SECURITY ACTION 宣言事業者（二つ星）における情報セキュリティ自社診断の実態調査

2025 年 8 月 8 日
Ver.1.0
特定非営利活動法人日本ネットワークセキュリティ協会
社会活動部会中小企業支援施策ワーキンググループ

目次

（図表目次）

はじめに

近年、中小企業における情報セキュリティ対策の重要性が増しており、多くの中小企業が情報セキュリティ対策を実践している。その一方で、実践にあたり、課題を感じている企業も少なくない。NPO 法人日本ネットワークセキュリティ協会（以下、JNSA）の「インシデント損害額調査レポート第 2 版[1] 」によると、中小企業においてもセキュリティに関するインシデントの損害額についてはケースバイケースではあるものの、場合によっては数千万円から数億円単位の損失が発生する恐れがあるとしている。こうしたことから企業においては業界に関係なく、さらなる情報セキュリティに対する取り組みが必要である。

JNSA では独立行政法人情報処理推進機構（以下、IPA）と共同で、情報セキュリティ対策の実施状況や取り組む際の課題を把握し、より有効な支援をするための参考情報として、IPA が示す「中小企業の情報セキュリティ対策ガイドライン[2]」の「5 分でできる！情報セキュリティ自社診断[3]」25 項目を基準に、各項目の実施状況の調査を実施した。

本報告書が、中小企業の情報セキュリティ対策を支援する皆様にとって有益な資料となり、中小企業のセキュリティ向上につながることを願ってやまない。

1　アンケート調査概要

1.1　SECURITY ACTION（二つ星）宣言事業者へのアンケート調査

SECURITY ACTION 宣言事業者（二つ星）に対して、IPA の SECURITY ACTION 導入に関する目的や効果、および「5 分でできる！情報セキュリティ自社診断」の各項目の実施状況やその課題などを調査するために、アンケート調査を実施した。

1.2　実施概要

アンケート調査の実施概要を表 1 に示す。

表 1 アンケート実施概要

項目	内容
実施対象	SECURITY ACTION 宣言事業者（二つ星）
対象数	33,573 件
実施期間	2024 年 10 月 28 日～2024 年 11 月 18 日
実施方法	アンケート回答依頼のメールに基づき、以下のいずれかの方法によるアンケートを実施した。 ① Web フォームによるアンケート ② メールにて Excel シートを送付し、アンケート記入を依頼
回収方法	２つの実施方法に合わせそれぞれ下記に従い回収を行う。 ① 期限までに記入した Web フォームの入力情報を収集 ② 記入済み Excel シートをメールにて提出して頂き入力情報を収集
回答数	1,867 件

1.3 アンケート内容

アンケート内容について、その内容を表 2 に示す。
尚、本調査のアンケートにおいて「５分でできる！情報セキュリティ自社診断」の各項目名は、IPA の下記リンク先にある「5 分でできる！情報セキュリティ自社診断(Excel 版)」を用いている。

https://www.ipa.go.jp/security/guide/sme/5minutes.html

上記 Excel 版と、「中小企業の情報セキュリティ対策ガイドラインサイト」の「付録 3：5 分でできる！情報セキュリティ自社診断」（PDF 版）の項目名との対比を別紙に示す。

表 2 アンケートの構成

項目	内容
アンケート協力のお願い	アンケートの趣旨、回答方法、回答期間、および実施主体についての説明
回答企業の属性	回答企業の業種、主たる事業所の所在地、従業員数、「5 分でできる！情報セキュリティ自社診断」の実施時期、実施者、企業の情報セキュリティ対策担当、情報セキュリティの情報収集手段を問う内容。
SECURITY ACTION の効果	SECURITY ACTION 宣言を行ったことによる効果、および具体的な取り組み内容を問う内容。
5 分でできる！自社診断の実施状況の取り組み	SECURITY ACTION「二つ星（★★)」を宣言される際に実施する「５分でできる！情報セキュリティ自社診断」の 25 項目のそれぞれに対して、以下の①から④を問う内容。 ①実施状況 「5 分でできる！情報セキュリティ自社診断」の各項目について実施状況を 5 択から回答 実施している/一部実施している/実施していない（予定あり）/実施していない（予定なし）/わからない ②①にて、「実施していない（予定なし)」の場合、その理由について、4 択から回答 必要なしと判断/必要だが優先順位が低い/実施に当たって障害がある/その他 ③②にて、「実施にあたって障害がある」と回答した場合に具体的な内容を自由記述で回答。 ④実施をするために必要な支援施策について、以下の選択肢に対し、複数回答を含めた回答。 支援者（専門家派遣）/人材育成支援/補助金支給/税等の優遇措置/法などによる義務化/ソリューション紹介/アウトソース（マネージドサービス）/その他（自由記述）

1.4 ヒアリング

アンケートの回答者に対して、さらに詳しい状況や背景を把握することを目的にヒアリングを実施した。ヒアリングの実施内容について、その内容を表 3 に示す。

表 3 ヒアリング実施概要

項目	内容
実施対象	アンケート回答者からピックアップした
実施期間	2025 年 2 月 27 日～2025 年 3 月 4 日
実施方法	オンライン
主なヒアリング内容	「5 分でできる！情報セキュリティ自社診断」25 項目に関するヒアリング内容 1. 対応するにあたって実施しやすかった項目と対応開始方法 2. 必要だが対応が難しいと感じた項目あるいは見送った項目とその理由 3. 対応が難しいと感じた項目についてどのように対応しましたか 4. どのような支援があると、難しい項目や見送った項目の対応が容易になりますか 5. 対応するにあたってどのようにして情報収集を行いましたか 6. 気になっているが項目に含まれていない事項があれば教えてください 7. 情報発信者への要望

2　アンケート結果

2.1　回答企業の属性

本節では、実態調査のためのアンケートに回答した企業（1,867 件）に関する属性を示す。

2.1.1 業種

アンケートに協力した企業の主たる事業の業種について図 1 に示す。

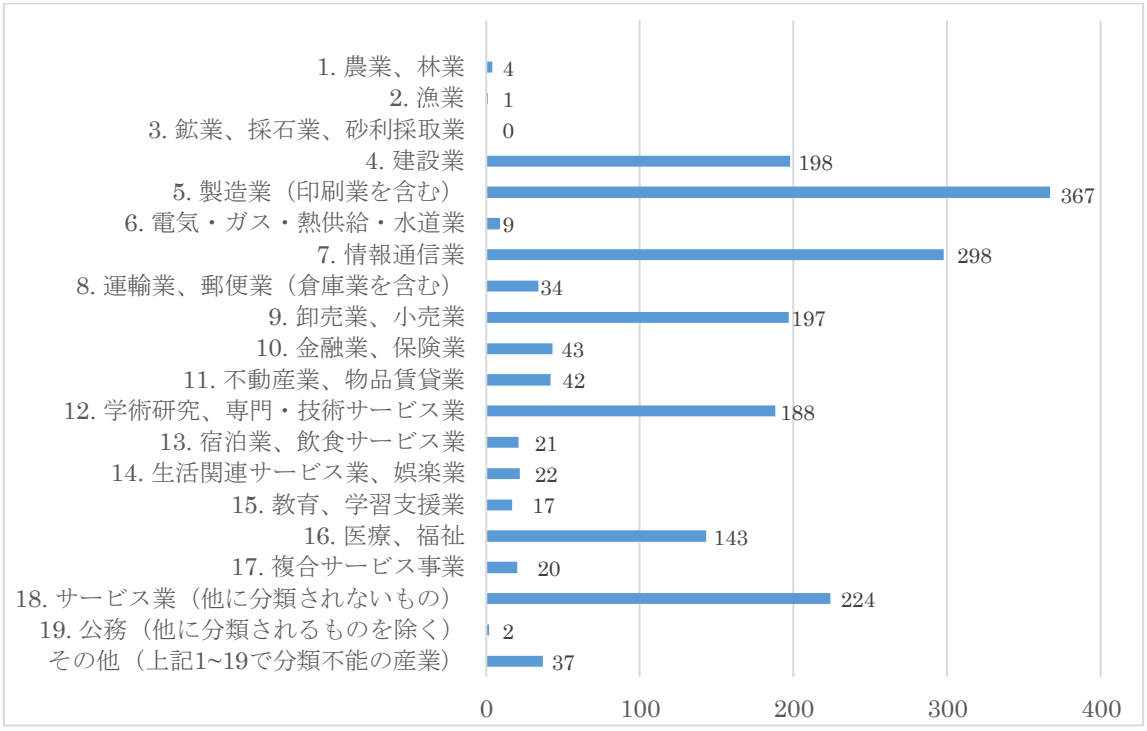


図 1 主たる事業の業種

2.1.2 地域

アンケートに協力した企業の主たる事業所の所在地を都道府県単位で集計したものを図 2 に示す。

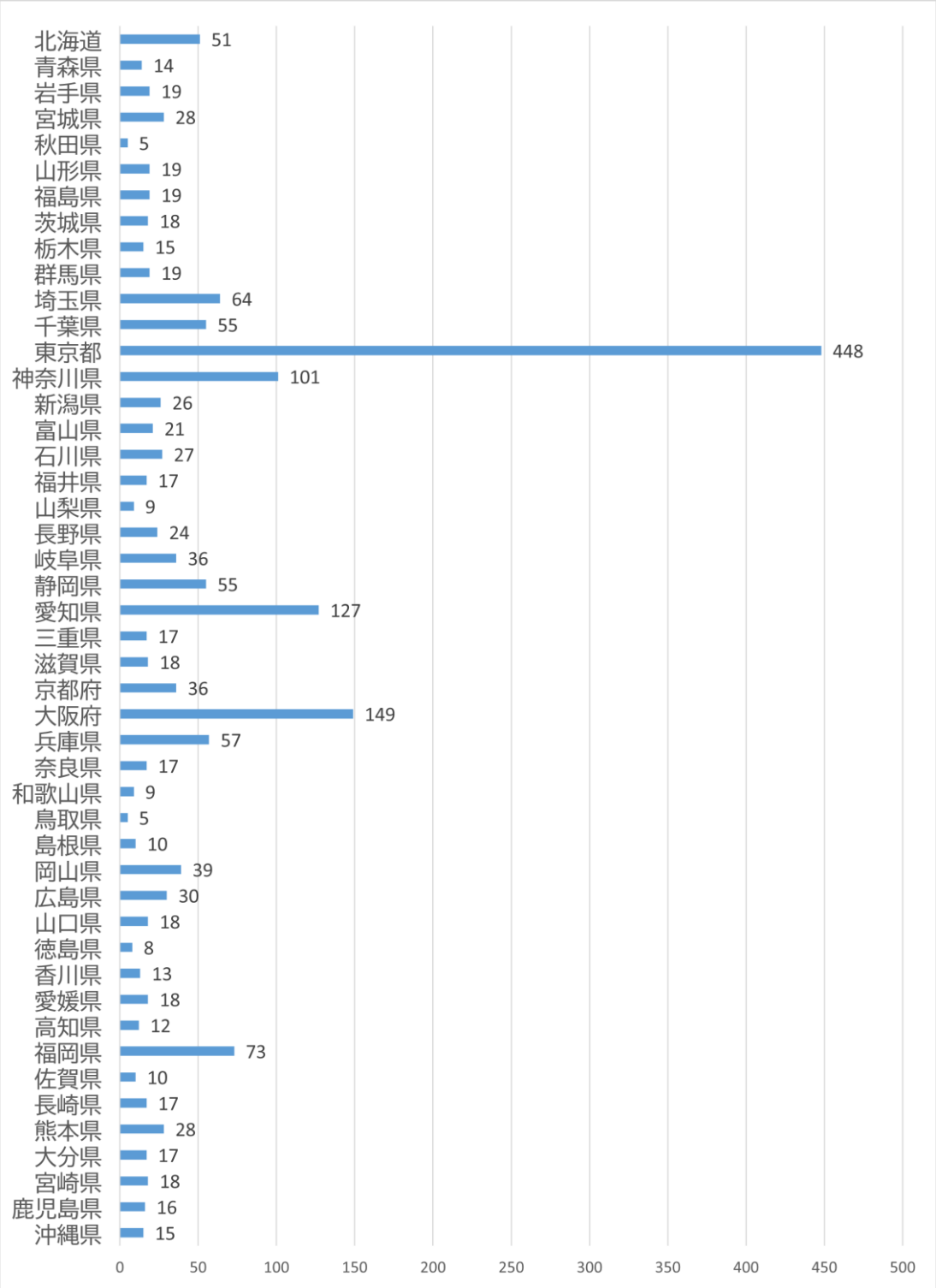


図 2 主たる事業所の所在地

2.1.3 従業員数

アンケートに協力した企業の従業員数を図 3 に示す。（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く）

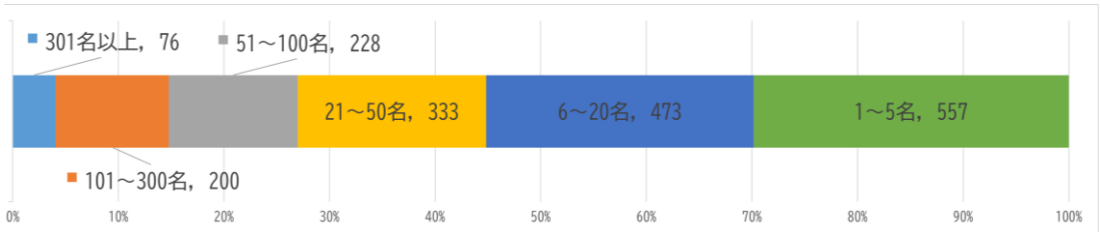


図 3 従業員数

2.1.4 実施時期

アンケートに協力した企業が、「5 分でできる！情報セキュリティ自社診断」を最後に実施した時期を図 4 に示す。

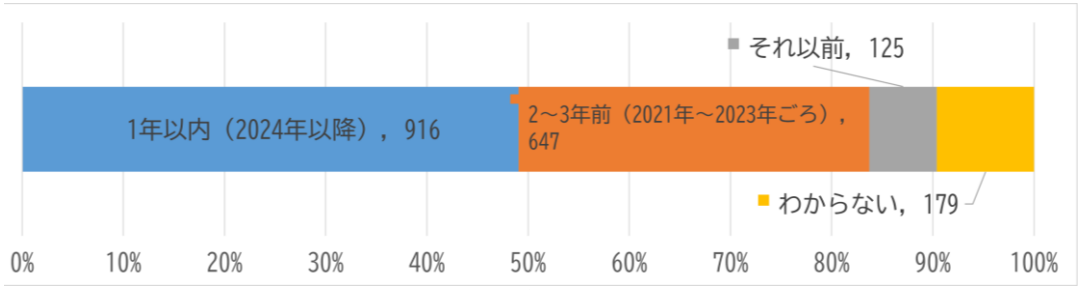


図 4 実施時期

2.1.5 実施者

アンケートに協力した企業の「5 分でできる！情報セキュリティ自社診断」実施者を図 5 に示す。

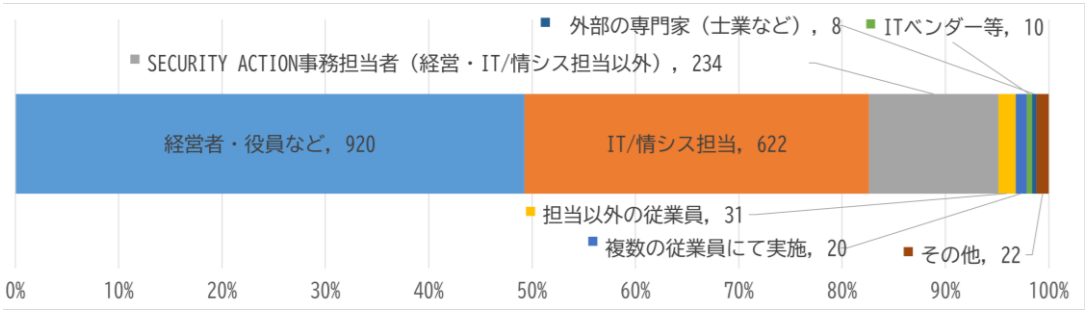


図 5 自社診断の実施者

2.1.6 担当者

アンケートに協力した企業の情報セキュリティ担当者について図 6 に示す。情報セキュリティ担当者は、専任か、または兼務か。また、兼務の場合は、どの様な業務との兼務かについても併せて質問を行った。

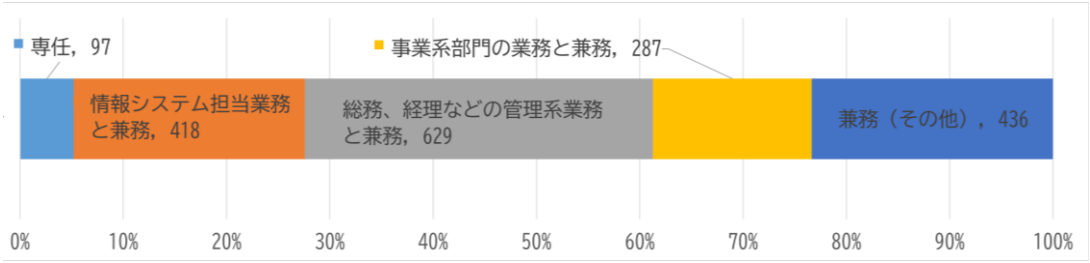


図 6 情報セキュリティの担当者

2.1.7 情報収集先

アンケートに協力した企業の情報セキュリティ担当者の情報セキュリティに関する情報収集先、および学習手段を図 7 に示す。なお、回答については、複数回答を可としている。

