Kibana入門

水戸 祐介 / @y_310

誰？

水戸祐介 Mito Yusuke

COOKPAD株式会社 技術部

アプリケーションエンジニア

以前はサービス開発、最近はREST APIの開発など

y310

@y_310

American Gun Deaths

Dec 13, 2012 12:30:05 to Sep 7, 2013 05:42:33

gender:male | gender:female | gender:unknown

QUERY

FILTERING

ABOUT THIS DASHBOARD — TEXT

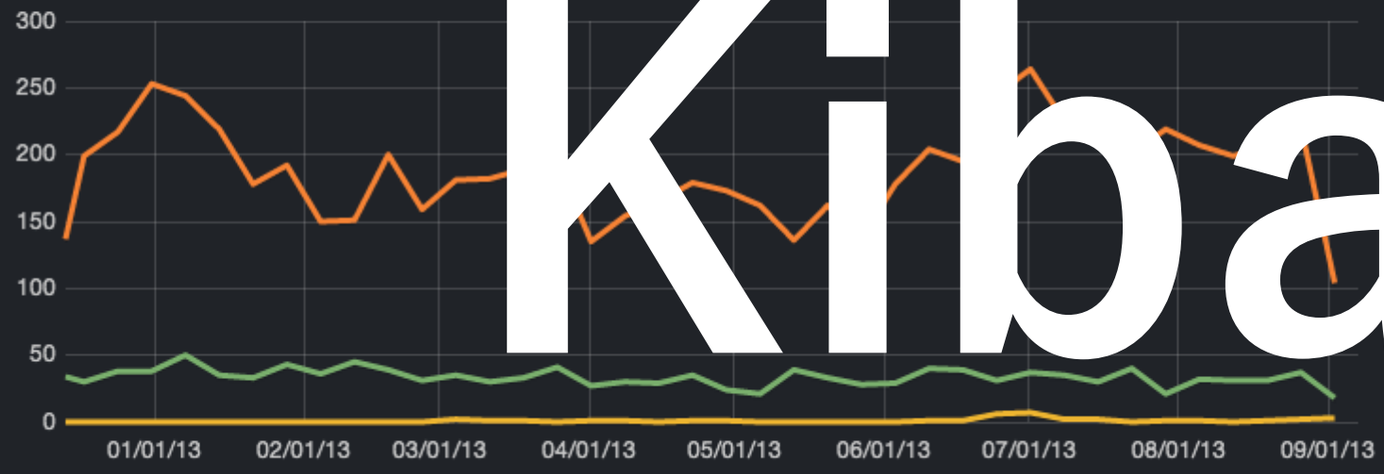
This dashboard is updated daily from data provided by **slate.com**. Every data point is a single human life taken by a gun in the United States since December 12th 2012. Click on clusters to drill down. Hover over blue markers to see the names of the deceased.

TOTAL GUN DEATHS — HITS

8637

GUN DEATHS PER WEEK — HISTOGRAM

View | Zoom Out | Men (7291) Women (1311) Unknown (35) count per **1w** | (**8637** hits)



TOTAL FIREARMS FATALITIES BY STATE — MAP

Kibana

TABLE

Fields

0 to 50 of 500 available for paging

All / Current

Type to filter...

- _id
- _index
- _type
- age
- city

date	name	gender	state	source
2013-09-06	John W. Keepers	male	WI	http://www.jsonline.com/news/crime/milwaukee-man-sh
2013-09-06	Damar Daniel Rigsby	male	CA	http://projects.latimes.com/homicide/post/damar-daniel-
2013-	Nathaniel	male	MD	http://www.baltimoresun.com/news/maryland/crime/bloc

COLUMN

FILTERS — FILTERING

querystring must
query : state:AZ

querystring must
query : state:TX

querystring must
query : state:CA

time must
field : date
from : 2012-12-13T03:30:05.000Z
to : 2013-09-06T20:42:33.250Z

今日のお話

- なぜKibana？
- Kibanaの使い方
- Kibana Tips

今日のお話

- なぜKibana？
- Kibanaの使い方
- Kibana Tips

まずは基本情報から

Kibanaとは？

- ログ解析&可視化ツール
- logstashで集めたログを可視化するために作られた
- 2013年にElasticsearchの公式ツール化
  - https://github.com/elasticsearch/kibana
- logstashへの依存はなく、fluentdなども簡単に連携可能

seamless integration with other technologies

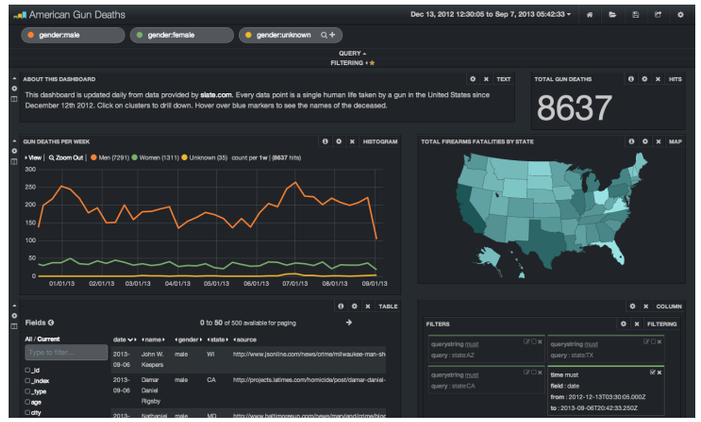
Well-suited to log aggregators like Logstash and Apache Flume, among others, Kibana fits well into a matrix of other technologies.

構成

fluentd

logstash

Elasticsearch



Kibana

特徴

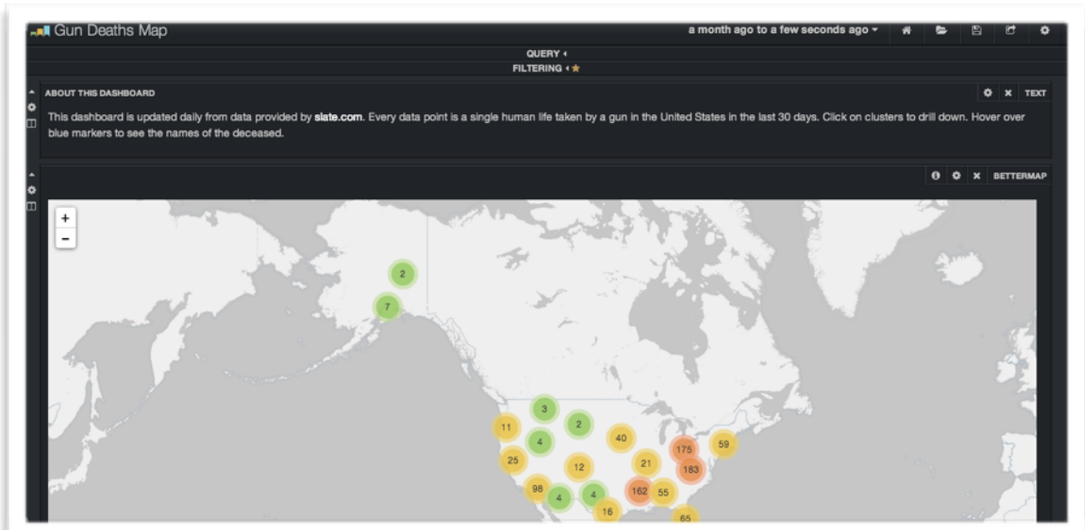
- Kibana自体はHTML/CSS/JSのみ
- つまりWebサーバだけで配信可能

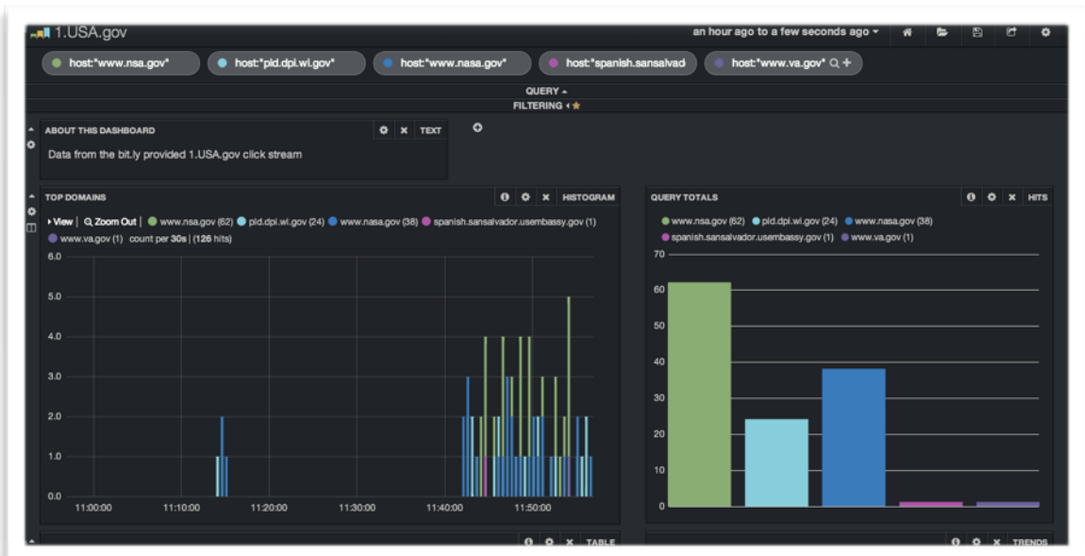
```
wget http://download.elasticsearch.org/kibana/kibana/kibana-latest.zip
unzip kibana-latest.zip
ruby -rsinatra -e 'set :public_dir, “./kibana-latest"'
```

