中小企業におけるサイバーセキュリティに関する調査

●はじめに

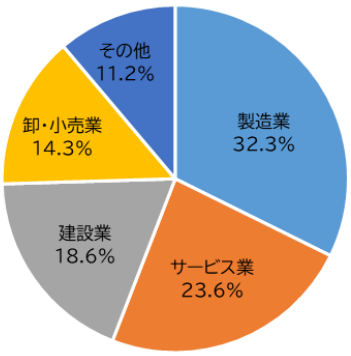
近年、サイバー攻撃や情報漏えいに関する報道が相次いでおり、サイバーセキュリティ対策の重要性が高まっている。こうした問題は大企業に限ったものではなく、中小企業においても適切な対策が求められている。

そこで、地域中小企業を対象にサイバーセキュリティに対する意識や対策状況、課題、今後求める支援策について調査した。

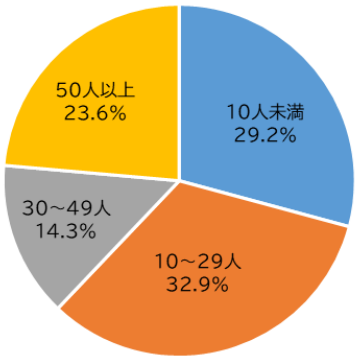
●調査概要

調査時期　：　令和８年１月１９日（月）　「せいしんビジネスクラブ　新春講演会」開催時
調査対象　：　せいしんビジネスクラブ（※）会員
（※）静清信用金庫取引先企業の経営者および後継者で構成する異業種交流組織
回 答 数　：　対象企業数　195 社　　回答数 161 社　　有効回答率：82.6%

≪業種内訳（n=161）≫



≪従業員規模内訳（n=161）≫



●要旨

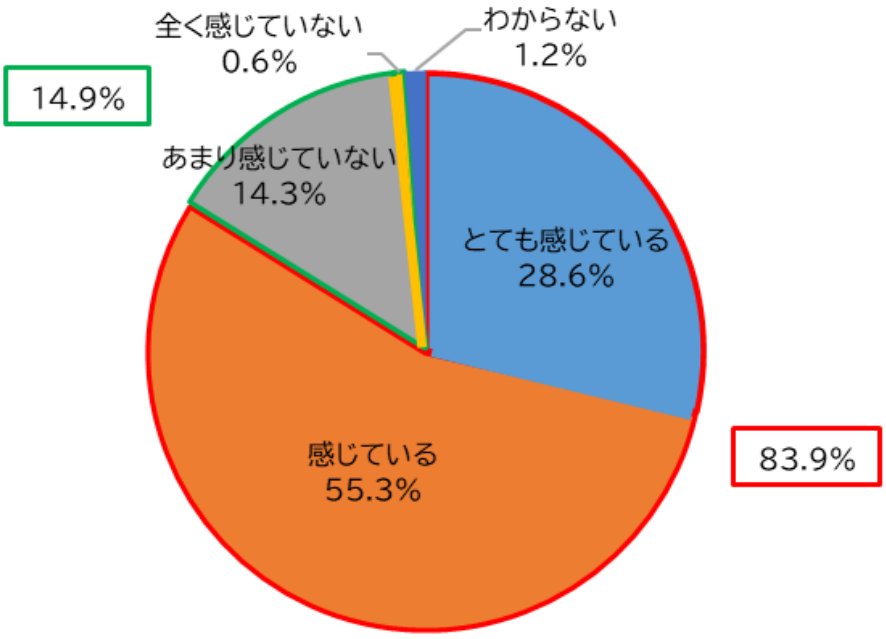
● <u>他社の被害・報道を契機に、８割超がサイバーセキュリティの必要性を感じている</u>
- ◆ サイバーセキュリティの必要性を感じている企業は 83.9%となり、多くの企業で危機意識が高まっている傾向が窺える。必要性を感じたきっかけは、他社の被害事例やニュースを挙げる企業が 68.1%で最多となった。

● <u>セキュリティ対策状況は二分されており、外部サービス活用の有無が進捗に影響</u>
- ◆ サイバーセキュリティ対策については、「対策できている」が 49.0%である一方、「対策できていない」も 44.7%と同程度存在した。
- ◆ 対策が進んでいる企業は、セキュリティサービスや専門業者を活用している割合が相対的に高く、外部サービスの活用状況が対策の進捗に影響している可能性がある。

