経路制御の信頼性向上

NTT Communications
JPNIC IP Address Committee, JPNIC IRR-Plan Chair
NSP-SEC-JP, IRS Workshop
Tomoya Yoshida <yoshida@ocn.ad.jp>

通信障害が引き起こす連鎖障害

- 1つのネットワークにおける通信障害がインターネット全体へ波及
- 偽/誤経路情報が引き起こす連鎖障害の撲滅に向けて…

BGP AS利用者の変遷

- ISP、xSP
- 研究組織、研究機関
- CATV
- 大学
  - Private AS → Global ASへ
- 大企業、IT企業

Inter-ASにおける経路制御の脆弱性

- 受信した経路情報の Origin AS は正しいか？
- 受信した経路情報の AS-PATH は正しいか？

- 予防方法は幾つかあるが、、
  - AS-PATH Filtering
  - Prefix Limitation
  - Special Address Block Filtering : RFC3330
  - Prefix Filtering

ルーティングハイジャック問題

- 実際に観測されている
  - 意図的なハイジャック、或いは単なる数字の書き間違い
  - more specific な経路には勝てない
- Origin AS の検証が必要
  - 通常 Origin AS が正しいか否かに関わらず受信
  - インターネットフルルート受信時は非現実的
- 対応方法は？
  - 被害者が more more specific な経路を広告

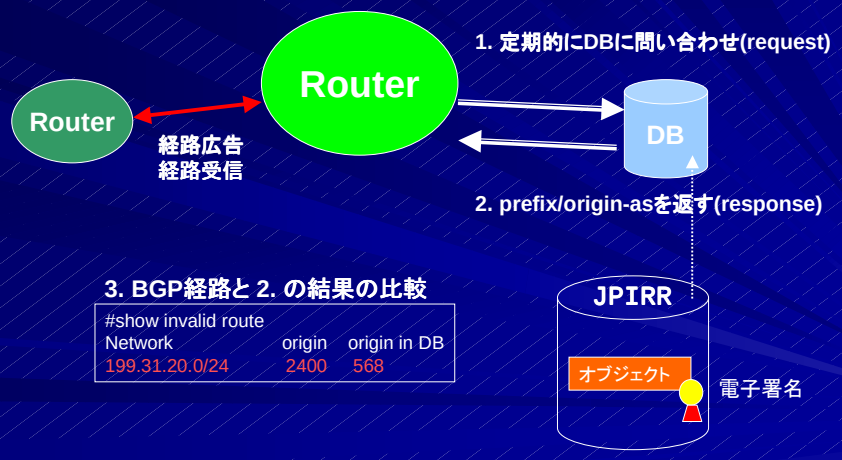
Origin AS の認証

- 本来保有すべき Origin AS 以外からの経路情報を排除する仕組み
  - IRR（Internet Routing Registry）の利用
    - IRRデータベースの情報と経路情報との整合性を確認する手法
  - S-BGP / soBGP
    - 電子署名の技術を利用した経路配信メカニズム
    - 一部実装あり

IRRの利用と現在の問題点

- 利用方法
  - 経路情報の信憑性確認
  - Transit ISP が Customer に対して経路フィルタを実施する際の参照元データベースとして利用
  - コンタクト情報の取得 他
- 問題点、課題点
  - 情報の分散化
  - 信憑性の維持
  - IRRシステムの安全性

