202604a

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

独立行政法人情報処理推進機構
セキュリティセンター

はじめに

手引き作成の背景と目的

IPA が実施した中小企業の実態調査[1]では、中小企業がセキュリティに関して困ったことがあった際の相談先として、「社外の IT 関連業者」の割合がもっとも高く（約 5 割）、地域の IT 関連企業（以下「地域 IT ベンダー」という）が重要な役割を担っていることが分かりました。

他方、サイバー攻撃の被害にあった事案の中には、IT ベンダー側の知識や対応不足等が起因するものもあるなど、地元企業に対して IT システムを納入する地域 IT ベンダーの皆様のセキュリティ対応の強化が求められています。

本手引きは、中小企業のセキュリティ対応のレベル向上を促すために、地域 IT ベンダーが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記載することで、地域 IT ベンダーが中小企業の「良き相談相手」としての役割を担っていただくことを目的としています。ぜひ、本手引きをご一読いただき、セキュリティ対応が不十分な中小企業のお客様がサイバー攻撃の被害に遭う前に、すみやかに手立てが講じられることを期待します。

なお、本手引きの記載内容は、IPA が実施した地域 IT ベンダー向け調査[2]にもとづくものになります。詳細は当該事業の実施報告書も併せてご参照ください。

本手引きの対象

本手引きは、中小企業の顧客向けに、システムやソフトウェア製品、または IT サービスを提供している地域 IT ベンダーの開発・運用担当者、営業担当者を対象とし、経営者やリスク管理担当者も想定読者に含みます。

[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]「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」地域 IT ベンダー状況調査
https://www.ipa.go.jp/security/reports/sme/ it-vendor.html

本手引きの全体構成

本手引きは、「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ます。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、本手引きに掲載の IPA セキュリティ支援施策を紹介しています。

本手引きの全体構成

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

本手引きの活用方法

第 1 部で中小企業が抱えている現状の課題を認識した上で、第 2 部は、地域 IT ベンダーに求められる責務とその責務を果たすための取組について記載しています。地域 IT ベンダーは、自社が提供するシステム等のセキュリティ対応について責務があり、提供するシステム等に起因するリスク回避を心がける必要があります。地域 IT ベンダー自身も「サイバーセキュリティを実践する企業」であることを認識し、本手引きをサイバーセキュリティ対策に取組む際の参考にしてください。

