BoFまとめを企画いただいた
冨永さんに感謝！

見つけた！
モダンなトラフィック可視化 BoF
まとめ

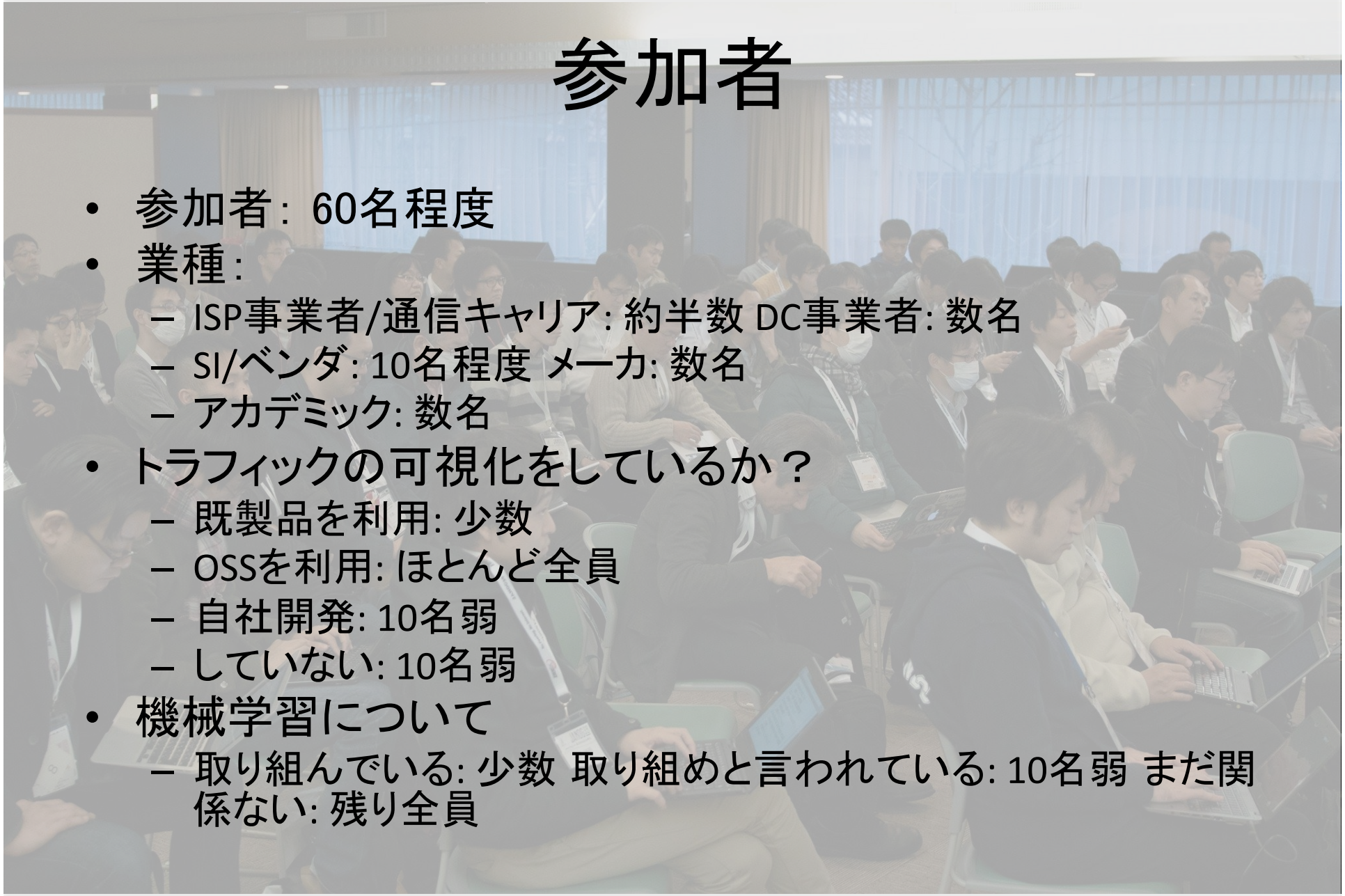
JANOG 39.5 / 2017.04.14

西塚要 @__kaname__

見つけた！
モダンなトラフィック可視化 BoF

- 内容:
  - 新しいOSSの可視化ツールの導入事例・利点/欠点を相互紹介する
- 目的:
  - 新しい可視化ツールの導入のハードルを下げる

参加者



- 参加者 : 60名程度
- 業種 :
  - ISP事業者/通信キャリア: 約半数 DC事業者: 数名
  - SI/ベンダ: 10名程度 メーカ: 数名
  - アカデミック: 数名
- トラフィックの可視化をしているか？
  - 既製品を利用: 少数
  - OSSを利用: ほとんど全員
  - 自社開発: 10名弱
  - していない: 10名弱
- 機械学習について
  - 取り組んでいる: 少数 取り組めと言われている: 10名弱 まだ関係ない: 残り全員

モダンなOSSによるトラフィック可視化

- 従来

統合型のソフトウェアや
アプライアンス装置

- 現在

  - ほぼ同等のことが、各機能を持つOSSの組み合わせで実現できるようになっている。
  - 色々なデータソースからの可視化を統合することができる。

事例集(URL)

説明文	URL
EFK構成によるflowの可視化事例	http://labs.gree.jp/blog/2015/12/15515/
NANOG66: オープンソースでDDoS検知と対策	https://www.nanog.org/sites/default/files/OpenSource-DDoS.pdf
JANOG33: イベントトラフィックに対するトラフィックエンジニアリング	https://www.janog.gr.jp/meeting/janog33/doc/janog33-traffic-kamei-1.pdf
JANOG38: peering見えるか自力でやってみた	https://www.janog.gr.jp/meeting/janog38/program/pa.html
