テレワークセキュリティに関する実態調査（R3年度）

➢ 企業等におけるテレワークに関するセキュリティ等の実態を把握するための調査をWebアンケートにより実施。
期間：2021.12.10-2022.1.14　　回答数：8264（うちテレワーク実施企業2640）
調査手法：調査票郵送・Web回答　対象地域：全国　対象数：各30000(従業員等が10名以上)（昨年調査回答者(4856)＋昨年調査非対象者(25144)）

スクリーニング調査　※スクリーニング設問は8264社が回答
S-1　テレワークの導入状況
S-2　テレワークを導入しない理由
S-3　セキュリティに関する具体的な懸念点
S-4　テレワーク導入に当たり課題と考えている点
S-5　会社所有PC端末のOSの種類
S-6　Windows8、7、XPの公式サポート期限切れの認知状況
S-7　サポート期限が切れたPC端末を使用している理由
S-8　サポート期限が切れているPC端末の割合

1　テレワーク導入状況　※これ以降の設問はテレワーク導入済みの2640社が回答
1-1　テレワークの導入時期
1-2　今後のテレワークの活用予定
1-3　今後テレワークを活用しないまたはやめた理由
1-4　最も多くテレワークを利用した時期と利用割合

2　テレワーク実施における各種対策
2-1　テレワークを実施する上での検討・実施事項（システム関係）
2-2　テレワークを実施する上での検討・実施事項（セキュリティ対策）
2-3　テレワーク時のクラウドサービスの利用状況
2-4　テレワーク方式の選定に当たり最も重視した観点

3　テレワーク端末　※3-3～3-6はS-5～S-8と同設問
3-1　テレワーク利用を許可している端末の形態
3-2　テレワーク利用する会社支給PC端末のOSの種類
3-3　会社所有PC端末のOSの種類
3-4　Windows8、7、XPの公式サポート期限切れの認知状況
3-5　サポート期限が切れたPC端末を使用している理由
3-6　サポート期限が切れているPC端末の割合
3-7　サポート期限が切れたOSが入っている端末を使用しないようにする対策

4　その他のテレワーク利用製品
4-1　テレワークで利用している端末側のウイルス対策製品
4-2　テレワークで利用している端末側のデバイス管理製品・サービス
4-3　社内システムやドキュメントにアクセスする際に用いるブラウザ等
4-4　インターネットにアクセスする際に利用しているブラウザ
4-5　リモートアクセス製品のうちVPN製品
4-6　リモートアクセス製品のうちリモートデスクトップ製品
4-7　社内打合せで使うWEB会議システム
4-8　社外打合せで使うWEB会議システム
4-9　従業員・職員が利用しているメールサービス
4-10　従業員・職員が利用しているチャットツールの製品
4-11　従業員・職員が利用しているストレージサービスの製品
4-12　従業員・職員が利用しているネットワークセキュリティ製品
4-13　従業員・職員が利用している仮想デスクトップ方式の製品
4-14　従業員・職員が利用しているアプリケーション・ラッピング方式の製品

5　情報セキュリティ対策
5-1　情報セキュリティ対策に関する取組の実施状況
5-2　情報セキュリティ対策に関する取組が未実施の理由
5-3　情報セキュリティ対策に関する組織体制
5-4　社内で最もセキュリティに詳しい者の水準

6　テレワーク時のセキュリティ対策を推進するに当たって
6-1　テレワークの導入に当たり課題となった点
6-2　セキュリティ確保への具体的な課題
6-3　現在、行っているセキュリティ対策
6-4　セキュリティ対策の継続に当たっての検討課題

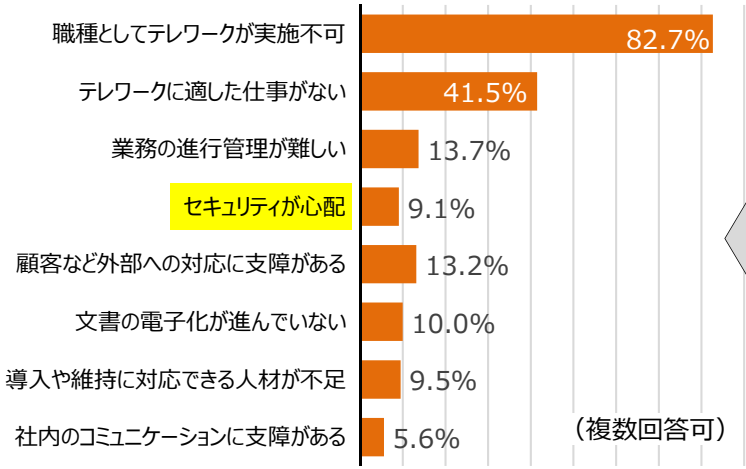
7　総務省が作成するガイドライン
7-1　「テレワークセキュリティガイドライン」の認知度
7-2　「テレワークセキュリティガイドライン」で参考になった内容
7-3　「テレワークセキュリティガイドライン」で記載を充実させた方がよい内容
7-4　「テレワークセキュリティの手引き」の認知度
7-5　「テレワークセキュリティの手引き」で参考になった内容
7-6　「テレワークセキュリティの手引き」で記載を充実させた方がよい内容
7-7　「設定解説資料」の認知度
7-8　テレワークセキュリティに関するキーワードの認知度

