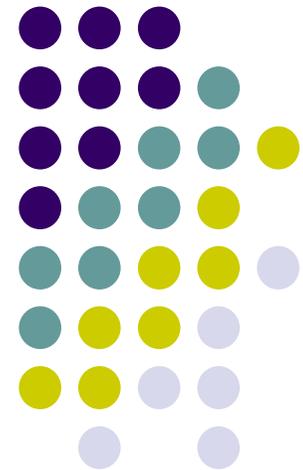


JPIRRの現状と今後の IRRについて

NTTコミュニケーションズ
JPNIC IRR企画策定専門家チーム 主査
吉田 友哉 <yoshida@ocn.ad.jp>



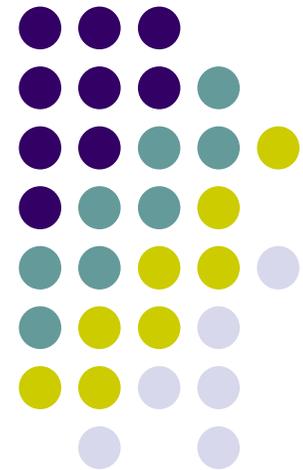
内容



- JPIRRサービス
 - 現在の試験サービス
 - 今後提供予定の正式サービス
- IRRの現在と未来

JPIRRサービス

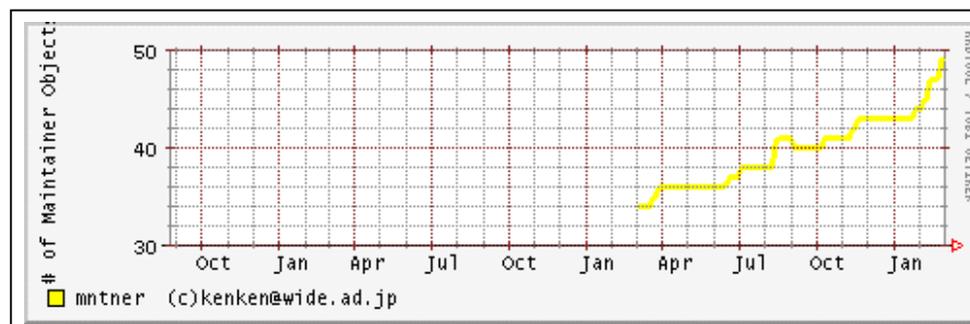
- 現在の試験サービス
- 今後提供予定の正式サービス





試験サービス概要

- 2002年8月よりサービス開始
 - 2004年4月より提供期間無期限へ
- 当初は、IPアドレス管理指定事業者を対象に実施
 - 日本国内でサービスを行っている人も可へ
- ミラーリング先
 - APNIC、RADB、RIPE NCC
- 2005/3/1現在の登録オブジェクト数
 - mntner: 49
 - aut-num: 30
 - route: 303
 - as-set: 22
 - <http://jpirr.nic.ad.jp/stat/>





現在提供しているサービス

- オブジェクトの新規登録/更新/削除
 - 初期登録時はJPIRR管理者がメンテナ情報を登録
 - JPIRR管理者=irr-admin@nic.ad.jp
 - それ以降の更新作業はユーザ側で実施
- オブジェクトの検索
 - JPIRR情報の他、ミラーリング対象のオブジェクトに対する検索結果の参照提供
 - 現在は、RADB、APNIC、RIPE NCC
- ミラーリングサービス
 - JPIRRの情報を参照



現在提供しているサービス

- ガーベージコレクタサービス
 - 一定の更新期間を超えたオブジェクトの通知、削除など
 - 1年間更新されていないオブジェクトがあった場合、事前に告知、数ヶ月後に削除を実施、など
- ポリシーチェックサービス
 - ASオブジェクト同士のポリシー比較
 - ASオブジェクトに記載されている、import/export などのポリシーの整合性を他のASオブジェクトのポリシー情報と比較
- IRRに関する情報提供
- 上記内容に関する問い合わせ



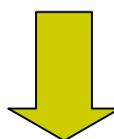
サービスに関する情報

- サービス情報
 - <http://www.nic.ad.jp/ja/irr/>
⇒「IRR (Internet Routing Registry)」に詳細情報を掲載
- ユーザ情報交換メーリングリスト
 - <http://www.nic.ad.jp/ja/profile/ml.html#irr>
 - 自動登録で、登録者に制限はありません
- 申請、登録窓口等
 - 初期登録申請 irr-admin@nic.ad.jp
 - 更新窓口 auto-dbm@nic.ad.jp
 - 質問窓口 irr-query@nic.ad.jp



サービス目的

- IRR企画策定チームが提案しているモデルの検証
- IRRサーバ運用経験の取得
- 日本におけるIRRの必要性に関する調査
- 次期IRRサーバ実装に向けてのプラットフォーム作り
- JPNICメンバに対するIRRサービスの提供とサービスの認知度向上、普及活動



インターネットの円滑な運用のための情報提供
JPNIC会員、指定事業者などへの付加価値提供

提供予定の正式サービス



- サービス対象
 - IPアドレス管理指定事業者
 - JPNIC管理下のPIアドレスホルダー
 - 割り振り/割り当てを行ったレジストリがリソースの正当性保証を行うという観点
 - AS番号については、今後の状況に応じて対象に
- サービス提供開始
 - 2005年10月(予定)



提供予定の正式サービス

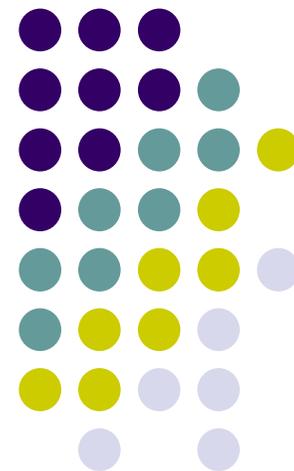
- オブジェクトの新規登録、更新、削除
 - メールやWebインターフェース (**HTTPS**)
- 登録情報の参照/検索:
 - WHOISコマンドや**Webインターフェース**
- 各種ツール類の提供
 - **経路比較結果表示サービス**
 - ガーベージコレクタサービス
 - **Filter生成ツール**
- 上記に関する問い合わせ
- IRRに関する情報提供



