BGPと IRR

～経路制御の 信頼性向上に 向けて ～

インターネットイニシアティブ
松崎吉伸 maz@iij.ad.jp

NTTコミュニケーションズ / JPNIC IRR-Plan
吉田友哉 yoshida@ocn.ad.jp

BGP

Inter-AS

- BGPで経路の交換
- 世界のどこかで生成された経路が、世界中に伝わっていく
- インターネットは常に変化し続けている
  - どこから、どんな経路が流れてくるか事前にはわからない場合が多い

BGP AS利用者の変遷

- ISP、xSP
- **研究組織、研究機関**
- CATV
- **大学**
  - Private AS → Global ASへ
- **大企業、IT企業**

hijack経路

- 悪意
  - SPAM送信
  - サイト/ネットワークの乗っ取り
- 設定ミス
  - filter
  - redistribute
  - 打ち間違い

hijack経路vs正しい経路

- hijack経路の生成場所
  - 外部のAS　普通想定している生成場所
  - 自網内　そんな事になってる時点でダメ

hijack経路vs正しい経路

- hijack経路の 流入場所
  - 顧客　利用アドレスのチェックとprefix filter
  - ピア　　ありがち
  - 上流　ありがち

hijack経路vs正しい経路

- hijack経路の prefix長
  - 同じ　接続&契約、AS Path長次第
  - 短い　影響は無視できるけど気持ち悪い
  - 長い　負け。吸い込まれる

hijack経路vs正しい経路

- hijack経路のAS Path長
  - 同じ　　接続＆契約次第
  - 短い　　接続＆契約に依存するが、結構負け。
  - 長い　　絶対大丈夫とはいえないかも･･･

hijack経路vs正しい経路

- hijack**経路の** origin AS
  - **同じ　　気がつきにくいかも**
  - **違う　　気がつきやすいかも**

hijack経路vs正しい経路

- hijack経路のMED
  - 同じ　接続構成次第
  - 小さい　AS Path長まで同じだと負け
  - 大きい　絶対大丈夫だとはいえないかも

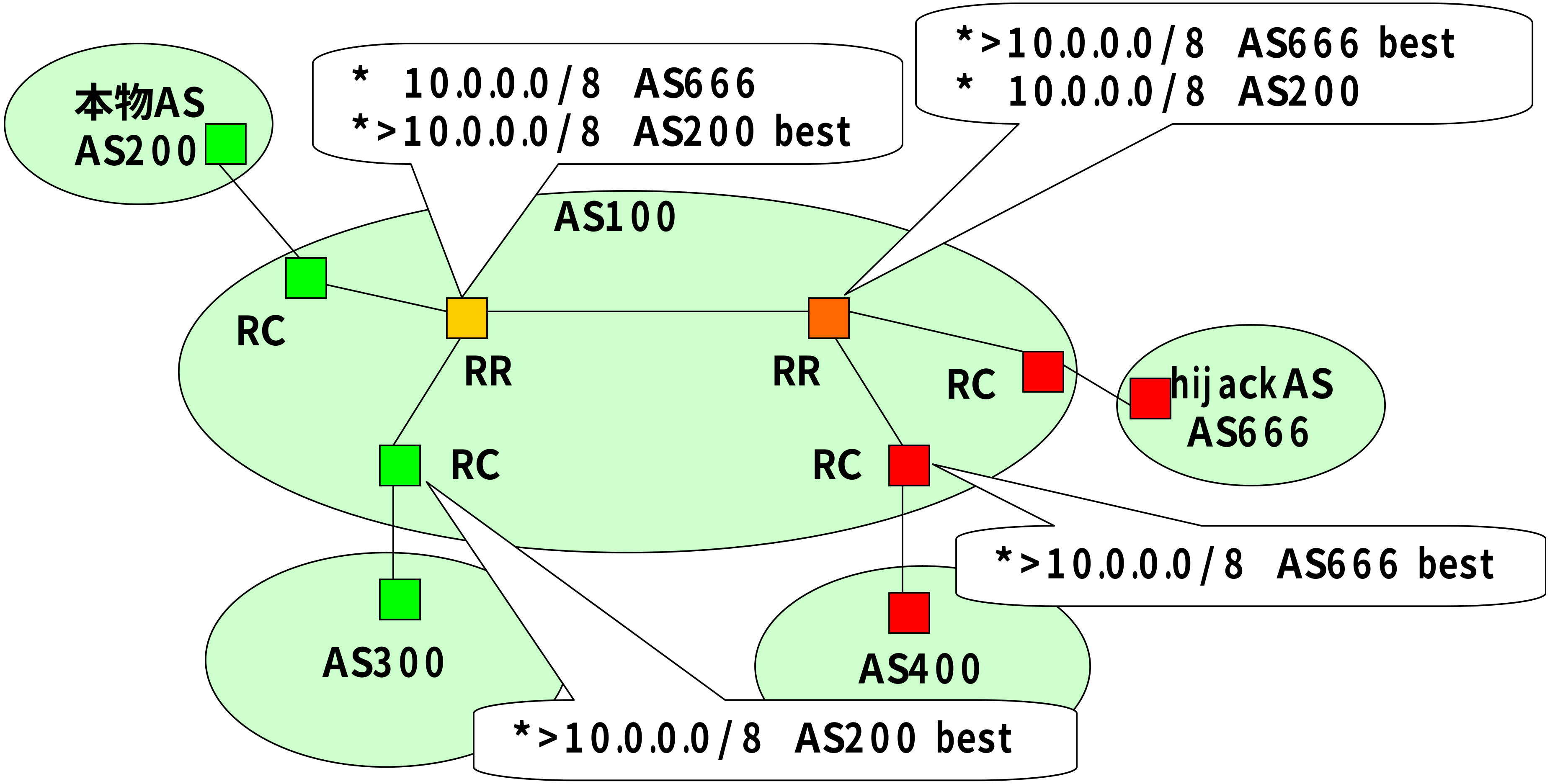
hijack経路vs正しい経路

- hijack経路の bgp community
  - 同じ　bgp community filter次第
  - 違う　bgp community filter次第

ルータの汚染具合

- hijack経路のみ
  - 完全にダメ
- hijack経路 (best) +正常な経路
  - ぎりぎりダメ
- hijack経路+正常な経路(best)
  - セーフ。でも危うい
- 正常な経路のみ
  - 綺麗な体

ASの中でさえ、汚染具合は違う



今できそうなこと

- 間違った経路をいち早く検出する
  - 正しい経路とは？
  - 検出方法は？
- IR,IRRの情報を適正に保つ
  - 正当な経路であると主張する

IRRだけで頑張れそうな範囲

違えば検出可能

- 違うorigin AS
- 違うprefix長

object依存

- AS Path
- bgp community
- MED

難しい

- 同じorigin AS
- 同じprefix長
- 生成場所
- etc...

信頼できる情報

- 乱立するIRR
  - 登録場所としてのIRR
  - データの正当性は確認されない場合が多い
- 信頼できる情報は？
  - 割り振り情報
  - IRが知っている

ここで主張の整理

経路はhijackされるかもしれない

↓

経路の正当性を確認する手法が必要

↓

まずは信頼できる情報が必要

IRR

IRRデータベースで経路確認

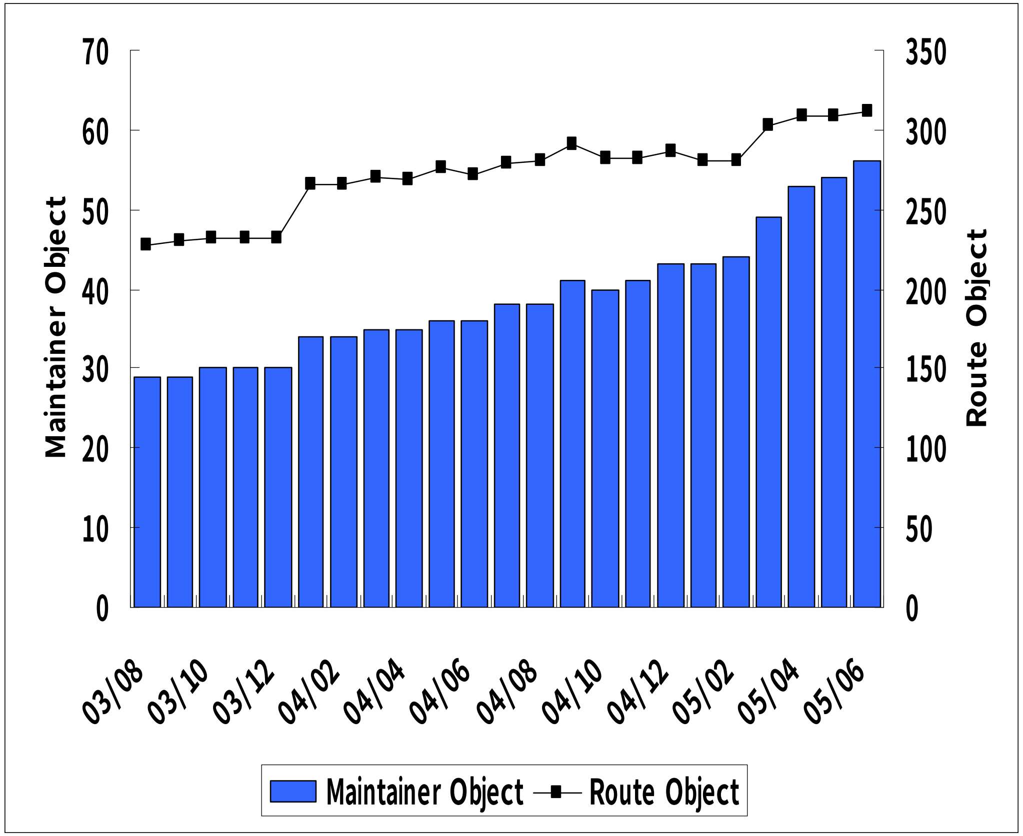
- 経路情報の信憑性確認
- コンタクト情報の取得
- フィルタリング
- 問題点、課題点
  – 信憑性の欠如、維持(ゴミ多し)
  – 情報の分散化
  – IRRシステムの安全性

JPNICで試験サービスやってます

- 費用は無料
- ミラーリング先：APNIC、RADB、RIPE NCC
- 登録オブジェクト数

(2005/06/21現在)

Maitainainerオブジェクト :52
Routeオブジェクト :315
Aut-numオブジェクト :35
As-setオブジェクト :23



試験サービスの背景

日本におけるIRRの必要性に関する調査
インターネットの円滑な運用のための情報提供
IRRサーバ運用経験の取得とフィードバック

2002年8月より試験サービス開始
日本国内で活動する組織であれば、オブジェクトの登録が可能(検索は特に制限を設けず)

いつなんどき無くなるような、他とあまり変わりのないIRRでは駄目だろう

信頼性の高いIRRを作るには

- IRRの情報を健全に保つために、IPアドレスのデータベースと連携することが必要(必須)
  - ISPがやるIRRサービスでは、正しいvalidationが出来ない
  - 日本ではJPNICがIRRを運用することで、より信頼性の高いIRRの情報提供が十分期待できる
- JPNICがサービスを行うことで、外貨建てでの支払や、外国語でのやり取りの煩雑さを軽減できる
- IRRの活用により、ミスオペレーションなどの危険性を低減し、安全なインターネットの運用に貢献できる