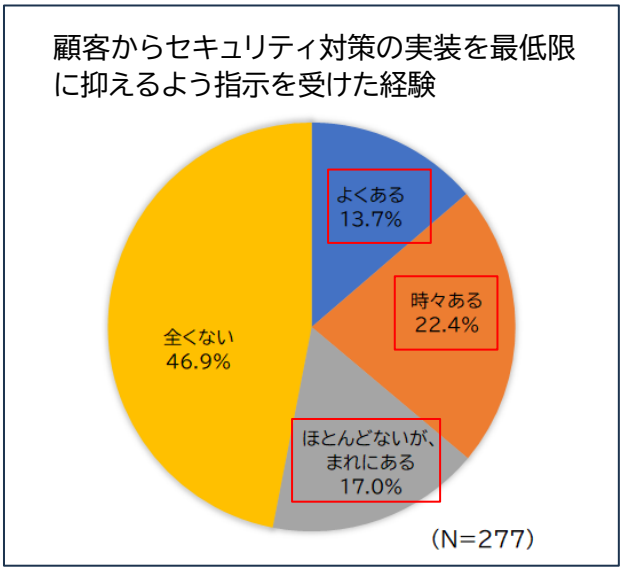
第1部　中小企業のお客様が抱えるセキュリティ対応上の課題

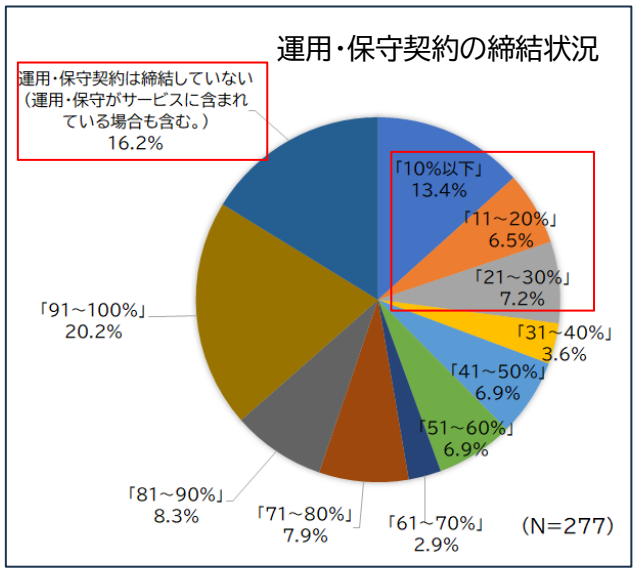
第1部では、中小企業への提供サービス・システムのセキュリティ確保上の問題点をあげ、中小企業のお客様が抱えるセキュリティ対応上の課題について説明します。

1.1 提供サービス・システムのセキュリティ対策の現状

IPA が実施した地域 IT ベンダー向け調査では、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、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ました。同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ました。

また、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 割にのぼることや、サービスやシステム導入後の運用・保守契約の締結状況に関しては、3 割以下と回答した地域 IT ベンダーが 27.1%、「運用・保守契約は締結していない」が 16.2%で、提供サービス・システムのセキュリティ対策の導入や保守における契約上の問題が少なからず存在します。

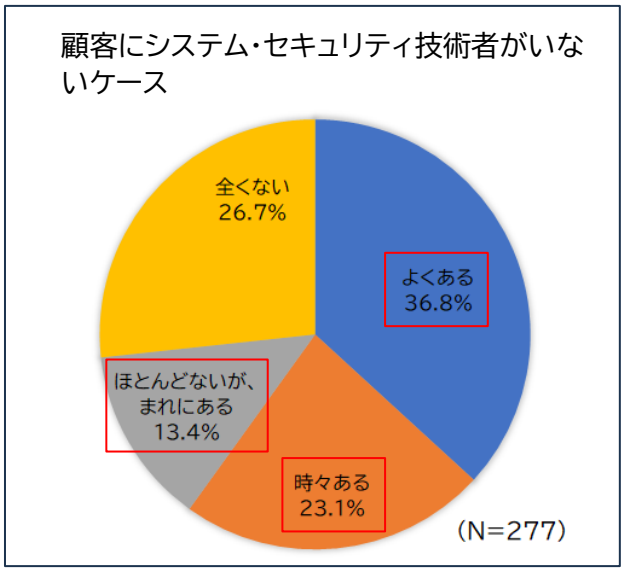


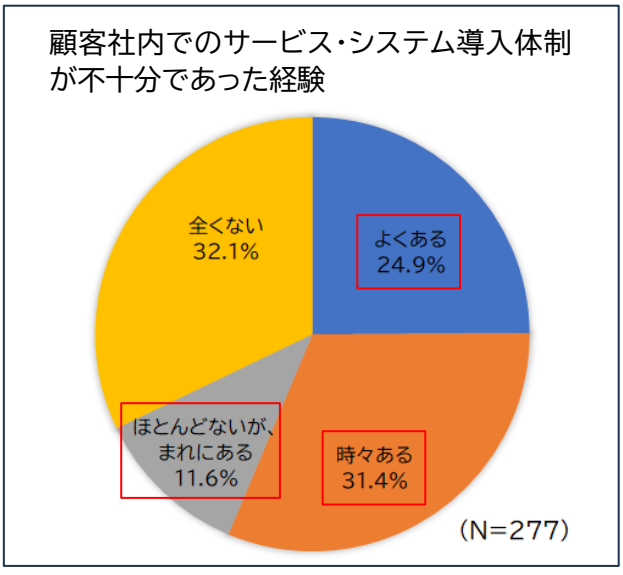


1.2 中小企業のセキュリティ対応上の課題

IPA が実施した地域 IT ベンダー向け調査では、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）、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ました。同ヒアリング調査では、これらの問題に対して「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りました。