提供予定の正式サービス

- IPv6対応
 - IPv6アドレスの経路も登録可能に
 - 標準サービスとして提供
- セキュリティ
 - 登録時の認証強化
 - 実装例: JPIRRの登録用インターフェースでクライアント認証
 - JPIRRを参照したユーザが登録情報の正当性を検証する機能
- ミラーリングに関する検討
 - 主要なIRRへのミラーリングを追加
 - 各ISPのIRR上で、JPIRRへの登録データが参照可能なように今後調整

現在のIRRと未来のIRR





現在のIRR

- 経路データベースとしての利用
 - ISPにおける経路参照、抽出元情報
 - IRRによるPrefixフィルタ自動生成
 - 外部経路監視システムの監視情報の抽出
 - <http://www.ntt.com/release/2004NEWS/0002/0226.html>
 - 経路の信憑性確認
 - 異常時のコンタクト
- 問題点や課題
 - 信憑性の欠如、維持、ゴミオブジェクト問題
 - 情報の分散化、必要情報取得性の低下
 - 最低50以上のIRRが世界に存在 (MeritのIRRリストより)
 - IRRシステムの安全性の問題

IRRの利用



Config の自動生成
経路の信憑性確認
コンタクト先情報取得
トポロジー情報取得

自分が登録する許可
があるデータベース
に登録

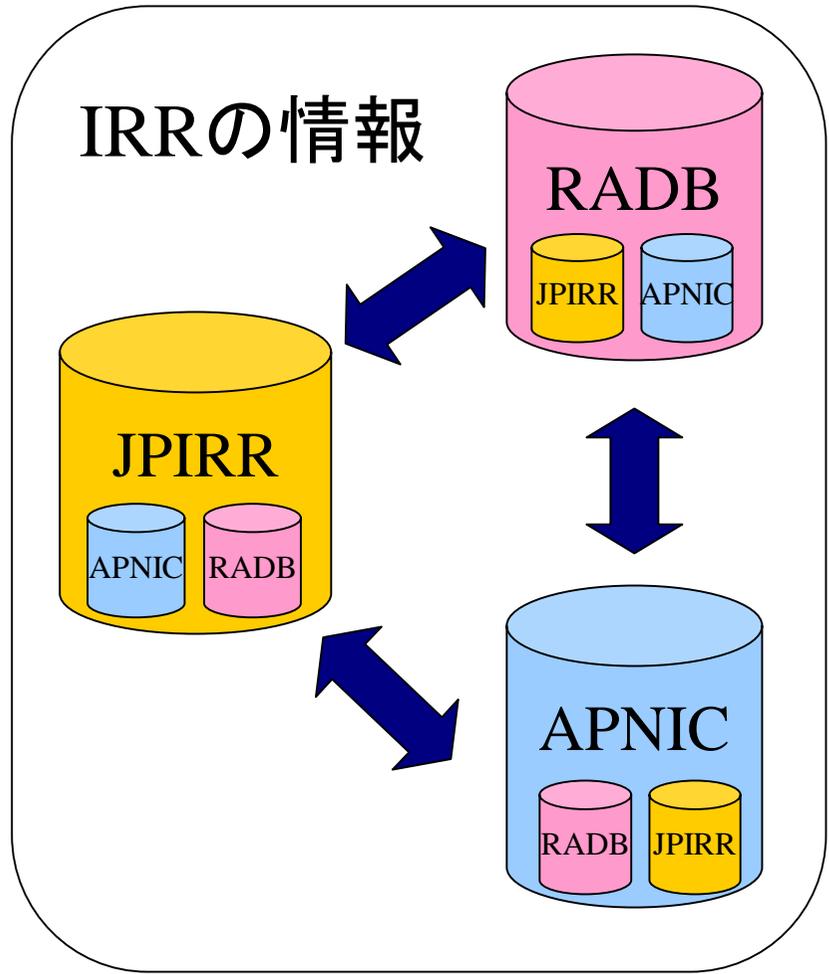