テレワークセキュリティに関する実態調査結果①

- 2020年4月の緊急事態宣言をきっかけに、以降テレワークが急拡大。今後も活用する予定との回答が75%を超え、テレワーク実施企業での定着が見られる。

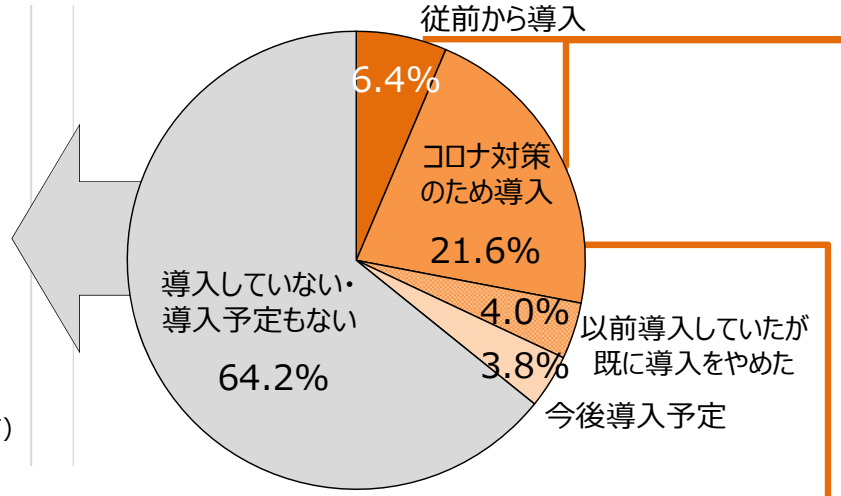
テレワークを導入しない理由

（n=5297：テレワーク未導入企業）



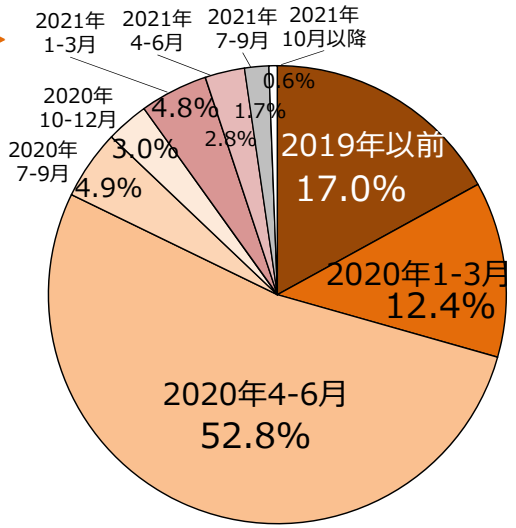
テレワークの導入状況

（n=8264：全回答者）



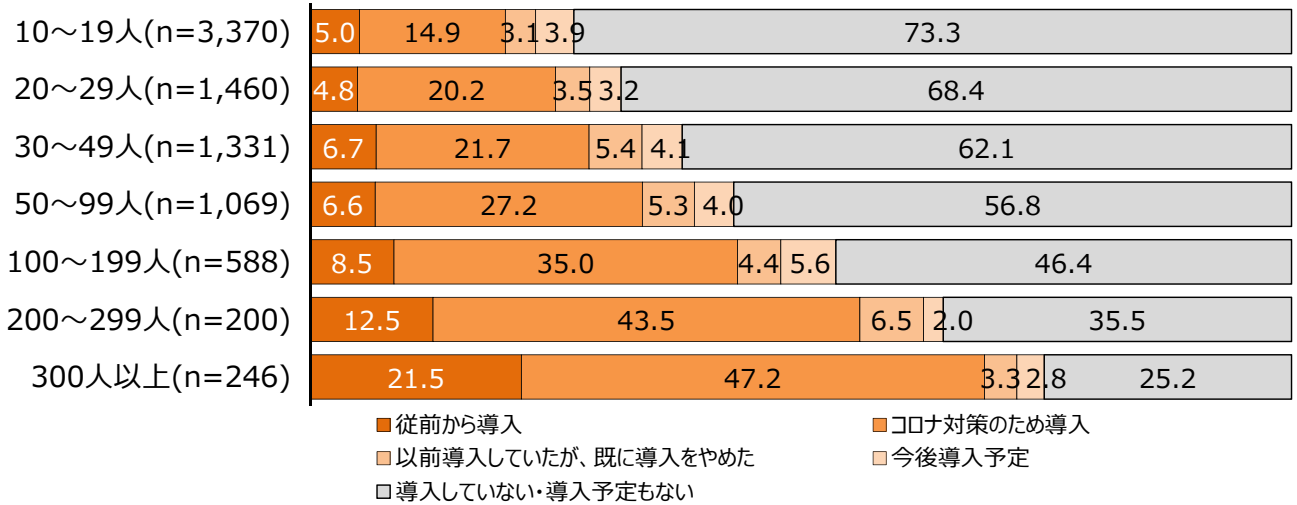
テレワークの導入時期

（n=2630：テレワーク実施企業）



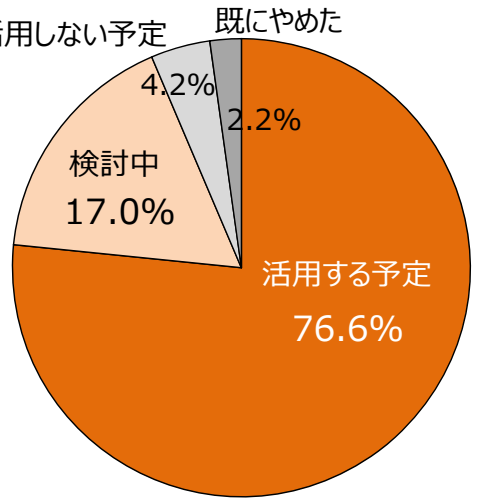