また、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、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くありました。同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」との声が寄せられました。





第2部　地域 IT ベンダーが中小企業の良き相談相手となるための取組

第 2 部では、地域 IT ベンダーに求められる責務と、責務を果たすための取組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します。（掲載の IPA セキュリティ支援施策の参考 URL は「付録　中小企業へのセキュリティ対応に役立つ情報」を参照）

2.1 地域 IT ベンダーに求められる責務

（1）自社のセキュリティ体制を整備しましょう！

中小企業にとって、地域 IT ベンダーはセキュリティの困りごとがあった際の主たる相談先であり、言わば地域のセキュリティの守護神の役割が期待されています。

一方、IPA が実施した地域 IT ベンダー向け調査では、地域 IT ベンダー内のセキュリティ専門人材の不足しており、約 4 割の地域 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課題として、「社内のセキュリティ専門知識や技術力のある人材不足」をあげています。これに関する要因として、同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ます。

しかし、近年、IT ベンダーにおけるサイバー事案もみられるところ、自らも「サイバーセキュリティを実践する企業」であり、顧客企業にも影響を及ぼし得る存在であることを認識して、セキュリティ対策に取組む必要があります。顧客である中小企業の期待を裏切り、提供サービス・システムにセキュリティリスクがある状態で納品することがないよう、地域 IT ベンダー自らが自社のセキュリティ体制を整備する必要があります。

（2）システム提供時にセキュリティを考慮した対応をしましょう！

中小企業の顧客から、口約束でセキュリティ対応を依頼されたり、追加対応について十分な対価が支払われなかったりすることがないように、契約上、責任範囲を明示しておくことが大切です。しっかりと、中小企業側にセキュリティ上のリスクを説明し、セキュリティ対策の重要性を理解してもらう必要があります。そのことが、その後のトラブル回避になるとともに、顧客との良好な関係構築にもつながります。

また、中小企業の顧客が採用可能なセキュリティ対策を適切に提案することで、顧客

側に選択の余地が生まれます。同時に、地域 IT ベンダーにとっても、技術者に製品知識習得の機会が生じ、顧客提案や保守運用の提供範囲が広がります。

（3）システムライフサイクル各フェーズでセキュリティを確保しましょう！

地域 IT ベンダーは、システム開発・運用や製品・サービス提供のそれぞれの場面でのセキュリティ対応力の強化が求められています。まずは責任分界に沿って、IT ベンダー側がやるべきことをしっかりと実施することが重要です。その際、顧客である中小企業側がセキュリティ対策に前向きとは限らないので、都度、中小企業側がやるべきことをしっかり伝達し、履行を促してください。万が一、セキュリティインシデントが発生した時は、とりわけ責任分界の問題が顕在化しがちです。予め、インシデントが発生した場合の基本動作について、顧客である中小企業側とコミュニケーションを取っておきましょう。

運用保守契約を締結している場合、中小企業側は暗黙的にセキュリティ対応もシステムの運用保守契約に包括されていると思っている場合があります。一方、IT ベンダー側は運用保守の中で対処できないセキュリティリスクは、顧客側が対応すべきと考えていることが多く、双方にギャップが生じているケースが見られます。顧客である中小企業側には、一般的なシステムの運用保守契約に含まれるセキュリティ対応は必要最低限のもので、サイバー攻撃への対処に限界があり十分にカバーし切れない場合があることや、サイバー攻撃の被害を受けた場合にその損害を補償できないことを理解してもらい、その上で、セキュリティインシデント発生時に顧客側で行うべき事業継続のための取組や、必要な対策について備えるように促してください。

