

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



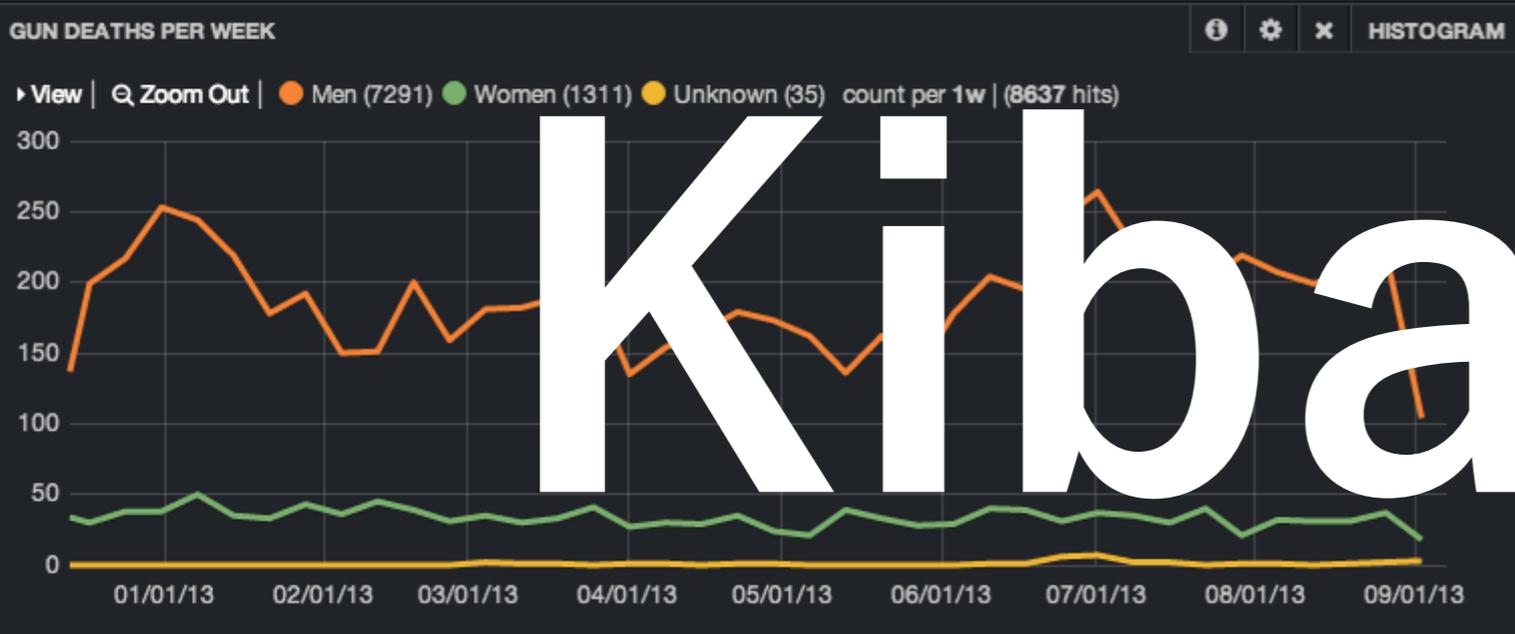
@y_310

gender:male gender:female gender:unknown

QUERY FILTERING

ABOUT THIS DASHBOARD 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 8637



Kibana

Table with columns: date, name, gender, state, source. Shows entries for John W. Keepers, Damar Daniel Rigsby, and Nathaniel.

FILTERS section with querystring and time filters for state:AZ, state:TX, and state:CA.

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？

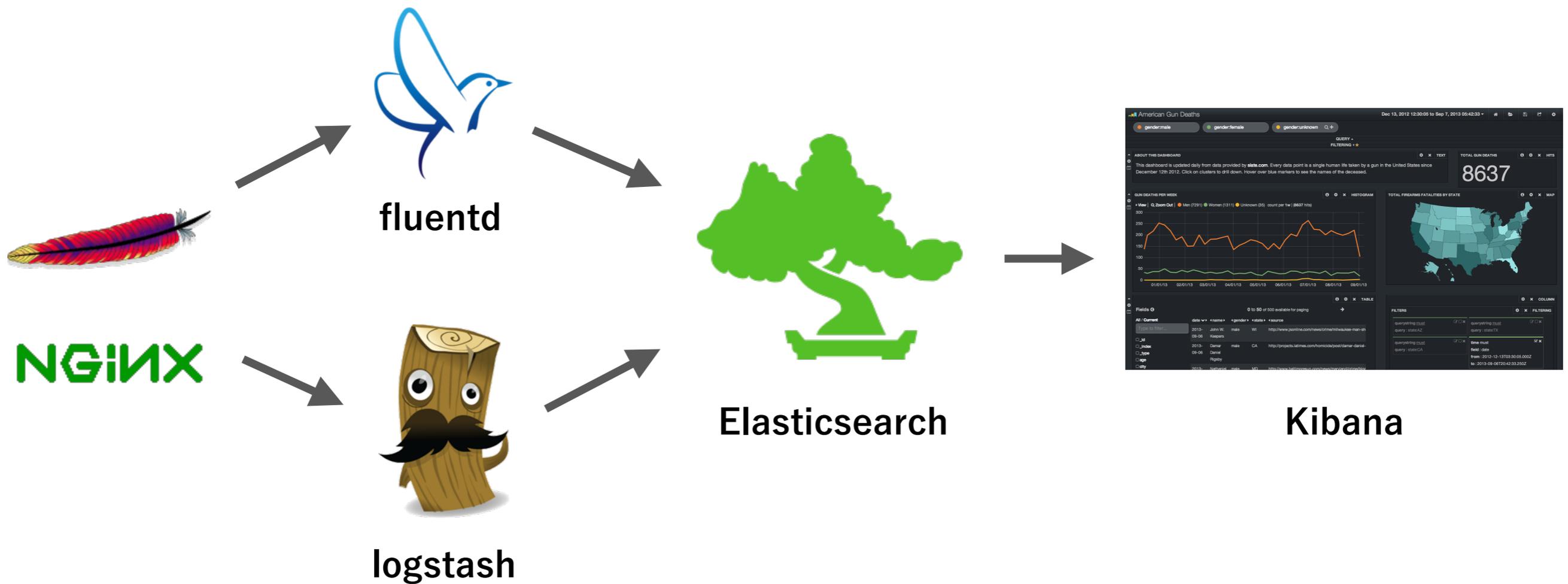
- ログ解析&可視化ツール
- logstashで集めたログを可視化するために作られた
- 2013年にElasticsearchの公式ツール化
 - <https://github.com/elasticsearch/kibana>
- logstashへの依存はなく、fluentdなども簡単に連携可能

