

ハンズオンの前に(1/3)

- 本日使用するスライドおよびデータを取得してください

1. jjug_2017_fall.pdf

2. work.zip

- github → <https://github.com/higu0shin/JJUG-CCC-fall-2017>
- USBメモリ(貸し出しますのでお声かけください)
のいずれか取得してください。

ハンズオンの前に(2/3)

- 下記の3点をダウンロードして解凍する

1. elasticsearch

2. kibana

3. logstash

※3点とも、配布しているworkフォルダの直下に解凍してください

- 公式サイト → <https://www.elastic.co/downloads>

- USBメモリ(貸し出しますのでお声かけください)

のいずれかから媒体入手してください。

ハンズオンの前に(3/3)

- それぞれに拡張プラグイン(X-Pack)をインストールする

1. それぞれ解凍したフォルダの下で

"bin/elasticsearch-plugin install x-pack" を実行する

※下線部を "kibana", "logstash" で置き換えてそれぞれ実行する。

2. インターネットに繋がらない場合は、

下記のコマンドでオフラインインストールを実施する

"bin/elasticsearch-plugin install x-pack file:///path/to/x-pack-6.0.0.zip"

Elastic6.0ハンズオン

2017/11/18

#jjug_ccc #ccc_i3

自己紹介

名前：樋口 慎（Acroquest Technology@新横浜）

業務：データ分析・検索基盤などの開発や構築支援

Twitter：@shin0higuchi

コンテンツ

- 概要説明
- データの投入
- ダッシュボードの作成
- Machine Learning
- まとめ

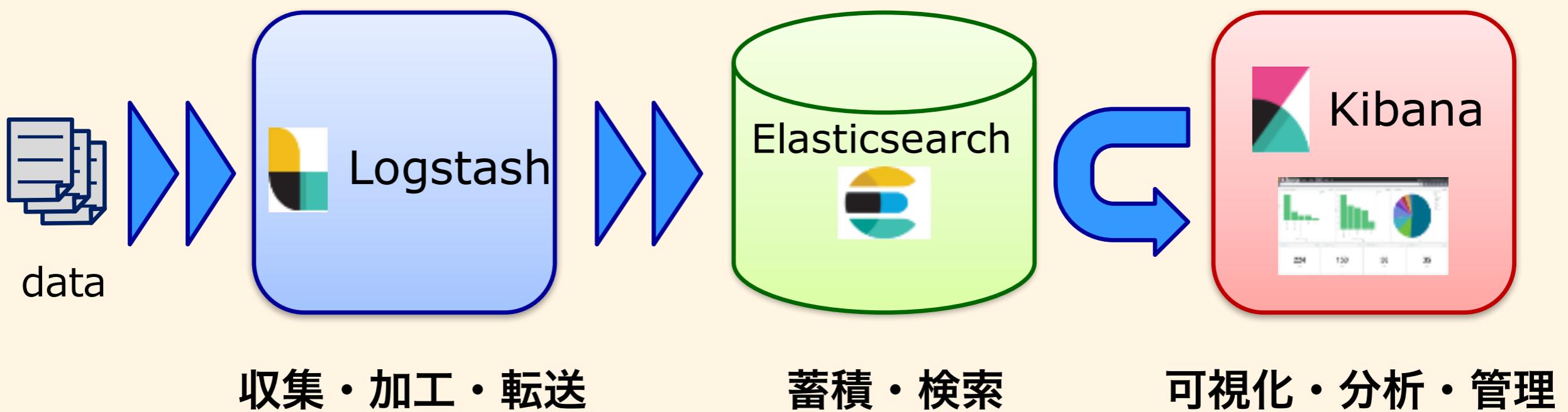
コンテンツ

- 概要説明 ←
- データの投入
- ダッシュボードの作成
- Machine Learning
- まとめ

概要説明

- Elasticsearchとは?
 - ドキュメント指向の全文検索エンジン
 - スケーラビリティが高い
→高速な検索が可能なため、データ分析などにも活用されている

概要說明



コンテンツ

- 概要説明
- データの投入 ←
- ダッシュボードの作成
- Machine Learning
- まとめ

データ投入の流れ

1.elasticsearch・kibanaの起動

2.indexの設定(mapping)

3.logstashによるデータ投入

Elasticsearchの起動

- 下記のコマンドでelasticsearchを起動する

```
$ bin/elasticsearch
```

```
$ bin\elasticsearch.bat
```

- パスワードを生成する

別ウィンドウorタブを開いて実行

```
$ bin/x-pack/setup-passwords auto
```

*elastic,kibana,logstash_systemというユーザーのパスワードが表示されるので控えてお

<

*auto のかわりにinteractiveを使うと手動で設定できる

Kibanaの起動

- config/kibana.ymlを編集する
 - + elasticsearch.username: "kibana"
 - + elasticsearch.password: "生成されたパスワード"
- kibanaを起動する

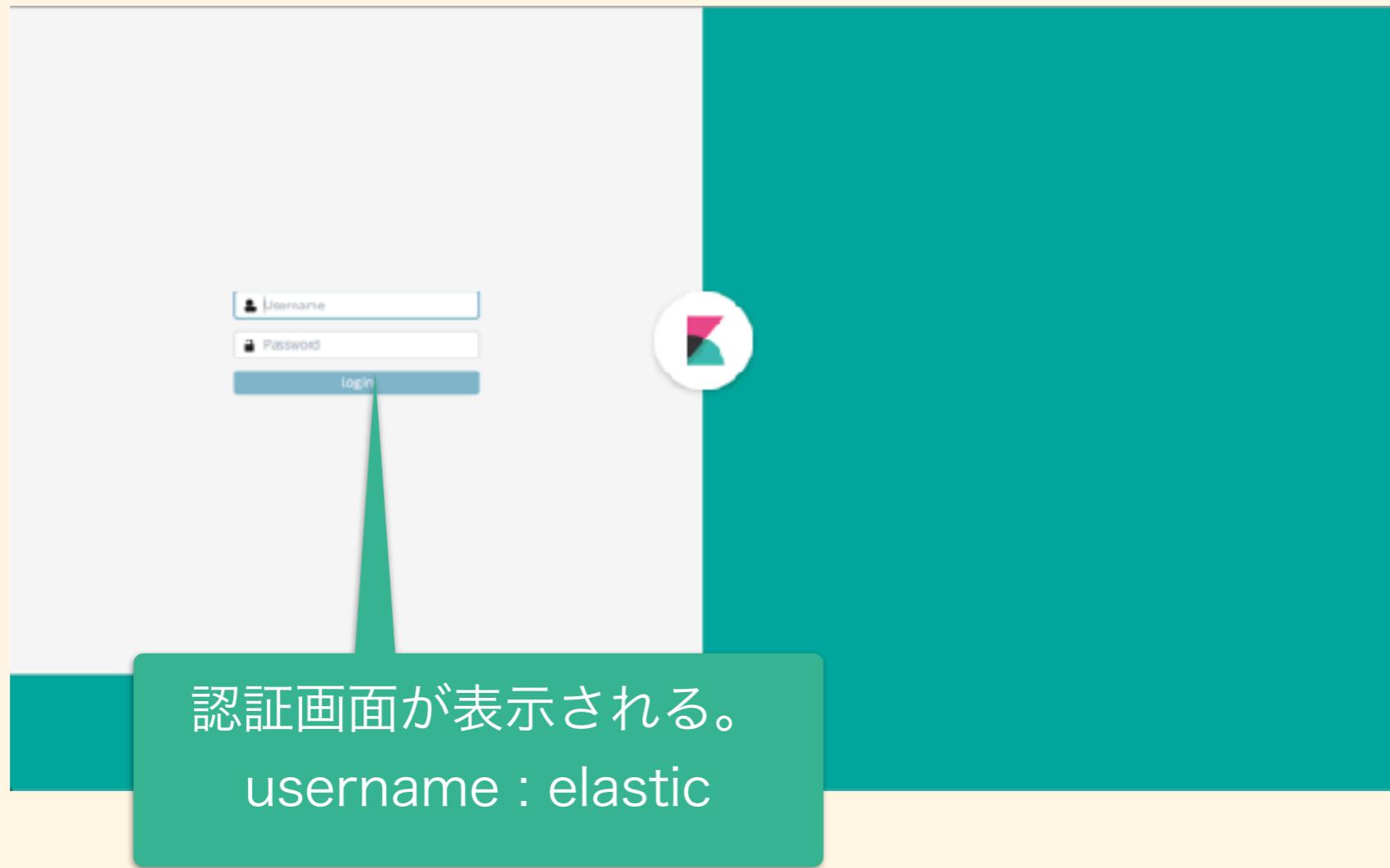
```
$ bin/kibana
```

```
$ bin\kibana.bat
```

Kibana・Elasticsearchの起動確認

認
心

- ・ ブラウザからlocalhost:5601にアクセスする



Mappingの設定

The screenshot shows the Kibana interface with the Dev Tools tab selected. In the Dev Tools console, a JSON configuration for a template is pasted:

```
PUT _template/server-metrics
{
  "index_patterns": "server-*",
  "settings": {
    "number_of_shards": 1,
    "number_of_replicas": 0
  },
  "mappings": {
    "metric": {
      "properties": {
        "@timestamp": {
          "type": "date"
        },
        "accept": {
          "type": "long"
        },
        "deny": {
          "type": "long"
        },
        "host": {
          "type": "keyword"
        },
        "response": {
          "type": "float"
        },
        "service": {
          "type": "keyword"
        },
        "total": {
          "type": "long"
        }
      }
    }
}
```

A green callout box with the number 1 points to the 'Dev Tools' button in the sidebar. A green callout box with the number 2 points to the text 'mapping.txt の内容を貼り付ける'.

1. DevToolsを選ぶ

2. mapping.txt の
内容を貼り付ける

Mappingの設定

The screenshot shows the Kibana interface with the 'Console' tab selected. A code editor window displays a PUT request to '_template/server-metrics' with the following JSON payload:

```
1 PUT _template/server-metrics
2 {
3   "index_patterns": "server-*",
4   "settings": {
5     "number_of_shards": 1,
6     "number_of_replicas": 0
7   },
8   "mappings": {
9     "metric": {
10       "properties": {
11         "@timestamp": {
12           "type": "date"
13         },
14         "accept": {
15           "type": "long"
16         }
17       }
18     }
19   }
20 }
```

A red box highlights the green 'Run' button icon at the top right of the code editor. A callout bubble with a green background and white text says '1. クリックして実行' (Click to execute). To the right, the response pane shows the JSON result of the request:

```
1 {
2   "acknowledged": true
3 }
```

A callout bubble with a green background and white text says '2. {"acknowledged":true} と表示されればOK' (If it displays {"acknowledged":true}, it's OK).

Logstashの設定・実行

- config/logstash.ymlを編集する
 - + xpack.monitoring.elasticsearch.url: ["localhost:9200"]
 - + xpack.monitoring.elasticsearch.username: "logstash_system"
 - + xpack.monitoring.elasticsearch.password: "**changeme**"

自分の環境で設定した、
logstash_systemユーザー
のパスワード

Logstashの設定・実行

- server_metrics.confを編集する(input)

```
input{  
    file{  
        path => "/Users/SHIN/jjug_2017_fall/work/server_metrics/*"  
        start_position => "beginning"  
        since_db_path => "/dev/null" ←Windowsの方は "nul"に書き換える  
    }  
}
```

Logstashの設定・実行

- server_metrics.confを編集する(output)

```
output{
  stdout{省略}

  elasticsearch{
    hosts => "localhost:9200"
    user => "elastic"
    password => 'P6kHQ$&sj-Aoo^pj1B16'
    index => "server-metrics"
    document_type => "metric"
  }
}
```

自分の環境で設定した、
elasticユーザーのパスワード

Logstashの設定・実行

- 下記のコマンドでlogstashを実行

```
$ bin/logstash -f ..\server_metrics.conf
```

```
$ bin\logstash.bat -f ..\server_metrics.conf
```

※実行するとドットが多数出力されます

index patternの作成

The screenshot shows the Kibana Management interface. A green arrow points from the top-left towards the 'Index Patterns' link in the 'Kibana' section. A green callout box labeled '1. Management' is positioned above the main navigation bar. Another green callout box labeled '2. Index Patterns' is positioned below the 'Index Patterns' link.

