ルーティングアワー(2)
相互信頼を脅かすもの

～そのつながらないルーティングかも ～

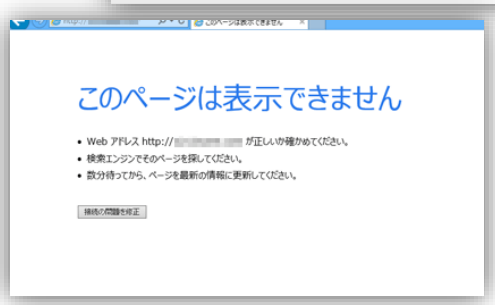
InternetWeekショーケース in 名古屋

2017年6月1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

つながらない？

- **ある日Webが繋がらない**
  - スマホの電波の問題か？
  - IPアドレスとDHCPの問題？
  - プロバイダの障害？
  - DNSの問題？
  - Webが本当に落ちている？絵
  - 実は経路が乗っ取られている？？

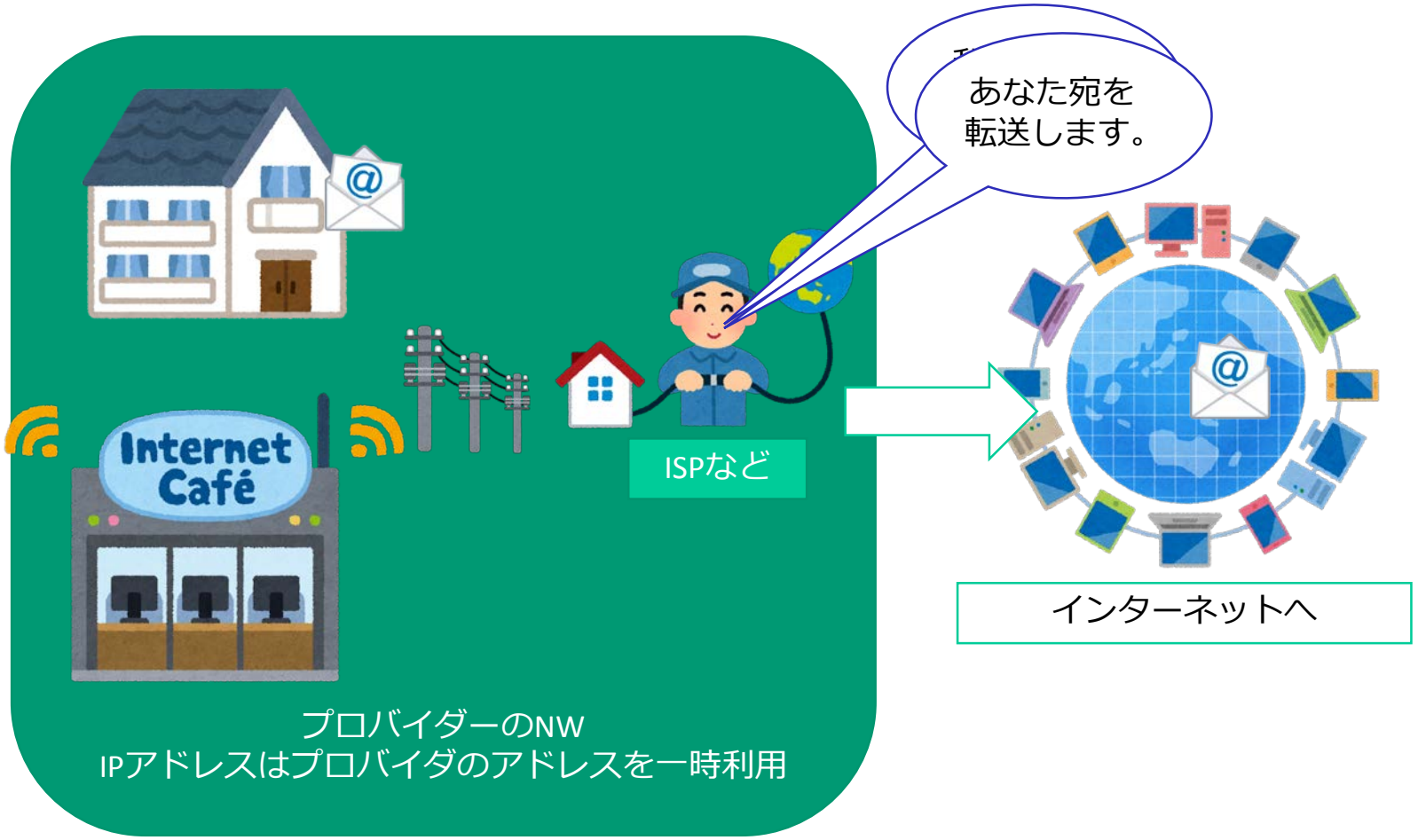


- **本セッションでは**
  - パケットの宛先制御(ルーティング)のトラブル、主に、”経路の乗っ取り”について深堀

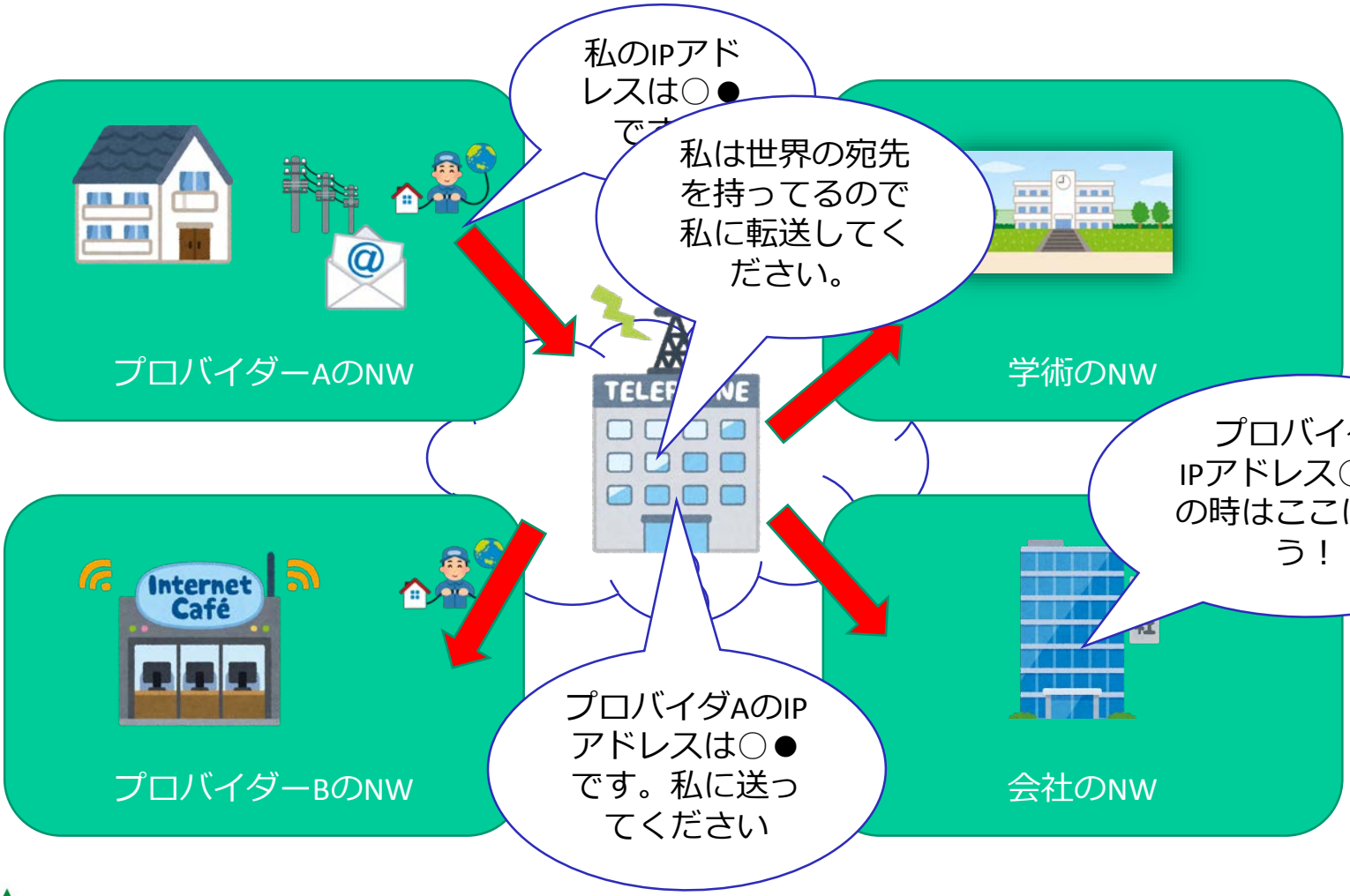
１．ルーティングと相互信頼

ルーティングの世界：家庭～ISP

- 家庭～ISPのネットワーク

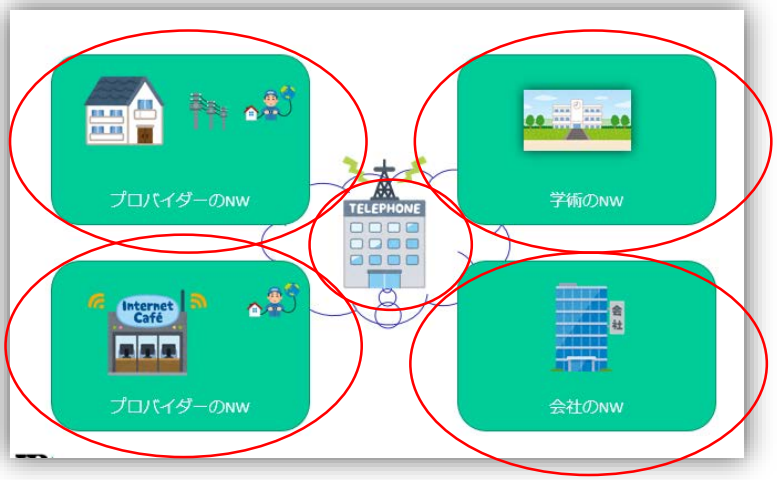


ルーティングの世界：ネットワーク同士



ルーティングの世界：ISP~BGP

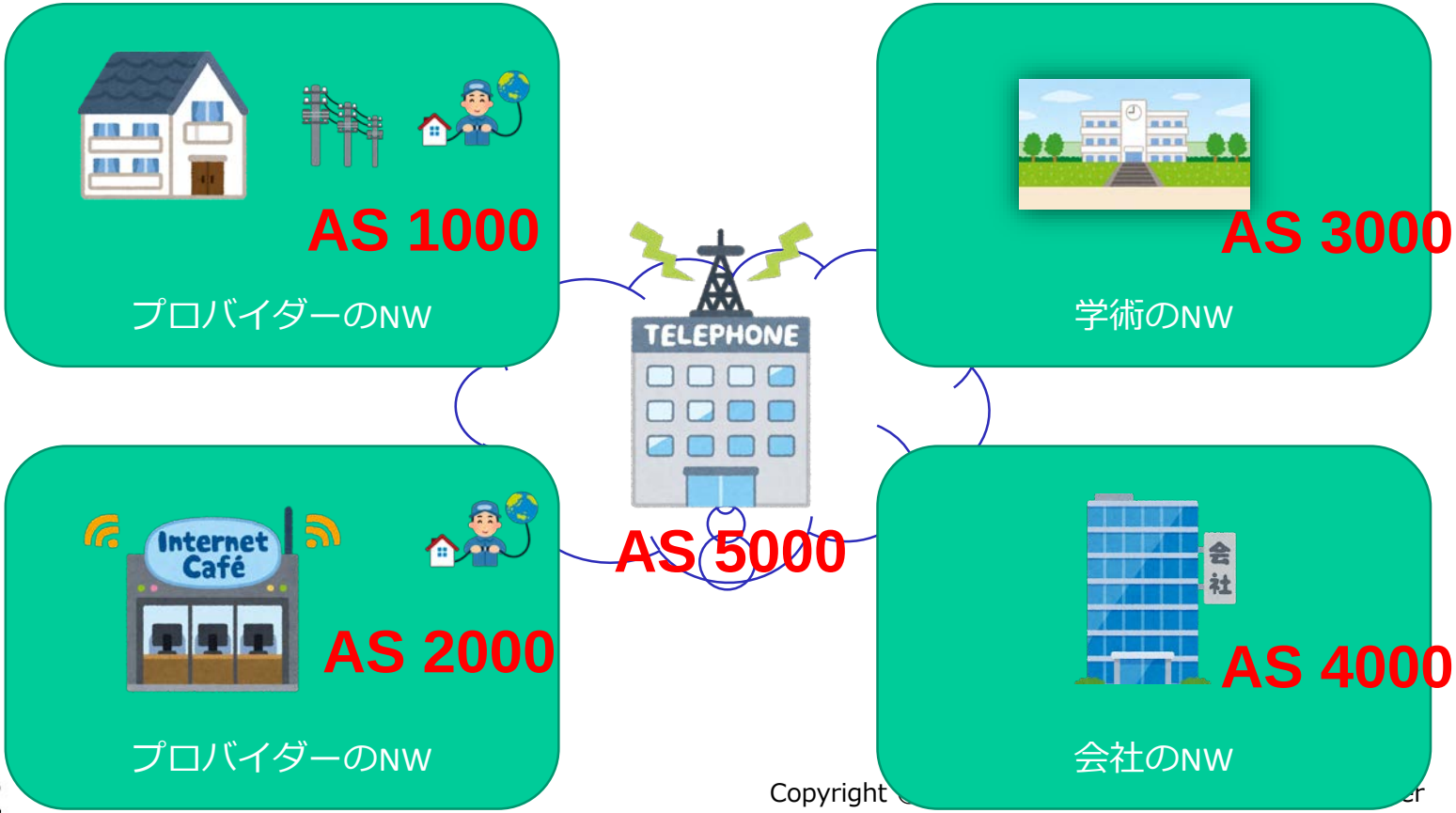
- **組織毎内部ルーティングからインターネットへ**



- **インターネットのルーティング**
  - Autonomous System(赤丸単位くらい:AS)Number
  - Boarder Gateway Protocol（AS間のやりとり)
  - IPアドレス/マスク（やり取りする主な情報）
- **上記三つをセットでやりとり**

