PKIを用いた認証強化実験

社団法人日本ネットワークインフォメーションセンター
技術部／インターネット基盤企画部
セキュリティ事業担当
木村 泰司

はじめに　ー　本発表のポイント

- PKIを用いた認証強化実験の紹介
  - IPレジストリシステムにおけるSSLの「クライアント証明書」を使った認証

  - ポイント
    1. 希望される方にIPレジストリシステムのログインに使える電子証明書を発行いたします。
    2. 継続してパスワードを使うこともできます。
    3. 本日の資料をお持ち帰り下さい。
       - 情報の入手元URL
       - JPNICルート認証局のfingerprint

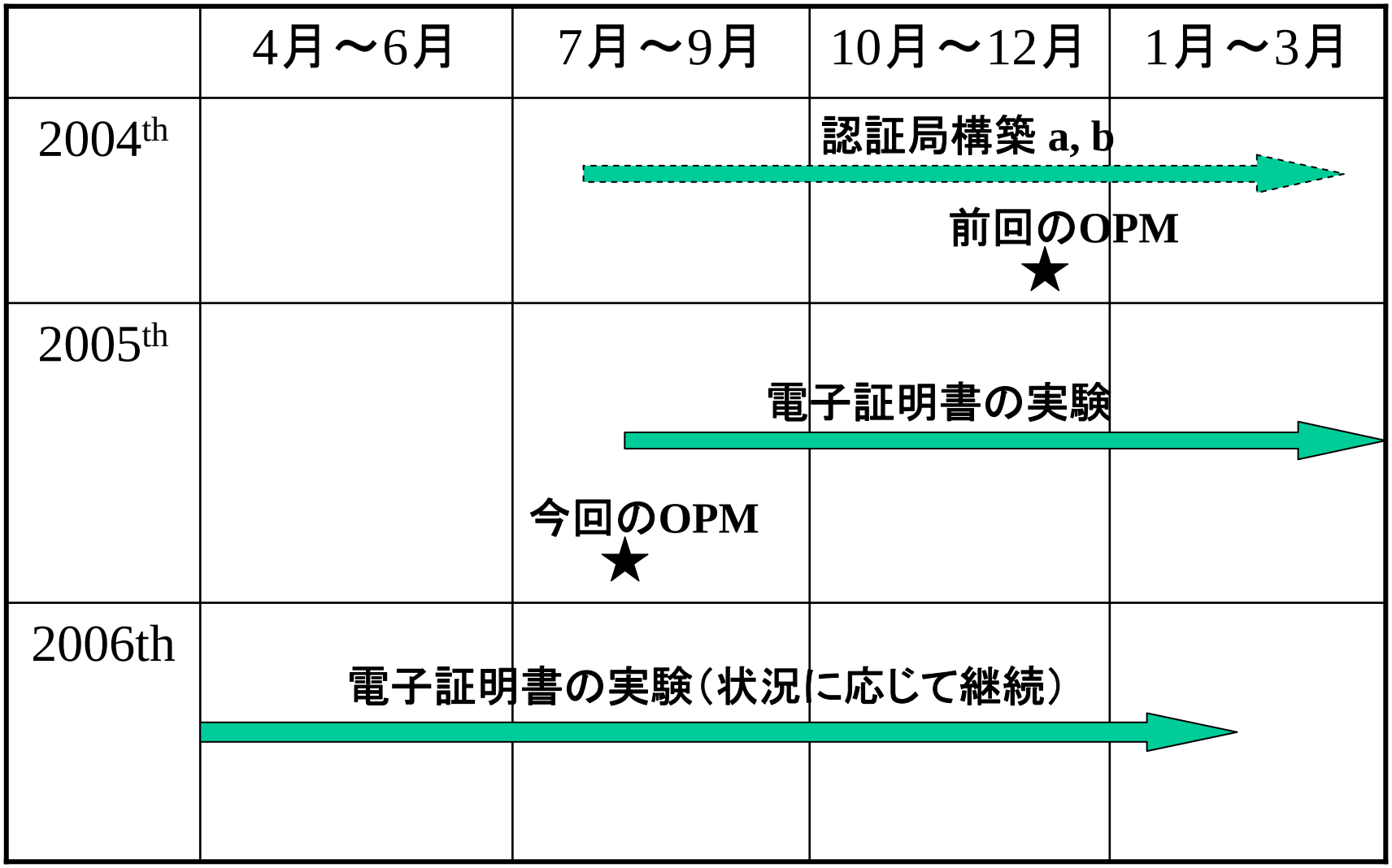
内容

- 実験の背景