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



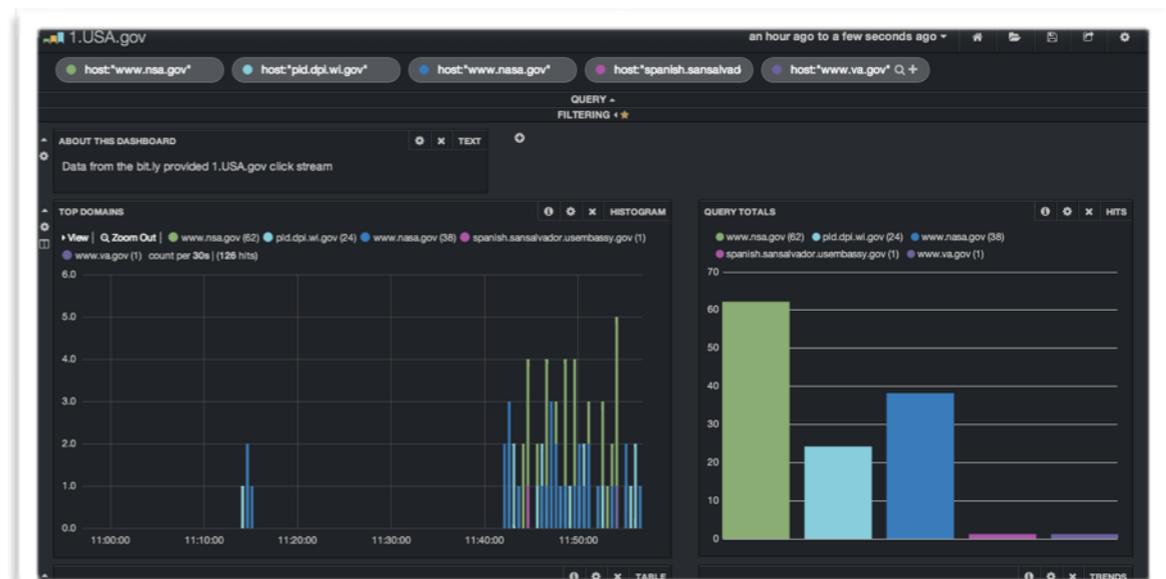
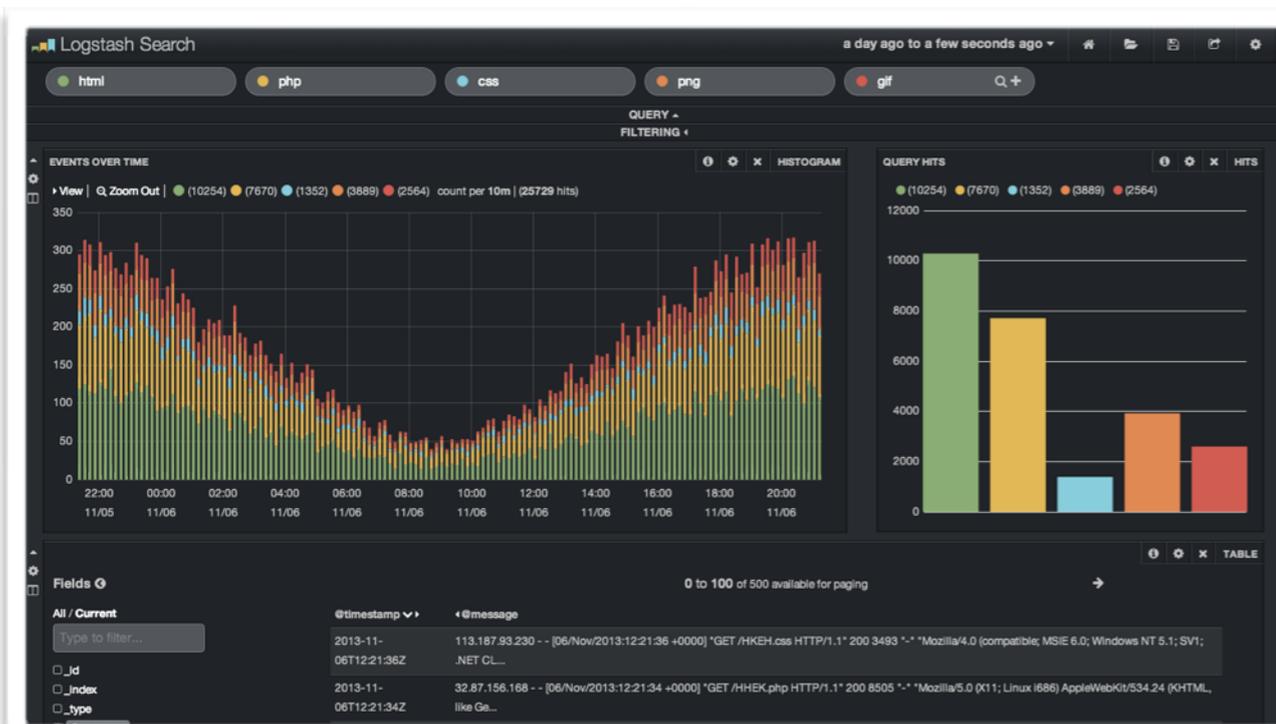
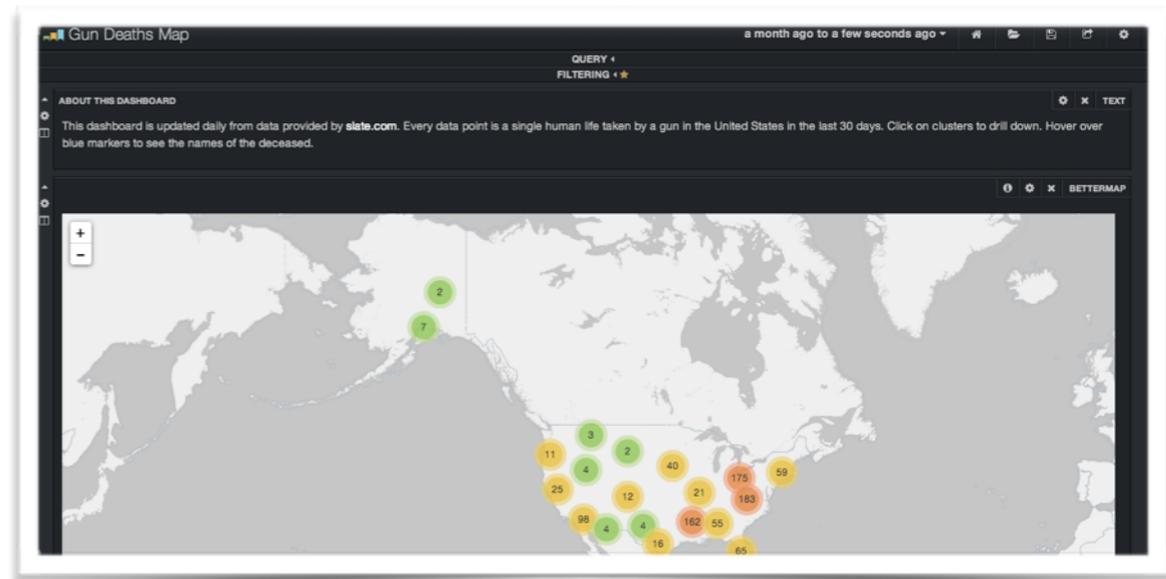
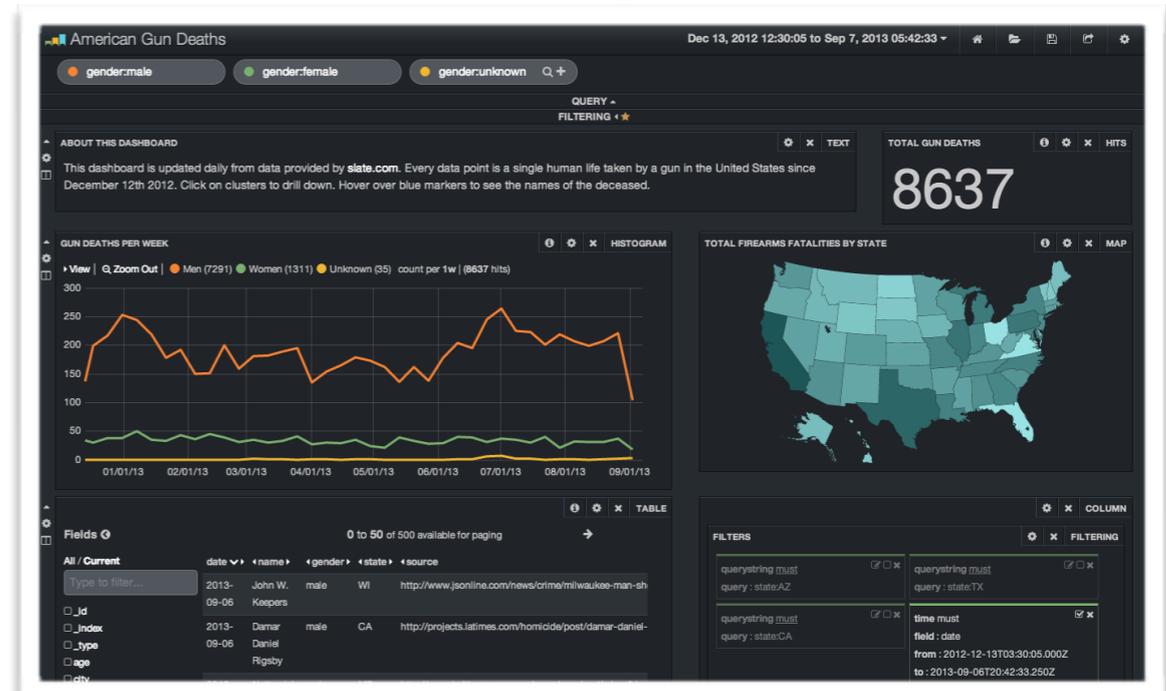
特徴

- 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

```
Result Source
arched 5 of 5 shards. 6 hits. 0.004 seconds
index: kibana-int
_type: dashboard
_id: My Dashboard
version: 4
_score: 1
_source: {
  user: guest
  group: guest
  title: My Dashboard
  dashboard: {
    "title": "My Dashboard",
    "services": {
      "query": {
        "idQueue": [],
        "list": {
          "0": {
            "query": "status:200",
            "alias": "OK",
            "color": "#7EB26D",
            "id": 0,
            "pin": true,
            "type": "lucene"
          },
          "1": {
            "id": 1,
            "color": "#EAB839",
            "query": "-
            status:200",
            "alias": "Error",
            "pin": true,
            "type": "lucene"
          },
          "2": {
            "id": 2,
            "color": "#6ED0E0",
            "query": "*",
            "alias": "",
            "pin": false,
            "type": "lucene"
          }
        }
      },
      "ids": [0,1,2]},
      "filter": {
        "idQueue": [1],
        "list": {
          "0": {
            "from": "2013-09-09T13:47:36.144Z",
            "to": "2013-10-09T13:47:36.144Z",
            "field": "@timestamp",
            "type": "time",
            "mandate": "must",
            "active": true
          }
        }
      },
      "rows": [
        {
          "title": "Graph",
          "height": "350px",
          "editable": true,
          "collapse": false,
          "collapsible": true,
          "panel": {
            "span": 12,
            "editable": true,
            "group": [
              "default",
              "type": "histogram",
              "mode": "count",
              "time_field": "@timestamp",
              "value_field": "count",
              "axis": true,
              "y-axis": true,
              "percentage": false,
              "interactive": true,
              "queries": {
                "mode": "all",
                "ids": [0,1,2]},
                "title": "OK",
                "tooltip": {
                  "value_type": "cumulative",
                  "query_as_alias": false
                },
                "intervals": [
                  "auto",
                  "1s",
                  "1m",
                  "5m",
                  "10m",
                  "30m",
                  "1h",
                  "3h",
                  "12h",
                  "1d",
                  "1w",
                  "1M",
                  "1y"
                ],
                "options": {
                  "title": "Events",
                  "height": "350px",
                  "editable": true,
                  "collapse": false,
                  "collapsible": true,
                  "panel": {
                    "error": false,
                    "span": 12,
                    "editable": true,
                    "group": [
                      "default",
                      "type": "table",
                      "size": 100,
                      "pages": 5,
                      "offset": 0,
                      "sort": [
                        "@timestamp",
                        "desc"
                      ],
                      "style": {
                        "font-size": "9pt"
                      },
                      "overflow": "min-height",
                      "fields": [
                        "@timestamp",
                        "@message",
                        "runtime",
                        "action",
                        "controller",
                        "method",
                        "path",
                        "user_agent"
                      ],
                      "sortable": true,
                      "header": true,
                      "paging": true,
                      "spyable": true,
                      "queries": {
                        "mode": "all",
                        "ids": [0,1,2]},
                        "field_list": true,
                        "status": "Stable",
                        "trimFactor": 300,
                        "normTimes": true,
                        "all_fields": true
                      }
                    }
                  }
                }
              }
            ]
          }
        }
      ]
    }
  }
}
```

