サイバー防犯診断
調査結果の概要

愛知県警察
AICHI POLICE

サイバー防犯診断

ランサムウェア等による企業のサイバー犯罪被害等が相次ぐ中、
捜査の過程で得た知見を踏まえた具体的な助言・指導をもって、中小企業の
情報セキュリティ対策の促進を図るため、サイバー防犯診断を実施しました。

○ アンケート調査　→ **４０３件**

○ 個別調査　→ **ホームページの調査　１２１件**

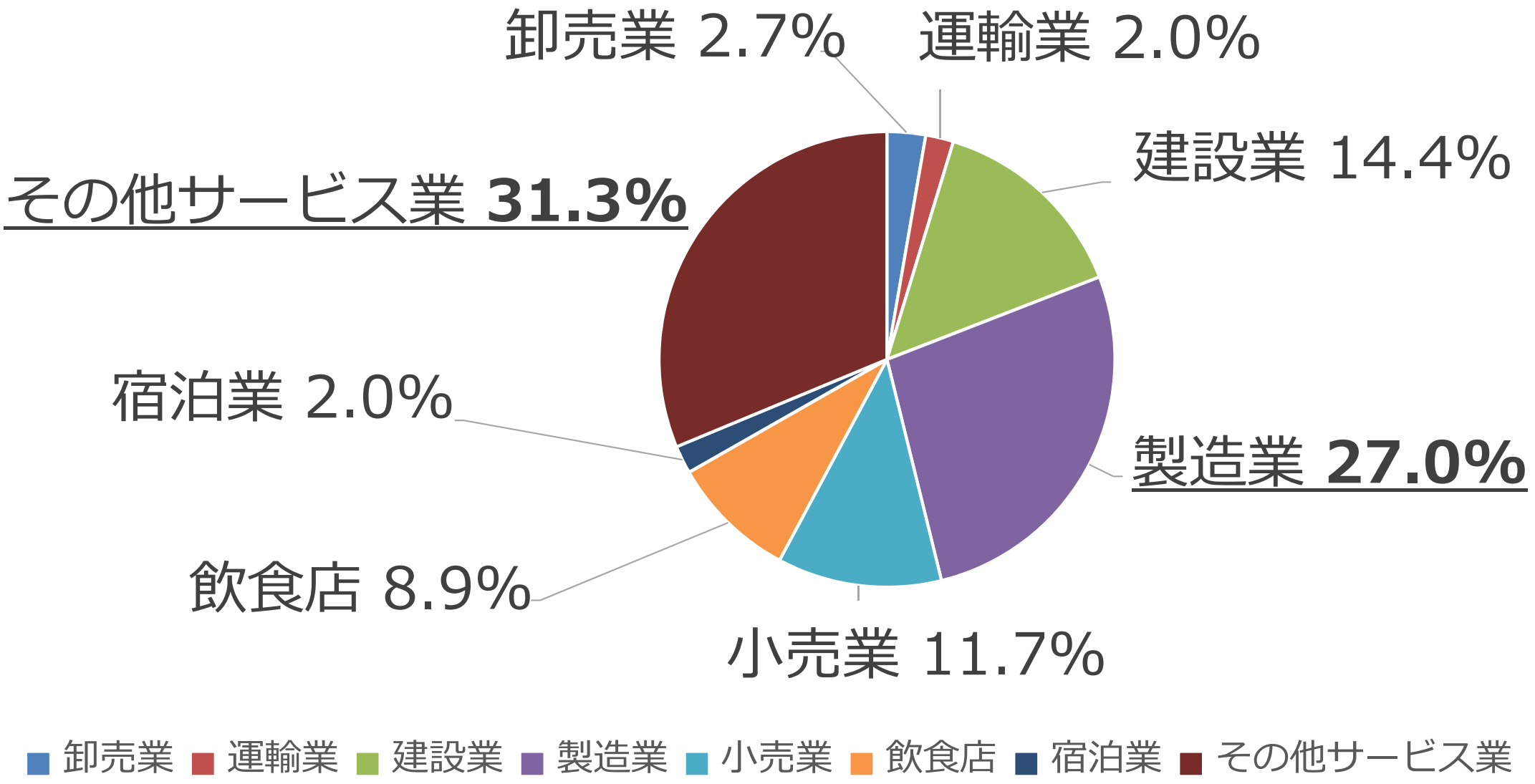
実地調査　４８件

（アンケート調査に協力いただいた事業者の中から希望に応じて）

サイバー防犯診断【アンケート結果から】

※%は小数点第一位まで表示（四捨五入）

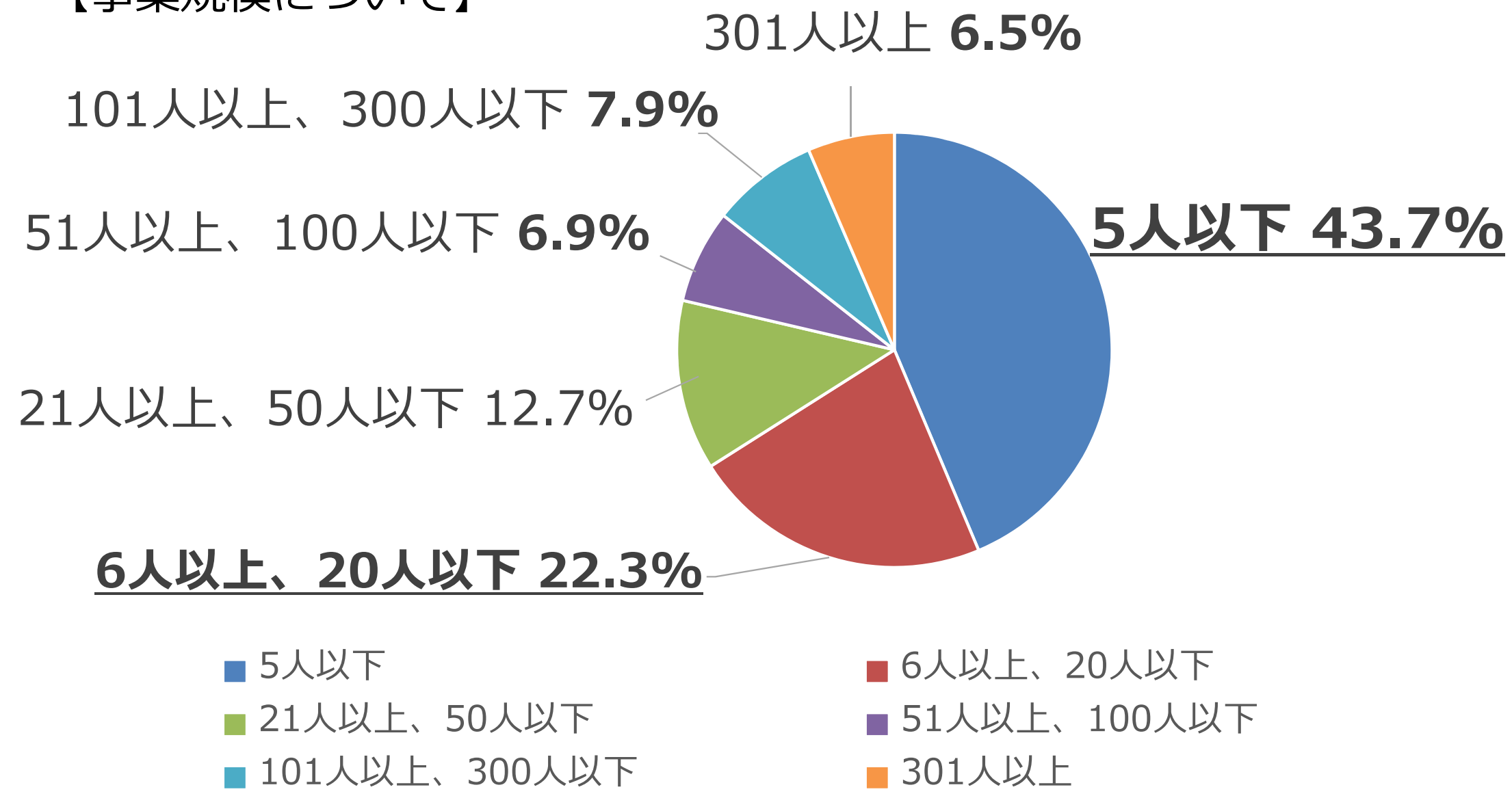
【業種について】



サイバー防犯診断【アンケート結果から】

※%は小数点第一位まで表示（四捨五入）

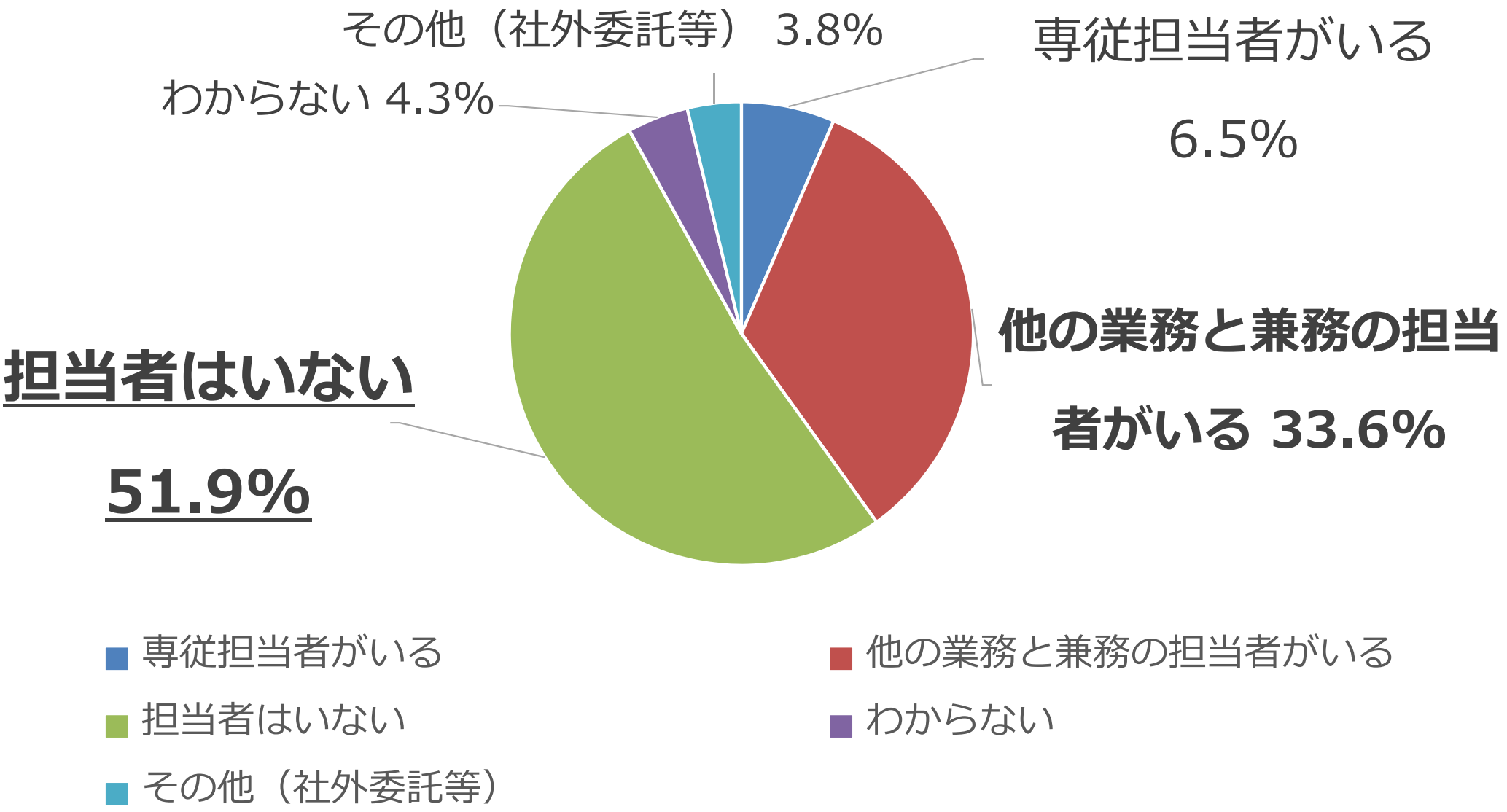
【事業規模について】



サイバー防犯診断【アンケート結果から】

※%は小数点第一位まで表示（四捨五入）

【情報セキュリティ担当者の有無について】

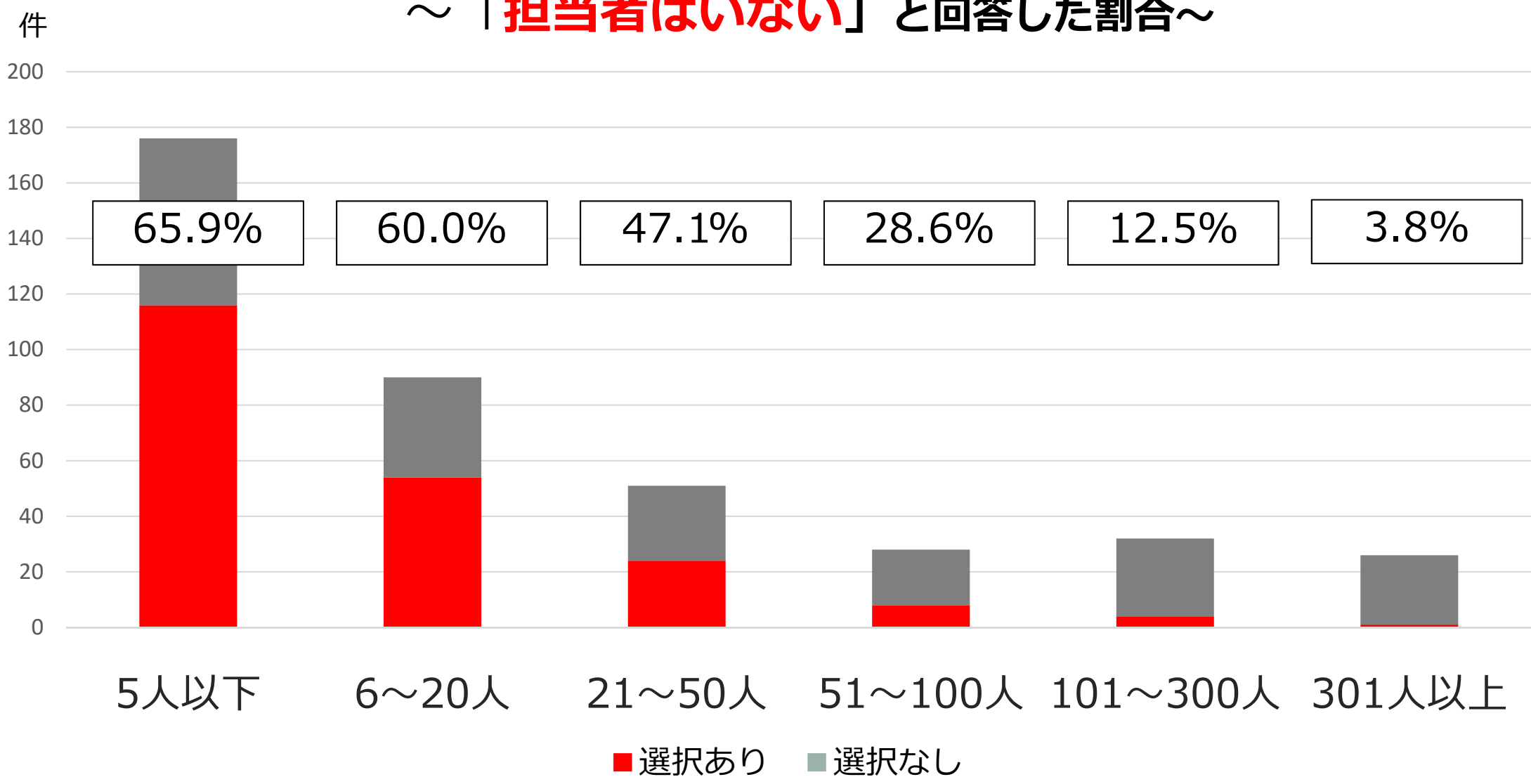


サイバー防犯診断【アンケート結果から】

※%は小数点第一位まで表示（四捨五入）

【情報セキュリティ担当者の有無】 ※事業規模別

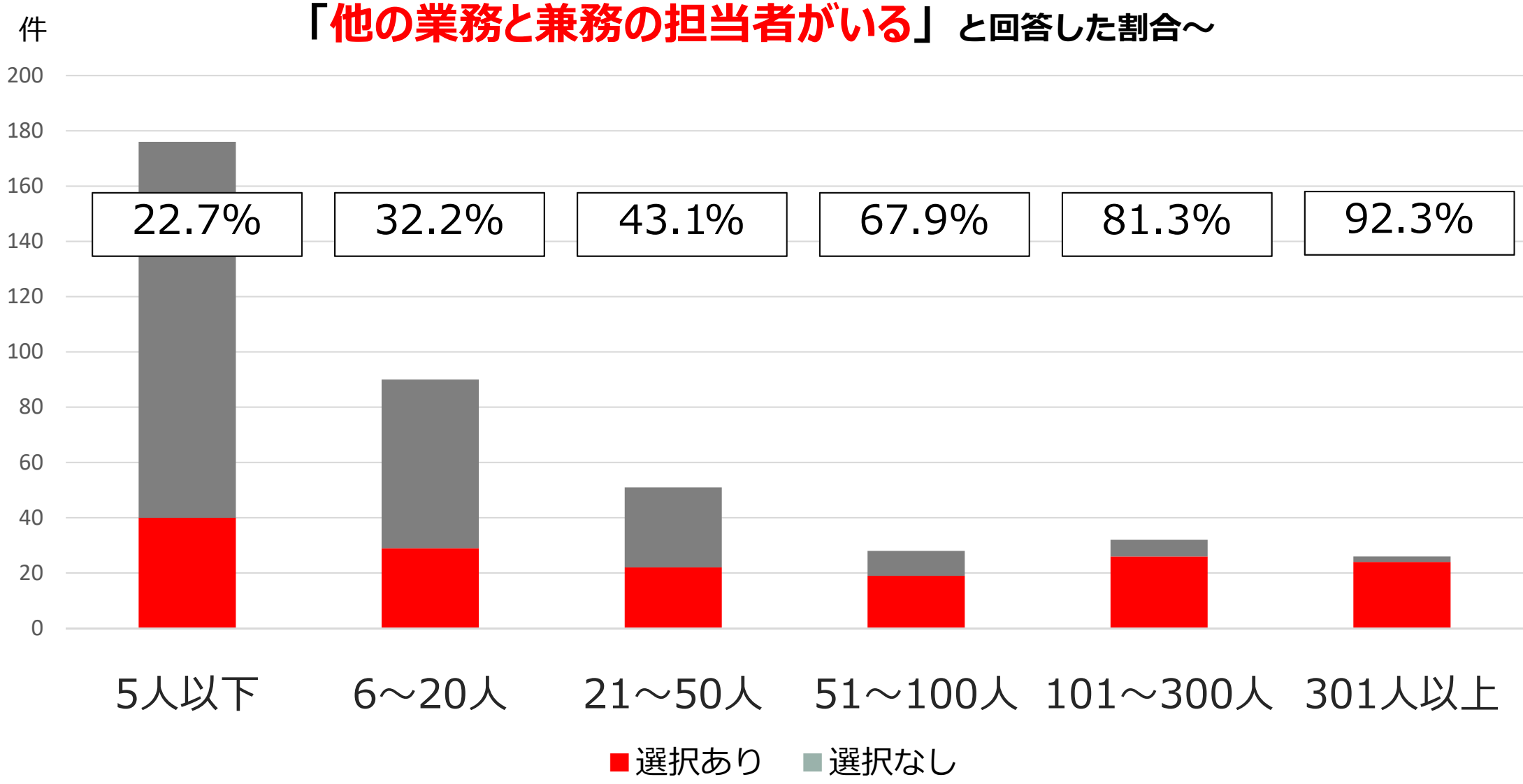
～「**担当者はいない**」と回答した割合～



サイバー防犯診断【アンケート結果から】

※%は小数点第一位まで表示（四捨五入）

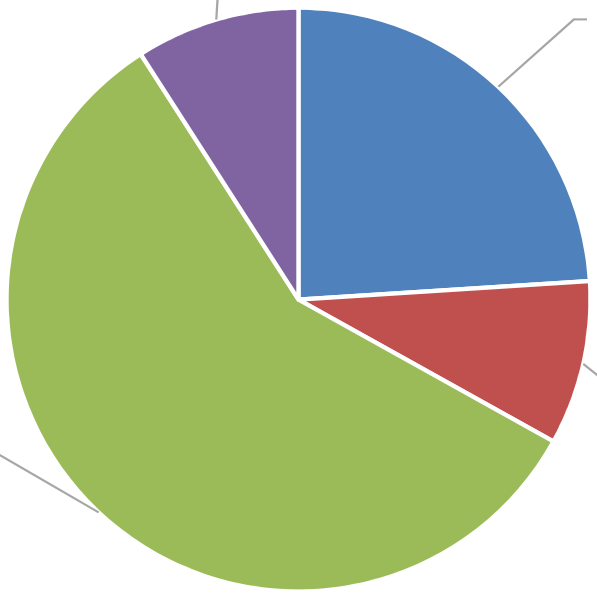
【情報セキュリティ担当者の有無】 ※事業規模別
～「専従担当者がいる」または「他の業務と兼務の担当者がいる」と回答した割合～