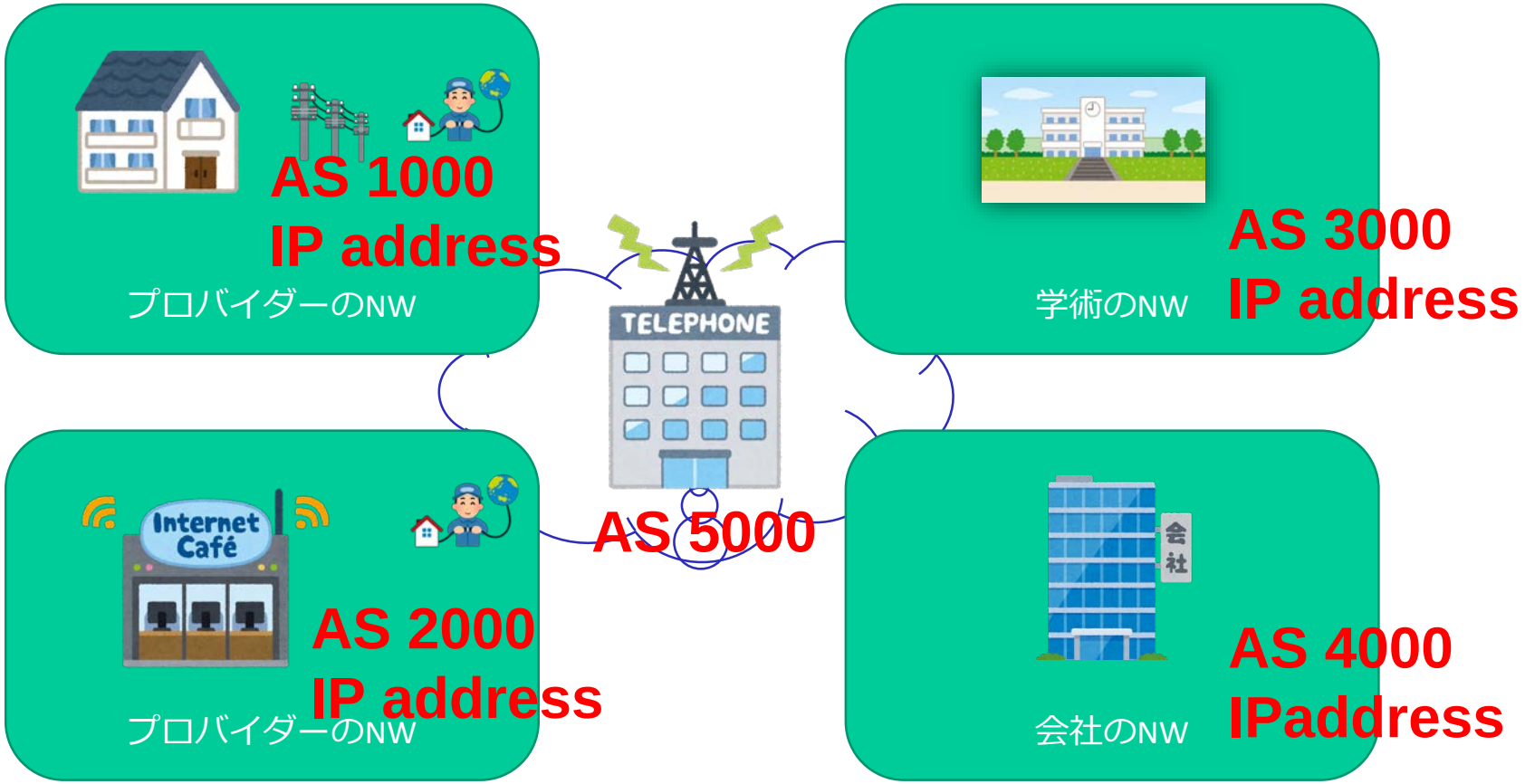
ルーティングの世界：AS番号

- **IPアドレスと同じく、重複のない番号**
  - AS単位で一つの0番～43億番まで
  - 世界で重複しないように管理団体から借りる番号



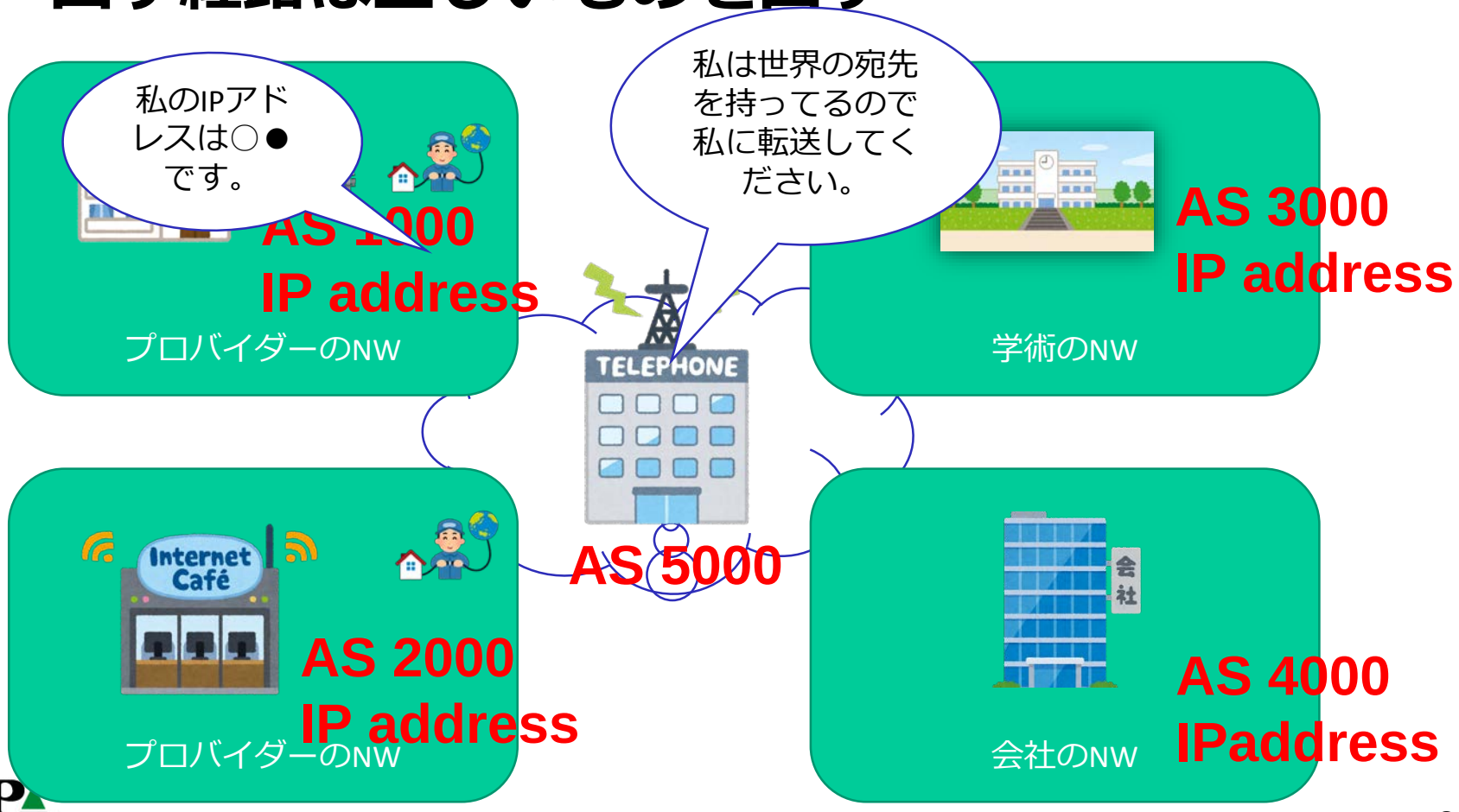
ルーティングの世界：BGP運用

- AS間のルーティング＝経路情報の交換



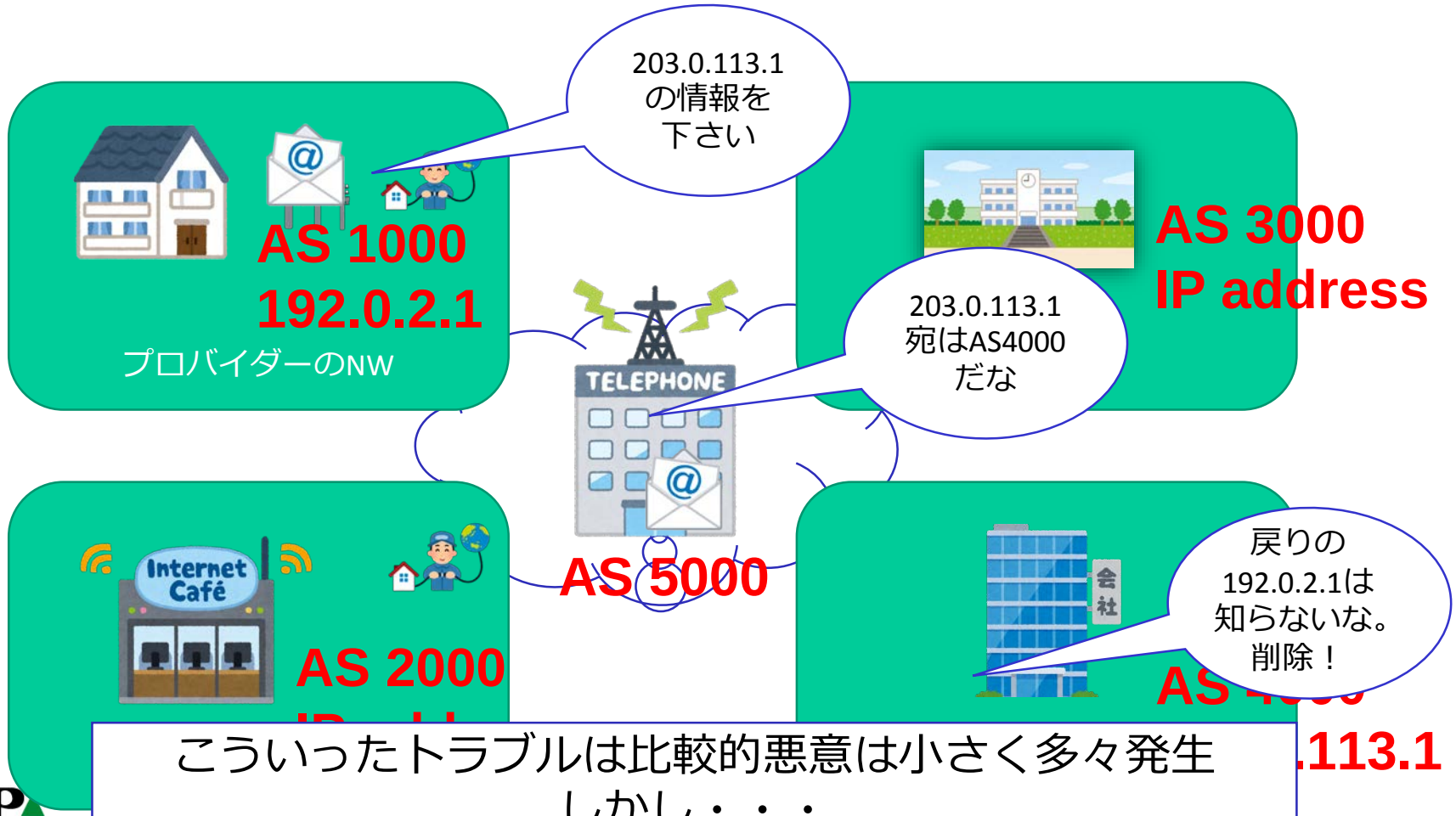
ルーティングの世界：相互信頼の実際

- いただく経路は信頼
- 出す経路は正しいものを出す



ルーティングの世界：よくある不具合

