テレワークセキュリティに関する実態調査（R3年度）

参考資料2

➢ 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

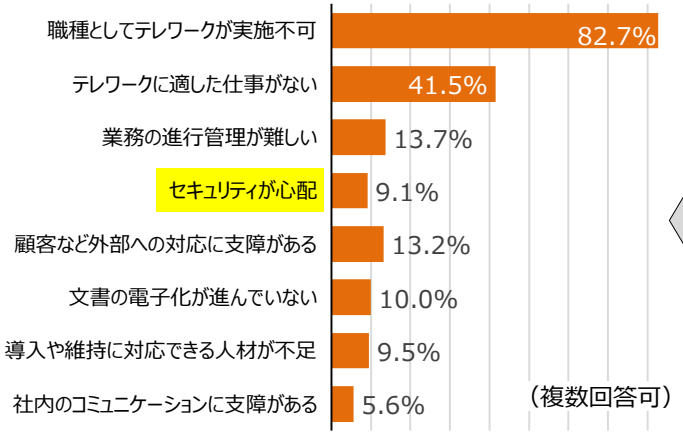
7　総務省が作成するガイドライン
7-1 「テレワークセキュリティガイドライン」の認知度
7-2 「テレワークセキュリティガイドライン」で参考になった内容
7-3 「テレワークセキュリティガイドライン」で記載を充実させた方がよい内容
7-4 「テレワークセキュリティの手引き」の認知度
7-5 「テレワークセキュリティの手引き」で参考になった内容
7-6 「テレワークセキュリティの手引き」で記載を充実させた方がよい内容
7-7 「設定解説資料」の認知度
7-8 テレワークセキュリティに関するキーワードの認知度

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として、業務都合を除くとセキュリティに関する懸念がトップ。