特徴

パネルを追加して

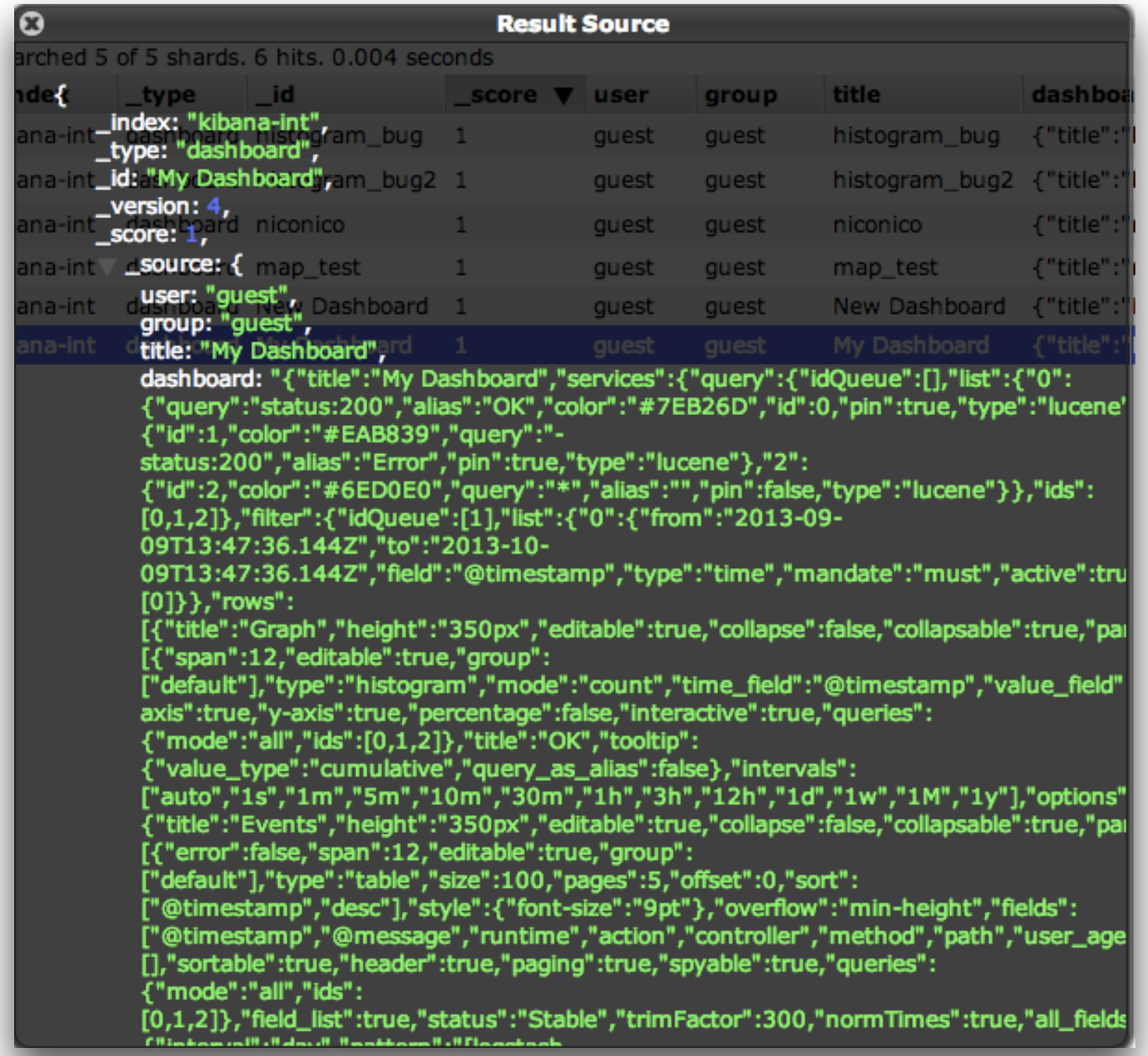
好みのダッシュボードを作れる





特徴

- 作ったダッシュボードは elasticsearchに保存
- ストレージ不要



Kibanaを使う理由

ログを見るときに

よくあること

毎回見たい条件が変わる

あるユーザのアクセスを追跡したい
このページにアクセスされた回数
iOSとAndroidのアクセス比率
平均レスポンスタイム
etc…

素早く傾向を見たい

ピークタイムは何時頃？
休日のトラフィックは平日に比べてどう？
エラーは起きていない？
etc…

でも、詳細も見たい

この時のクエリパラメータは何？
このグラフのスパイクは何？
どこからこのページに来たの？
etc…

見たい時に

見たい情報を

素早く

Kibanaなら全部できる

今日のお話

- なぜKibana？
- Kibanaの使い方
- Kibana Tips

サンプルデータ

ニコニコデータセット 動画メタデータ

http://www.nii.ac.jp/cscenter/idr/nico/nico.html

提　　供

(株)ドワンゴ

国立情報学研究所

Navigation

Jun 25, 2010 02:05:29 to Dec 30, 2012 22:37:35

QUERY

Row

Panel

VIDEOS

video (type) (7850) count per 7d | (7850 hits)

400
250
200
150
100
50

2010-07-01 2010-10-01 2011-01-01 2011-04-01 2011-07-01 2011-10-01 2012-01-01 2012-04-01 2012-07-01 2012-10-01

Panel

FORMAT

mp4 (7094) flv (458) swf (298)

mp4
90%

Row

Panel

0 to 100 of 500 available for paging

Current

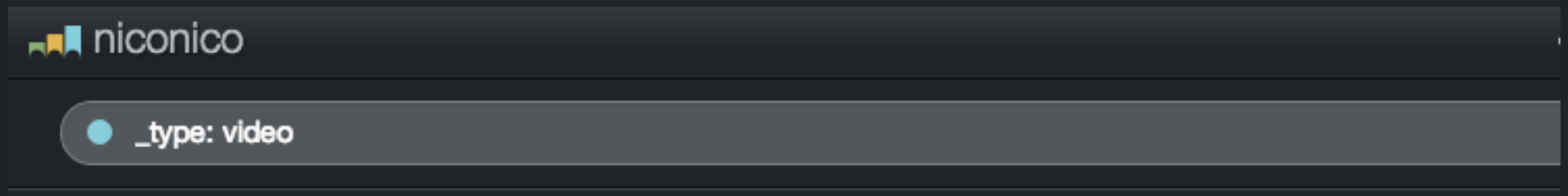
@timestamp
_id
_index

@timestamp	_type	video_id	title	length
2010-08-07T15:13:47+09:00	video	sm11663246	まどかのテーマ ～ひとりぼっちのConcert （きまぐれオレンジ☆ロード）	149
2010-11-05T06:36:07+09:00	video	sm12651318	「魔法少女まどか☆マギカ」 第１弾キャラ＆声優発表！	15
2010-11-12T03:41:29+09:00	video	sm12722302	シャフトオリジナルアニメ　魔法少女まどか★マギカ　CM	15
2010-12-06T20:51:44+09:00	video	sm12957333	魔法少女まどか★マギカ キャラクターCM集	74

