# 「中小企業の経営者のサイバーリスク意識調査2019」

2020年1月

一般社団法人　日本損害保険協会

# 目次

# 1．調査概要

- 調査目的　：損保協会が2018年度に日本企業1,113社を対象に実施した「サイバー保険に関する調査2018」の結果、企業規模が小さくなるほどサイバーリスクに対する危機意識が低く、取り組みが進んでいない実態が明らかになった。そこで、中小企業のサイバーリスクに対する意識と対応実態を把握し、今後の啓発活動に資することを目的として、本調査を実施した。

- 調査実施方法　：インターネット・リサーチ法

- 調査実施時期　：2019年11月12日（火）～11月15日（金）

- 有効回答数　：中小企業の経営者・役員825サンプル／大企業の経営者・役員207サンプル（計1,032サンプル）

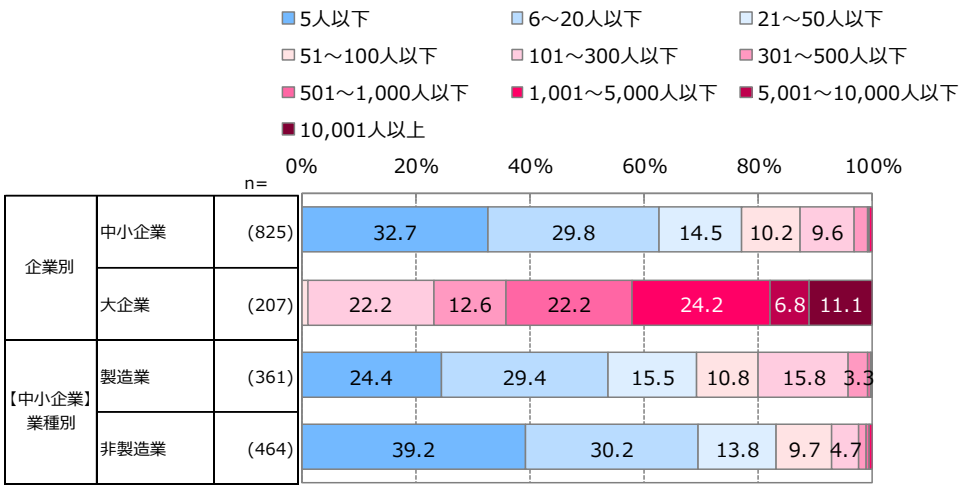
- 割付　：割付ごとのサンプル数は右表の通り。
※中小企業は、中小企業法の定義に基づく。

| | | |
|---|---|---|
| 中小企業 | 製造業 | 361 |
| | 非製造業 | 464 |
| 大企業 | 製造業 | 75 |
| | 非製造業 | 132 |
| 全体 | | 1,032 |

- 調査実施機関　：株式会社マクロミル

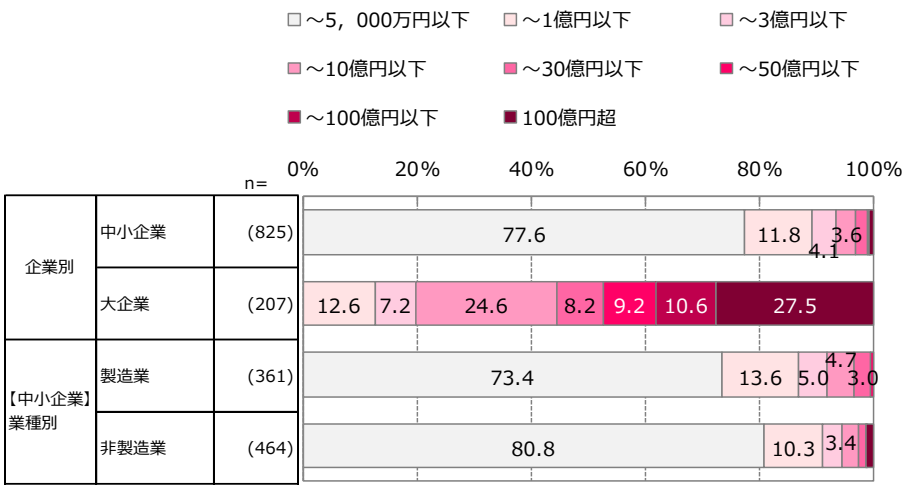
# 2．回答企業プロフィール

## ＜従業員数＞



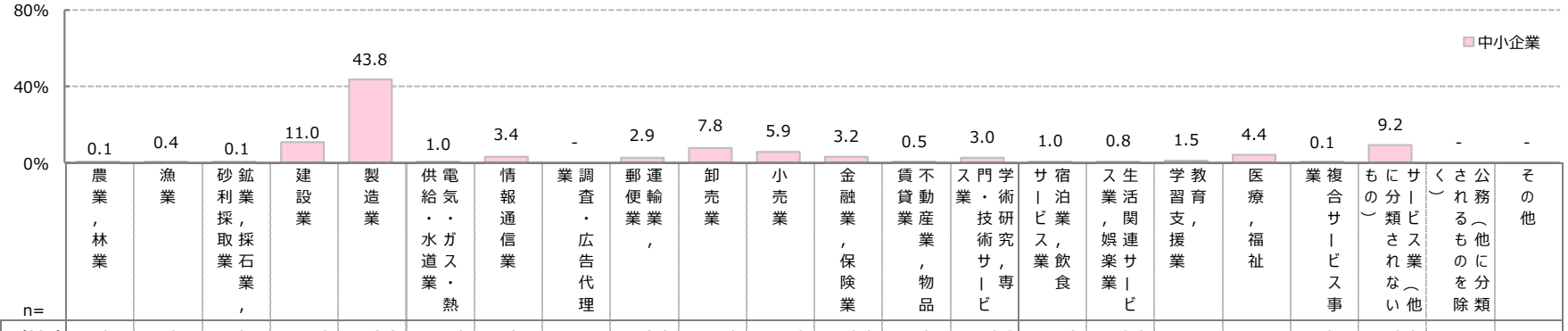

※2%未満は非表示

## ＜資本金＞




※2%未満は非表示

## ＜業種＞



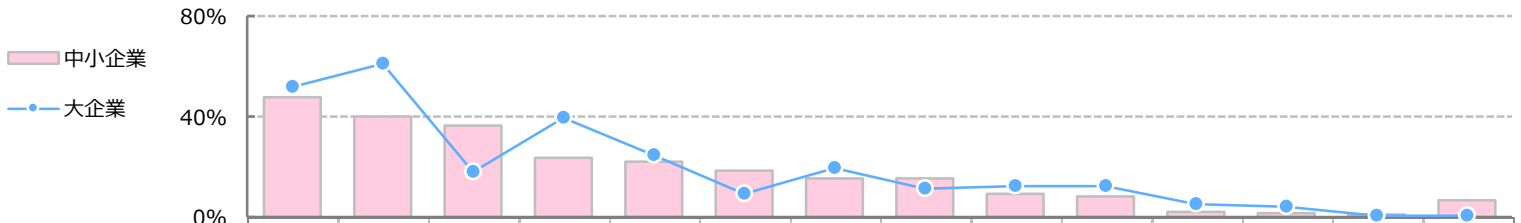

| | | n= | 農業，林業 | 漁業 | 鉱業，採石業，砂利採取業 | 建設業 | 製造業 | 電気・ガス・熱供給・水道業 | 情報通信業 | 調査・広告代理業 | 運輸業，郵便業 | 卸売業 | 小売業 | 金融業，保険業 | 不動産業，物品賃貸業 | 学術研究，専門・技術サービス業 | 宿泊業，飲食サービス業 | 生活関連サービス業，娯楽業 | 教育，学習支援業 | 医療，福祉 | 複合サービス事業 | サービス業（他に分類されないもの） | 公務（他に分類されるものを除く） | その他 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 企業別 | 中小企業 | (825) | 0.1 | 0.4 | 0.1 | 11.0 | 43.8 | 1.0 | 3.4 | - | 2.9 | 7.8 | 5.9 | 3.2 | 0.5 | 3.0 | 1.0 | 0.8 | 1.5 | 4.4 | 0.1 | 9.2 | - | - |
| | 大企業 | (207) | - | - | - | 4.3 | 36.2 | 1.0 | 12.1 | - | 2.4 | 5.3 | 4.8 | 4.8 | 1.0 | 1.0 | 1.0 | 1.9 | 3.4 | 7.2 | 0.5 | 13.0 | - | - |
| 【中小企業】業種別 | 製造業 | (361) | - | - | - | - | 100.0 | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| | 非製造業 | (464) | 0.2 | 0.6 | 0.2 | 19.6 | - | 1.7 | 6.0 | - | 5.2 | 13.8 | 10.6 | 5.6 | 0.9 | 5.4 | 1.7 | 1.5 | 2.6 | 7.8 | 0.2 | 16.4 | - | - |

# 3．調査結果（1）経営課題の優先度

- 中小企業の経営者にとって優先度の高い経営課題は、「収益性の向上」や「人材の育成」であり、これらに比べると「サイバーリスクへの対応」の優先度は極めて低い。
- 経営課題における「サイバーリスクへの対応」の優先度は、中小企業だけでなく、大企業の経営者にとっても低い。

Q1　貴社の経営課題について、優先度の高いものをお選びください。（３つまで）

※全体ベース




| | | n= | 収益性の向上 | 人材の育成 | 新規顧客の開拓 | 業務効率化 | 後継者育成 | 既存顧客のつなぎとめ | 新製品の開発 | 採用 | 組織づくり | 長時間労働の是正 | 企業の合併・買収 | サイバーリスクへの対応 | その他 | 特になし |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 企業別 | 中小企業 | (825) | 48.0 | 40.4 | 36.7 | 23.8 | 22.1 | 18.8 | 15.8 | 15.6 | 9.6 | 8.6 | 2.2 | 1.6 | 1.2 | 6.8 |
| | 大企業 | (207) | 52.2 | 61.4 | 18.4 | 39.6 | 24.6 | 9.2 | 19.8 | 11.6 | 12.6 | 12.6 | 5.3 | 4.3 | 1.0 | 1.0 |
| 【中小企業】業種別 | 製造業 | (361) | 50.7 | 42.7 | 33.0 | 25.8 | 19.9 | 15.5 | 27.4 | 14.4 | 11.1 | 9.4 | 2.2 | 1.9 | 0.8 | 4.2 |
| | 非製造業 | (464) | 45.9 | 38.6 | 39.7 | 22.2 | 23.7 | 21.3 | 6.7 | 16.6 | 8.4 | 8.0 | 2.2 | 1.3 | 1.5 | 8.8 |
| 従業員数別 | 50名以下 | (636) | 48.3 | 34.3 | 39.8 | 20.6 | 23.1 | 23.0 | 14.3 | 12.7 | 8.0 | 7.2 | 1.9 | 1.3 | 1.1 | 8.6 |
| | 51～100名 | (86) | 47.7 | 54.7 | 36.0 | 33.7 | 20.9 | 5.8 | 16.3 | 24.4 | 15.1 | 11.6 | 3.5 | 3.5 | - | - |
| | 101～1,000名 | (219) | 48.4 | 61.6 | 19.6 | 41.1 | 20.1 | 6.4 | 21.0 | 19.6 | 14.2 | 12.3 | 4.1 | 3.2 | 2.3 | 0.5 |
| | 1,001名以上 | (91) | 54.9 | 65.9 | 15.4 | 30.8 | 26.4 | 9.9 | 22.0 | 8.8 | 11.0 | 15.4 | 5.5 | 4.4 | - | 2.2 |

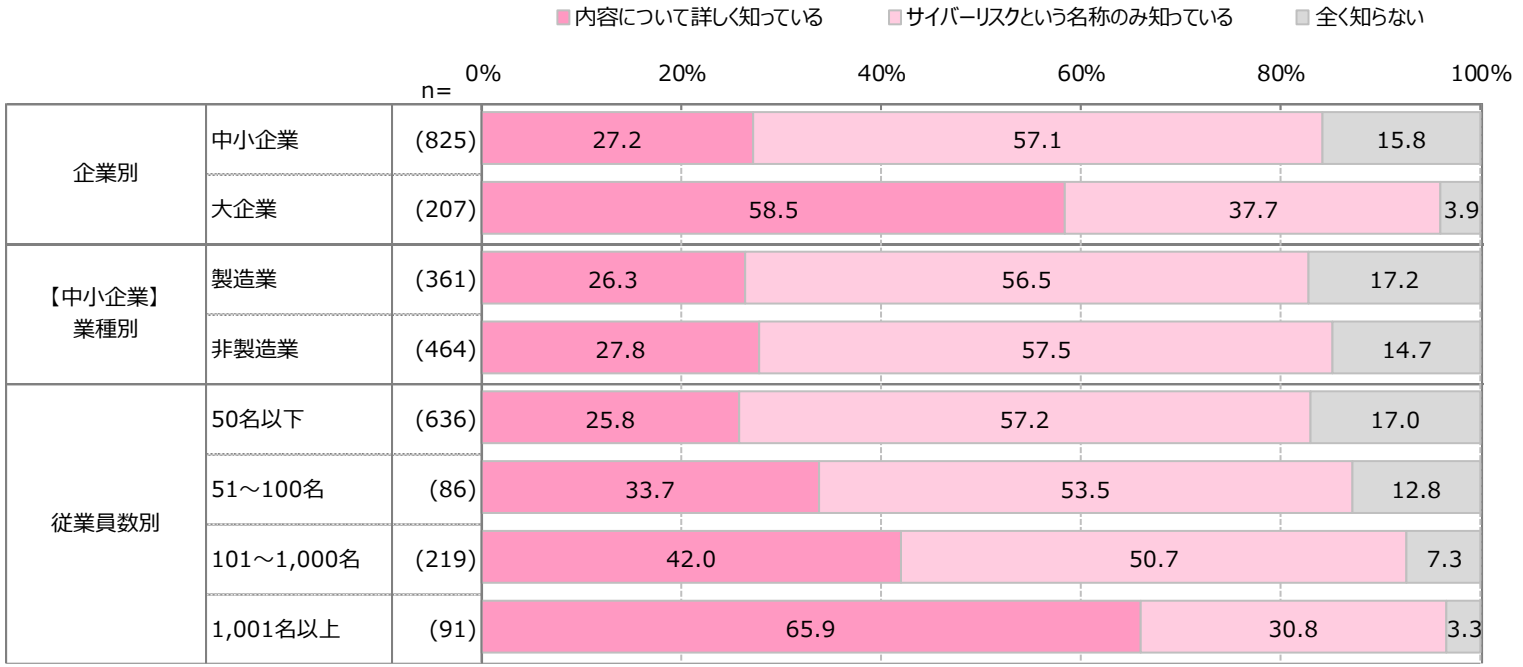
※「中小企業」のスコアで降順ソート

# （2）サイバーリスクの認知度

- 中小企業の経営者の80%以上がサイバーリスクを認知しているが、「内容について詳しく知っている」と回答したのは27.2%にとどまる。
- 従業員数別に見ると、企業規模が小さいほどサイバーリスクを「全く知らない」という回答が増えている。

