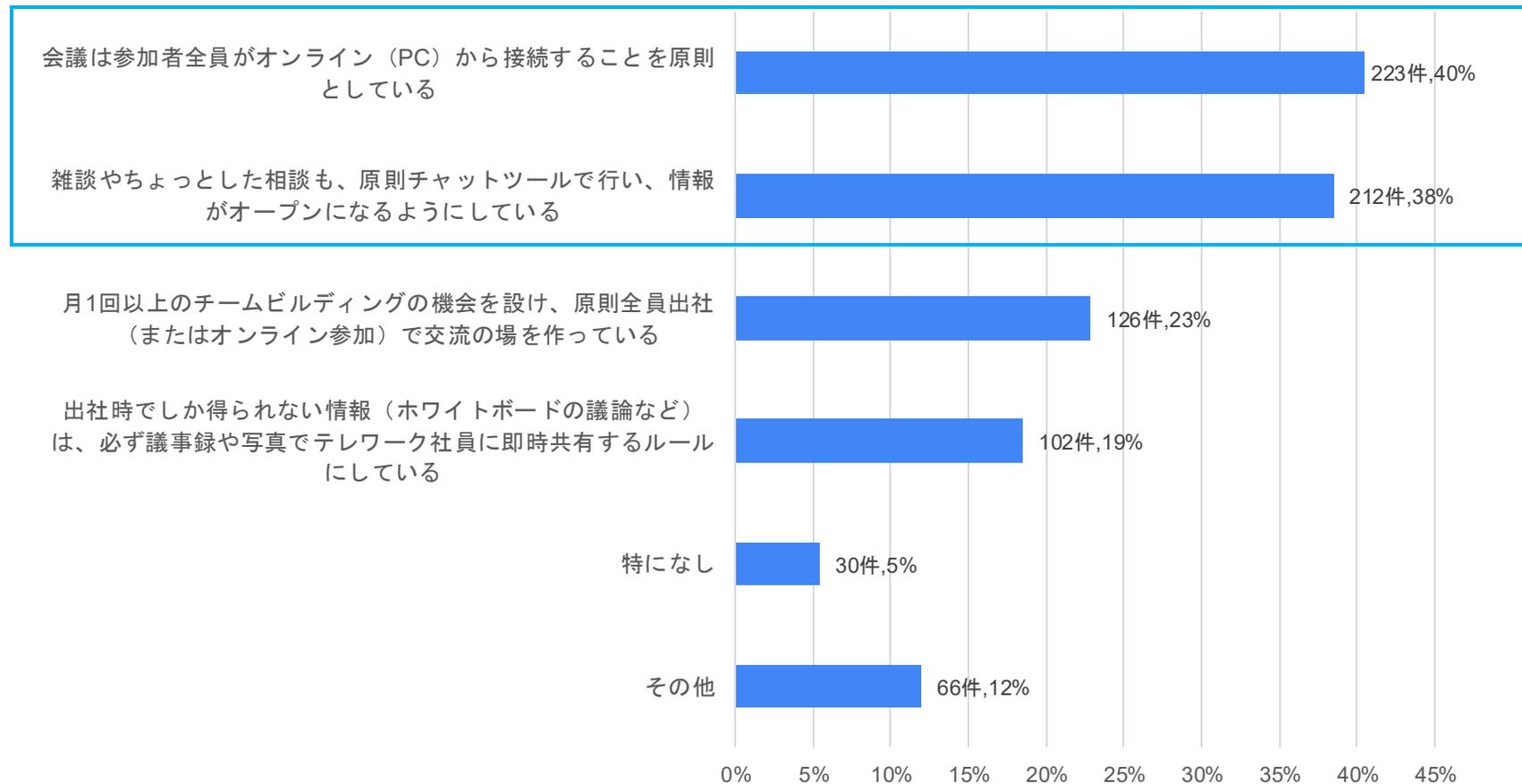
トップダウンではない柔軟な運用を可能にするため、チームや個人の裁量を重視するための評価制度やスケジュール共有ツールを活用しています。



8 出社している従業員とテレワークの従業員が混在するチームにおいて、情報格差やコミュニケーションの質に差が出ないように、御社が「特に意識して」取り組んでいる工夫について教えてください。（複数選択可）