↓

JPNICがきちんとIRRを運用していく＝正式にやる

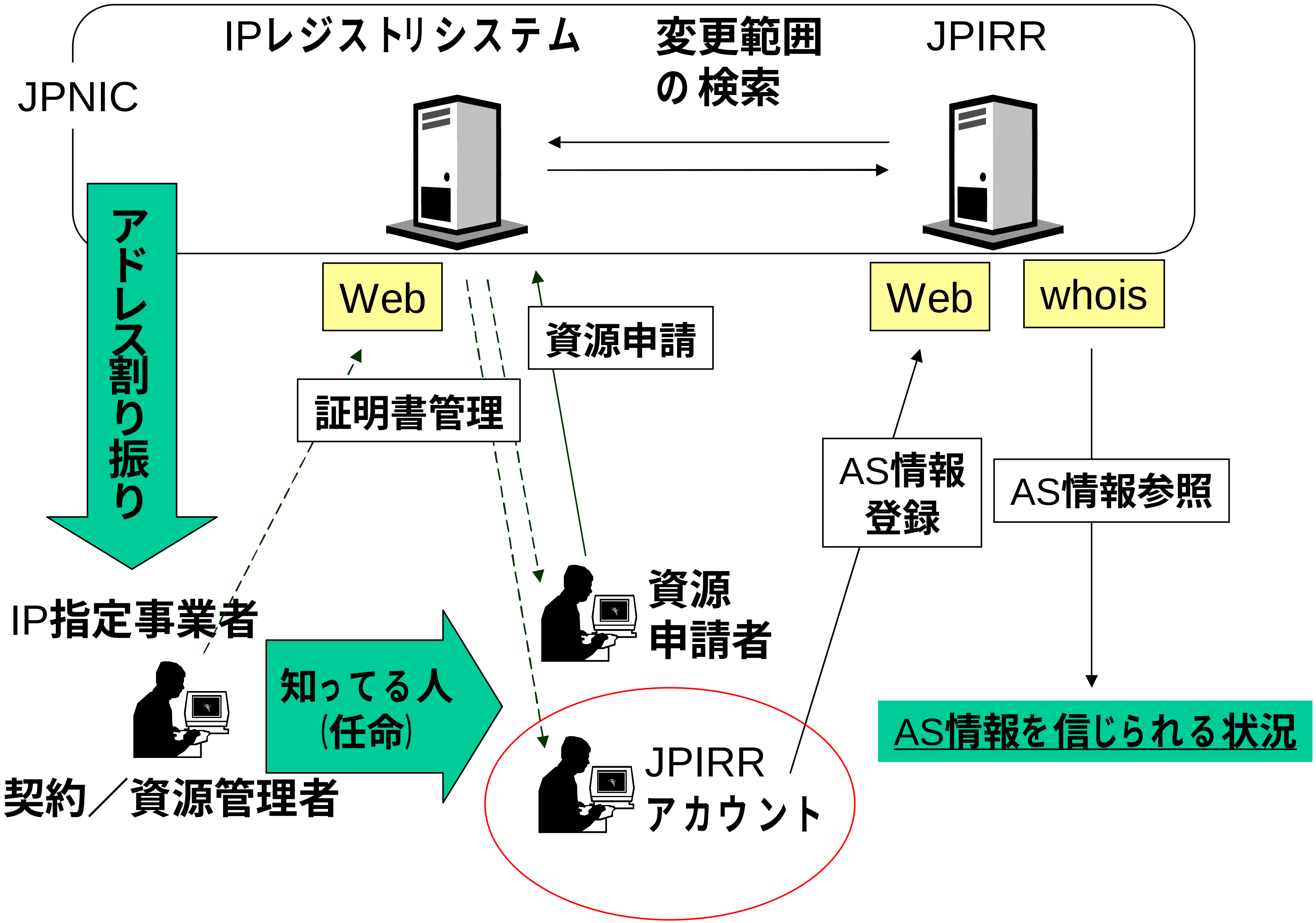
JPIRRのすすむ道1

- 信頼性の高いIRRの構築
  - IPアドレスのデータベースと連動して、正しい登録者が正しい情報を登録できるIRRを作る
    - 他人に勝手に自分のルートを登録されないように、確認されたうえで登録される仕組みが必要
    - 認証局や電子証明書を積極的に活用
  - ミラーリングを適切に行う(監視もする)
  - 登録情報の精度を保つ仕組み
    - 経路情報とのマッチングによる不整合の検出
    - オブジェクト同士のマッチング

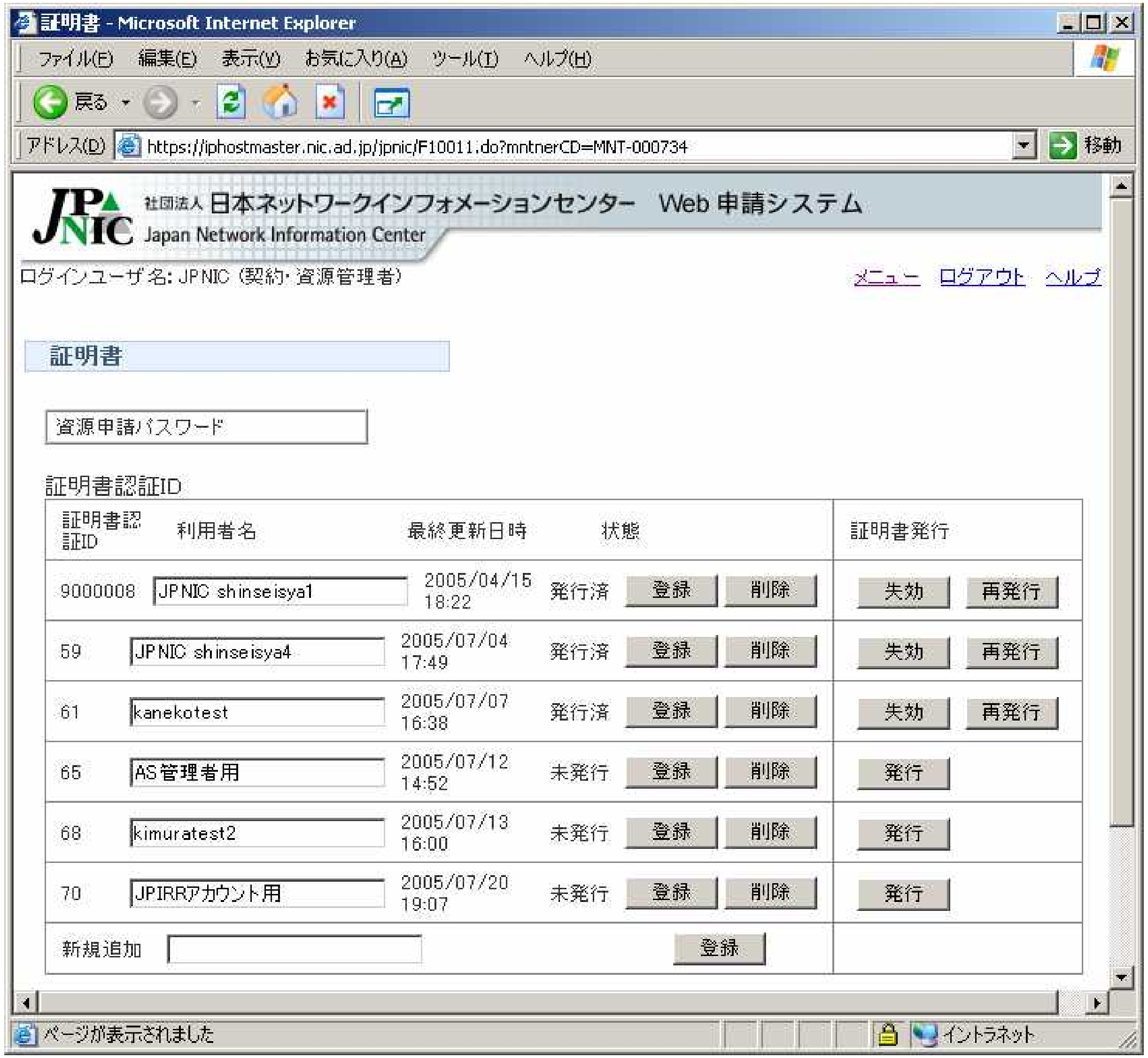
↓

インターネットの円滑な運用への情報提供

認証メカニズム


IPレジストリシステム
変更範囲
の検索
JPIRR
JPNIC
アドレス割り振り
Web
Web
whois
資源申請
証明書管理
AS情報
登録
AS情報参照
資源
申請者
IP指定事業者
知ってる人
(任命)
JPIRR
アカウント
契約／資源管理者
AS情報を信じられる状況