Q2　あなたは、サイバーリスクについてどの程度ご存知ですか。

※全体ベース



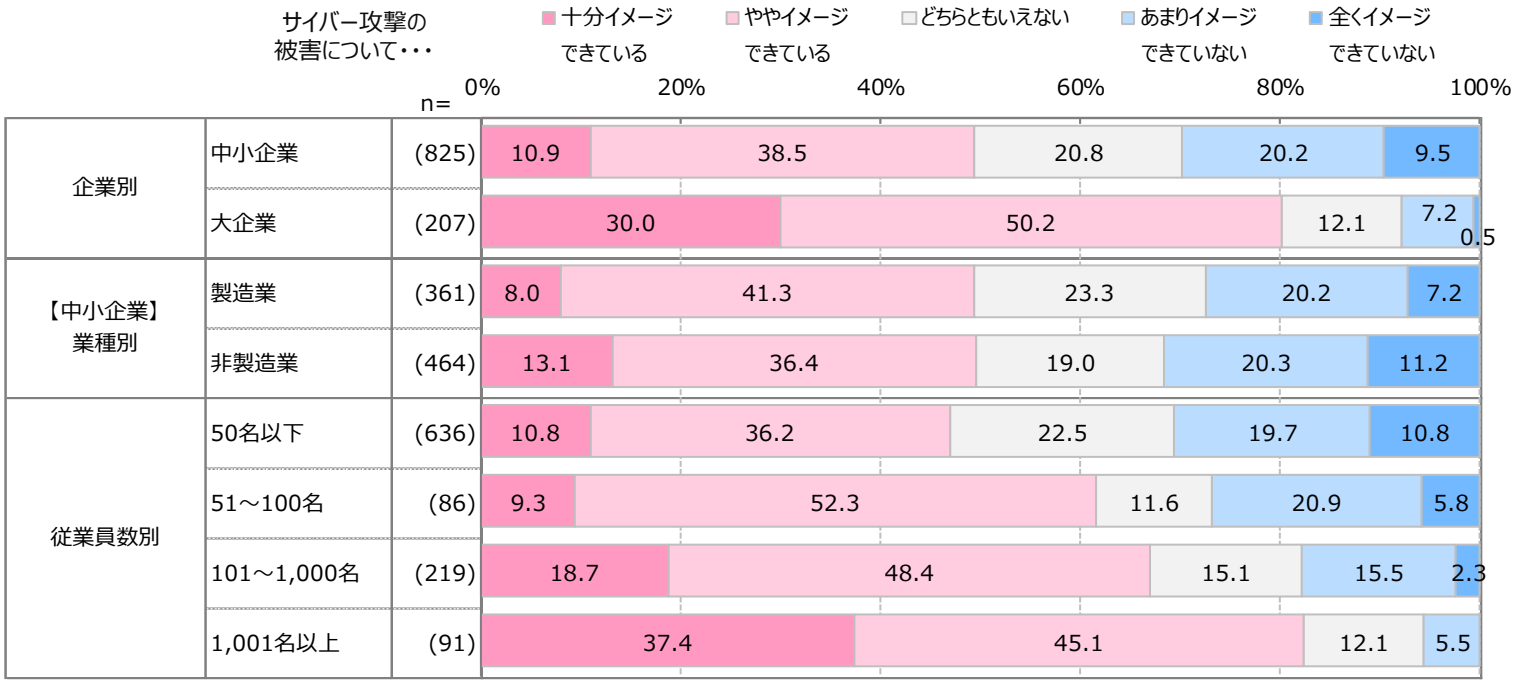

| | | n= | 内容について詳しく知っている | サイバーリスクという名称のみ知っている | 全く知らない |
|---|---|---|---|---|---|
| 企業別 | 中小企業 | (825) | 27.2 | 57.1 | 15.8 |
| | 大企業 | (207) | 58.5 | 37.7 | 3.9 |
| 【中小企業】業種別 | 製造業 | (361) | 26.3 | 56.5 | 17.2 |
| | 非製造業 | (464) | 27.8 | 57.5 | 14.7 |
| 従業員数別 | 50名以下 | (636) | 25.8 | 57.2 | 17.0 |
| | 51～100名 | (86) | 33.7 | 53.5 | 12.8 |
| | 101～1,000名 | (219) | 42.0 | 50.7 | 7.3 |
| | 1,001名以上 | (91) | 65.9 | 30.8 | 3.3 |

# （3）サイバー攻撃の被害イメージ有無

- 中小企業の経営者の約50%がサイバー攻撃による被害をイメージできている（「十分イメージできている」「ややイメージできている」）。一方、大企業の経営者は、 80%以上がイメージできていると回答している。
- 一方、イメージできていない（「あまりイメージできていない」「全くイメージできていない」）と回答した中小企業の経営者は29.7%。大企業の経営者は10%を下回った。

Q3 サイバー攻撃によって貴社が被る被害について、どの程度イメージできていますか。

※全体ベース

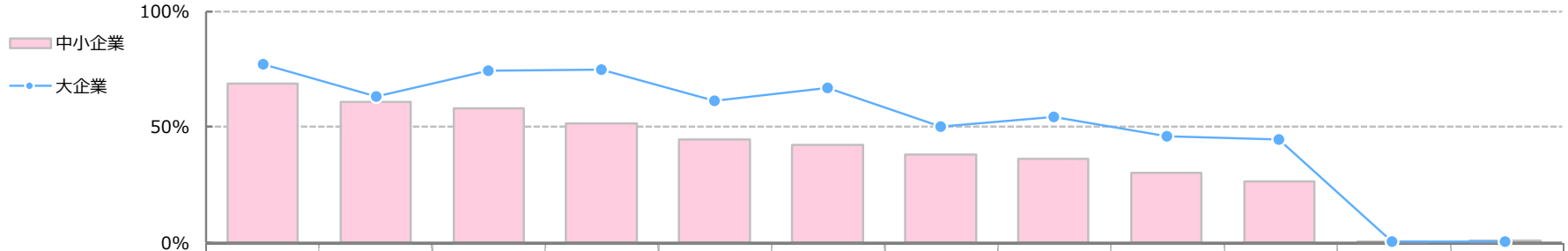


# （4）サイバー攻撃があった際の被害・損失

- サイバー攻撃の被害をイメージできていると回答した中小企業の経営者のうち、最も多く挙げられた被害・損失は、「機密情報・個人情報の盗難」（68.9%）であった。
- 「システムダウン」「業務の停止」「取引の停止」など、サイバー攻撃により事業活動が中断されるという回答は、大企業と中小企業の回答に開きがあった。
- 同様に「企業イメージ・信用力の低下」も大企業と中小企業の経営者の回答に開きがあった。

Q4　前問で「サイバー攻撃の被害についてイメージができている」とお答えになった方にお伺いします。
サイバー攻撃があった場合に、どのような被害や損失が生じると思いますか。あてはまるものをすべてお選びください。

※サイバー攻撃の被害について、イメージができている方ベース




| | | n= | 機密情報・個人情報の盗難 | データの損壊・改ざん | システムダウン | 企業イメージ・信用力の低下 | 取引先や顧客への損害賠償 | 業務の停止 | 原因究明のための調査・復旧費用の捻出 | 顧客の喪失 | 他者への攻撃に利用される | 取引の停止 | その他 | わからない・特に思い浮かぶものはない |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 企業別 | 中小企業 | (408) | 68.9 | 60.5 | 57.8 | 51.5 | 44.4 | 42.4 | 38.0 | 36.3 | 30.1 | 26.5 | 0.2 | 1.0 |
| | 大企業 | (166) | 77.1 | 63.3 | 74.1 | 74.7 | 61.4 | 66.9 | 50.0 | 54.2 | 45.8 | 44.6 | 0.6 | 0.6 |
| 【中小企業】業種別 | 製造業 | (178) | 64.0 | 61.8 | 61.8 | 47.2 | 39.9 | 41.6 | 33.7 | 33.7 | 29.2 | 23.6 | 0.6 | 1.1 |
| | 非製造業 | (230) | 72.6 | 59.6 | 54.8 | 54.8 | 47.8 | 43.0 | 41.3 | 38.3 | 30.9 | 28.7 | - | 0.9 |
| 従業員数別 | 50名以下 | (299) | 68.9 | 58.2 | 53.8 | 48.8 | 44.5 | 40.5 | 36.8 | 37.1 | 31.1 | 25.8 | 0.3 | 1.3 |
| | 51～100名 | (53) | 64.2 | 58.5 | 64.2 | 52.8 | 35.8 | 45.3 | 37.7 | 24.5 | 30.2 | 24.5 | - | - |
| | 101～1,000名 | (147) | 72.8 | 66.7 | 76.2 | 70.7 | 52.4 | 58.5 | 42.9 | 52.4 | 36.1 | 39.5 | - | - |
| | 1,001名以上 | (75) | 82.7 | 65.3 | 69.3 | 74.7 | 72.0 | 70.7 | 60.0 | 49.3 | 49.3 | 45.3 | 1.3 | 1.3 |

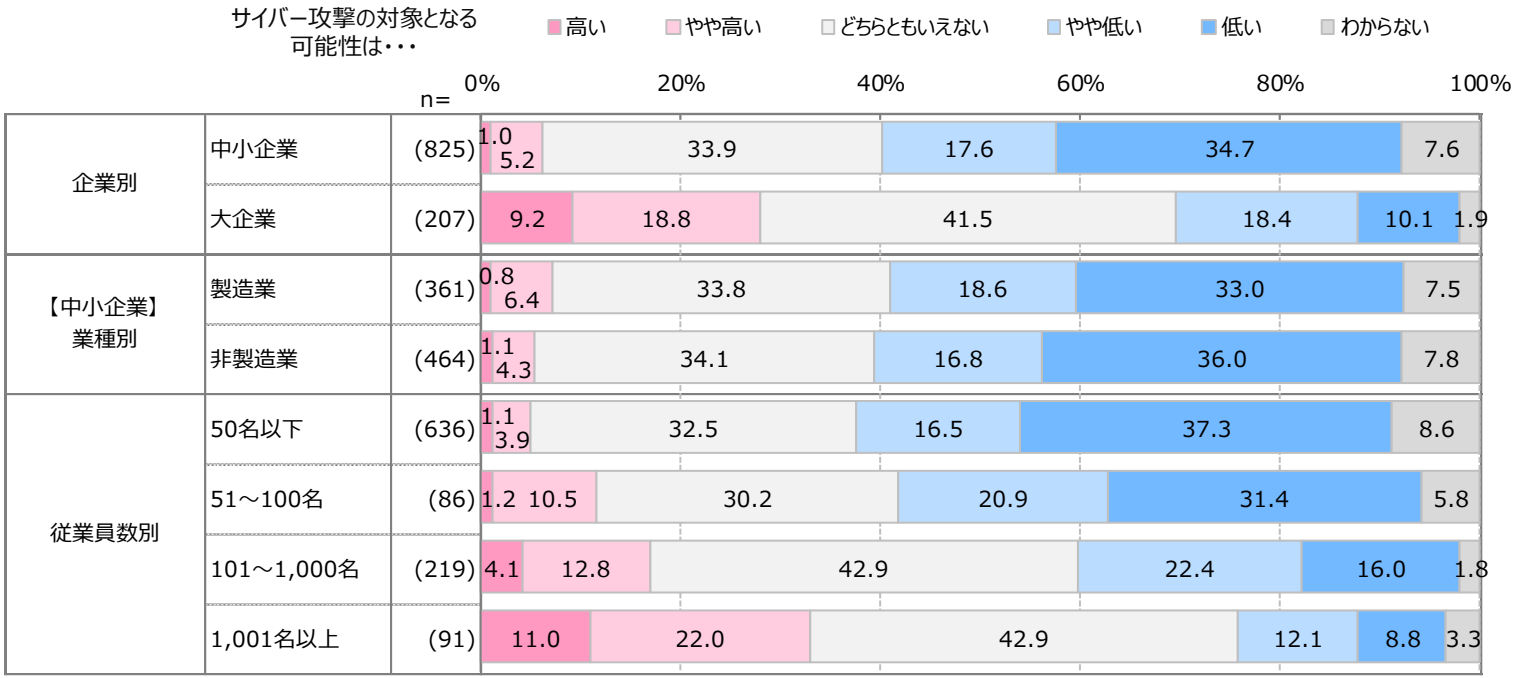
※「中小企業」のスコアで降順ソート

# （5）サイバー攻撃の対象となる可能性

- サイバー攻撃の対象となる可能性が高い（「高い」「やや高い」）と考えている中小企業の経営者は10%未満（6.2%）であり、大企業の経営者（28.0%）と比べて少ない。
- 従業員数別に見ると、企業規模が小さいほどサイバー攻撃の対象となる可能性が低い（「やや低い」「低い」）と考えている傾向が顕著。

Q5　貴社がサイバー攻撃の対象となる可能性は、どの程度あると考えていますか。

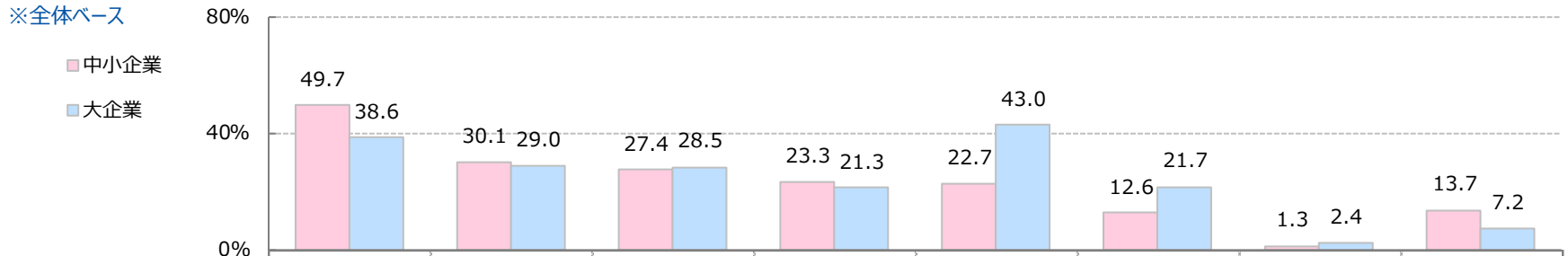
※全体ベース



# （6）サイバー攻撃の対象となる可能性の理由

- 中小企業の経営者の約半数が、サイバー攻撃の対象となる可能性に「自社の企業規模」が影響していると回答している。
- サイバー攻撃の対象となる可能性について、その理由を「個人情報の保有件数」「知的財産の保有状況」「取引先の数」と回答した経営者の割合は20%~30%前後であり、中小企業と大企業の間に大きな差はない。

Q6　貴社がサイバー攻撃の対象となる可能性について、【Q5の選択内容】と回答した理由はどれですか。あてはまるものをすべてお選びください。




| | | n= | 自社の企業規模（従業員数、資本金など）が大きいから／小さいから | 個人情報の保有件数が多いから／少ないから | 自社が知的財産（特許、その他高度な企業機密など）を保有しているから／いないから | 取引先の数が多いから／少ないから | 十分なセキュリティ対策を講じているから／いないから | 取引先に大企業や官公庁があるから／ないから | その他 | わからない・特に思い浮かぶものはない |
|---|---|---|---|---|---|---|---|---|---|---|
| 企業別 | 中小企業 | (825) | 49.7 | 30.1 | 27.4 | 23.3 | 22.7 | 12.6 | 1.3 | 13.7 |
| | 大企業 | (207) | 38.6 | 29.0 | 28.5 | 21.3 | 43.0 | 21.7 | 2.4 | 7.2 |
| 【中小企業】業種別 | 製造業 | (361) | 51.5 | 29.1 | 29.1 | 24.4 | 23.8 | 8.9 | 1.1 | 11.4 |
| | 非製造業 | (464) | 48.3 | 30.8 | 26.1 | 22.4 | 21.8 | 15.5 | 1.5 | 15.5 |
| 従業員数別 | 50名以下 | (636) | 51.6 | 32.2 | 28.6 | 24.2 | 19.8 | 12.6 | 1.3 | 14.8 |
| | 51～100名 | (86) | 48.8 | 22.1 | 17.4 | 17.4 | 29.1 | 11.6 | 1.2 | 9.3 |
| | 101～1,000名 | (219) | 38.4 | 28.3 | 28.8 | 19.2 | 37.0 | 16.4 | 1.8 | 8.2 |
| | 1,001名以上 | (91) | 39.6 | 24.2 | 27.5 | 27.5 | 48.4 | 25.3 | 3.3 | 8.8 |

