システムの異常予兆を検知するリアルタイム監視ソリューション

Real-time Monitoring Solution to Detect Symptoms of System Anomalies

● 花森利弥　　● 西村利浩

あらまし

従来，システムの異常検知は，しきい値やルール設定により行われてきた。しかし，システムが多様化し解析対象が膨大かつ複雑化した現在においては，監視するパラメーターが多過ぎ，人間がそれらの関係性を把握することは不可能になってきている。また，そうした関係性をデータ分析によって把握するためには，高度な専門知識が必要となり，それがデータ活用が進まない一因となっている。この問題を解決するために富士通が開発した予兆監視ソリューションは，正常時の稼働データを機械学習し，「いつもと違う状態」を自動的に検知する異常予兆検知モデルを，対象データの絞込みから異常原因の特定に至るまでのプロセスと一体で提供する。これにより，高度な分析ノウハウを必要とすることなく，現場レベルでシステムの異常予兆を高精度かつリアルタイムに捉えられるようになる。

本稿では，ICTシステムのダウンや製造業における製造設備の故障による製造ラインの停止など，システムの異常予兆をリアルタイムに監視可能とするソリューションを紹介する。

Abstract

Conventionally, system anomaly detection has been based on setting thresholds and rules. Today, as systems have diversified and the targets of analysis have become enormous in volume and complicated, there are too many parameters to monitor and it is becoming impossible for humans to grasp the relation between them. In addition, resolving these issues with data analysis requires advanced expertise, which is one factor that hinders data utilization. Fujitsu's symptom monitoring solution provides a model to detect anomaly symptoms. In it, the results of machine learning of operation data in normal times is used to automatically detect any "state different from usual," and that step is combined with the process of narrowing down the target data to identify the cause of the anomaly. This allows high-accuracy and real-time detection of anomaly symptoms at the site level without requiring advanced analysis know-how. This paper presents a solution that allows real-time monitoring of symptoms of problems such as information and communications technology (ICT) system failures and suspension of a manufacturing line due to failure of operating equipment in the manufacturing industry.

ま え が き

海外におけるIndustry 4.0やIndustrial Internetに代表されるIoT（Internet of Things）およびビッグデータを活用した新たな産業革命は，国内でも製造業を中心としたM2M（Machine to Machine）や機器の高度化，工場の高度化，ヒトの行動可視化などに適応する機運を盛り上げている。

これらの実現に向け，異常監視の方法も属人的な知見によるしきい値設定から，収集済みのデータや新たに設置したセンサーのデータを組み合わせた機械学習などの高度な分析技術の適用に変わりつつある。例えば，ICTシステムにおいては，サーバの稼働状況の推移を学習することで，運用監視対象のメッセージが出力されないサイレント故障の兆候を捉え，システムダウンのようなトラブルを未然に防ぐことができる。また，製造ラインに掛かる荷重，温度，電流値の変動の相関関係を分析することで，異常な状態をいち早く検知できる。これによりライン停止につながる重大な影響が出る前にメンテナンスが可能となり，自社を含むサプライチェーンの安定稼働を実現できる。

このように，大量に発生するデータをリアルタイムに分析し異常を検知するには，主流になりつつあるApache Sparkなどのインメモリ型のビッグデータ処理と高度な機械学習による分析を融合することが有効である。更に，得られた分析結果を実業務へ即座に適用し，結果の是非を常にフィードバックするサイクルを構築することが成功の鍵となっている。

課　　題

昨今，様々な分析用のツールが無償のOSS（Open Source Software）として提供されたり，クラウド上で安価に利用できる形態で提供されたりしている。しかし，いざ機械学習を利用した分析モデルを開発しようとすると，分析に関する高度なノウハウを有するデータサイエンティストやデータアナリストなどと呼ばれる専門家が必要となる。これが，現場部門でのデータ活用が進まない主要な要因の一つである。

また，リアルタイム型のビッグデータ処理は，蓄積型に比べてデータが過剰に投入された場合のフロー制御方法やデータ処理を行うアプリケーションがダウンした際の再開方法など，データを整合させながらスループットや検知レスポンスを確保する方式が複雑である。これらは，単にプロダクトを組み合わせただけでは実現することが困難である。そのため，検知タイミングは遅れるものの，リアルタイム型ではなくバッチ型でデータを処理するケースもある。

更に，分析の投資対効果が不明確な状況で，これらデータ分析のスキームやビッグデータの処理システムの構築に多額の投資を行うことを顧客側は躊躇（ちゅうちょ）することが多い。こうした理由から，高度な分析ノウハウを必要とせず安価なスモールスタートから始め，効果を確認しながら徐々に適用範囲を拡大できるデータ活用のアプローチが求められている。

