



Route Authorization
ルーティングのセキュリティに配慮したIRR
(Web公開版)

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
セキュリティ事業担当
木村泰司

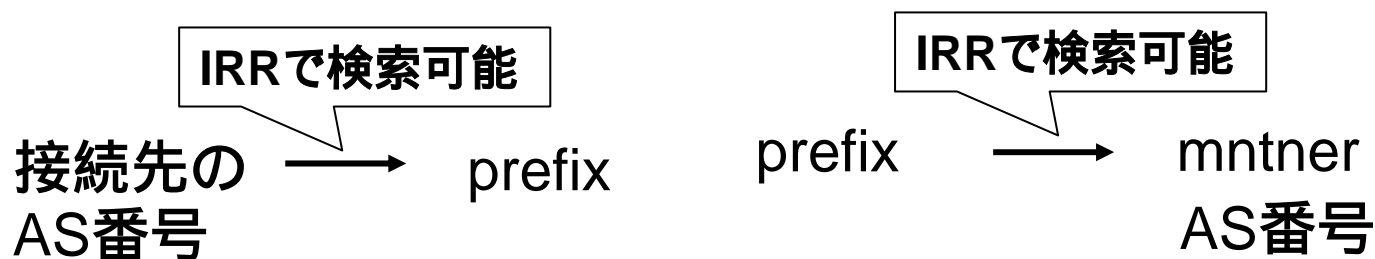


概要

- 次のJPIRRが目指すものの一提案
 - ルーティングのセキュリティに配慮したIRR
 - route authorization

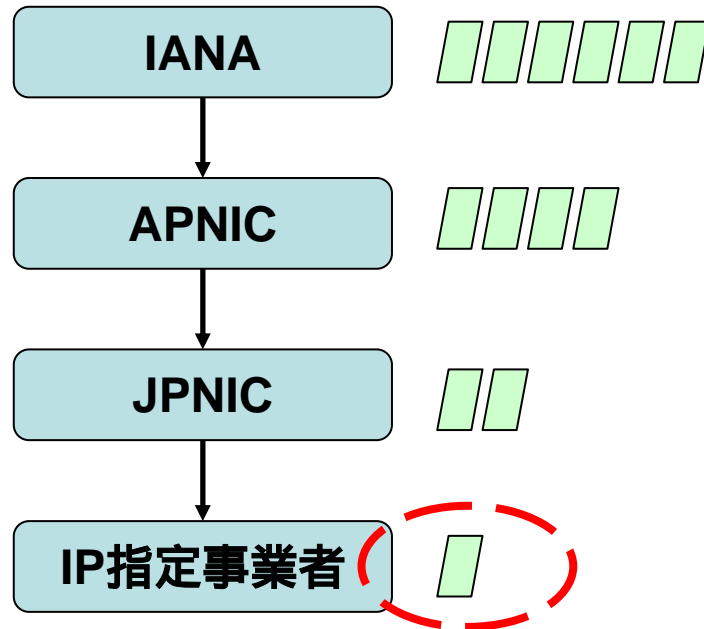
この機構についてご意見を頂きたいと思います。

- IRRの用途として...
 - 新しく経路が追加されるとき、接続先やトランジット対象となるprefixを確認する
 - ルータの経路フィルタ / パケットフィルタへの反映
 - BGPで広告されているprefixの管理主体 (mntner等) を調べる



