

(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2025年1月9日(09.01.2025)



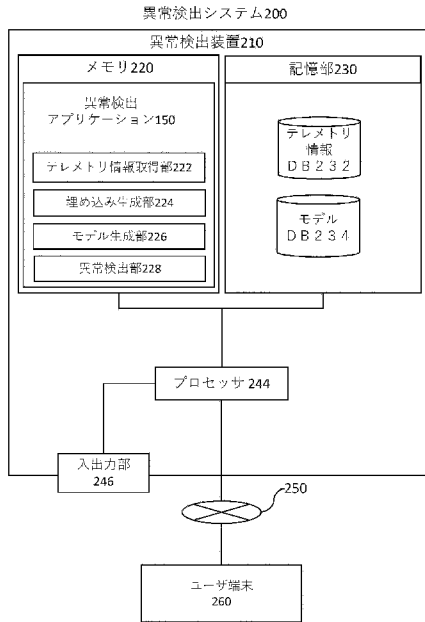
(10) 国際公開番号
WO 2025/009381 A1

- (51) 国際特許分類:
G06F 11/07 (2006.01) *G06N 20/00* (2019.01)
G06F 11/34 (2006.01)
- (21) 国際出願番号: PCT/JP2024/021994
- (22) 国際出願日: 2024年6月18日(18.06.2024)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願 2023-109014 2023年7月3日(03.07.2023) JP
- (71) 出願人: 株式会社日立製作所(HITACHI, LTD.)
[JP/JP]; 〒1008280 東京都千代田区丸の内
一丁目6番6号 Tokyo (JP).
- (72) 発明者: グエン バホン(NGUYEN, Bahung);
〒1008280 東京都千代田区丸の内一丁目6番
6号 株式会社日立製作所内 Tokyo (JP). 相
楽 恭宏(SAGARA, Takahiro); 〒1008280 東京
都千代田区丸の内一丁目6番6号 株式会
社日立製作所内 Tokyo (JP). 永井 崇之(NAGAI,
Takayuki); 〒1008280 東京都千代田区丸の内
一丁目6番6号 株式会社日立製作所内
Tokyo (JP). 水越 裕也(MIZUKOSHI, Hiroya);
〒1008280 東京都千代田区丸の内一丁目6番
6号 株式会社日立製作所内 Tokyo (JP).
- (74) 代理人: 弁理士法人第一国際特許
事務所(DAI-ICHI INTERNATIONAL PATENT

(54) Title: ABNORMALITY DETECTION DEVICE, ABNORMALITY DETECTION SYSTEM, AND ABNORMALITY DETECTION METHOD

(54) 発明の名称: 異常検出装置、異常検出システム及び異常検出方法

[図2]



150 Abnormality detection application
200 Abnormality detection system
210 Abnormality detection device
220 Memory
222 Telemetry information acquisition unit
224 Embedding generation unit
226 Model generation unit
228 Abnormality detection unit
230 Storage unit
232 Telemetry information database
234 Model database
244 Processor
246 Input/output unit
260 User terminal

(57) Abstract: The purpose of this disclosure is to provide an abnormality detection method capable of highly accurate abnormality detection related to a microservice. To achieve the foregoing, an abnormality detection device according to the present disclosure includes: a telemetry information acquisition unit that acquires, from a set of first microservices, first telemetry information including log information, trace information, and metric information; an embedding generation unit that generates a trace embedding corresponding to the trace information, generates a log embedding corresponding to

[続葉有]

OFFICE, P.C.); 〒1010041 東京都千代田区神田
須田町二丁目 8 番地 2 Tokyo (JP).

- (81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.
- (84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, ME, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類：

一 国際調査報告 (条約第21条(3))

the log information, and generates a metric embedding corresponding to the metric information; a model generation unit that generates a machine learning model for abnormality detection that determines whether there is an abnormality in a microservice on the basis of a trace embedding, a log embedding, and a metric embedding; and an abnormality detection unit that uses the machine learning model for abnormality detection to analyze second telemetry information acquired for a set of second microservices, thereby generating abnormality detection results indicating the presence or absence of an abnormality in the second microservices.

(57) 要約：本開示は、マイクロサービスに関する高精度の異常検出が可能な異常検出手法を提供することを目的とする。このため、本開示の異常検出装置は、第1のマイクロサービスのセットから、ログ情報、トレース情報及びメトリック情報を含む第1のテレメトリ情報を取得するテレメトリ情報取得部と、トレース情報に対応するトレース埋め込みを生成し、ログ情報に対応するログ埋め込みを生成し、メトリック情報に対応するメトリック埋め込みを生成する埋め込み生成部と、トレース埋め込み、ログ埋め込み及びメトリック埋め込みに基づいてマイクロサービスについて異常の有無を判定する異常検出用の機械学習モデルを生成するモデル生成部と、異常検出用の機械学習モデルを用いて、第2のマイクロサービスのセットについて取得された第2のテレメトリ情報を解析することで、第2のマイクロサービスにおける異常の有無を示す異常検出結果を生成する異常検出部とを含む。

明 細 書

発明の名称： 異常検出装置、異常検出システム及び異常検出方法
技術分野

[0001] 本発明は、異常検出装置、異常検出システム及び異常検出方法に関する。

背景技術

[0002] 近年、モバイル、SNS、IoT等をはじめ、デジタル技術を活用して、ビジネス環境は大きく変化してしる。また、企業は、顧客のニーズの変化に柔軟に対応することが求められている。

[0003] そのような中、アプリケーション開発を効率化する手法として、いわゆる「マイクロサービスアーキテクチャ」という開発手法が注目を集めている。このマイクロサービスアーキテクチャでは、全ての機能やコンポーネントが1つのコードベースに統合されている従来のモノリシック（一枚板）アーキテクチャとは異なり、アプリケーションが持つ機能が細かい「サービス」に分割され、それぞれのサービスはAPIを通じて連携している。マイクロサービスは、従来のモノリシックなアプローチに比べて、拡張性・柔軟性に優れており、柔軟でスケーラブルなシステムを構築し、効率的なソフトウェアの開発と運用を実現させることができる。

[0004] このようなマイクロサービスアーキテクチャがクラウドコンピューティング、分散システムアーキテクチャ及びCI/CD（Continuous Integration/Continuous Delivery）と共に普及する中、アプリケーションを監視し、異常を検出することが重要となりつつある。そして、アプリケーションに対する異常検出を支援するためには、アプリケーションの挙動やサービス間の相互作用に関する情報として、メトリック、ログ、及びトレースを含むテレメトリ情報を用いることが有用である。

[0005] 例えば、所定の期間においてアプリケーションについて発生したイベントを記録するログを用いて、異常検出を行う手法として、米国特許第9928

1 5 5 号（特許文献 1）が存在する。

特許文献 1 には、「本特許出願には、異種のシステムやアプリケーション、センサ、又は計器からのログデータを処理するためのシステム及び方法が開示されている。これは、任意の未知のシステムやアプリケーションから異種のログを受信し、機械学習を使用して異種のログソースから正規表現のパターンを生成し、ログパターンを抽出する。また、異なる条件に基づいてトレーニングログからモデルやプロファイルを生成し、時間の経過と共に生成された全てのモデルを格納するグローバルなモデルデータベースを更新する。さらに、本番システムで実行されている1つ以上のアプリケーション、センサ、又は計器からの生のログメッセージをトークン化し、トークン化されたストリームをデータオブジェクトに変換して異常検出及びログメッセージの異常警告のためにログメッセージを異なる異常検出器に転送する。そして、本番システムで実行されている1つ以上のアプリケーション、センサ、又は計器から異常警告を生成する。」技術が開示されている。

先行技術文献

特許文献

[0006] 特許文献1：米国特許第 9 9 2 8 1 5 5 号

発明の概要

発明が解決しようとする課題

[0007] 特許文献 1 に記載の手段では、アプリケーションの挙動を記録するログデータを用いて機械学習モデルを訓練することで、アプリケーションにおいて発生する異常の挙動を検出する手法が記載されている。

[0008] しかし、特許文献 1 のような従来のログデータに基づく異常検出手法では、ログの意味的特徴、グラフベースの特徴、又はその相互作用は考慮されないため、クラウド環境等のような、複雑且つダイナミックなシステム環境への有効性が限定されてしまう。

[0009] また、実際には、テレメトリ情報は、ログデータのみならず、メトリック及びトレースの情報を含む。グラフ特徴を有するトレースは、サービス間の相互作用を示し、時間的特徴を有するメトリックは、サービス内の依存関係を示すため、アプリケーション全体の挙動に関する洞察を得る観点から、ログデータと共に解析することが望ましい。しかし、ログ、メトリック及びトレースの基本構造の相違により、ログ、メトリック及びトレースを全て考慮する異常検出手法が提供されていない。

[0010] そこで、本開示は、テレメトリ情報におけるログ、メトリック及びトレースのそれぞれの特徴を考慮する機械学習モデルを生成することで、マイクロサービスに関する高精度の異常検出が可能な異常検出手法を提供することを目的とする。

課題を解決するための手段

[0011] 上記の課題を解決するために、代表的な本発明の異常検出装置の一つは、プロセッサとメモリとを備え、前記メモリは、第1のマイクロサービスのセットから、マイクロサービスの挙動を示すログを含むログ情報と、複数のマイクロサービスの関係を示すトレースを含むトレース情報と、マイクロサービスの性能に関する測定値を示すメトリックを含むメトリック情報と、を含む第1のテレメトリ情報を取得するテレメトリ情報取得部と、前記第1のテレメトリ情報から抽出した学習用テレメトリ情報をニューラルネットワークによって処理することで、前記トレース情報に対応するトレース埋め込みを生成し、前記ログ情報に対応するログ埋め込みを生成し、前記メトリック情報に対応するメトリック埋め込みを生成する埋め込み生成部と、前記トレース埋め込み、前記ログ埋め込み及び前記メトリック埋め込みに基づいて、マイクロサービスについて異常の有無を判定する異常検出用の機械学習モデルを生成するモデル生成部と、前記異常検出用の機械学習モデルを用いて、第2のマイクロサービスのセットについて取得された第2のテレメトリ情報を解析することで、前記第2のマイクロサービスにおける異常の有無を示す異常検出結果を生成する異常検出部として前記プロセッサを機能させるための

処理命令を含む。

発明の効果

[0012] 本開示によれば、テレメトリ情報におけるログ、メトリック及びトレースのそれぞれの特徴を考慮する機械学習モデルを生成することで、マイクロサービスに関する高精度の異常検出が可能な異常検出手法を提供することができる。

上記以外の課題、構成及び効果は、以下の発明を実施するための形態における説明により明らかにされる。

図面の簡単な説明

[0013] [図1]図1は、本開示の実施形態を実施するためのコンピュータシステムを示す図である。

[図2]図2は、本開示の実施形態に係る異常検出システムの構成の一例を示す図である。

[図3]図3は、本開示の実施形態に係る異常検出手法の全体の流れを示す図である。

[図4]図4は、本開示の実施形態に係るモデル生成段階におけるモデル生成処理の流れを示す図である。

[図5]図5は、本開示の実施形態に係る異常検出段階における異常検出処理の流れを示す図である。

[図6]図6は、本開示の実施形態に係る異常検出用の機械学習モデルを生成する際の動作の一例を示す図である。

[図7]図7は、本開示の実施形態に係るトレースに対する埋め込みを生成する処理の一例を示す図である。

[図8]図8は、本開示の実施形態に係るメトリックに対する埋め込みを生成する処理の一例を示す図である。

[図9]図9は、本開示の実施形態に係るログに対する埋め込みを生成する処理の一例を示す図である。

[図10]図10は、本開示の実施形態に係る集約層の動作の一例を示す図であ

る。

[図11]図 1 1 は、本開示の実施形態に係る異常検出用の機械学習モデルとして機能するニューラルネットワークの構成の一例を示す図である。

[図12]図 1 2 は、本開示の実施形態に係る異常検出用の機械学習モデルの格納・取得処理の一例を示す図である。

[図13]図 1 3 は、本開示の実施形態に係るモデルDBの論理的データベーススキーマの一例を示す図である。

[図14]図 1 4 は、本開示の実施形態に係る異常検出管理画面の一例を示す図である。

[図15]図 1 5 は、本開示の実施形態に係るクラウドコンピューティング環境の一例を示す図である。

発明を実施するための形態

[0014] 以下、図面を参照して、本発明の実施形態について説明する。なお、この実施形態により本発明が限定されるものではない。また、図面の記載において、同一部分には同一の符号を付して示している。

また、「第1」、「第2」、「第3」等の用語は、本開示において様々な要素又は構成要素を説明するのに用いられる場合があるが、これらの要素又は構成要素はこれらの用語によって限定されるべきでないことが理解されるであろう。これらの用語は、或る要素又は構成要素を別の要素又は構成要素と区別するためにのみ用いられる。したがって、以下で論述する第1の要素又は構成要素は、本発明概念の教示から逸脱することなく第2の要素又は構成要素と呼ぶこともできる。

