

押えておきたい基盤技術(3)

インターネットルーティングセキュリティ 最新動向

～そのつながらないルーティングかも～

InternetWeekショーケース in 広島

2018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

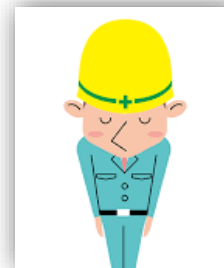
岡田 雅之



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？
- 実は経路が乗っ取られている？？



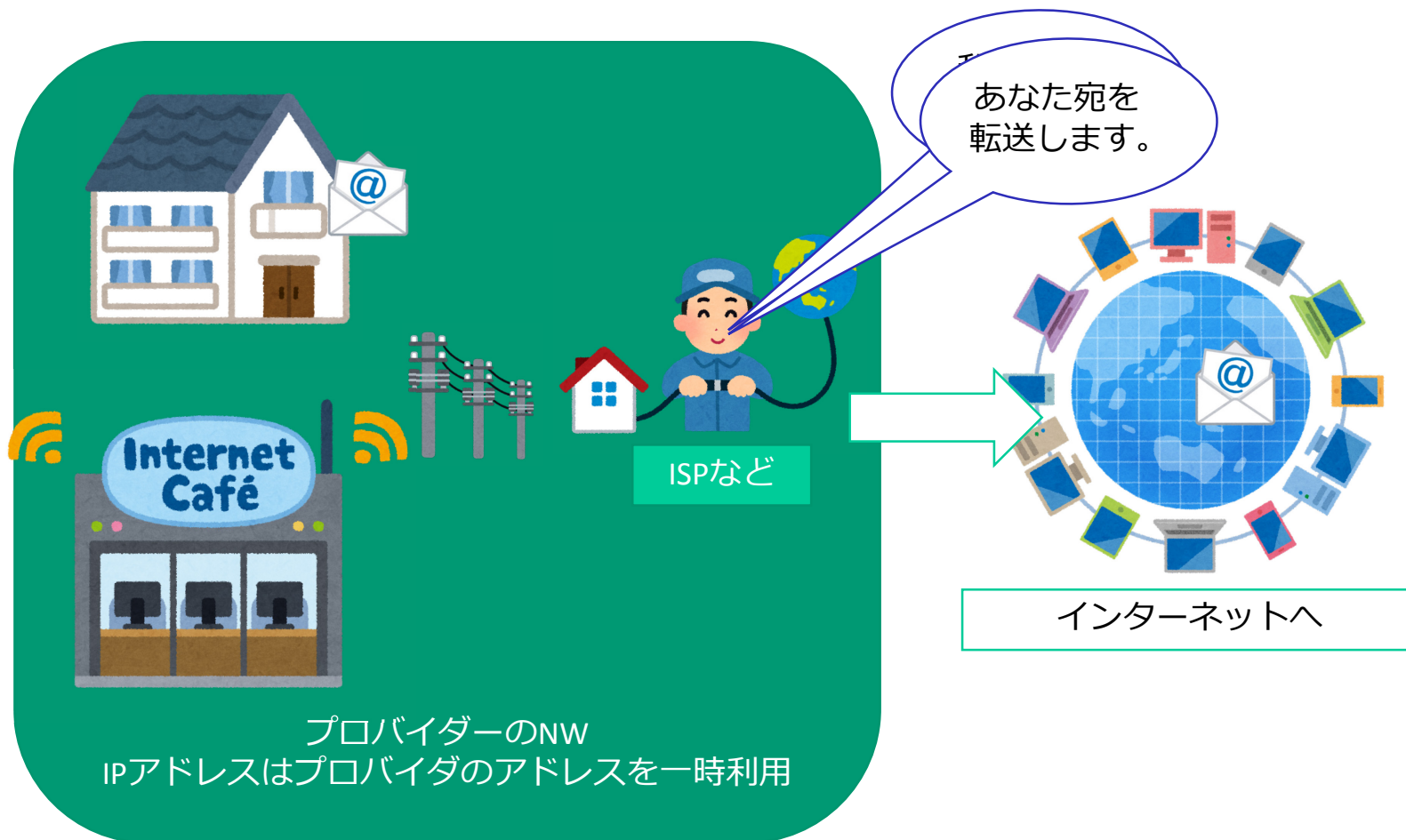
- 本セッションでは

