2016 年度 中小企業における情報セキュリティ対策の実態調査票

独立行政法人情報処理推進機構

◎ 原則、**貴社の経営層（経営者、役員）の方**がご回答ください。
質問によっては、貴社の IT や情報セキュリティの担当者等、より詳しい方が回答して頂いても構いません。

◎ 独立行政法人情報処理推進機構（以下、IPA）では、**中小企業における情報セキュリティ対策への取り組みや被害の状況、対策実施における課題等を捉える**ことを目的としたアンケートを実施しております。今回の調査結果は、2017 年 3 月以降、IPA のホームページにて公開する予定です。ご回答の内容については、すべて統計数値として集計いたしますので、会社名や個人名、個別のご回答内容などが公表されることは一切ございません。

◎ 本調査は、IPA より委託を受け、みずほ情報総研株式会社が実施しております。なお、アンケート回答用のウェブページにつきましては、同社からの再委託のもと、楽天リサーチ株式会社が提供するアンケートシステムを利用いたします。

◎ 本調査の設問数は、IT 依存度、セキュリティ被害の有無などによって 30 問～最大 53 問となります。**IT をほとんど利用していないという企業も、今回の調査の対象となっております。**IT の依存度、セキュリティ対策、被害の実態を広く捉え、統計的に有意な結果を得るために、ご回答へのご協力を何卒よろしくお願い申し上げます。

◎ ご回答くださった方で、希望される方には、今回のアンケート調査における企業の回答傾向の中で、**業種内における貴社の状態や対策レベルの把握に役立つ資料**を電子メールにてお送りいたします。詳しくは Q30 をご覧ください。

◎ 本調査へのご回答には、以下の2種類の方法がございます。いずれか1つの方法でご回答ください。

方法１） 本調査票にご記入いただき、郵送にてご返送いただく

・お答えは、特に説明のないかぎり、あてはまる項目をお選びのうえ、該当する番号に○をご記入ください。
また、お答えが「その他」にあてはまる場合は、（ ）にその内容を具体的にご記入ください。
・お答えいただいた内容により、次にご回答いただく設問が変わる場合ありますので、調査票上の説明にご注意ください。
・ご記入いただいた用紙は、同封の返信用封筒（切手不要）に入れ、平成 28 年 11 月 18 日（金）までにご投函くださいますようお願い申し上げます。

方法２） アンケート回答用ウェブページにてご回答いただく

・楽天リサーチ株式会社の提供するアンケートシステムを用いて回答結果の収集を行います。このとき、貴社名と回答 ID の対応関係を楽天リサーチ株式会社は関知せず、ご回答いただいた内容を同社が利用することもございません。
・次の手順でご回答ください。（平成 28 年 11 月 18 日（金）まで）
① 本調査票に同封した「ご協力のお願い」に記載された回答 ID とパスワードをご用意ください。
（貴社専用の ID とパスワードになります）
② ウェブブラウザにて、「ご協力のお願い」に記載された URL にアクセスしてください。
③ ①で用意した ID とパスワードでログインし、表示される設問にご回答ください。

◎ 本調査についてご不明な点がございましたら、下記までお問合せください。

【調査主旨に関するお問合せ先】
独立行政法人情報処理推進機構
技術本部 セキュリティセンター
担当：江島、金子
電話：03-5978-7508
E-mail: isec-pr-nw@ipa.go.jp

【調査実施に関するお問合せ先】
みずほ情報総研株式会社
経営・IT コンサルティング部
担当：築島、冨田、小川
電話：03-5281-5283 FAX：03-5281-5429
E-mail: sec-survey@mizuho-ir.co.jp

I. 貴社の属性、あなたについてお伺いします。

問 1　貴社の主な業種をお答えください。（○は 1 つ）

1. 農業
2. 林業
3. 漁業
4. 鉱業, 採石業, 砂利採取業
5. 建設業
6. 製造業
7. 電気・ガス・熱供給・水道業
8. 情報通信業
9. 運輸業, 郵便業
10. 卸売業
11. 小売業
12. 金融業, 保険業
13. 不動産業, 物品賃貸業
14. 学術研究, 専門・技術サービス業
15. 宿泊業, 飲食サービス業
16. 生活関連サービス業, 娯楽業
17. 教育, 学習支援業
18. 医療, 福祉
19. 複合サービス事業
20. その他のサービス業

問 2　貴社の所在地をお答えください。（○は 1 つ）

1. 北海道
2. 青森県
3. 岩手県
4. 宮城県
5. 秋田県
6. 山形県
7. 福島県
8. 茨城県
9. 栃木県
10. 群馬県
11. 埼玉県
12. 千葉県
13. 東京都
14. 神奈川県
15. 新潟県
16. 富山県
17. 石川県
18. 福井県
19. 山梨県
20. 長野県
21. 岐阜県
22. 静岡県
23. 愛知県
24. 三重県
25. 滋賀県
26. 京都府
27. 大阪府
28. 兵庫県
29. 奈良県
30. 和歌山県
31. 鳥取県
32. 島根県
33. 岡山県
34. 広島県
35. 山口県
36. 徳島県
37. 香川県
38. 愛媛県
39. 高知県
40. 福岡県
41. 佐賀県
42. 長崎県
43. 熊本県
44. 大分県
45. 宮崎県
46. 鹿児島県
47. 沖縄県

