報道各位

2018 年 10 月 3 日
株式会社インプレスR&D
https://nextpublishing.jp/

定番 BI ツール ElactickStack 最新版解説書！

# 『Elastic Stack で作る BI 環境　バージョン 6.4 対応版』発行

技術書典シリーズ・10 月の新刊

インプレスグループで電子出版事業を手がける株式会社インプレスR&Dは、『Elastic Stackで作るBI環境　バージョン6.4対応版』(著者:石井 葵)を発行いたします。

**『Elastic Stackで作るBI環境　バージョン6.4対応版』**
https://nextpublishing.jp/isbn/9784844398608


著者:石井 葵
小売希望価格:電子書籍版　1600 円(税別)／印刷書籍版　1800 円(税別)
電子書籍版フォーマット:EPUB3／Kindle Format8
印刷書籍版仕様:B5 判／カラー／本文 112 ページ
ISBN:978-4-8443-9860-8
発行:インプレス R&D

## ＜＜発行主旨・内容紹介＞＞

【誰でも簡単にログ分析！OSS の BI ツール Elastic Stack・最新版対応解説書！】

サーバーのアクセスログや Twitter のつぶやき、様々な機器の動作状況など各種のログファイルを Excel で分析していませんか？

本書は OSS で提供されている BI 環境「Elastic Stack」を使ってログファイルを集計し、グラフなどでビジュアル豊かに分析するための環境構築チュートリアルです。

(本書は、次世代出版メソッド「NextPublishing」を使用し、出版されています。)

# 様々なツールからなる Elastic Stack の概要を紹介

## Elastic Stackって何？

「Elastic Stack はElastic社が提供しているツールっていうのはわかったけど、どれを使えばいいのかな？公式サイトを見るといっぱい種類があるみたいだけど…。」

おや？もふもふちゃん、なんだかお困りのようです。それもそうですね。Elastic Stackにはたくさん便利ツールがあるのはわかりますが、ログ分析にはどのツールが必要なのかわかりません。この章でElastic Stackを構成するツールには何があり、どのように使えば良いのか一緒にみてみましょう。

### Logstash

Logstashは、各環境に散らばっているログを集め、指定した対象に連携できるツールです。ログの連携だけではなく、ログの加工機能も持ち合わせています。コード自体はRuby言語で記載されています。

肝心のどんなログが取り込みできるかですが、ログの出力形式としてよくあるテキストファイルはもちろん、xmlやjsonファイルも対象として指定できます。ファイルの情報以外にもTwitter APIと連携してTwitterのつぶやき情報を取り込む事や、データベース（RDB）に接続して情報を取得する事も可能です。RSDBと連携する際はSQL文を用いて情報を取得するため、欲しい情報だけSQLで取得し、情報を付け足す事も可能です。

ログの出力先は、このあと出てくるElasticsearchだけでなく、プロジェクトの進捗状況管理ツールであるRedmineにも送信できます。取り込んだ情報をCSVファイルとして出力する事や、syslogとして転送することも可能です。利用方法によってはログ解析以上の威力を発揮するツールだと言えます。

### Elasticsearch

Elasticsearchは、Javaで作られている分散処理型の検索エンジンです。クラスター構成を組むことができるのが特徴なので、大規模な環境で検索エンジンとして利用されることがあります。GitHubのリポジトリ情報や、Dockerのコンテナ検索、Facebook上での検索などが導入事例として有名です。

クラスターとは、物理的には複数存在しているにも関わらず、論理的には1つとして見せることができる技術です。処理の負荷分散ができるため、高い性能を求められる環境で多く選択されています。

図1.1　クラスターを利用しない場合

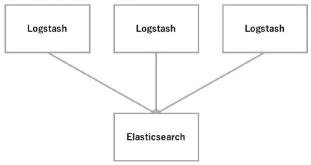
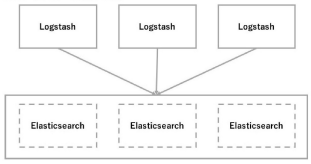



