



ノンサンプリングフロー分析 でBogonフィルタ対策

イツツ・コミュニケーションズ株式会社

芦田 宏之

2008年 1月



Agenda

- 自己紹介
 - 困ったこと(何が起こったのか)
 - Bogonフィルタについて(おさらい)
 - やったこと
 - まとめ
 - 議論
 - 到達性について考えてみよう
 - 場外乱闘
- 25分
ぐらい
- 20分
ぐらい
- 無制限?

困ったこと
～闘いのはじまり～

What's happen?

- IPv4アドレス追加割り振り (おかわり)
 - 2007/01: IANA⇒APNIC ... 116/8
 - 2007/03: APNIC⇒(JPNIC)⇒当社
生後3ヶ月?
- 到達性ボロボロ
- リナンバング

こ、これが噂のBogonフィルタ!?

- 通じない・使えない!

JANOG18: New IANA IPv4 allocationsなアドレス利用の手引き
資料より引用

- 利用開始までの手続きは問題なし
 - 割振り(申請/審議)～IRR登録～peerフィルタ解除～経路広告
 - でも一部のサイトにアクセスできない
 - ⇒ ネットワークにある条件のフィルタが散在
- Bogon prefix = IANA Reserved、本来未使用の空間
 - 悪用される事例多々 ...
 - DDoSのランダムアドレススプーフ
 - 一時的に広報して、SPAM/フィッシングに使用
 - IANAからRIRに割振りが行われるまではフィルタ
 - ← 割振りのアナウンスを見落とす/無視してると ...

Bogonフィルタについて少々

IANA Reserved (2007/11現在)



<http://www.iana.org/assignments/ipv4-address-space>

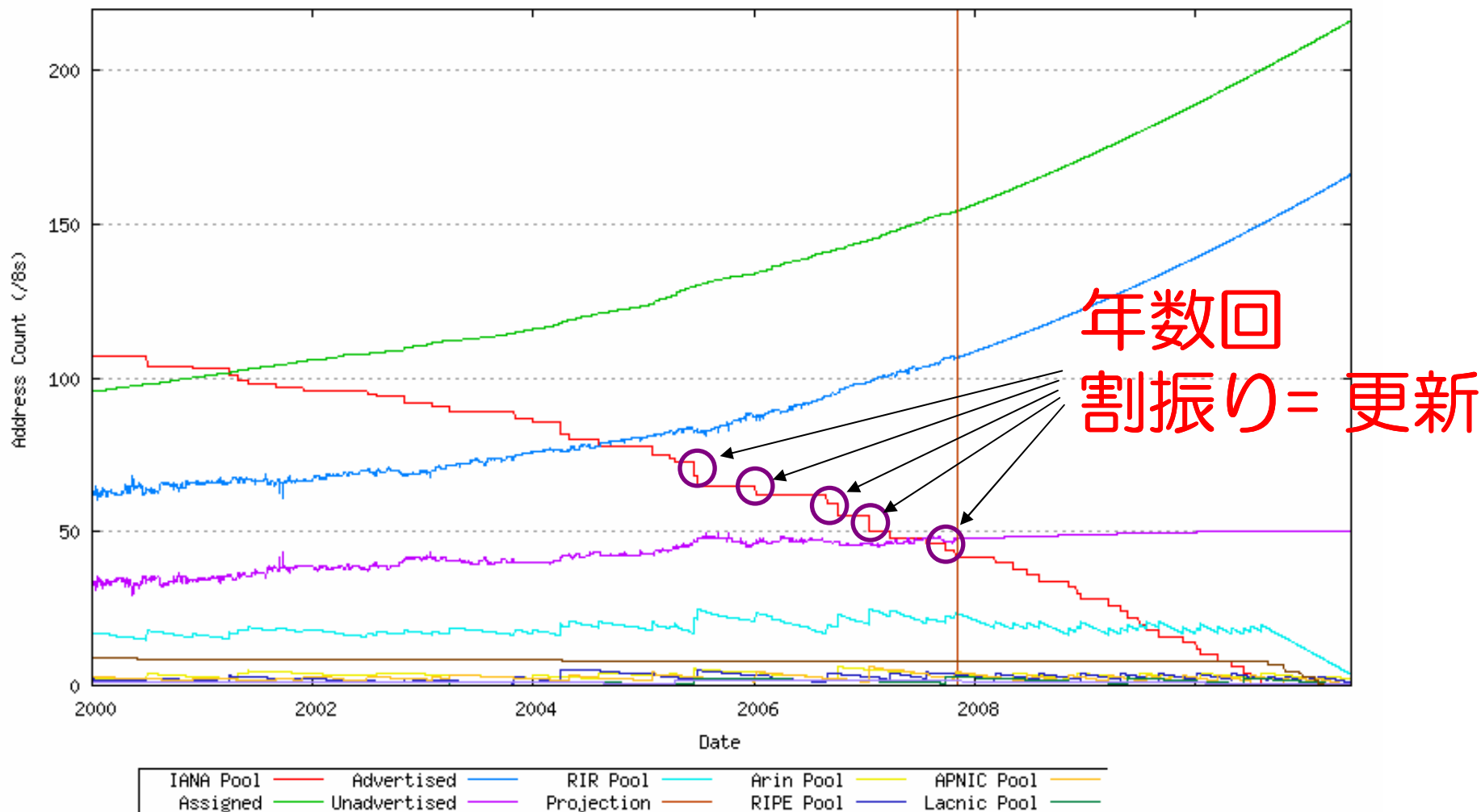
Internet Protocol v4 Address Space
(last updated 2007-10-28)

