IRR Security

JPNIC **セキュリティ事業担当**
木村泰司

概要

- Route Hijacking
- IRRを利用した防御策
- JPIRRのセキュリティ機能
  - メカニズムの説明
- 視点･論点

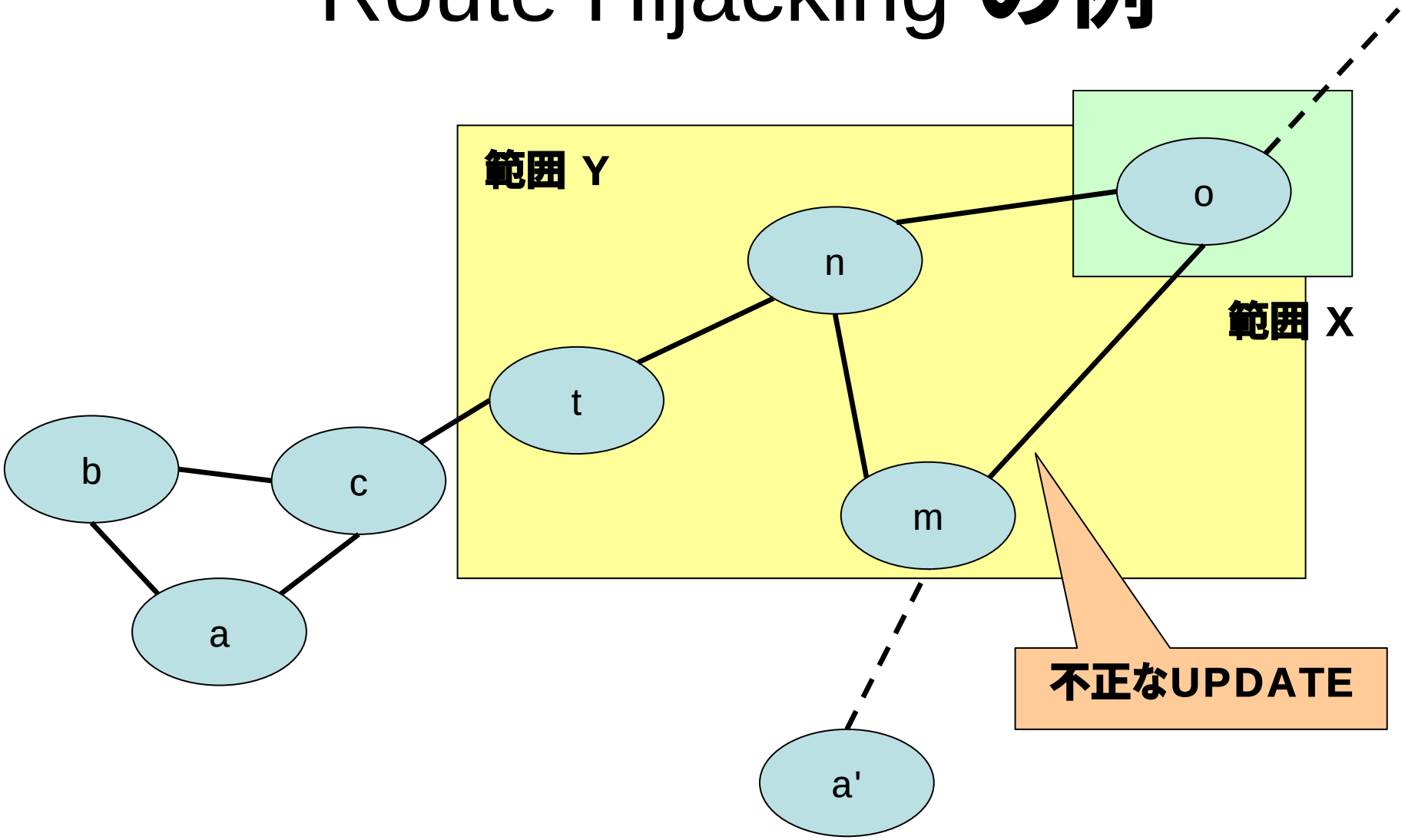
Route Hijacking

- **聞いた話によりますと**
  - Route Hijacking **が年間数件程度観測されている**
    - **設定ミスらしき現象と共に故意とも取れる現象がある**
  - **その手法から想定される**Hijack**の種類**
    - prefix**違い**
    - AS**番号違い**
    - **ほか色々と考えられる**

