JANOG18 ミーティング
『2006年版 ISPのトラフィック こんな状況です』
地域密着型アクセス系編

ベライゾン ビジネス
伊賀野康生

株式会社富士通ソフトウェアテクノロジーズ
村松正浩

自己紹介

伊賀野康生 (ベライゾン ビジネス)

1999年よりIPサービスのお客様向け技術支援をさせて頂いています。最近は、一般法人様のクローズドなグローバルIPネットワークで気軽にNetFlowが使えないか画策中です。

村松正浩 (株式会社富士通ソフトウェアテクノロジーズ)

某地域ISPにて、ネットワーク関連全般の仕事をしております。2003年6月より、ASを取得してBGPによる運用を開始しました。

トラフィック調査のきっかけは・・・

村松　「上位トランジットのトラフィックバランシングが思うようにいかないんですけど、どうしたらいいですかね？プリペンドとか、いろいろ試みたのですが・・・」

伊賀野「なんか、全然、プリペンドが効いてませんね。どんなトラフィックがどこから流れているか、調べてみましょうか？」

とりあえず、１週間のデータの採取

- cflowdによるNetFlowデータの収集
- bgpviewによるBGP経路のUpdateの収集

この発表の趣旨・目的は？

- 当初の目的はトラフィックコントロール ⇒ これは実現

【今回の調査のポイント】

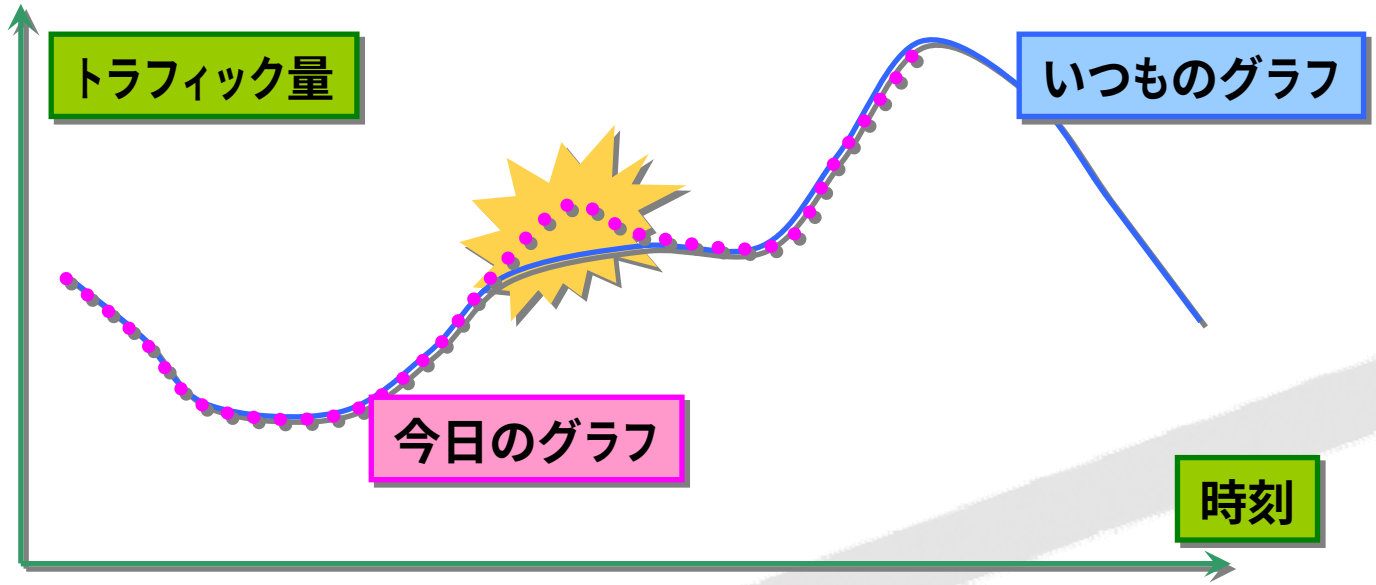
1. そもそも・・・トラフィックってどこから、どれくらい流れているものなの？

2. 地域ISPのトラフィックって、大手ISPさんと違うものなの？

Section 1
トラフィックデータ収集と分析方法について

verizon business

ある土管のグラフを見て



- なんか急にトラフィック増えた（減った）なぁ
- これなんのトラフィックやろ？
  - オペレータとしての素朴な疑問

verizon business

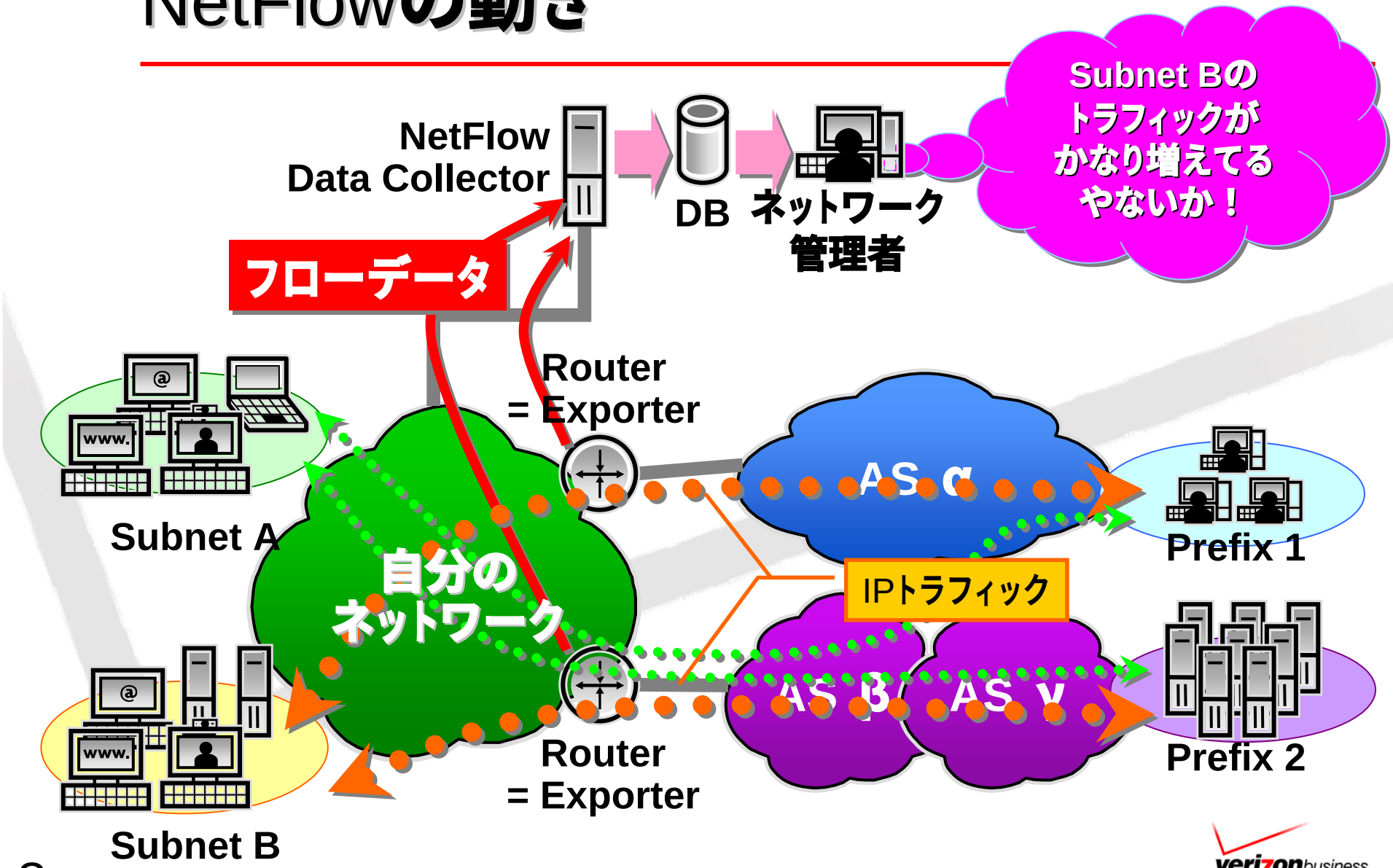
トラフィックデータの取り方

- 回線（インタフェース）の使用率
  - MRTGとかで、普通にやってますよね

- 「Prefix毎のトラフィック」とか分からないと「トラフィックマネージメント」できないですよね
  - 途中経路でパケットキャプチャして覗いてやる
    - たぶん、知りたい所の「トラフィック量」って半端ではないですよね
    - それ以外にも、思い当たる問題もあるし・・・
  - パケットのヘッダ情報を集める
    - RMON
    - NetFlow ← 今回はこれのお話