- IPレジストリシステムにおける認証強化実験
- 電子証明書と利用例
- 電子証明書の申請方法

背景

- 前回のOPMでの発表
  - 「JPNICにおけるレジストリデータの保護と応用の考え方について」 2004年12月
    a. JPNIC認証局の構築
    b. IPレジストリシステムの保護機能の実現
    c. レジストリデータを使った認証基盤に関する調査
  - このうち、a と b が構築済み ⇒ 今回の実験
    c は継続して取り組み中。

実験のスケジュール

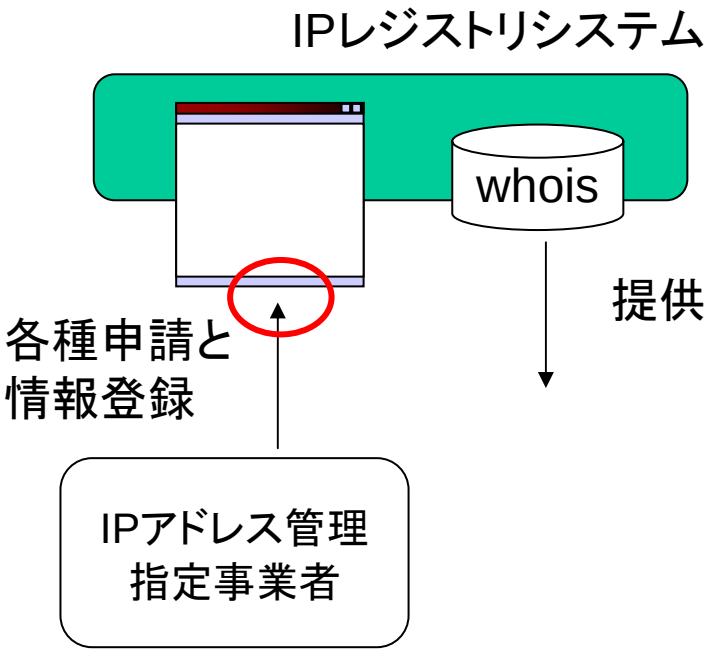

4月～6月
7月～9月
10月～12月
1月～3月
2004th
認証局構築 a, b
前回のOPM
2005th
電子証明書の実験
今回のOPM
2006th
電子証明書の実験（状況に応じて継続）