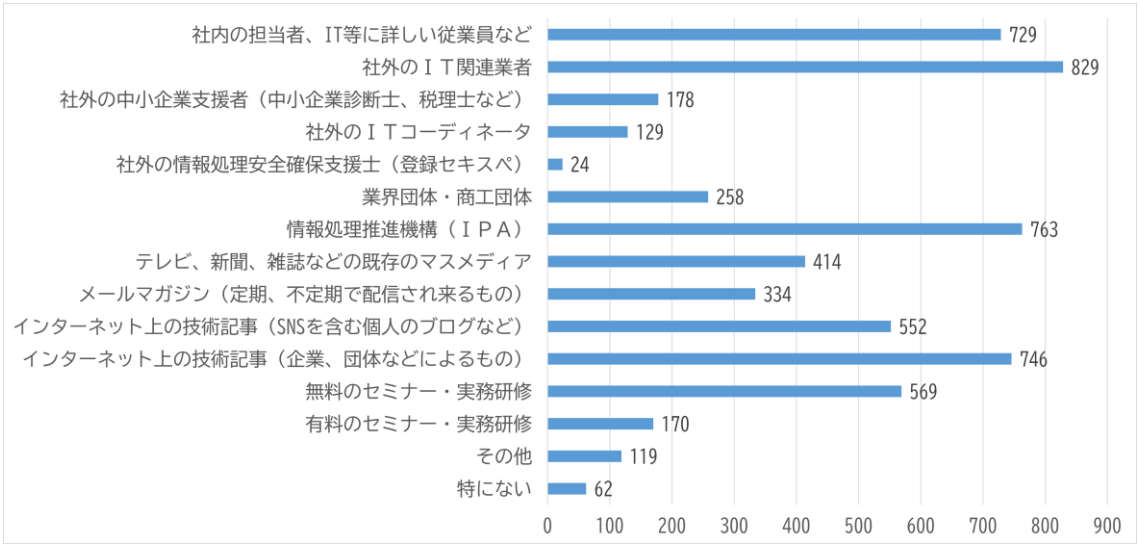


図 7 情報セキュリティの情報収集先と学習手段

2.2 SECURITY ACTION の効果

2.2.1 きっかけ

アンケートに協力した企業が、SECURITY ACTION 宣言を行おうとしたきっかけの回答を図 8 に示す。「取引先からの信頼性の向上」が一番多く、「自社の社会的な知名度向上」や「新規の取引先の増加」といった回答を大きく上回る。このことから、SECURITY ACTION 宣言による現在の顧客（取引先）との信頼関係の強化に重きを置く傾向が読み取れる。次に「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」、「経営層の情報セキュリティ対策に関する意識の向上」と続いており、経営層を含めた自社内での 情報セキュリティに関する意識の向上に重きを置いていることが推察される。一方で数は少ないものの、「特に得られた効果はない」、「わからない」といった回答もあり、導入目的・きっかけが伝わっていない、あるいは理解されていない企業も 185 社（10%）ほどあることが分かった。183 社が「その他」と回答しており、この内訳を見たところ、140 社（7%）の企業が補助金について言及していることがわかった。このことから一部の企業が補助金をきっかけに SECURITY ACTION への取り組みをしていることが読み取れた。

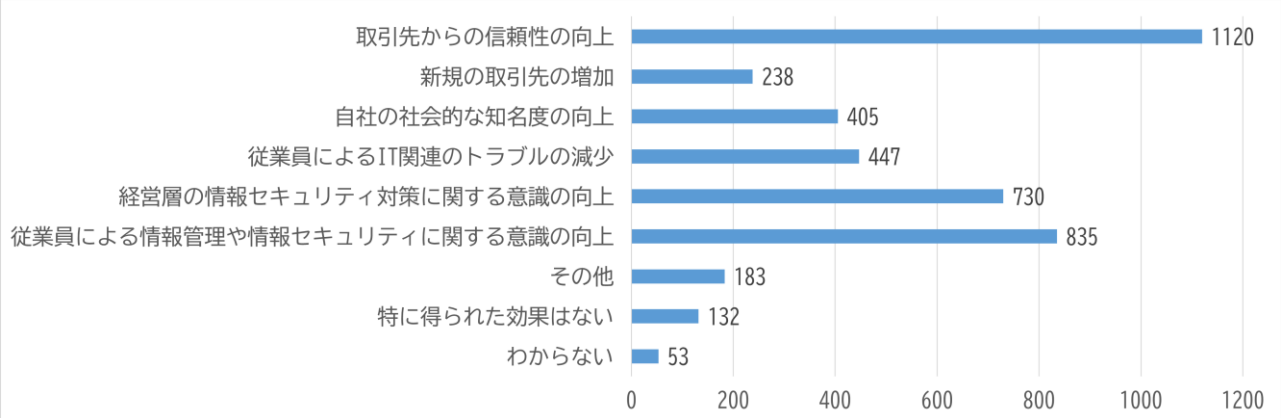


図 8 SECURITY ACTION 宣言を行うきっかけ

2.2.2 効果

アンケートに協力した企業が SECURITY ACTION 宣言を行ったことによる効果として特に多かったキーワードを、表 4 に示す。また、アンケートに協力した企業が SECURITY ACTION 宣言を行ったことによる効果についてのアンケートの回答から特に頻出する単語を抽出したものを図 9 に示す。

回答内容には、「意識が高まった」、あるいは「社員のリテラシー向上につながる」といった育成的な効果を回答する企業が多くみられた。また、「顧客からの信頼」、「補助金の支給につながる」などといった回答も見受けられた。一方で、「なし」、「実感がない」などの回答も一定数見受けられた。

表 4 効果において多くみられたキーワード（抜粋）

キーワード	内容
意識（234 社）	・ 社員などのセキュリティ意識向上につながったという回答が多かった。 ・ 一部危機管理意識、心構え的な意味での意識向上などもあった。
情報（160 社）	・ 情報リテラシー、個人情報保護などといった情報の管理の取り組み ・ 情報セキュリティに関する意識向上、
こと（133 社）	・ 「～をしたこと」などの語尾に使われている。このキーワードによる特段とした内容はなかった。
ない（113 社）	・ 変わらないといったような効果がないという意味合いで使われている箇所が多かった。 ・ あわせて、実感がない、わからないなど結果について気づけないといった回答も多かった。
向上（167 社）	・ 「意識の向上」という文脈で使われているところが多かった。（例えば、セキュリティ意識向上、リテラシー・スキルの向上など） ・ 「取引先からの信頼の向上」といった使われ方もあった。
効果（89 社）	・ 導入の効果について書かれている。効果が感じられない、効果がわからないといったネガティブな内容の方が多かった。一方、教育の効果や助成金申請時に効果があったなどといったポジティブな内容は比較的少なかった。
従業（74 社）	・ 「従業員」の教育的な効果、意識改革につながったといった内容が多かった。
取引（59 社）	・ 「取引先」への信頼性向上や、アピールに役立つなどが見られた。

図 9 SECURITY ACTION 実施の効果（頻出単語の抽出）

2.2.3 取り組み

アンケートに協力した企業が SECURITY ACTION 宣言をしたことによる取り組みとして特に多かったキーワードを、表 5 に示す。また、アンケートに協力した企業が SECURITY ACTION 宣言をしたことによる取り組みとしてのアンケートの回答から頻出する単語を抽出したものを図 10 に示す。

アンケートに協力した企業が SECURITY ACTION 宣言における取り組みとして回答したものの中では、「マルウェア対策を進めている。」「アーカイブの暗号化、オフライン保護等」「ウィルスソフトパターンファルアップデート、Windows Update 等、アプリの更新忘れが無い様取り組んでいます」などのように具体的に 25 項目の取り組みを進めていると回答する企業が多かった。中には「3D セキュアの導入」など、より高度なセキュリティ対策への取り組みを回答する企業もあり、SECURITY ACTION 宣言をきっかけに情報セキュリティ対策に対する取り組みが進んだことを回答する企業が多かった。また、回答企業の中では、ISMS や P マークなどを取得している企業 もあり、これらの企業においては、あまり問題なく宣言へとこぎつけることができたという回答が多かった。こうした取り組みについて、社外へＨＰ、ブログや業界団体への報告などを行い、自社の取り組みを周知する企業も一定数あった。

表 5 取り組みにおいて多くみられたキーワード（抜粋）

キーワード	内容
情報（219 社）	・ 情報セキュリティ教育、対策の実施など情報セキュリティに対する取り組み強化、組織づくりなどを記載されていた。 ・ 個人情報や、情報漏洩などの純粋に「情報」という言葉で使われることが多かった、また、情報共有、情報管理の強化、および機密情報管理規定などのルール策定なども見られた。
社内（135 件）	・ 社内への周知や、社内向けに情報共有を行ったという内容が多かった。 ・ 社内体制整備、社内セキュリティ、社内ネットワークセキュリティ対策など、社内を対象として、セキュリティ強化を行ったという内容が多かった。
対策（95 件）	・ マルウェア対策、(サイバー) セキュリティ対策、ランサムウェア対策などのセキュリティ脅威に対する対策を回答する企業が多かった。
実施（85 社）	・ 「セキュリティ対策の実施」、「セキュリティ教育の実施」などセキュリティ強化のための行動が多かった。 ・ 取り組み内容をもとに、認証取得の実施といったものや、実施計画といったものも見受けられた。
ない（68 社）	・ 特にないといった意味合いのものが多かった。 ・ 一方で、「身に覚えのないメールは開かない」、「怪しいサイトをあけない、みない」などセキュリティ上望ましくない行動を行わないといった対策を挙げる回答も多かった。
導入（66 社）	・ セキュリティ機器の導入、技術の導入などセキュリティ対策に必要なサービス、機器、ルール等を導入する内容が多かった。 ・ IT 導入補助金の申請、活用といった内容も見られた。
強化（61 社）	・ すでに行われているセキュリティ対策を強化するといった文脈が多かった。(情報管理の強化、社内教育の強化、セキュリティの強化等)
教育（59 社）	・ 社員教育、IT セキュリティ教育など、社員への情報セキュリティリテラシー向上のための教育活動をされた回答が多かった。
社員	・ 社員向けのセキュリティ教育実施、情報共有など社員を対象者とした情報セキュリティリテラシー向上活動、また、社員による情報セキュリティ向上のための取り組みを行ったという回答が多かった。
従業（51 社）	・ 従業員向けの情報共有、セキュリティ教育などの情報セキュリティリテラシー向上活動が多かった。

図 10 SECURITY ACTION 宣言における取り組み

2.3　25 項目の実施状況

2.3.1 項目別実施割合

アンケートの結果から、項目別の実施割合を図 11 に示す。アップデート(No.1)、ウイルス感染(No.2)、電子メール受信(No.6)など、外部から社内への攻撃に対する対策は実施率が高い傾向にある。これは昨今のサイバー攻撃に関する報道により、外部からの攻撃から社内を守る意識が高まっているためと考えられる。一方で事故対応(No.24)や対策の明確化(No.25)といった、インシデント発生時の報告先を明確にして共有する、社内ルールを共有するなど、情報共有に関する対策がなかなか進みにくい傾向にある。

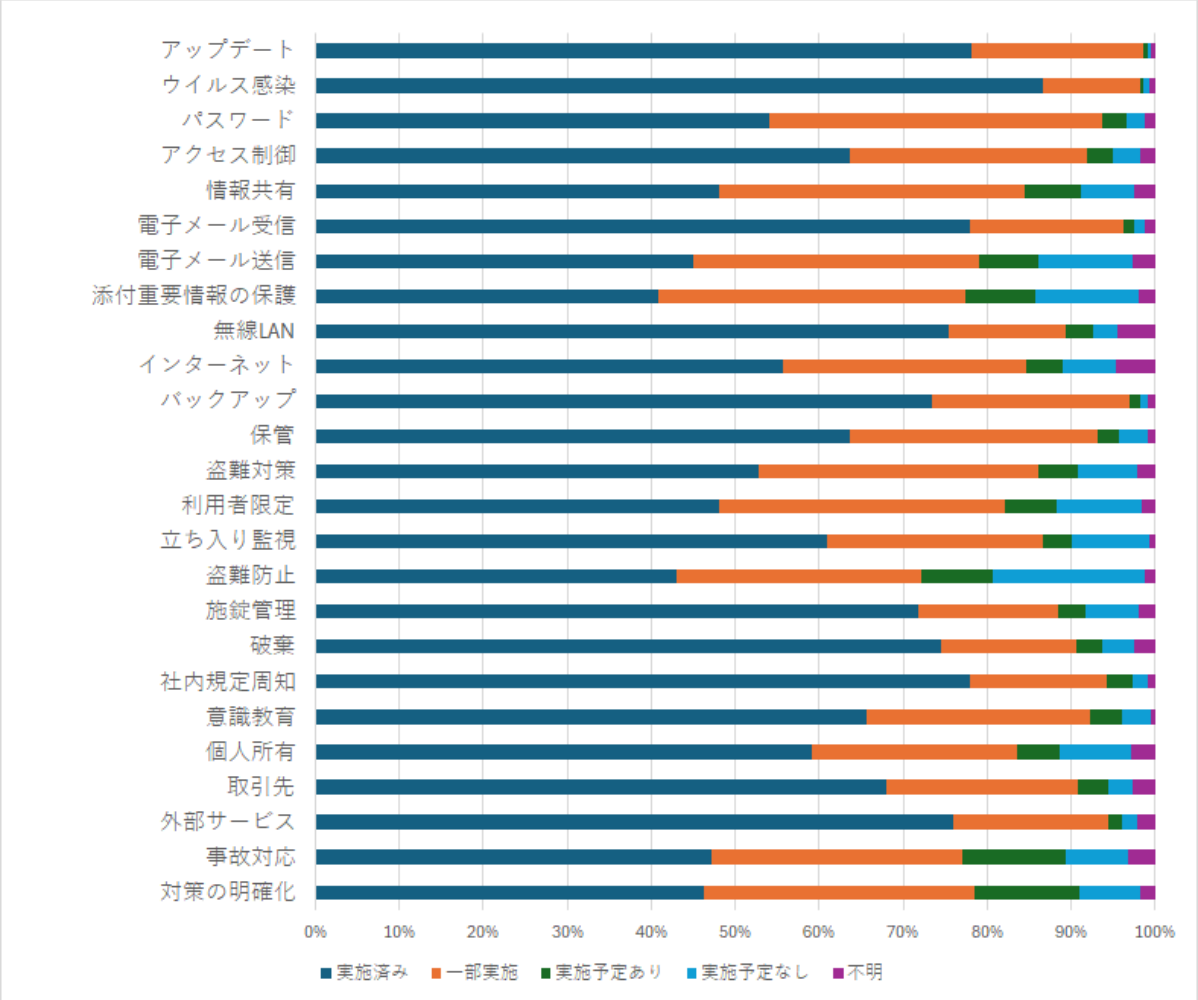


図 11　項目別実施割合

2.3.2 業種別実施状況

アンケートの結果から、有効回答数が多い上位 5 業種に絞った各項目の業種別実施割合を図 12 に示す。全体の実施済み項目割合に対して情報通信業の実施率が高い。
多角形の大きさは業種によって異なっているものの形に大きな違いはなく、全体的に実施率の低い項目は業種に関係なく実施率が低い状況となっている。

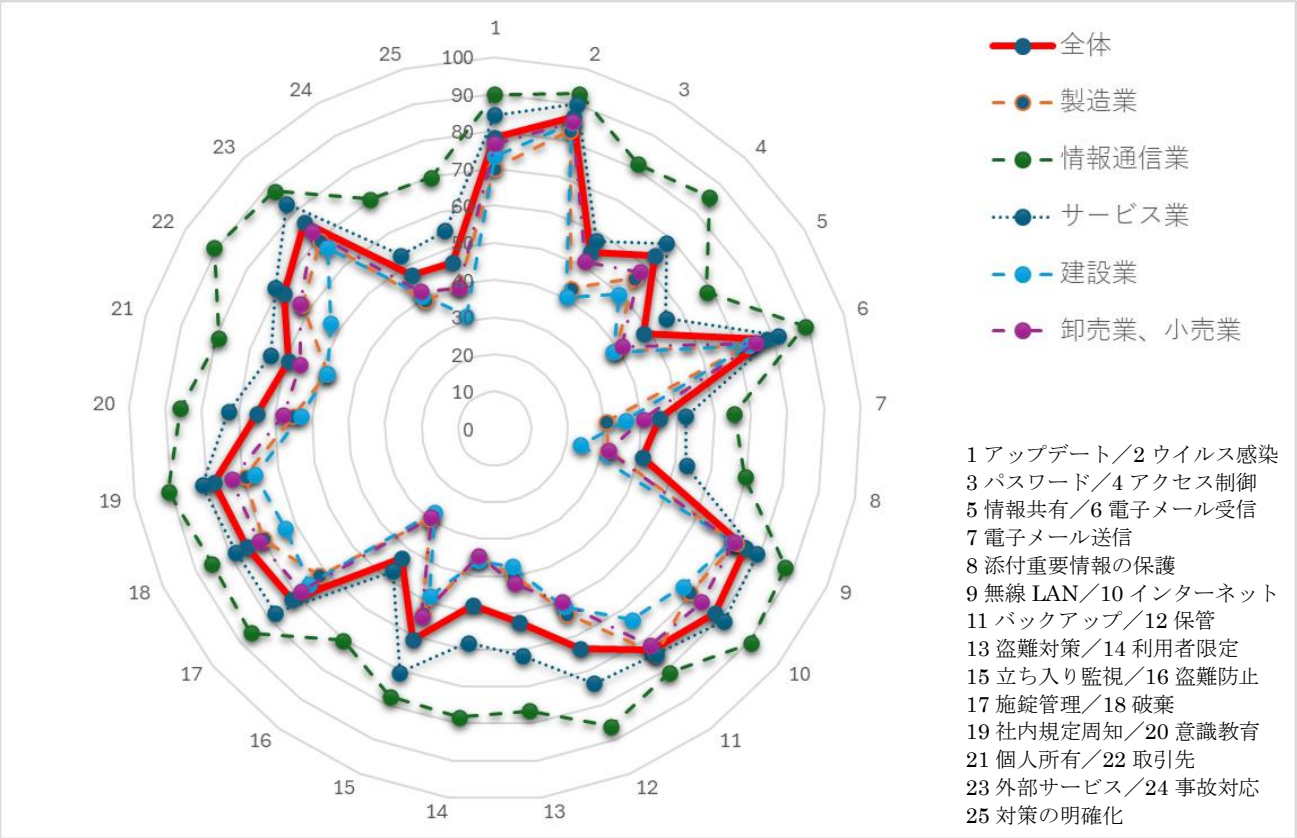


図 12 業種別の実施済み項目割合

2.3.3 項目別の実施予定がない理由

項目別に実施予定がない理由に関する回答をまとめたものを図 13 に示す。この結果、どの項目も実施にあたって「優先順位が低い」ため実施予定が立っていない状況にあり、実施にあたって「障害がある」と考えている企業数を上回っている。

