Sec01-01-02\_「中小企業向けサイバーセキュリティ対策の極意」 【電子書籍（Web版）】での発信情報【案】

ドキュメントを参照: <https://bluemoon55.github.io/Sharing_Knowledge3/MindManager3/Sec01-01-02.html>

1. 改訂履歴
   1. 【2020年7月9日15:00版】全体調整
   2. 【2020年7月3日16:00版】
   3. 【2020年6月23日16:00版】修正すべき項目の再構成
   4. 【2020年6月19日】検討メモ反映
   5. 【2020年6月15日】最新動向関連加筆
   6. 【2020年6月12日】全体目次項目調整結果
   7. 【2020年6月11日19:00版】全体目次項目を精査中
   8. 【2020年6月9日】全体目次項目再構成
   9. 【2020年6月4日】全体構成見直し、リナンバリング、目次候補洗い出し、ポータルでの公開内容加筆
   10. 【2020年6月2日】目次内容再構成
   11. 【2020年5月28・29日】Sec01-01-01の内容をマージし、記載のポイントとなる事項を追記【未完】

ドキュメントを参照: <https://bluemoon55.github.io/Sharing_Knowledge3/MindManager3/Sec01-01-01.html>

* 1. 【2020年5月25日】ビジネスを発展させるために（攻めのIT投資とサイバーセキュリティ対策）への追加項目の検討
  2. 【2020年4月29日】目次構成再整理
  3. 【2020年3月25日】サイバーセキュリティ経営ガイドライン実践状況ツールを追加
  4. 【2020年3月17日】Sec01-01-01\_「中小企業向けサイバーセキュリティ対策の極意」の改訂 （追補資料の作成） から分離

1. リンク
   1. html版

ドキュメントを参照: <https://bluemoon55.github.io/Sharing_Knowledge3/MindManager3/Sec01-01-02.html>

* 1. MindManager版（Download）

ドキュメントを参照: <https://bluemoon55.github.io/Sharing_Knowledge3/MindManager3/Sec01-01-02_「中小企業向けサイバーセキュリティ対策の極意」の改訂案（素材）.mmap>

* 1. EXCEL版（Download）

ドキュメントを参照: <https://bluemoon55.github.io/Sharing_Knowledge3/MindManager3/Sec01-01-02.xlsx>

* 1. Docx版（Download）

ドキュメントを参照: [Page not found &middot; GitHub Pages](https://bluemoon55.github.io/Sharing_Knowledge3/MindManager3/Sec01-01-02.docx)

1. 凡例
   1.  既存項目
   2.  新規項目
   3.    担当
   4.  改訂箇所
   5.  参考資料
   6.  目次掲載項目
2.  情報収集・整理業務と本資料の位置づけ
   1. Webポータルサイト内「サイバーセキュリティ対策情報の書庫」「ナレッジデータベース」「アーカイブ」を公開
      1. 専門員が収集した情報を体系的に整理し、ナレッジデータベースとして公開する
   2. Webポータルサイト内で、電子書籍版「中小企業向けサイバーセキュリティ対策の極意」、その他普及啓発資料を公開
      1. 「サイバーセキュリティ対策情報の書庫」から、普及啓発の目的・媒体に応じて情報を選別・編集し提供内容の材料を提示する
   3. 冊子体版「中小企業向けサイバーセキュリティ対策の極意」を印刷発行
      1. 本資料は、電子書籍版「中小企業向けサイバーセキュリティ対策の極意」の内容をイラスト化、コピーリライトする形で、読みやすい読本を提示する
         1. 1～2年の間に大きく変動しない内容
         2. 数年先の社会の動向（市場動向）、IT関連の技術動向を想定する
         3. 中小企業の経営者向けとしての狙い
            1. 現時点においてはITリテラシーがあまり高くなくても、今後はITの活用が重要性を理解し、 そのためにセキュリティ対策もしっかり行う必要があると認識できるように
   4. ポータルサイトでの情報発信の想定
      1. 中小企業の経営者向け必要最小限の情報提供
         1. 「極意」（Webでの都度更新版）
            1. html版
            2. EPUB版
            3. PDF版
         2. 極意（冊子体としての固定版）
            1. 冊子体の紹介
            2. 冊子体イメージPDF
      2. 中小企業向けのサイバーセキュリティ対策 に関する体系的な情報発信⇒2021年度に充実
         1. 中小企業が事業を継続・発展させるためのIT化において、認識すべきサイバーセキュリティ関連の情報へ、 的確にナビゲートするための情報提供
            1. 体系的・網羅的に情報を整理。相談者、相談対応者が共に参照しあえる情報
            2. 【参考】