● <u>セキュリティ対策状況によって直面する課題は異なる。対策の初期段階にある企業には、外部専門家のハンズオン支援を提案するなど進捗に合わせた支援が重要</u>
- ◆ 対策できている企業は、コストや投資効果を課題に挙げているのに対し、対策できていない企業は、何から手をつけてよいか分からない状態にある。
- ◆ 対策できていない企業の支援にあたっては、補助金等の資金支援と並行して、具体的な対策手順の整備や外部サービスに関する情報提供など、初期段階を後押しする施策が有効といえる。

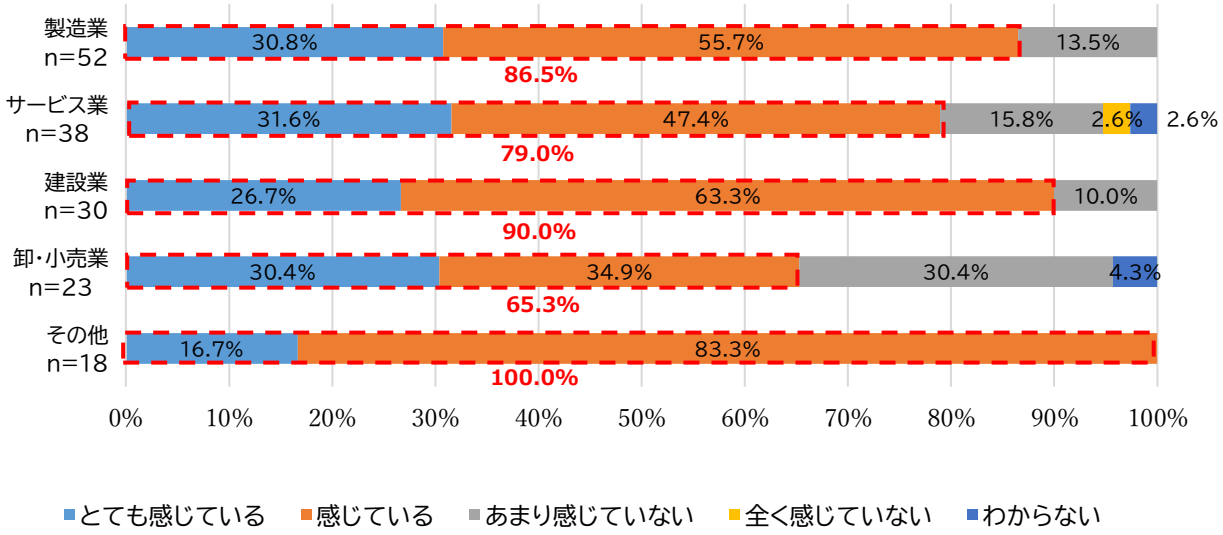
※本アンケートの数値は小数点第二位を四捨五入しております。

1．サイバーセキュリティの必要性（n＝161　SA）



サイバーセキュリティの必要性について、「とても感じている」・「感じている」の合計が 8 割超を占め、多くの企業で必要性を認識している状況が窺える。

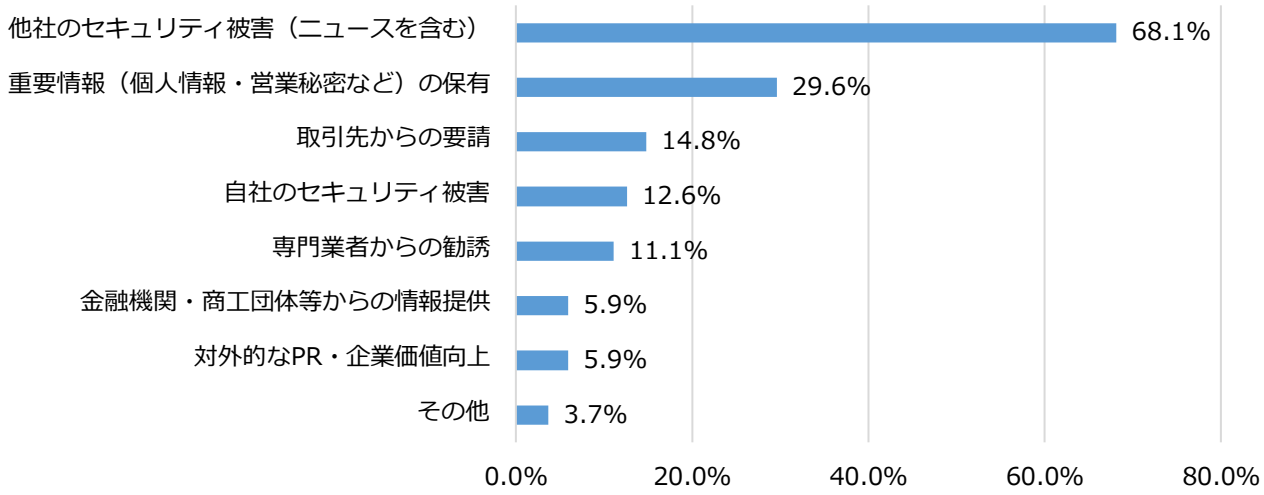
