JPNIC認証局
～IPアドレス認証局(認証)～

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

- JPNICの認証局構築事例のご紹介
  - 検討の必要があった事項
    - CAを実用的にするための一つの工夫
    - ⇒　開発したシステム
  - CA構築の検討ポイント
- あるとうれしい4つの事
  - PKIのほんとうの普及を考えて

JPNIC
IPアドレス事業

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：日本のIPアドレスレジストリ

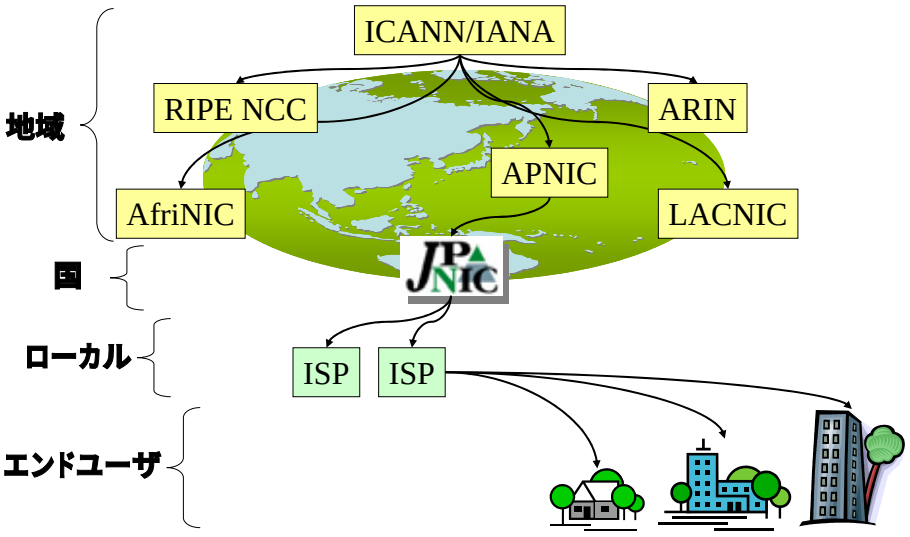
- IPアドレス事業
  - **IPv4アドレスの管理**
  - IPv6アドレスエージェントサービス
  - AS番号の管理
  - **IPアドレスレジストリシステムの提供（whois）**
  - **ポリシー策定**(IPv4,IPv6,AS)
  - **ほか**

