

経路情報の登録認可機構に関する取り組みについて

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
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”

はじめに

- 現在利用実験を行っている「経路情報の登録認可機構」についてのご紹介です。
 - 利用実験について
 - 仕組み
 - 利用実験へのご参加について

利用実験について(1)

2007年12月以降、指定事業者の皆様を対象にした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する。

- **実験の対象**

- 参加を希望されるIP指定事業者、及びJPIRRの登録者
- IPアドレス管理業務で使われる電子証明書(資源申請者証明書)を利用

利用実験について(2)

- **実験の内容**
 - 本機構の実験用に立ち上げたIRRサーバを利用
 - 自組織に割り振り済みのIPアドレスを登録
 - 登録されたIPアドレスだけが、IRRに登録できることを確認
 - 業務上の実行可能性等についてアンケートに回答
- **実験期間**
 - 2007年12月以降～2009年3月末
 - 実験結果を受けて継続運用を検討
- **参加費用**
 - 無料 (USBトークンを無償で貸し出し)

IPアドレス管理指定事業者 仕組み(1)

Web申請システム



経路情報の登録認可機構



自組織に割り振られているIPアドレスを確認する。
 “情報表示” “資源管理者情報”

IP指定事業者の
 資源申請者

IPアドレスとそのIPアドレスが経路広告されるAS番号などを登録する。
 “許可リスト登録”

IPアドレス管理指定事業者 仕組み(2)

経路情報の登録認可機構



許可リスト一覧

検索条件入力

許可リストID: 資源管理者略称:

IPバージョン: Prefix:

ASN番号: allow/deny:

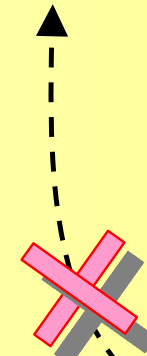
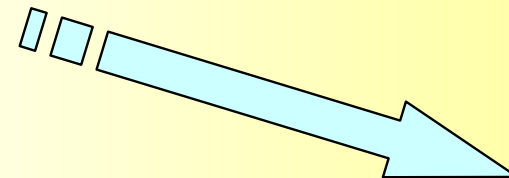
登録者種別:

検索項目の条件はAND条件として検索します。

検索結果 4件

許可リストID	資源管理者略称	Prefix	ASN番号	allow/deny	登録者種別
19	ROUTE6TEST	100.0.10.0/24	AS9.9, AS2.5	allow	
23	ROUTE6TEST	100.0.32.0/19	AS00001.00001, AS37911	allow	grtc
30	ROUTE6TEST	202.210.56.0/23	AS37911	allow	
27	ROUTE6TEST	202.210.58.0/23	AS37911	allow	
26	ROUTE6TEST	2001.0x40.0/2	AS37911, AS2.5	allow	
24	ROUTE6TEST	5000.0/2	AS99999.99999, AS37911	allow	grtc

