SECURITY ACTION 制度解説

SECURITY ACTION 制度概要

- 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
  - 「中小企業の情報セキュリティ対策ガイドライン」の実践をベースに2段階の取組み目標を用意

1段階目（一つ星）

「情報セキュリティ5か条」に取組むことを宣言

2段階目（二つ星）

「5分でできる！情報セキュリティ自社診断」で自社の状況を把握したうえで、「情報セキュリティ基本方針」を定め、外部に公開したことを宣言

  - SECURITY ACTION 自己宣言数35万件を突破！（2024年6月）

SECURITY ACTION 制度の特長

- 情報セキュリティ対策への取組みの見える化
  - ロゴマークをウェブサイトに掲出したり、名刺やパンフレットに印刷することで自らの取組み姿勢をアピール
- 顧客や取引先との信頼関係の構築
  - 既存顧客との関係性強化や、新規顧客の信頼獲得のきっかけに
- 公的補助・民間の支援を受けやすく
  - SECURITY ACTIONを要件とする補助金の申請、普及賛同企業等から提供される様々な支援策が利用可能

普及賛同企業等

SECURITY ACTION 制度の趣旨に賛同し、当制度の普及促進のための積極的な取組みを実施する企業及び団体等。中小企業等が SECURITY ACTION制度を活用し、情報セキュリティ対策に取組むことを自己宣言するための支援策等を提供

【普及賛同企業等が提供する支援策の例】

- セキュリティに関する情報提供
- セキュリティ体制の構築を支援
- セキュリティ関連サービス提供時に優遇

登録事業者数　464社（2024/6時点）

SECURITY ACTION公式サイト

https://www.ipa.go.jp/security/security-action/

- SECURITY ACTIONの制度紹介や申込（宣言）、セキュリティ対策推進に役立つ情報・ツールを提供

ロゴマークの
使用申込（宣言）

SECURITY ACTION 公式 検索

ロゴマーク申込手順

STEP 1
取組目標を決める

一つ星 or 二つ星のどちらを宣言するか、取組目標を決めてください。

STEP 2
申込みフォームに入力

ロゴマーク使用規約に同意後、自己宣言のお申し込みを行います。

STEP 3
申込み手続き完了

STEP2 の後、1 週間程度で自己宣言 ID をお知らせするメールが届きます。

STEP 4
ダウンロード

STEP3 の後、1～2週間程度でロゴマークのダウンロード方法をお知らせするメールが届きます。

SECURITY ACTION公式サイト

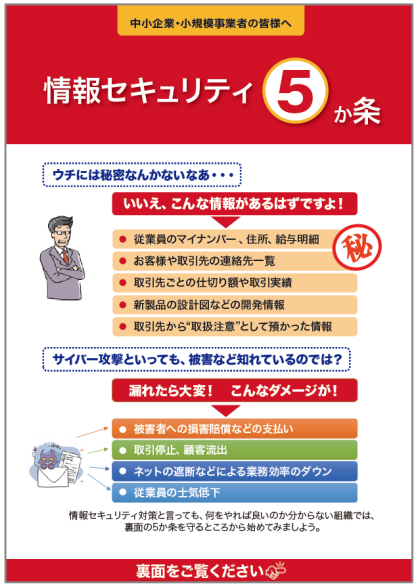
https://www.ipa.go.jp/security/security-action/

一つ星

一つ星の取組み目標

- 「情報セキュリティ5か条」に取組むことを宣言

1. OSやソフトウェアは常に最新の状態にしよう
2. ウイルス対策ソフトを導入しよう
3. パスワードを強化しよう
4. 共有設定を見直そう
5. 脅威や攻撃の手口を知ろう



1. OSやソフトウェアは常に最新の状態に

- OSやソフトウェアを古いまま放置していると、セキュリティ上の問題点が解決されず、それを悪用したウイルスに感染してしまう危険性がある
- お使いのOSやソフトウェアには、修正プログラムを適用する、もしくは最新版を利用する

