

RPKIの技術課題と信頼構造

一般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
木村泰司

内容

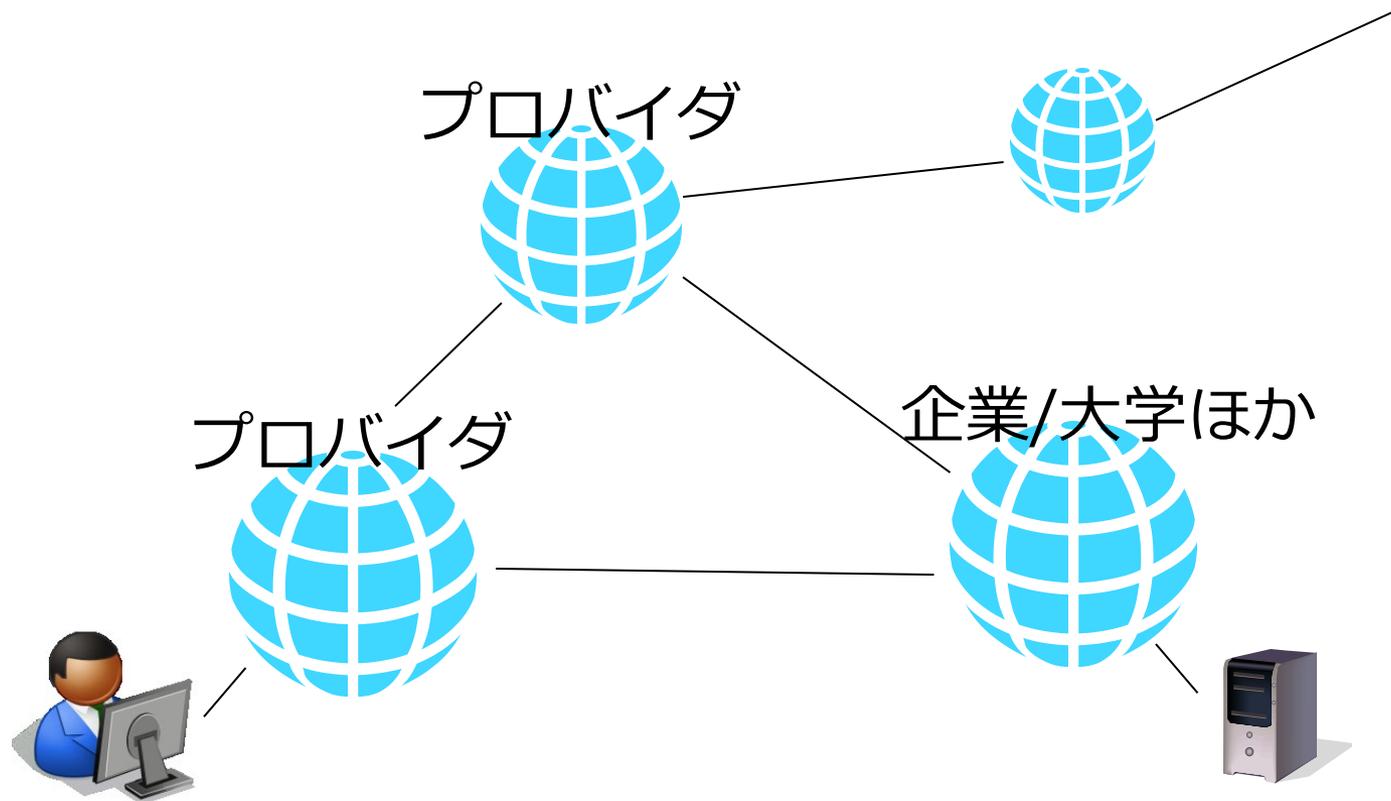
- インターネットとAS
- AS間ルーティングにおけるインシデント
- IPアドレス管理とRPKI
- Origin Validationの仕組みと現状
- 技術課題
- 信頼構造