テレワークの導入状況（従業員規模別）

（n= 8264 ：全回答者）



今後のテレワーク活用予定

（n=2231：従前から及びコロナ対策でテレワーク導入した企業）

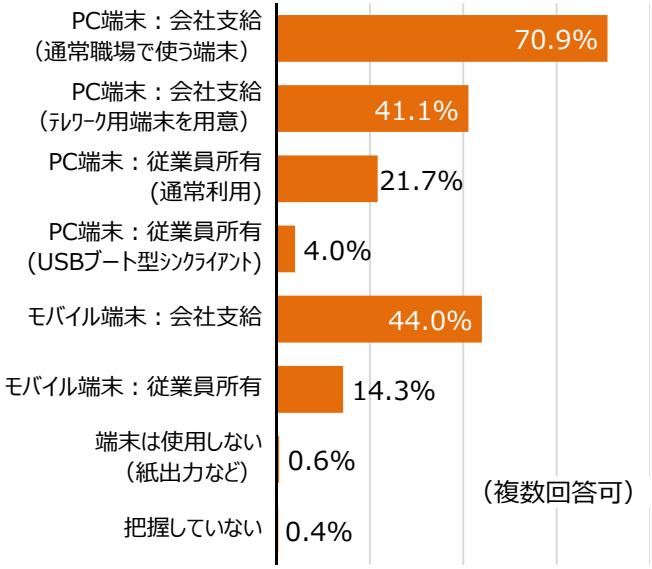


テレワークセキュリティに関する実態調査結果②

- テレワークでは会社支給端末や、クラウドサービスが広く利用されている。
- テレワークの導入に当たっては、「セキュリティの確保」が依然大きな課題となっている。

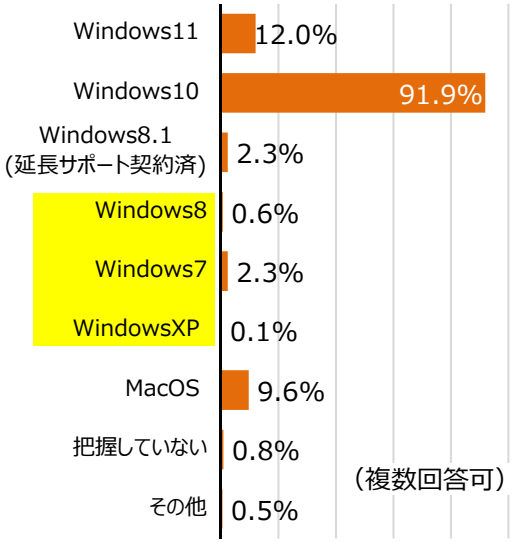
テレワーク利用を許可している端末

（n=2634：テレワーク実施企業）