サイバー防犯診断【アンケート結果から】

※%は小数点第一位まで表示（四捨五入）

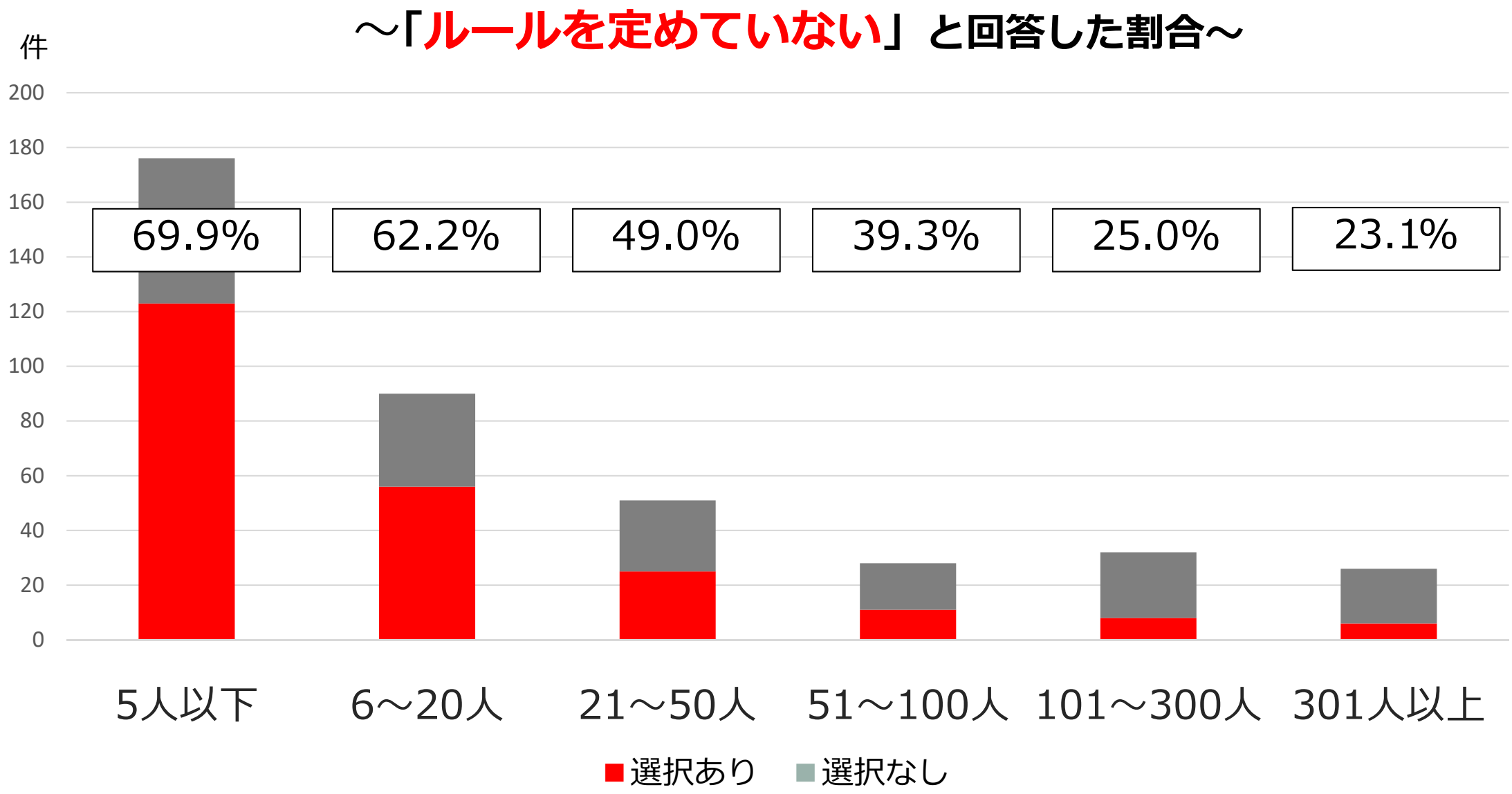
【情報セキュリティに対するルールについて】



サイバー防犯診断【アンケート結果から】

※%は小数点第一位まで表示（四捨五入）

【情報セキュリティに対するルールについて】 ※事業規模別

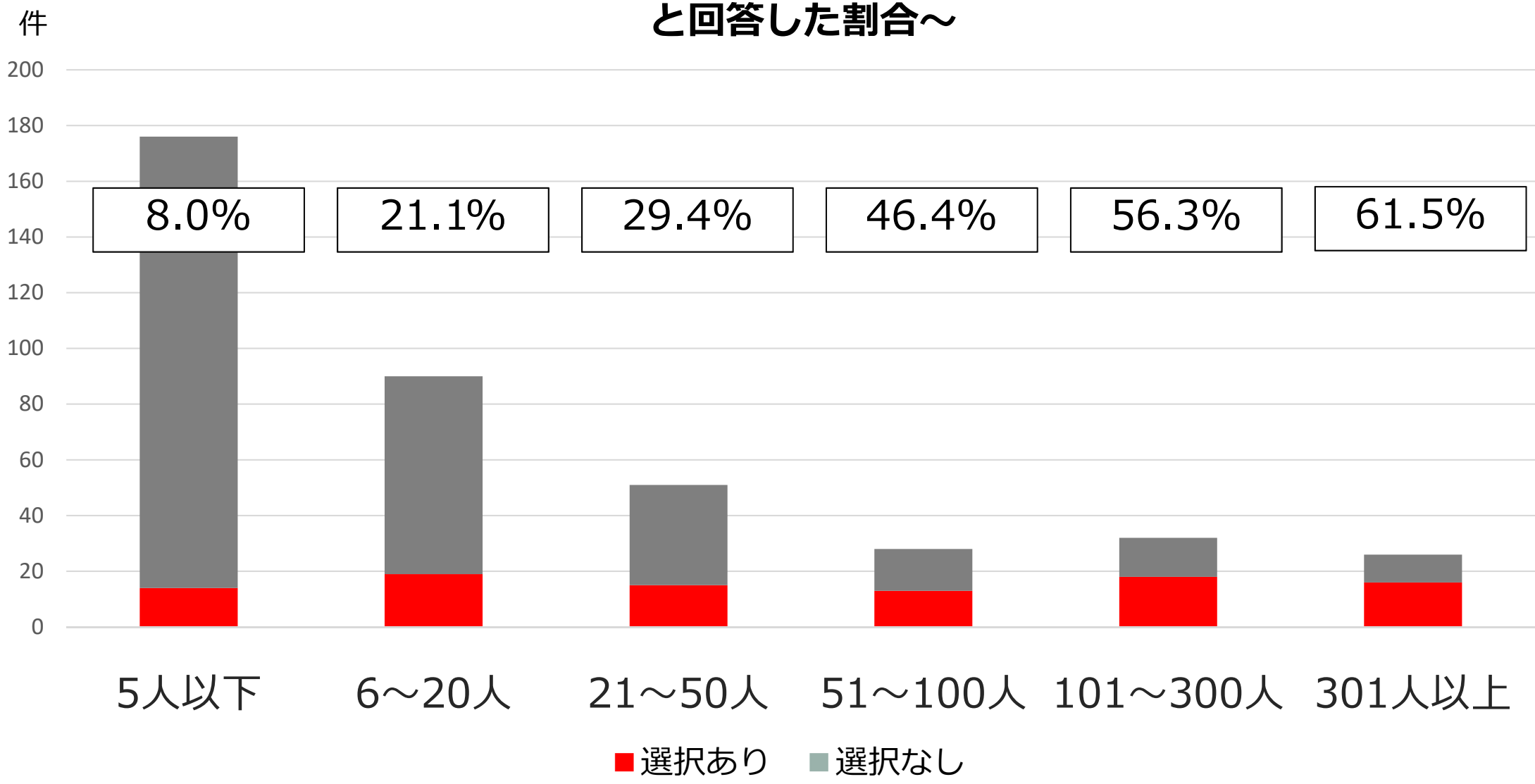


サイバー防犯診断【アンケート結果から】

※%は小数点第一位まで表示（四捨五入）

【情報セキュリティに対するルールについて】※事業規模別

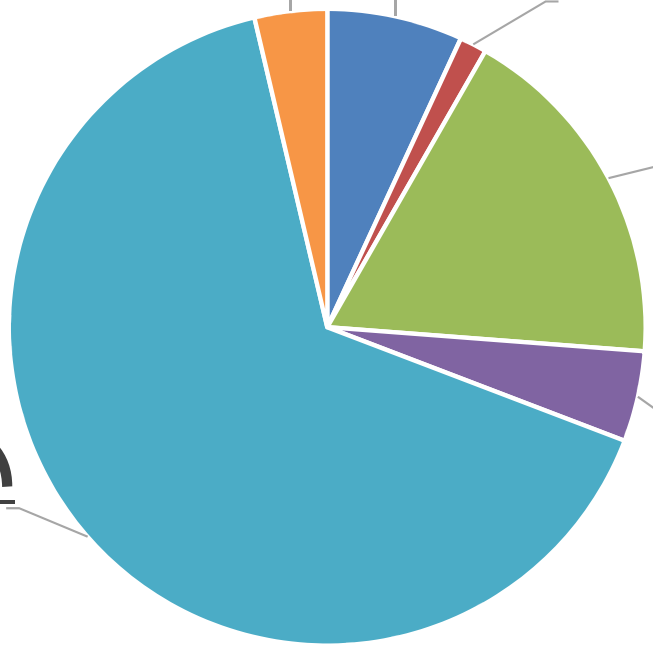
～「**業務で情報機器を扱う上でのルールが定められ、従業員に周知されている**」**と回答した割合**～



サイバー防犯診断【アンケート結果から】

※%は小数点第一位まで表示（四捨五入）

【従業員に対する情報セキュリティ教育について】



定期的に従業員等に対して集合教養を実施している 6.9%

その他の取り組みをしている 3.7%

グループ単位などで検討会などしている 1.4%

回覧、社内メール、社内掲示板などで、社内報などを展開している 17.9%

特にしていない 65.5%

情報システム監査の際に社員に指摘をしている 4.6%

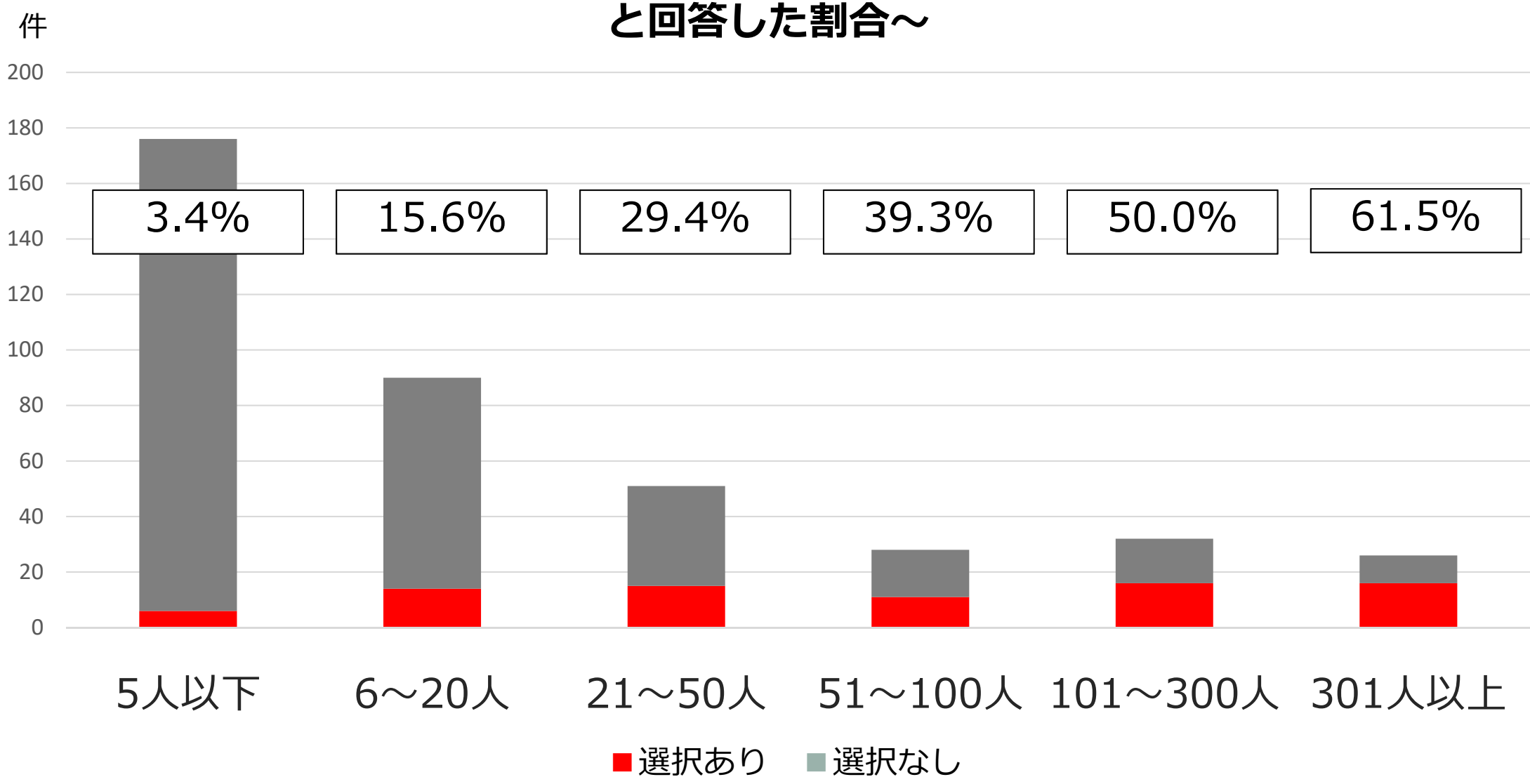
■ 定期的に従業員等に対して集合教養を実施している

■ グループ単位などで検討会などしている

サイバー防犯診断【アンケート結果から】

※%は小数点第一位まで表示（四捨五入）

【従業員に対する情報セキュリティ教育について】
～「回覧、社内メール、社内掲示板などで、社内報などを展開している」と回答した割合～



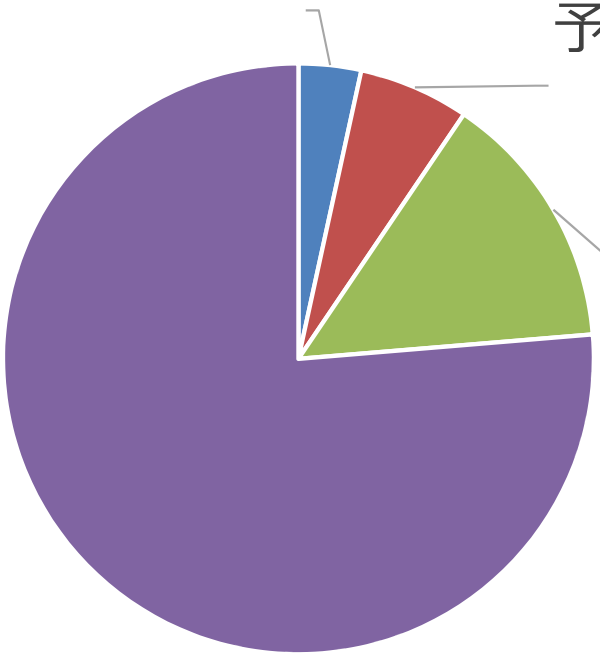
サイバー防犯診断【アンケート結果から】

※%は小数点第一位まで表示（四捨五入）

【IPAの中小企業の情報セキュリティ対策ガイドラインについて】

SECURITY ACTIONを自己宣言している、もしくはガイドラインに沿って取り組み始めている 3.4%

内容は理解しているが取り組み予定はない 6.1%



あることは知っているが内容はわからない 14.2%

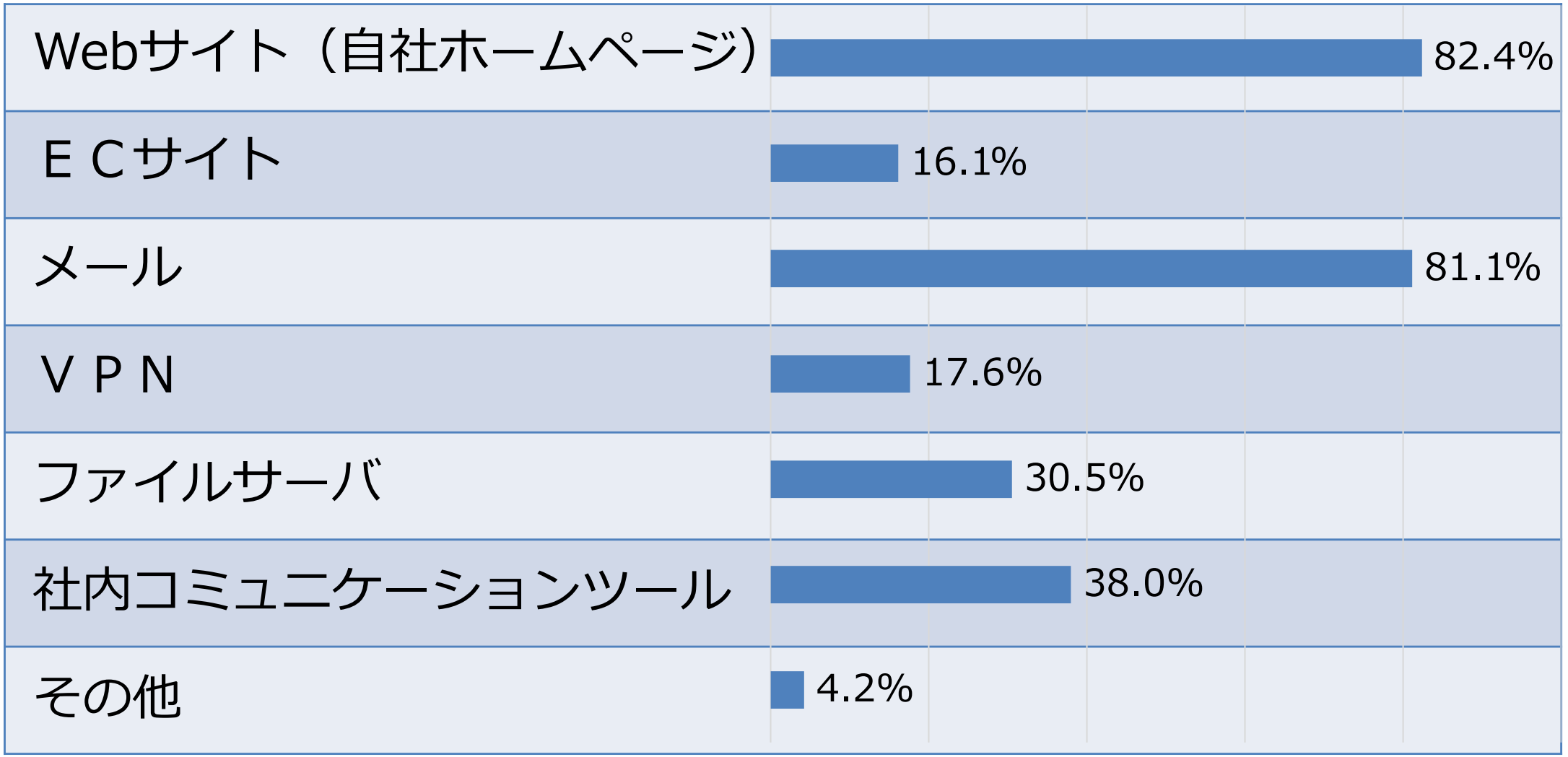
<u>知らない 76.3%</u>

- SECURITY ACTIONを自己宣言している、もしくはガイドラインに沿って取り組み始めている
- 内容は理解しているが取り組み予定はない
- あることは知っているが内容はわからない
- 知らない