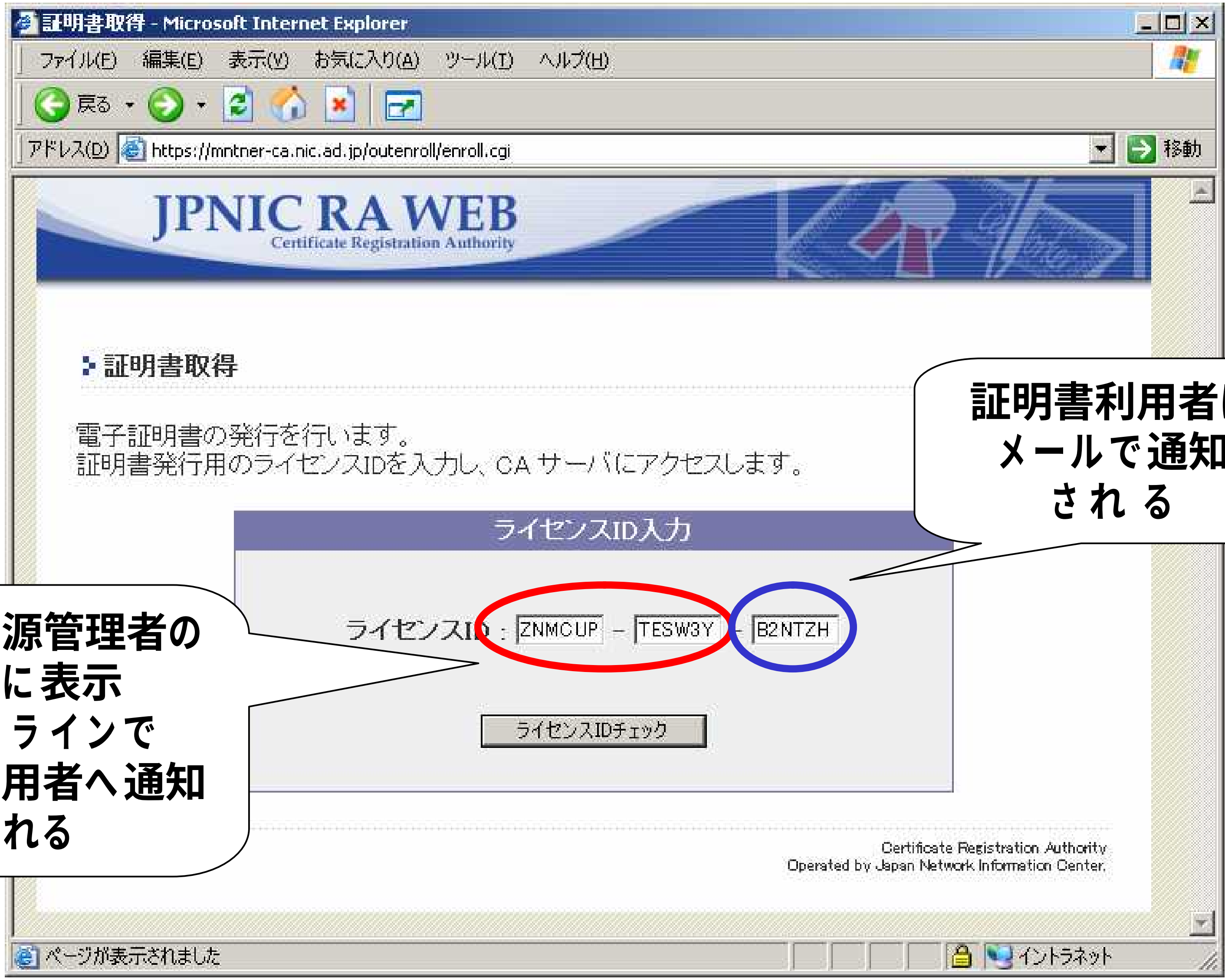
認証IDの管理


証明書 - Microsoft Internet Explorer
ファイル(F) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)
戻る
アドレス(D) https://iphostmaster.nic.ad.jp/jpnic/F10011.do?mntnerCD=MNT-000734
移動
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 Web 申請システム
Japan Network Information Center
ログインユーザ名: JPNIC (契約・資源管理者)
メニュー ログアウト ヘルプ
証明書
資源申請パスワード
証明書認証ID
証明書認証ID 利用者名 最終更新日時 状態 証明書発行
9000008 JPNIC shinseisya1 2005/04/15 18:22 発行済 登録 削除 失効 再発行
59 JPNIC shinseisya4 2005/07/04 17:49 発行済 登録 削除 失効 再発行
61 kanekotest 2005/07/07 16:38 発行済 登録 削除 失効 再発行
65 AS管理者用 2005/07/12 14:52 未発行 登録 削除 発行
68 kimuratest2 2005/07/13 16:00 未発行 登録 削除 発行
70 JPIRRアカウント用 2005/07/20 19:07 未発行 登録 削除 発行
新規追加 登録
ページが表示されました
イントラネット

証明書の申請


サーバーが見つかりません - Microsoft Internet Explorer
ファイル(F) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)
戻る
アドレス(D) /outside/regist.cgi?MNTNER=MNT-000734&CERT_ID=0000070&MNT_AR=5&ORG=Japan+Network+Information+Center&OP=
移動
JPNIC RA WEB
Certificate Registration Authority
管理者
組織名(Organization): Japan Network Information Center
メンテナーコード: MNT-000733
操作対象者
メンテナーコード: MNT-000734
権限種別: 申請者用
認証ID: 0000070
証明書申請
証明書の発行申請を行ないます。発行対象者の名称とEMAILアドレスを入力してください。
なお、名称・EMAILともに半角64文字まで入力できます。
名称 :
EMAIL :
種別 :
資源申請者用
JPIRRアカウント用
証明書を申請する
ページが表示されました
インターネット

