2024年度 中小企業における情報セキュリティ対策に関する実態調査
業種ごとの効果的な取組事例集

2025年5月

独立行政法人情報処理推進機構

IPA Better Life with IT

2024年度 中小企業における情報セキュリティ対策に関する実態調査

共通の対策

1 SECURITY ACTION 二つ星の対策実施によるサイバーインシデント被害低減の効果

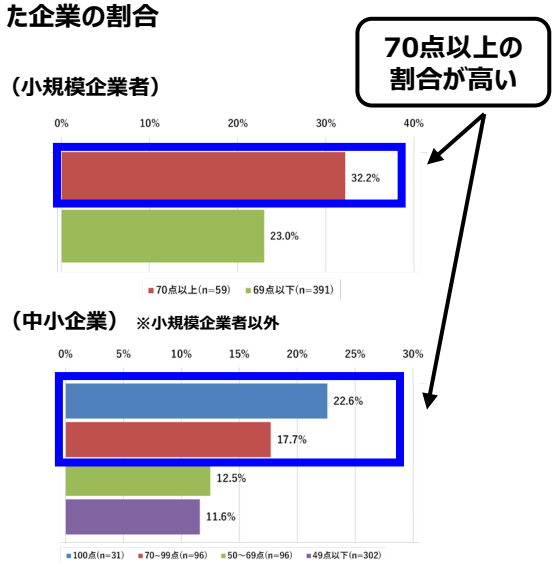
SECURITY ACTION 二つ星の対策（「5分でできる！情報セキュリティ自社診断」の診断項目）を多く実施している企業ほど、サイバーインシデント被害が少なく、被害額も少ないと回答していることが明らかになっています。診断項目の実施により、サイバーインシデント被害（発生率・被害額）の低減が期待されます。

※アンケート回答企業の自社診断の合計点は、「5分でできる！情報セキュリティ自社診断」の診断項目に該当するアンケート設問の回答結果を元に算出。

診断項目の合計点が高い方がサイバーインシデント被害が少ない

- 自社診断の合計点が70点以上の企業は、69点以下の企業より、2023年度中にサイバーインシデントが発生した経験が少なく、さらに発生経験があった企業においてもサイバーインシデントによる影響がなかったと回答した割合が高くなっています。
- また、自社診断の合計点が100点の企業はサイバーインシデントで発生した被害額が他の企業と比べてかなり低い結果となっており、**診断項目の対策を多く実施することでサイバーインシデント被害の低減が期待されます。**

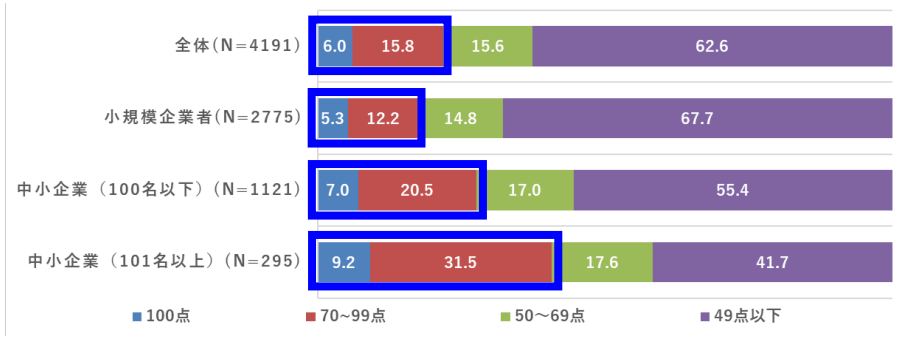
サイバーインシデントによる影響がなかったと回答した企業の割合



自社診断の合計点	被害額の平均	被害額の最大値
100点	約26万円	500万円
70点～99点	約120万円	3000万円
50～69点	約134万円	8000万円

アンケート結果からみえた実施状況と取組むべき項目

- 診断項目の合計点が70点以上の割合は**全体の21.8%**
- 企業規模別では70点以上の割合は小規模企業者で**17.5%**、中小企業(100名以下)では**27.5%**、中小企業(101名以上)で**40.7%**
- **全ての企業でさらに積極的な取組みが望まれます。**



- **以下の項目は実施率が特に低いため、積極的な取組みが望まれます。**
  - 新たな脅威や攻撃の手口を知り対策を社内共有する仕組み
  - サイバーセキュリティ事故に備えた緊急時の体制整備や対応手順の作成
  - サイバーセキュリティ対策のルール化と従業員への明示

2024年度 中小企業における情報セキュリティ対策に関する実態調査

共通の対策

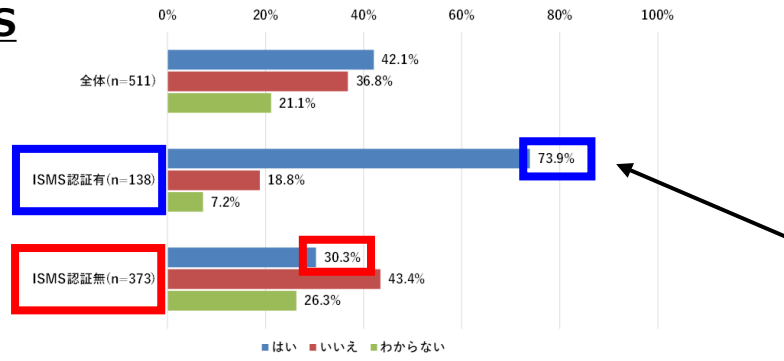
2 第三者評価制度（ISMS認証、Pマーク）の取得による取引先からの信頼獲得の効果

第三者評価制度（ISMS認証、Pマーク）を取得している企業では、取引先からのサイバーセキュリティ要請に応じたことが取引につながった大きな要因であると考えている企業の割合が、取得していない企業に比べ約2倍となりました。これは、サイバーセキュリティ対策に関する第三者評価制度の取得が、取引上の信頼を得るための重要な要素であることを示しています。

質問

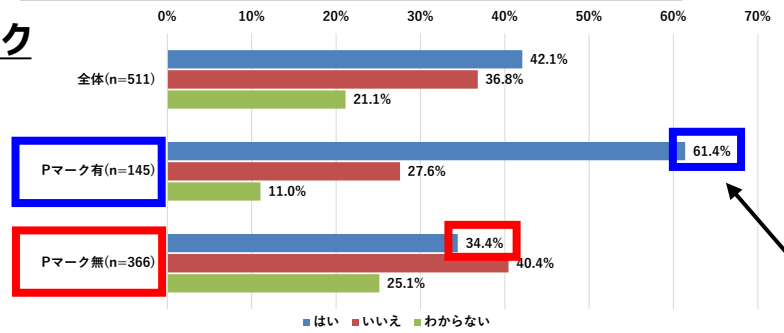
貴社は販売先（発注元企業）から要請された情報セキュリティ対策を行ったことが取引先との取引につながった大きな要因だと思いますか。（SA）