- 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

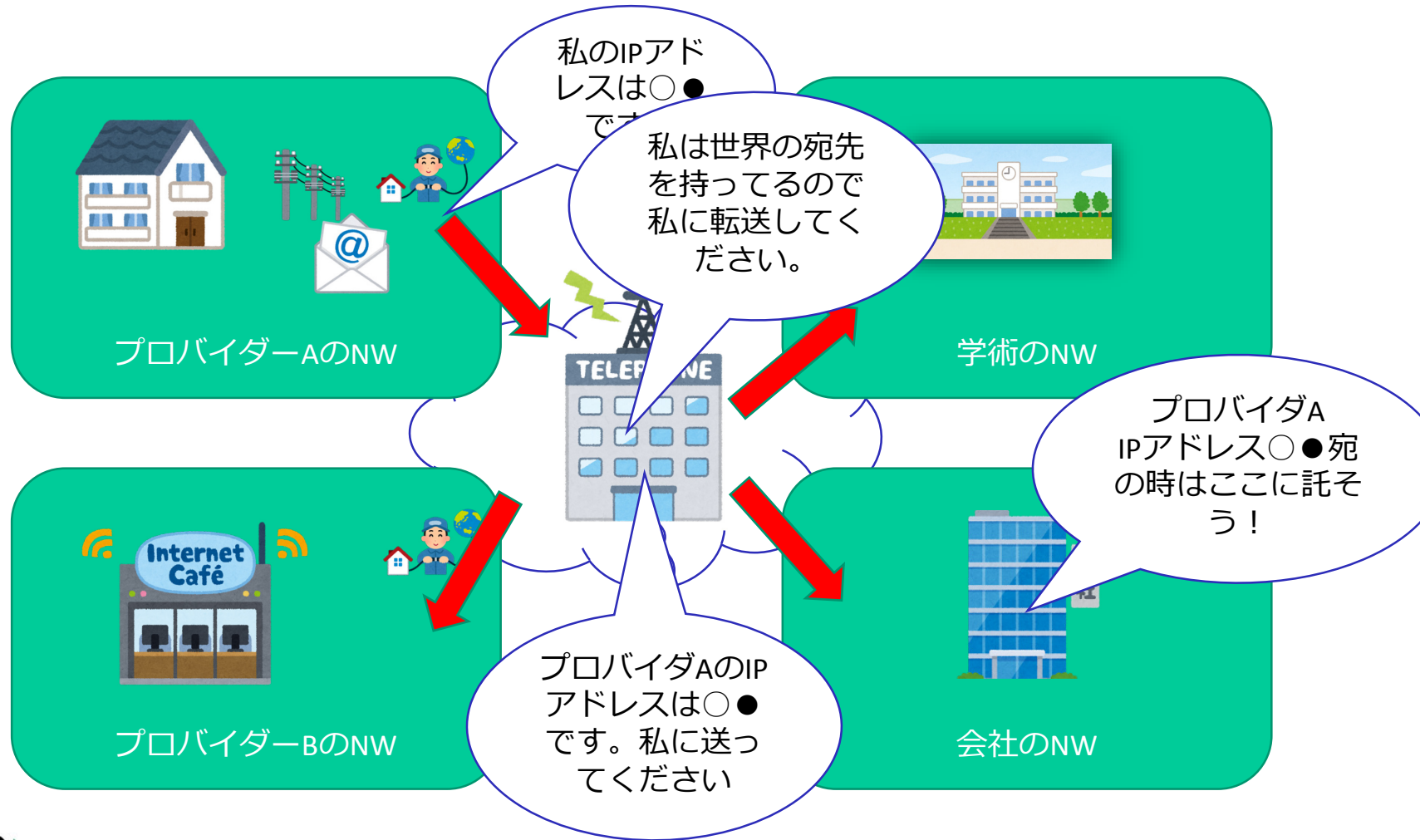
1. ルーティングと相互信頼

ルーティングの世界：家庭～ISP

- 家庭～ISPのネットワーク

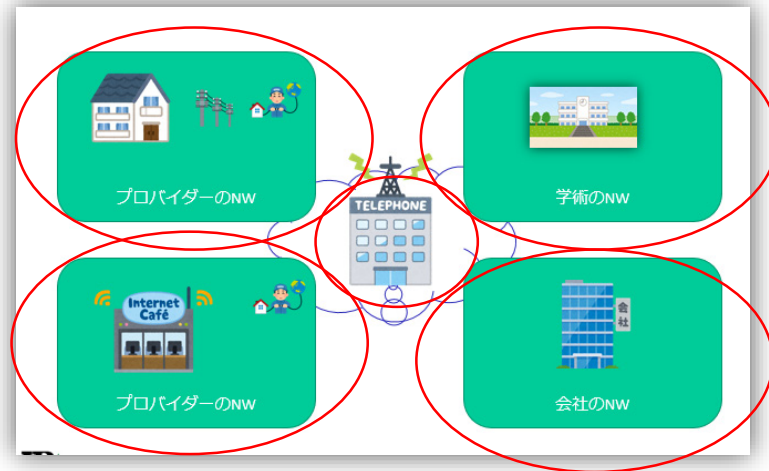


ルーティングの世界：ネットワーク同士



ルーティングの世界：ISP～BGP

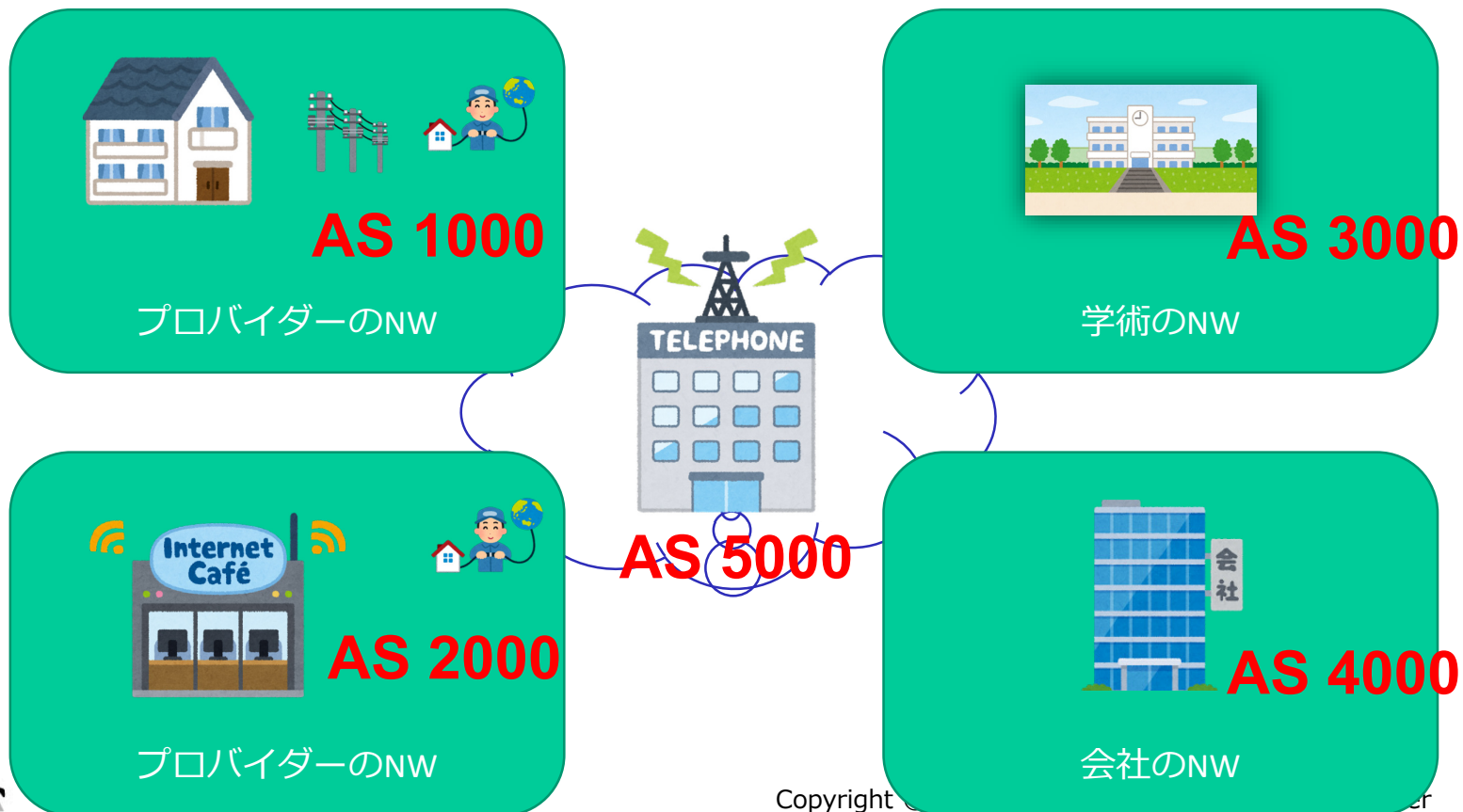
- 組織毎内部ルーティングからインターネットへ



- 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

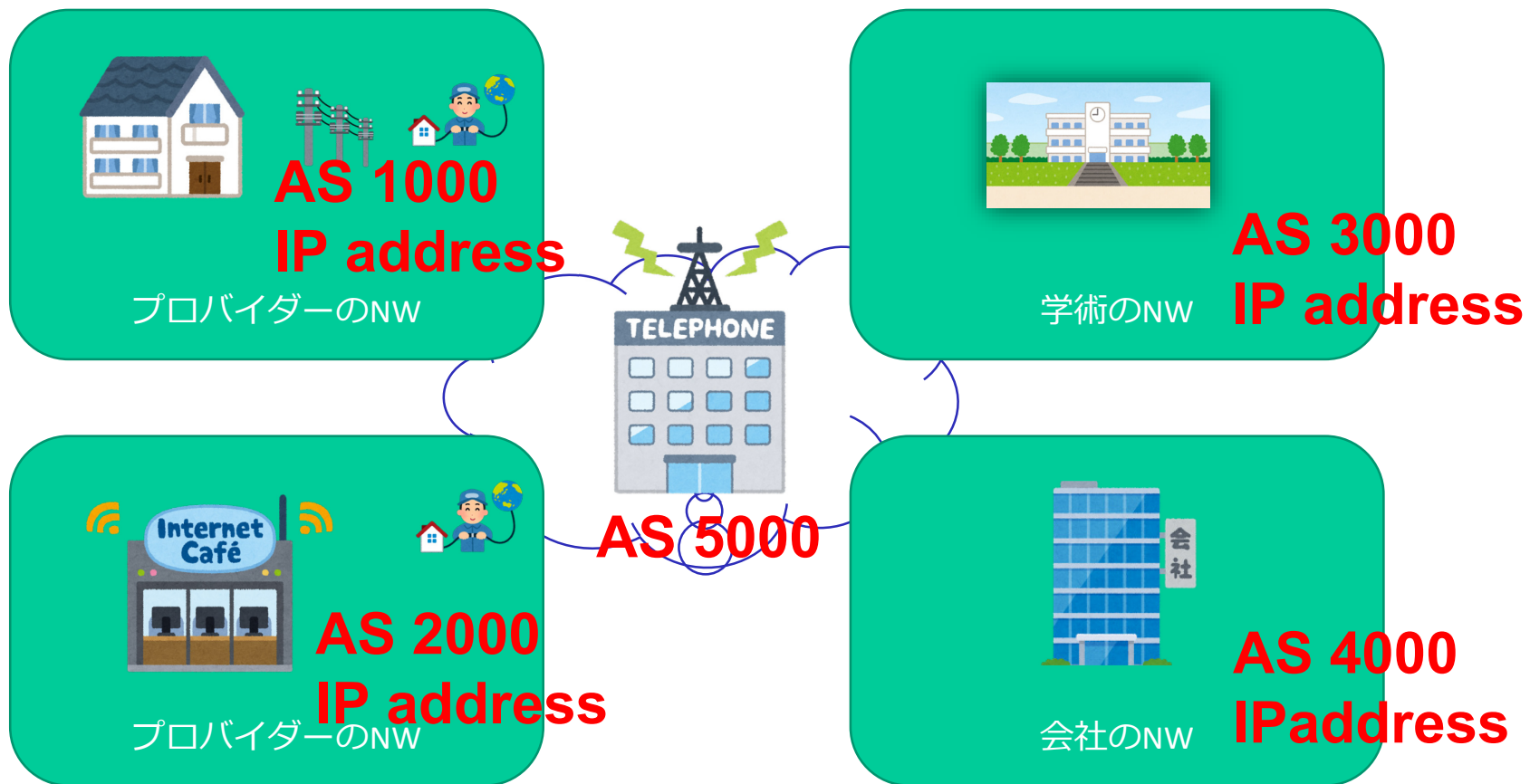