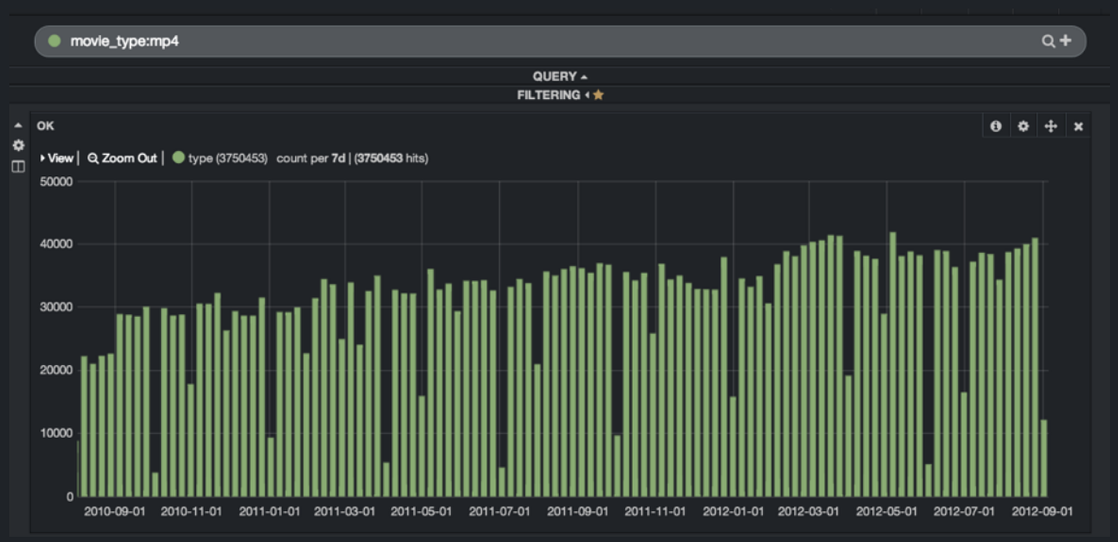
Query

検索クエリを入力する一番基本となるパネル

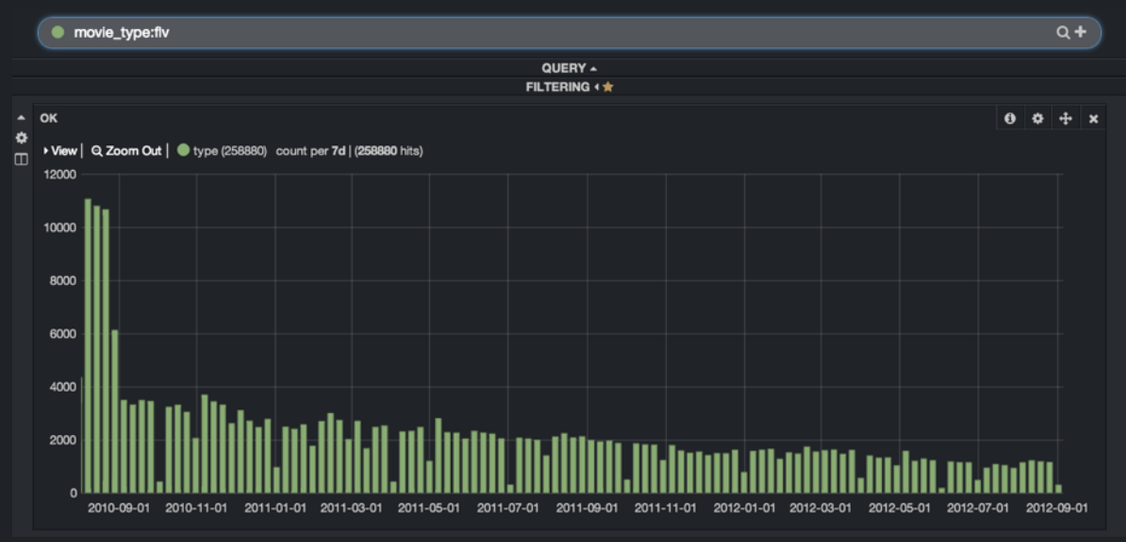
luceneクエリが書ける



movie_type:mp4

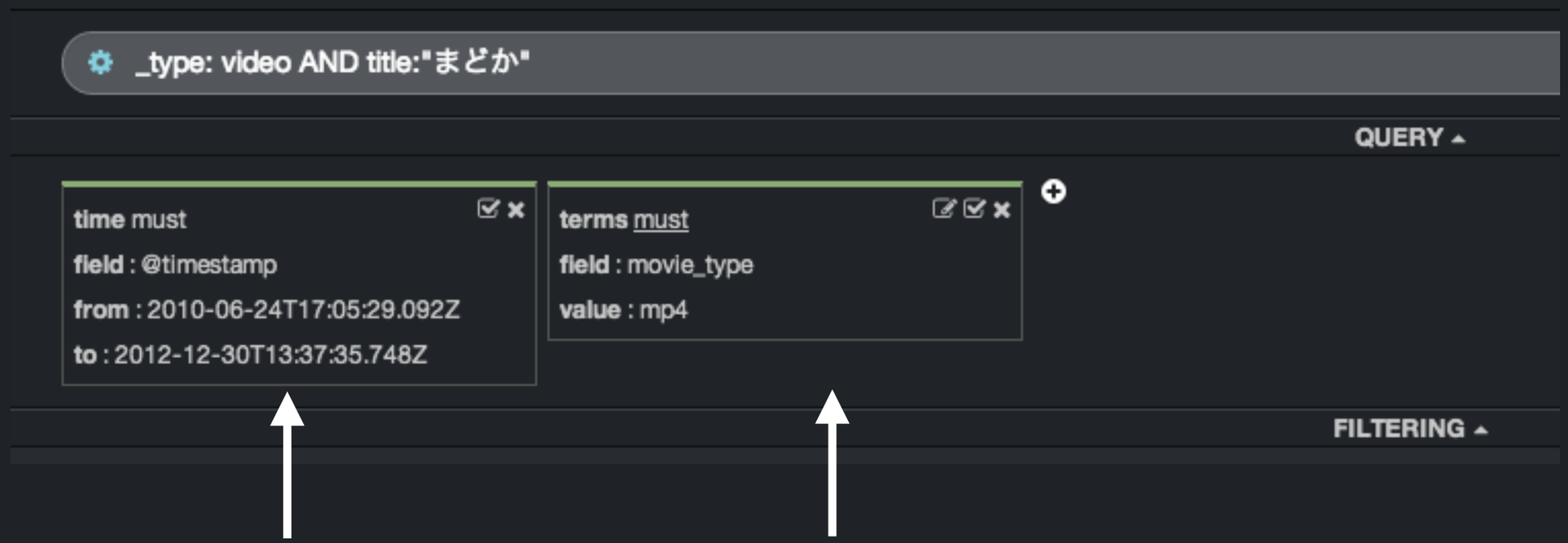


movie_type:flv



Filtering

現在のクエリに対してかかっている絞り込み条件を表示

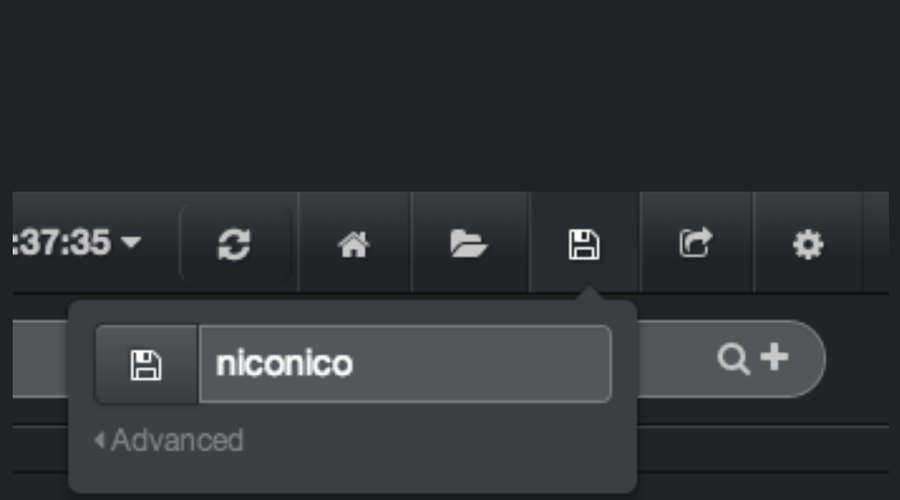


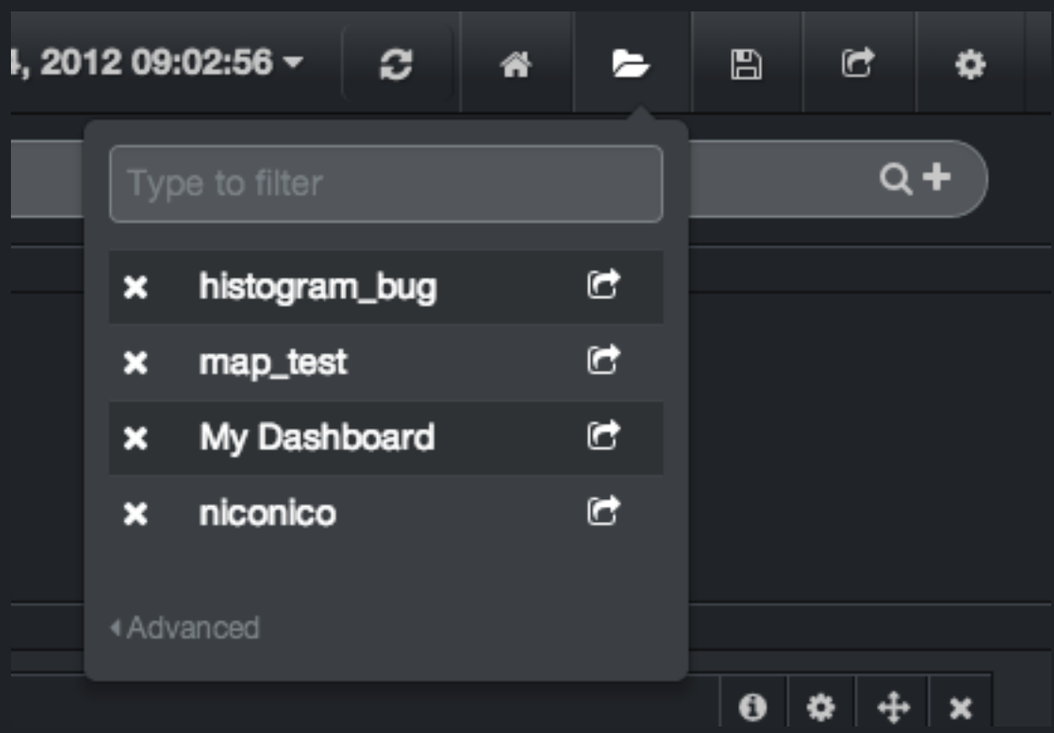
期間の絞り込み

movie_typeの絞り込み

