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

～中小企業のセキュリティ課題と支援施策～

JNSA　社会活動部会　中小企業支援施策WG　古川英規

アジェンダ

はじめに

JNSA 中小企業支援ワーキンググループでは、これまで、中小企業の情報セキュリティ対策導入を促進する支援施策を検討してきました。

- 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の検討とその実践
- 中小企業の情報セキュリティ市場の拡大を捉えた、JNSA会員のソリューション展開への寄与

近年、サイバー攻撃による被害は、中小企業にとっても経営上の大きなリスクとなっています。
こうした状況を踏まえ、
「**中小企業は実際にどこまで情報セキュリティ対策に取り組めているのか**」
「**どのような対策に課題を抱えているのか**」
を把握するため、
2024年10月にIPAの協力をいただき、中小企業のセキュリティ対策の実際を調査しました。

アンケート調査の実施概要

調査対象	SECURITY ACTION（二つ星）宣言事業者　（全国 33,573件対象）
回答数	1,867件（有効回答）
実施期間	2024年10月28日 ～ 11月18日
実施手法	IPAの協力のもと、WebフォームおよびExcelシートによる回答収集

アンケート内容
IPA「中小企業の情報セキュリティ対策ガイドライン_V3.1」の
「新5分でできる！情報セキュリティ自社診断」25項目の実施状況を聞いてみた。

できている対策・できていない対策・どんな支援があれば対策を実現できるのか

アンケート調査の実施概要

No	項目名	内容
1	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	パスワード管理	強固なパスワードを使用する
4	機器の設定	共有設定を見直す
5	情報収集	脅威や攻撃の手口を知り、対策に生かす
6	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	電子メールのルール	宛先の送信ミスを防ぐ
8	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のルール	無線LANの盗聴や無断使用を防ぐ
10	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	バックアップのルール	バックアップを励行する
12	保管のルール	重要情報の放置を禁止する
13	持ち出しのルール	重要情報は安全な方法で持ち出す
14	事務所の安全管理	機器を勝手に操作させない
15	事務所の安全管理	見知らぬ人には声をかける

No	項目名	内容
16	事務所の安全管理	機器・備品の盗難防止対策を行う
17	事務所の安全管理	オフィスの戸締まりに気を配る
18	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	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	従業員教育	従業員に情報セキュリティ教育を行う
21	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	取引先管理	取引先に秘密保持を要請する
23	外部サービスの利用	信頼できる外部サービスを使う
24	事故への備え	事故発生に備えて事前に準備する
25	ルールの整備	情報セキュリティ対策をルール化する

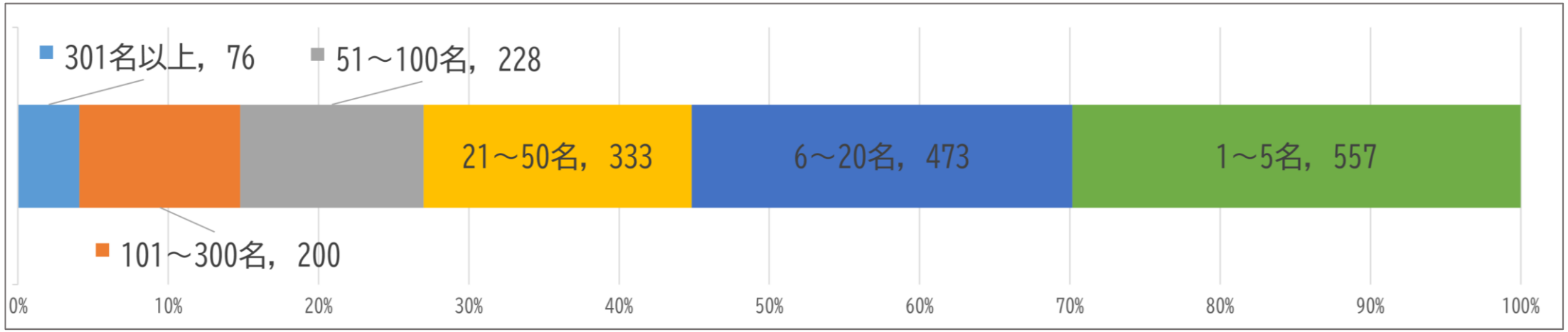
アンケート調査の実施概要

実施状況	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・なし）／わからない
予定なしの理由	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
障害内容	自由記述
支援施策	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）