verizon business

NetFlowの動き


NetFlow
Data Collector
DB
ネットワーク
管理者
Subnet Bの
トラフィックが
かなり増えてる
やないか！
フローデータ
Router
= Exporter
Subnet A
自分の
ネットワーク
AS α
Prefix 1
IPトラフィック
AS β
AS γ
Prefix 2
Router
= Exporter
Subnet B

NetFlowで取れるデータ

- Version 5では、こんなデータが取れます
  - 時刻 (フローの最初と最後)
  - パケット数、バイト数
  - 送信AS、受信AS
    - Peer AS、もしくは、Origin ASのいずれか
  - 送信アドレス、受信アドレス、Next Hop
  - 送信/受信のサブネットマスク
  - InとOutのインタフェース (ifIndex)
  - 送信ポート番号、受信ポート番号
  - IPプロトコル (ICMP, TCP, UDP,...)
  - TOSフィールド値
  - TCPフラグ

} このあたりは、使ったことないです（＾＾；

verizon business

Exporterの設定時の注意点

- 設定前の不具合の確認
  - ルータのベンダさんに事前確認
- CPUの負荷は上がります
  - 事前に検証しましょう
    - Ciscoさんからは、こんなドキュメントも出てます

    NetFlow Performance Analysis

    http://www.cisco.com/en/US/products/ps6601/products_white_paper0900aecd802a0eb9.shtml
  - CPUの負荷等のルータのリソースは
    ちゃんとモニタリングしておきましょう

Exporterの設定例 – Cisco編

- **Sample Configuration**

```
interface FastEthernet0/0
  ip route-cache flow
interface ATM2/0
  ip route-cache flow
ip flow-export source FastEthernet0/0
ip flow-export version 5 origin-as
ip flow-export destination <コレクタのアドレス> <ポート番号>
```

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cg/honf_c/chap05/onf_bcf.htm

Exporterの設定例 – Juniper Mシリーズ編 (1)

- **サンプリングを実行するファイアウォール･フィルタを作成する**

```
firewall {
    filter sample-all {
        term one {
            then {
                sample;
                accept;
            }
        }
    }
}
```


verizon business

Exporterの設定例 – Juniper Mシリーズ編 (2)

- **ファイアウォール･フィルタをサンプリングするインタフェースに適用する**

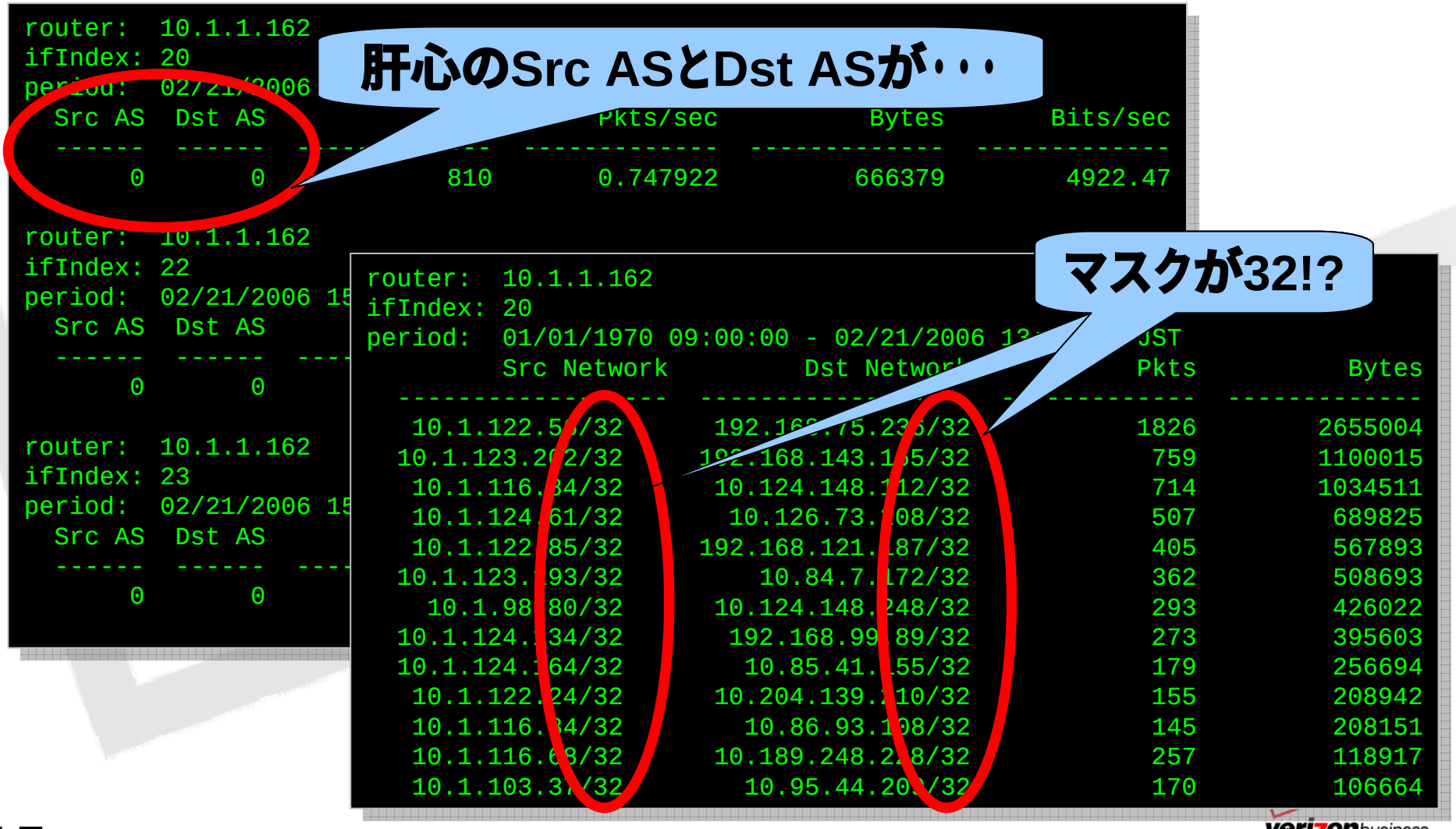
```
interfaces {
        ge-0/0/0 {
            description “Sampling Interface";
            link-mode full-duplex;
            unit 0 {
                family inet {
                    filter {
                    input sample-all;
# そのインタフェースへのInputトラフィックをサンプリングする
                    output sample-all;
# そのインフェースへのOutputトラフィックをサンプリングする
                    }
                address ***.***.***.***/30;
                }
            }
        }
}
```

Exporterの設定例 – Juniper Mシリーズ編 (3)

