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報告書（概要説明資料）

2025年5月

独立行政法人情報処理推進機構

IPA Better Life with IT

目次

1．調査目的

- **背景**
  - 近年、サプライチェーン上の弱点を狙って、攻撃対象への侵入を図るサイバー攻撃が顕在化・高度化している。サプライチェーンを構成する中小企業等がサイバー攻撃に対する対策が不十分である場合、当該中小企業等の事業活動に支障が生じ得ることに加えて、取引先が提供した重要な情報が流出してしまうおそれや、当該企業を踏み台にして取引先が攻撃されるおそれ等がある。
  - IPAでは、「2021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」（以下、「2021年度調査」という）を実施し、中小企業等における情報セキュリティ対策の実態を明らかにした。2023年度に「SA宣言事業者における情報セキュリティ対策の実態調査」（以下「2023年度調査」という。）を実施した。その結果、SA宣言により取引先からの信頼性が高まる等の期待に反して十分な効果が得られていないこと、二つ星の宣言事業者の中には現状の取組より一層高度化させたい意向があること等を明らかにした。
- **目的**
  - 「2021年度調査」からの経年変化の把握、および「2023年度調査」の結果を踏まえ、中小企業等におけるサイバーセキュリティ対策の実態及び課題等を明らかにし、中小企業等における規模・業種等に応じた効果の高いサイバーセキュリティ対策の分析・整理することで、サプライチェーン全体のサイバーセキュリティ強化に資することを目的とする。
  - また、SECURITY ACTION一つ星及び二つ星に求められる基準について分析・調査し、SECURITY ACTION宣言及びサイバーセキュリティお助け隊サービスを導入する中小企業が、中小企業全体の割合に対して低い水準となっている理由を分析・調査する。

2．調査概要

- 文献調査、アンケート調査及びインタビュー調査を実施のうえ、調査結果を取りまとめた調査報告書を作成した。

文献調査

【概要】
「2021年度調査」からの経年変化の把握、中小企業等における規模・業種等に応じた効果の高いサイバーセキュリティ対策の分析・整理を行うにあたり、以下を調査観点として設定し、関連する文献および制度に関する調査を行った。

調査対象	以下を調査観点として設定し、20件の文献について調査を実施した。 【調査の観点】 • 中小企業の実態（経営状況）と支払意思 • 中小企業が被るサイバーインシデント被害と被害額の動向 • 自社が行っているサイバーセキュリティ対策に関する認識 • 中小企業向けサイバーセキュリティ対策ソリューションの動向とコスト感 • 業界に限らず中小企業等が実施すべきサイバーセキュリティ対策等の観点 • サプライチェーンの一員としてセキュリティ対策の必要性に関する認識 • サプライチェーンセキュリティにおける評価取得のメリット等の観点

アンケート調査

【概要】
中小企業のサイバーセキュリティ対策への取り組みや被害の状況、対策実施における課題、経営層の関与や認識に関する実態を把握するためアンケート調査を実施した。調査手法はWebアンケートモニタ調査とし、モニタの中から本調査の対象となる経営層及び情報システムの担当者に対してアンケート依頼を送付し、4,191件の有効回答を得た。

調査対象	中小企業等の経営層及び情報システム／情報セキュリティの担当マネージャ
調査期間	2024年10月25日（金）～11月６日（水）
調査項目数	概要設問8問、本設問104問 ※概要設問（業種、回答者の役職等）スクリーニングを実施し、有効回答を得られると判断した回答者が本設問へ進む
調査項目	1. 回答者の属性 2. 回答企業の属性 3. ITの導入状況 4. 情報セキュリティに関する意識・状況 5. 情報セキュリティ教育の状況 6. サイバーインシデント被害の状況 7. 取引先を含む情報セキュリティ対策 8.「SECURITY ACTION」の宣言状況 9.「サイバーセキュリティお助け隊サービス」の導入状況 10. 情報セキュリティ対策の状況（25項目）
調査手法	Webアンケートモニタ調査（NTTコム リサーチ） Webモニタに対してアンケートを実施
有効回答数	４,１９１件

インタビュー調査

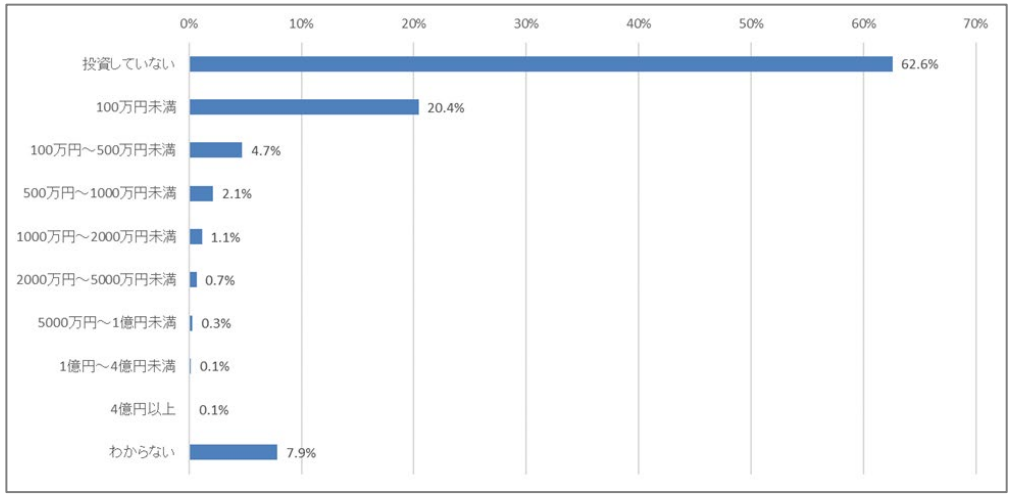
【概要】
アンケート調査の結果を踏まえ、有効な取組を実施していると想定される中小企業等を抽出のうえ、アンケート調査では捉えきれない実態等を把握し、有効な対策や効果を明らかにすることを目的にインタビュー調査を実施し、インタビュー調査結果をもとに、他社の模範となる取組や、他社にとって参考になる取組について、グッドプラクティスを整理した。

調査対象	アンケート回答者のうち有効な取組を実施していると想定される中小企業等を抽出し、実際にインタビュー調査の了解を得た回答者
調査期間	2024年11月28日（木）～12月20日（金）
調査項目数	15問
調査項目	1. 管理体制の確保状況 2. セキュリティ対策を行う上で重視していること 3. セキュリティ対策にかかるコストの相場観 4. コストをかけずに実施した対策 5. 対策によるメリット 6. 必要としている対策とその実現性 7. 費用対効果の悪い対策 8. セキュリティ対策の要請とコストの考え方
調査手法	オンラインインタビューを実施
有効回答数	２１件

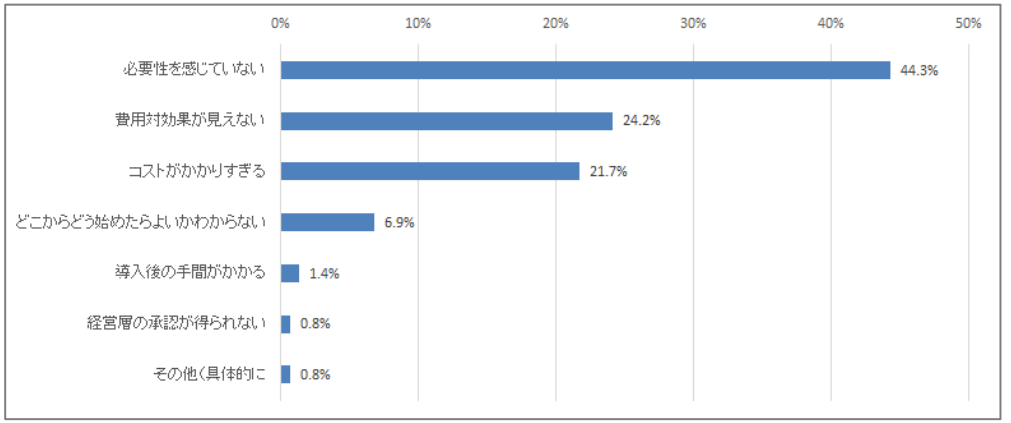
3．アンケート調査結果
サイバーセキュリティ対策への取組状況

- サイバーセキュリティ対策への取組状況として、情報セキュリティ対策投資の状況を見ると、全体の約7割が「投資していない」または「わからない」という回答である。投資を行っていても、約2割は「100万円未満」であり、中小企業等においては情報セキュリティ対策への投資を行うケースは限られている。（左図）
- また「投資していない」理由としては、「必要性を感じていない」が約44%であり半数近くが情報セキュリティへの意識がそもそも低いという結果が出ている。さらに「費用対効果が見えない」と「コストがかかりすぎる」を合わせると45%を超えており、中小企業として資金が限られる中で情報セキュリティ投資に踏み出せない状況がうかがえる。（右図）

