JANOG Special Session 2006
～とある首都圏ISPのトラフィック事情についての考察～

NEC

川村　聖一

kawamucho@mesh.ad.jp

データ取得方法

■様々なやり方があると思いますが、以下の方針でみてみました。

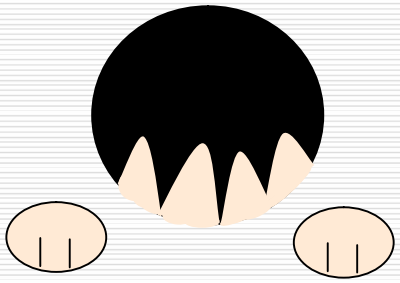
－用途に応じたデータ取得（エッジ側、バックボーン側）
－代表的なポート番号で識別する程度にしている
－主なデータはWeb,mail,stream,sip,p2p,iTunes,spoof
※spoofとは、自AS内で発生しているのに、sourceアドレスが
自ASのアドレスでないもの

■簡単に、首都圏ISPのTraffic事情を紹介する、という程度の目的です。
ただし、すべての首都圏ISPがそう、というわけじゃなく、Exampleとして

データ取得方法や、取得結果の細かい分析は
JANOG18でプログラムが企画されています。

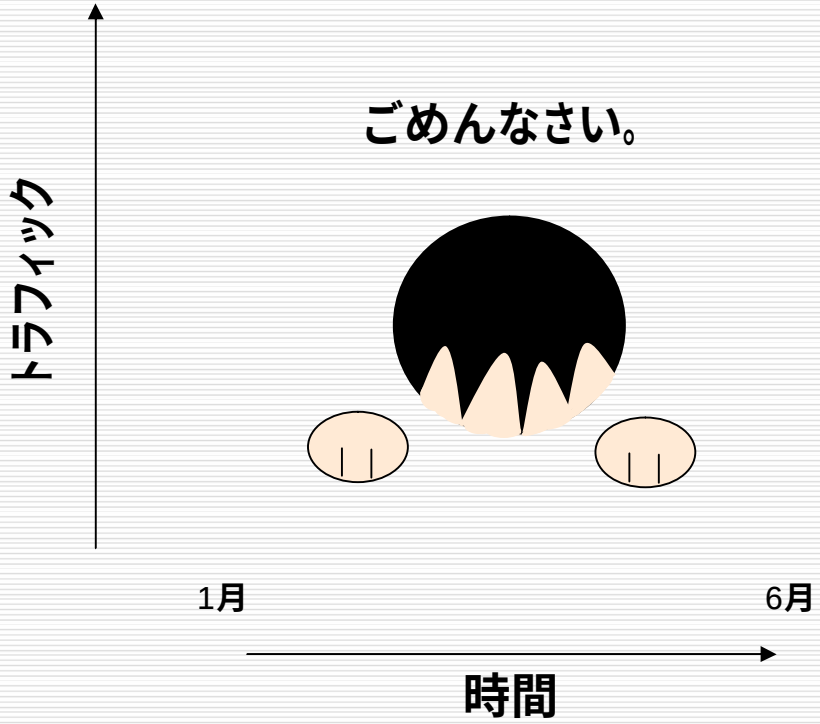
GW付近のデーターエッジ側

ごめんなさい。



※データはISP内の一部Trafficをサンプリングしたものです。

半年間でのStreamingの伸び



-バックボーン側で取得

-ISP内のStreamingTraffic
だけに焦点をあてたデータ

-約半年で倍近くのPeak増加

※データはISP内の一部Trafficをサンプリングしたものです。

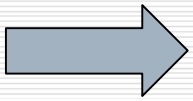
感想

【わかったこと】
・ヒューマンな活動は、過去に比べると顕著でないかもしれないが、
GWになると昼間のWebアクセスTrafficが増えるなど、現象は見える。
～平日はロボット的、祝日はサッカーとかあるとすぐ減る、など人間的～
・P2Pが相変わらずNo.1Trafficジェネレータですが、Streamが3番手にきている
ところが割と最近のTrend。どんどんのびている。
・DoSがくるとすぐわかる。わりと有効かも。
・今回のとり方では、あまり顕著にWindows自動Rebootは見えなかったが、
急速な落ちは観測された。
【わからなかったこと】
・SIPはうまく計れなかった・・・Skypeもちょっと勉強が必要。（netflowで定義
するのは難しいかも？パターンマッチングが一番いい）
－音声サービスは今後増える。ツブれてほしくない
・Webの中にRSSがどの程度あるのか、を調べたい。。。
・TCPとUDPの比率は？

おまけ

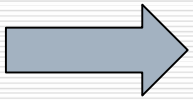
■グラフにはなりませんが、以下の事もやってみました。

－HTTPアクセス先ドメイン top xx
・・・Byteベースの測定方法とFlowベースの測定方法がある
・・・ネット広告、Blog、あやし～いサイトが上位。フローベースだとネットゲームも多い



ネット広告はユーザの意思とは無関係なHTTP
BLOG、RSSが最近はわりと多いと見ている(推測)

－DestinationAddress top xx
・・・NNTP、ダイナミックプールアドレス（大半はコンシューマサービス）がほとんど。



一部のIPアドレス（ダイナミックアドレス）は
*ものすごい*TrafficをGenerateしている。
NNTPはご存知のとおり無法地帯

データを見て思うところ

- Netflowだけでもちょっと触るだけでここまでわかる。
- ネットワークエンジニアリングに新たな運用技術と運用手段が見えてきた
- 活用するといいことがある
  - 一般的なネット利用に支障を及ぼすような使い方を検知できる。
  - そもそも一般ユーザのネット使用にどのような傾向があるのか、という現実をISPは知る事ができる。
    - 時期設備投資の参考になる
    - 強化ポイントが見えてくる
- オーバーサブスクリプションされているブロードバンド回線に*広帯域通信*を*自動的*に行うアプリが増えるなかで、こういうツールを使って、ISPが自身内部の通信を分析して、効率的にかつフェアに保つ努力をしていくのはもっと世の中的に認められていいのでは？

Special Thanks

-今日来ていただいたみなさま
-南さん@NEC
-JANOG　近藤会長　&　JANOG運営委員のみなさま