Non Sampledトラフィック解析の応用例　－　iDC編

さくらインターネット（株）
技術部　ネットワークチーム
大久保 修一　ohkubo@sakura.ad.jp

さくらインターネットって？

いわゆるインターネットデータセンターを
運営している会社です。

専用サーバ	→	約6,000台
ホスティング	→	約12万アカウント、 収容サーバ数：約1,000台
ハウジング	→	約450回線
トランジット	→	約40回線

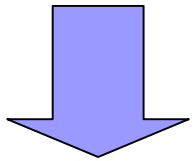
バックボーン容量：102Gbps （2006年12月現在)

AS番号：9370(東京)、9371(大阪)、7684(IPv6)

DoSアタックの憂鬱

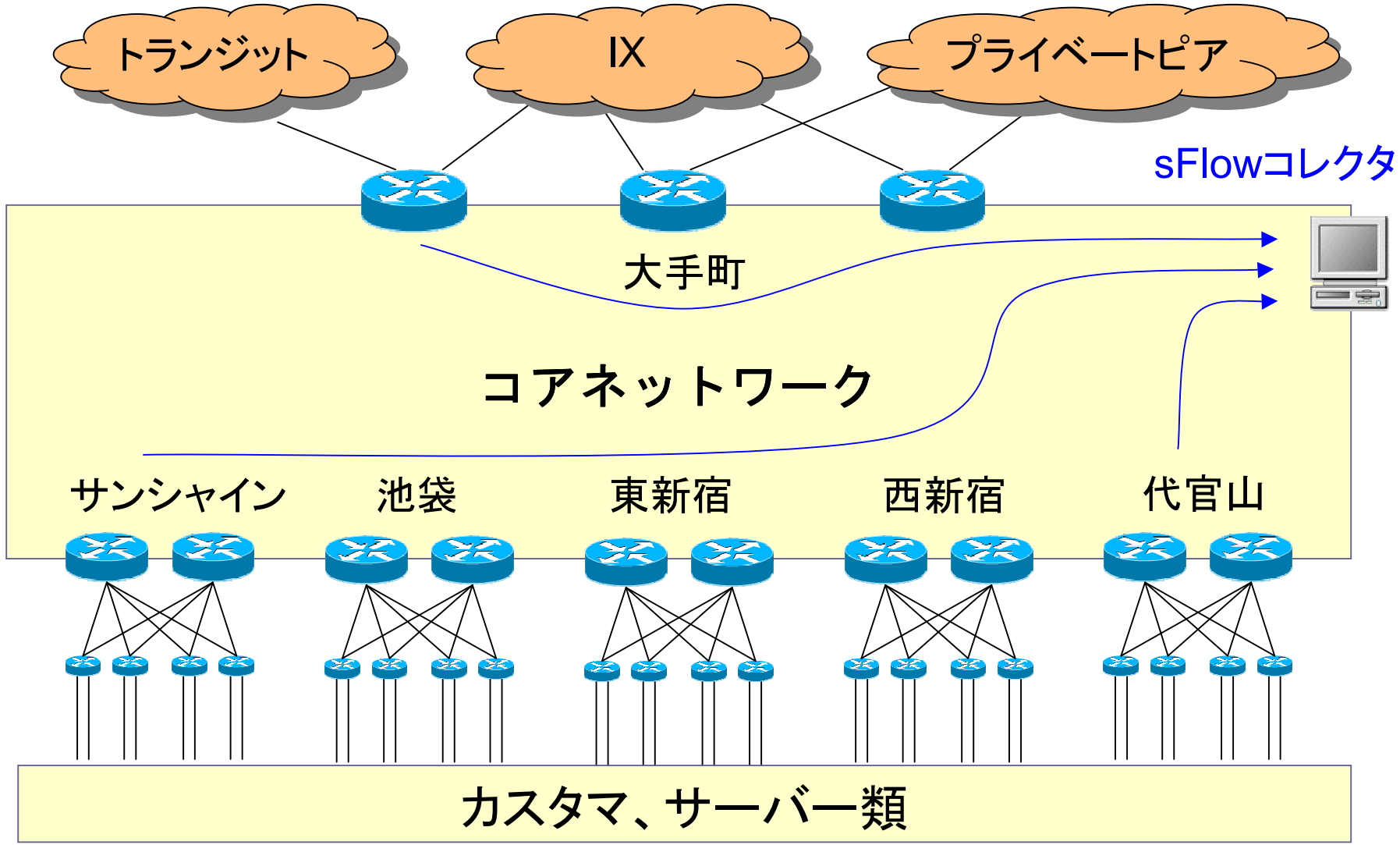
DoSアタックに狙われるサーバもたくさん (>_<)

