WG3-6

事業者間での障害連鎖などに関する対策例 ～IRRの活用など～

2004年3月10日

日本インターネットエクスチェンジ株式会社

jpix

事業者間をまたがる障害の例

- 経路情報が原因の世界的なインターネットの停止
  - 1997年4月　AS7007からの大量の経路情報の逆流
  - 1997年10月　UUNET (AS701) からの大量の経路情報の広報
- 経路情報が原因の日本国内での大規模な障害
  - 1994〜95年　NSPIXPにおける誤った (大量の) 国際経路の広報→ルータの過負荷
  - 2000年9月　ISPから誤ったピアリングに必要なIX経路の広報→ピアリングの停止
  - 2002年1月　ISPからの誤った (大量の) 国際経路の広報

- DDoS攻撃
  - 1997年 Smurfing
    - Routerの工場出荷時設定の不備をついた攻撃
  - 2001年〜 Yahoo、Microsoft
    - 特定の有名サイトをねらったDoS攻撃
  - 2002年10月 Root-servers.net
    - インターネットの名前サービスDNSの根幹の13台をねらった流行
  - 2003年 ウィルス・ワーム
    - メールやセキュリティホールをついたワームの大流行 (Nimda、MyDoom) → トラフィックの異常増加
    - 韓国のインターネットの大規模な停止 (SQLslammer)

障害の傾向と対策

- 傾向
  - 悪意ある第三者のDoS攻撃の増加
  - 大規模なルーティング・メルトダウンは最近では起こっていない
  - ルーティングの障害は、多くのISPを巻き込む大規模な停止となる
  - ルーティングが障害の原因の多くは、バグや運用者のミスが原因のものが多い
- 緊急障害時の対策
  - 緊急時のISP間の連絡は、個人間の人間関係の繋がり（携帯電話）により行われている
  - NANOG、JANOGなどのメーリング・リストによる情報交換
  - 緊急遮断（ピアリング停止）やポートフィルタリングの実施
- 対策：緊急時の接続解除など
  - 接続解除（ピアリング停止）は実施しにくい
    - 正常か？異常か？の判断が困難
    - 正常なトラフィックも同時に止めてしまうことによる運用者の躊躇
    - サービス提供側は、約款に記述があったとしても、営業的な配慮が働く
  - 緊急ポート・フィルタリングによる攻撃からの防御
    - SQL SlammerのDoSの際に実施例あり
    - IABは、ISPが常時フィルタリングを行うことに対する反対意見を表明

障害の傾向と対策（つづき）

- 対策：自社網の強化
  - ルータの設定のチューニング
    - 重要な経路情報を受け付けない設定
  - 過負荷に耐えられるルータの導入
    - メモリーを大量につんで高速のCPUを持つルータ
  - 運用の強化：（例）Routing Registry（RR）の活用
    - 自社用RRによる経路情報のフィルタリング（MCIなど）
- 対策：ISP間の協調
  - Network Operators Group（NANOG・JANOG）や、IXユーザ・ミーティングでのノウハウの技術交流（ルータのお勧め設定の啓蒙など）
  - Ingress・egressでのフィルタリングによる、攻撃パケットの流入停止
  - 国際連携の必要
    - トラブルは国境（インターネットにはそもそもない？）を越える
    - 発展途上国の技術力の底上げなどのケアも必要
- 対策：その他
  - 運用からのフィードバック：ルータなどの工場出荷設定の品質向上

インターネットと事業者間の協調

- インターネット＝発展をつづけるオープンで相互接続された網
  - メリット
    - さまざまなサービスやコンテンツが生まれるワークベンチ
  - デメリット
    - 相手を信用するモデル＝悪意に対して無防備
    - さまざまなタイプの障害が起こりうる＝予期不可能
  - 運用による解決
    - もぐらたたき的対策の連続
- ユーザにとってのインターネット･サービス
  - クオリティ
    ＝自社網のクオリティ ＋ 他社網のクオリティ
  - セキュリティ
    ＝Your Security is My Security. といわれる世界
- 対策の肝
  - ***自社努力も重要だが、ISP間の協調も重要***
  - エンドユーザのサイトのセキュリティの向上も必要