インターネットとAS

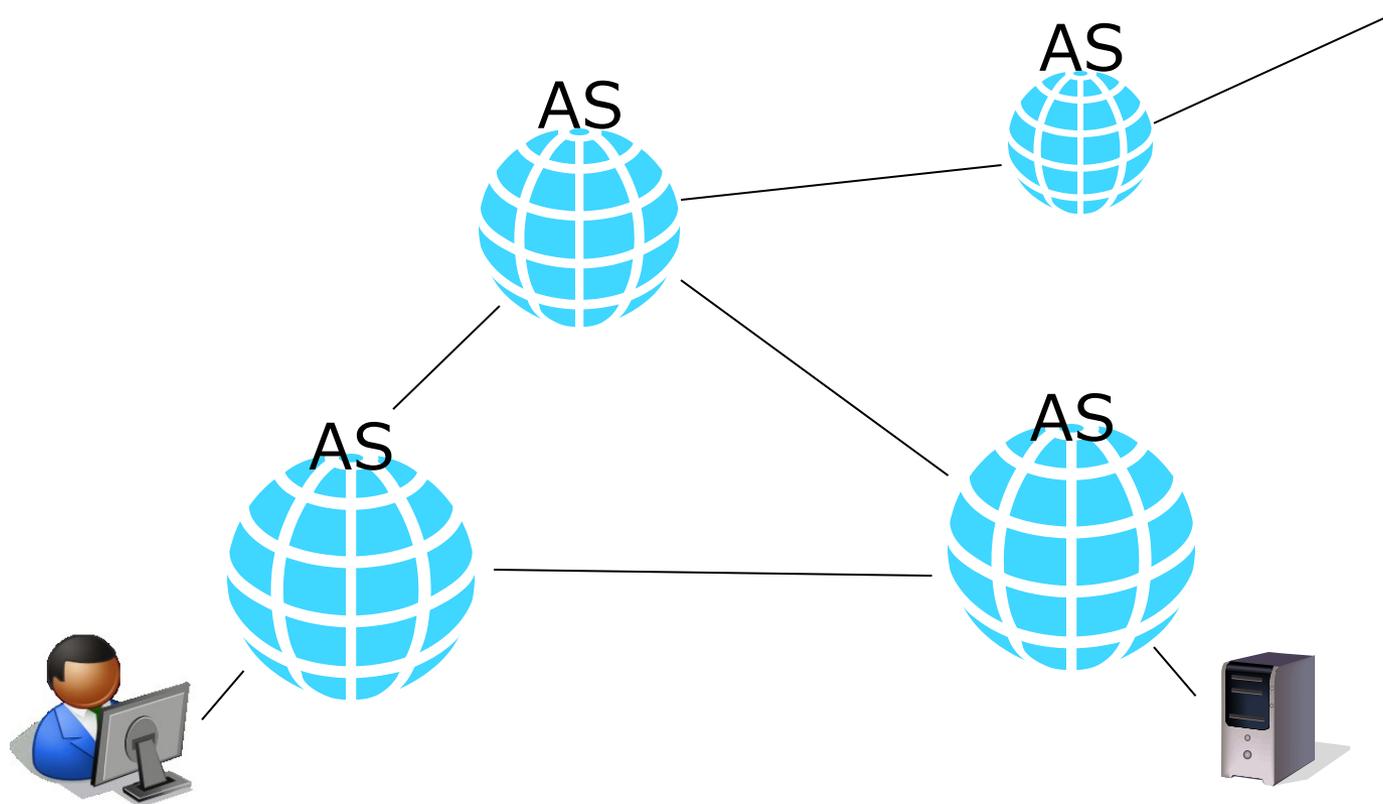
インターネットの姿（1）



インターネットの姿（２）

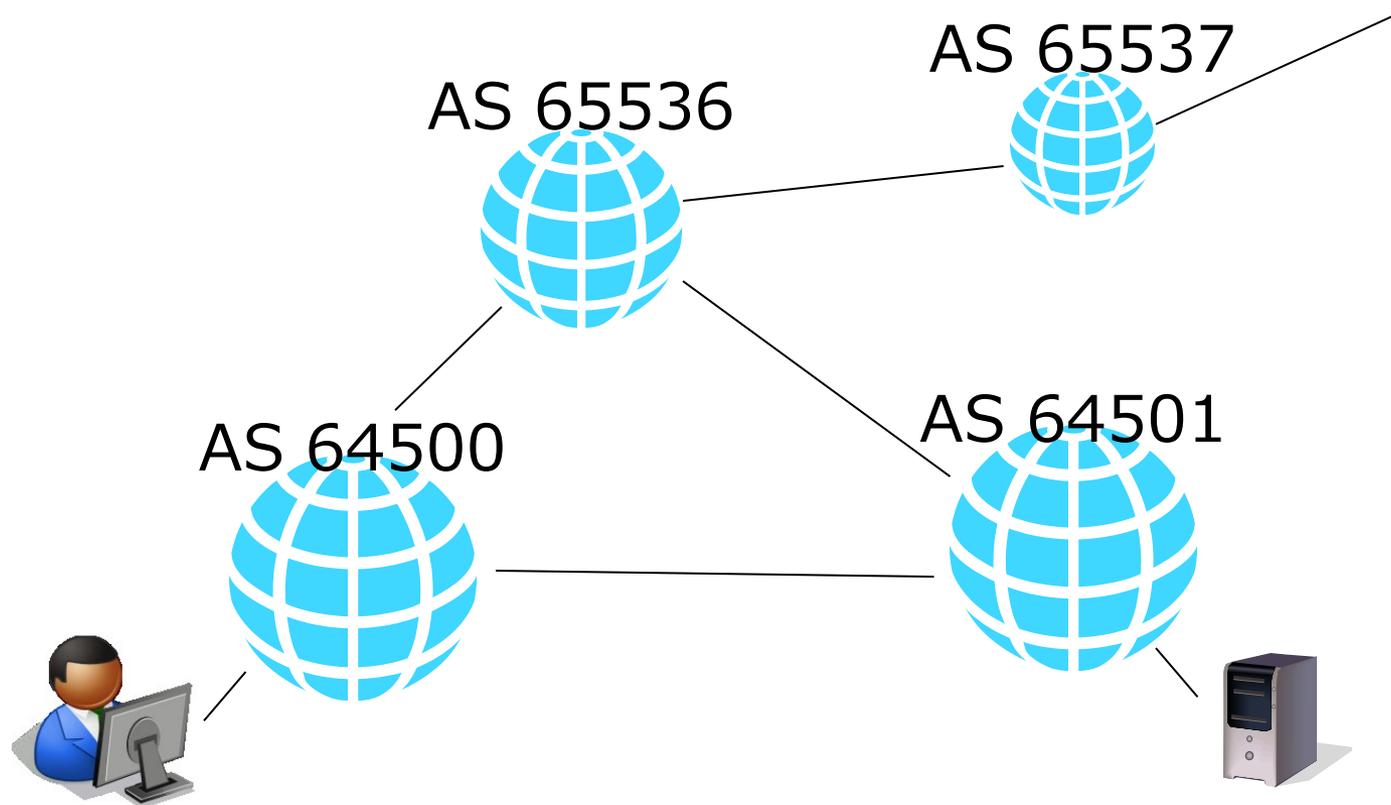


AS(Autonomous System) – 自律システム



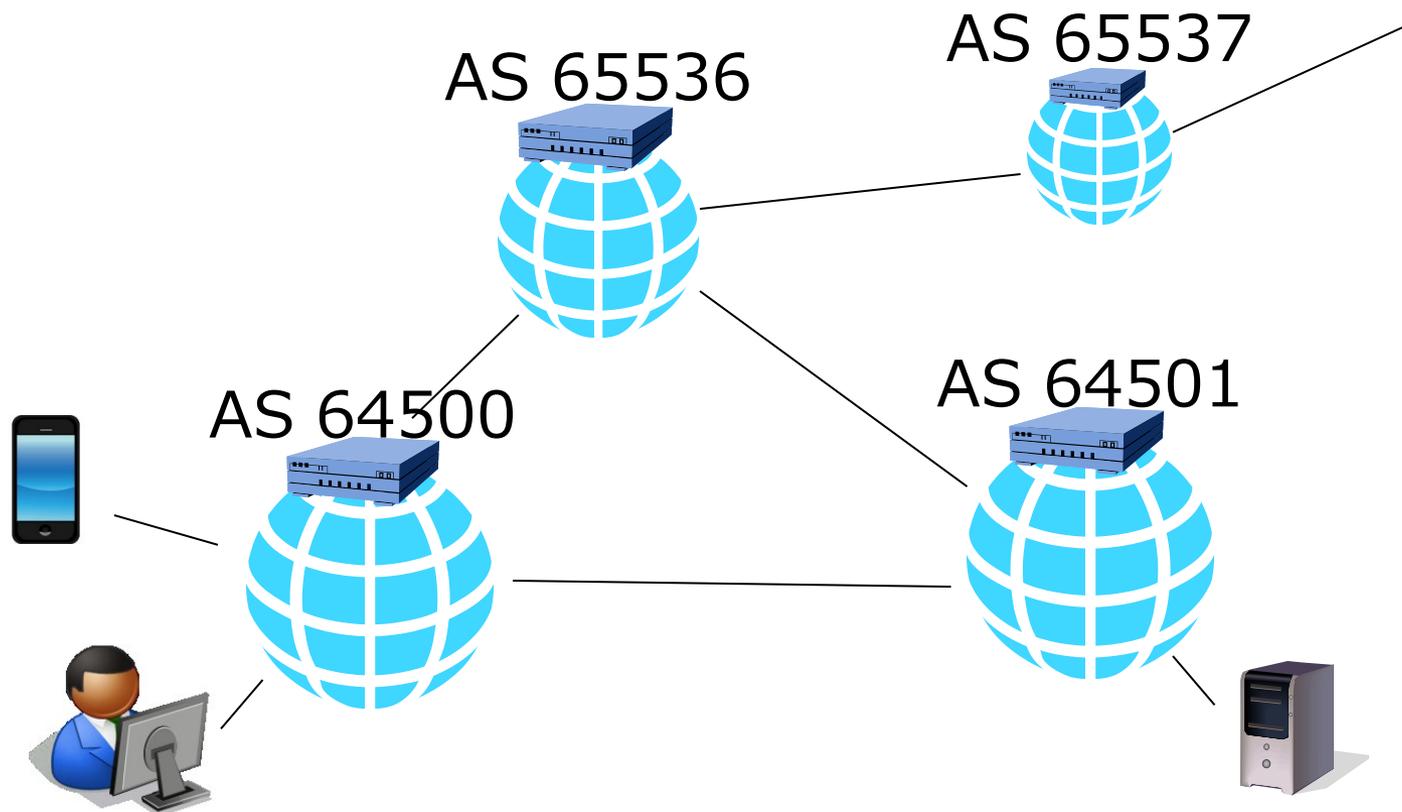
インターネットは、自律的なネットワークである「AS」のつながりによって構成されている。