質問：直近過去3期の情報セキュリティ対策投資額（IT機器や社員への 教育等も含む）の概算について教えてください。(SA)



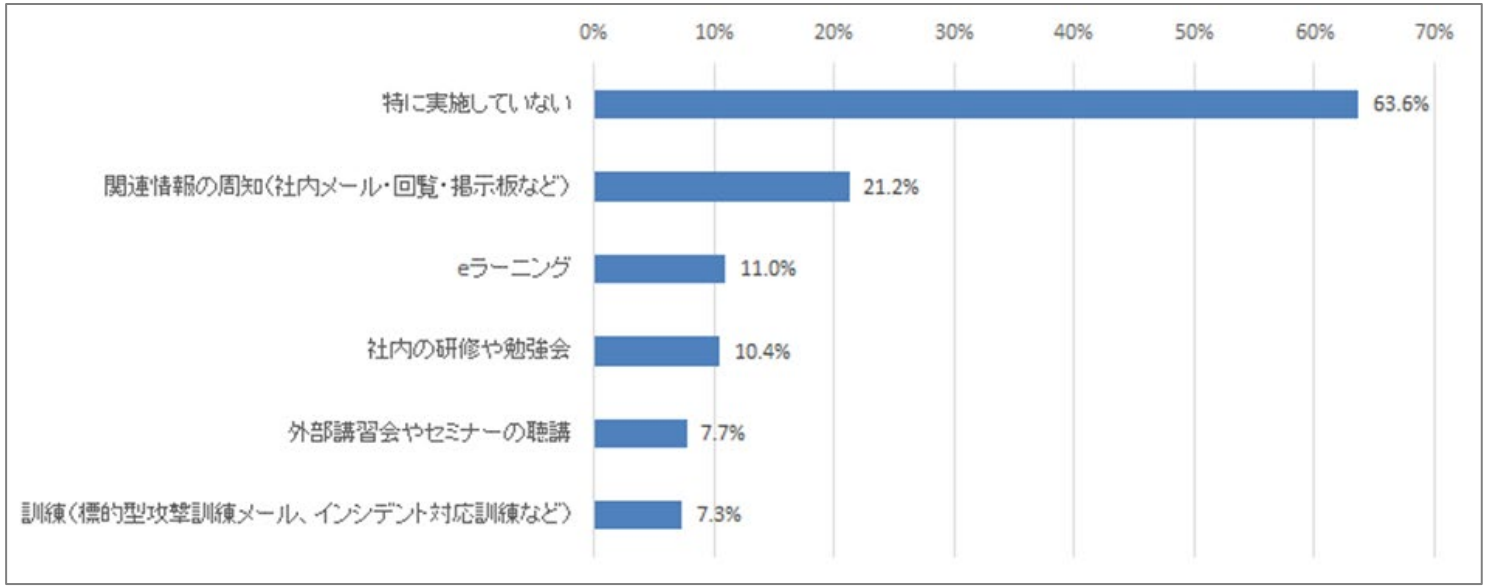
質問：情報セキュリティ対策投資額について「投資をしていない」とお答えになった一番の理由について教えてください。(SA)



3．アンケート調査結果
従業員に対する情報セキュリティ教育の実施状況

- 経営層が積極的に従業員に対する情報セキュリティ教育を実施することは、組織全体としての情報セキュリティ人材育成に向けた重要課題であるが、情報セキュリティ教育として特に実施していないと回答した企業が63.6%である。この高い割合は、経営層を含めた全社的なセキュリティ意識向上の機会が不足していることを示唆している。（下図）

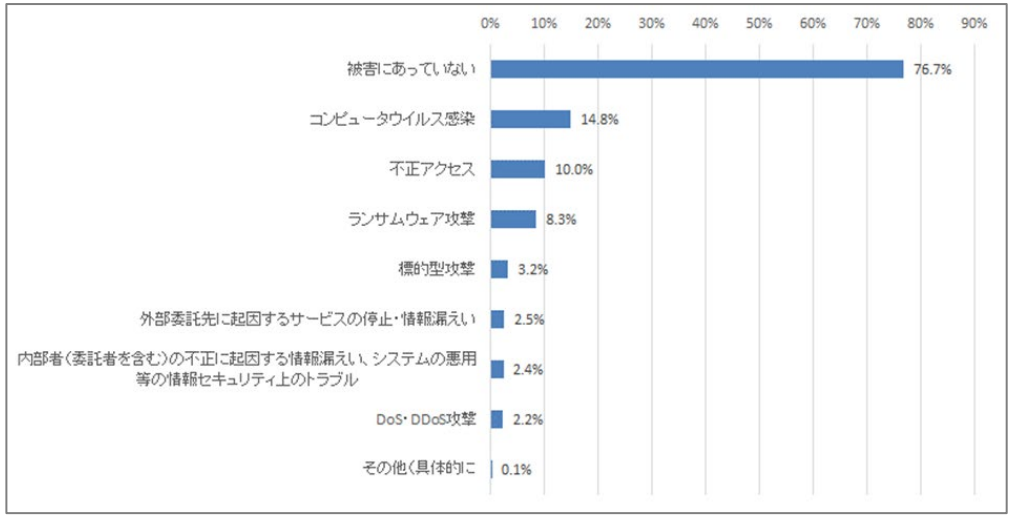
質問：貴社では従業員に対する情報セキュリティ教育をどのように実施していますか。(MA)



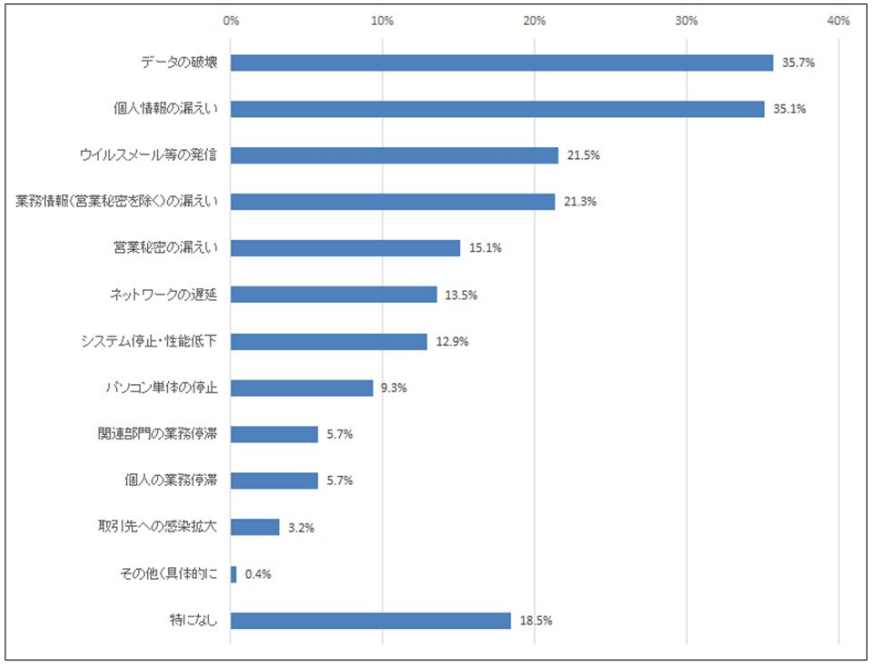
3．アンケート調査結果
サイバーセキュリティに関する被害の状況

- 2023年度において、サイバーインシデントの被害を受けた企業はコンピュータウイルスの感染が14.8%と最も多く、その次に不正アクセスの影響を10.0%の企業が受けている。これらの被害は中小企業にとって現実的な脅威であることが示されている。（左図）
- サイバーインシデントによる影響として、データの破壊（35.7%）や個人情報の漏えい（35.1%）が最も多く発生している。これによって企業の信頼性や業務運営に直結する深刻な問題が発生している状況が分かる。（右図）