ルーティングの世界：AS番号

- 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



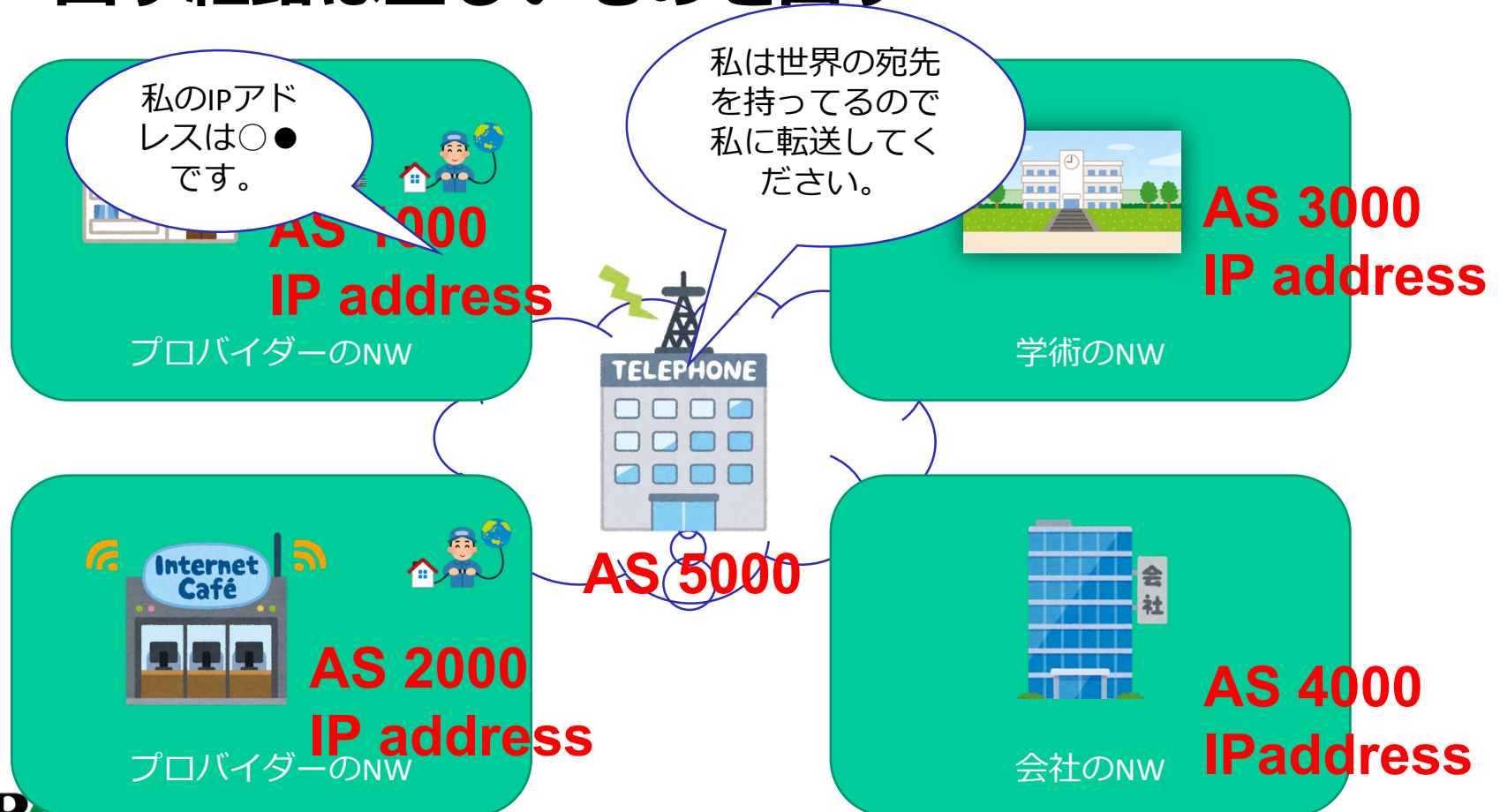
ルーティングの世界：BGP運用

- AS間のルーティング＝経路情報の交換



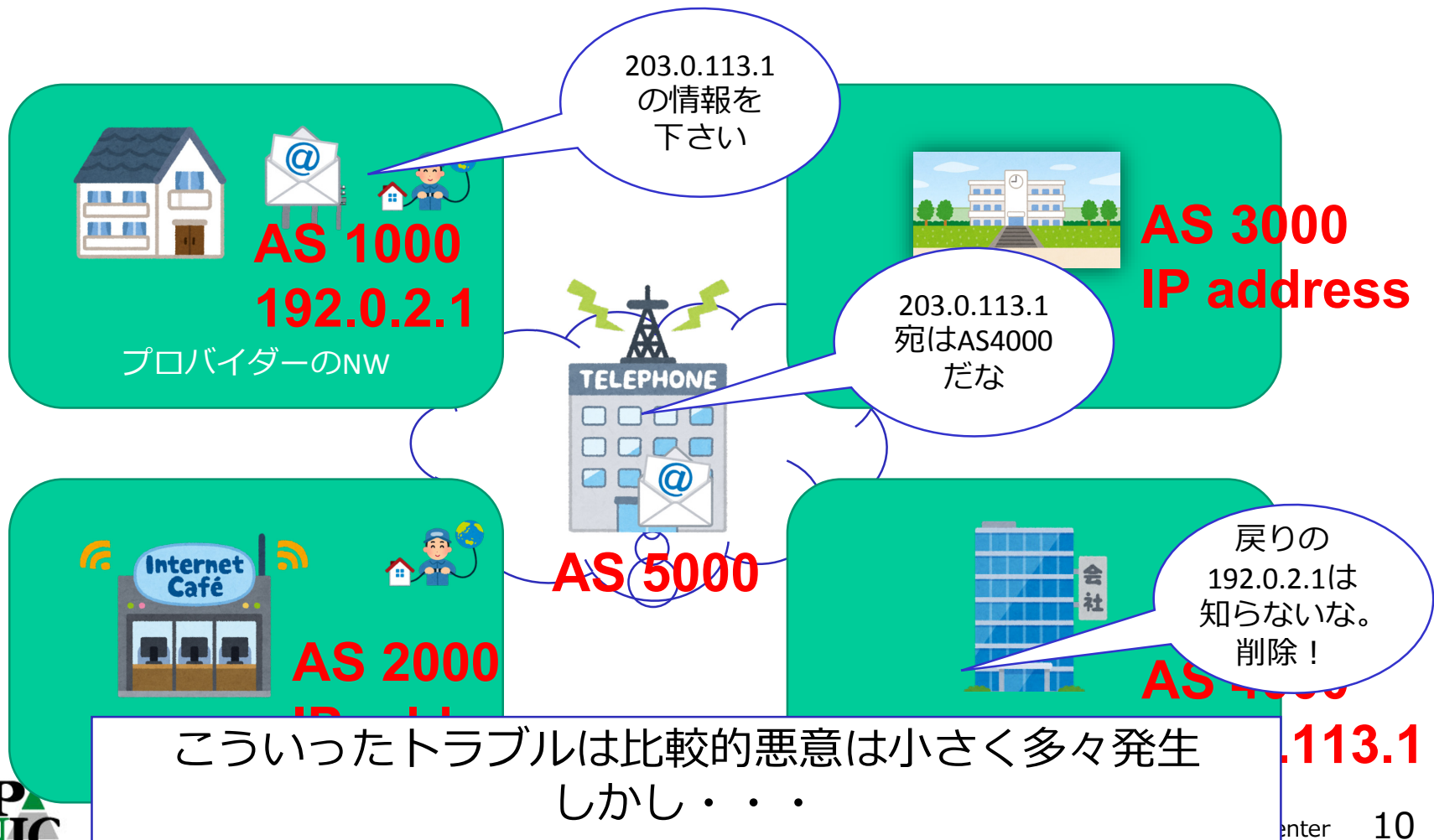
ルーティングの世界：相互信頼の実際

- 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



2. ルーティングを脅かすもの

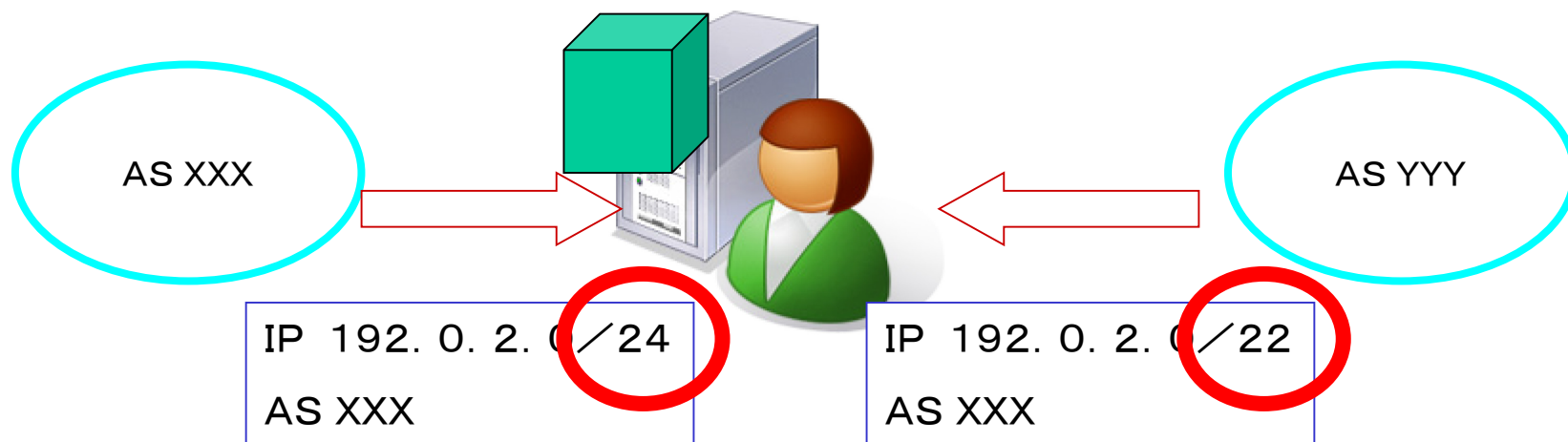
