

# 大規模BGPハイジャック (Mis-Origination) JANOG37mtg

2016年1月20日

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  
岡田 雅之



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 © 2016 Japan Network Information Center

# なぜハイジャック (Mis-Origination) が起きるのか

- **大原則**

- BGPの経路交換は“相互信頼”の原則

- **仮説**

- 誰もが“自分は発生源にならない”と思ってる
  - Filter漏れ、Configのミスにより当事者に・・・
  - 主に悪意は無い
- ハイジャックをしても・・・
  - 加害者と被害者が離れていると発覚が遅れる
  - 被害者の取るべき行動がはっきりしない
    - 回復に向けた行動：地道に証拠を集める
    - 加害者へのアプローチ：国内：？偽計業務妨害？
    - 国外：????????

# 自分は発生源にならない

- Prefix設定ミス



192.167.0.0/24  
とTypoしてしまう・・・

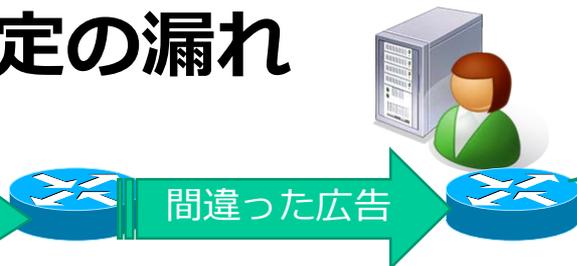
- 顧客フィルタ漏れ



顧客を全てPermitしていた  
ので自分経由で拡散

- 検証設定の漏れ

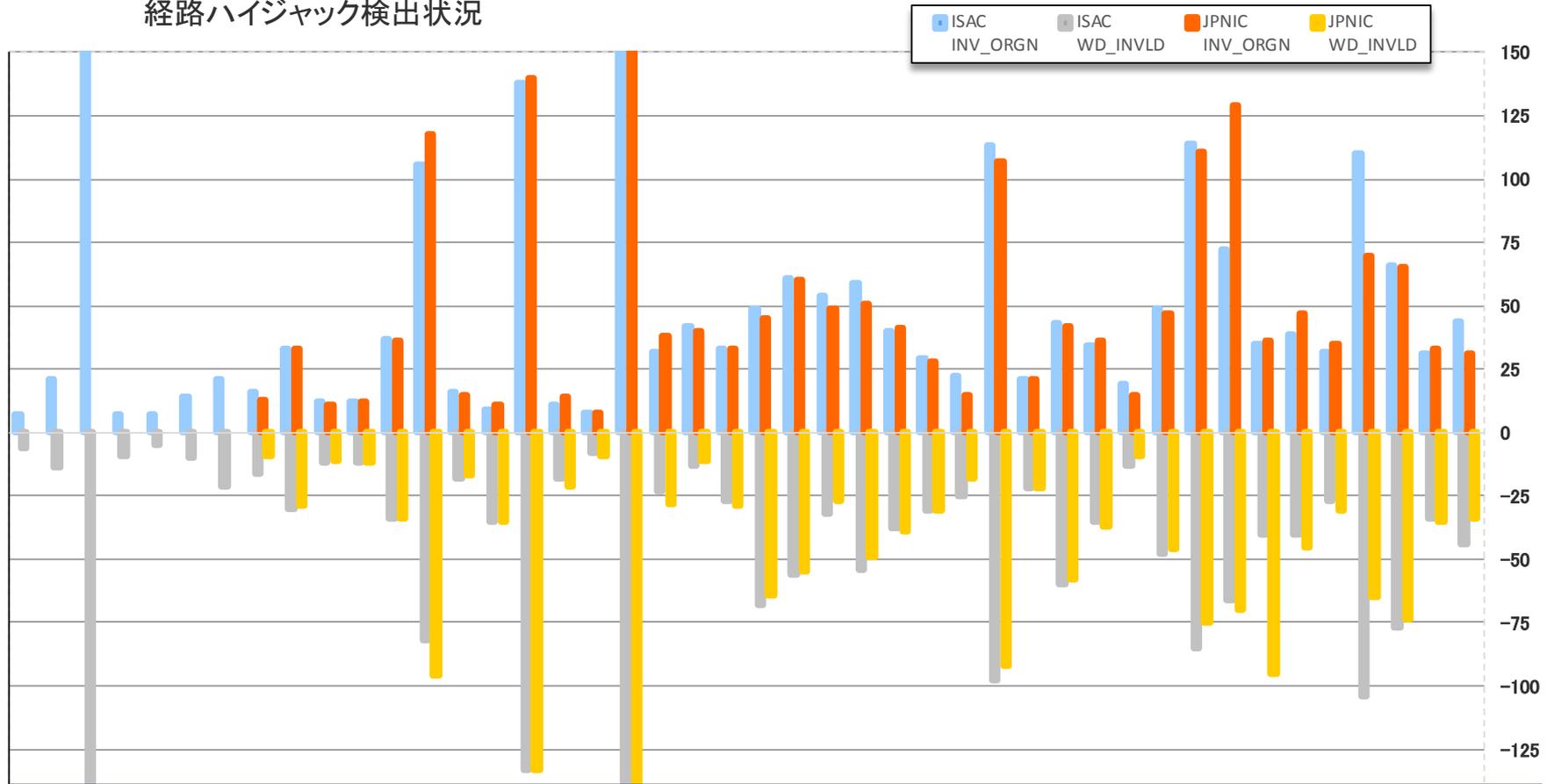
検証設定：  
1.0.0.0/16  
2.0.0.0/16  
3.0.0.0/16  
:  
:



検証用の設定を拡散

# ハイジャック/Mis-Origin(と思われる)の件数

経路ハイジャック検出状況



Telecom-ISAC 経路情報共有ワーキンググループ(BGPWG)  
経路奉行の検出結果より

# 発覚されないように・・・

- 広告対象を制限



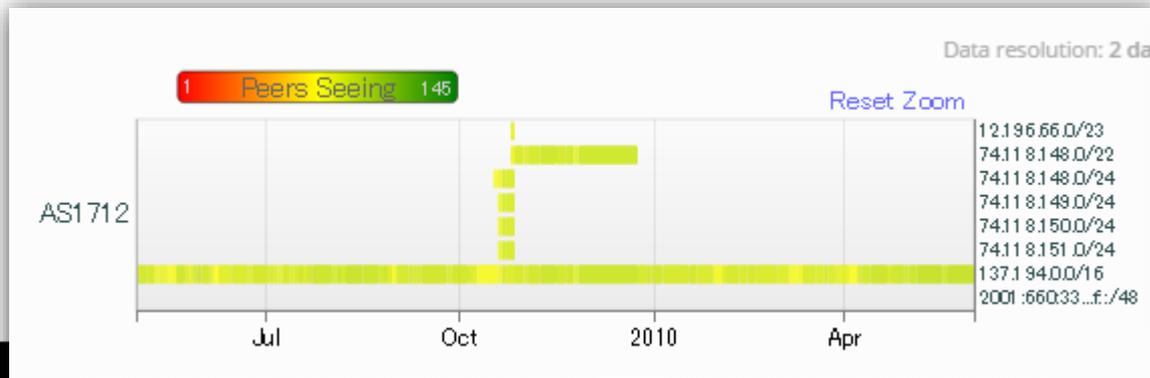
ターゲットに"NO-Export"  
を付与

- 未広告Prefixを



割り振られているけど経  
路広告されていないとこ  
ろを探す

- (AS番号の衝突) : 過去IRの不具合で発生



# 傾向と対策

- **これまでの対策**

- 経路フィルタ

- 経路フィルタ生成元の発明：IRR/RPKI/AS-PATHのメール

- 監視活動

- 経路フィルタ生成元と経路のチェック：経路奉行・BGPMON他

- **最近の傾向**

- 経路広告されていないPrefixがターゲットに
- 内部や閉域のため、より発見が遅く・・・
- 環境悪化を招いてしまう・・・

たとえば：経路広告が本来不要のPrefixも何らかのASから常時経路広告（空広告）することはできないか。

# 今考える対策

---

- **性質の異なる二つの問題へ対処が必要**
  - 従来型の“うっかり型”への有効な対策
    - ミスを前提としたFail Safeな設計
    - 連絡先データベースの維持
    - 経路の監視
  - 悪意が疑われる問題への踏み込んだ対策
    - 特定経路の複数ポイントでの監視
    - 悪用された場合特有の監視？
      - SPAMデータベースのチェック
    - 通常経路広告されていない経路を守る
      - . . .
  - 司法や国際協調の面はこれから検討か

# 参考資料（事前予習資料）

過去JANOG・IXユーザ会資料などより

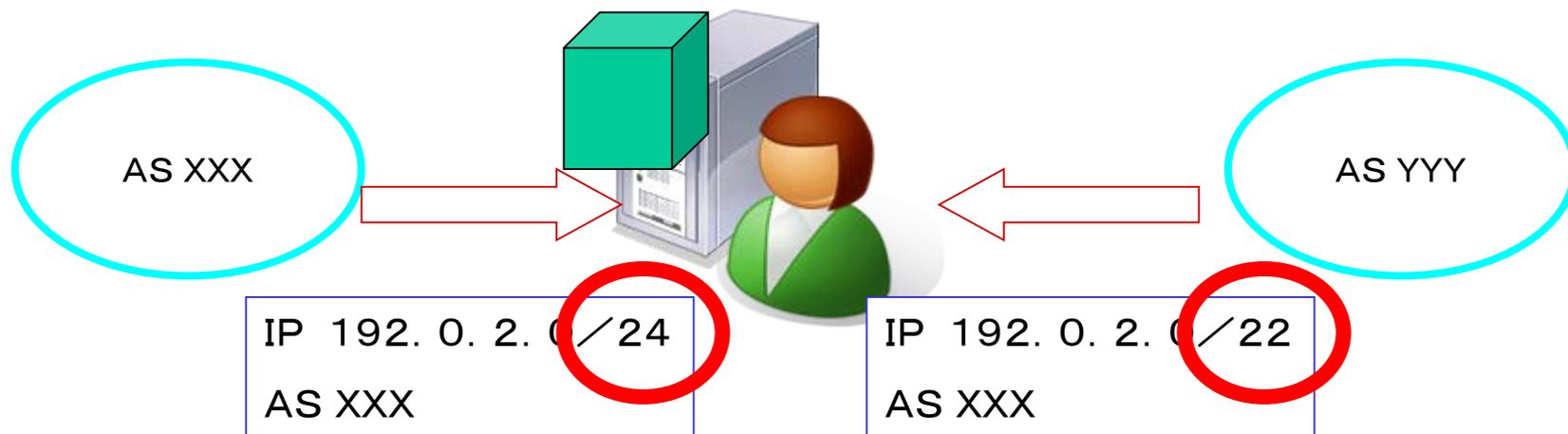
# Mis-Origination / 経路ハイジャック

---

- ルーティングは性善説に基づく
- **Mis-Origination**
  - Typoやルータのソフトウェアの不具合による過失
- **経路ハイジャック**
  - 悪意を持った攻撃
  - 経路ハイジャックは手段
  - 乗っ取ったアドレスで迷惑メールを送信など
- **過去から複数事例が発生**

