

**お手軽！**  
**BGP RIBのリアルタイム解析+可視化**

BIGLOBE Inc.  
Toshiya Mabuchi

# 自己紹介

- 名前：馬淵 俊弥 (Mabuchi Toshiya)
- 所属：ビッググローブ株式会社
- お仕事：
  - ISPバックボーンネットワークの全般
    - 設計/開発/検証/運用/顧客サポート
    - 最近は自動化/可視化回りに注力中!

---

# ASの経路監視ってどうしてます？

## ● 運用面

- 障害時の原因究明
- 顧客の経路変動/正常性
- 主要なPeerの経路変動
  - Peerしてるのに上流から流れてないか
  - 遅延の大きいPeerを選択してないか？

## ● マネジメント面

- 上流トランジットへの経路依存率の把握
  - 手軽に見れるようにしてPeering交渉に役立てる
  - すぐに出せるグラフがあるとKPIにも役立つ
- 上流トランジットの選定/更改時に使う為のデータ

---

経路情報を見るのは運用の時だけじゃない

**トランジット依存率の指標など  
コストマネジメントの目的でも使いたい**

## いままで経路記録としてやっていたこと

- Quagga + MRT Dump + libBGPdump
  - データとしては記録できている
  - 時間毎にファイル分割して保存している
  - 文字でしか読めないので、  
時系列で何が起きているか見るのがつらい
  - いつも見るのにはちょっと厳しい
    - かなりの障害が発生した時くらいしか見ない

## こういう感じ経路情報のログを見てた

```
> bgpdump dump2015.11.27.1000  
TIME: 11/27/15 01:00:00  
TYPE: TABLE_DUMP_V2/IPV4_UNICAST  
PREFIX: 1.0.0.0/24  
SEQUENCE: 0  
FROM: 133.205.1.155 AS2518  
ORIGINATED: 07/13/70 11:03:57  
ORIGIN: IGP  
ASPATH: 2518 15169  
NEXT_HOP: 133.205.1.155  
MULTI_EXIT_DISC: 100  
TIME: 11/27/15 01:00:00  
TYPE: TABLE_DUMP_V2/IPV4_UNICAST  
PREFIX: 1.0.0.0/24  
SEQUENCE: 0  
FROM: 133.205.1.142 AS2518  
ORIGINATED: 07/13/70 11:03:37
```

