ルーティングセキュリティってなに？

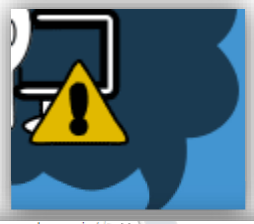
InternetWeekショーケース in 仙台

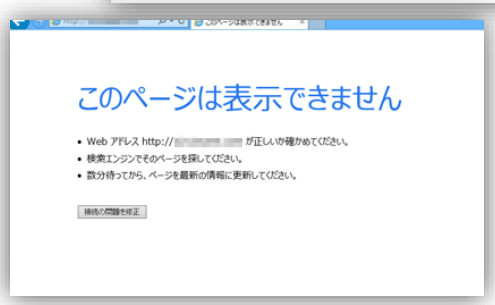
2019年5月30日

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？？



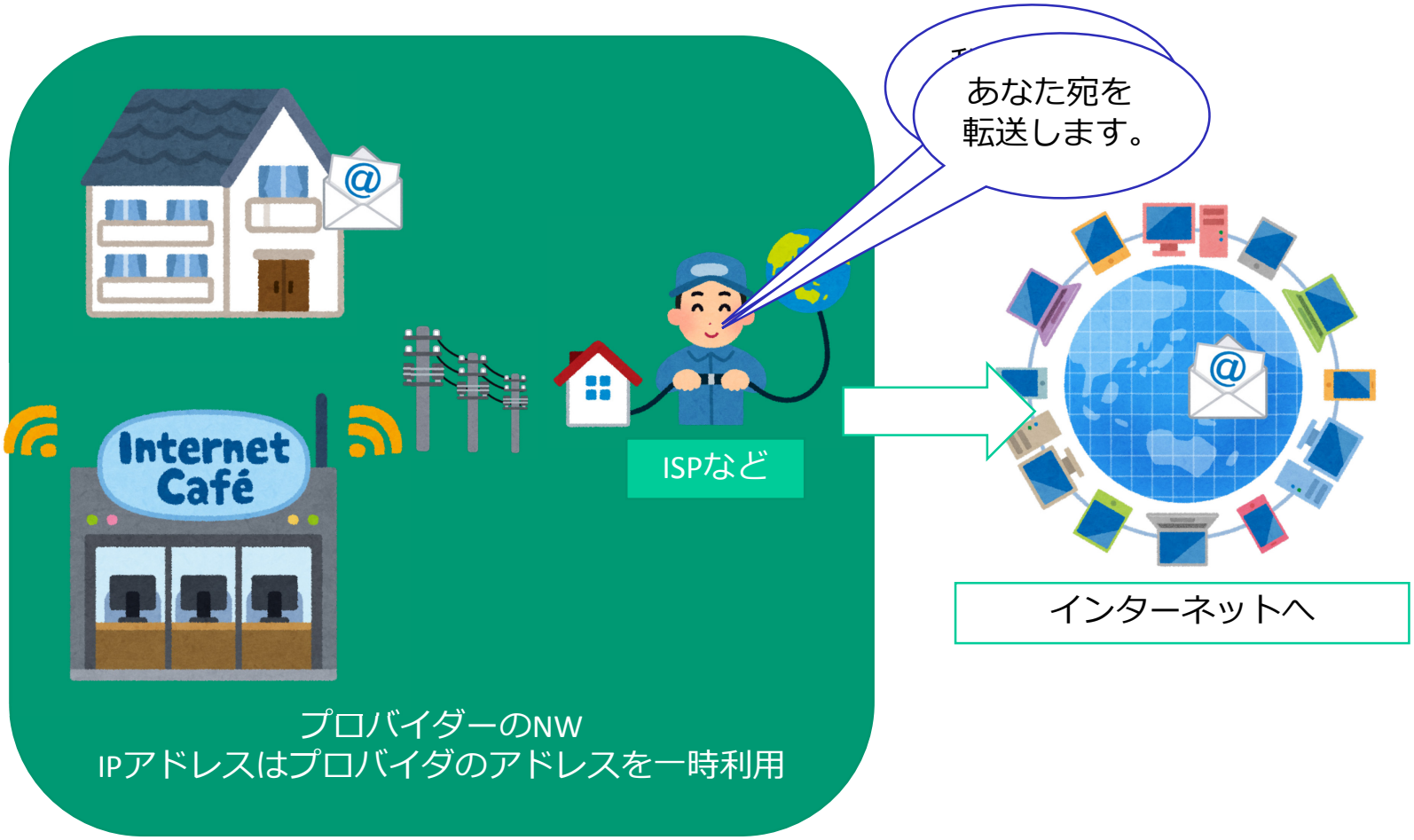


- **本セッションでは**
  - パケットの宛先制御(ルーティング)のトラブル、主に、”経路の乗っ取り”について深堀

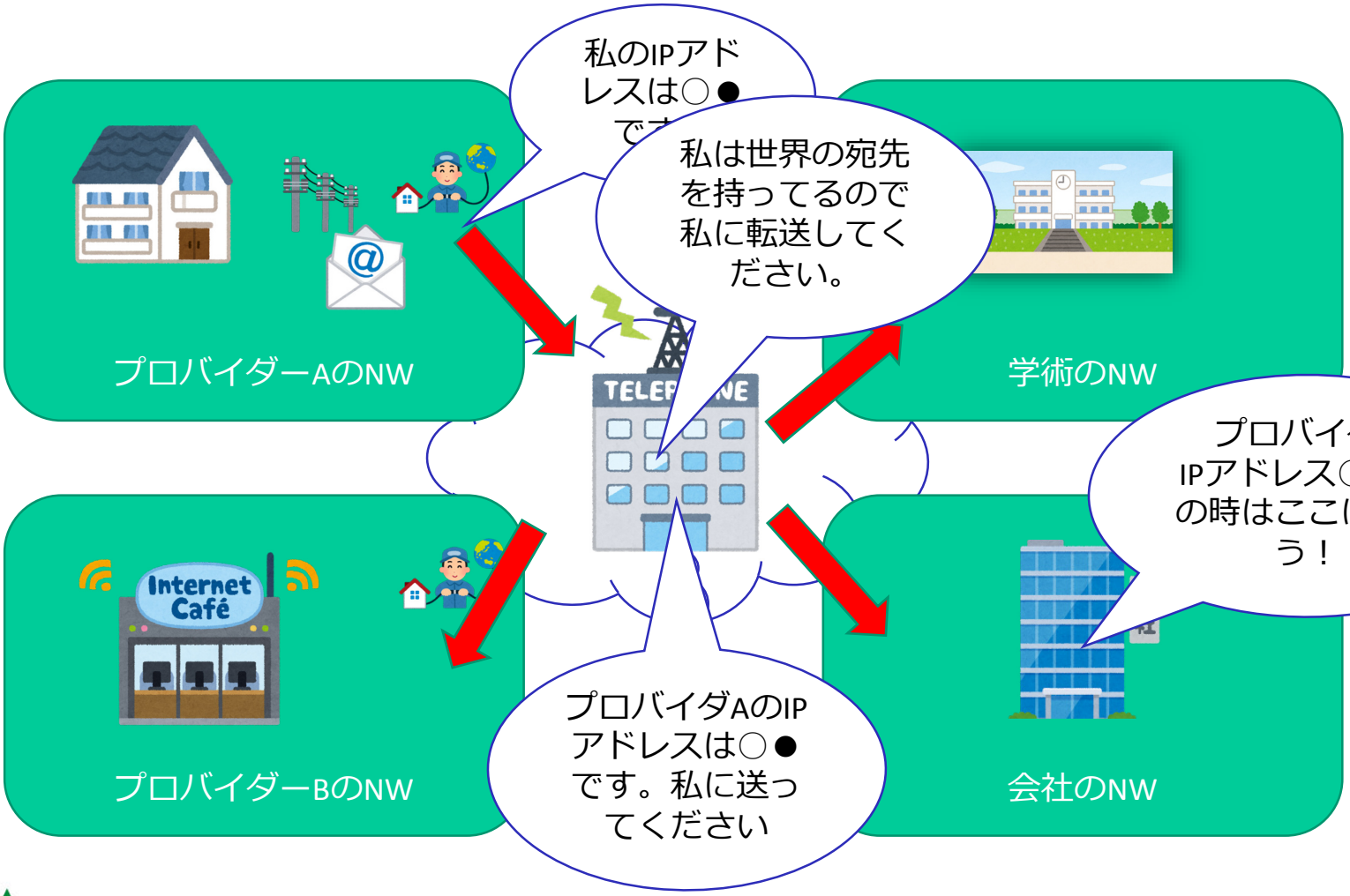
