

New IANA allocationな IP Address利用の手引き

ご協力者の皆様と

河野誠

BBテクノロジー株式会社

松崎吉伸

株式会社インターネットイニシアティブ

水口孝則

NTTコミュニケーションズ株式会社

吉田友哉

NTTコミュニケーションズ株式会社



New IANA allocationな IP Address利用の手引き

～ 1. 悲しい編～



新しいアドレスが使えない！！

☹ RIR/NIRからのアドレス割り振り

- ★新しいアドレスブロック取得

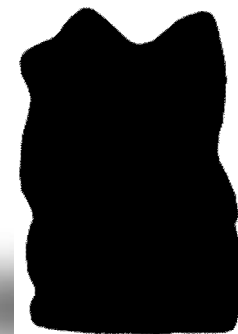
- ★経路を広告して利用開始

☹でも、なんだか通信できない！

- ★「wwwが見えません」

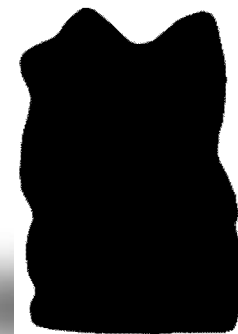
- ★「ほにやららにアクセスできません」

☹なにが起こってる？



新規アドレス利用までの簡易プロセス

- A) NIR/RIRへのアドレス申請
- B) NIR/RIRによる審議
- C) アドレス割り振り
- D) 上流ISPへのアドレスFilterの解除依頼
- E) IRRへの登録
- F) 経路広告
- G) アドレスの利用開始



通常想定される原因

☺ 上流ISPの問題

★ 経路フィルタ

- 顧客経路フィルタの設定ミス
- ピアISPへの経路広告フィルタの設定ミス
- ピアISPでのフィルタ解除依頼の誤り

★ パケットフィルタ

- 顧客用のパケットフィルタの更新ミス
- uRPFがStrickモード設定され、経路が選択されていない場合

経路フィルタ

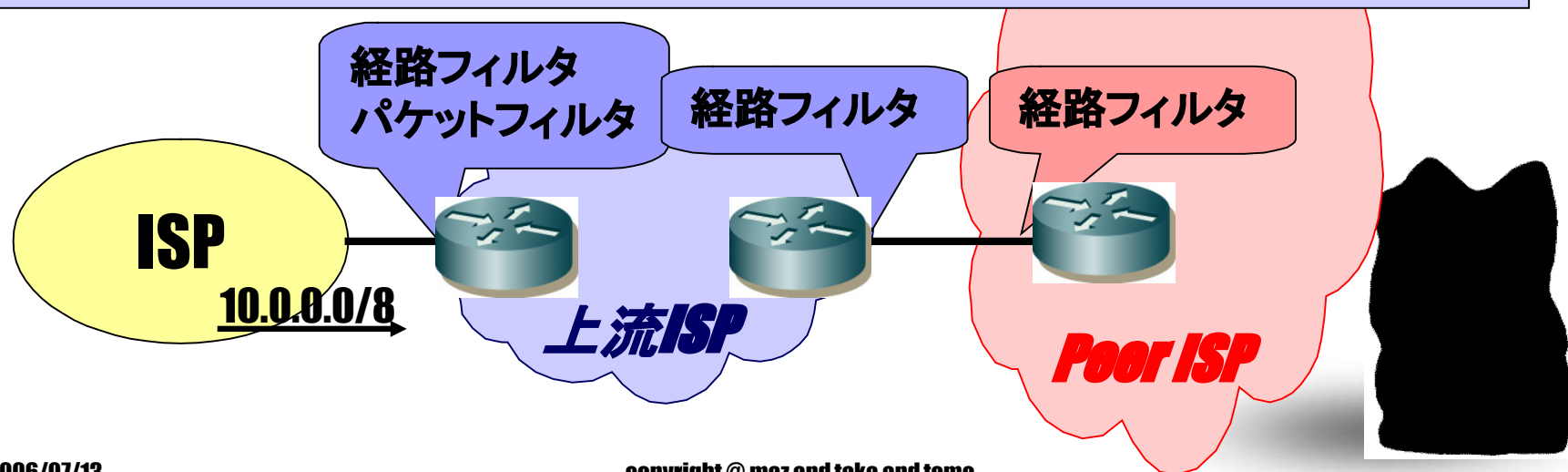
- ☺ IP Prefix
- ☺ AS-Path

生成方法

- ☺ 手動
- ☺ IRRで自動化

IRRの登録誤り

- ☺ Route
- ☺ AS-Set



障害時の状況

☯ 上流ISPでの確認

- ✳ 経路を受信している OK!
- ✳ ピアISPに広告し、相手にも到達している OK!