回答企業の属性（従業員数）

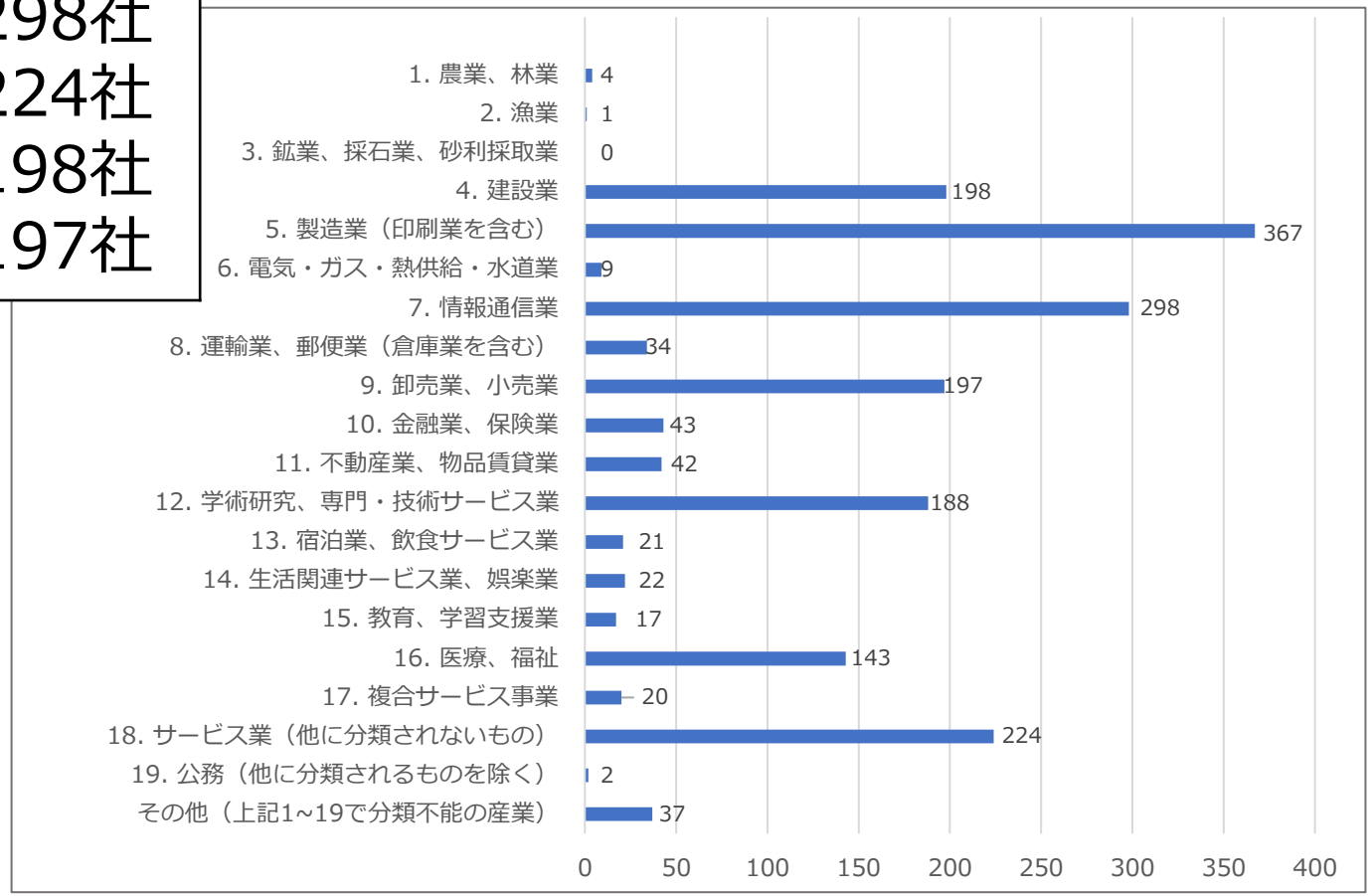
従業員数構成	1～5名　：　29.8%（557社） 6～20名　：　25.3%（473社） 21～50名　：　17.8%（333社） 51名以上　：　27.0%（504社）