質問：2023年度にサイバーインシデントの発生、もしくは発生があった可能性が高い経験はありましたか。(MA)



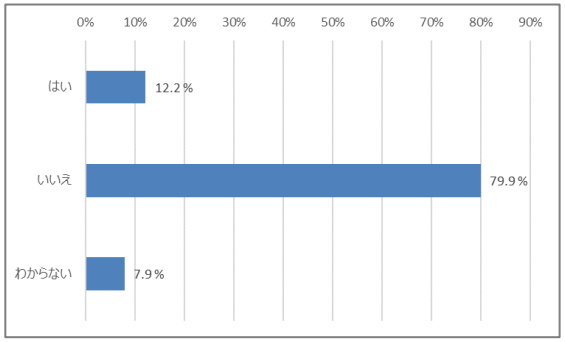
質問：貴社でサイバーインシデントによる影響で、生じた被害について教えてください。(MA)



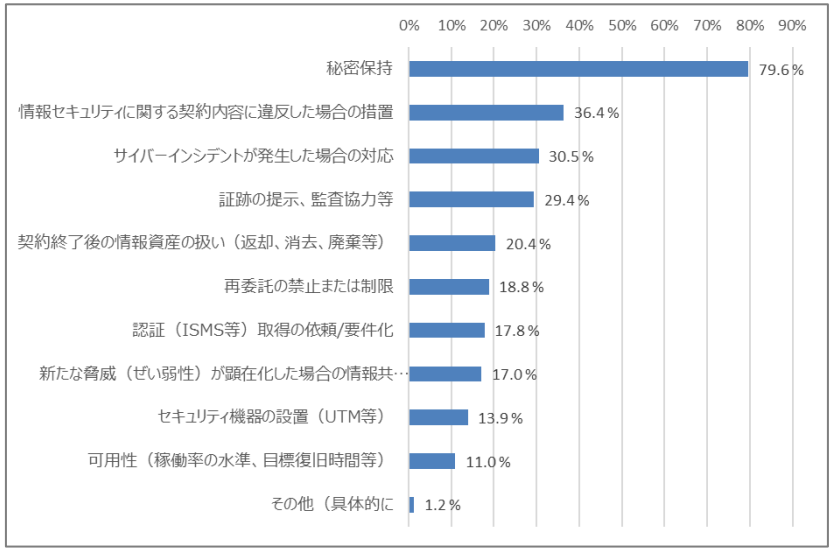
3．アンケート調査結果
発注元企業からの情報セキュリティに関する要請と対応状況

- 発注元企業から情報セキュリティに関する要請を受けた経験がある企業の割合は1割強である。（右図）
- 要請された内容は、8割が「秘密保持のための措置」（79.6%）である。（左下図）
- 要請された対策の実施に向けての課題は、「対策費用（具体的な対策と費用）の用意、費用負担の検討」（51.3%）が最も多く、次いで「情報セキュリティ対策に関する販売先（発注元企業）との契約内容の明確化」（47.0%）、「専門人材の確保・育成」（32.9%）であり、コストや人材不足が課題となっていることがうかがえる。（右下図）

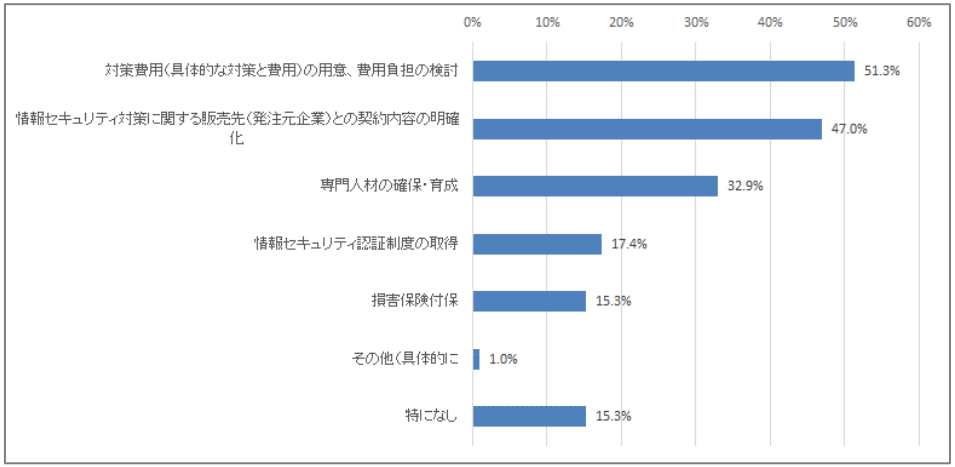
質問：発注元企業から貴社への情報セキュリティに関する要請を受けた経験はありますか。(SA)



質問：貴社への情報セキュリティに関する要請の具体的な内容について教えてください。(MA)



質問：発注元企業から情報セキュリティ対策の要請を受けた場合に、対策の実施に向けての課題となることについて教えてください。(MA)



4. 考察

中小企業等における規模・業種等に応じた効果の高いサイバーセキュリティ対策について（1/8）

- アンケート調査の結果に基づき、回答企業のサイバーセキュリティ対策の内容及びサイバーセキュリティ対策投資に関する設問を分析軸として、サイバーセキュリティ対策の効果を示すと考えられる設問とのクロス集計分析を実施した。
- この分析を通じて、各設問における回答結果間との関係性を明らかにし、サイバーセキュリティ対策と期待される効果との関連性を評価した分析のアプローチとして、セキュリティ対策投資が発生するアンケートの設問について効果と考えられる設問とのクロス分析を行い、各対策投資が効果にどのような影響を及ぼすか傾向を評価した。
- 評価の結果、以下の点が明らかになった。
  - 企業の規模に関わらず、①IPAが提供する「5分でできる！情報セキュリティ自社診断」の評価項目の対策の実施がサイバーインシデント被害の低減に効果のある対策であり、特に中小企業(100名以下)及び中小企業(101名以上)においては、取引上におけるメリットに効果のある対策でもあること。
  - 企業の規模・業種に関わらず、②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（ISMS認証、Pマーク）、③サイバーセキュリティ体制の整備、④取引におけるリスク認識は、取引上における効果のある対策である。

4. 考察

中小企業等における規模・業種等に応じた効果の高いサイバーセキュリティ対策について（2/8）

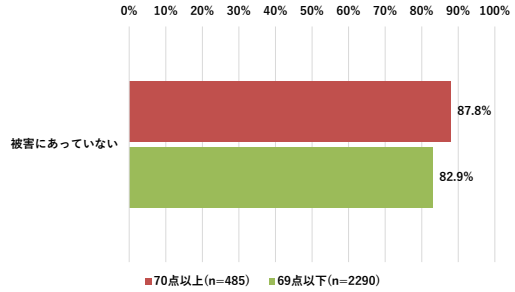
①IPAが提供する「5分でできる！情報セキュリティ自社診断」の評価項目の対策の実施（小規模企業）

分析結果

IPA「5分でできる！情報セキュリティ自社診断」の項目に該当するアンケート設問(Q80)の回答結果を自社診断の基準に沿って点数化し、分析を行った結果、小規模企業者においては、自社診断の合計点とサイバーインシデント被害との間に、一貫した関連性があることが分かった。

