

日程	項目	講義形式	所用時間	実施概要	学習目標	目次
3/3	Elastic Stack入門講義	座学+実技	3h	全文検索エンジンという印象の強いElasticsearchですが、データ分析のユースケースとして活用されることが増えてきたElastic Stackについて、各プロダクトの役割や機能について座学形式で解説します。	Elasticsearchというプロダクト名は聞いたことがあるが、Elastic Stack全体像を理解していない人に対して、Elastic Stackにはどんなコンポーネントがあり、それぞれのコンポーネントでどんなことが出来るのかを理解してもらうことを目標としています。 また簡単にElasticsearchの検索機能について、実際にDev ToolsのConsoleからAPIを叩いて頂き、検索結果の違いを体感して頂くことも目標としています。	<ul style="list-style-type: none"> <li>・ Elastic概要</li> <li>・ Elasticsearchとは</li> <li>・ Kibanaとは</li> <li>・ Beatsとは</li> </ul>
3/3	Kibana入門講義・演習 (Kibanaデモ講義)	座学+実技	1h	Kibanaの基礎レベルの内容を、座学・演習を通じて学びます。Kibanaへのデータ登録方法からIndexPath登録方法、可視化方法まで一通りの操作をカバーします。	単にKibanaのいくつかの機能が触れるだけではなく、Kibanaは主に時系列データの可視化・分析に向いているため、ElasticsearchのAggregationとVisualizeの関係など背景についても理解しながら各自がデータ特性をふまえて分析の目的に沿ったDashboardを作れるようになることを目指します。	<ul style="list-style-type: none"> <li>・ Kibana概要</li> <li>・ Kibanaの具体的な利用方法</li> </ul>
3/10	Elasticsearchクラスタ構築講義	座学+実技	4h	複数ノードからなるElasticsearchクラスタの構成と設定について座学・演習を通じて理解します。 インフラ環境や非機能要件に合わせたクラスタ設計・設定をポイントを学び、演習を通じて体験します。	実運用における非機能要件からElasticsearchクラスタの構成をデザインし、設定・実装が行えることを目標にします。 また、Securityモジュールや環境ごとのplugin導入など実環境で利用するトピックも演習に組み込み、最終的にはLogstash/Beatsとも連携させて、フルデザインのElasticStackを構成できることを目指します。	<ul style="list-style-type: none"> <li>・ Elasticsearchクラスタの概要</li> <li>・ Elasticsearchクラスタ管理の応用</li> <li>・ Elasticsearchクラスタトラブルシュート</li> <li>- クラスタ障害時のふるまいと復旧対応</li> </ul>
3/17	Elastic Stack運用講義	座学+実技	4h	Elastic Stackを運用していく上で必要なシステム監視、バックアップ、メンテナンス、障害対応、インデックス管理について、Kibanaでの操作も交えながら解説していきます。また、ベーシックレベルで利用できる運用のための便利機能についても紹介していきます。	Elasticsearchをはじめ、Elastic Stackとして運用していく中で必要となる運用業務をベースに考え方や実施方法、利用できる機能について身に付けて頂くことを目標としています。	<ul style="list-style-type: none"> <li>・ Elastic Stackにおける運用業務</li> <li>・ システム監視</li> <li>・ バックアップ</li> <li>・ メンテナンス</li> <li>・ 障害対応</li> <li>・ インデックス管理</li> </ul>
3/24	ElasticStack応用講義 (Kibana高度なビジュアライズ講義)	座学+実技	4h	実環境におけるログ管理・分析やSIEM、k8sコンテナ基盤における監視といったユースケースに対応できるようにするために必要なElasticStackの高度な内容について学びます。	Kibanaの機能について目的に応じて適切な機能を選択できるようになり、基本的な操作を体験すること、また、ObservabilityやElastic Common Schemaといった比較的新しいElasticStackの概念・ユースケースの背景・目的を理解し、演習を通じて構成・実装できることを目標とします。	<ul style="list-style-type: none"> <li>・ Kibanaの高度なVisualize</li> <li>・ ElasticStack Observability (コンテナワークロードの監視)</li> <li>・ ログ管理の高度なトピック</li> </ul>
宿題	Elastic Stack入門講義 (Logstash/Beatsによるデータ加工講義)	宿題	-	シングルノードクラスタのElasticsearchに対して、Filebeatを利用して、ログの取り込みを行います。1. ログの加工が全くされていない状態のログ、2. Filebeat Modulesを利用して定型パーサによって加工された状態のログ、3. Filebeat Modulesでは対応できずLogstashを用いて加工された状態のログの違いをKibanaのDashboardを通して、確認します。分析に必要な形でデータを用意することの難しさと重要性をElastic Stackを通して、実機上で体感頂きます。	Elastic Stackがインストールされた環境から実際にログを取り込み、分析した形にKibanaで可視化することを目標としています。 エンタープライズで利用することを前提に必要な最低限のセキュリティ機能の実装も行います。	<ul style="list-style-type: none"> <li>・ ハンズオン環境の説明</li> <li>・ Elastic Stackの初期設定</li> <li>・ Beatsによるログ取得</li> <li>・ Logstashによるデータ加工</li> <li>・ Kibanaによる可視化</li> </ul>