公開版

flow最新動向

2006/9/22

株式会社ネットマークス
田島弘隆

tajima.hirotaka@netmarks.co.jp

今日のメニュー

- flow最新動向
  - T島@ネットマークス
    - Flow全体と動向をざっくり
- sFlowで遊ぼう
  - 大久保修一さん@さくらインターネット
    - sFlowと奮闘されているあたりを
- パケットサンプリングとフロー分析

  ～サンプリングで統計はどう変わるか?～
  - 森達哉さん@NTT SI研
    - サンプリングの研究　＋　サンプリング以外の観測

Flowの概要とサービス例

なぜいまFlowか？

- 10G の普及
  - インラインでタップはちょっとね
  - 10G食えるボードとかアナライザは超高価
- トラヒックの中身分析(観察の可否は別にして)
  - SNMP/MRTGでは力不足
  - NW設計/運用にとっても役立つ

みんな集めてる？　中身見てる？　解析してる？

用語が紛らわしいので確認。

- IPフロー / NetFlow
  - 前者：*「一定時間に観測点を通るIPパケット集合」*
    - {src[IP,port],dst[IP,port],IP protcol + TOS,入力I/F}
  - 後者：*「IPフローの情報を提供するサービス」*
    - データそのものは「Flowレコード」「NetFlowデータ」
      - 》(以上参考：RFC3954「NetFlow v9」)

ここではflow ＝ NetFlow とします

用語の確認。(Cont.)

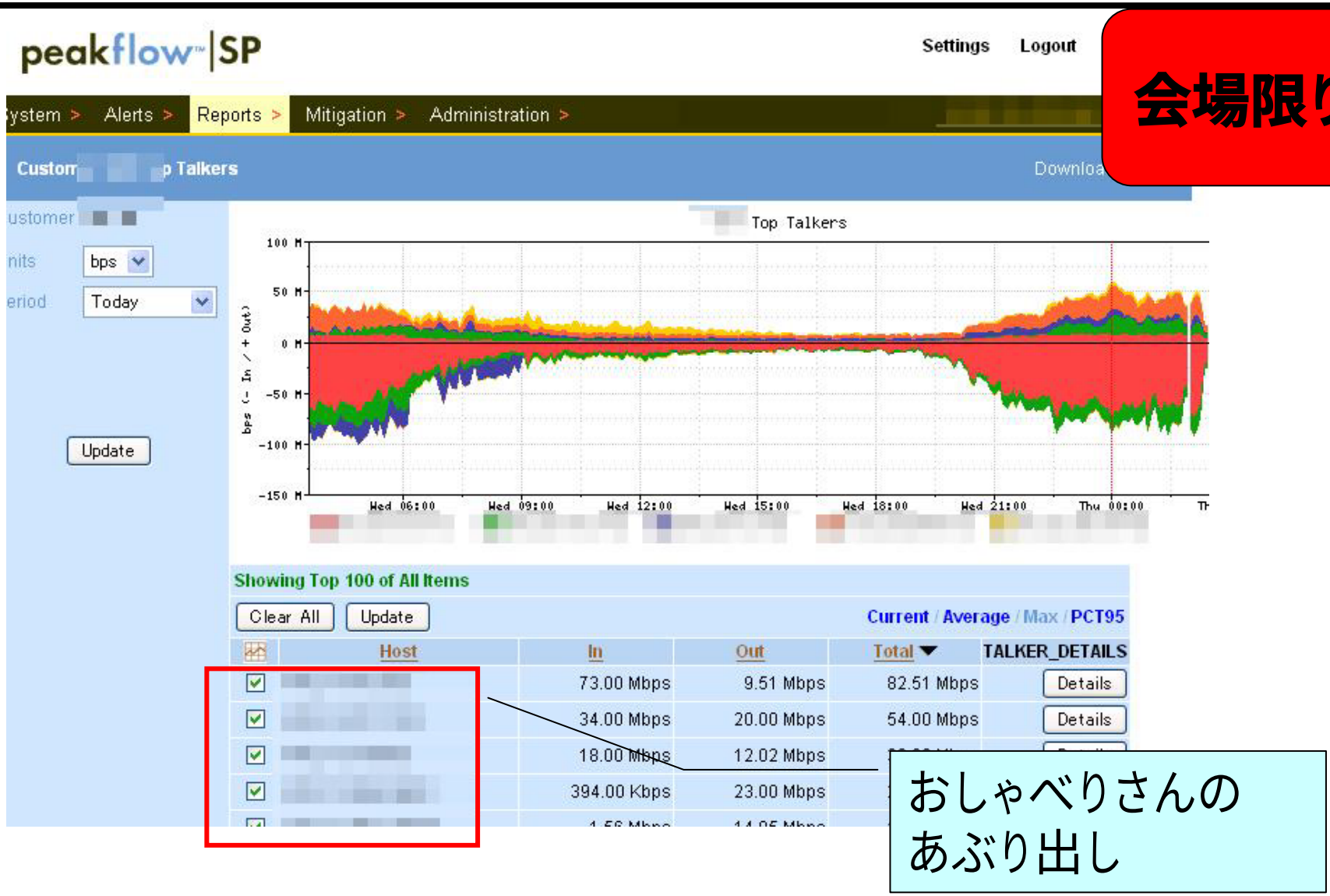
- エクスポータ/コレクタ
  - 前者：flowデータをはき出すモノ
    ルータとかスイッチなど
  - 後者：NetFlowを集めるモノ
    ソフトであったり、専用箱であったり

