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

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
木村 泰司

JPNICにおけるセキュリティについての調査研究

- IPアドレス認証局に関する調査研究
  - 2002年度より、JPNICにおける認証局に関して調査
  - 経済産業省からの受託研究でもあり、毎年報告書を公開
    - IPアドレス認証局のあり方に関する調査研究（2003年3月）
      http://www.nic.ad.jp/ja/research/200303-CA/
    - IPアドレス認証局のマネジメントに関する調査研究（2004年4月）
      http://www.nic.ad.jp/ja/research/200404-CA/

はじめに　－　本発表の目的

- JPNIC認証局を紹介
  - "レジストリデータの信頼性を向上させ、IPアドレスとAS番号、またはレジストリ構造を用いた認証環境を作る"という考え方について

- ご意見を頂きたい点
  1. JPNIC認証局のアイディアの妥当性
  2. レジストリデータ（アドレスブロック、AS番号）の認証局基盤を使ったネットワーク運用の安全性向上について。JPNIC認証局はどこまで役割を持つべきか。

内容

1. レジストリデータとJPNIC認証局について
   - レジストリデータのセキュリティとRIRの動向
   - 認証の考え方と保護機能

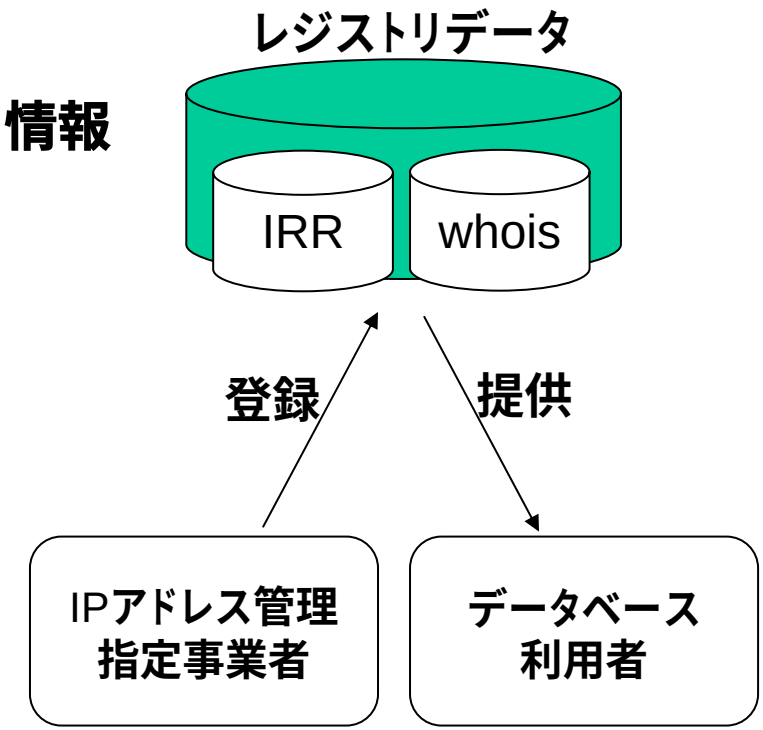
2. アドレスブロックの認証基盤
   - レジストリデータと証明書の応用

1.レジストリデータとJPNIC認証局について

- レジストリデータのセキュリティとRIRの取り組み
- 認証の考え方と保護機能

アドレス資源とレジストリデータ

- JPNICにおけるレジストリデータ
  - レジストリデータの要素
    - IP指定事業者への割り振り情報
    - ユーザネットワークへの割り当て情報
    - AS番号の割り当て情報
    - (連絡先、ホスト情報ほか)
  - レジストリデータの公開
    - whoisを使った公開
      - whois.nic.ad.jp
      - IRR (jpirr.nic.ad.jp)



レジストリデータはアドレス資源管理の元本

レジストリデータのセキュリティ

- レジストリデータの間違いによって起こりうる問題
  - 登録時／変更時の改ざん
    - 各種設定として参照される場合の影響
      - アドレスブロックの不正利用（利用妨害、なりすまし）
        e.g. 追跡不可能なDoSやスパム
      - BOGONアドレスの検知妨害
    - アドレス利用状況の把握に対する影響
      - アドレス資源の利用率への影響
        例：割り当て報告の削除
    - インシデント／問題対応のためのコンタクトへの影響
      - 問題対応時のなりすまし／情報収集
      - コンタクトの遅延を利用したハイジャック