AS番号



ASを識別する番号の「AS番号」は、JPNICのような「レジストリ」によって割り当てられる。

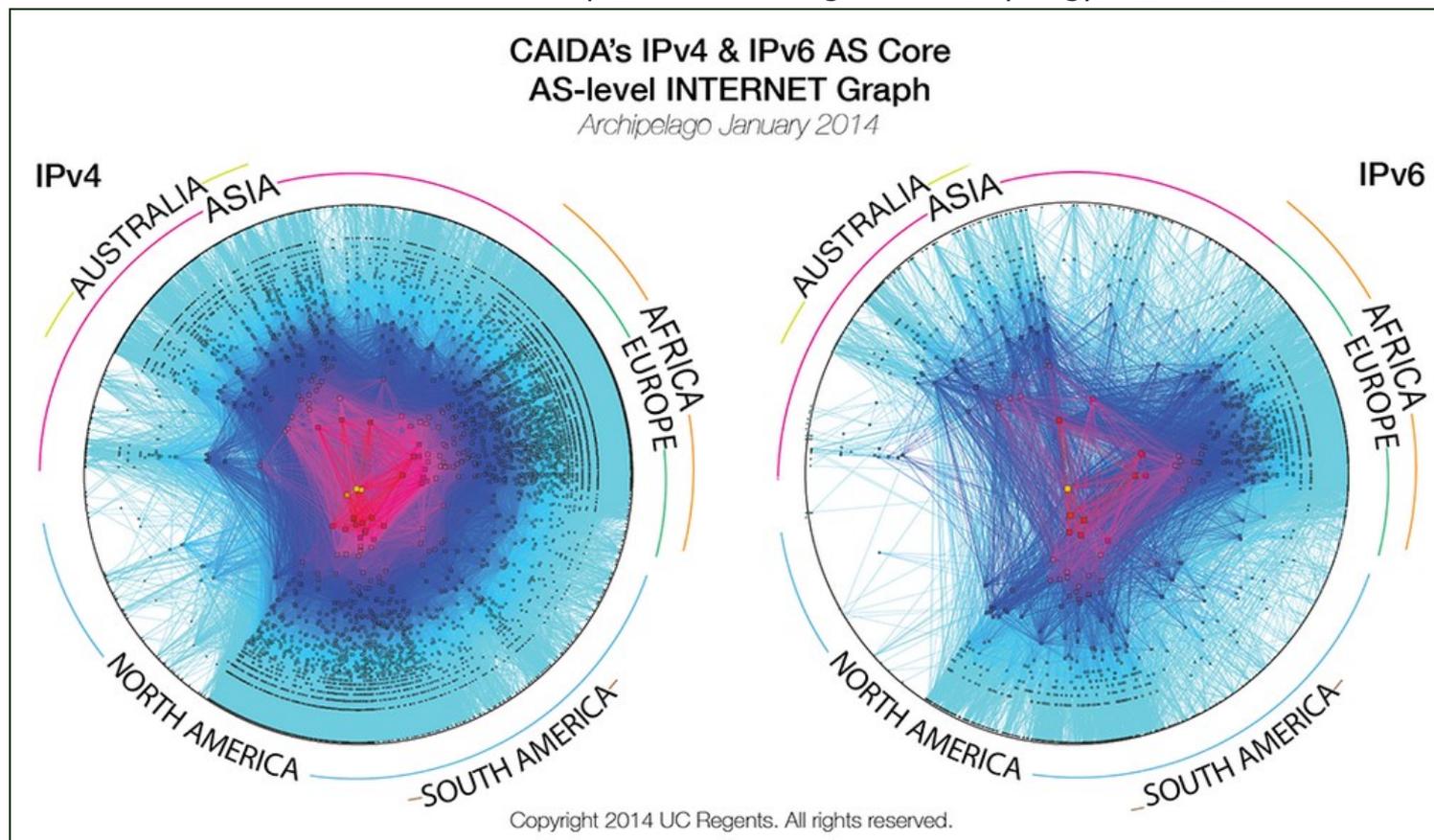
AS間ルーティングとBGP



ASで収容されているIPアドレスは「経路情報」と呼ばれ「BGP」を使って伝播される。

インターネットとASのつながり

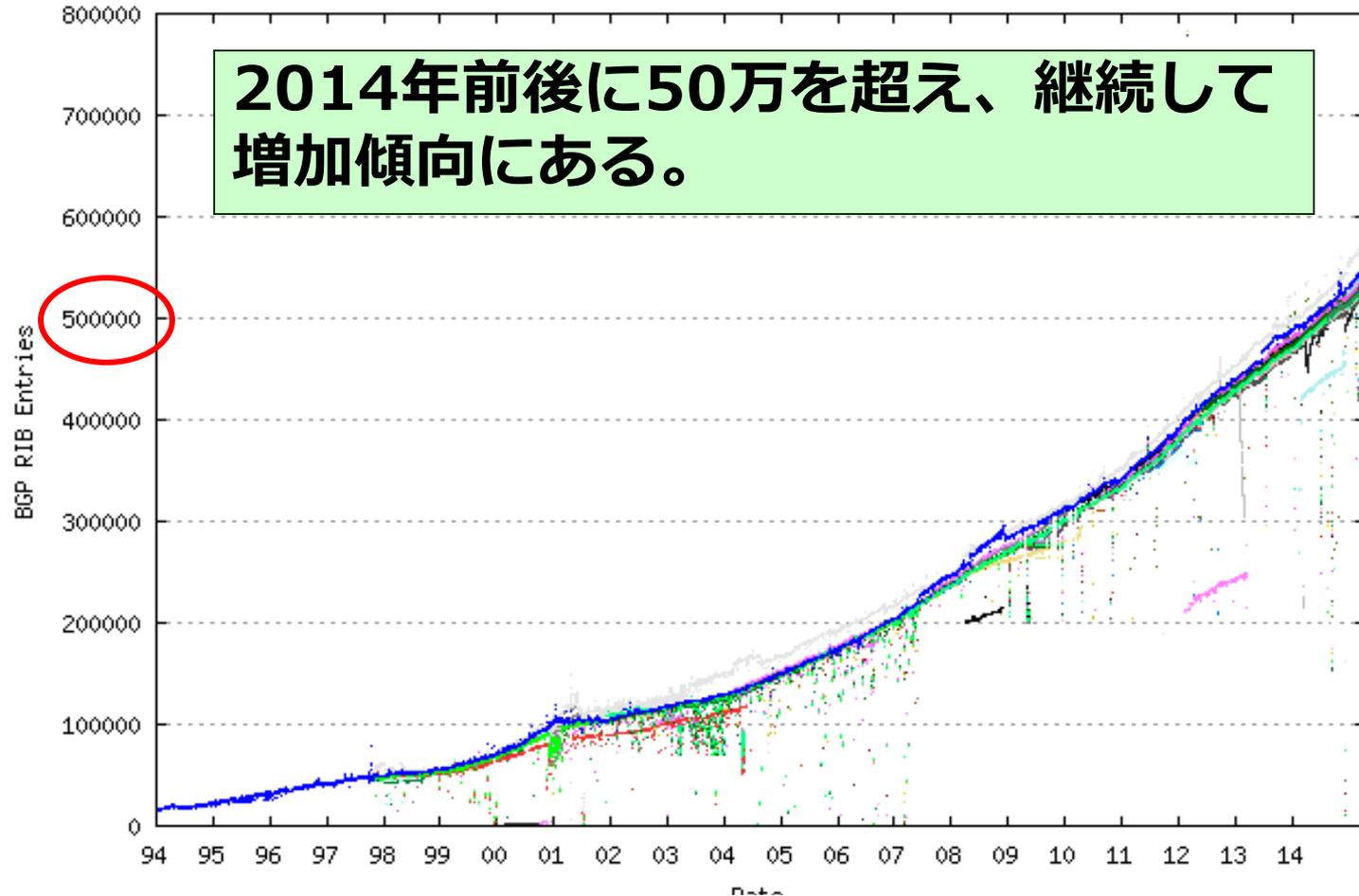
IPv4 and IPv6 AS Core: Visualizing IPv4 and IPv6 Internet Topology at a Macroscopic Scale in 2014
http://www.caida.org/research/topology/as_core_network/2014/



現在のAS番号割り当て数 **79,870**

The 32-bit AS Number Report
<http://www.potaroo.net/tools/asn32/>

BGPにおける経路情報の数

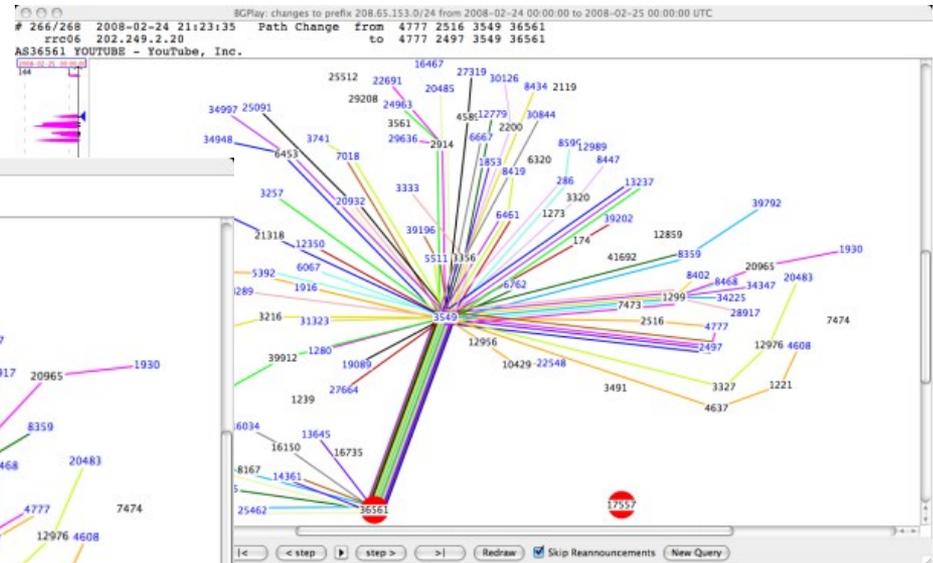
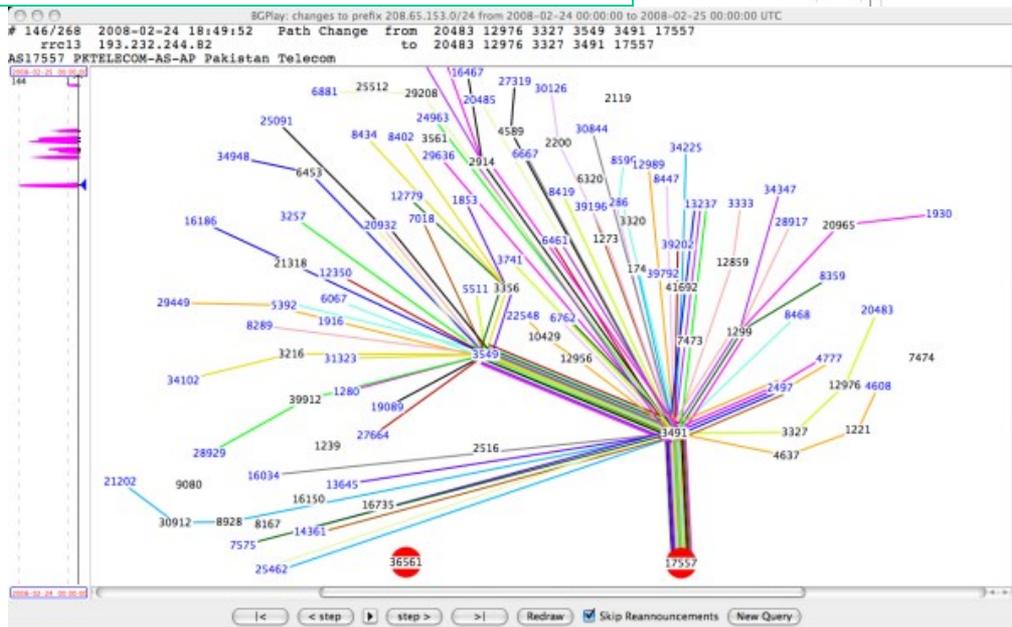


BGP Statistics from Route-Views Data, 2 April, 2015
<http://bgp.potaroo.net/bgprpts/rva-index.html>

AS間ルーティングにおけるインシデント

2008年のYouTubeインシデント

インシデント発生時



平常時

YouTube Hijacking: A RIPE NCC RIS case study, 17 Mar 2008, RIPE NCC,
<http://www.ripe.net/internet-coordination/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study>

YouTubeの経路情報が別のASによって広告され、
約2時間半の間、アクセスできなくなった。

```
show router bgp routes 8.8.8.8
```

```
=====
```

```
BGP Router ID:212.156.116.127 AS:9121 Local AS:9121
```

```
=====
```

```
Legend -
```

```
Status codes : u - used, s - suppressed, h - history, d - decayed, * - valid
```

```
Origin codes : i - IGP, e - EGP, ? - incomplete, > - best, b - backup
```

```
=====
```

```
BGP IPv4 Routes
```

```
=====
```

```
Flag Network LocalPref MED
```

```
Nexthop Path-Id VPNLabel
```

```
As-Path
```

```
-----
```

```
u*>? 8.8.8.8/32 100 None
```

```
212.156.253.130 None -
```

```
No As-Path
```

```
*? 8.8.8.8/32 100 None
```

```
212.156.253.130 None -
```

```
No As-Path
```

```
-----
```

```
Routes : 2
```

```
=====
```

GoogleパブリックDNSのIPアドレスを持つ、別のDNSサーバに誘導される状況を示している。

We would expect to see 8.8.8.0/24 here originated by AS 15169.

This is the proof of Turk Telekom hijacking Google DNS.