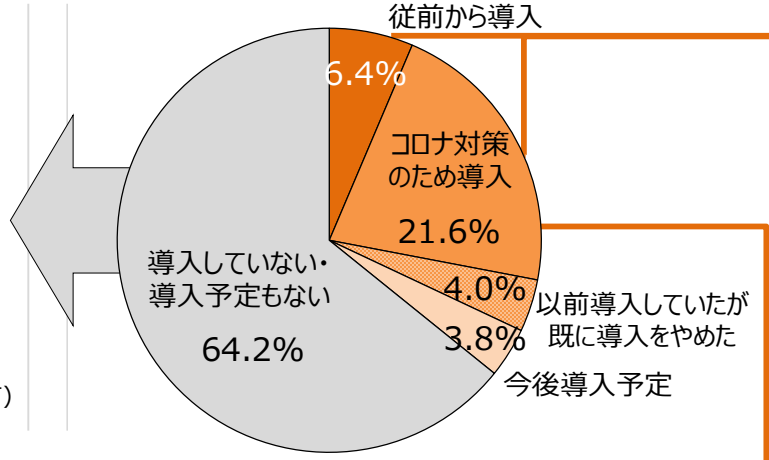
テレワークを導入しない理由

（n=5297：テレワーク未導入企業）



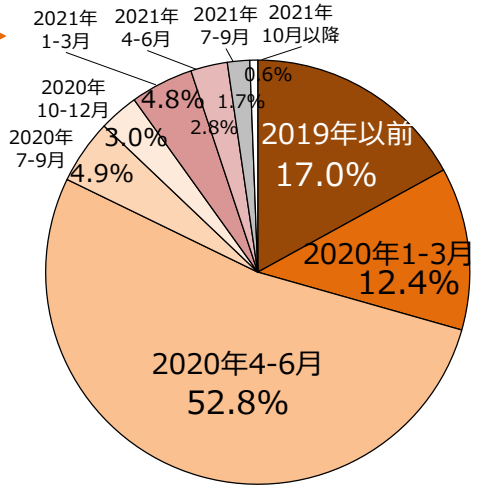
テレワークの導入状況

（n=8264：全回答者）



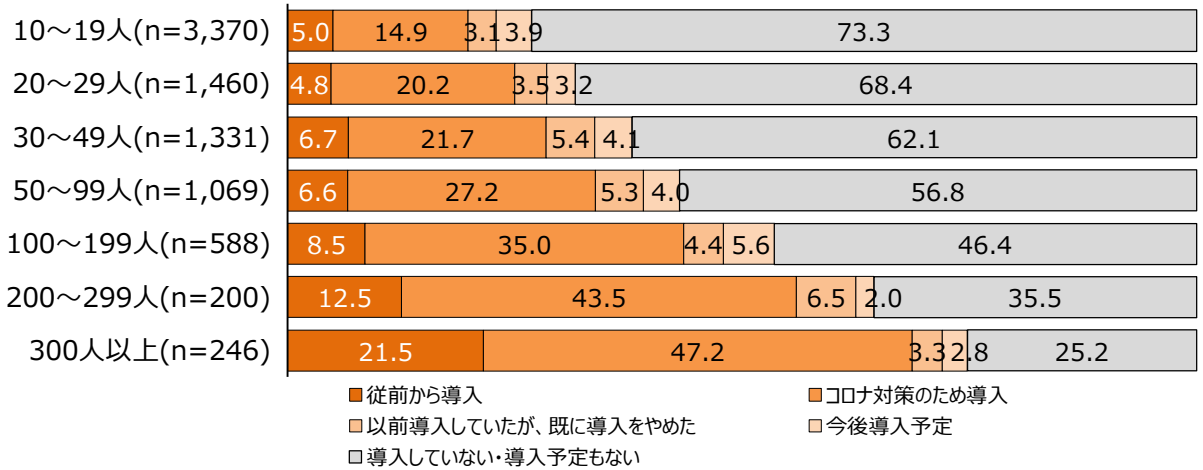
テレワークの導入時期

（n=2630：テレワーク実施企業）



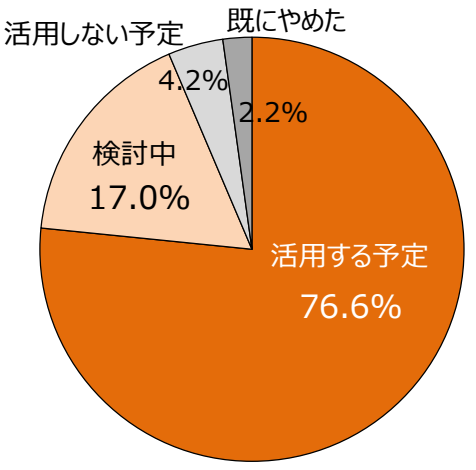
テレワークの導入状況（従業員規模別）

（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）

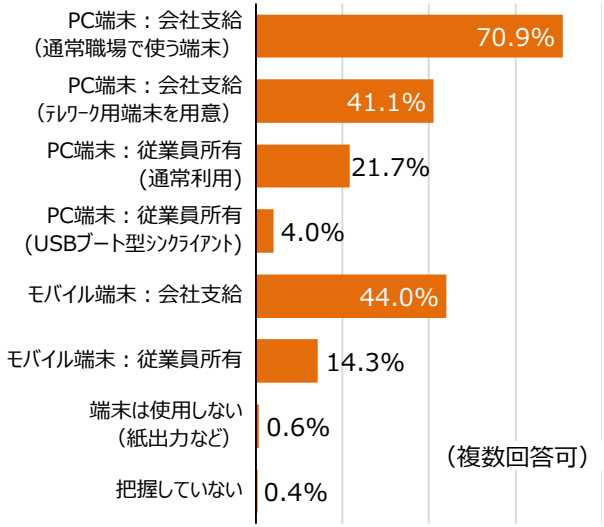


テレワークセキュリティに関する実態調査結果②

- 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。

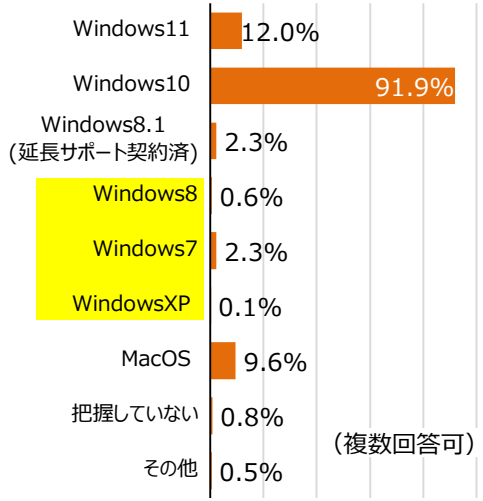
テレワーク利用を許可している端末

（n=2634：テレワーク実施企業）



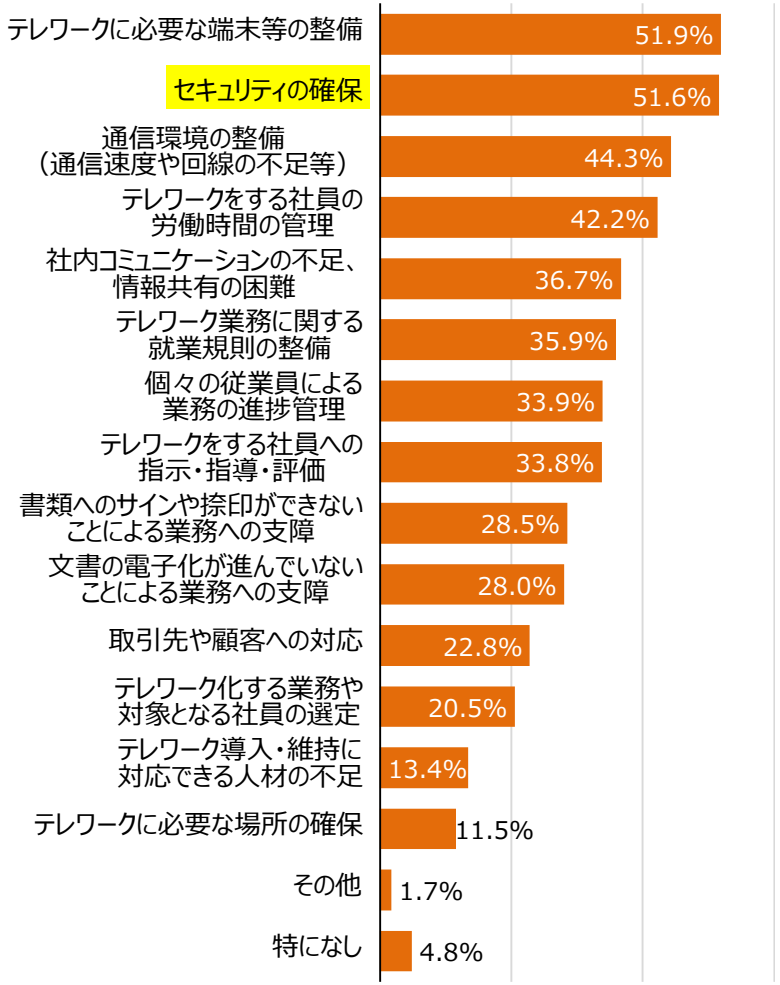
会社支給PC端末のOS

（n=2352：会社支給PC端末を利用）



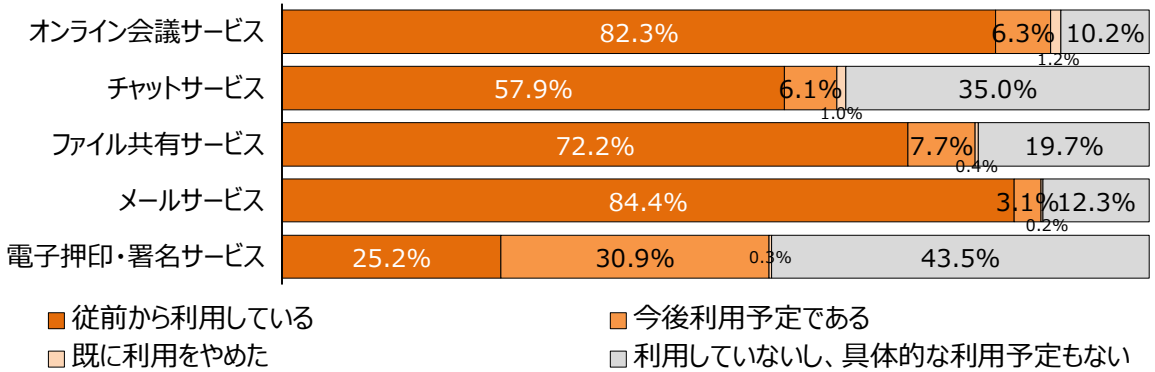
テレワークの導入に当たり課題となった点

（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）

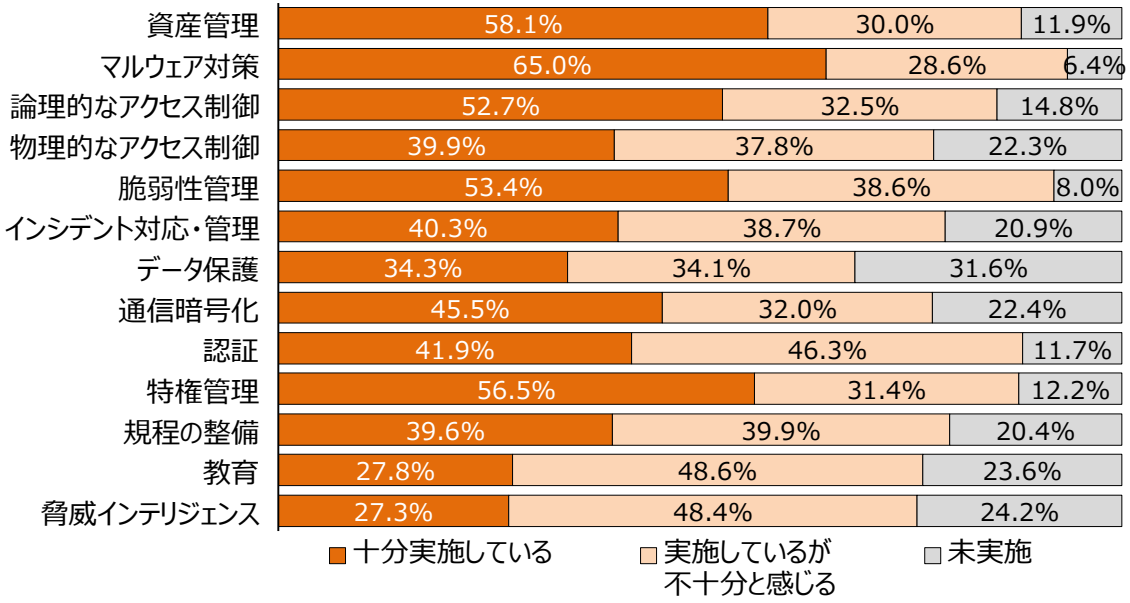


テレワークセキュリティに関する実態調査結果③