＜対策例＞

- Windows Update(Windows OSの場合)/
  ソフトウェア・アップデート(Mac OSの場合)/
  OSバージョンアップ(Android の場合)
- Adobe Reader/Java実行環境(JRE) など
  利用中のソフトウェアを最新版にする

2. ウイルス対策ソフトを導入

- ID・パスワードを盗んだり、遠隔操作を行ったり、ファイルを勝手に暗号化するウイルスが増えている
- ウイルス対策ソフトを導入し、ウイルス定義ファイル（パターンファイル）は常に最新の状態になるようにする

＜対策例＞

- ウイルス定義ファイルが自動更新されるように設定する
- 統合型のセキュリティ対策ソフト(ファイアウォールや脆弱性対策など統合的なセキュリティ機能を搭載したソフト)を導入する

3. パスワードを強化

- パスワードが推測や解析されたり、ウェブサービスから流出したID・パスワードが悪用されたりすることで、不正にログインされる被害が増えている
- パスワードは「長く」「複雑に」「使い回さない」ようにして強化する

＜対策例＞

- パスワードは英数字記号含めて長い文字数にする
- 名前、電話番号、誕生日、簡単な英単語などはパスワードに使わない
- 同じID・パスワードをいろいろなウェブサービスで使い回さない

4. 共有設定を見直す

- データ保管などのウェブサービスやネットワーク接続した複合機の設定を間違ったために、無関係な人に情報を覗き見られるトラブルが増えている
- 無関係な人がウェブサービスや機器を使うことができるような設定になっていないことを確認する

＜対策例＞

- ウェブサービスの共有範囲を限定する
- ネットワーク接続の複合機やカメラ、ハードディスク(NAS)などの共有範囲を限定する
- 従業員の異動や退職時に設定の変更(削除)漏れがないように注意する

5. 脅威や攻撃の手口を知る

- 取引先や関係者と偽ってウイルス付のメールを送ってきたり、正規のウェブサイトに似せた偽サイトを立ち上げてID・パスワードを盗もうとする巧妙な手口が増えている
- 脅威や攻撃の手口を知って対策をとる

＜対策例＞

- IPAなどのセキュリティ専門機関のウェブサイトやメールマガジンで最新の脅威や攻撃の手口を知る
- 利用中のインターネットバンキングやクラウドサービスなどが提供する注意喚起を確認する

二つ星

二つ星の取組み目標

- 「5分でできる！情報セキュリティ自社診断」で自社の状況を把握したうえで、情報セキュリティ基本方針を定め、外部に公開したことを宣言

＋

情報セキュリティ基本方針の記載項目例

- 管理体制の整備
- 法令・ガイドライン等の順守
- セキュリティ対策の実施
- 継続的改善　　など

1. 基本方針の作成と周知

- 経営者が定めた情報セキュリティに関する基本方針を、従業員や関係者に伝えるために簡潔な文書を作成・周知する
- 中小企業の情報セキュリティ対策ガイドライン付録「情報セキュリティ基本方針（サンプル）」を参考

情報セキュリティ基本方針の記載項目例

- 管理体制の整備
- 法令・ガイドライン等の順守
- セキュリティ対策の実施
- 継続的改善　　など

2. 実施状況の把握

- 自社のセキュリティ対策の実施状況を把握するために「5分でできる!情報セキュリティ自社診断」を活用する
  - 25項目の設問に答えるだけで、自社の情報セキュリティの問題点を簡単に把握できる
  - 解説編の対策例を参考に、社内ルールを作成することができる
  - 付録の情報セキュリティハンドブックを活用すると従業員に対する社内ルールの周知が簡単にできる

基本的対策

- 情報セキュリティ自社診断の「基本的対策」は、情報セキュリティ5か条を質問化したもの

No.	診断内容	実施している	一部実施している	実施していない	わからない
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？	4	2	0	-1
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※1 は最新の状態にしていますか？	4	2	0	-1
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？	4	2	0	-1
4	重要情報※2 に対する適切なアクセス制限を行っていますか？	4	2	0	-1
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？	4	2	0	-1