Flowでできること、やりやすいこと

できるっちゅーか使う目的ね。

- トラヒックの中身をしらべる
  - MRTGは「観測点を通過した通信量」のみ
- トラヒック量の評価
  - Peer/transitのコスト・負荷分散
  - Top Talkerとか
- DDoSなど攻撃の検知
  - Flow自身でなくコレクタの機能だけど
- AAA(特に課金)

例：TopTalker

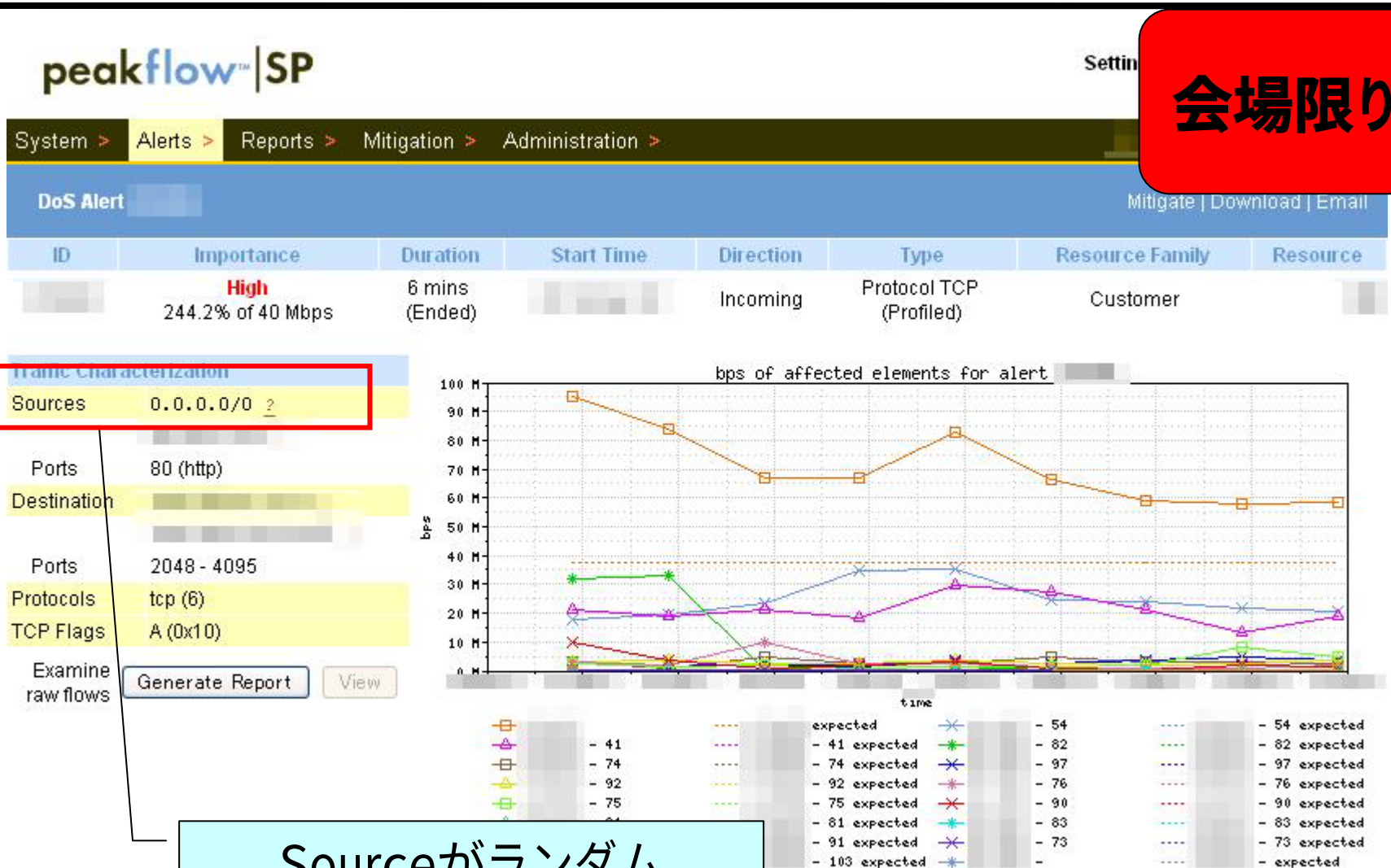


会場限り。

おしゃべりさんの
あぶり出し

We are here

例：DDoS検知

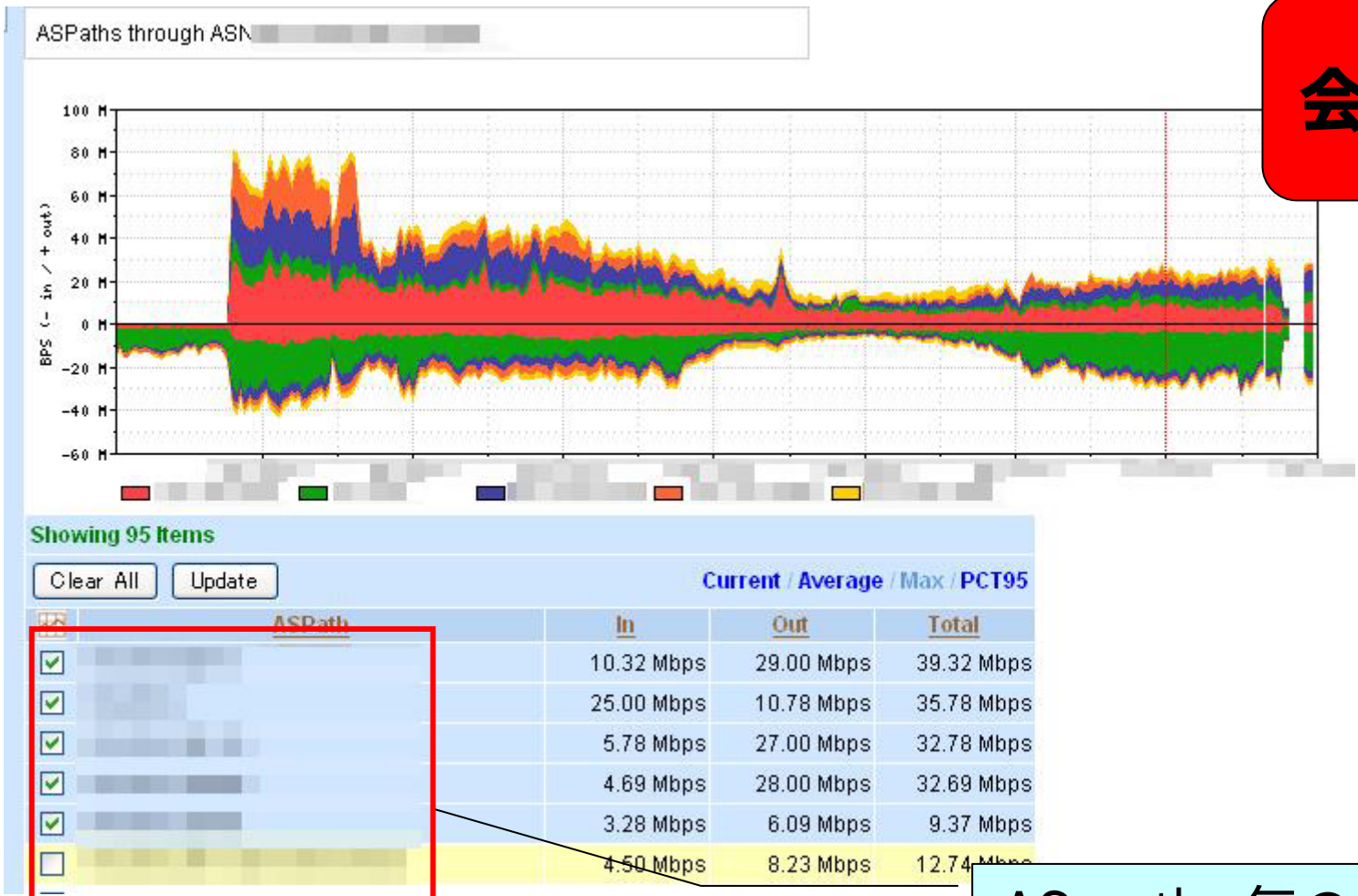


会場限り。

Sourceがランダム
→ DDoS

We are here

例:peer / transit 評価



会場限り。

AS path　毎のtop talker
→ Peer 判断の材料に

We are here

flowを活用しているサービス例

- DDoSの検知とミチゲーション(緩和)