- 「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。

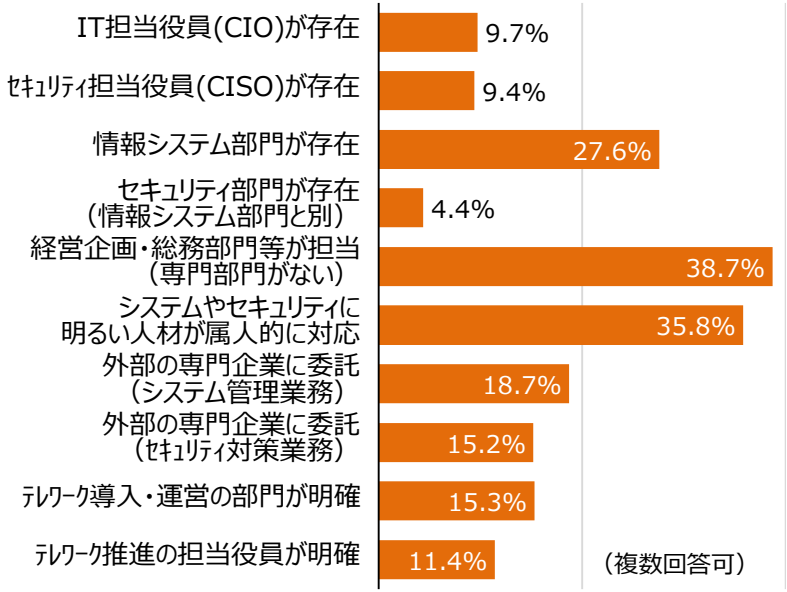
情報セキュリティ対策に関する取組の実施状況

（n=2590～2609：テレワーク実施企業）



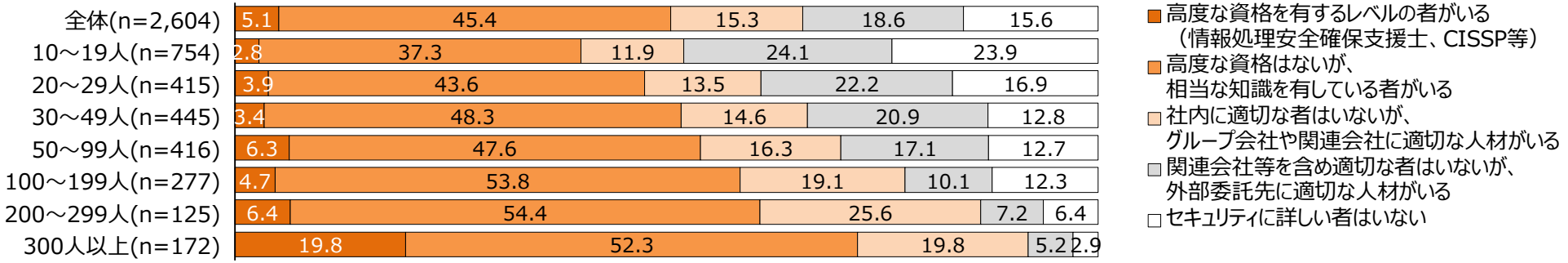
情報セキュリティ対策に関する組織体制

（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）

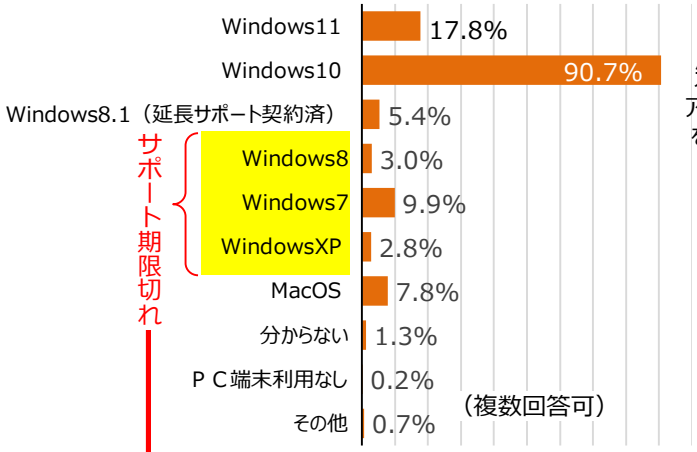


テレワークセキュリティに関する実態調査結果④

- 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。

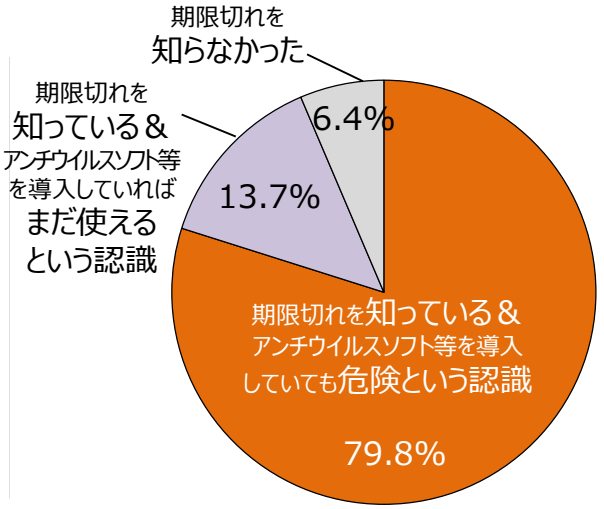
職場・テレワークに関わらず 会社所有PC端末のOSの種類

（n=7901：全回答者）



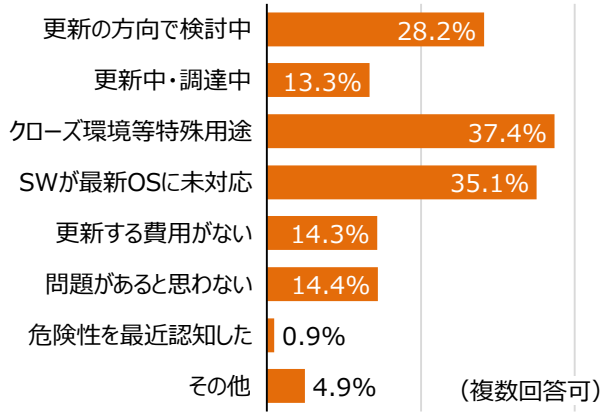
サポート期限切れOSに対する認識

（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）



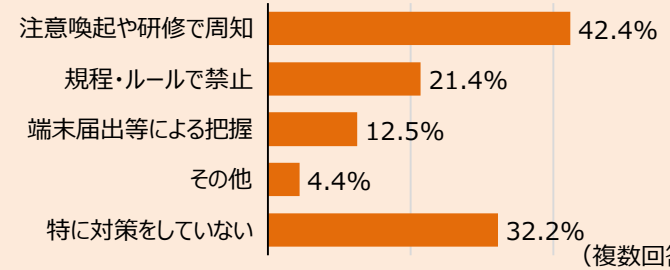
業種別	全回答数	期限切れOS使用 数	期限切れOS使用 割合
全体	7901	978	12 %
建設業	1059	67	6 %
製造業	**1718**	**305**	**18 %**
情報通信業	328	38	12 %
運輸業・郵便業	474	72	15 %
卸売・小売業	1806	214	12 %
金融・保険業	69	7	10 %
不動産業	149	14	9 %
サービス業、その他	2298	261	11 %