問 3　あなたの主な役職・担当をお答えください。（○は 1 つ）

1. 経営者
2. 役員
3. IT または情報セキュリティ担当者
4. 一般社員（IT または情報セキュリティ担当者以外）

問 4　貴社の総従業員数について、2015 年度（2015 年 4 月～2016 年 3 月）の人数をお答えください。（○は 1 つ）

※常時従業者の総数。有給役員及び常時雇用者（正社員・正職員、準社員・準職員、アルバイト等、1 ヶ月を超える雇用契約者）とし、人材派遣業者からの派遣従業者は含めません。

1. 5 名以下
2. 6～20 名
3. 21～50 名
4. 51 名～100 名
5. 101 名～300 名
6. 301 名以上

問 5　貴社の資本金について、直近会計年度の金額をお答えください。（○は 1 つ）

1. 5000 万円以下
2. 5000 万円超～1 億円以下
3. 1 億円超～2 億円以下
4. 2 億円超～3 億円以下
5. 3 億円超

問 6　貴社の総売上高（単体）について、2015 年度（2015 年 4 月～2016 年 3 月）の金額をお答えください。
※決算期が 3 月でない場合、決算期に合わせた回答で構いません。
※学校、組合団体など営業活動を行わない組織の場合は、当該年度における収入高とします。

千億	百億	十億	億	千万	百万

百万円

II.　貴社の IT の導入状況についてお伺いします。

Q1　貴社において、業務で PC を利用していますか。利用している場合は、台数をご記入ください。なお、シンクライアント端末（用語集：No.1）を導入している場合は、その端末も含めてカウントしてください。

1.　利用している ⇒　約【　　】台　　2.　利用していない

Q1-1　Q1 で「1 利用している」と回答された方にお尋ねします。
貴社では、Windows Update などによるパソコンへのセキュリティパッチ（ぜい弱性の修正（用語集：No.2））の適用をどのようにされていますか。最も近いものをお答えください。（○は 1 つ）

1.　常に適用し、適用状況も把握している
2.　常に適用する方針・設定だが、実際の適用状況は不明
3.　各ユーザに適用を任せている
4.　ほとんど適用していない
5.　わからない

Q2　貴社において、業務でタブレット端末及びスマートフォンを利用していますか。利用している場合は、台数をご記入ください。

1.　利用している ⇒　約【　　】台　　2.　利用していない

Q2-1　Q2 で「1 利用している」と回答された方にお尋ねします。業務で利用されているスマートフォンやタブレット端末について、以下のうち実施されている対策をお答えください。（いくつでも）

1.　端末のパスワード設定
2.　紛失・盗難時のデータ消去
3.　セキュリティソフトの導入
4.　MDM（モバイルデバイス管理ツール）による端末管理
5.　利用ルールの策定（アプリケーションの導入制限等）
6.　その他　（具体的に：【　　】）
7.　特に実施していない

Q2-2　業務で利用するスマートフォンやタブレット端末について、社員の私有端末の業務利用（BYOD: Bring Your Own Device）を認めていますか。（○は 1 つ）

1.　認めている
2.　現在、認めるかどうかを検討中
3.　未検討
4.　認める予定はない

Q3　貴社において、業務でサーバを利用していますか。利用している場合は、台数をご記入ください。なお、クラウドコンピューティングサービス（用語集：No.3））として利用しているサーバは台数に加えないでください。

1.　利用している ⇒　約【　　】台　　2.　利用していない

Q3-1 Q3 で「1 利用している」と回答された方にお尋ねします。貴社ではサーバにセキュリティパッチ（ぜい弱性の修正（用語集：No.2））を適用していますか。最も近いものをお答えください。（a,b それぞれ○は1つ）

a) 外部に公開しているネットワークサーバ（メールサーバ、Web サーバなど）

1. ほぼ全サーバに適用している
2. アプリケーションに影響がないことを確認できたもののみを適用している
3. 情報セキュリティ対策上重要なもののみを適用している
4. ほとんど適用していない
5. 外部事業者に運用を委託しているので、自ら適用する必要がない
6. 該当するようなサーバを利用していない
7. わからない

b) 内部で利用しているローカルサーバ（ファイルサーバ、プリントサーバなど）

1. ほぼ全サーバに適用している
2. アプリケーションに影響がないことを確認できたもののみを適用している
3. 情報セキュリティ対策上重要なもののみを適用している
4. ほとんど適用していない
5. 外部事業者に運用を委託しているので、自ら適用する必要がない
6. 該当するようなサーバを利用していない
7. わからない