・某有名サイトとか・・・
・SPAMをまいてDoSの対象に・・・
・乗っ取られて踏み台に利用された人とか・・・

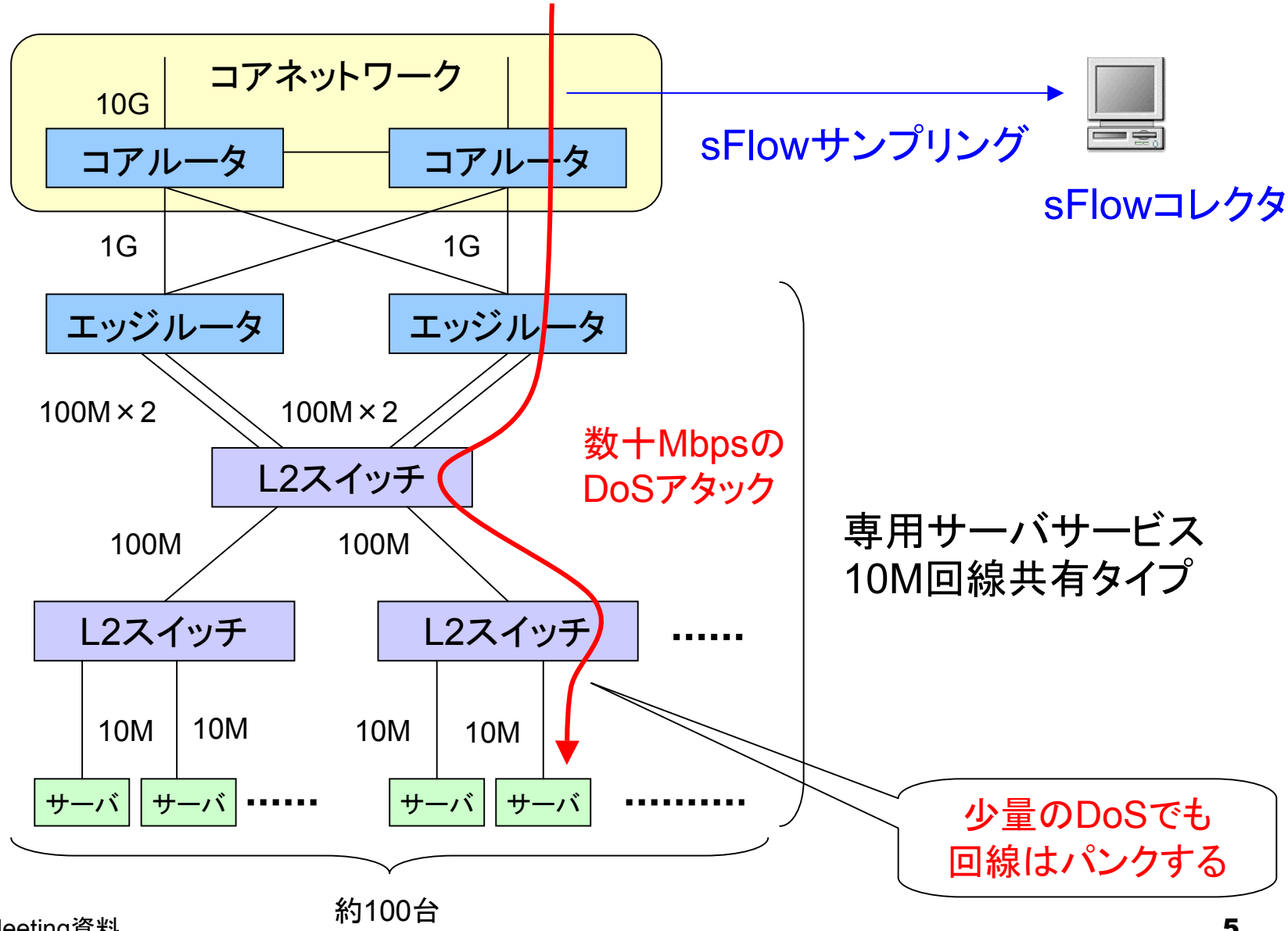


現在、sFlowで検出を行っていますが問題点が・・

sFlowによるDoSアタック検出

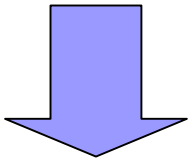


sFlowによるDoSアタック検出



Non SampledによるDoSアタック検出

- 1G～10Gの回線に流れている数十MbpsのDoS
  - 十分なサンプルが収集できるまで時間が必要
  - リアルタイム検出は難しい