  - AT&T（主にUS)
    - 『Internet Protect –DDoS Defenseオプション』
  - Verizon Business(USのみ)
    - 『DOS Defense Detection and Mitigation』
  - SAVVIS
    - 『DDoS Atack Mitigation Service』
  - COLT(EU)
    - 『Clean Internet Services』
  - 他海外多数
  - 国内数社　　←「flowを利用」とは言ってない

国内でフローを使ってるYo!と明言しているのはあんまりない？

flowを活用しているサービス例(cont.)

- IXで
  - Internet Multifeedさま:『PeerWatcher』
    - sFlowで解析
    - なんとL2まで見ている！
    - 苦労されているそうで、、、
- トラヒック解析に
  - 主にNW運用で

Flowテクノロジ

Flowテクノロジ

- NetFlow - C,J,A
- sFlow - F,E,A,F10,Allied
- cflowd - J (NetFlow v.5とほぼ同じ)
- IPFIX - ルータ実装は無し？コレクタは複数
- NetStream – Houwei

NetFlowあれこれ

- version.5 / version.9が主流
- もともとはQoSの仕組み
  - IP flowを分類してswitchingする
  - でもL2情報は持ってない
- flow情報をキャッシュするのでフラッシュする必要あり
  - タイマ、キャッシュfull、RST / FINなど
- Ver.9は「テンプレート」に対応(後述)

sFlowあれこれ

- 最近の流行かな？
- 「この箱sFlow対応だムフッ」と甘く見てると痛い目にあいます
  - 実装がまちまち　(→大久保さんとこで)
  - ツールの「sFlow対応」は疑ってかかれ
    - 》若干自分の首を絞めている感が、、、
- サンプリングなので「IPフロー」は意識しない
  - NetFlowとは異なる