Q3-2 Q3-1 で「4 ほとんど適用していない」と回答した方にお尋ねします。
セキュリティパッチを適用しない理由として、当てはまるものをお答えください。（いくつでも）

1. パッチの適用が悪影響を及ぼすリスクを避けるため
2. パッチ適用以外の手段が有効であるため
3. パッチを適用しなくても問題ないと判断したため
4. パッチの評価や適用に多大なコストがかかるため
5. その他 （具体的に：【 】）

Q4 貴社のパソコン・タブレット・サーバなどで電子データとして保有している情報はありますか？あてはまるものを全てお答えください。（いくつでも）

1. 自社の顧客の個人情報 ⇒（個人情報の件数：【 】件）
2. 従業員の個人情報 ⇒（個人情報の件数：【 】件）
3. 自社の業務上の機密情報
4. 取引先等（親会社を除く）から預かっている個人情報 ⇒（個人情報の件数：【 】件）
5. 取引先等（親会社を除く）から預かっている業務上の機密情報
6. 親会社から預かっている個人情報 ⇒（個人情報の件数：【 】件）
7. 親会社から預かっている業務上の機密情報
8. 上記いずれも電子データでは保有していない
9. わからない

Q5　貴社では IT 分野の投資を過去 3 年間の間に行いましたか。（○は 1 つ）

1. 行った　　2. 行っていない　　3. わからない

Q5-1 Q5 で「1　行った」と回答された方にお尋ねします。（以下、Q5-2 まで同じ）。

IT 投資額は、概算でどのくらいですか。（○は 1 つ）

1. 1 百万円未満　　2. 1 百万円～5 百万円未満　　3. 5 百万円～1 千万円未満
4. 1 千万円～2 千万円未満　　5. 2 千万円～5 千万円未満　　6. 5 千万円～1 億円未満
7. 1 億円～4 億円未満　　8. 4 億円以上　　9. わからない

Q5-2 その IT 投資の中に情報セキュリティ対策は含まれていましたか。（○は 1 つ）

1. 含まれている　　2. 含まれていない　　3. わからない

Q5-3 Q5-2 で「1　含まれている」と回答された方にお尋ねします。

情報セキュリティ対策に関する投資額は概算でどのくらいですか。（○は 1 つ）

1. 1 百万円未満　　2. 1 百万円～5 百万円未満　　3. 5 百万円～1 千万円未満
4. 1 千万円～2 千万円未満　　5. 2 千万円～5 千万円未満　　6. 5 千万円～1 億円未満
7. 1 億円～4 億円未満　　8. 4 億円以上　　9. わからない

Q5-4 Q5-2 で「2　含まれていない」と回答された方にお尋ねします。含まれていない理由は何ですか。

1. コストがかかり過ぎる　　2. 費用対効果が見えない　　3. どこからどう始めたらよいかわからない
4. 導入後の手間がかかる　　5. その他（具体的に：【　　】）

Q6　貴社の下記項目における状況について、それぞれお答えください。（それぞれ○は 1 つ）

a) IT を十分に活用していると思いますか

1. そう思う　　2. ややそう思う　　3. あまりそう思わない
4. 思わない　　5. わからない

b) 社員の不正により営業上の秘密や個人情報等の情報漏えいが発生する可能性はあると思いますか

1. そう思う　　2. ややそう思う　　3. あまりそう思わない
4. 思わない　　5. わからない

c) 外部からサイバー攻撃を受け、情報漏えいが発生する可能性はあると思いますか

1. そう思う　　2. ややそう思う　　3. あまりそう思わない
4. 思わない　　5. わからない

d) 貴社の情報セキュリティへの理解度は高いと思いますか

1. そう思う　　2. ややそう思う　　3. あまりそう思わない
4. 思わない　　5. わからない

Q7 貴社では経営資源の確保や業務の効率化に IT を活用されていますか。利用・導入されているサービスやシステムを次の項目から選択してください。(いくつでも)

1. フリーメール(Gmail,hotmail など)
2. 顧客管理システム（CRM）
3. Web サイト、ホームページの開設
4. インターネットを活用した流通・決済（例：ネット販売等）
5. 会計システム・アプリケーション
6. 人事システム・アプリケーション
7. 給与システム・アプリケーション
8. 出退勤管理システム
9. 稟議システム
10. 文書管理システム
11. 生産管理システム
12. コミュニケーションツール
13. クラウドストレージ・無料
14. クラウドストレージ・有料
15. クラウドファンディング
16. クラウドソーシング
17. その他　（具体的に：【　　】）
18. 活用していない

