

## 付録 C. ヒアリング調査シート

## 【中小企業における情報セキュリティ対策の実施状況等調査ヒアリングシート】

事前に組織的な対策ガイドライン、自社診断シートを送った上で、ヒアリングで詳細に聞き取る。

- ・このヒアリング時の重要な聞き取りポイントは以下の3点。
  - 1.情報セキュリティの企業としての実態と考え方
  - 2.情報セキュリティガイドラインの妥当性や気づきの確認、評価
  - 3.情報セキュリティの緊喫の課題、問題点
- ・自社診断シートは事前にFAXで回収し、未実施項目、点数を確認しておく。
- ・組織的な対策ガイドラインを事前に送ることで、実際に自社の情報セキュリティの実態に合致しているか？またはこのガイドラインをもとに情報セキュリティ対策を実施（検討）してみた時の、違和感や充足度合を確認する。
- ・ガイドライン付録のチェックシートも記入してもらい、それをもとに詳細なヒアリングを行う。
- ・ヒアリングとは別に、社内の様子で気づいた点についてもチェックしていく。
- ・ヒアリングシートについては取材先に開示は行わず、取材後の項目整理、まとめとして活用する。
- ・ヒアリング実施に際して、会社概要についても聞き取りを行う。（資本関係など）

### Q1)情報セキュリティに対する組織的な取り組み状況

Q1-1：情報セキュリティに関する経営者、企業としての情報セキュリティに対する重要性の認識

- ・ガイドラインのセキュリティポリシーを明確化（実施していない理由、実施している理由）（5分のできる自社診断シート70点以上の企業に対して）
- ・情報セキュリティの考え方、経営、企業としての方針の現状とその理由

Q1-2：情報セキュリティ実施状況把握のための施策を行っているか？

- ・5分のできる自社診断シートの項目のうち、No1～20のテクニカルな項目については、（個別ではなく）全体的に確認した事があるか。あれば、その方法。無ければ、その理由

Q1-3：従業者（派遣を含む）に対してセキュリティに関して就業上何をしなければいけないか情報セキュリティルールの周知徹底を行なっているか？またそのための教育、指導、知識習得の機会を与えているか？

セキュリティ周知の方法（朝礼、回覧、会議等、外部研修、定期研修、実施していない）  
適応範囲（正社員、派遣、アルバイト、その他、実施していない）  
社内ルール（明確化している、規定作成が大変なので行わない、明確化するほど検討時間がない、文書化するほど対策実施を求めている、その他）

- ・5分のできる自社診断シートの項目のうち、No22を実施している場合は、その手法（朝礼、回覧、会議）及び範囲（派遣社員を含むか）、実施していない場合はその理由

- ・ 5分のできる自社診断シートの項目のうち、No25 社内ルール明確にしていない場合、その理由
- ・ ガイドラインの従業員のセキュリティ責務の明確化(派遣含む、実施している理由、していない理由) (5分のできる自社診断シート 70点以上の企業に対して)
- ・ ガイドラインのルールの周知と知識習得機会の設定(手法)(5分のできる自社診断シート 70点以上の企業に対して)

Q1-4: 外部の企業や取引先と情報をやり取りする際に、情報の取り扱いに関する注意事項の合意を取っていますか?(契約書、覚書などの締結)

機密保持依頼を実施していない理由

(機密を渡していない、取引先との関係が長く信頼している、契約書がない、契約書を書いても朗詠防止の効果が薄い、取引先との立場上要求できない)

- ・ 5分のできる自社診断シートの項目のうち、No23 取引先に対する機密保持依頼を実施していない場合はその理由
- ・ ガイドラインの外部との情報の取扱いに関する合意(実施していない理由)(5分のできる自社診断シート 70点以上の企業に対して)
- ・ 取引先からの情報セキュリティ対策の要請及び実施状況確認の有無
- ・ 具体的な合意方法、手法、また対象(すべての取引先と行なっているのか?限られた取引先との場合のみか)について

Q1-5: 情報セキュリティ対策の実施体制(5分のできる自社診断シート 70点以上の企業に対して)

- ・ ガイドラインのセキュリティ責任者、担当者の明確化(どの部署か。実施していない場合はその理由も)(5分のできる自社診断シート 70点以上の企業に対して)

## Q2) 物理的セキュリティ対策について

情報セキュリティの関わるオフィスやハードウェア、サーバールームなどの物理的なセキュリティ対策の現状を把握する。特に外部の人間が許可や確認も無く勝手に出入りできなくするような抑止施策とディザスターリカバリ対策のような災害対策(BCP)などの対策を確認する。

