Internet Week 2009

H10 一歩進める

インターネットルーティングセキュリティ

第二部：14：50～15：40

インターネットルーティングセキュリティに関する取り組みと関連事例の紹介

財団法人日本データ通信協会 Telecom-ISAC Japan

インターネットマルチフィード株式会社 渡辺 英一郎

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 岡田 雅之

NTTコミュニケーションズ株式会社 吉田 友哉

JPNIC 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 © 2008 Japan Network Information Center

第二部：取り組みと関連事例の紹介 アジェンダ

- 岡田
  - 今効くIRR「経路台帳を取り巻く現状と課題」
    - ルーティングセキュリティの維持をサポートする、経路台帳の今を説明します。
- 渡辺
  - 経路奉行 ～ 日本国内での経路ハイジャック検知 ～
    - 日本国内で経路ハイジャック検出を継続して行っている経路奉行について成果と課題をお知らせします。
- 吉田
  - 2009年 BGP属性問題に関わるインシデントの解説
    - 経路ハイジャックとは性質の異なる、2009年度に発生したルーティング上の問題について深く説明します。

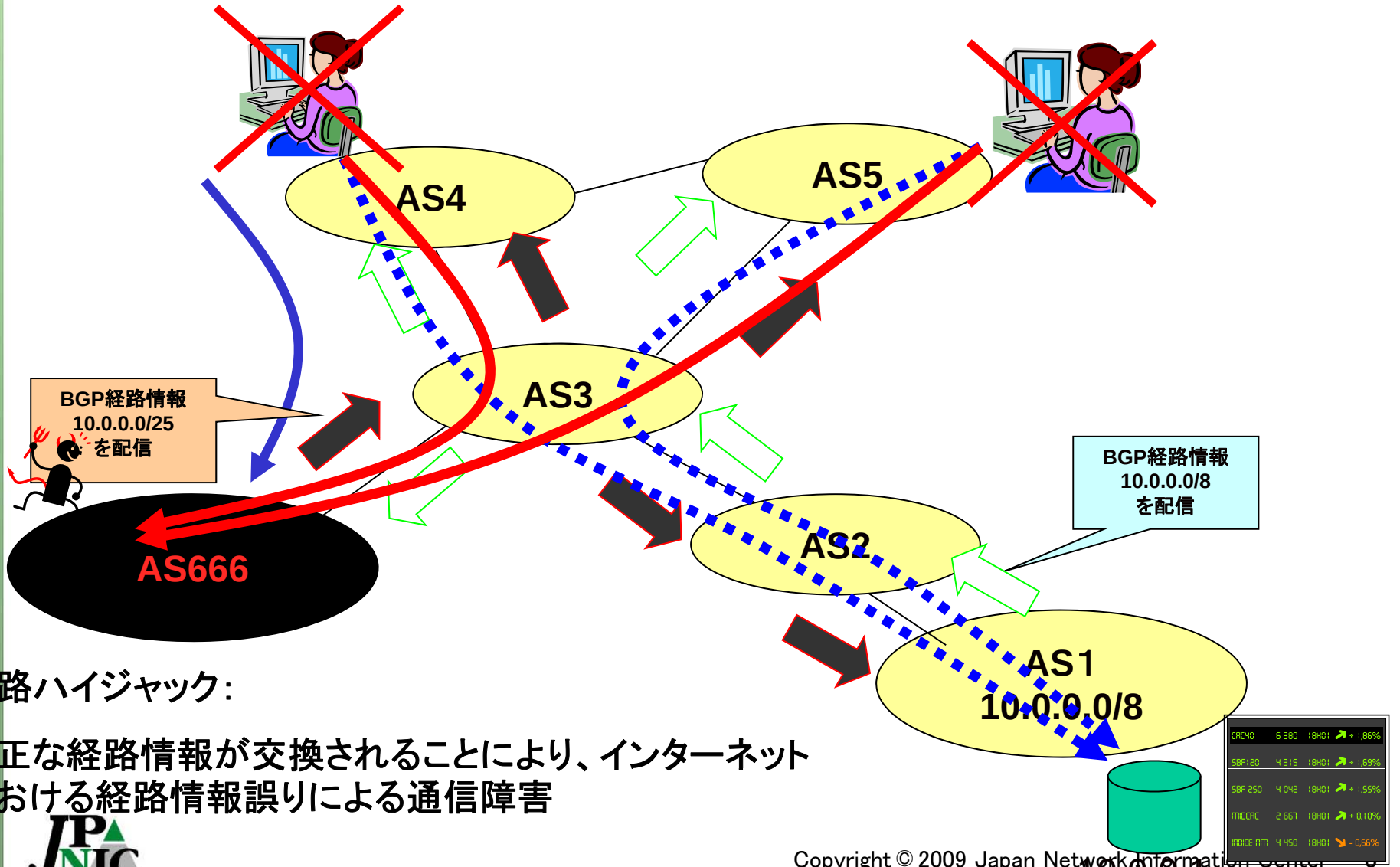
Copyright © 2009 Japan Network Information Center

