

# Telemetryワーキンググループ 中間報告

2018/7/12(木)

フューチャーアーキテクト株式会社 日比野 恒

ネットワンシステムズ株式会社 井上 勝晴

# Agenda

1. ワーキンググループの紹介
2. 参画企業の紹介
3. ミーティングの報告
4. Interop2018
5. 今後の活動

# チェア紹介①

名前：日比野 恒 (ひびの ひさし)

所属：フューチャーアーキテクト株式会社

セキュリティアーキテクト (CISSP、CISA、情報処理安全確保支援士)



- ✓ AIなどの「システム高度化」により、ITリテラシーの非対称性が拡大している
- ✓ IoT/コネクテッド領域など、ITが人々の生活に密接に関わるにつれ、危機感を持つようになる
- ✓ オープンな技術を用いたセキュリティログの分析プラットフォーム開発に目覚め、今に至る

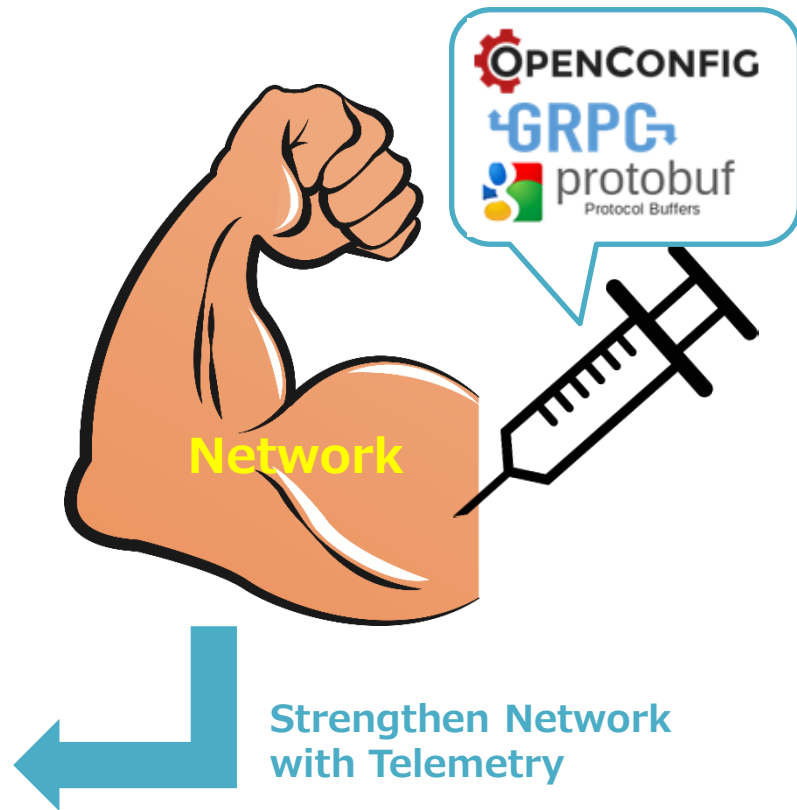
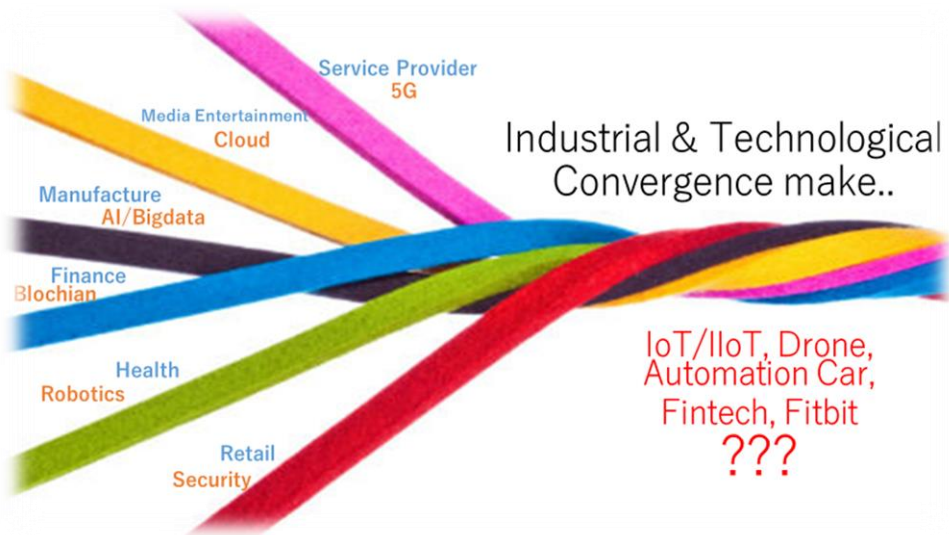
## チェア紹介②