１．ルーティング=宛先制御と相互信頼

ルーティングの世界：家庭～ISP

- 家庭～ISPのネットワーク

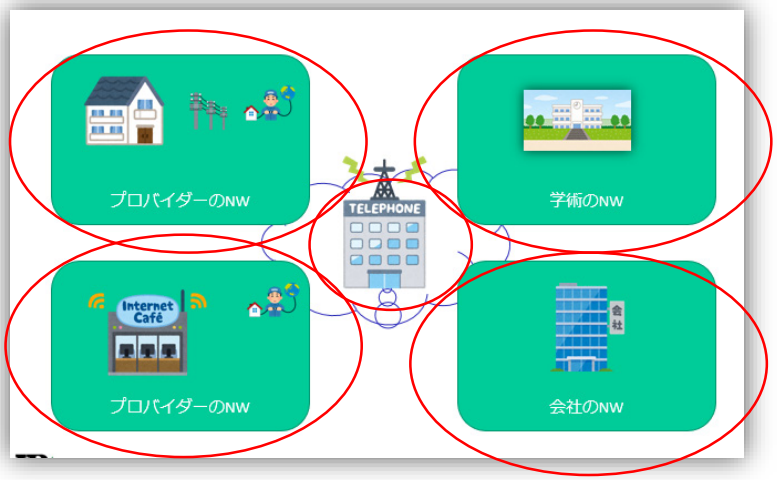


ルーティングの世界：ネットワーク同士



ルーティングの世界：ISP~BGP

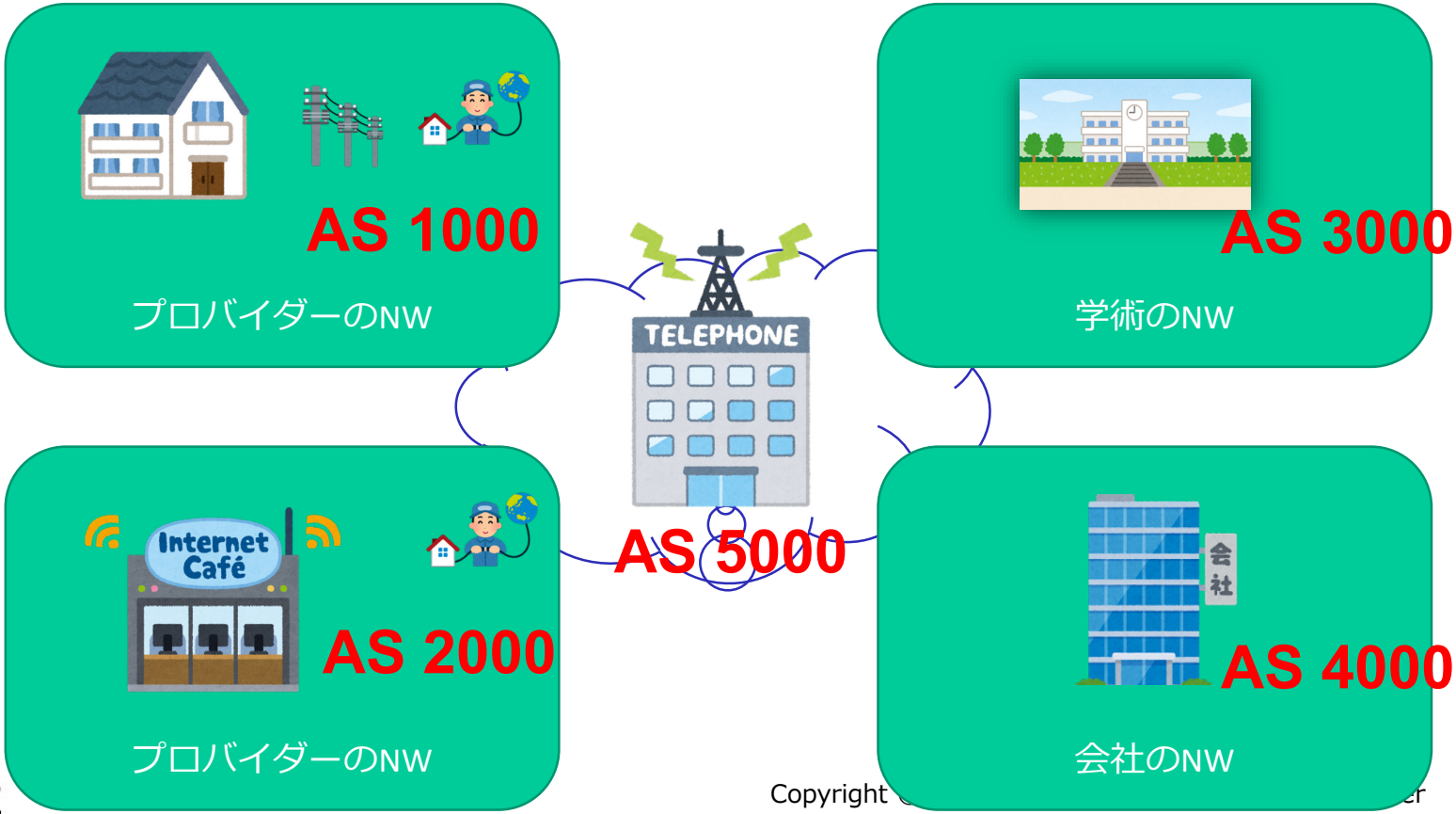
- **組織毎内部ルーティングからインターネットへ**



- **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/サブネットマスク（やり取りする主な情報）
- **上記三つをセットでやりとり**