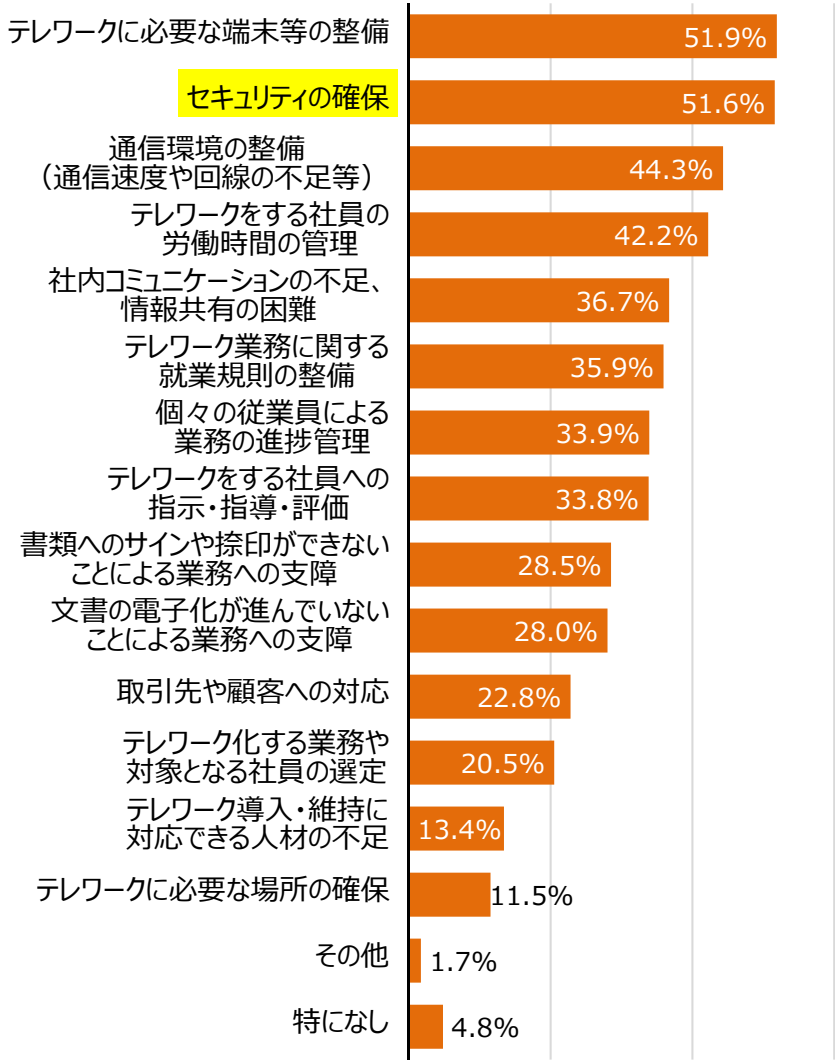
会社支給PC端末のOS

（n=2352：会社支給PC端末を利用）



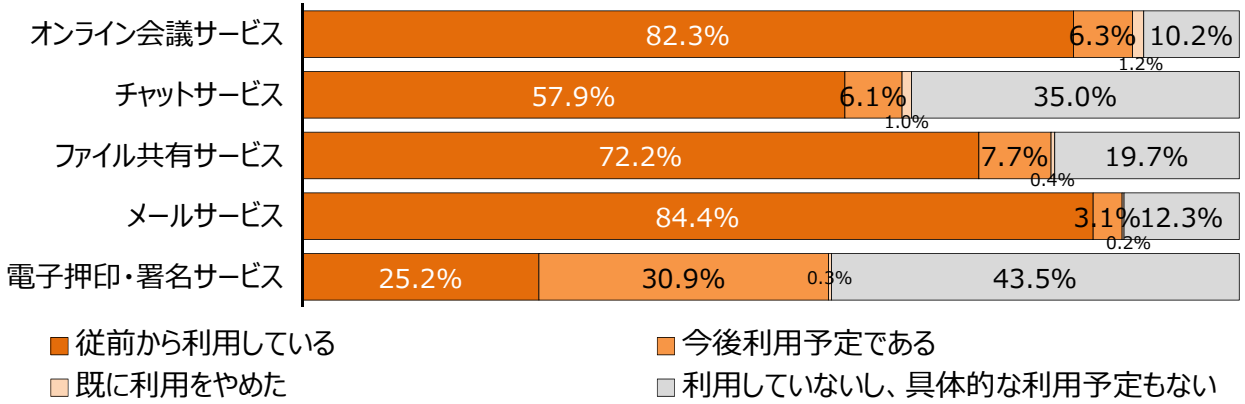
テレワークの導入に当たり課題となった点

（n=2624：テレワーク実施企業）



クラウドサービスの利用状況

（n=2398～2593：テレワーク実施企業）

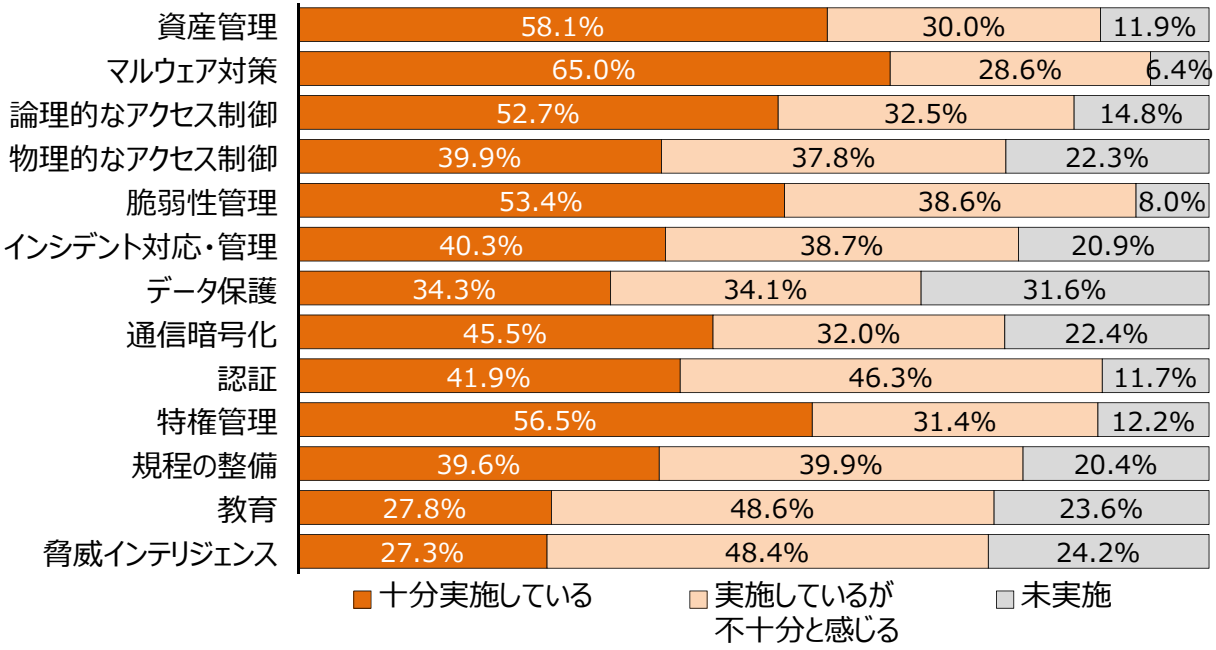


テレワークセキュリティに関する実態調査結果③

- 「マルウェア対策」は6割半ばが十分実施、一方で「教育」「脅威インテリジェンス」は７割強が不十分か未実施と回答。
- 多くの企業で情報セキュリティ対策の組織体制整備ができていない状況が見受けられる。