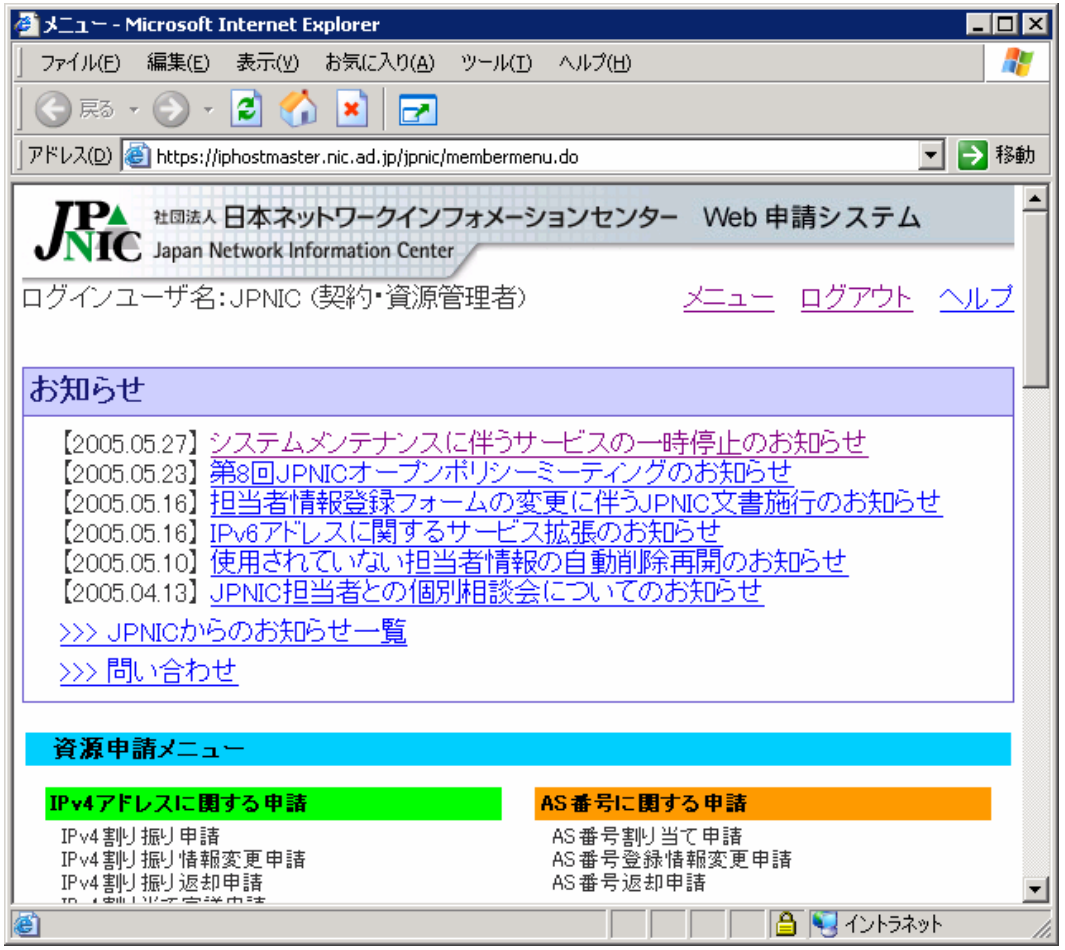
IPレジストリシステムにおける
認証強化実験

社団法人日本ネットワークインフォメーションセンター

IPレジストリシステム

- 各種申請と情報登録の為のシステム





IPレジストリシステムのユーザ認証

- パスワード
  - 利点
    - 仕組みがわかりやすい
    - 作業の委任が簡単
  - 欠点
    - 第三者に漏洩してもわからない
    - 担当者が変わった時の変更に手間がかかる
      又は変更しない…

パスワードには慎重な管理が必要

登録者のなりすましによる影響

- IP Hijacking
  - Hijacked IPs
    http://www.completewhois.com/hijacked/index.htm
- whoisの返答内容の改ざん
  - IPネットワークアドレスの登録
  - ネームサーバの情報
  - 管理者連絡窓口、技術連絡担当者