（4）中小企業のセキュリティ対応の自律化支援をしましょう！

中小企業にとって、地域 IT ベンダーは身近な相談相手となっています。相談の場面を絶好の機会と捉え、セキュリティ対策の提案や、検討の見直しの契機になるよう、有用な知識・知見を中小企業の経営者やシステム責任者に効果的に伝えるための準備をしておくことが重要です。特にセキュリティ対応の意思決定を担う経営者への理解を得るためには、経営者視点でセキュリティ対策の重要性を説明できるようにする必要があります。

2.2 責務を果たすための取組のプラクティス

（1）専門人材の確保と対応力を強化（サービス提案・提供力）

●組織内リソースの確保、外部リソースの活用

IPA が実施した地域 IT ベンダー向け調査では、地域 IT ベンダーは社内のセキュリティ専門人材の不足が課題となっています。これに対する自社の人的リソース確保策としては、「ISMS をベースとしたセキュリティ教育の実施」等のセキュリティ社内教育や、「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」等のセキュリティ資格の取得奨励の取組が行われています。この点 IPA の「中小企業の情報セキュリティ対策ガイドライン」や、「情報セキュリティマネジメント試験」の受験及び「情報処理安全確保支援士（登録セキスペ）」の資格取得・登録等、人材育成施策の活用が効果的です。

しかし、実際には「社内の人材育成に経済的・時間的な余裕がない」、「資格を取得すると給与が高いところに転職してしまう」等の問題があることも聞かれます。これに対しては、「顧客へ無料セキュリティ診断を提供し、セキュリティ技術者のノウハウを蓄積する」モチベーション向上や、「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」ビジネススキームの取組例があります。

一方、社内の人的リソースのみでは対応が難しい場合は、専門知識を有する外部リソースの活用を検討する必要があります。例えば、「脆弱性診断等、自社で対応できないものはセキュリティ専門ベンダーに外部委託する」、「専門資格を有する外部セキュリティ専門家の協力」等があげられます。この点 IPA では、情報処理安全確保支援士（登録セキスペ）でセキュリティ対策支援が実施できる専門家を「中小企業向けサイバーセキュリティ対策支援者リスト」として公開していますので、この中から自社のビジネスに合った専門家を探して依頼することも可能です。

（2）有用な知識・知見を効果的に伝える工夫（コミュニケーション力）

●経営者へのセキュリティ対策の説得

中小企業の顧客では、コスト制約や経営層のセキュリティ対策に対する理解不足から、なかなか対策導入が進まない状況があります。IPA が実施した地域 IT ベンダー向け調査では、「経営者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」等の声が聞かれました。セキュリティ対策は、顧客の情報システム部門や IT 担当だけで導入できるものではありません。企業内のセキュリティに対する意識喚起と財源確保が不可欠です。そのためには、これらの意思決定を担う経営者の理解を得ることが重要です。

経営者への理解を促すためには、専門用語を使わないことや、費用対効果の高い解決

策を提示するなど、うまく経営者の関心を引き出す必要があります。具体的には、「セキュリティ専門用語を使わず IT リテラシーが高くない人でも理解できるようなで言葉で説明する」、「顧客の対象事業に即した図表に書き換えて資料提供する」、「担当者から依頼があれば、経営層への説明に立ち会う」等の取組が行われています。顧客の担当者を情報面で支援しつつ、経営者の IT リテラシーや経営姿勢、IT 投資の判断基準等について理解しておくことが必要です。この点 IPA では、中小企業のセキュリティ対策事例として「サイバーセキュリティ対策に関する経営者インタビュー集」を公開していますので、こちらを顧客の経営層に紹介して、経営者視点でのセキュリティ対策の考え方について理解を深めてもらうことも効果的です。

●平時からのリスクコミュニケーション

IPA が実施した地域 IT ベンダー向け調査では、中小企業の顧客から地域 IT ベンダーへの過度な依存で、言わば丸投げに近い形でセキュリティ対策の対応が求められているケースがありました。これに対しては、システム開発・運用や製品・サービス提供時の契約で、顧客と IT ベンダー双方の責任範囲を明確化することが必要になりますが、セキュリティ対策はシステムや製品の提供側だけでは対応できないので、平時から顧客と IT ベンダー間のリスクコミュケーションが大切になります。すなわち、セキュリティインシデント発生時に顧客側で行うべき事業継続のための取組を明確にした上で、顧客の主体的な対応を促すことが重要となります。