※1　コンピュータウイルスを検出するためのデータベースファイル「パターンファイル」とも呼ばれる
※2　営業秘密など事業に必要で組織にとって価値のある情報や顧客や、従業員の個人情報など管理責任を伴う情報のこと

5分でできる!情報セキュリティ自社診断

従業員としての対策

No.	診断内容	実施している	一部実施している	実施していない	わからない
6	電子メールの添付ファイルや本文中のURL リンクを介したウイルス感染に気をつけていますか？	4	2	0	-1
7	電子メールやFAX の宛先の送信ミスを防ぐ取り組みを実施していますか？	4	2	0	-1
8	重要情報は電子メール本文に書くのではなく、添付するファイルに書いてパスワードなどで保護していますか？	4	2	0	-1
9	無線LAN を安全に使うために適切な暗号化方式を設定するなどの対策をしていますか？	4	2	0	-1
10	インターネットを介したウイルス感染やSNSへの書き込みなどのトラブルへの対策をしていますか？	4	2	0	-1
11	パソコンやサーバーのウイルス感染、故障や誤操作による重要情報の消失に備えてバックアップを取得していますか？	4	2	0	-1

5分でできる!情報セキュリティ自社診断

従業員としての対策

No.	診断内容	実施している	一部実施している	実施していない	わからない
12	紛失や盗難を防止するため、重要情報が記載された書類や電子媒体は机上に放置せず、書庫などに安全に保管していますか？	4	2	0	-1
13	重要情報が記載された書類や電子媒体を持ち出す時は、盗難や紛失の対策をしていますか？	4	2	0	-1
14	離席時にパソコン画面の覗き見や勝手な操作ができないようにしていますか？	4	2	0	-1
15	関係者以外の事務所への立ち入りを制限していますか？	4	2	0	-1
16	退社時にノートパソコンや備品を施錠保管するなど盗難防止対策をしていますか？	4	2	0	-1
17	事務所が無人になる時の施錠忘れ対策を実施していますか？	4	2	0	-1
18	重要情報が記載された書類や重要なデータが保存された媒体を破棄する時は、復元できないようにしていますか？	4	2	0	-1