⇒ 不正な経路情報の発見などにも影響

IPレジストリシステムの認証強化の実験

RIRにおける認証強化

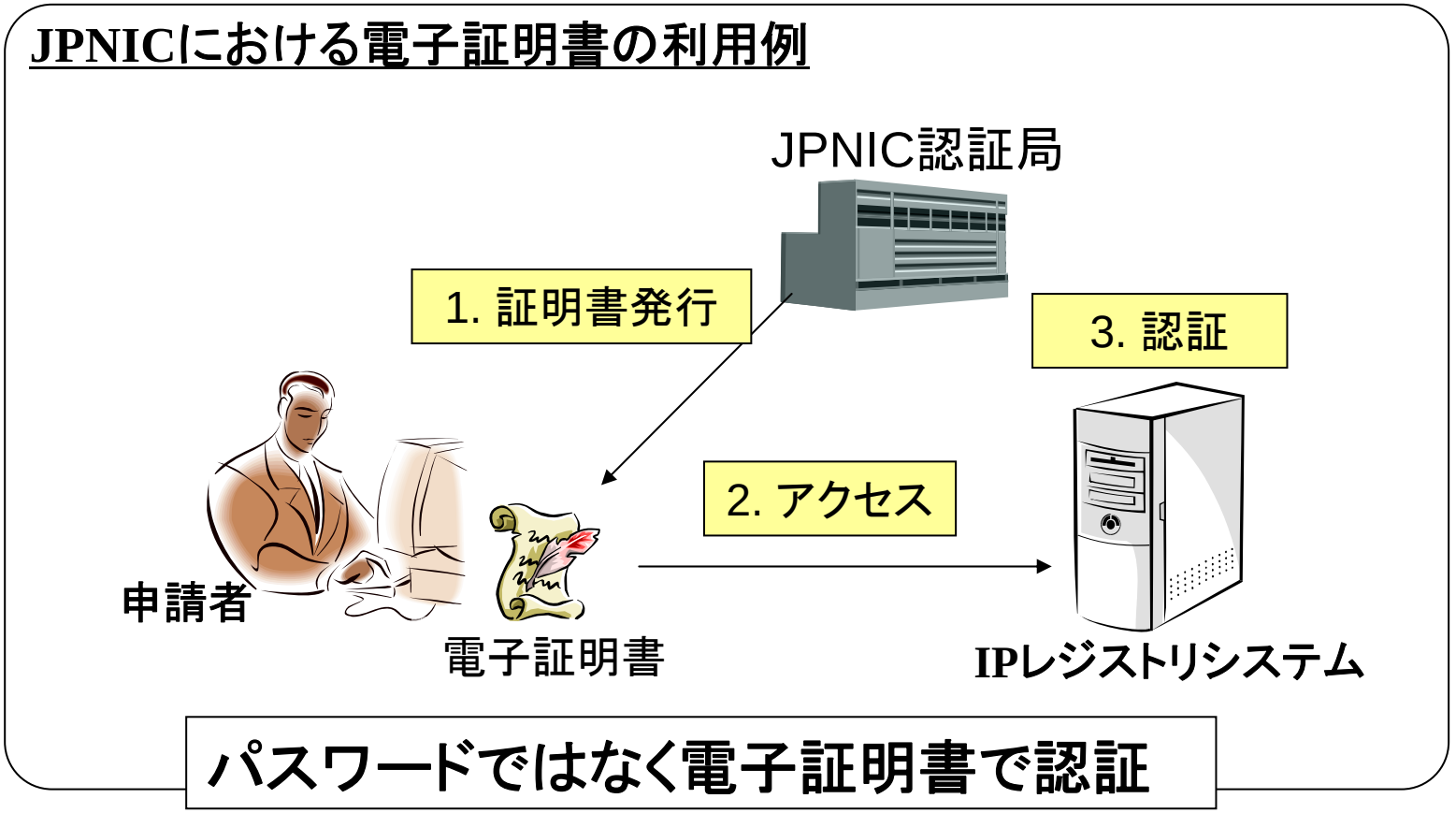
- APNIC
  - 個人認証を行い電子証明書を発行
  - MyAPNIC（LIR向けWebページ）で使用
- RIPE NCC
  - LIR認証を行い電子証明書を発行
  - LIRPortal（LIR向けWebページ）で使用
- ARIN
  - LIR認証と個人認証を行い電子証明書を発行
  - 申請書のメールに電子署名

