

その時何が起きたか

Internet Week 2018 S1ネットワーク運用チュートリアル～
分かった楽しいインターネットのお仕事～～

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
技術部 岡田 雅之

自己紹介

- **理学部情報科学科卒業**
- **2000年理学研究科情報科学専攻前期博士課程修了**
- (2012年筑波大学大学院博士後期課程修了)
 - 大学院在学中よりネットワーク運用に関係
 - インターネットの運用にハマる
- **2003年日本ネットワークインフォメーションセンター**
 - IPアドレス重複利用検出の研究とシステムの実運用
 - IPアドレス配り続けて15年
- **2014年東邦大学理学部情報科学科 訪問研究員**
- **その後、非常勤講師、JANOG運営委員など**

JPNICはインターネットの円滑な運営を支えるための組織です



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

インターネット運用と"そのとき"

• ≡つながらない

○ 内部要因

- 設定変更にともなうもの
- ユーザ挙動に伴うもの
- 利用する設備等の意図しない動作

○ 外部要因

- 上流・接続ISPの誤動作によるもの
- DDoS攻撃
- 基盤システムの意図しない動作
 - 経路制御上の誤動作
 - DNSなど名前解決の問題
 - 何らかの意図をもった基盤システムの操作

自律・分散・協調

IPアドレスは配るが
誰も中央統制しない

参考 IPアドレス

0番 ~

42億9496万7296

地球上でユニーク

0. 0. 0.

0~255.255.255.255

単純な例:コピペ技術者の影響

1.2.3.4

1.1.1.1

172.15.0.0

192.167.0.0

インターネット つながらない IPアドレス

すべて

動画

画像

ショッピング

ニュース

もっと見る

設定

ツール

約 121,000 件 (0.34 秒)

[PDF] DNSを「きちんと」設定しよう

<https://www.nic.ad.jp/ja/materials/iw/2002/main/dns/PM3-minda.pdf>

DNSを「きちんと」設定しよう. 4. DNSの復習. DNS(Domain Name System)は、. サーバーとクライアントから成り立つ。ネーム ... ns.example.jp. A 1.2.3.4. dig @<nameserver> www.example.gr.jp. ; AUTHORITY SECTION: www.example.gr.jp.

DNSの仕組み | Yakst

<https://yakst.com/ja/posts/4063>

DNSの仕組みと一般的な使い方について、DNSに関する作業をする時によく使うコマンドや、具体的な例を交えてまとめた入門的記事。... どうってことはありません。あなた(あるいはあなたの使っているWebブラウザ)がキー(www.example.com)に対する値を尋ねれば、1.2.3.4 が返ってくるというわけです。... DNSはIPをホスト名、この場合 f.root-servers.net にマップする PTRレコードを返します。元のクエリーに戻って、フルート...

DNSレコード(ホストレコード)の登録方法[利用マニュアル]- ドメイン取得

...