NetOpsCoding#3: Monitoring Intelligence（Microsoft 北島さん）	http://www.slideshare.net/netopscoding/monitoring-intelligence
オープンソースでキメる DDoSトラヒック分析 (田島さん)	https://www.janog.gr.jp/meeting/janog34/program/lt_tanal.html
neflow見てみた(ヨシノジュンペイさん)	https://www.janog.gr.jp/meeting/janog34/doc/janog34-lt4bg-yoshino-1.pdf
Telemetry (土屋さん)	https://www.janog.gr.jp/meeting/janog37/program/telemetry.html
pcapファイルをNetFlowに変換した際にフロー開始時刻が未来にずれた件と修正方法	http://qiita.com/t_umeno/items/25b6d80addde277cdcb8

Google Spreadsheetを利用した事前アンケートより

事例集(発表)

- FastNetMonを試してみた
  - 石崎豊(フリービット株式会社)
- InfluxDataのTICK Stack(Telegraf, InfluxDB, Chronograf, Kapacitor) on DockerでNW監視と可視化
  - 堀内晨彦(NTTコミュニケーションズ)
- データ収集・解析基盤の構築苦労話
  - 亀井聡(NTTコミュニケーションズ)
- pmacct->kafka->presto->re:dashを使った高速なflow解析
  - 西塚要(NTTコミュニケーションズ)

Grafanaで可視化すると

情報量少ない..

Kibanaによる可視化

- **可視化ツール「Kibana」**
  - Sensuは監視のコアのみ提供
  - ElasticsearchのデータをWeb上で可視化

- **ダッシュボードは自動生成**
  - 構成管理ツール「Ansible」を使用
  - ポート数に合わせてクエリとパネルを生成
  - github.com/hico-horiuchi/ansible-playbooks

ダッシュボードを作成

TICK Stackとは?