## ● 要件！

- グラフとして表示できる
- リアルタイム性がある
- 他の情報(トラフィック等)と一元的に見る方法がある
- そんなに難しいことしたくない



- **B**GP **M**onitoring **P**rotocol

- BGPのUPDATE情報等をモニタリングできるプロトコル
- これを使わない手は無い！

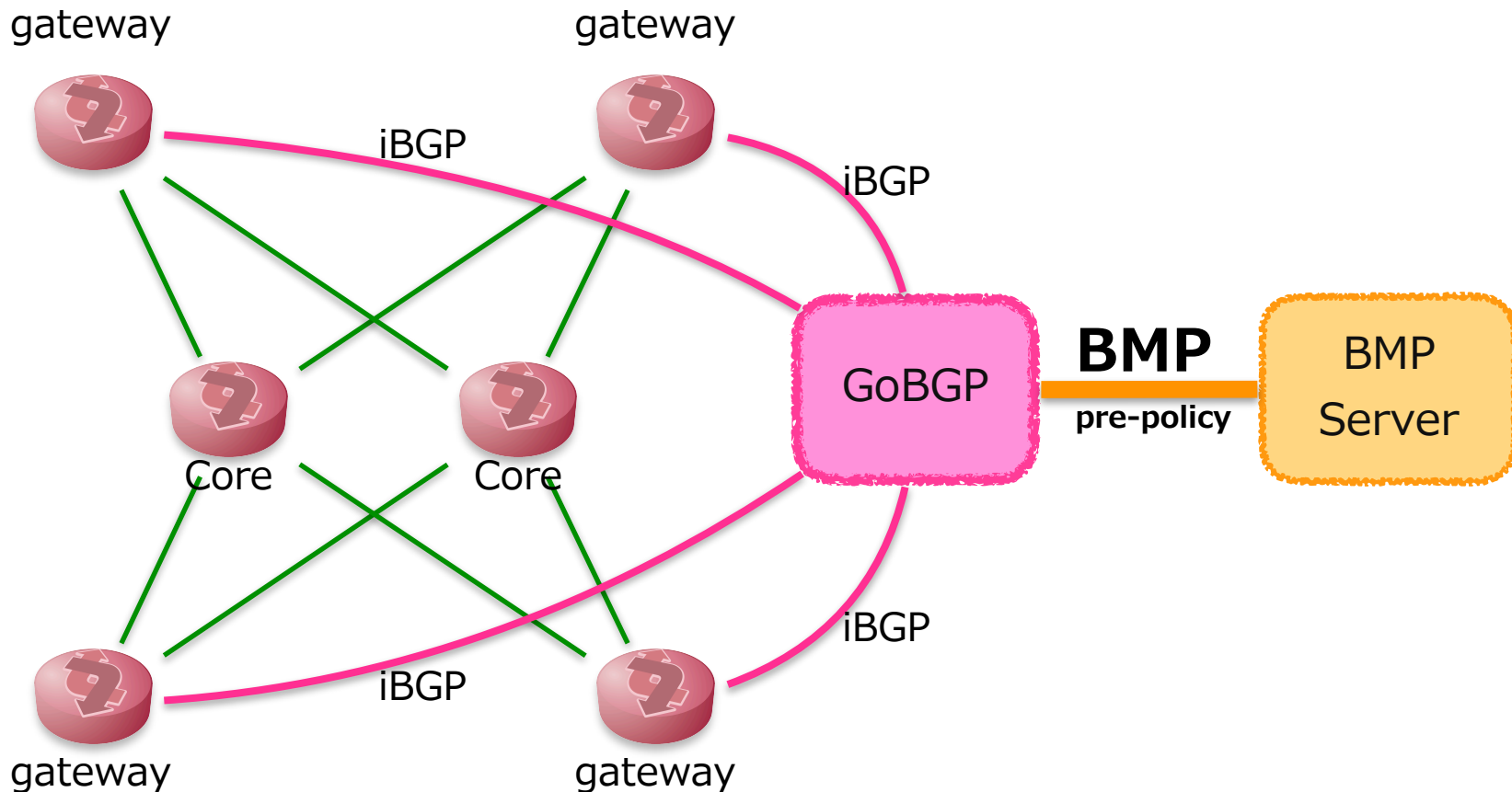
- . . . しかし！！！！

- 商用ルーターのバージョンで一部非対応  
→ すぐには使えない

- **iBGPで経路を収集**する
  - 経路収集用にGoBGPを立てる
  - GoBGPとルータをiBGPで繋ぐ
    - GoBGPからBMP Serverに送信