Turkey Hijacking IP addresses for popular Global DNS providers,
Posted by Andree Toonk - March 29, 2014, BGPMON

<http://www.bgpmon.net/turkey-hijacking-ip-addresses-for-popular-global-dns-providers/>

Origination of 46.244.81.0/24 (Mada Network)

07 Jan 2015 - 09 Jan 2015 (Times in UTC)



他のASによる経路情報は、国際的な観測地点のASのうち約50%で観測されたという報告がある。

Source: BGP Data



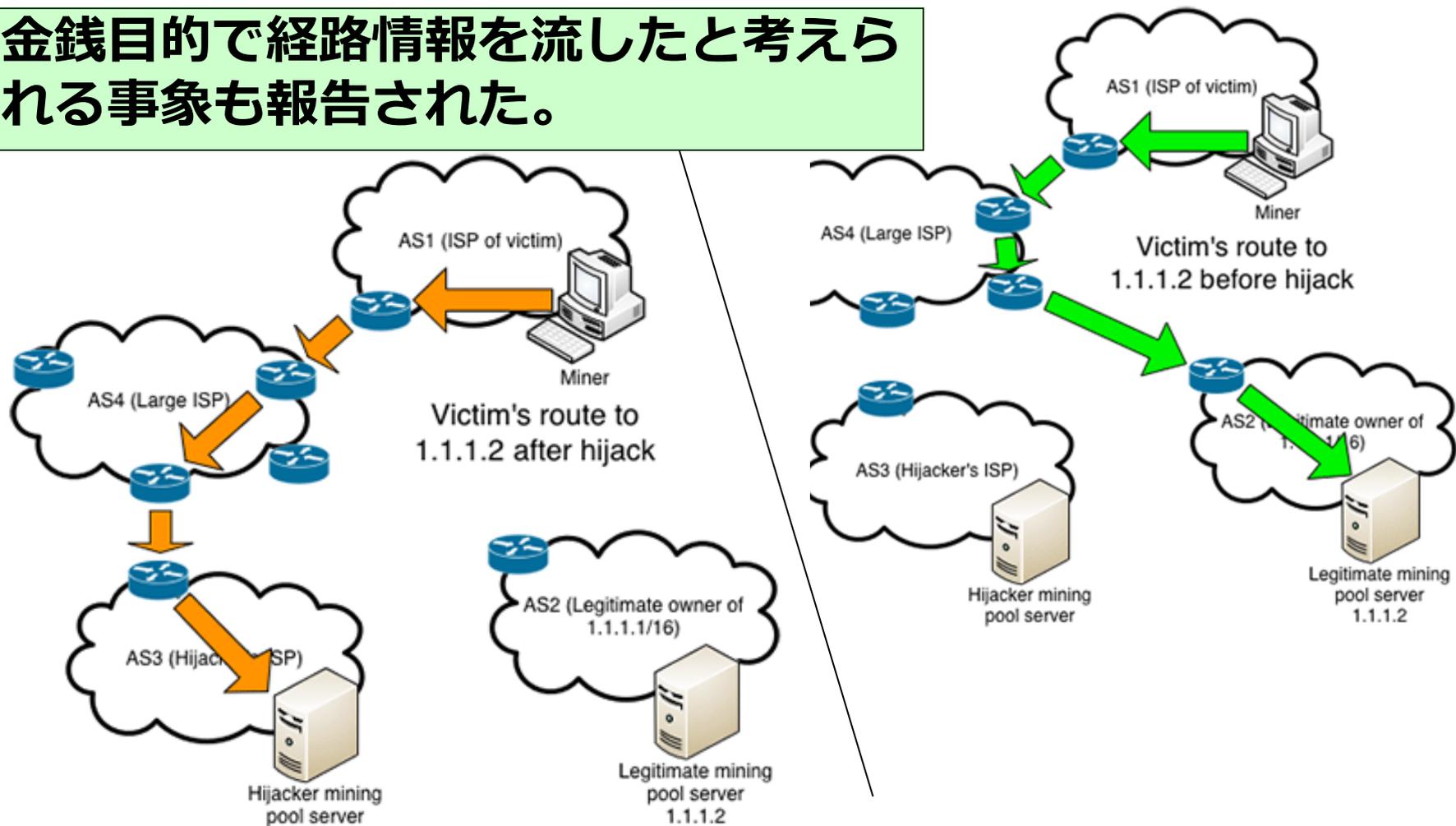
On-going BGP Hijack Targets Palestinian ISP, Apr 10, 2015, Dyn Research
<http://research.dyn.com/2015/01/going-bgp-attack-targets-palestinian-isp/#!prettyPhoto>

AS間のルーティングにおいては…

- インターネットにおける到達性が大規模に失われたり、本来とは異なるサーバに誘導される可能性がある。
 - ただし、DDoSを避けるため、といった目的で意図的に行われることもある。

Bitcoinのマイニングプールへの経路をハイジャック

金銭目的で経路情報を流したと考えられる事象も報告された。



BGP Hijacking for Cryptocurrency Profit, 7 August 2014

Pat Litke and Joe Stewart, Dell SecureWorks Counter Threat Unit

<http://www.secureworks.com/cyber-threat-intelligence/threats/bgp-hijacking-for-cryptocurrency-profit/>

国内における観測



AS番号が本来とは異なる疑いのある経路情報が毎月平均で10件程度観測されている。(JPIRRの登録情報との比較)

AS間ルーティングに必要なものは…

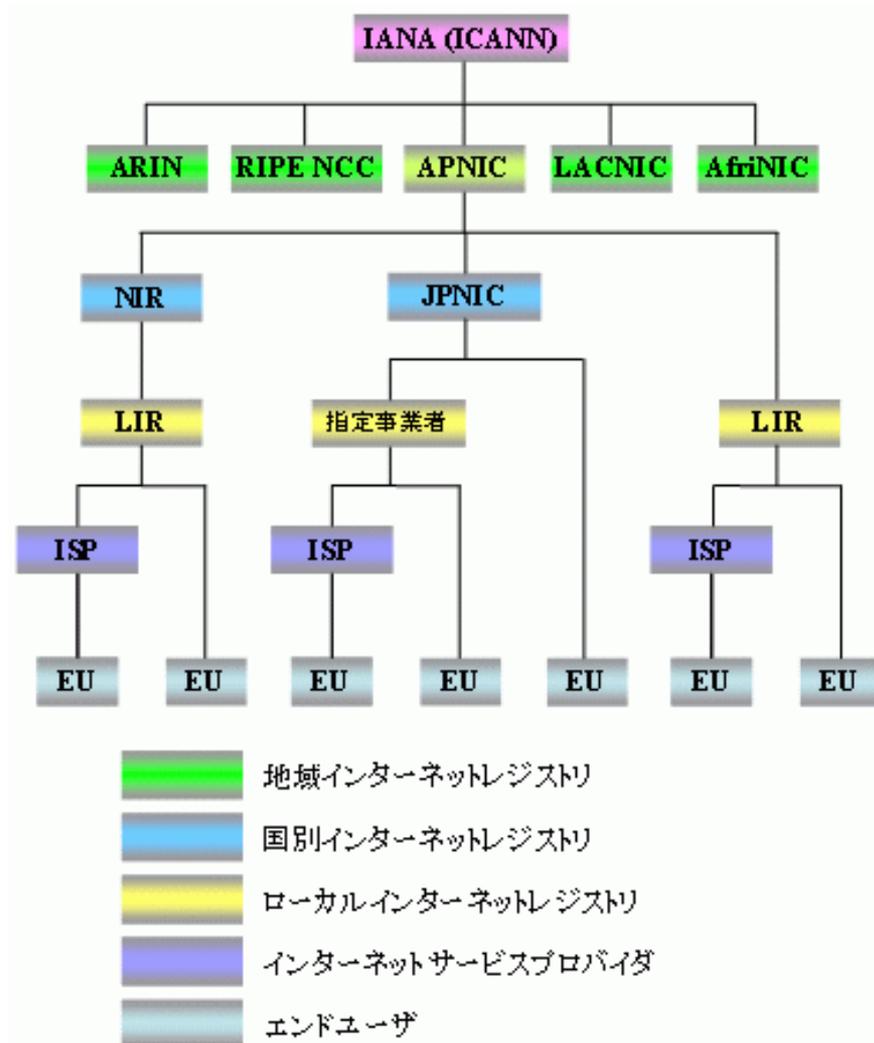
- **IPアドレスとASの正しい情報**
 - IPアドレスの割り当てを受けている方が把握している「本来の」ASによって経路情報が広報されているかどうか
 - IPアドレスが正しく割り当てられたものかどうか
- **伝達してきた経路情報に対する判断の仕組み**
 - 伝播してきたBGPメッセージに含まれるIPアドレスやAS番号に対して、正しさを確認できる仕組み

IPアドレス管理とRPKI

IPアドレス管理（1）

- **IPアドレスの階層的な管理**
 - IPアドレスはIANA（Internet Assigned Numbers Authority）によって5つのRIR（Regional Internet Registry）に割り振られ、更に地域ごとに階層的に管理されている。
- **ネットワーク情報の登録**
 - IPアドレスの割り振り／割り当ての情報（ネットワーク情報）は、階層ごとのInternet Registryに登録され、WHOISなどを通じてネットワーク運用のために利用される。