ルーティングの問題

- **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

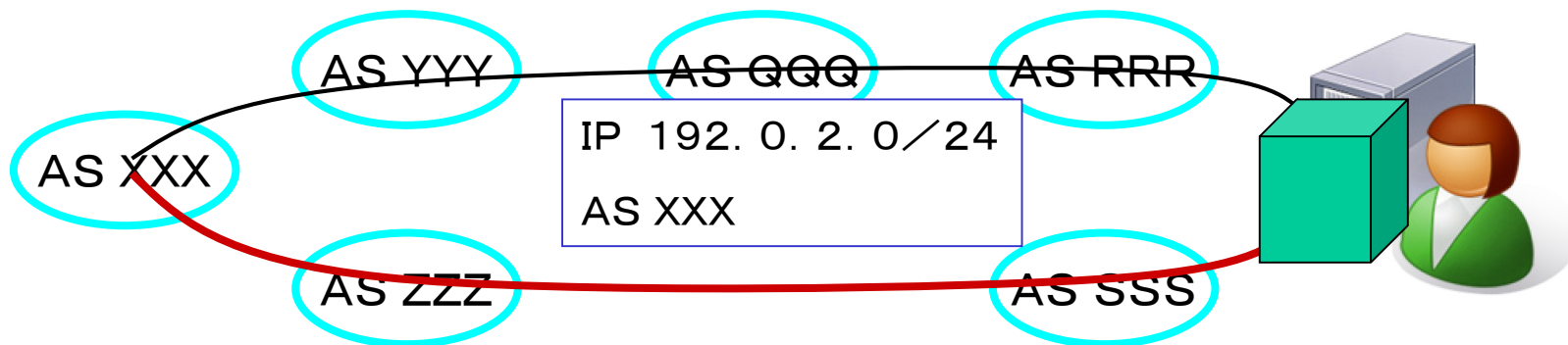
- 受け取った経路情報のうちサブネットマスク長がもっとも長い経路が優先される



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

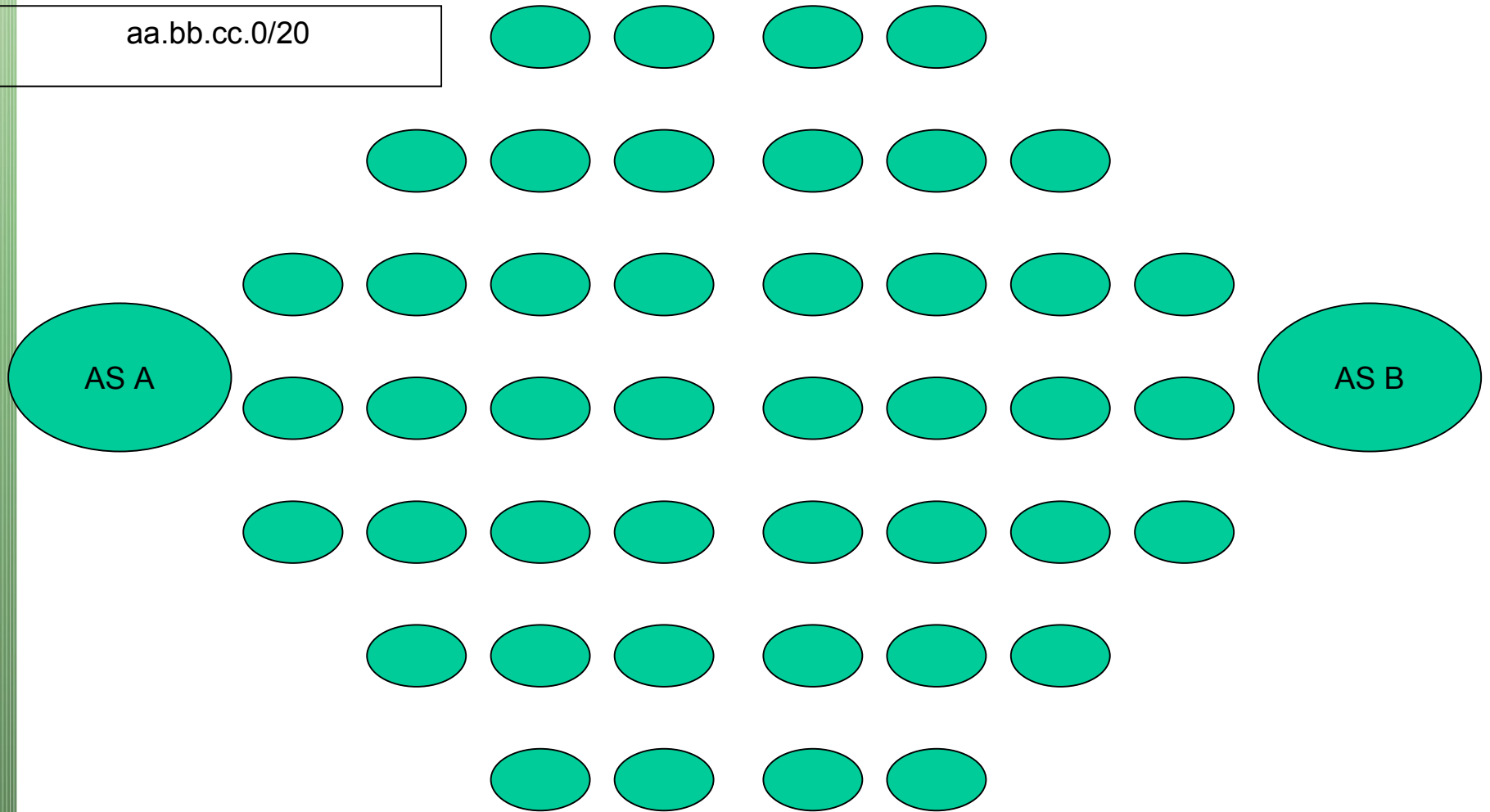
- マスク長が引き分けの場合、AS-PATH長(=経由してきたASの数)の短い経路を優先
 - AS XXX→AS YYY→AS QQQ→ AS RRR
 - AS XXX→AS ZZZ→AS SSS