第二部：前半 経路ハイジャックとIRR

- 経路ハイジャックを中心に現在の取り組みを解説
  - インターネットルーティングを脅かす脅威の一つ
  - 特に、日本国内の取り組みである経路奉行について
- 経路ハイジャックを検出するための台帳
  - 台帳の一つとしてIRR（Internet Routing Registry）
- 経路ハイジャックの簡単なおさらいと、検出の現状
  - 経路奉行＝日本の経路ハイジャック検知システム
  - 検知システムをサポートするIRRのできることと課題

Copyright © 2009 Japan Network Information Center

経路ハイジャックとは



経路ハイジャック:

不正な経路情報が交換されることにより、インターネットにおける経路情報誤りによる通信障害

Copyright © 2009 Japan Network Information Center

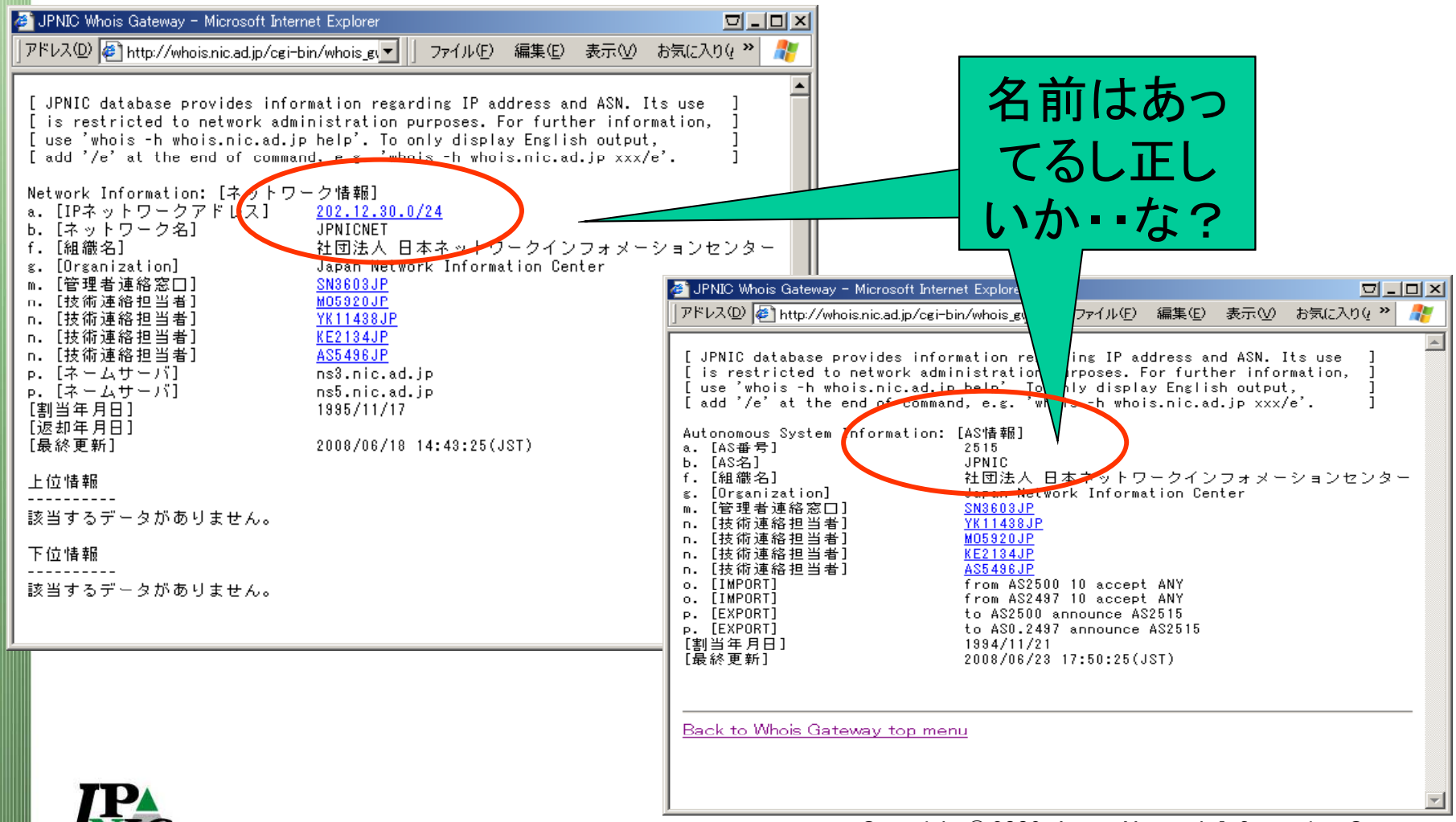
経路ハイジャックかどうか、調べたい。〇〇のASへ連絡したい。。。

- 経路の台帳=Internet Routing Registryがあります！
