



# Elastic Stack ver.5

## ハンズオン

**Acroquest Technology 株式会社**

**樋口 慎**

## 樋口 慎 (Acroquest Technology 株式会社)

- Elasticテクニカルワークショップ講師  
(<https://info.elastic.co/japan-technical-workshop.html>)
- Data Analytics Showcase  
(<http://www.db-tech-showcase.com/data-analytics-showcase>)
- elasticsearch勉強会
- JJUG CCC 2016 spring

Twitter : @shinOhiguchi



# ハンズオン概要

- 1. Elastic Stackを用いて、ログデータの分析を行う**
- 2. Elastic Stack 5.0に触れる**
- 3. X-packを使ってみる**

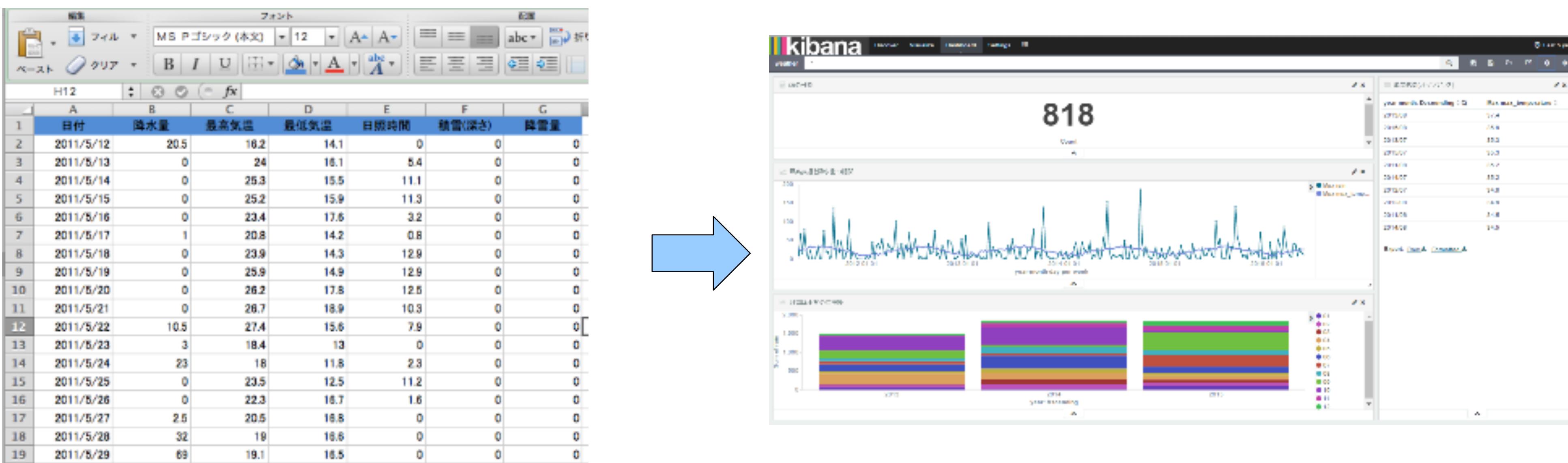
# ハンズオン概要

---

- 1. Elastic Stackを用いて、ログデータの分析を行う**
- 2. Elastic Stack 5.0に触れる**
- 3. X-packを使ってみる**

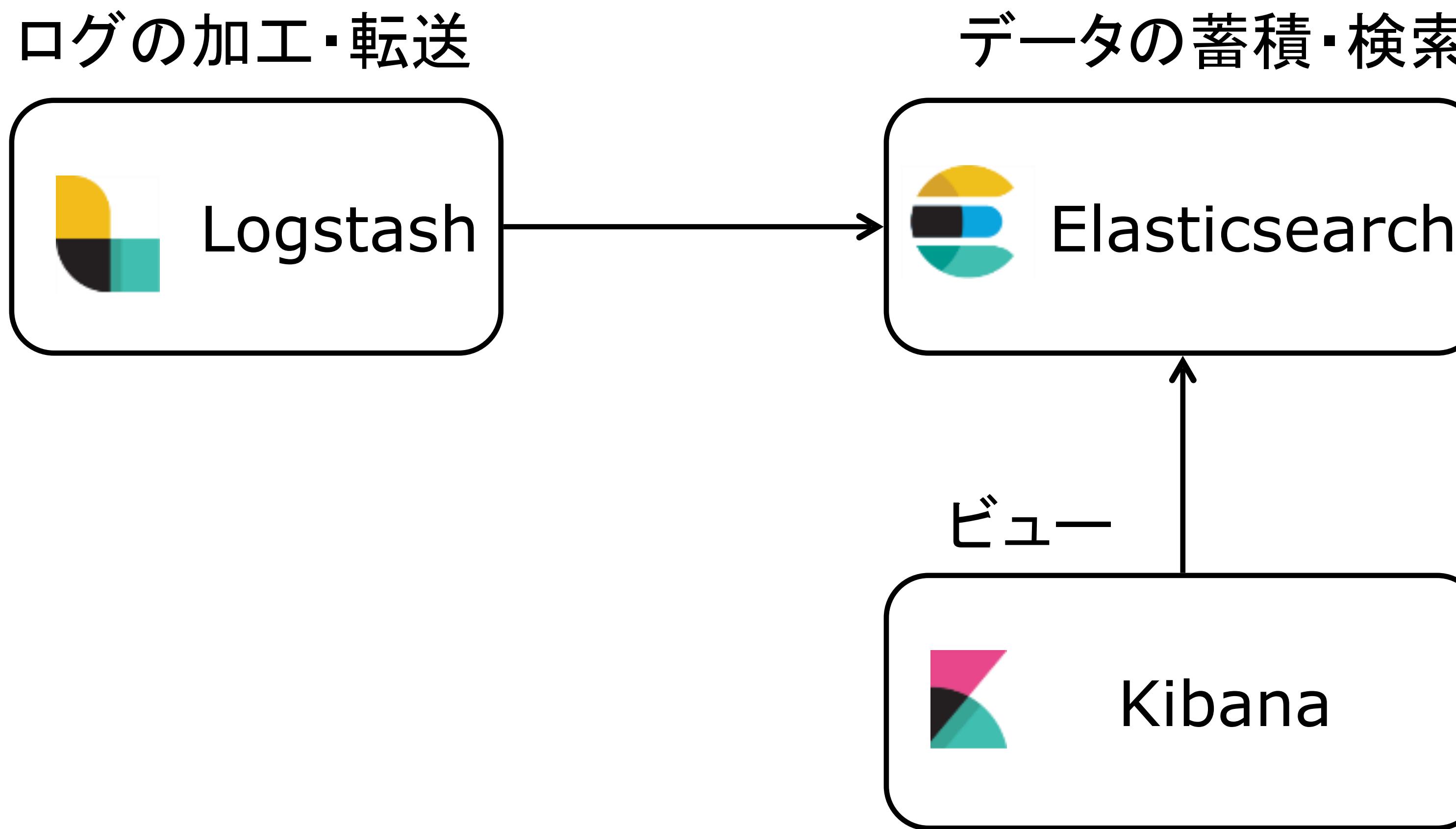
# ハンズオン概要

◆ Elastic Stackを用いて、ログデータの分析を行う。



# Elastic Stackとは

Elasticのオープンソース製品のこと。

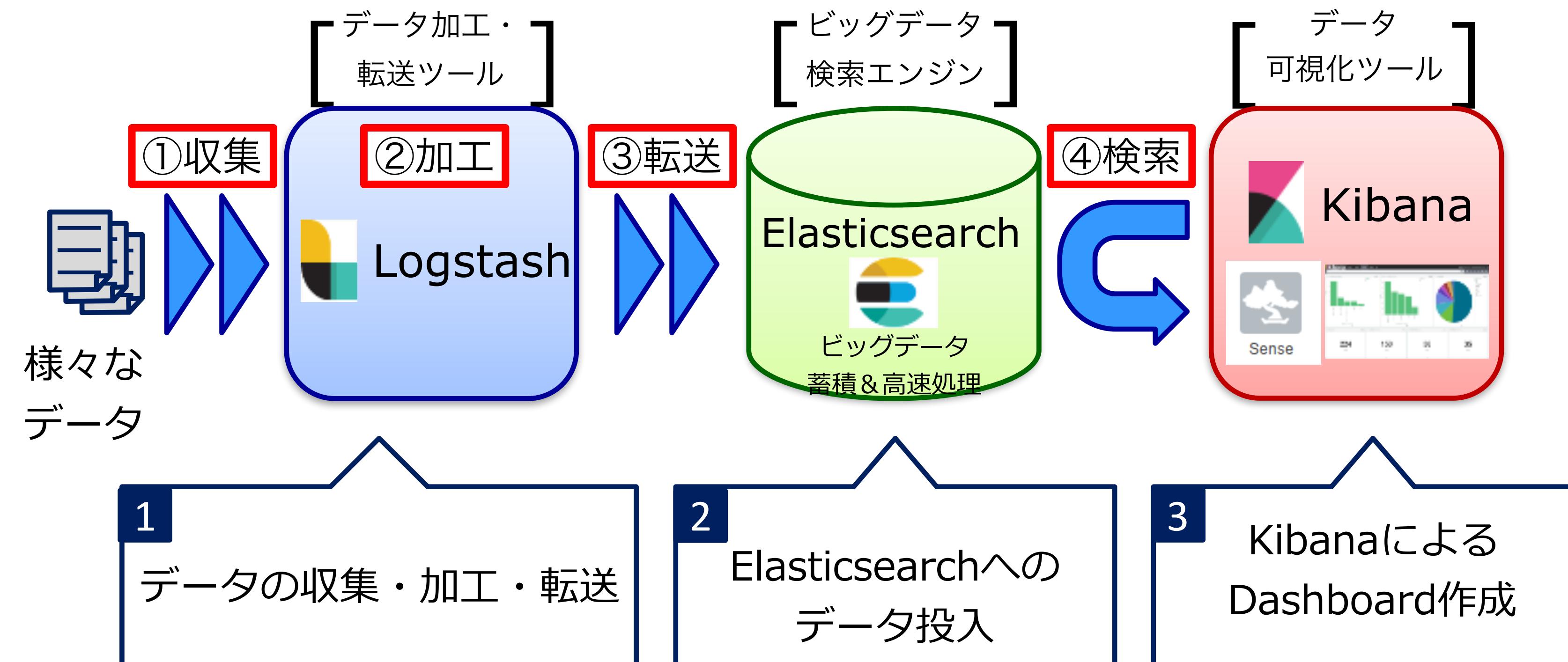


# Elastic Stackとは

---

- **Beats**   
データ収集に特化したサーバ常駐エージェント。  
GO言語で書かれており、軽量。
- **Elastic Cloud**   
**Elasticsearch**を**AWS**上で構築・提供するサービス。  
商用プラグインなども利用することができる。

# ハンズオン概要



# ハンズオンの目的

- 1. Elastic Stackを用いて、ログデータの分析を行う**
- 2. Elastic Stack 5.0に触れる**
- 3. X-packを使ってみる**

# ハンズオンの目的

- 1. Elastic Stackを用いて、ログデータの分析を行う**
- 2. Elastic Stack 5.0に触れる**
- 3. X-packを使ってみる**

# ハンズオンの目的

---

- ◆ X-packを使ってみる 

拡張プラグインのパッケージ

**Security** : ElasticStackへのアクセスを制御するセキュリティプラグイン

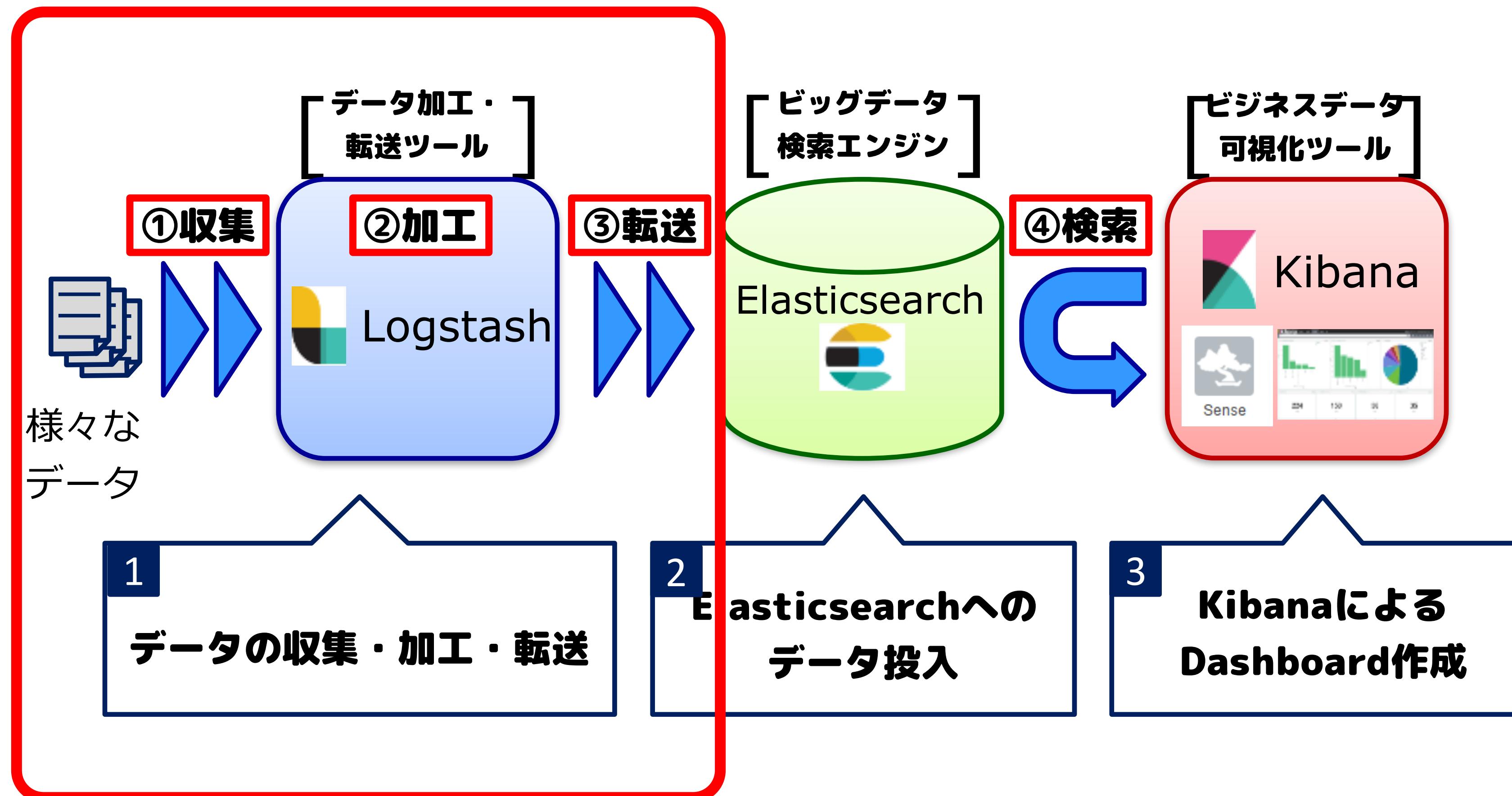
**Monitoring** : ElasticStackの稼働状況を監視する

**Alerting** : 特定の条件を満たしたとき、メールなどでアラートをあげる

**Graph** : 要素同士の関連を可視化する

**Reporting** : Dashboardなどからレポートを作成する

# 【再掲】全体フロー図



# Logstashによる データの収集・加工・転送



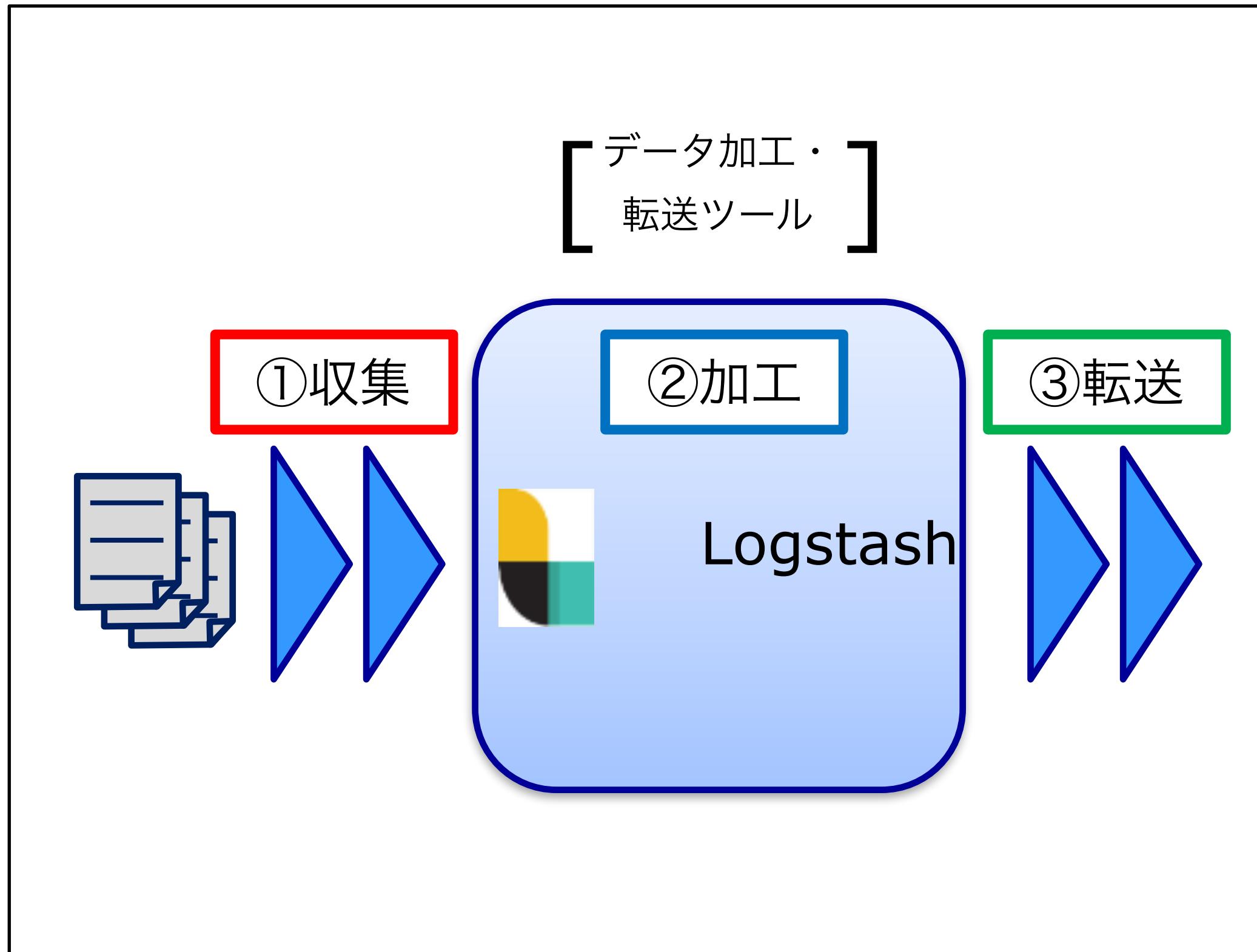
# Logstashとは

---

- Logstashは、ログを収集・加工し、転送する。(Elasticsearch以外への出力も可)
- 200以上の公式プラグインが用意されており、DBやHDFS、S3、Twitterなどとも連携できる。