Save & Load

elasticsearchのkibana-intインデックスから保存と読み込み

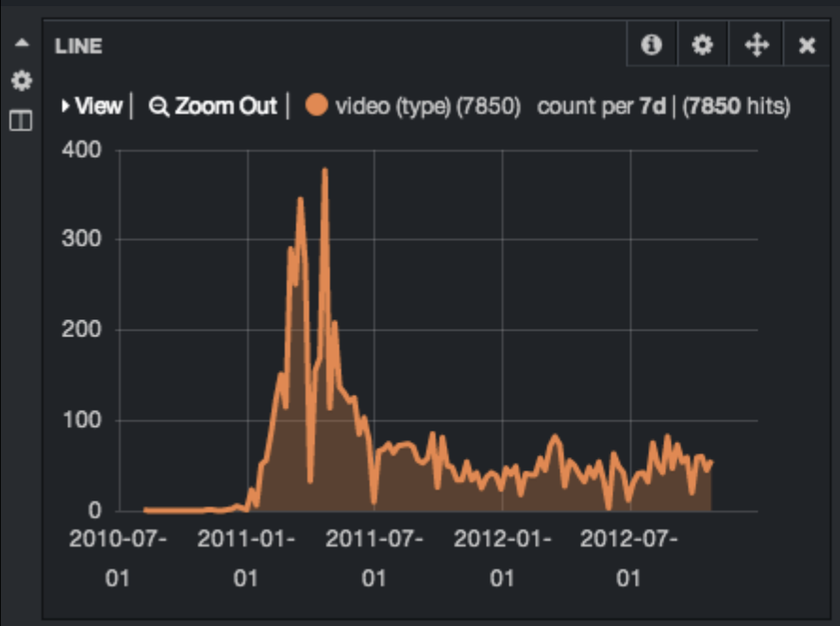




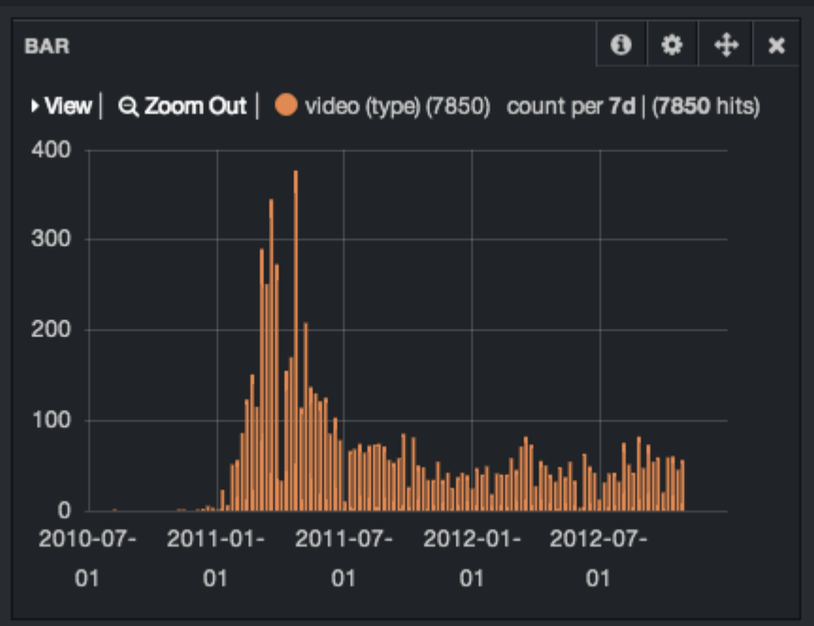
ダッシュボードを作ったら**リロード前に**必ず保存！

Histogram

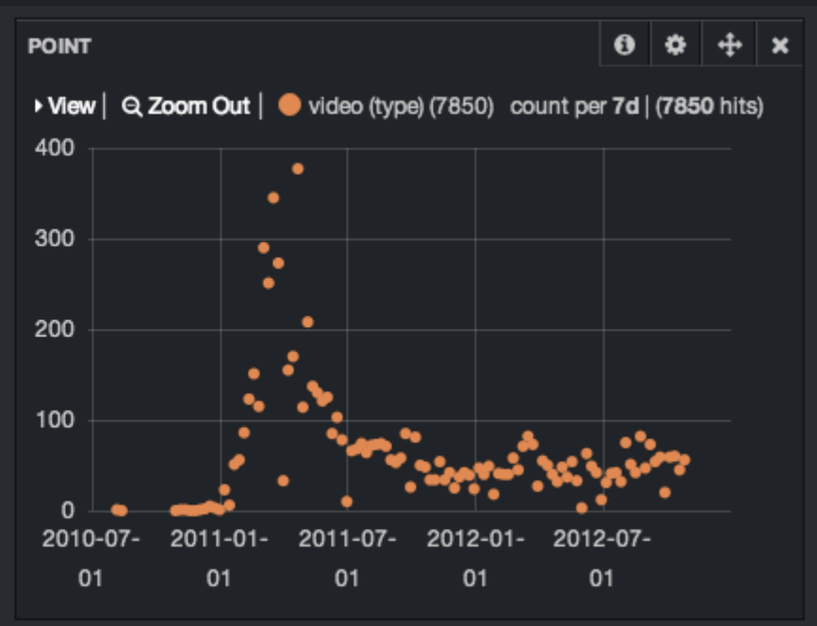
時系列データを表示する
一番使うことになるパネル



Lines



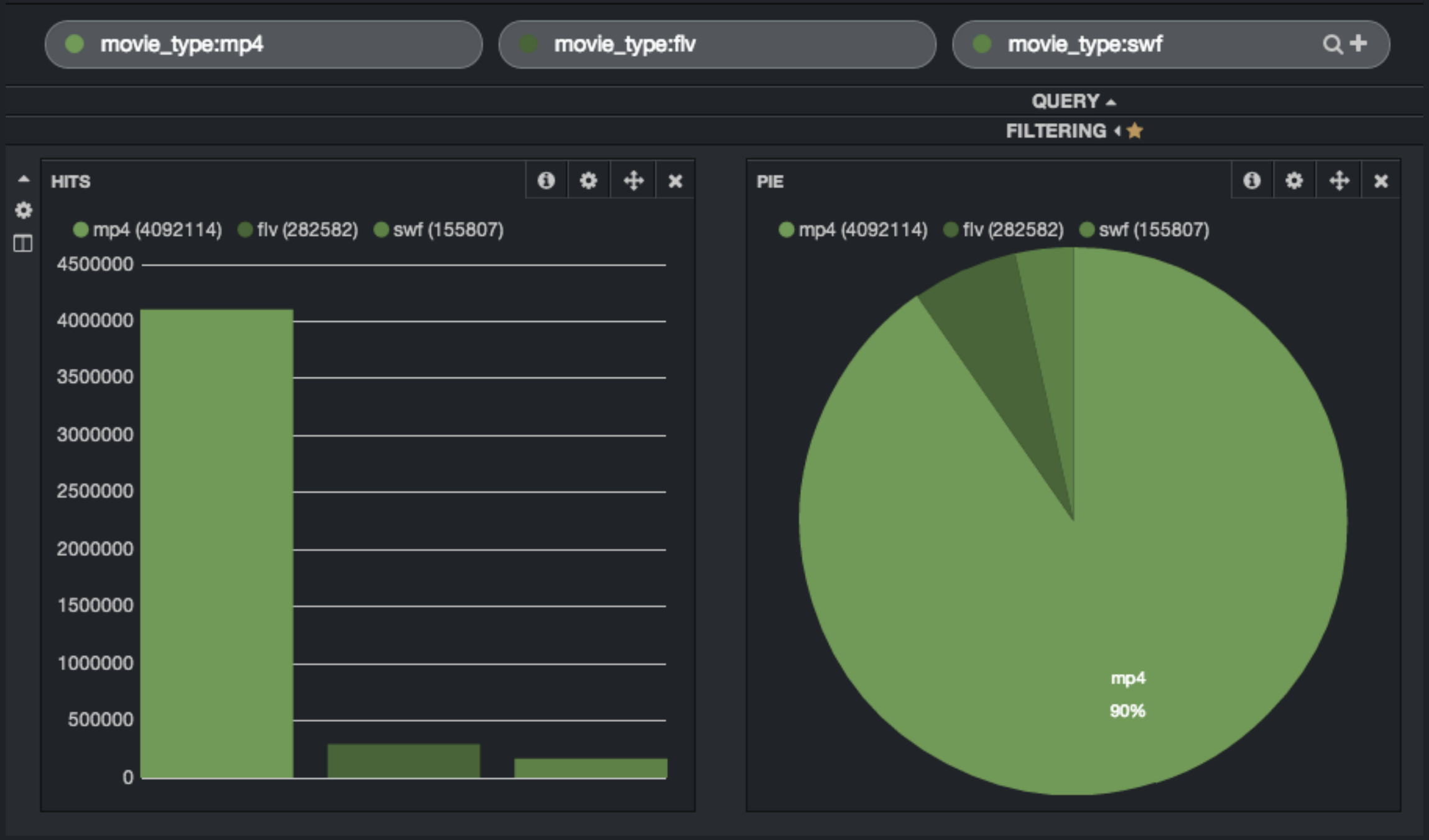
Bars



Points

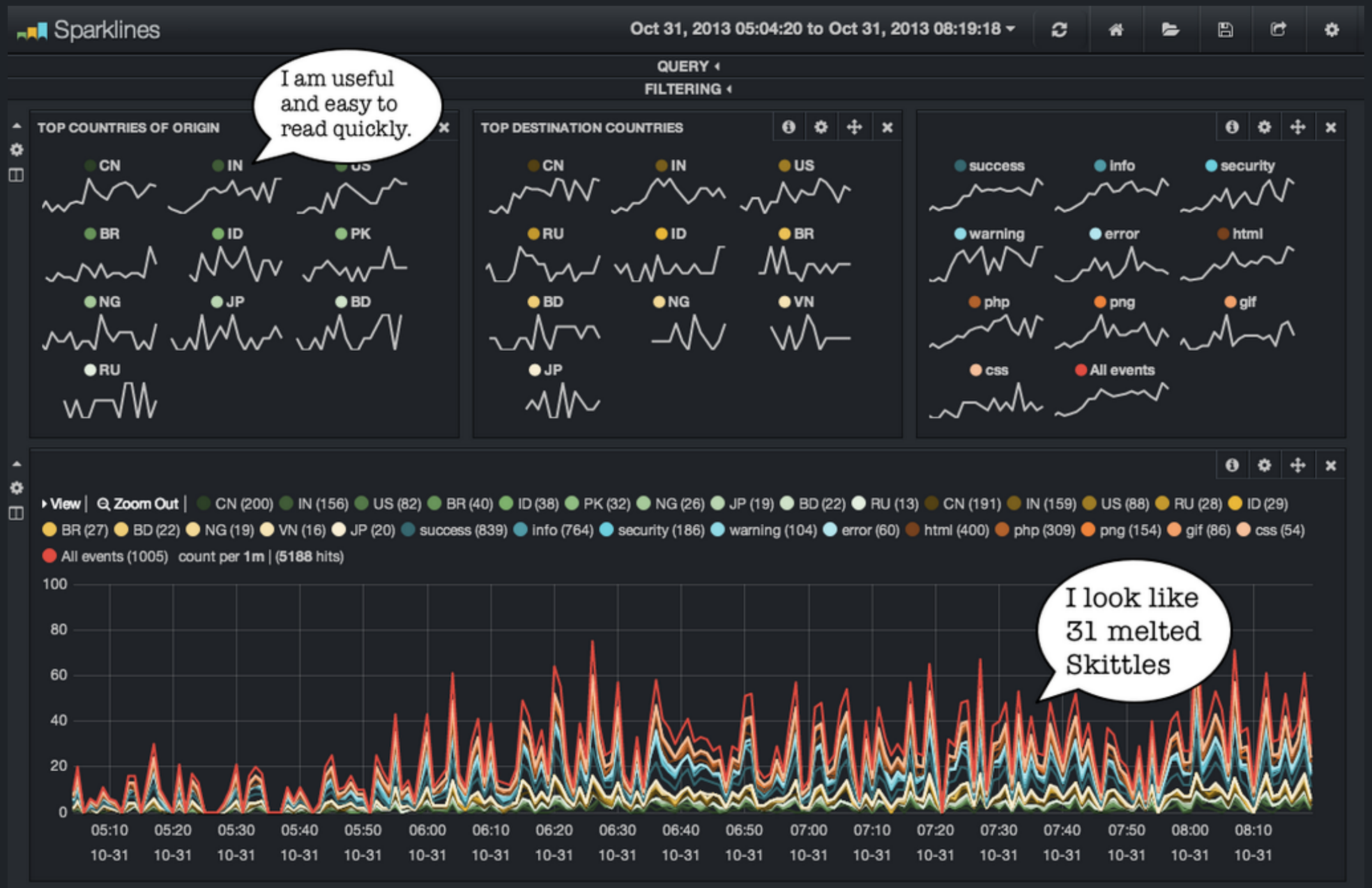
Hits

