「令和 2 年度中小企業サイバーセキュリティ対策促進事業
（関西サイバーセキュリティ促進強化事業）」
関西におけるサイバーセキュリティ対策の実態把握（アンケート調査結果）

調査概要

主催：経済産業省近畿経済産業局（事務局　一般財団法人関西情報センター）

調査目的：近畿圏における中小企業を中心としたサイバーセキュリティの取り組みの現状やサイバー攻撃の被害状況等についての実態の把握、またテレワークの実施状況やそのセキュリティ対策の実態を把握し、経済産業省近畿経済産業局において今後のサイバーセキュリティ施策を展開するための基礎資料とする。

調査期間：2020 年 10 月中旬～11 月 13 日

調査方法：Web フォームによる回答（設問数 24 問）

調査対象：近畿 2 府 5 県（福井県、滋賀県、京都府、大阪府、兵庫県、奈良県、和歌山県）に本社をおく、下記条件に該当する企業
- 「製造業、情報通信業、運輸業の従業員 5 名以上」
- 「卸売業・小売業の従業員 10 名以上」

調査数：10,000 社（企業情報データベースから無作為抽出）

回答数：1,522 件（回収率 15.2%）

調査結果のポイント

1．サイバーセキュリティ対策の取組状況

- **サイバーセキュリティ対策の実施企業は 8 割以上に達する一方、未実施企業が 1 割程度存在。サイバーセキュリティ対策を実施しない理由として、自社でそれほど重要な情報を取り扱っていない点を挙げる企業の割合が最多（約 4 割）。次いで、予算の確保ができない、実施方法がわからないと回答する企業が多い。**
- **取り組み割合が高い対策は、アンチウイルスソフトの導入（約 9 割）、次いでファイアウォールや侵入検知システム（IDS）の導入（約 7 割）である。**

2．サイバー攻撃の被害状況とサイバーリスクに対する意識

- **これまで受けたサイバー攻撃の手口として、「ウイルス添付メールの受信」が最多（約 7 割）。次いで、「ビジネスメール詐欺」「標的型メール攻撃」である。**
- **実際に業務への影響を受けた手口についても、「ウイルス添付メールの受信」が最多（約 4 割）。次いで、「標的型メール攻撃」「ビジネスメール詐欺」である。**
- **サイバーセキュリティ対策を必要と考えるものの、極力コストをかけず対応している企業の割合が最多（約 6 割）。また、最低限のセキュリティ対策を施しておれば十分であると考える企業も約 2 割に達する。**

３．テレワーク実施時におけるサイバーセキュリティ対策

・テレワークの実施歴がある企業は約 4 割。特に新型コロナウイルス感染拡大により急遽制度化した企業が約 3 割を占める。実施にあたって導入を行ったセキュリティ対策として、アンチウイルスソフトの導入、VPN 導入が挙げられる。

・実施に当たっての課題として、実施部門が限定されてしまうことがおよそ過半数を占める。また、IT インフラやアプリケーションの未整備、就業規則や IT 規則の未対応を挙げる割合が高い。

４．サイバーセキュリティ対策の実施体制

・専門部署や専門人員を置かず、兼務でサイバーセキュリティ対策に取り組む企業が最多（約 6 割）。

・従業員に対するサイバーセキュリティ教育の実施状況についても、未実施が最多（約 6 割）である。

５．サイバーセキュリティ対策に関する要望等

・サイバー攻撃に関する最新動向・事例へのニーズが高く、情報提供の拡充が求められる。また、地域セキュリティコミュニティの認知度は 1 割に満たない状況である。

設問ごとの結果

１．サイバーセキュリティ対策の取組状況

・「サイバーセキュリティ対策を実施している」が 82.4%と多数だが、一方で、「サイバーセキュリティ対策を行っていない」企業が 11.5%と一定程度存在することが明らかとなった。

・サイバーセキュリティ対策を行っていない理由として、「自社ではそれほど重要な情報を取り扱っていないため」が 36.0%、「セキュリティ対策の予算を確保できないため」が 20.6%、「セキュリティ対策を実施する方法がわからないため」が 20.0%、「セキュリティ対策を実施する人材が不足しているため」が 18.9%となっている。

・アンチウイルスソフトの導入割合は 93.7%であり、回答企業の殆どで導入が行われていることがわかる。次いで導入割合が高いのは、ファイアウォールや侵入検知システム（IDS）の導入であり、導入割合は 68.9%に達する。

・サイバーセキュリティ対策の実施状況について、「これまでは順調に進んできたが、これからはやや不安である」が 40.1%と最多であり、「現在順調に進んでおり、今後も引き続き問題はない」が 35.4%を占めている。

・サイバーセキュリティ対策の結果、得られた効果として、「目に見える効果は実感できていない、わからない」が 63.6%であり、次いで「従業員のセキュリティ意識が高まり、サイバー攻撃を未然に防げている」が 48.6%となっている。

・サイバーセキュリティ対策を推進する上での課題として、「サイバーセキュリティ担当人材が不足している」が 53.0%と約半数を占めており、次いで、「サイバーセキュリティリスクの見える化が困難である」が 37.2%、「従業員に向けたサイバーセキュリティ教育が十分に行われていない」が 32.1%となっている。
・サイバーセキュリティ対策を推進する上での相談先として、「システムインテグレータ、システムベンダ」が 41.8%と最多であり、次いで「セキュリティベンダ」が 30.1%であった。

２．サイバー攻撃の被害状況とサイバーリスクに対する意識

・これまで受けたサイバー攻撃の手口として、「ウイルス添付メールの受信」が 65.6%で 1 位、「ビジネスメール詐欺」が 27.7%で 2 位、「標的型メール攻撃」が 22.3%で 3 位であった。
・また、これまで受けたサイバー攻撃のうち、業務への影響を受けた手口は、「ウイルス添付メールの受信」が 37.2%で 1 位、「標的型メール攻撃」が 9.9%で 2 位、「ビジネスメール詐欺」が 6.7%で 3 位であった。
・自社におけるサイバーセキュリティ対策の取り組みの位置づけとして、「自社のビジネスやブランドを守るために必要であるが、極力コストをかけず対応している」企業が 58.3%と最多であった。なお、「自社ではそれほど重要な情報を取り扱っておらず、最低限のセキュリティ対策を施しておれば十分である」と考える企業が 18.0%と一定程度存在している。
・自社でサイバーセキュリティ対策が大きく進む契機となると想定される事象は、1 位が「顧客や取引先、親会社等からセキュリティ対策状況を問われたり、義務付けられたりする」(23.7%)、2 位が「法制度が変わり、企業のセキュリティ対策実施が義務付けられる」（22.2%）であった。