# 1-2. Logstashの処理の流れ

## フロー図（Logstash部分）



## 設定ファイルの例

```
input { stdin {} } ] ①  
filter {} ] ②  
output {  
  stdout {  
    codec => rubydebug } } ③
```

# 設定例

```
input {
  stdin { }
}
filter {
  grok {
    match => {
      "message" => '%{IPORHOST:clientip} %{USER:ident} %{USER:auth} \[%{HTTPDATE:timestamp}\] "%
      {WORD:verb} %{DATA:request} HTTP/%{NUMBER:httpversion}" %{NUMBER:response:int} (?:-|%
      {NUMBER:bytes:int}) %{QS:referrer} %{QS:agent}"
    }
  }
  date {
    match => [ "timestamp", "dd/MMM/YYYY:HH:mm:ss Z" ]
  }
  geoip {
    source => "clientip"
  }
  useragent {
    source => "agent"
    target => "useragent"
  }
}
output {
  elasticsearch {
    hosts => "localhost"
  }
}
```

# Input

---

Inputの設定例を以下に示す。

- `input {stdin{}}`
- `input {  
 plugin {  
 setting_1 => "value"  
 array_2 => ["value1","value2"]  
 hash_3 => { key => "value" }  
 # comment  
 }  
}`

# filter

---

```
filter {
  grok {
    match => {
      "message" => '%{IPORHOST:clientip} %{USER:ident} %{USER:auth} \[%{HTTPDATE:timestamp}\] "%{WORD:verb} %{DATA:request} HTTP/%{NUMBER:httpversion}" %{NUMBER:response:int} (?:-|%{NUMBER:bytes:int}) %{QS:referrer} %{QS:agent}"
    }
  }
  date {
    match => [ "timestamp", "dd/MMM/YYYY:HH:mm:ss Z" ]
  }
  geoip {
    source => "clientip"
  }
  useragent {
    source => "agent"
    target => "useragent"
  }
}
```

# 演習 1

# Logstashを使ってみよう！

# 演習1. Step2

---

- ・ テキストエディタなどで**logstash1.conf**を開く

※ファイルのエンコードは**UTF-8(BOM無し)**にする。

# 演習1. Step2(設定ファイル内容)

---

```
input { stdin {} }
```

```
filter {}
```

```
output {  
    stdout {  
        codec => rubydebug  
    }  
}
```

```
}
```

# 演習1. Step3

---

作成したファイルでテスト実行を行う。

**1.** コマンドラインツールを起動する

**2.** **logstash-5.0.0**に移動する。

① **cd ~/JJUG\_fall/logstash-5.0.0 (Mac,Linux)**

② **cd C:\JJUG\_fall\logstash-5.0.0 (Windows)**

**3.** **bin/logstash -f logstash1.conf** と打ち込んで実行する

**4.** 最終行に

**"Successfully started Logstash API endpoint {:port=>9600} "**

と表示されればOK

# 演習1. Step3(実行)

実行すると

"Successfully started Logstash API endpoint {:port=>9600}"

と表示された状態で出力がとまる(標準入力からの入力待ち状態)

## 画面例

```
SHIN /Users/SHIN/AcroWorks/hands-on-workshop_temp/logstash-5.0.0-beta1 16-10-06 0:56:09
bin/logstash -f logstash.conf
The stdin plugin is now waiting for input:
[2016-10-06T00:56:29,679][INFO ][logstash.pipeline] Starting pipeline {"id"=>"main", "p
ipeline.workers"=>4, "pipeline.batch.size"=>125, "pipeline.batch.delay"=>5, "pipeline.max_infl
ight"=>500}
[2016-10-06T00:56:29,702][INFO ][logstash.pipeline] Pipeline main started
[2016-10-06T00:56:29,833][INFO ][logstash.agent] Successfully started Logstash API e
ndpoint {:port=>9600}
```

# 演習1. Step3

---

文字列を入力してみる:

1. **Hello, world!** と入力して、**return**キーを押す
2. 以下のような結果が表示されれば成功

```
{  
    "@timestamp" => 2016-10-05T16:08:32.486Z,  
    "@version" => "1",  
    "host" => "$HOST",  
    "message" => "Hello, world!"  
}
```

## 演習2. Filterの設定(grok filter)

---

目標:

ログの特定部分を抜き出すための**grok filter**を定義し、動作を確認する。

- ① 設定に**grok filter**を追加する。
- ② **grok filter**がどのような挙動を行うのか確認する。

## 演習2. Step1

---

- logstash2.confを開く

```
filter {  
    grok {  
        match => {  
            "message" =>'%{HTTPDATE:timestamp} %{IP:ip} <%{DATA:msg}>'  
        }  
    }  
}
```

## 演習2. Step2

---

作成したファイルでテスト実行を行う:

- 1. logstash**が実行中の場合、**Ctrl+C**で終了する
- 2. bin/logstash -f logstash2.conf**  
と打ち込んで実行する
- 3. 22/Mar/2014:16:38:00 -0700 183.60.215.50 <This>**  
と打ち込んで実行する
- 4.** 次ページのような結果が表示されれば成功

## 演習2. Step2

---

入力した文字列: **22/Mar/2014:16:38:00 -0700 183.60.215.50 <This>**

出力例:

{

```
"msg" => "This",
"@timestamp" => 2016-10-08T02:21:37.761Z,
"ip" => "183.60.215.50",
"@version" => "1",
"host" => "$HOST",
"message" => "22/Mar/2014:16:38:00 -0700 183.60.215.50 <This>",
"timestamp" => "22/Mar/2014:16:38:00 -0700"
```

}

## 演習2. Step2

入力した文字列: 22/Mar/2014:16:38:00 -0700 183.60.215.50 <This>



grokフィルターのパターン一覧:

<https://github.com/elastic/logstash/blob/v1.4.2/patterns/grok-patterns>

## 演習3. date

---

目標:

ログに記載されている時刻を利用して、  
**timestamp**フィールドを設定する。

①**date filter**を設定する。

②**remove\_field** の設定を追加し、不要なカラムを削除する。

## 演習3. Step1

---

**logstash3.confを開く**

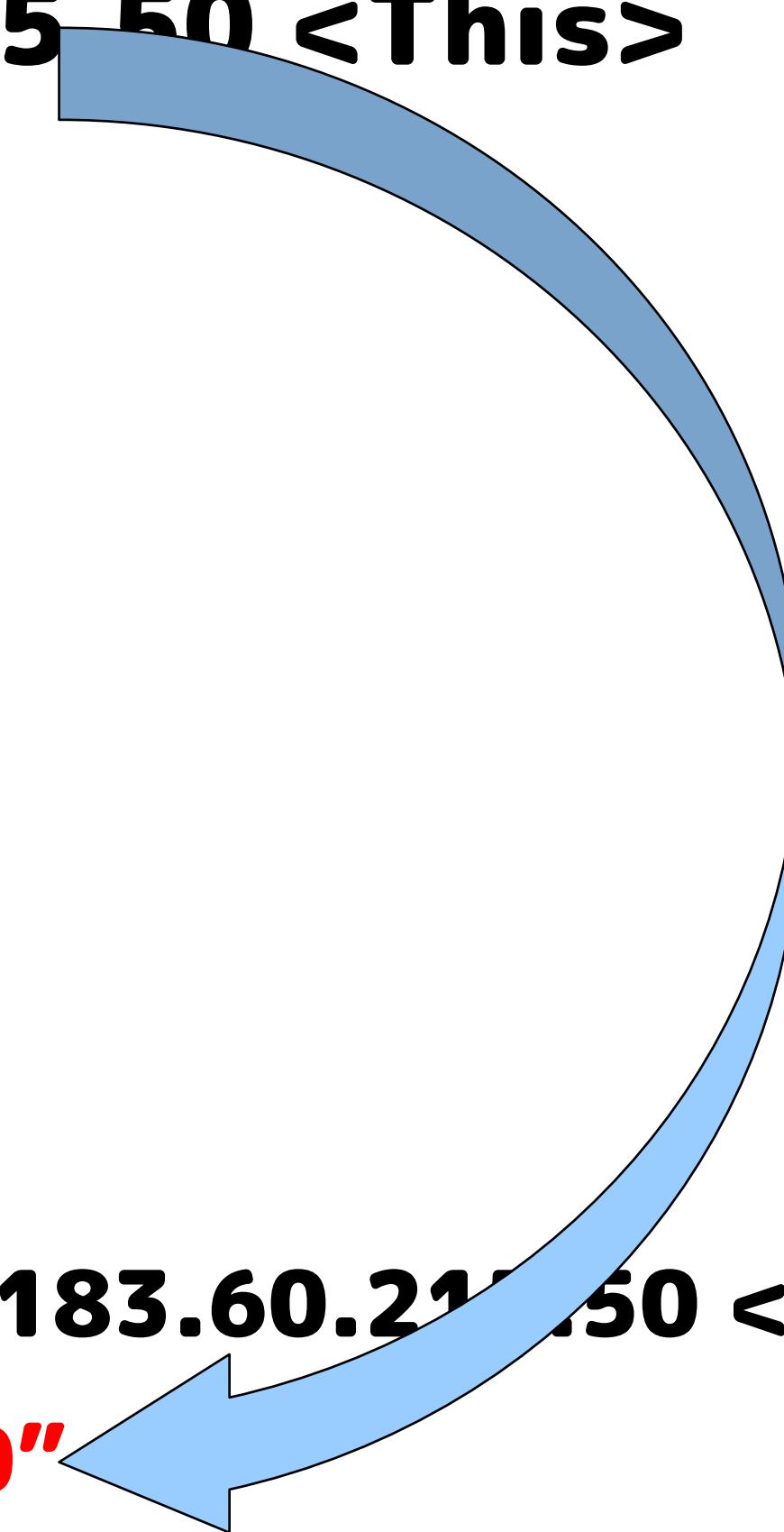
```
date {  
    match => [ "timestamp", "dd/MMM/YYYY:HH:mm:ss Z" ]  
    locale => jp  
}  
}
```

## 演習3. Step2

```
% bin/logstash -f logstash.conf
```

```
22/Mar/2014:16:38:00 -0700 183.60.215.50 <This>
```

```
{  
    "msg" => "This",  
    "@timestamp" => 2014-03-22T23:38:00.000Z,  
    "ip" => "183.60.215.50",  
    "@version" => "1",  
    "host" => "HIGUCHI-2.local",  
    "message" => "22/Mar/2014:16:38:00 -0700 183.60.215.50 <This>",  
    "timestamp" => "22/Mar/2014:16:38:00 -0700"  
}
```

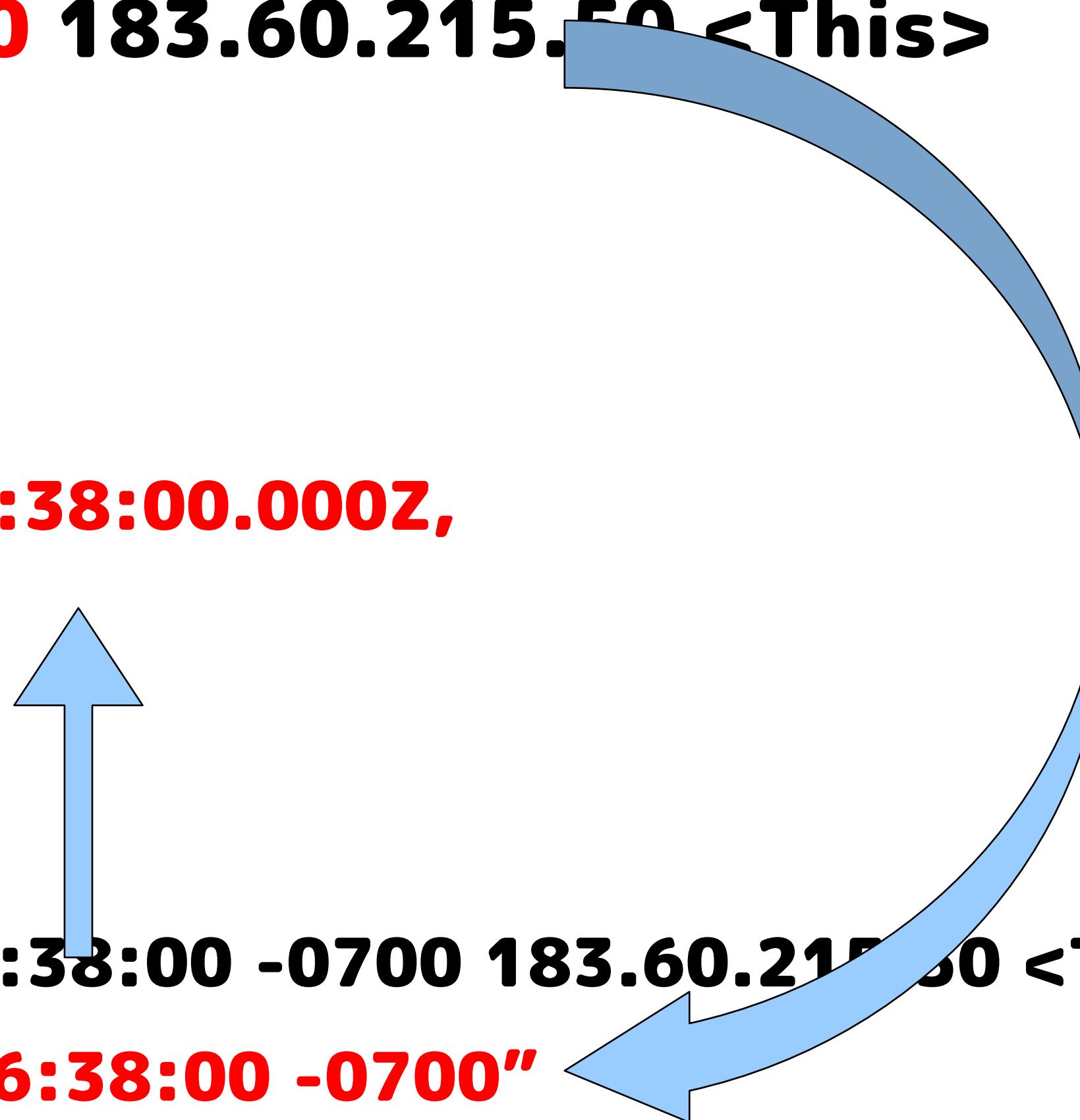


## 演習3. Step2

```
% bin/logstash -f logstash.conf
```

```
22/Mar/2014:16:38:00 -0700 183.60.215.50 <This>
```

```
{  
    "msg" => "This",  
    "@timestamp" => 2014-03-22T23:38:00.000Z,  
    "ip" => "183.60.215.50",  
    "@version" => "1",  
    "host" => "HIGUCHI-2.local",  
    "message" => "22/Mar/2014:16:38:00 -0700 183.60.215.50 <This>",  
    "timestamp" => "22/Mar/2014:16:38:00 -0700"  
}
```



