SEC01-08-90\_サイバーセキュリティ対策相談事例

1. 改訂履歴
   1. 2020年1月14日
2. T社【20200115】
   1.  事前に確認しておきたい事項
      1. ●相談のきっかけ
         1. ・きっかけとなったことは？誰にどのようなことを指摘されたのでしょうか？
      2. ●相談内容の列挙に参考にした資料
         1. ・相談内容の項目が多岐に亘っています。何をご覧になってリストアップされたのでしょうか？
      3. ●グループ会社全体のセキュリティ対策状況
         1. ・御社の情報セキュリティ対策の現状は？
         2. ・関連会社、主な取引先等、サプライチェーンを構成する組織のセキュリティ対策の現状と御社の対策のレベルの差はどの程度？目的な差を埋めること？
      4. ●相談者の職務
         1. 情報システム、情報セキュリティの責任者、担当者でしょうか？
      5. ■事前に参照しておいていただきたい資料・情報
         1. 下記の資料を事前に確認しておいていただき、不明な点を相談として対応させていただくことが効率的と思われます。
         2. ●基礎知識として
            1. ・「中小企業向けサイバーセキュリティ対策の極意」

Http://www.sangyo-rodo.metro.tokyo.jp/chushou/shoko/cyber/guidebook/

ドキュメントを参照: [guidebook](http://www.sangyo-rodo.metro.tokyo.jp/chushou/shoko/cyber/guidebook/)

PDF版をダウンロードして、一読しておいていただきたい。

* + - * 1. ・「小さな中小企業とNPO向け情報セキュリティハンドブック」

Https://www.nisc.go.jp/security-site/blue\_handbook/index.html

ドキュメントを参照: [index.html](https://www.nisc.go.jp/security-site/blue_handbook/index.html)

* + - 1. ●相談内容として挙げられた内容の具体的な策定手順、作成ドキュメントのサンプルとして
         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

Https://www.ipa.go.jp/security/keihatsu/sme/guideline/

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

具体的な相談対応として、このガイドラインに沿った手順とサンプル。

* + - * 1. 関連会社のセキュリティ対策内容
  1.  相談内容
     1. ・情報セキュリティ方針と対策の策定
        1. 最高責任者の任命
        2. セキュリティ方針（目指姿）の確定および周知
     2. ・リスク管理とＰＤＣＡの策定
        1. ＰＣのウイルス感染防止への取組み
        2. 機密管理への取組み
        3. 顧客、従業員のマイナンバー情報への取組み
        4. 内部監査もしくは自己診断の定期的な実施
        5. 教育体系の整備（内容、周期）
     3. ・インシデントの対応策定
        1. 発生に対する組織、体制、連絡ルートの確立
     4. ・サプライチェーン管理策定
        1. チェックシートなどでと系列取引先の状況を把握できる仕組み整備
        2. 定期的な監査の実施
  2.  相談回答例
     1. 全般
        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」
        2.  新5分でできる！情報セキュリティ自社診断
           1. 自己評価
     2. ・情報セキュリティ方針と対策の策定
        1. 最高責任者の任命
           1.  「情報セキュリティ関連規程（サンプル）」

１．組織的対策

* + - 1. セキュリティ方針（目指姿）の確定および周知
         1.  「情報セキュリティ関連規程（サンプル）」を参考にセキュリティポリシーの策定
         2.  「情報セキュリティハンドブック（ひな形）」の作成
    1. ・リスク管理とＰＤＣＡの策定
       1. ＰＣのウイルス感染防止への取組み
          1.  「情報セキュリティ5か条」の遵守
       2. 機密管理への取組み
          1.  「情報セキュリティ関連規程（サンプル）」

４．アクセス制御及び認証

９．委託管理

* + - 1. 顧客、従業員のマイナンバー情報への取組み
         1.  「情報セキュリティ関連規程（サンプル）」

１１．個人番号及び特定個人情報の取扱い

* + - 1. 内部監査もしくは自己診断の定期的な実施
         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」

第2部実践編

4.本格的に取り組む

(5)点検と改善

5.より強固にするための方策

(4)セキュリティサービス例と活用

情報セキュリティサービス基準審査登録制度

③情報セキュリティ監査サービス

* + - 1. 教育体系の整備（内容、周期）
         1.  「情報セキュリティ関連規程（サンプル）」

2．人的対策

* + 1. ・インシデントの対応策定
       1. 発生に対する組織、体制、連絡ルートの確立
          1.  「情報セキュリティ関連規程（サンプル）」

１０．情報セキュリティインシデント対応ならびに事業継続管理

* + 1. ・サプライチェーン管理策定
       1. 全般
          1.  サイバーセキュリティ経営ガイドライン Ver 2.0【2017年11月16日METI】

III．サイバーセキュリティ経営の重要１０項目

指示９：ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握

付録Aサイバーセキュリティ経営チェックシート

* + - * 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」

第 1部 経営者編

3.経営者は何をやらなければならないのか

(1)認識すべき「３原則」

原則２ 委託先における情報セキュリティ対策まで考慮する

* + - * 1. 情報セキュリティ10大脅威2019【IPA】

サプライチェーンの弱点を悪用した攻撃の高まり

* + - 1. チェックシートなどでと系列取引先の状況を把握できる仕組み整備
      2. 定期的な監査の実施
  1.  参考情報
     1.  サイバーセキュリティ経営ガイドライン Ver 2.0【2017年11月16日METI】
     2.  「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. 第1部　経営者編
        2. 第2部　実践編
        3. 付録1：「情報セキュリティ５か条」
        4. 付録2：「情報セキュリティ基本方針（サンプル）
        5. 付録3：「５分でできる！情報セキュリティ自社診断」
        6. 付録4：「情報セキュリティハンドブック（ひな形）
        7. 付録5：「情報セキュリティ関連規程（サンプル）
        8. 付録6：「中小企業のためのクラウドサービス安全利用の手引き」
        9. 付録7：「リスク分析シート」