電子証明書による申請について

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

内容

- 電子証明書による申請について
- 電子証明書の利用方法について
- 資源申請者用の電子証明書
  発行の流れ

背景

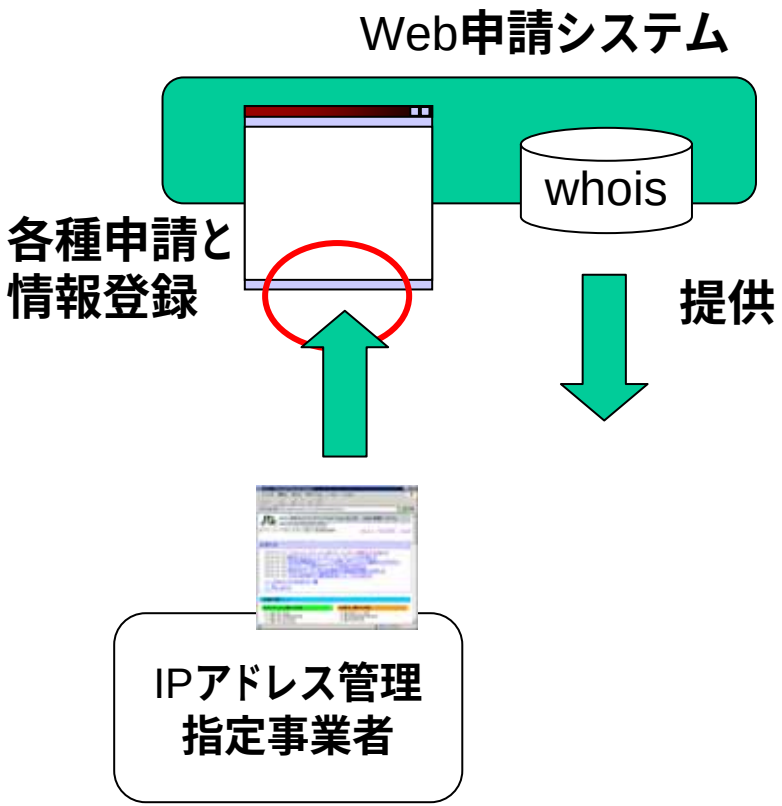
- **電子証明書の利用開始**
  - 「PKIを用いた認証強化実験」
    2005年7月7日 第8回OPM
  - **認証強化実験の説明会**
    2005年9月1日 JPNIC

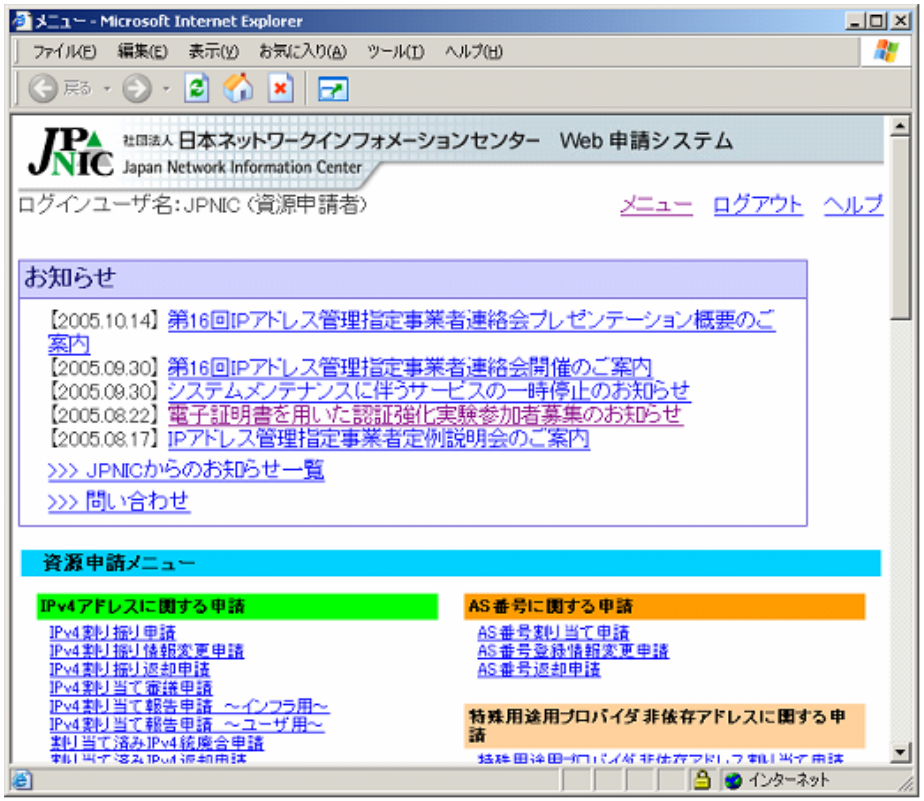
電子証明書による申請

- Web申請システムへのログインに電子証明書を利用
  - "PKIを用いた認証強化実験"の実施中
    - 目的：電子証明書の利用可能性の検証
      - パスワードも利用可能
      - ユーザ認証の方式が異なるだけで、一旦ログインした後の申請業務は従来通り