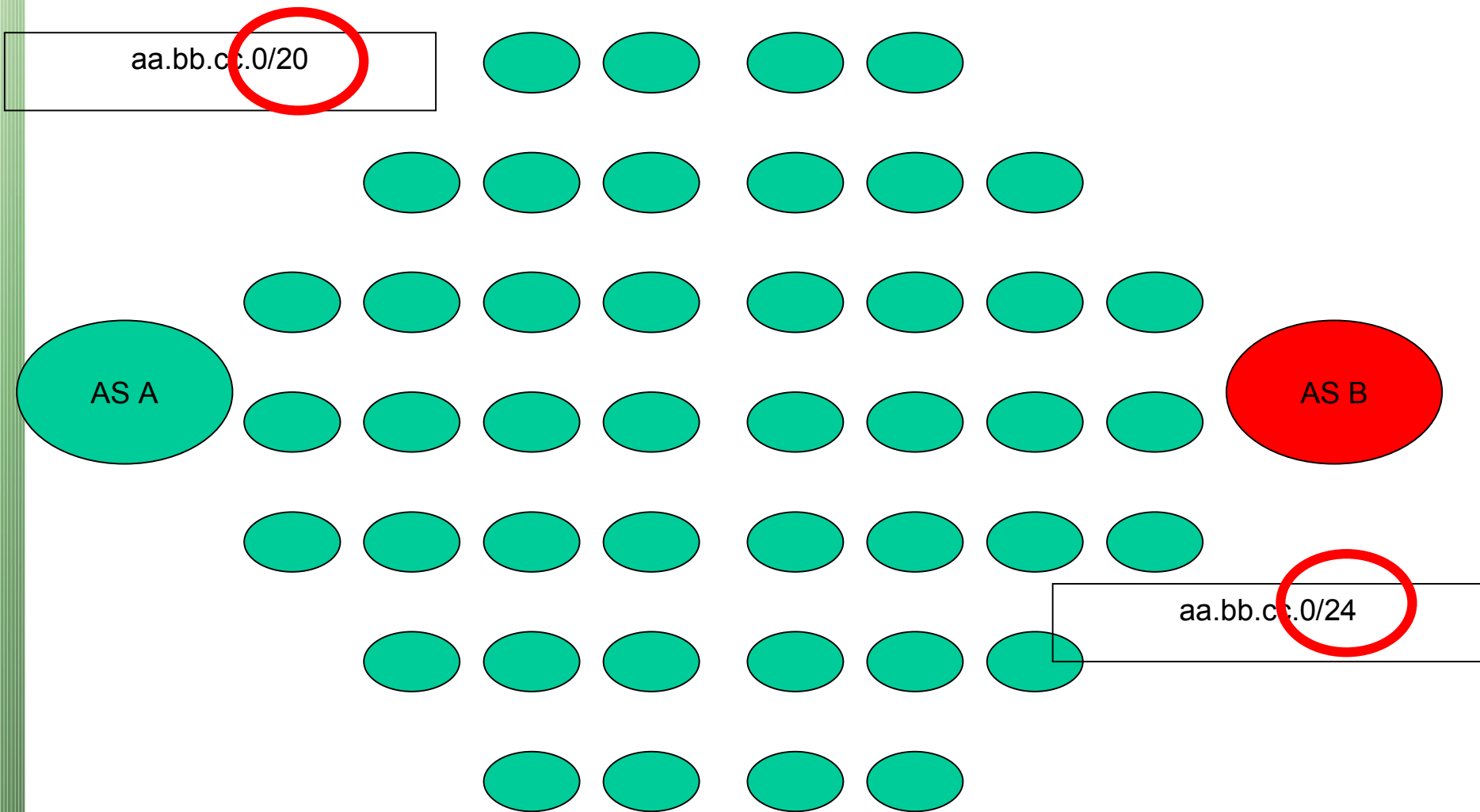
この場合、経由AS(=ASPATH)の少ない経路が選択されます。

乗っ取られていない無い状態

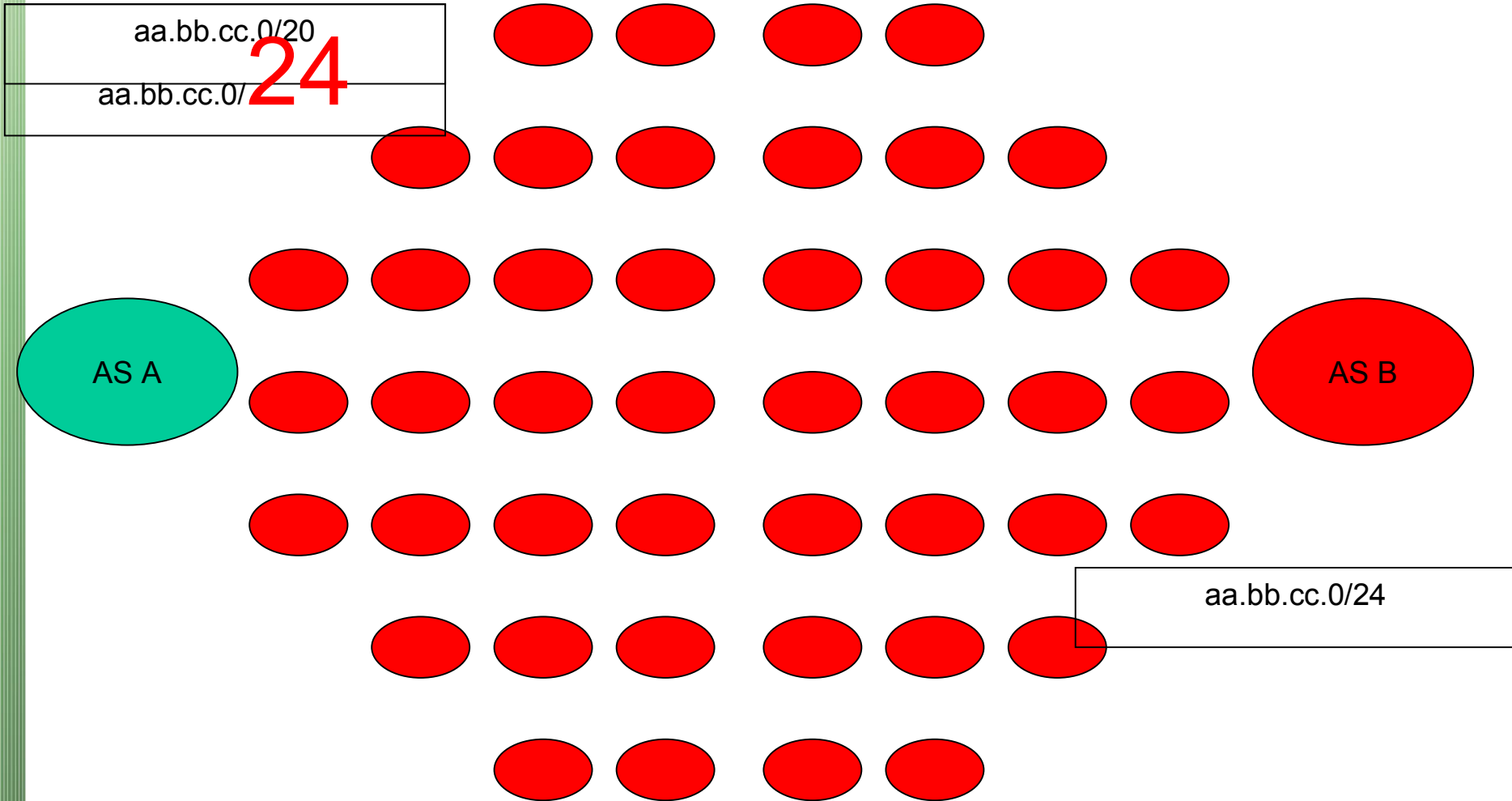
aa.bb.cc.0/20



乗っ取り発生発生

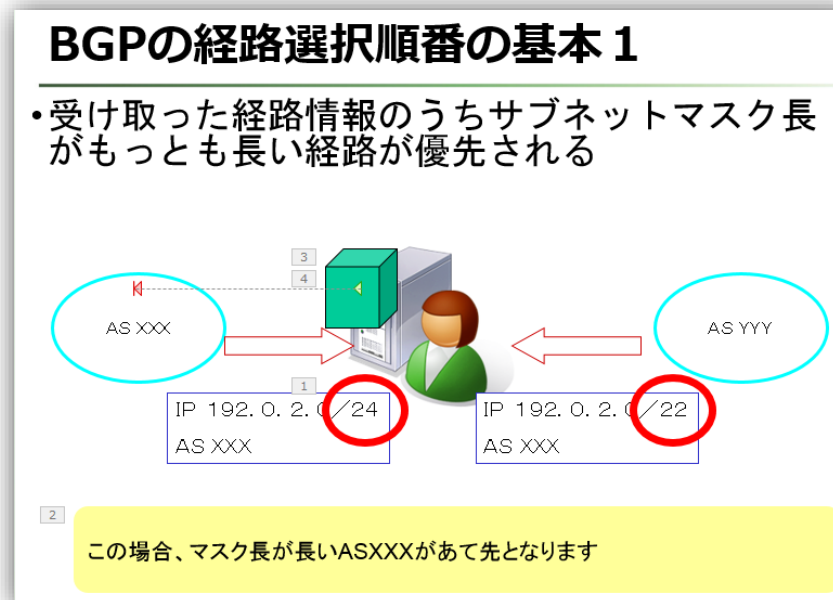


経由したASの距離 勝負

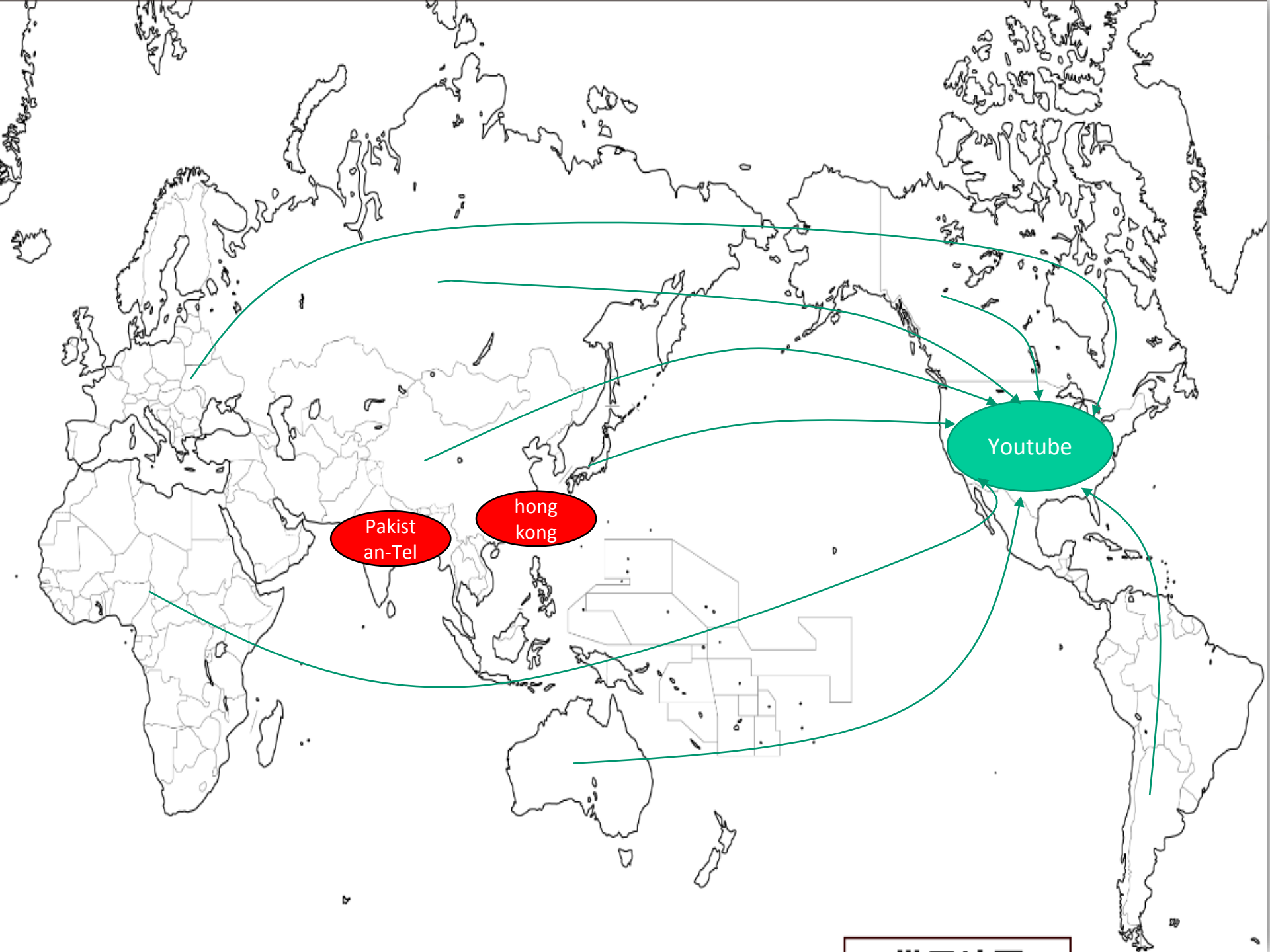


代表的名事例：Youtubeの乗っ取り

- 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



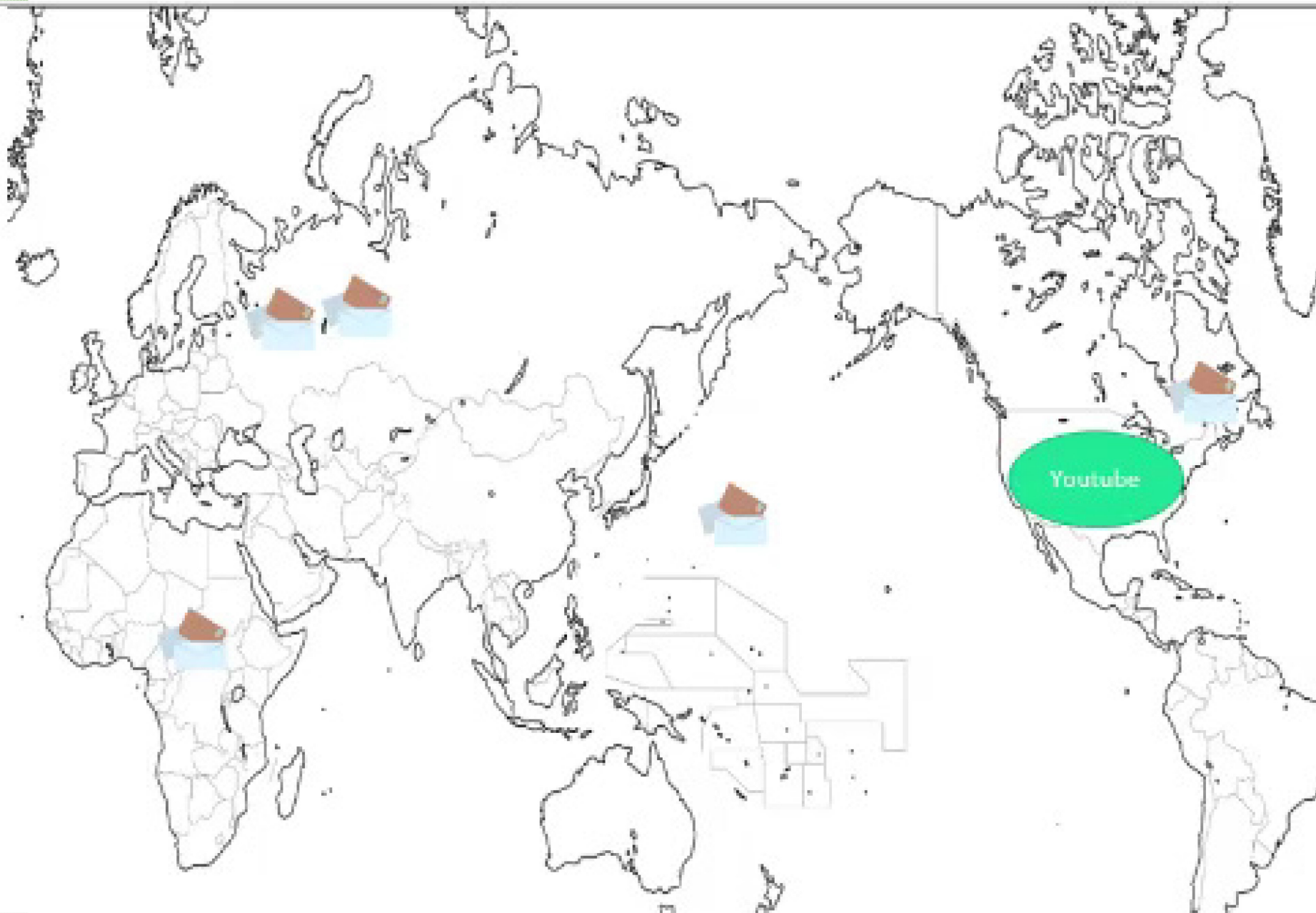
以後2時間の間、地域によってはYoutube断



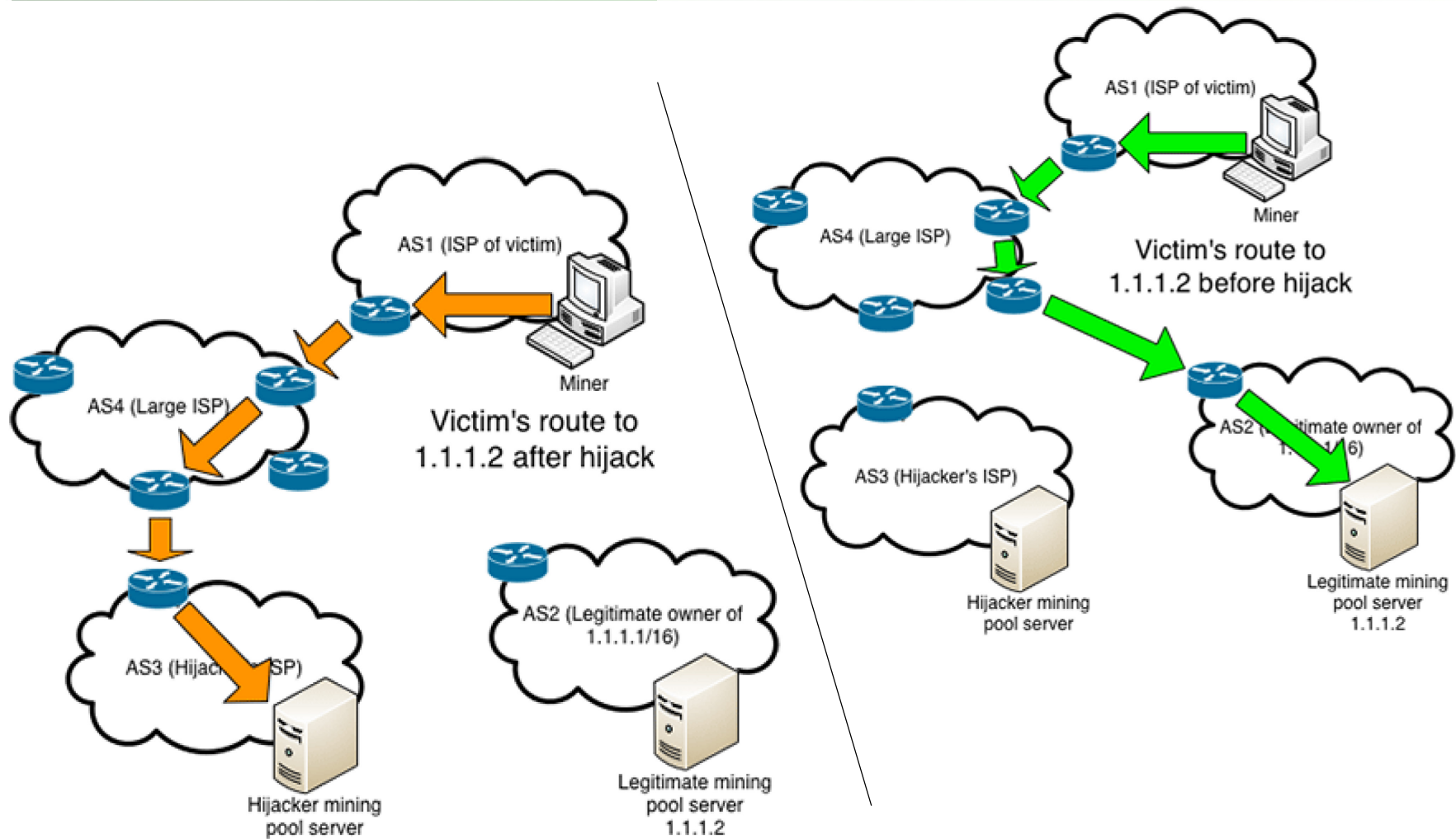
Pakist
an-Tel

hong
kong

Youtube



BitCoin発掘の乗っ取り



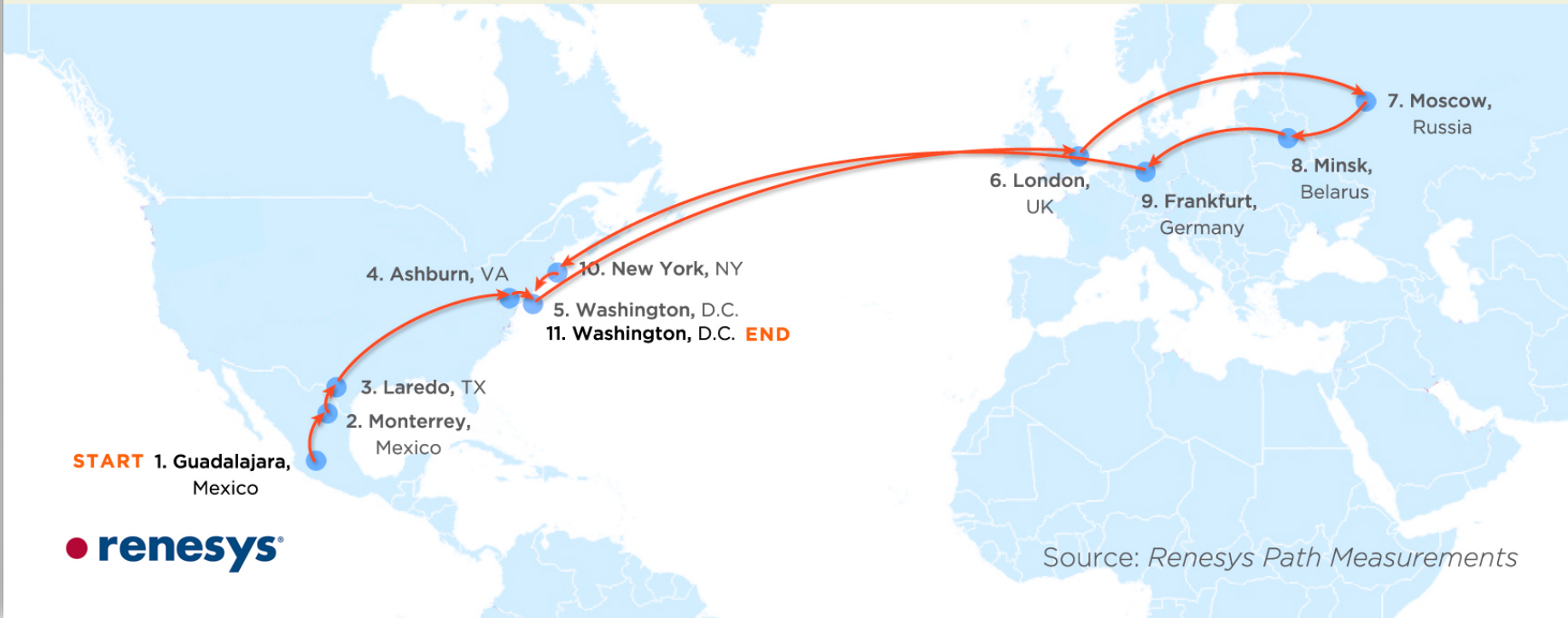
BGP Hijacking for Cryptocurrency Profit, 7 August 2014

Pat Litke and Joe Stewart, Dell SecureWorks Counter Threat Unit