JPNIC概要	
設立年月日	1997年3月31日
理事長	後藤 滋樹
（前理事長	村井 純）
監督官庁	総務省 文部科学省 経済産業省

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

インターネットレジストリシステム

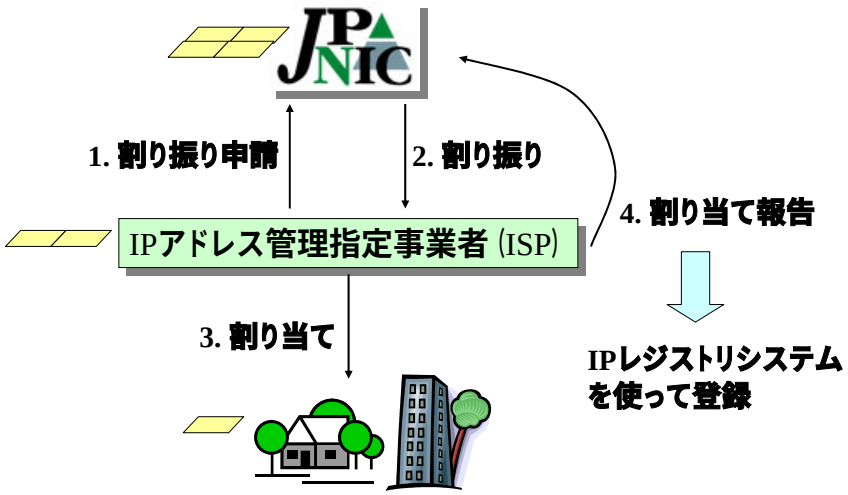
5



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アドレスの割り振りと割り当て

6



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

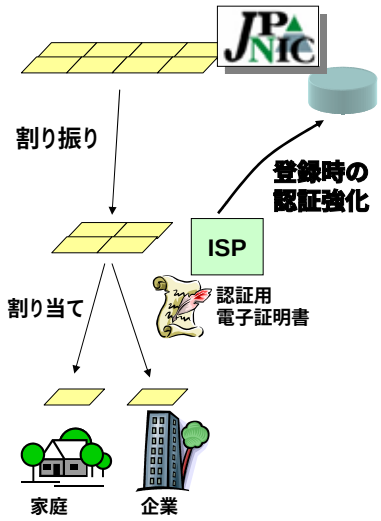
WHOIS

- WHOIS (JPNIC)
  http://www.nic.ad.jp/ja/whois/index.html

```
Network Information: [ネットワーク情報]
a. [IPネットワークアドレス]    202.12.30.0
b. [ネットワーク名]            JPNICNET
f. [組織名]
     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
g. [Organization]          Japan Network Information Center
m. [運用責任者]              SN3603JP
n. [技術連絡担当者]            HK8068JP
n. [技術連絡担当者]            NM050JP
p. [ネームサーバ]             ns1.nic.ad.jp
p. [ネームサーバ]             ns2.nic.ad.jp
```

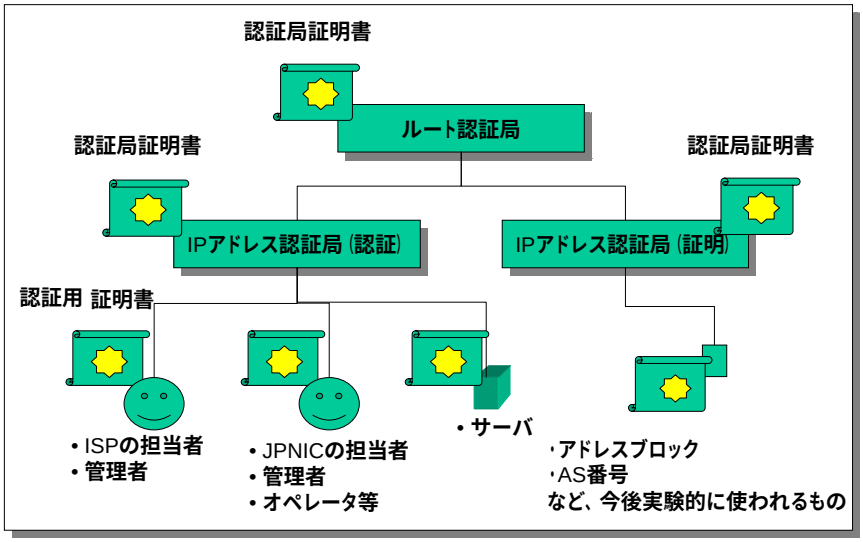
- **ネットワーク管理を目的とした検索**
  - **障害対応連絡、インシデントレスポンス、運用上の連絡ほか…**

IPアドレス認証局 (認証)



- JPNIC認証局の一つ
  - ISPにクライアント証明書(X.509形式)を発行
- IPレジストリシステム
  - IP指定事業者向け「Web申請システム」でTLSの相互認証で証明書を利用

JPNIC認証局（参考）



"簡単な電子証明書"
と
本人性確認問題

電子証明書を簡単に使ってもらうには

11

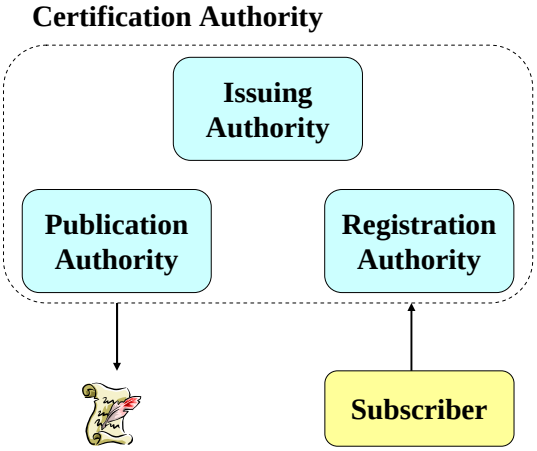
- パスワードとの手続きの比較
  - 利用開始／利用停止の時
    - 業務用パスワード：システム部にお願いする
      - ⇒　周りに経験者あり　身近　⇒　簡単
    - 電子証明書：認証局に申請
      - ⇒　本人性確認書類、経験少ない、身近？
  - 利用時
    - 業務パスワード：
      - 単純：主に自分の記憶の問題
    - 電子証明書：
      - 複雑：証明書検証の問題（対応方法も複雑）

