

官公庁向けElasticsearch トレーニングのご案内

データセンターのインフラ監視に向けたElasticsearchの学習コースをご案内します。
トレーニングメニューの詳細は、p.2~3をご覧ください。

| # | コース | トレーニングメニュー | 受講者レベル | 学習目標 |
|---|------------------|--|--|---|
| 1 | 初級者コースA (2日間) | 1.Elasticsearch基礎 2.データ取込と画面作成 | Elasticsearchに触れたことが無い方で、監視業務従事者のうち、監視基盤の運用に関わらない方向けの講座です。 | Elasticsearchの構築からデータ取込、蓄積、画面作成、簡易なデータ参照操作スキルを習得します。 |
| 2 | 初級者コースB (3日間) | 1.Elasticsearch基礎 2.データ取込と画面作成 3.監視設定と運用準備 | Elasticsearchに触れたことが無い方で、監視業務従事者のうち、監視の運用に関わる方向けの講座です。 | Elasticsearchの構築、データ取込、蓄積、画面作成、データ参照操作に加え、アラート設定や監視基盤のモニタリング手法を習得します。 |
| 3 | 中級者コース (2日間) | 4.インフラ監視の高度化① 5.インフラ監視の高度化② | Elasticsearchを利用しており、基本的なデータ取込や画面作成ができる方向けの講座です。 | データの加工手法やAgentを使った、より高度なインフラ機器監視に必要なスキルを習得します。 |

官公庁向けElasticsearch トレーニングメニュー（初級者コース）

1. Elasticsearch基礎

午前の部

- **Elasticsearchの説明**
- **Elasticシステム概念**
 - システム構成と構成モジュール
 - 各Elasticノードの役割・用語の説明
 - 処理の流れ（Beats>Logstash>Elasticsearch）
- **ライセンス種類でできることの違い**
- **研修の進め方**
- **研修の範囲とゴール**
- **Elastic環境構築**
 - Elasticsearch、Kibana、Beatsの構築と初期設定
 - 演習

午後の部

- **インデックスの考え方**
 - インデックスとシャード
 - データライフサイクルとData Stream
 - インデックスの設計方法（設定／型定義）
 - インデックスの作成
 - 演習
- **データ取込基礎編**
 - データ収集とデータ加工
 - FilebeatによるSyslogの取込み
 - 取込み済みログの検索（DISCOVER）
 - 演習

2. データ取込と画面作成

午前の部

- **データ取込応用編 その1**
 - Logstashの構築と初期設定
 - ログのパース処理
 - データ取込のデバッグ方法
 - 取込済みログの後処理
 - 演習

午後の部

- **データ取込応用編 その2**
 - Metricbeatによるメトリクスの取込み
 - AuditBeatによるログ取込み
 - インテグレーションの紹介
 - インテグレーションドキュメントの参照方法
 - FleetServer（Elastic Agent）の構築
 - 演習
- **Kibanaによる画面作成**
 - 画面とデータの関係
 - DataViewの作成
 - Lensによるグラフの作成
 - ダッシュボードと検索フィルター設定
 - ドリルダウンの設定
 - 演習
 - その他グラフの紹介

3. 監視設定と運用準備

午前の部

- **アラート設定**
 - 通知の種類
 - 閾値によるアラートの設定
 - 演習
- **機械学習ノード構築**
 - 機械学習でできること
 - 機械学習ノードの構築と初期設定
 - 演習

午後の部

- **アノマリー検知と未来予測**
 - 異常値検出時のアラート発報
 - 演習
- **その他設定**
 - ユーザ管理
 - ロール管理
 - スペース設定
 - セキュリティ設定
 - バックアップ設定
- **監視基盤のモニタリング**
 - アプリケーションログ
 - 監査ログ
 - 監視基盤の状態監視

※各メニュー内のお時間は進み具合により多少前後する可能性があります。

官公庁向けElasticsearch トレーニングメニュー（中級者コース）

4.インフラ監視の高度化①

午前の部

- ・研修の進め方
- ・研修の範囲とゴール
- ・Elastic環境構築
Elasticsearch、Kibana、Beatsの構築と初期設定
演習
- ・効率的な監視に向けて必要なこと
- ・データ取込 上級編
インデックス設計
マスターデータの結合
任意項目の切り出し
不要データのフィルタリング

午後の部

- ・データ取込 上級編
演習
- ・画面作成 上級編
監視用ダッシュボードの作成
MAPレポートの作成
演習

5.インフラ監視の高度化②

午前の部

- ・インテグレーション
環境構築
Fleet
Elastic Agent
NetFlowAgent

午後の部

- ・NetFlow情報の取込
- ・NetFlow
画面の見方
- ・アラート設定（座学・演習）
通知の種類
閾値によるアラートの設定
演習
- ・機械学習ノード構築（座学・演習）
機械学習でできること
機械学習ノードの構築と初期設定
演習
アノマリー検知と未来予測
異常値検出時のアラート発報
演習

※各メニュー内のお時間は進み具合により多少前後する可能性があります。

トレーニング受講にあたって

学習形態／料金

■ 学習形態

- ・ 5名1セットでの対面形式での開催となります（場所は当社オフィス（横浜または田町））。
- ・ 受講時間は、10：00～17：30（お昼休憩時間含む）です。

■ 料金

- ・ 各コースの提供価格については、お問合せください。

トレーニングメニューの詳細内容は変更が生じる場合があります。
内容は2025年4月1日時点のものです。

本件お問い合わせ先

NTTテクノクロス株式会社

ビジネスイノベーション事業部

Elasticsearch製品担当

E-mail : elastic.info-ml@ntt-tx.co.jp

製品URL : <https://www.ntt-tx.co.jp/products/elastic/>

本資料ご使用上のお願い

- ◆ NTTテクノクロス株式会社による許可なく、それらの情報の一部または全文を使用または公開することは、いかなる場合も禁じます。
- ◆ 本資料の著作権は弊社または弊社が許諾を行った権利者に帰属しています。
- ◆ 記載されている商品名、会社名等の固有名詞は各社の登録商標、および、商標です。