- 情報セキュリティ安全管理措置
  - →
  - インターネット社会
    - Internet Device…多様化！
      - スマホ(Smartphone)
        - iOS
          - 2008/7：iPhone 3G-SoftBank
          - 2011/10：iPhone 4s-au
          - 2013/9：iPhone 5s-docomo
        - AndroidOS
          - 2009/7：HT-03A-docomo
          - 2010/4：XPERIA-docomo
          - 2010～：SoftBank,au
      - タブレットPC
        - 2010：iOS(iPad)-Apple
        - 2010：AndroidOS(タブレットPC)-各社
        - 2013：Windows8(Surface)-MicroSoft
      - 今後は？
        - BYOD 【 Bring Your Own Device 】
          - 企業などで従業員が私物の情報端末などを持ち込んで業務で活用すること。
    - 情報セキュリティマネジメント
      - 定義：情報セキュリティ(Information Security)
        - ISO/IEC 27001:2013(JIS Q 27001)
        - 情報の機密性，完全性及び可用性を維持すること。
          ＋（真正性、責任追跡性、否認防止、信頼性）等特性
      - 情報セキュリティのCIA(３要素)
        - Confidentiality-機密性（紙媒体と情報システム）：　レベル1・2・3・4
          - 無許可でのアクセス及び使用不可
        - Intergrity-完全性（情報システム）：　レベル1・2・3・4
          - 情報の正確さ及び完全さ
        - Availability-可用性（情報システム）：　レベル1・2・3・4
          - 要求に対しアクセス及び使用可…バックアップと復旧
      - ・脅威
        ・インシデント
        ・リスク
        ・ぜい弱性
        - 脅威：システムまたは組織に損害を与える可能性がある、インシデントの潜在的な原因
        - インシデント
          - ・事業運営を危うくする確立　及び
            ・情報セキュリティを脅かす確立が高いもの
        - リスク
          - 目的に対する不確かさの影響
            ・情報資産または管理策のぜい弱性につけ込み、組織に損害を与える可能性
            - 管理策：リスクを修正する対策
        - ぜい弱性
          - １つ以上の脅威によってつけ込まれる可能性のある、情報資産または管理策の弱点
        - なぜ、ぜい弱性があるのか？
          - 技術的
            - 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PC
            - 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
          - 組織的
            - リーダーシップと管理策
          - 人的
            - 啓蒙・教育
          - 物理的
            - 棟・部屋・書庫・引出内等管理
      - 脅威の5W1H
        - What（なにを）？
          - 通信インフラ攻撃 → 情報
        - Why（なぜ）？
          - 功名心 → 金銭…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 → ブラウザの脆弱性狙い！
      - 具体的対策
        - 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
              - リスク大
            - 外付け記録媒体（HDD、USB、CD/DVD等）
              - リスク小
            - オンラインストレージの活用 → OneDrive,Box,Dropbox,Evernote　etc.
              - 暗号化必須！
            - → 早稲田大学：全学生・教職員にオンラインストレージ「Box」を導入 2015/6
            - Why?
              - 米国医療保険の相互運用性と説明責任に関する法律：HIPAA (Health Information Portability and Accountability Act:) 1996年
                米国経済的および臨床的健全性のための医療情報技術に関する法律：HITECH 法 (Health Information Technology for Economic and Clinical Health (HITECH) Act:) 2003年
              - ■ Box社対応！
          - インターネット上の情報は全て記録されている！
            - 画像ファイルの脅威：Exif(Exchangeable image file format)情報
          - PC・外部記録媒体の管理
            - パスワード保護、暗号化が必須！
              - WinOS用：アタッシュケース
              - ➔ →http://hibara.org/software/attachecase/
              - オンラインストレージ用：Cloudfogger
              - ➔ →https://www.cloudfogger.com/en/
            - 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×
            - Firefox, Chrome, Opera, Sleipnir 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
            - ×プライベートネットワークではない！
            - ○パブリックネットワークである！　… スラム街ホテルの廊下をイメージ
          - PCのファイアウォール
            - ネットワーク・ファイアウォールの限界
            - ウイルス対策(マルウェア対策)ソフトの限界
            - 有線ルータの設置を！（バッファロー、コレガ等）＝ ファイアウォール機器
    - 安全管理措置
      - 個人情報保護法の４つの観点 →
        （個人情報の保護に関する法律についての
        経済産業分野を対象とするガイドライン）
        - ※ 安全管理について従業者の責任と権限を明確に定め、安全管理に対する規程や手順書を整備運用し、その実施状況を確認すること
        - 組織的
          - （1）個人データの安全管理措置を講じるための組織体制の整備
          - （2）個人データの安全管理措置を定める規程等の整備と規程等に従った運用
          - （3）個人データの取扱い状況を一覧できる手段の整備
          - （4）個人データの安全管理措置の評価、見直し及び改善
          - （5）事故又は違反への対処
        - 人的
          - ※ 従業者に対する、業務上秘密と指定された個人データの非開示契約の締結や教育・訓練等を行うこと
          - （1）雇用契約時及び委託契約時における非開示契約の締結
          - （2）従業者に対する教育・訓練の実施
        - 物理的
          - ※ 入退館（室）の管理、個人データの盗難の防止等の措置
          - （1）入退館（室）管理の実施
          - （2）盗難等の防止
          - （3）機器・装置等の物理的な保護
        - 技術的
          - ※ 個人データ及びそれを取り扱う情報システムへのアクセス制御、不正ソフトウェア対策、情報システムの監視等、個人データに対する技術的な安全管理措置
          - （1）個人データへのアクセスにおける識別と認証
          - （2）個人データへのアクセス制御
          - （3）個人データへのアクセス権限の管理
          - （4）個人データのアクセスの記録
          - （5）個人データを取り扱う情報システムについての不正ソフトウェア対策
          - （6）個人データの移送・送信時の対策
          - （7）個人データを取り扱う情報システムの動作確認時の対策
          - （8）個人データを取り扱う情報システムの監視
      - 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…？
        - 緩やかな保護規制により順次整備 … 現実とのギャップ