※110/8～128/8を抜粋

110/8	Sep 81	IANA - Reserved	
111/8	Sep 81	IANA - Reserved	未使用空間
112/8	Sep 81	IANA - Reserved	
113/8	Sep 81	IANA - Reserved	
114/8	Oct 07	APNIC	
115/8	Oct 07	APNIC	2007/10 割振り開始
116/8	Jan 07	APNIC	... 2007/9までは未使用空間
(中略)			
127/8	Sep 81	IANA - Reserved	See [RFC3330]
128/8	May 93	Various Registries	

“IANA Reserved” が更新される頻度

<http://www.potaroo.net/tools/ipv4/>



Bogonフィルタ書いちゃ悪いの？

- 正しいフィルタは有効(予防保全,etc)

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

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

- **問題: 更新された情報に追従していない**

- 安直or緊急に設定 ... 設定の背景や意図が後世へ残りにくい
- テンプレートを更新しない、古い情報を参照
- 現場の実情
 - サーバ屋 vs ネットワーク屋
 - Routerで通してもFirewallで閉めてる
 - アンテナの指向性違う(~NOGって何?)
 - ド忘れ、担当者焦げ付き
 - クレーム来たら対応すればいいじゃん♪

でも ... Bogonフィルタ痛い

- 顧客間で接続性に差が生じる
 - 同一顧客でもある日突然接続性が悪くなる
 - 動的アドレス割り当て
- ⇒ 顧客(利用者)にとっては一方的な品質低下、不利益
- ISPが責任を持ってない範囲で問題が発生
 - フィルタ解除してもらわないと解消しない
 - 長期化: 解決までに長時間を要する
 - 連絡から対応まで数週間～数ヶ月かかるケースも
 - 国内外問わず発生
 - 能動的に発見することが困難
 - どこで起こるか、障害があるまで分からない
 - 影響範囲、アプリケーションによる違い(MailO、WebX)

これまでの議論や動向(1/2)

- JANOG18@有明 2006/07
 - New IANA IPv4 allocationなアドレス利用の手引き
 - 河野さん、松崎さん、水口さん、吉田さんによるセッション
 - 事例紹介
 - フィルタされる理由、問題点
 - 対応事例
 - 情報共有と注意喚起
 - フィルタ自動化方法やその事例
- Bogonフィルタへの対応
 - アクセスできなかったらadmin-c/tech-cへひたすら連絡
 - 周知活動、啓蒙活動、フィルタ自動化

これまでの議論や動向(2/2)

- RIRによる確認、エージング
 - APNIC Debogon Project
 - RIPE/NCC: De-Bogonising New Address Blocks
<http://www.ris.ripe.net/debogon/>

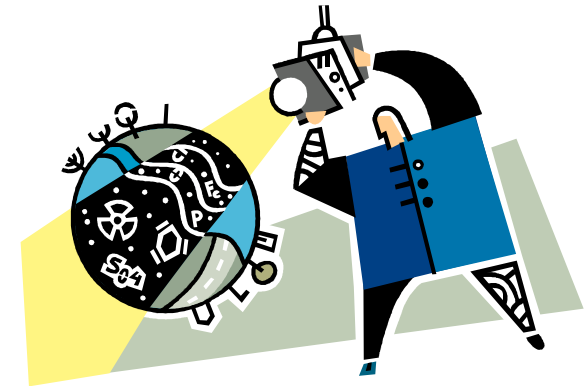
IPv4

AS Number	41.223.236.0 /22	95.192.0.0 /16	95.255.248.0 /21	186.128.0.0 /16	186.127.248.0 /21	114.0.0.0 /24	114.50.0.0 /21	114.200.0.0 /19	114.255.0.0 /16	115.0.0.0 /24	115.50.0.0 /21	115.200.0.0 /19	115.255.0.0 /16
286	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
513	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
1103	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
1221	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
1273	✓	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗
1280	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
1299	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
1853	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
1916	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
1930	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗

- Paper (SIGCOMM 2007)
 - Testing the reachability of (new) address space, Randy Bush 他

このへんからようやく本題ですが...

- このプログラムでは...
 - フィルタ解除(発見)のために何をしたか
 - 到達性の確認と確保



- フォーカスしないこと

- “通信の秘密” 問題

☆正当業務行為として確認 (総務省,会社)

帯広で紹介されたプロトコルに沿って霞ヶ関へ!