ISMS



取得の企業が未取得の企業の約２.5倍

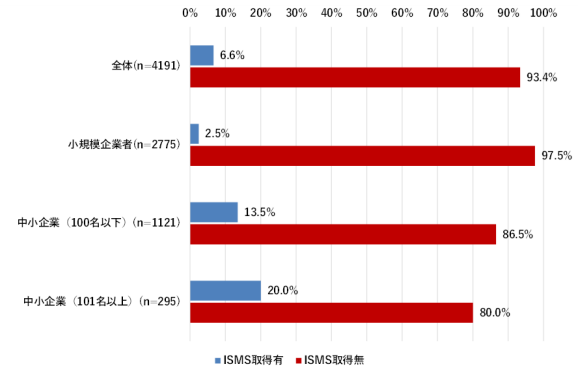
Pマーク



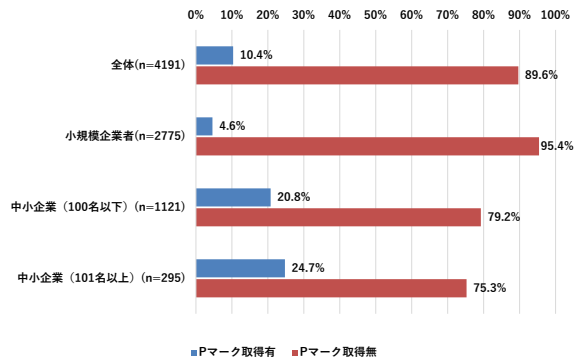
取得の企業が未取得の企業の約２倍

※アンケート結果からみえた、中小企業のISMS取得状況

- **ISMS取得企業は全体の6.6%**
- 企業規模別では小規模企業者が**2.5%**、中小企業(100名以下)では**13.5%**、中小企業(101名以上)では**20.0%**。
- 業種別では**製造業、情報通信業、複合サービス業の取得率が高い。**※



- **Pマーク取得企業は全体の10.4%**
- 企業規模別では小規模企業者が**4.6%**、中小企業(100名以下)で**20.8%**、中小企業(101名以上)では**24.7%**。
- 業種別では**医療・福祉、情報通信業、運輸業・郵便業、製造業の取得率が高い。**※



※ 業種別の回答数が少ない農業、林業、漁業、工業、採石業、砂利採取業は除外

2024年度 中小企業における情報セキュリティ対策に関する実態調査

共通の対策

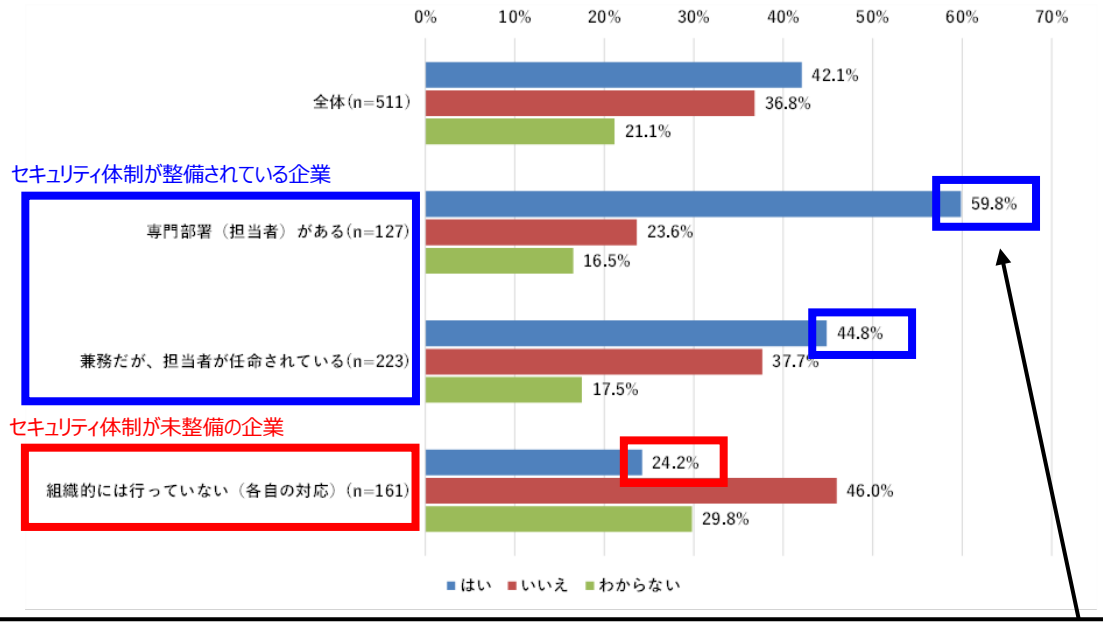
3 サイバーセキュリティ体制の整備による取引先からの信頼獲得の効果

普段からサイバーセキュリティ体制が整備されている企業※では、取引先からのサイバーセキュリティ要請に応じたことが取引につながった大きな要因であると考えている割合が、未整備の企業の約2倍になりました。これは、サイバーセキュリティ体制の整備が取引上の信頼を得るための重要な要素であることを示しています。

※ 自社のセキュリティ体制に関するアンケート設問に、「専門部署（担当者）がある」、「兼務だが、担当者が任命されている」、の何れかを選択した企業を指す。

質問

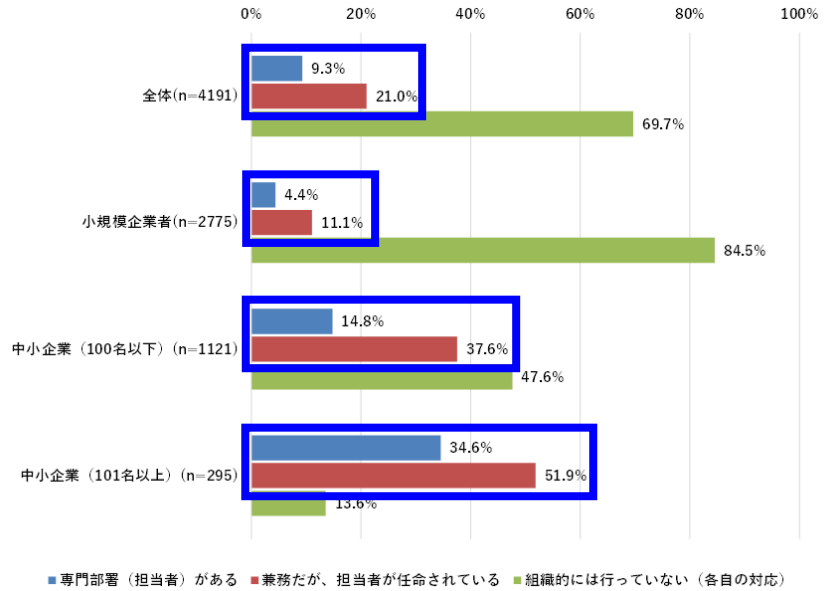
貴社は販売先（発注元企業）から要請された情報セキュリティ対策を行ったことが取引先との取引につながった大きな要因だと思いますか。（SA）



体制が整備されている企業が、未整備の企業の約２倍

※アンケート結果からみえた、中小企業のセキュリティ体制整備状況

- サイバーセキュリティ体制が整備されている企業は回答者全体の**30.3%**
- 企業規模別では小規模企業者で**15.5%**、中小企業(100名以下)では**52.4%**、中小企業(101名以上)で**86.6%**
- **小規模企業者で、積極的なサイバーセキュリティ体制の整備が望まれます。**



