Sec01-01-04\_「中小企業向けサイバーセキュリティ対策の極意」(第2版)【追補および解説】

<https://bluemoon55.github.io/Sharing_Knowledge3/MindManager3/Sec01-01-04.html>;

1. 改版履歴
   1. 2021年4月16日サイバーセキュリティ経営ガイドライン [Ver.2.0]【METI/IPA】参照
   2. 2021年4月15日初版：「情報資産台帳の作成と詳細リスク分析」初稿
2. 参考資料
   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. サイバーセキュリティ経営ガイドライン [Ver.2.0]（経済産業省/IPA）
   3. 情報技術－セキュリティ技術－情報セキュリティマネジメントシステム
      1. JISQ 27001（ISO/IEC 27001）要求事項
      2. JISQ 27002（ISO/IEC 27002）情報セキュリティ管理策の実践のための規範
         * JISQ27017（ISO/IEC 27017）－JISQ 27002 に基づくクラウドサービスのための情報セキュリティ管理策の実践の規範
   4. 情報セキュリティマネジメント試験
      1. 情報セキュリティマネジメントに要求される知識と技能【シラバス】（Bib05-13）

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/Bib05-13.html>;

1. 

情報資産台帳の作成と詳細リスク分析（Mission6-4追補原稿）

* 1. 

概要

* + 1. 事業規模が大きくなったり、情報システムが複雑になると、想定外のリスクを見落とし、対策が不十分になることがあります。そこでここでは、もれなくリスクを特定し、対策を検討する手法
  1. 

手順1 情報資産の洗い出し

* + 1. 

●情報資産管理台帳の作成

* + - * 情報資産管理台帳は洗い出した情報資産を「見える化」するための方法の一つ



* + - * 記載項目
        + 情報資産諸元

業務分類

情報資産名称

備考

利用者範囲

管理部署

媒体・保存先

個人情報の種類

個人情報

要配慮個人情報

特定個人情報

保存期限

登録日

* + - * + 評価値

機密性

完全性

可用性

* + - * + 重要度
        + 現状から想定されるリスク

脅威の発生頻度

※「脅威の状況」シートに入力すると自動算出

脆弱性

※「対策状況チェック」シートに入力すると自動算出

被害発生可能性

リスク値

* + 1. 

●情報資産ごとの機密性・完全性・可用性の評価

* + - * 機密性
        + アクセスを許可された者だけが情報にアクセスできる
        + 機密性レベル２

法律で安全管理（漏えい、滅失又はき損防止）が義務付けられている

守秘義務の対象や限定提供データ12 として指定されている

漏えいすると取引先や顧客に大きな影響がある

自社の営業秘密として管理すべき（不正競争防止法による保護を受けるため）漏えいすると自社に深刻な影響がある

* + - * + 機密性レベル１

漏えいすると業務に大きな影響がある

* + - * + 機密性レベル０

漏えいしても業務にほとんど影響はない

* + - * 完全性
        + 情報や情報の処理方法が正確で完全である
        + 機密性レベル２

法律で安全管理（漏えい、滅失又はき損防止）が義務付けられている

改ざんされると自社に深刻な影響または取引先や顧客に大きな影響がある

* + - * + 機密性レベル１

改ざんされると業務に大きな影響がある

* + - * + 機密性レベル０

改ざんされても事業にほとんど影響はない

* + - * 可用性
        + 許可された者が必要な時に情報資産にアクセスできる
        + 可用性レベル２

利用できなくなると自社に深刻な影響または取引先や顧客に大きな影響がある

* + - * + 可用性レベル１

利用できなくなると事業に大きな影響がある

* + - * + 可用性レベル０

利用できなくなっても事業にほとんど影響はない

* + 1. 

●機密性・完全性・可用性の評価値から重要度を算定

* + - * 情報資産の重要度の判断基準
        + 重要度レベル２

機密性・完全性・可用性評価値のいずれかまたはすべてが「2」の情報資産

* + - * + 重要度レベル１

機密性・完全性・可用性評価値のうち最大値が「1」の情報資産

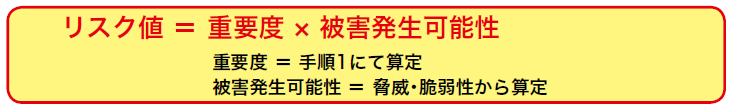
* + - * + 重要度レベル０

機密性・完全性・可用性評価値すべてが「0」の情報資産

* 1. 

手順２ リスク値の算定

* + 1. 優先的・重点的に対策が必要な情報資産を把握する
       - 洗い出した情報資産について、対策の優先度を決めるため、リスク値（リスクの大きさ）を算定
    2. リスク値＝重要度×被害発生可能性



* + 1. 「被害発生可能性」
       - 「被害発生可能性」は「脅威の起こりやすさ」と「脆弱性のつけ込みやすさ」の２つの数値から算出
       - 脅威の起こりやすさ
         * 脅威レベル３

通常の状況で脅威が発生する（いつ発生してもおかしくない）

* + - * + 脅威レベル２

特定の状況で脅威が発生する（年に数回程度）

* + - * + 脅威レベル１

通常の状況で脅威が発生することはない

* + - * 脆弱性のつけ込みやすさ
        + 脆弱性レベル３

対策を実施していない（ほぼ無防備）

* + - * + 脆弱性レベル２

部分的に対策を実施している

* + - * + 脆弱性レベル１

必要な対策をすべて実施している

* + - * 被害発生可能性
        + 被害発生可能性=脅威レベル÷（4－脆弱性レベル）



* + - * + 被害発生可能性レベル３

通常の状況で被害が発生する（いつ発生してもおかしくない）

* + - * + 被害発生可能性レベル２

特定の状況で被害が発生する（年に数回程度）

* + - * + 被害発生可能性レベル１

通常の状況で被害が発生することはない

* 1. 

手順３ 情報セキュリティ対策を決定

* + 1. リスクの大きな情報資産に対して必要とされる対策を決める
    2. リスク対策の分類
       - リスクを低減（リスクの発生確率を下げる対策）
         * 情報セキュリティ対策を導入ないし強化することで、脆弱性を改善し、事故が起きる可能性を下げる
         * 例：重要な情報へのアクセス制御、ソフトウェアの更新の徹底
       - リスクを回避（リスクが発生する可能性を除去する対策）
         * 仕事のやりかたを変える、情報システムの利用方法を変えるなどして、想定されるリスクそのものをなくす
         * 例：端末の持ち出し禁止 （外部での盗難のリスクを回避）
       - リスクを移転（リスクを他者等の移す対策）
         * 自社よりも有効な対策を行っている、あるいは補償能力がある他社のサービスを利用することで自社の負担を下げる
         * 例：クラウドサービスの利用、サイバー保険の加入
       - リスクを保有（残留リスクとして識別）
         * 事故が発生しても許容する
         * あるいは対策にかかる費用が損害額を上回る場合などは対策を講じず、現状を維持する
  1. 

参考資料

* + 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【IPA】

* + - * 第2部実践編
        + より強固にするための方策

詳細リスク分析の実施方法

* + 1. 

サイバーセキュリティ経営ガイドライン [Ver.2.0]【METI/IPA】

* + - * サイバーセキュリティ経営の重要10項目
        + 指示4：サイバーセキュリティリスクの把握とリスク対応に関する計画の策定