Route Hijacking の例

- **想定**
  - Inter-AS
  - 3 AS **以上遠方**
  - origin AS, MED**値などを好きな値に書き換えられるプログラムの噂あり**

Route Hijacking の例



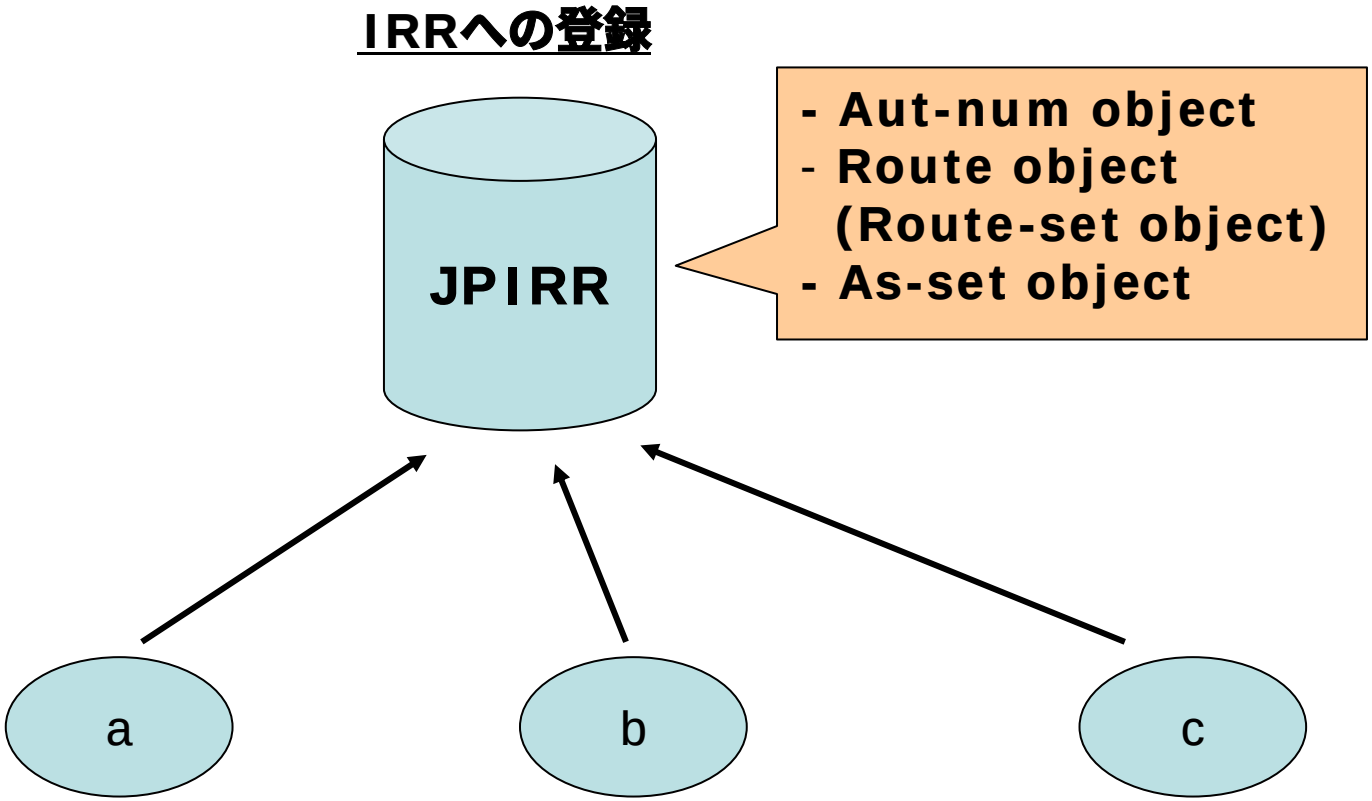
Route Hijacking の影響範囲

- **影響範囲**
  - /16で約70%の利用率 ⇒ 45,873ノード
- **損害額の試算**
  - **一秒間不到達の場合の損害額の範囲**
    (エンドユーザのプロバイダ加入料¥3,000/月とする)
    - **最大**:/8 ⇒ ¥7,046,430,720
    - **最小**:/24 ⇒ ¥107,520
  - 2005年12月1日現在のフルルート@JPNIC
    - /24〜/8 **の経路エントリ総数**:175,513
    - **総**IP**アドレス数**:33,554,176
    - 0.5%**が不正な経路の広告によって不到達になっていた場合**
      - **一秒当たりの平均損害額**:¥70,463,770