# 演習4. geoip

---

目標：

**geoip filter**を設定し、IPアドレスから地図情報  
を設定する。

①**geoip filter**を設定する。

②**geoip filter**を設定することで、緯度・経度・地域情報  
が取得できることを確認する。

## 演習4. Step1

---

**logstash4.confを開く。**

```
geoip {  
    source => "ip"  
}
```

# 演習4. Step1

---

実行した結果を以下に示します。

{

**"msg" => "This",**

**"@timestamp" => 2014-03-22T23:38:00.000Z,**

**"geoip" => {**

*... <this part is on next slide> ...*

**}**

**"ip" => "183.60.215.50",**

**"@version" => "1",**

**"host" => "\$HOST",**

**"message" => "22/Mar/2014:16:38:00 -0700 183.60.215.50 <This>"**

}

## 演習4. Step1 出力例

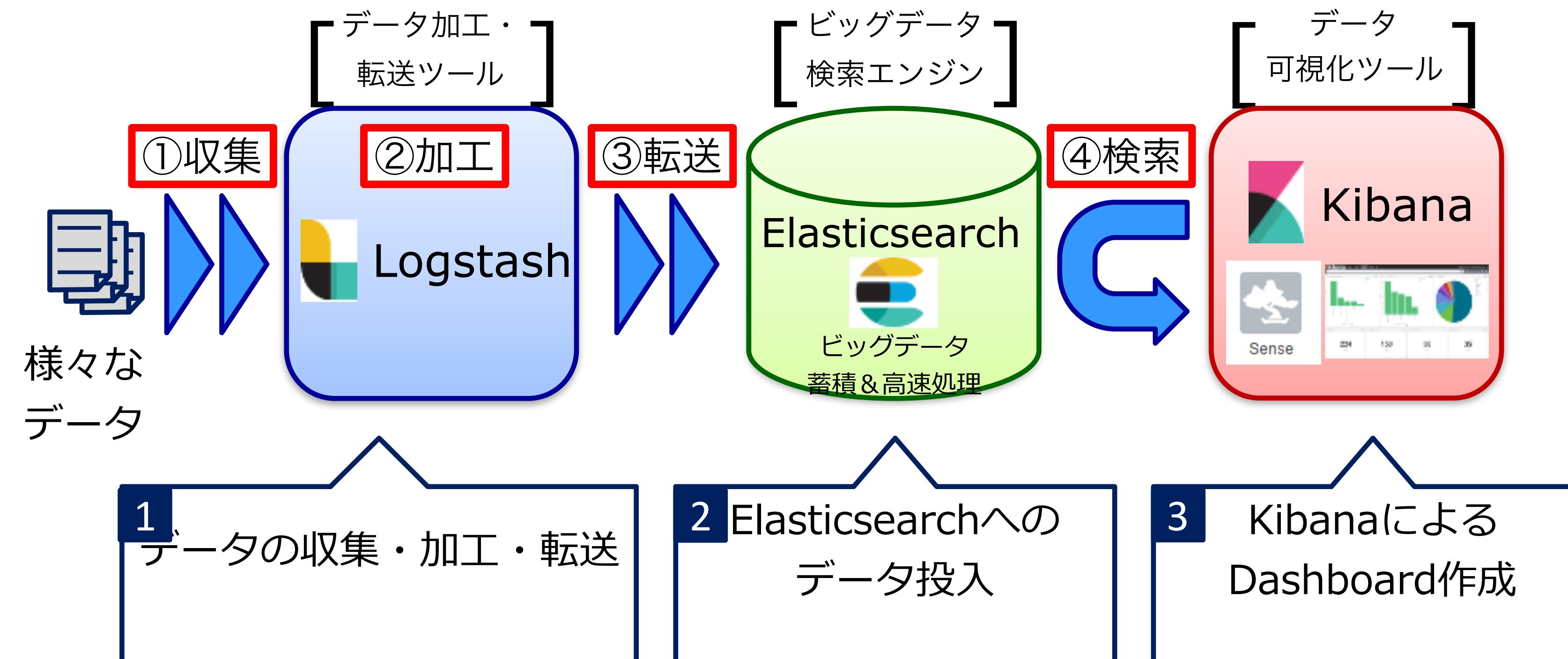
```
"geoip" => {
    "timezone" => "Asia/Shanghai",
    "ip" => "183.60.215.50",
    "latitude" => 23.1167,
    "continent_code" => "AS",
    "city_name" => "Guangzhou",
    "country_code2" => "CN",
    "country_name" => "China",
    "dma_code" => nil,
    "country_code3" => "CN",
    "region_name" => "Guangdong",
    "location" => [
        [0] 113.25,
        [1] 23.1167
    ],
    "postal_code" => nil,
    "longitude" => 113.25,
    "region_code" => "44"
},
```



# Elasticsearch

## ~Store, Search, Analyze~

# ハンズオン概要



演習

# Elasticsearch,Kibanaのセットアップ

# Elasticsearchの起動

---

## 1. カレントディレクトリを移動する

コマンド例:

```
$ cd ~/JJUG_fall/elasticsearch-5.0.0
```

## 2. Elasticsearchを起動する

```
$ bin/elasticsearch
```

# Elasticsearchの起動確認

---

- ・ ブラウザ(**Chrome or Safari**)でhttp://localhost:9200を開く。

**user:elastic , password:changeme**

- ・ 以下の内容が表示されること。

```
{  
  "name" : "1_lyK7k",  
  "cluster_name" : "elasticsearch",  
  "cluster_uuid" : "0Lwk8ZDITCOTXLfm9mO5Eg",  
  "version" : {  
    "number" : "5.0.0",  
    "build_hash" : "7eb6260",  
    "build_date" : "2016-09-20T23:10:37.942Z",  
    "build_snapshot" : false,  
    "lucene_version" : "6.2.0"  
  },  
  "tagline" : "You Know, for Search"  
}
```

# Kibana

# Kibanaの起動

---

- 新しくコマンドラインツールのウィンドウを開き、カレントディレクトリを移動する

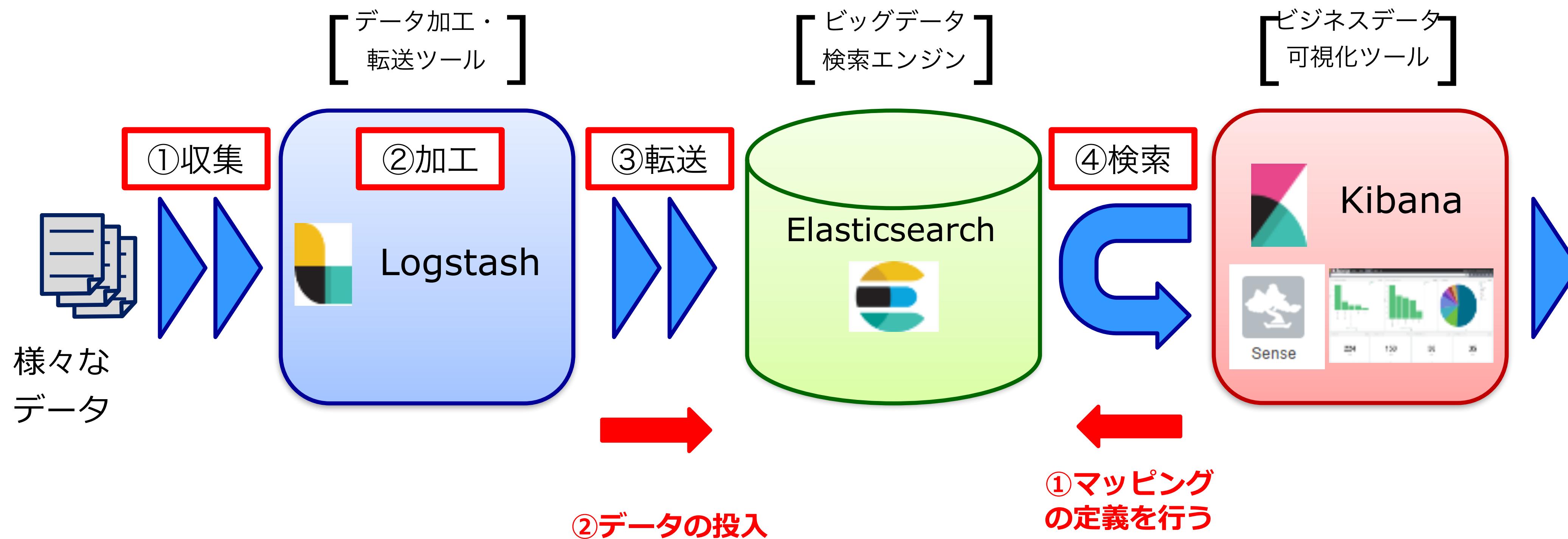
**\$ cd ~/JJUG\_fall/kibana-5.0.0-darwin-x86\_64**

※Macの場合のコマンド例

- Kibanaを起動する

**\$ bin/kibana**

# 全体の流れの確認





# Kibanaとは？

---

- 1. LogデータのDashboard**
- 2. さまざまな種類のグラフが用意されている**
- 3. 分かりやすいUIで、初心者でも可視化できる**
- 4. 作成したDashboardは、共有できる**
- 5. Webブラウザでアクセス可能**
  - モダンなブラウザが必要
  - **Chrome/Safari 推奨**

# 解析するログの説明



## Quick Draw

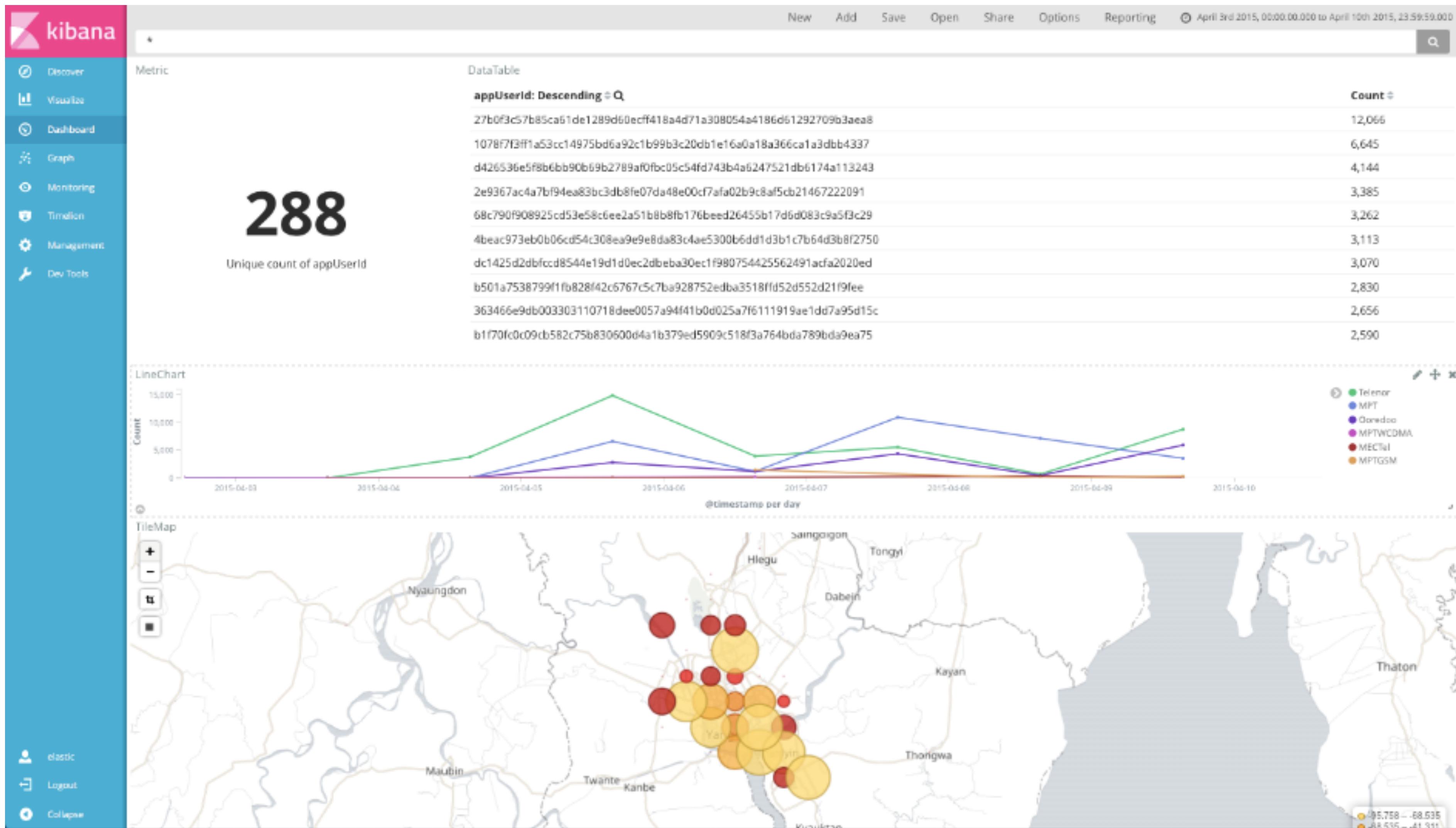
- ① ミャンマーで利用できる、スマホアプリ。
- ② スマホを操作すると、現在地の通信状況をサーバに送付する。
- ③ ユーザは、データを送付することで、景品が取得できるくじを引くことができる。

# ログのデータ形式

## 1. Quick Drawで取得できる項目の一部

項目名	内容
appUserId	アプリケーションのユーザID
@timestamp	ログ時刻
gender	性別
carrier	通信キャリア (Ooredoo, MPT, Telenor, 取得不可(null))
networkBean3G_neighboringCellInfo_rssi	3G回線の通信強度

# Kibana Dashboard



# マッピング定義を行う

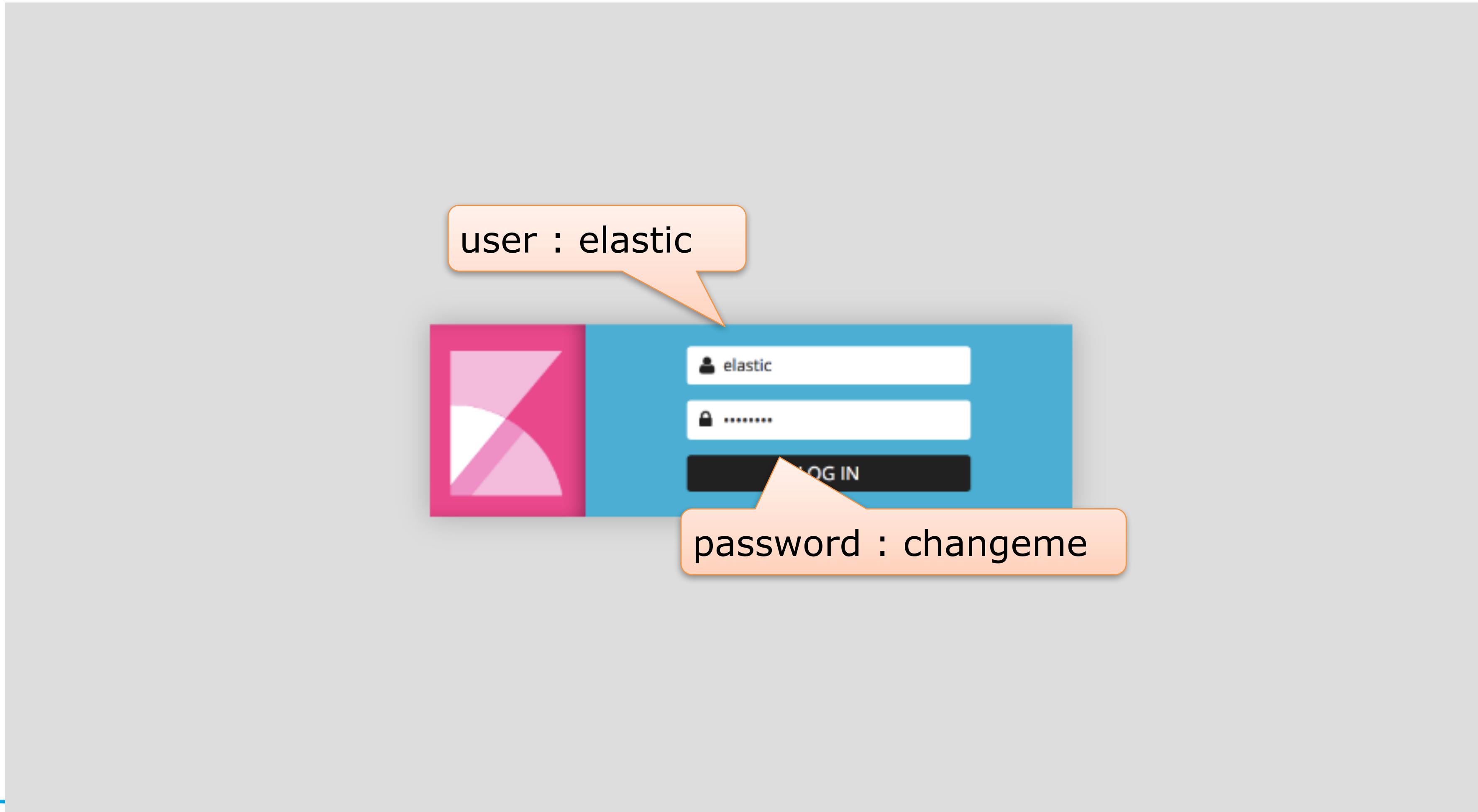
---

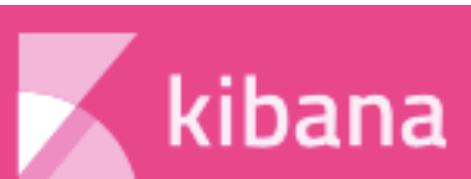
- ・ マッピング定義は、**Elasticsearch**に保存するドキュメントのデータ構造を設定するもの。
- ・ 以下の**URL**から**Kibana**にアクセスし**Console**を用いてマッピング定義を行う。

**http://localhost:5601**

# Kibanaログイン

- ・x-packをインストールすると認証がかかる





kibana

Discover

Visualize

Dashboard

Graph

Monitoring

Timelion

Management

Dev Tools

elastic

Logout

Collapse

## Welcome to X-Pack!

Sharing your cluster statistics with us helps us improve. Your data is never shared with anyone. Not interested? [Opt out here.](#)

[Dismiss](#)

Management / Kibana

[Index Patterns](#)   [Saved Objects](#)   [Reporting](#)   [Advanced Settings](#)

No default index pattern.  
You must select or create one to continue.

