

異常検知における ローカルLLMの使いどころ

ご購入はこちら

氏森 充

リスト1 事前学習なしでセンサ時系列データの異常を検知した例（詳細は第3章で紹介）

LLM分析結果：
分析結果は以下の通りです。

- 正常または異常を判定する：
 - * [1] - [5]、[7] - [9]、[11] - [13] は正常なパターンです。
 - * [6]、[8]、[10]、[14]、[15]、[16] は異常なパターンです。
 - * [17] - [19] は危険なパターンです。
- 異常なパターン・トレンド：
 - * 温度が急激に上昇する傾向があります。特に [6]、[8]、[10]、[14]
 - * 振動も異常なパターンを示しています。特に [17] - [19] の場合、振
- 予測される故障モードと推奨メンテナンス時期：
 - * 温度が急激に上昇する傾向があるため、予測される故障モードは軸受の故
 - * メンテナンス時期としては、[6]、[8]、[10]、[14]、[15]、[16]
- リスクレベル：
 - * 正常：[1] - [5]、[7] - [9]、[11] - [13]
 - * 注意：[6]、[8]、[10]、[14]、[15]、[16]
 - * 警告：[17] - [19]
 - * 危険：[20]

注：リスクレベルは個々のデータポイントに基づいて評価されます。

ローカルLLM (Large Language Models, 大規模言語モデル) を異常検出に利用する主なメリットは、セキュリティとリアルタイム性の確保、LLM特有の高度な分析能力にあります。特に機密性の高いデータを扱う産業（製造業，金融，医療）や，即時応答が必要なエッジ環境において有効です。

生産設備の故障やシステム・ログの監視，サイバー攻撃の検知など，多岐にわたる分野への導入が進んでいます。

● トライすること

本編ではローカルLLMを利用した異常検知にトライします。

第1章：どんな用途に向くのか

第2章：どんな検出方法があるのか

第3章：実装1…事前学習なしで異常を判断する（リスト1）

第4章：実装2…テキストを数値ベクトル化して類似度を計算し高精度な異常判定を行う（リスト2）

基礎知識

● LLMを異常検知に使うことで期待できる効果

LLMは，従来の統計的手法や機械学習モデルと比較して，文脈理解能力を生かした高度な推論や，自然言語による説明生成を行える点が強みです。具体的には，次のような応用が期待されています。

- 異常候補の要約：多様なログやアラートを整理し，要点を自動抽出する
- 原因仮説の提示：観測された現象から，可能性の高い原因を推定する
- 対応手順の自動生成：過去の事例やドキュメントを参照し，対応プロセスを提示する
- 未知異常の検出と解釈支援：既存ルールにない異常を浮かび上げらせ，人間の判断を補助する

● ローカルでもLLMを使える環境が整ってきた

当初はクラウド型LLMを利用した事例が主流でしたが，プライバシー保護や通信遅延，運用コストといった課題が指摘されていました。近年ではLlamaやMistralなど，ローカル環境で実行可能なオープン・

リスト2 ネットワーク・パケットの異常を検知した例（詳細は第4章で紹介）

src_ip	dst_ip	port	protocol	packets	bytes	label	predicted_label	is_correct
192.168.1.30	10.0.0.5	443	SSH	175	65662	normal	normal	TRUE
192.168.1.30	8.8.8.8	443	DNS	123	37657	normal	normal	TRUE
...	...	...	...	...	...	...	...	...
192.168.1.29	172.217.31.142	22	HTTP	85	55517	normal	normal	TRUE
192.168.1.24	185.220.102.165	051	TCP	6170	3938128	anomaly	anomaly	TRUE
192.168.1.44	8.8.8.8	53	SSH	264	5112	normal	normal	TRUE
...	...	...	...	...	...	...	...	...
192.168.1.70	8.8.4.4	3306	SSH	94	80060	normal	normal	TRUE
192.168.1.60	multiple	445	NetBIOS	12891	396278	anomaly	anomaly	TRUE

異常