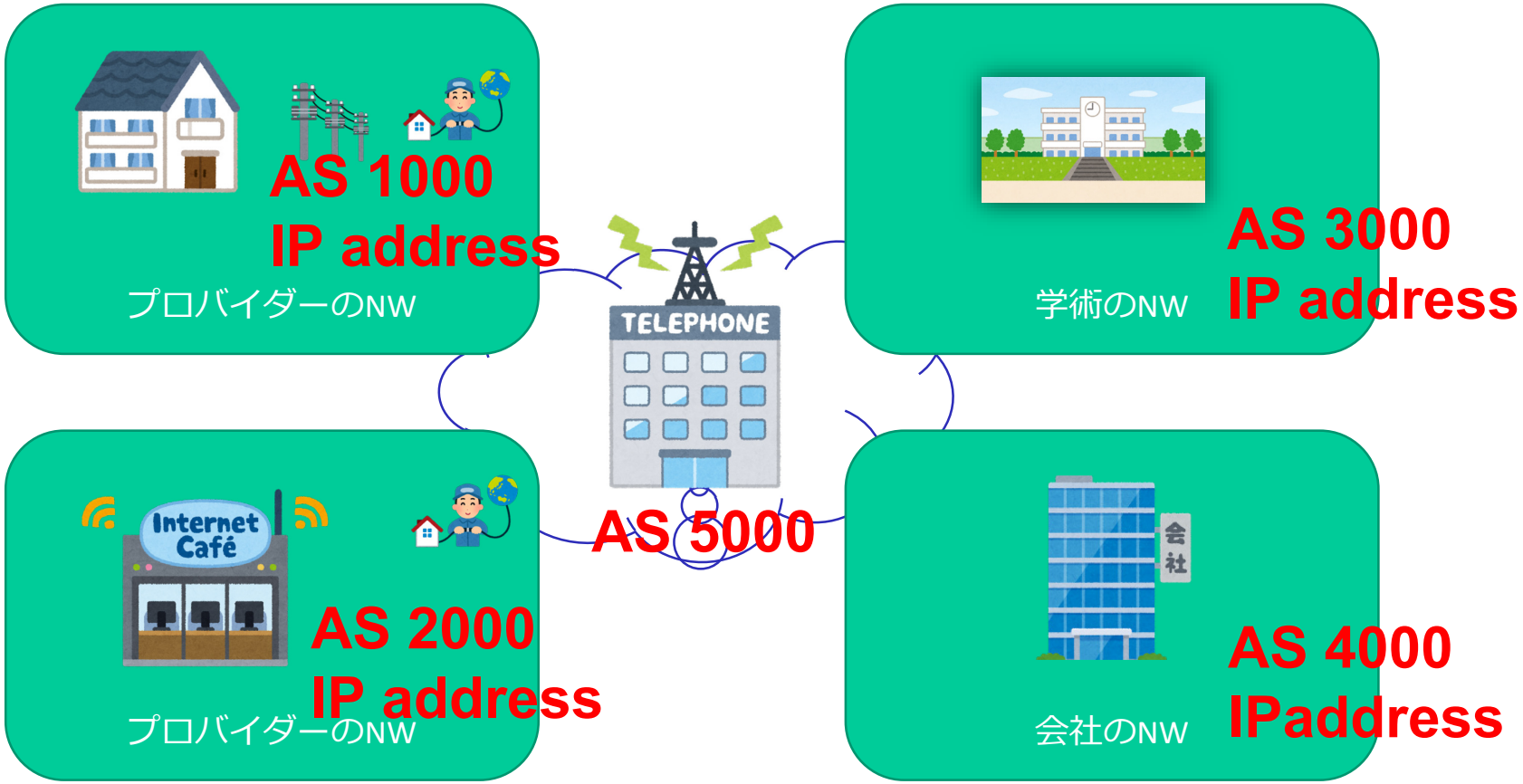
ルーティングの世界：AS番号

- **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



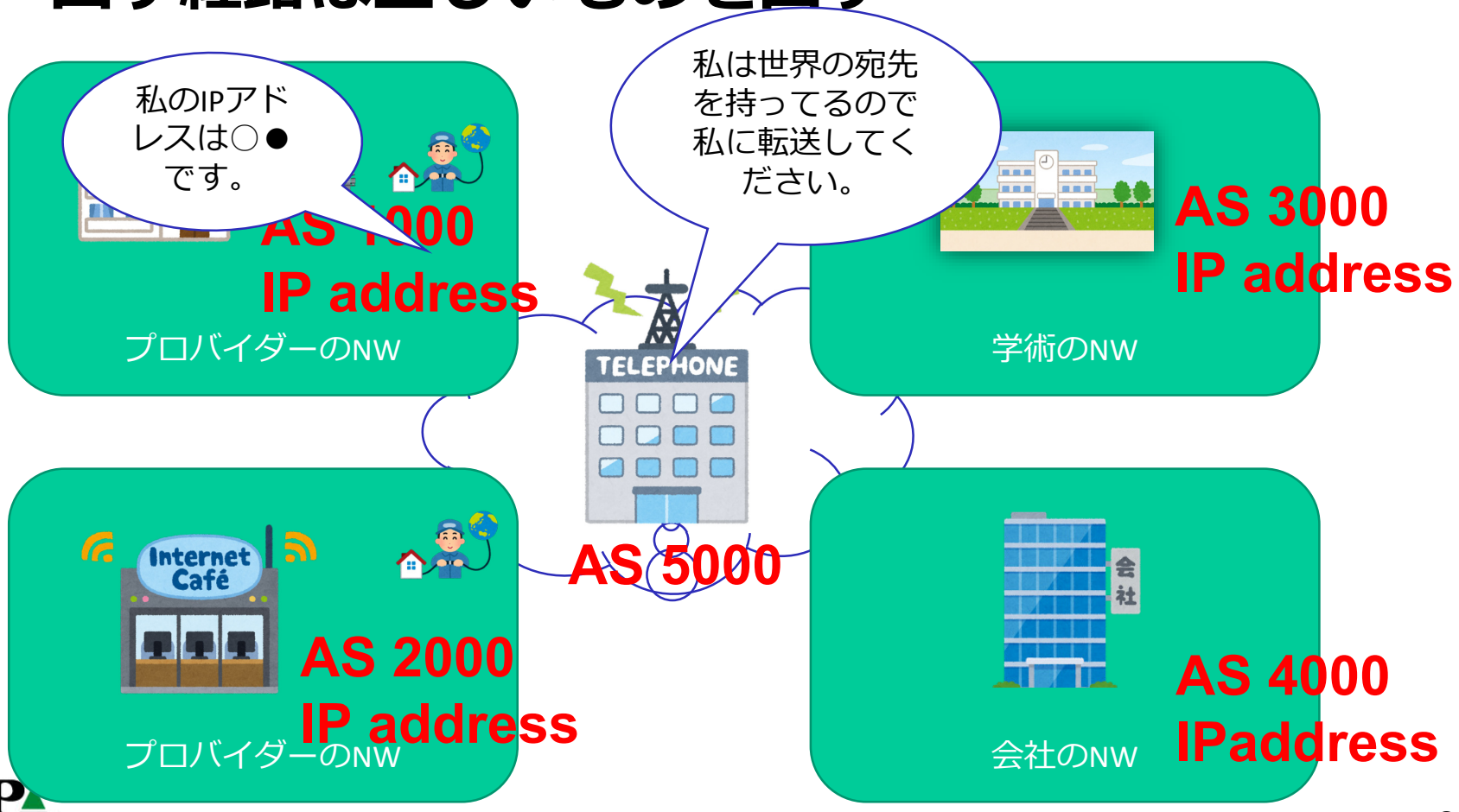
ルーティングの世界：BGP運用

- AS間のルーティング＝経路情報の交換