- 経路情報（IPアドレスとAS番号の組合せ）の台帳
  - WHOISの情報だけを使ってIPアドレスとAS番号の組合せを調査することは難しい(不可能ではない)
- IRRの使い方
  - AS運用者が登録します。
    - アドレス取得後、経路広告元のOriginASを登録
    - どこかのIRRへ登録しないと、通信できないネットワークも存在します。
  - AS運用者が参照します。
    - IRRを参照して、受け入れる経路の取捨選択をしているネットワークが存在します。
    - トラブル発生時の連絡先のデータベースとしても利用します。

Copyright © 2009 Japan Network Information Center

何故IRRが必要か
～ もしもWHOISしかなかったら ◎～

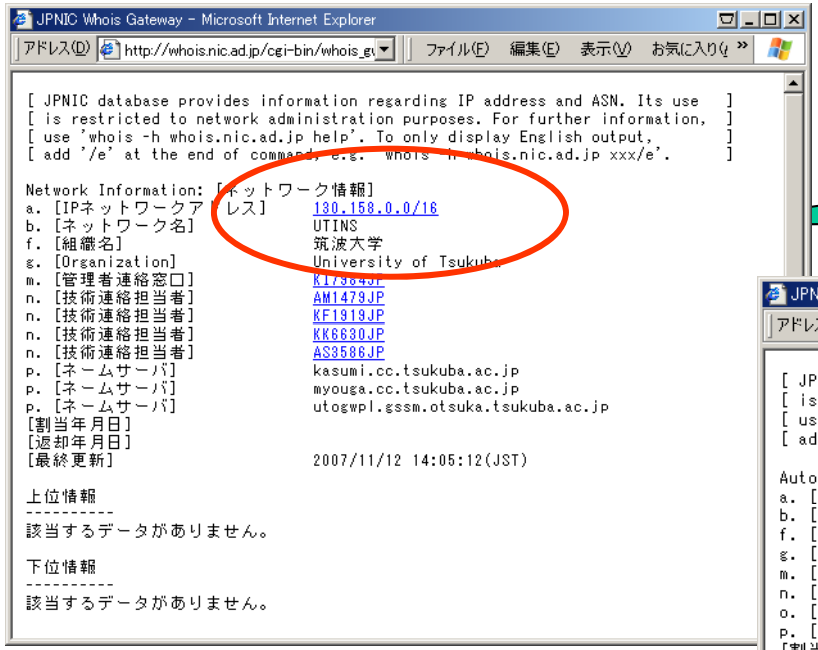
- 202.12.30.0/24の経路 Origin AS2515 正しいか？



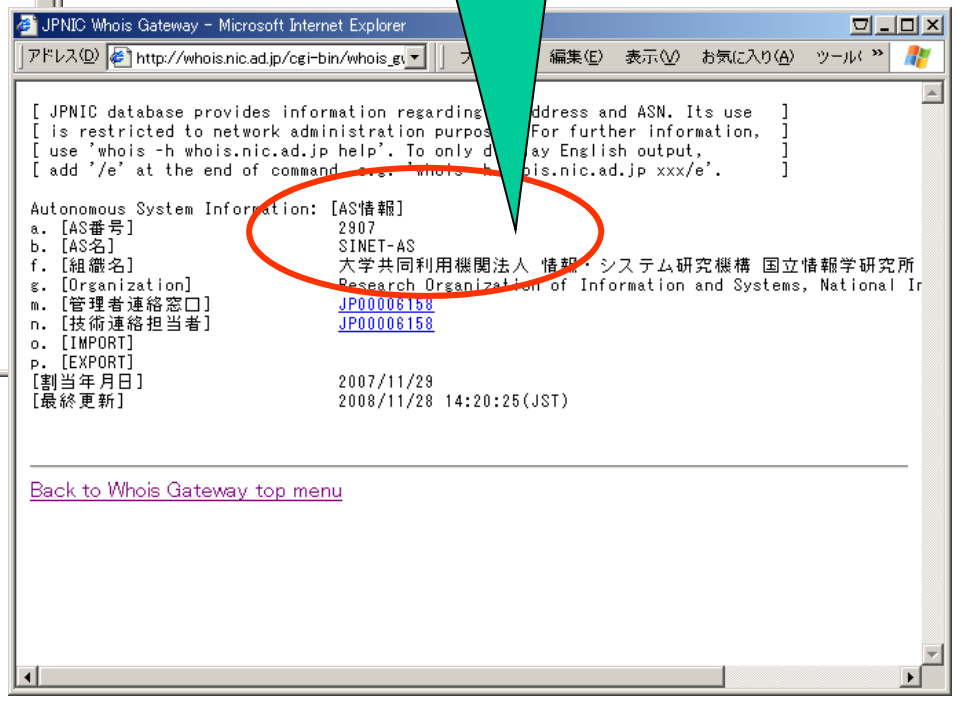
Copyright © 2009 Japan Network Information Center