[0015] (本開示の概要)

本開示の実施形態に係る異常検出手段は、マイクロサービスに関するテレメトリ情報に含まれるメトリック、ログ及びトレースのそれぞれの特徴を捉えた埋め込みに基づいて、テレメトリ情報における異常及び異常の要因を検出することができる機械学習モデルを生成することに関する。本開示の実施形態に係る異常検出手段は、マイクロサービスからテレメトリ情報を取得す

るテレメトリ情報取得処理、取得したテレメトリ情報に基づいて異常検出用の機械学習モデルを生成するモデル生成処理、及びこのように生成した異常検出用の機械学習モデルを用いてマイクロサービスにおける異常を検出する異常検出処理を含んでもよい。

[0016] テレメトリ情報取得処理は、マイクロサービスからテレメトリ情報を取得するための処理であり、例えばログファイル、メトリック及びトレースを取得するLoki（登録商標）、Prometheus（登録商標）及びTempo（登録商標）等の既存の手法によって行われてもよい。

[0017] モデル生成処理は、テレメトリ情報取得処理によって取得されたメトリック、ログ及びトレースのそれぞれの特徴を捉えた埋め込みを用いて機械学習モデルを生成するための処理である。ここでの「埋め込み」とは、メトリック、ログ及びトレースのそれぞれの特徴を低次元空間で表現するデータ構造であり、例えば連続ベクトルやグラフ表現を含んでもよい。埋め込みを生成するための特徴は、例えばPCA（Principal Component Analysis）、Mutual Information、又はSHAP（SHapley Additive exPlanations）等の手法によって選択されてもよい。

[0018] 異常検出処理は、モデル生成処理によって生成された異常検出用の機械学習モデルを用いてテレメトリ情報を解析することで、マイクロサービスにおける異常を検出するための処理である。この異常検出処理では、異常検出用の機械学習モデルは、所定のマイクロサービスにおいて異常が存在する確率を示す異常検出結果を生成し、ユーザに出力してもよい。

[0019] 本開示の実施形態に係る異常検出手段によれば、ログ、メトリック及びトレースにおける特徴を捉えた埋め込みを用いて機械学習モデルを訓練することで、マイクロサービスの様々な側面を考慮した、幅広い異常検出が可能な異常検出用の機械学習モデルを得ることができる。また、本開示の実施形態に係る異常検出手段の一態様では、解析したログ、メトリック及びトレースに基づいて、検出した異常の要因をユーザに通知することができる。

このように、マイクロサービスに関する高精度の異常検出が可能となる。

[0020] 次に、図1を参照して、本開示の実施形態を実施するためのコンピュータシステム100について説明する。本明細書で開示される様々な実施形態の機構及び装置は、任意の適切なコンピューティングシステムに適用されてもよい。コンピュータシステム100の主要コンポーネントは、1つ以上のプロセッサ102、メモリ104、端末インターフェース112、ストレージインターフェース113、I/O（入出力）デバイスインターフェース114、及びネットワークインターフェース115を含む。これらのコンポーネントは、メモリバス106、I/Oバス108、バスインターフェースユニット109、及びI/Oバスインターフェースユニット110を介して、相互的に接続されてもよい。

[0021] コンピュータシステム100は、プロセッサ102と総称される1つ又は複数の汎用プログラマブル中央処理装置（CPU）102A及び102Bを含んでもよい。ある実施形態では、コンピュータシステム100は複数のプロセッサを備えてもよく、また別の実施形態では、コンピュータシステム100は単一のCPUシステムであってもよい。各プロセッサ102は、メモリ104に格納された命令を実行し、オンボードキャッシュを含んでもよい。

[0022] ある実施形態では、メモリ104は、データ及びプログラムを記憶するためのランダムアクセス半導体メモリ、記憶装置、又は記憶媒体（揮発性又は不揮発性のいずれか）を含んでもよい。メモリ104は、本明細書で説明する機能を実施するプログラム、モジュール、及びデータ構造の全て又は一部を格納してもよい。例えば、メモリ104は、異常検出アプリケーション150を格納していてもよい。ある実施形態では、異常検出アプリケーション150は、後述する機能をプロセッサ102上で実行する命令又は記述を含んでもよい。

[0023] ある実施形態では、異常検出アプリケーション150は、プロセッサベースのシステムの代わりに、又はプロセッサベースのシステムに加えて、半導

体デバイス、チップ、論理ゲート、回路、回路カード、及び/又は他の物理ハードウェアデバイスを介してハードウェアで実施されてもよい。ある実施形態では、異常検出アプリケーション 150 は、命令又は記述以外のデータを含んでもよい。ある実施形態では、カメラ、センサ、又は他のデータ入力デバイス（図示せず）が、バスインターフェースユニット 109、プロセッサ 102、又はコンピュータシステム 100 の他のハードウェアと直接通信するように提供されてもよい。

[0024] コンピュータシステム 100 は、プロセッサ 102、メモリ 104、表示システム 124、及び I/O バスインターフェースユニット 110 間の通信を行うバスインターフェースユニット 109 を含んでもよい。I/O バスインターフェースユニット 110 は、様々な I/O ユニットとの間でデータを転送するための I/O バス 108 と連結していてもよい。I/O バスインターフェースユニット 110 は、I/O バス 108 を介して、I/O プロセッサ（IOP）又は I/O アダプタ（IOA）としても知られる複数の I/O インタフェースユニット 112、113、114、及び 115 と通信してもよい。

[0025] 表示システム 124 は、表示コントローラ、表示メモリ、又はその両方を含んでもよい。表示コントローラは、ビデオ、オーディオ、又はその両方のデータを表示装置 126 に提供することができる。また、コンピュータシステム 100 は、データを収集し、プロセッサ 102 に当該データを提供するように構成された 1 つ又は複数のセンサ等のデバイスを含んでもよい。

[0026] 例えば、コンピュータシステム 100 は、心拍数データやストレスレベルデータ等を収集するバイオメトリックセンサ、湿度データ、温度データ、圧力データ等を収集する環境センサ、及び加速度データ、運動データ等を収集するモーションセンサ等を含んでもよい。これ以外のタイプのセンサも使用可能である。表示システム 124 は、単独のディスプレイ画面、テレビ、タブレット、又は携帯型デバイスなどの表示装置 126 に接続されてもよい。

[0027] I/O インタフェースユニットは、様々なストレージ又は I/O デバイス

と通信する機能を備える。例えば、端末インタフェースユニット 112 は、ビデオ表示装置、スピーカテレビ等のユーザ出力デバイスや、キーボード、マウス、キーパッド、タッチパッド、トラックボール、ボタン、ライトペン、又は他のポインティングデバイス等のユーザ入力デバイスのようなユーザ I/O デバイス 116 の取り付けが可能である。ユーザは、ユーザインタフェースを使用して、ユーザ入力デバイスを操作することで、ユーザ I/O デバイス 116 及びコンピュータシステム 100 に対して入力データや指示を入力し、コンピュータシステム 100 からの出力データを受け取ってもよい。ユーザインタフェースは例えば、ユーザ I/O デバイス 116 を介して、表示装置に表示されたり、スピーカによって再生されたり、プリンタを介して印刷されたりしてもよい。

[0028] ストレージインタフェース 113 は、1 つ又は複数のディスクドライブや直接アクセスストレージ装置 117（通常は磁気ディスクドライブストレージ装置であるが、単一のディスクドライブとして見えるように構成されたディスクドライブのアレイ又は他のストレージ装置であってもよい）の取り付けが可能である。ある実施形態では、ストレージ装置 117 は、任意の二次記憶装置として実装されてもよい。メモリ 104 の内容は、ストレージ装置 117 に記憶され、必要に応じてストレージ装置 117 から読み出されてもよい。I/O デバイスインタフェース 114 は、プリンタ、ファックスマシン等の他の I/O デバイスに対するインタフェースを提供してもよい。ネットワークインタフェース 115 は、コンピュータシステム 100 と他のデバイスが相互的に通信できるように、通信経路を提供してもよい。この通信経路は、例えば、ネットワーク 130 であってもよい。

[0029] ある実施形態では、コンピュータシステム 100 は、マルチユーザメインフレームコンピュータシステム、シングルユーザシステム、又はサーバコンピュータ等の、直接的ユーザインタフェースを有しない、他のコンピュータシステム（クライアント）からの要求を受信するデバイスであってもよい。他の実施形態では、コンピュータシステム 100 は、デスクトップコンピ

ュータ、携帯型コンピューター、ノートパソコン、タブレットコンピューター、ポケットコンピューター、電話、スマートフォン、又は任意の他の適切な電子機器であってもよい。

[0030] 次に、図2を参照して、本開示の実施形態に係る異常検出システムについて説明する。

[0031] 図2は、本開示の実施形態に係る異常検出システム200の構成の一例を示す図である。異常検出システム200は、テレメトリ情報におけるログ、メトリック及びトレースのそれぞれの特徴を考慮する機械学習モデルを生成することで、マイクロサービスに関する異常を検出するためのシステムである。図2に示すように、異常検出システム200は、異常検出装置210と、通信ネットワーク250と、ユーザ端末260とからなる。異常検出装置210とユーザ端末260とは、通信ネットワーク250を介して互いに接続されてもよい。

[0032] 異常検出装置210は、テレメトリ情報におけるログ、メトリック及びトレースのそれぞれの特徴を考慮する機械学習モデルを生成することで、マイクロサービスに関する異常を検出する検出するための装置であり、図2に示すように、メモリ220、記憶部230、プロセッサ244及び入出力部246を主に含む。

ある実施形態では、異常検出装置210は、図1に示すコンピュータシステム100によって実装されてもよい。

[0033] メモリ220は、本開示の実施形態に係る異常検出手段の機能を実施するための異常検出アプリケーション150を格納するためのメモリである。この異常検出アプリケーション150は、図2に示すように、テレメトリ情報取得部222、埋め込み生成部224、モデル生成部226及び異常検出部228等のソフトウェアモジュールの機能を実施するための処理命令を含んでもよい。

[0034] テレメトリ情報取得部222は、マイクロサービスに関するテレメトリ情報を取得するための機能部である。ある実施形態では、テレメトリ情報取得

部 2 2 2 は、例えばログ情報、メトリック情報及びトレース情報をテレメトリ情報として取得する L o k i（登録商標）、P r o m e t h e u s（登録商標）及び T e m p o（登録商標）等の既存の手法であってもよい。また、テレメトリ情報取得部 2 2 2 は、取得したテレメトリ情報を記憶部 2 3 0 に格納されるテレメトリ情報 D B 2 3 2 に保存してもよい。

なお、テレメトリ情報取得部 2 2 2 による動作の詳細については後述するため、ここではその説明を省略する。

[0035] 埋め込み生成部 2 2 4 は、テレメトリ情報取得部 2 2 2 によって取得されたテレメトリ情報を処理し、特徴を捉えた埋め込みを生成するための機能部である。ある実施形態では、埋め込み生成部 2 2 4 は、トレース情報におけるサービス関係の特徴、ログ情報における意味的特徴及びログ関係の特徴、並びにメトリック情報における時間的特徴及びメトリック関係の特徴のそれぞれを低次元空間で表現する埋め込みを生成することができる。

なお、埋め込み生成部 2 2 4 による動作の詳細については後述するため、ここではその説明を省略する。

[0036] モデル生成部 2 2 6 は、埋め込み生成部 2 2 4 によって生成された埋め込みを用いて、テレメトリ情報における異常を検出するための機械学習モデルを生成する。ある実施形態では、モデル生成部 2 2 6 は、生成した機械学習モデルを記憶部 2 3 0 に格納されるモデル D B 2 3 4 に保存してもよい。

なお、モデル生成部 2 2 6 による動作の詳細については後述するため、ここではその説明を省略する。

[0037] 異常検出部 2 2 8 は、モデル生成部 2 2 6 によって生成され、モデル D B 2 3 4 に保存されている異常検出用の機械学習モデルを取得した後、当該異常検出用の機械学習モデルを用いてマイクロサービスに関するテレメトリ情報を解析することで、当該マイクロサービスにおける異常を検出するための機能部である。ある実施形態では、異常検出部 2 2 8 は、マイクロサービスに関して検出した異常と、当該異常の要因等に関する情報を示す異常検出結果をシステム管理者等のユーザに提示してもよい。

なお、異常検出部 228 による動作の詳細については後述するため、ここではその説明を省略する。

[0038] 記憶部 230 は、本開示の実施形態に係る各種情報を格納するためのデータベース（以下、「DB」）を収容する記憶領域であり、図 2 に示すように、テレメトリ情報 DB 232 及びモデル DB 234 を含んでもよい。