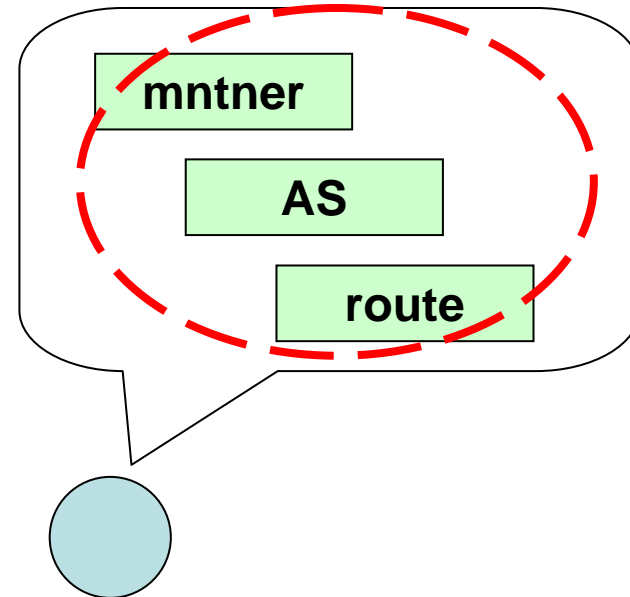
WHOISとIRRの関係

- WHOIS



AS情報
ネットワーク情報

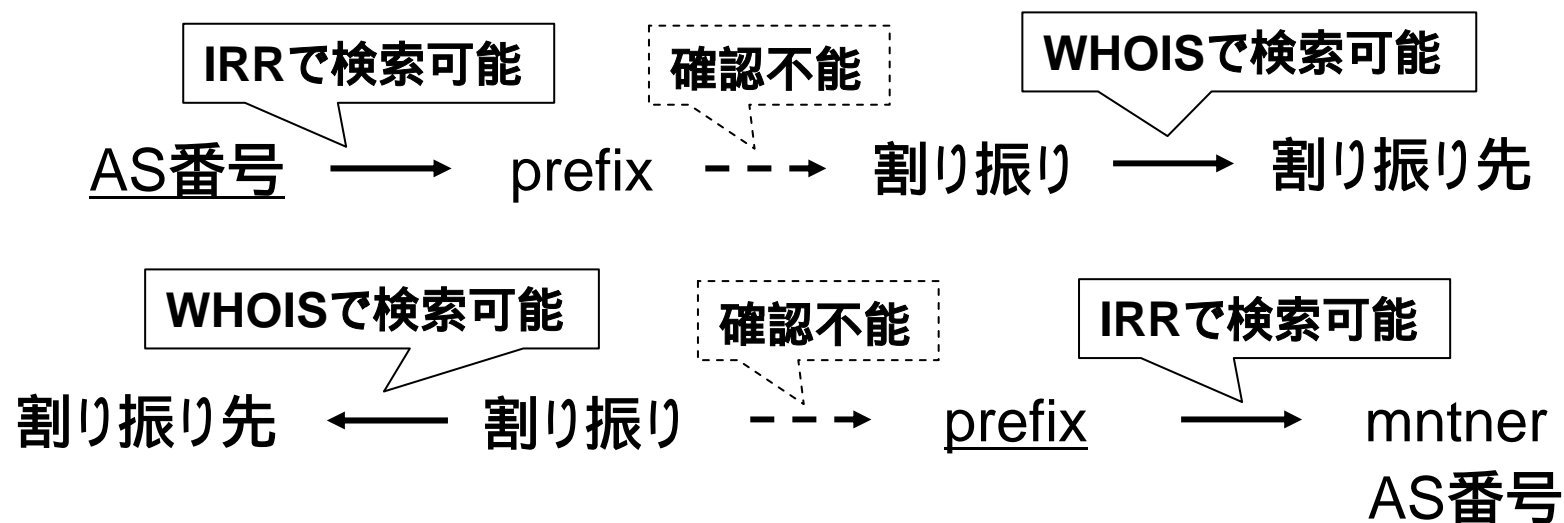
- IRR



登録される理由が違う

IRRの登録情報の信頼性

- WHOISでひける情報との関係は？



IRRに登録されている情報の信頼性は、よくわからないのが現状

- IRRとWHOISの各情報登録者の関係性は？
- IRRとWHOISの登録内容の整合性は？



IRRに登録された情報の信頼性

- ここで言う信頼性とは
 - 正規のユーザに登録されること
 - 登録するユーザの本人性が確認されること (a)
 - 登録数や慣例ではなくデータが正確であること
 - 登録されるデータの整合性が取れていること (b)



信頼性向上に必要なこと

- route authorization
 - IP指定事業者が管理下のprefixの経路広告をAS管理者に対して認可すること

 - route authorizationに必要なとなるチェック事項
 - a. IP指定事業者とAS管理者の本人性
 - b. IP指定事業者が認可したprefixとAS管理者が広告するprefixの整合性
 - prefixに対するOrigin ASの確認も必要