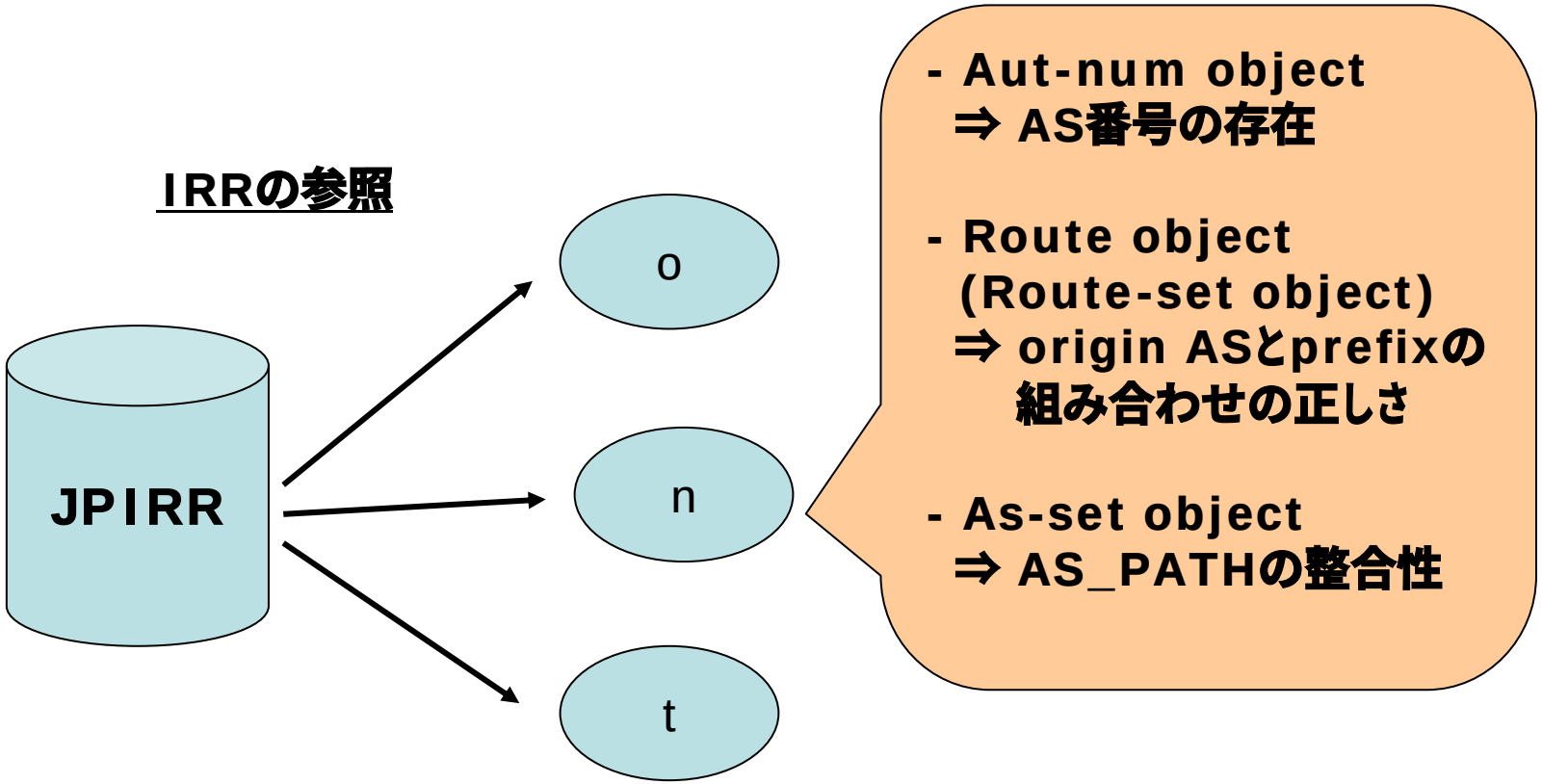
なぜHijackingが起こるのか

- prefix違い
  - origin ASとprefixの組み合わせが、正しいのかどうかがわからない。従ってルーターでその経路情報を無視すべきかどうかわからず、伝播していってしまう。
- AS番号違い
  - ある経路情報のorigin ASが本当にそのAS番号を使ってよいASなのかどうかがわからない。(同上)
- AS_PATH違い
  - ある経路情報のAS_PATHがオペレーターが正しいと思っているトポロジーと一致しているのかどうかわからない。(一部の方にはよくみるとわかるようですが)