www.quedomain.com > 利用マニュアル > その他・FAQ

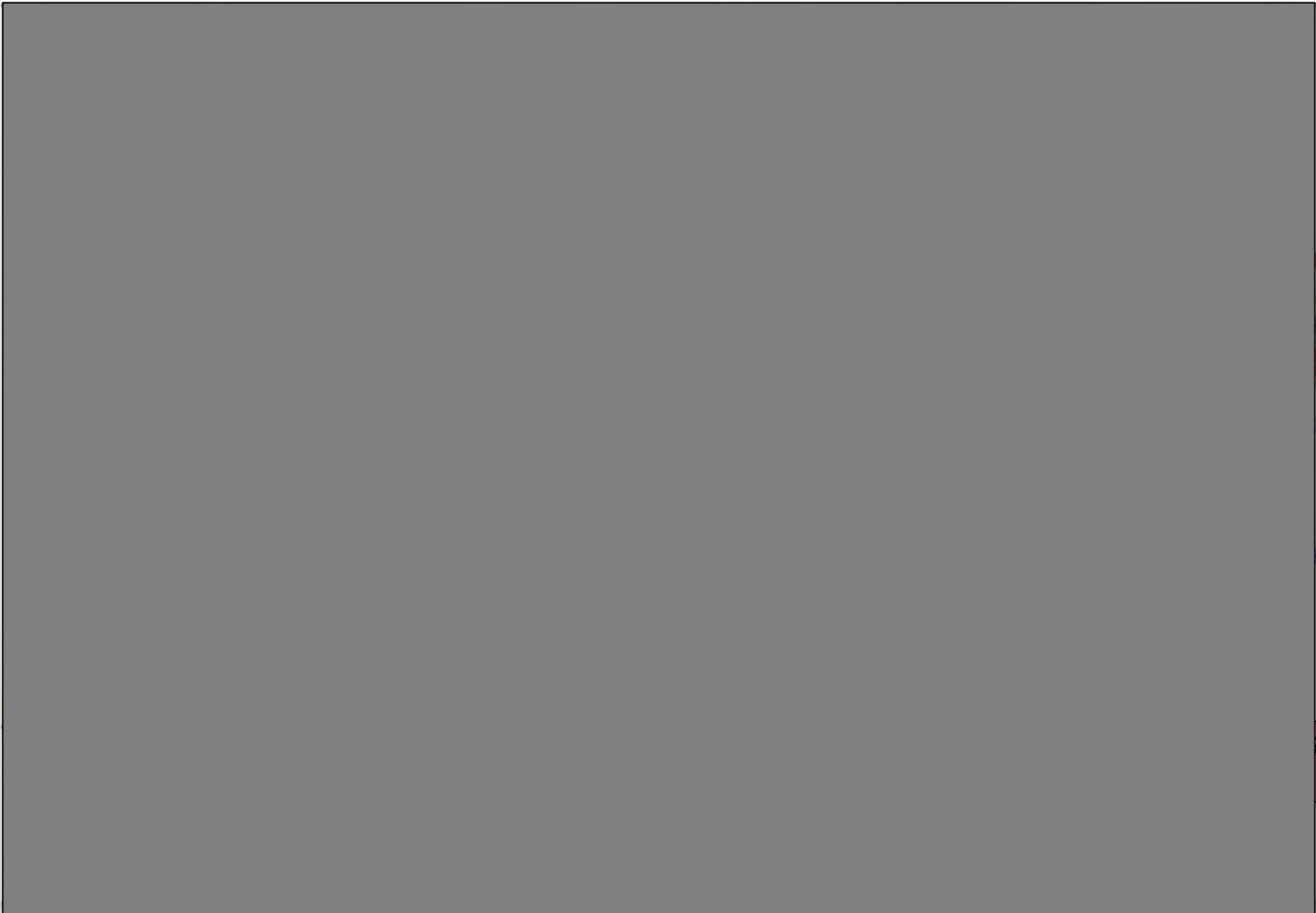
クイックでは、A、CNAME、TXT、MXの各種DNS(ホスト)レコードが登録可能です。各種レコードの解説を以下に... を結びつけるレコードです。例えば、example.comというドメインをお持ちで、IPアドレスが1.2.3.4 だった場合、以下のような書式で記述をします。

経路の乗っ取り、その時、なぜ？

IPアドレス重複利用(Youtube事件)