IPFIX、PSAMPを若干

- IPFIX - IP Flow Information eXport
  - http://www.ietf.org/html.charters/ipfix-charter.html
  - NetFlow v9がベース
  - IPsec/TLSでフロー情報をexport可能

- PSAMP
  - http://www.ietf.org/html.charters/psamp-charter.html
  - IPFIXと統合予定
  - パケットサンプリングの標準を策定中

テンプレートは万能ではない

- 「テンプレート」とは
  - Flow構造を自由に設計できる便利な機能
  - “C言語の構造体”、といえばわかる？

- NetFlow v9とIPFIXはテンプレートに対応
  - 一瞬ユーザが自由にflowデータを作れそうな気になる

  が

  - 結局は実装次第
  - テンプレートIDはreboot毎に変わっちゃう
    - エクスポータが個別に管理してる

Config例

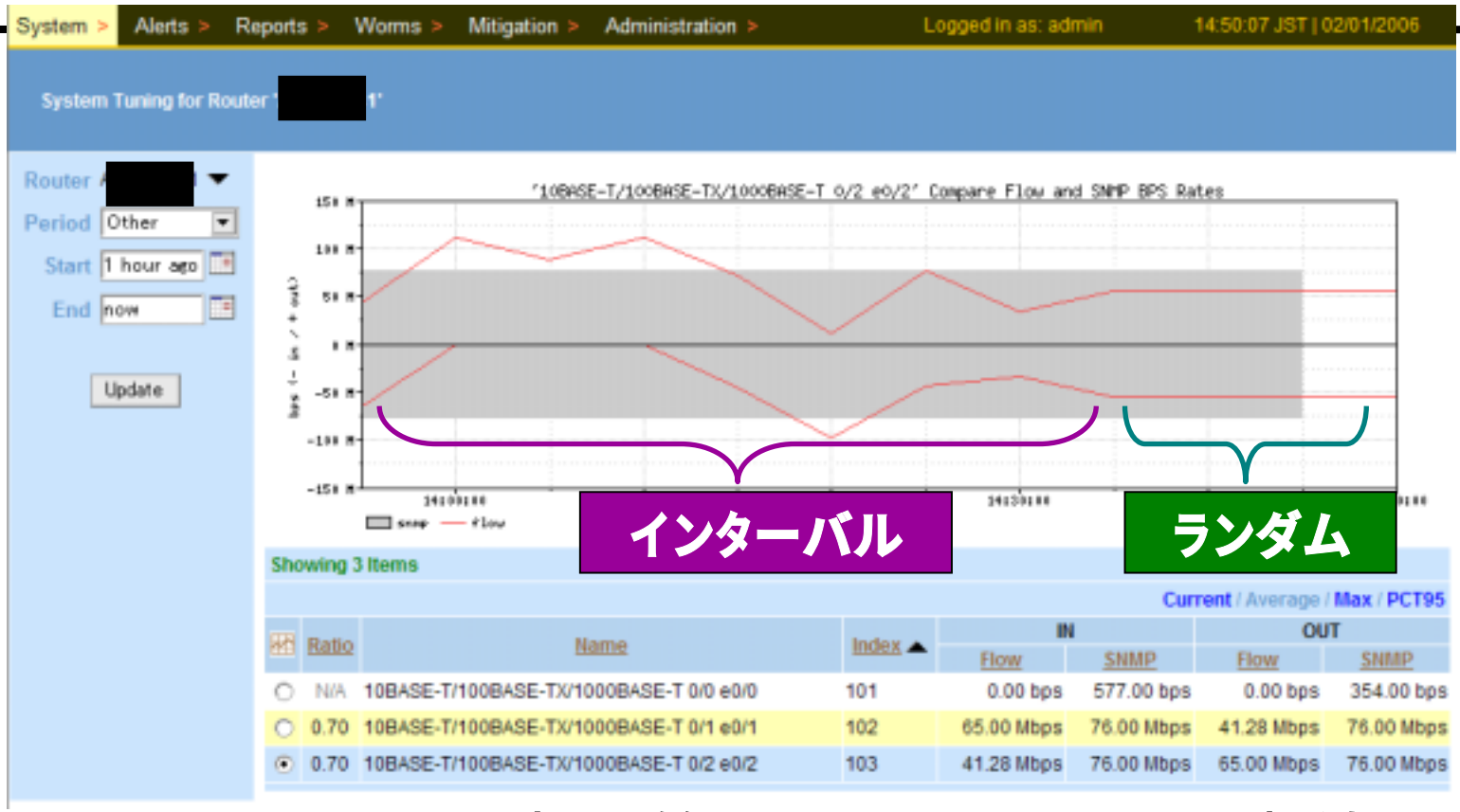
- 省略
  - マニュアルみて。

てのもなんなので、、、

幾つかポイント

- サンプリング間隔　→森さんのとこで詳しく…
  - CPU負荷に注意
  - 1:1024とか1:2048、トラヒック多めのとこで1:8192がよく使われる
- ランダム or インターバル
  - 基本はランダムがお勧め(→例)
- IP flowのタイムアウト
  - NetFlowの出力タイミングに関係
    - Active timeout　生きてるIPフローのkeepalive
    - Inactive timeout　死んでるIPフローかを判定

サンプリング例



インターバル(定期的にサンプル)は異常値になることがある(特に検証環境)