名前：井上 勝晴 (いのうえ まさはる)

所属：ネットワンシステムズ株式会社

Telemetryに期待すること：

ネットワークインフラ強化による**Innovationの醸成**



# 1. ワーキンググループの紹介

---

# Working Group Proposal

項目	内容
ワーキンググループ名称	Telemetryワーキンググループ
メーリングリスト名称	<a href="mailto:telemetry-wg@janog.gr.jp">telemetry-wg@janog.gr.jp</a>
チェア氏名	日比野 恒 (フューチャーアーキテクト) 井上 勝晴 (ネットワンシステムズ)
テーマ・目標	Streaming Telemetryの有効活用
予定される成果物	① Streaming Telemetryのユースケースまとめ ② 各機器ベンダーのTelemetry取り組み報告まとめ
期間	2018/04/01 - 2018/12/31
提案日	2018/03/17

# こんな活動しています

Cisco

Arista

Juniper

⋮

機器メーカー

- ✓ 現在の実装状況
  - ✓ 今後のロードマップ
  - ✓ 注意ポイント
- ...etc



- ✓ よく使うshowコマンド
  - ✓ 現行の運用方法
  - ✓ 運用課題や困り事
- ...etc

通信  
キャリア

ISP/IX

SNS系

機器  
メーカー

⋮

WGメンバ  
(機器メーカー含む)

## Streaming Telemetry UseCaseの発掘

# Working Group Schedule



★第1回MTG(5/18)

★第2回MTG(6/29)

★中間報告  
JANOG42(7/12)

★第3回MTG(9月予定)

★第4回MTG(10月予定)

詳細計画中  
【PoC検討中】

★第5回MTG(11月予定)

★最終報告  
JANOG43



## 2. 参画企業の紹介

---

# 参画企業23社、総勢40名メンバー



ARISTA



つながる 必ずわかる



### 3. ミーティングの報告

---

# 第一回ミーティングのAgenda

#	Topic	Speaker
1	開会の挨拶	チエア 井上さん、日比野
2	ARISTA Network Telemetry	アリスタネットワークスジャパン合同会社 宗像さん
3	Telemetryについて	シスコシステムズ合同会社 佐藤さん
4	TelemetryとSelf-Driving Network	ジュニパーネットワークス株式会社 有村さん、鈴木さん
5	ユーザ企業様①発表	KDDI株式会社 丹羽さん
6	ユーザ企業様②発表	ヤフー株式会社 高橋さん
7	ユーザ企業様③発表	ビッグロブ株式会社 松本さん
8	ユーザ企業様④発表	NTTコミュニケーションズ株式会社 西塚さん
9	QAタイム	

# 第一回ミーティングのサマリー

アスタ、シスコ、ジュニパーの3社3様のアプローチを熱くメッセージアウト！

## Real-time Streaming Strategy

### Self-Driving Network™

実現に向けての5つのステップ

+ Automatic service management

+ All processes with closed loop automation

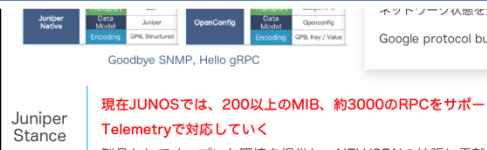
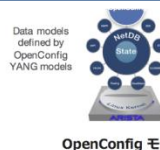
## Model Driven Manageability

Model-Driven API (NETCONF/RESTCONF)  
OpenConfig Streaming Telemetry / IETF YANG-Push

Model-Driven テレメトリ  
(Pub/Sub, イベントベース)

## 【まとめ】

- ✓ スケールに対応するためのTelemetryという考え方
- ✓ 運用効率化のための自動化としてのTelemetryという考え方
- ✓ 「Turned Off SNMP」、「Goodbye SNMP」というメッセージ
- ✓ 「Native vs OpenConfig」というデータモデルの話