Management

Version: 6.0.0-rc2

Security

Users Roles

Elast Watcher

Kibana

Index Patterns Saved Objects Reporting Advanced Settings

Logstash

Pipelines

index patternの作成

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.
run search and analysis

server-*

Index pattern advanced options

server-*

Patterns allow you to define dynamic index names using * as a wildcard. Examples

Time Filter field name i refresh fields

@timestamp

Create

@timestamp

The screenshot shows the Kibana Management interface. On the left is a sidebar with icons for Discover, Visualize, Dashboard, Timelion, Machine Learning, Graph, Dev Tools, Monitoring, and Management (which is selected). The main area has tabs for Index Patterns, Saved Objects, Reporting, and Advanced Settings. A warning message says 'No default index pattern. You must select or create one to continue.' Below it, a large green box highlights the 'server-*' input field in the 'Index pattern' section. Another green box highlights the '@timestamp' dropdown in the 'Time Filter field name' section. A green arrow points from the 'Create' button to the '@timestamp' dropdown.

logstash pipelines

- logstashのpipelineごとに、データの流れやスループットをKibana上で確認することができる。

logstash pipelines

The screenshot shows the Kibana interface with two main sections highlighted by green callout bubbles.

1. Monitoring (highlighted in a green bubble):

- Elasticsearch Overview:** Version: 6.0.0-rc2, Uptime: 21 hours, Jobs: 0.
- Nodes:** 1 (Disk Available: 19GB / 234GB (8.04%), JVM Heap: 28.41% (563MB / 2GB)).
- Indices:** 29 (Documents: 5,149,679, Disk Usage: 1GB, Primary Shards: 37, Replica Shards: 0).

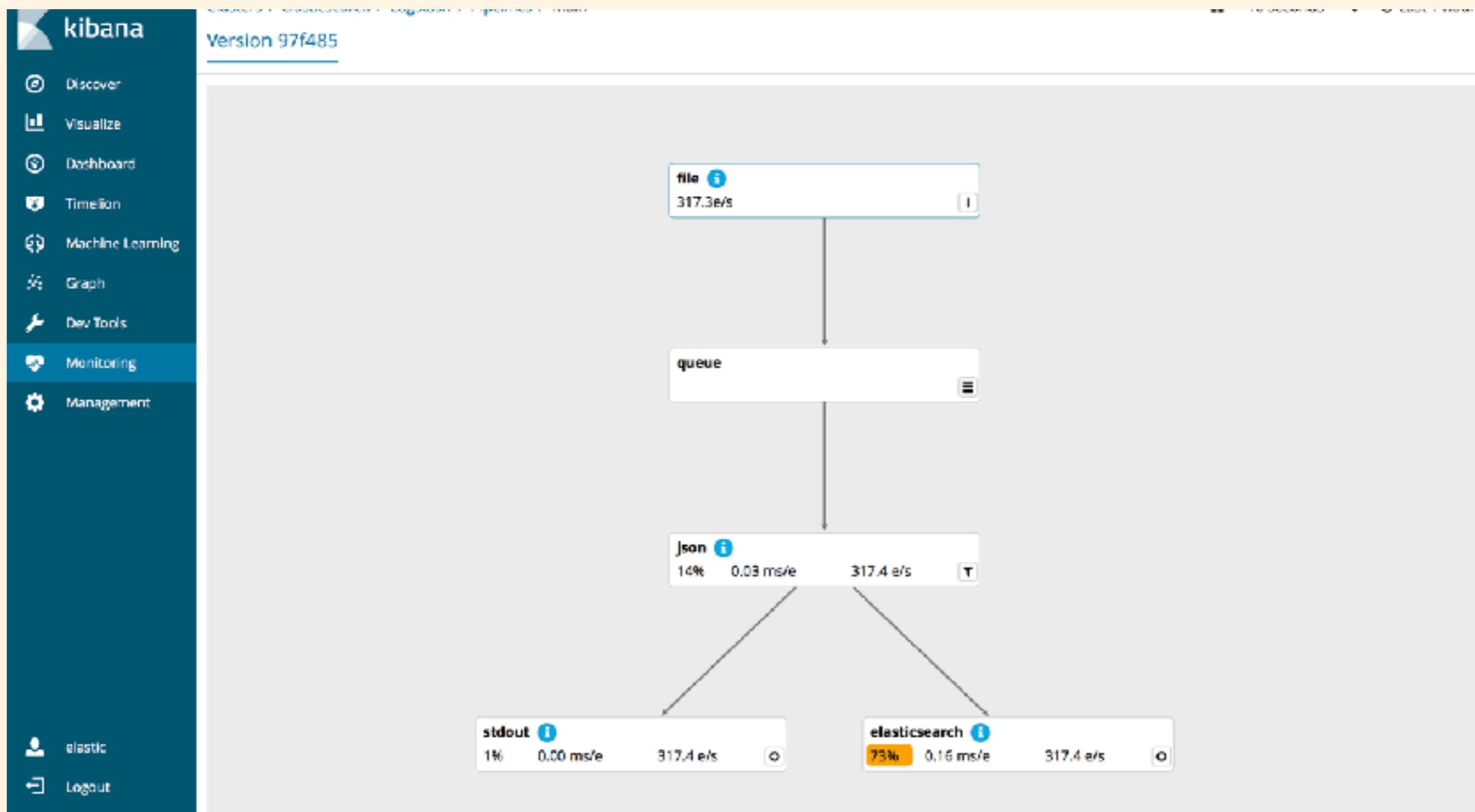
2. Pipelines (highlighted in a green bubble):

- Kibana Overview:** Requests: 1240, Max. Response Time: 865 ms.
- Logstash Overview:** Events Received: 121.6k, Events Emitted: 121.2k.
- Pipelines:** 1 (Nodes: 1, Uptime: 20 hours, JVM Heap: 28.66% (284MB / 990MB)).

The left sidebar includes links for Discover, Visualize, Dashboard, Timeline, Machine Learning, Graph, Dev Tools, Monitoring (which is selected), and Management. The bottom left corner shows the user is logged in as 'elastic'.

logstash pipelines

- logstash pipelineの状態が確認できる



コンテンツ

- 概要説明
- データの投入
- ダッシュボードの作成 ←
- Machine Learning
- まとめ

Dashboardのインポート

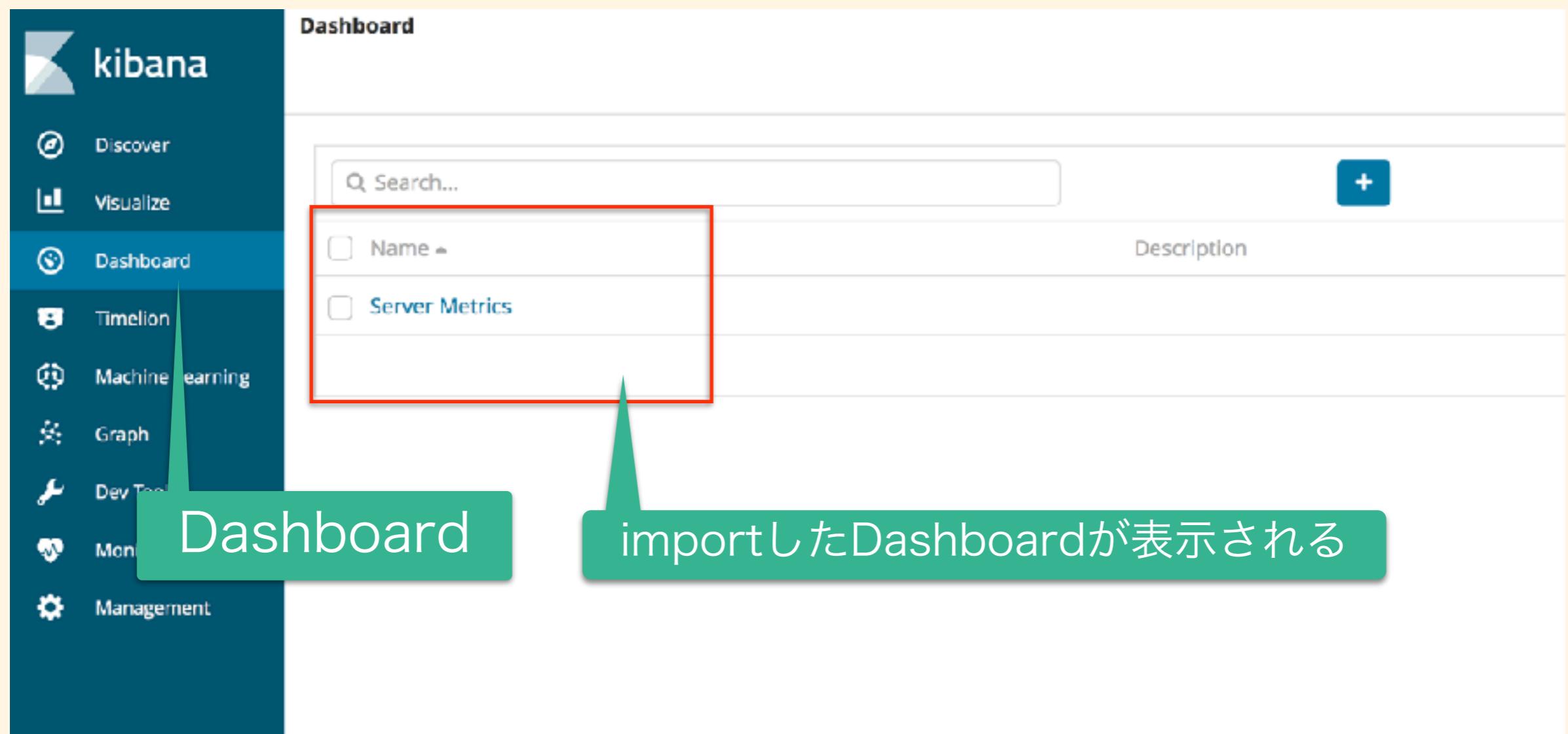
The screenshot shows the Kibana Management interface. On the left is a sidebar with icons for Discover, Visualize, Dashboard, Timelion, Machine Learning, Graph, Dev Tools, Monitoring, and Management. The Management icon is selected. The main area is titled 'Management' and shows the version '6.0.0-rc2'. It has sections for Security (with sub-links for Users and Roles), Elasticsearch, and Watcher. Below these is a 'Kibana' section with links for Index Patterns, Saved Objects, Reporting, Advanced Settings, Logstash, and Pipelines. A large green callout points to the 'Saved Objects' link, which is highlighted with a red border.