2024年度 中小企業における情報セキュリティ対策に関する実態調査

共通の対策

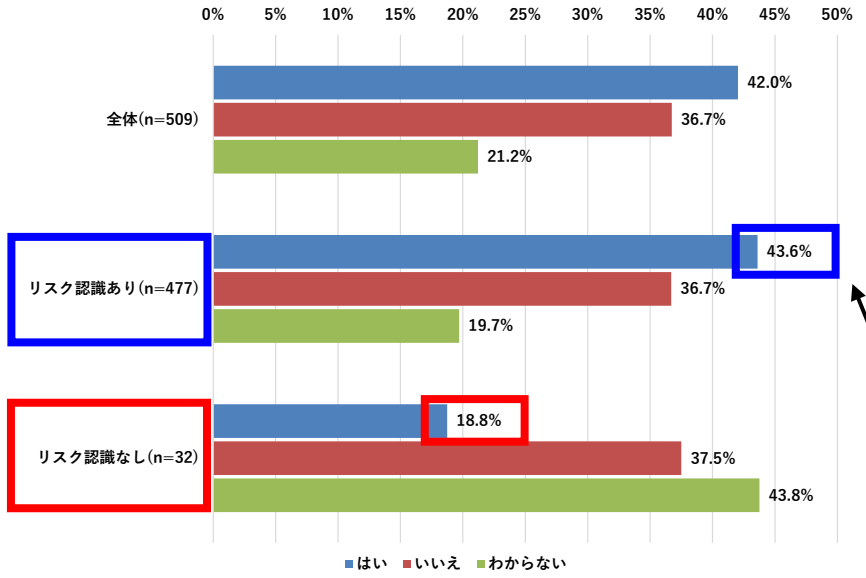
4 取引における自社の事業へのリスク認識を持つことによる取引先からの信頼獲得の効果

他社との取引におけるリスク認識がある企業※では、取引先からのサイバーセキュリティ要請に応じたことが取引につながった大きな要因であると考えている企業が、リスク認識がない企業の約2倍となりました。これは、サイバーセキュリティ対策を実施する上で、取引におけるリスク認識をもつことが、取引上の信頼を得るための重要な要素であることを示しています。

※ 他社との取引において自社の主要な事業に最も大きいリスクと考えていることに関するアンケート設問に、「機密性の高い情報（個人情報・設計図面等）の漏洩」、「供給している製品（原料・中間部品・最終品等）の途絶」、「可用性が重視されるサービス（インフラ・IT等）の停止」の何れかを選択した企業を指す。

質問

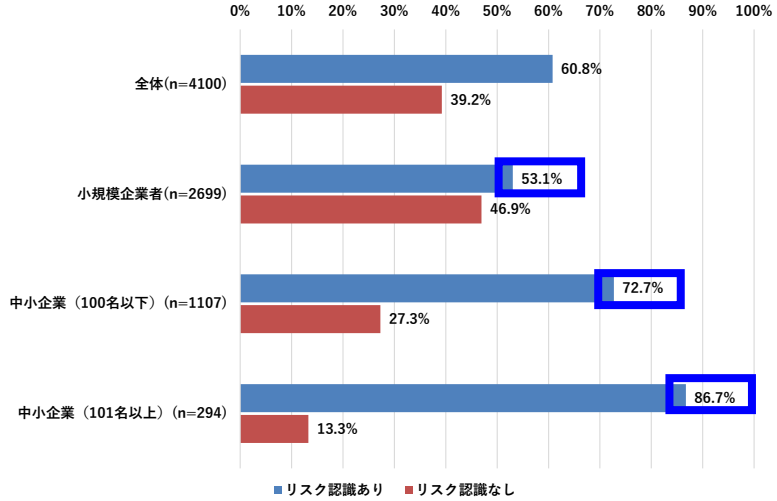
貴社は販売先（発注元企業）から要請された情報セキュリティ対策を行ったことが取引先との取引につながった大きな要因だと思いますか。（SA）



リスク認識ありの企業が、リスク認識無しの企業の約２倍

※アンケート結果からみえた、中小企業の取引におけるリスク認識状況

- 他社との取引において自社の主要な事業に最も大きいリスクと考えていることとして、「機密性の高い情報(個人情報・設計図面等)の漏えい」が**38.5%**と最も多く、**情報漏えいが大きなリスクと認識されています**。
- 企業規模別では小規模企業者では**53.1%**、中小企業（100名以下）では**72.7%**、中小企業（101名以上）では**86.7%**
- **小規模企業者でも自社の事業へのリスクを認識することが望まれます。**



2024年度 中小企業における情報セキュリティ対策に関する実態調査

業種別の対策

建設業

※回答企業数：566件

約３割弱がサイバーセキュリティ体制を組織的に整備し、経営基盤の強化と取引先からの信頼を獲得しています。また約３割強がサイバーセキュリティ教育を実施し、約１割強の企業がSECURITY ACTION 二つ星の対策を実施（「5分でできる！情報セキュリティ自己診断」の得点が70点以上）し、社内のサイバーセキュリティ対策を向上させサイバーインシデント被害の低減の効果を得ています。

■ サイバーセキュリティ対策で、安心感と取引先からの信頼を獲得！

サイバーセキュリティ対策のメリットに対するとして「安全・安心」「信頼・信用」が挙げられており、**企業がセキュリティ対策を通じて、経営基盤の強化に加え、取引先からの信頼の獲得という効果も実感していることが分かります。**

■対策で感じるメリットの回答例

- ウイルスなどの危険がないこと。
- 社員の意識が明らかに変わったこと。
- セキュリティ対策を講じていることで安心して仕事ができること。
- 社内の安心感と取引先へのアピールなどです。
- サーバーをクラウドにすることにより、外部へは必要最低限の情報を共有できるようになったこと。
- 他社からの信頼をえられたこと。
- スパムメールがセキュリティゲートによって弾かれるようになったこと。
- 詐欺メール等の危険なメールが受信されないので、ウイルス感染のリスクが減ったこと。
- 社員が細かい規定に囚われずITを単なるツールとして使えるようになったこと。
- 日々の不安感が抑えられたこと。
- 企業価値の向上に繋がっていると感じている。
- 顧客に対して安心感が増したこと。

■ アンケート結果から見えた、サイバーセキュリティ対策の状況

【サイバーセキュリティ対策投資の状況】

サイバーセキュリティ対策投資をしている割合	（投資していると回答した企業について）	
	年間投資額の平均値	売上高に占める投資額の割合
25.8%	293万円	1.8%

【サイバーセキュリティ対策状況】

「5分でできる！情報セキュリティ自己診断」の得点が70点以上	74件　（13.1%）

➡ SECURITY ACTION 二つ星の対策を多く実施している企業（「5分でできる！情報セキュリティ自己診断」の得点が高い企業）ほど**サイバーインシデントの経験が少なく、被害による影響が少ない**ことが明らかになっています。

サイバーセキュリティ体制を整備している	151件　（26.7%）

➡ サイバーセキュリティ体制が整備されている企業（専門部署がある、兼務だが担当者がいる企業）ほど**取引上の信頼を得ています。**

サイバーセキュリティ教育を実施している（eラーニング、訓練など）	187件　（33.0%）

➡ サイバーセキュリティ教育を実施し社内のサイバーセキュリティ対策を向上させ、サイバーインシデント被害の低減を図っています。

2024年度 中小企業における情報セキュリティ対策に関する実態調査

業種別の対策

製造業

※回答企業数：504件

約５割がサイバーセキュリティ体制を組織的に整備し、経営基盤の強化と取引先からの信頼を獲得しています。また約５割強がサイバーセキュリティ教育を実施し、約４分の１の企業がSECURITY ACTION 二つ星の対策を実施（「5分でできる！情報セキュリティ自己診断」の得点が70点以上）し、社内のサイバーセキュリティ対策を向上させサイバーインシデント被害の低減の効果を得ています。

■ サイバーセキュリティ対策で、安心感と取引先からの信頼を獲得！

サイバーセキュリティ対策のメリットに対するとして「安全・安心」「信頼・信用」が挙げられており、**企業がセキュリティ対策を通じて、経営基盤の強化に加え、取引先からの信頼の獲得という効果も実感していることが分かります。**