事業者間の協調

- ISP間のコーディネーションの成功例
  - NANOG・JANOG
    - {North America・JApan} Network Operators Group
    - メーリング・リストと年2～3回のミーティングの開催
    - ノウハウの技術情報の交流が目的
  - JPCERT/CC
    - セキュリティ情報の蓄積
    - 世界的には、数十のCSIRTがある
    - 日本では、JPCERT/CC
  - 2000年問題対策チーム
    - IAJ Y2K-TFを中心に ISPs のエンジニアにより構成
    - Y2K NOC（大手町）を運用
    - 「大きな問題は発生しなかった」のが成果
  - そもそも、インターネットが動き続けていることが協調の成果

経路情報とその正当性

- 経路情報の障害
  - 影響範囲大
    - 接続性そのものが影響をうけるので、経路情報にかかわる障害は被害が大きい
    - ミスを防ぐための***技術的な仕組み***が必要
  - 正当性の問題
    - ルーティング (BGP4) ：隣人が信じている隣人 (第三者) を信用するプロトコル ⇔ 悪意・ミスには無防備
    - 経路情報は、AS IS
    - ⇔ 裏づけの欠如
    - 経路情報が正しいのか、正しくないのか、判断の根拠がない (広報元のAS、マルチホーム、パンチングホール、運用ミスなど)
- 経路情報の正当性チェックの取り組み
  - DNSによる認証
    - Ciscoなどから提案 → 実現せず
  - BGP4プロトコルの改良
    - 経路に署名をつける → プロトコルが重過ぎる → 実現せず
  - IRRを使った認証
    - 実績：運用され続けている

経路情報の信頼性向上に向けて

- JPIXの取り組み：IRRとルート・サーバ
  - 目的：
    - 顧客が IX で交換している経路情報の信頼性の向上をサポート
  - システム：
    - ルートサーバで受信した顧客の経路とIRRのデータと比較

