情報セキュリティ

ISMS：組織で情報資産を守る・管理するためのフレームワーク

- フレームワーク：何かを実現するための手順やルールなどを纏めたもの
  - 「何」を実現？：「きちんと情報を守ること」
- 作成者：ISO/IEC 27001
  - 情報セキリティに関しての成功事例をまとめ、各国や企業がそれを基にセキュリティの仕組みを構築できるように作られました
- 実際の流れ
  - ISO/IEC 27001の要件に基づき、情報を守るためのポリシー、手順、仕組み（フレームワーク）を社内で整備（ISMSの元の作成）
  - 審査
    - 認証されれば、社内独自の情報セキュリティの仕組み(社内ISMSの運用)の作成が完了したことになる
    - 認可されなければ、きちんとセキュリティを守ることができていないということになる
  - 認証を受けたISMSを外部サイトなどでに公開する
    - その会社の情報セキュリティは信頼することができるものと示すことができる。これで第三者から見ても安心して利用できるということがわかるようになる
- 情報資産：ヒト・モノ・カネの情報のこと
- JIS Q No.27001

CIA：ISMSで記載された、情報セキュリティの定義

- C 機密性：情報を許可されたものだけがアクセスできる状態を維持すること。要は不正ログインなど本人でない第三者に情報を知れらることを防ぐためのもの
- I 完全性：規則で定められた特定の操作以外で情報が変化することがない性質のこと
  - 情報の変化：情報の改竄、削除、追加など
- A 可用性：情報をいつでも使用できる状態にしておくこと
  - 対策としてサーバーなどをダウンさせない、故障させないなどの仕組みを事前に作っておくこと

追加要素

- 真正性：指紋や目の虹彩など生体認証による、間違いない本人を認証する性質
- 責任追求性：ログを取得するなど、誰の責任なのかを追跡できるようにしておく性質
- 信頼性：決められた操作で、故障や矛盾のない意図した結果になる性質のこと。要は操作とその結果に一貫性があること
- 否認防止：デジタル署名などの証明により、作成したものが本人であることを否定させないようにすること
-

情報セキュリティポリシー

- 情報資産を脅威から守るために作成する
- 構成
  - 基本方針：経営者が作成する

        - **組織や情報資産を保護するための取り組みである情報セキュリティの目標**や、それを実現するための**行動の方向性**、さらにはその行動を実施する際の**手順や守るべきルール**を包括的に示した文書のこと以下は基本方針の一例
            - 我が社で情報を守ることの必要性
            - どんな方向性で情報を守っていくのか
            - 顧客情報などのプライバシーな情報をどう取り扱うのか
              どんなセキュリティ
        - 社内外で共有をする
    - 対策基準：基本方針実現のため、何を実施するのか？
        - セキュリティ対策を何を基準として実施するのか
        - 対策を行うであろう特定の状況・条件とその対策を記載する
            - 対策を実施するための基準は定量・定性、どちらも当てはまる
        - 公開する対策基準は一般的な規定のみを記述すること
            - 一般的な規定：業界全体でよく知られ、共通的に認識され適用される普遍的な対策や成功事例のこと
                - 一例

                  規定: パスワードの最低文字数を８文字以上とし、大文字、小文字、数字、特殊文字を含むこと。

                  対策: 従業員が簡単なパスワードを設定しないようにポリシーで自動強制する。
            - なぜ一般的な規定のみであるかの理由
                - 会社特有のものを公開すれば、それは企業秘密で企業争いで優位に立つ部分になりうる可能性がある
    - 実施手順：対策基準で設けた対策の具体的な手順を記載していく
        - 対策基準側では大まかなものしか書いていないので、細かく手順を記載していく

企業で一般的でない、企業特有の問題に対しての

明文化：言葉で明確に表現したものを文書として記録すること
社内の情報共有、議事録や契約書など後々確認する可能性がある時に効果がある

基本方針は、**組織やプロジェクト、事業活動が達成しようとする目的**や、それを実現するための**行動の方向性**、さらにはその行動を実施する際の**手順や守るべきルール**を包括的に示したものです。

「行動の方向性」は、全体の目標（目的地）に従い、どのような道（行動）を選ぶべきかを示しています。
示すのみであり、具体的な行動については記載なし