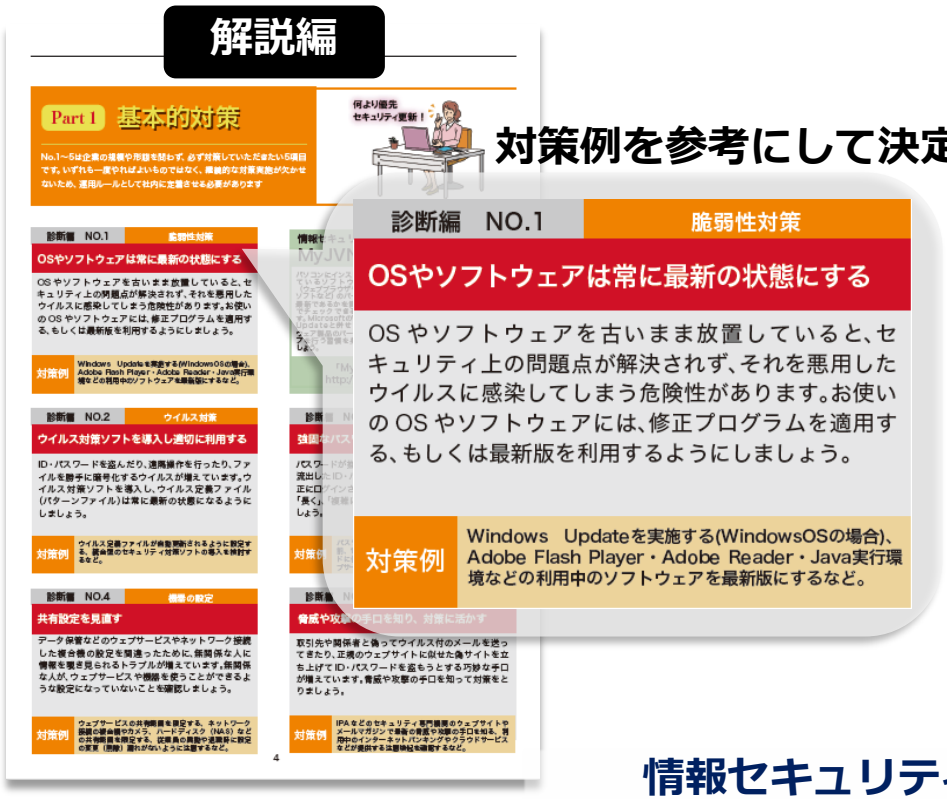
5分でできる!情報セキュリティ自社診断

組織としての対策

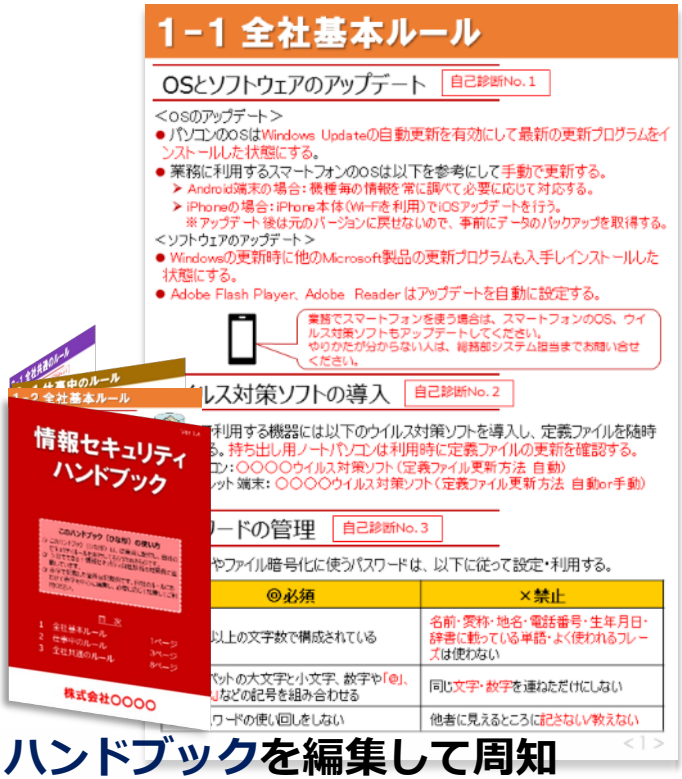
No.	診断内容	実施している	一部実施している	実施していない	わからない
19	従業員に守秘義務を理解してもらい、業務上知り得た情報を外部に漏らさないなどのルールを守らせていますか？	4	2	0	-1
20	従業員にセキュリティに関する教育や注意喚起を行なっていますか？	4	2	0	-1
21	個人所有の情報機器を業務で利用する場合のセキュリティ対策を明確にしていますか？	4	2	0	-1
22	重要情報の授受を伴う取引先との契約書には、秘密保持条項を規定していますか？	4	2	0	-1
23	クラウドサービスやウェブサイトの運用等で利用する外部サービスは、安全・信頼性を把握して選定していますか？	4	2	0	-1
24	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？	4	2	0	-1
25	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？	4	2	0	-1

3. 対策の決定と周知

- 問題があった項目は、解説編を参考に対策を決定
- 付録「情報セキュリティハンドブック(ひな形)」を編集して社内周知する



対策例を参考にして決定



情報セキュリティハンドブックを編集して周知

参考資料

● 中小企業の情報セキュリティ対策ガイドライン

中小企業の経営者や実務担当者が、情報セキュリティ対策の必要性を理解し、情報を安全に管理するための具体的な手順等を示したガイドライン

https://www.ipa.go.jp/security/guide/sme/about.html

● SECURITY ACTION

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

https://www.ipa.go.jp/security/security-action/

参考情報（SECURITY ACTION）

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

- 2018年度に続き、今回2回目の調査
- 2024年1月から2月にかけてウェブによるアンケート調査を実施し、5,577件の回答を入手

調査目的	情報セキュリティ対策の取り組み内容や課題等に関するアンケート調査を実施することで、現状を把握し、今後の支援施策の企画立案に生かすこと。
調査手法	ウェブによるアンケート調査
調査対象	SECURITY ACTION宣言事業者（一つ星・二つ星） ※アンケート回答依頼メールの配信件数：251,002件
調査期間	2024年1月15日(月)～2月13日(火)
有効回答数	5,577件（回答率：2.2%）