		OpenConfig(YANG)	UDP gRPC	GPB	
NXOS	7.3(0)J5(1)	Native(not YANG) Native(YANG) *	HTTP gRPC UDP *	JSON GPB	✓ *
IOS XE	16.6.1	Native(YANG) OpenConfig(YANG)	Netconf	XML	

\* Roadmap

# 【参考】第一回ミーティングの発表資料

WG運営発表資料

[https://www.janog.gr.jp/wg/telemetry-wg/wp-content/uploads/2018/06/【TelemetryWG】ミーティング01\\_20180518.pdf](https://www.janog.gr.jp/wg/telemetry-wg/wp-content/uploads/2018/06/【TelemetryWG】ミーティング01_20180518.pdf)

Arista様発表資料

<https://www.janog.gr.jp/wg/telemetry-wg/wp-content/uploads/2018/06/20180513-Arista-Telemetry-share.pdf>

Cisco様発表資料

[https://www.janog.gr.jp/wg/telemetry-wg/wp-content/uploads/2018/06/20180518\\_Cisco\\_Telemetry\\_WG01.pdf](https://www.janog.gr.jp/wg/telemetry-wg/wp-content/uploads/2018/06/20180518_Cisco_Telemetry_WG01.pdf)

Juniper様発表資料

[https://www.janog.gr.jp/wg/telemetry-wg/wp-content/uploads/2018/06/20180518\\_Juniper\\_Telemetry\\_WG01.pdf](https://www.janog.gr.jp/wg/telemetry-wg/wp-content/uploads/2018/06/20180518_Juniper_Telemetry_WG01.pdf)

議事メモ

[https://www.janog.gr.jp/wg/telemetry-wg/wp-content/uploads/2018/06/20180518\\_第一回Telemetry\\_WGメモ.txt](https://www.janog.gr.jp/wg/telemetry-wg/wp-content/uploads/2018/06/20180518_第一回Telemetry_WGメモ.txt)

# 第二回ミーティングのAgenda

#	Topic	Speaker
1	チエアより	フューチャーアーキテクト株式会社 日比野
2	OSSツールで作る、Telemetry初めの一步	ネットワンシステムズ株式会社 ハディさん、井上さん
3	ElasticStackの紹介	Elasticsearch株式会社 大谷さん
4	ユーザ企業様①発表	楽天株式会社 藤原さん
5	ユーザ企業様②発表	ソフトバンク株式会社 北上さん
6	QAタイム	

# 第二回ミーティングのサマリー

機器から出力されるTelemetryデータの取り扱い方法について、熱く議論！！

## 今日のGoalイメージ

Ciscoさま、Aristaさまが各々公開するCollectorツールを使い、RouterよりTelemetryデータを収集する。その収集したデータを可視化する。

## 【まとめ】

- ✓ Elasticsearchクラスタのデータ構造を解説
- ✓ LogstashとBeatsの役割の違いと特徴の説明
- ✓ Kibanaダッシュボードのサンプルの解説
- ✓ 検証環境をElasticStackと仮想ルータで構築するデモ

データ

Import

Sto



- 会社のメールアドレスのみ有効 (Gmail アカウントで苦労した方のブログ <https://www.ainoniwa.net/pelican/2016/0731a.html>)
- デモ版は60日限定で利用可能。機能制限、帯域制限なし

Arista vEOS-lab

- <https://qiita.com/souko2525/items/2e1478be0441f4c057e4> 入手からインストールまで書かれている
- 制限なし(?)、ラボ利用限定

まで



# 【参考】第二回ミーティングの発表資料

WG運営発表資料

[https://www.janog.gr.jp/wg/telemetry-wg/wp-content/uploads/2018/07/【TelemetryWG】ミーティング02\\_20180629.pptx](https://www.janog.gr.jp/wg/telemetry-wg/wp-content/uploads/2018/07/【TelemetryWG】ミーティング02_20180629.pptx)

ネットワンシステムズ様発表資料

[https://www.janog.gr.jp/wg/telemetry-wg/wp-content/uploads/2018/07/20180629\\_Telemetry\\_WG\\_NetoneSystems.pdf](https://www.janog.gr.jp/wg/telemetry-wg/wp-content/uploads/2018/07/20180629_Telemetry_WG_NetoneSystems.pdf)

