JANOG22

「経路ハイジャック(が疑われる状態の)通知実験開始しました」

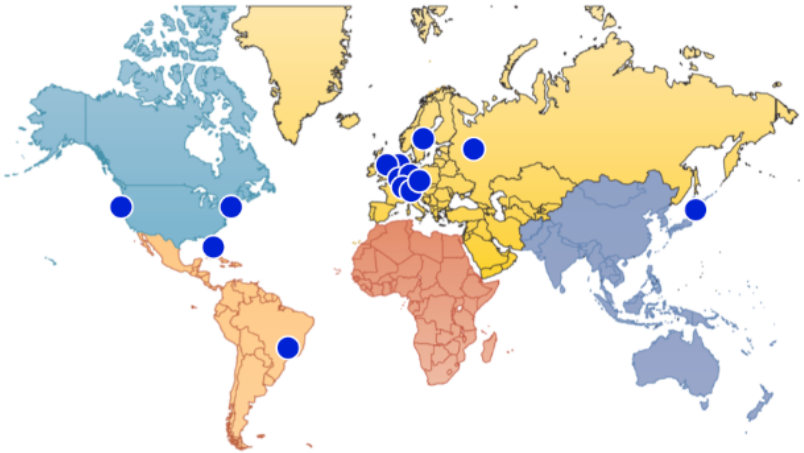
2008年7月10日
社団法人日本ネットワークインフォメーションセンター
技術部
岡田 雅之

本発表の内容

- BGPLayとYoutube事件
- IRRとJPIRR＋通知実験
- 経路ハイジャック通知実験の状況
  （が疑われる状態の）
- 事例紹介
- この後は、、、