Q8 貴社はサイバー保険（サイバー攻撃の被害にあったときの補償に特化した保険）や情報漏えい賠償責任保険（商工会議所保険制度）に加入されていますか。(a,b それぞれ○は1つ)

a) サイバー保険

1. 加入している
2. 検討しているが加入していない
3. 内容を知っているが加入する予定がない
4. 内容を知らないし加入していない
5. 加入しているかどうかわからない

b) 情報漏えい賠償責任保険

1. 加入している
2. 検討しているが加入していない
3. 内容を知っているが加入する予定がない
4. 内容を知らないし加入していない
5. 加入しているかどうかわからない

III. 貴社の情報セキュリティに関する意識・状況についてお伺いします。

Q9 貴社の情報セキュリティ対策はどのような体制で行われていますか。(○は1つ)

1. 専門部署（担当者）がある
2. 兼務だが担当者が任命されている
3. 組織的には行っていない（各自の対応）
4. わからない

Q10 情報セキュリティに関して困ったことがあった際にどこに相談しますか。(いくつでも)

1. 社内の担当者
2. IT 関連業者
3. 中小企業診断士
4. IT コーディネータ
5. 商工会議所・商工会・中小企業団体中央会
6. 情報処理推進機構（IPA）
7. その他 （具体的に：【　　】）
8. 特にない

Q11 貴社の情報セキュリティに関する情報収集先を教えてください。(いくつでも)

1. 社内の担当者
2. IT 関連業者
3. 中小企業診断士
4. IT コーディネータ
5. 商工会議所・商工会・中小企業団体中央会
6. 情報処理推進機構(IPA)
7. 新聞・雑誌
8. テレビ
9. インターネット
10. 無料のセミナー・実務研修
11. 有料のセミナー・実務研修
12. その他(具体的に:【 】)
13. 特にない

Q12 貴社へ情報セキュリティ対策の専門家を派遣する制度があれば利用してみたいですか。(○は 1 つ)

1. 既に似たようなサービス・制度を利用している
2. 有償無償に関わらず、機会があれば利用したい
3. 有償でも補助金等で経費負担が軽減されるのであれば利用したい
4. 無償であれば利用したい
5. 利用したいと思わない

Q13 貴社では従業員に対する情報セキュリティ教育はどのようにされていますか。(いくつでも)

1. 関連情報の周知 (社内メール・回覧・掲示板など)
2. e ラーニング (用語集 : No.4)
3. 外部講習会やセミナーの聴講
4. 社内の研修や勉強会
5. 特に実施していない

Q14 貴社において、情報漏えい等のインシデント又はその兆候を発見した場合、対応方法は規定されていますか。(○は 1 つ)

1. 規定されている
2. 規定されていない
3. 規定されているかわからない

→ Q14-1 Q14 で「1. 規定されている」と回答された方にお尋ねします。
情報漏えい等のインシデント又はその兆候を発見した場合の対応方法として規定されているものは何ですか。該当するものを下記よりすべてお選びください。(いくつでも)

1. 経営者への報告
2. 責任者への報告
3. 原因究明
4. 本人、関係者への連絡
5. 官公庁への報告
6. 再発防止策の策定
7. 世間への発表
8. その他 (具体的に:【 】)

Q15 社内の情報セキュリティに関するルールから逸脱した場合の措置について、就業規則等で規定されていますか。(○は 1 つ)

1. 規定されている
2. 規定されていない
3. 規定されているかわからない
4. そもそも就業規則はない

Q16 貴社では情報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。実施している対策をお答えください。（いくつでも）

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. 情報セキュリティマネジメントシステム（ISMS）の認証取得
4. プライバシーマーク（P マーク）の取得
5. セキュリティポリシー（セキュリティの規程やルール）が文章化されている
6. 一般ユーザアカウントの管理ルールの策定（パスワードの設定ルール等）
7. Web サイト管理者権限アカウントの管理ルールの策定
8. IT 資産構成や設定の文書化
9. フロアや施設への入退出管理
10. 情報（書類などの紙媒体）の施錠管理
11. セキュリティワイヤー等による機器の固定
12. 外部送信ファイルへのパスワード設定
13. 機器や記録媒体の持込み・持出しの制限
14. アカウント毎のアクセス制御
15. 一般ユーザのプログラムインストールの制限（exe ファイルの実行禁止等）
16. 重要なシステム・データのバックアップ
17. ハードディスク等の廃棄時の破砕／溶融
18. セキュリティ監視サービスの活用
19. ログやファイル情報に基づく Web コンテンツの改ざん検知
20. 定期的な Web コンテンツのセキュリティ診断サービス（ぜい弱性調査）の活用
21. 情報セキュリティ監査（内部監査）の実施
22. 情報セキュリティ監査（外部監査）の実施
23. 情報セキュリティ対策の定期的な見直し
24. 委託先の情報セキュリティ対策、体制、実施状況などの確認
25. （内容に応じて）委託先とＮＤＡ（機密保持契約）の締結
26. クラウドサービス利用のための情報セキュリティマネジメントガイドライン（経済産業省ガイドライン）の活用
27. 情報セキュリティ管理基準（経済産業省告示）の活用
28. SSL/TLS 暗号設定ガイドライン（IPA のガイドライン）の活用
29. 組織における内部不正防止ガイドライン（IPA のガイドライン）の活用
30. 中小企業における組織的な情報セキュリティ対策ガイドライン（IPA のガイドライン）の活用
31. その他　（具体的に：【　　】）
32. 特に実施していない