３．テレワーク実施時におけるサイバーセキュリティ対策

・これまでにテレワークの実施歴がある企業は 43.5%、実施歴のない企業は 56.5%であった。なお、テレワークの実施歴がある企業のうち、新型コロナウイルス感染拡大以前より制度を設けている企業は 9.8%、新型コロナウイルス感染拡大により急遽制度化した企業は 33.7%であった。
・テレワークを実施するに当たって導入を行ったセキュリティ対策として、「あてはまるものはない、わからない」が 51.3%とおよそ過半数を占めた。次いで、「テレワーク端末にアンチウイルスソフトをインストールし、最新の定義ファイルが適用される状態にする」が 30.0%、「インターネット経路での情報漏えいを防止するため、VPN を導入している」が 25.7%を占めた。
・テレワークを実施するに当たっての課題として、「テレワークを実施できる部門・業務が

限られている」が 55.3%とおよそ過半数を占めている。また、「テレワーク実施のための IT インフラやアプリケーションが不十分である」が 28.3%、「就業規則や IT 規則がテレワーク実施に対応していない」が 26.7%となっている。

４．サイバーセキュリティ対策の実施体制

・自社におけるサイバーセキュリティ対策の実施体制として、「セキュリティ専任の担当者はおらず、兼務で従事している」が 60.5%と大半を占めている。次いで、「セキュリティ担当者はいない、わからない」が 29.6%、「セキュリティ専門部署（担当者）を設置している」が 7.3%であり、専任者の人数は 1 名が 39.6%、2 名が 23.4%であった。

・従業員に向けたサイバーセキュリティ教育の実施状況については、「あてはまるものはない、わからない」（未実施）が 64.5%と大半を占めており、次いで「従業員（セキュリティ担当者等）を講師として、すべての従業員を対象として実施している」が 12.6%、「従業員（セキュリティ担当者等）を講師として、一部の従業員を対象として実施している」が 10.4%であった。

・自社におけるセキュリティ関連資格の取得状況については、「いずれも取得していない/わからない」が 90.5%と大半を占めている。各資格の取得状況については、プライバシーマーク（P マーク）が 4.4%、セキュリティアクション（SECURITY ACTION）が 3.0%、ISMS 認証が 2.5%、情報処理安全確保支援士（登録セキスペ）が 1.5%であった。

５．サイバーセキュリティ対策に関する要望等

・サイバーセキュリティ対策に対する要望は、「サイバー攻撃に関する最新の手口や具体的な事件・事故事例に関する情報を知りたい」が 44.8%、「特に要望はない」が 32.0%、「サイバー攻撃に関する技術的な情報を知りたい」が 29.0%であった。

・国や地方自治体等、公的支援機関に期待する役割は「情報提供（リスク情報、対策情報の発信など）」が 60.0%、次いで「金融支援（補助金、助成金の導入など）」は 58.3%であった。

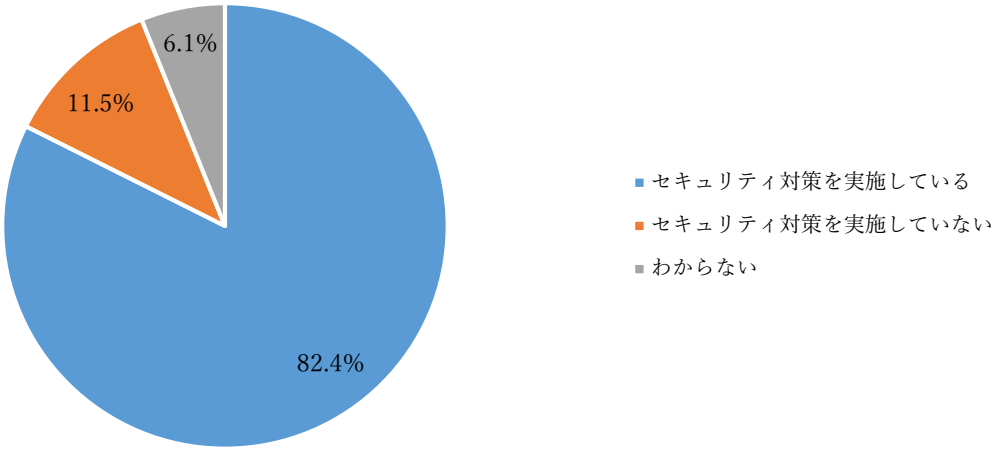
・地域セキュリティコミュニティの認知度は 6.3%と 1 割に満たず、実際に活動に参画している企業は 0.8%に過ぎない結果となった。また、参画コミュニティとして、「CSIRT 協議会」、「関西サイバーセキュリティ・ネットワーク」等が挙げられている。

（※地域セキュリティコミュニティ：サイバーセキュリティ関連の教育・普及・啓発や各種勉強会・研修会、地域での人的・組織的ネットワーク拡大に資する活動、市場開拓や受注促進活動などを目的に、地域の企業が参画して自主的に取り組んでいるコミュニティ活動）