※専門員が日々蓄積した知識から抜粋

Sec01-08-5【成果物】専門員業務ハンドブック【目次】

ドキュメントを参照: <https://bluemoon55.github.io/Sharing_Knowledge3/MindManager3/Sec01-08-5.html>

* + - * 1. ※IPA「ここからセキュリティ」の一般向け、中小企業向けのリンク先を含む
    1. 【参考】
       1. ※ポータルサイトでのページ構成案
       2. Sec01-08-2 専門員の所掌業務及び調査分析項目

ドキュメントを参照: <https://bluemoon55.github.io/Sharing_Knowledge3/MindManager3/Sec01-08-2.html>

1.  改訂理由
   1.  国のサイバーセキュリティ関連法規、施策対応
      1. サイバーセキュリティ基本法の改正（2019年4月1日施行）対応
      2. サイバーセキュリティ戦略2018(2018年7月)
         1. 今後3年間の基本的な計画として策定
      3. サイバーセキュリティ2019（2019年5月23日）
         1. （2018年度報告・2019年度計画）
   2.  「サイバーセキュリティ経営ガイドライン2.0対応
   3.  中小企業の情報セキュリティ対策ガイドライン第3版対応
   4.  IPA・NISC等のガイドラインの改訂対応
   5.  サイバーセキュリティ脅威の最新トレンド対応
   6.  ITの最新トレンド対応
   7.  制度・施策の改訂対応
   8.  関連法規の改正対応
   9.  新しい生活様式への移行対応
   10. ＜全般＞
       1. 経営者、CISOを対象読者としていることから、冗長な表現を見直し、全体の記載を簡素化。
       2.   改訂箇所：改訂部分は同時に表現も見直す
2.   目次ーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーー
   1.   【Mission0】 はじめに

参照: [【Mission1】　知っておきたいサイバー攻撃の知識](#a_Mission1__知っておきたいサイバ_攻撃の知識)

* + 1.  改版理由
       1.   国の「サイバーセキュリティ戦略」に沿ったセキュリティ対策を実施するために
       2.   NISC等の資料の反映、テレワークの継続化
    2.    ケーススタディー１：なぜ、こんな小さな会社が狙われたの？
    3.    ケーススタディー２：ある日突然、銀行口座の預金残高が消えた！
    4.    ケーススタディー３：取引先企業への踏み台にされた
    5.    ケーススタディー４：EMOTET、ランサムウェアの被害にあった？
    6.    ケーススタディー５：サイバーセキュリティ保険に入っていれば
    7.    BEC攻撃事例
    8.    サプライチェーンセキュリティの必要性が高まっていること
    9.    セキュリティ対策を怠ると他社に迷惑をかけることもある
    10.    その他ケーススタディー 新規
        1.   「昨今の産業を巡るサイバーセキュリティに係る状況の認識と今後の取組の方向性について」【2020年6月12日METI】等を参考に。
    11.  改訂箇所
        1.  「サイバーセキュリティ経営ガイドライン・概要＞の説明を全体的に修正。
        2.  IoTやAIの活用といった最近の情勢を踏まえる
  1.   【Mission1】　知っておきたいサイバー攻撃の知識
     1.    1-1：標的型攻撃による情報流出
     2.    1-2：ランサムウェアを使った詐欺・恐喝
        1.  【囲みコラム】「No More Ransam」　の紹介
     3.    1-3：Webサービスからの個人情報窃取
        1.  【囲みコラム】割賦販売法の改定とクレジットカードのセキュリティ
     4.    1-4：集中アクセスによるサービス停止
        1.  【囲みコラム】内容更新
     5.    1-5：内部不正による情報漏えいと業務停止
     6.    1-6：Webサイトの改ざん
     7.    1-7：インターネットバンキングの不正送金
     8.    1-8：悪意のあるスマホアプリ
        1.  【囲みコラム】スマートフォン決済不正アプリ
     9.    1-9：巧妙・悪質化するワンクリック詐欺
     10.    1-10：Webサービスへの不正ログイン
         1.  【囲みコラム】不正ログインを…多要素認証の取り込み
     11.    1-11：公開された脆弱性対策情報の悪用
     12.    1-12：IoT機器を踏み台にした攻撃
         1.  【囲みコラム】対策はこれだ…NICT　「NOTICE」の実証事例の結果を追加
     13.    1-13：中小企業におけるサイバー攻撃被害の例
     14.    1-XX：なりすましECサイトの被害と回避策
     15.    1-XX：ビジネスメール詐欺の被害と回避策
  2.   【Mission2】　すぐやろう！対サイバー攻撃アクション