IRRユーザ

IRRサーバを直接Whois
で検索することができる

メールやWEB
でのデータ
ベース登録

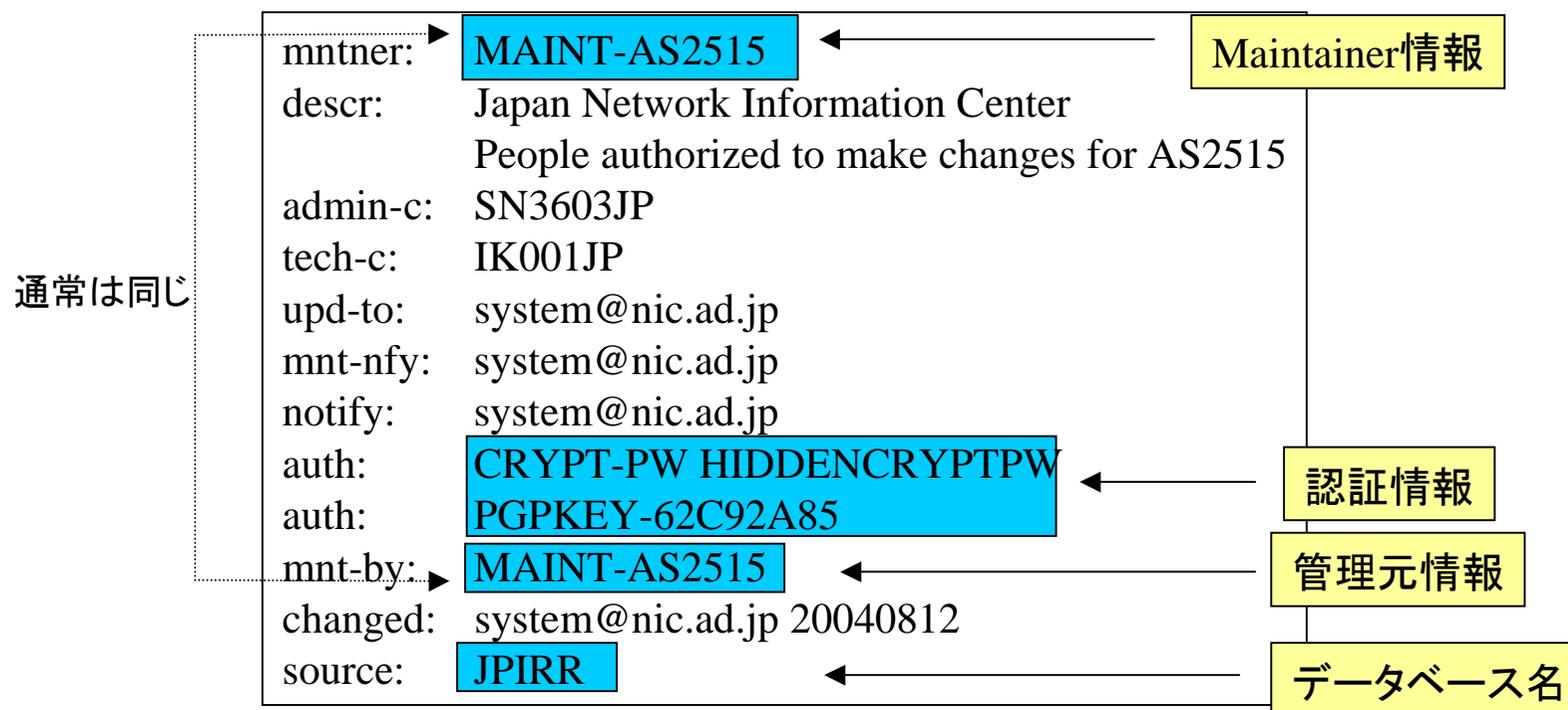
Whois やWEB
でのデータ
ベース参照



Maintainerオブジェクト



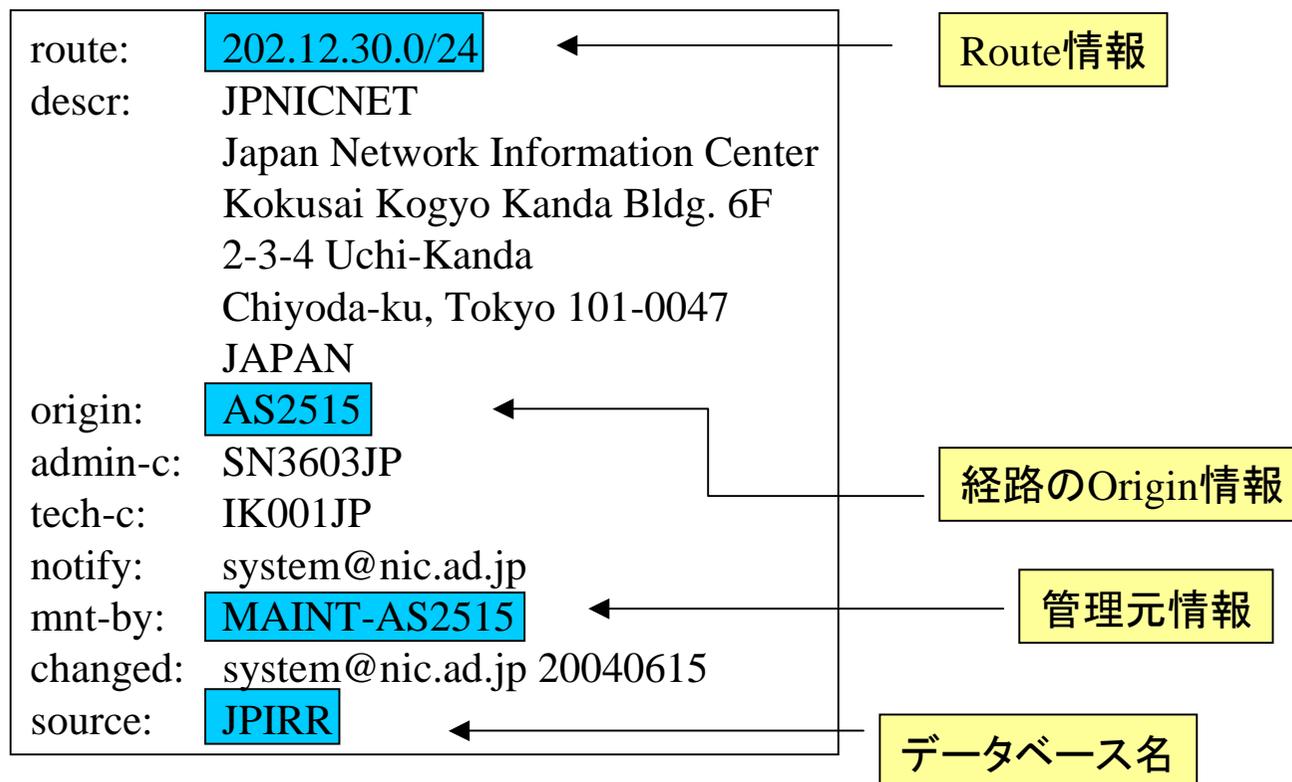
Maintainer Object (MAINT-AS2515) の例



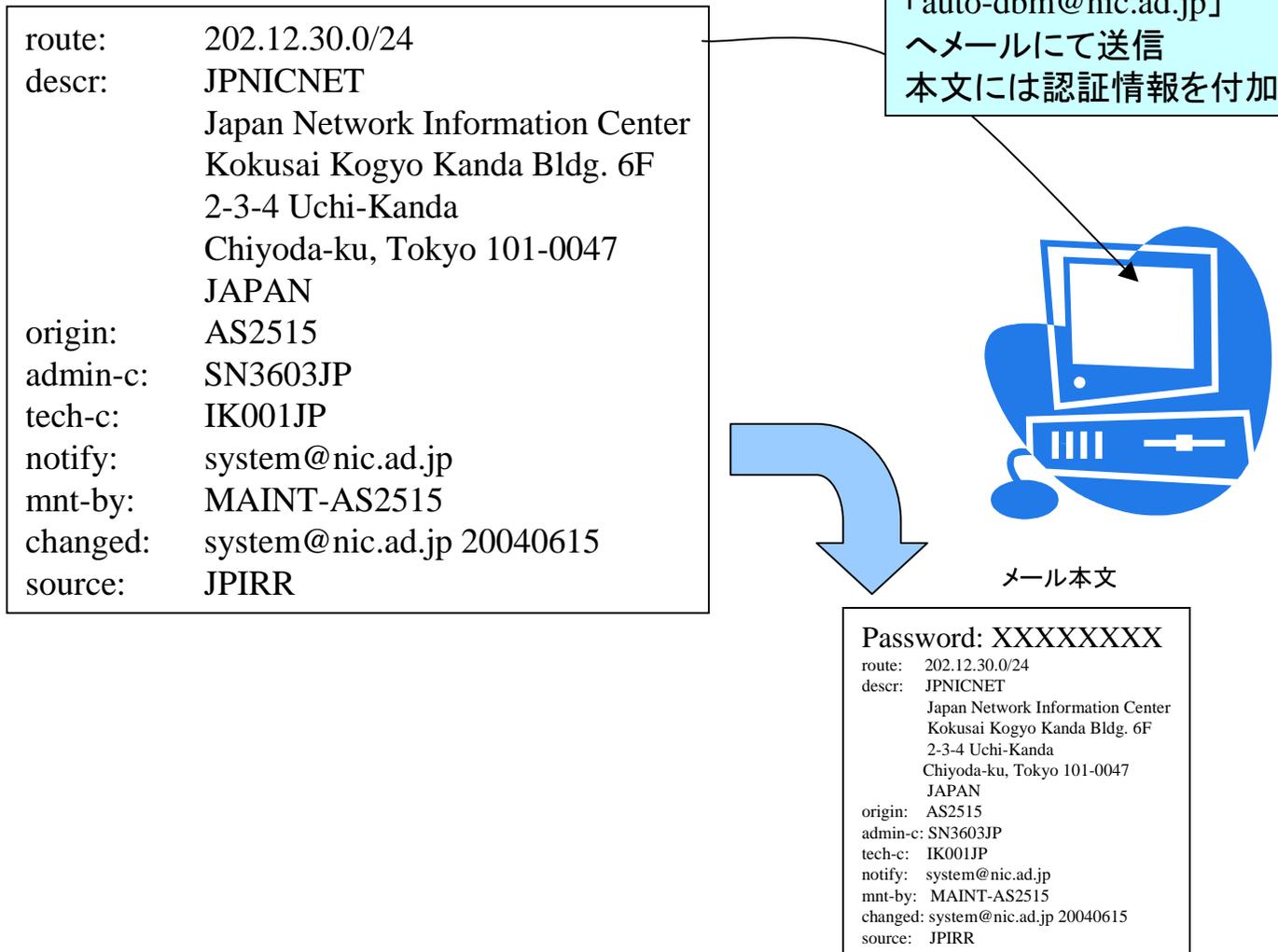
Routeオブジェクト



Route Object (202.12.30.0/24) の例



オブジェクトの登録





代表的なオブジェクト

オブジェクト名	説明
Maintainer オブジェクト	各IRRのオブジェクトの管理主体を表すオブジェクト。最初に必ず、他の全てのオブジェクトに先立って登録する必要がある。本オブジェクトが正しく生成された後は、他の全てのオブジェクトが本オブジェクトの管理化の元生成可能となる。また登録に際する認証情報も本オブジェクトに含まれている。
Route オブジェクト	所謂BGPの経路情報である、プリフィックス情報を表すオブジェクトのこと。プリフィックス情報に加え、ASの起源情報も記述される。
AS オブジェクト	AS情報を表す。また、そのASのポリシー情報(どのASからこういった経路を、どの程度の優先性をもって受信するか、など)も記述することが出来る。