本人性確認
手続きの複雑さ

本人性確認問題

12

本人性確認とバインディング

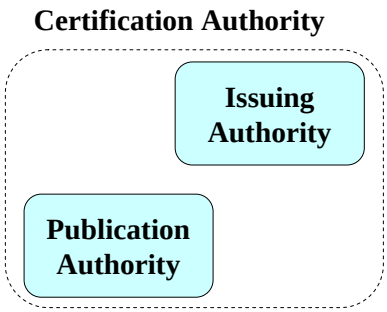


- 識別子
- 人
- 所属（性質）
- 権限
- 鍵

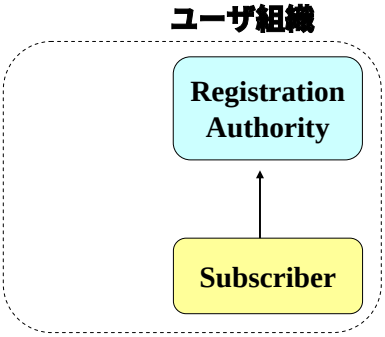
- 確認項目が多い程手間
- 第三者への手続きによる業務オーバーヘッド

外部RAモデル

13



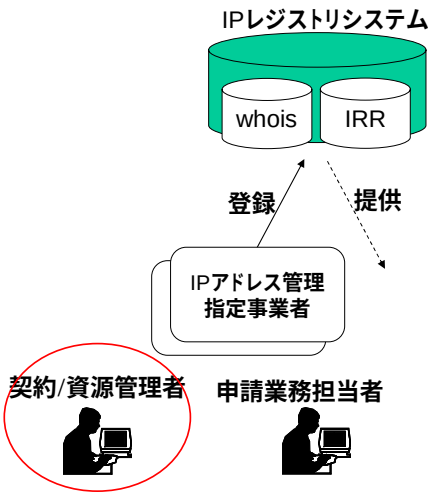
・RAが身近（経験者でもある）
・組織内の身分証明書あり
⇒ 人、所属、権限



商用サービスの多くが採用
・RA端末
・ICカード発行業務
などなど

JPNICの登録情報と登録主体

14



認証の責任はどこにあるのか？

JPNICに認証されるユーザと申請業務を行うユーザは異なる。

申請業務の担当者は契約者と別の組織にいる可能性がある。

契約/資源管理者に着目

対策：簡単さと本人性確認問題

15

- 簡単さ
  - 外部RAモデル
    - 単一の認証ドメインでの複数外部RA
      （身近、経験者あり、確認書類が減る）（不正抑止）
- 本人性確認問題
  - 識別子 ⇒ IPレジストリシステムより
  - 人 ⇒ 責任者の確認
  - 所属（性質） ⇒ 外部RAの身分証明
  - 権限 ⇒ IPレジストリシステムよりID
  - 鍵 ⇒ 申込時の初期パスワード

JPNIC RA Webの開発

IPアドレス認証局（認証）の場合

電子証明書のユーザ (1)

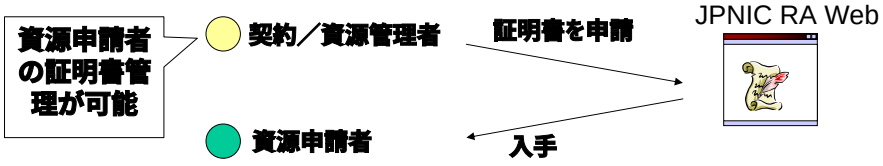
17

	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	ハードウェア･トークン (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)

