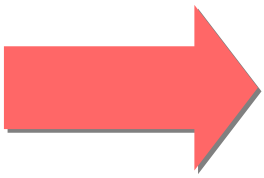
変化するセキュリティ管理の実情

山口　英
奈良先端科学技術大学院大学

概要・

- ・多くの組織では、IT化を進めてくる中でセキュリティ管理についても同時に取り組みを深めてきた。しかし、最近になって、急激にセキュリティ管理の方法、目的、使用する技術などが変化してきている。同時に、その変化は組織運営にも大きく影響を与えるようになっている。今回の講演では、どのような変化があり、その目的はなんであるかを概観し、どのような方針に基づいてセキュリティ管理を設計すべきかを述べる。

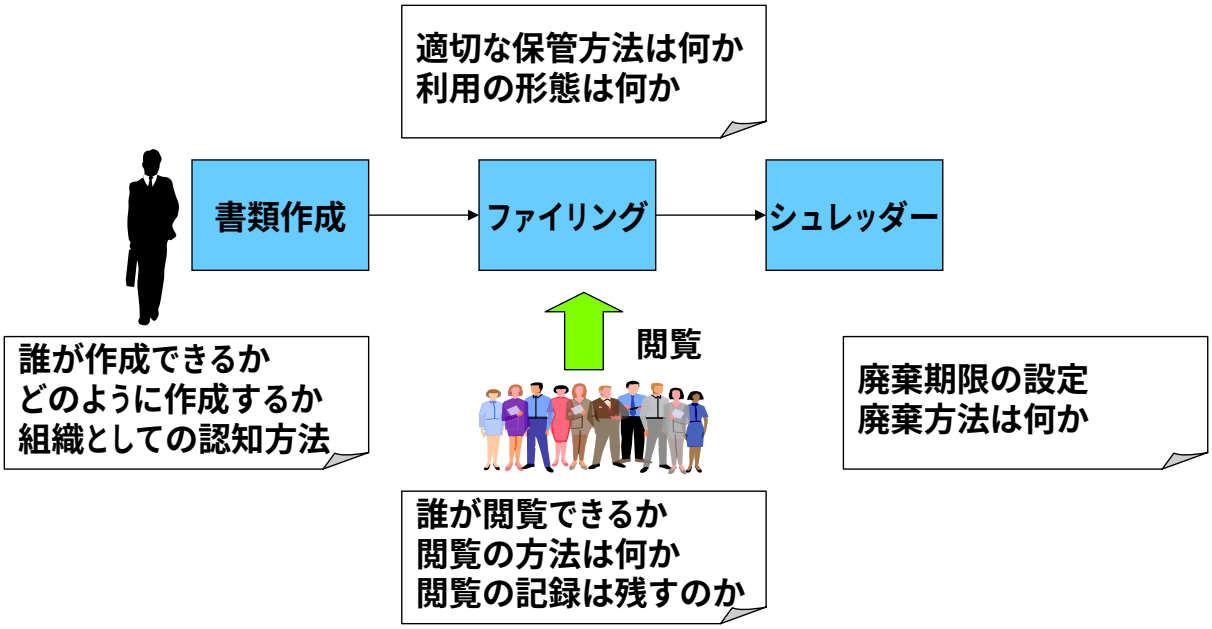
システムを守る  情報資産を守る

最近の言葉

- 個人情報保護
- 事業継続性計画 (BCP: Business Continuity Planning)
- 情報保証
- 情報化

情報のライフサイクル

- 紙で考えてみれば実は簡単!