Saved Objects

Dashboardのインポート

The screenshot shows the Kibana Management interface. On the left is a sidebar with icons for Discover, Visualize, Dashboard, Timeline, Machine Learning, Graph, Dev Tools, Monitoring, and Management. The Management icon is selected and highlighted in blue. The main area has a header with tabs: Index Patterns, Saved Objects (which is underlined), Reporting, and Advanced Settings. Below the header is a section titled "Edit Saved Objects" with a sub-section "From here you can delete saved objects, such as saved searches. You can also edit the raw data of saved objects. Typically objects are only modified via their associated application, which is probably what you should use instead of this screen. Each tab is limited to 100 results. You can use the filter to find objects not in the default list." There are three tabs at the top of this section: Dashboards (0), Searches (0), and Visualizations (0). A search bar below the tabs contains the placeholder "Search...". To the right of the search bar are two buttons: "Delete" and "Export". At the top right of the main content area are two more buttons: "Export Everything" and "Import". A red box highlights the "Import" button. A green callout bubble points to the "Import" button with the text "Import → dashboard.jsonを選択する".

Dashboardのインポート



Dashboardのインポート



Dashboardの作成方法

- 1.Dashboardに配置するvisualizationを作成する
- 2.Dahboard画面からvisualizationを配置する

Visualizationの作成

The screenshot shows the Kibana interface with the 'Visualize' tab selected in the sidebar. The main area displays a list of pre-built visualization types under the heading 'Type'. A red box highlights four items: 'Average Response Time (per application)', 'Average Response vs. time', 'Total Request vs. time', and 'Total Requests (by application)'. A callout bubble points to the '+ Type' button in the top right corner, which is also highlighted with a red box. Another callout bubble at the bottom points to the list of visualizations.

新規に作成する場合は
「+」をクリック

作成済みのvisualizationが表示される

Name	Type
Average Response Time (per application)	Visual Builder
Average Response vs. time	Visual Builder
Total Request vs. time	Visual Builder
Total Requests (by application)	Visual Builder

Visualizationの作成

The screenshot shows the Kibana interface for selecting a visualization type. On the left is a dark sidebar with icons and labels: Discover, Visualize (selected), Dashboard, Timeline, Machine Learning, Graph, Dev Tools, Monitoring, and Management. At the bottom are elastic, Logout, and Collection buttons.

The main area has a title "Select visualization type" and a search bar "Search visualization types...". It is divided into several sections:

- Basic Charts**: Area, Heat Map, Horizontal Bar, Line (highlighted with a green box), Pie, Vertical Bar.
- Data**: Data Table, Gauge, Goal, Metric (highlighted with a green box).
- Maps**: Coordinate Map, Region Map.
- Time Series**: Timeline, Visual Builder.

A green callout box points to the "Line" icon in the Basic Charts section, containing the text "Visualizationの種類を選択する(Line)".

Visualizationの作成

Visualize / New / Choose search source

From a New Search, Select Index

Or, From a Saved Search

Filter... 1 of 1

Saved Searches Filter... 0-0 of 0 Manage saved searches

Name

server-*

No matching saved searches found.

index patternを選択する(server-*)

Visualizationの作成

The screenshot shows the Kibana interface for creating a new visualization. On the left is a sidebar with icons for Discover, Visualize, Dashboard, Timeline, Machine Learning, Graph, Dev Tools, Monitoring, and Management. The 'Visualize' icon is selected. The main area has a title bar with 'Visualize / New Visualization (unsaved)' and a search bar. Below the search bar is a red box labeled 'Search... (e.g. status:200 AND extension:PHP)'. To the right of the search bar is a button 'Add a Filter' and a link 'Uses lucene query syntax'. The main content area shows a histogram titled 'server-*' with a Y-axis for 'Count' ranging from 0 to 200,000. A green callout box points to the histogram area with the text 'visualizationが表示される'. On the left side of the main area, there are two red boxes: one pointing to the 'Metrics' section with the text '集計方法の設定' (Aggregation method settings), and another pointing to the 'Buckets' section with the text 'データの絞り込み条件などを設定できる' (Set filtering conditions for data). The 'Metrics' section includes tabs for 'Data', 'Metrics & Axes', and 'Panel Settings', and a 'Metrics' panel with a 'Y-Axis' tab and a 'Add metrics' button. The 'Buckets' section includes tabs for 'X-Axis', 'Split Series', and 'Split Chart', and a 'Cancel' button.

Save Share Refresh Reporting ⌘ April 6th 2017, 09:03:24.237 to April 12th 2017, 23:19:26.889 ⌘

Uses lucene query syntax

server-*

Metrics

Y-Axis

Add metrics

Buckets

Select buckets type

X-Axis

Cancel

Count

Count

0 20,000 40,000 60,000 80,000 100,000 120,000 140,000 200,000

集計方法の設定

データの絞り込み条件などを設定できる

visualizationが表示される

Visualizationの作成

server*

Data Metrics & Axes Panel Settings

Metrics

Y-Axis

Aggregation

Select an aggregation

Metric Aggregations

Average

Count

Max

Median

Min

Percentile Ranks

Percentiles

X-Axis

Split Series

Split Chart

Cancel

y軸の集計方法
(Aggregation)設定

200,000
180,000
160,000
140,000
120,000
50,000
60,000
40,000

This screenshot shows the configuration interface for creating a visualization. The left sidebar contains tabs for 'Data', 'Metrics & Axes', and 'Panel Settings'. The 'Metrics' tab is active, showing a 'Metrics' panel with sections for 'Y-Axis' and 'Aggregation'. A red box highlights the 'Aggregation' section, which includes a dropdown menu titled 'Select an aggregation' with options like 'Metric Aggregations', 'Average', 'Count', 'Max', 'Median', 'Min', 'Percentile Ranks', and 'Percentiles'. A green callout points to the 'Count' option in this dropdown. Below the 'Metrics' panel is an empty chart area with axes ranging from 40,000 to 200,000. The bottom of the interface features buttons for 'Cancel'.

Visualizationの作成

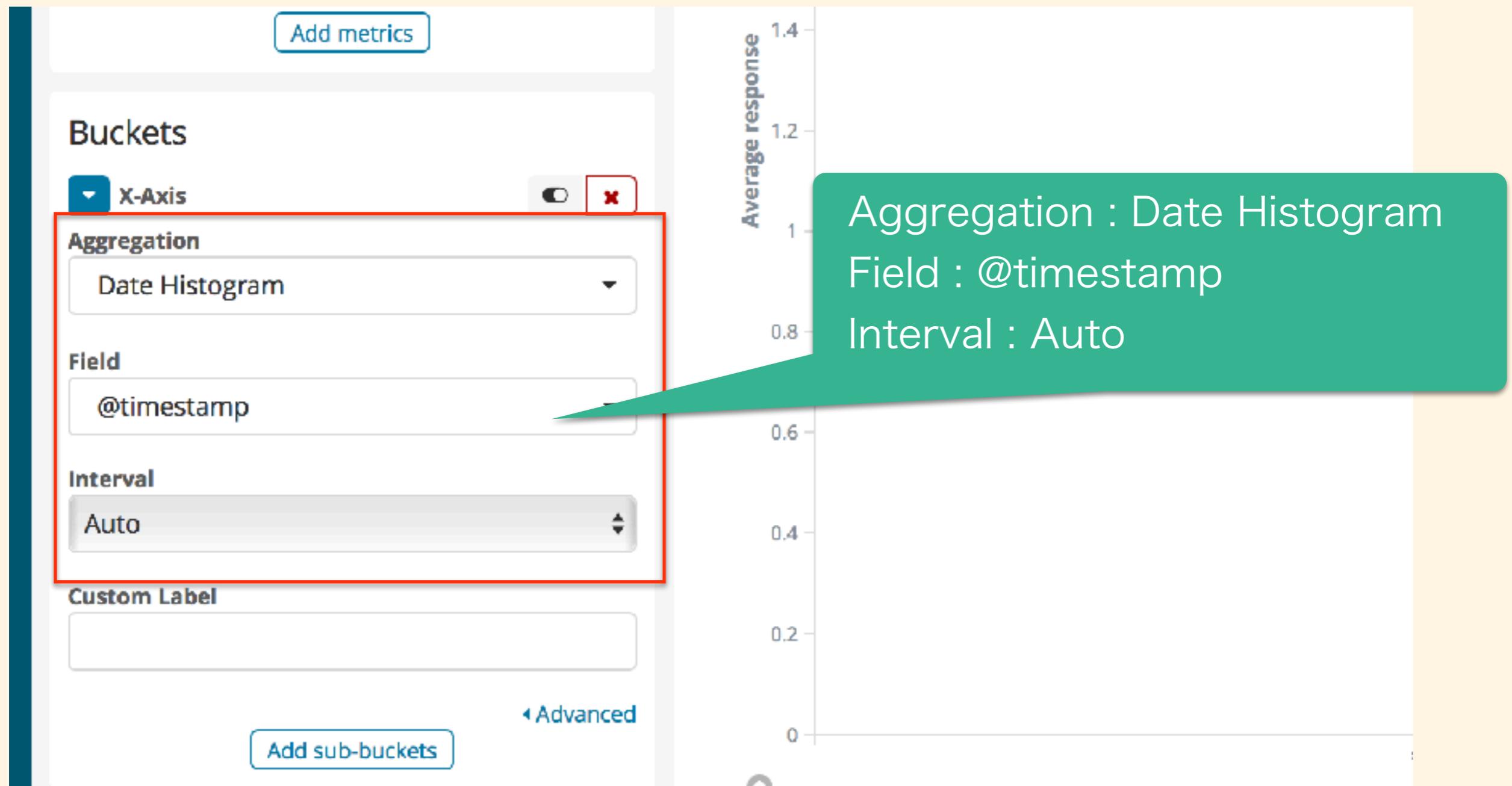
The screenshot shows the Grafana interface for creating a visualization. On the left, there's a sidebar with a 'Metrics' section and a 'Buckets' section. The main area is titled 'server-*' and contains a 'Data' tab, 'Metrics & Axes' tab, and 'Panel Settings' tab. Under the 'Data' tab, there's a 'Metrics' section with a 'Y-Axis' dropdown set to 'response'. This dropdown is highlighted with a red box. Below it is an 'Aggregation' dropdown set to 'Average', also highlighted with a red box. A green callout box points to these settings with the text 'Aggregation : Average' and 'Field : response'. At the top right of the configuration area is a 'Apply changes' button, which is also highlighted with a red box. A green callout box points to this button with the text '変更を反映' (Reflect changes). To the right of the configuration area is a chart showing a single data series with values ranging from 80,000 to 200,000.

