Sec01-08-10\_相談・届出クイックリスト

# 概要

## 改版履歴

* + 1. 2021年9月13日判断の流れに沿って改訂
    2. 2021年6月3日Web版作成用に校正
    3. 2020年7月22日テレワーク関連追加
    4. 2020年5月18日PPT版から移行

# 相談・届出先

## スライド

## Information 6-1　もしかしてサイバー攻撃？　ここに連絡を！

* + 1. ■PCやスマホの調子が悪い
       1. ■PC、スマホやネットワークに障害が発生している
          - ●システム担当者、購入先、保守業者のサポートセンターに連絡
       2. ■セキュリティ上の問題の可能性がある
          - ●システム担当者に相談する
          - ●システム担当者から関係機関に相談する
    2. ■セキュリティ上の問題ではないが相談したい
       1. ●消費生活でトラブルが起きた
          - ●消費者ホットライン【国民生活センター】

☎ 188番

http://www.kokusen.go.jp/map/

* + - 1. ●人権侵害の可能性を相談したい
         * ●「法務省人権擁護局みんなの人権110番

☎ 0570-003-110

* + 1. ×■セキュリティ侵害事象が発生している
       1. ●犯罪の可能性がある
       2. ●明らかに犯罪が発生していると思われるので届け出たい
       3. ●明らかにセキュリティ侵害が発生している
    2. ■犯罪の可能性？
       1. ●警視庁　サイバー犯罪対策課
          - http://www.keishicho.metro.tokyo.jp/kurashi/cyber/
          - ☎03-5805-1731　（都庁からは9110-7861-3038, 3089）
    3. ■サイバー犯罪の届出
       1. ●警視庁
          - ☎ 03-3581-4321（交換）
          - 管轄の警察署名を確認し転送を
          - http://www.keishicho.metro.tokyo.jp/kurashi/cyber/
    4. ■フィッシング詐欺？
       1. 【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】
       2. ●フィッシング対策協議会
          - https://www.antiphishing.jp/
    5. ■迷惑メールが送られてきた
       1. ●日本データ通信協会
       2. 不特定多数へ同意を得ずに送られる広告宣伝目的メール
       3. ☎ 03-5974-0068
       4. https://www.dekyo.or.jp/soudan/index.html
    6. ■なりすましECサイトを作られた？
       1. 事業者：①問合わせ対応メモ　②サイト内注意喚起 ③プロバイダ削除要請
       2. 利用者：警視庁サイバー犯罪対策課、管轄の警察署
       3. ●なりすましECサイト対策協議会
          - https://www.saferinternet.or.jp/narisumashi/
          - 違法情報の通報:

https://www.safe-line.jp/report/

* + 1. ■インターネット上での違法・有害情報を発見した
       1. ●「違法・有害情報センター」(総務省系)
          - http://ihaho.jp/
          - 【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
       2. ●「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)
          - http://www.internethotline.jp/pages/about/index
    2. ■事象について法律相談をしたい
       1. ●法テラス（日本司法支援センター）
          - ☎0570-078374
          - https://www.houterasu.or.jp/
    3. ■個人情報の取り扱いに関して相談したい
       1. 個人情報保護委員会
          - ☎ 03-6457-9849
          - https://www.ppc.go.jp/
    4. ■嫌がらせ、ネットストーカーの対応を相談したい
       1. ●管轄の警察署の生活安全課ブラウザで警察署一覧検索
          - https://www.keishicho.metro.tokyo.jp/about\_mpd/shokai/ichiran/kensaku/index.html
    5. ■インシデントが発生していることを報告（届け出）したい
       1. ●JPCERT/CC
          - ☎03-6811-0610
          - https://www.jpcert.or.jp/menu\_reporttojpcert.html
          - インシデント対応依頼

☎03-6271-8901

https://www.jpcert.or.jp/menu\_reporttojpcert.html

* + - * + （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。マルウエアに感染した際の駆除方法、復旧方法。）
      1. ●IPA J-CRAT／標的型サイバー攻撃特別相談窓口
         * https://www.ipa.go.jp/security/tokubetsu/index.html
         * ☎ 03-5978-7599
         * E-mail tokusou@ipa.go.jp
    1. ■ウイルスに関して届け出たい
    2. ■不正アクセスに関して届け出たい
    3. ■その他一般的な情報セキュリティ事象の緊急対応を相談したい
       1. ●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
          - https://www.ipa.go.jp/security/anshin/
          - ☎ 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