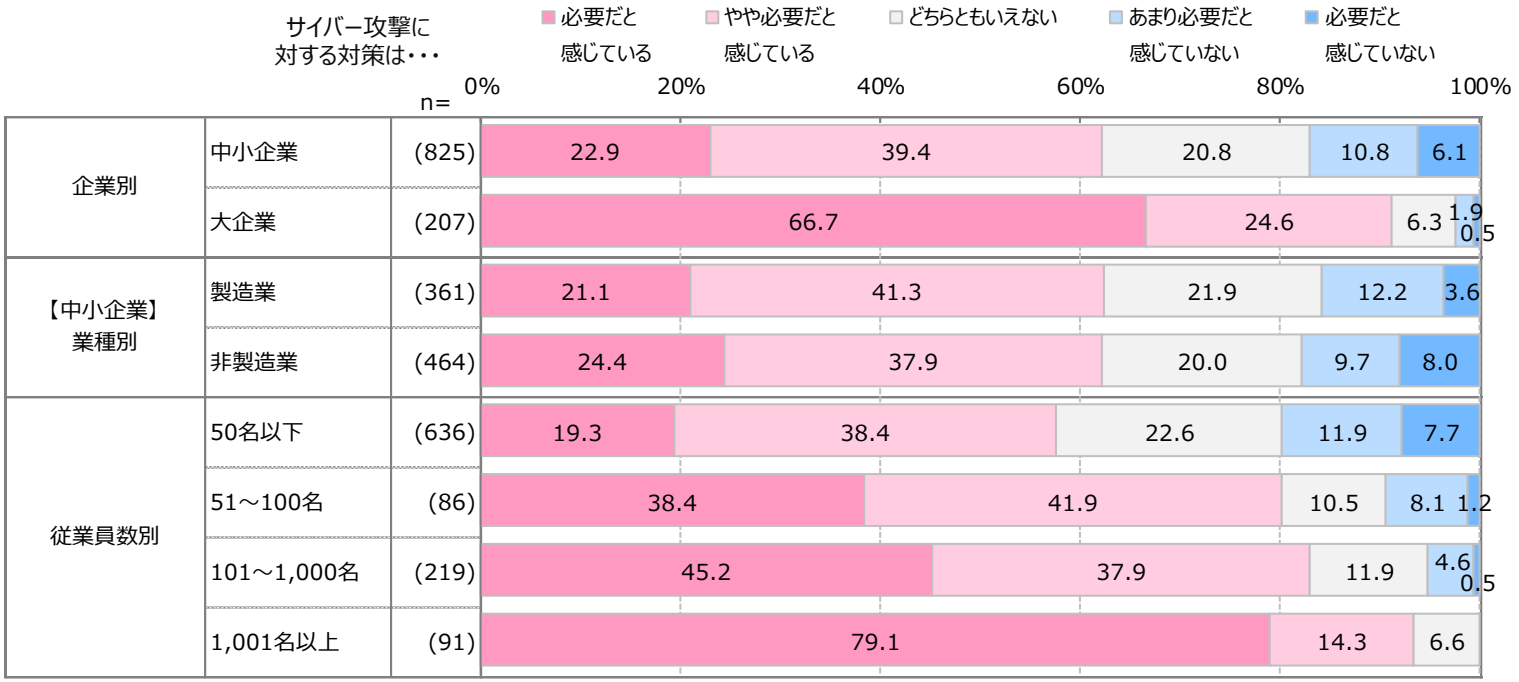
※「中小企業」のスコアで降順ソート

# （7）サイバー攻撃対策の必要性

- サイバー攻撃への対策が「必要だと感じている」と回答した中小企業の経営者は22.9%にとどまるが、大企業の経営者は約3倍の66.7%となっている。
- 従業員数別に見ると、企業規模が小さいほどサイバー攻撃への対策の必要性を感じている経営者が少ない傾向がある。

Q7　貴社において、サイバー攻撃に対する対策は、どの程度必要であると考えていますか。

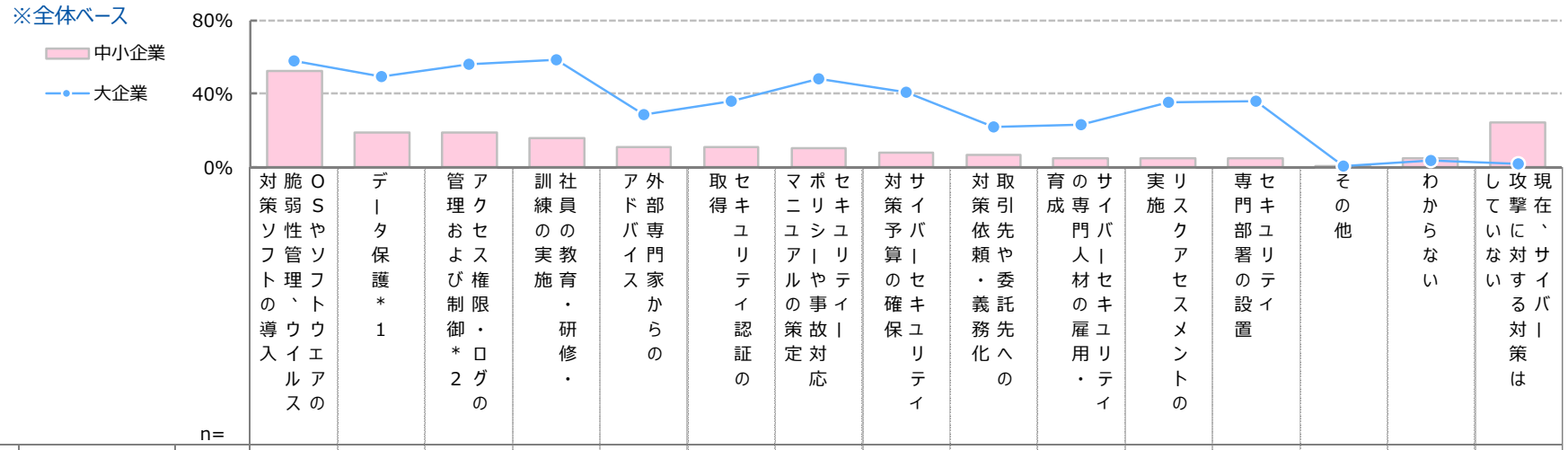
※全体ベース



# （8）サイバー攻撃への対策内容

- 中小企業の経営者の24.0%が「現在、サイバー攻撃に対する対策はしていない」と回答している。
- サイバー攻撃への対策を行っている中小企業の経営者の最も多い回答は「OSやソフトウェアの脆弱性管理、ウイルス対策ソフトの導入」であったが、52.4%にとどまった。

Q8　貴社では、現在、サイバー攻撃に対して対策を行っていますか。対策を行っている方は、その内容としてあてはまるものをすべてお選びください。




| | | n= | OSやソフトウェアの脆弱性管理、ウイルス対策ソフトの導入 | データ保護*1 | アクセス権限・ログの管理および制御*2 | 社員の教育・研修・訓練の実施 | 外部専門家からのアドバイス | セキュリティ認証の取得 | セキュリティポリシーや事故対応マニュアルの策定 | サイバーセキュリティ対策予算の確保 | 取引先や委託先への対策依頼・義務化 | サイバーセキュリティの専門人材の育成・雇用 | リスクアセスメントの実施 | セキュリティ専門部署の設置 | その他 | わからない | 現在、サイバー攻撃に対する対策はしていない |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 企業別 | 中小企業 | (825) | 52.4 | 19.0 | 18.8 | 15.9 | 11.0 | 10.9 | 10.5 | 8.1 | 6.4 | 4.8 | 4.7 | 4.7 | 0.6 | 4.8 | 24.0 |
| | 大企業 | (207) | 58.0 | 49.3 | 56.0 | 58.5 | 28.5 | 35.7 | 47.8 | 40.6 | 21.7 | 23.2 | 35.3 | 35.7 | 0.5 | 3.9 | 1.9 |
| 【中小企業】業種別 | 製造業 | (361) | 55.1 | 20.2 | 18.8 | 15.2 | 11.4 | 11.6 | 7.5 | 7.5 | 4.4 | 4.7 | 5.3 | 5.0 | 0.6 | 4.4 | 21.9 |
| | 非製造業 | (464) | 50.2 | 18.1 | 18.8 | 16.4 | 10.8 | 10.3 | 12.9 | 8.6 | 8.0 | 5.0 | 4.3 | 4.5 | 0.6 | 5.2 | 25.6 |
| 従業員数別 | 50名以下 | (636) | 49.7 | 16.5 | 14.8 | 13.2 | 9.9 | 8.6 | 7.1 | 6.1 | 6.0 | 3.1 | 3.8 | 2.8 | 0.6 | 5.3 | 27.2 |
| | 51～100名 | (86) | 59.3 | 25.6 | 29.1 | 19.8 | 15.1 | 14.0 | 23.3 | 17.4 | 8.1 | 8.1 | 3.5 | 9.3 | 1.2 | 2.3 | 16.3 |
| | 101～1,000名 | (219) | 60.3 | 37.0 | 43.4 | 42.0 | 19.2 | 26.0 | 32.0 | 23.3 | 13.7 | 15.1 | 20.5 | 18.7 | - | 4.1 | 6.4 |
| | 1,001名以上 | (91) | 58.2 | 56.0 | 62.6 | 64.8 | 35.2 | 44.0 | 56.0 | 50.5 | 25.3 | 30.8 | 44.0 | 50.5 | 1.1 | 3.3 | 1.1 |

*1（暗号化・DLPなど）　*2（リモートアクセス、モバイルデバイス含む）

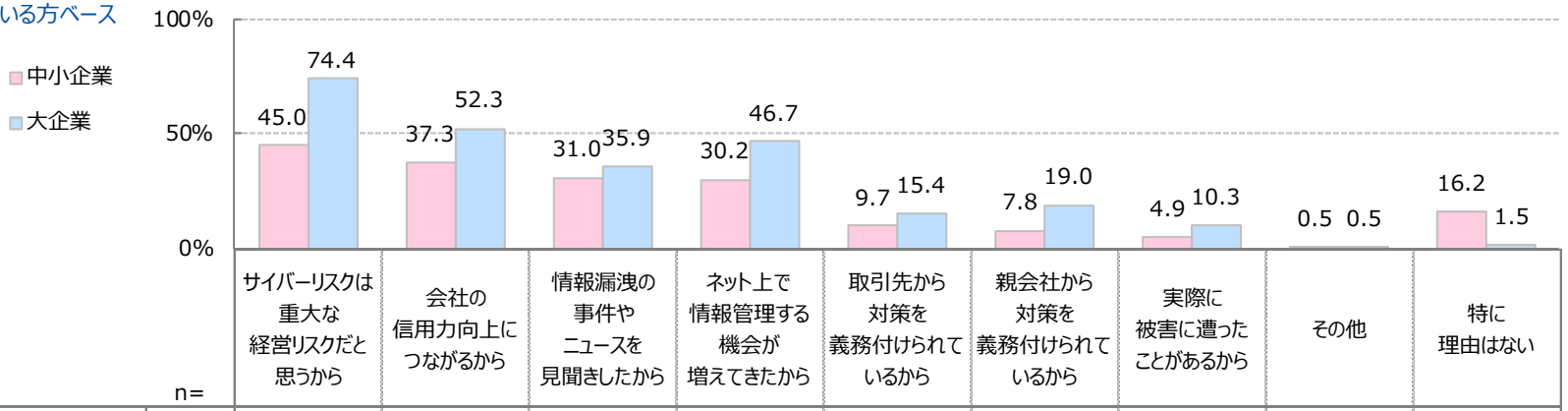
※「中小企業」のスコアで降順ソート

# （9）サイバー攻撃への対策を行っている理由

- 対策を行う理由として、中小企業の経営者の45.0%が「サイバーリスクは重大な経営リスクだと思うから」と回答している。
- 従業員数別に見ると、企業規模が大きいほどサイバー攻撃に起因する経営リスクの顕在化や会社の信用力の毀損に対する危機意識が強く影響している傾向がある。
- 「取引先から対策を義務付けられているから」は9.7%、「親会社から対策を義務付けられているから」は7.8%にとどまった。

Q9　現在、サイバー攻撃に対する対策を行っている方にお伺いします。貴社でサイバー攻撃の対策を行っている理由として、あてはまるものをすべてお選びください。

※現在、サイバー攻撃に対する対策を行っている方ベース




| | | n= | サイバーリスクは重大な経営リスクだと思うから | 会社の信用力向上につながるから | 情報漏洩の事件やニュースを見聞きしたから | ネット上で情報管理する機会が増えてきたから | 取引先から対策を義務付けられているから | 親会社から対策を義務付けられているから | 実際に被害に遭ったことがあるから | その他 | 特に理由はない |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 企業別 | 中小企業 | (587) | 45.0 | 37.3 | 31.0 | 30.2 | 9.7 | 7.8 | 4.9 | 0.5 | 16.2 |
| | 大企業 | (195) | 74.4 | 52.3 | 35.9 | 46.7 | 15.4 | 19.0 | 10.3 | 0.5 | 1.5 |
| 【中小企業】業種別 | 製造業 | (266) | 41.4 | 35.3 | 28.9 | 29.3 | 9.0 | 6.8 | 6.4 | 0.8 | 19.9 |
| | 非製造業 | (321) | 48.0 | 38.9 | 32.7 | 30.8 | 10.3 | 8.7 | 3.7 | 0.3 | 13.1 |
| 従業員数別 | 50名以下 | (429) | 41.3 | 36.8 | 30.8 | 28.9 | 7.7 | 6.5 | 3.7 | 0.7 | 18.9 |
| | 51～100名 | (70) | 50.0 | 42.9 | 35.7 | 38.6 | 18.6 | 10.0 | 7.1 | - | 8.6 |
| | 101～1,000名 | (196) | 65.8 | 44.9 | 30.1 | 40.3 | 14.8 | 17.9 | 7.7 | - | 5.1 |
| | 1,001名以上 | (87) | 78.2 | 51.7 | 41.4 | 43.7 | 13.8 | 14.9 | 14.9 | 1.1 | 1.1 |