Visualizationの作成

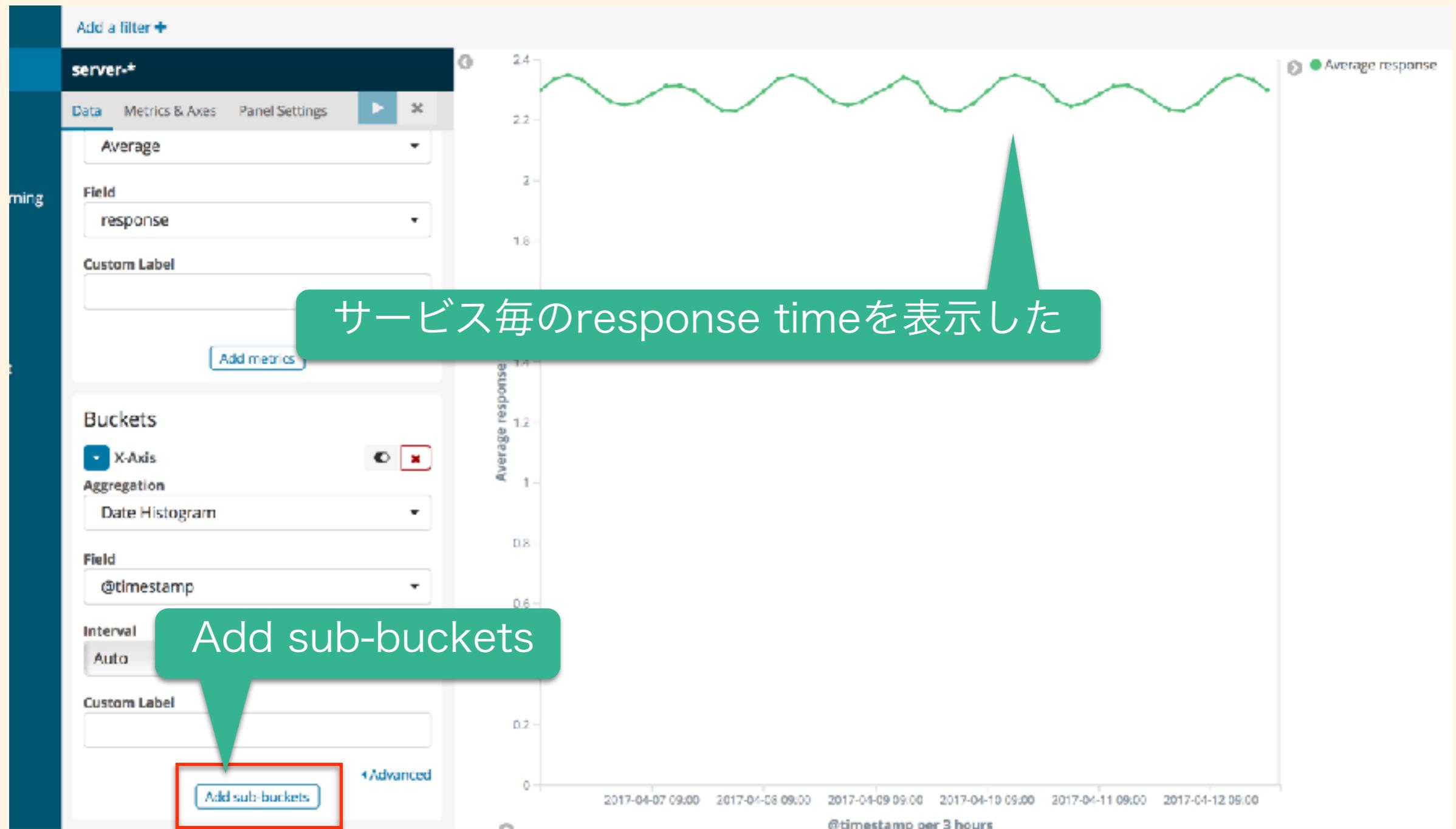
The screenshot shows the Grafana interface for creating a visualization. On the left, there's a sidebar with a 'Metrics' section containing 'Y-Axis' (set to 'Average' for 'response'), 'Field' (set to 'response'), and 'Custom Label'. Below it is a 'Buckets' section with a dropdown menu. A red box highlights the 'X-Axis' option in this menu. A green callout box with white text points to this 'X-Axis' option, instructing the user to select it and set up the X-axis configuration. The main area of the screen displays a chart with a single data series.

"X-Axis" を選択し、
x軸の設定をする

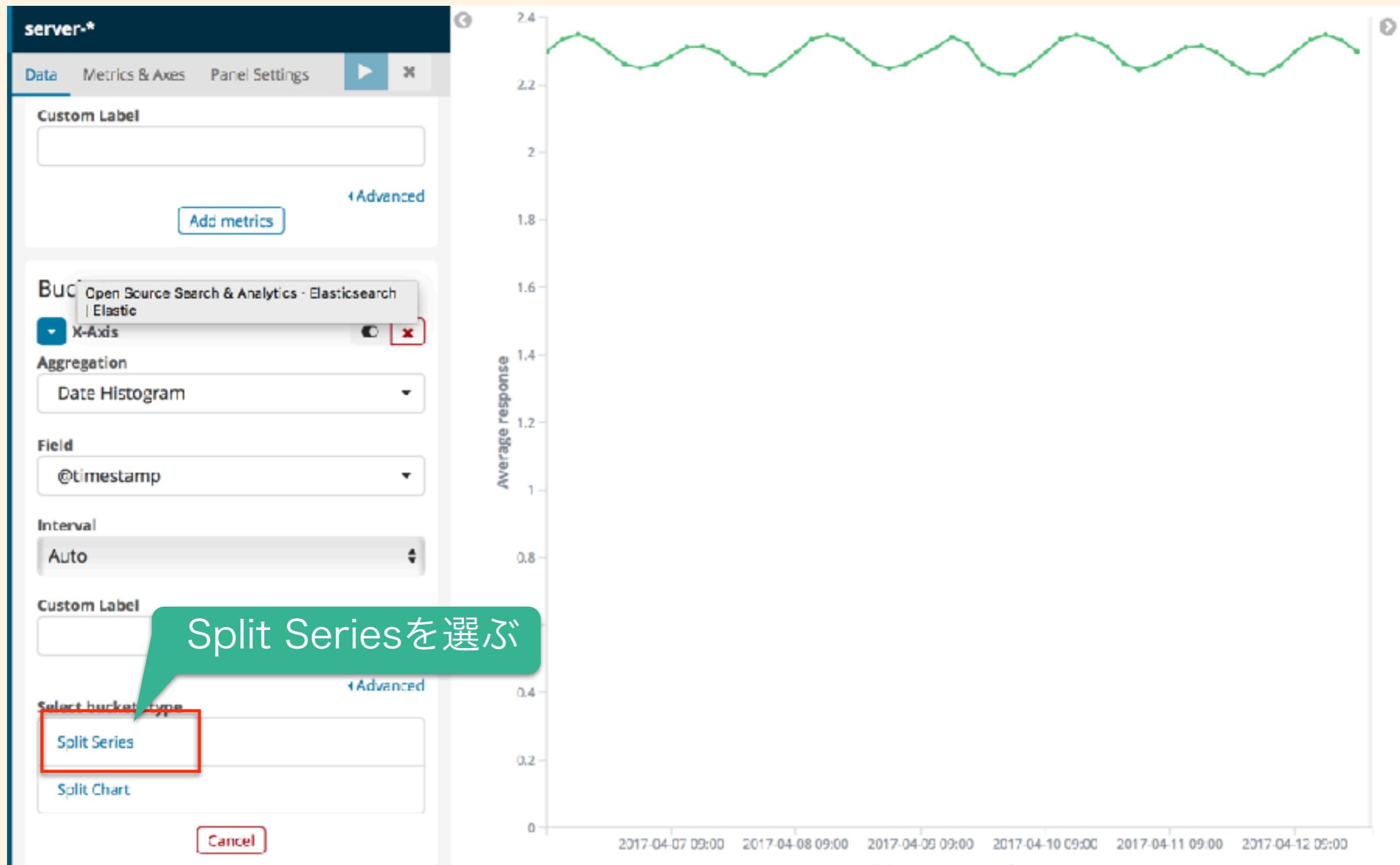
Visualizationの作成



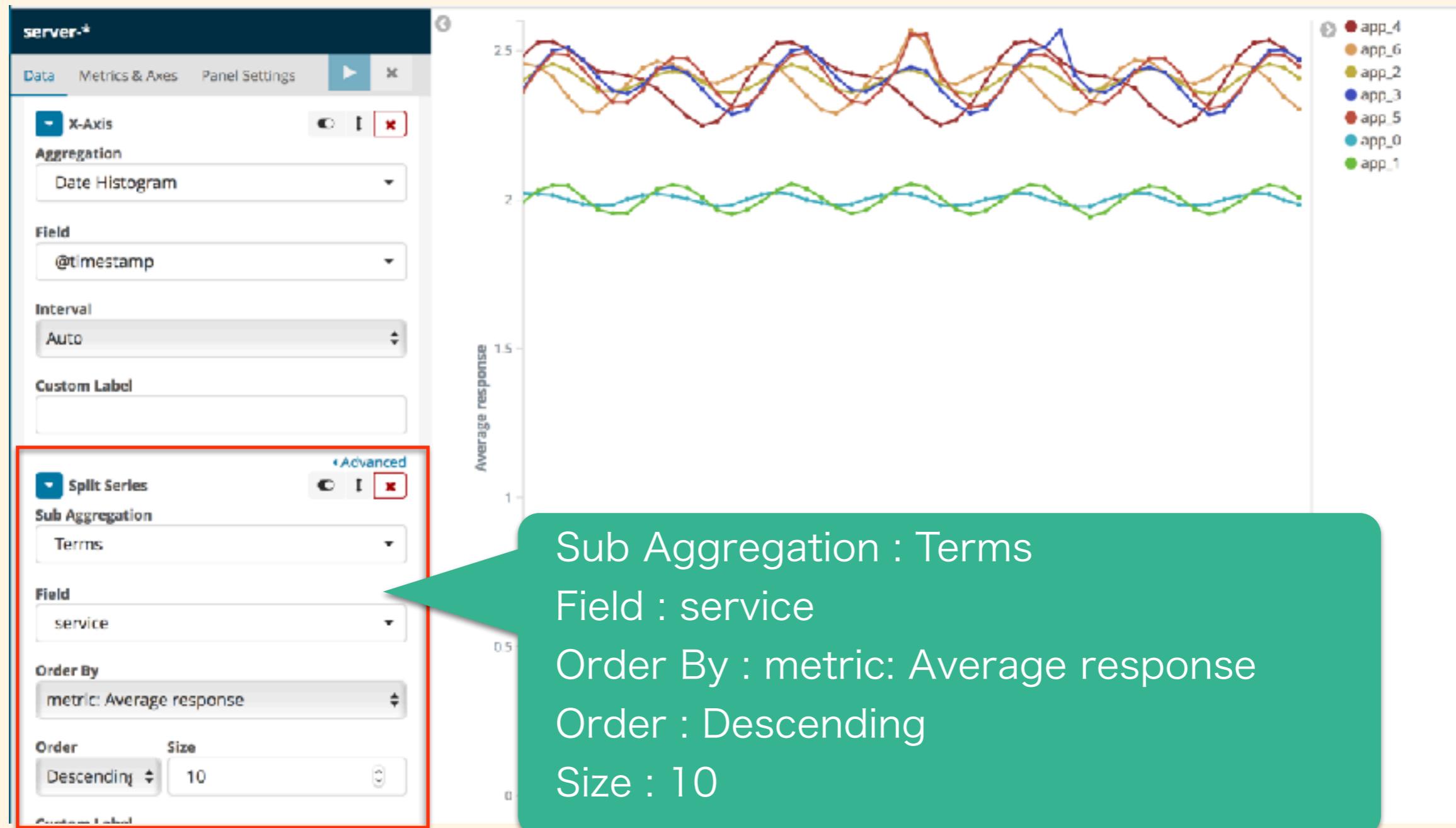
Visualizationの作成



Visualizationの作成



Visualizationの作成



Visualizationの作成

The screenshot shows the Kibana interface for creating a visualization. On the left, a sidebar menu includes options like Discover, Visualize (which is selected), Dashboard, Timelion, Machine Learning, Graph, Dev Tools, Monitoring, and Management. The main area is titled "Visualize / サービス別レスポンスタイム (unsaved)". It features a search bar, a "Save Visualization" section with a "Save" button, and a "Add a filter" button. A modal window titled "server-*" is open, showing configuration for the X-axis (Date Histogram, @timestamp, Auto interval) and Sub Aggregation (Terms). To the right is a line chart titled "Average response" showing multiple colored lines over time. A red box highlights the "Save" button at the top right of the visualization header, and a green callout bubble points to it with the text "作成したvisualizationを保存する".