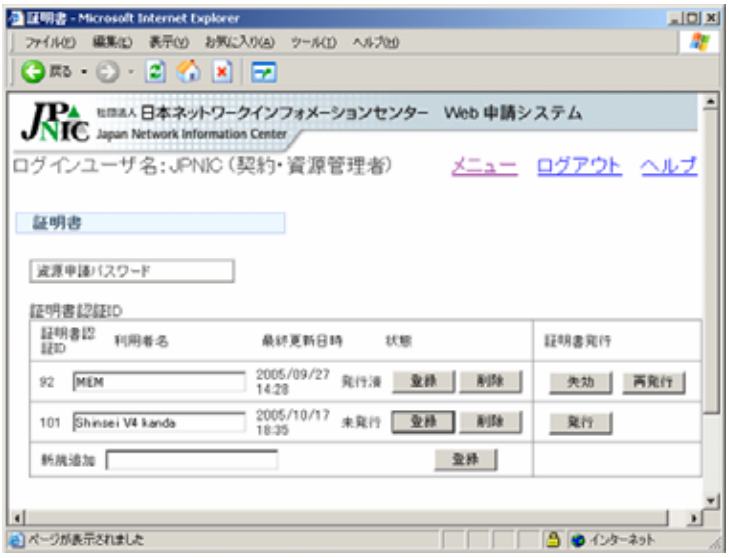
18

- 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



証明書認証IDの管理

19



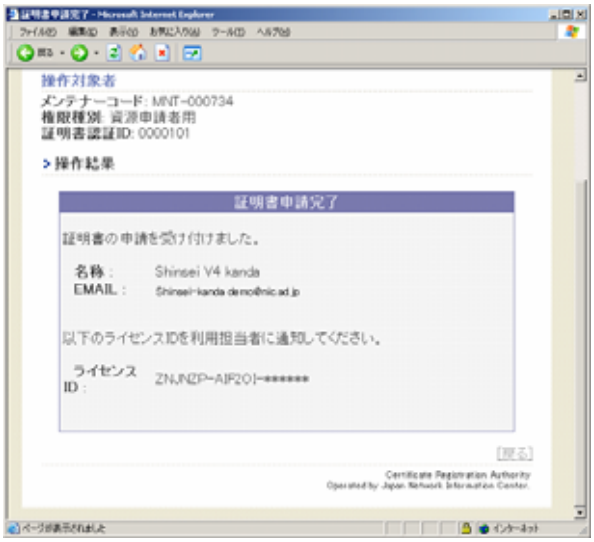
社団法人日本ネットワークインフォメーションセンター

電子証明書の申請 (1)

20

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

電子証明書の申請 (2)

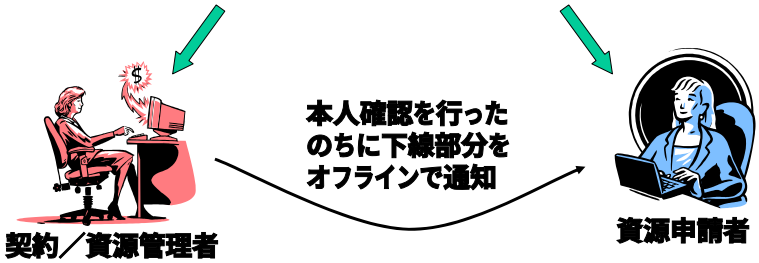


ライセンスIDの通知

ライセンスID

ZNCAP-TEST3Y-82NTJP

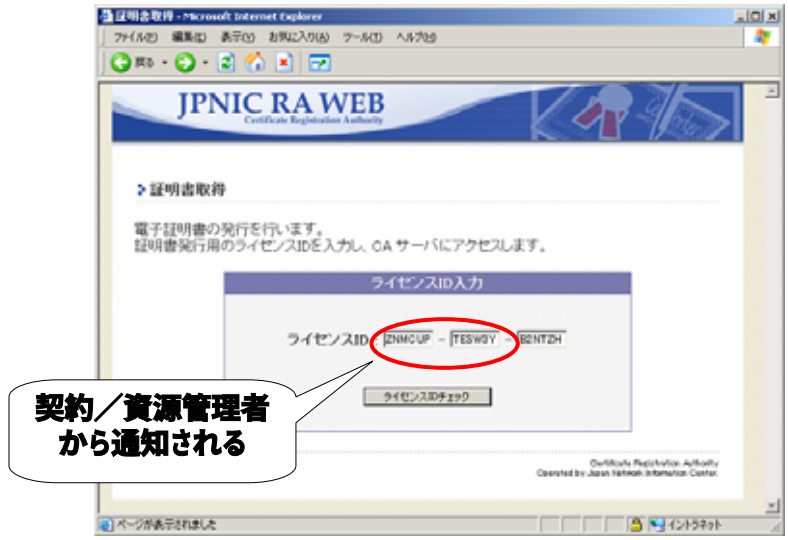
申請時に画面に表示　　メールで通知



契約／資源管理者　　資源申請者

資源申請者によるライセンスIDの入力

23



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

電子証明書の取得

24

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

電子証明書のインストール (1)

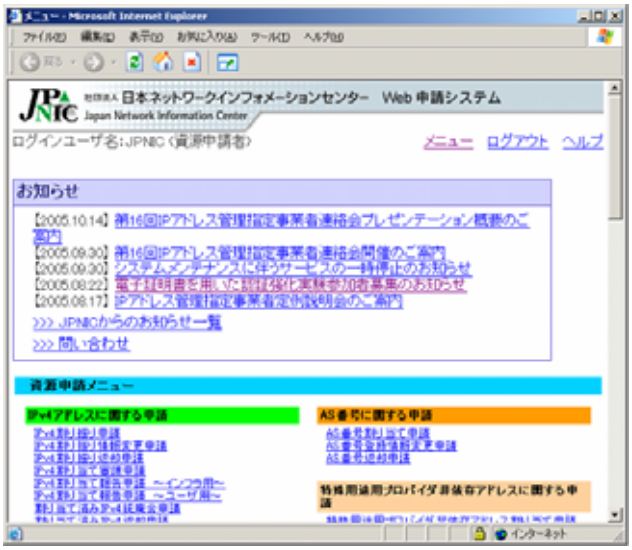
25

電子証明書のインストール (2)