**ルータ単位で発生する経路変動は収集できる！**

# iBGPで経路を収集

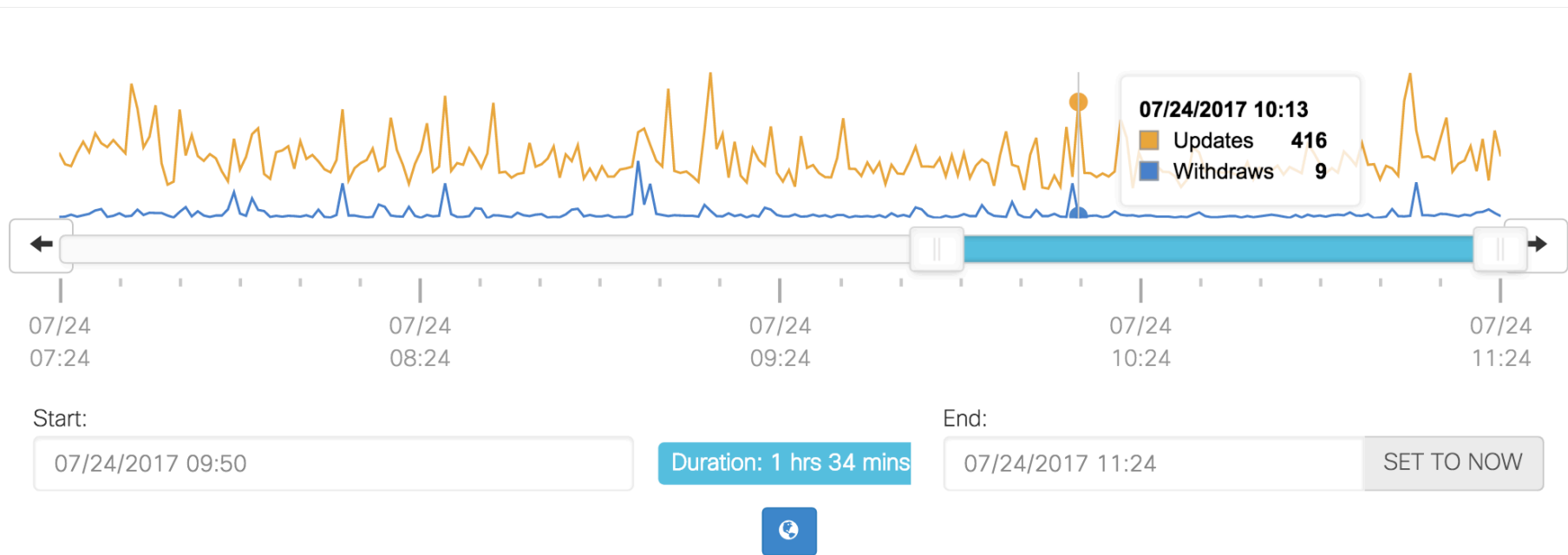


- **SNAS** Streaming Network Analytics System

<http://www.snas.io/>

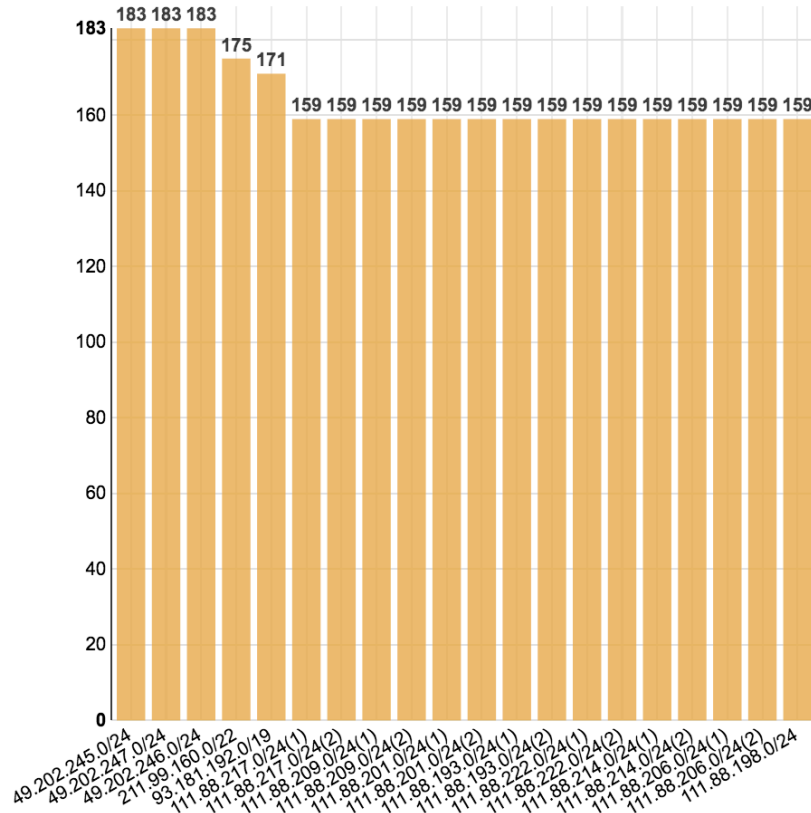
- 経路情報モニタリングのフレームワーク
- OpenBMP + Kafka + MySQL + WebUI で構成
  - 経路用モニタリングのWebUIが付いている
  - APIも豊富でデータを加工して使いやすい
  - Docker containerで構築が簡単