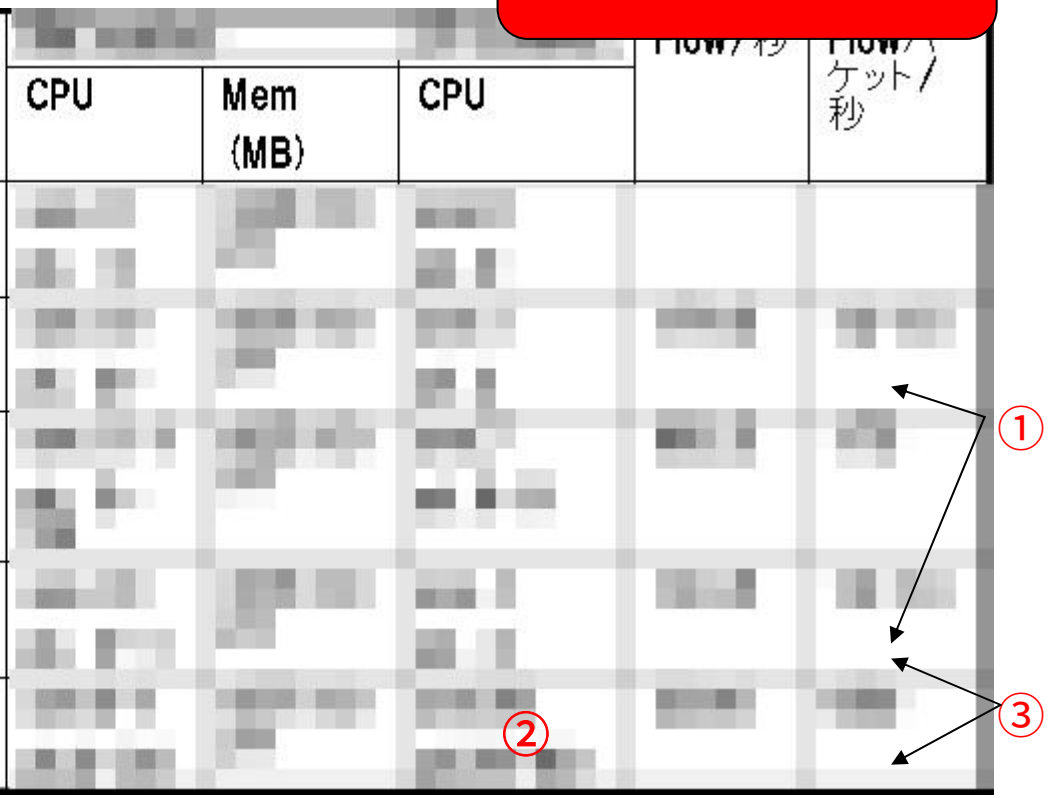
→サンプリング方式は原則ランダムを推奨

ルータへのインパクト

例：NetFlowとsFlowの比較

会場限り。

番号	フロー形式	サンプリングレート	トラフィック	CPU	Mem (MB)	CPU	Flow/秒	Flowパケット/秒
	停止							
A-1	Netflow	1/8192	6,758,400pps 8000フロー					
A-2	Sflow	1/8192	6,758,400pps 8000フロー					
A-3	Netflow	1/2048	6,758,400pps 8000フロー					
A-4	Sflow	1/2048	6,758,400pps 8000フロー					



①Netflowでは●●●●●●●●●●●●●●●●。
②sFlowはサンプリングレートを1/2048とすると●●●●●●●●●●●●●。
③NetflowとsFlowを比較した場合、●●●●●●●●●●●●●●●。

コレクタとツールたち

コレクタ・解析ツール

- そもそも何のため集めるのか？
  - なんでもできる魔法の箱はありません！
- 目的に従った選択ジューヨー
  - ＮW設計のため
  - 運用監視のため
  - DoS等の攻撃検知のため
  - 顧客へサービス提供のため
  - 証拠保全のため☺
- ここに山ほど
  - http://www.switch.ch/tf-tant/floma/software.html#netflow

ツールたち(商用)

メジャーなものをいくつか(順不同)

- ARBOR Peakflow
- InMon TrafficSentinel
- Foundry Iron View Network Manager
- GenieATM
- NetQoS

ほかいっぱい

ツールたち

- ARBOR Peakflow

  - フリーのツールを試行錯誤する時間と
    ノウハウを買いたい方むけ