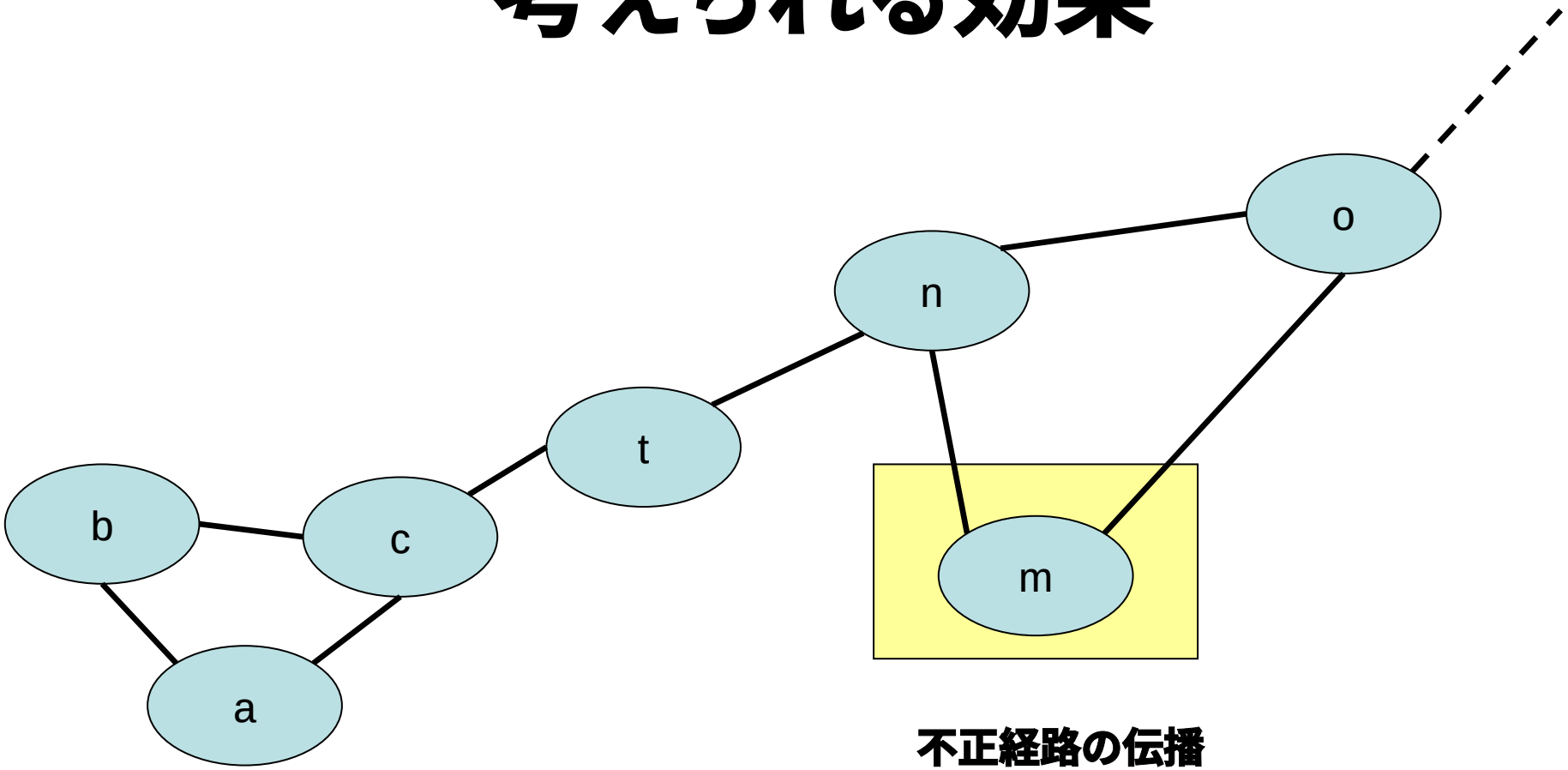
IRRを利用した防御策



IRRを利用した防御策



考えられる効果



不正経路の伝播範囲の極小化

課題のポイント

登録側

- Aut-num object
  (AS番号の存在)
  ⇒ AS登録者の本人性
- Route object
  (ASとprefixの組み合わせ)
  ⇒ レジストリデータとの整合性
  運用方針との整合性
- As-set object
  AS_PATHの整合性
  ⇒ 登録内容の正当性