- **サンプリング・オプションの設定をする**

```
forwarding-options {
    sampling {
        traceoptions {
            file sampled-debug size 5m;          # Debug用
        }
        input {
            family inet {
                max-packets-per-second 1000;
                # サンプリングパケットを送出する最大PPS
                rate 5000;                       # サンプリング・レイト
                run-length 0;
            }
        }
        output {
            cflowd ***.***.***.*** {             # コレクタ・サーバのアドレス
                port ****;                       # UDPパケットのポート番号
                version 5;                       # NetFlowパケットのフォーマット・バージョン
                autonomous-system-type origin;
                                                 # Src/Dst ASをOriginに設定
            }
        }
    }
}
```

Exporterの不具合例



Collector/Analyzer

お金のある方

- Cisco**社謹製**
- ARBOR peakflow, GenieATM

などなど

お金のない方々

- cflowd by CAIDA
- flow-tools
- nfdump/NfSen

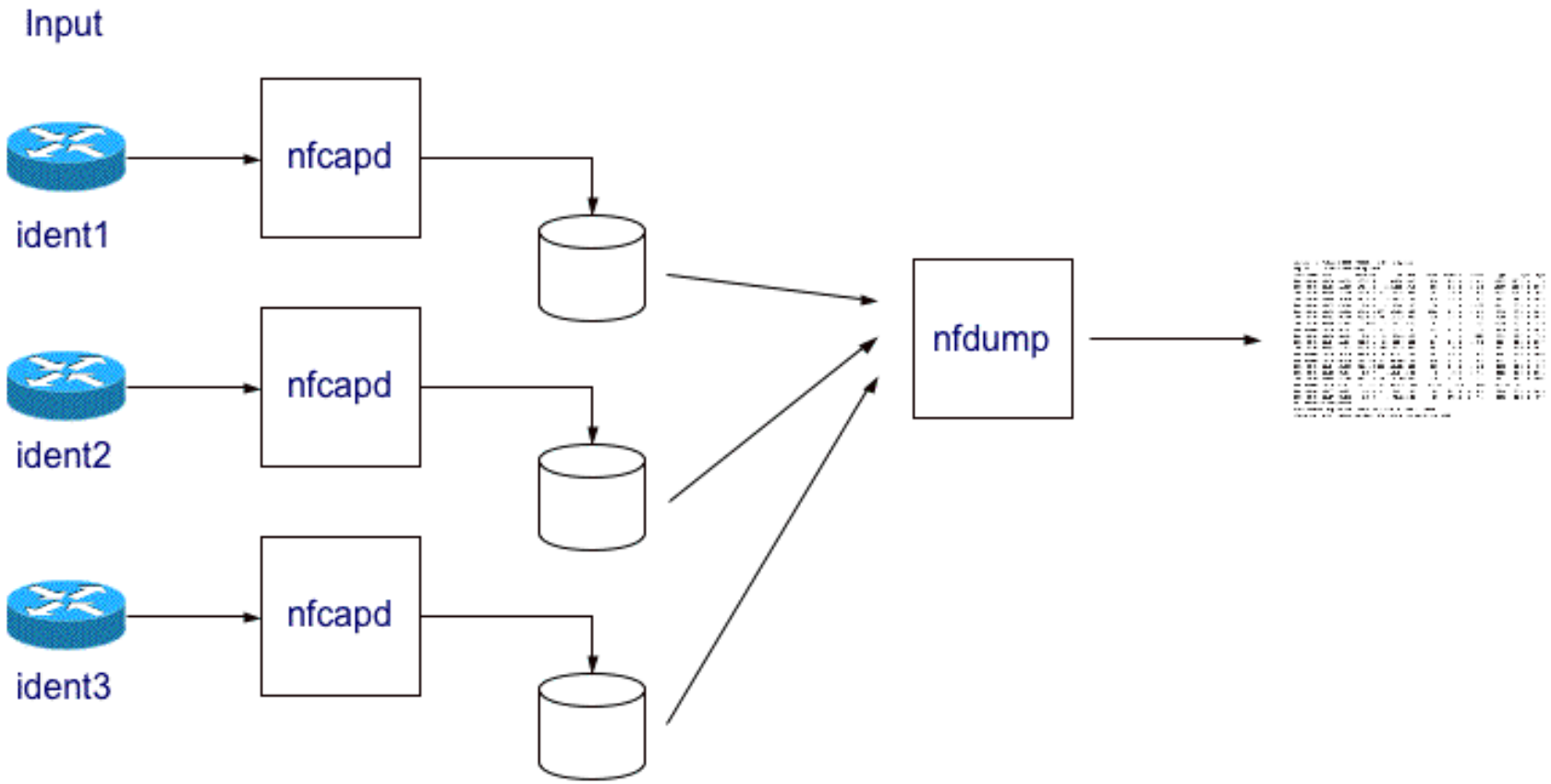
などなど

ちょっと前までは、『cflowd』使っていました。今回の分析では、主に『flow-tools』を使っています。

cflowd

- **古典的ツール**
- ARTS**形式**
  - **成分ごとに「マトリックス」と呼ばれるものに分解されて格納**
  - **つまり、条件付の分析ができない**
    - **特定の**Origin AS**から来ているトラフィックの中で**Dest Prefix**毎のトラフィックは？**
    - TCP**の中で使われているポート番号は？**
- **標準はテキストベースの出力**
- **トラフィック量の多い**Exporter**をサポートしようとすると、セマフォ（共有メモリ）を大きく取れるようにする必要があった（**FreeBSD**の場合、カーネルオプションを変更）**