図1.2　クラスターを利用する場合




バージョン6.3では、新しくSQLを用いた検索に対応する機能が追加されました。以前はJSON形式でクエリを記述していましたが、学習コストがかかることが難点でした。しかし、SQLを用いたSelect文は認知度が高いため、普段Elasticsearchに触れる機会が少ないエンジニアでも検索ができるようになります。これに対応して、KibanaからElasticsearchへクエリを発行することができるようにもなりました。

注意するべきこととして、SQLは基本的にSelect文だけが利用できます。Delete・Insert文など、データを操作するクエリは利用できません。合わせて、JDBCドライバ経由でのSQL操作はサブスクリプションの購入が必要です。詳しいライセンスは公式ホームページのElasticsearch・管理とツール（https://www.elastic.co/jp/subscriptions）を確認してください。





# Twitter の履歴を題材にデータを可視化する方法を解説

## データを集めて可視化しよう（Twitterのつぶやき履歴編）

「セットアップはできたけれど、実際にログをElasticsearchに集めてこないといけないな…。でもどうやってElasticsearchにデータを入れたらいいのかな？」

もふもふちゃん、ついにログの収集を始めるようです。まずはTwitterのつぶやき履歴をLogstashで収集・加工しElasticsearchへ連携するところから始めましょう。

### Twilogサービスを利用したログ取得（ログデータの準備）

まずはLogstashに取り込むデータを準備します。今回はTwitterアカウントの発言を追いかけるため、Twilogサービスを利用します。Twilogとは、Twitterでのツイートを自動で保存・閲覧できるサービスです。記録された履歴はCSV（SJIS/UTF-8）やXMLでダウンロードできます。今回はCSV（UTF-8）でダウンロードします。

Twilogサービスへの登録

まず、Twilog公式サイト（http://twilog.org）へアクセスします。Sign in with Twitterアイコンをクリックし、Twitterの認証画面でTwilogに自分のTwitterアカウントを登録してください。