<http://www.secureworks.com/cyber-threat-intelligence/threats/bgp-hijacking-for-cryptocurrency-profit/> 1

USの経路が乗っ取りによりロシア経由

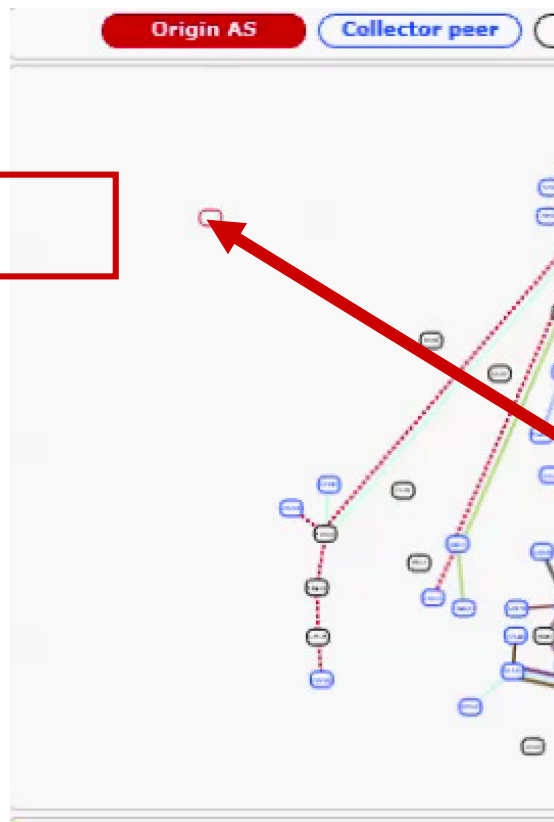
Traceroute Path 1: from Guadalajara, Mexico to Washington, D.C. via *Belarus*



- 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: Target x

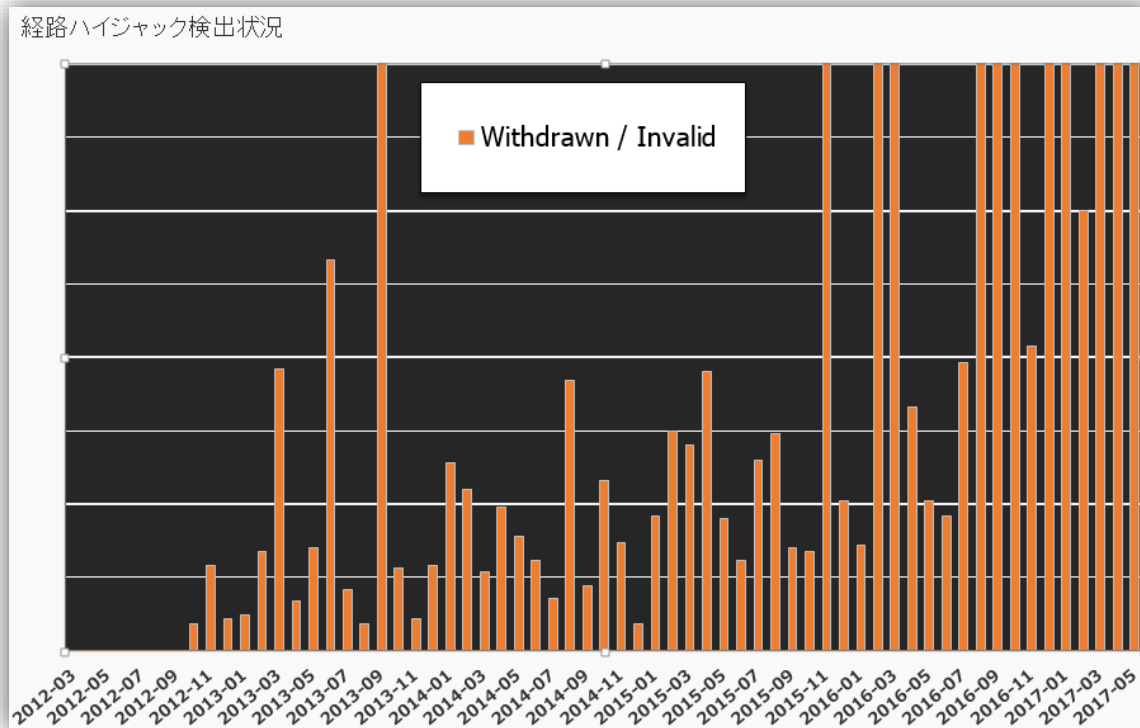
www.renesys.com/2013/11/mit

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

IP	Delay (ms)	Notes
201.151.31.149	15.482	po-gd2.alestra.net.mx (Guadalajara, MX)
201.163.102.1	17.702	po-mty2.alestra.net.mx (Monterrey, MX)
201.151.27.230	13.851	igmt2.alestra.net.mx (Monterrey, MX)