Elastic様発表資料

<https://speakerdeck.com/johtani/intro-elastic-stack-at-telemetry-wg>

議事メモ

[https://www.janog.gr.jp/wg/telemetry-wg/wp-content/uploads/2018/07/20180629\\_第2回Telemetry\\_WG\\_メモ.txt](https://www.janog.gr.jp/wg/telemetry-wg/wp-content/uploads/2018/07/20180629_第2回Telemetry_WG_メモ.txt)

# 皆さんにお願いしていた内容

各ミーティングにおいて、ユーザ企業様より以下内容を発表頂きました。

## 【WGでのヒアリング項目】

- ①障害対応でよく使うshowコマンド
- ②現行運用における課題や困りごと
- ③Telemetryに期待していること
- ④Telemetryとの関わり度合い  
(興味ある/試している/運用している等)

# ミーティングの総括①

- Telemetryに対する考え方

VendorとUserとの間で、**認識・温度感にギャップ**が存在

- Vendor side  
「Goodbye SNMP、Self-Driven Network」等のメッセージアウトがあり、**現運用を変え得る**という意味で、Telemetryに対する高い期待
- User side  
興味・期待はあるが、どちらかと言うと**現運用をベース**に、冷静にTechnologyを注視

認識ギャップを埋める施策が必要か・・・

**対応状況、設定方法、ユースケース**等の情報整備

## ミーティングの総括②

- ユースケースに対するディスカッション

運用において度々問題となる**Burst Traffic**について、参加者からの経験則シェア、ディスカスあり

- Burst Trafficの**早期検出**はGood Point！！
- しかし、**フロー情報**が解らないと対処が出来ない  
(どのSrc/DstのTrafficがBurstしているか解らないと対処出来ない)

現実的な利用には、**他技術（xFlow等）との併用利用、他システムとの連携**が必要か・・・

## ミーティングの総括③

- デプロイに対するディスカッション  
どの様な条件が整った時に、Telemetryを導入検討が現実的となるのか？
  - Telemetryで**出来る事、出来ない事**の整理
  - 1st stepでTryする上での**技術ドキュメント**
  - SNMP MIBとTelemetry Sensor pathの**対比情報**
  - その他諸々、、

「情報の少なさ」故に現実的な検討には至っていないが、**Telemetry**  
**ならではのユースケース**登場により状況は変化すると予想

## ミーティングの総括④

- システム複雑化への懸念
  - 取得した**膨大なデータへのケア**（Storage, DB管理が追加）
    - ✓ 圧縮やサマライズ機能等、Tool検討時に要考慮
  - **ベンダー毎のCollector**（現状）
    - ✓ OpenConfigによるデータモデル共通化と同じく、Transportの統一も期待したい – gNMIに期待

Network視点だけではなく**インフラ全体**で見る必要がある、  
このような視点から、運用の**Game Changing**も期待

# ミーティングで発表頂いたものをご紹介します※抜粋

## ①障害対応でよく使うshowコマンド

- ✓ show tech、show log、インターフェース状態確認、BGP状態確認、光レベル状態確認など
- ✓ コンフィグチェック(いつ変えたかの履歴チェックも)、HWステータス、Routing情報など

## ②現行運用における課題や困りごと

- ✓ TCAM監視がSNMPでは追いつけない。(Telemetryに期待している)
- ✓ Flowパケットの生成(CPUリソースを多く消費)、故にTelemetryに期待したい
- ✓ 情報不足で障害原因の特定が出来ないことで疑わしい箇所を全交換。
- ✓ マイクロバーストのようなサイレント障害。
- ✓ 設定変更後のTraffic変化量、変更して直ぐに確認したい。(今はSNMPで5分後にわかる)
- ✓ 多様なカウンタ、インターフェースだけだと全体が見えない、QoSクラスごとのカウンタとかも欲しい。

## ③Telemetryに期待していること

- ✓ 少ないリソースで動作するのであれば監視に使いしたい。(データ取得頻度を上げられると嬉しい)
- ✓ マルチベンダー環境のため、Open Configベースに期待。
- ✓ 自動データ収集や自動オペレーション対応に期待。(バースト時に自動でQoSをかける等)
- ✓ 課金データのクリティカルなデータ利用が可能な安定性が欲しい。