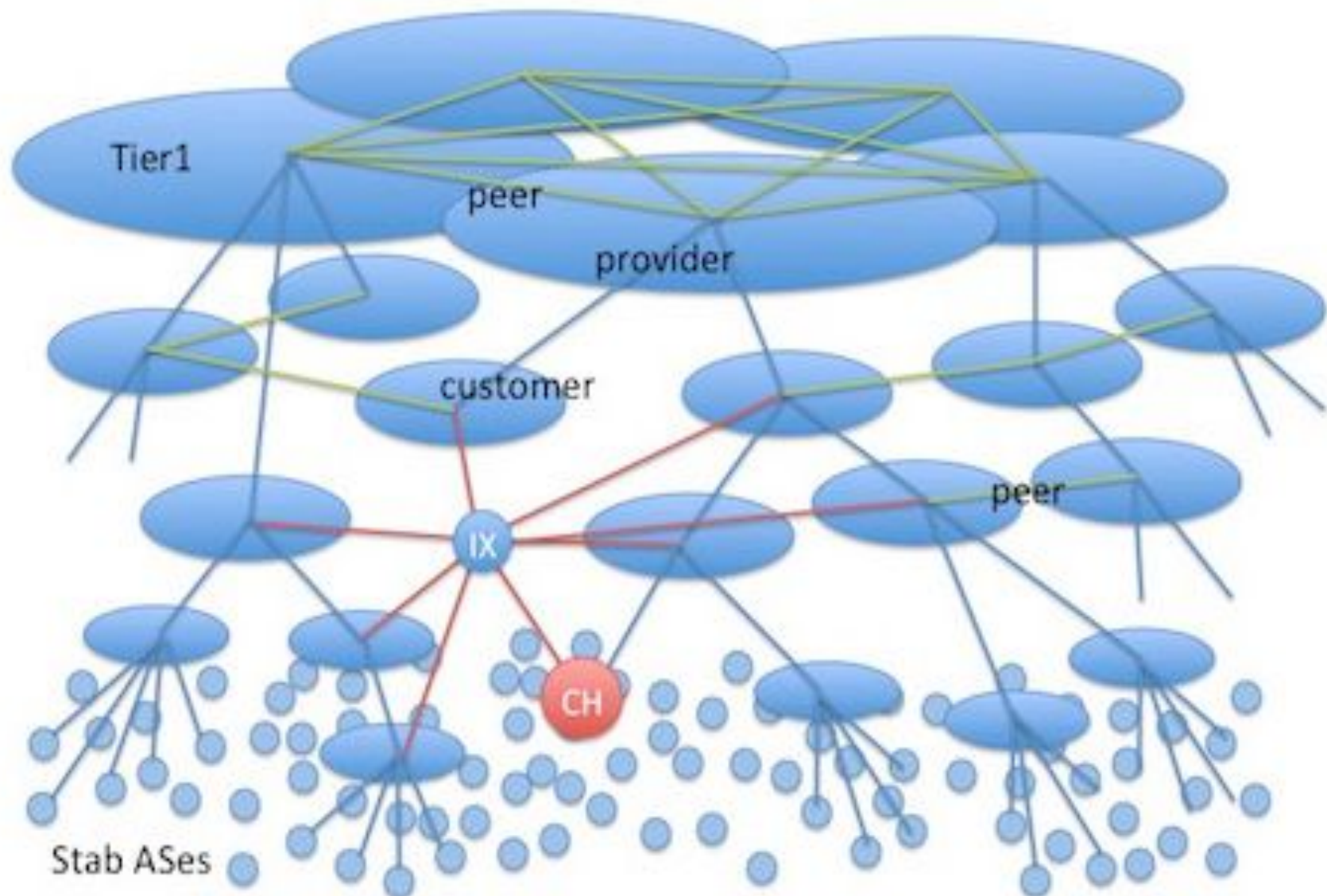
2008年2月24日



30

7474





AS: Autonomous System IX: Internet Exchange CH: Contents Holder

インターネットを止める＝破壊

- **動機**

- 言論統制や何らかのサイトの停止

- **手段**

- ぐぬぬぬぬ
 - やり方1
 - 国内だけ止めたいサイトのIPアドレスを乗っ取ってしまえ
 - やり方2
