

経路ハイジャック通知実験とJPIRR ～ お奉行様と1年 ～ IRS20

2009年5月21日 14時～17時

KDDI

谷津 航

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



本日の内容

■ 経路ハイジャック通知実験の状況

■ ちょうど去年の5月21日開始！

■ JPIRR近況報告

■ 1年の活動報告

■ 2009年の予定など

経路奉行さんとJPIRRの連携 ～ 1年がたちました～

経路奉行とJPIRR(おさらい)

- **連携の経緯**

経路奉行(経路ハイジャック検知システム)は参加ISPの経路とRADbの情報を比較していた

誤報が多いのでJPIRRにしてみたら結構うまくいった

JPIRRの情報をTelecom-ISACさんへ提供

2年くらいして、ハイジャック情報をJPIRRユーザへ還元

- **連携の内容**

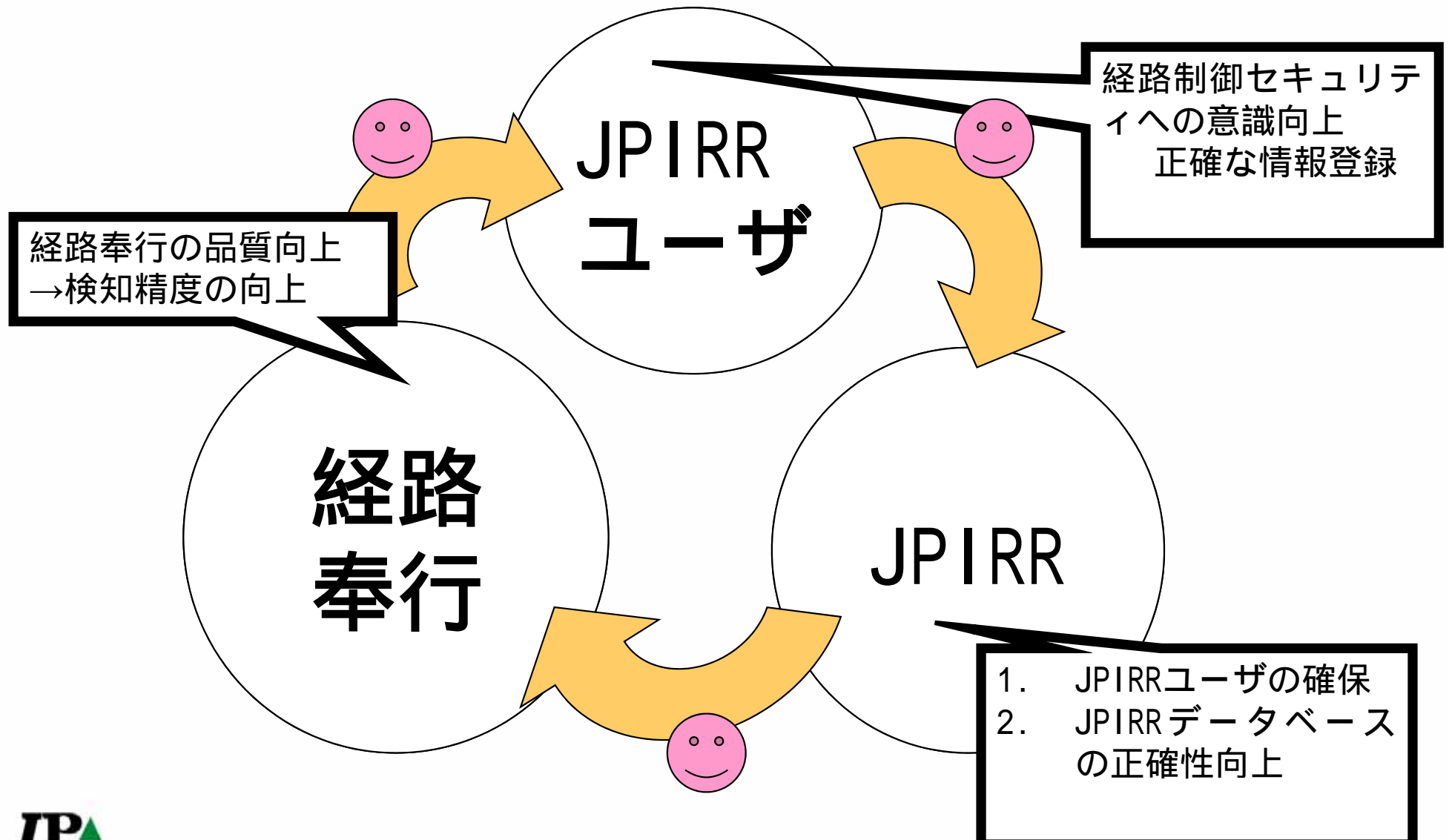
経路ハイジャック情報をJPIRRユーザへも通知

- 従来はTelecom-ISAC BGPWGメンバー内

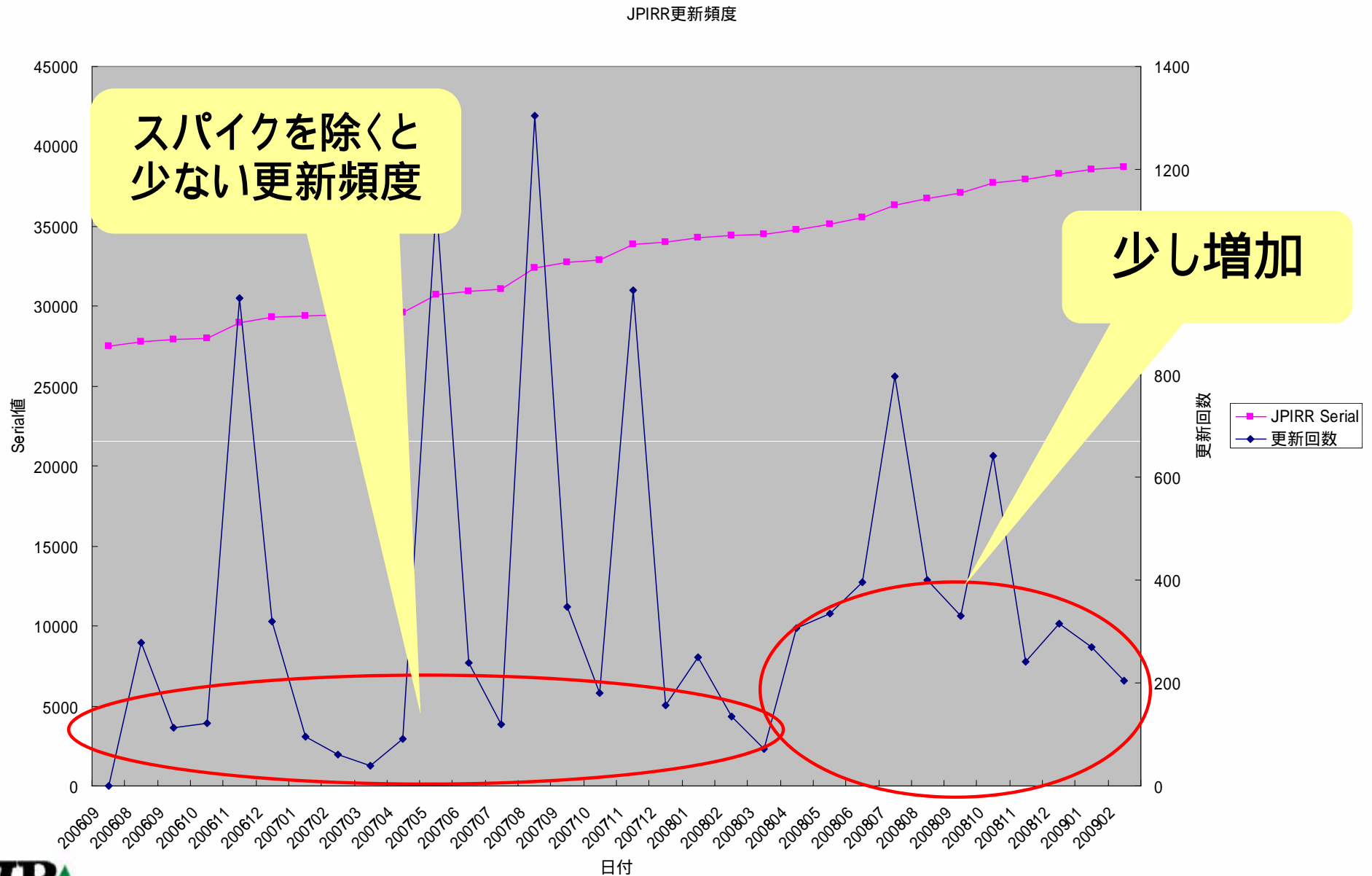
IRRのオブジェクトへX-Keiro:と書いてくれば通知！

連携実験の目的(と想定する相乗効果)

