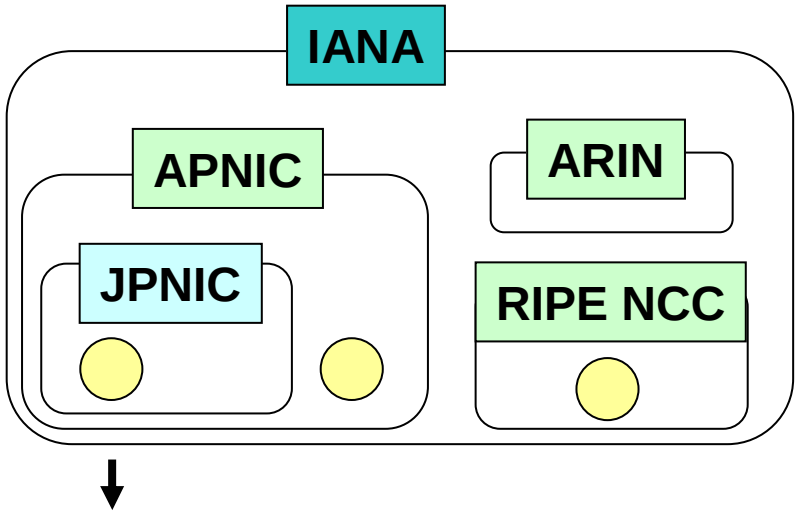
インターネットレジストリにおける レジストリデータの保護と応用

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）
木村 泰司

インターネットレジストリ

- アドレス資源の管理／運用
  - ネットワーク資源の割り振り
    - IPアドレス等をプロバイダへ
  - 登録情報の提供
    - 運用責任者、技術連絡担当者
    - ホスト情報
- 日本のNIR

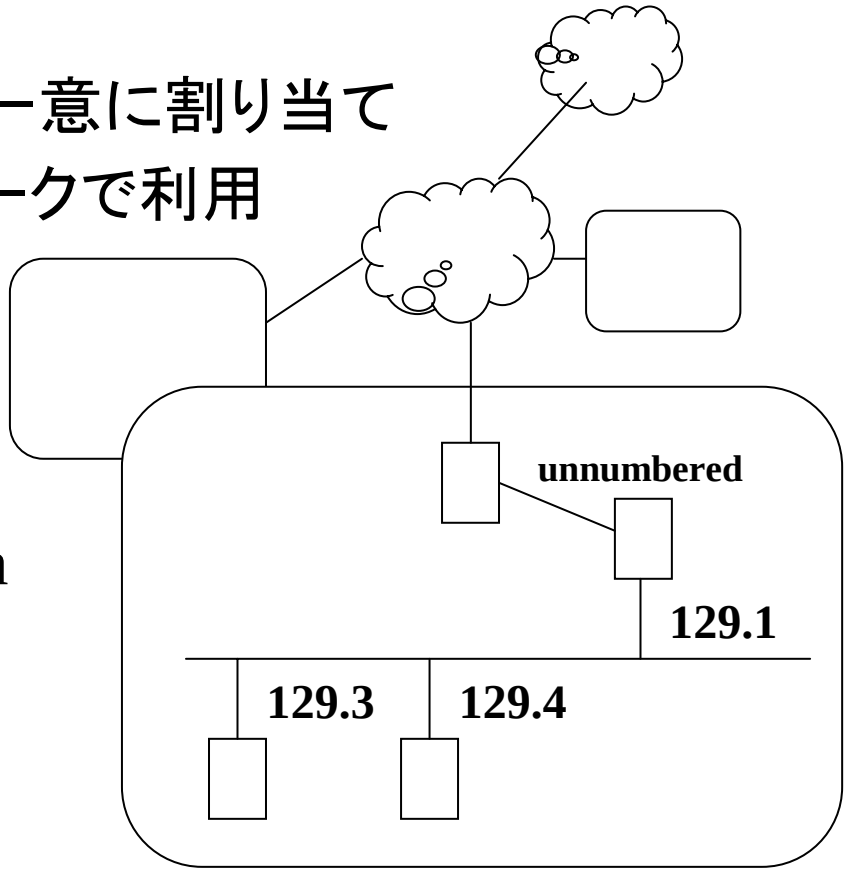
  - National Internet Registry
  - JPNICによるIPアドレスの割り振り
  - （株）日本レジストリサービス（JPRS）によるドメイン名の割り当て業務
  - JPNIC, JPRS共通の情報提供機構 whois



