2018 年度 SECURITY ACTION 宣言事業者における
情報セキュリティ対策の実態調査

－ 調査報告書 －

2019年3月28日

独立行政法人情報処理推進機構
Information-technology Promotion Agency, Japan

目　次

1. はじめに 2

2. 事業概要 3

3. SECURITY ACTION 制度の取組みに関するアンケート調査 4

3.1. アンケート調査概要 4

3.2. アンケート調査結果及び分析 6

3.2.1. 単純集計結果 6

3.2.2. クロス集計結果 22

4. SECURITY ACTION 制度の取組みに関する訪問調査 55

4.1. 訪問調査概要 55

4.2. 訪問調査結果及び分析 56

4.2.1. 訪問事業者の属性 56

4.2.2. 訪問調査結果 57

4.3. 訪問調査結果の分析 66

4.3.1. 他事業者への適用可能性 66

4.3.2. 二つ星宣言へのステップアップに向けた課題 67

4.4. 取組み事例について 68

5. 調査結果に基づく分析 70

5.1. 中小企業等における情報セキュリティ対策の課題等 70

5.1.1. 中小企業等における情報セキュリティ対策の課題 70

5.1.2. SECURITY ACTION 制度に対する今後の期待 70

5.2. 普及に向けた方策 71

5.2.1. 一つ星宣言を促すための方策 71

5.2.2. 二つ星宣言へのステップアップを促すための方策 71

5.2.3. 継続的な情報セキュリティ対策を促すための方策 72

6. まとめ 73

1. はじめに

第四次産業革命と呼ばれる大きな社会変化を迎える中、中小企業[1]についても急激に変化する社会に対応するために IT の利活用による新たな商品・サービスの開発、業務の高度化・効率化等が今後重要となる。一方、標的型攻撃などのサイバー攻撃の対象は政府機関や大企業だけでなく、中小企業の場合は取引先を標的とした攻撃の踏み台にされるケースも増加している。このような社会に深刻な影響を及ぼす可能性のあるセキュリティ脅威について、中小企業も意識を高め自発的な対策を実施していくことが必要である。

そうした昨今の状況を踏まえ、独立行政法人情報処理推進機構(以下「IPA」という。)は、2017 年 4 月から中小企業自らが情報セキュリティ対策に取組むことを自己宣言する制度である『SECURITY ACTION』の運用を開始し、多くの中小企業が情報セキュリティ対策への取組みを推進している。

一方で、IPA が実施した「2016 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 」によれば、中小企業における情報セキュリティ対策の主な課題として、「費用対効果が見えない」、「どこからどう始めたらよいかわからない」といった意見が多数挙げられている。

このような状況の下、本事業では SECURITY ACTION 自己宣言事業者における情報セキュリティ対策の実態調査を実施することで、他の SECURITY ACTION 自己宣言事業者をはじめとする中小企業にとって参考となる取組み事例を抽出し、SECURITY ACTION 制度に取組むきっかけや効果、実施手順等を取り纏める。

本事業の調査結果の提供を通じて、上記の課題解決を図るとともに、情報セキュリティ対策の取組みへのモチベーションを高め、SECURITY ACTION 自己宣言事業者をはじめとする中小企業の自律的かつ継続的な情報セキュリティ対策を促進することを目的とする。

[1] 本調査の対象である SECURITY ACTION 宣言事業者は、中小企業が大部分を占めるが、一部企業以外の法人、個人事業主が含まれる。

2. 事業概要

本事業では、SECURITY ACTION 自己宣言事業者における情報セキュリティ対策の実施状況や課題、経営層の認識等を把握するため、自己宣言事業者を対象としたアンケート調査を実施した。また、アンケート調査結果に基づく訪問によるヒアリング調査（以下「訪問調査」）を実施し、SECURITY ACTION 制度に取組むことで得られる成果やメリット、対策の工夫点等について収集した情報をもとに事例集として取り纏めた。

以下に事業概要と事業概要図を示す。

表 2-1　事業概要

項目	内容
調査目的	SECURITY ACTION 自己宣言事業者の情報セキュリティ対策の取組み状況等を調査することで実態を把握し、参考となる取組み事例を抽出することで、SECURITY ACTION 制度に取組むことで得られる成果やメリット、対策の工夫点等を示す。
調査対象	SECURITY ACTION 自己宣言事業者
実施期間	2018 年 10 月～2019 年 2 月
調査方法	アンケート調査と訪問によるヒアリング調査

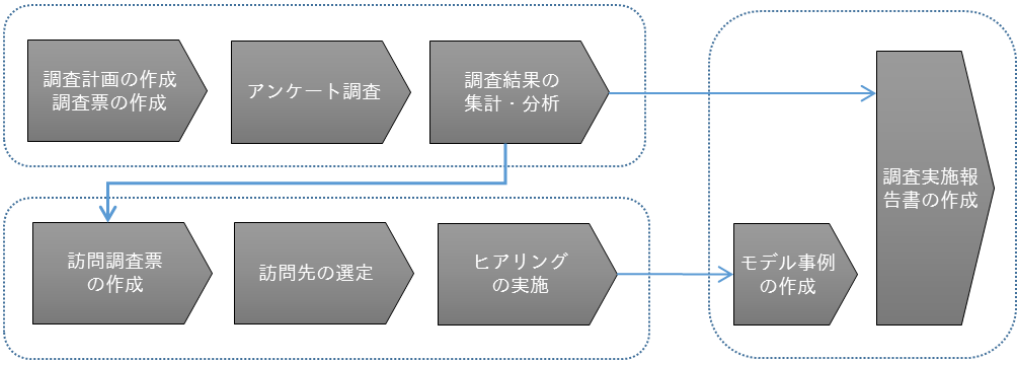

図 2-1　事業概要図

3. SECURITY ACTION 制度の取組みに関するアンケート調査

SECURITY ACTION 自己宣言事業者における情報セキュリティ対策の実施状況や課題、経営層の認識等を把握するため、アンケート調査を実施した。アンケート調査概要を 3.1 に、アンケート調査結果及び分析を 3.2 に報告する。

3.1. アンケート調査概要

アンケート調査は、2018 年 11 月から 2018 年 12 月まで実施し、回答数は、5,162 件であった。実施概要を表 3-1 に示す。

表 3-1 アンケート調査の実施概要

項目	内容
実施対象	SECURITY ACTION 自己宣言事業者
実施期間	2018 年 11 月下旬～2018 年 12 月下旬
実施方法	電子メールによるアンケート回答依頼 ウェブアンケートシステムによる回収
回答数	5,162 件

アンケート回答者及び事業者の属性については、回答事業者の IT 依存度や、SECURITY ACTION 自己宣言を主導的に進めた役割等も含み 7 点で確認した（下表 Q1～Q7）。SECURITY ACTION 自己宣言に関しては、回答者が宣言をしたきっかけやどのような効果を期待しているかを含み（下表 Q8、Q9）、これまでに発生した事故や今後、発生することを懸念している事故など（下表 Q11-1、Q11-2）を確認した。さらに、情報セキュリティ対策に関する取組みの内容や課題などを確認した（下表 Q12～Q16）。具体的な設問を表 3-2 に示す。

なお、以下に示す調査結果は、2018 年 12 月 21 日までに回答されたものに基づいている。

表 3-2　アンケート調査項目の内容[2]

回答方法	質問番号	質問
SA	Q1	貴社の主たる事業の業種について、次の中から最も近いものを 1 つ選んでください。
SA	Q2	貴社の総従業員数として、あてはまるものを 1 つ選んでください（正社員以外の雇用形態の社員を含み、派遣社員、他社に所属する常駐社員を除いてください）。
SA	Q3	貴社が直近で宣言した SECURITY ACTION の取組み目標の種類として、次のいずれか 1 つを選択してください。
SA	Q4	本アンケートにご回答いただく方の社内での立場についてお尋ねします。ご回答いただく方の社内での立場として、次の中からもっとも近いものを 1 つ選択してください。
MA	Q5	次の中で、貴社で利用している IT 製品やサービスをすべて選択してください。なお、自社で製品を購入せず、クラウドで提供されているサービスを利用する場合も含みます。
SA	Q6	貴社の事業はどの程度 IT に依存していますか。たとえばインターネットへの接続が止まったり、社内の PC などが使えなくなったりしたら、貴社の事業はどのようになるでしょうか。次の中から最も近いものを 1 つ選択してください。
SA	Q7	貴社が SECURITY ACTION に関する宣言を行うにあたって、社内で主導的に進めていったのはどのような役割の方ですか。次の中から最も近いものを 1 つ選択してください。
MA	Q8	貴社が SECURITY ACTION 自己宣言を行おうとしたきっかけはどのようなものですか。次の中からあてはまるものをすべて選択してください。
MA	Q9	貴社では SECURITY ACTION 自己宣言をしたことで、どのような効果を期待していますか。次の中からあてはまるものをすべて選択してください。
FA	Q10	情報セキュリティ対策を実施したことで貴社にとって効果があった事例がございましたら、下欄に記入して下さい
MA	Q11	貴社ではこれまで（過去 10 年程度）次のような事故が発生したことがありましたか。また今後次のような事故が発生することを懸念していますか。あてはまるものすべてを選択してください。
SA	Q12	次に示すセキュリティ対策について、貴社における取組み状況に最も近いものを一つずつ選択してください。
MA	Q13	貴社において情報セキュリティ対策を進める上での課題点として、次の中からあてはまるものをすべて選択してください。
SA	Q14	今後、経営層による情報セキュリティ対策に関する意識を高めていくためには、どのようなことが必要と思われますか。最も有効と思われるものを 1 つ選択してください。
MA	Q15	IPA では中小企業における情報セキュリティ対策の普及に向けて、次のような取組みを行っています。貴社において関心のある取組みについて、あてはまるものをすべて選択してください。
MA	Q16	貴社として、今後注力していきたい情報セキュリティ関連の取組みとして、次の中からあてはまるものすべてを選択してください。

SA:単一回答、MA:複数回答可、FA：フリー回答（自由記入）

[2] アンケート調査対象には、一部企業以外の法人、個人事業主が含まれるが、調査項目では、中小企業、貴社と記している。

3.2.　アンケート調査結果及び分析

アンケート調査結果として単純集計結果を 3.2.1 に、分析結果として各種のクロス集計結果を 3.2.2 に報告する。

なお、グラフ上の数値について単純集計は小数点第 1 位まで表示し、クロス集計[3]は小数点以下を視認性を考慮し記載を省略している。また、各グラフの構成比は小数点以下を四捨五入しているため、合計しても必ずしも 100%とはならない場合がある。

3.2.1.　単純集計結果

(1) 回答事業者の業種

業種は、「製造業（印刷業を含む）」が 17.8%と最も高く、次いで「建設業」が 16.9%、「卸売業・小売業」が 13.3%となっている。

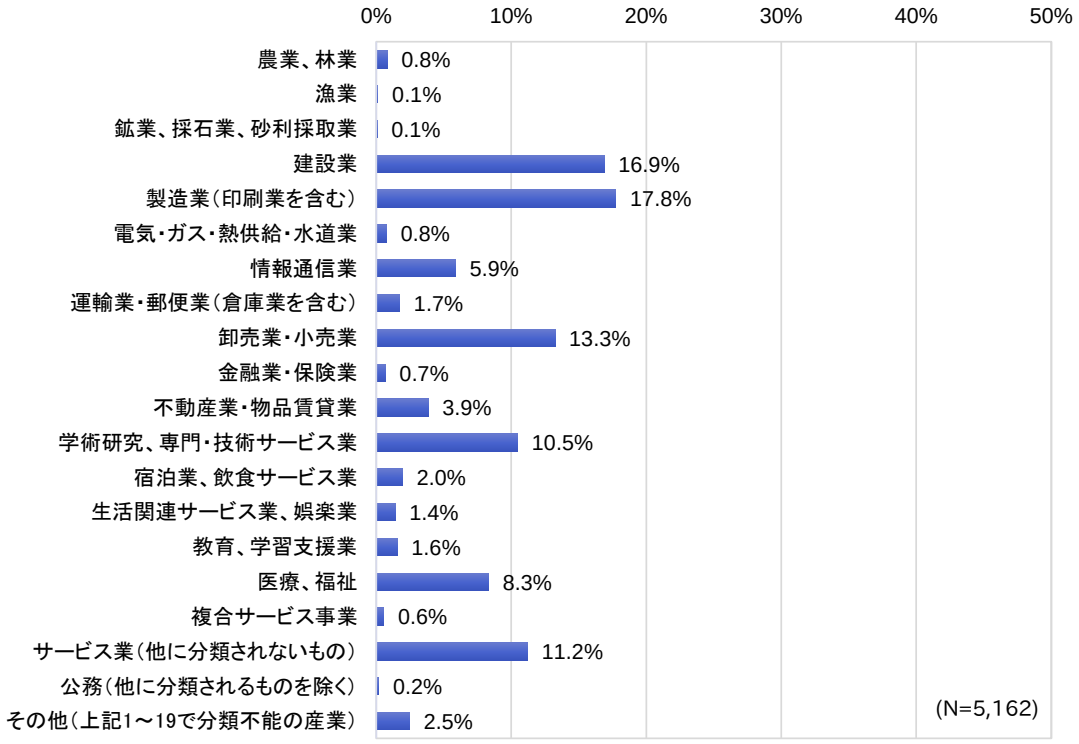

図 3-1　主たる事業の業種（Q1）

[3] 一部のクロス集計表は小数点第 1 位まで表示

(2) 回答事業者の従業員規模

従業員規模は、「1～5 名」が 30.6%と最も高く、次に「6～20 名」が 28.1%となっており、「1～20 名」が半数以上を占めている。

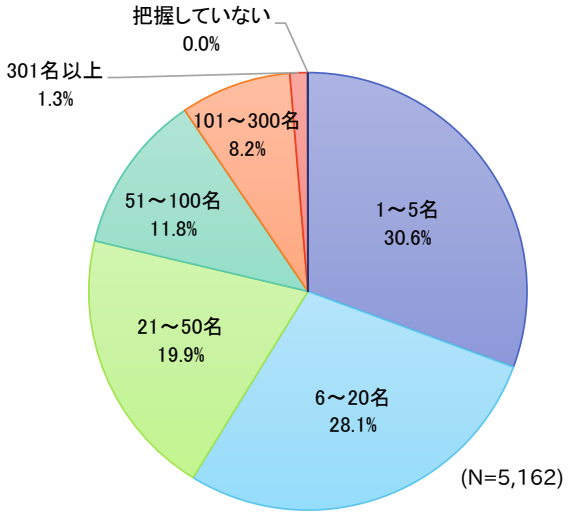

図 3-2 総従業員数（Q2）

(3) SECURITY ACTION の取組み目標

直近で宣言[4]した SECURITY ACTION の取組み目標は、「一つ星」が 80%以上となっている。

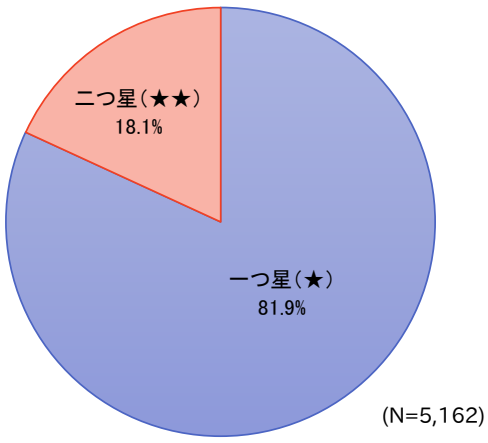

図 3-3 直近で宣言した SECURITY ACTION の取組み目標（Q3）

[4] アンケートでは、“最も最近”に行った SECURITY ACTION の自己宣言を尋ねている。SECURITY ACTION の自己宣言は、取組み目標に応じて「★一つ星」と「★★二つ星」のロゴマークがある。

(4) 回答者の社内での立場

本アンケートの回答者は、「経営者層」が 50%以上となっている。

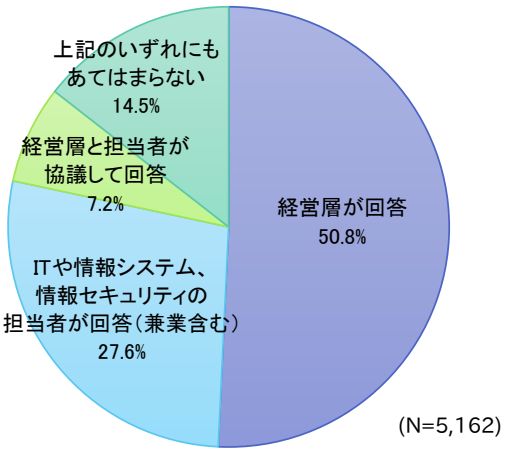

図 3-4　本アンケートの回答者役職（Q4）

(5) 利用している IT 製品やサービス

利用している IT 製品やサービスは、「オフィス文書作成ソフト」と「電子メールとスケジュール管理」が 90%以上となっている。また、会計ソフトは 75.5%となっている。

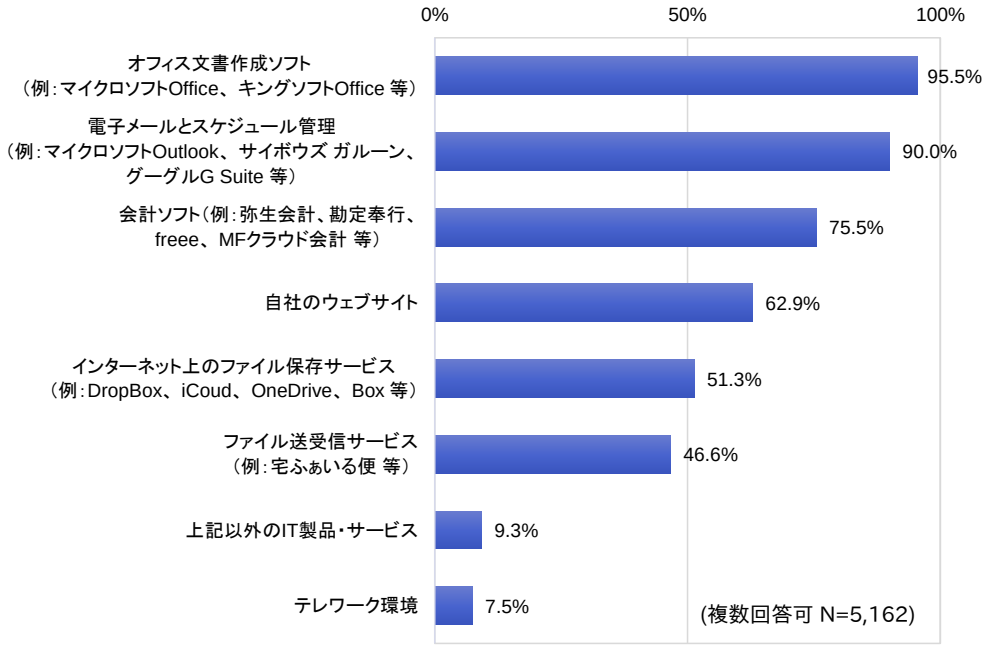

図 3-5　利用している IT 製品やサービス（Q5）

また、「上記以外の IT 製品・サービス」で回答のあったフリー回答（自由記入）は、下記のとおりである。

- CAD（Computer Aided Design：コンピュータによる設計支援ツール）
- CAM（Computer Aided Manufacturing : CAD で作成されたデータを入力データとして生産準備全般をコンピュータ上で行うためのツール）
- CAE（Computer Aided Engineering : コンピュータを使って製品の設計、製造や工程設計の事前検討の支援を行うためのツール）
- HP 作成ソフト・サービスなど
- POS 管理（Point of Sale：販売時点情報管理
- VPN（Virtual Private Network：インターネット上のプライベートネットワーク）
- セキュリティソフト
- 資産管理ソフト
- デザイン・編集ソフト
- ホテル管理システム
- 医療事務用システム
- 加工管理システム
- 勤怠管理システム
- 在庫管理システム
- 自社開発基幹システム
- 人事管理ソフト
- 生産管理システム
- 税務申告ソフト
- 電子カルテ
- 自社開発ソフト
- 保育業務システム
- 名刺管理ソフト
- チャットツール
- ERP（Enterprise Resource Planning：経営資源統合管理システム）
- HPC（high-performance computing：高性能計算システム）

(6) 回答事業者の IT 依存度

回答者の自社事業の IT 依存度は、「できる作業もありそうだが、実質的に事業は実施できない」が 41.9%と最も高く、次いで「通常の半分くらい程度しかできなくなりそう」が 26.9%となっている。また、「自社のあらゆる事業が完全に止まってしまう」が 12.0%である。

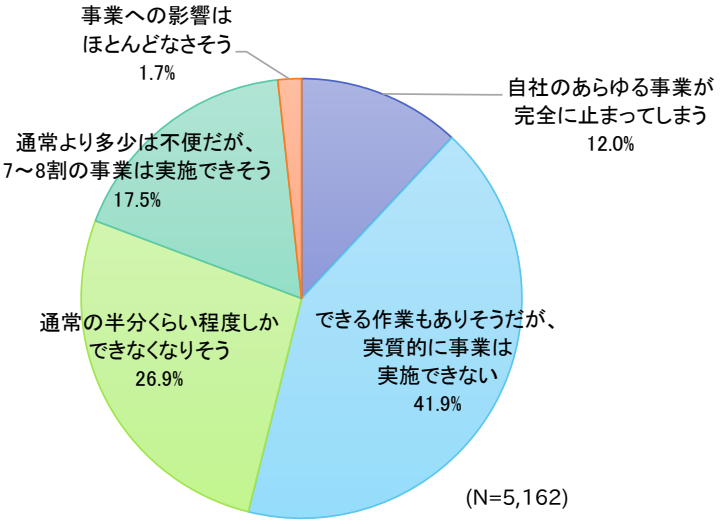

図 3-6 自社の事業がどの程度 IT に依存しているか（Q6）

(7) SECURITY ACTION 自己宣言の主導者（役割）

SECURITY ACTION に関する宣言を行うにあたり、社内で主導的に進めていった役割の方は、「経営者」が 53.3%と半数以上を占める。次いで、「総務担当者」が 16.9%、「IT や情報システムの担当者」が 16.4%である。

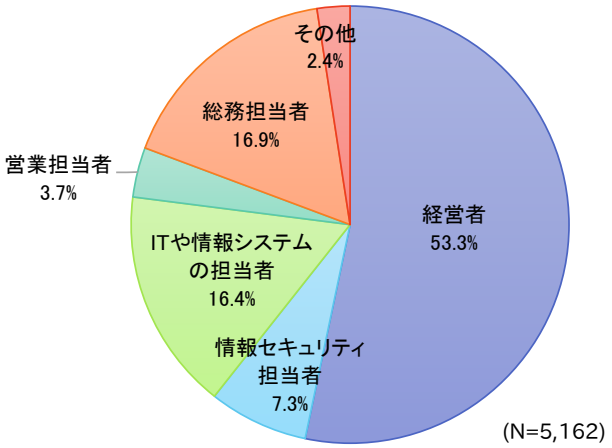

図 3-7 SECURITY ACTION に関する宣言の社内における主導者（Q7）

(8) SECURITY ACTION 宣言を行おうとしたきっかけ

SECURITY ACTION 宣言を行おうとしたきっかけは、「補助金を申請する際の要件となっていた」が 77.0%と最も高く、次いで「取引先からの信頼を高める手段として有用と考えた」が 29.8%、「事業拡大や顧客開拓に有用と考えた」が 20.5%となっている。

