資料3

# NDBデータの申請に向けたセキュリティ対策の実例

京都大学　医療経済学分野
猪飼　宏
hikai-kyt@umin.net

2013.1.17　レセプト情報等の提供
に関する事前説明会　資料

# ISMSとは

- Information Security Management System
  情報セキュリティマネジメントシステム
- 情報取り扱い手順を定めた「ルールブック」ではない。
- 情報取り扱いの「方針」を受けて、
  行動計画に落とし込み、
  PDCAサイクルによる運用改善を図る仕組み。
- 運用状況を評価する(民間の)第三者認証あり。

# 当研究室での従来のISMS運用

- 京都大学の情報セキュリティポリシーや疫学研究倫理指針など、各種規定に準拠
- 情報資産や各種の取り決めを文書化
  - データの重要度
  - データの受け渡し
  - バックアップ・障害復旧・停電対応の手順
  - ソフトウェアライセンスやハードウェアの管理
  - 不適合記録や改善要求の文書化・保存
- 定期的な内部監査で見直し事項を記録
- 年1回の外部監査

# NDB申請者へのセキュリティ要件

- ISMSの章立てを参考にして作成されている。
  - ポリシーの明示
  - 説明責任のための手順文書化や各種記録
    - データ受入・破棄の記録
    - 取扱者の範囲とそれぞれの権限
    - 不正アクセスや情報漏出の予防策・事故対応手順
- 厳しいセキュリティ要件
  - 個票データを扱うため
  - 研究者が複数の研究・医療機関にまたがるため。

# NDB申請に備えた強化のポイント

- 入退室記録の厳格化
  - 指静脈認証によるタイムレコーダ
  - 指静脈認証によるサーバ室入退室システム
  - 既存システムとは別系統のネットワーク構築
- 操作者の権限に応じて、操作システムを分離
  - 受領データを格納し、抽出・集計加工するサーバ
  - 統計解析やレポート作成を行うサーバ
  - 後者サーバにリモートデスクトップ接続するPC
- 内部監査に学部事務の情報担当者を同席依頼

# 生体認証による入退室管理

- 指静脈認証システムは高額
  - タイムレコーダ　20万円弱
  - 入退室管理システム　2~300万円
    - シリンダー錠を電気錠に交換
    - 入退室記録を行うPCとの間でケーブル配線
    - 電気工事
- 入退室記録と各種ログの照合を随時行う

# データ受領後に生じた課題と運用ルールの見直し

- システム担当者がデータの特徴に不慣れで作業が進みにくい。

⇒研究者の一部をシステム担当者に昇格すべく修正申請。

# Tips

- 個票データを受け取ると、管理は大変
  - 集計データでも十分かどうか、要点検。
- 多人数の研究グループでは役割分担を明確に。
- 運用中に明らかになった問題点は、運用ルール上で適切に修正を加える事で対応する。