参照: [【Mission2】　すぐやろう！対サイバー攻撃アクション](#a_Mission2__すぐやろう_対サイバ_攻撃アクション1)

* + 1.  改訂のポイント
       1. 冊子版は、敢えて改訂する必要があるか？
       2.  EPUB、Web版は、情報セキュリティ10大脅威レベルでリライトするか？
    2.    2-1：サイバー攻撃に対して何ができるか
    3.    2-2：OSとソフトウェアのアップデート
    4.    2-3：ウイルス対策ソフト・機器の導入
    5.    2-4：定期的なバックアップ
    6.    2-5：パスワードの管理
    7.    2-6：アクセス管理
    8.    2-7：紛失や盗難による情報漏えい対策
    9.    2-8：持ち込み機器対策
    10.    2-9：電子メールの安全利用
    11.    2-10：標的型攻撃メールへの対応
    12.    2-11：迷惑メール発信への対応
    13.    2-12：安全なWebサイト利用
        1.  【囲みコラム】詐欺サイトはこれ…内容更新する（NISC,IPAの資料参照）
    14.    2-13：閲覧制限
        1.  【囲みコラム】中小企業の規制は…事例を更新再調査
    15.    2-14：重要情報の洗い出し
    16.    2-15：重要情報の保管
  1.    【Mission03-A⇒Mission03】経営者は事前に何を備えればよいのか【守りの対策】

参照: [【Mission03-A⇒Mission3】経営者は事前に何を備えればよいのか【守り】](#a_Mission03_A_Mission3_経営者は事前に何を備えればよいのか_守り_)

* + 1.    サイバーセキュリティ対策は、事業継続を脅かすリスクの１つ。
       1.    3-1：サイバーセキュリティ対策が経営に与える重大な影響
       2.    3-2：サイバー攻撃を受けると企業が被る不利益
       3.    3-3：経営者に問われる責任
       4.   【参考：Web版】
          1.   【参考】情報セキュリティ対策を怠ることで企業が被る不利益 【中小企業の情報セキュリティ対策ガイドライン案】
          2.   【参考】経営者が負う責任【中小企業の情報セキュリティ対策ガイドライン （第2版⇒第3版）】

  【参考】Sec01-02-20\_中小企業の情報セキュリティ対策ガイドライン

ドキュメントを参照: <https://bluemoon55.github.io/Sharing_Knowledge3/MindManager3/Sec01-02-20.html>

* + - 1.     【Web版コラム】組織の姿勢3分類(企業経営のためのサイバーセキュリティの考え方の策定について （2016年8月2日）【NISC】より)