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）

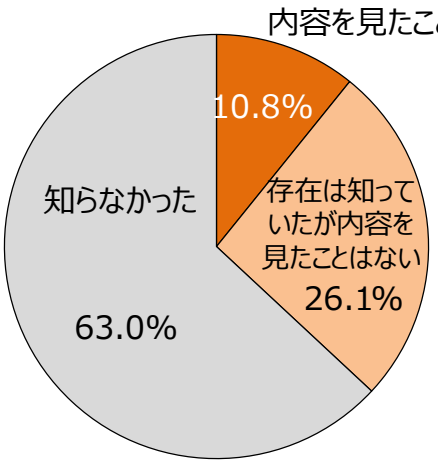


テレワークセキュリティに関する実態調査結果⑤

➢ 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。

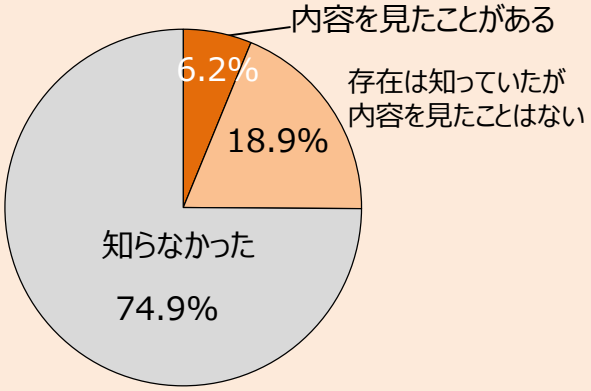
「テレワークセキュリティガイドライン」の認知状況

（n=2616：テレワーク実施企業）

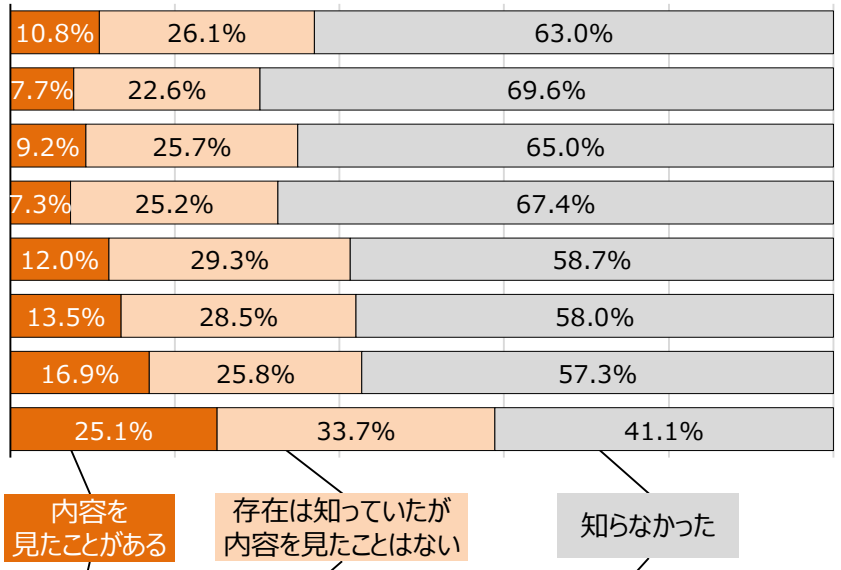


「中小企業等担当者向けテレワークセキュリティの手引き」の認知状況

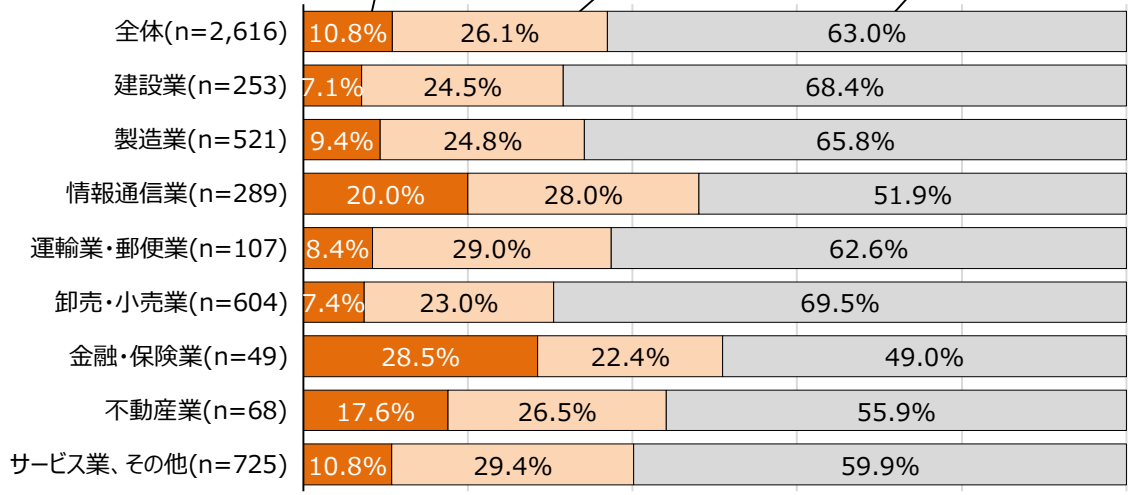
（n=2602：テレワーク実施企業）



規模別

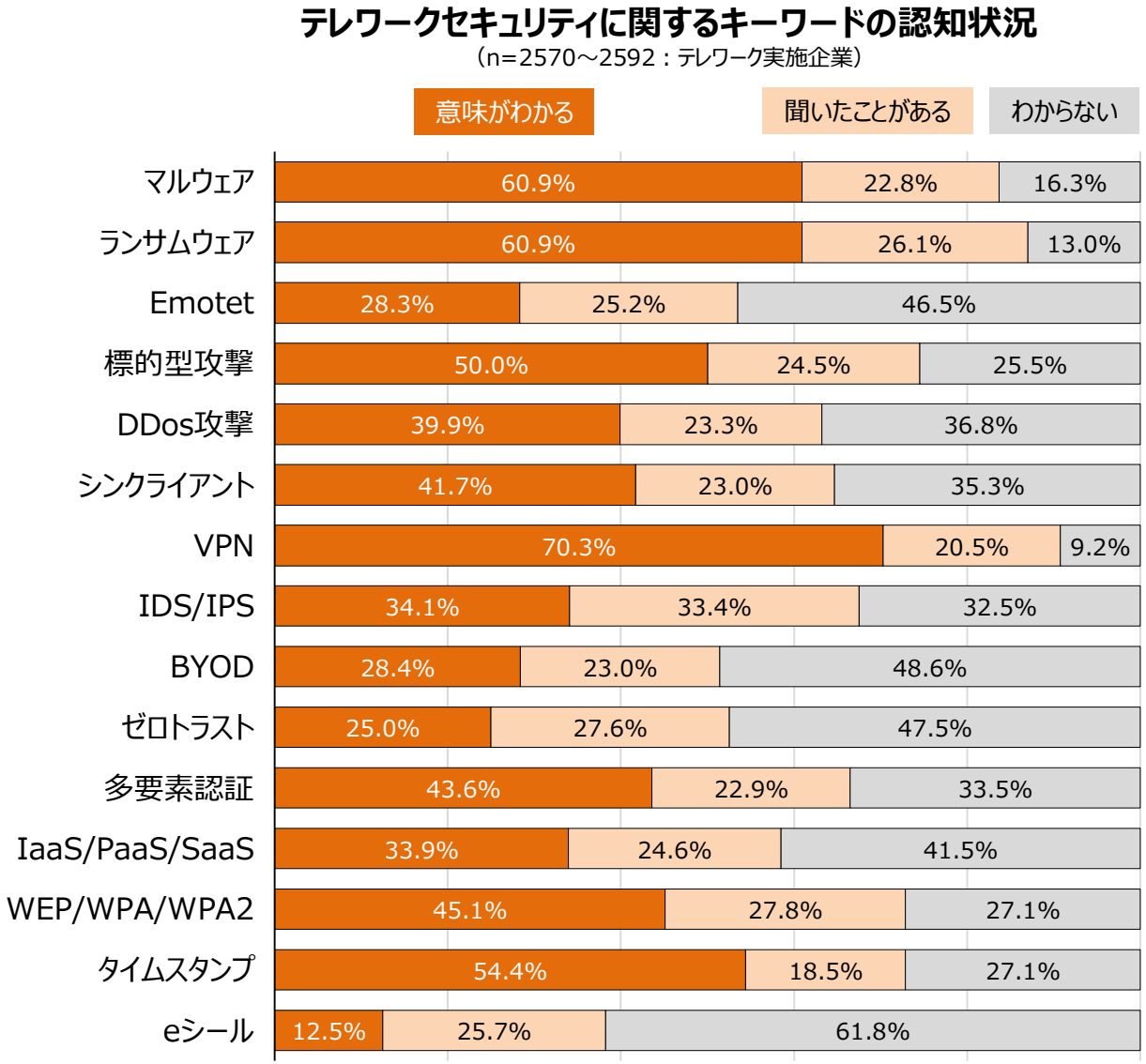


業種別



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。

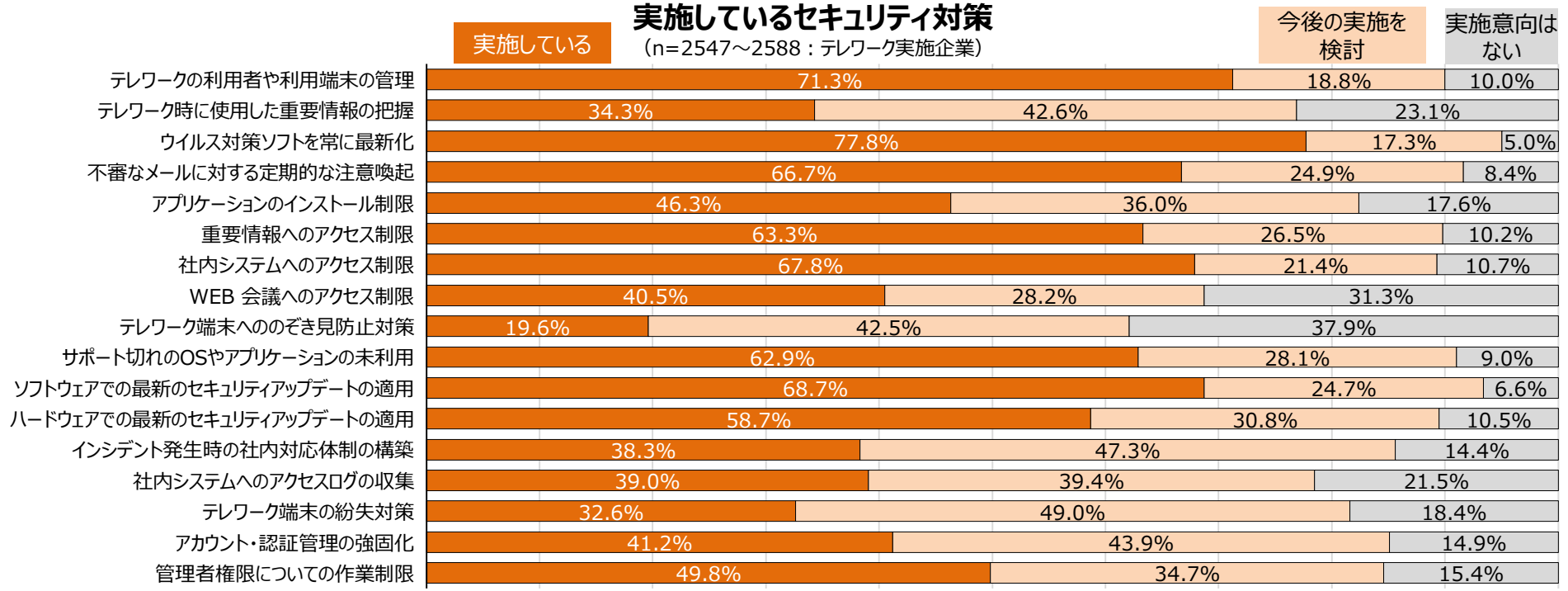


テレワークセキュリティに関する実態調査結果⑦

- 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。

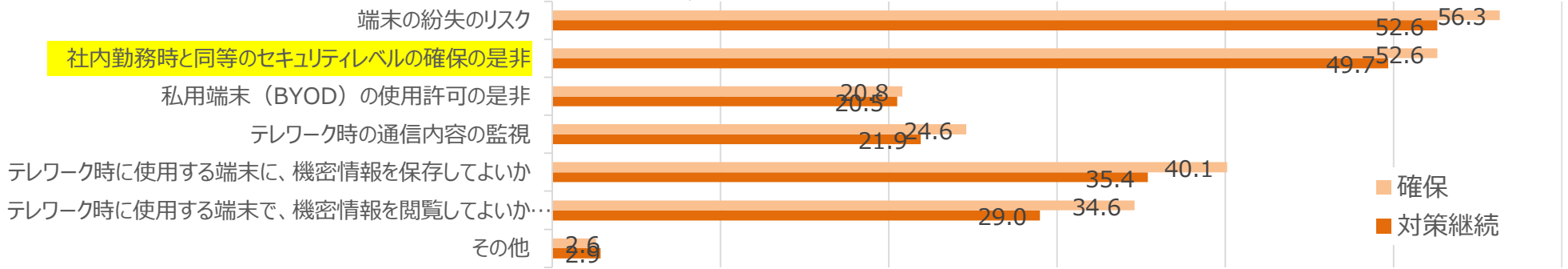
実施しているセキュリティ対策

（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）



参考：昨年度の結果

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

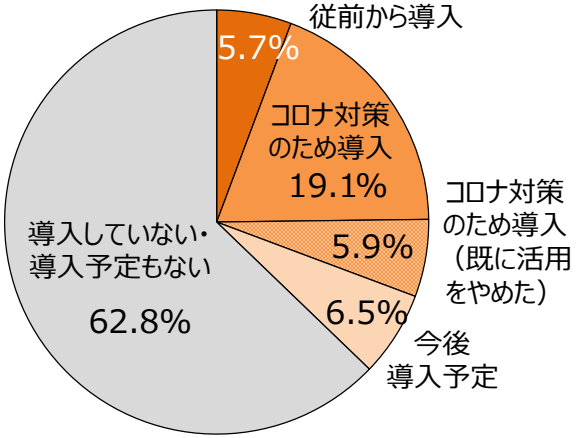
６　テレワーク導入のメリット・課題
6-1　テレワークの導入目的
6-2　テレワークの導入目的に対しての効果
6-3　テレワークの導入により働き方で大きく変革した点
6-4　テレワークの導入に当たり課題となった点
6-5　テレワークの導入後も残っている課題
6-6　セキュリティ確保への具体的な課題
6-7　文書の電子化や押印廃止の実施状況
6-8　文書の電子化や押印廃止について検討しない理由

