高等教育機関におけるセキュリティポリシーとは

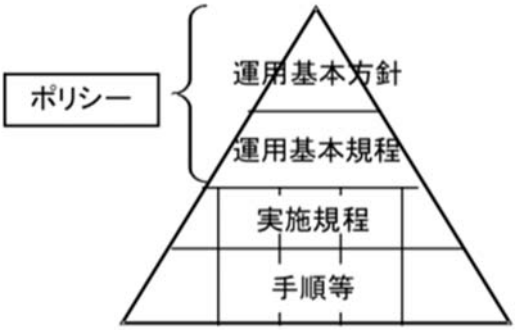
高倉弘喜
国立情報学研究所

情報セキュリティ対策がなぜ必要か？

- 人は易きに流れる
  - 統一ルールがなければ我流
    - 面倒臭いことはやりたくない→これくらいで大丈夫だろう
  - 平常時に事故防止策として最低限守って欲しいことを定める
- 技術による防御の限界
  - かけられるコストの上限
  - 導入できる仕組みにも限度
    - 事故を防げなかった場合の危機管理
      - 様々な事故のケースを想定
        - エリートパニックの防止
      - 想定外の事故への臨機応変な対応
    - 事故発生後の運用継続可否・業務再開の判断基準
      - 100%の安全性を求めない…使えないシステムを導入しかねない

セキュリティポリシーの立て付け(1/3)

- ポリシー
  - 運用方針＋運用基本規程
    - 理念を述べる部分
    - 用語の定義
    - 体制の定義
      - 誰が対象で、何を、どこまで守るのか？
      - 通常時と緊急時に分けた体制の必要性
        - 組織構成に沿った連絡体制の整備
        - インシデント対応を行うCSIRTの整備
  - 改定の頻度は極めて低い
    - 10年くらいは使えるものを



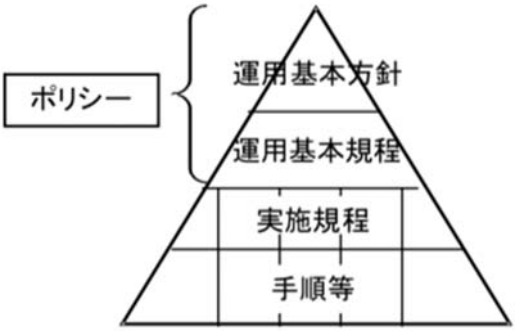
高等教育機関の情報セキュリティ対策のためのサンプル規程集（2017年版）

セキュリティポリシーの立て付け(2/3)

- 実施規程
  - 定義
    - 技術用語および組織体制の定義
  - 管理者側から見た体制・ルール
    - 運用・管理ルール
    - 情報の格付け
    - 利用者の管理
    - 監査
    - インシデント発生時の体制
  - 大改定の頻度は低い
    - 数年に一度の見直し程度

パスワードは強固なものを使わせましょう

ポリシーと実施規程は公開できる程度の内容
(大学ごとの違いは小さい)



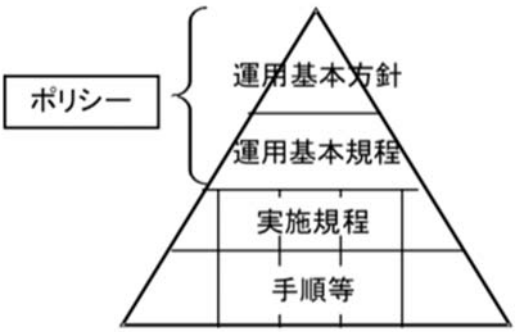
高等教育機関の情報セキュリティ対策のためのサンプル規程集（2017年版）

セキュリティポリシーの立て付け(3/3)

強固なパスワードの必須用件

- 手順・ガイドライン
  - 実施規程の各項目に対応した具体的な手順
  - 策定には各大学の実情把握が必須
    - 執行部の体制
    - 部局の構成
    - 関連組織の有無
      - 附属病院
      - 附属小・中・高
  - 年単位の細かな見直しと調整が必要
    - サイバー攻撃の手口の変化
    - セキュリティ対策の危殆化

この部分は原則非公開
(大学の防御体制を細かく記述)



高等教育機関の情報セキュリティ対策のためのサンプル規程集（2017年版）

高等教育機関の情報セキュリティ対策のためのサンプル規程集

- 政府機関統一基準をベースに国立大学向けに一部変更
  - 私学には馴染まない項目もあるのは事実
    - ポリシーと実施規程までは大きくは変わらない
      - 大学の規模により微調整は必要
        - 一人の人が複数の役割を兼ねることも

どう扱うべきか？

  - 995ページの百科事典のように思えるが…三分の一は逐条解説
    - 事務向けの実施規程(400ページ)
      - 事務系はすでになんらかの(文書)規程がある
    - 手順・ガイドライン(216ページ)
      - ここだけは内容を理解しつつカスタマイズが求められる
- 国のサイバーセキュリティ戦略2018
  - 役員層が情報セキュリティ対策に深く関わることを想定
  - 火消し役＋参謀役が求められるCISRT