☯ 状況の整理

- ✳ 上流ISPは通信可能 OK!
- ✳ その他のISPでも通信可能 OK!
- ✳ 特定のサイトのみ通信できない・・・
- ✳ どの上流ISP経由でも通信できない・・・
- ✳ 特定のDNSが引けない・・・



特定箇所でのフィルタ!

☹ 経路フィルタ (AS-Path/prefix)

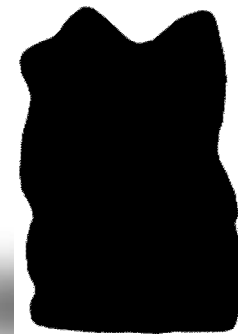
- ✳ 経路が受け取ってもらえてない
- ✳ 更新されてないBogon経路フィルタ

☹ パケットフィルタ

- ✳ パケットが受け取ってもらえてない
- ✳ ホスト単位、アプリケーション単位
- ✳ 更新されてないBogonパケットフィルタ

☹ さらに内部利用...

- ✳ プライベートアドレス代わりに使ってる
- ✳ その昔、誰かがこれで設定した



Bogonとは

- ☉ “Bogon prefix”とは本来使われないアドレス空間
- ☉ Bogonが使われる場合
 - ✳ DDoSのランダムアドレススプーフ
 - ✳ 一時的に広報して、SPAM/フィッシング/Pharmingに利用

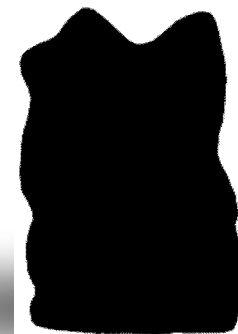
デフォルトルート	0.0.0.0/0
プライベートアドレス	10.0.0.0/8、172.16.0.0/12、192.168.0.0/16
ループバックアドレス	127.0.0.0/8
リンクローカルアドレス	169.254.0.0/16
TEST-NET	192.0.2.0/24
ベンチマークテスト	198.18.0.0/15
マルチキャストアドレス	224.0.0.0/3
IANA Reserve	

Bogonをフィルタして何が問題か？

正しいBogonのフィルタはOK!!

IANAリザーブなアドレス空間が問題

新しくIANAから割り振られた元Bogon
アドレスをフィルタしたまま！！



更新されないフィルタの原因推察

☯ 安易な実装

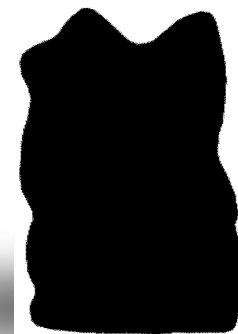
- ✳ その時はそれで良かった
- ✳ 設計者から運用者へのフィードバックがない
- ✳ 一個人による実装

☯ 継続性の無い運用

- ✳ 導入時には頑張るが、継続できてない
- ✳ セキュリティポリシーの崩壊

☯ 更新されていないtemplate

- ✳ 新しいアドレス割当に対応していない
- ✳ 古いBogonリストなどを参照



更新されていないtemplate

☯ ベンダによる設定例

★ 某社のコンフィギュレーション ガイド

– みんな注意書きを読んでもくれるかな？

Note that these ACLs might not be up to date.

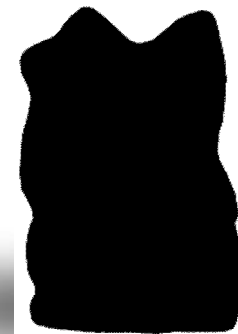
Visit IANA for update list.