# BGPの経路選択順番の基本 1

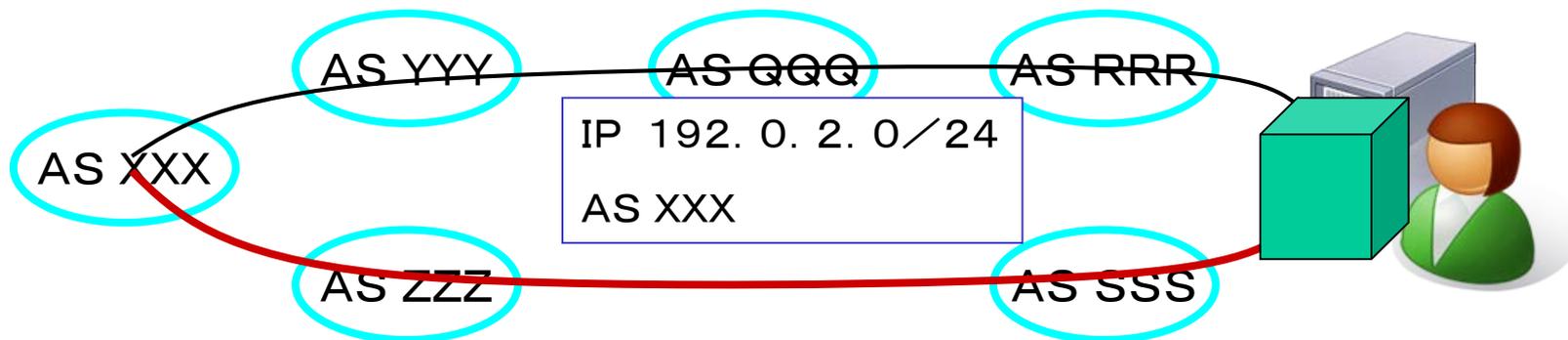
- 受け取った経路情報のうちサブネットマスク長がもっとも長い経路が優先される



この場合、マスク長が長いASXXXがあて先となります

# BGPの経路選択順番の基本 2

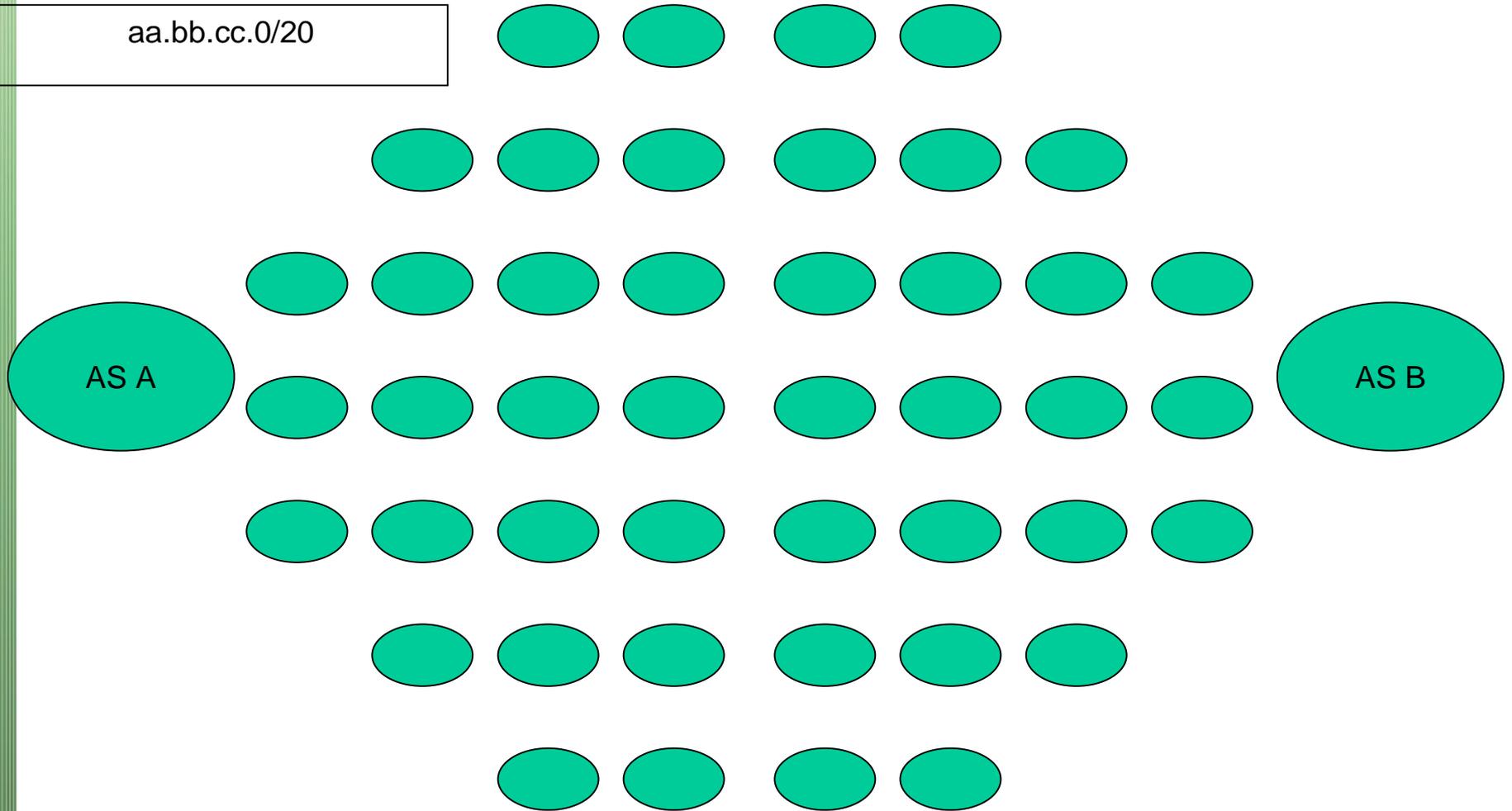
- マスク長が引き分けの場合、AS-PATH長(=経由してきたASの数)の短い経路を優先
  - AS XXX→AS YYY→AS QQQ→AS RRR
  - AS XXX→AS ZZZ→AS SSS