[0039] テレメトリ情報 DB 232 は、テレメトリ情報取得部 222 によって取得された、マイクロサービスに関するテレメトリ情報を格納するためのデータベースである。ある実施形態では、このテレメトリ情報 DB 232 は、複数のマイクロサービスに関するログ情報、トレース情報及びメトリック情報を含んでもよい。

[0040] モデル DB 234 は、モデル生成部 226 によって生成された、異常検出用の機械学習モデルを格納するためのデータベースである。このモデル DB 234 は、異常検出用の機学習モデルの特性や要件に基づいて選択されるデータベース方式で構成されてもよい。

[0041] プロセッサ 244 は、メモリ 220 によって格納される異常検出アプリケーション 150 の各機能部の機能を規定する処理命令を実施するための処理部である。

[0042] 入出力部 246 は、異常検出装置 210 に入力される情報を受け付けると共に、異常検出装置 210 によって生成される異常検出結果を出力するための機能部である。ある実施形態では、入出力部 246 は、例えばキーボード、マウス、GUI（Graphical User Interface）を表示するディスプレイ等を含んでもよい。ある実施形態では、入出力部 246 は、各種情報の入出力を行う GUI をユーザ端末 260 に提供してもよい。

[0043] 通信ネットワーク 250 は、例えばローカルエリアネットワーク（LAN）、ワイドエリアネットワーク（WAN）、衛星ネットワーク、ケーブルネットワーク、Wi-Fi ネットワーク、又はそれらの任意の組み合わせを含むものであってもよい。

[0044] ユーザ端末260は、異常検出装置210のユーザによって利用可能な端末装置である。ユーザは、ユーザ端末260を用いることで、特定のマイクロサービスに対する異常検出の実行を要求したり、異常検出結果を確認したりすることができる。一例として、ユーザ端末260は、例えばマイクロサービスを管理するユーザのスマートフォン、スマートウォッチ、タブレット、パソコン等を含んでもよく、特に限定されない。

なお、図2では、説明の便宜上、1つのユーザ端末260を含む構成を一例として説明しているが、ユーザ端末260の数は限定されず、複数のユーザ端末260を含む構成も可能である。

[0045] 以上説明した異常検出システムによれば、マイクロサービスに関するログ情報、メトリック情報及びトレース情報等のテレメトリ情報を考慮した、高精度の異常検出が可能となる。

[0046] 上述したように、異常検出装置210は、本開示の実施形態に係る異常検出手段のそれぞれの機能を実現するために、テレメトリ情報取得部222、埋め込み生成部224、モデル生成部226及び異常検出部228等の機能部や、テレメトリ情報DB232及びモデルDB234等のデータベースを含んでもよい。次に、図3を参照して、本開示の実施形態に係る異常検出装置に含まれる機能部やデータベースによって実現され、本開示の実施形態に係る異常検出手段の全体の流れについて説明する。

[0047] 図3は、本開示の実施形態に係る異常検出手段の全体の流れ300を示す図である。異常検出手段の全体の流れ300は、テレメトリ情報に基づいて異常検出用の機械学習モデルを生成するモデル生成段階と、生成した異常検出用の機械学習モデルを用いて所定のマイクロサービスに対する異常検出を行う異常検出段階との2つの段階を主に含む。

[0048] まず、ステップS305では、テレメトリ情報取得部222は、マイクロサービスに関するテレメトリ情報を取得する。ここで、テレメトリ情報取得部222は、例えばログ情報、メトリック情報及びトレース情報をテレメトリ情報として取得するLoki（登録商標）、Prometheus（登録

商標) 及びTempo (登録商標) 等の既存の手法を用いてもよい。

[0049] 本開示では、「メトリック情報」とは、ハードウェア又はソフトウェアの性能を定量的に示す測定値を示すメトリックの集合を含む情報である。ここでのメトリックは、例えば特定の期間におけるCPU使用率やメモリ使用量等を含んでもよい。

また、本開示では、「ログ情報」とは、マイクロサービスにおける特定のコードブロックが実行された時にシステムによって生成されるテキスト形式のログを含む情報である。ここでのログは、例えば実行されたコードブロックの内容を示すテキスト情報と、当該コードブロックが実行された日時を示すタイムスタンプとを含んでもよい。

また、本開示では、「トレース情報」とは、複数のマイクロサービスからなるマイクロサービスエコシステムの異なるコンポーネント間の関係を示すトレースを含む情報である。ここでのトレースは、例えばある処理タスクを実行するためサービスによって呼び出される従属サービスとの関係をグラフ形式で示す関係図であってもよい。

[0050] 次に、ステップS310では、埋め込み生成部224は、現在の処理がモデル生成段階にあるか異常検出段階にあるかを判定する。この判定は、例えばユーザの指示に基づいて行われてもよい。一例として、ユーザは、後述する異常検出管理画面1400において、モデル生成段階又は異常検出段階のいずれかを選択してもよい。

モデル生成段階の場合、本処理はステップS320へ進む。一方、異常検出段階の場合、本処理はステップS340へ進む。

[0051] 現在の処理がモデル生成段階にあると判定された場合、ステップS315では、埋め込み生成部224は、ステップS305で取得されたテレメトリ情報を、機械学習モデルを訓練するための学習セットと、訓練した機械学習モデルをテストするための検証セットとに分割した後、テレメトリ情報の学習セットにおける特徴を抽出し、抽出した特徴に基づいた埋め込みを生成する。ここでの埋め込みは、特徴を抽象化した低次元空間で表現するグラフ表

現やベクトル等であってもよい。

- [0052] 次に、ステップS 3 2 0では、モデル生成部2 2 6は、ステップS 3 1 5で生成されたグラフ表現やベクトル等のテレメトリ情報の埋め込みを用いて、異常検出用の機械学習モデルを訓練する。
- [0053] 次に、ステップS 3 2 5では、モデル生成部2 2 6は、ステップS 3 2 0で生成した異常検出用の機械学習モデルを用いて、ステップS 3 1 5で生成したテレメトリ情報の検証セットに対する異常検出処理を行う。テレメトリ情報の検証セットに対する異常検出の精度が所定の性能閾値未満の場合、本処理はステップS 3 1 5へ戻り、テレメトリ情報に対する新たな埋め込みが生成される。一方、テレメトリ情報の検証セットに対する異常検出の精度が所定の性能閾値以上の場合、本処理はステップS 3 3 0へ進む。
- [0054] 次に、ステップS 3 3 0では、モデル生成部2 2 6は、ステップS 3 2 5で生成した異常検出用の機械学習モデルと、モデルDB 2 3 4に保存されている既存の機械学習モデルを比較し、新たに生成した異常検出用の機械学習モデルに基づいて既存の機械学習モデルを更新するか、新たな異常検出用の機械学習モデルとして保存すべきかを判定する。ある実施形態では、モデル生成部2 2 6は、新たに生成した機械学習モデルに基づいて既存の機械学習モデルを更新するか、新たな異常検出用の機械学習モデルとして保存すべきかを、それぞれの機械学習モデルに関するメタデータ（モデルID、精度等）に基づいて判定してもよい。
- [0055] 次に、ステップS 3 3 5では、モデル生成部2 2 6は、ステップS 3 3 0の判定に従って、ステップS 3 2 5で生成した異常検出用の機械学習モデルに基づいてモデルDB 2 3 4に保存されている既存の機械学習モデルを更新するか、ステップS 3 2 5で生成した異常検出用の機械学習モデルを新たな機械学習モデルとしてモデルDB 2 3 4に保存する。
- [0056] ステップS 3 1 0で現在の処理が異常検出段階にあると判定された場合、ステップS 3 4 0では、異常検出部2 2 8は、モデルDB 2 3 4から、異常検出用の機械学習モデルを取得する。

- [0057] 次に、ステップS 3 4 5では、異常検出部2 2 8は、ステップS 3 4 0で取得した異常検出用の機械学習モデルを用いて、ステップS 3 0 5で取得されたテレメトリ情報を、ステップS 3 1 5で生成した埋め込みと同じ形式（例えば、グラフ表現、ベクトル）に変換する。
- [0058] 次に、ステップS 3 5 0では、異常検出部2 2 8は、ステップS 3 4 0で取得した異常検出用の機械学習モデルを用いて、ステップS 3 4 5で変換したテレメトリ情報を解析することで、当該テレメトリ情報に対応するマイクロサービスに関する異常を検出する。ここで、異常検出部2 2 8は、テレメトリ情報に対して異常を検出するために、例えばP C A等の統計的な手法や、S H A P等の機械学習手法を用いてもよい。
- [0059] 次に、ステップS 3 5 5では、異常検出部2 2 8は、ステップS 3 5 0での異常検出の結果を可視化し、マイクロサービスに関する異常及びその要因を示す異常検出結果を、図2に示す入出力部2 4 6を介して、ユーザ端末2 6 0に表示されるG U I（G r a p h i c a l U s e r I n t e r f a c e）でユーザに提示する。
- [0060] 図3に示す異常検出手段によれば、テレメトリ情報におけるログ、メトリック及びトレースのそれぞれの特徴を考慮する機械学習モデルを生成することで、マイクロサービスに関する高精度の異常検出が可能となる。
- [0061] 次に、図4を参照して、本開示の実施形態に係るモデル生成段階における処理の流れについて説明する。
- [0062] 図4は、本開示の実施形態に係るモデル生成段階におけるモデル生成処理4 0 0の流れを示す図である。図4に示すモデル生成処理4 0 0は、マイクロサービスに関するテレメトリ情報に基づいて、当該マイクロサービスにおける異常を検出するための異常検出用の機械学習モデルを生成するための処理であり、図2に示すテレメトリ情報取得部2 2 2、埋め込み生成部2 2 4及びモデル生成部2 2 6によって実施される。
- [0063] まず、ステップS 4 0 5では、テレメトリ情報取得部2 2 2は、対象のマイクロサービスに関するテレメトリ情報を取得する。上述したように、ここ

で、テレメトリ情報取得部222は、例えばログ情報、メトリック情報及びトレース情報をテレメトリ情報として取得するLoki（登録商標）、Prometheus（登録商標）及びTempo（登録商標）等の既存の手法を用いてもよい。

[0064] 次に、ステップS410では、埋め込み生成部224は、ステップS405で取得されたテレメトリ情報を、機械学習モデルを訓練するための学習セットと、訓練した機械学習モデルをテストするための検証セットとに分割した後、テレメトリ情報の学習セットにおける特徴を抽出し、抽出した特徴に基づいた埋め込みを生成する。ある実施形態では、埋め込み生成部224は、交差検証手法（cross-validation）を用いてテレメトリ情報を学習セットと検証セットとに分割してもよい。

[0065] テレメトリ情報に含まれるログ情報、トレース情報及びメトリック情報のそれぞれは、マイクロサービスに関する異なる特性を表現するために、異なるデータ構造を有する。例えば、複数のマイクロサービスの関係を示すトレースは、空間的及び時間的な依存性（spatial and temporal dependency）を有するグラフ形式で表現され、マイクロサービスの挙動を示すログは、特定の期間（periodicity）に関する自然言語形式で表現され、マイクロサービスの性能に関するメトリックは、時間的周期性（seasonality）を有する数値形式で表現される。

ログ情報、トレース情報及びメトリック情報のそれぞれの構造的な相違により、それぞれの重要な特徴を捉えた埋め込みの生成が難しく、従来では、ログ情報、トレース情報及びメトリック情報の全てを考慮した異常検出手段が提供されていない。

[0066] そこで、本開示の実施形態に係る埋め込み生成部224は、テレメトリ情報に含まれるログ情報、トレース情報及びメトリック情報のそれぞれの特性を考慮した埋め込み手段を用いて、ログ情報、トレース情報及びメトリック情報のそれぞれの特徴を低次元空間で表現する埋め込みを生成した後、これ

らの3つの埋め込みを集約することで、テレメトリ情報に基づいて高精度の異常検出が可能な機械学習モデルを生成することに関する。

[0067] より具体的には、埋め込み生成部224は、テレメトリ情報の学習セットにおけるトレース情報から、複数のマイクロサービス間の階層関係を示すサービス関係の特徴を抽出し、所定のグラフ埋め込み手法を用いてこれらのサービス関係の特徴を処理することで、サービス関係の特徴を低次元空間で表現するトレース埋め込みを生成する。

また、埋め込み生成部224は、テレメトリ情報の学習セットにおけるログ情報から、マイクロサービスの挙動をテキスト形式で示すログの内容を示す意味的特徴と、複数のログ間の関係を示すログ関係の特徴とを抽出し、所定のグラフ埋め込み手法を用いて意味的特徴及びログ関係の特徴を処理することで、意味的特徴及びログ関係の特徴とを低次元空間で表現するログ埋め込みを生成する。