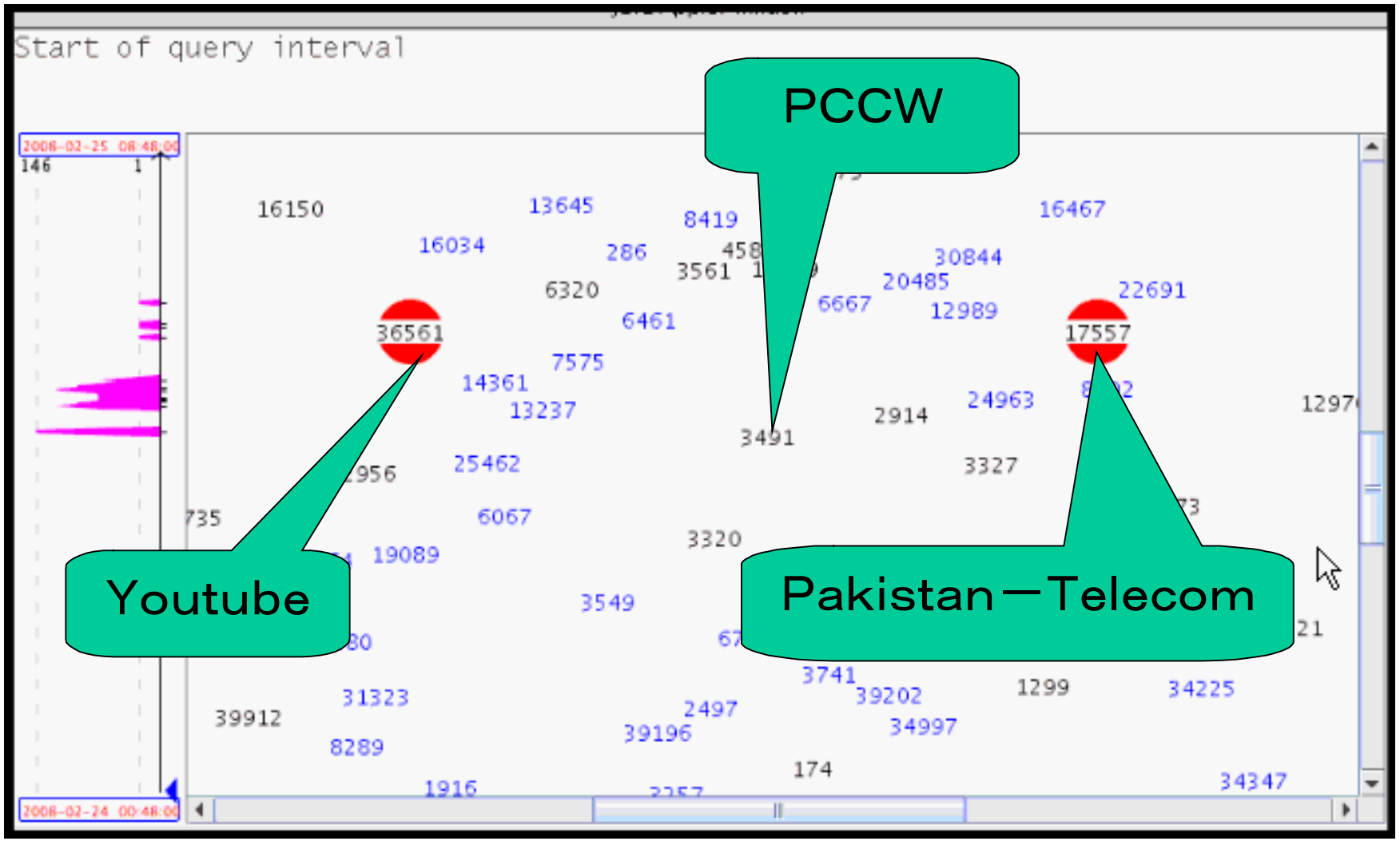
BGPlayというツールを使って説明します

- **BGPの経路情報を視覚化するツール**
  - RIPENCCやRoute-Views Projectなどで提供
  - BGP経路情報を時系列で視覚化
- **RIPENCC RISのBGPlay**
  - http://www.ris.ripe.net/bgplay/
  - 世界15拠点で経路情報収集