実験用IRR



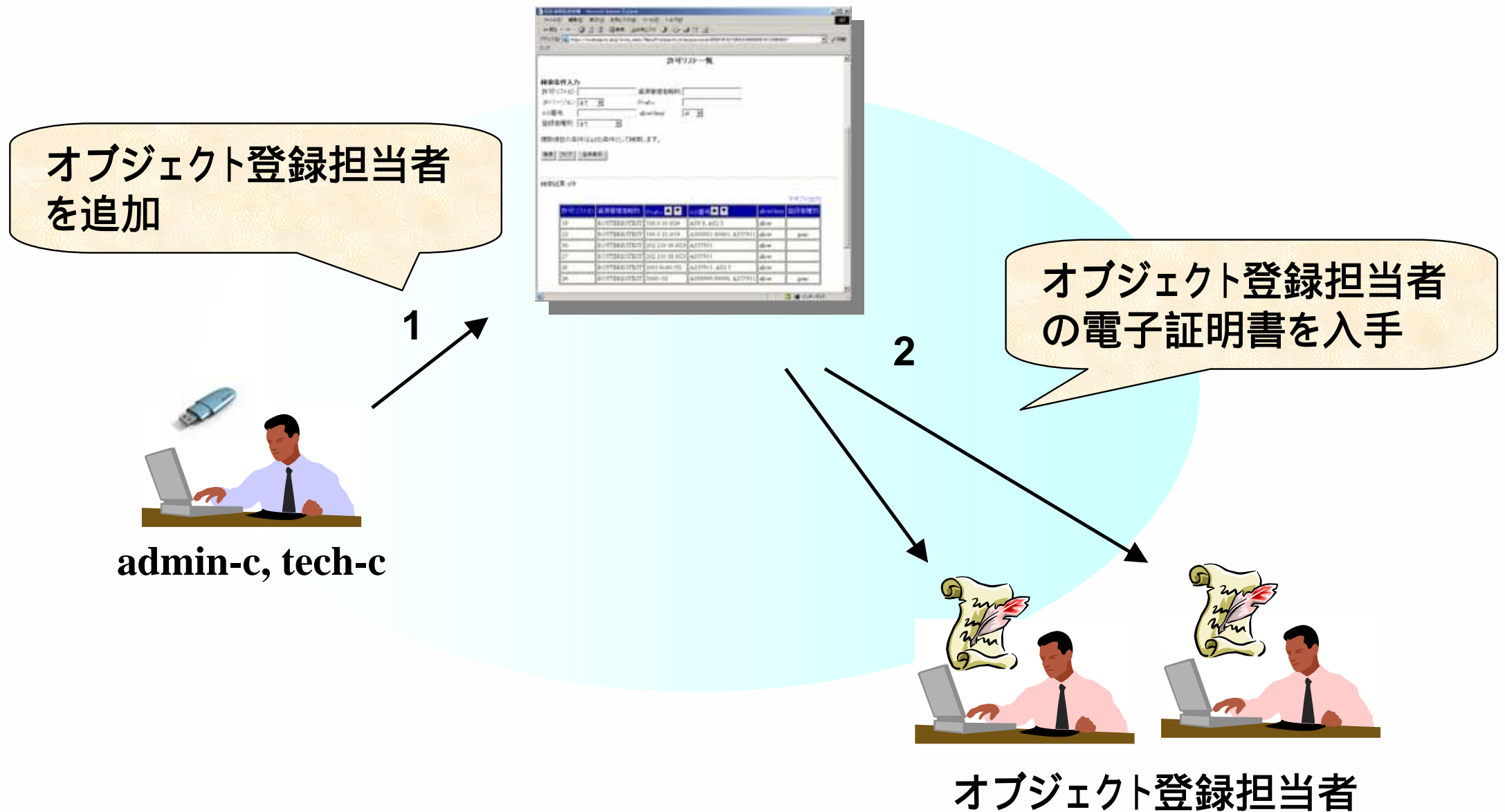
登録されたIPアドレス以外を拒否する。



不正な登録者
(ミスを含む)

JPIRRの登録担当者 仕組み (I)

経路情報の登録認可機構



JPIRRの登録担当者 仕組み(II)

経路情報の登録認可機構



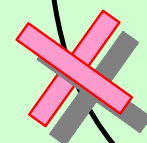
実験用IRR



不正な登録者による登録を拒否する。



オブジェクト登録担当者



不正な登録者
(ミスを含む)

経路ハイジャック
情報通知実験

将来のIRR



登録されたオブジェクト
の正しさを維持したIRR

ガーベージコレクター

ポリシーチェッカー

経路情報の登録認可機構

経路制御のセキュリティとの関連性について

利用実験へのご参加のお願い

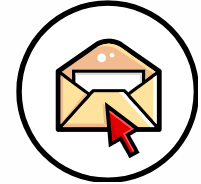
- JPIRRのセキュリティ向上を図るために、経路情報の登録認可機構は重要ですが、実用化には、業務の実行可能性を検証する必要があります。そのためには皆さまに実験に参加して頂く必要があります。

JPIRRへの登録をお願いいたします。

経路情報の登録認可機構の利用実験にご参加下さい。

ご利用までの流れ(IP指定事業者)

1. 資源管理者証明書発行申込書(郵送)



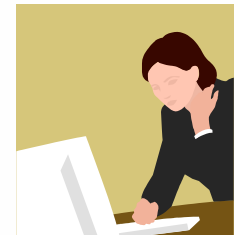
2. 資源管理カードを取得



3. 資源申請者証明書を発行
(資源管理カードを使って管理用Webにアクセス)



4. 資源申請者証明書を使ってWeb申請システムと
経路情報の登録認可機構を利用



ご利用までの流れ(JPIRR)

1. Maintainer オブジェクトを登録



2. Aut-Numオブジェクトの登録



3. その他のオブジェクトの登録: As-Set, Role, Person, Route



4. WhoisやIRR関連ツールを利用



ご利用までの流れ(経路情報の登録認可機構)

1. JPIRRのmntnerオブジェクトを登録 + 実験の参加申込



2. 認証トークンを取得



3. オブジェクト登録者の証明書を発行
(USBトークンを使って管理用Webにアクセス)



4. オブジェクト登録者がS/MIMEを使って実験用IRR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/>
- **電子証明書を用いた申請者認証について**
 - <http://www.nic.ad.jp/doc/lir-certificate-guide.html>
- **Telecom-ISAC Japan 経路奉行とJPIRR間の連携実験について**
 - http://www.nic.ad.jp/ja/ip/irr/jpirr_exp.html
- **JPIRRでのオブジェクト登録について**
 - <http://www.nic.ad.jp/doc/irr-registration.html>
- **お問合せ先**
 - ca-query at nic.ad.jp