JANOG58

あのネットワーク技術の今と予想する10年後

セッション Observability / Telemetry

安藤 格也 / LINEヤフー株式会社

自己紹介

LINEヤフー株式会社
安藤 格也 / Kakuya Ando
GitHub: @servak

- **経歴**: Webサービス開発 → NW運用 → NW運用のツール開発(現在)
  - 直近は Network Agent PF 開発
- **OSS**: mping (NW運用者向けpingコマンド)
- **JANOG登壇歴**: JANOG40
- **プライベート**: 子供3人（出張自体が久々で嬉しい）

はじめに - 前提の整理

概要文: **「SNMP中心の監視から Telemetry を活用した可視化へ」**

- SNMP は Metrics 取得手段の **1 つ**
- 対比軸は **Pull vs Push**

→ 今日は Pull 型主流の Metrics に Push 型が入ってくる話

今日話すこと

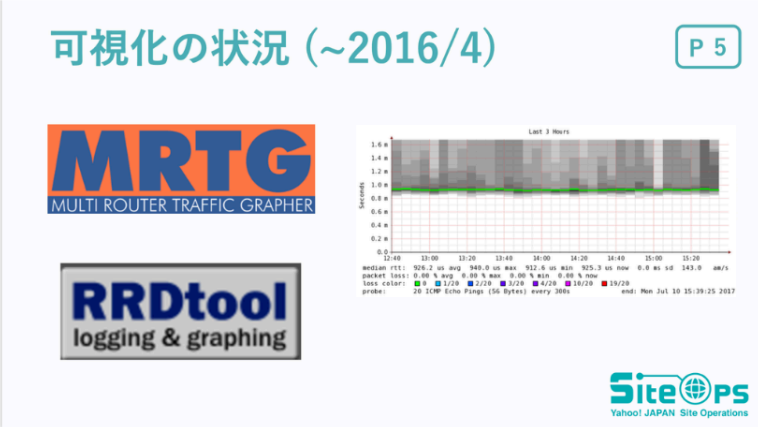
- **この 10 年**: Metrics 取得方法の変化
  - SNMP / Exporter / **Streaming Telemetry**
- **次の 10 年**: 3 つの方向性
  - **Traces** が進む
  - Metrics は **Streaming Telemetry 主体へ**（SNMPは縮小）
  - 読み手の変化 — **状態** が要る