サイバー防犯診断【アンケート結果から】

※%は小数点第一位まで表示（四捨五入）

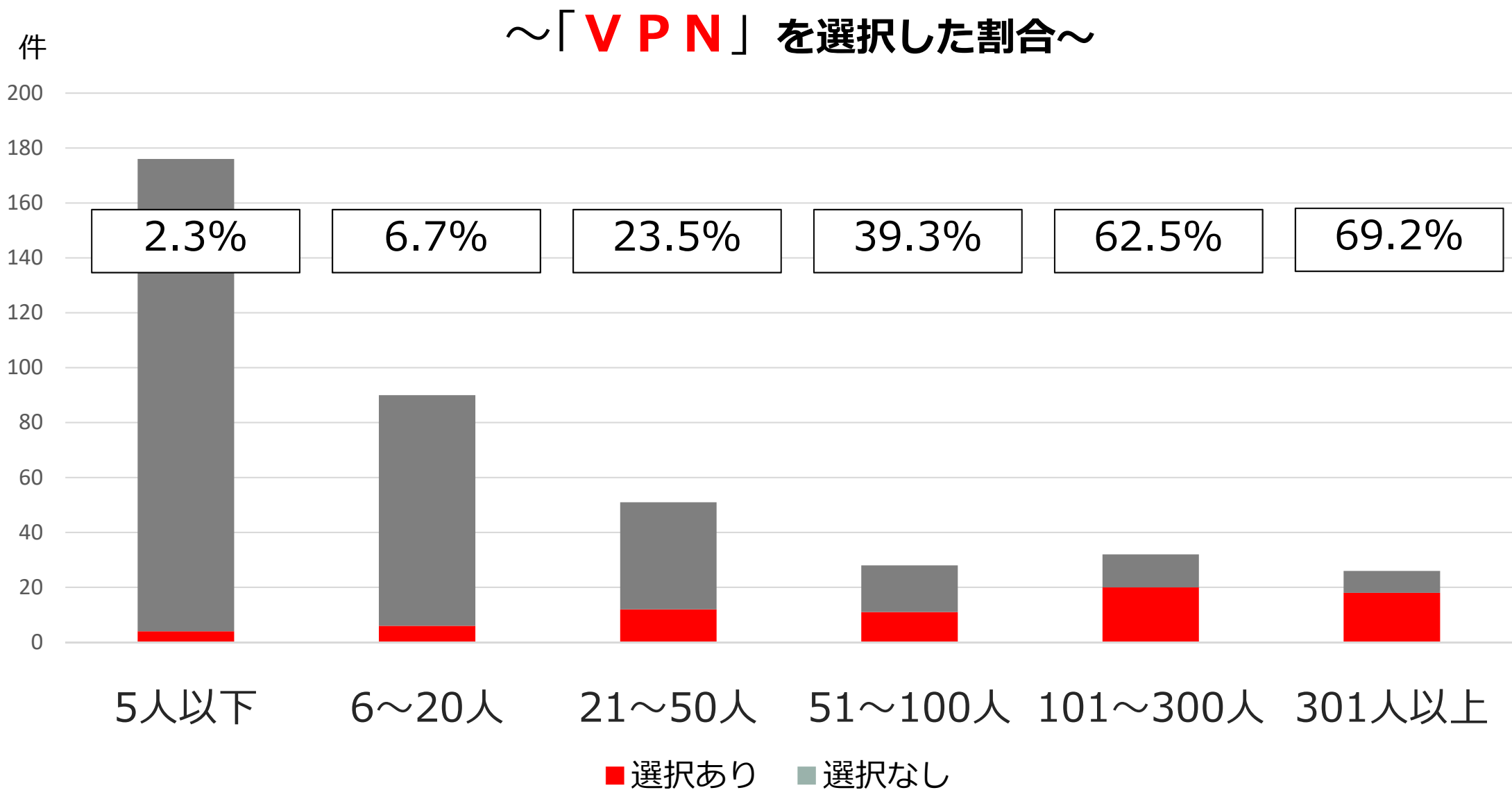
【運用している情報システムについて】※該当項目チェック式（複数回答可）



サイバー防犯診断【アンケート結果から】

※%は小数点第一位まで表示（四捨五入）

【運用している情報システムについて】 ※事業規模別

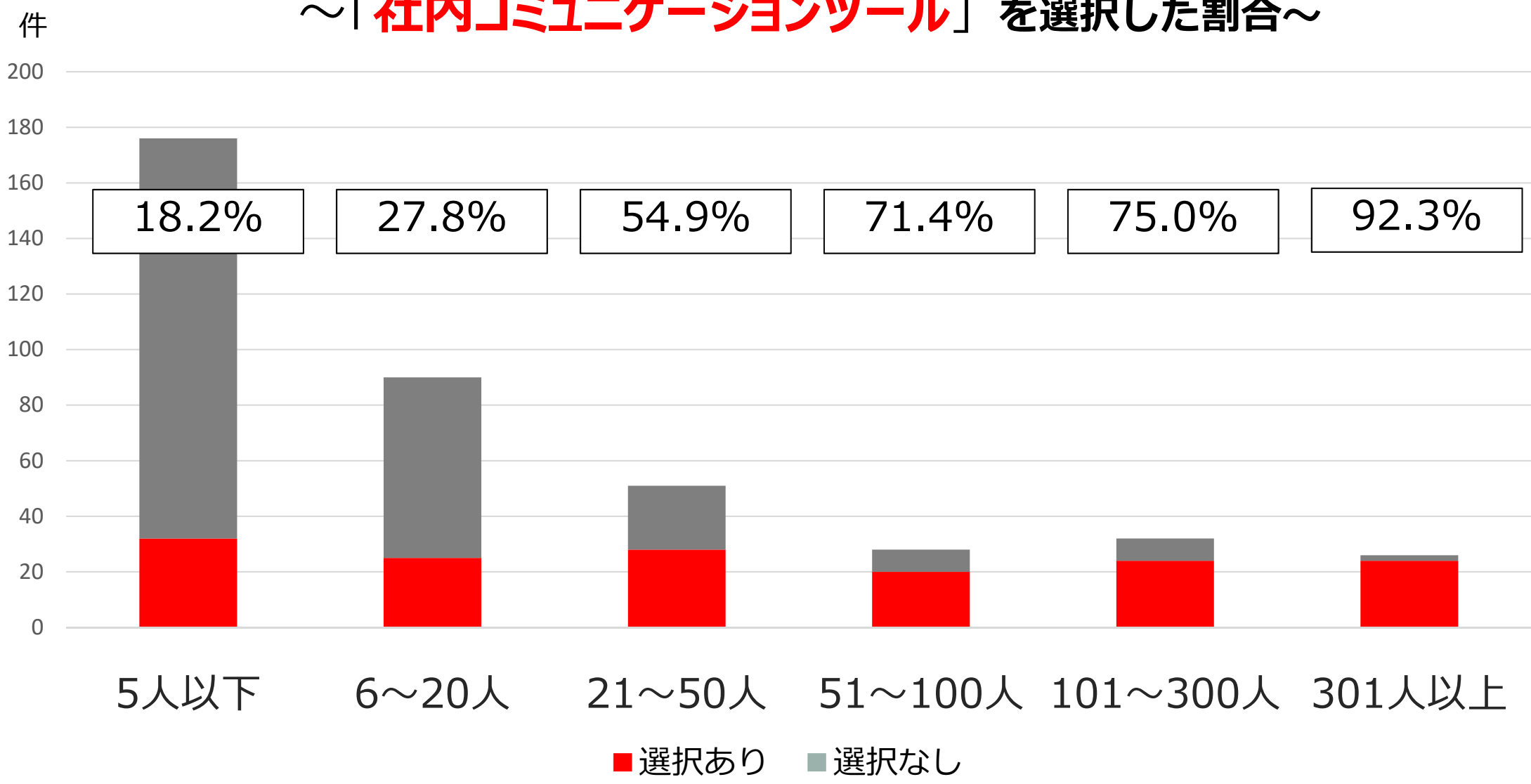


サイバー防犯診断【アンケート結果から】

※%は小数点第一位まで表示（四捨五入）

【運用している情報システムについて】 ※事業規模別

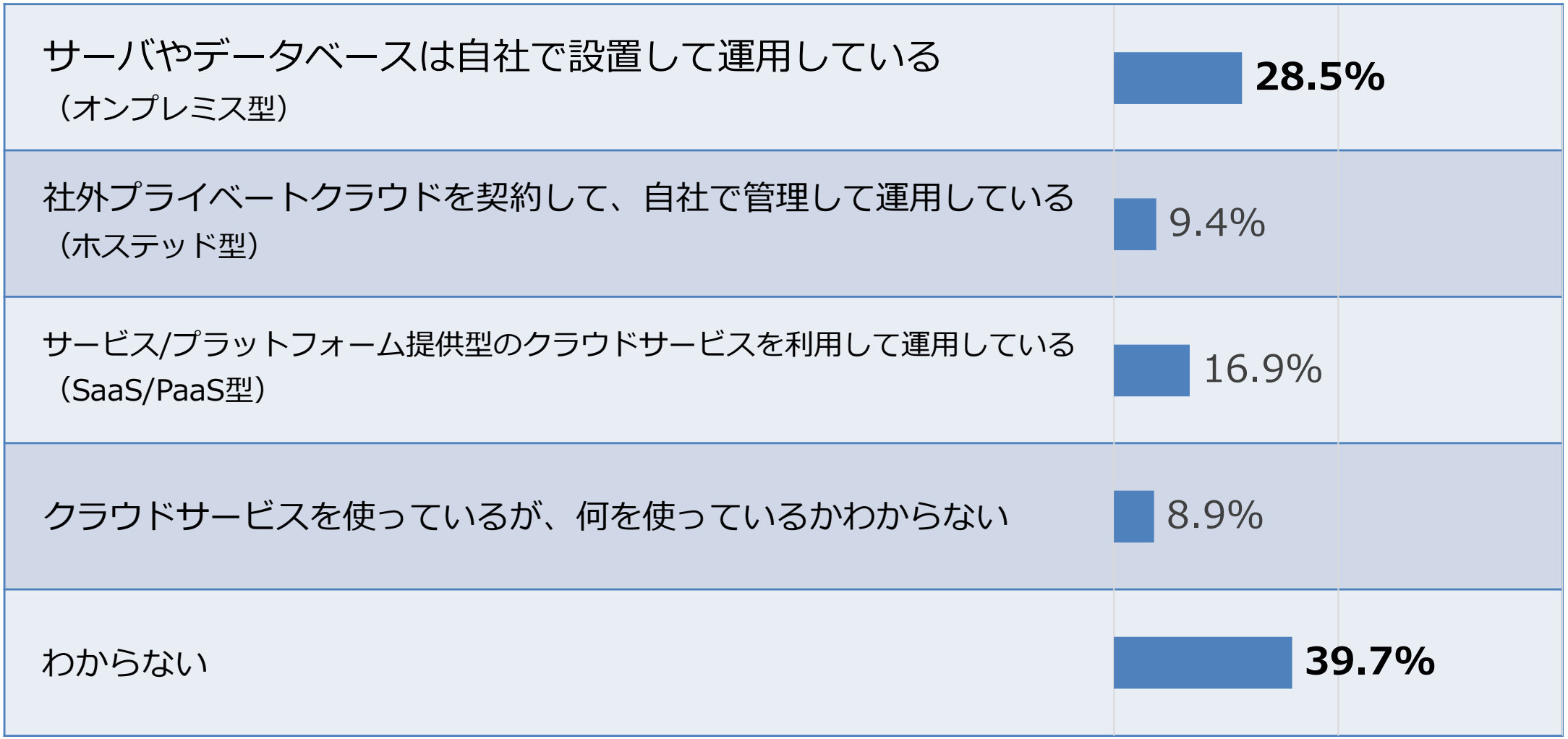
～「社内コミュニケーションツール」を選択した割合～



サイバー防犯診断【アンケート結果から】

※%は小数点第一位まで表示（四捨五入）

【クラウドサービスの利用状況について】　※該当項目チェック式（複数回答可）

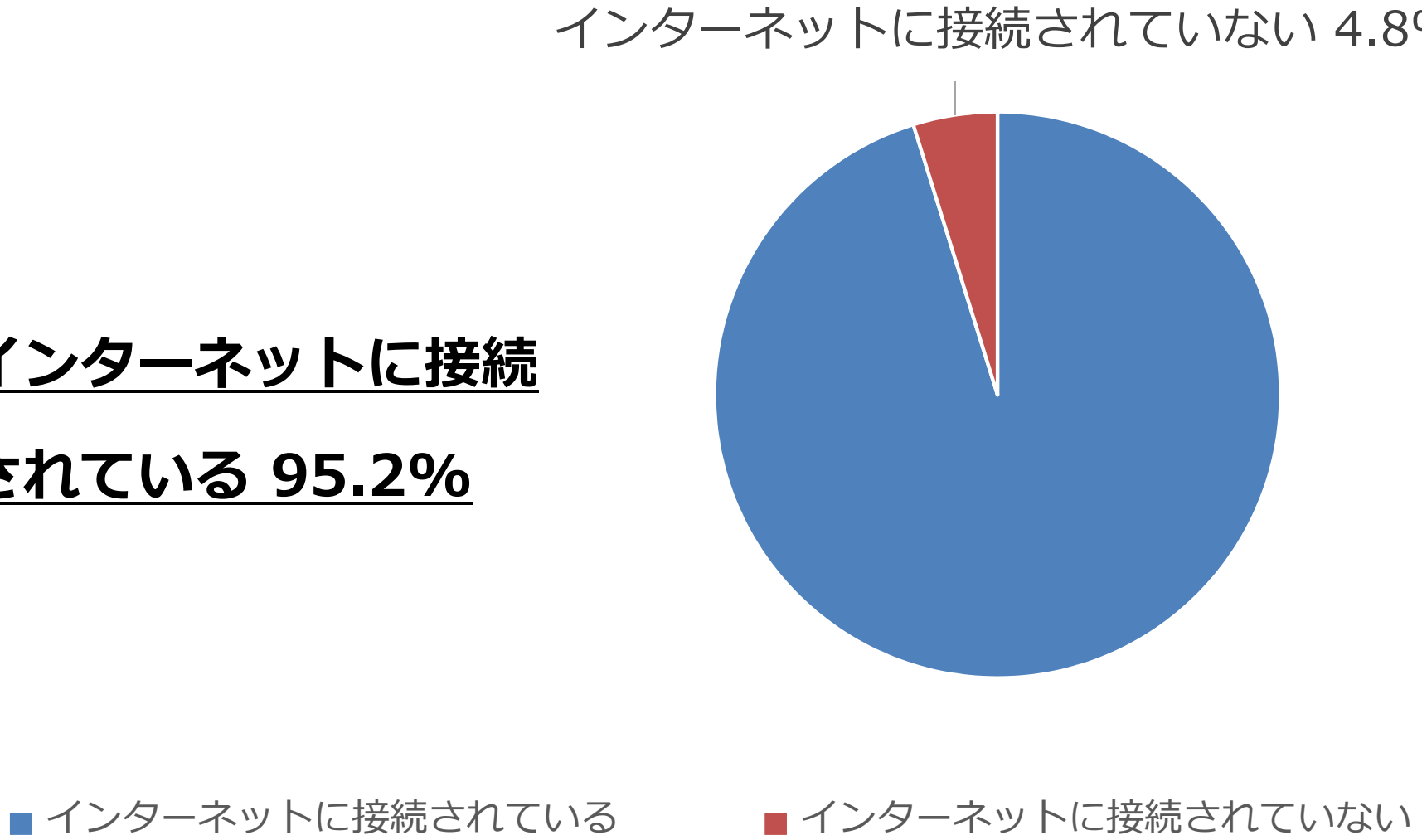


サイバー防犯診断【アンケート結果から】

※%は小数点第一位まで表示（四捨五入）

【システムのインターネット接続状況】

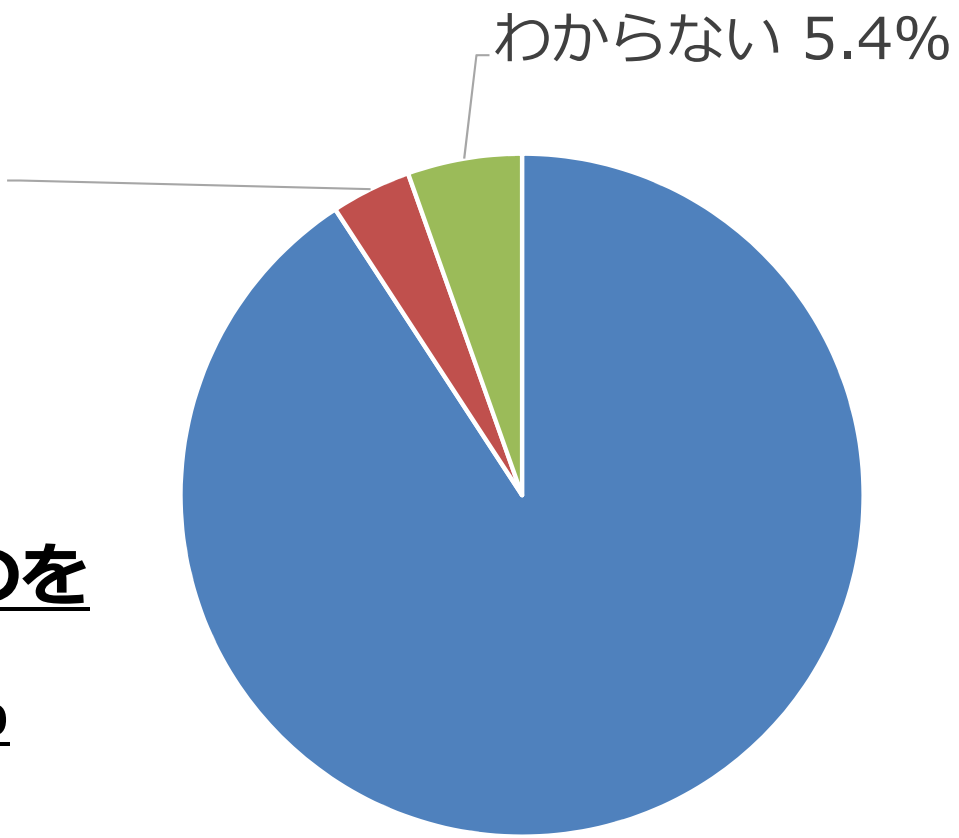
<u>インターネットに接続されている 95.2%</u>



サイバー防犯診断【アンケート結果から】

※%は小数点第一位まで表示（四捨五入）

【OSについて】



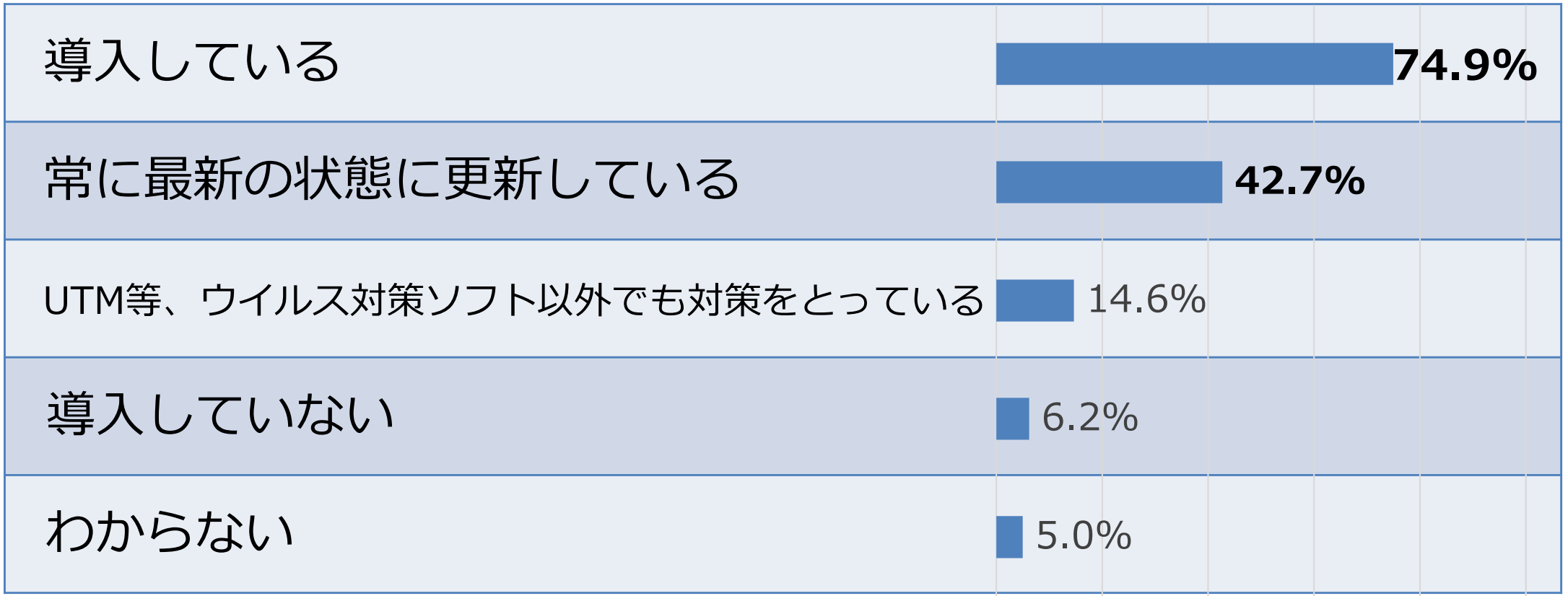
<u>サポート期間内のものを</u>

<u>使用している 90.8%</u>

サイバー防犯診断【アンケート結果から】

※%は小数点第一位まで表示（四捨五入）