日本に実在する組織が割り当てられるアドレスの範囲

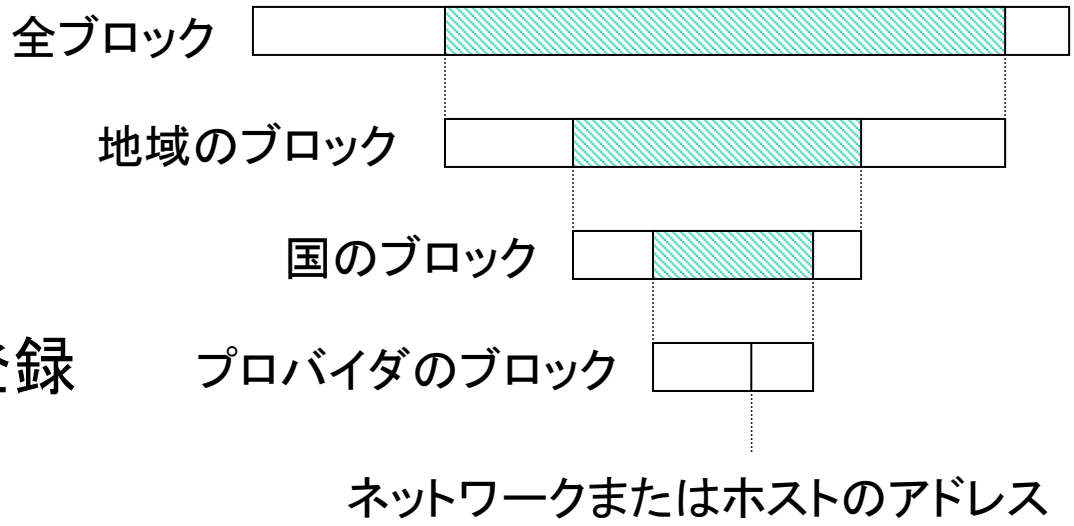
アドレス資源

- IPアドレス（グローバルIPアドレス）
  - IPを利用するネットワークインターフェースにふられるアドレス
  - 各ネットワーク利用組織に一意に割り当て
  - グローバルなIPのネットワークで利用
- AS番号
  - 経路情報の交換に使われる識別番号
  - 各AS - Autonomous System に割り当て
  - 経路交換プロトコルBGPで利用



