「やられたかな？その前に」ガイド

～　『やられてる』！と思ったら　～

２０１５年１０月１４日

日本セキュリティオペレーション事業者協議会 （ＩＳＯＧ－Ｊ）

あさまでＳＯＣプロジェクト

免責事項

- 本ガイドに登場する会社名、製品名、サービス名は、一般に各社の登録商標または商標です。本文中では®、TM、©　マークは明記していません。
- ISOG-J ならびに執筆関係者は、このガイド文書に関するいかなる責任も負うものではありません。全ては自己責任にてご活用ください。

目次

1. はじめに

本書「やられたかな？その前に」ガイドは、昨今のサイバー攻撃や標的型攻撃によって不安が高まるなか、セキュリティの専門家へ相談する際に事前に確認しておいてほしいことを問診票の形式でまとめたものである。

漠然とした不安の中で相談をする際に、今自分や企業がどういった状況にあるのかを見直し、不安の原因を確認し、スムーズに相談を進めることができることを目的としている。

問診票の項目は、裏を返せば普段から行っておいてほしい対策にもなるものである。本書が読者や企業のセキュリティ対策の向上につながり、いざという時にはセキュリティ事業者へ相談し、より適切な処置をできるようになることを期待する。

2. 想定シナリオ

あなたはある会社の社員です。社長が急に「うちは大丈夫か？」と言い出して、セキュリティの専門家に相談することになりました。

さて、どうしましょう？

外部のセキュリティの専門家に相談するとして、どう説明したらよいでしょう？

そこで、本書の問診票を記入し、相談を始めることとしました。

3. 問診票の使い方

相談をする前に、問診票を書きながら社内の状況や相談内容を明らかにする。無理にすべて記載する必要はないので、可能な範囲、わかる範囲で記載をする。

問診票を記載したところで、セキュリティ事業者や（すでに取引がある）IT サービス事業者へ相談をお願いしたい。

4. 問診票の各項目について

各項目と説明は以下の表のとおりである。

項番	項目	説明
	従業員数や端末数	どの程度の台数が存在し、調査が必要か概要を確認する。
問 1～5	相談の経緯について	現在の被害の有無や外部からの指摘といった状況についてのヒヤリングとなる。 相談の際に被害はまだないのだが不安がある場合は不安な箇所がどこかといったところからのヒヤリングとなる。
問 6～10	症状の詳細について	主にシステム管理を行っている方への質問となる。 既に何か症状がある場合、どのような症状があるかの確認となる。わからない場合は「□わからない」を選択頂きたい。 症状はシステム利用者に聞くことや、主観での回答でも良い。 調査を開始する際に、ネットワーク、サーバ、パソコンや端末、ログや心当たりをヒヤリングしておくことで、どこから着手するかの手がかりとなる。
問 11～14	現在の管理状況について	主にシステム管理を行っている方への質問となる。 調査に必要な現状把握の設問である。 ネットワークやシステムに関連した社内文書の有無や、調査の対象となるログについて確認する。 調査の中心がログの分析となる場合、社内のどこに何があるかがはっきりしていると、分析の手がかりとなる。 分析作業のために、ログの保管場所や保存期間を把握する必要がある。

		IT 関連をいつもお願いしている事業者や関連業者があれば記載をお願いしたい。 普段からのどの程度のセキュリティの対策を行っているかなどの把握が調査の手助けとなる。
問 15～19	社内の組織体制について	主に事案や事件の対応者や責任者の方向けの質問となる。明確に組織が存在しない場合は、システム管理者の方の回答でも良い。 今後の相談や調査、社内の対応に向けての確認となる。 調査や分析では、お客様の協力が必要不可欠である。 業者との窓口という意味だけではなく、調査や分析に当たって、社内の手続きを含めてどういった手順で進めることができるかを事前に把握する。
問 20～22	IPA 10 大脅威 2015 の基本対策	主に事案や事件の対応者や責任者の方向けの質問となる。明確に組織が存在しない場合は、システム管理者の方の回答でも良い。 セキュリティの基本対策がどの程度実施されているか確認する。 対策の内容によって調査や分析の手助けになる部分があるかの確認となる。 各項目の詳細な内容については「10 大脅威 2015」を確認されたい。

情報処理推進機構（IPA）の 「10 大脅威 2015」は以下のホームページから内容を確認されたい。

情報セキュリティ　１０大脅威　２０１５

https://www.ipa.go.jp/security/vuln/10threats2015.html

5. 相談後の流れ

相談後はセキュリティ事業者や IT サービス事業者のサービスを受けることとなる。サービス提供者によって内容や価格はまったく異なるため、直接ご確認いただきたい。

相談の際に、その後の調査や対策の費用の上限について目途を付けておくことで、セキュリティ事業者などへの相談がスムーズになる。

6. その後の対策について

相談、調査、処置の後は、予防としての対策である。病気と同様に、病気になってからの対処するより、予防をしておく方がコストを抑えられる。

普段からセキュリティについて相談できる「かかりつけ医」のような存在を得ておくことで、事件や事故発生時の対応を検討して、有事の際は迅速に対処できるようになる。

IPA 「10 大脅威 2015」を参考に、セキュリティの基本対策や本問診票の項目に加えて、今後の対策として以下を提言する。

提言：事故や事件に対応できる組織や危機管理体制の整備

1. 専門家に相談し、CSIRT[1]構築に着手する
2. 有事の指揮命令系統や対応者を策定する
3. 事故や事件の対応訓練の実施する
4. 組織体制と仕組みを維持する

