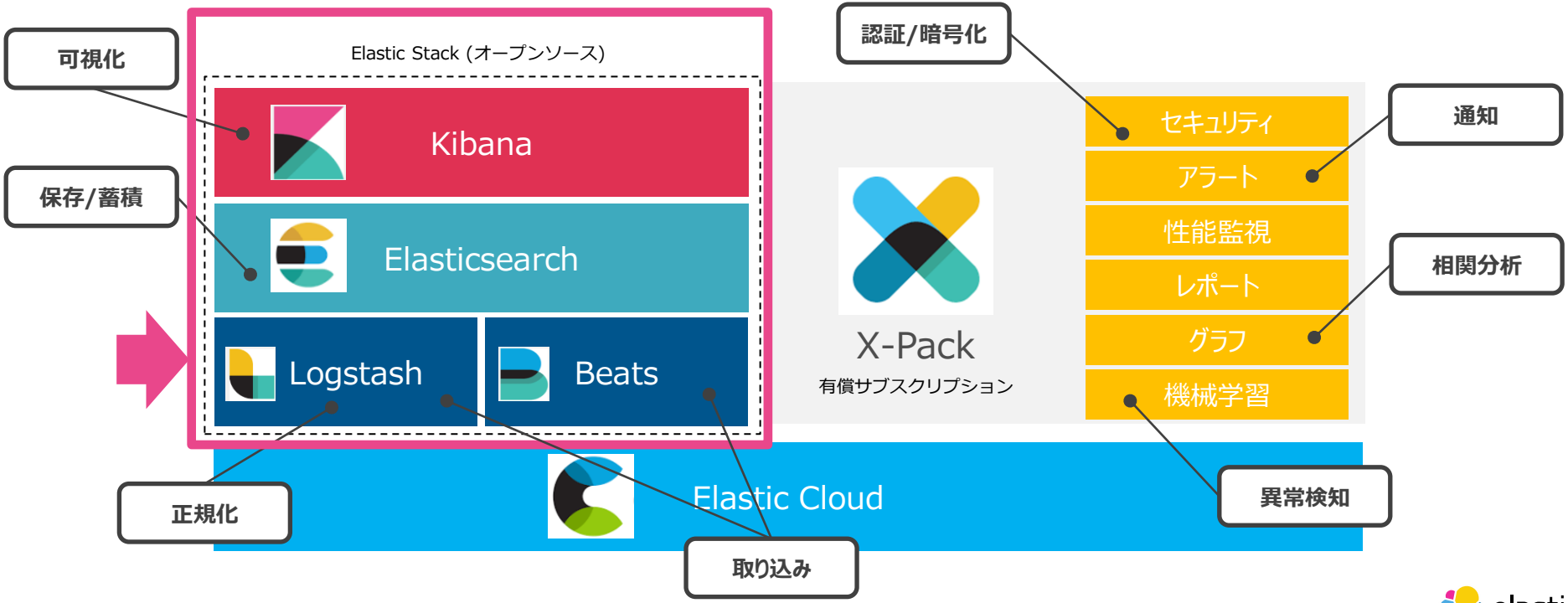
Elastic Stackのご紹介

Elastic Stackとは

全文検索エンジンであるElasticsearchを中心としたElastic社のオープンソースプロダクト群



elastic

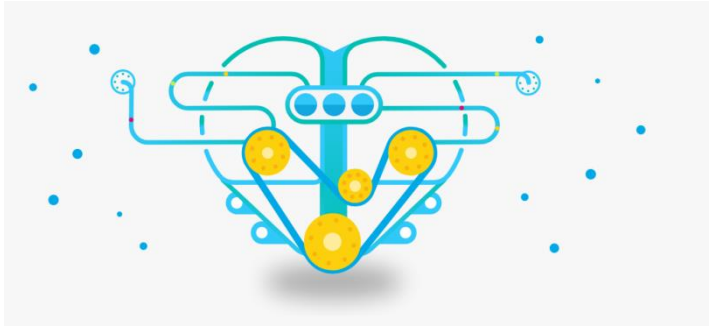
Elasticsearchとは

Elastic社が提供する「Lucene」ベースのオープンソース全文検索エンジン

【コンセプト】
✓ ユーザのほしいものを簡単に検索できるようにする

【優位性】
✓ 分析の柔軟性と検索のリアルタイム性

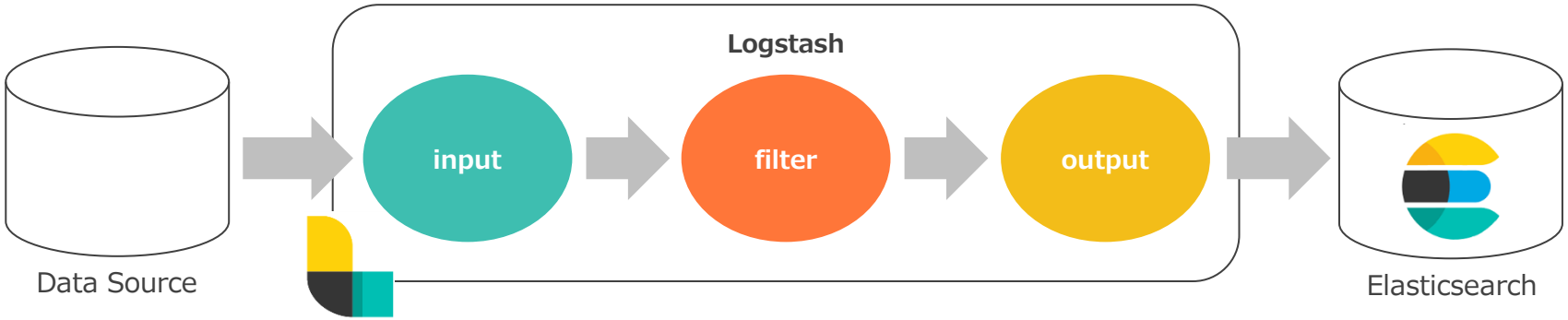
【特徴】
✓ 大規模分散
✓ リアルタイム性
✓ ドキュメント指向
✓ スキーマフリー
✓ RESTfulAPI