 - 結果:ドメイン名とIPアドレスの変換システムをとめてしまえ!

- **結果**

- やり方1:間違えて全世界でのっとり
- やり方2:人間はおもったよりがんばって回避する

- **回避**

- 後述

インターネットを博子うとする人達



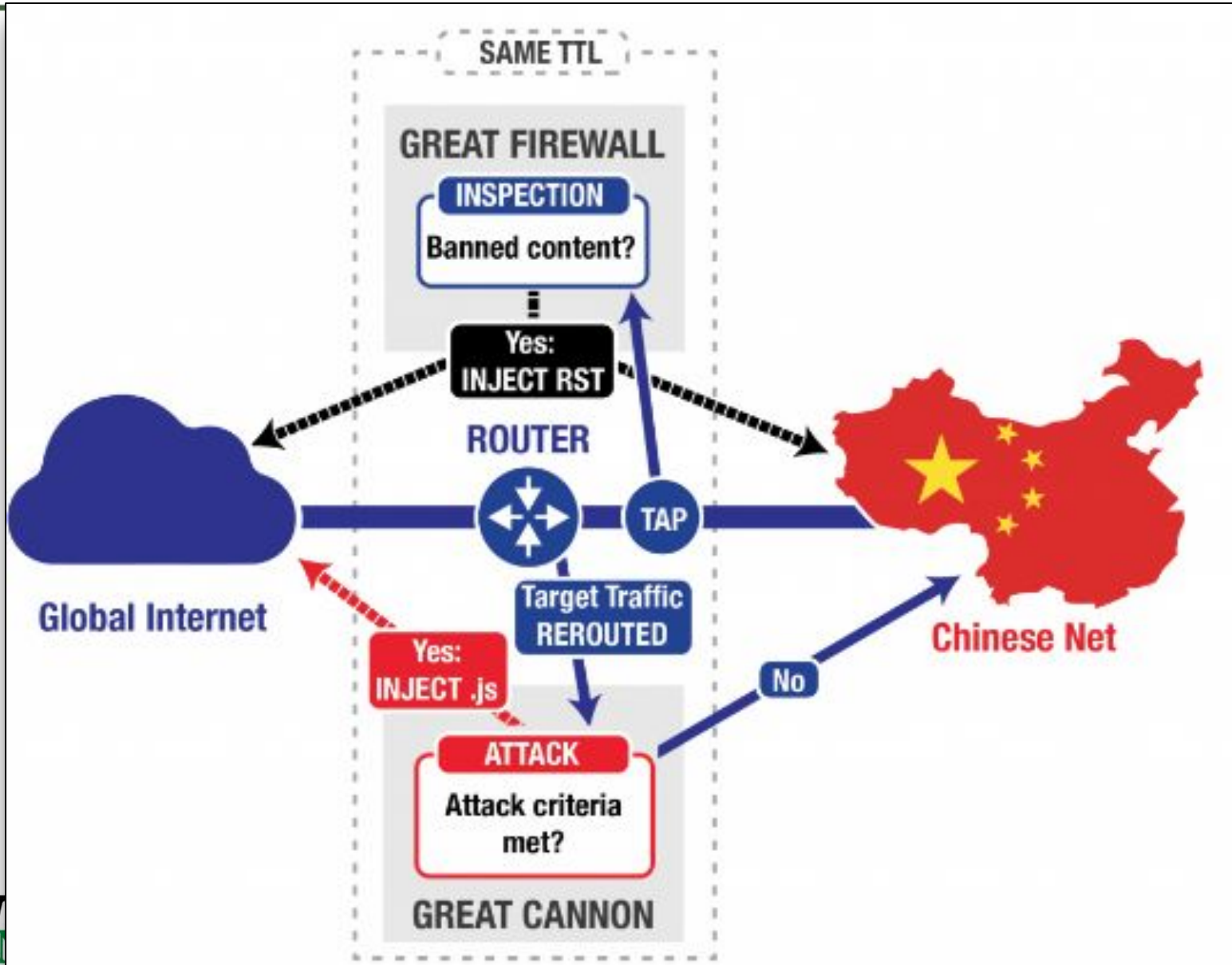
Compliance report should reach this office through return tax or at email