何故IRRが必要か
～ もしもWHOISしかなかったら ▲～

- 130.158.0.0/16の経路 Origin AS2907 正しいか？



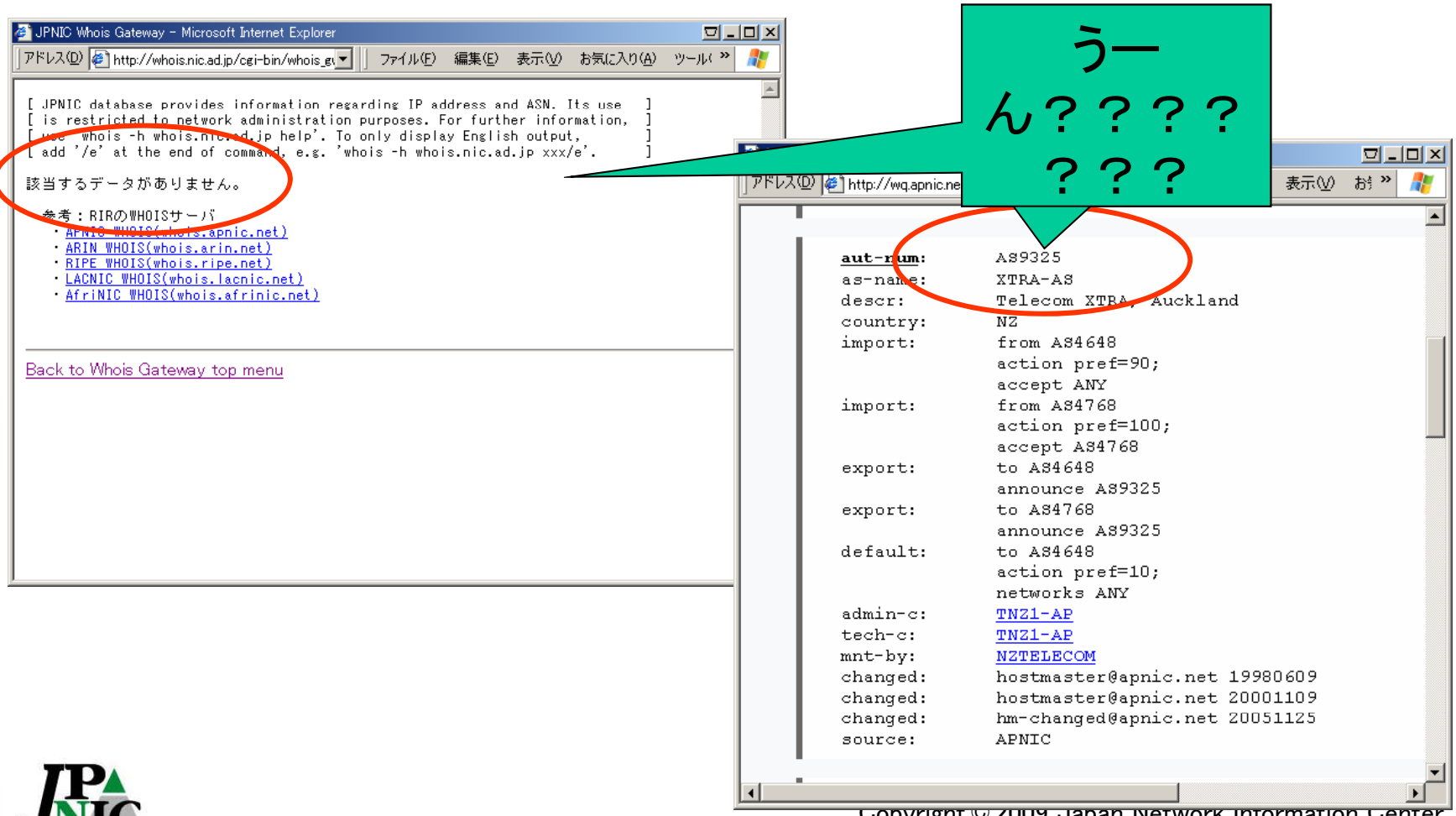
学術系だから・・正しいか・・な？



Copyright © 2009 Japan Network Information Center

何故IRRが必要か
～ もしもWHOISしかなかったら ×～

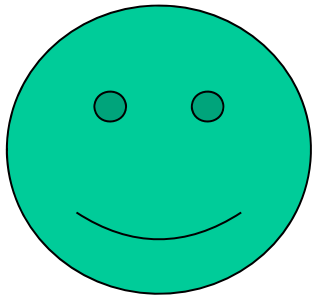
- 202.26.31.0/24の経路 Origin AS9325 正しいか？



Copyright © 2009 Japan Network Information Center

何故IRRが必要か
～ IRR登場　～ 先ほどの結果をIRRで見る

- 202.12.30.0/24 OriginAS 2515



route:　202.12.30.0/24

descr:　JPNICNET
Japan Network Information Center
Kokusai Kogyo Kanda Bldg. 6F
2-3-4 Uchi-Kanda
Chiyoda-ku, Tokyo 101-0047
JAPAN

origin:　AS2515

admin-c:　SN3603JP
tech-c:　YK11438JP
tech-c:　MO5920JP
notify:　system@nic.ad.jp
mnt-by:　MAINT-AS2515
changed:　apnic-ftp@nic.ad.jp 20090618
source:　JPIRR

あれれれれ？

- 202.26.31.0/24 Origin AS9325

route:　202.26.31.0/24

descr:　Proxy-registered route object

origin:　AS4648

notify:　noc@netgate.net.nz
remarks:　This route-object is created on behalf of
remarks:　Telecom New Zeland customers, and is used for
remarks:　route filtering at border routers.
remarks:
remarks:　If you have any inquiries, please contact noc@netgate.net.nz
mnt-by:　MAINT-AS4648
changed:　bart@netgate.net.nz 20050627
source:　RADB

アドレス利用時のAS番号を確認！

Copyright © 2009 Japan Network Information Center

202.26.31.0/24 Origin AS9325は一体？

To: noc@netgate.net.nz

202.26.31.0/24 Origin AS9325この経路おかしくない？

とIRRの結果を貼り付けてメール