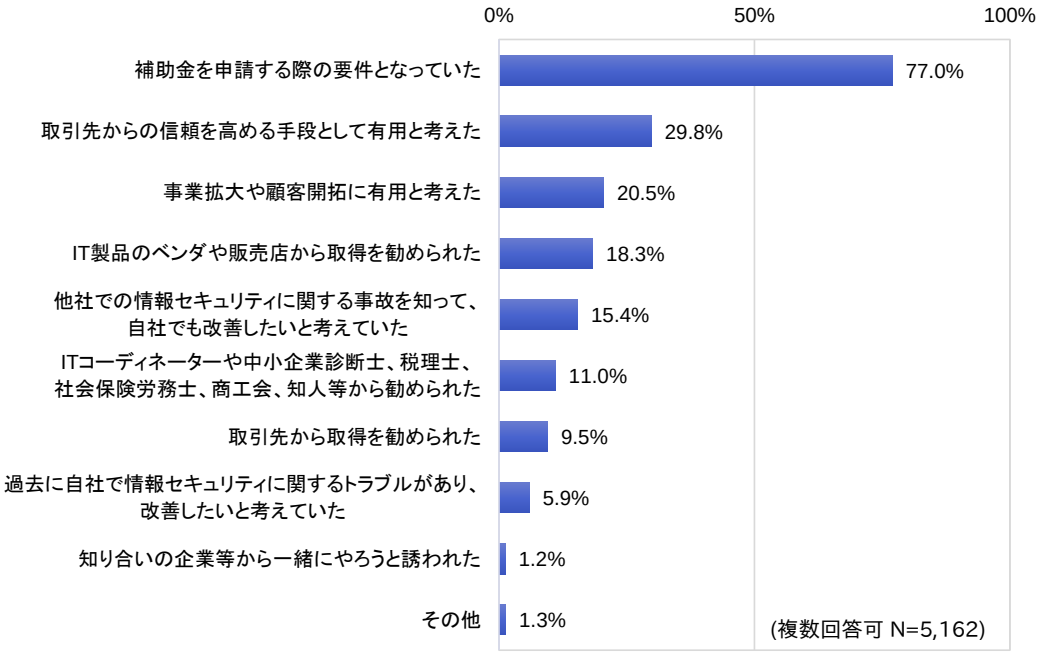

図 3-8 SECURITY ACTION 宣言を行ったきっかけ（Q8）

また、その他のフリー回答（自由記入）は、下記のとおりである。セキュリティ対策の必要性、事業に係る自主的な取組み、他機関等からの推奨・紹介などが、SECURITY ACTION 宣言を行うきっかけとなっている。

■ セキュリティ対策の必要性

- セキュリティ対策の必要性
- 社員の退職などの際、顧客情報などの漏えいを防ぐため
- グループ企業の方針として
- 経営陣でもある IT 担当兼セキュリティ担当が実施を決めた
- 自社の業務管理等を明確・迅速にしようと考えた
- 社内の情報セキュリティ意識を高めるため
- 取組み状況の客観評価のため
- プライバシーマークの取り止めに際して、有効な手段と判断したため
- 入札要件に入っていたから

■ 事業に係る自主的取組み

- IT 企業のため
- セキュリティ関連の事業をしているため
- IT 導入支援事業者（勧めるもの）として
- 顧客への信頼を高めるため。IT エンジニアとしての役目と考えるため

■ 他機関等からの推奨・紹介など

- IPA からの紹介、IPA の Web サイト
- 日本商工会議所からの勧め
- 取引先が取得したから
- 上部団体からの勧め
- 参加したセミナーでの紹介
- 情報セキュリティセミナーでの紹介

(9) SECURITY ACTION 宣言によって期待される効果

SECURITY ACTION 宣言によって期待される効果は、「取引先からの信頼が高まる」が 46.0%と最も高く、「従業員による情報管理や情報セキュリティに関する意識を高める」も 42.5%となっている。次いで、「経営層の情報セキュリティ対策に関する意識を高める」、「SECURITY ACTION 宣言企業を対象とする今後の支援制度に期待する」、「従業員による IT 関連のトラブルを減らす」の順となっている。

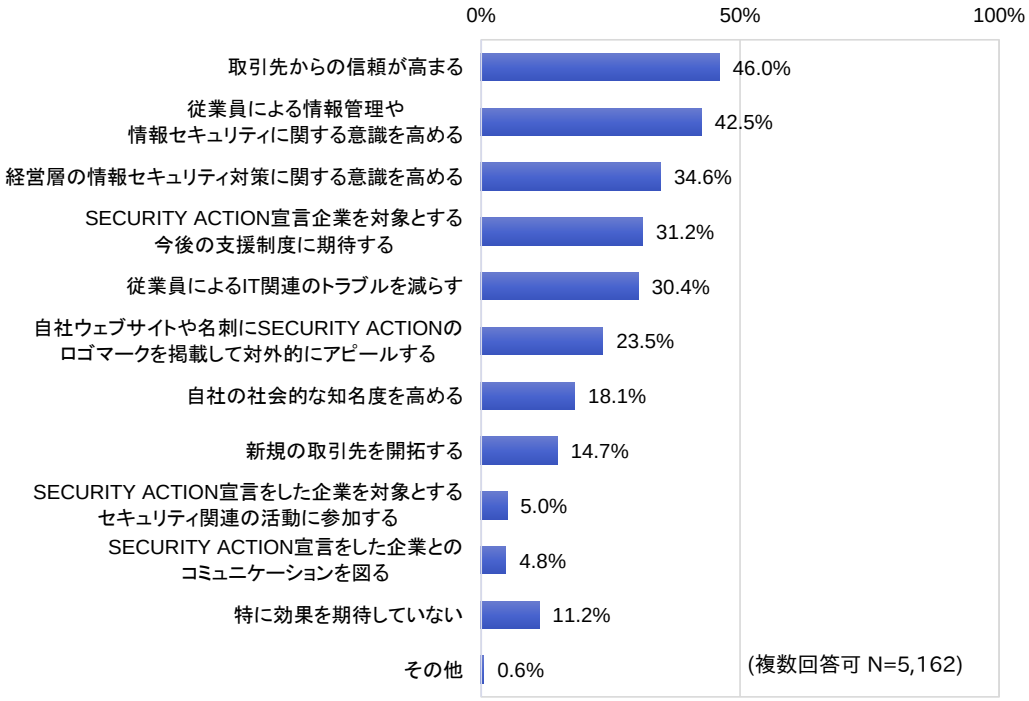

図 3-9　SECURITY ACTION 宣言によって期待される効果（Q9）

また、フリー回答（自由記入）は、下記のとおりである。信頼性・意識向上・対外認知、情報セキュリティ対策に関する情報収集の効果への期待がある一方、効果が分からないとする回答もある。

■ 信頼性・意識向上・対外認知
- 取組みをしていると外部から確認できる
- 関係企業の意識向上
- 社会的な信頼が高まる
- 社員（会員）の意識の向上
- 従業員の情報セキュリティへの意識向上

■ 情報セキュリティ対策に関する情報収集
- 情報セキュリティに関する情報収集（具体的問題点、事例、対策、方法など）
- 情報取得の機会
- 研修の案内
- 他社のセキュリティ担当者との情報交換、繋がりづくり

■ 補助等
- IT 導入補助金による助成
- 生産性向上設備の補助金申請
- 補助金交付の対象企業となること

■ 効果が分からない
- 効果がよく分からない
- 具体的には分からない
- 初めてなので、あまり予想がつかない
- 正直なところあまりよく分からない
- どんな効果があるか推移を見守っている
- 今後に期待

(10) 情報セキュリティ対策を実施したことで貴社にとって効果があった事例

フリー回答（自由記入）は下記のとおりである。情報セキュリティ対策に対する意識の向上、情報セキュリティ関連の事故の抑制、情報セキュリティ対策実施による信頼獲得、対外アピール、情報セキュリティルールの明確化・共有等に大別される。

■ 情報セキュリティ対策に対する意識の向上

- 経営者の意識が変わった
- 経営層の情報セキュリティに対する関心が高まった
- 情報管理の意識が高まった
- 情報セキュリティ担当者の意識向上
- 従業員の意識向上
- 社員の情報セキュリティに関するリテラシーが上がった
- 会社が情報セキュリティに力を入れていることが、従業員に伝わった
- 社員の情報取り扱いに対するの意識が高まった
- ルールを見直し、意識を高めることができた
- ウイルスやサイバー攻撃に関する意識が高まった
- パスワードなどの扱いの意識が高まった

■ 情報セキュリティ関連の事故の抑制

- 情報漏えい事故をゼロに抑えられている
- 情報セキュリティ事故が減少した
- 他社からウィルスメールが送信されて来ても、大きなトラブルにならずに済んでいる

■ 情報セキュリティ対策実施による信頼獲得、対外アピール

- 取引先から一層の信頼を得られた
- 顧客の信頼度を高めることができた
- 顧客へ信用度をアピールできた
- 同事業を行っている会社に比べて、顧客からの信頼は上がっている
- 名刺交換の際、信用度が高まった
- 他社から、情報セキュリティ対策をしている事業所と認知された
- 顧客の新規開拓がスムーズになった
- 顧客に勧める際に、まず自社で取組んでいることをアピールしたので、説得力が高まった
- 取引先からの信用が高まった。加えて、お客様から依頼されるセキュリティ監査を免除される場合もあり、効果があった

- プライバシーマーク取得を求められた際に、取得までの代替として SECURITY ACTION★★の価値を認めてもらえた
- 現時点まで特に効果は出ていないが、名刺やホームページにロゴマークと共に意義を記載することで、外部からの認識・評価が高まるものと期待

■ 情報セキュリティルールの明確化・共有

- 曖昧であった IT 関連のルールを明確にし、会社全体でルールの共有ができるようになった
- 情報セキュリティポリシーの策定における議論を通じて従業員のとるべき行動が明文化された
- セキュリティ対策方針について取組むべきことと、その運用方法について、参考にした

■ その他

- 健全な経営判断ができるようになった

(11) 発生した事故または発生を懸念している事故[5]

過去 10 年程度の間に発生した情報セキュリティ関連の事故の種類としては、「従業員の誤送信・誤操作による情報の漏えい・消失」が 44.8%と最も高く、次いで「コンピュータウイルス（マルウェア）感染による情報の漏えい・消失・改ざん」が 32.2%となっている。

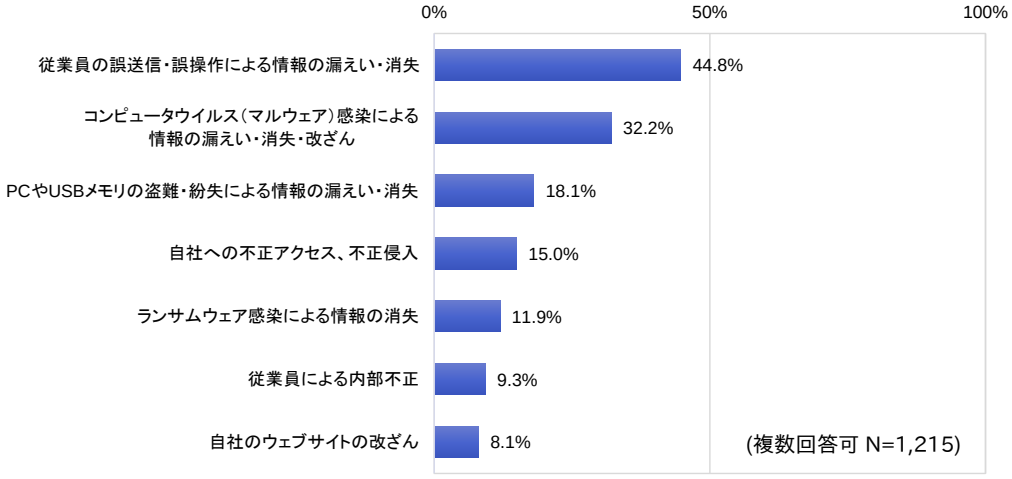

図 3-10　これまで（過去 10 年程度）の間に発生したことがある情報セキュリティ関連事故（Q11）

今後発生することを懸念している情報セキュリティ関連の事故の種類は、「コンピュータウイルス（マルウェア）感染による情報の漏えい・消失・改ざん」が 78.8%と最も高く、「PC や USB メモリの盗難・紛失による情報の漏えい・消失」、「従業員の誤送信・誤操作による情報の漏えい・消失」、「自社への不正アクセス、不正侵入」、「ランサムウェア感染による情報の消失」も 6 割以上になっている。

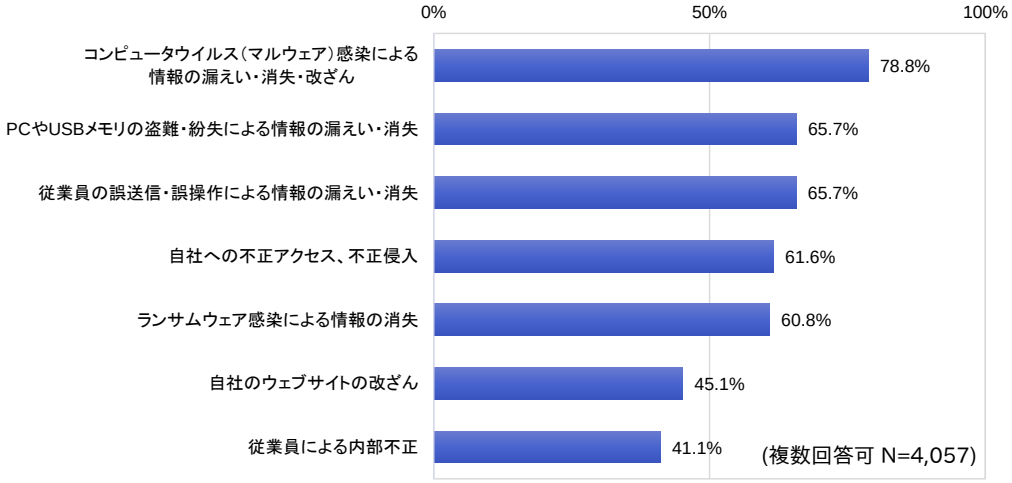

図 3-11　今後の発生を懸念している情報セキュリティ関連事故（Q11）

[5] アンケート回答の「上記のいずれにもあてはまらない」を除いた回答数を 100%とした割合。過去 10 年程度の間に発生した情報セキュリティ関連の事故に関しては、全体（N=5162）の 76.5%、今後発生することを懸念している情報セキュリティ関連の事故に関しては、全体（N=5162）の 21.4%が「上記のいずれにもあてはまらない」と回答している。

(12) 情報セキュリティ対策の取組み状況

情報セキュリティ対策の取組み状況として、「ほぼ実践できている」、「十分ではないが実践している」とする回答は、「重要情報のバックアップを定期的に行う」が 84.6%と最も高く、次いで「不審な電子メールを受信したときのルールを決めたり、そのための対策製品を活用する」が 74.5%となっている。「情報セキュリティに関する規定、手順書を策定する」に関しては、「ほぼ実践できている」、「十分ではないが実践している」とする回答は 30.9%と最も低い。

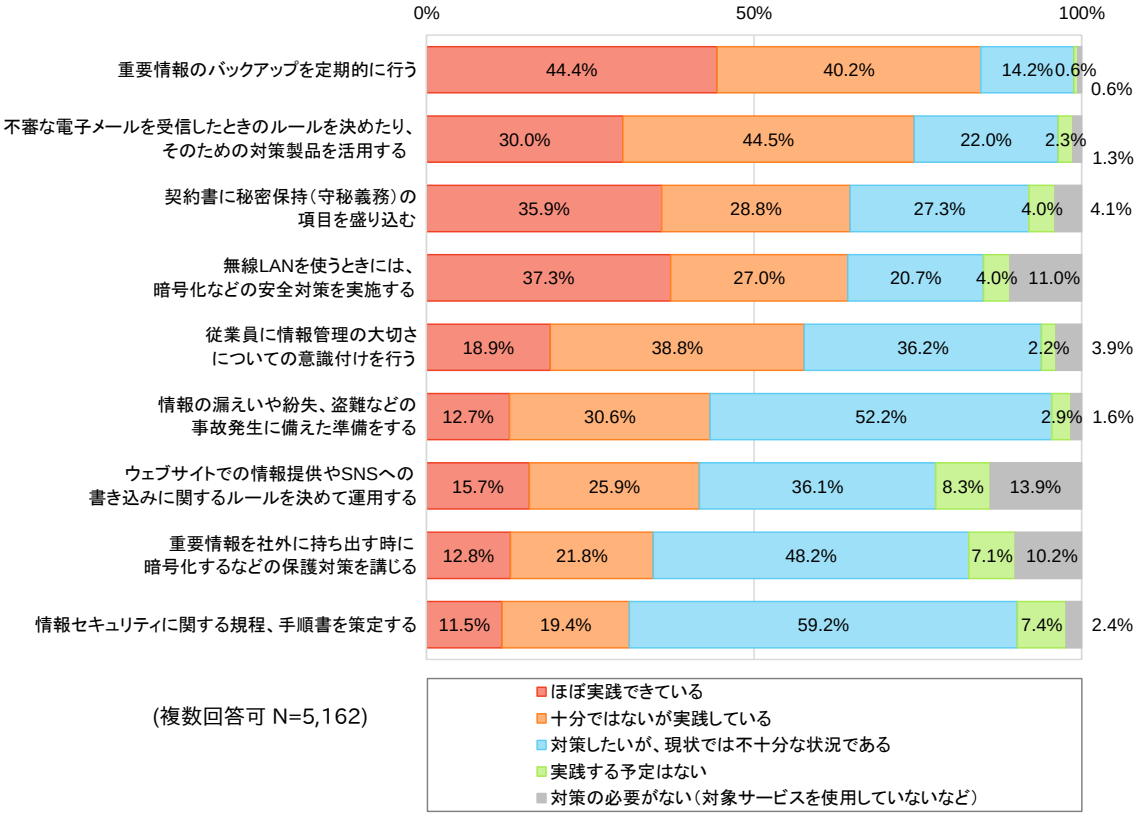

図 3-12　情報セキュリティ対策の取組み状況（Q12）

(13) 情報セキュリティ対策を進める上での課題点

情報セキュリティ対策を進める上での課題点は、「従業員の意識がまだ低い」が 56.6%と最も高い。また、「情報セキュリティ対策の知識をもった従業員がいない」が 42.7%、「業務を行うための人手が足りない状況である」が 41.8%である。

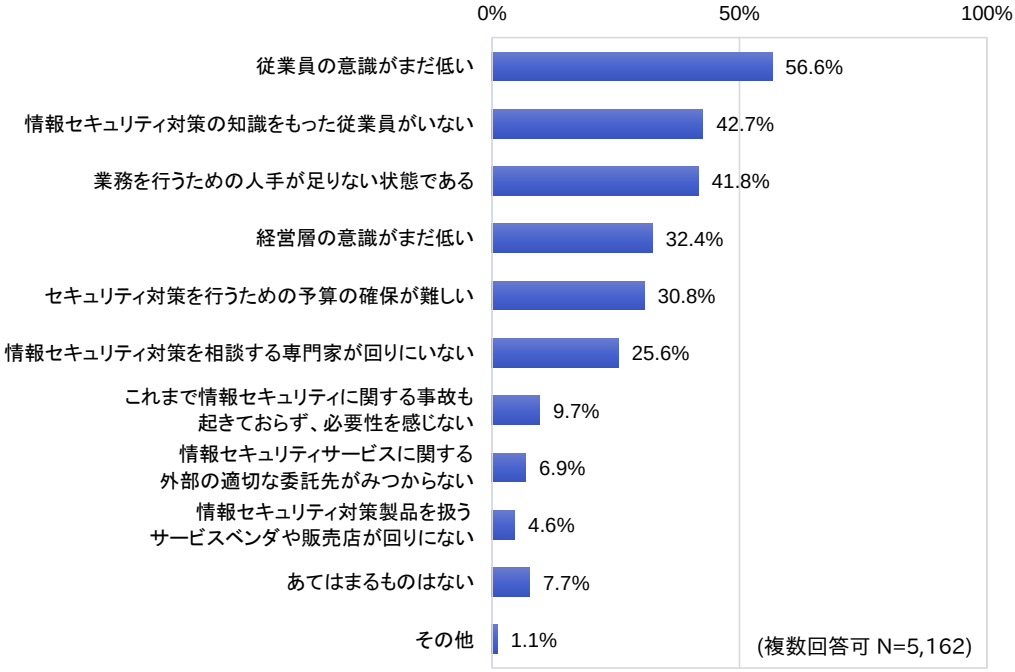

図 3-13　情報セキュリティ対策を進める上での課題点（Q13）

また、その他のフリー回答（自由記入）は、下記のとおりである。「情報セキュリティ対策のレベル、費用対効果」、「セキュリティ対策実施における課題」、「人材に関する課題」、「セキュリティ対策等に関する情報不足」、「外部委託、製品利用に関する課題」などの回答があった。

■　情報セキュリティ対策のレベル、費用対効果

- どこまで費用をかけ、どこまで対策するかの判断が難しい
- ここまでやればいい、という線引きが難しい
- 完璧な対策は難しい
- 対策と新たな脅威のイタチごっこ
- 対策の有効性と対策に掛ける価格の妥当性が分からない
- 費用対効果が判りにくい
- 目視できないものに対する費用対効果の説明が困難
- さらに対策する場合の費用対効果を見出すのが難しい
- 信頼できるモノやブランドが不十分

■ セキュリティ対策実施における課題

- IPA より提供されている情報セキュリティポリシーを参考に当社ポリシーを策定したが、テレワークや BYOD 等の最新の働き方にそぐわない部分もあり、課題に感じている
- 規程はあるが運用としてしっかり実施されているか、運用に無理のある規程になっていないかを十分に検証できていない
- 手順書等の作成
- クラウドサービス利用時の安全性
- 多様化したセキュリティインシデントへの迅速な対応
- 不審な電子メールによる標的型攻撃への対応
- IT ツールの利用が制限されており利便性が悪い
- 社屋の制約による物理的セキュリティの向上
- 繁忙時の対応
- 創立間もないため着手が難しい

■ 人材に関する課題

- 従業員が少ない為、経営者が自ら行っているが、専門の従業員が欲しい
- 従業員の意識に大きな差がある
- 情報セキュリティ対策を継承する次世代の人材がいない
- マンパワーが割けない
- 社内へのセキュリティ意識の更なる浸透

■ セキュリティ対策等に関する情報不足

- 最新対策や・事例の知識をあまり持ち合わせていない
- どの情報が正確かわからない
- 迅速に情報セキュリティに関する情報を入手すること

■ 外部委託、製品利用に関する課題

- 委託内容の妥当性の判断
- 企業規模や運用にマッチした製品がない
- 情報セキュリティ対策に関する事業者の専門知識

(14) 経営層の情報セキュリティ対策の意識を高める方策

前設問で「経営層の意識が低い」を選択した回答者のうち、今後、経営層による情報セキュリティ対策に関する意識を高めていくために必要と思うことは、「経営層が率先して情報セキュリティ対策を行うことに対するインセンティブ（補助金等）を設ける」が 24.1%と最も高く、次いで「被害事例や良事例を提示することで対策の必要性を実感してもらう」が 19.2%、「国や関係機関がより積極的に啓発活動を行う」、「経営層の参加する団体（業界団体、商工会等）を通じて取組を促す」が 18.5%である。