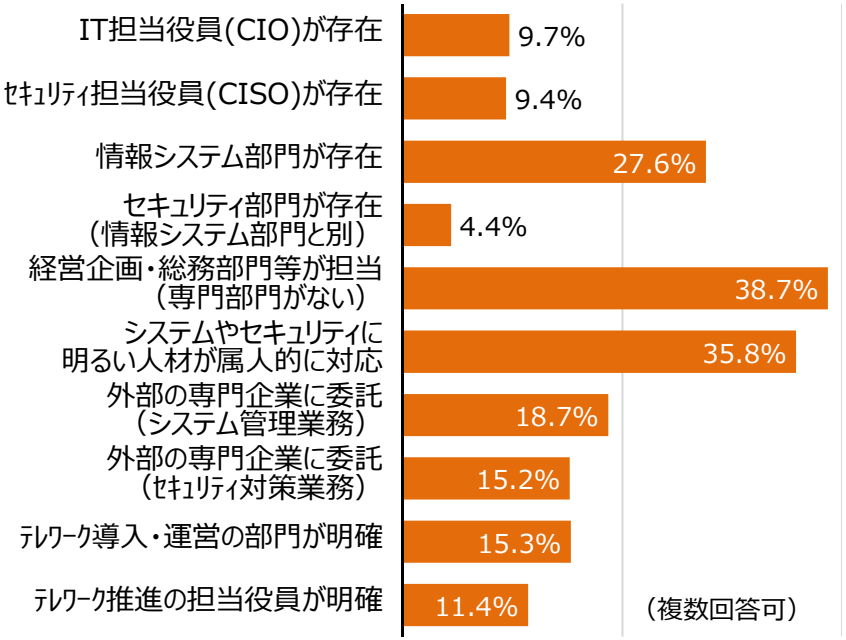
情報セキュリティ対策に関する取組の実施状況

（n=2590～2609：テレワーク実施企業）



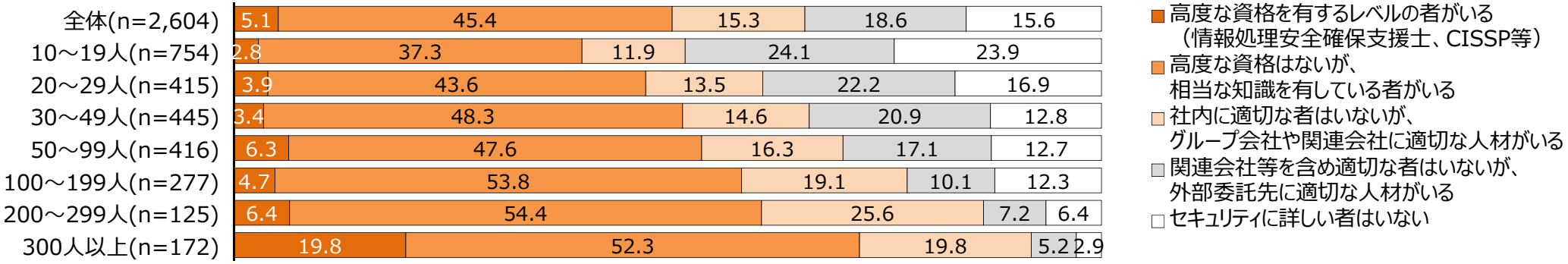
情報セキュリティ対策に関する組織体制

（n=2523：テレワーク実施企業）



情報セキュリティ対策に関する従事者の水準

（n=2604：テレワーク実施企業）

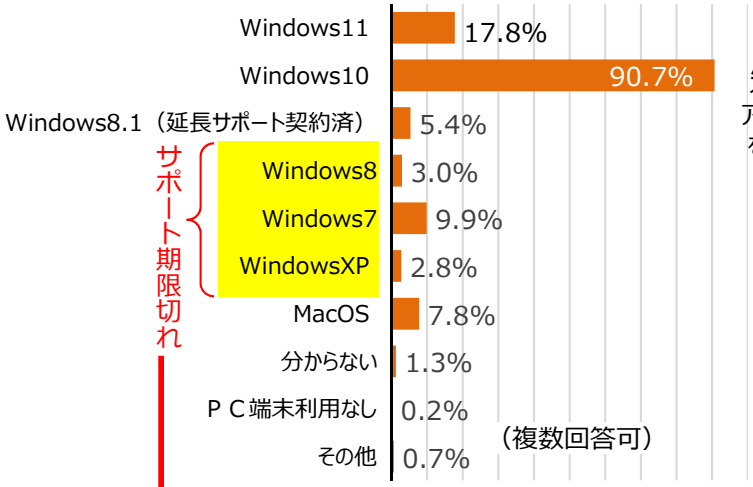


テレワークセキュリティに関する実態調査結果④

- サポート期限切れOSが一部で使用され続けており、製造業や、大規模企業に多い傾向。
  →製造装置やシステムに組み込まれており容易に更新できないような場合が想定
- サポート期限切れOSが危険という認識を持っていない場合も見受けられる。