- 行きはよいよい・帰りはこわい



こういったトラブルは比較的悪意は小さく多々発生
しかし・・・

2．ルーティングを脅かすもの

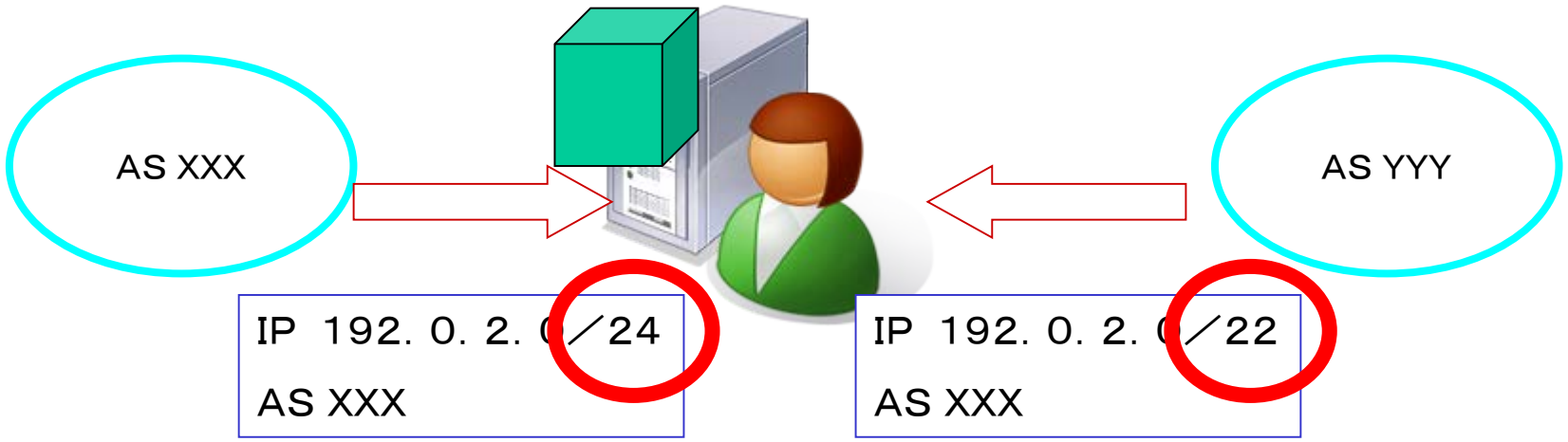
ルーティングの問題

- **経路上に存在する落とし穴**
  - 行き/帰り/途中
  - どこか1箇所でもおかしい経路があるとロスト
  - でもDefault Routeがあるのでは？
    - 原則BGPではDefault Routeを使いません
    - ルータ上に経路が存在しないと即アウト
- **それ以外：経路の乗っ取り**
  - なぜ乗っ取りが可能か？
  - 経路情報の確認手段などは？

