SEC01-08-10\_相談・届出クイックリスト

1. 改版履歴
   1. 2020年5月18日PPT版から移行
2. 相談・届出先
   1. スライド
      1. 
   2.  ＜＜＜＜インシデント対応＞＞＞＞
      1. ■一般的な情報セキュリティ相談
         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

ドキュメントを参照: [anshin](https://www.ipa.go.jp/security/anshin/)

* + - * 1. ☎ 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
    1. ■犯罪の可能性がある場合の相談窓口
       1. ●警視庁　サイバー犯罪対策課
          1. ☎ 03-5805-1731　（都庁からは9110-7861-3038, 3089）
    2. ■サイバー犯罪の届出
       1. ●警視庁☎ 03-3581-4321（交換）

ドキュメントを参照: [cyber](http://www.keishicho.metro.tokyo.jp/kurashi/cyber/)

* + - * 1. 管轄の警察署名を確認し転送を
    1. ■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
       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

ドキュメントを参照: [www.antiphishing.jp](https://www.antiphishing.jp/)

* + 1. ■迷惑メール相談センター　（日本データ通信協会）

ドキュメントを参照: [index.html](https://www.dekyo.or.jp/soudan/index.html)

* + - 1. 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　 ☎ 03-5974-0068
    1. ■なりすましECサイトを作られた事業者の対策ガイド
       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

ドキュメントを参照: [narisumashi](https://www.saferinternet.or.jp/narisumashi/)

* + - * 1. 違法情報の通報:

ドキュメントを参照: [report](https://www.safe-line.jp/report/)

* + 1. ■インターネット上での違法・有害情報の相談・通報
       1. ●「違法・有害情報センター」(総務省系)

ドキュメントを参照: [ihaho.jp](http://ihaho.jp/)

* + - * 1. 【削除依頼は行わない】
        2. Webでユーザ登録してから具体的な相談
      1. ●「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)

ドキュメントを参照: [index](http://www.internethotline.jp/pages/about/index)

* + 1. ■消費生活全般に関する苦情や問合せ
       1. ●消費者ホットライン【国民生活センター】☎ 188番

ドキュメントを参照: [map](http://www.kokusen.go.jp/map/)

* + 1. ■法律相談
       1. ●法テラス（日本司法支援センター）☎0570-078374

ドキュメントを参照: [www.houterasu.or.jp](https://www.houterasu.or.jp/)

* + 1. ■個人情報の取り扱いに関する相談
       1. 個人情報保護委員会 ☎ 03-6457-9849

ドキュメントを参照: [www.ppc.go.jp](https://www.ppc.go.jp/)

* + 1. ■嫌がらせ、ネットストーカーの相談
       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
    2. ■人権相談
       1. ●「法務省人権擁護局　みんなの人権110番 ☎ 0570-003-110
    3. ■インシデント報告・届出
       1. ●JPCERT/CC ☎03-6811-0610

ドキュメントを参照: [menu\_reporttojpcert.html](https://www.jpcert.or.jp/menu_reporttojpcert.html)

* + - * 1. インシデント対応依頼 ☎03-6271-8901

ドキュメントを参照: [menu\_reporttojpcert.html](https://www.jpcert.or.jp/menu_reporttojpcert.html)

* + - * 1. （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

ドキュメントを参照: [index.html](https://www.ipa.go.jp/security/tokubetsu/index.html)

* + - * 1. E-mail tokusou@ipa.go.jp　☎ 03-5978-7599

参照: [E-mail tokusou@ipa.go.jp　☎ 03-5978-7599](#E_mail_tokusou_ipa_go_jp___03_5978_7599)

* 1.  ＜＜＜＜恒久的対策＞＞＞＞
     1. ■IT化・セキュリティ対策支援企業(ITコーディネータ)
        1. ●情報セキュリティ対策支援サイト（IPA)

ドキュメントを参照: [IPA 独立行政法人 情報処理推進機構：](https://security-shien.ipa.go.jp/)

* + - * 1. ●IPAセキュリティプレゼンター検索（IPA)

ドキュメントを参照: [プレゼンター検索：IPA 独立行政法人 情報処理推進機構](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)

ドキュメントを参照: [情報セキュリティサービス基準適合サービスリストの公開：IPA 独立行政法人 情報処理推進機構](https://www.ipa.go.jp/security/it-service/service_list.html)

* + - 1. ●サイバーインシデント緊急対応企業一覧　(JNSA)

ドキュメントを参照: [�T�C�o�[�C���V�f���g�ً}�Ή���ƈꗗ | NPO���{�l�b�g���[�N�Z�L�����e�B����](https://www.jnsa.org/emergency_response/)

* + - 1. ●ITコーディネータ協会　「経営とIT化相談」窓口

ドキュメントを参照: [ITコーディネータ協会（ITCA）](https://www.itc.or.jp/)