nfdump

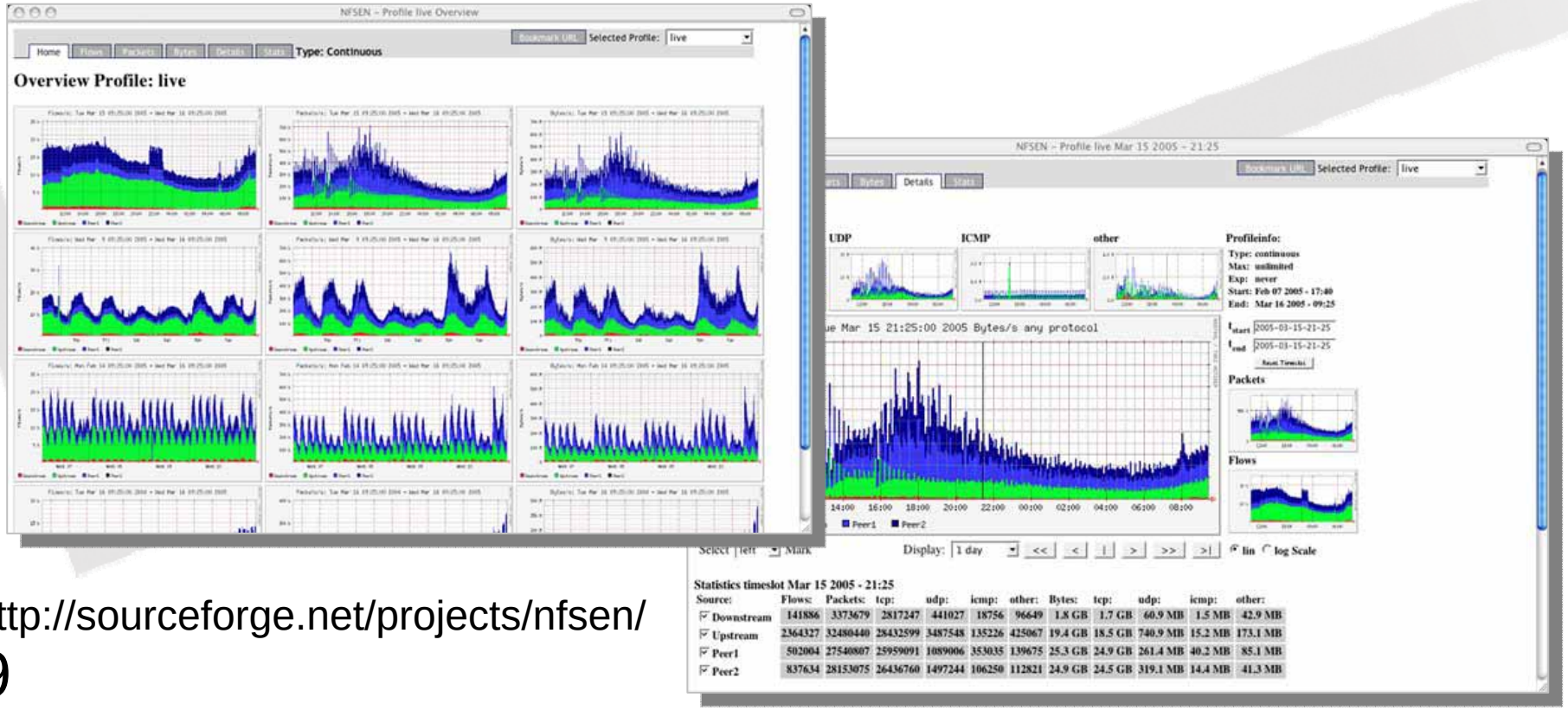


http://nfdump.sourceforge.net/

verizon business

NfSen

- NFDUMPで収集したデータをWebにグラフで表示



http://sourceforge.net/projects/nfsen/

flow-tools

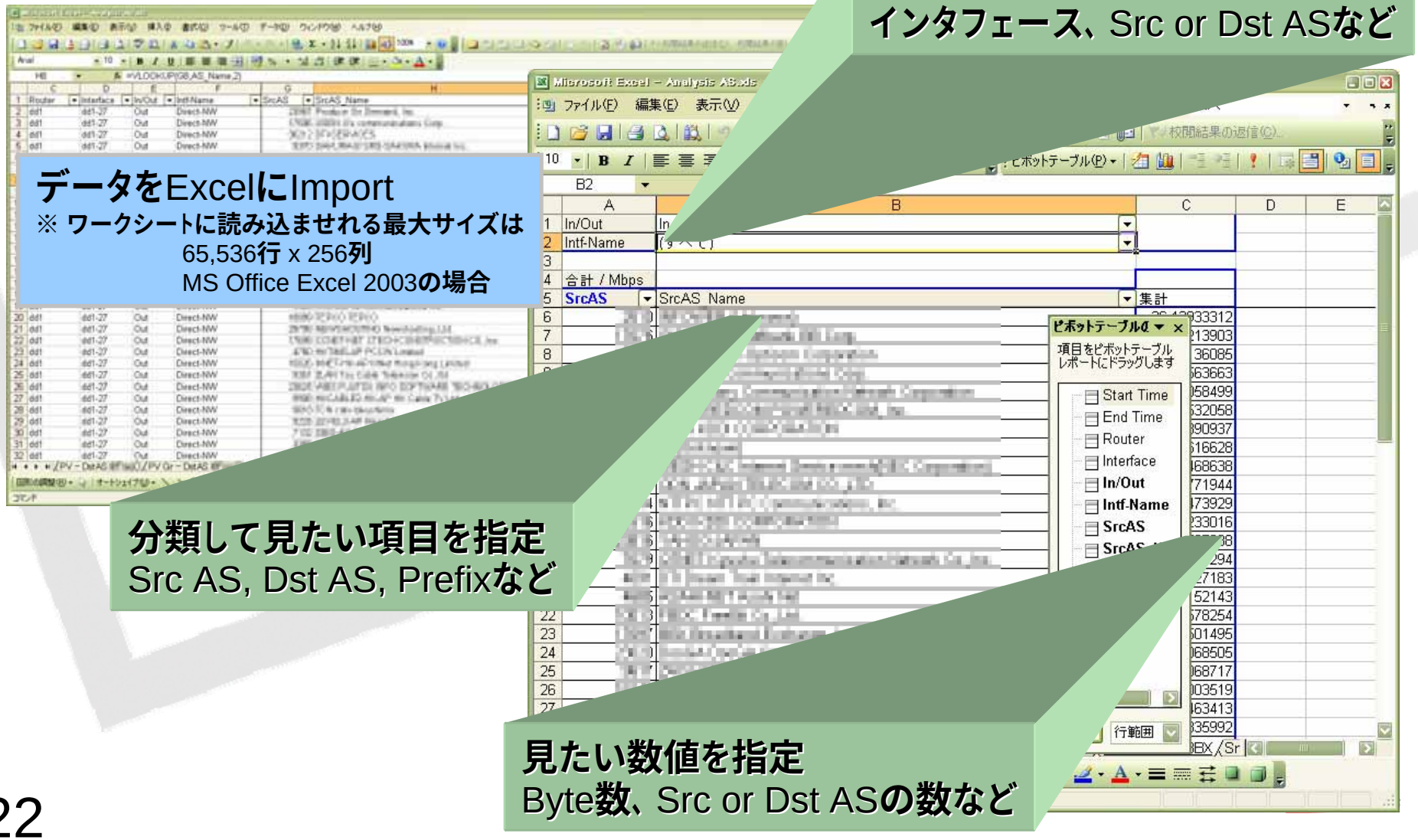
http://www.splintered.net/sw/flow-tools/

- **簡単にグラフの見たい人には向いてない**
- **受信したNetFlowのデータを、直接、PostgresSQL, MySQLなどDBに突っ込める**
  - Ad-Hocな分析
  - DWHなどの各種データ分析ツールが使える
- **一応、デフォルトでテキストベースのレポートも生成できます**
  - flow-report

取ったデータをどう料理するか？

- とりあえず、ツールの標準レポートを使う
- もっと、データ分析をしてみたい！！
  - Excelに読み込ませる
    - 『ピボットテーブル』でぐりぐり
  - 他のデータ分析ツール
    - お金のある方
      - 『S-PLUS』などの統計分析ツール
    - お金のない方々
      - R

Excelのピボットテーブルを使った分析



R – The R Project for Statistical Computing

- http://www.r-project.org/
- **統計解析ソフト**
- **いわゆる『S言語』**
  - **『R』はオープンソースなS言語環境**
- **読み込ませられるデータ量は、メモリ次第**
- **得意分野**
  - **もちろん、統計的な数値（平均、中央値、標準偏差など）は朝飯前**
  - **グラフ**
  - **回帰分析、検定・・・・（ごにょごにょ）**