## Information 6-2 やられる前に、しっかり予防を！

* + 1. ■IT化・セキュリティ対策の相談
       1. ●ITコーディネータ協会　「経営とIT化相談」窓口
          - https://www.itc.or.jp/
       2. ●東京都テレワーク推進センター
          - ☎0120-970-396
          - https://tokyo-telework.jp/
       3. ●テレワーク相談センター(厚労省委託)
          - ☎0120-91-6479
          - https://www.tw-sodan.jp/
       4. ●東京都中小企業振興公社ワンストップ総合相談
          - ☎03-3251-7881
          - https://www.tokyo-kosha.or.jp/support/shien/soudan/
    2. ■セキュリティ対策の相談
       1. ●情報セキュリティ対策支援サイト（IPA)
          - https://security-shien.ipa.go.jp/
          - ●IPAセキュリティプレゼンター検索（IPA)

https://security-shien.ipa.go.jp/presenter/search/

* + - 1. ●情報セキュリティサービス基準適合サービスリスト（IPA)
         * https://www.ipa.go.jp/security/it-service/service\_list.html
      2. ●サイバーインシデント緊急対応企業一覧　(JNSA)
         * https://www.jnsa.org/emergency\_response/
      3. ●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）
         * https://www.lac.co.jp/telework/security.html
    1. ■IT化・セキュリティ対策助成制度等
       1. ● SECURITY ACTION
          - 中小企業自ら取り組みを宣言する制度
          - ☎03-5978-7508
       2. ●令和３年度中小企業サイバーセキュリティ向上支援事業
          - https://cybersecurity-tokyo.jp/torikumi/332/
       3. 事前支援
          - ●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、登録セキスぺを派遣】【終了】
       4. 事後支援
          - ●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】

## 【コラム】日常的に、最新情報をウオッチしよう！

* + 1. ●Twitter
       1. 公的機関
          - 中小企業サイバーセキュリティ対策相談窓口

https://twitter.com/cys\_tokyo

* + - * + 警視庁サイバーセキュリティ対策本部

https://twitter.com/MPD\_cybersec

* + - * + IPA（情報セキュリティ安心相談窓口）

https://twitter.com/IPA\_anshin

* + - * + IPA （ICATalerts）

https://twitter.com/ICATalerts

* + - * + 内閣サイバー(注意・警戒情報)

https://twitter.com/nisc\_forecast

* + - * + JVN 脆弱性レポート

https://twitter.com/jvnjp

* + - * + JPCERTコーディネーションセンター

https://twitter.com/jpcert

* + - * + フィッシング対策協議会

https://twitter.com/antiphishing\_jp

* + - * + JNSA

https://twitter.com/jnsa

* + - 1. 民間
         * サイバーセキュリティ情報局

https://twitter.com/MalwareInfo\_JP

* + - * + マイクロソフト セキュリティチーム

https://twitter.com/JSECTEAM

* + - * + マカフィー株式会社

https://twitter.com/McAfee\_JP

* + - * + ノートン 公式 ツイッター

https://twitter.com/NortonJapan

* + - * + トレンドマイクロ

https://twitter.com/trendmicro\_jp

* + - * + F-Secure Japan 【公式】

https://twitter.com/FSECUREBLOG

* + - * + ラック公式

https://twitter.com/lac\_security

* + 1. ●ブックマーク
       1. キーワード「セキュリティ」を含む新着エントリー - はてなブックマーク
          - b.hatena.ne.jp/keyword/セキュリティ
    2. ●Webページ
       1. ●JC3 情報提供 注意喚起情報
          - https://www.jc3.or.jp/info/heads-up.html
          - ・JC3:あなたのパスワードが侵害されました
          - ・不正送金等
       2. ●JPCERT/CC　注意喚起
          - ・マルウエアEmotetの感染に関する注意喚起