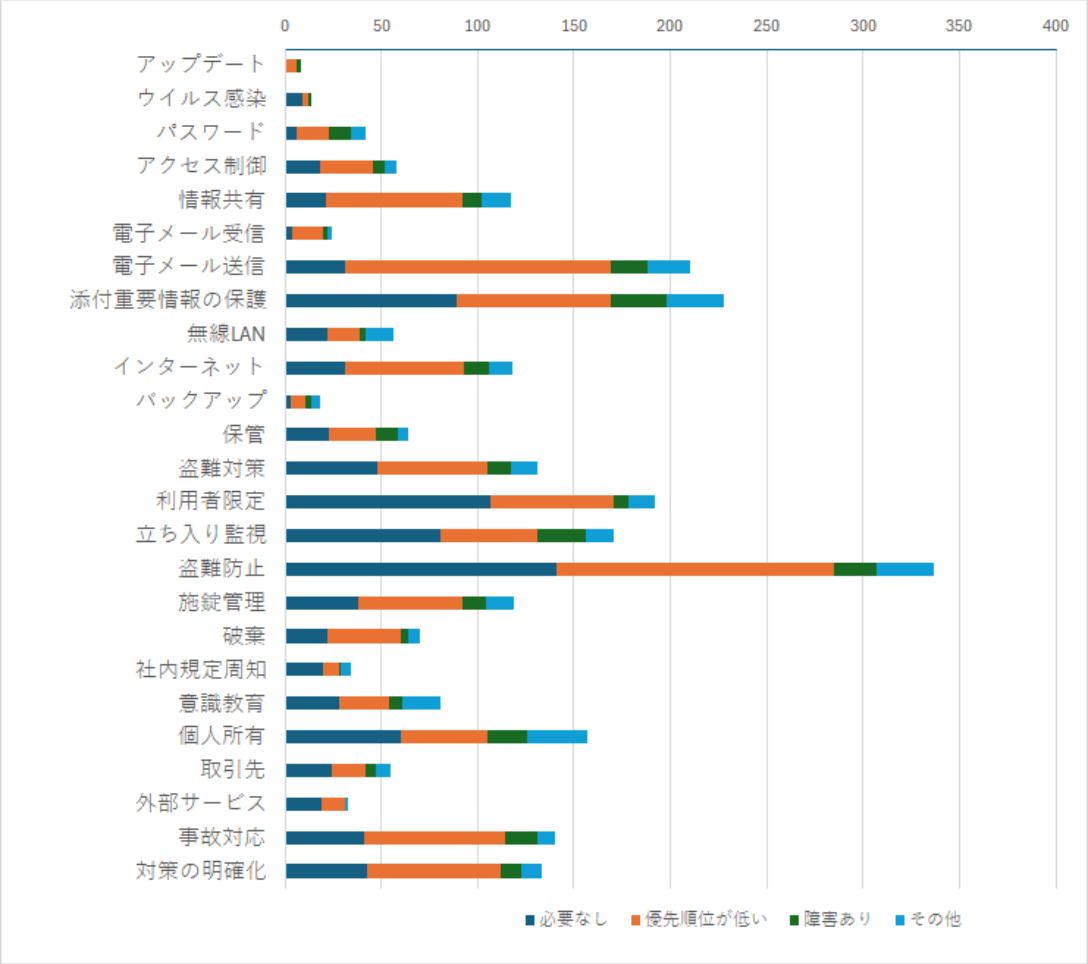


図 13 項目別に実施予定がない理由

2.3.4 必要な支援

実施に当たって障害があるとの回答について、どのような支援があれば実施できるかの回答の割合を面積の割合で表現したものを図 14 に示す。今後、必要なセキュリティ対策を行うにあたっては、「補助金」や「税制優遇」などの中小企業の導入・運用費用の負担を減らす金銭的支援とともに、「法的義務化」のような「情報セキュリティ対策を行っていることが評価される」という社会的な合意形成のための施策を求める回答も多かった。

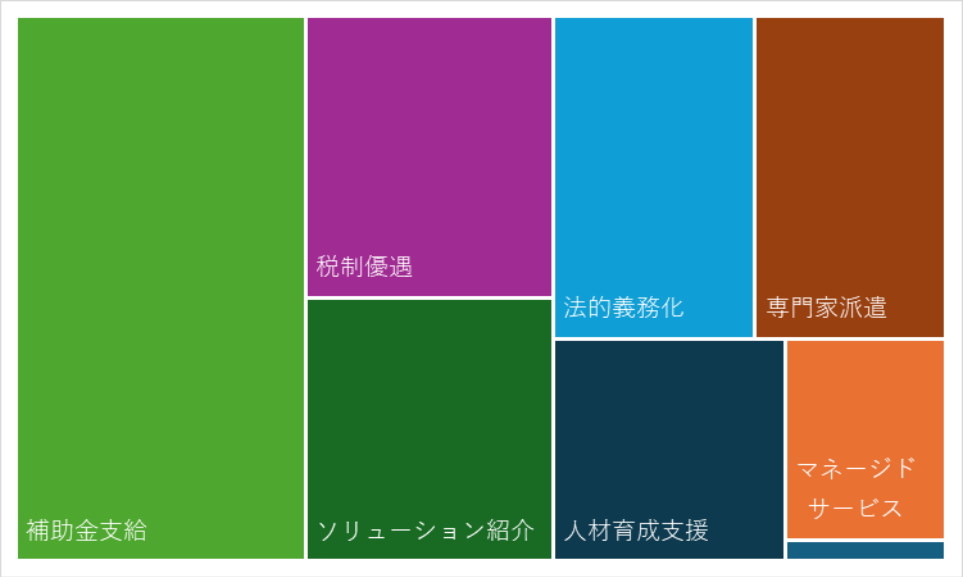


図 14 実施予定がない項目に対する必要な支援

2.4 アンケート結果に見る中小企業の情報セキュリティ対策の課題

今回のアンケート結果から、OS やソフトウェアのアップデート(No.1)、ウイルス感染(No.2)、電子メール受信(No.6)など、外部から社内への攻撃に対する対策は実施率が高い傾向にある。

基本的対策(No.1～No.5)では、パスワード(No.3)と情報共有(No.5)の実施率が低い傾向にある。パスワードの管理は、「従業員のリテラシーに依存する場合が多く、複雑なパスワードを適用できない」、「定期的に変更できない」等の課題があるとの意見があった。シングルサインオンを実現する ID 管理ツールなどの導入により、従業員の理解を得られる可能性もある。情報共有においては、まずは担当者が情報を入手し関係者で共有する手段を整えて欲しい。

従業員としての対策(No.6～No.18)では、電子メールに関して、電子メール受信(No.6)は実施率が高いが、電子メール送信(No.7)、添付重要情報の保護(No.8)は低く、中小企業では、従業員数が少ないため信頼しているのかもしれないが、ミスは起こるものであり、システム的な対策でなくても送信前に確認するなど、注意喚起・社員教育は実施して欲しい。利用者限定(No.14)、盗難防止(No.16)において、「必要なしと判断」した回答が多かった。立ち入り監視(No.15)や、施錠管理(No.17)を優先（実施）することで、盗難防止は不要と判断したのであれば、持ち出しする機器への盗難対策(No13)は実施して欲しい。

組織としての対策(No.19～No.25)では、事故対応(No.24)、対策の明確化(No.25)の実施率が低い。バックアップ(No.11)の実施率は高いので、確実にリストアできることを確認する。インシデント発生時の報告先を明確化にするなどの、対策は実施して欲しい。

実施に当たって障害があるとの回答を分析すると、費用面、社内合意の難しさ、人材不足などの問題が指摘されていて、それらに対して、補助金支給や税制優遇、法などによる対策実施の義務化、専門家派遣や人材育成支援、また、アウトソース（マネージド・サービス）を含むソリューション紹介等の支援施策の要望が寄せられた。経営層は IPA が公開している中小企業の情報セキュリティガイドラインの経営層編を理解して、リーダーシップを発揮し必要な投資をして欲しいと思うし、万一インシデントが発生した場合にその対応のために必要となるコスト(中小企業においても数千万円単位、場合によっては、億円単位の損害が発生する可能性がある[4])をイメージして欲しい。

3 ヒアリング結果

3.1 アンケート回答者へのヒアリング

アンケートの回答者に対して、さらに詳しい状況や背景を把握することを目的にヒアリングを実施した。ヒアリングでは、「5 分でできる！情報セキュリティ自社診断」の 25 項目をもとに、対応のしやすさや課題、支援のニーズなどについて具体的な意見を収集した。

3.1.1 対応するにあたって実施しやすかった項目と対応開始方法

実施しやすかった項目としては、社内 IT の刷新や事務所移転を契機に、各種対策が容易に実施された事例が挙げられた。また、施錠管理(No.17)については、周知後すぐに実施され、従業員にとってその必要性が理解しやすかったことが理由として考えられる。

ヒアリング結果（回答例）

- 社内 IT の刷新時にクラウド型メールサービスを選定したことで、電子メールの送受信対策(No.6、7）がすでに強化されており、対応が容易であった。
- 事務所移転をきっかけに事務所への立ち入り制限(No.15)が実施できた。
- 施錠管理(No.17)は、周知後にすぐに実施された。

3.1.2 対応が難しいと感じた項目あるいは見送った項目とその理由

必要だが対応が難しいと感じた項目については、人員や予算の制約、従業員の IT リテラシーの差、製品定の難しさなどが要因として挙げられた。

ヒアリング結果（回答例）

- 限られた予算と人員の中で最適なソリューションを選定することに苦労した。
- IT リテラシーが高くないため、パスワード(No.3)は複雑なパスワードの設定や定期的な更新が難しい。
- 重要書類やデータはシュレッダーで破棄(No.18)されているが、復元不可能なレベルかどうか確信が持てない。
- 社内規定周知(No.19)や意識教育(No.20)を通じてルールを守らせることに苦労した。
- 複数の選択肢の中から最適な製品を選ぶのに時間を要し、選定が容易ではなかった。
- インシデント対応体制の構築や具体的な BCP 策定は、実施が難しいと感じている。

3.1.3 対応が難しいと感じた項目への対応

対応が難しいと感じた項目への対応について、従業員にセキュリティ対策の必要性を理解してもらい、ルールを遵守してもらうことが難しいという事例が多く挙げられた。このため、必要性を理解してもらうための教育資料の作成や、従業員がセキュリティを自分事として捉えるように工夫された取り組みが行われた事例が挙げられる。

ヒアリング結果（回答例）

- 各部門に、担当を置き、社内 IT ツール刷新時に、最低限のセキュリティに関する注意事項を作成し、各部門に展開した。また、遵守事項をとりまとめた資料を作成し周知徹底した。
- ルールを守らせるために、なぜ守る必要があるのかを理解してもらうための教育資料を作成した。
- 自分事と思ってもらうために、研修の最後にセキュリティに関する目標（自分がこの 1 年注意して実施していくこと）を記述させ実践を促した。
- 巡回時に画面ロック未実施などのセキュリティ違反を確認した際には「イエローカード」を与え、複数回受けた場合には再教育を行う仕組みを導入した。
- 東京都の支援事業で専門家と共に具体化した。

3.1.4 難しい項目や見送った項目に対する必要な支援

対応が難しい項目や見送った項目に対する必要な支援について、以下のような支援があれば対応が容易になるとの意見が挙げられた。

ヒアリング結果（回答例）

- 課題を定期的に洗い出す仕組みがないため第三者の評価が欲しい。
- 中小企業にはセキュリティ専門家が不足しているため、第三者的に中立な立場でアドバイスしてくれる支援者が欲しい。その都度、相談できる支援者がいるといい。（費用的に見合えば常時サービスを受けたい）
- インシデント発生時にベンダー選定から行うのでは間に合わないため、発生時には即座に対応を開始してもらえる予約のような契約を平時に結んでおける仕組みが欲しい（平時にかかる費用は低額、実対応時には予め定めた稼働に応じた費用支払いなど）。
- 同業他社の状況を参考にしたい。
- IPA が提供する社内教育用コンテンツを知らなかった。プッシュ型で配信して欲しい。

3.1.5 対応時の情報収集

実施にあたり、情報収集では以下の事例が挙げられた。

ヒアリング結果（回答例）

- PC や IT ツール導入ベンダー、複合機導入業者に相談した。
- DM やインターネット検索を活用し気になっていることを調べた。
- 同業他社や業界の事例を調べ、最適なソリューションを見つけるための情報を集めた。
- 外部ベンダーや専門家からの意見や提案を受け、最適な製品やサービスを選定した。
- 主に IPA や SI ベンダー、クラウドサービス提供会社から情報を得ている。
- 会計システム等の外部委託業者から必要な情報を得ている。
- 社内でワーキンググループを設けて情報を持ち寄り機器の検討や決定を行った。

3.1.6 項目に含まれていないが気になっている事項

25 項目には含まれていないが、気になっている事項として、以下の事例が挙げられた。

ヒアリング結果（回答例）

- 業績向上のための EC サイト構築や SNS 活用が優先で、セキュリティ対策まで考慮に至っていない。
- クラウドサービス側でのインシデントを想定し、バックアップを含めた BCP 対策が気になっている。
- AI を使う上でのセキュリティ対策やルール作り。
- 事業に応じて影響が大きい部分を優先して脆弱性診断を実施すべき。

3.1.7 情報発信者への要望

情報発信者への要望として、以下の意見が挙げられた。

ヒアリング結果（回答例）

- 同規模の従業員数を持つ企業における、セキュリティ対策担当社員の数などについて知りたい。
- セキュリティ意識を新人も含めて全従業員数が持つ仕組みを作りたい、そのためのインシデント事例や教育的な資料があるとよい。
- IPA などから新着通知のような案内があると嬉しい。

3.2 ヒアリング結果に見る中小企業の情報セキュリティ対策の課題

今回のヒアリング結果から中小企業における情報セキュリティ対策の現状として、ヒアリング対象企業が情報セキュリティの重要性を認識し、可能な範囲で対策に取り組んでいる状況である。特に、環境変化を契機とした対策の実施や、従業員に理解しやすい対策からの着手は、限られたリソースの中で効率的にセキュリティレベルを向上させるための工夫が見られた。

一方で、リソース不足（人員・予算）や従業員の IT リテラシーのばらつきは、依然として大きな障壁として課題となっている。特に、高度な専門知識が求められる対策や、継続的な運用が必要となる対策については、実施が難しいという声が聞かれた。また、情報過多の状況下で、自社に適したソリューションを選定することの難しさに対する悩みも挙げられた。

興味深い点として、セキュリティ対策の推進において、従業員の意識改革の重要性が強く認識されていることが挙げられる。単にルールを押し付けるのではなく、「なぜ守る必要があるのか」という動機付けを重視する姿勢は、実効性の高い対策に繋がる可能性を示している。

支援ニーズからは、中小企業が外部からの専門的なサポートを切実に求めていることがわかる。特に、客観的な評価や中立的なアドバイス、インシデント発生時の迅速な対応に対するニーズは高く、自社内だけでは対応が難しい領域に対する不安の表れと言える。また、同業他社の具体的な事例や、従業員教育に活用可能なコンテンツへのニーズも顕著であり、他社の成功事例から学び、効率的に対策を進めたいという意向がうかがえる。

情報発信者への要望としては、より具体的かつ実践的な情報提供が求められている。特に、自社と同規模の企業における取り組み事例や、従業員の意識向上につながる教育コンテンツに対する関心が高い。さらに、プッシュ型の情報提供は、多忙な中小企業にとって、必要な情報をタイムリーに把握するための有効な手段であるとの評価が得られた。

中小企業における情報セキュリティ対策は、その重要性が一定程度認識されているものの、リソースや知識の制約により多くの課題を抱えているのが現状である。今後は、中小企業の実情に即した、費用対効果の高い支援策や情報提供が不可欠である。情報発信側は、プッシュ型の情報提供や、具体的な成功事例に基づいたコンテンツの充実を図ることで、中小企業のセキュリティ対策推進をより一層後押しできると考えられる。

4　調査に基づく考察

JNSA 中小企業支援施策ワーキンググループでは、「中小企業の情報セキュリティ対策導入を促進する官民による支援施策について[5]」、「中小企業向け情報セキュリティ対策ガイドラインの作成と運用において考慮すべき要件についての考察と提案[6]」を公表し、中小企業が情報セキュリティ対策を向上させる支援策を検討してきた。これらは、支援者側の視点であり、今回のアンケートにより中小企業のセキュリティに対する実態を理解し、関係者と連携して中小企業にとって、より効果的な支援策を検討するための有益な回答を頂いた。

アンケート・ヒアリングを通じて、ある程度の対策ができている企業・業種がある一方で、特定の対策ができていない項目があることが見えてきた。

情報通信業、金融業、および保険業の実施率が高かった。これは、個人情報など情報の保有数や過去の同業他社でのインシデントや監督官庁の指導が影響しているものと想定される。反面、建設業、製造業、卸売業、および小売業などは全般的に実施率が低かった。業界特有の習慣や業務状況に応じ、業界団体と連携したセキュリティガイドライン策定などの支援も必要と思われる。

業種や企業規模を問わずサイバー攻撃等を受ける状況を考慮し、全ての企業において、セキュリティ対策の底上げを一層進める必要があると考える。

また、実施にあたって障害がある場合、その理由を自由記述にて回答して頂いた。その中で工夫次第で実現できる項目もあるように見受けられた。例えば、情報共有(No.5)では、全従業員への情報共有が最終目的だが、まずは担当者同士で共有すべきである。ヒアリングした企業では、部署ごとに IT 担当を指定して情報システム担当と、部署ごとの担当で情報共有している事例もあった。

立ち入り監視(No.15)では、事務所内に商談エリアがある等、制限があると挙げられたが、事務所に外部の方が入室した際に履歴を残せばよい等の軽易な対策から進める方法を知らしめることもあると考えられる。