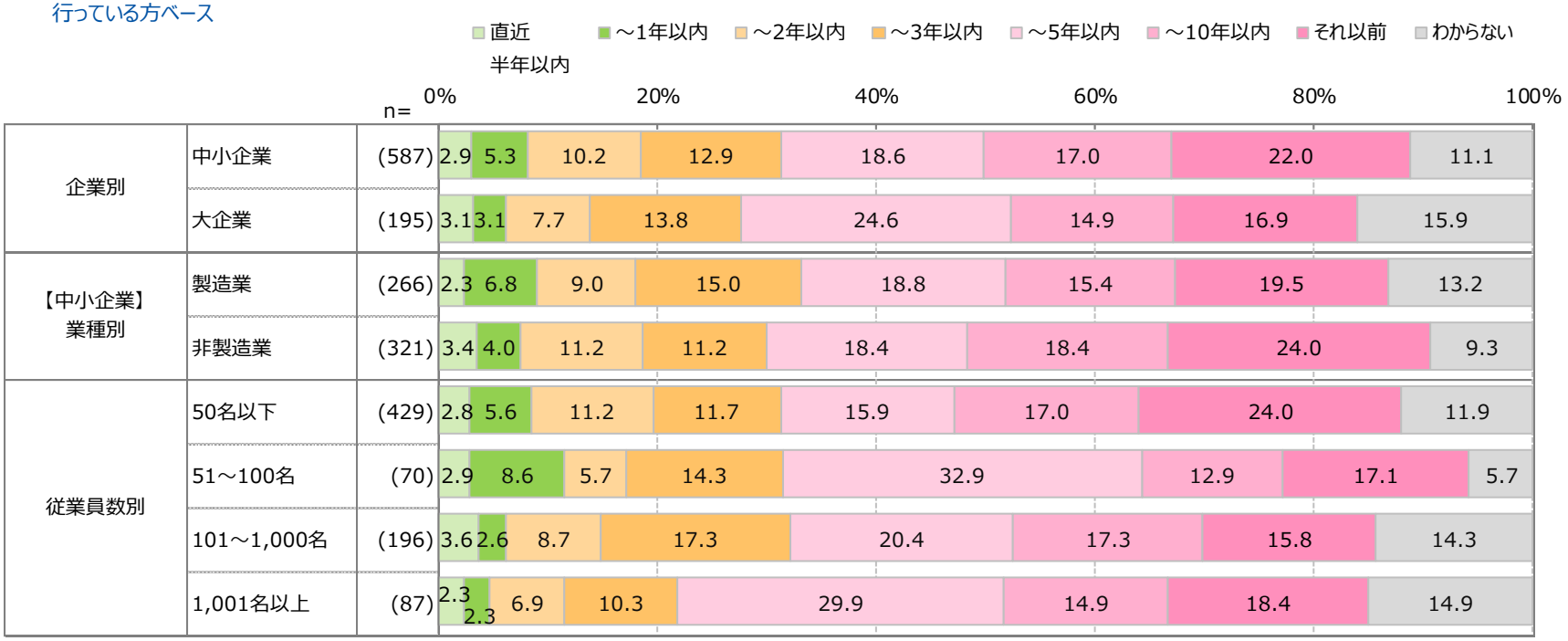
※「中小企業」のスコアで降順ソート

# （１０）サイバー攻撃への対策を開始した時期

- 中小企業の経営者の22.0%が「10年以上前から対策を行っている」と回答している。
- 中小企業と大企業において、対策開始時期に大きな違いは見られない。

Q10　現在、サイバー攻撃に対する対策を行っている方にお伺いします。貴社において、サイバー攻撃の対策を開始した時期をお選びください。

※現在、サイバー攻撃に対する対策を行っている方ベース



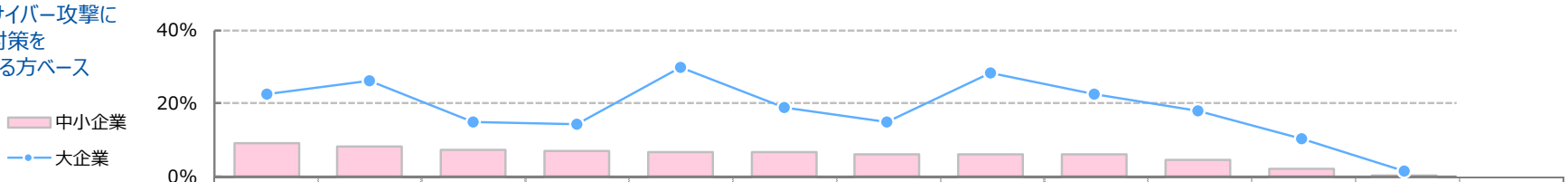

| | | n= | 直近半年以内 | ～1年以内 | ～2年以内 | ～3年以内 | ～5年以内 | ～10年以内 | それ以前 | わからない |
|---|---|---|---|---|---|---|---|---|---|---|
| 企業別 | 中小企業 | (587) | 2.9 | 5.3 | 10.2 | 12.9 | 18.6 | 17.0 | 22.0 | 11.1 |
| | 大企業 | (195) | 3.1 | 3.1 | 7.7 | 13.8 | 24.6 | 14.9 | 16.9 | 15.9 |
| 【中小企業】業種別 | 製造業 | (266) | 2.3 | 6.8 | 9.0 | 15.0 | 18.8 | 15.4 | 19.5 | 13.2 |
| | 非製造業 | (321) | 3.4 | 4.0 | 11.2 | 11.2 | 18.4 | 18.4 | 24.0 | 9.3 |
| 従業員数別 | 50名以下 | (429) | 2.8 | 5.6 | 11.2 | 11.7 | 15.9 | 17.0 | 24.0 | 11.9 |
| | 51～100名 | (70) | 2.9 | 8.6 | 5.7 | 14.3 | 32.9 | 12.9 | 17.1 | 5.7 |
| | 101～1,000名 | (196) | 3.6 | 2.6 | 8.7 | 17.3 | 20.4 | 17.3 | 15.8 | 14.3 |
| | 1,001名以上 | (87) | 2.3 | 2.3 | 6.9 | 10.3 | 29.9 | 14.9 | 18.4 | 14.9 |

# （１１）サイバー攻撃への対策に関するKPI設定有無

- 中小企業の経営者の70%以上が「特にKPIは設定していない」と回答している。
- KPIを設定している中小企業の経営者のうち、最も多かった回答は「セキュリティ投資額」となった。一方、大企業の経営者は「セキュリティ教育の受講率・受講回数」や「サイバー演習・標準型セキュリティ研修の状況」など、サイバーリスクに対する全社員の対応力向上に関する回答が多かった。

Q11　現在、サイバー攻撃に対する対策を行っている方にお伺いします。貴社では、サイバー攻撃に対する対策について、KPI（重要業績指標）を設定していますか。設定している場合、その内容としてあてはまるものをすべてお選びください。

※現在、サイバー攻撃に対する対策を行っている方ベース




| | | n= | セキュリティ投資額 | 法規制やガイドラインの準拠率 | 脆弱性発覚から対応完了までの平均時間・工数 | 外部委託先の監督進捗率 | セキュリティ教育の受講率・受講回数 | サイバー攻撃による被害発生から対応完了までの平均時間・工数 | 情報資産の棚卸進捗率 | サイバー演習・標的型セキュリティ研修の状況 | 事故対応手順の全社展開率 | サイバーセキュリティ関連の有資格者数・資格者率 | 監督官庁の指摘事項の対応完了率 | その他 | 特にKPIは設定していない |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 企業別 | 中小企業 | (587) | 9.2 | 8.2 | 7.3 | 7.0 | 6.8 | 6.8 | 6.1 | 6.1 | 6.0 | 4.4 | 2.2 | 0.2 | 72.1 |
| | 大企業 | (195) | 22.6 | 26.2 | 14.9 | 14.4 | 29.7 | 19.0 | 14.9 | 28.2 | 22.6 | 17.9 | 10.3 | 1.5 | 39.5 |
| 【中小企業】業種別 | 製造業 | (266) | 7.9 | 6.0 | 6.4 | 6.8 | 6.0 | 6.0 | 3.8 | 5.3 | 5.3 | 4.1 | 0.8 | - | 74.1 |
| | 非製造業 | (321) | 10.3 | 10.0 | 8.1 | 7.2 | 7.5 | 7.5 | 8.1 | 6.9 | 6.5 | 4.7 | 3.4 | 0.3 | 70.4 |
| 従業員数別 | 50名以下 | (429) | 7.9 | 7.2 | 7.0 | 4.9 | 5.1 | 5.6 | 4.7 | 4.7 | 3.5 | 4.7 | 1.6 | 0.2 | 75.3 |
| | 51～100名 | (70) | 11.4 | 8.6 | 5.7 | 11.4 | 14.3 | 8.6 | 14.3 | 10.0 | 12.9 | 4.3 | 4.3 | - | 61.4 |
| | 101～1,000名 | (196) | 16.3 | 17.9 | 10.7 | 15.8 | 19.4 | 13.3 | 10.7 | 17.9 | 15.8 | 8.2 | 5.6 | - | 53.6 |
| | 1,001名以上 | (87) | 27.6 | 31.0 | 19.5 | 10.3 | 32.2 | 24.1 | 16.1 | 33.3 | 27.6 | 25.3 | 13.8 | 3.4 | 33.3 |

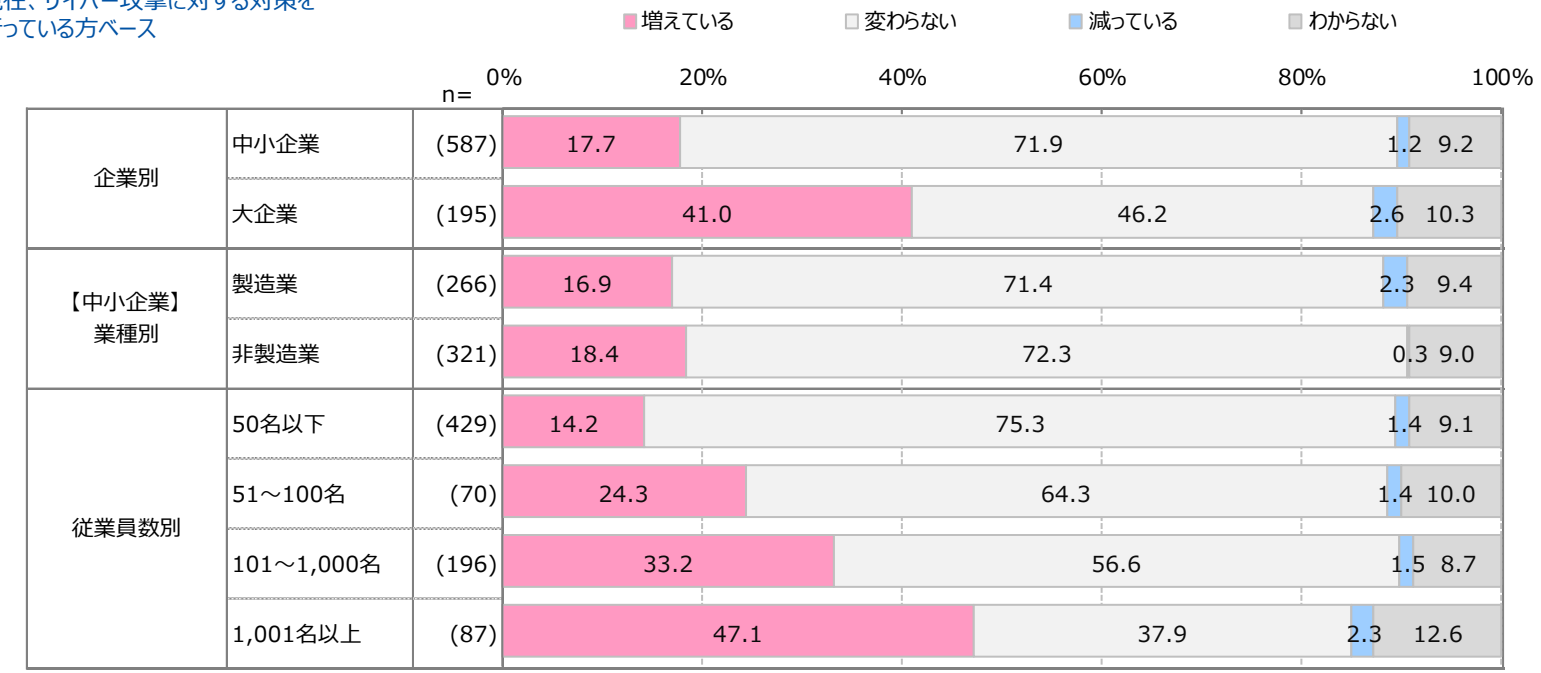
※「中小企業」のスコアで降順ソート

# （１２）サイバー攻撃への対策にかける投資額の変化

- ２年前と比べて対策にかける投資額が「増えている」と回答した中小企業の経営者は17.7%。一方、約70%は「変わらない」と回答している。
- 従業員数別に見ると、企業規模が大きいほど投資額が「増えている」の回答が多い。

Q12　現在、サイバー攻撃に対する対策を行っている方にお伺いします。
貴社において、2年前と比べてサイバー攻撃の対策にかける投資額は増えましたか。

※現在、サイバー攻撃に対する対策を行っている方ベース



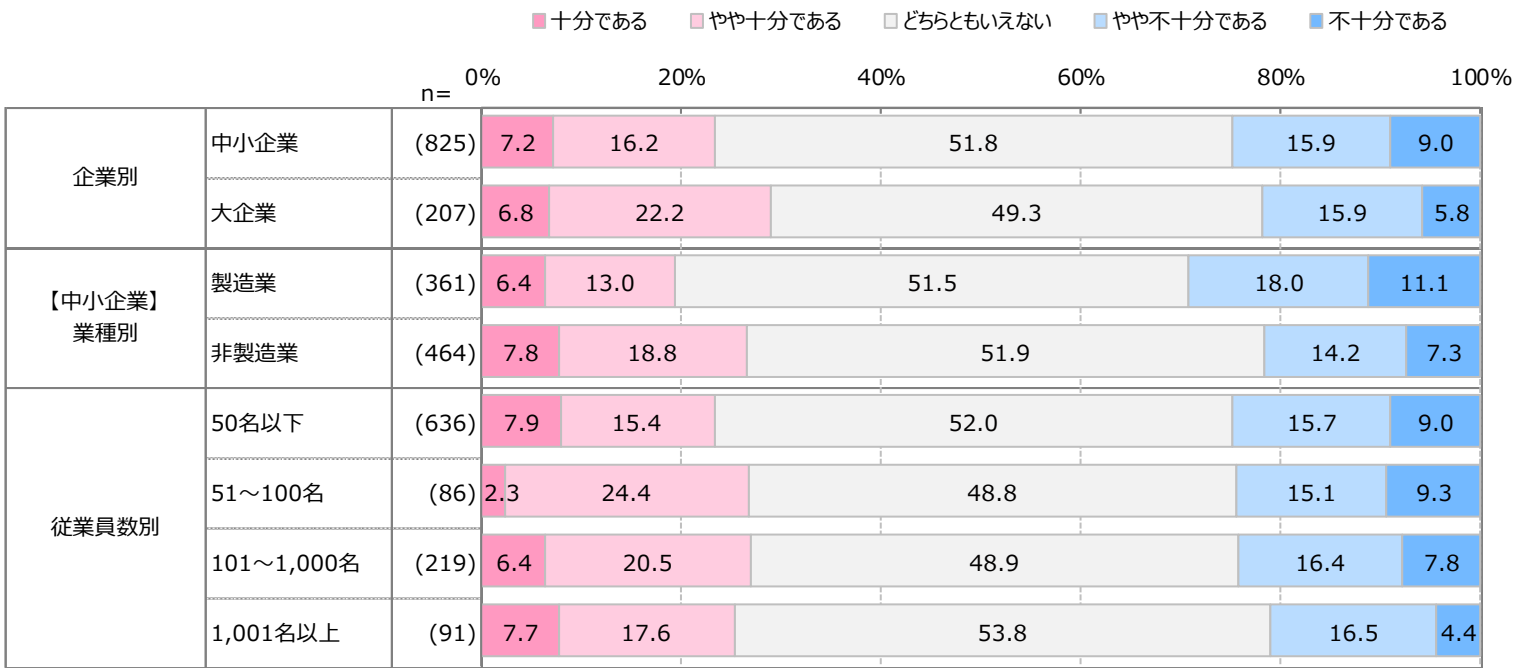

| | | n= | 増えている | 変わらない | 減っている | わからない |
|---|---|---|---|---|---|---|
| 企業別 | 中小企業 | (587) | 17.7 | 71.9 | 1.2 | 9.2 |
| | 大企業 | (195) | 41.0 | 46.2 | 2.6 | 10.3 |
| 【中小企業】業種別 | 製造業 | (266) | 16.9 | 71.4 | 2.3 | 9.4 |
| | 非製造業 | (321) | 18.4 | 72.3 | 0.3 | 9.0 |
| 従業員数別 | 50名以下 | (429) | 14.2 | 75.3 | 1.4 | 9.1 |
| | 51～100名 | (70) | 24.3 | 64.3 | 1.4 | 10.0 |
| | 101～1,000名 | (196) | 33.2 | 56.6 | 1.5 | 8.7 |
| | 1,001名以上 | (87) | 47.1 | 37.9 | 2.3 | 12.6 |

# （１３）サイバー攻撃の対策は十分か

- サイバーセキュリティ対応が「十分である」と回答した中小企業の経営者は7.2%にとどまる。
- 「どちらともいえない」を含めると、中小企業の経営者の70%以上は自社のサイバーセキュリティ対応が十分とはいえないと認識している。
- 企業規模を問わず、「どちらともいえない」の回答が半数近くを占めている。