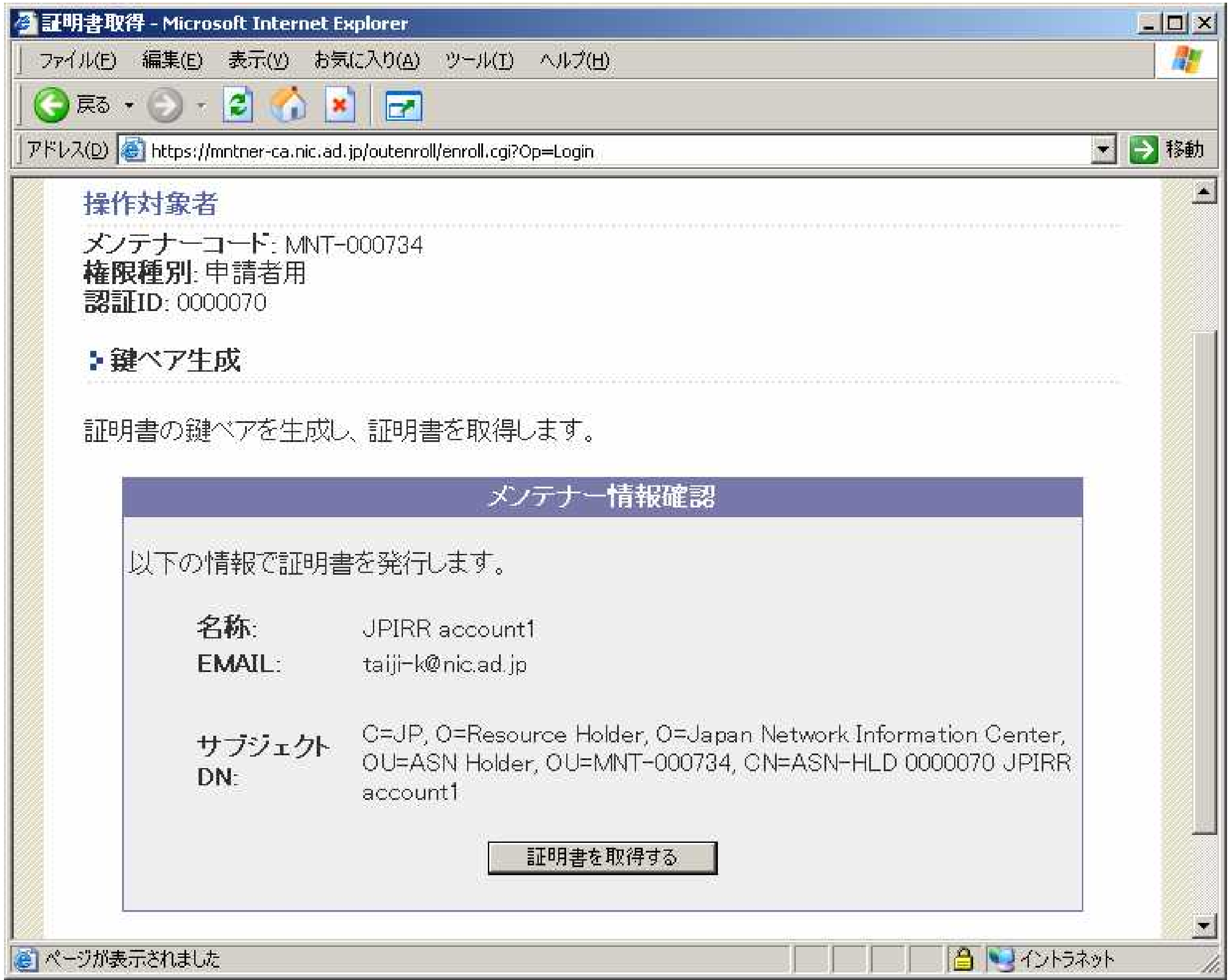
ライセンスID



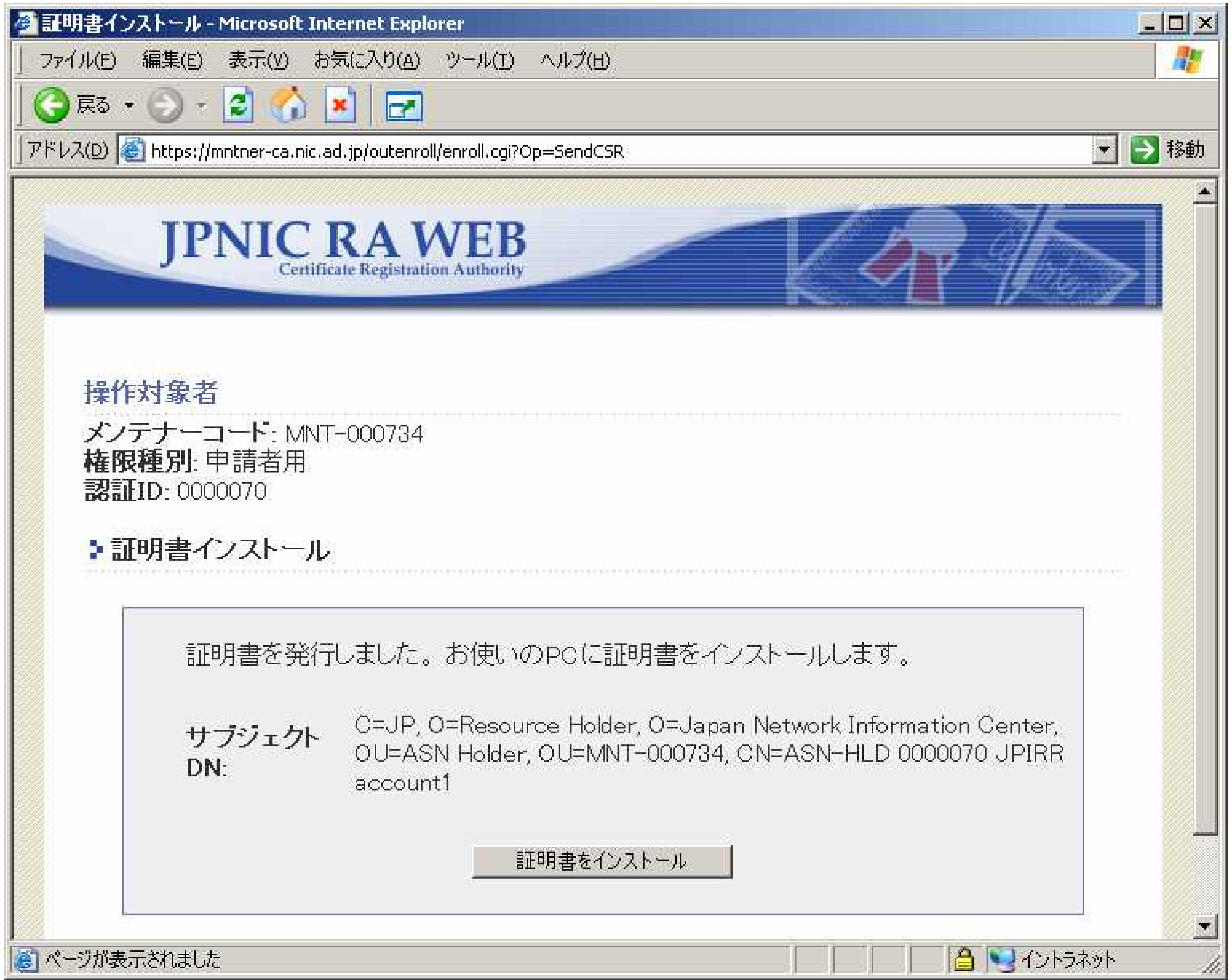
証明書利用者に
メールで通知
される

契約／資源管理者の
画面に表示
⇒ オフラインで
証明書利用者へ通知
される

証明書確認

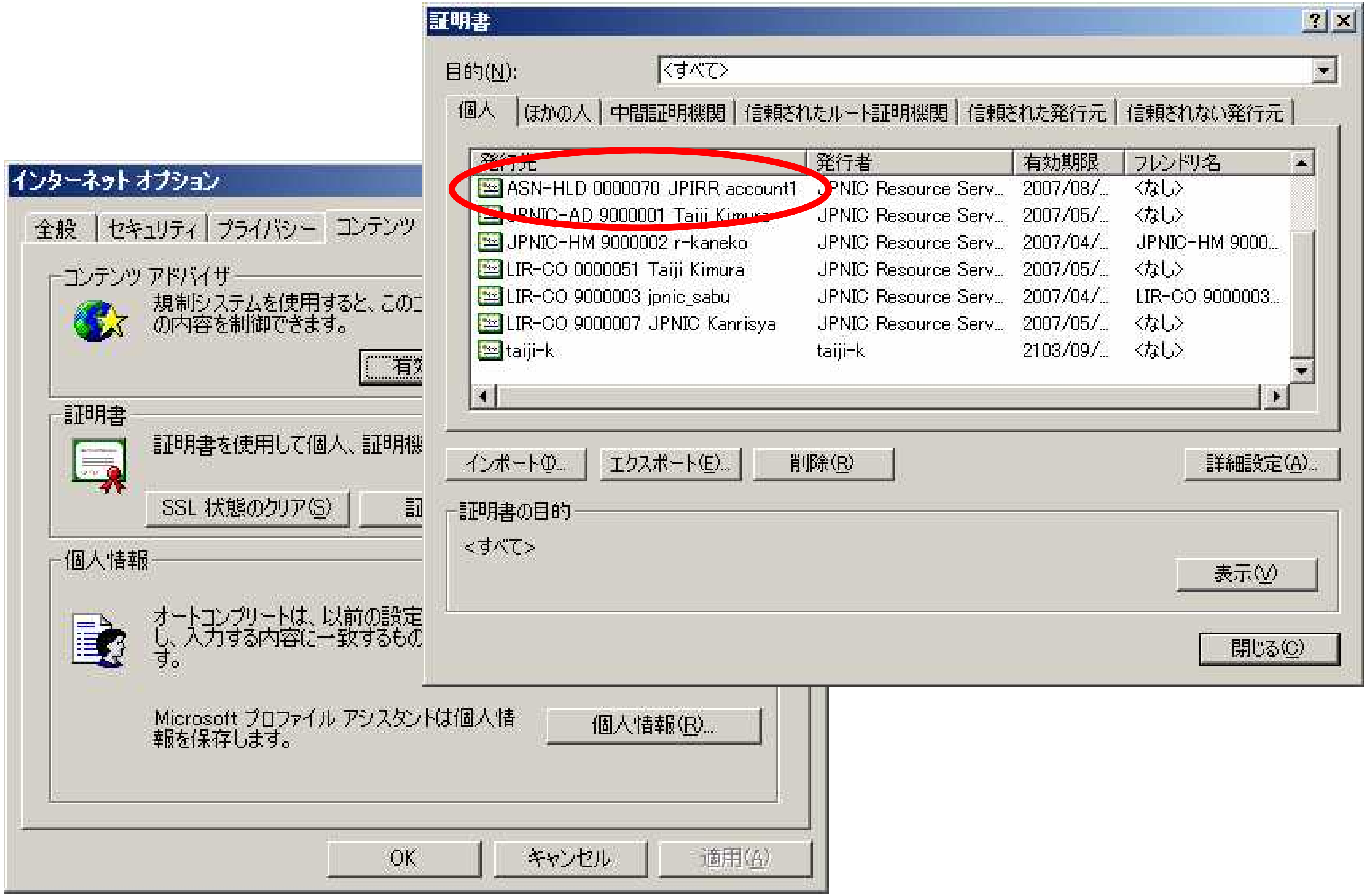

証明書取得 - Microsoft Internet Explorer
ファイル(F) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)
戻る
アドレス(D) https://mntner-ca.nic.ad.jp/outenroll/enroll.cgi?Op=Login
移動
操作対象者
メンテナーコード: MNT-000734
権限種別: 申請者用
認証ID: 0000070
鍵ペア生成
証明書の鍵ペアを生成し、証明書を取得します。
メンテナー情報確認
以下の情報で証明書を発行します。
名称: JPIRR account1
EMAIL: taiji-k@nic.ad.jp
サブジェクトDN: C=JP, O=Resource Holder, O=Japan Network Information Center, OU=ASN Holder, OU=MNT-000734, CN=ASN-HLD 0000070 JPIRR account1
証明書を取得する
ページが表示されました
イントラネット

インストール

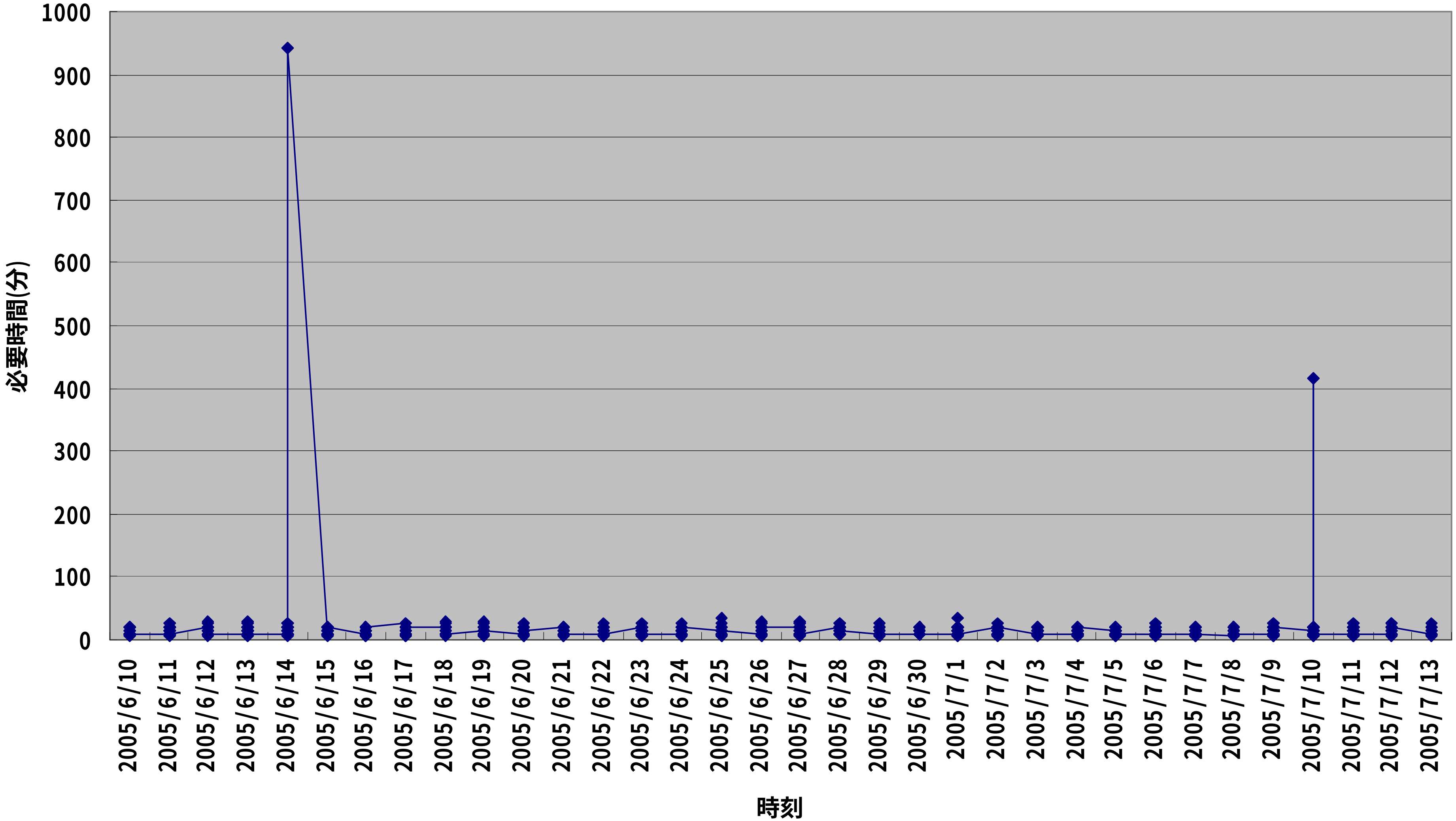


証明書インストール - Microsoft Internet Explorer
ファイル(F) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)
戻る
アドレス(D) https://mntner-ca.nic.ad.jp/outenroll/enroll.cgi?Op=SendCSR
移動
JPNIC RA WEB
Certificate Registration Authority
操作対象者
メンテナーコード: MNT-000734
権限種別: 申請者用
認証ID: 0000070
証明書インストール
証明書を発行しました。お使いのPCに証明書をインストールします。
サブジェクトDN:
C=JP, O=Resource Holder, O=Japan Network Information Center, OU=ASN Holder, OU=MNT-000734, CN=ASN-HLD 0000070 JPIRR account1
証明書をインストール
ページが表示されました
イントラネット