各項目に対し、高レベルの対策を求められていると担当者が認識し、実現できていないと回答した企業もあると思われる。25 項目について実施しない場合のリスクを認識し、実施するレベルをコントロールすることで、残っているリスクを認識・共有することが重要であり、定期的に見直してできることから対処すべきである。

情報セキュリティ対策の目的は、企業の経営、事業を継続し、ステークスホルダーの利益や権利を守ることである。中小企業であっても、経営層が積極的に取り組む姿勢が不可欠である。そのためには、自社における情報セキュリティ対策のインセンティブ（経営上のメリットとして現れる実施することで得られる便益・実施しないことでリスクとして負う費用)、とミッション（実施することが社会的責任として評価される）を検討すべきである。

実施における課題として上げられた内容の多くは、費用と情報が不足していると感じられる。特に、必要となる情報のうち、対策により実現できる効果など経営層・従業員に理解してもらうための情報、費用を押さえて実現できる対策や運用負担を抑える対策に関する情報、実現するためのソリューションに関する情報などが不足しているように思われる。自社で運用できるレベルのセキュリティ対策に関する情報も不足しており、これらは IT やセキュリティを専門としない中小企業の担当者では入手が難しいとあらためて認識した。
JNSA をはじめ支援者は、中小企業の経営層・担当者へ向けた情報の提供と、相談される関係を構築し、中小企業のセキュリティ対策実現のため、支援方法を検討し、支援を継続することが求められている。

実施にあたって必要な支援として、「補助金」や「税制優遇」や「法的義務化」を求める意見が多い背景には、費用や作業の発生が伴うことから、実施のための社内向けの説明が難しいことが課題となっている可能性がある。「法的義務化」は強制力があるため、こうした要望が出ているのではないかと想像できる。経営層、従業員の理解を得られるよう、社員教育や同業他社でのインシデントの共有など、まずはできることから実施すべきである

行政機関、IPA や JNSA など支援団体に対しては、経営層向けの呼びかけ（インセンティブを理解してもらう)、社会もしくは業界団体に対するミッション(社会的責任)の形成を継続的に実施していくことを期待する。

対策の支援では、対策の必要性は理解していても、「実際に何をすればよいのかわからない」などの回答が多数あった。自社に適した対策のアドバイスを求めている企業も多く、知識による支援（IPA の啓発資料など)、財務的な支援（補助金など)、人的な支援（専門家派遣など）技術的な支援（ツールやサービスの提供など）を JNSA 中小企業支援施策ワーキンググループでも IT ベンダー、行政機関、業界団体などと連携して幅広い支援を実施していきたい。

本報告書が、中小企業のセキュリティ向上のため、中小企業の経営者・担当者、およびセキュリティソリューションを提供するメーカー・SI 事業者その他支援者の参考になることを願っている。

謝辞

本報告書の作成に当たっては、多くの方々からのご協力をいただきました。ここに記して、深甚なる感謝の意を表します。
実態調査アンケート回答いただいた企業の皆様には、本趣旨をご理解いただき、情報セキュリティ自社診断について、アンケート、およびヒアリングなどにご協力いただきました。
IPA には、本実態調査アンケートについて、SECURITY ACTION 二つ星宣言事業者に対する回答依頼メールの配信、および趣旨に基づいた必要なアンケートの実施等のご協力をいただきました。

執筆メンバー
リーダー
古川　英規（株式会社 RS コネクト）
メンバー（五十音順）
安樂　啓之（インフォテック株式会社）
岩本　真人（トレンドマイクロ株式会社）
助川　賢二（ユニアデックス株式会社）
本多　規克（アルプス システム インテグレーション株式会社）

※この報告書は、JNSA 社会活動部会 中小企業支援ワーキンググループとしてとりまとめたものであり、所属企業・団体の立場、見解等を代表するものではありません。

参考文献

[1] NPO 日本ネットワークセキュリティ協会「インシデント損害額調査レポート 第 2 版」,
https://www.jnsa.org/result/incidentdamage/data/2024-1.pdf
[2] 独立行政法人情報処理推進機構「中小企業の情報セキュリティ対策ガイドライン」,
https://www.ipa.go.jp/security/guide/sme/about.html
[3] 独立行政法人情報処理推進機構「5 分でできる！情報セキュリティ自社診断」,
https://www.ipa.go.jp/security/guide/sme/5minutes.html
[4] NPO 日本ネットワークセキュリティ協会, 「サイバー攻撃を受けるとお金がかかる ～インシデント損害額調査レポートから考えるサイバー攻撃の被害額～」,
https://www.jnsa.org/result/incidentdamage/202407.html
[5] NPO 日本ネットワークセキュリティ協会「中小企業の情報セキュリティ対策導入を促進する官民による支援施策について」,
https://www.jnsa.org/result/act/2021/2021-001.pdf
[6] NPO 日本ネットワークセキュリティ協会「中小企業向け情報セキュリティ対策ガイドラインの作成と運用において考慮すべき要件についての考察と提案」,
https://www.jnsa.org/result/act/2022/2022-001.pdf

別紙：

1　「5 分でできる！情報セキュリティ自社診断」項目名

No	大分類	アンケートと本報告書で用いた「5 分でできる！情報セキュリティ自社診断（Excel 版）」での表記		「中小企業の情報セキュリティ対策ガイドラインサイト」の「付録 3：5 分でできる！情報セキュリティ自社診断」（PDF 版）での表記	
		項目名	診断内容	項目名	診断内容
1	基本的対策	アップデート	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？	脆弱性対策	OS やソフトウェアは常に最新の状態にする
2		ウイルス感染	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？ （※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）	ウイルス対策	ウイルス対策ソフトを導入し適切に管理する
3		パスワード	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？	パスワード管理	強固なパスワードを使用する
4		アクセス制御	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？ （※2:”重要情報”とは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）	機器の設定	共有設定を見直す
5		情報共有	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？	情報収集	脅威や攻撃の手口を知り、対策に生かす。
6	従業員としての対策	電子メール受信	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？	電子メールのルール	身に覚えのない電子メールは疑がってみる
7		電子メール送信	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？	電子メールのルール	宛先の送信ミスを防ぐ
8		添付重要情報の保護	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？	電子メールのルール	重要情報を送信するときは保護する
9		無線 LAN	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？	無線 LAN のルール	無線 LAN の盗聴や無断使用を防ぐ無線 LA を送信するときは保護する
10		インターネット	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？	インターネット利用のルール	インターネットを介したトラブルを防ぐ
11		バックアップ	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？	バックアップのルール	バックアップを励行する
12		保管	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？	保管のルール	重要情報の放置を禁止する
13		盗難対策	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？	持ち出しのルール	重要情報は安全な方法で持ち出す

No	大分類	アンケートと本報告書で用いた「5 分でできる！情報セキュリティ自社診断(Excel 版)」での表記		「中小企業の情報セキュリティ対策ガイドラインサイト」の「付録 3：5 分でできる！情報セキュリティ自社診断」（PDF 版）での表記	
		項目名	診断内容	項目名	診断内容
14	従業員としての対策	利用者限定	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？	事務所の安全管理	機器を勝手に操作させない
15		立ち入り監視	関係者以外の事務所への立ち入りを制限していますか？	事務所の安全管理	見知らぬ人には声をかける
16		盗難防止	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？	事務所の安全管理	機器・備品の盗難防止対策を行う
17		施錠管理	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？	事務所の安全管理	オフィスの戸締まりに気を配る
18		破棄	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？	情報の安全な処分	重要情報は復元できないように消去する
19	組織としての対策	社内規定周知	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？	守秘義務の周知	従業員に守秘義務について理解してもらう
20		意識教育	従業員にセキュリティに関する教育や注意喚起を行っていますか？	従業員教育	従業員に情報セキュリティ教育を行う
21		個人所有	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？	私物機器の利用	個人所有端末の業務での利用可否を決める
22		取引先	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？	取引先管理	取引先に秘密保持を要請する
23		外部サービス	クラウドサービスやウェブサイトの運用など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？	外部サービスの利用	信頼できる外部サービスを使う
24		事故対応	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？	事故への備え	事故発生に備えて事前に準備する
25		対策の明確化	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？	ルールの整備	情報セキュリティ対策をルール化する

2　業種別実施状況詳細

単位：%

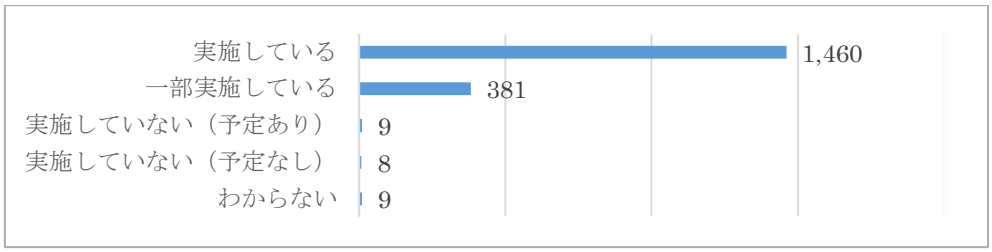
	業種(有効回答数)	全体 (1,867)	製造業 (367)	情報通信業 (298)	サービス業 (224)	建設業 (198)	卸売業、小売業 (197)	学術研究、専門・技術サービス業 (188)	医療、福祉 (143)	金融業、保険業 (43)	不動産業、物品賃貸業 (42)
1	アップデート	78.2	70.0	89.9	84.4	73.2	76.7	85.6	69.2	79.1	69.1
2	ウイルス感染	86.7	82.8	93.0	90.2	84.9	85.3	94.2	80.4	93.0	81.0
3	パスワード	54.1	43.1	81.2	57.6	40.4	51.3	54.8	40.6	79.1	59.5
4	アクセス制御	63.7	55.6	85.6	68.3	49.5	57.9	68.6	58.0	69.8	61.9
5	情報共有	48.0	39.0	68.5	55.4	38.4	41.1	52.1	33.6	81.4	40.5
6	電子メール受信	77.9	72.8	88.9	81.3	72.7	74.6	84.0	72.0	95.4	73.8
7	電子メール送信	45.0	30.5	65.4	52.2	35.9	40.6	54.8	35.7	83.7	42.9
8	添付重要情報の保護	40.9	31.3	69.5	53.1	23.7	31.5	39.9	25.9	81.4	33.3
9	無線 LAN	75.4	72.8	87.6	79.0	71.7	72.1	73.9	68.5	93.0	69.1
10	インターネット	77.9	69.2	90.6	81.3	66.7	73.1	78.2	86.0	97.7	76.2
11	バックアップ	73.4	74.9	81.2	75.0	63.6	72.1	76.6	70.6	72.1	69.1
12	保管	63.6	53.7	86.2	73.7	51.5	50.3	64.9	53.2	95.4	57.1
13	盗難対策	52.7	39.8	76.5	61.6	37.4	42.1	52.1	52.5	88.4	47.6
14	利用者限定	48.0	34.9	78.2	58.0	35.9	34.5	51.1	40.6	65.1	38.1
15	立ち入り監視	61.0	53.4	77.5	70.5	48.5	54.3	68.1	53.2	76.7	57.1
16	盗難防止	43.0	30.0	70.5	47.3	27.8	29.4	43.1	40.6	88.4	42.9
17	施錠管理	71.9	62.1	86.2	77.7	65.7	68.5	73.4	65.0	90.7	73.8
18	破棄	74.6	69.8	85.2	78.1	63.1	71.1	80.9	70.6	97.7	61.9
19	社内規定周知	77.9	69.2	90.6	81.3	66.7	73.1	78.2	86.0	97.7	76.2
20	意識教育	65.0	55.0	85.9	72.8	53.0	57.9	67.0	58.0	90.7	61.9
21	個人所有	59.2	48.0	79.2	64.3	48.0	55.8	62.2	54.6	83.7	59.5
22	取引先	68.0	62.1	90.6	71.0	53.0	62.9	73.4	59.4	76.7	57.1
23	外部サービス	76.1	69.5	87.6	83.0	66.7	72.6	82.5	71.3	93.0	64.3
24	事故対応	47.2	39.2	70.5	53.1	40.9	42.1	41.0	43.4	79.1	26.2
25	対策の明確化	46.2	39.5	69.8	54.9	31.3	39.1	44.7	37.1	74.4	35.7

3　各項目のアンケート結果

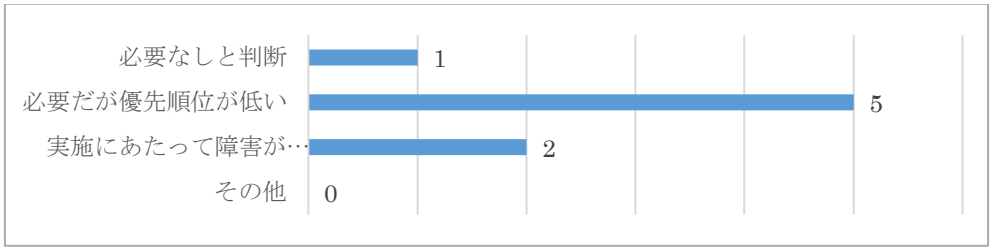
3.1　【No.1】アップデート

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るか。

3.1.1 実施状況



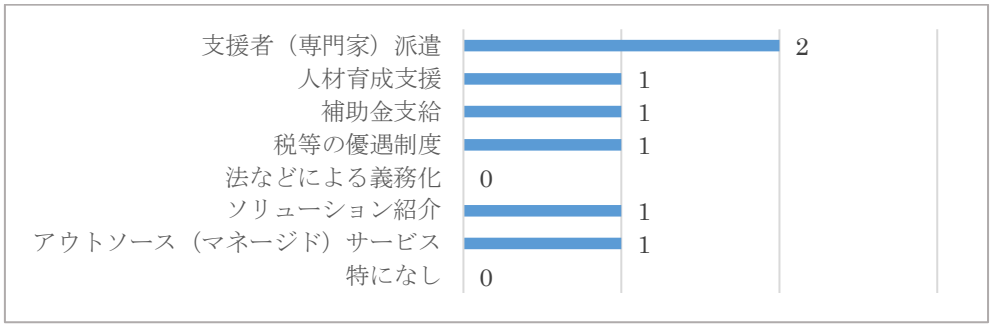
3.1.2 実施していない（予定なし）の理由



3.1.3 具体的な障害の内容

・　利用が必要なソフトウェアが最新版に対応していない

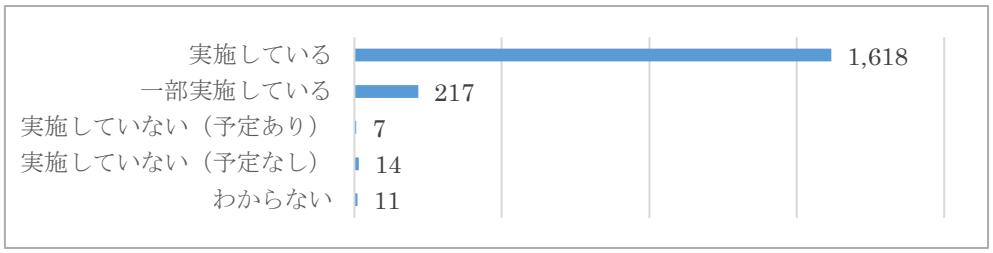
3.1.4 どのような支援施策があれば実施できそうか



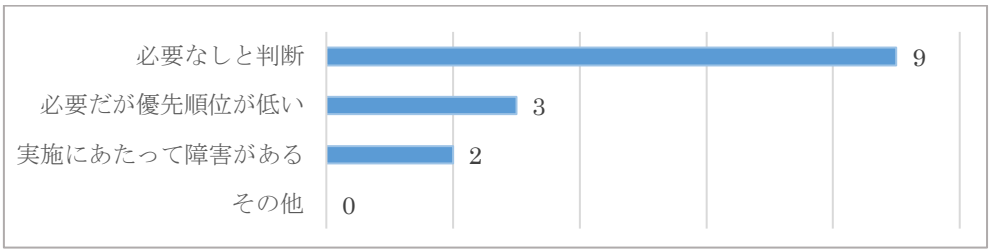
3.2 【No.2】ウイルス感染

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する

3.2.1 実施状況



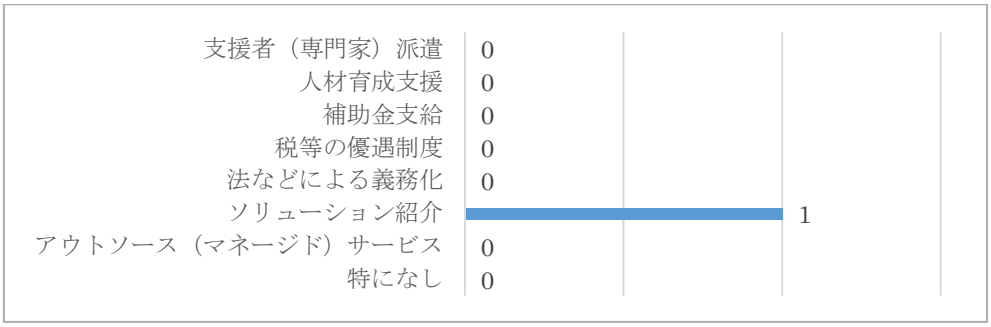
3.2.2 実施していない（予定なし）の理由



3.2.3 具体的な障害の内容

・ Mac のセキュリティソフトの動作が不安定

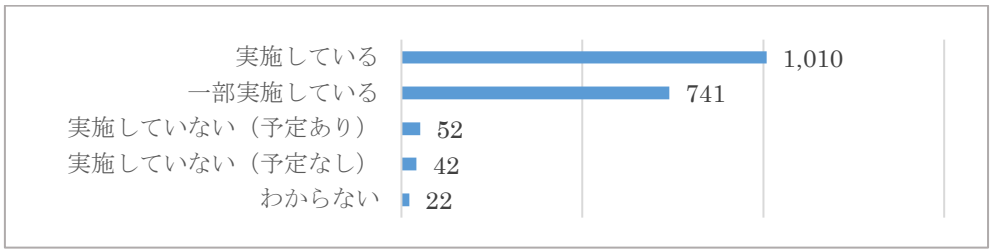
3.2.4 どのような支援施策があれば実施できそうか



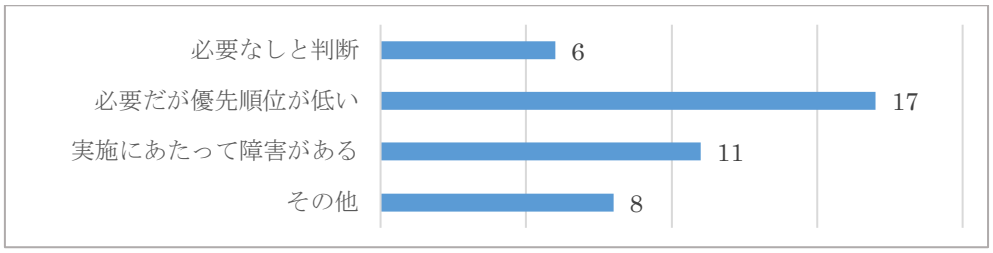
3.3 【No.3】パスワード

パスワードは破られにくい「長く」「複雑な」パスワードを設定する

3.3.1 実施状況



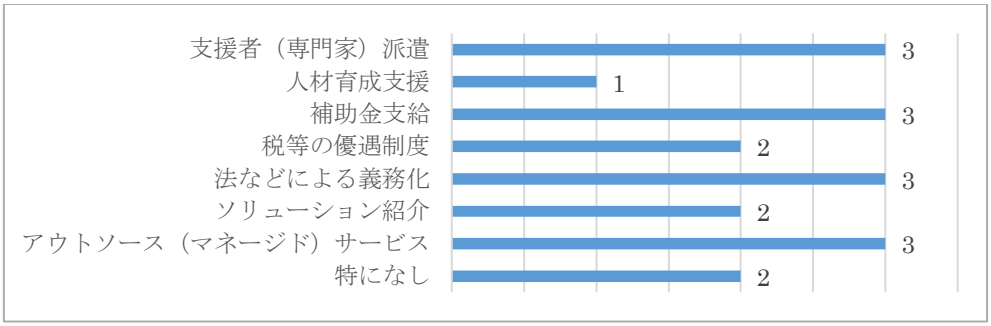
3.3.2 実施していない（予定なし）の理由



3.3.3 具体的な障害の内容

- 社内合意が得られない／合意が難しい
- 長く複雑なパスワードだと、紙でパスワードを張り出してしまう
- 管理するパスワードの数が増大している
- IT リテラシーの低い人に水準を合わせる必要がある