その実態は・・・・

BGPの経路選択順番の基本１

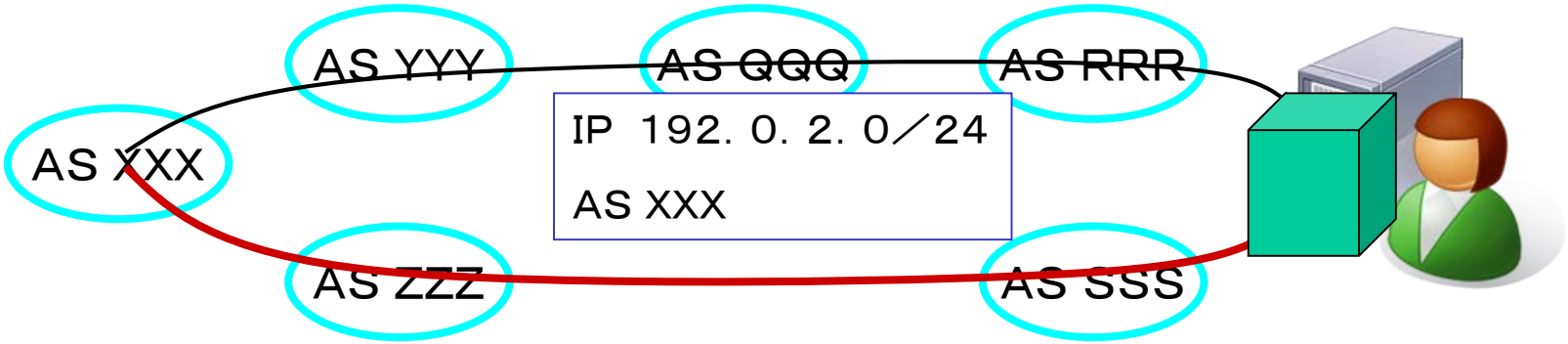
- 受け取った経路情報のうちサブネットマスク長がもっとも長い経路が優先される



この場合、マスク長が長いASXXXがあて先となります

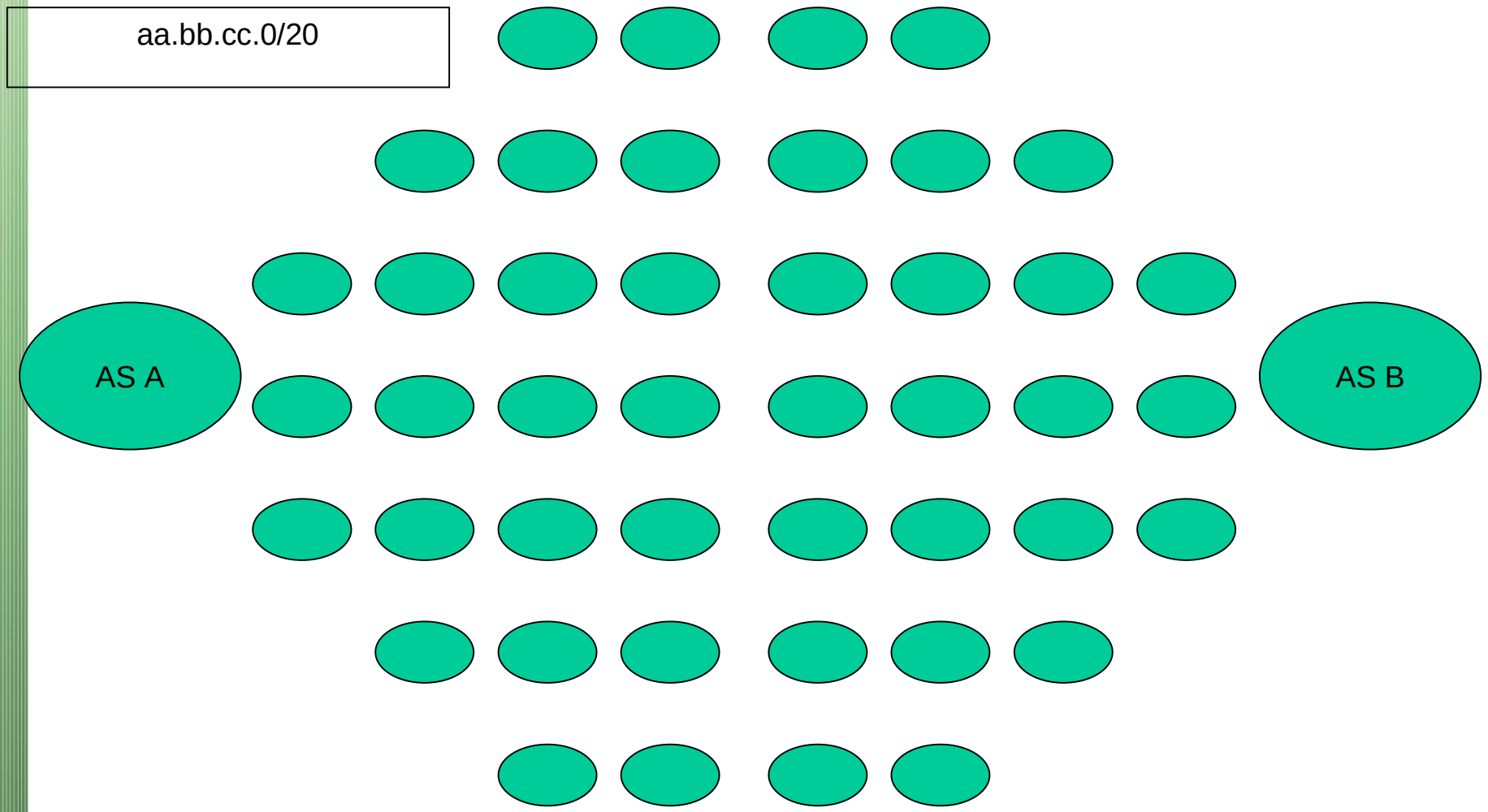
BGPの経路選択順番の基本２

- 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

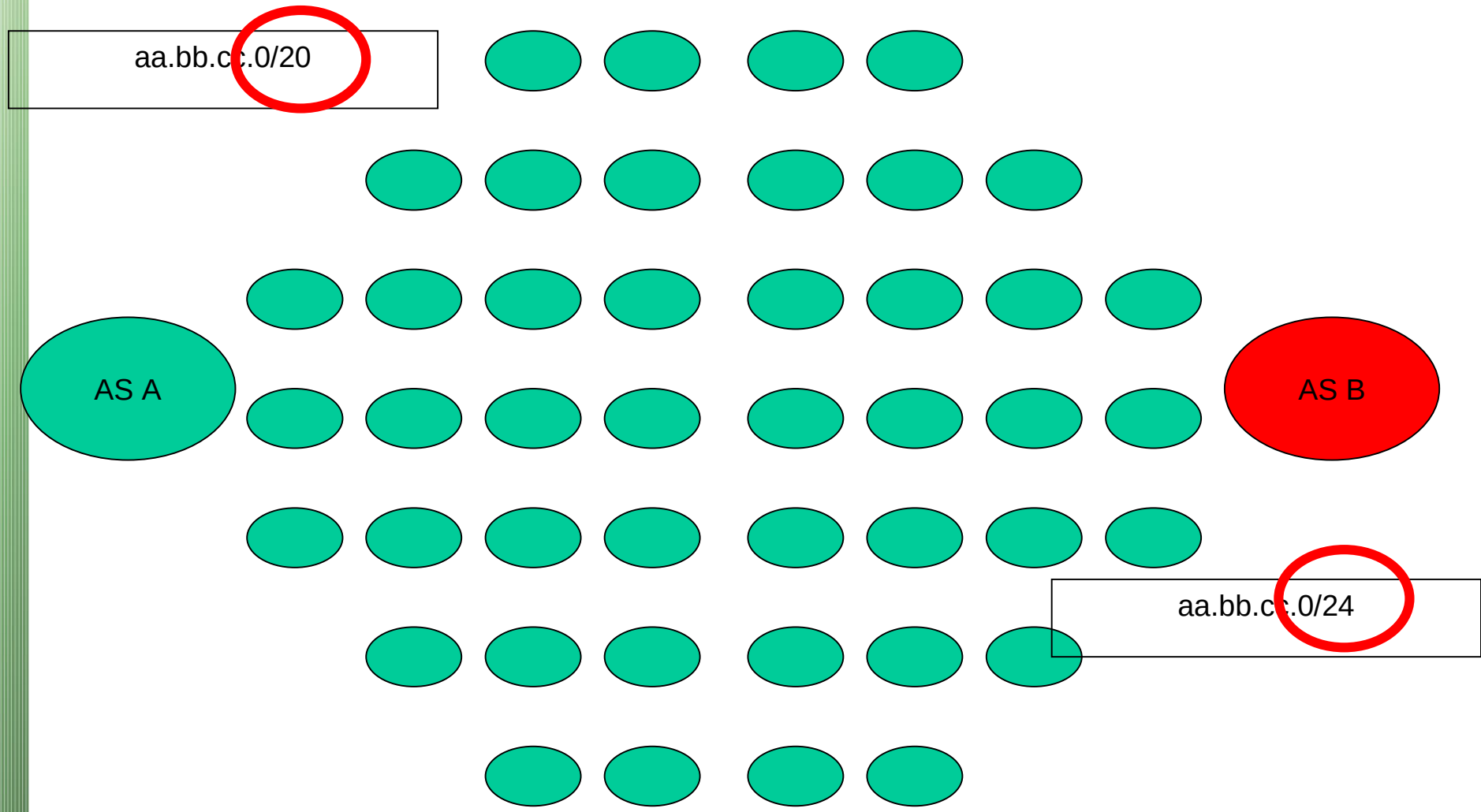


この場合、経由AS(＝ASPATH)の少ない経路が選択されます。

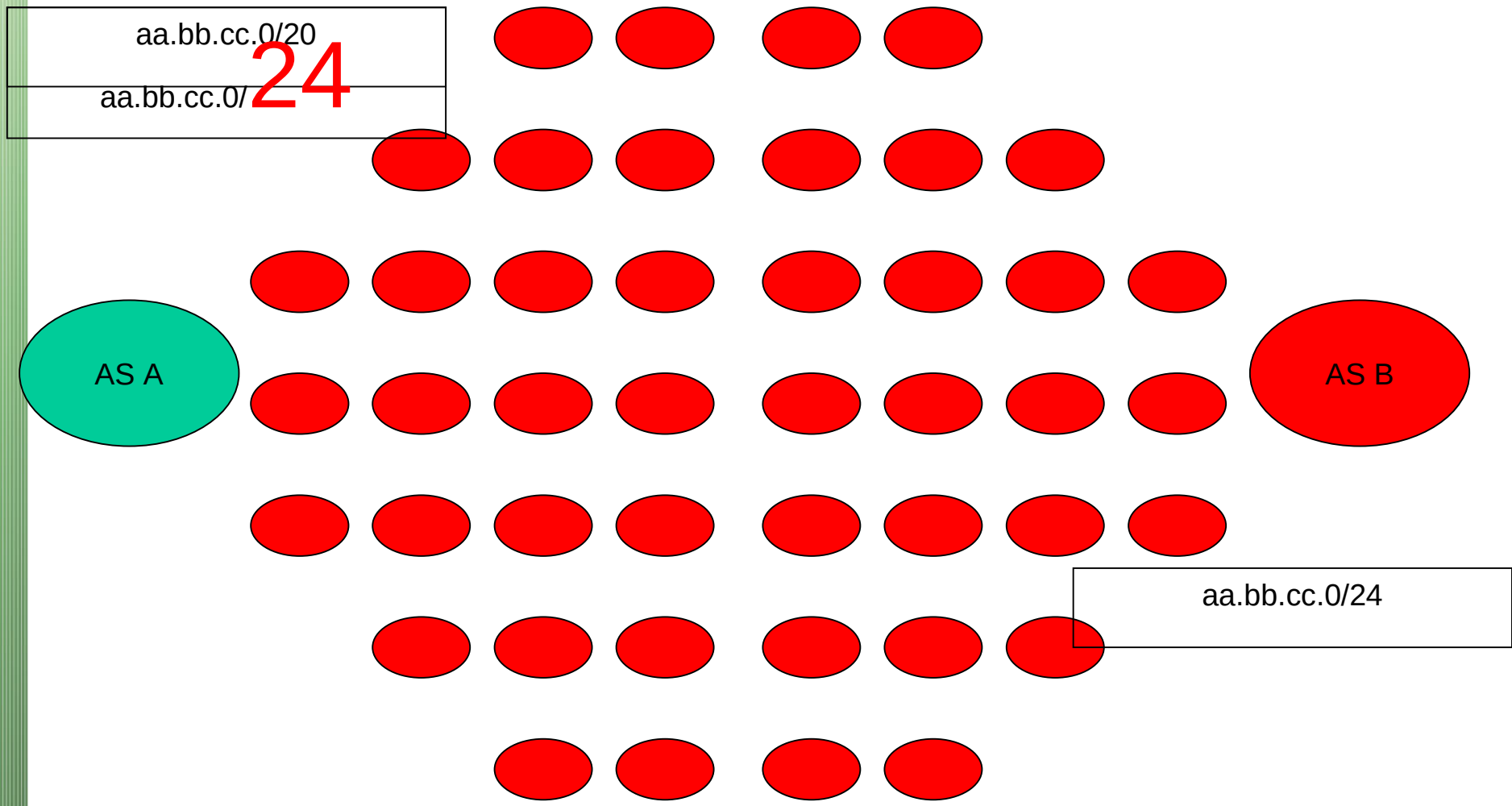
