テレワークセキュリティに関する２次実態調査

➢ 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。
２次調査）　期間：2020.12.16-2021.1.8　　回答数：5,037（うちテレワーク実施企業1,996）
調査手法：調査票郵送・Web回答　対象地域：全国　対象数：各30,000(従業員等が10名以上)（1次調査回答者(1,569)＋1次調査非対象者(28,431)）

スクリーニング調査　※スクリーニング設問は4,385社が回答（1次調査回答者はスクリーニング設問省略）
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　職場・テレワークで利用する会社所有PC端末のOSの種類
S-5　サポート期限切れOSに対する認識
S-6　サポート期限切れOSを使用している理由
S-7　サポート期限切れOSを使用している割合

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1,996社が回答
1-1　テレワークの導入時期
1-2　新型コロナ収束後のテレワークの活用予定
1-3　新型コロナ収束後にテレワークを活用しない理由
1-4　テレワークをやめた理由
1-5　テレワークの利用割合
1-6　テレワークの形態
1-7　サテライトオフィスの利用費用の会社負担有無
1-8　サテライトオフィスの利用費用を会社が負担する理由

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　テレワークを実施する上での検討・実施事項（人的・組織的対策）
2-4　テレワーク時のクラウドサービスの利用状況
2-5　テレワーク時のセキュリティ対策を検討する際の主な情報収集先
2-6　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
3-1　テレワーク利用を許可している端末の形態
3-2　コロナ対応のためテレワーク利用を許可した端末の形態
3-3　テレワーク利用する会社支給PC端末のOSの種類
3-8　サポート期限が切れた端末を使用しないようにする対策

４　情報セキュリティ対策　※3-4～3-7はS-4～S-7と同設問
4-1　情報セキュリティ対策に関する取組の実施状況
4-2　情報セキュリティ対策に関する取組が不十分と感じた部分
4-3　情報セキュリティ対策に関する取組が未実施の理由
4-4　情報セキュリティ対策に関する組織体制
4-5　情報セキュリティ対策に関する従事者の水準

５　総務省が作成するガイドライン
5-1　「テレワークセキュリティガイドライン」の認知度
5-2　「テレワークセキュリティガイドライン」を見たときの所感
5-3　「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
5-4　「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
5-5　「テレワークセキュリティガイドライン」の改定頻度
5-6　「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」の認知度
5-7　「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」で参考になった内容
5-8　「設定解説資料」の認知度
5-9　テレワークセキュリティに関するキーワードの認知度

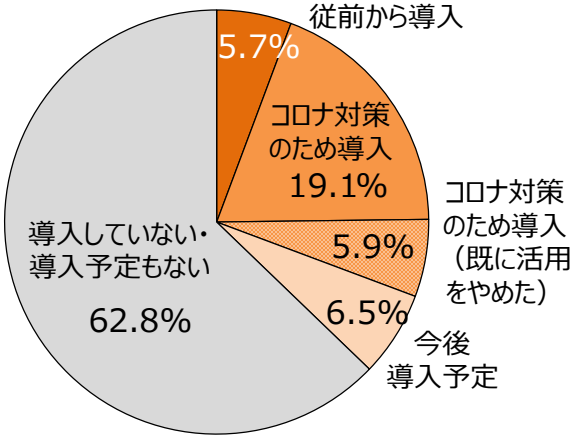
６　テレワーク導入のメリット・課題
6-1　テレワークの導入目的
6-2　テレワークの導入目的に対しての効果
6-3　テレワークの導入により働き方で大きく変革した点
6-4　テレワークの導入に当たり課題となった点
6-5　テレワークの導入後も残っている課題
6-6　セキュリティ確保への具体的な課題
6-7　文書の電子化や押印廃止の実施状況
6-8　文書の電子化や押印廃止について検討しない理由

テレワークセキュリティに関する２次実態調査結果①

- 新型コロナ対応のため、中小企業を含めてテレワークが急速に拡大。（緊急事態宣言＝2020年4月）
- 緊急事態宣言解除後も、規模は縮小しつつも引き続きテレワークを実施している企業が多い。