verizon business

Section 2
トラフィックデータの分析結果 - 村松編

verizon business

データの分析結果

データの分析結果の詳細については、
『JANOG18 会場限定の公開』
とさせていただきます。

以下、事後公開資料として、分析結果の一部を
公開いたします。

AS分析結果（一部公開）

AS毎のトラフィック量の分析
⇒ 全トラフィックを 100% とし、各AS の割合を算出
⇒ さらに、AS番号から国別に割合を計算

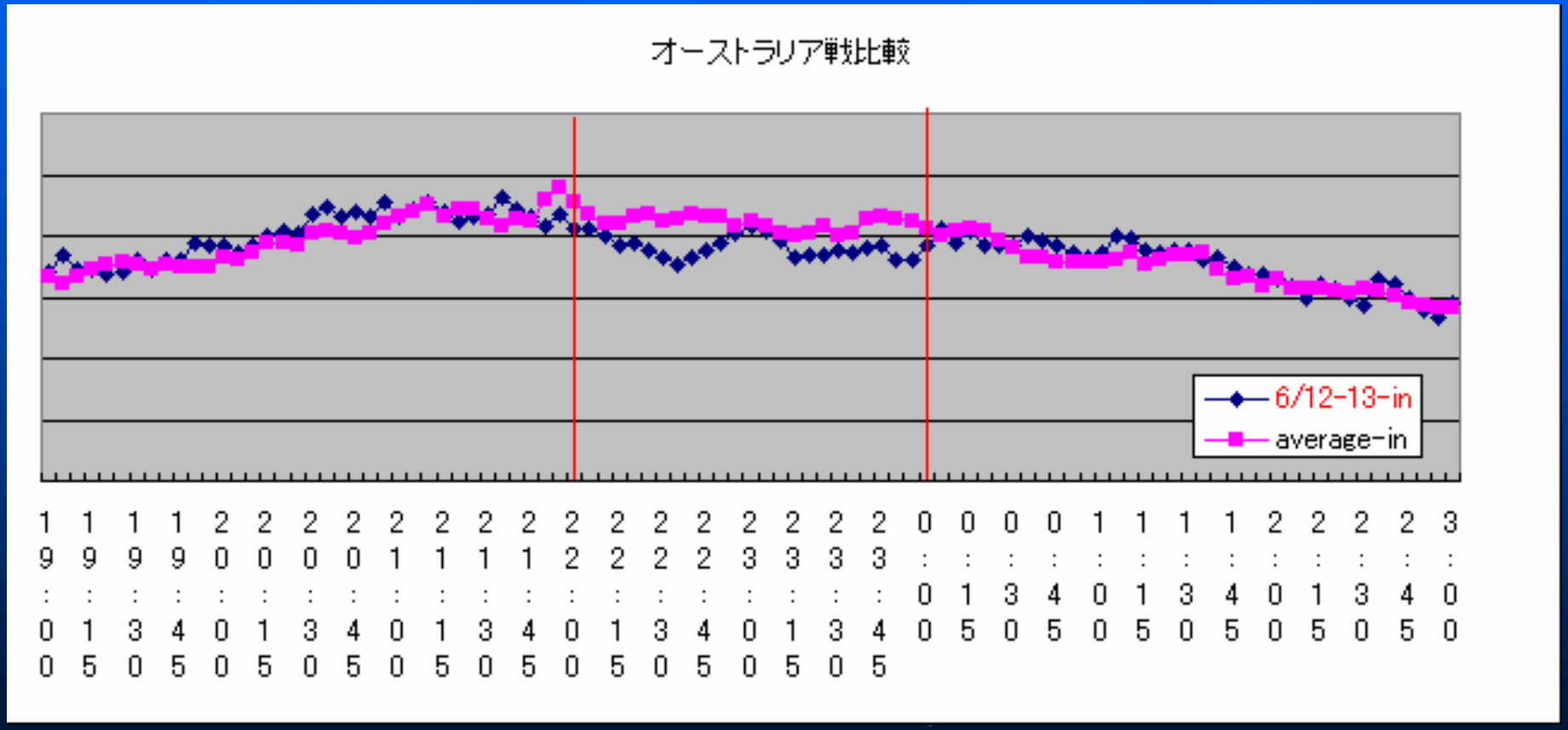
※調査対象：DSL または Fiber の回線を利用している
エンドユーザのトラフィック
(6月のある1週間)

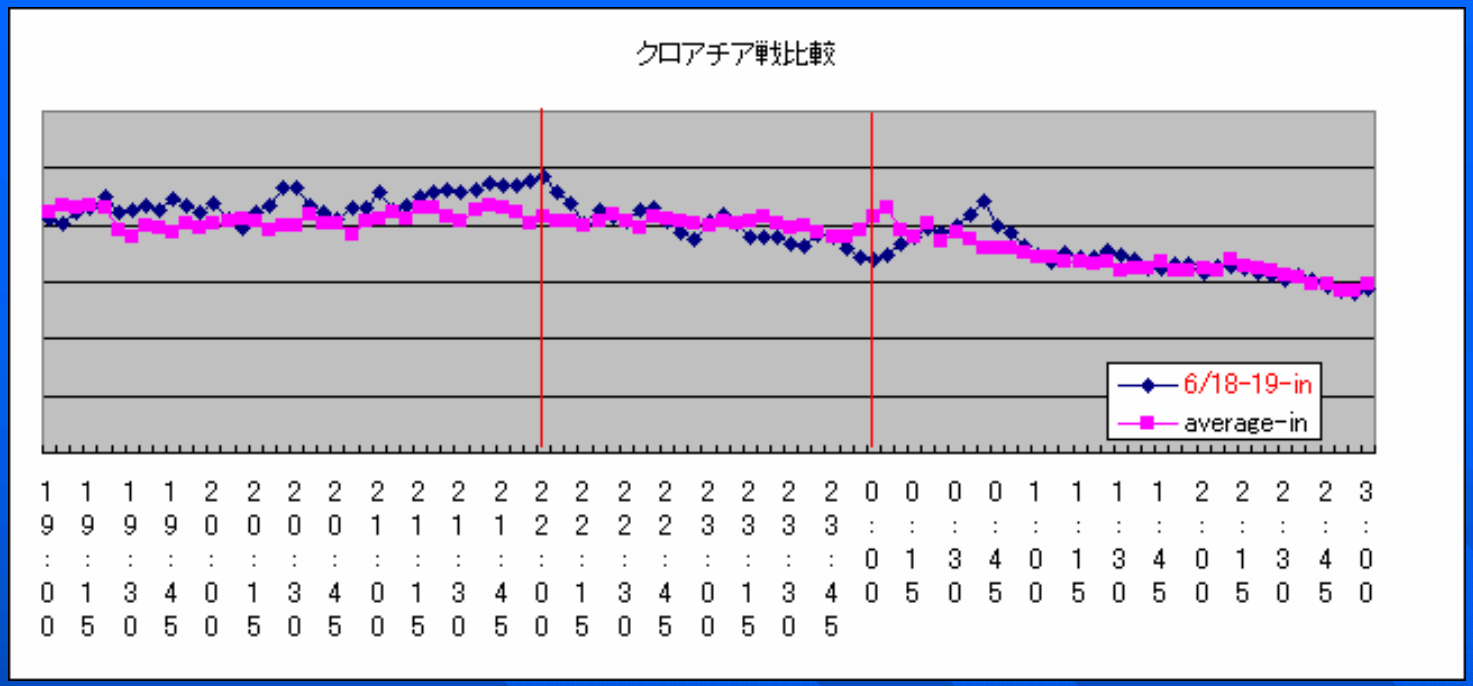
- トラフィックの多いASってどのＡＳでしょう？
- 国内外のトラフィック比率は？
- アジア系（特に中国）の通信はどれくらい？
- In – Out のトラフィック傾向は？