Webブラウザで利用

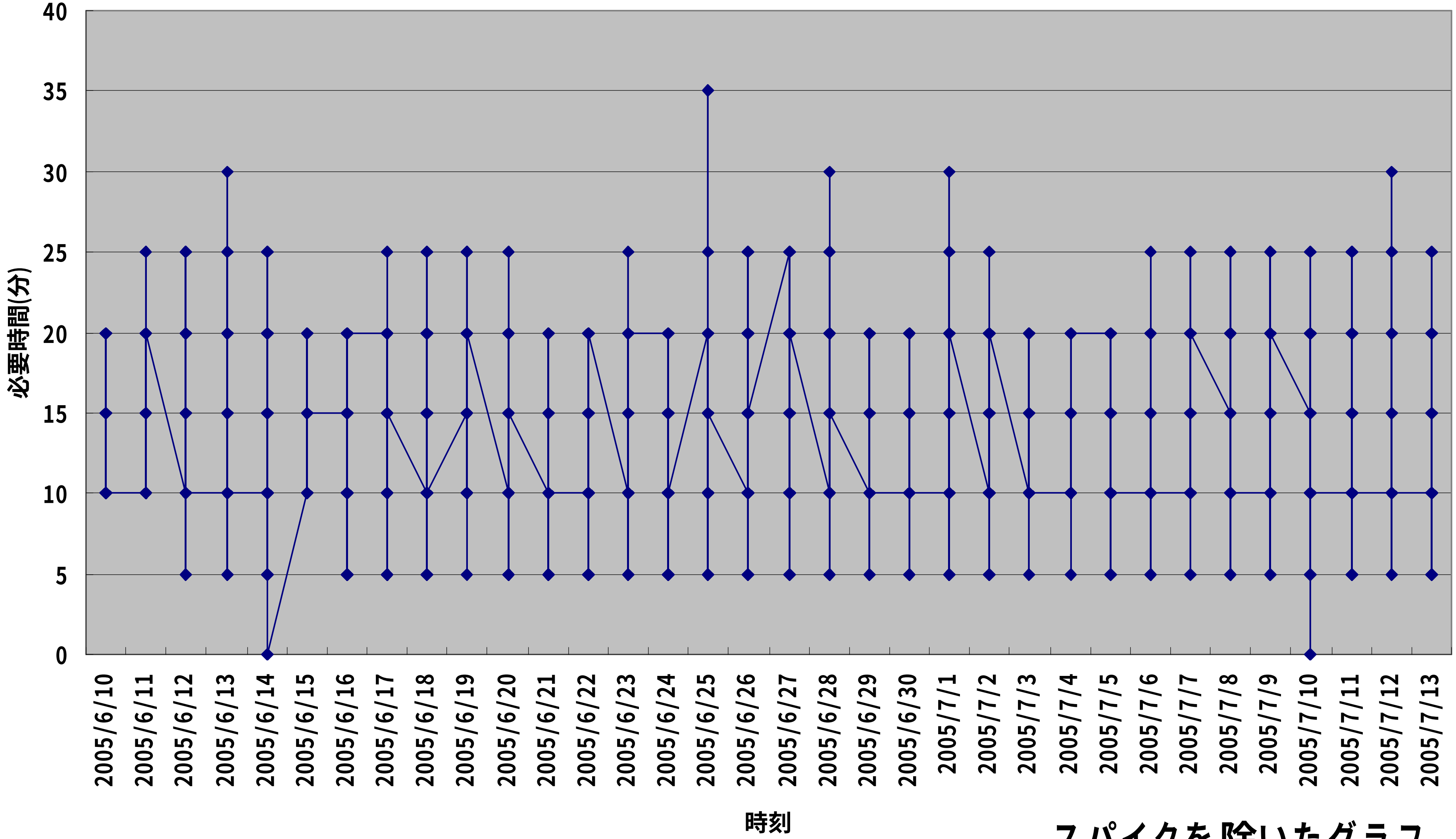

証明書
目的(N): <すべて>
個人 ほかの人 中間証明機関 信頼されたルート証明機関 信頼された発行元 信頼されない発行元
発行先 発行者 有効期限 フレンドリ名
ASN-HLD 0000070 JPIRR account1 JPNIC Resource Serv... 2007/08/... <なし>
JPNIC-AD 9000001 Taiji Kimura JPNIC Resource Serv... 2007/05/... <なし>
JPNIC-HM 9000002 r-kaneko JPNIC Resource Serv... 2007/04/... JPNIC-HM 9000...
LIR-CO 0000051 Taiji Kimura JPNIC Resource Serv... 2007/05/... <なし>
LIR-CO 9000003 jpnic_sabu JPNIC Resource Serv... 2007/04/... LIR-CO 9000003...
LIR-CO 9000007 JPNIC Kanrisya JPNIC Resource Serv... 2007/05/... <なし>
taiji-k taiji-k 2103/09/... <なし>
インポート(I)... エクスポート(E)... 削除(R) 詳細設定(A)...
証明書の目的
<すべて>
表示(V)
閉じる(C)
インターネット オプション
全般 セキュリティ プライバシー コンテンツ
コンテンツ アドバイザ
証明書
SSL 状態のクリア(S)
個人情報
Microsoft プロファイル アシスタントは個人情報を保存します。
個人情報(R)...
OK キャンセル 適用(A)

JPIRR→RADB



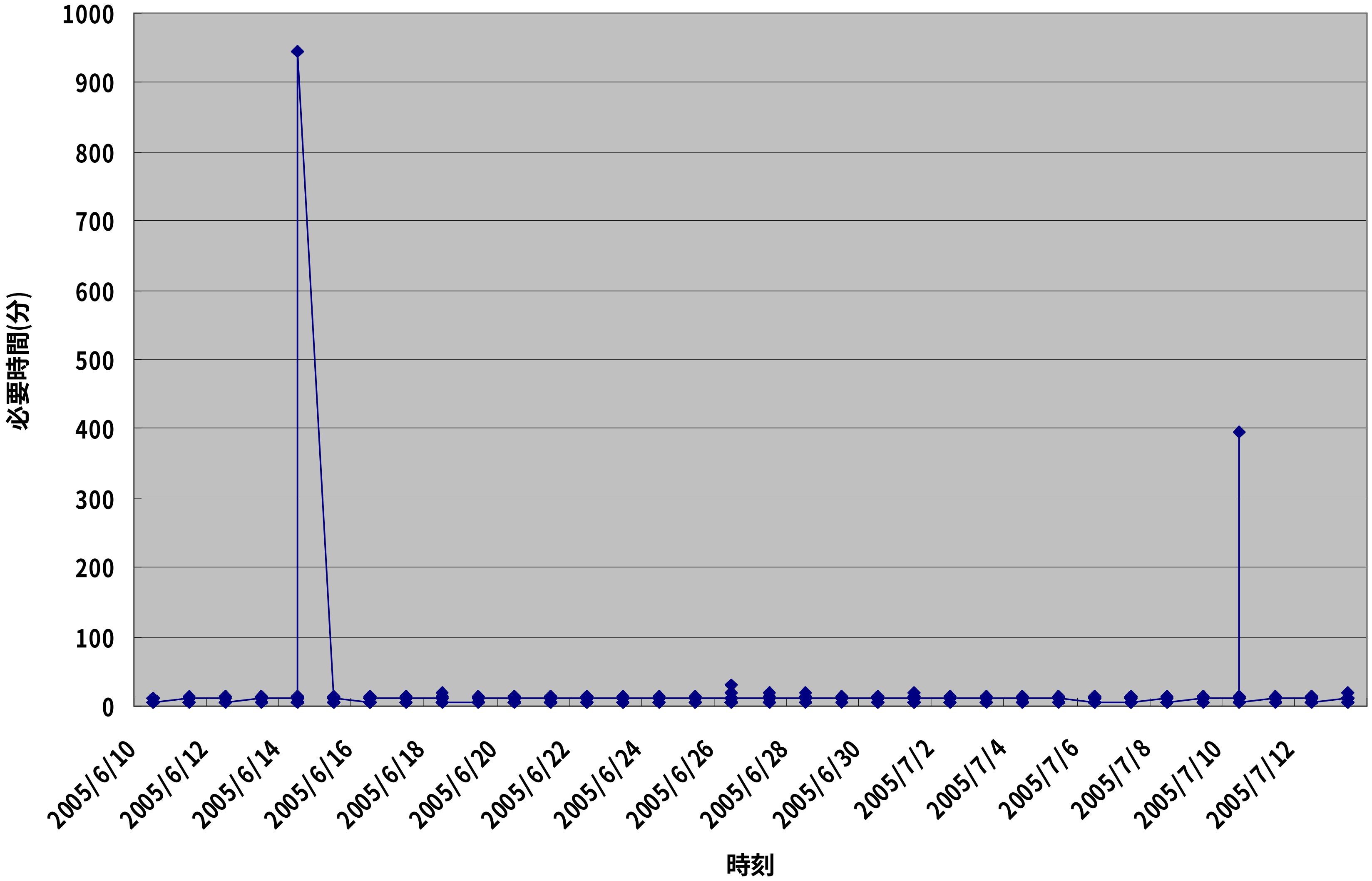
1000
900
800
700
600
500
400
300
200
100
0
必要時間(分)
2005/6/10
2005/6/11
2005/6/12
2005/6/13
2005/6/14
2005/6/15
2005/6/16
2005/6/17
2005/6/18
2005/6/19
2005/6/20
2005/6/21
2005/6/22
2005/6/23
2005/6/24
2005/6/25
2005/6/26
2005/6/27
2005/6/28
2005/6/29
2005/6/30
2005/7/1
2005/7/2
2005/7/3
2005/7/4
2005/7/5
2005/7/6
2005/7/7
2005/7/8
2005/7/9
2005/7/10
2005/7/11
2005/7/12
2005/7/13
時刻