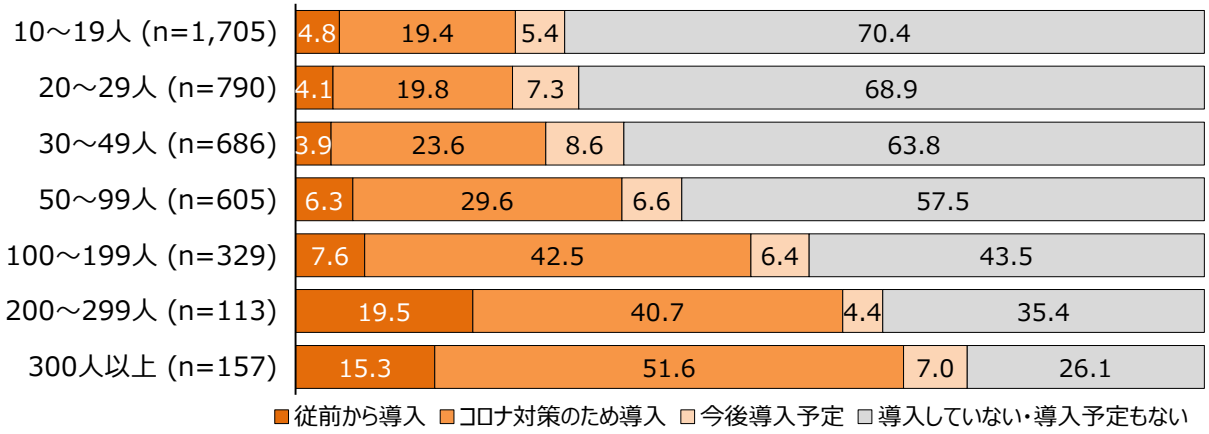
テレワークの導入状況

（n=4,385：全回答者（１次調査対象者を除く））



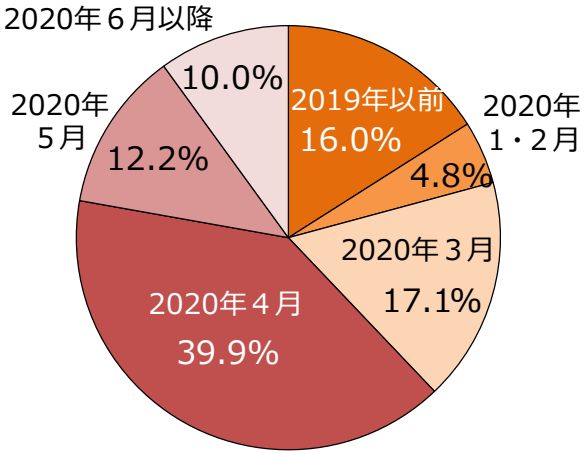
テレワークの導入状況（従業員規模別）

（n=4,385：全回答者（１次調査対象者を除く））



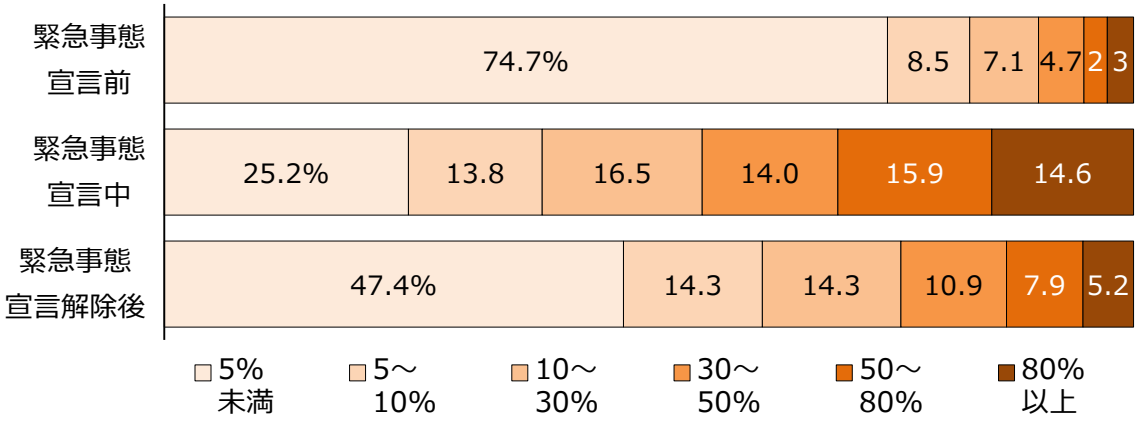
テレワークの導入時期

（n=1,996：テレワーク実施企業）



（各企業における）テレワークの導入割合

（n=1,996：テレワーク実施企業）