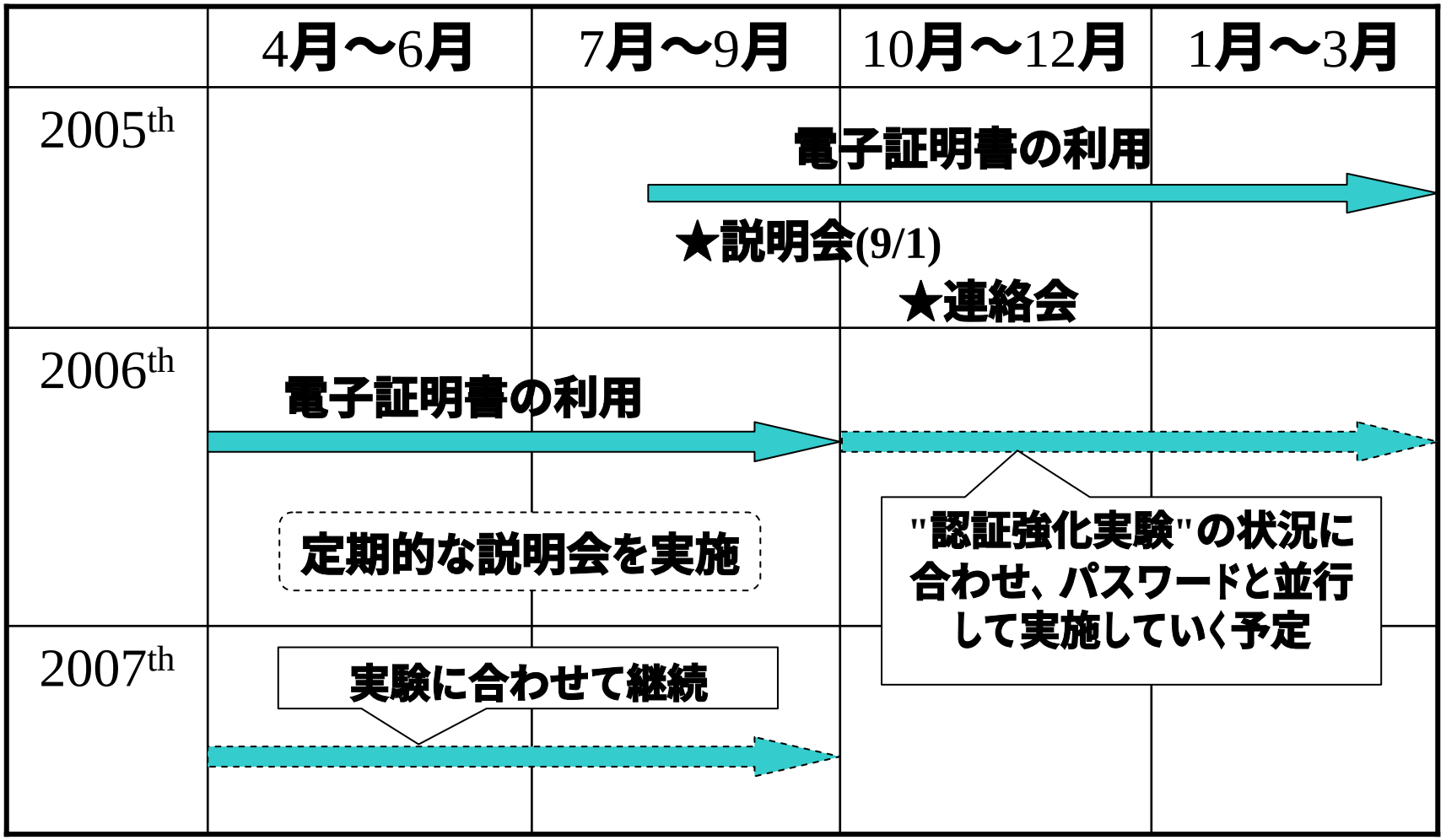
Web申請システムにおける認証

- Web申請システム
  - 各種申請と情報登録の為のシステム





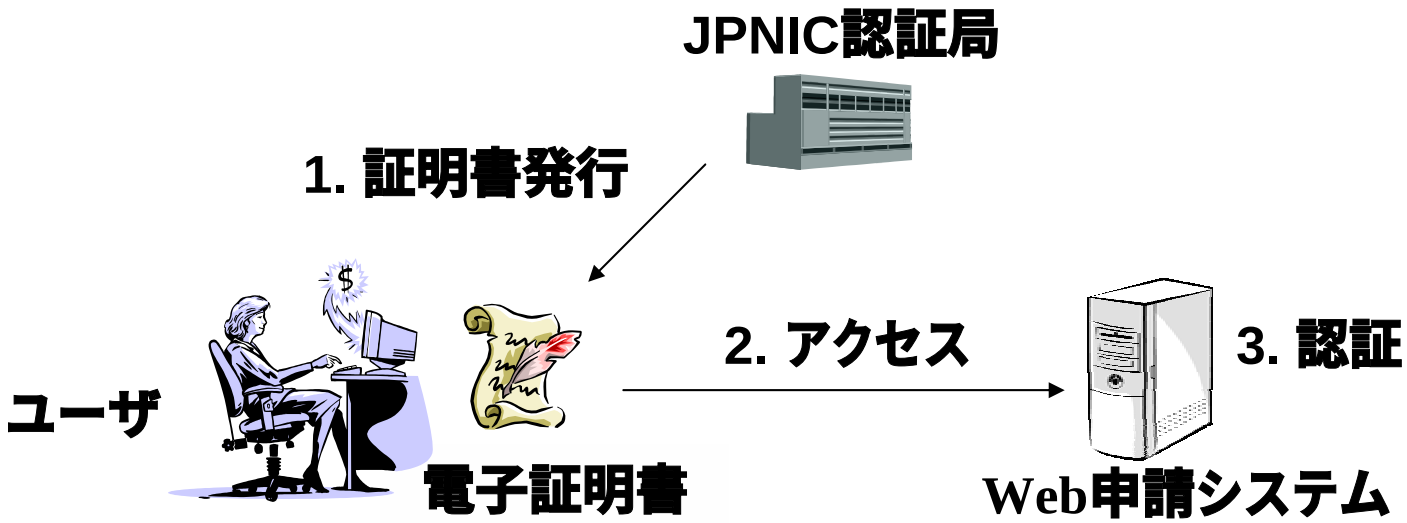
電子証明書利用のスケジュール



電子証明書

- ユーザ認証の為の電子証明書の利用

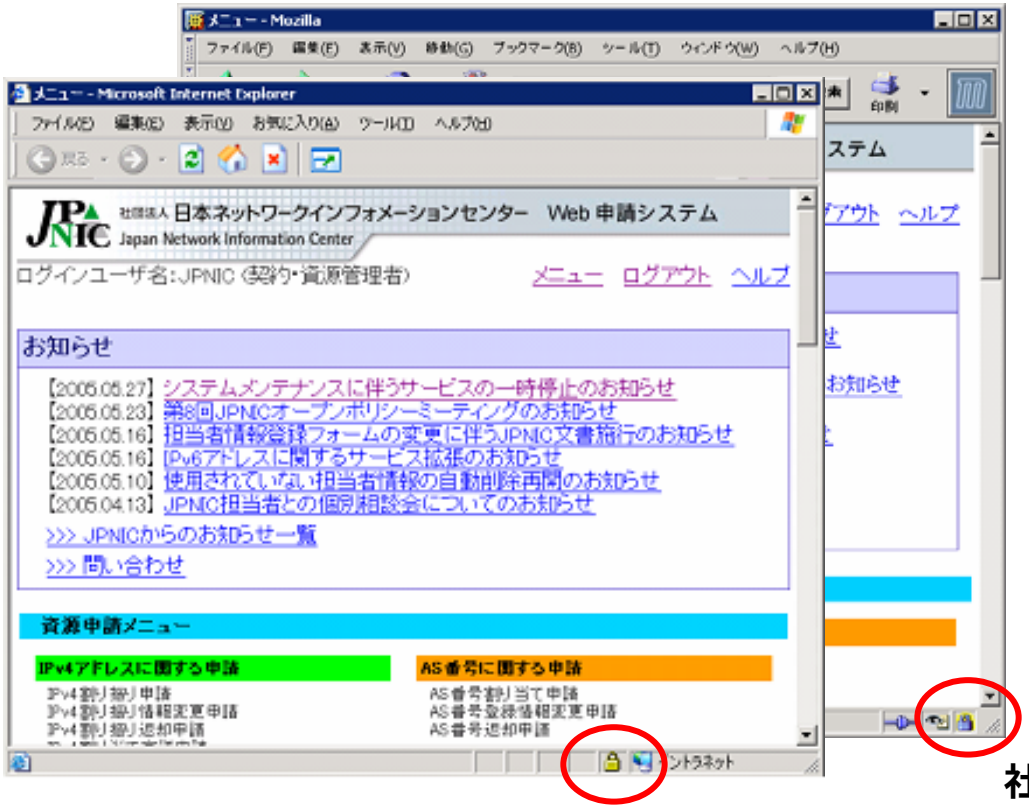
JPNICにおける電子証明書の利用例

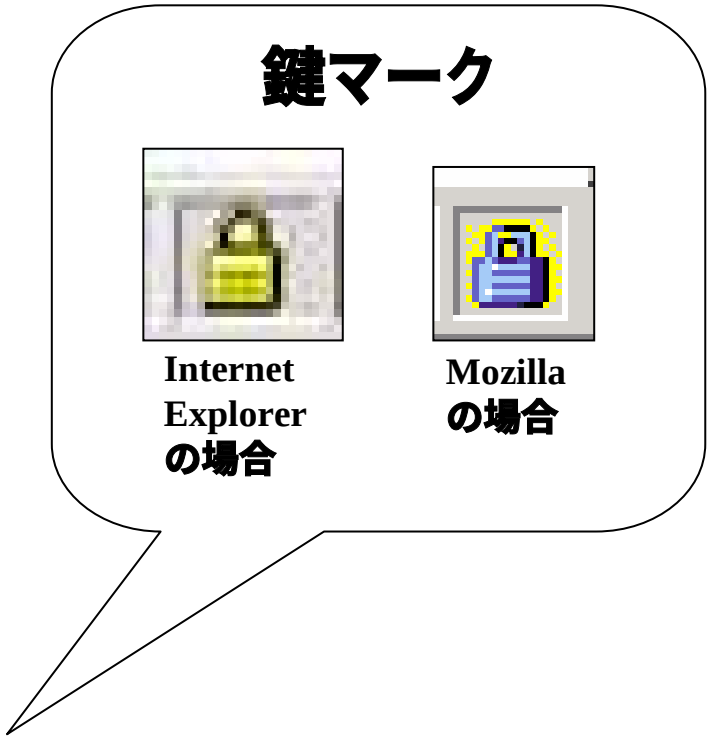


予め認証局から発行された
電子証明書を使ってユーザを認証

電子証明書の利用例

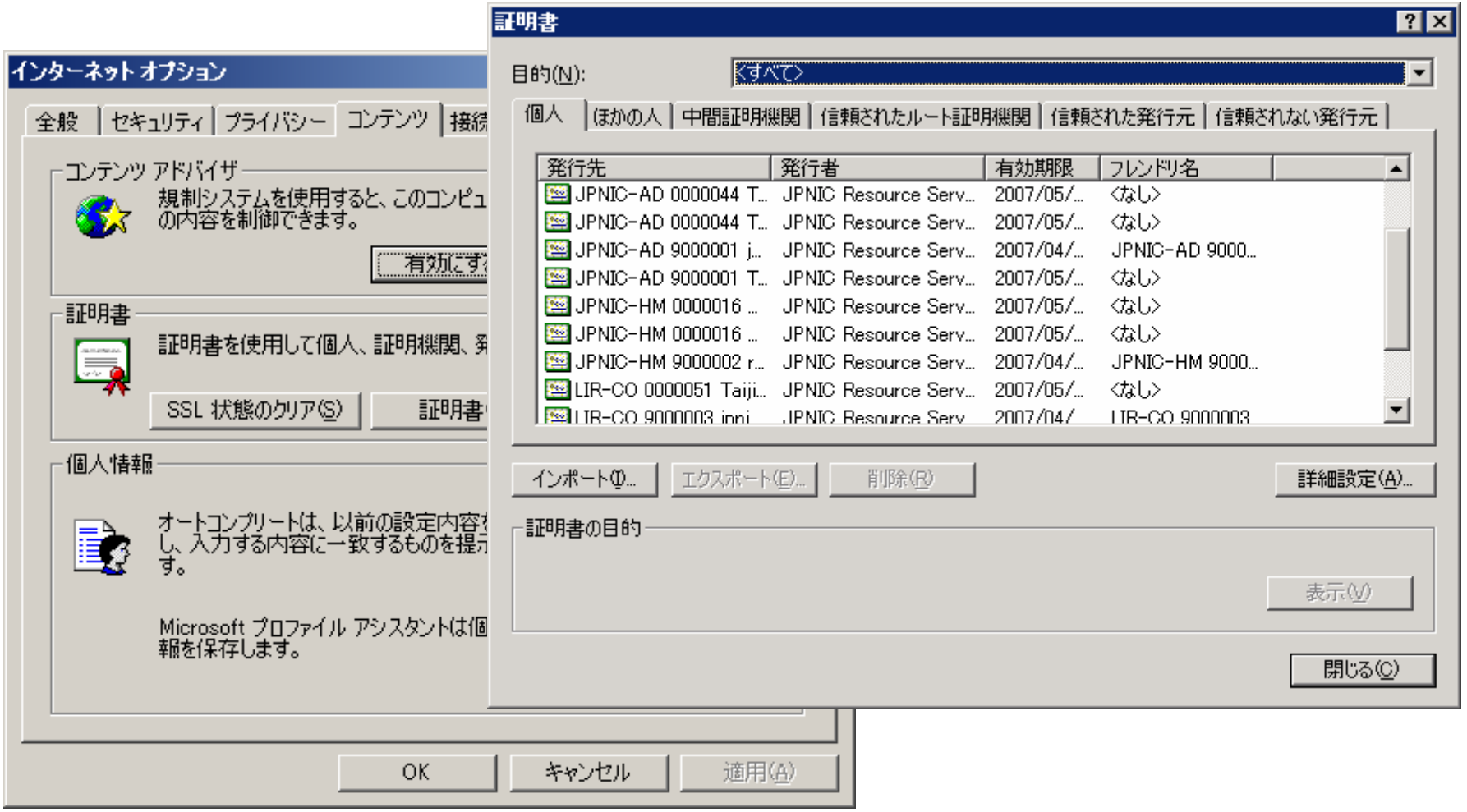
- SSLのクライアント認証
  - サーバとクライアントで相互に認証（なりすましを検出）
  - 暗号通信（通信路の盗聴が難しい）





Webブラウザにおける電子証明書の利用