# SNAS UI

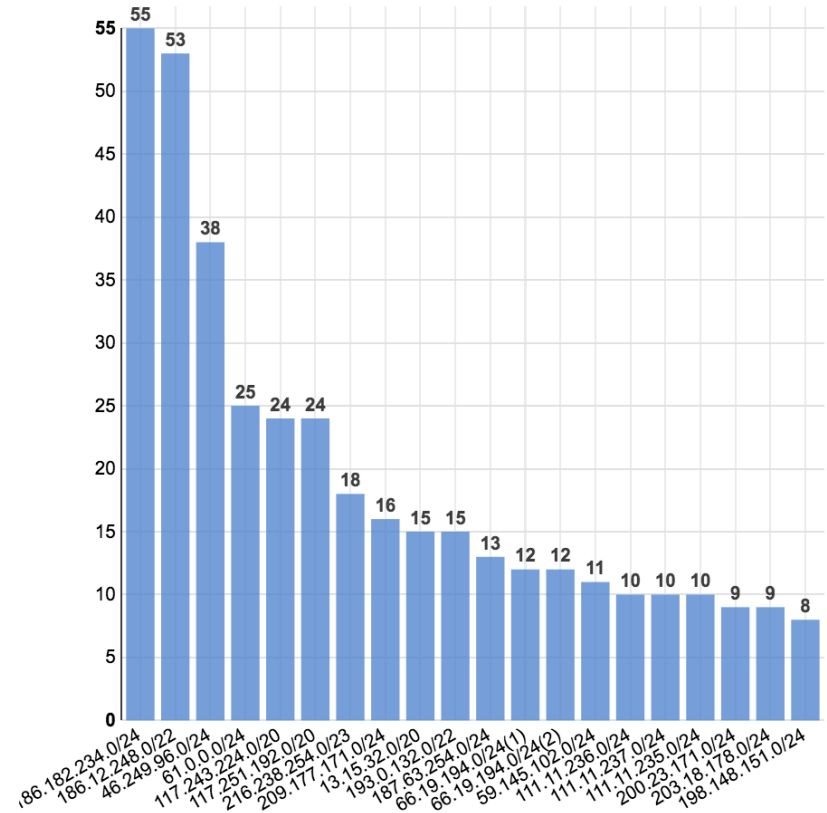


# SNAS UI

Top 20 Prefixes By Number of Updates

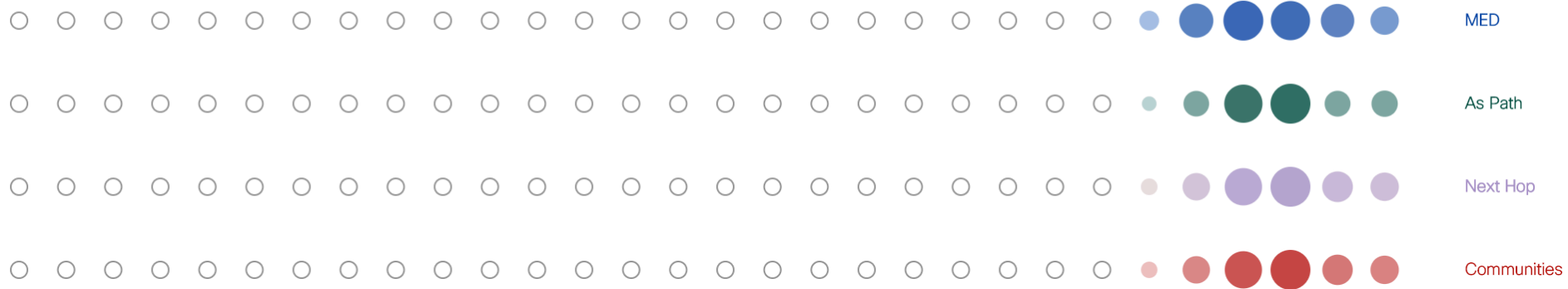


Top 20 Prefixes By Number of Withdraws



# SNAS UI

07/24 10:25 07/24 10:30 07/24 10:35 07/24 10:40 07/24 10:45 07/24 10:50 07/24 10:55 07/24 11:00 07/24 11:05 07/24 11:10 07/24 11:15 07/24 11:20



RouterName	NH	AS_Path	Peer_ASN	MED	Communities	Last_Modified
r00.testtx09.us....	4.68.63.177	3356 12389 44237	65000	42949...	2914:1004	2017-07-24 11:20:56.0000...
r00.testtx09.us....	129.250.9.94	3356 12389 44237	65000	42949...	2914:1005	2017-07-24 11:20:56.0000...
r00.testtx09.us....	4.68.111.69	3356 12389 44237	65000	42949...	2914:1003	2017-07-24 11:20:56.0000...
r00.testtx09.us....	4.68.111.69	3356 12389 44237	65000	42949...	2914:1003	2017-07-24 11:20:56.0000...
r00.testtx09.us....	4.68.62.205	3356 12389 44237	65000	42949...	2914:1008	2017-07-24 11:20:56.0000...
r16.testtx09.us.bb	4.68.63.177	3356 12389 44237	65000	42949...	2914:1004	2017-07-24 11:20:55.8520...
r16.testtx09.us.bb	129.250.9.94	3356 12389 44237	65000	42949...	2914:1005	2017-07-24 11:20:55.7750...
r1.sea	165.254.106.17	2914 3356 12389	3130	5099	2914:1005	2017-07-24 11:20:55.0000...