AS Set オブジェクト	複数のASを1つの共通したポリシーにまとめて記述するオブジェクト。トランジットISPなどが、特定の管理ポリシーの元に、自ASの複数の顧客ASを1つにまとめて記述するなどが最もよく使われる方法で、IRRを利用するほぼ全てのトランジットISPが利用しているといっても過言ではないであろう。
Person オブジェクト	特定の個人に関する詳細の情報を表すオブジェクト。住所やメールアドレス、電話番号などの詳細な情報まで記載される。
Role オブジェクト	ある特定の組織や同一の役割を表すグループの詳細情報を記載したオブジェクト。住所やメーリングリスト等の共通のメールアドレス、組織の電話番号などが記載される。

IRRの歴史



- RAプロジェクト
 - 昔IRRを研究していた有名なプロジェクト
 - Internet eXchange 上における経路交換時に、ルートサーバの技術を利用
 - そのルートサーバはデータベースに蓄積された経路情報とポリシー情報を元にBGPピア間の経路制御を実施、そのデータベース
⇒ IRRデータベース
- 5極体制(1999年以前)
 - RADB、RIPE NCC、C&W、ANS、Canet
- IRRdの無料配布、RADB有料化(1999年～)
 - 手ごろで強力なツール
 - ミラーリングもサポート
 - 徐々にISP間に広まっていき、ISP独自のIRRサーバが林立へ



