

# 相談・届出先クイックリスト

## <<<<インシデント対応>>>>

### ■一般的な情報セキュリティ相談

#### ●IPAセキュリティセンター情報セキュリティ安心相談窓口

- ☎ 03-5978-7509 -可能な限り公開されているFAQを参照してから相談

### ■犯罪の可能性がある場合の相談窓口

#### ●警視庁 サイバー犯罪対策課

- ☎ 03-5805-1731 (都庁からは9110-7861-3038, 3089)

### ■サイバー犯罪の届出

- 警視庁 ☎ 03-3581-4321 (交換) 管轄の警察署名を確認し転送を

### ■フィッシング詐欺に関連するメールやサイトにアクセスした場合のメール相談

【ビジネスメール詐欺は、自社と取引先のどちらにも損害賠償責任があり得る】

#### ●フィッシング対策協議会

### ■迷惑メール相談センター (日本データ通信協会)

不特定多数へ同意を得ずに送られる広告宣伝目的のメール ☎ 03-5974-0068

### ■なりすましECサイトを作られた事業者の対策ガイド

- 事業者: ①問い合わせ対応メモ ②サイト内注意喚起 ③プロバイダ削除要請
- 利用者: 警視庁サイバー犯罪対策課、管轄の警察署

#### ●なりすましECサイト対策協議会

- 違法情報の通報:

### ■インターネット上での違法・有害情報の相談・通報

#### ●「違法・有害情報センター」(総務省系) 【削除依頼は行わない】

Webでユーザ登録してから具体的な相談

#### ●「インターネット・ホットラインセンター」: (警察庁・総務省 フォームで通報)

### ■消費生活全般に関する苦情や問合せ

#### ●消費者ホットライン【国民生活センター】☎ 188番

### ■法律相談

#### ●法テラス (日本司法支援センター) ☎0570-078374

### ■個人情報の取り扱いに関する相談

- 個人情報保護委員会 ☎ 03-6457-9849

### ■嫌がらせ、ネットストーカーの相談

- 管轄の警察署の生活安全課 [ブラウザで警察署一覧検索](#)

### ■人権相談

- 「法務省人権擁護局 みんなの人権110番 ☎ 0570-003-110

### ■インシデント報告・届出

- JPCERT/CC ☎03-6811-0610

#### ●インシデント対応依頼 ☎03-6271-8901

(サイトの改ざん箇所の特定や、改ざんされた際の復旧手順。サーバへの侵入やDoS攻撃が発生した際の対処。マルウェアに感染した際の駆除方法、復旧方法。)

#### ●IPA J-CRAT / 標的型サイバー攻撃特別相談窓口

- E-mail [tokusou@ipa.go.jp](mailto:tokusou@ipa.go.jp) ☎ 03-5978-7599

## <<<<恒久的対策>>>>

### ■IT化・セキュリティ対策支援企業(ITコーディネータ)

#### ●情報セキュリティ対策支援サイト (IPA)

#### ●IPAセキュリティプレザンター検索 (IPA)

#### ●情報セキュリティサービス基準適合サービスリスト (IPA)

#### ●サイバーインシデント緊急対応企業一覧 (JNSA)

#### ●ITコーディネータ協会「経営とIT化相談」窓口

#### ●東京都テレワーク推進センター ☎0120-970-396

#### ●テレワークのセキュリティあんしん相談窓口 ネットで申込み (総務省⇒LAC)

#### ●テレワーク相談センター(厚労省委託) ☎0120-91-6479

#### ●東京都中小企業振興公社ワンストップ総合相談 ☎03-3251-7881

### ■IT化・セキュリティ対策助成制度等

#### ●SECURITY ACTION 自ら取り組みを宣言する制度 ☎03-5978-7508

#### ●IT導入補助金(サービス等生産性向上IT導入支援事業)(終了)

#### ●サイバーセキュリティ対策促進助成金(東京都)「標的型メール訓練」

●中小企業の情報セキュリティマネジメント指導業務(METI補助事業)【主に事前支援、登録セキスベを派遣】(今年度は募集終了)