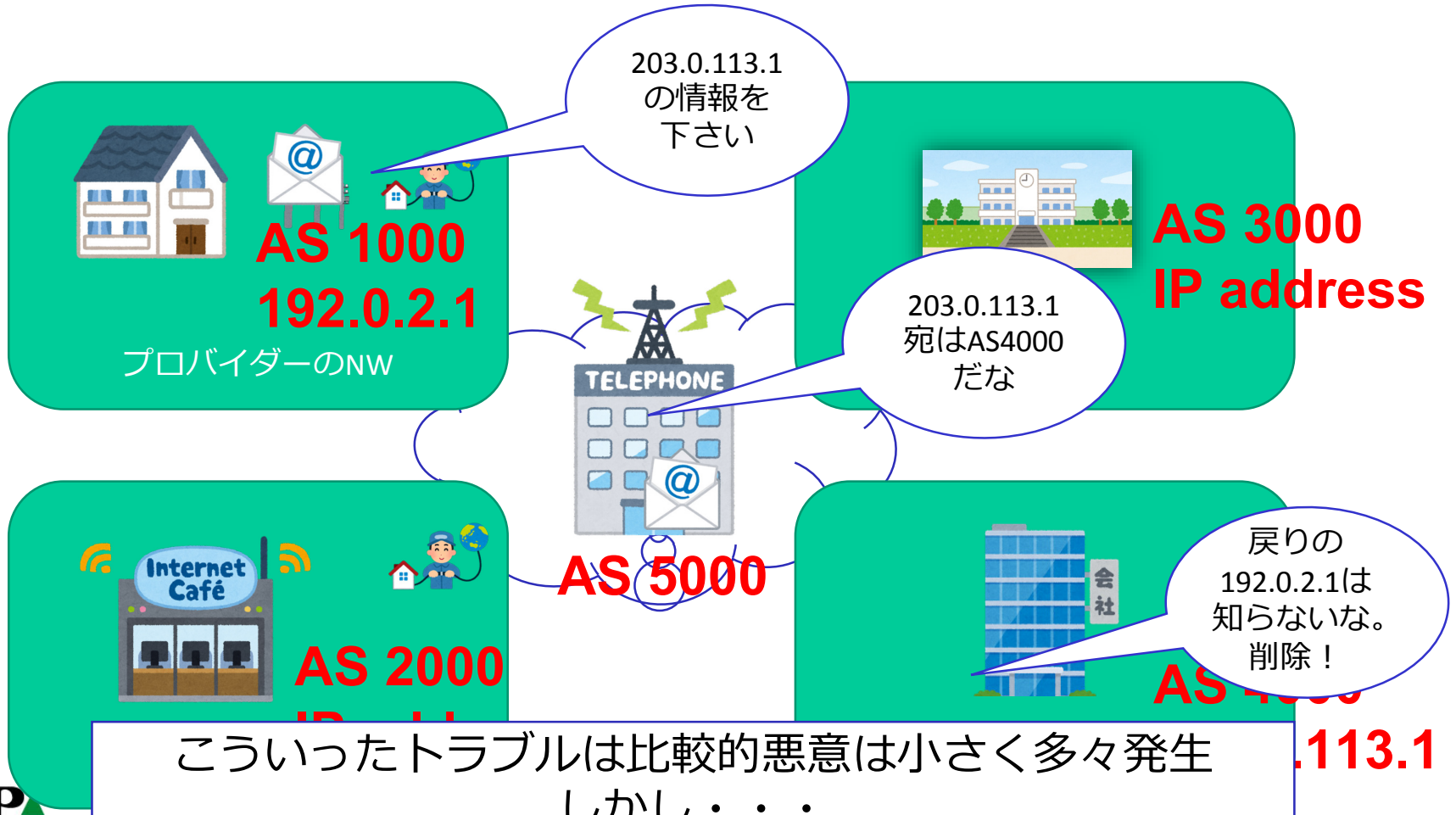
ルーティングの世界：相互信頼の実際

- 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

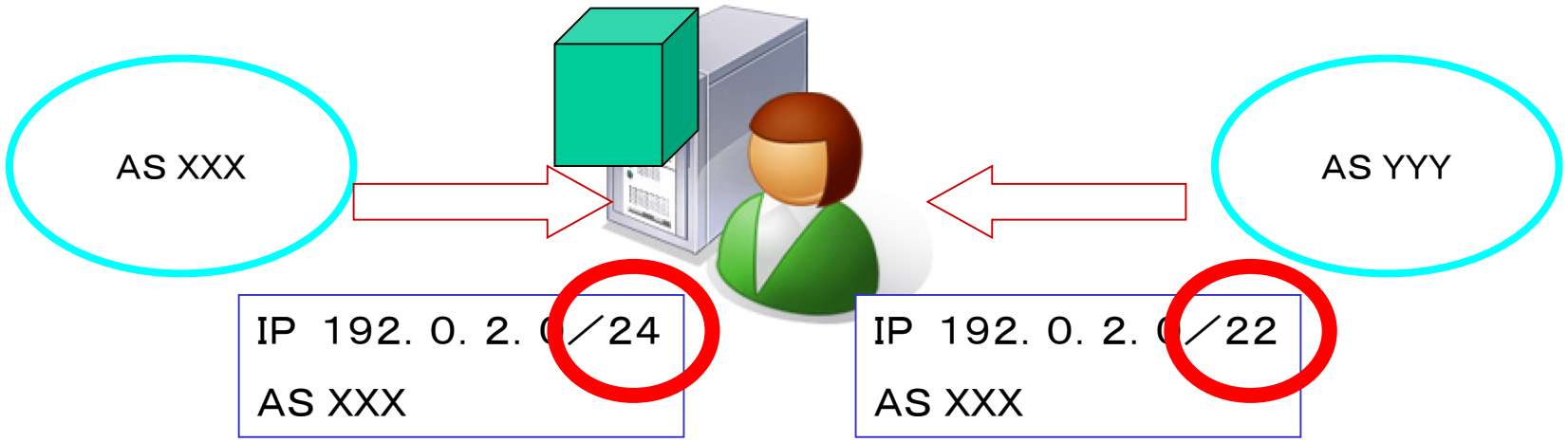
ルーティングの問題

- **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