更に、埋め込み生成部224は、テレメトリ情報の学習セットにおけるメトリック情報から、マイクロサービスの性能に関する測定値の時間的周期性を示す時間的特徴と、複数のメトリック間の依存関係を示すメトリック関係の特徴とを抽出し、所定の時間的埋め込み手法を用いて時間的特徴及びメトリック関係の特徴を処理することで、時間的特徴とメトリック関係の特徴とを低次元空間で表現するメトリック埋め込みを生成する。

[0068] 一例として、ここで、埋め込み生成部224は、ログ及びトレースに存在する関係やパターンを示す低次元のグラフ表現を生成し、メトリックを低次元のベクトルに変換してもよい。このメトリックの変換は、例えばいわゆるワンホットエンコーディング (One-Hot Encoding) やラベルエンコーディング (Label Encoding) によって行われてもよい。

[0069] このように、所定のマイクロサービスのセットについて、複数のマイクロサービス間の階層関係を示すサービス関係の特徴、マイクロサービスの挙動をテキスト形式で示すログの内容を示す意味的特徴、複数のログ間の関係を

示すログ関係の特徴、マイクロサービスの性能に関する測定値の時間的周期性を示す時間的特徴と、複数のメトリック間の依存関係を示すメトリック関係の特徴とを考慮した異常検出が可能な機械学習モデルを生成することができる。

[0070] 次に、ステップS 4 1 5では、モデル生成部2 2 6は、ステップS 4 1 0で生成されたグラフ表現やベクトル等のテレメトリ情報の埋め込みを用いて、異常検出用の機械学習モデルを訓練する。より具体的には、ここで、モデル生成部2 2 6は、ステップS 3 1 5で生成されたグラフ表現やベクトル等の埋め込みを用いて、テレメトリ情報における特徴や関係を未訓練のG N N等の機械学習モデルに学習させることで、訓練済みの異常検出用の機械学習モデルを生成してもよい。

[0071] 次に、ステップS 4 2 0では、モデル生成部2 2 6は、ステップS 4 1 0で生成した異常検出用の機械学習モデルを用いて、ステップS 4 1 0で生成したテレメトリ情報の検証セットに対する異常検出処理を行う。テレメトリ情報の検証セットに対する異常検出の精度が所定の性能閾値未満の場合、本処理はステップS 4 1 0へ戻り、テレメトリ情報に対する新たな埋め込みが生成される。一方、テレメトリ情報の検証セットに対する異常検出の精度が所定の性能閾値以上の場合、本処理はステップS 4 2 5へ進む。

なお、ここでの性能閾値は、ビジネスのニーズ、試行錯誤、シミュレーション結果等に基づいて、ユーザによって適宜に設定されてもよい。

[0072] 次に、ステップS 4 2 5では、モデル生成部2 2 6は、ステップS 4 2 0で生成した異常検出用の機械学習モデルを、モデルDB 2 3 4に保存されている既存の機械学習モデルと比較し、新たに生成した異常検出用の機械学習モデルに基づいて既存の機械学習モデルを更新するか、新たな異常検出用の機械学習モデルとして保存する。

[0073] 以上説明したモデル生成処理4 0 0によれば、ログ情報、メトリック情報及びトレース情報におけるサービス関係の特徴、意味的特徴、ログ関係の特徴、時間的特徴及びメトリック関係の特徴を捉えた埋め込みを用いてG N N

等の機械学習モデルを訓練することで、マイクロサービスの様々な側面について異常検出が可能な異常検出用の機械学習モデルを生成することができる。

[0074] 次に、図5を参照して、本開示の実施形態に係る異常検出段階における異常検出処理について説明する。

[0075] 図5は、本開示の実施形態に係る異常検出段階における異常検出処理500の流れを示す図である。図5に示す異常検出処理500は、図4に示すモデル生成処理400によって生成された異常検出用の機械学習モデルを用いて、所定のマイクロサービスに関するテレメトリ情報を解析することで、当該マイクロサービスにおける異常を検出するための処理であり、図2に示す異常検出部228によって実施される。

[0076] まず、ステップS505では、テレメトリ情報取得部222は、対象のマイクロサービスに関するテレメトリ情報を取得する。上述したように、ここで、テレメトリ情報取得部222は、例えばログ情報、メトリック情報及びトレース情報をテレメトリ情報として取得するLoki（登録商標）、Prometheus（登録商標）及びTempo（登録商標）等の既存の手法を用いてもよい。

[0077] 次に、ステップS510では、異常検出部228は、モデルDB234から、図4に示すモデル生成処理400によって生成された異常検出用の機械学習モデルを取得する。

[0078] 次に、ステップS515では、異常検出部228は、ステップS510で取得した異常検出用の機械学習モデルを用いて、ステップS505で取得されたテレメトリ情報を、図4に示すモデル生成処理400のステップS410で生成した埋め込みと同じ形式（例えば、グラフ表現、ベクトル）に変換する。

[0079] 次に、ステップS520では、異常検出部228は、ステップS510で取得した異常検出用の機械学習モデルを用いて、ステップS515で変換したテレメトリ情報を解析することで、当該テレメトリ情報に対応するマイク

ロサービスに関する異常を検出する。ここで、異常検出部228は、テレメトリ情報に対して異常を検出するために、例えばPCA等の統計的な手法や、SHAP等の機械学習手法を用いてもよい。

[0080] 次に、ステップS525では、異常検出部228は、ステップS520での異常検出の結果を可視化し、マイクロサービスに関する異常及びその要因を示す異常検出結果を、図2に示す入出力部246を介して、ユーザ端末260に表示されるGUI (Graphical User Interface) でユーザに提示する。

[0081] 以上説明した異常検出処理500によれば、マイクロサービスに関するテレメトリ情報を解析することで、当該マイクロサービスにおける異常を検出することができる。

[0082] 次に、図6を参照して、本開示の実施形態に係る異常検出用の機械学習モデルを生成する際の動作について説明する。

[0083] 図6は、本開示の実施形態に係る異常検出用の機械学習モデルを生成する際の動作の一例を示す図である。図6に示す動作は、図4を参照して説明したモデル生成処理400におけるステップS415に実質的に対応し、テレメトリ情報を用いて異常検出用の機械学習モデルを生成するための動作である。

[0084] まず、図6に示すように、テレメトリ情報取ステップS610では、トレース情報611、メトリック情報612及びログ情報613を含むテレメトリ情報がテレメトリ情報取得部222によって取得される。

その後、トレース情報611、メトリック情報612及びログ情報613のそれぞれは、ニューラルネットワークの異なる埋め込み層に入力される。より具体的には、トレース情報611は、トレース埋め込み層621に入力され、メトリック情報612はメトリック埋め込み層622に入力され、ログ情報613はログ埋め込み層623に入力されてもよい。

[0085] トレース埋め込み層621、メトリック埋め込み層622及びログ埋め込み層623のそれぞれは、入力されるテレメトリ情報から特徴を抽出する。

例えば、トレース埋め込み層 6 2 1 は、トレース情報 6 1 1 から、複数のマイクロサービス間の階層関係を示すサービス関係の特徴を抽出してもよい。

[0086] メトリック埋め込み層 6 2 2 は、メトリック情報 6 1 2 から、マイクロサービスの性能に関する測定値の時間的周期性を示す時間的特徴と、複数のメトリック間の依存関係を示すメトリック関係の特徴とを抽出してもよい。

ログ埋め込み層 6 2 3 は、ログ情報 6 1 3 から、マイクロサービスの挙動をテキスト形式で示すログの内容を示す意味的特徴と、複数のログ間の関係を示すログ関係の特徴とを抽出してもよい。

ここで、特徴を抽出するためには、トレース埋め込み層 6 2 1、メトリック埋め込み層 6 2 2 及びログ埋め込み層 6 2 3 のそれぞれは、既存の特徴抽出手段を用いてもよく、ここでは特に限定されない。

[0087] トレース埋め込み層 6 2 1、メトリック埋め込み層 6 2 2 及びログ埋め込み層 6 2 3 のそれぞれは、入力されるテレメトリ情報の特性に基づいて設定された埋め込み手段を適用するように構成されてもよい。一例として、トレース埋め込み層 6 2 1 及びログ埋め込み層 6 2 3 は、抽出した特徴に対してグラフ埋め込み (graph embedding)、メトリック埋め込み層 6 2 2 は、抽出した特徴に対して時間的埋め込み (temporal embedding) を実施するように構成されてもよい。

[0088] 次に、集約ステップ S 6 3 0 では、埋め込み層 6 2 1、6 2 2、6 2 3 によって生成されるそれぞれの埋め込みは、集約層 6 3 5 (aggregation layer) によって集約され、予測層 6 4 1 (全結合層や dense layer ともいう) に入力されるための単一の潜在表現が生成される。この潜在表現は、トレース埋め込み、ログ埋め込み及びメトリック埋め込みを低次元空間で表現する情報であり、例えばベクトルやグラフ表現であってもよい。

[0089] 次に、予測ステップ S 6 4 0 では、集約ステップ S 6 3 0 で生成された潜在表現が予測層 6 4 1 (dense layer) に入力される。予測層 6

41は、入力される潜在表現に対してReLU (Rectified Linear Unit) 関数等の活性化関数を用いることで、マイクロサービスに関するテレメトリ情報における異常の有無を示す異常スコア645を生成することができる。生成された異常スコア645を、例えばテレメトリ情報における実際の異常を示すグラウンドトゥールズと比較することで、予測層641の精度を評価することができる。この比較の結果、予測層641の精度が所定の精度閾値以上の場合、トレース埋め込み層621、メトリック埋め込み層622及びログ埋め込み層623、集約層635及び予測層641のパラメータが凍結され、異常検出用の機械学習モデルとして保存されてもよい。

[0090] 図6に示す、異常検出用の機械学習モデルを生成する際の動作によれば、ログ情報、メトリック情報及びトレース情報におけるサービス関係の特徴、意味的特徴、ログ関係の特徴、時間的特徴及びメトリック関係の特徴を捉えた埋め込みを用いてGNN等の機械学習モデルを訓練することで、マイクロサービスの様々な側面について異常検出が可能な異常検出用の機械学習モデルを生成することができる。

[0091] 上述したように、本開示の一態様は、テレメトリ情報に含まれるメトリック情報、トレース情報及びログ情報のそれぞれについて、有意義な特徴を低次元のデータ空間で表現する埋め込みを生成することに関する。

次に、図7～9を参照して、本開示の実施形態に係るメトリック情報、トレース情報及びログ情報に対する埋め込みを生成する処理の一例について説明する。

[0092] 図7は、本開示の実施形態に係るトレース情報に対する埋め込みを生成する処理の一例を示す図である。上述したように、本開示の実施形態に係るトレース情報とは、複数のマイクロサービスからなるマイクロサービスエコシステムの異なるコンポーネント間の関係を示すトレースを含む情報である。ここでのトレースは、例えばある処理タスクを実行するためサービスによって呼び出される従属サービスとの関係をグラフ形式で示す関係図であっても

よい。

上述したように、本開示の実施形態に係る異常検出手段は、トレースで表現されるサービス間の関係を考慮することによって、より高精度の異常検出結果を生成することができる。

[0093] より具体的には、マイクロサービスにおける第1のサービスが第2のサービスを呼び出した場合、第1のサービス及び第2のサービスの間には依存関係が形成される。また、第2のサービスは、他のサービス（第3、第4のサービス）を呼び出し、これらのサービスも他のサービスを更に呼び出す場合があり、これらの全ての呼び出されたサービスの間には依存関係が存在する。このように、多数のサービスが依存関係で結ばれる「サービス呼び出し連鎖」が形成され、このサービス呼び出し連鎖を示す情報は「トレース」と呼ばれる。

図7に示すように、一例として、トレース710が示される。トレース710には、第1のサービス700に対応するノードや、第2のサービス702に対応するノードは、依存関係701によって接続される。

[0094] トレース710に対する埋め込みを生成する場合、トレース710における各ノードがGNN等のグラフベースの機械学習モデルのトレース埋め込み層715に入力される。その後、トレース埋め込み層715は、トレース710に示される、複数のマイクロサービス間の階層関係を示すサービス関係の特徴を抽出した後、各ノードのノード属性、ノード間の関係を示す近隣情報（neighborhood information）、マイクロサービスが実装されているクラスタを示すグローバル情報（global information）をベクトル形式で表現するトレース埋め込み720を生成する。

ここで、トレース埋め込み720を生成するグラフ埋め込み手段として、例えば行列因子分解（Matrix factorization）、ランダムウォークベース手法（Random walk-based methods）、グラフ畳み込みネットワーク（Graph Convolution

al Networks ; GCN)グラフ注意ネットワーク(Graph Attention Networks ; GAT)等を用いてもよい。

[0095] このように、トレース情報に対してグラフ埋め込み手法を用いることで、複数のマイクロサービス間の階層関係を示すサービス関係の特徴を表現するトレース埋め込みを生成することができる。

