インターネット社会の安全対策

- 入門
  - 何歳からの対策？
    - 2009年まで
      - インターネットに繋がるPCが操作できる年齢
        - キーボード入力のため
      - 9～10歳：小学校４年生…「ローマ字」を習う学年
        - 新指導要領では小学校３年生
      - 無線LAN対応ゲーム機の発売まで
        - 2009年11月SONY PSPgo販売開始
        - ゲームカートリッジなし、オンラインソフトのみ
    - 2010年以降
      - ３歳から！
        - ゲーム機を操作できる年齢
        - Wi-Fi等でインターネット接続
        - 2012年8月：ドラゴンクエストX発売
          - オンラインゲーム
          - 30日：千円
      - 14歳から刑事告訴
        - 刑法としての著作権法
        - 2007年少年法改定：少年院送致年齢→おおむね12歳以上
  - 安全対策：情報セキュリティ
    - 定義：情報セキュリティ(Information Security)
      - ISO/IEC 27001:2005(JIS Q 27001)
      - 情報の機密性，完全性及び可用性を維持すること．更に，真正性，責任追跡性，否認防止及び信頼性のような特性を維持することを含めてもよい
    - セキュリティの３要素
      - 機密性（紙媒体と情報システム）：　レベル1・2・3
        - 情報の重要度
      - 完全性（情報システム）：　レベル1・2
        - 性能の保証
      - 可用性（情報システム）：　レベル1・2
        - バックアップと復旧
    - 脅威(インシデント)とリスク
      - 情報資産に対しての脅威(インシデント)
        - 危害を及ぼす、または発生する可能性のある事象
        - セキュリティ、コンテンツ、物理インシデント
        - 不正アクセス、不正書き込み、盗難、紛失、操作ミス、故障、天災等
      - リスク
        - 情報セキュリティの脆弱性により被害を及ぼす可能性
      - 脆弱性
        - 脅威に対する攻撃に弱い状態のこと
      - なぜ脆弱性があるのか？
        - PCは開発者向けに設計された情報機器
          - システム内部の設定を自由に変更できる
        - マルウェア(Malware：悪意のあるソフトウェア)に侵される可能性大
          - ウイルス、ワーム、スパイウェア、悪質なアドウェア、クラックツール等
    - 脅威(インシデント)の5W1H
      - What（なにを）？
        - 通信インフラ攻撃から情報へ
      - Why（なぜ）？
        - 功名心から金銭へ…グローバルな不正アクセスのビジネス化
      - When（いつ）？
        - 週末・祝日…”Patch Tue, Exploit Wed” → “0-day Attack”
      - Who（だれが）？
        - 組織化、低年齢化、ドメイン内部の人的ミス
      - Where（どこで）？
        - 米国＆中国＆ブラジル＆ナイジェリア経由…複数サーバ経由
      - How（どうやって）？
        - 通信の脆弱性からブラウザの脆弱性狙い！
    - 情報の防御
      - 情報資産
        - 情報システム内外の情報
        - アナログ・デジタル媒体に記録された情報
      - アナログ媒体(紙)管理
        - 個人情報記録媒体(紙)の管理は？　→　鍵付き引出、部屋
        - 個人情報記録の廃棄は？　→　燃やす or シュレッダー
      - デジタル媒体
        - PC内蔵ハードディスク・ドライブ：HDD、SSD
        - 外付け記録媒体（HDD、USB、CD/DVD等）
        - オンラインストレージの活用 → SkyDrive,Dropbox,Evernote　etc.
      - インターネット上の情報は記録されている！
      - PC・外部記録媒体の管理
        - パスワード保護、暗号化
        - バックアップ（定期的・周期的に!）
    - コンピュータの防御
      - OS（Windows, MacOS, Linux）を最新の状態に保つ
      - OS以外のソフトウェアを最新の状態に保つ
        - JRE(Java Runtime Environment)は、SunからOracleへ
        - 脆弱性対策情報データベースサイトの活用 → myJVN
        - 無料オンラインウイルススキャン → Symantec etc.
      - ブラウザの使い分け…InternetExplorerだけでは×
        - InternetExplorer, Firefox, chrome, Opera etc.
        - ブラウザのプラグインを最新の状態に保つ
        - Flash, QuickTime, Adobe Acrobat, Media Player etc.