Ref. つぶらな瞳?で総務省 (JANOG20)

<http://www.janog.gr.jp/meeting/janog20/pg-soumu.html>

- フィルタ自動化の話題

- JANOG18で詳しく紹介されてます

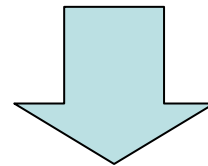
あくまで“時間の都合上” です
ご理解ください



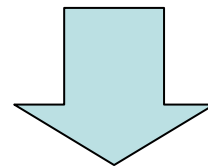
やったこと
～拳^H検討と格闘～

当時の状況

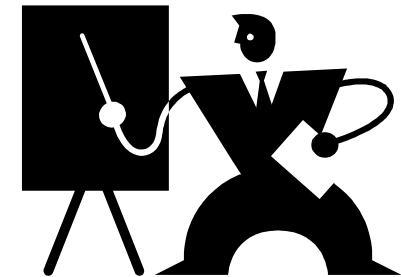
- 生後3ヶ月のprefixを早く一人前にしなきゃ
 - このままでは割当てられない
 - 割当てするために割振り受けた



- 到達性を自分で検査してひたすら解除(依頼)



- “人並みになりましたよ” と説明しなきゃ
 - 定性的に
 - 可能な限り検査&解除本来の意味?でベストエフォート



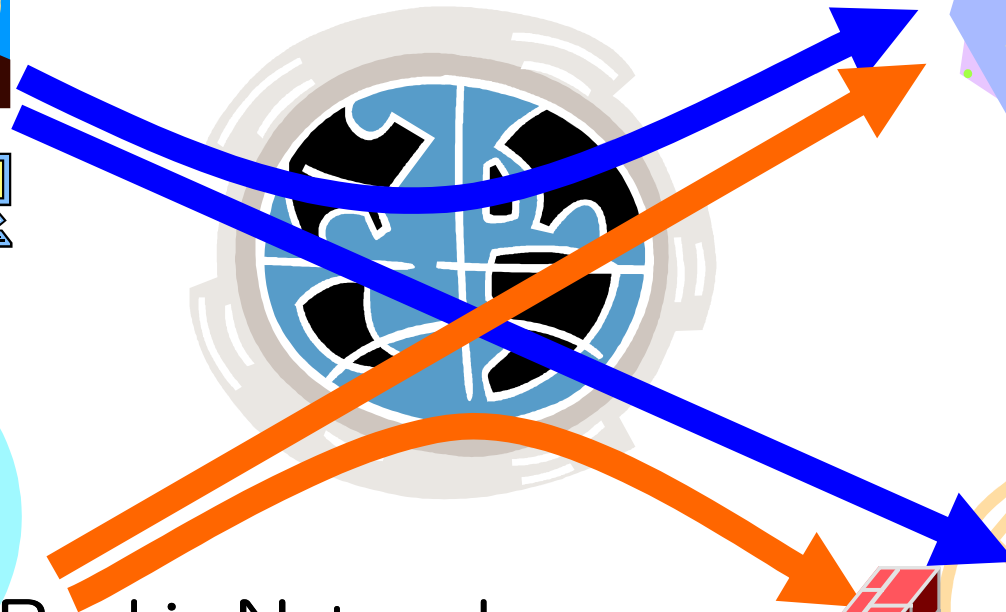
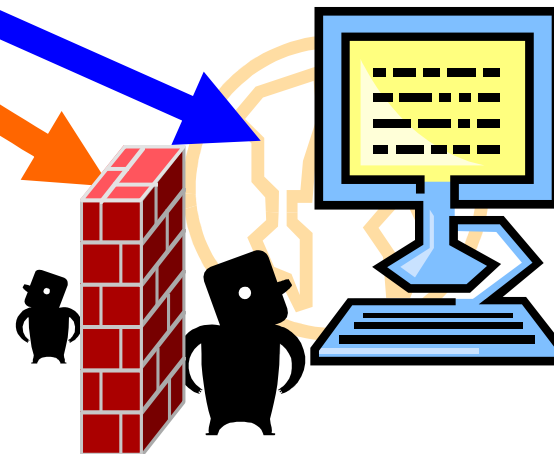
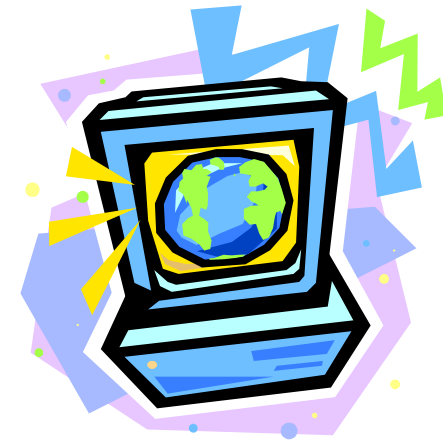
ようは



Senior Network



Rookie Network



確認にあたっての課題(1/2)

pingでいいんですか?