[0096] 図8は、本開示の実施形態に係るメトリックに対する埋め込みを生成する処理の一例を示す図である。上述したように、本開示の実施形態に係るメトリックとは、ハードウェア又はソフトウェアの性能を定量的に示す測定値を示すメトリックの集合を含む情報である。ここでのメトリックは、例えば特定の期間におけるCPU使用率やメモリ使用量等を含んでもよい。

[0097] また、一般に、マイクロサービスの使用量は、周期的に変動することがある（例えば、企業で用いられるマイクロサービスは、当該企業の営業時間内では使用量が増加し、営業時間外では使用量が減る等）。このため、マイクロサービスにおける時間的な周期性は、メトリックにおいても反映される。更に、複数のメトリックの中で、依存関係にあるメトリックが存在する（例えば、CPU使用量がメモリ使用量と比例する等）。

上述したように、本開示の実施形態に係る異常検出手段は、メトリックにおける周期性や、メトリック間の関係を考慮することにより高精度の異常検出結果を生成することができる。

[0098] 図8に示すように、取得したテレメトリ情報におけるメトリック805は、ニューラルネットワークの埋め込み層810に入力することで、埋め込み層810は、入力したメトリック805から、マイクロサービスの性能に関する測定値の時間的周期性を示す時間的特徴と、複数のメトリック間の依存関係を示すメトリック関係の特徴とを抽出し、抽出した特徴に基づいて、ベクトル等の低次元表現をメトリック埋め込み815として生成することができる。

[0099] ここでの埋め込み層810は、例えば、複数のメトリックの相互依存性を学習するアテンションメカニズムを備える回帰型ニューラルネットワークの

レイヤや、メトリックの周期性や内部依存性の特徴を学習する時間的アテンションレイヤ (Temporal attention layer) であってもよい。

このように、メトリック情報に対して時間的埋め込み主要を用いることで、メトリックにおける周期性を示す時間的特徴や、メトリック間の関係性を示すメトリック関係の特徴を表現するメトリック埋め込みを生成することができる。

[0100] 図9は、本開示の実施形態に係るログに対する埋め込みを生成する処理の一例を示す図である。上述したように、本開示の実施形態に係るログとは、マイクロサービスにおける特定のコードブロックが実行された時にシステムによって生成されるテキスト形式のログを含む情報である。ここでのログは、例えば実行されたコードブロックの内容を示すテキスト情報と、当該コードブロックが実行された日時を示すタイムスタンプとを含んでもよい。

[0101] 一般に、ログの内容は、自然言語で構成されているテキストで表現されているため、ログに対する埋め込みを生成するに当たって、このテキストの意味的内容 (semantic content) を考慮することが望ましい。また、ログは、他のログ (例えば、連続するログ) に関連する内容を含むことがあるため、これらのログ間の関係を埋め込みに反映させることが望ましい。

[0102] 図9には、特定のマイクロサービスの挙動に関する複数のログからなるログシーケンス910の一例を示す。ログシーケンス910における各ログのテキストの内容は、意味的ベクトル912として表現することができる。この意味的ベクトル912は、例えばワンホットエンコーディング等によって生成されてもよい。

このログシーケンス910に基づいて、各ログを、意味的ベクトルを特徴として有するノード922として示し、連続するログ間の関係をエッジ924として示すロググラフ920を生成することができる。

[0103] 次に、ロググラフ920に対する埋め込みを生成する場合、図7を参照し

て説明したトレースの埋め込みと同様に、ロググラフ920における各ノードがGNN等のグラフベースの機械学習モデルのログ埋め込み層930に入力される。その後、ログ埋め込み層930は、マイクロサービスの挙動をテキスト形式で示す前記ログの内容を示す意味的特徴と、複数のログ間の関係を示すログ関係の特徴とを抽出した後、各ノードのノード属性、ノード間の関係を示す近隣情報 (neighborhood information)、マイクロサービスが実装されているクラスタを示すグローバル情報 (global information) をベクトル形式で表現するログ埋め込み935を生成する。

ここで、ログ埋め込み935を生成するグラフ埋め込み手段として、例えば行列因子分解 (Matrix factorization)、ランダムウォークベース手法 (Random walk-based methods)、グラフ畳み込みネットワーク (Graph Convolutional Networks; GCN) グラフ注意ネットワーク (Graph Attention Networks; GAT) 等を用いてもよい。

[0104] このように、ログ情報に対してグラフ埋め込み手法を用いることで、ログの意味的内容を示す意味的特徴や、ログ間の関係を示すログ関係の特徴を表現するログ埋め込みを生成することができる。

[0105] 次に、図10を参照して、本開示の実施形態に係る集約層の動作について説明する。

[0106] 図10は、本開示の実施形態に係る集約層の動作の一例を示す図である。上述したように、異常検出用の機械学習モデルを生成する際、テレメトリ情報に含まれるトレース情報、ログ情報及びメトリック情報のそれぞれについて生成された埋め込みは、ニューラルネットワークの集約層によって集約され、単一の潜在表現が生成される。図10では、集約層の動作の一例について説明する。

[0107] まず、トレース埋め込み、ログ埋め込み及びメトリック埋め込みからなる埋め込みセット1010は、集約層1020に入力される。集約層1020

は、埋め込みセット 1010 に含まれるそれぞれの埋め込みの元となったテレメトリ情報（トレース情報、ログ情報、メトリック情報）が取得された期間の細かなタイムスタンプを、時間単位、日単位、週単位などの離散単位にマッピングさせた後、同じ時間単位に対応する埋め込みを時間単位埋め込み（`time-unit embeddings`）に集約する。

その後、集約層 1020 は、例えば加算や行列内積などの連結演算によって、時間単位埋め込みを時間的埋め込み（`temporal embedding`）1030 に集約する。

[0108] 次に、融合層 1040 は、例えば加算や行列内積などの連結演算によって、時間的埋め込み 1030 を融合し、単一の潜在表現 1050 を生成する。この潜在表現 1050 は、トレース埋め込み、ログ埋め込み及びメトリック埋め込みを低次元空間で表現する情報であり、例えばベクトルやグラフ表現であってもよい。

[0109] このように、集約層を用いてトレース埋め込み、ログ埋め込み及びメトリック埋め込みを集約することで、テレメトリ情報における異常を検出するための異常検出用の機械学習モデルを生成することができる。

[0110] 次に、図 11 を参照して、本開示の実施形態に係る異常検出用の機械学習モデルとして機能するニューラルネットワークの構成について説明する。

[0111] 図 11 は、本開示の実施形態に係る異常検出用の機械学習モデルとして機能するニューラルネットワーク 1150 の構成の一例を示す図である。図 11 に示すように、ニューラルネットワーク 1150 は、入力層 1100、複数の隠れ層 1101、及び出力層 1102 を含む。また、入力層 1100、隠れ層 1101 及び出力層 1102 は、エッジ 1104、1106 によって互いに接続されている。

[0112] 入力層 1100 は、低次元空間に表現されているテレメトリ情報（例えば、テレメトリ情報から生成されている埋め込み）を入力する。次に、入力層 1100 における各ノード 1103 は、入力したテレメトリ情報に対する処理や変換を行うことで、テレメトリ情報から抽出した特徴からなる特徴ベク

トルを生成する。その後、これらの特徴ベクトルは、隠れ層 1 1 0 1 に入力される。

[0113] 隠れ層 1 1 0 1 のそれぞれは、入力データに対して一連の演算を実行する複数のノード 1 1 0 5 からなる。より具体的には、隠れ層 1 1 0 1 は、入力する特徴ベクトルに対する重みを適用することで得られる値に対して活性化関数を適用する。特徴ベクトルに対する重みは、ニューラルネットワーク 1 1 5 0 によって生成される結果（異常の予測）のグラウンドトゥルースに対する誤差を最小化する訓練処理によって判定されてもよい。

[0114] 出力層 1 1 0 2 は、最後の隠れ層 1 1 0 1 から、重みの適用及び活性化関数の適用によって変換された特徴ベクトルを入力し、これらの特徴ベクトルに基づいて、テレメトリ情報における異常の有無を示す異常予測結果を生成する。次に、出力層 1 1 0 2 は、例えばソフトマックス関数等の隠れ層 1 1 0 1 とは異なる活性化関数を用いて、出力クラスにわたって確率分布を生成する。ある実施形態では、この異常予測結果は、テレメトリにおいて異常が存在する確率を示す情報であってもよい。例えば、異常予測結果が「50%」を超える確率を示す場合、テレメトリ情報において異常が存在すると判定されてもよい。

なお、異常検出用の機械学習モデルを生成するモデル生成段階では、特徴ベクトルに対して適用する重みは調整可能であるが、異常検出段階では、重みや、ニューラルネットワーク 1 1 5 0 の各層のパラメータはフリーズ（凍結）される。

[0115] ある実施形態では、異常予測結果の生成に用いられる特徴のランク付けを行う SHAP (SHapley Additive exPlanations) 等のラッパー (wrapper) をニューラルネットワーク 1 1 5 0 に実装してもよい。ラッパーは、ニューラルネットワーク 1 1 5 0 による予測に用いられる各特徴の重要性の尺度を計算することができる。

異常検出用の機械学習モデルを生成するモデル生成段階では、SHAP 等のラッパーを用いることで、異常検出に対するテレメトリ情報の各特徴の相

対的な貢献度を特定し、貢献度がより高い特徴に対してより高い重みを適用してもよい。また、異常検出段階では、このSHAPは、異常予測結果の生成に用いられる特徴のランク付けを行うことで、特定の異常予測結果が生成された理由（なぜ異常があると判定されたかを示す説明等）や、異常の要因の候補を生成し、出力することができる。

[0116] 図11に示すニューラルネットワーク1150によれば、マイクロサービスのテレメトリ情報に基づいて、マイクロサービスにおける異常の有無を高精度で検出することが可能となる。

[0117] 次に、図12を参照して、本開示の実施形態に係る異常検出用の機械学習モデルをモデルDBに格納又は取得する処理の流れについて説明する。

[0118] 図12は、本開示の実施形態に係る異常検出用の機械学習モデルの格納・取得処理1200の一例を示す図である。格納・取得処理1200は、異常検出用の機械学習モデルを生成した後、モデルDB234に格納するための処理や、テレメトリ情報に対して異常検出を行う際に、訓練済みの異常検出用の機械学習モデルをモデルDB234から取得するための処理であり、モデル生成部226及び異常検出部228によって実施される。

[0119] まず、ステップS1205では、モデル生成部226は、例えば図4に示すモデル生成処理400によって生成した異常検出用の機械学習モデル1201を所定の形式に変換するシリアル化を行う。例えば、ここで、モデル生成部226は、異常検出用の機械学習モデル1201をJSON、Pickle、Protocol Buffer等の形式に変換してもよい。

[0120] 次に、ステップS1210では、モデル生成部226は、異常検出用の機械学習モデル1201を保存するデータベース方式を選択する。ここでのデータベース方式とは、データの格納及び取得に関するルールを規定する、データベースの構成・管理方法である。原則として、大量のデータの高性能の読み書き動作や、バイナリーデータ及びメタデータの格納が可能なデータベース方式を選択することが望ましいが、異常検出用の機械学習モデル1201の用途や性能に応じて選択されてもよい。データベース方式の例として、

例えばMongoDB（登録商標）、Cassandra（登録商標）、Redis（登録商標）及びDynamoDB（登録商標）等が考えられる。

[0121] 次に、ステップS1215では、モデル生成部226は、異常検出用の機械学習モデル1201を、メタデータ及びプロフィール情報1213に対応付けた後、ステップS1210で選択したデータベース方式で構成されるモデルDB234に格納する。メタデータ及びプロフィール情報1213は、例えば異常検出用の機械学習モデル1201の生成日時、アーキテクチャ、評価するためのメトリック統計、データカバレッジ、バージョン、プロジェクトID、シリアル形式の情報を含んでもよい。

上述したように、異常検出用の機械学習モデル1201をモデルDB234に格納する際、異常検出用の機械学習モデル1201を新たなモデルとして保存してもよく、既存のモデルを異常検出用の機械学習モデル1201に基づいて更新してもよい。ある実施形態では、モデル生成部226は、新たに生成した機械学習モデルに基づいて既存の機械学習モデルを更新するか、新たな異常検出用の機械学習モデルとして保存すべきかを、それぞれの機械学習モデルに関するメタデータ及びプロフィール情報1213に基づいて判定してもよい。

[0122] 次に、ステップS1220では、テレメトリ情報に対して異常検出を行う際、異常検出部228は、モデルDB234から、異常検出用の機械学習モデル1201を取得する。ここで、異常検出部228は、例えば異常検出用の機械学習モデル1201に対応付けられているメタデータ及びプロフィール情報1213に基づく検索を実施することで、適切な異常検出用の機械学習モデル1201をモデルDB234から取得してもよい。また、異常検出用の機械学習モデル1201を取得した後、異常検出部228は、取得した異常検出用の機械学習モデル1201をシリアル形式からモデルオブジェクト形式に変換してもよい。

