令和 6 年度 地域 IT ベンダーの
セキュリティ対応能力強化支援業務

実施報告書

2025 年 9 月

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

目　次

1.業務の背景と目的

近年、中小企業を対象としたサイバー攻撃や、それに起因する取引先の大企業等の被害が顕在化しており、中小企業を含めたサプライチェーン全体でのセキュリティ対策の強化が求められている。独立行政法人情報処理推進機構（以下「IPA」という。）が実施した「2021 年度中小企業における情報セキュリティ対策に関する実態調査」[1]では、情報セキュリティ対策投資を行わなかった理由について中小企業の 20.7%が「どこからどう始めたらよいかわからない」と回答しており、中小企業における情報セキュリティ対策の実践において適切な支援が求められている実態が明らかになった。また、同調査によると、中小企業で情報セキュリティに関する問題が発生した際の相談先について、「社外の IT 関連業者」の割合が最も高く 49.2%となっており、地域の IT 関連企業（以下「地域 IT ベンダー」という）が中小企業の主たる相談相手となっていることがわかった。

一方で、自社が取り扱うセキュリティ製品の詳細説明ができず、販売することのみが目的となっている地域 IT ベンダーも存在し、顧客のセキュリティレベルを向上させるための意識が必ずしも十分ではないのではないかとの指摘もある。その結果、顧客は勧められるままにセキュリティ製品を導入するものの、その後必要なアップデートが行われていない例も散見され、地域全体のセキュリティレベルを低下させる懸念がある。

このような背景を踏まえて、本業務は、地域 IT ベンダーによる中小企業へのシステム導入・運用時の情報セキュリティに関する現状について、アンケート及びヒアリング調査で明らかにした上で、地域 IT ベンダーが中小企業の良き相談相手となるために果たすべき役割を整理し、地域 IT ベンダーのセキュリティ対応能力強化に資する支援策を検討することを目的として実施した。

[1]「2021 年度 中小企業における情報セキュリティ対策に関する実態調査」報告書について
https://www.ipa.go.jp/security/reports/sme/about.html

2. 地域 IT ベンダー状況調査

2.1. 調査実施方法

2.1.1. アンケート調査

① 調査目的：

地域 IT ベンダーが、中小企業向けのシステム導入・運用を行う際に直面しているセキュリティ確保の現状と課題について把握し、地域 IT ベンダーが実施すべき事項の整理や支援策の検討を目的に実施した。

② 調査対象：

本調査は、以下の企業を対象として実施した。

- 一般社団法人情報サービス産業協会（以下「JISA」という。）の団体会員（27 団体／図表 1 参照）に加盟する地域 IT ベンダー（約 2,750 社）
- その他の各地域 IT 団体（16 団体／図表 2 参照）に加盟する地域 IT ベンダー
- SECURITY ACTION の 1 つ星、2 つ星宣言事業者のうち情報通信業（一つ星：約 8,850 社、二つ星：約 3,150 社）

No	地域	団体名
1	北海道	北海道ＩＴ推進協会
2	宮城県	宮城県情報サービス産業協会
3	秋田県	秋田県情報産業協会
4	山形県	山形県情報産業協会
5	茨城県	茨城県情報サービス産業協会
6	栃木県	栃木県情報サービス産業協会
7	群馬県	群馬県情報サービス産業協会
8	埼玉県	埼玉県情報サービス産業協会
9	千葉県	千葉県情報サービス産業協会
10	神奈川県	神奈川県情報サービス産業協会
11	富山県	富山県情報産業協会
12	山梨県	山梨県情報通信業協会
13	岐阜県	岐阜県情報産業協会
14	静岡県	特定非営利活動法人 静岡情報産業協会
15	愛知県	愛知県情報サービス産業協会
16	京都府	京都府情報産業協会
17	和歌山県	和歌山情報サービス産業協会
18	島根県	島根県情報産業協会

No	地域	団体名
19	岡山県	システムエンジニアリング岡山
20	広島県	広島県情報産業協会
21	香川県	香川県情報サービス産業協議会
22	福岡県	福岡県情報サービス産業協会
23	長崎県	長崎県情報産業協会
24	熊本県	熊本県情報サービス産業協会
25	大分県	大分県情報サービス産業協会
26	鹿児島県	鹿児島県情報サービス産業協会
27	沖縄県	沖縄県情報産業協会

図表 1　情報サービス産業協会の団体会員

No	地域	団体名
1	青森県	一般社団法人 青森県情報サービス産業協会
2	岩手県	岩手県情報サービス産業協会
3	福島県	一般社団法人 福島県情報産業協会
4	東京都	一般社団法人東京都情報産業協会
5	新潟県	新潟市ソフトウェア産業協議会
6	石川県	NPO 法人　石川県情報化支援協会
7	福井県	福井県情報化支援協会
8	長野県	一般社団法人 長野県情報サービス振興協会
9	奈良県	一般社団法人奈良情報活用推進協会
10	鳥取県	一般社団法人 鳥取県情報産業協会
11	山口県	山口県情報産業協会
12	徳島県	一般社団法人徳島県情報産業協会
13	愛媛県	愛媛県情報サービス産業協議会
14	高知県	一般社団法人 高知県情報産業協会
15	佐賀県	佐賀県ソフトウェア協同組合
16	宮崎県	一般社団法人 宮崎県情報産業協会

図表 2　その他の各地域 IT 団体

③ 調査方法：

IPA ウェブサイト上にアンケート回答サイトを開設し、JISA の団体会員に加盟する地域 IT ベンダー等にメール等でアンケート協力依頼を送付して回答を得た。

（有効回答数：277 件）

④ 調査期間： 2024 年 12 月 16 日（月）～2025 年 2 月 4 日（火）

⑤ 調査項目：

本調査は、以下の調査項目を設定して実施した。設問の詳細は、参考資料（アンケート調査票）を参照のこと。

- 地域 IT ベンダーの企業/組織の属性を把握するための設問
  - 主な事業
  - 組織の成り立ち
  - 総従業員数
  - 資本金
  - 総売上高
  - 総売上高のうち中小企業からの売上高が占める割合
  - 本社所在地
- 地域 IT ベンダーの提供サービスやシステムにおけるセキュリティ確保において、必要な取組・支援策を把握するための設問
  - 提供サービスやシステム
  - 提供サービスやシステムにおけるセキュリティ確保の取組
  - 取組実施上の課題
  - 提供しているセキュリティ製品・サービス
- 中小企業との各種調整における対応状況、課題を把握するための設問
  - 運用・保守契約の締結状況
  - 顧客からのセキュリティに関する相談状況
  - 自社以外の構築システムを扱う際の対応状況
  - セキュリティ要素が不十分な要求仕様を提示された際の対応状況
  - 顧客にシステム・セキュリティ技術者がいない際の対応状況
  - セキュリティ対策を最低限の実装に抑えるよう指示を受けた際の対応状況
  - 顧客にセキュリティ対策の運用に係る応分の負担を求める際の対応状況
  - 顧客社内での導入体制が不十分な際の対応状況
  - 顧客でのインシデント発生の際の対応状況
- 地域 IT ベンダーのセキュリティ対応能力の強化ポイントを把握するための設問
  - 自社の組織面・運用面の対策
  - 自社のセキュリティ技術者の数
  - 自社のセキュリティ教育の内容
  - IPA の施策活用ニーズ
  - 顧客のセキュリティ対応の行動変容を促すために貴社で必要なこと
- 地域 IT ベンダー向け手引きの活用ニーズを把握するための設問
  - 地域 IT ベンダー向け手引きに必要な情報

⑦ 集計方法：

アンケート結果の集計・分析においては、回答データをもとに、以下の方法により、データクリーニングを実施した。

- 同一社の回答が複数含まれていないかのチェック
  - アンケート回答時に、事業者名（会社名）、回答者の部署・氏名・電話番号・メールアドレスを記入してもらい、その情報をもとに確認を実施。メールアドレスのドメインが異なる場合、いずれも集計対象とする
- 同一企業で同一人物からの回答が複数含まれていないかのチェック

- アンケート回答時に、事業者名（会社名）、回答者の部署・氏名・電話番号・メールアドレスを記入してもらい、その情報をもとに確認を実施。同一人物の回答は、最初の回答を正とする（重複回答は集計対象外）

● 同一企業で別部署からの回答が複数含まれていないかのチェック
- アンケート回答時に、事業者名（会社名）、回答者の部署・氏名・電話番号・メールアドレスを記入してもらい、その情報をもとに確認を実施。
- 例 1）代表取締役と事業部：より実態を把握していると想定される、「事業部」の回答を正とする
- 例 2）管理部門と IT 部門：より実態を把握していると想定される、「IT 部門」の回答を正とする

● アンケート対象とは異なる企業（地域 IT ベンダー以外）からの回答が含まれていないかのチェック
- 問 1（主な事業）の選択肢 14「その他」を選択している場合、「その他」の自由記述を一件ずつ精査し、集計対象を決定する

● 無回答項目や回答の矛盾点のチェック
- アンケートサイトの仕様上、必須質問の無回答項目は存在しないため割愛

また、回答データをもとに、単純集計に加えて以下の観点でのクロス集計を行った。

No	検証仮説	設問番号
1	中小企業から相談を受けている/受けていない企業の属性に差分があるか	問 13（顧客からのセキュリティに関する相談頻度）と以下のクロス集計 ・問 2（組織の成り立ち） ・問 1（主な事業）
2	地域 IT ベンダーの成り立ち（地域密着型/全国展開型）によって、中小企業への対応に差分があるか	問 2（組織の成り立ち）と以下のクロス集計 ・各種中小企業への対応設問 （問 18、20、22、24、26）
3	地域 IT ベンダーの成り立ちによって、セキュリティ技術者の数に差分があるか	問 32（自社のセキュリティ技術者の数）と以下のクロス集計 ・問 2（組織の成り立ち）

図表 3　アンケート調査のクロス集計の観点

2.1.2. ヒアリング調査

① 調査目的：

中小企業へのセキュリティ対応において、地域 IT ベンダーが果たしている役割や実施している取組等で、充実強化している点や課題解決で工夫している点等の具体的な取組内容を把握することを目的に実施した。

② 調査対象：

本調査は、以下の企業を対象として実施した。

- JISA 団体会員のうち、北海道、愛知県、福岡県、熊本県、沖縄県の 5 団体に加盟する地域 IT ベンダー企業（計 15 社）
- サイバーセキュリティお助け隊サービスの再販協力会社 4 社

③ 調査方法：

オンライン会議ツールを利用し、約 1 時間のヒアリングを実施した。

（有効回答数：19 件）

④ 調査期間： 2025 年 1 月 15 日（水）～2025 年 1 月 29 日（水）

⑤ 調査項目：

地域 IT ベンダーが、中小企業向けのシステム導入・運用を行う際に直面しているセキュリティ確保の現状と課題を把握するため、以下の項目を調査した。

- 提供サービスやシステムに関する状況を把握するための設問
  - セキュリティ確保の取組実施の考え方・方針、実施にあたっての課題
- 中小企業への対応状況を把握するための設問
  - セキュリティ意識が低い顧客とのやりとりにおける工夫
- 地域 IT ベンダーのセキュリティ対応能力の強化ポイントを把握するための設問
  - IPA の施策活用ニーズ
- 地域 IT ベンダー向け手引きの活用ニーズを把握するための設問
  - 地域 IT ベンダー向け手引きに必要な情報

2.2. アンケート調査結果

アンケート調査結果として、単純集計結果を 2.1.1～2.1.3 に、クロス集計結果を 2.1.4 に記載する。

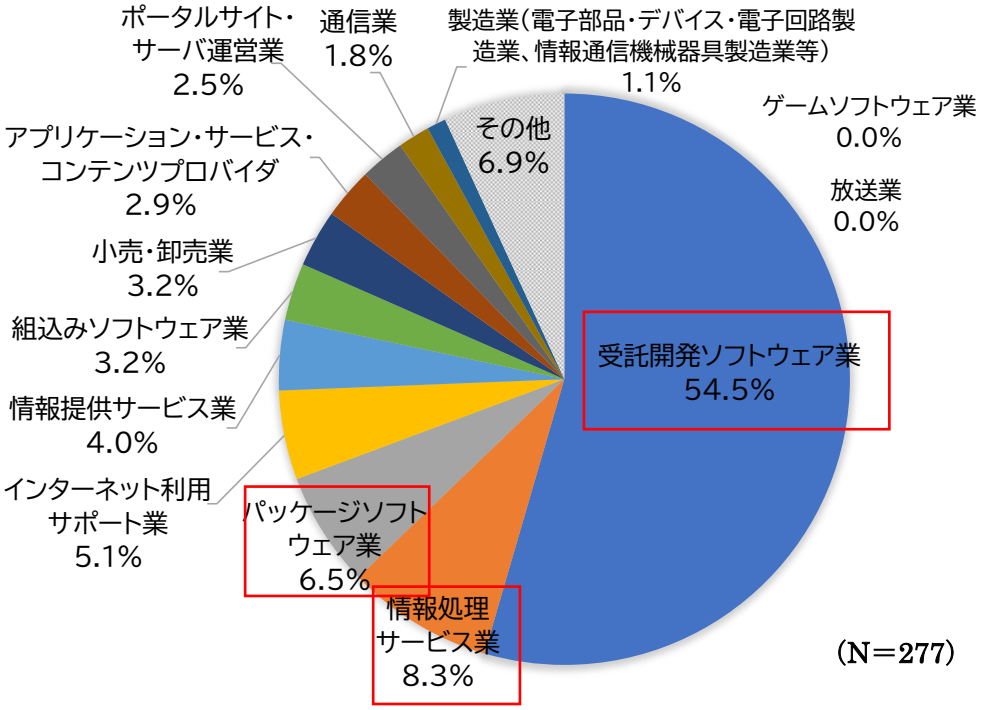
なお、グラフ上の数値について単純集計は小数点第 1 位まで表示している。また、図表タイトルにおいて（SA）は単一回答、（MA）は複数回答を表す。

2.2.1. 地域 IT ベンダー組織の属性

アンケート調査対象の地域 IT ベンダー組織の属性は以下のとおりである。

（1）地域 IT ベンダー組織の主な事業（問 1）

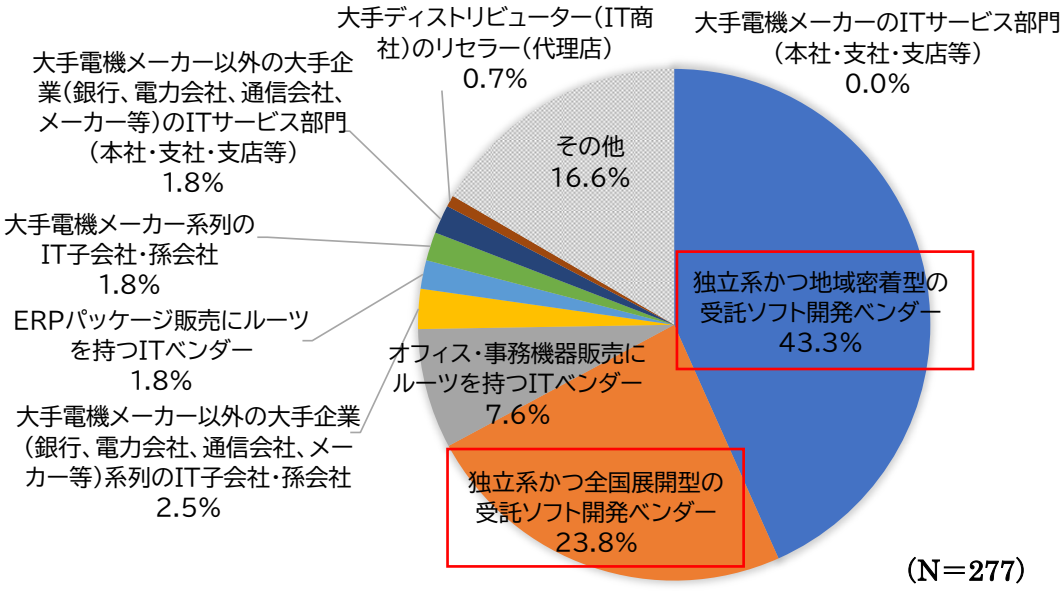
地域 IT ベンダー組織の主な事業は、「受託開発ソフトウェア業」が 54.5%で最も多く、次いで「情報処理サービス業」が 8.3%、「パッケージソフトウェア業」が 6.5%となっている。



図表 4　地域 IT ベンダー組織の主な事業（SA）

（2）地域 IT ベンダー組織の成り立ち（問 2）

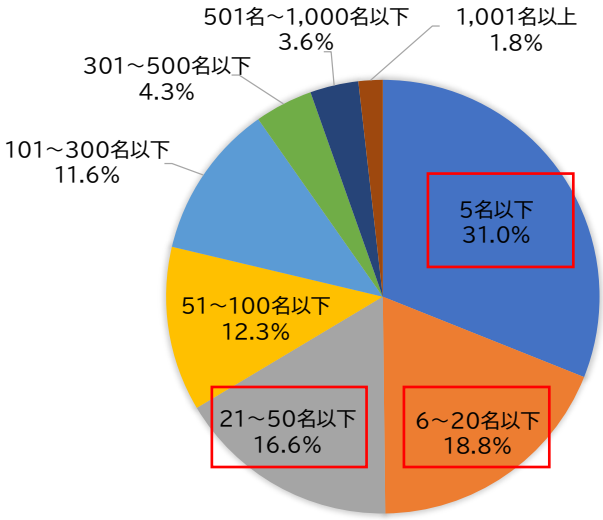
地域 IT ベンダー組織の成り立ちは、「独立系かつ地域密着型の受託ソフト開発ベンダー」が 43.3%で最も多く、次いで「独立系かつ全国展開型の受託ソフト開発ベンダー」が 23.8%であり、回答者全体の約 7 割を独立系の受託ソフト開発ベンダーが占めている。



図表 5　地域 IT ベンダー組織の成り立ち（SA）

（３）総従業員数（問 3）

地域 IT ベンダー組織の総従業員数は、「5 名以下」が 31.0%で最も多く、次いで「6 名～20 名以下」が 18.8%、「21～50 名以下」が 16.6%となっている。

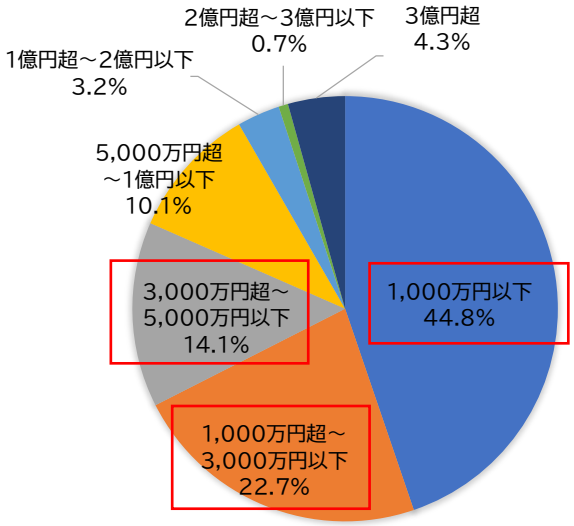


（N＝277）

図表 6　総従業員数（SA）

（４）資本金（問 4）

地域 IT ベンダー組織の資本金は、「1,000 万以下」が 44.8%で最も多く、次いで「1,000 万円超～3,000 万円以下」が 22.7%、「3,000 万円超～5,000 万円以下」が 14.1%となっている。

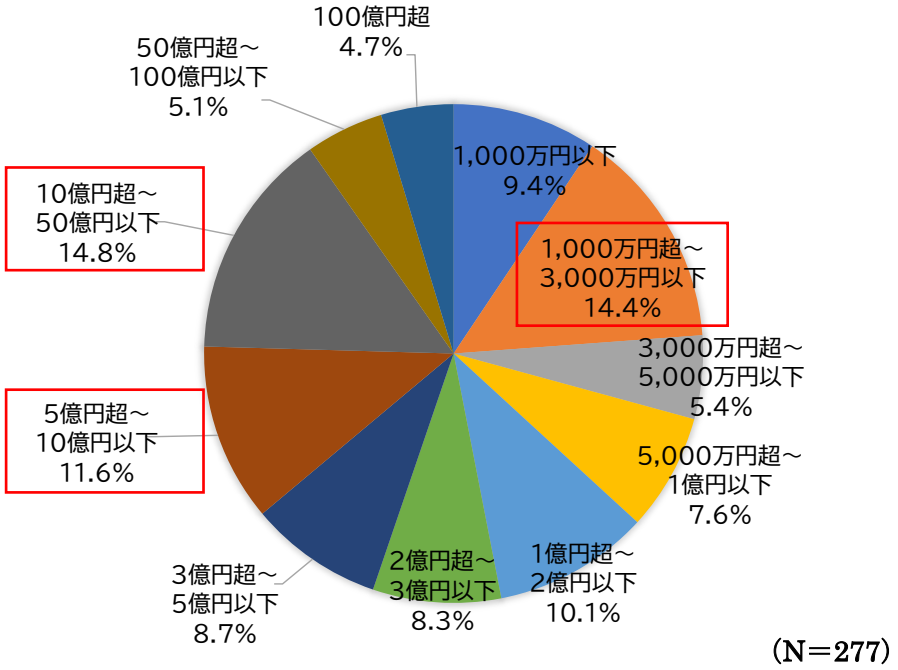


（N＝277）

図表 7　資本金（SA）

（5）総売上高（問 5）

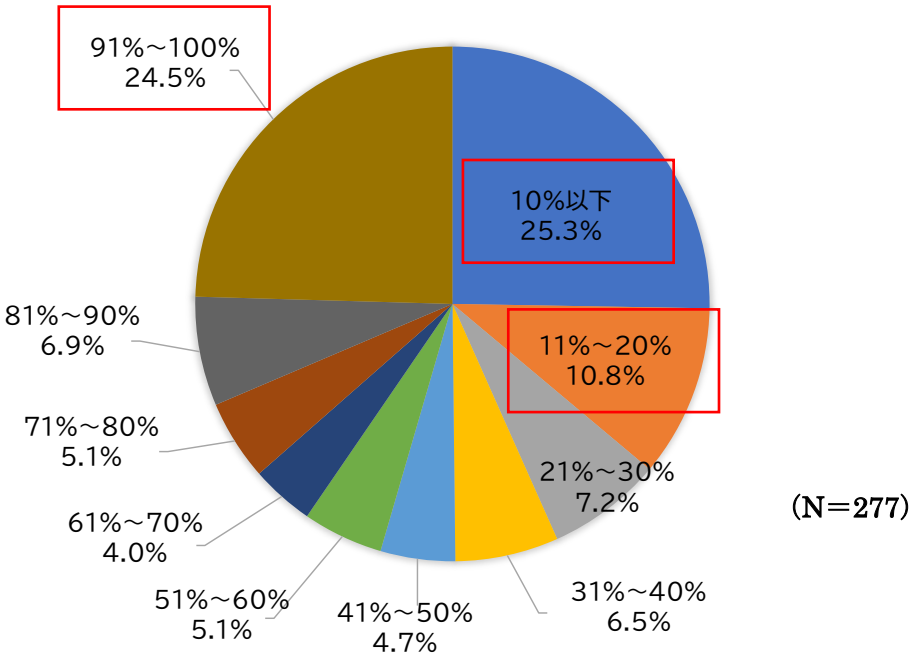
地域 IT ベンダー組織の総売上高は、「10 億円超～50 億円以下」が 14.8%で最も多く、次いで「1,000 万円超～3,000 万円以下」が 14.4%、「5 億円超～10 億円以下」が 11.6%となっている。



図表 8　総売上高（SA）

（6）総売上高のうち中小企業からの売上高が占める割合（問 6）

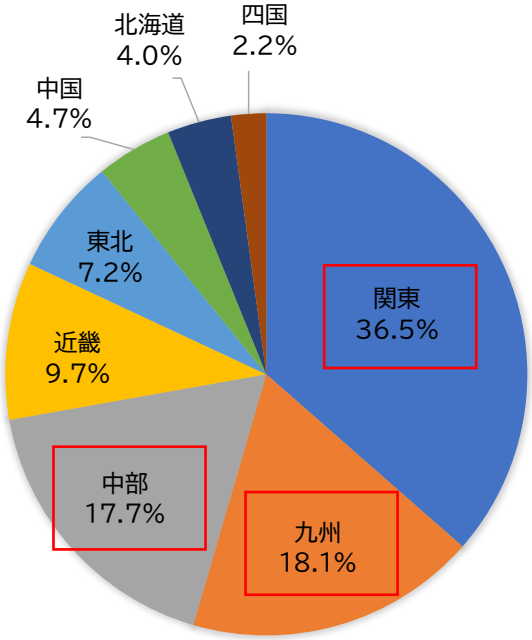
地域 IT ベンダー組織の総売上高のうち中小企業からの売上高が占める割合は、「10%以下」が 25.3%で最も多く、次いで「91%～100%」が 24.5%、「11%～20%」が 10.8%となっている。



図表 9　総売上高のうち中小企業からの売上高が占める割合（SA）

（7）本社所在地（問 7）

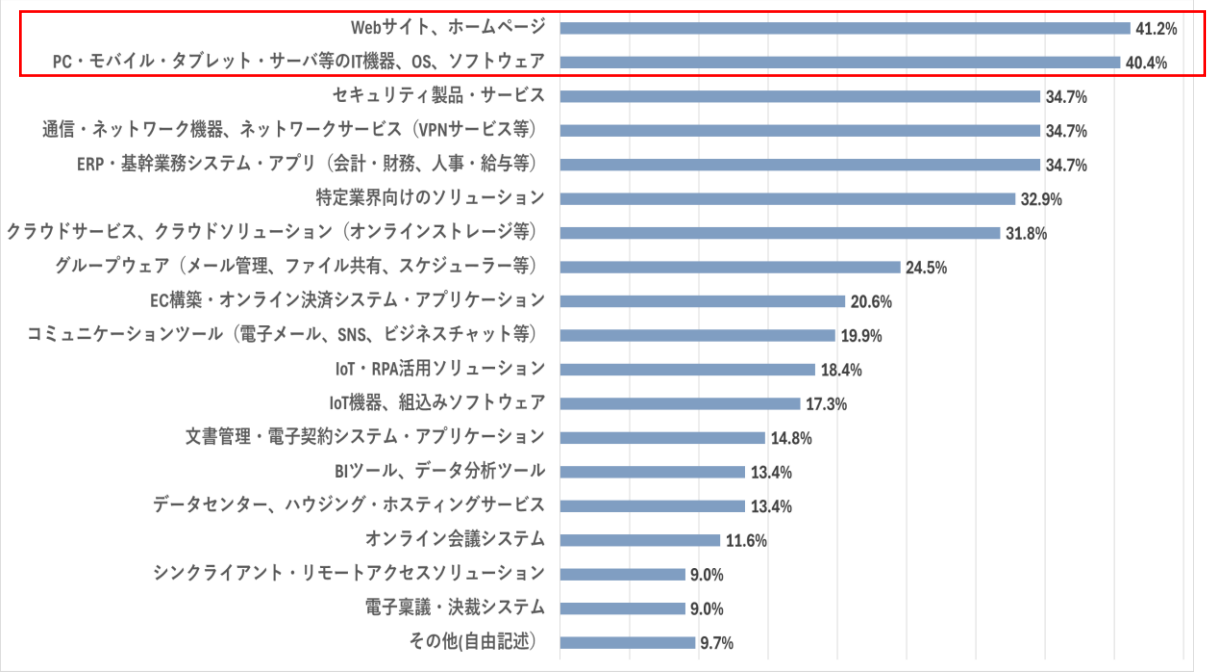
地域 IT ベンダー組織の本社所在地は、「関東」が 36.5%で最も多く、次いで「九州」が 18.1%、「中部」が 17.7%となっている。