乗っ取られていない無い状態



乗っ取り発生発生

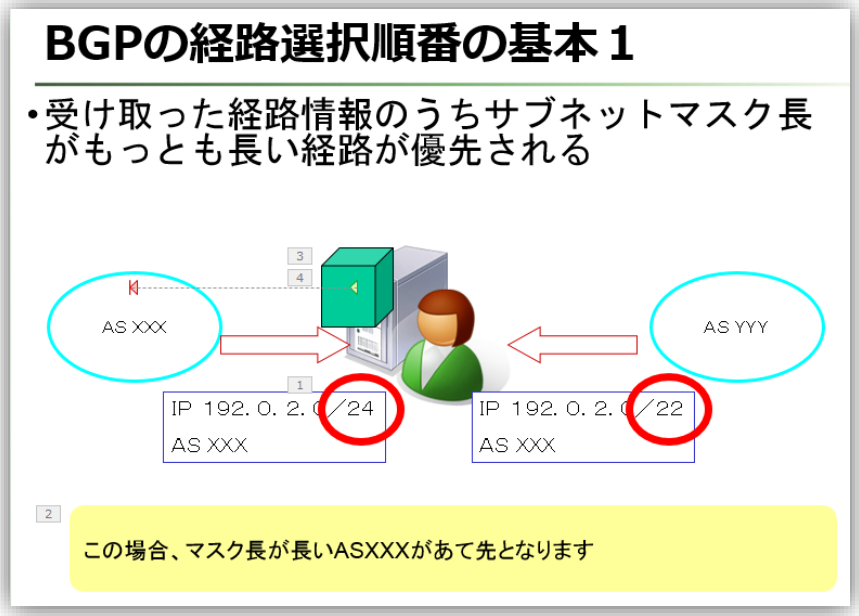


経由したASの距離 勝負

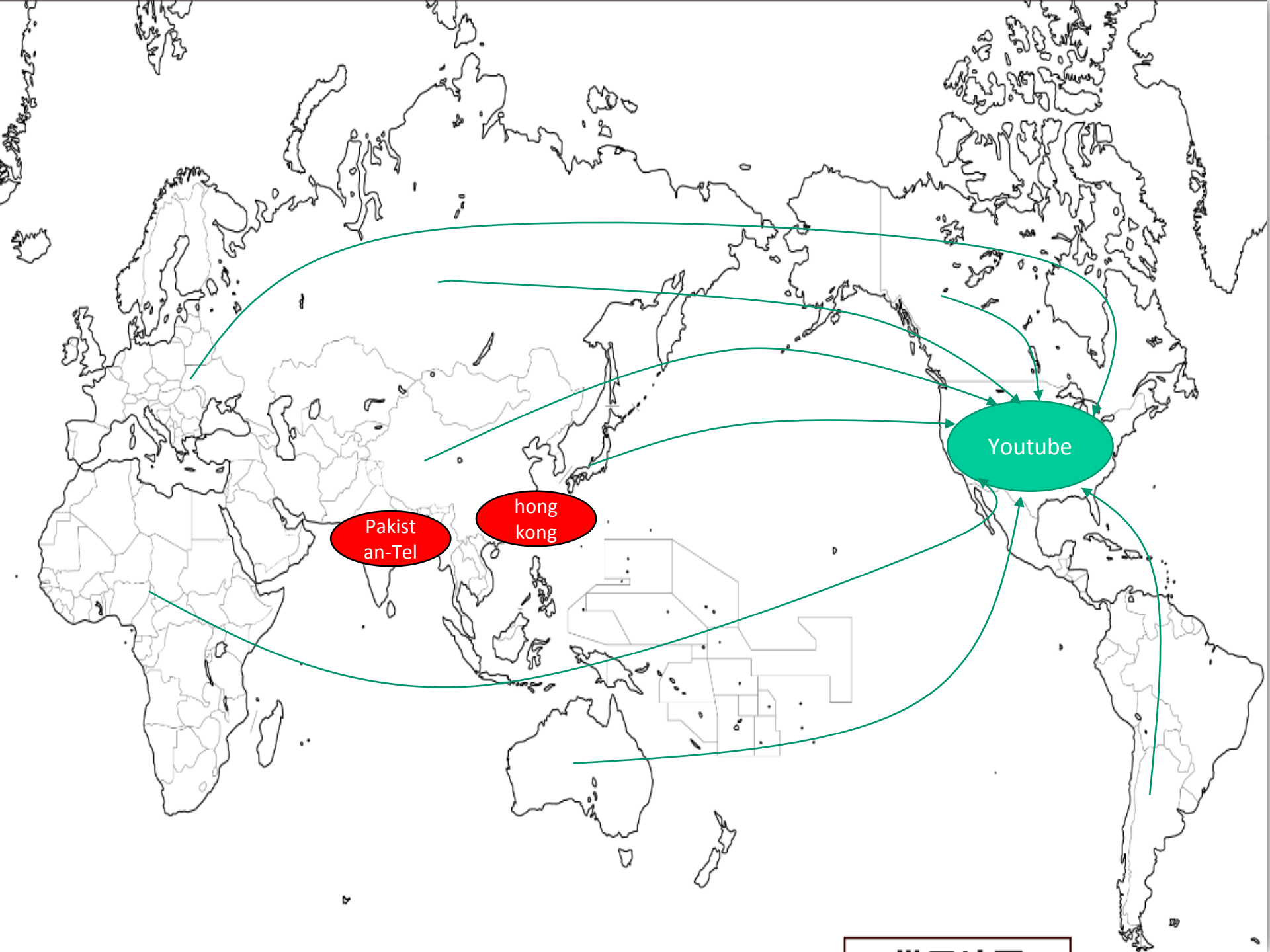


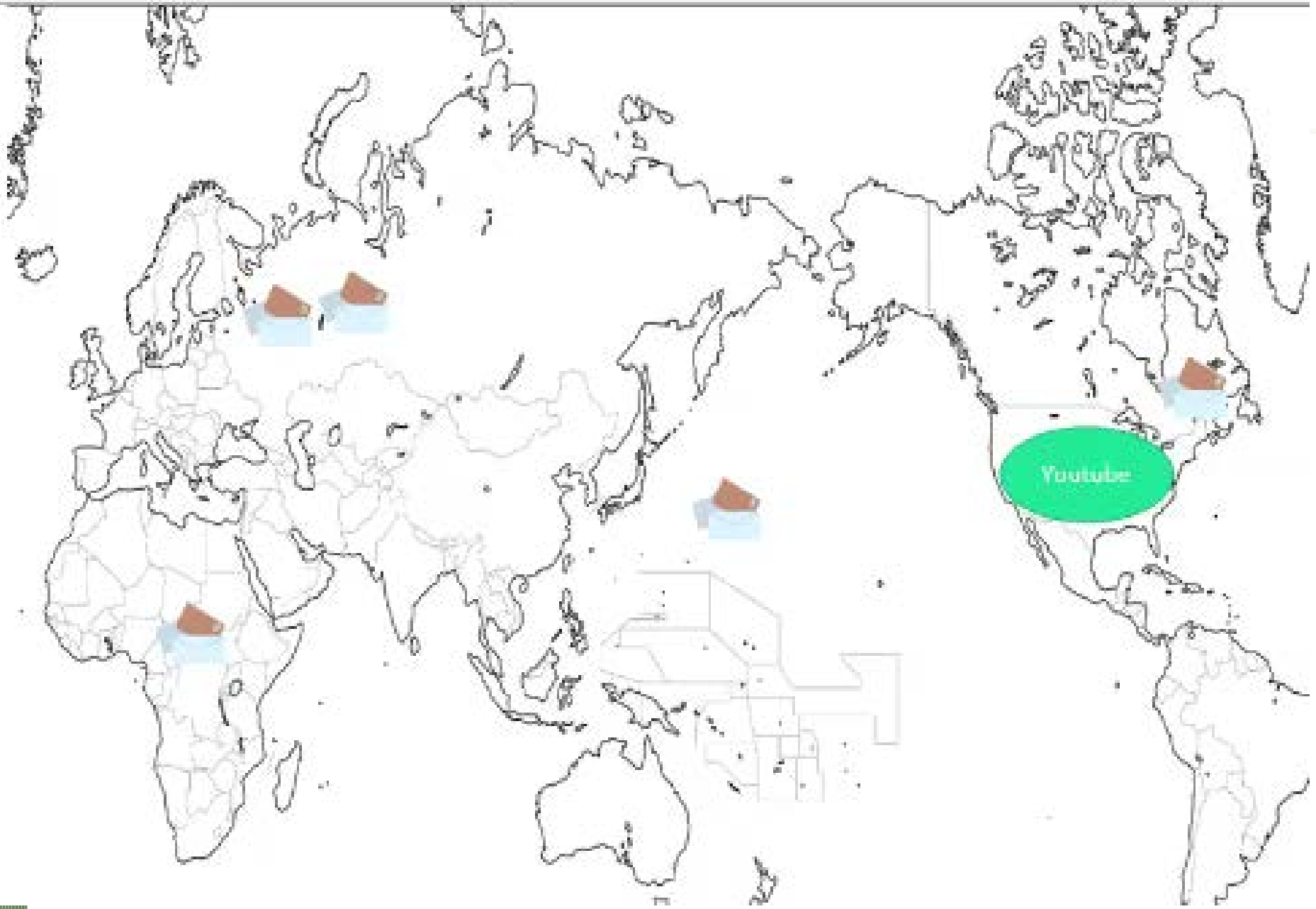
代表的名事例：Youtubeの乗っ取り

- **通常：AS36561 Youtube**
  - 208.65.152.0/22にてサービス
- **2008年2月24日 18:47**
  - AS17557 Pakistan Telecom 208.65.153.0/24

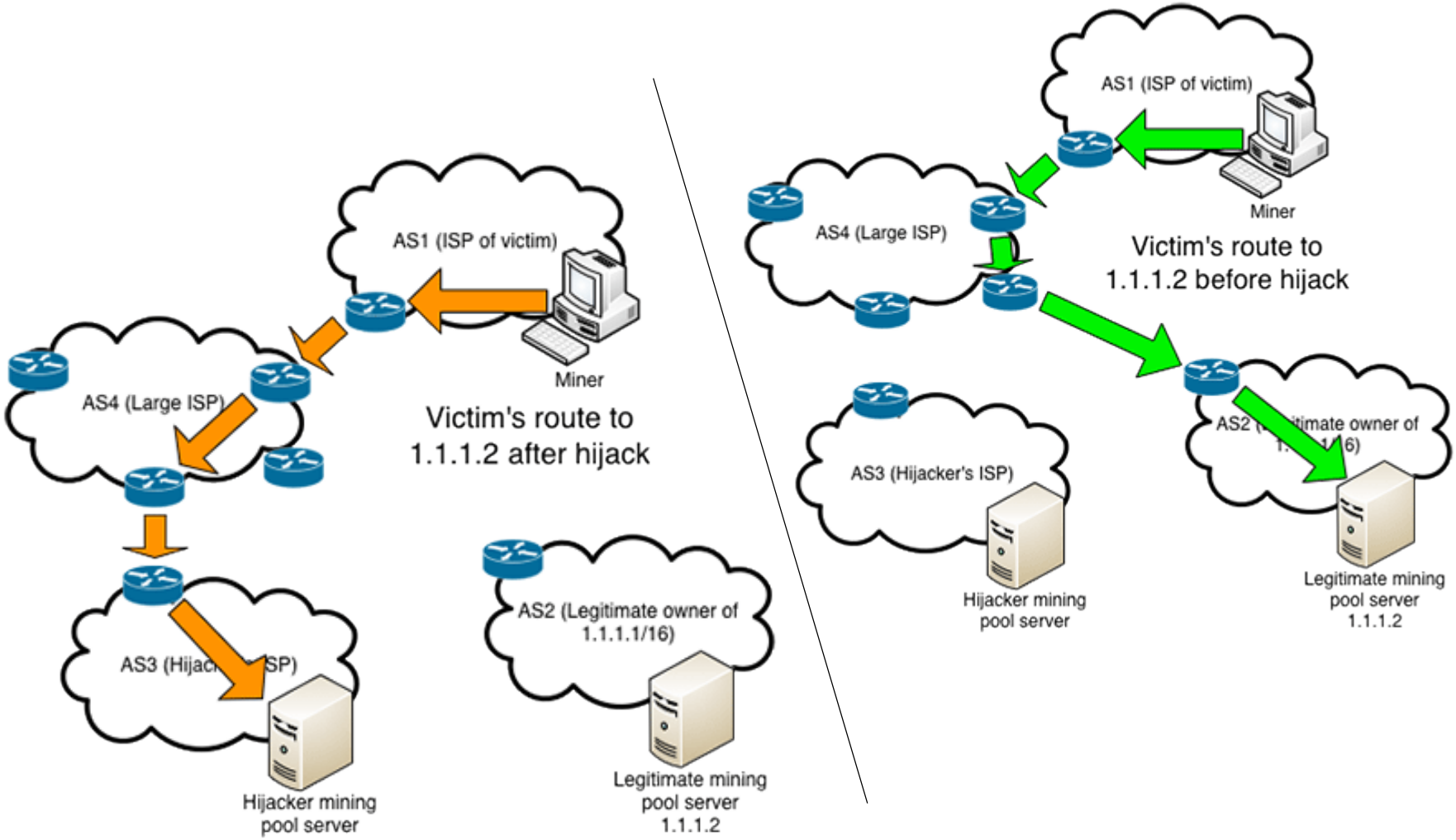