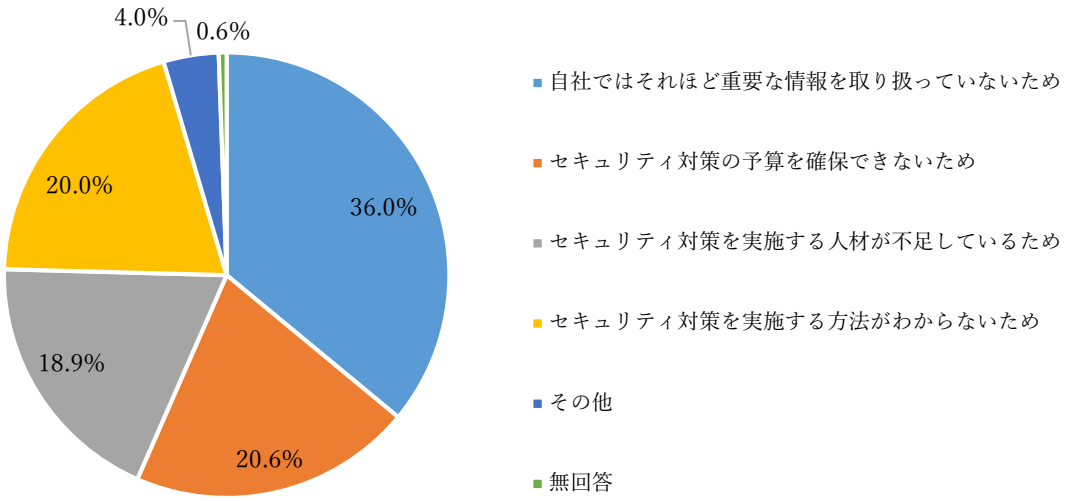
集計結果（抜粋）

１．サイバーセキュリティ対策の取組状況

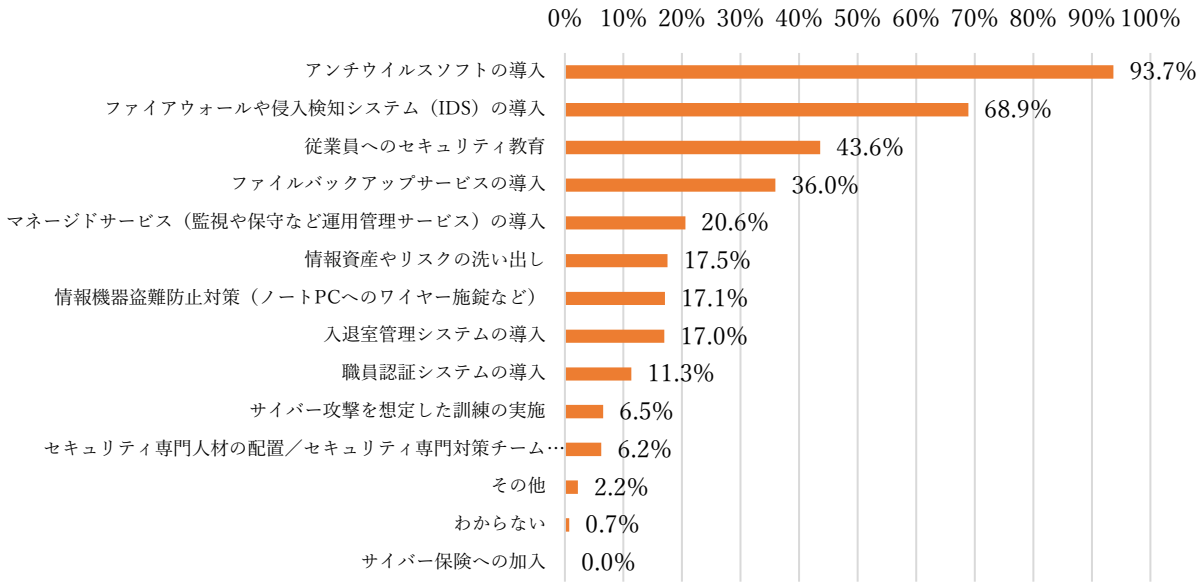
①サイバーセキュリティ対策の実施有無（n=1,522）



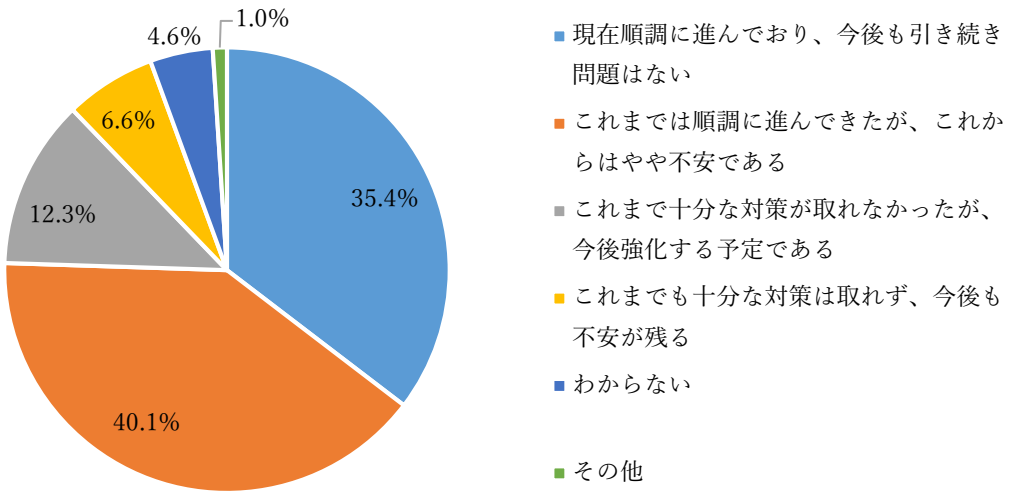
②サイバーセキュリティ対策の未実施理由（n=175）



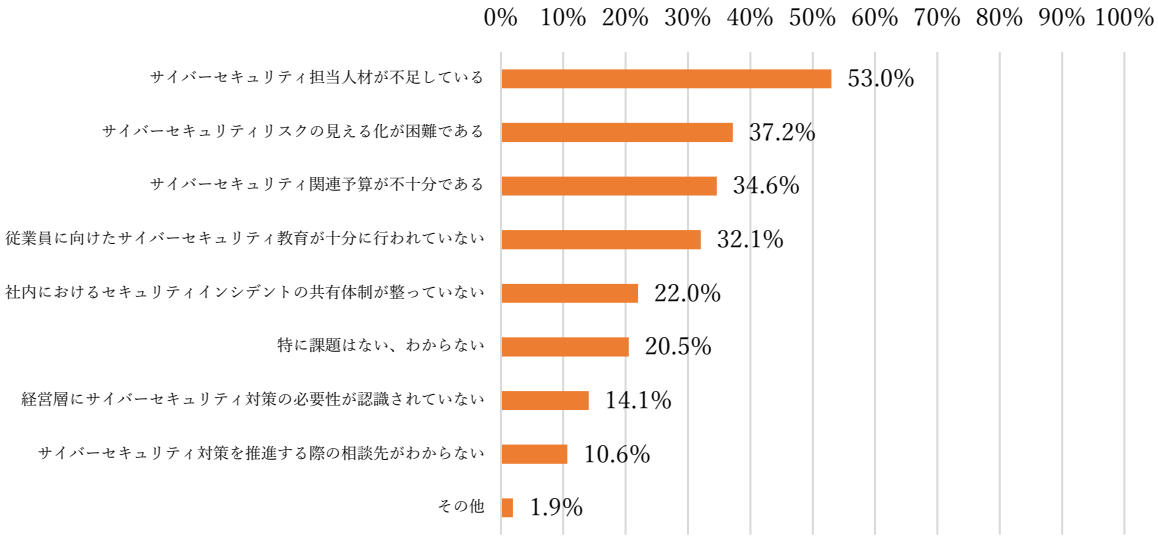