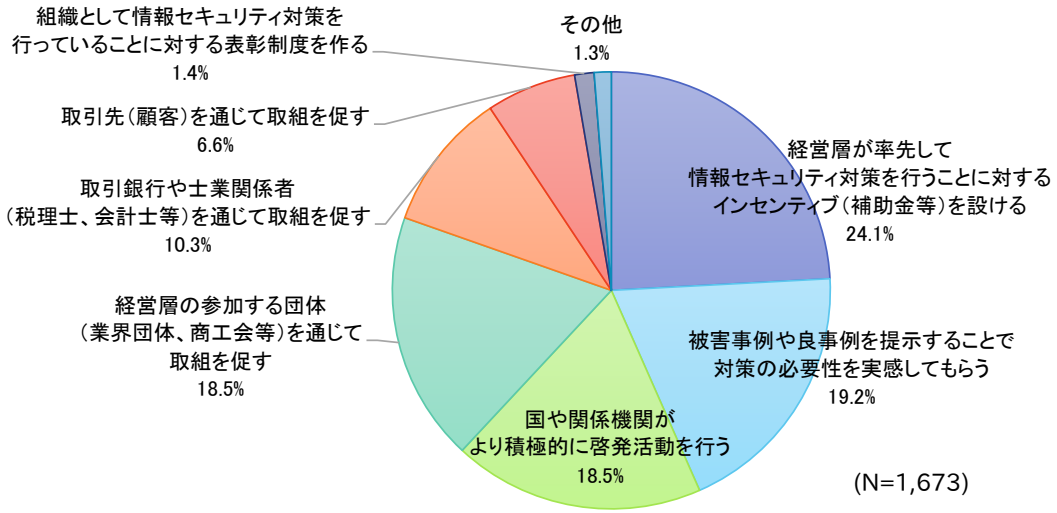

図 3-14　経営層が情報セキュリティ対策の意識を高めるために必要な取組（Q14）

また、フリー回答（自由記入）は、下記のとおりである。

- 画一化されたルールの策定と導入基準・資料を提供し、日本の企業（特に中小企業）が簡単に取組めるような仕組みを作る
- インセンティブではなく罰則・罰金による刑罰化
- IT リテラシーの向上（PC が苦手な人の利用制限）
- 企業におけるセキュリティの有資格者の雇用を義務化する
- 関係機関の経営層に対する情報セキュリティの重要性（経営の責任）に関する発信
- 国や関係機関、商工会議所による対策のための補助金など支援
- 地域での取組み
- 認証取得
- 事例集
- 分かり易いセキュリティ対策のやり方

(15) IPA が実施している中小企業の情報セキュリティ対策の普及策で関心のある取組み

関心のある取組みは、「わが社の情報セキュリティポリシー作成ツールの提供」が 34.2%、「映像で知る情報セキュリティ教材の配布」が 34.1%となっている。

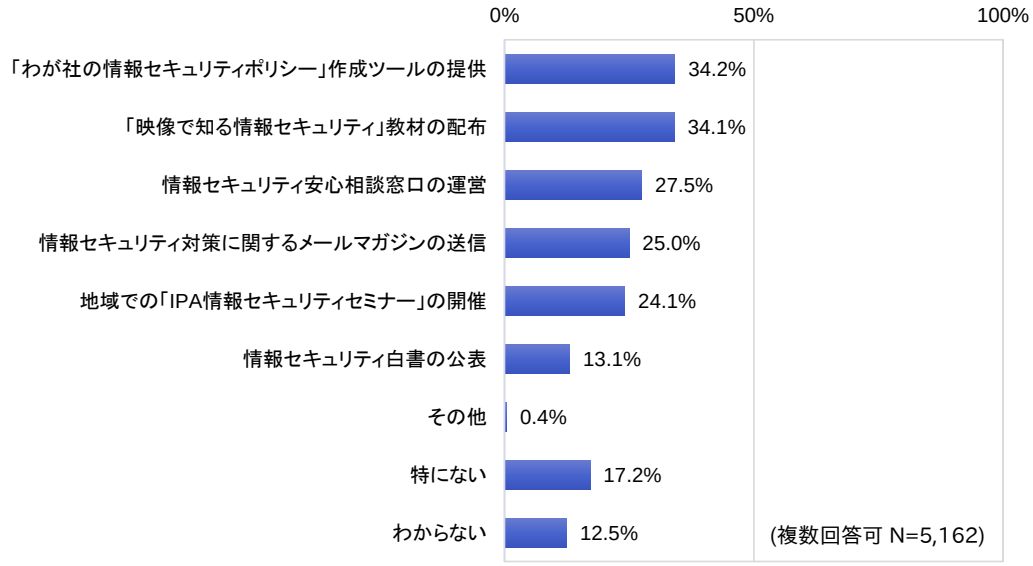

図 3-15　関心のある取組み（Q15）

(16) 今後注力していきたい情報セキュリティ関連の取組み

今後注力していきたい情報セキュリティ関連の取組みは、「従業員への情報セキュリティ教育」が 63.7%と最も高くなっている。

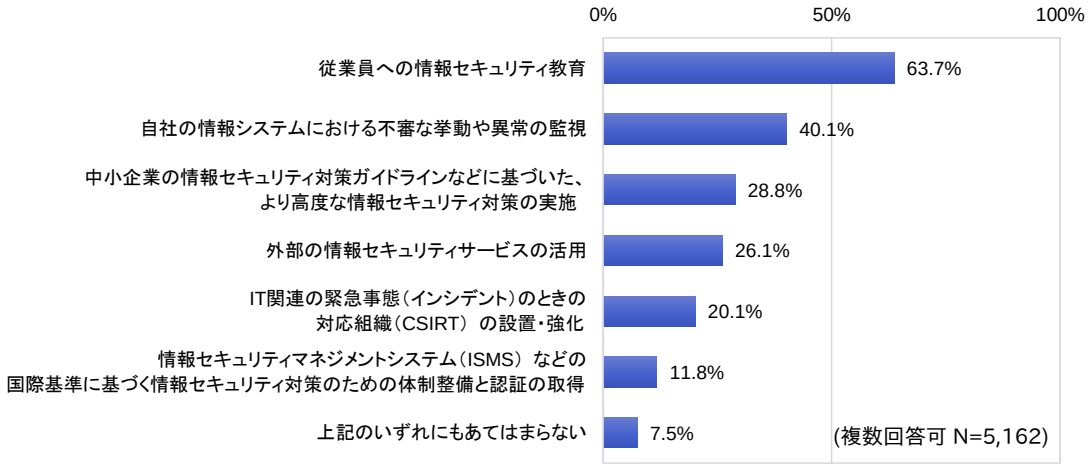

図 3-16　今後注力していきたい情報セキュリティ関連の取組（Q16）

3.2.2. クロス集計結果

以下には、業種、総従業員数といった回答事業者の基本的な属性、SECURITY ACTION 自己宣言の取組み目標（以下、取組み目標と記す。）、回答者の社内の立場（以下、回答者別と記す。）SECURITY ACTION 自己宣言の主導者（役割）等に着目し、アンケート回答をクロス集計した結果を示す。以下にはクロス集計の対象とした回答項目の一覧は下記のとおりである。

表 3-3 クロス集計の対象とした回答項目の一覧

番号	回答項目	アンケート質問番号
(1)	IT 依存度	Q6
(2)	総従業員数と取組み目標	Q3
(3)	総従業員数と回答者の立場	Q4
(4)	SECURITY ACTION 自己宣言の主導者（役割）	Q7
(5)	SECURITY ACTION 自己宣言を行おうとしたきっかけ	Q8
(6)	SECURITY ACTION 自己宣言で期待した効果	Q9
(7)	これまでに発生した事故（過去 10 年程度）	Q11
(8)	今後懸念している事故	Q11
(9)	情報セキュリティ対策の取組み状況	Q12
(10)	情報セキュリティ対策を進める上での課題点	Q13
(11)	経営層の情報セキュリティ対策の意識を高める方策	Q14
(12)	今後注力していきたい情報セキュリティ関連の取組み	Q16

なお、各回答のクロス集計のうち、属性や回答等により特徴が見られないものに関しては、クロス集計によるグラフ等は、報告書に掲載していない。

また、図表タイトル中の「Q#×Q#'」は「設問番号 Q#×設問番号 Q#'」のクロス集計を指す。

(1) IT 依存度

① 業種別

「IT への依存度」を「業種」別にみると、「情報通信業」、「金融業・保険業」、「複合サービス業」、「学術研究・専門・技術サービス業」などの IT 依存度が高い。なお、IT 依存度が低い業種は回答数が少ない傾向がある。

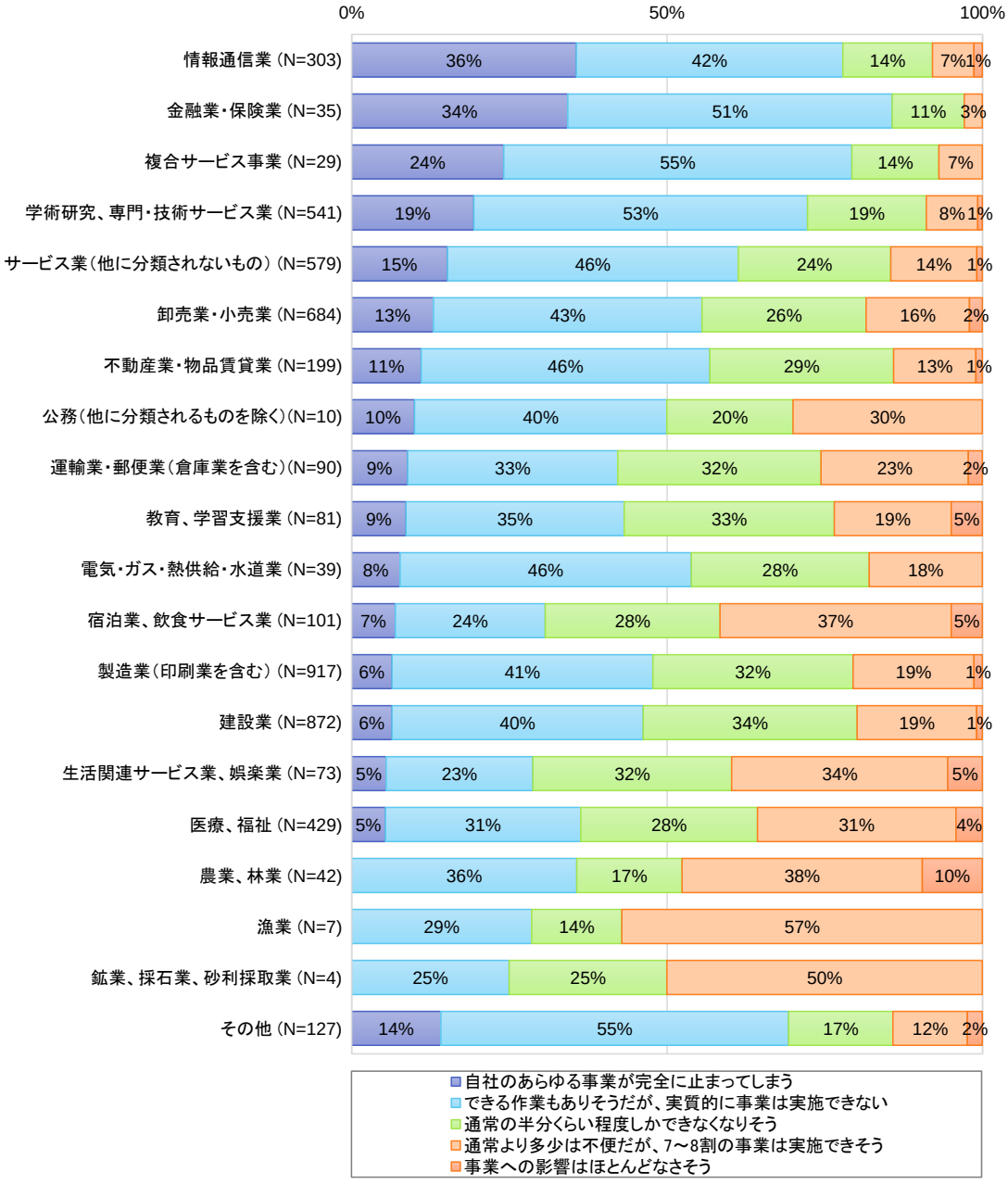

図 3-17 業種別の IT 依存度（Q1×Q6）

② 総従業員数別

「IT への依存度」を「総従業員数」別にみると、「301 名以上」の場合、「自社のあらゆる事業が完全に止まってしまう」と「できる作業もありそうだが、実質的に事業は実施できない」が合わせて 64%と IT 依存度の割合が最も高い。

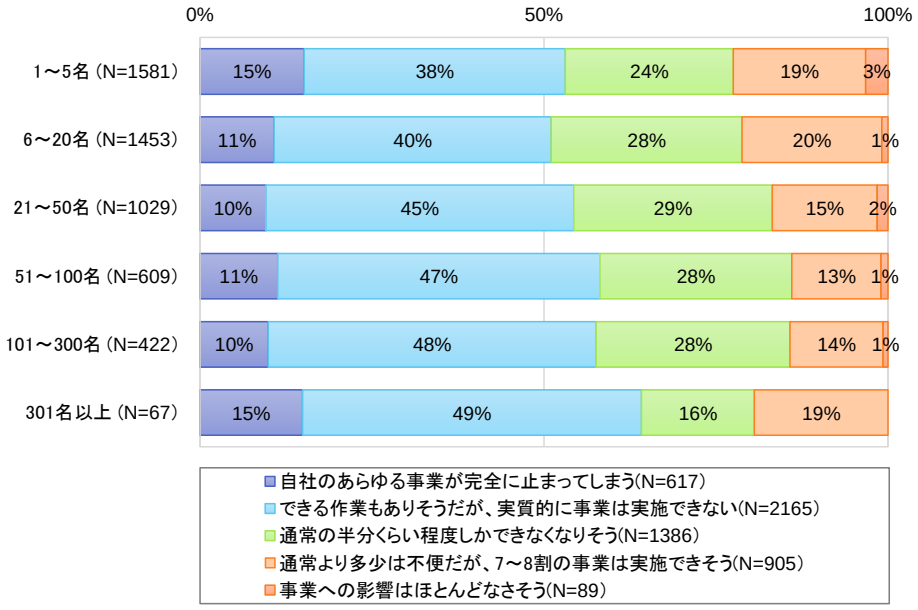

図 3-18 総従業員数別の IT 依存度（Q2×Q6）

(2) 総従業員数別の取組み目標

「取組み目標」を「総従業員数」別にみると、「301 名以上」では「2 つ星」の割合が 24%と最も高いものの、従業員規模による取組み目標に大きな差異がない。

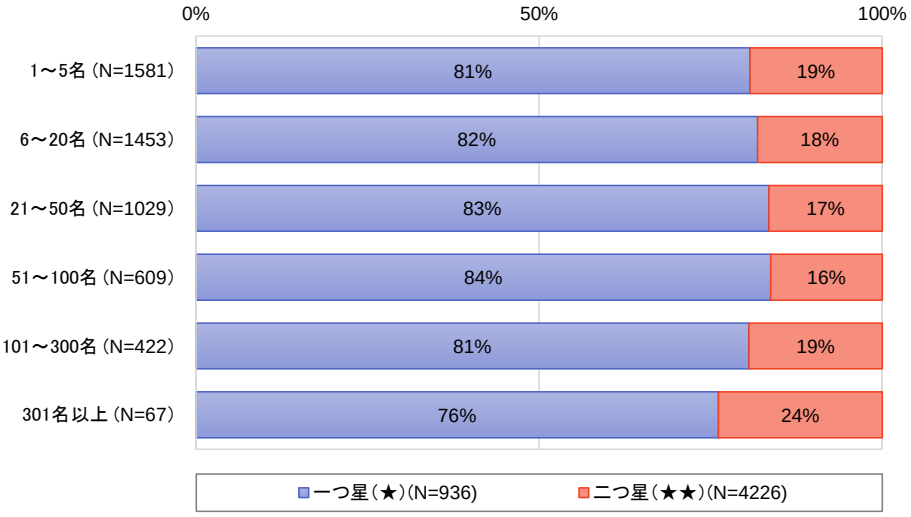

図 3-19 総従業員数別の取組み目標（Q2×Q3）

(3) 総従業員数別のと回答者の立場

「回答者の立場」を「総従業員数」別にみると、「1～5 名」の事業者では、「経営者」が 79%、「6～20 名」の事業者では経営者が 51%である。以降、従業員規模が多くなるに従い、経営者が回答する割合は低下し、「IT や情報セキュリティの担当者」の割合が増加する。従業員規模の大きさに伴い、情報セキュリティ対策に関する担当者が任命されている傾向が伺える。

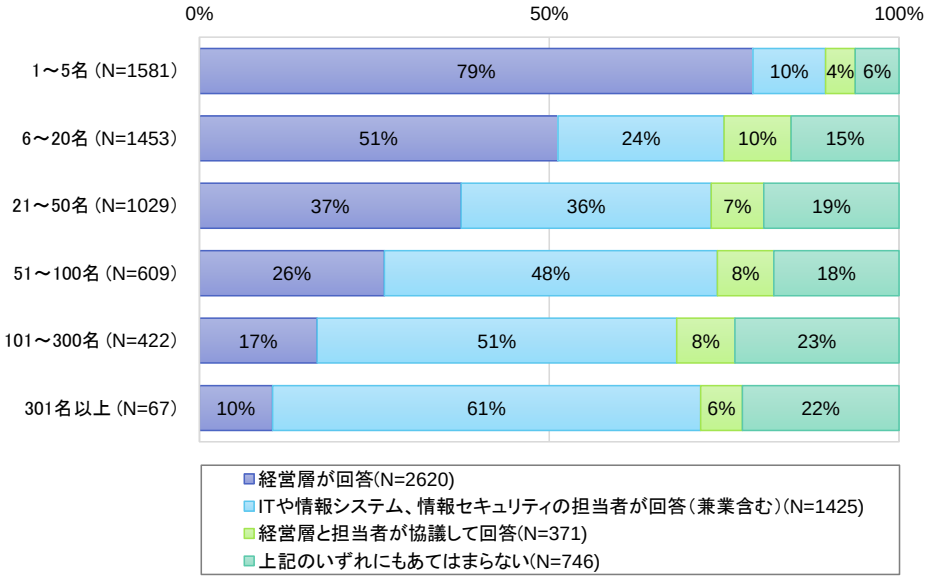

図 3-20 総従業員数別の回答者の立場（Q2×Q4）

(4) SECURITY ACTION 自己宣言の主導者（役割）

① 総従業員数別

「SECURITY ACTION に関する宣言を行うにあたって社内で主導的に進めていった役割の方」を「総従業員数」別にみると、従業員規模が少ないほど「経営者」が主導的に進めていった割合が高い。また、21 名以上の事業者では、「IT や情報システムの担当者」が主導する割合は 21～34%であり、総従業員数の増加に伴い、割合が高くなる傾向がある。また、「21～300 名」の場合には、「総務担当者」が主導的に進めた割合が 25～29%となっている。また、「301 名以上」の事業者では、「情報セキュリティ担当者」が主導的に進めた割合が 25%であり、「総従業員数」それ以下の事業者と比べて高い。

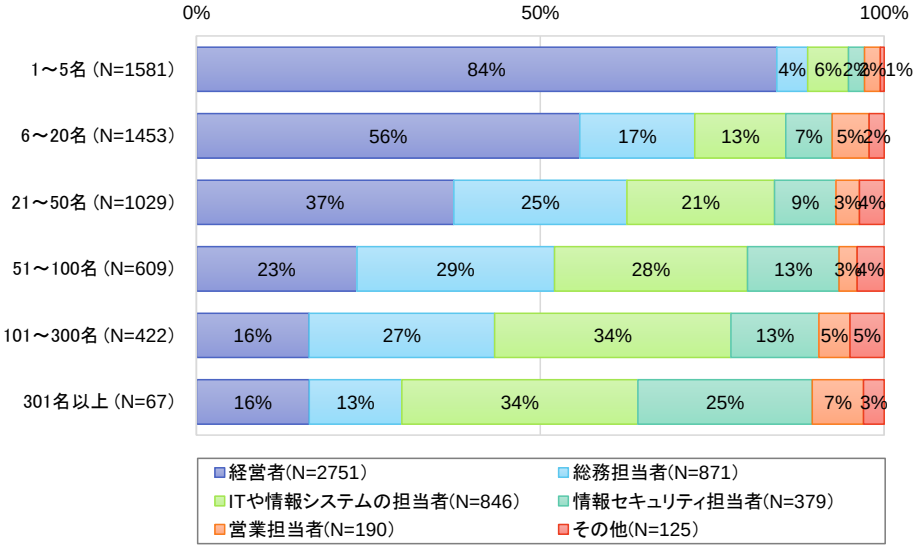

図 3-21 総従業員数別 SECURITY ACTION 宣言の主導者（役割）（Q2×Q7）

② 取組み目標別

「SECURITY ACTION に関する宣言を行うにあたって社内で主導的に進めていった役割の方」を「直近で宣言した SECURITY ACTION の取組み目標」別にみると、いずれも「経営者」が 50%以上と最も高い。「一つ星」の場合、「経営者」に次いで、「総務担当者」18%、「IT や情報システムの担当者」が 17%、「二つ星」の場合、「経営者」に次いで、「IT や情報システムの担当者」が 15%、「情報セキュリティ担当者」が 14%となっている。

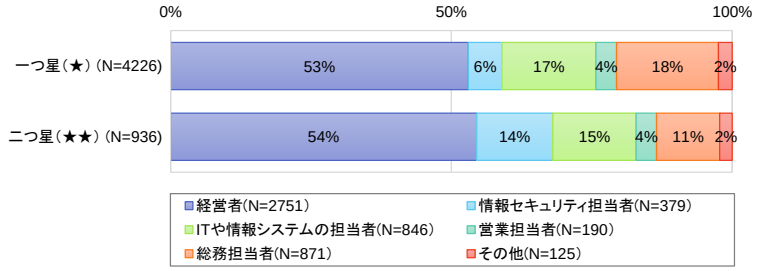

図 3-22 取組み目標別 SECURITY ACTION 宣言の主導者（役割）（Q3×Q7）

(5) SECURITY ACTION 宣言を行おうとしたきっかけ

① 業種別

「SECURITY ACTION 宣言を行おうとしたきっかけ」を「業種」別にみると、業種を問わず「補助金を申請する際の要件となっていた」の割合が高いが、「情報通信業」のみ「取引先からの信頼」が「補助金を申請する際の要件となっていた」を上回り、53.8%である。