To: JPNICの岡田さん

From: ろぶ

Greetings,

I do apologise. This range was ass
customers in the past, and was m
their service was removed.

It has been removed now.

Rob.

意訳:
やぁ、岡田さん。
NZのロブです。

いや一昔の顧客の設定が
残ってたんだ。
削除したよ。
ハッハッハ！

元々日本のアドレスがNZから広報されるのが怪しい・・・

APNICの割振りリストでは↓

.

apnic|JP|ipv4|202.26.0.0|65536|19950329|allocated

apnic|NZ|ipv4|202.27.0.0|2048 |19940304|allocated

.

Copyright © 2009 Japan Network Information Center

簡単なIRRのまとめ

- IPアドレスを利用する人がAS番号を宣言する場所
- AS運用者が自分の子供ASを宣言する場所
- その他、連絡窓口なども記入可能
- IRRを参照して、アドレスの制限をするASが存在
- 「宣言」する場所なので、叫んだもの勝ち
  - 宣言（＝IRR登録）自体が間違う可能性もあり

Copyright © 2009 Japan Network Information Center

現在考えられる経路ハイジャック対策

- IRRなどによる経路フィルタリング
  - AS-PATH・Prefix-Filtering
- Secure-BGPs(S-BGP、so-BGP、ps-BGP,etc)
  - 2009年現在、実装が見えません
- 経路情報の監視による検知
  - 世界でさまざまなプロジェクトが存在
  - ルーティングセキュリティを脅かす、経路ハイジャックの検知が不完全ながらもできるようになってきた
- 経路ハイジャック発生後の対策
  - ？？？

JPNIC

Copyright © 2009 Japan Network Information Center

経路ハイジャック検知システムの比較

	ISAlarm	BGPmon	IAR	Cyclops	経路奉行
監視している経路の情報源	RIPE-RIS	RIPE-RIS route-view	RIPE-RIS route-view 運営者の経路	RIPE-RIS route-view abilene PCH その他	日本ISP
ハイジャック検知方法	ユーザ入力情報との比較	ユーザ入力情報との比較 IRRとの比較	ユーザ入力情報との比較 IRRとの比較 新規AS経路の隔離	ユーザ入力情報との比較 IRRとの比較	IRRとの比較
通知方法	Web メール SYSLOG	Web/RSS メール	Web メール	Web	メール
監視BGPピア数	9拠点95	15拠点175	15拠点175	80拠点250	15
特徴	RIPENCC 運営・老舗	活動活発 Blogがよい	経路一見さんお断り方式	細かい状態監視が可能	活動活発 日本周辺情報

