

IRS25 DDoS対策あれこれ

2016.09.20

西塚要(NTTコミュニケーションズ)

@__kaname__

自己紹介

- 2006年 NTTコミュニケーションズ入社
 - OCNアクセス系ネットワークの設計
 - 大規模ISP保守運用サービス担当
- 現在、研究開発部門にてDDoS対策ソリューション関連技術およびデータ解析技術開発とIETF提案活動に従事
 - IETF DOTS WGでドメイン間で協力したDDoS対策手法の標準化頑張ってます😊



BGPを利用したDDoS対策

- BGPを利用したInter-DomainのDDoS対策手法
 1. RTBH(Remotely Triggered Black-Hole Routing)
 2. BGPを利用したトラフィック引き込み
 3. BGP Flowspec

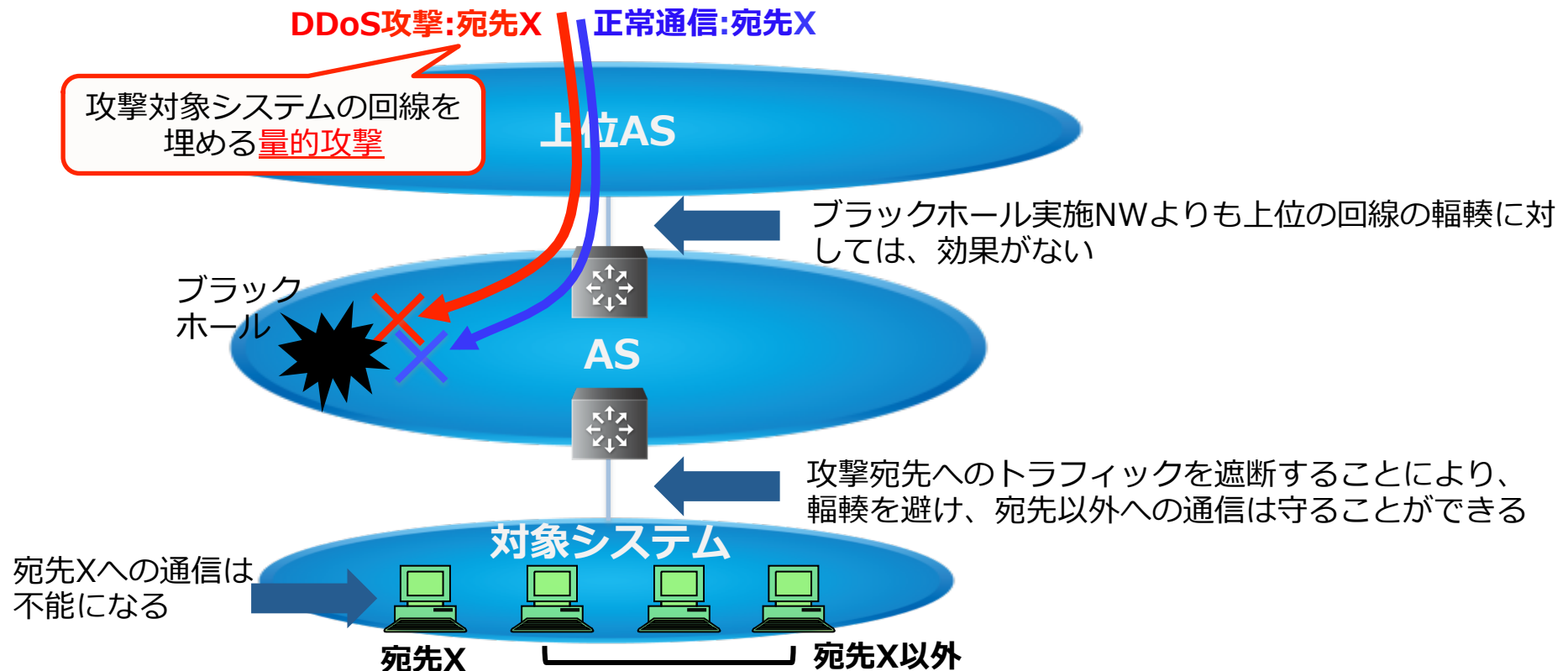


今回は、1,2の手法の実例について話します

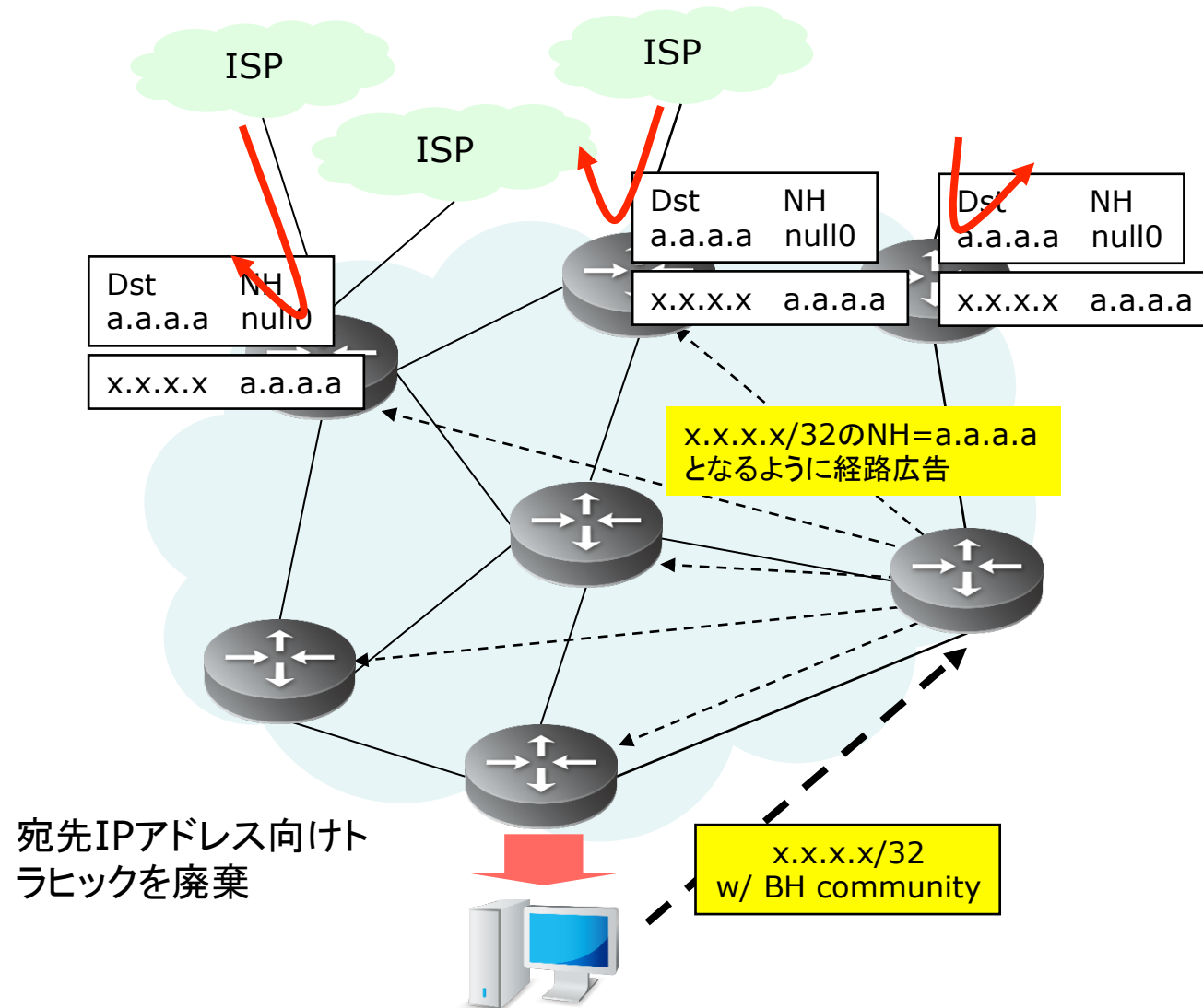
1. RTBH(Remotely Triggered Black-Hole Routing)
2. BGPを利用したトラフィック引き込み