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

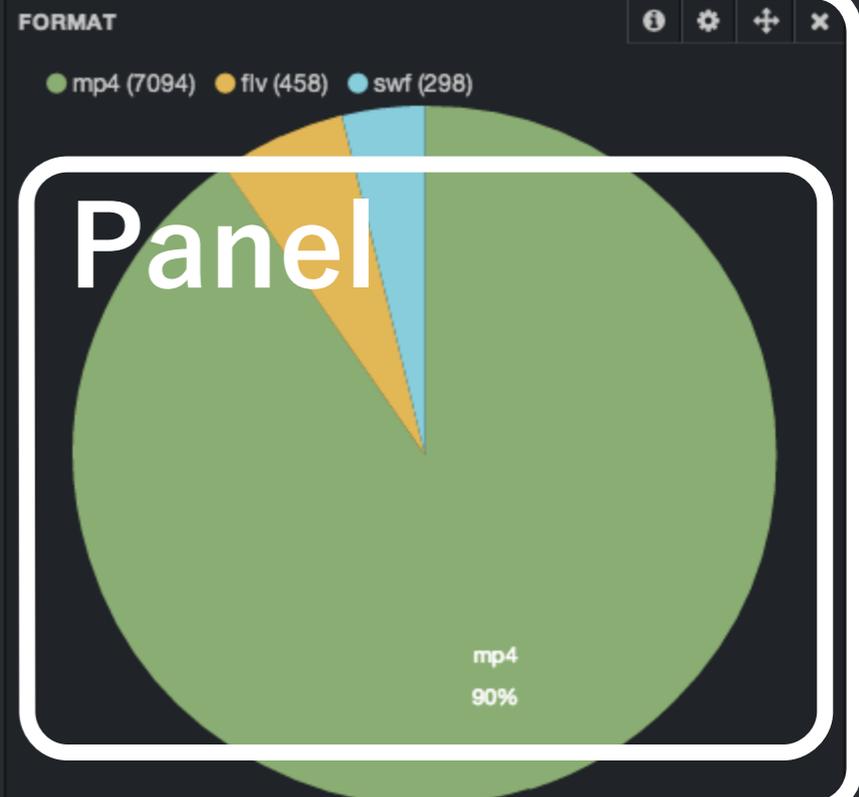
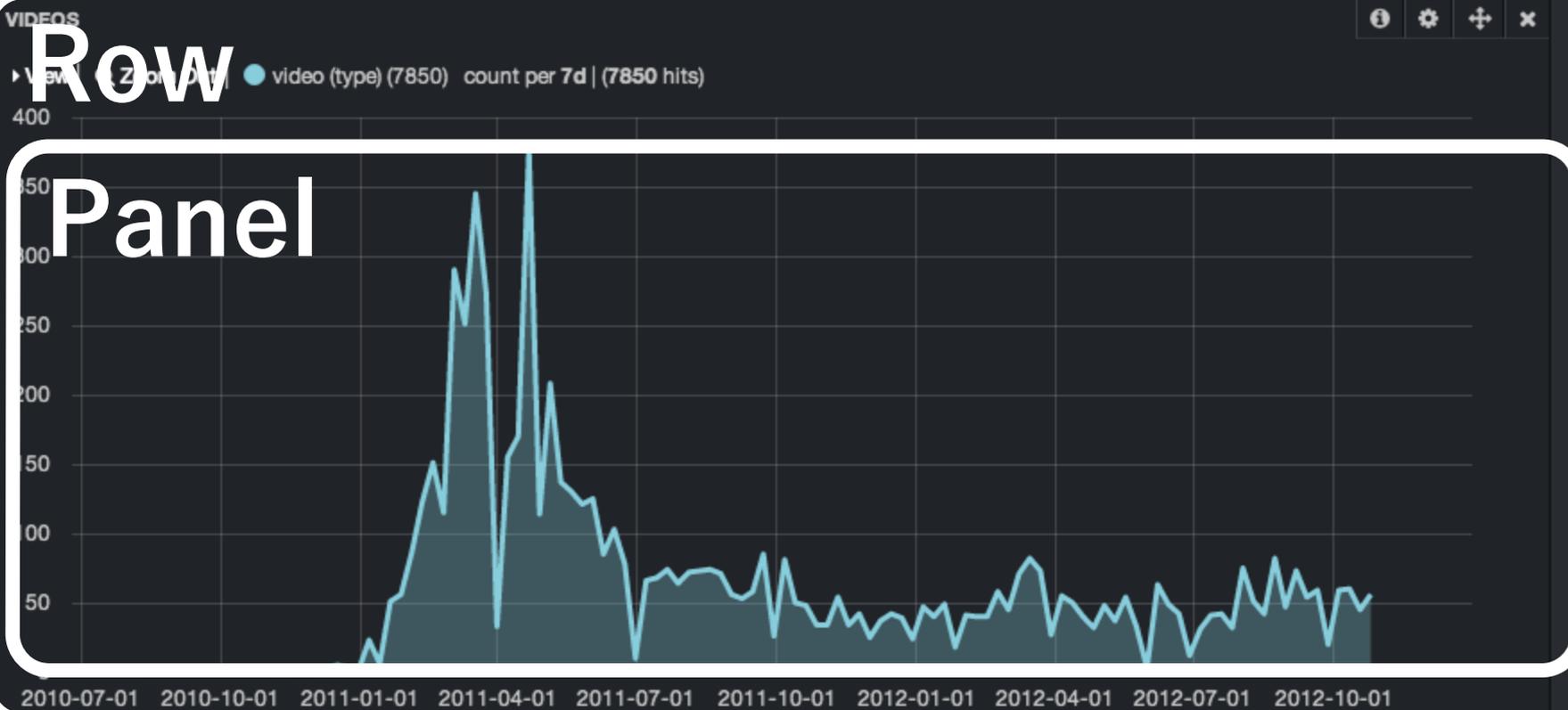
Navigation

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

_type: video AND title: まどか

QUERY

Row



Row

0 to 100 of 500 available for paging

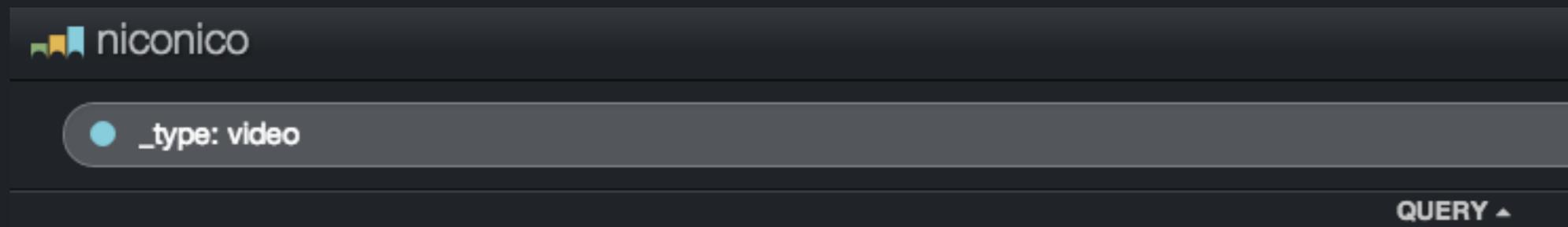
@timestamp	_type	video_id	title	length
2010-08-07T15:13:47+09:00	video	sm11663246	まどかのテーマ～ひとりぼっちのConcert (きまぐれオレンジ☆ロード)	149
2010-11-05T06:36:07+09:00	video	sm12651318	「魔法少女まどか☆マギカ」 第1弾キャラ&声優発表!	15
2010-11-12T03:41:29+09:00	video	sm12722302	シャフトオリジナルアニメ 魔法少女まどか☆マギカ CM	15
2010-12-06T20:51:44+09:00	video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

Panel

Query

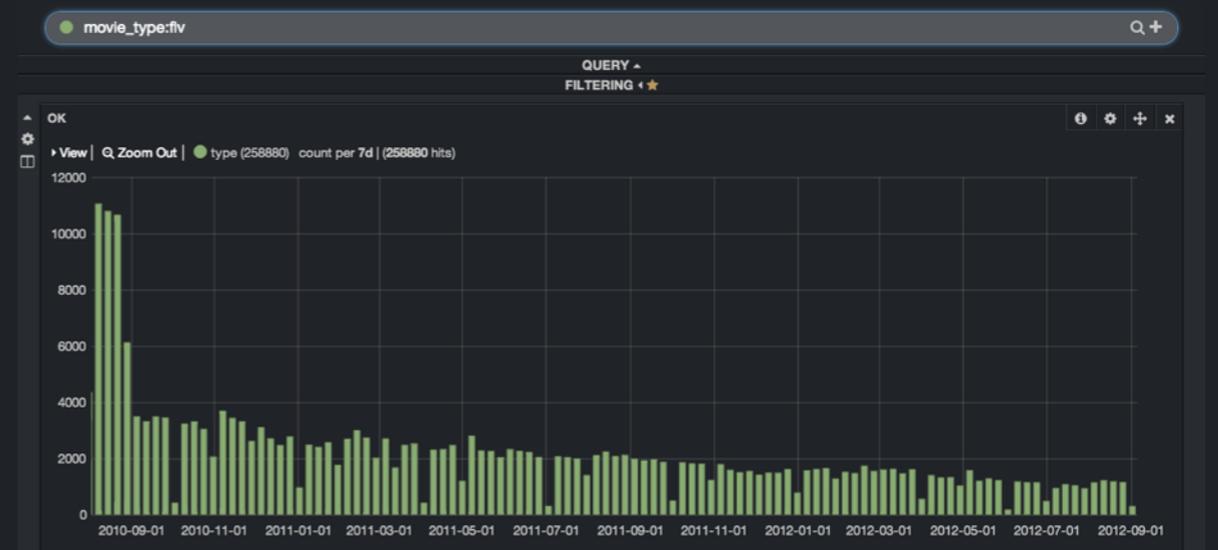
検索クエリを入力する一番基本となるパネル

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

The screenshot shows a query editor interface. At the top, a search bar contains the query: `_type: video AND title:"まどか"`. Below the search bar, there are two tabs: "QUERY" and "FILTERING". The "FILTERING" tab is active, showing two filter conditions:

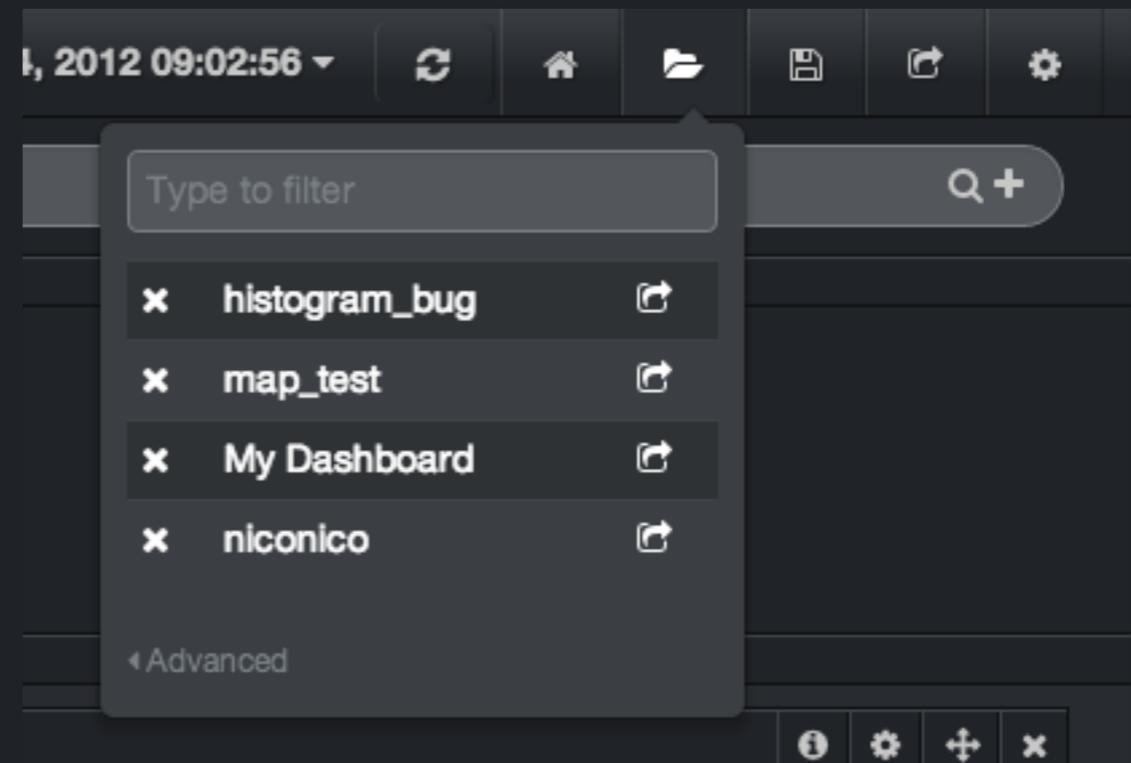
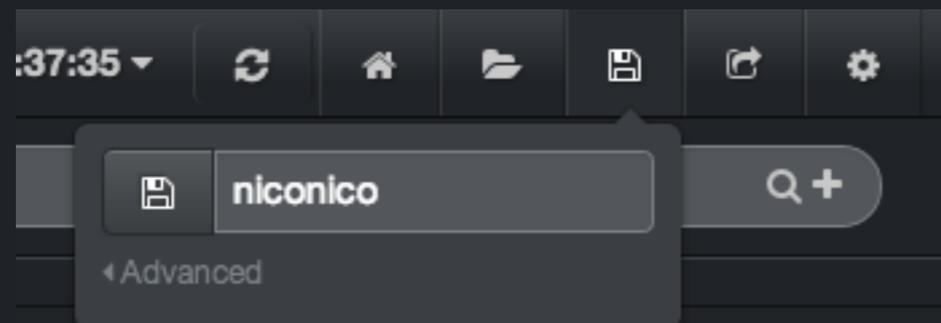
- time must**:
 - field : @timestamp
 - from : 2010-06-24T17:05:29.092Z
 - to : 2012-12-30T13:37:35.748Z
- terms must**:
 - field : movie_type
 - value : mp4