具体的には、地域 IT ベンダーから「公開情報を活用したセキュリティリスクの指摘」、「顧客の類似事業で発生したインシデント事例の共有」、「顧客の従業員に対するセキュリティ教育への協力」等の取組が行われています。これらの取組を通じて、中小企業が自らセキュリティ対応を意識して実践する自律化の支援を行うことが必要です。この点 IPA では、中小企業を対象に実施した診断事業で作成した「中小企業のための実例で学ぶサイバーセキュリティリスク事例集」や、中小企業の情報セキュリティ対策ガイドラインの付録として「中小企業のためのセキュリティインシデント対応の手引き」を公開しており、これらを活用することが有効です。

また、IPA では情報セキュリティ関連を中心とした「中小企業支援セミナー」を全国の中小企業支援団体とともに開催しているので、こちらを中小企業の顧客へ紹介することも有効です。

（3）開発・運用時にセキュリティ機能をフォーカス（マネジメント力）

●運用保守契約に基づくセキュリティ対応

IPA が実施した地域 IT ベンダー向け調査では、中小企業の顧客へのサービスやシステムのセキュリティ対策の導入や保守において、契約上の問題が少なからず存在することが分かりました。特に運用保守契約の締結状況は、3 割以下と回答した地域 IT ベンダーが約 3 割で、運用・保守契約は締結していない地域 IT ベンダーも約 1 割強存在します。

また、運用保守契約を締結している場合でも、セキュリティ対応をどこまで包含する

か明確でないケースが見られました。これに対して、顧客へしっかりとした運用保守サービスを提供するために、SLA（Service Level Agreement）を定義した上で、運用保守契約締結している地域 IT ベンダーの取組もあり、顧客との間で責任範囲を明確にした対応が求められます。この点 IPA では、顧客と IT ベンダーがそれぞれ各開発段階で担うべき責務等の解説と契約書のひな型を示した「情報システム・モデル取引・契約書（第二版）」を公開しています。この中に、システム開発及びパッケージ利用等における運用保守についても解説しているので参考にすることができます。

●ソフトウェアの脆弱性管理

地域 IT ベンダーは、システム開発・運用や製品・サービス提供のそれぞれの場面でのセキュリティ対応力の強化が求められています。IPA が実施した地域 IT ベンダー向け調査では、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、約 5 割の地域 IT ベンダーが「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」、「ソフトウェア開発におけるセキュアな開発環境の整備」を実施しています。また、約 4 割の地域 IT ベンダーが「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」をあげています。この点 IPA では、ソフトウェア開発の計画から廃棄段階に至るまでのライフサイクル全体における脆弱性管理の内容・手順を取りまとめた「製品開発者向け脆弱性対策関連ガイド」を公開していますので、具体的な取組内容の確認ができます。

●脆弱性対応と注意喚起

地域 IT ベンダーは、セキュリティインシデントの発生抑止や、顧客の適切なリスク管理を支援するため、提供するシステムやサービスの脆弱性対応と注意喚起を行う必要があります。IPA が実施した地域 IT ベンダー向け調査では、5 割以上の地域 IT ベンダーが「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）の最新バージョンを提供」しており、「修正パッチのリモート対応により運用・保守を効率化しつつ脆弱性対応を行う」、「毎月のセキュリティ運用レポート提出時にインシデントに至らないケースも説明する」等の取組例もあります。