＜業種別＞



業種別に見ると、全体的にサイバーセキュリティ対策の必要性を高く認識している傾向が確認された。ただし、卸・小売業は「とても感じている」・「感じている」の合計が 6 割程度と他業種に比べて低水準であった。

2．サイバーセキュリティの必要性を感じたきっかけ（n＝135　MA）

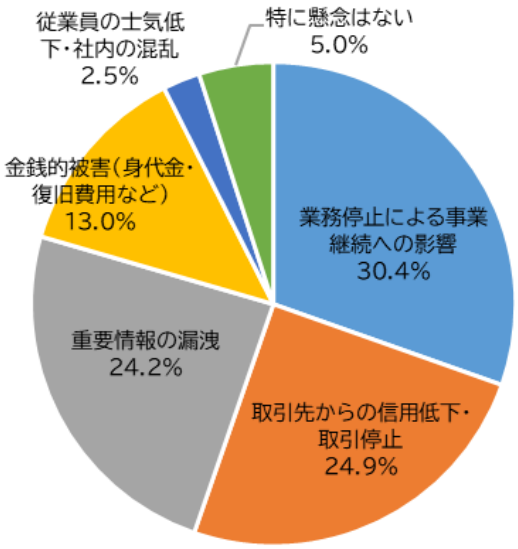
問１で「とても感じている」「感じている」と回答した方のみ



サイバーセキュリティの必要性を感じたきっかけは、「他社のセキュリティ被害（ニュースを含む）（68.1%）」が最多となり、「重要情報（個人情報・営業情報など）の保有（29.6%）」、「取引先からの要請（14.8%）」と続いた。

大手ビールメーカーや大手オフィス用品通販会社等の近時相次ぐサイバー被害報道により、他社のセキュリティ被害や影響を身近に感じたことで、危機意識が高まっている企業が多いことが推察される。