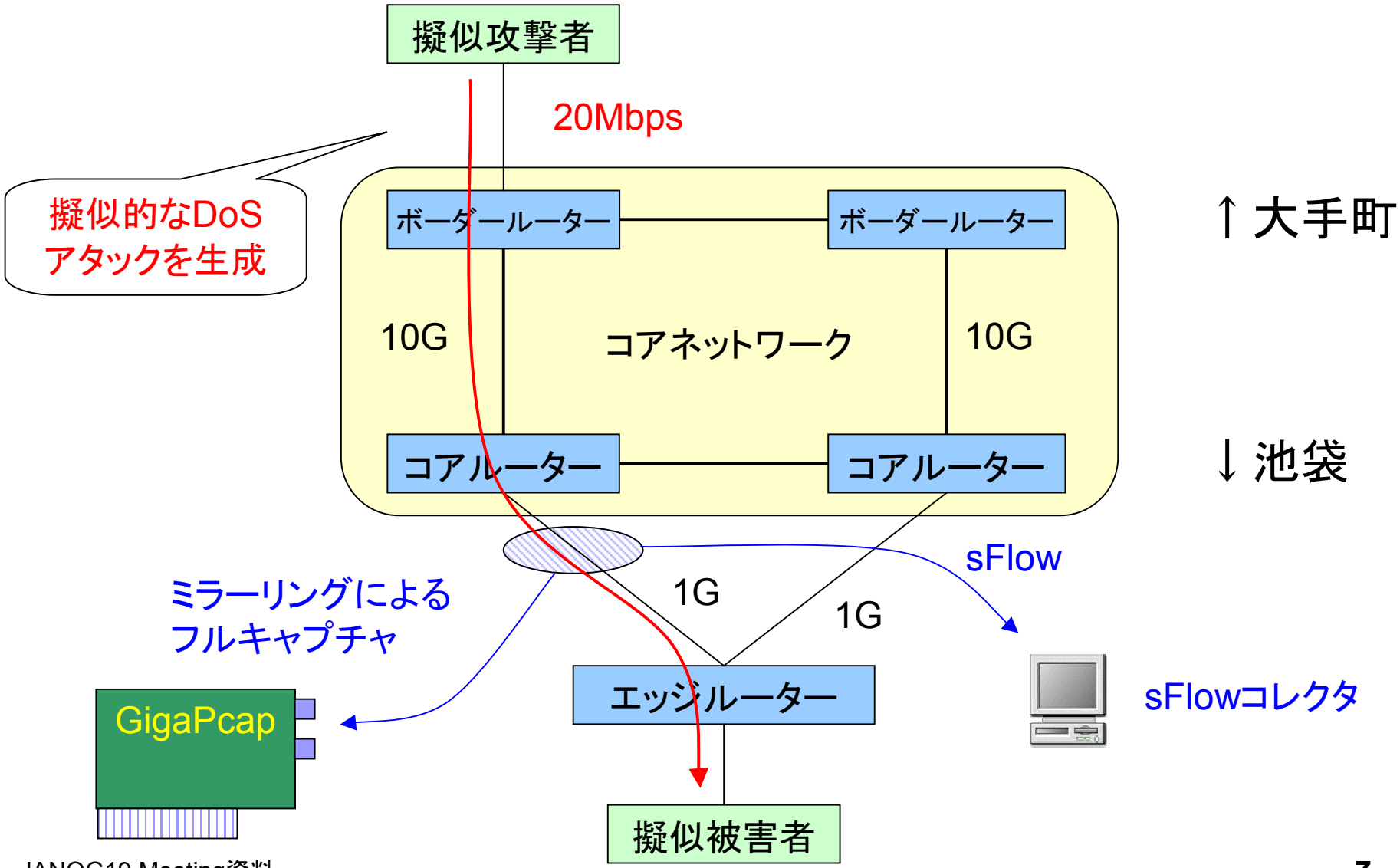
そこで・・・

GigaPcapを使って、全てのパケットを調査してみると！？

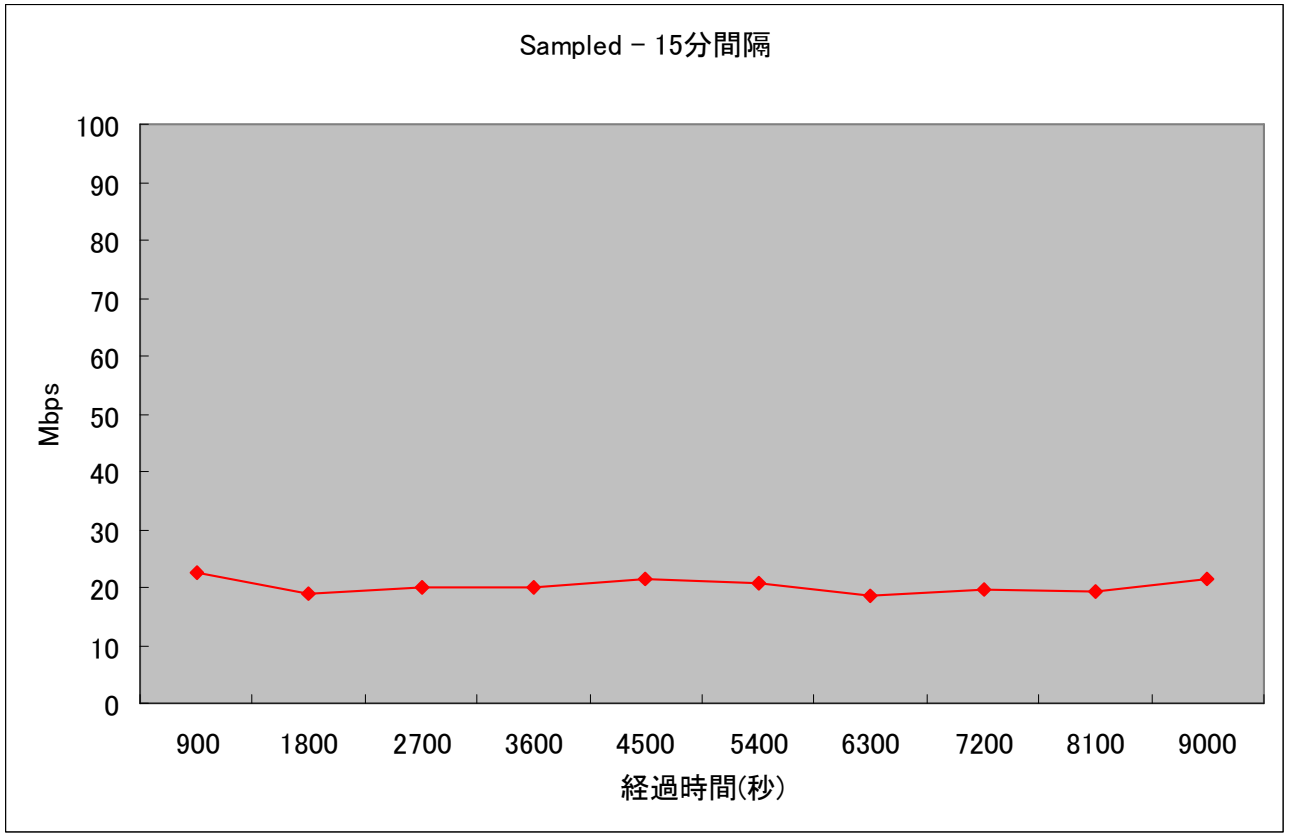
＝Non Sampled

sFlowとGigaPcapで比較してみました。

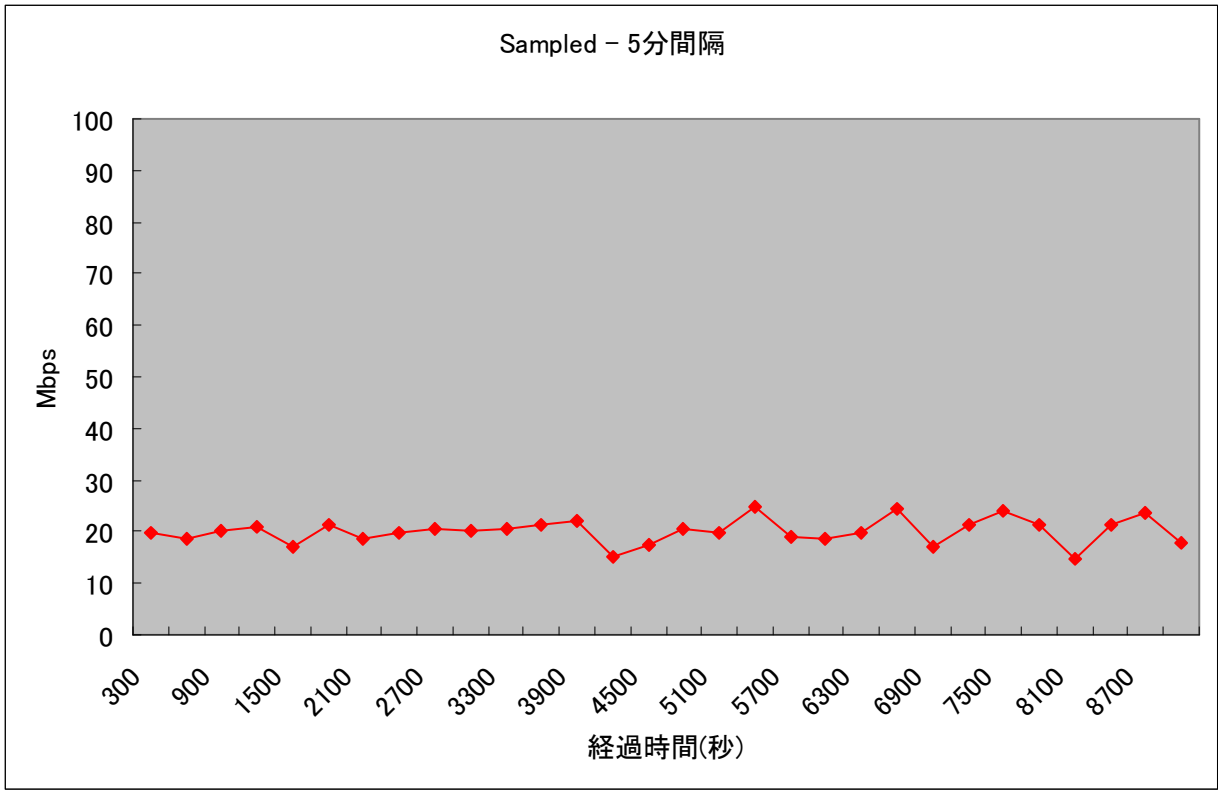
Sampled vs Non Sampled比較環境



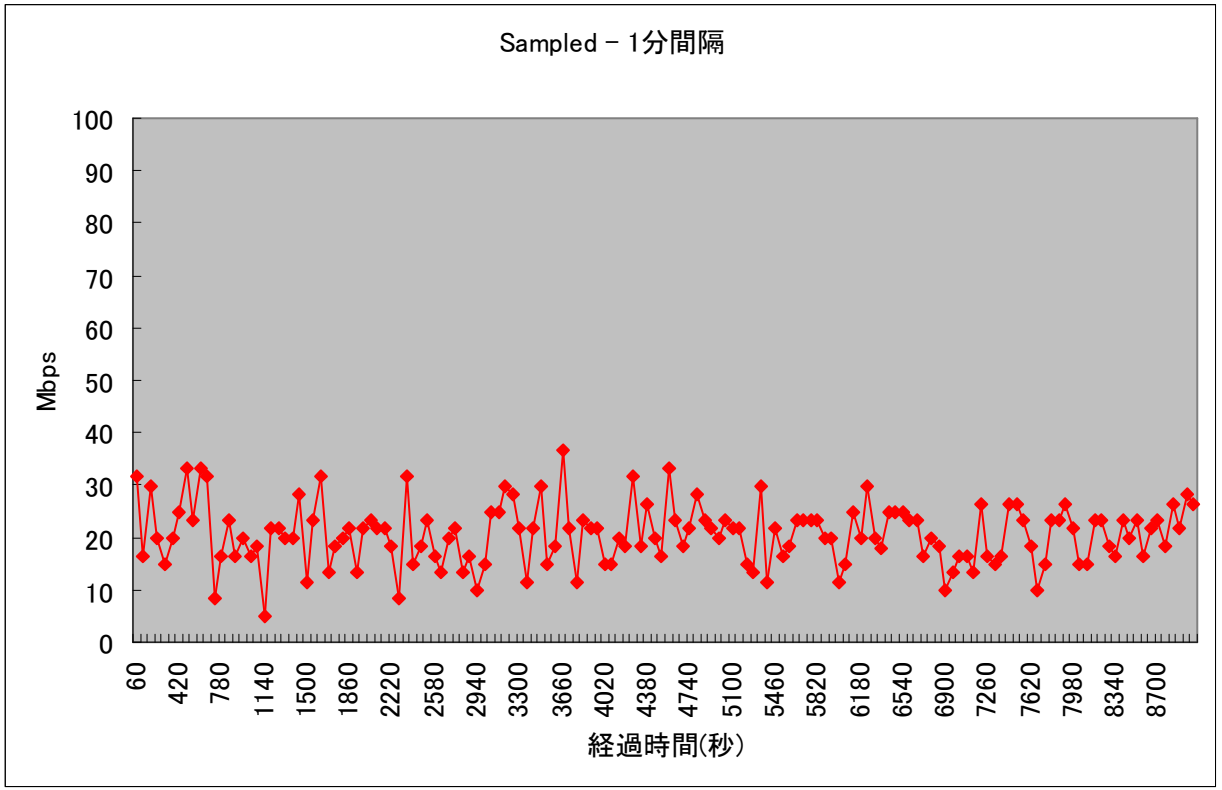
Sampledの場合 – 15分間隔



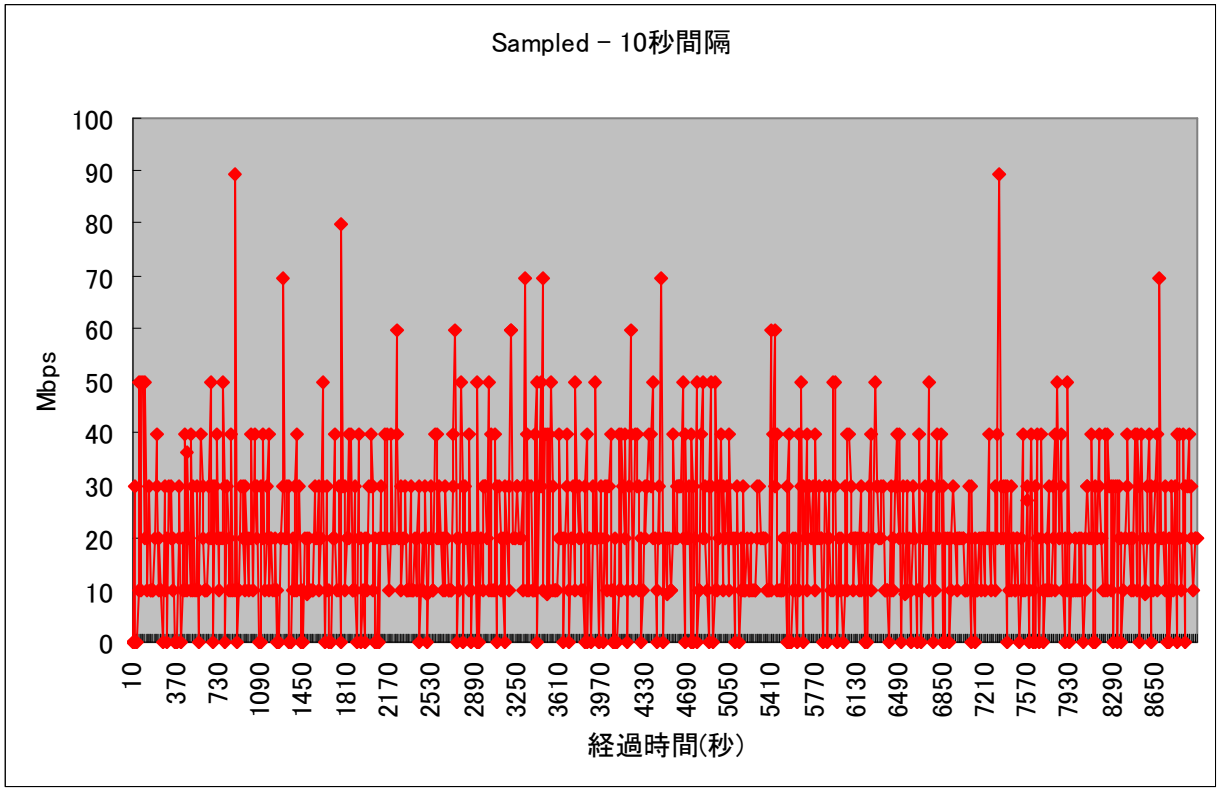