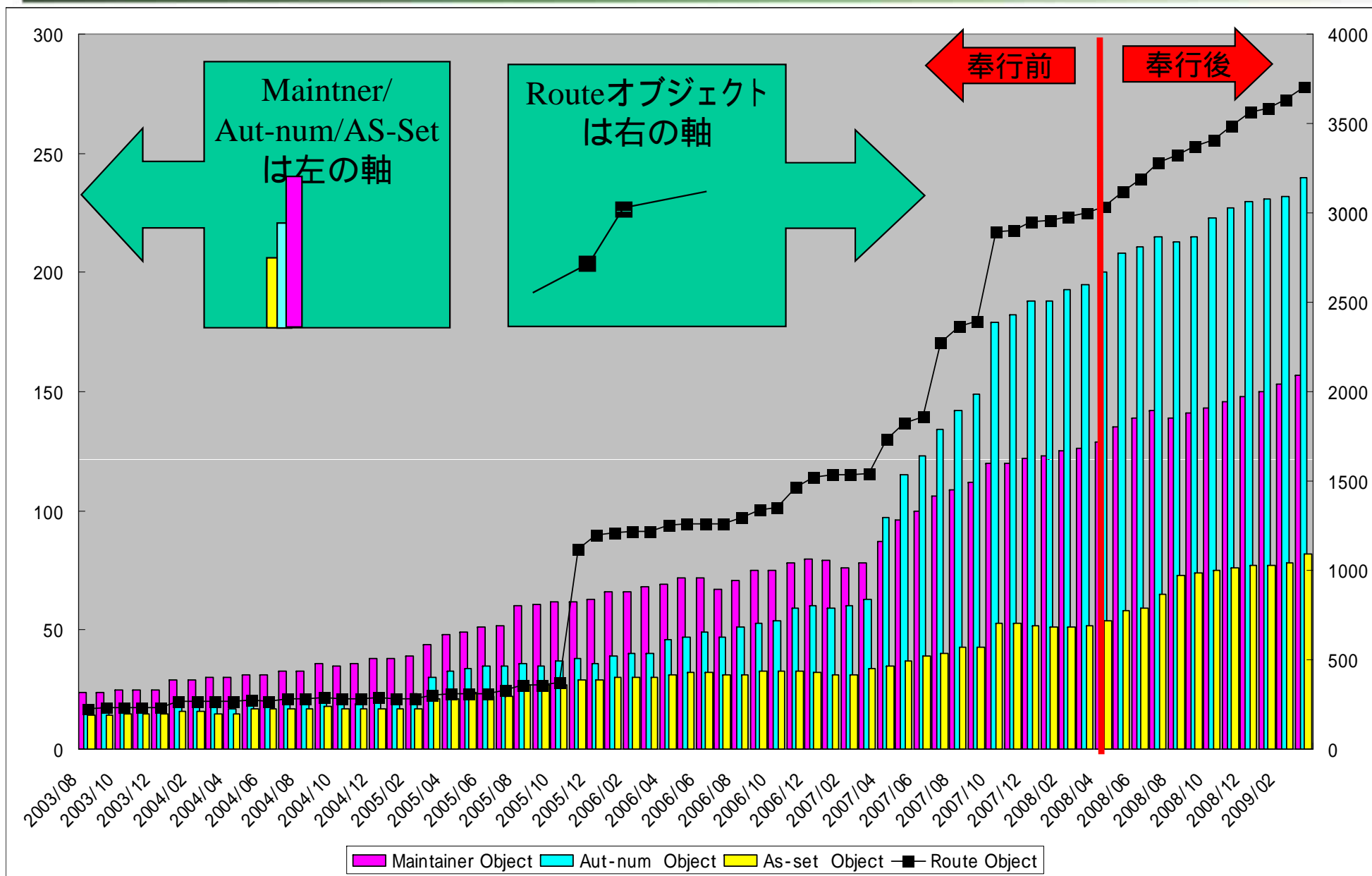
•持続的な3者にとって良好なサイクル



連携実験の効果 更新頻度



JPIRRの中身の成長の証・・・



現在の実験参加数

- **実験参加組織**

64組織

- **奉行からの通知数**

245件

- **JPIRRユーザへの通知数**

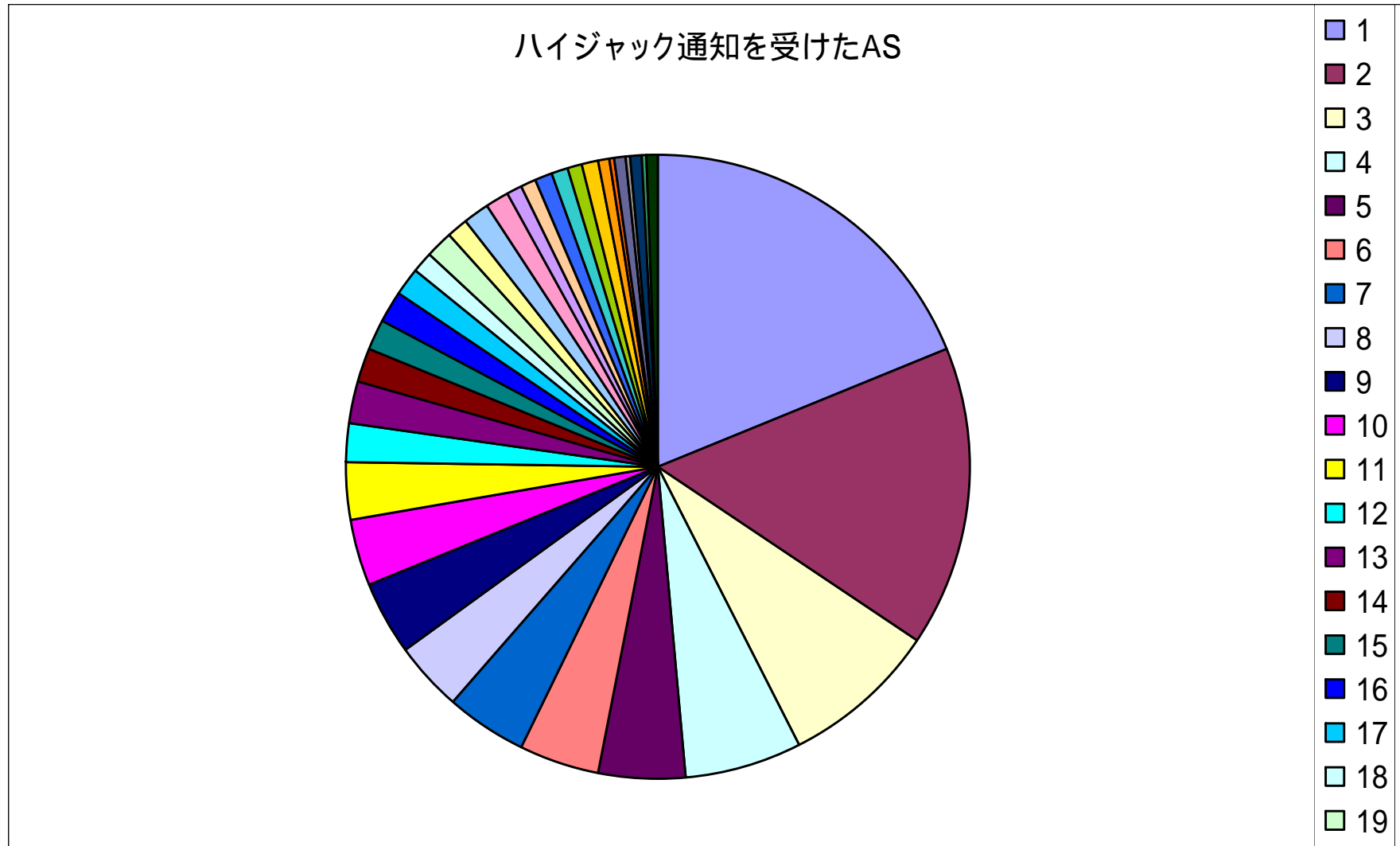
165件

- **アラートの傾向**

上位4ASが半分以上を占める

- いろいろがんばっても大変(某AS談)

ハイジャック通知を受けたASの分類



去年のJANOG (7月)以後の特殊例

- **疑われた状態が継続しているAS/Prefix**
このままでいいの??
- **大量警報**
数千の誤報
オペレーションによりシステム全体が停止する可能性
- **地球の裏側からの疑われる状態発生**
これは誤報ではなく、、、
本当にトラフィックが吸い込まれている???
BGPMONのようなRISアーカイブも監視する必要性?