peshawar@pta.gov.pk today please.

インターネットを壊そうとする人達

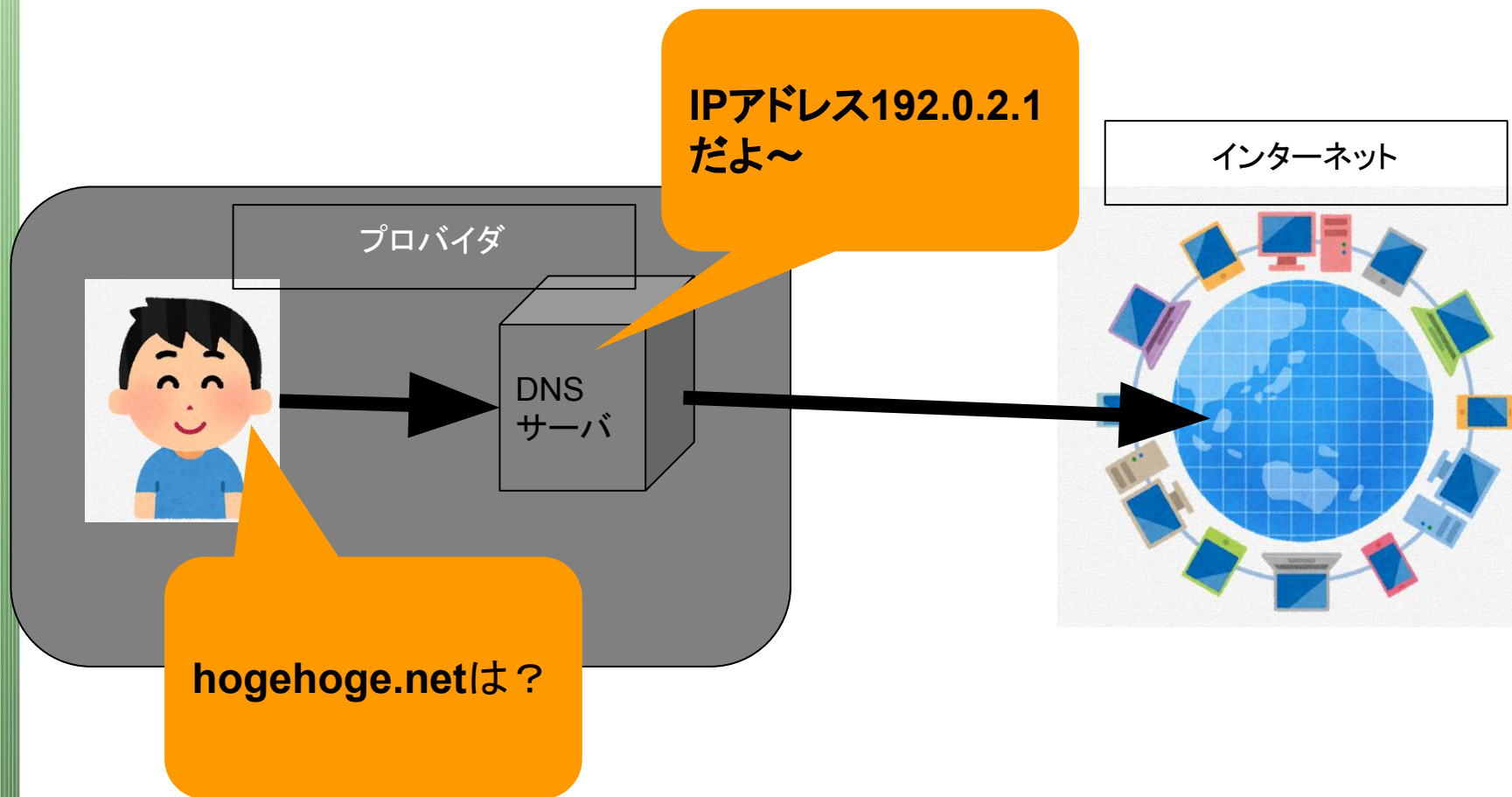


インターネットを止める人達：中国

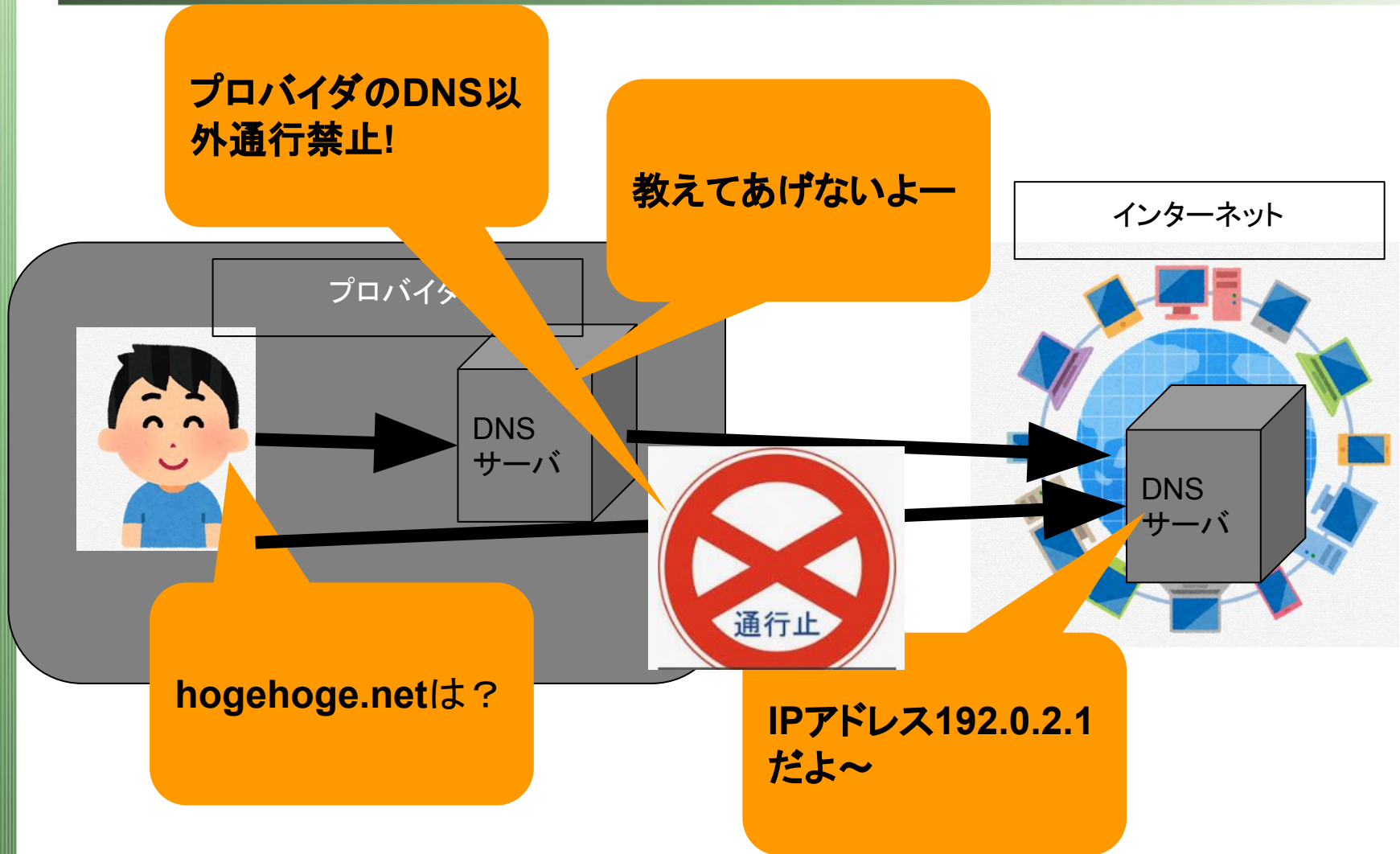


さて、仮に日本で実施する場合、実際にどういうことがおこなわれているのでしょうか。

ドメイン名からIPアドレスの変換