クエリごとの総ヒット件数をグラフ化



Sparklines

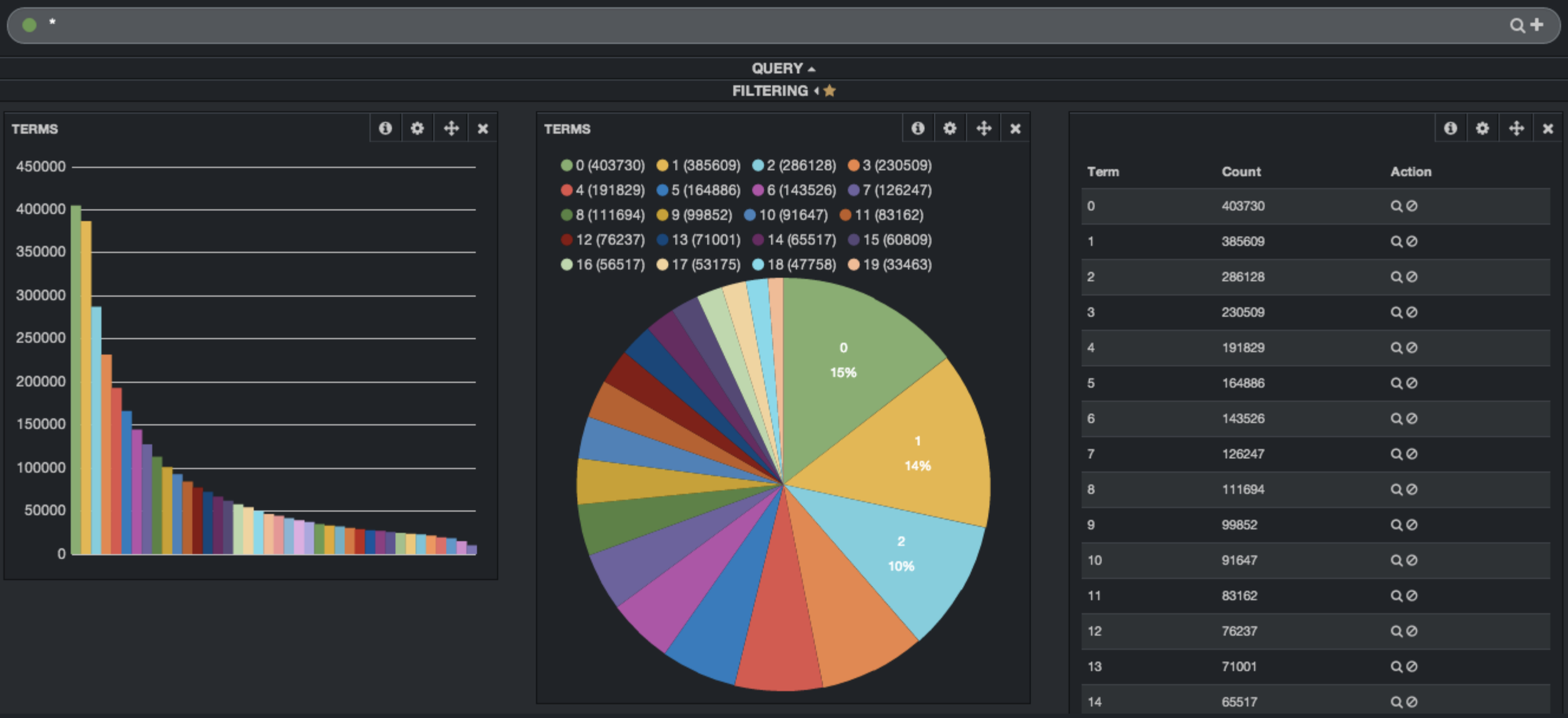
クエリごとの傾向だけを可視化



https://twitter.com/rashidkpc/status/396020792384684032

Terms

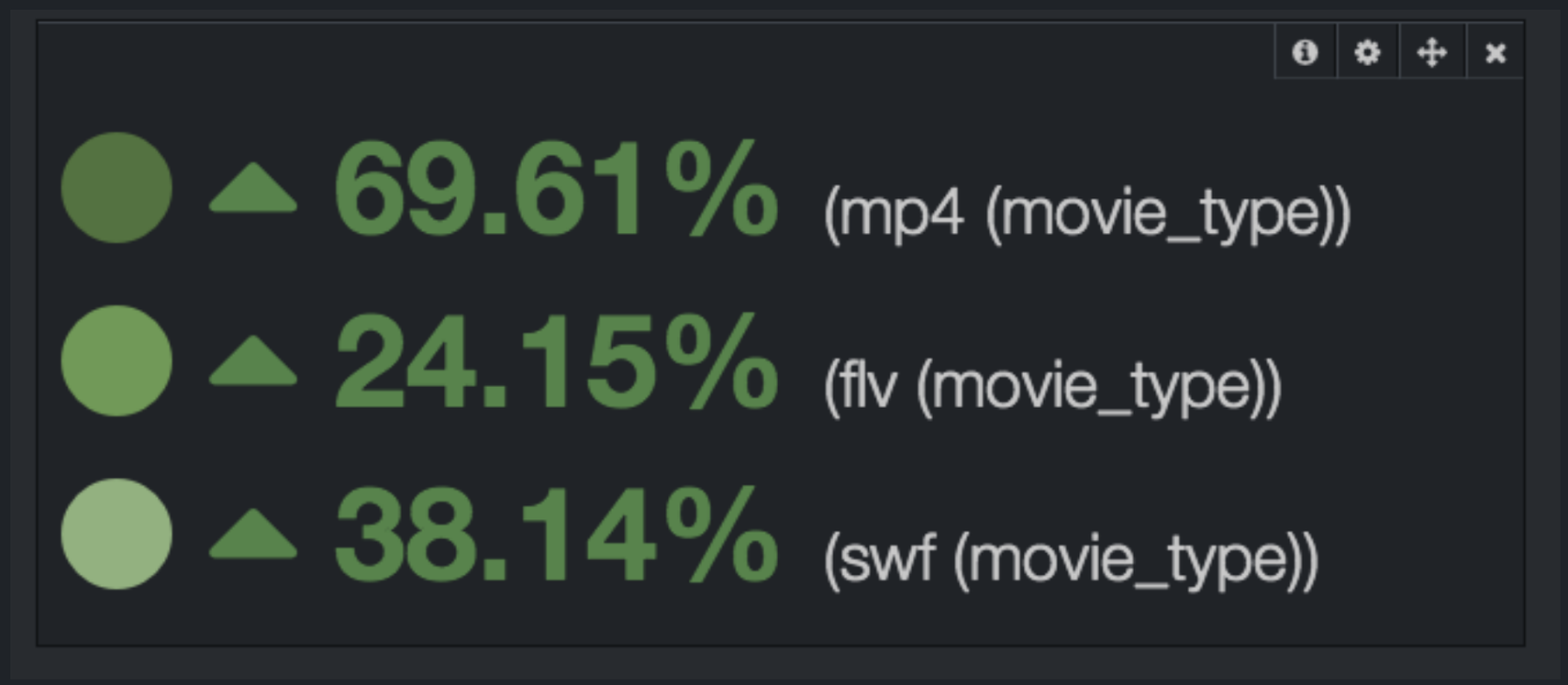
facetsの結果をBar, Pie, Tableでグラフ化



コメント数のfacet

Trends

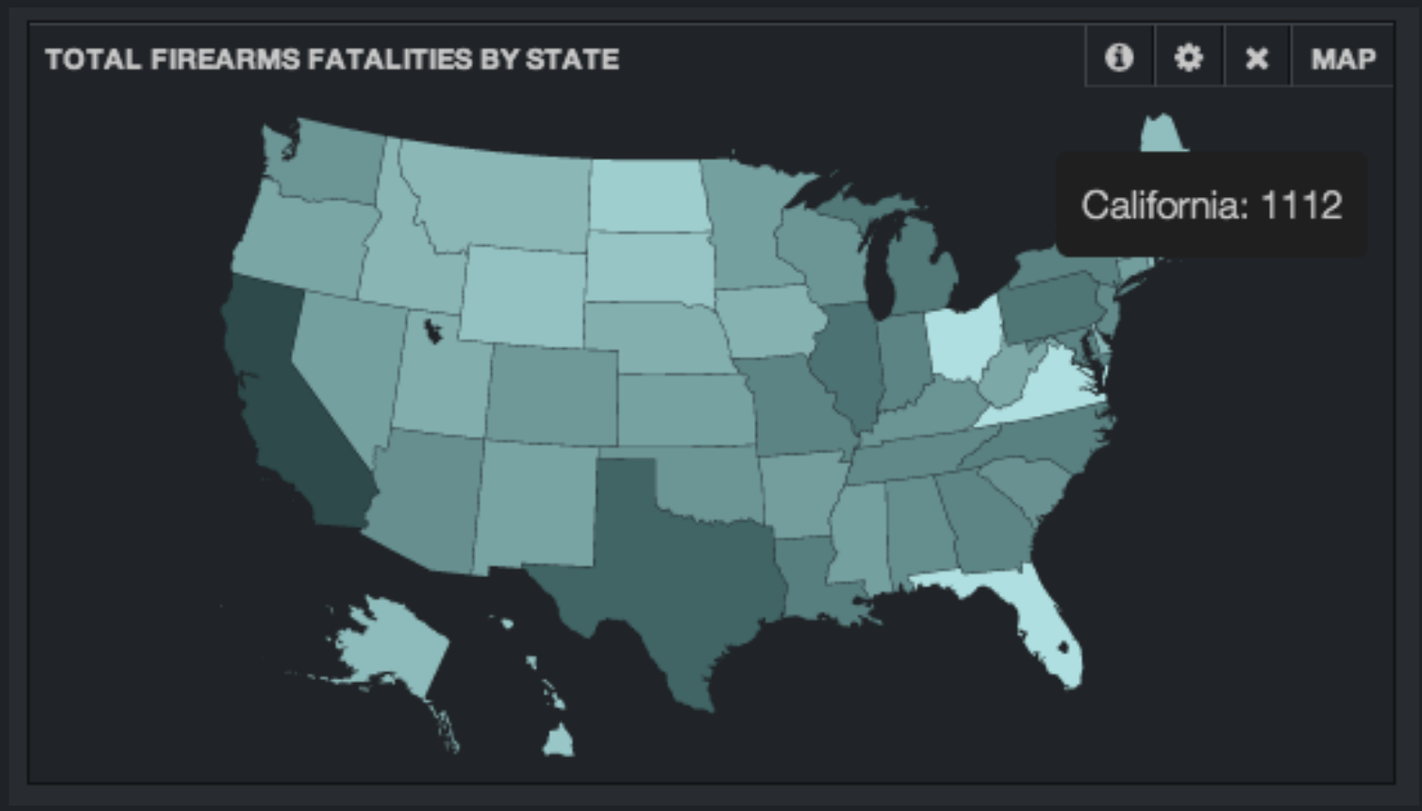
指定した時点からの値の変化を表示



「前日比N%増加」，「前年比M%減少」など

Map

facetの結果を地図上で可視化