JPIRR→RADB



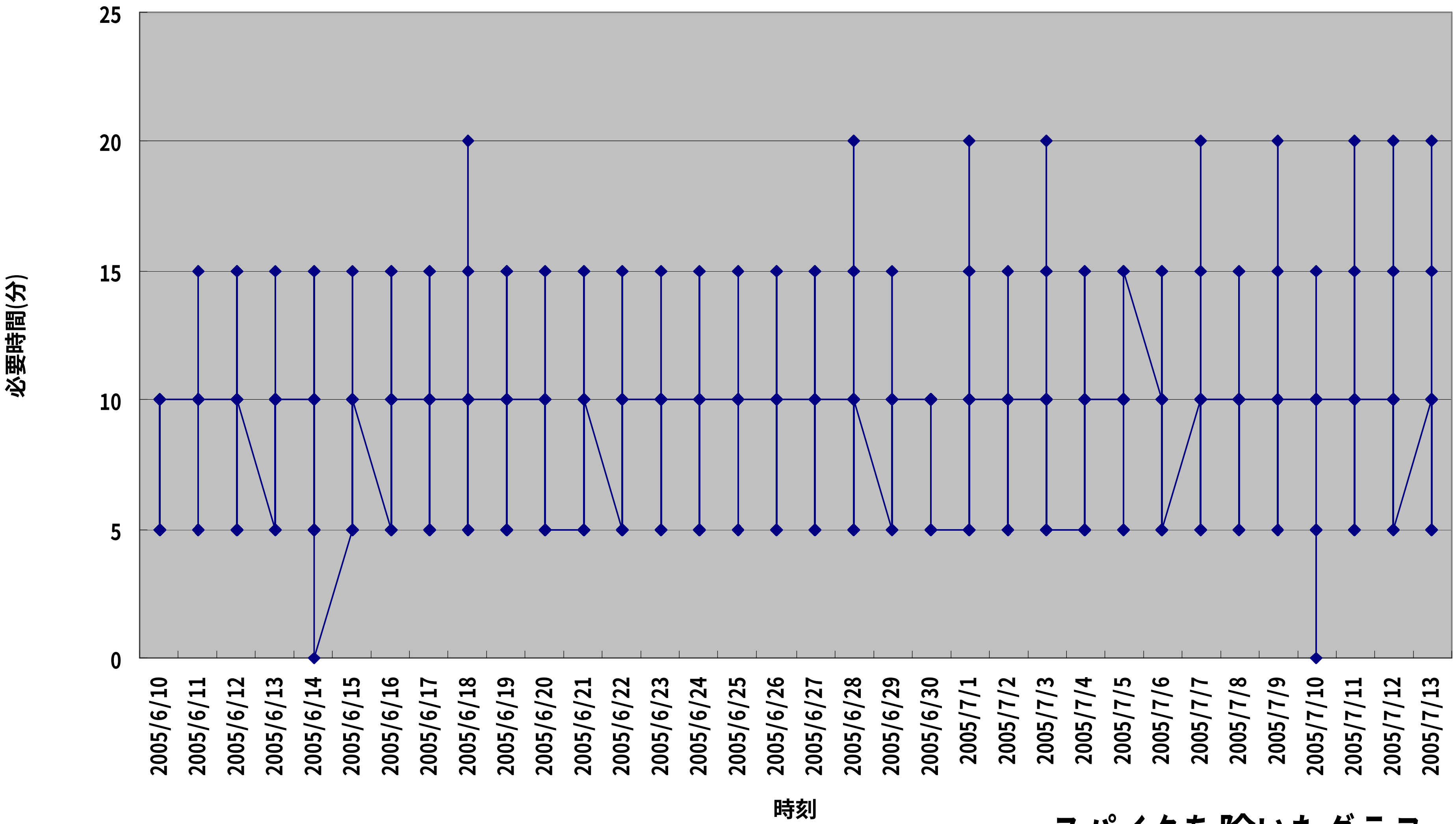
スパイクを 除いたグラフ

JPIRR→APNIC



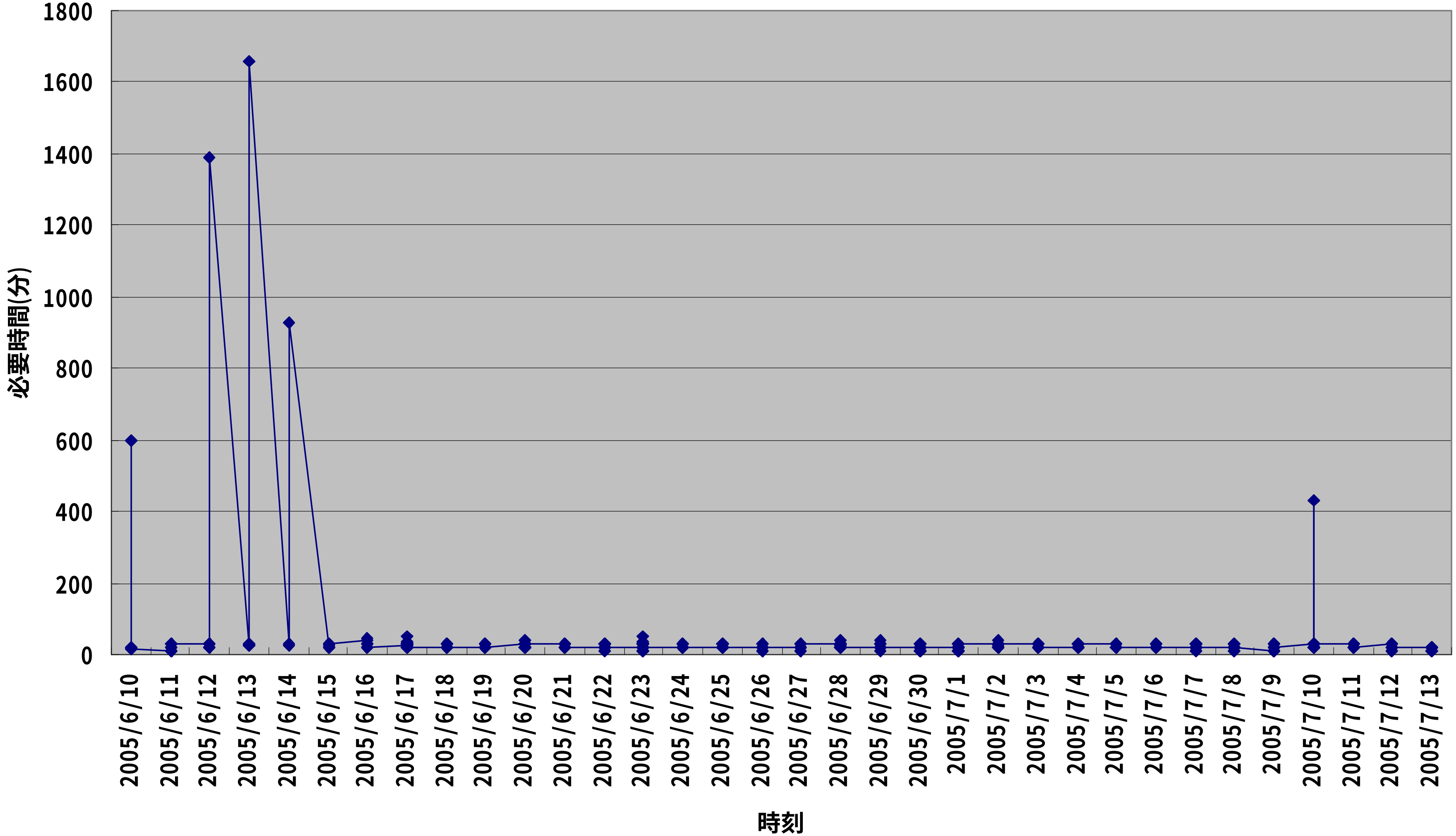
1000
900
800
700
600
500
400
300
200
100
0
必要時間(分)
2005/6/10
2005/6/12
2005/6/14
2005/6/16
2005/6/18
2005/6/20
2005/6/22
2005/6/24
2005/6/26
2005/6/28
2005/6/30
2005/7/2
2005/7/4
2005/7/6
2005/7/8
2005/7/10
2005/7/12
時刻