この場合、経由AS(=ASPATH)の少ない経路が選択されます。

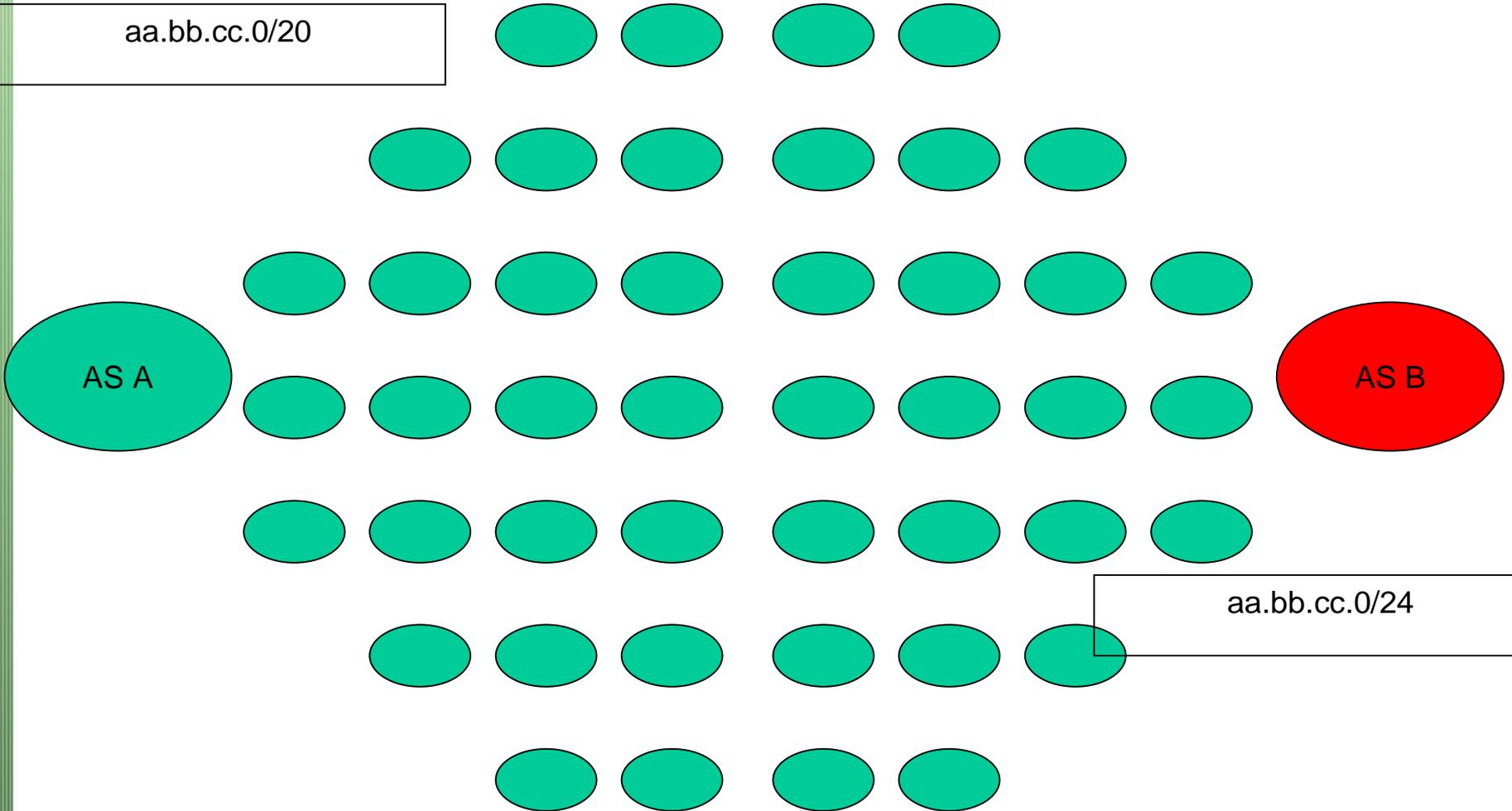
# Mis-Originでは無い状態

aa.bb.cc.0/20



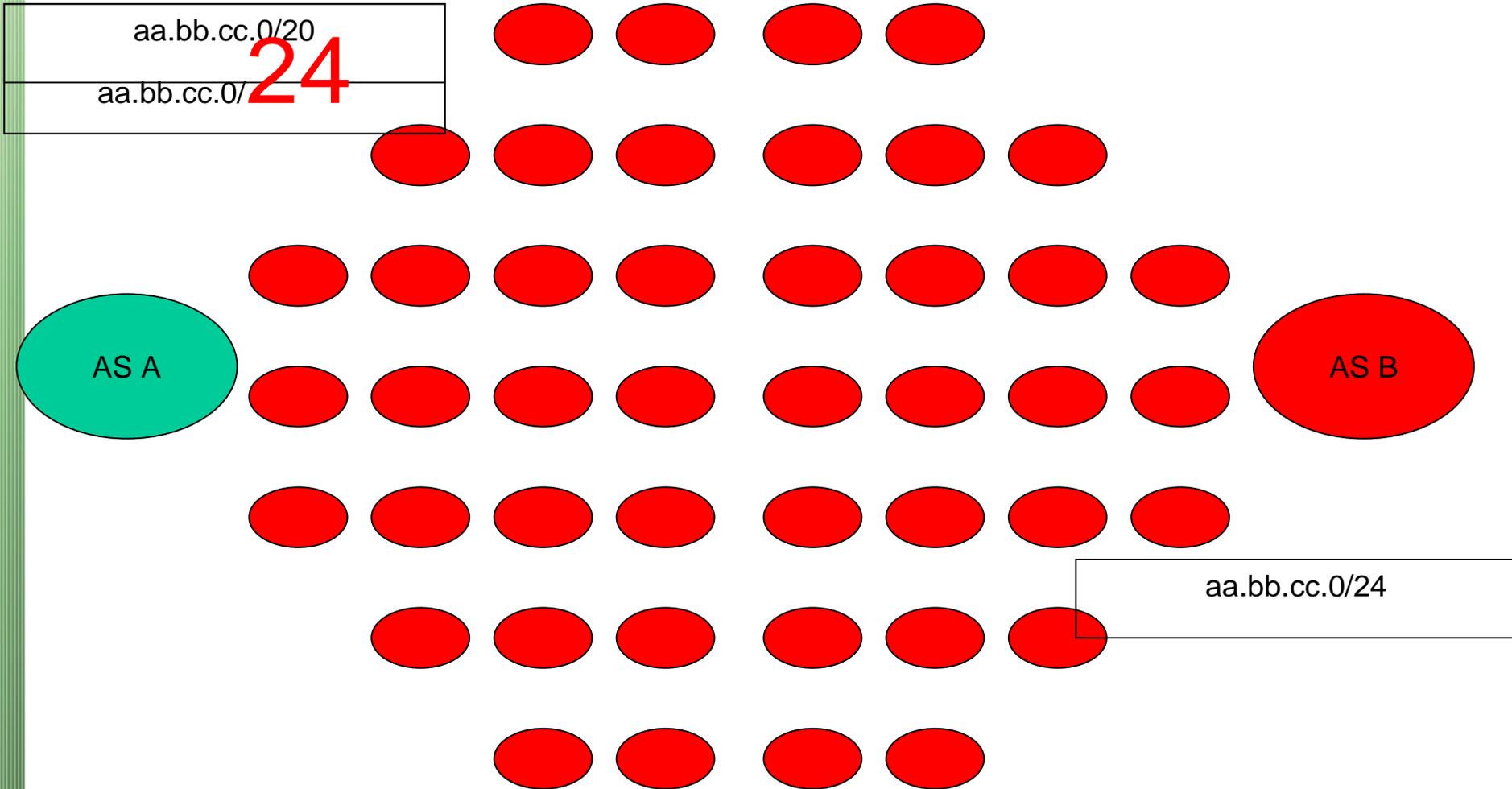
# Mis-Origin発生

aa.bb.cc.0/20

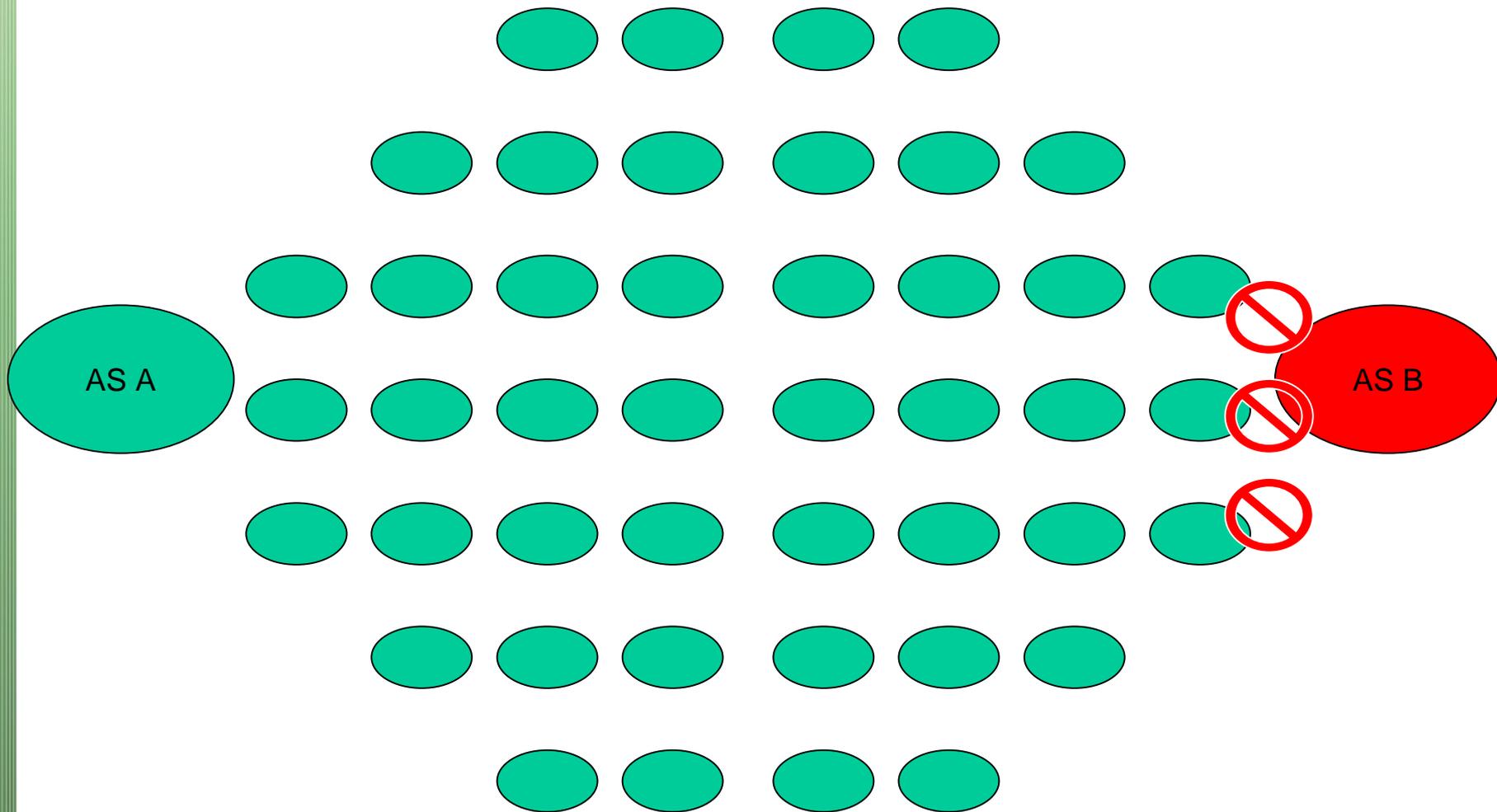


aa.bb.cc.0/24