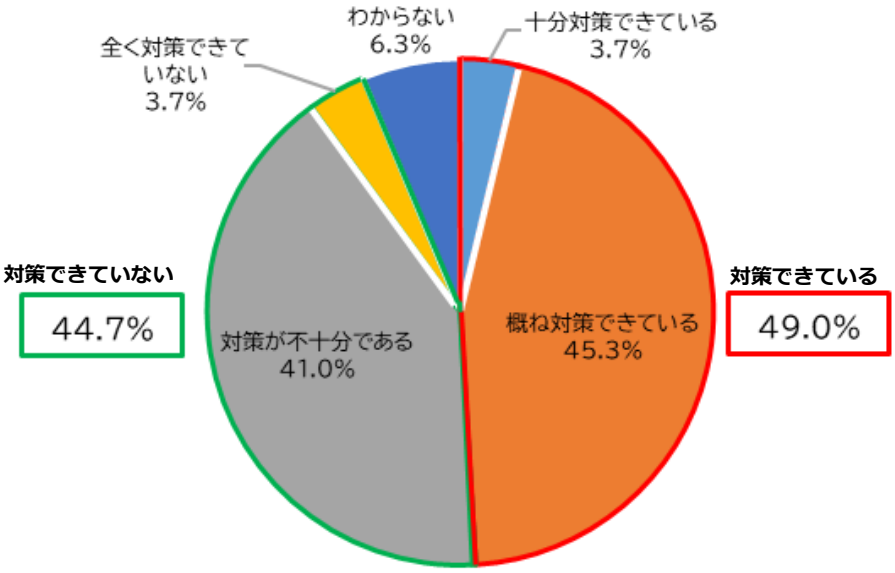
3．サイバー攻撃を受けた際に最も懸念する影響について（n＝161　SA）



サイバー攻撃を受けた際の影響として最も懸念する点は、「業務停止による事業継続への影響」が 30.4%と最多であった。次いで「取引先からの信用低下・取引停止（24.9%）」、「重要情報の漏えい（24.2%）」が続いた。一方、「金銭的被害（身代金・復旧費用など）」は 13.0%にとどまった。

金銭的損失そのものよりも、事業の停滞や信用低下を通じて売上高や利益の減少に波及し得る影響を、重く捉えている企業が多い傾向が窺える。

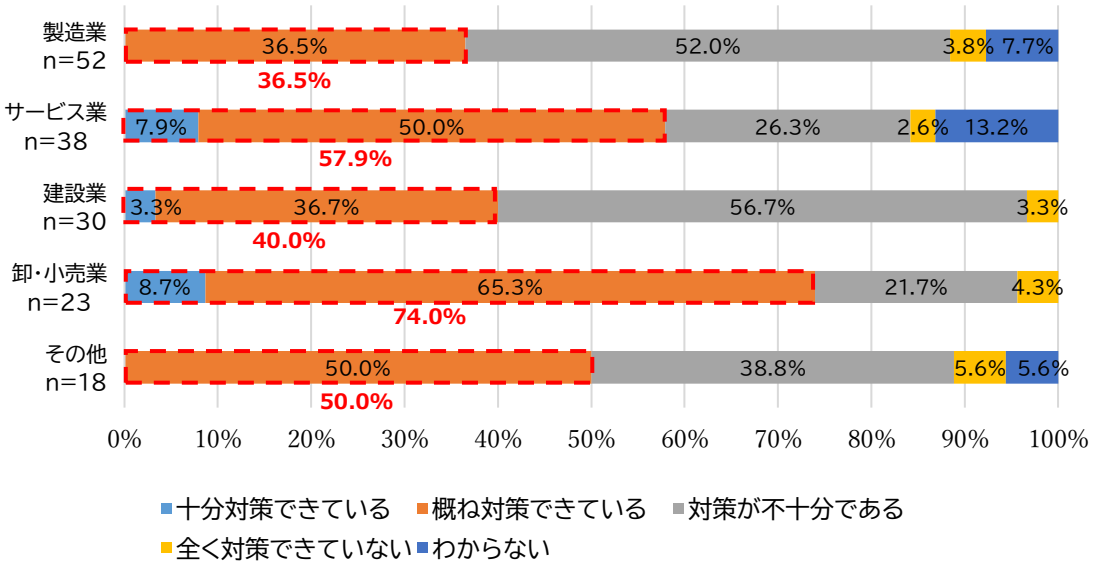
4．自社のサイバーセキュリティ対策について（n＝161　SA）



自社のサイバーセキュリティ対策状況について尋ねたところ、「十分対策できている」と「概ね対策できている」を合計した「対策できている」とした先が 49.0%と約半数を占めたものの、「対策が不十分である」と「全く対策できていない」を合計した「対策できていない」とした先も 44.7%と同程度存在した。