→ 50名以下の企業が全体の約73%を占める



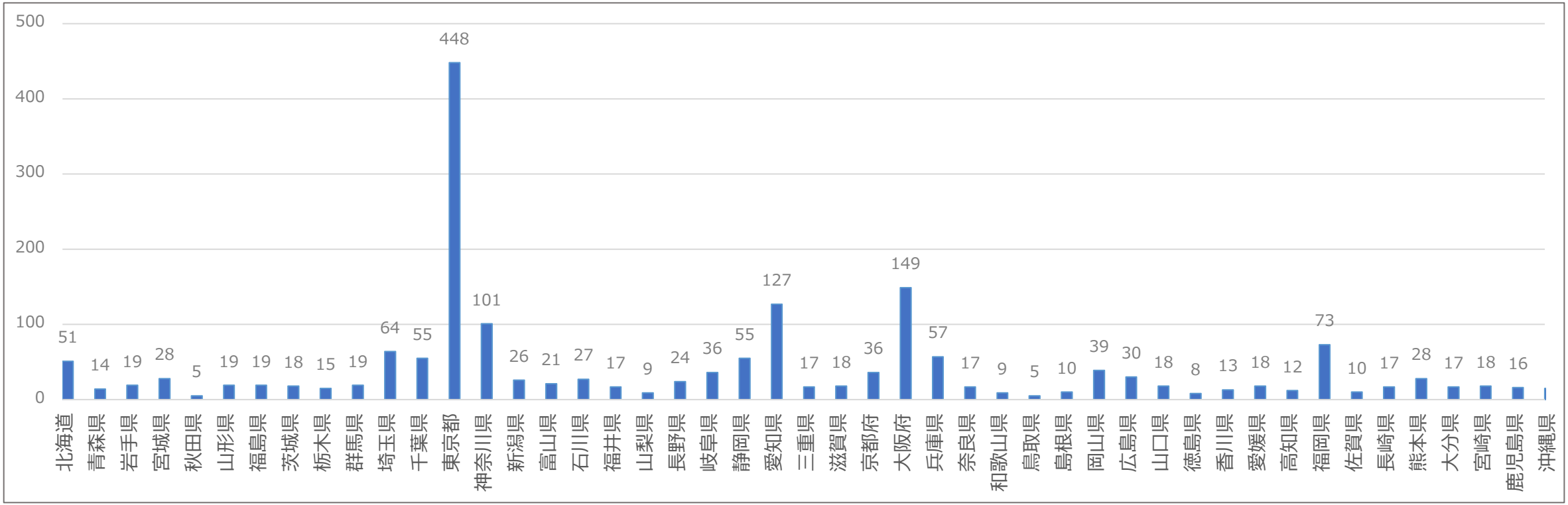
回答企業の属性（業種）

主要業種構成			
	製造業	：	367社
	情報通信業	：	298社
	サービス業	：	224社
	建設業	：	198社
	卸売・小売業	：	197社



回答企業の属性（地域別）

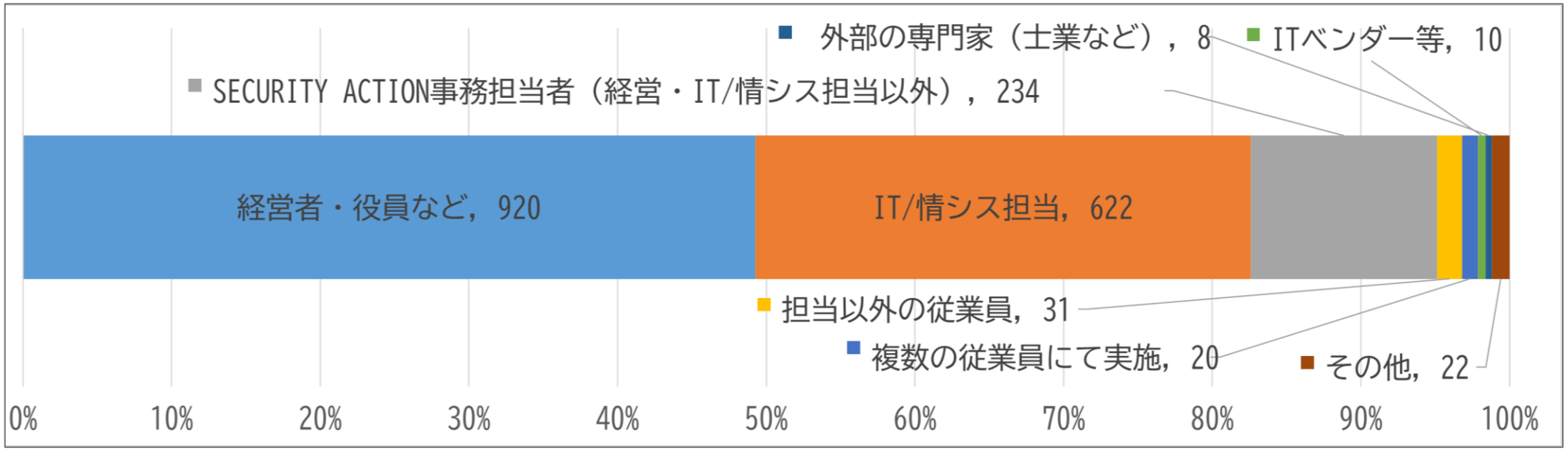
地域別	全国都道府県から回答（東京都448社、大阪府149社）



自社診断の実施者

自社診断の実施者	経営者・役員等　：　49.3%（920社） IT/情シス担当事務　：　33.3%（622社） 担当者　：　12.5%（234社）

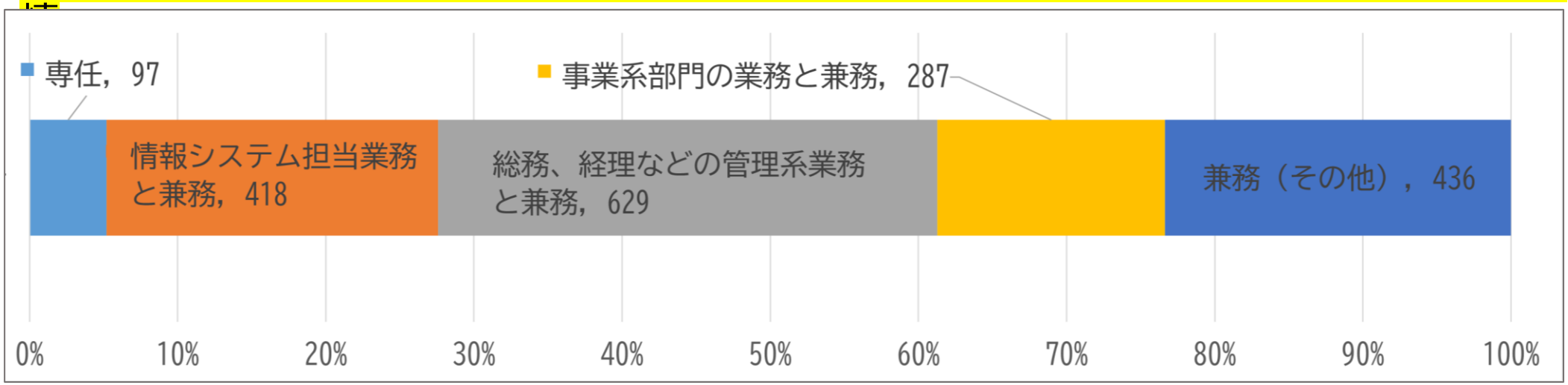
→経営者自らが診断を行うケースが約半数



セキュリティ担当者

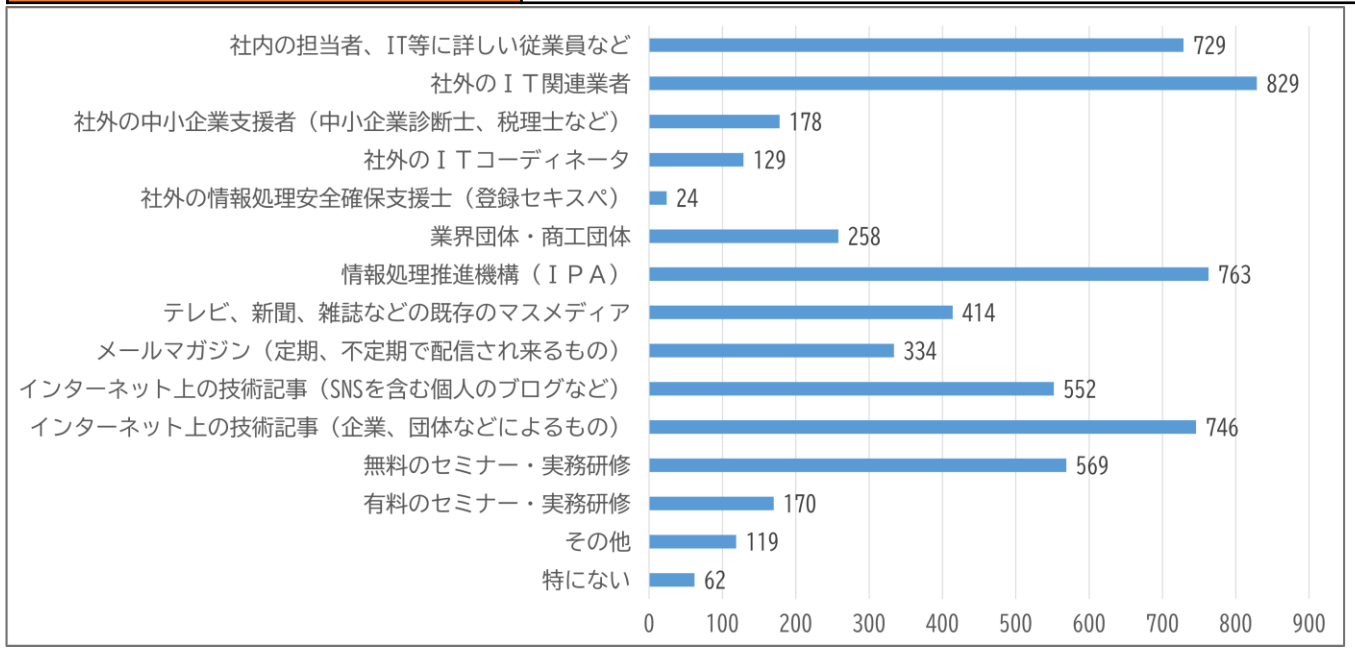