IPアドレス管理（2）



IPアドレス管理とルーティング

- **IPアドレス管理**

- インターネットレジストリ (Internet Registry) によってネットワークを持つ組織などに割り当てられるもの

- **ルーティング**

- ISPなどの接続性を提供する組織などが、ルータの設定を通じて行うもの

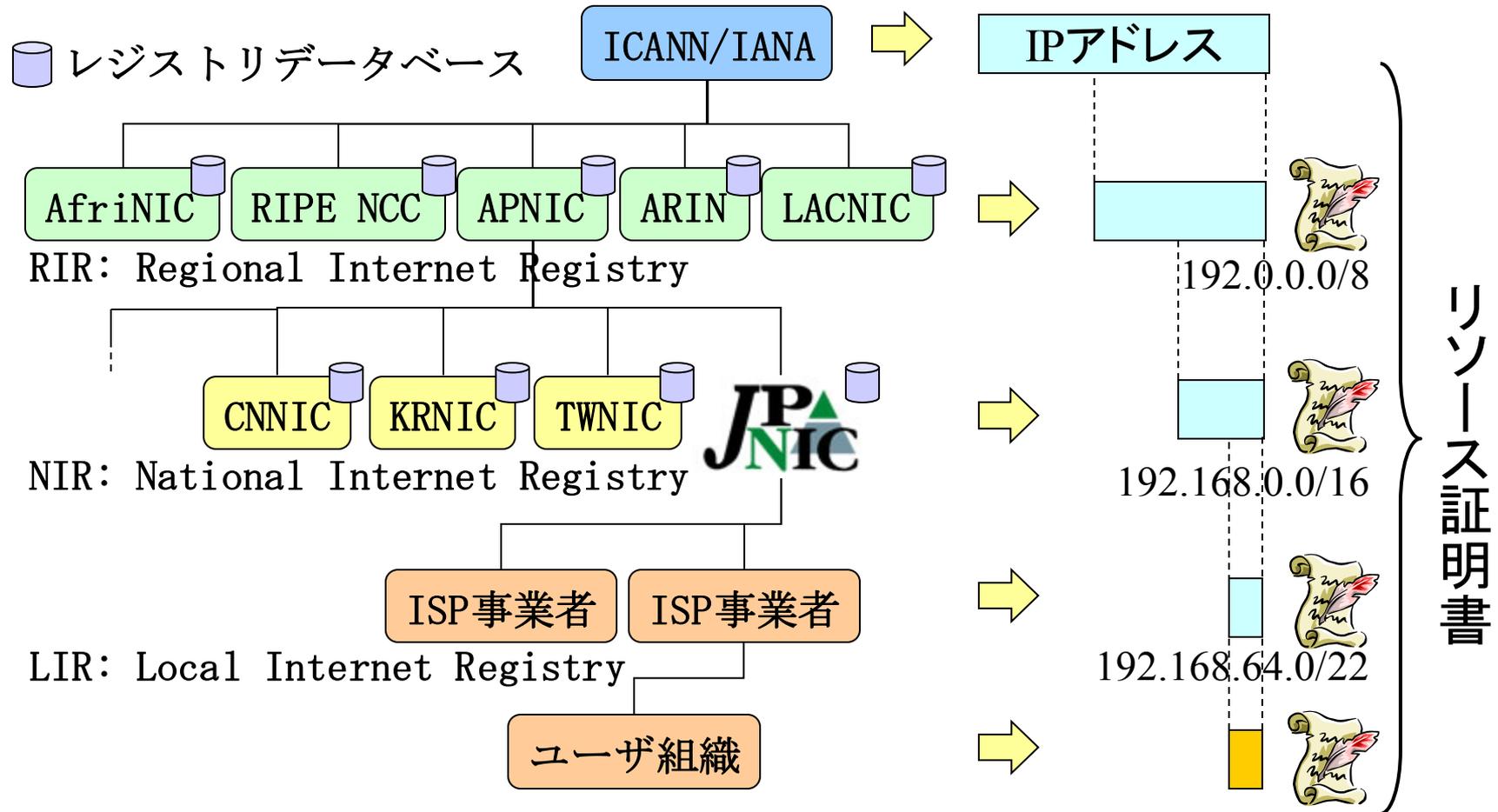
IPアドレス管理とルーティングは、これまでは技術的に連動していなかったと言える。

RPKI

- **Resource Public-Key Infrastructure**
 - IPアドレスやAS番号といった番号資源 (Number Resource) の割り振り／割り当てを証明するPKI
 - 1997年頃、Stephen Kent氏 (BBN Technologies) によって提案され、IETF (Internet Engineering Task Force) で仕様策定が行われている。

**IPアドレスの割り振り／割り当てを証明する
「リソース証明書」のためのPKI**

リソース証明書



リソース証明書の例

Certificate:

Data:

Version: 3 (0x2)

Serial Number: 1 (0x1)

Signature Algorithm: sha256WithRSAEncryption

Issuer: CN=D5BBADA3

Validity

Not Before: Apr 15 10:24:39 2014 GMT

Not After : Apr 14 10:24:39 2019 GMT

Subject: CN=D5BBADA3

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (2048 bit)

sbgp-autonomousSysNum: critical

Autonomous System Numbers:

0-4294967295

sbgp-ipAddrBlock: critical

IPv4:

0.0.0.0/0

IPv6:

::/0

X509v3 extensions:

X509v3 Basic Constraints: critical

CA:TRUE

X509v3 Subject Key Identifier:

18:CE:ED:52:F0:99:02:8A:58:3C:F1:7B:53:71:0E:1F:5D:37:4F:8D

X509v3 Key Usage: critical

Certificate Sign, CRL Sign

Subject Information Access:

CA Repository - URI:rsync://rpki01.nic.ad.jp/repository/

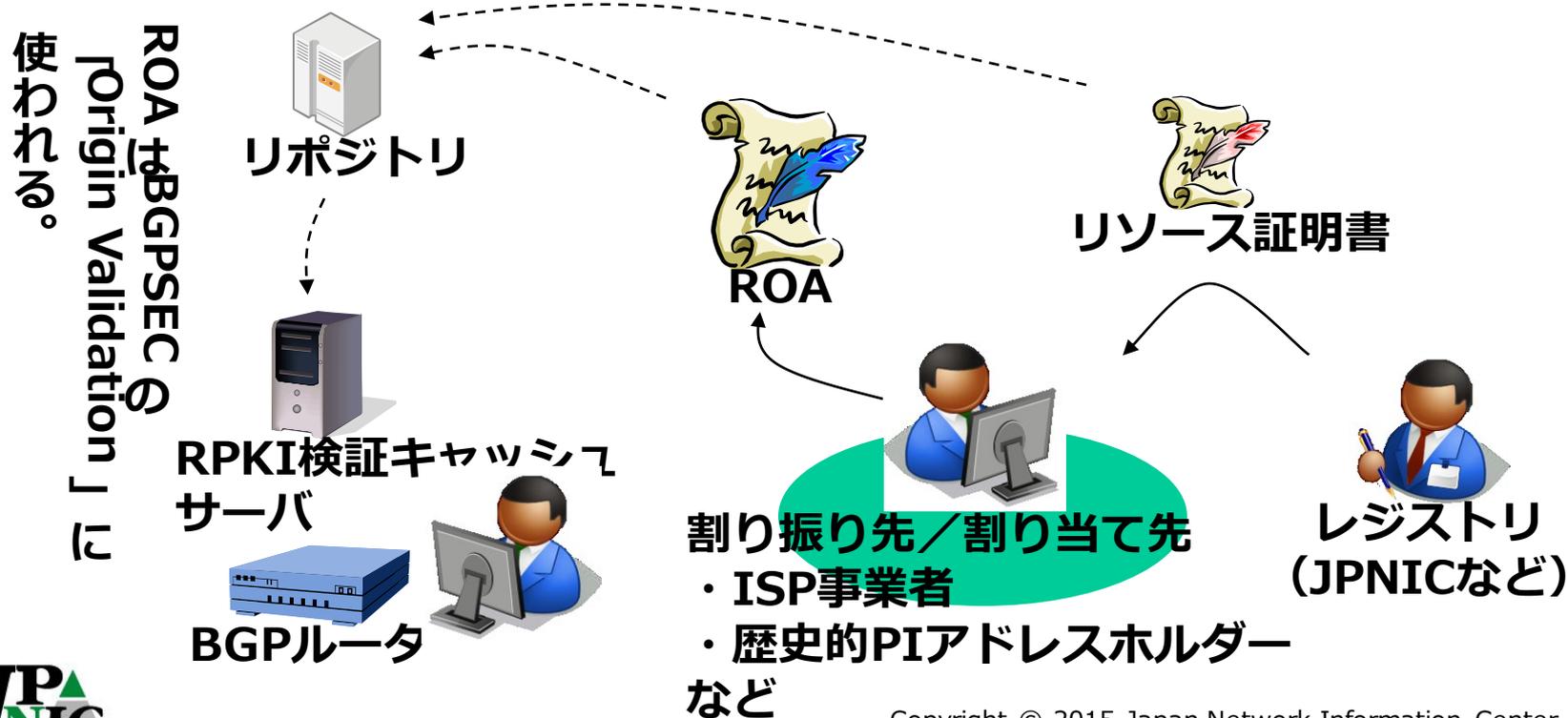
1.3.6.1.5.5.7.48.10 - URI:rsync://rpki01.nic.ad.jp/repository/jpnic-ta-03.mft