ブラックホールルーティング

- 攻撃のターゲットとなったIPアドレス宛の通信を遮断
- ターゲットに対する全てのトラフィックが遮断されるため、攻撃自体は成立

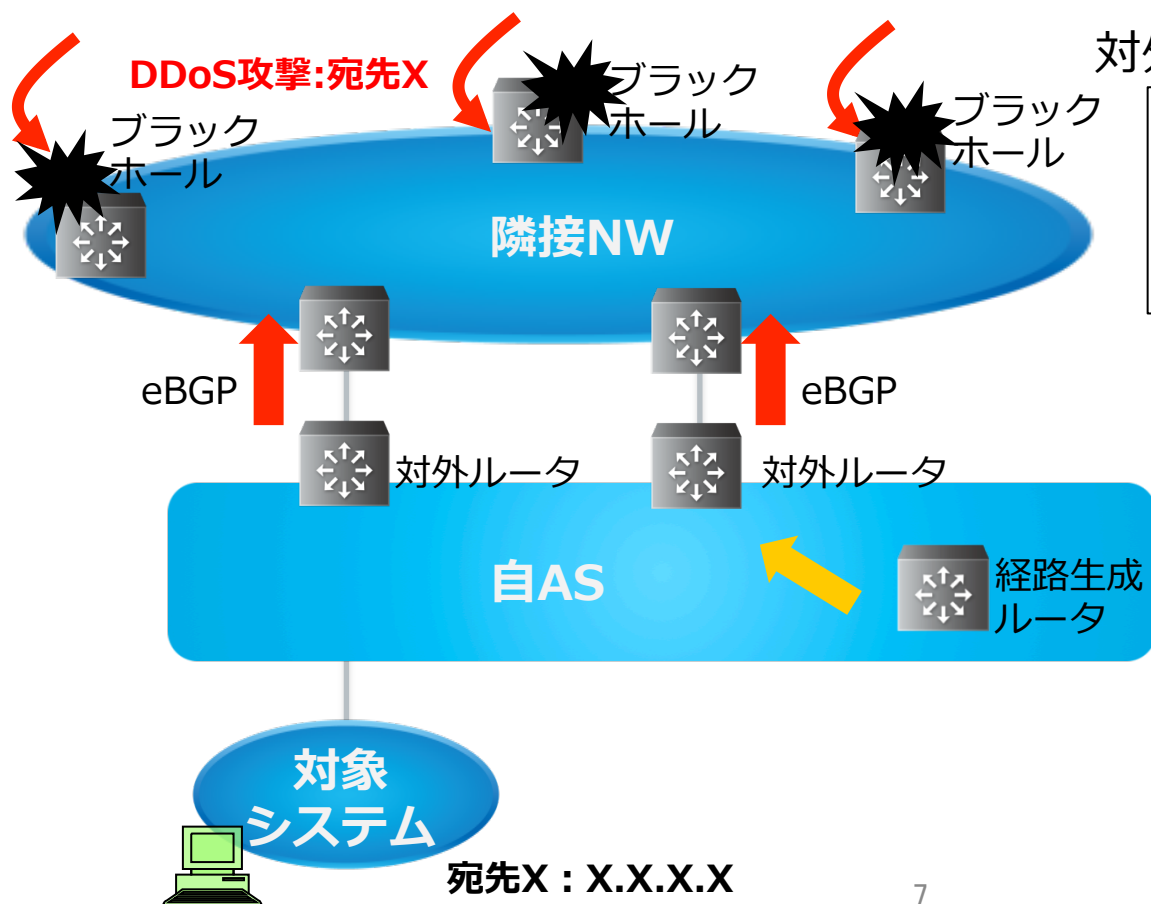


RTBH(Remotely Triggered Black-Hole Routing)



隣接NWにおけるRTBHサービス

- 一部のトランジットASやIX事業者は、顧客からのRTBH経路を受け入れている



対外ルータ :

経路広告 :
eBGP
match community <AS>:666
then set community 65535:666

経路生成ルータ :

経路生成 :
ip route X.X.X.X/32 null0
static-to-BGP

経路広報 :
iBGP
community <AS>:666

隣接するNW(ISP/IXP)によるRTBH

- メリット
 - 自ASに攻撃が入ってくる前に攻撃を止められるため、上流回線の輻輳を避けることができる
 - 自ASのRTBHと組み合わせて利用できる
 - 自動化が容易である
- デメリット
 - 攻撃が止まったかどうかの判断ができない
- 注意点
 - 対応していない事業者もある
 - RTBH用の広告経路を受け入れてもらえるようフィルタを空けてもらうことを忘れないように

RTBH用のBGP community

- IETF GROW WGにてCommunityの共通化の提案がされている (draft-ietf-grow-blackholing)
 - 65535:666 になる見込み

Motivation: Different Triggers for Blackholing

- Different triggers for Blackholing at IXPs (selection):
 - DE-CIX Apollon Blackhole IP Address: FRA: 80.81.193.66, NY: 206.130.10.66
 - Netix Blackhole Community: 65499:999
 - MSK-IX.ru Blackhole Community: 0:666 ⚡
 - NIX.CZ Fenix: RTBH
 - TPIX.pl Blackhole Community: 29535:666 ⚡

⚡ Policy control at route servers
- Different triggers for Blackholing at ISPs (selection):
 - Init7: Blackhole Community: 65000:666
 - Team Cymru: Blackhole Community: 64496: 666
 - Hurrican Electric: Blackhole Community: 6939:666
 - NTT: Blackhole Community: 2914:666
- Proposal: One commonly agreed way to trigger Blackholing at IXPs and ISPs -> Internet Draft

Selective RTBH

- 全網内でブラックホール化するのではなく、地域ごとや国ごとなどの特定エリアのルータでのみパケットを破棄する
- 自国内の折り返しについてはブラックホールさせたくない場合などの利用方法が考えられる
- 例: AS2914

Selective Blackhole communities	
2914:661	only blackhole inside the region the announcement originated
2914:663	only blackhole inside the country the announcement originated
2914:660	only blackhole outside the region the announcement originated
2914:664	only blackhole outside the country the announcement originated

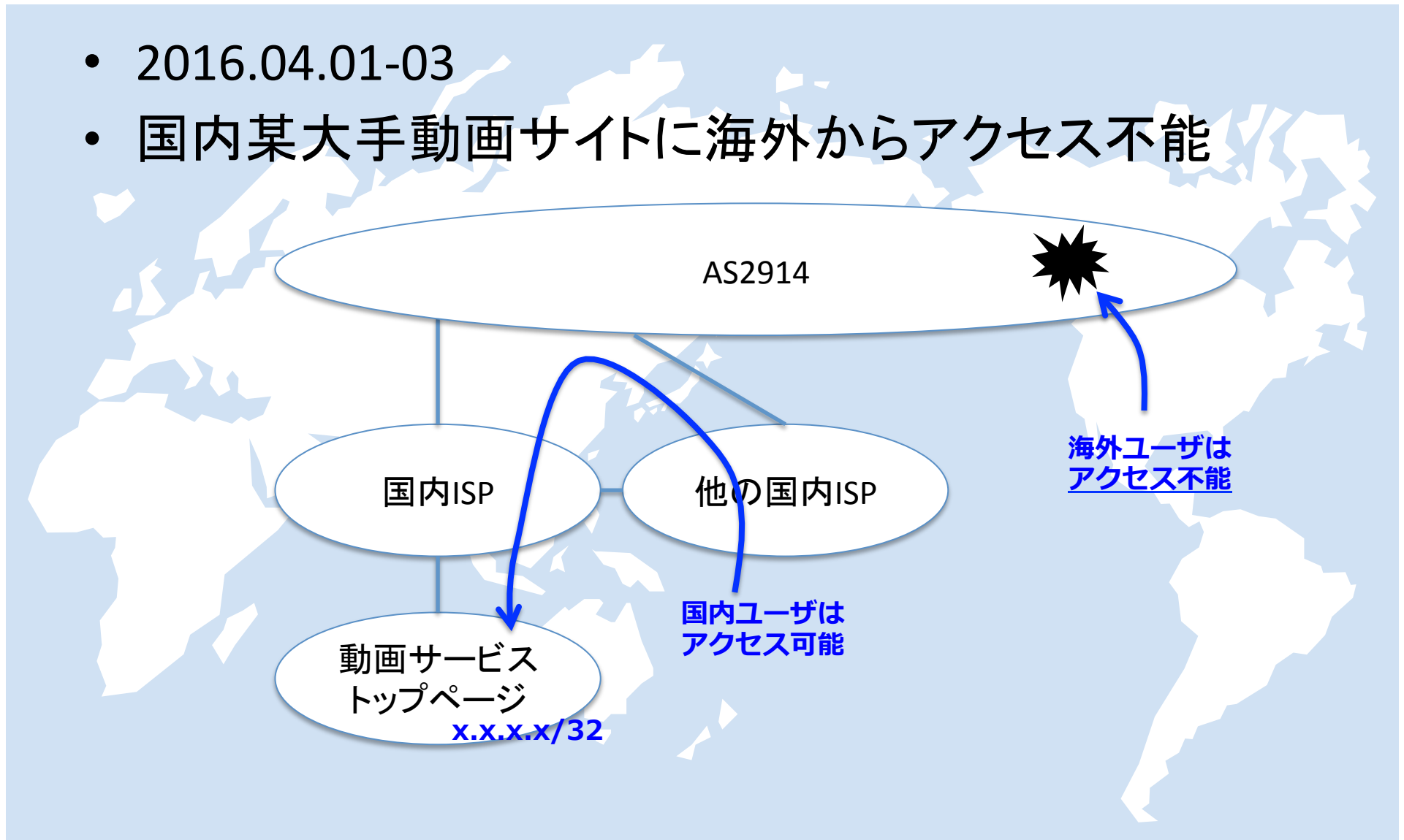
<https://www.us.ntt.net/support/policy/routing.cfm>