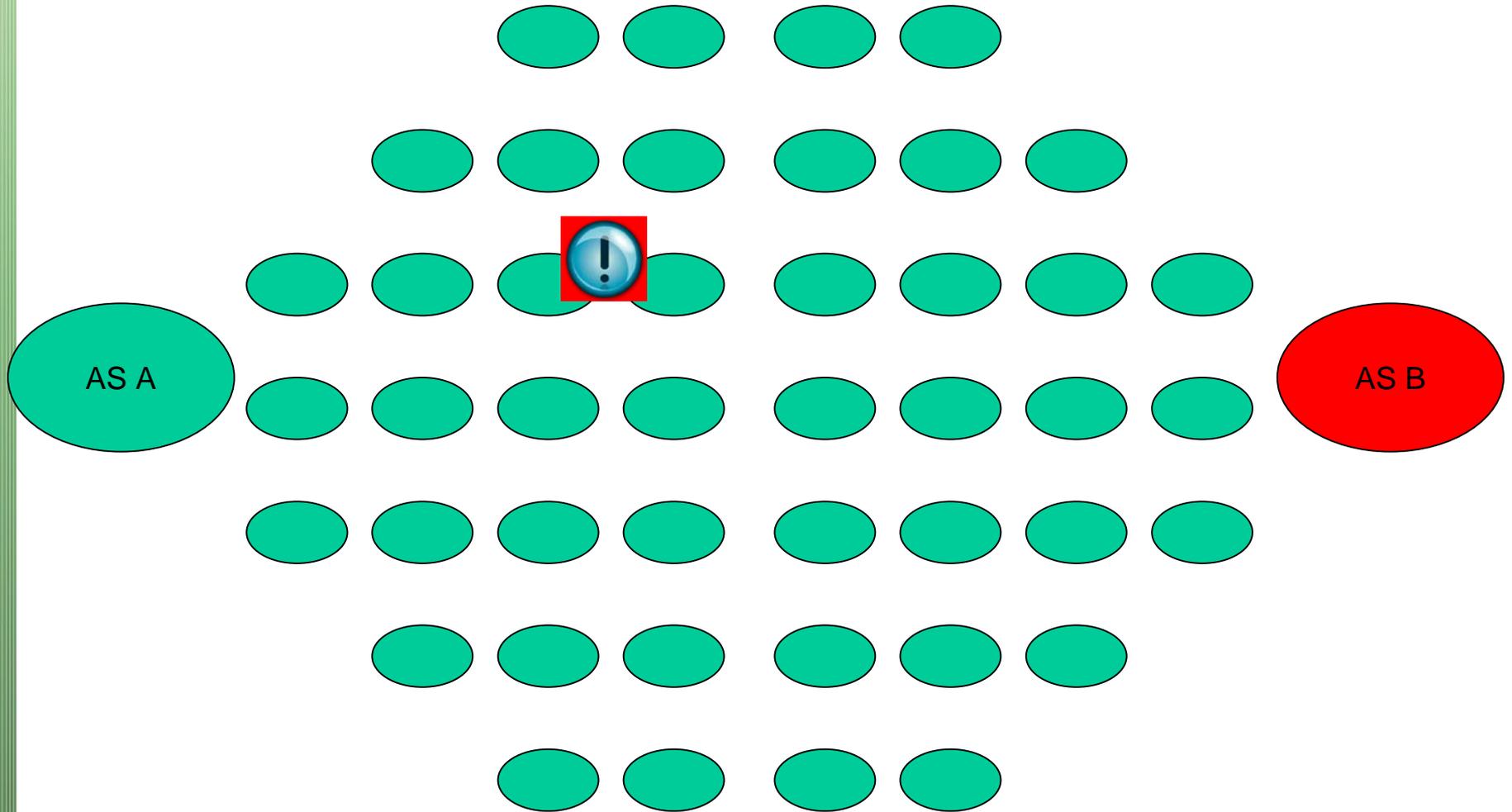
# AS-PATH勝負



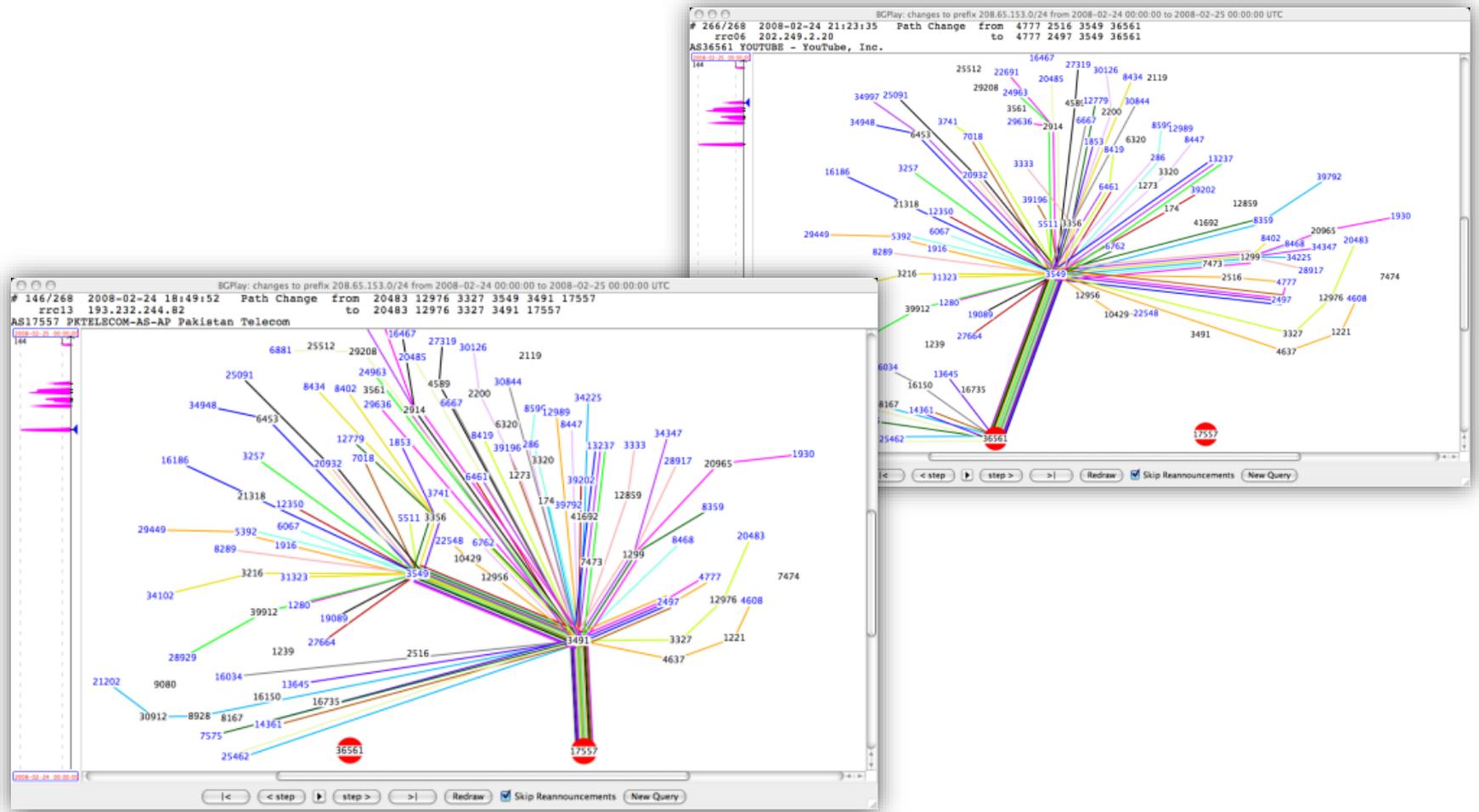
# RPKIはどこに効くのか？防ぐ（理想）



# RPKIはどこに効くのか？検知



# YouTube経路ハイジャック事件



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>

```