Sampledの場合 – 5分間隔



Sampledの場合 – 1分間隔

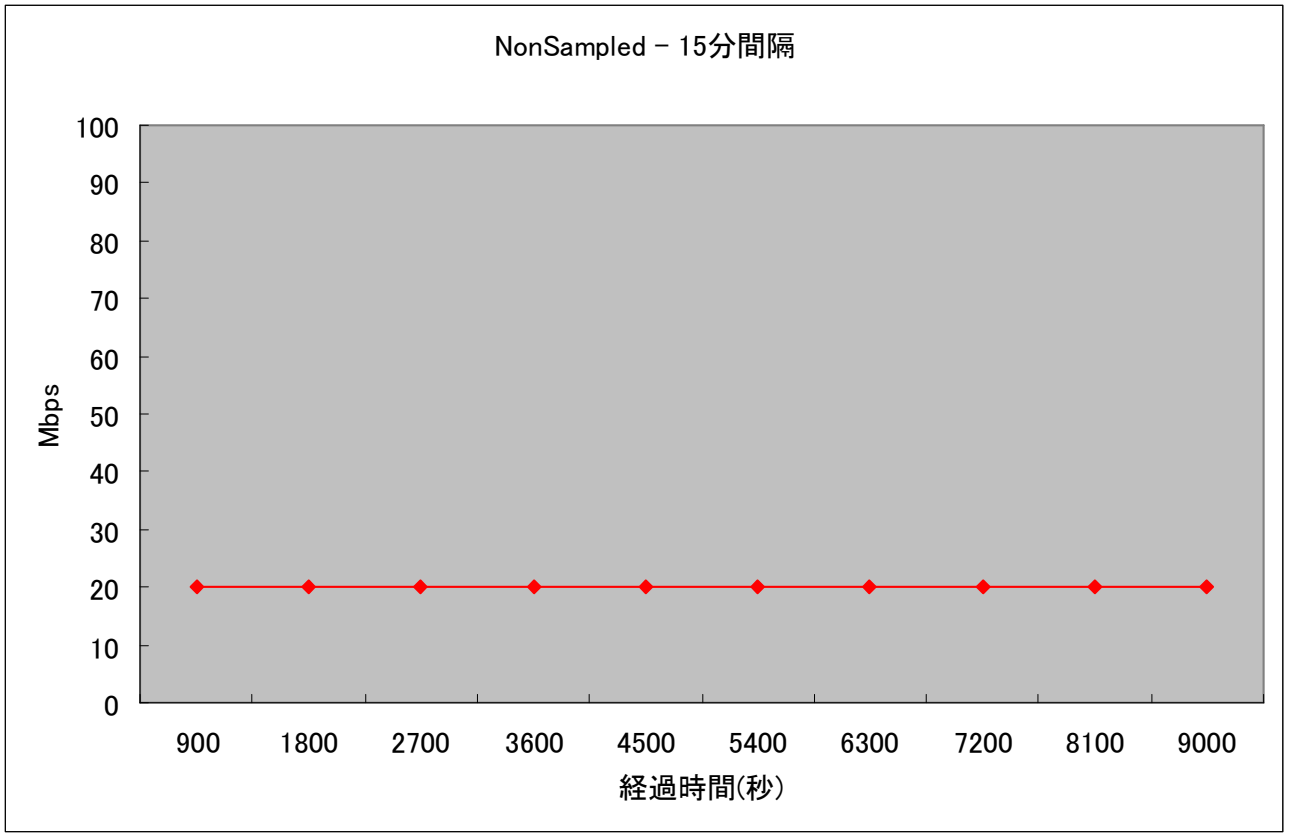


Sampledの場合 – 10秒間隔

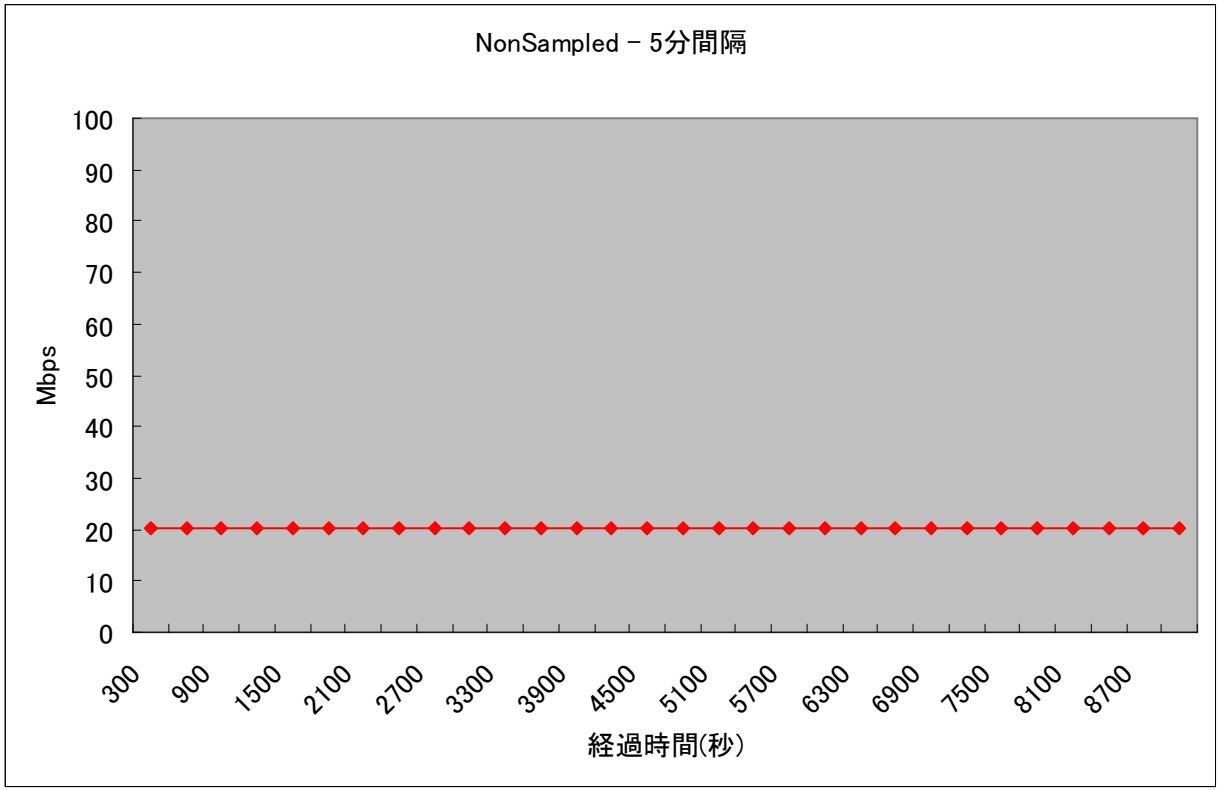


DoSアタックのリアルタイム検出は難しい

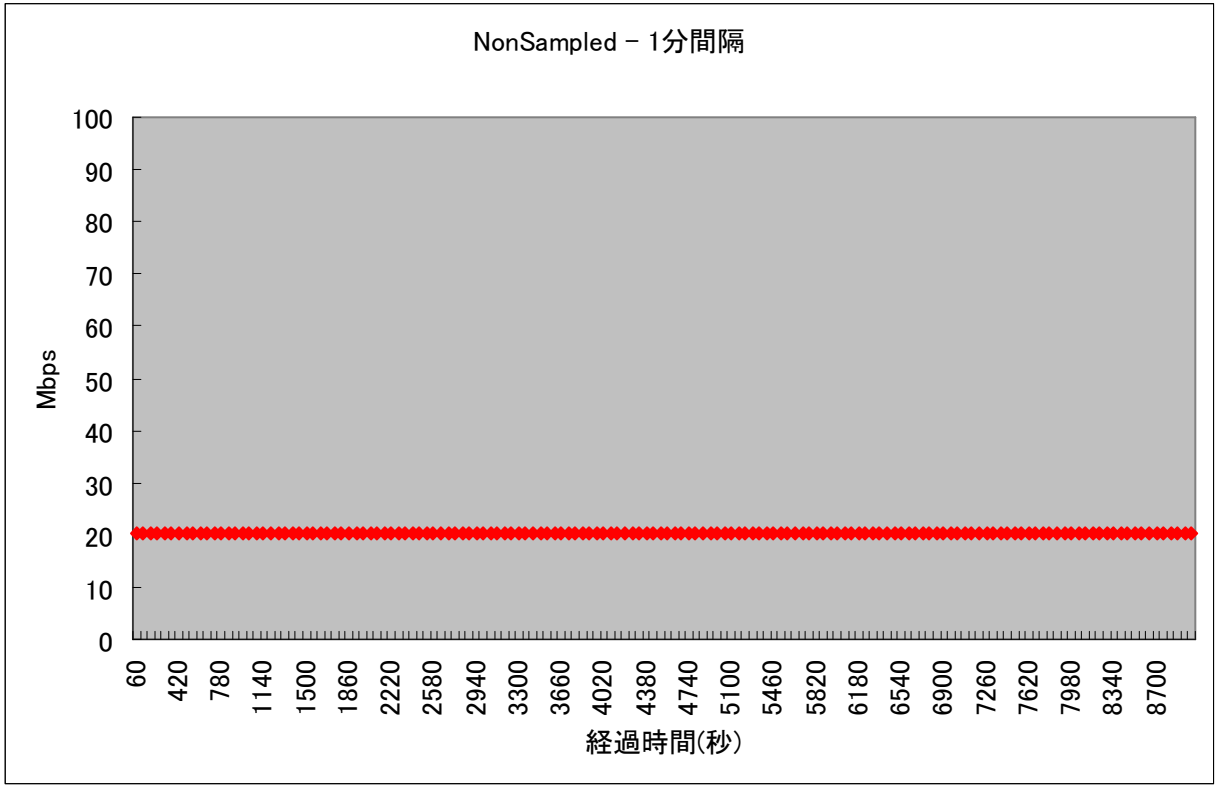
Non Sampledの場合 – 15分間隔



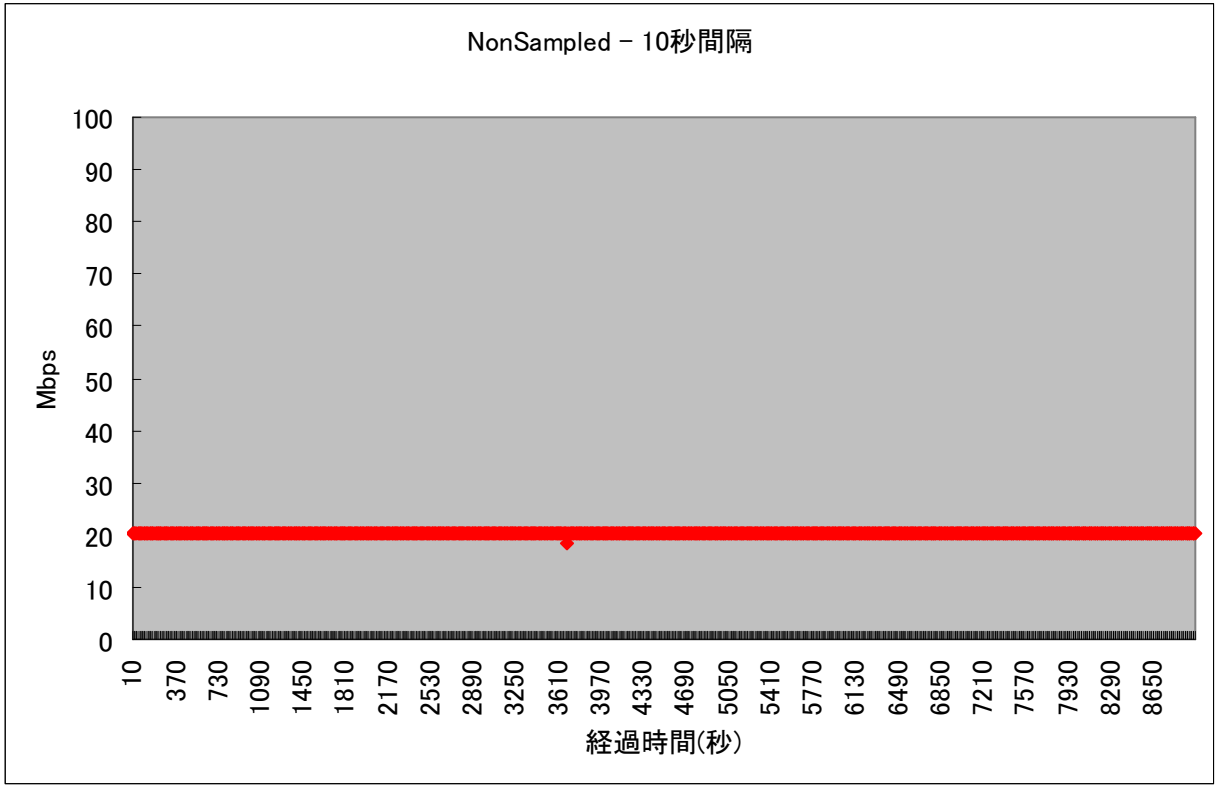
Non Sampledの場合 – 5分間隔