ホントは使えてるのにNG判定

		ICMP (ping)	
TCP/UDP (アプリ)	○	○	×
	×		

ホントは使えてないのにOK判定

確認にあたっての課題(2/2)

- ネット広すぎ
 - 端から端までやっちゃただの port scan
- どこへ?: サイトによってインパクト違う
- お客様がよく使っているところは?
 - 重要性≠トラフィック量
 - “見えなきゃ痛い” 順

“アクセス”が多いサイトを重く見る

- 沢山のユーザがアクセスするサイト
- 特定のユーザが何回もアクセス

IPアドレス+ポート番号に重み付け

- 重み = アクセス回数
- 同じユーザが1時間以内(NN:00~NN:59)に同一サイトへ何回アクセスしても1カウント
- TCP establish できればOK

試行方針と接続性の数値化(2/2)



[重み]	[IPaddr:Port]	[Senior]	[Rookie]	[点数]
1000:	A.A.A.A:NN	⇒ OK	⇒ OK	1000
200:	B.B.B.B:NN	⇒ OK	⇒ NG	0
50:	C.C.C.C:NN	⇒ OK	⇒ OK	50
10:	D.D.D.D:NN	⇒ NG		

満点=1250点

得点=1050点

接続性: $1050 / 1250 = 84\%$

どーやってカウントします？

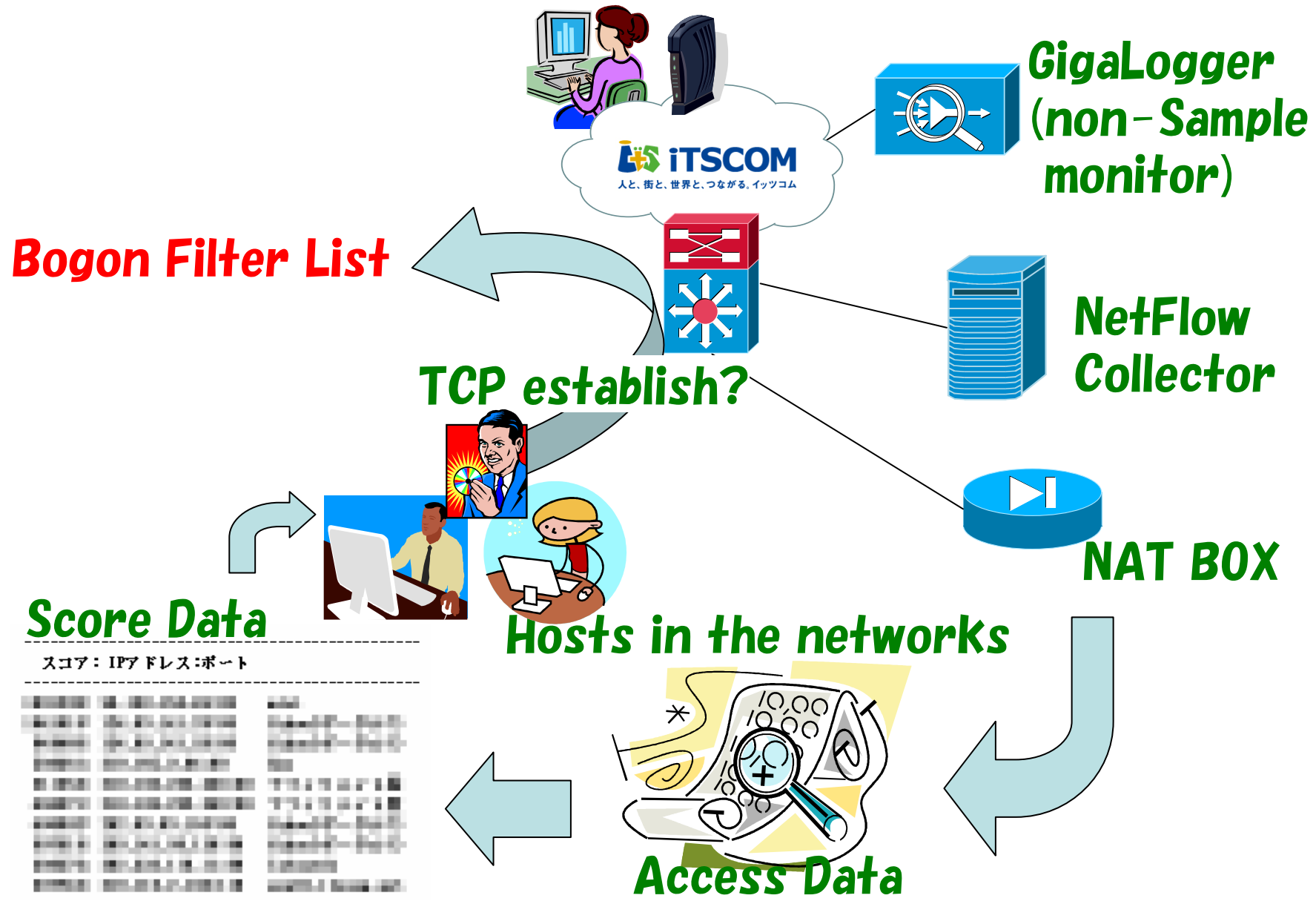
ユーザトラフィックのセッション情報記録

TCP: FIN+ACKがあったら1本

UDP: ペイロード見る必要あり(断念)