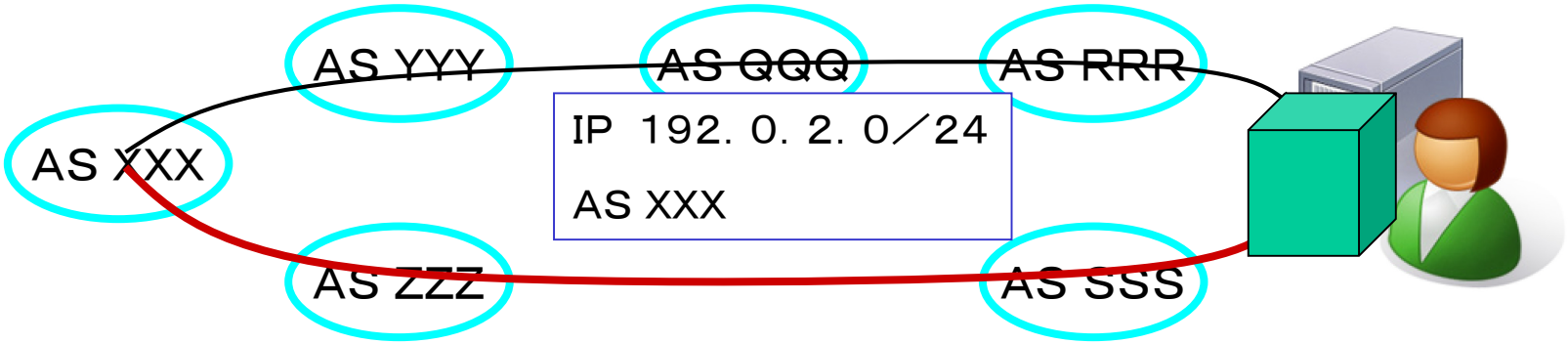
- 受け取った経路情報のうちサブネットマスク長がもっとも長い経路が優先される



この場合、マスク長が長いASXXXがあて先となります

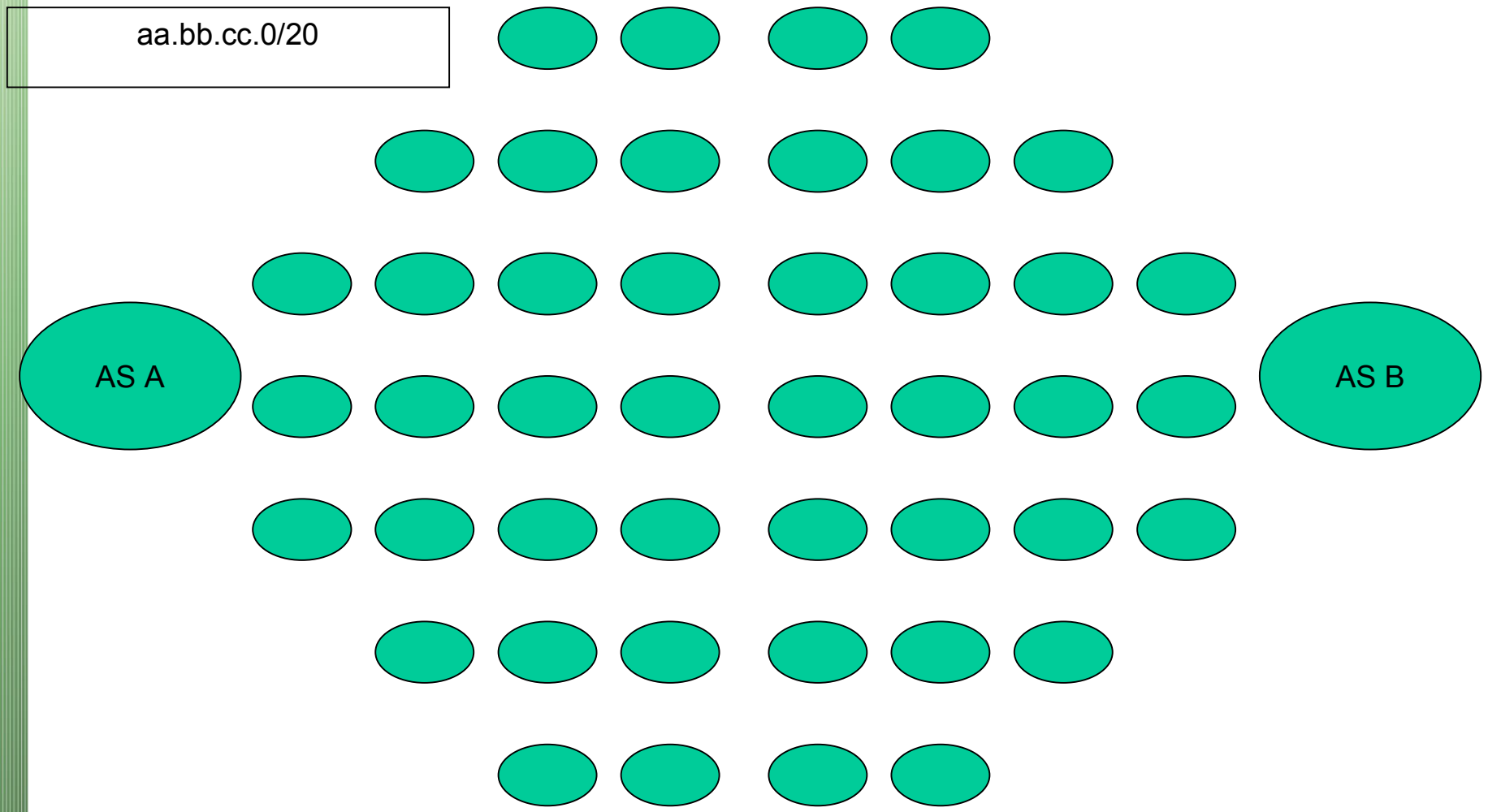
BGPの経路選択順番の基本２

