ELKではじめる お手軽Flowコレクター

ELK = Elasticsearch + Logstash + Kibana

2015/9/4 ENOG34

（株）創風システム

外山 文規

ELKってなんぞや

- E = Elasticsearch

  全文検索エンジン、json形式でデータを追加

- L = Logstash

  ログを集めたりパースして、任意のDBやファイル等に出力

  fluentdのようなもの

- K = Kibana

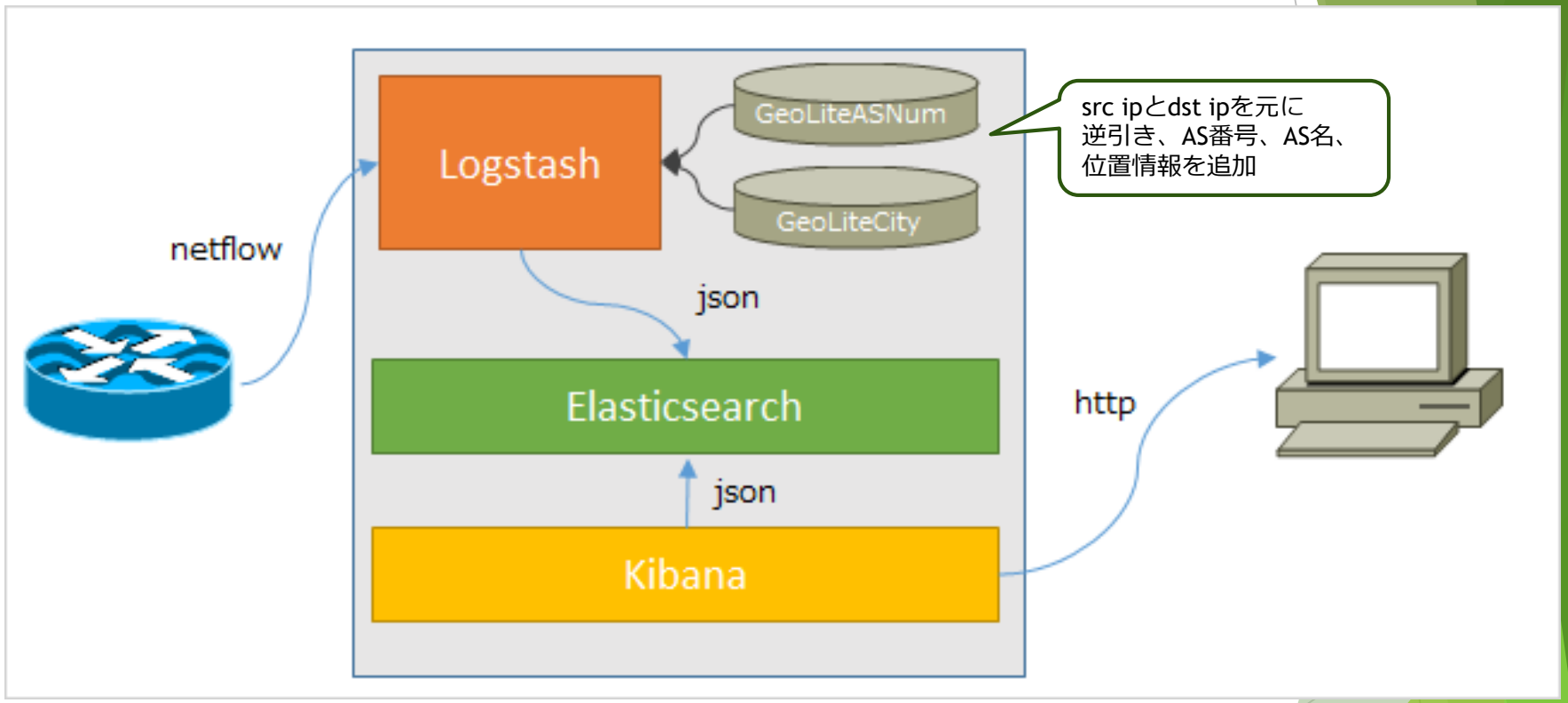
  ログデータの可視化ツール、 Elasticsearchのフロントエンド

  検索、グラフ化できる

NetflowがKibanaで可視化できたらカッコいいかも

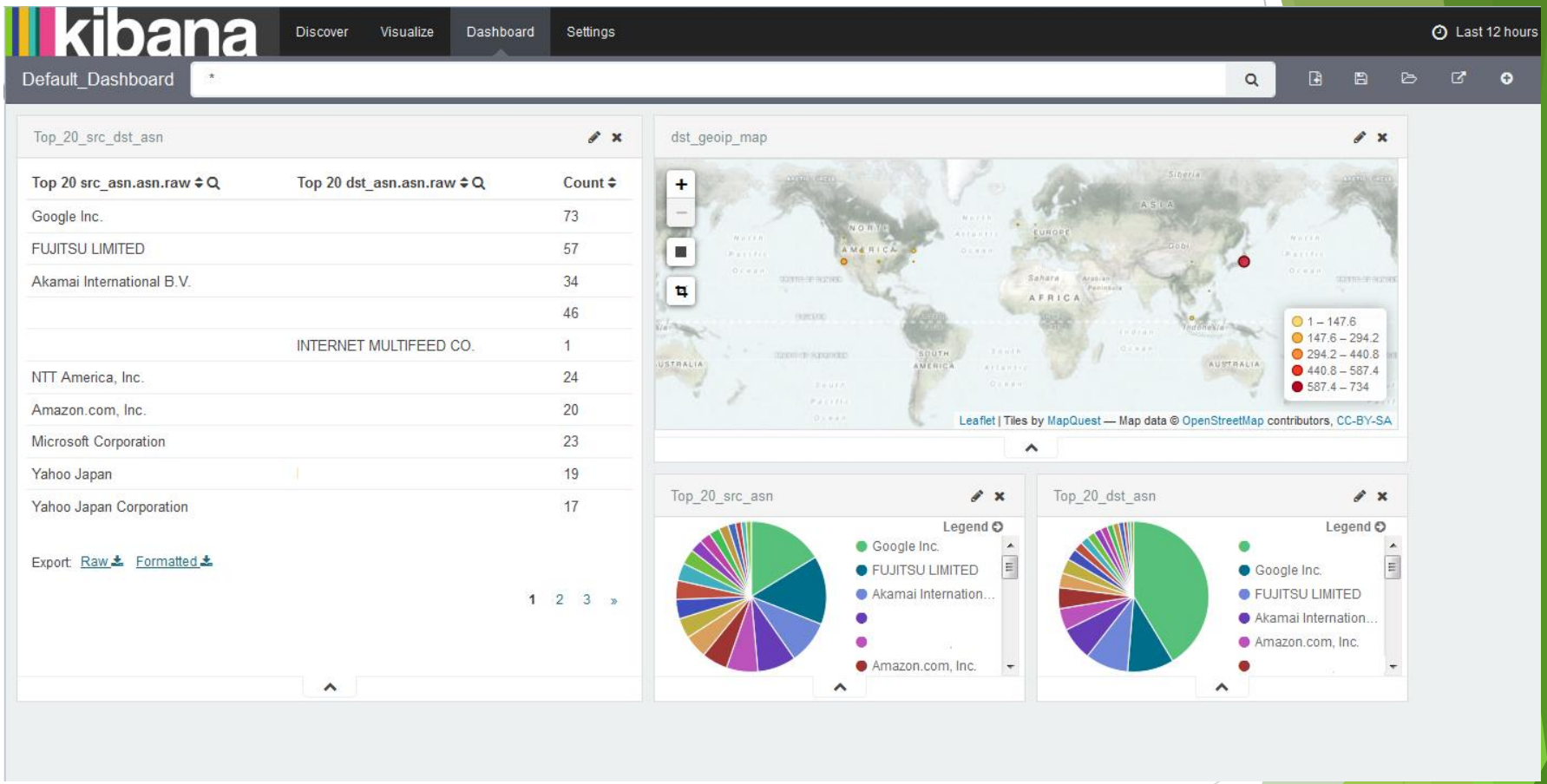
今回の環境

- CentOS 7
- Elasticsearch 1.6
- Logstash 1.5
- Kibana 4.1

