

Web公開用資料

経路情報の登録認可機構のご紹介

技術部／インターネット推進部
セキュリティ事業担当
木村 泰司

YouTubeのASに対する経路ハイジャック

- 2008年2月24日18:47～21:03 UTC
- 別のOrigin ASによる経路広告
- more specific route(/24)
- 経路広告が止まるまで復旧せず

- RIPE NCCにおける分析
 - 「YouTube Hijacking: A RIPE NCC RIS case study」
<http://www.ripe.net/news/study-youtube-hijacking.html>
 - 「BGPPlay and ‘The Youtube Incident’ - As Seen Through RIS」
(RIPE-56)

 - “ROUTE FILTERING”

内容

- 経路情報の登録認可機構のご紹介
 - 仕組み
 - デモンストレーション

経路情報の登録認可機構

IRRに不適切なprefixが登録されることを防ぐ。

開発の背景

IRRには不適切なprefixが登録される可能性がある。

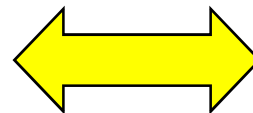
不適切なIPアドレス： 他のISPのprefix、未割り振りのprefix

⇒ 不適切なprefixでも経路広告さえすれば使える状態

IPレジストリシステム



IPアドレスの照合は
行われていない



IRR



経路情報の登録認可機構の仕組み

- WHOISの情報と照合
- IPアドレス割り振り先組織による、IRRの登録者の指定

主な機能の紹介



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

許可リスト

経路情報登録認可機構 - Microsoft Internet Explorer

アドレス(D) https://routerreg.nic.ad.jp/irrms_webs/Login.do

allow/deny 全て 登録者種別 全て

Prefix (equal or less specific equal or more specific)

複数項目の条件はAND条件として検索します。

検索 クリア 全件表示

追加

検索結果 5件

テキスト出力

許可リストID ▲▼	Prefix ▲▼	メンテナ名 ▲▼	AS番号 ▲▼	allow/deny	登録者種別
33	100.0.32.0/19	MAINT-ROUTEREG2	AS37911, AS00001.00001	allow	jpnict
30	202.210.56.0/23	MAINT-ROUTEREG2	AS37911	allow	
19	100.0.10.0/24	MAINT-ROUTEREG2	AS9.9, AS2.5	allow	
18	100.0.10.0/32	MAINT-ROUTEREG	AS2.2	allow	
14	100.0.32.0/19	MAINT-ROUTEREG		allow	jpnict

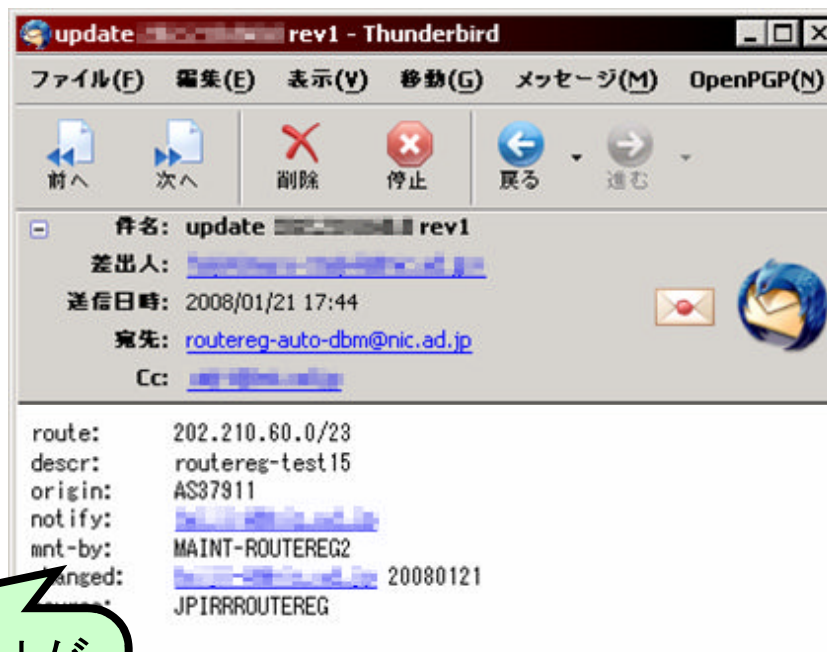
ページが表示されました

インターネット

割り振り先組織がメンテナを指定する

IPアドレスの割り振り先が、IRRに登録されるIPアドレスを管理できる

routeオブジェクトの登録制限



指定されたprefixだけが、
routeオブジェクトとして
登録可能

経路ハイジャック
の検知に役立つ

経路フィルターの
生成に役立つ

正しいIPアドレスとAS番号の組み合わせがIRRに蓄積される

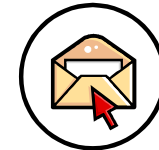
利用実験

- 2007年12月以降、IP指定事業者を対象に利用実験を行っています。
 - 実験の目的
 - 本機構を使った業務の実行可能性を検証
 - 実験期間
 - 2007年12月以降～2009年3月末
 - 継続運用中
 - 利用できる人
 - 「資源管理カード」をお持ちのIP指定事業者
 - 電子証明書を用いた認証方式
 - JPIRRの登録者
 - 登録するprefixの割り振り先事業者が、電子証明書を利用している必要がある
 - 参加費用
 - 無料（USBトークンを無償で貸し出し）
 - 登録されるIRRサーバ
 - jpirr-routereg.nic.ad.jp（本実験向けのJPIRRサーバ）

電子証明書を利用した
認証方式に関する説明会
7月25日（金）15:00～

ご利用までの流れ(IP指定事業者の電子証明書)

1. 認証強化実験の参加申し込み(申込書の郵送)



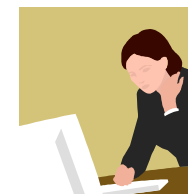
2. 管理者用証明書(資源管理カード)を取得



3. 管理者が**申請者用証明書**を発行
(資源管理カードを使って管理用Webにアクセス)

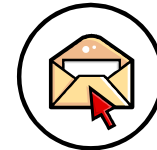


4. **申請者用証明書**を使ってWeb申請システムと
経路情報の登録認可機構を利用開始



ご利用までの流れ (JPIRRのメンテナー)

1. メンテナーオブジェクトを登録 + 実験の参加申込



2. 管理者用証明書を取得



3. 管理者が**オブジェクト登録者**の証明書を発行
(USBトークンで管理用Webにアクセス)



4. **オブジェクト登録者**がS/MIMEを使って
JPIRR-ROUTEREGにオブジェクトを登録



参照

- 経路情報の登録認可機構

<http://www.nic.ad.jp/ja/research/ca/routereg-outline/>

- 資源管理証明書

<http://www.nic.ad.jp/ja/research/ca/lir-certificate/>

- 電子証明書を利用した認証方式に関する説明会のお知らせ

<http://www.nic.ad.jp/ja/topics/2008/20080710-01.html>

- お問い合わせ先

ca-query at nic.ad.jp