事例：

- IP address hijacking
- whois hijacking

従来のレジストリシステムの保護機能

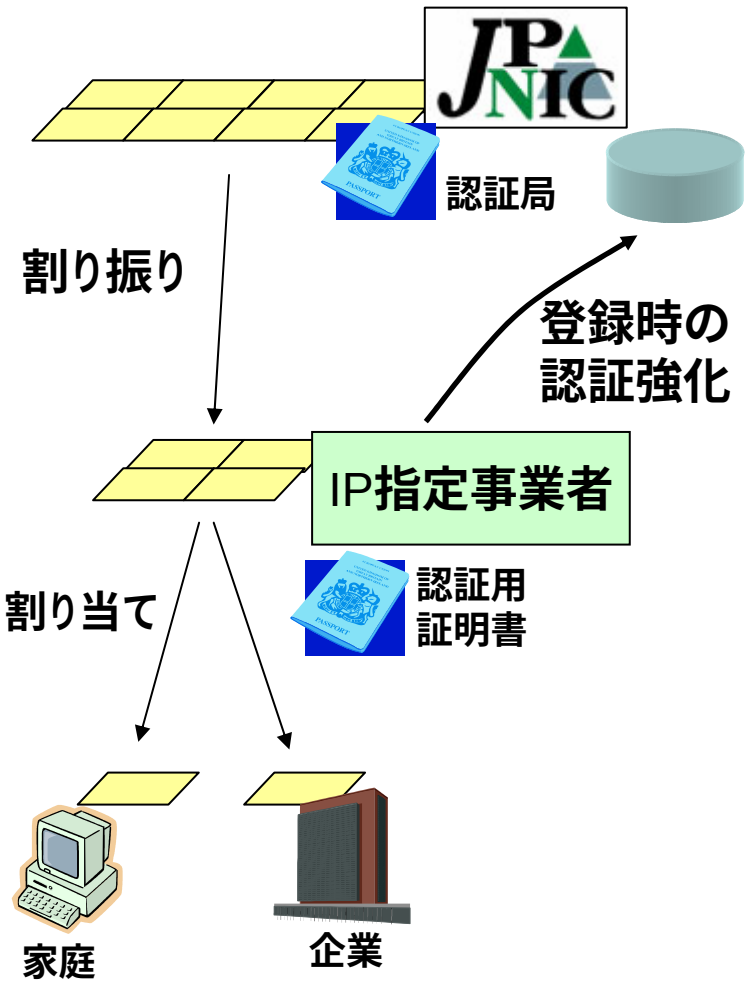
- JPNIC
  - mail-from, ID/**パスワード**
  - **通知アドレス**
- APNIC
  - mail-from, crypto-pw, pgp-key
  - notify
- RIPE NCC
  - mail-from, RegID/**パスワード**, crypto-pw, pgp-key, md5
  - notify

より強い認証が必要とされている。

APNIC、RIPE NCC、ARINの取り組み

- APNIC
  - APNIC CA
    - MyAPNICのクライアント認証に使用される証明書を発行。役割ごとのアクセスコントロール。
  - MyAPNIC： メンバ向け資源管理Webインターフェース
    - サーバ証明書を使ったサーバ認証
- RIPE NCC
  - RIPE NCC CA
    - LIRの登録時に与えられる登録ID (Regid) とパスワードを使った電子証明書発行。S/MIME (電子メール) でも利用。
  - LIRPortal： メンバ向け資源管理Webインターフェース
    - サーバ証明書を使ったサーバ認証
- ARIN
  - ARIN CA
    - POC(point of contact)向けの個人証明書を発行。
  - S/MIMEで利用。

JPNIC の取り組み



- JPNIC認証局の検討
  - IP指定事業者の申請者／業務担当者にクライアント証明書(X.509)を発行。(2005年4月に実験的に導入予定)
  - 既存のユーザ管理方法と同様のシステムに。
- IPレジストリシステム
  - IP指定事業者向け資源管理Webインターフェース
  - サーバ認証／クライアント認証