サイバーセキュリティ対策の必要性は多くの企業が認識しているものの、対策の取組み状況は二分されている。

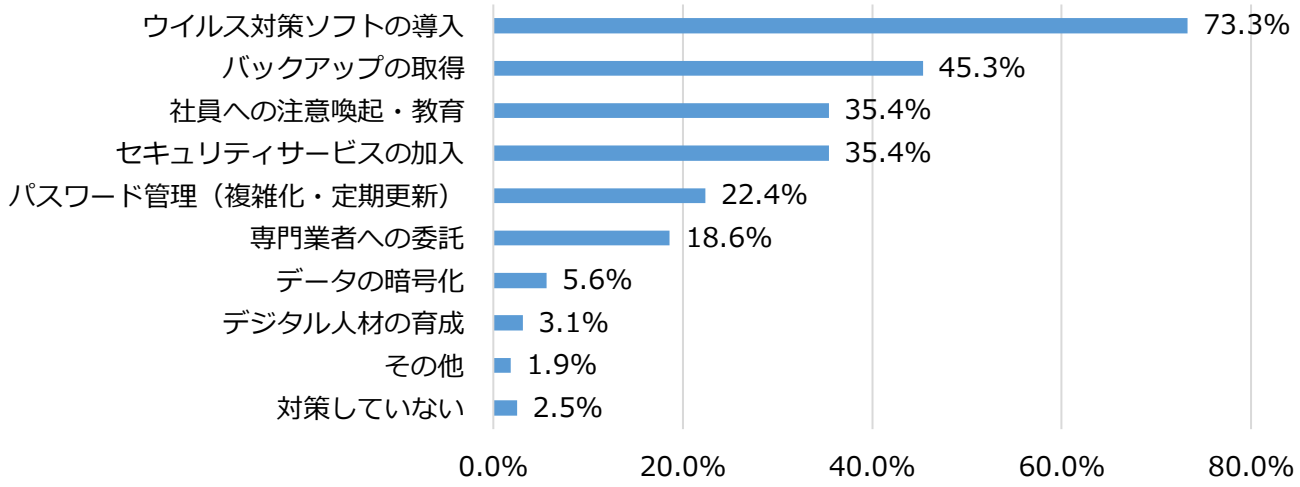
＜業種別＞



業種別では、卸・小売業、サービス業、その他の業種では「対策できている」とした先が半数以上を占めた一方、建設業は 40.0%、製造業は 36.5%にとどまった。

製造業や建設業で対策が進んでいないのは、工場や現場など拠点が分散しやすいこと、協力会社や外部関係者との接点が多いこと、発注先からの高度な対策要請といった要因が考えられ、結果としてサイバーセキュリティ対策の運用・管理が相対的に難しくなっていることが一因と考えられる。

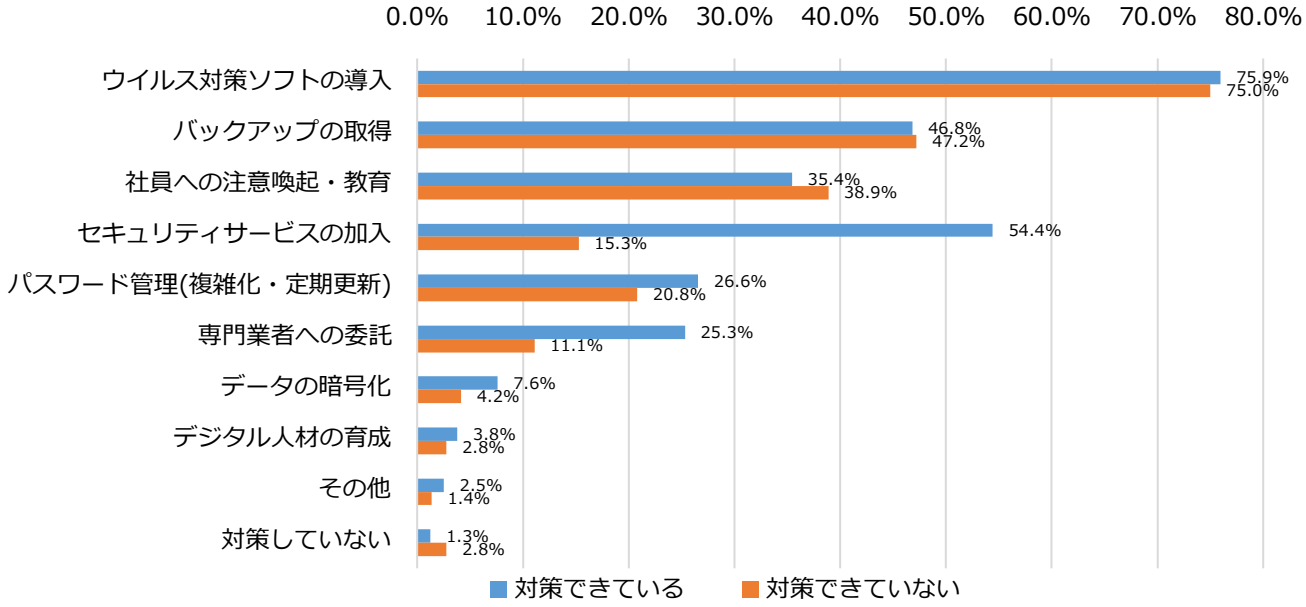
5．現在実施しているサイバーセキュリティ対策について（n＝161　MA）



現在実施しているサイバーセキュリティ対策としては、「ウイルス対策ソフトの導入（73.3%）」が最も多く、次いで「バックアップの取得（45.3%）」、「社員への注意喚起・教育（35.4%）」、「セキュリティサービスの加入（35.4%）」と続いた。