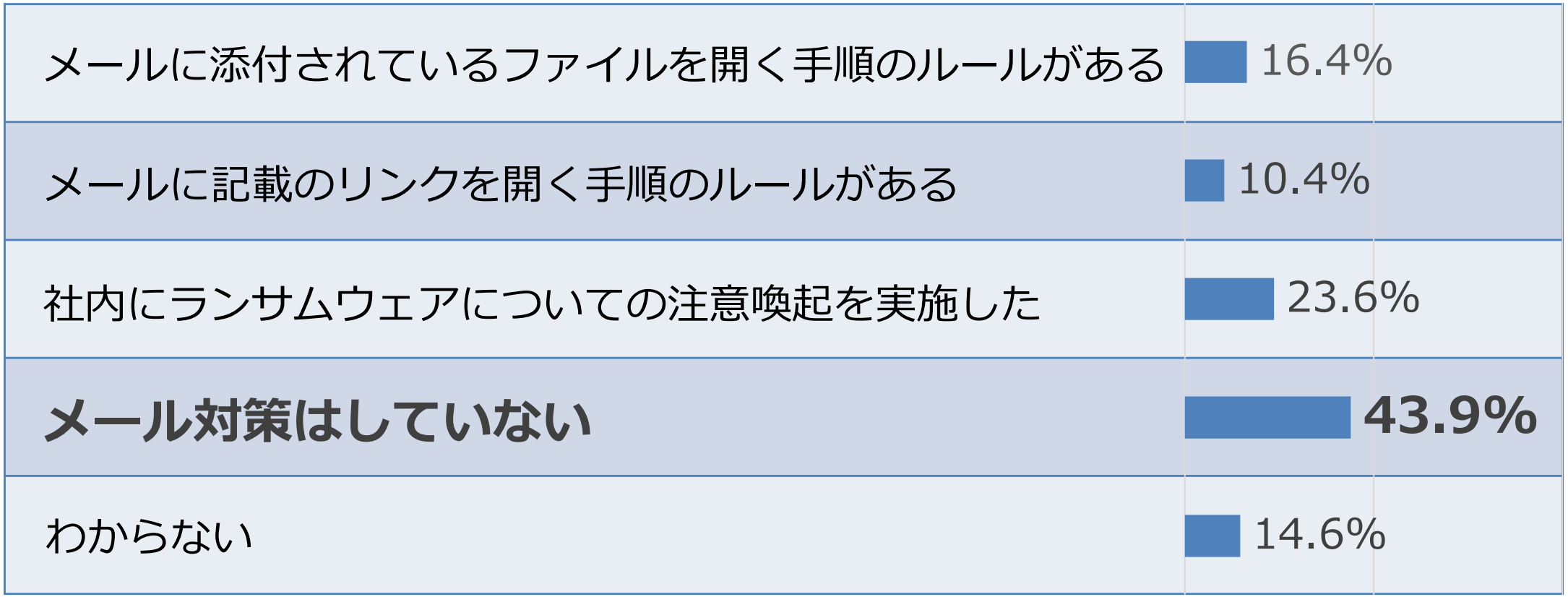
【ウイルス対策ソフトの導入について】 ※該当項目チェック式（複数回答可）



サイバー防犯診断【アンケート結果から】

※%は小数点第一位まで表示（四捨五入）

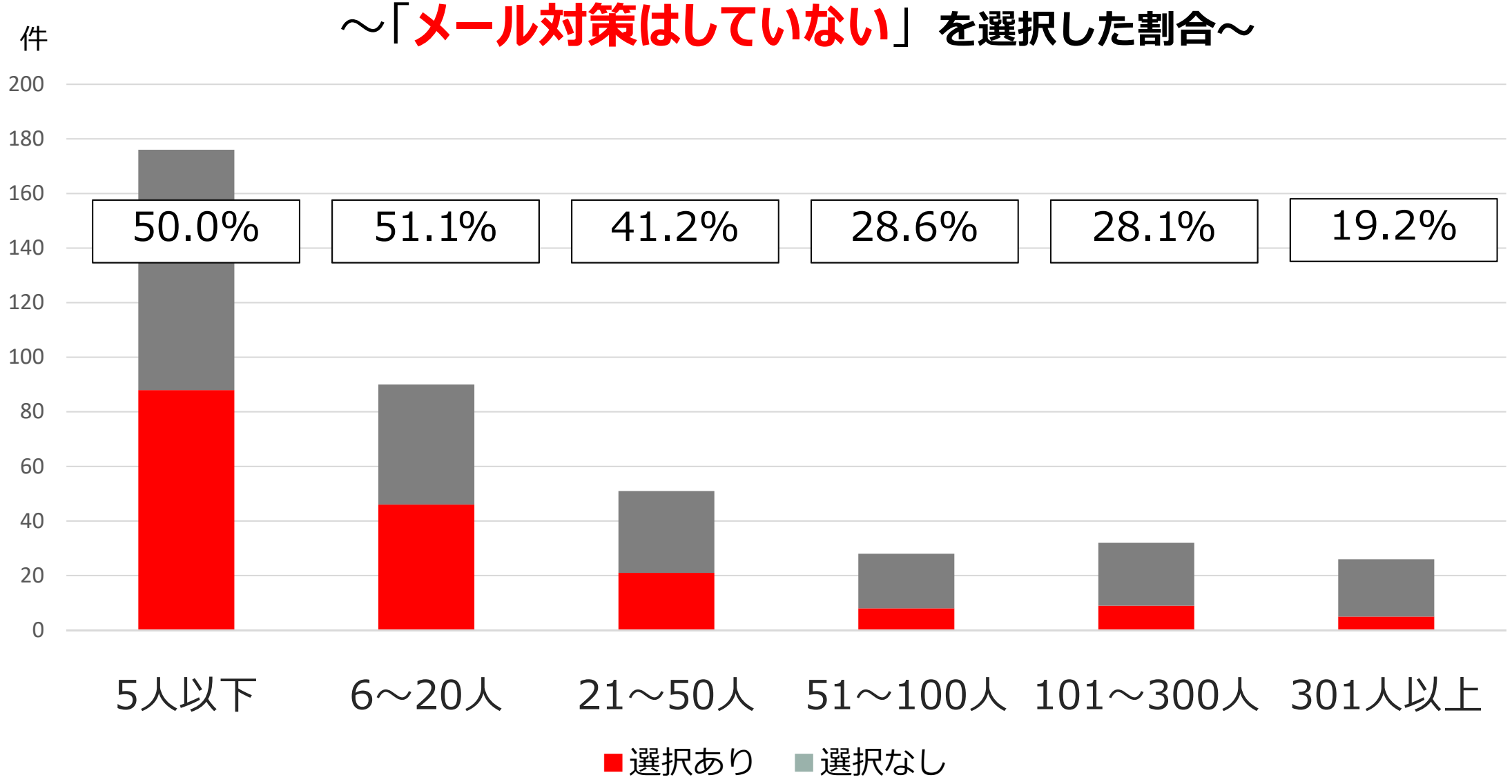
【メール対策について】 ※該当項目チェック式（複数回答可）



サイバー防犯診断【アンケート結果から】

※%は小数点第一位まで表示（四捨五入）

【メール対策について】　※事業規模別

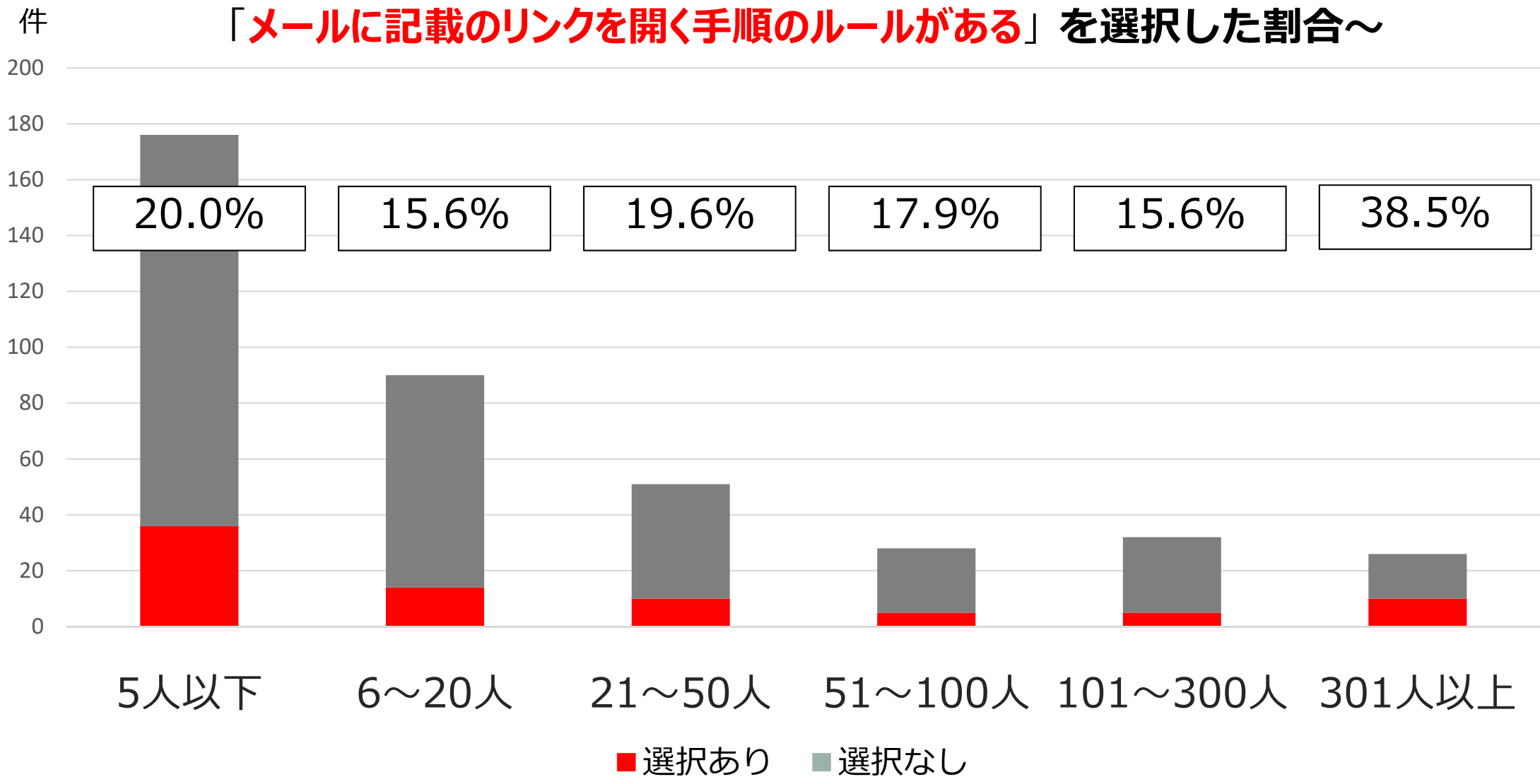


サイバー防犯診断【アンケート結果から】

※%は小数点第一位まで表示（四捨五入）

【メール対策について】　※事業規模別

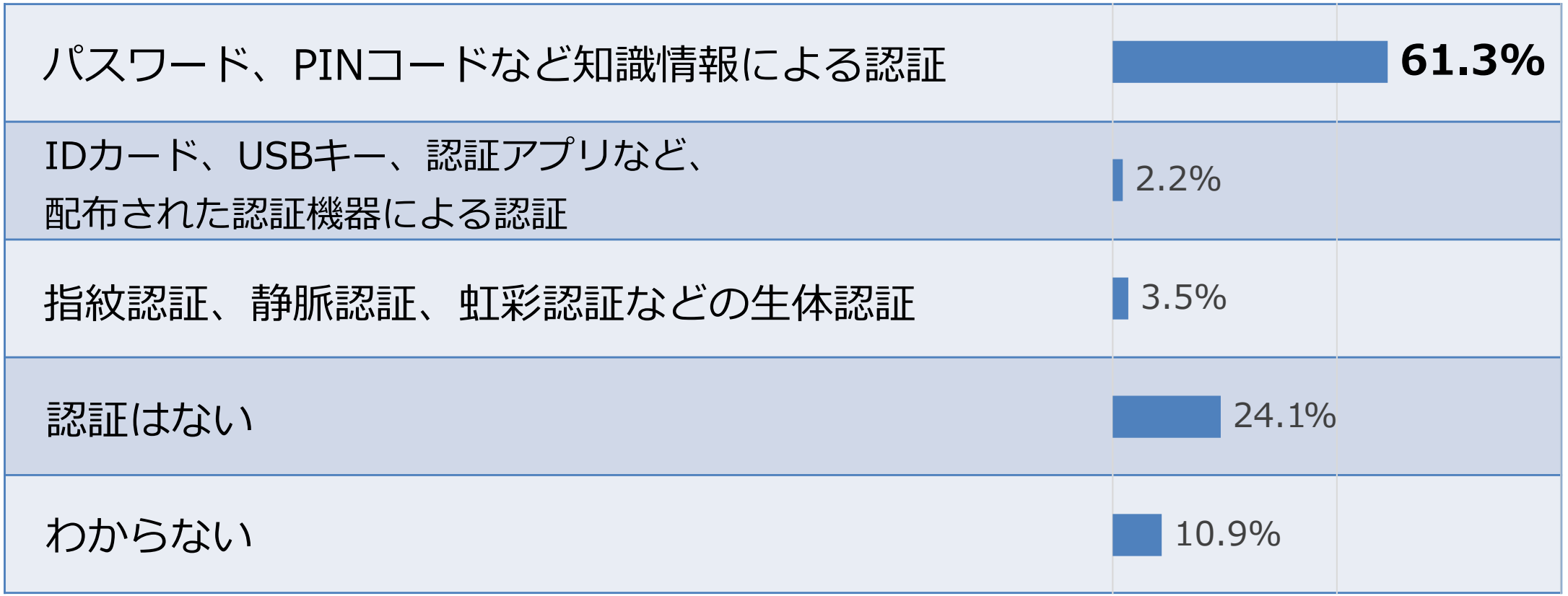
～「**メールに添付されているファイルを開く手順がある**」または
「**メールに記載のリンクを開く手順のルールがある**」を選択した割合～



サイバー防犯診断【アンケート結果から】

※%は小数点第一位まで表示（四捨五入）

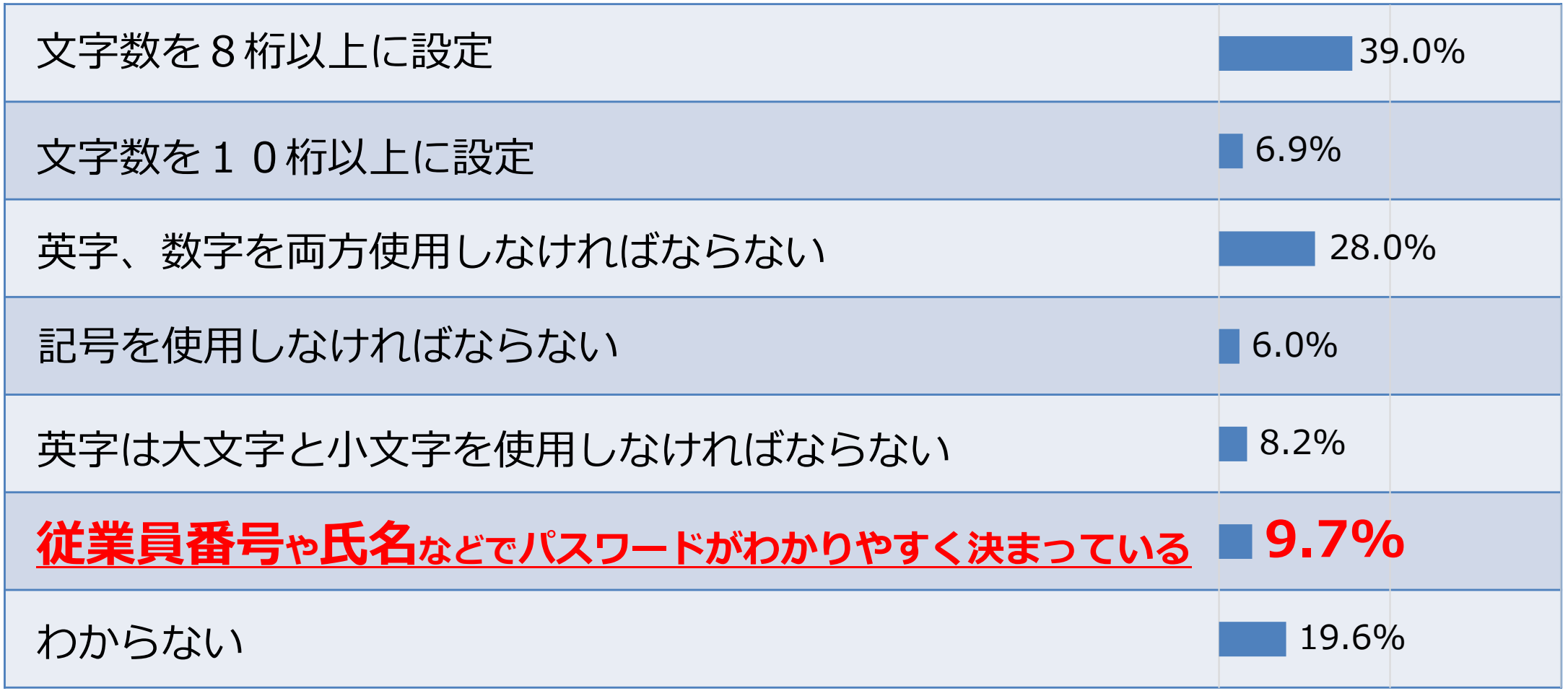
【認証方法について】 ※該当項目チェック式（複数回答可）



サイバー防犯診断【アンケート結果から】

※%は小数点第一位まで表示（四捨五入）

【パスワード設定について】※該当項目チェック式（複数回答可）



パスワード設定について　【補足】

従業員番号や氏名　→　**推測されるおそれ**があります。

グループウェアと呼ばれる業務システムのパスワードが、
まさに従業員番号や名前の組み合わせなどだったために、
外部からの侵入を許し、業務データが消去された事例が発生しています。