☯ 有志による設定例

★ BIND, linux, cisco, juniper などなど

★ secure-template

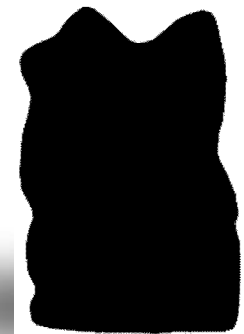
★ iptable 等アプリケーション毎の設定例



あるISPでの事例

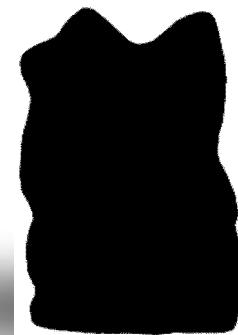
☯ 河野さん、よろしく
お願いいたします！

これから話される内容はあくまで
事実にもとづく話です。
フィクションではありません。



New IANA allocationな IP Address利用の手引き

～2. 対応編～



IANAリザーブアドレスフィルタの状況！

☯ 複数のISPでBogonとして設定している。

<http://www.ris.ripe.net/debogon/2006/07/20060709.html>

☯ 大企業のWebサーバなどでも設定されている

✳ *cnn.com*

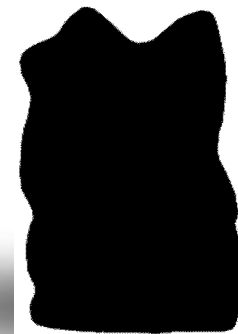
✳ *microsoft.com*

☯ フィルタの更新タイミングは？

✳ IANAのアドレス割当開始時に更新すべき

✳ マニュアルの運用では限界がある

✳ サーバは、数が多いので運用上の問題が大きい



対応時の問題点

☯ 切り分け上の問題

★ 障害箇所、影響範囲の特定が困難

- ネットワーク
- ホスト単体
- アプリケーション/ポート番号

★ フロント窓口では詳しい調査をしてもらえない

★ 修復後も原因連絡がない

☯ コントクトを持っていない

★ 直接コンタクトが必要

上流ISPはサポートとして機能する程度

★ コントクトの特定が難しい



対応時の問題点 2

☯ 能動的な障害発見が困難

- ✳ 不特定多数のISP・サーバで発生しうる・している
- ✳ 通信障害が起こるまでわからない
- ✳ 影響範囲、影響アプリが特定しづらい

☯ 対応日数

- ✳ 連絡から対応まで、数週間から数ヶ月くらい
- ✳ 間接的なため強く依頼できない
- ✳ 疎通が完全にはならないだろう…



問題発生時の対応策

☯ 問題発生箇所の管理者に対応を依頼

- ✳ サーバ、ネットワークなどの管理者
- ✳ 個別の連絡(メール、電話、Messenger?)
 - 複数の宛先へメールする
 - 電話は正しいコンタクト先を探すのが難しい
 - iNOC-DBAは便利！
- ✳ 上流ISPとの連携
 - コンタクトをサポートしてもらう



宛先の探し方

☯ ネットワーク系

- ★noc@

- ★<http://puck.nether.net/netops/nocs.cgi>

- ★IR/IRR whoisのコンタクト (tech, admin)

- ★iNOC-DBAでASの運用者に一斉同報

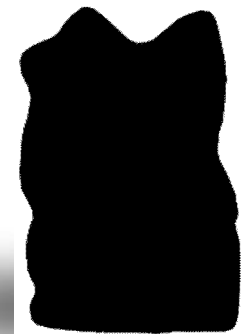
☯ コンテンツ系

- ★webmaster@, hostmaster@

☯ 友達の友達

- ★オープンなML (NANOOG等) へポストする

- ★駄目もとで上流ISPに聞いてみる



対応お願い時の工夫

☺ いくつかのパターンを問い合わせる

- ✳️ 相手の検索を手助けする

- ✳️ 異なるマスク長でフィルタしているかもしれない

例: X.0.0.0/15 – 自Prefix

X.0.0.0/8 – IANAリザーブ

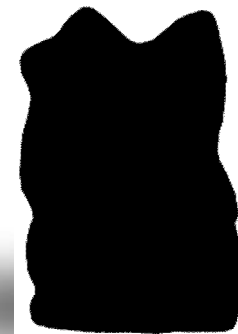
X.0.0.0/3 – ????

☺ ping/tracerouteを試せる宛先を用意

- ✳️ 他のCIDRブロック

- ✳️ route-server

- ✳️ looking-glass



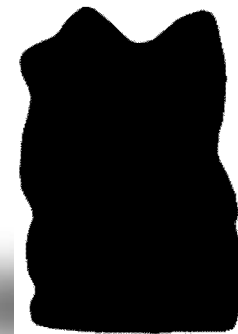
対応を素早くするために

☯ 状況を分かりやすく説明する

- ✳ 送信元、宛先
- ✳ ネットワークの疎通は？
- ✳ アプリレベルの問題か？

☯ 問題箇所を推測して連絡する

- ✳ 素早く必要な人にエスカレーションしてもらおう



RIRの対応策(例: APNIC)

- ☯️ 新規アドレスの到達性に関して問題認識有
- ☯️ 割当前に、複数の経路を広告し疎通性を確認し公開している

- ★ <http://www.ris.ripe.net/debagon/>

- ★ 最近のAPNIC, RIPE, Afrinicの経路で開始

- ☯️ 不到達の場合:

- ★ 主要 ML(*nog) への通知。

- ★ APNIC は個別に ISP へ連絡を実施することも

- # 強制力はなく、強くは押せていない

- # ARIN/RIPE は未対応



つまり

☯ 新しいアドレス空間だと届かないことがある

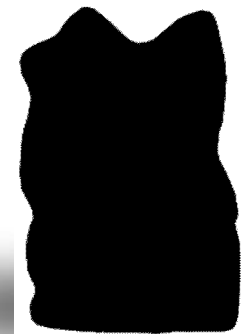
- ✳ フィルタ

- ✳ 勝手に内部利用

☯ 到達性を得るために不断の努力が必要

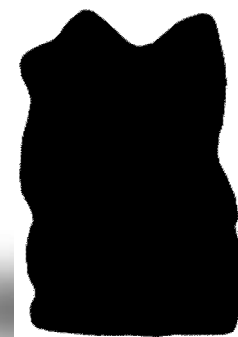
- ✳ 新規利用の周知

- ✳ 更新のためのコンタクト



New IANA allocationな IP Address利用の手引き

～ 3. 議論編～



ここでやりたいこと

☯ 対応策や事例の共有をしましょう

- ✳ 要注意箇所の共有！！
- ✳ 事前に確認した方が良くいこととか

☯ 古い文章は更新を依頼しましょう

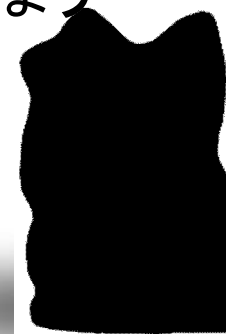
- ✳ テンプレートを使う時は注意書きを読んで
- ✳ IANAリザーブのフィルタを止める？
 - どうせIPv4リザーブはあと数年？？？
 - IPv6でやられると同じ問題がさらに大変…。

☯ 継続的な運用を

- ✳ 頑張って更新 or 自動化などの手法を検討しましょう

☯ xxNOGなどで訴えましょう

- ✳ 遠方のISPの意識は低い？？？



提案: RIR/LIRの協力

- ☯️ 新規IANA割り振りの周知の充実化
- ☯️ 新規ブロック(/8)はまず到達性を確認
 - ✳️ 経路を広報し到達性を確認できるアドレスを用意
 - ✳️ 経路の受信を確認
 - ✳️ 皆がping/tracerouteを試せる
 - ✳️ その後に割り振り開始



Bogonフィルタ会場への質問！！

☺ Bogonフィルタを設定している人！

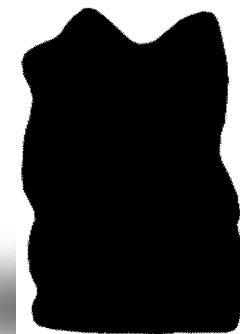
☺ IANAリザーブアドレスを設定している人！

☺ どこでしてますか？（ルータの人）

☺ その種別は？

✳ 経路フィルタ

✳ パケットフィルタ



Bogonフィルタ会場への質問！(2)

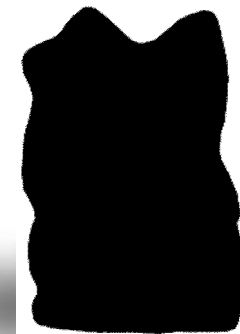
☯ どこでしてますか？(サーバの人)

☯ その種別は？

✳ サーバ単体に関するフィルタ？

✳ アプリケーション毎のフィルタ？

☯ 更新方法は？



Bogon Filterの自動化 (Bogon-RS編)

【ポイント】

- ☯ **Bogon-RSからbogon経路を受信する**
- ☯ **Bogon経路をBlackholeするように設定する**
※Bogon-RSはIANA/RIRs/NIRsと連携運用

1.0.0.0/8
2.0.0.0/8
:
169.254.0.0/16
:

①事前に特定アドレスを破棄する設定
ip route 192.0.2.1 255.255.255.255 null0



eBGP Multi-hop

Bogon経路



Bogon-RS

②受信時にNextHop変更

Recived-Route	Nexthop
1.0.0.0/8	192.0.21
2.0.0.0/8	192.0.21
:	:
169.254.0.0/16	192.0.21
:	:

Dest=bogon なパケットを破棄できる

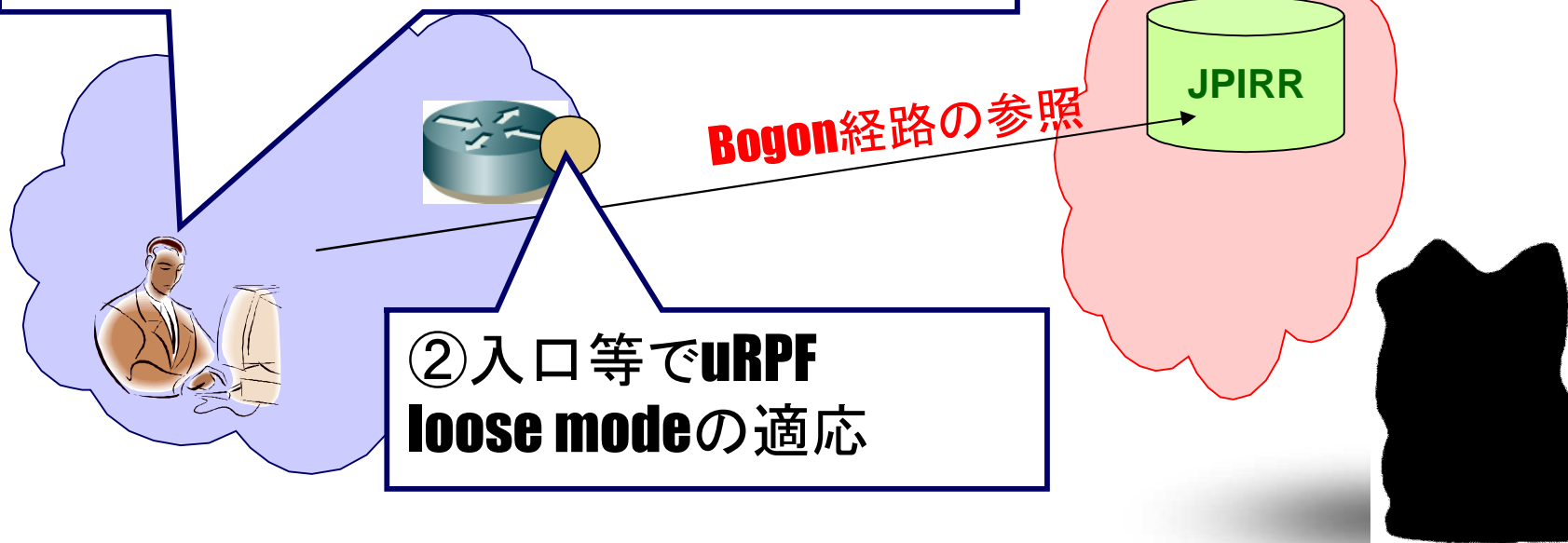
※**Src=bogon**を防ぎたい場合には、
ACL Filter or uRPF (loose)等に対処

Bogon Filterの応用 (IRR+uRPF編)

☯【ポイント】

- ☯ **経路フィルタ: IRR filter-setからがっつり生成**
- ☯ **パケットフィルタ: uRPFにまかせる**

① IRRよりbogonルート情報を取得
サーバ等が自動scriptでconfig生成



Bogon Filterの自動化 (IRR編)

☯ RIPE/RADBのFilter-setを利用

★ fltr-unallocated

IANAのIPv4未割当アドレス.

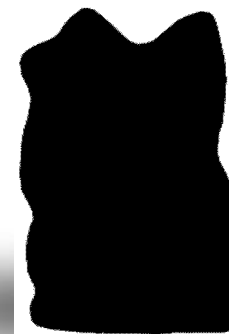
★ fltr-martian

IPv4用特定利用 (loopback、Private) アドレス.

★ fltr-bogons

上記2つの合計

☯ IRRToolSetのRtConfigを利用



Bogon Filterの自動化 (IRR編)

☺ Team CymruがFilter-set objectを更新

```
$ whois -h jpirr.nic.ad.jp fltr-martian
```

```
filter-set: fltr-martian
filter: {
  0.0.0.0/8^+ ,
  10.0.0.0/8^+ ,
  127.0.0.0/8^+ ,
  169.254.0.0/16^+ ,
  :
}
source: JPIRR
```

Source=RIPE のやつは
changed: radb@cymru.com 20040420
が若干古いですが、更新
されています。(今度言っときます)