基本的な対策を中心に進めている一方で、「データの暗号化」は 5.6%、「デジタル人材の育成」は 3.1%にとどまっており、より厳格なセキュリティ対策や、専門人材の育成などの組織整備に関する取組みは限定的であった。

＜「現在実施しているサイバーセキュリティ対策」と「自社の対策状況」とのクロス分析＞

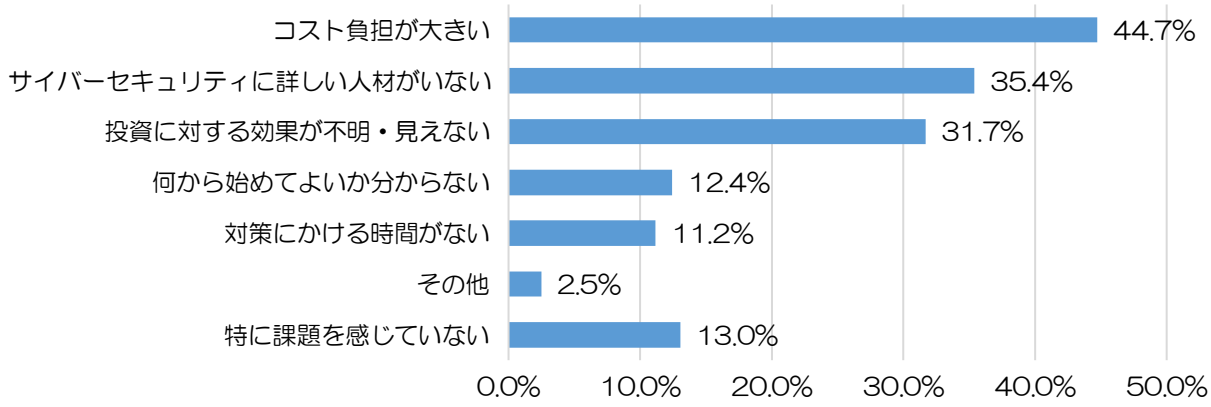


実施している対策内容と対策状況をクロスして見ると、「対策できている」企業では、「セキュリティサービスへの加入」や「専門業者への委託」など、外部サービスを活用した対策を実施している割合が相対的に高い傾向が見られた。

一方、「対策できていない」企業では、ウイルス対策ソフトやバックアップといった基本的な対策は実施されているものの、外部サービスの活用には至っていないケースが多いといえる。