# SNAS UI

+6453 -2914:1011 -2914:2000 -2914:3000 -65504:3356	●	AS Path: 6453 3356 12389 44237 13118 07/24/2017 11:21:02.844
+2914:1011 -2914:1009	●	AS Path: 3356 12389 44237 13118 Communities: 2914:1011 2914:2000 2914:3000 65504:3356 07/24/2017 11:21:01.278
	●	AS Path: 3356 12389 44237 13118 Communities: 2914:1009 2914:2000 2914:3000 65504:3356 07/24/2017 11:21:01.151
+2914:1009 -2914:1011	●	AS Path: 3356 12389 44237 13118 Communities: 2914:1009 2914:2000 2914:3000 65504:3356 07/24/2017 11:21:01.000
-11017 -6939 +2914:1011 +2914:2000 +2914:3000 +65504:3356	●	AS Path: 3356 12389 44237 13118 Communities: 2914:1011 2914:2000 2914:3000 65504:3356 07/24/2017 11:21:01.000
+11017 +6939 -3356:22 -3356:100 -3356:123 -3356:501 -3356:2065	●	AS Path: 11017 6939 3356 12389 44237 13118 07/24/2017 11:20:59.782



今までに比べたらかなり分かりやすい！

# (再掲)監視したい理由

## ● 運用面

- 障害時の原因究明
- 顧客の経路変動/正常性
- 主要なPeerの経路変動
  - Peerしてるのに上流から流れてないか
  - 遅延の大きいPeerを選択してないか？
- トラフィック + 経路変動一緒に見たい
  - 一緒に見れば分かる原因もある

## ● マネジメント面

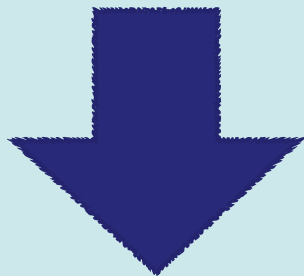
- 上流トランジットへの経路依存率の把握
  - 手軽に見れるようにしてPeering交渉に役立てる
  - すぐに出せるグラフがあるとKPI立てるのとかにも役立つ
- 上流トランジットの選定/更改時に使う為のデータ
  - いつでも出せるようにしたい