elastic

Logstashとは

多種多様なソースからのデータ取り込み、複雑な加工処理、指定場所への出力をしてくれるETLツール



input句：加工するデータを取得元を指定

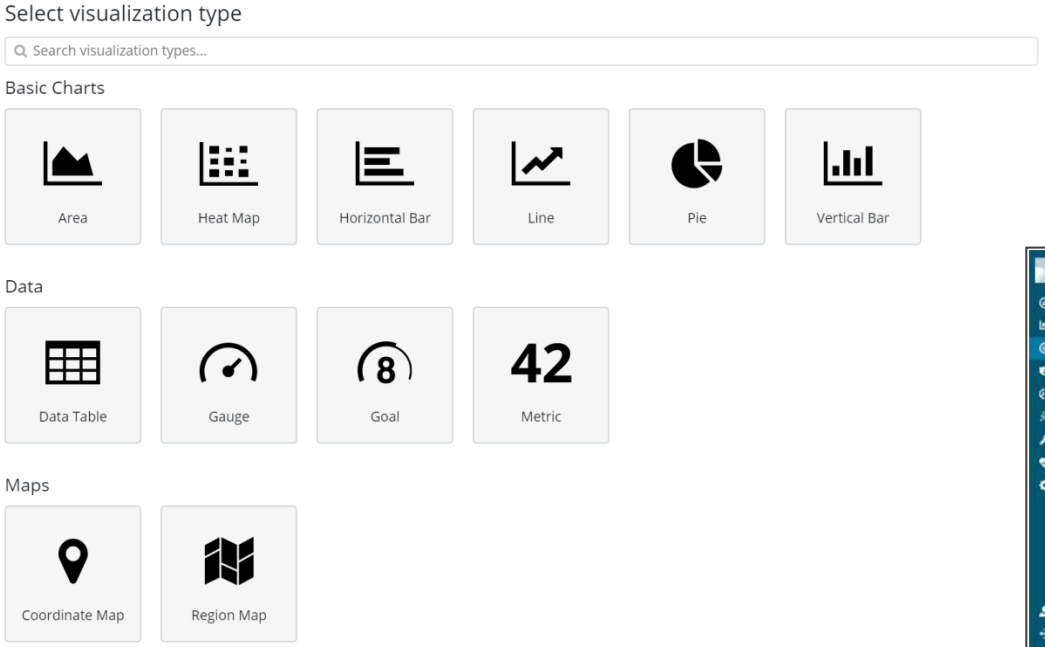
filter句：取得したデータの加工方法を指定

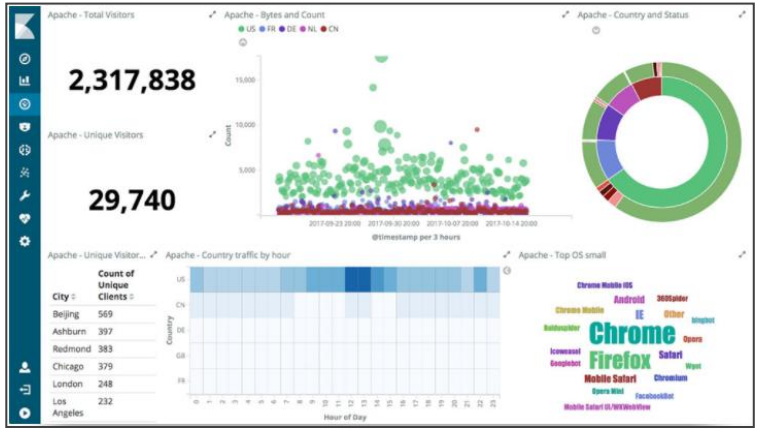
output句：加工したデータの保存先を指定

elastic

Kibanaとは

Elasticsearchに取り込まれたデータを可視化するツール（Webブラウザ上で操作可能）





elastic

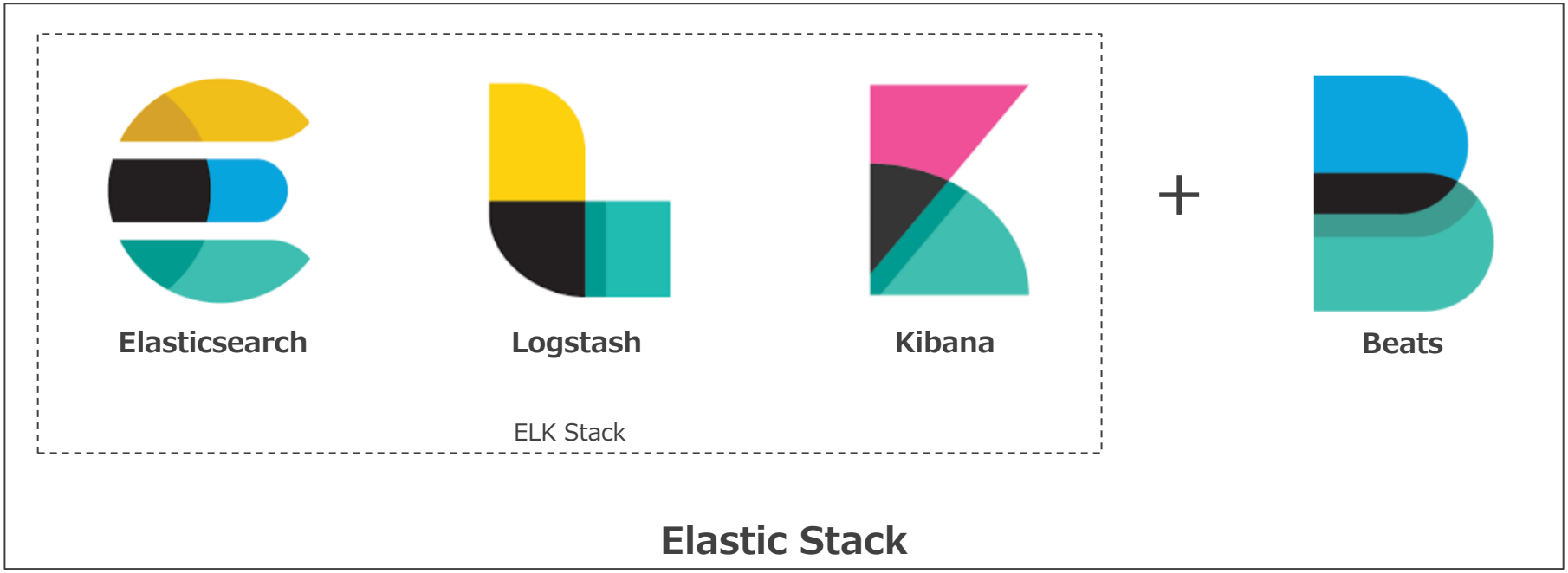
Beatsとは

データの取り込みに特化したシンプルで軽量なデータ取り込みツール

elastic

ELK Stack → Elastic Stack

BeatsのジョインによりELK StackからElastic Stackへ名称変更



elastic

有償プラグイン(X-Pack)とは

有償プラグインであるX-Packでは、エンタープライズ向けに6種類の製品を提供

Security

- ✓ Kibanaの認証
- ✓ Kibanaの通信暗号化
- ✓ AD/LDAP認証連携
- ✓ API監査
- ✓ ドキュメント暗号化

Monitoring

- ✓ Elasticsearchクラスタの性能情報
- ✓ Kibanaの性能情報
- ✓ Logstashの性能情報

Reporting

- ✓ ダッシュボードのレポート化(PDF等)
- ✓ Alertingと組み合わせたレポートのスケジュール通知

Alerting

- ✓ データの変化を検知
- ✓ 多種多様な通知方法

Graph

- ✓ データの関連性を可視化

Machine Learning

- ✓ 教師無し機械学習によるデータ分析
- ✓ 時系列異常検知
- ✓ はぐれ者検知
- ✓ 稀有な非構造メッセージ検知

今回利用した製品

elastic

今回の技術検証で活用したElasticプロダクト

Kibana、Elasticsearch、Logstash、MachineLearing(機械学習)を活用

elastic