[0123] 以上説明した格納・取得処理1200によれば、異常検出用の機械学習モデルを適切なデータベースに格納すると共に、テレメトリ情報に対して異常

検出を行う際に、容易に取得することができる。

[0124] 次に、図 1 3 を参照して、本開示の実施形態に係るモデル D B の論理的データベーススキーマについて説明する。

[0125] 図 1 3 は、本開示の実施形態に係るモデル D B の論理的データベーススキーマ 1 3 0 0 の一例を示す図である。ここでの論理的データベーススキーマ 1 3 0 0 は、上述したモデル D B 2 3 4 において本開示の実施形態に係る異常検出用の機械学習モデルを格納するためのデータベースの構造である。

[0126] 図 1 3 に示すように、モデル D B 2 3 4 の論理的データベーススキーマ 1 3 0 0 は、特定の異常検出用の機械学習モデルを一意に識別するモデル I D 1 3 0 1、異常検出用の機械学習モデルについて、モデル I D 1 3 0 1、生成日時 1 3 0 2、モデルアーキテクチャ 1 3 0 3、メトリック統計 1 3 0 4、データカバレッジ 1 3 0 5、バージョン 1 3 0 6、プロジェクト I D 1 3 0 7 及びシリアル形式 1 3 0 8 を含んでもよい。

[0127] モデル I D 1 3 0 1 は、異常検出用の機械学習モデルを識別するための一意の識別子を示す情報である。。

生成日時 1 3 0 2 は、異常検出用の機械学習モデルの生成日時や更新日時などのタイムスタンプを示す情報である。

モデルアーキテクチャ 1 3 0 3 は、異常検出用の機械学習モデルの設計や構造を表すアーキテクチャやネットワークの形式を示す情報である。

メトリック統計は、異常検出用の機械学習モデルの性能を評価するために計測される統計的な指標や評価指標を示す情報である。

データカバレッジ 1 3 0 5 は、異常検出用の機械学習モデルの訓練や評価に使用されるデータの範囲や網羅性を示す指標である。

[0128] バージョン 1 3 0 6 は、異常検出用の機械学習モデルのバージョン管理をするための番号や識別子を示す情報である。

プロジェクト I D 1 3 0 7 は、異常検出用の機械学習モデルが所属するプロジェクトを識別するための一意の識別子を示す情報である。

シリアル形式 1 3 0 8 は、異常検出用の機械学習モデルをシリアル化する

際のデータの形式やフォーマットを示す情報である。

行 1 3 0 9 は、論理的データベーススキーマ 1 3 0 0 に格納される各種データのデータ種類を示す情報である。

行 1 3 1 0 は、論理的データベーススキーマ 1 3 0 0 に格納される異常検出用の機械学習モデルの情報の一例を示す。

[0129] 図 1 3 に示すモデル DB 2 3 4 の論理的データベーススキーマ 1 3 0 0 によれば、異常検出用の機械学習モデルの効率的な格納や検索が可能となる。例えば、ある実施形態では、ユーザは、論理的データベーススキーマ 1 3 0 0 において、「精度が 9 7 % 以上」の異常検出用の機械学習モデルを検索したり、「GNN」とのアーキテクチャ形式の異常検出用の機械学習モデルを検索したりすることができる。また、論理的データベーススキーマ 1 3 0 0 によれば、ユーザは、複数のアーキテクチャやプロジェクトの間で、複数のモデルを容易に比較することができる。

[0130] 次に、図 1 4 を参照して、本開示の実施形態に係る異常検出管理画面について説明する。

[0131] 図 1 4 は、本開示の実施形態に係る異常検出管理画面 1 4 0 0 の一例を示す図である。異常検出管理画面 1 4 0 0 は、異常検出用の機械学習モデルを生成する際の設定を入力すると共に、テレメトリ情報に対して実施される異常検出処理の結果を確認するためのユーザインターフェースであり、例えば図 2 に示す入出力部 2 4 6 を介して、ユーザ端末 2 6 0 に出力し、表示されてもよい。

[0132] 図 1 4 に示すように、異常検出管理画面 1 4 0 0 は、保存ボタン 1 4 0 1、設定ボタン 1 4 0 2、クラスタ名設定ウィンドウ 1 4 0 3、ネームスペース設定ウィンドウ 1 4 0 4、時間範囲設定ウィンドウ 1 4 0 5、異常グラフ表示ウィンドウ 1 4 0 6、メトリック表示ウィンドウ 1 4 0 7、ログ表示ウィンドウ 1 4 0 8、トレース表示ウィンドウ 1 4 0 9 及び詳細表示ウィンドウ 1 4 1 0 を含んでもよい。

[0133] 保存ボタン 1 4 0 1 は、異常検出管理画面 1 4 0 0 に表示されている情報

を保存するためのボタンである。

設定ボタン 1402 は、異常検出用の機械学習モデルを生成する際の設定を入力するための画面（図示せず）を開くためのボタンである。

クラスタ名設定ウインドウ 1403 は、対象のマイクロサービスが実装されている物理的なクラスタ（サーバのセット等）を選択し、特定するためのボタンである。

ネームスペース設定ウインドウ 1404 は、1つの物理的なクラスタ上で実装されている仮想クラスタを選択し、特定するためのボタンである。

時間範囲設定ウインドウ 1405 は、テレメトリ情報が取得される時間範囲を設定するためのボタンである。

[0134] 異常グラフ表示ウインドウ 1406 は、所定の期間について、対象のテレメトリ情報において検出された異常の数を時間毎に示す異常グラフを示すウインドウである。

メトリック表示ウインドウ 1407 は、所定の期間について、異常が最も多発しているメトリックを時間毎に示すウインドウである。メトリック表示ウインドウ 1407 によれば、ユーザは、異常が最も多発しているメトリックが発生したマイクロサービスを特定することができる。

ログ表示ウインドウ 1408 は、所定の期間について、異常が最も多発しているログを時間毎に示すウインドウである。ログ表示ウインドウ 1408 によれば、ユーザは、異常が最も多発しているメトリックが発生したマイクロサービスを特定することができる。

トレース表示ウインドウ 1409 は、所定の期間について、異常が最も多発しているトレースを時間毎に示すウインドウである。トレース表示ウインドウ 1409 によれば、ユーザは、異常が最も多発しているトレースにおけるサービスの階層関係を確認することができる。

[0135] 詳細表示ウインドウ 1410 は、ユーザによって選択された特定のメトリック、ログ、又はトレースに関する詳細情報を表示するためのウインドウである。例えば、ユーザは、詳細表示ウインドウ 1410 を用いることで、異

常が発生した特定のマイクロサービスに関するログを確認することができる。

[0136] 図14に示す異常検出管理画面1400によれば、本開示の実施形態に係る異常検出装置210のユーザは、異常検出用の機械学習モデルを生成する際の設定を入力すると共に、テレメトリ情報に対して実施される異常検出処理の結果を容易に確認することができる。

[0137] 次に、図15を参照して、本開示の実施形態に係るクラウドコンピューティング環境について説明する。

[0138] 図15は、本開示の実施形態に係るクラウドコンピューティング環境1500の一例を示す図である。クラウドコンピューティング環境1500は、本開示の実施形態に係る異常検出システム200を実現するために用いてもよい。例えば、本開示の実施形態に係る異常検出システム200や、異常検出の対象となるマイクロサービスは、同一又は異なるクラウドコンピューティング環境において実装されてもよい。

[0139] クラウドコンピューティング環境1500は、1つ以上のクラウドコンピューティングノードから構成されており、各コンピューティングノードは、ストレージデバイス1507、コンピューティングマシン1508及びネットワークデバイス1509が連携して動作する。また、各コンピューティングノードは、デスクトップコンピューター1510、ノートパソコン1501、スマートフォン1502、ドローン1503、病院のコンピュータシステム1504、自動車のコンピュータシステム1505、銀行のコンピュータシステム1506などの、クラウドユーザが使用するローカルのコンピューティングデバイスと通信する。

[0140] また、各コンピューティングノードは、プライベート、コミュニティ、パブリック、又はハイブリッドクラウドなど、物理的又は仮想的に1つ以上のサブネットワークにグループ化されてもよい。このクラウドコンピューティング環境1500によれば、様々なソフトウェアやサービスをクラウドコンピューティングモデルとして提供することが可能となる。

[0141] 一般に、クラウドコンピューティングモデルとは、最小限の管理努力又はサービス・プロバイダとの対話で迅速に供給及び解放することができる構成可能なコンピューティング・リソース（例えば、ネットワーク、ネットワーク帯域幅、サーバ、処理、メモリ、ストレージ、アプリケーション、仮想マシン、及びサービス）の共有プールに対するオンデマンドの便利なネットワーク・アクセスを可能にするためのサービス配信のモデルである。このクラウドモデルは、少なくとも5つの特性、少なくとも3つのサービスモデル、及び少なくとも4つの展開モデルを含むことができる。

[0142] 具体的には、以下が典型的な特性である。

オンデマンドのセルフサービス：クラウド・コンシューマは、サーバ時間及びネットワーク・ストレージといったコンピューティング能力を、必要に応じて、人間がサービスのプロバイダと対話する必要なく自動的に、一方的に供給することができる。

[0143] 広範なネットワーク・アクセス：能力は、ネットワーク上で利用可能であり、異種のシン又はシック・クライアント・プラットフォーム（例えば、携帯電話、ラップトップ及びPDA）による使用を促進する標準的な機構を通じてアクセスされる。

リソースのプール化：プロバイダのコンピューティング・リソースは、マルチ・テナント・モデルを用いて、複数のコンシューマに供されるようにプールされ、異なる物理及び仮想リソースは、要求に応じて動的に割り当て及び再割り当てされる。コンシューマは、一般に、提供されるリソースの正確な位置に関する制御又は知識を有していないが、より高いレベルの抽象概念（例えば、国、州、又はデータセンタ）で位置を指定することができる場合があるという点で、位置独立の感覚が存在する。

[0144] 迅速な弾力性：能力は、迅速かつ弾力的に、場合によっては自動的に供給されてすばやくスケール・アウトし、迅速に解放されてすばやくスケール・インすることができる。コンシューマにとっては、供給するために利用可能な能力は、無制限に見えることが多く、いつでもどんな量でも購入すること

ができる。

[0145] 計測されるサービス：クラウド・システムは、サービスのタイプ（例えば、ストレージ、処理、帯域幅、及びアクティブなユーザアカウント）に適した何らかの抽象レベルで計量能力を活用することによって、リソース使用を自動的に制御及び最適化する。リソース使用は、利用されるサービスのプロバイダとコンシューマの両方にとって透明性をもたらすように、監視し、制御し、報告することができる。

[0146] サービス・モデルは、典型的には以下のとおりである。

サービスとしてのソフトウェア（SaaS；Software as a Service）：コンシューマに提供される能力は、クラウド・インフラストラクチャ上で実行されるプロバイダのアプリケーションを使用することである。アプリケーションは、ウェブブラウザなどのシンクライアント・インタフェース（例えば、ウェブ・ベースの電子メール）を通じて、種々のクライアントデバイスからアクセス可能である。限定されたユーザ特有のアプリケーション構成設定を可能な例外として、コンシューマは、ネットワーク、サーバ、オペレーティング・システム、ストレージ、又は個々のアプリケーション能力をも含む基盤となるクラウド・インフラストラクチャを管理又は制御しない。

[0147] サービスとしてのプラットフォーム（PaaS；Platform as a Service）：コンシューマに提供される能力は、プロバイダによってサポートされるプログラミング言語及びツールを用いて作成される、コンシューマが作成又獲得したアプリケーションを、クラウド・インフラストラクチャ上に展開することである。コンシューマは、ネットワーク、サーバ、オペレーティング・システム、又はストレージを含む基盤となるクラウド・インフラストラクチャを管理又は制御しないが、展開されたアプリケーション、及び場合によってはアプリケーション・ホスティング環境構成に対する制御を有する。

[0148] サービスとしてのインフラストラクチャ（IaaS；Infrastru

cture as a Service) : コンシューマに提供される能力は、処理、ストレージ、ネットワーク、及び他の基本的なコンピューティング・リソースを供給することであり、ここで、コンシューマは、オペレーティング・システム及びアプリケーションを含むことができる任意のソフトウェアを展開して実行させることができる。コンシューマは、基盤となるクラウド・インフラストラクチャを管理又は制御しないが、オペレーティング・システム、ストレージ、展開されたアプリケーションに対する制御、及び場合によっては選択されたネットワーキング・コンポーネント（例えば、ホストのファイアウォール）の限定的な制御を有する。

[0149] 展開モデルは典型的には以下の通りである。

プライベート・クラウド：クラウド・インフラストラクチャは、ある組織のためだけに操作される。クラウド・インフラストラクチャは、その組織又は第三者によって管理することができ、オンプレミス又はオフプレミスで存在することができる。

