INSec#1
情報とシステムへの脅威とリスク

- 情報への脅威とその変遷
  - 脅威（インシデント）
    - 主体
      - 物理的インシデント
      - セキュリティインシデント
      - コンテンツインシデント
    - 手段や理由
  - リスク
    - …被害を受ける可能性
    - 被害を受ける可能性を生じさせるもの＝「脅威」（インシデント）
  - 例えば
    - スパイ
      - 暗号
        - 徳川時代の薩摩弁（正確には大隅方言）
    - 第二次世界大戦
      - 日本の暗号
      - ドイツの暗号機（エニグマ）
    - 米国のウォーターゲート事件
  - コンピュータシステムへの侵入
    - パスワードを破る
      - 直接
      - 電話回線
  - コンピュータの一般的利用
    - 攻撃のためのコンピュータ利用
    - デジタル媒体(FD,MO,CD,DVD)でウイルス配布
  - インターネットの発達
    - セキュリティホールへの攻撃
      - OS
      - OS以外のソフトウェア
    - コンピュータウイルスが翼を！
      - 電子メールで自らを複製し配布
      - ソフトウェアの脆弱性を自動的に攻撃
        - 侵入後に複製、次の攻撃先検索
        - コンピュータワーム
- 外的脅威の変化
  - 目的の変化
    - 興味本位、自己顕示から
      - Webページの改ざん →
        - ・その成功を誇示
      - マルウェアの流布→
        - ・ウイルス対策を出し抜く、早く大量感染
        - ・発生時のインパクト
    - 悪意、営利目的に
      - 犯罪組織の資金源
        - マルウェアや不正アクセスの技法の販売
        - ポットのスパム業者への貸し出し
      - ファイル交換ソフトによる情報流出
        - Winny、Share等を通して
        - Antinnyウイルス：暴露ウイルス
          - 感染の9割以上日本語版Windows
      - 自己顕示欲以上の社会に対する悪意を持った攻撃
  - 攻撃対象の変化
    - 特定の相手に絞られた、静かな攻撃
      - 特定の相手→
        - 誰もが標的：企業、機関、個人
      - 静かな攻撃→
        - 利用者に気付かれないよう
          - トロイの木馬：rootkitの実装
      - 攻撃の踏み台サーバ
        - Webサイト改ざん
          - マルウェアをダウンロードさせるスクリプトの仕込み
        - 電子メールの添付から、現在の主流へ
      - OSの脆弱性より、アプリケーションの脆弱性攻撃
  - 攻撃方法の変化
    - マルウェアによる攻撃と複合型の脅威
      - マルウェア→
        - Malicious Software（悪意のあるソフトウェア）
        - ※ 不正なソフトウェアの総称
        - ウイルス
        - ワーム
        - スパイウェア
        - トロイの木馬
        - etc.
      - マルウェア感染を引き起こす手法の技術的確立可
        - ファイアウォールの無効化
        - 電子メールによる媒体
        - ネットワーク経由の進入
        - Webサイトからのダウンロード
      - 攻撃手法の集大成による、複合型脅威
    - 心理的手法による攻撃
      - SNSによる個人の趣味・興味から
      - 振り込め詐欺
      - フィッシング
- 内的脅威とその対策
  - 悪意と不注意
    - 組織内部者
      - 悪意
      - 不注意
      - 怠慢
      - 無知
    - 業務上の支障が生じない対策、ルール化
    - ルールを緩める代わりにチェック強化
  - ルール化とモニタリング
    - 情報セキュリティ管理のためにはルール作りが不可欠
    - ルール自身が適切か？ → 常にモニタリング
    - 主体とは独立：監査、主体：モニタリング
    - モニタリングの方法
      - アクセスログ
      - 利用ルールのチェック
      - 入退室記録管理
    - PDCAサイクルで利用者にフィードバック
  - システムによる制御と統制
    - ルールを順守
      - パスワード管理
      - アクセス制御
      - バックアップ管理
    - ルールの啓蒙活動
- 脅威（インシデント）とリスク、脆弱性
  - 脅威（インシデント）とリスク
    - 直接的な損失の原因となるリスク要因
    - -個人情報漏洩
    - -Webサイトの停止
    - -業務効率低下
    - ※ 脅威に対してどの程度弱いか？　強いか？
    - 風評被害
    - リスクの大きさは、「脅威の強さ」と「脆弱性の大きさ」に相関する
- 情報システムの脆弱性
  - 機器やソフトウェアが内包するセキュリティ上の弱点そのもの
  - 脆弱性が含まれる対象
    - ハードウェア＆ファームウェア
    - ソフトウェア
    - これらが組み合わされたシステム
  - 脆弱性によって生じる問題
    - システム機能・データへの不正なアクセス（読み取り、変更、破壊等）
    - 意図しない情報の暴露
    - 不正なプログラムの実行
    - システム制御兼の奪取
    - 他システム攻撃への踏み台利用…加害者！
  - 脆弱性が発生する原因
    - プログラム上のバグ
    - 不正な操作
    - データ管理、アクセス制御の不備
    - システム上の問題