Q13　貴社のサイバーセキュリティ対応について、現在の対応・対策で十分だと感じていますか。

※全体ベース



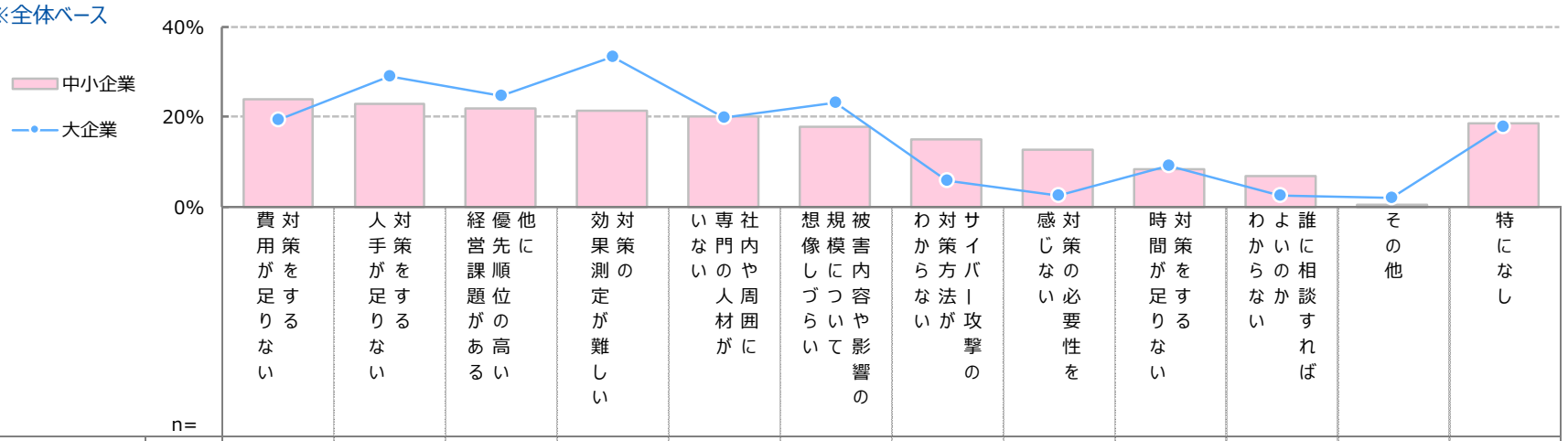

| | | n= | 十分である | やや十分である | どちらともいえない | やや不十分である | 不十分である |
|---|---|---|---|---|---|---|---|
| 企業別 | 中小企業 | (825) | 7.2 | 16.2 | 51.8 | 15.9 | 9.0 |
| | 大企業 | (207) | 6.8 | 22.2 | 49.3 | 15.9 | 5.8 |
| 【中小企業】業種別 | 製造業 | (361) | 6.4 | 13.0 | 51.5 | 18.0 | 11.1 |
| | 非製造業 | (464) | 7.8 | 18.8 | 51.9 | 14.2 | 7.3 |
| 従業員数別 | 50名以下 | (636) | 7.9 | 15.4 | 52.0 | 15.7 | 9.0 |
| | 51～100名 | (86) | 2.3 | 24.4 | 48.8 | 15.1 | 9.3 |
| | 101～1,000名 | (219) | 6.4 | 20.5 | 48.9 | 16.4 | 7.8 |
| | 1,001名以上 | (91) | 7.7 | 17.6 | 53.8 | 16.5 | 4.4 |

# （１４）サイバー攻撃への対策の課題

- 中小企業の経営者は、費用や対応人員の不足、他に優先順位の高い経営課題があること、効果測定が難しいことなどを課題として挙げており、多岐に渡っている。
- 大企業の経営者と比べ、「サイバー攻撃の対策方法がわからない」「誰に相談すればよいのかわからない」と回答した中小企業の経営者が多く、サイバー攻撃の対策の進め方がイメージできていない実態が顕著となった。

Q14　サイバー攻撃への対策を進めるうえで、貴社の課題は何ですか。あてはまるものをすべてお選びください。

※全体ベース



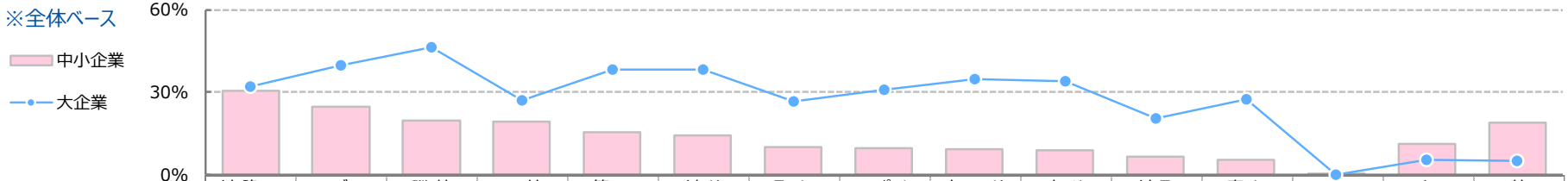

| | | n= | 費用が足りない | 対策をする人手が足りない | 他に優先順位の高い経営課題がある | 対策の効果測定が難しい | 社内や周囲に専門の人材がいない | 被害内容や影響の規模について想像しづらい | サイバー攻撃の対策方法がわからない | 対策の必要性を感じない | 対策をする時間が足りない | 誰に相談すればよいのかわからない | その他 | 特になし |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 企業別 | 中小企業 | (825) | 24.0 | 23.0 | 21.8 | 21.5 | 20.0 | 17.9 | 15.0 | 12.6 | 8.5 | 6.8 | 0.5 | 18.7 |
| | 大企業 | (207) | 19.3 | 29.0 | 24.6 | 33.3 | 19.8 | 23.2 | 5.8 | 2.4 | 9.2 | 2.4 | 1.9 | 17.9 |
| 【中小企業】業種別 | 製造業 | (361) | 24.4 | 24.9 | 24.7 | 22.7 | 23.8 | 23.0 | 13.9 | 11.9 | 8.6 | 7.8 | 0.6 | 18.3 |
| | 非製造業 | (464) | 23.7 | 21.6 | 19.6 | 20.5 | 17.0 | 14.0 | 15.9 | 13.1 | 8.4 | 6.0 | 0.4 | 19.0 |
| 従業員数別 | 50名以下 | (636) | 25.3 | 18.7 | 21.5 | 17.5 | 17.6 | 16.8 | 15.3 | 14.5 | 8.6 | 7.5 | 0.5 | 21.7 |
| | 51～100名 | (86) | 14.0 | 33.7 | 17.4 | 33.7 | 20.9 | 23.3 | 17.4 | 5.8 | 5.8 | 5.8 | 1.2 | 12.8 |
| | 101～1,000名 | (219) | 20.5 | 32.4 | 28.3 | 32.4 | 27.4 | 20.1 | 9.1 | 4.6 | 8.2 | 3.2 | 1.4 | 12.8 |
| | 1,001名以上 | (91) | 22.0 | 34.1 | 18.7 | 38.5 | 17.6 | 27.5 | 4.4 | 2.2 | 12.1 | 1.1 | 1.1 | 15.4 |

※「中小企業」のスコアで降順ソート

# （１５）サイバーセキュリティについて今後打つべき対策

- 今後打つべき対策として、中小企業の経営者は「OSやソフトウェアの脆弱性管理、ウイルス対策ソフトの導入」の回答が最も多かった。一方、大企業は「社員の教育・研修・訓練の実施」と回答した経営者が最も多く、46.4%となっている（中小企業の経営者は19.6%）。
- 中小企業の経営者の19.0%は「特になし」と回答している。

Q15　貴社のサイバーセキュリティ対応について、今後どのような対策を打つべきだと思いますか。あてはまるものをすべてお選びください。




| | | n= | OSやソフトウェアの脆弱性管理、ウイルス対策ソフトの導入 | データ保護*1 | 社員の教育・研修・訓練の実施 | 外部専門家からのアドバイス | アクセス権限・ログの管理および制御*2 | サイバーセキュリティ対策予算の確保 | セキュリティ認証の取得 | セキュリティインシデントや事故対応マニュアルの策定 | サイバーセキュリティの専門人材の雇用・育成 | リスクアセスメントの実施 | 取引先や委託先への対策依頼・義務化 | セキュリティ専門部署の設置 | その他 | わからない | 特になし |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 企業別 | 中小企業 | (825) | 30.5 | 24.5 | 19.6 | 19.3 | 15.3 | 14.4 | 9.8 | 9.6 | 9.3 | 9.0 | 6.7 | 5.5 | 0.4 | 11.3 | 19.0 |
| | 大企業 | (207) | 31.9 | 39.6 | 46.4 | 27.1 | 38.2 | 38.2 | 26.6 | 30.9 | 34.8 | 33.8 | 20.3 | 27.5 | - | 5.3 | 4.8 |
| 【中小企業】業種別 | 製造業 | (361) | 33.8 | 24.7 | 23.0 | 19.4 | 16.6 | 15.5 | 9.1 | 10.2 | 10.8 | 10.0 | 4.2 | 5.5 | 0.3 | 10.0 | 17.2 |
| | 非製造業 | (464) | 28.0 | 24.4 | 17.0 | 19.2 | 14.2 | 13.6 | 10.3 | 9.1 | 8.2 | 8.2 | 8.6 | 5.4 | 0.4 | 12.3 | 20.5 |
| 従業員数別 | 50名以下 | (636) | 29.9 | 23.4 | 14.5 | 17.3 | 13.5 | 11.8 | 8.8 | 6.9 | 5.8 | 5.7 | 5.7 | 4.1 | 0.5 | 12.7 | 22.3 |
| | 51～100名 | (86) | 30.2 | 23.3 | 32.6 | 22.1 | 18.6 | 17.4 | 10.5 | 15.1 | 15.1 | 15.1 | 9.3 | 8.1 | - | 10.5 | 12.8 |
| | 101～1,000名 | (219) | 30.6 | 36.5 | 42.9 | 26.9 | 28.3 | 28.8 | 20.1 | 21.9 | 27.9 | 26.0 | 12.3 | 17.8 | - | 5.0 | 3.7 |
| | 1,001名以上 | (91) | 38.5 | 38.5 | 48.4 | 29.7 | 45.1 | 49.5 | 29.7 | 41.8 | 41.8 | 41.8 | 28.6 | 33.0 | - | 3.3 | 6.6 |

*1（暗号化・DLPなど）　*2（リモートアクセス、モバイルデバイス含む）

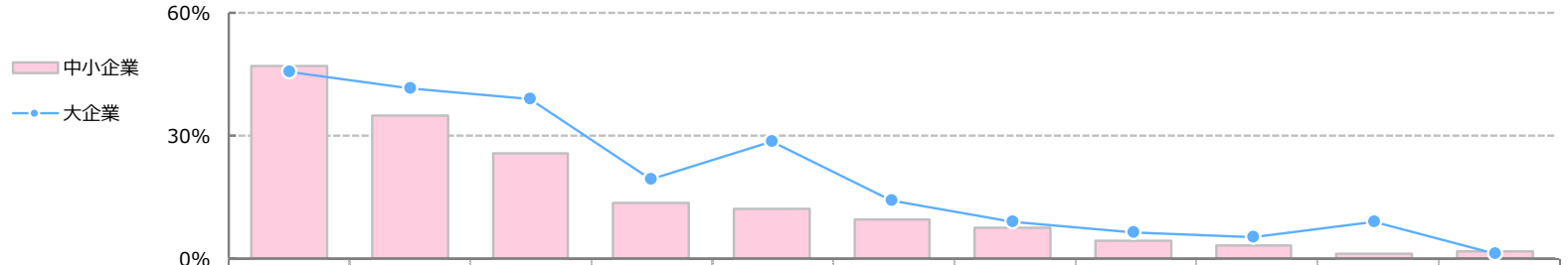
※「中小企業」のスコアで降順ソート

# （１６）サイバー攻撃の被害経験【被害ありベース】

- 中小企業の経営者の約2割（825人中155人）が何らかの被害に遭ったと回答している。
- 特に多かった被害は「不正送金を促すビジネスメール詐欺やフィッシングサイト」（47.1%）、「マルウェア」（34.8%）、「ランサムウェア」（25.8%）となった。

Q16　貴社では、サイバー攻撃の被害を受けたことはありますか。実際に被害に遭った経験がある場合は、その被害内容をすべてお選びください。

※サイバー攻撃被害者ベース




| | | n= | 不正送金を促すビジネスメール詐欺やフィッシングサイト | マルウェア | ランサムウェア | Webサービスへの不正ログイン・情報窃取およびWebサイトの改ざん | 標的型攻撃 | 制御システムに対する攻撃 | DDoS（サービス妨害）攻撃 | PWリスト攻撃 | IoTデバイスに対する攻撃 | ゼロデイ攻撃 | その他 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 企業別 | 中小企業 | (155) | 47.1 | 34.8 | 25.8 | 13.5 | 12.3 | 9.7 | 7.7 | 4.5 | 3.2 | 1.3 | 1.9 |
| | 大企業 | (77) | 45.5 | 41.6 | 39.0 | 19.5 | 28.6 | 14.3 | 9.1 | 6.5 | 5.2 | 9.1 | 1.3 |
| 【中小企業】業種別 | 製造業 | (79) | 44.3 | 31.6 | 24.1 | 12.7 | 12.7 | 12.7 | 6.3 | 1.3 | 2.5 | - | 1.3 |
| | 非製造業 | (76) | 50.0 | 38.2 | 27.6 | 14.5 | 11.8 | 6.6 | 9.2 | 7.9 | 3.9 | 2.6 | 2.6 |
| 従業員数別 | 50名以下 | (99) | 44.4 | 39.4 | 26.3 | 13.1 | 12.1 | 10.1 | 7.1 | 5.1 | 1.0 | 1.0 | 3.0 |
| | 51～100名 | (25) | 52.0 | 20.0 | 32.0 | 20.0 | 12.0 | 8.0 | 12.0 | - | 12.0 | 4.0 | - |
| | 101～1,000名 | (60) | 48.3 | 35.0 | 26.7 | 11.7 | 20.0 | 11.7 | 10.0 | 6.7 | 1.7 | 5.0 | 1.7 |
| | 1,001名以上 | (48) | 45.8 | 43.8 | 41.7 | 22.9 | 29.2 | 14.6 | 6.3 | 6.3 | 8.3 | 8.3 | - |