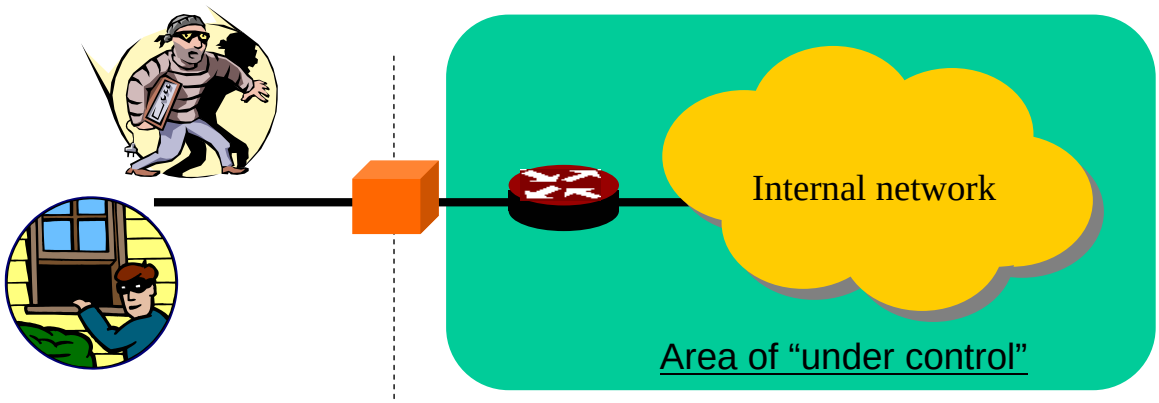
一般的な対策

- 情報の区分け
  - CIA (Confidentiality, Integrity, Availability) に注目
- 人の区分け
  - Qualification, security clearance
- 情報と人のマッピング
  - Access privilege management
  - Enforcing mechanism
- ネットワーク環境での実装努力
  - PKI, service server
  - Audi trail の設定と監査運用

外部から守る → どこでも守る

復習：これまでのネットワーク環境

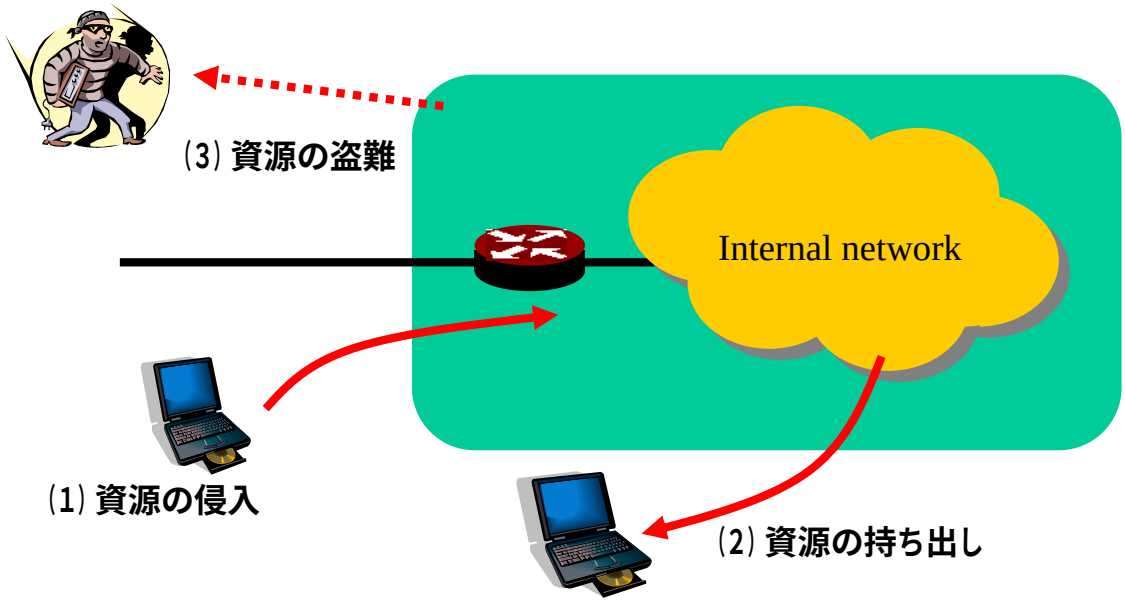
- 境界防衛（Perimeter Defense / Boarder Protection）