[0150] コミュニティ・クラウド：クラウド・インフラストラクチャは、幾つかの組織によって共有され、関心事項（例えば、ミッション、セキュリティ要件、ポリシー、及びコンプライアンス上の考慮事項）を共有する特定のコミュニティをサポートする。クラウド・インフラストラクチャは、それらの組織又は第三者により管理することができ、オンプレミス又はオフプレミスで存在することができる。

[0151] パブリック・クラウド：クラウド・インフラストラクチャは、一般公衆又は大規模な業界グループが利用できるようにされており、クラウド・サービスを販売する組織によって所有される。

[0152] ハイブリッド・クラウド：クラウド・インフラストラクチャは、固有のエンティティを残しているが、データ及びアプリケーションのポータビリティを可能にする標準化された又は専用の技術（例えば、クラウド間の負荷平衡のためのクラウド・バースティング）によって互いに結び付けられた2つ又はそれより多いクラウド（プライベート、コミュニティ、又はパブリック）

の組合せである。

[0153] クラウドコンピューティング環境は、サービス提供を中心としており、無国籍性、低い結語ウド、モジュール性、及び意味論的相互運用性に焦点を合わせている。クラウドコンピューティングの中心は、相互接続されたノードのネットワークを含むインフラストラクチャである。代表的なクラウドコンピューティングノードは、上記図2に示すようなものである。具体的には、クラウドコンピューティングノード内には、他の多数の汎用又は専用コンピューティングシステム環境又は構成で動作可能なコンピュータシステム／サーバが存在する。コンピュータシステム／サーバと共に用いるのに適したものとすることができる周知のコンピューティングシステム、環境、及び／又は構成の例は、パーソナルコンピュータシステム、サーバコンピュータシステム、シンクライアント、シッククライアント、手持ち式又はラップトップ型デバイス、マルチプロセッサシステム、マイクロプロセッサ・ベースのシステム、セットトップボックス、プログラム可能コンシューマ・エレクトロニクス、ネットワークPC、ミニコンピュータシステム、メインフレームコンピュータシステム、及び上記システム又はデバイスなどのいずれかを含む分散型クラウドコンピューティング環境を含むが、これらに限定されない。コンピュータシステム／サーバは、コンピュータシステムによって実行されているプログラム・モジュールなどのコンピュータシステム実行可能命令の一般的なコンテキストで説明することができる。一般に、プログラム・モジュールは、特定のタスクを実施する、又は特定の抽象データ型を実装する、ルーチン、プログラム、オブジェクト、コンポーネント、論理、データ構造などを含むことができる。コンピュータシステム／サーバは、通信ネットワークを通じてリンクされた遠隔処理デバイスによってタスクが行われる分散型クラウドコンピューティング環境内で実施することができる。分散型クラウドコンピューティング環境においては、プログラム・モジュールは、メモリ・ストレージデバイスを含むローカル及び遠隔の両方のコンピュータシステム・ストレージ媒体内に配置することができる。

[0154] 上述したように、本開示の実施形態に係る異常検出手段は、以下の態様を含む。

[0155] (態様1)

異常検出装置であって、

プロセッサとメモリとを備え、

前記メモリは、

第1のマイクロサービスのセットから、

マイクロサービスの挙動を示すログを含むログ情報と、

複数のマイクロサービスの関係を示すトレースを含むトレース情報と

、

マイクロサービスの性能に関する測定値を示すメトリックを含むメトリック情報と、

を含む第1のテレメトリ情報を取得するテレメトリ情報取得部と、

前記第1のテレメトリ情報から抽出した学習用テレメトリ情報をニューラルネットワークによって処理することで、前記トレース情報に対応するトレース埋め込みを生成し、前記ログ情報に対応するログ埋め込みを生成し、前記メトリック情報に対応するメトリック埋め込みを生成する埋め込み生成部と、

前記トレース埋め込み、前記ログ埋め込み及び前記メトリック埋め込みに基づいて、マイクロサービスについて異常の有無を判定する異常検出用の機械学習モデルを生成するモデル生成部と、

前記異常検出用の機械学習モデルを用いて、第2のマイクロサービスのセットについて取得された第2のテレメトリ情報を解析することで、前記第2のマイクロサービスにおける異常の有無を示す異常検出結果を生成する異常検出部、

として前記プロセッサを機能させるための処理命令を含むことを特徴とする異常検出装置。

[0156] (態様2)

前記埋め込み生成部は、

前記トレース情報から、複数のマイクロサービス間の階層関係を示すサービス関係の特徴を抽出し、

所定のグラフ埋め込み手法を用いて前記サービス関係の特徴を処理することで、前記サービス関係の特徴を低次元空間で表現する前記トレース埋め込みを生成する、

ことを特徴とする、態様 1 に記載の異常検出装置。

[0157] (態様 3)

前記埋め込み生成部は、

前記ログ情報から、マイクロサービスの挙動をテキスト形式で示す前記ログの内容を示す意味的特徴と、複数のログ間の関係を示すログ関係の特徴とを抽出し、

所定のグラフ埋め込み手法を用いて前記意味的特徴及び前記ログ関係の特徴を処理することで、前記意味的特徴及び前記ログ関係の特徴とを低次元空間で表現する前記ログ埋め込みを生成する、

ことを特徴とする、態様 1 又は 2 に記載の異常検出装置。

[0158] (態様 4)

前記埋め込み生成部は、

前記メトリック情報から、前記マイクロサービスの性能に関する測定値の時間的周期性を示す時間的特徴と、複数のメトリック間の依存関係を示すメトリック関係の特徴とを抽出し、

所定の時間的埋め込み手法を用いて前記時間的特徴及び前記メトリック関係の特徴を処理することで、前記時間的特徴と前記メトリック関係の特徴とを低次元空間で表現する前記メトリック埋め込みを生成する、

ことを特徴とする、態様 1 乃至 3 に記載の異常検出装置。

[0159] (態様 5)

前記埋め込み部は、

ニューラルネットワークにおける埋め込み層を含み、

前記モデル生成部は、

前記ニューラルネットワークにおける集約層及び予測層を含み、

前記集約層は、

所定の連結演算手法を用いて前記トレース埋め込み、前記ログ埋め込み及び前記メトリック埋め込みのそれぞれを集約した潜在表現を生成し、前記潜在表現を前記予測層に入力し、

前記予測層は、

前記潜在表現に基づいて、前記第 1 のテレメトリ情報から取得した検証用テレメトリ情報に対する異常予測結果を生成し、

前記異常予測結果が所定の精度閾値を満たす場合、前記埋め込み層、前記集約層及び前記予測層のそれぞれのパラメータを前記異常検出用の機械学習モデルとする、

ことを特徴とする、態様 1 乃至 4 に記載の異常検出装置。

[0160] (態様 6)

前記異常検出装置は、

前記異常検出用の機械学習モデルに関する情報を保存するモデルデータベースを格納する記憶部を更に含み、

前記モデル生成部は、

生成した前記異常検出用の機械学習モデルに対するシリアル化を行うことで、シリアル形式の機械学習モデルを生成し、

前記シリアル形式の機械学習モデルと、前記シリアル形式の機械学習モデルを特徴付けるメタデータ及びプロフィール情報とを前記モデルデータベースに保存する、

ことを特徴とする、態様 1 乃至 5 に記載の異常検出装置。

[0161] (態様 7)

前記異常検出部は、

前記モデルデータベースに対して、前記プロフィール情報に基づく検索を実施することで、前記シリアル形式の機械学習モデルを取得し、

取得したシリアル形式の機械学習モデルをシリアル形式からモデルオブジェクト形式に変換することで、前記異常検出用の機械学習モデルを取得する、

ことを特徴とする、態様 6 に記載の異常検出装置。

[0162] (態様 8)

前記第 2 のテレメトリ情報におけるログ情報、トレース情報及びメトリック情報のそれぞれに関する異常の有無を示す前記異常検出結果を GUI に表示する入出力部を更に含む、

ことを特徴とする、態様 1 乃至 7 に記載の異常検出装置。

[0163] 本開示の実施形態に係る異常検出手段において、テレメトリ情報に含まれるトレース情報、メトリック情報及びログ情報を用いて機械学習モデルを訓練することで、テレメトリ情報に基づいてマイクロサービスにおける異常を検出することが可能となる。

[0164] より具体的には、本開示の実施形態に係る異常検出手段では、トレース情報、メトリック情報及びログ情報のそれぞれの固有の特徴及び構造を考慮して選択した埋め込み手法を用いることで、トレース情報、メトリック情報及びログ情報のそれぞれの特徴を抽象化した、低次元空間で表現する埋め込みを生成することができる。例えば、本開示では、時間的周期性を有するメトリック情報に対しては時間的埋め込み (temporal embedding)、グラフ構造を有するログやトレースに対してはグラフ埋め込み (graph embedding) を用いることで、メトリック情報の時間的な特徴、トレース情報の階層関係、ログ情報の意味的内容などの特徴を捉えた埋め込みを生成することができる。

[0165] また、トレース情報、メトリック情報及びログ情報のそれぞれについて生成した埋め込みに基づいて機械学習モデルを訓練することで、メトリック情報の時間的な特徴、トレース情報の階層関係、ログ情報の意味的内容等に関する異常を検出することができる、異常検出用の機械学習モデルを得ることができる。このように生成した異常検出用の機械学習モデルをマイクロサー

ビスから取得したテレメトリ情報に対して適用することで、メトリック情報、トレース情報及びログ情報を全て考慮する、高精度の異常検出が可能となる。

[0166] 更に、異常検出用の機械学習モデルを用いてテレメトリ情報に対する異常検出を行う際、異常予測結果の生成に用いられる特徴のランク付けをラッパーなどを行うことで、特定の異常予測結果が生成された理由（なぜ異常があると判定されたかを示す説明等）や、異常の要因の候補を判定することができる。このように判定した異常や、異常の要因は、例えばGUIを介してユーザに提示することで、ユーザは、マイクロサービスにおける異常やその原因を容易に確認することができる。

[0167] このように、本開示によれば、テレメトリ情報におけるログ、メトリック及びトレースのそれぞれの特徴を考慮する機械学習モデルを生成することで、マイクロサービスに関する高精度の異常検出が可能な異常検出手法を提供することができる。

[0168] 以上、本発明の実施の形態について説明したが、本発明は、上述した実施の形態に限定されるものではなく、本発明の要旨を逸脱しない範囲において種々の変更が可能である。

符号の説明

[0169] 150：異常検出アプリケーション，200：異常検出システム，210：異常検出装置，220：メモリ，222：テレメトリ情報取得部，224：埋め込み生成部，226：モデル生成部，228：異常検出部，232：テレメトリ情報DB，234：モデルDB，244：プロセッサ，246：入出力部，250：通信ネットワーク，260：ユーザ端末

請求の範囲

[請求項1]

異常検出装置であって、
プロセッサとメモリとを備え、
前記メモリは、

第1のマイクロサービスのセットから、

: マイクロサービスの挙動を示すログを含むログ情報と、

: 複数のマイクロサービスの関係を示すトレースを含むトレース情報
と、

: マイクロサービスの性能に関する測定値を示すメトリックを含むメ
トリック情報と、

を含む第1のテレメトリ情報を取得するテレメトリ情報取得部と
、

前記第1のテレメトリ情報から抽出した学習用テレメトリ情報を
ニューラルネットワークによって処理することで、前記トレース情報
に対応するトレース埋め込みを生成し、前記ログ情報に対応するログ
埋め込みを生成し、前記メトリック情報に対応するメトリック埋め込
みを生成する埋め込み生成部と、

前記トレース埋め込み、前記ログ埋め込み及び前記メトリック埋
め込みに基づいて、マイクロサービスについて異常の有無を判定する
異常検出用の機械学習モデルを生成するモデル生成部と、

前記異常検出用の機械学習モデルを用いて、第2のマイクロサー
ビスのセットについて取得された第2のテレメトリ情報を解析するこ
とで、前記第2のマイクロサービスにおける異常の有無を示す異常検
出結果を生成する異常検出部、

として前記プロセッサを機能させるための処理命令を含むことを特
徴とする異常検出装置。

[請求項2]

前記埋め込み生成部は、

前記トレース情報から、複数のマイクロサービス間の階層関係を示

すサービス関係の特徴を抽出し、

所定のグラフ埋め込み手法を用いて前記サービス関係の特徴を処理することで、前記サービス関係の特徴を低次元空間で表現する前記トレース埋め込みを生成する、

ことを特徴とする、請求項 1 に記載の異常検出装置。

[請求項3]

前記埋め込み生成部は、

前記ログ情報から、マイクロサービスの挙動をテキスト形式で示す前記ログの内容を示す意味的特徴と、複数のログ間の関係を示すログ関係の特徴とを抽出し、

所定のグラフ埋め込み手法を用いて前記意味的特徴及び前記ログ関係の特徴を処理することで、前記意味的特徴及び前記ログ関係の特徴とを低次元空間で表現する前記ログ埋め込みを生成する、