■対策で感じるメリットの回答例

- 社員の安全安心感が高まって、仕事に集中できる。
- 情報の安全性が高くなり、利用方法も多岐にわたるようになった。
- 安心感が得られる。取引先からの信頼もいただける。
- 安心して仕事に打ち込めるようになった。
- 取引先の信用度向上。
- 事業の安定化。
- 信頼を得られる機会が増えた。
- 取引先より信頼が得たこと。
- ユーザーに対する信頼性。
- 顧客からの信頼獲得による受注増 特命発注の獲得。

■企業が実際に取り組んでいるサイバーセキュリティ対策　※インタビュー調査結果より

企業が取り組んでいる対策	効果
月額５万円程度の、民間の総合セキュリティ（UTM）を導入しており、個別にセキュリティ機器を導入するよりもコストを抑えられた。また**地元の商工会議所が開催する講習会に参加して情報収集している**。これにより、**セキュリティ意識が向上し25年近くもウイルス感染が起きていない。**	被害の低減
「サイバーセキュリティお助け隊サービス」を導入したことで、**社員による情報漏えいなどの事故が未然に防げるといった安心感を得られた。**	被害の低減

■ アンケート結果から見えた、サイバーセキュリティ対策の状況

【サイバーセキュリティ対策投資の状況】

サイバーセキュリティ対策投資をしている割合	（投資していると回答した企業について）	
	年間投資額の平均値	売上高に占める投資額の割合
44.4%	208万円	1.0%

【サイバーセキュリティ対策状況】

「5分でできる！情報セキュリティ自己診断」の得点が70点以上	125件　（24.8%）

➡ SECURITY ACTION 二つ星の対策を多く実施している企業（「5分でできる！情報セキュリティ自己診断」の得点が高い企業）ほど**サイバーインシデントの経験が少なく、被害による影響が少ない**ことが明らかになっています。

サイバーセキュリティ体制を整備している	244件　（48.4%）

➡ サイバーセキュリティ体制が整備されている企業（専門部署がある、兼務だが担当者がいる企業）ほど**取引上の信頼を得ています。**

サイバーセキュリティ教育を実施している（eラーニング、訓練など）	264件　（52.4%）

➡ サイバーセキュリティ教育を実施し社内のサイバーセキュリティ対策を向上させ、サイバーインシデント被害の低減を図っています。

2024年度 中小企業における情報セキュリティ対策に関する実態調査

業種別の対策

情報通信業

※回答企業数：317件

約５割強がサイバーセキュリティ体制を組織的に整備し、経営基盤の強化と取引先からの信頼を獲得しています。また約５割強がサイバーセキュリティ教育を実施し、約５割弱の企業がSECURITY ACTION 二つ星の対策を実施（「5分でできる！情報セキュリティ自己診断」の得点が70点以上）し、社内のサイバーセキュリティ対策を向上させサイバーインシデント被害の低減の効果を得ています。

■ サイバーセキュリティ対策で、安心感と取引先からの信頼を獲得！

サイバーセキュリティ対策のメリットに対するとして「安全・安心」「信頼・信用」が挙げられており、**企業がセキュリティ対策を通じて、経営基盤の強化に加え、取引先からの信頼の獲得という効果も実感していることが分かります。**

■対策で感じるメリットの回答例

- 従業員の意識向上、漏洩などの安心性、安全性、顧客からの信用や信頼の獲得がなされたこと。
- お客様からの信頼感が違うのと、業界全体では当たり前だという認識を社内で共有できたこと。取引先に安心感を与えられること。
- 文書や資料が整理された。システムの信頼性が 上がった。
- 取引先の信用度が高まること。
- 普段のメールのやりとりが安心してできるようになったこと。
- サーバーの安全性が増した。
- 社員の意識向上と業務への安心感

■企業が実際に取り組んでいるサイバーセキュリティ対策　※インタビュー調査結果より

企業が取り組んでいる対策	効果
全社的な情報セキュリティ対策を行い、ISMS認証を取得したことで**全社的なセキュリティ意識が向上し、新規取引のきっかけになった。**	経営基盤の強化 信頼の獲得
費用をかけずに行ったセキュリティ対策として、不要なソフトの見直しと削除を実施した。	被害の低減

■ アンケート結果から見えた、サイバーセキュリティ対策の状況

【サイバーセキュリティ対策投資の状況】

サイバーセキュリティ対策投資をしている割合	（投資していると回答した企業について）	
	年間投資額の平均値	売上高に占める投資額の割合
39.4%	79万円	0.6%

【サイバーセキュリティ対策状況】

「5分でできる！情報セキュリティ自己診断」の得点が70点以上	151件　（47.6%）

➡ SECURITY ACTION 二つ星の対策を多く実施している企業（「5分でできる！情報セキュリティ自己診断」の得点が高い企業）ほど**サイバーインシデントの経験が少なく、被害による影響が少ない**ことが明らかになっています。

サイバーセキュリティ体制を整備している	143件　（51.7%）

➡ サイバーセキュリティ体制が整備されている企業（専門部署がある、兼務だが担当者がいる企業）ほど**取引上の信頼を得ています。**

サイバーセキュリティ教育を実施している（eラーニング、訓練など）	164件　（51.7%）

➡ サイバーセキュリティ教育を実施し社内のサイバーセキュリティ対策を向上させ、サイバーインシデント被害の低減を図っています。

2024年度 中小企業における情報セキュリティ対策に関する実態調査

業種別の対策

運輸業、郵便業

※回答企業数：109件

約４割強がサイバーセキュリティ体制を組織的に整備し、経営基盤の強化と取引先からの信頼を獲得しています。また約５割がサイバーセキュリティ教育を実施し、約１割強の企業がSECURITY ACTION 二つ星の対策を実施（「5分でできる！情報セキュリティ自己診断」の得点が70点以上）し、社内のサイバーセキュリティ対策を向上させサイバーインシデント被害の低減の効果を得ています。

■ サイバーセキュリティ対策で、安心感と取引先からの信頼を獲得！

サイバーセキュリティ対策のメリットに対するとして「安全・安心」「信頼・信用」が挙げられており、**企業がセキュリティ対策を通じて、経営基盤の強化に加え、取引先からの信頼の獲得という効果も実感していることが分かります。**

■対策で感じるメリットの回答例

- 漏洩対策として安心感が有ること。
- 日常業務遂行にある程度の安心感が図れるようになった。
- 情報に対する安心、安全性が上がったこと。
- 安全なシステム運用が確保できたこと。
- 顧客信頼度の向上、セキュリティ意識の向上、情報漏洩に対するリスク認識の共有化ができたこと。
- 業務の信頼性が高まり効率化が図れたこと。
- 信頼失墜リスクの予防。
- 社員の不用意な社内情報のSNSアップなどを防止できたこと。
- 社員のセキュリティ意識の高まりがあったこと。
- 取引先からの要望に応えられたこと。
- 社員の意識が大きく変わったこと。
- 安全なシステム運用が確保できたこと。

■ アンケート結果から見えた、サイバーセキュリティ対策の状況

【サイバーセキュリティ対策投資の状況】

サイバーセキュリティ対策投資をしている割合	（投資していると回答した企業について）	
	年間投資額の平均値	売上高に占める投資額の割合
28.4%	191万円	0.9%

【サイバーセキュリティ対策状況】

「5分でできる！情報セキュリティ自己診断」の得点が70点以上	16件 （14.7%）

➡ SECURITY ACTION 二つ星の対策を多く実施している企業（「5分でできる！情報セキュリティ自己診断」の得点が高い企業）ほど**サイバーインシデントの経験が少なく、被害による影響が少ない**ことが明らかになっています。