表 3-4　業種別 SECURITY ACTION 宣言を行ったきっかけ（Q8×Q1）（複数回答可）

	過去に自社で情報セキュリティに関するトラブルがあり、改善したいと考えていた	他社での情報セキュリティに関する事故を知って、自社でも改善したいと考えていた	取引先からの信頼を高める手段として有用と考えた	事業拡大や顧客開拓に有用と考えた	取引先から取得を勧められた	IT製品のベンダや販売店から取得を勧められた	ITコーディネーターや中小企業診断士、税理士、社会保険労務士、商工会、知人等から勧められた	知り合いの企業等から一緒にやろうと誘われた	補助金を申請する際の要件となっていた	その他
全体（N=5162）	6%	15%	30%	20%	9%	18%	11%	1%	77%	1%
農業、林業(N=42)	2.4%	9.5%	28.6%	28.6%	16.7%	11.9%	9.5%	－	78.6%	－
漁業(N=7)	－	14.3%	28.6%	28.6%	14.3%	14.3%	－	－	71.4%	－
鉱業、採石業、砂利採取業(N=4)	25.0%	25.0%	－	－	－	25.0%	25.0%	－	50.0%	－
建設業(N=872)	5.8%	13.8%	27.8%	20.4%	10.0%	24.4%	9.3%	1.1%	81.8%	0.1%
製造業（印刷業を含む）(N=917)	7.1%	14.3%	24.4%	14.1%	4.6%	19.0%	10.9%	0.2%	85.8%	0.7%
電気・ガス・熱供給・水道業(N=39)	7.7%	10.3%	28.2%	10.3%	7.7%	33.3%	5.1%	－	76.9%	2.6%
情報通信業(N=303)	3.6%	17.8%	53.8%	29.0%	15.2%	6.9%	9.6%	4.6%	49.5%	4.3%
運輸業・郵便業（倉庫業を含む）(N=90)	6.7%	17.8%	25.6%	13.3%	2.2%	24.4%	11.1%	－	75.6%	1.1%
卸売業・小売業(N=684)	5.3%	15.2%	26.6%	21.3%	8.5%	21.5%	13.2%	0.9%	78.9%	0.6%
金融業・保険業(N=35)	11.4%	22.9%	42.9%	31.4%	11.4%	11.4%	11.4%	－	80.0%	－
不動産業・物品賃貸業(N=199)	9.5%	16.6%	33.7%	22.6%	16.6%	16.6%	9.5%	1.5%	76.4%	－
学術研究、専門・技術サービス業(N=541)	6.3%	15.2%	34.9%	20.9%	6.5%	17.9%	10.2%	1.1%	78.7%	1.5%
宿泊業、飲食サービス業(N=101)	3.0%	14.9%	21.8%	25.7%	14.9%	11.9%	13.9%	1.0%	76.2%	1.0%
生活関連サービス業、娯楽業(N=73)	6.8%	9.6%	19.2%	21.9%	13.7%	12.3%	8.2%	1.4%	74.0%	－
教育、学習支援業(N=81)	7.4%	22.2%	37.0%	32.1%	17.3%	18.5%	12.3%	－	71.6%	－
医療、福祉(N=429)	3.5%	17.7%	18.6%	20.7%	14.2%	18.9%	12.6%	1.4%	79.3%	0.2%
複合サービス事業(N=29)	13.8%	31.0%	44.8%	17.2%	13.8%	3.4%	13.8%	10.3%	62.1%	－
サービス業（他に分類されないもの）(N=579)	5.9%	15.4%	37.3%	22.8%	9.5%	14.0%	11.6%	1.4%	70.3%	2.6%
公務（他に分類されるものを除く）(N=10)	10.0%	20.0%	40.0%	10.0%	－	10.0%	20.0%	－	40.0%	20.0%
その他(N=127)	3.9%	15.7%	23.6%	16.5%	10.2%	12.6%	14.2%	1.6%	63.8%	11.0%

表中の－は 0.0%を示す

② 取組み目標別

「SECURITY ACTION 自己宣言を行おうとしたきっかけ」を「目標」別にみると、何れも「補助金を申請する際の要件となっていた」ことがきっかけであった割合が高く、特に一つ星は 81%と二つ星に比べ割合が高い。また、二つ星では、「取引先からの信頼を高める手段として有用と考えた」や、「事業拡大や顧客開拓に有用と考えた」とする割合が一つ星より高い。

このことから補助金の申請要件であったことが情報セキュリティ対策の第一ステップの取組み契機となっており、取組みが進むにつれ、取引先との信頼関係の強化、事業拡大や顧客を意識する割合が高くなると考えられる。

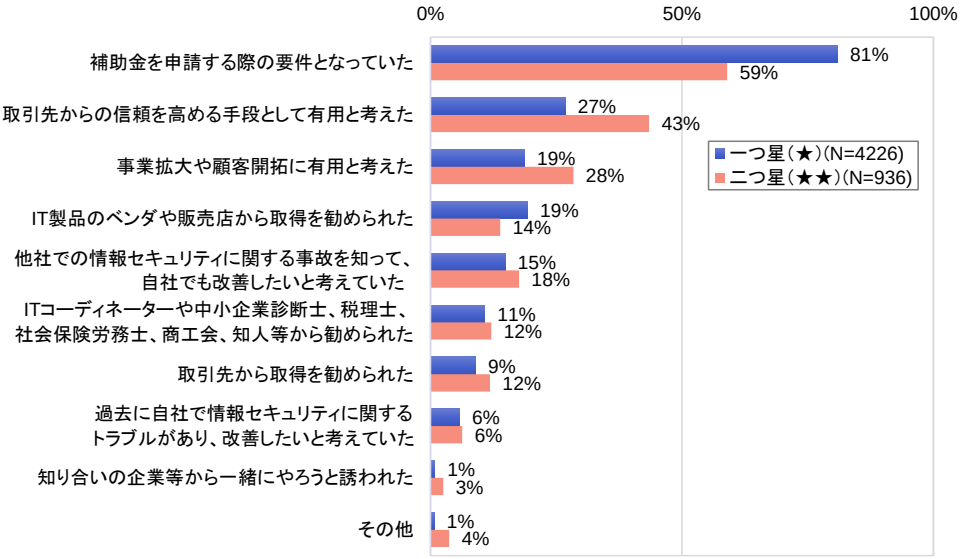

図 3-23 取組み目標別 SECURITY ACTION 宣言を行ったきっかけ（Q8×Q3）

③　SECURITY ACTION 自己宣言の主導者（役割）別

「SECURITY ACTION 自己宣言を行おうとしたきっかけ」を「宣言を行うにあたって社内で主導的に進めていった役割の方」別にみると、いずれも「補助金を申請する際の要件となっていた」の割合が高いが、情報セキュリティ担当者、経営者は「取引先からの信頼」の割合が高い。情報セキュリティ担当者、経営者の場合、その対策が持つ効果の理解度が高いためと考えられる。

表 3-5　SECURITY ACTION 宣言の主導者（役割）別 SECURITY ACTION 宣言を行ったきっかけ（Q8×Q7）（複数回答可）

	過去に自社で情報セキュリティに関するトラブルがあり、改善したいと考えていた	他社での情報セキュリティに関する事故を知って、自社でも改善したいと考えていた	取引先からの信頼を高める手段として有用と考えた	事業拡大や顧客開拓に有用と考えた	取引先から取得を勧められた	IT製品のベンダや販売店から取得を勧められた	ITコーディネーターや中小企業診断士、税理士、社会保険労務士、商工会、知人等から勧められた	知り合いの企業等から一緒にやろうと誘われた	補助金を申請する際の要件となっていた	その他
全体 (N=5162)	5.9%	15.4%	29.8%	20.5%	9.5%	18.3%	11.0%	1.2%	77.0%	1.3%
経営者 (N=2751)	5.9%	16.4%	33.1%	25.1%	10.0%	17.8%	12.8%	1.5%	74.1%	0.9%
情報セキュリティ担当者 (N=379)	9.0%	20.6%	41.2%	20.6%	12.1%	13.2%	7.9%	0.8%	61.5%	2.9%
IT や情報システムの担当者 (N=846)	6.6%	15.2%	24.6%	15.1%	7.1%	19.6%	9.1%	1.2%	79.8%	1.8%
営業担当者 (N=190)	4.2%	10.5%	26.3%	24.2%	12.6%	14.7%	11.1%	1.1%	84.2%	1.1%
総務担当者 (N=871)	3.9%	12.1%	22.3%	10.9%	8.5%	21.7%	9.0%	0.3%	87.6%	0.9%
その他 (N=125)	7.2%	8.0%	16.0%	14.4%	8.8%	18.4%	8.8%	1.6%	82.4%	4.8%

(6) SECURITY ACTION 自己宣言で期待した効果

① 取組み目標別

「SECURITY ACTION 自己宣言をしたことで、どのような効果を期待しているか」を「取組み目標」別にみると、二つ星は一つ星と比べ、ほとんどの項目[6]において、効果を期待している割合が高い。特に、「取引先からの信頼が高まる」、「新規の取引先を開拓する」、「自社の社会的な知名度を高める」、「SECURITY ACTION のロゴマークを掲載して対外的にアピールする」の割合の差が大きく、対外的な効果を期待していることが伺える。

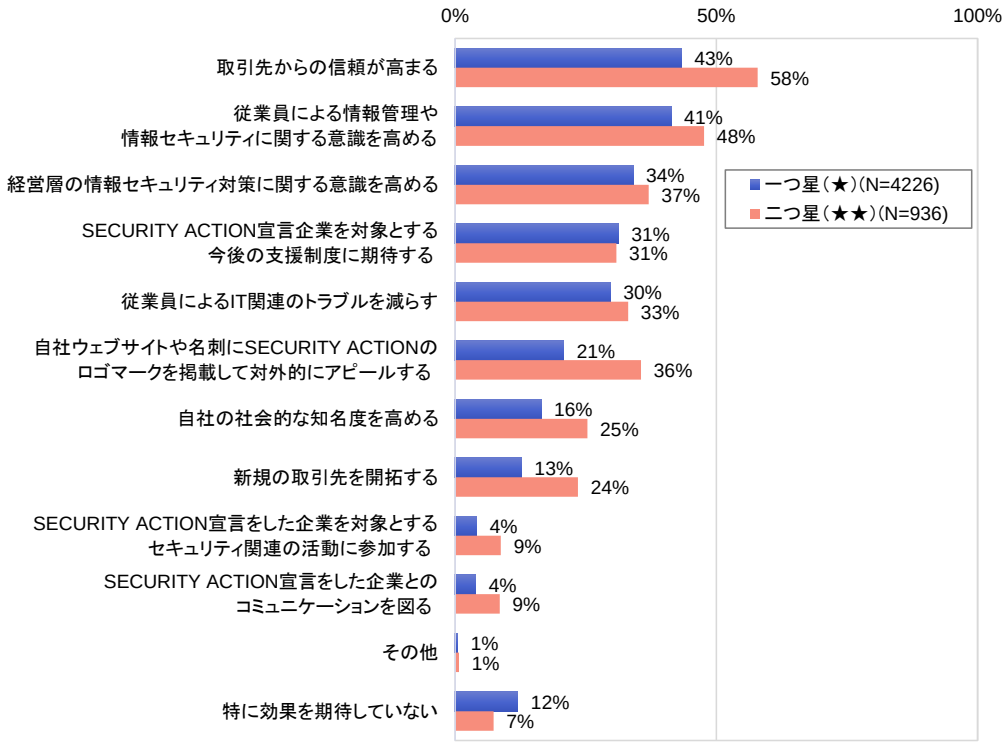

図 3-24　取組み目標別 SECURITY ACTION 宣言に期待する効果（Q9×Q3）

[6] 「SECURITY ACTION 宣言企業を対象とする今後の支援制度に期待する」のみ、同程度の割合である。

② SECURITY ACTION 自己宣言の主導者（役割）別

「SECURITY ACTION 自己宣言をしたことで、どのような効果を期待しているか」を「SECURITY ACTION 自己宣言を行うにあたって、社内で主導的に進めていった役割の方」別にみると、「取引先からの信頼が高まる」効果を期待する割合は、「情報セキュリティ担当者」、「経営者」が高く、5 割を超える。また、「従業員による情報管理や情報セキュリティに関する意識を高める」効果を期待する割合は、「情報セキュリティ担当者」は、5 割を超えるが、「経営者」は 37.7%に止まる。

表 3-6　SECURITY ACTION 宣言の主導者（役割）別 SECURITY ACTION 宣言をしたことで、どのような効果を期待しているか（Q9×Q7）（複数回答可）

	取引先からの信頼が高まる	従業員による情報管理や情報セキュリティに関する意識を高める	経営層の情報セキュリティ対策に関する意識を高める	SECURITY ACTION 宣言企業を対象とする今後の支援制度に期待する	従業員による IT 関連のトラブルを減らす	自社ウェブサイトや名刺に SECURITY ACTION のロゴマークを掲載して対外的にアピールする	自社の社会的な知名度を高める	新規の取引先を開拓する	SECURITY ACTION 宣言をした企業を対象とするセキュリティ関連の活動に参加する	SECURITY ACTION 宣言をした企業とのコミュニケーションを図る	その他	特に効果を期待していない
全体 (N=5162)	46.0%	42.5%	34.6%	31.2%	30.4%	23.5%	18.1%	14.7%	5.0%	4.8%	0.6%	11.2%
経営者 (N=2751)	50.3%	37.7%	36.8%	30.5%	28.7%	26.2%	21.0%	18.6%	5.8%	6.5%	0.5%	10.4%
情報セキュリティ担当者 (N=379)	54.1%	50.7%	38.0%	24.8%	36.7%	30.3%	20.6%	16.9%	7.7%	5.0%	0.3%	9.5%
IT や情報システムの担当者 (N=846)	40.2%	46.5%	34.0%	33.0%	33.5%	22.2%	14.9%	9.2%	4.7%	2.8%	0.9%	11.6%
営業担当者 (N=190)	45.8%	43.7%	25.3%	28.4%	22.6%	23.7%	20.5%	18.4%	3.2%	4.7%	－	13.2%
総務担当者 (N=871)	36.9%	48.3%	30.3%	33.3%	31.2%	14.4%	11.3%	6.5%	1.8%	1.6%	0.6%	13.4%
その他 (N=125)	29.6%	55.2%	26.4%	44.0%	32.8%	14.4%	12.8%	11.2%	6.4%	4.0%	2.4%	14.4%

表中の－は 0.0%を示す

(7) これまでに発生した事故（過去 10 年程度）[7]

① 業種別[8]

製造業、卸業・小売業、学術研究、専門・技術サービス業、サービス業（他に分類されないもの）では、「従業員の誤送信・誤操作による情報の漏えい・消失」、「コンピュータウイルス（マルウェア）感染による情報の漏えい・消失・改ざん」の順で発生割合が高い。これに対し、建設業では、「コンピュータウイルス（マルウェア）感染による情報の漏えい・消失・改ざん」、「従業員の誤送信・誤操作による情報の漏えい・消失」の順で発生割合が高い。

表 3-7　業種別 過去 10 年ほどの間に次のような事故が発生したか（Q11-1×Q1）

	従業員の誤送信・誤操作による情報の漏えい・消失	コンピュータウイルス（マルウェア）感染による情報の漏えい・消失・改ざん	PC や USB メモリの盗難・紛失による情報の漏えい・消失	自社への不正アクセス、不正侵入	ランサムウェア感染による情報の消失	従業員による内部不正	自社のウェブサイトの改ざん
全体(N=1215)	44.8%	32.2%	18.1%	15.0%	11.9%	9.3%	8.1%
農業、林業(N=9)	22.2%	55.6%	22.2%	－	11.1%	－	11.1%
漁業(N=1)	－	－	－	100.0%	－	－	－
鉱業、採石業、砂利採取業(N=1)	－	－	100.0%	－	－	－	－
建設業(N=197)	37.6%	40.6%	22.3%	14.7%	12.7%	8.6%	5.6%
製造業（印刷業を含む）(N=262)	50.8%	29.0%	15.6%	11.5%	13.4%	6.5%	8.8%
電気・ガス・熱供給・水道業(N=9)	66.7%	33.3%	11.1%	－	11.1%	－	－
情報通信業(N=72)	56.9%	26.4%	19.4%	13.9%	11.1%	8.3%	5.6%
運輸業・郵便業（倉庫業を含む）(N=15)	33.3%	26.7%	13.3%	6.7%	13.3%	6.7%	－
卸売業・小売業(N=179)	45.3%	31.8%	13.4%	12.3%	16.8%	12.8%	7.8%
金融業・保険業(N=7)	28.6%	14.3%	28.6%	14.3%	14.3%	42.9%	14.3%
不動産業・物品賃貸業(N=40)	50.0%	32.5%	15.0%	12.5%	20.0%	10.0%	5.0%
学術研究、専門・技術サービス業(N=118)	43.2%	31.4%	22.0%	17.8%	4.2%	3.4%	7.6%
宿泊業、飲食サービス業(N=22)	31.8%	36.4%	22.7%	22.7%	9.1%	9.1%	4.5%
生活関連サービス業、娯楽業(N=8)	－	50.0%	－	75.0%	12.5%	－	12.5%
教育、学習支援業(N=21)	42.9%	19.0%	19.0%	19.0%	14.3%	9.5%	9.5%
医療、福祉(N=81)	40.7%	24.7%	24.7%	16.0%	4.9%	16.0%	8.6%
複合サービス事業(N=10)	50.0%	20.0%	－	20.0%	20.0%	－	10.0%
サービス業（他に分類されないもの）(N=137)	46.7%	36.5%	16.8%	19.0%	10.2%	12.4%	11.7%
公務（他に分類されるものを除く）(N=4)	75.0%	－	25.0%	－	－	25.0%	－
その他（上記 1～19 で分類不能の産業）(N=22)	36.4%	36.4%	18.2%	27.3%	13.6%	13.6%	22.7%

表中の－は 0.0%を示す。

7 アンケート回答の「上記のいずれにもあてはまらない」を除いた回答数を 100%とした割合

8 回答数が 100 以上業種（青色）の傾向を示した。

② 総従業員数別

「従業員の誤送信・誤操作による情報の漏えい・消失」は総従業員数が大きくなるほど増加する傾向にある。「コンピュータウイルス（マルウェア）感染による情報の漏えい・消失・改ざん」は、「1~5 名」の事業者で、それ以上の総従業員数の事業者と比較して、発生した割合が高い。また、「自社のウェブサイトの改ざん」は、「301 名以上」の事業者で発生した割合が高い。

表 3-8 総従業員数別 過去 10 年ほどの間に発生した情報セキュリティに関する事故（Q11-1×Q2）

	従業員の誤送信・誤操作による情報の漏えい・消失	コンピュータウイルス（マルウェア）感染による情報の漏えい・消失・改ざん	PC や USB メモリの盗難・紛失による情報の漏えい・消失	自社への不正アクセス、不正侵入	ランサムウェア感染による情報の消失	従業員による内部不正	自社のウェブサイトの改ざん
全体 (N=1215)	44.8%	32.2%	18.1%	15.0%	11.9%	9.3%	8.1%
1～5 名 (N=283)	32.9%	43.1%	21.2%	20.5%	7.1%	7.4%	9.2%
6～20 名 (N=289)	42.6%	29.4%	13.5%	15.9%	9.7%	12.1%	10.0%
21～50 名 (N=274)	49.3%	31.8%	17.2%	12.0%	15.0%	9.5%	5.8%
51～100 名 (N=185)	56.2%	22.2%	18.9%	13.0%	13.5%	7.0%	3.8%
101～300 名 (N=153)	45.8%	32.0%	22.2%	10.5%	17.6%	11.1%	8.5%
301 名以上 (N=31)	61.3%	22.6%	16.1%	16.1%	12.9%	3.2%	22.6%

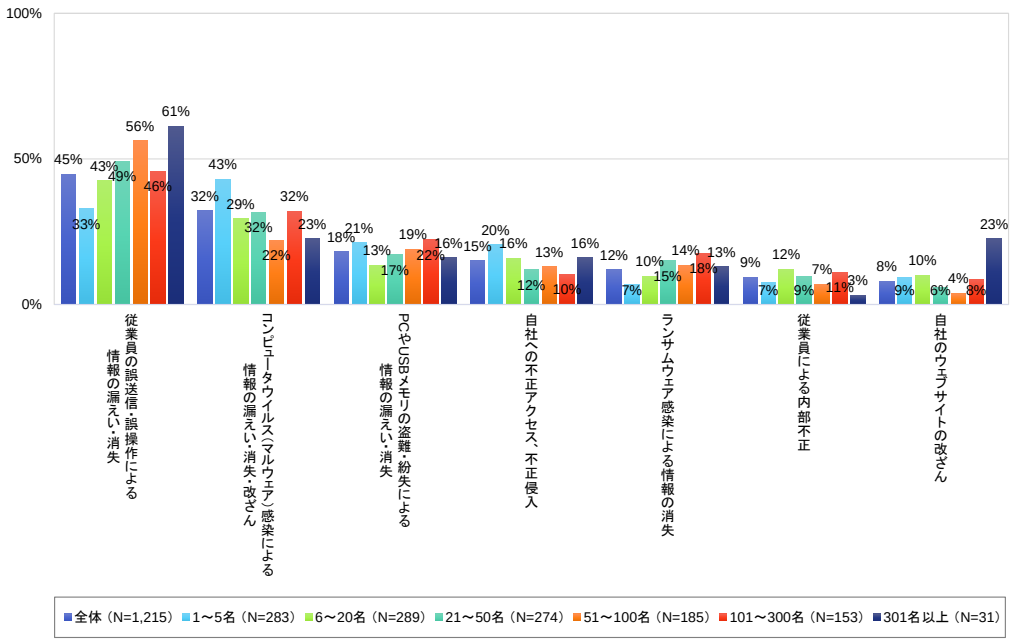

図 3-25 総従業員数別 過去 10 年ほどの間に発生した情報セキュリティに関する事故（Q11-1×Q2）

(8) 今後懸念している事故[9]

① 総従業員数別

「今後次のような事故が発生することを懸念しているか」を「総従業員数」別にみると、全体的に従業員数が多くなるにつれ、事故の発生を懸念している割合が高くなる傾向がある。「301 名以上」の事業者は「従業員の誤送信・誤操作による情報の漏えい・消失」、「自社のウェブサイトの改ざん」、「従業員による内部不正」を懸念している割合が高い。「従業員による内部不正」に関しては、51 名以上の事業者では、「自社のウェブサイトの改ざん」を懸念する割合を上回り、「301 名以上」の事業者は、「1～5 名」の事業者と比較して約 2 倍の割合の事業者が発生を懸念している。内部不正は、目の行き届かない環境で発生する傾向[10]があるため、従業員数が増えるほど内部不正に対する監視性の確保が困難になり、懸念する割合が高くなると考えられる。

表 3-9 総従業員数別 今後発生が懸念される情報セキュリティに関する事故（Q11-2×Q2）

	コンピュータウイルス（マルウェア）感染による情報の漏えい・消失・改ざん	PC や USB メモリの盗難・紛失による情報の漏えい・消失	従業員の誤送信・誤操作による情報の漏えい・消失	自社への不正アクセス、不正侵入	ランサムウェア感染による情報の消失	自社のウェブサイトの改ざん	従業員による内部不正
全体（N=4,057）	78.8%	65.7%	65.7%	61.6%	60.8%	45.1%	41.1%
1～5 名（N=1,177）	81.3%	63.0%	55.0%	60.2%	57.9%	44.8%	31.2%
6～20 名（N=1,129）	77.1%	64.0%	66.1%	61.8%	59.6%	42.2%	38.1%
21～50 名（N=825）	78.8%	65.7%	70.5%	61.3%	61.6%	44.4%	43.9%
51～100 名（N=509）	80.0%	70.1%	73.5%	61.1%	64.6%	49.1%	52.5%
101～300 名（N=358）	75.1%	73.2%	74.6%	64.8%	66.2%	49.7%	56.7%
301 名以上（N=59）	69.5%	71.2%	83.1%	71.2%	67.8%	57.6%	62.7%

[9] アンケート回答の「上記のいずれにもあてはまらない」を除いた回答数を 100%とした割合

[10] 独立行政法人情報処理推進機構「内部不正による情報セキュリティインシデント実態調査」（2016 年）
https://www.ipa.go.jp/files/000051140.pdf