期間の絞り込み

movie_typeの絞り込み

Save & Load

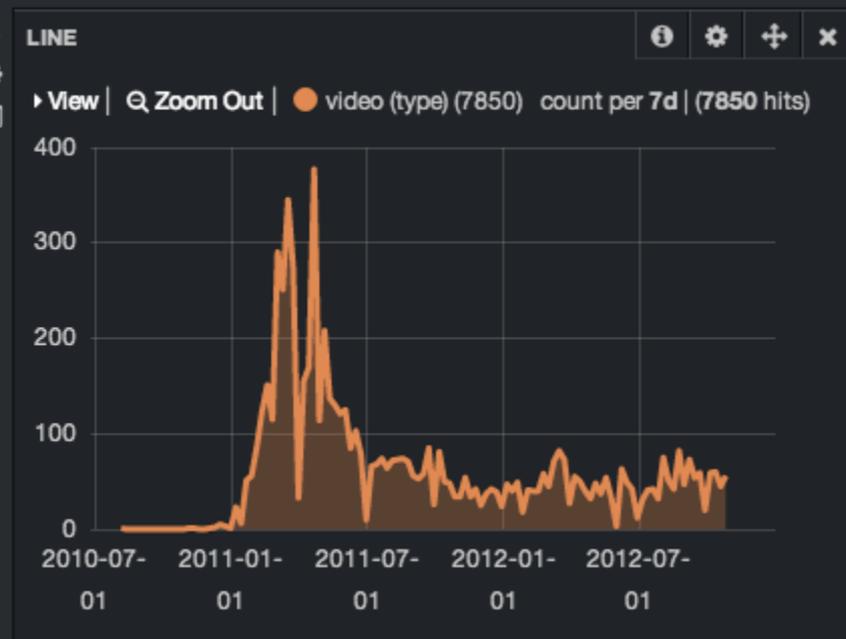
elasticsearchのkibana-intインデックスから保存と読み込み



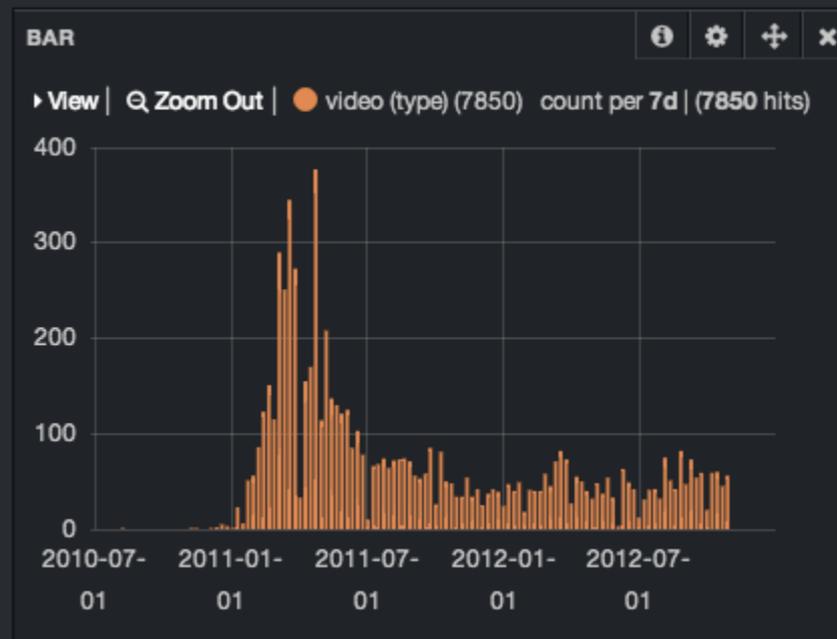
ダッシュボードを作ったら **リロード前に必ず保存!**

Histogram

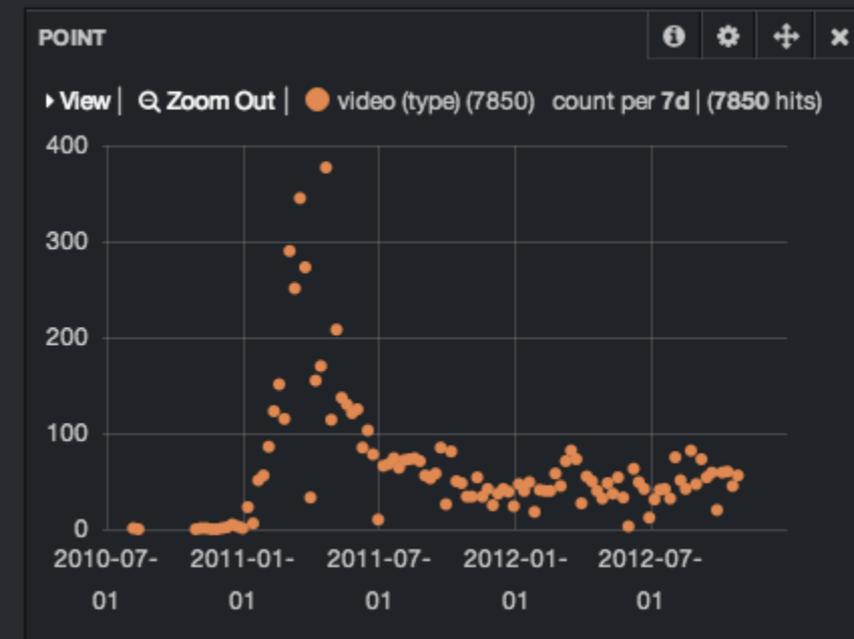
時系列データを表示する
一番使うことになるパネル



Lines



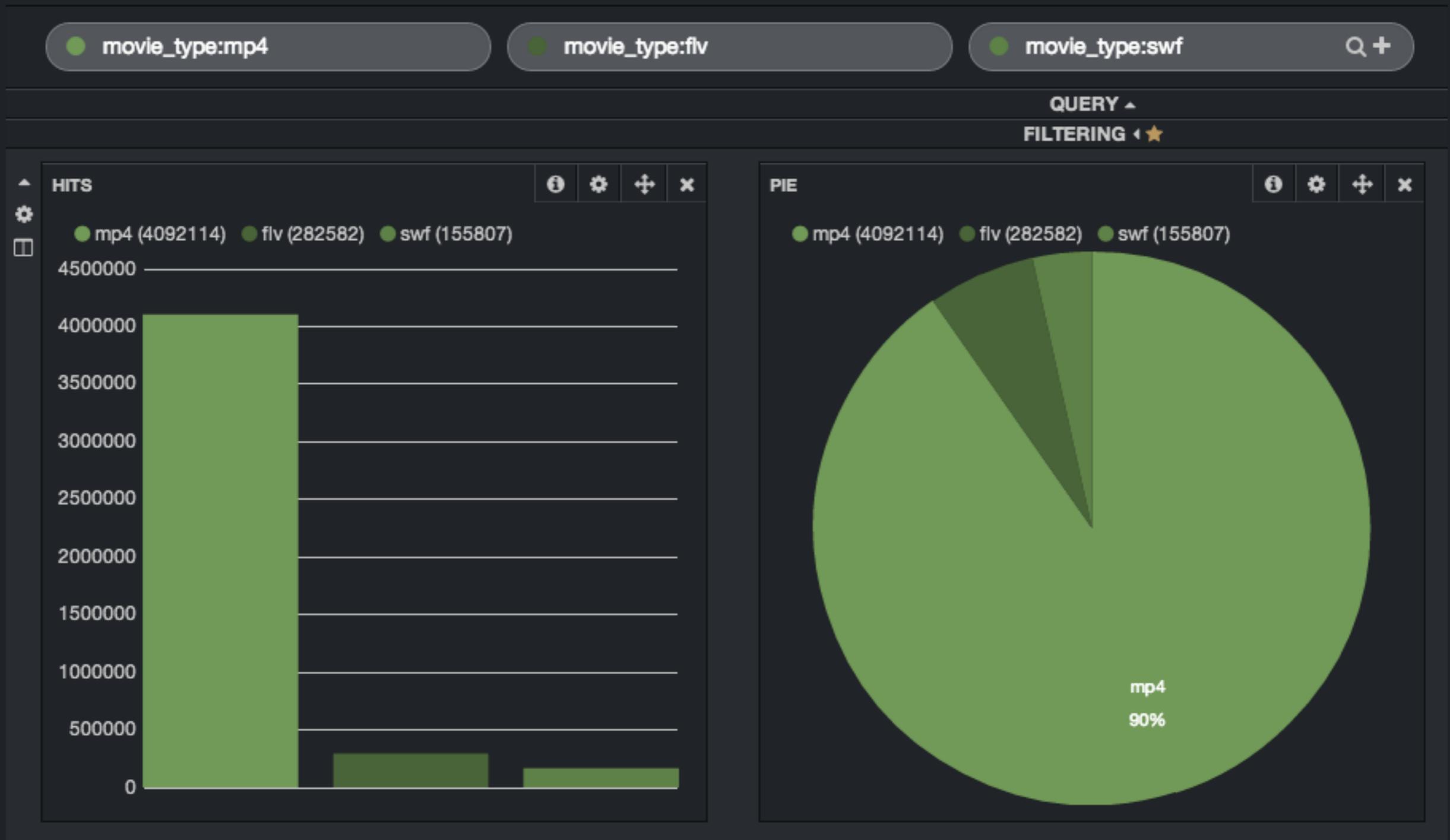
Bars



Points

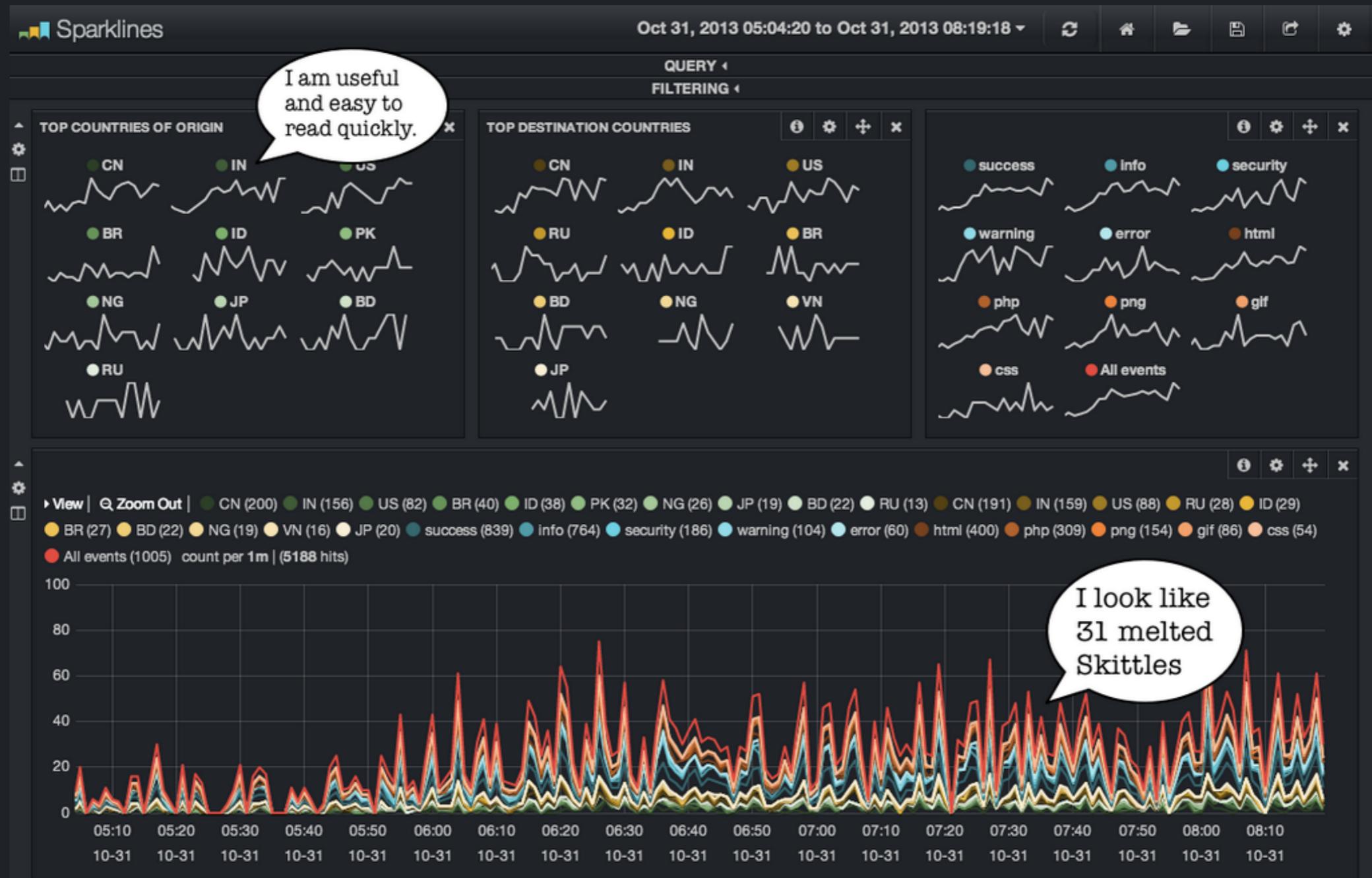
Hits

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

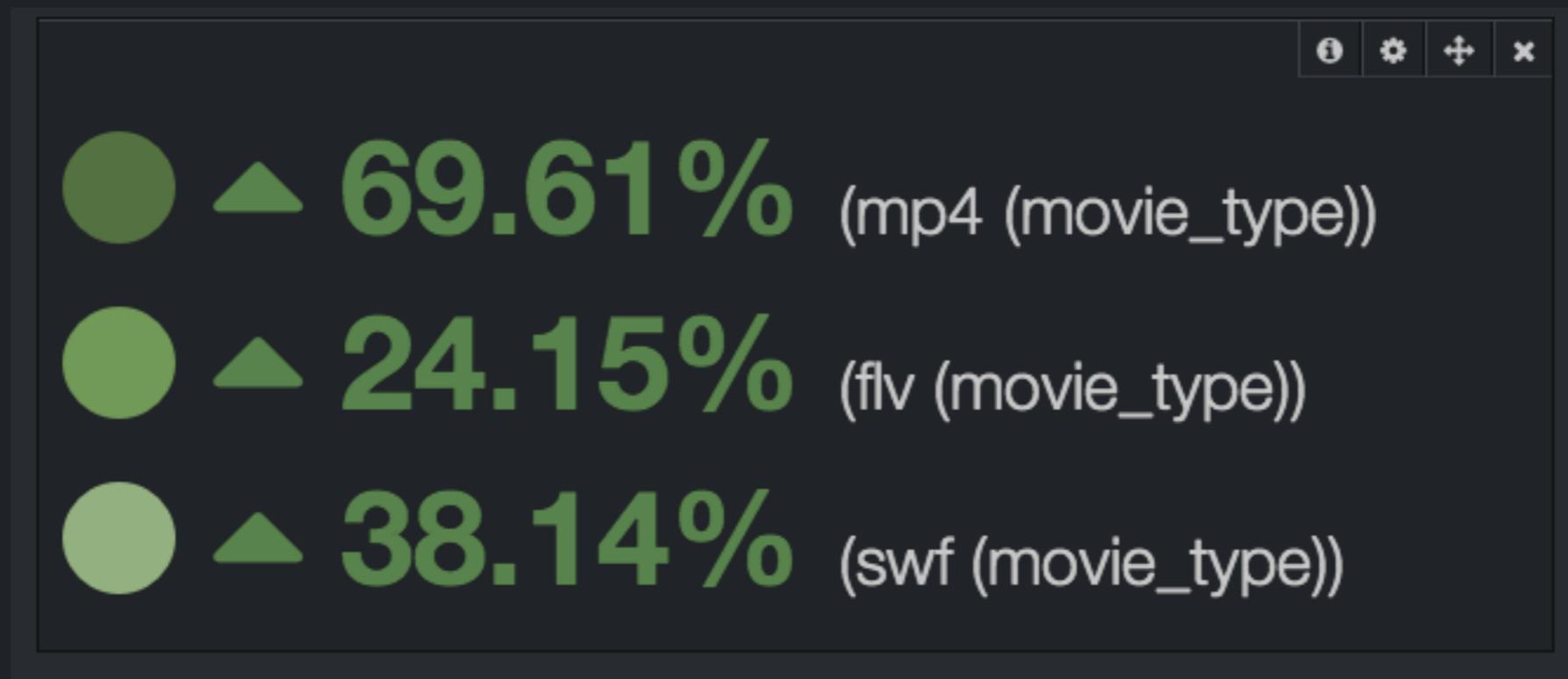
facetsの結果をBar, Pie, Tableでグラフ化



コメント数のfacet

Trends

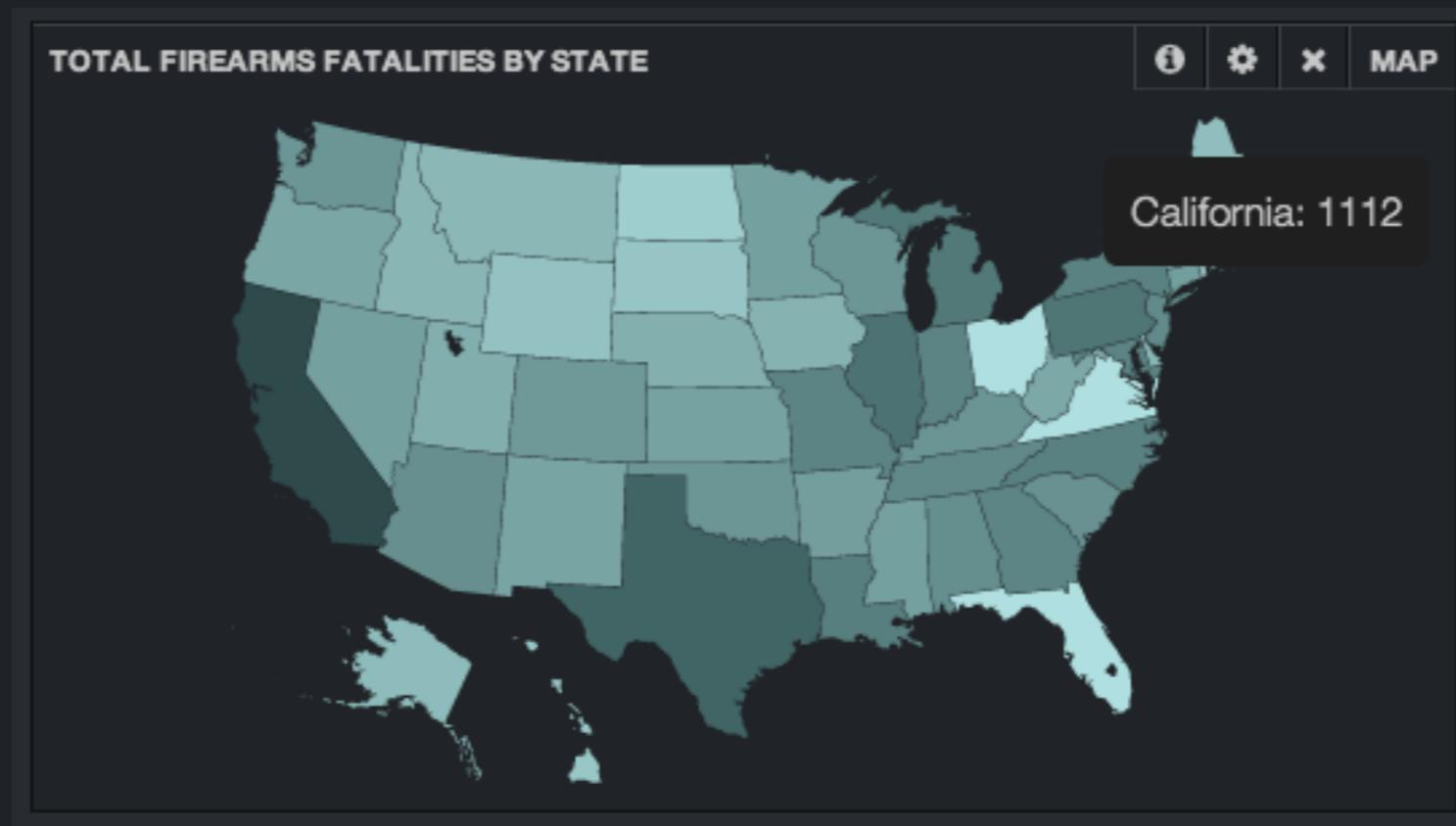
指定した時点からの値の変化を表示



「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



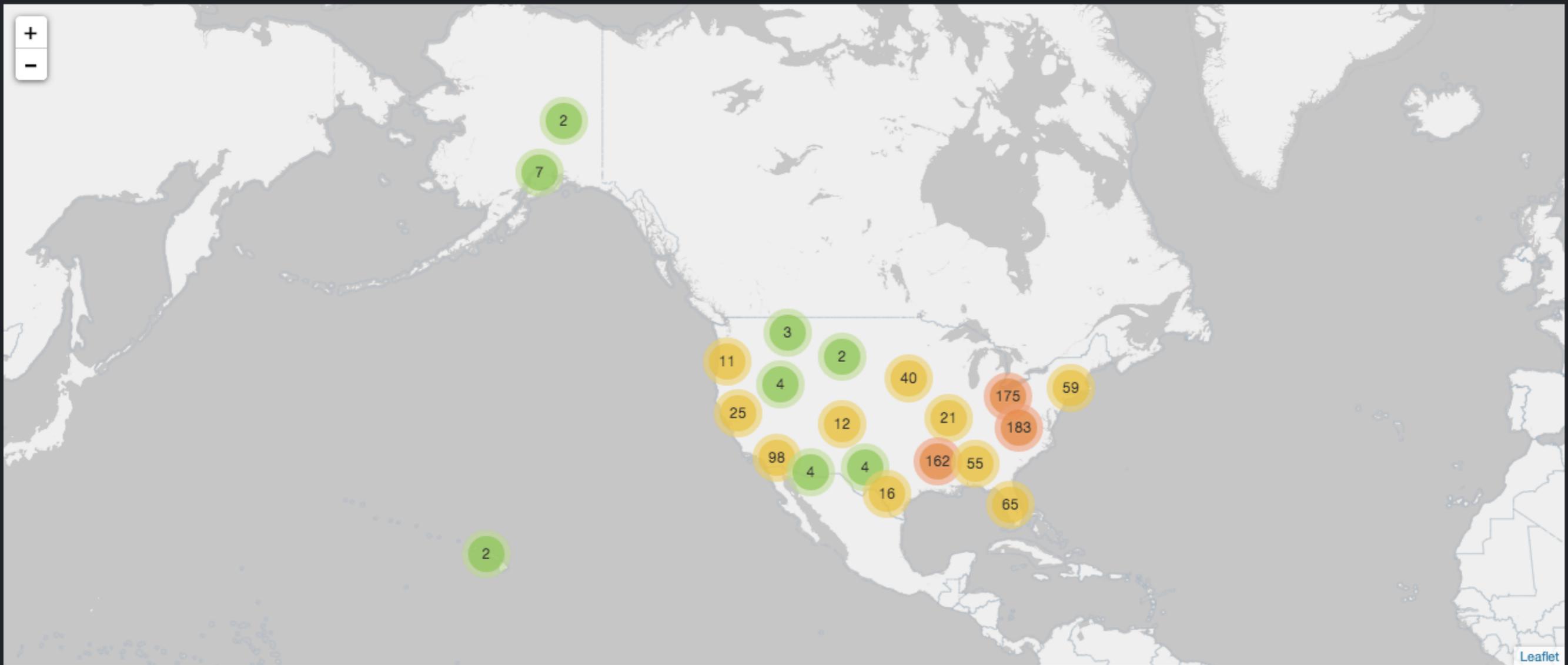
日本地図はPull requestを出したものの議論中...

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

BetterMap

緯度・経度を元にマッピング

ⓘ ⚙ × BETTERMAP



Table

クエリにマッチしたドキュメントの内容を表示

title:歌ってみた



QUERY
FILTERING

TABLE



Fields

0 to 100 of 500 available for paging



All / Current

@timestamp | movie_type | video_id | title | comment_counter

Type to filter...

- @timestamp
- _id
- _index
- _type
- comment_counter
- description