サイバーセキュリティ体制を整備している	47件 （43.1%）

➡ サイバーセキュリティ体制が整備されている企業（専門部署がある、兼務だが担当者がいる企業）ほど**取引上の信頼を得ています。**

サイバーセキュリティ教育を実施している（eラーニング、訓練など）	51件 （46.8%）

➡ サイバーセキュリティ教育を実施し社内のサイバーセキュリティ対策を向上させ、サイバーインシデント被害の低減を図っています。

2024年度 中小企業における情報セキュリティ対策に関する実態調査

業種別の対策

卸売業

※回答企業数：235件

約３割がサイバーセキュリティ体制を組織的に整備し、経営基盤の強化と取引先からの信頼を獲得しています。また約３割強がサイバーセキュリティ教育を実施し、約１割強の企業がSECURITY ACTION 二つ星の対策を実施（「5分でできる！情報セキュリティ自己診断」の得点が70点以上）し、社内のサイバーセキュリティ対策を向上させサイバーインシデント被害の低減の効果を得ています。

■ サイバーセキュリティ対策で、安心感と取引先からの信頼を獲得！

サイバーセキュリティ対策のメリットに対するとして「安全・安心」「信頼・信用」が挙げられており、**企業がセキュリティ対策を通じて、経営基盤の強化に加え、取引先からの信頼の獲得という効果も実感していることが分かります。**

■対策で感じるメリットの回答例

- 安心感が生まれた。
- 取引先からの信頼を得て受注が増えたこと。
- 情報漏洩の回避による信頼の維持ができたこと。
- 事業継続への担保に対する安心感が得られたこと。
- ファイヤーウォールからUTMに変更。アンチウィルスやIDSなど、アクセス内容に不正がないかまでチェックしてくれているので安心度がある。
- 対外的な信頼獲得を得ている。
- 社会的信用力の強化がえられたこと。

■ アンケート結果から見えた、サイバーセキュリティ対策の状況

【サイバーセキュリティ対策投資の状況】

サイバーセキュリティ対策投資をしている割合	（投資していると回答した企業について）	
	年間投資額の平均値	売上高に占める投資額の割合
29.8%	293万円	1.3%

【サイバーセキュリティ対策状況】

「5分でできる！情報セキュリティ自己診断」の得点が70点以上	29件	（12.3%）

➡ SECURITY ACTION 二つ星の対策を多く実施している企業（「5分でできる！情報セキュリティ自己診断」の得点が高い企業）ほど**サイバーインシデントの経験が少なく、被害による影響が少ない**ことが明らかになっています。

サイバーセキュリティ体制を整備している	71件	（30.2%）

➡ サイバーセキュリティ体制が整備されている企業（専門部署がある、兼務だが担当者がいる企業）ほど**取引上の信頼を得ています。**

サイバーセキュリティ教育を実施している（eラーニング、訓練など）	78件	（33.2%）

➡ サイバーセキュリティ教育を実施し社内のサイバーセキュリティ対策を向上させ、サイバーインシデント被害の低減を図っています。

2024年度 中小企業における情報セキュリティ対策に関する実態調査

業種別の対策

小売業

※回答企業数：372件

約２割がサイバーセキュリティ体制を組織的に整備し、経営基盤の強化と取引先からの信頼を獲得しています。また約２割強がサイバーセキュリティ教育を実施し、約１割強の企業がSECURITY ACTION 二つ星の対策を実施（「5分でできる！情報セキュリティ自己診断」の得点が70点以上）し、社内のサイバーセキュリティ対策を向上させサイバーインシデント被害の低減の効果を得ています。

■ サイバーセキュリティ対策で、安心感と取引先からの信頼を獲得！

サイバーセキュリティ対策のメリットに対するとして「安全・安心」「信頼・信用」が挙げられており、**企業がセキュリティ対策を通じて、経営基盤の強化に加え、取引先からの信頼の獲得という効果も実感していることが分かります。**

■対策で感じるメリットの回答例

- 重要情報の流出を未然に防げること。
- 取引先との信頼感構築。
- 個人情報流出に対して、安心感がある。
- 危機に備えて，個々の役割が明確になってきたこと。
- 取引先からの信頼度が上がったように感じられる。
- 取引先の信頼度が向上している。
- 詐欺が少なくなった。
- 顧客からの信頼度が向上した。
- アクセス増につながった。
- 今までも特に問題等は無かったが、より安全、安心感が高まった！
- 迷惑メールが減少。
- 個人情報流出に対して、安心感があること。
- 顧客情報の漏洩を防ぐことができるという安心感を得られたこと。
- 取引先との信頼関係が高まったことで、より多くの取引を行うことが出来ている。
- 顧客情報の管理が楽になった。

■ アンケート結果から見えた、サイバーセキュリティ対策の状況

【サイバーセキュリティ対策投資の状況】

サイバーセキュリティ対策投資をしている割合	（投資していると回答した企業について）	
	年間投資額の平均値	売上高に占める投資額の割合
20.4%	46万円	0.4%

【サイバーセキュリティ対策状況】

「5分でできる！情報セキュリティ自己診断」の得点が70点以上	59件　（15.9%）

➡ SECURITY ACTION 二つ星の対策を多く実施している企業（「5分でできる！情報セキュリティ自己診断」の得点が高い企業）ほど**サイバーインシデントの経験が少なく、被害による影響が少ない**ことが明らかになっています。

サイバーセキュリティ体制を整備している	72件　（19.4%）

➡ サイバーセキュリティ体制が整備されている企業（専門部署がある、兼務だが担当者がいる企業）ほど**取引上の信頼を得ています。**

サイバーセキュリティ教育を実施している（eラーニング、訓練など）	84件　（22.6%）

➡ サイバーセキュリティ教育を実施し社内のサイバーセキュリティ対策を向上させ、サイバーインシデント被害の低減を図っています。

2024年度 中小企業における情報セキュリティ対策に関する実態調査

業種別の対策

金融業、保険業

※回答企業数：125件

約３割強がサイバーセキュリティ体制を組織的に整備し、経営基盤の強化と取引先からの信頼を獲得しています。また約６割がサイバーセキュリティ教育を実施し、約４割強の企業がSECURITY ACTION 二つ星の対策を実施（「5分でできる！情報セキュリティ自己診断」の得点が70点以上）し、社内のサイバーセキュリティ対策を向上させサイバーインシデント被害の低減の効果を得ています。

■ サイバーセキュリティ対策で、安心感と取引先からの信頼を獲得！

サイバーセキュリティ対策のメリットに対するとして「安全・安心」「信頼・信用」が挙げられており、**企業がセキュリティ対策を通じて、経営基盤の強化に加え、取引先からの信頼の獲得という効果も実感していることが分かります。**

■対策で感じるメリットの回答例

- 従業員のセキュリティー意識が向上したこと。
- 従業員の意識が変わり、サイバーに関しての情報を認知し事前対策を講じるようになったこと。
- ウィルス感染時のフォレンジック費用が出ること。
- 迷惑メールの排除ができていること。
- 社員の行動様式にも良い変化と意識が芽生えたこと。
- コンプライアンスの要求があり実施している。
- 一人一人が情報セキュリティーの大切さが分かったこと。
- 個人情報漏洩事故防止。
- 信用アップ。