図表 10　本社所在地（SA）

（8）提供しているサービスやシステム（問 8）

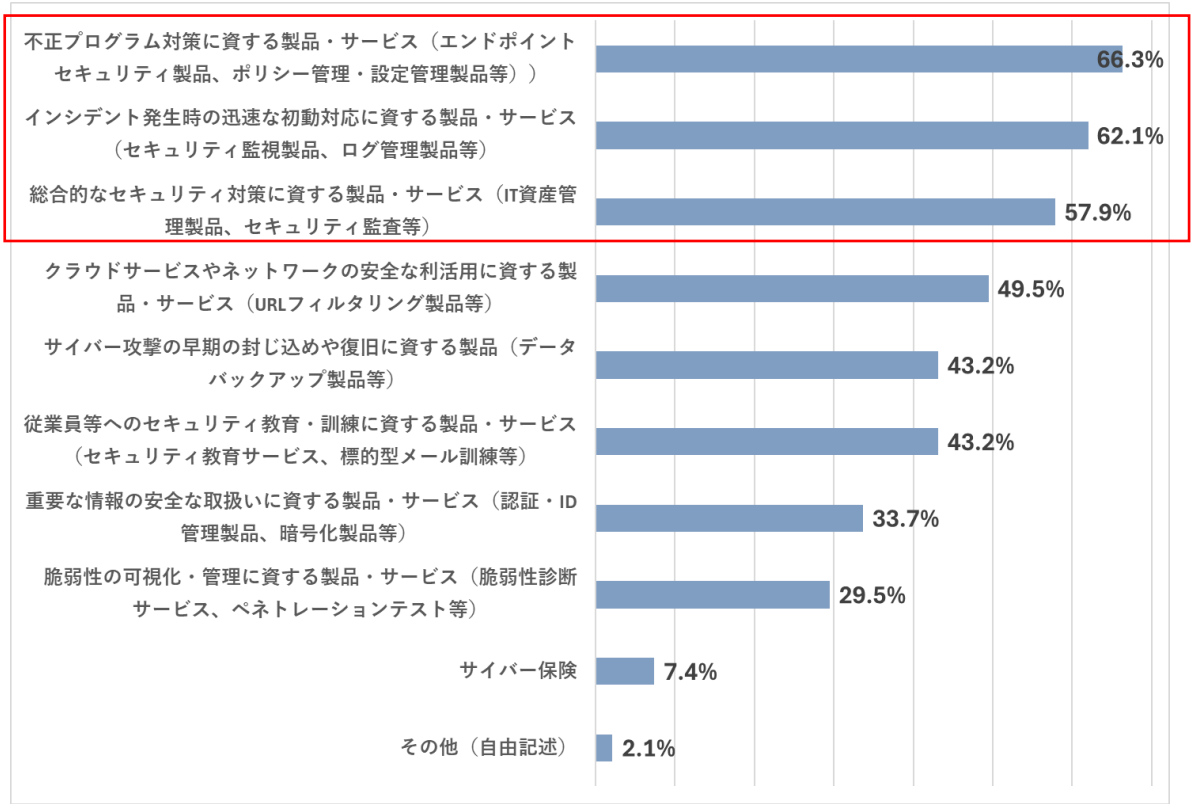
地域 IT ベンダーが中小企業向けに提供しているサービスやシステムは、「Web サイト、ホームページ」が 41.2%と最も多く、次いで「PC・モバイル・タブレット・サーバ等の IT 機器、OS、ソフトウェア」が 40.4%となっている。



図表 11　提供しているサービスやシステム（MA）

（9）提供しているセキュリティ製品・サービス（問 11）

地域 IT ベンダーが中小企業向けに提供しているサービスやシステムのうち、セキュリティ製品・サービスの具体的な内容は、「不正プログラム対策に資する製品・サービス」が 66.3%と最も多く、次いで「インシデント発生時の迅速な初動対応に資する製品・サービス」が 62.1%、「総合的なセキュリティ対策に資する製品・サービス」が 57.9%となっている。



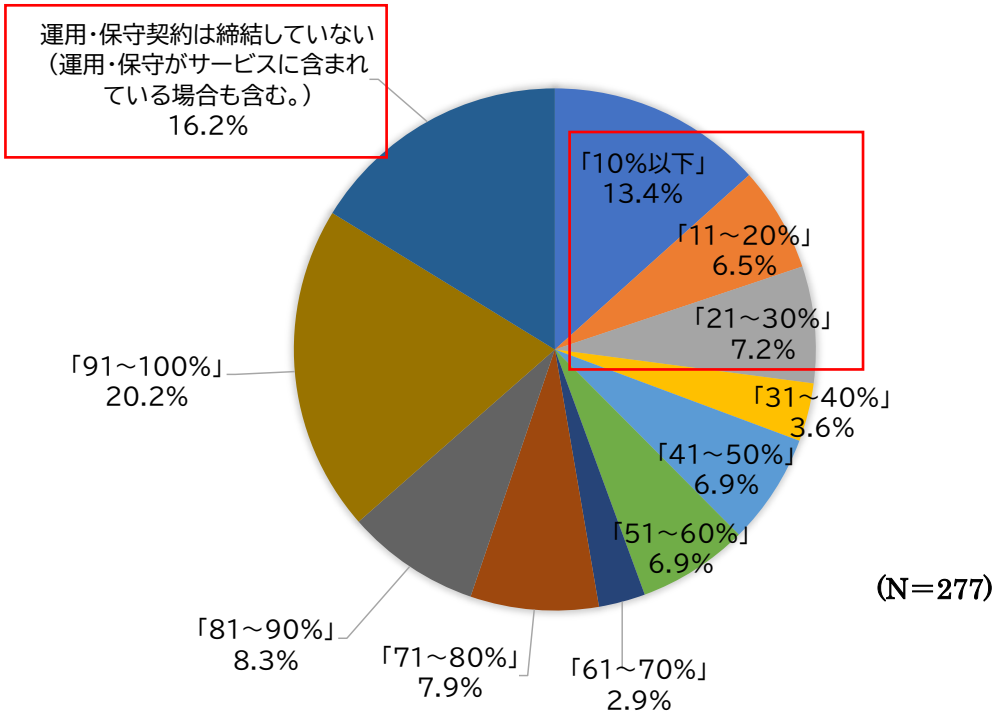
図表 12　提供しているセキュリティ製品・サービス（MA）

2.2.2. 中小企業のセキュリティ対応上の問題

アンケート結果から伺える、地域 IT ベンダーの顧客である中小企業が抱えるセキュリティ対応上の問題は以下のとおりである。

（1）運用・保守契約の締結状況（問 12）

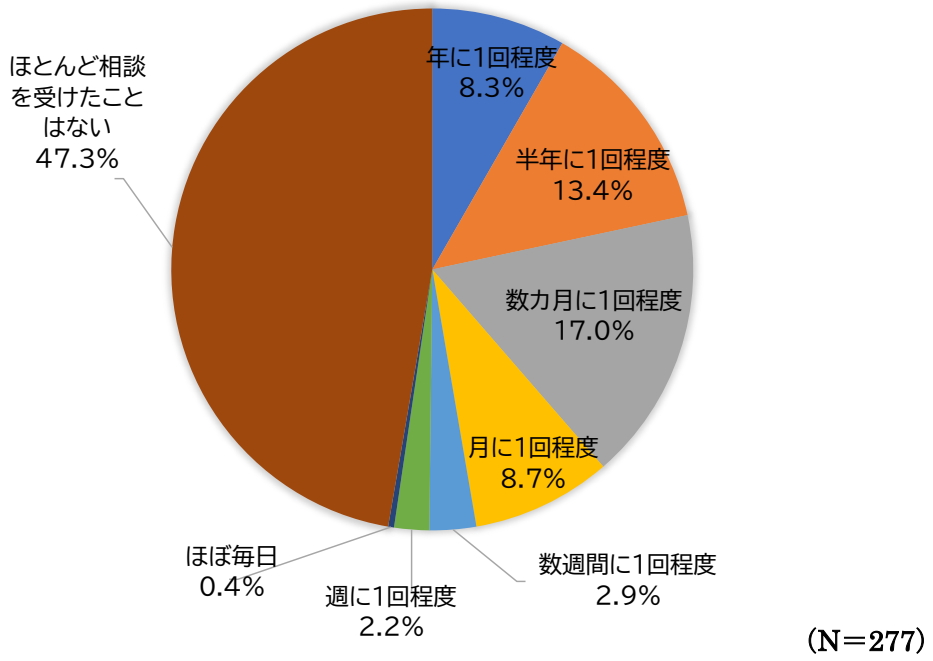
中小企業にサービスやシステムを導入後、顧客との間で締結する運用・保守契約を締結している顧客の割合について、3 割以下と回答した地域 IT ベンダーが 27.1%にのぼり、「運用・保守契約は締結していない」地域 IT ベンダーが 16.2%も存在するなど、IT システムを納品しても、その後の保守契約を締結していないケースが相当数に上っている。



図表 13　運用保守契約の締結状況（SA）

（2）顧客からのセキュリティに関する相談頻度（問 13）

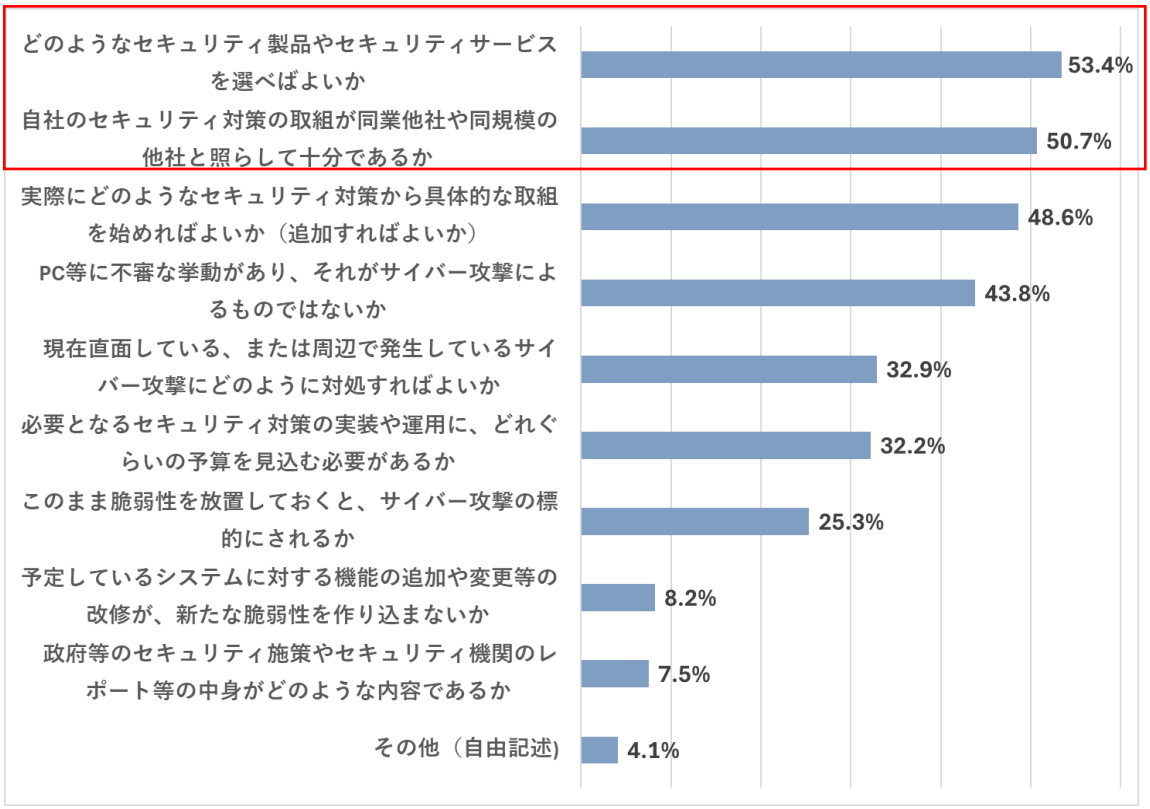
5 割以上の地域 IT ベンダーが、中小企業の顧客から自社が抱えるセキュリティ面の課題について相談を受けたことがあり、相談頻度は「数か月に 1 回程度」が 17.0%で最多く、次いで「半年に 1 回程度」が 13.4%となっている。



図表 14　顧客からのセキュリティに関する相談頻度（SA）

（3）顧客からのセキュリティに関する相談内容（問 14）

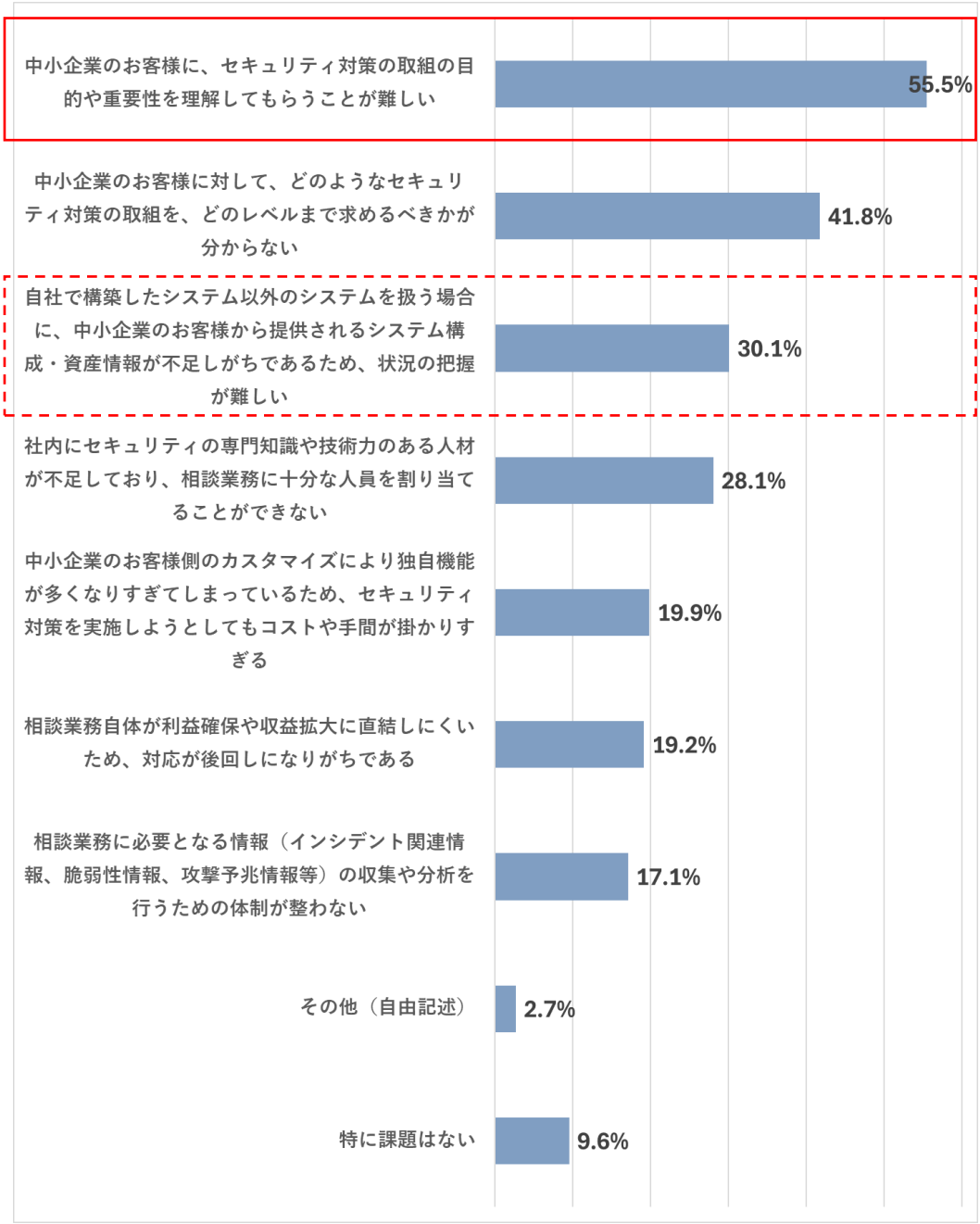
顧客から地域 IT ベンダーへのセキュリティに関する相談内容は、「どのようなセキュリティ製品やセキュリティサービスを選べばよいか」が 53.4%と最も多く、次いで「自社のセキュリティ対策の取組が同業他社や同規模の他社と照らして十分であるか」が 50.7%となっており、顧客からは地域 IT ベンダーを頼るような相談が多いといえる。



図表 15　顧客からのセキュリティに関する相談内容（MA）

（4）顧客からのセキュリティに関する相談対応にあたっての課題（問 15）

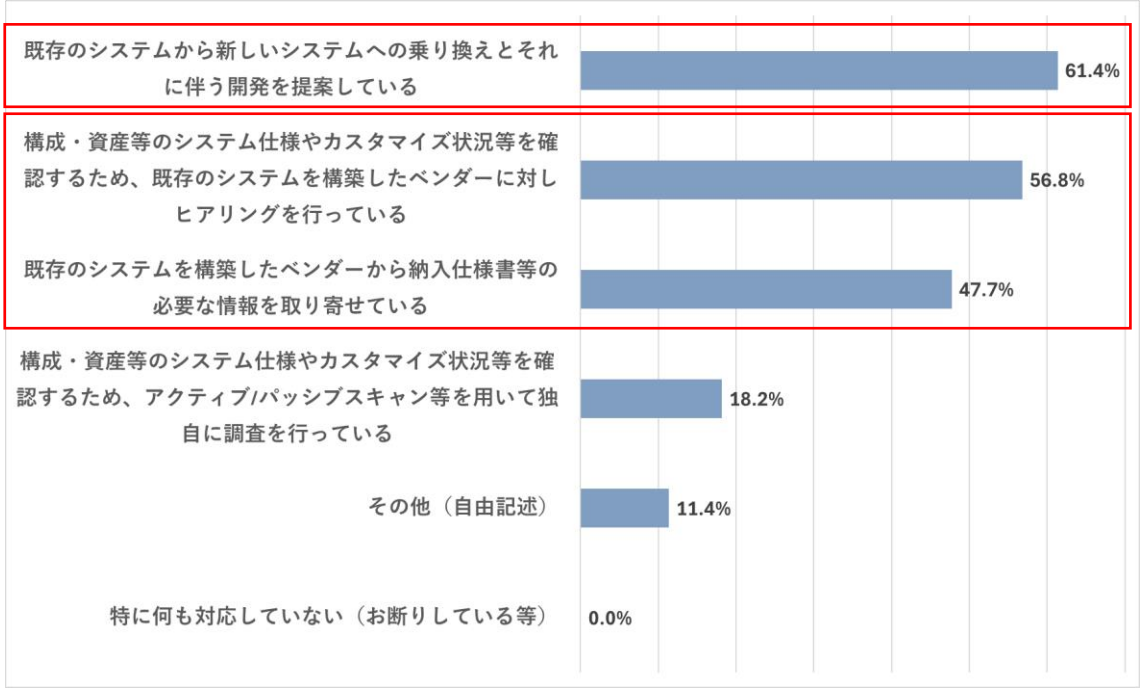
地域 IT ベンダーが顧客のセキュリティに関する相談対応にあたり直面している課題としては、「中小企業のお客様に、セキュリティ対策の取組の目的や重要性を理解してもらうことが難しい」が 55.5%と最も多く、顧客にセキュリティの重要性を理解してもらうことが困難な状況が伺える。



図表 16　顧客からのセキュリティに関する相談対応にあたっての課題（MA）

（５）自社以外の構築システムを扱う際にシステム構成等の把握が難しい場合の対応（問16）

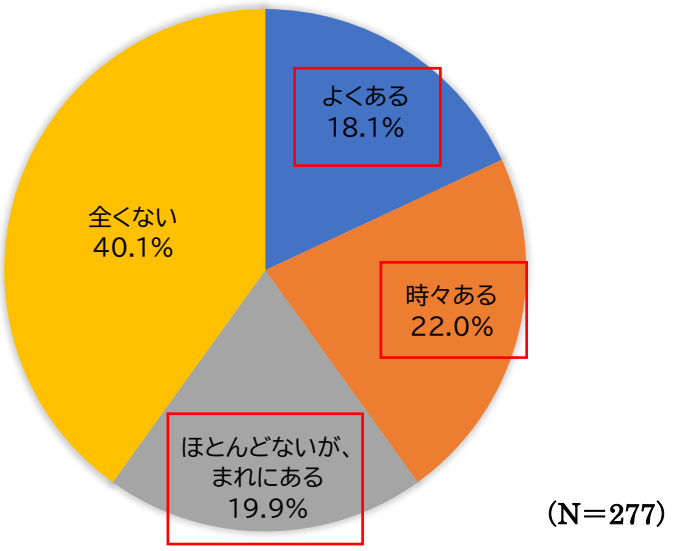
地域 IT ベンダーが顧客のセキュリティに関する相談対応にあたり直面している課題として、「自社で構築したシステム以外のシステムを扱う場合に、中小企業のお客様から提供されるシステム構成・資産情報が不足しがちであるため、状況の把握が難しい」と回答した地域 IT ベンダーが、そのような状況把握が難しい中、中小企業の顧客よりサポートを求められた場合の対応としては、「既存のシステムから新しいシステムへの乗り換えとそれに伴う開発を提案している」が 61.4%と最も多かった。一方で、「構成・資産等のシステム仕様やカスタマイズ状況等を確認するため、既存のシステムを構築したベンダーに対しヒアリングを行っている」が 56.8%、「既存のシステムを構築したベンダーから納入仕様書等の必要な情報を取り寄せている」が 47.7%と、積極的にベンダー間の連携を図る動きも見てとれる。



図表 17　自社以外の構築システムを扱う際にシステム構成等の把握が難しい場合の対応（MA）

（６）顧客からセキュリティ要素が不十分な要求仕様を提示された経験（問 17）

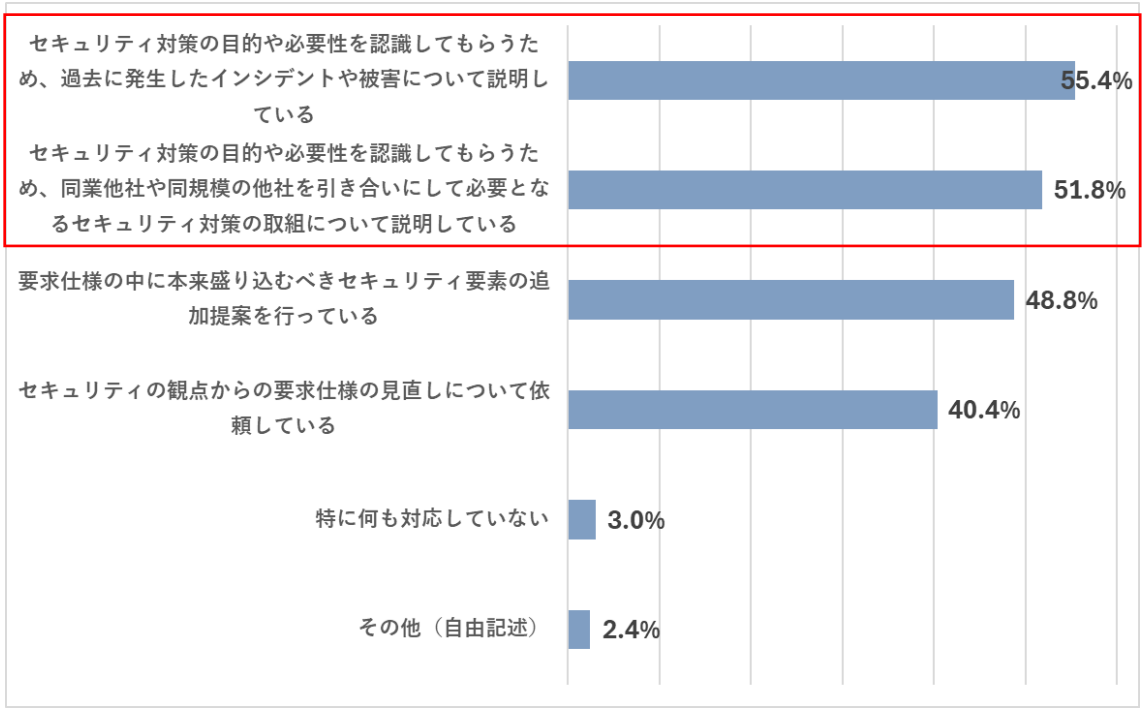
中小企業の顧客から地域 IT ベンダーに対して、セキュリティ要素が十分に考慮されていない要求仕様を含む提案依頼書を提示された経験があるか、の問いに対して、「よくある」（18.1%）、「時々ある」（22.0%）、「まれにある」（19.9%）を含め、約 6 割の地域 IT ベンダーが、経験があると回答している。



図表 18　顧客からセキュリティ要素が不十分な要求仕様を提示された経験（SA）

（7）顧客のセキュリティ要素が不十分な要求仕様に対する対応（問 18）

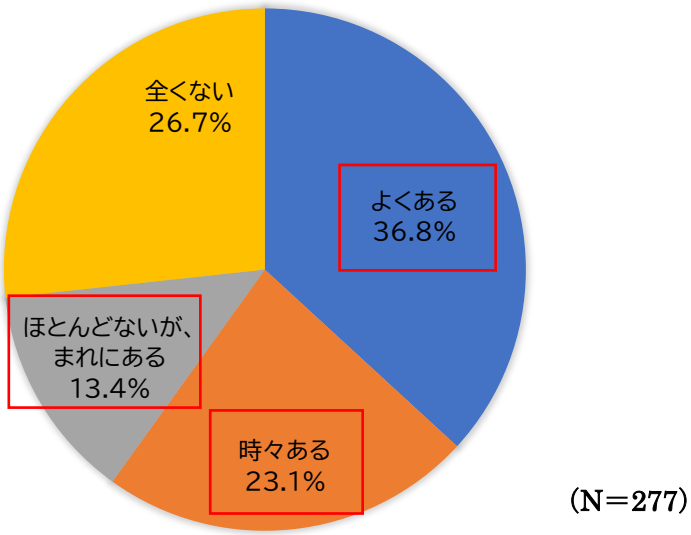
地域 IT ベンダーが中小企業の顧客からセキュリティ要素が不十分な要求仕様を提示された際の対応としては、「セキュリティ対策の目的や必要性を認識してもらうため、過去に発生したインシデントや被害について説明している」が 55.4%と最も多く、次いで「セキュリティ対策の目的や必要性を認識してもらうため、同業他社や同規模の他社を引き合いにして必要となるセキュリティ対策の取組について説明している」が 51.8%となっている。