Q16-1 Q16 で「5. セキュリティポリシー（セキュリティの規程やルール）の文章化」を選択された方にお尋ねします。
セキュリティポリシーで規定されているものは何ですか。該当するものを下記よりすべてお選びください。（いくつでも）

1. 基本規程（基本方針）
2. 詳細規則（対策基準、実施手順・運用規則等）
3. 責任者の任命
4. 従業員又は部署ごとの情報取扱に関する役割明確化
5. アクセス権限明確化
6. 情報資産の識別、重要度の分類
7. 守秘義務
8. 機器、メール、インターネットアクセスの私的利用制限
9. 機器等の取扱、破損、紛失に留意する項目
10. 紛失した場合などの届け出義務
11. 著作権侵害
12. その他　（具体的に：【　　】）
13. 特にはない

Q16-2 Q16 で「24. 委託先の情報セキュリティ対策、体制、実施状況などの確認」を選択された方にお尋ねします。
契約において、委託先に対し情報セキュリティ対策等で規定されているものは何ですか。該当するものを下記よりすべてお選びください。（いくつでも）

1. 情報セキュリティを確保するための体制の整備
2. 取り扱う情報の秘密保持等
3. セキュリティ機能の装備
4. 運用・保守・点検における情報セキュリティ対策の実施
5. ぜい弱性対策の実施
6. 外部委託する業務以外の情報資産の保全
7. 情報セキュリティ対策のサービスレベルに関する事項
8. 情報セキュリティが侵害された場合の対処
9. 情報セキュリティ対策の履行状況の確認
10. 情報セキュリティ監査の実施
11. 情報セキュリティ対策の履行が不十分であると思われる場合の対処
12. 確認書等に委任する事項
13. 再委託に関する事項
14. その他　（具体的に：【　　】）
15. 特にはない

Q17 貴社では情報セキュリティ関連製品やサービスを導入していますか。導入しているものをお答えください。（いくつでも）

1. ウイルス対策ソフト・サービスの導入
2. ウェブ閲覧のフィルタリングソフトウェア
3. ファイアウォール
4. VPN （用語集:No.5）
5. 暗号化製品（ディスク、ファイル、メール等）
6. ソフトウェアライセンス管理/IT 資産管理製品
7. ワンタイムパスワード、IC カード、USB キー、生体認証等による個人認証
8. アイデンティティ管理／ログオン管理／アクセス許可製品（SSO（用語集：No.6）を含む）
9. セキュリティ情報管理システム製品（ログ情報の統合・分析、システムのセキュリティ状態の総合的な管理機能）
10. クライアント PC の設定・動作・ネットワーク接続等を管理する製品（検疫ネットワーク（用語集：No.7）を含む）
11. メールフィルタリングソフトウェア（誤送信防止対策製品、スパムメール対策製品を含む）
12. その他 （具体的に：【 】）
13. 特に導入しているものはない

Q18 情報セキュリティ業務の外部委託（システム子会社への委託を含む）の状況について、もっともあてはまるものをお答えください。（○は 1 つ）

1. ほぼ全てを委託している （情報セキュリティ業務だけでなく、システムの委託も含めて）
2. ほぼ全てを委託している （情報セキュリティ業務のみ）
3. 一部委託している
4. 委託していない
5. わからない

→ Q18-1 Q18 で「3 一部委託している」と回答した方にお尋ねします。
委託している内容として、当てはまるものをお答えください。（いくつでも）

1. セキュリティ/BCP コンサルティングサービス （ISMS やプライバシーマークの取得など含む）
2. CSIRT（用語集:No.8）構築支援サービス
3. セキュリティ検査・監査サービス
4. Web アプリケーションぜい弱性検査サービス
5. ウイルス監視サービス
6. ファイアウォール運用管理サービス
7. 不正アクセス監視サービス
8. 統合セキュリティ監視サービス
9. DDoS（用語集:No.9）攻撃対策サービス
10. メールセキュリティサービス
11. イベントログ管理サービス
12. セキュリティ教育・トレーニングサービス
13. メール標的型攻撃訓練サービス
14. セキュアファイル交換サービス
15. 電子認証サービス
16. その他 （具体的に:【 】）

Q19 情報セキュリティ対策の実施内容（プライバシーポリシーや業務情報の取り扱い基準等）を外部に公開していますか。もっともあてはまるものをお答えください。（○は1つ）