ドキュメントを参照: <https://www.nisc.go.jp/conference/cs/jinzai/wg/index.html>

* + 1.    投資効果（費用対効果）を認識する
       1.    3-4：投資効果（費用対効果）を認識する
    2.    【自社の対策状況把握】自社のIT活用・セキュリティ対策状況を自己診断する
       1.    3-5：ITの活用診断
       2.    3-6：サイバーセキュリティ投資診断
       3.    3-7：情報セキュリティ対策診断
    3.    ビジネスを継続するために（守りのIT投資とサイバーセキュリティ対策）
       1.    3-8：業務の効率化、サービス維持のために
       2.    【コラム】クラウドサービスのメリットは？
       3.    【コラム】クラウドサービス導入の留意点
       4.    【Web版コラム】生産性向上のための「デジタル・ワークプレイス」
       5.     【コラム】テレワークではじめる働き方改革テレワークの導入・運用ガイドブック【厚生労働省】
       6.     【コラム】テレワークセキュリティガイドライン（第4版）【2018年4月総務省】
       7.     【コラム】電子印鑑の活用
       8.    【Web版コラム】私用端末のビジネス利用(BYOD)
       9.    【Web版コラム】事業継続計画（BCP）の一環としてのサイバーセキュリティ対策（明文化）
       10.    3-9：経営者が意識すべきサイバーセキュリティ経営3原則
           1.    【参考】経営者が認識すべき「3原則 【中小企業の情報セキュリティ対策ガイドライン（第2版⇒第3版）】
           2.    経営者として取り組むべき「重要7項目の取組」 【中小企業の情報セキュリティ対策ガイドライン（第2版⇒第3版）】
       11.    3-10：経営者がやらなければならないサイバーセキュリティ経営の重要10項目
           1.   経営者からCISOへの10項目の指示

  「サイバーセキュリティ経営ガイドライン」Ver2.0の重要10項目の分類及び内容の改訂に伴う記述の加筆訂正

Sec01-04-1サイバーセキュリティ経営ガイドライン新旧対応関係【2017年12月6日】

ドキュメントを参照: <https://bluemoon55.github.io/Sharing_Knowledge3/MindManager3/Sec01-04-1.html>

* + - 1.    【コラム】サイバーセキュリティ経営ガイドライン実践状況の可視化ツールβ版
      2.    【Web版コラム】サイバーセキュリティ経営ガイドライン 実践のためのプラクティス
         1.   サイバーセキュリティ経営ガイドライン 実践のためのプラクティス集第2版

ドキュメントを参照: <https://www.ipa.go.jp/files/000072309.pdf>

* 1.   【Mission03-C⇒Mission6.6】【組織維持のため】網羅的なサイバーセキュリティ管理と実践 （予防・予兆・事象発生時のための備え）

参照: [【Mission03-C⇒Mission6-6】【組織維持のため】網羅的なサイバーセキュリティ管理と実践 （予防・予兆・事象発生時のための備え）](#a_Mission03_C_Mission6_6__組織維持のため_網羅的なサイバ_セキュリティ管理と実践__予防_予兆_事象発生時のための備え_1)

* + 1.   セキュリティホールを減らす網羅的・体系的な対策の策定方法
       1.   3-XX 網羅的・体系的な対策のために
          1.  ※、詳細は、「Mission6-6情報セキュリティポリシーサンプル」で、 中小企業の情報セキュリティ対策ガイドライン第3版を紹介する形で一括提示
  1.    【Mission03-B⇒Mission04】経営者は事前に何を備えればよいのか【攻めの対策】

参照: [【Mission03-B⇒Mission4】経営者は事前に何を備えればよいのか【攻め】](#a_Mission03_B_Mission4_経営者は事前に何を備えればよいのか_攻め_)

* + 1.    ビジネスを発展させるために(攻めのIT投資とサイバーセキュリティ対策)
       1. 【持続的発展のため】組織の発展を目指した戦略的なIT活用とサイバーセキュリティ対策
       2.    3-11⇒4-X：次世代技術を活用したビジネス展開
       3.   【参考】ITの最新トレンド
       4.    【Web版コラム】攻めのIT投資対応、Society5.0時代に必要なセキュリティ対策
          1.    【Web版コラム】IoT関連セキュリティ対応
          2.    【Web版コラム】クラウドサービスとセキュリティ
          3.    【Web版コラム】５Gセキュリティ対応
          4.    【Web版コラム】BYODセキュリティ対応
          5.    【コラム】IDと認証セキュリティ
          6.    【Web版コラム】AIが人間をアシストする「インテリジェント・ワークプレイス」の活用におけるサイバーセキュリティ対策
          7.    【コラム】DXレポート（ITシステム2025年の崖の克服