☺ RtConfigを使ってFilter-set objectからルータの設定を作成

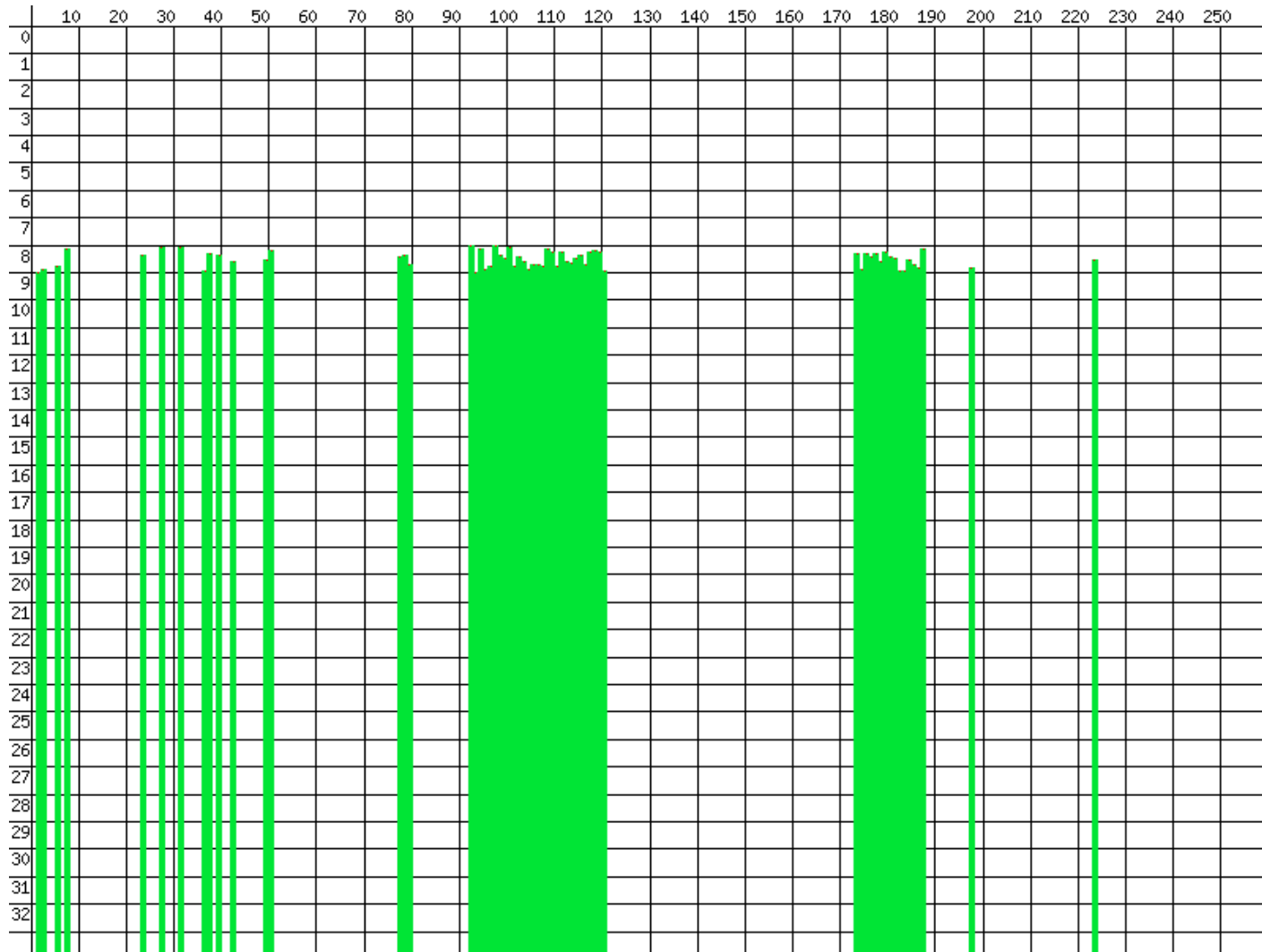
```
$ RtConfig -s JPIRR -h jpirr.nic.ad.jp
```

```
RtConfig> @RtConfig access_list filter fltr-martian
!
no access-list 100
access-list 100 permit ip 0.0.0.0 0.0.0.0 255.0.0.0 0.0.0.0
access-list 100 permit ip 10.0.0.0 0.0.0.0 255.0.0.0 0.0.0.0
:
```