26

Web申請システムへのアクセス

27



つまり　～この外部RAモデルの効用～

28

- 簡単さ
  - ユーザの登録時の手間を減らす
    - (契約／資源管理者だけに絞った)
  - ユーザの証明書管理の手間を減らす
    - (Webインターフェースで管理)
- 本人性確認問題
  - 確認の為の書類を減らす
    - (実質的に契約／資源管理者のみ)
    - (責任の所在を明らかにしておく必要)
  - 残った課題 (まだ難しいこと)
    - ICカード環境設定
    - 認証局証明書インストール手順

CA構築の検討ポイント

私はここで困りました

CA構築の検討ポイント　その1

- 認証局証明書を作るとき
  - fingerprintの残し方
  - 鍵ペアの残し方
  - 忘れちゃいけないパスフレーズの扱い方
- 認証局証明書を作ったとき
  - fingerprintの配り方
  - 運用の粛正
    - 発行プロセス／承認プロセス
  - 認証局証明書の操作
    - キーロールオーバー
    - CRLの更新間隔

CA構築の検討ポイント　その2

31

- EE認証用の証明書を始めるとき　**本日の話題**
  - 本人性確認を行うところ
    - 組織、部署
  - 本人性確認の実施方法
    - ルーズな本人性確認の抑止方法
  - 目的外使用の禁止
    - 禁止／禁止しない（責任とらない）
  - アカウント（ID）とEEの整合性
    - 業務システムのアカウントの有効性

CA構築の検討ポイント　その3

32

- 証明書フィールド
  - アカウントの識別子（ID）をどう入れるか
  - 有効期限
  - criticality
  - CRLDP / authorityInfoAccess
  - ポリシーID

あるとうれしい4つの事

PKIのほんとうの普及を考えて

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

1.EE証明書取り扱いの共通認識

- 証明書にどんなフィールド入れたらいいか
  - critical / non-critical （実際の効用を踏まえて）
  - 最低限入れておきたいフィールド
  - 検証者の挙動を想定できる何か（ドキュメント）

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

2.EE認証レベルの定義（運用面）

35

- 民間企業／法人で担当者や社印と推定される証明書は何か
  - 本人性確認のレベル
  - 失効情報提供のコモンセンス
  - （その業界の）オフライン／オンライン認証のあり方ガイド
    - 認証局監査基準
    - ガイドライン

3.CA証明書の取り扱いガイド（認証局）

36

- CA証明書の取り扱い
  - 証明書とfingerprintの配り方
  - キーロールオーバー
  - CRLの更新間隔の考え方
- 運用の粛正（不正の抑止）
  - 発行プロセス／承認プロセス

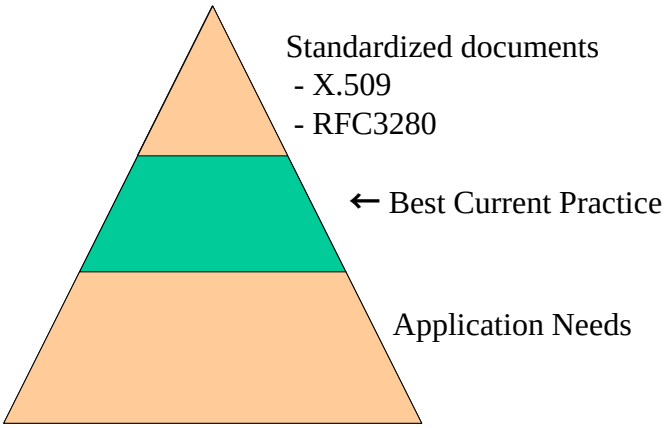
4.CA証明書の取り扱いガイド (RP)

37

- CA証明書の取り扱い
  - トラストポイントの種別
  - 検証時の表示では何が出ているべきか
  - 失効検証に期待できること

PKI 利用現場の現状

38



まとめ

- IPアドレス認証局（認証）の事例紹介
  - 外部RAモデルの効用
- CA構築の検討ポイント
  - あるとうれしい4つの事

これからも認証はなくならない
⇒ PKIはあるけど、使うには検討事項が多くて…
⇒ 運用のための実用的な情報が足りない！
⇒ やってみてわかったこと（Best Current Practice）を皆さんで持ち寄りましょう！

ご清聴、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

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