図表 19　顧客のセキュリティ要素が不十分な要求仕様に対する対応（MA）

（8）顧客にシステム・セキュリティ技術者がいないケース（問 19）

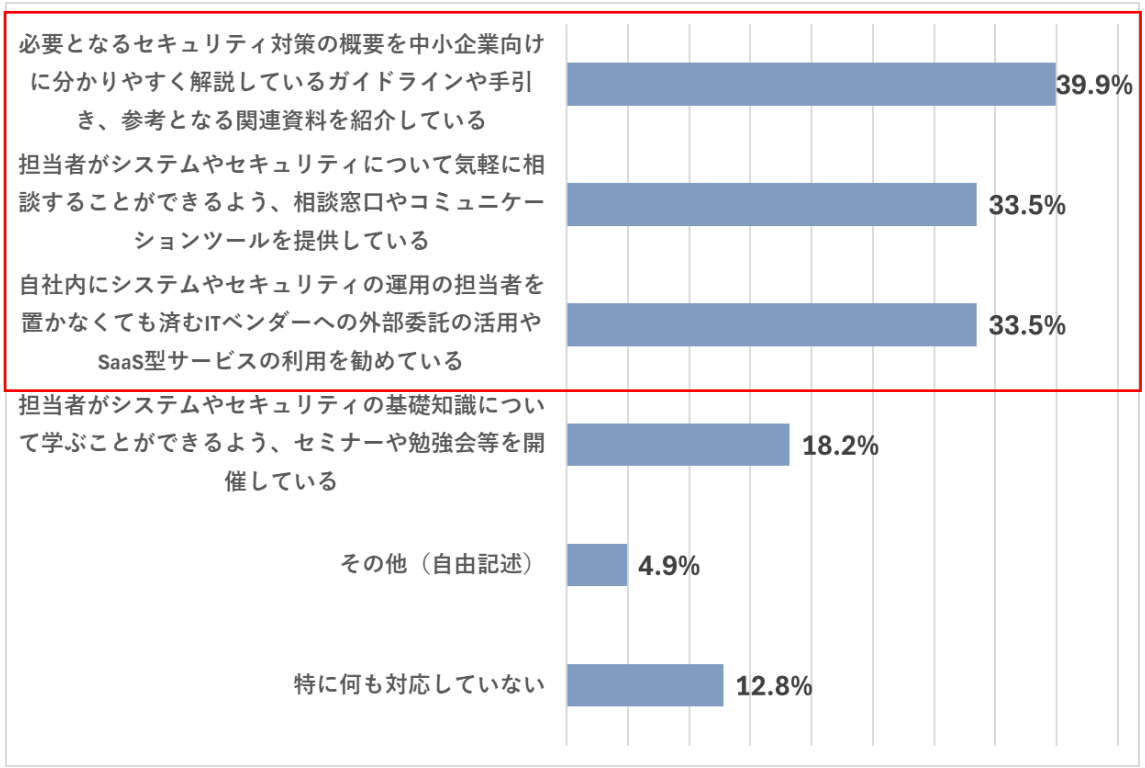
地域 IT ベンダーへの発注後、中小企業の顧客側にシステムやセキュリティに関する技術や知識を持つ技術者がいないケースは、「よくある」が 36.8%と最も多く、「時々ある」（23.1%）と「まれにある」（13.4%）まで含めると約 7 割となっており、中小企業の顧客側にシステム・セキュリティの技術者がいない状況であることが分かる。



図表 20　顧客にシステム・セキュリティ技術者がいないケース（SA）

（9）顧客にシステム・セキュリティ技術者がいない際の対応（問 20）

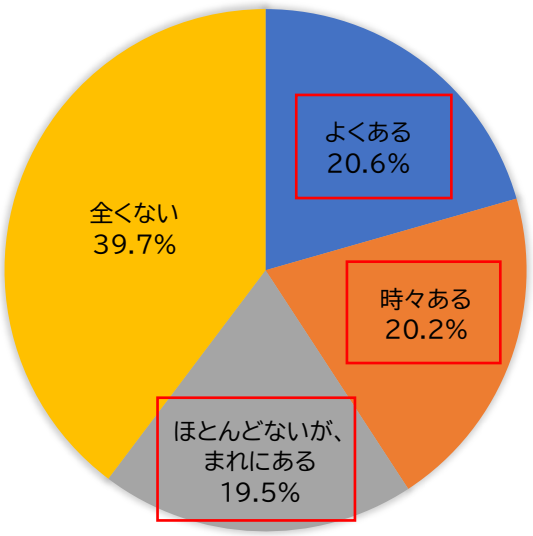
中小企業の顧客側にシステム・セキュリティの技術者がいない際の地域 IT ベンダーの対応としては、「必要となるセキュリティ対策の概要を中小企業向けに分かりやすく解説しているガイドラインや手引き、参考となる関連資料を紹介している」が 39.9%と最も多く、「自社内にシステムやセキュリティの運用の担当者を置かなくても済む地域 IT ベンダーへの外部委託の活用や SaaS 型サービスの利用を勧めている」が 33.5%、「担当者がシステムやセキュリティについて気軽に相談することができるよう、相談窓口やコミュニケーションツールを提供している」が 33.5%となっている。



図表 21　顧客にシステム・セキュリティ技術者がいない際の対応（MA）

(10)顧客からセキュリティ対策の実装を最低限に抑えるよう指示を受けた経験(問21)

地域 IT ベンダーが中小企業の顧客との間で要件定義の調整を行う際に、コスト制約等の理由によりセキュリティ対策については最低限の実装に抑えるよう指示を受けることがあるか、の問いに対して、「よくある」(20.6%)、「時々ある」(20.2%)、「まれにある」(19.5%) を含め、約 6 割の地域 IT ベンダーが、経験があると回答している。

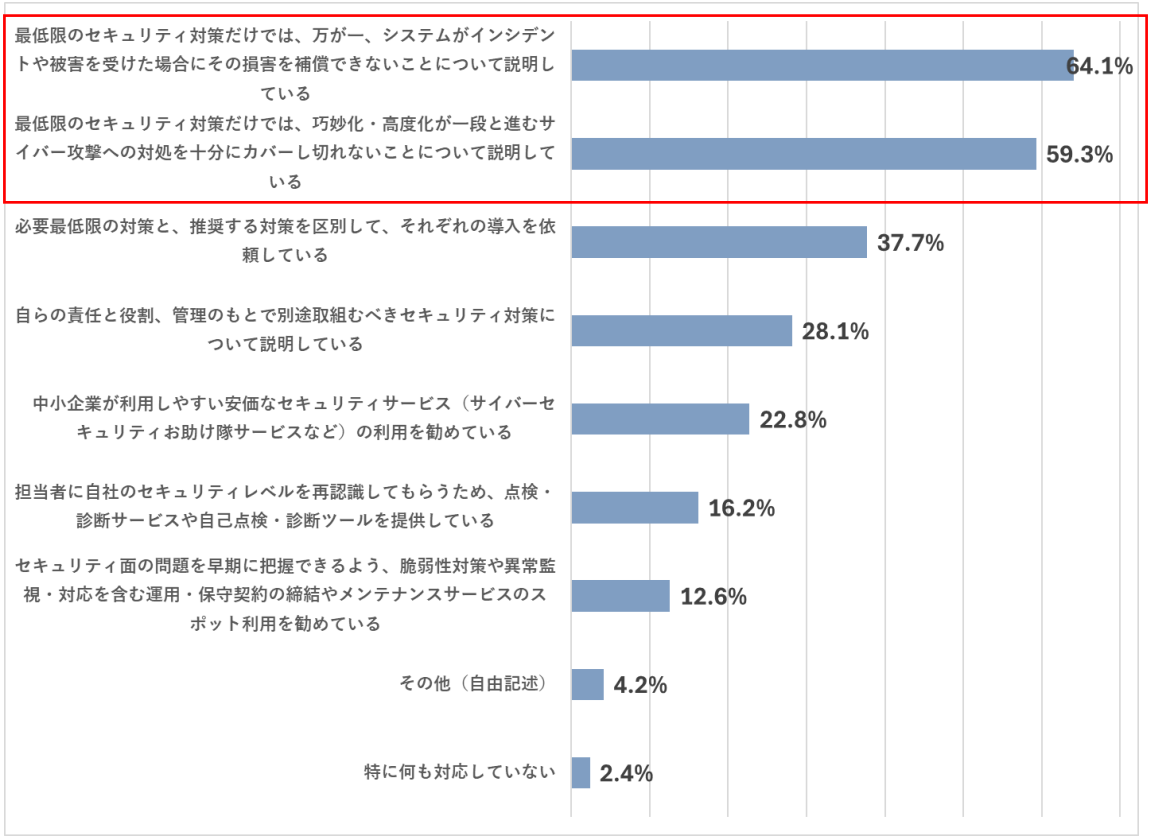


(N=277)

図表 22　顧客からセキュリティ対策の実装を最低限に抑えるよう指示を受けた経験 (SA)

（11）顧客のセキュリティ対策実装の抑制指示に対する対応（問 22）

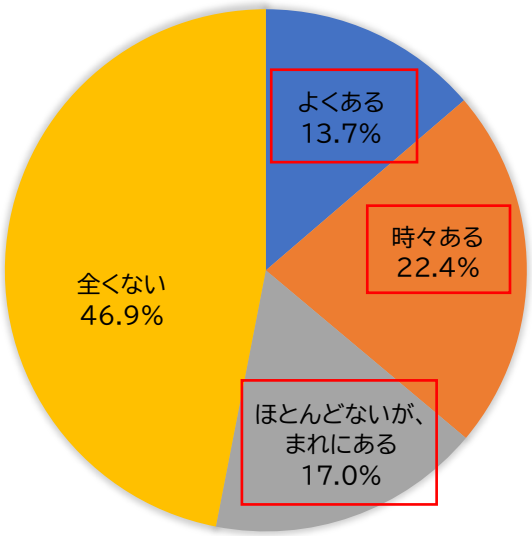
顧客のセキュリティ対策実装の抑制指示を受けた際に、地域 IT ベンダーがおこなった対応としては、「最低限のセキュリティ対策だけでは、万が一、システムがインシデントや被害を受けた場合に、その被害を補償できないことについて説明している」が 64.1%で最も多く、次いで「最低限のセキュリティ対策だけでは、巧妙化・高度化が一段と進むサイバー攻撃への対処を十分にカバーし切れないことについて説明している」が 59.3%となっている。



図表 23　顧客のセキュリティ対策実装の抑制指示に対する対応（MA）

（12）顧客にセキュリティ対策の運用に係る応分の負担を求めた経験（問 23）

地域 IT ベンダーが中小企業の顧客との間で要件定義の調整を行う際に、コスト制約等の理由により顧客に対してセキュリティ対策の運用に係る応分の負担を求めたことがあるか、の問いに対して、「よくある」（13.7%）、「時々ある」（22.4%）、「まれにある」（17.0%）を含め、約 5 割の地域 IT ベンダーが、経験があると回答している。

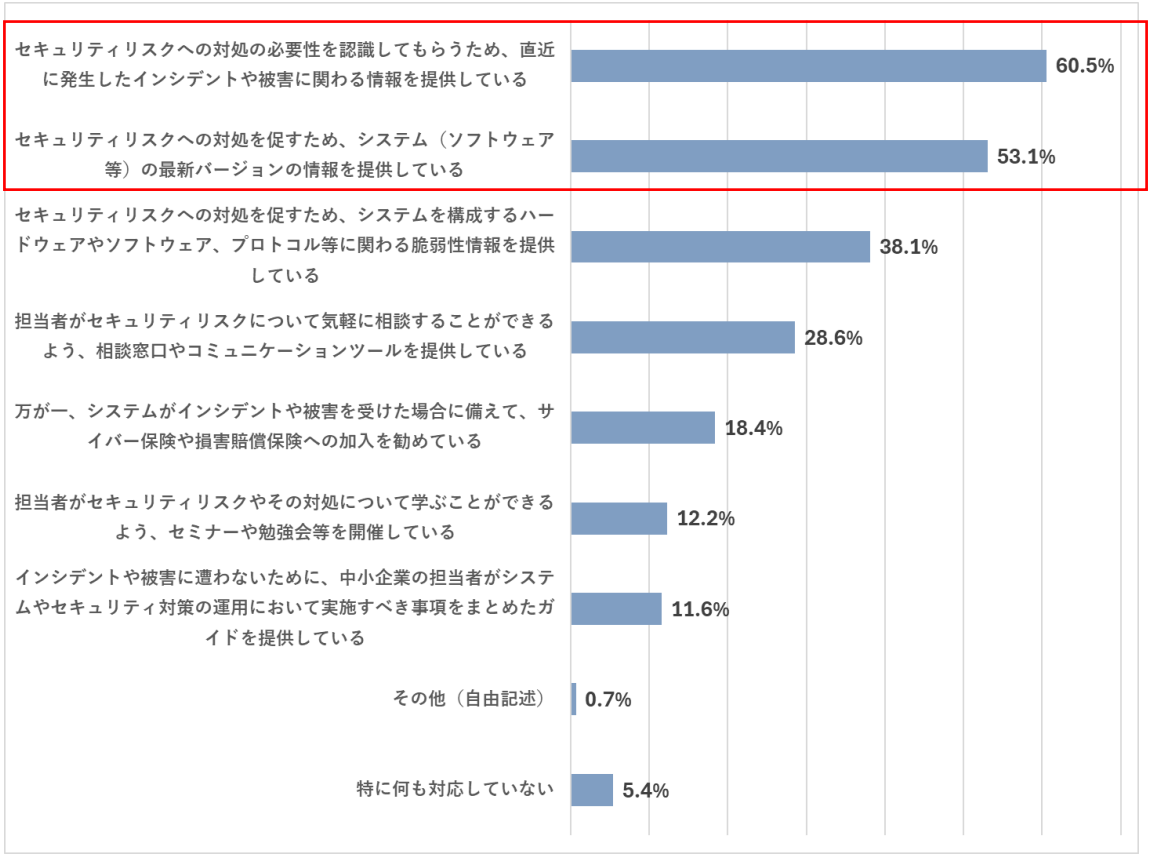


（N＝277）

図表 24　顧客にセキュリティ対策の運用に係る応分の負担を求めた経験（SA）

（13）顧客にセキュリティ対策の運用に係る応分の負担を求める際の対応（問 24）

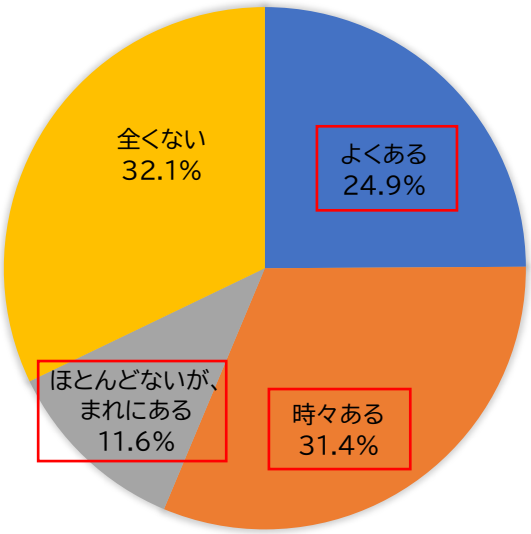
地域 IT ベンダーが、中小企業の顧客にセキュリティ対策の運用に係る応分の負担を求める際の対応としては、「セキュリティリスクへの対処の必要性を認識してもらうため、直近に発生したインシデントや被害に関わる情報を提供している」が 60.5%で最も多く、次いで「セキュリティリスクへの対処を促すため、システムの最新バージョンを提供している」が 53.1%、となっている。



図表 26　顧客にセキュリティ対策の運用に係る応分の負担を求める際の対応（MA）

(14) 顧客社内でのサービス・システム導入体制が不十分であった経験（問 25）

地域 IT ベンダーが中小企業の顧客にサービスやシステムを導入し、運用を開始する際に、顧客側の社内での導入体制が十分に整備されていない状況に直面したことがあるか、の問いに対して、「よくある」(24.9%)、「時々ある」(31.4%)、「まれにある」(11.6%) を含め、約 7 割の地域 IT ベンダーが、経験があると回答している。

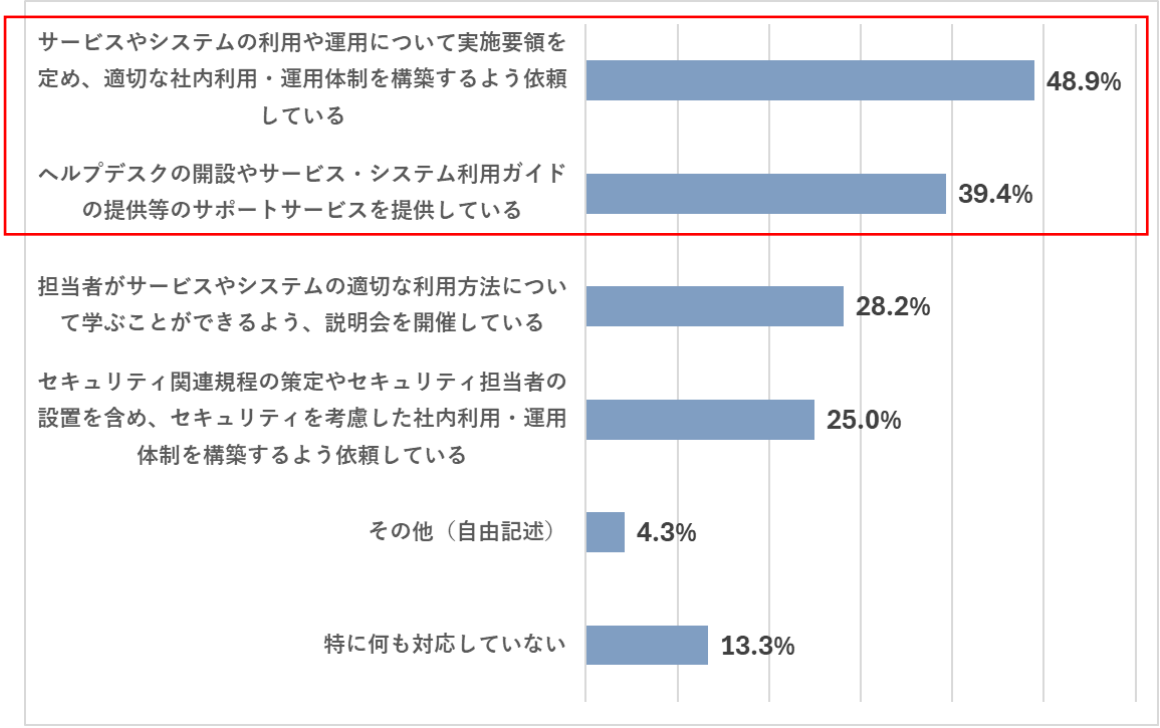


(N＝277)

図表 27　顧客社内でのサービス・システム導入体制が不十分であった経験（SA）

(15) 顧客社内でのサービス・システム導入体制が不十分な際の対応（問 26）

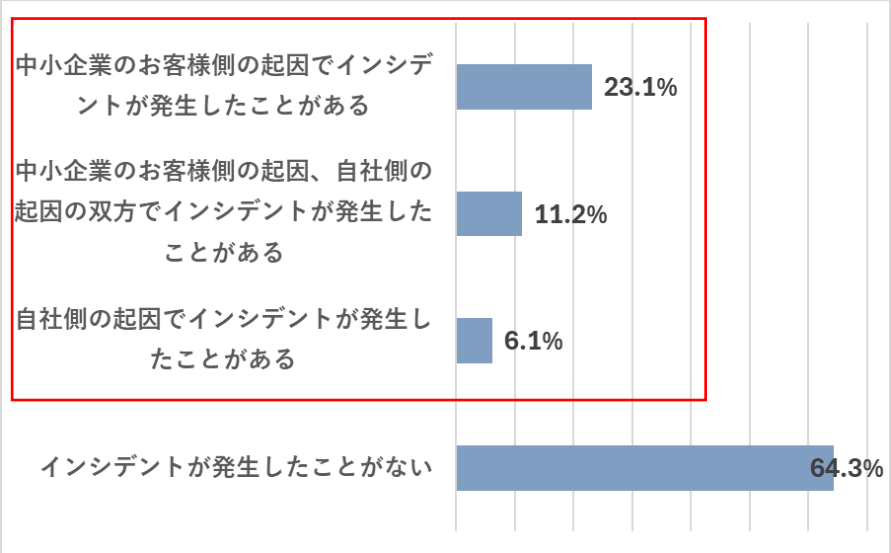
顧客社内でのサービス・システム導入体制が不十分な際の地域 IT ベンダーの対応としては、「サービスやシステムの利用や運用について実施要領を定め、適切な社内利用・運用体制を構築するよう依頼している」が 48.9%と最も多く、続いて「ヘルプデスクの開設やサービス・システム利用ガイドの提供等のサポートサービスを提供している」が 39.4%となっている。



図表 28　顧客社内でのサービス・システム導入体制が不十分な際の対応（MA）

（16）顧客のサービス・システム運用時のインシデント発生の経験（問 27）

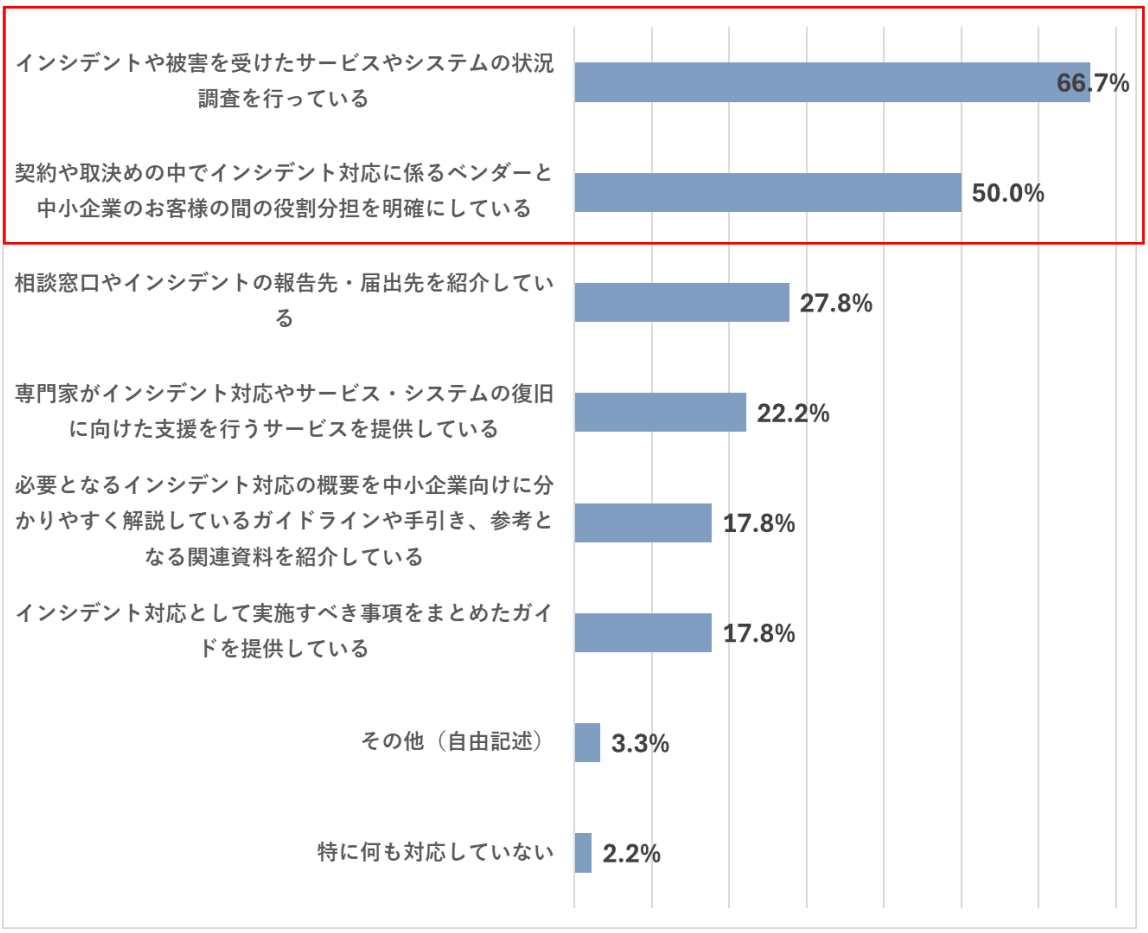
中小企業の顧客のサービスやシステムの運用時に、当該サービスやシステムに関連して、顧客側の起因または地域 IT ベンダー（自社）側の起因、またはその双方によりインシデントが発生したことがあるか、の問いに対して、約 4 割の地域 IT ベンダーが、インシデント発生の経験があると回答している。



図表 29　顧客のサービス・システム運用時のインシデント発生の経験（MA）

（17）顧客側起因のインシデント発生の際の対応（問 28）

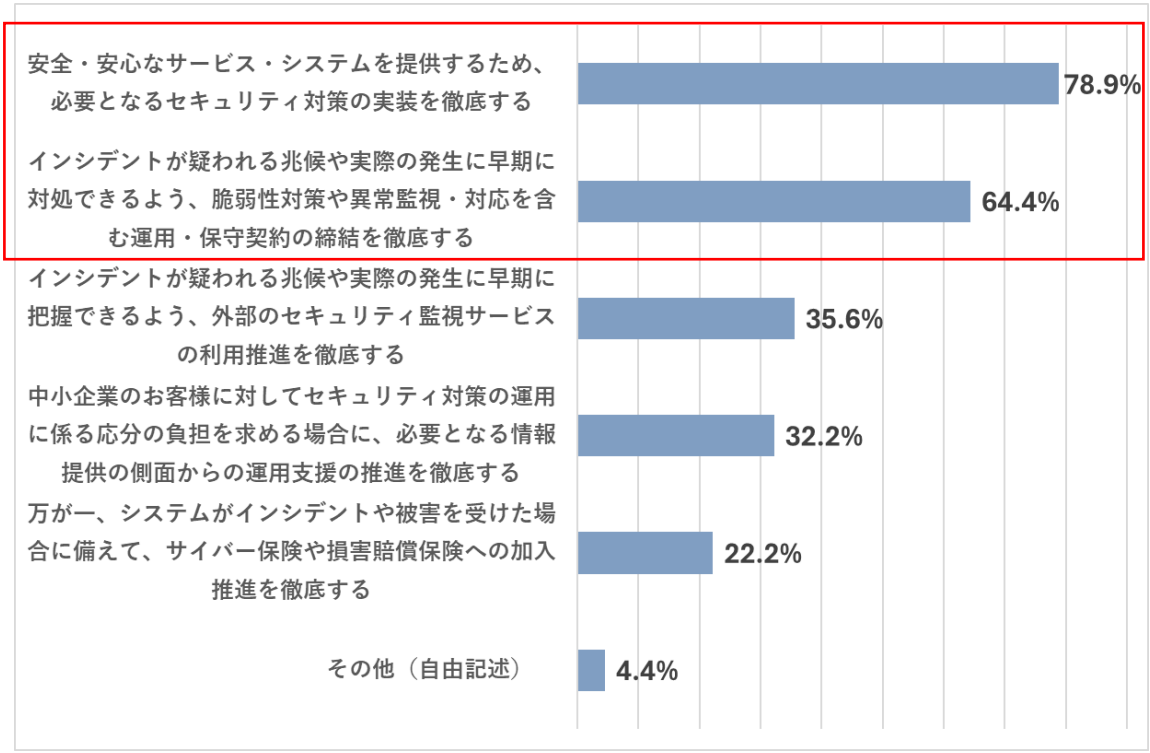
中小企業の顧客側起因のインシデントが発生した場合の地域 IT ベンダーの支援対応としては、「インシデントや被害を受けたサービスやシステムの状況調査を行っている」が 66.7%と最も多く、続いて「契約や取決めの中でインシデント対応に係るベンダーと中小企業のお客様の間の役割分担を明確にしている」が 50.0%となっている。