1. ホームページで公開している
2. 取引先からの要望があれば個別に提示している
3. 公開していない
4. わからない

Q20 情報セキュリティ対策の必要性を感じたきっかけは何ですか。該当するものを下記よりすべてお選びください。（いくつでも）

1. 法令（個人情報保護法等）の制定
2. 業界基準の制定、業界団体の呼びかけ
3. 取引先からの要請
4. 自社社員からの要請
5. 自社のセキュリティ事故
6. 他社のセキュリティ事故（ニュースを含む）
7. 対外（取引先、ユーザ等）へのアピール
8. セキュリティベンダーからの勧奨
9. 同業他社の対策状況をみたこと
10. マイナンバー制度の開始
11. IT 関連業者・専門家（商工会議所・商工会・中小企業団体中央会等）の勧奨
12. 重要情報（個人情報、営業秘密、技術情報等）の保持
13. その他 （具体的に：【 】）
14. 対策の必要性を感じたことがない

Q21 以下の情報セキュリティに関する事象に対して、どの程度脅威と感じていますか。（それぞれ○は1つ）

a) コンピュータウイルス （用語集：No.10）

1. 非常に大きな脅威である　2. どちらかといえば脅威である　3. あまり脅威ではない

b) 不正アクセス （用語集：No.11）

1. 非常に大きな脅威である　2. どちらかといえば脅威である　3. あまり脅威ではない

c) DoS 攻撃 （用語集：No.9）

1. 非常に大きな脅威である　2. どちらかといえば脅威である　3. あまり脅威ではない

d) 標的型攻撃 （用語集：No.12）

1. 非常に大きな脅威である　2. どちらかといえば脅威である　3. あまり脅威ではない

e) 情報漏えい

1. 非常に大きな脅威である　2. どちらかといえば脅威である　3. あまり脅威ではない

f) 内部犯行（内部不正）

1. 非常に大きな脅威である　2. どちらかといえば脅威である　3. あまり脅威ではない

g) システム機能不全

1. 非常に大きな脅威である　2. どちらかといえば脅威である　3. あまり脅威ではない

h) 外部委託先のサービス停止

1. 非常に大きな脅威である　2. どちらかといえば脅威である　3. あまり脅威ではない

Q22 前問の脅威に対して実施している対策は十分だと感じますか。（それぞれ〇は1つ）

a) コンピュータウイルス （用語集:No.10）

1. 十分と感じる　2. どちらかと言えば十分と感じる　3. 十分と感じない

b) 不正アクセス （用語集:No.11）

1. 十分と感じる　2. どちらかと言えば十分と感じる　3. 十分と感じない

c) DoS 攻撃 （用語集:No.9）

1. 十分と感じる　4. どちらかと言えば十分と感じる　5. 十分と感じない

d) 標的型攻撃 （用語集:No.12）

1. 十分と感じる　6. どちらかと言えば十分と感じる　7. 十分と感じない

e) 情報漏えい

1. 十分と感じる　8. どちらかと言えば十分と感じる　9. 十分と感じない

f) 内部犯行（内部不正）

1. 十分と感じる　10. どちらかと言えば十分と感じる　11. 十分と感じない

g) システム機能不全

1. 十分と感じる　12. どちらかと言えば十分と感じる　13. 十分と感じない

h) 外部委託先のサービス停止

1. 十分と感じる　14. どちらかと言えば十分と感じる　15. 十分と感じない

Q23 貴社の情報セキュリティ対策は十分だと思いますか

1. そう思う　2. ややそう思う　3. あまりそう思わない
4. 思わない　5. わからない

Q24 貴社の情報セキュリティ対策を、更に向上させるために必要と思われることをお選びください。（いくつでも）

1. 経営者への情報セキュリティ意識向上
2. 経営者への情報セキュリティ対策方法の教育
3. 従業員の情報セキュリティ意識向上
4. 従業員への情報セキュリティ対策実践教育
5. 市場や顧客からの信頼・評価
6. 企業内の体制整備
7. 情報セキュリティ関連法制度の整備
8. 対策支援費等の補助制度の充実
9. 情報セキュリティ対策技術の習得・向上、対策ツールの利用・啓発
10. 地域での支援者育成や確保、サポートセンターの充実
11. その他 （具体的に：【　　】）
12. 特にはない

IV. 貴社の情報セキュリティ被害についてお伺いします。

Q25 貴社では、2015 年度 1 年間(2015 年 4 月～2016 年 3 月)に、**コンピュータウイルス**(用語集:No.10)に感染したことがありましたか。一度でもあればお答えください。(○は1つ)