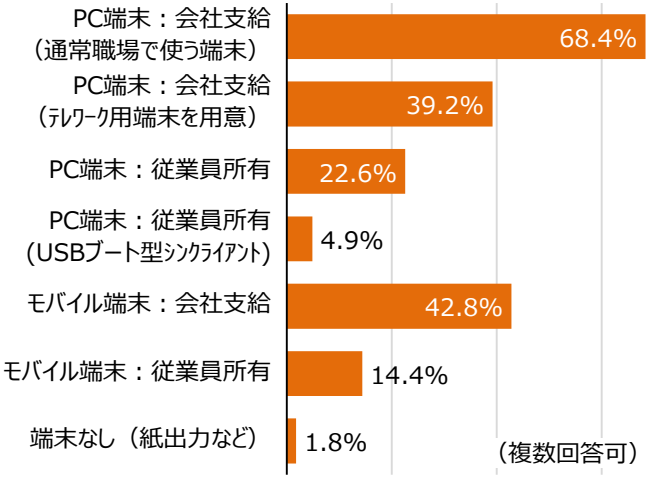


テレワークセキュリティに関する２次実態調査結果②

- 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、「セキュリティの確保」が最大の課題となっている。

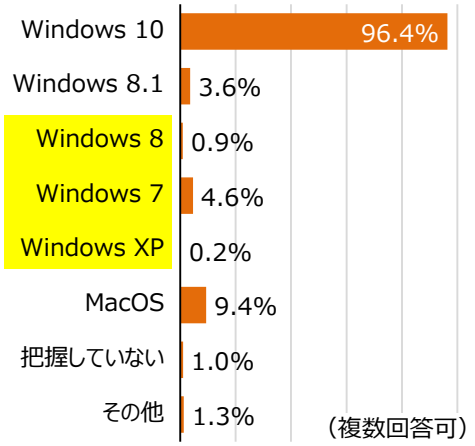
テレワーク利用を許可している端末

（n=1,996：テレワーク実施企業）



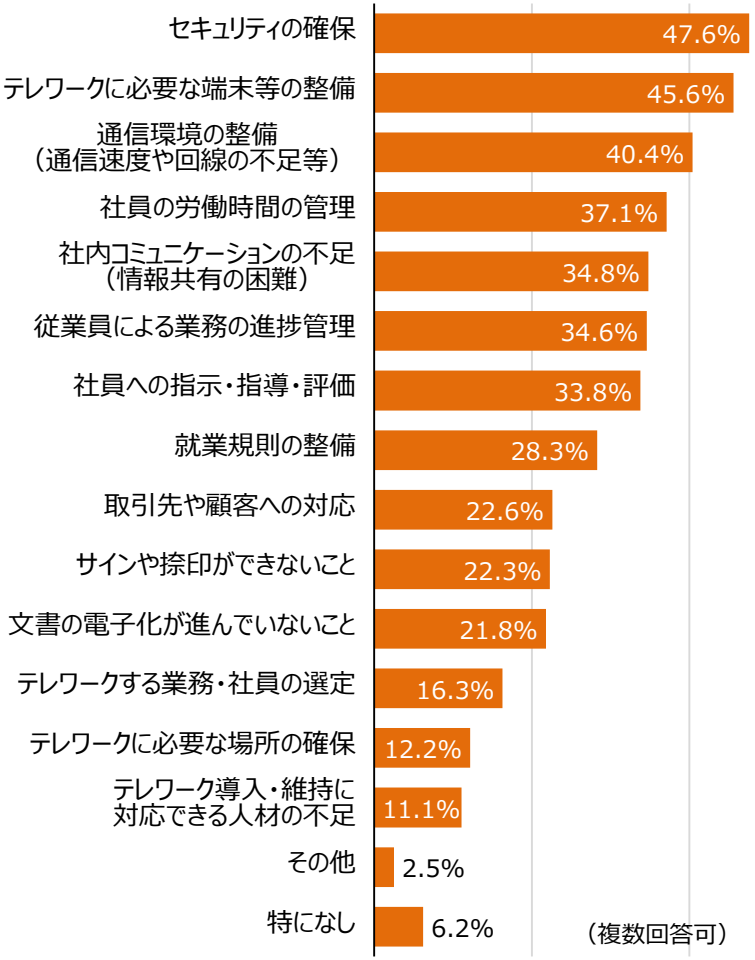
会社支給PC端末のOS