これらの結果から、外部サービスの活用がセキュリティ対策の進捗に影響している可能性がある。

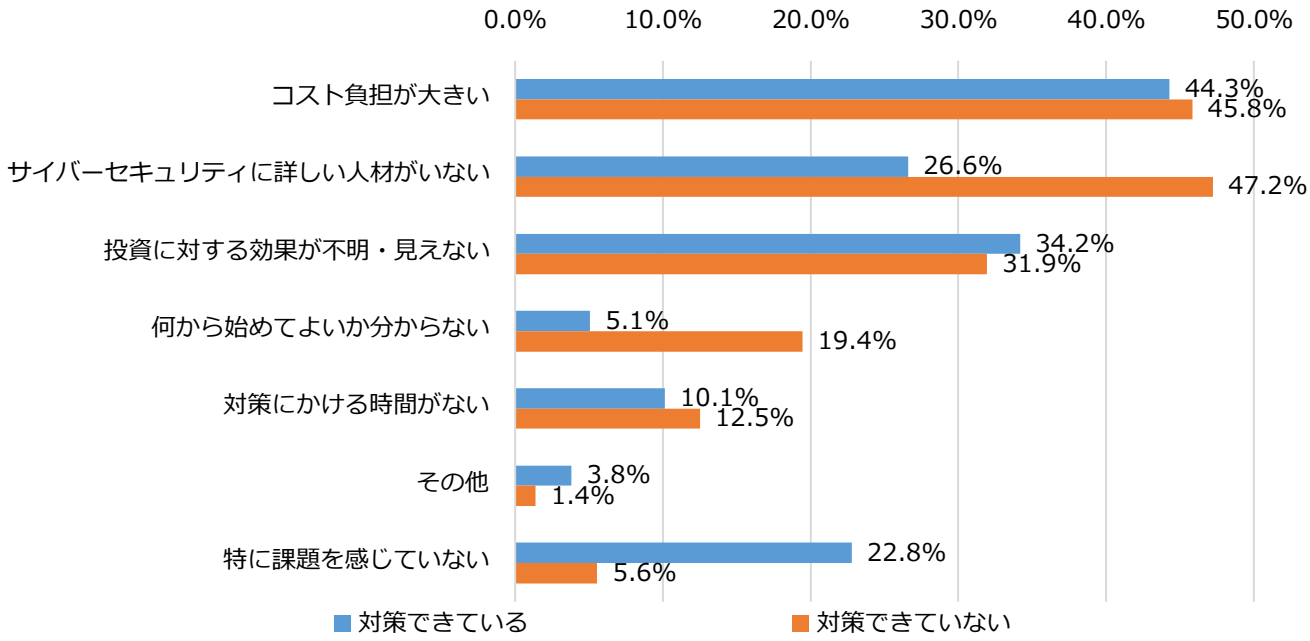
6．サイバーセキュリティ対策における課題（ｎ＝161　MA 3 つまで）



サイバーセキュリティ対策における課題は、「コスト負担が大きい（44.7%）」が最も多く、「サイバーセキュリティに詳しい人材がいない（35.4%）」、「投資効果が不明・見えない（31.7%）」と続いた。

必要性を認識しつつも、金銭的負担や費用対効果の検証が難しいことが対策推進の課題となっている様子が窺える。また、人材や知識の制約も背景にあるものと考えられる。

＜「サイバーセキュリティ対策における課題」と「自社の対策状況」とのクロス分析＞

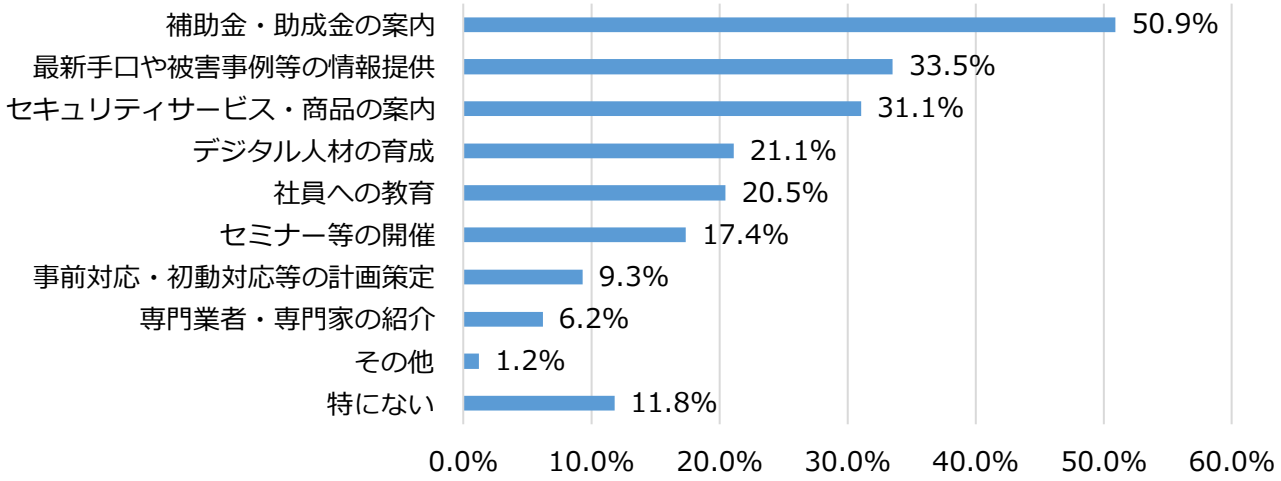


課題と対策状況をクロスして見ると、「対策できていない」企業は、「何から始めてよいか分からない」「サイバーセキュリティに詳しい人材がいない」といった課題を挙げる割合が相対的に高かった。対策できていない企業は、コストや時間の問題よりも、そもそも何から手をつけてよいか分からない状態であることが窺える。