Non Sampledの場合 – 1分間隔



Non Sampledの場合 – 10秒間隔



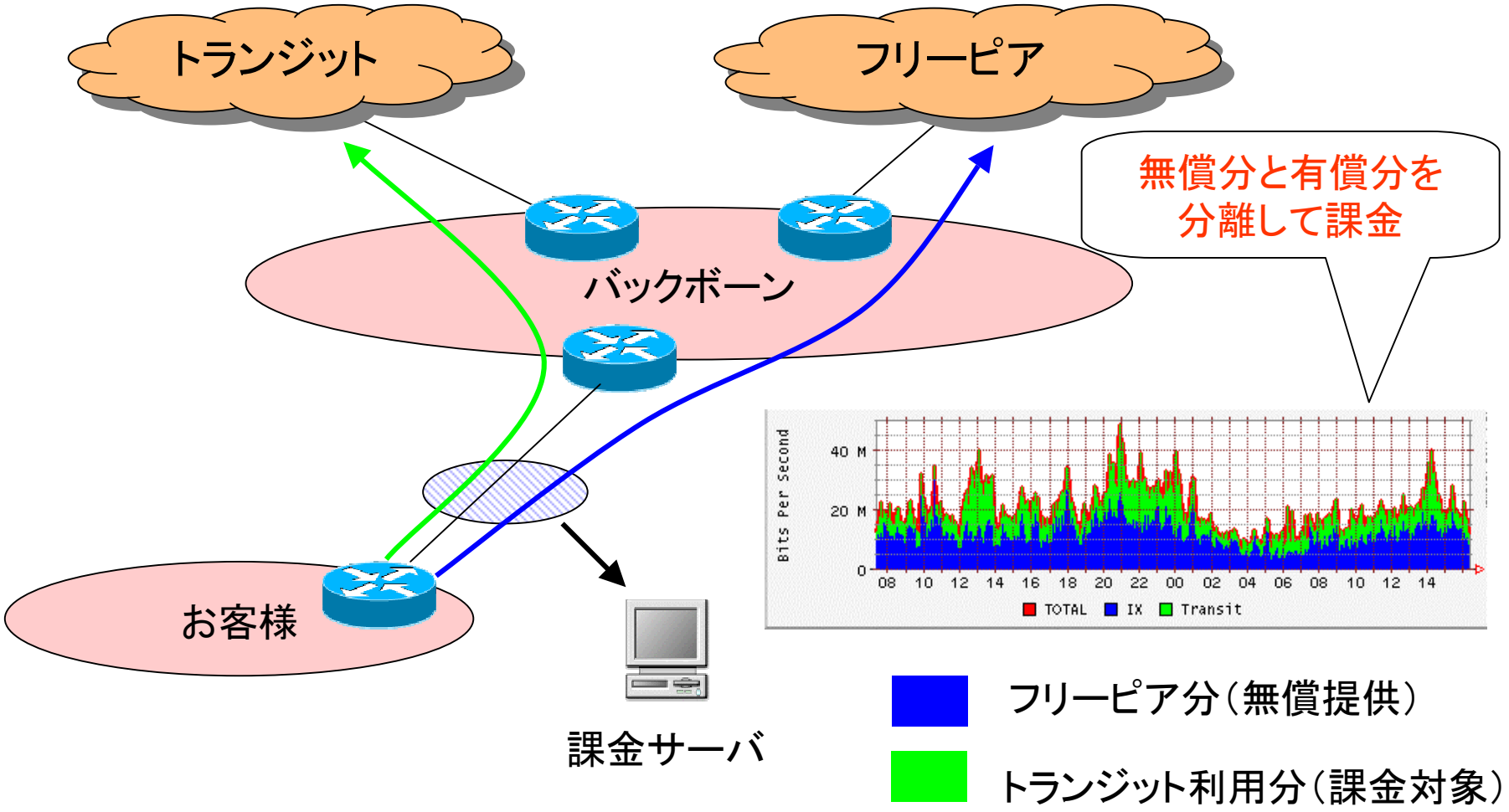
高精度！
DoSアタックのリアルタイム検出が可能！

実際の検出例

```
IP xx.xx.60.6.80     > xx.xx.12.207.28805: S 884726201:884726201(0)
IP xx.xx.89.130.80   > xx.xx.12.207.8:     S 2465266801:2465266801(0)
IP xx.xx.43.220.80   > xx.xx.12.207.4135:  S 269923584:269923584(0)
IP xx.xx.105.26.80   > xx.xx.12.207.104:   S 353258233:353258233(0)
IP xx.xx.55.249.80   > xx.xx.12.207.49283: S 2396364559:2396364559(0)
IP xx.xx.248.4.80    > xx.xx.12.207.180:   S 1281806202:1281806202(0)
IP xx.xx.7.137.80    > xx.xx.12.207.92:    S 2182644779:2182644779(0)
IP xx.xx.159.34.80   > xx.xx.12.207.49250: S 758383403:758383403(0)
IP xx.xx.68.100.80   > xx.xx.12.207.126:   S 3064163126:3064163126(0)
IP xx.xx.130.80      > xx.xx.12.207.32847: S 1238623010:1238623010(0)
IP xx.xx.11.182.80   > xx.xx.12.207.24266: S 1945505603:1945505603(0)
IP xx.xx.117.166.80 > xx.xx.12.207.62037: S 3030352818:3030352818(0)
```