- 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

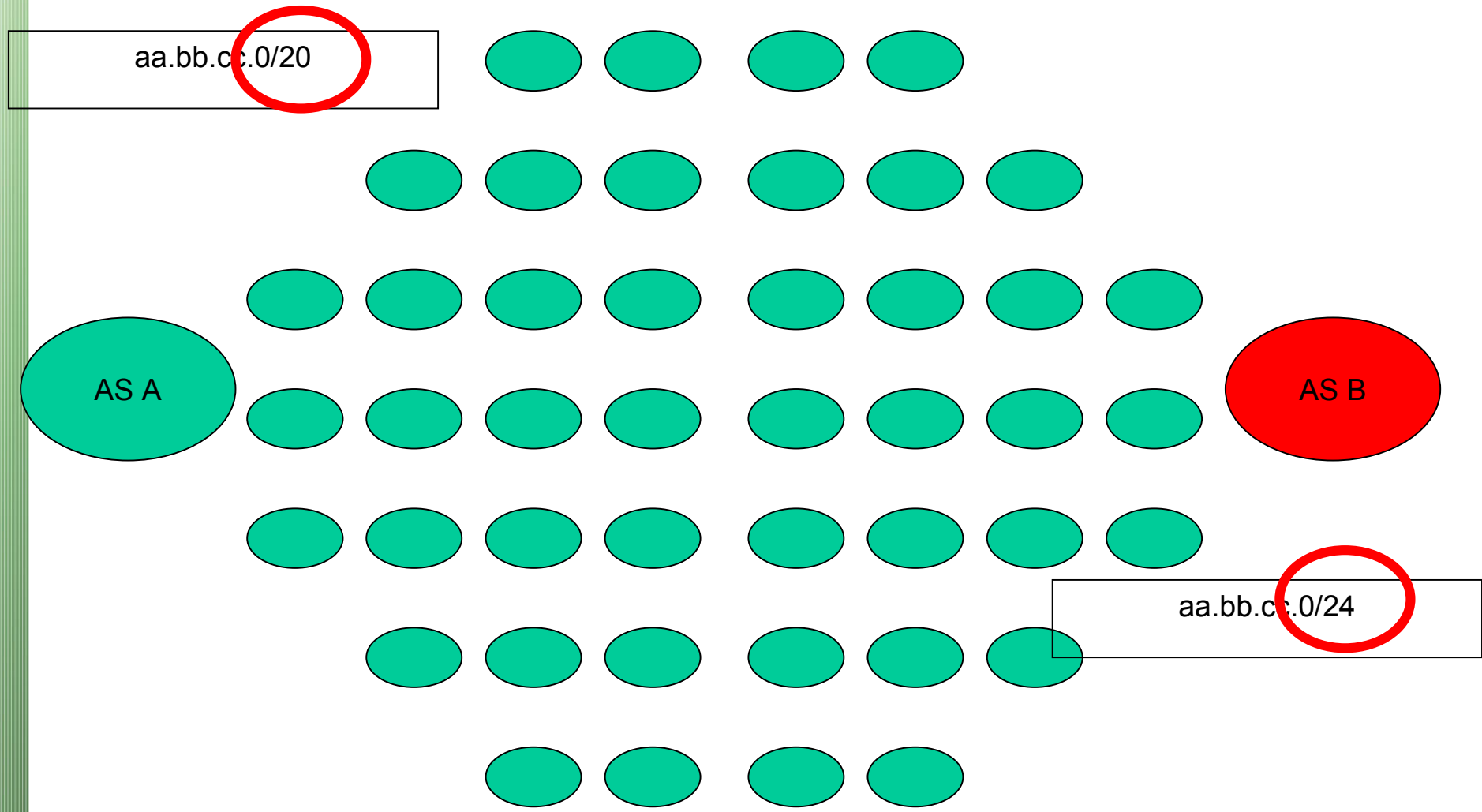


この場合、経由AS(＝ASPATH)の少ない経路が選択されます。

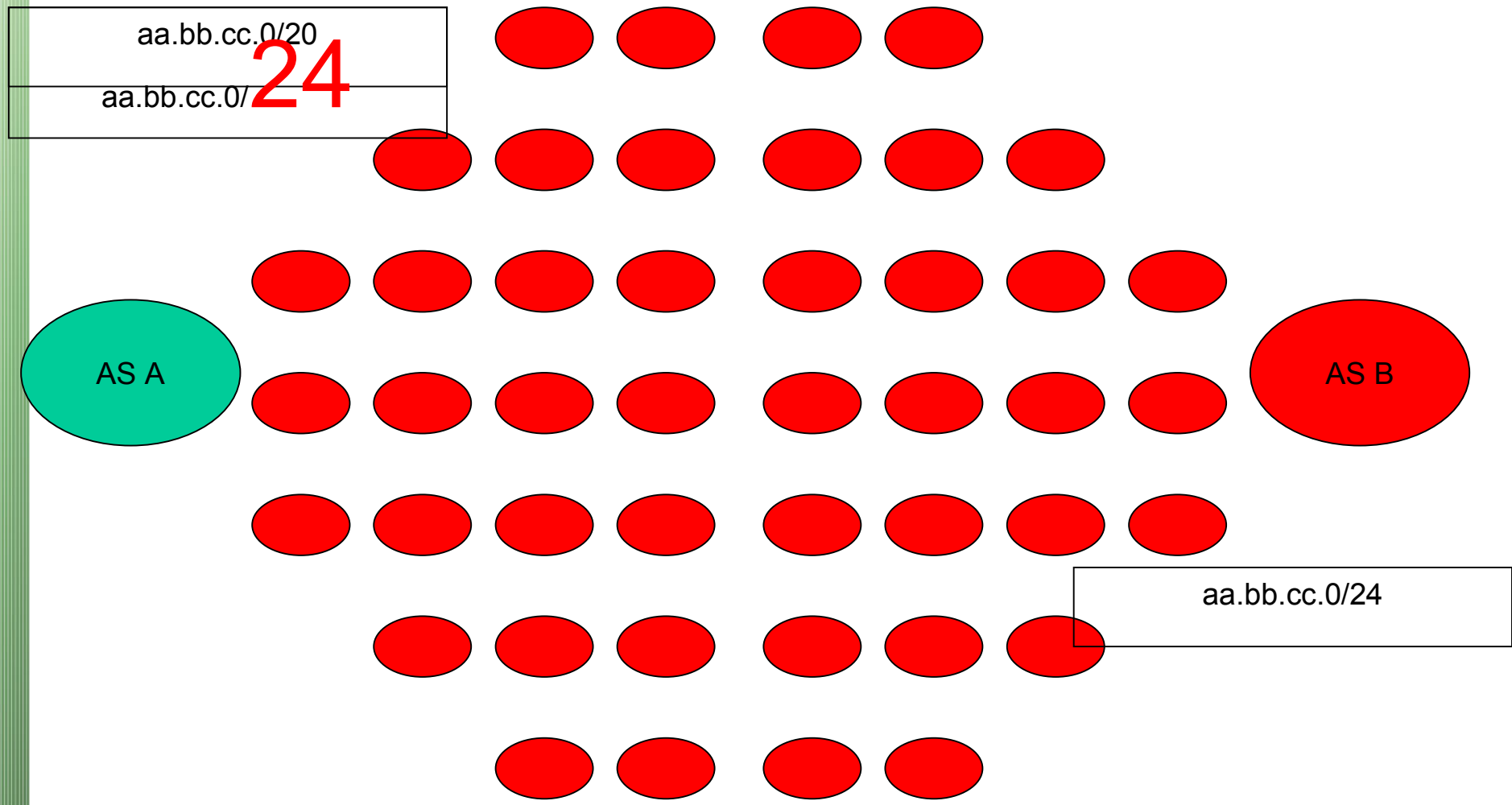
乗っ取られていない無い状態



乗っ取り発生発生