■企業が実際に取り組んでいるサイバーセキュリティ対策　※インタビュー調査結果より

企業が取り組んでいる対策	効果
内部からの情報漏洩防止の観点による社員からの誓約書の徴集、メモ紙や記録文書の持出に対する意識付けの実施、情報漏洩時のエスカレーションを規定、サイバー保険に加入	被害の低減

■ アンケート結果から見えた、サイバーセキュリティ対策の状況

【サイバーセキュリティ対策投資の状況】

サイバーセキュリティ対策投資をしている割合	（投資していると回答した企業について）	
	年間投資額の平均値	売上高に占める投資額の割合
42.4%	127万円	0.9%

【サイバーセキュリティ対策状況】

「5分でできる！情報セキュリティ自己診断」の得点が70点以上	53件　（42.4%）

➡ SECURITY ACTION 二つ星の対策を多く実施している企業（「5分でできる！情報セキュリティ自己診断」の得点が高い企業）ほど**サイバーインシデントの経験が少なく、被害による影響が少ない**ことが明らかになっています。

サイバーセキュリティ体制を整備している	46件　（36.8%）

➡ サイバーセキュリティ体制が整備されている企業（専門部署がある、兼務だが担当者がいる企業）ほど**取引上の信頼を得ています。**

サイバーセキュリティ教育を実施している（eラーニング、訓練など）	76件　（60.8%）

➡ サイバーセキュリティ教育を実施し社内のサイバーセキュリティ対策を向上させ、サイバーインシデント被害の低減を図っています。

2024年度 中小企業における情報セキュリティ対策に関する実態調査

業種別の対策

不動産業、物品賃貸業

※回答企業数：410件

約２割がサイバーセキュリティ体制を組織的に整備し、経営基盤の強化と取引先からの信頼を獲得しています。また約２割強がサイバーセキュリティ教育を実施し、約１割強の企業がSECURITY ACTION 二つ星の対策を実施（「5分でできる！情報セキュリティ自己診断」の得点が70点以上）し、社内のサイバーセキュリティ対策を向上させサイバーインシデント被害の低減の効果を得ています。

■ サイバーセキュリティ対策で、安心感と取引先からの信頼を獲得！

サイバーセキュリティ対策のメリットに対するとして「安全・安心」「信頼・信用」が挙げられており、**企業がセキュリティ対策を通じて、経営基盤の強化に加え、取引先からの信頼の獲得という効果も実感していることが分かります。**

■対策で感じるメリットの回答例

- 全社員のセキュリティ意識の向上。
- 取引先の信用がついた。
- 情報の漏洩防止。
- リテラシーの向上。
- 必要不可欠な事項として重要。
- 取引先からの信用アップ。
- 顧客からの信頼。
- 個人情報保護。
- 顧客に対して安心感を与えられる。
- 外部からの攻撃に耐えうる安心感がある。
- しっかりとしたセキュリティ対策を出来ていることで安心感が生まれたししっかりと対策を講じている企業として信頼も上がった。
- 大手取引先からの業務提携での仕事、情報機器は、セキュリティはすべて支給される。
- 社員、顧客からの信用・信頼増加。
- 金融取引や個人情報保護は自社の責任として徹底した対策が必要です。その対策として色々な角度からのウイルス防御を慣行している企業は信頼性があるし安心して事業を勧められます。
- 安全安心でのストレス緩和。

■ アンケート結果から見えた、サイバーセキュリティ対策の状況

【サイバーセキュリティ対策投資の状況】

サイバーセキュリティ対策投資をしている割合	（投資していると回答した企業について）	
	年間投資額の平均値	売上高に占める投資額の割合
24.4%	260万円	1.9%

【サイバーセキュリティ対策状況】

「5分でできる！情報セキュリティ自己診断」の得点が70点以上	65件　（15.9%）

➡ SECURITY ACTION 二つ星の対策を多く実施している企業（「5分でできる！情報セキュリティ自己診断」の得点が高い企業）ほど**サイバーインシデントの経験が少なく、被害による影響が少ない**ことが明らかになっています。

サイバーセキュリティ体制を整備している	83件　（20.2%）

➡ サイバーセキュリティ体制が整備されている企業（専門部署がある、兼務だが担当者がいる企業）ほど**取引上の信頼を得ています。**

サイバーセキュリティ教育を実施している（eラーニング、訓練など）	101件　（24.6%）

➡ サイバーセキュリティ教育を実施し社内のサイバーセキュリティ対策を向上させ、サイバーインシデント被害の低減を図っています。

2024年度 中小企業における情報セキュリティ対策に関する実態調査

業種別の対策

学術研究、専門・技術サービス業

※回答企業数：227件

約３割がサイバーセキュリティ体制を組織的に整備し、経営基盤の強化と取引先からの信頼を獲得しています。また約３割がサイバーセキュリティ教育を実施し、約２割強の企業がSECURITY ACTION 二つ星の対策を実施（「5分でできる！情報セキュリティ自己診断」の得点が70点以上）し、社内のサイバーセキュリティ対策を向上させサイバーインシデント被害の低減の効果を得ています。

■ サイバーセキュリティ対策で、安心感と取引先からの信頼を獲得！

サイバーセキュリティ対策のメリットに対するとして「安全・安心」「信頼・信用」が挙げられており、**企業がセキュリティ対策を通じて、経営基盤の強化に加え、取引先からの信頼の獲得という効果も実感していることが分かります。**

■対策で感じるメリットの回答例

- 脅威に対する感度の向上。
- 危機管理の意識向上。
- 信頼感と安心感が増した。
- 安心してインターネットを利用できる。
- 事故が発生しなかったこと。
- お客様に安心してサービスを利用してもらうため。
- セキュリティ対策の周知と共に重要データのバックアップの必要性について周知できたこと。
- マルウェアなどの脅威への対応と情報漏洩のリスクが減少した。
- 効率化と同時に実現できた。
- データ流出のリスクを低減できたこと。
- 安心して業務に取り組める。
- 万が一への対応の重要性の理解。
- 顧客からの信頼。
- 顧客にセキュリティ対策を実施している旨の説明を行い、評価されている。
- 添付ファイルは開かないと言うマインドになったこと。
- 社員のセキュリティ意識も向上した。
- サイバー攻撃やウイルス感染を意識せず業務に注力できる。

■ アンケート結果から見えた、サイバーセキュリティ対策の状況

【サイバーセキュリティ対策投資の状況】

サイバーセキュリティ対策投資をしている割合	（投資していると回答した企業について）	
	年間投資額の平均値	売上高に占める投資額の割合
34.4%	73万円	0.7%

【サイバーセキュリティ対策状況】

「5分でできる！情報セキュリティ自己診断」の得点が70点以上	53件 （23.3%）

➡ SECURITY ACTION 二つ星の対策を多く実施している企業（「5分でできる！情報セキュリティ自己診断」の得点が高い企業）ほど**サイバーインシデントの経験が少なく、被害による影響が少ない**ことが明らかになっています。

サイバーセキュリティ体制を整備している	65件 （28.6%）

➡ サイバーセキュリティ体制が整備されている企業（専門部署がある、兼務だが担当者がいる企業）ほど**取引上の信頼を得ています。**

サイバーセキュリティ教育を実施している（eラーニング、訓練など）	71件 （31.3%）

➡ サイバーセキュリティ教育を実施し社内のサイバーセキュリティ対策を向上させ、サイバーインシデント被害の低減を図っています。

2024年度 中小企業における情報セキュリティ対策に関する実態調査

業種別の対策

宿泊業、飲食サービス業

※回答企業数：175件

約２割がサイバーセキュリティ体制を組織的に整備し、経営基盤の強化と取引先からの信頼を獲得しています。また約３割がサイバーセキュリティ教育を実施し、約１割強の企業がSECURITY ACTION 二つ星の対策を実施（「5分でできる！情報セキュリティ自己診断」の得点が70点以上）し、社内のサイバーセキュリティ対策を向上させサイバーインシデント被害の低減の効果を得ています。