# Configure an index pattern

In order to use Kibana you must configure at least one index pattern. Index patterns are used to identify the Elasticsearch index to run search and analytics against. They are also used to configure fields.

**Index contains time-based events**

**Use event times to create index names** [DEPRECATED]

### Index name or pattern

Patterns allow you to define dynamic index names using \* as a wildcard. Example: logstash-\*

logstash-\*

**Do not expand index pattern when searching** (Not recommended)

By default, searches against any time-based index pattern that contains a wildcard will automatically be expanded to query only the indices that contain data within the currently selected time range.

Searching against the index pattern *logstash-\** will actually query elasticsearch for the specific matching indices (e.g. *logstash-2015.12.21*) that fall within the current time range.

Unable to fetch mapping. Do you have indices matching the pattern?

# LogをElasticsearchに送る(マッピング定義)

The screenshot shows the Kibana Dev Tools interface. On the left, there's a sidebar with icons for Discover, Visualize, Dashboard, Timelion, Management, and Dev Tools. The Dev Tools icon is highlighted with a red box and has a callout bubble pointing to it with the text '「DevTools」を選択する。' (Select 'DevTools'). The main area is a code editor with syntax highlighting for JSON. The code is a PUT request to create a template named 'twitter\_template'. The template defines a 'twitter' type with a '\_default\_' mapping for '\_all' fields and a 'string\_fields' mapping for '\*' fields. The '\_default\_' mapping includes a 'message\_field' with a 'string' type and an 'index' type of 'analyzed'. The 'string\_fields' mapping includes a 'raw' field with a 'string' type and an 'index' type of 'not\_analyzed'. There are also 'omit\_norms' settings for both types.

```
14 PUT _template/twitter_template
15 {
16   "template" : "twitter",
17   "mappings" : {
18     "_default_" : {
19       "_all" : {"enabled" : true, "omit_norms" : true},
20       "dynamic_templates" : [ {
21         "message_field" : {
22           "match" : "message",
23           "match_mapping_type" : "string",
24           "mapping" : {
25             "type" : "string", "index" : "analyzed", "omit_norms" : true
26           }
27         }
28       }, {
29         "string_fields" : {
30           "match" : "*",
31           "match_mapping_type" : "string",
32           "mapping" : {
33             "type" : "string", "index" : "analyzed", "omit_norms" : true,
34             "fields" : {
35               "raw" : {"type": "string", "index" : "not_analyzed",
36               "ignore_above" : 256}
37             }
38           }
39         }
40       }
41     }
42   }
43 }
```

# LogをElasticsearchに送る(マッピング定義)

The screenshot shows the Kibana Dev Tools Console interface. On the left, there is a sidebar with various navigation options: Discover, Visualize, Dashboard, Timelion, Management, and Dev Tools. The Dev Tools option is currently selected. The main area is titled "Console" and contains a code editor with the following JSON code:

```
PUT _template/qd-template
{
  "template" : "qdlog-*",
  "mappings": {
    "logs": {
      "dynamic_templates" : [
        {
          "my_multi_strings" : {
            "match_mapping_type" : "string",
            "mapping" : {
              "type" : "string", "index" : "not_analyzed"
            }
          }
        }
      ],
      "properties": {
        "location": {
          "type": "geo_point"
        },
        "timeRange": {
          "type": "integer"
        },
        "networkBean3G_neighboringCellInfo_rss": {
          "type": "float"
        },
        "networkBean3G_neighboringCell": {
          "type": "float"
        }
      }
    }
  }
}
```

Two orange callout boxes provide instructions:

- ①「mapping\_template.txt」の内容を貼る。
- ②「実行」ボタンをクリックする。

The "Execute" button (green triangle icon) is highlighted with a red box and an orange arrow pointing to it.

# LogをElasticsearchに送る(マッピング定義)



The screenshot shows the Kibana Dev Tools Console interface. On the left, there's a sidebar with icons for Discover, Visualize, Dashboard, Timelion, Management, and Dev Tools. The Dev Tools tab is selected. The main area contains a code editor with the following JSON template definition:

```
1 PUT _template/qd-template
2 {
3   "template" : "qdlog-*",
4   "mappings": {
5     "logs": {
6       "dynamic_templates": [
7         {
8           "my_multi_strings" : {
9             "match_mapping_type" : "string",
10            "mapping" : {
11              "type" : "string", "index" : "not_analyzed"
12            }
13          }
14        }
15      ],
16      "properties": {
17        "location": {
18          "type": "geo_point"
19        },
20        "timeRange": {
21          "type": "integer"
22        },
23        "networkBean3G_neighboringCellInfo_rssi": {
24          "type": "float"
25        },
26        "networkBean3G_neighboringCellInfo_psc": {
27          "type": "float"
28        }
29      }
30    }
31  }
32 }
33 }
```

To the right of the code editor, there's a status bar with "History" and "Settings" buttons. Below the status bar, a message box contains the text: "acknowledged" : true と表示されれば成功". A red box highlights the "acknowledged" field in the status bar message.

"acknowledged" : true  
と表示されれば成功

# LogをElasticsearchに送る

---

- Logstashの設定ファイルは"**complete.conf**"を使用

※**JJUG\_fall**直下に移動してから以下のコマンドを実行する

※Linux, Macの方

```
% cat qdlog.csv | logstash-5.0.0/bin/logstash -f complete.conf
```

※Windowsの方

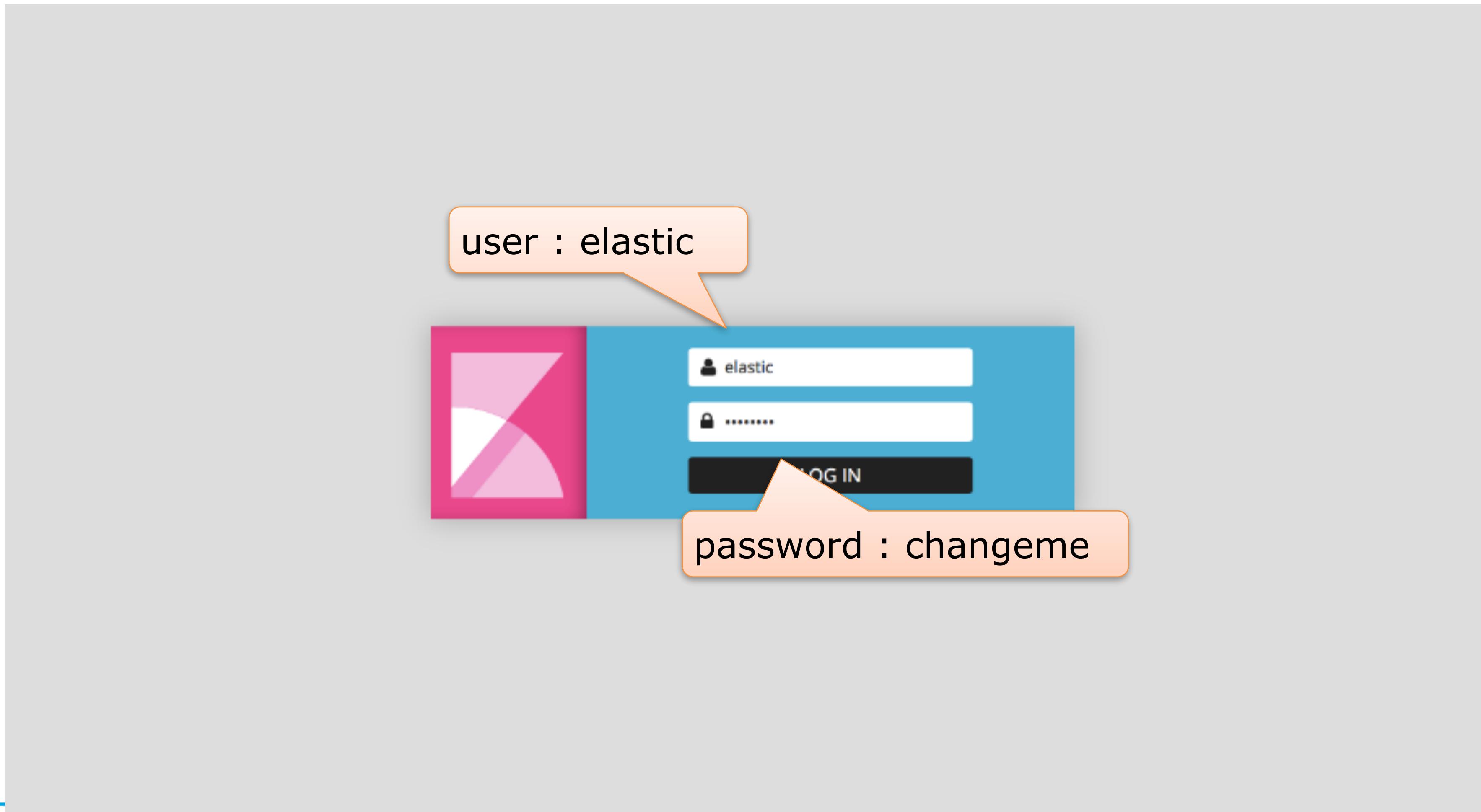
```
% type qdlog.csv | logstash-5.0.0\bin\logstash -f complete.conf
```

演習

KibanaでDashboardを作成してみよう！

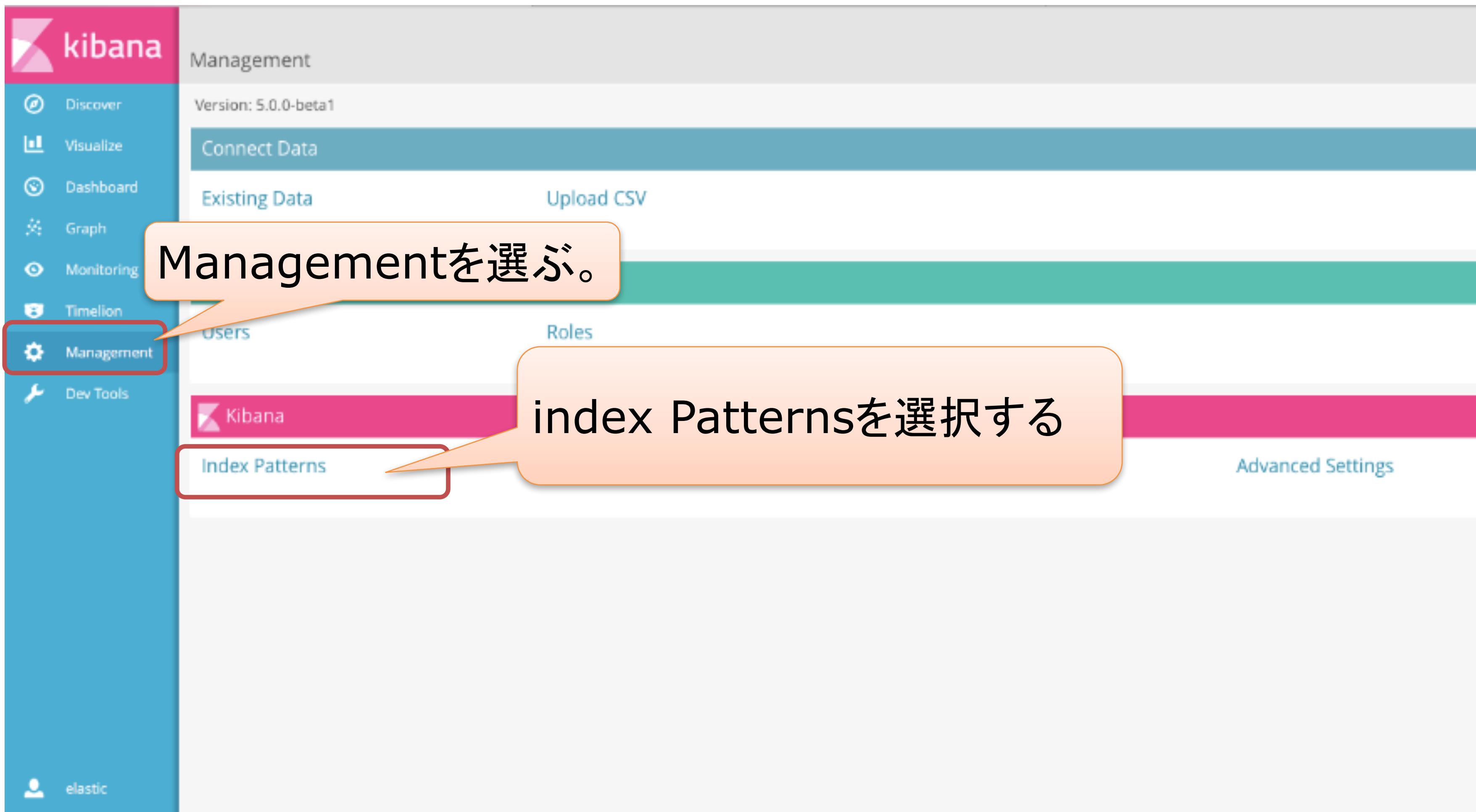
# Security

- ・x-packをインストールすると認証がかかる



# Settings

index patternを設定する



# Settings

## index patternを設定する

The screenshot shows the Kibana interface with the following details:

- Left Sidebar:** Shows navigation options: Discover, Visualize, Dashboard, Graph, Monitoring, Timelion, Management, and Dev Tools. The Management option is currently selected.
- Header:** Management / Data, Existing Data (selected), Upload CSV.
- Warning Message:** No default index pattern. You must select or create one to continue.
- Title:** Configure an index pattern
- Description:** In order to use Kibana you must configure at least one index pattern. Index patterns are used to identify the data against. They are also used to configure fields.
- Checkboxes:**
  - Index contains time-based events
  - Use event times to create index names (DEPRECATED)
- Text Input:** Index name or pattern. A placeholder says "Patterns allow you to define dynamic index names". The input field contains "qdlog-\*".
- Checkboxes:**
  - Do not expand index pattern when searching (Not recommended)
- Description:** By default, searches against any time-based index pattern that contains a wildcard will automatically be expanded to search all indices within the currently selected time range.
- Description:** Searching against the index pattern `logstash-*` will actually query Elasticsearch for the specific matching index within the current time range.
- Text Input:** Time-field name. A placeholder says "refresh fields". The input field contains "@timestamp".
- Buttons:** Create

**Annotations:**

- An orange callout points to the "Index name or pattern" input field with the text: 参照するindexパターンを qdlog-\* にする。
- An orange callout points to the "Time-field name" input field with the text: Time-field nameとして @timestamp を指定する。

# Discover

## 1. Discoverを選択し、画面右上の時計マークをクリックする

The screenshot shows the Kibana interface with the 'Discover' tab selected (highlighted by a red box). The search bar contains the query '\*'. The time range is set to 'Last 15 minutes'. The main message says 'No results found 😞'. It suggests expanding the time range or refining the query. Examples of queries are provided:

- Find requests that contain the number 200, in any field:  
200
- Or we can search in a specific field. Find 200 in the status field:  
status:200
- Find all status codes between 400-499:  
status:[400 TO 499]
- Find status codes 400-499 with the extension php:  
status:[400 TO 499] AND extension:PHP
- Or HTML  
status:[400 TO 499] AND (extension:php OR extension:html)

# Discover

## 2. データの表示期間を設定する

The screenshot shows the Kibana Discover interface with the following elements:

- Top Bar:** Displays "155,840 hits" and navigation buttons: New, Save, Open, Share, Reporting, Auto-refresh, and a date range selector from "April 3rd 2015, 00:00:00.000" to "April 11th 2015, 23:59:59.000".
- Left Sidebar:** Shows navigation links: Discover (selected), Visualize, Dashboard, Graph, Monitoring, Timeline, Management, and Dev Tools.
- Time Range Selection:** A red box highlights the "Absolute" button under "Quick" mode. Below it, a date range is set from "2015-04-03 00:00:00.000" to "2015-04-11 23:59:59.000". A calendar view shows April 2015 with days 03 and 11 selected. An orange callout labeled ② 表示期間の設定 (Setting the display period) points to the calendar. Another orange callout labeled ① 表示期間の設定方法をAbsoluteにする (Set the display period method to Absolute) points to the "Absolute" button.
- Bottom Panel:** Shows a histogram titled "00:00:00.000 - April 11th 2015, 23:59:59.000 — by 3 hours". The Y-axis is "Count" (0 to 20,000) and the X-axis is "Time" (2015-04-04 09:00 to 2015-04-11 09:00). The chart displays data points for @timestamp per 3 hours.
- Selected Fields:** A sidebar on the left lists "Selected Fields" (e.g., \_source) and "Available Fields" (e.g., @timestamp, @version, \_id, \_index, \_score).