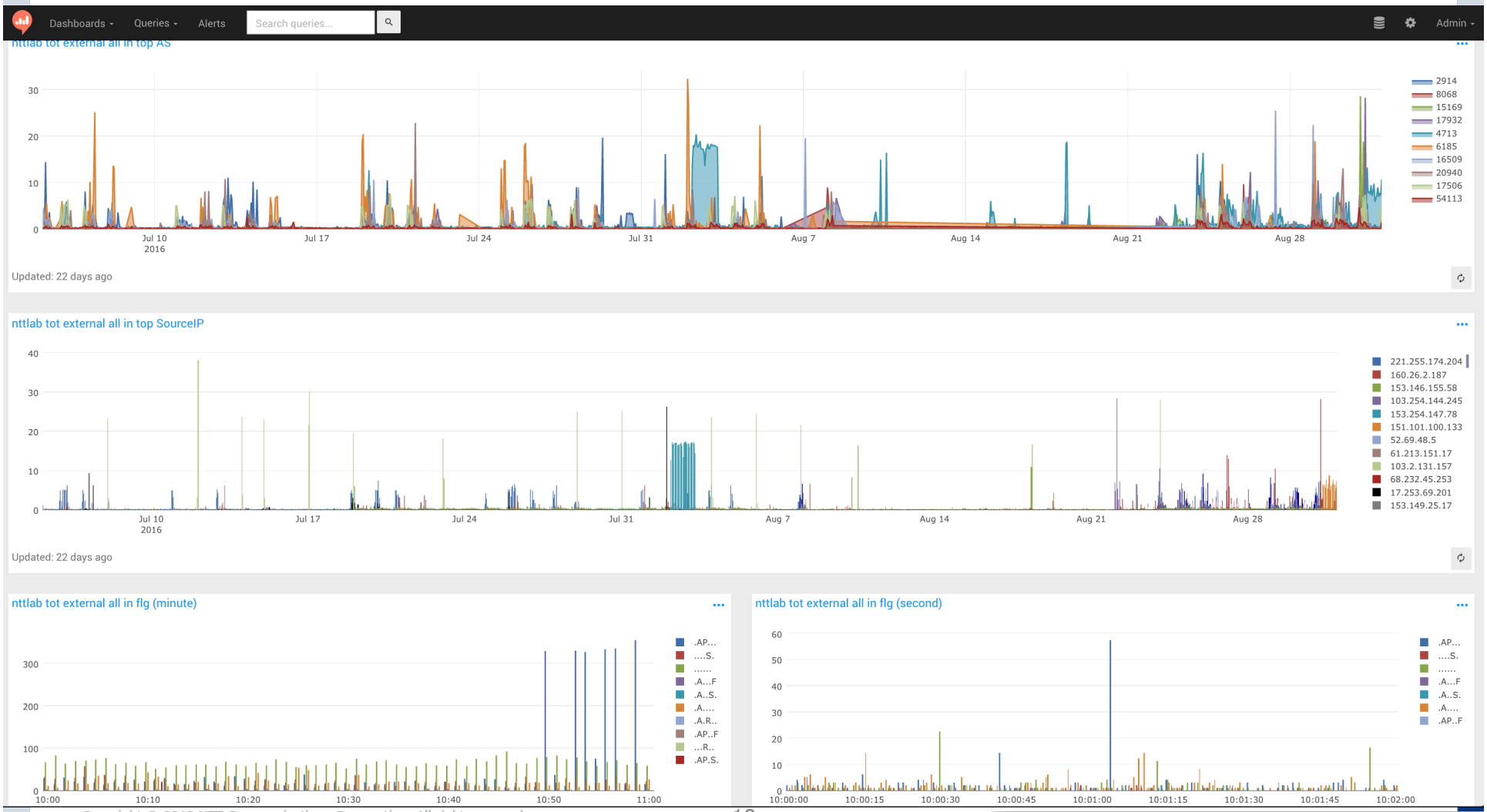
時系列データの収集・保存・可視化・監視
するためのソリューション

Telegraf	：メトリクスコレクタ
InfluxDB	：時系列データベース
Chronograf	：グラフ化・可視化
Kapacitor	：アラート・異常検知

全てGo言語製なので軽量、高速

Re:dashで可視化

- Prestoでの高速なクエリ実行
  - TopN分析:1ヶ月分のflowデータに対して数秒で結果を返す



まとめ

- こちらから伝えられたもの
  - 各ツールのはまったポイント・使い勝手
  - 連携部分の苦労(監視や安定性など)
- 伝えきれなかったもの
  - それでも、既存の慣れたMRTG/Cactiなどのツールと比べて、「導入のハードルが高い」
  - 可視化の目的自体にも、もっと触れてほしかった