参照側

- どのIRRを見るか
  ミラーリングの範囲と遅延
- 検証のオーバーヘッド
  - prefix、AS_PATHの比較
  - 各種delay
- 不整合への対応方針
  登録情報と流れている経路情報との不整合にどう対応するか
  - ルール、タイミング

JPIRRのSecurity機能

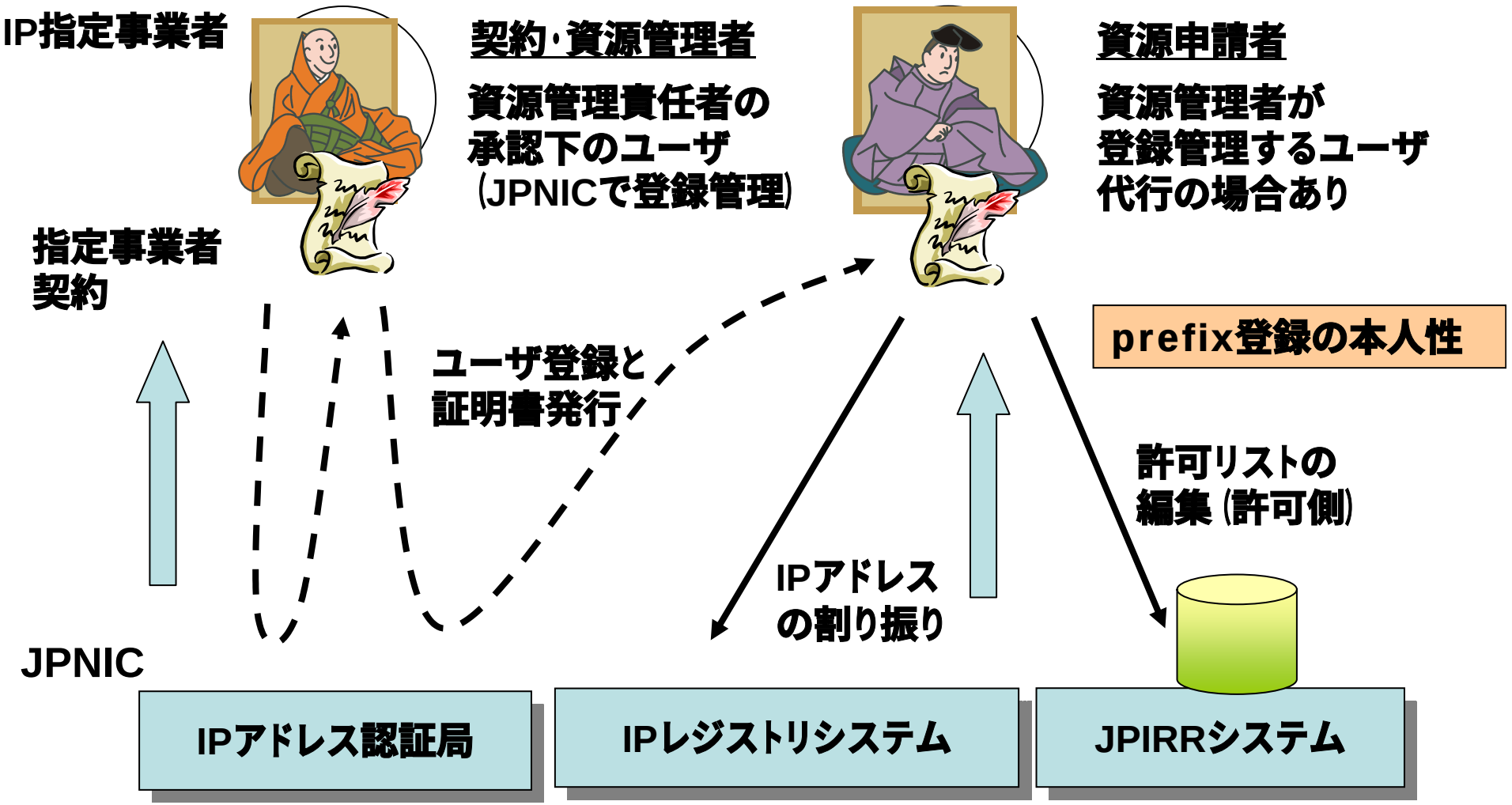
JPIRRのSecurity機能

- 目的
  - 防衛範囲の登録情報の正当性確保
  - 範囲の拡大 ⇒ Mirroring, CRISP
- 手法
  - IPレジストリの情報を利用した認可機構
- 対象
  - JPIRRを利用するASの運用者
    - ただしJPNICからIPアドレスやAS番号の割り振りを受けた運用者に限定しない