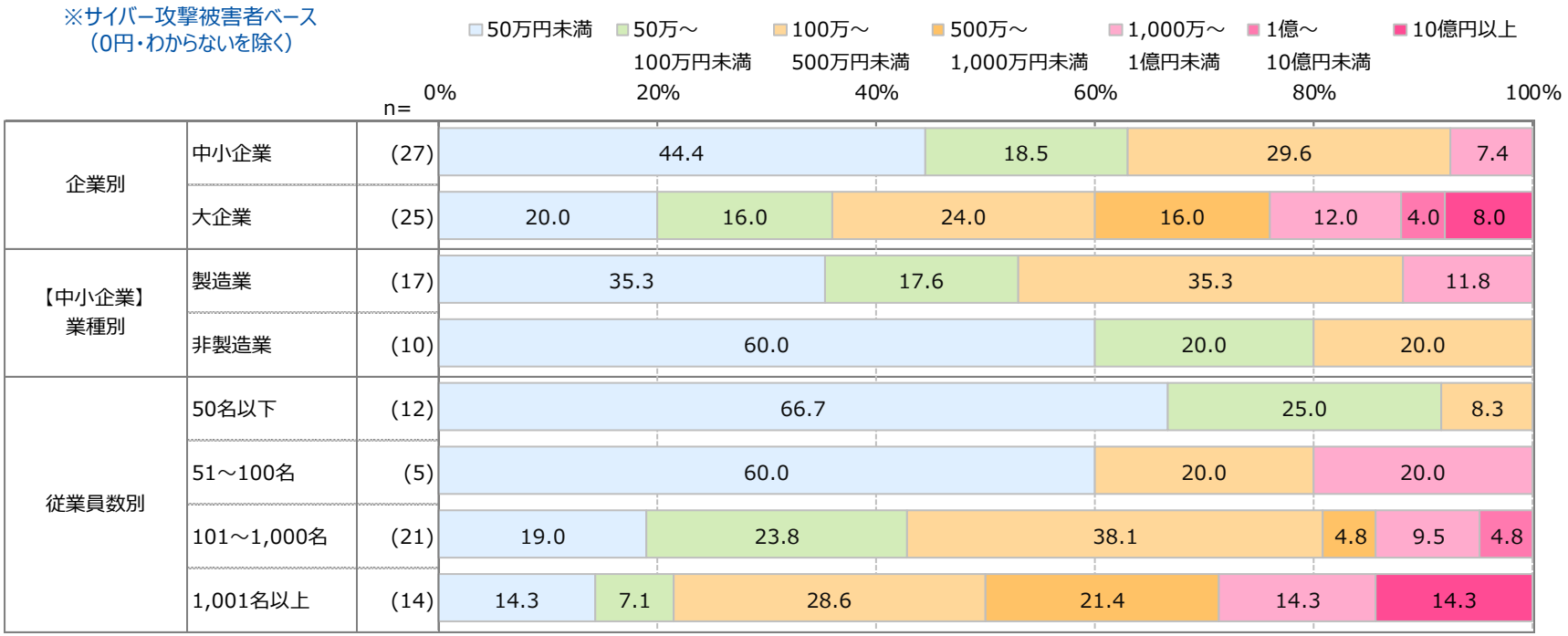
※「中小企業」のスコアで降順ソート

# （１７）サイバー攻撃による被害額

■ 中小企業の経営者によれば、サイバー攻撃による被害総額は「50万円未満」の回答が最も多かったが、「1,000万～1億円未満」の被害を受けた事例も発生していることがわかった。

Q17 以前に、サイバー攻撃の被害に遭ったことがある方にお伺いします。被害として金銭的被害があった場合には、その被害総額をお答えください。
※これまでに複数回被害に遭った場合には、最も大きかった被害についてお考えください。

※サイバー攻撃被害者ベース
（0円・わからないを除く）



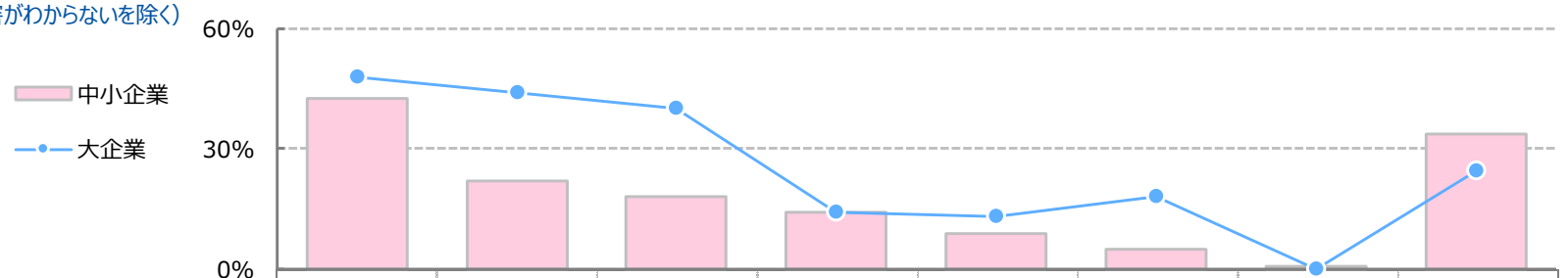

| | | n= | 50万円未満 | 50万～100万円未満 | 100万～500万円未満 | 500万～1,000万円未満 | 1,000万～1億円未満 | 1億～10億円未満 | 10億円以上 |
|---|---|---|---|---|---|---|---|---|---|
| 企業別 | 中小企業 | (27) | 44.4 | 18.5 | 29.6 | | | | 7.4 |
| | 大企業 | (25) | 20.0 | 16.0 | 24.0 | 16.0 | 12.0 | 4.0 | 8.0 |
| 【中小企業】業種別 | 製造業 | (17) | 35.3 | 17.6 | 35.3 | | | | 11.8 |
| | 非製造業 | (10) | 60.0 | | | 20.0 | | 20.0 | |
| 従業員数別 | 50名以下 | (12) | 66.7 | | | 25.0 | | | 8.3 |
| | 51～100名 | (5) | 60.0 | | | 20.0 | | 20.0 | |
| | 101～1,000名 | (21) | 19.0 | 23.8 | 38.1 | | 4.8 | 9.5 | 4.8 |
| | 1,001名以上 | (14) | 14.3 | 7.1 | 28.6 | 21.4 | 14.3 | | 14.3 |

# （１８）サイバー攻撃の被害に遭った際に苦労した点

- 中小企業の経営者にとって、サイバー攻撃の被害直後に苦労したことは「復旧対応」が最も多かった（42.6%）。
- 従業員数別に見ると、企業規模が大きいほど「影響範囲の特定」「社内・社外への周知」といった回答が多かった。

Q18　引き続き、以前に、サイバー攻撃の被害に遭ったことがある方にお伺いします。
被害直後の対応で苦労したことがあれば、あてはまるものをすべてお選びください。

※サイバー攻撃被害者ベース
（被害がわからないを除く）




| | | n= | 復旧対応 | 影響範囲の特定 | 社内・社外への周知 | 対応人員の手配 | 対応資金の確保 | 謝罪対応 | その他 | 特になし |
|---|---|---|---|---|---|---|---|---|---|---|
| 企業別 | 中小企業 | (155) | 42.6 | 21.9 | 18.1 | 14.2 | 9.0 | 5.2 | 0.6 | 33.5 |
| | 大企業 | (77) | 48.1 | 44.2 | 40.3 | 14.3 | 13.0 | 18.2 | - | 24.7 |
| 【中小企業】業種別 | 製造業 | (79) | 45.6 | 17.7 | 16.5 | 15.2 | 7.6 | 5.1 | 1.3 | 31.6 |
| | 非製造業 | (76) | 39.5 | 26.3 | 19.7 | 13.2 | 10.5 | 5.3 | - | 35.5 |
| 従業員数別 | 50名以下 | (99) | 34.3 | 17.2 | 14.1 | 9.1 | 8.1 | 4.0 | 1.0 | 38.4 |
| | 51～100名 | (25) | 56.0 | 20.0 | 20.0 | 16.0 | 20.0 | 8.0 | - | 24.0 |
| | 101～1,000名 | (60) | 51.7 | 38.3 | 33.3 | 20.0 | 5.0 | 15.0 | - | 25.0 |
| | 1,001名以上 | (48) | 50.0 | 47.9 | 41.7 | 16.7 | 16.7 | 14.6 | - | 25.0 |

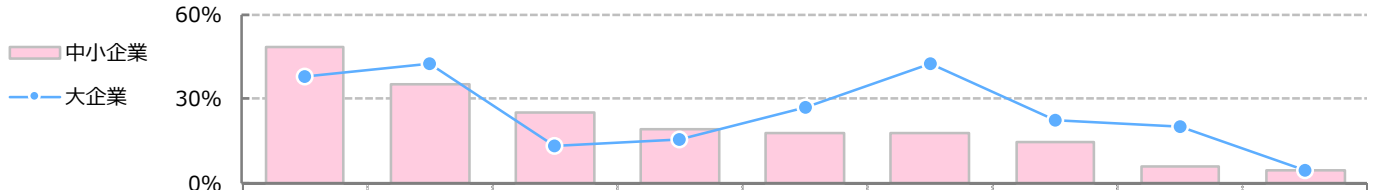
※「中小企業」のスコアで降順ソート

# （１９）サイバー攻撃の被害に遭った際の影響【被害後影響ありベース】

- 被害に遭った後の自社内の影響として、中小企業の経営者の回答は「原因の調査・復旧対応にかかる費用の捻出」が最も多かった。
- 「社会的評価の低下」「取引先・顧客への損害賠償」といった回答は、企業規模が大きいほど多かった。

Q19　引き続き、以前に、サイバー攻撃の被害に遭ったことがある方にお伺いします。
被害に遭った後の貴社内の影響について、あてはまるものをすべてお選びください。

※サイバー攻撃被害者ベース
（被害がわからないを除く）




| | | n= | 原因の調査・復旧対応にかかる費用の捻出 | 営業機会の損失 | 納期遅れ | 取引先からの受注停止・減少 | 顧客の流出 | 社会的評価の低下 | 取引先・顧客への損害賠償 | 人材の流出 | その他 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 企業別 | 中小企業 | (68) | 48.5 | 35.3 | 25.0 | 19.1 | 17.6 | 17.6 | 14.7 | 5.9 | 4.4 |
| | 大企業 | (45) | 37.8 | 42.2 | 13.3 | 15.6 | 26.7 | 42.2 | 22.2 | 20.0 | 4.4 |
| 【中小企業】業種別 | 製造業 | (37) | 45.9 | 37.8 | 32.4 | 16.2 | 21.6 | 16.2 | 10.8 | 5.4 | 5.4 |
| | 非製造業 | (31) | 51.6 | 32.3 | 16.1 | 22.6 | 12.9 | 19.4 | 19.4 | 6.5 | 3.2 |
| 従業員数別 | 50名以下 | (36) | 36.1 | 33.3 | 19.4 | 19.4 | 22.2 | 19.4 | 13.9 | 8.3 | 5.6 |
| | 51～100名 | (12) | 50.0 | 33.3 | 25.0 | 8.3 | 8.3 | 16.7 | 16.7 | - | 8.3 |
| | 101～1,000名 | (38) | 50.0 | 26.3 | 26.3 | 21.1 | 18.4 | 23.7 | 18.4 | 15.8 | 5.3 |
| | 1,001名以上 | (27) | 44.4 | 63.0 | 11.1 | 14.8 | 29.6 | 48.1 | 22.2 | 14.8 | - |

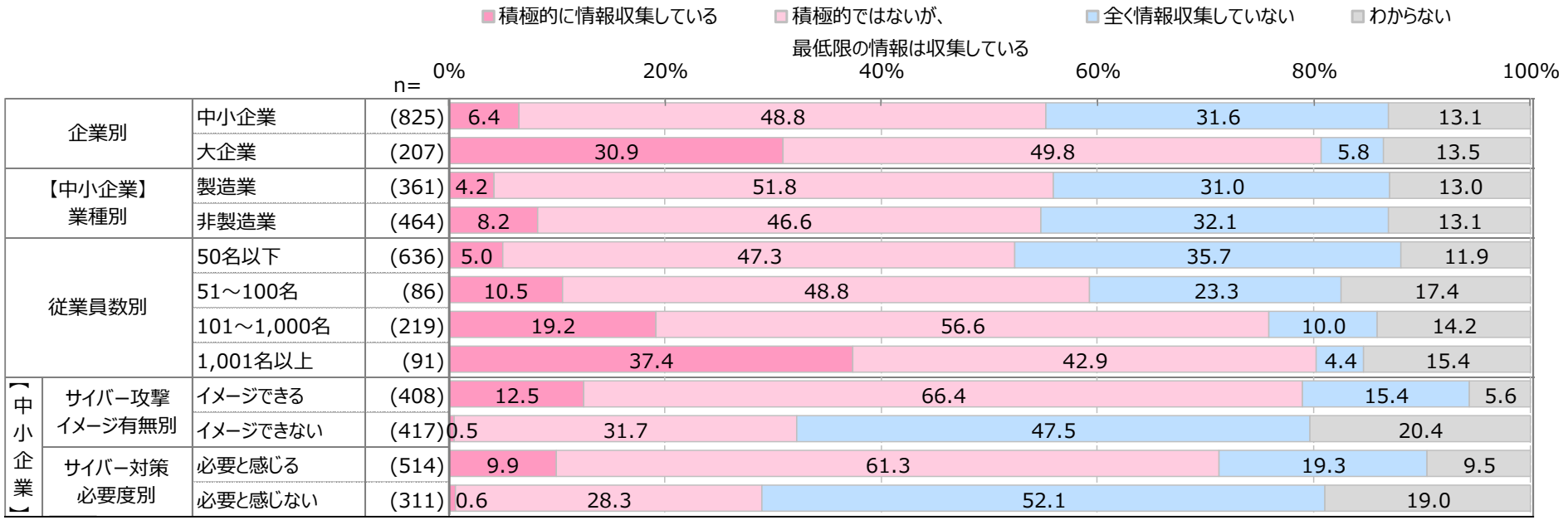
※「中小企業」のスコアで降順ソート

# （２０）サイバーセキュリティに関する情報収集状況

- サイバーセキュリティに関して情報収集している中小企業の経営者は約半数（55.2%）にとどまり、大企業の経営者（80.7%）に比べて低い。
- 全く情報収集していない中小企業の経営者は、大企業の経営者の約5倍（31.6%）である。
- 【中小企業】のクロス軸を見ると、経営者が「サイバー攻撃を受けた場合の被害をイメージできている」「サイバー攻撃への対策を必要と感じている」と回答した企業は、サイバーセキュリティに関する情報収集をしている傾向がある。

Q20　貴社では、サイバーセキュリティについて、どの程度情報収集していますか。

※全体ベース



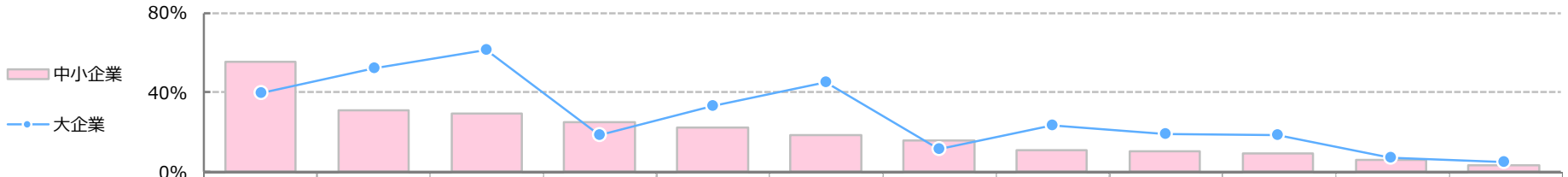

| | | | n= | 積極的に情報収集している | 積極的ではないが、最低限の情報は収集している | 全く情報収集していない | わからない |
|---|---|---|---|---|---|---|---|
| 企業別 | | 中小企業 | (825) | 6.4 | 48.8 | 31.6 | 13.1 |
| | | 大企業 | (207) | 30.9 | 49.8 | 5.8 | 13.5 |
| 【中小企業】業種別 | | 製造業 | (361) | 4.2 | 51.8 | 31.0 | 13.0 |
| | | 非製造業 | (464) | 8.2 | 46.6 | 32.1 | 13.1 |
| 従業員数別 | | 50名以下 | (636) | 5.0 | 47.3 | 35.7 | 11.9 |
| | | 51～100名 | (86) | 10.5 | 48.8 | 23.3 | 17.4 |
| | | 101～1,000名 | (219) | 19.2 | 56.6 | 10.0 | 14.2 |
| | | 1,001名以上 | (91) | 37.4 | 42.9 | 4.4 | 15.4 |
| 【中小企業】 | サイバー攻撃イメージ有無別 | イメージできる | (408) | 12.5 | 66.4 | 15.4 | 5.6 |
| | | イメージできない | (417) | 0.5 | 31.7 | 47.5 | 20.4 |
| | サイバー対策必要度別 | 必要と感じる | (514) | 9.9 | 61.3 | 19.3 | 9.5 |
| | | 必要と感じない | (311) | 0.6 | 28.3 | 52.1 | 19.0 |