  【参考】DAX21\_デジタルトランスフォーメーション（DX）

ドキュメントを参照: <https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX21.html>

* + - 1.    3-12⇒4-X：IoT、ビッグデータ、AI、ロボットの活用
      2.    3-13⇒4-X：IoTが果たす役割と効果
      3.    3-14⇒4-X：人工知能（AI）が果たす役割と効果
      4.    3-15⇒4-X：IoTを活用する際のサイバーセキュリティ上の留意点
      5.    【コラム】IoT活用企業におけるプライバシー保護に関する考慮事項とは | PwC Japanグループ
      6.    3-16⇒4-X：IoTを活用する一般利用者のための基本ルール
      7.    【Web版コラム】攻めの姿勢の企業向け
         1.    【コラム】ITの利活用を事業戦略上に位置づけ、 サイバーセキュリティを強く意識し、 積極的に競争力強化に活用しようとしている企業
         2.    【コラム】企業経営のためのサイバーセキュリティの考え方の策定について【NISC】
         3.    【コラム】IT活用の必然性
         4.    【コラム】IT活用のためには、情報セキュリティ対策は必須
         5.    【コラム】次世代サービス、技術の利用に当たってのサイバーセキュリティ対策
    1.    【Web版コラム】サイバーセキュリティ分野で機械学習が活用される背景と期待
    2.    【コラム】サイバー・フィジカル・セキュリティ対策フレームワーク対応
       1. サプライチェーン全体での対策（中小企業向け）
       2.    【コラム】NIST SP800-171 「連邦政府外のシステムと組織における管理された非格付け情報の保護」 改訂Revishon2対応
       3.    【コラム】NIST SP800-53 「連邦政府情報システムおよび連邦組織のための セキュリティ管理策とプライバシー管理策」改訂Rev4.0対応
  1.   【Mission4⇒Mission5】　もしもマニュアル

参照: [【Mission04⇒Mission5】もしもマニュアル](#a_Mission04_Mission5_もしもマニュアル)

* + 1.    4-1⇒5-X：緊急事態応用マニュアルの作成
    2.    4-2⇒5-X：基本事項の決定
    3.    4-3⇒5-X：漏えい・流出発生時の対応
    4.    4-4⇒5-X：改ざん・消失・破壊・サービス停止発生時の対応
    5.    4-5⇒5-X：ウイルス感染時の初期対応
    6.    4-6⇒5-X：届け出および相談
    7.    4-7⇒5-X：大規模災害などによる事業中断と事業継続管理
  1.   【Mission5⇒Mission6】　やってみよう！サイバー攻撃対策シミュレーション

参照: [【MISSION5⇒Mission６】やってみよう！サイバー攻撃対策シミュレーション](#a_MISSION5_Mission__やってみよう_サイバ_攻撃対策シミュレ_ション)

* + 1.    5-1⇒6-X：サイバー攻撃前夜
    2.    5-2⇒6-X：攻撃発生その瞬間
    3.    5-3⇒6-X：サイバー攻撃直後
    4.    5-4⇒6-X：潜入拡大
    5.    5-5⇒6-X：顧客への被害拡大 取引先への被害拡大
    6.    5-6⇒6-X：サイバー攻撃の発覚
    7.    5-7⇒6-X：原因が判明 ウイルス感染が原因
    8.    5-8⇒6-X：再発防止策の作成
    9.    EMOTET、ランサムウェア対策
    10.    6-X：復旧回復
  1.  【MISSION6⇒Mission7】　インフォメーション

参照: [【Mission6⇒Mission7】　インフォメーション](#a_Mission6_Mission7__インフォメ_ション)

* + 1.    6-1⇒7-X：もしかしてサイバー攻撃？ここに連絡を！
    2.    6-2⇒7-X：やられる前に、しっかり予防を！
       1.    「相談・届出先クイックリスト」から抜粋

ドキュメントを参照: <https://bluemoon55.github.io/Presentation_Doc/Cyber/相談・届出先クイックリスト（張り紙用）.pdf>