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。

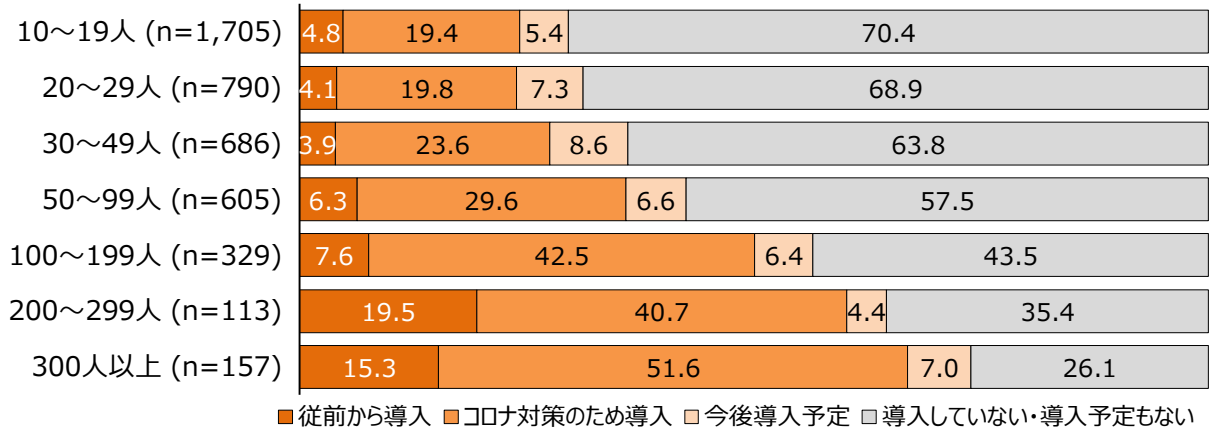
テレワークの導入状況

（n=4,385：全回答者（１次調査対象者を除く））



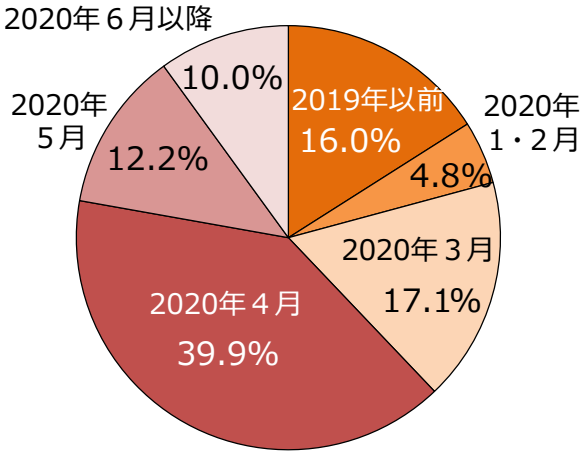
テレワークの導入状況（従業員規模別）

（n=4,385：全回答者（１次調査対象者を除く））



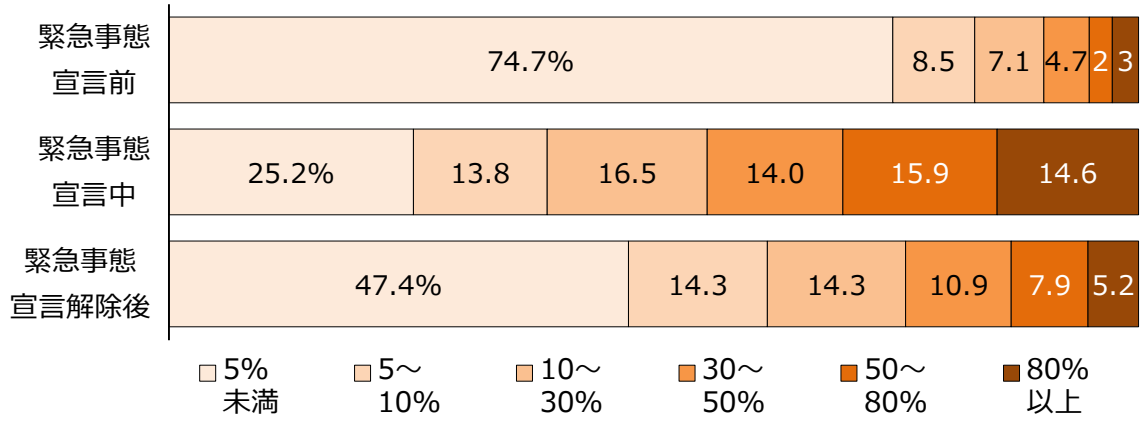
テレワークの導入時期

（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）

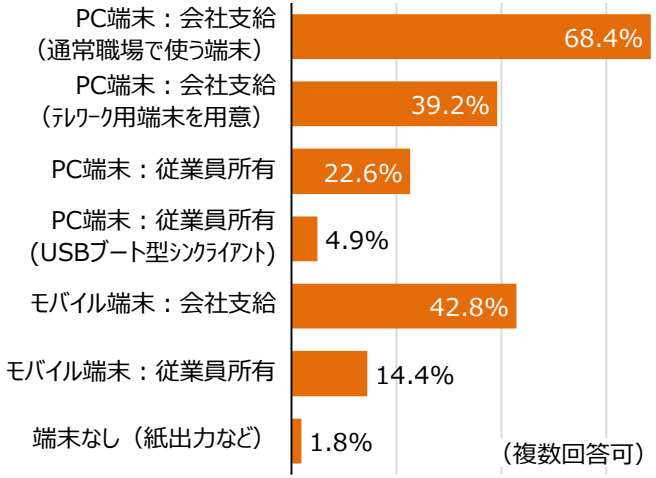


テレワークセキュリティに関する２次実態調査結果②

- 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。

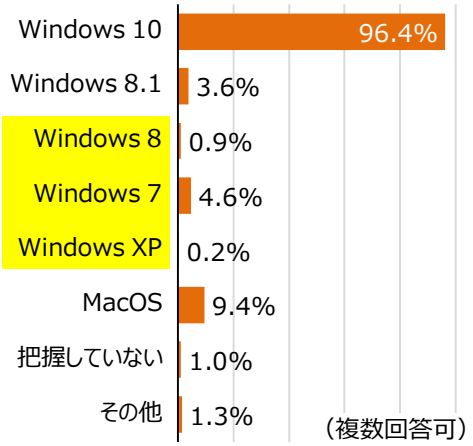
テレワーク利用を許可している端末

（n=1,996：テレワーク実施企業）



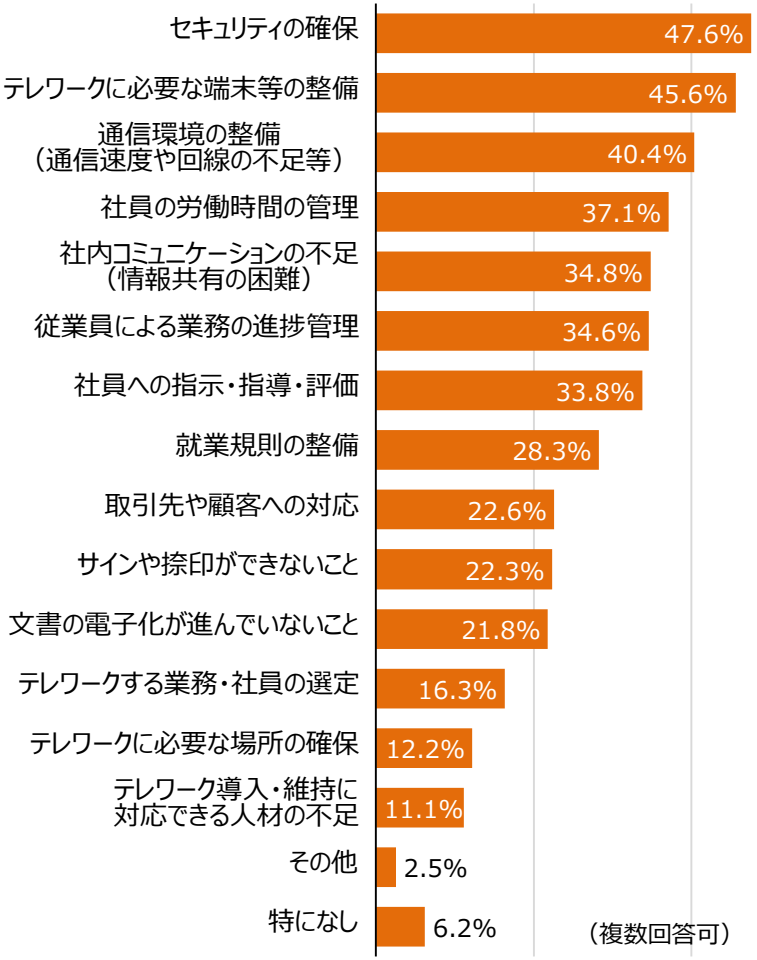
会社支給PC端末のOS

（n=1,735：会社支給PC端末を利用）



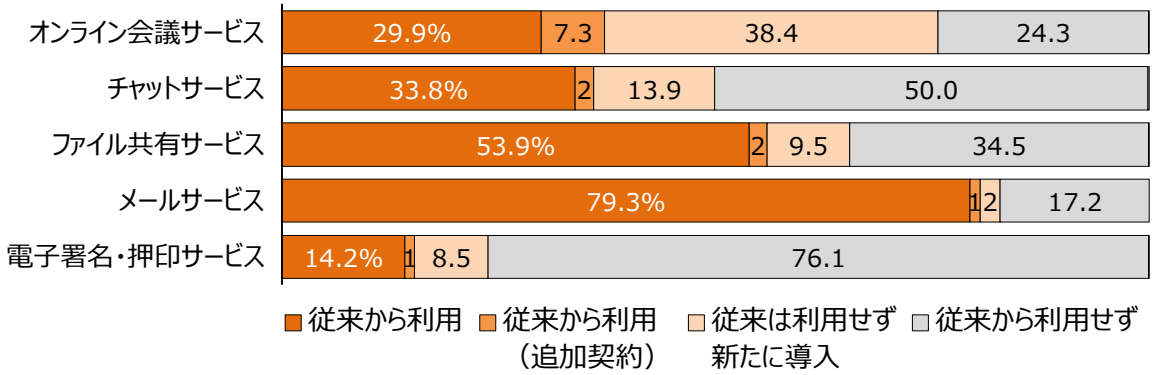
テレワークの導入に当たり課題となった点

（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）