JPIRR→APNIC

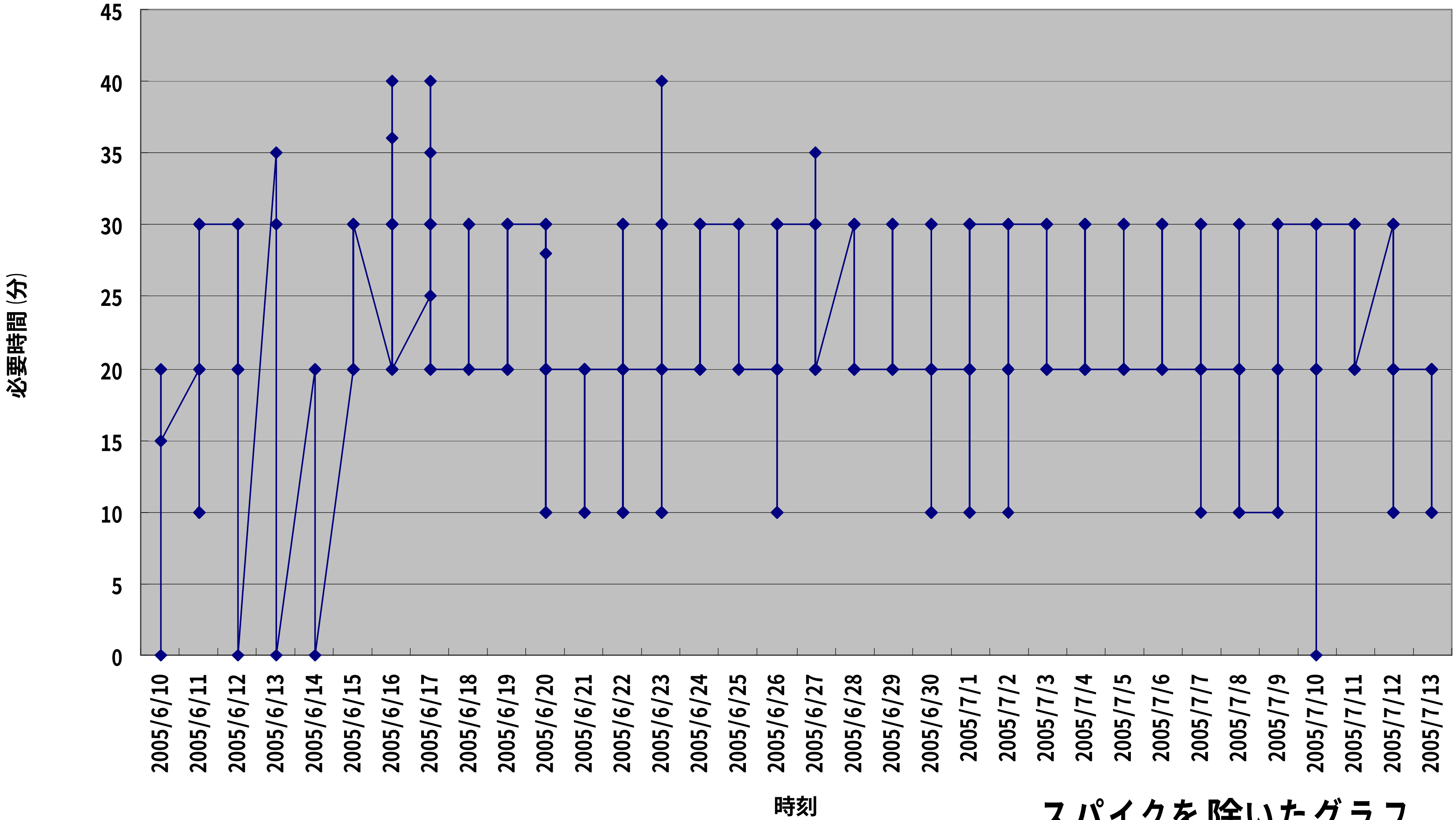


スパイクを 除いたグラフ

JPIRR→RIPE NCC

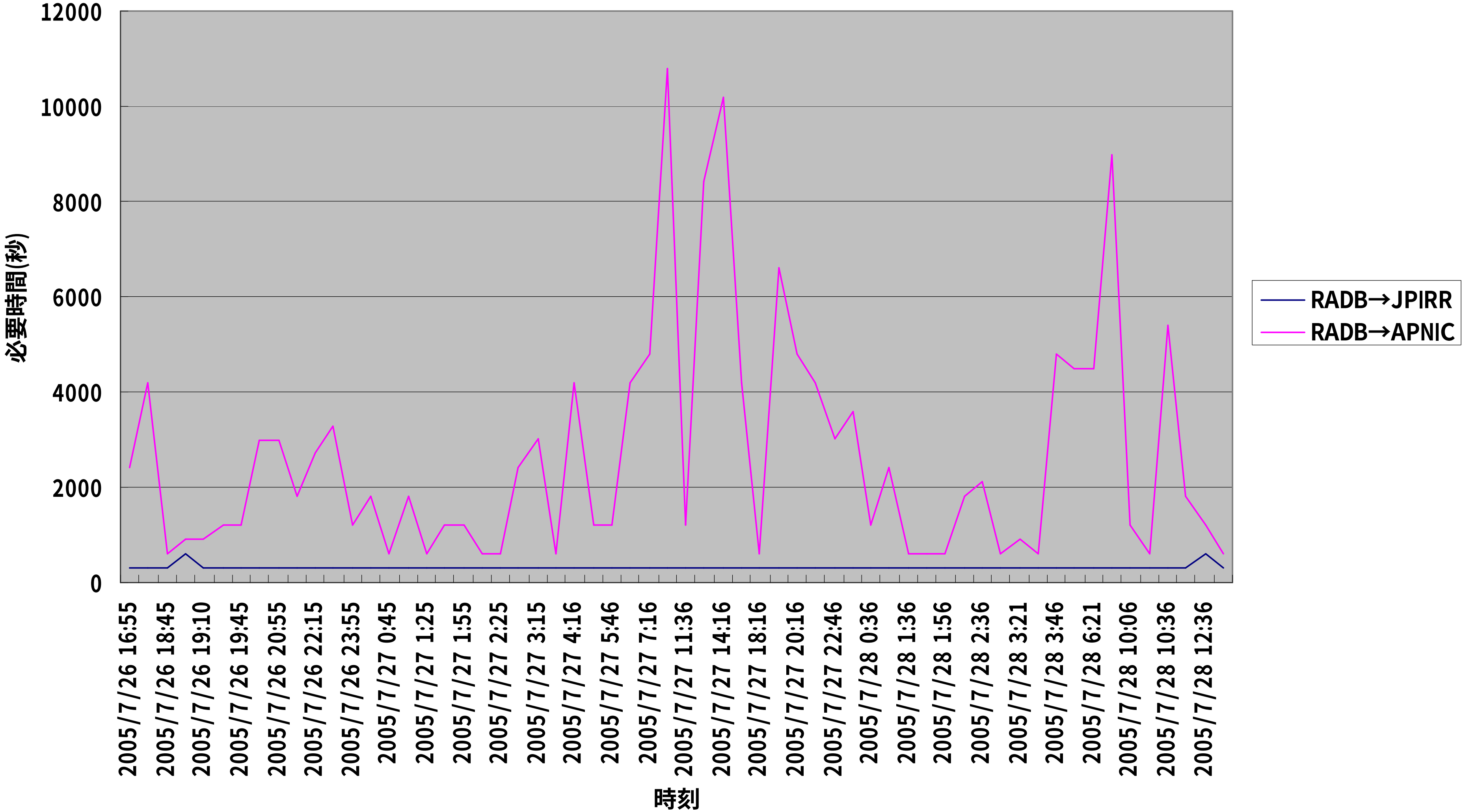


JPIRR→RIPE NCC



スパイクを除いたグラフ

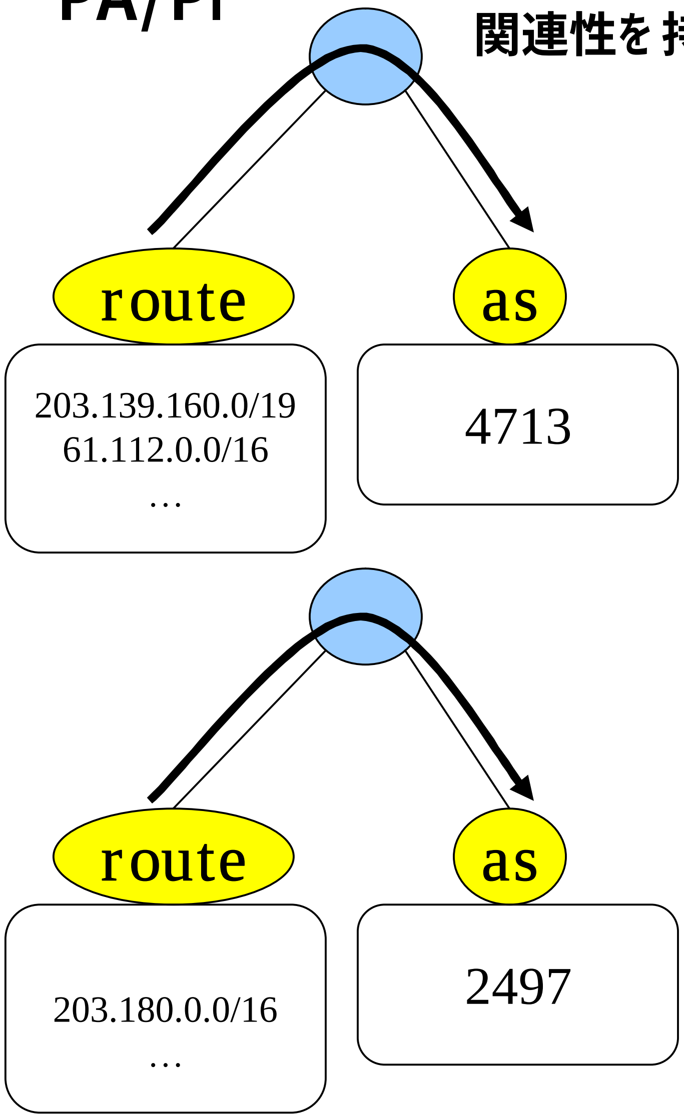
APNIC経由のRADB→JPIRR



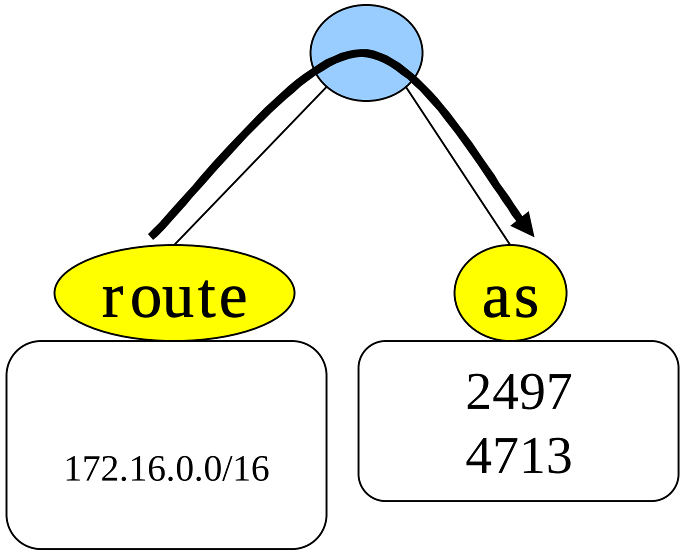
変更範囲の 検索 (1)

PA/PI

関連性を 持たせる



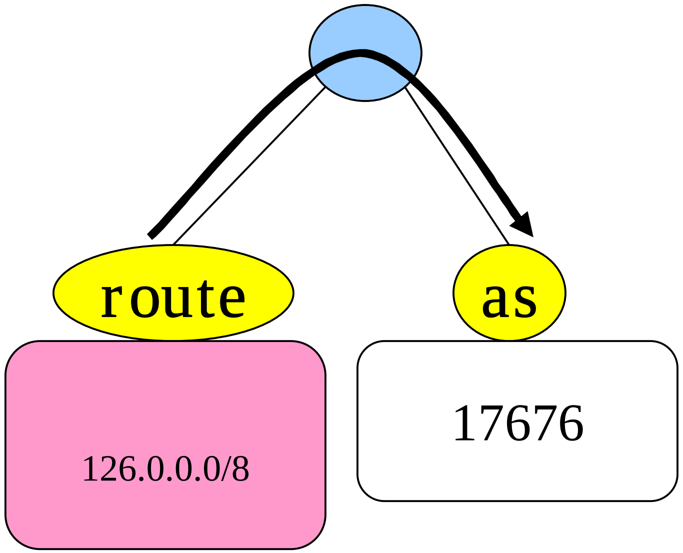
PI(multiple-origin)



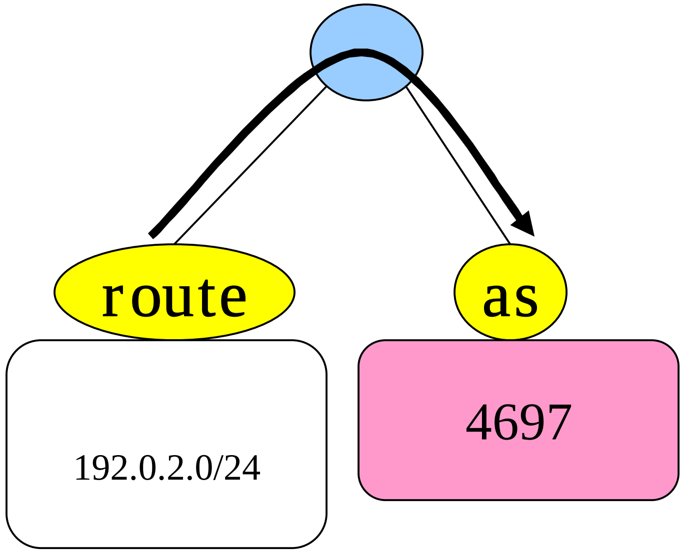
ここに書かれたツリー上で
辿れないものについては、
登録許可しない

変更範囲の検索 (2)

AS = JP
route = not-JP



AS = not-JP
route = JP



きちんと辿れるようなツリーを作る

JPIRRのすすむ道2

- 対象
  - 割り振り/割り当てを行ったレジストリが、リソースの正当性の保証を行うという観点から

    - IPアドレス管理指定事業者
    - JPNICが管理するプロバイダ非依存アドレスの割り当て先組織
    - JPNICよりASを取得している組織

  - オブジェクト検索は対象を限定せず
- 正式サービス開始:2005年第4四半期(予定)
- 費用:RADBのFeeを参考に、現在検討中

日本の経路＝JPIRR

(まずは) 日本の正しい経路データベースを作りたい

JPNICがIRとしてやるIRR

IPv6も今の段階からきちんとやっていく

BGPの経路情報の正当性を担保可能な、
日本を中心としたBGPオペレーションの元経路データベースができる

IRRを用いたBGPオペレーション

- 国内のＡＳ数もピア数もPATH数も増えてきて、そろそろ更新作業が大変
- 昔からやってきたAS PATHのオペレーションは、今の時代に合わなくなってきている
- 各ISPの入り口でしっかりフィルタがされていれば、変なPATHの経路が流れることはそうないだろうと想定して、、

IRRを使って自動化

- AS-Set オブジェクトを使う
  - 相手に as-set オブジェクトを事前に連絡しておいて、あとはそれを見てねというオペレーション

```
as-set:     AS-IIJ
descr:      ASes routed by IIJ
members:    AS112, AS2497, AS2504, AS2508, AS2515,
            AS2523, AS2526, AS2527, AS4459, AS4672,
            AS4685, AS4688, AS4695, AS4718, AS4723,
            AS4777, AS4996, AS6303, AS7500, AS7502,
            AS7511, AS7516, AS7517, AS7519, AS7521,
            AS7522, AS7524, AS7529, AS7531, AS7664,
            AS7668, AS7670, AS7671, AS7672, AS7679,
            AS7682, AS7684, AS7685, AS7686, AS7687,
                        :
```

```
as-set:     AS-OCN
descr:      ASes advertised by OCN
members:    AS4713,
            AS290,   AS2504,  AS2526,  AS4249,  AS4688,
            AS4710,  AS4711,  AS4718,  AS7502,  AS7511,
            AS7521,  AS7522,  AS7524,  AS7529,  AS7668,
            AS7671,  AS7672,  AS7674,  AS7676,  AS7682,
            AS7684,  AS7686,  AS9351,  AS9353,  AS9363,
            AS9368,  AS9370,  AS9374,  AS9601,  AS9602,
            AS9605,  AS9612,  AS9614,  AS9617,  AS9618,
                        :
```

- もう少しひねれるかな？

mnt-nfy attribute

- 各々ISPでやり取りしている update mail を IRRの object updateで代替する案

- mntner notify attribute ＝「mnt-nfy:」
  - 登録情報の変更時に通知されるメールアドレス
  - Prefixの追加削除時には、update情報が自動的に伝達される

ルートの追加例
192.0.2.0/24 = as18131

Dear Colleague,

This is to notify you that one or more objects in which you are designated for notification have been modified in the JPIRR routing registry database.