※tcpdumpの出力結果を加工、一部抜粋

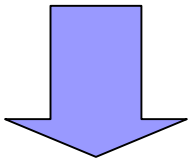
Non Sampledの応用例　その2



トランジットの一部メニューで提供してます

宛先別トラフィック課金

- Sampledでもできなくないが精度が・・
- お客様は当然、精度を要求される

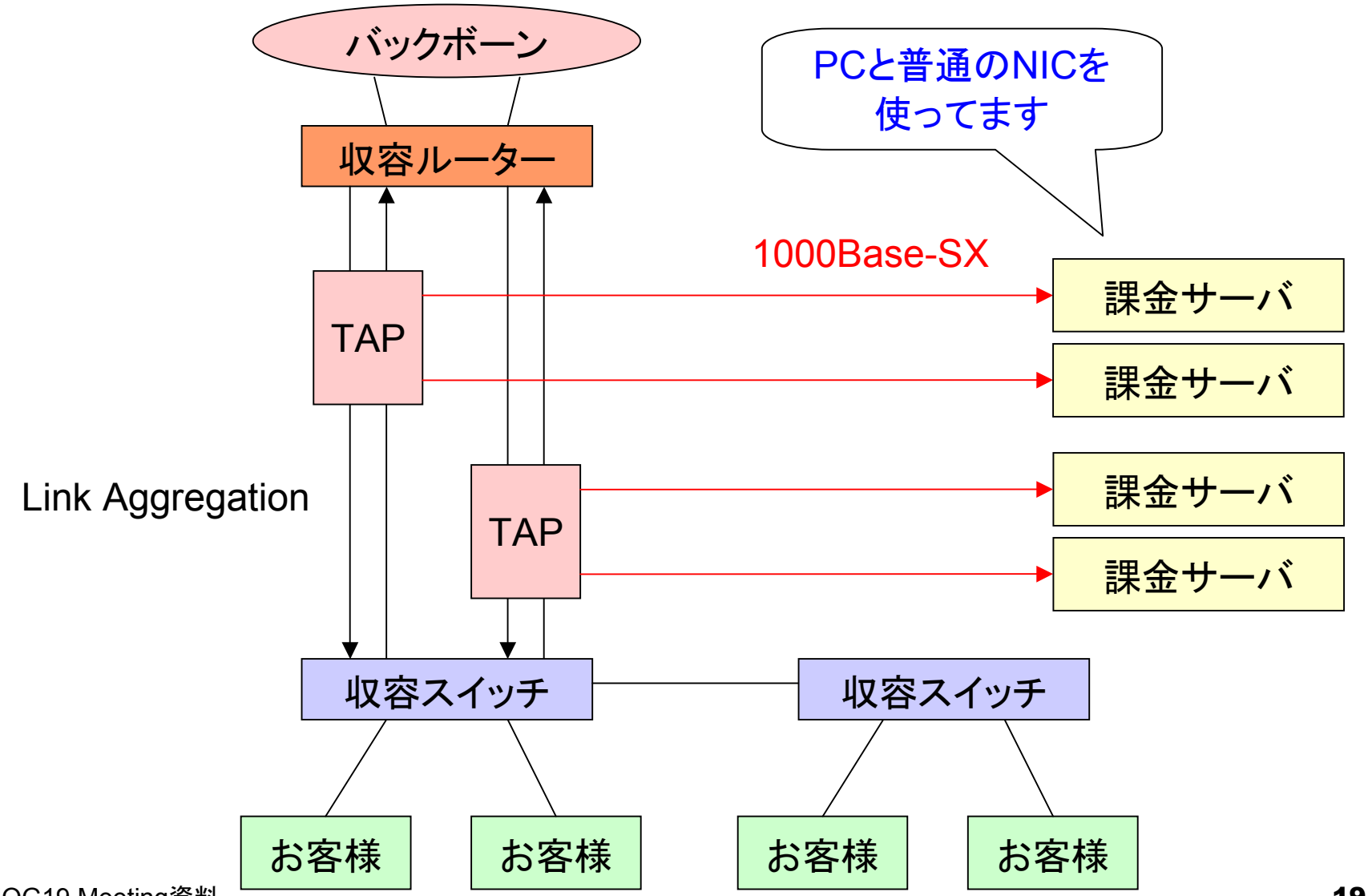


そこで・・・

Non Sampledで、全てのパケットをモニタ！

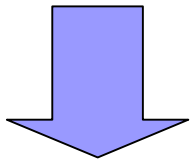
正確な算出が可能になる！！

宛先別トラフィック課金の実装



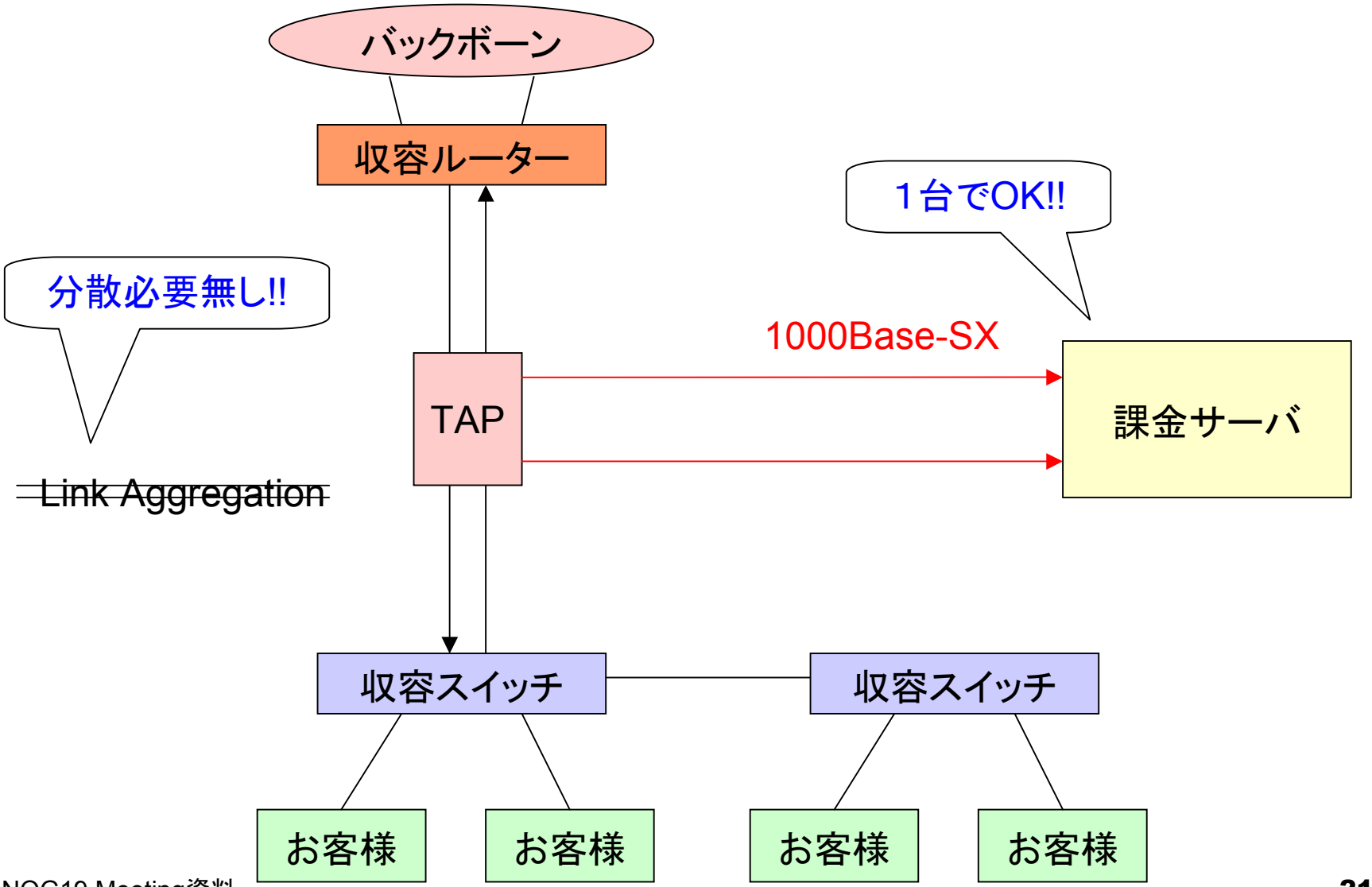
GigaPcapを使うと・・・

- ハードウェアでフィルタ処理
  - 監視対象外のトラフィックは、最初から見ない
- ヘッダ部のみ抽出
  - CPUで処理するデータの量削減
- １枚で2ポート（inとout）監視できる



- 課金サーバ1台あたりの処理能力拡大
- シンプルなシステム構成！！

宛先別トラフィック課金の実装



Discussion!

- 大規模なDoSアタックであれば検出しやすいが・・
  - すでに優秀な箱が売られてたり(P〇akFl〇wとか・・)
- 個別サーバが狙われるような小規模のDoSアタックは意外と把握しにくいのでは？
  - 皆さんどうしてますか？
  - 困ってませんか？
  - お客さんから問い合わせを受けてわかったとか・・・
- 宛先別課金が簡単にできるようになるとして、、、
  - そもそも需要はどれくらいあるのかしら？
  - 既にやってます！っていうところ、ありますか？
  - どのようにやってます？