## ④Telemetryとの関わり度合い

(興味ある/試している/運用している等)


- ✓ PoCでAristaのTelemetryをKafkaに流して確認をしている。
- ✓ PoCでTelemetryをinfluxDBに格納し、Grafanaで可視化させてみた。

## 4. Interop2018

---



# Juniper様展示ブースにて登壇



セッション スケジュール

Time	Session	
10:30 10:50	マルチクラウド環境のすべてをセキュアに統合運用する切り札 ～ 仮想マシン、コンテナ、ベアメタル、パブリッククラウドを一つのコントローラーで統合的に自動化 ～	
11:05 11:25	クラウド環境選択の自由度を高める ～ OpenShift Networkingとその拡張 ～	レッドハット株式会社
11:40 12:00	Telemetryの匠が解説 ～ オープン技術を用いたマイクロバースト検知の最前線 ～	Telemetry Working Group
12:50 13:10	ジュニパーの簡易SD-WANソリューション	
13:25 13:45	キルチェーンを可視化する次世代の脅威対策	
14:00 14:20	高度な脅威検知と対処の自動化を実現するSDSN	ジェイズ・コミュニケーション株式会社
14:35 14:55	VMware NSX Data Centerに最適な物理ネットワークとは?	ガイムウェア株式会社
15:10 15:30	Telemetryの匠が解説 ～ オープン技術を用いたマイクロバースト検知の最前線 ～	Telemetry Working Group

6/14(木)に計2回

# MXルータのTelemetry検証を交えて

Telemetryの匠より優しくTelemetryとは何なのか、何が嬉しいのかを解説！！

## 何故、今、Telemetry??

Googleに  
SNMPによる

- 1) Hyper Scale Player
  - 超大規模Data Center
  - White Box Switch積

→ 従来のOperation

- 2) Operation変革
  - NetworkをIntent
  - Workflowの洗練

→ その為にNetworkリアルタイム把握が

## Telemetry Framework Requirement by Google

- network elements stream data to collectors (push model)

NW機器はストリーム形式にてCollect

- data populated based on vendor-neutral models

可能な限りベンダー非依存なモデル

- utilize a publish/subscribe API to select desired data

データ選択にはpublish / subscribe

- scale for next 10 years of density growth with high density

other protocols distribute load to hardware, so should  
向こう10年のデータ増加に対応出来

- utilize modern transport mechanisms with active

最新Transportメカニズムを利用す

## テストシナリオ

- ① バースト性トラフィックの検知
- ② Packet DropとInterface Queueの相関
- ③ 機械学習によるアノマリ検知

# 想像以上の注目度の高さに圧倒

展示ブース前の通路を完全にふさいでしまって、ごめんなさい(; °Д°)



## 5. 今後の活動

---

# このような取り組みを計画中

Vendor NativeとOpen Configの出来ること/出来ないことを比較。  
Telemetryデータを取り扱うOSSツールのメリット/デメリットを整理。etc...