予兆監視ソリューション

富士通は，現場部門でのビッグデータの効果的な利活用を実現する統合ソリューションとして，FUJITSU Business Application Operational Data Management & Analytics（ODMA）[(1)]を開発した。そのソリューションの一つとして提供する「ODMA予兆監視」では，正常時の稼働データから機械学習により高精度な異常予兆検知モデルを自動生成する技術と，本技術を簡易に利用するためのデータの抽出や可視化を行うツールを含めた，分析に必要な一連の作業プロセスを体系化している。生成した異常検知モデルは，Apache SparkやElasticsearchといったOSSをベースに富士通の運用ノウハウを加えたリアルタイム処理基盤上で実行可能な状態で提供されるため，すぐに運用を開始できる。これらにより，短期間で導入から効果の確認まで行える。

なお，ODMA予兆監視に含まれる予兆検知モデルを自動生成する技術は，富士通が培ったAI（Artificial Intelligence）技術を体系化して発表した「Human Centric AI Zinrai（ジンライ）」[(2)]の構成要素である機械学習機能を実装したものである。

ソリューションの構成

ODMA予兆監視では，お客様の目的に沿った柔軟なサービスを提供できるよう，以下の3階層構造

でソリューションを提供する（**図-1**）。

（1）ストリーミングデータ処理基盤

データの収集，加工，ストリーミング処理，検知，判断といった基本的な機能を，共通の運用やセキュリティのもとに利用できる。大量のデータに対応できるインメモリ処理，並列分散処理の実行基盤を含んでいる。

（2）分析ライブラリ

取り扱うデータのモデル，アノマリ検知（教師なし学習）や予測分析（教師あり学習）といった分析モデル，画面に表示するためのUI部品をライブラリとして取り揃える。

（3）テンプレート

リアルタイムなデータの可視化，検知した異常を通知するダッシュボード，工場の稼働状況の俯瞰など，用途に合わせてカスタマイズし，すぐに使用できる。

分析ライブラリに含まれる分析モデルは，多様な分析手法の中から有効なものを随時取り入れていくことになる。またテンプレートは，お客様の業種などに応じて随時増やしていくことになる。以降の章では，ソリューションの共通基盤となるストリーミングデータ処理基盤と，最初に提供する分析モデルであるアノマリ検知機能について説明する。

ストリーミングデータ処理基盤

ストリーミングデータ処理基盤は，オープンテクノロジーをベースに「分析フロー」と「運用ノウハウ」を統合・型決めした使いやすいフレームワークとして提供する（**図-2**）。

処理の中心には，インメモリ型で並列分散処理ができるApache Sparkと，その上でストリーミング処理を可能とするSpark Streamingを採用している。データ量に応じたスケーリングを可能にするとともに，受信データをリアルタイムに加工・整形して分析するまでの一連の処理を，JavaやSQLなどの開発で蓄積したノウハウを活用して実現できる。

また，受信データや分析結果データのリアルタイムな可視化にはElasticsearchとKibanaを採用し，柔軟なダッシュボードの作成を可能としている。ODMA予兆監視では，これらのOSSにデータ保証やセキュリティといった非機能要件を含む運