- Webブラウザへの組み込み



電子証明書の利用方法について

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)

	役割	電子証明書の利用形式
契約・資源管理者	・契約情報等の変更 ・資源申請者の証明書管理	資源管理カード(ICカード)
資源申請者	・資源申請	ソフトウェア・トークン(Webブラウザに組み込み)

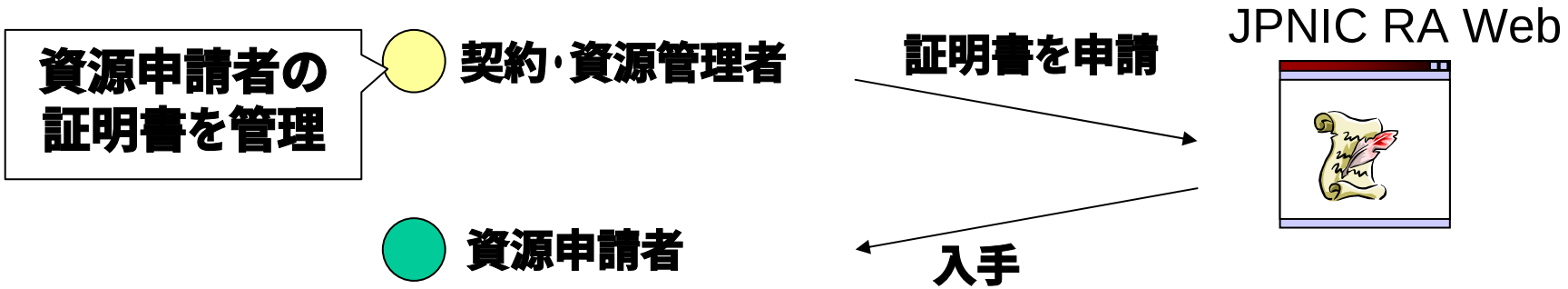
電子証明書のユーザ(2)

- 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

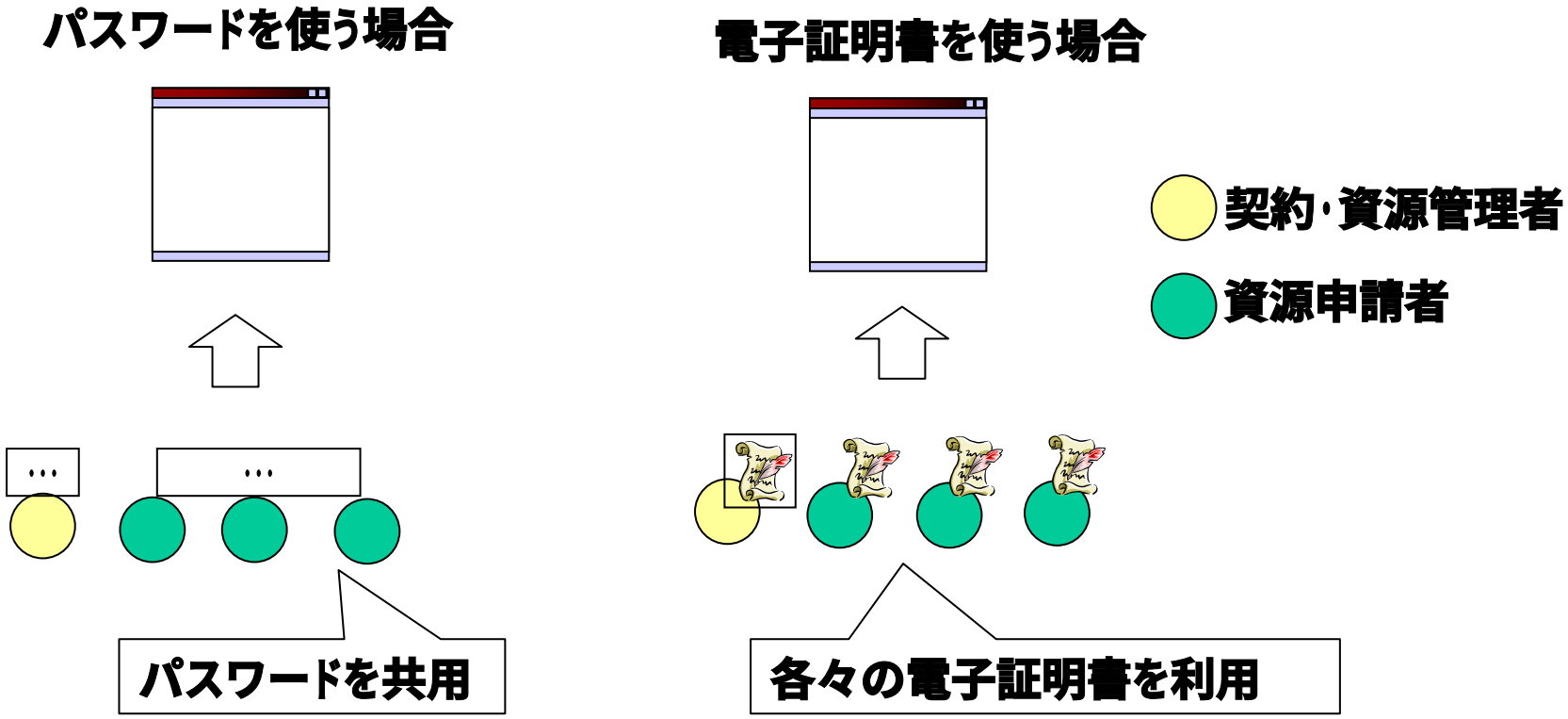
資源申請者 → 契約･資源管理者が"JPNIC RA Web"を使って申請

- 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認証との違い
  - 各々の申請者が別々の電子証明書を利用