担当者の体制	専任担当者	：	5.2%（97社）
	総務・経理等と兼務	：	33.7%（629社）
	その他業務と兼務	：	23.4%（436社）
	情シスと兼務	：	22.4%（418社）
	事業系部門の業務と兼務	：	15.3%（287社）

→セキュリティ専任担当を置ける中小企業は極めて稀で、「ほぼ100%兼務体制」が実情



セキュリティ情報の収集先・学習手段

主な情報収集先			
	社外のIT関連業者	：	829社
	IPA（情報処理推進機構）	：	763社
	インターネット上の技術記事・企業・団体	：	746社
	社内の担当者・詳しい従業員	：	729社
	無料セミナー・実務研修	：	569社



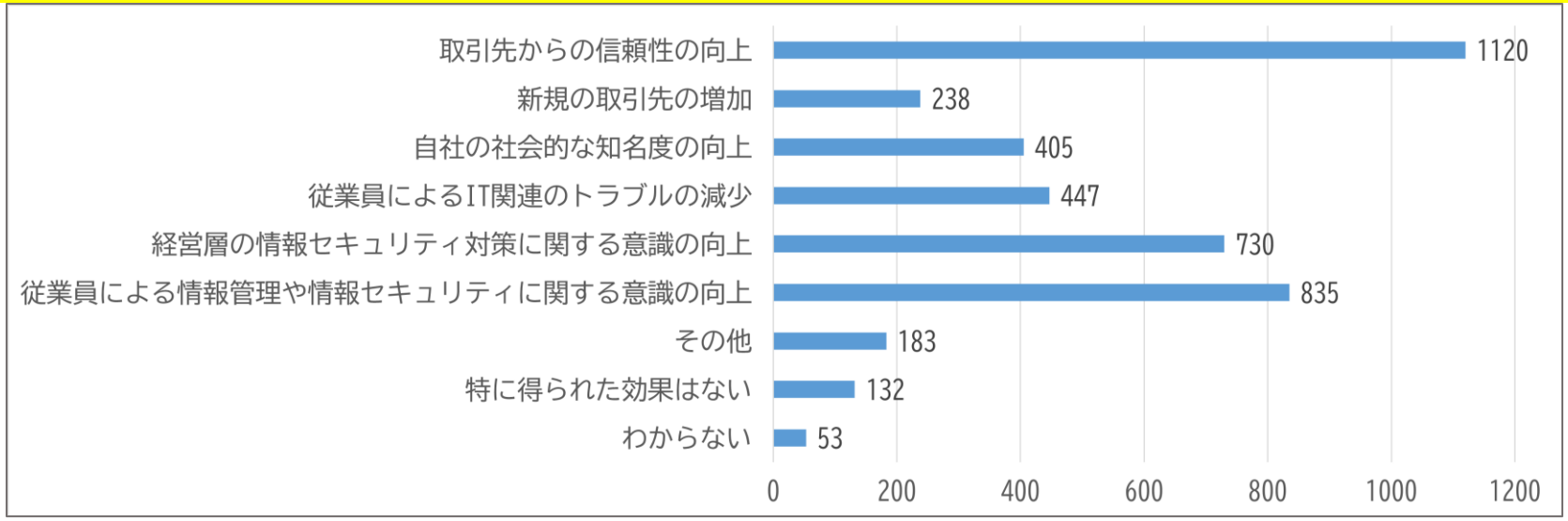
外部のベンダー頼み、またはIPAの公的情報
Web検索に依存。
専門資格者（登録セキスペ24社）への直接相談は極めて少ない 。