- NAT log
- Sampling (NetFlow) パケットモニタ
 - TCP_FLAG取ってるのでフィルタ書いて抽出
- Non-sampling パケットモニタ
 - 全パケットの中から条件に合うものを抽出

評価の流れ



数字で見るBogonフィルタ



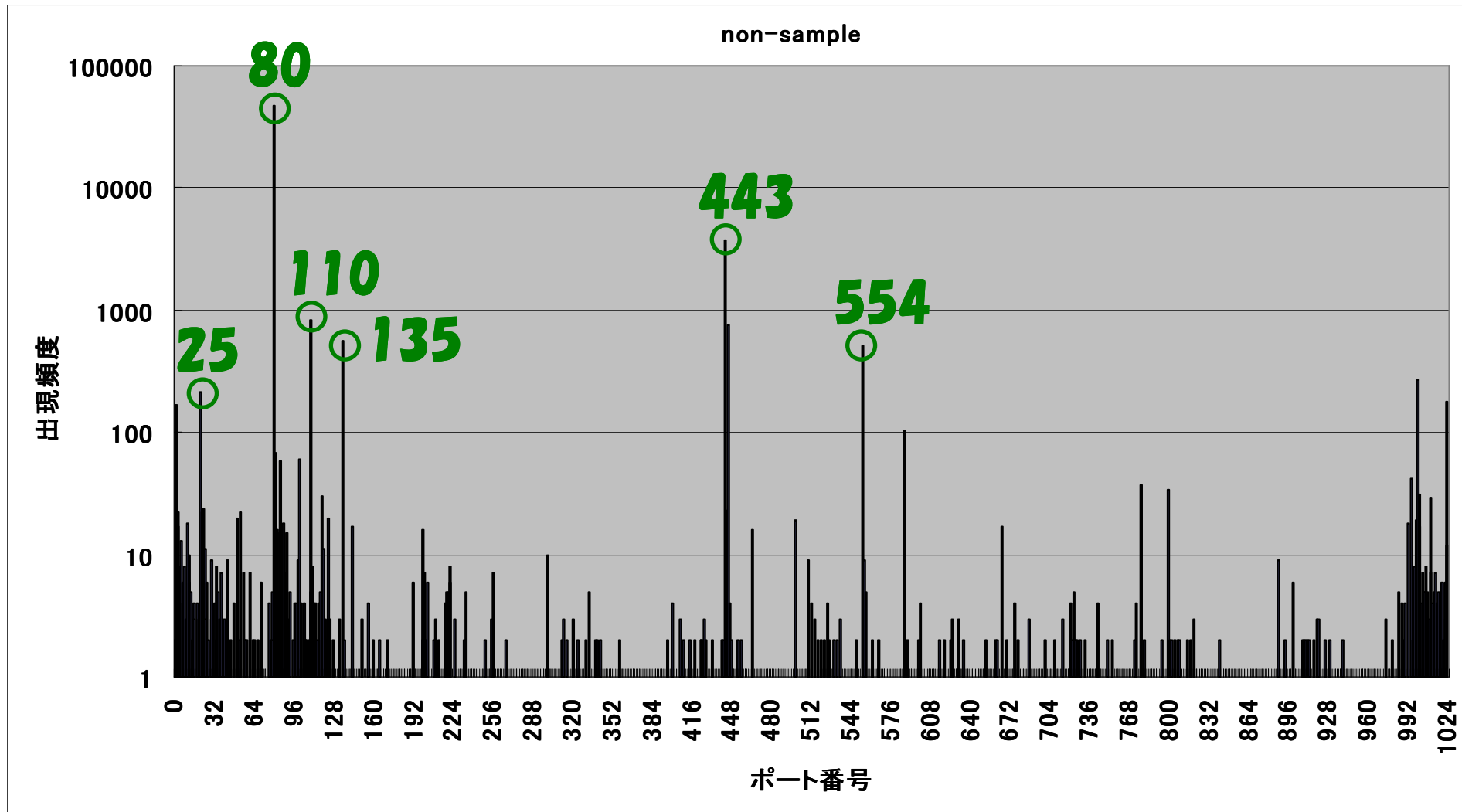
ホスト数: 333

(TCP通らないけどpingOKだった=74/333)