図表 30　顧客側起因のインシデント発生の際の対応（MA）

（18）顧客側起因のインシデント発生に備えて今後対応を強化したいこと（問 29）

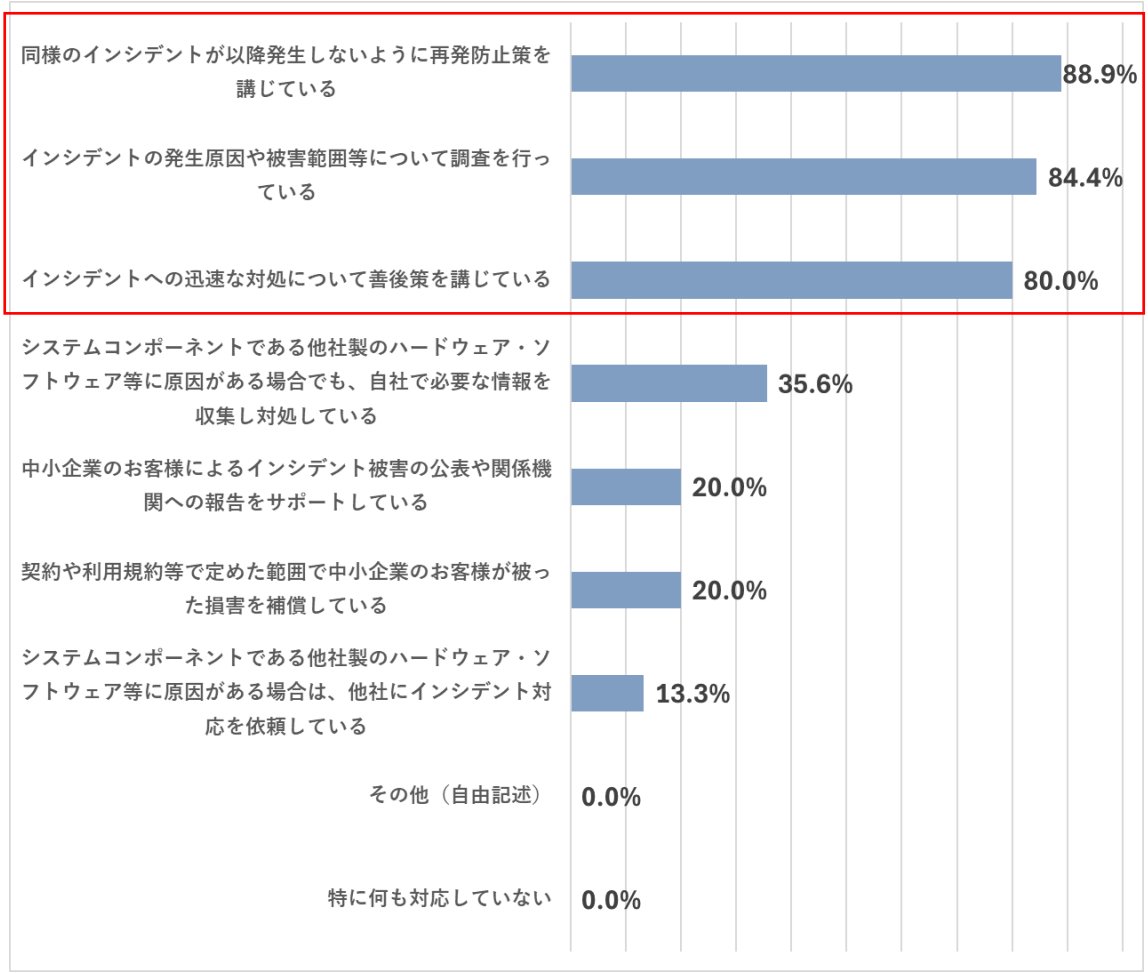
中小企業の顧客側起因のインシデントが発生した場合に備えて、地域 IT ベンダーが顧客との間で今後どのような対応強化が重要になると考えるか、の問いに対する回答としては、「安全・安心なサービス・システムを提供するため、必要となるセキュリティ対策の実装を徹底する」が 78.9%と最も多く、次いで「インシデントが疑われる兆候や実際の発生に早期に対処できるよう、脆弱性対策や異常監視・対応を含む運用・保守契約の締結を徹底する」が 64.4%となっている。



図表 31　顧客側起因のインシデント発生に備えて今後対応を強化したいこと（MA）

(19) 自社側起因により顧客のサービス・システムでインシデントが発生した際の対応（問 30）

地域 IT ベンダー（自社）側の起因により顧客のサービス・システムでインシデントが発生した際の対応としては、「同様のインシデントが以降発生しないように再発防止策を講じている」が 88.9%で最も多く、続いて「インシデントの発生原因や被害範囲等について調査を行っている」が 84.4%、「インシデントへの迅速な対処について善後策を講じている」が 80.0%となっている。



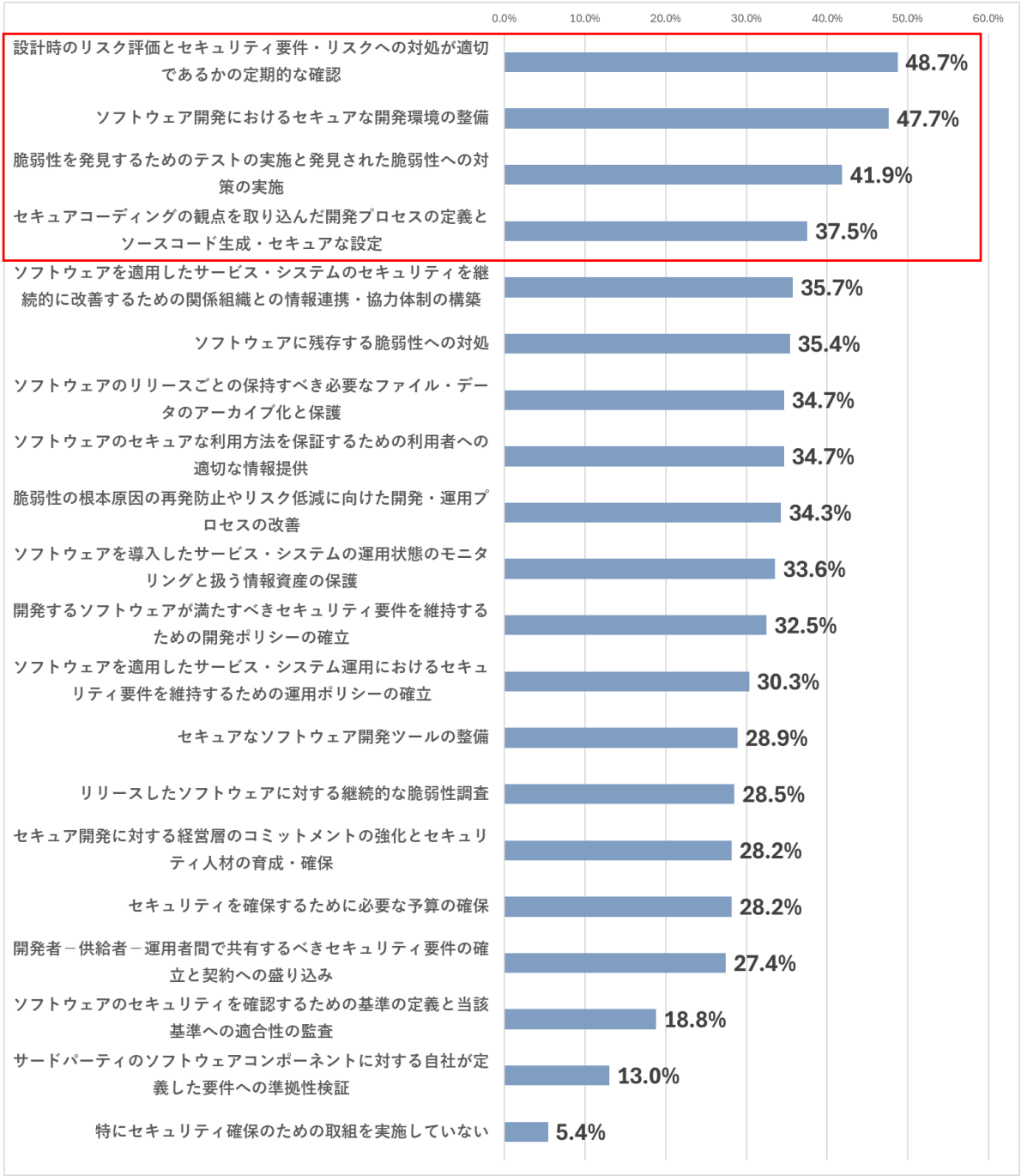
図表 32　自社側起因により顧客のサービス・システムでインシデントが発生した際の対応（MA）

2.2.3. 地域 IT ベンダーのセキュリティ確保の取組状況

アンケート結果から伺える、地域 IT ベンダーにおけるセキュリティ確保の取組状況及び対策実施上の課題は以下のとおりである。

（1）提供サービスやシステムにおけるセキュリティ確保のための取組（問 9）

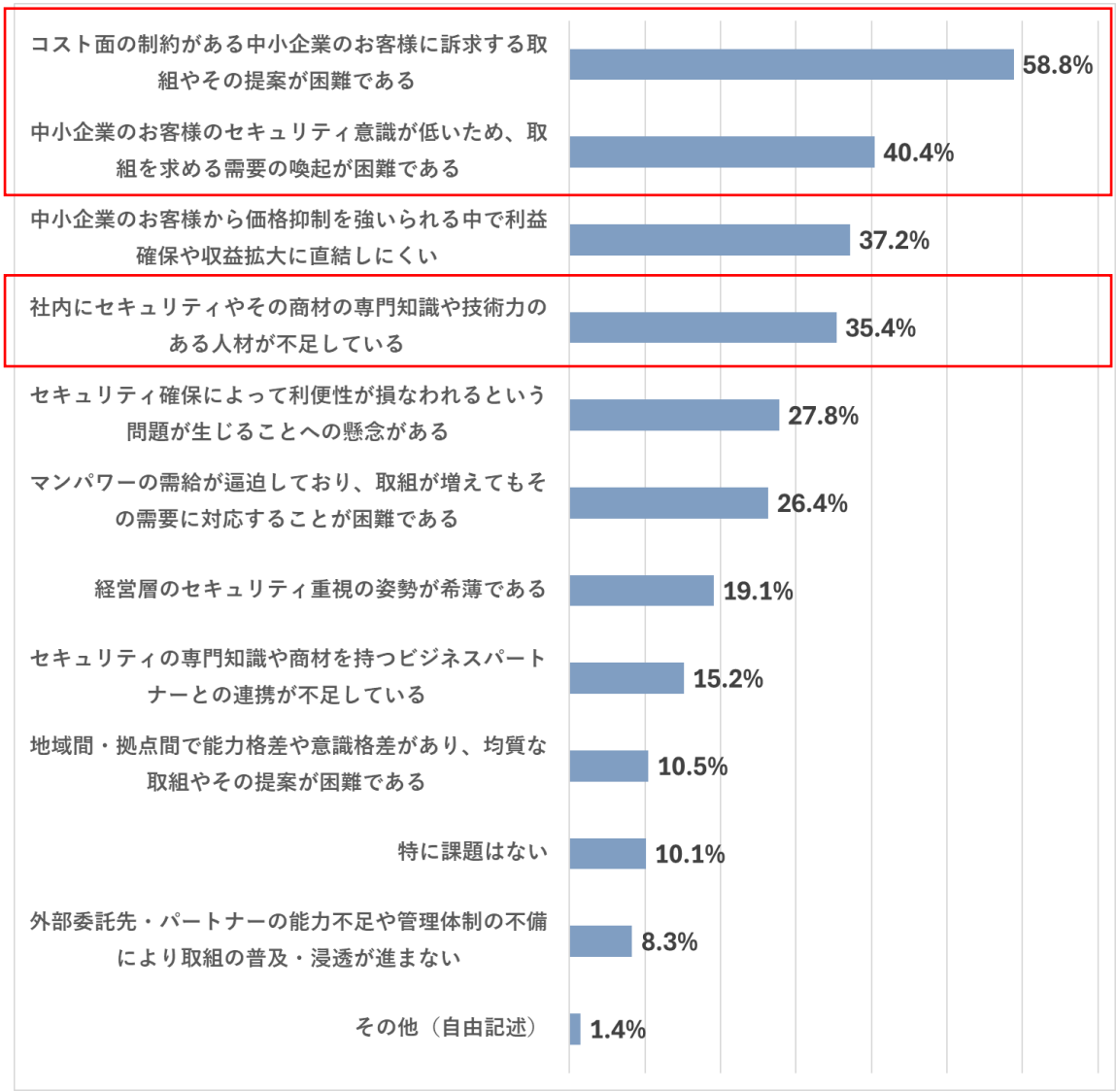
地域 IT ベンダーが、提供サービスやシステムにおけるセキュリティ確保のために実施している取組としては、「設計時のリスク評価とセキュリティ要件・リスクへの対処が適切であるかの定期的な確認」が 48.7%と最も多く、次いで「ソフトウェア開発におけるセキュアな開発環境の整備」が 47.7%、「脆弱性を発見するためのテストの実施と発見された脆弱性への対策の実施」が 41.9%となっている。



図表 33　提供サービスやシステムにおけるセキュリティ確保のための取組（MA）

（2）提供サービス・システムのセキュリティ確保の取組の実施上の課題（問 10）

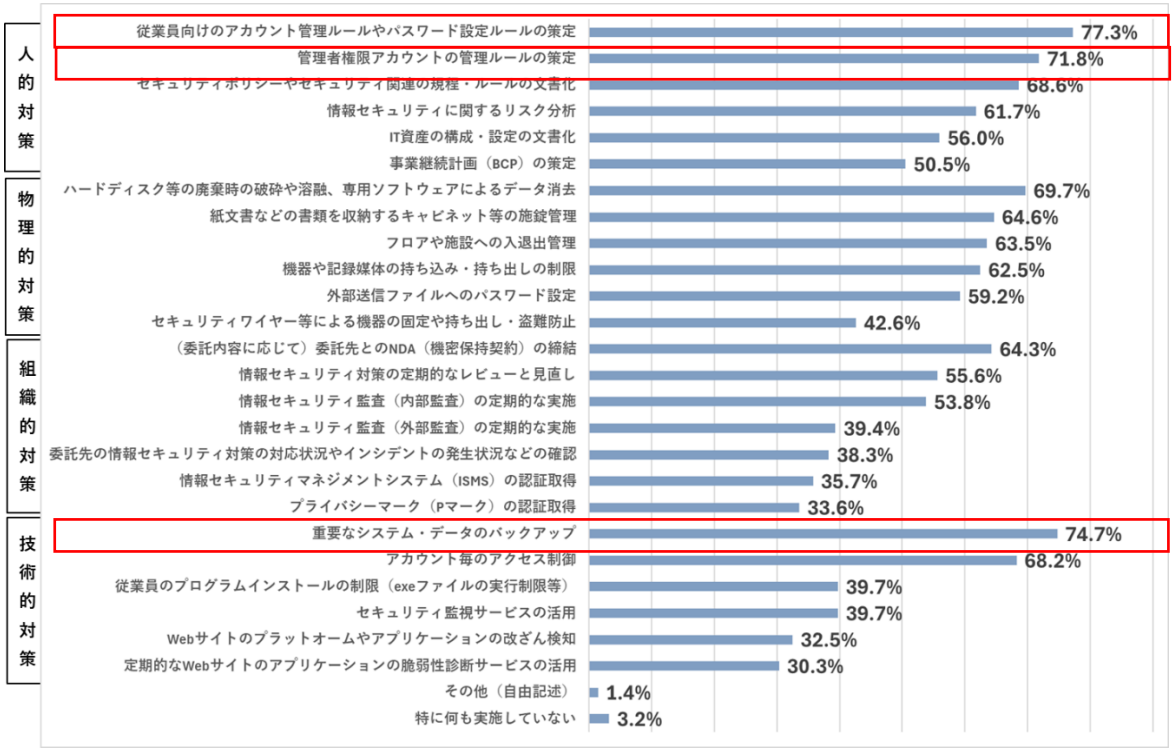
地域 IT ベンダーが、提供サービス・システムのセキュリティ確保のための取組を実施する上での課題は、「コスト面の制約がある中小企業のお客様に訴求する取組やその提案が困難である」が 58.8%、と最も多く、次いで「中小企業のお客様のセキュリティ意識が低いため、取組を求める需要の喚起が困難である」が 40.4%となっており、中小企業の顧客側のコスト制約やセキュリティ意識に起因して、セキュリティ対策を実施することが困難な状況であることが伺える。一方、「社内にセキュリティやその商材の専門知識や技術力のある人材が不足している」が 35.4%で、地域 IT ベンダーの人的リソース不足も課題となっている。



図表 34　提供サービス・システムのセキュリティ確保の取組の実施上の課題（MA）

（3）地域 IT ベンダー社内で実施しているセキュリティ対策（問 31）

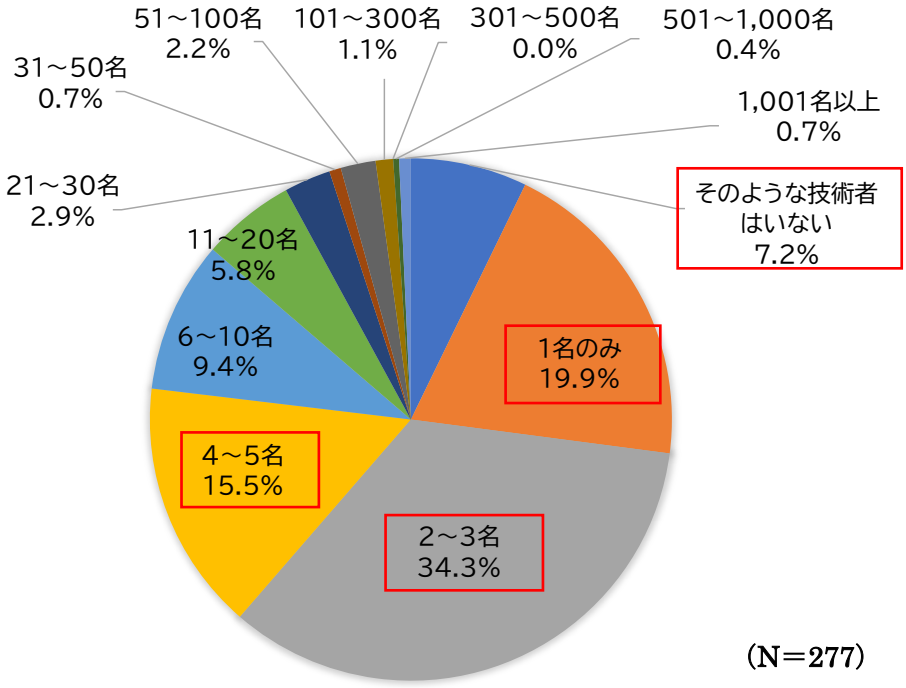
地域 IT ベンダー社内で実施しているセキュリティ対策としては、「従業員向けのアカウント管理ルールやパスワード設定ルールの策定」が 77.3%と最も多く、次いで、「重要なシステム・データのバックアップ」が 74.7%、「管理者権限アカウントの管理ルールの策定」が 71.8%となっている。



図表 35　地域 IT ベンダー社内で実施しているセキュリティ対策（MA）

（4）地域 IT ベンダー社内のセキュリティ技術者の人数（問 32）

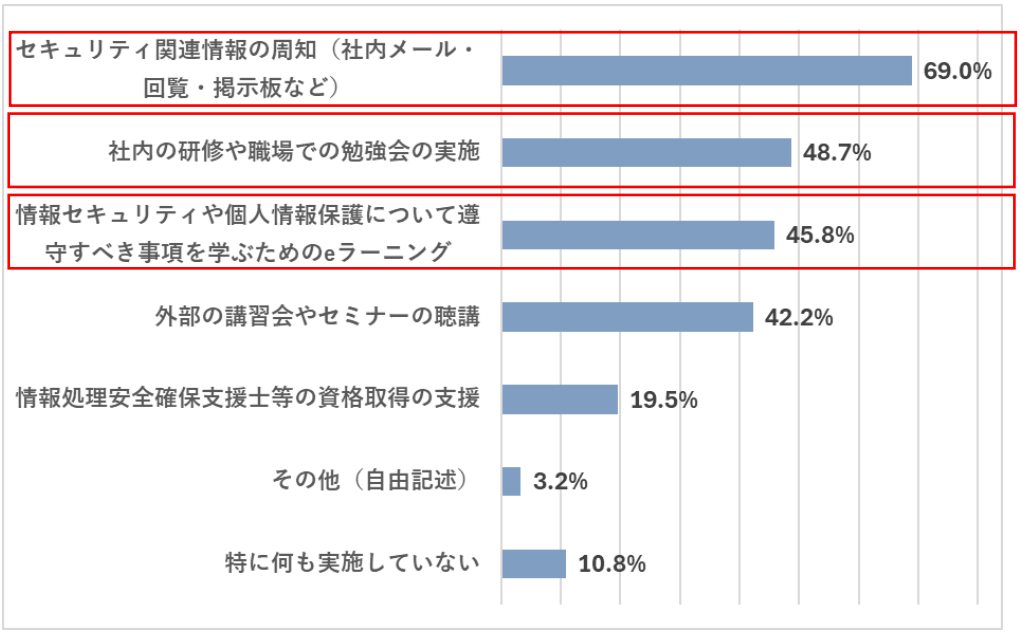
地域 IT ベンダー社内のセキュリティ技術者の人数は、1 名のみ（19.9%）、2～3 名（34.3%）、4～5 名（15.5%）であり、セキュリティ技術者を置いていない（7.2%）を含めて、約 8 割に地域 IT ベンダーが社内のセキュリティ技術者が 5 名以下となっている。



図表 36　地域 IT ベンダー社内のセキュリティ技術者の人数（SA）

（５）地域 IT ベンダー社内で実施しているセキュリティ教育の内容（問 33）

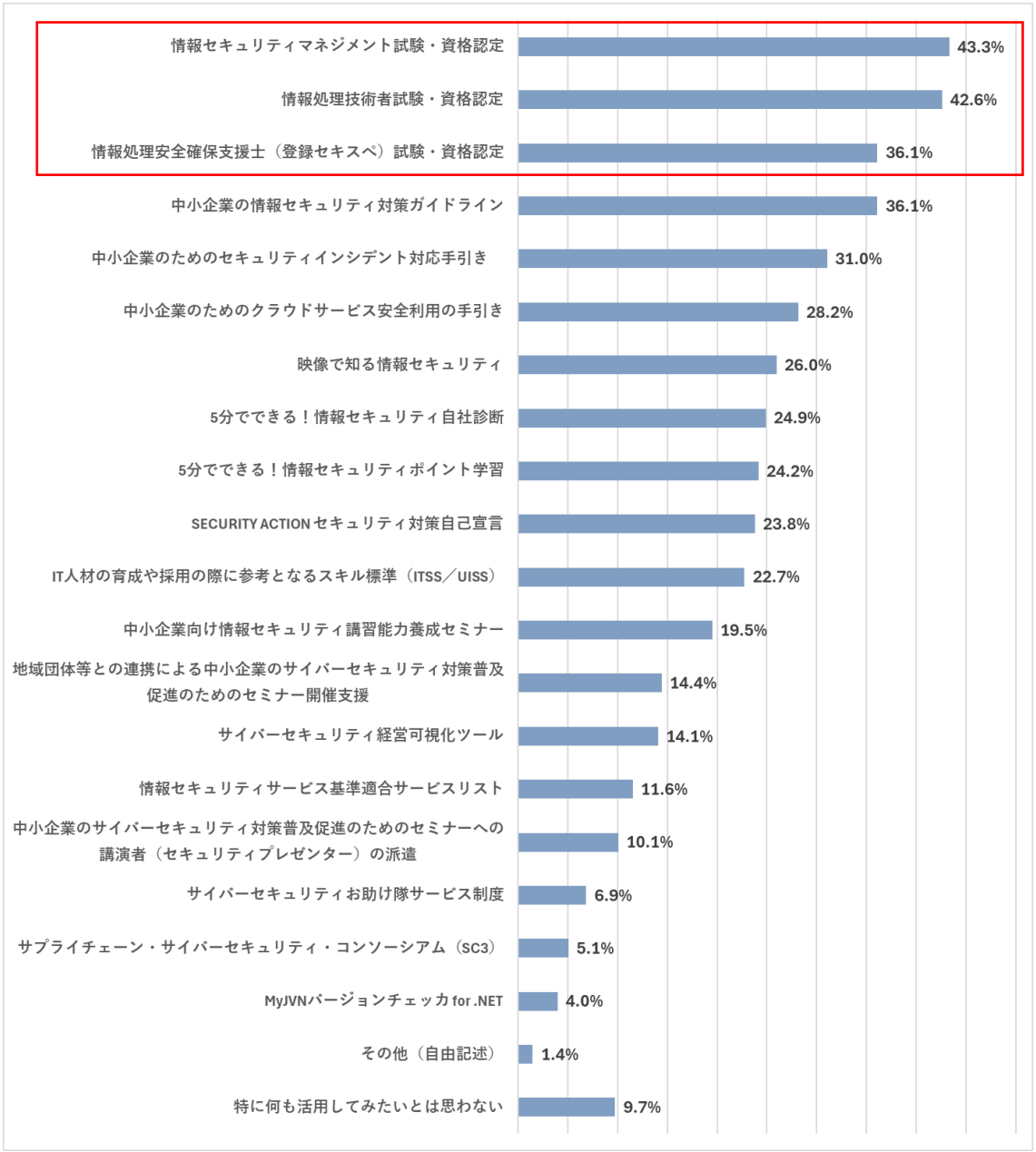
地域 IT ベンダー社内で実施しているセキュリティ教育の内容としては、「セキュリティ関連情報の周知」が 69.0%と最も多く、次いで「社内の研修や職場での勉強会の実施」が 48.7%、「情報セキュリティや個人情報保護について遵守すべき事項を学ぶための e ラーニング」が 45.8%となっている。