ドメイン名からIPアドレスの変換



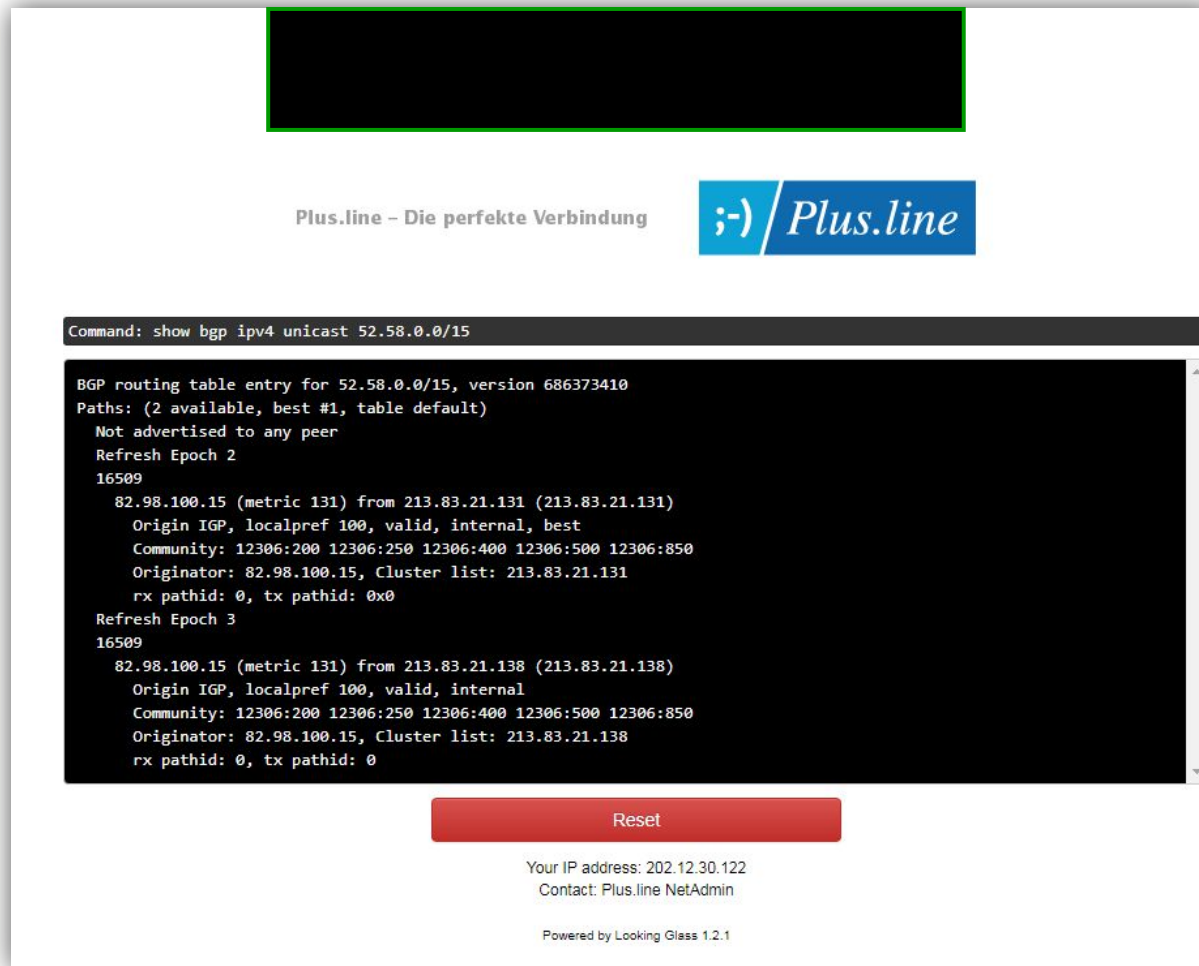
インターネットへの影響

- **インターネット停止の連鎖**
 - プロバイダでブロック
 - 第三者のDNSで回避
 - 外部のDNSをブロック
 - ブラウザによる名前解決へ回避(今開発中)
 - ブラウザでの閲覧をブロック
 - この段階でインターネットの利便は相当に悪化
 - VPNなどで回避?
 - **インターネット停止**