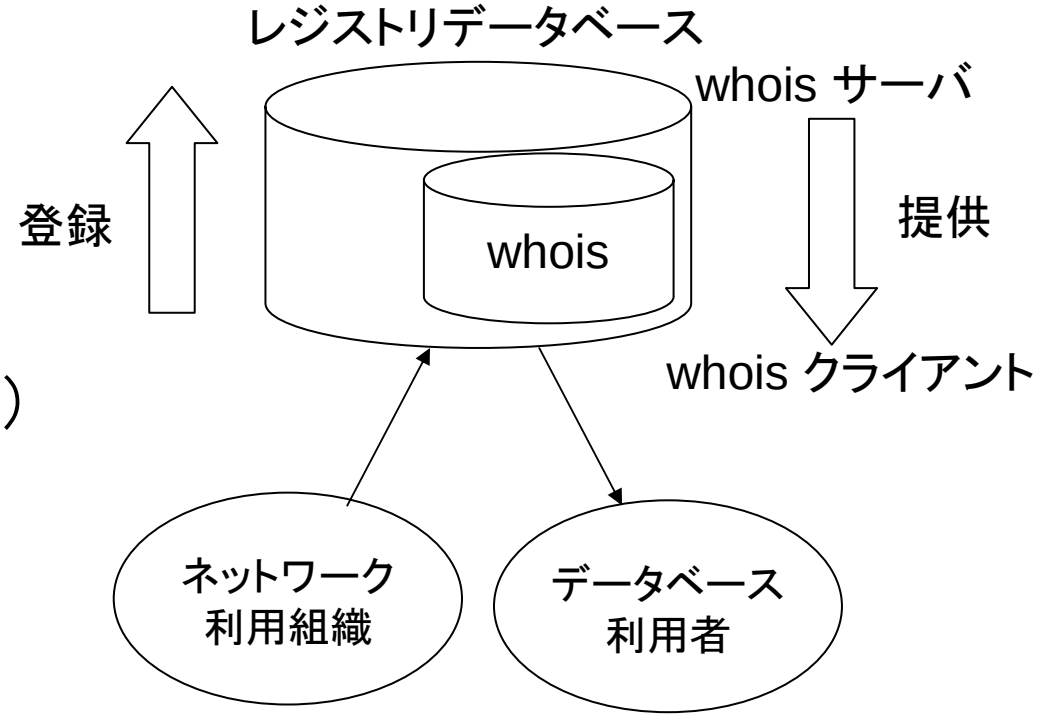
アドレス資源の運用要件

- 一意な割り当て
  - 分割したブロックの割り振り
- 集約可能な経路情報
  - 地域的な割り振りの階層構造
- 自律分散的な運用
  - 利用組織の情報登録と情報公開



アドレス資源とレジストリデータ

- アドレスの割り振り／割り当て情報
  - LIR - Local Internet Registry の情報
  - ネットワーク利用組織の情報
- Whois
  - ネットワーク情報
  - AS番号の情報
  - 担当者に関する情報
  - ドメイン情報（JPRS社）
  - ホスト情報
    - ネームサーバの情報



インシデント対応と登録情報

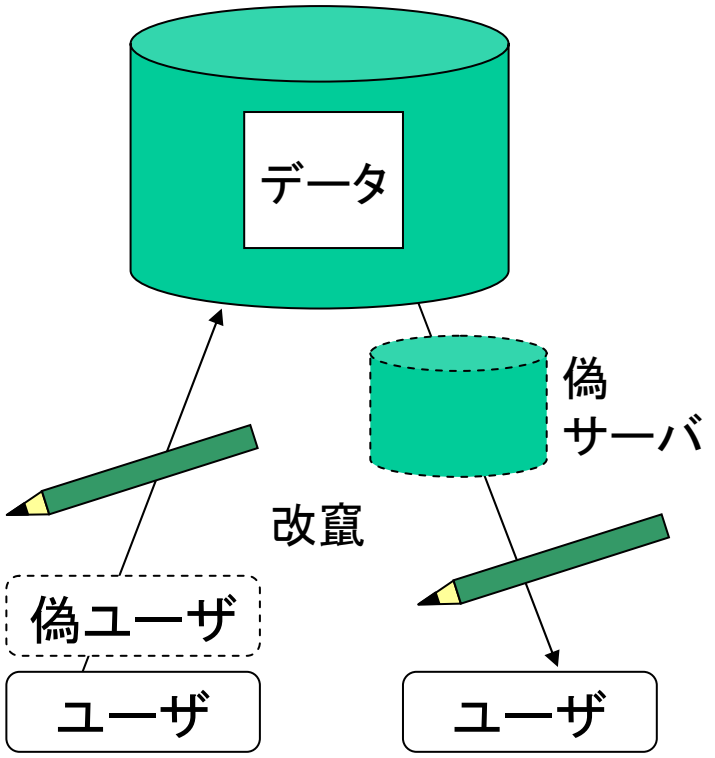
- Whoisの利用例
  - 未確認のパケット発見…
  - どの組織が使っているか…
  - その連絡先は…
  - 逆引きネームサーバは…
  - アドレスブロックを管理しているLIRは…

```
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
```

レジストリデータの安全性

レジストリデータに関わる攻撃

- データの保持
  - 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



レジストリシステムの保護機能

- JPNIC（日本のNIR）
  - mail-from
  - 通知アドレス
  - ホストマスターによる個別連絡
- APNIC（アジア太平洋地域のRIR）
  - mail-from, crypto-pw, pgp-key
  - notify
- RIPE NCC（ヨーロッパ地域のRIR）
  - mail-from, crypto-pw, pgp-key, md5
  - notify

より強い認証とデータ保護機能が求められている

RIRの認証機能に関する活動（1）

- APNIC
  - MyAPNIC
    - クライアント証明書（個人認証）を利用したユーザ認証とアクセスコントロール
    - LIRのコンタクト情報等の編集
    - 将来的にネットワーク情報も編集可能になる予定
  - Database SIG
    - 認証機能 none のデータエントリの削除の提案に合意
- ARIN（アメリカ地域のRIR）
  - "none"にあたる認証の行なわれない登録はない
  - Database WGにおける議論
    - X.509形式の証明書を利用したレジストリデータの管理