63.218.121.49	17.064	ge3-1.br02.lar01.pocwbtn.net (Laredo, TX)
63.218.44.78	64.012	TenGE11-1.br03.ash01.pocwbtn.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-transtele.com.ether.net8-4.ar9.lon3.gblx.net (London, UK)
217.150.62.234	212.869	mkn01.transtele.com.net (Moscow, RU)
217.150.62.233	228.461	BelTelecom-gw.transtele.com.net (Minsk, Belarus)
87.245.233.198	225.516	ae0-3.r1.jrx.fkt.de.ret.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

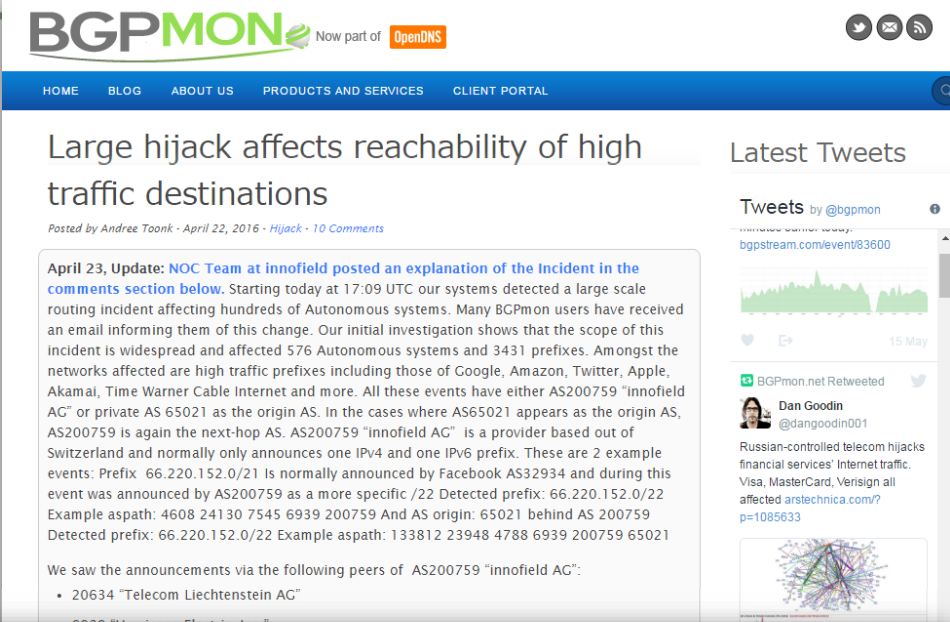
- ほとんどがルータの設定ミス
 - Typoなど"set ip address 192.16"7".0.0/24
 - Global アドレスを設定してしまっている等
 - 相互信頼のため相手は正しいと思ってしまう
- 国内の発生状況