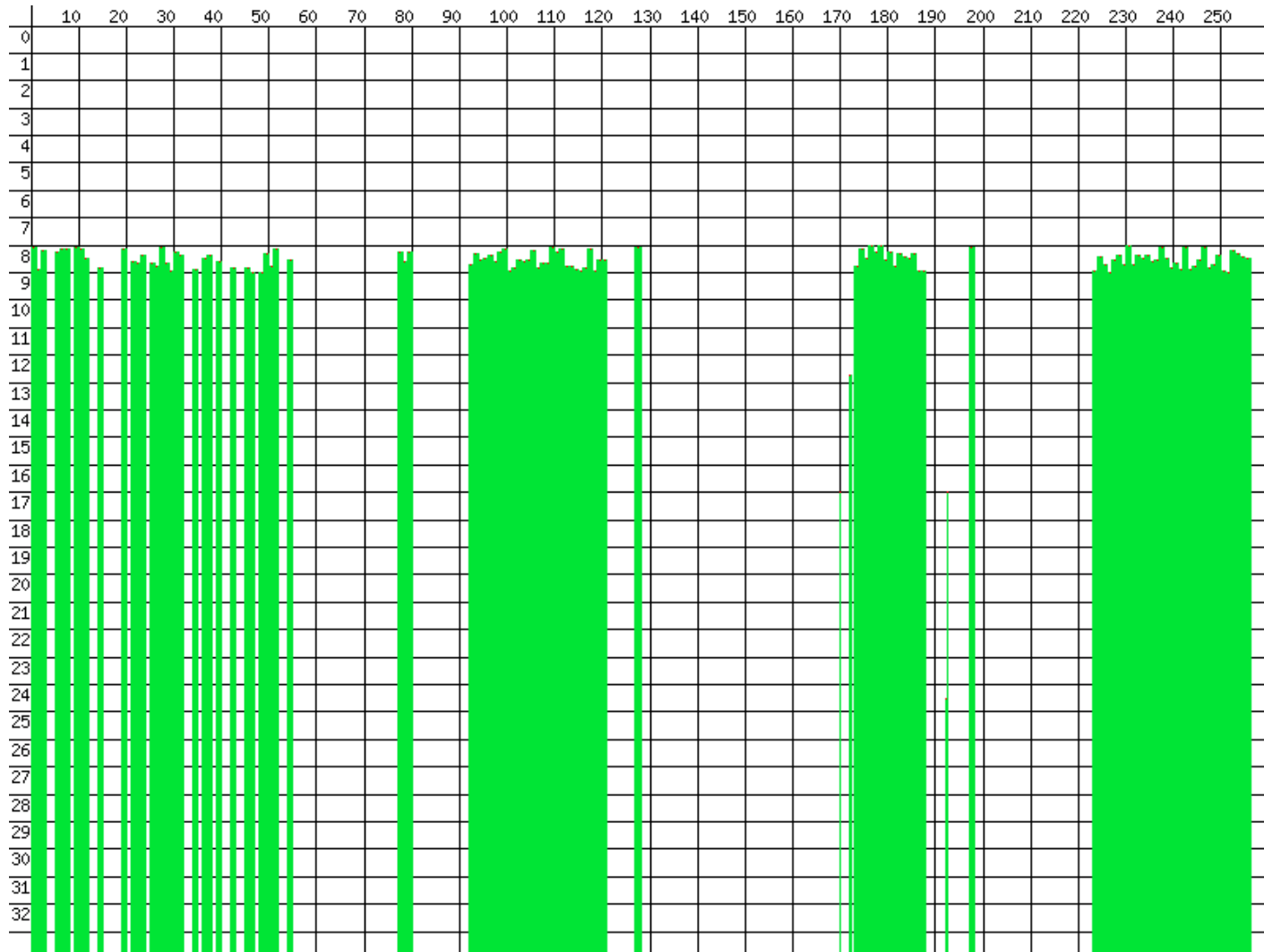
※他、Cisco prefix-list, JUNOS, NORTELなどにも対応