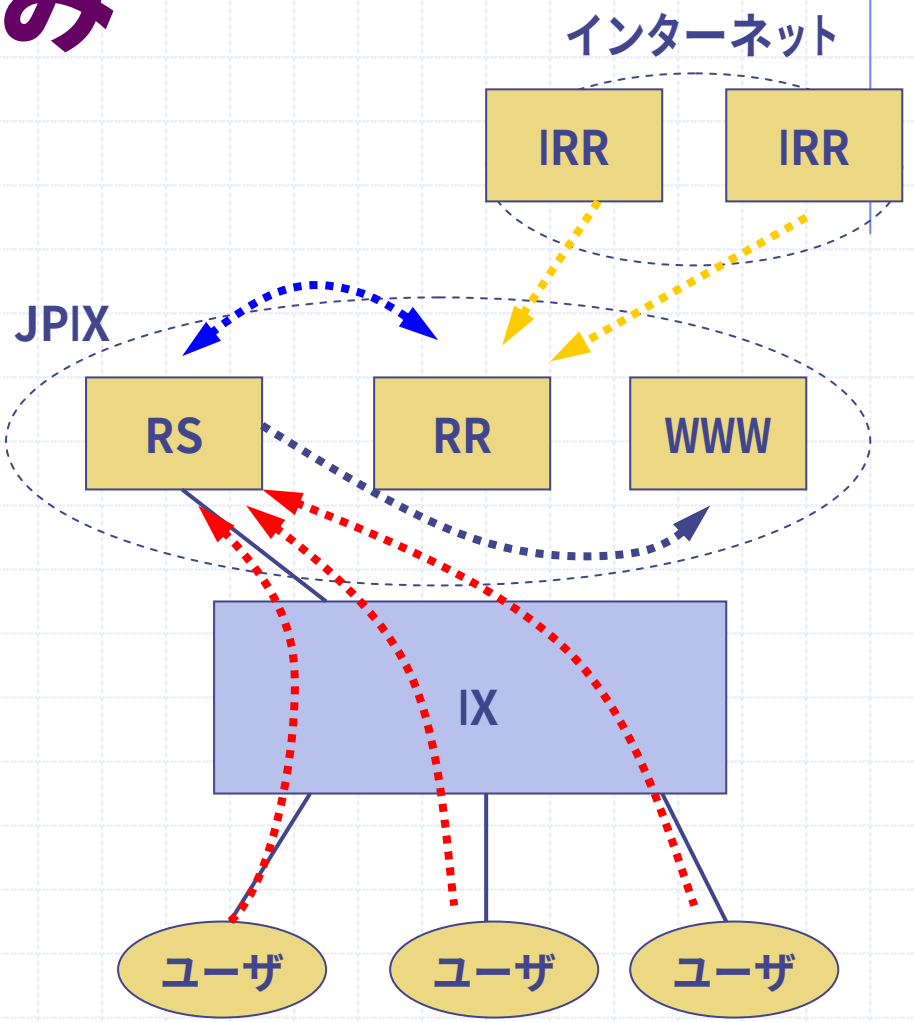
→ **交換される経路情報の品質管理が重要**

- IRR (Internet Routing Registry)
  - 経路情報のデータベース
    (運用者、AS情報、経路情報などを登録)
  - MeritのRAプロジェクト (RADB) が有名
  - 1999年のRADBが登録を有料化した後、小規模のIRRが乱立
  - RIRの階層を利用した運用が提案されている
    - RIPE、APNIC、JPNICでは、すでに運用を開始

