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。（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～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４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 28 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. アカウント毎のアクセス制御
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 サイトのプラットオームやアプリケーションの改ざん検知
25. 定期的な Web サイトのプラットオ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ことが必要であると思われますか。（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。