# (再掲)監視したい理由

## ● 運用面

- 障
- 雇
- 三

自社特有の観点が入ると、  
標準のWebUIでは見にくい場合もある



定常的に見るデータだけをAPIで取得  
Influxdb + Grafanaで可視化

- 相に元々はわかる原因もある

## ● マネジメント面

- いつでも出せるようにしたい

の  
て  
る  
あると  
役立つ  
選定/  
ータ

# 最終的な構成

gateway

gateway



iBGP

iBGP



Core



Core



Core



Core



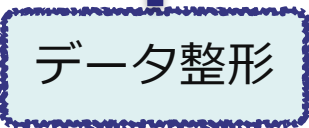
iBGP

iBGP

GoBGP



Influxdb



データ整形



Grafana



Open  
BMP

gateway

gateway

# 作った経路監視用のDashboard



openbmp

Zoom Out now-80m to now-30m

BMP STATUS

OK

Peer Establ %

300%

Transit Total Route

293472 Routes

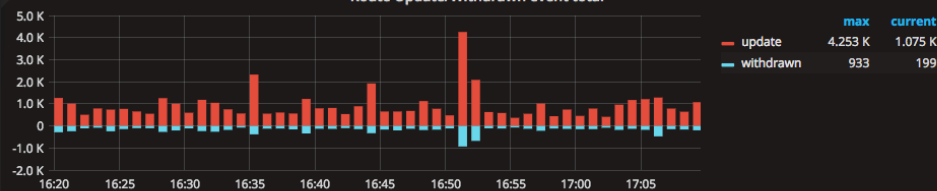
Customer ORIGIN Route

240 Routes

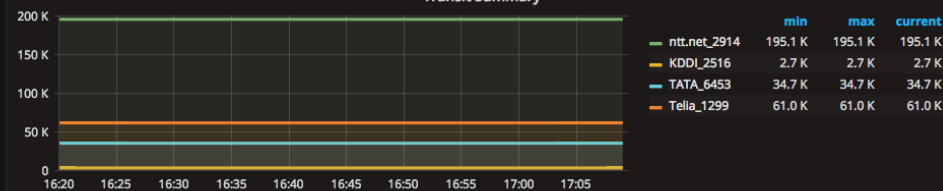
sub-customer route

121 Routes

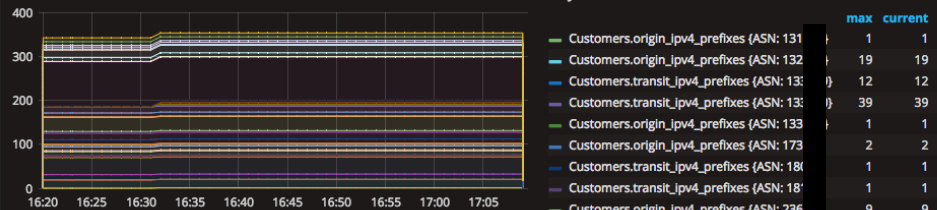
Route Update/Withdrawn event total



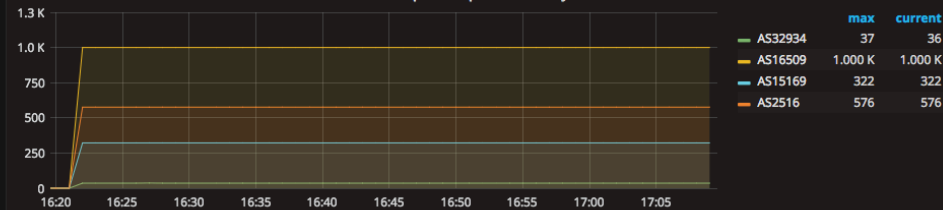
Transit Summary



CUSTOMER ROUTE summary



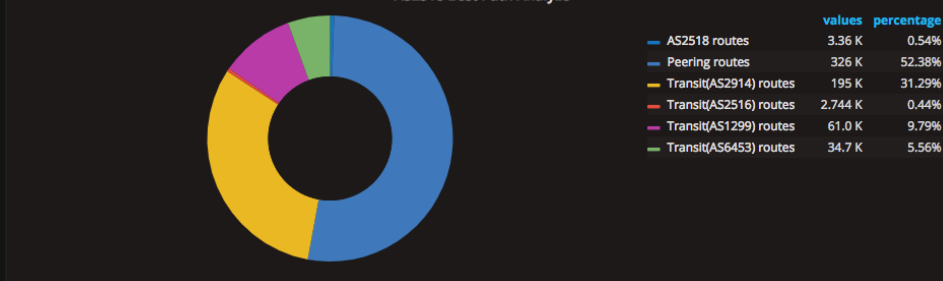
important peer summary



most recent update/withdrawn

Time	Prefix	PrefixLen	AS_Path	communities	isWithdrawn
2017-07-25 17:09:02	31.13.80.0	24.00	2914 3356 32934	2518:8 2518:11	false
2017-07-25 17:09:02	157.240.3.0	24.00	2914 32934	2518:8 2518:11	false
2017-07-25 17:09:02	31.13.65.0	24.00	2914 32934	2518:8 2518:11	false
2017-07-25 17:09:02	157.240.7.0	24.00	2914 32934	2518:8 2518:11	false
2017-07-25 17:09:02	185.60.216.0	24.00	2914 32934	2518:8 2518:11	false
2017-07-25 17:09:02	31.13.76.0	24.00	2914 32934	2518:8 2518:11	false
2017-07-25 17:09:02	31.13.84.0	24.00	2914 32934	2518:8 2518:11	false