Twilogへの登録

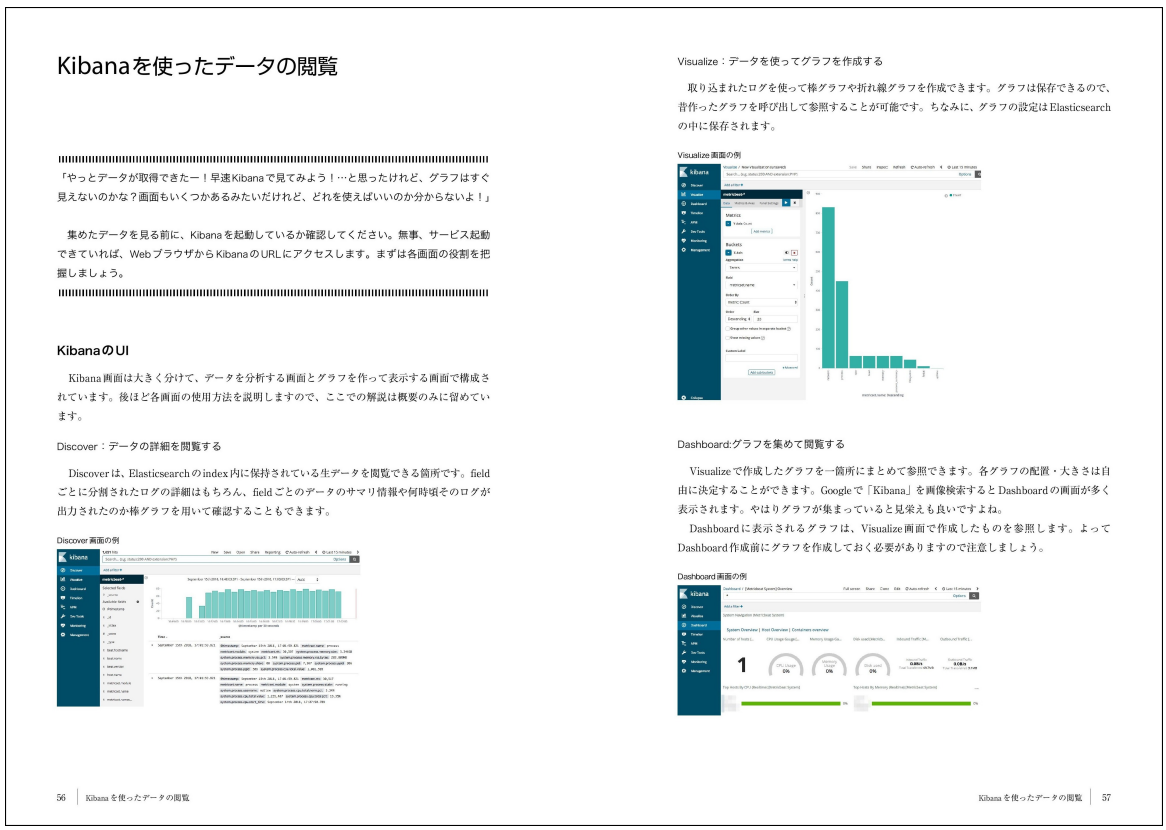

認証後、Twilogの管理画面へアクセスします。Twilogのデフォルト設定では、直近200件分の過去ツイート情報しか取得できません。ログ数を増やすため、過去ツイートの取得から昔のツイートを全て取得しておきましょう。

過去ツイートの取得


過去ログのダウンロード

いよいよ過去ログのダウンロードを行います。とは言っても図3.3の画面から好きな形式を選択してダウンロードするだけです。zip圧縮されているため、適宜解凍してください。ログは好きなディレクトリに配置して良いですが、読み取り権限がついているか確認してください。

# Kibana を使って実際に収集したログを閲覧する方法を解説



## Kibanaを使ったデータの閲覧

「やっとデータが取得できたー！早速Kibanaで見てみよう！…と思ったけれど、グラフはすぐ見えないのかな？画面もいくつかあるみたいだけれど、どれを使えばいいのか分からないよ！」

集めたデータを見る前に、Kibanaを起動しているか確認してください。無事、サービス起動できていれば、WebブラウザからKibanaのURLにアクセスします。まずは各画面の役割を把握しましょう。

### KibanaのUI

Kibana画面は大きく分けて、データを分析する画面とグラフを作って表示する画面で構成されています。後ほど各画面の使用方法を説明しますので、ここでの解説は概要のみに留めています。

Discover：データの詳細を閲覧する

Discoverは、Elasticsearchのindex内に保持されている生データを閲覧できる箇所です。fieldごとに分割されたログの詳細はもちろん、fieldごとのデータのサマリ情報や何時頃そのログが出力されたのか棒グラフを用いて確認することもできます。

Discover画面の例

56 | Kibanaを使ったデータの閲覧

Visualize：データを使ってグラフを作成する

取り込まれたログを使って棒グラフや折れ線グラフを作成できます。グラフは保存できるので、昔作ったグラフを呼び出して参照することが可能です。ちなみに、グラフの設定はElasticsearchの中に保存されます。

Visualize画面の例

Dashboard:グラフを集めて閲覧する

Visualizeで作成したグラフを一箇所にまとめて参照できます。各グラフの配置・大きさは自由に決定することができます。Googleで「Kibana」を画像検索するとDashboardの画面が多く表示されます。やはりグラフが集まっていると見栄えも良いですよね。

Dashboardに表示されるグラフは、Visualize画面で作成したものを参照します。よってDashboard作成前にグラフを作成しておく必要がありますので注意しましょう。

Dashboard画面の例

Kibanaを使ったデータの閲覧 | 57

## ＜＜目次＞＞


Elastic Stack って何？
- Logstash
- Elasticsearch
- Kibana
- Beats
- Elastic Cloud
- 基本的な構成