本当にこのブロッキングの連鎖を実施してインターネットは維持できるのか？

いたちごっこの例

- 裁判所の命令により、ロシアのLINEのようなアプリを



Plus.line – Die perfekte Verbindung

;-) / Plus.line

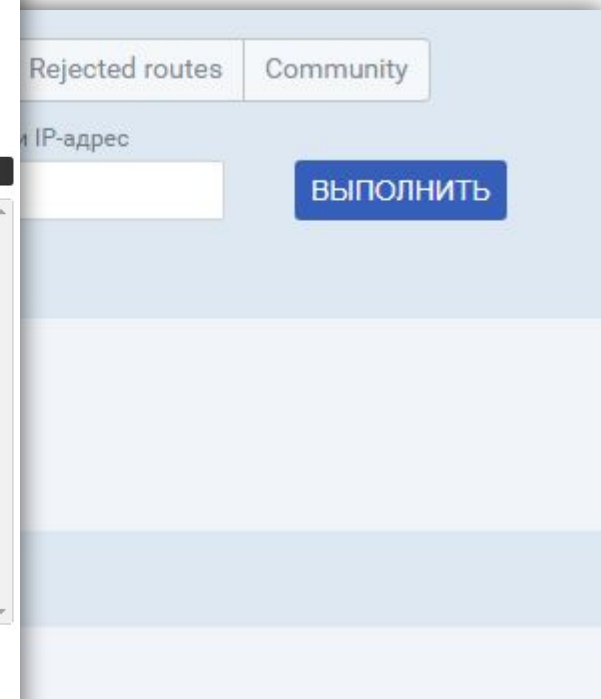
```
Command: show bgp ipv4 unicast 52.58.0.0/15
```

```
BGP routing table entry for 52.58.0.0/15, version 686373410
Paths: (2 available, best #1, table default)
  Not advertised to any peer
  Refresh Epoch 2
  16509
    82.98.100.15 (metric 131) from 213.83.21.131 (213.83.21.131)
      Origin IGP, localpref 100, valid, internal, best
      Community: 12306:200 12306:250 12306:400 12306:500 12306:850
      Originator: 82.98.100.15, Cluster list: 213.83.21.131
      rx pathid: 0, tx pathid: 0x0
  Refresh Epoch 3
  16509
    82.98.100.15 (metric 131) from 213.83.21.138 (213.83.21.138)
      Origin IGP, localpref 100, valid, internal
      Community: 12306:200 12306:250 12306:400 12306:500 12306:850
      Originator: 82.98.100.15, Cluster list: 213.83.21.138
      rx pathid: 0, tx pathid: 0
```