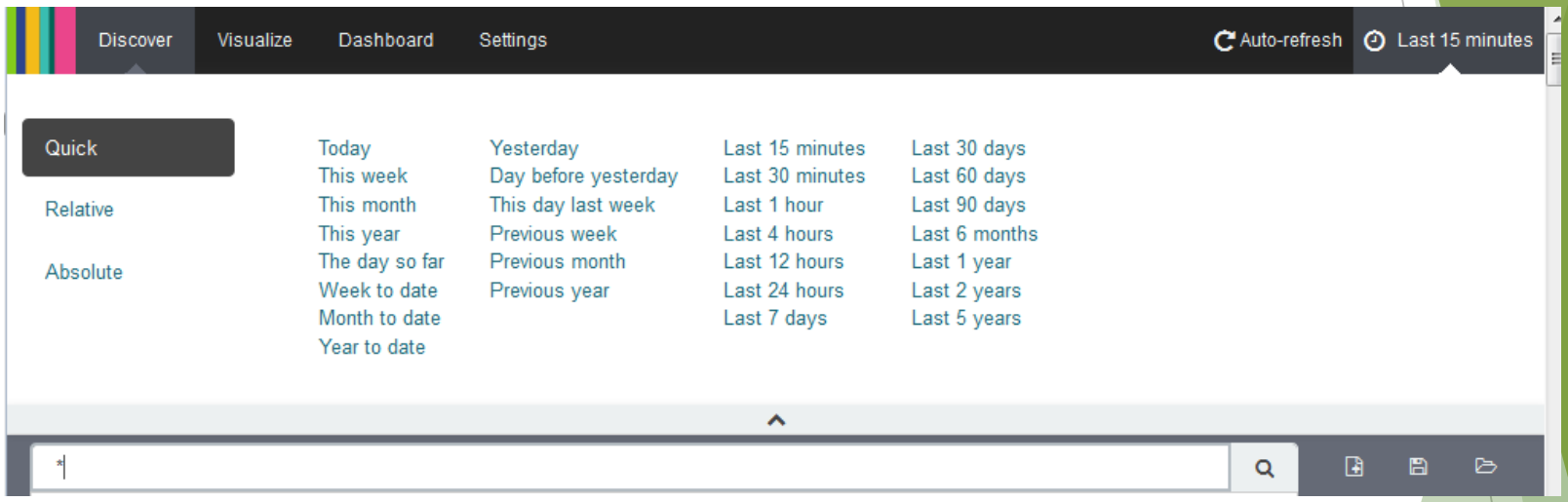

Logstash
GeoLiteASNum
GeoLiteCity
src ipとdst ipを元に
逆引き、AS番号、AS名、
位置情報を追加
netflow
json
Elasticsearch
json
Kibana
http

Netflowのデータにあるsrc_ipとdst_ipを元にmaxmindのGeoLiteASNum、GeoLiteCityを使って、AS情報と位置情報を付加しました。

