## **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

## **手順1 情報資産の洗い出し**

* 1. 業種、事業内容、IT環境によって保有する情報資産は異なるため、自社の情報資産を一通り洗い出し、情報資産ごとの機密性・完全性・可用性を評価し、それぞれの評価値から重要度を算定する
  2.  ●情報資産管理台帳の作成
     1. 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



* + 1. 情報資産諸元
       - ①業務分類
         * 情報資産に関連する業務や部署名を記入します。情報資産は業務に関連して発生しますので、まず関連業務や部署を特定し、その業務や部署で利用している情報を洗い出すと記入漏れが少なくなります。
       - ②情報資産名称
         * 情報資産の内容を簡潔に記入します。正式名称がないものは社内の通称で構いません。管理方法や重要度が同じものは1行にまとめます。
       - ③備考
         * 必要に応じて説明等を記入します。
       - ④利用者範囲
         * 情報資産を利用してよい部署等を記入します。
       - ⑤管理部署
         * 情報資産の管理責任がある部署等を記入します。小規模事業者であれば担当者名を記入しても構いません。
       - ⑥媒体・保存先
         * 情報資産の媒体や保存場所を記入します。書類と電子データの両方で保存している場合は、それぞれ完全性・可用性（機密性は同一）や脅威・脆弱性が異なるので2行に分けて記入します。 例）見積書「電子データを事務所PC に保存」「印刷して書類を保管」
       - ⑦個人情報の種類
         * 各項目が個人情報保護法、マイナンバー法で定義されています。
       - ⑧重要度
         * 重要度定義シートまたは中小企業の情報セキュリティ対策ガイドラインP.45表10を参照して、情報資産の機密性、完全性、可用性それぞれの評価値を記入します。3種類の評価値から中小企業の情報セキュリティ対策ガイドラインP.46表11に基づき重要度が表示されます。なお、⑦でいずれかの個人情報が「有」の場合、重要度は自動的に「2」となります。
       - ⑨保存期限
         * 法定文書は法律で定められた保存期限を、それ以外は利用が完了して廃棄、消去が必要となる期限を記入します。
       - ⑩登録日
         * 登録した日付を記入します。内容を更新した場合は更新日に修正します。
  1.  ●情報資産ごとの機密性・完全性・可用性の評価
     1. 機密性、完全性、可用性が損なわれた場合の事業への影響や、法律で安全管理義務があるなど、評価基準を参考に評価値２～０を記入します。
     2. 評価
        + レベル
          - 内容
     3. 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
     4. 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
     5. 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
  2.  ●機密性・完全性・可用性の評価値から重要度を算定
     1. 重要度は、機密性、完全性、可用性いずれかの最大値で判断します。 「情報資産管理台帳」に記入した機密性・完全性・可用性の評価値をもとに、判断基準に従い、重要度を算定します。
        + ※下記の場合は、算定結果に関わらず、重要度は２とします。
          - 企業の存続を左右しかねない場合

事故が起きると法的責任を問われる

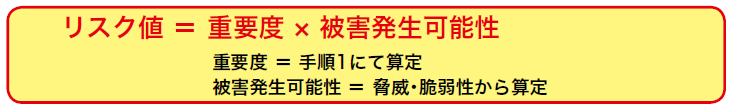
取引先、顧客、個人に大きな影響がある

事業に深刻な影響を及ぼす

* + - * + 個人情報を含む場合
    1. 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

## **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
     1. 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」
     1. 「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
     2. 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
     3. 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
     4. 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

## **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
     1. 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
     2. 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）
     3. 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
     4. 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

## **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】
     1. 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
  2.  サイバーセキュリティ経営ガイドライン [Ver.2.0]【METI/IPA】
     1. 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