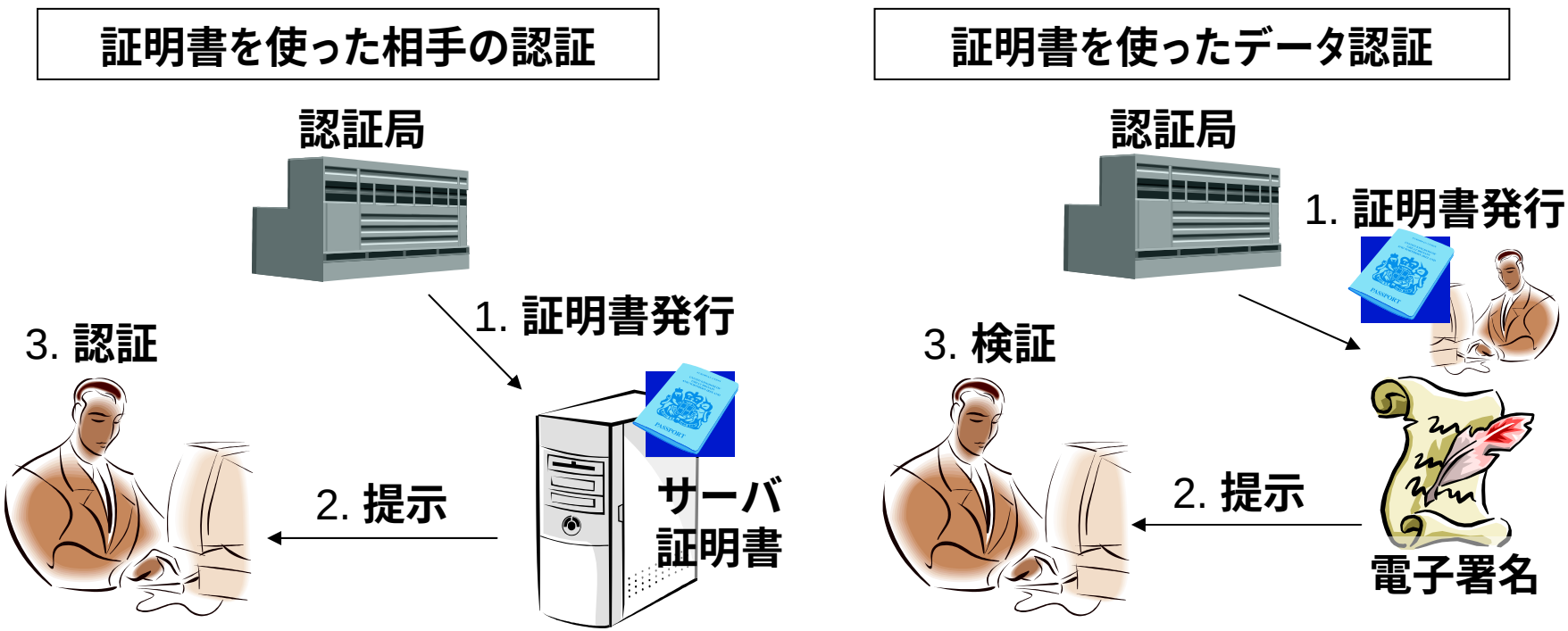
⇒ 登録時／変更時の改ざんを検出したり未然に防止したりすることが可能

認証の考え方と保護機能 (1)

- PKI - Public Key Infrastructure を導入
  - JPNIC認証局を構築し、認証の基盤とする
- JPNICでは、レジストリデータの安全性についてのセキュリティモデルを検討
  - 脅威の起こる場面
    - データの登録／保持 ⇒ 登録／更新時の認証強化
    - データの提供
  - セキュリティモデル
    - トランスポートモデル (SSL/TLS)
    - オブジェクトモデル (電子署名／電子証明書)
  - 認証に使われるアカウントの保護
    - アカウントの個別管理
    - 公開鍵証明書の利用

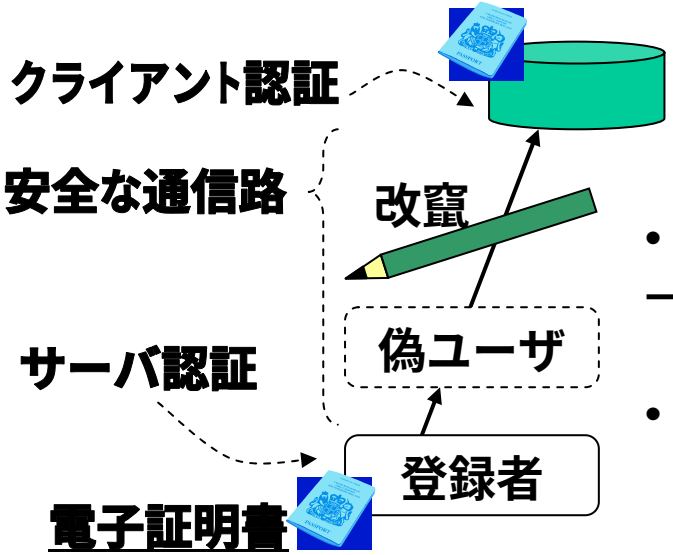
PKI － Public Key Infrastructure

- 公開鍵暗号を利用した認証基盤（認証の仕組み）
  - 認証局に発行された電子証明書を利用
  - 通信相手の認証や、データの正しさの検証が可能



認証の考え方と保護機能 (2)