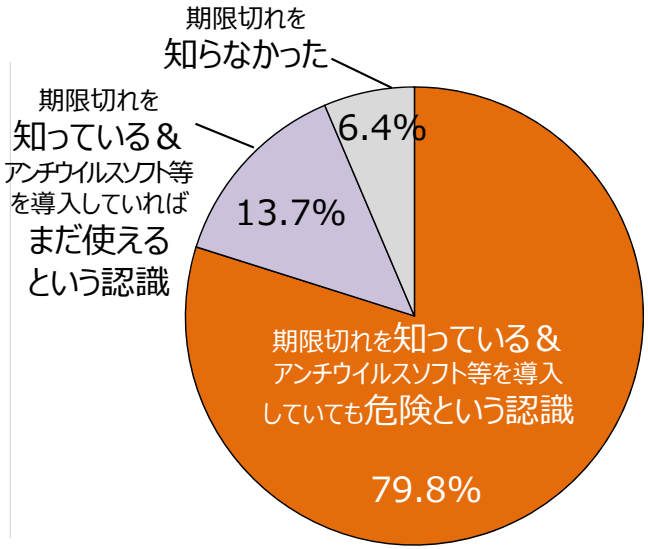
職場・テレワークに関わらず会社所有PC端末のOSの種類

（n=7901：全回答者）



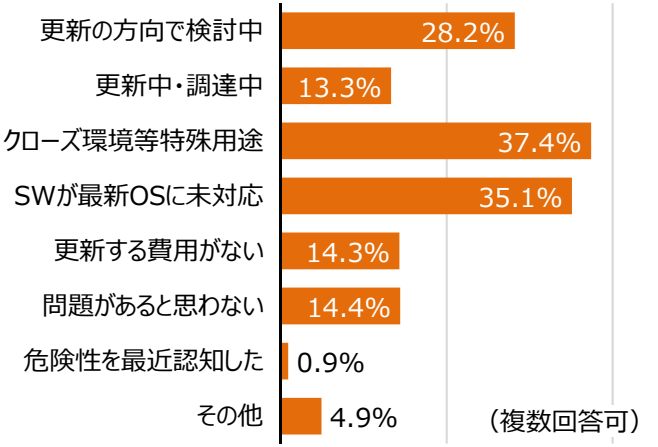
サポート期限切れOSに対する認識

（n=7815：全回答者）



サポート期限切れOSを使用している理由

（n=966：サポート期限切れOSを使用している者）

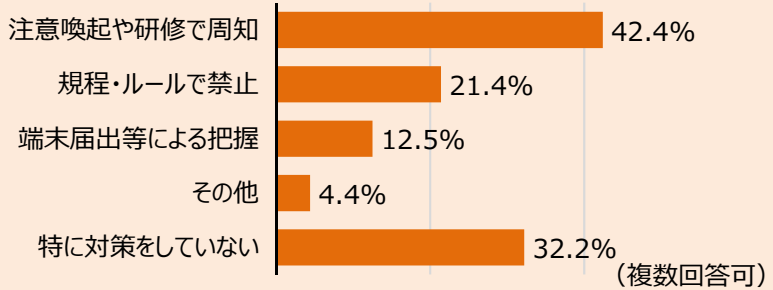


業種別	全回答数	期限切れOS使用 数	期限切れOS使用 割合
全体	7901	978	12 %
建設業	1059	67	6 %
製造業	**1718**	**305**	**18 %**
情報通信業	328	38	12 %
運輸業・郵便業	474	72	15 %
卸売・小売業	1806	214	12 %
金融・保険業	69	7	10 %
不動産業	149	14	9 %
サービス業、その他	2298	261	11 %

規模別	全回答数	期限切れOS使用 数	期限切れOS使用 割合
全体	7901	978	12 %
10～19人	3173	325	10 %
20～29人	1415	166	12 %
30～49人	1284	151	12 %
50～99人	1026	154	15 %
100～199人	566	97	17 %
200～299人	194	36	19 %
300人以上	**243**	**46**	**20 %**