ORIGIN AS: 92

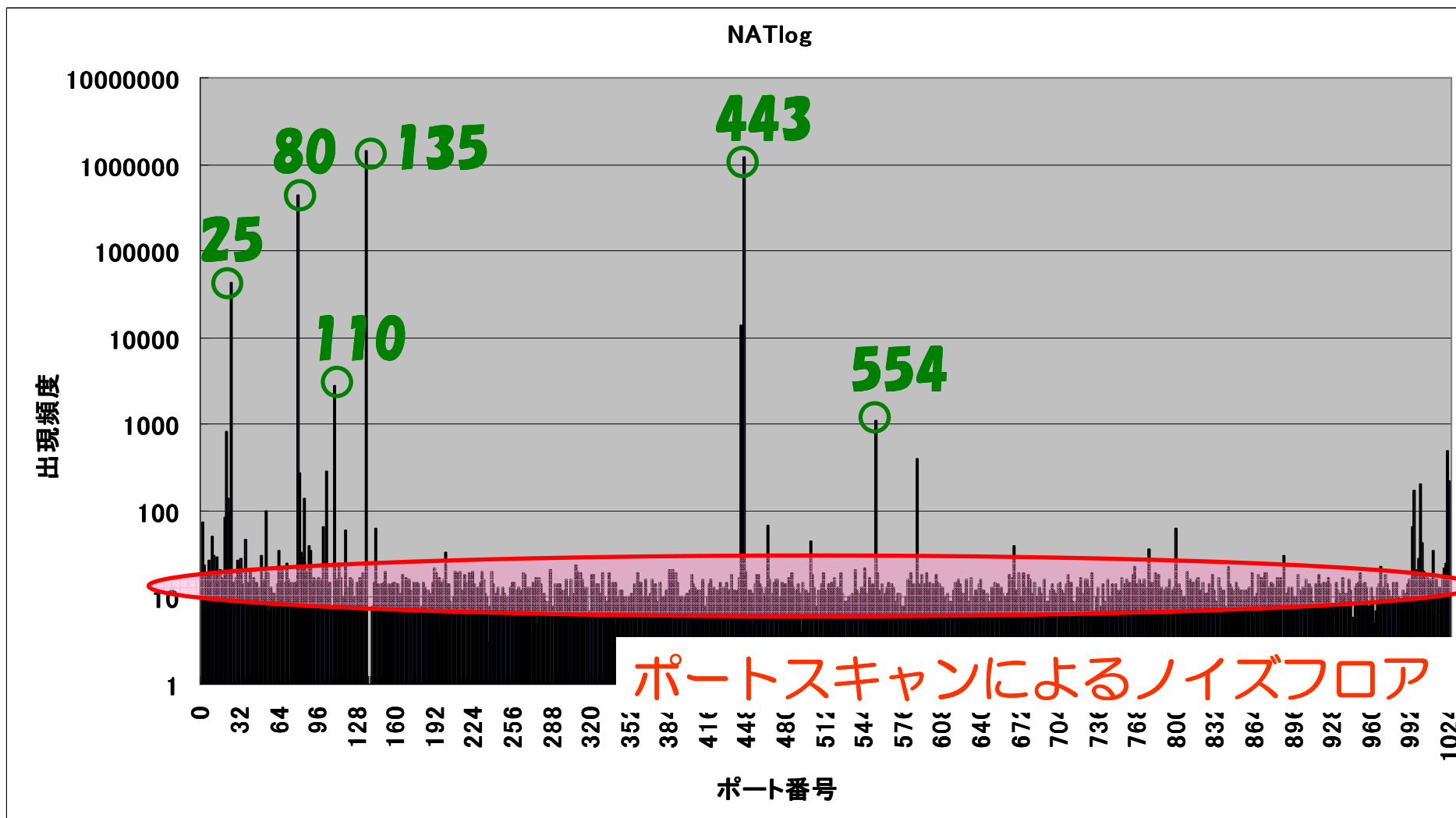
ルーキーprefixの接続性(得点%) = 98.79%

ポート数分布(non-sample, 1~1024)



ポート数分布(NAT, 1~1024)

未成立コネクションもコミコミ



各方式の比較

	NAT log	NetFlow	Non-sample
雑音	多い 除去大変	TCP_FLAG 見て除去	任意フィルタ 可能
ランク傾向	あまり変わらず		
HDD容量/day	とても沢山	我慢できる	NetFlowより少ない
検知実績		-	NetFlowの約5倍
全数検査?	商品依存	抜き取り	全数

要件

- 雑音少ないこと
 - ノイズ除去に恣意的操作必要
 - 処理を定型化したい
- ストレージに優しいこと
- 検知精度 (漏れちゃダメ)



ここまでのまとめ

- 若いprefix&Bogonフィルタに悩まされる
- お客様より先にフィルタ発見したい！！
 - コスト(手間+時間)パフォーマンス最適化
- フロー分析して重み付けして接続試験
 - NAT log, NetFlow, non-sample