■サイバーインシデントの被害経験

Q34において「被害にあっていない」と回答した企業の割合は、自社診断の合計点が高いほど高くなる傾向が見られる。



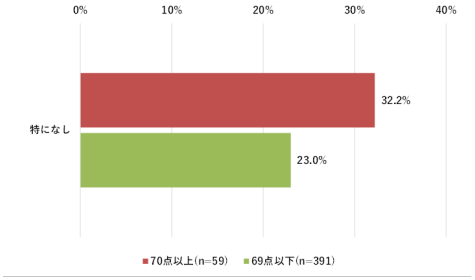
■サイバーインシデントの被害額

Q39において自社診断の合計点が高いほど、インシデントの被害額の最大値が下がっていることが確認できる。

自社診断の合計点	回答企業数	平均値	最大値
70点以上	59	約10万円	100万円
69点以下	391	約20万円	5000万円

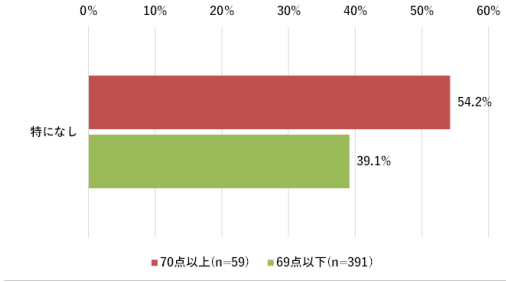
■サイバーインシデントによる影響

自社診断の合計点が高い企業ほど、サイバーインシデントによる影響を「特になし」と回答する割合が高い傾向が認められた。



■サプライチェーンへの影響

自社診断の合計点が高いほど、サプライチェーンへの影響について特になしと回答している企業の割合が高くなっていることが分かる。



4. 考察

中小企業等における規模・業種等に応じた効果の高いサイバーセキュリティ対策について（3/8）

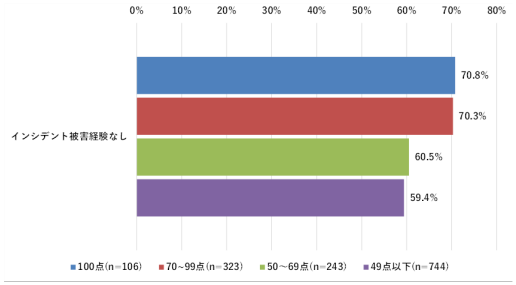
①IPAが提供する「5分でできる！情報セキュリティ自社診断」の評価項目の対策の実施（中小企業）

分析結果

IPA「5分でできる！情報セキュリティ自社診断」の項目に該当するアンケート設問(Q80)の回答結果を自社診断の基準に沿って点数化し、分析を行った結果、中小企業(100名以下)及び中小企業(101名以上)においては、自社診断の合計点とサイバーインシデント被害との間に、一貫した関連性があることが分かった。

■サイバーインシデントの被害経験

Q34において「被害にあっていない」と回答した企業の割合は、自社診断の合計点が高いほど高くなる傾向が見られる。



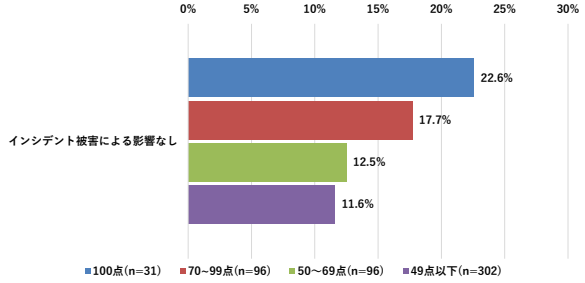
■サイバーインシデントの被害額

Q39.において自社診断の合計点が高いほど、インシデントの被害額の最大値が下がっていることが確認できる。

自社診断の合計点	回答企業数	平均	最大値
100点	31	約39万円	500万円
70～99点	96	約162万円	3000万円
50～69点	96	約180万円	8000万円
49点以下	302	約96万円	1億円

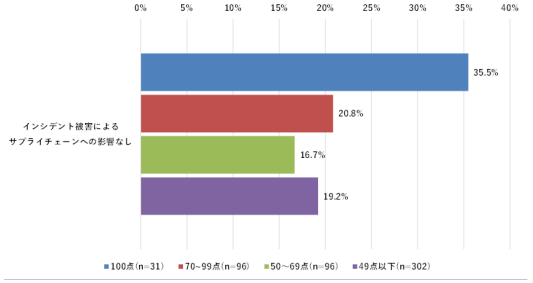
■サイバーインシデントによる影響

自社診断の合計点が高い企業ほど、サイバーインシデントによる影響を「特になし」と回答する割合が高い傾向が認められた。



■サプライチェーンへの影響

自社診断の合計点が高いほど、サプライチェーンへの影響について特になしと回答している企業の割合が高くなっていることが分かる。



4. 考察

中小企業等における規模・業種等に応じた効果の高いサイバーセキュリティ対策について（4/8）

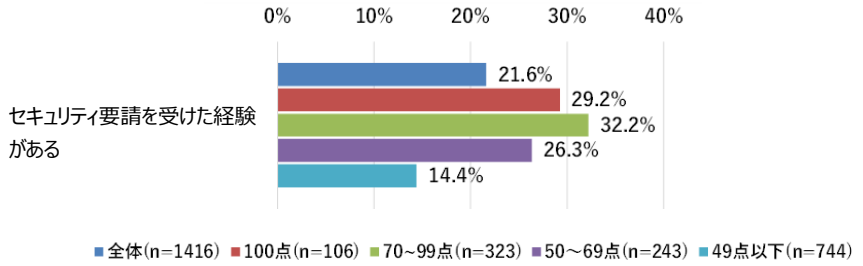
①IPAが提供する「5分でできる！情報セキュリティ自社診断」の評価項目の対策の実施（中小企業）

分析結果

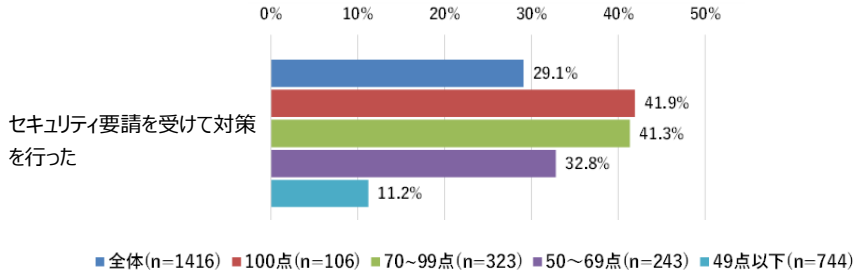
自社診断の基準に沿って点数化し、分析を行った結果、中小企業(100名以下)及び中小企業(101名以上)においては、自社診断の合計点の高さが、取引先からのセキュリティ要請への対応状況や、それを取引上のメリットとして認識する度合いと、一貫した関連性があることが分かった。

■取引におけるセキュリティ要請とその対応

自社診断の合計点が70点以上の企業はセキュリティ要請経験があると回答している割合が高いことが分かる。

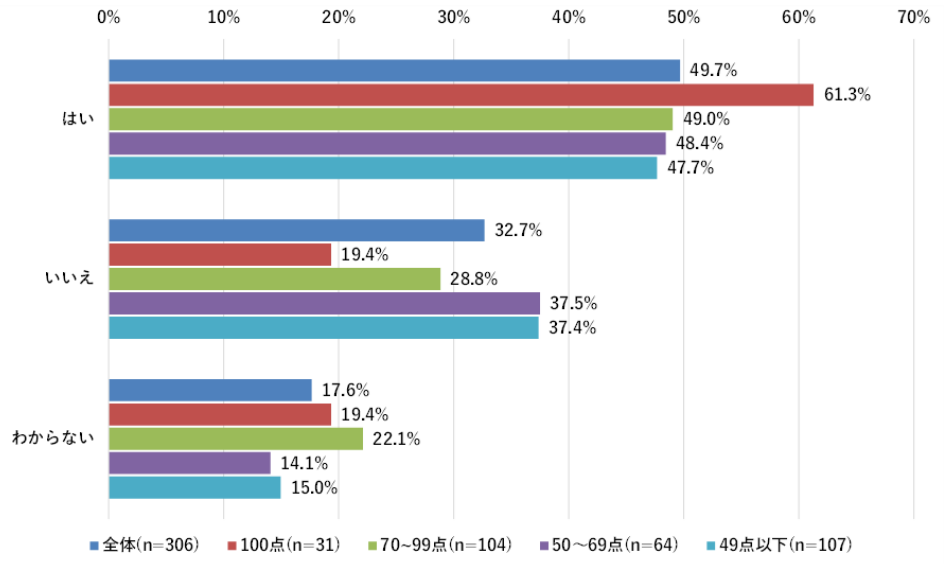


セキュリティ要請に応じたと回答している割合は自社診断の合計点が高い方が多いことが分かる。



■セキュリティ要請応じたことが取引につながったか

自社診断の合計点が高い企業ほど、はい（取引につながった）と回答している割合が高い傾向が読み取れる。



4. 考察

中小企業等における規模・業種等に応じた効果の高いサイバーセキュリティ対策について（5/8）

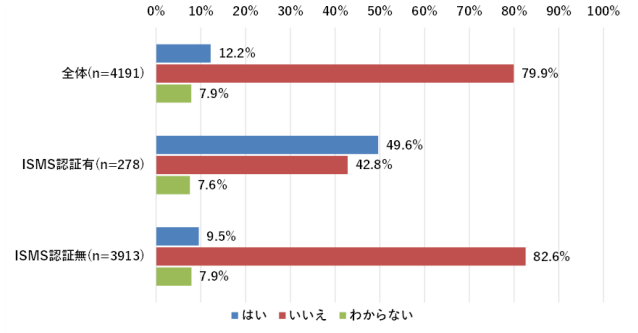
②サイバーセキュリティ対策に関する第三者評価制度の取得（ISMS取得、Pマーク取得）による効果