（テレワーク時に従業員所有PCを許可している場合）サポート期限切れ端末を使用しないようにする対策

（n=566：テレワーク時に従業員所有PC端末の利用を許可している者）

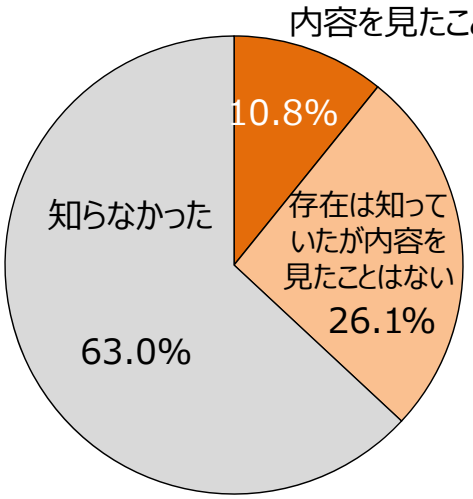


テレワークセキュリティに関する実態調査結果⑤

➢ テレワークセキュリティガイドラインは、企業規模にかかわらず４割弱の企業に認知。

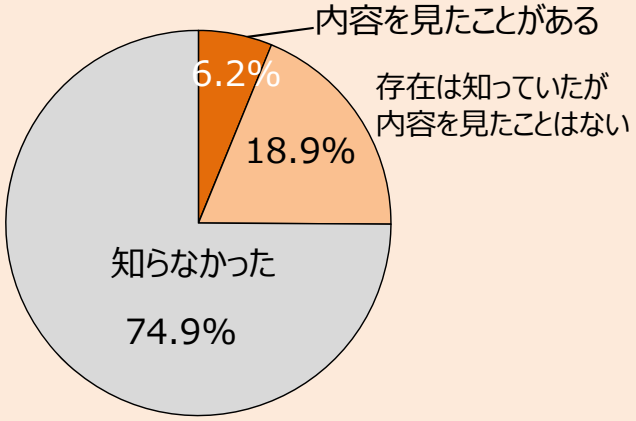
「テレワークセキュリティガイドライン」の認知状況

（n=2616：テレワーク実施企業）

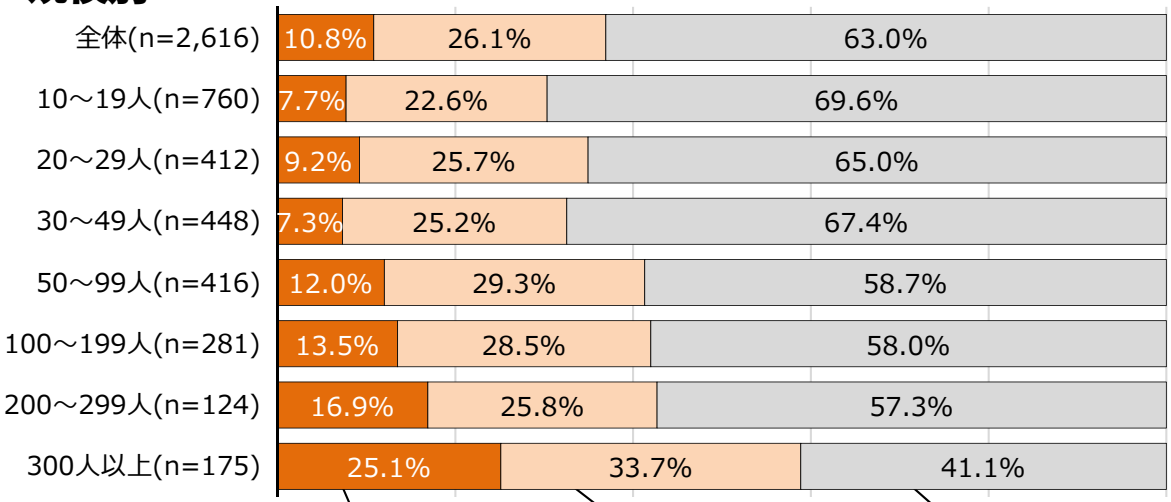


「中小企業等担当者向けテレワークセキュリティの手引き」の認知状況

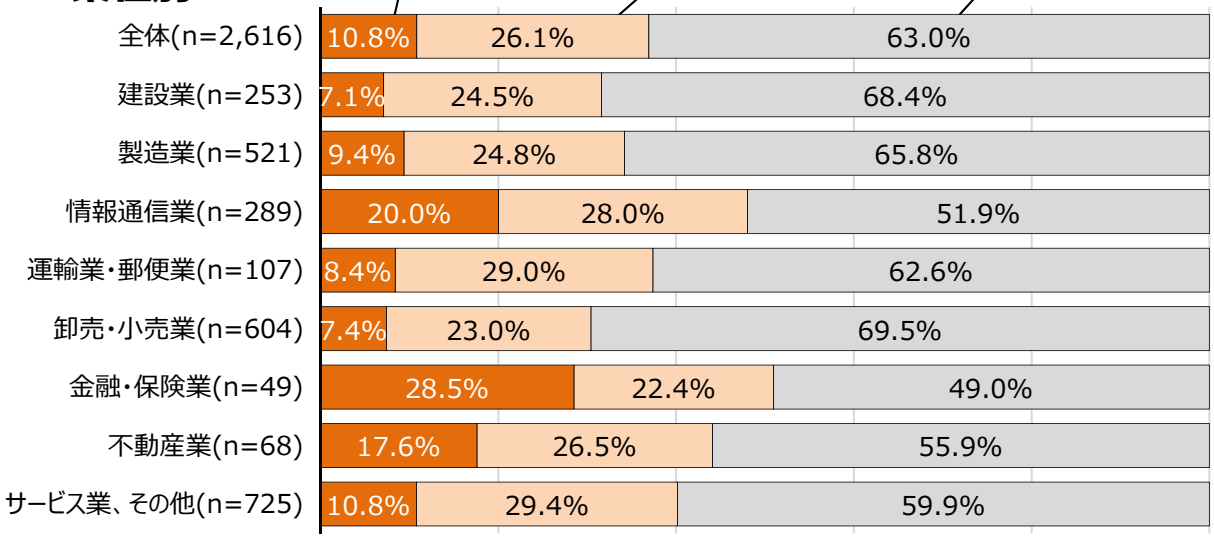