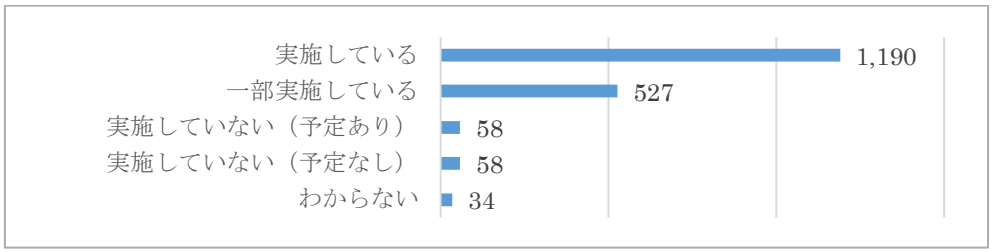
3.3.4 どのような支援施策があれば実施できそうか



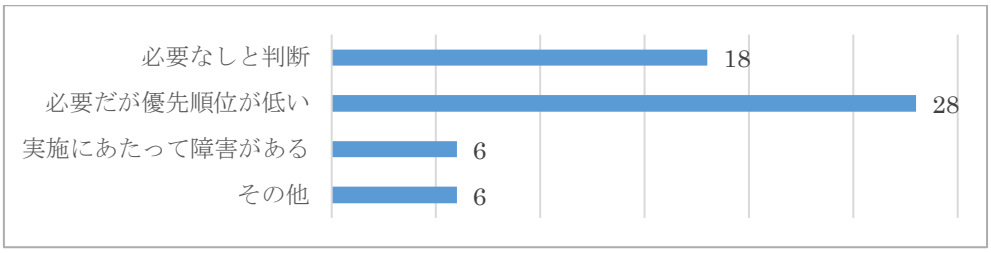
3.4 【No.4】アクセス制御

重要情報に対する適切なアクセス制限を行う

3.4.1 実施状況



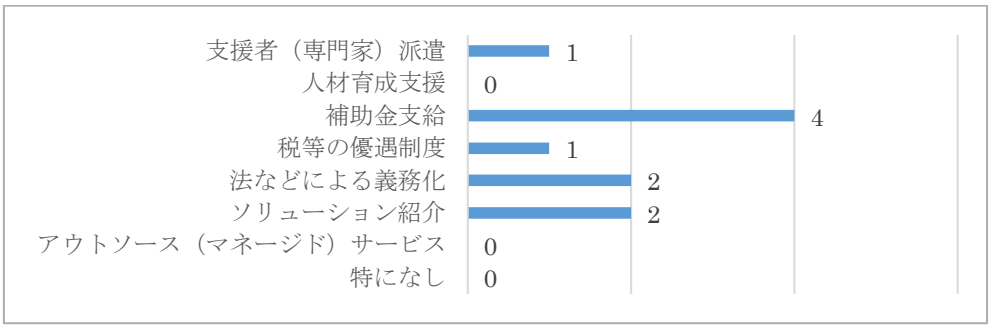
3.4.2 実施していない（予定なし）の理由



3.4.3 具体的な障害の内容

- 費用の問題がある
- ソフト導入のためのコストと実態が見合わない
- ソフトウェアの利用に不具合が出る
- 社内の合意が得られない
- 社内での知識不足などにより、現在のものを変更することの合意が得られないと考える。変更できても担当者に負担がかかり他の仕事に影響が出る

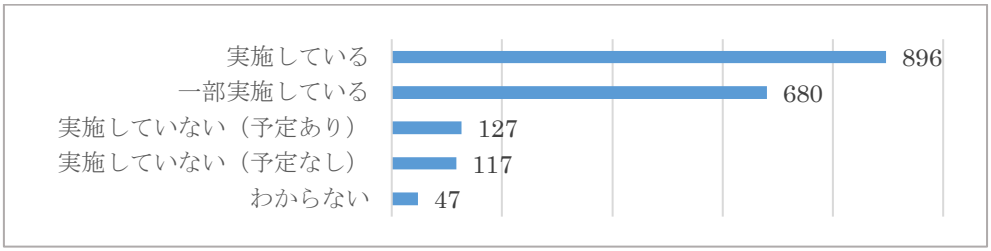
3.4.4 どのような支援施策があれば実施できそうか



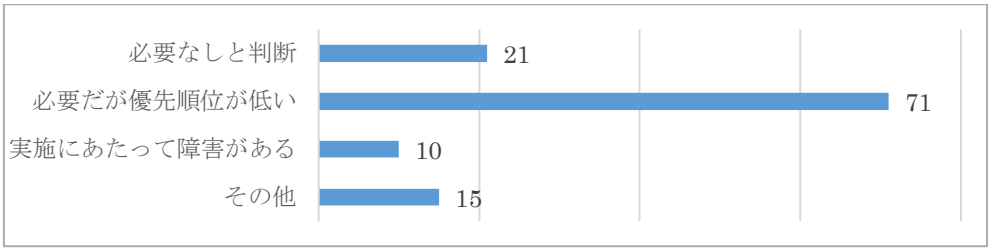
3.5 【No.5】情報共有

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がある

3.5.1 実施状況



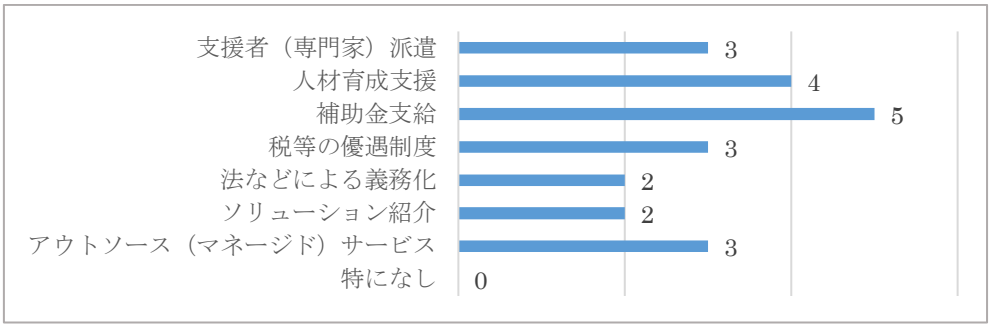
3.5.2 実施していない（予定なし）の理由



3.5.3 具体的な障害の内容

- 共有するシステムが無い、個々のパソコンと社内ネットワークを切り離している
- 情報の入手先とリソース不足
- 仕組みづくりがわからない
- 専門家に任せるのも一つの解決方法だろうが、金銭的、時間的負担が重すぎる。最近はリモートや電話で済まされることも多く、こちら側にもある程度の知識が必要とされる
- 資金面の問題あり
- どうやって対策や仕組みをつくればいいのかわからないし、担当できる人材もいない

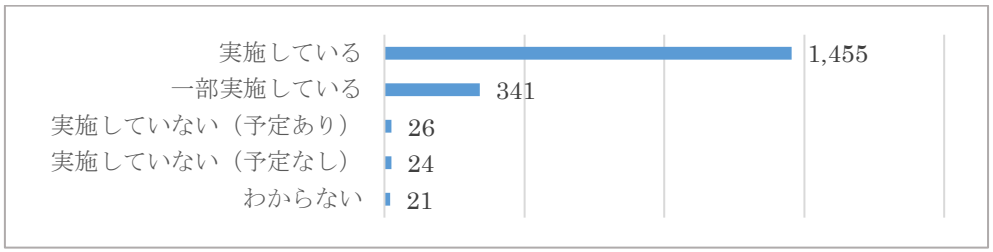
3.5.4 どのような支援施策があれば実施できそうか



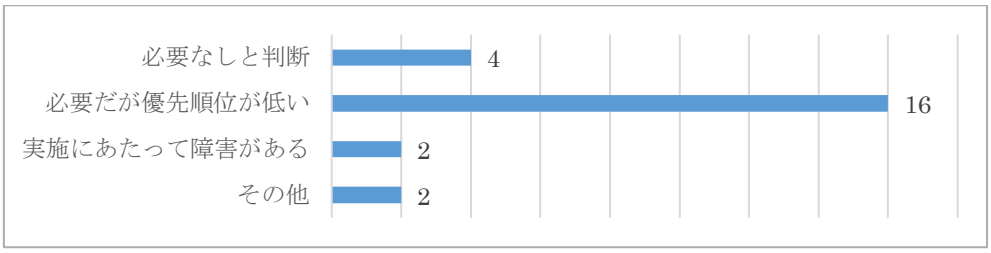
3.6 【No.6】電子メール受信

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る

3.6.1 実施状況



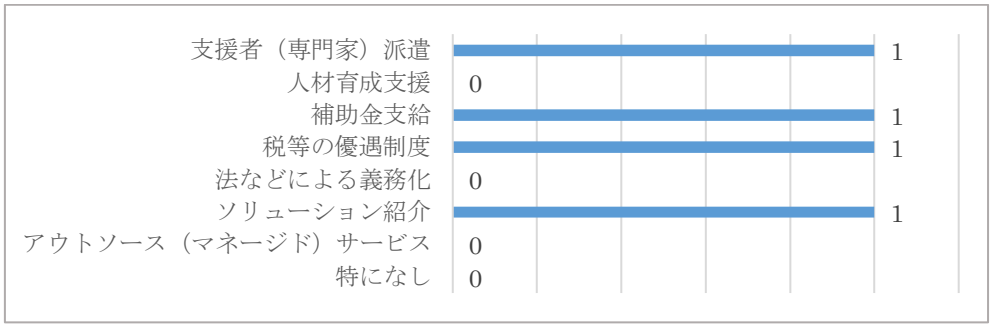
3.6.2 実施していない（予定なし）の理由



3.6.3 具体的な障害の内容

- フリーメールを利用しているフリーランスとの取引が多く、制御すると業務遂行に支障が出るため
- 資金面の問題あり

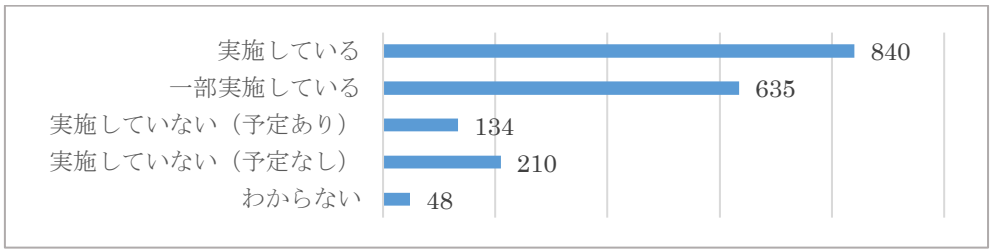
3.6.4 どのような支援施策があれば実施できそうか



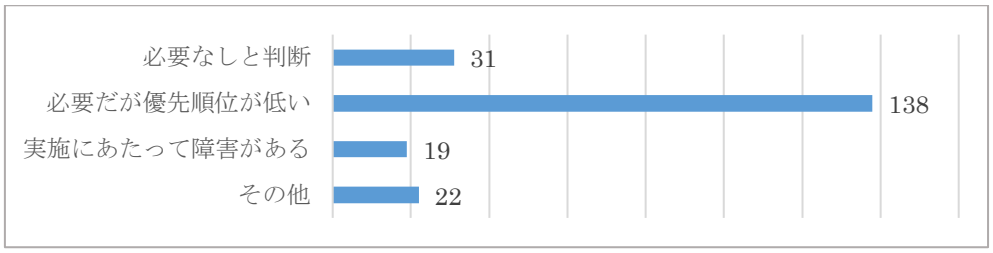
3.7 【No.7】電子メール送信

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する

3.7.1 実施状況



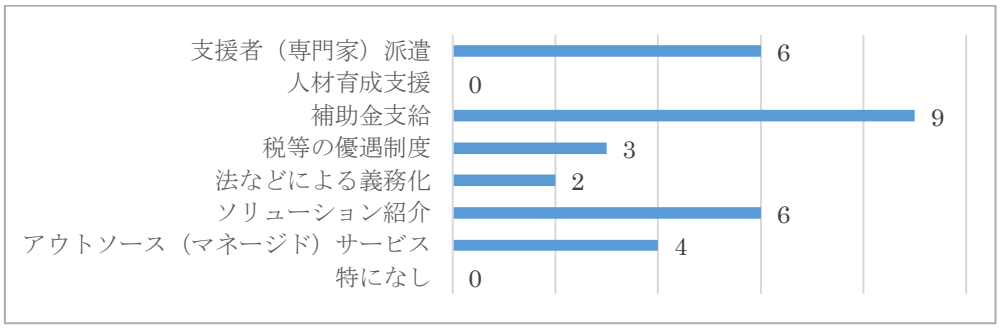
3.7.2 実施していない（予定なし）の理由



3.7.3 具体的な障害の内容

- システム対応するための知識の不足（具体的な対策方法が分からない等）
- リソース（人、資産）不足による社内ルールの未整備
- 具体的なソリューションがわからない
- 利用しているサービスにて、メールの誤送信対策機能として、送信保留、あるいは上司による事前承認機能があるが、複雑である、即時に送信できない等が問題となり、機能が利用できない

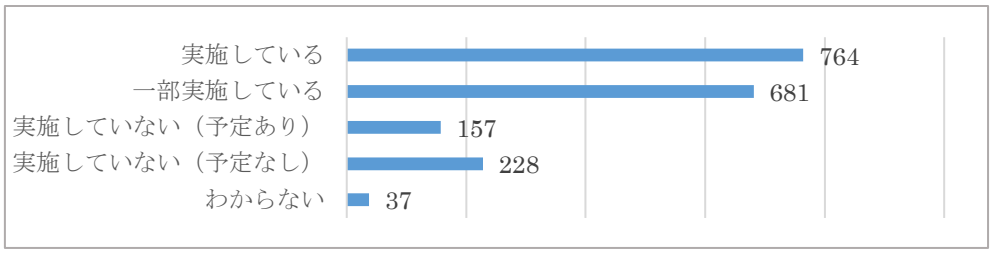
3.7.4 どのような支援施策があれば実施できそうか



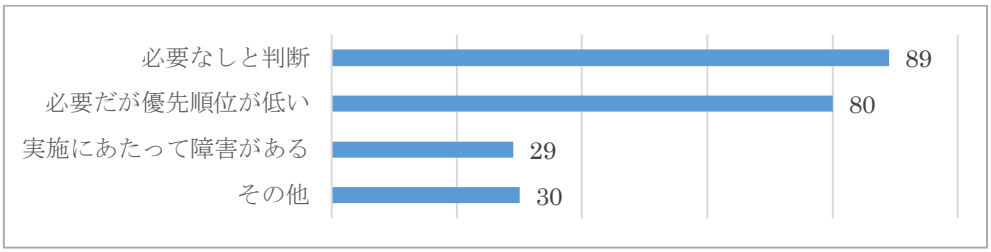
3.8 【No.8】添付重要情報の保護

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する

3.8.1 実施状況



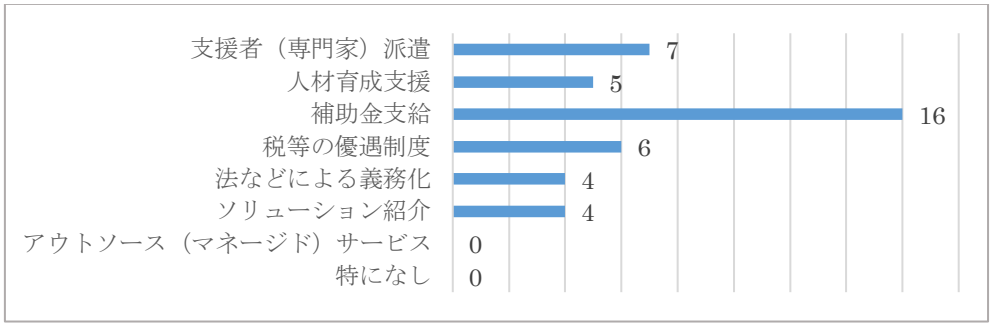
3.8.2 実施していない（予定なし）の理由



3.8.3 具体的な障害の内容

- 添付ファイルをパスワードで暗号化するとマルウェアのスキャンができないため、メールによる重要書類の送付はしていない
- 官公庁はパスワードで暗号化された添付ファイルの提出に難色を示す。
- 重要な情報のやり取りは、対面での受け渡しとしている
- 顧客の理解が得られない、あるいは顧客の対応が期待できないので、導入に踏み切れない