③サイバーセキュリティ対策の取り組み内容（n=1, 254）



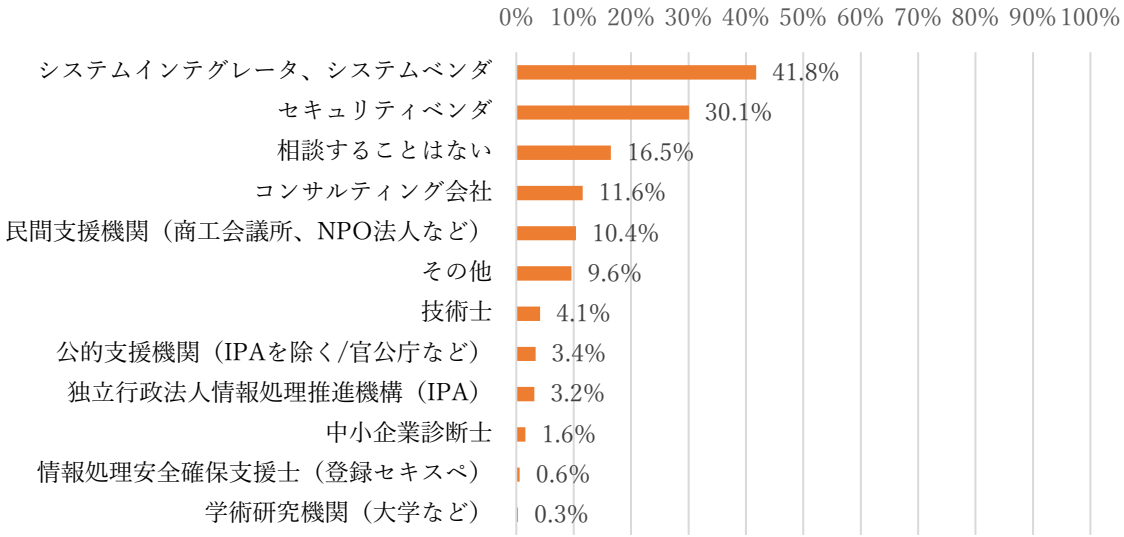
④サイバーセキュリティ対策の取り組み状況（n=1, 074）



⑤サイバーセキュリティ対策を推進する上での課題（n＝1, 522）

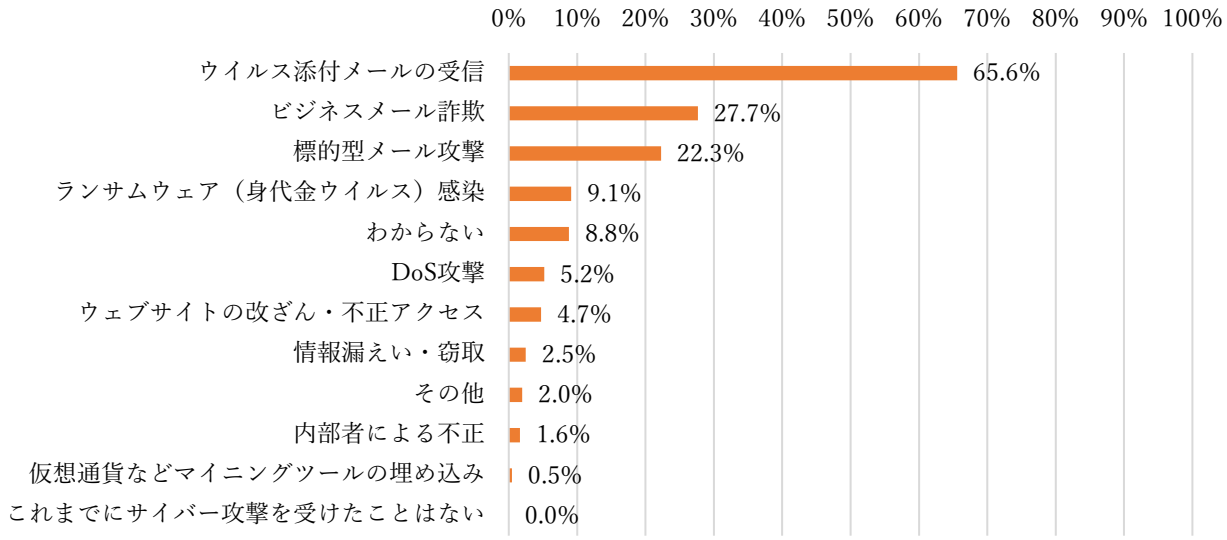


⑥サイバーセキュリティ対策の相談先

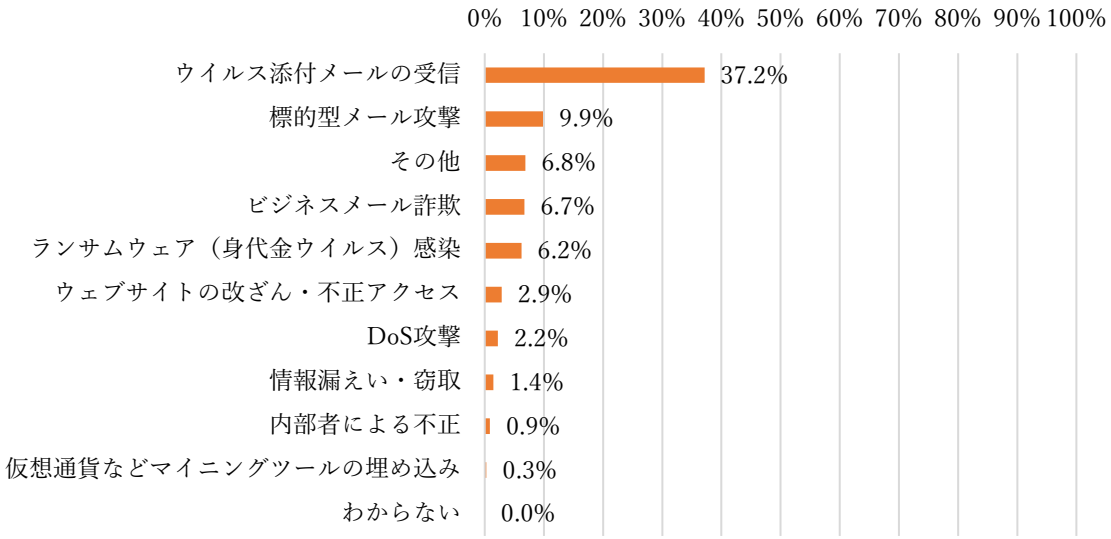