- 調査報告書を2024年4月9日に公開

https://www.ipa.go.jp/security/reports/sme/sa-survey2023.html

調査結果 ～主なポイント～（1/4）

(1) SECURITY ACTION宣言のきっかけは補助金申請が大半ではあるものの、情報セキュリティ対策の意欲を後押ししている。

補助金を申請する際の要件となっていた」が75.1%と最も高く、大半を占めています。次いで「情報セキュリティに係る自社の対応を改善したいと考えていた」が24.4%、「事業拡大や顧客開拓、取引先からの信頼を高める手段として有用と考えた」が16.6%と、SECURITY ACTION宣言が自社の情報セキュリティ対策の意欲を後押ししているようにも考えられます。

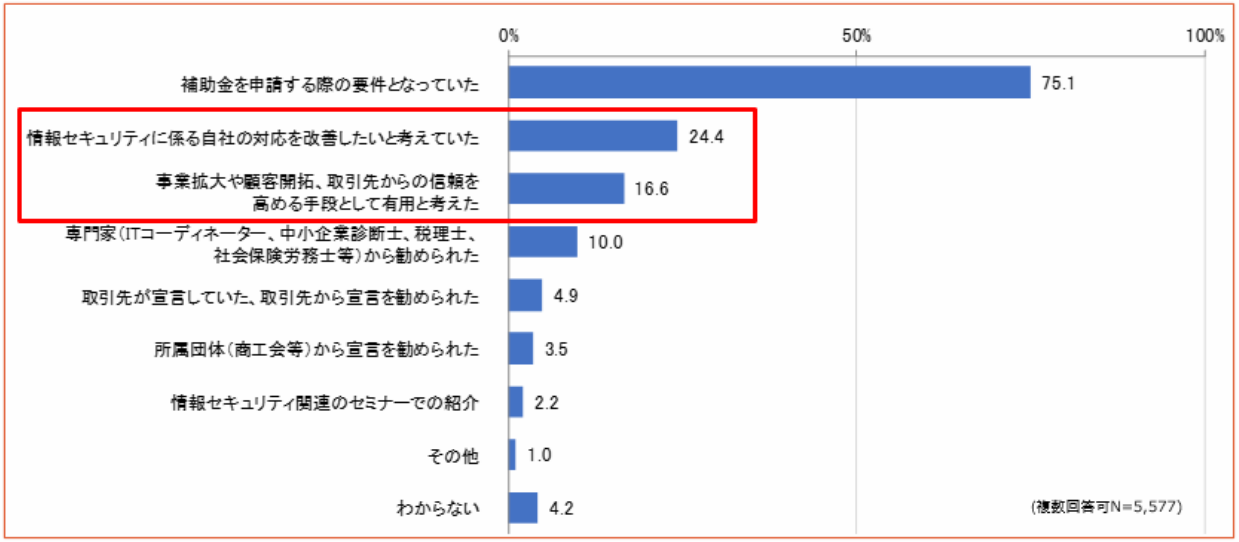


図1：SECURITY ACTION宣言を行おうとしたきっかけ（調査報告書p21 図4-13）

調査結果 ～主なポイント～（2/4）

(2) SECURITY ACTION宣言事業者の約40%が意識向上や取引先からの信頼性向上等の効果を感じている。

回答者の40%は効果があったと回答している。最も多いのは「経営層の情報セキュリティ対策に関する意識の向上」（23.0%）、「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の向上」（22.8%）、「取引先からの信頼性の向上」（13.2%）と続いています。