●中小企業向けサイバーセキュリティお助け隊(サイバーセキュリティ事後対応支援実証事業)(IPA)【主に事後支援】(現在、東京都はなし)

## <<<<参考情報サイト>>>>

#### ●「ここからセキュリティ!」:ポータルサイト(事象・対象)(IPA)

#### ●JC3 情報提供 注意喚起情報

#### ●JC3:あなたのパスワードが侵害されました

#### ●不正送金等

#### ●JPCERT/CC 注意喚起

#### ●マルウェア Emotet の感染に関する注意喚起

#### ●迷惑メール相談センター

#### ●迷惑メール・チェーンメール関連パンフレット

#### ●迷惑メール関連の関係法令・窓口等(迷惑メール白書2019より)

#### ●中小企業の情報セキュリティ対策ガイドライン 第3版電子版(IPA)

#### ●情報セキュリティ5か条、5分でできる! 情報セキュリティ自社診断

#### ●国民のための情報セキュリティサイト(総務省)

# 主な対策の例示：マルウェア感染【Emotet 等を含む】

## ■ 事前対応策

- <<「技術的対策」と「管理的対策（人的対策・組織的対策・物理的(環境的)対策を含む）」>>
- 【**ルールの策定**】
  - － 事業継続計画（BCP）の策定
  - － 情報セキュリティポリシーの策定
    - ・ 5分でできる情報セキュリティ自社診断
    - ・ 情報セキュリティ5か条
    - ・ リスク分析シート（まずは主要な情報資産から）
      - － リスク値＝重要度×被害発生可能性（脅威×脆弱性）
    - ・ 情報セキュリティ基本方針
      - － 基本方針、対策基準、実施手順
    - ・ 情報セキュリティハンドブック（従業員向け）
      - － 人的対策
    - ・ 情報セキュリティ関連規程（社内規則）
      - － 管理的対策
- 【**感染予防・事象の検出**】
  - － 組織内への注意喚起の実施
  - － Word マクロの自動実行の無効化
  - － メールセキュリティ製品の導入によるマルウェア付きメールの検知
  - － メールの監査ログの有効化
  - － OS に定期的にパッチを適用（SMBの脆弱性をついた感染拡大に対する対策）
  - － 定期的なオフラインバックアップの取得（標的型ランサムウェア攻撃に対する対策）

## ■ 事後対応策

- 【**事実認識・対応の判断・被害の拡大防止**】
  - － 感染している可能性
    - ・ 自組織のメールアドレスになりすまし、Word 形式のファイルを送るメールが届いたと外部組織から連絡を受けた場合
    - ・ 自組織のメールサーバなどを確認し、Word 形式のファイルが添付されたメールやなりすましメールが大量に送信されていることを確認した場合
  - － 被害拡大防止の観点より初期対応
    - ・ 感染した端末のネットワークからの隔離
    - ・ 感染した端末が利用していたメールアカウントのパスワード変更
  - － 必要に応じて、次のような対処を行うことを推奨
    - ・ 組織内の全端末のウイルス対策ソフトによるフルスキャン
    - ・ 感染した端末を利用していたアカウントのパスワード変更
    - ・ ネットワークトラフィックログの監視
    - ・ 調査後の感染した端末の初期化
  - － 「JPCERT/CC インシデント報告窓口」までご連絡
    - ・ JPCERT/CC インシデント報告窓口
    - ・ メール：[info@jpcert.or.jp](mailto:info@jpcert.or.jp)
    - ・ 電話：03-6271-8901
    - ・ ● [JPCERT/CC 注意喚起](#)
    - ・ [マルウェア Emotet の感染に関する注意喚起](#)
- 【**早期復旧・事業継続**】【**原因調査**】【**復旧**】
  - － 対策対応業者リスト
    - ・ [情報セキュリティサービス基準適合サービスリスト](#)（IPA）
    - ・ [サイバーインシデント緊急対応企業一覧](#)（JNSA）