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



BGPMON Now part of **OpenDNS**

HOME BLOG ABOUT US PRODUCTS AND SERVICES CLIENT PORTAL

Large hijack affects reachability of high traffic destinations

Posted by Andree Toonk - April 22, 2016 - Hijack - 10 Comments

April 23, Update: NOC Team at innofield posted an explanation of the incident in the comments section below. Starting today at 17:09 UTC our systems detected a large scale routing incident affecting hundreds of Autonomous systems. Many BGPmon users have received an email informing them of this change. Our initial investigation shows that the scope of this incident is widespread and affected 576 Autonomous systems and 3431 prefixes. Amongst the networks affected are high traffic prefixes including those of Google, Amazon, Twitter, Apple, Akamai, Time Warner Cable Internet and more. All these events have either AS200759 "innofield AG" or private AS 65021 as the origin AS. In the cases where AS65021 appears as the origin AS, AS200759 is again the next-hop AS. AS200759 "innofield AG" is a provider based out of Switzerland and normally only announces one IPv4 and one IPv6 prefix. These are 2 example events: Prefix: 66.220.152.0/21 Is normally announced by Facebook AS32934 and during this event was announced by AS200759 as a more specific /22 Detected prefix: 66.220.152.0/22 Example aspath: 4608 24130 7545 6939 200759 And AS origin: 65021 behind AS 200759 Detected prefix: 66.220.152.0/22 Example aspath: 133812 23948 4788 6939 200759 65021

We saw the announcements via the following peers of AS200759 "innofield AG":

- 20634 "Telecom Liechtenstein AG"
- 6939 "Hurricane Electric, Inc."

Latest Tweets

Tweets by @bgpmon

bgpstream.com/event/83600

BGPmon.net Retweeted

Dan Goodin @dangoodin001

Russian-controlled telecom hijacks financial services' Internet traffic. Visa, MasterCard, Verisign all affected arstechnica.com/?p=1085633



University of Oregon Route Views Project

[Advanced Network Technology Center](#)
University of Oregon

ANNOUNCEMENT: [route-views.chicago](#) collector up and running.
ANNOUNCEMENT: [CAIDA BGPstream Toolkit](#)
ANNOUNCEMENT: [CERT routeviews mirror](#)
ANNOUNCEMENT: [sfmix perth nwx sq](#) collectors.

MAINTENANCE: [03-17-2017 bgp large communities data format](#)
MAINTENANCE: [03-17-2017 route-views3 directory merge](#)
MAINTENANCE: [03-17-2017 archive2 rsync enabled](#)

- Introduction and Goals

RIPE Stats

- <https://stats.ripe.net/>

The screenshot displays the RIPE Stats interface for the prefix 202.12.30.0/24. On the left is a navigation sidebar with categories: At a Glance (4), Routing (9), DNS (2), Anti Abuse (2), Database (9), Geographic (2), Activity (4), and Suggestions (1). Below these is a '+ MyView' button with a help icon.

The main content area is divided into several panels:

- Prefix Overview (202.12.30.0/24):** Features a green 'Announced' badge. Text indicates the prefix is announced by AS2515, "JPNIC Japan Network Information Center, JP". A table shows the resource 202.12.30.0/24, RIR APNIC, and Country JP. A 'Show IANA Registry Information' button is present. A note at the bottom states: 'Showing results for 202.12.30.0/24 as of 2017-05-29 00:00:00 UTC'. Navigation links for source data, embed code, permalink, and info are at the bottom.
- Geoloc (202.12.30.0/24):** Includes a map of Japan with a 100.00% visibility marker. Below the map is a 'Geoloc details' section with an information icon and text: 'Data is based on MaxMind's GeoLite City data set and valid for the stated query time (see below)'. A note at the bottom says: 'Showing results for 202.12.30.0/24 as of 2017-05-02 00:00:00 UTC'. Navigation links for source data, embed code, permalink, and info are at the bottom.
- Whois Matches (202.12.30.0/24):** A table listing matches for the prefix. The first match is for JPNIC-NET-JP, Japan Network Information Center, located at Urbannet-Kanda Bldg 4F, 3-6-2, Uchi-Kanda, Chiyoda-ku.
- Routing Status (202.12.30.0/24):** A green box with a checkmark indicates: 'At 2017-05-29 00:00:00 UTC, 202.12.30.0/24 was 100% visible (by 156 of 156 RIS full peers)'. Below this, it notes: 'First ever seen announced by AS2515, on 2000-08-18 00:00:00 UTC'.

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

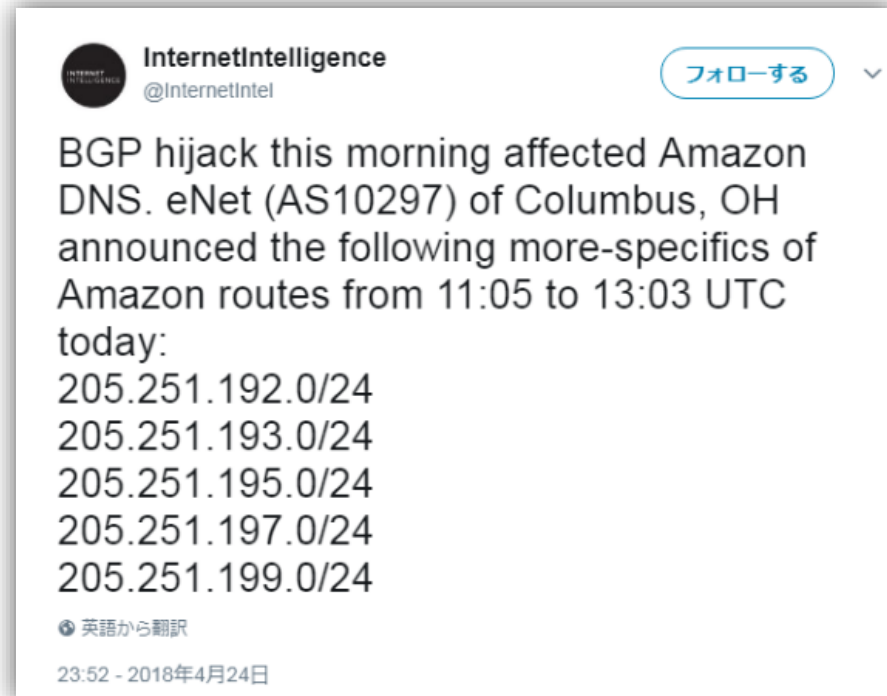
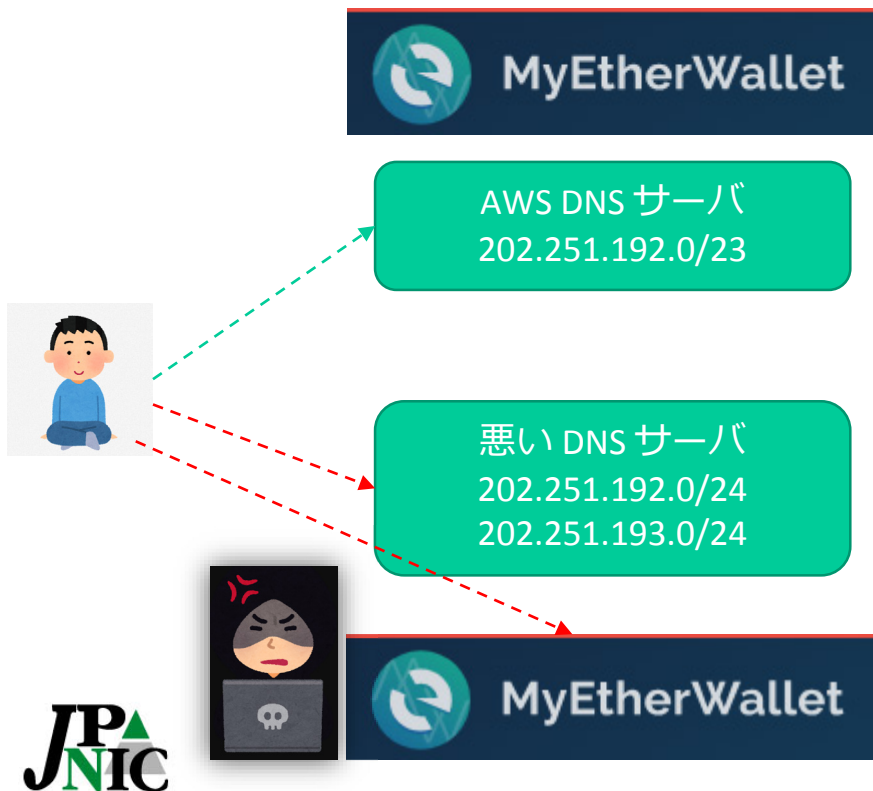
4. ルーティングトラブル 最新事例

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**

最近の事例：DNSをのっとり誘導

- 4/24 20:05~22:03(JST)
 - AWSのRoute53のIPアドレスが乗っ取られる
 - 偽者のDNSサーバが偽の応答を返す
 - 結果としてMyEtherWalletで仮想通貨を詐取



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！