Origin Validationの仕組みと現状

リソース証明書とROA

• Route Origination Authorization

- IPアドレスのホルダーによる署名付きデータで、割り当てられたIPアドレスの経路広告を特定のASから経路広告することを認可したことを示す。



Origin Validationの仕組み

- **RPKIキャッシュ**

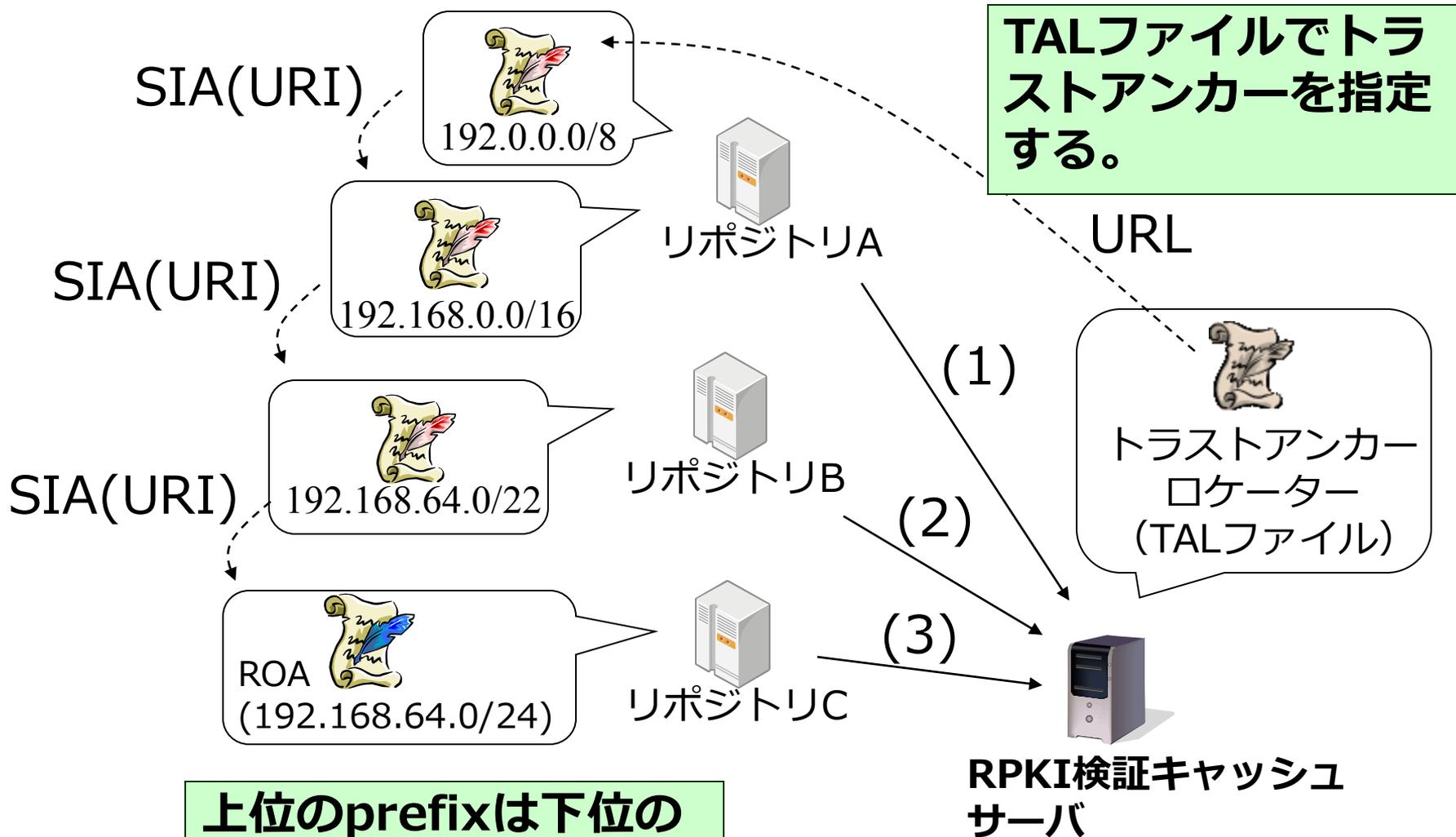
- リソース証明書の署名検証を通じて、IPアドレスが正式に割り当てられたものであることを確認
- ROAの署名検証を通じて、経路広告元のAS番号が正式なIPアドレスの割り当て先によって指定されたものであることを確認

- **BGPルータ**

- BGP Updateメッセージとして伝播してきたIPアドレスprefixと経路広告元のAS番号を確認

BGPルータにおいて、BGP経路情報の中の不適切なIPアドレスや本来とは異なる経路広告元が検出できる。

トラストアンカーと署名検証



TALファイル – trust anchor locator

TALファイルの例

rsync://rpki-repository.nic.ad.jp/ta/jpnic-preliminary-ca-s1.cer

MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAnjfovjOzuZP5zOT5iHtB
3z35k9uarx3ltKHrh4eq1xO4f7i0Dt/VEsqLJxubfuRPUwskaH/96ewzqeeL9iPv
vGHL479kJ6YrhN7StkNXLVePwx4uHe7DWuw0CSsRCLCu+SssWTiXyEp3olkgutUV
mwZrNZ1aCfi8tvibz44v1iYvOYcTXRXgvwneJbxepqt+2xchHwMrjBIWsexdqVK7
1/iMHXChEr6wCzZyFW2rJjeFEAF6nFnu1DDhb1bSve+PEd4PmrQ5vNeYkcffC3dL
Y8ZrjCU51LFD441EA8ae0gDRBnnD7+O3J0rjUi+Y34xLu5XSw8nDordErnX31sqV
XwIDAQAB

署名検証するためには、入手済みのTALファイルを読み込んでトラストアンカーの証明書をダウンロードする。

ROA – Route Origination Authorization

ROAの内容表示

```
$ cd /var/rcynic/data/authenticated/rpki-repository.nic.ad.jp/  
$ print_roa 1003/6gaLktvYFfRfkbwTJnYU-STtxYI.roa  
ROA Version: 0  
SigningTime: 2015-03-20T11:12:21Z  
asID: 2515  
addressFamily: 1  
  IPAddress: 192.41.192.0/24  
  
$ print_roa publication/1003/HKEK_75JQYmCWP26zFDz2IcXSIg.roa  
ROA Version: 0  
SigningTime: 2015-03-20T11:12:21Z  
asID: 2515  
addressFamily: 1  
  IPAddress: 202.11.240.0/21  
$
```

ROAには署名日時とAS番号、IPアドレスの範囲が記載されている。

RPKIの現在

- **RIRのリソース証明書の開始**
 - 5つのRIRでリソース証明書の提供がすでに行われている。
 - アジア太平洋地域のNIRでは、2015年3月3日にJPNICが試験提供を開始した。
- **Origin Validation実装の安定化**
 - Cisco、Juniper、Alcatelといった大手ルータベンダーのサポートが始まっている。

国際的な普及の状況

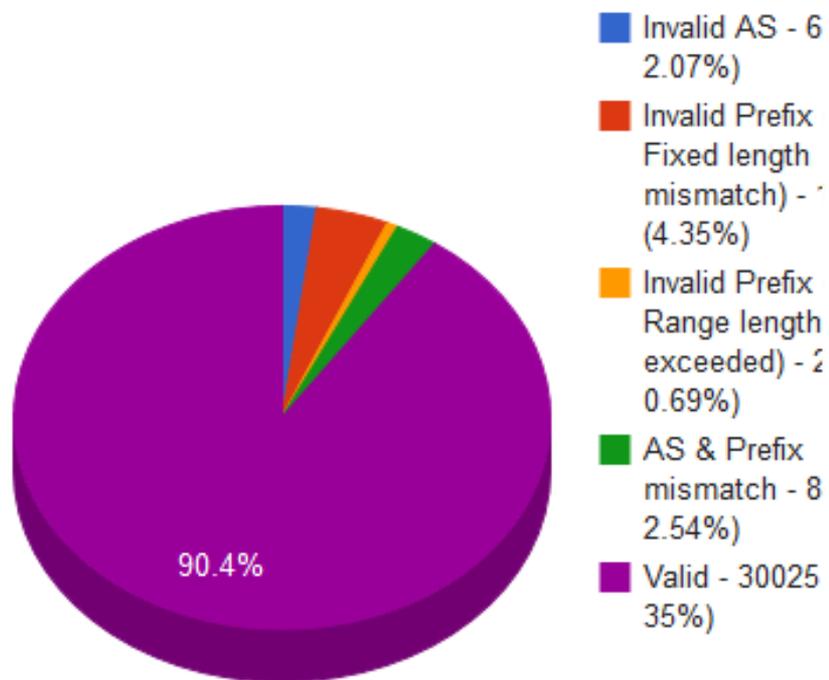
RPKI Dashboard, SURFnet, 2015/4/3
<http://rpki.surfnet.nl/>

RIR	Total	Valid	Invalid	Unknown	Accuracy	RPKI Adoption Rate
AFRINIC	12664 (100%)	52 (0.41%)	45 (0.36%)	12567 (99.23%)	53.61%	0.77%
APNIC	142987 (100%)	1059 (0.74%)	661 (0.46%)	141267 (98.8%)	61.57%	1.2%
ARIN	205818 (100%)	1339 (0.65%)	325 (0.16%)	204154 (99.19%)	80.47%	0.81%
LACNIC	72797 (100%)	16573 (22.77%)	970 (1.33%)	55254 (75.9%)	94.47%	24.1%
RIPE NCC	146611 (100%)	12960 (8.84%)	1349 (0.92%)	132302 (90.24%)	90.57%	9.76%