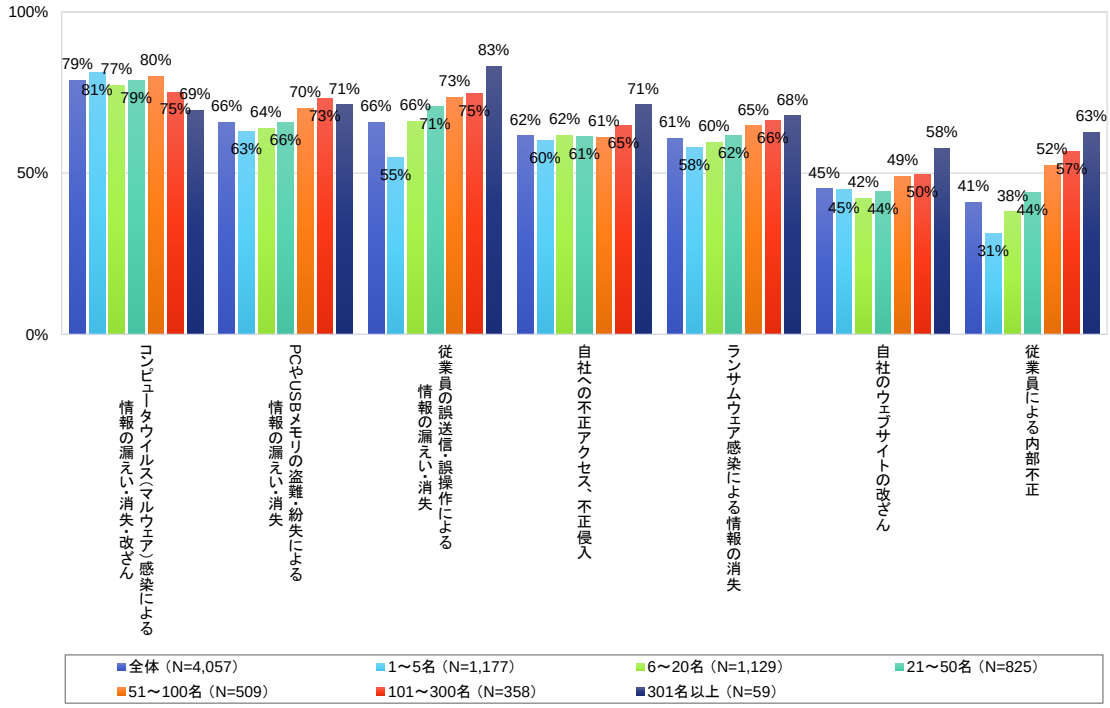

図 3-26　総従業員数別 今後発生が懸念される情報セキュリティに関する事故（Q11-2×Q2）

(9) 情報セキュリティ対策の取組み状況

① 業種別

「情報セキュリティ対策の取組み状況」を「業種」別にみると、「情報通信業」はいずれの対策も「ほぼ実践できている」「十分ではないが実践している」が 7 割を超え、次いで「金融業・保険業」が 5 割と高い割合になっている。

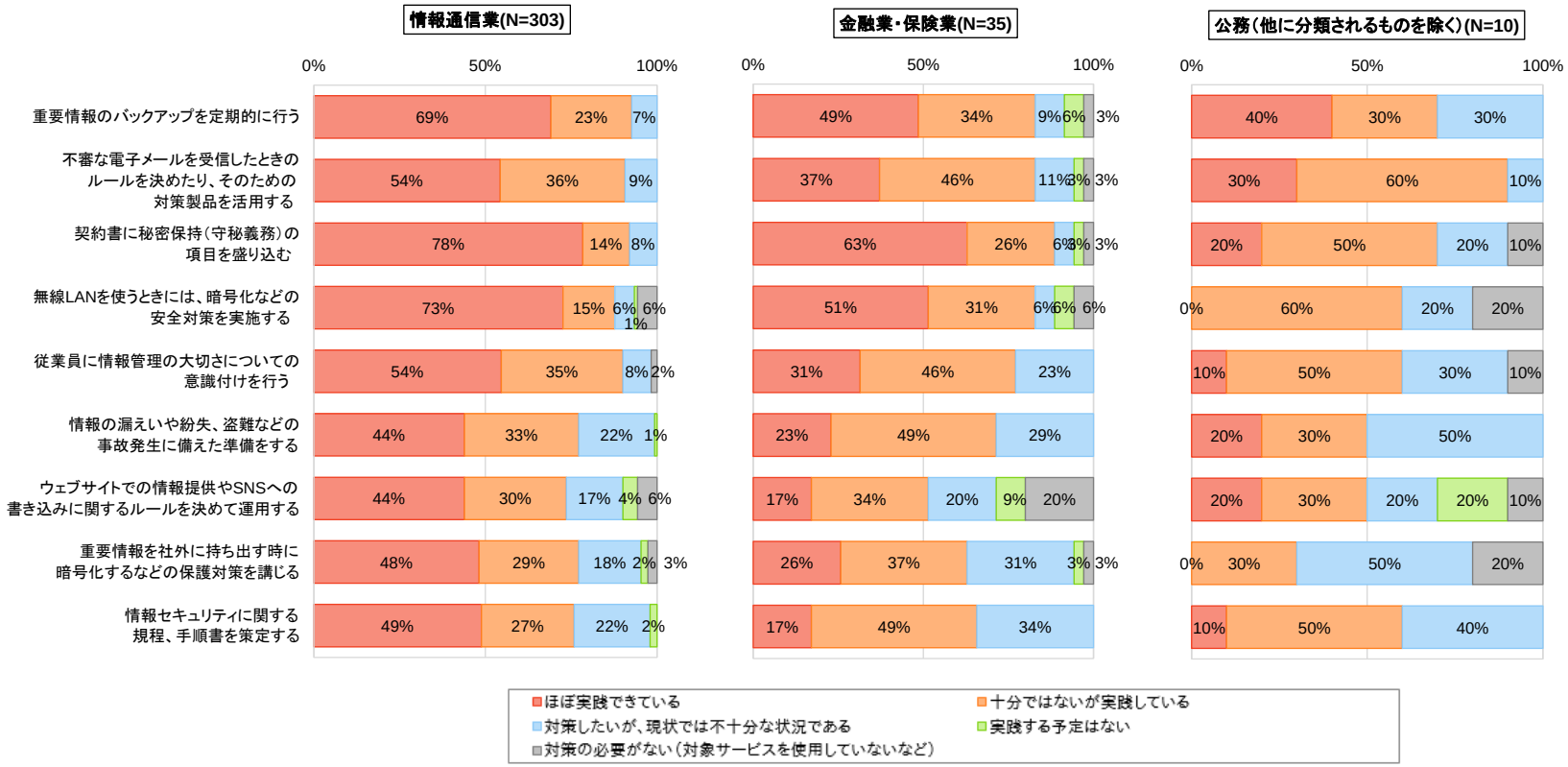

図 3-27 業種別 情報セキュリティ対策について貴社の取組み状況①(Q12×Q1)

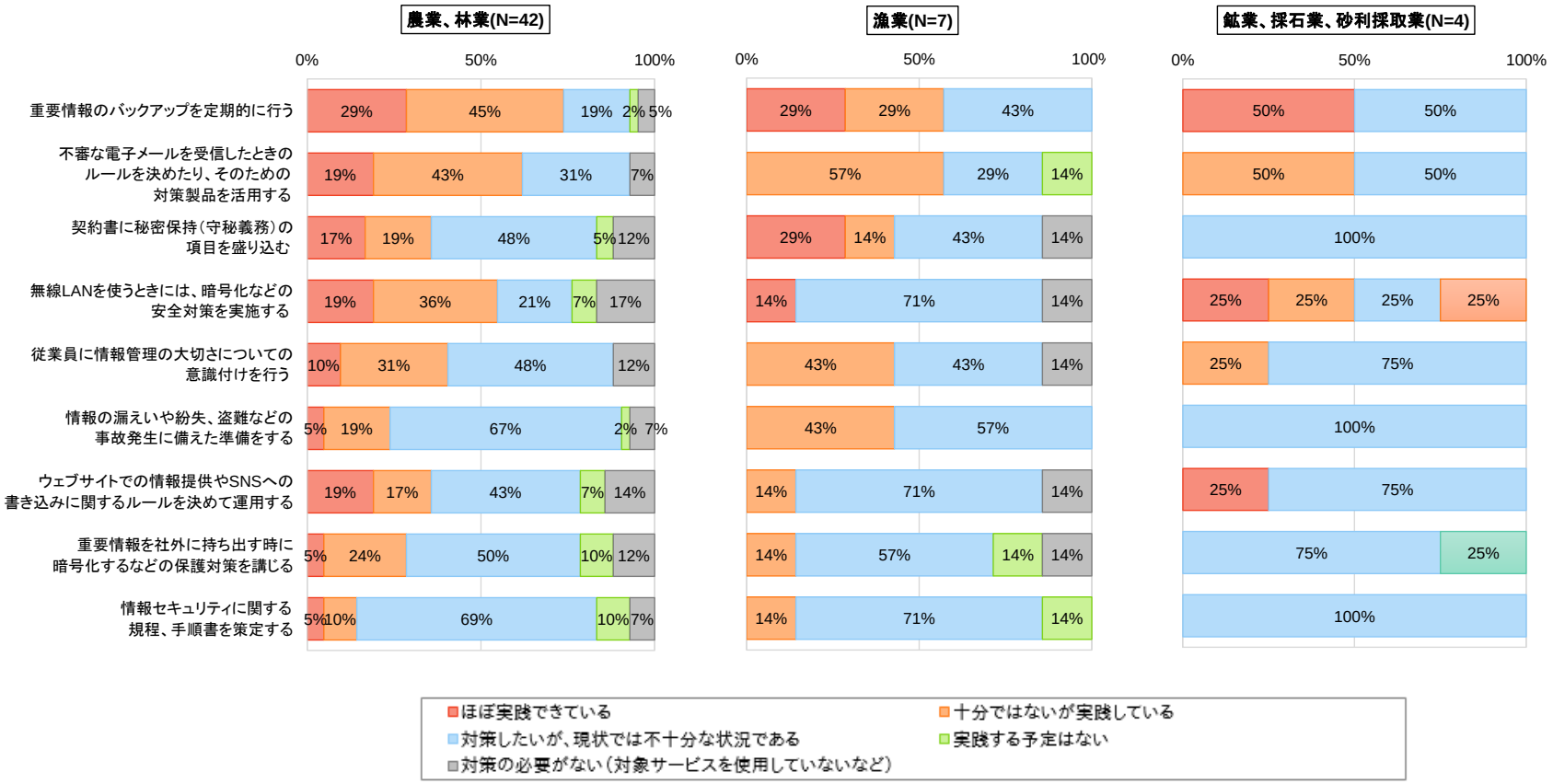

図 3-28　業種別 情報セキュリティ対策について貴社の取組み状況②(Q12×Q1)

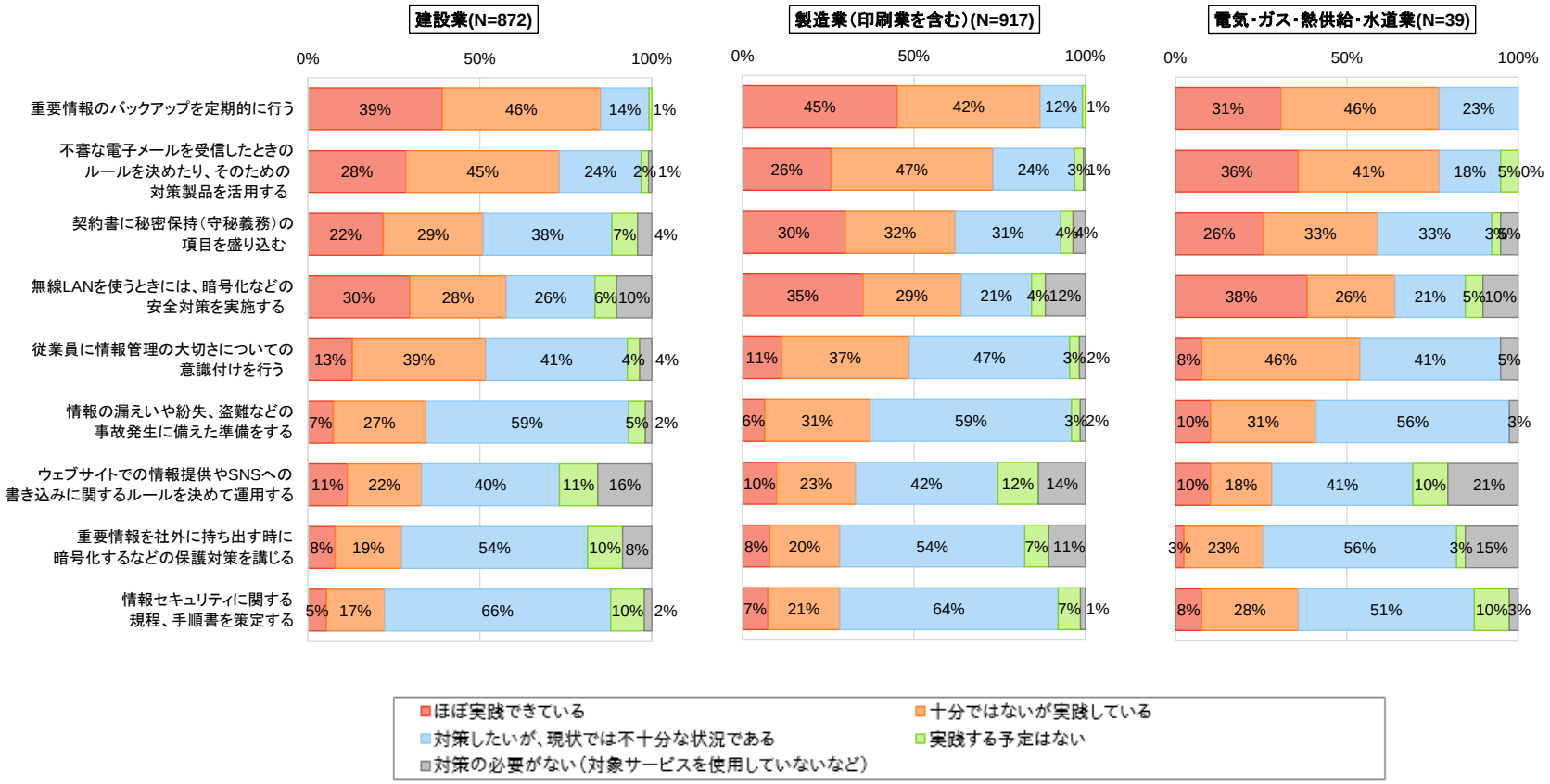

図 3-29　業種別情報セキュリティ対策について貴社の取組み状況③(Q12×Q1)

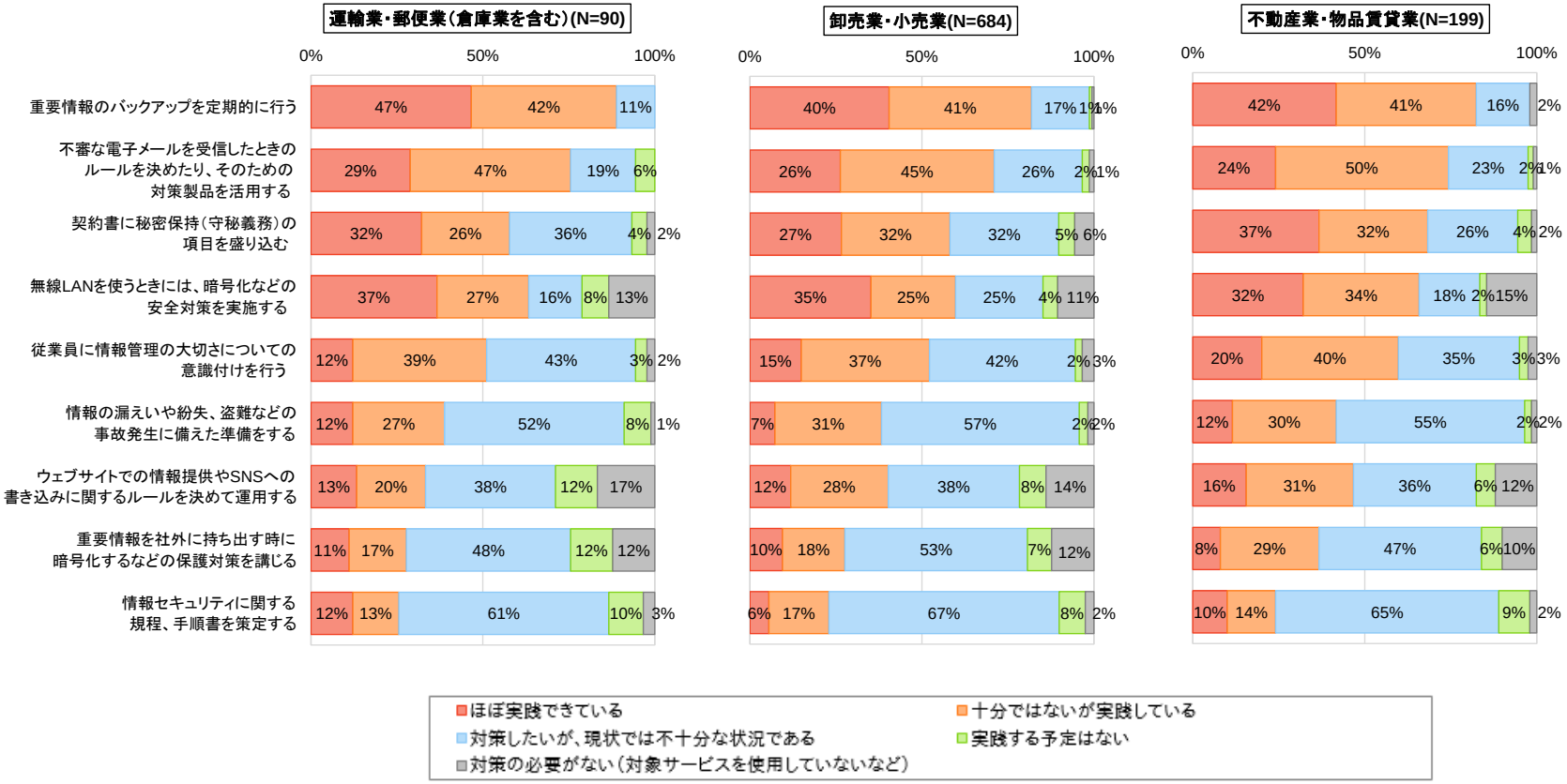

図 3-30　業種別情報セキュリティ対策について貴社の取組み状況④(Q12×Q1)

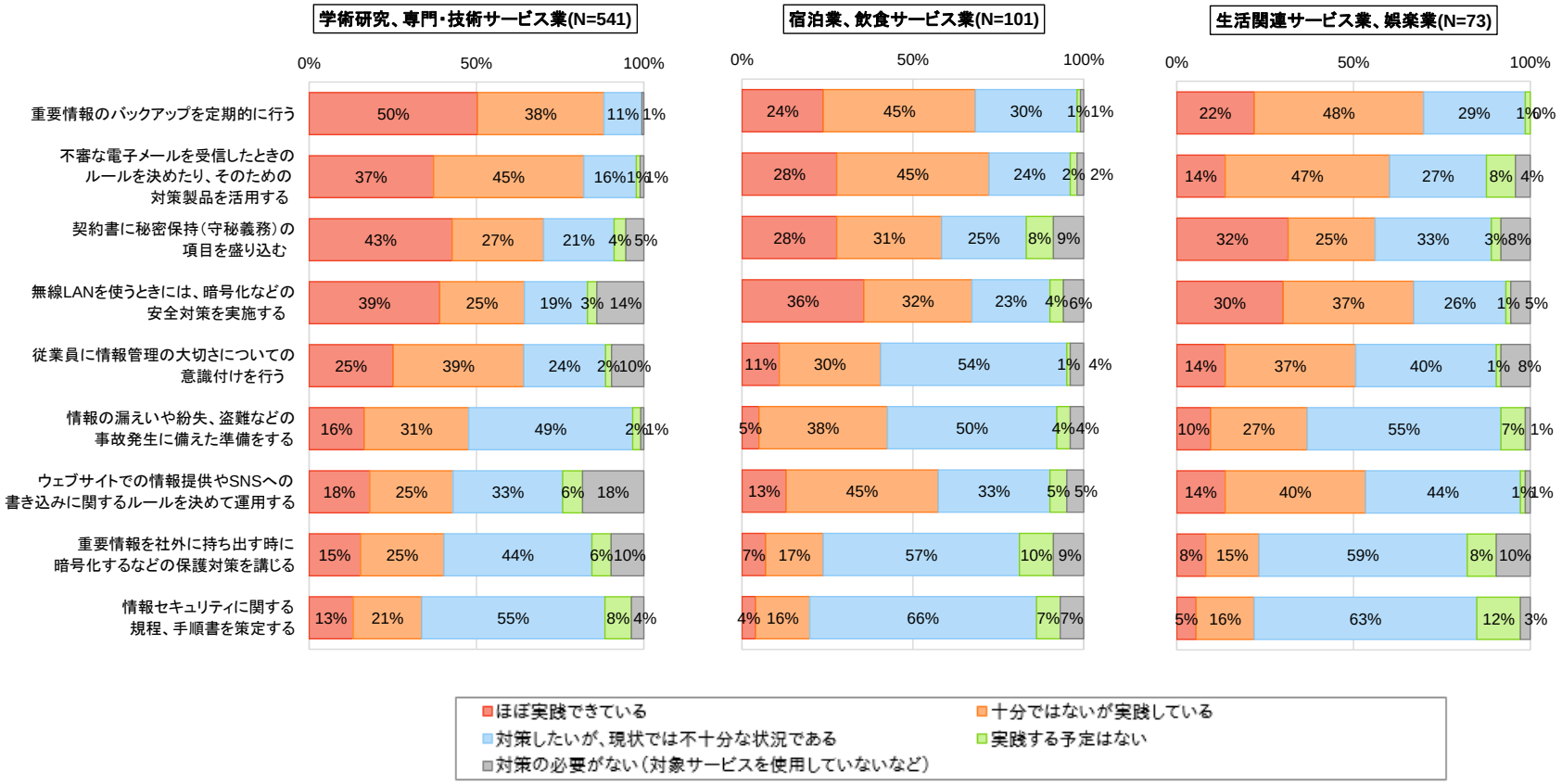

図 3-31　業種別情報セキュリティ対策について貴社の取組み状況⑤(Q12×Q1)