AS2518 Best Path Analyze



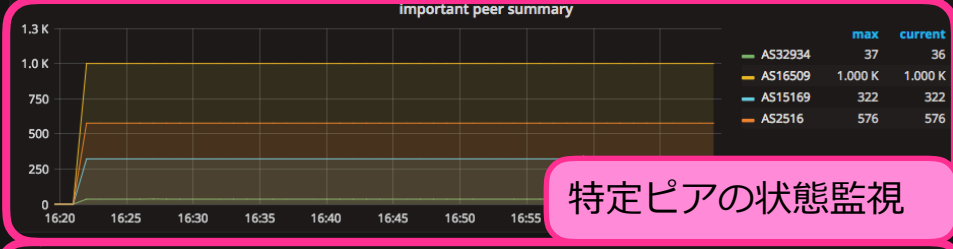
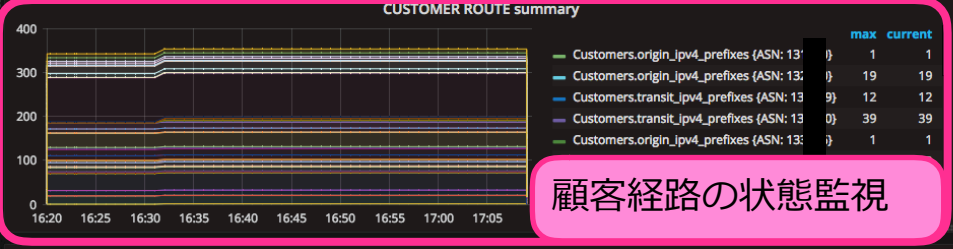
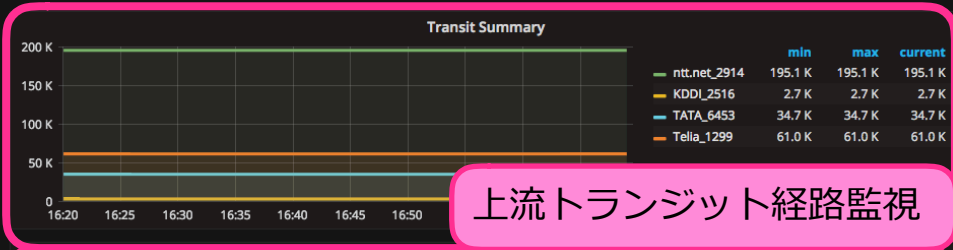
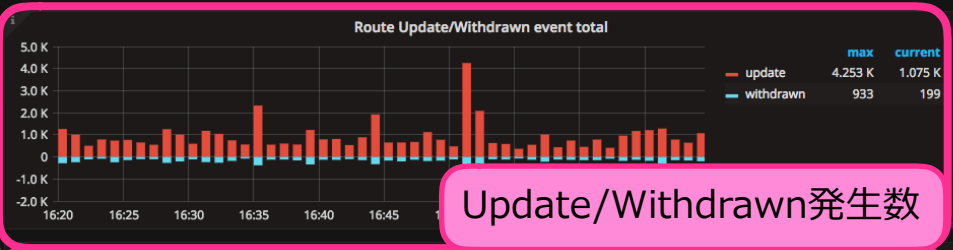
# 作った経路監視用のDashboard