SECURITY ACTION宣言を行ったきっかけ

きっかけ	取引先からの信頼性の向上	:	1,120社
	従業員の意識向上	:	835社
	経営層の意識向上	:	730社
	従業員によるITトラブル減少	:	447社

新規顧客開拓よりも、既存取引先との信頼関係維持・強化が最大の動機

「その他」自由記述のうち140社（約7%）がIT導入補助金等の申請要件を契機に挙げる



SECURITY ACTION宣言により得られた「効果」

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）	• 情報リテラシー向上、個人情報保護などといった情報の管理の取り組みに役立った。 • 情報セキュリティに関する意識向上
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。 • 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。

「5分でできる！自社診断」25項目の実施傾向（全体）

実施率が高い項目（80%前後）

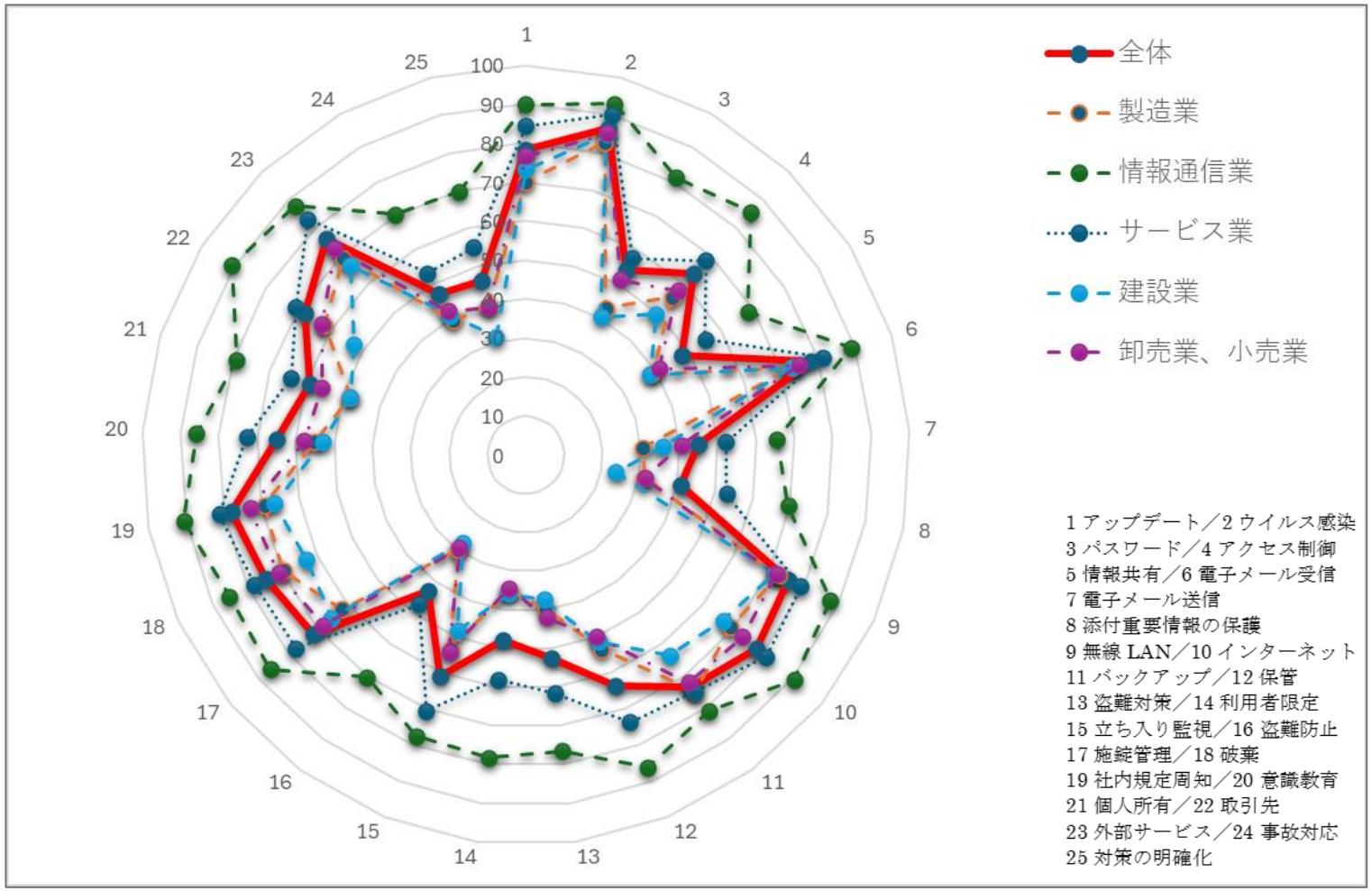
【No.2】	ウイルス感染対策（86.7%）
【No.1】	OS・ソフトのアップデート（78.2%）
【No.6】	電子メール受信注意（77.9%）
【No.10】	インターネット利用規則（77.9%）