仕組み

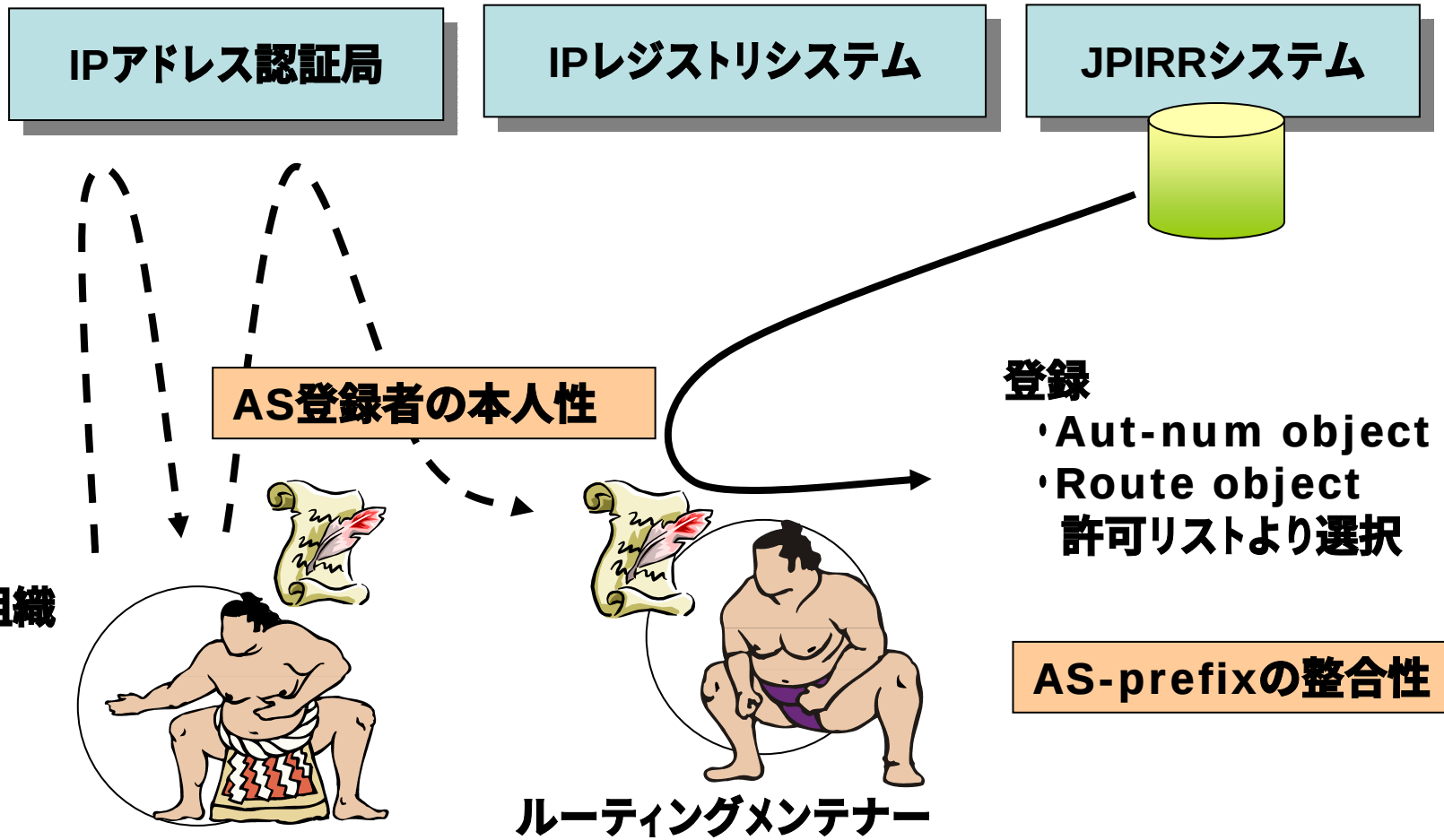
1. AS登録者の本人性
   - JPNICの"AS情報"登録者に"AS管理証明書"を発行
   - JPIRR WebシステムはAS管理証明書でユーザ認証、As-num objectの登録を許可
2. レジストリデータ、運用方針との整合性
   - "許可リスト"
     - IP指定事業者が指定したASのmntnerにprefix利用を"許可"
     - AS管理証明書を使ってRoute objectを登録
     - JPNICに登録されていないAS番号、IPアドレスについては任意登録。ただしその意味のフラグが立つ。
3. 登録内容の正当性
   - ガーベージコレクター
   - フルルートとの比較：整合性確認