作成したvisualizationを保存する

Dashboardの作成

kibana

Discover Visualize Dashboard Timelion Machine Learning Graph Dev Tools Monitoring Management

Dashboard / Server Metrics Full screen Share Clone **Edit** Reporting ⌂ March 24th 2017, 10:58:51.018 to April 23rd 2017, 05:46:08.734 Uses lucene query syntax

Total Request vs. time

Average Response vs. time

Total Requests (by application)

Dashboardを編集モードにする

app_0 app_1 app_2 app_3 app_4 app_5 app_6

Dashboardの作成

The screenshot shows the Kibana interface for creating a dashboard titled "Editing Server Metrics (unsaved)". The top navigation bar includes "Save", "Cancel", "Add", "Options", "Share", and "Reporting". A red box highlights the "Add" button. Below it is a search bar labeled "Visualizations Filter..." and a list of visualization names. A green callout bubble with the text "1. Addをクリックする" points to the "Add" button. Another green callout bubble with the text "2. 追加したいvisualization名をクリックする" points to the "サービス別レスポンスタイム" visualization name, which is also highlighted with a red box. The bottom section displays a line chart titled "Total Request vs. time" showing request counts over time, with a legend indicating "Total requests: 16,518,453". The left sidebar lists various Kibana features: Discover, Visualize, Dashboard (which is selected and highlighted in blue), Timeline, Machine Learning, Graph, Dev Tools, Monitoring, and Management.

1. Addをクリックする

2. 追加したいvisualization名をクリックする

Dashboard / Editing Server Metrics (unsaved)

Save Cancel Add Options Share Reporting ⏪ ⏴ March 30th 2017, 19:15:16.363 to April 4th 2017, 08:43:38.181 ⏵

Add Panels

Visualization Saved Search

Q Visualizations Filter... 1-5 of 5 Add new Visualization

Name ↗

- Average Response Time (per application)
- Average Response vs. time
- Total Request vs. time
- Total Requests (by application)
- サービス別レスポンスタイム

Uses lucene query syntax

Total Request vs. time

25,000,000
20,000,000
15,000,000
10,000,000
5,000,000

Mar 31 00:00 Mar 31 12:00 Apr 01 00:00 Apr 01 12:00 Apr 02 00:00 Apr 02 12:00 Apr 03 00:00 Apr 03 12:00 Apr 04 00:00