（n=1,735：会社支給PC端末を利用）



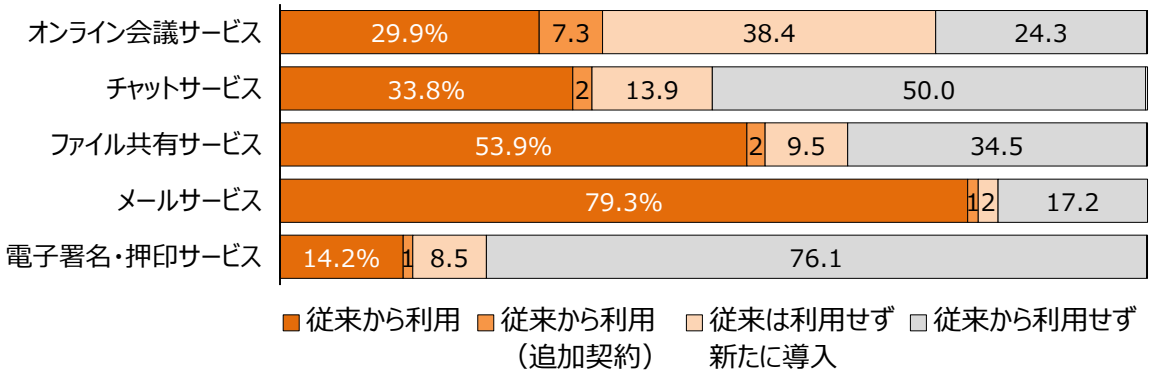
テレワークの導入に当たり課題となった点

（n=1,996：テレワーク実施企業）



クラウドサービスの利用状況

（n=1,996：テレワーク実施企業）

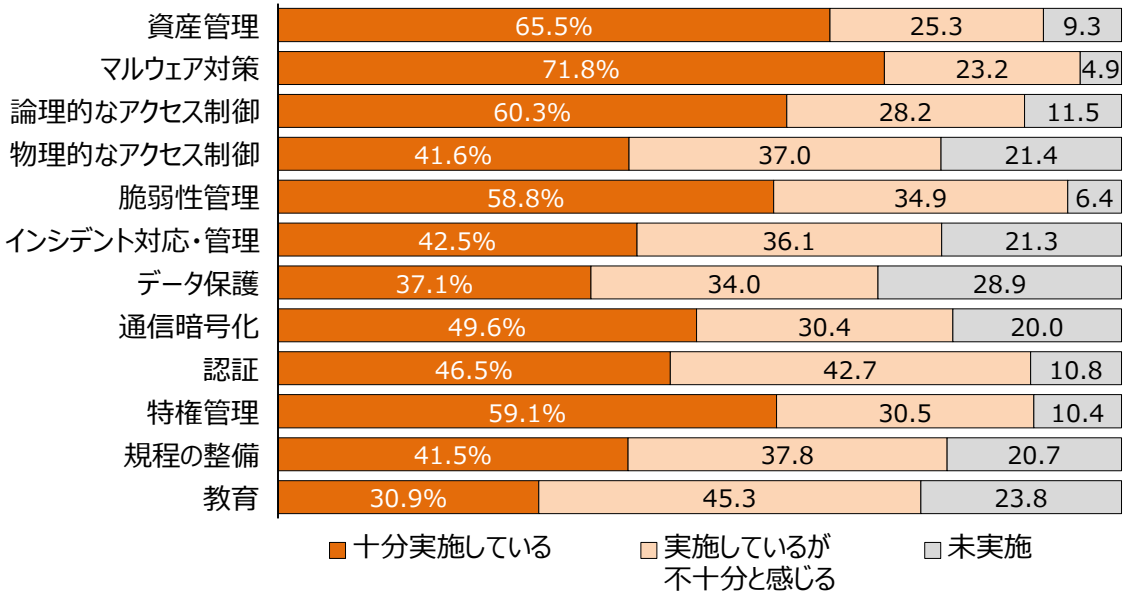


テレワークセキュリティに関する２次実態調査結果③

- 「マルウェア対策」は７割が十分実施していると回答。一方で「教育」は７割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。