■ サイバーセキュリティ対策で、安心感と取引先からの信頼を獲得！

サイバーセキュリティ対策のメリットに対するとして「安全・安心」「信頼・信用」が挙げられており、**企業がセキュリティ対策を通じて、経営基盤の強化に加え、取引先からの信頼の獲得という効果も実感していることが分かります。**

■対策で感じるメリットの回答例

- 情報管理などのリスクマネジメントが向上した。
- 従業員の意識が高まった。
- 防犯対策として効果があり。
- 個人情報(従業員含む)と、仕事関連企業へ迷惑をかけないため。
- 顧客の情報の管理や安全性の確保等が確固たるモノになった。
- お取引様・顧客の安心感。
- 顧客の情報が守られるようになった。
- 従業員の意識向上にはつながった。
- ウィルス対策が強固になって時間を有効活用できている。
- WEBサイトで、発表して、顧客の信頼を勝ち得たと思います。
- 会計事務所とのやりとりなど、取引先とのやりとりを、安心して行うことができる。
- 不正決済の防止。
- 顧客情報などの情報漏洩を防いでいる。

■ アンケート結果から見えた、サイバーセキュリティ対策の状況

【サイバーセキュリティ対策投資の状況】

サイバーセキュリティ対策投資をしている割合	（投資していると回答した企業について）	
	年間投資額の平均値	売上高に占める投資額の割合
16.6%	36万円	0.3%

【サイバーセキュリティ対策状況】

「5分でできる！情報セキュリティ自己診断」の得点が70点以上	22件 （12.6%）

➡ SECURITY ACTION 二つ星の対策を多く実施している企業（「5分でできる！情報セキュリティ自己診断」の得点が高い企業）ほど**サイバーインシデントの経験が少なく、被害による影響が少ない**ことが明らかになっています。

サイバーセキュリティ体制を整備している	37件 （21.1%）

➡ サイバーセキュリティ体制が整備されている企業（専門部署がある、兼務だが担当者がいる企業）ほど**取引上の信頼を得ています。**

サイバーセキュリティ教育を実施している（eラーニング、訓練など）	49件 （28.0%）

➡ サイバーセキュリティ教育を実施し社内のサイバーセキュリティ対策を向上させ、サイバーインシデント被害の低減を図っています。

2024年度 中小企業における情報セキュリティ対策に関する実態調査

業種別の対策

生活関連サービス業、娯楽業

※回答企業数：175件

約２割がサイバーセキュリティ体制を組織的に整備し、経営基盤の強化と取引先からの信頼を獲得しています。また約２割強がサイバーセキュリティ教育を実施し、約１割強の企業がSECURITY ACTION 二つ星の対策を実施（「5分でできる！情報セキュリティ自己診断」の得点が70点以上）し、社内のサイバーセキュリティ対策を向上させサイバーインシデント被害の低減の効果を得ています。

■ サイバーセキュリティ対策で、安心感と取引先からの信頼を獲得！

サイバーセキュリティ対策のメリットに対するとして「安全・安心」「信頼・信用」が挙げられており、**企業がセキュリティ対策を通じて、経営基盤の強化に加え、取引先からの信頼の獲得という効果も実感していることが分かります。**

■対策で感じるメリットの回答例

- 社員のリスク管理に対する意識の向上と、クライアントへの信頼度の向上。
- 効率アップ。
- 安心感。
- 自社社員だけではなく、取引先からも安心して貰えたこと。
- 資料などがパソコン内で管理運用出来、紙媒体が削減出来て書類等余り持ち出しせずに済むこと。
- 社員の意識改革。
- 顧客情報の管理が万全であること。
- 安心感。
- 安心してインターネット作業ができる。
- 信頼性を向上させられたと思っている。
- 情報管理に対する安心感。
- 個人情報保護法に準じた個人情報の保管方法の徹底。メリットは従業員の意識が変わった事、従業員毎にまちまちだった保管方法が一律管理出来るようになったこと。
- 社員の意識改革につながっている。
- 仕事に専念できる。
- 信頼性向上。

■ アンケート結果から見えた、サイバーセキュリティ対策の状況

【サイバーセキュリティ対策投資の状況】

サイバーセキュリティ対策投資をしている割合	（投資していると回答した企業について）	
	年間投資額の平均値	売上高に占める投資額の割合
20.0%	413万円	3.4%

【サイバーセキュリティ対策状況】

「5分でできる！情報セキュリティ自己診断」の得点が70点以上	26件	（14.9%）

➡ SECURITY ACTION 二つ星の対策を多く実施している企業（「5分でできる！情報セキュリティ自己診断」の得点が高い企業）ほど**サイバーインシデントの経験が少なく、被害による影響が少ない**ことが明らかになっています。

サイバーセキュリティ体制を整備している	34件	（19.4%）

➡ サイバーセキュリティ体制が整備されている企業（専門部署がある、兼務だが担当者がいる企業）ほど**取引上の信頼を得ています。**

サイバーセキュリティ教育を実施している（eラーニング、訓練など）	40件	（22.9%）

➡ サイバーセキュリティ教育を実施し社内のサイバーセキュリティ対策を向上させ、サイバーインシデント被害の低減を図っています。

2024年度 中小企業における情報セキュリティ対策に関する実態調査

業種別の対策

教育、学習支援業

※回答企業数：133件

約３割がサイバーセキュリティ体制を組織的に整備し、経営基盤の強化と取引先からの信頼を獲得しています。また約４割弱がサイバーセキュリティ教育を実施し、約３割の企業がSECURITY ACTION 二つ星の対策を実施（「5分でできる！情報セキュリティ自己診断」の得点が70点以上）し、社内のサイバーセキュリティ対策を向上させサイバーインシデント被害の低減の効果を得ています。

■ サイバーセキュリティ対策で、安心感と取引先からの信頼を獲得！

サイバーセキュリティ対策のメリットに対するとして「安全・安心」「信頼・信用」が挙げられており、**企業がセキュリティ対策を通じて、経営基盤の強化に加え、取引先からの信頼の獲得という効果も実感していることが分かります。**

■対策で感じるメリットの回答例

- 情報を守る重要性。
- 安心安全な運用。
- 危機管理意識。
- 情報を守る重要性。
- ステークホルダーからの信頼の獲得。
- 取引先から、それなら安心、と言われた。
- 不正利用の排除。
- 法令順守の従業員の意識向上。
- 情報漏洩や情報セキュリティ事故の防止。コスト削減。
- 顧客情報漏洩の軽減に対する安心感。
- 新規取引先の獲得。
- 対クライアントアピール。
- 個人情報の取り扱いの厳正さを再認識できた。
- 社内の情報管理体制が、良い意味でピリピリしはじめた。
- 顧客からの信頼性の獲得。
- セキュアは、当塾にとっても顧客にとっても信用につながる。

■企業が実際に取り組んでいるサイバーセキュリティ対策　※インタビュー調査結果より

企業が取り組んでいる対策	効果
大手塾の情報漏洩事案を受けて個人塾についても顧客等から情報管理に不信感が抱かれたため、**ISMS認証を取得**し、**情報管理の意識向上と顧客からの信頼獲得を図った。**	**経営基盤の強化 信頼の獲得**