  - DDoSとか異常な通信を検知・停止・緩和
    - トラヒックを学習　← 単純な閾値チェックでない！
    - ノウハウのかたまり
  - 最近MPLSのパス内部が見えるようになった
    - MPLS VPNのトラヒック/経路の解析が可能

ツールたち(オープンソース)

使いこなすのが大変なので腕に覚えのある方むけ

- flow-tools
- sflowtool
- Flowd
- nProbe
- ntop
- NfSen
- Nfdump
- ほかいっぱい

FAQ
&
将来の妄想

FAQ

- IPv6への対応は？
  - NetFlow v9,sFlowは対応済だが、エクスポータでの実装は要確認
  - コレクタは一部対応もしくは未対応が大半

- MPLSは？
  - プロトコル的には上記同様
  - コレクタでパス内トラヒック解析できるのはほぼ皆無
    - →Peakflowは見えるよ！

FAQその２

- NetFlow v9対応なら○○ができるんでしょ？
  - 甘い！
  - エクスポータが吐くflowデータをコレクタがすべて解析できるなんて考えは甘すぎ。
  - IPv6,MPLSは前述の通り。
  - ASパスなんかも注意(バグもちアリ)

今後のflowについて勝手な妄想(私見)

- セキュリティ！
  - flowはとってもセンシティブな情報を含む
  - AAAとかもっと活用されるだろう
  - 一般企業内でもフツーに使うようになるかも
  - もしかしたらCor●gaの箱でも吐くようになるかも

でもね。

- 基本的にNetFlowはエクスポータ・コレクタが近くにあることが前提で設計している
- UDPじゃ怖くて使えない
- サンプリングで情報落ち問題もある

で、

- TLS/IPsecでのflow情報のガード　(→IPFIX)
- コレクタの防御
- Per Packetでもへこたれない仕組み

We are here.

On Customers' Side.