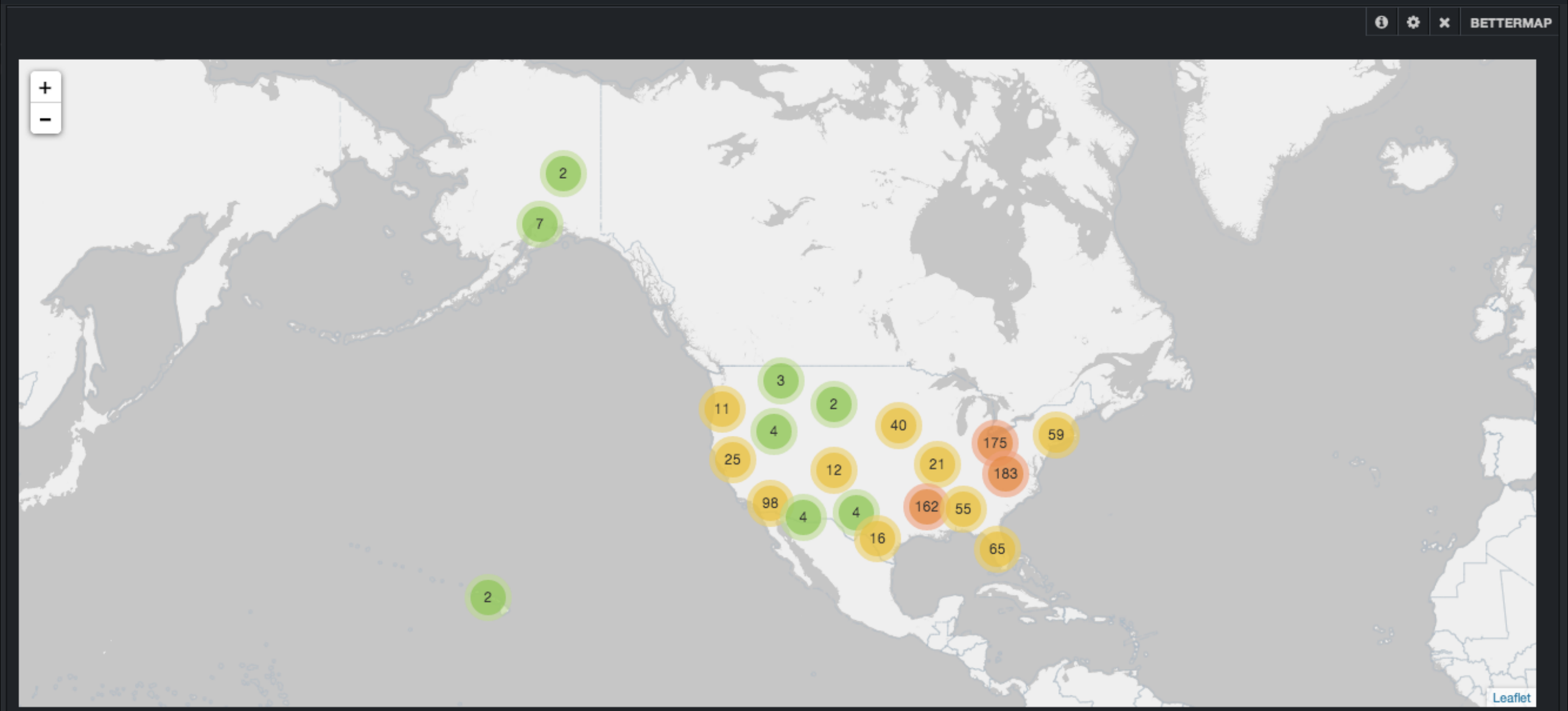


日本地図はPull requestを出したものの議論中…

https://github.com/elasticsearch/kibana/pull/630

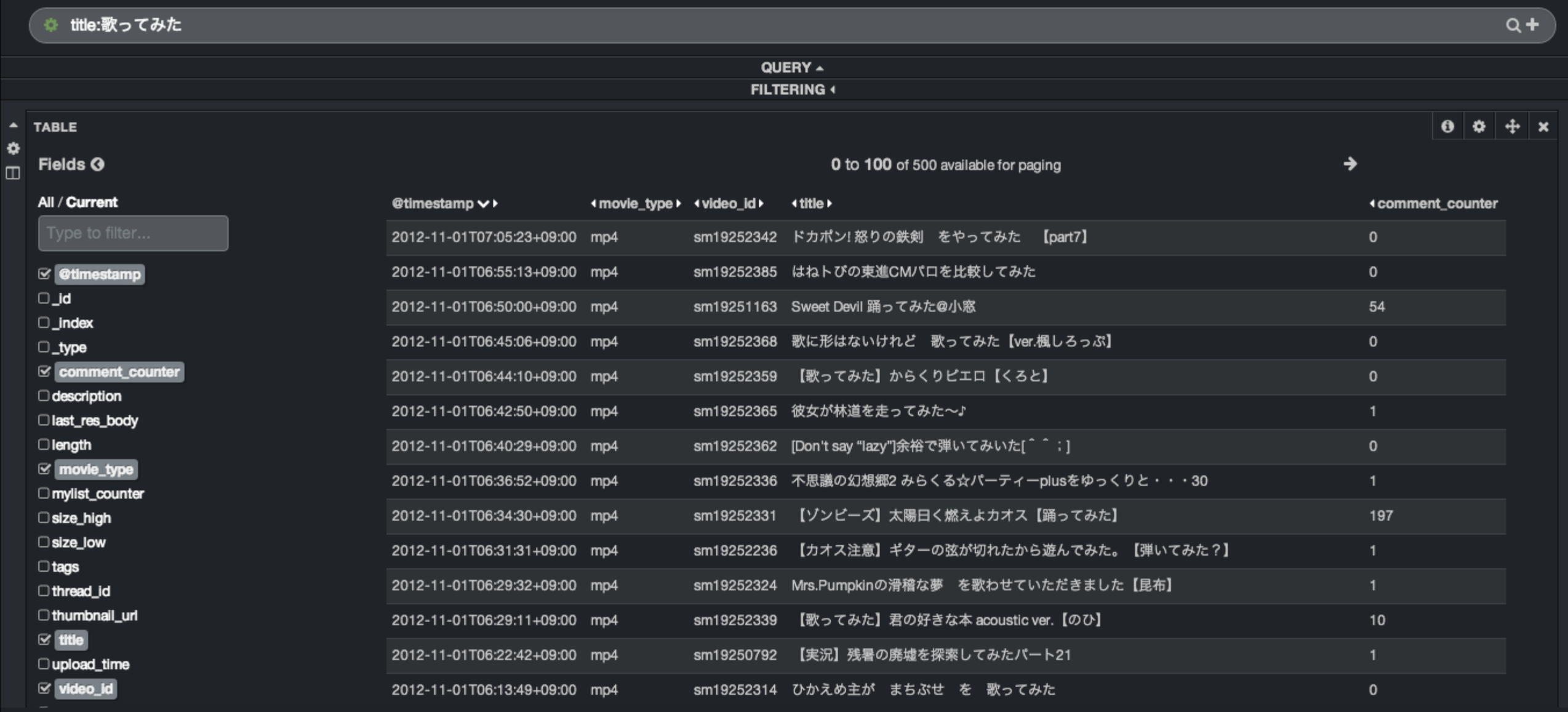
BetterMap

緯度・経度を元にマッピング



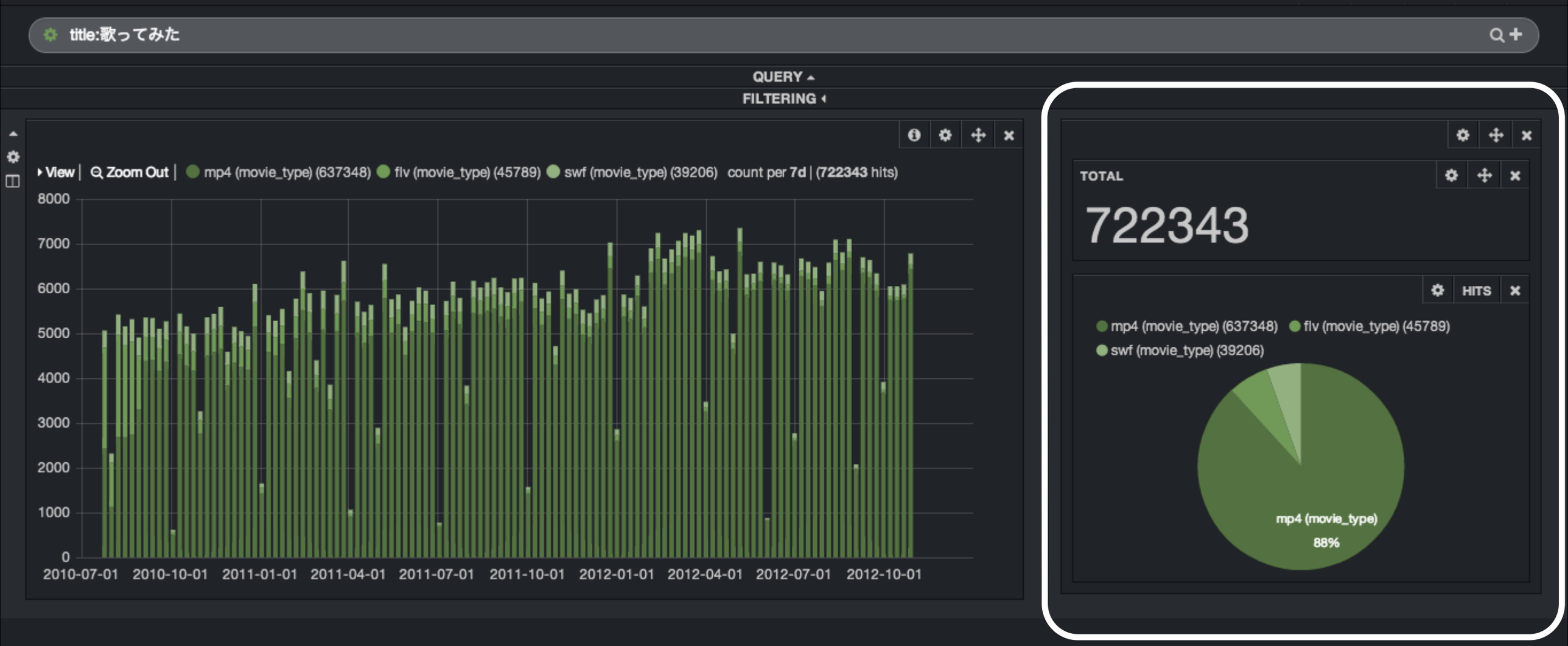
Table

クエリにマッチしたドキュメントの内容を表示



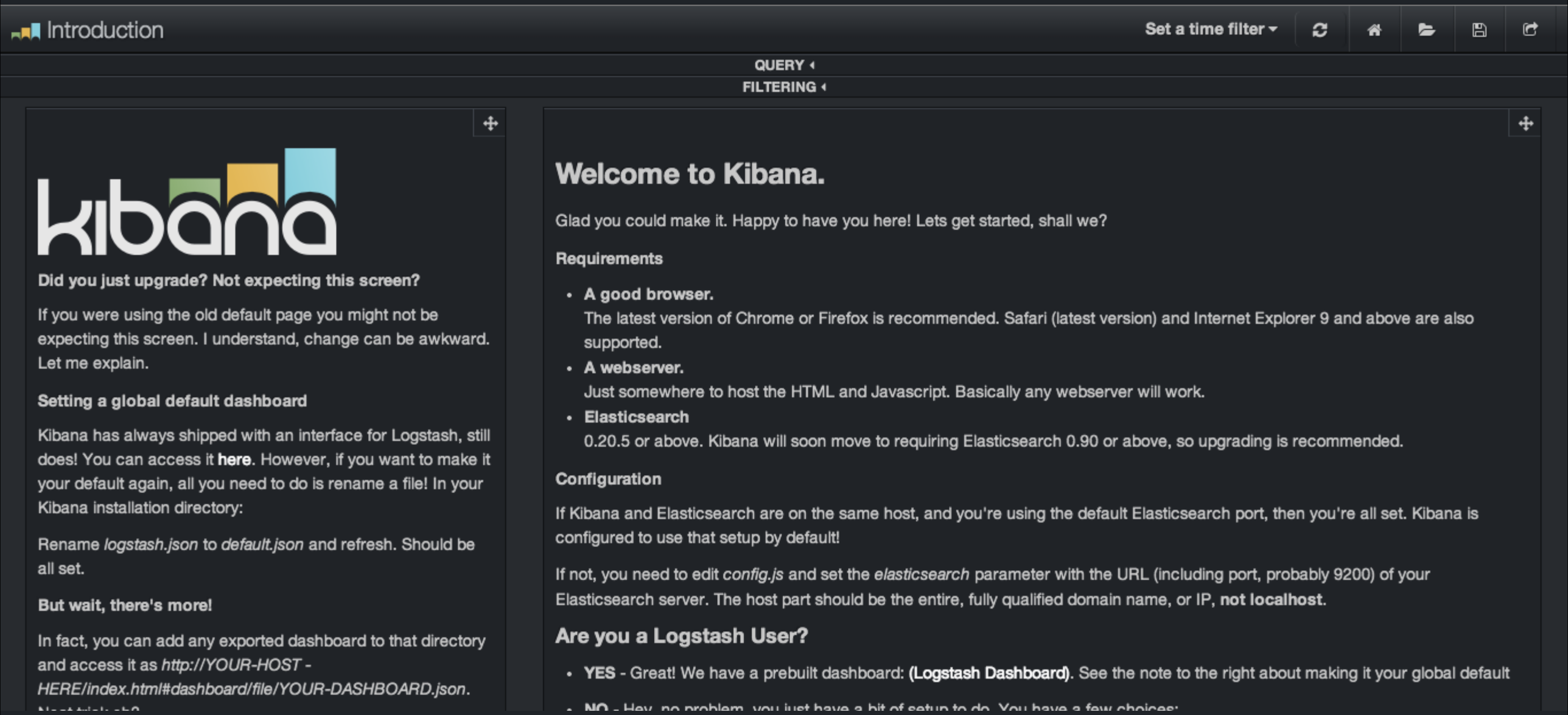
Column

パネルを縦に並べられるパネル



Text

HTML, markdown, plain textでテキストを表示