契約･資源管理者の電子証明書
発行申込の方法

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

契約／資源管理者の電子証明書

- 申込方法
  - 書類を入手
    - 電子証明書の利用規約
    - 実験参加申込書
  - 記入後、JPNICへ送付
    - その他の必要書類
      - IP指定事業者である組織の身分証明書（社員証）の写し
- 発行
  - 資源管理カード（ICカード）、ICカードリーダ
    各種マニュアル等を郵送

資源管理カード

資源管理カードをICカード
リーダに挿入

資源管理カード

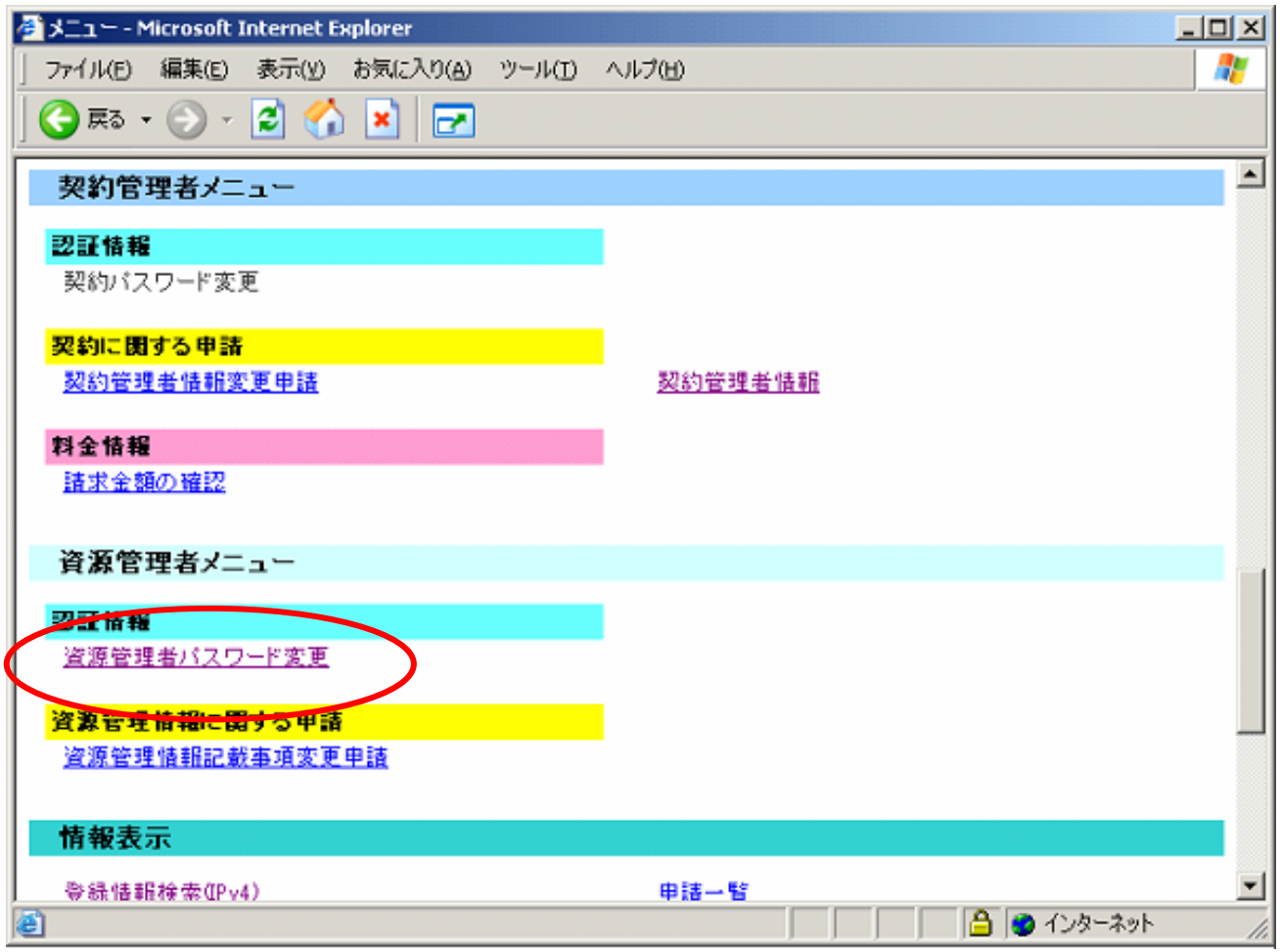
Webブラウザでアクセスし
パスフレーズを入力

トップページに直接アクセス

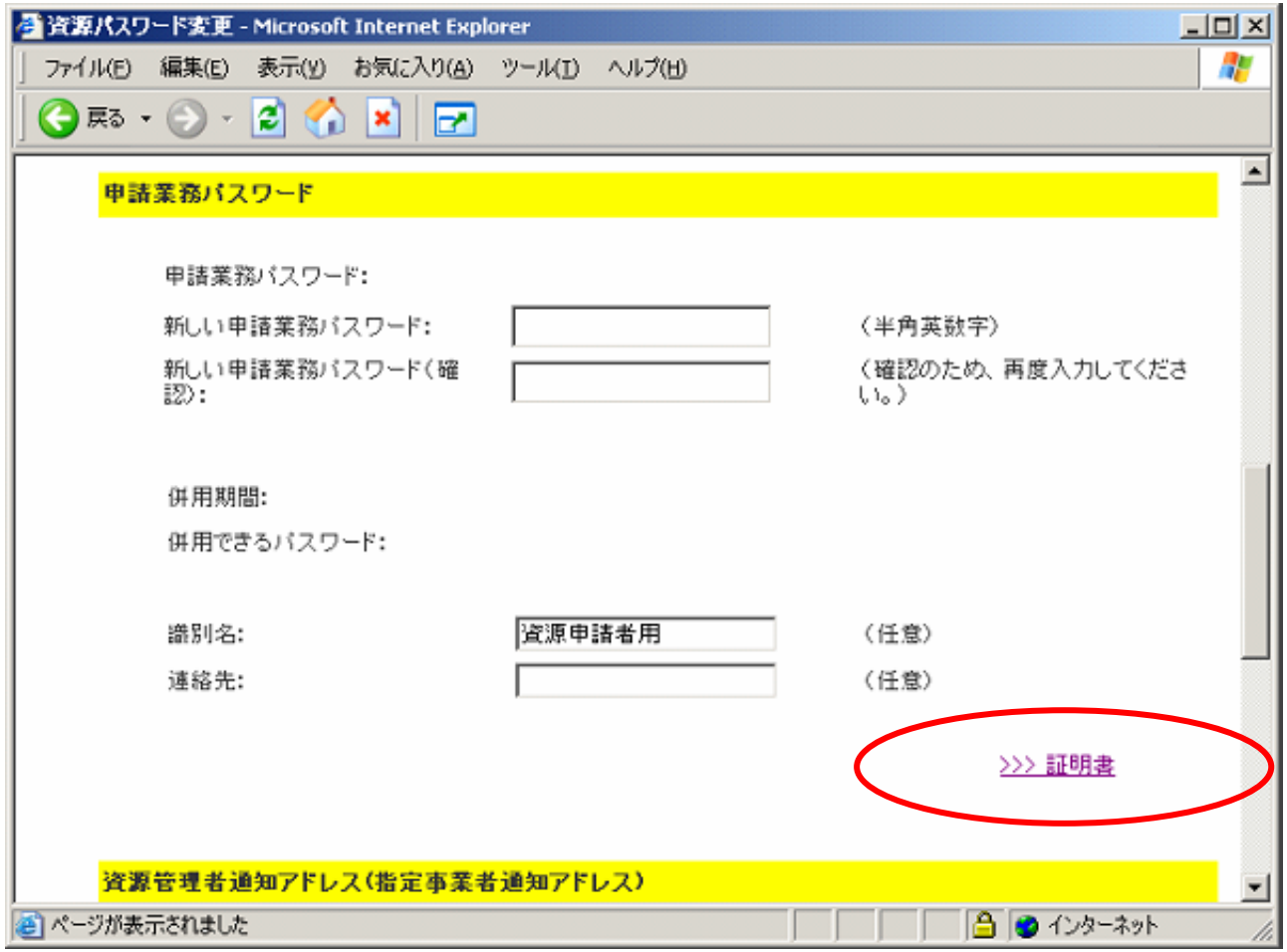
資源申請者用の電子証明書
発行の流れ

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

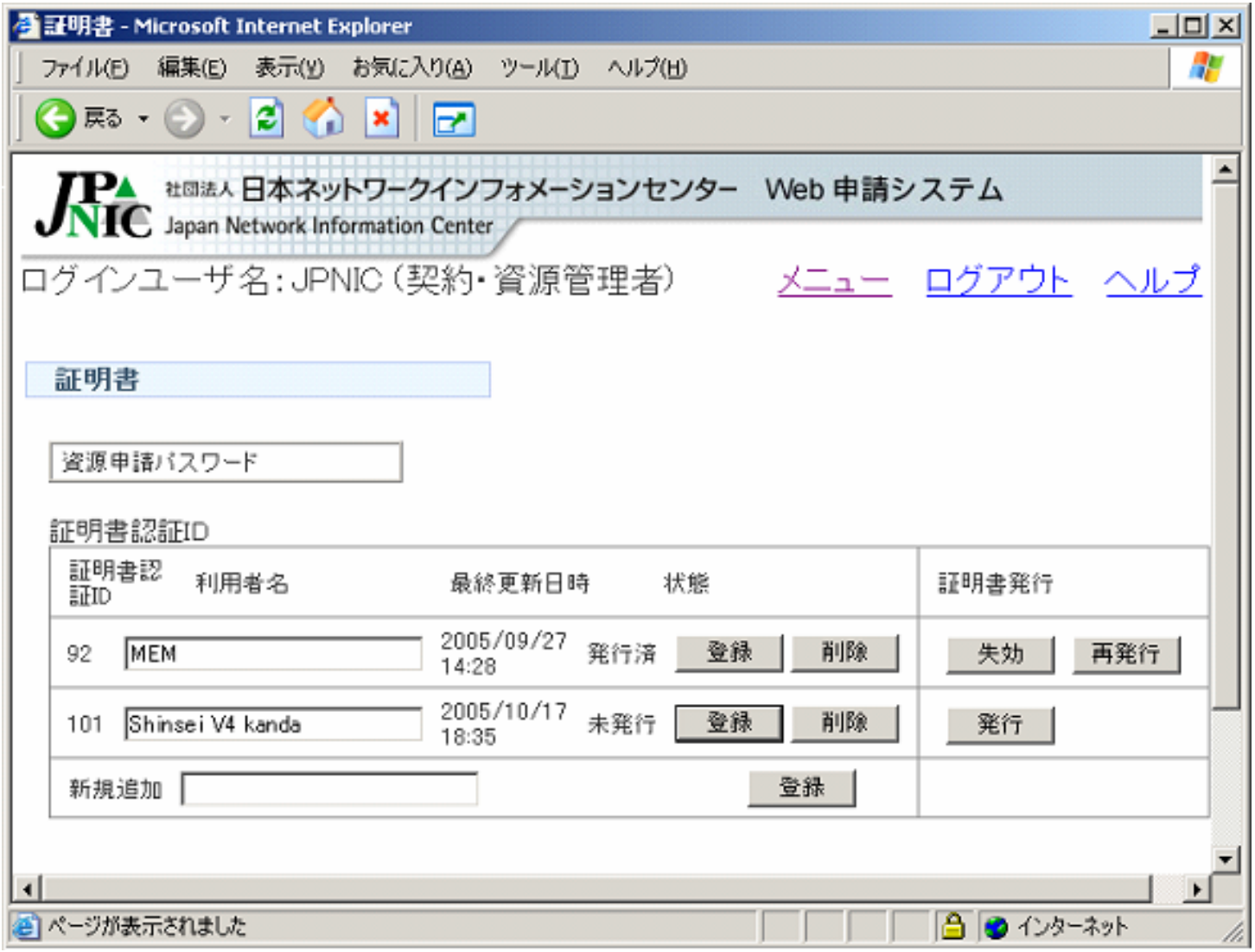
証明書管理 (1)


メニュー - Microsoft Internet Explorer
ファイル(F) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)
戻る
契約管理者メニュー
認証情報
契約パスワード変更
契約に関する申請
契約管理者情報変更申請
契約管理者情報
料金情報
請求金額の確認
資源管理者メニュー
認証情報
資源管理者パスワード変更
資源管理情報に関する申請
資源管理情報記載事項変更申請
情報表示
登録情報検索(IPv4)
申請一覧
インターネット

証明書管理 (2)


資源パスワード変更 - Microsoft Internet Explorer
ファイル(F) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)
戻る
申請業務パスワード
申請業務パスワード:
新しい申請業務パスワード:
(半角英数字)
新しい申請業務パスワード(確認):
(確認のため、再度入力してください。)
併用期間:
併用できるパスワード:
識別名:
資源申請者用
(任意)
連絡先:
(任意)
>>> 証明書
資源管理者通知アドレス(指定事業者通知アドレス)
ページが表示されました
インターネット