⇒ 成果あり

⇒ 検知精度(最重要)で non-sample



あんなこと、こんなこと

- establishしてもダメなケース
 - メールサーバとか



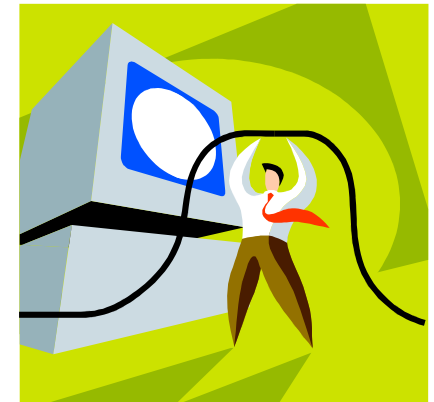
- UDPに挑戦?
 - DNS引ける/引けないは大きい
 - TCPみたいに3wayハンドシェイクで判断できない
 - 成立してるかどうかは応答見なきゃ
 - non-samplingキャプチャ必須



フィルタと到達性 ～議論編～

結局何をしたのか？

- 到達性の確認、確保
 - 通じる？ 通じない？
 - 通じなかったら通じるまで頑張る
... 先方が開通作業するまで通じない

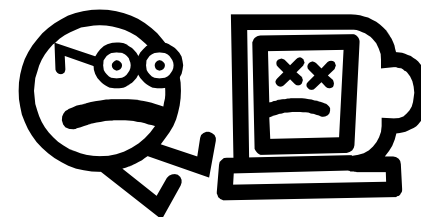


- 次から次へと
 - 確認しても問い合わせゼロにならず
 - 生後1年経っても通じないところ有り
- フィルタ自動化以外にも...
 - アプリフィルタ⇒TCPの確認必須？
 - サーバオペレータへのリーチ

会場の皆さんに質問(1)

Q. 到達性の確認って
必要だと思いますか? やらうと思いますか?

- IPv6 ホワイトリストで書いてる?
- IPv4 枯渇⇒再割り振り(前オーナーのお行儀)
 - 自分で書いたフィルタにrejectされる?
- クラスフル(/8,/16,/24)でフィルタされて巻き添え
- 4byteASで広報したときの到達性
 - バグをきっかけにフィルタ広まる



... 確認しなくちゃいけない状況広がってそう

会場の皆さんに質問(2)

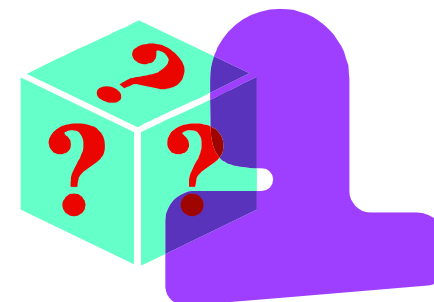
Q. Bogonフィルタをプリセットしてる
ディストリビューションorツール知りませんか?

- NGサイトでCentOSなapacheよく見かける
 - 単にシェア高いから?
- shorewall プロジェクト
- その筋のサーバ上げるテンプレ
追従してない?、更新遅い?

個人サーバでリーチできずに開通に苦勞

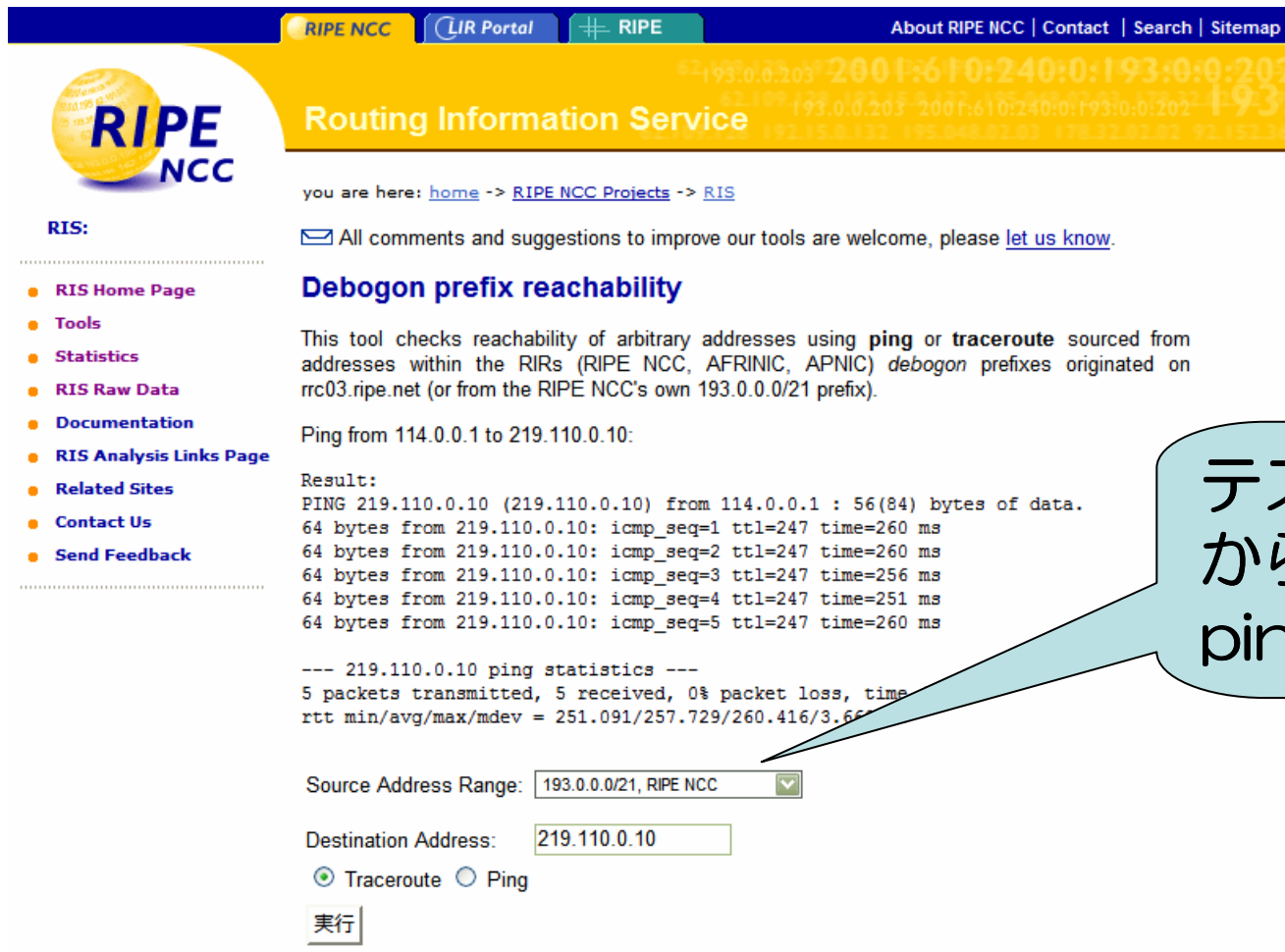
Q. サーバオペレータさんへ情報届けるために
良い連絡先は?