# Visualizationの作成

---

1. 以下のVisualizationを作成する。

- ① 「Metrics」を利用し、ユニークユーザ数を表示する。
- ② 「Data Tables」を利用し、データ数の多い上位10ユーザの一覧を表示する。
- ③ 「Line Chart」を利用し、日毎・キャリア毎のアクセス数を表示する。
- ④ 「Tile Map」を利用し、キャリアMPTの3G回線通信強度を地図上に可視化する

# Visualizeの作成方法

The screenshot shows the Kibana interface. On the left, the navigation bar includes 'Discover', 'Visualize' (which is highlighted with a red box), 'Dashboard', 'Graph', 'Monitoring', 'Timeline', 'Management', and 'Dev Tools'. Below the navigation is the elastic logo and a 'Logout' button. The main content area is titled 'Visualize / Step / 1 Create New'. It displays several chart types: 'Area chart', 'Data table', 'Line chart', 'Markdown widget', 'Metric' (which is highlighted with a red box and has a speech bubble pointing to it), and 'Pie chart'. A large orange speech bubble points from the text 'visualizeを選択する' (Select Visualize) to the 'Visualize' button in the sidebar. Another orange speech bubble points from the text 'グラフの種類を選択する。' (Select chart type) to the 'Metric' section.

visualizeを選択する

Or, Open a Saved Visualization

Visualizations Filter... 0 of 0 Manage Visualizations

Name ▾

No matching visualizations found.

# Visualizationの作成

The screenshot shows the Kibana interface at 'Visualize / Step / 2'. On the left, a sidebar menu includes 'Discover', 'Visualize' (selected), 'Dashboard', 'Graph', 'Monitoring', 'Timelion', 'Management', and 'Dev Tools'. The main area is titled 'From a New Search, Select Index'. It features a search bar labeled 'Filter...' and a table with one entry: 'Name ▲ qdlog-\*'. A large orange callout bubble with the Japanese text 'qdlog-\*を選択する。' (Select qdlog-\*.) points to the 'qdlog-\*' entry. To the right, another section titled 'Or, From a Sa...' is partially visible.

qdlog-\*を選択する。

# Visualizationの作成

The screenshot shows the Kibana interface with the following details:

- Left Sidebar:** A vertical sidebar with a pink header containing the Kibana logo. Below it are icons for Discover, Visualize (selected), Dashboard, Graph, Monitoring, Timeline, Management, and Dev Tools. At the bottom is an elastic logo.
- Top Bar:** A navigation bar with buttons for New, Save, Load, Share, Refresh, Reporting, and a date range selector set to April 3rd 2015 to April 10th 2015. There is also a search icon.
- Central Area:** A visualization card for "qdlog-\*". It has tabs for Data and Options, with "Data" selected. The visualization type is "metrics".
  - Metric:** Set to "Count".
  - Custom Label:** An empty input field.
  - Advanced:** A button to expand advanced settings.
  - Add metrics:** A button to add more metrics.
- Result:** A large bold number "92,025" displayed below the visualization card, labeled "Count".

# Visualizationの作成

The screenshot shows the Kibana interface with the following details:

- Left Sidebar:** Discover, Visualize (selected), Dashboard, Graph, Monitoring, Timelion, Management, Dev Tools.
- Top Bar:** New, Save, Load, Share, Refresh, Reporting, Date range (April 3rd 2015, 00:00:00.000 to April 10th 2015, 23:59:59.000), Search icon.
- Central Area:** Index pattern: qlog-\*  
Panel: Data Options  
Metrics:
  - Metric: Aggregation (highlighted with a red box)
    - Aggregation: Unique Count (highlighted with a red box)
    - Field: appUserId
- Bottom Right:** Large number 288, Text: Unique count of appUserId.
- Callout Box:** Aggregation : Unique Count, Field : appUserId

# Visualizationの作成



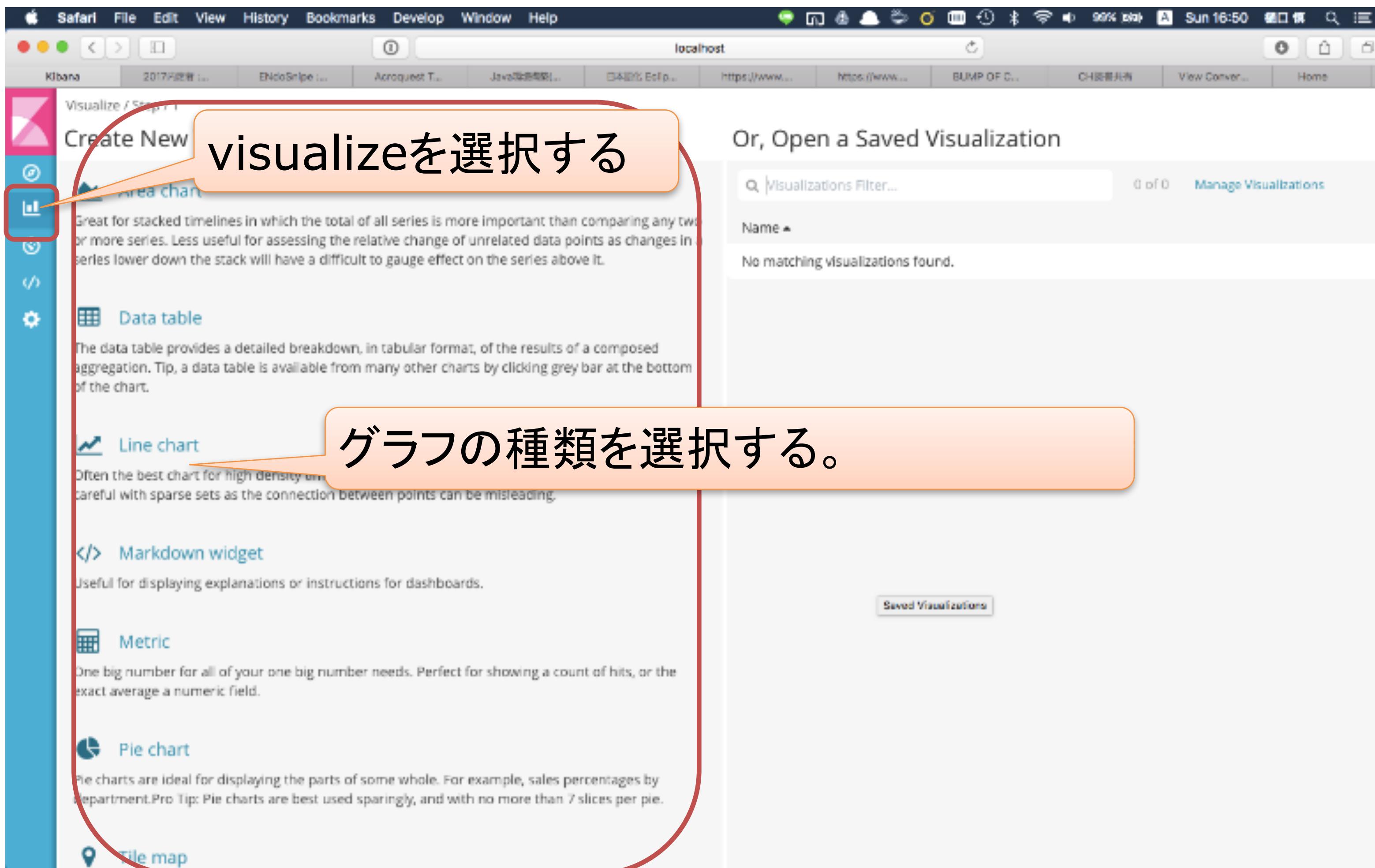
# Visualizationの作成

---

1. 以下の**Visualization**を作成する。

- ① 「Metrics」を利用し、ユニークユーザ数を表示する。
- ② 「Data Tables」を利用し、データ数の多い上位10ユーザの一覧を表示する。
- ③ 「Line Chart」を利用し、日毎・キャリア毎のアクセス数を表示する。
- ④ 「Tile Map」を利用し、キャリアMPTの3G回線通信強度を地図上に可視化する。

# Visualizationの作成



# Visualizationの作成

Visualize / Step / 2

From a New Search, Select Index

Or, From a Saved Search

Filter... 3 of 3

Saved Searches Filter... 0 of 0 Manage Saved Searches

Name:

- qdlog-\* (highlighted with a red box)
- qdlog-csv
- weather

saved searches found.

qdlog-\*を選択する。

# Visualizationの作成(Data Tables)

The screenshot shows the Kibana interface with a Data Table visualization titled "appUserId: Descending". The visualization displays a list of appUserIds along with their counts. The interface includes a sidebar with "qlog-\*" selected, and sections for "metrics" and "buckets". The "buckets" section is expanded, showing "Terms" selected under "Type", "appUserId" under "Field", "metric: Count" under "Order By", and "Descending" with a size of "10" under "Order". A search bar at the top right shows the date range "April 3rd 2015, 00:00:00,000 to April 10th 2015, 23:59:59,000".

① Terms

② appUserId

③ Count

④ Descending 10

appUserId	Count
27b0f3c57b85ca61de1289d60ecff418a4d71a308054a4186d61292709b3aea8	12,066
1078f7f3ff1a53cc14975bd6a92c1b99b3c20db1e16a0a18a366ca1a3dbb4337	6,645
d426536e5f8b6bb90b69b2789af0fc05c54fd743b4a6247521db6174a113243	4,144
2e9367ac4a7bf94ea83bc3db8fe07da48e00cf7afa02b9c8af5cb21467222091	3,385
68c790f908925cd53e58c6ee2a51b8b8fb176beed26455b17d6d083c9a5f3c29	3,262
4beac971b8f2750	3,113
dc12020ed	3,070
b501a7538799f1fb828f42c6767c5c7ba928752edba3518ffd52d552d21f9fee	2,830
363466e9db003303110718dee0057a94f41b0d025a7f6111919ae1dd7a95d15c	2,656
b1f70fc9a9ea75	2,590

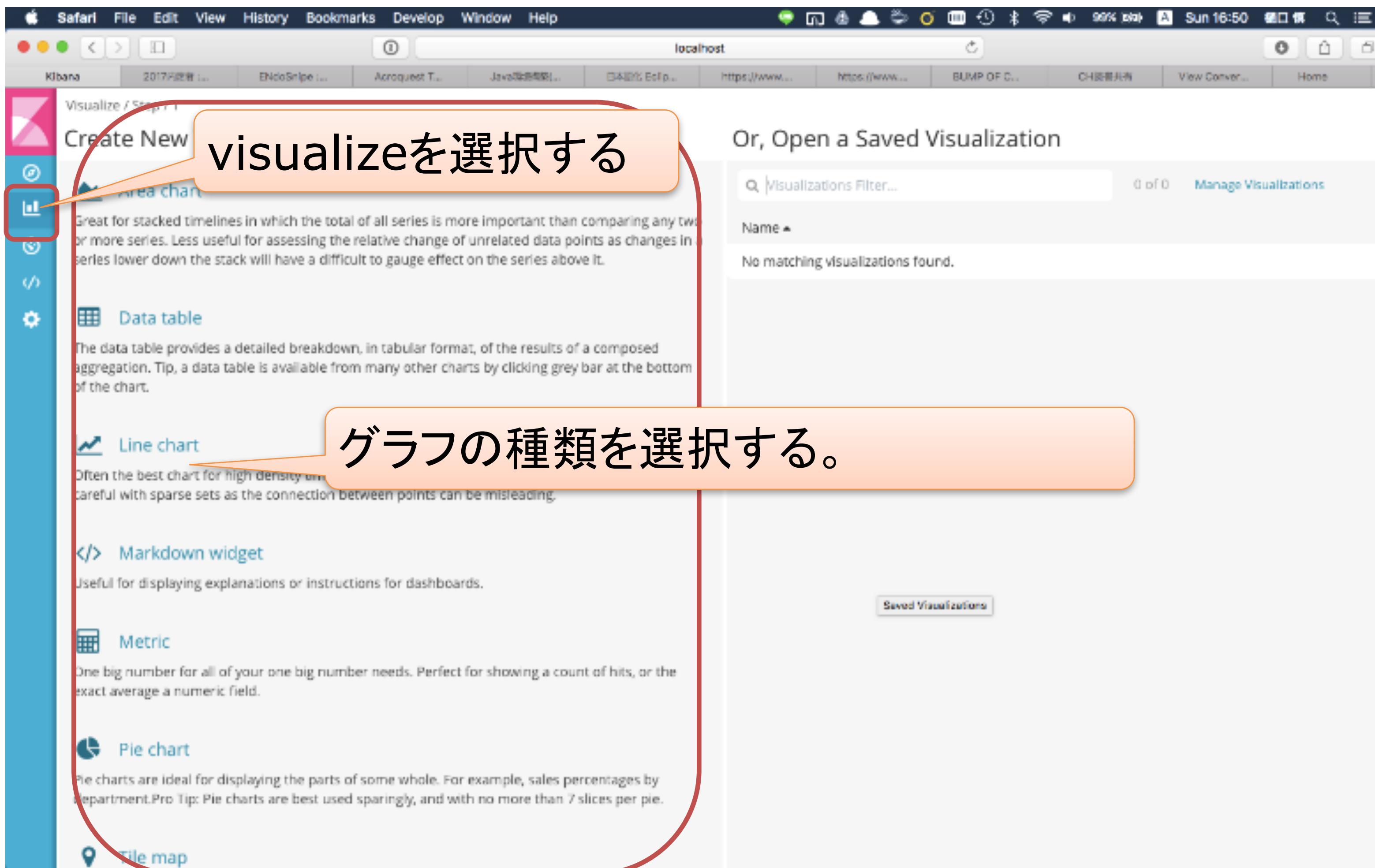
# Visualizationの作成

---

1. 以下の**Visualization**を作成する。

- ① 「Metrics」を利用し、ユニークユーザ数を表示する。
- ② 「Data Tables」を利用し、データ数の多い上位10ユーザの一覧を表示する。
- ③ 「Line Chart」を利用し、日毎・キャリア毎のアクセス数を表示する。
- ④ 「Tile Map」を利用し、キャリアMPTの3G回線通信強度を地図上に可視化する。

# Visualizationの作成



# Visualizationの作成

Visualize / Step / 2

From a New Search, Select Index

Or, From a Saved Search

Filter... 3 of 3 | Saved Searches Filter... 0 of 0 Manage Saved Searches

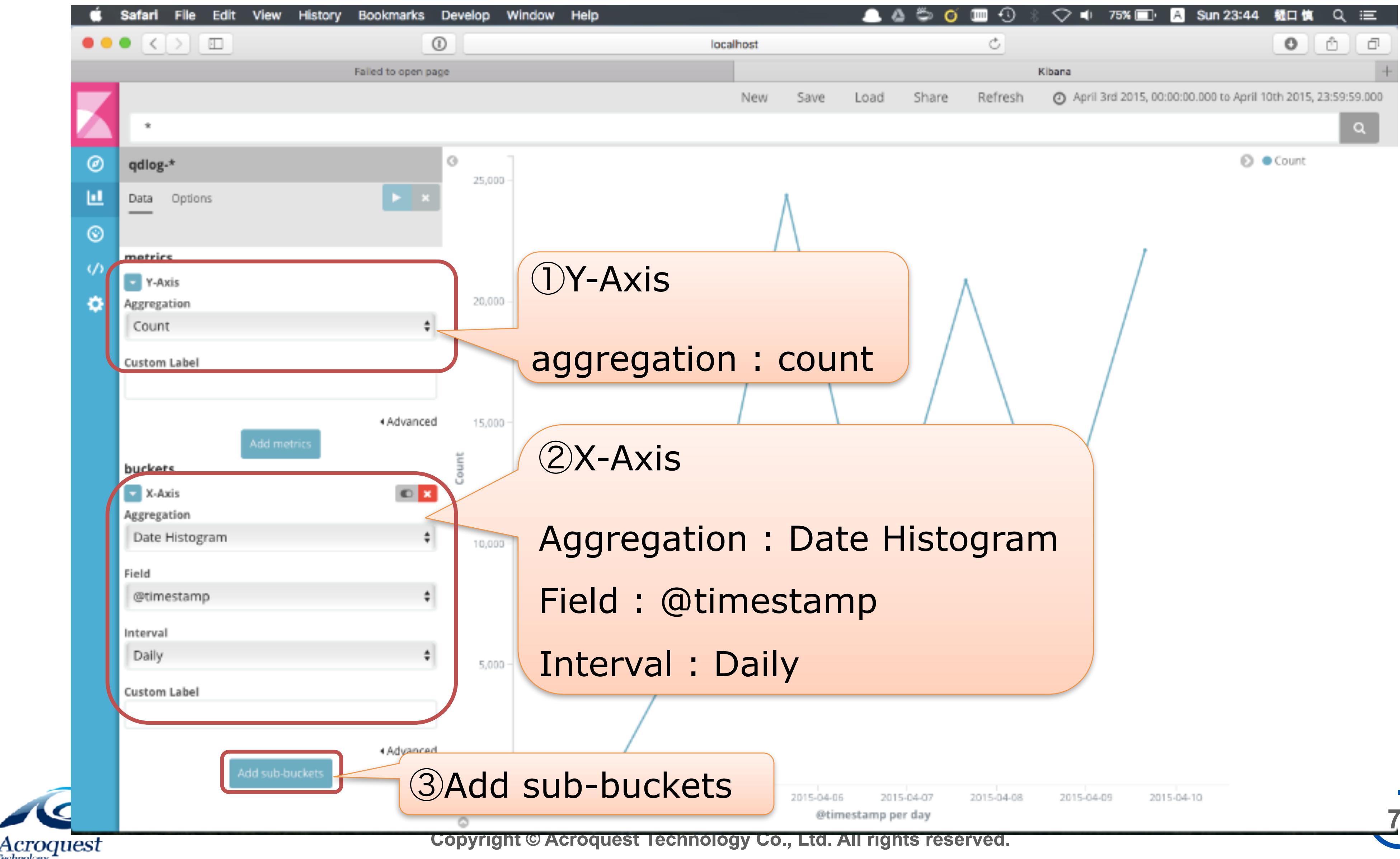
Name:

- qdlog-\* (highlighted with a red box)
- qdlog-csv
- weather

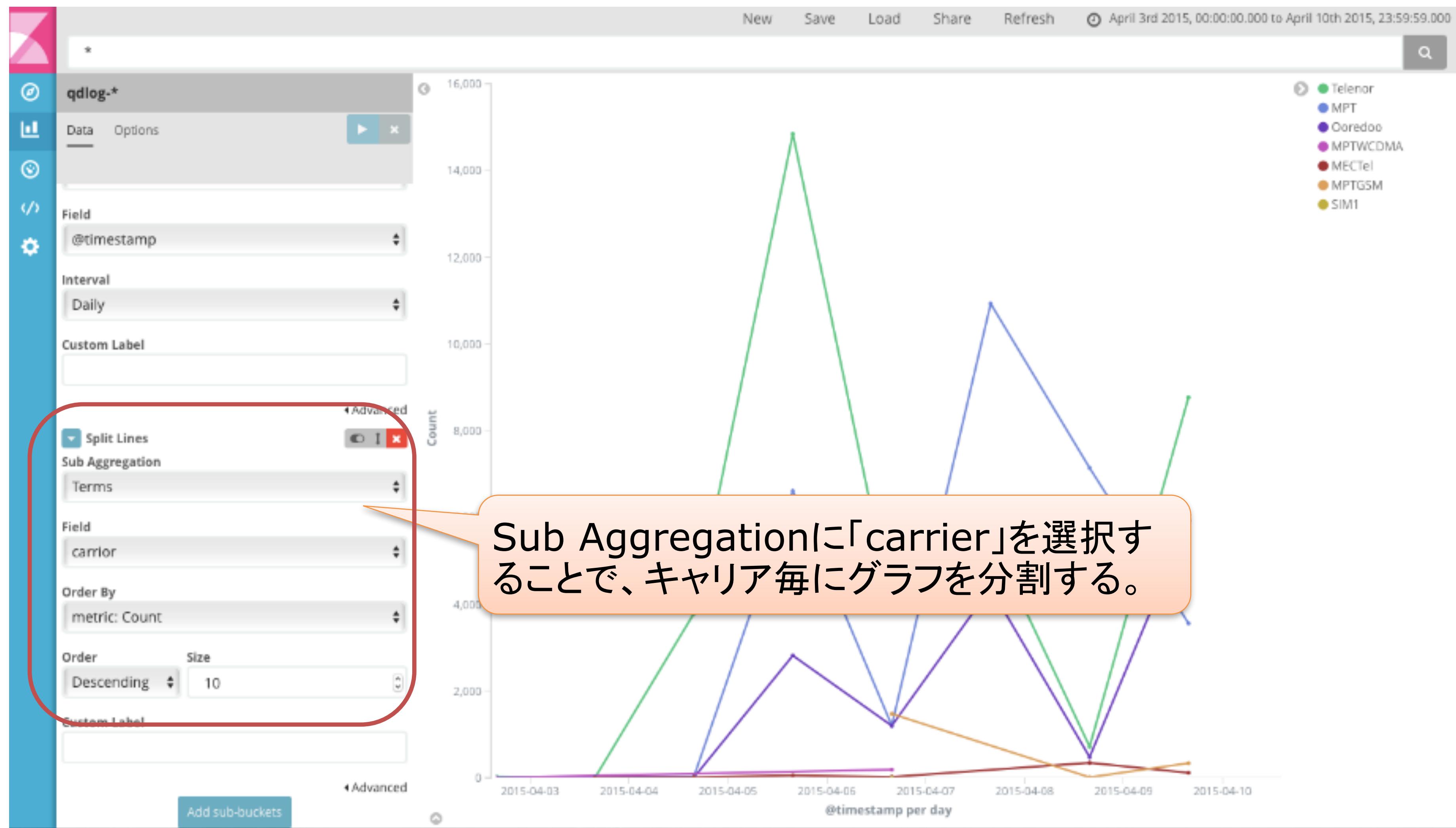
saved searches found.

qdlog-\*を選択する。

# Visualizationの作成(Line Chart)



# Visualizationの作成(Line Chart)



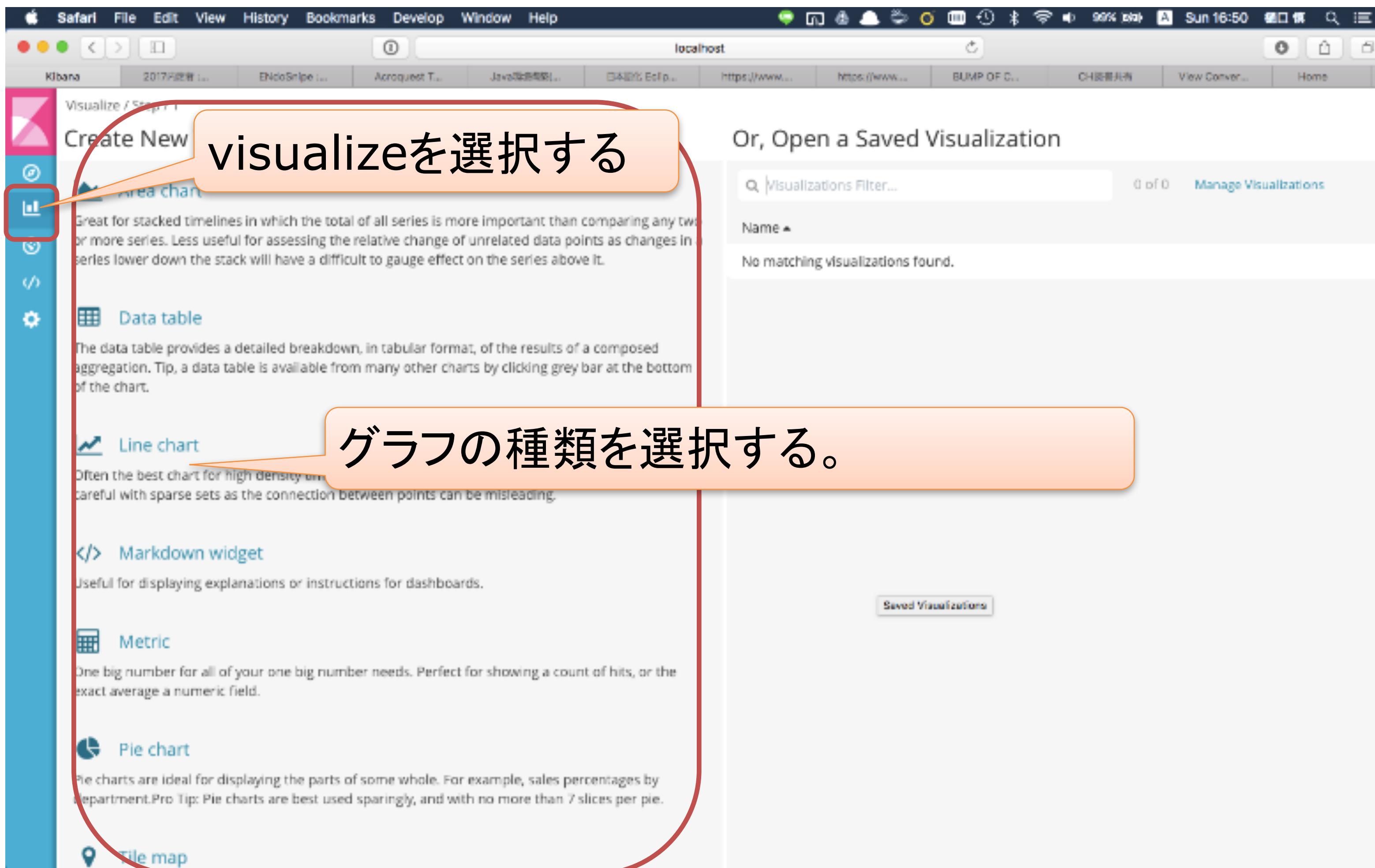
# Visualizationの作成

---

1. 以下の**Visualization**を作成する。

- ① 「Metrics」を利用し、ユニークユーザ数を表示する。
- ② 「Data Tables」を利用し、データ数の多い上位10ユーザの一覧を表示する。
- ③ 「Line Chart」を利用し、日毎・キャリア毎のアクセス数を表示する。
- ④ 「Tile Map」を利用し、キャリアMPTの3G回線通信強度を地図上に可視化する。

# Visualizationの作成



# Visualizationの作成

Visualize / Step / 2

From a New Search, Select Index

Or, From a Saved Search

Filter... 3 of 3

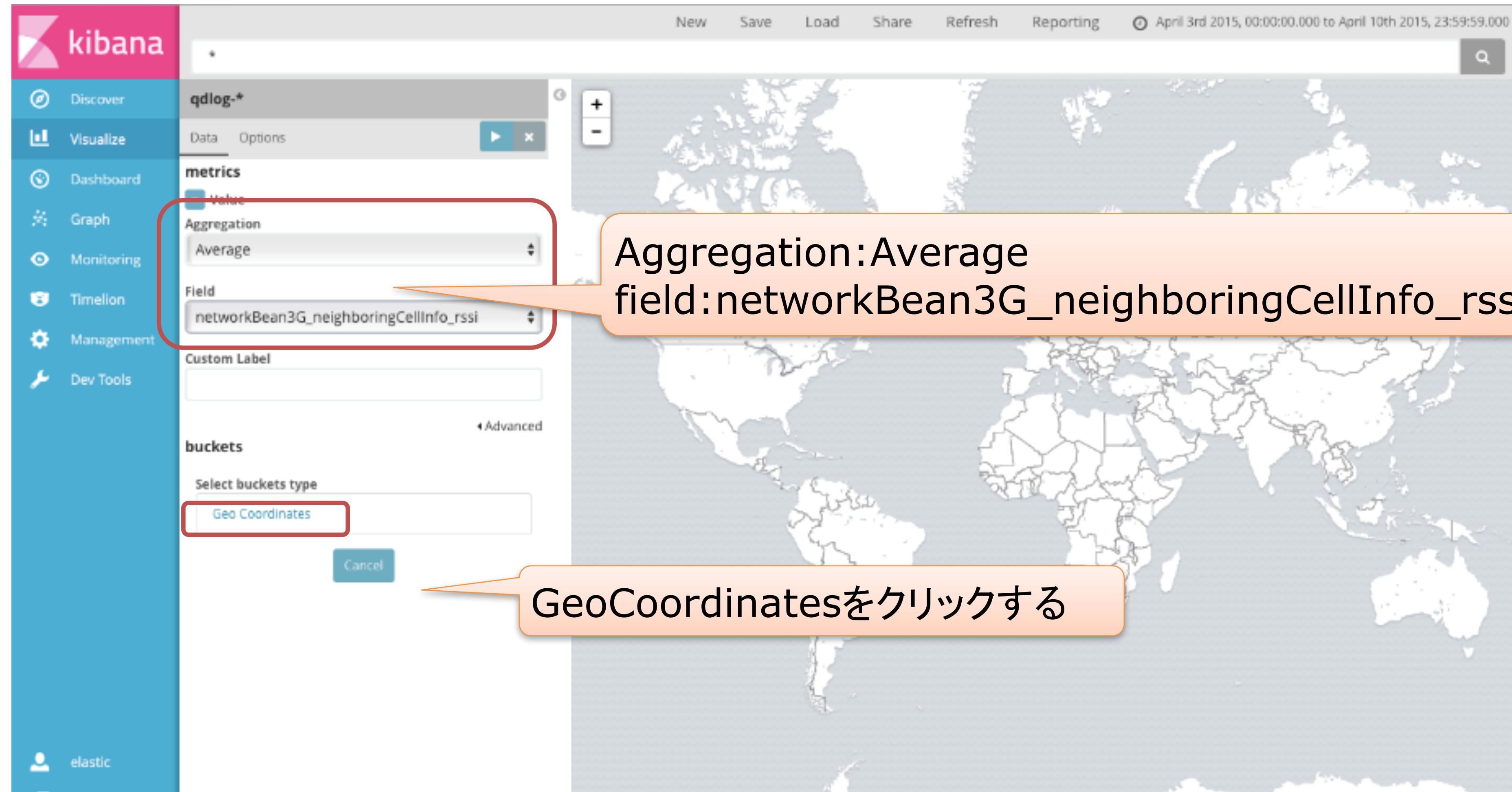
Saved Searches Filter... 0 of 0 Manage Saved Searches

Name:

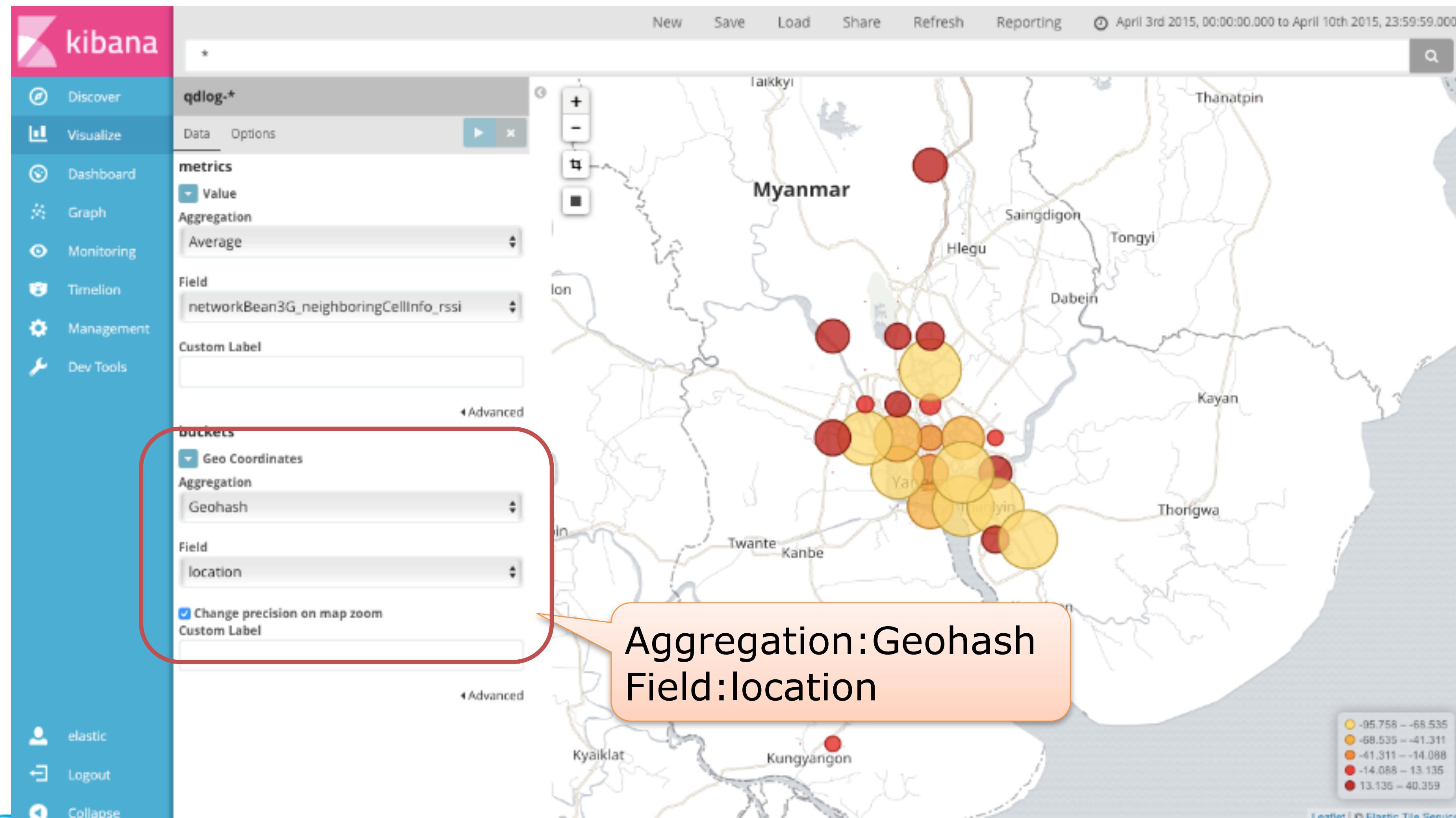
- qdlog-\* (highlighted)
- qdlog-csv
- weather