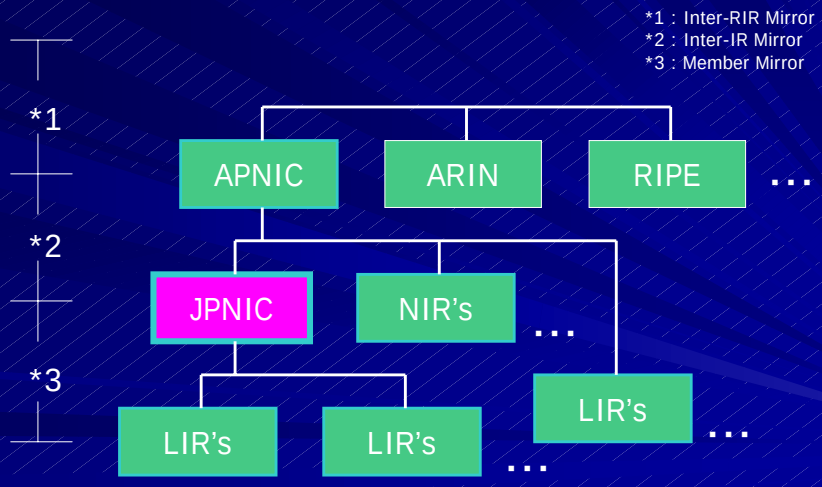
IRRを用いた経路制御の可能性



3. BGP経路と 2. の結果の比較

#show invalid route		
Network	origin	origin in DB
199.31.20.0/24	2400	568

IR階層モデルの実装



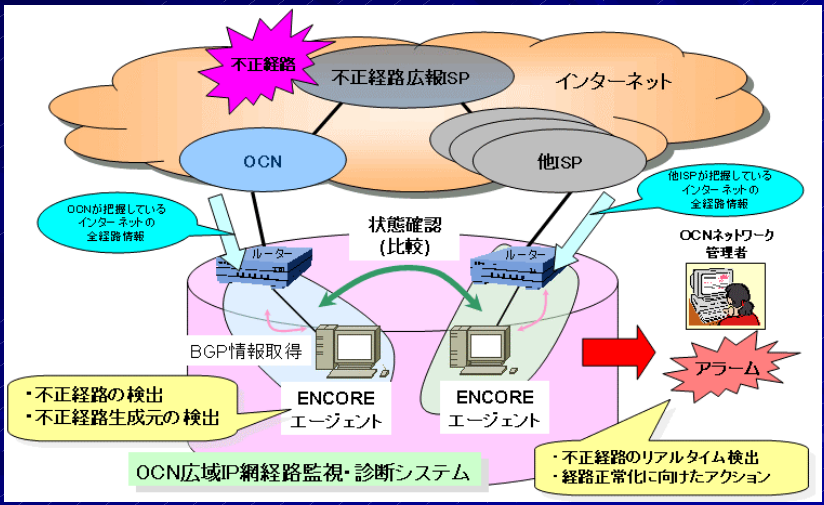
システムの融合は可能か？

- レジストリ認証局の一元化
  - IPアドレス、AS番号
  - IRR
- 検索システム
  - CRISP（Cross Registry Information Service Protocol）のIRRへの適応
    - IR階層モデルによるIRRの検索システムの構築

ISPの協調運用

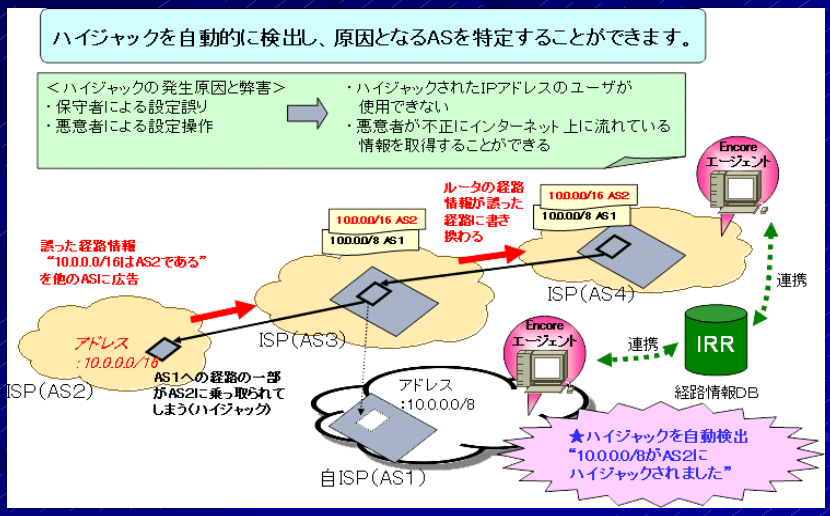
- 自AS内のみでは解決出来ない問題
  - 自分は適切な経路を選択している
  - 一寸先は闇
  - 実空間を利用した偽装パケット
- 互いのboundaryを超えた協調運用の重要性
  - コミュニティの活用、連携
- インターネットのマナーは皆で守りましょう
  - RFC 3013
    - Recommended Internet Service Provider Security Services and Procedures

OCN広域IP網経路監視・診断システム



http://www.ntt.co.jp/news/news04/0402/040226.html

OCN広域IP網経路監視・診断システム



http://www.ntt.co.jp/news/news04/0402/040226.html