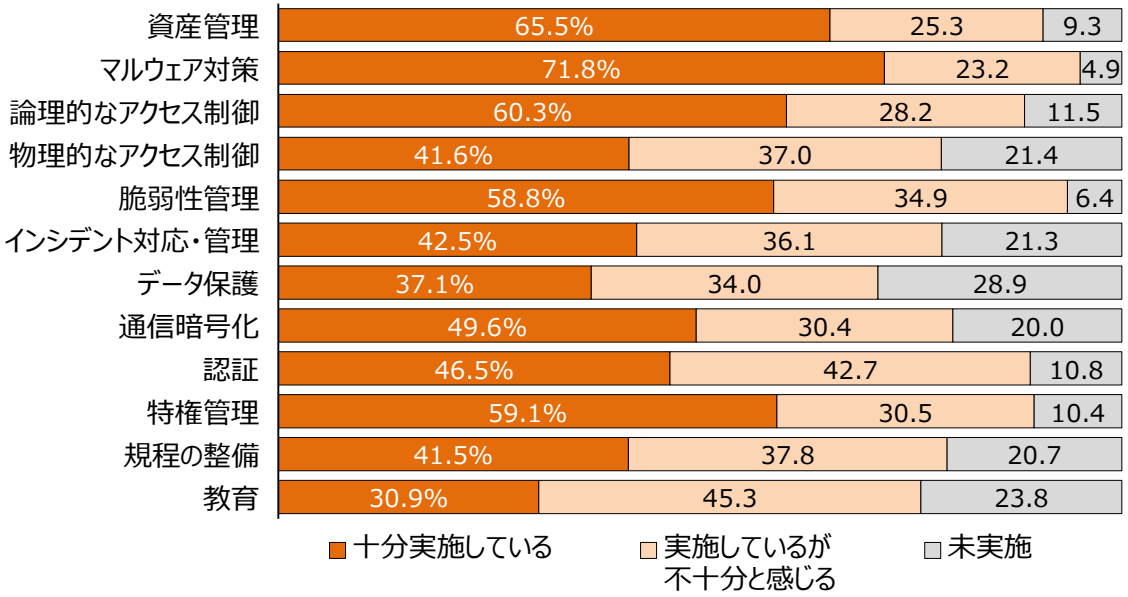


テレワークセキュリティに関する２次実態調査結果③

- 「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。

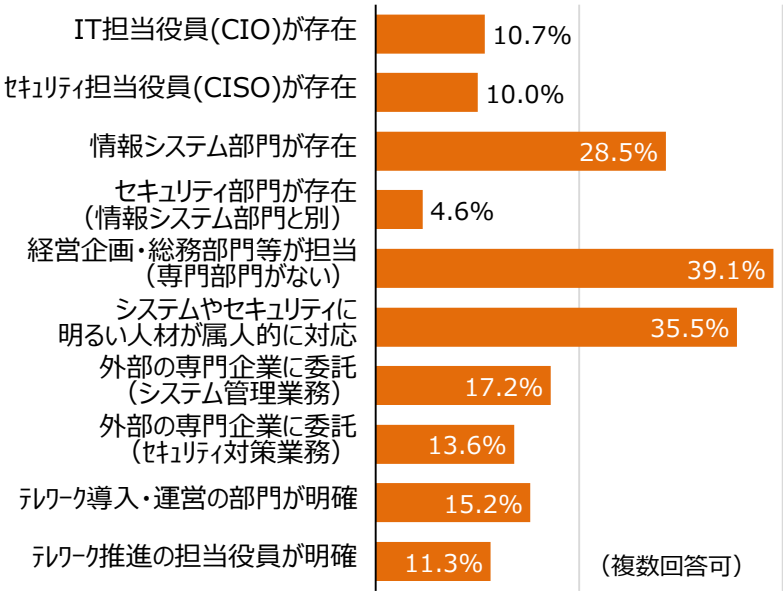
情報セキュリティ対策に関する取組の実施状況

（n=1,996：テレワーク実施企業）



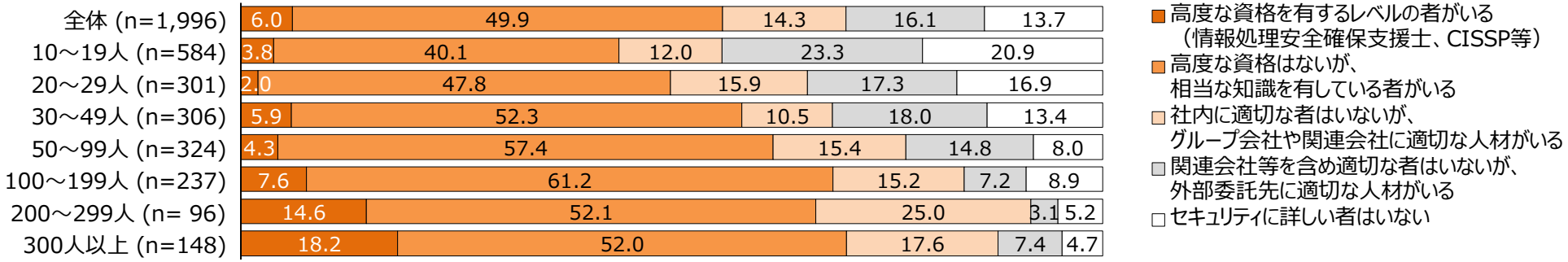
情報セキュリティ対策に関する組織体制

（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）

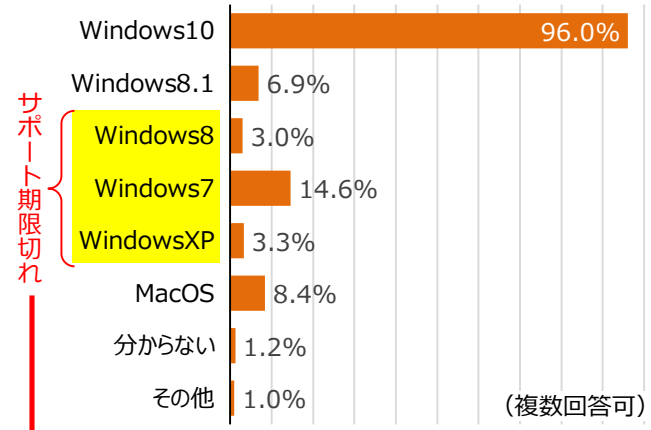


テレワークセキュリティに関する２次実態調査結果④

- 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。

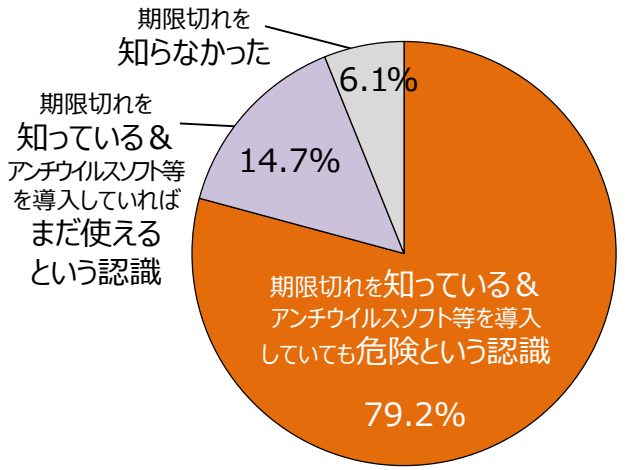
職場・テレワークに関わらず 会社所有PC端末のOSの種類

（n=5,037：全回答者）



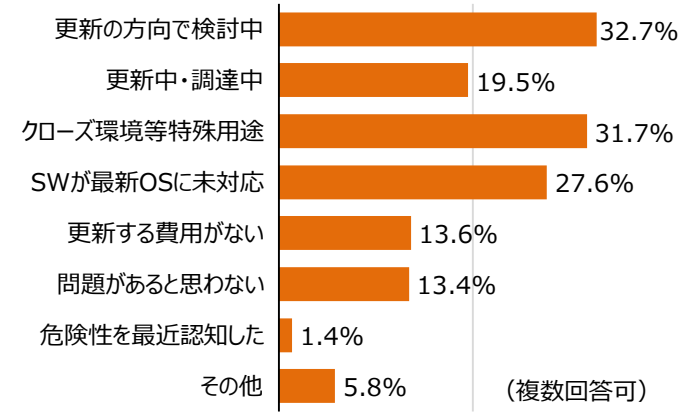
サポート期限切れOSに対する認識

（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）



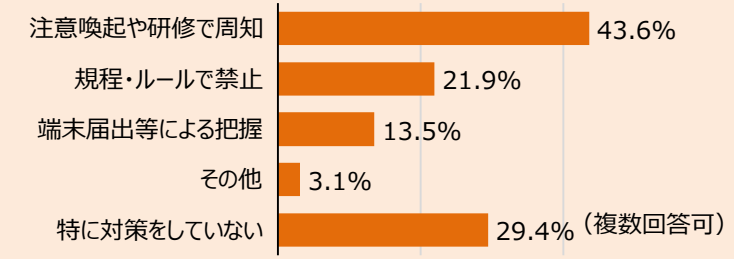
(注)自由回答により、ESUを使用している企業も見受けられた
（ESU：Windows 7 拡張セキュリティ更新プログラム（最大で2023年1月まで））