DEMO

クエリの書き方

タイトルに「**歌ってみた**」を含む動画

```
title: “歌ってみた”
```

タイトルに「**歌ってみた**」を含む**mp4**動画

```
title: “歌ってみた” AND movie_type: mp4
```

動画形式**mp4以外**の動画

```
-movie_type: mp4
```

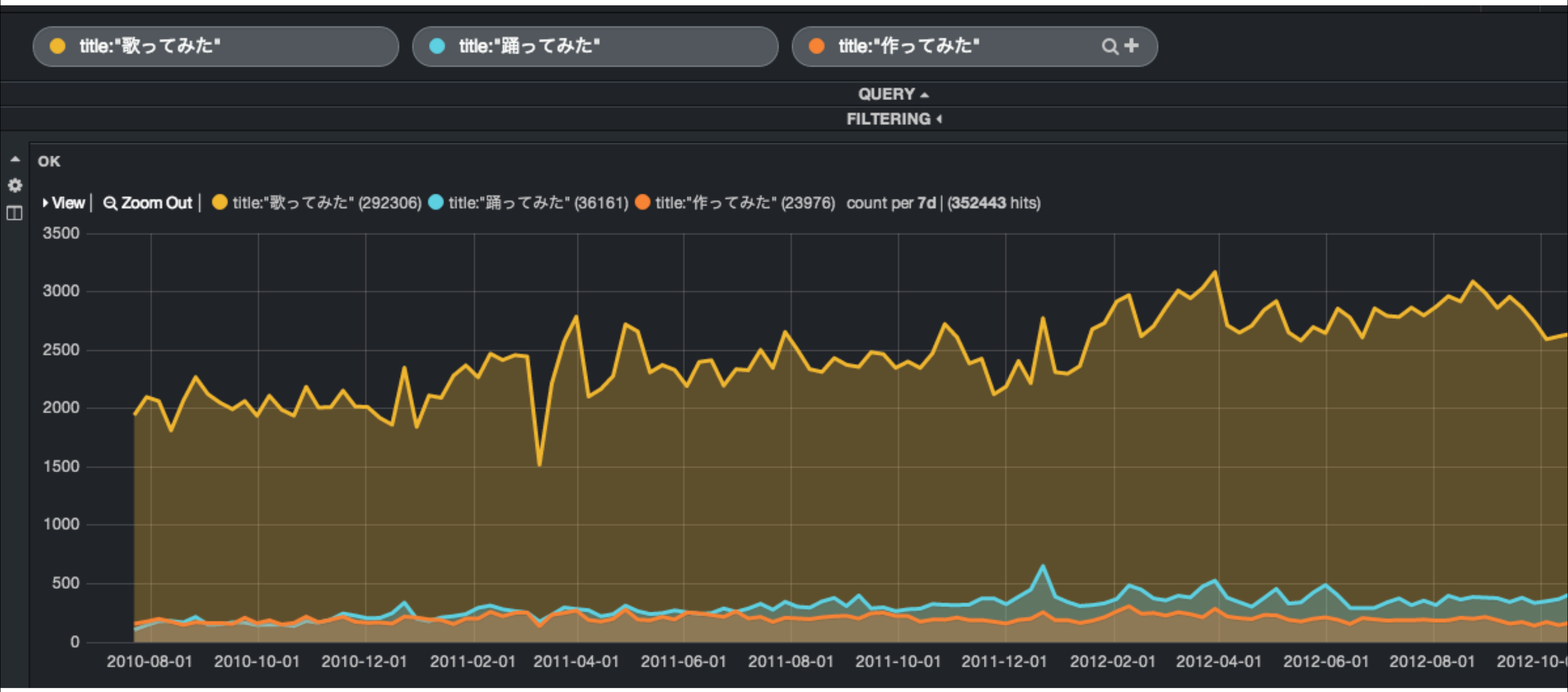
または

```
NOT(movie_type: mp4)
```

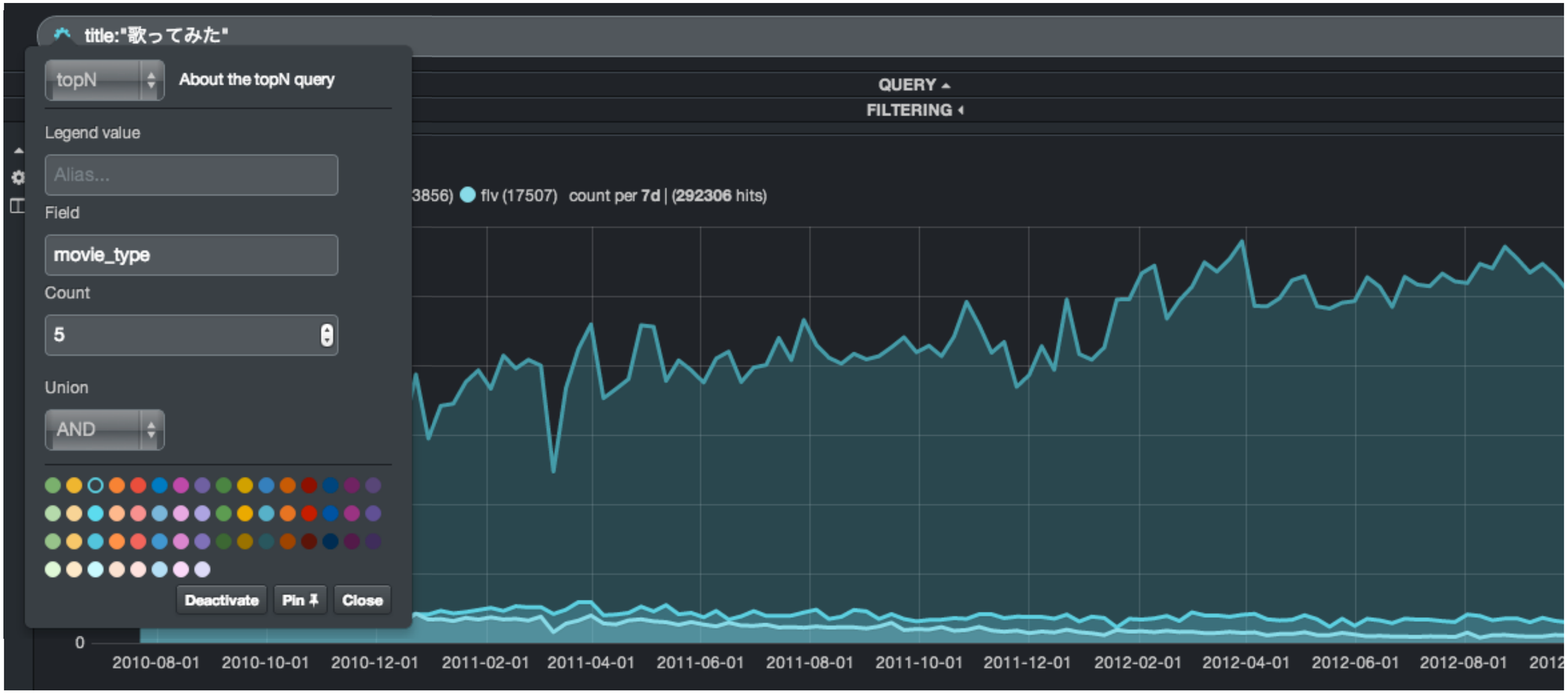
再生時間**1分未満**の動画

```
length: [* TO 60]
```