Copyright © 2009 Japan Network Information Center

経路ハイジャック検出システムの仕組み

- 世界の経路ハイジャック検知システム同じ仕組み
  - インターネットの経路情報を収集
    - BGPのUpdateとWithDrawnパケットを収集
    - 経路情報は、独自に収集した情報と、経路情報収集公開サイト：RIPE-RIS、Route-Views、そのほかを利用
  - 何らかのデータベースと経路をつき合わせ
    - IRRや、あらかじめ登録したAS/IPアドレスの組あわせ
    - 新規で経路広告されたアドレスを隔離する仕組みもあります
  - サイトごとの基準で検出した異常を通知
    - Webや電子メール・SYSLOGによる検知報告
    - RSSなどによる配信もアリ

Copyright © 2009 Japan Network Information Center

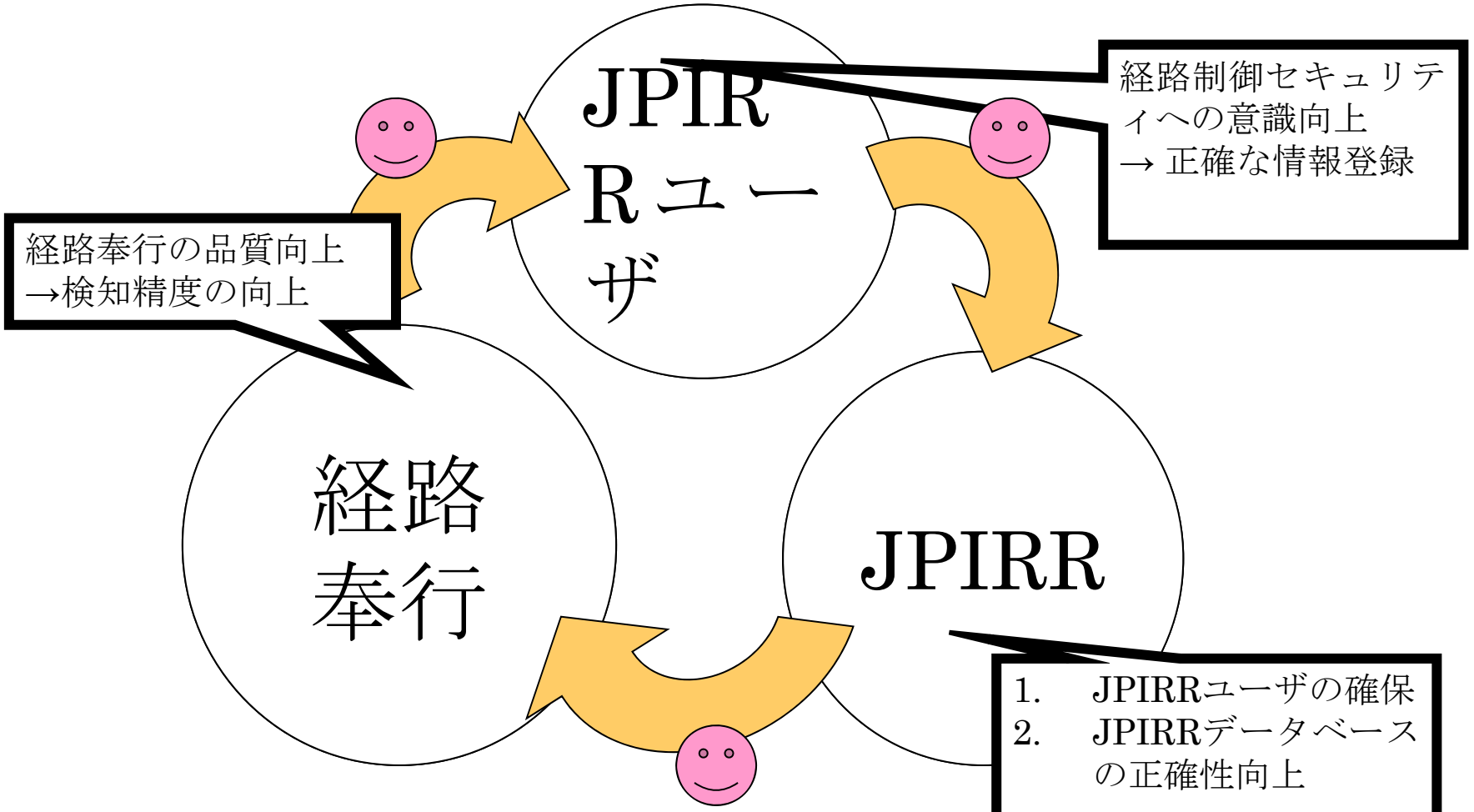
日本国内の取り組み：経路奉行とJPIRR

- 経路奉行による経路ハイジャック検知
  - JPNIC運営のJPIRRの情報と経路奉行参加組織の経路を比較
  - 日本周辺地域を主対象とした唯一のシステム
- JPIRRは、みんなでIRRの情報を正確にして、経路奉行の検知精度を高めることで寄与したい
  - 経路奉行の検出結果をIRRユーザへ提供
    - 仮説：悪意の無い、経路ハイジャックをIRRの登録漏れとする
    - 狙い：仮説の登録漏れをユーザへ通知し、データ更新を促す
  - IRRデータの正確性向上に向け、よいサイクルができると期待