参照: http://www.janog.gr.jp/meeting/janog9/pdf/yoshida_janog9.pdf

Unallocated space



non (rough) advertised space



謝辞

今回の発表に際し、ご協力・ご助言頂いた
皆様にこの場をお借りしてお礼申し上げます。

NECビッグロブ株式会社

南雄一様

KDDI株式会社

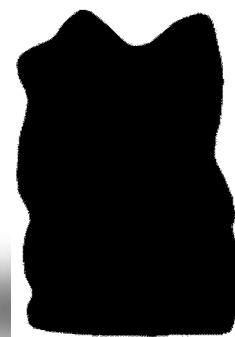
榎本啓様

富士通株式会社

中庭憲一様

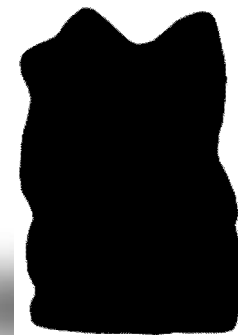


おわり



New IANA allocationな IP Address利用の手引き

～4. おまけ編～



なぜbogonをFilterするのか？

☹ DDoSの軽減

- ✳ RFC2827 – Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing

<http://www.ietf.org/rfc/rfc2827.txt>

☹ 不要な経路・トラフィックのFilterの推奨

- ✳ Team Cymru Bogon List

<http://www.cymru.com/Documents/bogon-list.html>

- ✳ RFC3704 – Ingress Filtering for Multihomed Networks

<http://www.ietf.org/rfc/rfc3704.txt>

- ✳ RFC3330 – Special-Use IPv4 Addresses

<http://www.ietf.org/rfc/rfc3330.txt>

- ✳ JANOG Comment 0001

(xSP のルータにおいて設定を推奨するフィルタの項目につ

<http://www.janog.gr.jp/doc/janog-comment/jc1001.txt>

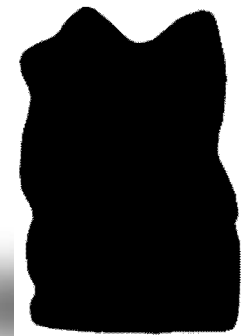


packet filterとtraceroute

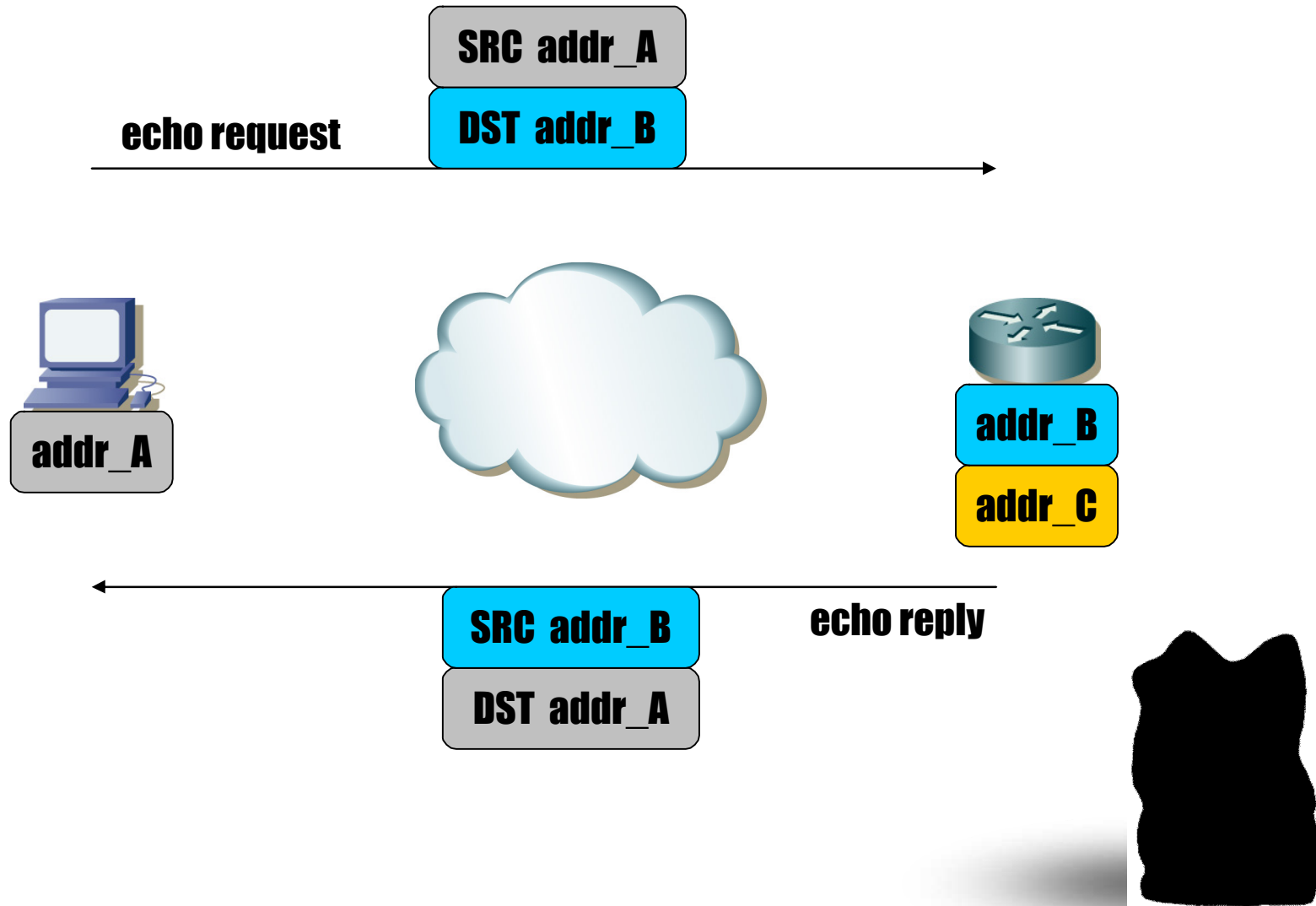
☹ packet filterとtracerouteの関係には要注意

✳ pingは届かないけどtracerouteは届く

✳ source addressが違う場合がある



ping



tracerouteだとこんな事も・・・