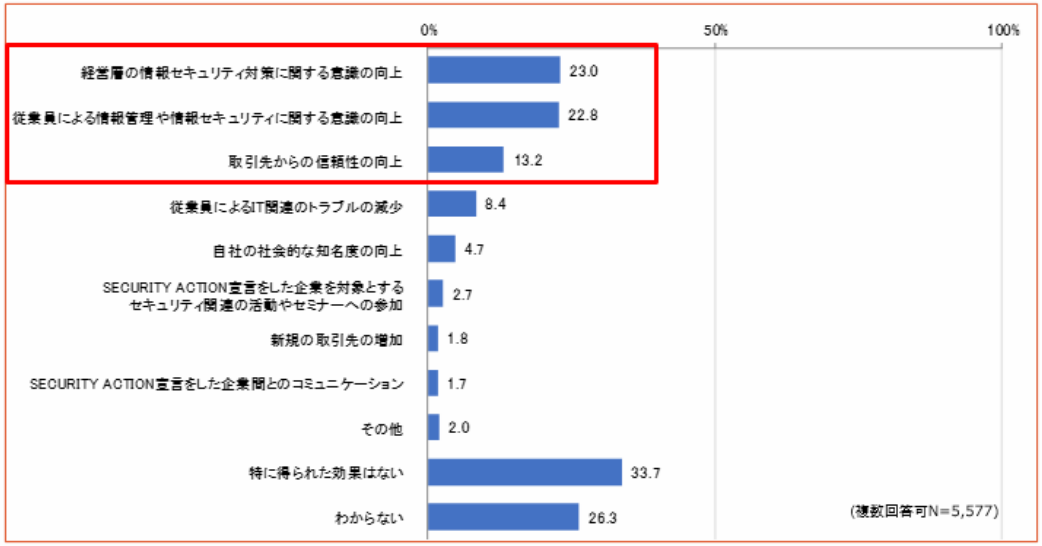


図2：SECURITY ACTION宣言による効果（調査報告書p22 図4-14）

効果の具体例としては、経営層や従業員の情報セキュリティに対する意識向上により社内でのセキュリティソフト導入のきっかけになった、SECURITY ACTIONロゴマークを名刺に記載、またSECURITY ACTION宣言を社内にお知らせしたことで、意識向上につながっているなどの効果を実感している事業者も見られました。

その他、取引先からのセキュリティ調査などでの信頼向上、新規得意先の獲得に役立ったなどの対外的な効果を挙げられている例がありました。

調査結果 ～主なポイント～（3/4）

(3) SECURITY ACTION宣言が継続的な情報セキュリティ対策への取り組みを後押ししている。

1年以内に実施した、あるいは1年以内に実施実施を予定している情報セキュリティ対策について質問しました。結果、いずれの対策も実施しない（18.3%）、わからない(19.8%）を除くと、回答者の60%以上の事業者が、いずれかの対策を実施しているとの回答を得ました。中でも「従業員に対する情報セキュリティ対策ルールの教育」が30.7%と最も高く、次いで「クラウドサービスやウェブサイトで利用している外部サービスの安全性、信頼性の確認」が24.1%となっています。

