

Operators' Life with no-Sampling Flow Data

ベライゾン ビジネス
伊賀野 康生

Yasuo.Igano@verizonbusiness.com



前回のJANOG19にて

『トラフィックデータ取れるんです
– 高精度データ収集編』と題して、

通常のルータが吐く**Sampling Flow Data**

VS

Probeを使って収集した

no-Sampling Flow Data

その違いについて発表しました

http://www.janog.gr.jp/meeting/janog19/2006/10/post_25.html

で、復習

データをSampling(間引き)すると
見え方が違うものがある

少量でも影響の大きいFlow Dataを
見るにはno-Samplingがイイ!!

特にセキュリティ的な観点からは
応用範囲が広そう

でも、データ量が膨大で大変だよね

このJANOG20では



オペレーションの現場で更に使い込み、
現場で使いたいモノを考えてみました

no-Sampling Flow Dataは
ISPのオペレータをHappyにするのか？

発表者紹介

現在

倉敷ケーブルテレビ 小山さん
Flow分析のASPソリューション

さくらインターネット 大久保さん
DoS攻撃の検出と対応

将来

NTT情報流通プラットフォーム研 近藤さん
お客様に優しいDoS対応

NTT情報流通プラットフォーム研 石橋さん
サービスレベルの計測とBotnetの検出

各発表者さんの発表

おさらい

できる事

現在

倉敷ケーブルテレビ 小山さん
Flow分析のASPソリューション

日々の
運用

さくらインターネット 大久保さん
DoS攻撃の検出と対応

DoSとの
戦い

できそうな事

これから

NTT情報流通プラットフォーム研 近藤さん
お客様に優しいDoS対応

NTT情報流通プラットフォーム研 石橋さん
サービスレベルの計測とBotnetの検出

応用編