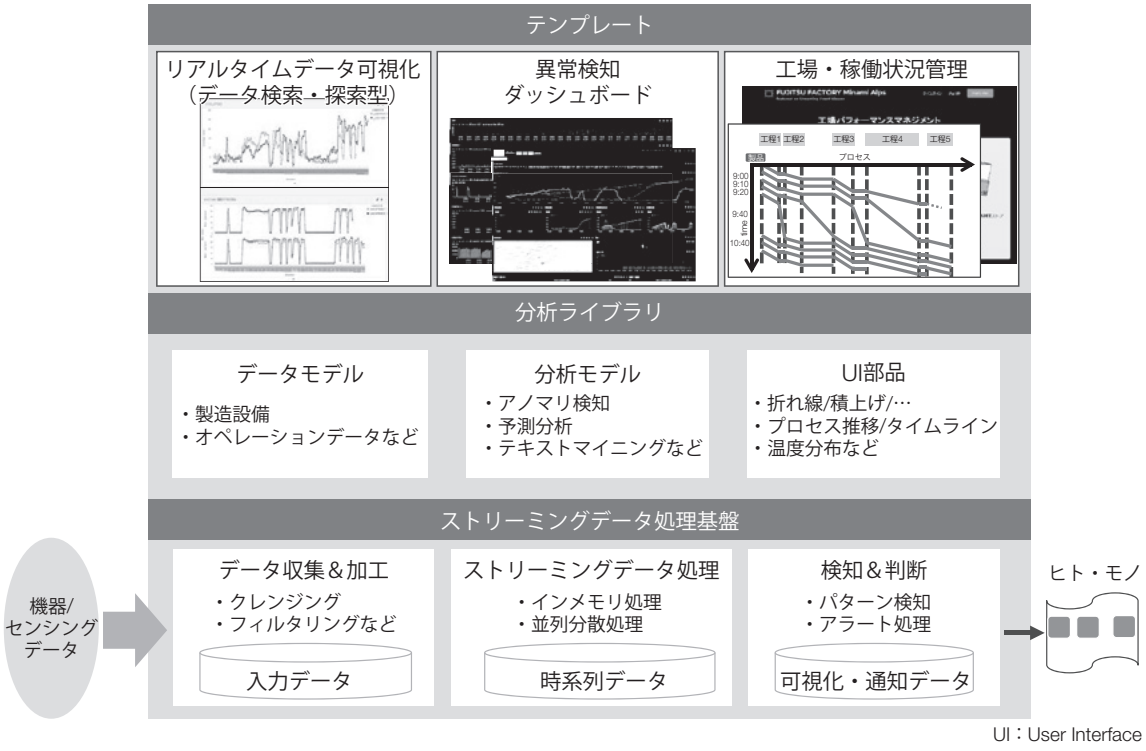

図-1　ODMA予兆監視ソリューションの構成

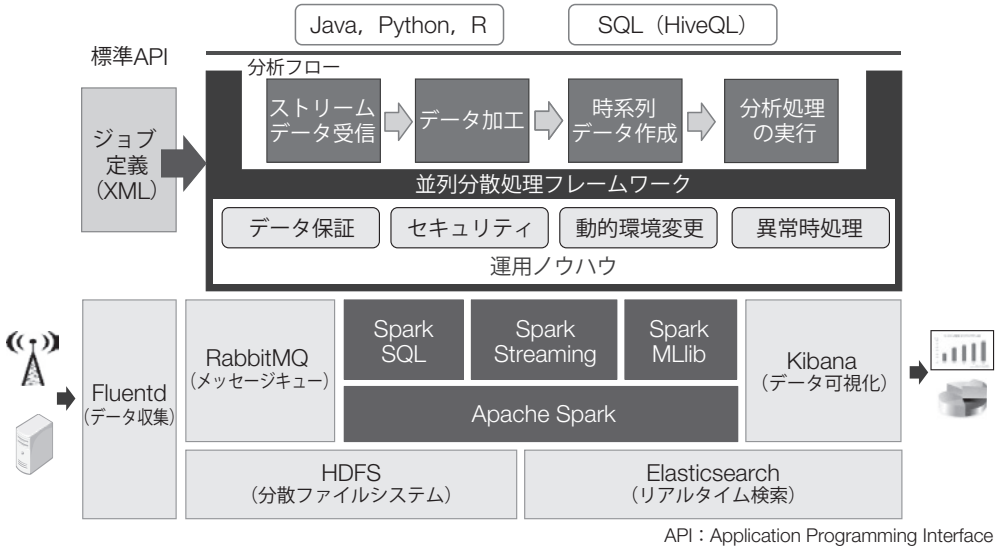

図-2　ストリーミングデータ処理基盤

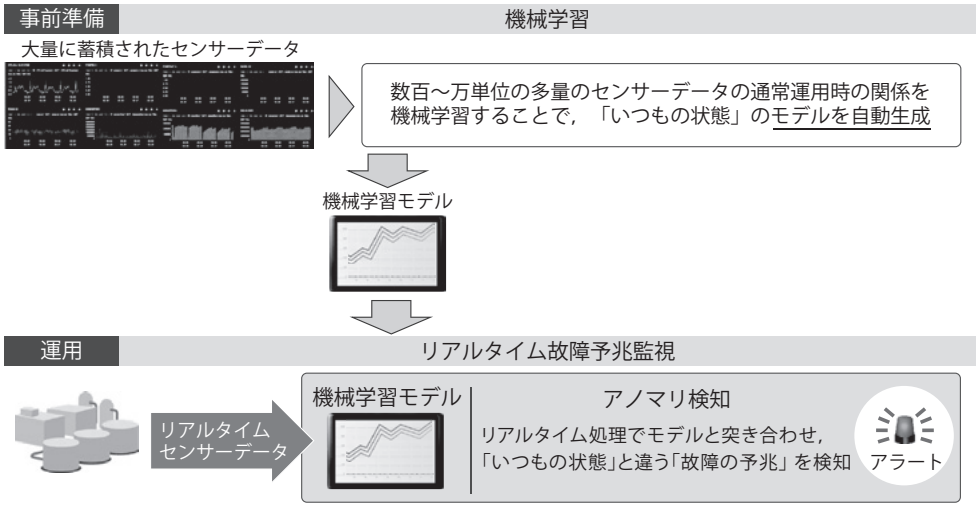

図-3　アノマリ検知機能

用ノウハウを組み込んで提供する。

アノマリ検知機能

「アノマリ」という言葉は「いつもと違う状態」を意味している。「いつもと違う状態」は必ずしも異常というわけではないが，異常につながる可能性のある状態と考えることができる。