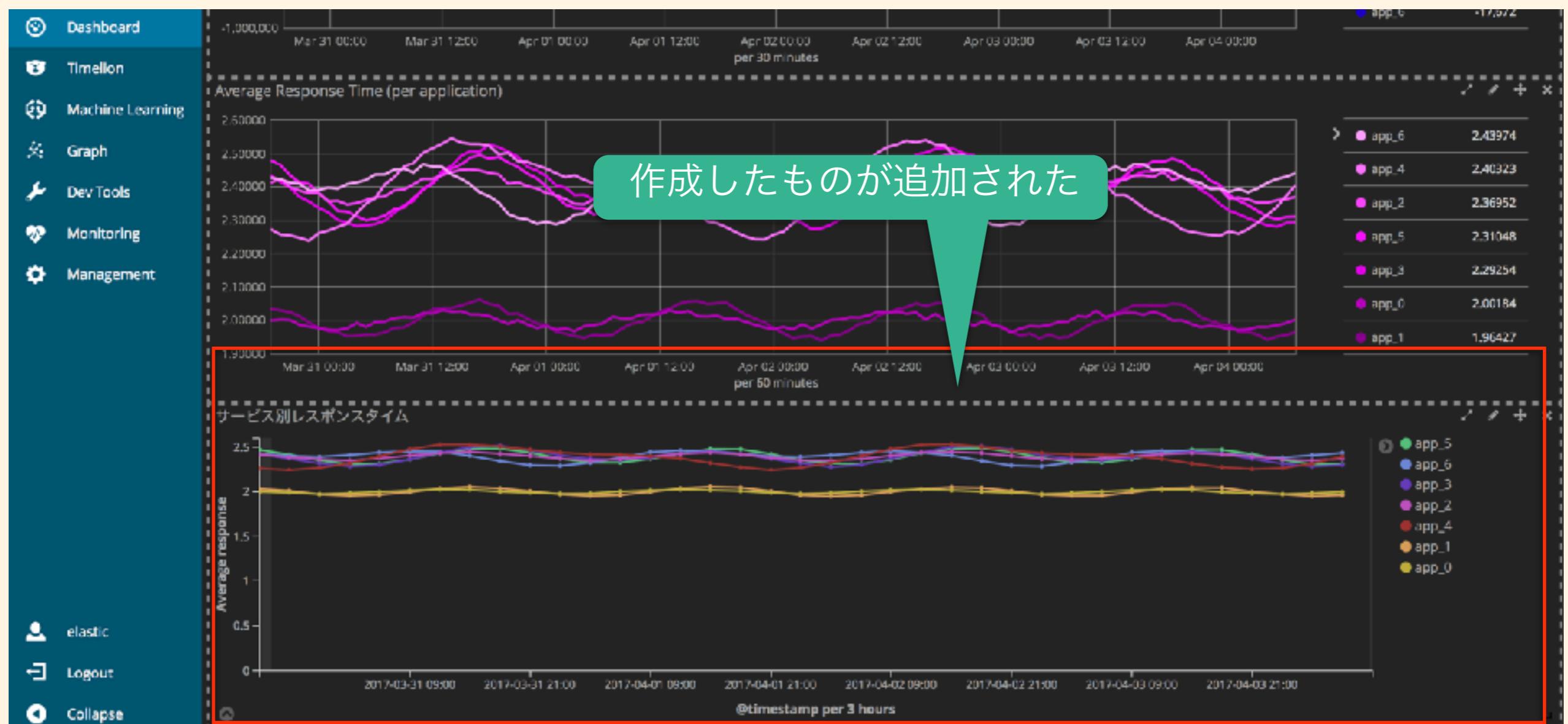
per 30 minutes

Total requests: 16,518,453

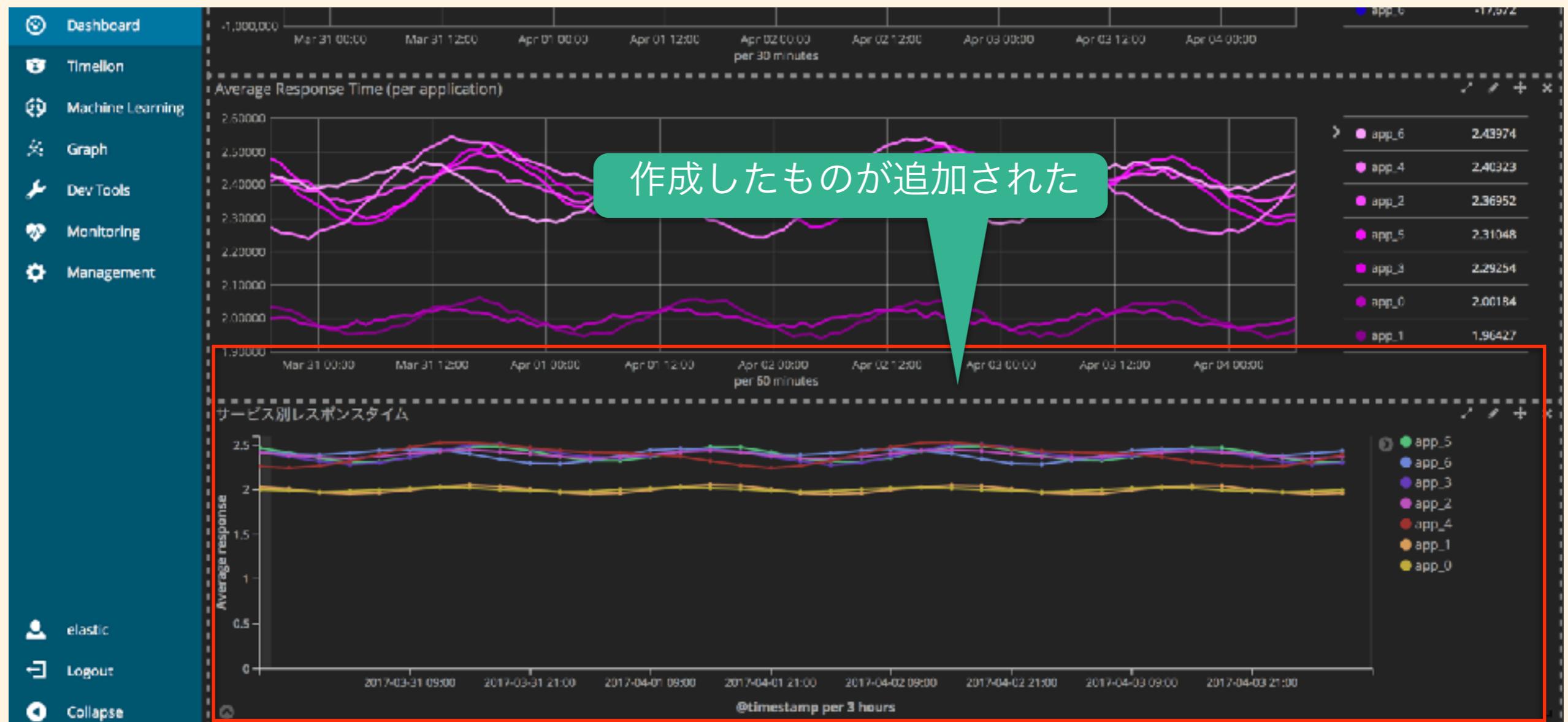
Average Response vs. time

elastic

Dashboardの作成



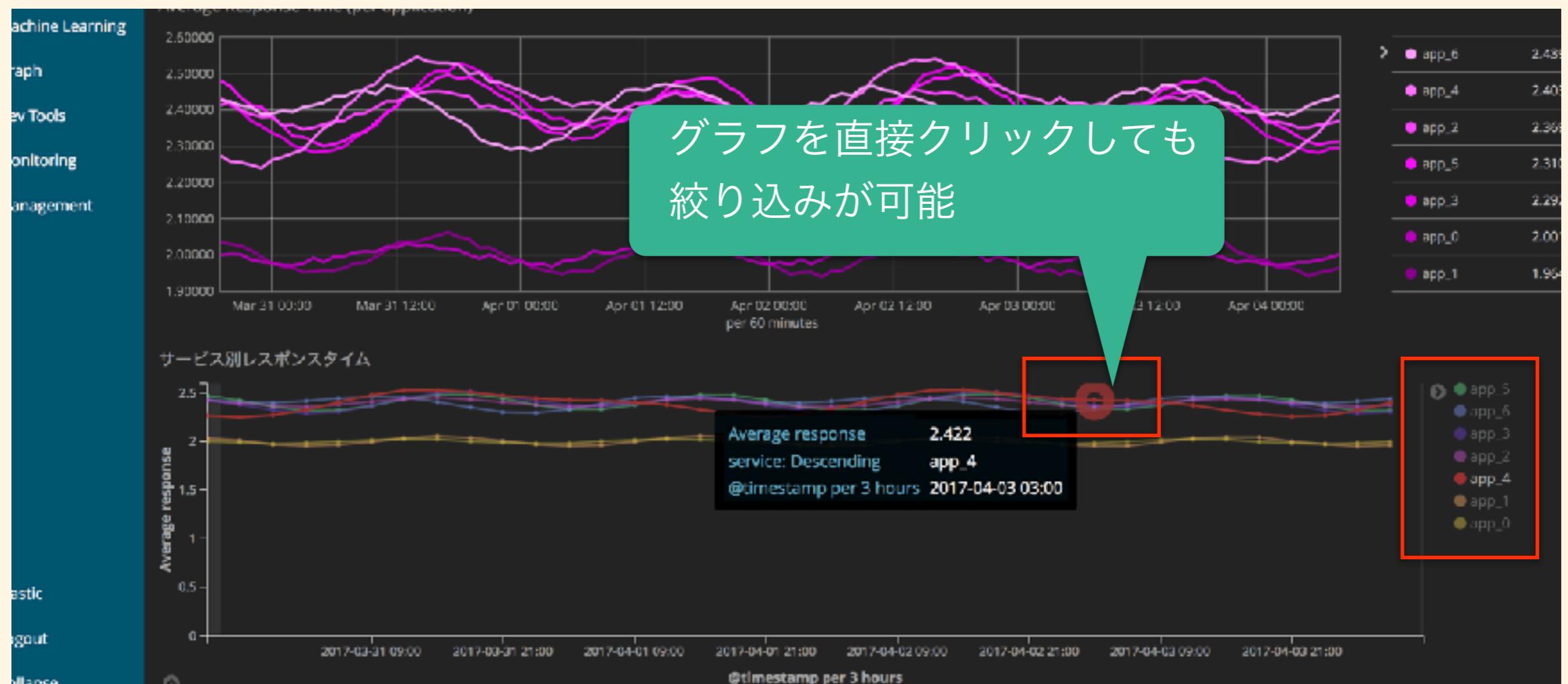
Dashboardの操作



Dashboardの操作

The screenshot shows the Kibana interface for a 'Server Metrics' dashboard. On the left, a sidebar menu lists various features: Discover, Visualize, **Dashboard**, Timelion, Machine Learning, Graph, Dev Tools, Monitoring, and Management. The 'Dashboard' item is currently selected and highlighted in blue. A red box highlights the 'Add a filter +' button at the top of the main content area. A modal window titled 'Add filter' is open, showing a dropdown for 'Filter' set to 'host' and 'is' set to 'Values...', with a list of three server names: 'server_3' (selected and highlighted in blue), 'server_2', and 'server_1'. A green callout bubble points to the 'server_3' entry with the Japanese text 'filterによる絞り込み' (Filterによる絞り込み). Below the modal, there are two line charts. The top chart, titled 'Total Requests (by application)', shows multiple blue lines representing different applications over time from March 31 to April 4. The bottom chart shows a single blue line for 'Total Requests' over the same period. The Y-axis for the top chart ranges from 2.2 to 2.8, and for the bottom chart, it ranges from 3,000,000.000 to 6,000,000.000.

Dashboardの操作



Watcher UI

- Watcherとは
 - 特定の条件を満たした時に、メール・slackなどで通知をしたり、indexを作成することができる監視機能
- 例) CPU使用率が一定値を超えたらメール通知する
レスポンスタイムが閾値を超えたデータのみ別indexに登録する
アクセス数が急激に増加したらslackで通知する

Watcher UI

The screenshot shows the Kibana Management interface. On the left, a sidebar lists various management sections: Discover, Visualize, Dashboard, Timelion, Machine Learning, Graph, Dev Tools, Monitoring, and Management. The 'Management' section is highlighted with a red box and a green callout labeled 'Management'. In the main content area, a header reads 'Management' and 'Version: 6.0.0-rc2'. Below this, there are sections for Security (with links to Users and Roles), Elasticsearch (with a link to Watcher, which is also highlighted with a red box and a green callout labeled 'Watcher'), Kibana, Index Patterns, Saved Objects, Reporting, Advanced Settings, Logstash, and Pipelines. The bottom left corner of the page has the 'elastic' logo.

Watcher UI

Management / Elasticsearch / Watcher

Watches

Search...

Create new watch

Delete

Threshold Alert
Send out an alert on a specific condition.

Advanced Watch
Set up a custom watch in raw JSON.

ID ↑	Name	State
M4qd7xtUTpC0VW...	X-Pack Monitoring:...	Firing
M4qd7xtUTpC0VW...	X-Pack Monitoring:...	OK

Discover

Visualize

Dashboard

Timeline

Machine Learning

Graph

Dev Tools

Monitoring

Management

設定が簡単な "Threshold Alert"と
複雑な監視ができる "Advanced Watch"がある

Watcher UI

The screenshot shows the 'New Watch' configuration page in the Elasticsearch Watcher UI. The page title is 'Management / Elasticsearch / Watcher / Watches / New Watch'. The main section is titled 'Create a new threshold alert' with the sub-instruction 'Send out an alert when specific conditions are met. This will run once every 5 minutes.' A green callout bubble points to the 'Run this watch every' field, which is set to '5 minutes'. Another green callout bubble points to the 'Select an Index' dropdown, which contains the value '.monitoring*' (also highlighted with a red box). A third green callout bubble points to the 'Select a time field' dropdown, which contains the value '@timestamp'.

Management / Elasticsearch / Watcher / Watches / New Watch

New Watch

Create a new threshold alert

Send out an alert when specific conditions are met. This will run once every 5 minutes.

Name

test_watch

Select an Index

.monitoring*

Broad searches can be done by adding * to your query

Select a time field

@timestamp

Run this watch every

5 minutes

index : .monitoring*

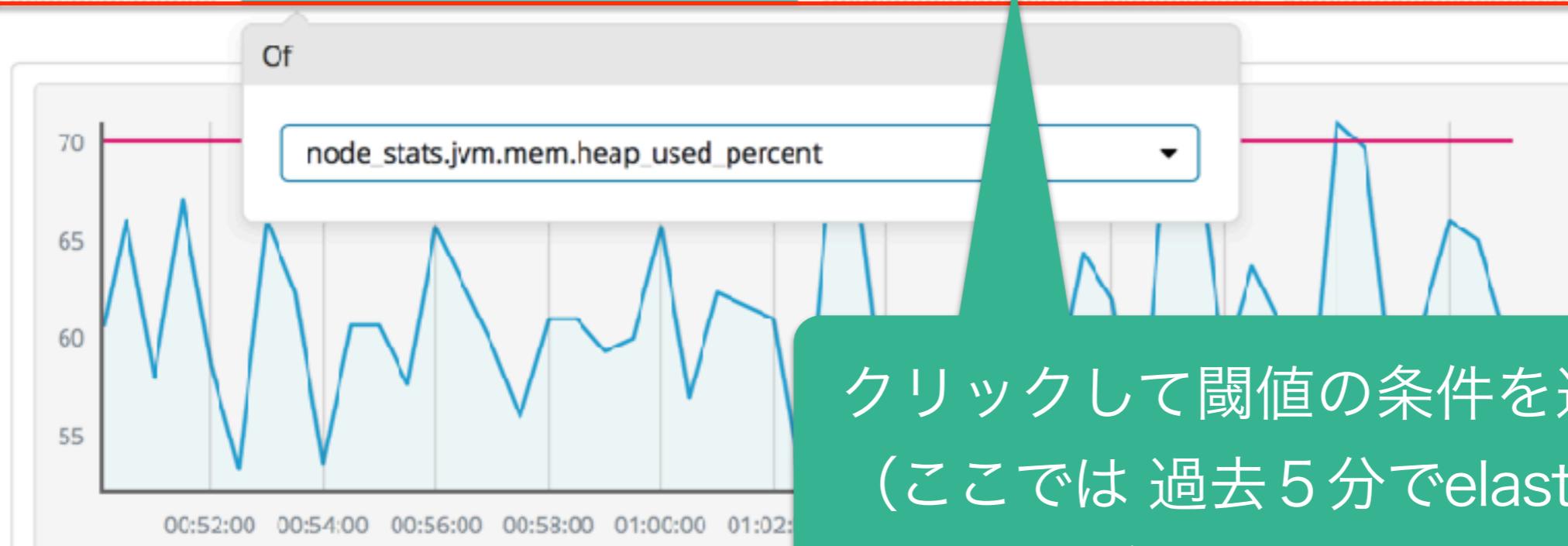
@timestamp

5分毎に実行

Watcher UI

Matching the following condition

WHEN average() OF node_stats.jvm.mem.heap_used_percent OVER all documents IS ABOVE 70 FOR THE LAST 5 minutes



クリックして閾値の条件を選択する
(ここでは 過去 5 分でelasticsearchのヒープ使用率が70%を超えるという条件)

Watcher UI



Watcher UI

The screenshot shows the Watcher UI interface. On the left, there's a sidebar with 'Monitoring' and 'Management' tabs. Below that, it says 'elastic' followed by 'Logout' and 'Collaborate'. The main area has a title 'Will perform 1 action once met' and a dropdown menu 'Add new action'. A 'Logging' action is selected, shown with a red box around its configuration. It includes a 'Log text' input field containing 'これはWatcherのテスト' and a 'Remove Logging Action' button. A large green callout bubble points to this section with the text '1. loggingアクションを選び
ログに出力したいメッセージを入力'. To the right, there's a 'Log a sample message now' button with a red box around it, and a 'Save' button at the bottom right. Another green callout bubble points to this section with the text '2. 保存する前に動作を確認できる'.

1. loggingアクションを選び
ログに出力したいメッセージを入力

2. 保存する前に動作を確認できる

Watcher UI

```
[2017-11-18T01:22:05,763][WARN ][o.e.c.r.a.DiskThresholdMonitor] [ZV1XgHZ] high disk watermark [90%] exceeded on [ZV1XgHZCR5r0Ekw][ZV1XgHZ][/Users/SHIN/jjug_2017_fall/work/elasticsearch-6.0.0-rc2/data/nodes/0] free: 14.8gb[6.3%], shards will be r  
d away from this node  
[2017-11-18T01:22:05,763][INFO ][o.e.c.r.a.DiskThresholdMonitor] [ZV1XgHZ] rerouting shards: [high disk watermark exceeded or more nodes]  
[2017-11-18T01:22:35,865][WARN ][o.e.c.r.a.DiskThresholdMonitor] [ZV1XgHZ] high disk watermark [90%] exceeded on [ZV1XgHZCR5r0Ekw][ZV1XgHZ][/Users/SHIN/jjug_2017_fall/work/elasticsearch-6.0.0-rc2/data/nodes/0] free: 14.8gb[6.3%], shards will be r  
d away from this node  
[2017-11-18T01:22:59,337][INFO ][o.e.x.w.a.l.ExecutableLoggingAction] [ZV1XgHZ] hogehoge  
[2017-11-18T01:23:03,111][INFO ][o.e.x.w.a.l.ExecutableLoggingAction] [ZV1XgHZ] hogehoge  
[2017-11-18T01:23:05,867][WARN ][o.e.c.r.a.DiskThresholdMonitor] [ZV1XgHZ] high disk watermark [90%] exceeded on [ZV1XgHZCR5r0Ekw][ZV1XgHZ][/Users/SHIN/jjug_2017_fall/work/elasticsearch-6.0.0-rc2/data/nodes/0] free: 14.8gb[6.3%], shards will be r  
d away from this node  
[2017-11-18T01:23:05,867][INFO ][o.e.c.r.a.DiskThresholdMonitor] [ZV1XgHZ] rerouting shards: [high disk watermark exceeded or more nodes]  
[2017-11-18T01:23:25,313][INFO ][o.e.x.w.a.l.ExecutableLoggingAction] [ZV1XgHZ] これはWatcherのテスト
```

ログに出力されている

コンテンツ

- 概要説明
- データの投入
- ダッシュボードの作成
- Machine Learning ←
- まとめ

Machine Learning

- Machine Learningとは
 - X-Packの機能の1つ
 - 時系列データの傾向を学習し、異常を検知する。
(教師無し学習)

Machine Learning

The screenshot shows the Kibana interface with the following details:

- Sidebar:** A dark sidebar on the left contains icons and labels for various features: Discover, Visualize, Dashboard, Timelion, **Machine Learning** (which is highlighted with a red box), Graph, Dev Tools, Monitor, and Manage.
- Header:** The header displays "Machine Learning / Job Management".
- Sub-Header:** Below the header are three links: Job Management (underlined), Anomaly Explorer, and Single Metric Viewer.
- Metrics:** A row of metrics shows: Active ML Nodes: 0, Total jobs: 0, Open jobs: 0, Closed jobs: 0, and Active datafeeds: 0.
- Buttons:** A blue button labeled "+ Create new job" is highlighted with a red box.
- Text:** The text "No jobs configured" is displayed on the right.
- Annotations:** Two green callout boxes with arrows point to the "Machine Learning" feature in the sidebar and the "+ Create new job" button.

