- INSec#11
  管理・開発・運用
  - 情報セキュリティマネジメント
  - セキュア開発
  - セキュリティ運用
    - 運用設計
      - 運用ポリシー
        - ネットワークのアクセス制限
        - サーバのアクセス制限
        - アカウント管理
        - ログ管理
      - 運用要件
        - 1.職責の分離
        - 2.作業の追跡性(トレーサビリティ)
        - 実装項目
          - アカウント管理
          - アクセス制御
          - ログ管理
          - 監視
          - セキュリティ管理
          - バックアップ・リストア
      - セキュリティ監査
      - ユーザへのセキュリティ啓発
    - 運用
      - アカウント管理
        - アカウントとユーザは１対１
      - アクセス制御
        - 「職責の分離」をシステムに適用
      - ログ管理
        - インシデントレスポンスにおける重要な情報
        - 分類
          - システムログ
          - アプリケーションログ
          - トラフィックログ
          - 監査ログ
          - セキュリティログ
        - 集中管理
          - SIM(Security Information Manager) or SEM(Security Event Manager)
          - ↑セキュリティデバイスが発生するイベントログの集中管理を行うシステム
          - 実装
            - ・ログ収集用アプリケーション(エージェント)をシステムにインストール→SIMサーバにログ収集
            - ・システムから既存の通信(Syslog, FTP…)を使い、SIMサーバにログ転送
        - 保存期間
          - ログ
            - １か月-ハードディスク
          - アーカイブされたログ
            - ３か月-外部ハードディスク
          - 保管されたログ
            - ３年-ROMメディア
      - 監視
        - 監視カテゴリと監視対象：
        - 性能監視
          - システム資源
        - 稼働監視
          - サービス
        - セキュリティ監視
          - 通信、ファイルシステムへのアクセス
        - トラフィック監視
          - トラフィック量
        - ↑監視システムと監視対象システムは別のコンポーネント
      - セキュリティ管理
        - システムの脆弱性
          - 設計の不備
          - 構築・設定の不備
          - ソフトウェアの設計ミス・バグ
          - 人
        - パッケージ・ソフトウェア依存
          - パッチの適応サイクル
            - 1.パッチのリリース
            - 2.テスト環境へのパッチ適用、システムの動作確認
            - 3.本番環境へのパッチ適用
        - 脆弱性情報
          - SecurityFocus → http://www.securityfocus.com/
          - JVN Pediai → http://jvndb.jvn.jp/
          - JPCERT/CC → http://www.jpcert.or.jp/
          - US-CERT → http://www.us-cert.gov/
      - バックアップ・リストア
        - ソフトウェアへのパッチ適用作業
          - パッチ適用時のシステム障害に備える
        - バックアップ種類
          - フルバックアップ
            - 初期構築時
          - 増分バックアップ
            - 更新ファイル
          - 差分バックアップ
            - 常に基準となるバックアップからの更新ファイル
          - ↑世代管理
      - インシデントレスポンス
        - → インシデントの検知から収束までの一連の対応プロセス
        - 対応フロー
          - 検知
            - インシデント検知から対応開始までのプロセス
          - 対応
            - インシデント対応を実施するプロセス
          - 事後対応
            - インシデントが収束し、インシデントレスポンスのレビューを実施するプロセス
        - インシデントレスポンスチーム(IRT) or Computer Security Incident Response Team(CSIRT)
        - → http://www.atmarkit.co.jp/fsecurity/rensai/inci01/inci01.html
        - 日本シーサート協議会
          - 日本コンピュータセキュリティインシデント対応チーム協議会
          - → http://www.nca.gr.jp/
      - 検知
        - ↓「インシデントらしき」事象の検知
        - 監視
        - ログ監査
        - 組織内外からの通報
          - 通報者がインシデント公開の危険性
      - 対応
        - 流れ
          - 1.IRTの招集・対応フローの確認
            - システム運用者がIRT活動 → 運用業務を行わない → インシデント対応に専念
          - 2.被害範囲の特定・拡大防止措置
            - ホスト単体停止 → サブネット停止
            - 必要最小限の措置を早急に実施
          - 3.関係各所への第一報連絡
            - ・インシデント発生日時
            - ・内容
            - ・影響範囲
            - ・今後の対応方針
            - ・連絡方法
          - -4.インシデント環境の保存・複製
            - 訴訟も視野に入れたエビデンス確保
            - コンピュータフォレンジック(computer forensics)
              - デジタル鑑識
            - → 不正アクセスや機密情報漏洩などコンピュータに関する犯罪や法的紛争が生じた際に、原因究明や捜査に必要な機器やデータ、電子的記録を収集・分析し、その法的な証拠性を明らかにする手段や技術の総称
          - -5.原因調査
            - ログ管理
          - -6.復旧措置
            - バックアップからリストア
              - いつのバックアップから？
          - 7.関係各所への復旧連絡
            - ・インシデントの発生原因
            - ・インシデントへの対策
      - 事後対応
        - ↓同様のインシデント再発防止
        - ・インシデントレスポンス対応フローの見直し
        - ・セキュリティ対策・運用フローの見直し
  - コンプライアンス