VS

Vendor Native



ARISTA

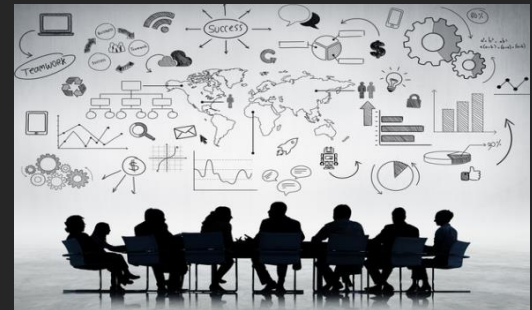


VS



elastic stack

# Q & A



*Thank  
you*



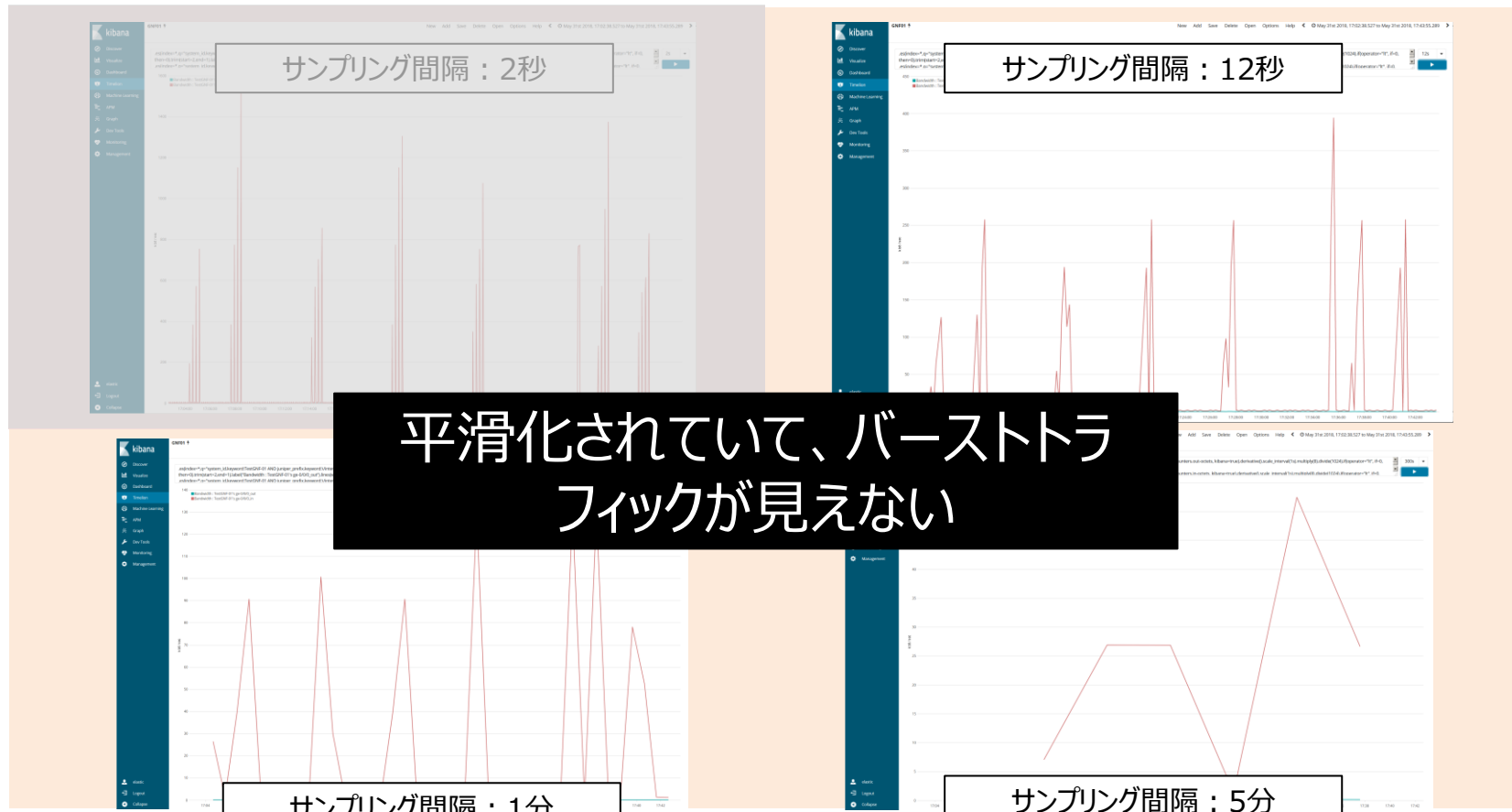
# Appendix



# Interop2018 テストシナリオ

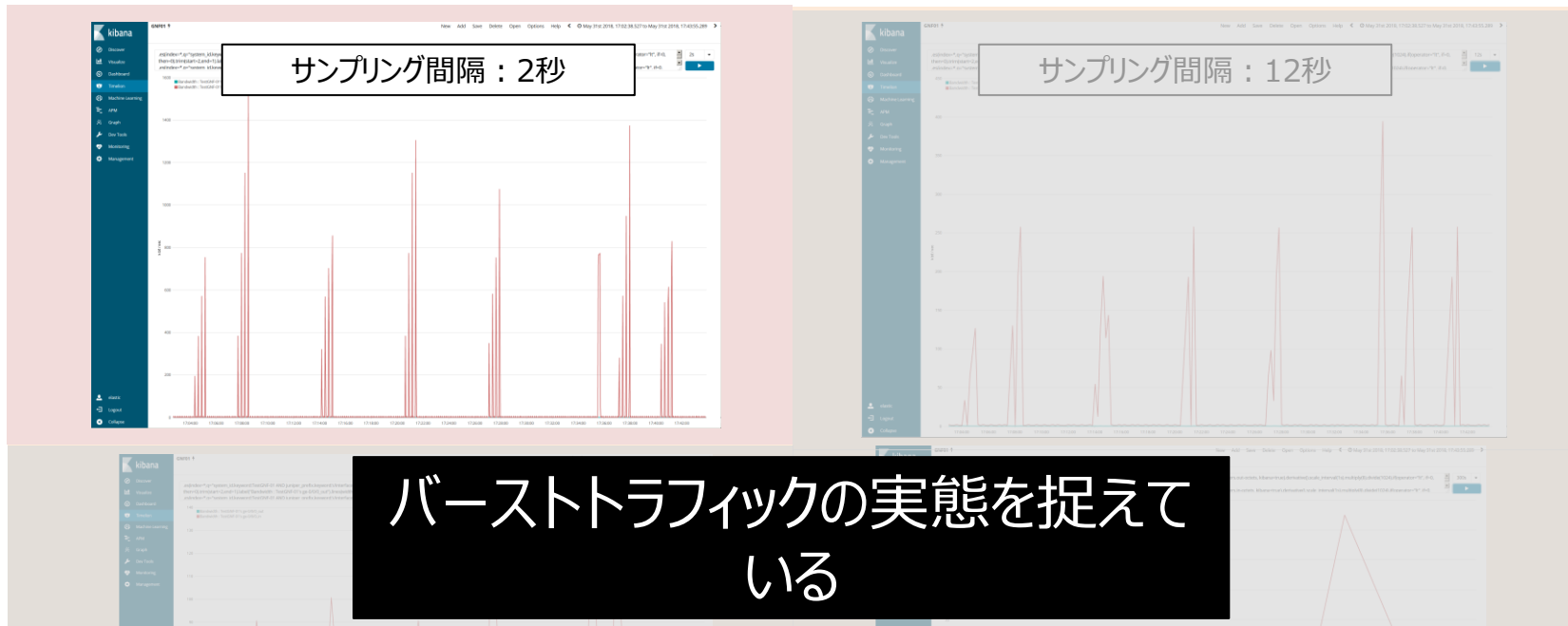
- ① バースト性トラフィックの検知
- ② Packet DropとInterface Queueの相関
- ③ 機械学習によるアノマリ検知