RTBH事例紹介

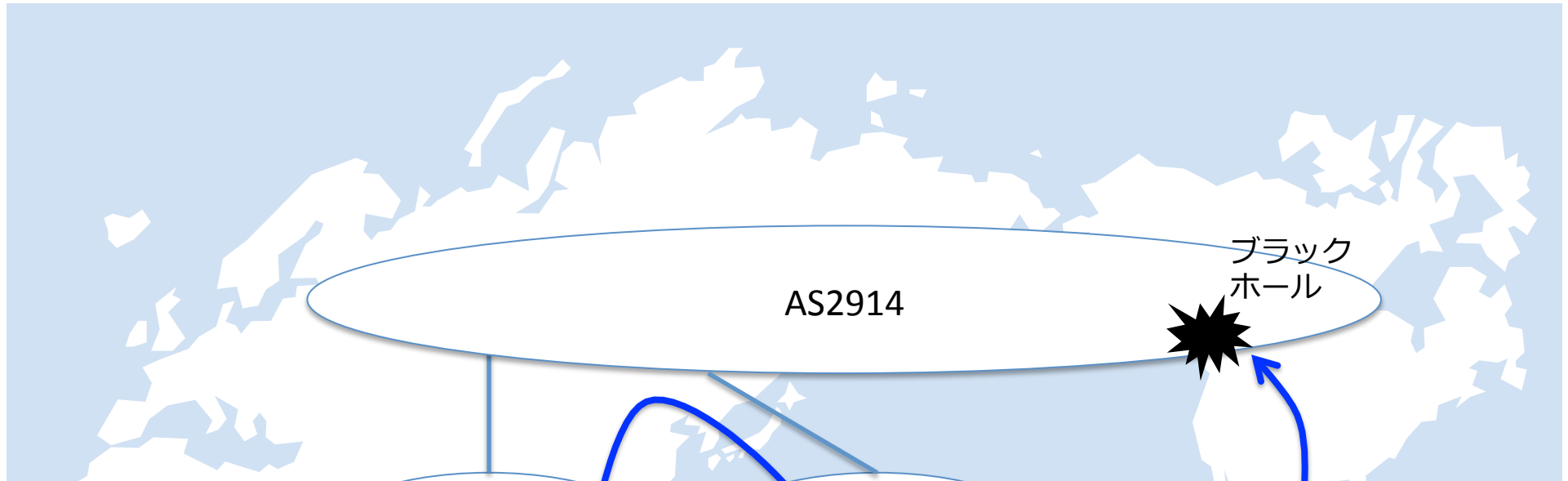
(公開情報から推定したもののため、実際の事象と異なる可能性あることはご承知ください)

事象

- 2016.04.01-03
- 国内某大手動画サイトに海外からアクセス不能



traceroute



海外からのトレース

```
$ traceroute -a x.x.x.x
```

```
traceroute to x.x.x.x (x.x.x.x), 64 hops max, 52 byte packets
```

```
1 [AS19230] 31.133.160.3 (31.133.160.3) 4.869 ms 3.705 ms 3.897 ms
2 [AS56554] 31.130.232.18 (31.130.232.18) 7.053 ms 1.354 ms 1.258 ms
3 [AS27757] 190.216.88.9 (190.216.88.9) 1.614 ms 5.052 ms 5.173 ms
4 [AS22566] po2-30g.ar2.mia2.gblx.net (67.17.106.162) 132.509 ms 133.579 ms 130.583 ms
5 * * *
6 *^C
```

looking glass@AS2914

該当アドレスが/32で広告され、経路に
Selective RTBH Community 2914:664 が付与
されていることを確認
2914:666 -> アナウンスされた国の外でのみ
ブラックホール