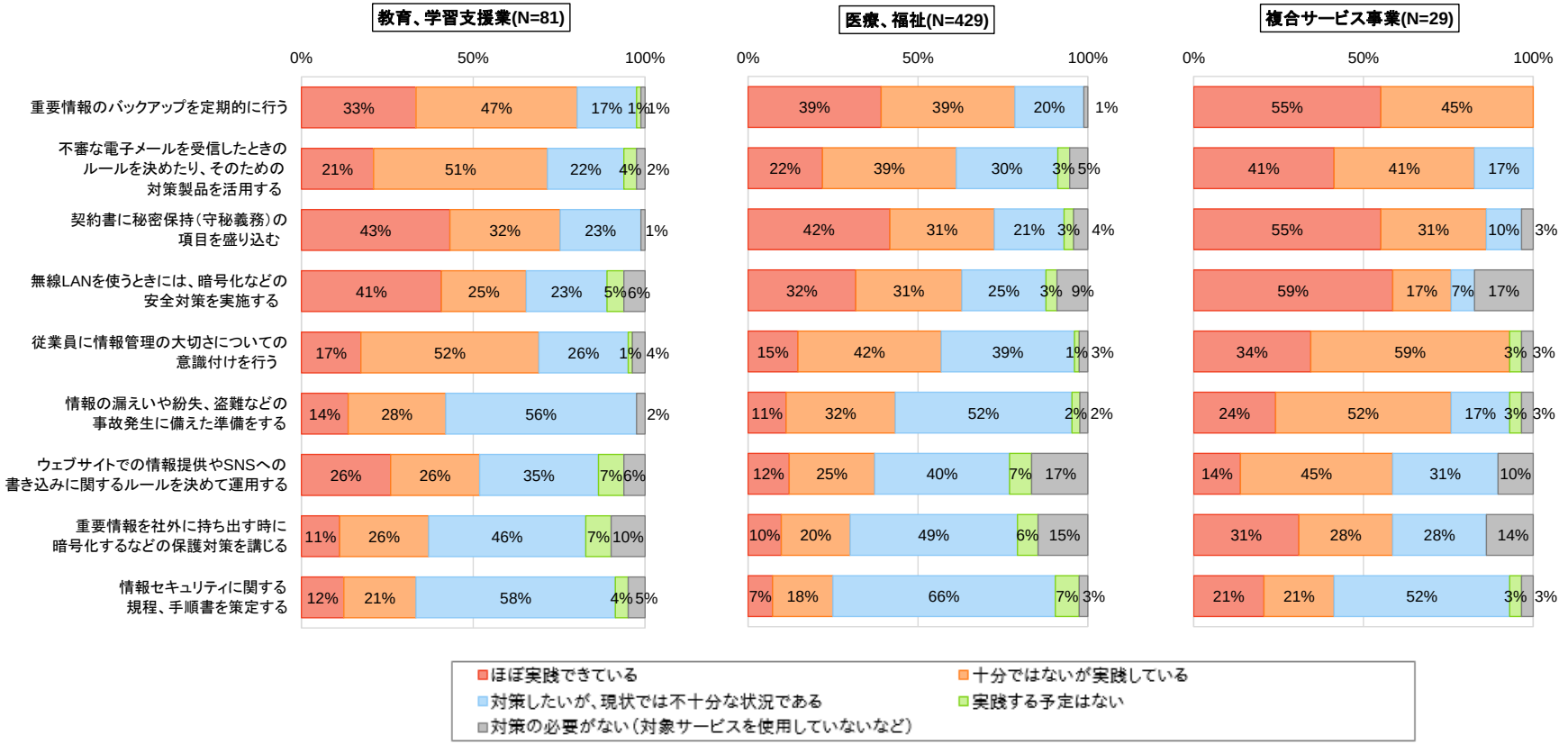

図 3-32　業種別情報セキュリティ対策について貴社の取組み状況⑥(Q12×Q1)

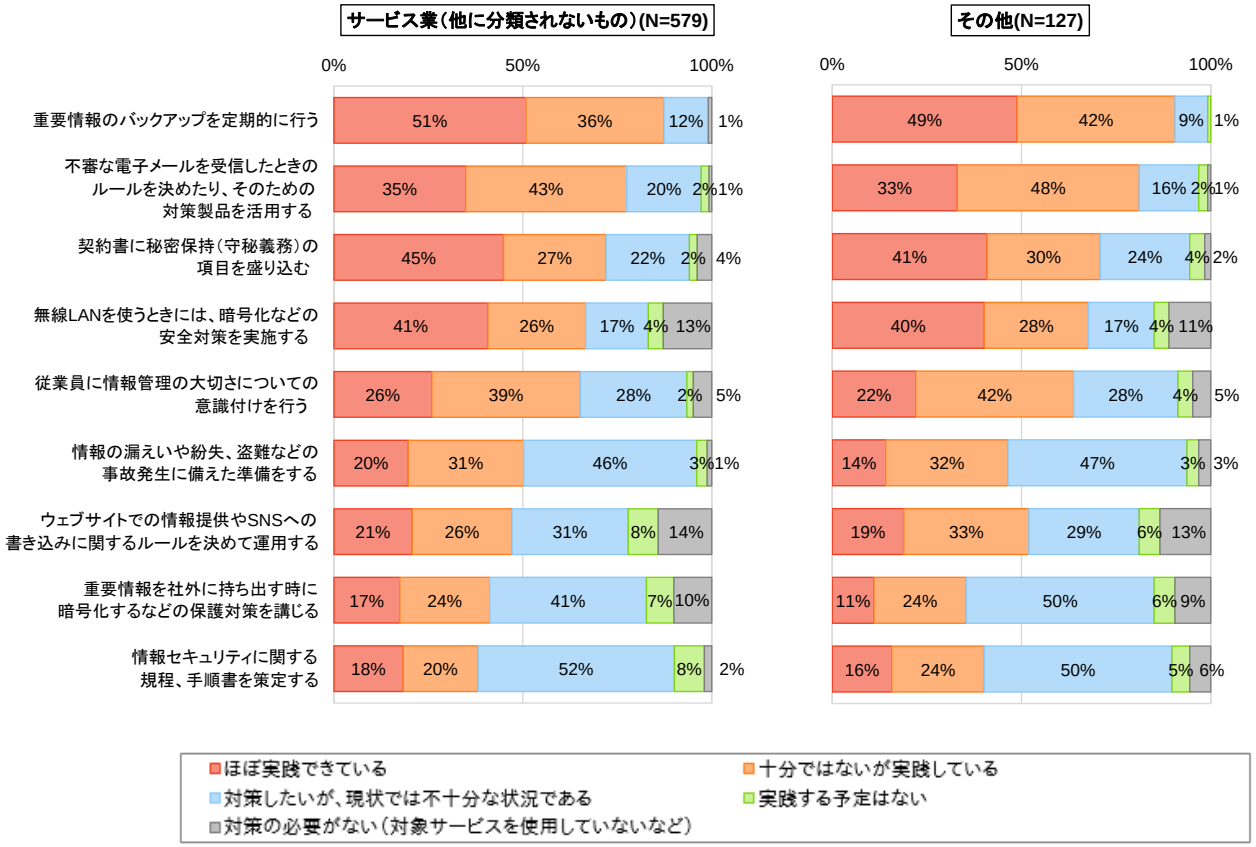

図 3-33　業種別情報セキュリティ対策について貴社の取組み状況⑦(Q12×Q1)

② 総従業員別 「実践できている/十分でないが実践している」を合わせた割合が低い情報セキュリティ対策の取組み状況

3.2.1(12)図 3-12 に示した情報セキュリティ対策の取組み状況（単純集計）において、「ほぼ実践できている」、「十分でないが実践している」を合わせた割合が低い（50%未満）、「情報セキュリティに関する規程、手順書を策定する」、「重要情報を社外に持ち出す時に暗号化するなどの保護対策を講じる」、「ウェブサイトでの情報提供や SNS への書き込みに関するルールを決めて運用する」、「情報漏えいや紛失、盗難などの事故発生に備えた準備をする」の取組み状況を「従業員規模」別にみる。

「情報セキュリティに関する規程、手順書を策定する」は総従業員数の規模に応じて、「ほぼ実践できている」、「十分でないが実践している」を合わせた割合が高くなる傾向があり、「301 名以上」では過半数を超える 56%、「1~20 名」では 3 割以下に止まる。

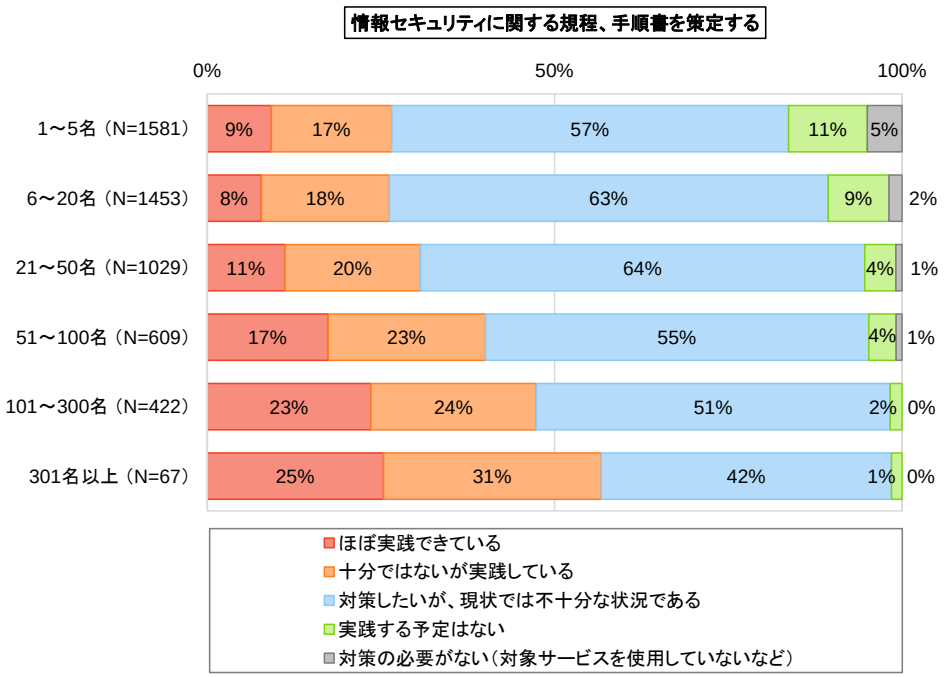

図 3-34 総従業員別 セキュリティ対策について貴社の取組み状況①（Q12×Q2）

「重要情報を社外に持ち出す時に暗号化するなどの保護対策を講じる」については、総従業員数が「6～100 名」の事業者において、「ほぼ実践できている」、「十分でないが実践している」を合わせた割合が、それ以外の総従業員数の事業者に比べやや低い。

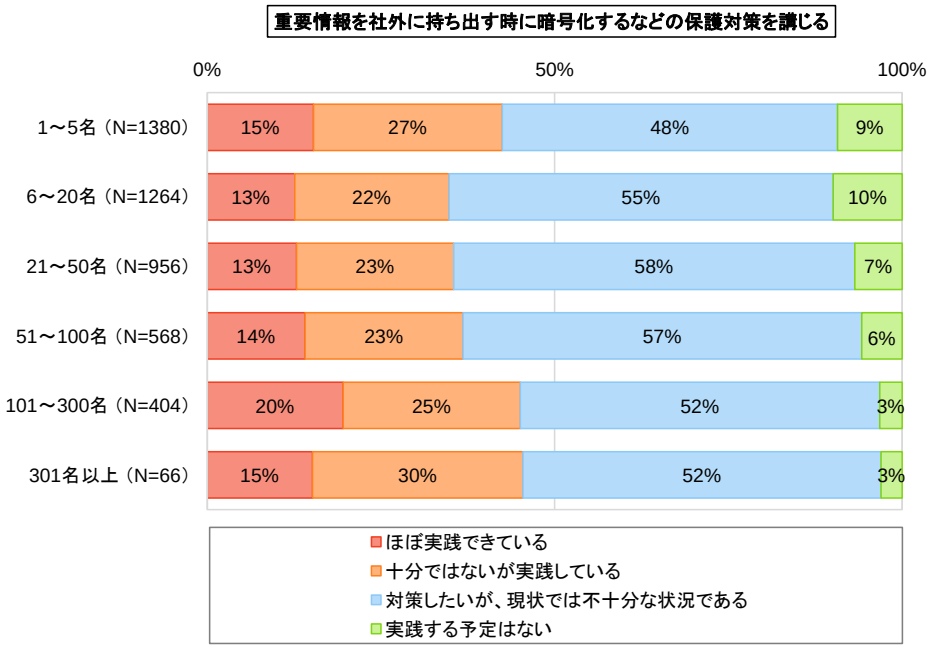

図 3-35　総従業員別 セキュリティ対策について貴社の取組み状況③(Q12×Q2)

（※「対策の必要がない（対象サービスを使用していないなど）」を除いた回答をもとにした割合）

「ウェブサイトでの情報提供や SNS への書き込みに関するルールを決めて運用する」は、「1～5 名」の事業所で「ほぼ実践できている」、「十分でないが実践している」を合わせた割合が高く、それ以外では、総従業員数の規模に応じて「ほぼ実践できている」、「十分でないが実践している」を合わせた割合が増加する傾向がみられる。

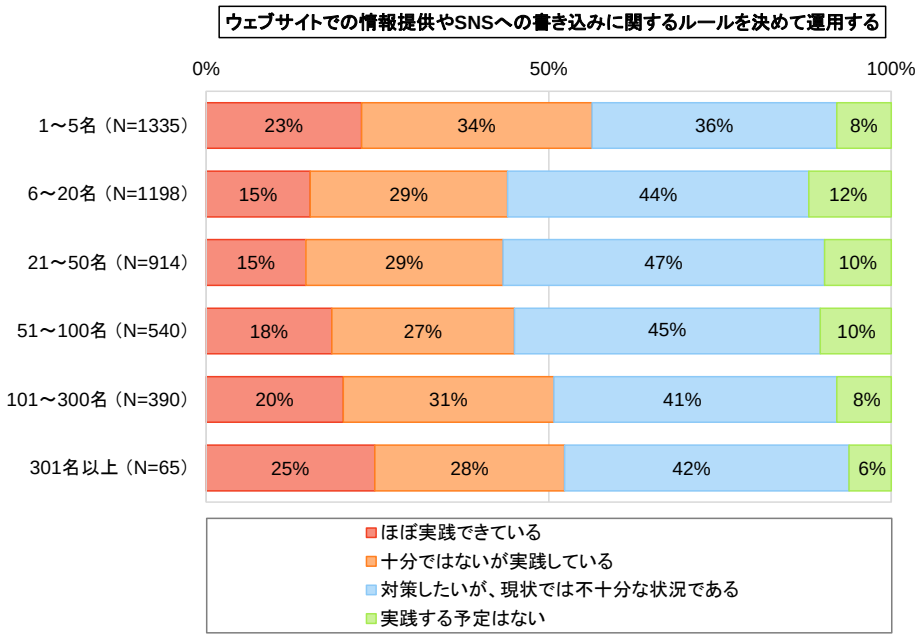

図 3-36　総従業員別 セキュリティ対策について貴社の取組み状況④(Q12×Q2)

（※「対策の必要がない（対象サービスを使用していないなど）」を除いた回答をもとにした割合）

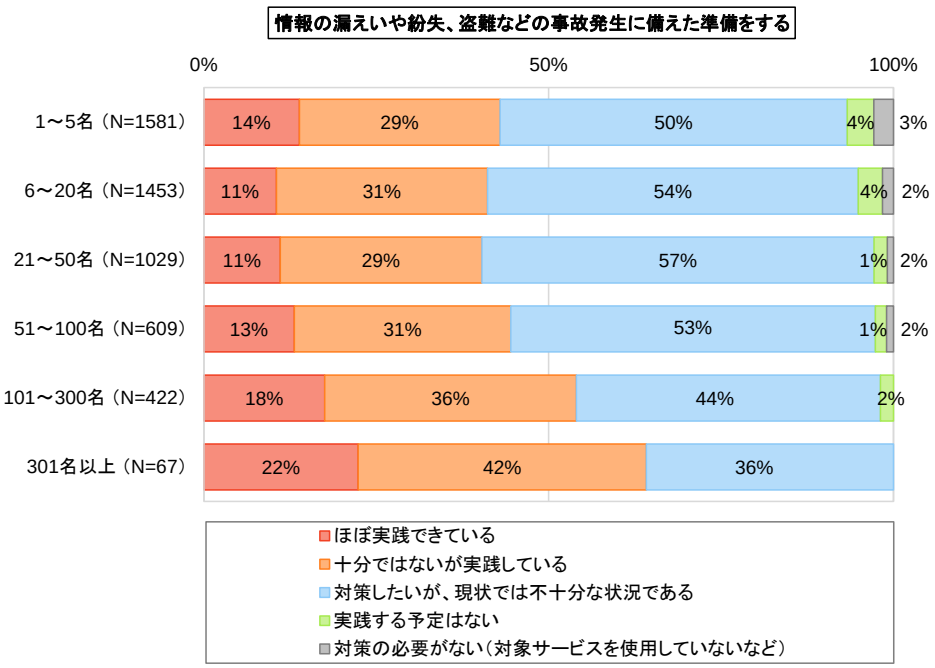

図 3-37　総従業員別 セキュリティ対策について貴社の取組み状況②(Q12×Q2)

(10) 情報セキュリティ対策を進める上での課題点

① 業種別

「情報セキュリティ対策を進める上での課題点」を「業種」別にみると、全体的に「従業員の意識がまだ低い」の割合が最も高いものの、「情報通信業」は、他の業種に比べ、「経営層の意識がまだ低い」、「従業員の意識がまだ低い」、「情報セキュリティ対策の知識をもった従業員がいない」が低い。

表 3-10 業種別 情報セキュリティ対策を進める上での課題点（Q13×Q1）

	従業員の意識がまだ低い	情報セキュリティ対策の知識をもった従業員がいない	業務を行うための人手が足りない状態である	経営層の意識がまだ低い	セキュリティ対策を行うための予算の確保が難しい	情報セキュリティ対策を相談する専門家が回りにいない	これまでに関する情報セキュリティ事故も起きておらず、必要性を感じない	情報セキュリティサービスに関する外部の適切な委託先がみつからない	情報セキュリティ対策製品を扱うサービスベンダや販売店が回りにない	その他
全体（N=5162）	56.6%	42.7%	41.8%	32.4%	30.8%	25.6%	9.7%	7.7%	6.9%	4.6%
農業、林業(N=42)	57.1%	47.6%	50.0%	40.5%	21.4%	31.0%	9.5%	7.1%	7.1%	4.8%
漁業(N=7)	71.4%	42.9%	42.9%	57.1%	14.3%	14.3%	42.9%	－	－	－
鉱業、採石業、砂利採取業(N=4)	75.0%	50.0%	50.0%	50.0%	25.0%	25.0%	25.0%	－	－	－
建設業(N=872)	63.5%	44.3%	40.0%	37.0%	26.6%	24.0%	11.9%	6.0%	6.9%	3.7%
製造業（印刷業を含む）(N=917)	68.6%	48.0%	49.5%	38.5%	31.7%	26.6%	9.8%	4.5%	6.2%	4.4%
電気・ガス・熱供給・水道業(N=39)	66.7%	35.9%	38.5%	38.5%	30.8%	23.1%	10.3%	10.3%	5.1%	2.6%
情報通信業(N=303)	31.7%	14.5%	39.9%	13.2%	37.0%	15.5%	5.0%	24.1%	5.0%	1.7%
運輸業・郵便業（倉庫業を含む）(N=90)	68.9%	45.6%	50.0%	37.8%	24.4%	18.9%	12.2%	4.4%	7.8%	1.1%
卸売業・小売業(N=684)	60.8%	46.8%	43.3%	36.4%	32.7%	25.7%	10.1%	5.1%	8.0%	6.9%
金融業・保険業(N=35)	60.0%	37.1%	28.6%	37.1%	25.7%	34.3%	5.7%	8.6%	2.9%	2.9%
不動産業・物品賃貸業(N=199)	53.3%	43.2%	39.7%	26.6%	23.6%	20.6%	9.0%	8.5%	5.0%	3.5%
学術研究、専門・技術サービス業(N=541)	38.4%	37.9%	38.4%	23.3%	30.3%	28.5%	8.3%	8.9%	7.6%	4.6%
宿泊業、飲食サービス業(N=101)	66.3%	45.5%	56.4%	36.6%	36.6%	28.7%	12.9%	4.0%	10.9%	10.9%
生活関連サービス業、娯楽業(N=73)	58.9%	54.8%	39.7%	27.4%	32.9%	23.3%	15.1%	4.1%	11.0%	2.7%
教育、学習支援業(N=81)	49.4%	37.0%	39.5%	27.2%	42.0%	32.1%	8.6%	11.1%	4.9%	6.2%
医療、福祉(N=429)	65.3%	57.3%	39.6%	32.4%	30.3%	31.5%	10.3%	3.3%	7.9%	5.4%
複合サービス事業(N=29)	44.8%	27.6%	34.5%	24.1%	37.9%	20.7%	20.7%	6.9%	3.4%	6.9%
サービス業（他に分類されないもの）(N=579)	45.8%	35.4%	35.9%	28.5%	32.5%	25.6%	6.7%	11.9%	6.6%	5.4%
公務（他に分類されるものを除く）(N=10)	60.0%	50.0%	50.0%	70.0%	40.0%	20.0%	－	－	－	10.0%
その他(N=127)	46.5%	37.8%	33.1%	37.0%	31.5%	26.0%	10.2%	11.8%	5.5%	3.1%

表中の－は 0.0%を示す

② 総従業員数

「情報セキュリティ対策を進める上での課題点」を「総従業員数」別にみると、従業員規模「1～5 名」では、「情報セキュリティ対策の知識をもった従業員がいない」とする割合が他の課題点に比べて高い。「従業員の意識がまだ低い」とする割合は、「1～5 名」の事業者と比較して、それ以上の総従業員数の事業者が高い。また、「経営層の意識がまだ低い」とする割合は、従業員規模「1～5 名」では、それ以上の総従業員数の事業者と比較して低い。

表 3-11 総従業員数別 情報セキュリティ対策を進める上での課題点（Q13×Q2）（複数回答可）

	従業員の意識がまだ低い	情報セキュリティ対策の知識をもった従業員がいない	業務を行うための人手が足りない状態である	経営層の意識がまだ低い	セキュリティ対策を行うための予算の確保が難しい	情報セキュリティ対策を相談する専門家が回りにいない	これまで情報セキュリティに関する事故も起きておらず、必要性を感じない	情報セキュリティサービスに関する外部の適切な委託先がみつからない	情報セキュリティ対策製品を扱うサービスベンダや販売店が回りにない	その他
全体（N=5162）	56.6%	42.7%	41.8%	32.4%	30.8%	25.6%	9.7%	6.9%	4.7%	1.1%
1～5 名（N=1581）	30.8%	40.4%	33.6%	25.9%	32.1%	28.5%	11.0%	8.0%	6.3%	0.9%
6～20 名（N=1453）	61.8%	46.0%	41.4%	31.9%	29.4%	23.7%	10.8%	7.4%	5.2%	0.8%
21～50 名（N=1029）	70.4%	45.9%	46.6%	36.5%	29.4%	25.9%	8.8%	5.5%	3.1%	1.4%
51～100 名（N=609）	74.9%	41.7%	49.4%	38.3%	33.7%	24.5%	7.2%	6.2%	3.9%	2.1%
101～300 名（N=422）	73.2%	35.5%	48.1%	37.4%	31.0%	21.8%	7.6%	4.7%	1.4%	0.9%
301 名以上（N=67）	73.1%	26.9%	58.2%	47.8%	28.4%	26.9%	1.5%	9.0%	6.0%	1.5%

③　回答者の立場別

「情報セキュリティ対策を進める上での課題点」を「回答者の立場」別にみると、「経営者」は、「従業員の意識がまだ低い」が 49.2%と低く、他と比べて課題認識が低い傾向がある。また、「IT や情報システム、情報セキュリティの担当者」は、「経営者の意識がまだ低い」ことを課題と感じている割合が高い傾向がある。

表 3-12　回答者の立場別 情報セキュリティ対策を進める上での課題点（Q13×Q4）（複数回答可）

	従業員の意識がまだ低い	情報セキュリティ対策の知識をもった従業員がいない	業務を行うための人手が足りない状態である	経営層の意識がまだ低い	セキュリティ対策を行うための予算の確保が難しい	情報セキュリティ対策を相談する専門家が回りにいない	これまで情報セキュリティに関する事故も起きておらず、必要性を感じない	情報セキュリティサービスに関する外部の適切な委託先がみつからない	情報セキュリティ対策製品を扱うサービスベンダや販売店が回りにない	その他
全体	56.6%	42.7%	41.8%	32.4%	30.8%	25.6%	9.7%	6.9%	4.6%	1.1%
経営層が回答 (N=2620)	49.2%	45.6%	39.7%	28.7%	31.0%	27.6%	10.1%	8.2%	5.9%	1.0%
IT や情報システム、情報セキュリティの担当者が回答（兼業含む） (N=1425)	68.1%	36.5%	45.4%	40.4%	34.7%	24.1%	6.9%	5.8%	3.2%	1.4%
経営層と担当者が協議して回答 (N=371)	60.4%	39.6%	41.0%	29.6%	25.3%	23.7%	9.7%	7.3%	4.3%	1.3%
上記のいずれにもあてはまらない (N=746)	58.7%	45.6%	42.4%	31.5%	25.7%	22.0%	13.5%	4.2%	3.1%	0.9%