レジストリ(RIR)におけるIRR

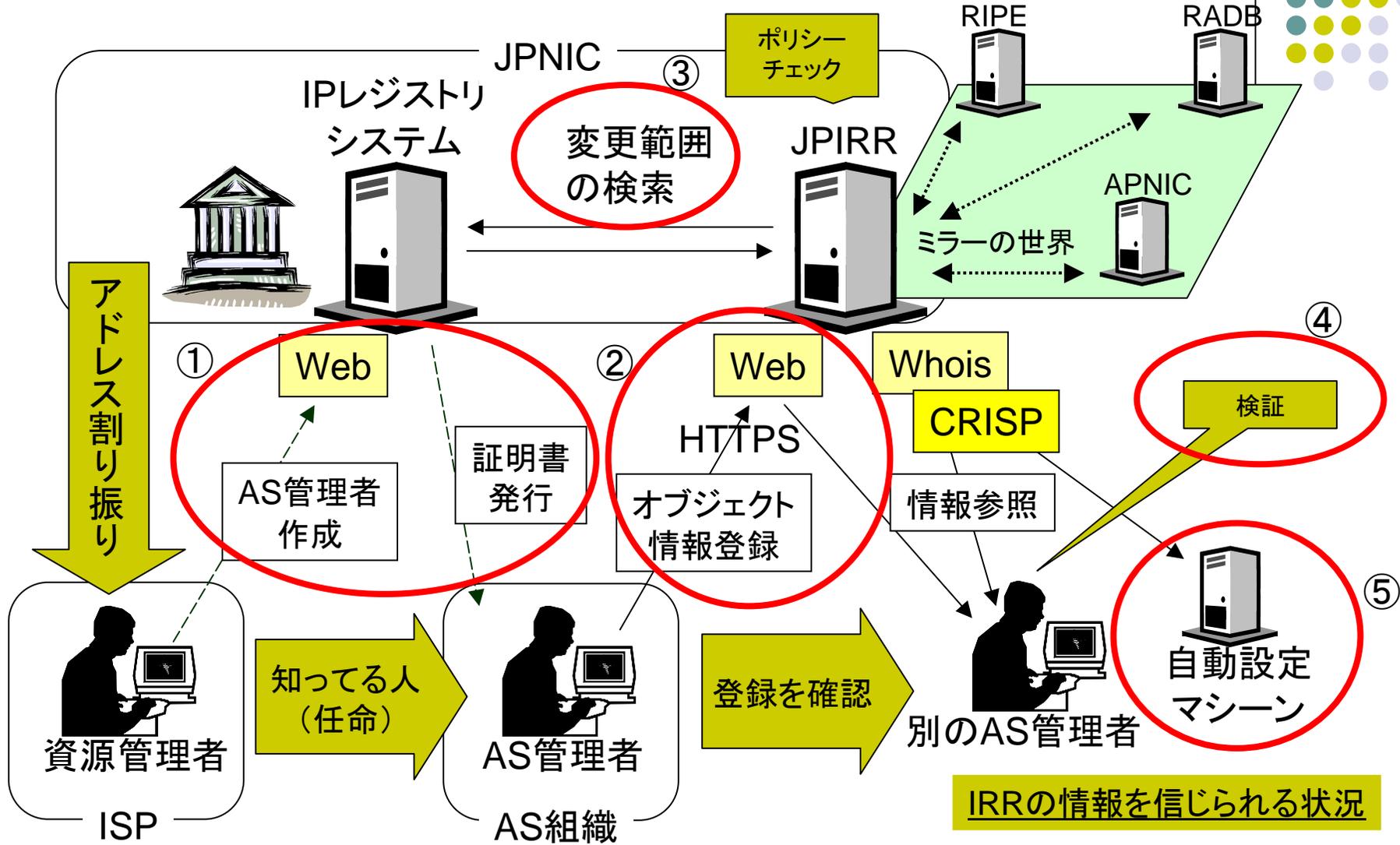
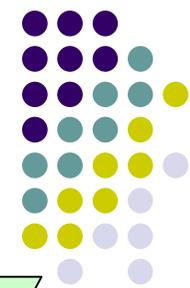
- RIPE NCC
 - 古くからIRRをサポート
 - 昨年12月にIPv6サポート開始
- APNIC
 - 2001年より実験サービスの開始(APIRRプロジェクト)
 - 2002年より正式にサポート
 - 2005年4月にIPv6サポート開始予定
- ARIN
 - 試験サービスを提供
- LACNIC
 - IRRのサービスを提供予定



未来のIRRへ向けて

- 信憑性、信頼性の高いIRRを作る
 - 安心して登録出来る ⇒ 認証局との連携
 - 登録内容を信じて利用出来る ⇒ レジストリが保証
 - 情報から相手の認証が可能 ⇒ 電子署名
 - 情報の更新(の促進) ⇒ ガーベージコレクタシステム
- IRRの情報の扱い、Mirroring Levelの明確化
 - Public IRR情報、Private IRR情報
 - Global Level、Local Level
 - 特にIPv6の世界を作っていく上では重要
 - 情報の保証範囲がおのずと出来あがる
- Origin ASの認証、検証システム
 - IRRを用いたOrigin認証、検証システム
 - Routing Hijack の撲滅へ