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
```

```
=====
```

*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.*

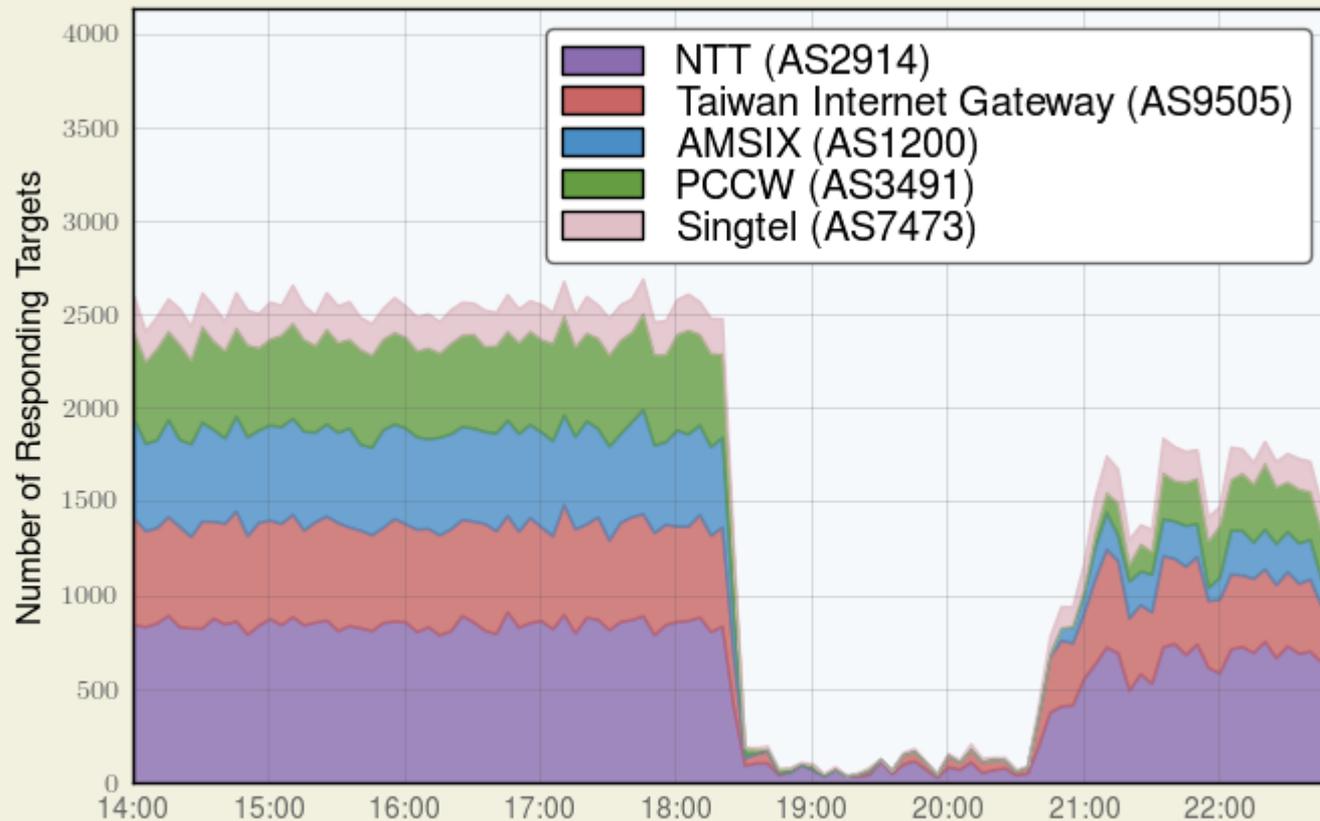
Turkey Hijacking IP addresses for popular Global DNS providers,