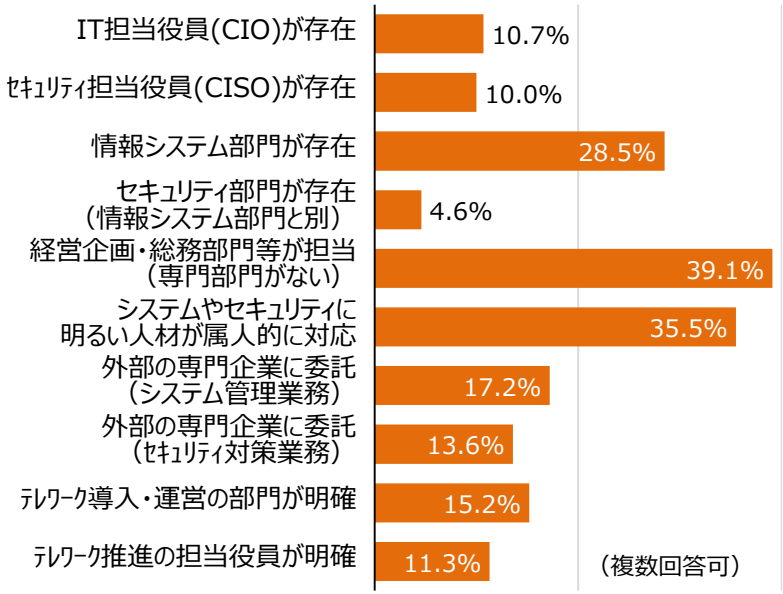
情報セキュリティ対策に関する取組の実施状況

（n=1,996：テレワーク実施企業）



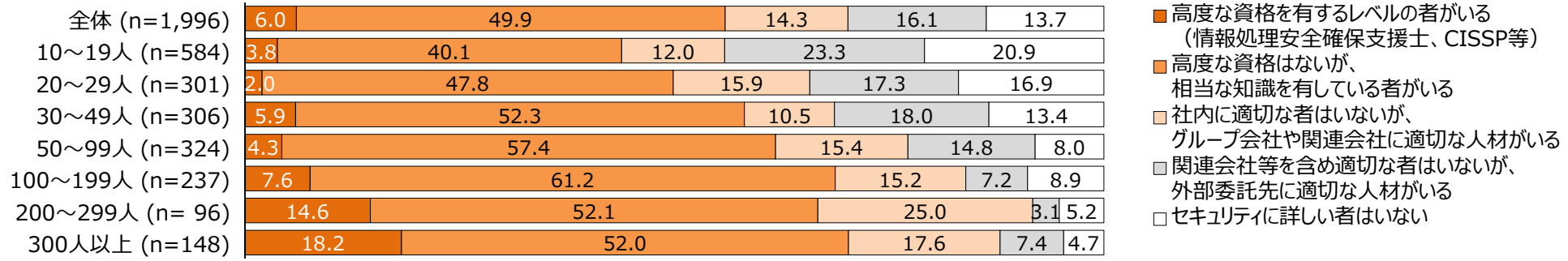
情報セキュリティ対策に関する組織体制

（n=1,996：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=1,996：テレワーク実施企業）

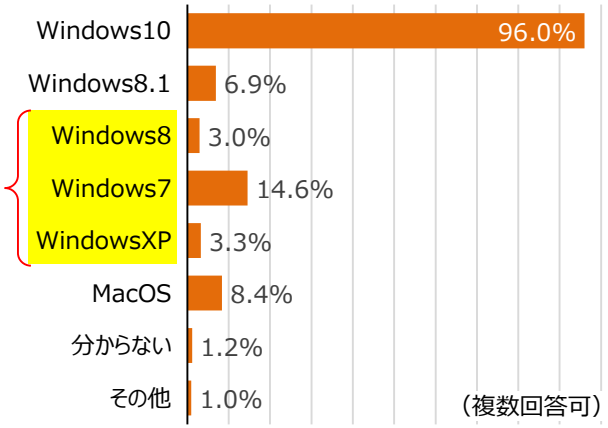


テレワークセキュリティに関する２次実態調査結果④

- 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。

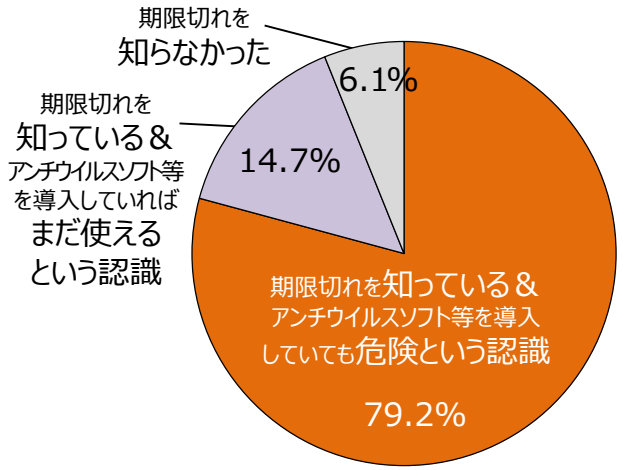
職場・テレワークに関わらず 会社所有PC端末のOSの種類

（n=5,037：全回答者）



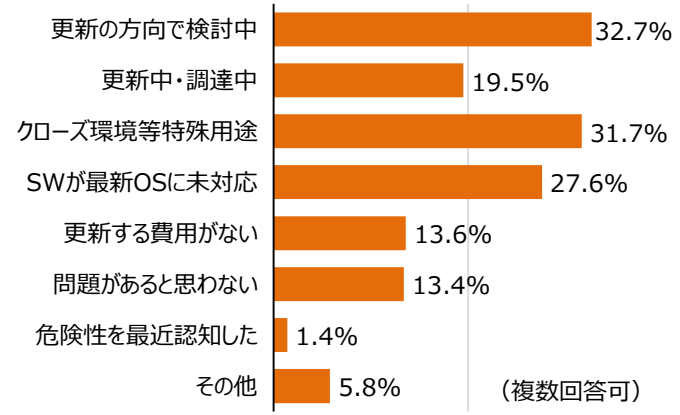
サポート期限切れOSに対する認識

（n=5,037：全回答者）



サポート期限切れOSを使用している理由

（n=851：サポート期限切れOSを使用している者）



(注)自由回答により、ESUを使用している企業も見受けられた