（n=2602：テレワーク実施企業）



規模別

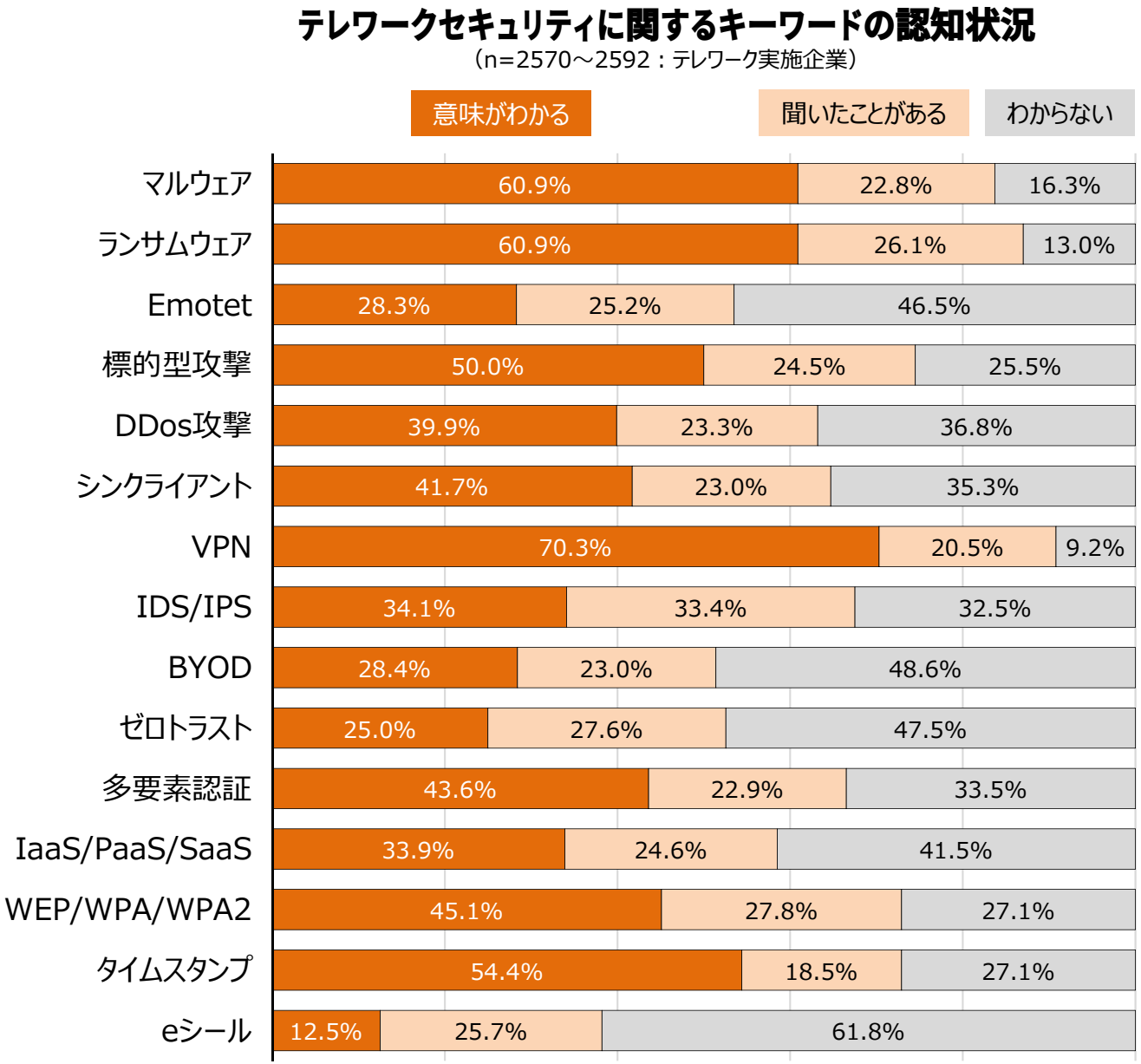


業種別



テレワークセキュリティに関する実態調査結果⑥

➢ セキュリティ関係者にとっては馴染みのあるキーワードでも、一般には通じない場合があることに留意。

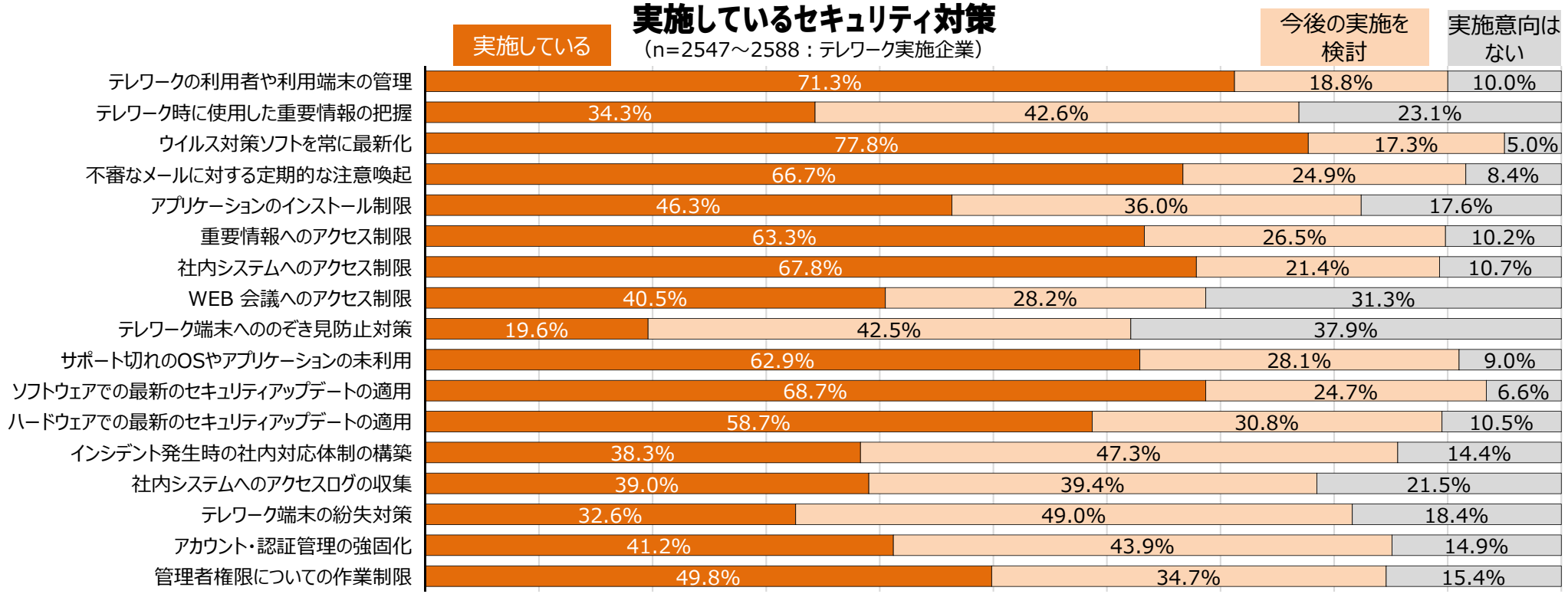


テレワークセキュリティに関する実態調査結果⑦

- テレワーク利用者・利用端末の管理は７割超、ウイルス対策ソフトを常に最新化は8割弱が実施。
- セキュリティ確保・対策継続に当たっての課題として、社内勤務と同等のセキュリティレベルの確保が挙げられている。

実施しているセキュリティ対策

（n=2547～2588：テレワーク実施企業）



セキュリティ確保・対策継続に当たっての課題

（n=2491, 2526：テレワーク実施企業）