1. Machine Learning

2. Create new job

Machine Learning

Machine Learning / Job Management / Create New Job

kibana

- Discover
- Visualize
- Dashboard
- Timeline
- Machine Learning
- Graph
- Dev Tools
- Monitoring
- Management

Select job type

 Create a single metric job
Based on a kibana index pattern or saved search

 Create a multi metric job
Based on a kibana index pattern or saved search

 Create an advanced job
Advanced configuration options for creating a job

jobの種類を選択する
(Create a single metric job)

Machine Learning

Visualize / New / Choose search source

From a New Search, Select Index Or, From a Saved Search

Filter... 1 of 1 Saved Searches Filter... 0-0 of 0 Manage saved searches

Name ▾

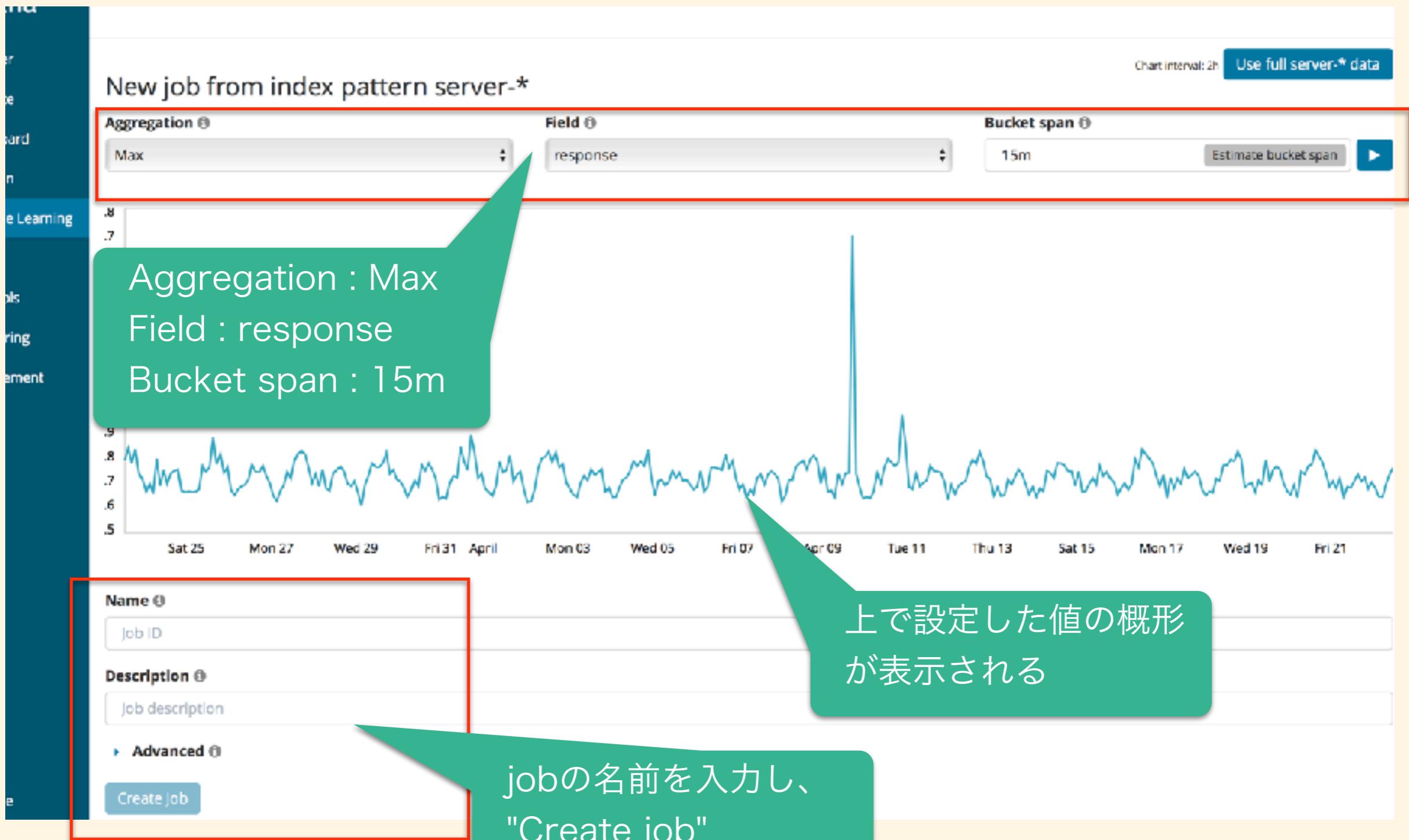
server-*

No matching saved searches found.

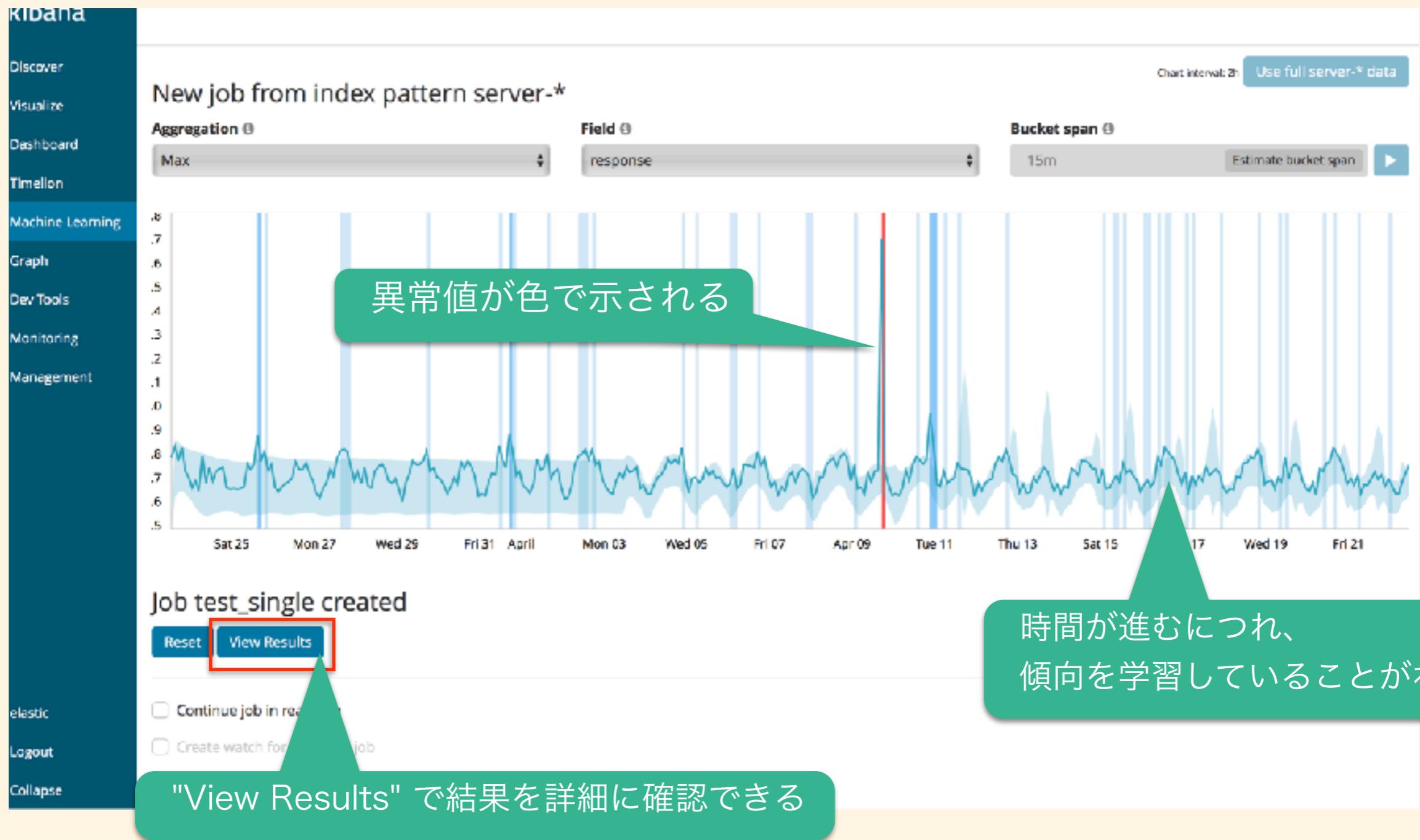
server-*

- Discover
- Visualize
- Dashboard
- Timeline
- Machine Learning
- Graph
- Dev Tools
- Monitoring
- Management

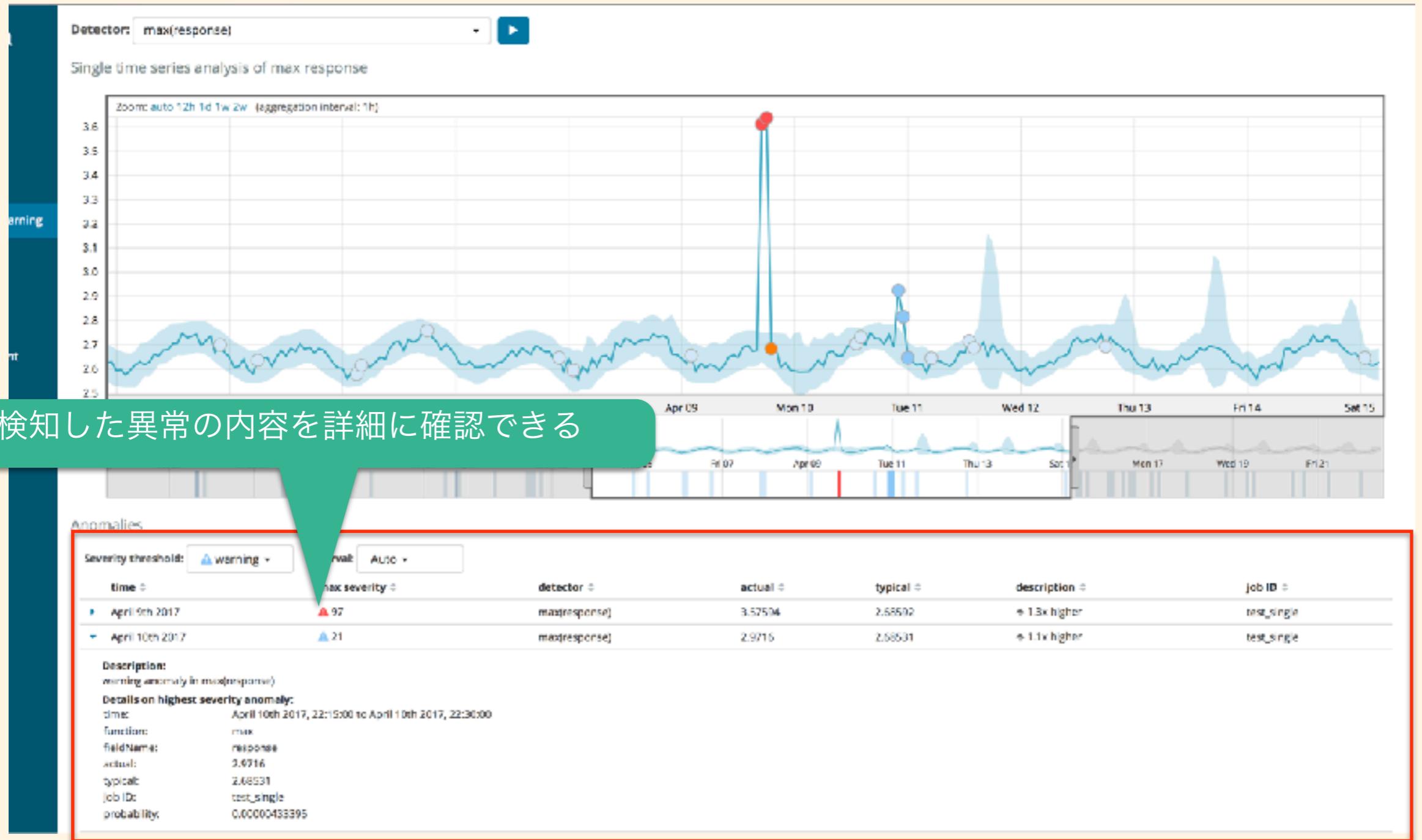
Machine Learning



Machine Learning



Machine Learning



発展

Machine Learning

Machine Learning / Job Management / Create New Job

kibana

Discover

Visualize

Dashboard

Timeline

Machine Learning

Graph

Dev Tools

Monitoring

Management

Select job type

Create a single metric job
Based on a kibana index pattern or saved search

Create a multi metric job
Based on a kibana index pattern or saved search

Create an advanced job
Advanced configuration options for creating a job

複数パラメータの異常検知が可能

Machine Learning

Saved Search
Visualize
Dashboard
Machine Learning
Graph
View Tools
Monitoring
Management

job 'test_multifielded'