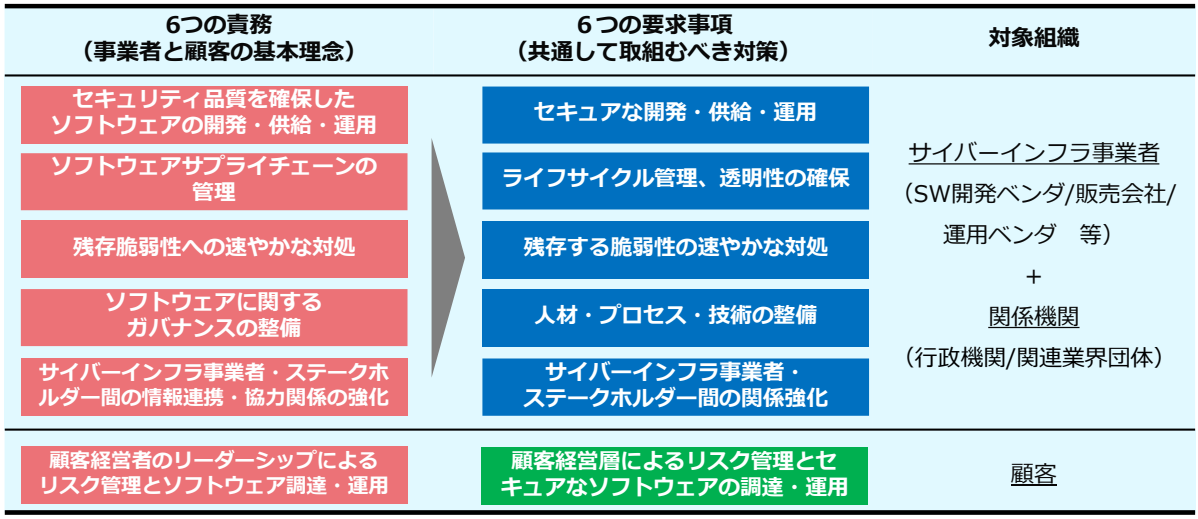
一方で、顧客側起因のインシデント発生に備えて今後対応を強化したいこととして、6 割以上の地域 IT ベンダーが「インシデントが疑われる兆候や実際の発生に早期に対処できる脆弱性対策や異常監視・対応」をあげており、「異常を検知してくれる AI をいれることで監視を自動化できる提案」を行っている取組もあります。この点 IPA では、中小企業に対するサイバー攻撃への対処として、24 時間の異常監視、緊急時の駆け付け支援等をワンパッケージにまとめた「サイバーセキュリティお助け隊サービス制度」を展開しています。同サービス制度の登録（参入）を希望する IT ベンダーは、サービス基準適合性審査を受けて適合性が認められるとサービス登録することができます。

また、万が一顧客でセキュリティインシデント等が発生した際は、IPA の「サイバーセキュリティ相談窓口（企業組織向け）」へ連絡することを勧めてください。

【コラム】
サイバーインフラ事業者に求められる役割等に関するガイドライン

経済産業省及び内閣官房国家サイバー統括室は、ソフトウェアの開発・供給・運用を行う「サイバーインフラ事業者」に求められる役割等について整理・解説し、当該事業者やその顧客がサイバーセキュリティ対策の実効性を確保するための参考となる考え方を示した「サイバーインフラ事業者に求められる役割等に関するガイドライン」を策定しました。当該ガイドラインは、サイバーインフラ事業者とその顧客を対象に、ソフトウェア・サプライチェーンのサイバーセキュリティに関するレジリエンス向上のために求められる責務と、責務を果たすための要求事項（具体的取組）について、6 つのカテゴリで整理しています。

また、ガイドラインの活用促進に向けた付属文書として評価チェックリスト等を整備しました。今後、サイバーインフラ事業者やその顧客等が当該ガイドライン及び評価チェックリスト等の活用を通じ、セキュリティ確保のために求められる役割を互いが認識しながら共に責務を果たすことにより、ソフトウェアのサプライチェーン全体でのサイバーセキュリティに関するレジリエンスの向上が期待されます。



https://www.meti.go.jp/press/2025/03/20260331001/20260331001.html

付録　中小企業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します（本手引き掲載順）。

中小企業の情報セキュリティ対策ガイドライン

中小企業の経営者や実務担当者が、情報セキュリティ対策の必要性を理解し、情報を安全に管理するための具体的な手順等を示したガイドラインです。（2026 年 3 月改訂　第 4.0 版）