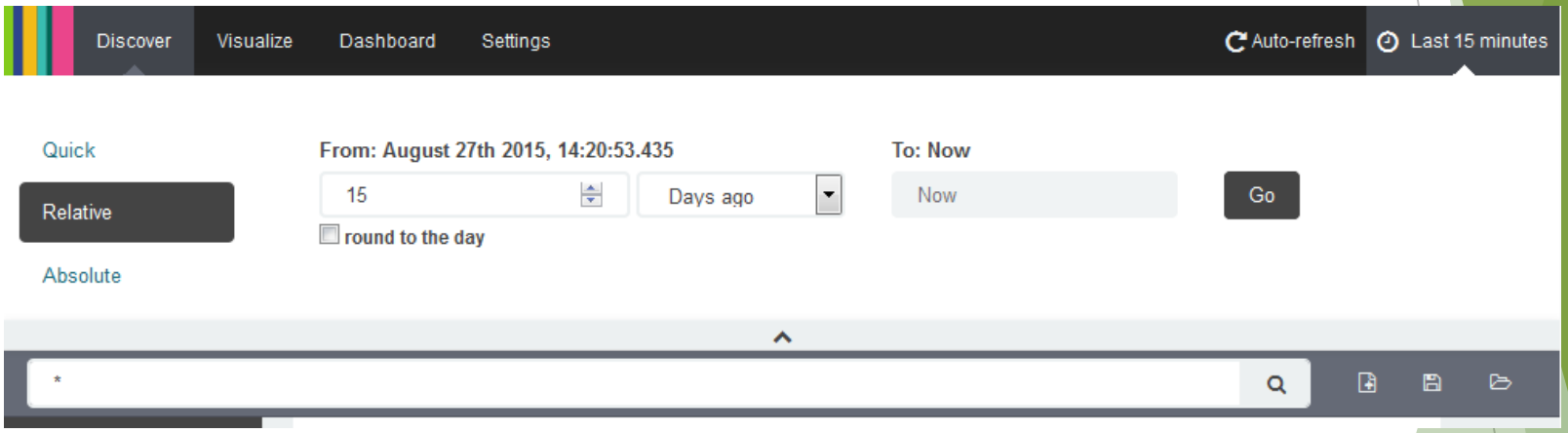
ダッシュボード作成例


kibana
Discover
Visualize
Dashboard
Settings
Last 12 hours
Default_Dashboard
*
Top_20_src_dst_asn
Top 20 src_asn.asn.raw
Top 20 dst_asn.asn.raw
Count
Google Inc. 73
FUJITSU LIMITED 57
Akamai International B.V. 34
46
INTERNET MULTIFEED CO. 1
NTT America, Inc. 24
Amazon.com, Inc. 20
Microsoft Corporation 23
Yahoo Japan 19
Yahoo Japan Corporation 17
Export: Raw Formatted
1 2 3 »
dst_geoip_map
1 – 147.6
147.6 – 294.2
294.2 – 440.8
440.8 – 587.4
587.4 – 734
Leaflet | Tiles by MapQuest — Map data © OpenStreetMap contributors, CC-BY-SA
Top_20_src_asn
Legend
Google Inc.
FUJITSU LIMITED
Akamai Internation...
Amazon.com, Inc.
Top_20_dst_asn
Legend
Google Inc.
FUJITSU LIMITED
Akamai Internation...
Amazon.com, Inc.