* + - 1. ●東京都テレワーク推進センター ☎0120-970-396

ドキュメントを参照: [東京テレワーク推進センター - テレワークのことが相談できる -](https://tokyo-telework.jp/)

* + - 1. ●テレワーク相談センター(厚労省委託) ☎0120-91-6479

ドキュメントを参照: [�ݑ�Ζ���������Ȃ�b�e�����[�N���k�Z���^�[�i�����J���Ȉϑ����Ɓj](https://www.tw-sodan.jp/)

* + - 1. ●東京都中小企業振興公社ワンストップ総合相談☎03-3251-7881

ドキュメントを参照: [ワンストップ総合相談窓口 | 総合支援事業 | 東京都中小企業振興公社](https://www.tokyo-kosha.or.jp/support/shien/soudan/)

* + 1. ■IT化・セキュリティ対策助成制度等
       1. ● SECURITY ACTION

ドキュメントを参照: [SECURITY ACTION セキュリティ対策自己宣言](https://www.ipa.go.jp/security/security-action/)

* + - * 1. 中小企業自ら取り組みを宣言する制度　☎03-5978-7508
      1. ●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)

ドキュメントを参照: [トップページ | IT導入補助金](https://www.it-hojo.jp/)

* + - 1. ●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」

ドキュメントを参照: [サイバーセキュリティ対策促進助成金の申請案内 | 設備助成 | 東京都中小企業振興公社](https://www.tokyo-kosha.or.jp/support/josei/setsubijosei/cyber.html)

* + - 1. 事前支援
         1. ●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】（今年度は募集終了）

ドキュメントを参照: [中小企業の情報セキュリティマネジメント指導業務：IPA 独立行政法人 情報処理推進機構](https://www.ipa.go.jp/security/keihatsu/sme/management.html)

* + - 1. 事後支援
         1. ●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）

ドキュメントを参照: [中小企業向けサイバーセキュリティ事後対応支援実証事業（サイバーセキュリティお助け隊）：IPA 独立行政法人 情報処理推進機構](https://www.ipa.go.jp/security/keihatsu/sme/otasuketai/index.html)

* 1.  ＜＜＜＜参考情報サイト＞＞＞＞
     1. ●「ここからセキュリティ！」:ポータルサイト（事象・対象）(IPA)

ドキュメントを参照: [ここからセキュリティ！ 情報セキュリティ・ポータルサイト](http://www.ipa.go.jp/security/kokokara/)

* + 1. ●JC3 情報提供 注意喚起情報

ドキュメントを参照: [注意喚起情報：情報提供｜一般財団法人日本サイバー犯罪対策センター](https://www.jc3.or.jp/info/heads-up.html)

* + - 1. ・JC3:あなたのパスワードが侵害されました

ドキュメントを参照: [400 Bad Request](https://www.jc3.or.jp/topics/v_log/201903.html#d20190318a)

* + - 1. ・不正送金等

ドキュメントを参照: [注意情報｜一般財団法人日本サイバー犯罪対策センター](https://www.jc3.or.jp/topics/virusmail.html)

* + 1. ●JPCERT/CC　注意喚起

ドキュメントを参照: [注意喚起](https://www.jpcert.or.jp/at/2019.html)

* + - 1. ・マルウエア Emotet の感染に関する注意喚起

ドキュメントを参照: [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. ●迷惑メール相談センター

ドキュメントを参照: [迷惑メール相談センター | デ協](https://www.dekyo.or.jp/soudan/index.html)

* + - 1. ・迷惑メール・チェーンメール関連パンフレット

ドキュメントを参照: [迷惑メール・チェーンメール関連パンフレットのお申し込みについて | 迷惑メール相談センター](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)

ドキュメントを参照: <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>

* + 1. ●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)

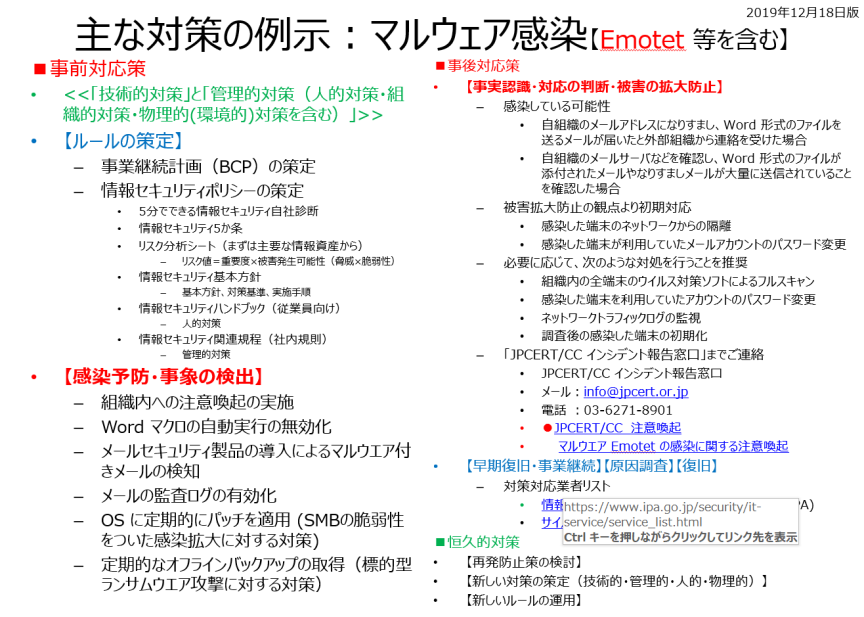
ドキュメントを参照: [中小企業の情報セキュリティ対策ガイドライン：IPA 独立行政法人 情報処理推進機構](https://www.ipa.go.jp/security/keihatsu/sme/guideline/)