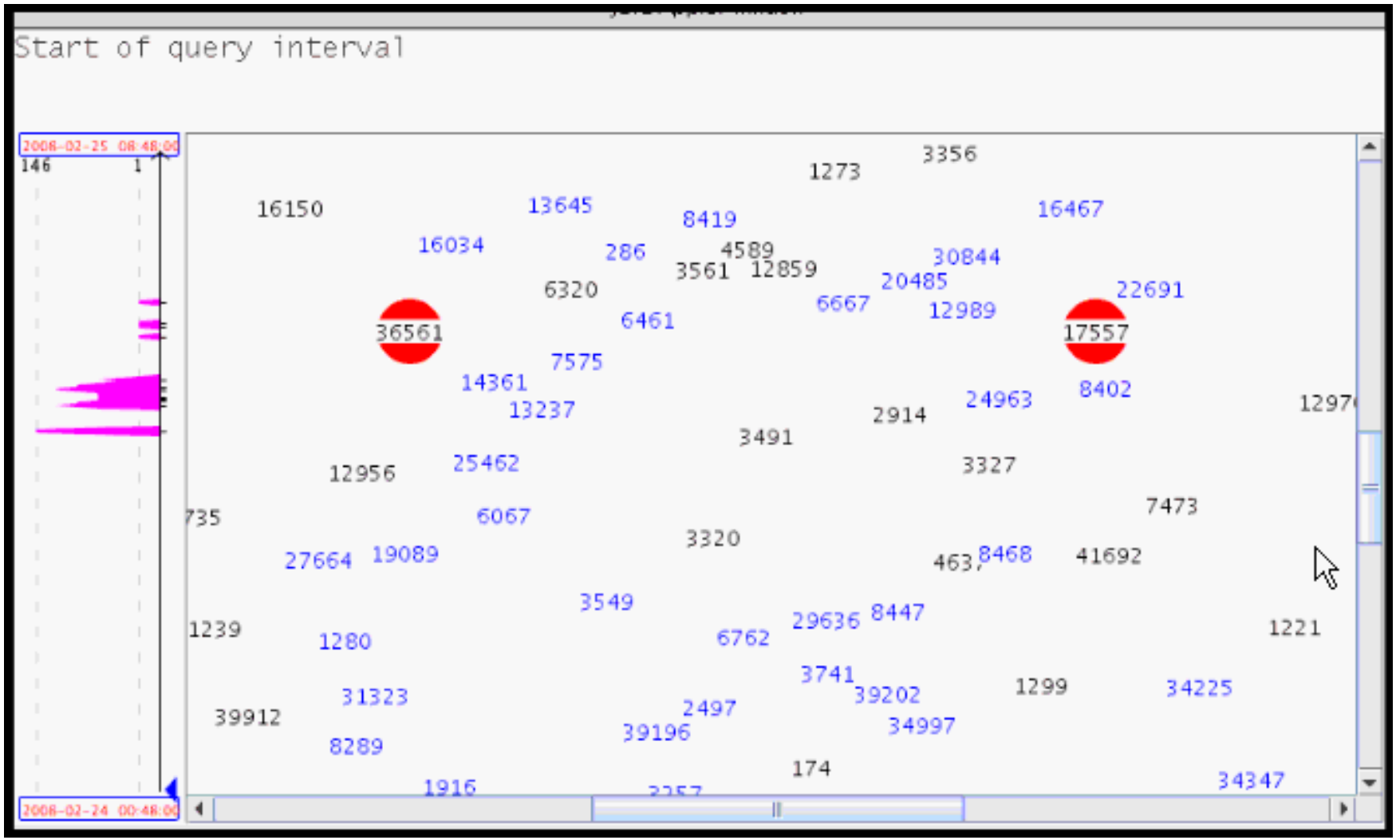


出典：http://www.ris.ripe.net/bgplay/ RRCs Locations Dataより

BGPlayで見るYoutube事件（主な登場人物）



BGPlayで見るYoutube事件

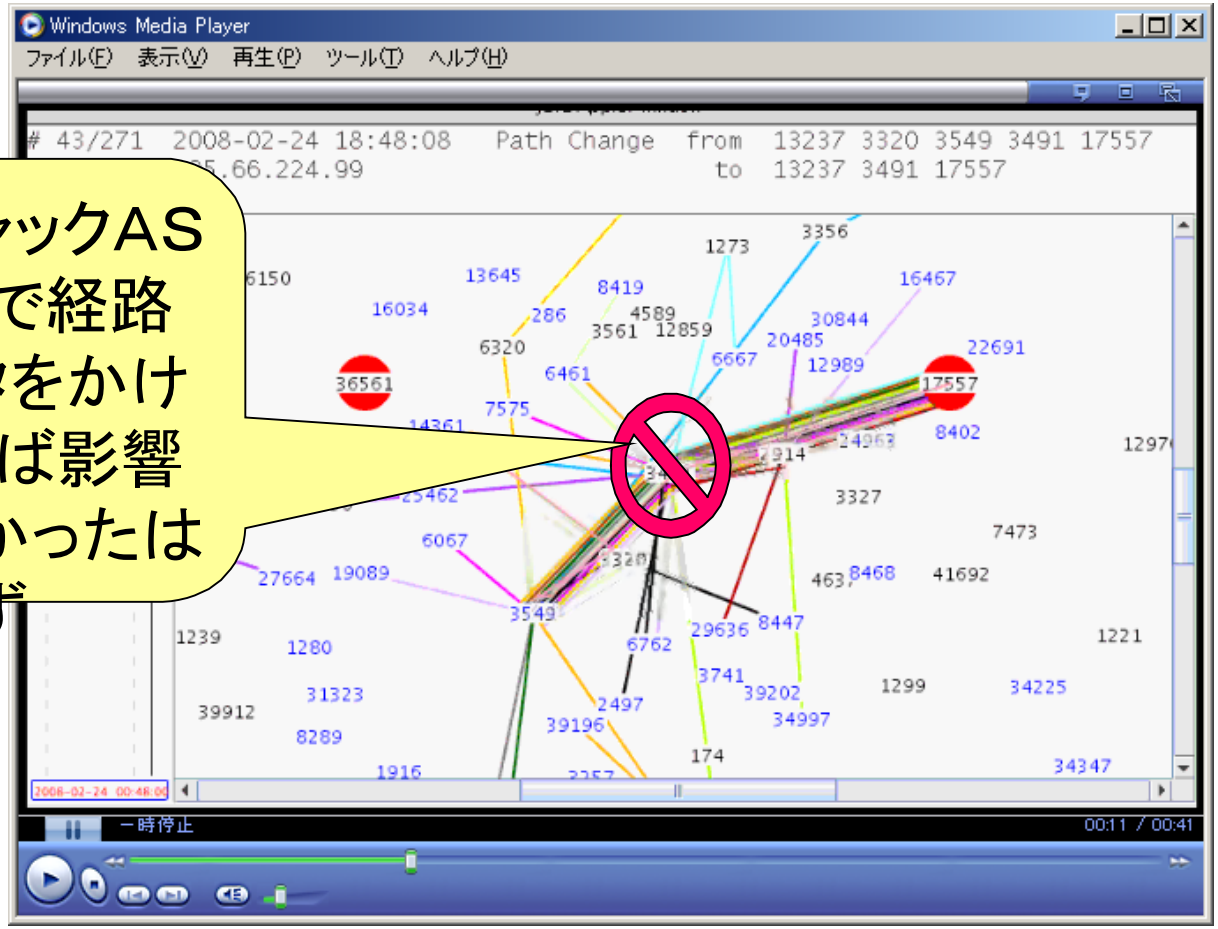


IRRとJPIRR＋ハイジャック通知実験
（が疑われる状態の）

- **IRR**
  - Internet Routing Registryの略で経路情報の台帳
- **IPアドレスが使えるようになるまで**
  1. レジストリからIPアドレスを取得
  2. **どこかのIRRへ登録**
  3. 上流ISP、ピア先と調整
  4. ルータへ設定→経路広告開始
  5. ある程度の時間待つ（インターネット全体へ染み渡る）
  6. サーバ屋さん、後はお願いします
- **ハイジャック通知実験**
  - Telecom-ISAC Japan 経路奉行の検知結果をJPIRRユーザへ
    - JPIRRのユーザへ登録データをより正確にしていただきたい
      - 検知精度が高まる

IRRはどう効くか！！一つの例

- 先ほどのYoutube事件の例では、



ハイジャックASの近くで経路フィルタをかけていれば影響は小さかったはず

ハイジャック通知実験の状況

- **JPNICが割り当てたAS番号の数**
  - ≒500
  - JPIRRのユーザ数
    - ≒140
    - 通知実験へご参加いただいた組織数
      - 47組織
- **ハイジャック(が疑われる状態)の検知数**
  - 5月21日～7月3日の間
    - 47件
    - 4組織

通知を受けた事例　～行動編～

- **アラートを受けてどうしましたか？**