信頼性向上で得られること

- フィルタの正確さ
 - 経路フィルタ、パケットフィルタをかけるとき、不正に登録された情報に騙されることがない
- 経路ジャックの検出・防止
 - 経路ジャックがあったとき、他のIRR利用者にもそれがわかる
 - 影響を受ける領域を極小化できる可能性がある
- Secure BGP
 - S-BGP、soBGPの電子証明書(RFC3779)の発行に必要な情報がそろふ
 - IPアドレスとAS番号の組み合わせと発行対象



route authorizationの仕組み

JPNIC IRR企画策定専門家チームで
検討されているモデル



route authorizationの仕組み

1. 認証の連携

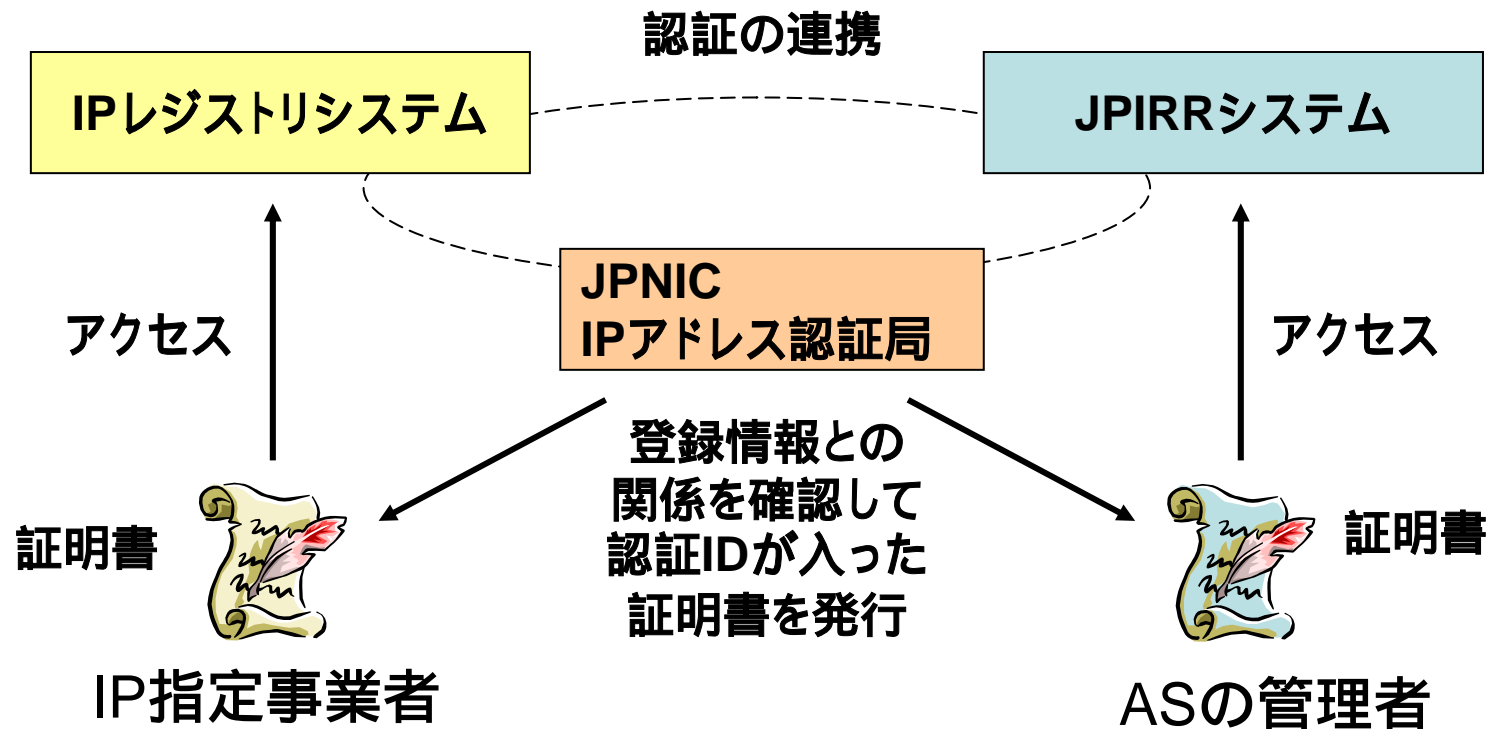
- IP指定事業者とAS管理者の認証を行う
 - IPレジストリシステムの「AS管理者」とJPIRRシステムのユーザの関係を確認する