モデル：トランスポートセキュリティ



- SSL/TLSの利用
→導入は比較的容易

- データ自体の安全性は確認不可能
例：なりすまし攻撃

認証に使われるアカウントの保護

- **アカウントの個別管理**
メンバ変更を伴って共通パスワードを変更するなどが不要に。
- **公開鍵証明書の利用**
クラッキング対策を強化。
  - オンライン推測攻撃対策

はじめに、トランスポートセキュリティ (SSL/TLS) を適用し、登録／変更時のセキュリティに取り組む。

今後、オブジェクトセキュリティ (電子署名) のモデルを検討、ミラー／提供時のセキュリティにも取り組む。

2.アドレスブロックの認証基盤

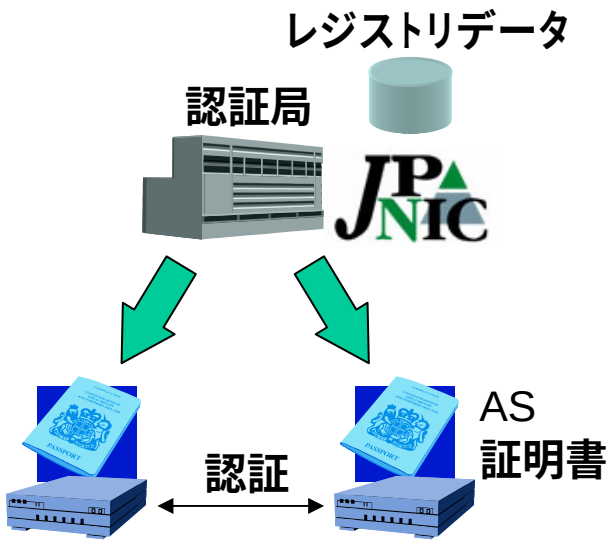
- JPNIC認証局における取り組み
- レジストリデータを使った認証基盤

JPNIC認証局における取り組み

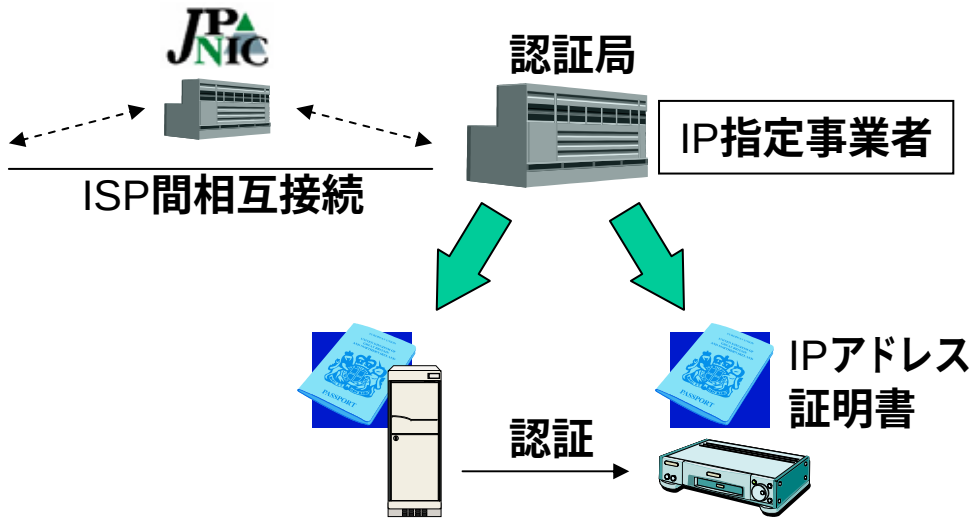
- JPNIC認証局における取り組み
  1. **認証強化の為の認証局構築**
     - JPNICにおけるクライアント認証の導入検討
       ⇒ "JPNICにおける認証強化"が目標
  2. **レジストリデータと電子証明書の利用検討**
     - **認証基盤の調査研究**（ASP/ISPによる事業化を含めて）
       ⇒ "IPの通信ノードにおける認証の導入"が目標

レジストリデータを使った認証基盤

- **認証基盤のアイディア**



AS情報の証明書
- origin の認証



IPアドレス証明書によるノード認証
- 通信時のISPの特定 (P2P, CDN)
- 付帯情報 (地理、運用レベル)