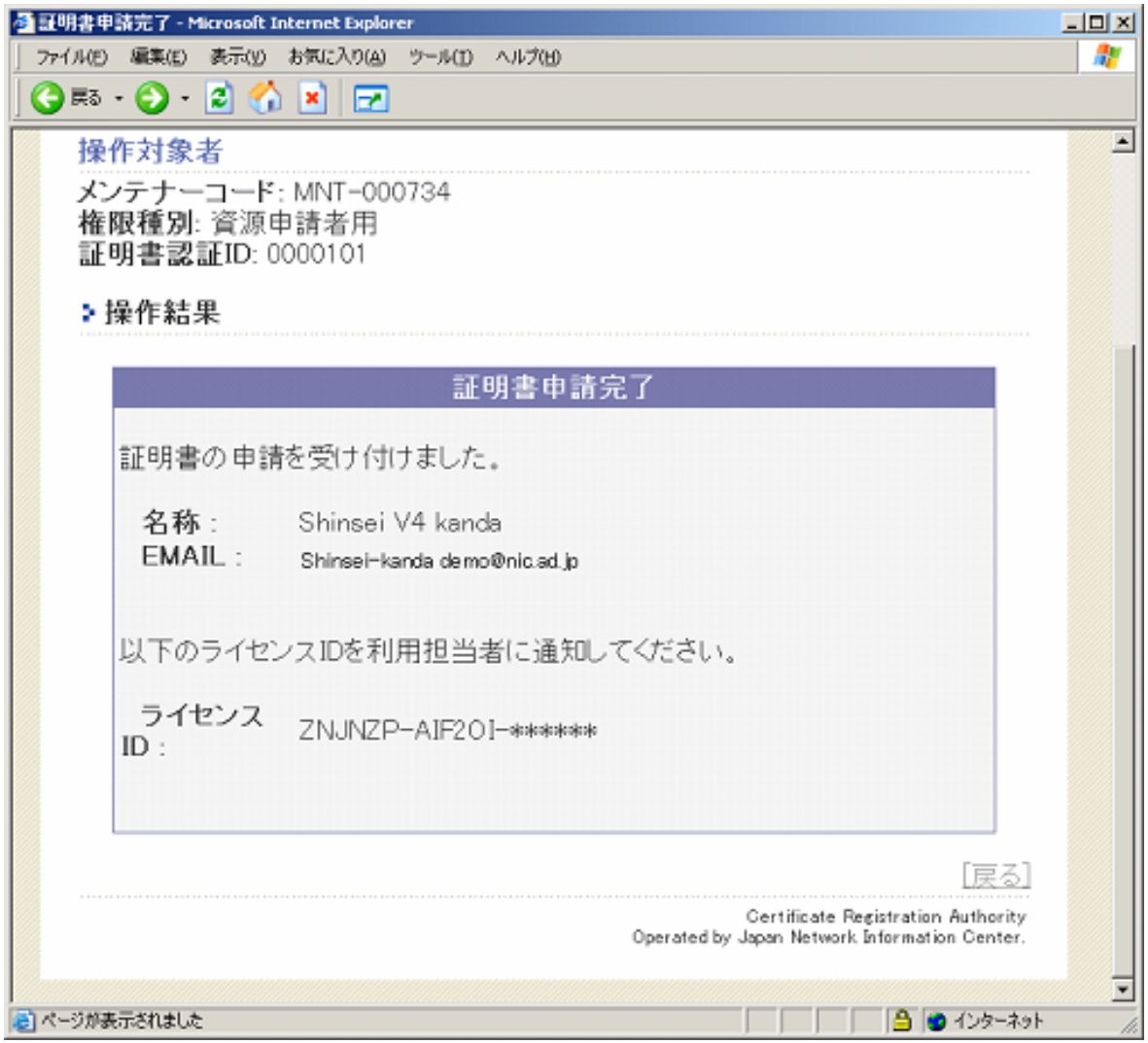
証明書認証IDの管理


証明書 - Microsoft Internet Explorer
ファイル(F) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)
戻る
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 Web 申請システム
Japan Network Information Center
ログインユーザ名：JPNIC（契約・資源管理者）
メニュー ログアウト ヘルプ
証明書
資源申請パスワード
証明書認証ID
証明書認証ID 利用者名 最終更新日時 状態 証明書発行
92 MEM 2005/09/27 14:28 発行済 登録 削除 失効 再発行
101 Shinsei V4 kanda 2005/10/17 18:35 未発行 登録 削除 発行
新規追加 登録
ページが表示されました
インターネット

電子証明書の申請 (1)


証明書申請 - Microsoft Internet Explorer
ファイル(F) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)
JPNIC RA WEB
Certificate Registration Authority
管理者
メンテナーコード: MNT-000733
操作対象者
メンテナーコード: MNT-000734
権限種別: 資源申請者用
証明書認証ID: 0000101
証明書申請
証明書の発行申請を行ないます。発行対象者の名称とEMAILアドレスを入力してください。
なお、名称・EMAILともに半角64文字まで入力できます。
名称 :
Shinsei V4 kanda
EMAIL :
shinsei-kanda@nic.ad.jp
種別 :
資源申請者用
証明書を申請する
インターネット

電子証明書の申請 (2)


証明書申請完了 - Microsoft Internet Explorer
ファイル(F) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)
戻る
操作対象者
メンテナーコード: MNT-000734
権限種別: 資源申請者用
証明書認証ID: 0000101
操作結果
証明書申請完了
証明書の申請を受け付けました。
名称 : Shinsei V4 kanda
EMAIL : Shinsei-kanda demo@nic.ad.jp
以下のライセンスIDを利用担当者に通知してください。
ライセンス ID : ZNJNZP-AIF201-******
[戻る]
Certificate Registration Authority
Operated by Japan Network Information Center.
ページが表示されました
インターネット