（ESU：Windows 7 拡張セキュリティ更新プログラム（最大で2023年1月まで））

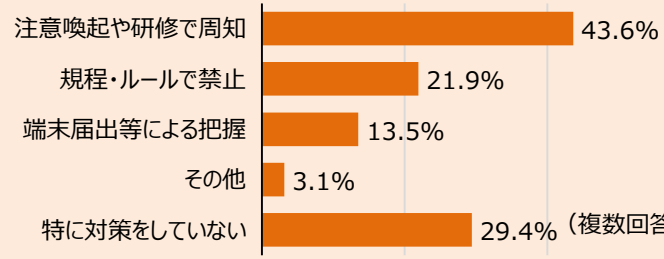
業種別	全回答数	期限切れOS使用 数	期限切れOS使用 割合
全体	5,037	851	17 %
建設業	585	59	10 %
製造業	1,023	237	23 %
情報通信業	243	34	14 %
運輸業・郵便業	328	58	18 %
卸売・小売業	1,145	199	17 %
金融・保険業	52	7	13 %
不動産業	105	15	14 %
サービス業、その他	1,556	242	16 %

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	5,037	851	17 %
10～19人	1,877	268	14 %
20～29人	903	142	16 %
30～49人	803	130	16 %
50～99人	712	129	18 %
100～199人	401	93	23 %
200～299人	141	31	22 %
300人以上	200	58	29 %

（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=482：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）

