その時何が起こったか

Internet Week 2018 S1ネットワーク運用チュートリアル～
分かると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

Copyright©2018 Japan Network Information Center

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

JPNIC 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

JPNIC Copyright©2018 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

Copyright©2018 Japan Network Information Center

インターネットの精神・根幹

自律・分散・協調
IPアドレスは配るが誰も中央統制しない

Copyright©2018 Japan Network Information Center

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

JPNIC Copyright©2018 Japan Network Information Center

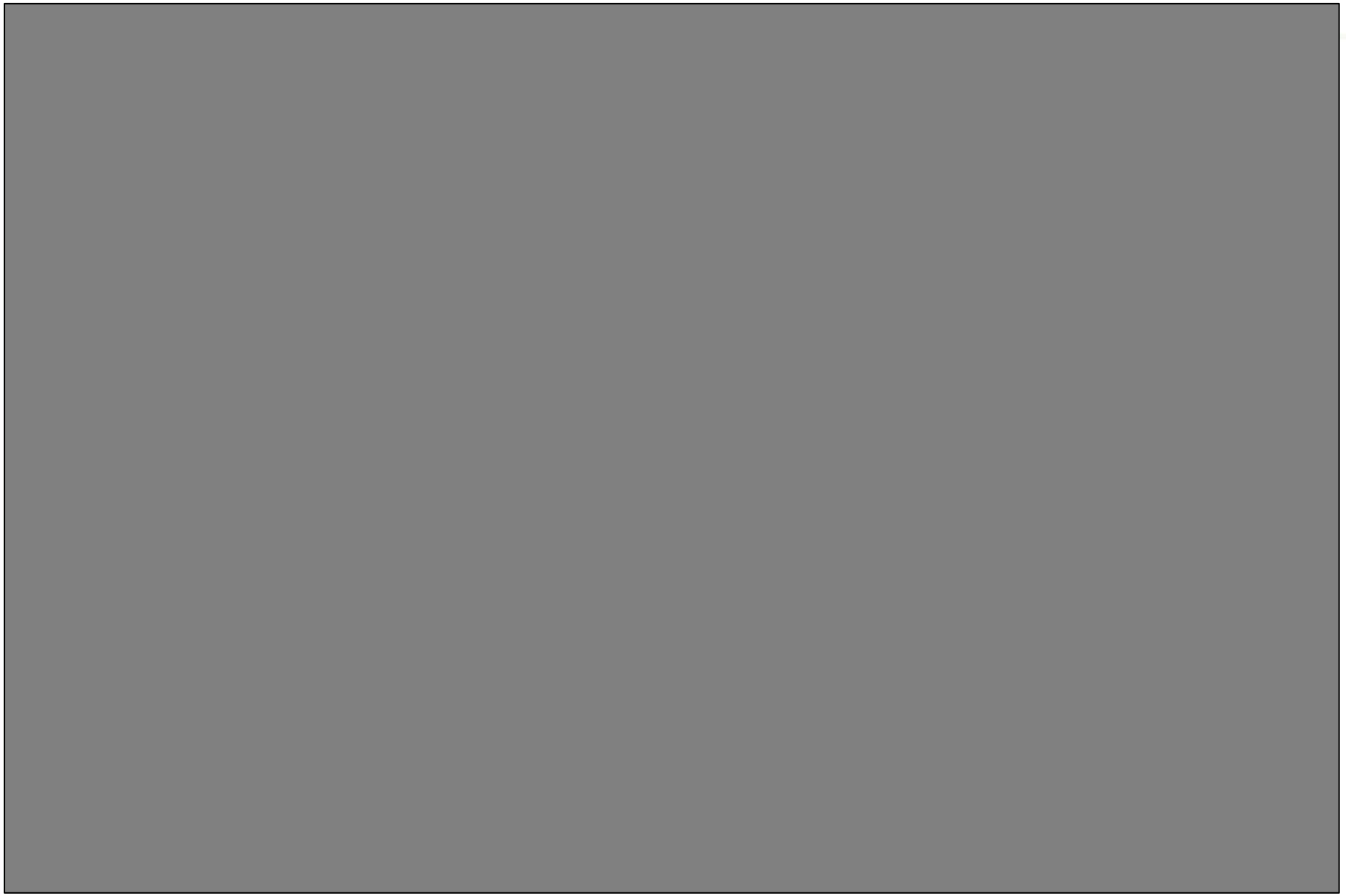
単純な例:コピペ技術者の影響