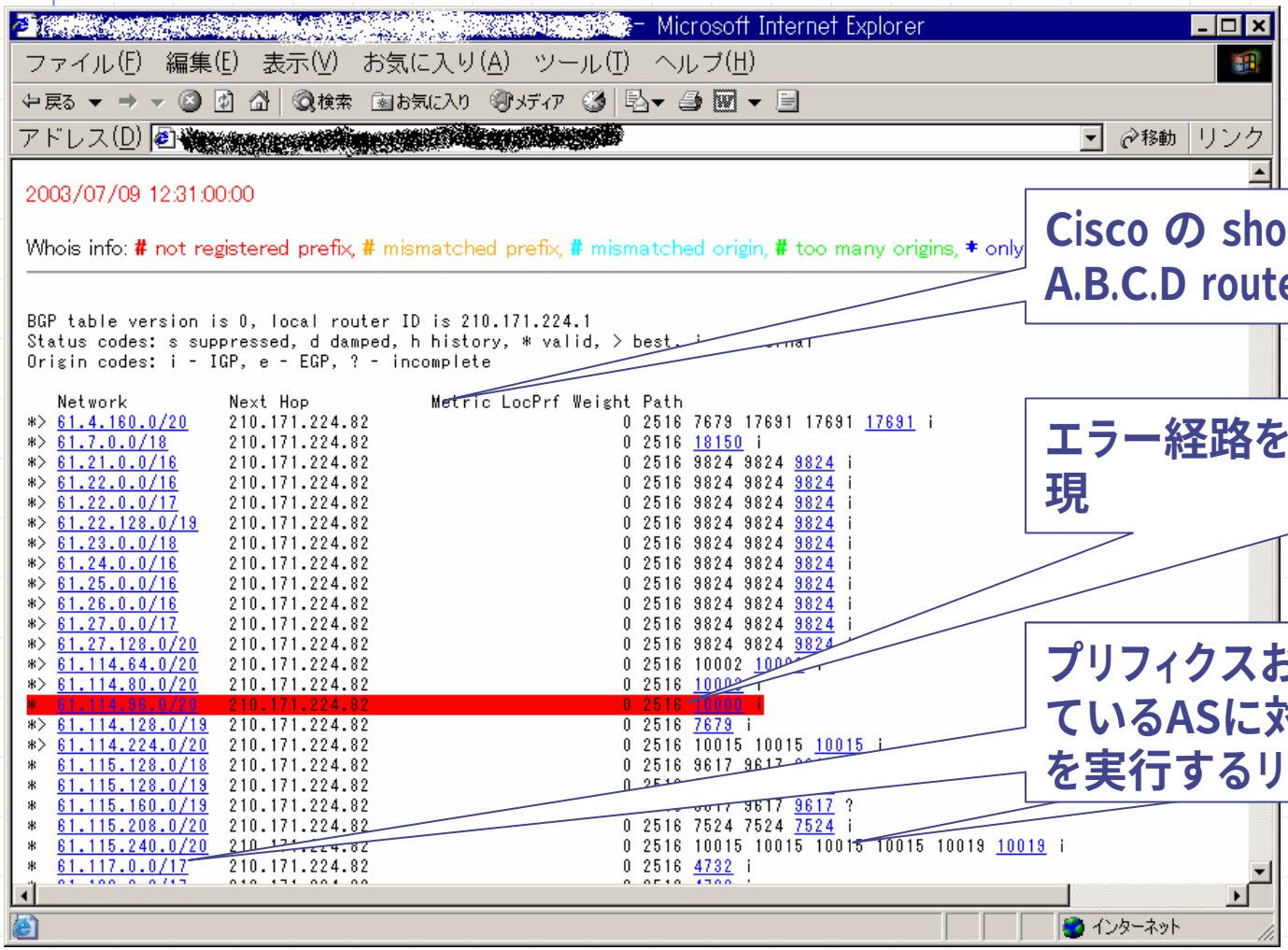
経路確認の仕組み

- IRRに登録されている正しい(と思われる)経路情報をRRにコピー
- RSはユーザのルータとBGPピアを張り、経路情報を受信
- RSで受信した経路とRR上の経路情報とを比較

- 比較した結果をWebサイトにてユーザに提供



経路確認のインタフェース(1)