looking glass

<https://www.us.ntt.net/support/looking-glass/>

AS2914

ブラック
ホール

海外ユーザは
アクセス不能

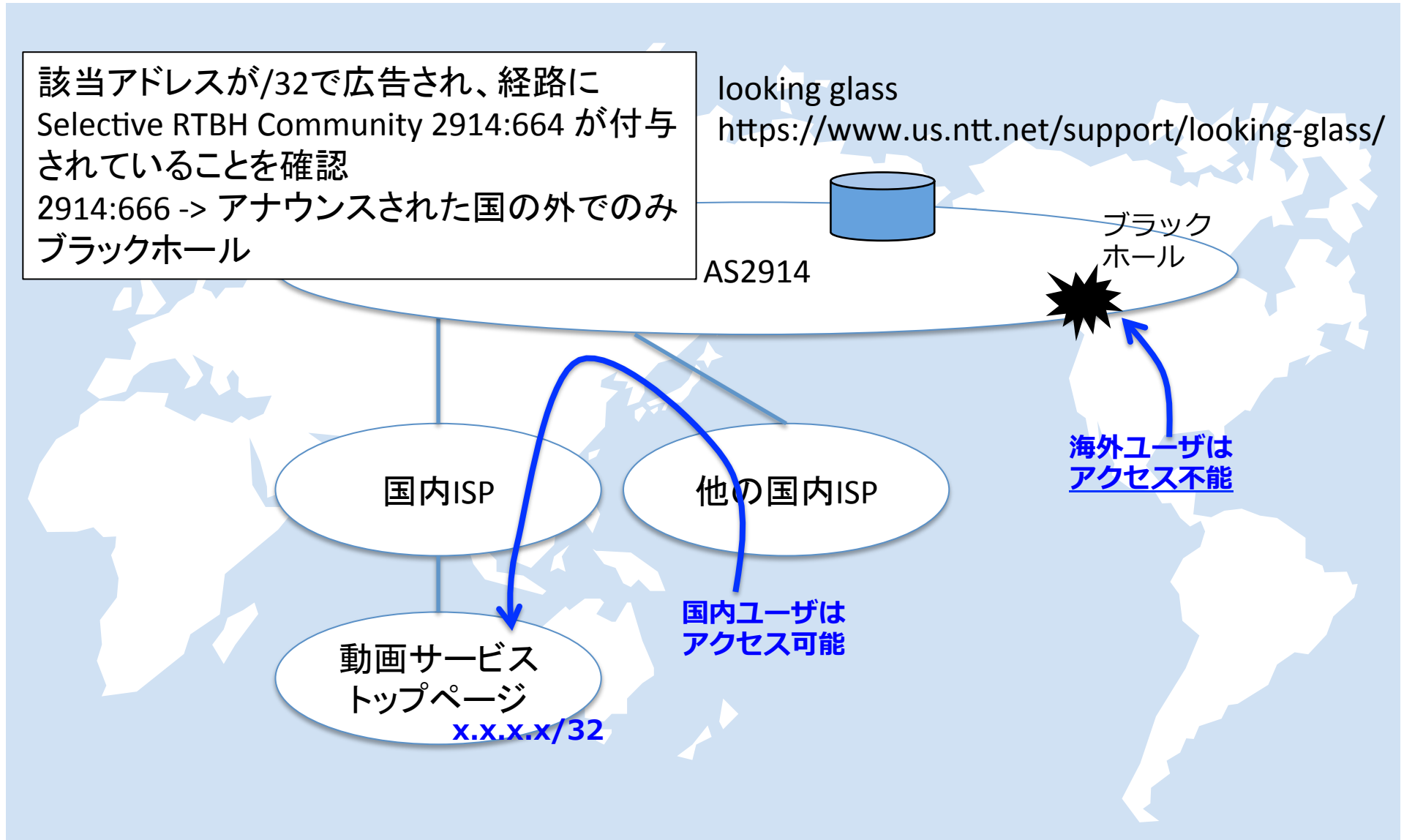
国内ISP

他の国内ISP

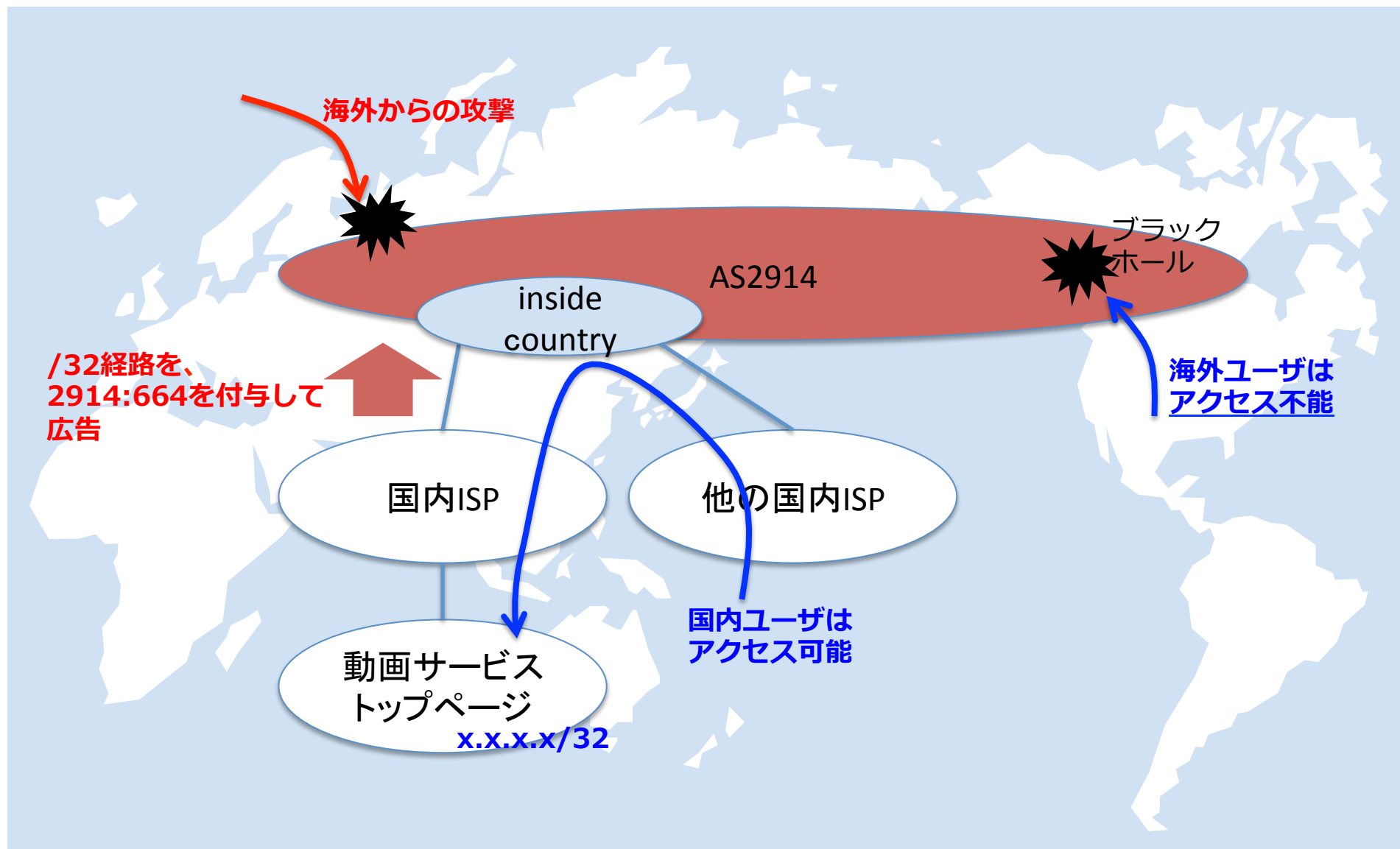
動画サービス
トップページ

x.x.x.x/32

国内ユーザは
アクセス可能



DDoS攻撃への対処(推測)



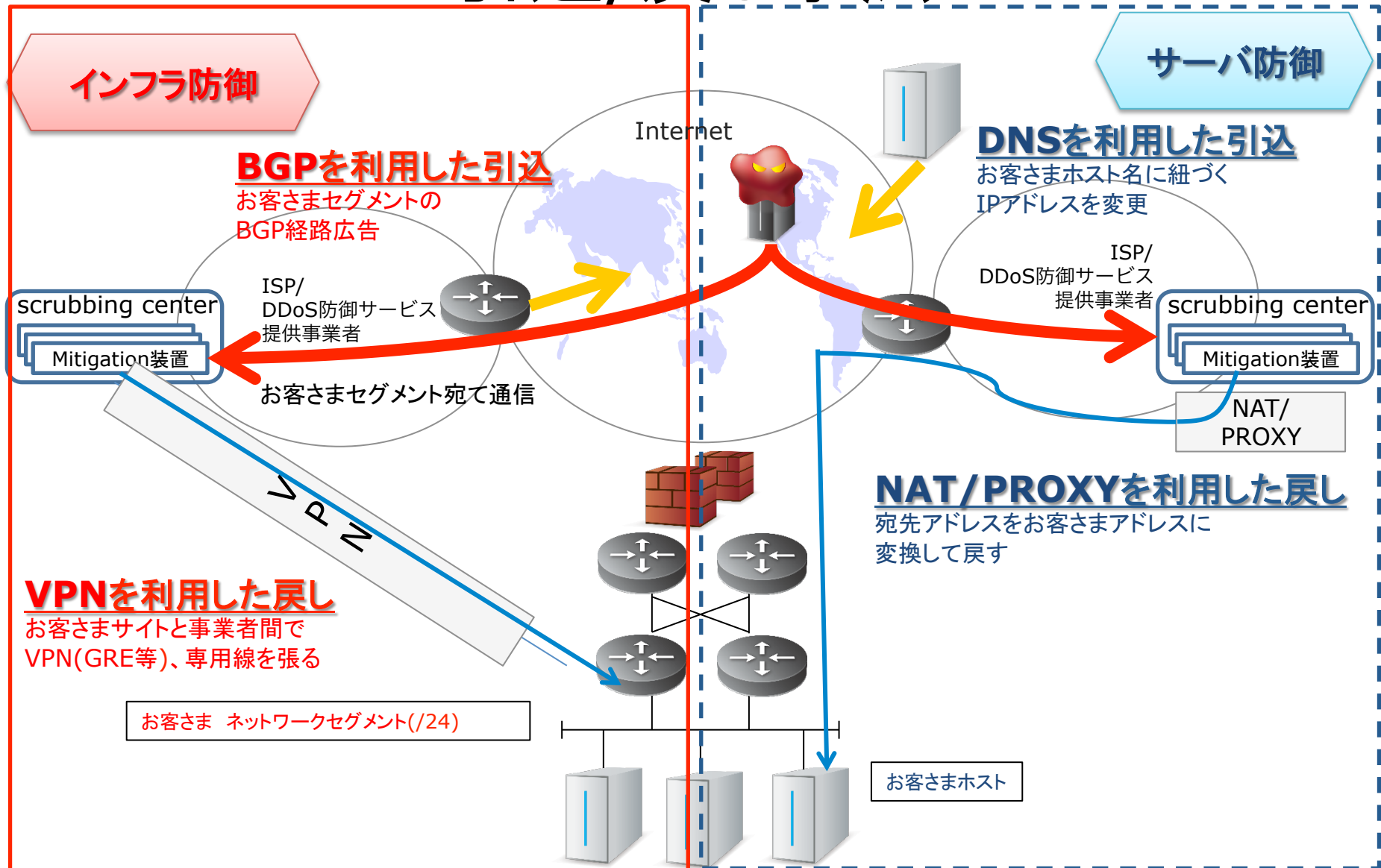
RTBH - Lessons Learned

- Selective RTBHでも、巻き込み被害の範囲(メリット・デメリット)を理解して利用することが重要
- エンドユーザの立場だと、意図的なものかどうか気づきにくい
 - Looking Glassなど、RTBHの状況を把握できる手法の提供が必要
- JANOG38 BoF(*)より
 - コンテンツプロバイダとしては、RTBHは何も守っていないことになるので、緩和する対策が欲しい