# （２１）サイバーセキュリティに関する情報収集先

- 中小企業の経営者のサイバーセキュリティに関する情報収集先は「Webサイト」が最も多い。
- また、中小企業の経営者は、「コンサルタントや社外の専門家」「公的機関（ガイドライン等）」「セミナー・シンポジウム・勉強会」からの情報収集が大企業に比べて少ない。

Q21　貴社では、サイバーセキュリティに関する情報をどこから収集していますか。あてはまるものをすべてお選びください。

※サイバーセキュリティに関する情報収集者ベース




| | | n= | Webサイト | セミナー・シンポジウム・勉強会 | コンサルタントや社外の専門家 | テレビ | 新聞（業界新聞除く） | 公的機関（ガイドライン等） | メールマガジン | 業界誌 | 雑誌（一般誌）※業界誌除く | 業界新聞 | SNS | その他 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 企業別 | 中小企業 | (456) | 55.3 | 31.1 | 29.6 | 25.2 | 22.4 | 18.6 | 15.8 | 10.7 | 10.5 | 9.6 | 6.4 | 3.3 |
| | 大企業 | (167) | 39.5 | 52.1 | 61.1 | 18.6 | 32.9 | 44.9 | 11.4 | 23.4 | 19.2 | 18.6 | 7.2 | 4.8 |
| 【中小企業】業種別 | 製造業 | (202) | 56.4 | 29.7 | 28.2 | 22.8 | 15.8 | 17.8 | 12.4 | 10.9 | 10.9 | 11.4 | 5.9 | 3.5 |
| | 非製造業 | (254) | 54.3 | 32.3 | 30.7 | 27.2 | 27.6 | 19.3 | 18.5 | 10.6 | 10.2 | 8.3 | 6.7 | 3.1 |
| 従業員数別 | 50名以下 | (333) | 59.5 | 25.8 | 24.3 | 27.3 | 22.2 | 15.3 | 18.0 | 9.6 | 10.5 | 5.7 | 6.6 | 3.0 |
| | 51～100名 | (51) | 52.9 | 45.1 | 47.1 | 23.5 | 27.5 | 31.4 | 15.7 | 17.6 | 9.8 | 17.6 | 7.8 | 2.0 |
| | 101～1,000名 | (166) | 42.2 | 47.0 | 47.6 | 18.1 | 27.7 | 35.5 | 9.6 | 16.3 | 12.7 | 20.5 | 6.0 | 5.4 |
| | 1,001名以上 | (73) | 31.5 | 57.5 | 72.6 | 17.8 | 31.5 | 46.6 | 9.6 | 27.4 | 26.0 | 17.8 | 6.8 | 4.1 |

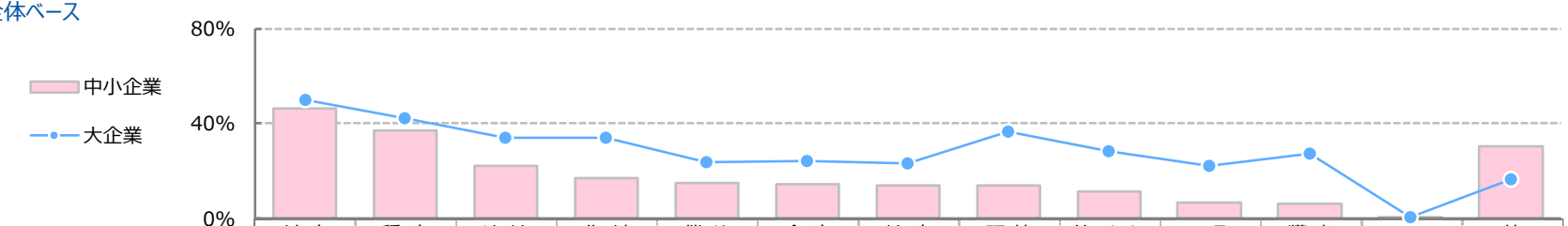
※「中小企業」のスコアで降順ソート

# （２２）サイバーセキュリティに関して知りたい情報

- 中小企業の経営者がサイバーセキュリティに関して知りたい情報は、「攻撃を受けた際の対処方法」「攻撃の種類と内容」が多かった。
- 「社員の教育・研修・訓練方法」「専門人材の獲得方法」は、大企業に比べると中小企業の経営者の回答は少なかった。

Q22　サイバーセキュリティに関して知りたい情報について、あてはまるものをすべてお選びください。

※全体ベース




| | | n= | 攻撃を受けた際の対処方法 | 攻撃の種類と内容 | 被害に遭った際の法的措置 | 対応マニュアルの作成方法 | サイバー保険の補償内容 | 攻撃を受けた際の金銭面以外の被害 | 攻撃を受けた際の被害額 | 社員の教育・研修・訓練方法 | セキュリティーポリシーの策定方法 | 取引先や委託先への普及方法 | 専門人材の獲得方法 | その他 | 特になし |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 企業別 | 中小企業 | (825) | 46.4 | 36.8 | 21.9 | 17.1 | 15.0 | 14.3 | 14.1 | 13.9 | 11.0 | 6.7 | 6.2 | 0.1 | 30.3 |
| | 大企業 | (207) | 49.8 | 42.0 | 33.8 | 33.8 | 23.7 | 24.2 | 23.2 | 36.7 | 28.5 | 22.2 | 27.1 | 0.5 | 16.4 |
| 【中小企業】業種別 | 製造業 | (361) | 46.8 | 33.8 | 19.1 | 17.2 | 13.6 | 14.1 | 15.0 | 15.2 | 11.1 | 6.4 | 5.3 | - | 29.9 |
| | 非製造業 | (464) | 46.1 | 39.2 | 24.1 | 17.0 | 16.2 | 14.4 | 13.4 | 12.9 | 11.0 | 6.9 | 6.9 | 0.2 | 30.6 |
| 従業員数別 | 50名以下 | (636) | 45.9 | 37.3 | 22.2 | 14.0 | 14.5 | 13.8 | 13.7 | 10.1 | 8.3 | 5.8 | 4.1 | 0.2 | 32.2 |
| | 51～100名 | (86) | 39.5 | 30.2 | 22.1 | 19.8 | 20.9 | 9.3 | 11.6 | 18.6 | 18.6 | 8.1 | 8.1 | - | 33.7 |
| | 101～1,000名 | (219) | 52.1 | 39.7 | 26.9 | 33.3 | 17.8 | 24.7 | 22.4 | 35.2 | 24.2 | 16.9 | 19.6 | 0.5 | 16.4 |
| | 1,001名以上 | (91) | 50.5 | 45.1 | 35.2 | 35.2 | 26.4 | 19.8 | 19.8 | 37.4 | 30.8 | 22.0 | 34.1 | - | 15.4 |

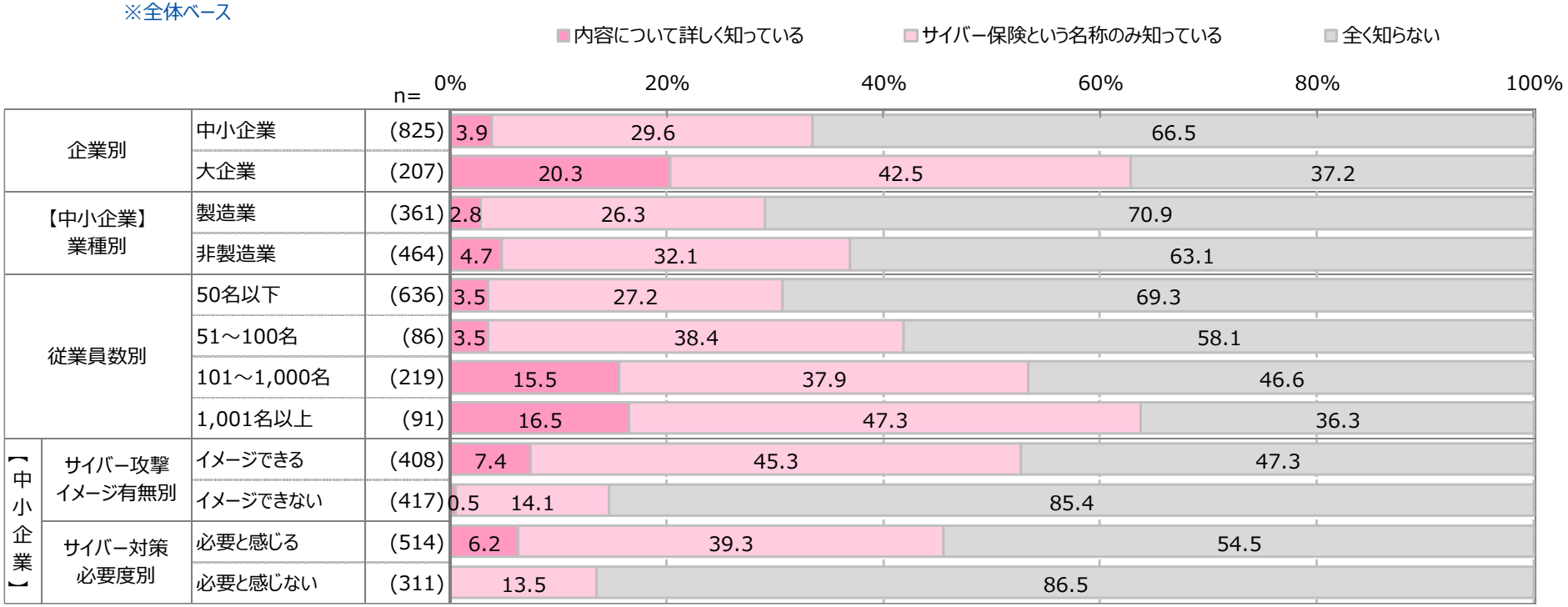
※「中小企業」のスコアで降順ソート

# （２３）サイバー保険の認知度

- サイバー保険を認知している（「内容について詳しく知っている」「名称のみ知っている」）と回答した中小企業の経営者は33.5%となっている。大企業の経営者の約半分（62.8%）にとどまる。
- サイバー保険を「全く知らない」と回答した中小企業の経営者は66.5%にのぼる。
- 【中小企業】のクロス軸を見ると、「サイバー攻撃をイメージできている」「サイバー対策の必要性を感じている」と回答した中小企業の経営者ほど、サイバー保険の認知度は高い。

Q23 あなたご自身は、サイバー保険についてどの程度ご存知ですか。

※全体ベース



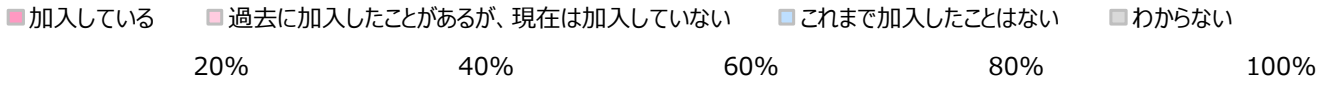

| | | | n= | 内容について詳しく知っている | サイバー保険という名称のみ知っている | 全く知らない |
|---|---|---|---|---|---|---|
| 企業別 | | 中小企業 | (825) | 3.9 | 29.6 | 66.5 |
| | | 大企業 | (207) | 20.3 | 42.5 | 37.2 |
| 【中小企業】業種別 | | 製造業 | (361) | 2.8 | 26.3 | 70.9 |
| | | 非製造業 | (464) | 4.7 | 32.1 | 63.1 |
| 従業員数別 | | 50名以下 | (636) | 3.5 | 27.2 | 69.3 |
| | | 51～100名 | (86) | 3.5 | 38.4 | 58.1 |
| | | 101～1,000名 | (219) | 15.5 | 37.9 | 46.6 |
| | | 1,001名以上 | (91) | 16.5 | 47.3 | 36.3 |
| 【中小企業】 | サイバー攻撃イメージ有無別 | イメージできる | (408) | 7.4 | 45.3 | 47.3 |
| | | イメージできない | (417) | 0.5 | 14.1 | 85.4 |
| | サイバー対策必要度別 | 必要と感じる | (514) | 6.2 | 39.3 | 54.5 |
| | | 必要と感じない | (311) | 13.5 | | 86.5 |

# （２４）サイバー保険の加入有無【保険認知者ベース】

- サイバー保険を認知している中小企業の経営者であっても、85.5%がこれまでにサイバー保険に加入したことがないと回答。
- サイバー保険を認知している経営者の回答によると、サイバー保険の加入状況は中小企業に比べて大企業の方が高く、従業員数別にみると、従業員数が多いほど「加入している」の回答が増えている。

Q24　貴社は、現在サイバー保険に加入していますか。

※サイバー保険認知者ベース

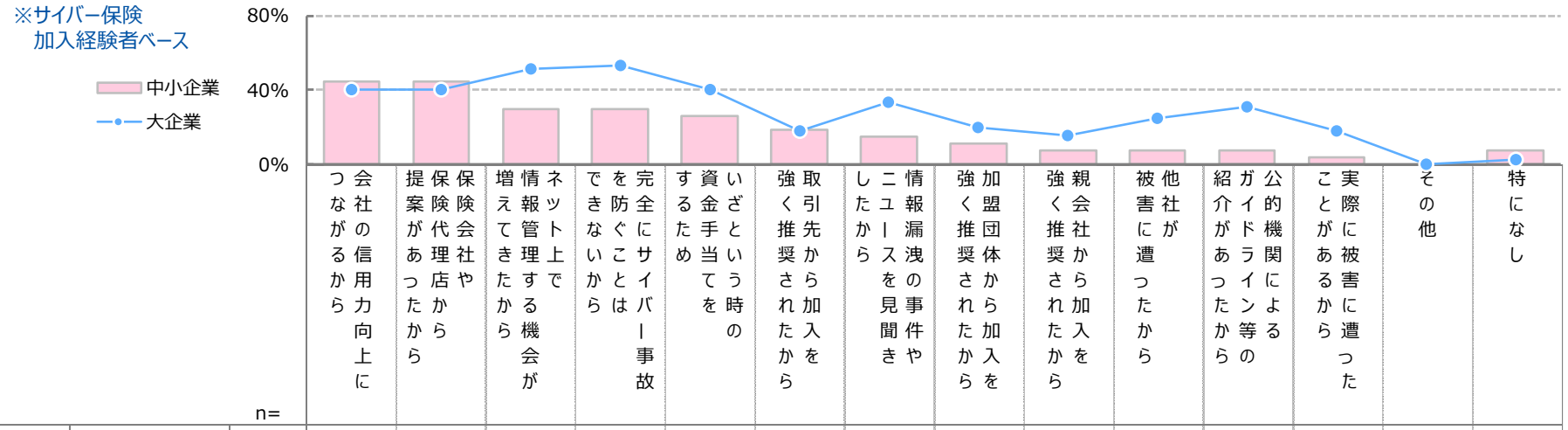



| | | n= | 0% 20% 40% 60% 80% 100% |
|---|---|---|---|
| 企業別 | 中小企業 | (276) | 6.9 / 2.9 / 85.5 / 4.7 |
| | 大企業 | (130) | 30.8 / 3.8 / 58.5 / 6.9 |
| 【中小企業】業種別 | 製造業 | (105) | 4.8 / 4.8 / 83.8 / 6.7 |
| | 非製造業 | (171) | 8.2 / 1.8 / 86.5 / 3.5 |
| 従業員数別 | 50名以下 | (195) | 5.6 / 2.1 / 88.7 / 3.6 |
| | 51～100名 | (36) | 8.3 / 2.8 / 86.1 / 2.8 |
| | 101～1,000名 | (117) | 17.9 / 6.0 / 70.9 / 5.1 |
| | 1,001名以上 | (58) | 41.4 / 1.7 / 43.1 / 13.8 |

# （２５）サイバー保険の加入理由

- 中小企業の経営者がサイバー保険に加入した理由は、「会社の信用力向上につながるから」「保険会社や保険代理店から提案があったから」が多い。
- 次いで「ネット上で情報管理する機会が増えてきたから」「完全にサイバー事故を防ぐことはできないから」「いざという時の資金手当てをするため」が多かったが、いずれも大企業と比べると少なく、「公的機関によるガイドライン等の紹介があったから」「他社が被害に遭ったから」の回答も大企業に比べて少ない。