# リアルタイム可視化 – Burst Traffic検知



試験条件：1000byte 100~400pps×1秒とOpps×600秒を繰り返すTrafficを印加

# リアルタイム可視化 – Burst Traffic検知



Telemetryを使用する事で、今まで見えていなかった事象  
(≡**サイレント障害**)を可視化、検知する事が出来る

# リアルタイム可視化 - Packet DropとQueueの相関①

## Interface毎の使用帯域 / Dropカウンタ



Interface単位の帯域(リアルタイム)

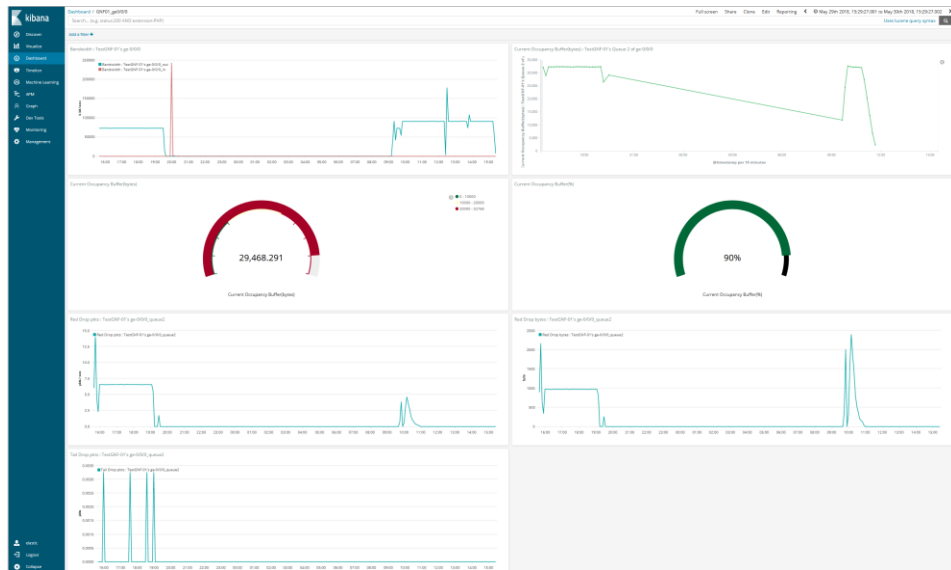
Packet Drop状況(リアルタイム)  
※この例では、ge 0/0/0 のqueue 2上での