RIRの認証機能に関する活動（2）

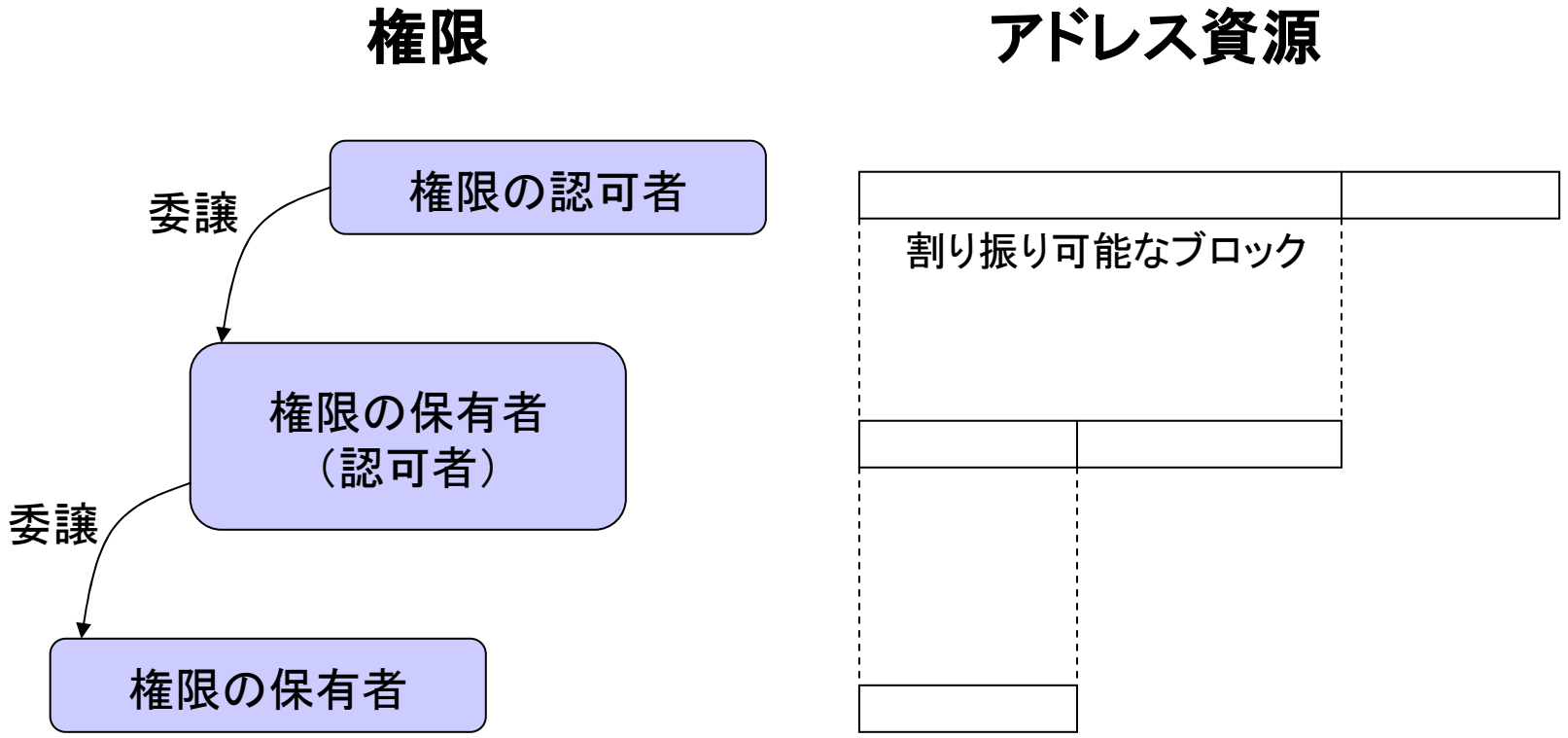
- RIPE NCC
  - LIRPortal
    - クライアント証明書（ユーザID確認と自動発行）を利用したユーザ認証とアクセスコントロール
    - LIRのコンタクト情報等の編集
  - Database WG
    - ネットワーク情報とクライアント証明書の情報の関連付けに関する提案
      - ネットワーク情報の編集実現に近づく
    - 依然、認証機能がnone, mail-fromに設定されたデータがあり、議論が続いている。