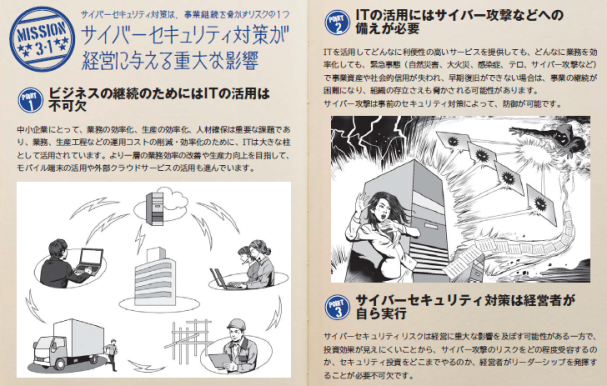
* + 1.    6-4⇒削除：情報セキュリティ用語解説
    2.    6-5⇒7-X：セキュリティお役立ちリンク
       1.    【Web版コラム】セキュリティお役立ちリンク【詳細版】
          1.    主な文献のリストアップと複数文献を典拠とした内容の要約を纏める
       2.    【Web版コラム】サイバーセキュリティ経営チェックシート
       3.    【コラム】IoT機器調査及び利用者への注意喚起プロジェクト（NOTICE対応）
       4.    【Web版コラム】システム管理者としての基本技術の解説
    3.    7-X：経営者向けサイバーセキュリティ経営のための啓発資料
    4.    7-X：中小企業の情報セキュリティ対策ガイドライン【第3版】
       1.   6-6⇒7-X：情報セキュリティポリシーサンプル
       2.   6-3⇒7-X：情報セキュリティ5か条
       3.   3-XX⇒7-X：情報セキュリティ基本方針
       4.   3-17⇒7-X：新・5分でできる自社診断シート
       5.   3-18⇒7-X：情報セキュリティハンドブックひな形（従業員向け）
       6.   3-19⇒7-X：情報セ⇒7-Xキュリティポリシーの明文化
       7.   7-X：情報資産管理台帳の作成
       8.   3-20⇒7-X：リスク分析シート
       9.   3-XX⇒7-X 中小企業のためのクラウドサービス安全利用の手引き
    5.    7-X：IT人材育成・人材確保
       1.    iコンピテンシ・ディクショナリ(iCD)
       2.    情報処理技術者試験制度
    6.    6-4+付-1→7-X：情報管理が不適切などの場合の処罰など
       1.    制度・施策
       2.    関係法令：法律違反の可能性への対応方法の解説
  1.   【付録】

参照: [付録](#付録)

* + 1.    付-2：主な参考文献
       1. 本書で引用した文献名一覧
    2.    付-3：用語解説インデックス
       1. 索引