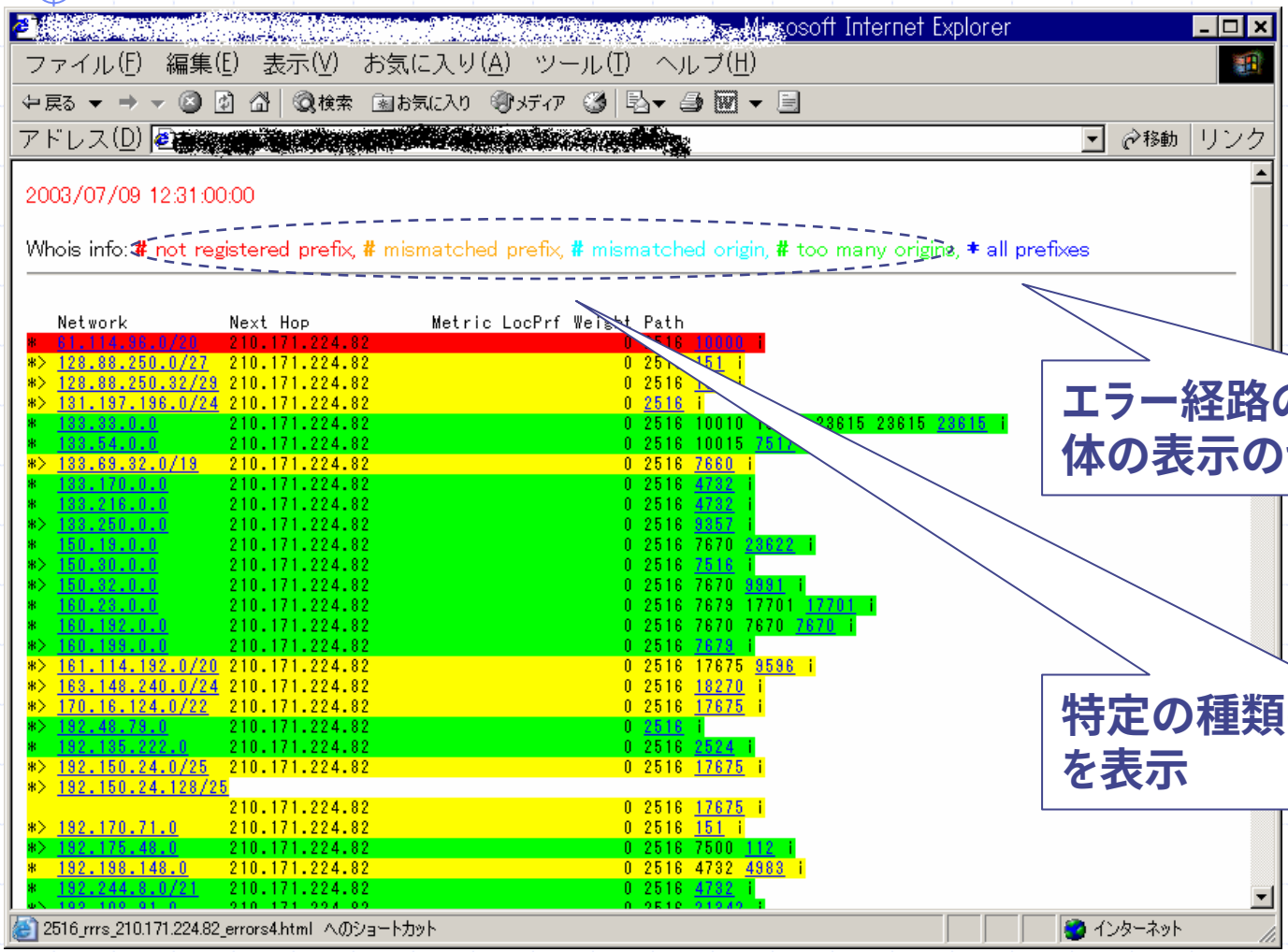


Cisco の show ip bgp neighbor A.B.C.D routes を模した画面

エラー経路を背景色を変えて表現

プリフィクスおよびオリジネートしているASに対する whois クエリを実行するリンク

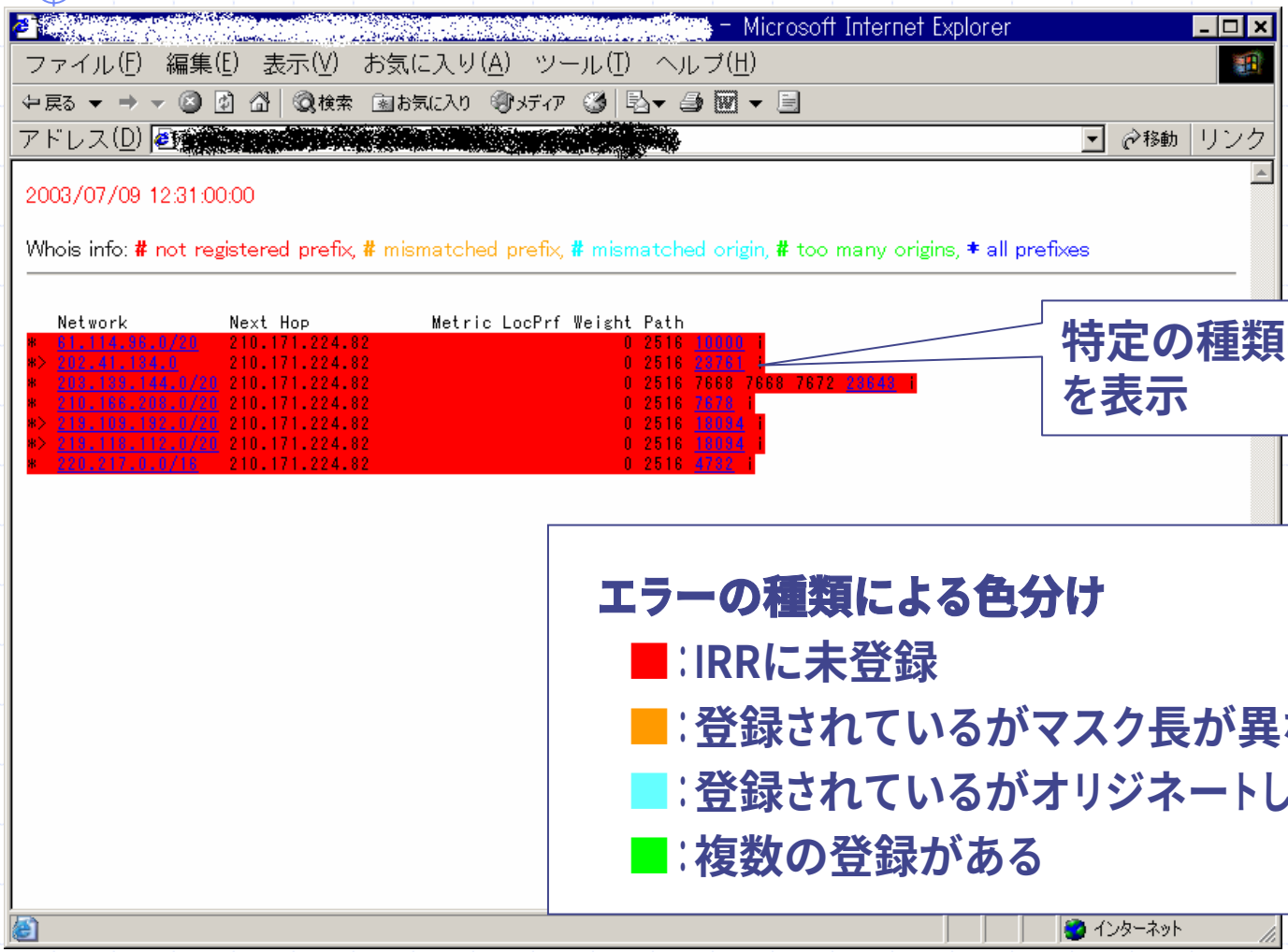
経路確認のインタフェース(2)



エラー経路のみの表示と経路全体の表示の切替

特定の種類のエラー経路のみを表示

経路確認のインタフェース(3)



特定の種類のエラー経路のみを表示

エラーの種類による色分け

- ■：IRRに未登録
- ■：登録されているがマスク長が異なる
- ■：登録されているがオリジネートしているASが異なる
- ■：複数の登録がある

IRRとルートサーバによる経路情報確認サービスを導入して

- 現在JPIXユーザの約1/3が利用中。
- 「経路情報の正確性を確認する仕組み」、というより「経路情報がIRRに登録されていること」、あるいは「IRRに登録されている内容を確認する仕組み」、として活用されている。

- 今後の課題
  - ユーザの利用率向上
    - カバー率が高くないと運用時に信頼できない
  - IRRのデータベースの信頼性（メンテナンス）が重要
    - データベースの内容が信頼をおけるものにするためには？せめて、国内ASだけでも → JPIRRへの期待
  - RADB有料化以後の問題
    - 世界的な分散の進行に対しては、国際協調による対応

まとめ

- IRRとルート･サーバによる経路確認の仕組みは一定の効果はあげていると思われる。
  - 障害時の経路情報のトラブルシューティング目的というより、安定運用時の品質チェックに効力を発揮。
  - IRRのデータの信頼性などの本質的な問題は残る。
- 障害の防止･障害発生時の対策において、事業者間の連携、情報共有は不可欠。
  - 国内の事業者の連携は、草の根的な活動にささえられている。
- エンジニアの交流･情報交換がインターネット全体の運用の品質を向上させている。
  - JANOGなどの活動に対するポジティブな評価が必要。