以後2時間の間,地域によってはYoutube断


Youtube
hong kong
Pakist an-Tel



BitCoin発掘の乗っ取り



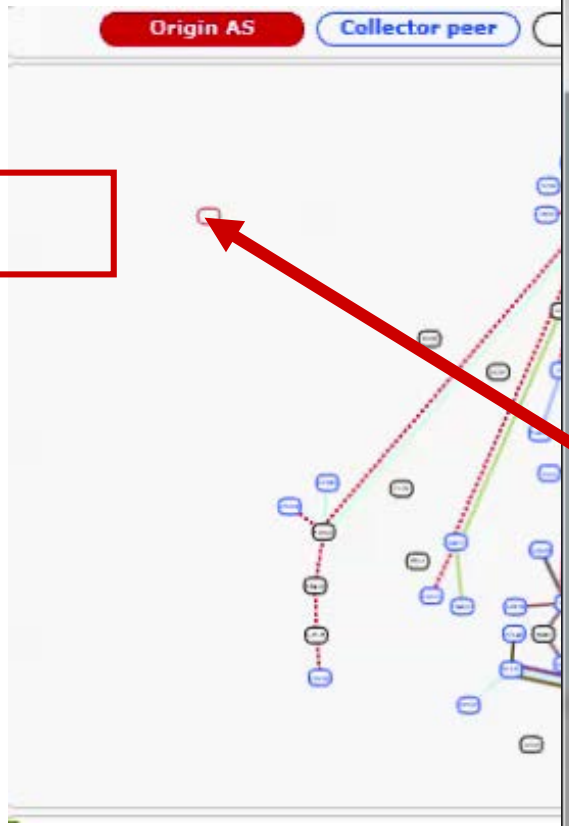
BGP Hijacking for Cryptocurrency Profit, 7 August 2014
Pat Litke and Joe Stewart, Dell SecureWorks Counter Threat Unit
http://www.secureworks.com/cyber-threat-intelligence/threats/bgp-hijacking-for-cryptocurrency-profit/