実施率が低い項目（40%～50%前後）

【No.8】	添付重要情報の保護（40.9%）
【No.16】	機器の盗難防止（43.0%）
【No.7】	電子メール送信ミス防止（45.0%）
【No.25】	対策のルール明確化（46.2%）
【No.24】	事故対応体制（47.2%）

「外部からの攻撃を防ぐ技術対策」は進んでいるが、
「自社内のルール化・誤送信防止・事後対応」は大きく遅れている

業種ごとの実施割合



高実施率業種

情報通信業

全25項目にわたり高い実施割合。

監督官庁の指導や過去のインシデント事例、扱う個人情報の多さが要因

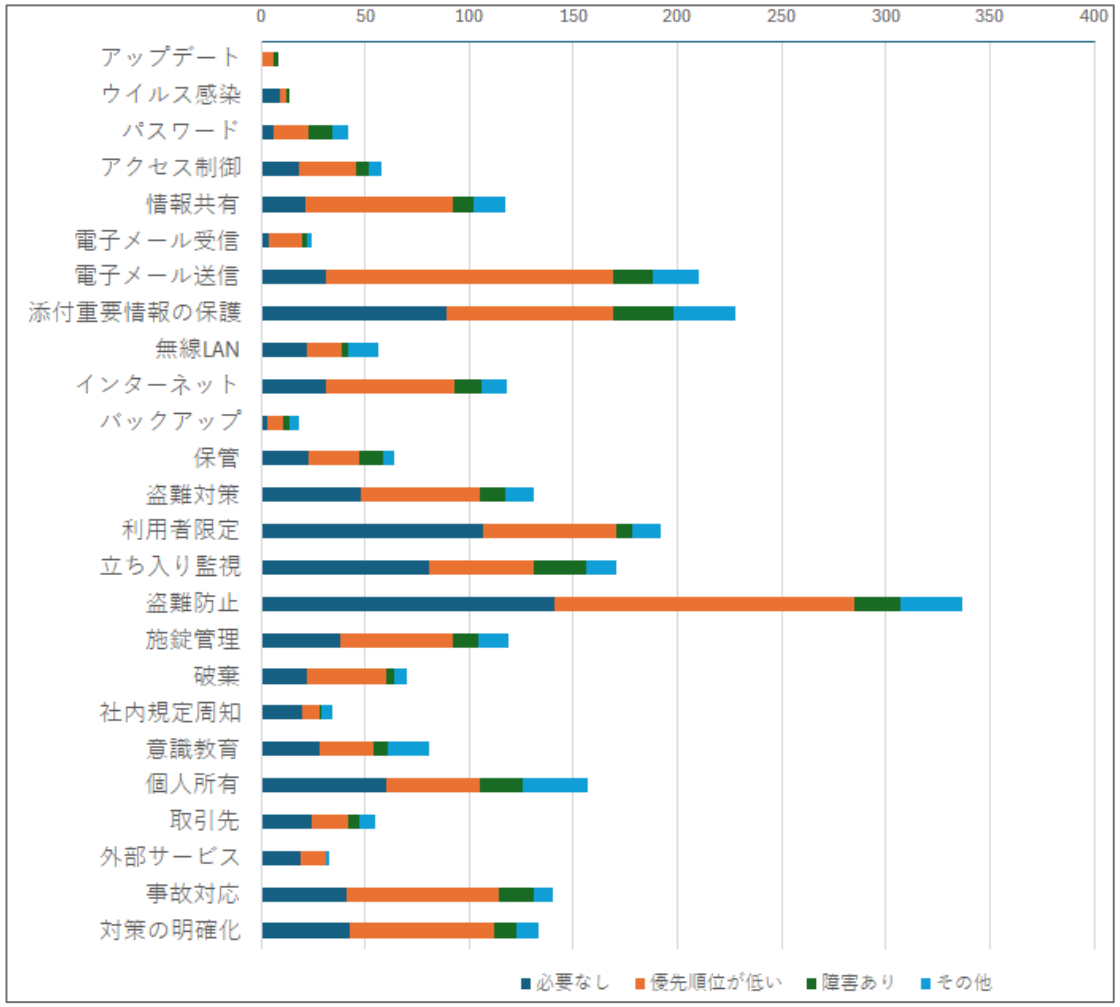
低実施率業種

建設業、製造業、卸売・小売業

全体的に実施率が低迷。

特に現場仕事や手作業が多い環境でIT対策が後回しになりがち

対策を実施しない・予定がない理由



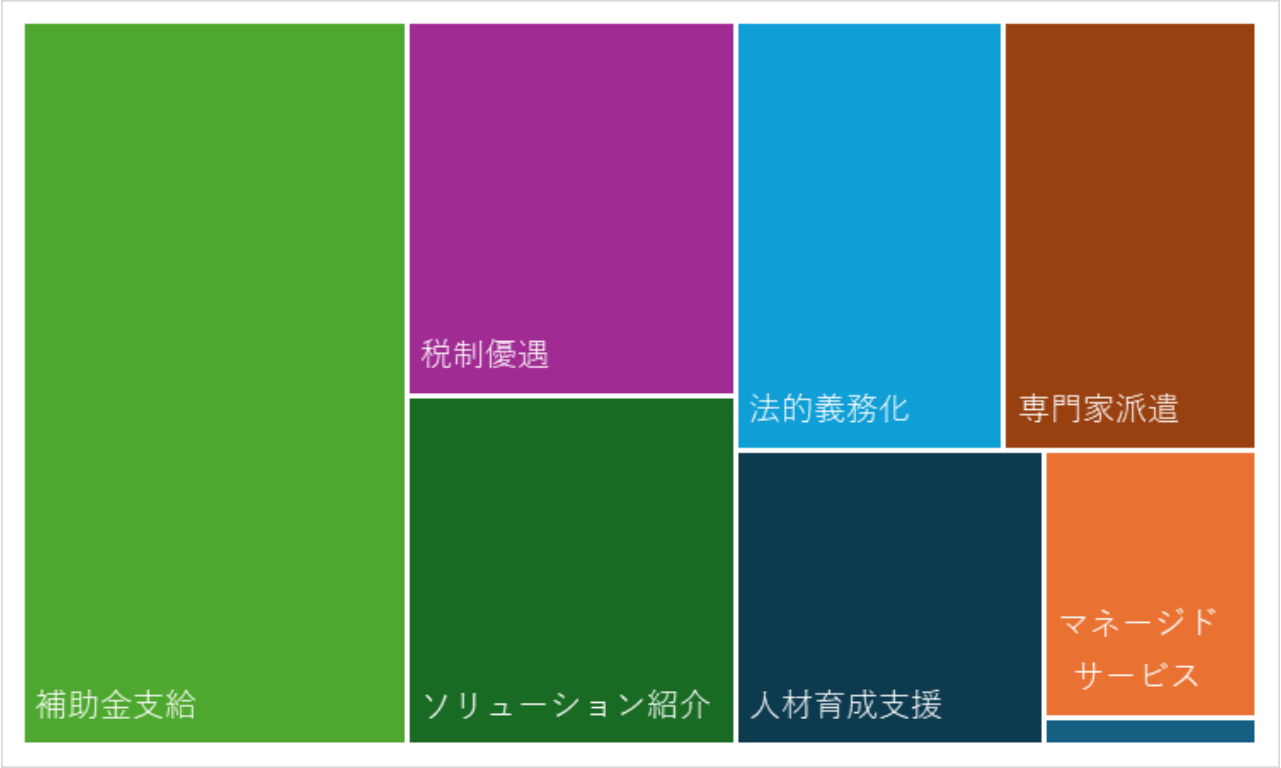
「障害がある」よりも「優先順位が低い」が圧倒的多数

優先順位が低い
業務に直接繋がらないため、後回しにされている
（例：盗難防止、事故対応、ルール化）

必要なしと判断
「自社には関係ない」「小規模だから不要」
という誤った安全神話

技術的・資金的障害
「コストがかかる」
「具体的なやり方がわからない」

実施に向け中小企業が求める支援策



1. 金銭的支援（最多数）

・補助金支給

・税制優遇措置

補助金など、費用面での支援を求めている

2. 伴走・環境支援

・専門家派遣・人材育成

・ソリューション紹介 / マネージドサービス

・法などによる義務化

「法的な義務化」を求める声が一定数存在。
社内説得や予算確保の「口実」として公的な強制力を望む傾向が見られる

【基本的対策】パスワードと情報共有の壁

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

項目	実施率	主な障害・課題の内容