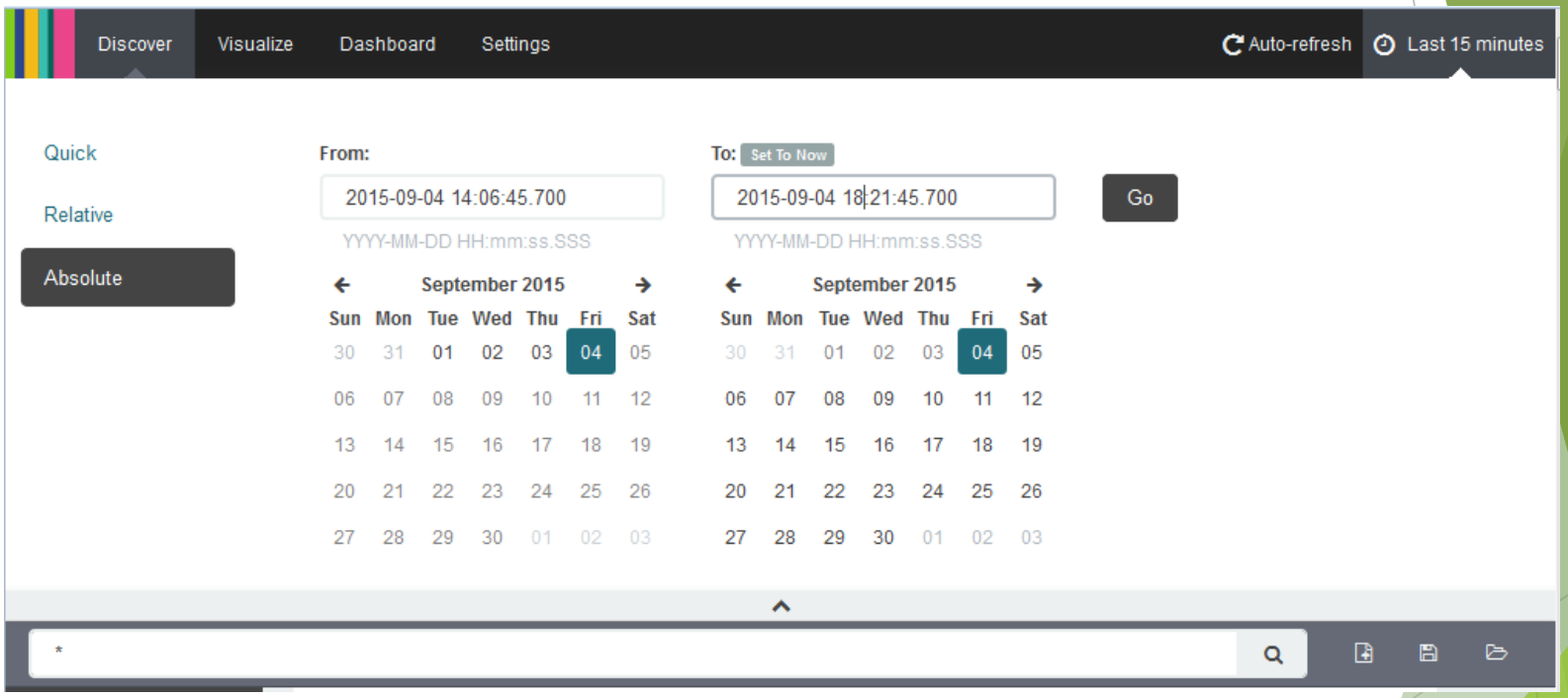
日時により指定できる
フィルタ項目1



日時により指定できる フィルタ項目2



日時により指定できる フィルタ項目3



Elasticsearchのインストール

以下のURLを参考にして yum install で完了

https://www.elastic.co/guide/en/elasticsearch/reference/current/setup-repositories.html#_yum

Elasticsearchの確認

curl -X GET http://localhost:9200/
以下が返ってくる


```
{
  "status" : 200,
  "name" : "Magnus",
  "cluster_name" : "elasticsearch",
  "version" : {
    "number" : "1.6.0",
    "build_hash" : "cdd3ac4dde4f69524ec0a14de3828cb95bbb86d0",
    "build_timestamp" : "2015-06-09T13:36:34Z",
    "build_snapshot" : false,
    "lucene_version" : "4.10.4"
  },
  "tagline" : "You Know, for Search"
}
```

Logstashのインストール

以下のURLを参考にして yum install で完了

https://www.elastic.co/guide/en/logstash/current/package-repositories.html#_yum

Logstashの設定 1 (netflowを受け取る)

※/etc/logstash/conf.d/ の下に ○○.conf で作成する
Netflowのパケット取得するための設定

```
input {
  udp {
    port => 2055
    codec => netflow {
      versions => [5]
    }
  }
}
```

Logstashの設定２
(逆引き情報追加の準備)

※/etc/logstash/conf.d/ の下に ○○.conf で作成する
Netflowのデータをもとに、geoip、ASN、逆引き情報を追加

```
filter {
  mutate {
   add_field => [ "[netflow][ipv4_dst_host]","%{[netflow][ipv4_dst_addr]}" ]
   add_field => [ “[netflow][ipv4_src_host]","%{[netflow][ipv4_src_addr]}" ]
  }
```

※逆引き情報のために、IPアドレス情報をコピー

Logstashの設定３
(src, dstのIPから逆引き情報追加)

```
dns {
    action => 'replace'
    reverse => "[netflow][ipv4_dst_host]"
  }
  dns {
    action => 'replace'
    reverse => "[netflow][ipv4_src_host]"
  }
}
```