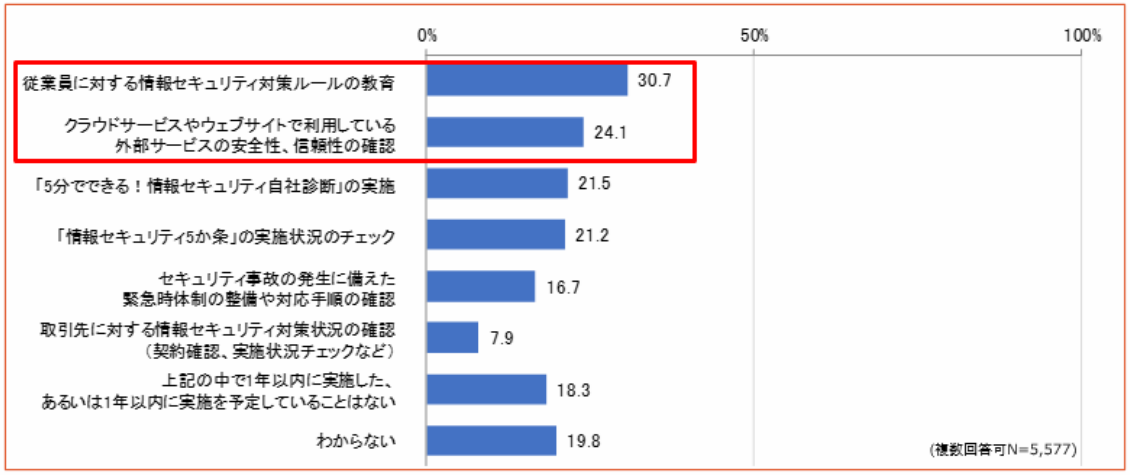


図3：1年以内に実施した、あるいは1年以内に実施を予定しているセキュリティ対策（調査報告書p27 図4-16）

補助金申請がきっかけのSECURITY ACTION宣言事業者を含めても、情報セキュリティ対策を1年以内に実施、あるいは1年以内に実施を予定しているが60%を超えており、SECURITY ACTION自己宣言することが継続的な情報セキュリティ対策に対する意識向上につながっていると考えられます。

調査結果 ～主なポイント～（4/4）

(4) 情報セキュリティ対策を進める上での問題点は依然として人員と知識不足。

情報セキュリティ対策を進める上での問題点は、「情報セキュリティ対策を行うための人員が不足している」が38.6%と最も高く、次いで「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33.3%、「従業員の情報セキュリティに対する意識が低い」が31.9%となっています。

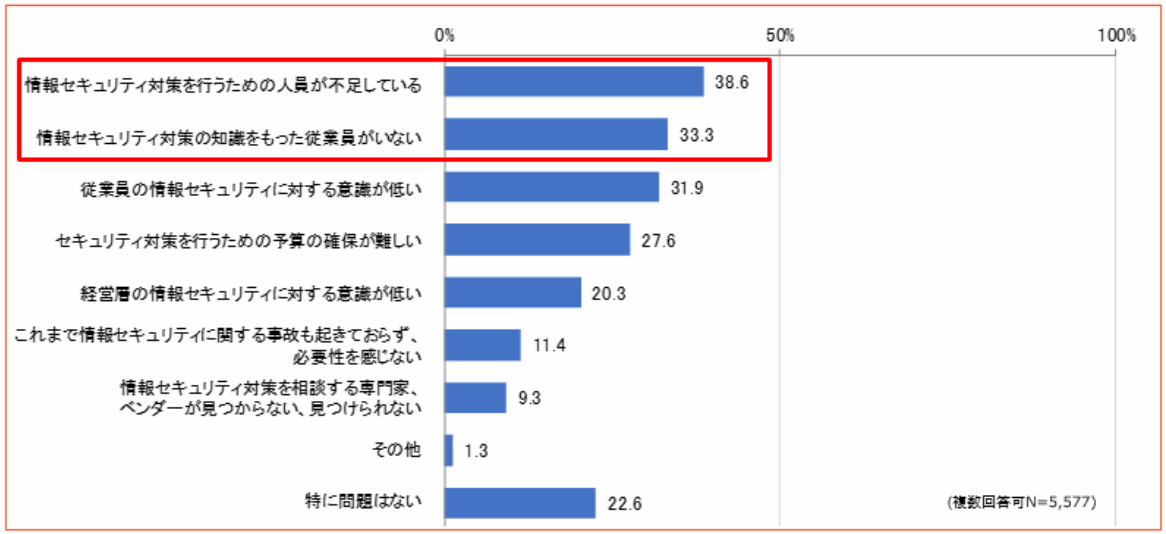


図4：情報セキュリティ対策を進める上での問題点（調査報告書p31 図4-20）

依然として情報セキュリティに関する人材や知識不足から、対策の実施に苦労されている事業者も多く見られます。特に一つ星宣言事業者に向けては、従業員教育に活用できるツール、情報セキュリティ対策を進める際に参考となるガイドラインなどの拡充に加え、取り組み段階に応じて閲覧をナビゲートするなどの提供方法の工夫も必要なことが再確認されました。