ライセンスIDの通知

ライセンスID

ZNCAP-TEST3Y-82NTJP

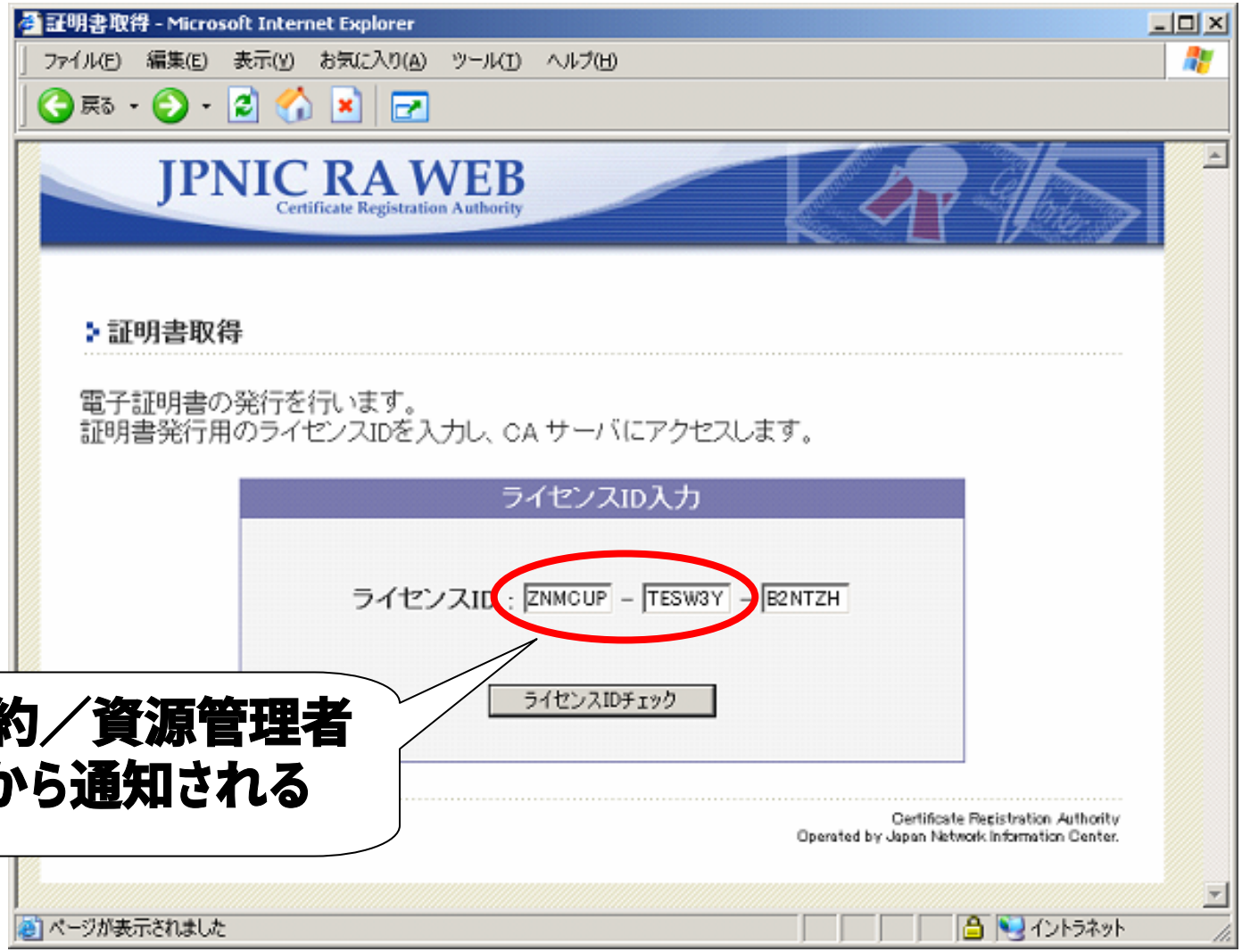
申請時に画面に表示　　メールで通知

契約／資源管理者

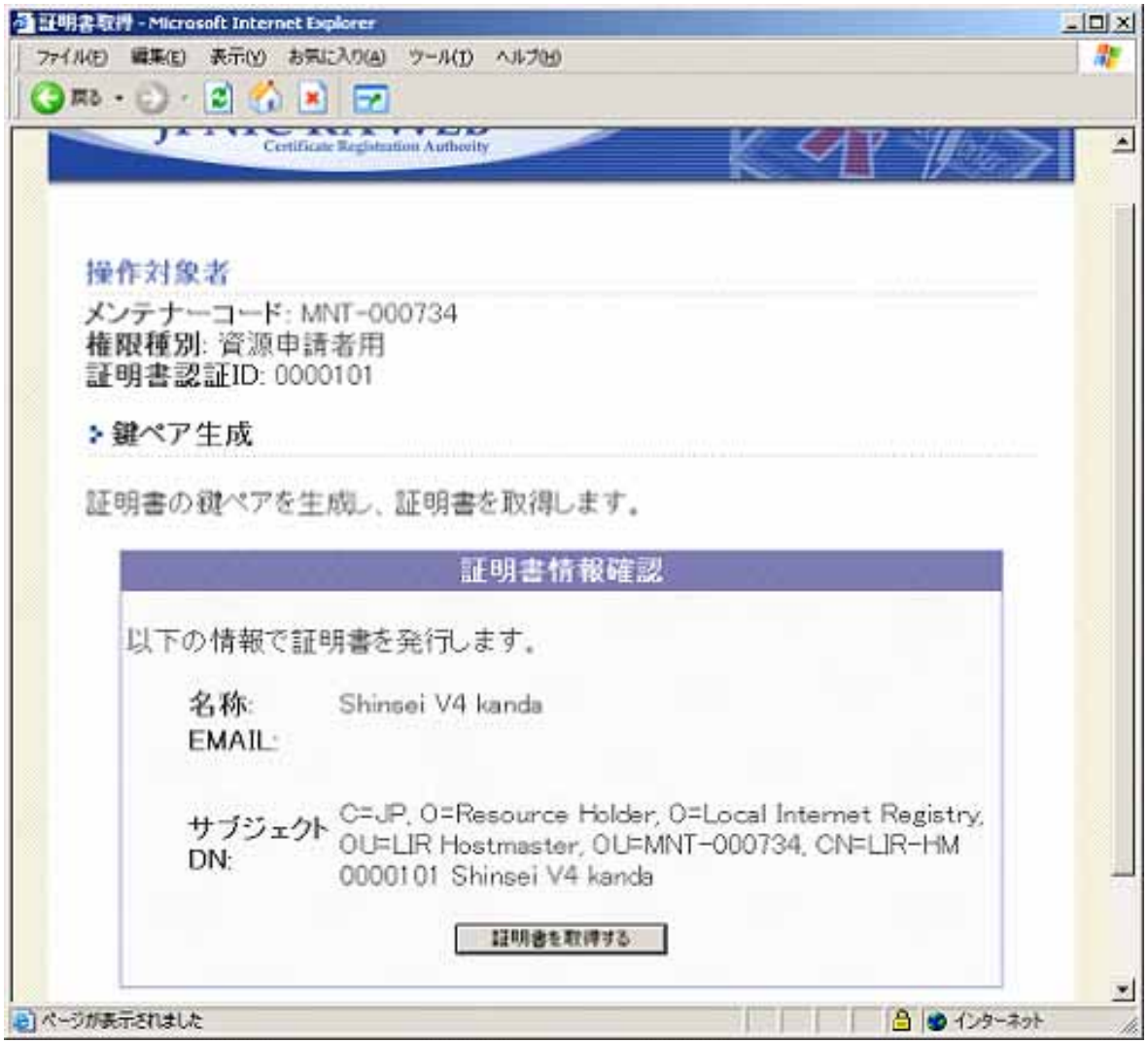
本人確認を行った
のちに下線部分を
オフラインで通知

資源申請者

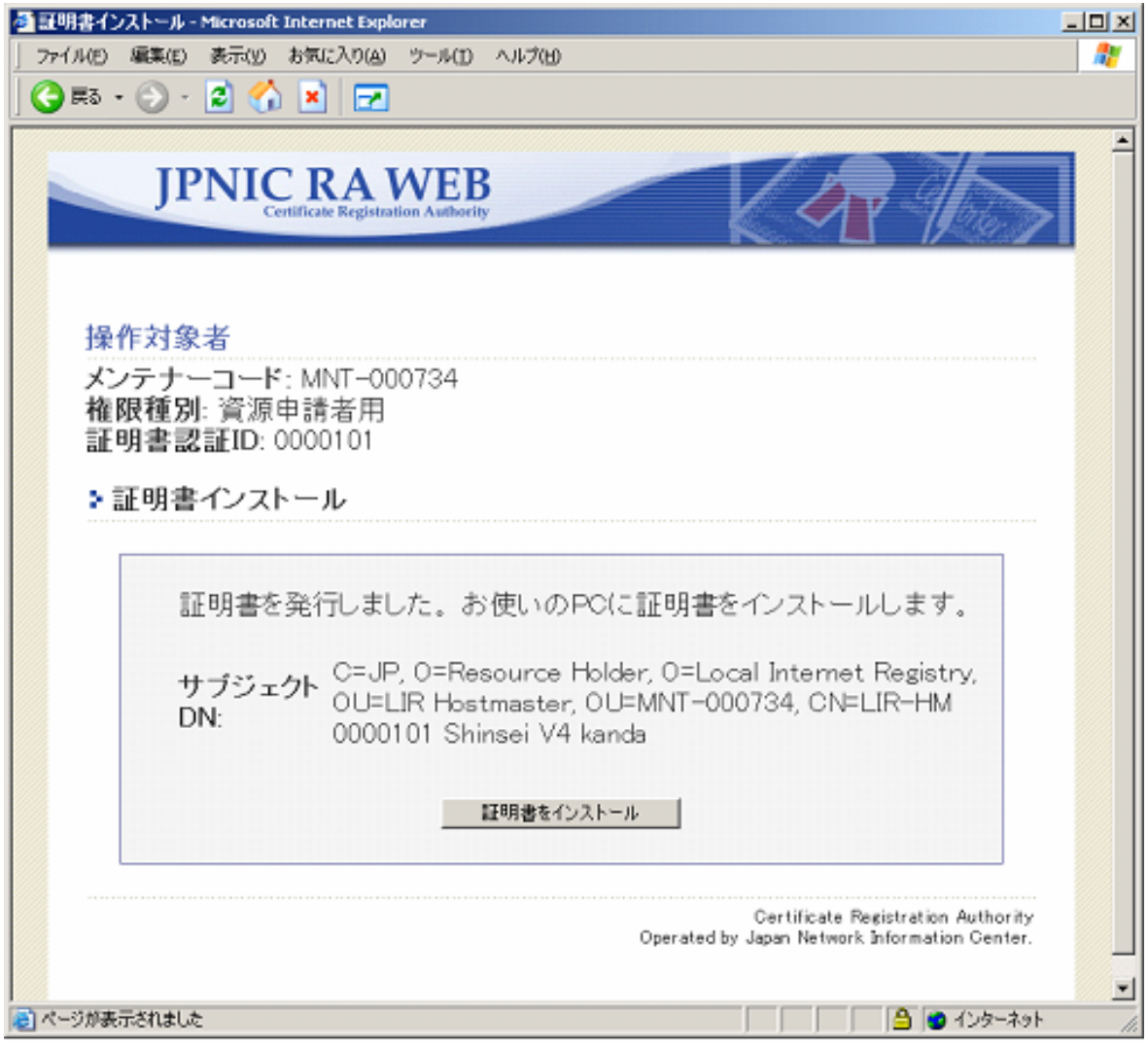
資源申請者によるライセンスIDの入力



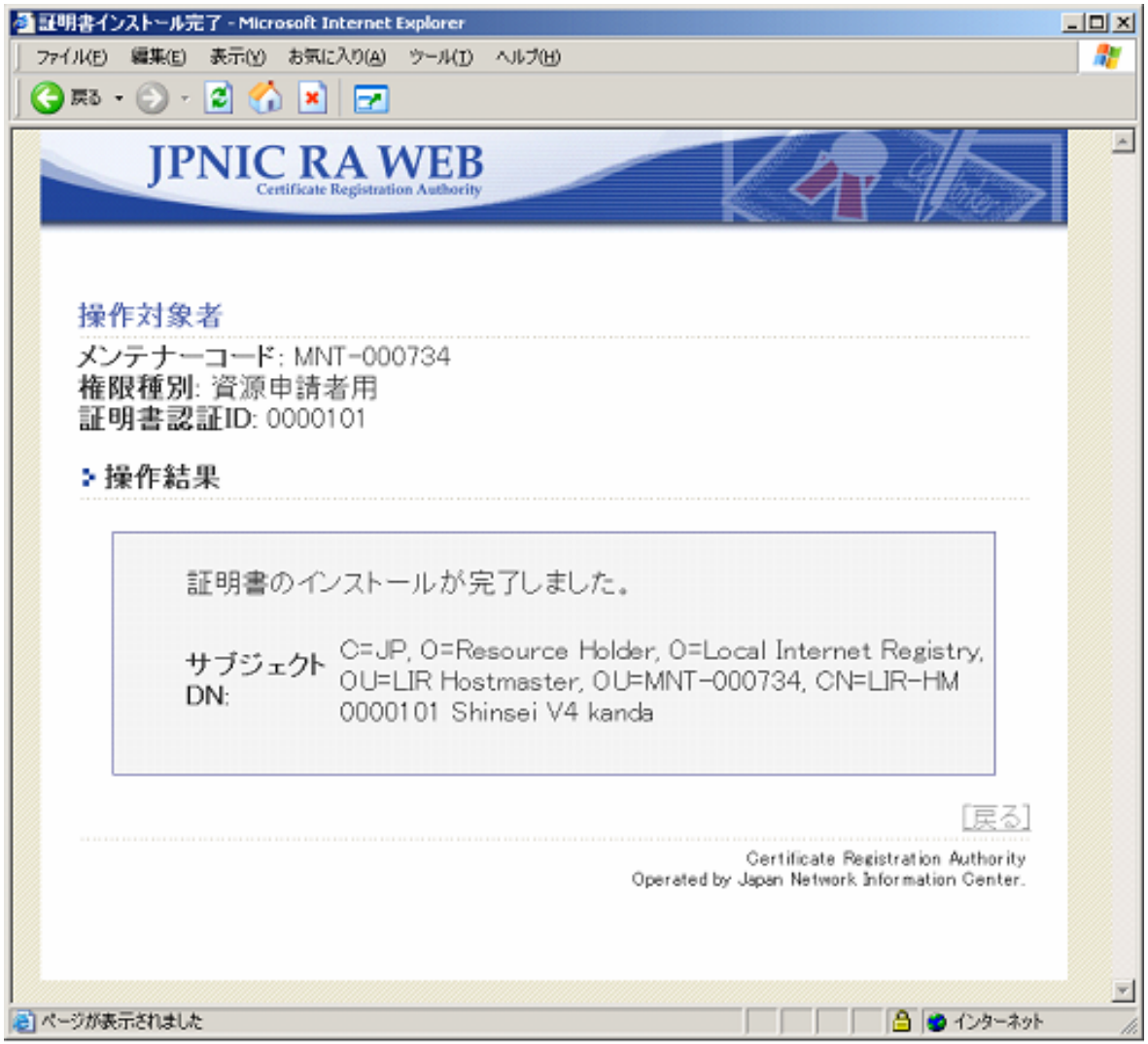
電子証明書の取得


証明書取得 - Microsoft Internet Explorer
ファイル(F) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)
戻る
Certificate Registration Authority
操作対象者
メンテナーコード: MNT-000734
権限種別: 資源申請者用
証明書認証ID: 0000101
鍵ペア生成
証明書の鍵ペアを生成し、証明書を取得します。
証明書情報確認
以下の情報で証明書を発行します。