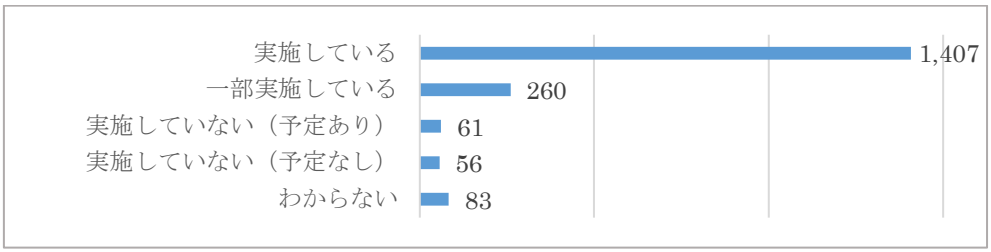
3.8.4 どのような支援施策があれば実施できそうか



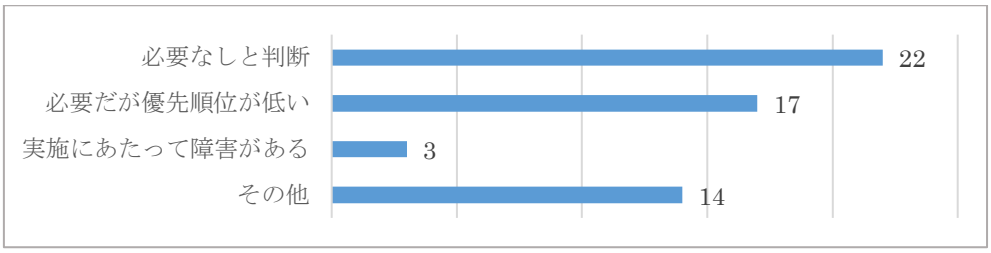
3.9 【No.9】無線 LAN

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する

3.9.1 実施状況



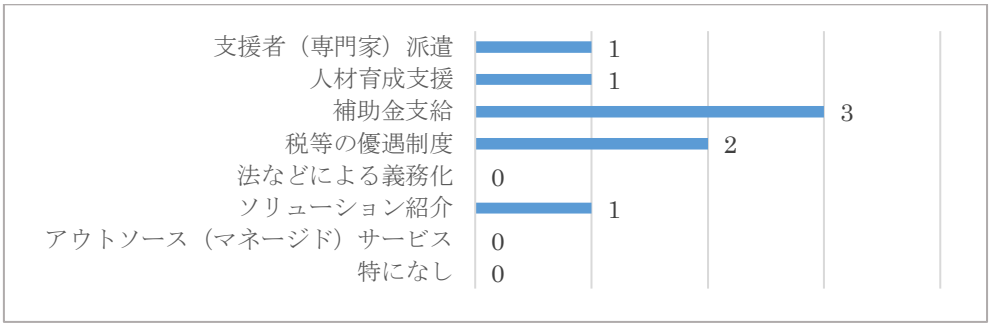
3.9.2 実施していない（予定なし）の理由



3.9.3 具体的な障害の内容

- 資金面の問題があり導入できない
- 有償のサービスの利用が難しい

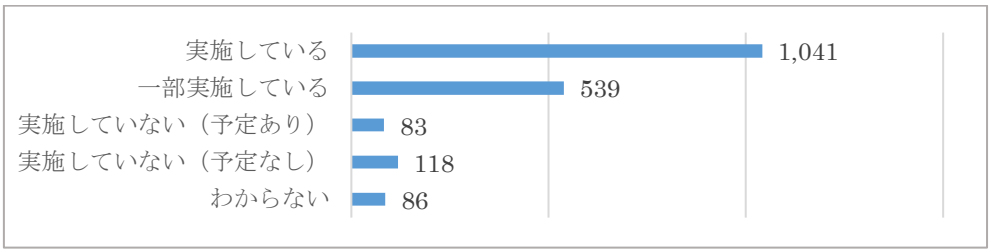
3.9.4 どのような支援施策があれば実施できそうか



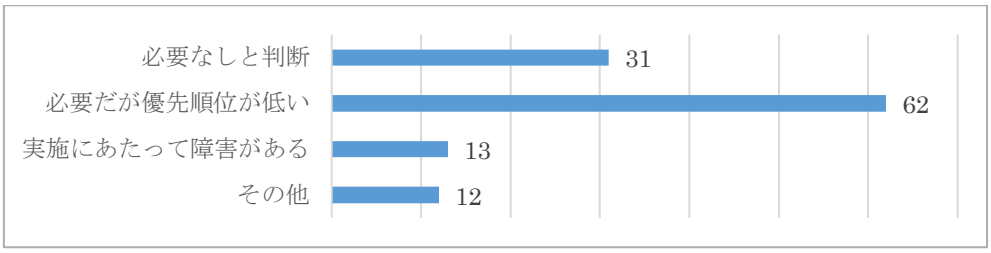
3.10 【No.10】インターネット

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行う

3.10.1実施状況



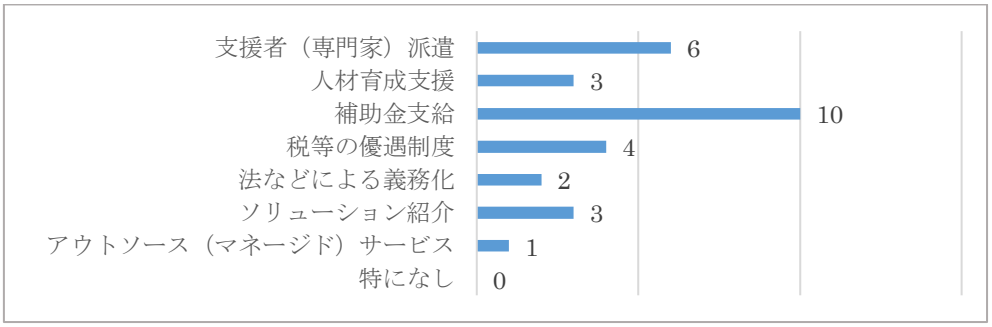
3.10.2実施していない（予定なし）の理由



3.10.3具体的な障害の内容

- 何をすればいいのかがわからない
- 対応できる人材がいない
- 在宅勤務者を考慮すると、システム的な解決策を取ろうとするとリソース（人、費用）が必要となるため、社員への注意喚起のみとしている
- SNS運用リスクについて、経営層の理解が得られない

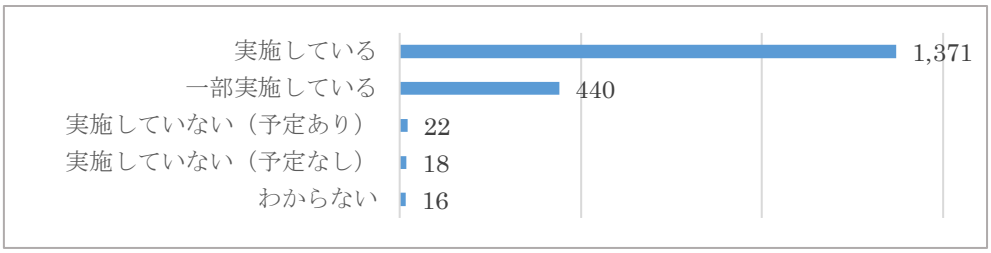
3.10.4どのような支援施策があれば実施できそうか



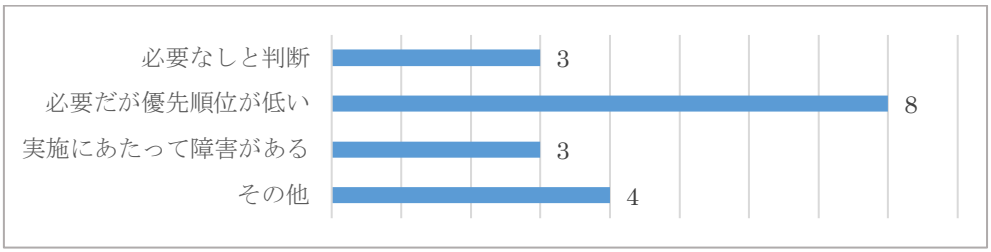
3.11 【No.11】バックアップ

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する

3.11.1 実施状況



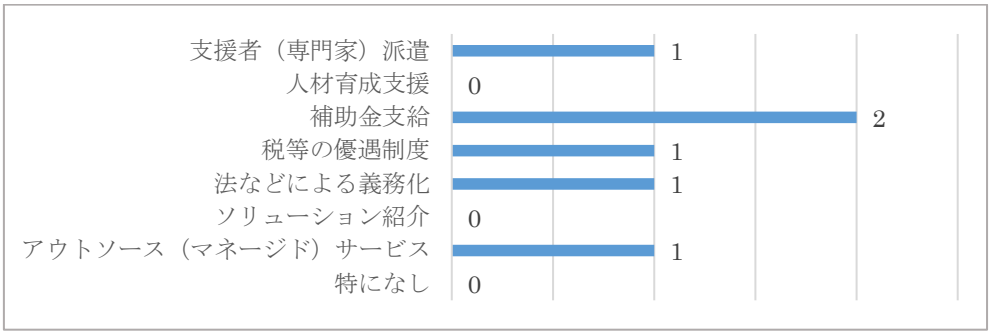
3.11.2 実施していない（予定なし）の理由



3.11.3 具体的な障害の内容

- リソース（人、費用）が不足しているため実施できない
- 導入のための進め方がわからない。また、対応できる人材がいない

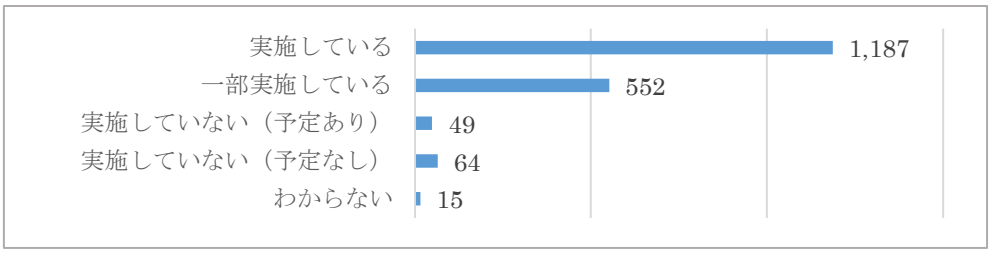
3.11.4 どのような支援施策があれば実施できそうか



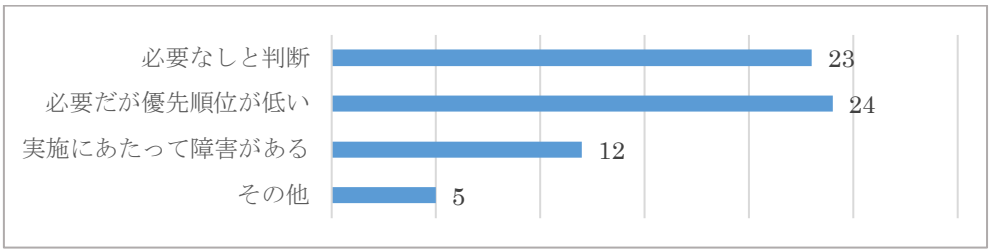
3.12 【No.12】保管

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する

3.12.1 実施状況



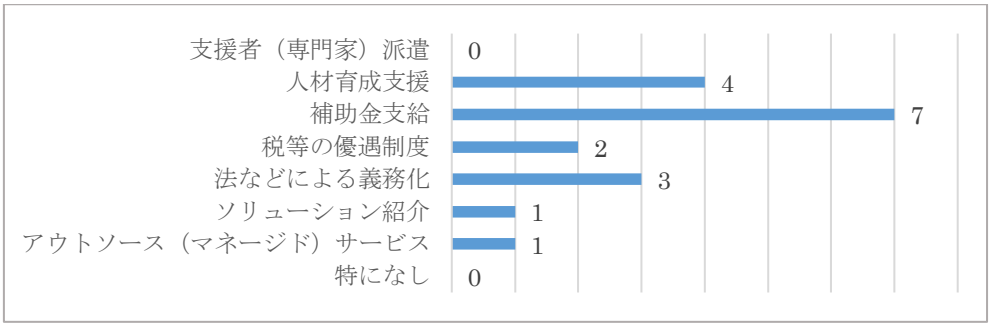
3.12.2 実施していない（予定なし）の理由



3.12.3 具体的な障害の内容

- 費用対効果（保管先が自宅の場合など）、および責任分界点の設定（外部委託の場合など）に課題がある
- 情報漏洩に対する危機意識が低い。また、導入を強制的に進めても、社内の理解が得らない。無理に進めると、問題のある運用などが水面下で行われる可能性がある
- 必要なスペース、社内ルールの検討などが必要であり、そのための費用が発生するので、推進が難しい
- リモートワークの場合などの個別のケースがあり、それらを考慮した対応策が分からない
- 個人のセキュリティ意識の低さから、徹底できない

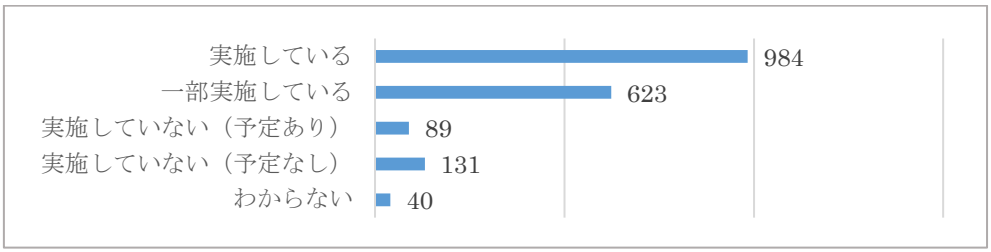
3.12.4 どのような支援施策があれば実施できそうか



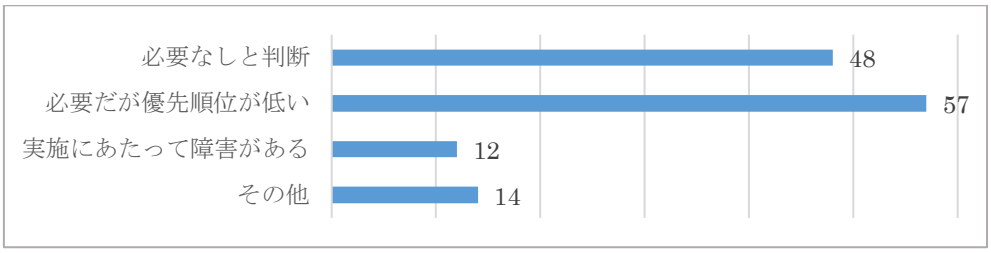
3.13 【No.13】盗難（情報漏えい）対策

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

3.13.1 実施状況



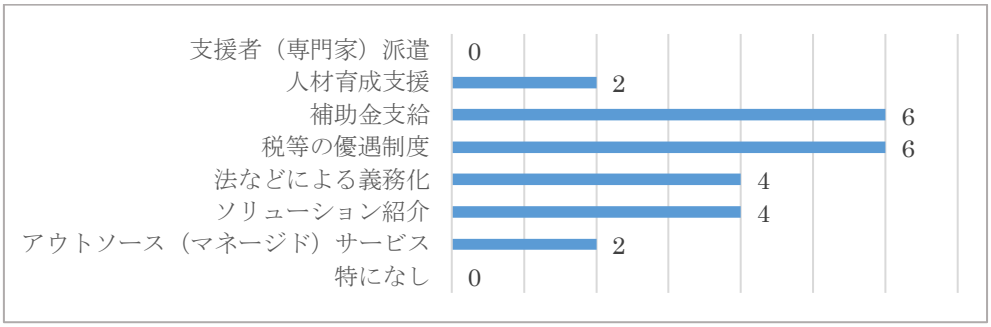
3.13.2 実施していない（予定なし）の理由



3.13.3 具体的な障害の内容

- 対策をとるために必要な資源（人・物・金・情報）の不足
- 社員の意識改革、うっかりミス、許可制による煩雑さ
- ルールとして返却している前提で、セルフチェックシートを利用した運用でしか出来ていない
- 「重要情報が何であって、どこにあるのか」がアセスメント出来ていない
- リモートワーク等、業務環境から考えてどう対応できるのかわからない