Reset

Your IP address: 202.12.30.122
Contact: Plus.line NetAdmin

Powered by Looking Glass 1.2.1



Rejected routes | Community

IP-адрес

ВЫПОЛНИТЬ

いちごの例

- ブロックされてしまったので、G社やA社へ移動
→ G社やA社のアドレスも追加でブロック

18.xxx.0.0/15

18.xxx.0.0/15

18.xxx.0.0/15

35.xxx.0.0/14

35.xxx.0.0/12

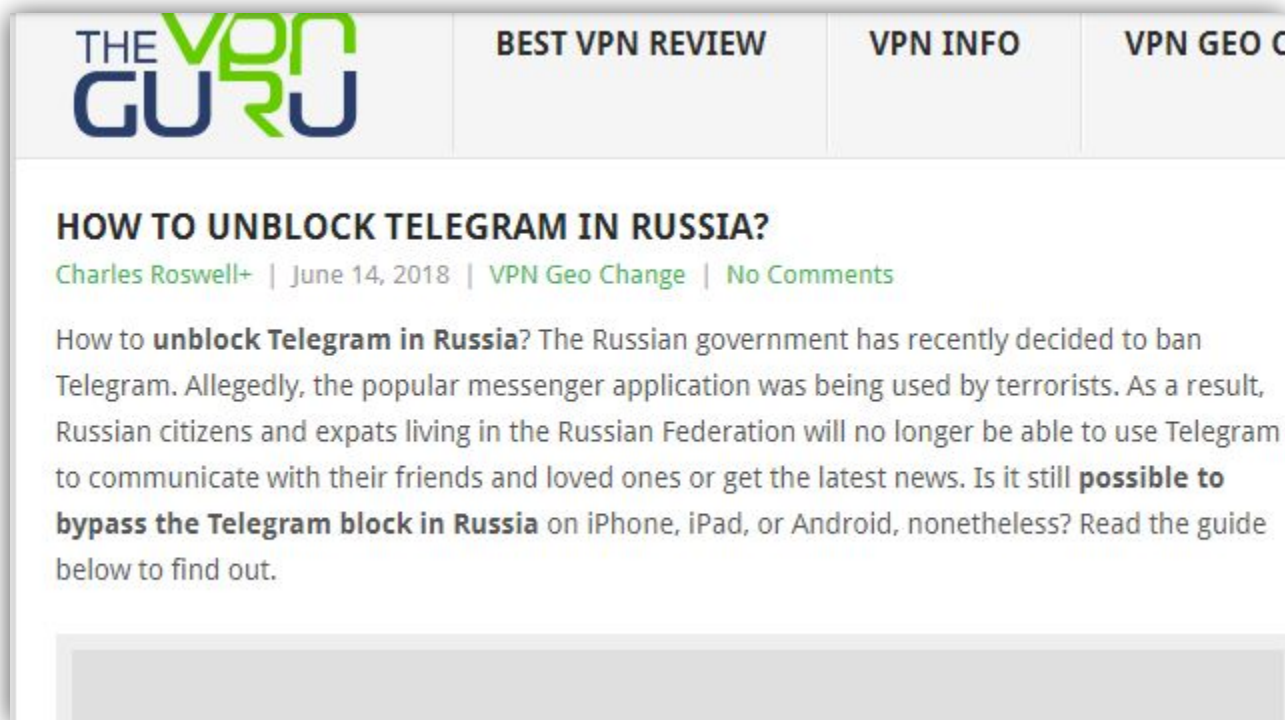
さりげなくオーバーブロッキングされて泣いている人も。

Dear users, due to the blocking of @telegram on the territory of Russia Roskomnadzor blocked more than 2 million ip addresses of the Amazon company where our servers are included, perhaps the Coinface application will temporarily not be available in Russia.

– Coinface (@coinfaceme) April 16, 2018

いちごっこの例 VPNGuRU

- ・ロシア人向けボランタリー接続サービス？
- ・自宅のインターネットを提供する人々w



本日もVPN経由でアクセスできている模様

さらに回避の例：2014年トルコ



←トルコのとある路地裏
に・・・



このようなブロッキング
回避策が・・・→

Twitter社も支援
SMSでTweet可能



ブロッキングと回避の本質

- 積極的にブロッキング回避の人は止められない

ブロッキングの効果は少なくインターネットも壊れかねないので避けましょう。

- 追加の懸念
 - ブロッキング回避アプリ等による被害も懸念
 - マルウェアや不要不急なログなどの取得も懸念



おまけ: ネットワーク運用の現場から

- IPアドレス移転の前後で経路がどれだけ細かくなったか

- 経路アーカイブからsed/awk/grep,,,,
- 遅い遅い遅い

- DBに突っ込んでみよう

- → `okadams=> create table route20180618 (ip cidr not null);`

- postgresqlはCIDR型が便利
 - 他のDBは32bitの数値に変換して比較・検索

- IPアドレスを直接DBへ入れることも可能

```
1 insert into route (ip) values ('101.0.10.0/24'); ↓
2 insert into route (ip) values ('101.0.11.0/24'); ↓
3 insert into route (ip) values ('101.0.12.0/24'); ↓
4 insert into route (ip) values ('101.0.127.0/24'); ↓
5 insert into route (ip) values ('101.0.128.0/17'); ↓
6 insert into route (ip) values ('101.0.13.0/24'); ↓
7 insert into route (ip) values ('101.0.14.0/24'); ↓
8 insert into route (ip) values ('101.0.15.0/24'); ↓
9 insert into route (ip) values ('101.0.16.0/22'); ↓
```


おまけ2

```
select ip from route where ip<=&'103.10.156.0/22' or ip>='103.10.156.0/22';  
select ip from route where ip<=&'103.10.162.0/23' or ip>='103.10.162.0/23';  
select ip from route where ip<=&'103.10.192.0/22' or ip>='103.10.192.0/22';  
select ip from route where ip<=&'103.10.196.0/24' or ip>='103.10.196.0/24';  
select ip from route where ip<=&'103.10.197.0/24' or ip>='103.10.197.0/24';  
select ip from route where ip<=&'103.10.198.0/24' or ip>='103.10.198.0/24';  
transfer.sql
```

移転されたIPアドレスがどうなったか、検索。この場合、マスク長が大きく or 小さくなった数をQuery

フルルートにこの問い合わせ(739453経路、2347の移転アドレス)の問い合わせの実行速度

- スクリプト: 87601秒(n=20)
- DB検索: 1秒以下(n=100)

おまけ 結論

- なんらかのマイDBを確保しておくで便利
- Create/Insert/Selectだけやればいい環境
- **DBインストール、権限作成がやる気を萎えさせる**
- ただし、sed/awk/grep/shellは必要
 - データを加工、DBに突っ込むところまでは
まだまだ必須
- データベースだけでなく、IaaSのスク립トエンジンなども今後必須かも。