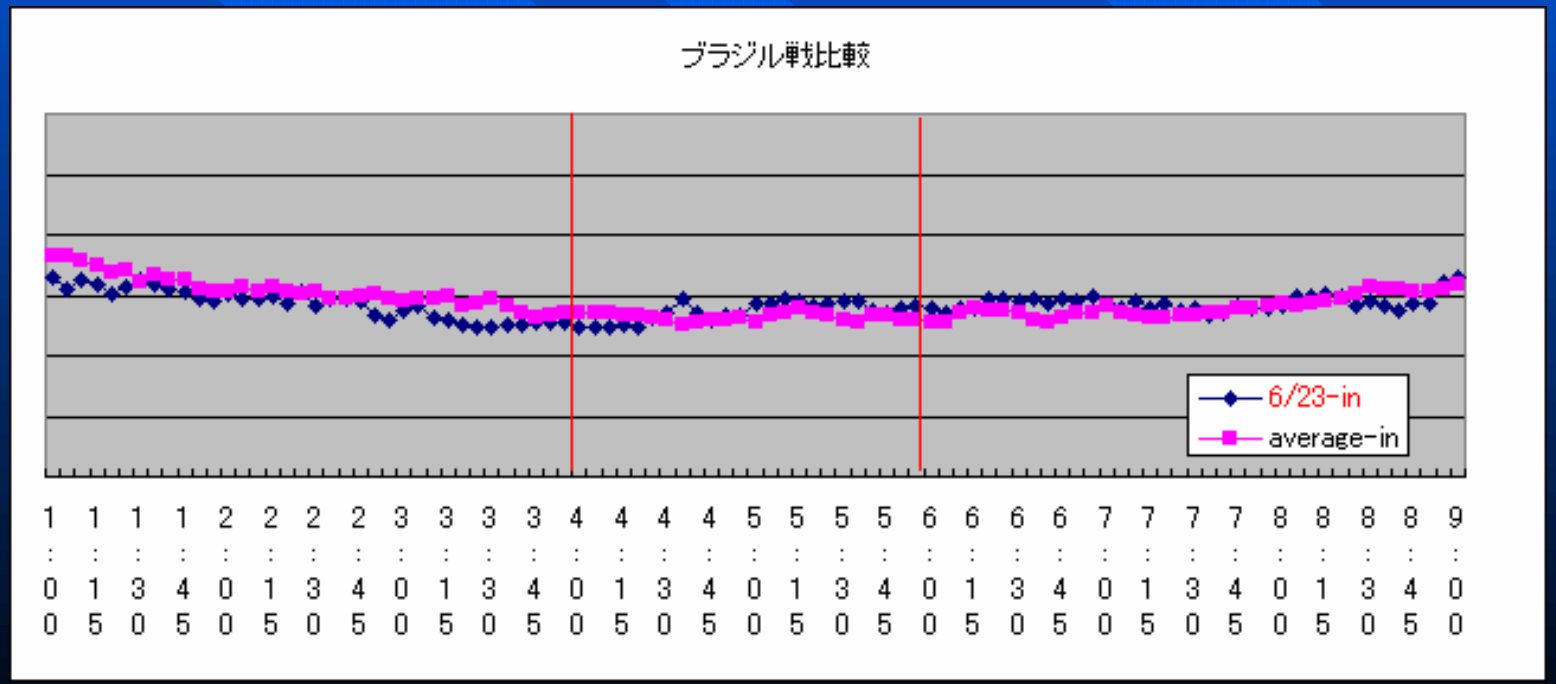
AS分析結果（一部公開）

- Inbound、Outbound 共に、全トラフィックの80%以上が国内間通信のトラフィック
- Inbound の 10% 程は US からのトラフィック
- Outbound は、中国と台湾を合わせて10%程度、US は 1% 程度
- 全体的にアジア系の通信料は多い