1.2.3.4
1.1.1.1
172.15.0.0
192.167.0.0

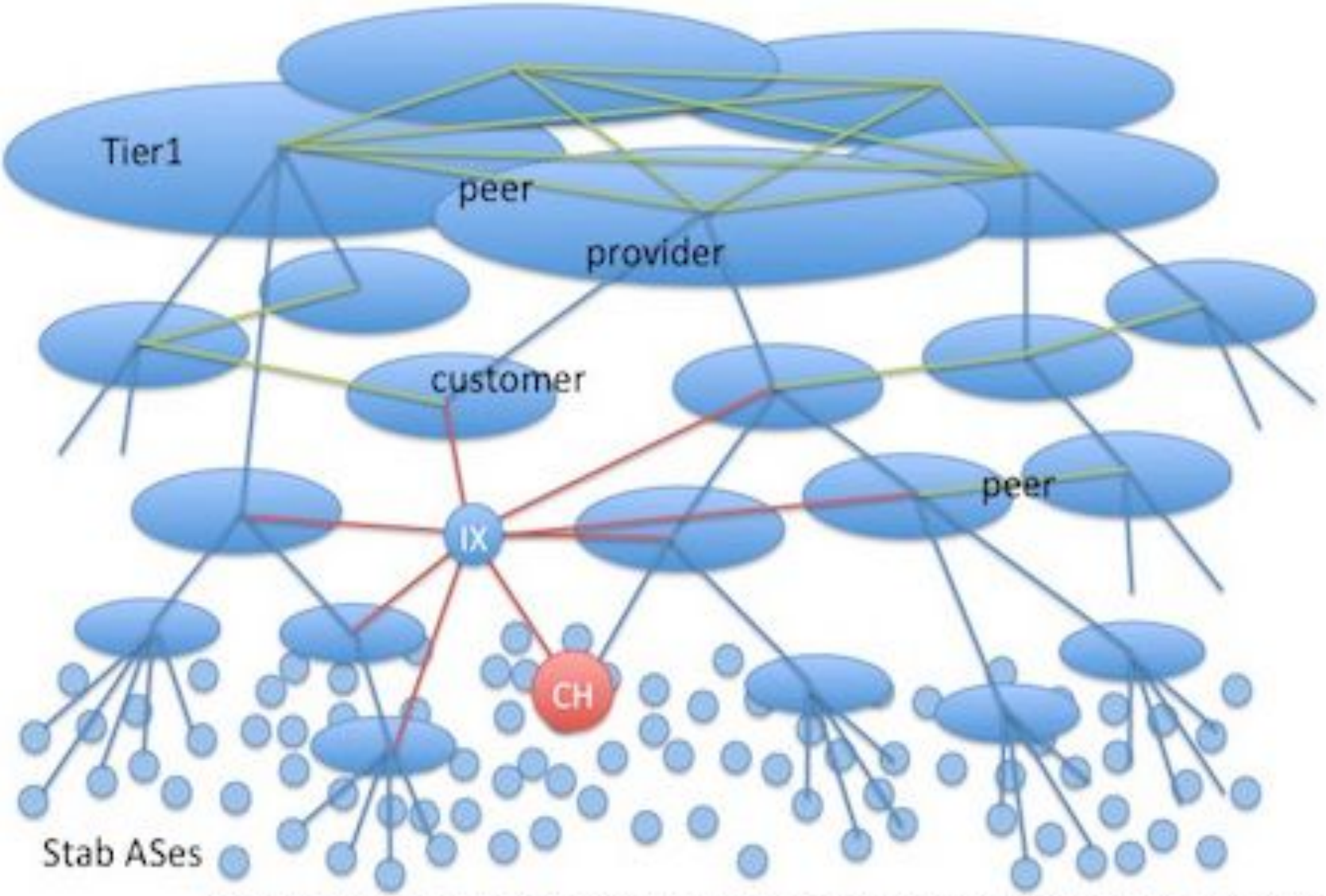
経路の乗っ取り、その時、なぜ？

Copyright©2018 Japan Network Information Center

IPアドレス重複利用（Youtube事件）



2008年2月24日



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

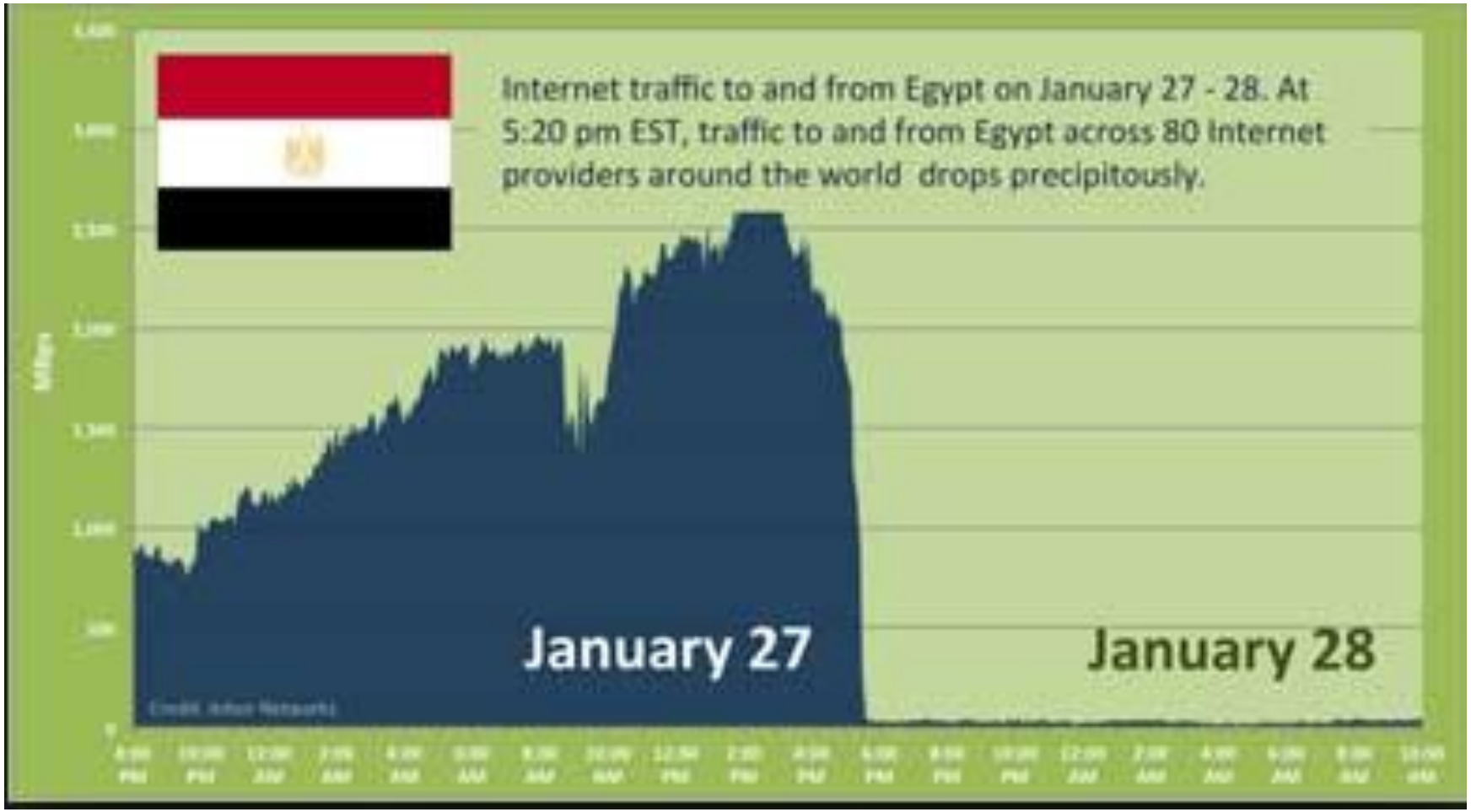
Copyright©2018 Japan Network Information Center