FEBA: Fighting Edge of Battle Area, perimeter / boarder

モーバイルコンピューティングの本質

Perimeterを無視した移動



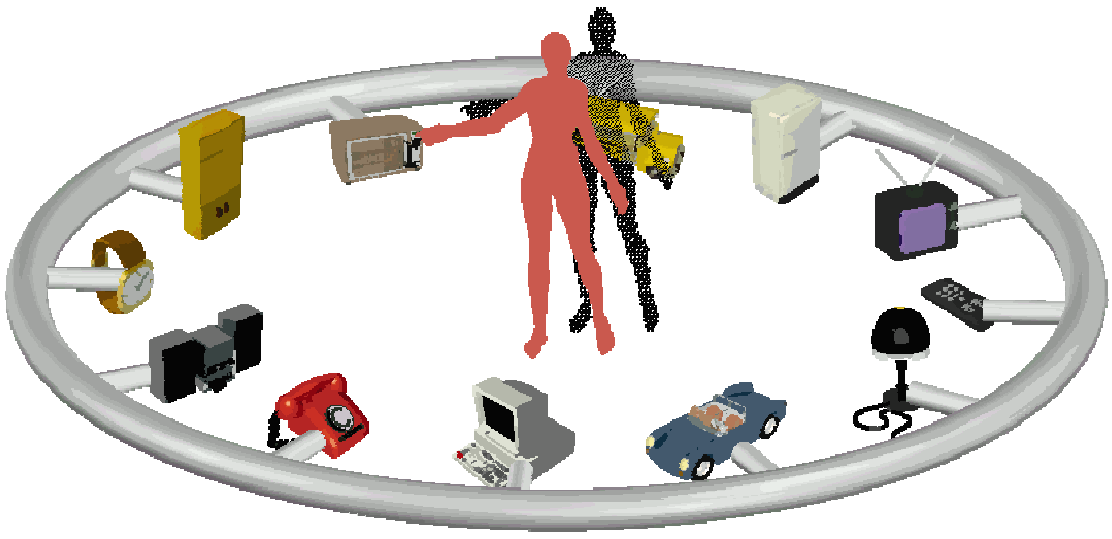
情報、人、システムを分離する

取り扱う情報に応じて、使うシステムと、使うユーザを限定し、明示する。(特別作業室のイメージ)

Desktop PC → 情報処理機器全部

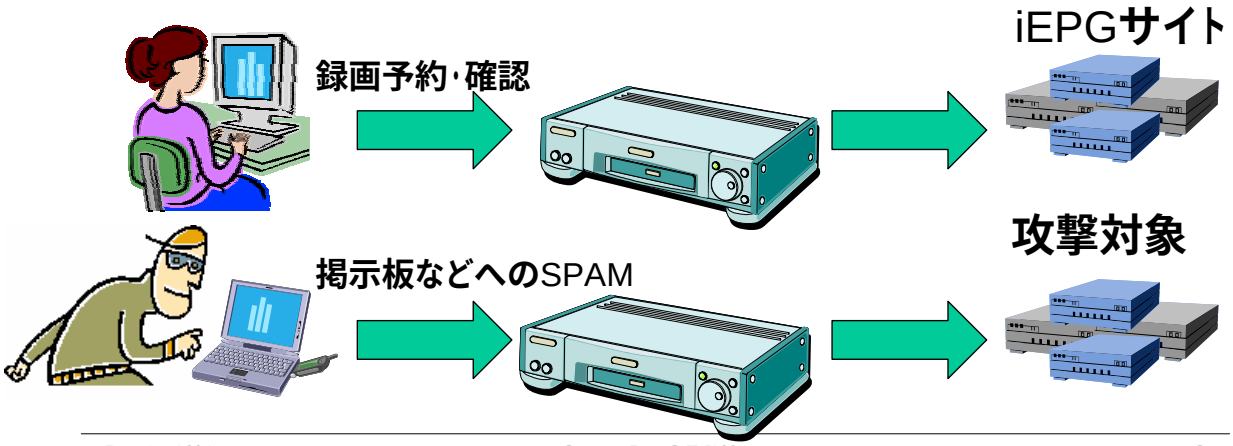
Internet for Everything

- Always connected with global address
- New services with various kind of devices