## ■ 恒久的対策

- 【再発防止策の検討】
- 【新しい対策の策定（技術的・管理的・人的・物理的）】
- 【新しいルールの運用】

# 情報セキュリティ緊急対応

## ■ 緊急対応（自然災害、大火災、感染症、テロも）

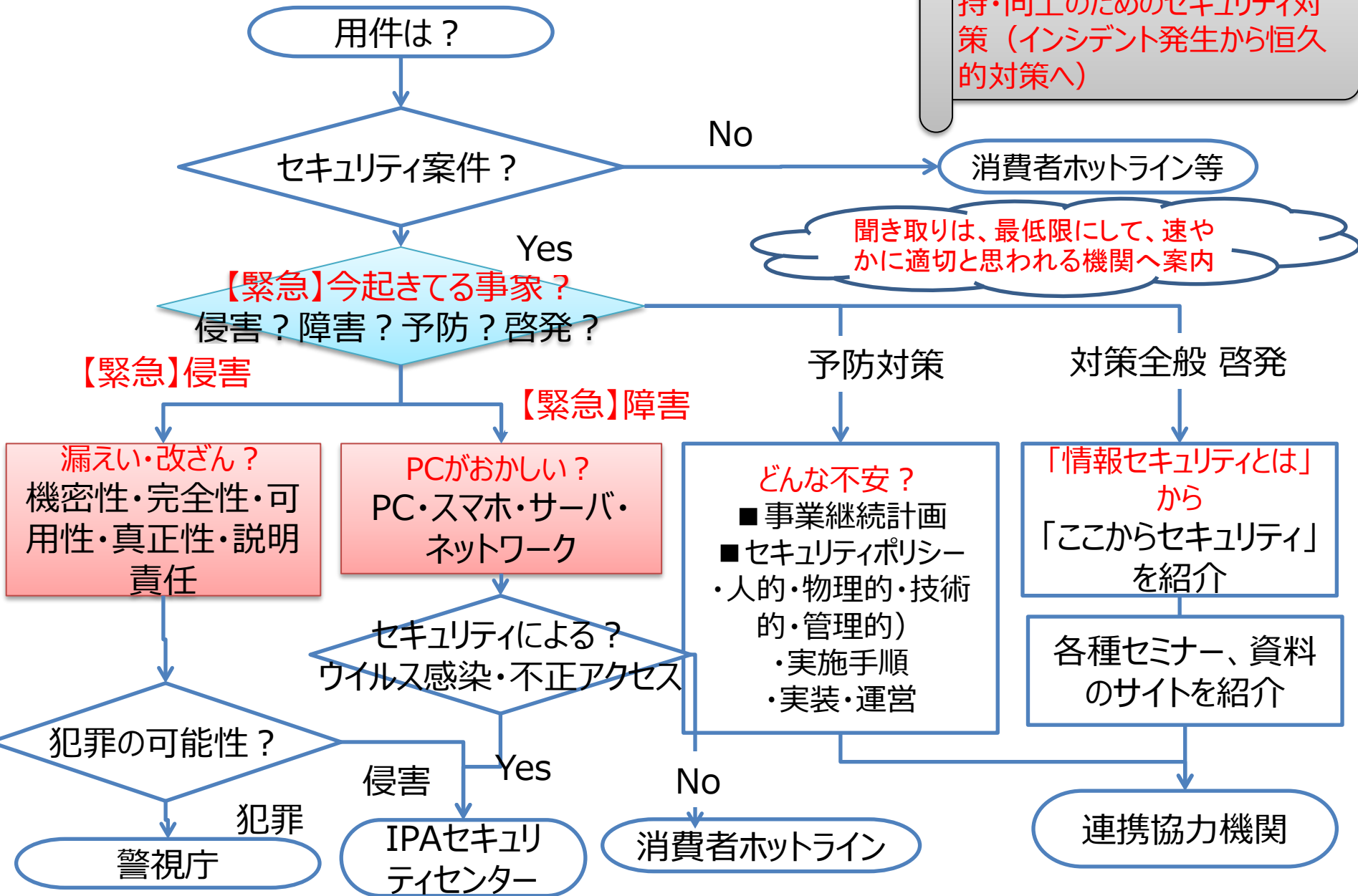
- 攻撃発生
- 攻撃・被害の認知
- 初動対応
  - ・ 事象の検知、報告受付(Detect)
  - ・ 被害の範囲の確認
  - ・ 事実確認、対応の判断
  - ・ サービス停止有無の判断
    - － 被害の局所化(拡大防止)(Triage)
      - ・ 該当システムをネットワークから切り離し、使用を中止する。
      - ・ 被害の範囲を確認し、使用を停止する
  - ・ 顧客・取引先対応
  - ・ 外部専門企業等への調査依頼
  - ・ 早期（暫定）復旧・事業継続(Respond)
    - － 分析、対処、エスカレーション、連携
- 原因調査
  - － なぜ情報セキュリティ侵害が起きたか？
- ・ 侵害原因調査
- ・ システムの脆弱性等の確認
- ・ 被害の詳細確認
- 事後対策
- ・ 復旧
  - － システム管理者に連絡してその指示に従って、適切な復旧を行う。
- ・ 再発防止策の検討・実施
  - － インシデントからの知見の学習
  - － 恒久的対策