※先ほどコピーしたフィールドを逆引き情報に置換

Logstashの設定４ (src,dstのIPから位置情報追加)

```
geoip {
    database => "/usr/share/GeoIP/GeoLiteCity.dat"
    source => "[netflow][ipv4_dst_addr]"
    target => "dst_geoip"
  }
  geoip {
    database => "/usr/share/GeoIP/GeoLiteCity.dat"
    source => "[netflow][ipv4_src_addr]"
    target => "src_geoip"
  }
```

※IPアドレスを元に位置情報を追加

Logstashの設定５
(AS番号、AS名を追加)

```
geoip {
        database => "/usr/share/GeoIP/GeoLiteASNum.dat"
        source => "[netflow][ipv4_dst_addr]"
        target => "dst_asn"
    }
    geoip {
        database => "/usr/share/GeoIP/GeoLiteASNum.dat"
        source => "[netflow][ipv4_src_addr]"
        target => "src_asn"
    }
```

※IPアドレスをもとにASN情報を追加

Logstashの設定６ (elasticsearchにデータ投げる)

加工した結果をelasticsearchに投げる

```
 output {
elasticsearch {
       index => "logstash-%{+YYYY.MM.dd}"
      host => "localhost"
    }
  }
```

位置情報はElasticsearchのtemplateを修正しないと、正しく位置情報として扱えません。

elasticsearchのtemplateの修正

※dst_geoipのテンプレートを設定

```
"dst_geoip"  : {
          "type" : "object",
            "dynamic": true,
            "properties" : {
              "location": {
                "geohash": true,
                "geohash_precision": 10,
                "geohash_prefix": true,
                "lat_lon": true,
                "type": "geo_point"
              }
            }
       },
```

elasticsearchのtemplateの修正

※src_geoipのテンプレートを設定

```
“src_geoip”  : {
          “type” : “object”,
            “dynamic”: true,
            “properties” : {
              “location”: {
                “geohash": true,
                "geohash_precision": 10,
                "geohash_prefix": true,
                "lat_lon": true,
                "type": "geo_point"
              }
            }
       },
```

GeoIPのインストール設定、

yum install GeoIP GeoIP-update –y

vi /etc/GeoIP.conf

ProductIds 506 533

↓に変更

ProductIds GeoLite2-City GeoLite2-Country GeoLite-Legacy-IPv6-City GeoLite-Legacy-IPv6-Country 506 517 533

geoipupdate

参考:
http://dev.maxmind.com/geoip/geoipupdate/

Logstashの確認

curl -X GET http://localhost:9200/_cat/shards

logstash-2015.07.29 0 p STARTED 251554 127.3mb 210.236.208.14 Karolina Dean

kibanaのインストール

```
# wget https://download.elastic.co/kibana/kibana/kibana-4.1.0-linux-x64.tar.gz

# tar -zxvf kibana-4.1.0-linux-x64.tar.gz

# mkdir -p /opt/kibana

# cp -vR kibana-4.1.0-linux-x64/* /opt/kibana/
```

kibanaのインストール

vi /etc/systemd/system/kibana4.service

```
[Service]
ExecStart=/opt/kibana/bin/kibana
Restart=always
StandardOutput=syslog
StandardError=syslog
SyslogIdentifier=kibana4
User=root
Group=root
Environment=NODE_ENV=production

[Install]
WantedBy=multi-user.target
```

flow数が多かったり、貯めるデータ数が多い場合は、シンプルな構成では収まらないのでクラスタを組むなど対策が必要

参考情報

Blog:

Netflowコレクターを無償のFluend＋ElasticSearch＋Kibanaで構築する
http://komeiy.hatenablog.com/entry/2014/09/26/212000

Step-by-Step Setup of ELK for NetFlow Analytics

http://blogs.cisco.com/security/step-by-step-setup-of-elk-for-netflow-analytics

How To Install Elasticsearch, Logstash, and Kibana 4 on CentOS 7

https://www.digitalocean.com/community/tutorials/how-to-install-elasticsearch-logstash-and-kibana-4-on-centos-7

書籍:

サーバ/インフラエンジニア養成読本 ログ収集~可視化編
(Software Design plus)