それに対し、「対策できている」企業は、「コスト負担が大きい」「投資に対する効果が不明・見えない」を課題に挙げる割合が高かった。

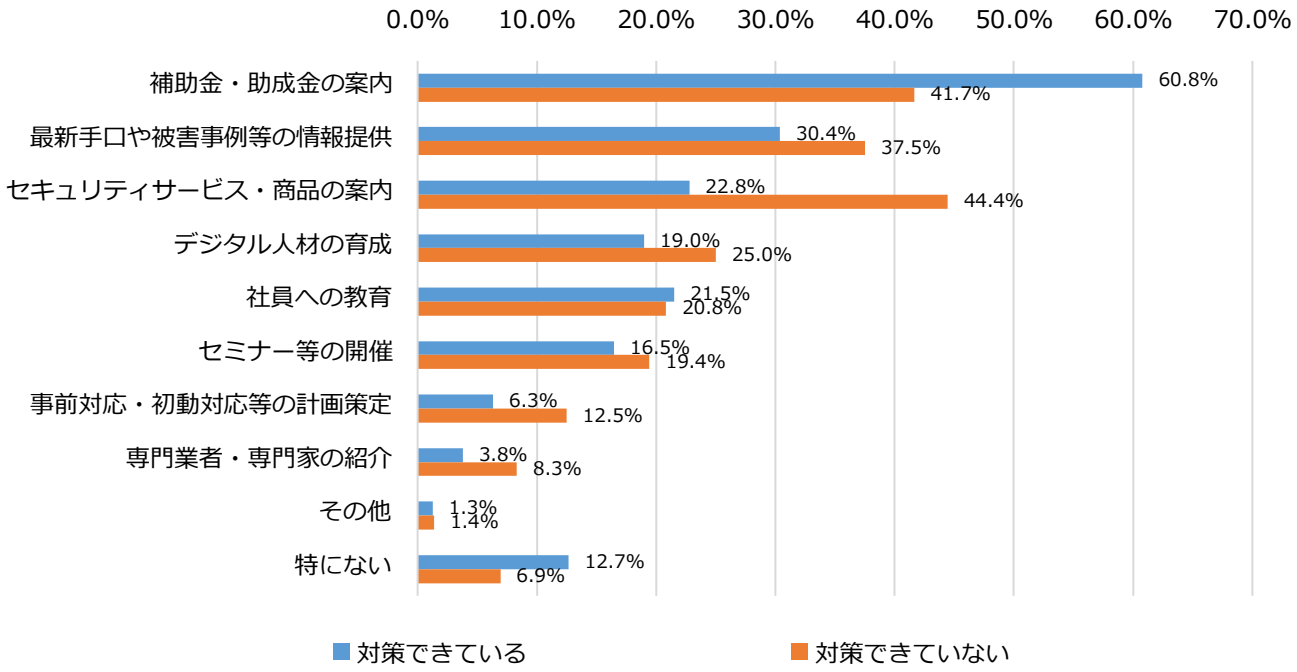
セキュリティ対策の進捗状況によって、直面する課題が異なる傾向が明らかとなった。

7．求める支援について（n＝161　MA 3 つまで）



求める支援としては、「補助金・助成金の案内」が 50.9%と最多であった。また、「最新手口や被害事例等の情報提供」が 33.5%、「セキュリティサービス・商品の案内」が 31.1%と続いた。

＜「求める支援について」と「自社の対策状況」とのクロス分析＞



求める支援と対策状況をクロスしてみると、「対策できている」企業は、「補助金・助成金の案内」を挙げる割合が相対的に高かったのに対し、「対策できていない」企業では、「セキュリティサービス・商品の案内」や「最新手口や被害事例等の情報提供」を挙げる割合が相対的に高かった。

セキュリティ対策の進捗状況によって求める支援は異なり、各企業の進捗や課題に合わせた支援が重要である。対策が進んでいない企業の支援にあたっては、補助金・助成金による資金支援と並行して、具体的な対策手順の整備や外部サービスに関する情報提供など、初期段階を後押しする施策が有効といえる。

以上

（静清信用金庫　経営相談部　令和８年１月作成）