④　IT への依存度別

「情報セキュリティ対策を進める上での課題点」を「IT 依存度」別にみると「経営層の意識がまだ低い」、「情報セキュリティ対策の知識をもった従業員がいない」は、「事業への影響はほとんどなさそう」を除き、IT 依存度が高い場合に低くなる傾向がある。特に「自社のあらゆる事業が完全に止まってしまう」とする事業者において割合が低いことから、すでに経営者や従業員の意識を高める、知識をもった従業員を配置する取組みを実施していることが伺える。

表 3-13　IT への依存度別 情報セキュリティ対策を進める上での課題点（Q13×Q6）（複数回答可）

	従業員の意識がまだ低い	情報セキュリティ対策の知識をもった従業員がいない	業務を行うための人手が足りない状態である	経営層の意識がまだ低い	セキュリティ対策を行うための予算の確保が難しい	情報セキュリティ対策を相談する専門家が回りにいない	これまで情報セキュリティに関する事故も起きておらず、必要性を感じない	情報セキュリティサービスに関する外部の適切な委託先がみつからない	情報セキュリティ対策製品を扱うサービスベンダや販売店が回りにない	その他
全体(N=5162)	56.6%	42.7%	41.8%	32.4%	30.8%	25.6%	9.7%	6.9%	4.6%	1.1%
事業への影響はほとんどなさそう (N=89)	42.7%	39.3%	15.7%	39.3%	21.3%	21.3%	24.7%	4.5%	3.4%	1.1%
通常より多少は不便だが、7～8 割の事業は実施できそう (N=905)	56.8%	47.2%	36.6%	36.5%	28.8%	25.4%	13.7%	5.0%	4.9%	0.7%
通常の半分くらい程度しかできなくなりそう (N=1386)	61.0%	44.9%	44.9%	36.6%	30.3%	26.1%	9.8%	6.5%	5.1%	0.7%
できる作業もありそうだが、実質的に事業は実施できない (N=2165)	57.6%	42.0%	43.2%	30.3%	31.5%	25.6%	8.0%	7.8%	4.4%	1.2%
自社のあらゆる事業が完全に止まってしまう (N=617)	45.2%	33.9%	40.8%	23.5%	34.2%	25.0%	7.0%	7.6%	4.4%	2.3%

(11) 経営層の情報セキュリティ対策の意識を高める方策

（※Q13 で経営者と回答した方のみ対象(N= 1,673)）

① 総従業員数

「今後、経営層による情報セキュリティ対策に関する意識を高めていくために必要なこと」を「総従業員数」別にみると、「300 名以下」の事業者は、「経営層が率先して情報セキュリティ対策を行うことに対するインセンティブ（補助金等）を設ける」、「被害事例や良事例を提示することで対策の必要性を実感してもらう」の割合が、「301 名以上」の事業者と比較して高く、取組みを進める直接的なメリットや具体例などを求めていると考えられる。一方、「301 名以上」は、「経営層の参加する団体（業界団体、商工会等）を通じて取組みを促す」、「国や関係機関がより積極的に啓発活動を行う」の割合が高く、外部機関による啓発活動等を必要としていることが伺える。

表 3-14 総従業員数別 経営層が情報セキュリティ対策の意識を高めるのに必要と思われること（Q14×Q2）（複数回答可）

	経営層が率先して情報セキュリティ対策を行うことに対するインセンティブ（補助金等）を設ける	被害事例や良事例を提示することで対策の必要性を実感してもらう	国や関係機関がより積極的に啓発活動を行う	経営層の参加する団体（業界団体、商工会等）を通じて取組みを促す	取引銀行や士業関係者（税理士、会計士等）を通じて取組みを促す	取引先（顧客）を通じて取組みを促す	組織として情報セキュリティ対策を行っていることに対する表彰制度を作る	その他
全体 (N=1,673)	24.1%	19.2%	18.5%	18.5%	10.3%	6.6%	1.4%	1.3%
1～5 名 (N=410)	23.9%	19.8%	23.4%	15.9%	9.8%	3.9%	2.0%	1.5%
6～20 名 (N=464)	24.4%	21.6%	17.2%	17.0%	12.5%	5.6%	0.9%	0.9%
21～50 名 (N=376)	22.9%	16.8%	14.4%	22.3%	11.2%	10.4%	1.1%	1.1%
51～100 名 (N=233)	29.6%	18.9%	18.0%	14.6%	6.4%	8.6%	1.7%	2.1%
101～300 名 (N=158)	21.5%	19.0%	19.0%	23.4%	8.9%	5.7%	1.9%	0.6%
301 名以上 (N=32)	12.5%	12.5%	25.0%	31.3%	9.4%	3.1%	3.1%	3.1%

② 回答者の立場別

「今後、経営層による情報セキュリティ対策に関する意識を高めていくために必要なこと」を「回答者の立場」別にみると、「経営層」は、「被害事例や良事例を提示することで対策の必要性を実感してもらう」、「経営層が率先して情報セキュリティ対策を行うことに対するインセンティブ（補助金等）を設ける」の割合が高く、「IT や情報システム、情報セキュリティの担当者が回答（兼業含む）」は、「経営層が率先して情報セキュリティ対策を行うことに対するインセンティブ（補助金等）を設ける」が最も高い割合となっている。

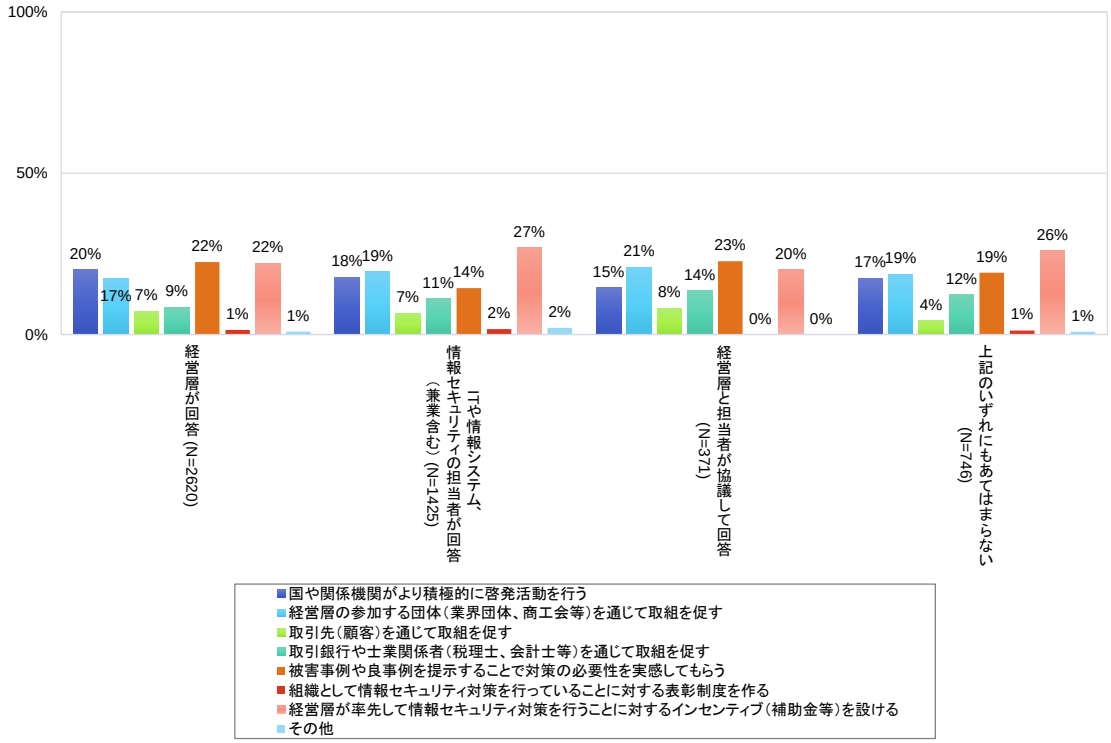

図 3-38 回答者の立場別 経営層が情報セキュリティ対策の意識を高めるのに必要と思われること（Q14×Q4）（複数回答可）

(12) 今後注力していきたい情報セキュリティ関連の取組み

① 総従業員数別

「今後注力していきたい情報セキュリティ関連の取組み」を「総従業員数」別にみると、「1～5 名」は「従業員への情報セキュリティ教育」の割合が低い。一方、「301 名以上」は、全般的に割合が高く、特に「情報セキュリティマネジメントシステム（ISMS）などの国際基準に基づく情報セキュリティ対策のための体制整備と認証の取得」、「IT 関連の緊急事態（インシデント）のときの対応組織（CSIRT）の設置・強化」の割合が、総従業員数が「300 名以下」と比較して高い。

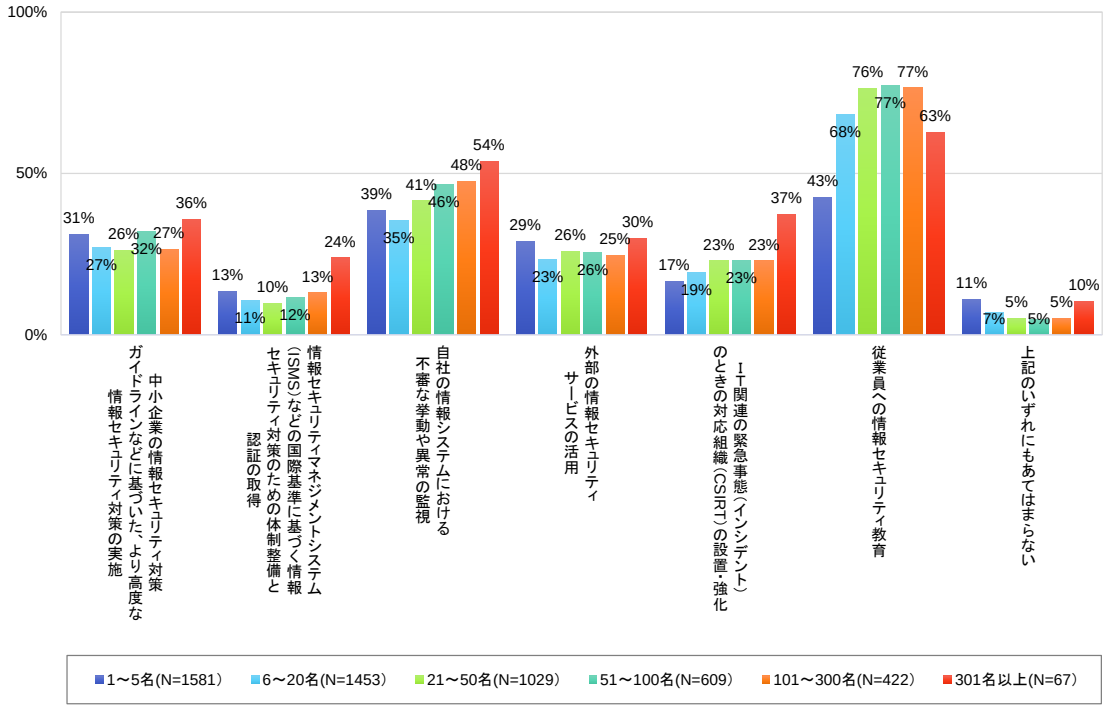

図 3-39 総従業員数別 今後注力していきたい情報セキュリティ関連の取組み
（Q16×Q2）（複数回答可）

② 取組み目標別

「今後注力していきたい情報セキュリティ関連の取組み」を「取組み目標」別にみると、いずれも「従業員への情報セキュリティ教育」が高いが、二つ星宣言事業者は、「情報セキュリティマネジメントシステム（ISMS）などの国際基準に基づく情報セキュリティ対策のための体制整備と認証の取得」の割合が高く、より高度な情報セキュリティ対策を実施することを目指していることが伺える。

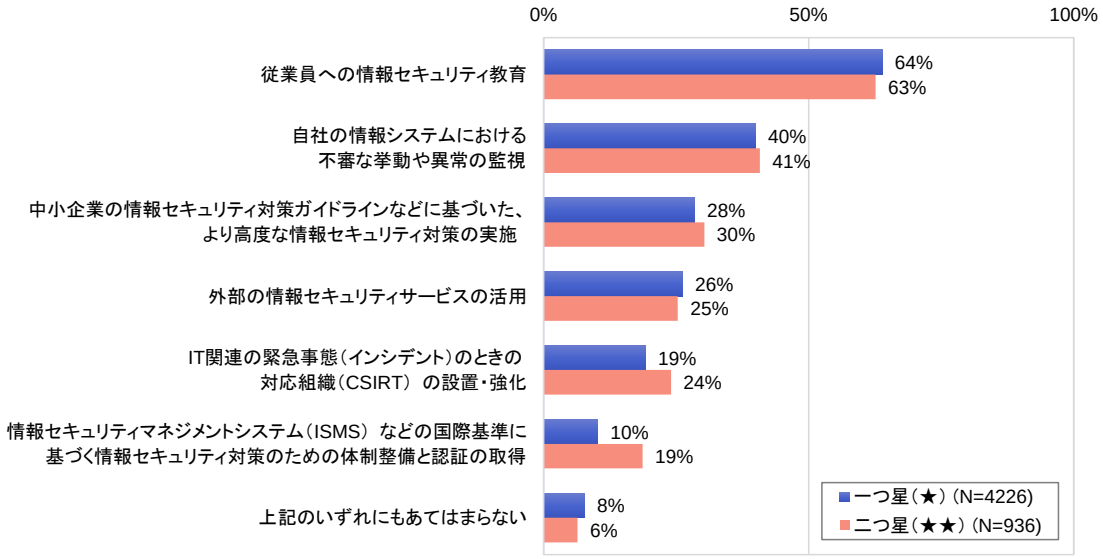

図 3-40 取組み目標別 今後注力していきたい情報セキュリティ関連の取組み（Q16×Q3）

③　回答者の立場別

「今後注力していきたい情報セキュリティ関連の取組み」を「回答者の立場」別にみると、「経営層」が回答した場合、「従業員への情報セキュリティ教育」の割合が低い他、「IT や情報システム、情報セキュリティの担当者」が回答した場合と比較して、「IT 関連の緊急事態（インシデント）のときの対応組織（CSIRT）の設置・強化」の割合が低い。また、「経営層」が回答の場合、「外部の情報セキュリティサービスの活用」の割合が他の「回答者の立場」と比較してやや高い。

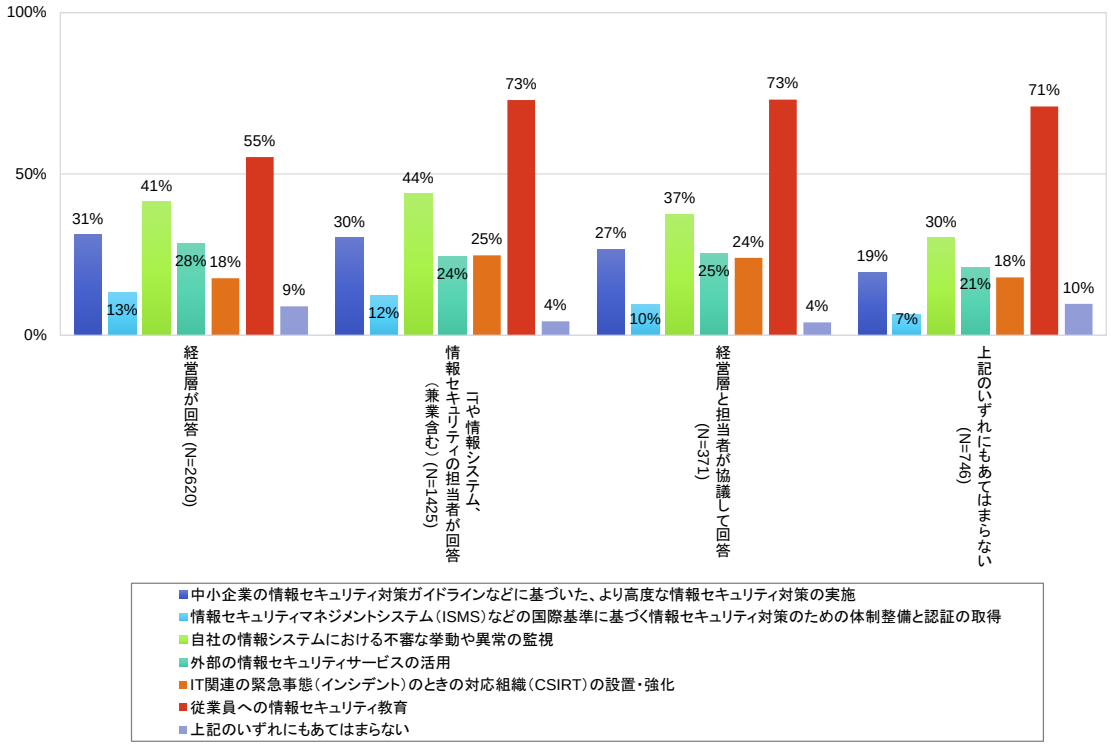

図 3-41　回答者の立場別 今後注力していきたい情報セキュリティ関連の取組み（Q16×Q4）

4. SECURITY ACTION 制度の取組みに関する訪問調査

前章のアンケート調査結果を踏まえ、より具体的な情報を得ることを目的に訪問調査を実施した。その結果、SECURITY ACTION 制度に取組むことで得られる成果やメリット、対策の工夫点等について収集した情報をもとに別添の事例集として取り纏めた。訪問調査の概要を 4.1 に、訪問調査結果を 4.2、分析結果を 4.3 に、訪問調査で得られた取組み事例の構成を 4.4 に報告する。

4.1. 訪問調査概要

訪問調査は、2019 年 1 月から 2019 年 2 月まで実施し、21 件訪問した。表 4-1 に訪問調査の実施概要を示す。

表 4-1 訪問調査の実施概要

項目	内容
実施対象	SECURITY ACTION 自己宣言事業者 （前述のアンケート回答にて訪問調査を許諾した事業者）
実施期間	2019 年 1 月～2019 年 2 月
訪問数	21 件

訪問調査では、アンケート調査結果を基に、ヒアリングを通じてさらに詳細な対策内容や課題等を確認した。主な確認項目を表 4-2 に示す。

表 4-2 訪問調査における主な確認項目

内容
1. 情報セキュリティ対策を検討したきっかけ 2. 情報セキュリティ対策の実践による効果 3. 継続的な対策のための工夫点 4. 情報セキュリティ対策に関する体制構築等の工夫点 5. 情報セキュリティ対策の課題 6. SECURITY ACTION 自己宣言の手順

4.2. 訪問調査結果及び分析

訪問調査結果及び分析結果を報告する。訪問企業の属性を 4.2.1 に、各社の取組み状況、情報セキュリティ対策を検討したきっかけや効果及び継続的な取組みへの意識などを 4.2.2 に報告する。なお、訪問調査結果及び分析に関しては、訪問調査先のうち分析に有効であると考えられる 18 事業者を対象に整理した。

4.2.1. 訪問事業者の属性

訪問調査の実施にあたっては、SECURITY ACTION 自己宣言事業者の地域、業種、従業員規模、SECURITY ACTION 制度の取組み段階（星の数）を考慮し、偏りや事例の重複等が極力生じないようにアンケート調査回答企業からサンプリングし、実施した。訪問事業者の属性を以下に示す。

表 4-3 訪問企業の属性

属性項目	内訳	訪問企業数
取組み段階	一つ星	10
	二つ星	8
従業員規模	1～5 名	2
	6～20 名	5
	21～50 名	8
	51～100 名	2
	101～300 名	1
	301 名以上	0
業務の IT 依存度	1.事業への影響はほとんどなさそう	0
	2.常より多少は不便だが、7～8 割の事業は実施できそう	3
	3.通常の半分くらい程度しかできなくなりそう	2
	4.できる作業もありそうだが、実質的に事業は実施できない	11
	5.自社のあらゆる事業が完全に止まってしまう	2
地域	東北地方	3
	関東地方	3
	中部地方	2
	近畿地方	4
	中国・四国地方	3
	九州地方	3
業種 業種に関しては、複数の内訳に該当する企業あり	製造業（印刷業を含む）	4
	学術研究、専門・技術サービス業	3
	情報通信業	1
	建設業	3
	医療、福祉	2
	不動産業・物品賃貸業	1
	卸売業・小売業	2
	農林水産業	1
	サービス業（他に分類されないもの）	2

4.2.2. 訪問調査結果

訪問調査によって確認した各事業者の情報セキュリティ対策への取組みのきっかけ、効果、工夫点、課題について報告する。

なお、訪問調査結果は、各事業者の取組み事例としてまとめた。具体的な内容は、別添の事例集を参照されたい。

(1) 情報セキュリティ対策を検討したきっかけ

情報セキュリティ対策を検討したきっかけは、「技術情報や個人情報保護のための対策実施」「組織的な対策の実施・対策状況の確認」「取組み姿勢のアピール」「顧客などとの関係性強化」を目的とした事例がある。その他には、SECURITY ACTION による顧客の情報セキュリティ意識の向上、ISMS 認証の更新準備（ポリシー見直し）で活用などの事例がある。

表 4-4 情報セキュリティ対策を検討したきっかけ

１．技術情報や個人情報保護のための対策実施
• 機密情報（製造図面など）の外部漏えい対策
• 園児などの情報を扱うクラウドサービス利用のための情報セキュリティ対策
• 従業員に対して個人情報保護の漏えいリスクを理解してもらうため
２．組織的な対策の実施・対策状況の確認
• 組織として必要な情報セキュリティ対策の実施
• 従業員のセキュリティ教育の実施
• 自社の情報セキュリティ対策の状況確認
３．取組み姿勢のアピール
• 機密情報を預かるサービス事業者として情報セキュリティ対策をアピール
• 情報セキュリティに対する姿勢の対外的アピール
４．顧客などとの関係性強化
• 取引先から情報セキュリティ対策状況を確認されるため
• 取引先などから勧められたため
５．その他
• 顧客の情報セキュリティ意識の向上
• ISMS 認証更新準備にガイドラインを活用

(2) 情報セキュリティ対策の実践による効果

「顧客からの評価」、「対外的なアピールによる意識向上・対策継続」などの対外的な効果や、従業員のセキュリティ意識が高まったことで「組織的な情報セキュリティリスクの低減」につながったと評価している事例がある。その他には、「情報セキュリティ関連の事業化」、「ISMS 認証取得への寄与」などの事例がある。

表 4-5　情報セキュリティ対策の実践による効果

１．顧客からの評価
- セキュリティ対策状況を重視する顧客から、自社の情報セキュリティ対策の取組みが高く評価された
- 情報セキュリティ対策（守り）を PR することで顧客からの信頼を獲得し、受注拡大に貢献

２．対外的なアピールによる従業員の意識向上・継続的な対策の気運醸成
- 名刺に SECURITY ACTION のロゴマークを掲載。制度や自らの情報セキュリティ対策の説明を行うようになったことで社員の意識が向上
- 対外的に宣言したことによる継続した対策へのモチベーション向上

３．組織的な情報セキュリティリスクの低減
- 情報セキュリティ対策に関する経営者の認識不足への気づき
- 全社員がセキュリティ対策（OS やソフトウェアの更新など）の重要性を認識
- 不用意にメールを開かないなど従業員のセキュリティ意識が向上
- ID／パスワードの管理の徹底、アクセス制限の仕組みの構築