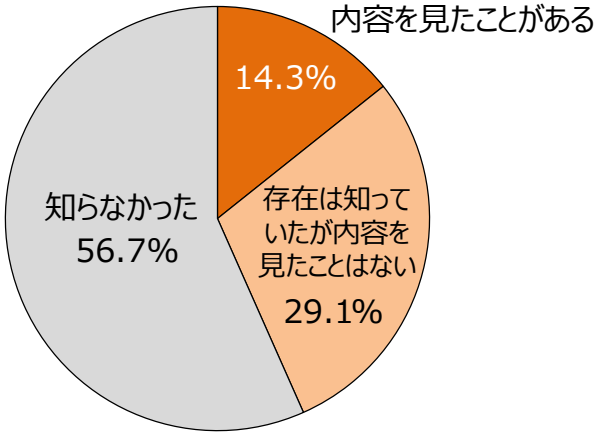


テレワークセキュリティに関する２次実態調査結果⑤

➢ 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割程度の企業に認知。

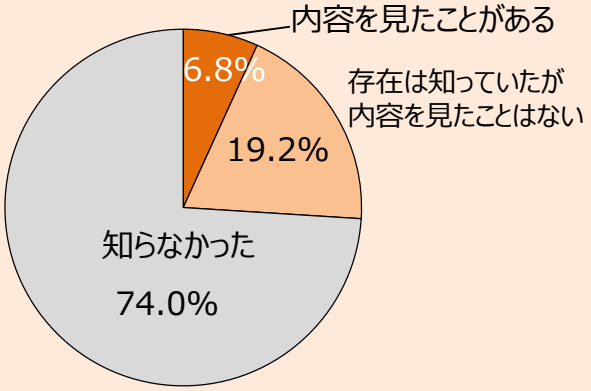
「テレワークセキュリティガイドライン」の認知状況

（n=1,996：テレワーク実施企業）

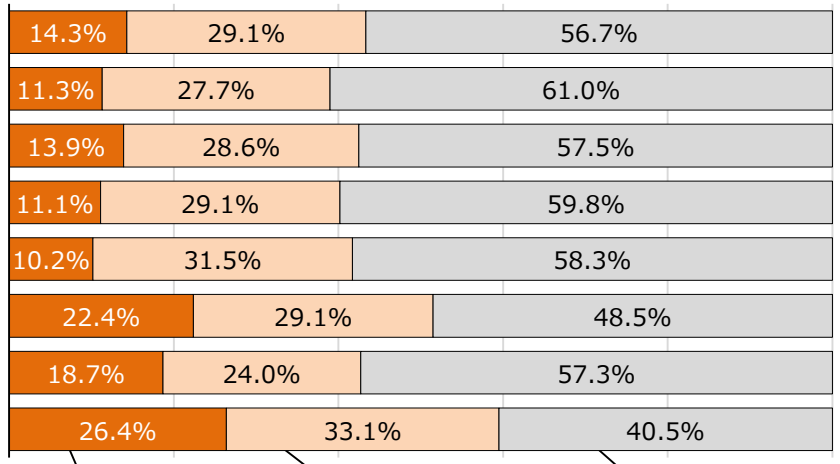


「中小企業等担当者向けテレワークセキュリティの手引き」の認知状況

（n=1,996：テレワーク実施企業）

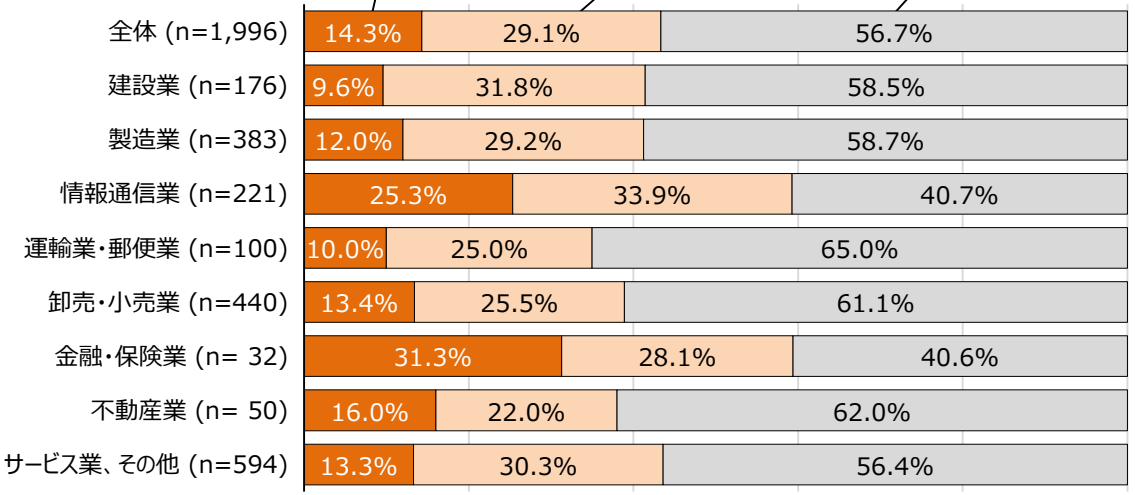


規模別



内容を見たことがある　存在は知っていたが内容を見たことはない　知らなかった

業種別



テレワークセキュリティに関する２次実態調査結果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。