この問題は、従業員が退職した場合にも問題となる場合があります。
退職した従業員のパスワードは、当然、使えないようにしますが、
退職した従業員が、共用のパスワードを知っていたり、他の現役の従業員のパスワードが推測できたりする場合、実際に事件が起きることになります。

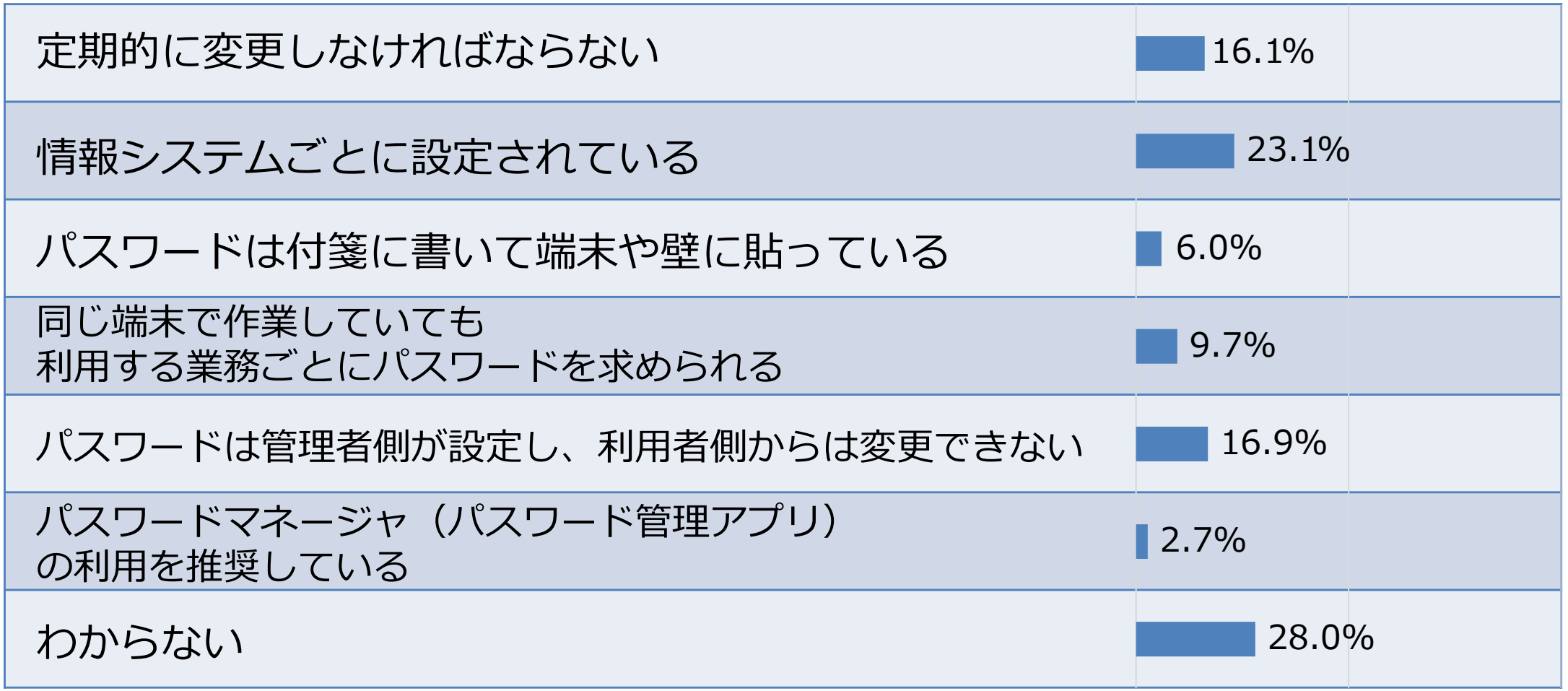
これでは、パスワードが役割を果たしているとは言えません。

実際に事件が起きていますので、見直しをお願いします。

サイバー防犯診断【アンケート結果から】

※%は小数点第一位まで表示（四捨五入）

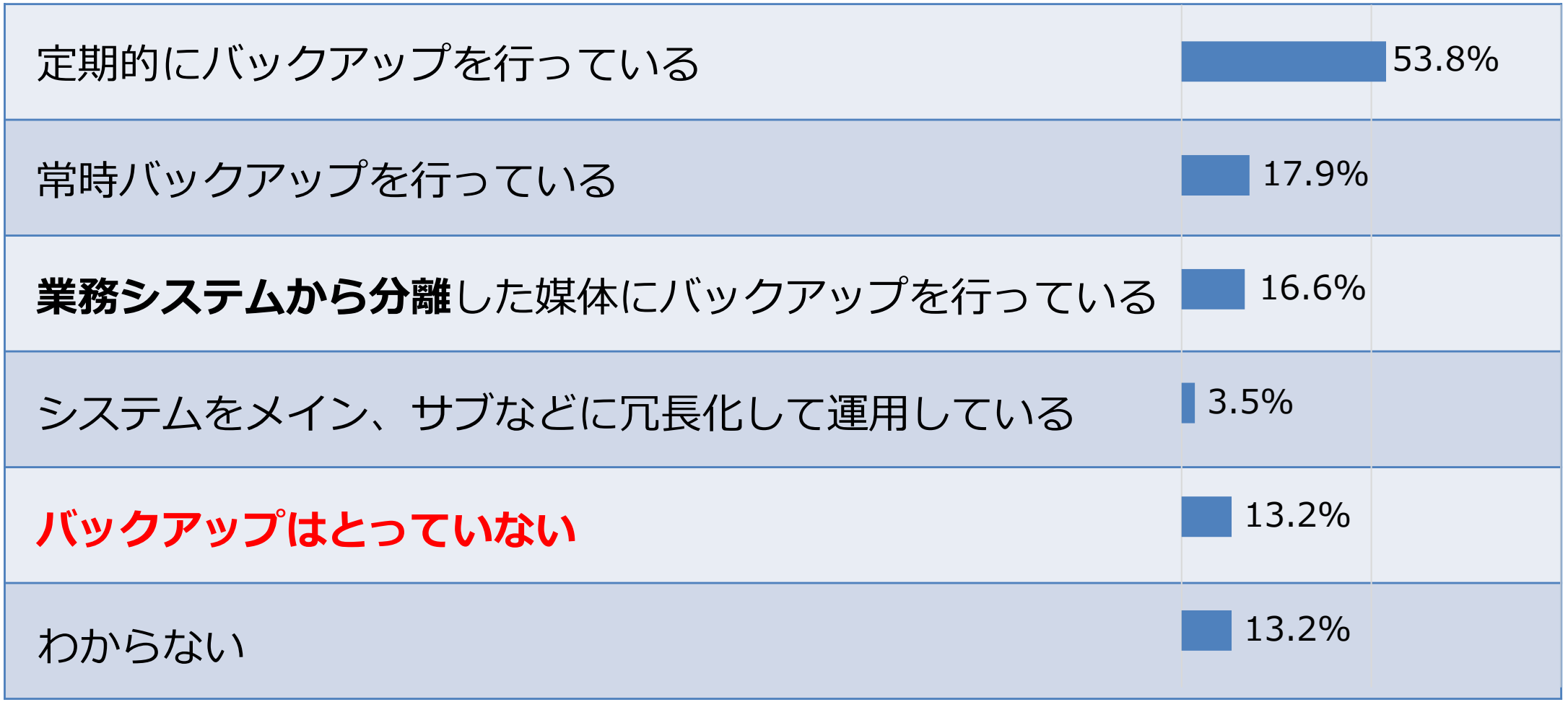
【パスワードの管理について】※該当項目チェック式（複数回答可）



サイバー防犯診断【アンケート結果から】

※%は小数点第一位まで表示（四捨五入）

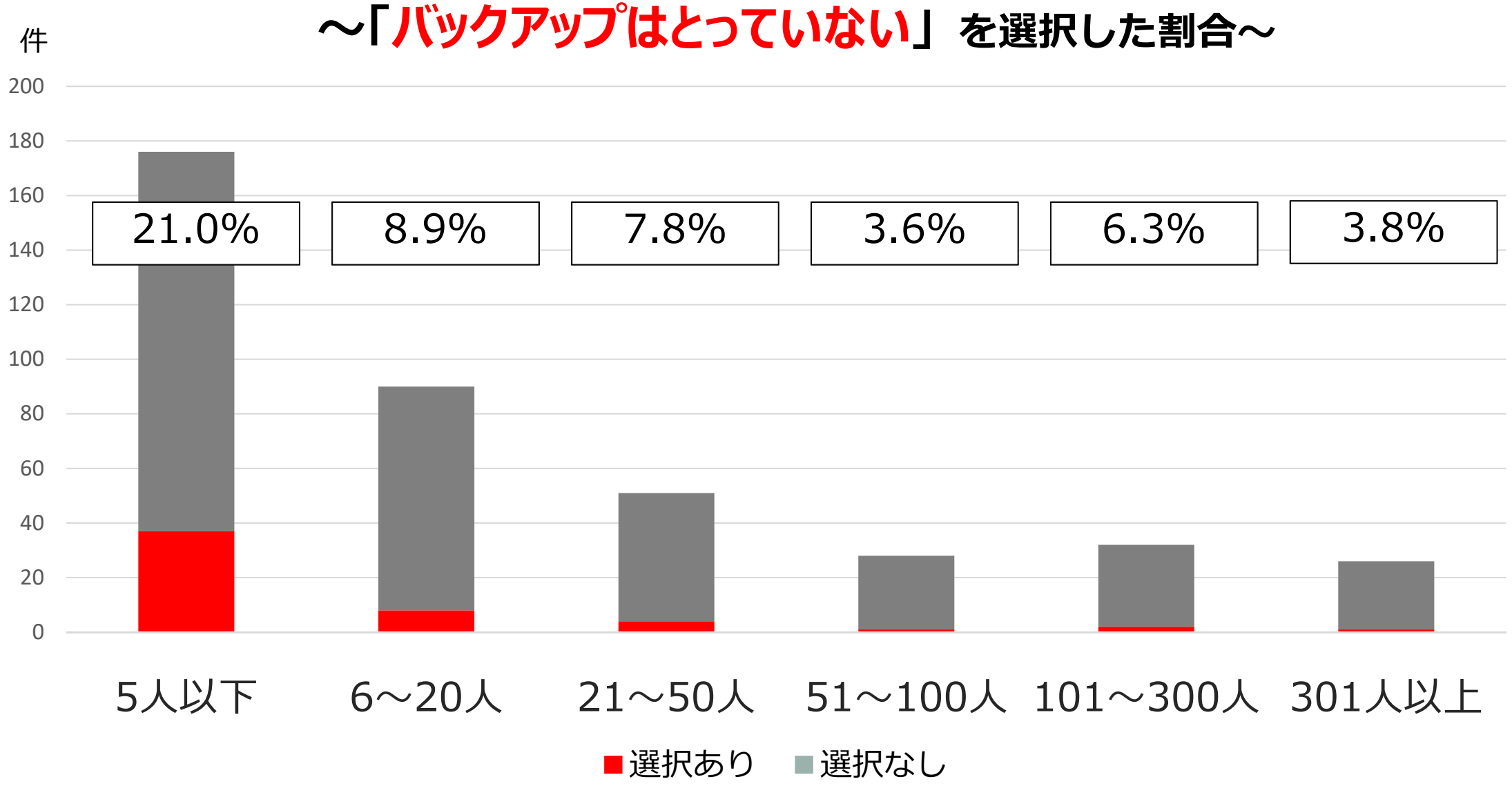
【データのバックアップについて】※該当項目チェック式（複数回答可）



サイバー防犯診断【アンケート結果から】

※%は小数点第一位まで表示（四捨五入）

【データのバックアップについて】　※事業規模別

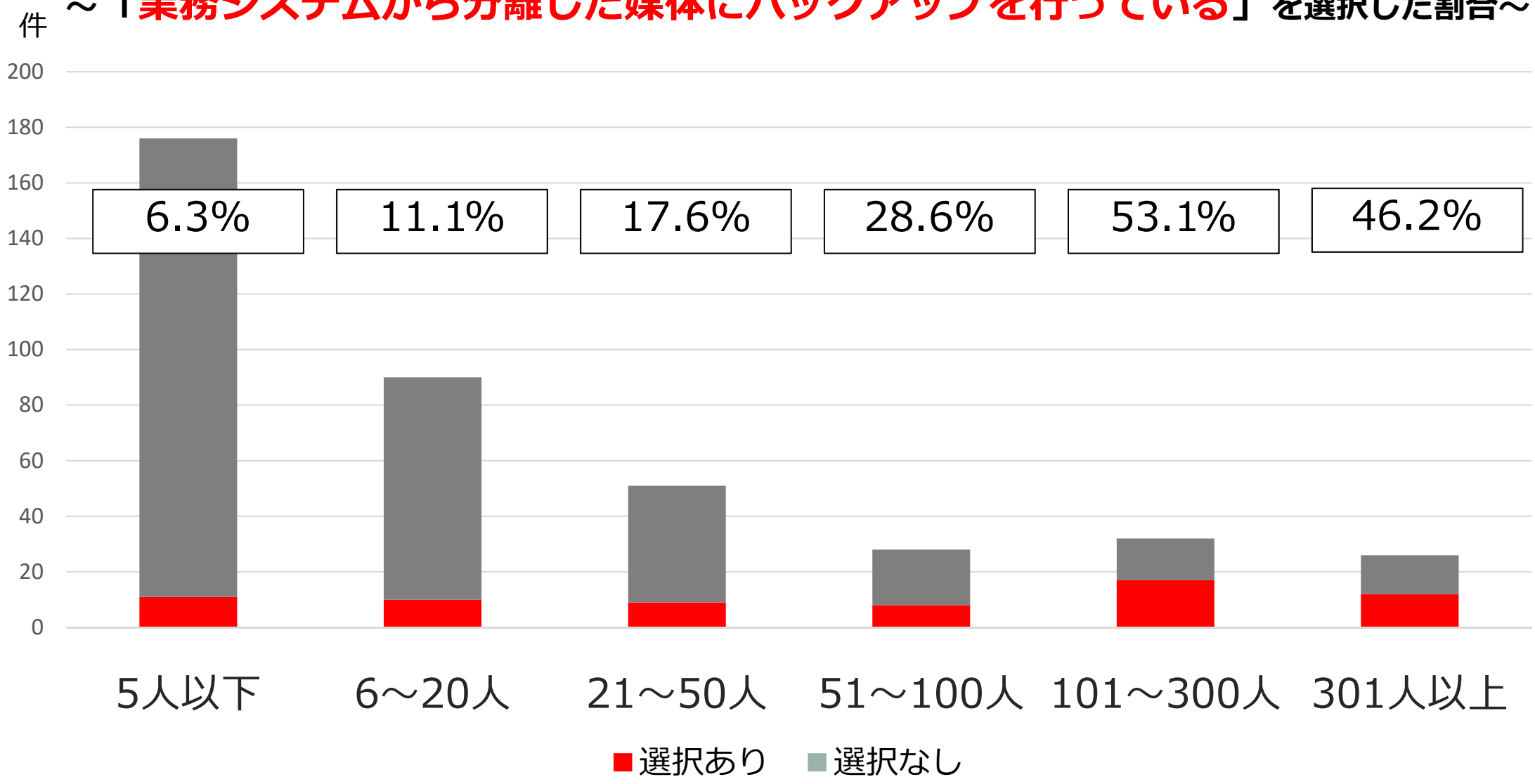


サイバー防犯診断【アンケート結果から】

※%は小数点第一位まで表示（四捨五入）

【データのバックアップについて】　※事業規模別

～「**業務システムから分離した媒体にバックアップを行っている**」**を選択した割合**～



サイバー防犯診断【アンケート結果から】

※%は小数点第一位まで表示（四捨五入）

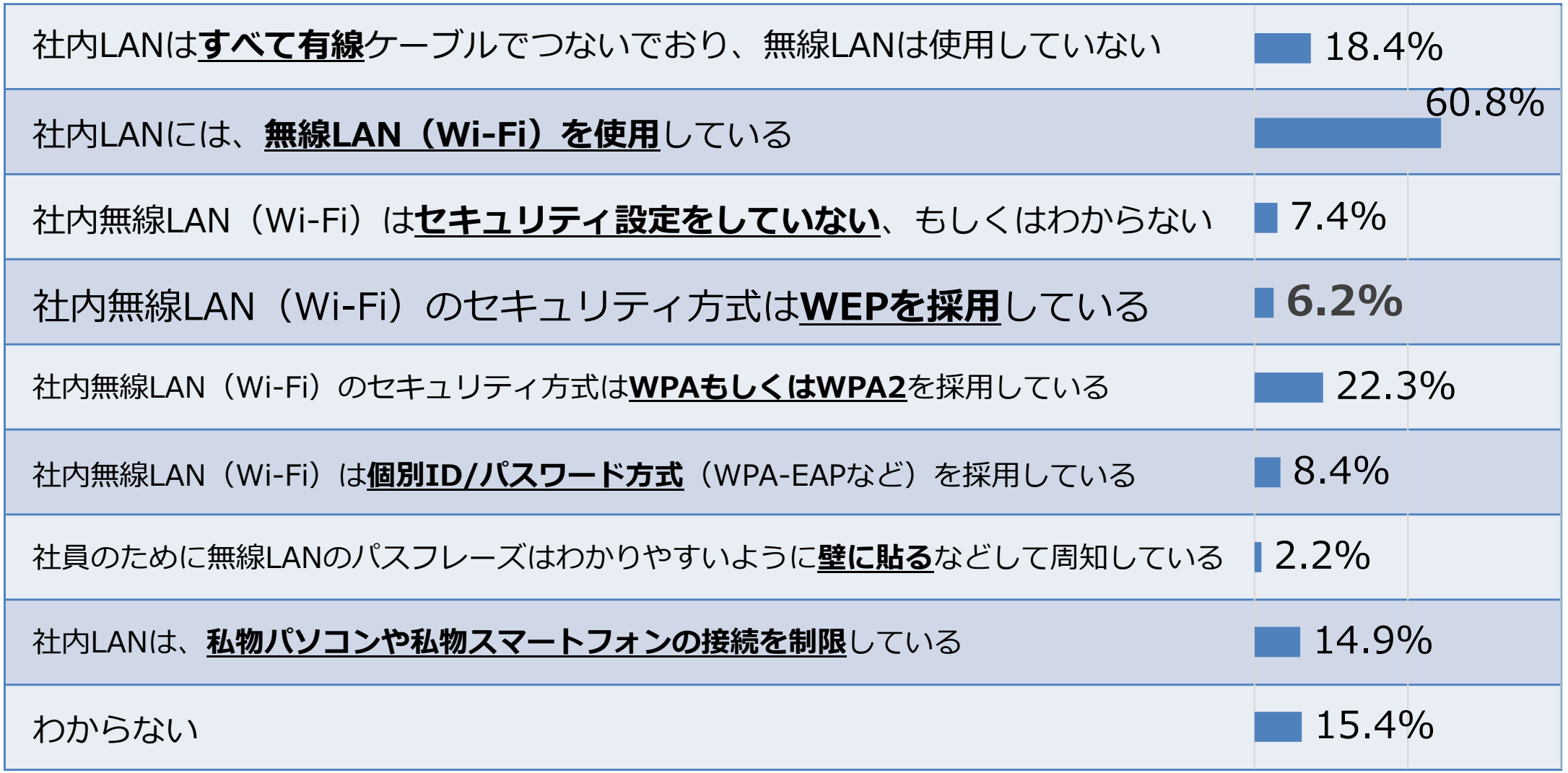
【端末のセキュリティ対策について】※該当項目チェック式（複数回答可）

出先では、私物のスマートフォンや私物のパソコンを使用している	37.2%
各パソコンの管理者アカウントは、通常業務には使用しない	12.9%
ソフトウェアのインストールに制限がかかっている	9.7%
役職や部署によって、アクセスできるファイルやフォルダが分けられている	23.1%
パソコンに接続できるUSBメモリなどの記録媒体を制限している	9.7%
データ等を社外に持ち出す際の許可を求めるルールを定めている	11.9%
業務利用する機器や媒体に管理番号を付けて一覧表を作成し、管理者と種類・数を明確化している	14.1%
媒体を持ち出す際には盗難や紛失の対策をしている	8.9%
関係者以外の事務所への立ち入りを制限している	23.3%
退社時にノートパソコンや備品を施錠補完するなど盗難対策をしている	8.4%
事務所が無人になる時の施錠忘れ対策をしている	25.1%
該当なし	23.6%