Q2-1: 重要な情報を保管したり、扱ったりする場所の入退管理と施設管理を行っていますか?(5分のできる自社診断シート 70点以上の企業に対して)

- ・ ガイドラインの重要情報の保管と入退室または施錠管理(実施していない理由)(5分のできる自社診断シート 70点以上の企業に対して)

Q2-2: 物理的な情報セキュリティ対策として実施している内容(実施していない場合はその理由)

5分のできる自社診断シート及び情報セキュリティ対策チェックリストを見た上でインタビュアーが気になるチェック項目等について質問する

対象項目：5分のできる自社診断シート設問 No1,2,3,4,5,6,7  
情報セキュリティ対策チェックリスト No2-1,2-2,2-3

### Q3) 情報システム及び通信ネットワークの運用管理状況について

ここでは運用管理に関する情報システムそのものの情報セキュリティの実態を詳細に聞き取る。特にセキュリティの観点からシステム担当者の運用管理状況及びユーザのシステム利用方法について把握する

Q3-1：情報システムの運用に関して運用ルールを策定していますか？(実施している内容、していない場合はその理由) (5分のできる自社診断シート 70点以上の企業に対して)

- ・ ガイドラインの情報システムの運用ルールの策定(実施していない理由) (5分のできる自社診断シート 70点以上の企業に対して)

Q3-2：情報セキュリティ対策として運用管理面で実施している内容(実施していない場合はその理由)

5分のできる自社診断シート及び情報セキュリティ対策チェックリストを見た上でインタビュアーが気になるチェック項目等について質問する

対象項目：

5分のできる自社診断シート設問 No2,8,9,10,11,12,13,14,15,16,17,18,19,20,25  
情報セキュリティ対策チェックリスト No3-1,3-2,3-3,3-4,3-5

### Q4) 情報システムのアクセス制御の状況及び情報システムの開発、保守におけるセキュリティ対策の状況

情報システムでのネットワーク管理上のアクセス管理やクライアント管理など情報漏えい対策の実施状況について把握する。

Q4-1：情報(データ)や情報システムへのアクセスを制限するために、利用者IDの管理(パスワードの管理など)を行っていますか？(5分のできる自社診断シート 70点以上の企業に対して)

- ・ ガイドラインの情報システムへのアクセス管理(実施していない理由) (5分のできる自社診断シート 70点以上の企業に対して)

Q4-2：情報漏えい対策として情報システム面、管理面で実施している内容(実施していない場合

はその理由)

5分のできる自社診断シート及び情報セキュリティ対策チェックリストを見た上でインタビュアーが気になるチェック項目等について質問する

対象項目：5分のできる自社診断シート設問 No15,20,23

情報セキュリティ対策チェックリスト No4-1,4-2,4-3,4-4,4-5

#### **Q5) 情報セキュリティ上の事故対応状況について**

情報システムで実際にセキュリティ上のトラブルが発生した場合の対処方法と具体的な事例があれば聞き取り、その際の処理、対処状況などを聞き取る。

Q5-1：情報システムに障害が発生した場合、業務を再開するために何をすべきかを把握していますか？(5分のできる自社診断シート 70点以上の企業に対して)

- ・ ガイドラインの障害時対策の策定(実施していない理由)(5分のできる自社診断シート 70点以上の企業に対して)

Q5-2：情報セキュリティに関連する事件や事故等(ウイルス感染、情報漏えい等)の緊急時に、何をすべきかを把握していますか？(5分のできる自社診断シート 70点以上の企業に対して)

- ・ ガイドラインのセキュリティ事故(不正アクセス、情報漏えい等)発生時の対策の策定(実施していない理由)(5分のできる自社診断シート 70点以上の企業に対して)

Q5-3：情報セキュリティに関連する事件や事故等(ウイルス感染、情報漏えい等)の経験はありますか？

- ・ 具体的な事例とその時の対処方法の詳細

#### **Q6) 情報セキュリティのガイドラインの内容について**

情報セキュリティのガイドライン及び5分で出来る自己診断シートの内容についての感想はいかがですか？(別紙『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』『5分で出来る！中小企業のための情報セキュリティ自社診断』参照)

- ・ 大体理解できていたか、実施済みか、情報が不足していないかなどの状況を具体的にヒアリングする

(わかりやすさ、目的の明確さ、対象の明確さ、内容の網羅性、過不足のポイントなど)

- ・ その他感想や改善すべき点はあるか

#### Q7) 情報セキュリティのガイドラインの活用効果について

情報セキュリティのガイドライン及び5分で出来る自己診断シートの効果、利活用について(別紙『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』『5分で出来る!中小企業のための情報セキュリティ自社診断』参照)

- ・ 自社診断シートや組織的な対策ガイドライン(対策チェックリスト含む)は今後の対策を検討するのに役立ちそうか
- ・ 効果があったか(また調査以前に認知していたか。認知していた場合はすでに利用したことがあるか)いなか
- ・ 実際の企業への活用度合い、マッチ度、基準のラインとしての妥当性など具体的にヒアリングする

#### Q8) 情報セキュリティ投資についての重要性、課題について

経済環境の悪化に伴って、IT投資も低下傾向ですが、情報セキュリティに関連する投資はどう考えますか?