インターネットレジストリにおける認証局

認証局を利用したインターネットレジストリ間の
連携のアイディア

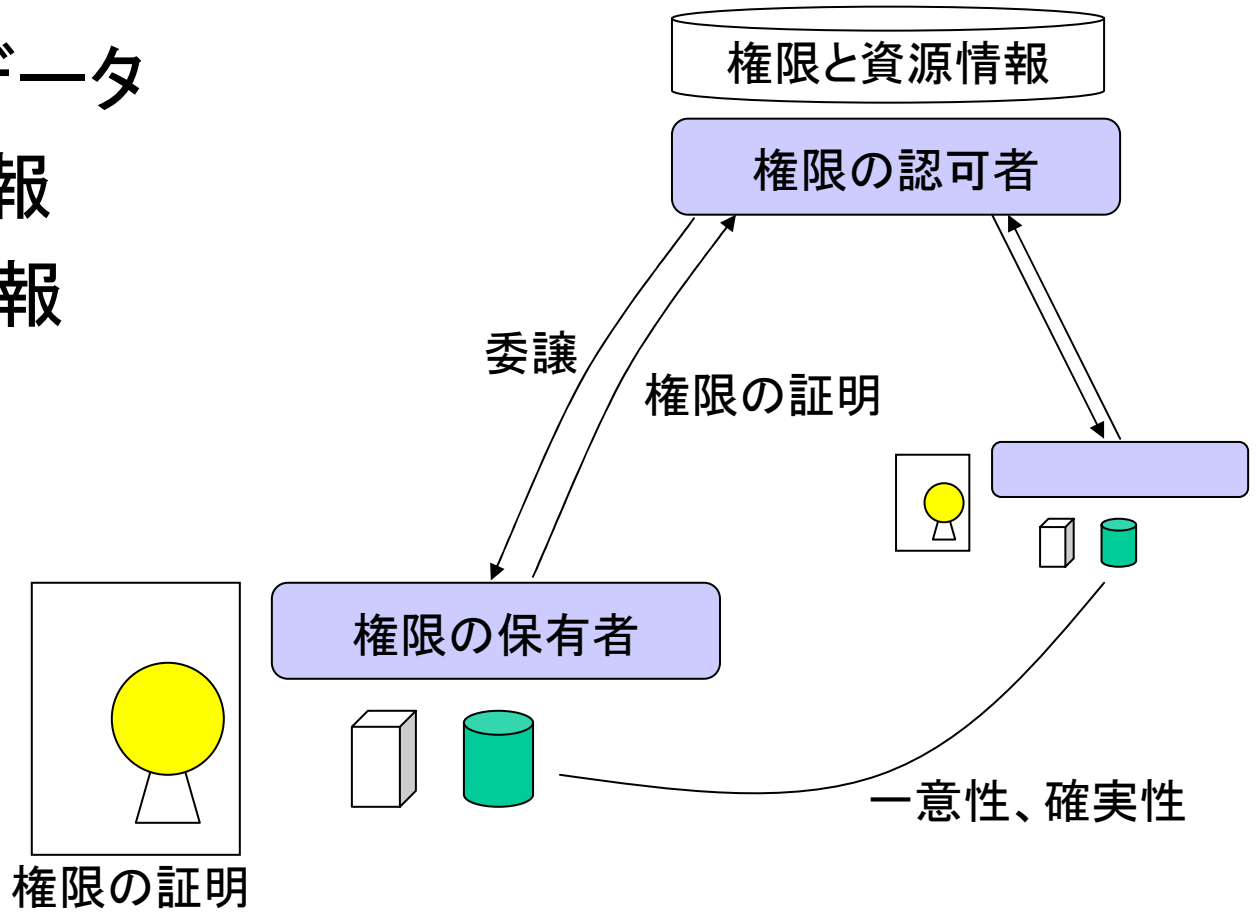
アドレス資源と認可

- アドレス管理権限の認可の構造



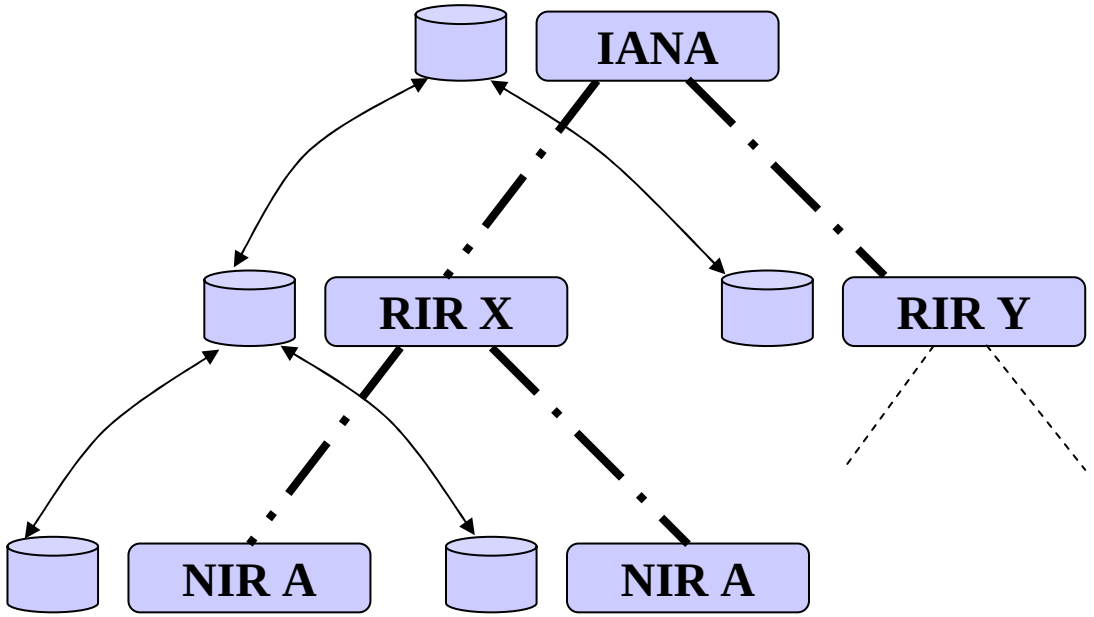
レジストリが発行する証明書の意味

- 登録とLIRの認証
- レジストリデータ
- 割り振り情報
- 割り当て情報
- ホスト情報



レジストリデータの電子署名（1）

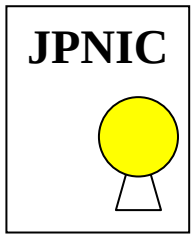
- Whoisとレジストリデータの同期
  - レジストリデータの同期によって他のレジストリのデータを包括的に検索しやすくなる。
    - データ表示形式
    - カバー範囲



※RIRの同期だけで全地域のアドレス資源をカバーできる

レジストリデータの電子署名（2）

- IPアドレスとレジストリの特定
  - origin:（出所）の値によって、LIRを含め、どのインターネットレジストリによって登録されたかがわかる。
- 登録情報の検証
  - 署名の検証による出所情報の検証
  - 出所の登録の確かさの特定
    - 登録ポリシーの参照などによる



レジストリ証明書

アドレス：202.12.30.0
利用組織：JPNIC
管理組織：JPNIC
出所：JPNIC
電子署名：<signature>

whois 検索結果の例

ここまでのまとめ

- レジストリデータの安全性
  - 登録者の認証とレジストリデータの正当性
- 管理権限の認可と証明書
  - アドレス資源の管理権限の委譲
  - 管理権限を示す証明書
  - 割り当てを示す証明書
- 電子署名を使ったレジストリデータの交換
  - レジストリ間のデータ同期
  - whoisを使った包括的な検索機能の実現
    - データ表現形式
    - 資源のカバー範囲

レジストリシステムの安全性に
関わる動向

プロトコルの策定

- CRISP – Cross Registry Information Service Protocol
  - IETF CRISP WGにおける議論
    - FIRS（LDAP）
      - LDAPはPKIX WGなどX.509のコミュニティでは一般的
      - 実装が多い（OpenLDAP、ActiveDirectory等）
      - 運用知識が豊富
    - IRIS（XML）
      - WGとして出した要求事項を満たす。柔軟な表現が可能。
      - 実装が少ない（VeriSign社）
      - 運用知識が少ない