- 今は**NOGに偏ってるような ...
- 業種、業界に分散?



LIRによる確認

JANOG18以降の成果 ... (NTT.com吉田さん提案) <http://www.ris.ripe.net/cgi-bin/debogon.cgi>



The screenshot shows the RIPE NCC Routing Information Service (RIS) website. The page title is "Routing Information Service". The navigation bar includes "RIPE NCC", "LIR Portal", "RIPE", "About RIPE NCC", "Contact", "Search", and "Sitemap". The main content area is titled "Debogon prefix reachability" and describes the tool's function: "This tool checks reachability of arbitrary addresses using ping or traceroute sourced from addresses within the RIRs (RIPE NCC, AFRINIC, APNIC) debogon prefixes originated on rc03.ripe.net (or from the RIPE NCC's own 193.0.0.0/21 prefix)." The interface shows a "Ping from 114.0.0.1 to 219.110.0.10:" result with the following output:

```
Result:
PING 219.110.0.10 (219.110.0.10) from 114.0.0.1 : 56(84) bytes of data.
64 bytes from 219.110.0.10: icmp_seq=1 ttl=247 time=260 ms
64 bytes from 219.110.0.10: icmp_seq=2 ttl=247 time=260 ms
64 bytes from 219.110.0.10: icmp_seq=3 ttl=247 time=256 ms
64 bytes from 219.110.0.10: icmp_seq=4 ttl=247 time=251 ms
64 bytes from 219.110.0.10: icmp_seq=5 ttl=247 time=260 ms

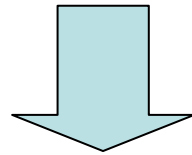
--- 219.110.0.10 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time
rtt min/avg/max/mdev = 251.091/257.729/260.416/3.65 ms
```

The interface also includes a "Source Address Range" dropdown menu set to "193.0.0.0/21, RIPE NCC", a "Destination Address" input field containing "219.110.0.10", radio buttons for "Traceroute" (selected) and "Ping", and an "実行" (Execute) button.

テストネットワーク
から任意の宛先へ
ping&traceroute

LIRによる確認をもっと実用的に(案)

- 確認したい先 ... いっぱい
- ping, traceroute => TCPでも試したい



RIPE/NCC debogonツールを拡張

- 接続先リスト(IPaddr:port)をUPLOAD
- 確認した結果を返送

⇒おかわりする前にISP自身で
アプリレベルの到達性を確認

※悪用されると攻撃ツールになるので
LIR限定、要認証?

謝辞



今回の発表にあたり、ご助力・ご助言いただいた皆様に心より御礼申し上げます。

- 道を開いてくれた Flow Inspection Project の皆様
- 総務省 電気通信事業部 の皆様
- 漢らしい箱をありがとう u10Networks 様
VIVA! GigaLogger1000
- JANOG21 ミーティングスタッフの皆様
- フィルタ解除に応じて下さったオペレータの皆様

会場の皆様、JANOGERの皆様