電子証明書と利用例

社団法人日本ネットワークインフォメーションセンター

PKIと電子証明書

- PKI（Public-Key Infrastructure）の「電子証明書」を使ったユーザの認証

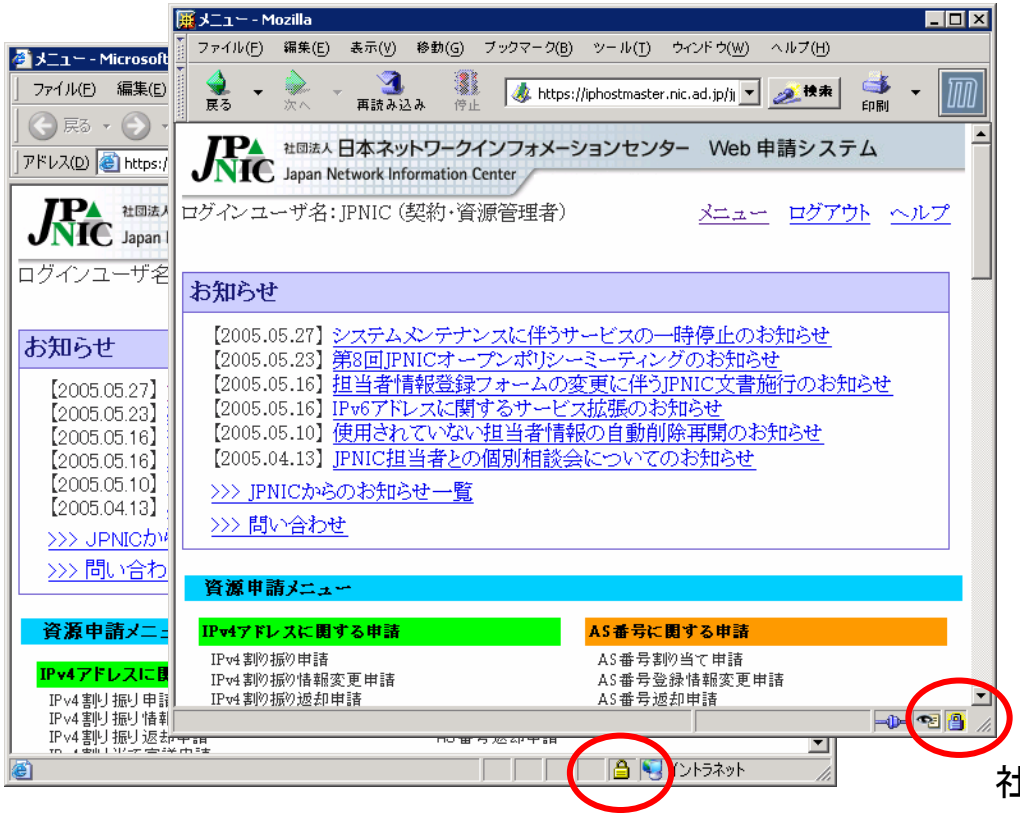


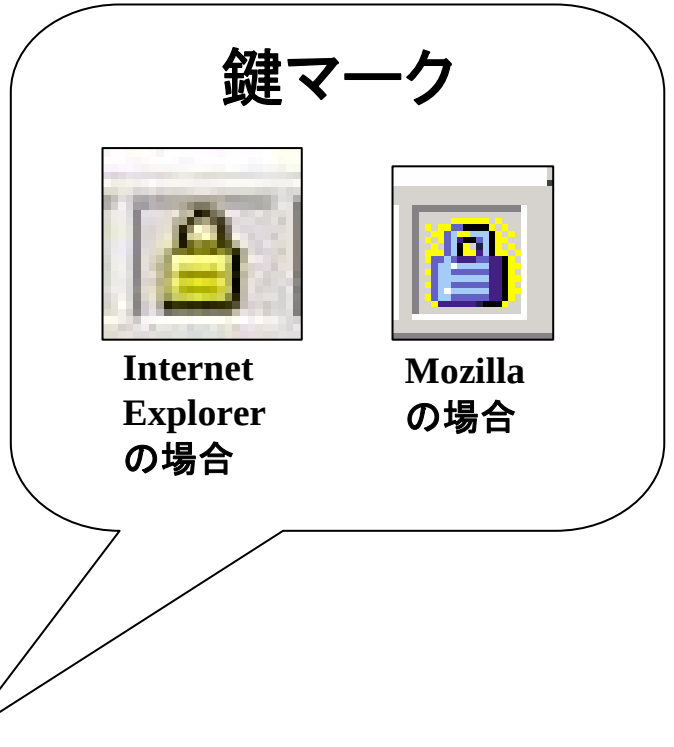
電子証明書とは

- パスワードに比べて優れているところ
  - 暗号技術を使った認証
    - 通信路を盗聴しても内容が分からない、なりすましが難しい
  - 漏洩対策
    - 「電子証明書」と「パスフレーズ」の二要素
      - パスワードの場合は一要素の盗用だけでなりすましできてしまう。