２．サイバー攻撃の被害状況とサイバーリスクに対する意識

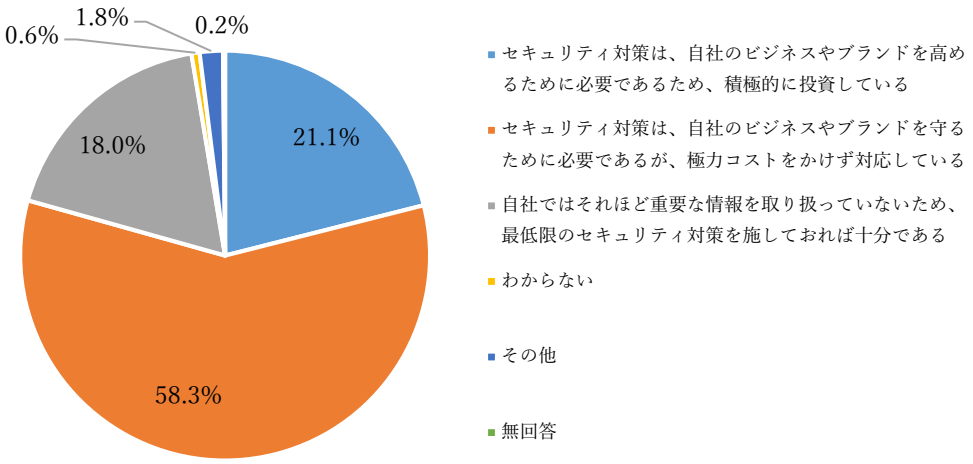
①これまで受けたサイバー攻撃の手口（n＝1,522）



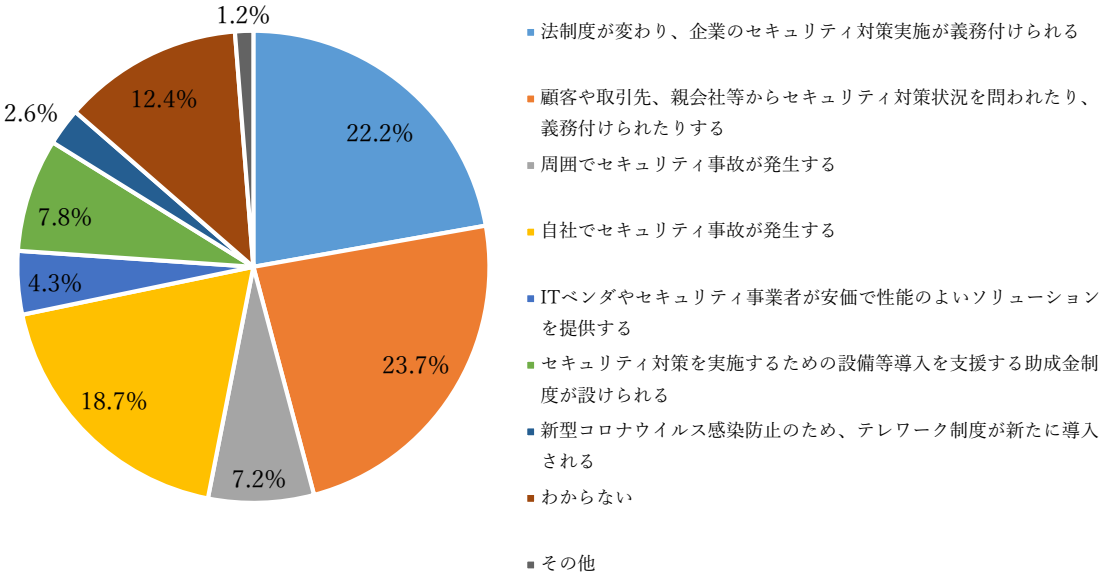
②業務への影響を受けたサイバー攻撃の手口（n=1,388）



③サイバーセキュリティ対策の取り組みの位置づけ（n=1, 254）

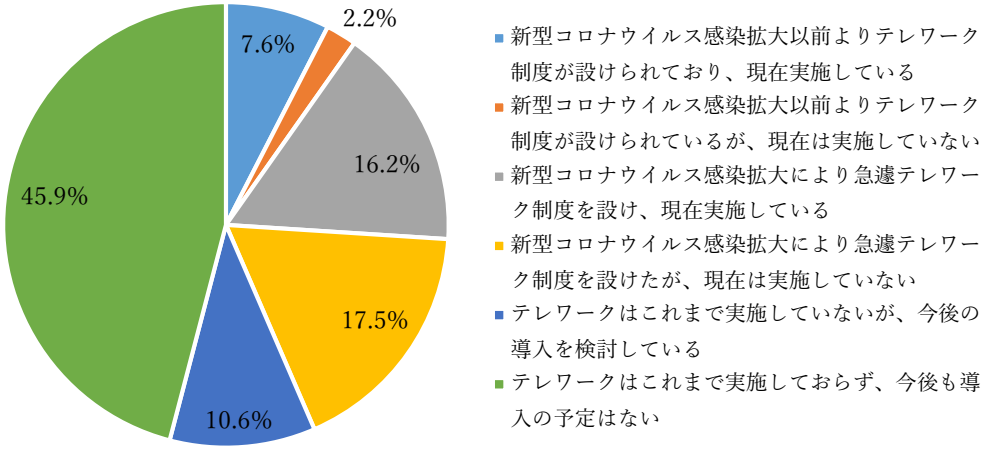