「重要性の認識」

  
  

「課題・問題点」

- ・ 情報セキュリティ対策関連で課題と認識していること、悩み
- ・ 投資増減や必須項目など全般的な投資と絡めて具体的にヒアリングを行う

#### Q9) 情報セキュリティについての情報、提案について

情報セキュリティに関連する情報収集、提案などは誰が行いますか?

情報収集先(商工会議所・商工会(経営指導員、等)、ITコーディネータ、ITベンダ、税理士、中小企業診断士、取引先(親会社含む)、友人・知人、IPA(Web、セミナー等)、その他)

- ・ 情報収集手段、改善提案作成者(今後の普及・情報提供手段の考慮材料としての観点も含める)(複数可)
- ・ 具体的な情報収集、提案先など、その理由、要因

#### Q10) 具体的な事例としてのご紹介

特徴的な事例や先進事例または失敗・トラブル事例としてご紹介して頂く場合のコメント(伝聞可)

「成功・先進事例」

「失敗・トラブル事例」

- ・ 自社の対策を進めるに当たって、効果的だった事例はあるか。
- ・ 自社または取引先等（伝聞でも可）で情報セキュリティに関するトラブルの発生はあるか。また、そこから得た教訓はあるか。

**Q11) 貴社独自の情報セキュリティに関する課題、問題点**

貴社のビジネス上で発生するまたは必須となる情報セキュリティの課題と問題点をお聞かせください。

- ・ 取引先や親会社との関係性などビジネスを行って行く上で必須となる情報セキュリティについて
- ・ Q9 までに含まれない特記事項などを具体的に聞き出す

**Q12) 経営層の意識、情報セキュリティ認定、各種資格、その他について**

公的な認証制度、担当者の持っている資格・必要と考える資格、IPA など公的機関への期待などについて聞き取る。

- ・ IPA についての認知状況
- ・ IPA（及び関連団体）に期待することがあるか
- ・ セキュリティベンチマークについての認知、使ってみたいかなど
- ・ 公的な認証等（ISMS、プライバシーマーク）についての考え
- ・ 担当者が持っている資格や今後取得していく（させていく）資格

## 【企業プロフィール情報】

### 概要属性

1. 企業規模分類：\_\_\_\_\_（A: 20 人未満、B: 20-100 人、C: 100-300 人）
2. 業種分類：\_\_\_\_\_（A: 製造・建設業、B: 小売・卸売・飲食業、C: サービス業・その他）
3. 地域分類：\_\_\_\_\_（A: 大都市、B: 地方）
4. S: ネット系企業

### 詳細情報

企業概要： \_\_\_\_\_  
従業員数： \_\_\_\_\_  
拠点数： \_\_\_\_\_  
情報システム部門有無： \_\_\_\_\_  
情報システム部門内訳： 人数 \_\_\_\_\_ 内訳 \_\_\_\_\_  
IT 導入状況： \_\_\_\_\_  
主な利用用途： \_\_\_\_\_  
主な IT システム（業務システムなど保守サポートしている）の購入先： \_\_\_\_\_  
サーバの有無：（有） \_\_\_\_\_ 台 \_\_\_\_\_ メーカー名： \_\_\_\_\_ （無） \_\_\_\_\_  
クライアント状況： 台数 \_\_\_\_\_ 台  
資本金： \_\_\_\_\_ 百万円  
年間売上高： \_\_\_\_\_ 百万円  
IPA の情報セキュリティ対策ベンチマークシステムの認知の有無 \_\_\_\_\_

〒 \_\_\_\_\_

住所： \_\_\_\_\_

（ヨミ）

社名： \_\_\_\_\_

部署： \_\_\_\_\_

役職： \_\_\_\_\_

回答者氏名： \_\_\_\_\_

e - mail アドレス： \_\_\_\_\_

調査日付： \_\_\_\_\_

調査担当： \_\_\_\_\_

本シートは、調査実施者のインタビューに用いるもので、調査対象企業には記入をお願いしておりません。  
個人情報の取り扱いに関しては、調査協力依頼状に法令遵守及び適切な取扱いについて明記したほか、面接調査時に口頭説明しております。