インターネットを壊そうとする人達

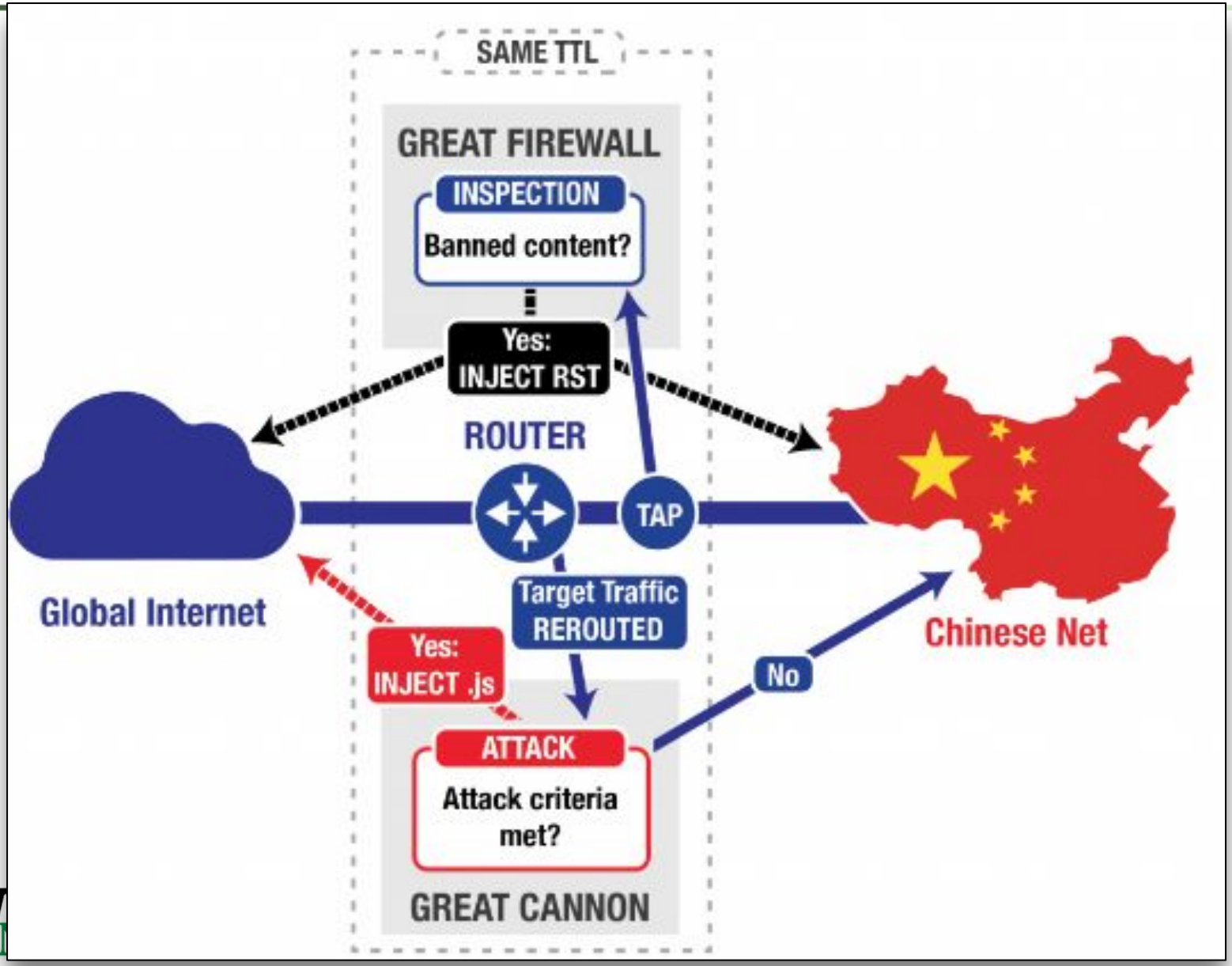
Compliance report should reach this office through return fax or at email

peshawar@pta.gov.pk today please.