Diagnostic output:

The submission contained the following mail headers:

- From: yoshida@ocn.ad.jp
- Subject: test8
- Date: Wed, 20 Jul 2005 23:22:06 +0900
- Msg-Id: <20050720232206.75C1DCE0.yoshida@ocn.ad.jp>

NEW OBJECT CREATION:

route: 192.0.2.0/24
descr: JPIRRTEST
origin: AS18131
admin-c: JPIRR Operation Team
tech-c: JPIRR Operation Team
notify: irr-admin@nic.ad.jp
mnt-by: MAINT-JPIRR
changed: irr-admin@nic.ad.jp 20050720
source: JPIRR

JPNIC IRR (JPIRR) experiment service is provided by JPNIC.
If you have any questions, please send mail to
irr-admin@nic.ad.jp. - db-admin

作成したことが必要な人に伝達される
＝PREFIXが追加されたことがわかる

Subjectのフォーマットを統一、あるいは
通知される情報を必要十分な情報のみ
に限定するなど
（Subject例） JPIRR as18131 ADD 192.0.2.0/24

NEW OBJECT CREATION

フィルタに反映したことを伝達するには？
フィルタ反映確認はしているんだけど、
実際に流れてくるのはもっとあと。
それって確認するの大変

AS Set オブジェクトの変更例

PREVIOUS OBJECT:

as-set: AS-JPIRR
descr: ASes advertised by AS-JPIRR
members: AS18131
admin-c: JPIRR Operation Team
tech-c: JPIRR Operation Team
notify: irr-admin@nic.ad.jp
mnt-by: MAINT-JPIRR
changed: irr-admin@nic.ad.jp 20050720
source: JPIRR

REPLACED BY:

as-set: AS-JPIRR
descr: ASes advertised by AS-JPIRR
members: AS18131, AS2515
admin-c: JPIRR Operation Team
tech-c: JPIRR Operation Team
notify: irr-admin@nic.ad.jp
mnt-by: MAINT-JPIRR
changed: irr-admin@nic.ad.jp 20050720
source: JPIRR

差分がわかるような形で通知される工夫があると便利

Member: AS18131, AS2515

追加

提案

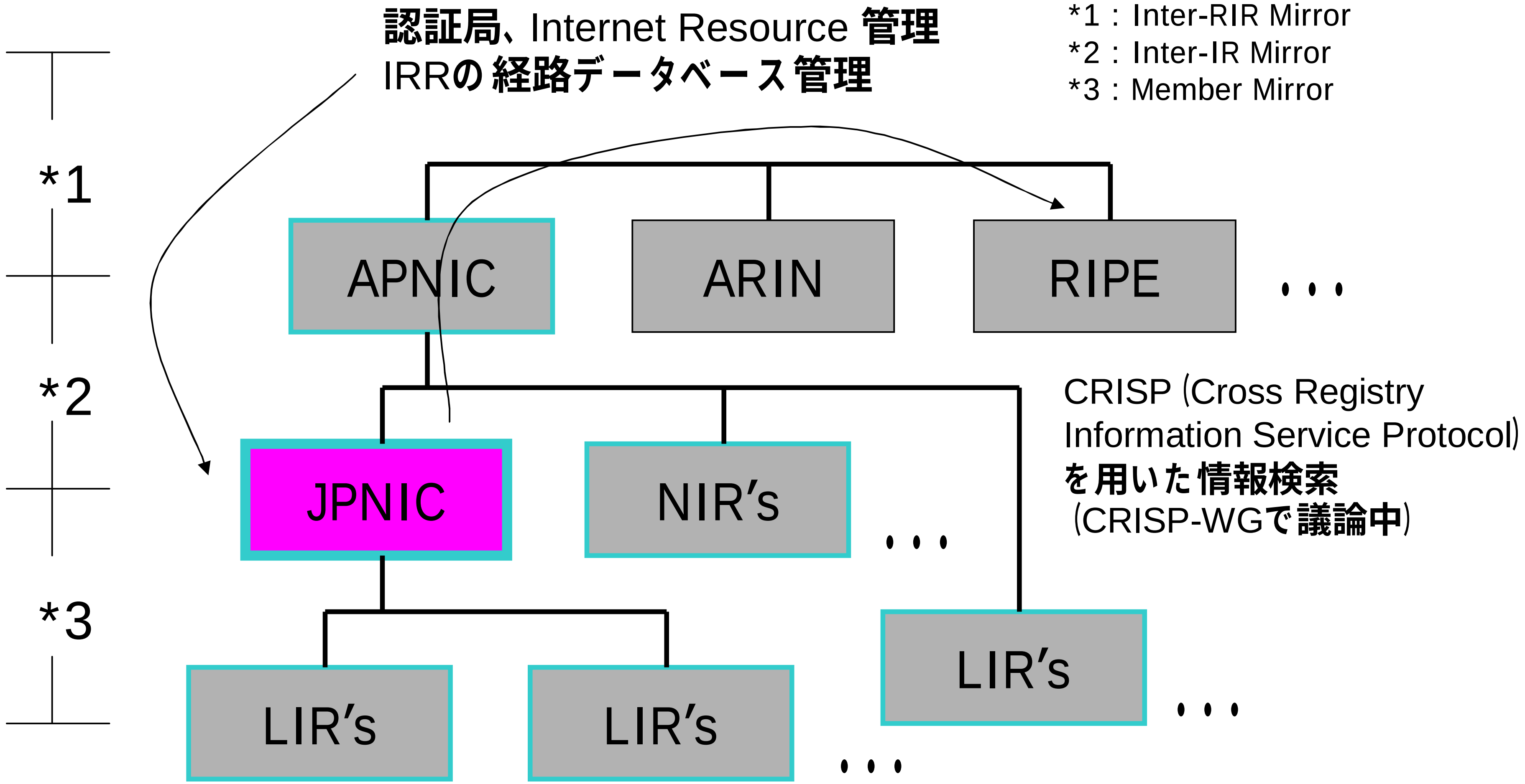
- 現在：メールで連絡、手動更新
    - ^(100_)+$
    - ^(100_)+(200_)+$
- 今後：as-set/prefix update から自動生成
    - as-pathでの filter
        - _100$
        - _200$
    - prefixでの filter
        - 10.100.0.0/16
        - 10.200.0.0/16
    - 上記の複合

Peer先のISPぐらいは
Prefixベースで（も）フィルタ
してもよいのでは

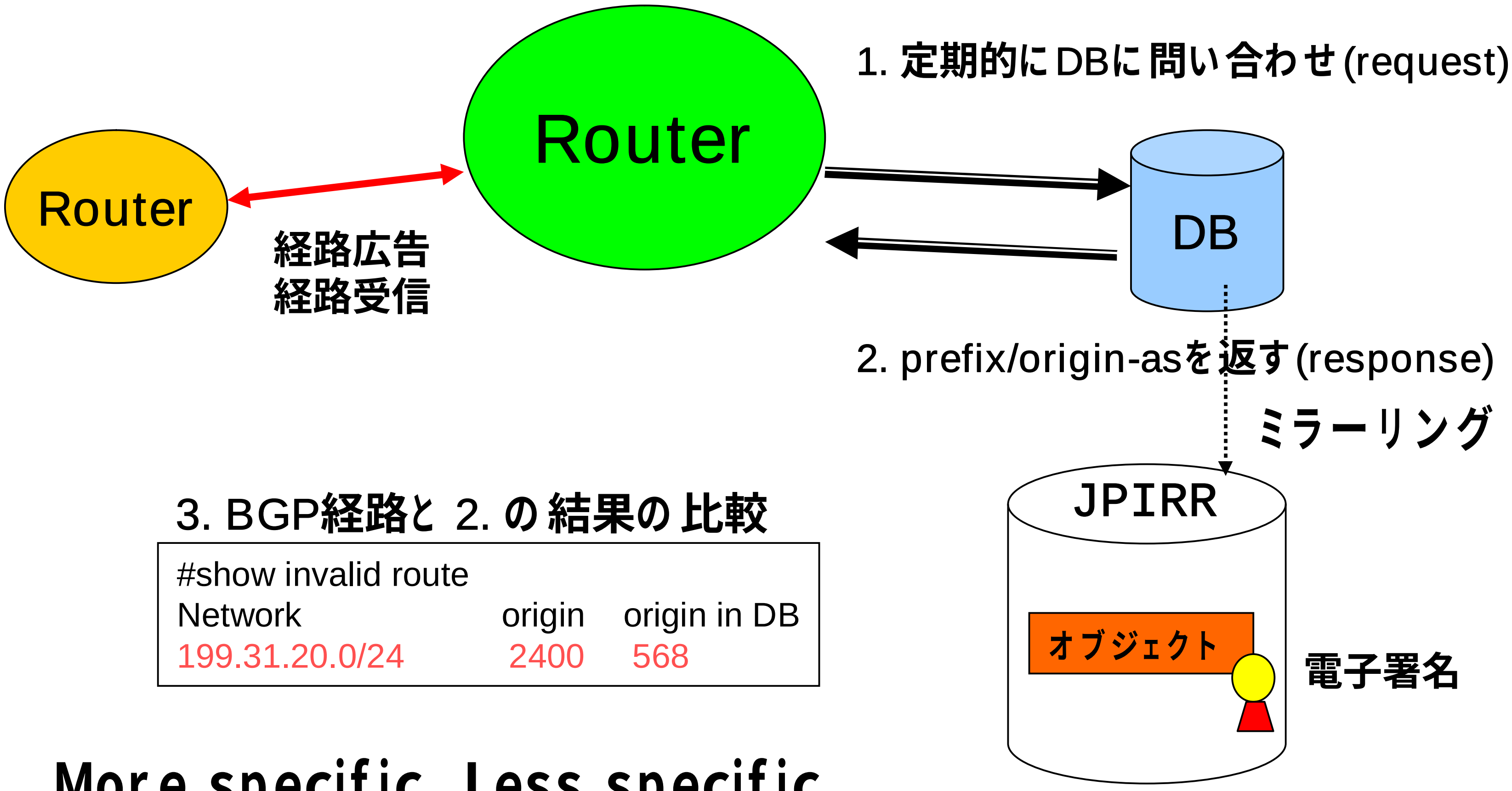
国際連携

- レジストリ階層構造に基づく運用
  - 各々のレジストリは自国あるいは自分の管理化のルート情報をきちんと管理していく
    - レジストリ間の連携
  - CRISP、(EPP)

IR階層モデル


認証局、Internet Resource 管理
IRRの 経路データベース管理
*1：Inter-RIR Mirror
*2：Inter-IR Mirror
*3：Member Mirror
*1
*2
*3
APNIC
ARIN
RIPE
・・・
JPNIC
NIR's
・・・
LIR's
LIR's
・・・
LIR's
・・・
CRISP（Cross Registry
Information Service Protocol）
を用いた情報検索
（CRISP-WGで議論中）

BGP+IRR

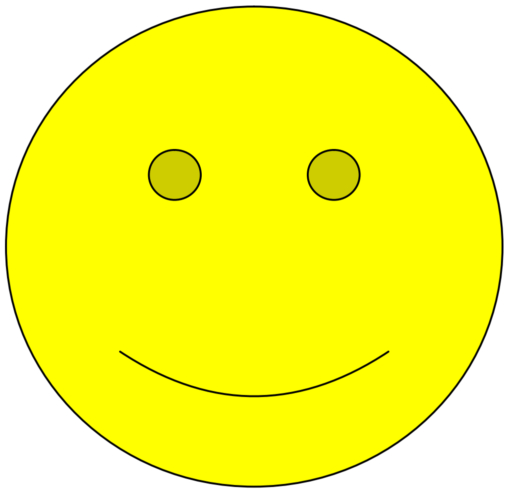


More specific、Less specific
Origin validation etc

あらかじめ証明書をCAから発行された人が電子署名付きでIRRのオブジェクトを登録する（アイディア）

IRRを用いたBGPオペレーション＝標準

- 経路データベースを利用した、信頼性、汎用性の高いBGPオペレーションを実現
- 日本で成功例を作って国外にもアピールし、国際的な連携や枠組みを作って行く



今後

メンテナー情報をおまちしております
　＝＞irr-admin@nic.ad.jp

試験的に、「mnt-nfy」を使ってBGP
オペレーションしてみませんか？

皆様のご意見をお待ちしております