* + - 1. ・　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

ドキュメントを参照: <https://www.ipa.go.jp/files/000055516.pdf>

* + 1. ●国民のための情報セキュリティサイト (総務省)

ドキュメントを参照: [国民のための情報セキュリティサイト](http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/)

1. 主な対策の例示：マルウェア感染【EMOTET 等を含む
   1. スライド
      1. 
   2. ■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
            1. 5分でできる情報セキュリティ自社診断
            2. 情報セキュリティ5か条
            3. 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）

* + - * 1. 情報セキュリティ基本方針

基本方針、対策基準、実施手順

* + - * 1. 情報セキュリティハンドブック（従業員向け）

人的対策

* + - * 1. 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）
  1. ■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
           1. 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
           2. 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
           1. 感染した端末のネットワークからの隔離
           2. 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
           1. 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
           2. 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
           3. ネットワークトラフィックログの監視
           4. 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
           1. JPCERT/CC インシデント報告窓口
           2. メール：info@jpcert.or.jp
           3. 電話 ：03-6271-8901
           4. ●JPCERT/CC　注意喚起

ドキュメントを参照: [注意喚起](https://www.jpcert.or.jp/at/2019.html)

* + - * 1. マルウエア Emotet の感染に関する注意喚起

ドキュメントを参照: [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)

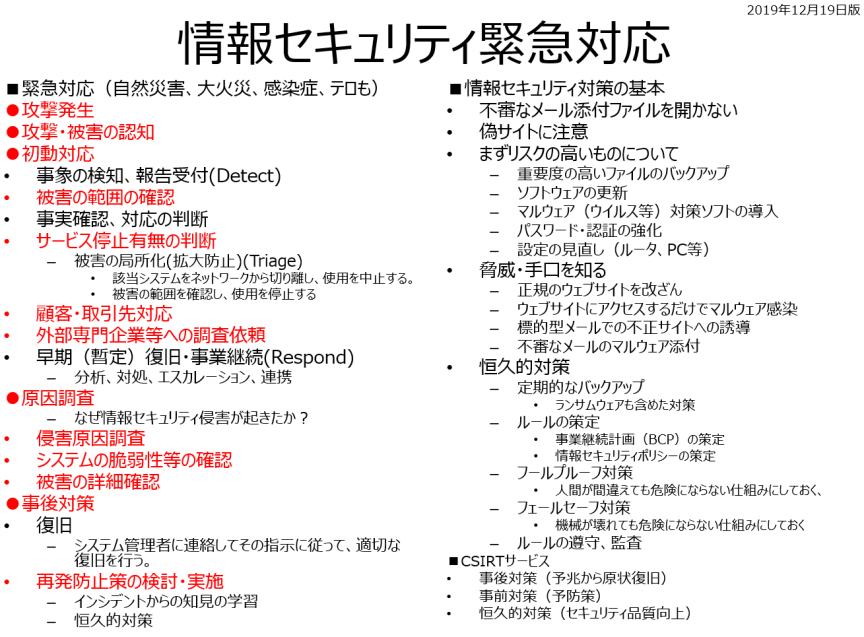
* + 1. 【早期復旧・事業継続】【原因調査】【復旧】
       1. 対策対応業者リスト
          1. 情報セキュリティサービス基準適合サービスリスト（IPA)

ドキュメントを参照: [情報セキュリティサービス基準適合サービスリストの公開：IPA 独立行政法人 情報処理推進機構](https://www.ipa.go.jp/security/it-service/service_list.html)

* + - * 1. サイバーインシデント緊急対応企業一覧　(JNSA)

ドキュメントを参照: [�T�C�o�[�C���V�f���g�ً}�Ή���ƈꗗ | NPO���{�l�b�g���[�N�Z�L�����e�B����](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】

1. 情報セキュリティ緊急対応
   1. スライド
      1. 
   2. ■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
            1. 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
          1. 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
          1. インシデントからの知見の学習
          2. 恒久的対策
  1. ■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
           1. ランサムウェアも含めた対策
        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
        3. フールプルーフ対策
           1. 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
           1. 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
  2. ■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）

1. 相談対応フロー
   1. スライド
      1. 