【No.3】 パスワード	54.1%	• 複雑にすると忘れる・紙で貼ってしまう • ITリテラシーの低い社員に合わせざるを得ない • 社内合意が得られない
【No.5】 情報共有	48.0%	• 最新脅威情報を共有する仕組みやシステムがない • 何をどこから入手し、どう社内に周知すべきかわからない

【メール対策】受信はできるが「送信・保護」ができない

メール対策(No.6～No.8)では、受信対策の実施率（86.7%）は高い一方、送信対策および添付ファイル保護の実施率が低い

項目	実施率	主な障害・課題の内容
【No.7】 誤送信防止	45.0%	• 誤送信防止機能（保留・上司承認等）を導入しても「即時送信できず業務が滞る」「操作が複雑」と批判され運用停止
【No.8】 添付重要情報の保護	40.9%	• 官公庁や顧客の制約 • または暗号化でウイルススキャンをすり抜ける懸念

【物理セキュリティ】立ち入り・盗難・離席対策の課題

物理的対策(No.14～No.17)　職場の環境や業務上の都合から、実施率が低い

項目	実施率	主な障害・課題の内容
【No.14】 利用者限定	48.0%	• 共用PCの利用や、ID使い回し、業務の効率優先で画面ロックが徹底されない
【No.15】 立ち入り監視	61.0%	• 自宅兼事務所、シェアオフィス、店舗併設など「物理的に区画・制限できない」構造的限界
【No.16】 盗難防止	43.0%	• 保管庫のスペース不足、交代勤務で施錠できない

【組織対策】ルール化と事故対応体制の未整備

事故対応（No.24：47.2%）と対策の明確化（No.25：46.2%）は過半数が未実施

項目	実施率	主な障害・課題の内容
【No.24】 事故への備え	47.2%	• ルール作成の人材不足： 「何をどこまでルール化すれば良いかわからない」「作成する時間と人がいない」
【No.25】 ルールの整備	46.2%	• 「ルールで縛ると現場の業務が回らなくなる」という経営者・社員の懸念