サイバー防犯診断【アンケート結果から】

※%は小数点第一位まで表示（四捨五入）

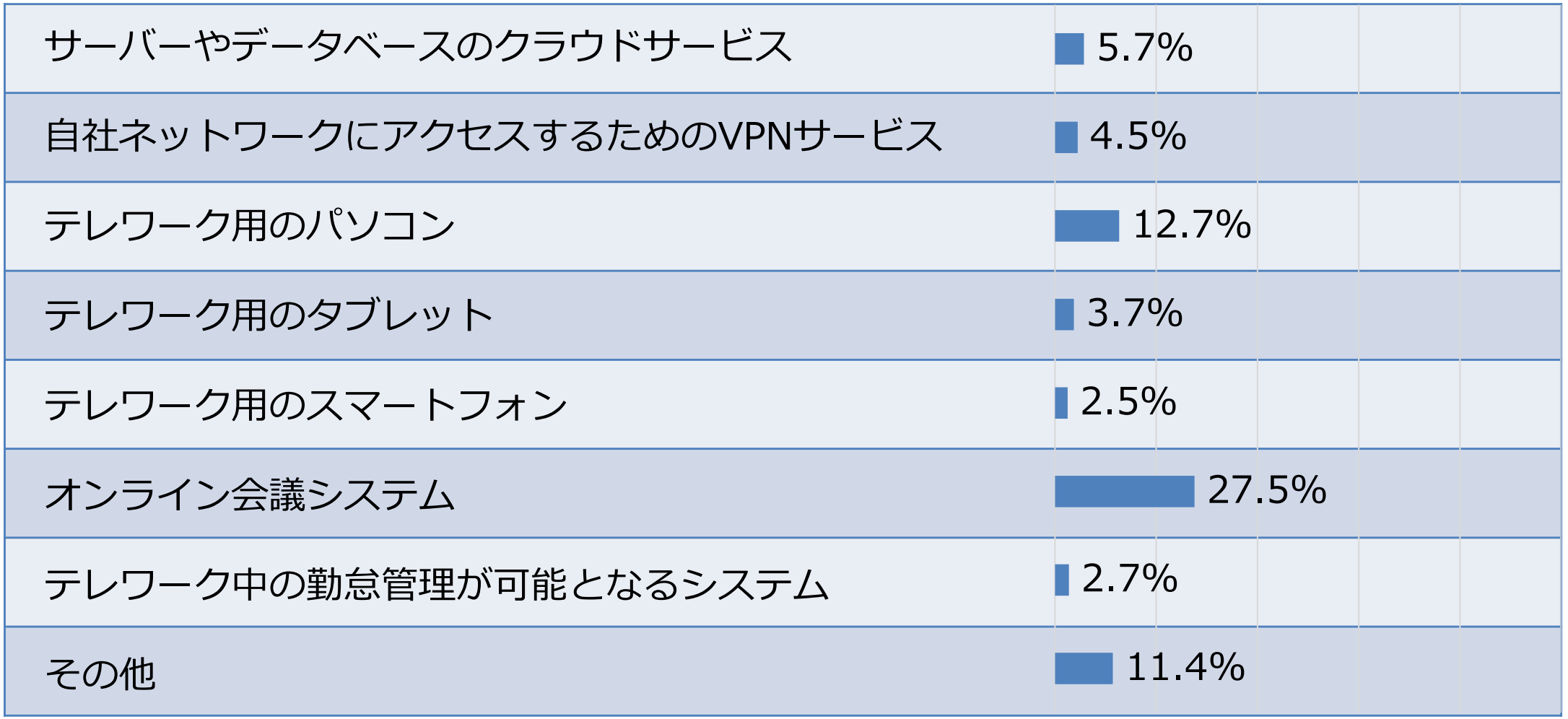
【社内無線LANについて】※該当項目チェック式（複数回答可）



サイバー防犯診断【アンケート結果から】

※%は小数点第一位まで表示（四捨五入）

【新型コロナウイルス感染症対策に際して導入したものについて】※該当項目チェック式（複数回答可）



サイバー防犯診断【アンケート結果から】

※%は小数点第一位まで表示（四捨五入）

【サイバー攻撃により生じた被害について（過去３年間）】 ※該当項目チェック式（複数回答可）

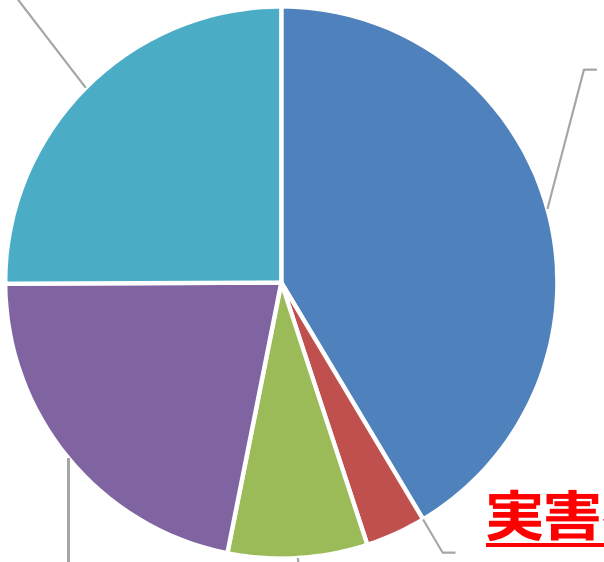
被害を受けたことはない	84.1%
業務データの損失	1.2%
システムの停止	1.2%
個人情報（顧客、従業員のもの等）の流出	1.0%
営業秘密、営業データ等の流出	0.0%
関連会社や取引先に攻撃メールが送られてしまった	1.7%
攻撃者に社内のデータを暗号化され、業務が停滞した	1.0%
攻撃者に社内のデータ復旧と引き換えに身代金を要求された	0.5%
自社のシステムが踏み台とされた	0.5%
Webサイトの改ざん	1.5%
業務システムの改ざん	0.0%
その他	4.5%

サイバー防犯診断【アンケート結果から】

※%は小数点第一位まで表示（四捨五入）

【マルウェアについて】

※小数点以下四捨五入
合計が100%にならないことがあります。



サイバー防犯診断【アンケート結果から】

※%は小数点第一位まで表示（四捨五入）

【メール攻撃について（過去３年間）】

※該当項目チェック式（複数回答可）

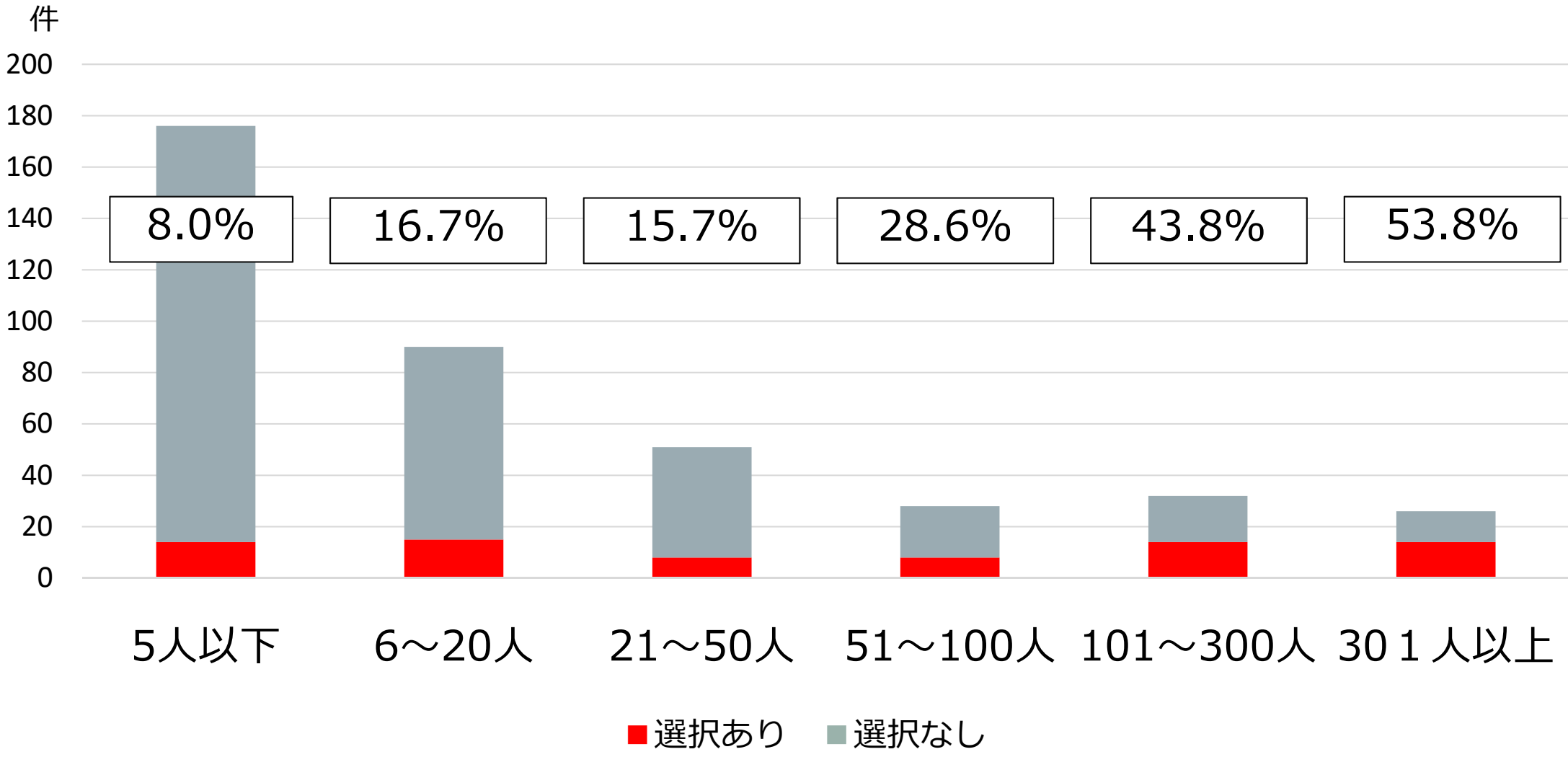
取引先や従業員を騙ったメール攻撃を受けたことがある	**18.1%**
社内や取引先から、自社からのメールがウイルスに感染しているなどと指摘された	**3.0%**
エモテットと思われる攻撃は受けたことがない	21.8%
社内でエモテットについての注意喚起があった	8.7%
社内の実態は把握していない	13.4%
エモテットについて聞いたことがあるがよく知らない	6.2%
エモテットについて聞いたことがない	**34.0%**
その他	1.5%

