

## 【WP6】 S/MIME証明書試験運用

---

国立情報学研究所

学術ネットワーク研究開発センター

島岡 政基

# 目的と作業概要

- 目的
  - S/MIME証明書の発行業務および利用に関する試験運用
- H17年度の成果
  - S/MIME証明書の試験発行
    - ・ H18.4月から認証作業部会関係者有志に発行
  - S/MIME証明書の試用
    - ・ H18.4月から認証作業部会関係者有志が試用中
- H18年度の作業計画(案)
  - 試験運用スキームの整理・検討
    - ・ 昨年度運用スキームの問題点整理・改善案検討
  - S/MIME証明書需要調査
    - ・ 学術市場における需要および利用形態等に関する調査
  - その他各種調査等を検討中

# 試験運用スキームの整理・検討

- 登録業務設計について
  - あくまで小規模(500名)運用前提の業務設計。
    - ・ メール到達性確認と分割PINコードの手渡し
  - 大規模運用を想定した登録業務を試験運用するのはコスト、リソース、運用負荷等の面で難しいことがわかった。
- 証明書プロフィールについて
  - 事業者側ポリシによってはカスタマイズできない項目がある。
    - ・ 事業者のサービス仕様を確認した時点ではわからなかった話。
  - 利用したい**プロフィールを明確に**示して、実現可能か確認する必要がある。
  - 曖昧な調達仕様では、齟齬が起きる可能性がある。
- 認証作業部会関係者有志での試用について
  - 5カ月の運用を経て大きな混乱は起きていない。
  - いくつかの失効事例
    - ・ HDDのクラッシュ、鍵生成時の鍵長指定ミスなど