1. ウイルスに感染した	2. ウイルスを発見したが、感染には至らなかった

3. ウイルスをまったく発見しなかった・感染していない　4. わからない

Q25-1 Q25 で「1. ウイルスに感染した」もしくは「2 ウイルスを発見したが、感染には至らなかった」と回答された方にお尋ねします。

感染あるいは発見したコンピュータウイルスの侵入経路はどのように想定されますか。(いくつでも)

1. 電子メール
2. インターネット接続 (ホームページ閲覧など)
3. 自らダウンロードしたファイル
4. P2P(Peer to Peer)などのファイル共有ソフト
5. USB メモリ等の外部記憶媒体
6. 持ち込みパソコン
7. その他 (具体的に:【　　】)
8. わからない

Q25-2 Q25 で「1. ウイルスに感染した」と回答された方にお尋ねします。

ウイルスに感染した影響で生じた被害としてあてはまるものをお答えください。(いくつでも)

1. データの破壊
2. 個人情報の漏えい
3. 業務情報(営業秘密を除く)の漏えい
4. 営業秘密の漏えい
5. ウイルスメール等の発信
6. ネットワークの遅延
7. システム停止・性能低下
8. パソコン単体の停止
9. 関連部門の業務停滞
10. 個人の業務停滞
11. 取引先への感染拡大
12. その他 (具体的に:【　　】)
13. 特になし

Q26 貴社では、2015 年度 1 年間(2015 年 4 月～2016 年 3 月)に、内部者(委託者を含む)の不正に起因する情報漏えいやシステムの悪用等の情報セキュリティ上のトラブルがありましたか。一度でもあればお答えください。(○は1つ)

1. 内部者の不正による被害があった
2. 委託者の不正による被害があった
3. 内部者(委託者を含む)の不正による被害はなかった
4. わからない

Q27 貴社では、2015 年度 1 年間(2015 年 4 月～2016 年 3 月)に、自社のサーバやパソコンがサイバー攻撃(DoS 攻撃(用語集:No.9)、**不正アクセス**(用語集:No.11)、**標的型攻撃**(用語集:No.12)など)にあったことがありましたか。一度でもあればお答えください。(○は1つ)

1. サイバー攻撃で被害にあった	2. サイバー攻撃を受けたが、被害には至らなかった

3. サイバー攻撃をまったく受けなかった　4. わからない

Q27-1 Q27 で「1. サイバー攻撃で被害にあった」もしくは「2 サイバー攻撃を受けたが、被害には至らなかった」と回答された方にお尋ねします。

貴社が受けたサイバー攻撃の手口にあてはまるものをお答えください。（いくつでも）

1. ID・パスワードを騙し取られてユーザになりすまされたことによる不正アクセス
2. ぜい弱性（セキュリティパッチの未適用）を突かれたことによる不正アクセス
3. SQL インジェクション （用語集：No.13）
4. DoS 攻撃 （用語集：No.9）
5. 標的型攻撃 （用語集：No.12）
6. ランサムウェア （用語集：No.14）
7. その他 （具体的に：【 】）
8. 手口はわからない

Q27-2 Q27 で「1. サイバー攻撃で被害にあった」と回答された方にお尋ねします。

貴社が受けたサイバー攻撃の被害としてあてはまるものをお答えください。（いくつでも）

1. 貴社の Web サイトが改ざんされた
2. 貴社の Web サイトのサービスが停止、または機能が低下させられた
3. 業務サーバの内容が改ざんされた
4. 業務サーバのサービスが停止、または機能が低下させられた
5. 貴社が提供するネットサービスにおいて、第三者のなりすましによる不正使用があった
6. 取引先の企業や個人に被害が拡大した
7. 個人情報が盗まれた
8. 業務情報(営業秘密を除く)が盗まれた
9. 営業秘密が盗まれた
10. その他 （具体的に：【 】）

V. ヒアリングへのご協力について

Q28 独立行政法人情報処理推進機構（IPA）をご存知ですか？

1. はい
2. いいえ

Q29 独立行政法人情報処理推進機構（IPA）の活動について認識のあるものをご選択ください。（いくつでも）

1. 情報処理技術者試験 （IT パスポート等）
2. 情報セキュリティに関する注意喚起
3. ぜい弱性対策情報収集ツール MyJVN
4. 映像で知る情報セキュリティ
5. 情報セキュリティ関連対策資料 （10 大脅威、対策のしおり）
6. サイバー情報共有イニシアティブ（J-CSIP（ジェイシップ））、サイバーレスキュー隊（J-CRAT）
7. ここからセキュリティ！ 情報セキュリティ・ポータルサイト
8. 中小企業向け講習能力養成セミナー
9. 情報セキュリティ対策支援サイト iSupport
10. インターネット安全教室
11. 情報セキュリティ安心相談窓口
12. セキュリティ・キャンプ
13. スキル標準（IT 人材育成）
14. ソフトウェア高信頼化
15. その他 （具体的に：【 】）