よくある質問の掲載箇所

- お問い合わせの前に
  ご一読ください

SECURITY ACTION公式サイトの
フッター「よくある質問」をクリック

よくある質問

制度について

Q.「SECURITY ACTION」とはどのような制度ですか。

A.「SECURITY ACTION」は、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」する制度です。中小企業の自発的な情報セキュリティ対策への取組みを促す活動を推進し、安全・安心なIT社会を実現するためにIPAが創設した制度です。「SECURITY ACTION」は、情報セキュリティ対策状況等をIPAが認定するあるいは認証等を与える制度ではありません。

Q.「一つ星」と「二つ星」のロゴマークの違いは何ですか。

A.「一つ星」は、中小企業の情報セキュリティ対策ガイドライン付録の「情報セキュリティ5か条」に取組むことを宣言した中小企業等であることを示すロゴマークです。

「二つ星」は、同付録の「5分でできる！情報セキュリティ自社診断」で自社の状況を把握したうえで、情報セキュリティ基本方針を定め、外部に公開したことを宣言した中小企業等であることを示すロゴマークです。

よくある質問

申込について（1/2）

Q.自己宣言の申込方法を教えてください。

A.自己宣言事業者の場合は「SECURITY ACTION 自己宣言者サイト」からお申込みください。

Q.自己宣言の申込み受付から正式な受理通知までの所要日数はどのくらいですか。

A.「自己宣言完了のお知らせ」メールをお送りしてから約１週間後に、「申込み受理のご連絡」メールにてロゴマークの使用手順等をお知らせします。

Q.情報セキュリティ対策にまだ取組んでいなくても、申込むことができますか。

A. 一つ星は「情報セキュリティ5か条」に取組むことを宣言するもので、始めの一歩としてお申込みいただけます。（これから情報セキュリティ対策を始める行動を起こす意味での「SECURITY ACTION」です）

Q.「二つ星」の申込時、「5分でできる！情報セキュリティ自社診断」で何点以上の得点が必要でしょうか。

A.何点でも構いません。

よくある質問

申込について(2/2)

Q.「二つ星」の申込時、情報セキュリティ基本方針を外部に公開する場合、自社ウェブサイトに掲載する必要があるのでしょうか。

A.いいえ、外部に公開とは自社ウェブサイトへの掲載に限定するものではありません。

会社案内等へ記載していただくなど、外部の方からお問い合わせいただいた際に提示できる状況であればかまいません。なお、「SECURITY ACTION自己宣言」入力時の「情報セキュリティ基本方針外部公開方法」において、「自社ウェブサイト」「会社案内」「パンフレット」「その他」のいずれかを選んでいただく必要があります。

Q.「二つ星」の申込時、個人情報保護方針を公開している場合は、情報セキュリティ基本方針を公開しているとみなすことができますか。

A. いいえ、できません。 情報セキュリティ基本方針は、個人情報保護に限定するものではなく、情報セキュリティに関する「理念」「方針」「声明」「宣言」などを示すものです。

よって、個人情報保護方針の公開は、情報セキュリティ基本方針を公開しているとはみなせません。

よくある質問

ロゴマークの使用等について

Q.ロゴマークの使用に際して、ルールがありますか。

A.「ロゴマーク使用規約」は、こちらをご確認ください。

https://www.ipa.go.jp/security/security-action/mark/

「ロゴマーク使用ガイドライン」は、使用許諾後の通知により、参照いただけるようになります。

Q.ウェブサイト等に記載する際の正しい表記と注意点を教えてください。

A.「SECURITY ACTION」は情報セキュリティ対策状況、普及促進の取組み等を、IPAが認定するものではありませんので、次のような不適切な表現を使用されますと、第三者の誤解を招く可能性が懸念されますので、ご注意願います。

適切な例　…「一つ星（二つ星）を宣言しました」

不適切な例 …「一つ星（二つ星）の認定を受けました」