図表 37　地域 IT ベンダー社内で実施しているセキュリティ教育の内容（MA）

（6）IPA のセキュリティ施策活用のニーズ（問 34）

地域 IT ベンダーが自社のセキュリティ対応能力の強化のために今後活用してみたい IPA 施策は、「情報セキュリティマネジメント試験・資格認定」が 43.3%と最も多く、次いで「情報処理技術者試験・資格認定」が 42.6%、「情報処理安全確保支援士試験・資格認定」、「中小企業の情報セキュリティ対策ガイドライン」が 36.1%となっており、人材育成を中心とした IPA の施策への期待が高い。



図表 38　IPA のセキュリティ施策活用のニーズ（MA）

（7）地域 IT ベンダー社内において必要なセキュリティ対応ポイント（問 35）

地域 IT ベンダーが今後、中小企業の顧客の良き相談相手として、顧客のセキュリティ対応の行動変容を促していくために、社内のリソースや体制において何を充実強化していく必要があるか、自由回答を求めた。主な回答としては、顧客である中小企業がセキュリティ対策に積極的に取り組むよう働きかけるために、自社内の体制強化のため、「人材育成」等の必要性を感じている地域 IT ベンダーが多く、地域 IT ベンダー自身の能力向上が鍵となっていることが伺える。

＜自由回答（抜粋）＞

社内のリソースや体制において必要なセキュリティ対応ポイント

① 人材育成・社内体制

【主な回答】

- 社内にセキュリティの専門・有識者で構成する部門を立ち上げると共に、社員全員へ知識向上を根差した継続的な教育の実施
- 顧客のセキュリティ意識を高める上で、一部の担当者をセキュリティの専門家にするのではなく、フロントに立つ営業マンも一定のセキュリティスキルを持ち、ある程度は相談にのれることが必要
- ISMS をベースとしたセキュリティ教育の実施
- 質・量共にセキュリティ人材の強化、利益が確保できるビジネスモデルの確立

② 中小企業への意識改革

【主な回答】

- 中小企業の経営者に対し、セキュリティ対策の必要性とコスト負担を社会的に浸透させていく必要がある
- 顧客の行動変容と意識改革を根気強く訴える
- タイムリーなセキュリティ関連情報の提供、例えば直近でのセキュリティ関連事故状況など

③ 外部連携・パートナーシップ

【主な回答】

- 社内リソースのみでは対応が難しい場合が多く、専門知識を有するパートナーの開拓が必要
- 製品を導入して終わりのケースが多く、適切な運用が行われているかどうかを定期的にチェックし、運用自体をアウトソースするような提案ができる体制

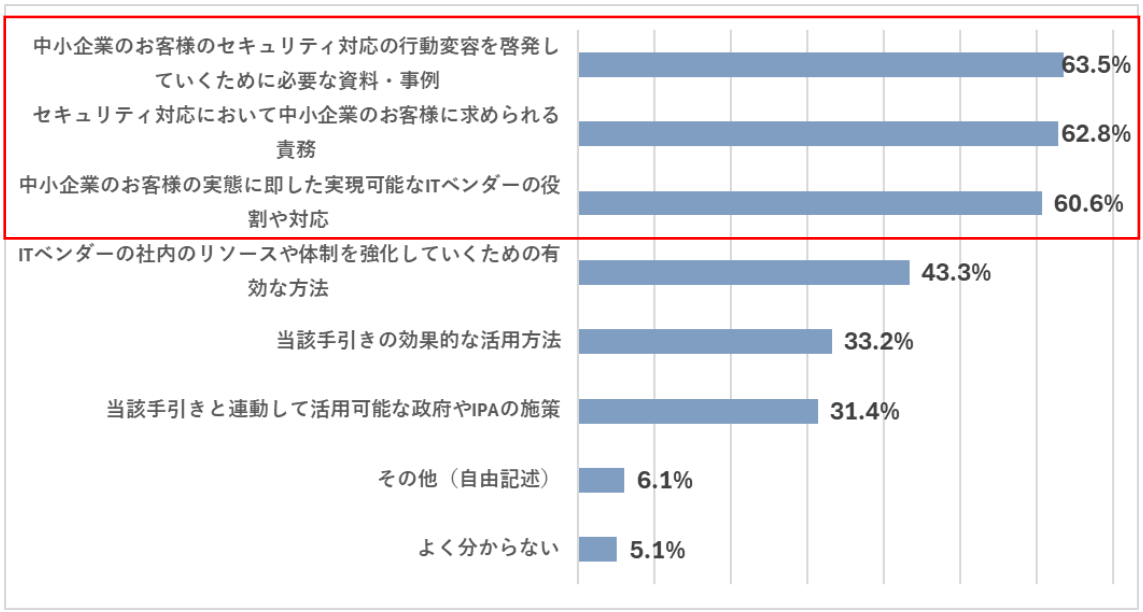
④ その他

【主な回答】

- 自己防衛ができるセキュリティソフトの導入
- 中小企業の顧客は予算の制約が大きく、高額なセキュリティ製品の導入領域での体制の強化はビジネス的に難しい。意識が高い顧客へはオールインワンで概ねカバーする汎用的なツールを勧める開拓が必要
- プライバシーマークの取得、ISMS の認証取得

（８）地域 IT ベンダー手引きに必要な情報（問 36）

IPA では、本アンケートの結果を踏まえ、地域の IT ベンダーが採るべき役割や対応をまとめた「地域 IT ベンダー向け手引き」を作成する予定であることを伝え、その上で当該手引きをより有効なものとするには、手引きの中にどのような情報を盛り込むべきだと思うか、回答を求めた。回答結果は、「中小企業のお客様のセキュリティ対応の行動変容を啓発していくために必要な資料・事例」が 63.5%と最も多く、次いで「セキュリティ対応において中小企業のお客様に求められる責務」が 62.8%、「中小企業のお客様の実態に即した実現可能な地域 IT ベンダーの役割や対応」が 60.6%となっている。



図表 29　地域 IT ベンダー手引きに必要な情報（MA）

2.2.4. クロス集計結果

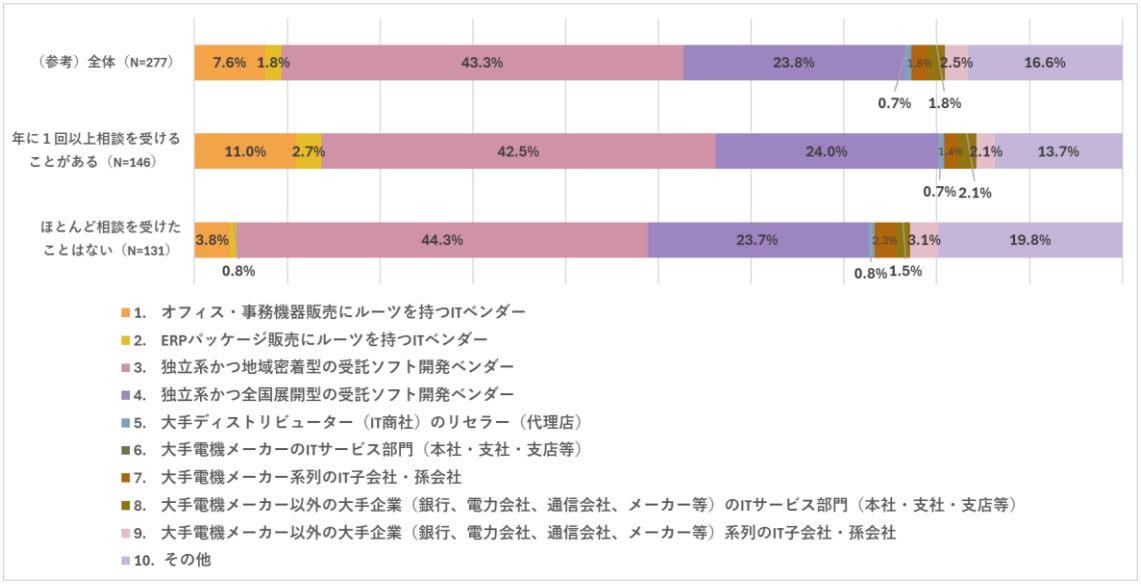
アンケートの回答データをもとに、以下の観点で検証仮説を立て、設問間のクロス集計を行った。

No	検証仮説	設問番号
1	中小企業から相談を受けている/受けていない企業の属性に差分があるか	問 13（顧客からのセキュリティに関する相談頻度）と以下のクロス集計 ・問 2（組織の成り立ち） ・問 1（主な事業）
2	地域 IT ベンダーの成り立ち（地域密着型/全国展開型）によって、中小企業への対応に差分があるか	問 2（組織の成り立ち）と以下のクロス集計 ・各種中小企業への対応設問 （問 18、20、22。24、26）
3	地域 IT ベンダーの成り立ちによって、セキュリティ技術者の数に差分があるか	問 32（自社のセキュリティ技術者の数）と以下のクロス集計 ・問 2（組織の成り立ち）

図表 40　アンケート調査のクロス集計の観点（再掲）

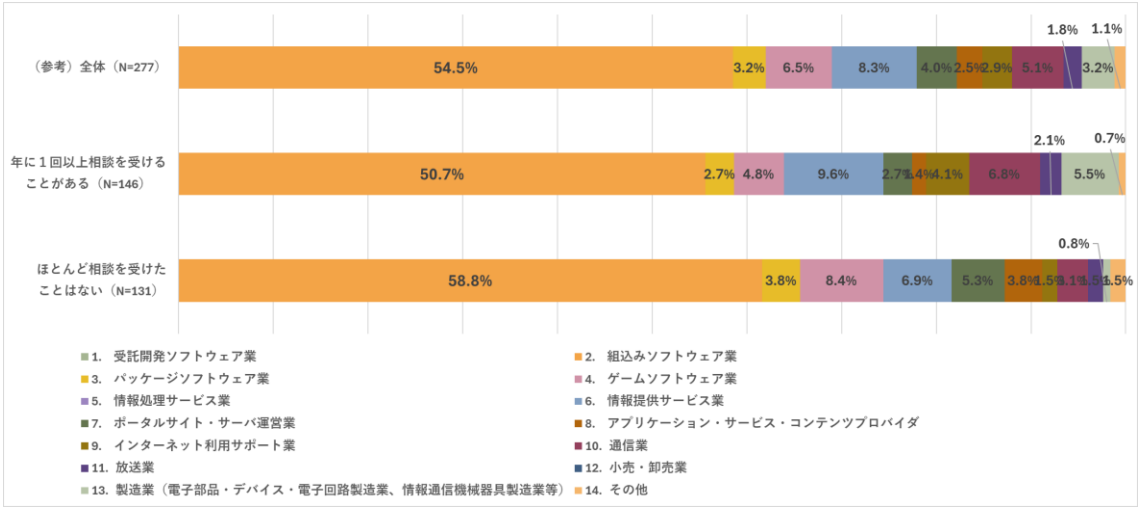
（1）検証仮説①：中小企業から相談を受けている/受けていない企業の属性に差分があるか

- 【設問文】
  - 問 13. 顧客からのセキュリティに関する相談頻度
  - 問 2. 組織の成り立ち
- 【検証結果】
  - セキュリティに関する相談頻度は、地域 IT ベンダーの成り立ちで大きな差分はない
  - 年に 1 回以上相談を受けるベンダーは、独立系・地域密着型の半数強、全国展開型の 8 割弱



図表 41　顧客からのセキュリティに関する相談頻度

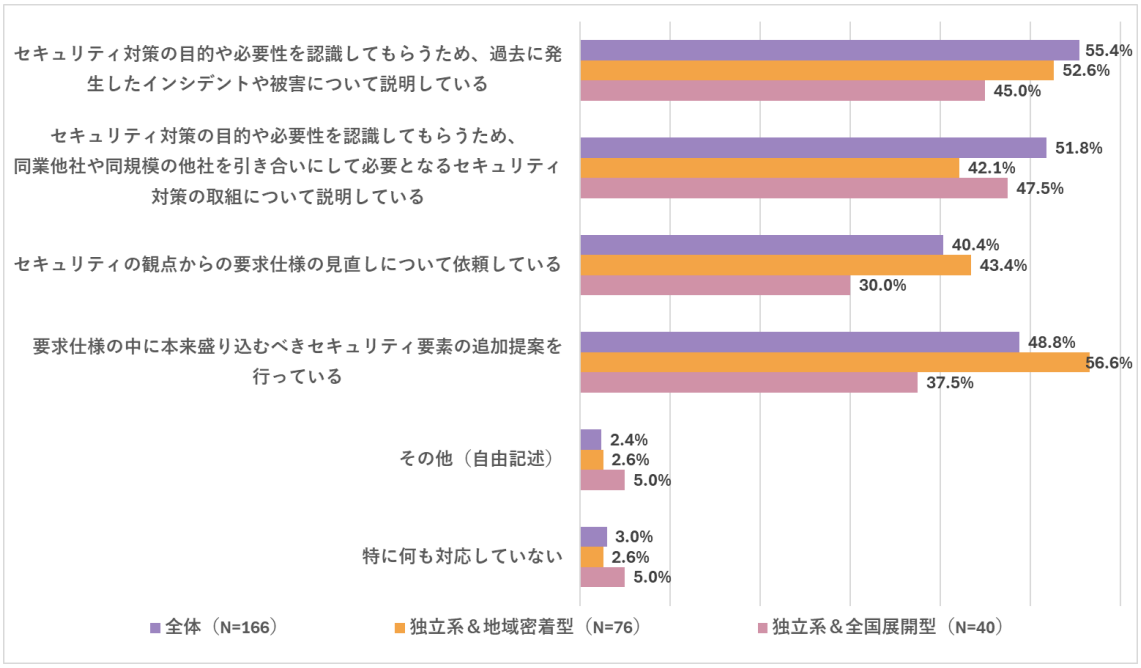
- 【設問文】
  - 問 13. 顧客からのセキュリティに関する相談頻度
  - 問 1. 主な事業
- 【検証結果】
  - セキュリティの相談頻度は、事業別で大きな差分はない



図表 42　顧客からのセキュリティに関する相談頻度

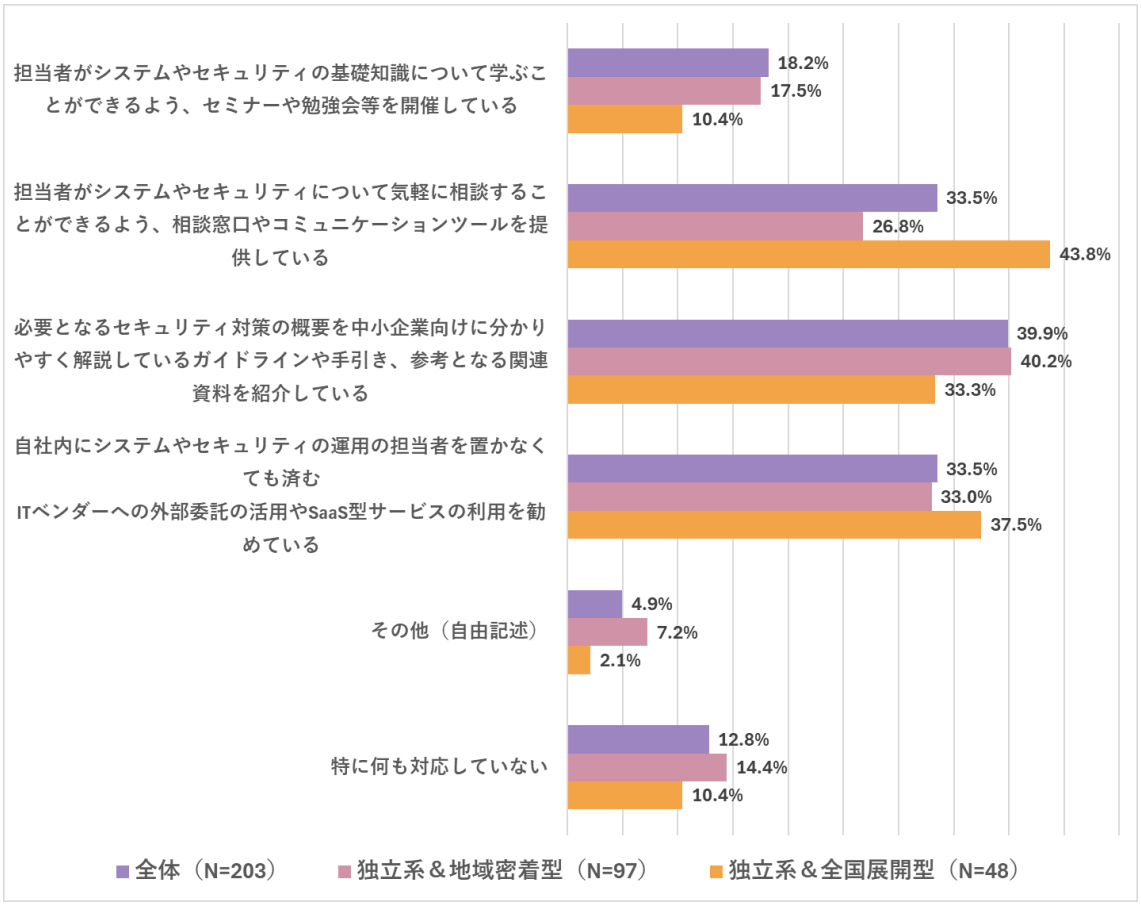
（2）検証仮説②：地域 IT ベンダーの成り立ち（地域密着型/全国展開型）によって、中小企業への対応に差分があるか

- 【設問文】
  - 問 2. 組織の成り立ち
  - 問 18. セキュリティ要素が不十分な要求仕様を提示された際の対応
- 【検証結果】
  - セキュリティ要素が不十分な提案依頼書の提示を受けた際、追加提案や要求仕様の見直しを依頼する割合は、地域密着型ベンダーの方が高い



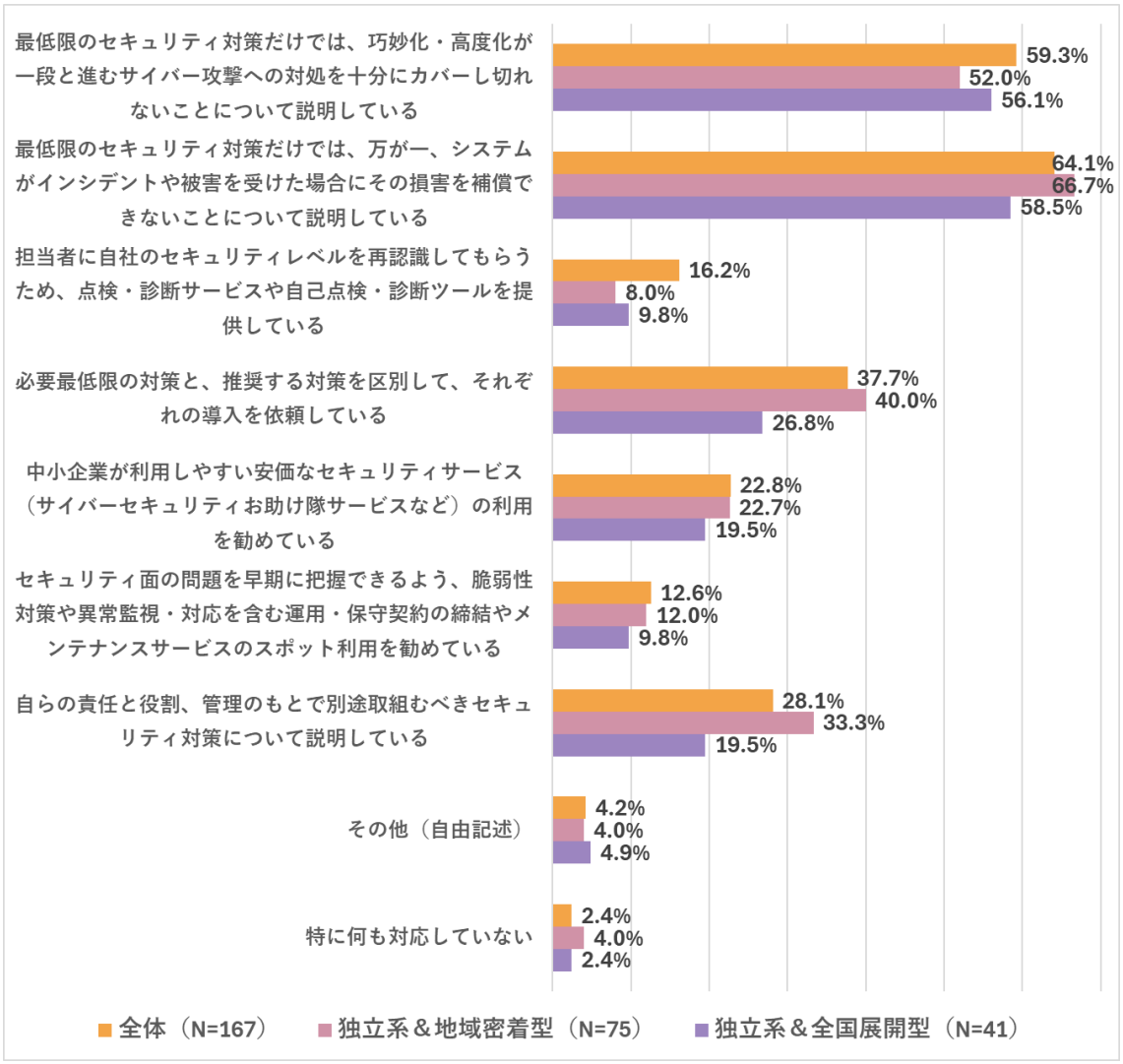
図表 43　セキュリティ要素が不十分な要求仕様を提示された際の対応

- 【設問文】
  - 問 2. 組織の成り立ち
  - 問 20. 顧客にシステム・セキュリティ技術者がいない際の対応
- 【検証結果】
  - 中小企業の顧客にセキュリティ担当者がいない場合、全国展開型の方が相談窓口/コミュニケーションツールの提供割合が高い。特に何も対応していない割合は、地域密着型の方が高い



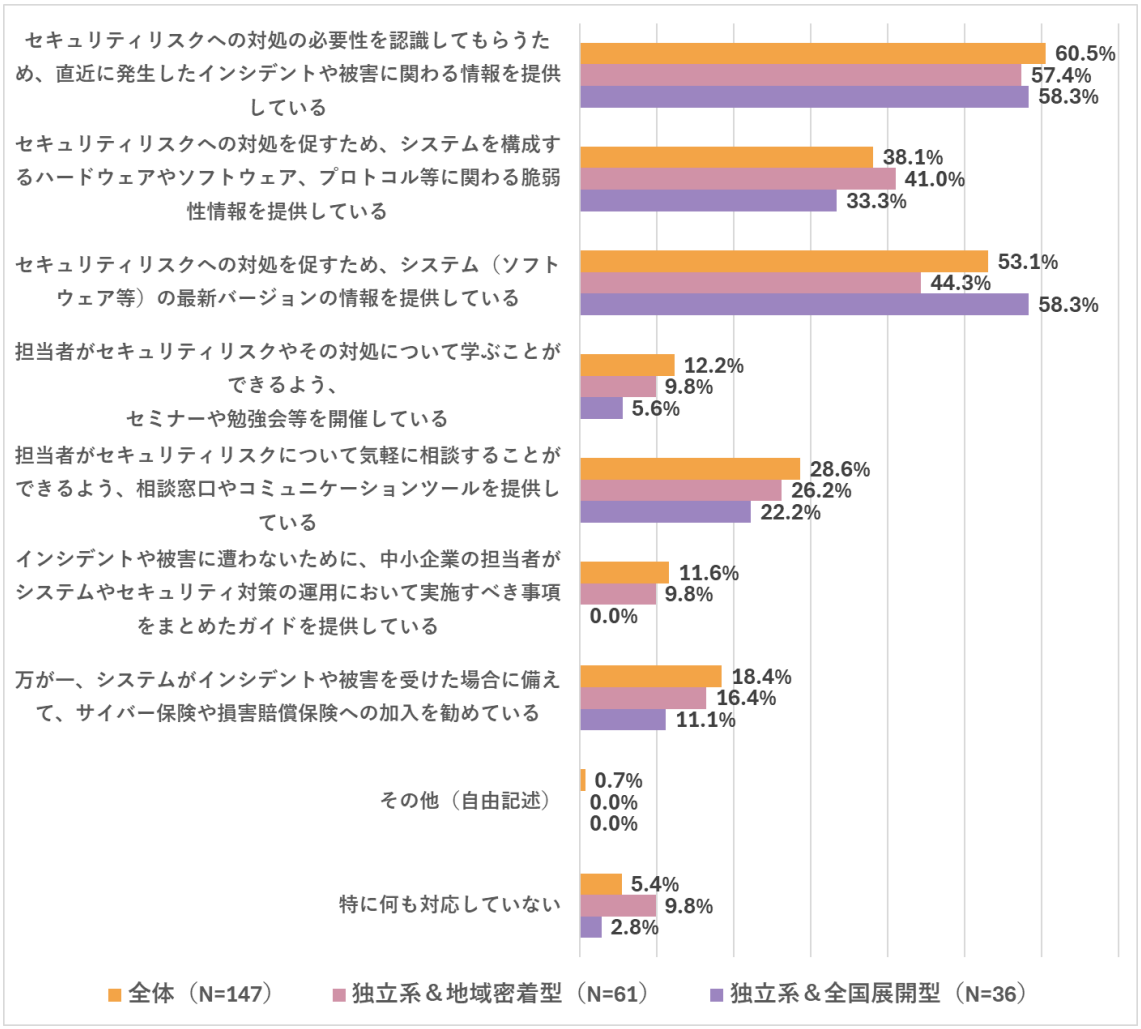
図表 44 顧客にシステム・セキュリティ技術者がいない際の対応

- 【設問文】
  - 問 2. 組織の成り立ち
  - 問 22. セキュリティ対策を最低限の実装に抑えるよう指示を受けた際の対応
- 【検証結果】
  - セキュリティ対策を最低限の実装に抑えるよう指示を受けた際、地域密着型の方が、最低限の対策と推奨対策を区別して導入を依頼している割合が高い