分析結果

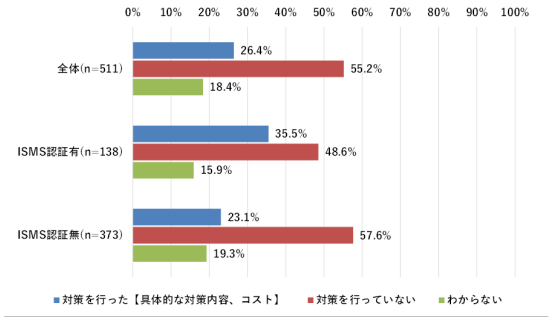
ISMS評価制度取得およびPマーク取得状況に関する設問（Q77）を軸としたクロス集計の結果、ISMSおよびPマークを取得している企業の方が、取引先からのセキュリティ要請への対応状況や、それを取引上のメリットとして認識する度合いと、一貫した関連性があることが分かった。

■ISMS取得状況と取引におけるセキュリティ要請

ISMSを取得している企業では50%の企業、ISMSを取得していない企業では約１０％の企業でセキュリティ対策の要請を受けた。（取得有無で約5倍）

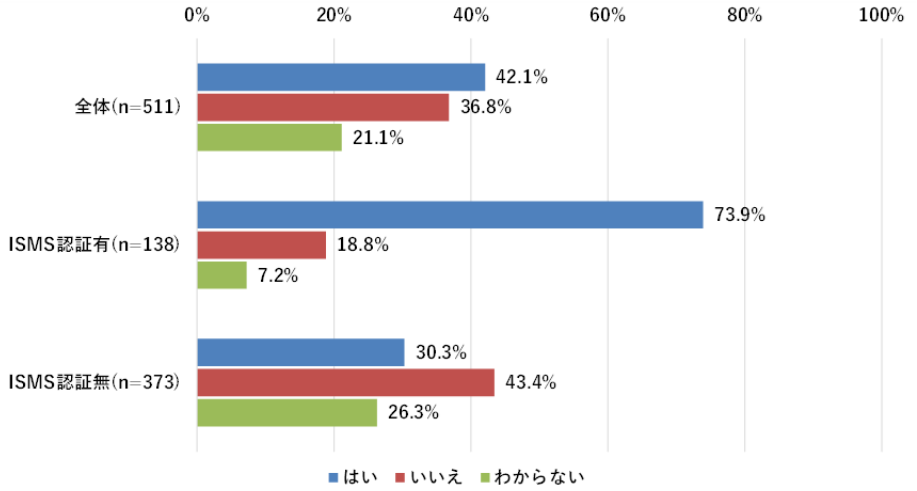


セキュリティ要請に応じた割合に関してはISMSを取得している企業の方が約1.5倍高かった。（取得有無で約1.5倍）



■セキュリティ要請応じたことが取引につながったか

セキュリティ要請に応じたことが取引につながったと回答した企業がISMSを取得している企業の方が約2.5倍高かった（取得有無で約2.5倍）



4. 考察

中小企業等における規模・業種等に応じた効果の高いサイバーセキュリティ対策について（6/8）

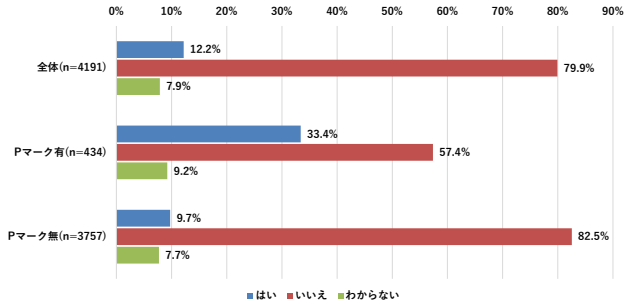
②サイバーセキュリティ対策に関する第三者評価制度の取得（ISMS取得、Pマーク取得）による効果

分析結果

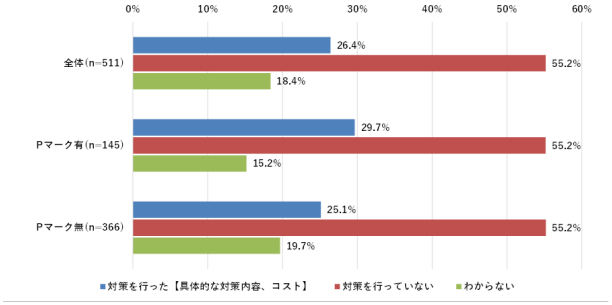
ISMS評価制度取得およびPマーク取得状況に関する設問（Q77）を軸としたクロス集計の結果、ISMSおよびPマークを取得している企業の方が、取引先からのセキュリティ要請への対応状況や、それを取引上のメリットとして認識する度合いと、一貫した関連性があることが分かった。

■Pマーク取得状況と取引におけるセキュリティ要請

Pマークを取得している企業では50%の企業、 Pマークを取得していない企業では約10%の企業でセキュリティ対策の要請を受けた。（取得有無で約5倍）

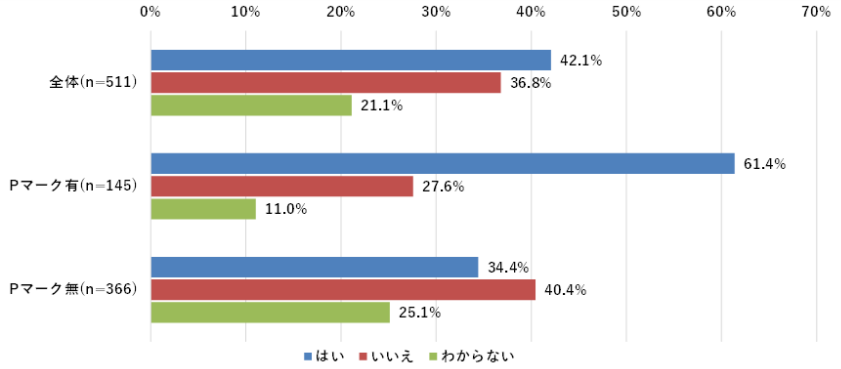


セキュリティ要請に応じた割合に関してはPマークを取得している企業の方が約1.5倍高かった。（取得有無で約1.5倍）



■セキュリティ要請応じたことが取引につながったか

セキュリティ要請に応じたことが取引につながったと回答した企業がPマークを取得している企業の方が約2.5倍高かった（取得有無で約2.5倍）



4. 考察

中小企業等における規模・業種等に応じた効果の高いサイバーセキュリティ対策について（7/8）

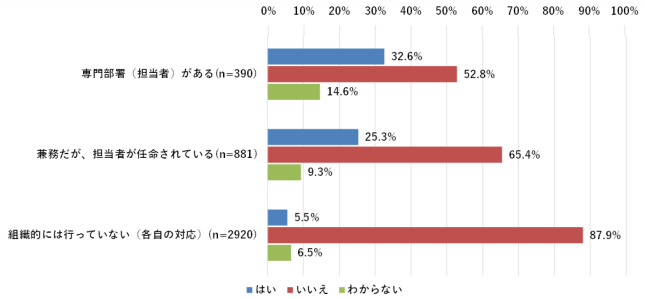
③体制として「専門部署（担当者）」または「兼務だが、担当者が任命されている」ことによる効果