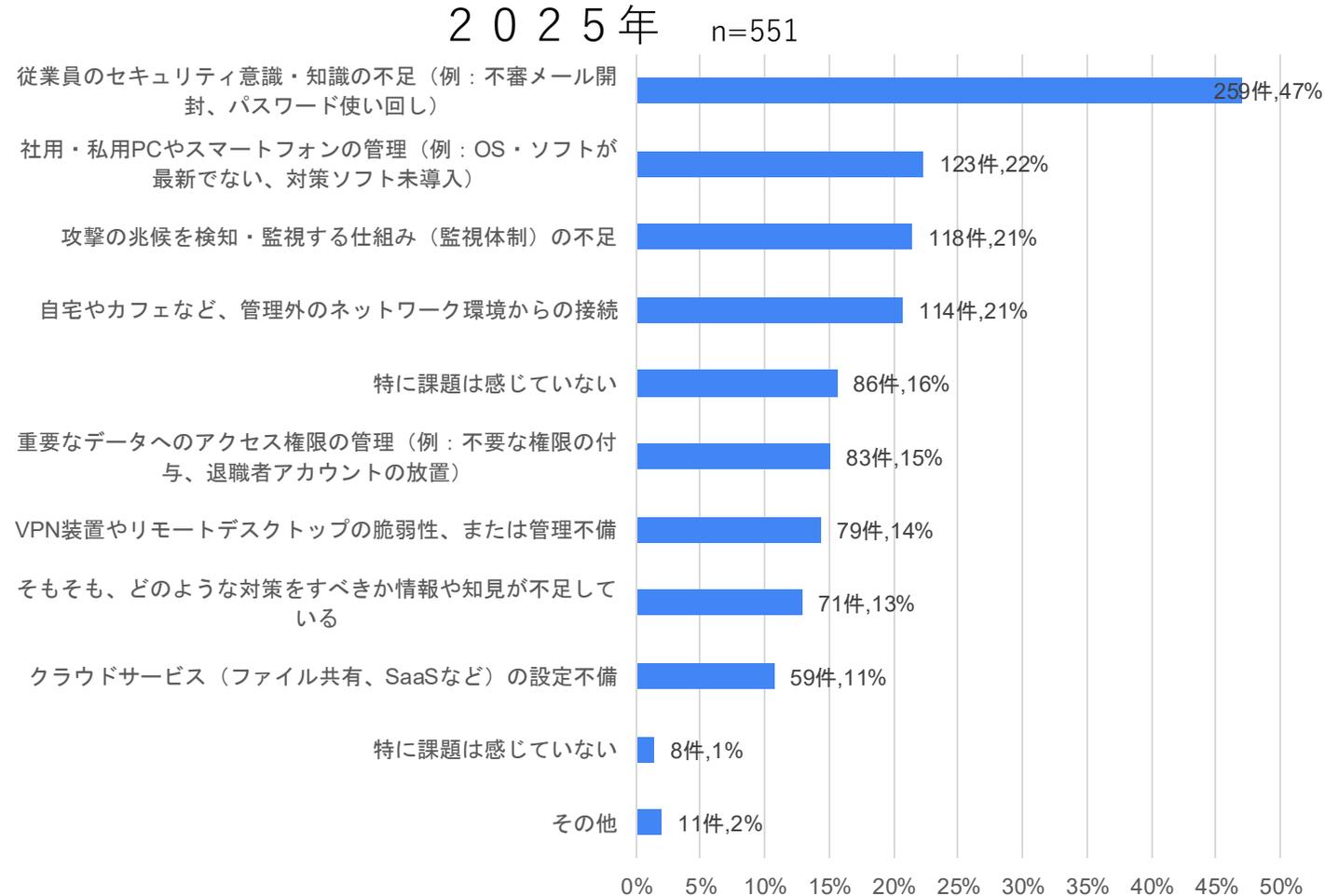
対面優位の文化を脱却し、デジタルを主軸とした平等な情報共有を行うために全員がPCからの接続を原則としたり、雑談や相談も原則チャットツールで行うなどの工夫をしています。

2025年 n=551



9 テレワークの導入・拡大に伴い、ランサムウェアなどのサイバー攻撃リスクについて、御社が現在最も課題（または脆弱性）と感じている点はどれですか？（最も当てはまるもの2つまで選択）