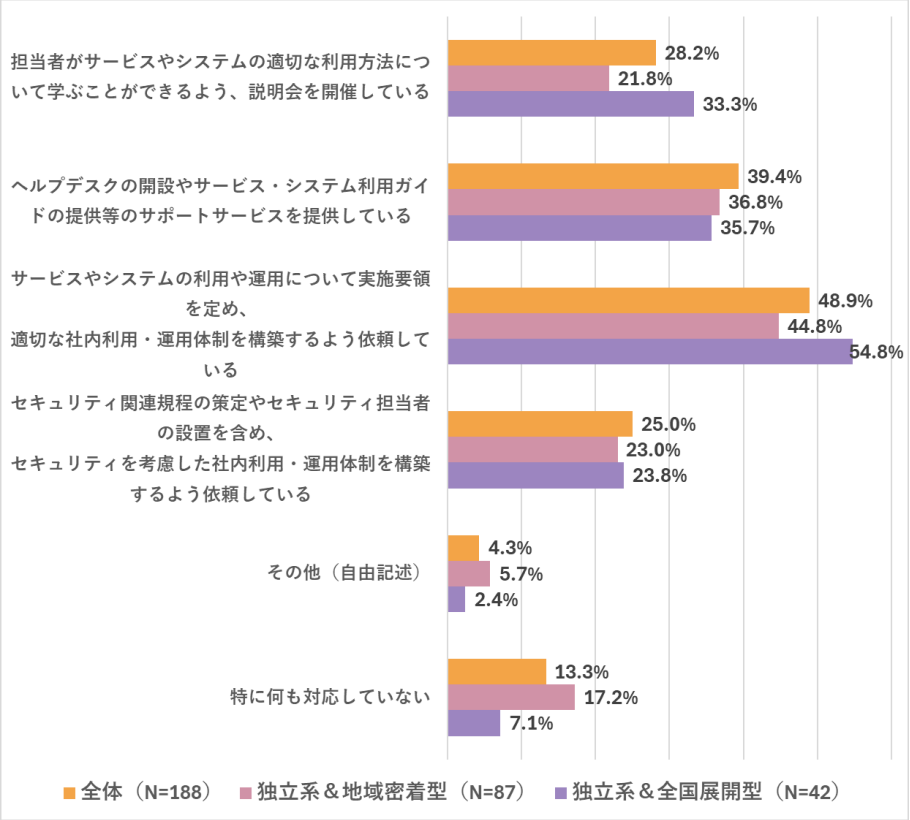
図表 45　アンケート調査 問 2 × 問 22 集計結果

- 【設問文】
  - 問 2. 組織の成り立ち
  - 問 24. 顧客にセキュリティ対策の運用に係る応分の負担を求める際の対応
- 【検証結果】
  - セキュリティ対策の運用に係る応分の負担を顧客に求めた際、地域密着型はその後何も対応していない割合が高い



図表 46　顧客にセキュリティ対策の運用に係る応分の負担を求める際の対応

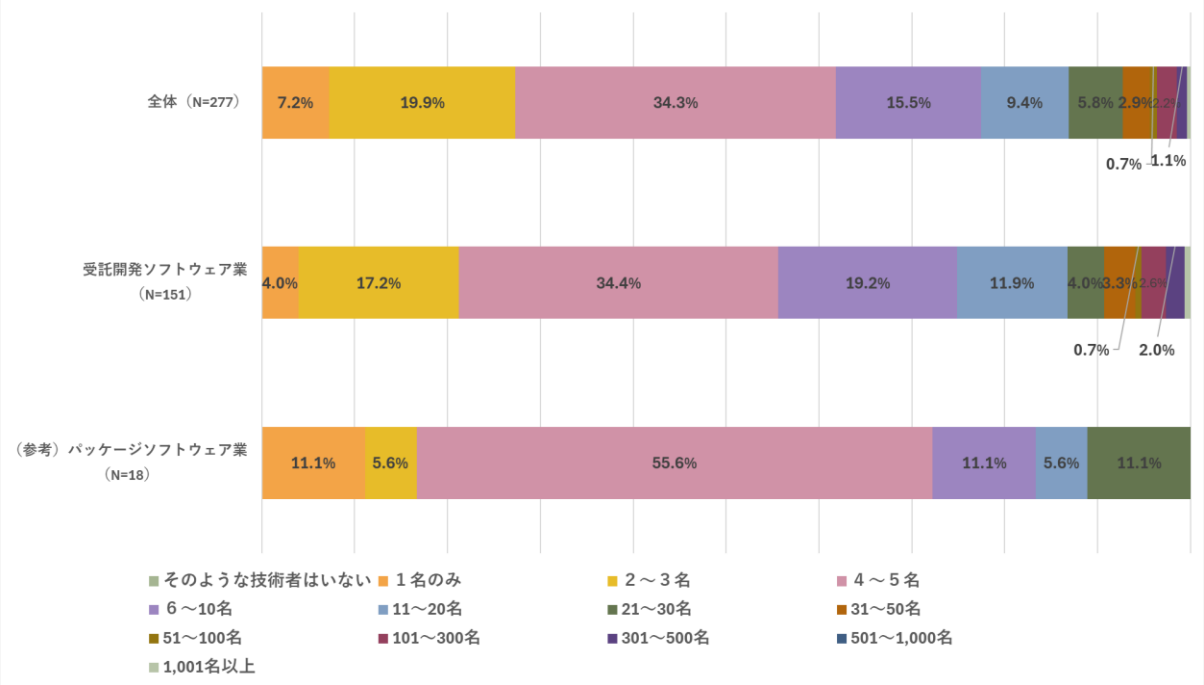
- 【設問文】
  - 問 2. 組織の成り立ち
  - 問 26. 顧客社内での導入体制が不十分な際の対応
- 【検証結果】
  - 運用開始時、顧客社内での導入体制が不十分な状況に直面した際、地域密着型は、特に何も対応していない割合が高い



図表 47 顧客社内での導入体制が不十分な際の対応

（3）検証仮説③：地域 IT ベンダーの成り立ちによって、セキュリティ技術者の数に差分があるか

- 【設問文】
  - 問 2. 組織の成り立ち
  - 問 32. 自社のセキュリティ技術者の数
- 【検証結果】
  - セキュリティ技術者がいない割合は、受託ソフトウェア業は全体の傾向とそれほど差はない



図表 48　自社のセキュリティ技術者の数

2.3. ヒアリング調査結果

ヒアリング調査について、以下の項目別に整理を行った。

① 自社の人的リソース確保状況と課題 ② システム提供時における自社のセキュリティ対策 ③ 中小企業へのシステム提供時における顧客側の課題 ④ 中小企業の課題への地域 IT ベンダーの対応状況 ⑤ システムの設計時・構築時におけるセキュリティ確保の取組と対応上工夫しているポイント ⑥ システムの運用時・保守時におけるセキュリティ確保の取組と対応上工夫しているポイント ⑦ IPA 施策の活用ニーズ ⑧ 地域 IT ベンダー向け手引きの活用ニーズ

なお、以下の【主なヒアリング結果】では、JISA 団体会員のうち、北海道、愛知県、福岡県、熊本県、沖縄県の情産協 5 団体に加盟する地域 IT ベンダー企業計 15 社（各道県 3 社）を A～O 社、IPA お助け隊サービスの再販協力会社（4 社）を P～S 社として記載している。

（1）自社の人的リソース確保状況と課題

自社の提供サービスを顧客に選んでもらうためにセキュリティ対応を必須する考えや、ISO27001 の適合対応を目的に、セキュリティに関する自社の人的リソース確保に取り組んでいる地域ベンダーが存在する。

その一方で、情報セキュリティの設計は協業先の大手 IT ベンダーが対応していて、セキュリティ人材の確保を積極的に行っていない地域ベンダーも存在する。

【主なヒアリング結果】

- セキュリティ技術者の育成に注力している。セキュリティのないデータセンターサービスやクラウドサービスはうちでは売れないというのが社長の口癖である。海外サービスではなく当社のサービスを契約してもらうためには、セキュリティが必須であると考えている。(A 社)
- ISO27001 を取得しているので、社内にセキュリティ委員を設けている。また、システム部門をはじめ､各部門にセキュリティに詳しいメンバーを配置している｡｢セキュリティとは何か」といった基礎的な教育は社内の中でできていると思う。(G 社)
- 資格取得が推奨されているものの、セキュリティの資格は優先度としては低い。セキュリティ設計の業務は、協業先である大手 IT ベンダーなどが対応しており、そこが主管になったうえで､当社は指示に基づいて､必要な開発を行っていくという対応をとっているためである。(F 社)

自社の人的リソース確保にあたり、以下のような課題が挙げられた。

- ✓ セキュリティ資格を取得すると給与のより高いベンダーに転職してしまう。給与面の課題が大きい。
- ✓ セキュリティ人材を増やす計画はあるが、開発作業に追われて人材育成に苦戦している。
- ✓ セキュリティ人材の育成にコストをかけても、ビジネスに繋がりにくい。

【主なヒアリング結果】

- セキュリティ資格取得者には資格報酬が出るが、資格を取得すると給与のより高いベンダーに転職してしまう状況。給与面の課題が大きいと思う。(C 社)
- 組織的に、高いレベルのセキュリティ知識を持つ人材を増やしていこうという計画はあるが、開発作業に追われ、人材育成に苦戦している状況である。(E 社)
- 人材不足により、セキュリティ意識を高めるための取組はできていない。コストをかけても、中々ビジネスに繋がるわけではない。(E 社)

自社の人的リソース確保に関する課題に対応するため、以下のような工夫が挙げられた。

- ✓ 顧客への無料セキュリティ診断を提供して、セキュリティ技術者を増やし、ノウハウを蓄積する。
- ✓ 人的リソースの提供と技術者教育をバーターとして、協力会社への人材派遣を行う。
- ✓ セキュリティ資格取得のインセンティブ制度をつくり、資格取得を個人目標に設定する。

【主なヒアリング結果】

- 診断サービスを独自で立ち上げ、最初は無料で提供して数をこなした。無料だと気持ち悪いという企業には 1 万円だけ請求した。診断サービスを通じて、技術者の数を増やし、ノウハウを蓄積していった。(A 社)
- 別地域にある協力会社に技術者を送り込み、OJT を通じて教育をしてもらっている。協力会社からすると、人材不足の中、案件に携わる人を増やせるという点がメリット、当社としては社員を教育してもらえるという点がメリットになる。(M 社)
- 資格取得制度では、自助努力で資格取得等を目指す人への報酬もあり、資格取得時には 20 万円までの一時金の支給と、月額の給与での資格手当が出る。(B 社)
- 高度セキュリティ人材に関しては、個人目標の中で、高度セキュリティ資格の取得という目標を個別に設定している。(I 社)
- プライバシーマークの講習は全員受けるようにしている。(B 社)

（2）システム提供時における自社のセキュリティ対策

地域 IT ベンダーは、顧客の予算制約を考慮しつつ、以下のような方法を活用して、最低限必要なセキュリティ対策を実現する工夫を行っている。

- ✓ リスクに応じた適切な対策の実施
- ✓ 一定水準のセキュリティが担保されたパッケージ、サービスの提案
- ✓ システム運用や顧客教育による対策の補完
- ✓ 外部リソースの活用

【主なヒアリング結果】

- 納品するシステムの環境に応じて、想定リスクを洗い出し、必要な対策をとっていく。例えば、ウェブホスティング系の業務であれば、リスクに対応したサーバーの設定をするなど。（F 社）
- セキュリティにお金をかけられないが、セキュリティも考えてくれないと困るという顧客が多いのではないか。そうなると、コストもかけられないのにどうすればいいのか、と迷っている IT ベンダーもたくさんいると思う。そうしたときに重要なのは、極力世界に一つしかない仕組みはつくらないこと、セキュリティ機能が確立しているサービス（パッケージ）の導入に顧客を誘導することである。（F 社）
- 汎用的なセキュリティツールには、中小企業向けの安価なライセンスがあり、そういった安価なライセンスの利用を提案することはある。大企業向けのものよりコストも下がるし、クラウドサービスを使うので、社内に技術要員がいなくても、対応できるというメリットがある。（I 社）
- 開発面でいうと、顧客にも予算の都合があるので、セキュリティの対策を紹介・提案しても、予算に応じた対応にならざるを得ないのが現状。その中で、最低限どこまでセキュリティ対策をするのかという進め方になる。システム面で対応できないところは、運用面や教育面にも頼るなどの施策を講じる必要がある。（I 社）
- エンドポイント系のセキュリティ提案であれば、当社を代理店として、メーカーと代理店契約を行い、セキュリティサービスを顧客に使ってもらうようにしている。また、数は多くないが、脆弱性診断は当社でできない部分もあるので、セキュリティベンダーに外部委託をして、診断をしてもらう形をとっている。（E 社）
- 保守が必要にもかかわらず、どうしても保守は付けたくないという顧客の依頼はお断りしている。経験上こういった顧客は、納品後も度々無償のサービスを要求してくることが多い。そもそも保守が必須のシステムに対して保守が不要というのであれば、会社としてシステムを導入するべきではないと考えている。（R 社）

その一方で、自社の事業範囲をパッケージの機能追加等に限定し、システムインフラやセキュリティ全般対策を大手 IT ベンダーやパッケージベンダーに任せる地域ベンダーも存在する。このようなベンダーは、顧客からの要望が少ないことやコスト制約、人的リソース不足等を理由に、セキュリティ対策のビジネスの優先度を低く設定していると考えられる。

【主なヒアリング結果】

- セキュリティだけでなくシステムインフラ全般のコントロールを大手 IT ベンダーに任せている。あくまで、当社が担うのは、システムの機能追加やカスタマイズに関わる開発・プログラミングの部分だけである。(F 社)
- パッケージベンダーのセキュリティ対策で、カバーされていないところはほとんどない。パッケージを出す際には、一般的な脆弱性のテストなどは十分に実施している。したがって、当社が追加でセキュリティ対策を行うことはあまりなく、パッケージ導入をする際に、ファイアウォールやネットワーク周りのセキュリティなどの話をするぐらいである。(J 社)
- セキュリティ対策のニーズに対応しようという問題意識はあるものの、中小企業に対する提案となると、どうしてもコストが限られるため、セキュリティ部分を外した提案になりがちである。セキュリティに対して提案を求められれば提案するが、そういった要望をする顧客がそもそもいない。新しいセキュリティ製品・サービスや、既存の製品・サービスに追加された新しいセキュリティ機能に関する勉強会を実施しているが、そのような製品・サービスを扱う実践の場があまりなく、積極的に市場に対してアプローチもできていない。よって、ビジネスの優先度としては低いのが現状である。(G 社)

（3）中小企業へのシステム提供時における顧客側の課題

中小企業へのシステム提供時における顧客側の課題として、以下の内容が挙げられた。

- ✓ 顧客の経営層のセキュリティ対策に対する理解不足から、なかなか導入が進まない。
- ✓ AI や IoT など先端技術のシステムや機器の導入が注目されるが、運用体制が未整備だと、かえってセキュリティリスクが広がってしまう。
- ✓ 地域 IT ベンダーへの過度な依存で、セキュリティ対策も当然やってくれていると思い込んでいる。

【主なヒアリング結果】

- セキュリティ対策は費用対効果が見えづらいことから、顧客の決裁権をもった役員の説得が難しい。セキュリティ対策が、事業継続に必要なものであるという理解が乏しく、費用対効果が見えないという言い方をされる。(O 社)
- 顧客の経営層は、自分のところは大丈夫だと思っている。担当者レベルでは危ないと思っていても、経営層までそれが浸透しない。当社営業から、セキュリティリスクやサイバー攻撃の情報を提示しても、「ふーん」といわれてしまう。そこに思い切ってお金をかけてもらうのは難しい。(C 社)
- 納品時などに IT の脆弱性など説明しても、なかなか顧客側に聞き入れてはもらえない。地方の企業の多くが、「本社からの対応指示がない」からと消極的である。(P 社)
- AI や IoT、SaaS、DX などの流行り物を打ち上げ花火的に普及させることに熱心で、かえってセキュリティリスクのすそ野が広がっているのではないか。例えば IoT は、高性能なデバイスとして登場したが、それが野良デバイスとして放置されるようになると、設置したことすら忘れられて、アップデートやメンテンナンスがなされない。地方に中途半端に中央の流行り物のシステムや機器が入ってしまうと、最終的に

それが放置されてリスクだけが残ってしまう。(D 社)

- 顧客は、普段から御用聞きとしてお抱えの地域 IT ベンダーに、暗黙の了解でいろいろお願いしているため、セキュリティ対策も当然やってくれていると思い込んでいるところがある。(A 社)
- 顧客の経営層はセキュリティに対する優先度が低いため、なかなか承認をもらえず、セキュリティ対策の導入に至らないケースがある。経営層向けにセキュリティ対策の重要性をレクチャーするが、それでも導入が進まないということが多々ある。(O 社)

また、中小企業では、セキュリティに割ける予算の不足や専門人材の不足により、以下のような状況が発生していることが明らかになった。

✓ システム発注内容（要求仕様）から、セキュリティ要素が対象外になっている。
✓ 顧客のセキュリティに関する理解レベルが低い。
✓ システム構築後の保守の依頼がされない。

【主なヒアリング結果】

- 中小企業はお金が十分に払えないため、前提として、セキュリティ要件は発注内容から対象外になっているというのが実状である。(F 社)
- 顧客からは、セキュリティの専門用語がわからず、内容が理解できないので説明してほしいとよく言われ、セキュリティに関する顧客の理解レベルは低い。顧客に技術者がいない場合、中小企業であれば会社全体について当社が面倒を見る形で対応している。問い合わせ対応やサポートなど、一括で対応する IT サポート契約を締結している。(K 社)
- 業務上、保守はほとんど行っていない。ネットワークシステムを構築した場合などは保守が必須となるが、(導入時に) セキュリティ対応を行ったとしても、そこから保守を依頼されるところまでは至らない。(Q 社)

（4）中小企業の課題への地域 IT ベンダーの対応状況

中小企業の顧客の課題への地域 IT ベンダーの対応状況として、以下のような内容が挙げられた。

✓ セキュリティに割ける予算の不足への対応

顧客のコスト負担を軽減するため、柔軟な提案が求められる。具体的には、低コストで必要最低限の対策を提供する仕組みや、段階的あるいは一時的な料金設計の提案、補助金制度の活用などが挙げられる。また、長期的な視点での費用対効果を訴求することで、導入のハードルを下げる取り組みも行われている。

【主なヒアリング結果】

- 中小企業からは、月額の固定料金では払えないと言われることが多い。年単位の従量料金で請求するにしても、何のセキュリティ対策を行うかによって月ごとに費用が

変動する場合もある。中小企業は、1年分や5年分など、年単位でまとめる形であれば、セキュリティ対策の運用費用についても支払い可能な場合があるので、当社で月ごとの費用変動も見越して、まとめて請求することにしている。(K社)

- コストの壁があるのであれば、例えば 3 年間で段階的にやっていくのはどうか？とロードマップのような形で提案する。そうするとコストを許容してもらえ、運用を通じてリスクを認識してもらえるので、契約になることがある。(A社)
- インシデント対応は、事業を圧迫するくらい工数がかかることもあるため、そういう場合は、工数に応じた費用請求をするが、そうでない場合は、スポット対応として費用を低く抑えることが多い。(C社)
- 顧客のほとんどが中小企業、なかでも小規模な企業が多いのでコスト面の課題はかなり大きいため、低コストで必要最低限の機能を備えている IPA のお助け隊サービスを提供している。(A社)
- セキュリティベンダーの無償の診断ツールを使って、顧客に対してセキュリティ診断を実施している。具体的には、セキュリティ診断の結果を提示して、「こういった対策が必要である」と提案するアプローチを採っている。(G社)
- システムの導入コストが高くても、運用保守契約がそこまで高くなければ、長い目でみるとリーズナブルであるといったメリットを訴求している。(H社)
- 県独自の補助金予算や補助事業をうまく活用して、セキュリティ関連も含めた提案をしている。補助金は、IT導入に関わるコンサルにもITツールの導入にも適用できる。(O社)

✓ 専門人材の不足やセキュリティ意識の低さへの対応

セキュリティ教育を通じた意識向上が重要である。具体的には、実際のインシデント事例の共有や、セミナー・教育コンテンツを活用した危機意識の醸成などが挙げられる。また、顧客と伴走しながら進める仕組みを取り入れることで、より実効性のある教育の実現が期待される。

【主なヒアリング結果】

- 昨今、いろいろな側面で「内製化」が注目を浴びているが、セキュリティの担保を顧客に丸投げするのではなく、伴走型ビジネスとすることで、顧客で対応できるところは顧客側が担当し、プロでないと対応できないところはITベンダー側が担当する、という形がうまく適用できれば、良いのではないか。中小企業のなかでも、ある程度大きな企業であれば実現可能と考えている。(F社)
- 危機意識を持ってもらうためのセキュリティ教育が重要である。セミナーを開催して、顧客の危機意識を高めていくことができたら良いと思う。中小企業には外国籍の従業員もいるので、外国籍の従業員向けのセキュリティ教育も提案していくと面白い。外国籍の従業員の場合、人の入れ替わりも激しく、顧客が自社で教育するのは大変だと思うので、身近なコンテンツを活用したセキュリティ教育の提案があると良いのではと思う。(H社)
- 「○○病院がランサムウェアに感染して業務が止まった」など、類似事業で発生した

インシデント事例の共有を実施している。(M 社)

- 営業をしていると、そもそも情報セキュリティとは何か、と顧客に言われることがある。基礎知識が無いのでセキュリティ商材の説明をしても、何故それが必要になるのかが理解されない。そのため、まずは基礎知識から説明した方が良いと思う。(S 社)

✓ 運用体制の不備への対応

専門人材が不足している企業に対しては、使いやすい製品の提供や、包括的なサポート体制の構築が有効である。また、リスクの高い状況に対しては、公開情報を活用した指摘や、外部セミナーの紹介を通じて意識啓発を図るなど、柔軟なアプローチが求められる。

【主なヒアリング結果】

- 社内にセキュリティの専門知識や技術力のある人材が不足しており、対応が後回しになっている企業に対しては、広く売れていて使い勝手が良い商品に絞って、社内検証をしたうえで顧客に提供する形をとっている。提案できるメニューを可能な限り揃えておくことが重要。(A 社)
- 従業員 300 名未満の規模の中小企業の場合、会社全体について当社が面倒を見る形で対応している。問い合わせ対応やサポートなど、一括で対応する IT サポート契約を締結しているため、極端な例では、プリンターが接続できなくなっただけで問い合わせが寄せられることもある。(K 社)
- OSINT（オープンソースインテリジェンス）を使っているので、対策をしないとまずいような状態のものは、公開情報のみを用いて、契約行為がなくても確認している。最近、あまりに状況がひどい（リスクが大きい）ものは、良くないと指摘するようにしている。(C 社)
- 顧客にセキュリティ技術者がいない場合は、顧客の意識啓発も大事なので、「ここにコストをかけてください。」という思いもこめて外部のオンラインセミナーを紹介した事例がある。(G 社)

✓ 地域 IT ベンダーへの過度な依存への対応

顧客と IT ベンダー双方の責任範囲を明確化することが求められる。具体的には、契約時点で役割分担を明確にすることで、顧客の主体的な対応を促す仕組みが有効である。

【主なヒアリング結果】

- 特に保守契約を結んでいる顧客でよくみられるが、「セキュリティについて全部地域 IT ベンダーに対応してもらえる。」と思っている顧客は多いと思う。社内ではこういった状況を問題視しており、保守契約において顧客とベンダー双方の責任を明確にするため、保守契約書の標準フォーマットの検討を始めている。(E 社)

✓ 経営層と現場担当者のディスコミュニケーションへの対応

専門用語を避け、リテラシーに応じた分かりやすい説明が求められる。また、経営層への説明に立ち会ったり、リーダー教育を実施したりするなど、顧客の状況に応じた柔軟なサポートを行うことで、意思決定を円滑に進める工夫が有効である。

【主なヒアリング結果】

- 担当者に説明する際、その担当者が経営層に説明しやすいような情報提供を心掛けている。エンジニアや技術者は専門用語を多用することが多いが、そうではなく、ITリテラシーが高くない人でも理解できるような言葉に置き換えて説明するように工夫している。それでも説明しにくい場合は、顧客の対象事業に即した図表に書き換えてお渡しすることもある。担当者から依頼があれば、経営層への説明にも当社が立ち会うスタンスである。(M社)
- 情報セキュリティが十分でない場合、ITリテラシーに近いような話かもしれないが、1～2 日かけて、有料で説明を行うことがある。顧客側でセキュリティ確保を推進していくリーダーを養成する場合には、リーダー教育を実施する場合がある。また、顧客にシステムのマニュアルを渡しているが、それだけでは顧客が対応できないという場合は仕方なく当社が対応して説明を行っている。顧客のレベルに合わせてケースバイケースで対応している。(J社)

また、顧客とセキュリティに関わる要件定義について調整することができない場合や、地域 IT ベンダーが納入したシステムの運用体制が顧客側の社内で整備されていない場合における地域ITベンダーの対応として、以下のような内容が挙げられた。

✓ 契約前に実施する社内審査
✓ セキュリティ要件の優先度付け
✓ リスク説明と責任の明確化
✓ 包括的な料金体系/体制の提示
✓ サイバー保険等補助的なサービスの提供

【主なヒアリング結果】

- 案件規模等を踏まえリスクが高いと判断したものは、提案・注文を受ける直前の2回、必ず社長まで参加する審査会を受けなければいけない。その審査会に合格しないと提案や契約が許可されない。その審査の中に、セキュリティの要求項目がテンプレートとして盛り込まれている。ただし、最低限はここまで、という基準が明確に文書化されて定められているわけではなく、都度相談をする形である。セキュリティ担当者や営業担当者、システム技術担当者に全員に相談するような流れになっている。(A社)
- 提示されたRFPにセキュリティの要件が足りない場合は、追加提案をしている。コストの都合上、セキュリティ対策を削る必要が発生した場合、何を削るかは顧客によって異なるが、顧客の課題を見極めたうえで優先度をつけている。例えばインシデント対応支援は優先度を下げて、まずは日常的にインシデントを起こさないためのツール導入や運用を重視する。あとは、顧客と自社が果たす役割をきちんと定義することで、外部に出す部分(当社に依頼する部分)のコストを抑えるなどの方法も考えうる。

（B 社）

- 当社が顧客に導入するシステム、サーバー、ファームウェア、OS については、要件によるセキュリティ対策を明確にして提案をしている。また、サーバーには必ずウイルス対策ソフトを入れるように、提案はするものの、コストの問題などで実装できない場合には、そのリスクは顧客に許容してもらうことを前提としている。セキュリティリスクをきちんと説明し、当社と顧客の責任範囲を明確にすることで、リスクヘッジをしている。（G 社）
- 保守メニューの提案において、地元だからこそ電話対応だけではなく、駆け付けられるなどのメリットを伝え、エンジニアと営業が一緒に動いて契約の働きかけを行っている。また、セキュリティ以外のサービスも含めて提案・販売している。（J 社）
- 運用保守契約は締結しておらず、パッケージの利用料として、月額数千円の基本料金を設けており、利用するデータ量に応じて従量型の利用料を請求したり、定額型の利用料を請求したりしている。WebEDI 系システムのパッケージ導入においては、ソフトウェアの更新や脆弱性診断も、その利用料の中に含めている。（N 社）
- コスト等の理由から、セキュリティの対策を施せなかったことで何らかのリスクが発生する場合、品揃えの一つとしてサイバー保険を取り扱っている。（G 社）