アノマリ検知機能が取り扱うことのできるデータは，一定間隔の時系列の数値データである。対象とする全てのデータが必ずしも一定間隔で計測されたものでなかったり，データの欠損などがあったりする場合，アノマリ検知機能にデータを入れる前段階で，そういったデータの補間操作が必要である。その操作は，前述のストリーミングデータ処理基盤を使うことで可能となっている。

アノマリ検知は，事前準備と運用の二つのフェーズに分かれている（**図-3**）。事前準備のフェーズでは，蓄積されたデータを「いつもの状態」として機械学習（事前学習）し，そのモデルを生成していく。データ間の相関を含む各種情報を基に，蓄積データの各時刻におけるシステム全体の状態を決め，各状態の生起確率や遷移確率などを計算する。

運用のフェーズでは，リアルタイムに入力されてくるデータを「いつもの状態」のモデルと突き

合わせることによって，「いつもの状態」との相違の度合いをアノマリスコアという指標として出力する。アノマリスコアは0から1までの値で，0に近いほど「いつもの状態」に近く，1に近いほど「いつもと違う状態」と判断できるものである。リアルタイムに入力されるデータから計算される現時点の状態が，生起確率が低い場合や前時刻の状態からの遷移確率が低い場合に1に近い値となる。

アノマリスコアは，事前学習に利用したデータに依存している。学習データが少ないと，本来はアノマリと言える状態ではないにも関わらず，偶然事前学習データにその状態が含まれていなかったためにアノマリスコアが高く出てしまう可能性もある。アノマリ検知機能にはオンライン学習機能があり，リアルタイムに入力されてくるデータを随時学習できる。オンライン学習はオン/オフすることができ，オンにしておくと最初はアノマリスコアが高く出た状態でも，その状態が何度も出現することによって次第にアノマリスコアが小さくなっていくことになる。また，高いアノマリスコアが出たときに，それが異常であれば今後もアラーム対象とし，正常であれば次回から検知を無効化する機能も検討中である。

実　証　事　例

ストリーミングデータ処理基盤は，これまで以下のようなPoC（Proof of Concept）を通じて得た知見を基に確立してきた。

- FUJITSU Cloud Service IoT Platform[3]で収集されるデータをリアルタイムに加工し，ルールで条件判断し，リアルタイムに可視化
- 船舶の運航時に発生するデータを基に，航路と燃費などの運行状況を表示
- 工場の製造ラインの設備や機器から発生するデータを集め，製造プロセスの進行状況のタイムラインや滞留状況をリアルタイムに可視化

また，アノマリ検知技術については，もともとICT機器の稼働監視をターゲットにサーバの稼働状況に対して適用し，実際にいつもと違う状態の検知に成功している。本稿の執筆時点では，複数のお客様とプラントや工場ラインのセンシングデータを用いたPoCを開始したところである。

む　す　び

本稿では，Operational Data Management & Analytics予兆監視のソリューションを構成する機能と技術について紹介した。

ODMA予兆監視では，まず本稿で説明したアノマリ検知技術を機能として提供するが，予兆検知を含むリアルタイムなデータの分析手法はほかにも様々なものがある。一般的に用いられている分析手法もあれば，富士通研究所独自のものも存在する。そのような技術についても，PoCを行いながらお客様に提供しやすい形で取り込み，分析ライブラリの拡充を図っていく予定である。

ODMA予兆監視は，ビッグデータを処理できるシステムであるが，スモールスタートできることが特徴である。ビッグデータを利活用した異常の予兆検知にご関心をお持ちであれば，是非ご検討いただきたい。

参考文献

(1) 富士通：FUJITSU Business Application Operational Data Management & Analytics.
http://www.fujitsu.com/jp/solutions/business-technology/intelligent-data-services/ba/product/operational-data-management-and-analytics/index.html
(2) 富士通：当社が培ったAI技術を「Human Centric AI Zinrai」として体系化.
http://pr.fujitsu.com/jp/news/2015/11/2.html
(3) 富士通：IoTデータ活用基盤サービスFUJITSU Cloud Service IoT Platform.
http://jp.fujitsu.com/solutions/cloud/paas/iot-platform/

著者紹介

花森利弥（はなもり　としや）
イノベーティブソリューション事業本部情報統合システム事業部 所属
現在，IoTを活用した分析ソリューションの開発に従事。

西村利浩（にしむら　としひろ）
イノベーティブソリューション事業本部情報統合システム事業部 所属
現在，IoTを活用した分析ソリューションの開発に従事。