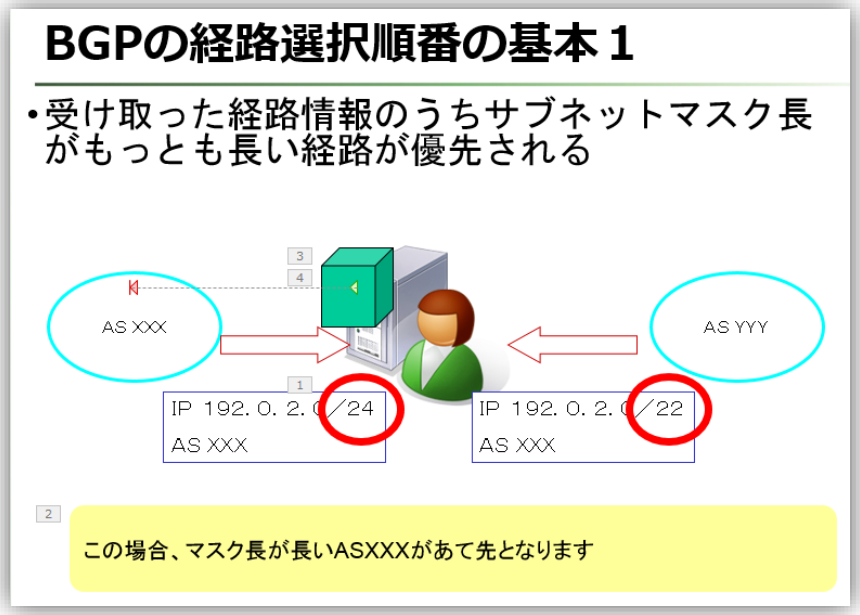


経由したASの距離 勝負

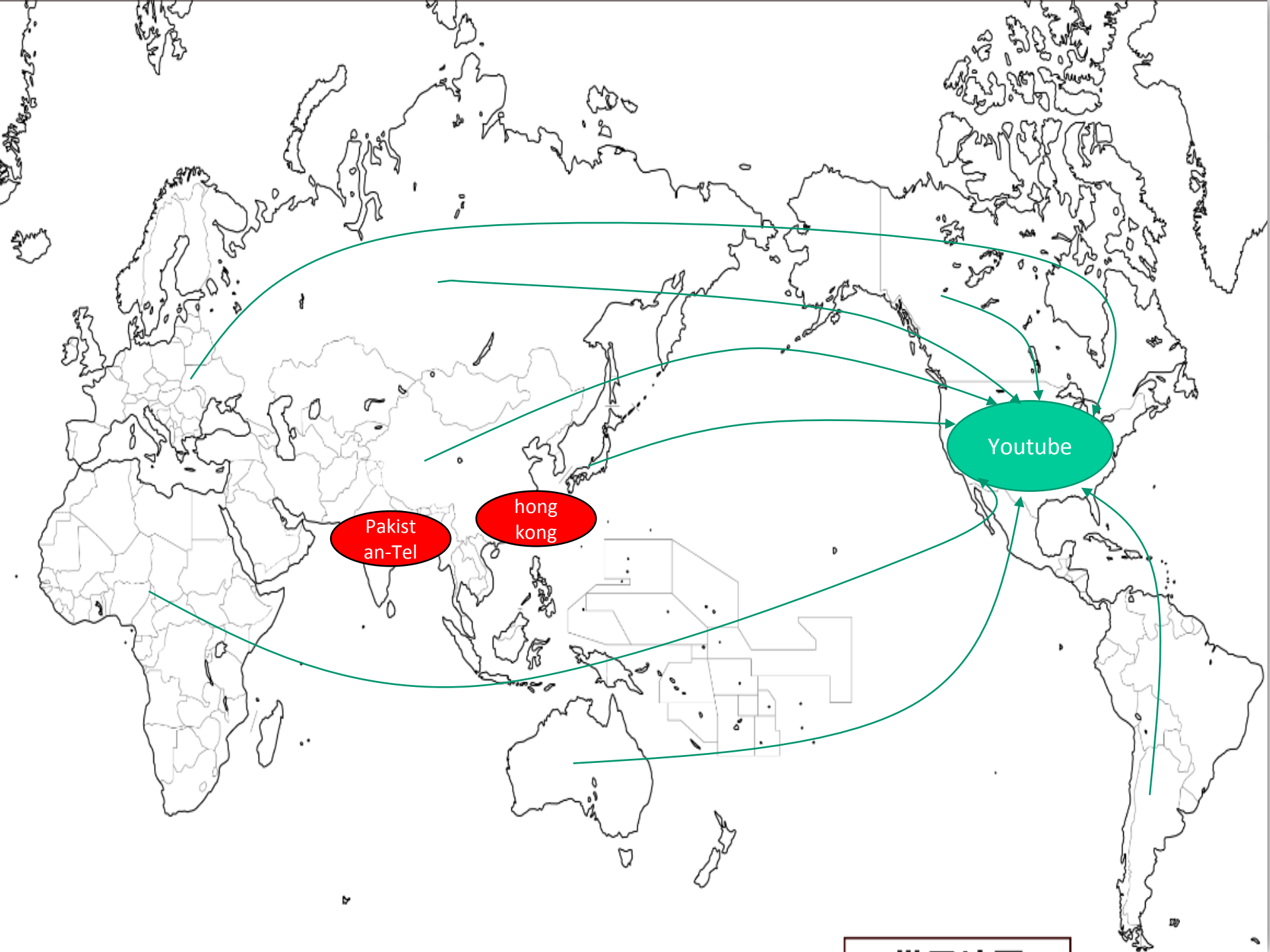


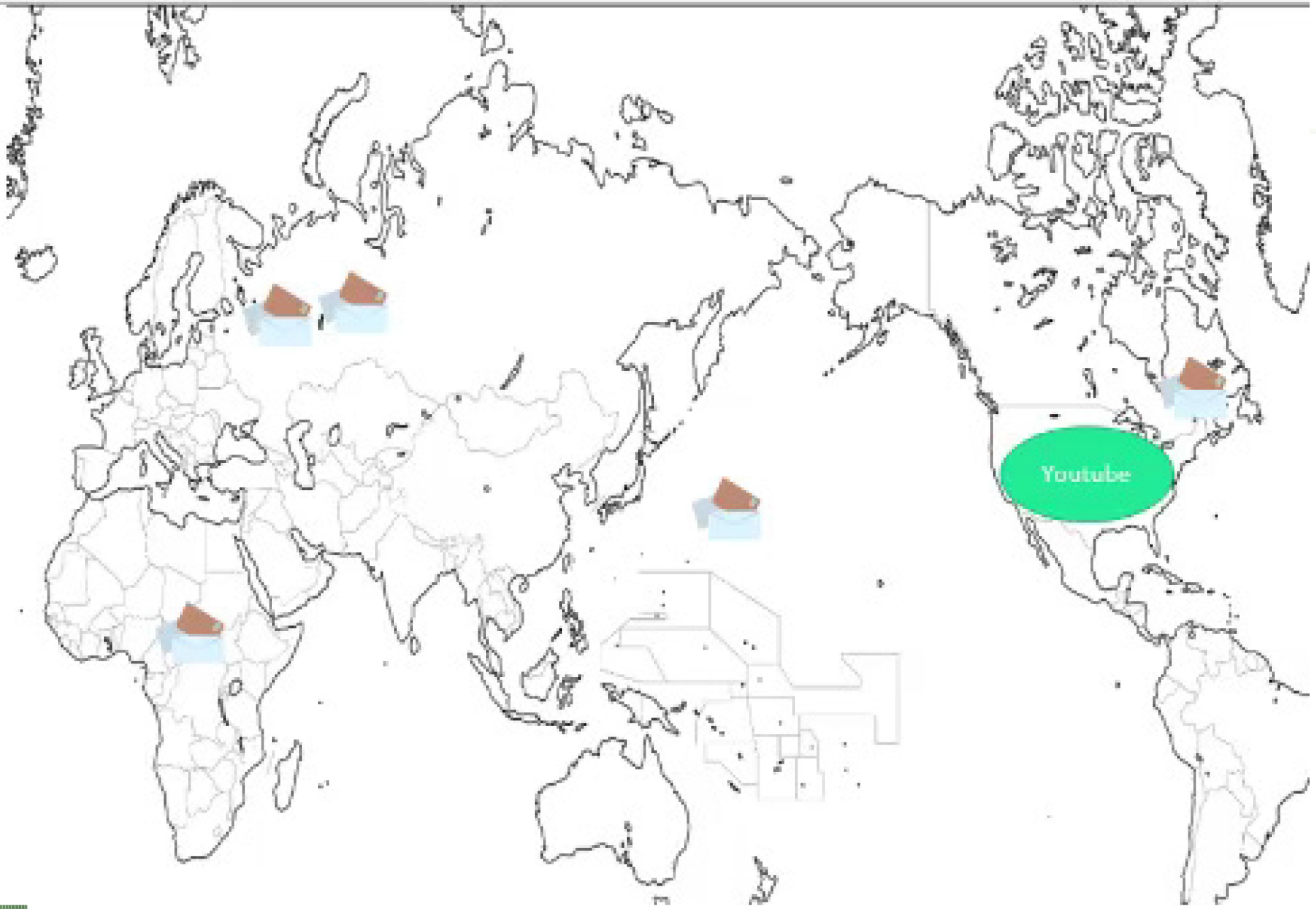
代表的名事例：Youtubeの乗っ取り

- **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