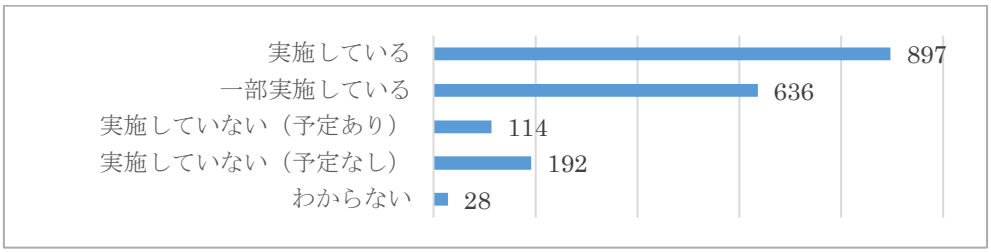
3.13.4 どのような支援施策があれば実施できそうか



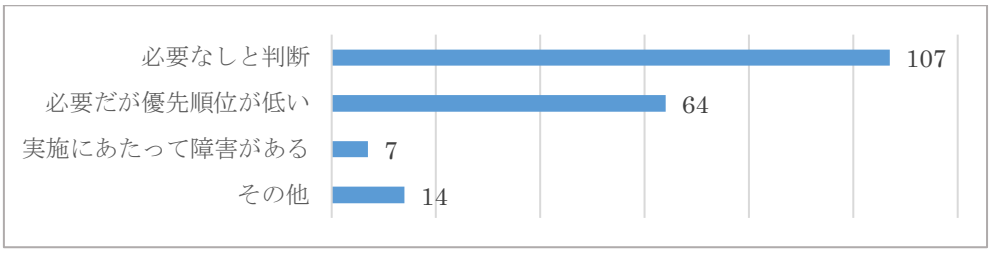
3.14 【No.14】利用者限定

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する

3.14.1 実施状況



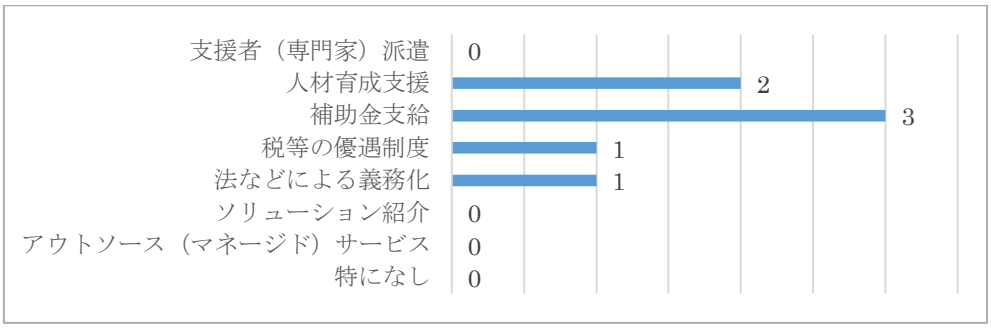
3.14.2 実施していない（予定なし）の理由



3.14.3 具体的な障害の内容

- 社内の合意が得られない/業務遂行に支障がでる
- 従業員の IT 技術に対しての理解がない
- 資金面の問題あり
- 作業を行う担当が入れ替わる都合上、PC を共用し、ID も共用している
- 防犯カメラにて対応している

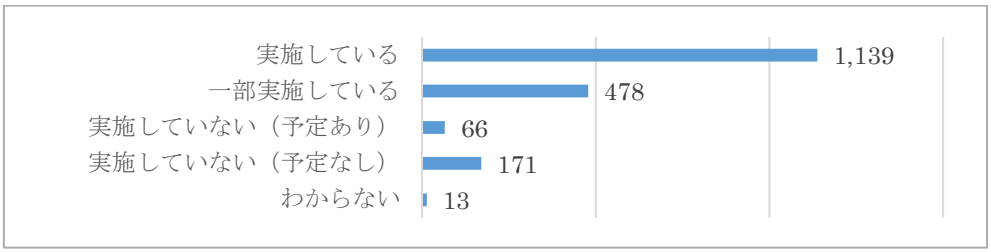
3.14.4 どのような支援施策があれば実施できそうか



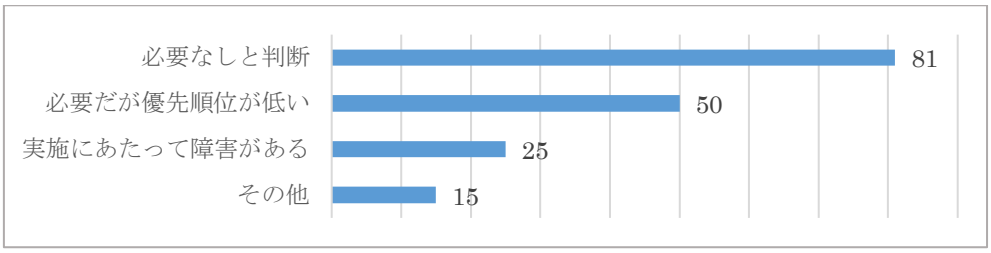
3.15 【No.15】立ち入り監視

関係者以外の事務所への立ち入りを制限する

3.15.1実施状況



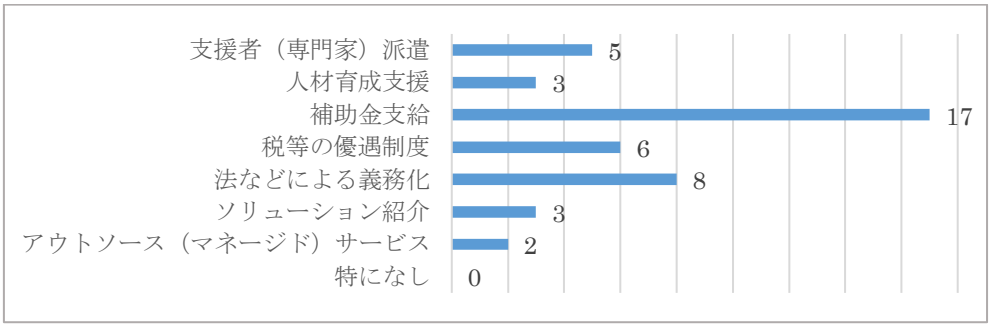
3.15.2実施していない（予定なし）の理由



3.15.3具体的な障害の内容

- 事務所の構造上の問題（シェアオフィス・事務所兼店舗・事務所兼自宅等）
- 事務所に人の出入りが多い
- 社内の合意が得られない
- 資金面の問題あり
- 事務所への立ち入りを制限するのは、通常業務に支障をきたす。重要書類だけを別室にできるようなスペースがない

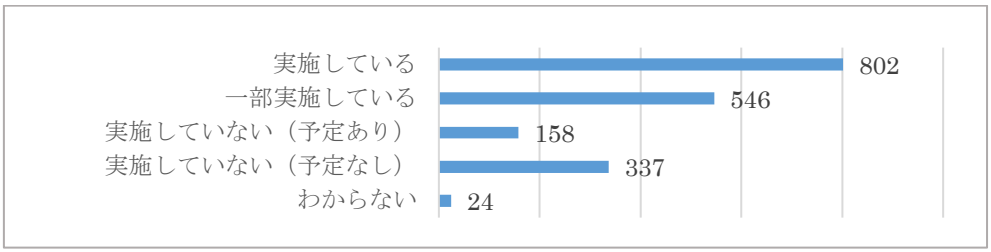
3.15.4どのような支援施策があれば実施できそうか



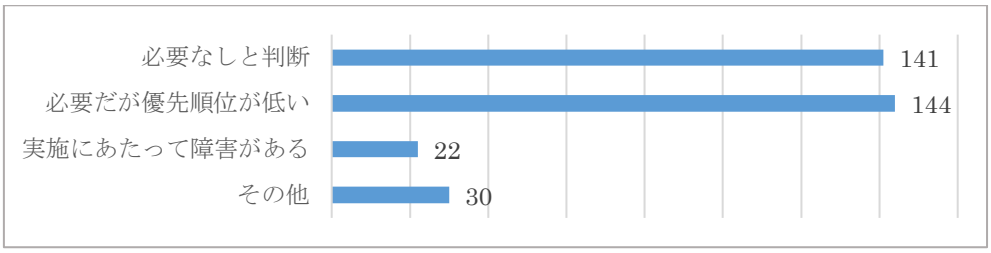
3.16 【No.16】盗難防止

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行う

3.16.1 実施状況



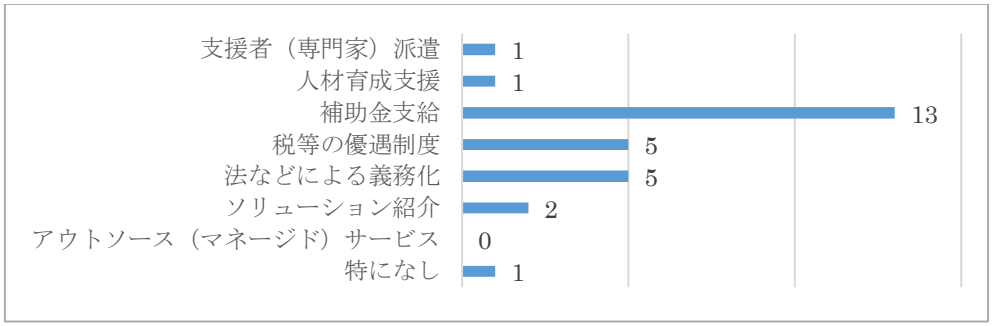
3.16.2 実施していない（予定なし）の理由



3.16.3 具体的な障害の内容

- 施錠付き保管庫の整備、スペースの確保が困難
- 設置している部屋の入口施錠・警備会社による遠隔監視で対応している
- 情報は個人使用している PC に保存せず共有ファイルに保存、アクセス制限を設けている
- 手間がかかるなど実際の運用に課題がある
- ノート PC は、昼夜別の人が使うため全て施錠する事は困難
- 資金面の問題あり

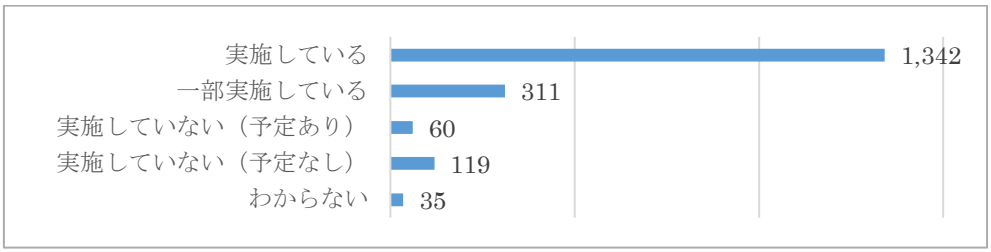
3.16.4 どのような支援施策があれば実施できそうか



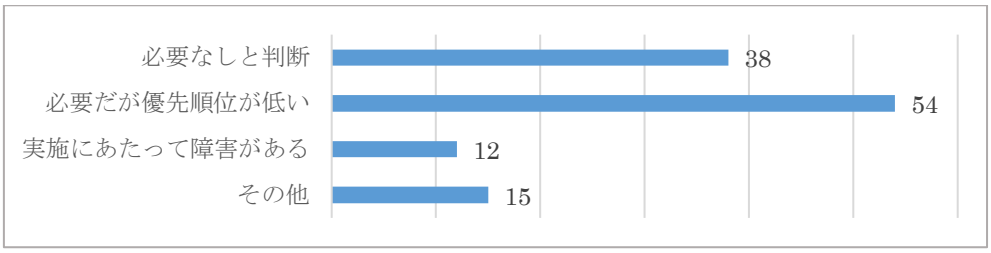
3.17 【No.17】施錠管理

事務所が無人になる時の施錠忘れ対策を実施する

3.17.1実施状況



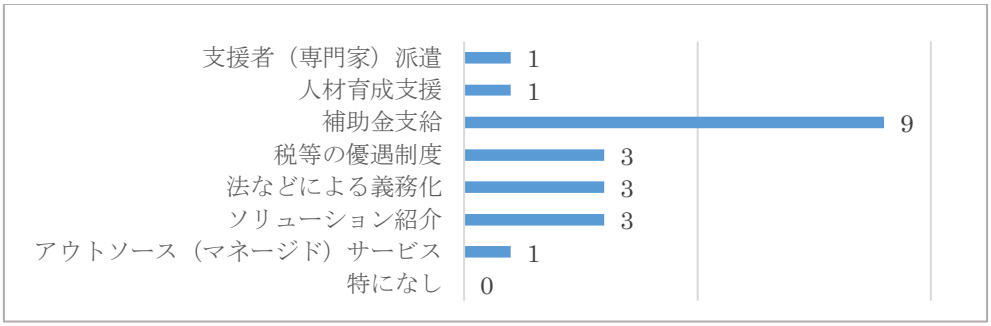
3.17.2実施していない（予定なし）の理由



3.17.3具体的な障害の内容

- 建物の構造上困難/自宅兼事務所のため自動施錠、家族への教育など、建物レベルの管理設計は難しい
- レンタルオフィスのため、勝手な施策を行うことができない
- 施錠忘れを対策するには、ビル管理などを巻き込んで高度な対策が必要となるため、実施が難しく、監視カメラで対応している
- 資金面の問題あり
- 導入と導入後の保守管理にコストがかかる