Webブラウザを使った利用例

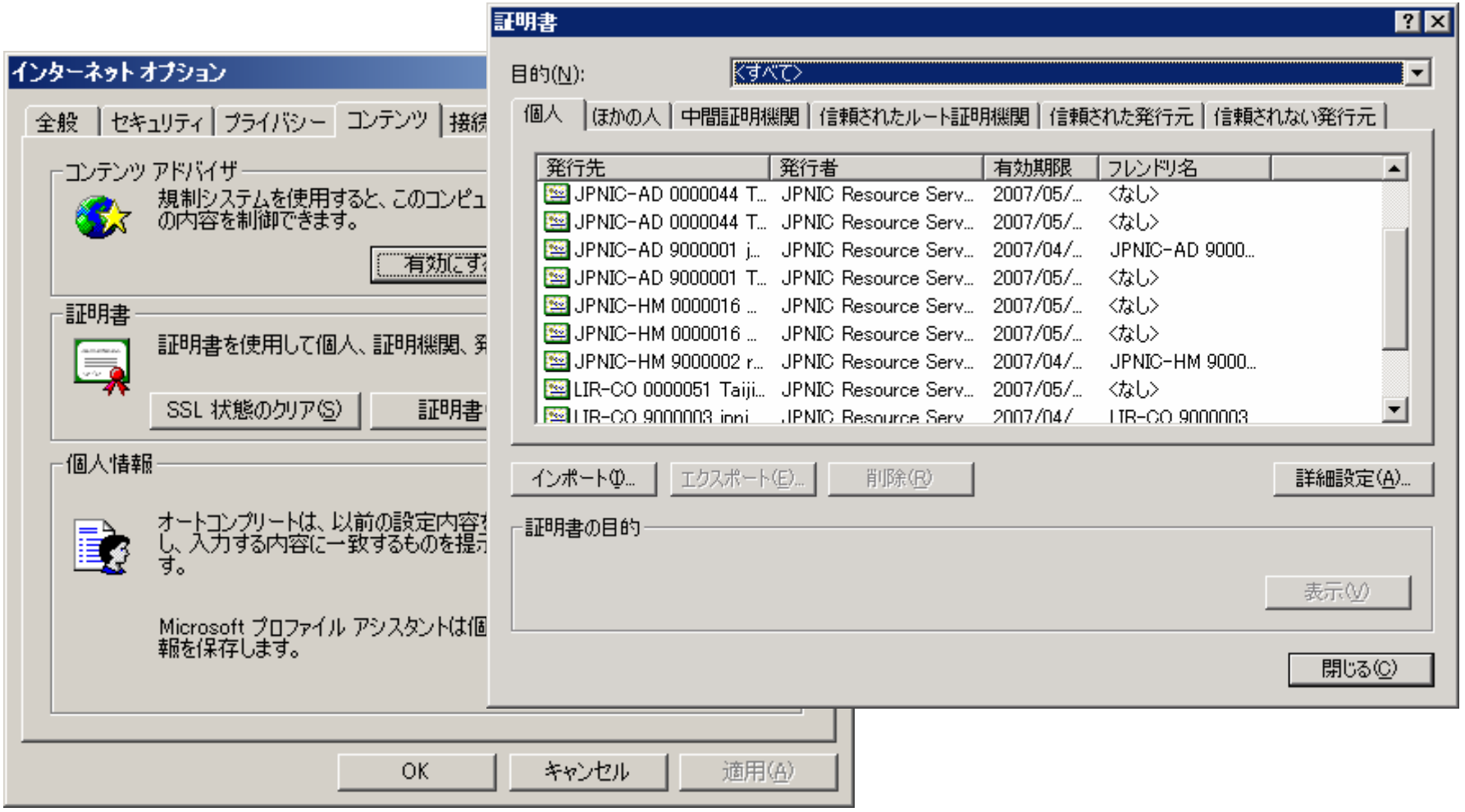
- SSLのクライアント認証
  - サーバとクライアントで相互に認証（なりすましを検出）
  - 暗号通信（通信路の盗聴が難しい）