USの経路が乗っ取りによりロシア経由

- Renesys Blogより
- http://www.renesys.com/2013/11/mitm-internet-hijacking/

USの経路が乗っ取り

ベラルーシ



The New Threat: Targe ×

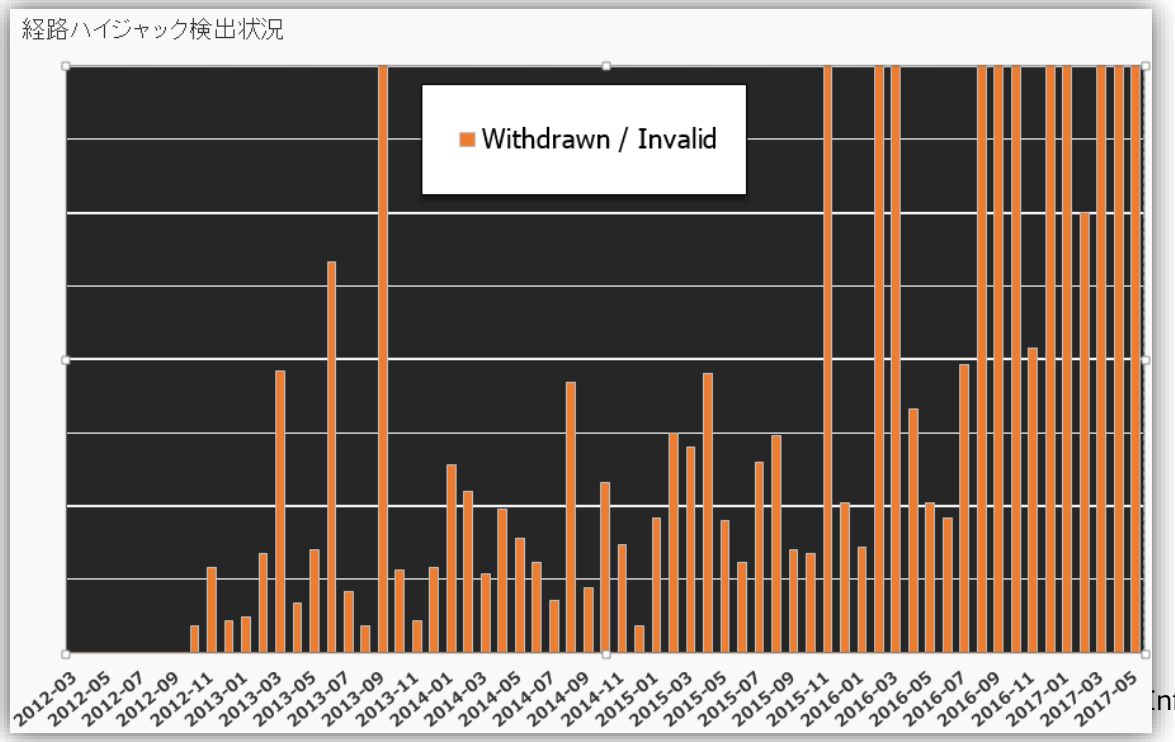
www.renesys.com/2013/11/mil

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

IP	Delay (ms)	Notes
201.151.31.149	15.482	pc-gdl2.alestra.net.mx (Guadalajara, MX)
201.163.102.1	17.702	pc-mty2.alestra.net.mx (Monterrey, MX)
201.151.27.230	13.851	igmty2.alestra.net.mx (Monterrey, MX)
63.218.121.49	17.064	ge3-1.cr02.lar01.pccwbtn.net (Laredo, TX)
63.218.44.78	64.012	TenGE11-1.br03.ash01.pccwbtn.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	mskn01.transtelecom.net (Moscow, RU)
217.150.62.233	228.461	BelTelecom-gw.transtelecom.net (Minsk, Belarus)
87.245.233.198	225.516	ae0-3.RTJRX.FKT.DE.retn.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)

被害が都度報告されない頻発事例

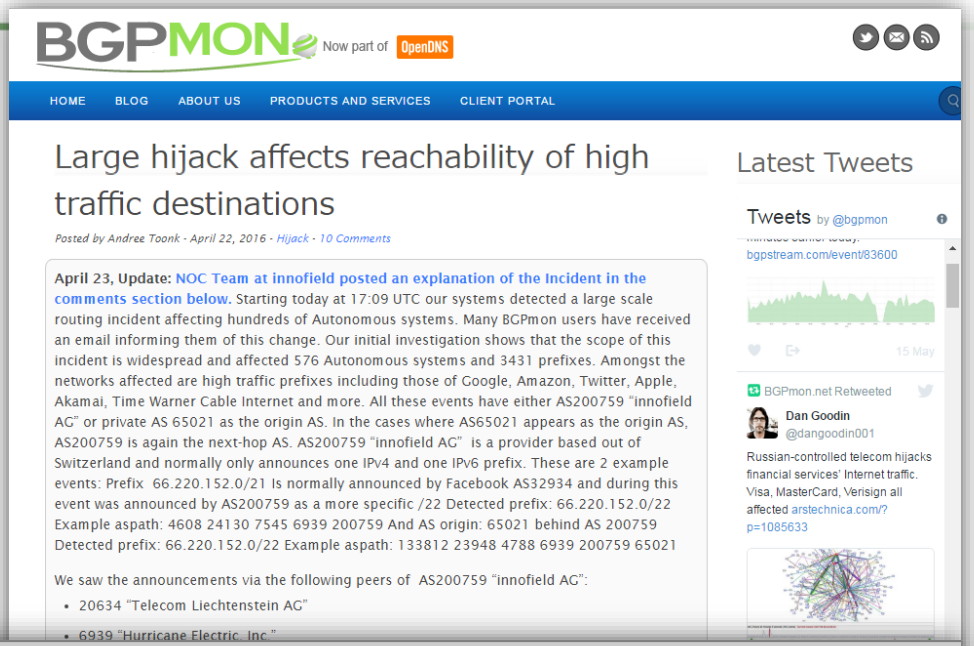
- **ほとんどがルータの設定ミス**
  - Typoなど”set ip address 192.16”7”.0.0/24
    - Global アドレスを設定してしまっている等
    - 相互信頼のため相手は正しいと思ってしまう
- **国内の発生状況**



３．国内・国外の乗っ取り検知の取り組みと状況

世界の検知・記録システム

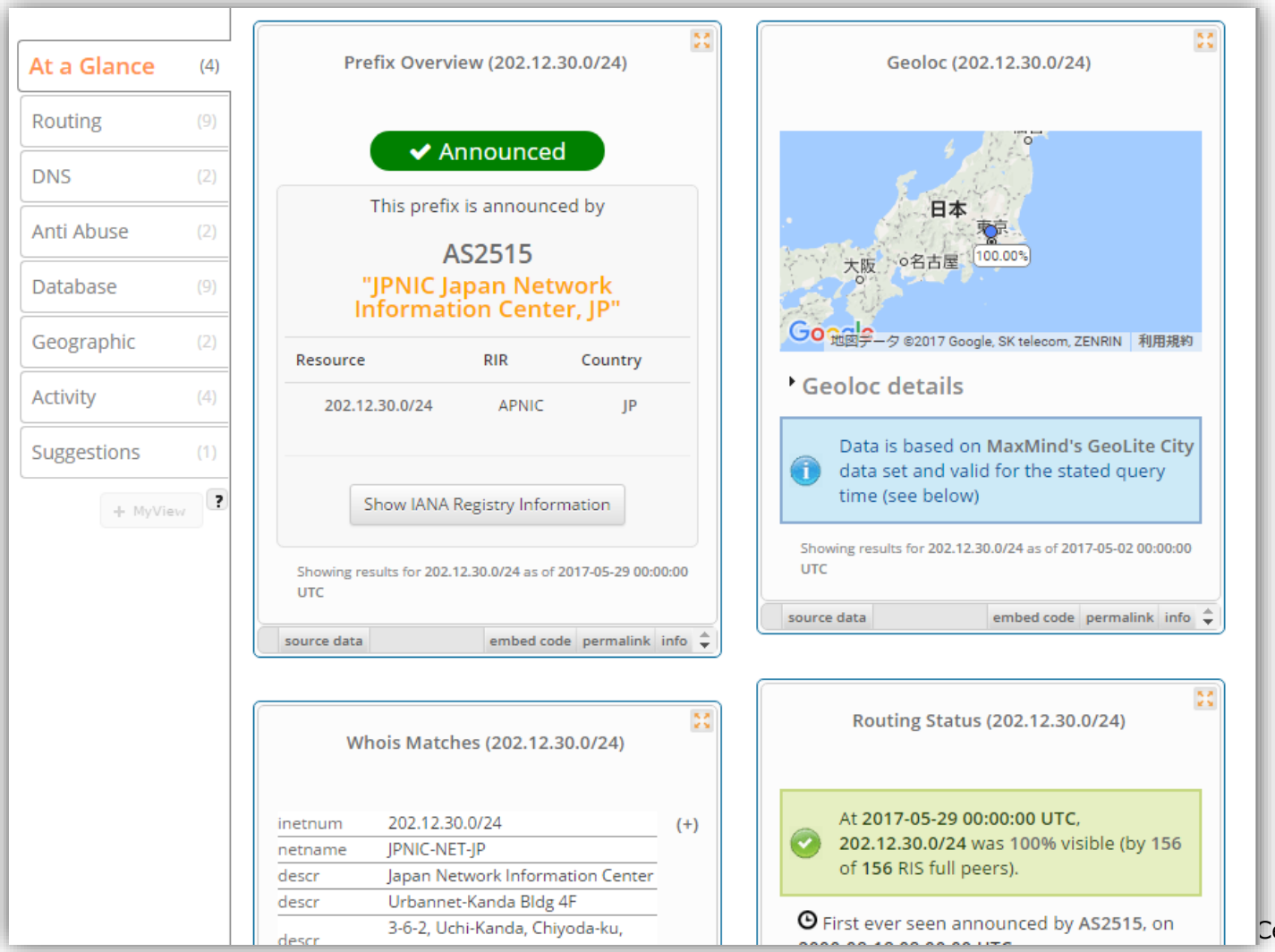
- **BGPMON**
  - USの観測団体
- **RIPE Stats**
  - EU地域の技術集団
- **RouteViews Proj**
  - US Oregon大学



JPNIC

RIPE Stats

- https://stats.ripe.net/



日本国内の検知の状況(経路奉行)

- 日本のISP・通信事業者の経路13社を観測
- 必要があれば事業者へ乗っ取りを通知

JPNICのアドレスの情報とICT-ISAC 経路情報共有WGによる突合せシステム

検知システムの課題

- **IPアドレスとASをセットにした情報が不完全**
  - IPアドレスとASの組み合わせは何を信じる？
  - 経路が先か？別途運用者のデータベースが先？
- **観測点を多くしないと検知率低**
  - 遠くの乗っ取りは”見えない“
  - 遠隔地との連携が不可欠
- **防ぐことができていない**
  - 利用者･運用者の人の輪による誤経路の排除が現状
  - 最終的に誤経路の直近にて遮断

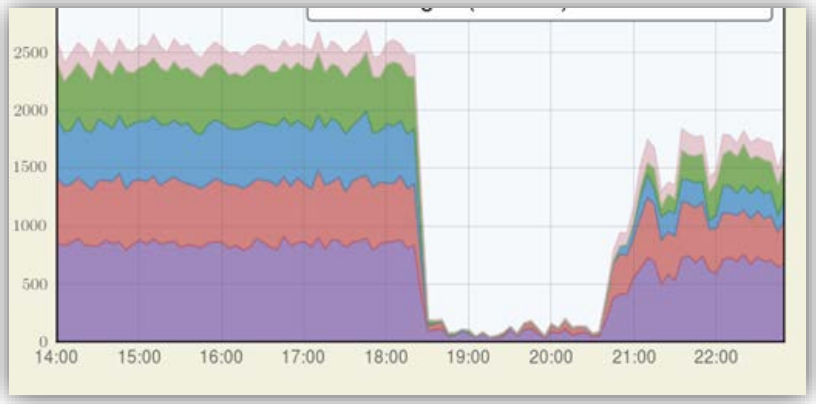
４．ルーティングトラブル 具体例と将来の対策？

つながらない！

- **Webを見るさまざまな要素に乗っ取りが関係**
  - 絵(DNS、コンテンツ、Web自体)
- **乗っ取りの可能性のあるポイント**
  - DNS：DNSサーバのIPアドレスの乗っ取り
  - Web：WebサーバのIPアドレスの乗っ取り
  - パケット転送：
    - たまたま途中の経路で落ちているだけ
    - **不適切なASへの転送**
- **これらの要因が関係してつながらないor不適切なサイトへの誘導が発生**