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）

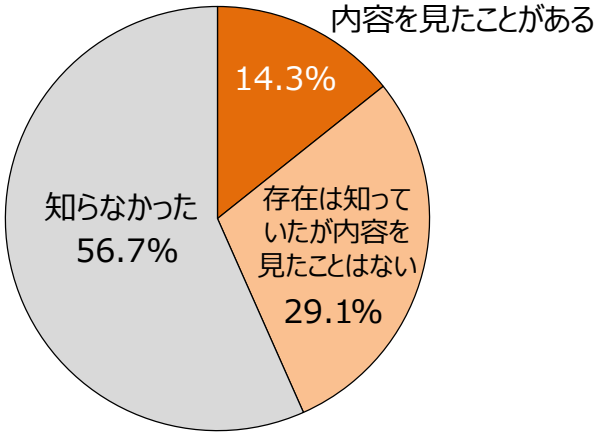


テレワークセキュリティに関する２次実態調査結果⑤

➢ 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。

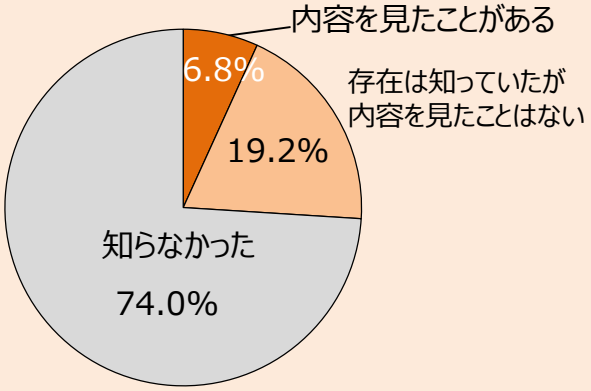
「テレワークセキュリティガイドライン」の認知状況

（n=1,996：テレワーク実施企業）

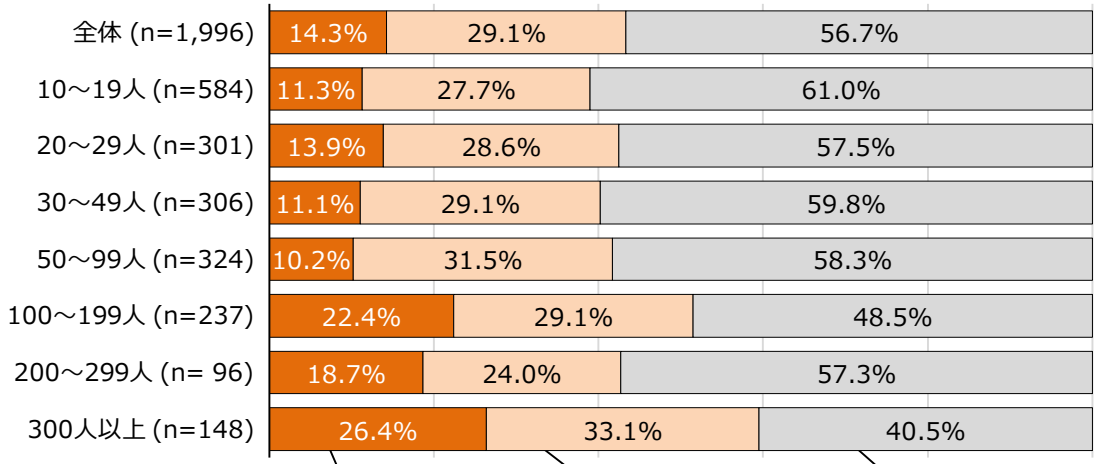


「中小企業等担当者向けテレワークセキュリティの手引き」の認知状況

（n=1,996：テレワーク実施企業）

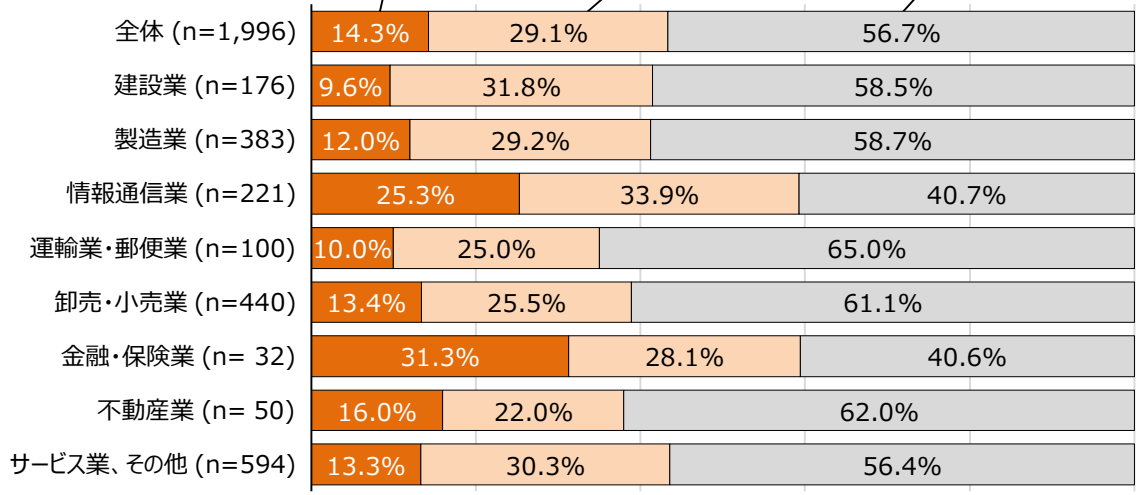


規模別



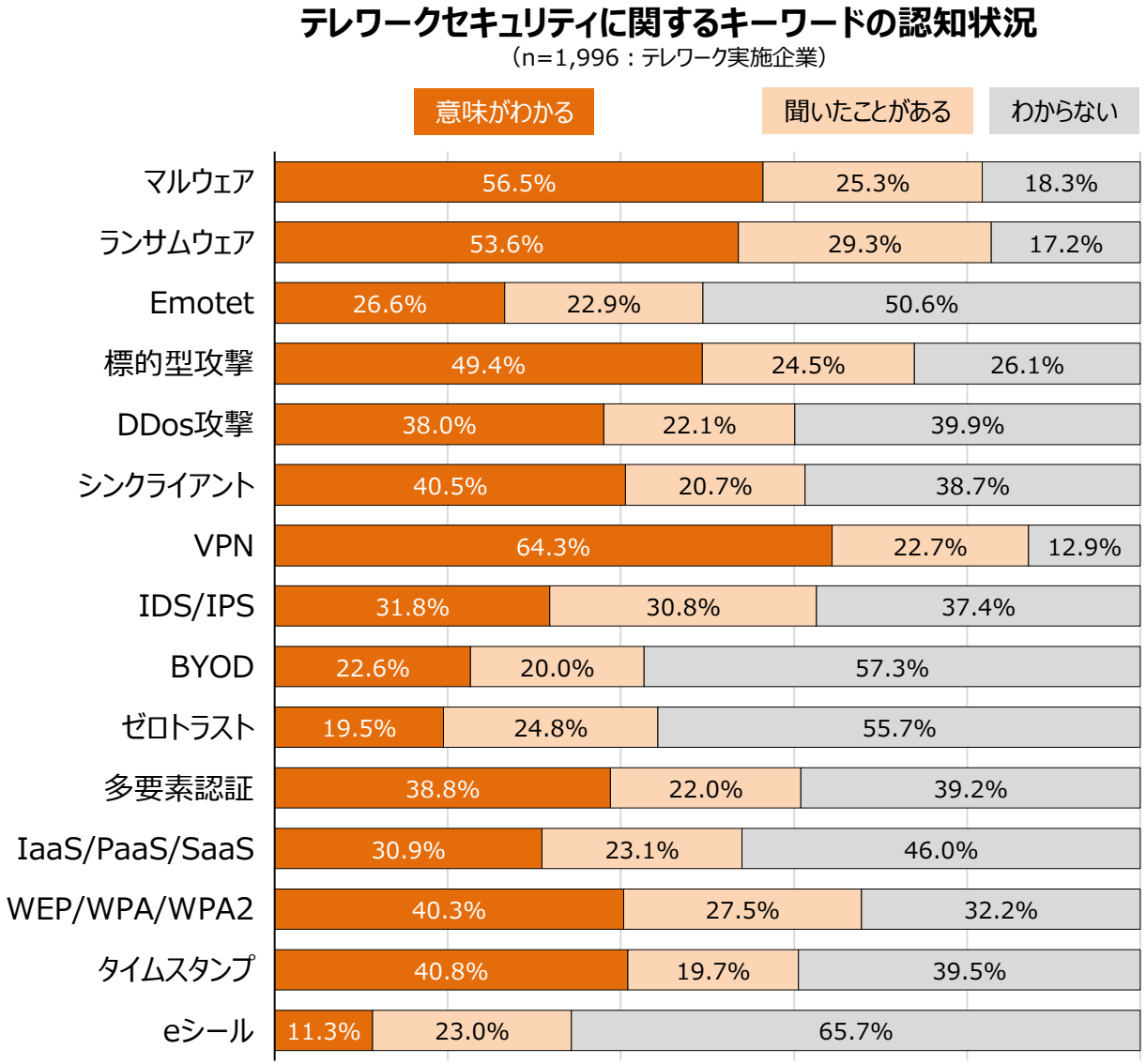
内容を見たことがある　存在は知っていたが内容を見たことはない　知らなかった

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。



テレワークセキュリティに関する１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。
１次調査）　期間：2020.7.29-2020.8.24　　回答数：5,433（うちテレワーク実施企業1,569）
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)

スクリーニング調査　※スクリーニング設問は5,433社が回答
S-1　テレワークの導入状況
S-2　テレワークの導入時期
S-3　新型コロナウイルス収束後のテレワークの活用予定
S-4　新型コロナウイルス収束後にテレワークを活用しない理由
S-5　テレワークの全従業員に対する利用割合
S-6　導入しているテレワークの形態
S-7　テレワークを導入しない理由
S-8　テレワークで行っている具体的な業務・実施方法
S-9　新たにテレワーク化・テレワーク利用拡大したい業務・実施方法

１　情報セキュリティ管理体制　※これ以降の設問はテレワーク導入済みの1,569社が回答
1-1　情報セキュリティ管理体制
1-2　昨年度のIT投資予算
1-3　今年度のテレワーク推進の予算
1-4　セキュリティに予算を割くことへの理解

２　テレワークの使用端末・構成方式
2-1　テレワークに使用しているPC端末
2-2　「会社支給のPC端末」の具体的な使用方法
2-3　「従業員所有のPC端末」へのデータ保存に関する対応
2-4　テレワークに使用しているモバイル端末
2-5　「会社支給のモバイル端末」へのデータ保存に関する対応
2-6　「従業員所有のモバイル端末」へのデータ保存に関する対応
2-7　使用している会社所有の端末(PC端末・モバイル端末)の種類
2-8　テレワーク用のPC端末から社内のシステムや情報にアクセスする場合の接続方法
2-9　テレワーク用のモバイル端末から社内のシステムや情報にアクセスする場合の接続方法

３　その他のテレワーク利用製品
3-1　テレワークで利用しているウイルス対策製品
3-2　テレワークで利用しているデバイス管理製品・サービス
3-3　テレワークで利用しているセキュアブラウザ
3-4　テレワークで通常利用しているブラウザ
3-5　テレワークで利用しているVPN製品
3-6　テレワークで利用しているリモートデスクトップ製品
3-7　テレワークで利用しているWEB会議システム
3-8　テレワークで利用しているメールサービス
3-9　テレワークで利用しているチャットツール
3-10　テレワークで利用しているストレージサービス
3-11　テレワークで利用しているクラウドアクセス用のネットワークセキュリティ製品
3-12　テレワークで利用している仮想デスクトップ方式の製品
3-13　テレワークで利用しているアプリケーション・ラッピング方式の製品

４　セキュリティ対策の状況
4-1　「テレワークセキュリティガイドライン」の認知度
4-2　テレワークセキュリティガイドラインの活用により役立った点
4-3　テレワークセキュリティガイドラインを活用しなかった理由
4-4　テレワーク導入検討に当たり時間や労力を費やした点
4-5　情報セキュリティの管理体制等に関する対策の実施状況
4-6　各種サイバー攻撃に関する対策の実施状況

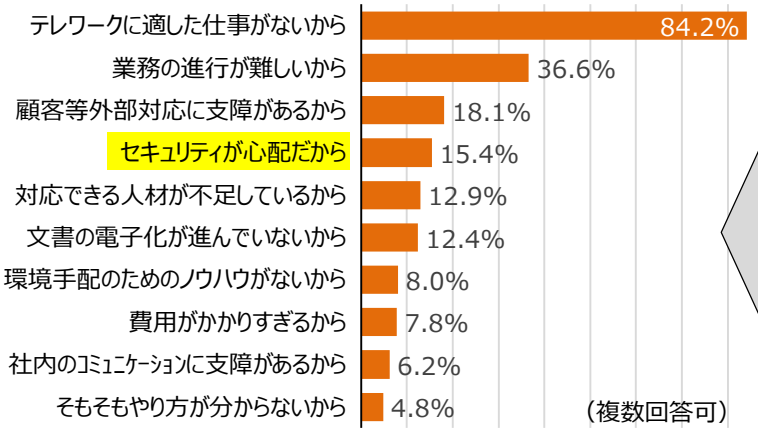
５　その他
5-1　テレワーク導入目的
5-2　テレワーク導入目的に対しての効果
5-3　テレワークの導入により働き方で大きく変革した点
6-1　テレワークの導入に当たっての課題
6-2　セキュリティ確保への具体的な課題
7-1　テレワークを導入する際に必要を感じた支援
7-2　テレワークを有効活用する上で利用したい支援

テレワークセキュリティに関する１次実態調査結果①

- テレワーク導入企業の過半が、緊急事態宣言前後（2020年３月・４月）にテレワークを導入。
- テレワークを導入しない理由として、業務都合を除くとセキュリティに関する懸念がトップ。