この 10年

Metrics取得方法の変化

SNMP / Exporter / Streaming Telemetry

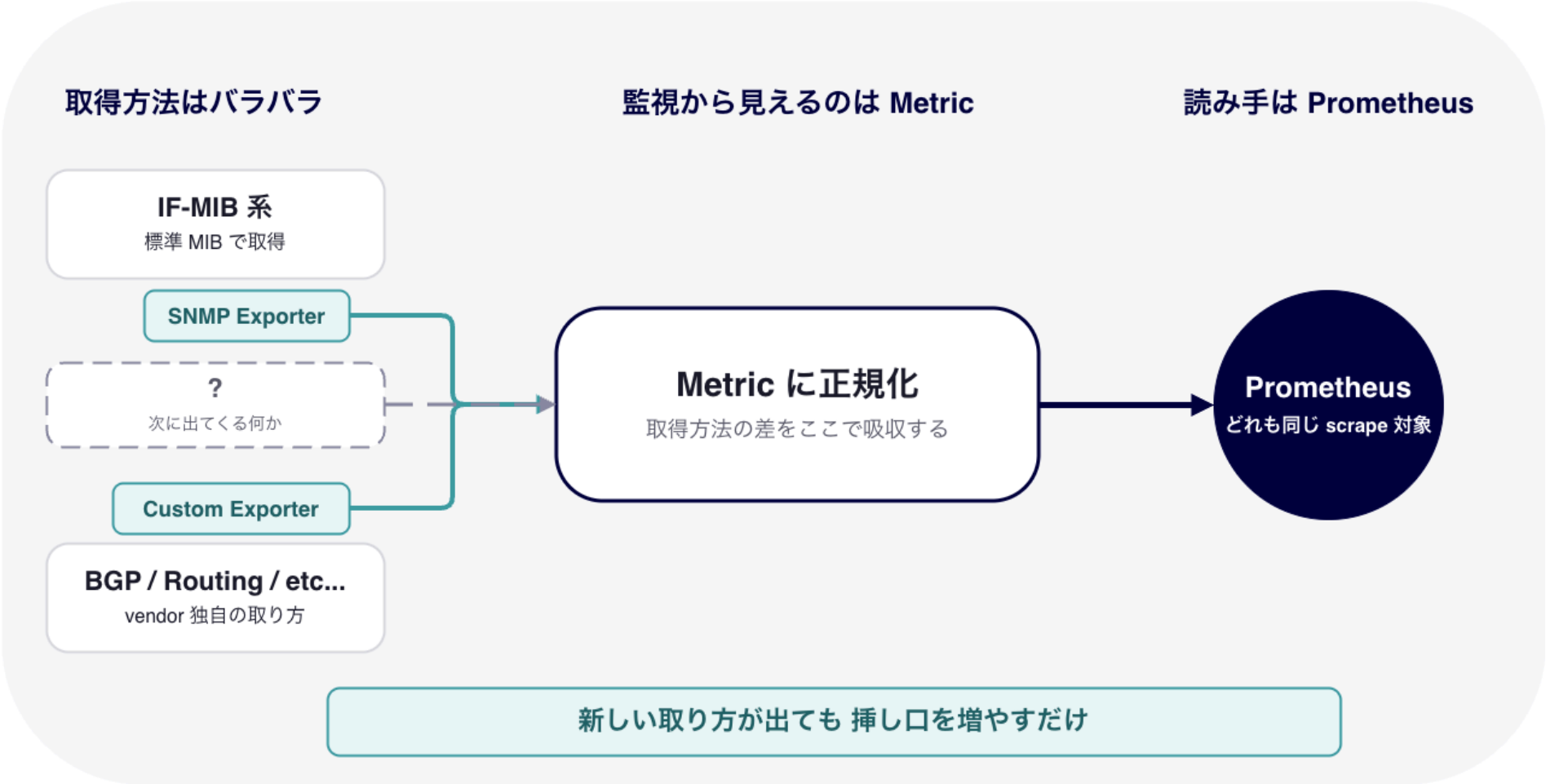
10 年前にやったこと



- ~2016: MRTGを利用
- 2017~: Prometheusを利用(**SNMPは取得方法の一つ**)