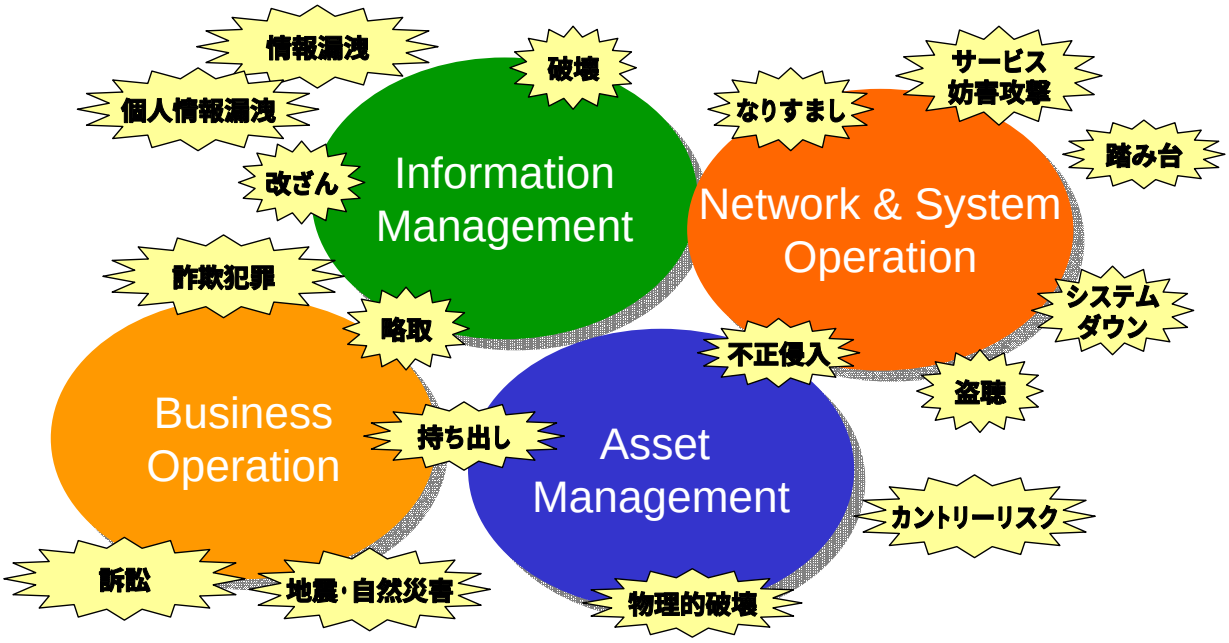
難問：家電が攻撃元に!?

- 2004年9月に発覚
  - 家庭用ビデオレコーダーが攻撃を中継してしまった
  - 東芝HDD/DVD recorder RD-XS40
    - HTTP proxy機能をもったWebサーバ内蔵で、open proxyだった
    - 録画予約などのUIをユーザに提供
    - LAN機能内蔵



限定的リスク管理 → 総合リスク管理

情報システムを取り巻くリスク



明確な目標設定

- 情報通信技術から得られる恩恵は最大化する
  - セキュリティ管理原理主義に陥らない
  - そもそもIT投資は何のために行ったのか
- システムが抱えるリスクは最小化する
  - セキュリティ対策
  - 情報管理対策
  - しかし、だれも見向きもしないようなシステムにしてはいけない
- この二つの目標は両立可能
  - 相当知恵をしぼらなければいけない
  - Moving target
  - セキュリティ対策の「万能型紙」は無い