Posted by Andree Toonk - March 29, 2014, BGPMON

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

## Upstreams of Indosat (4761)

02 Apr 2014 through 02 Apr 2014



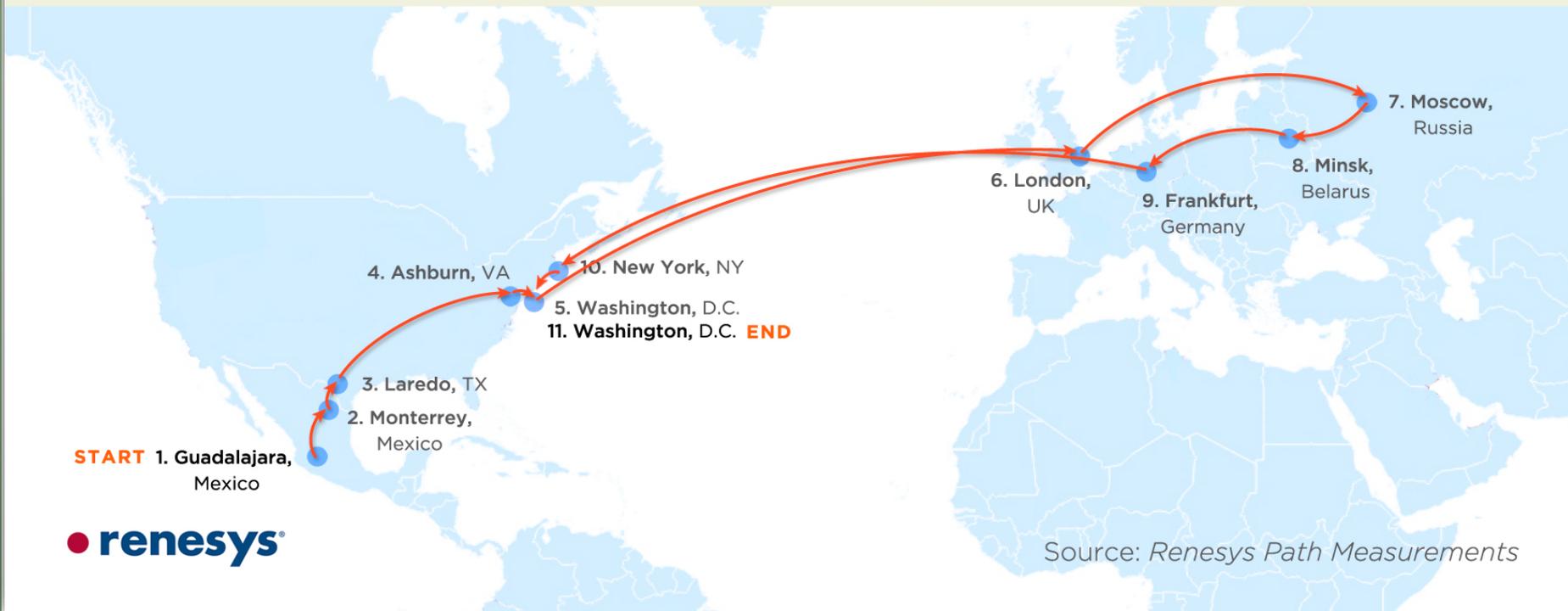
Source: *Traceroute Data*



Indonesia Hijacks the World, 03 Apr, 2014 | 3:09 PM | By Earl Zmijewski, Renesys  
<http://www.renesys.com/2014/04/indonesia-hijacks-world/>

# MITM (Man In The Middle)

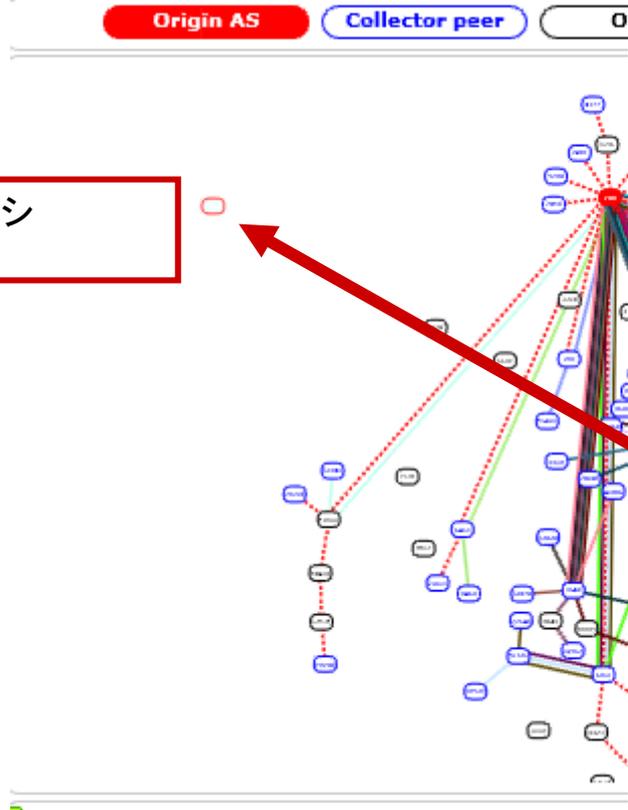
Traceroute Path 1: from Guadalajara, Mexico to Washington, D.C. via *Belarus*