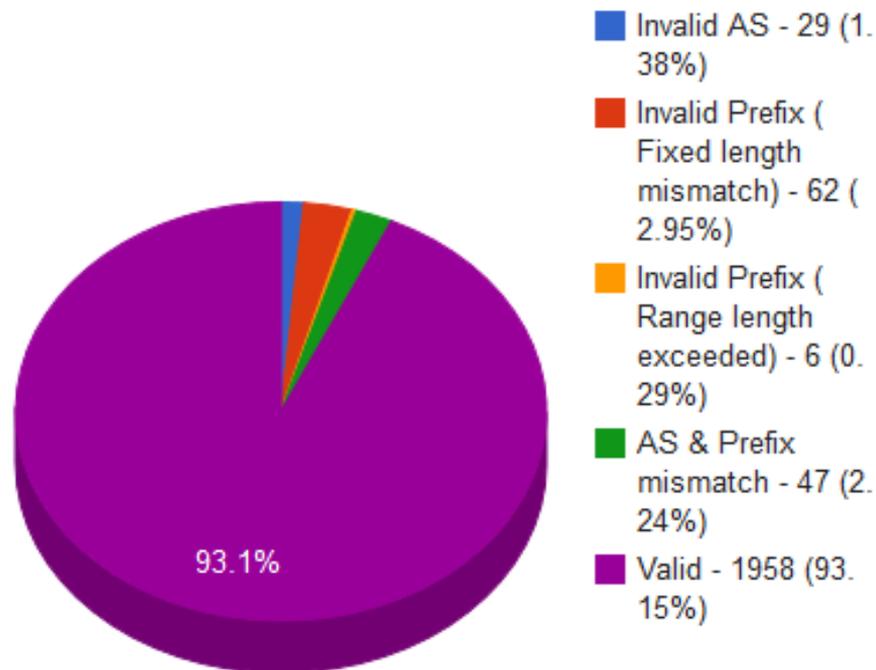
ROAによってカバーされるIPアドレスの割合はまだ低い。ただしRIPE地域は単純増加の傾向にある。

ROAを使った検証結果の内訳

Distribution of reasons for all invalid IPv4 prefixes



Distribution of reasons for all invalid IPv6 prefixes



RPKI Dashboard, SURFnet, 2015/4/3
<http://rpki.surfnet.nl/>

実際の経路情報とは異なるROAが約10%発行されている。(IPアドレス管理とAS運用の違いも一因)

国内での試験提供



一般社団法人 日本ネットワークインフォメーションセンター

Copyright © 2015 Japan Network Information Center

JPNICのRPKIシステム

The screenshot shows the JPNIC RPKI website. The browser address bar displays <https://rpki.nic.ad.jp/start>. The page header includes the JPNIC logo and the text "一般社団法人 日本ネットワークインフォメーションセンター Japan Network Information Center". Below the header, there are two buttons: "最新の情報に更新(メイン画面)" and "ROA Webの利用を停止". The main content area features a "RPKIシステム (JPNICNET)" section. A "ご注意:" box contains the following text: "RPKIシステムにアクセスするには資源申請者証明書が必要です。詳しくは下記のページをご覧ください。" and provides two links: "申請における認証について <https://www.nic.ad.jp/ja/ip/id-procedure.html>" and "ご利用条件をご確認ください。 <https://serv.nic.ad.jp/capub/rpki/rpki-terms-conditions.pdf>". At the bottom of the main content, there are two buttons: "ROA Webを開始" and "BPKI接続設定を開始". The footer contains the JPNIC logo and the text "Copyright © 1998-2015 Japan Network Information Center. All Rights Reserved."

The dialog box is titled "個人証明書の要求". It contains the following information: "このサイトはあなたの個人証明書を求めています: rpki.nic.ad.jp:443", "組織: 'Japan Network Information Center'", and "発行者: 'Japan Network Information Center'". Below this, it says "個人認証を行うために送信する証明書を選択してください:" and shows a dropdown menu with the selected option: "LIR-HM 0011431 JPNIC-PA taiji-k 07 openssl の Japan Network Information Center ID [01:AA:2B]". A "選択した証明書の詳細:" section lists the following details: "発行対象: CN=LIR-HM 0011431 JPNIC-PA taiji-k 07 openssl,OU=MNT-000734,OU=LIR Hostmaster,O=Local Internet Registry,O=Resource Holder,C=JP", "Serial Number: 01:AA:2B", "有効期限: 2015/03/20 9:00:00 から 2017/04/18 9:00:00", "Certificate Key Usage: Signing,Key Encipherment,Data Encipherment", "メール: taiji-k@nic.ad.jp", and "発行者: OU=JPNIC Resource Service Certification Authority S2,OU=Internet Resource". At the bottom, there is a checked checkbox "☑ 今後も同様に処理する" and two buttons: "OK" and "キャンセル".

ROA Webを開始

ROA Webとは、Webページで操作を行うだけでリソース証明書やROAの発行を行うことができるWebサービスです。利用を「開始」すると自動的にリソース証明書が発行されます。本来はリソース証明書の発行を受けた方が行う「鍵の管理」などをJPNICが代行して行います。(ご利用条件の「ROA発行代行機能」を参照のこと)

BPKI接続設定を開始

BPKI接続とは、JPNICのRPKIシステムと利用者側で用意されたRPKIシステムをBusiness PKIと呼ばれる方式で接続するRPKIの利用方法です。BPKI接続はidentityファイルのアップロードとresponseファイルのダウンロードを通じて行うことができます。(ご利用条件の「BPKI接続」を参照のこと)

IPアドレスの申請者の証明書を使ってユーザを認証する。利用を開始するとリソース証明書が発行される。

BPKI(Business PKI)接続設定

JPNIC 一般社団法人 日本ネットワークインフォメーションセンター
Japan Network Information Center

最新の情報に更新(メイン画面) ROA Webの利用を停止

BPKI接続設定 (JPNICNET)

BPKI接続

IDファイル (identity.xml)の登録

1. お使いのRPKIシステムでidentity.xmlを作成します。(例: \$ rpkic initialize)
2. identity.xmlを下のボタンをクリックしてアップロードします。
3. 表示が変わった下のボタンをクリックしてparent-response.xmlをダウンロードします。
4. ダウンロードしたparent-response.xmlを使ってご利用のRPKIシステムの設定を行います。(例: \$ rpkic configure_parent parent-response.xml)
5. repository-request.xmlが生成されます。

リポジトリ接続

リポジトリリクエストの登録

6. repository-request.xmlを下のボタンをクリックしてアップロードします。
7. 表示が変わった下のボタンをクリックしてrepository-

ユーザ側に設けられたRPKIシステムとの接続のために使われる。(大手ISP向け)

リソース証明書の一覧

リソース	有効期限	割り振り元	状態
------	------	-------	----

JPNIC 一般社団法人 日本ネットワークインフォメーションセンター
Copyright© 1996-2015 Japan Network Information Center. All Rights Reserved.

ROA Web

The screenshot shows the ROA Web interface in a browser window. The URL is https://rpki.nic.ad.jp/roa. The page header includes the JPNIC logo and the text "一般社団法人 日本ネットワークインフォメーションセンター Japan Network Information Center". There are buttons for "最新の情報に更新(メイン画面)" and "ROA Webの利用を停止".

ROA Web (JPNICNET)

ROAの管理

状態が「発行済」になるとそのROAはRPKIのリポジトリで公開されている状態になっていることを示しています。ROAが発行済になるまでには5分程度かかることがあります。

Prefix	AS番号	状態
--------	------	----

Buttons: 作成, インポート, エクスポート, ROAを全て削除

ROA発行のできるリソース一覧

ROA発行のできるリソースです。この一覧は正規化処理されているため、WHOISデータベースと表記が異なる場合があります。

ROAの一括作成

IPv4

Prefix	操作
192.41.192.0/24	ROAを作成
202.11.240.0/21	ROAを作成
202.12.30.0/24	ROAを作成

リソース証明書の一覧

ROAはリソース証明書が発行済になると作成できます。状態が「発行済」になるとそのリソース証明書はRPKIのリポジトリで公開されている状態になっていることを示しています。リソース証明書が発行済になるまでには5分程度かかることがあります。

リソース	状態	有効期限
192.41.192.0/24	発行済	2016年4月2日 10:55:39
202.11.240.0/21	発行済	2016年4月2日 10:55:39
202.12.30.0/24	発行済	2016年4月2日 10:55:39

Webの操作のみでROAの作成ができる。(ROA発行代行機能)

ROA Webを使ったROA作成

RPKI

https://rpki.nic.ad.jp/roa_create_all

日本語

一般社団法人 日本ネットワークインフォメーションセンター
Japan Network Information Center

最新の情報に更新(メイン画面) ROA Webの利用を停止

一つのAS番号を指定してROAを一括作成 (JPNICNET)

AS番号を入力

AS番号

作成 キャンセル

ROAの発行対象となるPrefixの一覧

Prefix
192.41.192.0/24
202.11.240.0/21
202.12.30.0/24

一般社団法人 日本ネットワークインフォメーションセンター
Copyright© 1996-2015 Japan Network Inform

AS番号を指定してROAを作成する。

ROA WebのROA管理画面



RPKI

https://rpki.nic.ad.jp/roa

日本語

最新の情報に更新(メイン画面) ROA Webの利用を停止

ROA Web (JPNICNET)

ROAの管理

状態が「発行済」になるとそのROAはRPKIのリポジトリで公開されている状態になっていることを示しています。ROAが発行済になるまでには1分程度かかることがあります。

Prefix	AS番号	状態			
192.41.192.0/24	2515	発行済	🔍	🗑️	🔄
202.11.240.0/21	2515	発行済	🔍	🗑️	🔄
202.12.30.0/24	2515	発行済	🔍	🗑️	🔄

🔍 作成 🔄 インポート 🔄 エクスポート

🗑️ ROAを全て削除

リソース証明書の一覧

ROAはリソース証明書が発行済になると作成できます。状態が「発行済」になるとそのリソース証明書はRPKIのリポジトリで公開されている状態

発行されたROAとリソース証明書はrsyncを使ってリポジトリからダウンロードできるようになる。

ROA Webでは…

- **私有鍵はRPKIシステム側に存在する。**
 - 私有鍵の用途 = 電子署名 “digital signature”
 - 電子署名のメッセージ認証としては…
 - ほぼ全てのRIRで採用されているモデル
 - ただし、リソース証明書ではエンティティの識別はできない。