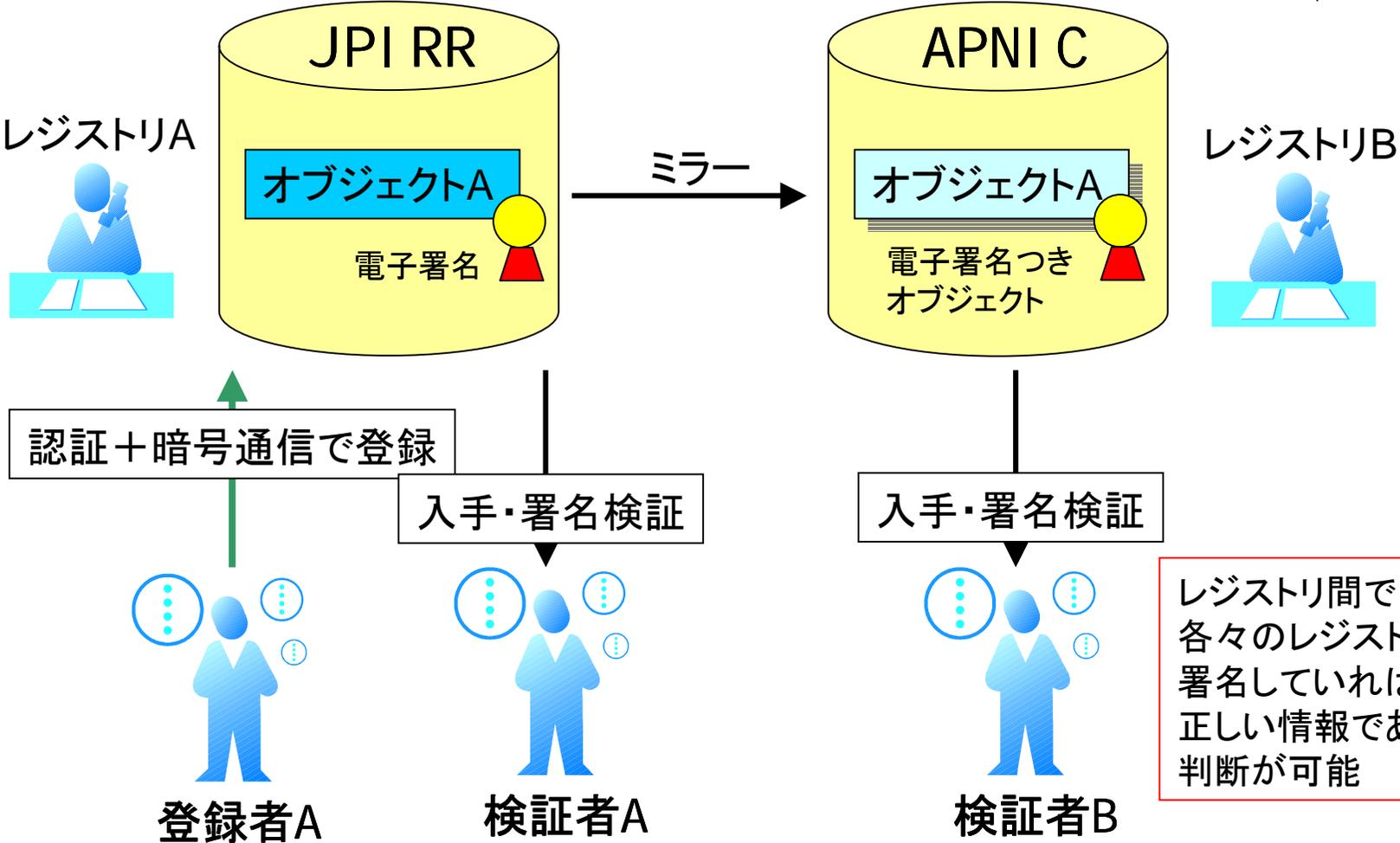
次世代IRR基盤システム



次世代IRR基盤システム (Cont.)