- last_res_body
- length
- movie_type
- mylist_counter
- size_high
- size_low
- tags
- thread_id
- thumbnail_url
- title
- upload_time
- video_id

2012-11-01T07:05:23+09:00	mp4	sm19252342	ドカボン! 怒りの鉄剣 やってみた 【part7】	0
2012-11-01T06:55:13+09:00	mp4	sm19252385	はねトビの東進CMバロを比較してみた	0
2012-11-01T06:50:00+09:00	mp4	sm19251163	Sweet Devil 踊ってみた@小窓	54
2012-11-01T06:45:06+09:00	mp4	sm19252368	歌に形はないけれど 歌ってみた【ver.楓しるっぷ】	0
2012-11-01T06:44:10+09:00	mp4	sm19252359	【歌ってみた】 からくりピエロ【くると】	0
2012-11-01T06:42:50+09:00	mp4	sm19252365	彼女が林道を走ってみた〜♪	1
2012-11-01T06:40:29+09:00	mp4	sm19252362	[Don't say "lazy"]余裕で弾いてみいた[^_^:]	0
2012-11-01T06:36:52+09:00	mp4	sm19252336	不思議の幻想郷2 みらくる☆パーティーplusをゆっくりと・・・30	1
2012-11-01T06:34:30+09:00	mp4	sm19252331	【ゾンビーズ】 太陽曰く燃えよカオス【踊ってみた】	197
2012-11-01T06:31:31+09:00	mp4	sm19252236	【カオス注意】 ギターの弦が切れたから遊んでみた。【弾いてみた?】	1
2012-11-01T06:29:32+09:00	mp4	sm19252324	Mrs.Pumpkinの滑稽な夢 を歌わせていただきました【昆布】	1
2012-11-01T06:29:11+09:00	mp4	sm19252339	【歌ってみた】 君の好きな本 acoustic ver.【のひ】	10
2012-11-01T06:22:42+09:00	mp4	sm19250792	【実況】 残暑の廃墟を探索してみたパート21	1
2012-11-01T06:13:49+09:00	mp4	sm19252314	ひかえめ主が まちぶせ を 歌ってみた	0