⇒ 「ROA発行代行機能」と定義

- ROAにおける電子署名は、電子文書への電子署名とは意味が異なり、IPアドレスの登録情報を「改ざん検知」と「有効期限」という二つの仕組みと共に提供する仕組みであると考えられている。

技術課題

RPKIの持つ性質と技術課題

RPKIの持つ性質と技術課題

- 署名付きオブジェクトを提供するPKIとして
- 上位認証局証明書から検証するPKIとして
- 運用上の課題

署名付きオブジェクトを提供するPKIとして

課題	対応策と考え方
最新の署名付きオブジェクト ROAの提供	リポジトリのサーバrsyncdを分散化。IETFでは新しい差分転送プロトコルも提案されている。
失効情報の伝播	CRLをリポジトリデータ一式の中で配布
オブジェクト欠損への対応	発行済みオブジェクトの一覧であるマニフェスト MFT を配布
RIRでは主流な「ROA Web」のような形態での提供	エンティティによる署名という概念をなくしつつ鍵管理

なおこの仕組みでは一つの不整合が複数のエラーを起こすことが多い。一つの署名が有効ではない理由を調べるために、複数の仕組みを調べる必要あり。

上位認証局証明書から検証するPKIとして

- **署名検証の結果としては「有効なIPアドレスとAS番号の組み合わせリスト」が得られる**
 - その中から特定の経路情報の有効性を確認するのはRPの役割
- ⇒ Origin Validationというアプリケーションの上では、一つのROAの有効性ではなく、有効なROAの塊に意味がある

一つのエラーが多数の検証結果に一度に現れてしまう。有効性の監視を行う場合には、単一のROAの有効性ではなく結果全体を対象にする必要がある。

運用上の課題

- **自律分散への影響**

- 単一障害点ができないようにするにはどうすればよいのか
 - レジストリのRPKI認証局
 - リポジトリ
 - ROAキャッシュサーバ

- **システムの信頼性**

- 暗号アルゴリズムはRSA2,048/SHA-256のみ
- TALやSIAではドメイン名で指定 → DNSに依存

BGPを使ったルーティングの自律分散という特徴を崩さずにセキュリティ技術を導入するにはどうすべきなのか

信頼構造



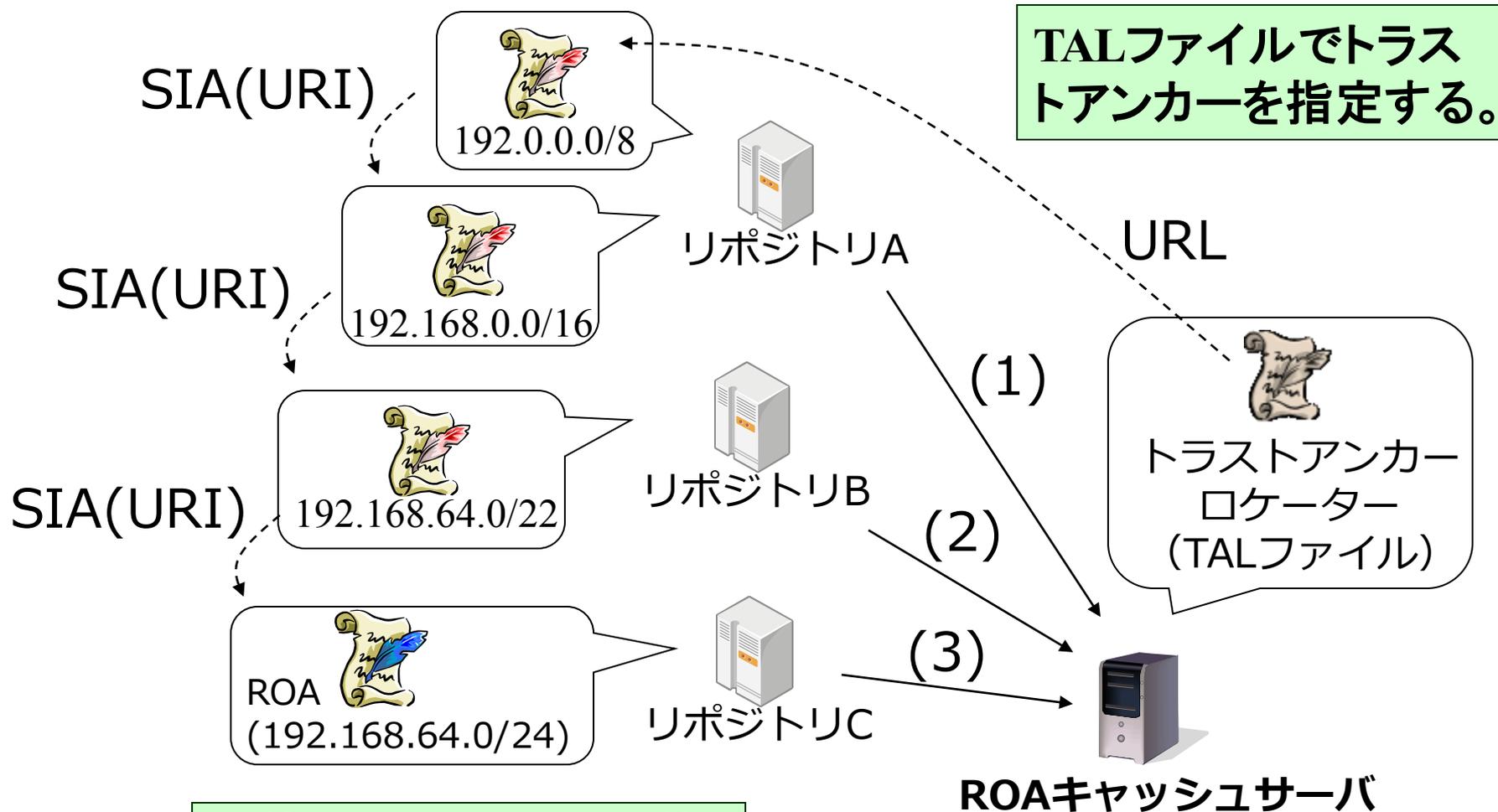
一般社団法人 日本ネットワークインフォメーションセンター

Copyright © 2015 Japan Network Information Center

信頼構造

- **トラストアンカー**
- **依拠当事者としてのROAキャッシュサーバ**

トラストアンカーと署名検証



上位のprefixは、下位のprefixを内包する。

RPKIのトラスト構造

- 5つのRIRがトラストアンカーローケーターを提供

- ひとつのCA証明書の有効性によってNIR全域の有効性が影響を受ける？

- NIRもトラストアンカーに設定？
- RP側に別の仕組みを設ける？

draft-ietf-sidr-ltamgmt

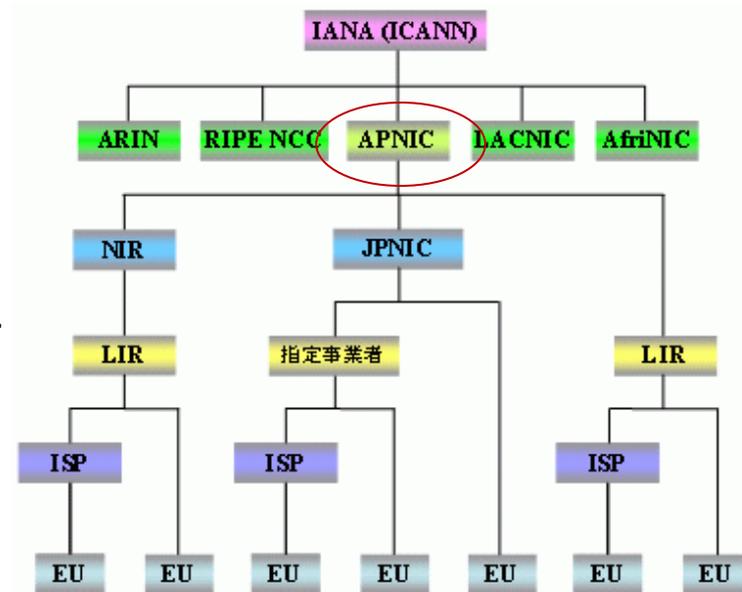
draft-dseomn-sidr-slurm

draft-kent-sidr-suspenders

- 設定はRPのプログラムに依存

- service agreement (ARIN)

- LIRはWeb上の提供
(鍵はRIR/NIRサーバ上)



依拠当事者としてのROAキャッシュサーバ

- **パブリックキャッシュサーバ**
 - ROAの検証結果を返すサーバ
 - 対応したBGPルー他の設定を行うだけでROAとRPKIの検証結果が利用できる
 - 今後も増える可能性あり
- **RPKI RPのあるべき姿？**
 - 署名検証は手元で行うべき？
⇒ 署名検証サーバを立ち上げないと利用できないPKIになってしまう。
 - パブリックキャッシュサーバを併用？
⇒ 単一障害点になりうる。接続の安全性（本日まで紹介したような！）の担保は？

まとめ

まとめ

- RPKIはIPアドレス管理の構造に沿って、「リソース証明書」を発行する仕組み
 - 本来と異なる経路情報を検出するOrigin Validationが注目されている
 - JPNICにおける試験提供の開始
- 技術課題と信頼構造
 - 上から検証を行い「有効なIPアドレスとAS番号の組み合わせリスト」を得る仕組み
 - 鍵保有と署名検証
 - 国際的なツリー構造
 - パブリックキャッシュサーバによる署名検証

おわり



一般社団法人 日本ネットワークインフォメーションセンター

Copyright © 2015 Japan Network Information Center