    IRISが優勢。次回（第58回IETFには方向性が決まっていると予想される）
- PKIX WGにおけるInternet-Draft
  - draft-ietf-pkix-x509-ipaddr-as-extn-02.txt
    X.509v3拡張フィールドにアドレスブロックやAS番号の値を格納
- RPSLng
  - IETFセキュリティエリアとRIPE NCC Databaseスタッフによる提案

RIRにおける活動（1）- APNIC

- APNIC CA
  - NICハンドルを持ち、アドレス資源の管理ができるユーザに証明書を発行
  - ホストマスターとの暗号メールやMyAPNICのクライアント認証に使用される証明書を発行
  - MyAPNICのサーバ証明書を発行
  - パスポート等写真付き身分証明書を使った個人認証
- MyAPNIC – LIR向けのアドレス資源情報のWebインターフェース
  - https
    - クライアント認証を行なうTLSを使用
  - 証明書ごとに役割りを定義（フィールドに情報は含めない）
    - Corporate、Hostmaster、Admin、Technical、Training
  - 役割りごとのアクセスコントロール規則
    - 組織情報の編集
    - アドレス資源情報の閲覧（編集機能は今後実装の予定）
- アイディア
  - NIR、LIRとの認証システムの連携（電子署名を利用）

RIRにおける活動（2）- RIPE NCC

- RIPE NCC Root CA
  - LIRのアカウントがあるユーザに証明書を発行
  - LIRPortalのクライアント認証に使われる証明書を発行
  - LIRの登録時に与えられる登録ID（Regid）とパスワードを入力するとオンラインで証明書が発行される
- LIRPortal - LIR向けのアドレス資源情報のWebインターフェース
  - https
    - クライアント認証を行なうTLSを使用
    - パスワード（CGIプログラム）も使用可能
  - ユーザのできること
    - 組織情報の編集
    - アドレス資源情報の閲覧（編集機能は今後実装の予定）
- Database WGにおける提案
  - 既存の認証方式とX.509形式の証明書を使った認証の連携

RIRにおける活動（3）- ARIN

- Database WGにおける議論
  - X.509形式証明書を使ったクライアント認証
    - ただしRIPE NCCやAPNICとはデータベースの表現形式が異なっているため、認証システムの構造は異なると考えられる。
- 現状
  - mail-fromなど認証を行なわない方法でリクエストを受け付けていない。

JPNICにおける活動

- 認証局構築のための調査
  - IPアドレス認証局のあり方に関する調査
    - NIRにおける認証局のあり方
    - APNIC、RIPE NCCの現状
    - 運用要件の比較：認証局監査の基準の比較
    - 証明書利用のモデル
  - CP/CPS策定の為の調査
    - APNIC、RIPE NCCの証明書のアプリケーション
    - 認証システムと証明書の用途
- レジストリシステムにおける認証システムの検討
  - X.509形式の証明書を使ったクライアント認証