インターネットを壊そうとする人達



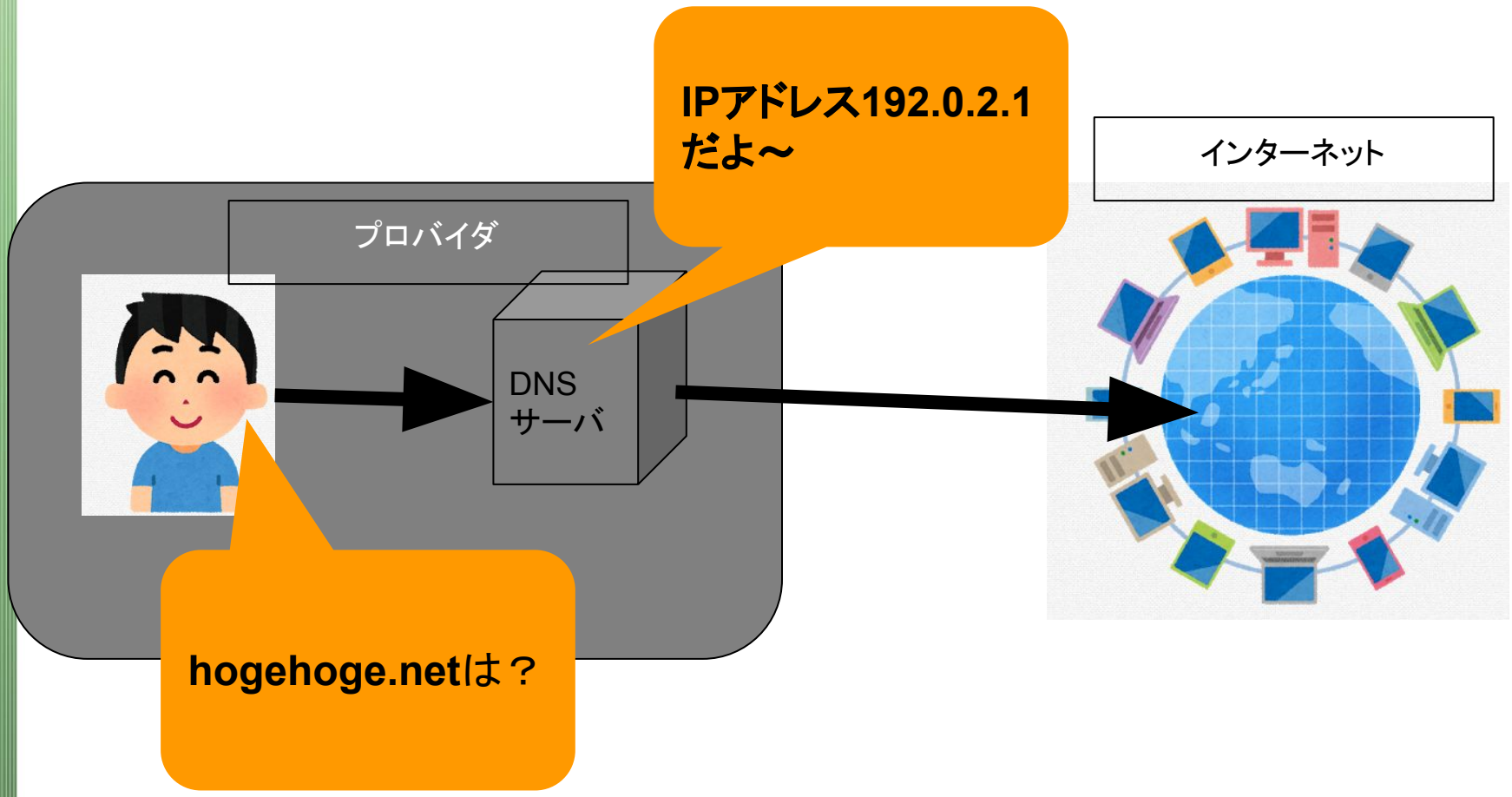
インターネットを止める人達：中国



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