## ■ 情報セキュリティ対策の基本

- ・ 不審なメール添付ファイルを開かない
- ・ 偽サイトに注意
- ・ まずリスクの高いものについて
  - － 重要度の高いファイルのバックアップ
  - － ソフトウェアの更新
  - － マルウェア（ウイルス等）対策ソフトの導入
  - － パスワード・認証の強化
  - － 設定の見直し（ルータ、PC等）
- ・ 脅威・手口を知る
  - － 正規のウェブサイトを改ざん
  - － ウェブサイトにアクセスするだけでマルウェア感染
  - － 標的型メールでの不正サイトへの誘導
  - － 不審なメールのマルウェア添付
- ・ 恒久的対策
  - － 定期的なバックアップ
    - ・ ランサムウェアも含めた対策
  - － ルールの策定
    - ・ 事業継続計画（BCP）の策定
    - ・ 情報セキュリティポリシーの策定
  - － フールプルーフ対策
    - ・ 人間が間違えても危険にならない仕組みにしておく、
  - － フェールセーフ対策
    - ・ 機械が壊れても危険にならない仕組みにしておく
  - － ルールの遵守、監査
- CSIRTサービス
- ・ 事後対策（予兆から原状復旧）
- ・ 事前対策（予防策）
- ・ 恒久的対策（セキュリティ品質向上）

# 相談対応フロー

中小企業におけるITを活用した業務の効率化、サービスの維持・向上のためのセキュリティ対策（インシデント発生から恒久的対策へ）



# 東京都中小企業サイバーセキュリティ 相談Webフォーム

- 産業労働局ページ内「相談窓口」へ直接
  - <http://www.sangyo-rodo.metro.tokyo.jp/chushou/shoko/cyber/soudan/index.html>
- 「中小企業向けサイバーセキュリティの極意」ポータルから
  - <https://cybersecurity-tokyo.jp>
    - トップ > 中小企業支援 > 商工 > サイバーセキュリティ > 相談窓口
    - [相談窓口](#) ⇒ 電話・ホームページ専用フォームでのご相談
      - 相談フォーム： [東京都共同電子申請・届出サービス](#)
      - [東京都電子申請 中小企業サイバーセキュリティ対策相談](#)
        - » [中小企業サイバーセキュリティ対策相談](#)
          - 中小企業サイバーセキュリティ対策相談申し込み内容の入力