Webブラウザにおける電子証明書の利用

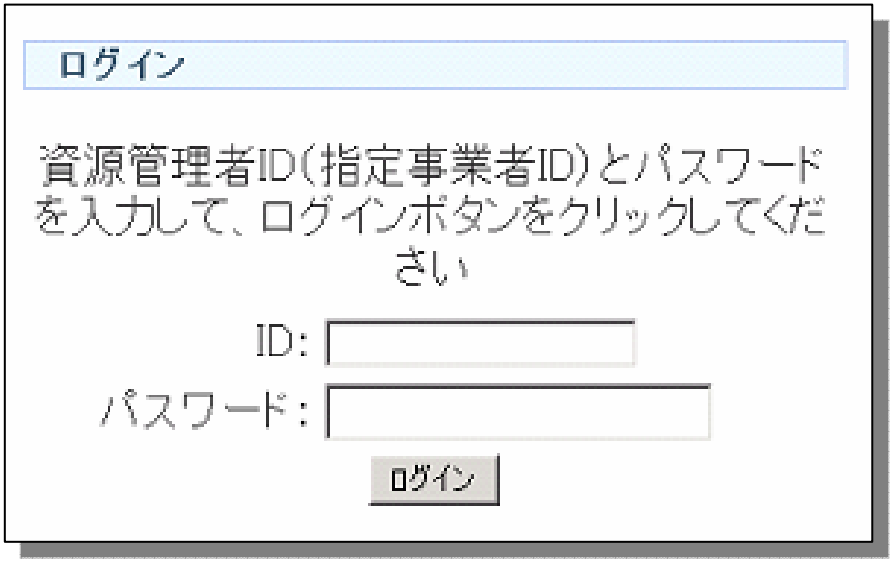
- Webブラウザに組み込んで利用



利用例

- IPレジストリシステムのログイン画面

パスワードの場合



電子証明書の場合

パスフレーズを入力

トップページに直接アクセス

認証方法が変わるだけで、各種申請業務は通常通りです。

電子証明書の申請方法

社団法人日本ネットワークインフォメーションセンター

電子証明書のユーザ（1）

- 契約／資源管理者
  - IP指定事業者の「契約情報」「資源管理情報」を管理
    - IPアドレス資源関連の申請は不可
    - 資源管理者の証明書 発行・失効・更新 申請
- 資源申請者
  - IPアドレス資源関連の申請などができる

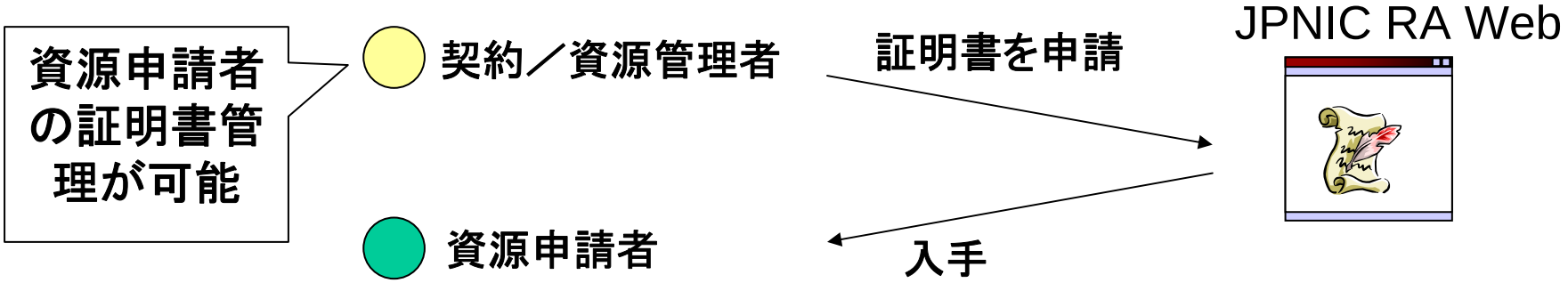
電子証明書のユーザ(2)