。

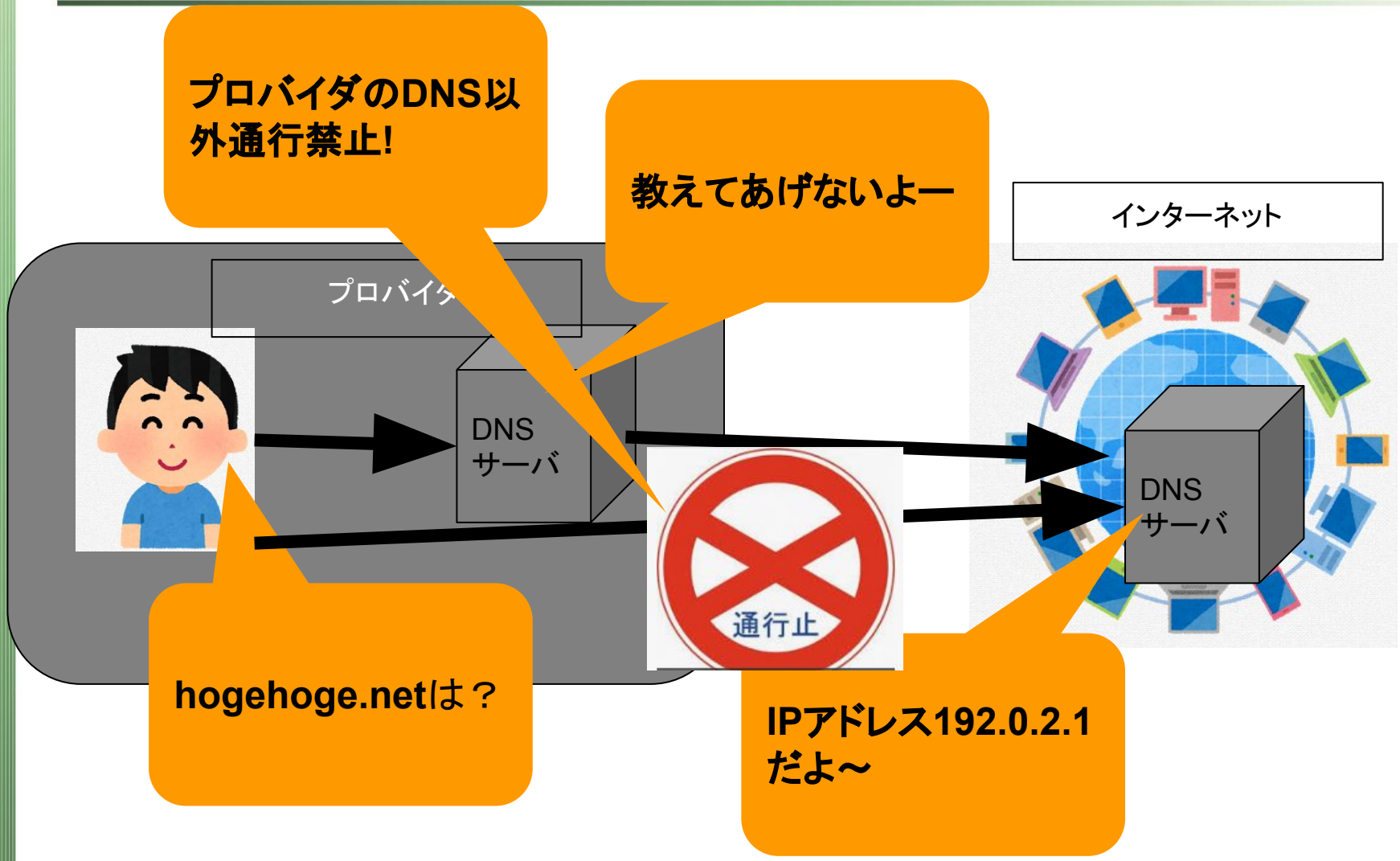
Copyright©2018 Japan Network Information Center