④サイバーセキュリティ対策が大きく進む契機

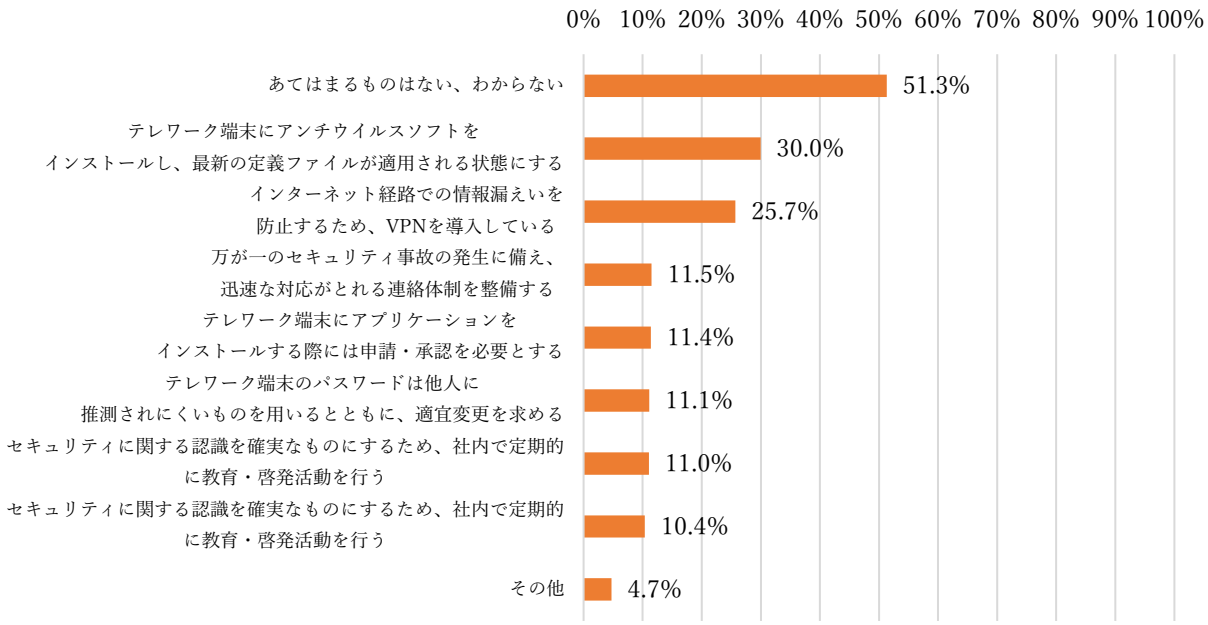


３．テレワーク実施時におけるサイバーセキュリティ対策

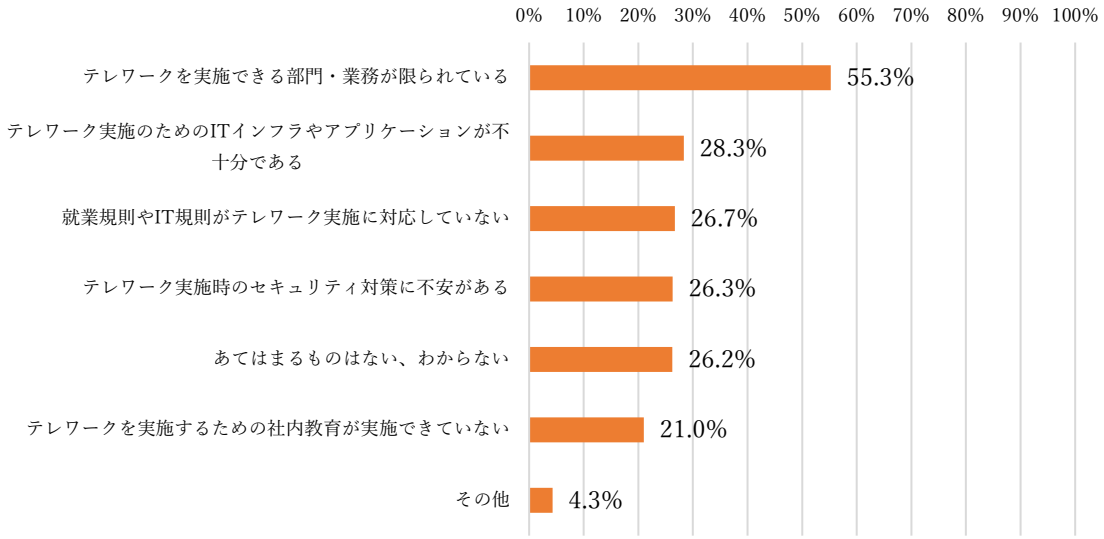
①テレワークの実施状況（n＝1,522）



②テレワーク実施に当たり導入を行ったセキュリティ対策（n＝1,522）

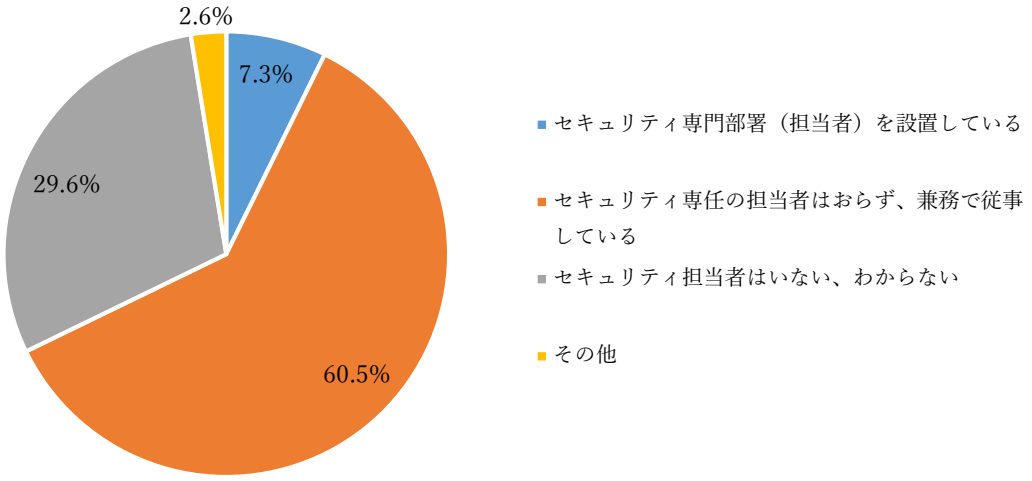