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

情報セキュリティマネジメント試験

情報セキュリティマネジメントの計画・運用・評価・改善を通して組織の情報セキュリティ確保に貢献し、脅威から継続的に組織を守るための基本的なスキルを認定する試験です。（CBT 方式で年間を通じて随時実施）

https://www.ipa.go.jp/shiken/kubun/sg/about.html

情報処理安全確保支援士（登録セキスペ）

サイバーセキュリティ対策を推進する人材の国家資格で、サイバーセキュリティに関する相談に応じ、必要な情報の提供及び助言等を行い、セキュリティの確保を支援します。（試験合格後、登録が必要）

https://www.ipa.go.jp/jinzai/riss/index.html

中小企業向けサイバーセキュリティ対策支援者リスト

情報処理安全確保支援士（登録セキスペ）のうち、中小企業向けのサイバーセキュリティ対策支援が実施できる専門家の得意分野・専門領域を可視化したリストです。（指導テーマ等に即した専門家に直接連絡可能）

https://www.ipa.go.jp/security/sme/shien/list.html

サイバーセキュリティ対策に関する経営者インタビュー集

サイバーセキュリティ対策を実践している中小企業の経営者にインタビューを行い、自社のセキュリティ対策に関わる課題にどう向き合っているか、経営視点での取組みを中心に対応事例をまとめました。

https://www.ipa.go.jp/security/sme/jirei/index.html

中小企業のための実例で学ぶサイバーセキュリティリスク事例集

複数業界の中小企業を対象に ASM 診断とアンケート＆ヒアリング調査を行い、攻撃シナリオ・実施対策を事例としてまとめました。（ASM 診断：自社の IT 資産を把握し、攻撃されやすいポイントを特定する仕組み）

https://www.ipa.go.jp/security/reports/sme/rcu1hd0000009k82-att/sme-jirei.pdf

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

インシデント発生による被害とその影響範囲を最小限に抑え、迅速に復旧し、再発を防止することで、 企業の事業継続を確保するために必要となる対応について、「情報漏えいや改ざん」、「ウイルス感染」、「情報システムの機能停止」のそれぞれの場合を説明しています。

https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/sme_guideline_v4.0_app_8.pdf

中小企業支援セミナー

中小企業支援団体との連携のもと、中小企業等を対象とする情報セキュリティ関連を中心としたセミナーを全国で開催しています。（セミナー開催状況は案内ページを参照）

https://www.ipa.go.jp/security/seminar/sme/supportseminar.html

情報システム・モデル取引・契約書（第二版）

顧客とIT ベンダーが、それぞれ各開発段階で担うべき責務等の解説と契約書のひな型を提供するものです。この中に、システム開発及びパッケージ利用等における運用保守についても解説しています。

https://www.ipa.go.jp/digital/model/model20201222.html

製品開発者向け脆弱性対策関連ガイド

製品開発者が実施すべき、ソフトウェア開発の計画から廃棄段階に至るまでのライフサイクル全体における脆弱性管理の内容・手順を取りまとめたガイドラインです。

https://www.ipa.go.jp/security/guide/vuln/for_dev_user.html

サイバーセキュリティお助け隊サービス制度

中小企業に対するサイバー攻撃への対処として、24 時間の異常監視、緊急時の駆け付け支援、相談窓口の設置、簡易的サイバー保険などをワンパッケージにまとめた、民間の事業者から提供されるサービスです。基準を満たすサービスに、IPA が「お助け隊マーク」を付与し、普及の促進活動を行っています。

https://www.ipa.go.jp/security/sme/otasuketai/index.html

サイバーセキュリティ相談窓口（企業組織向け）

企業組織のセキュリティインシデントに関する相談や、ウイルス・不正アクセス・脆弱性情報に関する届出を受け付ける窓口です。セキュリティインシデント等が発生した際などに活用できます。

https://www.ipa.go.jp/security/support/soudan.html