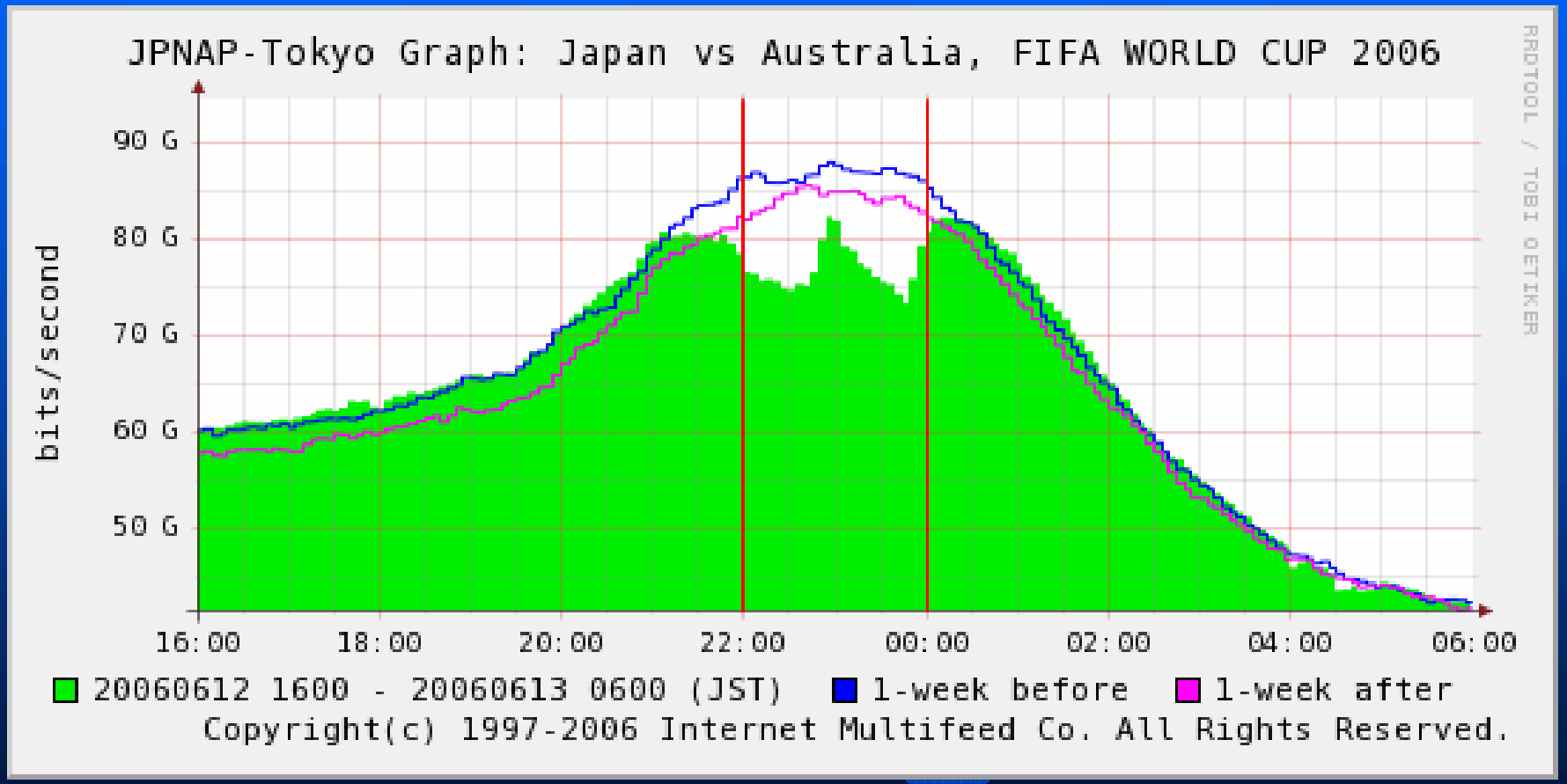
W杯 日本戦開催時
トラフィック変動について

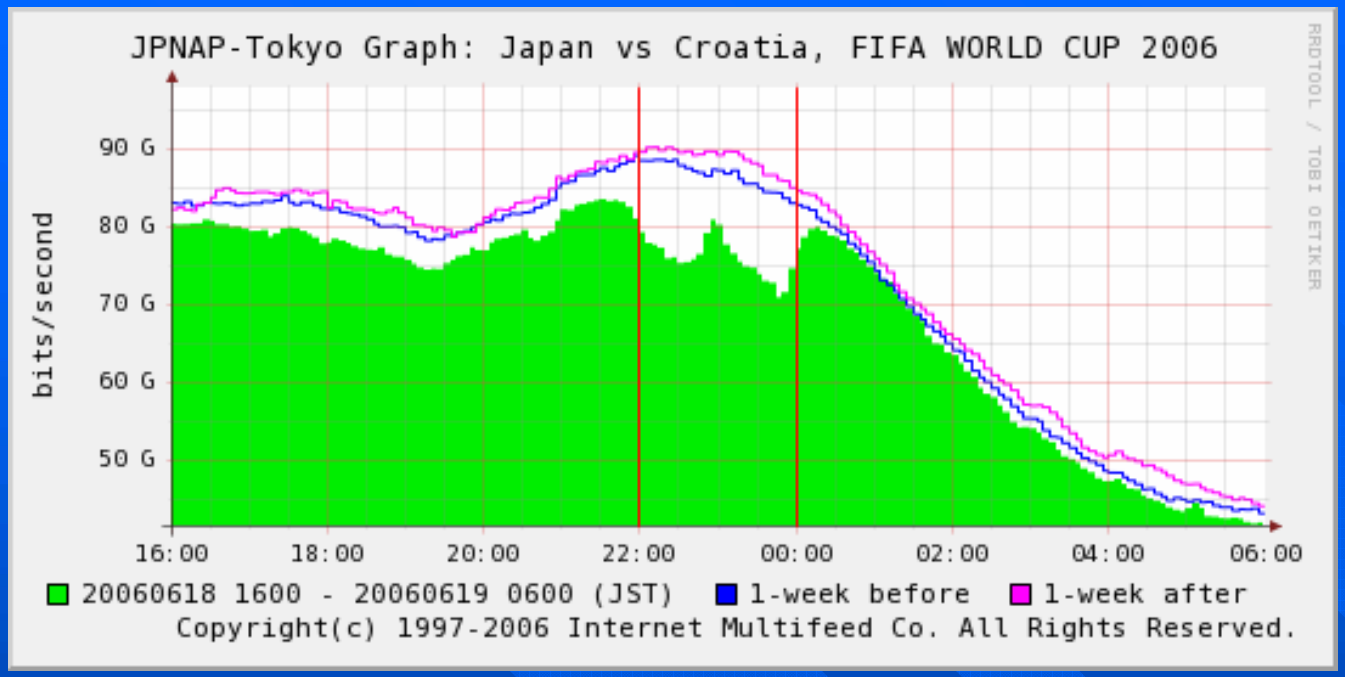


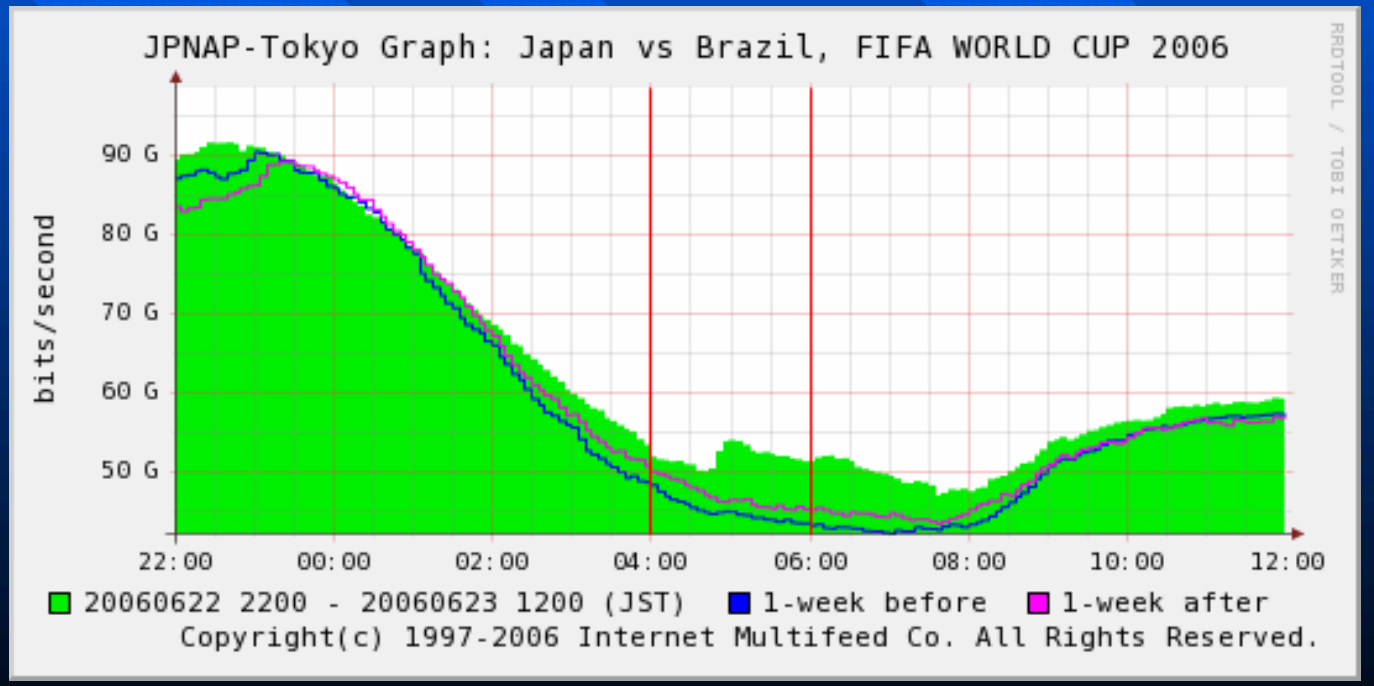

クロアチア戦比較
6/18-19-in
average-in
19:00
19:15
19:30
19:45
20:00
20:15
20:30
20:45
21:00
21:15
21:30
21:45
22:00
22:15
22:30
22:45
23:00
23:15
23:30
23:45
0:00
0:15
0:30
0:45
1:00
1:15
1:30
1:45
2:00
2:15
2:30
2:45
3:00


ブラジル戦比較
6/23-in
average-in
1:00
1:15
1:30
1:45
2:00
2:15
2:30
2:45
3:00
3:15
3:30
3:45
4:00
4:15
4:30
4:45
5:00
5:15
5:30
5:45
6:00
6:15
6:30
6:45
7:00
7:15
7:30
7:45
8:00
8:15
8:30
8:45
9:00

JPNAP のトラフィック変動




JPNAP-Tokyo Graph: Japan vs Croatia, FIFA WORLD CUP 2006
RRDTOOL / TOBI OETIKER
bits/second
90 G
80 G
70 G
60 G
50 G
16:00
18:00
20:00
22:00
00:00
02:00
04:00
06:00
20060618 1600 - 20060619 0600 (JST)
1-week before
1-week after
Copyright(c) 1997-2006 Internet Multifeed Co. All Rights Reserved.


JPNAP-Tokyo Graph: Japan vs Brazil, FIFA WORLD CUP 2006
RRDTOOL / TOBI OETIKER
bits/second
90 G
80 G
70 G
60 G
50 G
22:00
00:00
02:00
04:00
06:00
08:00
10:00
12:00
20060622 2200 - 20060623 1200 (JST)
1-week before
1-week after
Copyright(c) 1997-2006 Internet Multifeed Co. All Rights Reserved.

分析の感想とまとめ

- 地域プロバイダの小規模な調査でも、現在の日本のインターネットのトレンドを垣間見れた気がします！
- やはり定点観測ではなく、時系列での調査が理想
- 同じ条件で比較できる対象が欲しい
- 安定運用・品質向上のために、ネットワークオペレータは自分の管理するネットワークのトラフィック動向を知っておくべき！