・テレワークを実施するに当たっての課題（n＝1,522）

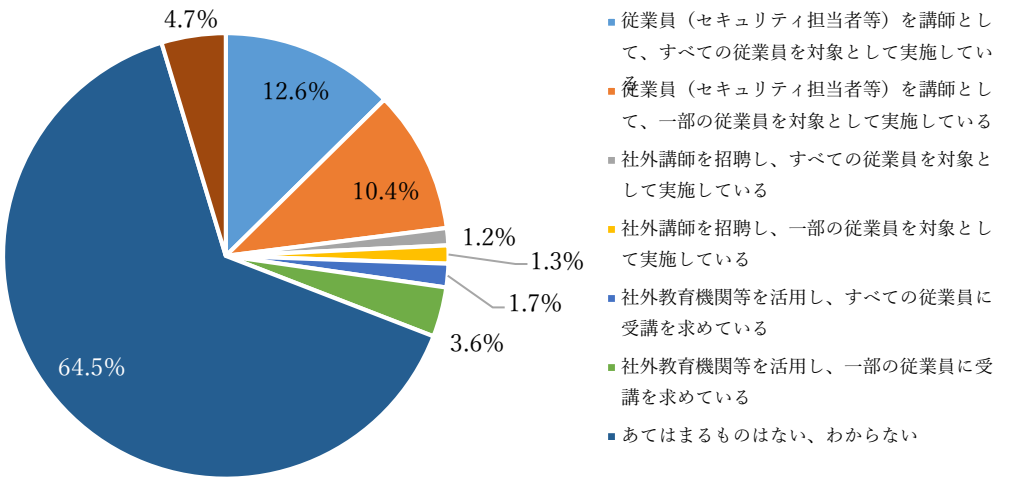


4．サイバーセキュリティ対策の実施体制

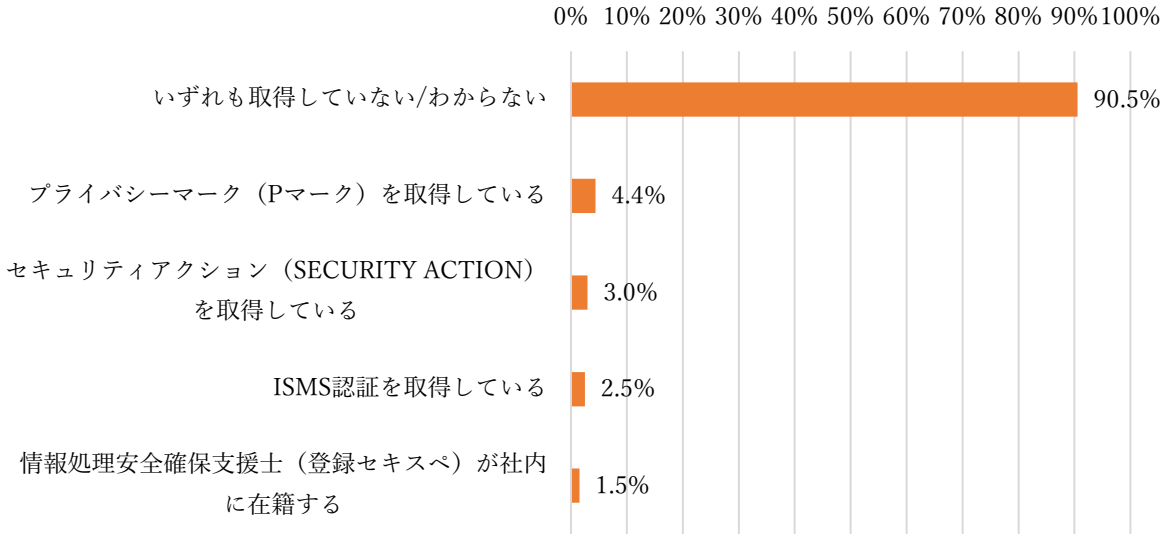
・サイバーセキュリティ対策の実施体制（n=1,522）



・従業員に向けたサイバーセキュリティ教育の実施状況（n=1, 522）

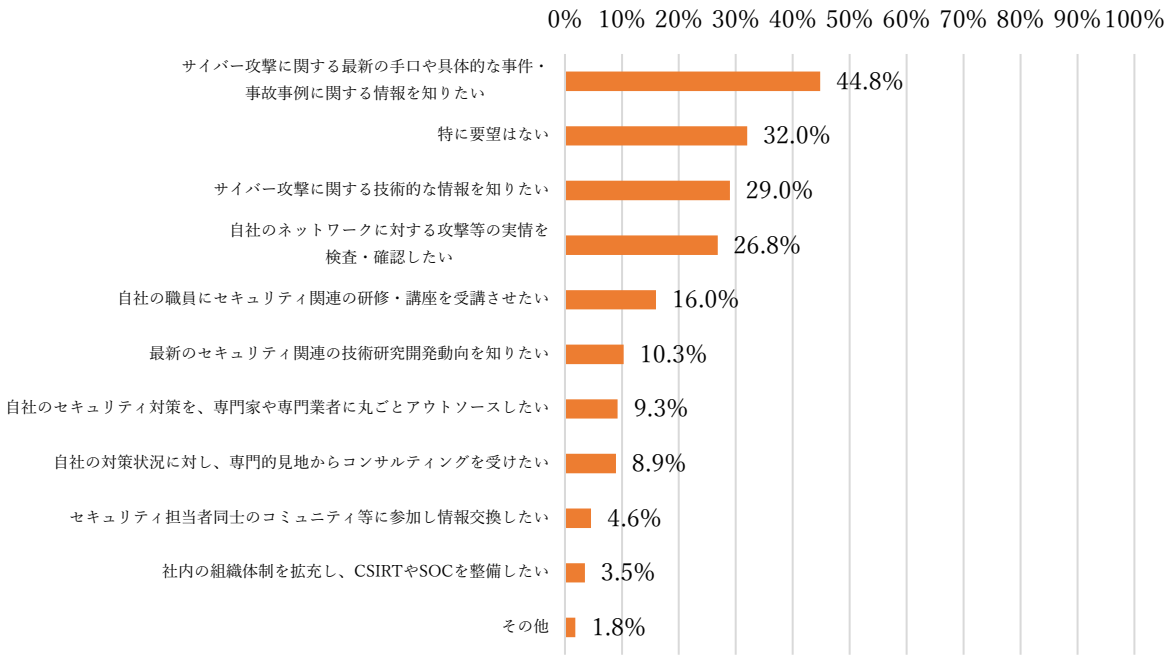