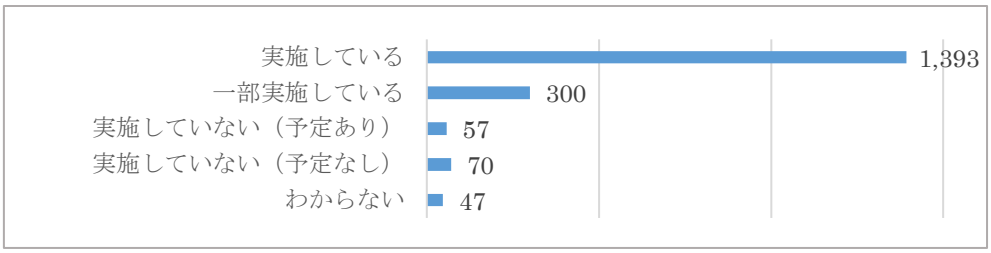
3.17.4どのような支援施策があれば実施できそうか



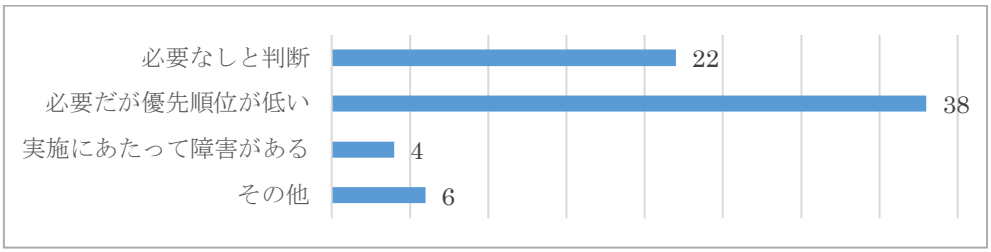
3.18 【No.18】破棄

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する

3.18.1実施状況



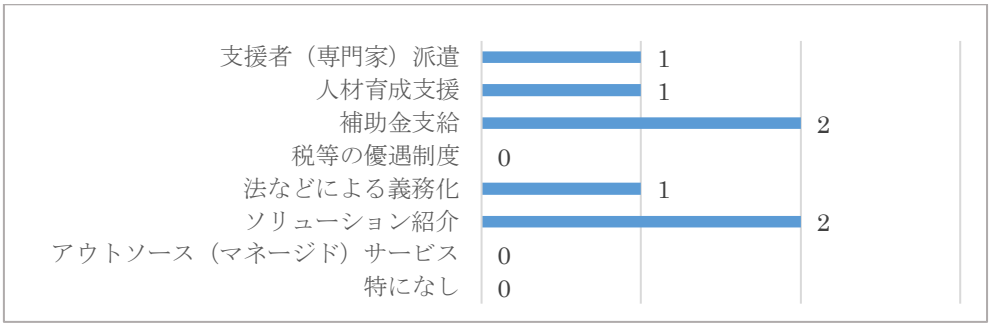
3.18.2実施していない（予定なし）の理由



3.18.3具体的な障害の内容

- 具体的に何をすべきか分からない
- 従業員のセキュリティ意識の向上が必要
- 宣言実施後に破棄した媒体がない
- 資金面の問題あり

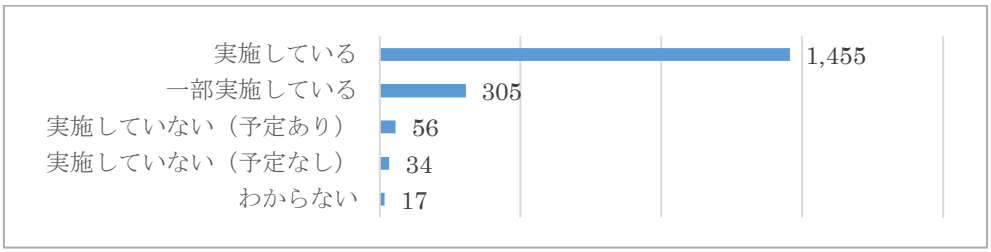
3.18.4どのような支援施策があれば実施できそうか



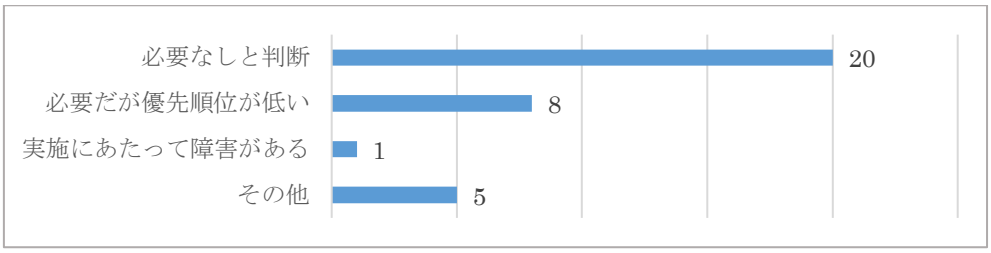
3.19 【No.19】社内規定周知

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る

3.19.1実施状況



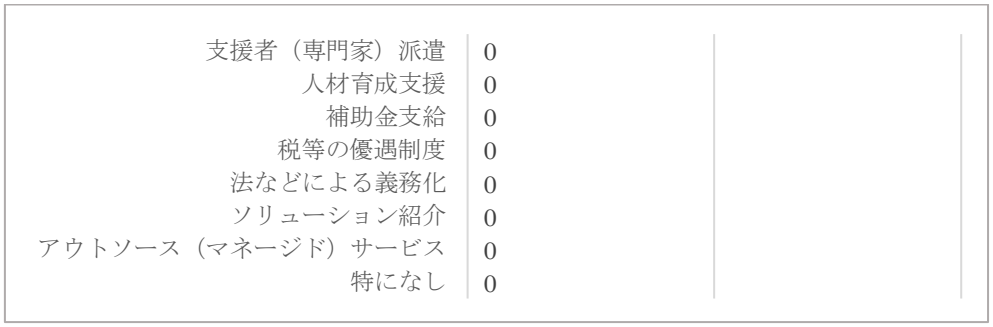
3.19.2実施していない（予定なし）の理由



3.19.3具体的な障害の内容

・ 対策を行うことの重要性が理解できない（理解力が追いつかない）

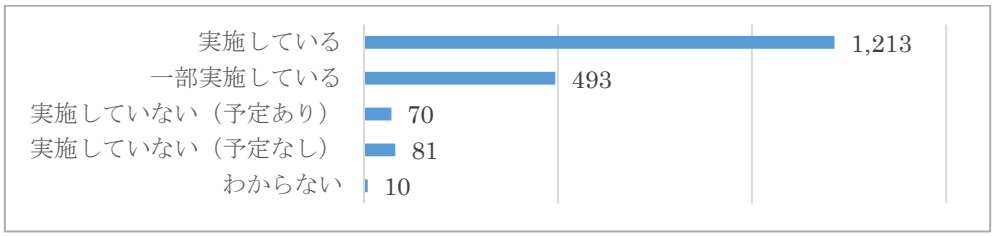
3.19.4どのような支援施策があれば実施できそうか



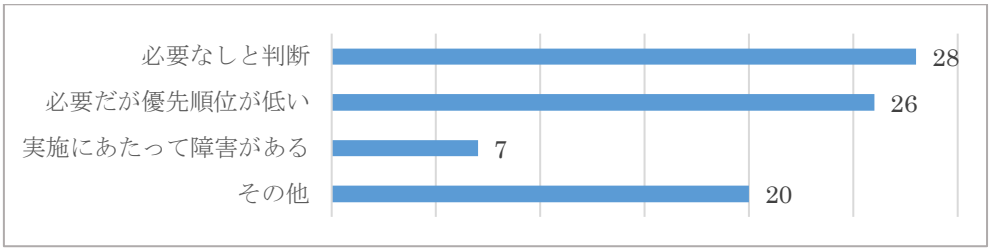
3.20 【No.20】意識教育

従業員にセキュリティに関する教育や注意喚起を行う

3.20.1実施状況



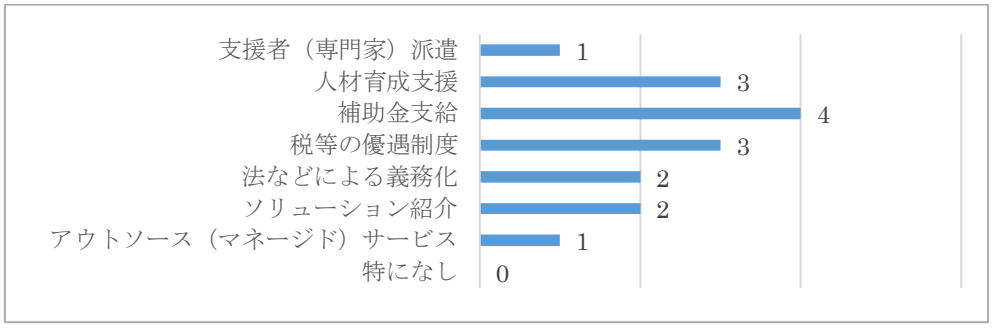
3.20.2実施していない（予定なし）の理由



3.20.3具体的な障害の内容

- 経営資源（教育を行える者、外部委託費用、教材など）の不足
- 社員全員に教育する時間を捻出できていない
- 人材の不足及び具体的な実施事項が不明なため、必要性の判断がつかない

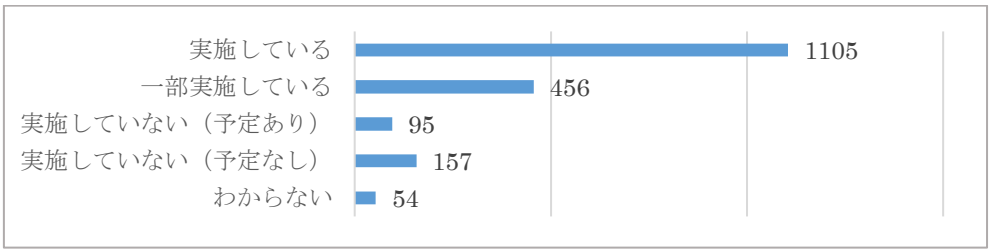
3.20.4どのような支援施策があれば実施できそうか



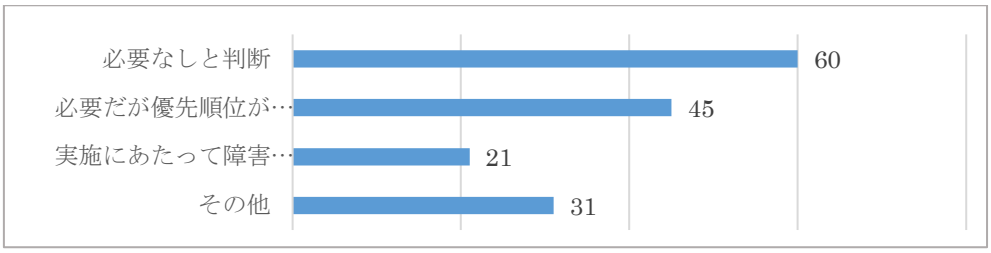
3.21 【No.21】個人所有

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する

3.21.1実施状況



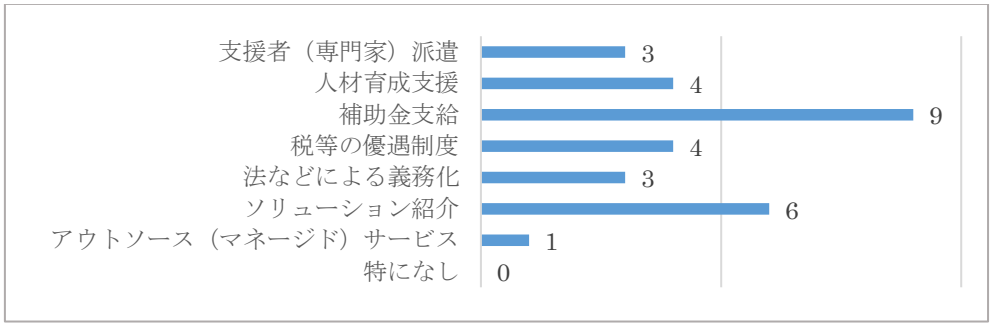
3.21.2実施していない（予定なし）の理由



3.21.3具体的な障害の内容

- 具体的な対策方法、導入手順が不明。マニュアルなどが無い
- 対策を進める知識と時間のある社員がいない
- 社員のモラル向上、教育などが出来ない
- ルールの線引きが難しく、個人の同意が得られないことが予測される
- 個人所有端末・機器への対策費用を補填する予算が無い（注意喚起に留まる）
- 個人の所有物なので徹底することが難しく、管理の手間が非常に大きい

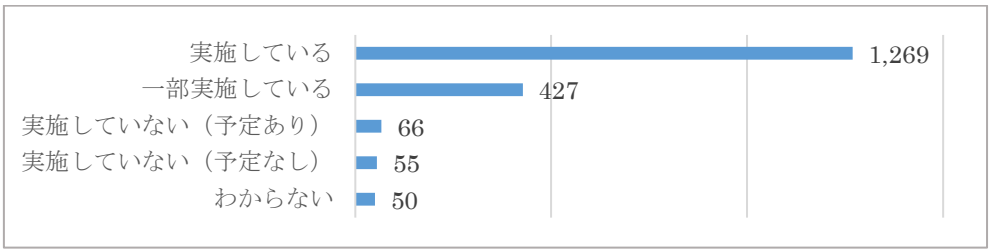
3.21.4どのような支援施策があれば実施できそうか



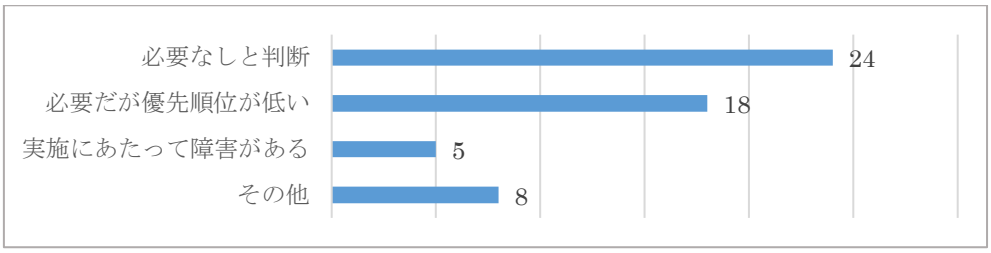
3.22 【No.22】取引先

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する

3.22.1 実施状況



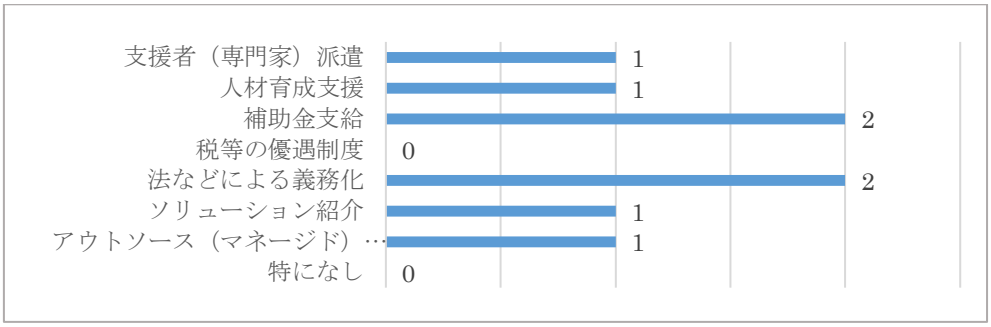
3.22.2 実施していない（予定なし）の理由



3.22.3 具体的な障害の内容

- 取引先との合意が出来ない。理解を得るための説明が難しい
- 取引先に面倒な会社だと思われるのではないかと危惧し要請できない
- NDA なども一部企業を除き業界的に認識されていない（行政等の理解促進の施策も取られていない）
- 時間が無い

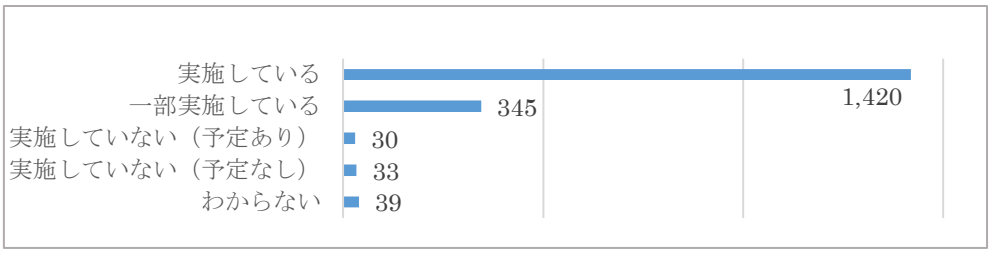
3.22.4 どのような支援施策があれば実施できそうか



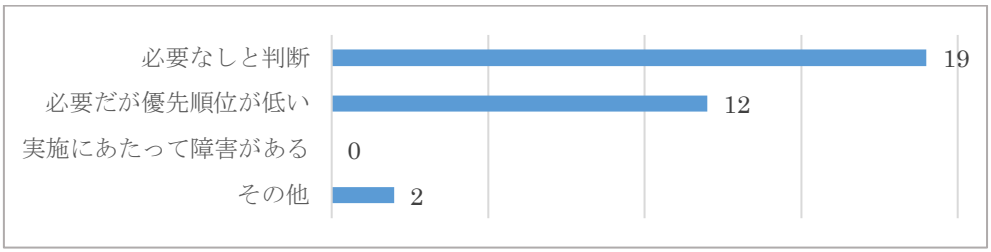
3.23 【No.23】外部サービス

クラウドサービスやウェブサイトの運用などで利用する外部サービスは、安全・信頼性を把握して選定する

3.23.1実施状況



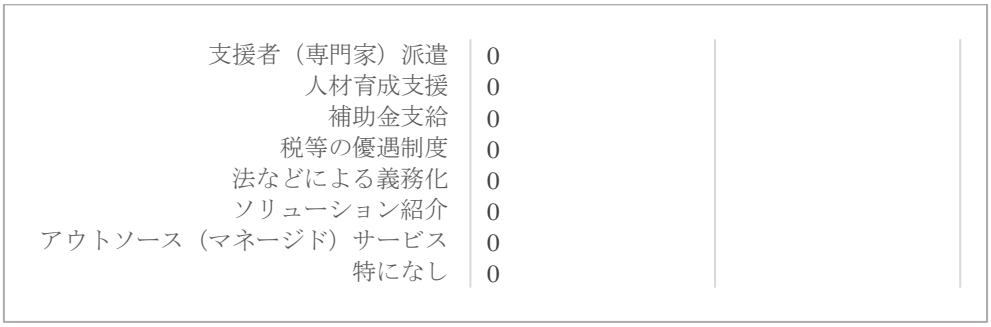
3.23.2実施していない（予定なし）の理由



3.23.3具体的な障害の内容

・ 回答無し

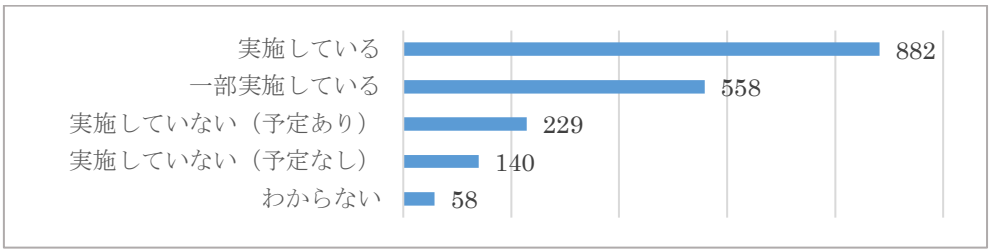
3.23.4どのような支援施策があれば実施できそうか



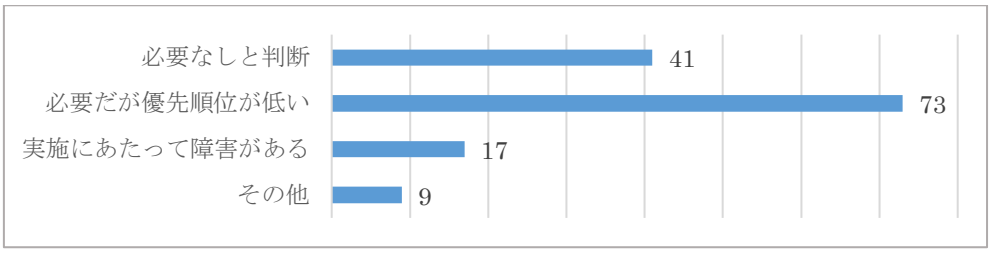
3.24 【No.24】事故対応

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行う

3.24.1実施状況



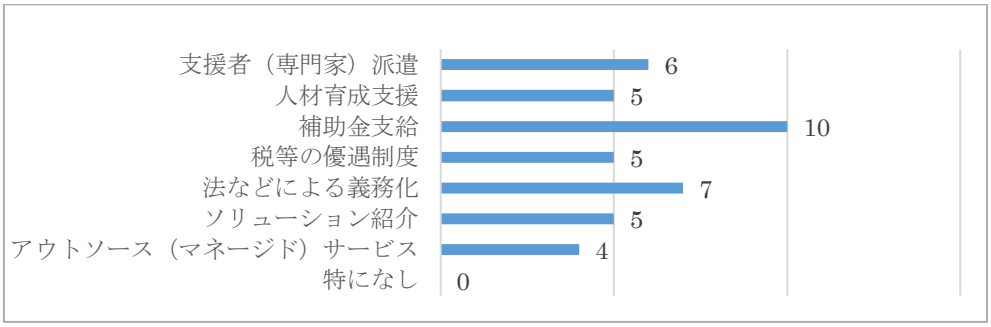
3.24.2実施していない（予定なし）の理由



3.24.3具体的な障害の内容

- 具体的に何をどうしたらよいのか分からない
- 経営層を含め社内の IT リテラシーが低く、対策実施の社内合意、決裁が得られない
- 人材がいないため準備できていない。外部からの支援を得る費用も予算化できない

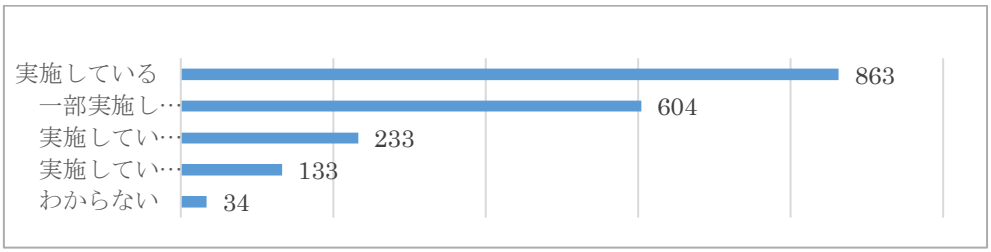
3.24.4どのような支援施策があれば実施できそうか



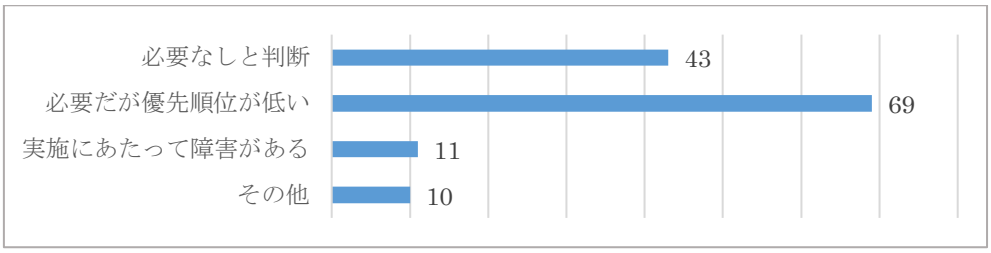
3.25 【No.25】対策の明確化

情報セキュリティ対策（上記 1～24 など）をルール化し、従業員に明示する

3.25.1 実施状況



3.25.2 実施していない（予定なし）の理由



3.25.3 具体的な障害の内容

- ルールの範囲や作成手順が分からない
- ルール作成に時間を割ける人材がいない
- ルールで縛ることで、現状の業務に支障が出ることが懸念され、社内の合意が得られそうにない

3.25.4 どのような支援施策があれば実施できそうか