オブジェクトの署名、保障 ⇒ レジストリ





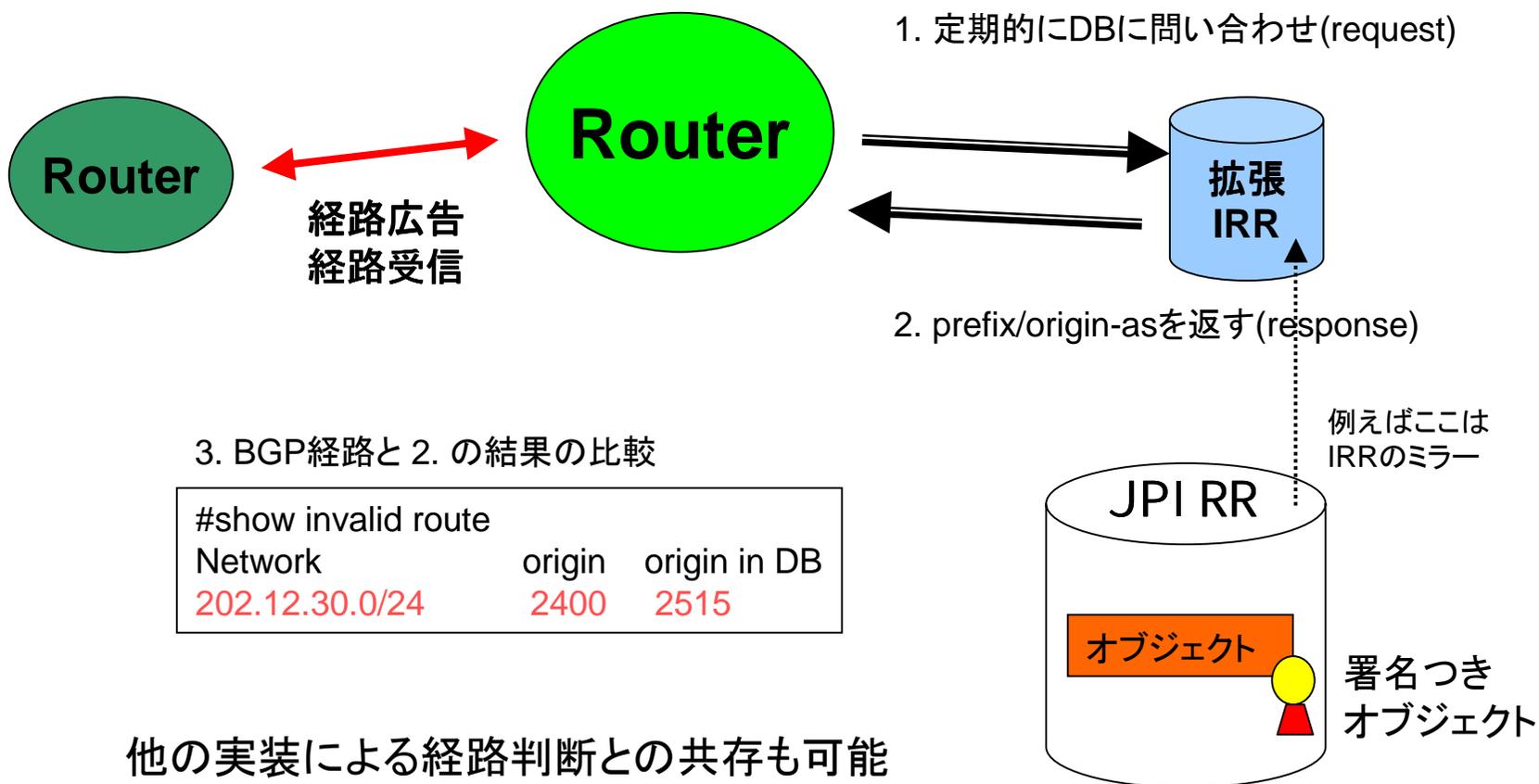
Origin ASの認証・検証

- Routing Hijack問題
 - 単なる間違いから意図的な悪意のあるものまで様々
 - 実際、ある程度の頻度で観測されている
 - 通常 Origin AS が正しいか否かに関わらず受信
- Origin ASの認証・検証方法
 - S-BGP / soBGP
 - PKIの技術を利用した経路配信メカニズム
 - 一部実装あり
 - IRRの利用
 - IRR情報とBGP経路情報との整合性を確認する手法

IRRを用いた未来の経路制御



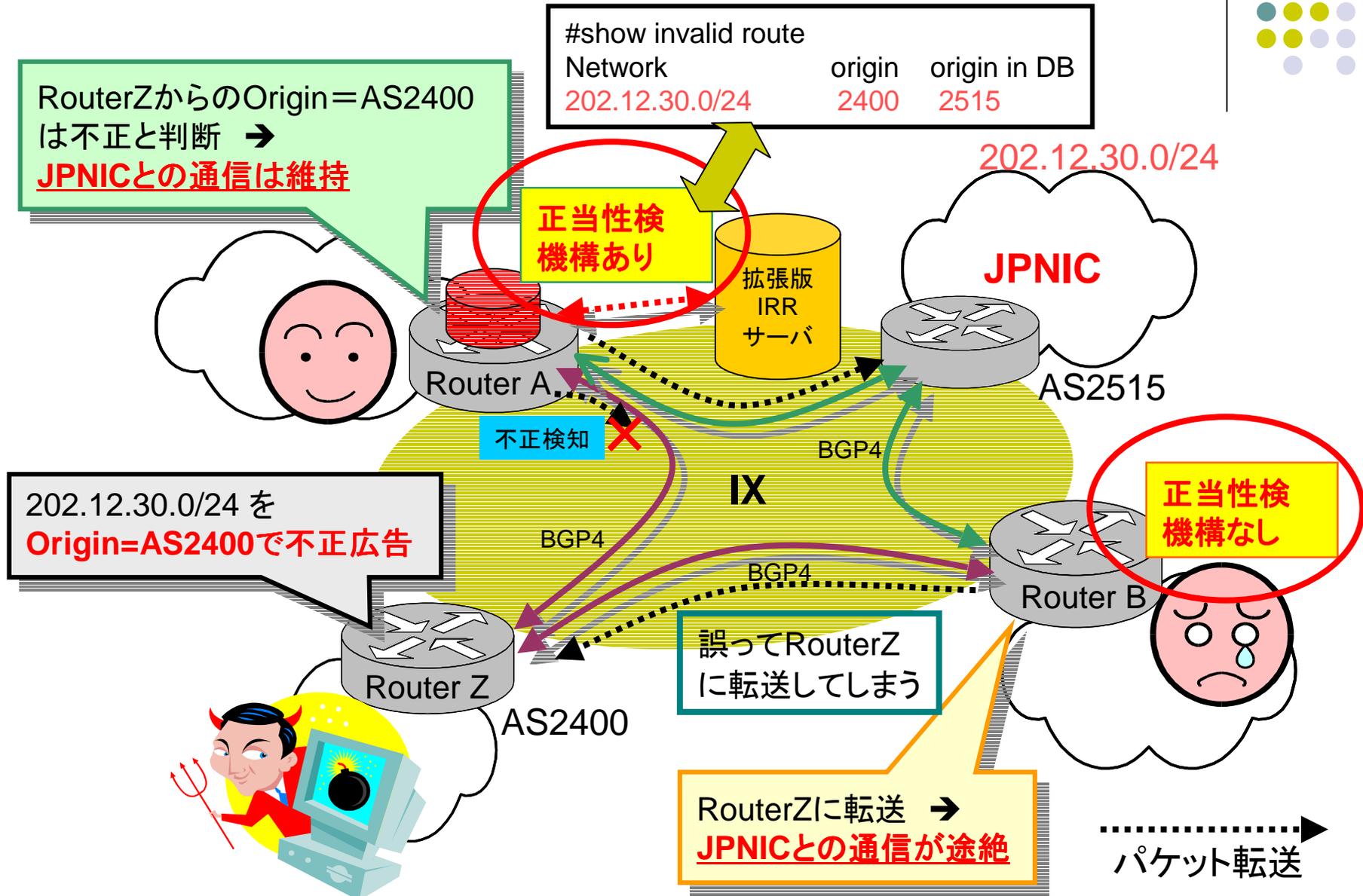
GWの機能をもったRouterが問い合わせを行う、あるいはRRのような部分が一括で問い合わせを行う、など