サイバー防犯診断【アンケート結果から】

※%は小数点第一位まで表示（四捨五入）

【メール攻撃について（過去３年間）】 ※事業規模別

～「**取引先や従業員を騙ったメール攻撃を受けたことがある**」**と回答した割合**～

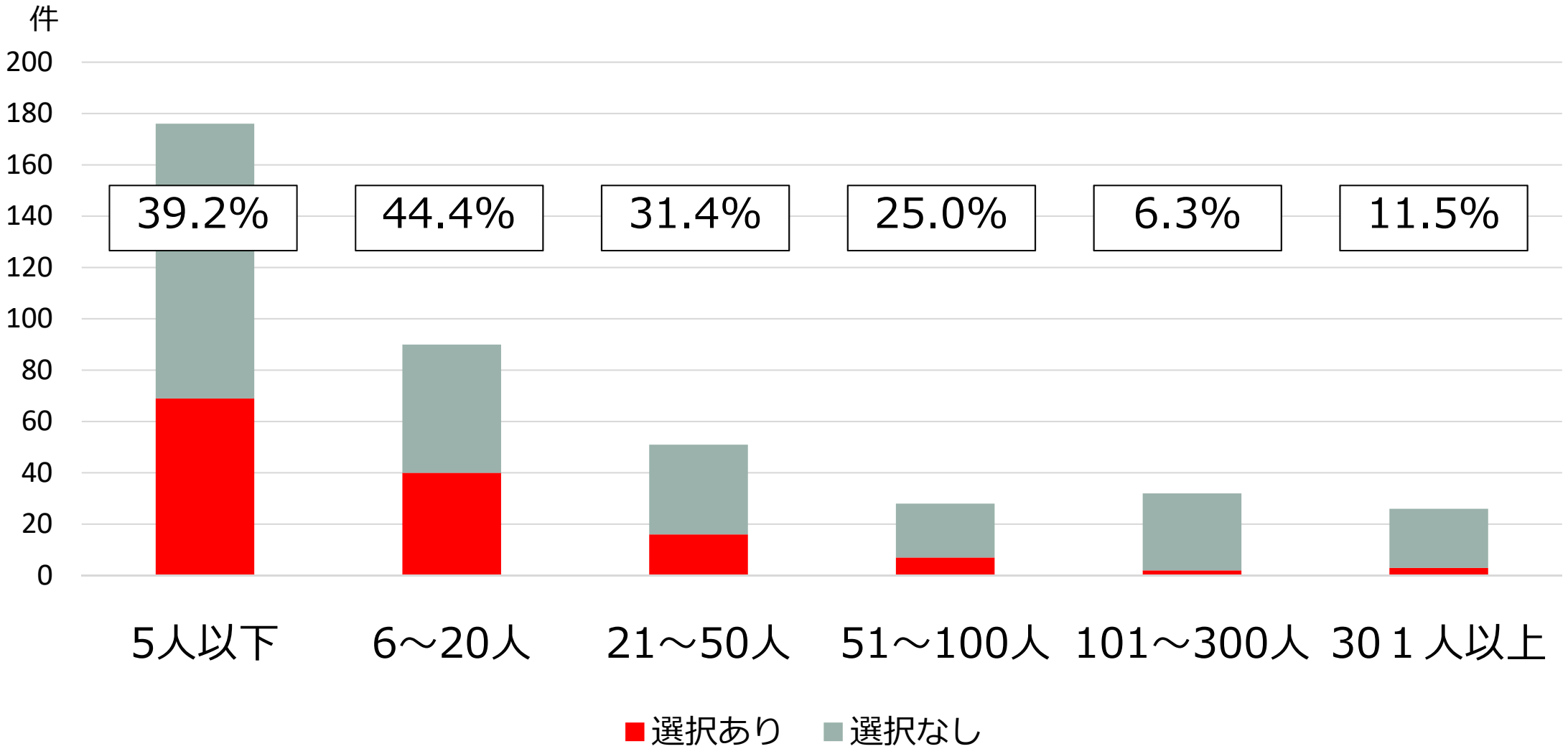


サイバー防犯診断【アンケート結果から】

※%は小数点第一位まで表示（四捨五入）

【メール攻撃について（過去３年間）】 ※事業規模別

～「**エモテットについて聞いたことがない**」と回答した割合～

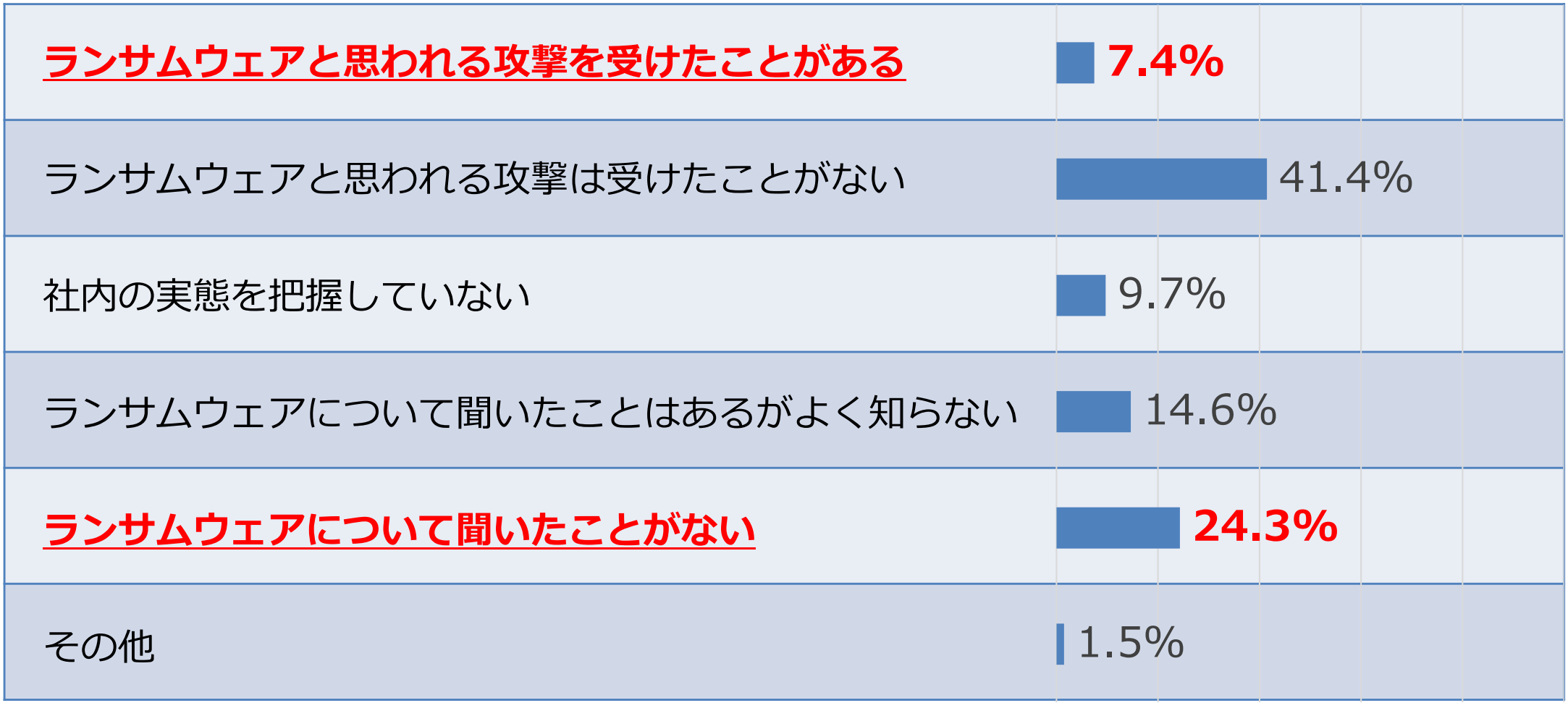


サイバー防犯診断【アンケート結果から】

※%は小数点第一位まで表示（四捨五入）

【ランサムウェアについて（過去３年間）】

※該当項目チェック式（複数回答可）

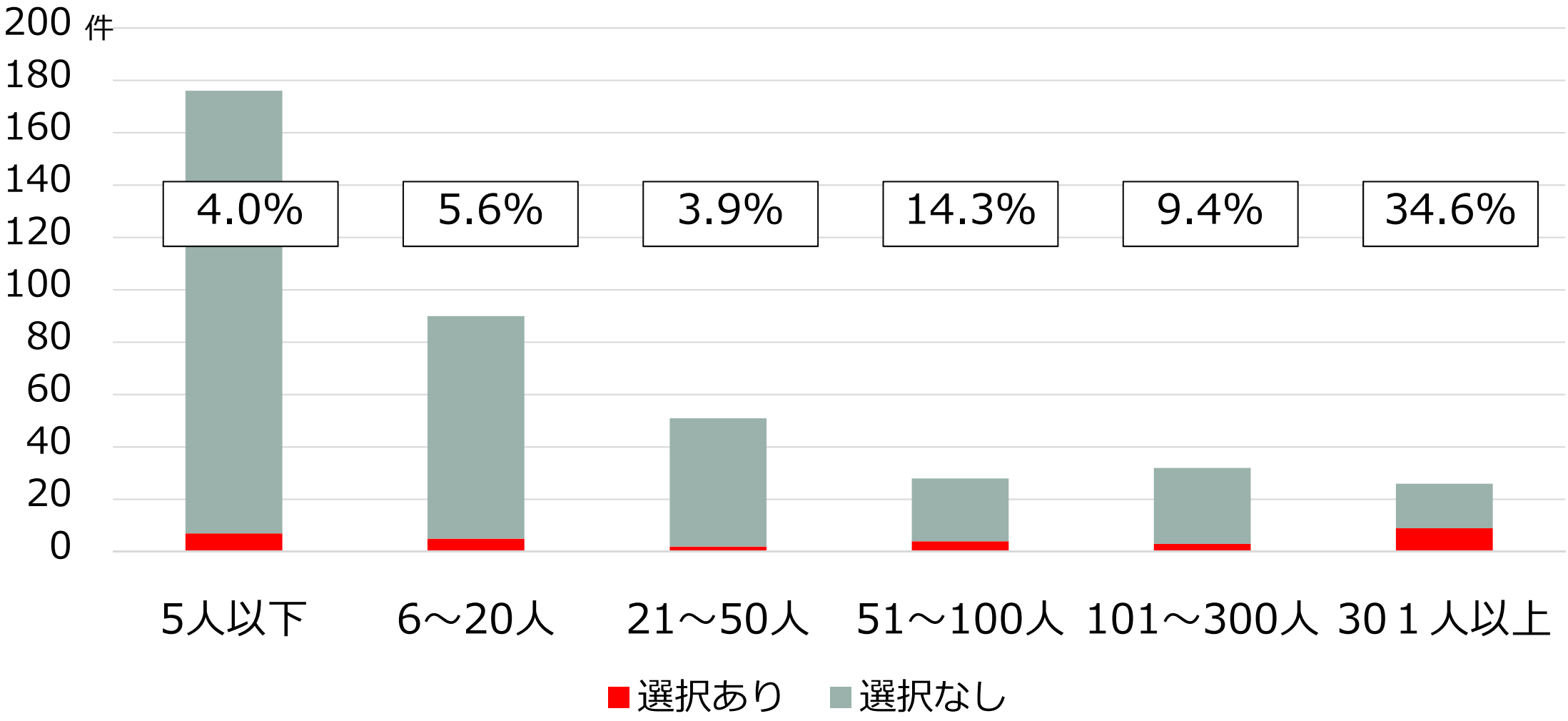


サイバー防犯診断【アンケート結果から】

※%は小数点第一位まで表示（四捨五入）

【ランサムウェアについて（過去３年間）】　※事業規模別

～「ランサムウェアと思われる攻撃を受けたことがある」と回答した割合～

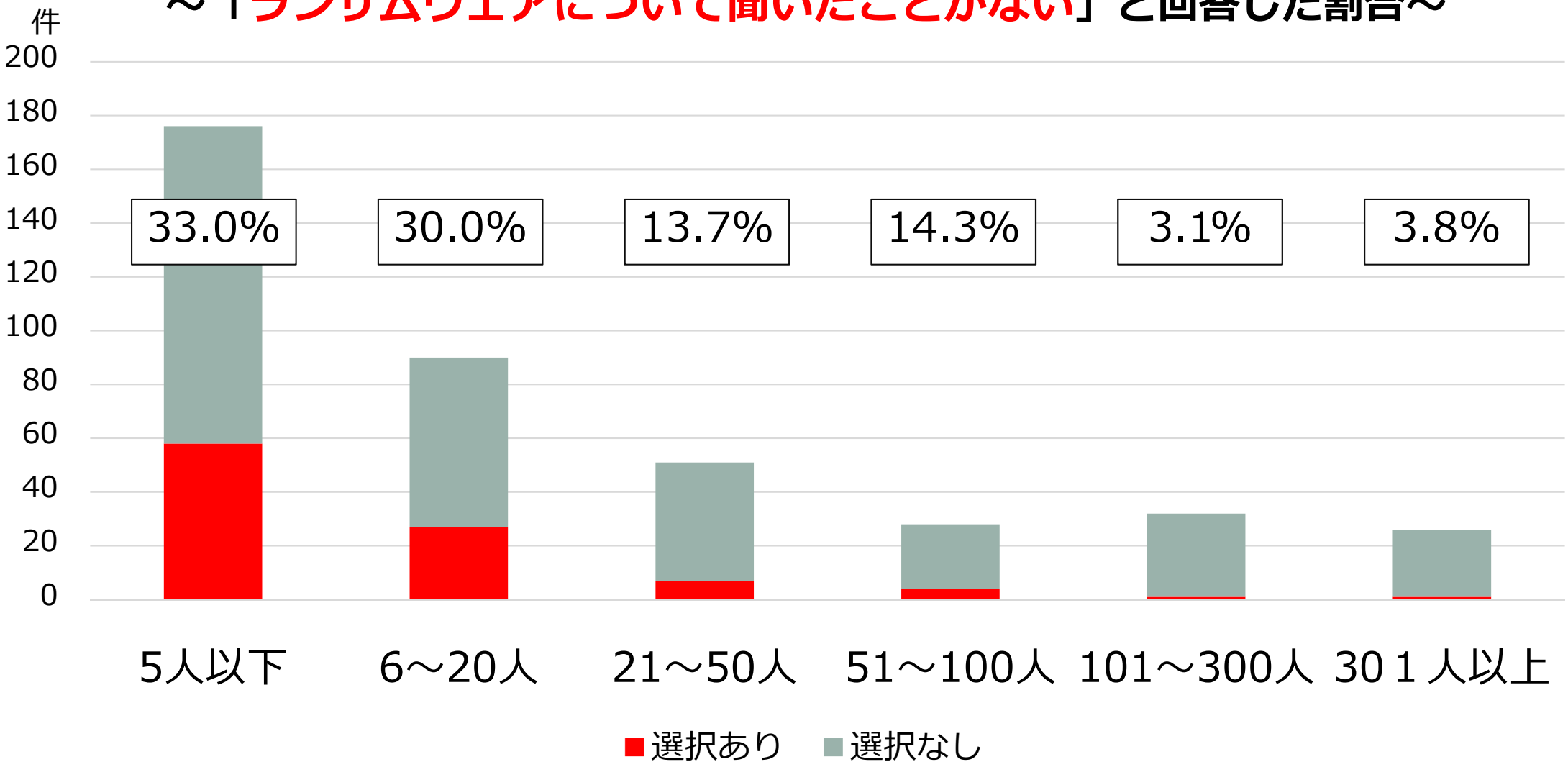


サイバー防犯診断【アンケート結果から】

※%は小数点第一位まで表示（四捨五入）

【ランサムウェアについて（過去３年間）】　※事業規模別

～「ランサムウェアについて聞いたことがない」と回答した割合～

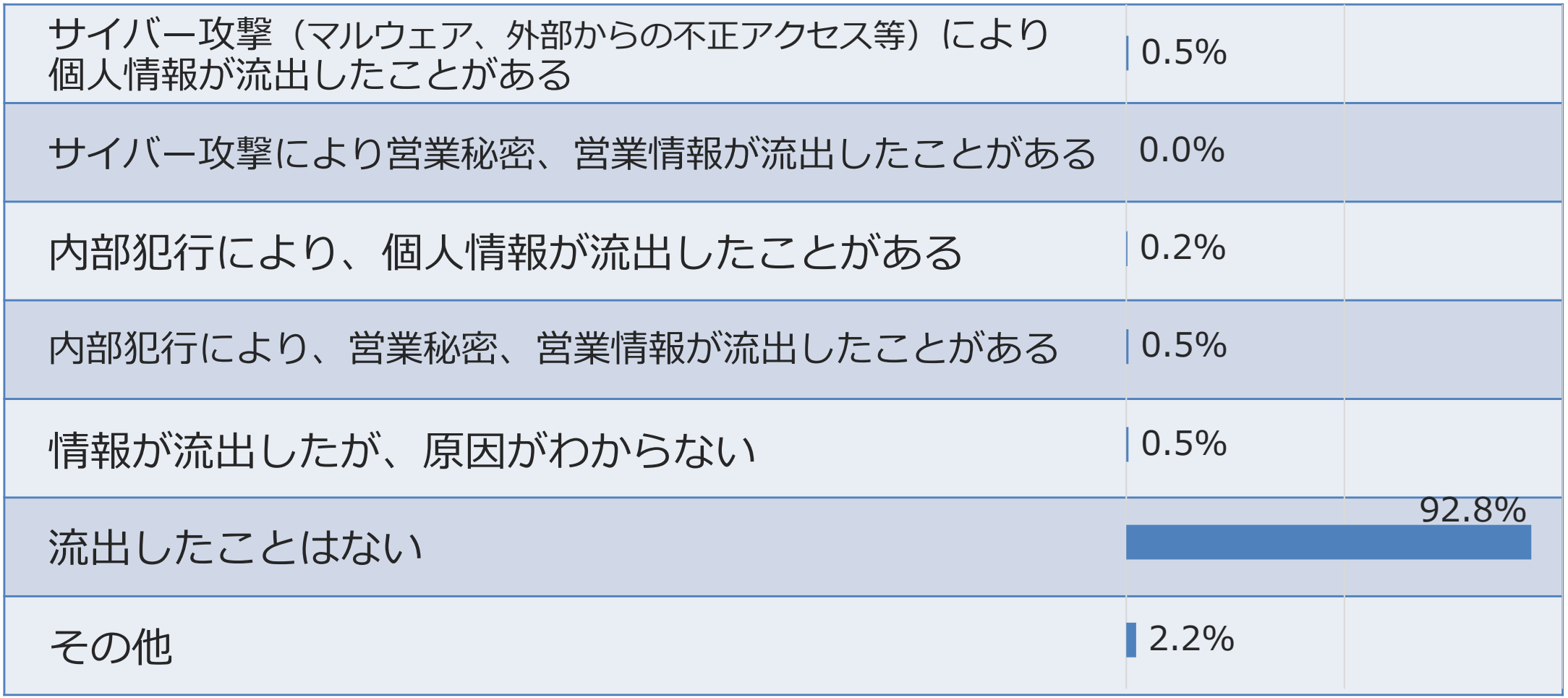


サイバー防犯診断【アンケート結果から】

※%は小数点第一位まで表示（四捨五入）

【情報流出について（過去３年間）】

※該当項目チェック式（複数回答可）

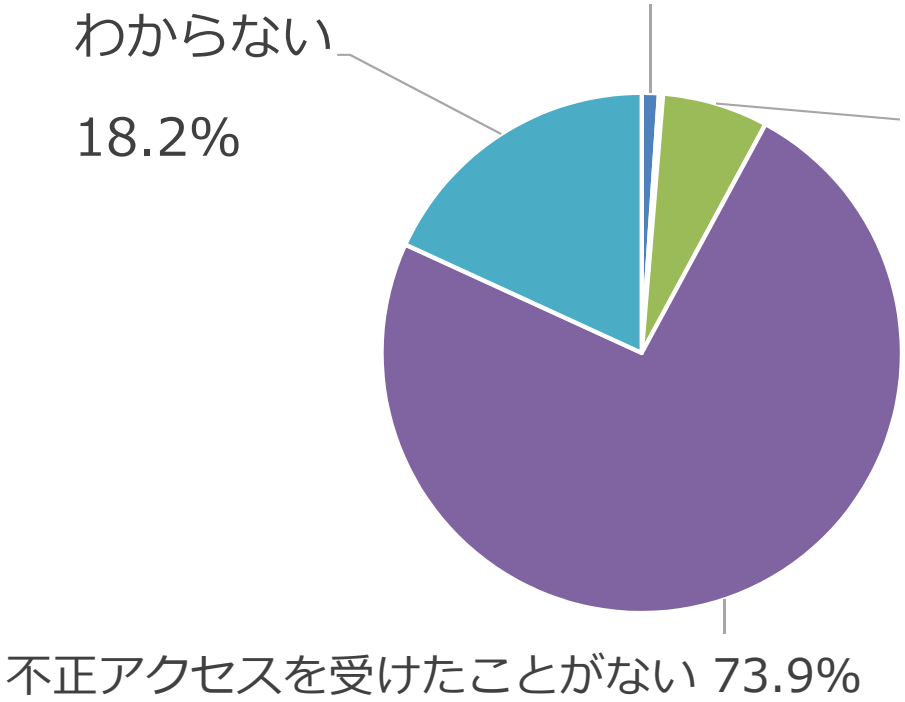


サイバー防犯診断【アンケート結果から】

※%は小数点第一位まで表示（四捨五入）

【不正アクセスについて（過去３年間）】

不正アクセスを受け、攻撃者等にシステムを不正利用された 1.1%



不正アクセスを受けた警告や痕跡はあったが、攻撃者等にシステムの不正利用が可能な状態とはならなかった **6.6%**

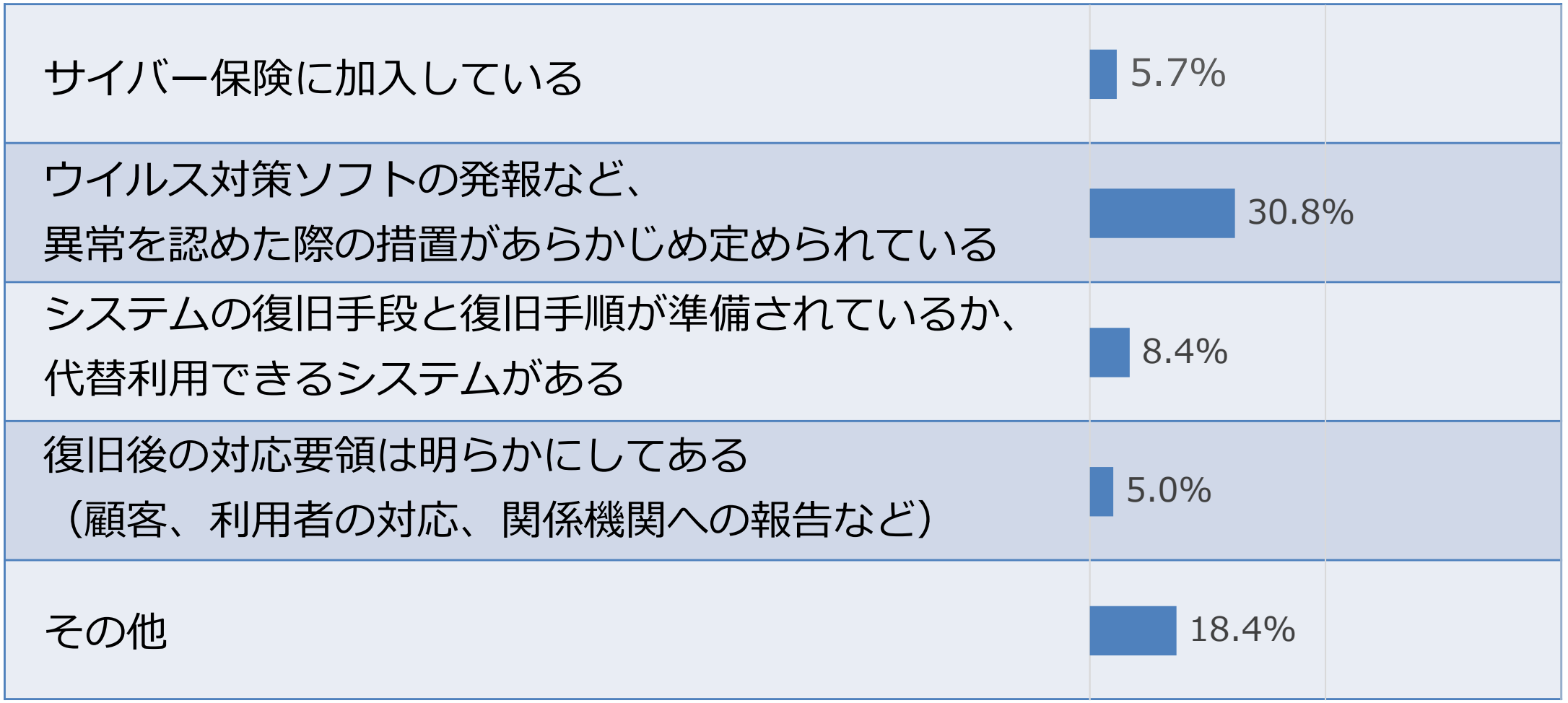
不正アクセスを受け、攻撃者等にシステムの不正利用が可能な状態となったが、不正利用されなかった 0.3%

- 不正アクセスを受け、攻撃者等にシステムを不正利用された
- 不正アクセスを受け、攻撃者等にシステムの不正利用が可能な状態となったが、不正利用されなかった
- 不正アクセスを受けた警告や痕跡はあったが、攻撃者等にシステムの不正利用が可能な状態とはならなかった