関連プロトコル
- RFC3779
- S-BGP / soBGP
- IPsec

- 新たなアドレスポリシーは必要か。
- 家電、地域的な機器の連携などが可能に？

ご意見を頂きたい点

1. JPNIC認証局のアイディアは妥当か
   - 登録／変更時の認証強化（PKI）
   - IPレジストリシステムのWebインターフェースで利用

2. IPアドレスとAS番号の認証基盤はありうるか
   - アドレスブロックの属性（運用レベル、情報等）の情報付加による応用方法として何がありうるか。
   - ネットワーク・セキュリティが要求される、家電や緊急ネットワークへのアプローチは可能か。
   - JPNIC認証局はどこまで役割を担うべきか。

リンク集

- 「IPアドレス認証局のあり方に関する調査報告書」
  http://www.nic.ad.jp/ja/research/200303-CA/
- 「IPアドレス認証局のマネジメントに関する調査報告書」
  http://www.nic.ad.jp/ja/research/200404-CA/

- APNIC CA
  https://www.apnic.net/ca/
- MyAPNICの説明
  http://www.apnic.net/services/myapnic/

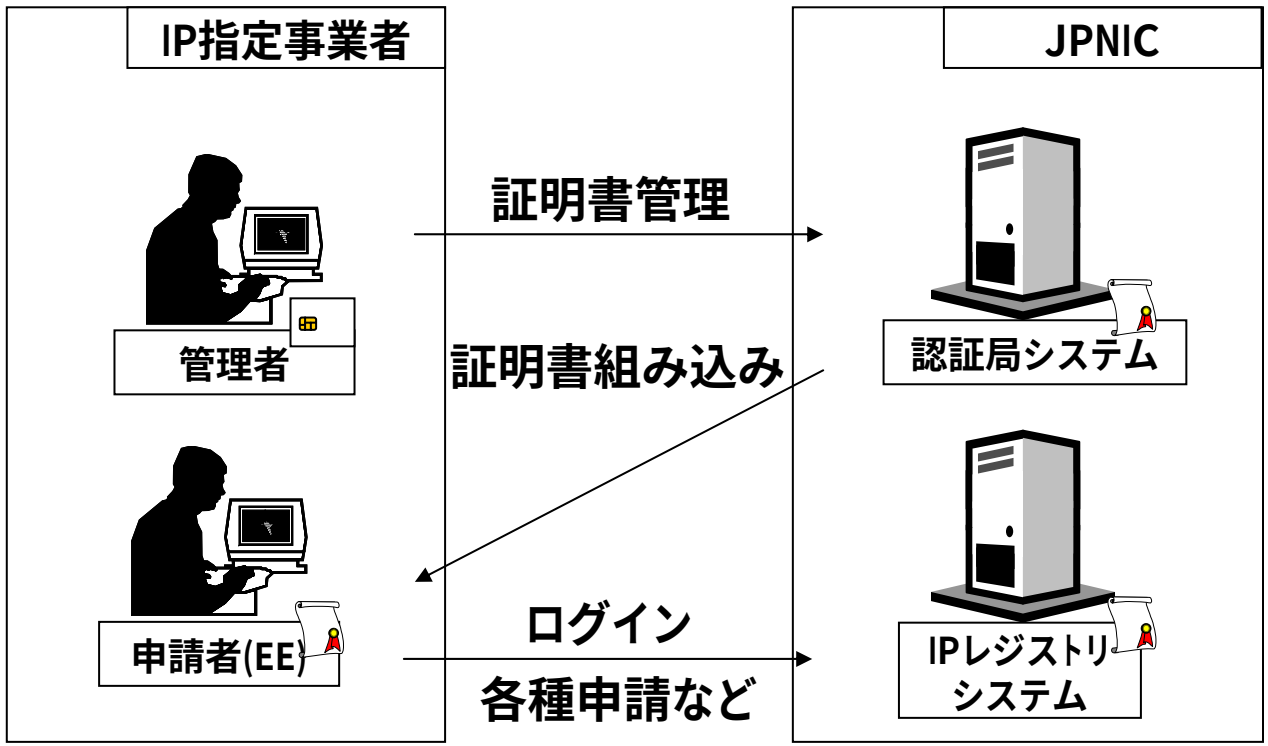
- LIRPortal (RIPE NCC)
  http://lirportal.ripe.net/

- Certificate Cryptographic Authentication at ARIN
  http://www.arin.net/CA/

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：認証強化について



詳細は指定事業者連絡会でご説明致します。

資料：認証の考え方と安全モデル

- 脅威の起こる場面：安全モデル
  - データの登録／保持
    - なりすまされた登録／更新／削除
    - 登録途中の書き換え
  - データの提供
    - 提供途中の書き換え
    - なりすまされた情報提供
    - 提供不能行為