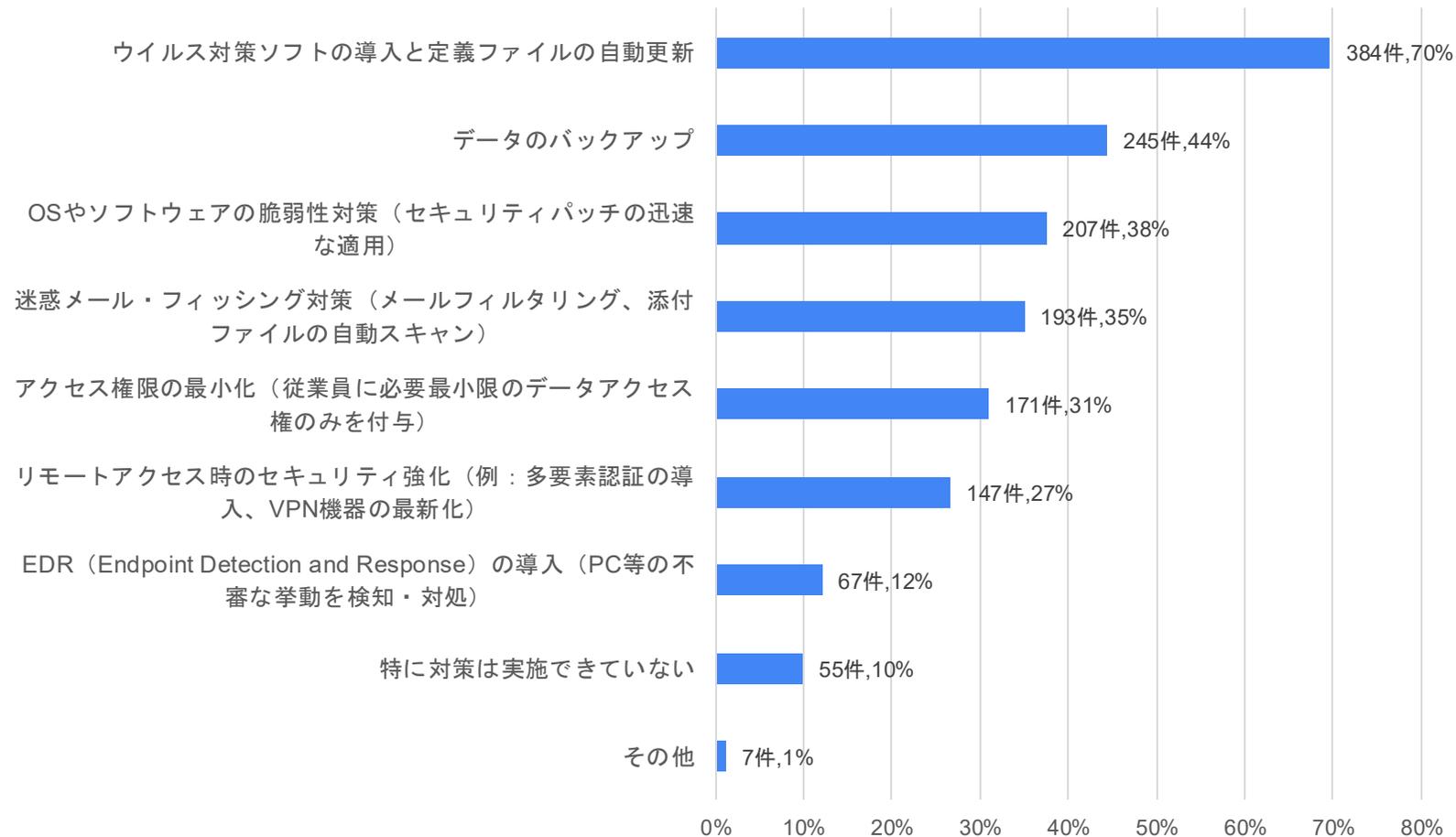
従業員のリテラシー不足やエンドポイントの弱点など、現場が抱える具体的な懸念材料が浮き彫りになっています。



10 ランサムウェア攻撃による被害を未然に防ぐため、御社で現在実施している技術的な対策はどれですか？（複数選択可）

ウィルス対策ソフトの導入と定義ファイルの自動更新が最も多く、様々な対策を実施しています。特に対策は実施できていないものも10%あり、危険な状況です。

2025年 n=551



1 1 万が一、ランサムウェアに感染した場合の「復旧」に関して、御社のバックアップ体制やインシデント（事故）対応の準備状況について、当てはまるものを選んでください。（複数選択可）

感染を前提としたバックアップ対策をしている企業が多いが、事後対応の計画策定や訓練などへの対応は少なく、対策や準備は不十分との回答も25%と多いです。