- 電子証明書の申請方法の違い

契約／資源管理者 → 書面で申請

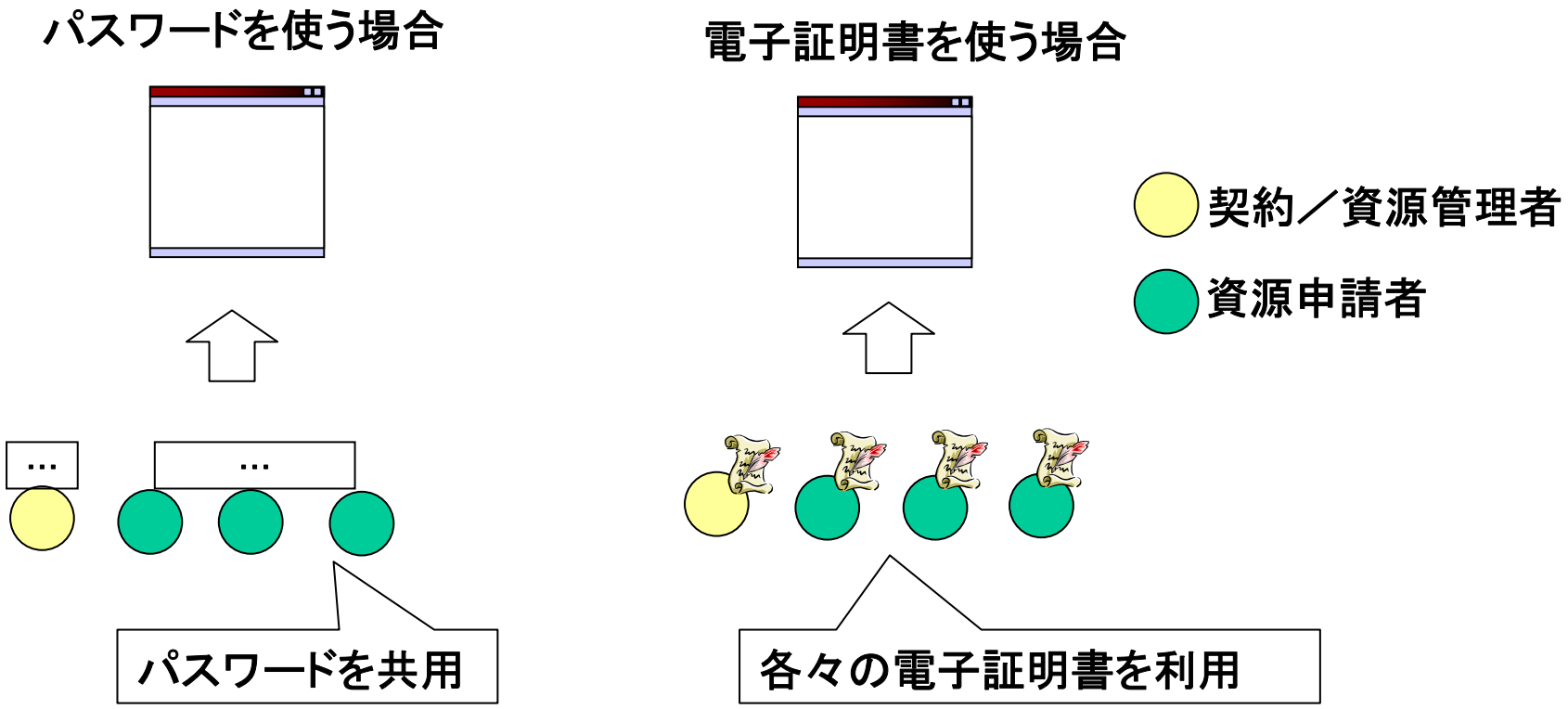
資源申請者 → 契約／資源管理者が"JPNIC RA Web"を使って申請

- 資源申請者の申請方法



電子証明書のユーザ(3)

- ログイン時のパスワードとの違い
  - 各々の申請者が別々の電子証明書を利用



まとめ：PKIを用いた認証強化実験

- IPレジストリシステムにおけるSSLの「クライアント証明書」を使った認証
  - 今回の実験参加の対象はIP指定事業者です。
  - ご参加をお待ちしております。
- JPNIC認証局のWebページ
  - http://jpnic-ca.nic.ad.jp/
- 証明書の利用上の各種お問い合わせ
  - ca-query@nic.ad.jp

ご静聴ありがとうございました。

社団法人日本ネットワークインフォメーションセンター
木村 泰司

資料編

社団法人日本ネットワークインフォメーションセンター

JPNIC認証局のfingerprint

- JPNIC Root Certification Authority
  - SHA-1
    ce89 1399 5cd0 b1a4 39de b455 2628 9ce1 fe85 af1e
  - MD5
    8A:79:EE:FE:5A:2D:FD:4A:6F:4E:8C:92:31:5F:DB:A1

- JPNIC Resource Service Certification Authority
  - SHA-1
    ab46 e8be cfde 1162 11df 4def 7cd3 d541 786f c68e
  - MD5
    92:57:25:96:17:3A:D9:DC:AA:38:38:7C:39:2E:59:9D

追加情報：Webトランザクション

- 電子証明書を使って割り当て報告のバッチ転送ができる機能を提供予定
  - https を使ったトランザクション
  - SSLの相互認証
  - マニュアル、サンプルコード提供予定
- 詳しくはJPNIC認証局のWebページをご覧下さい。