SIOS

Elasticって何ができるの？

-全文検索から監視・セキュリティまでを支えるデータ基盤-

サイオステクノロジー株式会社

よくある現場の課題

- 社内データが多すぎて、必要な情報が見つからない
- ログが分散し、障害時の原因特定に時間がかかる
- セキュリティインシデントの兆候を“後から”気づく
- 複数ツールを行き来し、分析に時間がかかっている

皆さんの現場でも、こうした悩みはないでしょうか？

データはあるけど活用しきれない。Elasticはそのボトルネックを解消します。

Elastic Platformとは？
検索・分析・可視化のすべてを1つで実現

Elastic Platform（以下、Elastic）は、あらゆるデータをリアルタイムで検索・分析・可視化し、ビジネスに不可欠なインサイトをもたらす統合プラットフォームです。オープンで柔軟、AIに対応した単一のプラットフォームとして、データへのアクセスと活用を加速します。
構成要素「Elastic Stack（旧ELK Stack）」は以下の4つから成ります

- **Elasticsearch： 高速な検索・集計エンジン**
- **Kibana： 可視化・ダッシュボード作成**
- **Logstash： データ取り込み・変換**
- **Beats： 軽量なデータ収集エージェント**

データ収集から保存、可視化までがこのスタックで完結します。

Elastic Stackの構成 – 検索・収集・可視化を1つの仕組みで

Elasticは、4つの主要なコンポーネントから構成されます。

◆ Elasticsearch

全文検索・分析エンジン。構造化／非構造化データをミリ秒単位で処理。
リアルタイム集計・フィルタ・ランキングも可能。

◆ Kibana

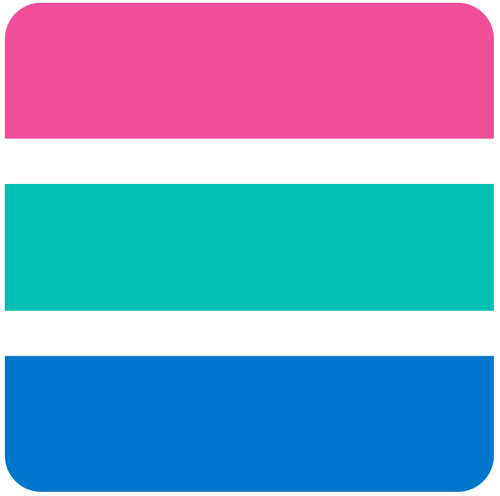
ダッシュボード・可視化ツール。検索結果をグラフ化・アラート設定。
セキュリティ監視・トレンド分析も対応。

◆ Logstash

多様なデータソースを一括集約し、整形・フィルタリングしてElasticに送信。
ETL的な前処理を担う柔軟なデータパイプライン。

◆ Beats

軽量データ収集エージェント。Filebeat（ログ）、Metricbeat（CPU等）、
Packetbeat（トラフィック）など、用途別に複数種類あり。



Elasticで“できること”

📊 ログ分析
システムログやアプリログを統合して可視化
→ 障害の検知と原因特定を迅速に

🔍 社内検索（Search AI Platform）
ナレッジ、議事録、ファイルなどの横断検索
→ コールセンター・情報共有に効果

🛡️ セキュリティ監視（SIEM）
社内ネットワークやクラウド環境の脅威を
リアルタイム検知
→ SOC業務の効率化／XDR対応

📈 業務データの可視化
売上、アクセス、アプリ使用状況などを見える化
→ データドリブンな意思決定を支援

Elasticの用途は非常に広く、業務データの分析や社内検索など、
企業全体の情報活用基盤としても導入が進んでいます。

Elasticの3大ソリューション

Elasticは、Elastic Stackをベースに3つのソリューションを提供しています。

🔍 Search AI Platform

圧倒的なスピードとAIで、必要な答えを検索。

📈 Observability

アプリ・システム・インフラの全体を可視化。
リアルタイムに状態監視・分析が可能。

🛡️ Security（SIEM/XDR）

ログ・ネットワーク・エンドポイントを統合的に監視。
サイバー攻撃をリアルタイムに検知・対応。

Elasticは「どこにでも使える検索エンジン」だけでなく、
ビジネス課題に直結した3つの領域に、特化したソリューションを用意しています。

Search AI Platform：情報を“探す”時間を削減

ElasticのSearch AI Platformは、旧Enterprise Searchの機能を継承し、
さらにAIを統合した次世代の検索基盤です。

- 社内文書、PDF、議事録、ナレッジを一括検索
- Google Drive、Slack、SharePointなどとも連携可能
- 自然言語処理（NLP）を活用した関連性の高い結果表示
- Webサイトやアプリの内蔵検索にも対応（App Search）

仕事の約30%は「情報を探す時間」と言われています。
Search AI Platformを導入することで、知識・ナレッジの再活用が加速し、
生産性が大きく向上します。

Observability：アプリ・システムの状態を“見える化”

ElasticのObservabilityは、アプリケーションやインフラの稼働状況を
リアルタイムに可視化します。

- ログ、メトリクス、APMトレースを統合的に可視化
- ボトルネック、レスポンス遅延の自動検知
- SLA違反や異常状態をリアルタイムにアラート
- Kubernetesやクラウド環境にも対応

Observabilityなら、
すべてのテレメトリデータを一元管理し、システム全体の状態を“今”把握できます。

Security：セキュリティ脅威をリアルタイムに可視化・対処

Elastic Securityは、SIEMおよびXDRの機能を提供し、組織全体の
セキュリティ監視を強化します。

- 組織内外のあらゆるセキュリティイベントを一元管理
- MITRE ATT&CKに基づく脅威検出ルールを搭載
- エンドポイントからクラウド、ネットワークまでカバー
- 脅威の自動検知・アラート、迅速なトリアージ対応

Elasticならログ管理と統合されており、 拡張も自在です。
攻撃の“兆候”を見逃しません。

Elasticを導入するメリット

✅ **圧倒的な検索性能**
→ 数百万件でもミリ秒単位で高速検索／集計が可能

✅ **あらゆるデータに対応**
→ 構造化／非構造化、ログ、ドキュメント、メトリクスなど柔軟に取り込み可能

✅ **スケーラビリティと拡張性**
→ 小規模から始めて、段階的に拡張・自動化が可能

✅ **一気通貫の統合プラットフォーム**
→ 分析・監視・可視化を1つでカバーし、ツール間の連携コストを削減

まとめ

📌 Elasticは、「検索・可視化・監視・セキュリティ」を一気通貫で実現できる統合プラットフォームです。
📌 多様な業界・業務課題に柔軟に対応し、スモールスタートも可能です。

データを活かす仕組みとして、Elasticをぜひご検討ください。

無料トライアル等まずはお気軽にご相談ください。
サイオステクノロジー株式会社
DXSL
Email：elastic-sales@sios.com
お問合せフォーム：https://mk.sios.jp/inquiry-ela


SIOS