ソフトウェアエンジニアがネットワーク部隊に来ていろいろやってみた - janog40

教訓 - 取り方と監視は疎結合



Pull型 監視の課題

Pull型 (SNMPなど) の限界 — 20〜30秒間隔が下限
→ 短時間の Burst が平均化で丸まる

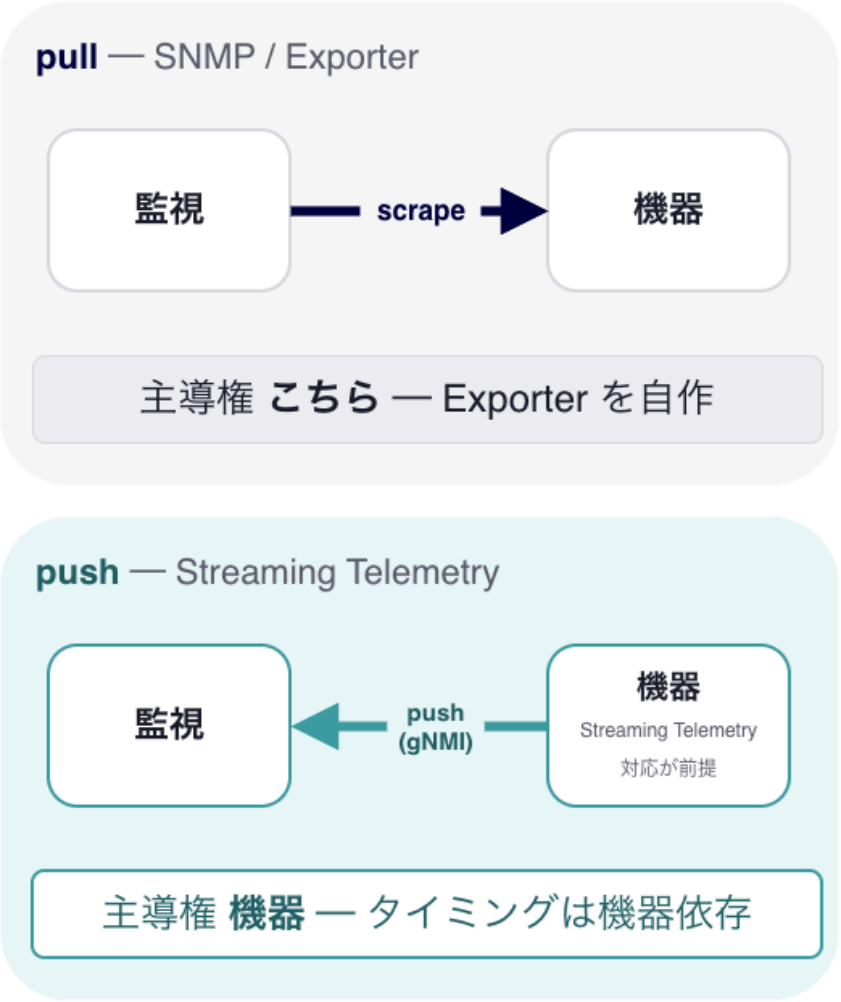
1s以下の 粒度で見たい

- Burst の詳細な可視化
- オペレーション判断を1秒でも早く
- AI 分析の入力として

→ Push型である、Streaming Telemetry が必要

この10年

Streaming Telemetry について



	Pull SNMP / Exporter	Push Streaming Telemetry
起点	監視	機器
主導権	**こちら**	**機器**
新しい指標が欲しい時	Exporter を自作	機器の対応待ち
タイミング	いつでも	機器依存
弊社導入機器での 対応可能な割合	全機種	**70%** MGMT ネットワーク向けの機器は除く

これ以降は個人的の考えです

この 10 年 → 次の 10 年

3 つの方向性

- Traces が進む
- Streaming Telemetry 主体
- Telemetry の読み手の変化

Observability の 3 本柱 - Traces

- **Observability** = Logs + Metrics + **Traces**
  - Logs: イベント / Metrics: 数値時系列 / **Traces: 経路と因果**
- **アプリの世界**では 3 本柱の考え方が定着
  - どのリクエストがどのPodへリクエストされたのかなど
    - 辿った経路 → 遅延・障害の原因追跡
- **ネットワークの世界**にもきっと来る
  - パケット / 制御プレーンの経路と因果を追える世界へ
  - どのPathを通った時はどうだったかなど

Traces が進む

	Metrics	Traces
取得	Streaming Telemetry / SNMP	INT(IOAM) / BMP など
蓄積	Prometheus など	(Tempo / ClickHouse)?
可視化	Grafana	Grafana?

Streaming Telemetry が主体に

目的ごとのNetworkによって利用するプロトコルが変わる

- 本番向けの機器: **Streaming Telemetry** を利用
- MGMTネットワーク向けの機器: **SNMP を継続**
  - 選定する機器は低スペックになりがち
  - 1s以下で見たい需要が無い

Telemetry の読み手の変化 - 人 + AI へ

AI が読み手 → Logs, Metrics(数値時系列) 以外の情報も必要に

例

- 未定義アラートの分類分け → **ベンダー情報 / 機器の状態**
- メンテナンス補助 → **Config / Topology / 機器の状態**

→ Metrics / Logs に加え、**機器の状態** を別の器で管理する必要がある

カーディナリティ問題もあるため、数値以外の情報(機器の状態)も別の器で管理する流れに

まとめ

1. Traces はNW界隈でも進む(希望)
2. Metrics は **Streaming Telemetry 主体へ**
3. 読み手が変わり **機器の状態** も取得する必要がありそう

議論の種

- **Streaming Telemetry について**
  - 本番への適用状況は？
  - 何が壁ですか？(機器の対応状況 / 1s の需要 / 受け側(監視基盤問題))
- **Metrics / Logs 以外に何を収集している？**
  - Config / Topology / 機器の状態 / …
- **Traces、皆さんの現場は?**
  - 導入状況
  - ニーズなど