４．その他
- 資産管理台帳や情報セキュリティポリシーの更新・見直しによる内容の充実化
- セミナーや研修会の開催による情報セキュリティ関連の事業化
- 情報セキュリティマネジメントシステム（ISMS）認証取得への寄与

(3) 継続的な対策のための工夫点

「情報収集・周知」などによる定期的な意識付け、「社内ルール・規定の策定」「情報セキュリティ教育の実施」により継続的な対策に取組む事例が多い。また、日常業務の効率化や声をかけやすい雰囲気作りによって継続的な対策に努めている事例がある。

表 4-6　継続的な対策の工夫点

１．情報収集・周知
- 定例会議などで繰り返しテーマに取上げ、関心を持ちそうな身近な情報セキュリティ事例を紹介することで効果的に注意喚起
- 各機関から発信される情報セキュリティ関連情報による注意喚起などを定期的に周知することで継続的な意識付けを図る
- 「情報セキュリティ５か条」のポスターを掲示して従業員の意識付けを図る
- セキュリティに関する従業員の困りごとなどを積極的にヒアリング

２．社内ルール・規定の策定
- 情報セキュリティ関連の情報や留意すべき社内ルールなどの周知徹底
- 業務やセキュリティ対策状況などの会社の実態に合った情報セキュリティハンドブックを作成することで、従業員への浸透を図る
- 作成した情報セキュリティ関連規定を社員教育等で活用することで、社内規定の形骸化を防ぐ

３．情報セキュリティ教育の実施
- IPA の「情報セキュリティマネジメント」試験の推奨や情報セキュリティ対策コンテンツを学習し、従業員のスキルアップを図る

４．業務の効率化
- 経営や業務との兼ね合いを踏まえ、無理のない範囲で時間・費用などのリソースを確保し、できることから対策を実践
- 従業員の業務効率の向上と必要な情報セキュリティ水準の確保を両立させる環境を整えていく

５．その他
- IT に苦手意識をもつ従業員に対し、わからないことがある場合に、気軽に声をかけやすい雰囲気作りを進める
- 失敗から学び、対策につなげていくような仕組み（予防的にできるテストなど）を検討

(4) 情報セキュリティ対策に関する体制構築等の工夫点

情報セキュリティ対策の体制構築や環境整備を進めるための工夫点を以下に示す。

SECURITY ACTION の取組み段階別にみると、一つ星では「少人数、管理者不在時にも情報セキュリティ水準を確保する取組み」や「サポート環境の整備」などの事例がある。二つ星では、「情報セキュリティ対策の体制強化」、従業員の「情報セキュリティ教育の理解度チェック」などを実施している事例がある。

表 4-7　情報セキュリティ対策に関する体制構築等の工夫点

■ 一つ星

少人数、管理者不在時にも情報セキュリティ水準を確保する取組み

- 少人数で管理・運用するためパソコンの使用場所、USB 不使用など利用方法の制限
- 管理者不在時の遠隔操作ソフトによる情報セキュリティ対策の支援
- 情報セキュリティサービス利用による情報セキュリティ対策に関する人手不足への対応

サポート環境の整備

- 経営者自らが情報セキュリティ対策を推進しつつも、相談しやすい環境を整える

対策の定着化に向けた取組み

- 独自のハンドブックに「情報セキュリティ５か条」を追加

■ 二つ星

情報セキュリティ対策の体制強化

- 部門ごとに情報セキュリティの責任者を配置。協力会社などの情報セキュリティ教育を担当

情報セキュリティ教育の理解度チェック

- 「５分でできる！自己診断」のチェックシートを活用し、従業員向けに理解度テストを実施

⑸ 情報セキュリティ対策の課題

① 宣言前

SECURITY ACTION 自己宣言前の課題については以下に示すとおりであり、「情報セキュリティ対策の具体的な実践方法」や「従業員への情報セキュリティ教育の継続」などを課題と感じている。

表 4-8　情報セキュリティ対策の課題（宣言前）

■ 一つ星
- どのような情報セキュリティ対策を実施すべきかわからない
- 最低限必要な情報セキュリティ対策の実施／実施状況の確認
- 情報セキュリティポリシーの作成
- 従業員への情報セキュリティ教育の継続的な実施

■ 二つ星
- 情報セキュリティ対策の実施／実施状況の確認
- 従業員への情報セキュリティ教育の継続的な実施

② 宣言後

SECURITY ACTION 自己宣言後の課題については以下に示すとおりであり、宣言前と比較すると情報セキュリティ対策の水準が向上し、より高度な取組みを志向するようになっていることが伺える。

表 4-9　情報セキュリティ対策の課題（宣言後）

■ 一つ星
- 「情報セキュリティ５か条」で求められる対策の徹底／定着／定期的な見直し
- 「５分でできる！情報セキュリティ自社診断」による自社のセキュリティ対策状況の確認と必要な対策の実施

■ 二つ星
- セキュリティ管理体制の高度化
- セキュリティ人材の育成、従業員のスキルアップ
- 取引先からの信頼向上

③　SECURITY ACTION 制度に関する課題

SECURITY ACTION 制度では、まずは一つ星からはじめて段階的に二つ星へステップアップすることや、ロゴマークによる対外的なアピールなどの取組みを中小企業等に対して期待している。これらの状況について訪問調査時に確認した結果を以下に示す。

なお、既に取り組んでいる対策から実質的に二つ星を宣言することが可能な事業者が、あえて一つ星を宣言している事例があった。こうした事業者は、二つ星を宣言しない理由として、「二つ星を宣言するメリットが見出せなかった」結果、一つ星を宣言したという意見があった。また、二つ星の宣言では「情報セキュリティポリシーの作成」として「基本方針」の作成を求められているところ、「関連規定や手順書」の作成が必要であると誤解したため、宣言が難しいと感じている企業があった。

表 4-10　SECURITY ACTION 制度に関する課題

■　一つ星から二つ星へのステップアップに関する課題
- 情報セキュリティポリシーの作成
- 二つ星宣言を行なうメリットが見出せない
- 最低限の対策を実施するだけで十分
- 最低限の対策が定着した後に検討する
- 制度の認知度や知名度の状況を踏まえ、今後二つ星を目指したい

■　対外的なアピールに関する課題
- 外部へ宣言することのメリットが見出せない
- 自社の取組みは最低限の対策だが、SECURITY ACTION 制度の知名度を踏まえ、自社の取組みをアピールしていきたい

(6) SECURITY ACTION 自己宣言の手順に関する事例

SECURITY ACTION 自己宣言の具体的な手順を報告する。図 4-1 には、一般的な宣言の手順を示す。宣言の手順は、一つ星、二つ星ともに自社の対策状況をチェックし、宣言する。また、宣言後にはステップアップや見直しを行う。

本節では、訪問調査で確認された特徴的な事例について説明する。

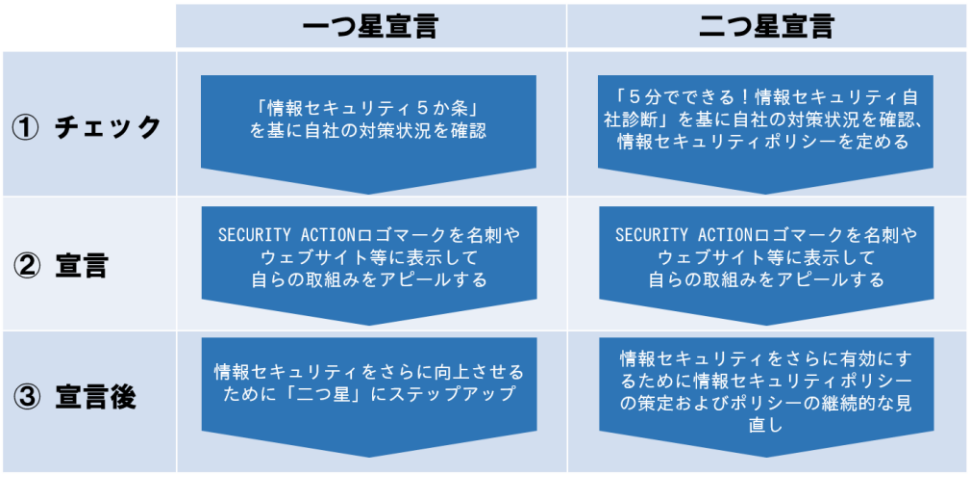

図 4-1　宣言の手順（左：一つ星、右：二つ星）

■　情報セキュリティ対策ハンドブックの作成

以下の事例では、自社の情報セキュリティ対策を組織的に理解し、従業員への意識付けを徹底するため、具体的な業務に照らし合わせた解説をハンドブックとして作成している。

表 4-7　一つ星手順事例 1（ハンドブック作成）

手順	具体的な内容
1	情報セキュリティ対策ハンドブックを作成するため、1 週間程度で、「情報セキュリティ 5 か条」に沿って、現時点でできていることと不十分なことを整理した。
2	社員が最低限守るべきルールをハンドブックにまとめ、社長の承認を得て宣言を実施した。
3	社員がハンドブックの内容をきちんと理解し、しっかり定着させることが重要課題。無理をせずに最低限から始めて、次のステップとして「二つ星」を目指す。

■　社内の対策状況を確認後に強化すべきポイントを整理

以下の事例では、サーバーやソフトウェア等のシステム導入に合わせ安心して利用できる環境を整備するため、「情報セキュリティ５か条」を活用して強化すべきポイントを整理している。

表 4-8　一つ星手順事例 2（強化すべきポイントの整理）

手順	具体的な内容
1	「情報セキュリティ５か条」により、社内の実施状況を確認。新たにサーバーとソフトウェアを導入する計画があり、安心して使える環境を整備するため、強化すべきポイントを整理。
2	チェックの結果を社長に報告し、SECURITY ACTION 宣言を行うことへの承認をもらう。
3	新たにサーバーとソフトウェアを導入する計画があり、安心して使える環境を整備するため、基本的対策の徹底・浸透を図る。

■　サポート人員による情報セキュリティ対策の確認

サポート人員（自社社員及び代理店をサポートする人員等）が情報セキュリティ対策の実施状況を確認した事例である。関係者に対して専門用語を使わずに情報セキュリティを説明する資料として「情報セキュリティ 5 か条」を有効利用している。

表 4-9　一つ星手順事例 3（サポート人員によるチェック）

手順	具体的な内容
1	「情報セキュリティ 5 か条」の取組みについて、サポート人員が実業務に照らし合わせて実施の有無をチェックし、結果を管理者へ報告
2	管理者が「情報セキュリティ 5 か条」をもとに、経営者に対して自己宣言の目的や一つ星の取組み内容等を説明し、了承を得て宣言を実施。
3	「5 分でできる！情報セキュリティ自社診断」などで、自社のセキュリティ状況を確認し、必要な対策を検討。従業員のセキュリティ意識の度合いについても確認。

■　社員による情報セキュリティ対策の確認

自社の対策の実施状況を確認する際に、経営者や情報セキュリティ担当者のみならず一般社員にも確認した事例である。一般社員に確認させることで、自社の情報セキュリティ対策の実施状況に対する理解度や、情報セキュリティ教育の有効性を確認している。

表 4-10　二つ星手順事例 1（社員によるチェック）

手順	具体的な内容
1	「5 分でできる！情報セキュリティ自社診断」の 25 項目のチェックを情報セキュリティ担当者ではなく、一般社員が回答することによって、社内の状況を把握した。
2	「中小企業の情報セキュリティ対策ガイドライン」を活用し、これまで見直しができていなかったセキュリティポリシー等を改善し、宣言を実施。
3	取引先からの信頼性向上と社会的責務を果たすことが最重要課題。今後も IPA が提供する対策ツールや資料などを有効活用し、継続的に情報セキュリティ対策に取組んでいく。

■　社内ルールや秘密保持契約の策定

以下の事例では、手順 1 のチェック時にセキュリティポリシーを策定した後、より強固なセキュリティ管理体制を推進するために、必要な社内ルールや秘密保持契約などの策定を検討している。

表 4-11　二つ星手順事例 2（宣言後により強固な体制を検討）

手順	具体的な内容
1	セキュリティポリシーを策定するため、他社のポリシーを確認したり、必要な情報収集を行ったが、その一連のプロセスが非常に勉強になった。
2	宣言を行うことを社員へ周知徹底。セキュリティの重要性の再確認と、顧客への説明責任を果たすよう意識の向上を図った。
3	自社の業務に則した秘密保持契約や、社内ルールの規定化を検討し、より強固なセキュリティ管理体制を推進する。

4.3.　訪問調査結果の分析

訪問調査結果の分析として、SECURITY ACTION 宣言の取組みに関する“他事業者への適用可能性”を 4.3.1 に、“二つ星へのステップアップに向けた課題”を 4.3.2 に示す。

4.3.1.　他事業者への適用可能性

SECURITY ACTION 宣言の取組みの中で、他の事業者でも参考・適用し得る考え方や取組みについてを以下に示す。

(1) 最低限対策すべき情報セキュリティ対策

IPA が実施した「2016 年度中小企業における情報セキュリティ対策の実態調査」では、中小企業における情報セキュリティ対策の主な課題として、「費用対効果が見えない」、「どこからどう始めたらよいかわからない」といった意見があった。一方、今回、訪問調査した一つ星を宣言した事業者は、最低限満たすべき情報セキュリティ対策として「情報セキュリティ５か条」を利用することで、対策の検討に有用である、理解しやすいなど、有用性を評価する意見が多い。このため、情報セキュリティ対策で何からはじめたらよいかわからないという中小企業等に対し、「情報セキュリティ５か条」を紹介することで一つ星の取組みが進むことが期待できる。

(2) 取引先等からの信頼性向上を意識した取組み

二つ星を宣言した事業者では、自らの情報セキュリティ対策に取組む姿勢を情報セキュリティ基本方針として公開することで、取引先や関係者との信頼関係の構築に役立てることを意識した事例があった。取引先からの信頼性向上など、情報セキュリティ対策や取組み姿勢を見える化することで得られるメリットを示すことで、他の事業者や一つ星宣言事業者の参考となり、二つ星の取組みが促進されることが期待できる。

(3) 一つ星及び二つ星に共通で参考となる取組み

一つ星、二つ星の共通した取組みとして、SECURITY ACTION のロゴマークを名刺やホームページに掲載し、自社の取組みを示すことで信頼を得るための一助となる。また、取組みの内容を説明することを通じ、社員や取引先の意識向上につながるメリットがあると考えられる。

4.3.2. 二つ星へのステップアップに向けた課題

SECURITY ACTION 制度は 2 段階の取組み段階を用意しており、一つ星から始めた中小企業等は、情報セキュリティへの取組みをさらに強化するために二つ星にステップアップすることを呼びかけている。しかしながら、一つ星を宣言した事業者の中には情報セキュリティポリシーの作成に課題があるため、二つ星を宣言することが難しいといった意見があったが、二つ星では基本方針の策定までを求めており、誤解を招いていることもステップアップに向けた障壁の 1 つであることがわかった。二つ星へのステップアップを促進するためにも、制度のわかりやすさや認知度の向上が引き続き重要である。

4.4.　取組み事例について

訪問調査の結果を取り纏め、SECURITY ACTION 制度に取組むことで得られる成果やメリット、対策の工夫点等を示した取組み事例を作成した。以下には、作成した取組み事例の構成を示す。具体的な事例の内容については別添の事例集に示す。

図 4-2　取組み事例の構成

① 事業者（企業）属性の紹介

表 4-3 に示した地域、SECURITY ACTION の取組み段階（宣言のタイプ）、業種、従業員規模及び業務の IT 依存度の情報に加え、取組みの概要、事業者名を記載している。なお、匿名希望の場合は、事業者名と A 社等と記載している。

② 取組み内容の紹介

SECURITY ACTION 自己宣言及び情報セキュリティ対策を検討したきっかけ、取組みによって得られた効果や取組みを推進する上で工夫している内容について記載している。

③ 事業者（企業等）紹介

事業者（企業等）の事業概要を記載している。

④ 経営者・実施者のコメントの紹介

SECURITY ACTION や情報セキュリティ対策に取組む上での考え方や今後の課題等についての経営者や実施者のコメントを記載している。なお、経営者と実施者両方のコメントを記載している事例、経営者または実施者のみのコメントを記載している事例がある。

⑤　対策のポイントの紹介

SECURITY ACTION 自己宣言を行う際に必要となる対策状況のチェック、宣言の実施、宣言後の検討など、具体的な工程ごとに対策のポイントを記載している。

なお、一部の事例では、①事業者（企業）属性の紹介、②取組み内容の紹介、③事業者（企業）紹介のみ記載している。

5. 調査結果に基づく分析

アンケート調査及び訪問調査の結果から中小企業等[11]における情報セキュリティ対策とSECURITY ACTIONの取組みに関する課題や普及に向けた方策について報告する。

5.1. 中小企業等における情報セキュリティ対策の課題等

中小企業等における情報セキュリティ対策の課題とSECURITY ACTION制度に対する今後の期待について以下に示す。

5.1.1. 中小企業等における情報セキュリティ対策の課題

中小企業等の情報セキュリティ対策の課題として、情報セキュリティに関する規程や手順書作成の実施率が低いことが挙げられる（3.2.1(12)図 3-12）。これは、二つ星の自己宣言数が少ないことからも伺える（3.2.1(3)図 3-3）。訪問調査では、ISMS認証取得事業者やプライバシーマーク取得事業者、及び情報セキュリティのコンサルティングを実施する事業者が二つ星を宣言していることが多く、一つ星宣言事業者は、ポリシー作成が難しいという意見が多かった。アンケート調査では、中小企業等の情報セキュリティ支援策のなかでも情報セキュリティポリシーの作成ツールを求める回答が最も高い（3.2.1(15)図 3-15）。

既にSECURITY ACTIONの説明資料や中小企業向けの情報セキュリティ対策ガイドラインの付録として提供しているため、今後はこれら資料の更なる周知や具体的な作成方法等を解説するセミナー等の実施が求められる。

また、宣言後の情報セキュリティ対策の課題として、従業員への継続的な情報セキュリティ教育の実施や対策を徹底するための仕組みの構築、対策の定期的な見直しなどがある。今後、これらの課題への対応策についても強化していくことが求められる。

5.1.2. SECURITY ACTION制度に対する今後の期待

SECURITY ACTION制度は、自らが情報セキュリティ対策の実施状況を確認し、対策への取組み姿勢などを対外的に示すために宣言を行う制度であり、中小企業等にとって取組みやすい制度である。一方で、宣言による具体的な効果がわからないという意見もある（3.2.1(9)）。また、訪問調査では、制度のより一層の普及や知名度向上を期待する意見もあった。

[11] 今回の調査の対象であるSECURITY ACTION自己宣言事業者には、一部企業以外の法人、個人事業主が含まれるが、本章では、中小企業等と記載する。

5.2. 普及に向けた方策

SECURITY ACTION 制度の普及を通じて、中小企業等の情報セキュリティ対策を促進するために、「一つ星の自己宣言を促すための方策」、「二つ星へのステップアップを促すための方策」、「継続的な情報セキュリティ対策を促すための方策」を示す。

5.2.1. 一つ星の自己宣言を促すための方策

宣言を行ったきっかけは、補助金の申請の要件という回答率が最も高いが（3.2.1(8)図 3-8）、期待した効果は、取引先からの信頼が高まるという回答率が高い（3.2.1(9)図 3-9）。そのため、新たに SECURITY ACTION の取組みを促すためには、情報セキュリティ対策の重要性の訴求のみならず、取引先などの信頼が高まるなどビジネス上のメリットがあることを示すことで訴求していく必要がある。

5.2.2. 二つ星へのステップアップを促すための方策

昨今の企業に求められる情報セキュリティ対策水準は、取引先を含むサプライチェーン全体での対策実施であることから、中小企業等が実施すべき情報セキュリティ対策として、一つ星の「情報セキュリティ５か条」に止まらず、さらなる取組みを促す必要があると考えられる。

以下に、対策のステップアップを促すための支援策について検討した結果を示す。

(1) ステップアップすることのメリットの提示

二つ星の自己宣言事業者は、取引先などの社外関係者を意識し、信頼性向上や新規開拓に役立てるため情報セキュリティ対策を実施している傾向があり（3.2.2(6)）、訪問調査においても取引先から評価されたことで効果があったとする意見もあった。これらを踏まえ、一つ星の自己宣言事業者に対して、情報セキュリティ対策を高度化することで、取引先などの信頼性向上や新規開拓などの経営上のメリットが得られるという点に気づいてもらうことで、二つ星へのステップアップを促すことが期待できる。

(2) SECURITY ACTION 宣言の知名度向上

訪問調査では、SECURITY ACTION 制度の知名度が向上すれば二つ星を検討するという意見もあった。そのため、SECURITY ACTION 自己宣言事業者の参考となる取組みを紹介することや、本調査で作成した取組み事例集を積極的に情報発信するなど、SECURITY ACTION の知名度向上に向けた活動が求められる。

(3) 解説資料の充実

現在の SECURITY ACTION の関連資料については、対策の検討に有用であるという意見がある一方で、セキュリティポリシー作成に関してわかりやすい解説資料を要望する意

見があった。アンケートにおいて、SECURITY ACTION を宣言する主導者の 53.3%が「経営者」を占め、「21 名～300 名」の従業員規模では、総務担当者が主導者となる割合が 25～29%（3.2.2(4)図 3-21）を占める。そのため、SECURITY ACTION の関連資料に関し、読み手を意識した改善等を行うことが求められる。

5.2.3. 継続的な情報セキュリティ対策を促すための方策

中小企業等において情報セキュリティ対策を定着し強化するためには、従業員等に対する継続的な情報セキュリティ教育の実施に加え、取り巻く環境の変化を踏まえた情報セキュリティ対策状況の確認・評価・対策の見直し・継続的な改善が求められる。そのため、効果的な情報セキュリティ教育を実施するための教材の普及を図るとともに、SECURITY ACTION 自己宣言事業者に対し、情報セキュリティ対策状況の定期的な確認・評価・見直し・改善の実施と、そのための支援を進めていくことが求められる。

さらに、SECURITY ACTION の取組みを促す上では、経営層の情報セキュリティ対策の意識を高めることが重要であることは言うまでもない。その方策として、「国や関連機関による啓発活動」と「経営層の参加する団体を通じて取組みを促す」を合わせると 37%（3.2.1(14)の図 3-14）であり、上記に資する普及活動を充実化することで、SECURITY ACTION をより一層促進することが期待できる。

6. まとめ

本事業では、SECURITY ACTION 自己宣言事業者における情報セキュリティ対策の実施状況や課題、経営層の認識等を把握するため、自己宣言事業者を対象とし、総回答数5,162 件のアンケート調査を実施した。さらに、アンケート調査回答者 21 社に対して具体的な対策状況などを確認するために訪問調査を実施した。

中小企業等における情報セキュリティ対策の主な課題として、どこからどう始めたらよいかわからないといった意見があるが、「情報セキュリティ５か条」は「できるところから始める」取組みとして、一定の効果があると考えられる。

また、一つ星宣言事業者に対しては、情報セキュリティ対策をステップアップし高度化することで、取引先などの信頼性向上や新規開拓など経営上のメリットが得られることの情報発信や、情報セキュリティポリシー（基本方針）の作成ツール等に関する情報提供を行うことで、二つ星へのステップアップを促すことが期待できる。

さらに、SECURITY ACTION 制度の知名度や認知度が高まることが、中小企業等の SECURITY ACTION の取組みを進める動機となり得ることから、引き続き制度の知名度向上のための取組みが求められる。

これらの調査結果を参考に中小企業等の情報セキュリティ対策が促進され、我が国の中小企業等の情報セキュリティ対策水準が向上することを期待する。