■ アンケート結果から見えた、サイバーセキュリティ対策の状況

【サイバーセキュリティ対策投資の状況】

サイバーセキュリティ対策投資をしている割合	（投資していると回答した企業について）	
	年間投資額の平均値	売上高に占める投資額の割合
28.6%	99万円	0.8%

【サイバーセキュリティ対策状況】

「5分でできる！情報セキュリティ自己診断」の得点が70点以上	36件　（27.1%）

➡ SECURITY ACTION 二つ星の対策を多く実施している企業（「5分でできる！情報セキュリティ自己診断」の得点が高い企業）ほど**サイバーインシデントの経験が少なく、被害による影響が少ない**ことが明らかになっています。

サイバーセキュリティ体制を整備している	36件　（27.1%）

➡ サイバーセキュリティ体制が整備されている企業（専門部署がある、兼務だが担当者がいる企業）ほど**取引上の信頼を得ています。**

サイバーセキュリティ教育を実施している（eラーニング、訓練など）	48件　（36.1%）

➡ サイバーセキュリティ教育を実施し社内のサイバーセキュリティ対策を向上させ、サイバーインシデント被害の低減を図っています。

2024年度 中小企業における情報セキュリティ対策に関する実態調査

業種別の対策

医療、福祉

※回答企業数：133件

約４割がサイバーセキュリティ体制を組織的に整備し、経営基盤の強化と取引先からの信頼を獲得しています。また約5割がサイバーセキュリティ教育を実施し、約２割の企業がSECURITY ACTION 二つ星の対策を実施（「5分でできる！情報セキュリティ自己診断」の得点が70点以上）し、社内のサイバーセキュリティ対策を向上させサイバーインシデント被害の低減の効果を得ています。

■ サイバーセキュリティ対策で、安心感と取引先からの信頼を獲得！

サイバーセキュリティ対策のメリットに対するとして「安全・安心」「信頼・信用」が挙げられており、**企業がセキュリティ対策を通じて、経営基盤の強化に加え、取引先からの信頼の獲得という効果も実感していることが分かります。**

■対策で感じるメリットの回答例

- 顧客に安心感を与えられる。
- 職員のセキュリティに対する意識が向上した。
- 運用は少し面倒であるが、稼働しだしてからは工数は減っている。取引先の信用度アップ。
- 不審メールの減少。
- 職員の意識改革が出来た。
- 若い社員の信頼が増した。
- 個人情報保護による信頼。
- 個人情報の管理が確実になった。
- 思っていたよりも簡単に対策できるし、社としても効率が上がりました。導入して本当に良かったと思いました。
- 顧客アピール。
- 顧客情報の漏洩防止。
- 顧客情報を扱う上でのセキュリティ対策はとても重要。
- 安心して業務ができる。
- 自社の情報を厳密に守ることができる。
- インターネット等を安心して利用できる。
- 情報漏えい等の事故の防止、顧客情報の持ち出しや紛失の防止。

■ アンケート結果から見えた、サイバーセキュリティ対策の状況

【サイバーセキュリティ対策投資の状況】

サイバーセキュリティ対策投資をしている割合	（投資していると回答した企業について）	
	年間投資額の平均値	売上高に占める投資額の割合
31.6%	91万円	0.7%

【サイバーセキュリティ対策状況】

「5分でできる！情報セキュリティ自己診断」の得点が70点以上	28件	（21.1%）

➡ SECURITY ACTION 二つ星の対策を多く実施している企業（「5分でできる！情報セキュリティ自己診断」の得点が高い企業）ほど**サイバーインシデントの経験が少なく、被害による影響が少ない**ことが明らかになっています。

サイバーセキュリティ体制を整備している	55件	（41.4%）

➡ サイバーセキュリティ体制が整備されている企業（専門部署がある、兼務だが担当者がいる企業）ほど**取引上の信頼を得ています。**

サイバーセキュリティ教育を実施している（eラーニング、訓練など）	63件	（47.4%）

➡ サイバーセキュリティ教育を実施し社内のサイバーセキュリティ対策を向上させ、サイバーインシデント被害の低減を図っています。

2024年度 中小企業における情報セキュリティ対策に関する実態調査

業種別の対策

その他のサービス業

※回答企業数：553件

約２割強がサイバーセキュリティ体制を組織的に整備し、経営基盤の強化と取引先からの信頼を獲得しています。また、約３割がサイバーセキュリティ教育を実施し、４分の1の企業がSECURITY ACTION 二つ星の対策を実施（「5分でできる！情報セキュリティ自己診断」の得点が70点以上）し、社内のサイバーセキュリティ対策を向上させサイバーインシデント被害の低減の効果を得ています。

■ サイバーセキュリティ対策で、安心感と取引先からの信頼を獲得！

サイバーセキュリティ対策のメリットに対するとして「安全・安心」「信頼・信用」が挙げられており、**企業がセキュリティ対策を通じて、経営基盤の強化に加え、取引先からの信頼の獲得という効果も実感していることが分かります。**

■対策で感じるメリットの回答例

- 従業員の情報セキュリティに関する意識が向上した。
- 取引先の要求基準に適合。
- 会社としての信用、信頼性の維持。
- 情報流出による単社のみならずグループ会社全体への信頼失墜を防ぐ。
- メールをはじめとするインターネット環境の安心感が高まった。
- 実際にインシデントが発生する可能性が減ることと、対外的な信頼度のアップ。
- 個人情報保護、事案機密の保護が具体化出来た。
- アウトソーシングや自社開発のアプリが多いため、情報セキュリティなしでは、ソースや文書のやり取りに不安があったが、不安が払拭された。
- セキュリティ対策をすることで新規獲得できた。
- 大手企業からの信頼が得られ受注数が増えた。

■企業が実際に取り組んでいるサイバーセキュリティ対策　※インタビュー調査結果より

企業が取り組んでいる対策	効果
業務終了時にオフィス内ネットワークを完全に遮断することで、不正アクセスによる**被害の低減とともに安心感を得られた。**	被害の低減
機密情報は別々のデバイスで管理することで、漏洩リスクを軽減	被害の低減

■ アンケート結果から見えた、サイバーセキュリティ対策の状況

【サイバーセキュリティ対策投資の状況】

サイバーセキュリティ対策投資をしている割合	（投資していると回答した企業について）	
	年間投資額の平均値	売上高に占める投資額の割合
24.8%	161万円	1.2%

【サイバーセキュリティ対策状況】

「5分でできる！情報セキュリティ自己診断」の得点が70点以上	140件　（25.3%）

➡ SECURITY ACTION 二つ星の対策を多く実施している企業（「5分でできる！情報セキュリティ自己診断」の得点が高い企業）ほど**サイバーインシデントの経験が少なく、被害による影響が少ない**ことが明らかになっています。

サイバーセキュリティ体制を整備している	132件　（23.9%）

➡ サイバーセキュリティ体制が整備されている企業（専門部署がある、兼務だが担当者がいる企業）ほど**取引上の信頼を得ています。**

サイバーセキュリティ教育を実施している（eラーニング、訓練など）	170件　（30.7%）

➡ サイバーセキュリティ教育を実施し社内のサイバーセキュリティ対策を向上させ、サイバーインシデント被害の低減を図っています。

2024年度 中小企業における情報セキュリティ対策に関する実態調査
業種ごとの効果的な取組事例集
https://www.ipa.go.jp/security/reports/sme/sme-survey2024.html

2025年5月
独立行政法人情報処理推進機構
©Information-technology Promotion Agency, Japan（IPA）
https://www.ipa.go.jp/