INSec#13 管理・開発・運用

情報セキュリティマネジメント

サイクル
- Plan → Do → Check → Action
- 情報システム：企画 → 開発 → 運用

Point
- 1.情報セキュリティを対象とした経営管理活動
  - 経営と組織体の理解
  - 指揮命令系統に横断的なマネジメント機能を組み込み・機能させる
- 2.リスクマネジメント
- 情報セキュリティマネジメントシステム(ISMS)

組織
- 経済産業省：情報セキュリティ管理基準 （平成20年改正版） → http://www.meti.go.jp/policy/netsecurity/downloadfiles/IS_Management_Standard.pdf
- 日本情報経済社会推進協会(JIPDEC) → http://www.isms.jipdec.jp/index.html
  - 日本でのISMS推進母体

情報セキュリティ (information security)
→情報の機密性、完全性および可用性を維持すること。さらに、真正性、責任追跡性、否認防止および信頼性のような特性を維持することを含めてもよい。

要素
- 3大要素から6要素・7要素へ(2006年改定)：JIS Q 27002:2006 および JIS Q 13335-1
- エンティティ(entity)：情報資源、データ資源として管理すべき対象のこと。実体。
  - 利用者
  - プロセス
  - システム
  - 情報
  - …
- 機密性(confidentiality)
  - 許可されていない個人、エンティティまたはプロセスに対して、情報を使用不可または非公開にする特性
  - 前：認可されたものだけが情報にアクセスされることを確実にすること
- 完全性(integrity)
  - 資産の正確さ及び完全さを保護する特性
  - 前：正確であることおよび完全であることを保護すること
- 可用性(availability)
  - 許可されたエンティティが要求したときに、アクセス及び使用が可能である特性
  - 前：認可されたユーザが、必要時に情報及び関連財産にアクセスできることを確実にすること
- 真正性(authenticity)
  - ある主体または資産が、主張どおりであることを確実にする特性。真正性は、利用者、プロセス、システム、情報などのエンティティに対して適用する。
  - 前：ユーザ、システムによる振る舞いが明確であること。なりすましや偽の情報ないことが証明できること
- 責任追跡性(accountability)
  - あるエンティティの動作が、その動作から動作主のエンティティまで一意に追跡できる事を確実にする特性
  - 前：ユーザやサービスの行動、責任が説明できること。ユーザIDなどで、システム上での行動を説明できるように扱うこと(主にログ)。
- 否認防止(non-repudiation)
  - ある活動又は事象が起きたことを、後になって否認されないように証明する能力
  - 前：ユーザやサービスの行動を、後になって否認されないように証明できること
- 信頼性(reliability)
  - 意図した動作及び結果に一致する特性
  - 前：システムやプロセスが矛盾なく動作すること、一貫して動作すること

リスクマネジメント

セキュリティマネジメント

リスクアセスメントとリスク対応

情報セキュリティポリシーの作成
体系の考え方
- 1.経営理念(Mission of society)：憲法前文
- 2.基本方針(Policy)：憲法
  - 例
    - 1.目的
    - 2.用語の定義
    - 3.適用範囲
    - 4.位置付け
    - 5.セキュリティ対策方針
    - 6.対策の基本原則
    - 7.組織体制、責任と権限
  - 原則
    - 1.知る必要性の原則：業務上必要となる権限のみ付与
    - 2.最小特権の原則：特権は必要最小限に付与
    - 3.リスク評価の原則：セキュリティ対策は適切なリスク評価を行って実施
    - 4.例外管理の原則：予算上、物理的制限などのために実施できない項目は例外事項として別途管理
- 3.基本規程(Why, Who, What)：法律：情報セキュリティ違反 → 罰則規定の取り扱い
- 4.基準／個別規程(Standards, Particulars)：施行規程
  - 情報セキュリティマネジメントに関する項目
  - 具体的なセキュリティ対策に関する項目
- 5.指針(Guidance to how)：通達
- 6.運用規則(How)：条例：業務手順書：現場レベルでの実施
  - 情報セキュリティを確保するための業務
  - 通常の業務に情報セキュリティについての手順を組み込んだ業務

有効性の測定
目的：実施した活動が予定した成果を出しているかについて確認（定量的に！）

考え方
- 1.期待した成果(Outcome)に対する、実際の成果(Outcome)の比率：達成度
- 2.期待した結果(Output)に対する、実際の結果(Output)の比率：実施度
- 3.投入した資源(Input)に対する、実際の成果(Outcome)の比率
- ↑ 成果(Outcome)：目的の達成そのもの
- ↑ 結果(Output)：目標達成につながる手段の実施の程度

有効性
- 1.情報セキュリティマネジメントシステム全体の有効性
- 2.セキュリティ対策(統制活動)の有効性

情報セキュリティ監査
日本セキュリティ監査協会 → http://www.jasa.jp/

目的
- 情報セキュリティに係わるリスクのマネジメントが効果的に実施されているか？
- リスクアセスメントに基づく適切なコントロールの整備、運用状況を検証・評価 → 保証、助言

種類
- 1.保証型監査：監査対象と判断尺度が一致していることを保証
- 2.助言型監査：監査対象と判断尺度との間のギャップを検出事項として指摘
- 3.合意された手続き：選択された検証手続きのみの結論報告

枠組み
- 監査の依頼者(利害関係者)、監査対象組織、監査主体との独立性
- 外観上の独立性と精神上の独立性

実施
- 1.監査基本計画の立案：目的を受け、対象範囲、対象期間、スケジュール等
- 2.監査実施計画の立案：具体的な監査手続きについての詳細計画
- 3.監査手続きの実施：技法
  - 1.質問：関係者に口頭で問い合わせ、説明や回答を求める
  - 2.閲覧：規程、手順書、記録を調査
  - 3.観察：監査人自らが現場に赴き、目視確認
  - 4.再実施：監査人自らが現場に赴き、コントロールの妥当性や適否を確認
- 4.監査調書の作成と保管：監査の結論に至った過程が重要であり、情報漏えいに留意

監査報告書
- 種類
  - 1.保証型監査報告書
  - 2.助言型監査報告書：内容：例
    - 検出事項があるものの、当面、緊急かつ重要な影響は予想されない
    - 検出事項を除いて、重要な問題はない
    - （総括、総合所見、総合意見として）重要な問題は発見されなかった
  - 3.合意された手続きに基づく報告書
- 記載区分
  - 1.導入区分：実施した監査対象
  - 2.概要区分：実施した監査の内容
  - 3.意見区分：保証意見または助言意見
  - 4.特記区分：その他特記すべき事項
- 意見の種類
  - 1.肯定意見：判断の尺度に準拠していると認められる
  - 2.限定的肯定意見：判断の尺度から逸脱があるが、その逸脱を除けば準拠していると認められる
  - 3.否定意見：判断の尺度から逸脱が大きく、準拠しているとは認められない

セキュア開発

セキュリティ運用

コンプライアンス