ドメイン名からIPアドレスの変換



Copyright©2018 Japan Network Information Center

ドメイン名からIPアドレスの変換



Copyright©2018 Japan Network Information Center

インターネットへの影響

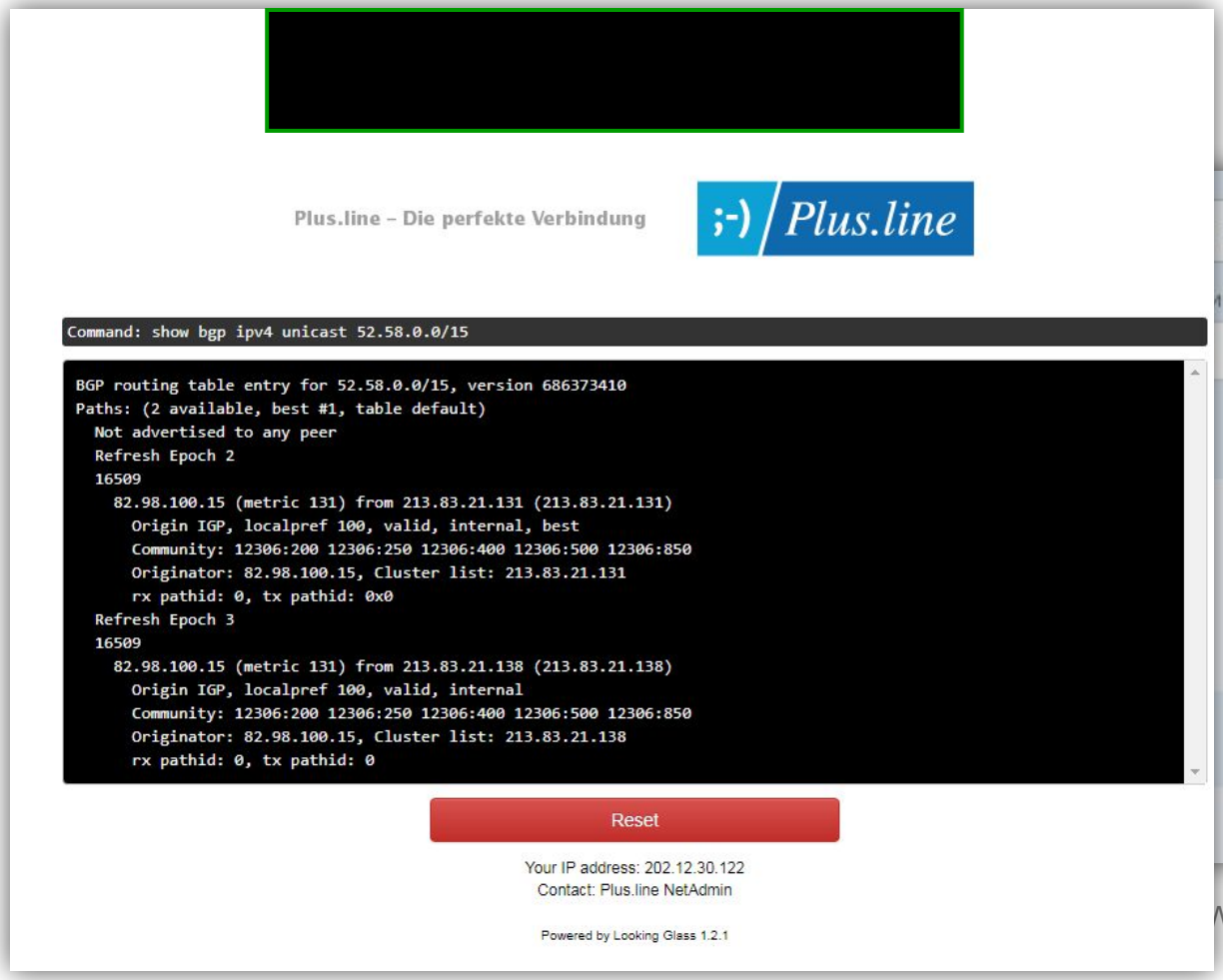
- **インターネット停止の連鎖**
  - プロバイダでブロック
    - 第三者のDNSで回避
  - 外部のDNSをブロック
    - ブラウザによる名前解決へ回避（今開発中）
  - ブラウザでの閲覧をブロック
    - この段階でインターネットの利便は相当に悪化
    - VPNなどで回避？
  - インターネット停止