- **Renesis Blog**より
- <http://www.renesys.com/2013/11/mitm-internet-hijacking/>

# MITM

ベラルーシ



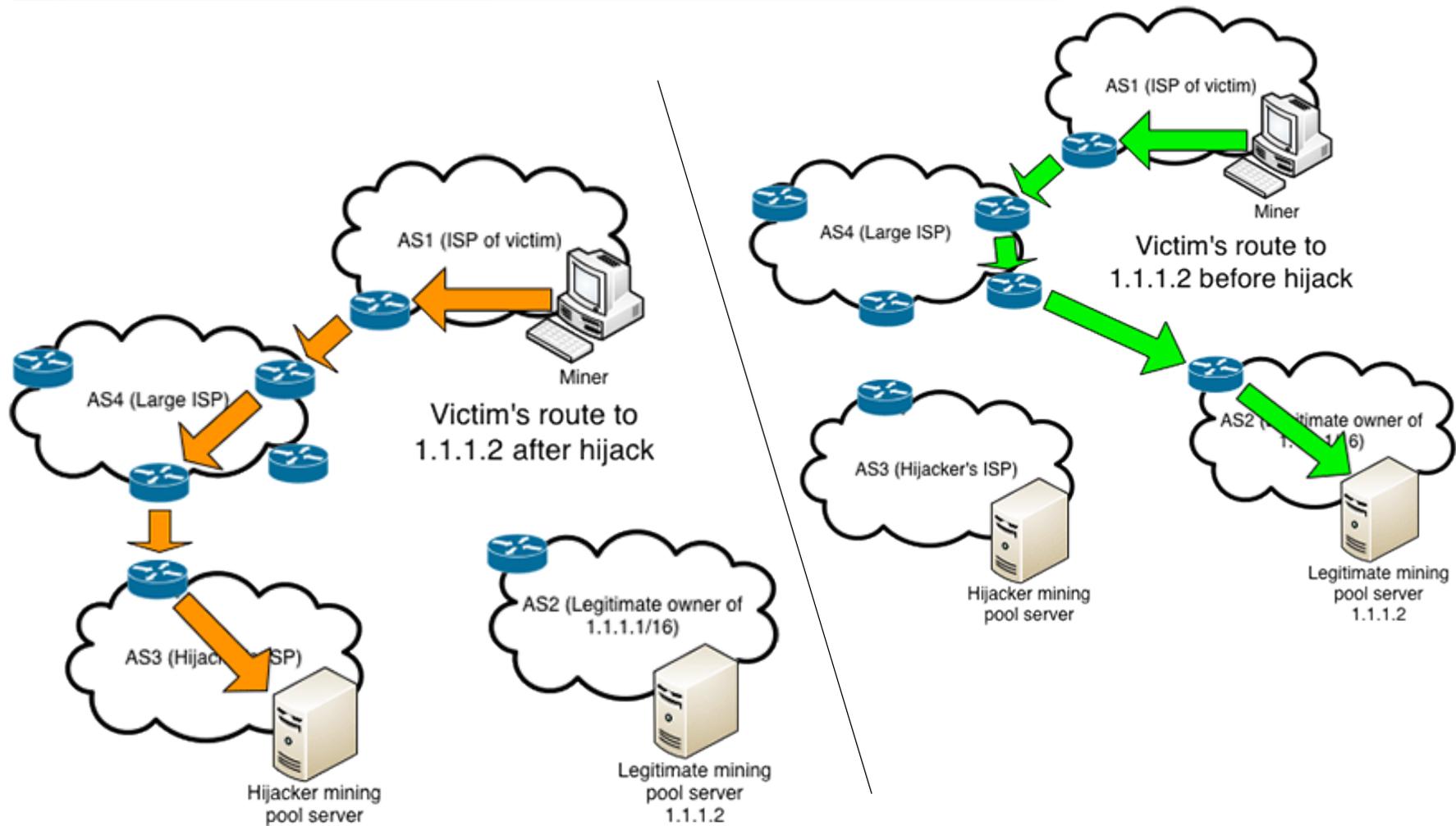
The New Threat: Target x

www.renesys.com/2013/11/mit

### 27 February 2013: Traceroute from Guadalajara, Mexico to Washington, DC via Minsk

IP	Delay (ms)	Notes
201.151.31.149	15.482	po-gd12.alestra.net.mx (Guadalajara, MX)
201.163.102.1	17.702	po-mty2.alestra.net.mx (Monterrey, MX)
201.151.27.230	13.851	igmtty2.alestra.net.mx (Monterrey, MX)
63.218.121.49	17.064	ge3-1.cr02.lar01.pcowbtn.net (Laredo, TX)
63.218.44.78	64.012	TenGE11-1.br03.ash01.pcowbtn.net (Ashburn, VA)
64.209.109.221	84.529	GBLX-US-REGIONAL (Washington, DC)
67.17.72.21	157.641	lag1.ar9.LON3.gblx.net (London, UK)
208.178.194.170	143.344	cis-company-transtelecom.ethernet8-4.ar9.lon3.gblx.net (London, UK)
217.150.62.234	212.869	mshk01.transtelecom.net (Moscow, RU)
217.150.62.233	228.461	BelTelecom-gw.transtelecom.net (Minsk, Belarus)
87.245.233.198	225.516	ae0-3.RT.JRX.FKT.DE.retir.net (Frankfurt, DE)
*		no response
*		no response
129.250.3.180	230.887	ae-3.r23.nycmny01.us.bb.gin.ntt.net (New York, NY)
129.250.4.69	232.959	ae-1.r05.nycmny01.us.bb.gin.ntt.net (New York, NY)
129.250.8.158	248.685	ae-0.centurylink.nycmny01.us.bb.gin.ntt.net (New York, NY)
*		no response
63.234.113.110	238.111	63-234-113-110.dia.static.qwest.net (Washington, DC)

# Bitcoinのマイニングプールへの経路をハイジャック



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/> 2

# もっと身近にある事例

## 作業ミス? によるMis-Originationの被害を受けた例 ～時系列～

2010年11月

- 
- 13:19 海外のISPがMis-Origination  
JPNIC(経路ハイジャック通知実験)からAlertメール受信
  - 13:30 Mis-Originationされているアドレスがユーザ向けとして  
利用中であることを確認。以下を実施することに
    - ・広告元へMis-Originationを止めるよう依頼する
    - ・さらに細かい経路を広告し、一時的に取り戻す
  - 13:45 広告元のASに停止をメールにて依頼
  - 14:05 細かい経路を広報し、取り返す

# 今できる対策

---

- **検知：経路の監視ツールの導入**
  - 経路監視ツールによる重要経路の監視
    - 日本：経路奉行
    - 国際：RIPEのツールやBGPmon
- **対策：上流ASとの事前準備**
  - 上流ASへ自分の経路を細分化するなどの調整
  - /22の経路では負ける→/24 4つに分割など
- **準備：自分が被害を受けたときの想定**
  - データベースへの精通
    - IRRやPeeringDBなどの活用が迅速に
  - 被害を受けたときの手順を事前に作成

# 例えば

---

- 支援ツールの作成 (簡単なスクリプト。以下を一度に実行)
- -JPIRR/RADBへのwhois
- -複数のホスト(含むLookingGlass)に対し traceroute/show ip bgpを実施する
- -AS RANK / HE BGP toolkitへのリンク生成

# そのほか参考資料

---

- **JANOG**
  - いっぱい
- **資料**
  - IRR・RPKI動向調査専門家チーム 調査報告書
  - <https://www.nic.ad.jp/ja/materials/irr/report-201308.pdf>