Copyright © 2009 Japan Network Information Center

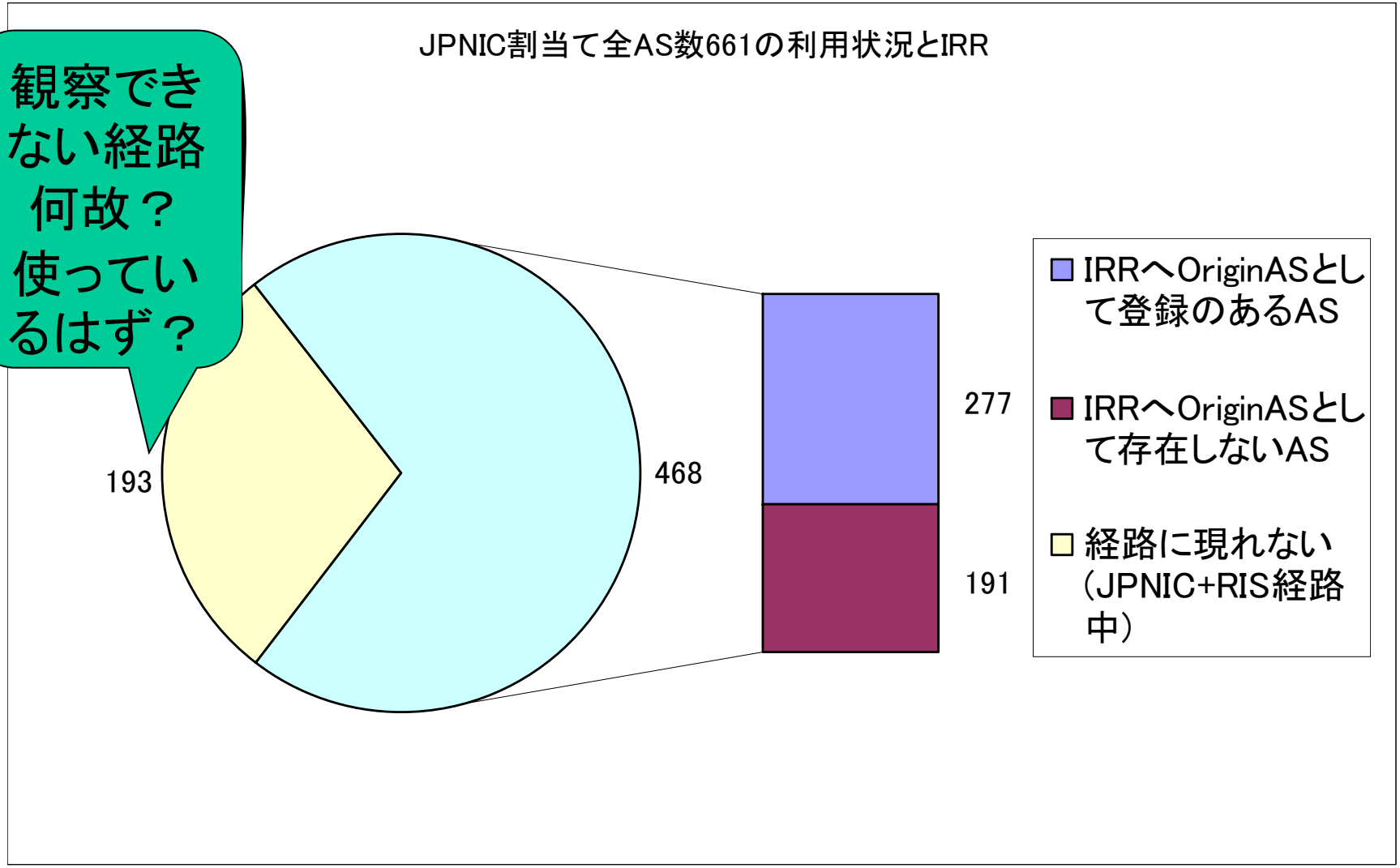
みんなで良好なサイクルを作りたい
経路奉行渡辺さんよろしくおねがいします

- 持続的な3者にとって良好なサイクル



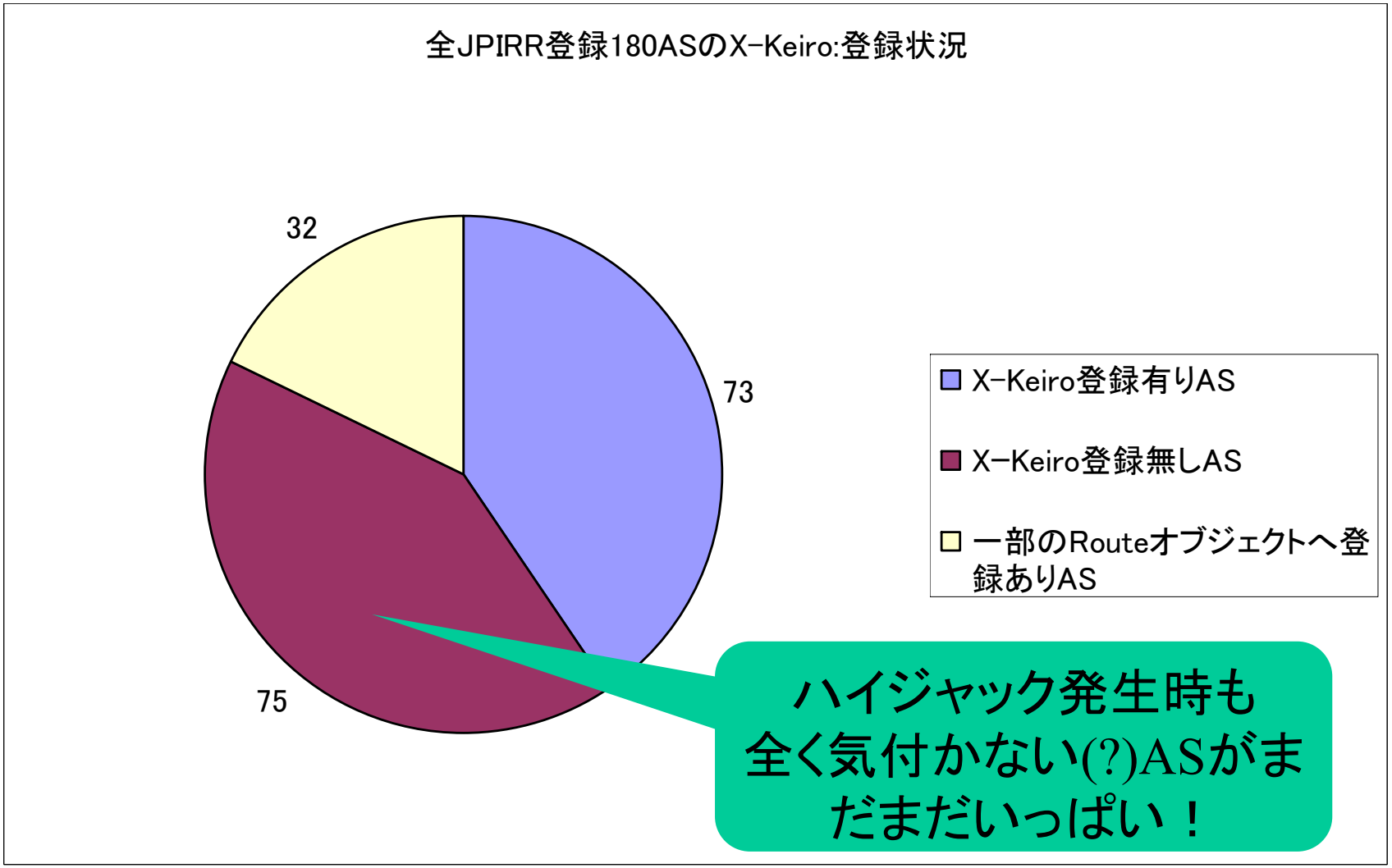
Copyright © 2009 Japan Network Information Center

ハイジャック通知実験、現状



Copyright © 2009 Japan Network Information Center

通知実験単体の状況



Copyright © 2009 Japan Network Information Center

最後に：IRRをさらによくするために

- **IRR登録情報の正確性**
  - レジストリの割り振り/割り当て情報と別個
  - アドレスをどのOrigin ASで広報するかは運用者の頭の中
    - レジストリで制限する仕組みを作っても自発的な登録が必要
- **フルルートへのフィルタは不可能**
  - Prefix Filter 30万行書けますか？
  - 末端ASで経路吸い上げ時にフィルタかければ解決！
- **Proxy Registeredの問題**
  - 経路が先か、IRRが先か
  - 流れている経路を勝手に登録するIRRの存在
    - 鶏が先か、卵が先か
- **これからもみなさんの協力が必要です！**

JPNIC

Copyright © 2009 Japan Network Information Center