サイバー防犯診断【アンケート結果から】

※%は小数点第一位まで表示（四捨五入）

【サイバー攻撃被害発生時の対応準備について】 ※該当項目チェック式（複数回答可）

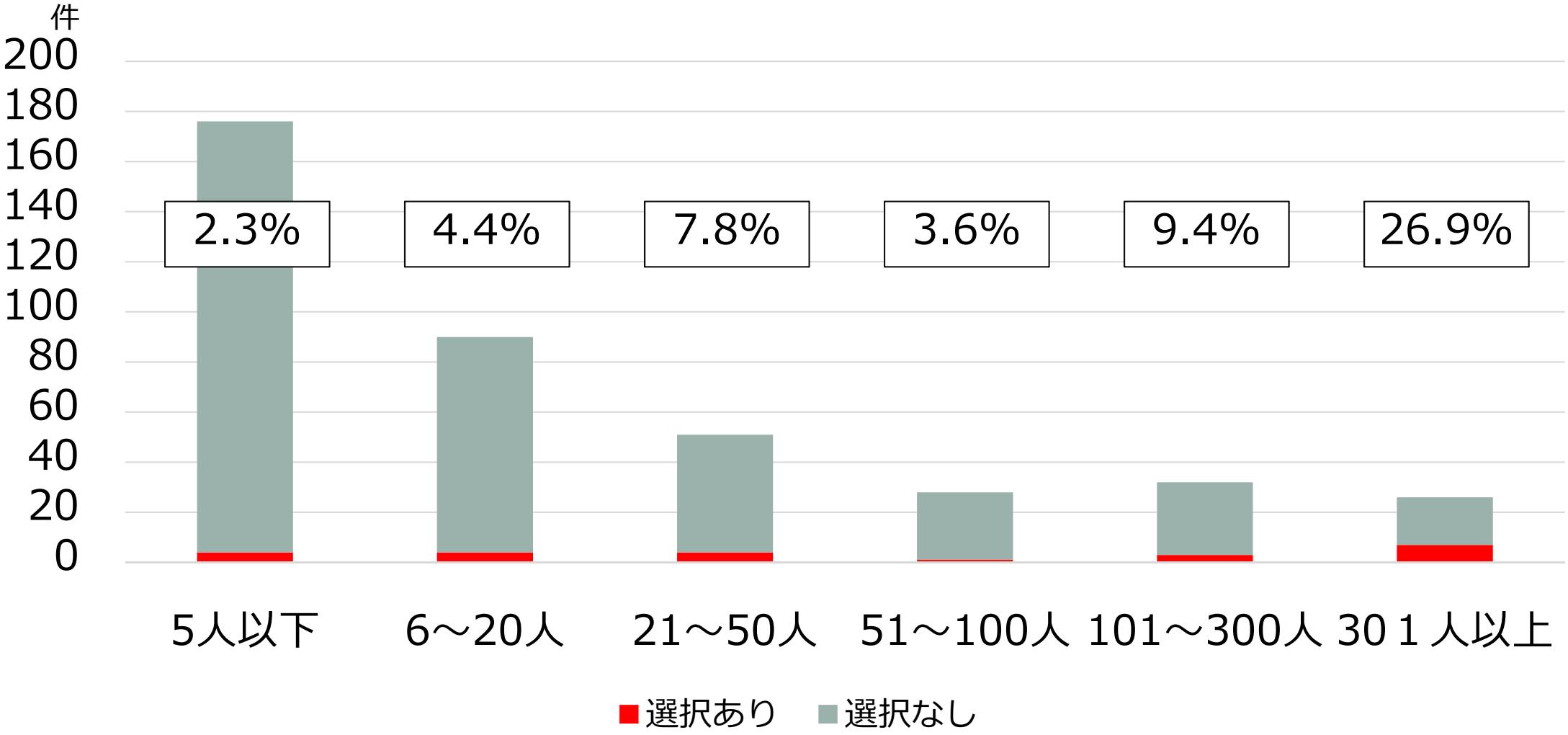


サイバー防犯診断【アンケート結果から】

※%は小数点第一位まで表示（四捨五入）

【サイバー攻撃被害発生時の対応準備について】※事業規模別

～「サイバー保険に加入している」と回答した割合～

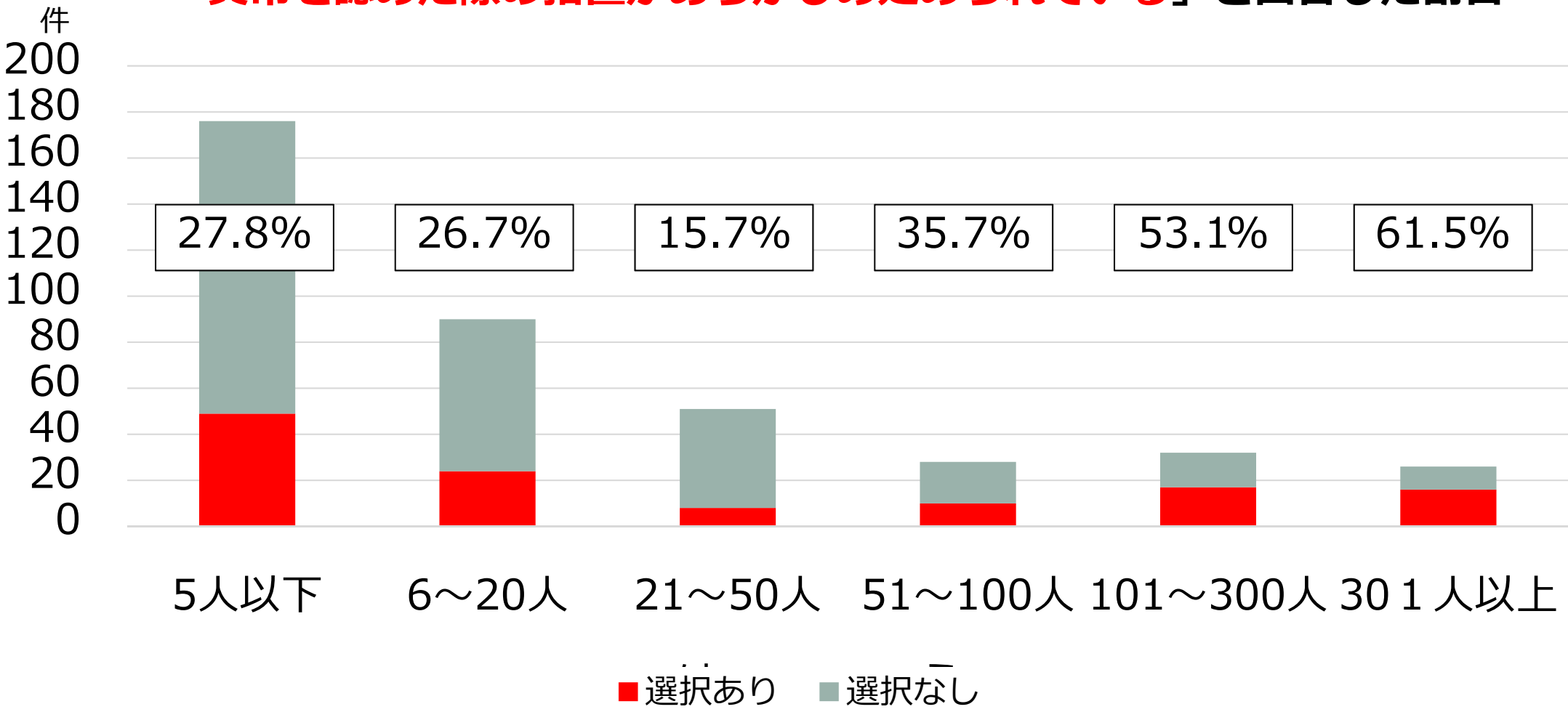


サイバー防犯診断【アンケート結果から】

※%は小数点第一位まで表示（四捨五入）

【サイバー攻撃被害発生時の対応準備について】※事業規模別

～「ウイルス対策ソフトの発報など、異常を認めた際の措置があらかじめ定められている」と回答した割合～

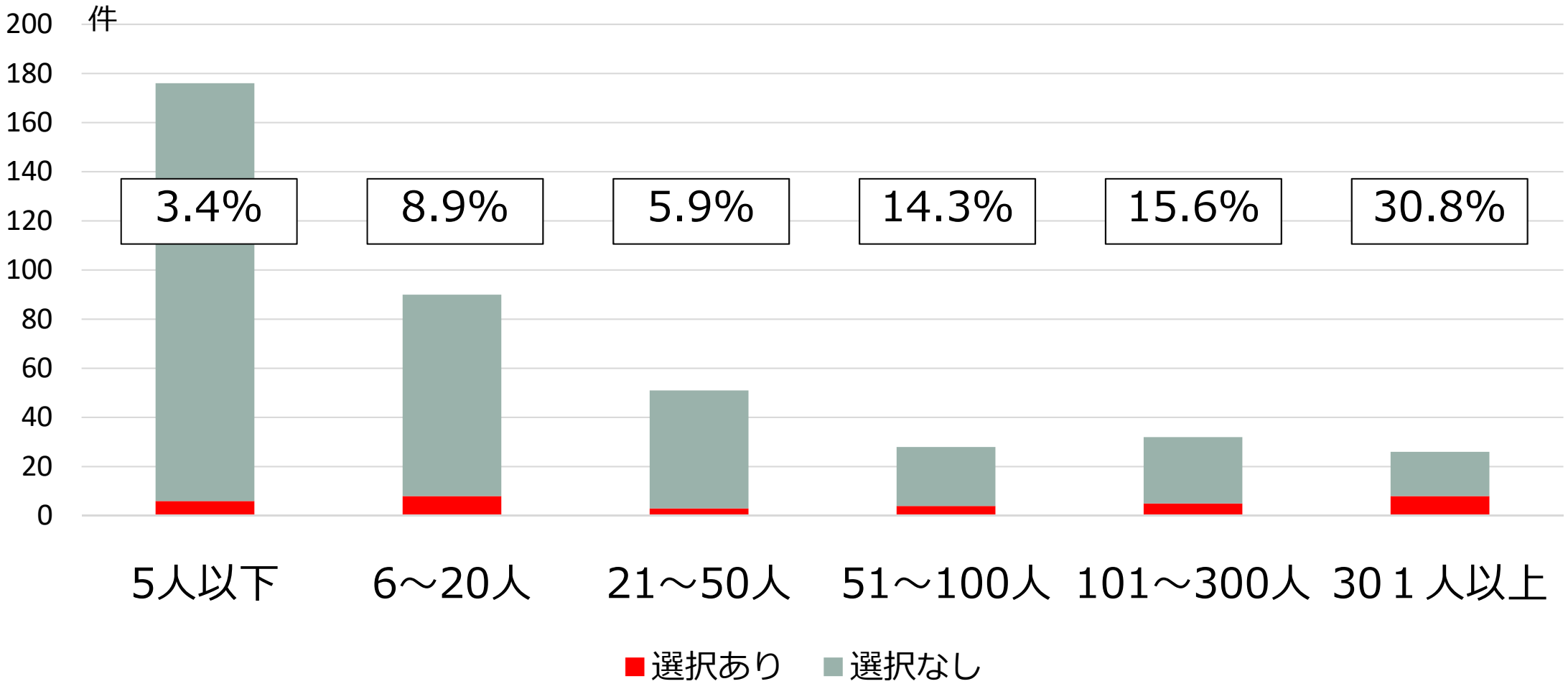


サイバー防犯診断【アンケート結果から】

※%は小数点第一位まで表示（四捨五入）

【サイバー攻撃被害発生時の対応準備について】※事業規模別

～「システムの復旧手段と復旧手順が準備されているか、代替利用できるシステムがある」と回答した割合～

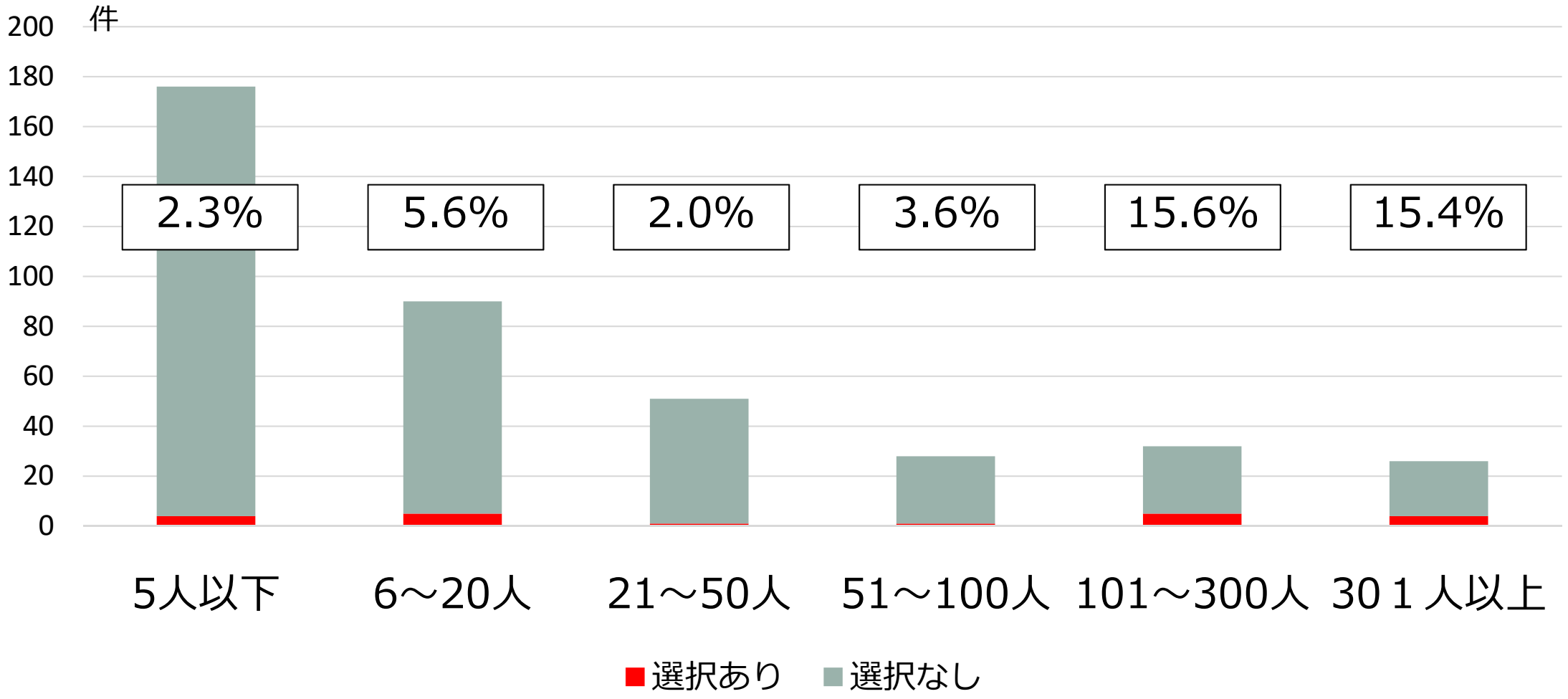


サイバー防犯診断【アンケート結果から】

※%は小数点第一位まで表示（四捨五入）

【サイバー攻撃被害発生時の対応準備について】※事業規模別

～「復旧後の対応要領は明らかにしてある」と回答した割合～

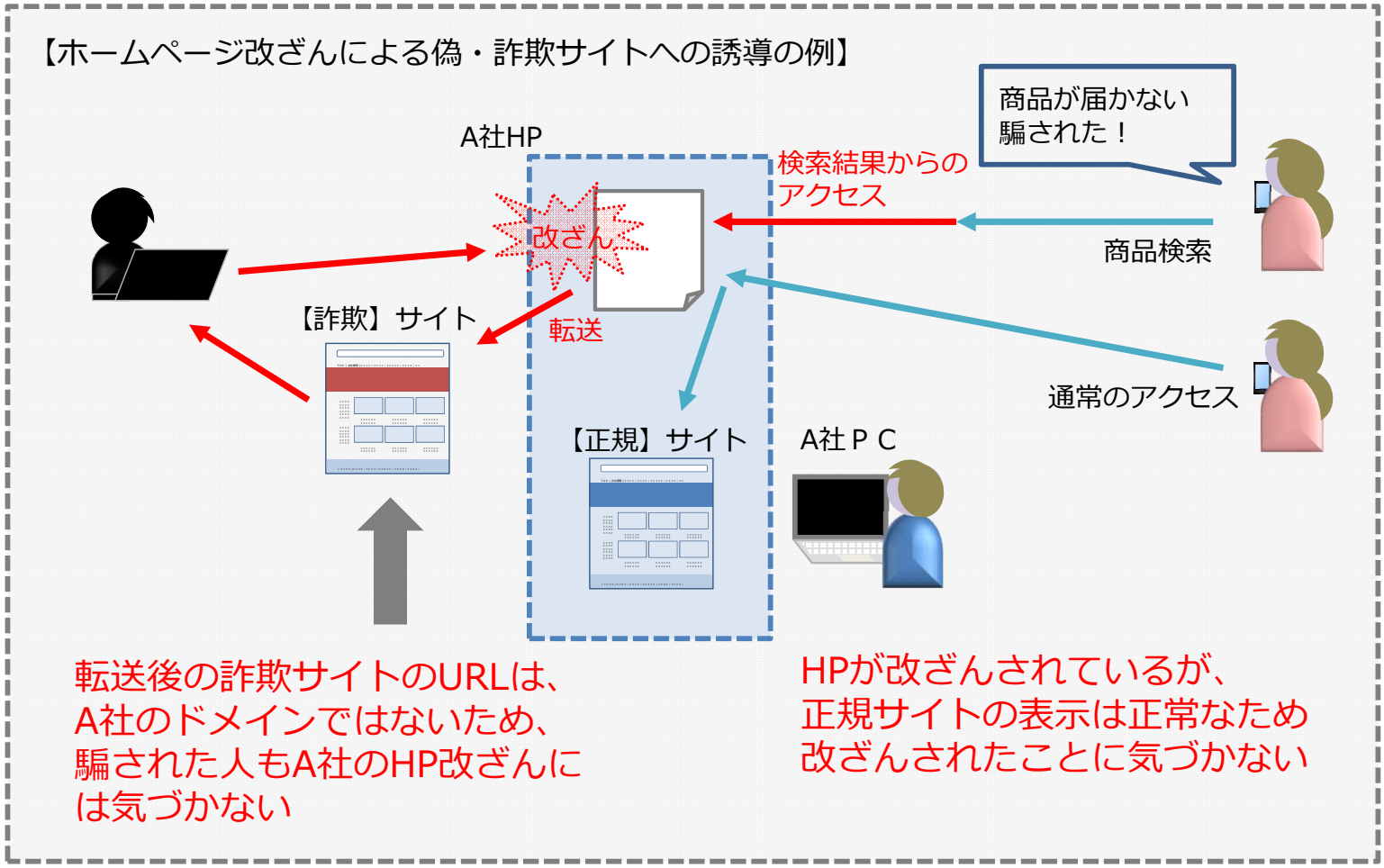


サイバー防犯診断【ホームページ調査から】

アンケートで希望した事業者のサイトを調査　　**121事業者のサイト**

サイバー防犯診断に参加した事業者のサイトのうち　**改ざんサイトを２件**　確認しました。

※本施策に伴い改ざんサイトの知見向上と詐欺サイトの調査を兼ね１０件の改ざんサイトを発見



改ざんの特徴のある事業者に連絡（委託先事業者含む）し、状況を説明して措置を依頼させていただきました。

ホームページは、作って終わりではなく、**保守管理が必須**となります。

ホームページ制作や管理を委託している場合は、委託先にソフトウェアの更新等の保守がなされているか確認を願います。

サイバー防犯診断【実地調査から】

※ 48 事業者を訪問

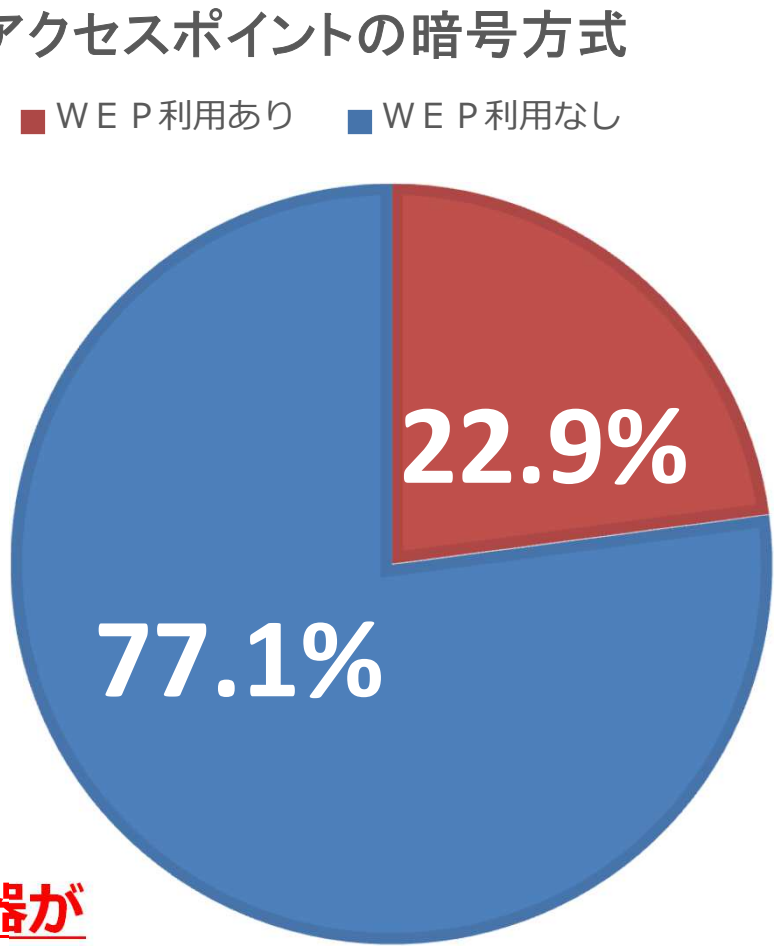
アンケートで希望をした事業者を実地調査

【不正プログラム調査】

警察で把握している特定の不正プログラムについて、
実地調査の際に可能な範囲で調査を実施しましたが、
結果、**調査したパソコンからは確認されませんでした。**

【アクセスポイント調査】

２割以上の事業者が　　アンケートでは**6.2%**
脆弱性が指摘されている古い暗号方式である
ＷＥＰ方式を利用していることを確認しました。



※未把握の機器や、使用を中止しているつもりの機器が稼働していた事例が多いため、社内の実態把握に努めてください。

特に機器の脆弱性対応では、このような機器がないか注意してください。