環境構築
- インストールの順番
- 事前準備
- Elasticsearch のインストール
- Logstash のインストール
- Kibana のインストール

データを集めて可視化しよう(Twitter のつぶやき履歴編)
- Twilog サービスを利用したログ取得(ログデータの準備)
- logstash.conf とは？
- output プラグイン
- filter プラグイン
- logstash.conf のテスト方法
- ここまでで作成した logstash.conf をおさらいする

データを集めて可視化しよう(Beats を使って情報を集めてみる)
- Beats のインストール
  - パッケージを使ってインストールする場合(Windows 以外の OS)

Windows にインストールする場合
Metricbeat のセットアップ
環境をセットアップする
Metricbeat の起動
Kibana を使ったデータの閲覧
Kibana の UI
Discover 画面を使ってみよう
index の紐付け
新しくデータを取り込んだ場合
Discover でログを閲覧する
データの検索期間を変更する
Discover 画面でログを詳しく閲覧しよう
自分で検索してみよう
検索条件を保存しよう
Visualize 画面でデータを可視化する
Visualize 画面で作成できるグラフの種類
Visualize 画面でグラフを作成する
Dashboard 画面を使ってグラフを一覧表示する
グラフを並べる
グラフの大きさを指定する
保存する(検索期間を保持する/しないを選択する)
グラフの色を変更
作成した Dashboard を編集する
トラブルシューティング
Elasticsearch が起動しない
Elasticsearch に対して curl コマンドを発行できない
Elasticsearch サービスを restart しようとすると、エラーが出力される
Kibana 画面の様子がおかしい

**＜＜著者紹介＞＞**

石井 葵

Elasticsearch、Kibana、Logstash を使用したデータ分析基盤の設計・構築をメインに行なうインフラエンジニアだったが、最近配属が変わって新卒なエンジニアの教育を実施している。新卒エンジニアと一緒にプログラミングやアプリケーション開発手法を学ぶ日々を過ごしている。

**＜＜販売ストア＞＞**

電子書籍:

Amazon Kindle ストア、楽天 kobo イーブックストア、Apple Books、紀伊國屋書店 Kinoppy、Google Play Store、honto 電子書籍ストア、Sony Reader Store、BookLive!、BOOK☆WALKER

印刷書籍:

Amazon.co.jp、三省堂書店オンデマンド、honto ネットストア、楽天ブックス

※　各ストアでの販売は準備が整いしだい開始されます。

※　全国の一般書店からもご注文いただけます。

**【株式会社インプレス R&D】** https://nextpublishing.jp/

株式会社インプレス R&D（本社：東京都千代田区、代表取締役社長：井芹昌信）は、デジタルファーストの次世代型電子出版プラットフォーム「NextPublishing」を運営する企業です。また自らも、NextPublishing を使った「インターネット白書」の出版など IT 関連メディア事業を展開しています。
※NextPublishing は、インプレス R&D が開発した電子出版プラットフォーム（またはメソッド）の名称です。電子書籍と印刷書籍の同時制作、プリント・オンデマンド（POD）による品切れ解消などの伝統的出版の課題を解決しています。これにより、伝統的出版では経済的に困難な多品種少部数の出版を可能にし、優秀な個人や組織が持つ多様な知の流通を目指しています。

**【インプレスグループ】** https://www.impressholdings.com/
株式会社インプレスホールディングス（本社：東京都千代田区、代表取締役：唐島夏生、証券コード：東証 1 部 9479）を持株会社とするメディアグループ。「IT」「音楽」「デザイン」「山岳・自然」「旅・鉄道」「学術・理工学」を主要テーマに専門性の高いメデイア&サービスおよびソリューション事業を展開しています。さらに、コンテンツビジネスのプラットフォーム開発・運営も手がけています。

**【お問い合わせ先】**
株式会社インプレス R&D NextPublishing センター
TEL 03-6837-4820
電子メール: np-info@impress.co.jp