https://www.jpcert.or.jp/at/2019/at190044.html

## ＜＜＜＜いつでも参考にできるようにしておきたい資料・情報サイト＞＞＞＞

* + 1. ●「ここからセキュリティ！」:ポータルサイト（事象・対象）(IPA)
       1. http://www.ipa.go.jp/security/kokokara/
    2. ●国民のための情報セキュリティサイト (総務省)
       1. http://www.soumu.go.jp/main\_sosiki/joho\_tsusin/security/
    3. ●「みんなで使おうサイバーセキュリティ・ポータル」
       1. https://security-portal.nisc.go.jp/
    4. ●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)
       1. https://www.ipa.go.jp/security/keihatsu/sme/guideline/
       2. ・　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
          - https://www.ipa.go.jp/files/000055516.pdf
    5. ●「中小企業向けサイバーセキュリティ対策の極意」
       1. https://cybersecurity-tokyo.jp/
    6. 個別
       1. ●迷惑メール相談センター
          - https://www.dekyo.or.jp/soudan/index.html
          - ・迷惑メール・チェーンメール関連パンフレット

https://www.dekyo.or.jp/soudan/contact/pamphlet/reserve-agree.html

* + - 1. ●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)
         * https://bluemoon55.github.io/Presentation\_Doc/Cyber/迷惑メール関係法令・窓口等【迷惑メール白書2019】.pdf

# 主な対策の例示：マルウェア感染【Emotet ・ランサムウェア等も含む】

## スライド

## ■事前対応策

* + 1. <<「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）」>>
    2. 【ルールの策定】
       1. 事業継続計画（BCP）の策定
       2. 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

* + 1. 【感染予防・事象の検出】
       1. 組織内への注意喚起の実施
       2. Word マクロの自動実行の無効化
       3. メールセキュリティ製品の導入によるマルウエア付きメールの検知
       4. メールの監査ログの有効化
       5. 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)
       6. 定期的なオフラインバックアップの取得（標的型ランサムウエア攻撃に対する対策）

## ■事後対応策

* + 1. 【事実認識・対応の判断・被害の拡大防止】
       1. 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
       2. 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
       3. 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
       4. 「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
          - ☎03-6271-8901
          - ●JPCERT/CC　注意喚起

https://www.jpcert.or.jp/at/2019.html

* + - * + マルウエア Emotet の感染に関する注意喚起

https://www.jpcert.or.jp/at/2019/at190044.html

* + 1. 【早期復旧・事業継続】【原因調査】【復旧】
       1. 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)

https://www.ipa.go.jp/security/it-service/service\_list.html

* + - * + サイバーインシデント緊急対応企業一覧　(JNSA)

https://www.jnsa.org/emergency\_response/

* + 1. ■恒久的対策
       1. 【再発防止策の検討】
       2. 【新しい対策の策定（技術的・管理的・人的・物理的）】
       3. 【新しいルールの運用】

# 情報セキュリティ緊急対応

## スライド

## ■緊急対応（自然災害、大火災、感染症、テロも）

* + 1. ●攻撃発生
    2. ●攻撃・被害の認知
    3. ●初動対応
       1. 事象の検知、報告受付(Detect)
       2. 被害の範囲の確認
       3. 事実確認、対応の判断
       4. 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

* + - 1. 顧客・取引先対応
      2. 外部専門企業等への調査依頼
      3. 早期（暫定）復旧・事業継続(Respond)
      4. 分析、対処、エスカレーション、連携
    1. ●原因調査
       1. なぜ情報セキュリティ侵害が起きたか？
       2. 侵害原因調査
       3. システムの脆弱性等の確認
       4. 被害の詳細確認
    2. ●事後対策
       1. 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。
       2. 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

* + 1. 不審なメール添付ファイルを開かない
    2. 偽サイトに注意
    3. まずリスクの高いものについて
       1. 重要度の高いファイルのバックアップ
       2. ソフトウェアの更新
       3. マルウェア（ウイルス等）対策ソフトの導入
       4. パスワード・認証の強化
       5. 設定の見直し（ルータ、PC等）
    4. 脅威・手口を知る
       1. 正規のウェブサイトを改ざん
       2. ウェブサイトにアクセスするだけでマルウェア感染
       3. 標的型メールでの不正サイトへの誘導
       4. 不審なメールのマルウェア添付
    5. 恒久的対策
       1. 定期的なバックアップ
          - ランサムウェアも含めた対策
       2. 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
       3. 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、
       4. 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
       5. ルールの遵守、監査

## ■CSIRTサービス

* + 1. 事後対策（予兆から原状復旧）
    2. 事前対策（予防策）
    3. 恒久的対策（セキュリティ品質向上）

# 相談対応フロー

## スライド

# メイン トピック