認証連携と許可リスト(ISP側)



認証連携と許可リスト(AS側)

JPNIC



許可リスト

許可リスト

mntner	prefix	許可／禁止	Origin AS
mnt1	1.1.0.0/16	allow	12345
mnt3	1.1.0.0/17	allow	(optional)

論点･視点

論点A：普及と効果

- 特定のグループ全員が使って初めて効果
- ある程度の普及を図る必要
  - IP指定事業者全員が必要とは限らないが
  - 守りたい範囲のASの全てが協力して初めて効果

  - 実現可能性は？
  - 別途MLなどで調整が必要？
  - アラートの仕組み(Option Service)
    - 自己矛盾、古いデータ
    - 割り振り情報
    - 流れてきた経路情報

論点B：登録情報の正当性

- 不整合の扱い方
  - 自己矛盾
  - ガーベージオブジェクト
  - ミラーによる流入
  - インターネットに流れている経路情報
    - 運用上の理由と不正な理由の違いの見つけ方は？
- 許可リストで運用状態を適切に表現できるか

論点C：認証強化のfeasibility

- 電子証明書を使ったクライアント認証
  - 使えるかどうか
- 個別のオペレーターの登録者管理
  - 管理し切れるのか
  - 電子証明書利用者は？
  - person or roleの把握は？

論点D：IPレジストリの関与

- グループによっては
  - JPIRRへの登録＝接続性の維持
  - 割り振りとの整合性　⇒　前提とするグループが出現？
- 現状
  - 登録は任意（義務ではない）
  - 正常利用も任意（〃）
  - 不正利用も任意（〃）
- この機構はIPレジストリのルーティングへの関与？
  - 登録は任意（義務ではない）
  - 登録するとその内容に則った運用開始
  - 登録内容は任意（ガーベージは削除？）

視点

- **論点**A：**普及と効果**
  - JPIRR**の範囲でならば可能ではないか**
  - **ルーターの運用シナリオは必要**
- **論点**B：**登録情報の正当性**
  - **ガーベージコレクター**
  - **ミラーされた情報と、流れている経路情報との矛盾については課題**
- **論点**C：**認証強化の**feasibility
  - PGP**ユーザがいるので、マニュアルを用意すれば可能ではないか。**IP**指定事業者の利用実験ではまだ大きな問題は起きていない。**
- **論点**D: IP**レジストリの関与**
  - AS**同士の判断による為、関与ではないのではないか**

スケジュールと判断ポイント

- 2005**年度**
  - **要求仕様の作成**
    - **経済産業省からの受託事業**
      「IPアドレス認証局の応用」の一環として

    [判断ポイント1]
- 2006**年度**
  - **[判断ポイント2] 基本仕様の設計**
  - **可能であれば詳細設計と共に開発**

    [判断ポイント3] JPOPMなど
- 2007**年度**
  - **実験運用**

その他の話題

- **リソース証明書**
  - RFC3779
- soBGP, s-BGP
  - APNIC20
  - IETF-64 SIDR BoF
  - RIPE NCC's action plan 2006

まとめ

- Route Hijacking
  - 観測されている
  - 地域性がある
- IRRを利用した防御策
  - 登録者の本人性、ASとprefixの整合性、データ正当性
- JPIRRのセキュリティ機能
  - 許可リスト
- 視点・論点
  - いかがでしょうか。

おわり

JPNIC セキュリティ事業担当
木村泰司

情報：認証強化実験について

- **情報源**
  - JPNIC CAのWebページ
    - http://jpnic-ca.nic.ad.jp/
- **実験参加方法**
  1. ca-query@nic.ad.jpに
     - 「申請書送付希望」
  2. フォーマットに従って記入・送付
  3. イラスト付きマニュアルに従ってインストール
  4. IPレジストリシステムにログイン
- **問合せ先**
  - ca-query@nic.ad.jp