分析結果

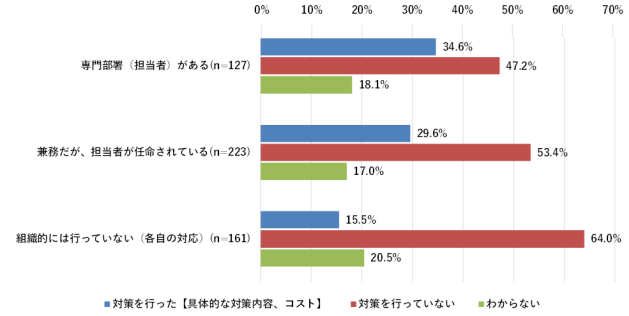
Q22の回答が「1. 専門部署（担当者）がある」と「2. 兼務だが、担当者が任命されている」である企業について分析を行った結果、セキュリティ体制が整備されている企業の方が、取引先からのセキュリティ要請への対応状況や、それを取引上のメリットとして認識する度合いと、一貫した関連性があることが分かった。

■セキュリティ体制整備と取引におけるセキュリティ要請

セキュリティ要請を受けた割合に関してはセキュリティ体制を行っている企業の方が約5～6倍高かった。（整備有無で約5～6倍）

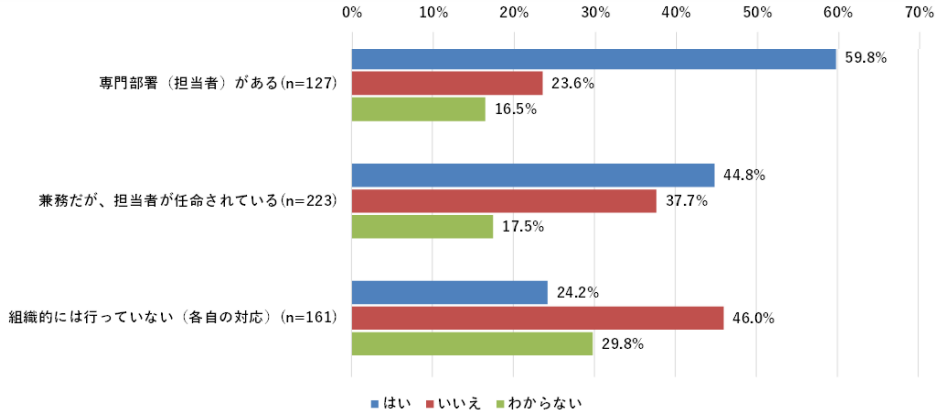


セキュリティ要請に応じた割合に関してはセキュリティ体制を行っている企業の方が約2倍高かった。（整備有無で約2倍）



■セキュリティ要請応じたことが取引につながったか

セキュリティ要請に応じたことが取引につながったと回答した企業の割合はセキュリティ体制を行っている企業の方が約2倍高かった（整備有無で約2倍）



4. 考察

中小企業等における規模・業種等に応じた効果の高いサイバーセキュリティ対策について（8/8）

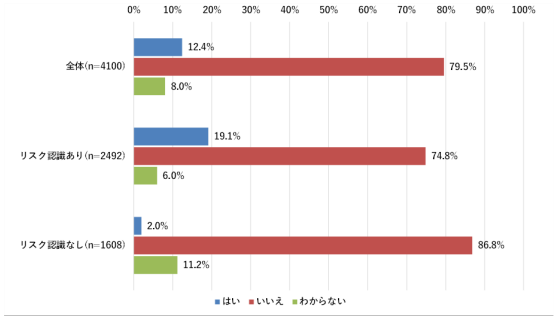
④他社との取引において、自社の主要な事業に影響を及ぼすリスクを認識していることによる効果

分析結果

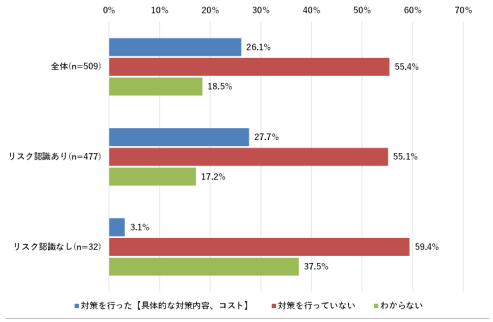
Q41の回答が「機密性の高い情報の漏洩」、「可用性が重視されているサービスの停止」、「供給している製品の途絶」である企業では、それらのリスク認識をしている企業は取引先からのセキュリティ要請への対応状況や、それを取引上のメリットとして認識する度合いと、一貫した関連性があることが分かった。

■セキュリティ体制整備と取引におけるセキュリティ要請

セキュリティ要請を受けた割合に関しては取引におけるリスク認識のある企業の方が約9倍高かった。

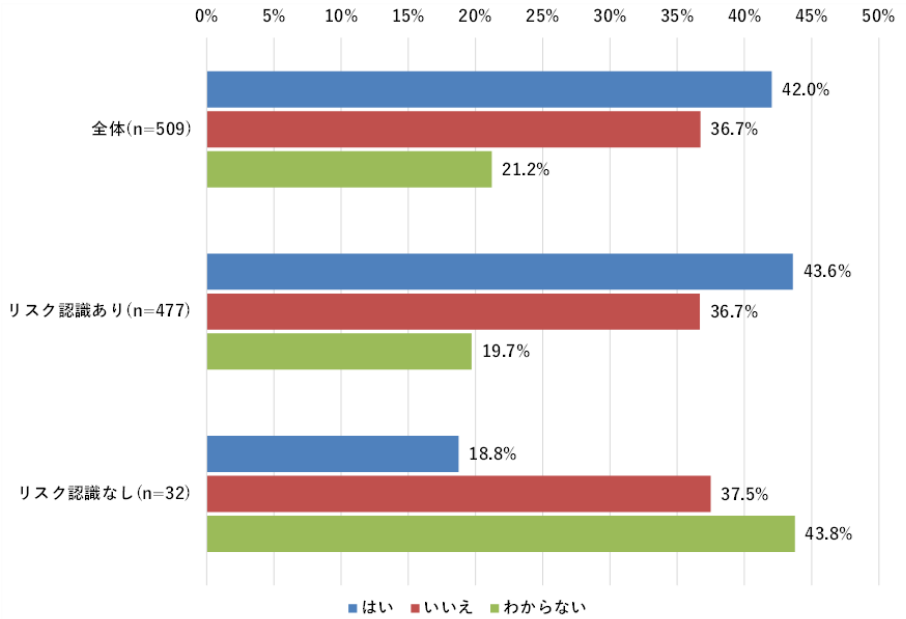


セキュリティ要請に応じた割合に関しては取引におけるリスク認識のある企業の方が約9倍高かった。



■セキュリティ要請応じたことが取引につながったか

セキュリティ要請に応じたことが取引につながったと回答した企業の割合は取引におけるリスク認識のある企業の方が約2倍高かった。



4. 考察
SECURITY ACTION一つ星及び二つ星に求められる基準について（1/3）

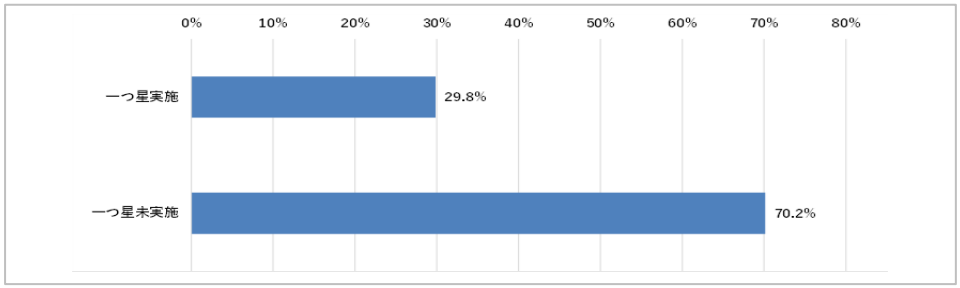
SECURITY ACTION 一つ星

分析

アンケート調査結果からSECURITY ACTION一つ星の診断項目に該当する設問（Q80の5項目）の回答結果を集計し、中小企業におけるの一つ星に求められるサイバーセキュリティ対策の実施度合いを分析する。その結果から中小企業が一つ星を宣言するにあたっての課題や、必要となる支援策の検討を行う。

一つ星

一つ星のサイバーセキュリティ対策項目を実施している企業は、
アンケート回答企業のうち 約30%



・一つ星実施 … 5つの診断項目の全てで「1．実施している」か「2．一部実施している」を回答した企業
・一つ星未実施 … 5つの診断項目の何れかで「3．実施していない」か「4．分からない」を回答した企業