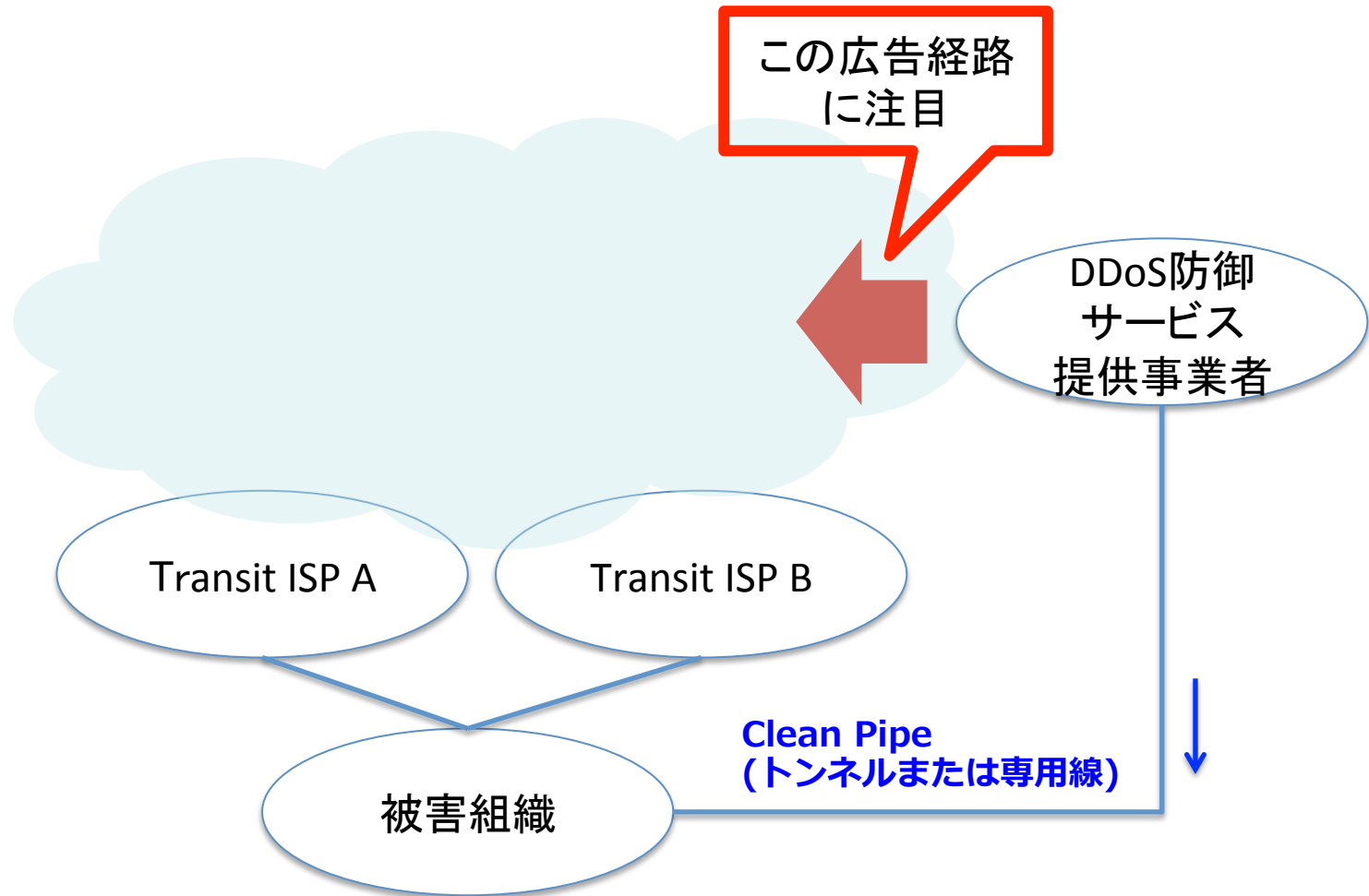
(*)<https://www.janog.gr.jp/meeting/janog38/program/ddos.html>

1. RTBH(Remotely Triggered Black-Hole Routing)
2. BGPを利用したトラフィック引き込み

Cloud型DDoS防御サービス 引込/戻し手法



引き込み経路



AS-PROLE(Prolexic)解析

- 2016.01.01～2016.09.19の期間の1時間ごとのフルルート(dump)から、AS-PATHにAS-PROLE(AS32787)を含むものを抽出
 - updateを追っていないので、1時間以内のイベントは対象から漏れています
- (プレフィックス,AS-PATH)の組みでユニークな広告数: 2706
 - うちユニークなプレフィックス数:2376

比較対象

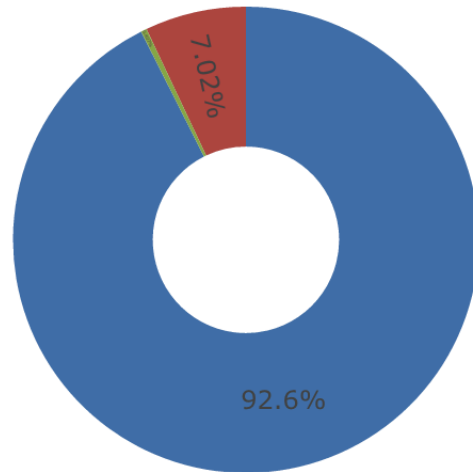
- Team Cymru:”IP to ASN Mapping”プロジェクト
 - <http://www.team-cymru.org/IP-ASN-mapping.html>
 - 4時間ごとの更新
 - 対象のprefixに対して、AS番号などを引く
 - 2016.09.19での応答を利用

```
% dig TXT 8.8.8.origin.asn.cymru.com
```

```
:: ANSWER SECTION:
```

```
8.8.8.origin.asn.cymru.com. 14400 IN  TXT "15169 | 8.8.8.0/24 | US | arin |"
```

