# 見つけた！
# モダンなトラフィック可視化 BoF

JANOG39 Day1 BoF
2017年1月18日

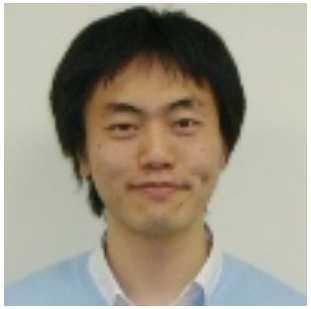
西塚要
@__kaname__
kaname@nttv6.jp



NTT Communications Global ICT Partner
Innovative. Reliable. Seamless.

# 自己紹介：西塚 要 (にしづかかなめ)

- 2006年 NTTコミュニケーションズ入社
  - OCNアクセス系ネットワークの設計
  - 大規模ISP保守運用サービス担当
- 現在、研究開発部門にてDDoS対策ソリューション関連技術およびデータ解析技術開発とIETF提案活動に従事



【JANOG活動履歴】

- JANOG28 実行委員長
- JANOG32 「HTTP 2.0のインパクト」
- JANOG37 「できる！データドリブン障害検知」
  「増え続けるDDoS攻撃に対抗するために事業者間で協力してできること」

NTT Communications Global ICT Partner Innovative. Reliable. Seamless.

# トラフィック可視化

# トラフィック可視化の目的

- トラフィック可視化：膨大なトラフィックデータから、情報あるいは知識を抽出する

- 人間が見て：
  - トラフィックの特性を直感的に理解する
  - 短期的・長期的な傾向を把握する
  - それを計画・運用・監視・対策に活かす
- 機械が見て：
  - 障害の自動検知を行う

可視化自体が目的ではなく、可視化後のアクションを導出し、その効果を測定するプロセスが重要

# アイスブレイク

- BoFに参加いただきありがとうございます: 60名程度
- みなさまの業種について
  - ISP事業者/通信キャリア: 約半数 DC事業者: 数名 アカデミック: 数名 SI/ベンダ: 10名程度 メーカ: 数名

- トラフィックの可視化をしている？
  1. 既製品を利用: 少数
  2. OSSを利用: ほとんど
  3. 自社開発: 10名弱
  4. していない: 10名弱
- 機械学習について
  1. 取り組んでいる: 少数
  2. 取り組めと言われている: 10名弱
  3. まだ関係ない: ほとんど

# トラフィック可視化事例 URLs

| 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 |

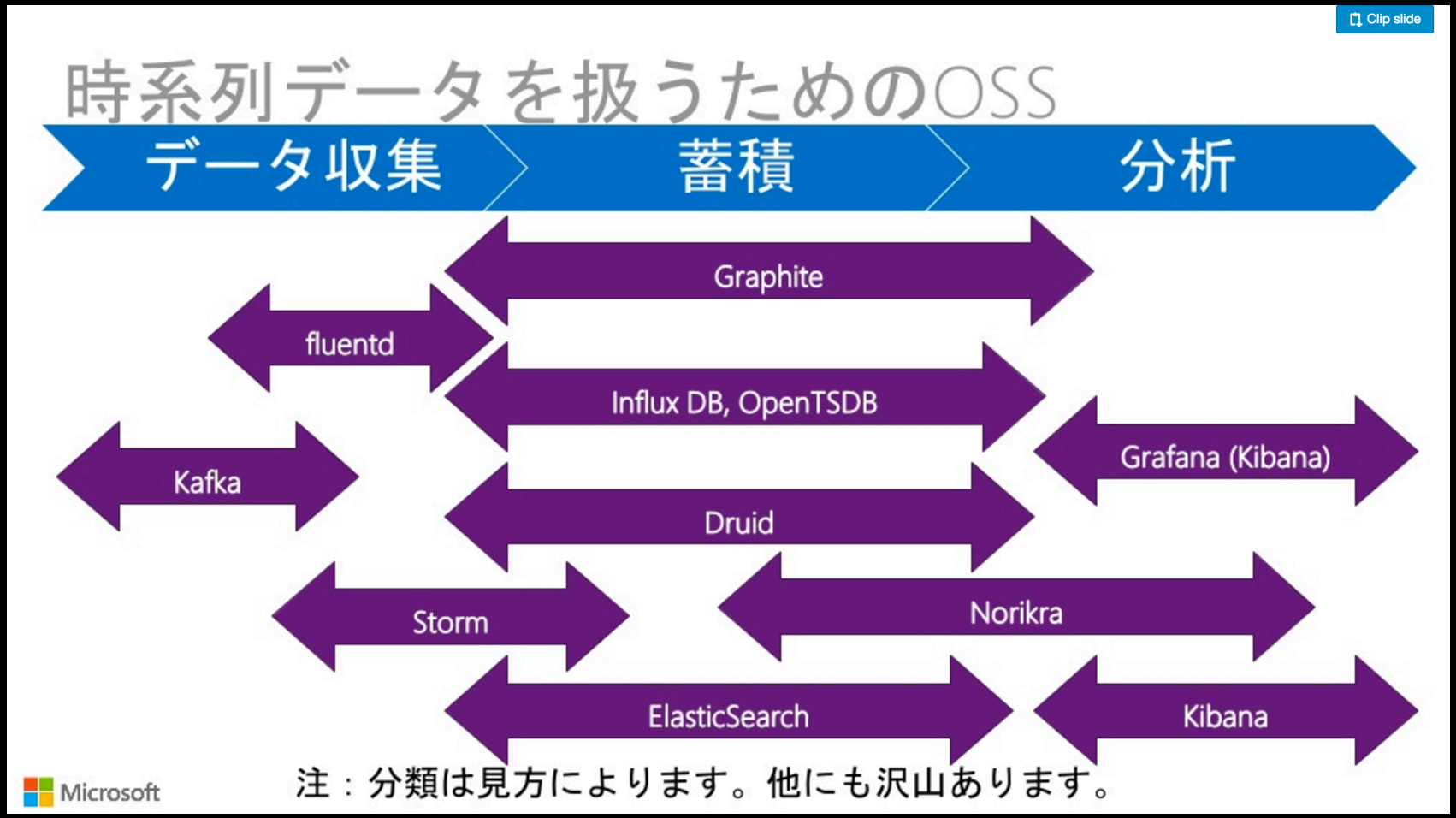
# モダンなOSSによるトラフィック可視化

- 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。




NetOpsCoding#3: Monitoring Intelligence（Microsoft北島さん）
http://www.slideshare.net/netopscoding/monitoring-intelligence

# 実際に手を動かしてみると…

- 解析機能をどの部分に入れるか？
- 追加情報の付与はどこで行うか？
- 解析結果を再蓄積するには？
- 短期的な解析なのか、長期的な解析なのか？
- 誰のための可視化なのか？(人か、マシンか)
- アクションのトリガーはどこか？

- 使えそうなOSSの組み合わせが多く、手探りでツールを試す日々
  - そうだ、JANOGでノウハウ共有しよう！

# 事例紹介パート

# 事例紹介

- 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)

# 即席パネル

# 即席パネル

1. はまったポイント
2. 監視をどうしてるか
3. データが全部入ってるかをどう担保するか
4. 公開データとの組み合わせアイデア
5. 取得したデータの冗長化、バックアップ等をどうしているか
6. PCAPファイルからpmacctなどで変換したNetFlow,IPFIXなどのフローデータを取り扱う事例を知りたいです。
7. (+会場質問)

# 最後に

- BoFに参加いただきありがとうございました
- 有益な情報交換だったでしょうか？
- 今後についてのアンケート
  1. 今回で十分
  2. まだ足りない-> 多数