しかしながら、顧客側のコスト制約や人材不足等の課題が原因でセキュリティ対応が必要な状況においては、地域 IT ベンダーの利益確保が難しいこともあり、手厚く対応することができない状況も見て取れる。

【主なヒアリング結果】

- パッケージ導入後、何かあったときに助け舟を求められることがあるが、いつもログを見ているわけではないので、そのアラートがいつも出ているものなのか否か判断がつかない。ログの解析を求められた場合は、IPA で出しているログ分析ツールなども使いながら実施しようとはしているが、普段からログを見るような契約を結んでいるわけではないので、中々分析も難しい。（C 社）
- ユーザー会が活発ではない理由は、当社の人材不足である。また、コスト（をかけても、中々ビジネスに繋がるわけではないという点）をどう見るかということもある。そのため、ユーザー向けに、セキュリティセミナーや勉強会などのような無償のサービスを提供できていない状況である。発注後の案件であれば、相談にのったり、個別にシステム対応をしたりしていることも多い。（E 社）
- 別ベンダーのインフラに口を出すのは、中々難しい面もある。当社は、受託したプログラム開発を行っている部分が多い。場合によって、別ベンダーに対してセキュリティ改善の提案をしていることはあったとしても、それは相手の事業者（ベンダー）に直接言うのではなく、顧客を通じて申し入れることになる。なお、協業している場合はその限りではないが、全く別発注の場合は、別ベンダーのインフラのシステム構成について話をすることはない。（E 社）
- IT の全てを 1 社の業者に丸投げしているため特定の業者に依存する状況となっており、セキュリティ対策の実施について業者に強く要請できない状況になっている顧客がある。その結果、単純パスワードの使用などセキュリティ対策を取られていない

ままま納品されているシステムを見ることがある。マルチベンダー化が可能になれば発注者側が有利になるためセキュリティ対策の実施も要件に加えることができるようになると思うが、複数のベンダーをコントロールできるIT人員がいない企業も多い。(R社)

（5）システムの設計時・構築時におけるセキュリティ確保の取組と対応上工夫しているポイント

地域ITベンダーがシステム設計・構築時に実施しているセキュリティ確保の取組としては、簡易診断ツールやIPAのチェックリストを活用するなどして、顧客の理解を得やすい形でセキュリティの重要性を訴求する工夫を行っている。

【主なヒアリング結果】

- 顧客から外部に公開するウェブサイト構築の依頼を受けたときは、脆弱性診断を必須にしている。これをやらないとこういうリスクがあると強く申し上げるようにしている。(A社)
- 外部公開されるものであっても診断をやりたくないという顧客の場合､オープンソースの脆弱性スキャンツールを用いて診断をすることがある。その場合、ソフト開発の部分のみお金をもらい、ライセンス料は徴収しない形になる。(C社)
- 当社で顧客のサーバーを預かるホスティングサービスで、サーバーを提供する際には、セットアップや、Windowsの最新版へのアップデート、ウイルススキャンを実施した状態で出荷をするなど、最低限のことは実施している。(G社)
- 様々なセキュリティリスクを判定するため､IPAの情報セキュリティに関するチェックリストを用いて､顧客にヒアリングを実施し､対策として抜けているものを把握する。そのうえで､必要なセキュリティ対策を顧客に理解してもらうという流れをとっている。自社でチェックリストを作るよりも､知名度の高いIPAが作っているものを活用する方が、顧客から見るとインパクトがある。(M社)

（6）システムの運用時・保守時におけるセキュリティ確保の取組と対応上工夫しているポイント

地域ITベンダーがシステムの運用・保守時に実施しているセキュリティ確保の取組としては、保守契約の締結に加えて、自動化技術の活用やリモート対応の導入等により、運用・保守を効率化しつつ、定期的な診断や提案を通じてセキュリティの維持と向上に努める等の工夫を行っている。

【主なヒアリング結果】

- SLA（Service Level Agreement）を定義し、運用保守契約締結を前提にパッケージを導入してもらっている。以前は、問合せ対応も含めて運用保守契約で対応していたが、それだと運用が回らないので、しっかりとSLAを結ぶ形態に切り替えた。(G社)
- 顧客にシステムの導入・運用体制が構築されていない場合､固定の担当者から当社に問い合わせしてもらい､マンツーマンで解決をするという方法をとっている。スポッ

ト契約を結んでおり、少額（ミニマム 1 万円とか）で問い合わせ・障害対応を実施する。大規模障害が発生した場合は、その対応について追加でお金をいただくこともある。(C 社)

- 少し大規模な中小企業の場合､ある程度の異常を検知してくれる AI をいれることで、監視を一定自動化できる旨も提案している。(B 社)
- データの自動バックアップ機能の設定確認やパッチ適用についても、当社がリモートで対応している。(K 社)
- サービス導入時に、顧客の緊急連絡窓口を決めてもらい、夜間でも電話連絡等ができるようにしている。また、定期的にインシデント時の連絡訓練をしているサービスもある。毎月セキュリティの運用レポートを顧客に出す際、インシデントではないがこういうことが起きている、という説明をしている。(A 社)
- 脆弱性診断を定期的に受けることを推奨している。(H 社)

（7）IPA 施策の活用ニーズ

IPA のセキュリティ支援施策としては、SECURITY ACTION やお助け隊サービスの認知度は低く、登録セキスペは制度として活用されていない印象があるため、顧客や業界内での認知を高める広報活動や、実務での活用を促進する仕組みが必要であるとの意見があった。また、セミナーや教育コンテンツ、ガイドライン等の充実を通じて、顧客や社内のセキュリティ意識を高める支援が期待されている。

【主なヒアリング結果】

- SECURITY ACTION やお助け隊サービスのブランドの認知度が低い。お助け隊サービスといっても同業者でも知らない人がいる。プライバシーマークくらい認知度があがればうれしい。(A 社)
- 登録セキスペは、制度として活用されていないイメージがある。登録者は増えていると思うが、類似の他資格と混在していている印象。(B 社)
- 社内で登録セキスペの認定資格者は何名かいるが、資格取得に向けたセミナーの開催や、受験料に対する補助が欲しい。(O 社)
- 「中小企業の情報セキュリティ対策ガイドライン」を中小企業に認知してもらえれば、セキュリティ確保はお金がかかることへの理解が進んでいくと思う。(H 社)
- IT ベンダーから顧客に対して現行のセキュリティリスクを伝えても響かないので、IPA のような公的団体が顧客の経営層に向けてセミナーを実施することが役立つのではないだろうか。(C 社)
- 自社の顧客でセキュリティに関するユーザー会を行うには、当社のスキルが不足している。IPA サイトにアップされているセキュリティ動画を、以前に社内向け教育で活用していた。同様に、ユーザー向けの意識啓発動画があると情報提供はやりやすくなる。講師派遣も含めコンテンツが充実するとありがたい。(G 社)

（8）地域 IT ベンダー向け手引きの活用ニーズ

IPA で作成を検討している「地域 IT ベンダー向け手引き」については、中小企業の実情に即した、具体的でわかりやすい内容が求められている。特に、経営層向けに図表や事例を用いた簡潔な説明や、中小企業特有の課題に対応した損害イメージや具体策の提示が重要とされている。また、同業他社の事例やベストプラクティス、チェックリストの掲載により、実践的な参考資料としての活用が期待されている。さらに、手引きの普及・啓発活動の強化についてもニーズが挙がっている。

【主なヒアリング結果】

- 企業の経営層は、「難しいとさっぱりわからない」という感じになってしまうため、図表や絵を使って簡単なインプットができるものだと良いのではないか。(C 社)
- セキュリティインシデントの事例は大手企業が多いが、世間では名前も知らないような中小企業の事例を掲載した方が、むしろ中小企業の顧客には刺さりそう。(A 社)
- 設計から運用までのセキュリティ対策のベストプラクティスが具体的にあるとありがたい。中小企業はセキュリティにコストをかけられないと言われるので、中小企業の方に向けたわかりやすい損害イメージ、被害額、それに対する具体的な対策を明示してほしい。一から対策を検討しているとコストがかさむので、標準的なソリューションも紐づけていただければありがたい。(F 社)
- 同業種の IT ベンダーの取組みには興味がある。事例などがたくさん載っていると手に取って活用しようと思う。そこから、“さらにこうしてみよう”などとフィードバックにつながると思う。(J 社)
- 中小企業はトップダウンなところがあるので、経営者向けの施策の記載があるとありがたい。セキュリティや IT の技術者は、中小企業の中に専門家がいたとしても兼任者である場合が多い。それでは不十分だと啓発してほしい。セキュリティや IT の専任の技術者を確保し、経営についてもわかっている人を育てる必要がある。このあたりが書いてあるとよいのではないだろうか。(B 社)
- 現場では効率性重視で、単純なパスワードにしてしまうケースなどが往々にしてあるので、設定作業をする人物とは別に、手引きを遵守しているかのチェックをする人物が必要だと思う。手引きにチェックリストをつけると良いのではないか。(R 社)
- 商工会議所などで、啓発活動を活発に行ってほしい。(O 社)
- 手引きを、商工会議所から配布してもらうのが良いのではないか。業界紙で宣伝するのも良いかもしれない。(P 社)

2.4. 調査結果まとめ

アンケート調査結果及びヒアリング調査結果のまとめを以下に記す。

（1）提供サービス・システムのセキュリティ対策の現状

アンケート調査では、地域 IT ベンダーが、中小企業への提供サービス・システムにおいて、セキュリティ確保の取組を実施する上での問題点は、「コスト面の制約がある中小企業のお客様に訴求する取り組みやその提案が困難である」が最も多く、次いで「中小企業のお客様のセキュリティ意識が低いため、取り組みを求める需要の喚起が困難である」となっており（図表 34）、中小企業側のコスト制約やセキュリティ意識に起因してセキュリティ対策の提案が困難な状況であることが示された。ヒアリング調査でも、「顧客の経営層のセキュリティ対策に対する理解不足からなかなか導入が進まない」、「システム発注内容（要求仕様）からセキュリティ要素が対象外になっている」などの声が寄せられた。

また、アンケート調査では、受注契約においてセキュリティ対策を最低限にするよう指示を受けた経験がある地域 IT ベンダーが約 6 割にのぼる（図表 22）ことや、サービスやシステム導入後の運用・保守契約に関しては、その後の保守契約を締結していないケースが相当数存在する（図表 13）ことも判明した。

（2）中小企業のセキュリティ対応上の課題

アンケート調査では、中小企業側に起因するセキュリティ対応上の課題として、中小企業側にシステムやセキュリティに関する技術や知識を持つ技術者がいない場合が多く（約 7 割）（図表 20）、顧客社内でのサービス・システム導入体制が不十分であった経験がある地域 IT ベンダーが約 7 割いる（図表 27）など、中小企業側の導入体制が不十分であることが挙げられた。これらの問題に対してヒアリング調査では、「実際のインシデント事例の共有」、「公開情報を活用したリスクの指摘」等を顧客に対して行いながら危機意識の醸成を図ると共に、「顧客と伴走しながら進める仕組みを取り入れる」ことが効果的であるとの意見があった。

また、アンケート調査では、約 5 割以上の地域 IT ベンダーが中小企業の顧客からセキュリティに関する相談を受けたことがあり（図表 14）、その内容は「どのようなセキュリティ製品やセキュリティサービスを選べばよいか」など、地域 IT ベンダーにすべて任せるような相談が多い（図表 15）。ヒアリング調査でも、「地域 IT ベンダーへの過度な依存でセキュリティ対策も当然やってくれていると思い込んでいる」との声も聞かれ、これらの問題に対しては、「顧客と IT ベンダー双方の責任範囲を明確化」し、「契約時点で役割分担を明確にすることで、顧客の主体的な対応を促す仕組みが有効」との声が寄せられた。

（3）地域 IT ベンダーのセキュリティ確保上の問題

アンケート調査では、地域 IT ベンダーの約 8 割が社内のセキュリティ技術者は 5 名以下であり、そのうち 7.2%はセキュリティ技術者を配置していない（図表 36）。また、提供サービス・システムのセキュリティ確保の課題として、「社内にセキュリティやその商材の専門知識や技術力のある人材が不足している」が 35.4%である（図表 34）ことから、地域 IT ベンダー内のセキュリティ専門人材の不足が課題となっていることが判明した。これに関する要因として、ヒアリング調査でも「セキュリティ人材の育成にコストをかけてもビジネスに繋がりにくい」、「セキュリティ資格を取得すると給与のより高いベンダーに転職してしまい、給与面の課題が大きい」等の声が聞かれ、地域 IT ベンダーがセキュリティ人材の確保に苦慮している状況が伺える。

一方、顧客である中小企業がセキュリティ対策に積極的に取り組むよう促すため、自社内の体制強化を目的に「人材育成」などの必要性を感じている地域 IT ベンダーもおり（問 35 自由回答）、ヒアリング調査でも、「自社の提供サービスを顧客に選んでもらうためにセキュリティ対応を必須する考え」等からセキュリティに関する自社の人的リソース確保の取組例が聞かれた。

（4）地域 IT ベンダーのセキュリティ対応能力強化に資する支援策

アンケート調査では、地域 IT ベンダーが自社のセキュリティ対応能力の強化のために今後活用してみたい IPA 施策として、「情報セキュリティマネジメント試験・資格認定」が 43.3%と最も多く、次いで「情報処理技術者試験・資格認定」が 42.6%、「情報処理安全確保支援士試験・資格認定」、「中小企業の情報セキュリティ対策ガイドライン」が 36.1%となっており（図表 38）、人材育成を中心とした IPA の施策への期待が高かった。ヒアリング調査でも、セミナーや教育コンテンツ、ガイドライン等の充実を通じて、顧客や社内のセキュリティ意識を高める支援の期待の声が寄せられた。

一方、IPA では本業務の結果を踏まえ、中小企業のセキュリティ対応において、地域 IT ベンダーの役割や対応をまとめた「地域 IT ベンダー向け手引き」を作成する予定であることを伝え、その上で当該手引きの中にどのような情報を盛り込むべきだと思うか、アンケート調査で回答を求めたところ、「中小企業のお客様のセキュリティ対応の行動変容を啓発していくために必要な資料・事例」が 63.5%と最も多く、次いで「セキュリティ対応において中小企業のお客様に求められる責務」が 62.8%、「中小企業のお客様の実態に即した実現可能な地域 IT ベンダーの役割や対応」が 60.6%であった（図表 39）。ヒアリング調査でも、「中小企業の実情に即した具体的でわかりやすい内容」、「経営層向けに図表や事例を用いた簡潔な説明」、「中小企業特有の課題に対応した損害イメージや具体策の提示」が重要との意見が寄せられた。また、また、同業他社の事例やベストプラクティスの掲載により、実践的な参考資料としての活用が期待されている。

3. 地域 IT ベンダー向け手引きの作成

本業務の地域 IT ベンダー状況調査（アンケート調査、ヒアリング調査）の結果を踏まえ、地域 IT ベンダーが中小企業のセキュリティ対応の「良き相談相手」を担うために果たすべき役割を整理し、有効な対応や取組のプラクティスをまとめた「地域 IT ベンダー向け手引き」を作成した。（詳細は別紙「中小企業のお客様へのセキュリティ対応のための地域 IT ベンダー向け手引き」を参照。）

地域 IT ベンダー向け手引きは、「第 1 部 中小企業のお客様が抱えるセキュリティ対応上の課題」、「第 2 部 地域 IT ベンダーが中小企業のお客様の良き相談相手となるための取組」の 2 つのパートからなる本編と付録により構成され、付録には中小企業のお客様へのセキュリティ対応に役立つ情報として、手引きに掲載の IPA セキュリティ支援施策を紹介している。

構成		概要
本編	第 1 部 中小企業のお客様が抱えるセキュリティ対応上の課題	中小企業への提供サービス・システムのセキュリティ確保上の問題点をあげ、中小企業のお客様が抱えるセキュリティ対応上の課題について説明
	第 2 部 地域 IT ベンダーが中小企業のお客様の良き相談相手となるための取組	1．地域 IT ベンダーに求められる責務 2．責務を果たすための取組のプラクティスについて記載し、地域 IT ベンダーが中小企業のお客様から信頼される良き相談相手となるための取組ヒントについて説明
付録	中小企業のお客様へのセキュリティ対応に役立つ情報	地域 IT ベンダーが中小企業へセキュリティ対応を行う際に役立つ情報として、本手引きに掲載の IPA セキュリティ支援施策を紹介

図表 49 地域 IT ベンダー向け手引きの全体構成

今後、地域 IT ベンダーが本手引きを活用して、セキュリティ対応が不十分な中小企業の顧客がサイバー攻撃の被害に遭う前に、すみやかな手立てが講じることが期待される。

4. まとめ（考察）

本業務の調査結果により、中小企業の顧客のセキュリティ意識の現状と、地域 IT ベンダーが抱えるセキュリティ対応上の課題が浮き彫りとなった。

中小企業の多くは情報セキュリティに関する知識や意識が必ずしも十分でなく、経営層の理解が得られていない中、コスト制約も強いため、地域 IT ベンダーは顧客へのセキュリティ対策の提案・実施に困難を感じている。これらの要因から、顧客との間で保守契約が締結されないケースもあり、インシデント対応体制の不備も散見される。

一方、地域 IT ベンダーは社内のセキュリティ人材が不足しており、社内のセキュリティ人材育成や外部専門家の活用検討が必要である。地域 IT ベンダー自身のセキュリティ技術力や顧客支援能力強化が向上すれば、中小企業全体の情報セキュリティ水準の底上げにつながると考えられる。

今後、中小企業の経営者層にセキュリティ対策の重要性を理解してもらうことが不可欠であるが、地域 IT ベンダーが自社のセキュリティ体制を整備したうえで、中小企業の顧客との責任範囲・役割分担を明確にし、良き相談相手として中小企業のセキュリティ対応の自律化支援を行っていくことが望まれる。

参考資料（アンケート調査票）

中小企業のセキュリティ対応における IT ベンダーの役割に関するアンケート

【回答者情報】

事業者名（会社名）	
部署名	
回答者氏名	
電話番号	
メールアドレス	

【調査票に回答する前に必ずお読みください】

（１）想定回答者について

アンケートの回答者については、各 IT ベンダーが提供するサービスやシステムの販売責任者とセキュリティ責任者による共同での回答をお願いいたします。

（２）本調査で対象としている中小企業の定義について

中小企業の定義は、中小企業庁が定める中小企業者の定義に従っています。

業種分類	定義
製造業その他	資本金の額又は出資の総額が 3 億円以下の会社又は 常時使用する従業員の数が 300 人以下の会社及び個人
卸売業	資本金の額又は出資の総額が 1 億円以下の会社又は 常時使用する従業員の数が 100 人以下の会社及び個人
小売業	資本金の額又は出資の総額が 5 千万円以下の会社又は 常時使用する従業員の数が 50 人以下の会社及び個人
サービス業	資本金の額又は出資の総額が 5 千万円以下の会社又は 常時使用する従業員の数が 100 人以下の会社及び個人

（３）独立行政法人情報処理推進機構(IPA)が、IT ベンダーや IT ベンダーによる中小企業のセキュリティ対応向けに実施している主な支援施策について

①IT 人材の育成や採用の際に参考となるスキル標準（ITSS／UISS）とは

IPA では、各種 IT 関連サービスの提供に必要とされる能力を明確化・体系化した指標であるスキル標準を作成しています。詳細は以下をご参照ください。

https://www.ipa.go.jp/jinzai/skill-standard/index.html

②SECURITY ACTION セキュリティ対策自己宣言とは

IPA では、中小企業自らが情報セキュリティ対策に取り組むことを自己宣言することを支援する制度を運営しています。詳細は以下をご参照ください。

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

③サイバーセキュリティお助け隊サービス制度とは
IPA では、中小企業に対するサイバー攻撃への対処として不可欠なセキュリティサービスをワンパッケージにまとめた、民間事業者から提供されるサービスを登録し公表する制度を運営しています。詳細は以下をご参照ください。
https://www.ipa.go.jp/security/sme/otasuketai/index.html

④サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）とは
IPA では、産業界が一体となって、中小企業を含むサプライチェーン全体でのサイバーセキュリティ対策の推進運動を進めていくことを目的に設立された SC3 の運営を支援しています。詳細は以下をご参照ください。
https://www.ipa.go.jp/security/sc3/

⑤中小企業の情報セキュリティ対策ガイドラインとは
IPA では、中小企業において情報セキュリティ対策に取り組む際の、経営者が認識し実施すべき指針や、社内において対策を実践する際の手順や方法をまとめたガイドラインを作成し公表しています。詳細は以下をご参照ください。
https://www.ipa.go.jp/security/guide/sme/about.html

その他にも、IPA の以下のホームページ上でさまざまな支援施策を紹介しています。
https://www.ipa.go.jp/security/sme/index.html

（4）本調査における情報の取扱い等について
①上記の【ご回答内容に関する問合せ先】で入力いただいた事業者や個人が特定される情報を、一般に公開することはありません。第三者に提供することはありません。
②アンケートの回答内容は、統計処理を行ったうえでの公開となります。回答内容を一般にそのまま公開することはありません。
③本調査の趣旨や、情報の取扱いについては、独立行政法人情報処理推進機構(IPA)の下記ウェブページをご参照ください。
https://info.ipa.go.jp/form/pub/survey/itvendor-tebiki

【質問内容】

問1. 貴社の主な事業についてお答えください。選択肢のうち、複数該当する場合、最もあてはまるものをお選びください。（ひとつだけ）※必須

1. 受託開発ソフトウェア業
2. 組込みソフトウェア業
3. パッケージソフトウェア業
4. ゲームソフトウェア業
5. 情報処理サービス業
6. 情報提供サービス業
7. ポータルサイト・サーバ運営業
8. アプリケーション・サービス・コンテンツプロバイダ
9. インターネット利用サポート業
10. 通信業
11. 放送業
12. 小売・卸売業

13. 製造業（電子部品・デバイス・電子回路製造業、情報通信機械器具製造業等）
14. その他（具体的に　　）

*上記事業の定義：
1. 受託開発ソフトウェア業:顧客の委託により、電子計算機のプログラムの作成及びその作成に関して、調査、分析、助言などを行う事業所
2. 組込みソフトウェア業：情報通信機械器具、輸送用機械器具、家庭用電気製品等に組み込まれ、機器の機能を実現するためのソフトウェアを作成する事業所
3. パッケージソフトウェア業:電子計算機のパッケージプログラムの作成及びその作成に関して、調査、分析、助言などを行う事業所
4. ゲームソフトウェア業：家庭用テレビゲーム機、携帯用電子ゲーム機、パーソナルコンピュータ等で用いるゲームソフトウェア（ゲームソフトウェアの一部を構成するプログラムを含む。）の作成及びその作成に関して、調査、分析、助言などを行う事業所
5. 情報処理サービス業：電子計算機などを用いて委託された計算サービス（顧客が自ら運転する場合を含む）、データエントリーサービスなどを行う事業所
6. 情報提供サービス業：各種のデータを収集、加工、蓄積し、情報として提供する事業所、または市場調査、世論調査などを行う事業所
7. ポータルサイト・サーバ運営業：ウェブ情報検索サービス業、インターネット・ショッピング・サイト運営業、インターネット・オークション・サイト運営業
8. アプリケーション・サービス・コンテンツプロバイダ：ＡＳＰ（アプリケーション・サービス・プロバイダ）、ウェブ・コンテンツ配信業（電気通信役務利用放送に該当しないもの）
9. インターネット利用サポート業：電子認証業、情報ネットワーク・セキュリティ・サービス業、課金・決済代行業務

問2. 貴社における組織の成り立ちについてお答えください。（ひとつだけ）※必須

1. オフィス・事務機器販売にルーツを持つ IT ベンダー
2. ERP パッケージ販売にルーツを持つ IT ベンダー
3. 独立系かつ地域密着型の受託ソフト開発ベンダー
4. 独立系かつ全国展開型の受託ソフト開発ベンダー
5. 大手ディストリビューター（IT 商社）のリセラー（代理店）
6. 大手電機メーカーの IT サービス部門（本社・支社・支店等）
7. 大手電機メーカー系列の IT 子会社・孫会社
8. 大手電機メーカー以外の大手企業（銀行、電力会社、通信会社、メーカー等）の IT サービス部門（本社・支社・支店等）
9. 大手電機メーカー以外の大手企業（銀行、電力会社、通信会社、メーカー等）系列の IT 子会社・孫会社
10. その他（具体的に　　）

問3. 貴社における直近の総従業員数（常時従業者の総数）についてお答えください。（ひとつだけ）※必須

1. 5 名以下
2. 6 名～20 名以下
3. 21 名～50 名以下
4. 51 名～100 名以下
5. 101 名～300 名以下
6. 301 名～500 名以下
7. 501 名～1,000 名以下
8. 1,001 名以上

問4. 貴社の資本金について、直近の会計年度の金額をお答えください。（ひとつだけ）※必須

1. 1,000 万円以下
2. 1,000 万円超～3,000 万円以下
3. 3,000 万円超～5,000 万円以下
4. 5,000 万円超～1 億円以下
5. 1 億円超～2 億円以下
6. 2 億円超～3 億円以下
7. 3 億円超

問5. 貴社の総売上高（単体）について、直近の会計年度の金額をお答えください。（とつだけ）※必須

1. 1,000 万円以下
2. 1,000 万円超～3,000 万円以下
3. 3,000 万円超～5,000 万円以下
4. 5,000 万円超～1 億円以下
5. 1 億円超～2 億円以下
6. 2 億円超～3 億円以下
7. 3 億円超～5 億円以下
8. 5 億円超～10 億円以下
9. 10 億円超～50 億円以下
10. 50 億円超～100 億円以下
11. 100 億円超

問6. 問 5 でお答えになられた総売上高（単体）のうち、中小企業のお客様からの売上高が占める割合はおおよそどれぐらいですか。（ひとつだけ）※必須

1. 10%以下
2. 11%～20%
3. 21%～30%
4. 31%～40%
5. 41%～50%
6. 51%～60%
7. 61%～70%
8. 71%～80%
9. 81%～90%
10. 91%～100%

問7. 貴社の本社所在地についてお答えください。（ひとつだけ）※必須

47 都道府県から選択

問8. 中小企業のお客様における IT 活用を支援するために、貴社が提供しているサービスやシステムについて、以下の中から当てはまるものをお選びください。（複数選択可）※必須