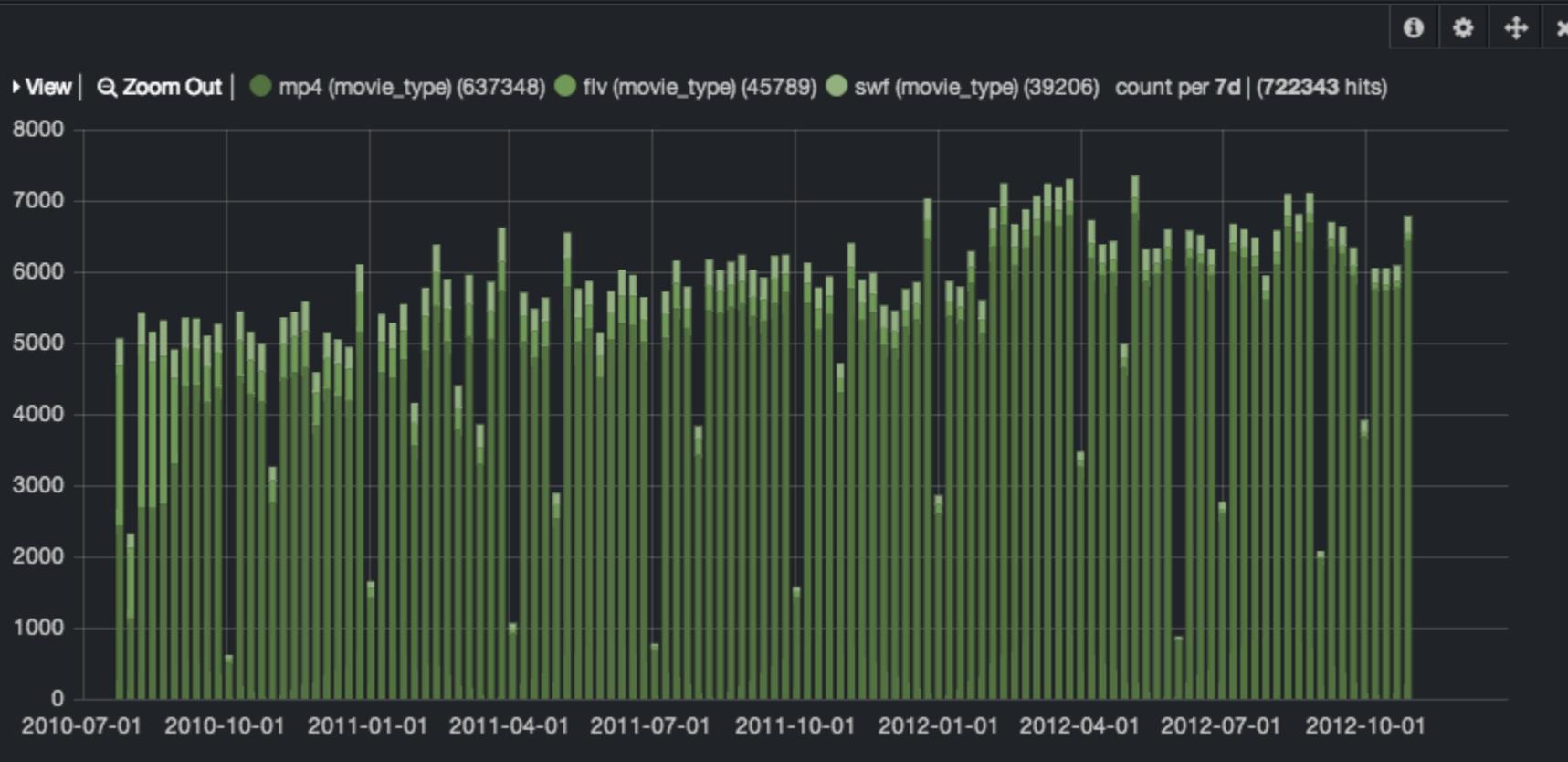
Column

パネルを縦に並べられるパネル

title:歌ってみた



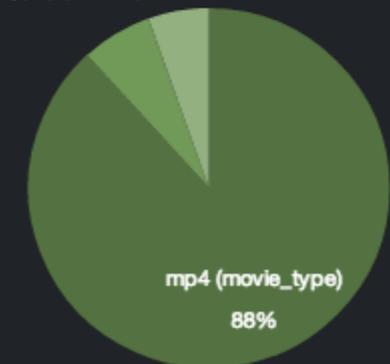
QUERY ^
FILTERING v



TOTAL

722343

mp4 (movie_type) (637348) flv (movie_type) (45789)
swf (movie_type) (39206)



Text

HTML, markdown, plain textでテキストを表示

Introduction

Set a time filter ▾



QUERY ▾

FILTERING ▾



Did you just upgrade? Not expecting this screen?

If you were using the old default page you might not be expecting this screen. I understand, change can be awkward. Let me explain.

Setting a global default dashboard

Kibana has always shipped with an interface for Logstash, still does! You can access it [here](#). However, if you want to make it your default again, all you need to do is rename a file! In your Kibana installation directory:

Rename `logstash.json` to `default.json` and refresh. Should be all set.

But wait, there's more!

In fact, you can add any exported dashboard to that directory and access it as `http://YOUR-HOST - HERE/index.html#dashboard/file/YOUR-DASHBOARD.json`.

Welcome to Kibana.

Glad you could make it. Happy to have you here! Lets get started, shall we?

Requirements

- **A good browser.**
The latest version of Chrome or Firefox is recommended. Safari (latest version) and Internet Explorer 9 and above are also supported.
- **A webserver.**
Just somewhere to host the HTML and Javascript. Basically any webserver will work.
- **Elasticsearch**
0.20.5 or above. Kibana will soon move to requiring Elasticsearch 0.90 or above, so upgrading is recommended.

Configuration

If Kibana and Elasticsearch are on the same host, and you're using the default Elasticsearch port, then you're all set. Kibana is configured to use that setup by default!

If not, you need to edit `config.js` and set the `elasticsearch` parameter with the URL (including port, probably 9200) of your Elasticsearch server. The host part should be the entire, fully qualified domain name, or IP, **not localhost**.

Are you a Logstash User?

- **YES** - Great! We have a prebuilt dashboard: **(Logstash Dashboard)**. See the note to the right about making it your global default
- **NO** - Hey, no problem, you just have a bit of setup to do. You have a few choices:

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
```

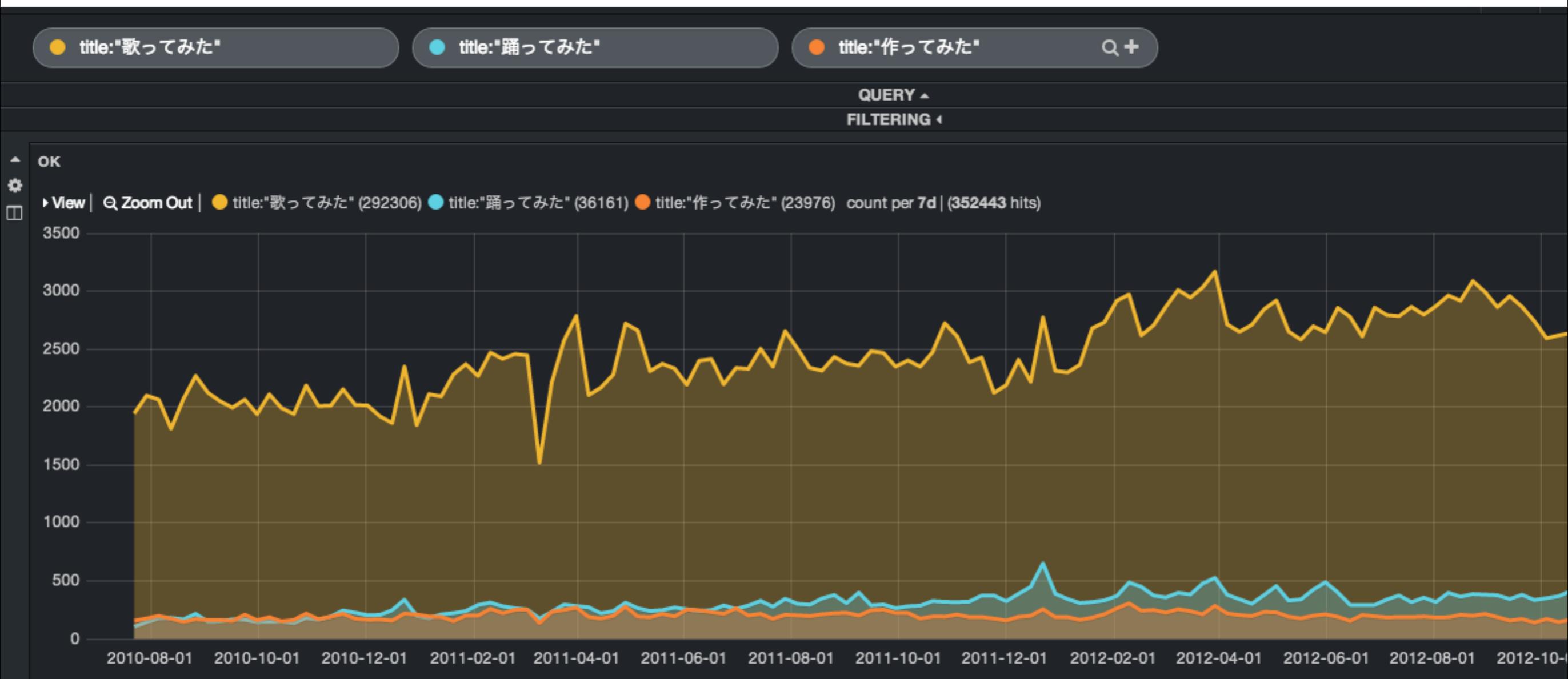
または

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

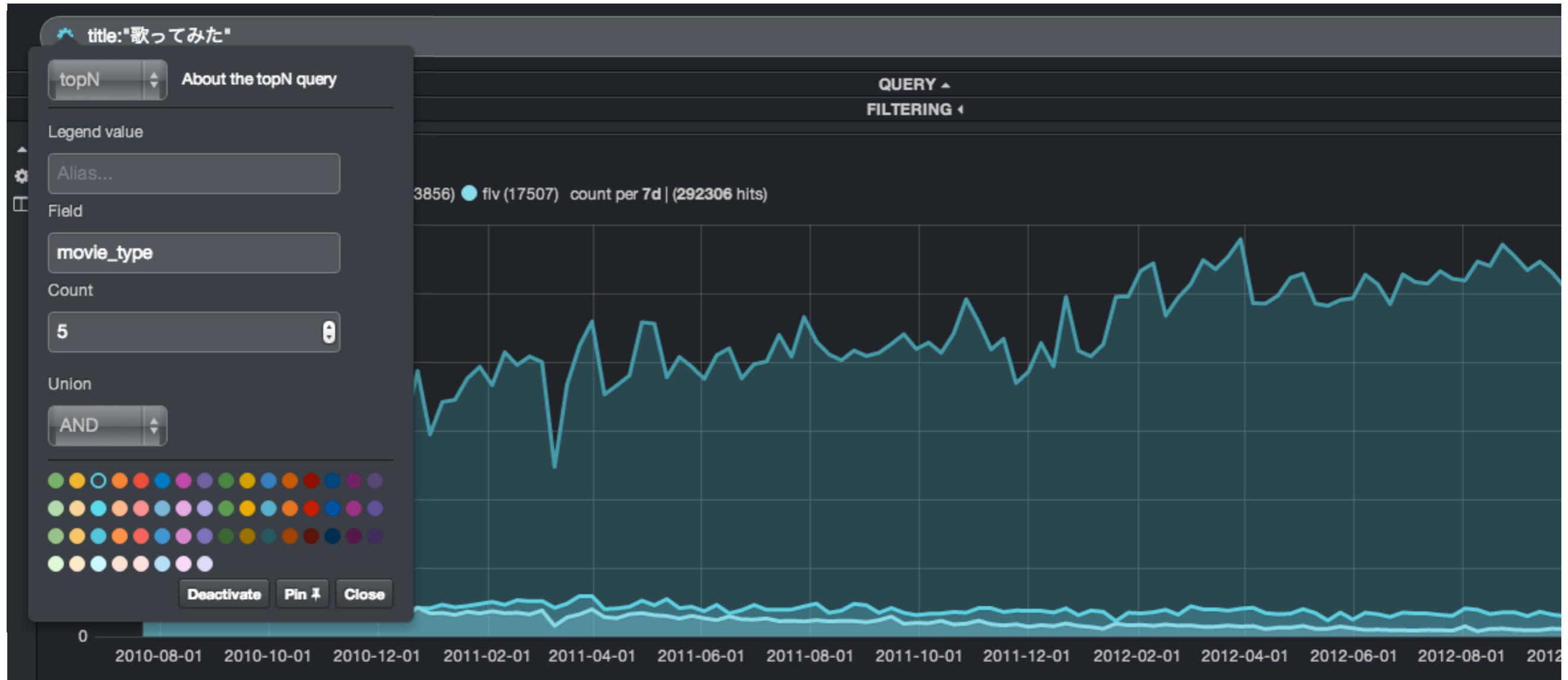
再生時間1分未満の動画

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

複数のクエリの結果を比較

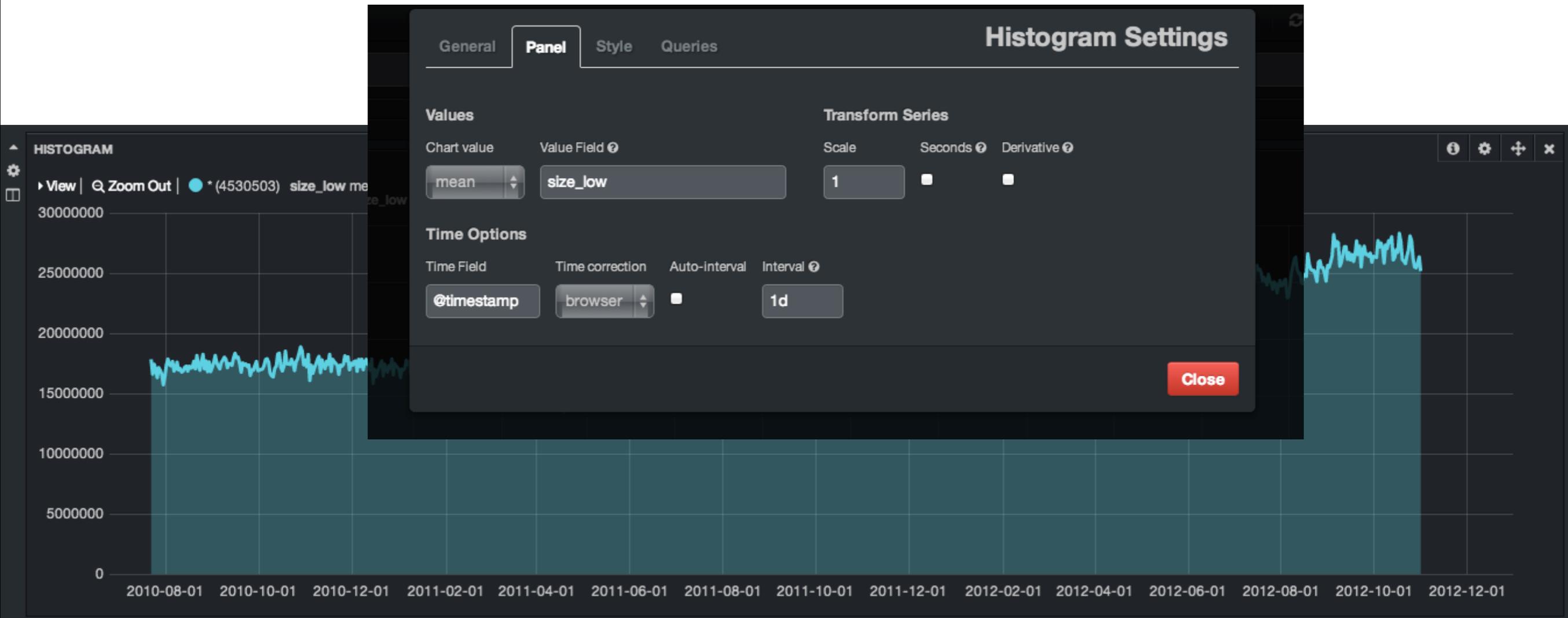


動画形式の比較



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

index logstash-2013.11.01

type access_log

type event_log

index logstash-2013.11.02

type access_log

type event_log

index logstash-2013.11.03

type access_log

type event_log

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

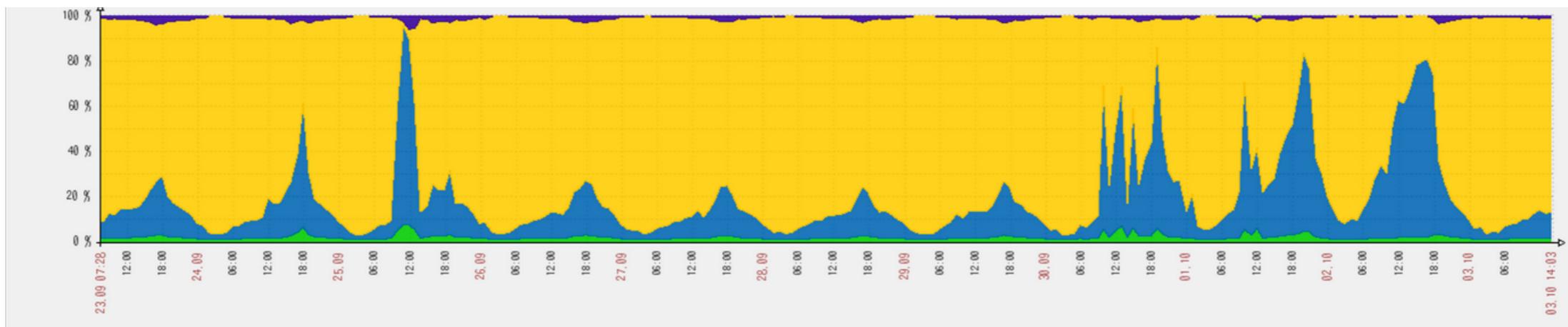
index template

curl -XPUT localhost:9200/_template/logstash_template

logstash-で始まるindexに自動的に適用

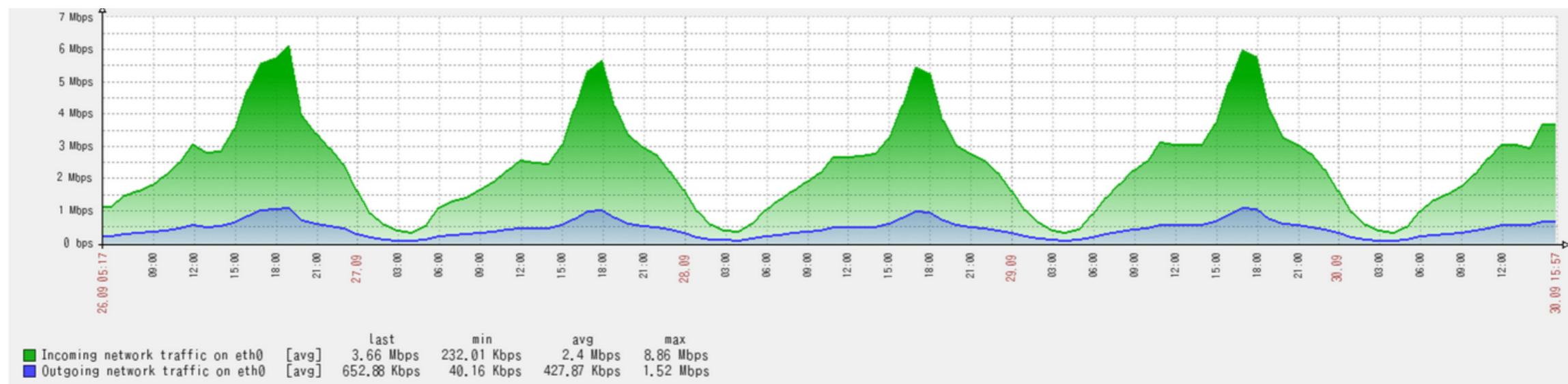
```
{
  "template": "logstash-*",
  "settings": {
    "number_of_shards": 1,
    "number_of_replicas": 0
  },
  "mappings": {
    "access_log": { typeがaccess_logのドキュメントに適用
      "_source": { "compress": true },
      "dynamic_templates": [
        {
          "string_template": {
            "match": "*",
            "mapping": { "type": "string", "index": "not_analyzed" },
            "match_mapping_type": "string"
          }
        }
      ],
      "properties": { 1つのプロパティを複数のfieldに展開
        "path": {
          "type": "multi_field",
          "fields": {
            "analyzed": {"type": "string", "index": "analyzed"},
            "no_analyzed": {"type": "string", "index": "not_analyzed"}
          }
        },
        "agent": { 分かち書きをしない
          "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ようとした

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