Q30　**独立行政法人情報処理推進機構（IPA）では、中小企業における情報セキュリティに対する意識啓発及び必要な情報セキュリティ対策の推進を目的とした活動を行っています。その活動の一環として、貴社の情報セキュリティ対策や情報セキュリティに関する悩み事等について、IPA からヒアリングをお願いした場合、ご協力いただくことは可能ですか。（○は1つ）**

1　協力してもかまわない　　2　協力はできない

※「1 協力してもかまわない」を選択された方で、2017 年 2 月までにヒアリングをお引き受け頂ける場合、**IPA が提供しているツールによる対策状況の診断や IT・セキュリティ有識者へのお悩み相談等**を無料にて実施致します。

次ページの「個人情報のお取り扱いについて」にご同意の上、差し支えない範囲でご記入をお願いいたします。

貴社・貴事業所名	
所属部署・役職	
お名前	
ご住所	
電話番号	
E-mail アドレス	
詳細結果希望	1　希望する　　2　希望しない

※ご回答くださった方には、独立行政法人情報処理推進機構（IPA）サイトにおける調査結果の公表を電子メールにてご案内させていただきます。また、上記「詳細結果希望」に「1　希望する」に○をつけた方には、今回のアンケート調査における企業の回答傾向の中で、業種内における貴社の状態や対策レベルの把握に役立つ資料を**電子メールにて**お送りいたします。

ご協力ありがとうございました

【用語集：調査票で使われる用語の解説】

No.	用語	内容
1	シンクライアント	ユーザが使用する端末の機能は必要最小限にとどめ、サーバ側で処理を行う仕組み。物理的に端末側のハードディスクドライブや CD-ROM などの入出力装置を外し、情報漏えい対策の 1 つとして利用されている。
2	セキュリティパッチ	ソフトウェアにセキュリティ上のぜい弱性(セキュリティホール)が発覚した時に配布される修正プログラム。
3	クラウドコンピューティング	従来は手元のコンピュータで管理・利用していたようなソフトウェアやデータなどを、インターネットなどのネットワークを通じてサービスの形で必要に応じて利用する方式。
4	e ラーニング	インターネットを利用した学習形態。パソコンやコンピュータネットワークなどを利用して教育を行う。
5	VPN	あたかも自社ネットワーク内部の通信のように、自宅や外出先などの遠隔地の拠点から安全に社内 LAN にアクセスが行える技術のこと。
6	SSO（シングルサインオン）	それぞれ別々に ID とパスワードなどの認証を要求する複数のシステムを、1 回の認証手続きで利用できるようにするためのサービス。
7	検疫ネットワーク	社内ネットワークに接続しようとするパソコンを、いったん社内ネットワークとは隔離された検査専用のネットワークに接続してパソコンの検査を行い、問題がないことを確認してから社内ネットワークへの接続を許可する仕組み。
8	CSIRT	Computer Security Incident Response Team の略。サイバー攻撃による情報漏えいや障害など、コンピュータセキュリティ上の問題に繋がる事象が発生した際に対応する組織。
9	DoS 攻撃、DDoS 攻撃	DoS 攻撃は、通信ネットワークを通じてコンピュータや通信機器などに行われる攻撃手法の一つで、大量のデータや不正なデータを送りつけて相手方のシステムを正常に稼働できない状態に追い込むこと。また、インターネットに繋がる多数の機器から一斉にデータを送信して標的を機能不全に陥らせる方式を DDoS 攻撃という。
10	コンピュータウイルス	第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムであり、感染によりコンピュータが予期しない動作を起こし、使用不能や情報漏えいを引き起こす。
11	不正アクセス	以下に示すような行為のこと。 • コンピュータの OS やアプリケーションあるいはハードウェアに存在するぜい弱性を利用して、コンピュータ内に侵入する行為(侵入行為) • 他の人に与えられた、利用者 ID およびパスワードを、その持ち主の許可を得ずに利用して、持ち主に提供されるべきサービスを受ける行為(なりすまし行為) • 持ち主の許可を得ずに、その持ち主の利用者 ID およびパスワードを第三者に提供する行為
12	標的型攻撃	メールの添付ファイルやウェブサイトを利用してパソコンにウイルスを感染させ、そのパソコンを遠隔操作して特定の組織や企業の重要情報を窃取する手法。典型的な例として、メール受信者の仕事に関係しそうな偽の話題等を含む本文や件名で騙し、添付ファイル（ウイルス等）のクリックを促す手口が知られている。
13	SQL インジェクション	Web サイトの入力欄に細工（特別な意味を持つ記号文字）を埋め込み、データベースを不正に操作する手法。
14	ランサムウェア	コンピュータウイルスの一種で、感染した PC をロックしたり、ファイルを暗号化したりすることによって使用不能にしたのち、元に戻すことと引き換えに「身代金」を要求する不正プログラムのこと。 ランサムは身代金のことで、身代金要求型不正プログラムとも呼ばれる。