名称: Shinsei V4 kanda
EMAIL:
サブジェクトDN: C=JP, O=Resource Holder, O=Local Internet Registry, OU=LIR Hostmaster, OU=MNT-000734, CN=LIR-HM 0000101 Shinsei V4 kanda
証明書を取得する
ページが表示されました
インターネット

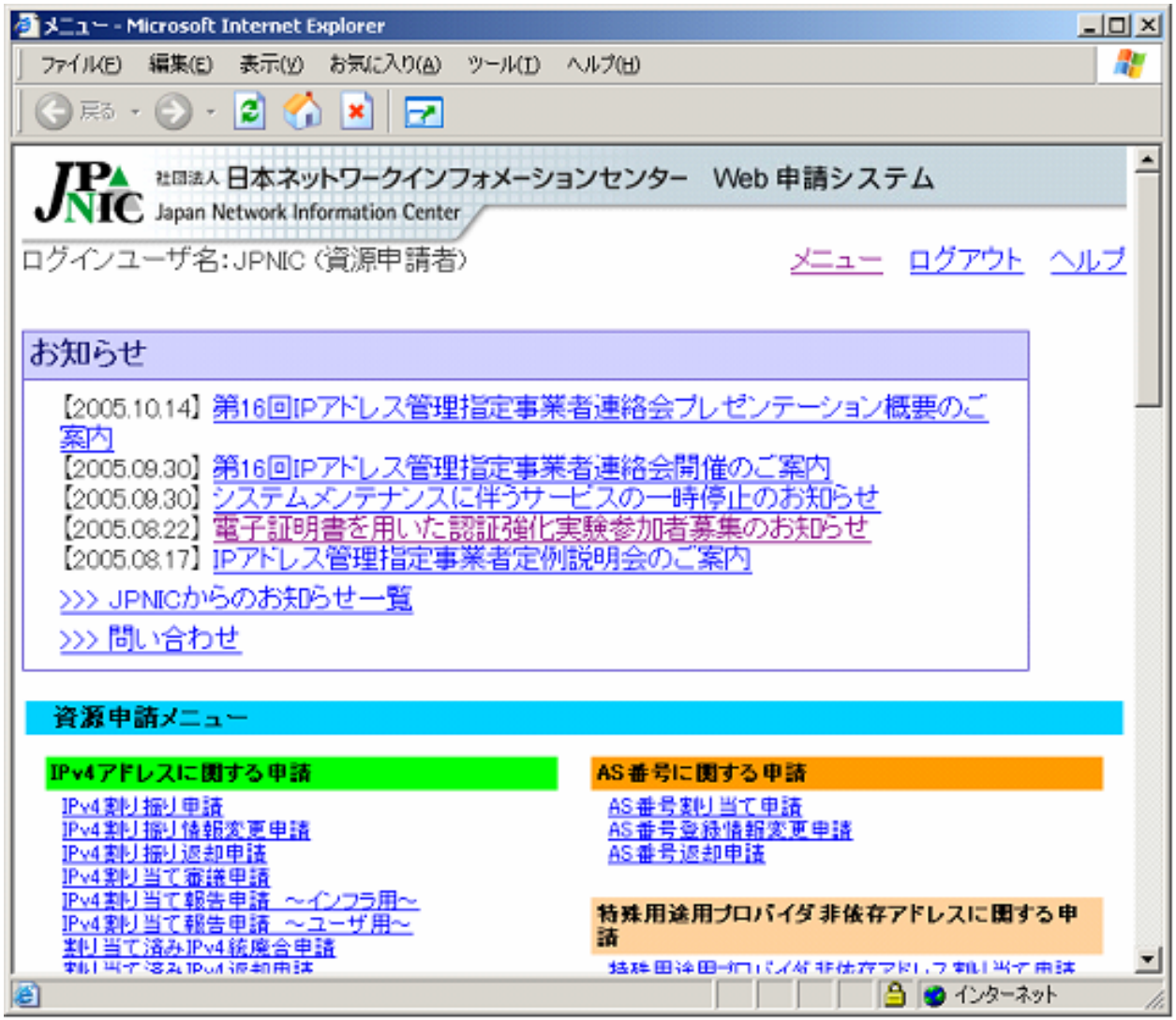
電子証明書のインストール (1)



電子証明書のインストール (2)



Web申請システムへのアクセス



まとめ

- 電子証明書による申請
  - "PKIを用いた認証強化実験"として実施している電子証明書を使ったWeb申請システムの利用
    - 契約／資源管理者
      - 「資源管理カード」を利用
      - 資源申請者の電子証明書を管理
    - 資源申請者
      - Webブラウザに電子証明書を組み込んで利用

情報提供と各種お問い合わせ

- JPNIC認証局のWebページ
  - http://jpnic-ca.nic.ad.jp/
- 電子証明書の利用上の各種お問い合わせ
  - ca-query@nic.ad.jp

  - IP指定事業者のみ、お申し込みが可能です。
  - ご利用をお待ちしております。

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 Primary Root Certification Authority S1
  - SHA-1
    07:B6:67:E7:73:04:0F:71:84:DB:0A:E7:B2:90:A3:38:D4:18:60:74
  - MD5
    DF:A6:2B:6B:CD:C6:D3:00:18:D5:67:2E:BE:76:D7:E9

- JPNIC Resource Service Certification Authority
  - SHA-1
    E1:0E:7E:2F:BE:C4:90:F7:89:74:2F:42:6D:8E:21:5E:12:D5:36:8E
  - MD5
    E6:41:A4:62:3C:1E:D4:0B:C1:9E:9B:AD:FC:44:D1:DA

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。