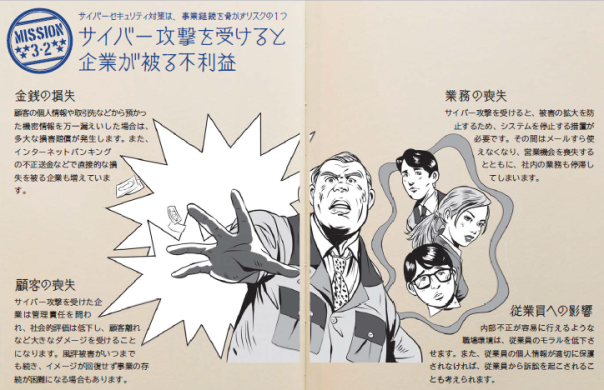
1.  本編ーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーー
   1.  【Mission0】 はじめに
      1.  改版理由
         1.   国の「サイバーセキュリティ戦略」に沿ったセキュリティ対策を実施するために
         2.   NISC等の資料の反映、テレワークの継続化
      2.   ケーススタディー１：なぜ、こんな小さな会社が狙われたの？
      3.   ケーススタディー２：ある日突然、銀行口座の預金残高が消えた！
         1.  人員不足〜以下囲みコラムの平成２７年度 ―平成XX年度の最新に更新
      4.   ケーススタディー３：取引先企業への踏み台にされた
      5.   ケーススタディー４：EMOTET、ランサムウェアの被害にあった？
      6.   ケーススタディー５：サイバーセキュリティ保険に入っていれば
      7.   BEC攻撃事例
      8.   サプライチェーンセキュリティの必要性が高まっていること
      9.   セキュリティ対策を怠ると他社に迷惑をかけることもある
      10.   その他ケーススタディー 新規
          1.   「昨今の産業を巡るサイバーセキュリティに係る状況の認識と今後の取組の方向性について」【2020年6月12日METI】等を参考に。
      11.  改訂箇所：「はじめに」(p.8～9)を改訂
          1.  「サイバーセキュリティ経営ガイドライン・概要＞の説明を全体的に修正。
          2.  IoTやAIの活用といった最近の情勢をふまえる
   2.  【Mission1】　知っておきたいサイバー攻撃の知識
      1.   1-1：標的型攻撃による情報流出
      2.   1-2：ランサムウェアを使った詐欺・恐喝
         1.  【囲みコラム】「No More Ransam」　の紹介
      3.   1-3：Webサービスからの個人情報窃取
         1.  【囲みコラム】割賦販売法の改定とクレジットカードのセキュリティ
      4.   1-4：集中アクセスによるサービス停止
         1.  【囲みコラム】内容更新
      5.   1-5：内部不正による情報漏えいと業務停止
      6.   1-6：Webサイトの改ざん
      7.   1-7：インターネットバンキングの不正送金
      8.   1-8：悪意のあるスマホアプリ
         1.  【囲みコラム】スマートフォン決済不正アプリ
      9.   1-9：巧妙・悪質化するワンクリック詐欺
      10.   1-10：Webサービスへの不正ログイン
          1.  【囲みコラム】不正ログインを…多要素認証の取り込み
      11.   1-11：公開された脆弱性対策情報の悪用
      12.   1-12：IoT機器を踏み台にした攻撃
          1.  【囲みコラム】対策はこれだ…NICT　「NOTICE」の実証事例の結果を追加
      13.   1-13：中小企業におけるサイバー攻撃被害の例
          1.  ＜統計データのアップデート＞
             1.  １．１節「サイバーセキュリティ経営ガイドラインの背景と位置づけ」で 参照している統計データをアップデート。それに伴い説明文も修正。
      14.   1-XX：なりすましECサイトの被害と回避策
          1.  改訂箇所：Mission1-12　(P.41)のあとに追加
          2. 事業者サイド
             1.  ウェブサイト開設等における運営形態の選定方法に関する手引き【2018年5月IPA】

ドキュメントを参照: [000066952.pdf](https://www.ipa.go.jp/files/000066952.pdf)

* + - * 1.  なりすましECサイト対策マニュアル【2015年3月一般社団法人セーファーインターネット協会】
      1. 利用者サイド
         1.  なりすましサイトの見極め方、被害の内容に応じた相談先、届け出先
    1.   1-XX：ビジネスメール詐欺の被害と回避策
       1.  改訂箇所：Mission1-12　(P.41)のあとに追加
  1.  【Mission2】　すぐやろう！対サイバー攻撃アクション
     1.  改訂のポイント
        1. 冊子版は、敢えて改訂する必要があるか？
        2.  EPUB、Web版は、情報セキュリティ10大脅威レベルでリライトするか？
     2.   2-1：サイバー攻撃に対して何ができるか
     3.   2-2：OSとソフトウェアのアップデート
     4.   2-3：ウイルス対策ソフト・機器の導入
     5.   2-4：定期的なバックアップ
     6.   2-5：パスワードの管理
     7.   2-6：アクセス管理
     8.   2-7：紛失や盗難による情報漏えい対策
     9.   2-8：持ち込み機器対策
     10.   2-9：電子メールの安全利用
     11.   2-10：標的型攻撃メールへの対応
     12.   2-11：迷惑メール発信への対応
     13.   2-12：安全なWebサイト利用
         1.  【囲みコラム】詐欺サイトはこれ…内容更新する（NISC,IPAの資料参照）
     14.   2-13：閲覧制限
         1.  【囲みコラム】中小企業の規制は…事例を更新再調査
     15.   2-14：重要情報の洗い出し
     16.   2-15：重要情報の保管
  2.  【Mission03-A⇒Mission3】経営者は事前に何を備えればよいのか【守り】
     1.  サブタイトル【組織維持のために】 経営者、 管理者が、自組織の現状として認識すべきこと
     2. 管理者が知っておくべきこと（管理者を設置していない場合は経営者が自ら知っておくべきこと）
     3. 総論
        1. サイバーセキュリティの被害に遭った場合、 組織の存立が危ぶまれる事態になりえることを自覚する ・世の中で起こっているセキュリティ被害を対岸の火事だと思っている経営者、 ITは導入しているにも関わらずセキュリティ対策のための費用はないとして対策に後ろ向きの経営者、 最も重要な情報にアクセスする権限を持ちながら、 セキュリティに関しての意識の低い経営者。 これらの経営者が最大のセキュリティリスク
        2. 国は、 大企業のみならず、 中小企業も、 「サインバーセキュリティ経営ガイドライン」を参照することを求めている
     4.  サイバーセキュリティ対策は、 事業継続を脅かすリスクの１つ。
        1.  改版理由
           1.   中小企業の情報背キュリティ対策ガイドラインの改版（第２版⇒第３版） 差分を説明する
        2. 組織の社会的責任の認識
        3.    3-1：サイバーセキュリティ対策が経営に与える重大な影響
           1. 
           2. 情報セキュリティ対策は、 経営に大きな影響を与えます！
           3. 経営者が法的・道義的責任を問われます！
           4. 組織として対策するために、 担当者への指示が必要です！