BMP STATUS **OK** Peer Establ % **300%**

Transit Total Route **293472** Routes

Customer ORIGIN Route **240** Routes

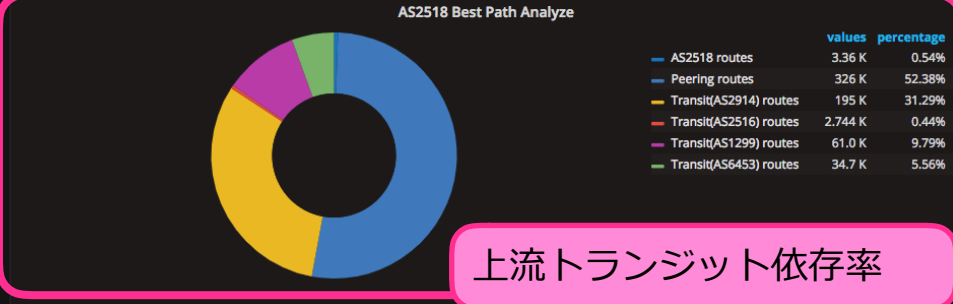
sub-customer route **121** Routes



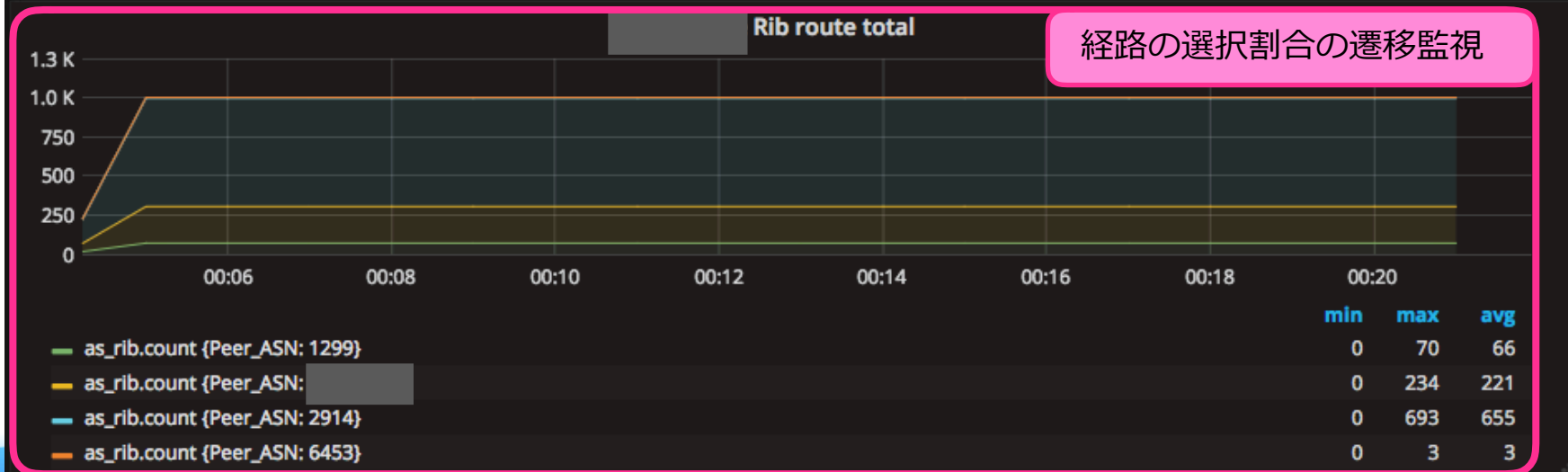
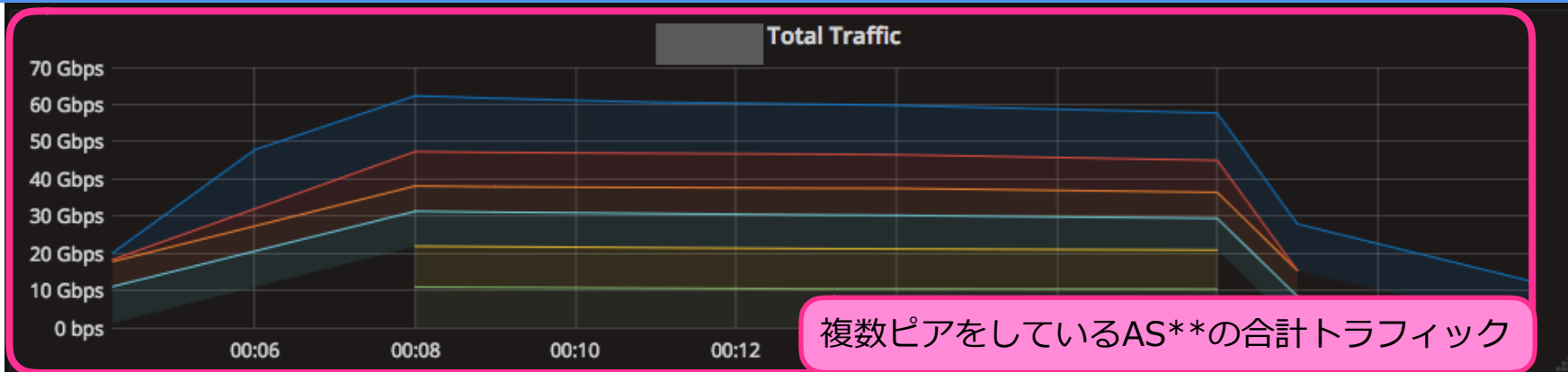
most recent update/withdrawn

Time	Prefix	PrefixLen	AS_Path	communities	isWithdrawn
2017-07-25 17:09:02	31.13.80.0	24.00	2914 3356 32934	2518:8 2518:11	false
2017-07-25 17:09:02	157.240.3.0	24.00	2914 32934	2518:8 2518:11	false
2017-07-25 17:09:02	31.13.65.0	24.00	2914 32934	2518:8 2518:11	false
2017-07-25 17:09:02	157.240.7.0	24.00	2914 32934	2518:8 2518:11	false
2017-07-25 17:09:02	185.60.216.0	24.00	2914 32934	2518:8 2518:11	false
2017-07-25 17:09:02	31.13.76.0	24.00	2914		false
2017-07-25 17:09:02	31.13.84.0	24.00	2914		false

Update/Withdrawn詳細



# 作った経路監視用のDashboard



## ● 良かった点

- 注視すべき経路情報に絞って監視できた
- Traffic/Error等,他情報と合わせて確認できるようになった
- 実装したのはDB間のデータ送受信部だけ
  - 非常に少ない手間で実装可能

## ● 改善点

- 各ルータ毎のBestPathしか見れない
  - BGP ADD-PATHを使ってGoBGPと各ルータを繋ぐ
    - (GoBGP中の人)「BGP ADD-PATH実装したよ！」
  - BMPを直接使う



- **経路状態は運用以外にも使える**
  - Peering/KPI
- **経路監視をGoBGP+openBMP+Influxdbへ**
  - 経路収集はiBGP
  - SNAS (OpenBMP)
    - 自分でUI作らなくても、十分なWebUIがある
    - 注視すべき情報のみREST APIでInfluxdbに投入
      - Grafanaで他のデータと一元的に可視化ができた