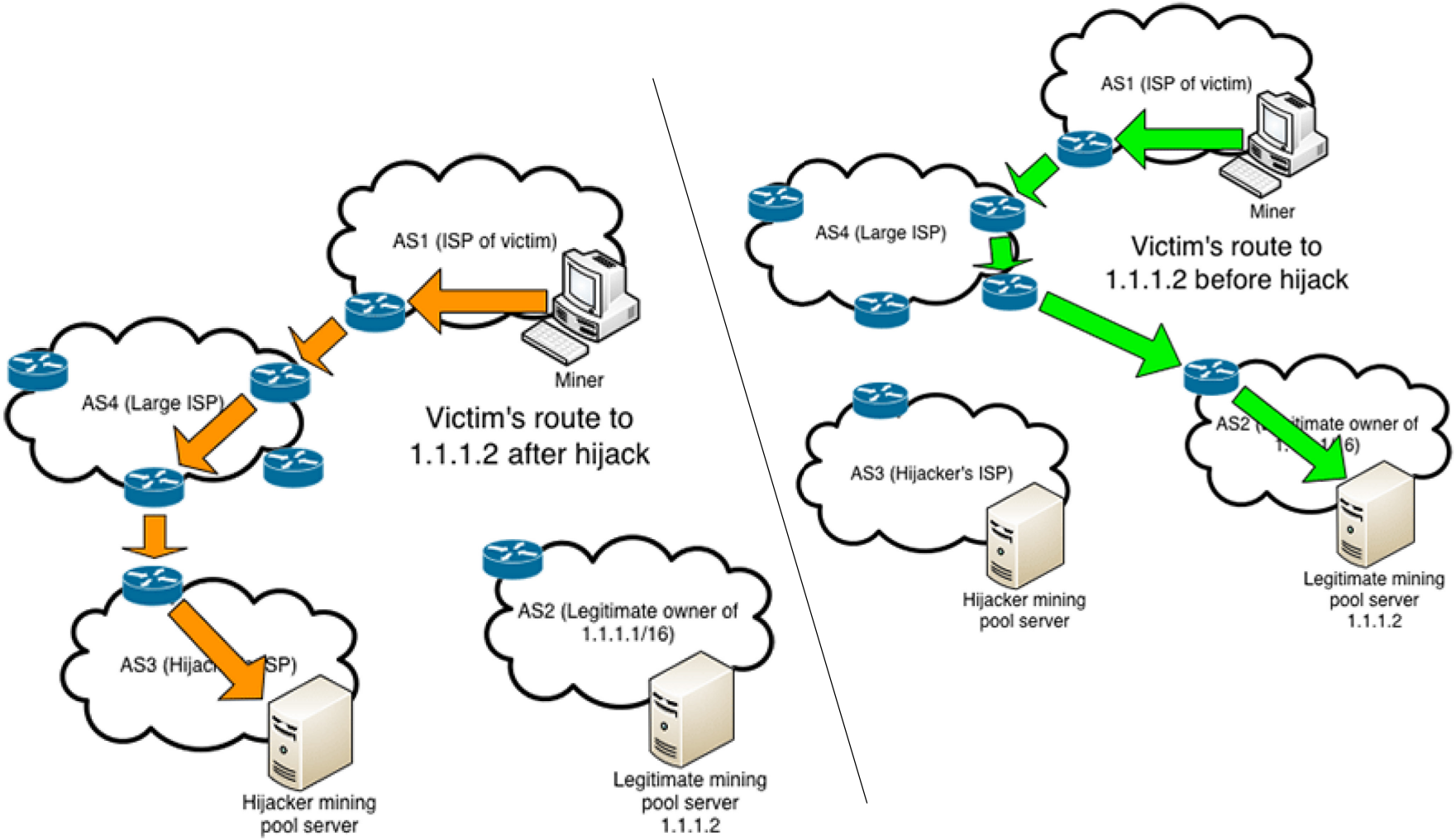


以後2時間の間,地域によってはYoutube断


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/

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！