実施状況

一つ星未実施の企業において実施割合が低い項目は、
アクセス制限 と 攻撃手口の周知

SECURITY ACTION 一つ星の診断項目	実施割合
項目1． パソコンやスマホなど情報機器のOSやソフトウェアは常に最新の状態にしていますか？	61.5%
項目2． パソコンやスマホなどにはウイルス対策ソフトを導入し、ウイルス定義ファイルは最新の状態にしていますか？	59.2%
項目3． パスワードは破られにくい「長く」「複雑な」パスワードを設定していますか？	44.2%
項目4． 重要情報に対する適切なアクセス制限を行っていますか？	26.9%
項目5． 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はできていますか？	11.5%

考察

- SECURITY ACTION 一つ星の対策が「未実施」である企業で実施割合が低い項目は、重要情報へのアクセス制限の実施、および攻撃の手口と対策の社内共有する仕組みであった。
- 中小企業は自社の管理責任が伴うような重要情報を特定し、重要情報の管理体制を構築することが望ましい。また、IPAや内閣サイバーセキュリティセンター（NISC）といった公的機関の情報を参照することや、知り合いやコミュニティへの参加で情報交換を積極的に行うことが望ましい。

4. 考察
SECURITY ACTION一つ星及び二つ星に求められる基準について（2/3）

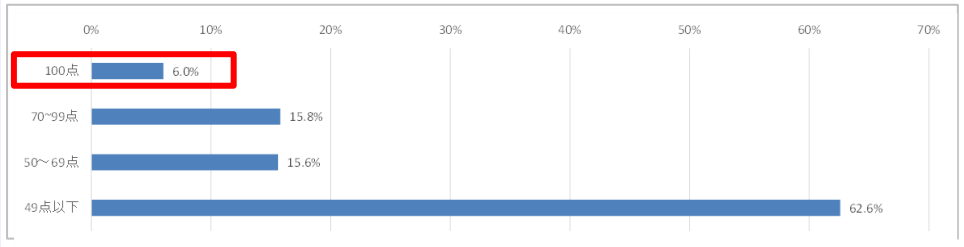
SECURITY ACTION 二つ星

分析

SECURITY ACTION二つ星宣言に必要な診断項目の実施状況を調査し、実施率が低い診断項目や、逆に実施率が高い診断項目を明らかにした。実施率が低い診断項目については、それらの実施の促進策などを検討した。

二つ星

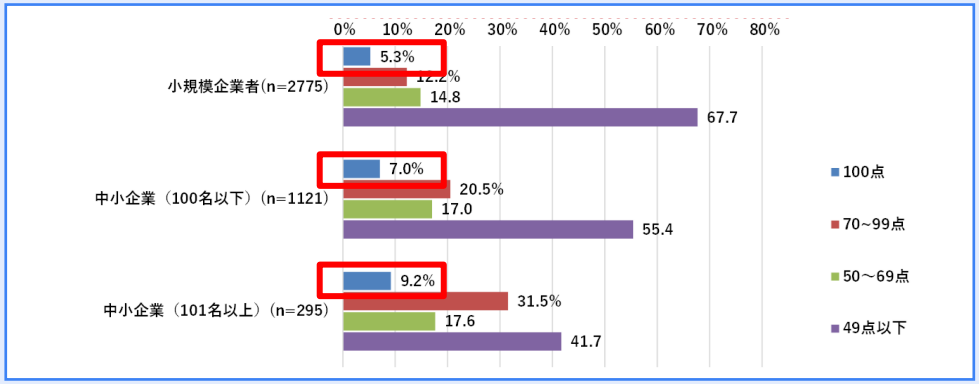
二つ星の診断項目を全て実施している企業は、
アンケート回答企業のうち 6.0%



※ 得点は、SECURITY ACTION二つ星宣言に必要な診断項目に該当するアンケート設問(Q80の25項目)の回答結果をIPAが提供する「5分でできる！情報セキュリティ対策自社診断」の基準に沿って得点化して算出した“自社診断の合計点”である。

実施状況

企業規模別では、二つ星の診断項目を全て実施しているのは、
小規模企業者で5.3%、中小企業(101名以上)で9.2%



考察

- 69点以下の企業群において、実施率が高い対策項目としては、サイバーセキュリティ対策として広く周知されているものや、PCやソフトウェアに標準機能として組み込まれているため利用者が受動的に対策実施のタイミングを知ることができる機能を持つものなどの特徴が見られた。
- 同様に69点以下の企業群において、実施率が低い診断項目として、特にサイバー攻撃に関する情報の周知、インシデント対応計画の策定、サイバーセキュリティ対策のルール化と周知があり、中小企業ではこれらの実施に課題があることが分かった。中小企業はIPAやNISCといった公的機関の情報を参照することや、知り合いやコミュニティへの参加で情報交換を積極的に行うことが望ましい。

4. 考察
SECURITY ACTION一つ星及び二つ星に求められる基準について（3/3）

SECURITY ACTION 二つ星

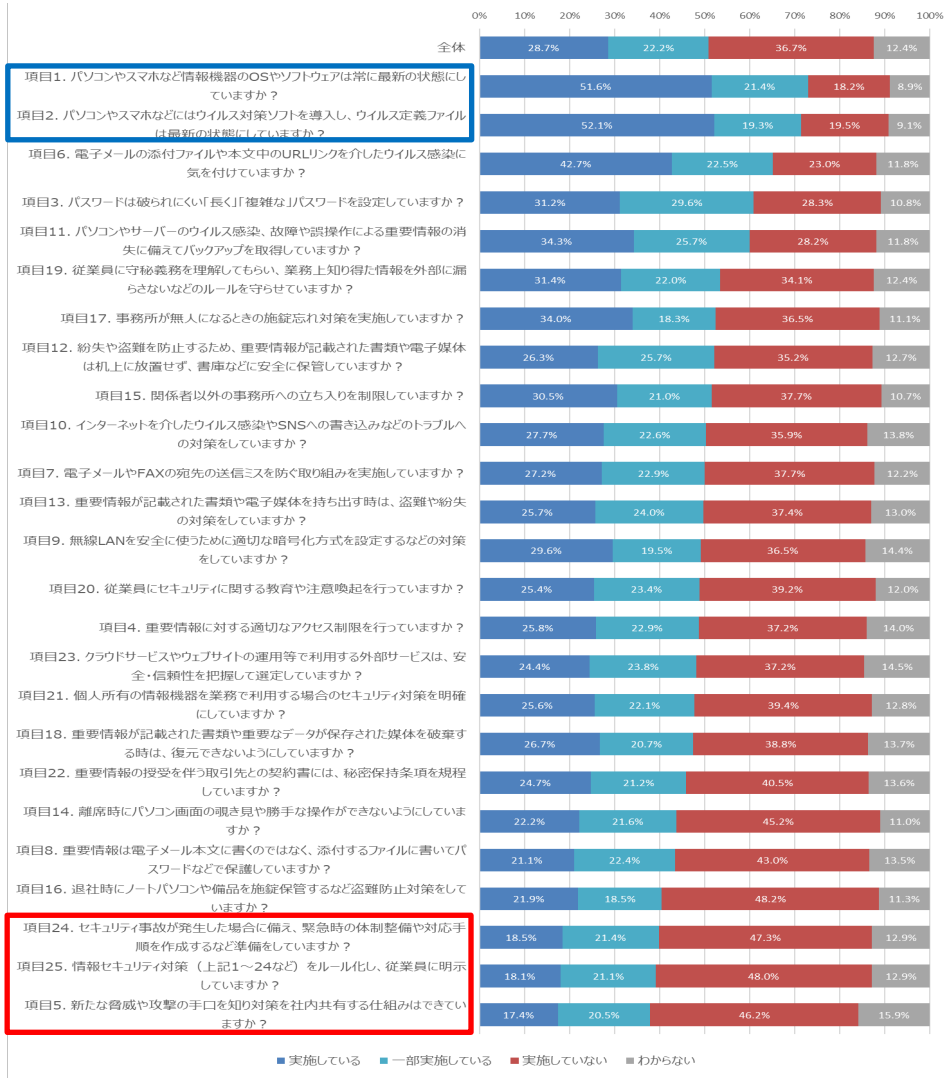
実施状況

企業規模に関わらず、実施割合の高い診断項目は、
ソフト更新、ウイルス対策、ウイルスメール対策

“自社診断の合計点”が69点以下の企業において実施割合が低い項目は、
攻撃手口の周知、インシデント対応体制、ルール化

「自社診断」の実施状況は、「実施している」及び「一部実施している」を合わせた割合は「パソコンやスマホなど情報機器のOSやソフトウェアは常に最新の状態にしていますか？」（73.0%）が最も高く、次いで「パソコンやスマホなどにはウイルス対策ソフトを導入し、ウイルス定義ファイルは最新の状態にしていますか？」（71.4%）であり、基本的なセキュリティ対策はある程度定着していることがうかがえる。