Section 3
トラフィックデータの分析結果 – 伊賀野編

verizon business

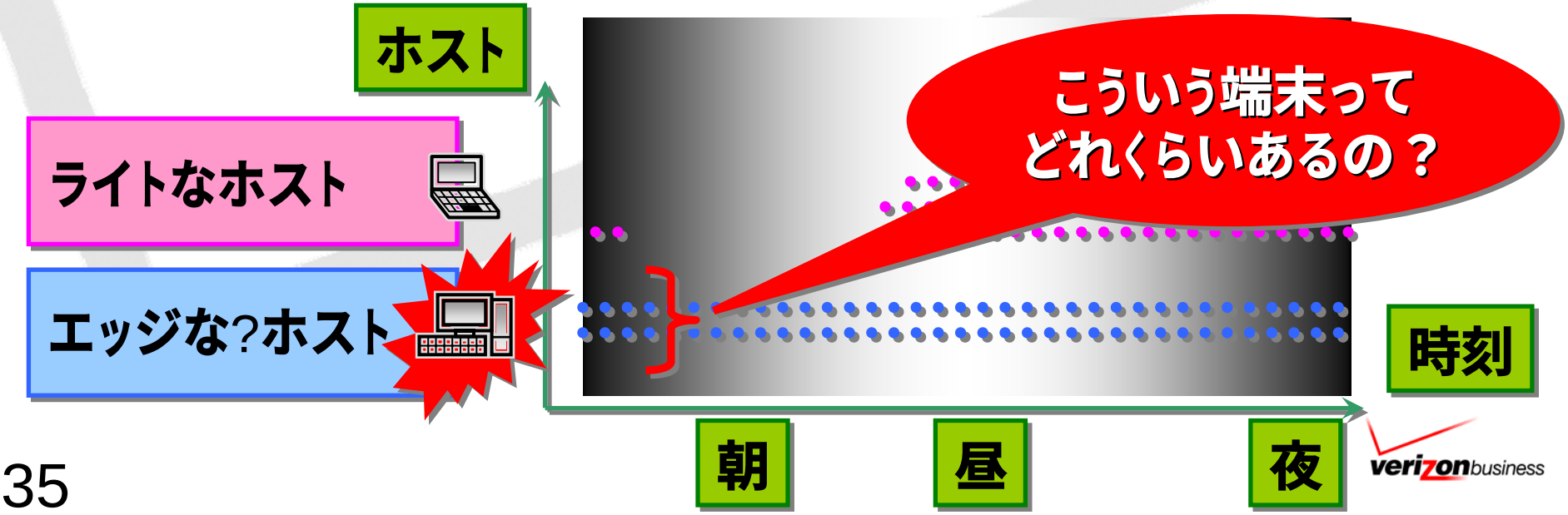
定義

- ホスト
  - ブロードバンドユーザに割り当てられるIPアドレス(ユーザ?)

- トラフィックの方向
  - Inbound : インターネットからホストへ
  - Outbound : ホストからインターネットへ

1. ホストのセッション

- ホスト毎に時間軸に沿ってOutboundのトラフィックの発生をポイントしたらどうなる？
  - トラフィック量の多い方から順番にソート
  - そのホストたちが24hトラフィックを吐き続けていたら、そのあたりが焦げる！？



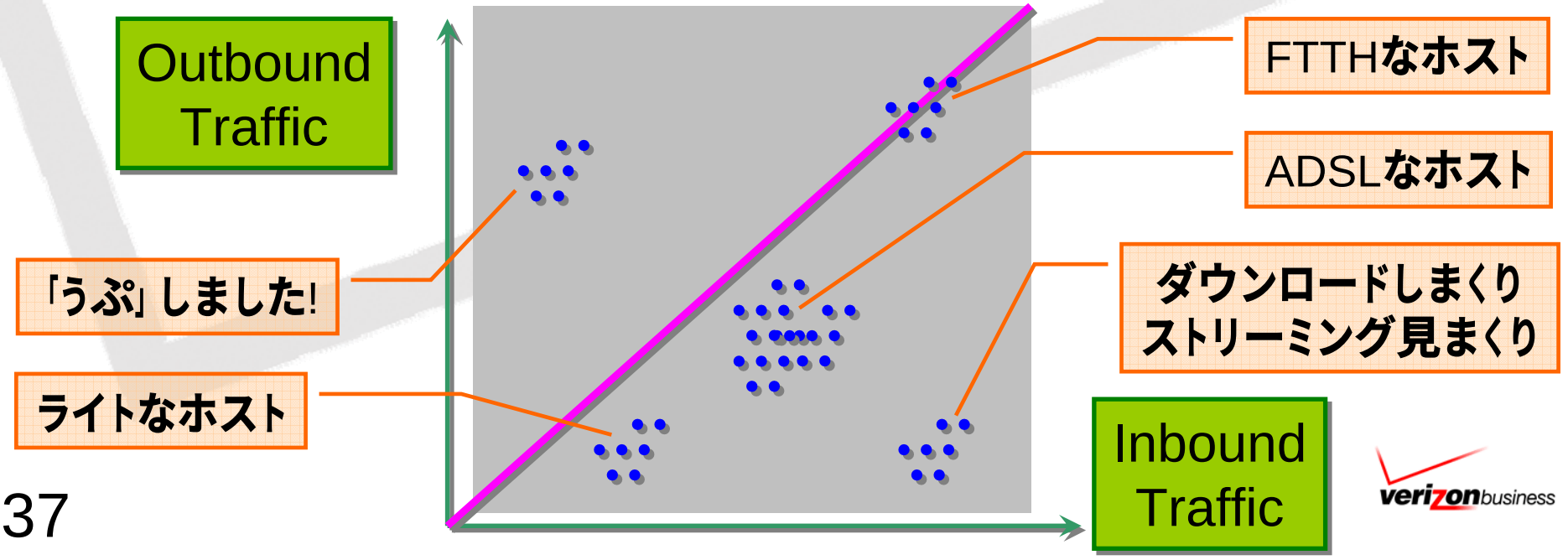
傾向 – ホストのセッション

- 12時台と20時以降は、濃くなっている

- 全体の7〜8%ぐらいのところが、常に濃くなっている
  - つまり、7〜8%ぐらいのホストが24時間トラフィックを出し続けている、っぽい

2. InとOutのトラフィック量

- ホスト毎に1日のInとOutのバイト数をポイントしたらどうなる？
  - ADSLって非対称だよね
  - FTTHって増えてきたよね
  - ダウンロードばっかりするホストってある!?



傾向 – InとOutのトラフィック量

- 2つのグループに分かれている
  - ヘビーなホストは、InとOutが対象な感じのグループを形成
  - 通常のホストは、Inの方が多い形でグループを形成
- ダウンロードだけ、アップロードだけのホストのトラフィック量はそれほどない
- ADSLでも、それなりにOutのトラフィックがある
- 1日10Gを超えるトラフィックのホストは、さすがにFTTHのみ
- ADSL, FTTH共に、大手ISPさんの分析結果に酷似している
  - Kenjiro Cho, Kensuke Fukuda, Hiroshi Esaki and Akira Kato.
    The Impact and Implications of the Growth in Residential User-to-User Traffic.
    SIGCOMM2006
- 全体の2割のホストが、全利用帯域の8割を占めている

verizon business

大手ISPさんの分析との違い

- 集計方法
  - 動的アドレスの考慮
    - 大手ISPさん：ユーザのIPアドレスの変更まで考慮
    - 今回：ざっくりとIPアドレス単位で集計
  - 集計期間
    - 大手ISPさん：特定の1週間のデータを1日平均に換算
    - 今回：6月の水曜日 一日のみ
- サンプリングレート
    - 大手ISPさん=1/2048, 今回=1/5000

これだけ大雑把な分析でも、
ヘビーユーザの動向は、十分分析できそう

結論

- 結構ラフな解析でも、ヘビーユーザの動向は把握できそう
- 大手ISPと地方ISPのトラフィック・トレンドは不思議なぐらい似通っている

- IPネットワークを運用する上で、
『今、自分たちが扱っているトラフィックは何なのか？』
という事を理解する事は必要では?

verizon business

THX!!

Special Thanks to

北海道大学情報基盤センタ
南先生

IIJ技術研究所 長様

その他、トラフィック分析について情報提供頂いた方々

JANOG18の運営委員の方々

何より、プログラムに参加頂いた皆さん

verizon business

おまけ

- このようなプログラムって、定期的に欲しい人いませんか？

- で、どなたか一緒にトラフィック分析やりませんか？
  手伝いまっせ。

by VzB **いがの**

verizon business