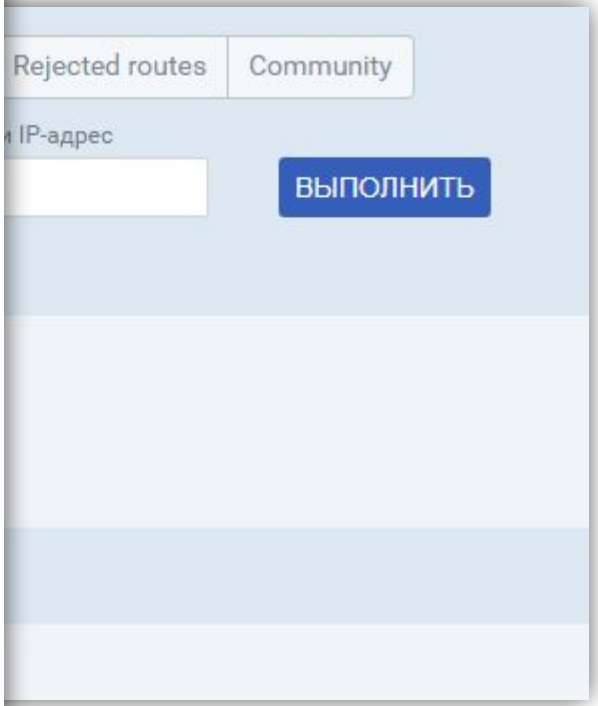
本当にこのブロッキングの連鎖を実施してインターネットは維持できるのか？

JPNIC Copyright©2018 Japan Network Information Center

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





いたちごっこの例

- 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

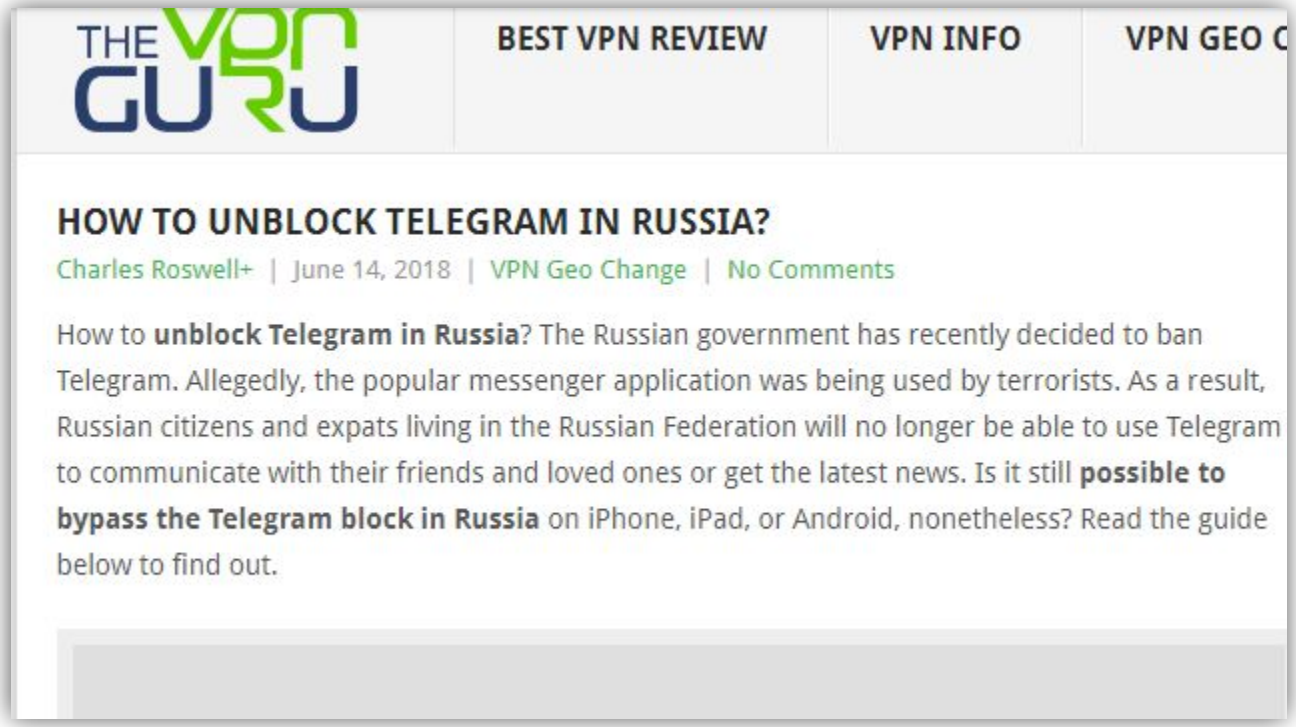
さりげなくオーバーブロッキングされて泣いている人も。

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

いたちごっこの例 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

Copyright©2018 Japan Network Information Center

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

JPNIC Copyright © 2018 Japan Network Information Center

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。

- **追加の懸案**
  - 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案

Copyright © 2018 Japan Network Information Center

Copyright© 2018 Japan Network Information Center

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');
```

Copyright©2018 Japan Network Information Center

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)

Copyright©2018 Japan Network Information Center

おまけ 結論

- なんらかのマイDBを確保しておくと便利
- 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のスクリプトエンジンなども今後必須かも。

Copyright©2018 Japan Network Information Center