New job from index pattern server-*

Chart interval: 1h Use full server-* data

Job settings

Fields

- event_rate Count
- accept Mean
- deny Mean
- response Mean
- total Mean

Sparse data

Split Data

-No split-

Key Fields (Influencers)

- host
- path.keyword
- service

Bucket span

15m Estimate bucket span

Results

Document count

Count event rate

Mean accept

Mean deny

複数パラメータを指定できる

Machine Learning

Split Data

service

Key Fields (Influencers)

host

path.keyword

service

Bucket span ⓘ

15m

Job Details

Name ⓘ

Job ID

Description ⓘ

Job description

Advanced ⓘ

COUNT event rate

Sat 25 Mon 27 Wed 29 Fri 31 April Mon 03 Wed 05

Mean accept

19,000
18,000
17,000

Sat 25 Mon 27 Wed 29 Fri 31 April Mon 03 Wed 05

Mean deny

2,400
2,000
1,800
1,600
1,400
1,200

データを分割することもできる
例) host毎、service毎

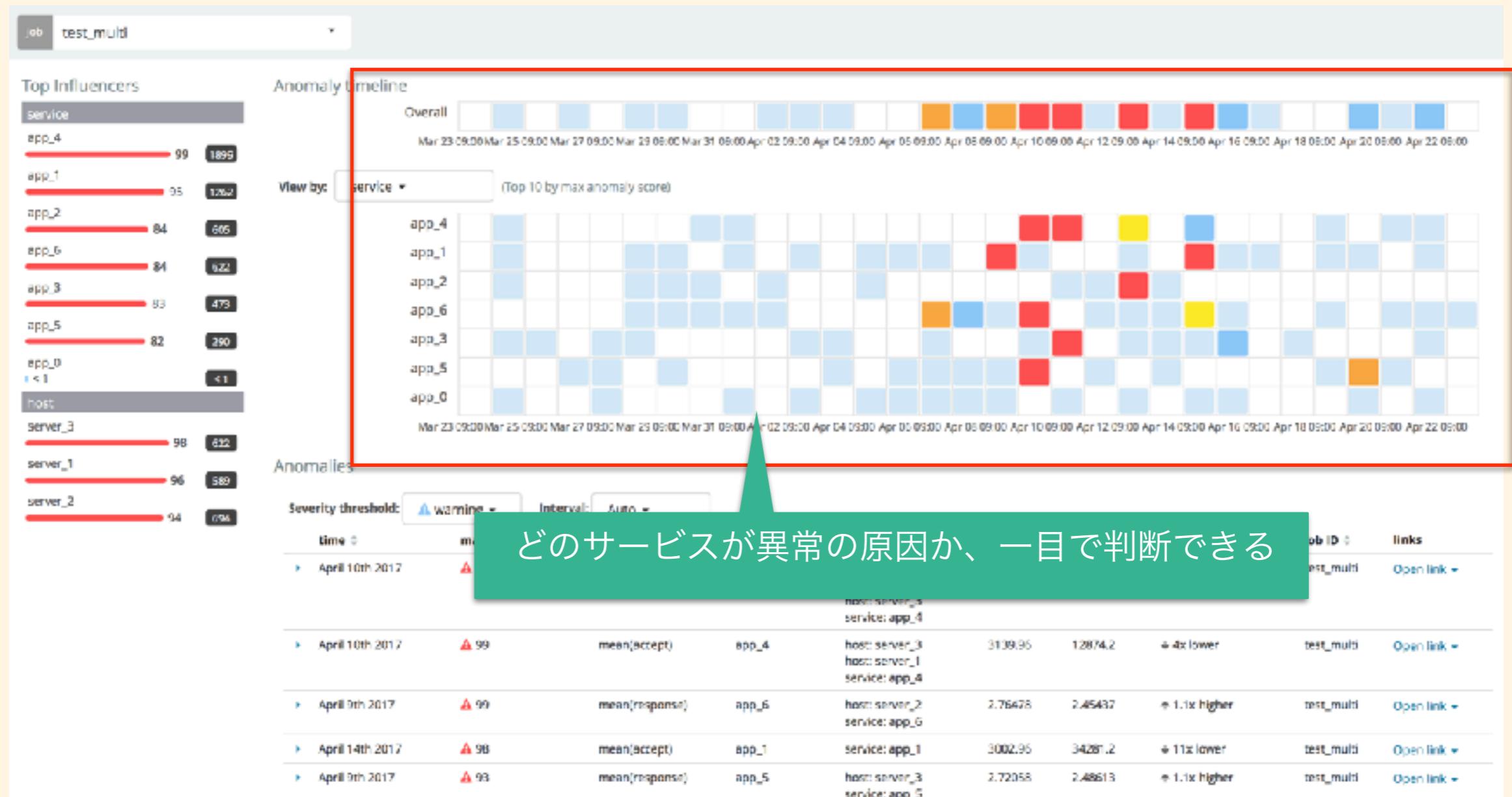
Machine Learning

The screenshot shows a machine learning analysis interface with the following components:

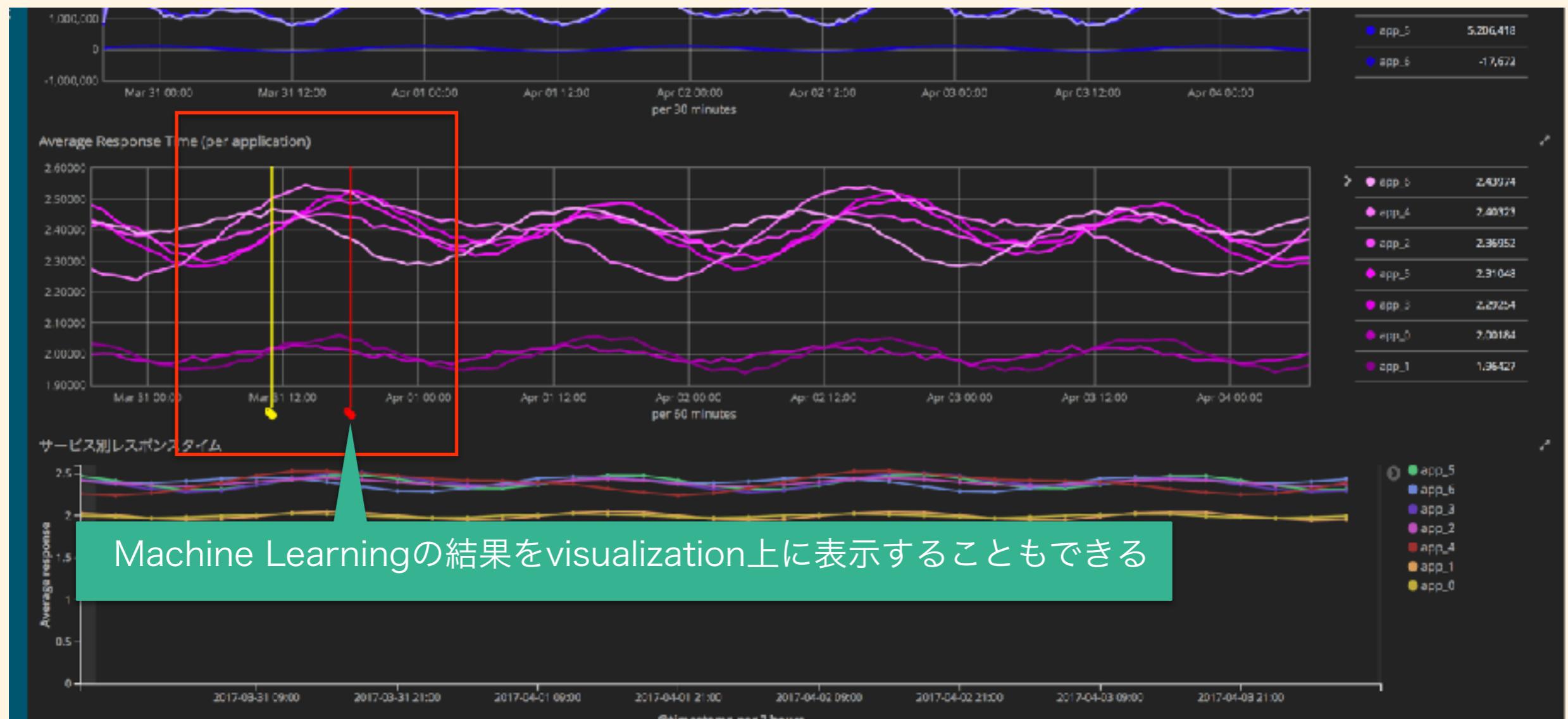
- Analysis Configuration:** Includes sections for "Split Data" (selected "service"), "Key Fields (Influencers)" (selected "host", "service"), "Bucket span" (set to 15m), and "Job Details" (Name: test_multi, Description: job description).
- Advanced Options:** A collapsed section labeled "Advanced" with a "View Results" button.
- Status:** Shows "Analysis running" with "Stop analysis" and "View Results" buttons. The "View Results" button is highlighted with a red box and a green arrow pointing to it from the right.
- Analysis Results:** Three time-series plots:
 - Mean accept:** Y-axis ranges from 8,000 to 18,000. The plot shows a highly volatile line with sharp peaks and troughs.
 - Mean deny:** Y-axis ranges from 0 to 4,000. The plot shows a line with several sharp spikes reaching up to 4,000.
 - Mean response:** Y-axis ranges from 2.01 to 2.03. The plot shows a line with small, frequent oscillations between 2.01 and 2.03.

A green callout box contains the Japanese text: 実行したら、"View Results"から結果を確認する (After execution, check the results from the "View Results" button).

Machine Learning



Machine Learning



余力のある方は試してみてください！

コンテンツ

- 概要説明
- データの投入
- ダッシュボードの作成
- Machine Learning
- まとめ ←

まとめ

- 5.x → 6.0.0で追加された機能に触れた
 - logstash pipeline visualizer
 - Machine Learning
 - Watcher UI
 - Visual Builder
- 今回紹介できなかった改善点も多くあります。
どんどん使ってみてください。

以上です。
ありがとうございました。