・セキュリティ関連資格の取得状況（n=1, 522）

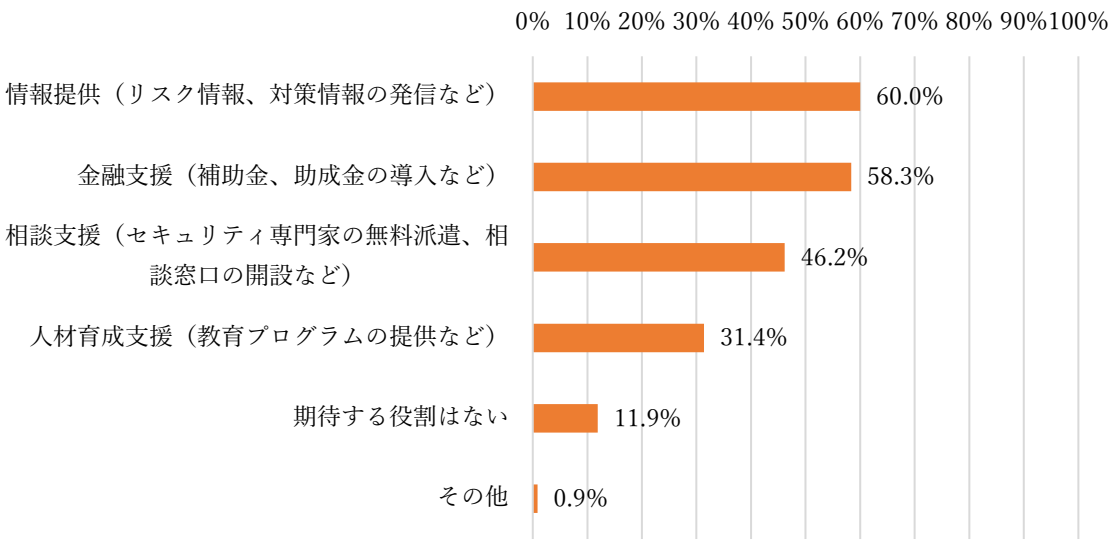


５．サイバーセキュリティ対策に関する要望等

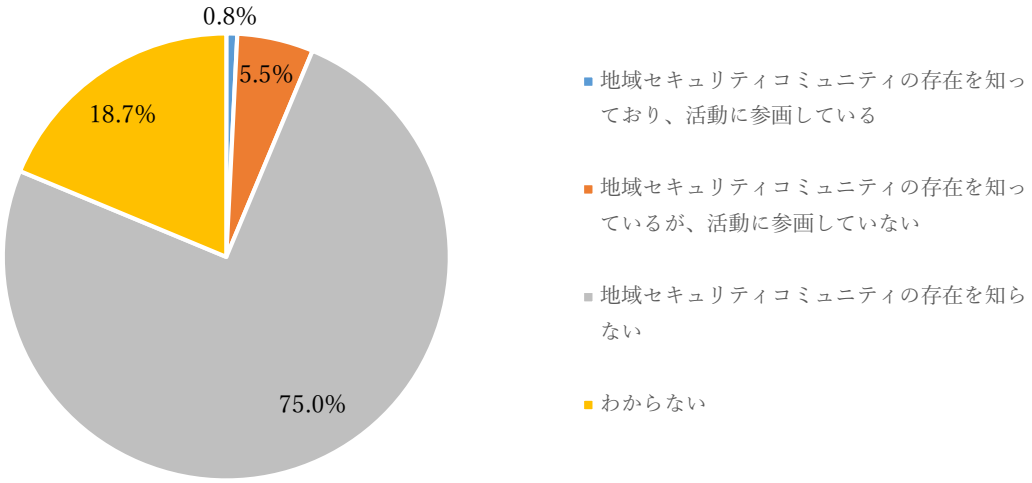
・サイバーセキュリティ対策に対する要望（n=1,522）



・国や地方自治体等、公的支援機関に期待する役割（n=1,522）



・地域セキュリティコミュニティの認知度(n=1,522)



以上