中小企業の情報セキュリティ対策ガイドライン（第3版）【2019年12月19日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/)

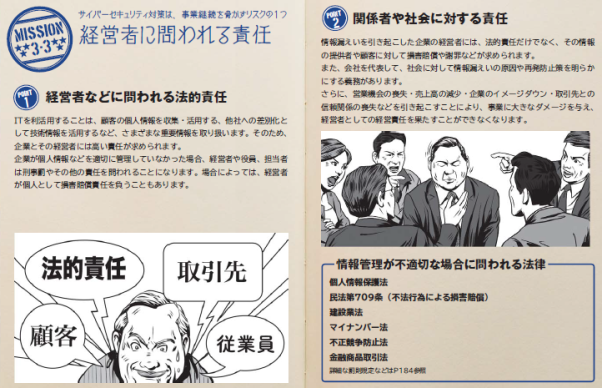
* + - * 1. セキュリティ侵害を受ける70～80%が人為的なミス、 故意
        2. サイバーセキュリティ対策の中で最もコストがかかるのが技術的対策。 しかし全てのリスクに対して技術的対策をすることは困難。 悪意があれば技術的な対策はすり抜けられる
        3. セキュリティー被害を受けた場合、 その被害に対し会社が被る損害の可能性が高い順に投資をすることが重要。
        4. また、 システムを入れる際に、 セキュリティーも同時に入れるなど、 ITとセキュリティー対策を一緒にすることも大切である。
        5. 更に、 経営者を含め、 社員全員に対し、 セキュリティーポリシーやガイドブックを作成したり、 併せてITパスポートの試験を受けさせることも大切である。
      1.    3-2：情報セキュリティ対策を怠ることで企業が被る不利益
         1. 
         2. (1) 金銭の喪失,(2) 顧客の喪失, (3) 業務 の喪失, (4) 従業員 への影響

  Sec01-02-20\_中小企業の情報セキュリティ対策ガイドライン

ドキュメントを参照: <https://bluemoon55.github.io/Sharing_Knowledge3/MindManager3/Sec01-02-20.html>

中小企業の情報セキュリティ対策ガイドライン（第3版）【2019年12月19日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.    3-3：経営者に問われる責任
         1. 
         2. (1) 経営者などに問われる法的責任

・個人情報・他社から預かった秘密情報・自社の秘密情報・株価に影響を与える可能性のある未公開内部情報

* + - * 1. (2) 関係者や社会に対する責任

・営業停止、 売上高の減少、 企業イメージの低下などで、 自社に損害をもたらずだけでなく、 取引先に対する信頼関係の喪失、 業界やサービス全体のイメージダウン・法令順守・顧客・取引先・従業員

 Sec01-02-20\_中小企業の情報セキュリティ対策ガイドライン

ドキュメントを参照: <https://bluemoon55.github.io/Sharing_Knowledge3/MindManager3/Sec01-02-20.html>

中小企業の情報セキュリティ対策ガイドライン（第3版）【2019年12月19日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.    【参考：Web版】
         1.  【参考】情報セキュリティ対策を怠ることで企業が被る不利益 【中小企業の情報セキュリティ対策ガイドライン案】

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

資金の喪失