Prole announce by different origin



same
diff
none

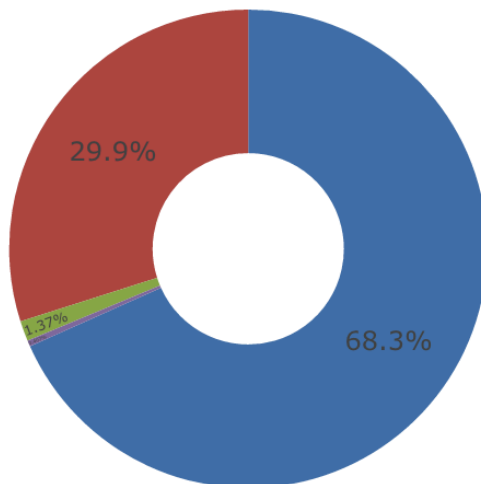
オリジン比較

diff: 広報されたprefixのオリジンと、cymruで引いたオリジンが異なる場合

same: 同じ場合

none: cymruサービスが引けなかった場合

Prole Longer announcement



eq
longer
shorter
none

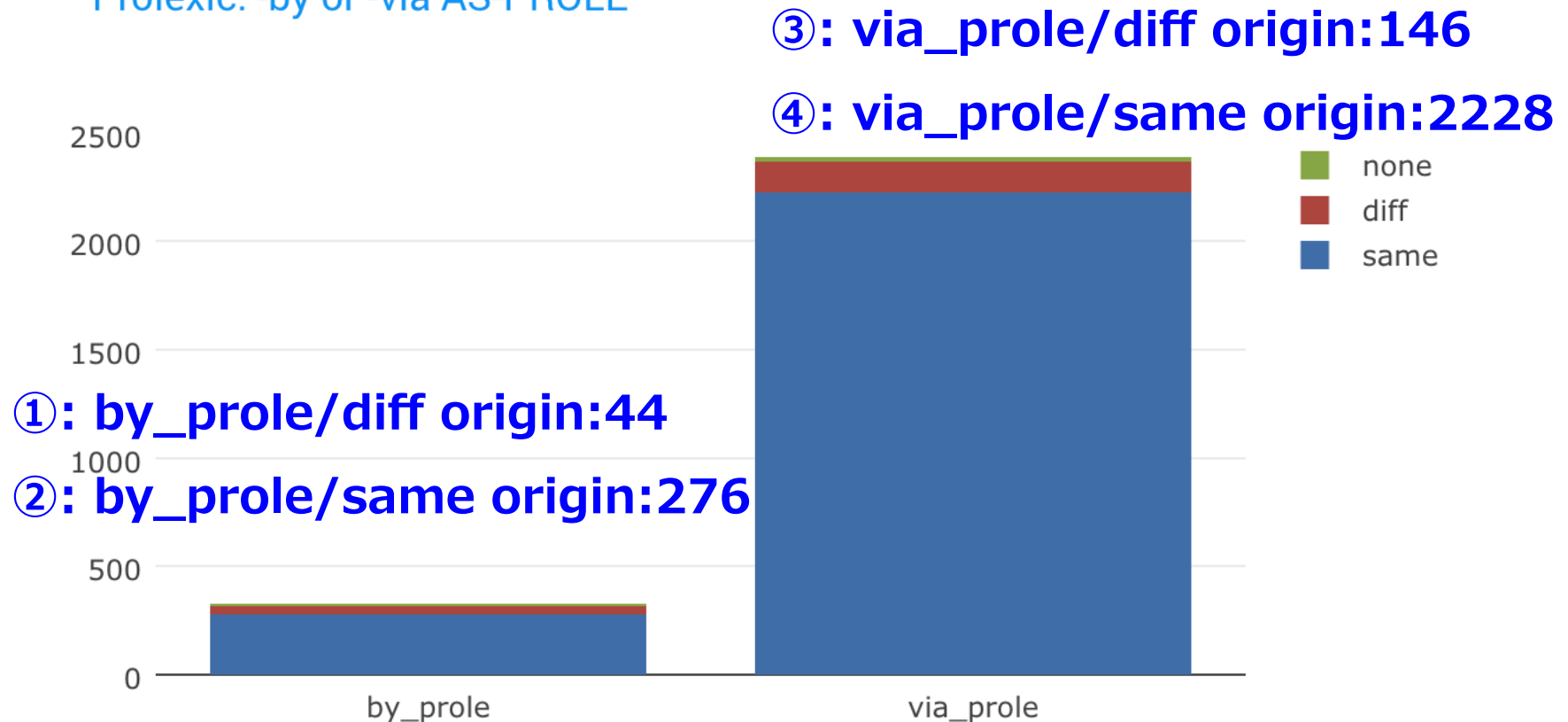
prefix長比較

longer: 広報されたprefixのprefix長が、cymruで引いたものより長い場合

eq: 同じ場合

shorter: 短い場合

Prolexic: -by or -via AS-PROLE



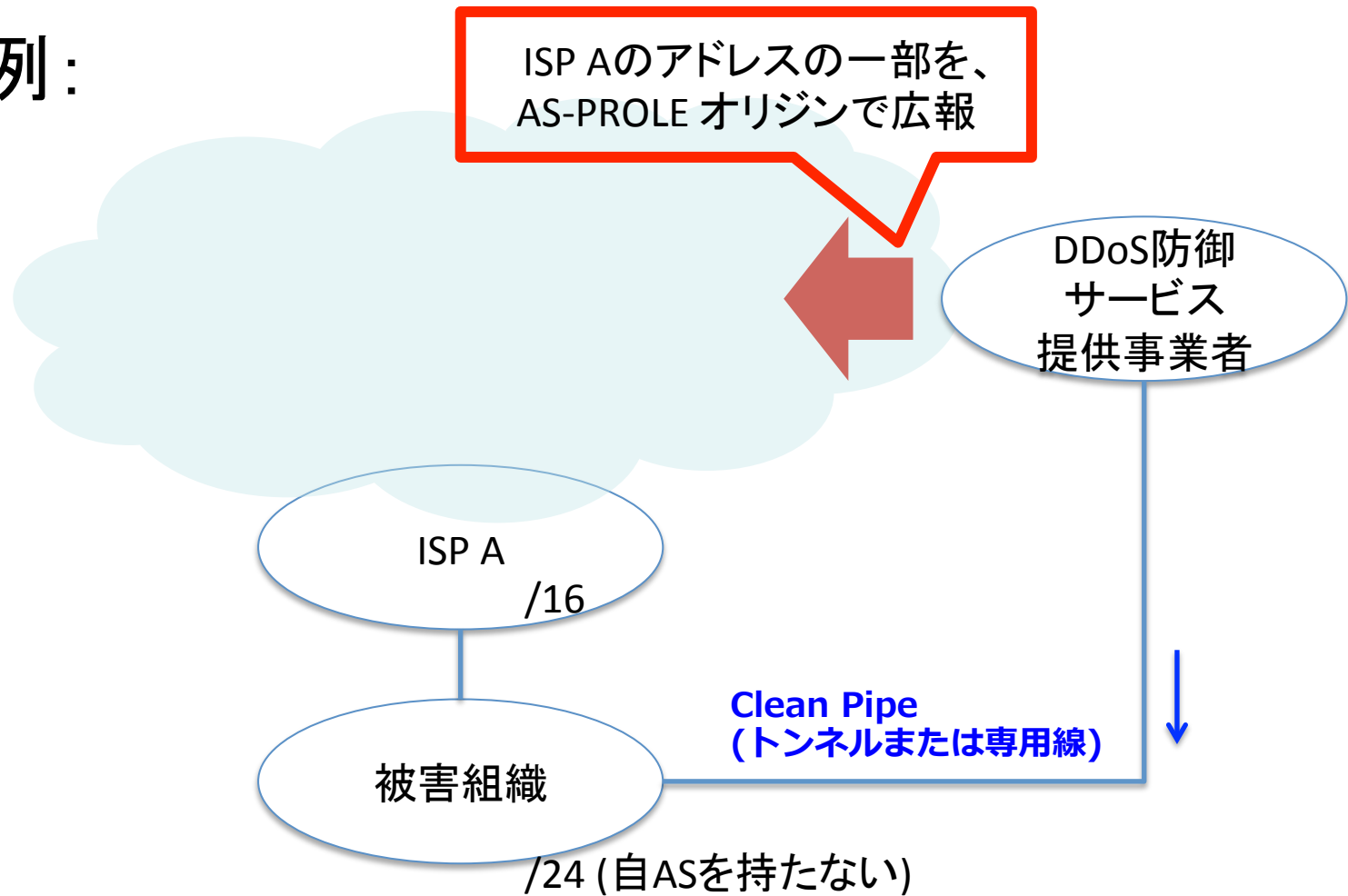
AS-PROLEがオリジンか否か

by_prole: AS-PROLEがオリジンASの広報

via_prole: AS-PROLEがパスの途中の広報

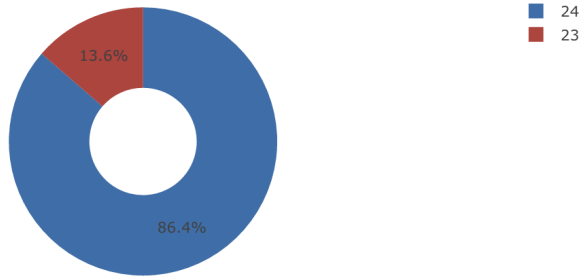
①: by_prole/diff origin: 44

例:



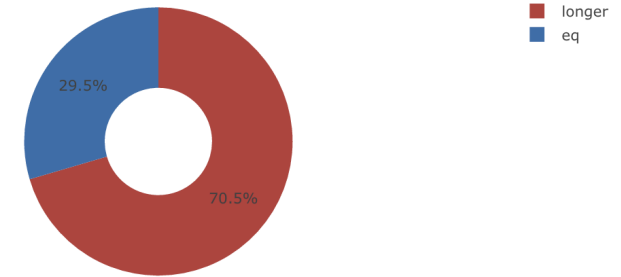
①: by_prole/diff origin: 44

Prolexic: 1.by_prole/diff origin prefix_len



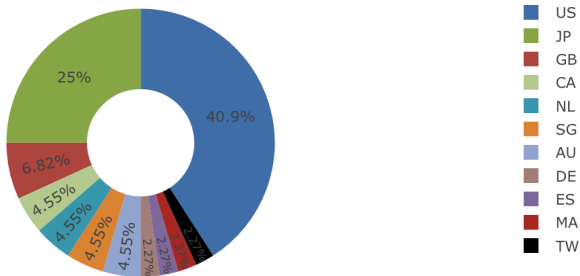
Updated: 5 hours ago

Prolexic: 1.by_prole/diff origin is_longer

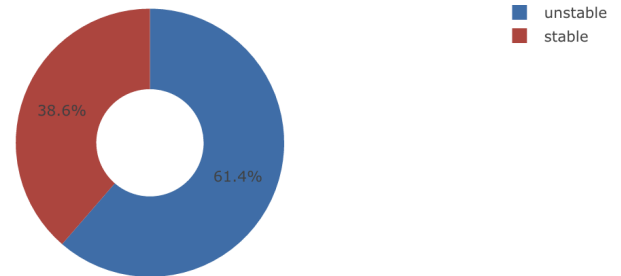


Updated: 4 hours ago

Prolexic: 1.by_prole/diff origin country

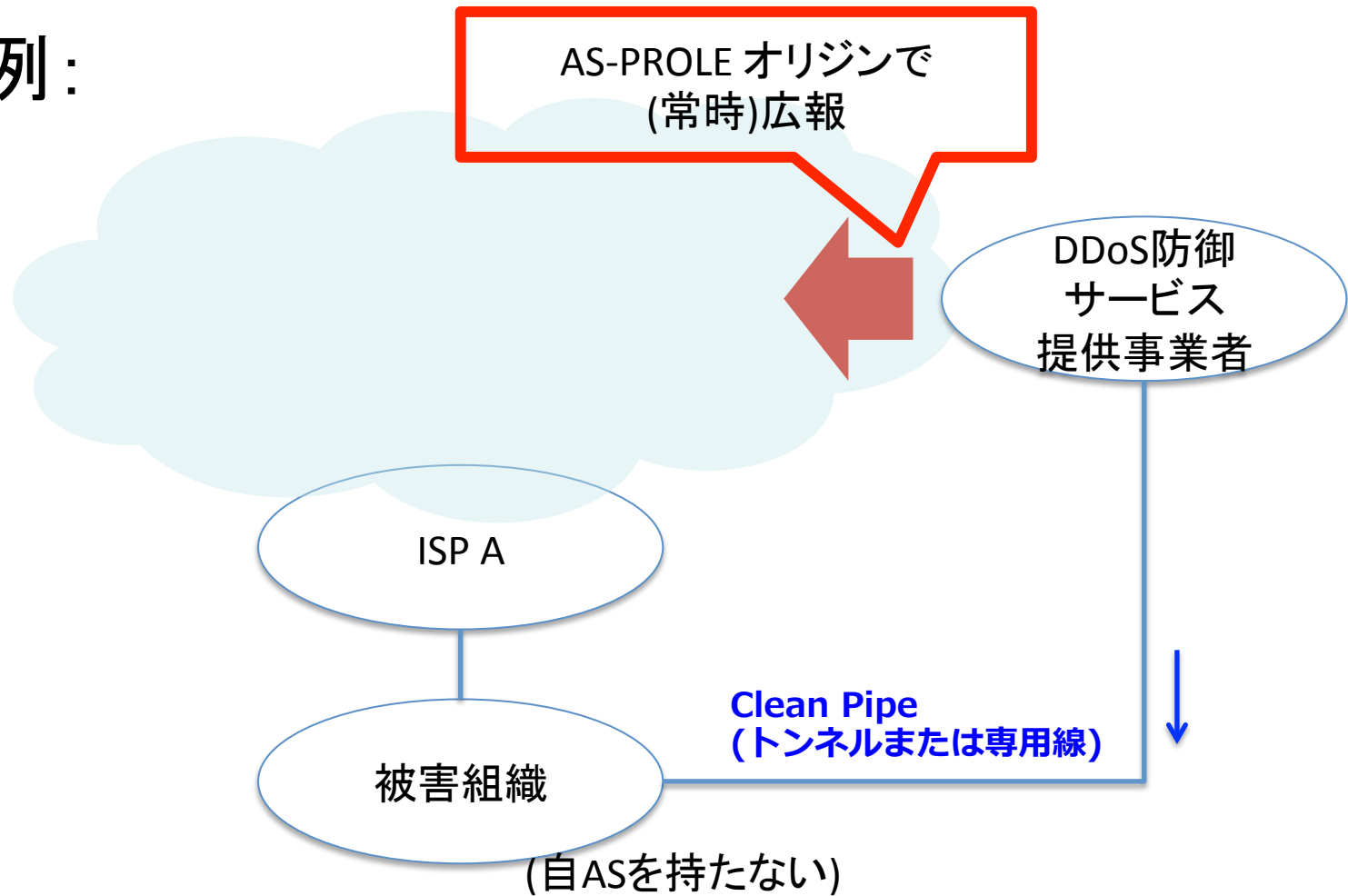


Prolexic: 1. by_prole/diff origin is_stable



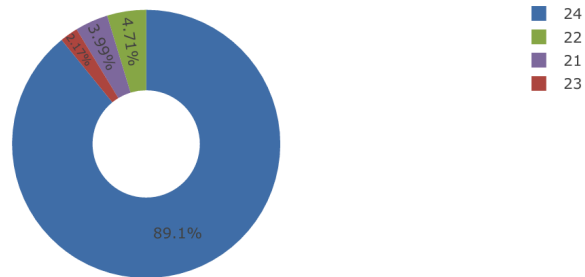
②: by_prole/same origin: 276

例:



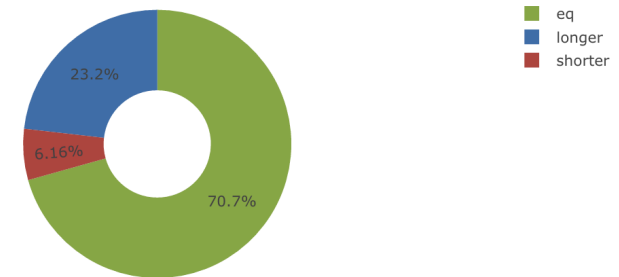
②: by_prole/same origin: 276

Prolexic: 2.by_prole/same origin prefix_len



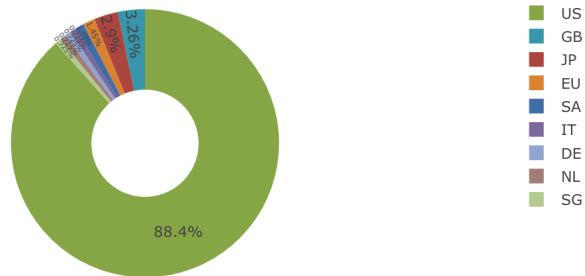
Updated: 5 hours ago

Prolexic: 2.by_prole/same origin is_longer

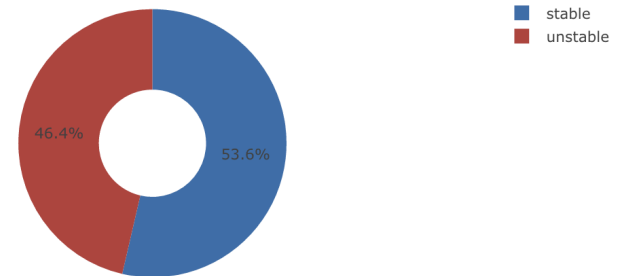


Updated: 4 hours ago

Prolexic: 2.by_prole/same origin country

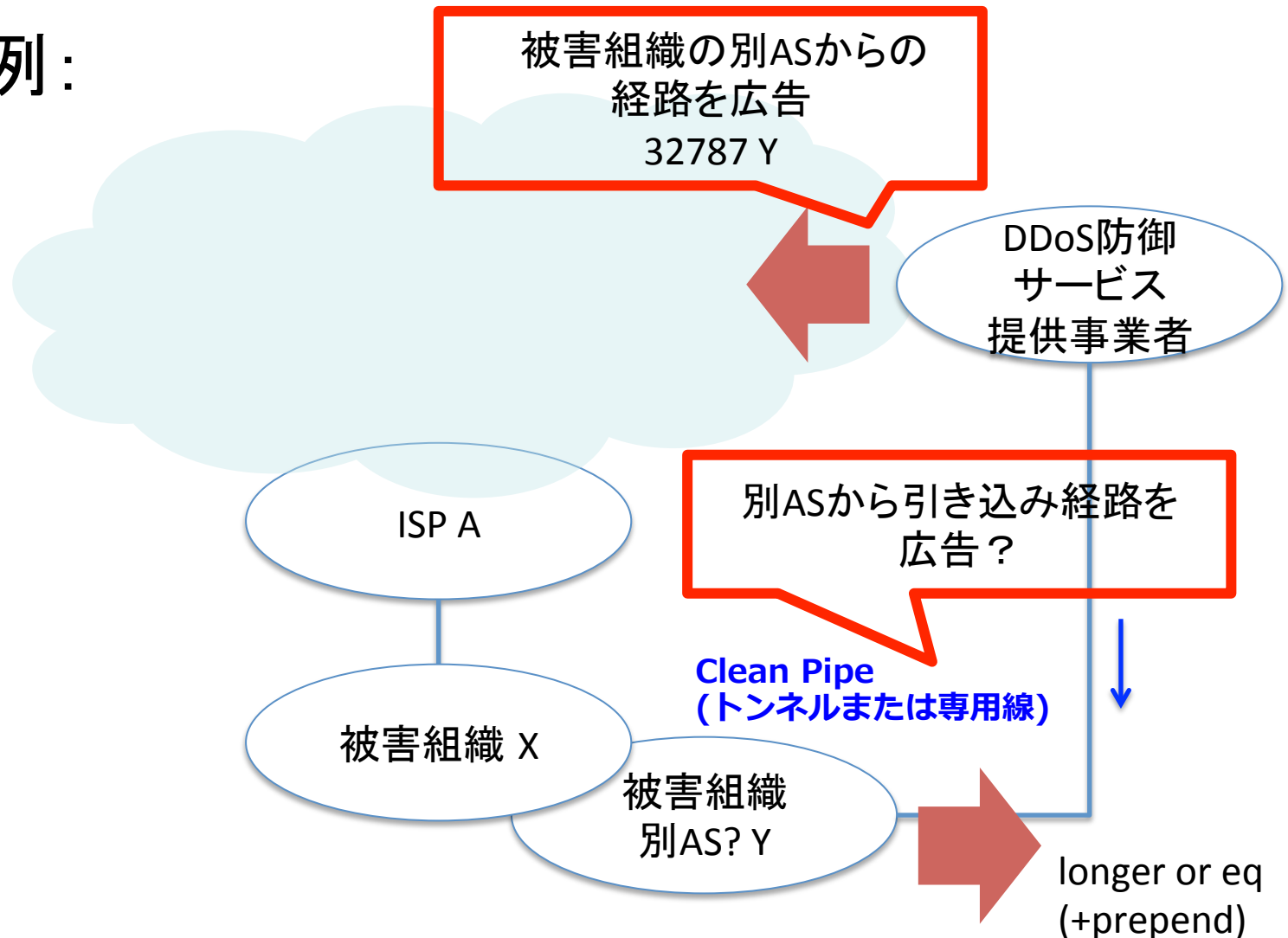


Prolexic: 2. by_prole/same origin is_stable



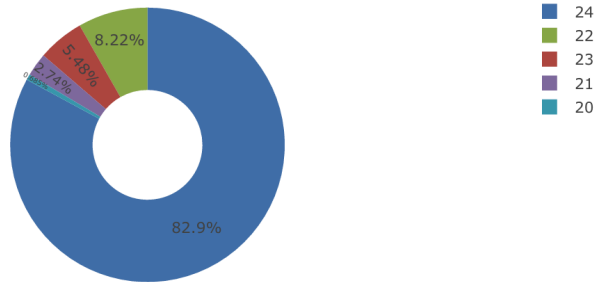
③: via_prole/diff origin: 146

例:



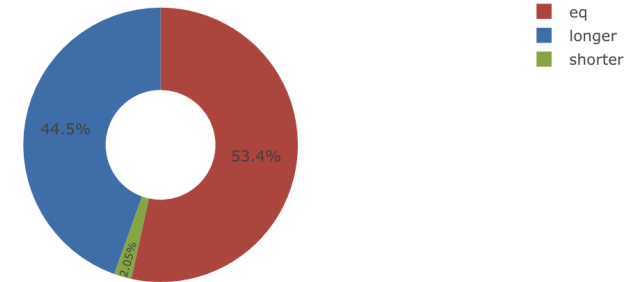
③: via_prole/diff origin: 146

Prolexic: 3.via_prole/diff origin prefix_len



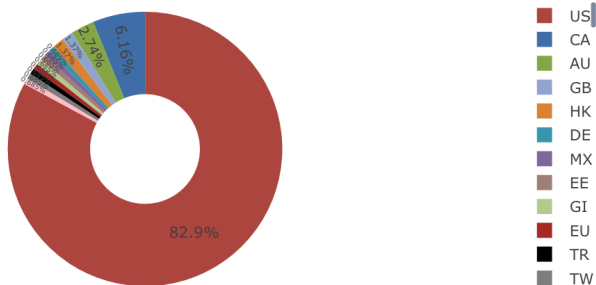
Updated: 5 hours ago

Prolexic: 3.via_prole/diff origin is_longer

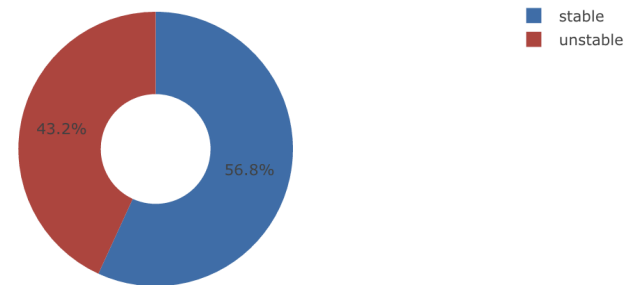


Updated: 4 hours ago

Prolexic: 3.via_prole/diff origin country

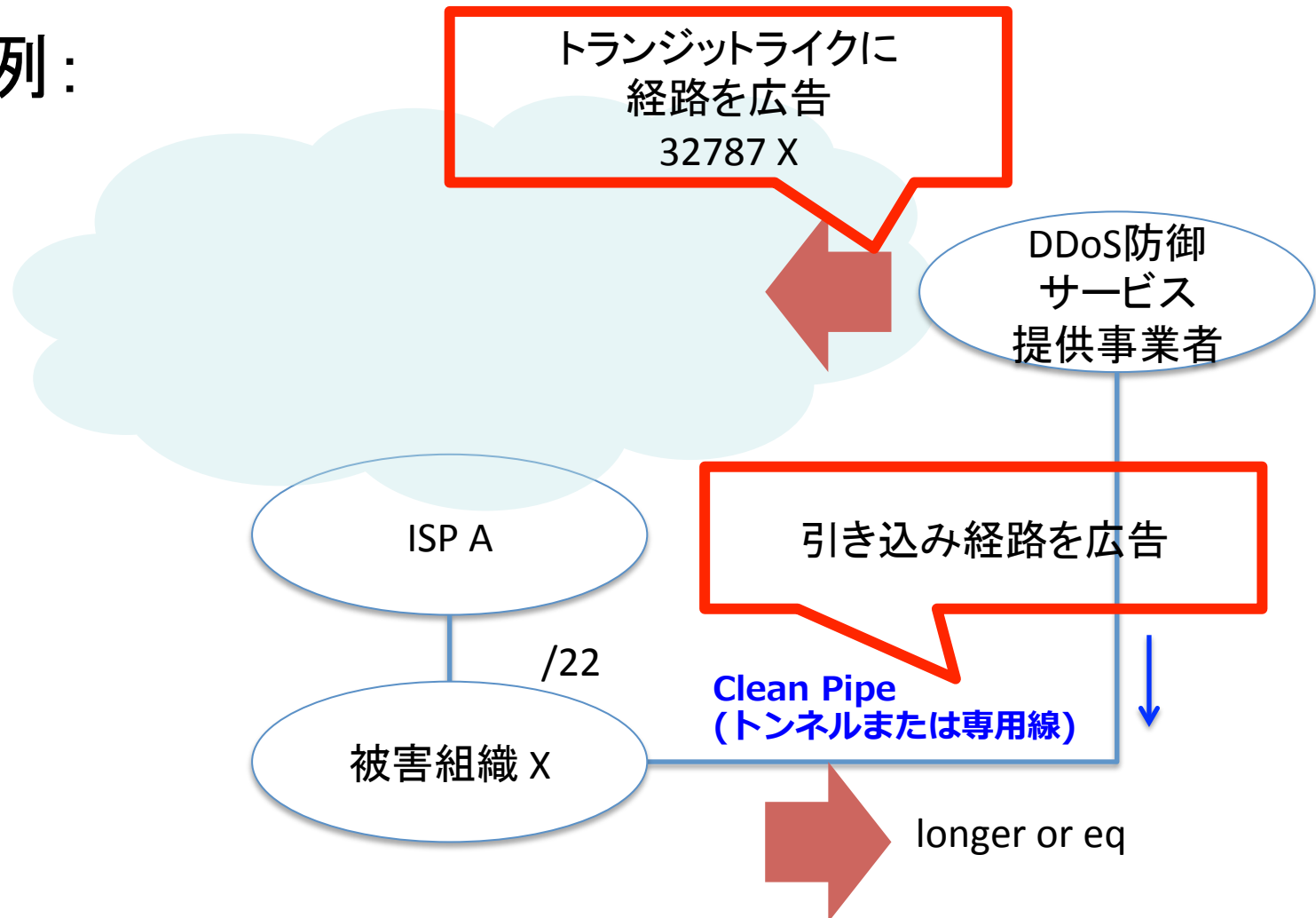


Prolexic: 3.via_prole/diff origin is_stable



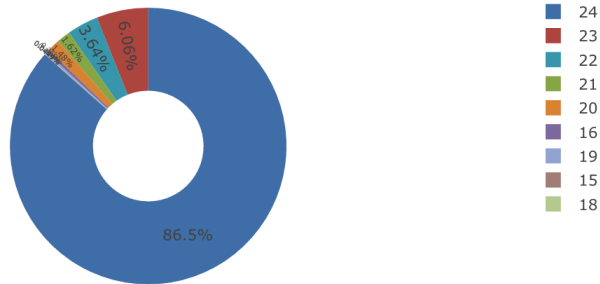
④: via_prole/same origin: 2228

例:



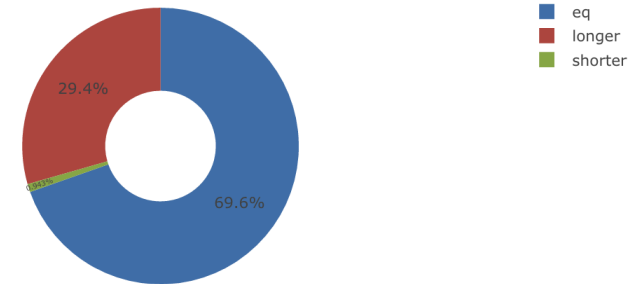
④: via_prole/same origin: 2228

Prolexic: 4.via_prole/same origin prefix_len



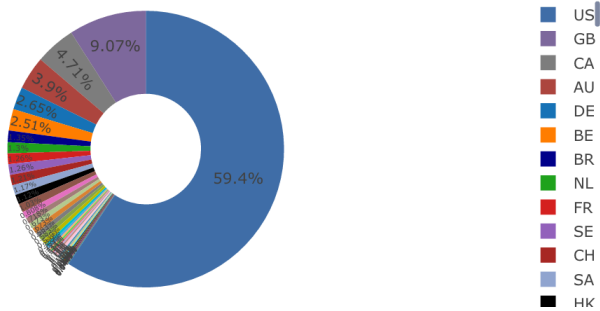
Updated: 5 hours ago

Prolexic: 4.via_prole/same origin is_longer

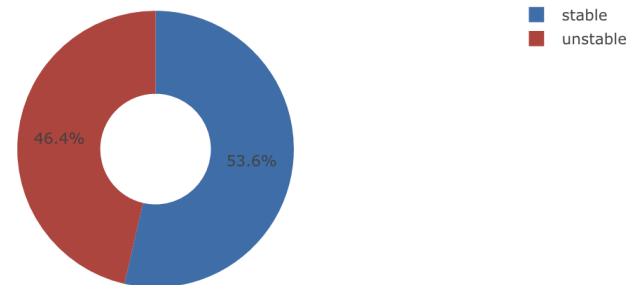


Updated: 4 hours ago

Prolexic: 4.via_prole/same origin country



Prolexic: 4. via_prole/same origin is_stable



AS-PROLE(Prolexic)解析より

- トランジットのように経路を出すケースが8割
- 一部、“hijack”に見えなくもない経路の出し方がある
 - 一時的なケースが多い

BGP引き込み手法まとめ

- 新たなトランジットの一つという見方も？
- 懸念事項
 - 引き込みによる遅延の延伸
 - longer経路のwithdraw時の経路の安定性
- (当然ですが)引き込んだ後に、
 - 攻撃トラフィックをちゃんとフィルタできるか
 - 正常トラフィックをちゃんと戻せるかをしっかりと見極めを