アンケート回答企業へのヒアリング調査概要

目的	アンケートの数値データの背景にある「現場の生の声」 「具体的な工夫」「直面している生の壁」を深掘り調査
対象	アンケート回答企業からピックアップした中小企業経営者・担当者
実施期間	2025年2月27日 ～ 3月4日
内容	対応しやすかった項目、断念した項目、独自の工夫、情報収集方法、 情報発信者（IPA等）への要望

成功事例：スムーズに対応できた項目とそのきっかけ

「環境の変化」をチャンスに変えた企業が成功している！

項目	主な内容
【No.6】 不審メール対応 【No.7】 誤送信防止	• クラウド型メール（Microsoft 365, Google Workspace等）へ移行したことで、意識せずともセキュリティ機能が自動強化された
【No.15】 立ち入り監視 【No.17】 オフィスの施錠管理	• 事務所移転に合わせてICカードキーや立ち入り制限を導入 • 「鍵をかける」という誰にでも理解しやすい明確な運用ルールは即座に定着

失敗・難航事例：なぜ対策が進まないのか？

製品・ベンダー選定の難しさ	• 「世の中に製品が多すぎて自社に最適・適正価格のソリューションが選べない」「選定に時間がかかり挫折」
社員のITリテラシーの格差	• 複雑なパスワードの設定や定期的な更新が難しい • ルールを守らせることに苦労した
BCP策定	• 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

工夫事例：ルールを形骸化させない現場の取り組み

実効性を高める工夫のアイデア集（ヒアリングより）

なぜ守るか」の動機付	• 理由を丁寧に説明する教育資料を自作
目標の宣言	• 研修の最後に「今年自分が注意するセキュリティ目標」を書かせる
イエローカード制度	• 離席時の画面ロック忘れ等に対し、巡回時にイエローカードを置き、累積で再教育を実施
部門担当者の配置	• 各部署にITセキュリティ担当を置き、最低限の注意事項を草の根で徹底
公的支援の活用	• 地域の専門家派遣支援事業を活用してルール化

ヒアリングから見えた「切実な支援ニーズ」

第三者による 中立な評価・助言	• ベンダーの営業ではなく、中立な立場で自社の課題を診断し、相談に乗ってくれる専門家が欲しい
インシデント時の 「駆け込み寺」予約	• 事故が起きてからベンダーを探しても間に合わない。平時は低額で、有事に即座に対応してくれるサブスク型契約が欲しい
同業他社の 具体的な事例	• 自社と同規模・同業種の企業が、何人の担当者でどんな対策をしているか知りたい
プッシュ型の情報提供	• 自らIPAのサイトに見に行かない。更新情報や教材をプッシュ通知で届けて欲しい

現場が「今、気になっている」新たなセキュリティ課題

25項目以外で現場が直面している関心事項

生成AIの利用ルール・セキュリティ	• 社員が業務でChatGPT等を使う際のガイドラインやデータ流入リスク
クラウド障害・SaaSインシデントへのBCP	• 利用しているクラウド側が停止・攻撃された際のバックアップ・事業継続計画
ECサイト・SNS運用リスク	• 売上に直結するECサイト構築やSNS活用が優先され、セキュリティ対策まで手が回っていない。

中小企業セキュリティ対策の構造的課題

セキュリティ対策が進まない3つの要因	1. リソース不足： 資金・人材・時間の欠如 2. 情報・知識不足： 自社に適した製品が選べない 3. 社内合意・意識の壁： 業務優先によるルールの形骸化
セキュリティ対策の打開の糸口	• 「高望み」をやめ、できるレベルから着手 • 外部クラウドや専門家の知見を活用 • 従業員への「動機付け（なぜ行うか）」徹底

「100点満点」を目指さず、リスクコントロールを行う

現場の誤解：完璧なシステム導入を求められていると思い込み断念している！

立ち入り監視（No.15）の例	• 高価なセキュリティゲートが買えなくても、「部外者入室時に台帳へ記入・履歴を残す」だけで十分対策になる
情報共有（No.5）の例	• 全社システムがなくても、まずは「担当者間で月1回情報を共有する」ことから始める
できることから始める	• すべてを完璧に対策しようとして何もしないより、自社でできる範囲から少しずつ取り組むことが重要。

ITベンダー・ソリューション提供者への期待

必要なレベルに合った製品提案	• 中小企業の予算・リソースに見合った「身の丈に合う」ソリューションの提供
運用負担を抑えたマネージドサービス	• 専門知識がない担当者でも運用できるパッケージ化
平時からのレスポンス契約	• インシデント発生時に即座に駆けつけ・リモート対応できる低価格なアライアンスモデルの確立

「取り組む」から「確認・改善」へ

- 中小企業は人・時間・予算に限りがある。
- セキュリティ対策が「優先順位が低い」とされやすい
- すべてを一度に対応することは難しい
- 自社でできることから始める
- 取り組んだ結果を確認し、改善していく

2026年3月27日
「中小企業の情報セキュリティ対策ガイドライン 第4.0版」を公表

最後に

ご清聴ありがとうございました！

本セミナーで発表した調査報告書の完全版は、

JNSA公式ウェブサイトよりダウンロードいただけます。

Thank you