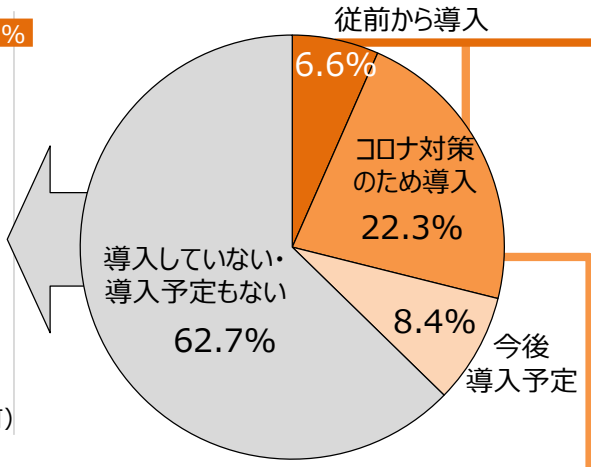
テレワークを導入しない理由

（n=3,406：テレワーク未導入企業）



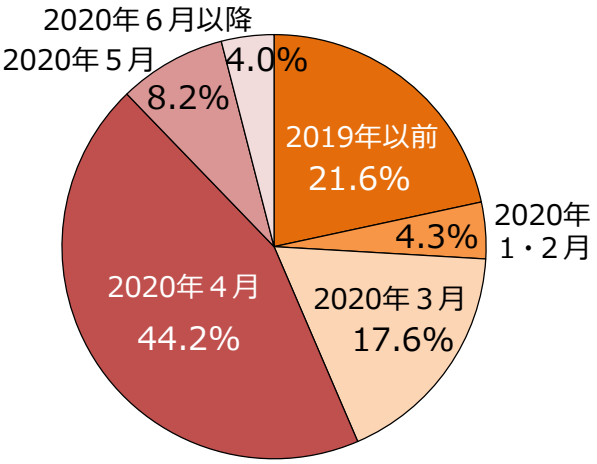
テレワークの導入状況

（n=5,433）



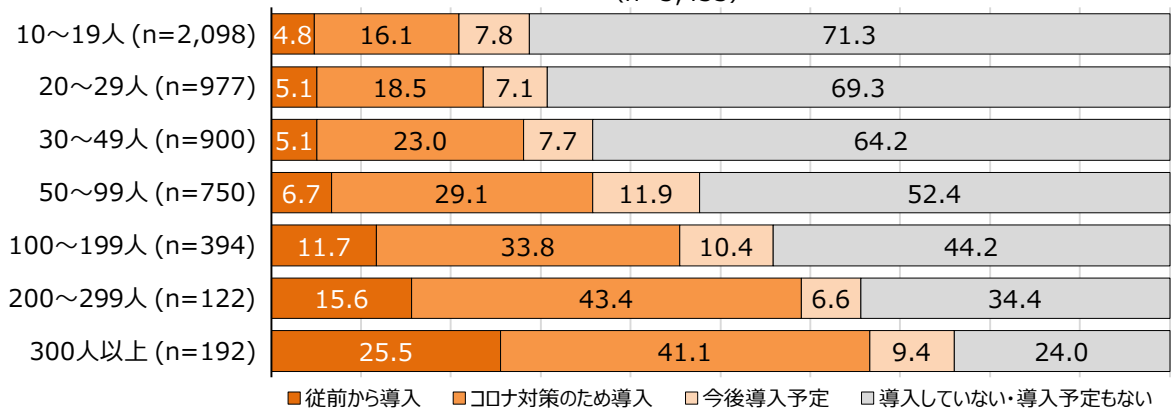
テレワークの導入時期

（n=1,569：テレワーク導入企業）



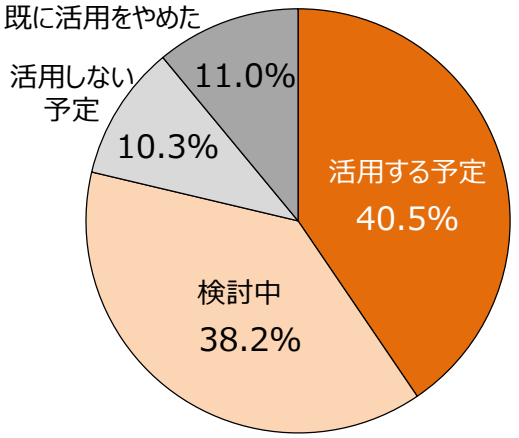
テレワークの導入状況（従業員規模別）

（n=5,433）



新型コロナ収束後のテレワーク活用予定

（n=1,209：コロナ対策のためテレワーク導入した企業）

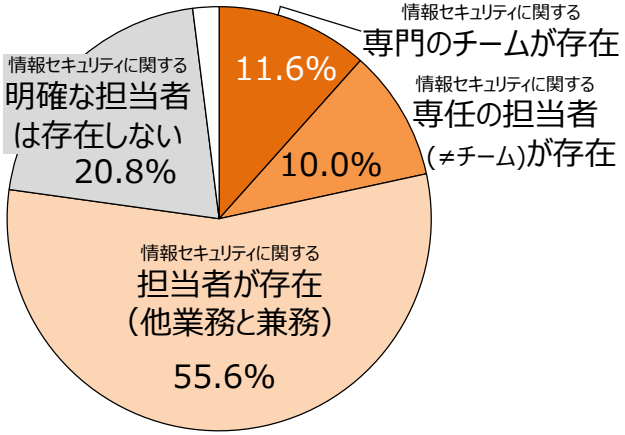


テレワークセキュリティに関する１次実態調査結果②

- セキュリティ確保がテレワーク導入に当たっての上位課題。サポート期限切れ端末の利用も見受けられる。
- テレワークセキュリティガイドラインについても、認知度は２割弱にとどまり、一層の周知が必要。

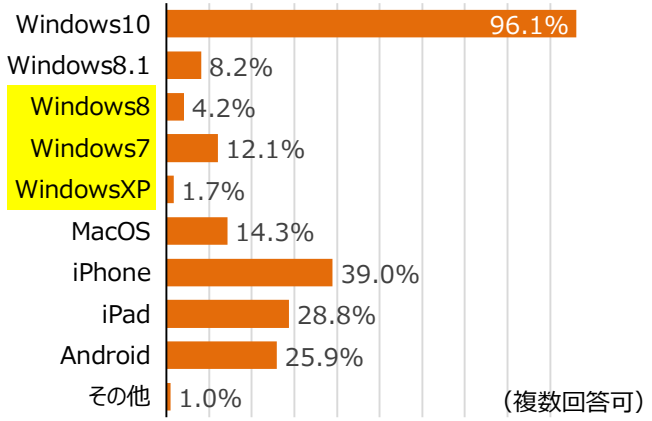
情報セキュリティ管理体制

（n=1,569：テレワーク導入企業）



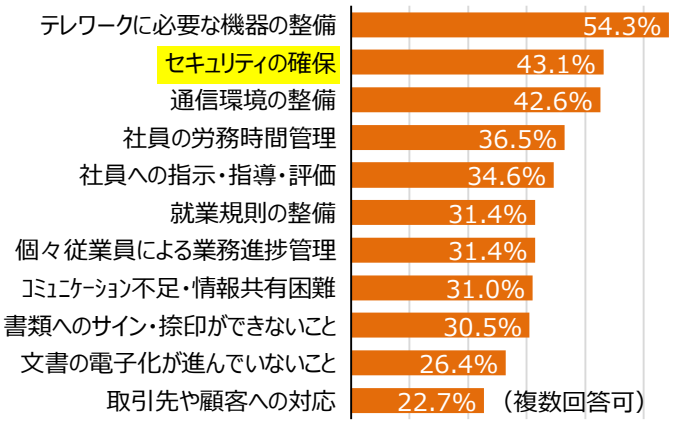
使用している会社所有の端末の種類

（n=1,569：テレワーク導入企業）



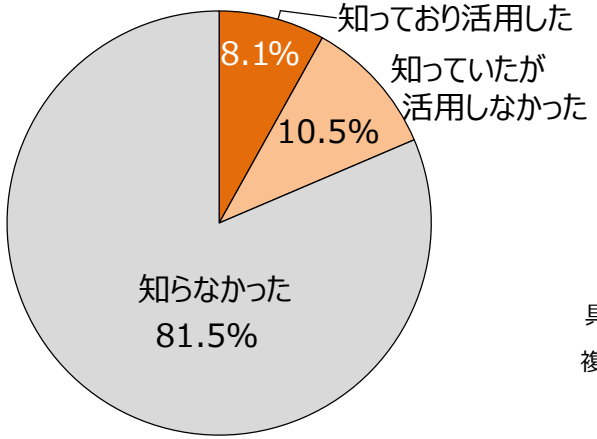
テレワークの導入に当たっての課題

（n=1,569：テレワーク導入企業）



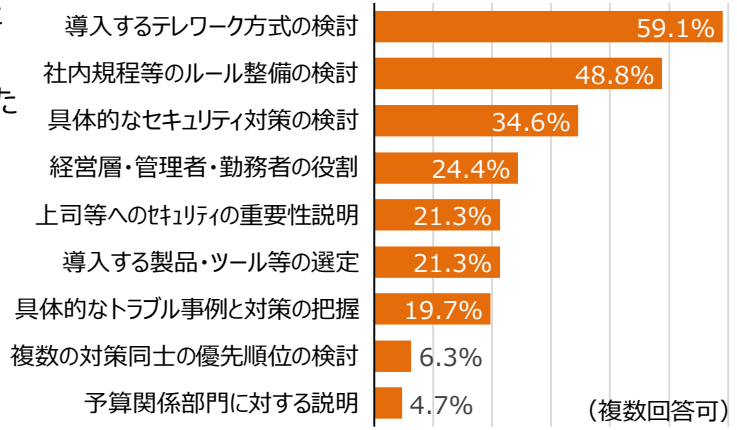
テレワークセキュリティガイドラインの認知度

（n=1,569：テレワーク導入企業）



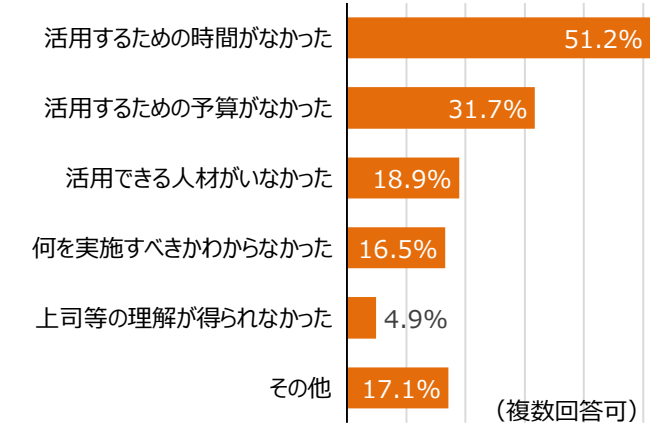
ガイドラインの活用により役立った点

（n=127：テレワーク導入企業＆ガイドライン活用）



ガイドラインを活用しなかった理由

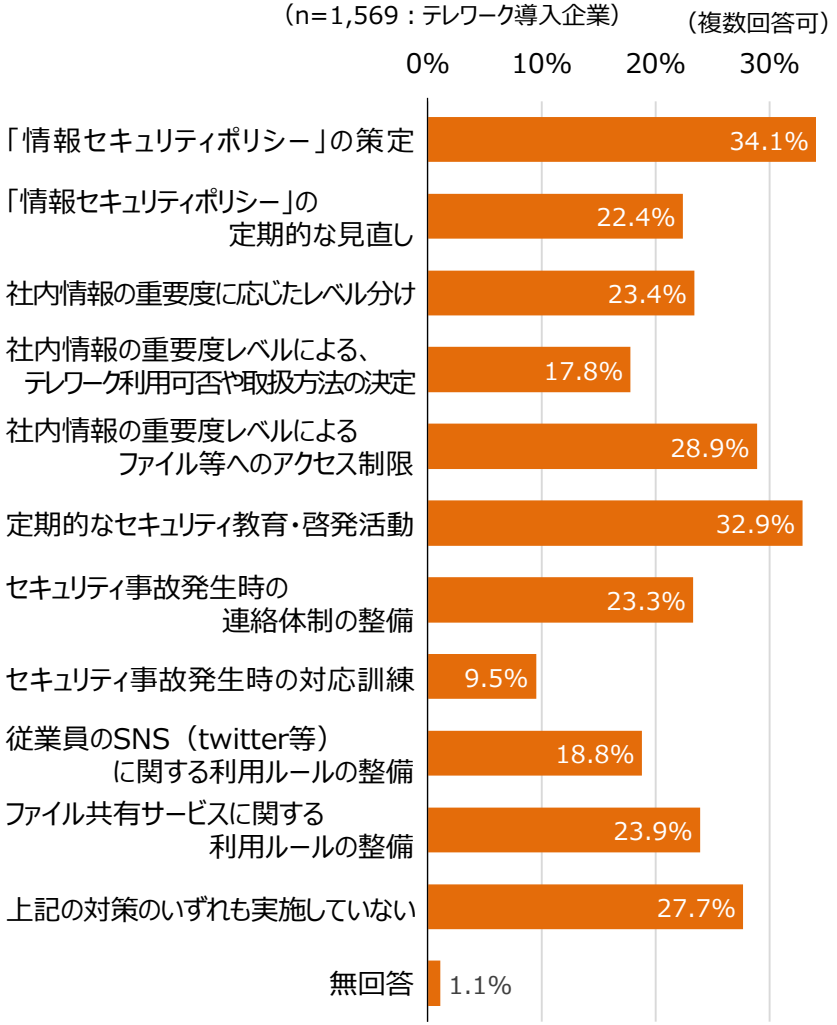
（n=164：テレワーク導入企業＆ガイドライン非活用）



テレワークセキュリティに関する１次実態調査結果③

- 情報セキュリティポリシーを策定している企業は約３分の１にとどまる。
- セキュリティ対策ソフトが常に最新になるように指示・設定している企業も約３分の２にとどまる。

情報セキュリティの管理体制等に関する対策の実施状況



各種サイバー攻撃に関する対策の実施状況