qdlog-\*を選択する。

# Visualizationの作成(Line Chart)



# Visualizationの作成(Line Chart)

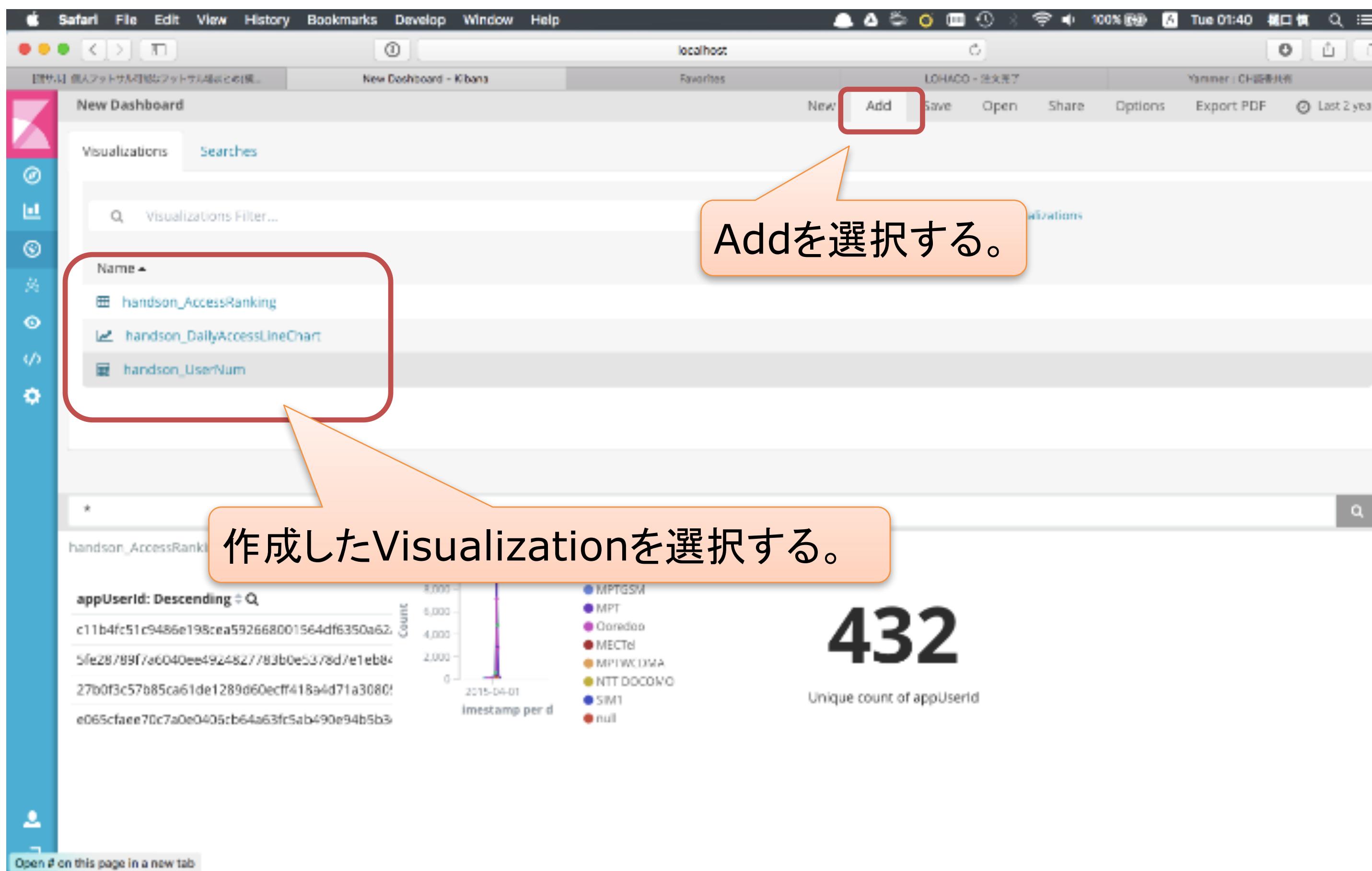


# Dashboardタブ

---

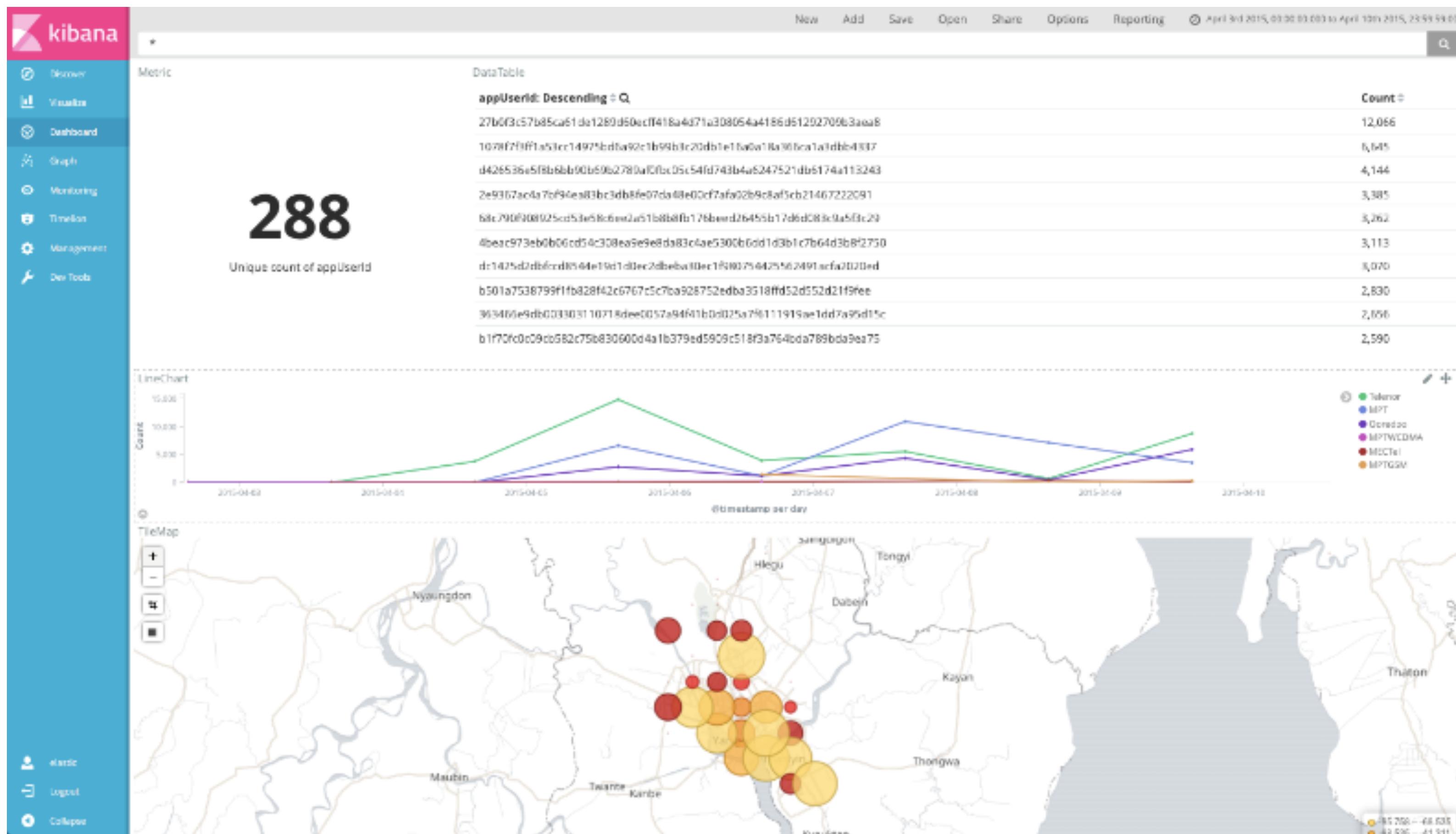
- 1. 演習2で作成したVisualizationを利用し、  
Dashboardを作成する。**
  
- 2. Dashboardを作成したら、Dashboardで表示  
した内容から、どのような情報が得られるか確認  
する。**

# Dashboardタブ



# Dashboardタブ

- ・ドラッグで位置変更やサイズ変更ができる



# 発展課題

---

- 1. Visualize**で、様々な種類のグラフを試しに作ってみましょう。
- 2. Percentile Area Chart**や**Heatmap**なども作れるので、試してみましょう。

# X-Packの機能

## Security

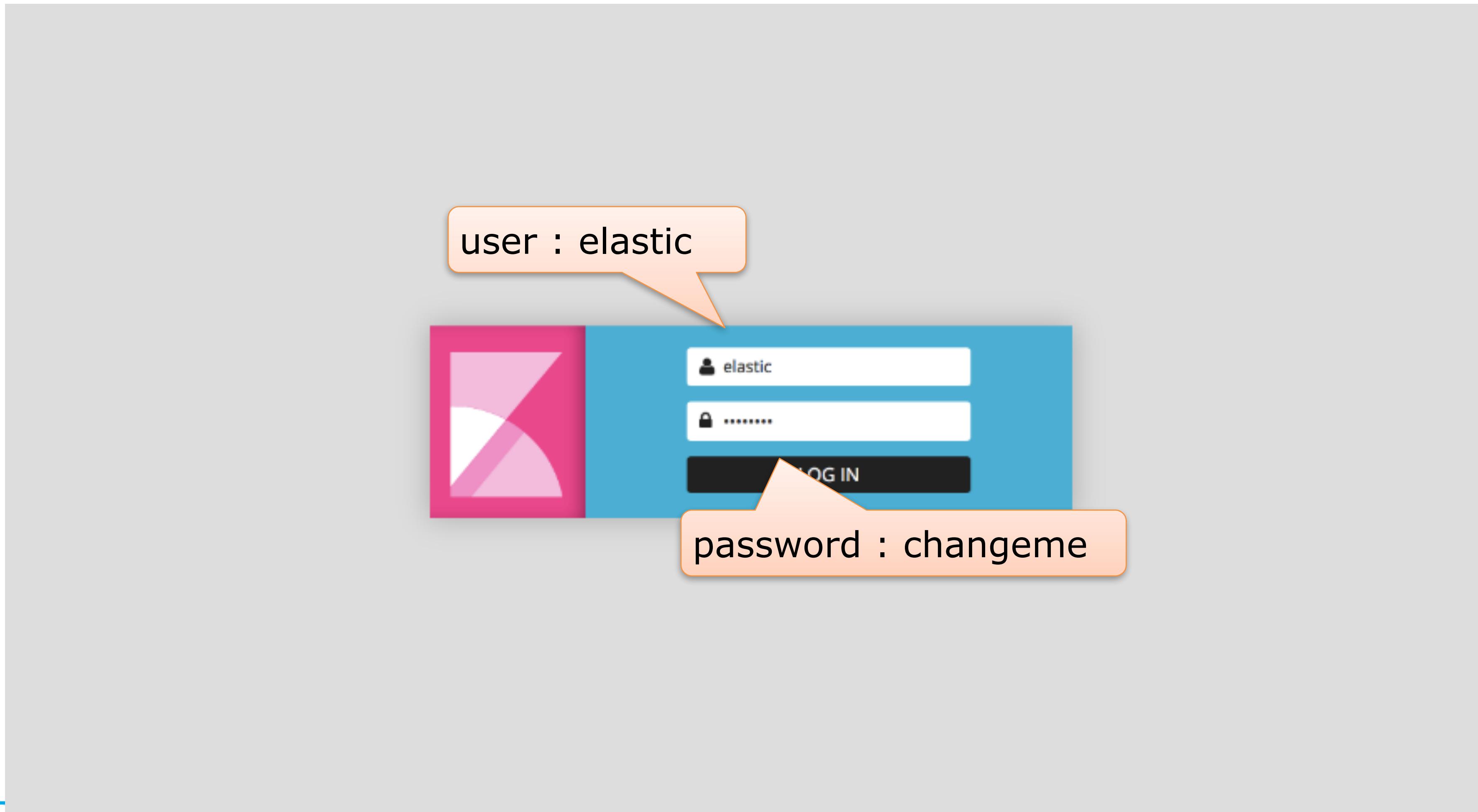
# Security

---

- 1. ユーザ認証機能を持つ  
LDAP/Active Directory/ファイルベース**
- 2. 認可機能を持つ  
ロールベースのACL  
インデックス、操作単位で設定可  
DocumentおよびFieldレベルのセキュリティ対応**
- 3. セキュアな通信が可能となる  
ノードおよびクライアント間、IPフィルタリング**
- 4. 監査ログを残すことができる**

# Security

- ・x-packをインストールすると認証がかかる



# Security

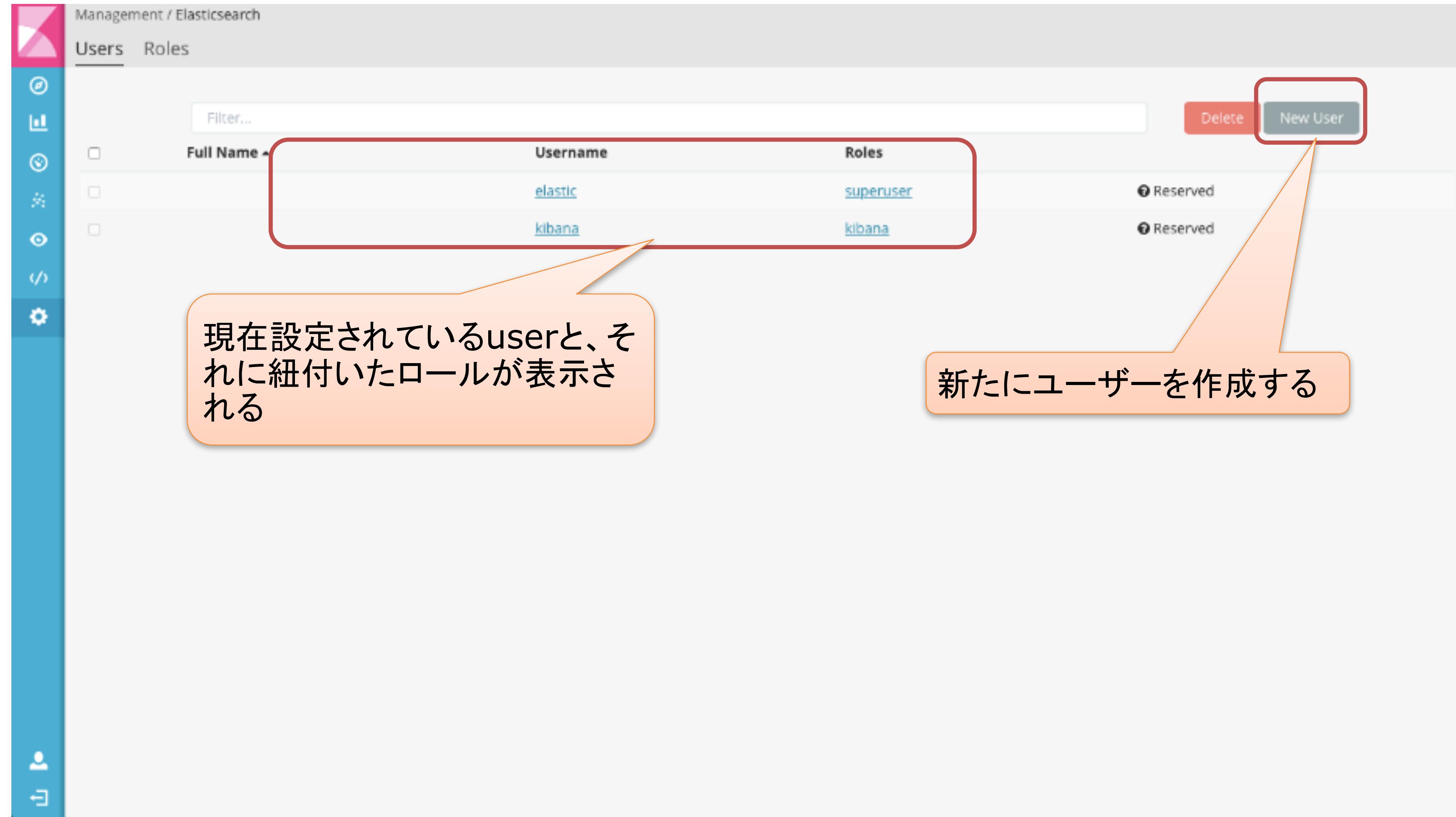
The screenshot shows the Kibana Management interface. On the left, there's a sidebar with icons for Discover, Visualize, Dashboard, Graph, Monitoring, Console, and Management. The Management icon is selected and highlighted with a red box. The main area has a teal header bar with 'Management', 'Version: 5.0.0-alpha4', 'Connect Data' (with 'Existing Data' and 'Upload CSV' options), and an 'Elasticsearch' section containing 'Users' and 'Roles' tabs. An orange callout bubble points to the 'userとroleの設定が増えている' (The number of user and role settings has increased) text above the 'Roles' tab. Below the main area, there are links for 'Index Patterns', 'Saved Objects', 'Reporting', and 'Advanced Settings'. At the bottom, it says 'Open #/management on this page in a new tab'.

userとroleの設定が増えている

# Security

The screenshot shows the Kibana Management interface. On the left, a sidebar menu includes Discover, Visualize, Dashboard, Graph, Monitoring, Console, and Management. The Management option is selected. The main area is titled 'Management' and shows 'Version: 5.0.0-alpha4'. A teal bar at the top has 'Connect Data' and 'Existing Data' and 'Upload CSV' buttons. Below this, there's a section for 'Elasticsearch' with 'Users' and 'Roles' tabs. An orange callout box with the text 'usersを選択する' (Select users) points to the 'Users' tab. At the bottom, there are links for 'Index Patterns', 'Saved Objects', 'Reporting', and 'Advanced Settings'. A footer bar at the bottom has the Kibana logo and a link to open the management page in a new tab.

# Security



Management / Elasticsearch

Users Roles

Full Name

Username

Roles

elastic

superuser

kibana

kibana

New User

Delete

① Reserved

② Reserved

現在設定されているuserと、それに紐付いたロールが表示される

新たにユーザーを作成する

# Security

Management / Elasticsearch / Users

Users Roles

New User

Username: test\_user

Password: .....  
.....

Full Name: shin higuchi

Email: xxx@gmail.com

Change Password

Return to All Users Save

Roles

Add a role...

Username : test\_user  
Password : password  
Fullscreen : 任意  
Email : 任意

# Security

Management / Elasticsearch

Users Roles

Filter...