  - 対象アドレスがPIだったので何もしなかった
    - PIはお客さん自身で解決していただく
      - PAは責任を持って守りますが・・・
  - 対象アドレスが自分のPAだったので驚いた
    - いわゆるパンチングホール状態
    - アラートが継続するので自分で代理IRR登録
      - この対応でいいのかどうかはグレーゾーン
  - システムの動作を確認するため、自分でハイジャック実施
    - この手のシステムは動作確認が必要
    - 少々ドキドキした

通知を受けた事例 ～要望編～

- **通知実験に足りないもの・こうなるといいな**
  - やっぱり、ハイジャックをしたASも教えてほしい
    - 誤報であった可能性を考えると言いがかりになりかねず・・・
  - ハイジャック終了時も教えてほしい
    - システムの都合で出ない場合もあるんです
    - それでもよければ・・・
  - X―Keiro：の登録メールアドレスを隠してほしい
    - そんなに隠したいですか・・・
    - 実装がんばります
  - ハイジャック発生時の模範行動を示してほしい
    - 詳しい人がきっと会場に沢山！

今後の展望

- **経路ハイジャック通知実験の今後**
  - 実験参加ユーザを増やす（が疑われる状態の）
    - JPIRRユーザの登録更新意識を刺激
    ↓
    - JPIRRの正確度向上
    ↓
    - 正確度向上に伴い、経路奉行の検知精度も向上（↑に戻る）

- **JPIRRの目指す姿**
  - 経路制御品質安定化のため、より正確な台帳を目指します
    - 経路情報登録認可機構、経路ハイジャック通知実験、、、etc

ありがとうございました。

- 15分で話せなかったこともあります
  - –ホワイトボード
  - –懇親会
  - –直接ご意見
- お待ちしております！！