Q25　これまでにサイバー保険に加入したことがある方にお伺いします。サイバー保険に加入した理由について、あてはまるものをすべてお選びください。




| | | n= | 会社の信用力向上につながるから | 保険会社や保険代理店から提案があったから | ネット上で情報管理する機会が増えてきたから | 完全にサイバー事故を防ぐことはできないから | いざという時の資金手当てをするため | 取引先から加入を強く推奨されたから | 情報漏洩の事件やニュースを見聞きしたから | 加盟団体から加入を強く推奨されたから | 親会社から加入を強く推奨されたから | 他社が被害に遭ったから | 公的機関によるガイドライン等の紹介があったから | 実際に被害に遭ったことがあるから | その他 | 特になし |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 企業別 | 中小企業 | (27) | 44.4 | 44.4 | 29.6 | 29.6 | 25.9 | 18.5 | 14.8 | 11.1 | 7.4 | 7.4 | 7.4 | 3.7 | - | 7.4 |
| | 大企業 | (45) | 40.0 | 40.0 | 51.1 | 53.3 | 40.0 | 17.8 | 33.3 | 20.0 | 15.6 | 24.4 | 31.1 | 17.8 | - | 2.2 |
| 【中小企業】業種別 | 製造業 | (10) | 30.0 | 40.0 | 10.0 | - | 20.0 | 30.0 | - | 20.0 | - | - | - | - | - | 10.0 |
| | 非製造業 | (17) | 52.9 | 47.1 | 41.2 | 47.1 | 29.4 | 11.8 | 23.5 | 5.9 | 11.8 | 11.8 | 11.8 | 5.9 | - | 5.9 |
| 従業員数別 | 50名以下 | (15) | 40.0 | 33.3 | 26.7 | 33.3 | 33.3 | 13.3 | 26.7 | 13.3 | 6.7 | 6.7 | 6.7 | - | - | 13.3 |
| | 51～100名 | (4) | 50.0 | 75.0 | 25.0 | 25.0 | - | 25.0 | - | - | 25.0 | - | - | - | - | - |
| | 101～1,000名 | (28) | 35.7 | 50.0 | 46.4 | 50.0 | 32.1 | 17.9 | 28.6 | 17.9 | 7.1 | 17.9 | 21.4 | 14.3 | - | - |
| | 1,001名以上 | (25) | 48.0 | 32.0 | 52.0 | 48.0 | 44.0 | 20.0 | 28.0 | 20.0 | 20.0 | 28.0 | 36.0 | 20.0 | - | 4.0 |

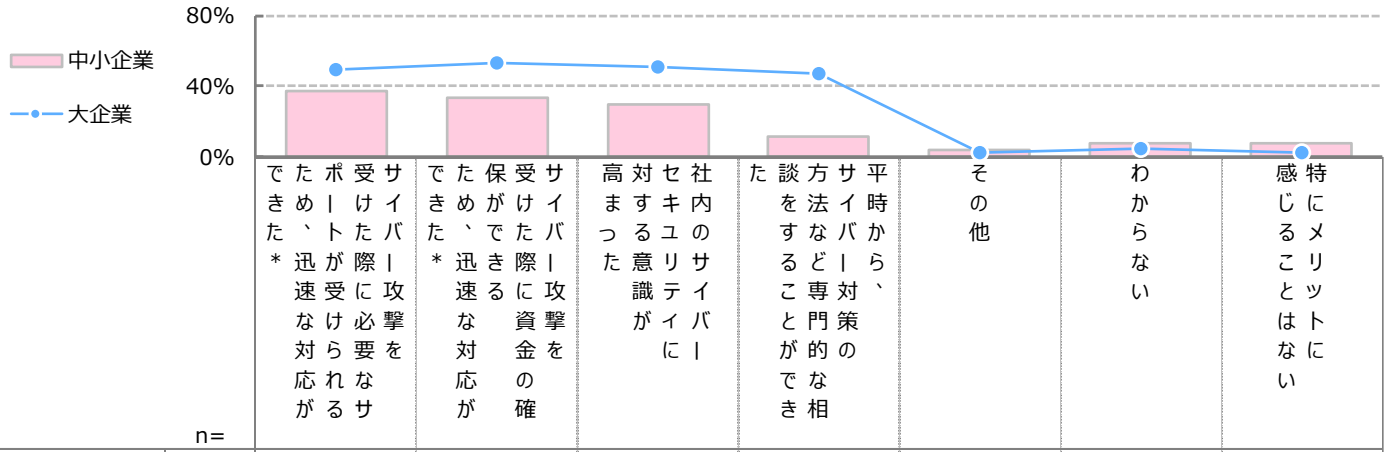
※「中小企業」のスコアで降順ソート

# （２６）サイバー保険の加入メリット

- サイバー保険に加入したことによるメリットについて、中小企業の経営者の回答は「サイバー攻撃を受けた際に必要なサポートが受けられるため、迅速な対応ができた」が最も多かった。
- 一方、「平時から、サイバー対策の方法など専門的な相談をすることができた」と回答した大企業の経営者は約半数にのぼったが、中小企業は11.1%にとどまった。

Q26　これまでにサイバー保険に加入したことがある方にお伺いします。
サイバー保険に加入したことによるメリットは何ですか。あてはまるものをすべてお選びください。

※サイバー保険
加入経験者ベース




| | | n= | サイバー攻撃を受けた際に必要なサポートが受けられるため、迅速な対応ができた* | サイバー攻撃を受けた際に資金の確保ができるため、迅速な対応ができた* | 社内のサイバーセキュリティに対する意識が高まった | 平時から、サイバー対策の方法など専門的な相談をすることができた | その他 | わからない | 特にメリットは感じることはない |
|---|---|---|---|---|---|---|---|---|---|
| 企業別 | 中小企業 | (27) | 37.0 | 33.3 | 29.6 | 11.1 | 3.7 | 7.4 | 7.4 |
| | 大企業 | (45) | 48.9 | 53.3 | 51.1 | 46.7 | 2.2 | 4.4 | 2.2 |
| 【中小企業】業種別 | 製造業 | (10) | 30.0 | 30.0 | 20.0 | - | - | 20.0 | 10.0 |
| | 非製造業 | (17) | 41.2 | 35.3 | 35.3 | 17.6 | 5.9 | - | 5.9 |
| 従業員数別 | 50名以下 | (15) | 33.3 | 33.3 | 20.0 | 13.3 | 6.7 | 6.7 | 13.3 |
| | 51～100名 | (4) | 75.0 | - | 50.0 | - | - | 25.0 | - |
| | 101～1,000名 | (28) | 42.9 | 57.1 | 39.3 | 32.1 | - | 7.1 | 3.6 |
| | 1,001名以上 | (25) | 48.0 | 48.0 | 60.0 | 52.0 | 4.0 | - | - |

＊（迅速な対応ができる態勢を構築できた）

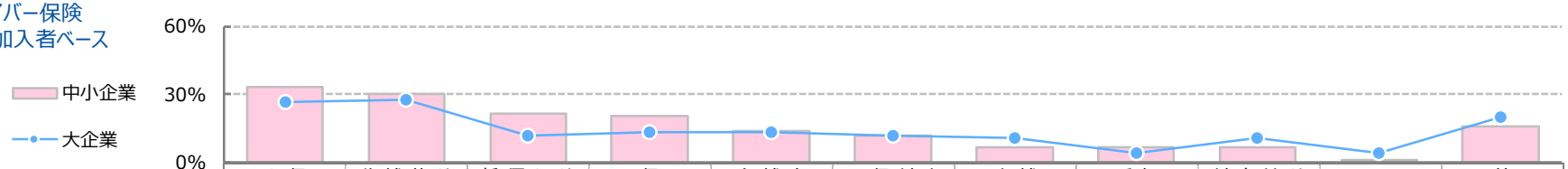
※「中小企業」のスコアで降順ソート

# （２７）サイバー保険の未加入理由

- 中小企業の経営者がサイバー保険に加入しない理由は、「保険についてよく知らないから」が最も多く、「サイバー攻撃に伴う損害額（必要な補償額）が分からないから」が続いた。
- 次いで「サイバーセキュリティ対策の優先度が低いから」の回答が多く、回答割合は大企業の約２倍になっている。

Q27　これまでにサイバー保険に加入したことがない方にお伺いします。
サイバー保険に加入したことがない理由について、あてはまるものをすべてお選びください。

※サイバー保険
未加入者ベース




| | | n= | 保険についてよく知らないから | 補償額（必要な）が分からないから | サイバー攻撃に伴う損害額 | サイバーセキュリティ対策の優先度が低いから | 保険料が高いから | 実際に補償が受けられるか心配だから | 十分なセキュリティ対策を講じており、保険の必要性を感じないから | 補償額が十分でないから | 加入にかかる手間が多いから | 被害に遭っても自己資金で対応できるから | サイバー攻撃の | その他 | 特になし |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 企業別 | 中小企業 | (236) | 33.1 | 30.1 | 21.6 | 20.3 | 13.6 | 11.9 | 6.8 | 6.8 | 6.4 | 0.8 | 15.7 | | |
| | 大企業 | (76) | 26.3 | 27.6 | 11.8 | 13.2 | 13.2 | 11.8 | 10.5 | 3.9 | 10.5 | 3.9 | 19.7 | | |
| 【中小企業】業種別 | 製造業 | (88) | 27.3 | 35.2 | 30.7 | 18.2 | 14.8 | 5.7 | 5.7 | 5.7 | 5.7 | 1.1 | 17.0 | | |
| | 非製造業 | (148) | 36.5 | 27.0 | 16.2 | 21.6 | 12.8 | 15.5 | 7.4 | 7.4 | 6.8 | 0.7 | 14.9 | | |
| 従業員数別 | 50名以下 | (173) | 32.9 | 28.9 | 23.7 | 20.2 | 11.0 | 11.0 | 6.9 | 6.4 | 4.6 | 1.2 | 14.5 | | |
| | 51～100名 | (31) | 32.3 | 29.0 | 12.9 | 16.1 | 22.6 | 16.1 | 12.9 | 12.9 | 12.9 | - | 19.4 | | |
| | 101～1,000名 | (83) | 31.3 | 27.7 | 16.9 | 16.9 | 14.5 | 10.8 | 4.8 | 4.8 | 10.8 | 3.6 | 19.3 | | |
| | 1,001名以上 | (25) | 20.0 | 40.0 | 4.0 | 16.0 | 16.0 | 16.0 | 16.0 | - | 8.0 | - | 20.0 | | |

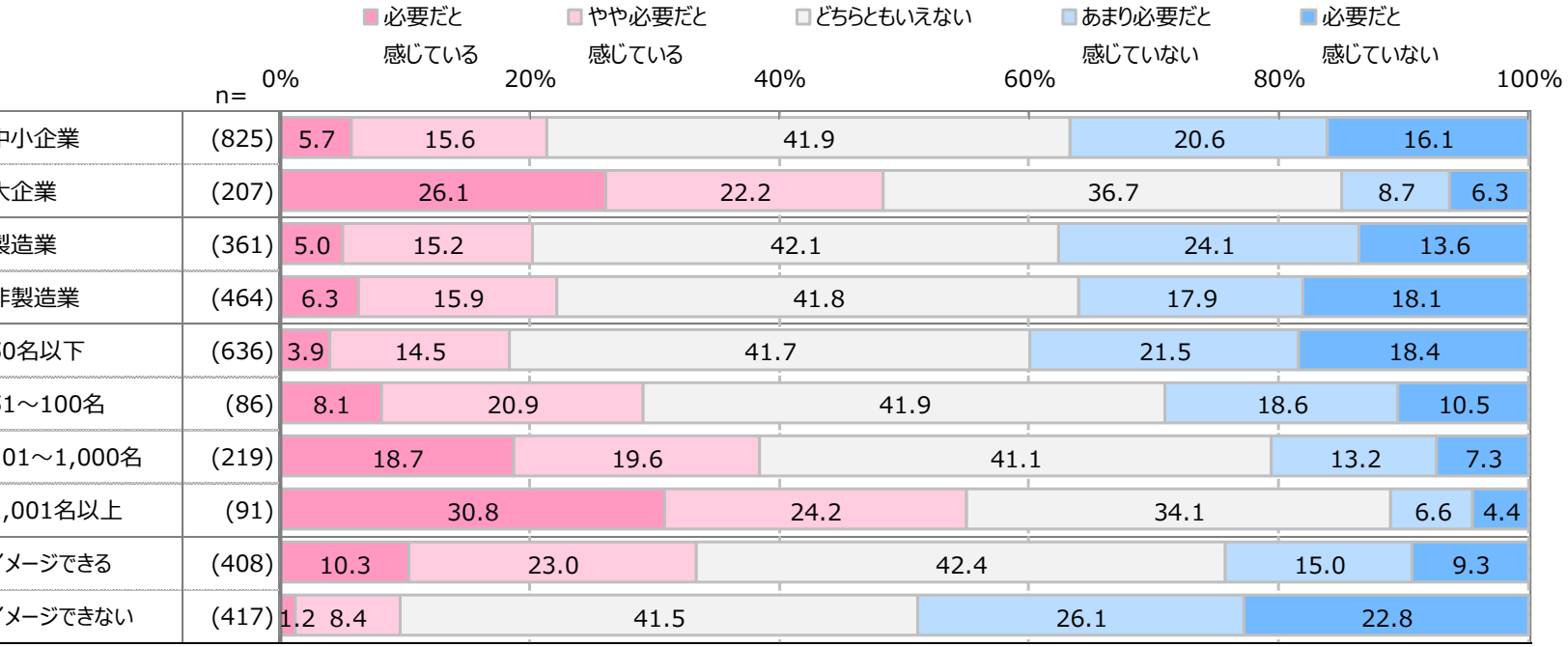
※「中小企業」のスコアで降順ソート

# （２８）サイバー保険の加入の必要度

- サイバー保険の加入が必要（「必要だと感じている」「やや必要だと感じている」）と考える中小企業の経営者は21.3%にとどまり、大企業の約半分の割合となっている。
- 【中小企業】のクロス軸を見ると、「サイバー攻撃による被害のイメージができていない」と回答した中小企業の経営者のうち、サイバー保険の加入が必要と考える割合は9.6%となった。

Q28　貴社において、サイバー保険への加入はどの程度必要であると考えていますか。

※全体ベース




| | | n= | 必要だと感じている | やや必要だと感じている | どちらともいえない | あまり必要だと感じていない | 必要だと感じていない |
|---|---|---|---|---|---|---|---|
| 企業別 | 中小企業 | (825) | 5.7 | 15.6 | 41.9 | 20.6 | 16.1 |
| | 大企業 | (207) | 26.1 | 22.2 | 36.7 | 8.7 | 6.3 |
| 【中小企業】業種別 | 製造業 | (361) | 5.0 | 15.2 | 42.1 | 24.1 | 13.6 |
| | 非製造業 | (464) | 6.3 | 15.9 | 41.8 | 17.9 | 18.1 |
| 従業員数別 | 50名以下 | (636) | 3.9 | 14.5 | 41.7 | 21.5 | 18.4 |
| | 51～100名 | (86) | 8.1 | 20.9 | 41.9 | 18.6 | 10.5 |
| | 101～1,000名 | (219) | 18.7 | 19.6 | 41.1 | 13.2 | 7.3 |
| | 1,001名以上 | (91) | 30.8 | 24.2 | 34.1 | 6.6 | 4.4 |
| 【中小企業】サイバー攻撃イメージ有無別 | イメージできる | (408) | 10.3 | 23.0 | 42.4 | 15.0 | 9.3 |
| | イメージできない | (417) | 1.2 | 8.4 | 41.5 | 26.1 | 22.8 |