        - SSL証明書のエラー　→　即刻ブラウザ終了
        - 警告メッセージを読む
    - ネットワークの防御
      - PCをネットワークに接続するということは
        - 双方向に情報のやり取りをしている → 有線・無線LAN共
        - 画面には表示されない → ネットワーク接続ポートのLEDで確認
      - PCのネットワーク接続
        - DHCP→有効？　無効？　（IPアドレスを自動的に割り当て）
        - IPv4アドレス・サブネットマスク設定
        - IPv4デフォルトゲートウェイ：最初の関所　→ この内は家族？
        - IPv4DNSサーバ：ホスト名をIPアドレスに変換 → 変更は？
      - PCのファイアウォール
        - ホワイトリストとブラックリスト
        - マルウェア対策にも
    - マネジメント＆コンプライアンス
      - 琉球大学情報セキュリティポリシー
        - 琉球大学情報システム運用・管理規程
        - 情報システム非常時行動計画に関する規程
          - インシデント対応手順
          - インシデント発生・再発防止策に関する報告・申請書
        - 順次、規程作成…？
      - 日本の情報政策の基本法「IT基本法」
        - サイバー犯罪、通信の秘密と情報開示
        - 電子商取引の推進とインターネット利用規制
        - 知的財産、個人情報保護、内部統制
      - 緩やかな保護規制により順次整備…現実とのギャップ
  - インターネット社会の情報防御
    - 個人情報の漏洩防止策が最も重要
      - 個人情報とは？
        - 個人を特定できる情報・組合せ：履歴書の項目等…学籍番号も！
    - 現状の企業内PC管理の矛盾
      - PC管理であり、データ管理ではない
        - 個人携帯(スマホ)はOK …？？？
        - 外部記録媒体の制限可能 …？？？
    - 琉大資産PC
      - 個人情報管理 →パスワードロック、施錠、外部媒体(暗号)
    - 個人資産PCの活用
      - 個人情報を分割し、個人情報がない情報活用等
  - 「情報セキュリティ白書2012」
    - Source
      - ➜ http://www.ipa.go.jp/security/vuln/10threats2012.html
    - 10大脅威
      - 1位 「機密情報が盗まれる！？ 新しいタイプの攻撃」
        - 情報窃取を目的とする標的型の諜報攻撃(APT)
          - APT(Advanced Persistent Threat)：先進的で執拗な脅威
          - =CE(Cyber Espionage)：サーバー空間における諜報活動
        - 事例
          - 2011/7：全衆議院議員ID流出
          - 2011/9：三菱重工ウイルス
      - 2位 「予測不能の災害発生！引き起こされた業務停止」
        - 自然災害や人為的災害によるITシステムの故障、業務データの消失
        - 資料
          - ➜ 読者調査で分かった、計画停電後に企業が実施している電源対策
          - ➜ みずほ銀行　システム障害特別調査委員会の調査報告書
          - ➜ 新日鉄ソリューションズ　通信障害
      - 3位 「特定できぬ、共通思想集団による攻撃」
        - 社会変革をめざす共通的な思想を持つ集団による暴露・妨害攻撃
        - 資料
          - ➜ アノニマス サイバー攻撃
          - ➜ 対アノニマス？ サイバー攻撃対策機動チーム「CYMAT」発足
      - 4位 「今もどこかで…更新忘れのクライアントソフトを狙った攻撃」
        - 標的型攻撃にも悪用されるクライアントソフトの脆弱性
        - 資料
          - ➜ いまー番危ない脆弱性は何だ? ～2011年版～
          - ➜ 2011年度 情報セキュリティの脅威に対する意識調査
      - 5位 「止まらない！ウェブサイトを狙った攻撃」
        - 狙われ続けるウェブサイトの脆弱性
        - 資料
          - ➜ 通称「LizaMoon（ライザムーン）」によるウェブサイトの改ざん被害が拡大
          - ➜ 大規模なIFRAMEインジェクション攻撃
      - 6位 「続々発覚、スマートフォンやタブレットを狙った攻撃」
        - 狙われる小さなパソコン-スマートデバイス
        - 資料
          - ➜ スマートフォン市場規模の推移・予測（12年3月）
          - ➜ McAfee脅威レポート：2012年第1四半期
      - 7位 「大丈夫！？電子証明書に思わぬ落し穴」
        - 電子証明書の管理不備により、引き起こされた問題
        - 資料
          - ➜ 政府機関から盗まれた証明書、マルウェアに利用される
          - ➜ DigiNotarの不正証明書問題
      - 8位 「身近に潜む魔の手・・・あなたの職場は大丈夫？」
        - 組織内部・関係者による業務妨害や情報漏えい
        - 資料
          - ➜ セディナ　お客様情報の不正売却
          - ➜ SB モバイルの大規模障害
      - 9位 「危ない！アカウントの使いまわしが被害を拡大！」
        - アカウント情報の管理不備が原因で発生するなりすまし被害
        - 資料
          - ➜ Facebook、新しい管理ツール提供へ　ログイン乗っ取りは「毎日60万件」
          - ➜ ソニー　ユーザアカウントへの第三者のなりすまし
      - 10位 「利用者情報の不適切な取扱いによる信用失墜」
        - 利用者との結びつきが強い情報(利用者情報)の取り扱いに関する問題
        - チェック項目
          - 必要以上に利用者情報を収集していませんか？
          - 利用者にきちんと使用目的を伝えていますか？
        - 資料
          - ➜ ソニー　オフィシャルサイトをご利用中のお客様へ
          - ➜ コネクトフリー　お客様情報の不正取得