1. セキュリティ製品・サービス
2. PC・モバイル・タブレット・サーバ等の IT 機器、OS、ソフトウェア

3. 通信・ネットワーク機器（ルーター、VPN 機器等)、ネットワークサービス（VPN サービス等)
4. IoT 機器、組込みソフトウェア
5. グループウェア（メール管理、ファイル共有、スケジューラー、ドキュメント管理等)
6. コミュニケーションツール（電子メール、SNS、ビジネスチャット等)
7. シンクライアント・リモートアクセスソリューション
8. オンライン会議システム
9. 電子稟議・決裁システム
10. 文書管理・電子契約システム・アプリケーション
11. ERP・基幹業務システム・アプリケーション（会計・財務、人事・給与、販売管理、勤怠管理、生産管理、顧客管理、購買・調達等)
12. 特定業界向けのソリューション
13. Web サイト、ホームページ
14. EC 構築・オンライン決済システム・アプリケーション
15. クラウドサービス、クラウドソリューション（オンラインストレージ、リモートバックアップ等)
16. BI ツール、データ分析ツール
17. AI・IoT・RPA 活用ソリューション
18. データセンター、ハウジング・ホスティングサービス
19. その他（具体的に　　）

問9. 問８でお答えになられた貴社の事業領域において、どのようなセキュリティ確保のための取組を実施していますか。以下の中から当てはまるものをお選びください。（複数選択可）※必須

1. 設計時のリスク評価とセキュリティ要件・リスクへの対処が適切であるかの定期的な確認
2. セキュアコーディングの観点を取り込んだ開発プロセスの定義とソースコード生成・セキュアな設定
3. 脆弱性を発見するためのテストの実施と発見された脆弱性への対策の実施
4. ソフトウェアを導入したサービス・システムの運用状態のモニタリングと扱う情報資産の保護
5. サードパーティのソフトウェアコンポーネントに対する自社が定義した要件への準拠性検証
6. ソフトウェアのリリースごとの保持すべき必要なファイル・データのアーカイブ化と保護
7. 開発者－供給者－運用者間で共有するべきセキュリティ要件の確立と契約への盛り込み
8. ソフトウェアのセキュアな利用方法を保証するための利用者への適切な情報提供
9. リリースしたソフトウェアに対する継続的な脆弱性調査
10. ソフトウェアに残存する脆弱性への対処
11. 脆弱性の根本原因の再発防止やリスク低減に向けた開発・運用プロセスの改善
12. セキュア開発に対する経営層のコミットメントの強化とセキュリティ人材の育成・確保
13. セキュリティを確保するために必要な予算の確保

14. 開発するソフトウェアが満たすべきセキュリティ要件を維持するための開発ポリシーの確立
15. ソフトウェアを適用したサービス・システム運用におけるセキュリティ要件を維持するための運用ポリシーの確立
16. ソフトウェアのセキュリティを確認するための基準の定義と当該基準への適合性の監査
17. セキュアなソフトウェア開発ツールの整備
18. ソフトウェア開発におけるセキュアな開発環境の整備
19. ソフトウェアを適用したサービス・システムのセキュリティを継続的に改善するための関係組織との情報連携・協力体制の構築
20. 取組を実施していない

問10. 問９でお答えになられたセキュリティ確保のための取組を実施するにあたり、貴社ではどのような課題がありますか。以下の中から当てはまるものをお選びください。（複数選択可）※必須

1. 中小企業のお客様のセキュリティ意識が低いため、取組を求める需要の喚起が困難である
2. コスト面の制約がある中小企業のお客様に訴求する取組やその提案が困難である
3. 中小企業のお客様から価格抑制を強いられる中で利益確保や収益拡大に直結しにくい
4. セキュリティ確保によって利便性が損なわれるという問題が生じることへの懸念がある
5. 経営層のセキュリティ重視の姿勢が希薄である
6. 社内にセキュリティやその商材の専門知識や技術力のある人材が不足している
7. セキュリティの専門知識や商材を持つビジネスパートナーとの連携が不足している
8. マンパワーの需給が逼迫しており、取組が増えてもその需要に対応することが困難である
9. 地域間・拠点間で能力格差や意識格差があり、均質な取組やその提案が困難である
10. 外部委託先・パートナーの能力不足や管理体制の不備により取組の普及・浸透が進まない
11. その他（具体的に　　）
12. 特に課題はない

問 11 は、問８で「1. セキュリティ製品・サービス」とお答えになられた方にお伺いします。それ以外の方は問 12 へお進みください。

問11. 問８でお答えになられた貴社が提供している具体的なセキュリティ製品・サービスについて、以下の中から当てはまるものをお選びください。（複数選択可）※必須

1. 総合的なセキュリティ対策に資する製品・サービス（セキュリティコンサルティング、IT 資産管理製品、セキュリティ監査、リスクアセスメントサービス等）
2. インシデント発生時の迅速な初動対応に資する製品・サービス（セキュリティ監視製品（ファイアウォール、UTM 等）、ログ管理製品、セキュリティ監視運用サービス等）

3. 重要な情報の安全な取扱いに資する製品・サービス（認証・ID 管理製品、暗号化製品、DLP、アクセス管理製品等）
4. 不正プログラム対策に資する製品・サービス（エンドポイントセキュリティ製品（ウイルス対策ソフト、EDR 等）、ポリシー管理・設定管理製品等））
5. クラウドサービスやネットワークの安全な利活用に資する製品・サービス（クラウドセキュリティ製品（CASB、セキュリティ管理等）、VPN 製品、URL フィルタリング製品等）
6. サイバー攻撃の早期の封じ込めや復旧に資する製品（データバックアップ製品、インシデント対応支援サービス等）
7. 脆弱性の可視化・管理に資する製品・サービス（脆弱性診断サービス、ペネトレーションテスト、脆弱性管理サービス等）
8. 従業員等へのセキュリティ教育・訓練に資する製品・サービス（セキュリティ教育サービス、標的型メール訓練、インシデント対応模擬訓練等）
9. サイバー保険
10. その他（具体的に　　）

問12. 貴社では、中小企業のお客様にサービスやシステムを導入した後に、中小企業のお客様との間で運用・保守契約を締結していますか。また中小企業のお客様のうち、運用・保守契約を締結しているお客様の割合は、おおよそどれぐらいですか。（ひとつだけ）※必須

1. 10%以下
2. 11%～20%
3. 21%～30%
4. 31%～40%
5. 41%～50%
6. 51%～60%
7. 61%～70%
8. 71%～80%
9. 81%～90%
10. 91%～100%
11. 運用・保守契約は締結していない（運用・保守がサービスに含まれている場合も含む。）

問13. 貴社では、中小企業のお客様から自社が抱えるセキュリティ面の課題について相談を受けることがありますか。（ひとつだけ）※必須

1. 年に 1 回程度
2. 半年に 1 回程度
3. 数カ月に 1 回程度
4. 月に 1 回程度
5. 数週間に 1 回程度
6. 週に 1 回程度
7. ほぼ毎日
8. ほとんど相談を受けたことはない

問 14 は、問 13 で、「1. 年に 1 回程度」から「7. ほぼ毎日」までの選択肢についてお答えになられた方にお

伺いします。それ以外の「8. ほとんど相談を受けたことはない」とお答えになられた方は問 17 へお進みください。

問14. 問 13 で相談を受けることがある場合に、中小企業のお客様から多く寄せられる相談内容についてお答えください。（複数選択可）※必須

1. 政府等のセキュリティ施策やセキュリティ機関のレポート等の中身がどのような内容であるか
2. 自社のセキュリティ対策の取組が同業他社や同規模の他社と照らして十分であるか
3. PC 等に不審な挙動があり、それがサイバー攻撃によるものではないか
4. このまま脆弱性を放置しておくと、サイバー攻撃の標的にされるか
5. 予定しているシステムに対する機能の追加や変更等の改修が、新たな脆弱性を作り込まないか
6. 現在直面している、または周辺で発生しているサイバー攻撃にどのように対処すればよいか
7. 実際にどのようなセキュリティ対策から具体的な取組を始めればよいか（追加すればよいか)
8. どのようなセキュリティ製品やセキュリティサービスを選べばよいか
9. 必要となるセキュリティ対策の実装や運用に、どれぐらいの予算を見込む必要があるか
10. その他（具体的に　　）

問 15 は、問 13 で、「1. 年に 1 回程度」から「7. ほぼ毎日」までの選択肢についてお答えになられた方にお伺いします。それ以外の「8. ほとんど相談を受けたことはない」とお答えになられた方は問 17 へお進みください。

問15. 問 14 でお答えになられた主な相談内容について、貴社が相談に乗っていくにあたり、直面している課題は何ですか。以下の中から当てはまるものをお選びください。（複数選択可）※必須

1. 中小企業のお客様に、セキュリティ対策の取組の目的や重要性を理解してもらうことが難しい
2. 中小企業のお客様に対して、どのようなセキュリティ対策の取組を、どのレベルまで求めるべきかが分からない
3. 中小企業のお客様側のカスタマイズにより独自機能が多くなりすぎてしまっているため、セキュリティ対策を実施しようとしてもコストや手間が掛かりすぎる
4. 自社で構築したシステム以外のシステムを扱う場合に、中小企業のお客様から提供されるシステム構成・資産情報が不足しがちであるため、状況の把握が難しい
5. 相談業務に必要となる情報（インシデント関連情報、脆弱性情報、攻撃予兆情報等）の収集や分析を行うための体制が整わない
6. 社内にセキュリティの専門知識や技術力のある人材が不足しており、相談業務に十分な人員を割り当てることができない
7. 相談業務自体が利益確保や収益拡大に直結しにくいため、対応が後回しになりがちである
8. その他（具体的に　　）
9. 特に課題はない

問 16 は、問 15 で「4. 自社で構築したシステム以外のシステムを扱う場合に、中小企業のお客様から提供されるシステム構成・資産情報が不足しがちであるため、状況の把握が難しい」とお答えになられた方にお伺

いします。それ以外の方は問 17 へお進みください。

問16. 問 15 のような状況の把握が難しい中、中小企業のお客様よりサポートを求められた場合に、貴社では、どのような対応を行っていますか。（複数選択可）※必須

1. 既存のシステムから新しいシステムへの乗り換えとそれに伴う開発を提案している
2. 構成・資産等のシステム仕様やカスタマイズ状況等を確認するため、アクティブ/パッシブスキャン等を用いて独自に調査を行っている
3. 構成・資産等のシステム仕様やカスタマイズ状況等を確認するため、既存のシステムを構築したベンダーに対しヒアリングを行っている
4. 既存のシステムを構築したベンダーから納入仕様書等の必要な情報を取り寄せている
5. その他（具体的に　　）
6. 特に何も対応していない

問17. 中小企業のお客様がサービスやシステムの調達を行う際に、貴社では、中小企業のお客様から、セキュリティ要素が十分に考慮されていない要求仕様を含む提案依頼書の提示を受けることがありますか。（ひとつだけ）※必須

1. よくある
2. 時々ある
3. ほとんどないが、まれにある
4. 全くない

問 18 は、問 17 で「1. よくある」、「2. 時々ある」、「3. ほとんどないが、まれにある」とお答えになられた方にお伺いします。それ以外の方は問 19 へお進みください。

問18. 問 17 のような提示を受けた場合に、貴社では、中小企業のお客様のセキュリティ対策の実装を後押し・支援するため、どのような対応を行っていますか。（複数選択可）※必須

1. セキュリティ対策の目的や必要性を認識してもらうため、過去に発生したインシデントや被害について説明している
2. セキュリティ対策の目的や必要性を認識してもらうため、同業他社や同規模の他社を引き合いにして必要となるセキュリティ対策の取組について説明している
3. セキュリティの観点からの要求仕様の見直しについて依頼している
4. 要求仕様の中に本来盛り込むべきセキュリティ要素の追加提案を行っている
5. その他（具体的に　　）
6. 特に何も対応していない

問19. IT ベンダーへの発注が決まり、中小企業のお客様との間で要件定義の調整を行う際に、貴社では、中小企業のお客様側にシステムやセキュリティに関する技術や知識を持つ技術者がいない状況に直面することがありますか。（ひとつだけ）※必須

1. よくある
2. 時々ある

3. ほとんどないが、まれにある
4. 全くない

問 20 は、問 19 で「1. よくある」、「2. 時々ある」、「3. ほとんどないが、まれにある」とお答えになられた方にお伺いします。それ以外の方は問 21 へお進みください。

問20. 問 19 のような状況に直面した場合に、貴社では、中小企業のお客様自身におけるシステムやセキュリティに関する技術や知識の補完を後押し・支援するため、どのような対応を行っていますか。（複数選択可）※必須

1. 担当者がシステムやセキュリティの基礎知識について学ぶことができるよう、セミナーや勉強会等を開催している
2. 担当者がシステムやセキュリティについて気軽に相談することができるよう、相談窓口やコミュニケーションツールを提供している
3. 必要となるセキュリティ対策の概要を中小企業向けに分かりやすく解説しているガイドラインや手引き、参考となる関連資料を紹介している
4. 自社内にシステムやセキュリティの運用の担当者を置かなくても済む IT ベンダーへの外部委託の活用や SaaS 型サービスの利用を勧めている
5. その他（具体的に　　）
6. 特に何も対応していない

問21. 中小企業のお客様との間で要件定義の調整を行う際に、コスト制約等の理由によりセキュリティ対策については最低限の実装に抑えるよう指示を受けることがありますか。（ひとつだけ）※必須

1. よくある
2. 時々ある
3. ほとんどないが、まれにある
4. 全くない

問 22 は、問 21 で「1. よくある」、「2. 時々ある」、「3. ほとんどないが、まれにある」とお答えになられた方にお伺いします。それ以外の方は問 23 へお進みください。

問22. 問 21 のような状況に直面した場合に、貴社では、中小企業のお客様におけるセキュリティ担保を後押し・支援するため、どのような対応を行っていますか。（複数選択可）※必須

1. 最低限のセキュリティ対策だけでは、巧妙化・高度化が一段と進むサイバー攻撃への対処を十分にカバーし切れないことについて説明している
2. 最低限のセキュリティ対策だけでは、万が一、システムがインシデントや被害を受けた場合にその損害を補償できないことについて説明している
3. 担当者に自社のセキュリティレベルを再認識してもらうため、点検・診断サービスや自己点検・診断ツールを提供している
4. 必要最低限の対策と、推奨する対策を区別して、それぞれの導入を依頼している
5. 中小企業が利用しやすい安価なセキュリティサービス（サイバーセキュリティお助け隊サービスなど）の利用を勧めている
6. セキュリティ面の問題を早期に把握できるよう、脆弱性対策や異常監視・対応を含む運用・保守契約の締結やメンテナンスサービスのスポット利用を勧めている
7. 自らの責任と役割、管理のもとで別途取組むべきセキュリティ対策について説明している

8. その他（具体的に　　）
9. 特に何も対応していない

問23. 中小企業のお客様との間で要件定義の調整を行う際に、コスト制約等の理由により、中小企業のお客様に対してセキュリティ対策の運用に係る応分の負担を求めることがありますか。（ひとつだけ）※必須

1. よくある
2. 時々ある
3. ほとんどないが、まれにある
4. 全くない

問 24 は、問 23 で「1. よくある」、「2. 時々ある」、「3. ほとんどないが、まれにある」とお答えになられた方にお伺いします。それ以外の方は問 25 へお進みください。

問24. 問 23 のような負担を求めた場合に、貴社では、中小企業のお客様におけるインシデントの発生抑止や、適切なリスク管理を後押し・支援するため、どのような対応を行っていますか。（複数選択可）※必須

1. セキュリティリスクへの対処の必要性を認識してもらうため、直近に発生したインシデントや被害に関わる情報を提供している
2. セキュリティリスクへの対処を促すため、システムを構成するハードウェアやソフトウェア、プロトコル等に関わる脆弱性情報を提供している
3. セキュリティリスクへの対処を促すため、システム（ソフトウェア等）の最新バージョンの情報を提供している
4. 担当者がセキュリティリスクやその対処について学ぶことができるよう、セミナーや勉強会等を開催している
5. 担当者がセキュリティリスクについて気軽に相談することができるよう、相談窓口やコミュニケーションツールを提供している
6. インシデントや被害に遭わないために、中小企業の担当者がシステムやセキュリティ対策の運用において実施すべき事項をまとめたガイドを提供している
7. 万が一、システムがインシデントや被害を受けた場合に備えて、サイバー保険や損害賠償保険への加入を勧めている
8. その他（具体的に　　）
9. 特に何も対応していない

問25. 中小企業のお客様にサービスやシステムを導入し、運用を開始する際に、貴社では、中小企業のお客様側の社内での導入体制が十分に整備されていない状況に直面することがありますか。（ひとつだけ）※必須

1. よくある
2. 時々ある
3. ほとんどないが、まれにある
4. 全くない

問 26 は、問 25 で「1. よくある」、「2. 時々ある」、「3. ほとんどないが、まれにある」とお答えになられた方にお伺いします。それ以外の方は問 27 へお進みください。

問26. 問 25 のような状況に直面した場合に、貴社では、中小企業のお客様における安全・安心なサービス・システム利用を後押し・支援するため、どのような対応を行っていますか。（複数選択可）※必須

1. 担当者がサービスやシステムの適切な利用方法について学ぶことができるよう、説明会を開催している
2. ヘルプデスクの開設やサービス・システム利用ガイドの提供等のサポートサービスを提供している
3. サービスやシステムの利用や運用について実施要領を定め、適切な社内利用・運用体制を構築するよう依頼している
4. セキュリティ関連規程の策定やセキュリティ担当者の設置を含め、セキュリティを考慮した社内利用・運用体制を構築するよう依頼している
5. その他（具体的に　　）
6. 特に何も対応していない

問27. 中小企業のお客様がサービスやシステムの運用を行っている際に、当該サービスやシステムに関連して、中小企業のお客様側の起因または自社側の起因、またはその双方によりインシデントが発生したことがありますか。（複数選択可）※必須

1. 中小企業のお客様側の起因でインシデントが発生したことがある
2. 自社側の起因でインシデントが発生したことがある
3. 中小企業のお客様側の起因、自社側の起因の双方でインシデントが発生したことがある
4. インシデントが発生したことがない

問 28 は、問 27 で「1. 中小企業のお客様側の起因でインシデントが発生したことがある」、「3. 中小企業のお客様側の起因、自社側の起因の双方でインシデントが発生したことがある」とお答えになられた方にお伺いします。それ以外の方は問 30 または問 31 へお進みください。

問28. 問 27 のような中小企業のお客様側の起因でインシデントが発生した場合、貴社では、中小企業のお客様の実効的なインシデント対応を後押し・支援するため、どのような対応を行っていますか。（複数選択可）※必須

1. 契約や取決めの中でインシデント対応に係るベンダーと中小企業のお客様の間の役割分担を明確にしている
2. 相談窓口やインシデントの報告先・届出先を紹介している
3. インシデントや被害を受けたサービスやシステムの状況調査を行っている
4. 必要となるインシデント対応の概要を中小企業向けに分かりやすく解説しているガイドラインや手引き、参考となる関連資料を紹介している
5. インシデント対応として実施すべき事項をまとめたガイドを提供している
6. 専門家がインシデント対応やサービス・システムの復旧に向けた支援を行うサービスを提供している
7. その他（具体的に　　）
8. 特に何も対応していない

問 29 は、問 27 で「1. 中小企業のお客様側の起因でインシデントが発生したことがある」、「3. 中小企業のお客様側の起因、自社側の起因の双方でインシデントが発生したことがある」とお答えになられた方にお伺いします。それ以外の方は問 30 または問 31 へお進みください。

問29. 問 27 のような中小企業のお客様側の起因でインシデントが発生した場合に備えて、中小企業のお客様との間で今後どのような対応の強化が重要になるとお考えですか。(複数選択可) ※必須

1. 安全・安心なサービス・システムを提供するため、必要となるセキュリティ対策の実装を徹底する
2. インシデントが疑われる兆候や実際の発生に早期に対処できるよう、脆弱性対策や異常監視・対応を含む運用・保守契約の締結を徹底する
3. インシデントが疑われる兆候や実際の発生に早期に把握できるよう、外部のセキュリティ監視サービスの利用推進を徹底する
4. 中小企業のお客様に対してセキュリティ対策の運用に係る応分の負担を求める場合に、必要となる情報提供の側面からの運用支援の推進を徹底する
5. 万が一、システムがインシデントや被害を受けた場合に備えて、サイバー保険や損害賠償保険への加入推進を徹底する
6. その他（具体的に　　）

問 30 は、問 27 で「2. 自社側の起因でインシデントが発生したことがある」、「3. 中小企業のお客様側の起因、自社側の起因の双方でインシデントが発生したことがある」とお答えになられた方にお伺いします。それ以外の方は問 31 へお進みください。

問30. 問 27 のような自社側の起因でインシデントが発生した場合、貴社では、自社の責務として、中小企業のお客様に対して、どのような対応を行っていますか。(複数選択可) ※必須

1. インシデントの発生原因や被害範囲等について調査を行っている
2. インシデントへの迅速な対処について善後策を講じている
3. 同様のインシデントが以降発生しないように再発防止策を講じている
4. 中小企業のお客様によるインシデント被害の公表や関係機関への報告をサポートしている
5. 契約や利用規約等で定めた範囲で中小企業のお客様が被った損害を補償している
6. システムコンポーネントである他社製のハードウェア・ソフトウェア等に原因がある場合でも、自社で必要な情報を収集し対処している
7. システムコンポーネントである他社製のハードウェア・ソフトウェア等に原因がある場合は、他社にインシデント対応を依頼している
8. その他（具体的に　　）
9. 特に何も対応していない

問31. 貴社の社内におけるセキュリティ対応体制についてお伺いします。貴社では、セキュリティ関連の被害を防止するために、どのような組織面・運用面の対策を実施していますか。以下の中から当てはまるものをお選びください。(複数選択可) ※必須

（人的対策）

1. 事業継続計画（BCP）の策定
2. 情報セキュリティに関するリスク分析
3. セキュリティポリシーやセキュリティ関連の規程・ルールの文書化
4. 従業員向けのアカウント管理ルールやパスワード設定ルールの策定
5. 管理者権限アカウントの管理ルールの策定
6. IT 資産の構成・設定の文書化

（物理的対策）
7. フロアや施設への入退出管理
8. 紙文書などの書類を収納するキャビネット等の施錠管理
9. 外部送信ファイルへのパスワード設定
10. セキュリティワイヤー等による機器の固定や持ち出し・盗難防止
11. 機器や記録媒体の持ち込み・持ち出しの制限
12. ハードディスク等の廃棄時の破砕や溶融、専用ソフトウェア・強磁気によるデータ消去
（組織的対策）
13. 情報セキュリティマネジメントシステム（ISMS）の認証取得
14. プライバシーマーク（P マーク）の認証取得
15. 情報セキュリティ監査（内部監査）の定期的な実施
16. 情報セキュリティ監査（外部監査）の定期的な実施
17. 情報セキュリティ対策の定期的なレビューと見直し
18. 委託先の情報セキュリティ対策の対応状況やインシデントの発生状況などの確認
19. （委託内容に応じて）委託先との NDA（機密保持契約）の締結
（技術的対策）
20. アカウントごとのアクセス制御
21. 従業員のプログラムインストールの制限（exe ファイルの実行制限等）
22. 重要なシステム・データのバックアップ
23. セキュリティ監視サービスの活用
24. ログやファイル情報に基づく Web サイトのプラットフォームやアプリケーションの改ざん検知
25. 定期的な Web サイトのプラットフォームやアプリケーションの脆弱性診断サービスの活用
26. その他（具体的に　　）
27. 特に何も実施していない

問32. 貴社では、社内にシステムやセキュリティに関する技術や知識を持つ技術者をおおよそ何人ぐらい抱えていますか。（ひとつだけ）※必須

1. そのような技術者はいない
2. １名のみ
3. ２名～３名
4. ４名～５名
5. ６名～10 名
6. 11 名～20 名
7. 21 名～30 名
8. 31 名～50 名
9. 51 名～100 名
10. 101 名～300 名
11. 301 名～500 名
12. 501 名～1,000 名
13. 1,001 名以上

問33. 問 32 でお答えになられた技術者に対して、セキュリティ教育をどのように実施していますか。(複数選択可) ※必須

1. セキュリティ関連情報の周知（社内メール・回覧・掲示板など）
2. 情報セキュリティや個人情報保護について遵守すべき事項を学ぶための e ラーニング
3. 外部の講習会やセミナーの聴講
4. 社内の研修や職場での勉強会の実施
5. 情報処理安全確保支援士等の資格取得の支援
6. その他（具体的に　　）
7. 特に何も実施していない

問34. IPA では、IT ベンダー向けにさまざまな支援施策を実施してきていますが、貴社のセキュリティ対応能力の強化のために、今後活用してみたい施策がありますか。(複数選択可) ※必須

1. 情報処理技術者試験・資格認定
2. 情報処理安全確保支援士（登録セキスペ）試験・資格認定
3. 情報セキュリティマネジメント試験・資格認定
4. IT 人材の育成や採用の際に参考となるスキル標準（ITSS／UISS）
5. SECURITY ACTION セキュリティ対策自己宣言
6. 地域団体等との連携による中小企業のサイバーセキュリティ対策普及促進のためのセミナー開催支援
7. 中小企業のサイバーセキュリティ対策普及促進のためのセミナーへの講演者（セキュリティプレゼンター）の派遣
8. サイバーセキュリティお助け隊サービス制度
9. 情報セキュリティサービス基準適合サービスリスト
10. サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）
11. 5 分でできる！情報セキュリティ自社診断
12. サイバーセキュリティ経営可視化ツール
13. MyJVN バージョンチェッカ for .NET
14. 5 分でできる！情報セキュリティポイント学習
15. 映像で知る情報セキュリティ
16. 中小企業向け情報セキュリティ講習能力養成セミナー
17. 中小企業の情報セキュリティ対策ガイドライン
18. 中小企業のためのセキュリティインシデント対応手引き
19. 中小企業のためのクラウドサービス安全利用の手引き
20. その他（具体的に　　）
21. 特に活用してみたいとは思わない

問35. 貴社では、今後、中小企業のお客様の良き相談相手として、セキュリティファーストの考え方から、中小企業のお客様のセキュリティ対応の行動変容を促していくために、社内のリソースや体制において何を充実強化していく必要があるとお考えですか。お考えを自由回答欄にご記入ください。(自由回答) ※必須

問36. IPA では、本アンケートの結果を踏まえつつ、今後、セキュリティ意識の低い中小企業のセキュリティ対応の行動変容を促すために、地域の IT ベンダーが採るべき役割や対応をまとめた「IT ベンダー向け手引き」を作成する予定ですが、当該手引きをより有効なものとするには、当該手引きの中にどのような情報を盛り込むべきだと思われますか。(複数選択可) ※必須

1. 中小企業のお客様の実態に即した実現可能な IT ベンダーの役割や対応
2. セキュリティ対応において中小企業のお客様に求められる責務
3. 中小企業のお客様のセキュリティ対応の行動変容を啓発していくために必要な資料・事例
4. IT ベンダーの社内のリソースや体制を強化していくための有効な方法
5. 当該手引きの効果的な活用方法
6. 当該手引きと連動して活用可能な政府や IPA の施策
7. その他（具体的に　　）
8. よく分からない

アンケートは以上です。ご協力ありがとうございました。