Red Drop, Tail Dropを把握

様々なデータを時系列データとして扱う事で、  
各データ間の相関を把握が可能となる

# リアルタイム可視化 - Packet DropとQueueの相関②

## Interfaceの使用帯域 / Packet Drop / Interface queueの相関



Interfaceの使用帯域(リアルタイム)

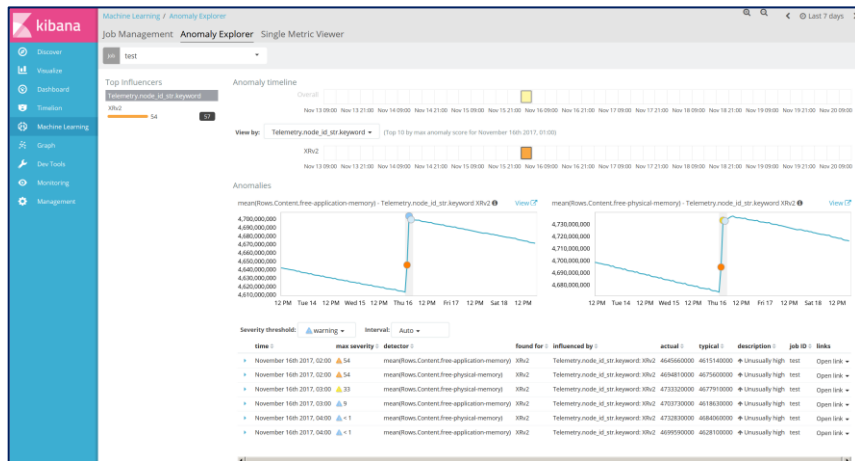
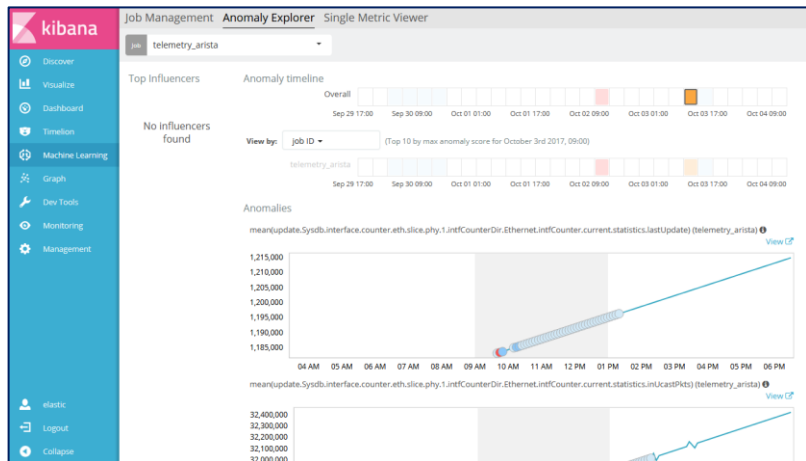
Queue 2 の利用状態(リアルタイム)  
Queue 2 の利用状態(%)

Queue 2のRed Drop bytes/pkts  
Tail Drop pkts(リアルタイム)

様々なデータを時系列データとして扱う事で、  
**各データ間の相関**を把握が可能となる

# 機械学習 - 異常性, 特異性の検知

Interface カウンター等を Machine Learning に掛け、異常性/特異性の検知に成功しています。  
人の目では気づき難い微小な変化を検知 (Interfaceカウンタ増減・メモリ解放等、微小変化の検知)



異常の検知をトリガーに、**サイレント障害**の通知や、設定修正のための**ワークフローエンジン**を実行する事が出来る