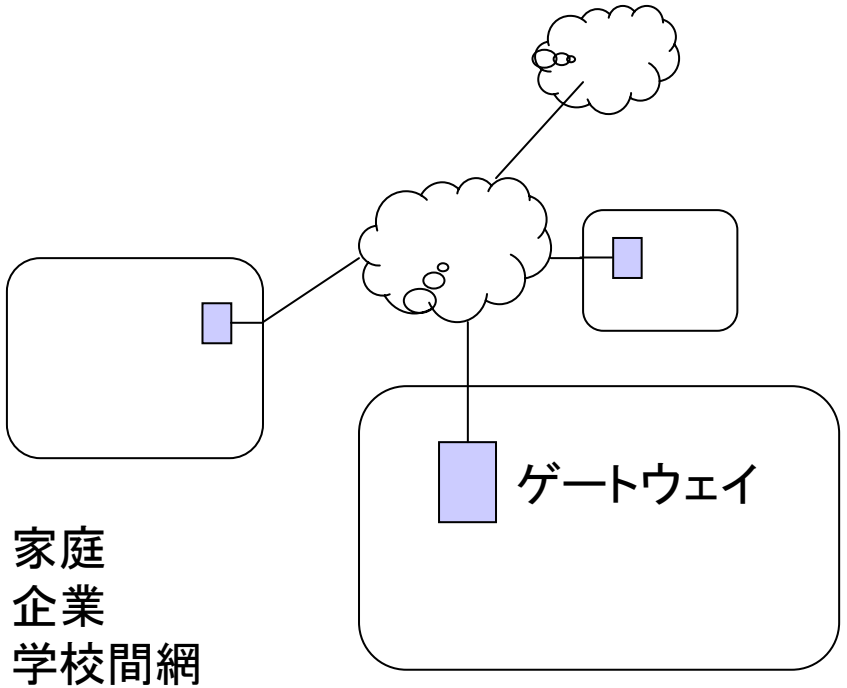
インターネットレジストリにおける認証局と証明書の応用

レジストリデータの意味と証明書

- ネットワーク情報
  - アドレスブロックと管理組織
    - 特定のアドレスブロックを割り振られている、または割り当てられている組織の名称
  - ネームサーバ
    - 特定のアドレスブロックを担当するサーバのホスト名
- ホスト情報
  - ホストとIPアドレス
    - あるホストのIPアドレス
- LIR情報
  - アドレスブロックを割り振られたISPの情報

レジストリデータ証明書の応用例

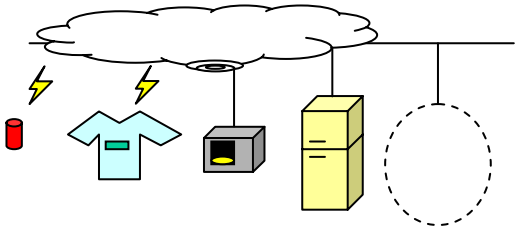
- アドレスブロック
  - 経路情報の証明
- ホスト
  - ネームサーバ
    - DNSSECの設計との違い
  - ゲートウェイ
    - VPNゲートウェイ
    - IP電話ゲートウェイ
    - ホームゲートウェイ
- キーサーバ
  - PGPキーサーバ



- 家庭
- 企業
- 学校間網
- 移動体通信網
- 流通網
- など

IPv6とアドレス管理の今後

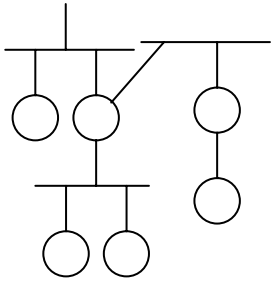
- IPv6とネットワーク境界
  - ノードの増加
    - IPv6の潜在的普及
    - 制御用タグとしての意味
  - ネットワークセグメントの増加
    - 一つのセグメントに収容できるホスト数は限られている（データリンクの性質による）
    - 局所のルーティング
  - アドレス管理の重要性
    - 多数のネットワークを収容／管理できる体制が必要になる
    - 属性情報を付加したアドレスブロックの管理
    - 経路情報の効率的な管理



データリンクの
実装技術の発展

IPv6アドレッシング

接続網にルータと
多数のネットワーク
が発生



JPNIC セキュリティ事業では

- ネットワーク利用を考えていらっしゃる業界の方にヒアリングを実施しています。
  - IPv6のアドレスの割り当てと応用
  - 証明書のゲートウェイ等応用

- アイディアなどお寄せ下されば幸いです。

まとめ

- インターネットレジストリとアドレス資源の管理
- レジストリデータとwhois
- 自律的な管理とインシデント対応
- レジストリシステムの認証システム
- アドレス資源の委譲構造とPKIの認可モデル
- レジストリデータと電子署名
- RIRの動向
- プロトコル策定の動向
- インターネットレジストリが発行する証明書の応用

リンク集

- JPNIC
  - トップページ
    http://www.nic.ad.jp
  - セキュリティ事業の2002年度の活動
    「IPアドレス認証局のあり方に関する調査報告
    http://www.nic.ad.jp/ja/research/200303-CA/index.html
- APNIC
  - トップページ
    http://www.apnic.net/
  - APNIC CA
    https://www.apnic.net/ca/
  - MyAPNICの説明
    http://www.apnic.net/services/myapnic/
- RIPE NCC
  - トップページ
    http://www.ripe.net/
  - LIRPortal
    http://lirportal.ripe.net/

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