2. 許可リスト

- IP指定事業者がAS管理者にprefixの利用を許可
 - IP指定事業者以外でIPアドレスやAS番号の割り当てを受けている組織でも利用できる仕組みを検討中

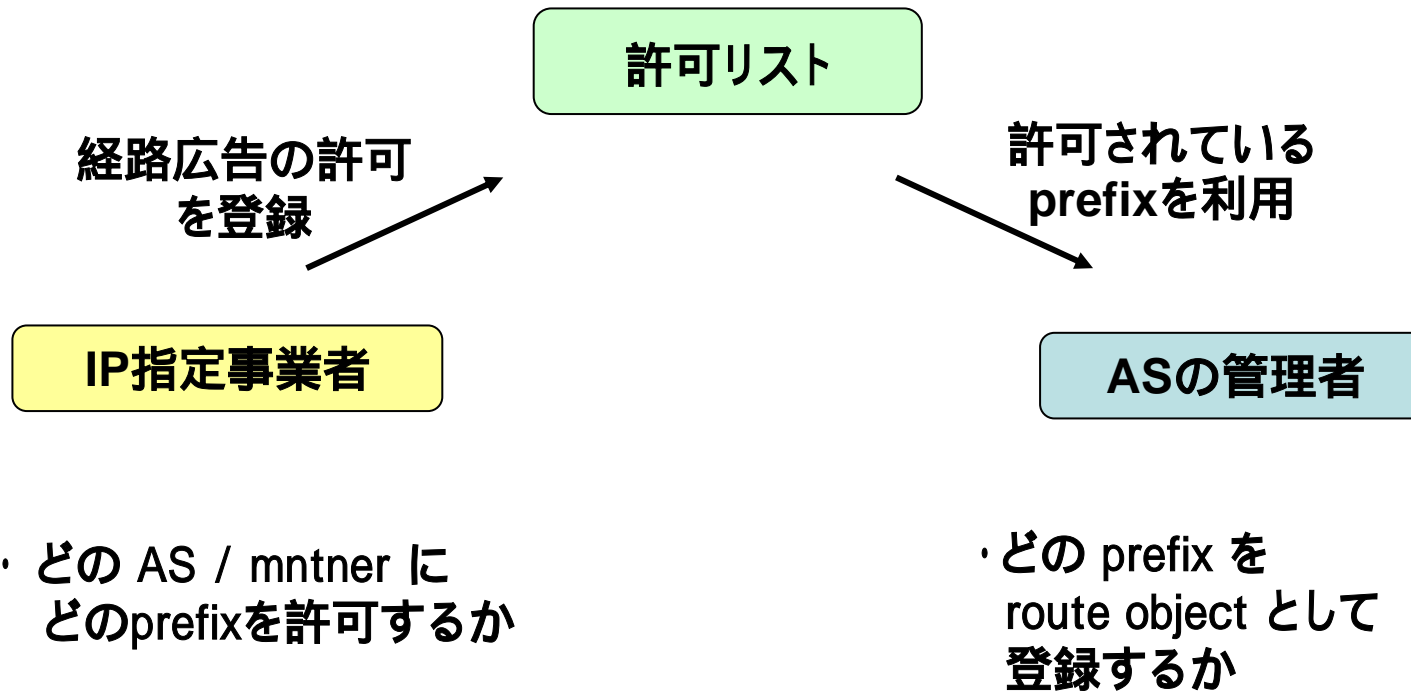
1. 認証の連携

- IPレジストリシステムとJPIRRの認証の連携



2. 許可リスト

- IPレジストリシステムとJPIRRの情報連携

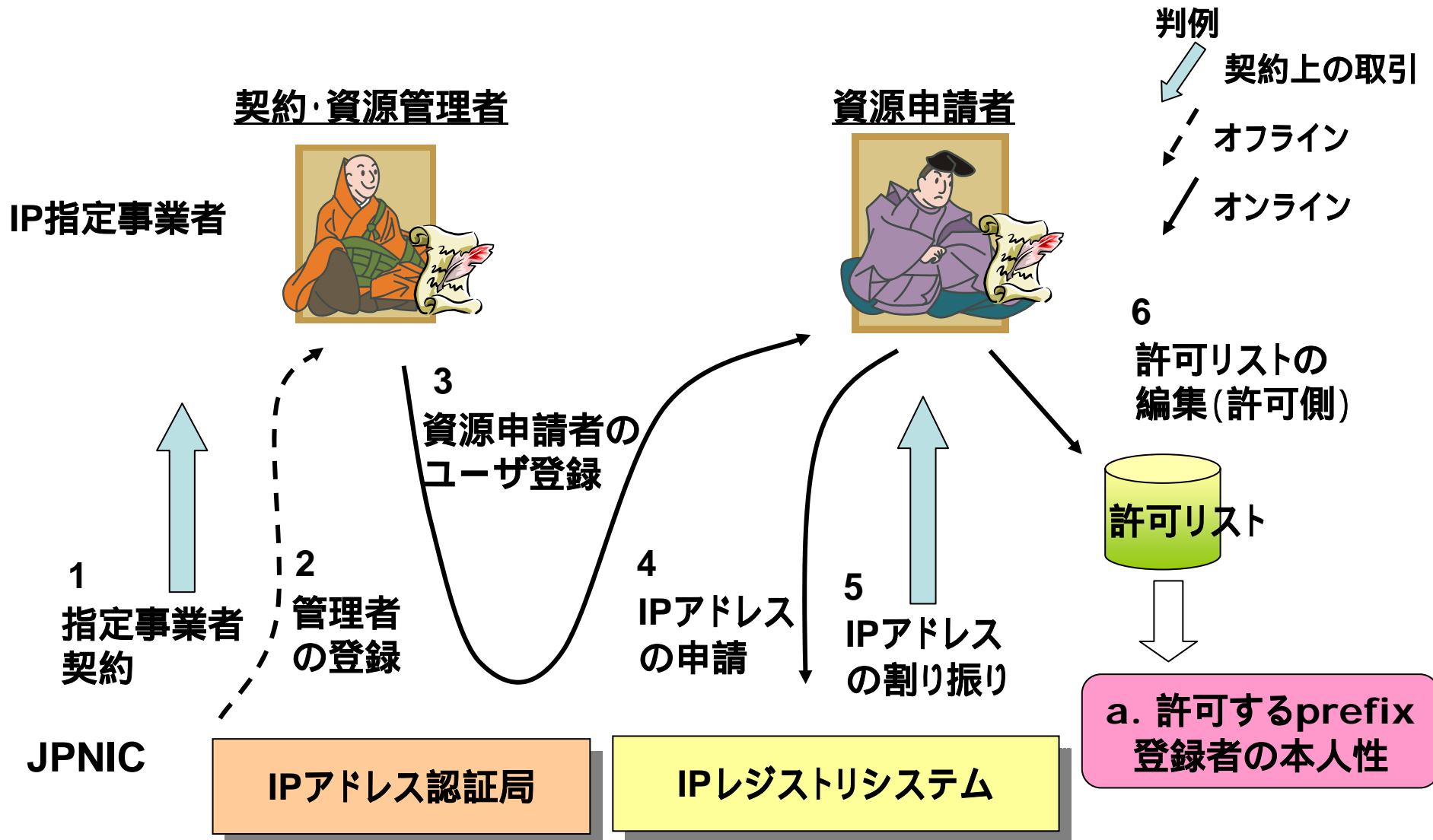




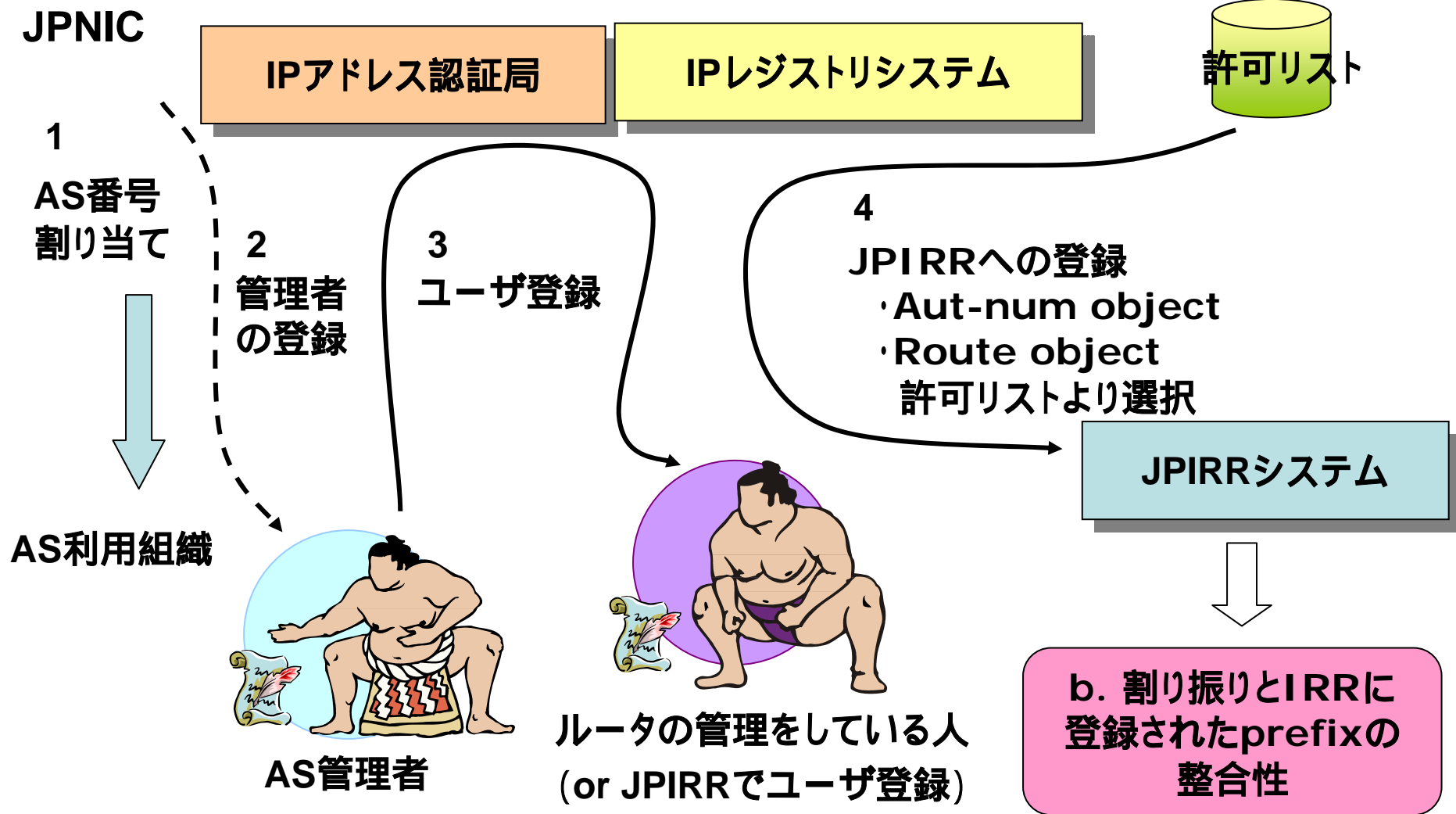
許可リストを使ったJPIRRへの 情報登録シナリオ



IPアドレスの割り振りと許可登録 (ISP側)



JPIRRへの登録 (AS側)



- 許可リストの例

prefix (登録できる 範囲)	許可 / 禁止	mntner	Origin AS (optional)
1.1.0.0/16	allow	mnt1	12345
1.1.0.0/17	allow	mnt2	

IP指定事業者の資源申請者が登録

JPIRRにroute objectが登録される際に、許可リストに登録されたprefixかどうかチェックされる。

- 機構の良い影響・悪い影響
- 許可リストを使った登録のチェック内容
 - 割り振られた範囲かどうか (IP指定事業者)
 - 許可された範囲かどうか (AS管理者)
- 登録者の範囲
 - JPNIC以外から割り振られたIPアドレス/AS番号をどうするか
 - ユーザ登録 JPNICにて行う(案)
 - APNICから割り振り flag(案)
- 新たに必要になること
 - JPIRRでのユーザ登録の仕組みの変更が必要
 - 割り振り先が経路広告するASのmntnerを知っていることが必要



情報: IP指定事業者の証明書利用 「認証強化実験」を実施中

- 情報源

- JPNIC CAのWebページ
 - <http://jpnica.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. 絵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





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
セキュリティ事業担当
木村泰司