乗っ取りにの場面ごとによくある事例

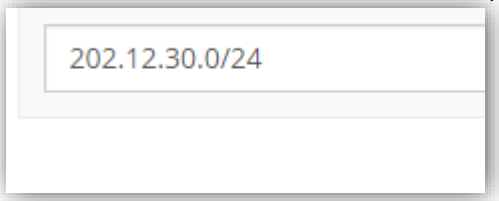
- **自組織のIPアドレスが乗っ取られた場合**
  - お客さんパケットが来ないためトラフィック減
  - 完全に0になるわけでないので発覚が遅れる

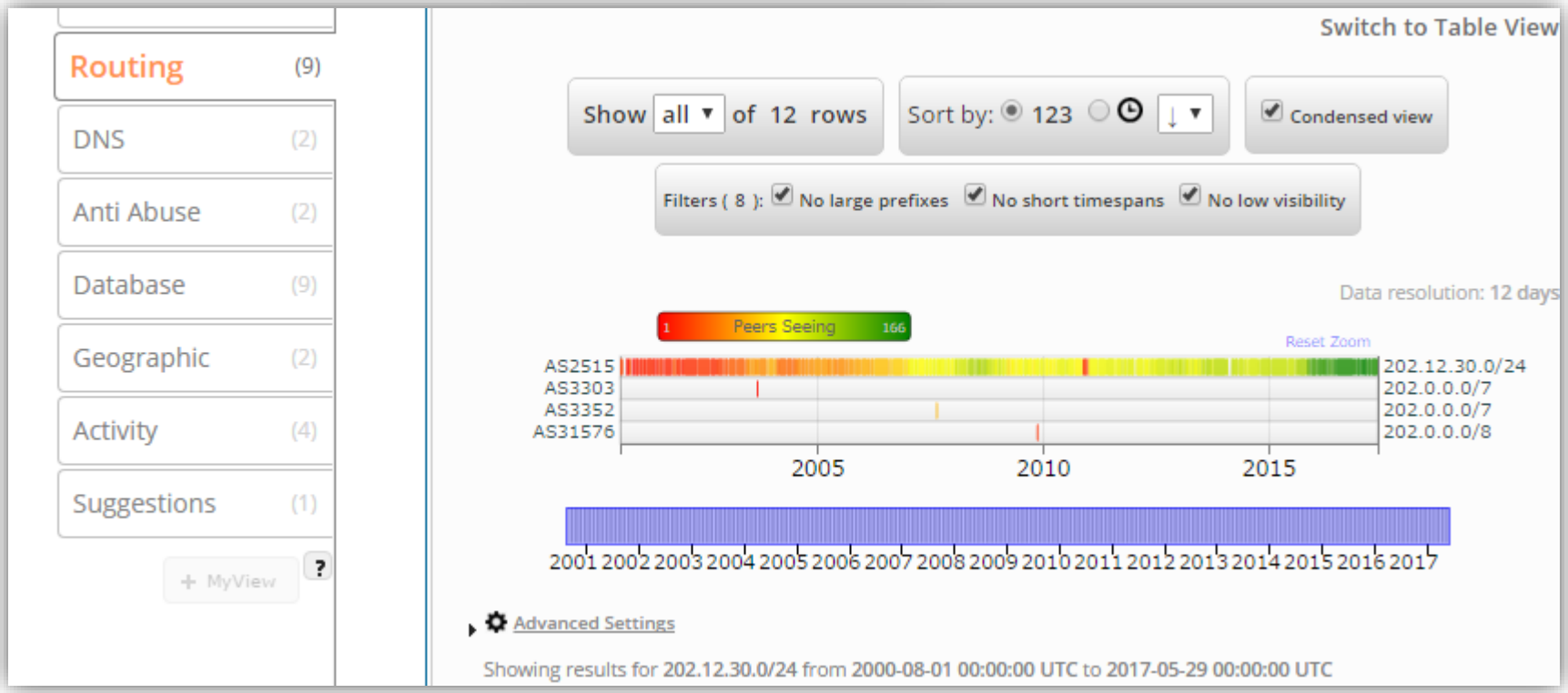


- **利用したいサービスが乗っ取られた場合**
  - つながらない・悪意のあるサイトへ接続
- **(意図せず)自分が乗っ取りを行ってしまった場合**
  - 大量のトラフィックによる自NWの停止

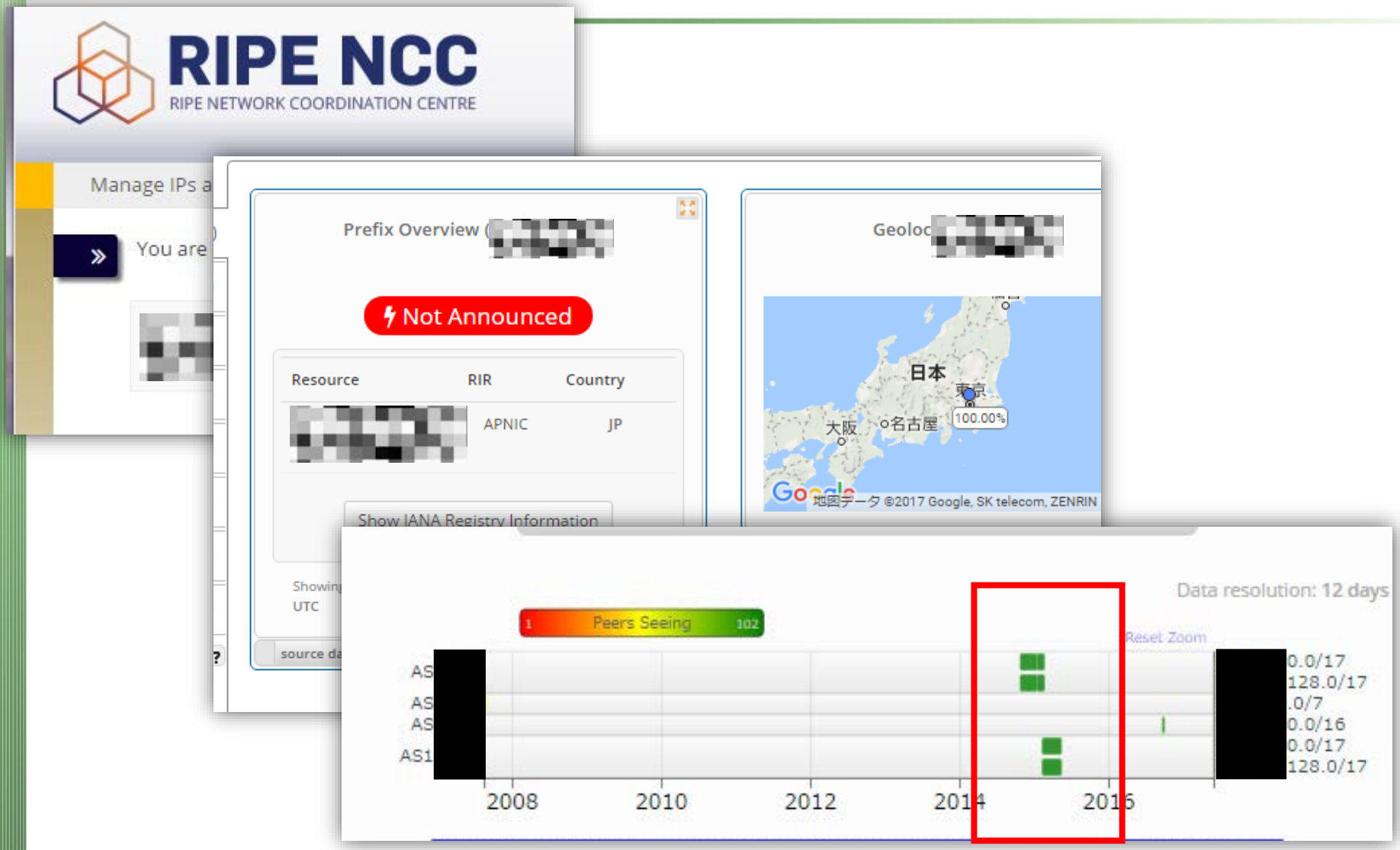
状況把握：適切な状態

- 前項の検出・RIPE Stats等過去経路を照会





状況把握：何らかの問題が存在



解決に向けて

- **まずは現状を把握**
  - 自分の接続に使うIPアドレスを調べる
  - ツールによって、遠方でどのようにみえる？
    - 自組織のIPアドレスに問題がなさそう
      - ルーティング以外の問題へ
- **ルーティングの問題であれば？**
  - 自組織の”上流”NWへ相談
  - コミュニティへ相談（ML・有識者・JPNIC）
  - 乗っ取っている組織へ直接連絡
  - 乗っ取っている組織へ接続している組織へ連絡

将来に向けて

- **脅威を見つけるための情報の整備**
  - IPアドレス＋AS番号＋PKIなどの仕組みの整備
    - 現在進行中
  - ルータによる上記仕組みの実装
    - 現在進行中・・・
  - 世界規模での上記の普及
    - これから！

まとめ

- **つながらない！にはルーティングも関係**
- **ルーティングによるつながらない**
  - BGPによる経路情報（IP＋ASの情報）の漏れ
    - 設定ミス・機械の問題など
  - ルーティングの乗っ取り
    - Webサービスののっとり
    - DNSののっとり
    - パケットを意図せず吸い込む乗っ取り

問題解決の際の一つの可能性として