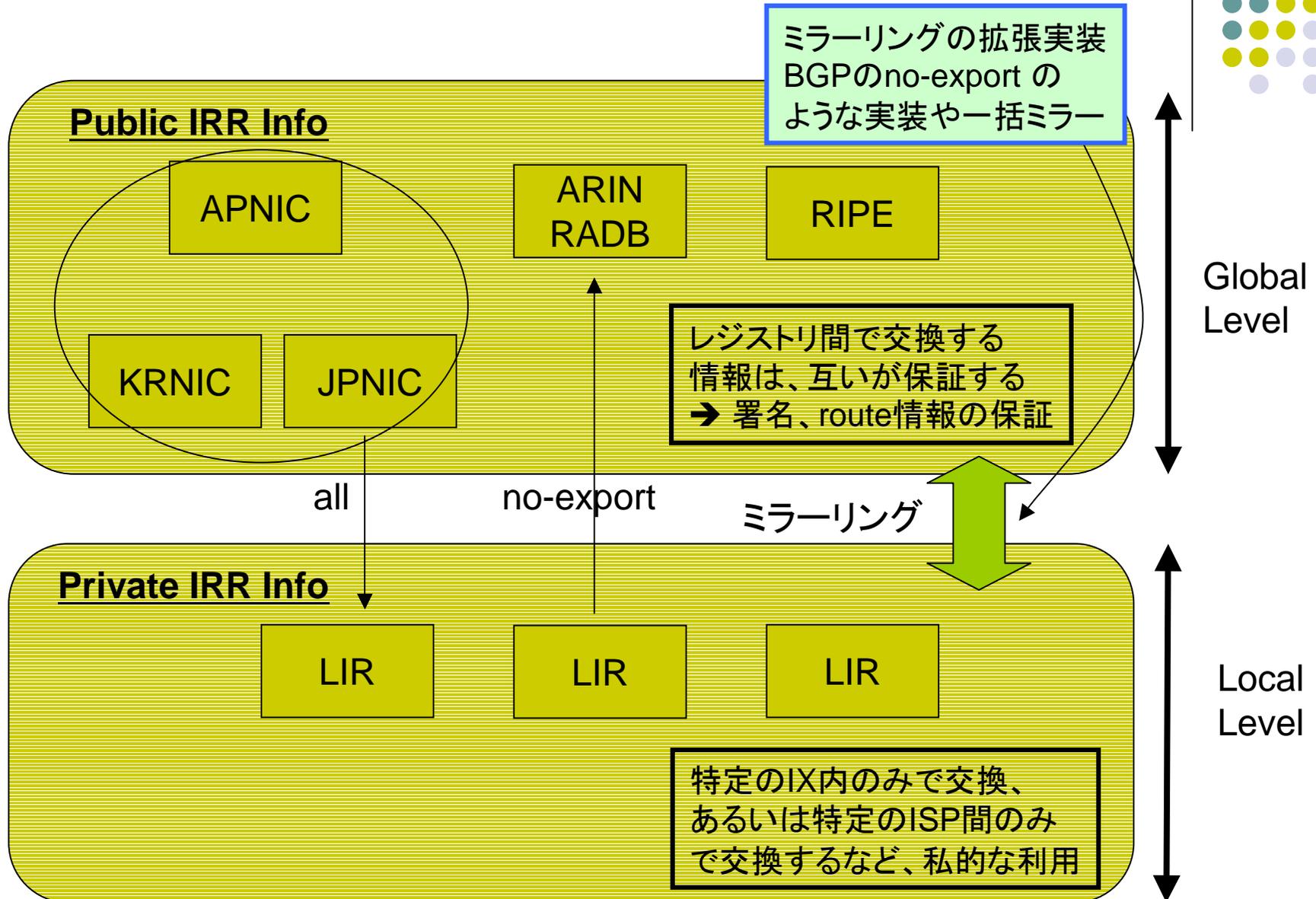
```
#show invalid route
Network          origin  origin in DB
202.12.30.0/24  2400   2515
```

他の実装による経路判断との共存も可能
出来る部分から徐々に実装 → 信憑性の向上

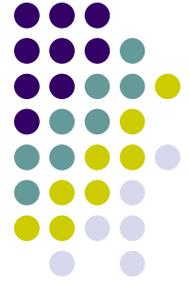
IRRを用いた未来の経路制御



情報の明確化とIRRの拡張



他システムとの融合・連携



- レジストリ認証局での統一管理
 - レジストリがIRRサービスを実施することで、IPアドレスやAS番号の管理と同じスキームでIRRのオブジェクトも管理出来る
- 検索システムの統合
 - CRISP (Cross Registry Information Service Protocol) が現在IPとDNSで実装検討中 (IDが存在する)
 - IRRへの拡張 (IDを提出)
 - IR階層モデルによるIRRの検索システムの構築

今後のIRR



- 目指すは、信頼性、信憑性の高い魅力のあるIRR
 - 日本では、Whoisデータベースと連動し、登録の範囲を特定した上で正しい登録者が登録できる状況へ（2005年度より試験提供予定）
 - 世界的には、同じ方向性を目指してより連携を蜜に
 - レジストリ認証局の実装、モデルの共有へ
- ユーザに魅力あるJPIRRサービスを提供
 - 経路情報とのマッチングによる不整合の検出機能
 - 定期的にUpdateを促すような実装
- IPv6では、日本がリードしていきたい
- sBGPやSo-BGPでも、最後はIRRが必要だということ
 - エンドユーザ同士が認証する仕組みにおいて、その正しさを判断するには、必ず何か判断元のデータベースが必要＝IRRデータベース

参考



- IRRに関する情報
 - <http://www.nic.ad.jp/ja/irr/index.html>
- IRRとは何か
 - <http://www.nic.ad.jp/ja/mailmagazine/backnumber/feature/vol063.html>
- サービスに関する検討報告書
 - <http://www.nic.ad.jp/ja/materials/irr/irr-report-2003.html>
- 登録マニュアル
 - http://jpirr.nic.ad.jp/jpirr_resistory.html

ご質問、ご意見等よろしくお願ひします