複数のクエリの結果を比較

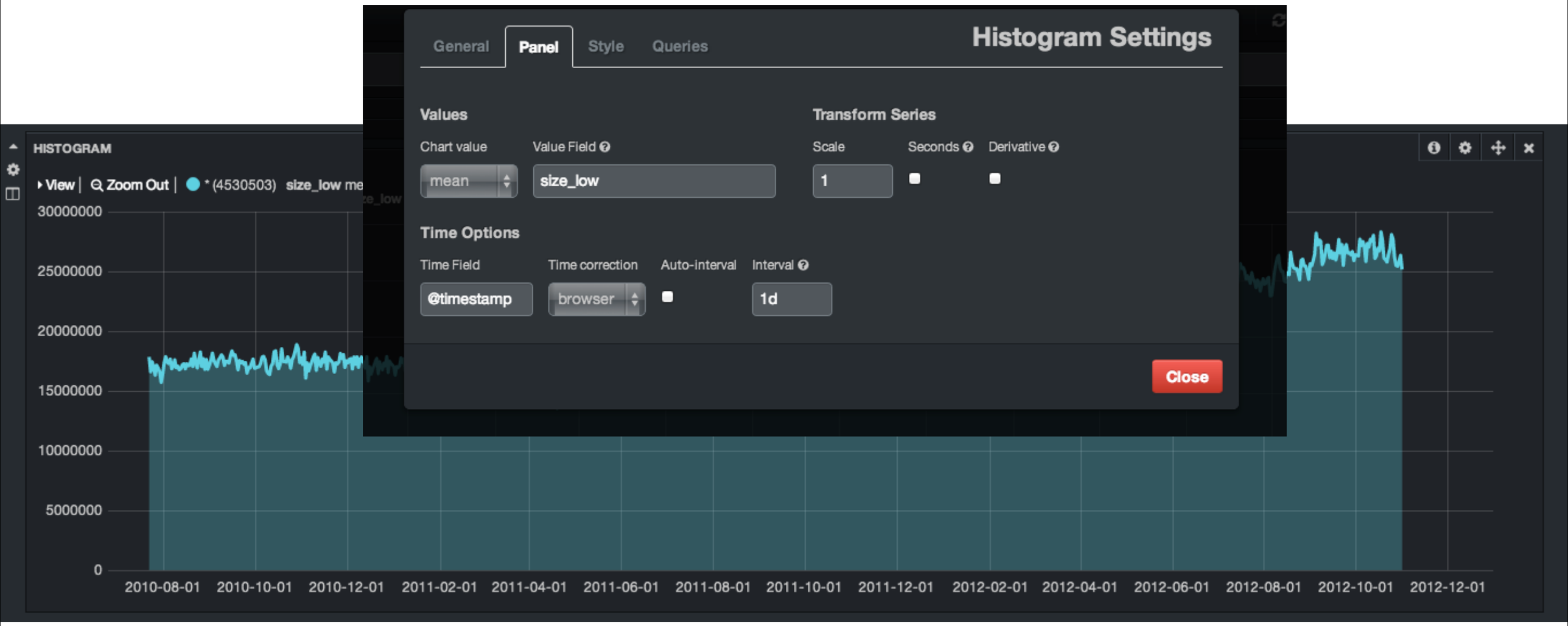


動画形式の比較



facetで取得したキーワードから自動的に検索

動画ファイルサイズの平均値



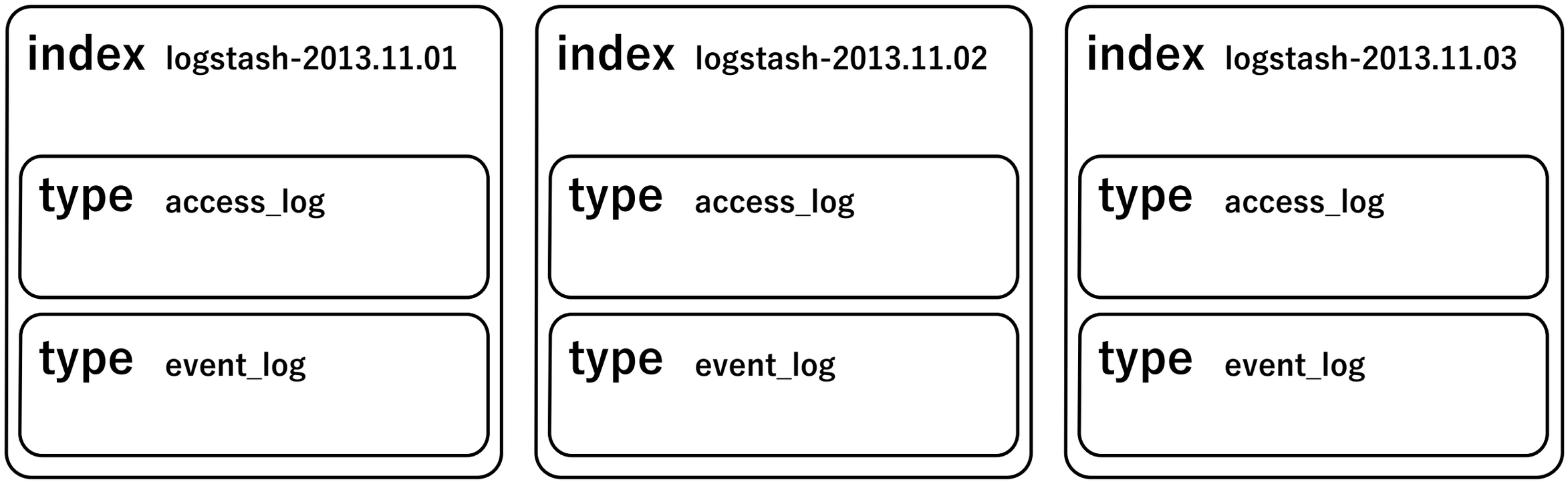
数値フィールドの平均値をグラフ化

他に、最大値、最小値、合計も計算可能

今日のお話

- なぜKibana？
- Kibanaの使い方
- Kibana Tips

indexとtype



1つのindexに異なるスキーマを持つデータを入れられる

1つのindexに入れることでグラフを重ねて比較などができる

mapping

- mappingは自動的に定義される
- 大概、ちょっとうまくいかない
  - 数値型がintegerではなくlongになる
  - パス文字列が分かち書きされてしまう
  - など

index template

```
curl -XPUT localhost:9200/_template/logstash_template
```

logstash-で始まるindexに自動的に適用

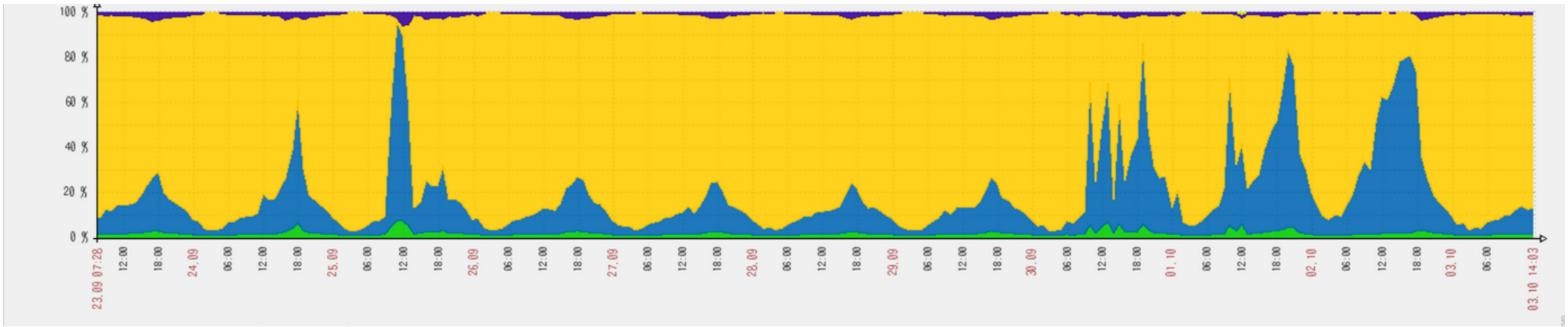
typeがaccess_logのドキュメントに適用

1つのプロパティを複数のfieldに展開

分かち書きをしない

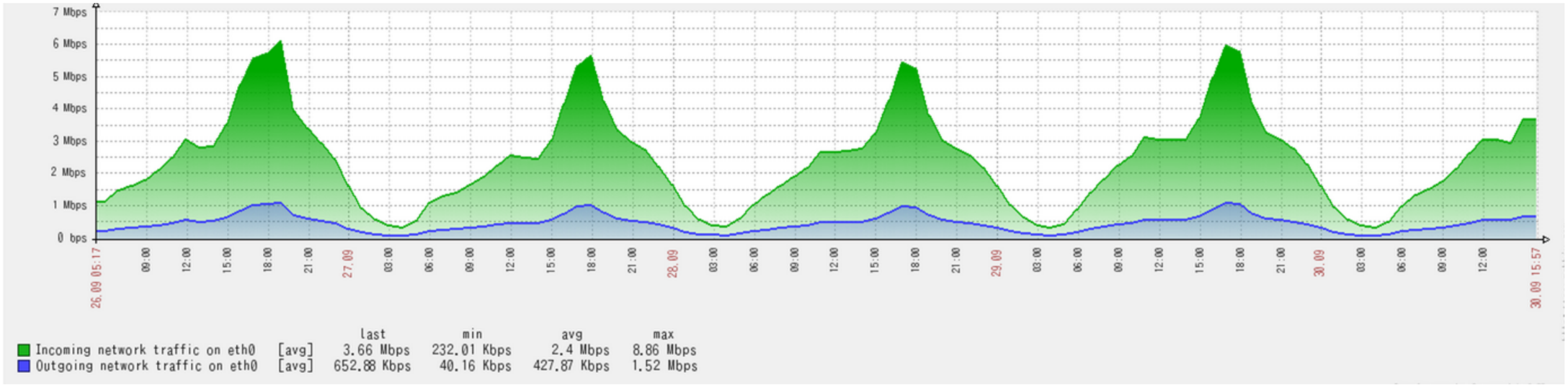
```
{
    "template": "logstash-*",
    "settings" : {
        "number_of_shards" : 1,
        "number_of_replicas" : 0
    },
    "mappings": {
        “access_log": {
            "_source": { "compress": true },
            "dynamic_templates": [
                {
                    "string_template" : {
                        "match" : "*",
                        "mapping": { "type": "string", "index": "not_analyzed" },
                        "match_mapping_type" : "string"
                    }
                }
            ],
            "properties" : {
              "path" : {
                "type": "multi_field",
                "fields" : {
                    "analyzed" : {"type":"string", "index" : "analyzed"},
                    "no_analyzed": {"type":"string", "index" : "not_analyzed"}
                }
              },
              "agent" : {
                "type": "multi_field",
                "fields" : {
                    "analyzed" : {"type":"string", "index" : "analyzed"},
                    "no_analyzed": {"type":"string", "index" : "not_analyzed"}
                }
              },
              "referer" : {
                "type": "multi_field",
                "fields" : {
                    "analyzed" : {"type":"string", "index" : "analyzed"},
                    "no_analyzed": {"type":"string", "index" : "not_analyzed"}
                }
              },
              "@timestamp" : { "type" : "date", "index" : "not_analyzed" }
            }
        }
    }
}
```

性能



- EC2 m1.large × 1台
- 1日のインデックスサイズが10GBを超えるあたりで elasticsearchが詰まり始める
- OutOfMemoryErrorなどを吐いてほとんどimportを受け付けなくなる
- fluentdにデータがたまりバッファオーバーでデータを失う…

性能



- **その後、JVMのGCパラメータチューニングによりなんとか安定**
- **ピーク時で6Mbps程度のトラフィックに耐えられることを確認**

オブジェクトが大量に生成、削除されることで頻繁にFull GCが走っていたのが原因

New領域のサイズを広げてScavenge GCで回収されるようにすることでFull GCの発生頻度をできるだけ下げるようにした

チューニングの詳細については
@con_mame に聞いてください

最新情報を追う

- **githubのmaster** https://github.com/elasticsearch/kibana
  - **毎日のように機能追加やデザイン変更が起きています**
  - **たまにちょっと壊れてます**
- **公式blog** http://www.elasticsearch.org/blog/
  - **Kibanaの記事は1,2ヶ月に1本ですが唯一の新機能紹介情報です**
- **demo.kibana.org** http://demo.kibana.org/
  - **手っ取り早く最新版を試せる**