一方、低かったのは「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はできていますか？」（37.9%）、次いで「情報セキュリティ対策（上記1～24など）をルール化し、従業員に明示していますか？」（39.2%）、「セキュリティ事故が発生した場合に備え、緊急時の体制整備や対応手順を作成するなど準備をしていますか？」（39.8%）であり、組織的に取り組む必要のあるセキュリティ対策が進んでいないことがうかがえる。



4. 考察

SECURITY ACTION宣言及びサイバーセキュリティお助け隊サービスを導入する中小企業が、中小企業全体の割合に対して低い水準となっている理由

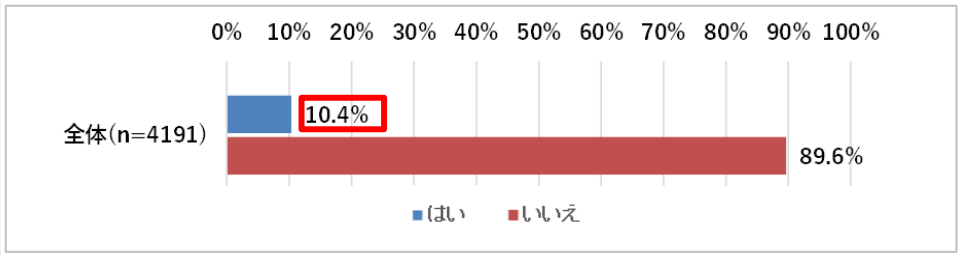
SECURITY ACTION 宣言

分析

SECURITY ACTIONの宣言状況および認知度を明らかにし、また宣言したきっかけや、宣言によるメリットに関する認識、宣言しない理由などについて調査結果を分析し、普及が進んでいない理由と対応策を検討する。

認知状況

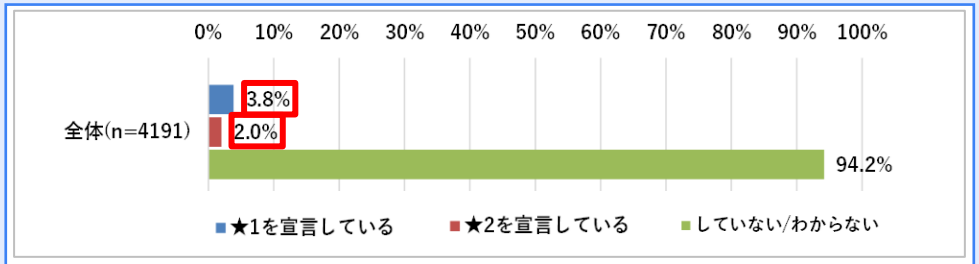
アンケート回答企業のうち **約10%**



SECURITY ACTION宣言の認知度は約10%となった。企業規模別では、企業規模が大きくなるほど認知度が上がっていることが明らかになった。また、企業規模が大きくなるほど認知度が上がっていることが明らかになった。

宣言状況

一つ星は **3.8%** / 二つ星は **2.0%**



企業規模が大きくなるほど宣言割合が上がっていることが明らかになった。中小企業（101名以上）では一つ星の宣言割合が10.8%であるが、一方で小規模企業者では1.4%であり、小規模企業者ではほとんど一つ星であってもほとんど普及していない。

考察

- 中小企業におけるSECURITY ACTIONの認知度が低いことが大きな課題であることが分かった。また、認知度以外の課題としては小規模企業者ではSECURITY ACTIONの必要性を感じない企業が多く、小規模企業者以外の中小企業ではセキュリティ人材の不足や費用対効果の不明瞭が挙げられている。
- 経営層（経営者、役員）の認知度が低いことが分かり、認知度向上のためには経営層へのアプローチが有効であると考えられる。また、中小企業がSECURITY ACTIONの宣言を行う際、経営層が最終的な決断を行うことから、経営層の認知度向上が、SECURITY ACTIONの普及促進の観点からも有効だと考えられる。

4. 考察

SECURITY ACTION宣言及びサイバーセキュリティお助け隊サービスを導入する中小企業が、中小企業全体の割合に対して低い水準となっている理由

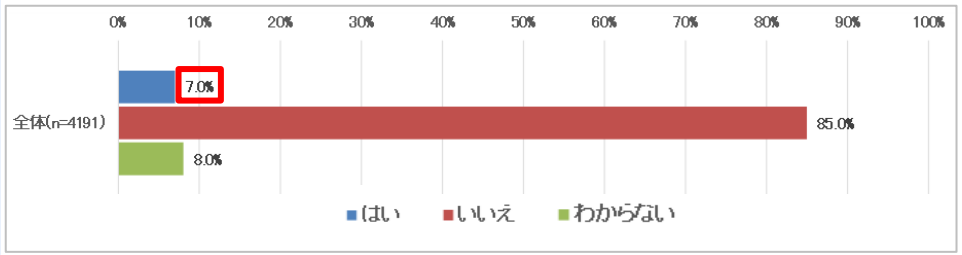
サイバーセキュリティお助け隊サービス

分析

サイバーセキュリティお助け隊サービスの導入状況および認知度を明らかにし、また導入のきっかけや導入によるメリットに関する認識、導入しない理由などについてアンケート調査およびインタビュー調査から得られた結果を分析し、導入割合が低い理由と対応策を検討する。

認知状況

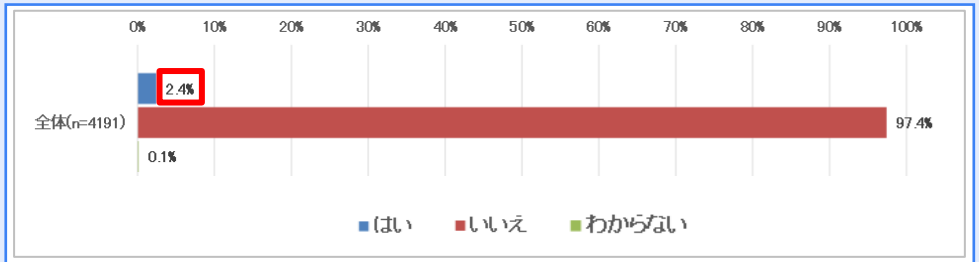
アンケート回答企業のうち **約７％**



サイバーセキュリティお助け隊サービスの認知度はアンケート回答企業のうち約7%に留まり、さらにサービスを導入している企業の割合はわずか約2%であった。企業規模が大きくなるほど認知度が上がっていることが明らかになった。

導入状況

アンケート回答企業のうち **約2%**



企業規模別にみると、企業規模が大きくなるほど導入割合が上がっていることが明らかになった。中小企業（101名以上）では導入割合が8.8%であるが、一方で小規模企業者では1%未満であり、小規模企業者にはほとんど普及していない。

考察

- 本サービスを導入している企業が非常に限られていることが改めて明らかになり、この要因として中小企業の認知度の低さが大きな課題であることが分かった。一方で、導入している企業からは本サービスの特徴となるワンパッケージでの導入の容易性、低コストなどのメリットを感じていることも明らかになっており、導入をしない理由として挙がっている「リソース不足」や「費用対効果が不明確」といった点を考慮すると、サービス内容および導入によって得られる効果が中小企業に理解されていない点も大きな課題であると考えられる。
- 経営層（経営者、役員）の認知度が低いことが明らかになっており、経営層へのアプローチがサイバーセキュリティお助け隊サービス隊の普及促進の観点からも有効であると考えられる。

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報告書
（概要説明資料）
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

https://www.ipa.go.jp/