2009年度の内容追加(予定)

- **Webの充実**

 - オペレータの心構えWeb公開予定

 - Telecom-ISAC Japan経路情報共有ワーキンググループの皆様と事例を議論し、まとめましたWeb

- **ハイジャック(が疑われる状態)終息通知**

 - 現在は、発生時にお知らせのみ

 - 終わりましたよ～という通知

- **その他(去年からの継続要望)**

 - X-Keiroの登録情報を隠します

 - 誤報ゼロ賞創設(?)

経路ハイジャックに対する ～ 経路ハイジャックに関する Web ～

経路ハイジャックが疑われる状態発生時の対応について - Microsoft Internet Explorer

ファイル(E) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)

アドレス(D) http://www.nic.ad.jp/ja/ip/irr/counter-hi-jack.html

申請ページTOP > JPIRR登録者・利用者向けページ

プリント用ページの表示

経路ハイジャックが疑われる状態発生時の対応について

2009年6月11日

はじめに

1. 検知 - 疑われる状態の発生 -
2. 情報の確認
 - 外部の経路情報確認サイトでの情報収集
3. 分析と対処
4. 留意事項
5. 平時の備え
 - 疑われる状態発生時の手順を整理

終わりに

はじめに

このページでは、経路ハイジャック通知実験への参加組織が、実際に経路ハイジャックが疑われた場合、どのようなケースや行動が存在するかを、実際の流れにあわせ、検知、情報確認、紹介します。

1. 検知 - 疑われる状態の発生 -

今回の経路ハイジャック通知実験では、疑われる状態が検知された段階で通知される仕組みで発生するわけではありません。そのため、通知を受けた場合、何をすべきか、自組織のASがどのようなから解析を行うことになります。

また、疑われる状態の通知を受けた時点でも、経路ハイジャックが短時間で終了している場合があります。このようなケースでは、通知を受

JPIRR近況報告



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

Copyright © 2009 Japan Network Information Center

JPIRR近況報告

- 現状報告と他のIRRとの比較
- asplainな話
- AS-SETオブジェクトな話
- 2009年度の予定

JPIRR現状

- **世界第5位のIRR**

メンテナーオブジェクトベース、某社団法人調べによる
母数はRADb中のIRRs = 40

- **海外ISPからのミラー希望が増加**

- **国内ミラーも増加**

JPIXさんへのJPIRR情報提供一方向ミラー開始

asplain

- **asplainサポート機能**

 - デフォルトがasplainへ

 - 先月公開のirrd-2.3.9を検証中

 - 合わせて、!gクエリのv6対応なども検証中

- **参考: JPNIC WHOIS**

 - JPIRRとは直接関係ありませんが、、、

 - 2009年度中にasplainでの登録検索を追加予定

 - デフォルト表示もasplainを予定

 - 今は4 octet AS番号はasdot

AS-SET

- 2008年7月7日以後

登録と検索が増

- 特にAS SETが1.3倍

JPIRR以外のIRRでは特に上記傾向は見えず

七夕 松崎さん宣言の影響(?)

- 検索

固定客の定期的なクエリが発生

ピアリングで利用されている(?)

利用方法のサーベイ・ヒアリングの際にはよろしくお願いします。

2009年の予定

- **オブジェクトお知らせ便**

今まで: ガーベージコレクタを運用

- 今までは、オブジェクト放置対策を実施
- 1年更新期限以後、放置オブジェクトを削除

これから: オブジェクトお知らせ便

- 定期的に、Routeオブジェクト保持者へJPIRR中に登録されたOrigin ASを通知、問題ないか確認
- ASお知らせ便は調整中

- **経路情報の登録認可機構**

今年も継続中

JPNIC木村が進めております

ありがとうございました。

- 質問・コメント・お願いします。
JPIRRです。

