  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】

1.   改訂履歴
   1.   【2020年8月14日】0.2版提出
2.   凡例
   1.   冊子体及び冊子体ベースWebページ
   2.    既存項目（見出し・項番等の軽微な修正は含む）
   3.    追加項目（大きな修正を含む）
3.    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)
      3.   サイバーセキュリティ2020（2020年7月）
   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.    テレワークの継続化
4.    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
      1.     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？
      2.     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⇒数字のみ修正
      3.     ケーススタディー３：取引先企業への踏み台にされた
         1.    サプライチェーン紹介のページへのリンク
      4.     ケーススタディー４：EMOTET、ランサムウェアの被害にあった？
      5.     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
      6.     ケーススタディーX：BEC攻撃事例⇒海外の取引先からのメール
         1.    海外からのメールを事例に
      7.      ケーススタディーX：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」
         1.   【2020年6月12日METI】等を参考に。
   2.     【はじめに】
      1.   改訂の趣旨を記述
   3.     【この冊子の使い方】
   4.    【目次】
   5.    【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
         1.    2016年の損害額を最新に
      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.    グラフ最新化
         2.    【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（NIST800-63-3対応）
      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】IoTとデータ利活用の全体像【総務省】

ドキュメントを参照: <https://www.soumu.go.jp/ict_skill/pdf/ict_skill_1_1.pdf>

* + 1.     1-13：中小企業におけるサイバー攻撃被害の例
    2.     1-XX：なりすましECサイトの被害と回避策
       1.    事業者サイド
       2.    利用者サイド
    3.     1-XX：ビジネスメール詐欺の被害と回避策
  1.    【Mission2】　すぐやろう！対サイバー攻撃アクション
     1.     2-1：サイバー攻撃に対して何ができるか
     2.     2-2：OSとソフトウェアのアップデート
        1.    OSサポート状況の注記更新
     3.     2-3：ウイルス対策ソフト・機器の導入
     4.     2-4：定期的なバックアップ
        1.    OneDrive等クラウドストレージの利用
     5.     2-5：パスワードの管理
        1.    【囲みコラム】電子的認証に関するガイドライン（NIST800-63-3対応）
     6.     2-6：アクセス管理
     7.     2-7：紛失や盗難による情報漏えい対策
        1.    【囲みコラム】Wifi利用者向け簡易マニュアル【総務省】
     8.     2-8：持ち込み機器対策
        1.    テレワーク等での持ち出し・持ち込み機器対策
     9.     2-9：電子メールの安全利用
     10.     2-10：標的型攻撃メールへの対応
         1.    事例は新規に
     11.     2-11：迷惑メール発信への対応
     12.     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）
     13.     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
  2.     【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】
     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
           1.     【削除】【囲みコラム】情報管理が不適切な場合に問われる法律
     2.     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
           1.    【囲みコラム】数値の見直し
     3.     【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
     4.     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.      【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】
        5.      【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】
        6.      【コラム】電子印鑑の活用
        7.     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
        8.     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

* 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】
     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
           1.    【要旨】DX時代→中小も対応しないと→対応するには新たなセキュリティ対策も
           2.    すでにデジタルトランスフォーメーション(デジタル変革)は始まっている
           3.    「攻めのIT経営中小企業百選」事例⇒ IPAのDXへの取組を取り込む （６月１０日付　「DX推進に向けた文書化公開」参照）
        3.    【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.     【コラム】DXレポート（ITシステム2025年の崖の克服
        4.     3-12～14⇒4-X～X：活用すべき次世代技術要素と活用の留意点
           1.    【要旨】Society5.0とは？インダストリー4.0とは？ クラウドコンピューティング, IoT, ビッグデータ, AI,ロボット,5G等の新たなIT活用が、中小企業においても必要
           2.     3-12⇒4-X：IoT、ビッグデータ、AI、ロボットの活用
           3.     3-13⇒4-X：IoTが果たす役割と効果
           4.     3-14⇒4-X：人工知能（AI）が果たす役割と効果
           5.     【コラム】クラウドサービスの活用
        5.     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
        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
           1.    【要旨】IoT, ビッグデータ, AI, ロボット等の新たなIT活用におけるサイバーセキュリティ対策
           2.     【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
     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）
     3.     【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
     4.     【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
     5.     【削除】おさらいクイズ
  2.   【Mission4⇒Mission5】　もしもマニュアル
     1.    【はじめに】サイバーセキュリティ経営ガイドラインVer.2.0の重要10項目とリンクした表現に
     2.     4-1⇒5-X：緊急事態応用マニュアルの作成
     3.     4-2⇒5-X：基本事項の決定
     4.     4-3⇒5-X：漏えい・流出発生時の対応
     5.     4-4⇒5-X：改ざん・消失・破壊・サービス停止発生時の対応
     6.     4-5⇒5-X：ウイルス感染時の初期対応
     7.     4-6⇒5-X：届け出および相談
     8.     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.     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）
     9.     【削除】ワークショップ
  3.    【Mission5⇒Mission6】　やってみよう！サイバー攻撃対策シミュレーション
     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.     6-X：EMOTET、ランサムウェア対策
     10.     6-X：復旧回復
  4.   【MISSION6⇒Mission7】　インフォメーション
     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！
     3.    6-4⇒削除：情報セキュリティ用語解説
     4.     6-5⇒7-X：セキュリティお役立ちリンク
        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
     5.     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.     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
     6.     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
     7.     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
  5.    【付録】
     1.     付-2：主な参考文献
        1.   典拠となる文献情報の更新
     2.     付-3：用語解説インデックス
        1.   新しい用語の解説及び本文へのリンク