Delete New User

Full Name	Username	Roles	
	elastic	superuser	Reserved
	kibana	kibana	Reserved
shin.higuchi	test_user		

userが追加された

# Security

The screenshot shows the Elasticsearch Management interface under the Security section. The 'Roles' tab is selected, indicated by a red box. A table lists three reserved roles: 'kibana\_user', 'superuser', and 'transport\_client'. Each role has a small checkbox icon to its left and a status indicator 'Reserved' to its right. A red box highlights the table area. An orange callout bubble points to the table with the text '設定されたroleの一覧が表示される' (A list of the roles set is displayed).

Role	Description
kibana_user	Reserved
superuser	Reserved
transport_client	Reserved

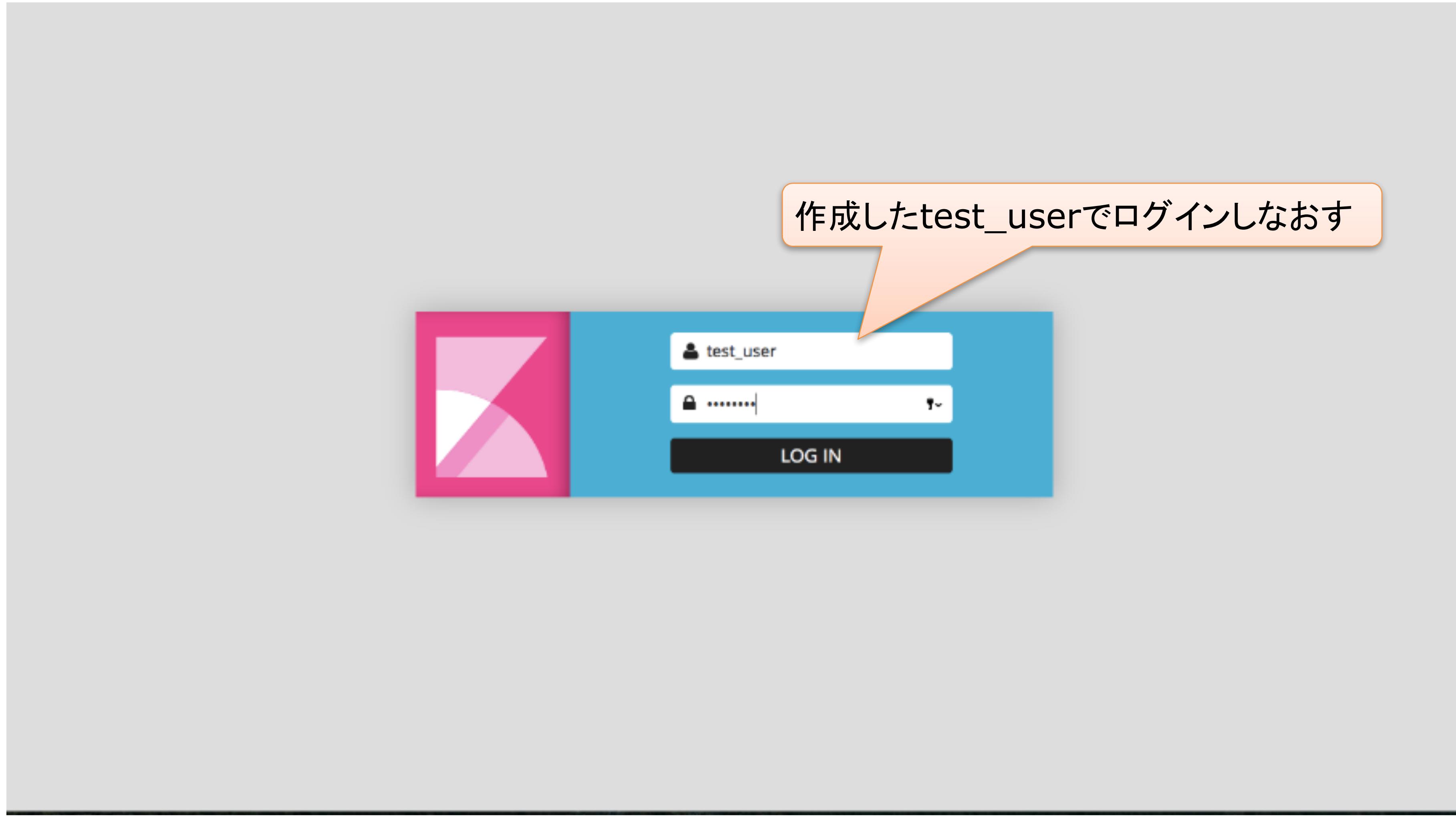
# Security

The screenshot shows the Elasticsearch Management interface under the 'Roles' tab. A role named 'test\_role' is being edited. The 'monitor' privilege is selected in the 'Cluster Privileges' section. In the 'Indices Privileges' section, three index patterns are defined with their respective privileges:

- weather : all
- .kibana\* : all
- qdlog-\* : read

Orange callout boxes highlight the 'monitor' privilege and the 'test\_role' name. Another orange callout box highlights the three index patterns listed under 'Indices Privileges'.

# Security



- 1. test\_userでログインした時にqdlog-\*にマッチするindexが作成できないことを確認してみましょう**
  
- 2. 他のユーザーも作成して、いろいろなアクセス制御を試してみましょう**

# Monitoring

# Monitoring

---

- **kibana**の画面上で**elasticsearch**や**kibana**の稼働状況を監視できる。

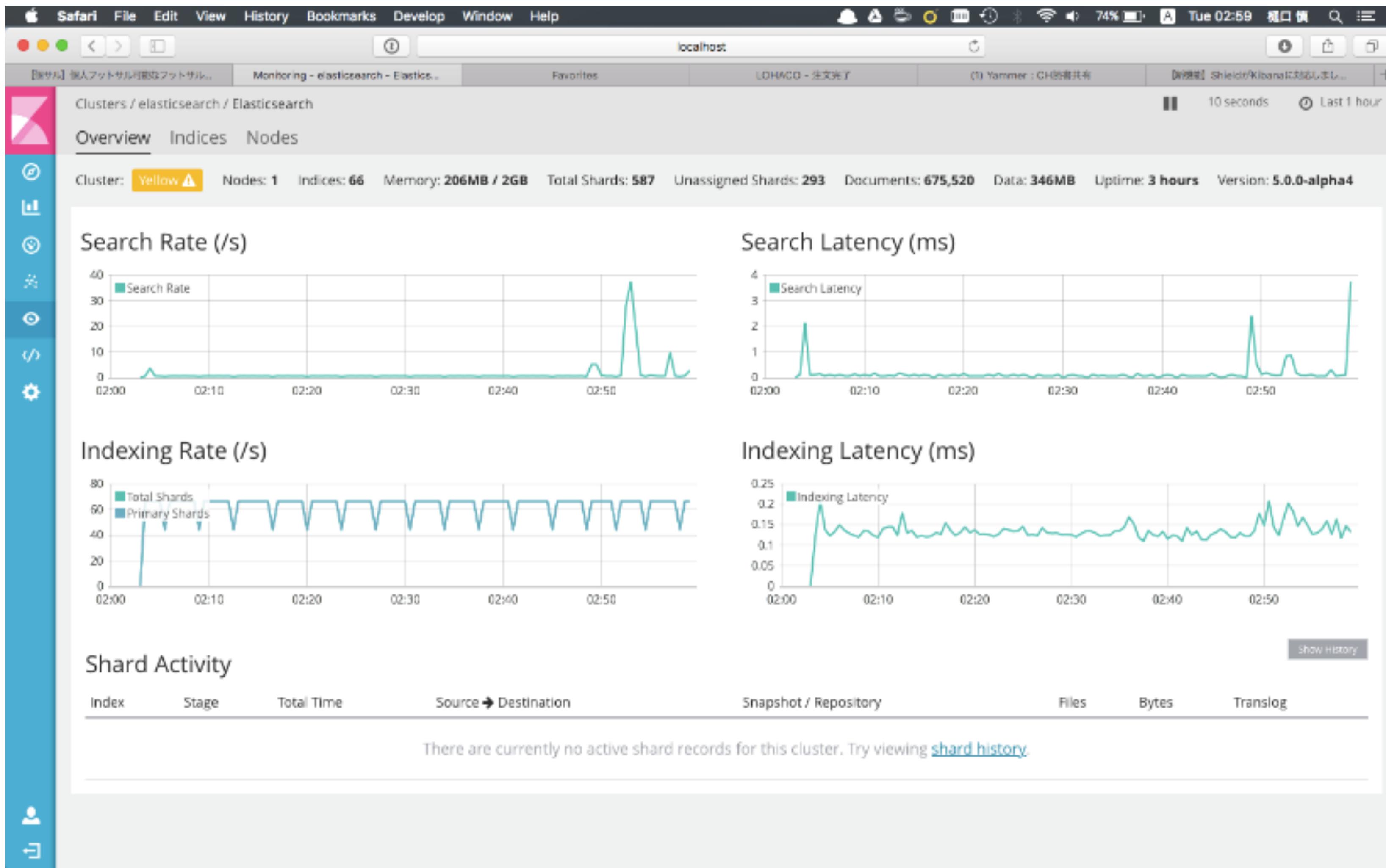
# Monitoring

The screenshot shows the Elasticsearch Monitoring interface within the Kibana application. The left sidebar has a red box around the 'Monitoring' tab. The main area displays a summary of cluster health and statistics. A red box highlights the 'Overview' section, which includes:

Nodes: 1	Indices: 66
FS: 4.6GB / 112GB	Doc Count: 674,715
	Min. Shard Replication: 0
	Total Shards: 294
	Data Store: 346MB

Below this, a message states: "Your Trial license will expire on August 17, 2016." To the right, there is another panel for Kibana with green status indicators.

# Monitoring (Overview)



# Monitoring (indices)

Safari File Edit View History Bookmarks Develop Window Help

localhost

Clusters / elasticsearch / Elasticsearch

Overview Indices Nodes

Cluster: Yellow⚠️ Nodes: 1 Indices: 66 Memory: 225MB / 2GB Total Shards: 587 Unassigned Shards: 293 Documents: 674,860 Data: 347MB Uptime: 3 hours Version: 5.0.0-alpha4

Indices Filter Indices 20 of 66

Name	Document Count	Data	Index Rate	Search Rate	Unassigned Shards
.kibana	11	30.8 KB	0/s	0.47/s	1
_monitoring-data-2	5	15.4 KB	0.27/s	0/s	1
_monitoring-es-2-2016.07.14	122	368.4 KB	0/s	0/s	1
_monitoring-es-2-2016.07.17	18k	4.8 MB	0/s	0/s	1
_monitoring-es-2-2016.07.18	359.9k	143.9 MB	65.9/s	0/s	1
_monitoring-kibana-2-2016.07.14	5	66.7 KB	0/s	0/s	1
_monitoring-kibana-2-2016.07.17	63	143.7 KB	0/s	0/s	1
_monitoring_kibana_2-2016.07.18	1.4k	745.3 KB	0.07/s	0/s	1
_security	2	12.8 KB	0/s	0.17/s	0
odlog-1970.01.03	1	12.0 KB	0/s	0/s	5
odlog-2015.01.04	2	23.5 KB	0/s	0/s	5
odlog-2015.01.11	3	34.8 KB	0/s	0/s	5
odlog-2015.01.23	3	34.5 KB	0/s	0/s	5
odlog-2015.01.25	1	12.1 KB	0/s	0/s	5
odlog-2015.02.01	1	12.1 KB	0/s	0/s	5
odlog-2015.02.03	2	23.5 KB	0/s	0/s	5
odlog-2015.02.05	1	12.1 KB	0/s	0/s	5
odlog-2015.02.07	4	35.8 KB	0/s	0/s	5
odlog-2015.02.09	17	55.4 KB	0/s	0/s	5
odlog-2015.02.13	45	96.3 KB	0/s	0/s	5

# Monitoring (Nodes)

The screenshot shows the Elasticsearch Monitoring interface for the 'Nodes' tab. The browser title bar reads 'Monitoring - elasticsearch - Elasticsearch'. The main content area displays cluster statistics and a table of nodes.

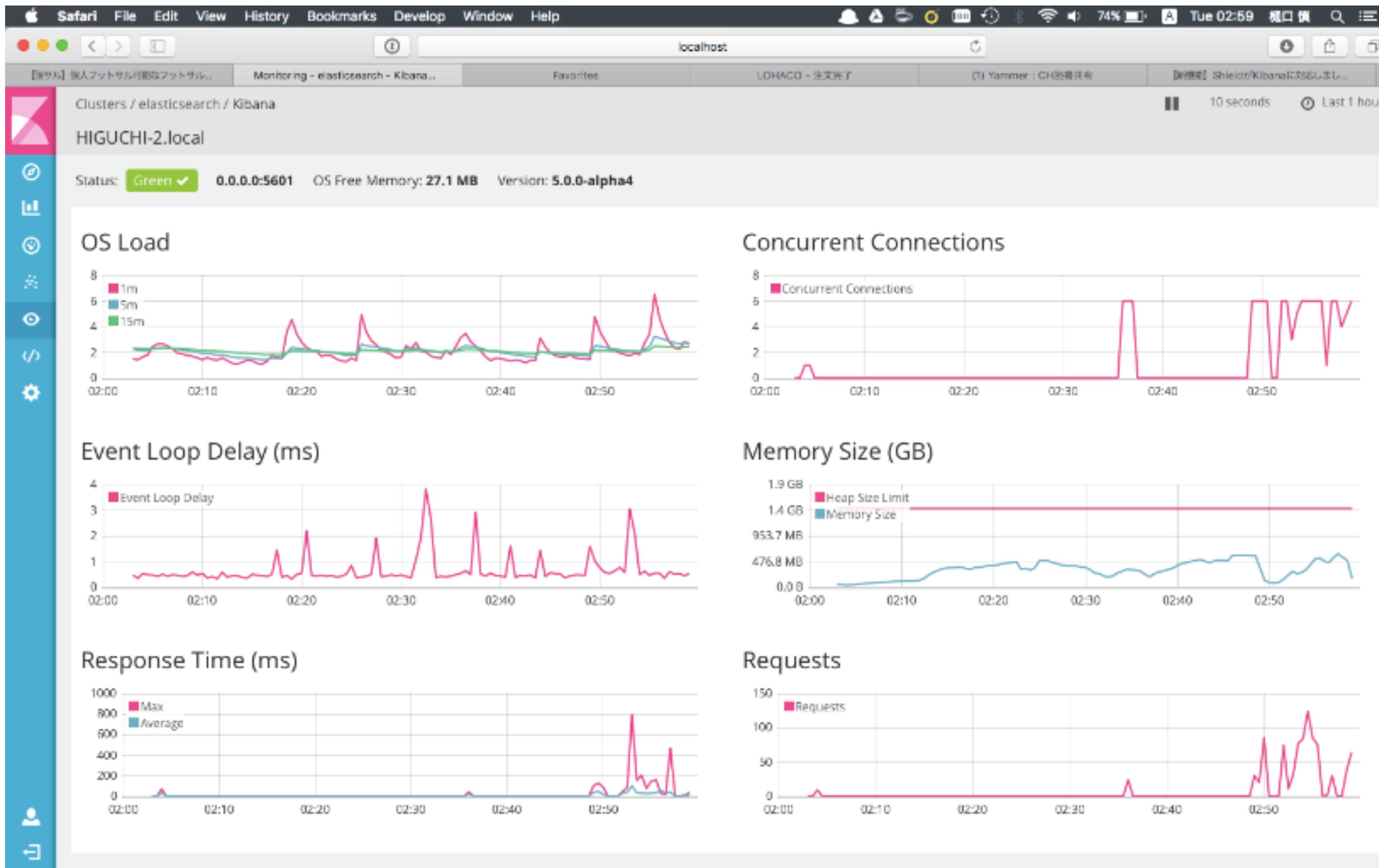
**Cluster Statistics:**

- Cluster: Yellow (warning icon)
- Nodes: 1
- Indices: 66
- Memory: 206MB / 2GB
- Total Shards: 587
- Unassigned Shards: 293
- Documents: 675,520
- Data: 346MB
- Uptime: 3 hours
- Version: 5.0.0-alpha4

**Nodes Table:**

Name	Status	CPU Usage	JVM Memory	Load Average	Disk Free Space	Shards
★ Blackheath 127.0.0.1:9300	Online ✓	3.33% ↓ 9% max 1% min	9.67% ↓ 11% max 7.67% min	2.32 ↓ 5.99 max 1.07 min	4.6 GB ↓ 4.8 GB max 4.6 GB min	294

# Monitoring (Kibana)



# X-Packのその他機能

# Watcher

# Watcherとは

---

1. クエリを登録し、条件に当てはまった場合に、通知を行う。

(例)

- 一定時間内に、特定の**URL**に大量にアクセスがあった。
- **CPU**使用率が閾値を超えた。
- 特定の商品に在庫ができた。

2. 通知方法

- メール送信
- 外部**API**の実行
- ログ出力

など

# Watcher、Monitoringとの組み合わせ

---

- **Watcher、Monitoring**を組み合わせると以下のことが実現できる。
  - クラスタのチェック  
直近**60**秒以内にクラスタの状態が**red**になつたらメールを送る。
  - メモリ使用量のチェック  
平均ヒープ使用量が**75%**以上になつたらメールを送る。
  - クラスタの構成チェック  
クラスタにノードが追加・削除されたらメールを送る。

## 1. Logstash → Elasticsearch → Kibana

を使って、簡単なデータ分析を体験した。

## 2. 拡張機能(X-pack)の一部を体験した。

→ 身近なデータを使って、実際に分析・検索を試してみてください。

# We're hiring!

---



---

ご清聴ありがとうございました。



*Acroquest Technology*

*Infrastructures Evolution*