実施例として、「経営者が事件や事故の対応を行う外部との窓口を任命する」や「サーバ・ネットワーク構成を文書化する」といった事から着手して、事件や事故に対応ができる組織作りを進められたい。

事件や事故発生時に組織全体で取り組む姿勢がなければ、事態の収束は難しい。予防のために着実に対策を進めていただきたい。

[1] Computer Security Incident Response Team：サイバー攻撃の検知から事件や事故の対応を行う組織体制

7. 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

8. 付録 2：セキュリティ問診票記入例（標的型攻撃の例）

記入日　2015 年　8 月　20 日

会社名：（**ある会社**）
問診票記入者：（**ある会社のセキュリティ担当兼システム担当の A さん**）

従業員数（　10）人、　端末数（　10）台、　拠点数（　1）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[illegible]にお答えください

問 1：外部から
被害があったかどうかからスタートします
例：情報が漏[illegible]かしくなった、など
■はい　（連絡元と、連絡の内容：**某機関から、不審な通信がある**）　□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：**パソコンの電源を抜いた　など**）□いいえ

問 4：現在どの[illegible]
相談までの状況、専門家への希望などを記載ください
□公開して
□内部から

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
当社へ某機関から不審な通信があると連絡があった。不審な通信の内容を聞いてみると、当社の機密情報のファイルが外部へ送信されていることが判明した。
機密情報を扱うパソコンは決まっているため電源を抜いたものの、その後どうしたら良いかわからないため、セキュリティの専門家に相談することとした。
どこから侵入されて、何が漏えいしたのか、今後の対策も含めて相談したい。

調査の手がかりを得るため、症状を確認します。
わからない項目は「わからない」とご回答ください。

主にシステム管理[illegible]

問 6：ネットワークが[illegible]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　　・決まった曜日）

・どの　　）

・何台　　）

■いいえ　□わからな

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

□はい

■いいえ

主にシステム管理を行ってい　　況について伺います

問 11：情報機器や情報資産、　　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：普段た

□はい　（

■いいえ

（次のページへ進みます）

調査の手がかりをとなりますので、
記録がある場合はご記入ください。

詳細な調査の際に、どこから着手するかの手助けとなります。
わからない場合は「わからない」でお答えください。
例として、情報機器や情報資産の一覧は重要度の判断や被害状況の
確認に、ネットワーク構成は侵入経路などの調査に使用します。

ログの分析が必要となった場合に、どこのログが取得され、どの
程度の期間保管されているかが重要です。

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
■はい　□いいえ

事案や事件の対応を進めるに当たって、社内体制などの確認です。
どこまでどう対応できるかの確認となります。

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
□守りたい情報資
（情報資産とその
□自発的なセキュ
□計画を策定し、必

普段から行っておきたい対策をどの程度実施しているかの確認です。
調査とは直接関連しませんが、調査範囲の目安となります。

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

執筆

日本セキュリティオペレーション事業者協議会 （ＩＳＯＧ－Ｊ）

あさまでＳＯＣプロジェクト

代表	武智 洋	日本電気株式会社
リーダー	武井 滋紀	エヌ・ティ・ティ・ソフトウェア株式会社
	桃井 康成	株式会社インターネットイニシアティブ
	亀田 勇歩	SCSK 株式会社
	早川 敦史	NEC ソリューションイノベータ株式会社
	阿部 慎司	NTT コムセキュリティ株式会社
	小澤 文生	NTT コムセキュリティ株式会社
	新柴 博之	NTT コムセキュリティ株式会社
	本橋 孝祐	NTT コムセキュリティ株式会社
	（他 1 名参加）	NTT コムセキュリティ株式会社
	河島 君知	NTT データ先端技術株式会社
	神山 竜二	株式会社セキュアソフト
	井上 博文	日本アイ・ビー・エム株式会社
	窪田 豪史	日本アイ・ビー・エム株式会社
	永沼 美保	日本電気株式会社
	尾花 悦正	日本ユニシス株式会社
	大森 雅司	株式会社日立システムズ
	本田 秀行	株式会社富士通ソーシアルサイエンスラボラトリ
	田中 朗	三菱電機インフォメーションネットワーク株式会社
	庄谷 卓也	三菱電機インフォメーションネットワーク株式会社
	阿部 正道	株式会社ラック
	賀川 亮	株式会社ラック
	品川 亮太郎	株式会社ラック

（執筆協力）	中西 克彦	NEC ネクサソリューションズ株式会社
（執筆協力）	前田 典彦	株式会社 Kaspersky Labs Japan
（執筆協力）	大崎 譲	セコムトラストシステムズ株式会社
（執筆協力）	加治川 剛	セコムトラストシステムズ株式会社
（執筆協力）	加賀谷 伸一郎	独立行政法人　情報処理推進機構

（執筆関係者、社名五十音順）