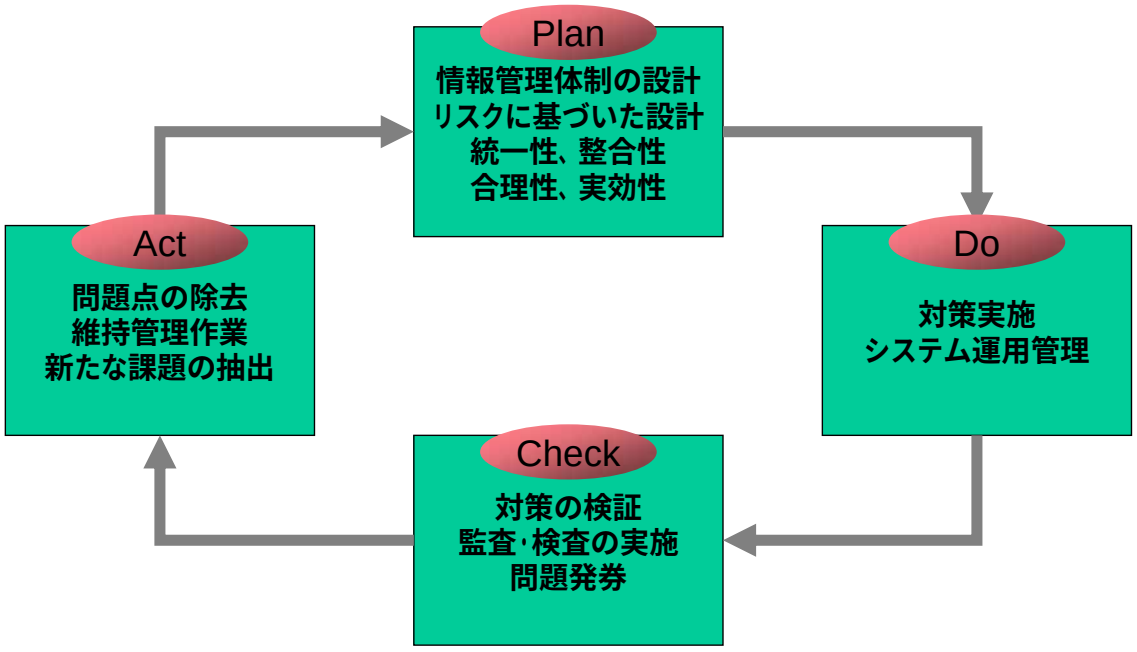
Two extremes

原理主義的 ⟷ 自由放任主義的

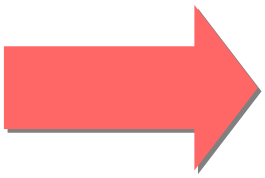
- 閉鎖ネットワーク
- 物理的持ち出し阻止
- 厳重な入退出管理
- ネットワーク全体の防護
- ユーザの挙動監視
- 厳格な運用の徹底

- 開放ネットワーク
- ユービキタス意識
- ホスト単位の管理徹底強化
- ネットワークのパイプ化
- サービスの徹底監視
- 事業活動優先

PDCAサイクル：合理性確保



情報セキュリティの特質から “P” の弾力化必須
→新たな脅威が顕在化する時は予見できない

主役はIS部門  組織全体

セキュリティ管理に必要となる人的資源

- 技術者は必要
  - セキュリティの実際的な管理の多くが技術的対策
  - セキュリティ技術を運用できる人材が必須となる
  - 場合によってはアウトソースしても大丈夫
- 技術者以外も必要
  - セキュリティについての教育を実施する人材確保
  - セキュリティ管理におけるポリシとガイドラインの開発･更新
  - 予算管理
  - 人的資源管理

誰が関わらなければいけないのか

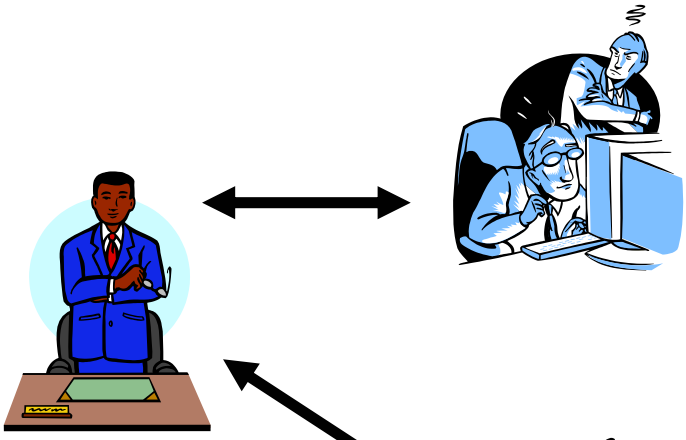
チームワークの大切さ

まだまだやることは沢山ある

あきらめたくなることも沢山あるけど

みんなで力を合わせれば怖くない

職員のマインド



成果が目に見えにくい部門
施策実施のためのシステム作り
既存機構の改善
情報通信システムの運用･保守
教育･研修
検査･監査
発掘して評価しない限り認められない

支援･環境構築

組織トップ
当然両方の部門が円滑に機能するために、全ての職員のマインド向上に尽力することが必要
→ 事故防止につながる

成果が目に見えやすい部門
政策･施策立案と予算策定
施策の具体的な実施
新たな法律作成と改正
新たな組織作り
直接評価可能