# 付録1：セキュリティ問診票

記入日 　　 　年　　　　　月　　　　日

|  |
| --- |
| 会社名：問診票記入者： |
| 従業員数（　　　　　　）人、　端末数（　　　　　）台、　拠点数（　　　　　）箇所 |
| 相談のきっかけや経緯について伺います。すでに被害がある方は問1〜3 と5に、不安がある方は問4と5にお答えください |
|  | 問1：外部から通報や連絡がありましたか？　例：情報が漏えいしている、改ざんされている、パソコンがおかしくなった、など　□はい　（連絡元と、連絡の内容：　　　　　　　　　　　　　　　　）　□いいえ |
|  | 問2：過去にサイバー攻撃と思われる被害を受けたことはありますか？　□はい　（被害の状況：　　　　　　　　　　　　　　　　　　　　　）　□いいえ |
|  | 問3：相談しようとするまでに、何か対処はしましたか？　□はい　（時系列でお答えください：　　　　　　　　　　　　　　　）　□いいえ |
|  | 問4：現在どのような不安がありますか？（複数回答可）　□公開しているサーバへの攻撃がある　□パソコンがウイルスに感染している　□内部から情報が漏えいしている　□その他（　　　　　　　　　　） |
|  | 問5：相談のきっかけや経緯についてできるだけ具体的にお書きください |
| 主にシステム管理者の方に、現在の症状についてより詳細に伺います |
|  | 問6：ネットワークが繋がりにくい・使えない　□はい　・いつごろからですか？　（　　　　　　　　　　　　　　　　　　　）　　　　　・頻度はどの程度ですか？（1回だけ・数回・決まった時間・決まった曜日）　　　　　・どのような時に症状を感じますか？　（　　　　　　　　　　　　　）　□いいえ　□わからない |
|  | （次のページへ進みます） |
|  | 問7：サーバの反応が悪い・反応がなくなる　□はい　・いつごろからですか？　（　　　　　　　　　　　　　　　　　　　）　　　　　・頻度はどの程度ですか？（1回だけ・数回・決まった時間・決まった曜日）　　　　　・どのようなサーバですか？　（　　　　　　　　　　　　　　　　　）　□いいえ　□わからない |
|  | 問8：PC・携帯端末の反応が悪い・動かなくなる　□はい　・いつごろからですか？　（　　　　　　　　　　　　　　　　　　）　　　　　・頻度はどの程度ですか？（1回だけ・数回・決まった時間・決まった曜日）　　　　　・どのような端末ですか？　（　　　　　　　　　　　　　　　　　）　　　　　・何台で起こっていますか？　（　　　　　　　　　　　　　　　　）　□いいえ　□わからない |
|  | 問9：不正な通信、アクセスの形跡がある・気になるログがある　□はい　　・いつごろからですか？　（　　　　　　　　　　　　　　　　　　）　　　　　　・どのような内容、不審点がありますか？　（　　　　　　　　　　）　□いいえ　□わからない |
|  | 問10：症状が始まった頃に、下記のような出来事がありましたか？　□はい　　・システム変更を行った / 新しいソフトを導入した・怪しいサイトやメールにアクセスした　　　　　　・情報記録媒体を紛失した　　　　　　・その他不安なこと（　　　　　　　　　　　　　　　　　　　　　）　□いいえ　□わからない |
| 主にシステム管理を行っている方に、管理状況について伺います |
|  | 問11：情報機器や情報資産、ネットワークの構成について把握されていますか？　□はい　□いいえ　□わからない |
|  | 問12：ネットワークやシステムのログを取得していますか？　□はい　□いいえ　□わからない |
|  | （問12が「はい」の方にお聞きします）問13：ログの保存期間は決めていますか？　□はい　（期間：　　　　　　　　　　　　　　）　□いいえ　□わからない |
|  | 問14：普段から付き合いのあるセキュリティ事業者やITサービス事業者はいますか？　□はい　（会社名：　　　　　）※複数社あれば複数社お答え下さい　□いいえ　□わからない |
|  | （次のページへ進みます） |
| 主に事案や事件の対応者や責任者の方に、社内の組織体制についてお聞きします |
|  | 問15：事案や事件の窓口担当者は決めていますか？　□はい　□いいえ |
|  | 問16：相談について事案や事件対応責任者の了解を得ていますか？　□はい　□いいえ |
|  | 問17：事案や事件の上位職への相談や報告をする順序は決まっていますか？　□はい　□いいえ　□わからない |
|  | 問18：既にどこかへ報告しましたか？　□はい（責任者、経営陣、関係者（監督官庁、取引先、顧客））　□いいえ |
|  | 問19：社内での調査や対処をする権限を持つ責任者や担当者がいますか？　□はい　□いいえ　□わからない |
| 主に事案や事件の対応者や責任者の方に、IPA 「10大脅威 2015」で示された「セキュリティ対策の基本」をどの程度実施しているかの確認です。 |
|  | 問20：「対策の前に」はどの程度実施していますか？（複数回答可）　□守りたい情報資産の把握 （情報資産とその場所： 　　　　　　　　　　　　　　　　　　　　　　　　　）　□自発的なセキュリティ対策への取り組み　□計画を策定し、必要な予算の確保 |
|  | 問21： 現在行っているセキュリティ対策はどのようなものですか？（複数回答可）　□利用しているソフトウェアを更新・最新のものに（OSやアプリケーションなど）　□セキュリティソフト（ウイルス対策ソフトなど）の導入　□パスワードの適切な管理と認証の強化（多要素認証など）　□ソフトウェアや機器の設定を見直す（サーバ・ネットワーク設定の管理）　□ソフトウェアや機器の脆弱性や犯罪への対策などの情報収集 |
|  | 問22：その他に実施している対策はありますか？（複数回答可）□文書による実施すべき対策の明文化　　□システムによる制限や強制□バックアップやシステムの冗長化　　□検査や監査□認証の取得（プライバシーマークやISO/IEC27001 など）□その他（　　　　　　　　　　　　　　　　　　　　　　　　　　　　　） |
| 質問は以上です。ご回答ありがとうございました |