ことを特徴とする、請求項 1 に記載の異常検出装置。

[請求項4]

前記埋め込み生成部は、

前記メトリック情報から、前記マイクロサービスの性能に関する測定値の時間的周期性を示す時間的特徴と、複数のメトリック間の依存関係を示すメトリック関係の特徴とを抽出し、

所定の時間的埋め込み手法を用いて前記時間的特徴及び前記メトリック関係の特徴を処理することで、前記時間的特徴と前記メトリック関係の特徴とを低次元空間で表現する前記メトリック埋め込みを生成する、

ことを特徴とする、請求項 1 に記載の異常検出装置。

[請求項5]

前記埋め込み部は、

ニューラルネットワークにおける埋め込み層を含み、

前記モデル生成部は、

前記ニューラルネットワークにおける集約層及び予測層を含み、

前記集約層は、

所定の連結演算手法を用いて前記トレース埋め込み、前記ログ埋

め込み及び前記メトリック埋め込みのそれぞれを集約した潜在表現を生成し、前記潜在表現を前記予測層に入力し、

前記予測層は、

前記潜在表現に基づいて、前記第1のテレメトリ情報から取得した検証用テレメトリ情報に対する異常予測結果を生成し、

前記異常予測結果が所定の精度閾値を満たす場合、前記埋め込み層、前記集約層及び前記予測層のそれぞれのパラメータを前記異常検出用の機械学習モデルとする、

ことを特徴とする、請求項1に記載の異常検出装置。

[請求項6]

前記異常検出装置は、

前記異常検出用の機械学習モデルに関する情報を保存するモデルデータベースを格納する記憶部を更に含み、

前記モデル生成部は、

生成した前記異常検出用の機械学習モデルに対するシリアル化を行うことで、シリアル形式の機械学習モデルを生成し、

前記シリアル形式の機械学習モデルと、前記シリアル形式の機械学習モデルを特徴付けるメタデータ及びプロフィール情報とを前記モデルデータベースに保存する、

ことを特徴とする、請求項1に記載の異常検出装置。

[請求項7]

前記異常検出部は、

前記モデルデータベースに対して、前記プロフィール情報に基づく検索を実施することで、前記シリアル形式の機械学習モデルを取得し、

取得したシリアル形式の機械学習モデルをシリアル形式からモデルオブジェクト形式に変換することで、前記異常検出用の機械学習モデルを取得する、

ことを特徴とする、請求項6に記載の異常検出装置。

[請求項8]

前記第2のテレメトリ情報におけるログ情報、トレース情報及びメ

トリック情報のそれぞれに関する異常の有無を示す前記異常検出結果をGUIに表示する入出力部を更に含む、

ことを特徴とする、請求項1に記載の異常検出装置。

[請求項9]

テレメトリ情報における異常を判定する異常検出装置と、

クライアント端末とが通信ネットワークを介して接続される異常検出システムにおいて、

前記異常検出装置は、

プロセッサとメモリとを備え、

前記メモリは、

第1のマイクロサービスのセットから、

: マイクロサービスの挙動を示すログを含むログ情報と、

: 複数のマイクロサービスの関係を示すトレースを含むトレース情報と、

: マイクロサービスの性能に関する測定値を示すメトリックを含むメトリック情報と、

を含む第1のテレメトリ情報を取得するテレメトリ情報取得部と、

前記第1のテレメトリ情報から抽出した学習用テレメトリ情報をニューラルネットワークによって処理することで、前記トレース情報に対応するトレース埋め込みを生成し、前記ログ情報に対応するログ埋め込みを生成し、前記メトリック情報に対応するメトリック埋め込みを生成する埋め込み生成部と、

前記トレース埋め込み、前記ログ埋め込み及び前記メトリック埋め込みに基づいて、マイクロサービスについて異常の有無を判定する異常検出用の機械学習モデルを生成するモデル生成部と、

前記異常検出用の機械学習モデルを用いて、第2のマイクロサービスのセットについて取得された第2のテレメトリ情報を解析することで、前記第2のマイクロサービスにおける異常の有無を示す異常検

出結果を生成し、前記クライアント端末に出力する異常検出部、

として前記プロセッサを機能させるための処理命令を含むことを特徴とする異常検出システム。

[請求項10]

前記異常検出装置は、

前記異常検出用の機械学習モデルに関する情報を保存するモデルデータベースを格納する記憶部を更に含み、

前記モデル生成部は、

生成した前記異常検出用の機械学習モデルに対するシリアル化を行うことで、シリアル形式の機械学習モデルを生成し、

前記シリアル形式の機械学習モデルと、前記シリアル形式の機械学習モデルを特徴付けるメタデータ及びプロフィール情報とを前記モデルデータベースに保存する、

ことを特徴とする、請求項9に記載の異常検出システム。

[請求項11]

前記異常検出部は、

前記モデルデータベースに対して、前記プロフィール情報に基づく検索を実施することで、前記シリアル形式の機械学習モデルを取得し、

取得したシリアル形式の機械学習モデルをシリアル形式からモデルオブジェクト形式に変換することで、前記異常検出用の機械学習モデルを取得する、

ことを特徴とする、請求項10に記載の異常検出システム。

[請求項12]

異常検出装置において実行されている異常検出方法であって、

異常検出装置は、

プロセッサとメモリと記憶部とを備え、

前記記憶部は、

異常検出用の機械学習モデルに関する情報を保存するモデルデータベースを格納し、

前記メモリは、

第1のマイクロサービスのセットから、

マイクロサービスの挙動を示すログを含むログ情報と、

複数のマイクロサービスの関係を示すトレースを含むトレース情報と、

マイクロサービスの性能に関する測定値を示すメトリックを含むメトリック情報と、

を含む第1のテレメトリ情報を取得する工程と、

前記第1のテレメトリ情報を学習用テレメトリ情報と検証用テレメトリ情報とに分割する工程と、

前記学習用テレメトリ情報における前記トレース情報から、複数のマイクロサービス間の階層関係を示すサービス関係の特徴を抽出する工程と、

前記学習用テレメトリ情報における前記ログ情報から、マイクロサービスの挙動をテキスト形式で示す前記ログの内容を示す意味的特徴と、複数のログ間の関係を示すログ関係の特徴とを抽出する工程と、

前記学習用テレメトリ情報における前記メトリック情報から、前記マイクロサービスの性能に関する測定値の時間的周期性を示す時間的特徴と、複数のメトリック間の依存関係を示すメトリック関係の特徴とを抽出する工程と、

ニューラルネットワークにおける第1の埋め込み層を用いて、所定のグラフ埋め込み手法によって前記サービス関係の特徴を処理することで、前記サービス関係の特徴を低次元空間で表現するトレース埋め込みを生成する工程と、

前記ニューラルネットワークにおける第2の埋め込み層を用いて、所定のグラフ埋め込み手法によって前記意味的特徴及び前記ログ関係の特徴を処理することで、前記意味的特徴及び前記ログ関係の特徴とを低次元空間で表現するログ埋め込みを生成する工程と、

前記ニューラルネットワークにおける第3の埋め込み層を用いて、

所定の時間的埋め込み手法によって前記時間的特徴及び前記メトリック関係の特徴を処理することで、前記時間的特徴と前記メトリック関係の特徴とを低次元空間で表現するメトリック埋め込みを生成する工程と、

前記ニューラルネットワークにおける集約層を用いて、所定の連結演算手法によって前記トレース埋め込み、前記ログ埋め込み及び前記メトリック埋め込みのそれぞれを集約した潜在表現を生成する工程と、

前記ニューラルネットワークにおける予測層を用いて、前記潜在表現に基づいて、前記検証用テレメトリ情報に対する異常予測結果を生成する工程と、

前記異常予測結果が所定の精度閾値を満たす場合、前記第1の埋め込み層、前記第2の埋め込み層、前記第3の埋め込み層、前記集約層及び前記予測層のそれぞれのパラメータに基づいて異常検出用の機械学習モデルを生成する工程と、

生成した前記異常検出用の機械学習モデルに対するシリアル化を行うことで、シリアル形式の機械学習モデルを生成する工程と、

前記シリアル形式の機械学習モデルと、前記シリアル形式の機械学習モデルを特徴付けるメタデータ及びプロフィール情報とを前記モデルデータベースに保存する工程と、

前記モデルデータベースに対して、前記プロフィール情報に基づく検索を実施することで、前記シリアル形式の機械学習モデルを取得する工程と、

取得したシリアル形式の機械学習モデルをシリアル形式からモデルオブジェクト形式に変換することで、前記異常検出用の機械学習モデルを取得する工程と、

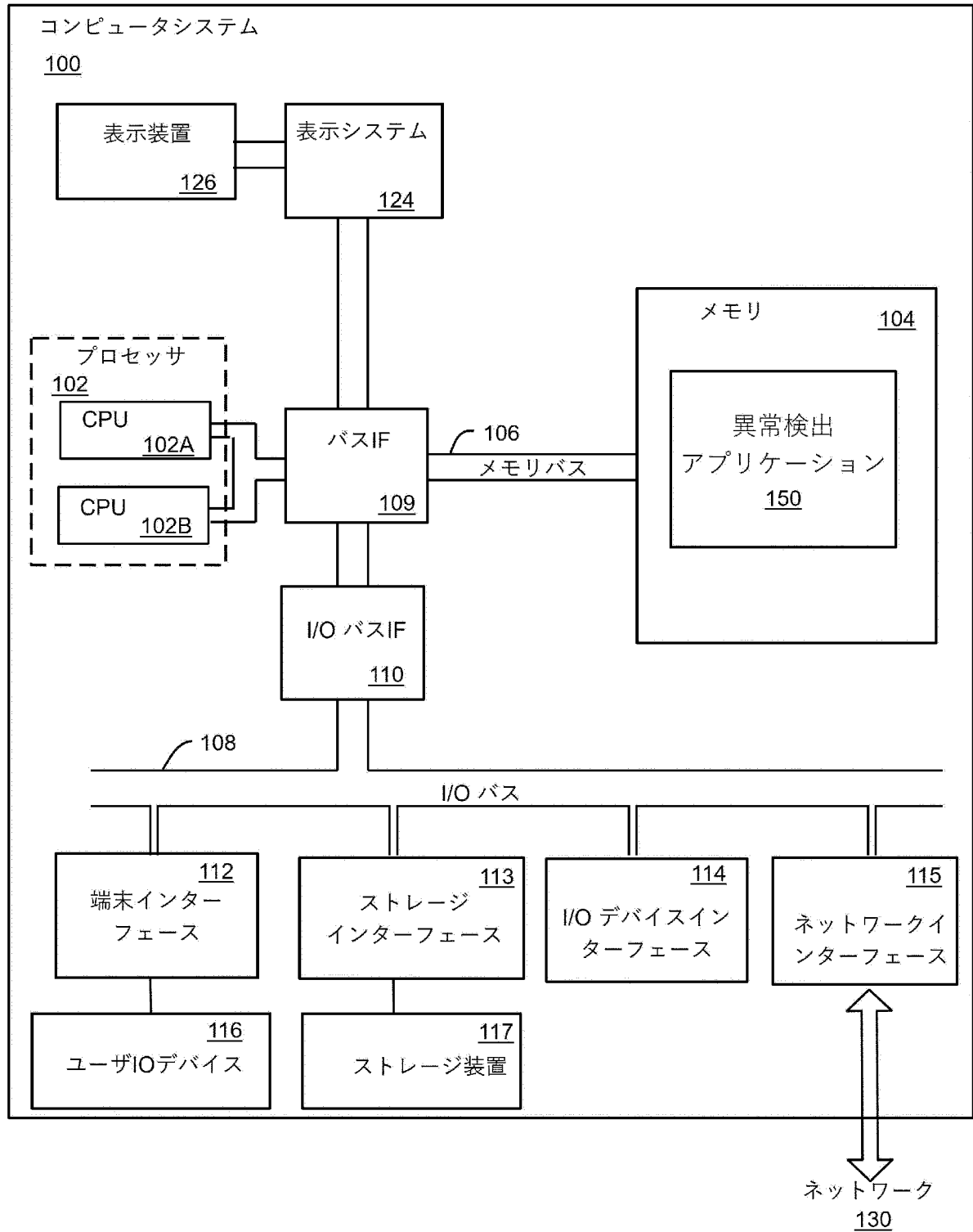
前記異常検出用の機械学習モデルを用いて、第2のマイクロサービスのセットについて取得された第2のテレメトリ情報を解析すること

で、前記第2のマイクロサービスにおける異常の有無を示す異常検出結果を生成する工程と、

を前記プロセッサに実行させる処理命令を含むことを特徴とする異常検出方法。

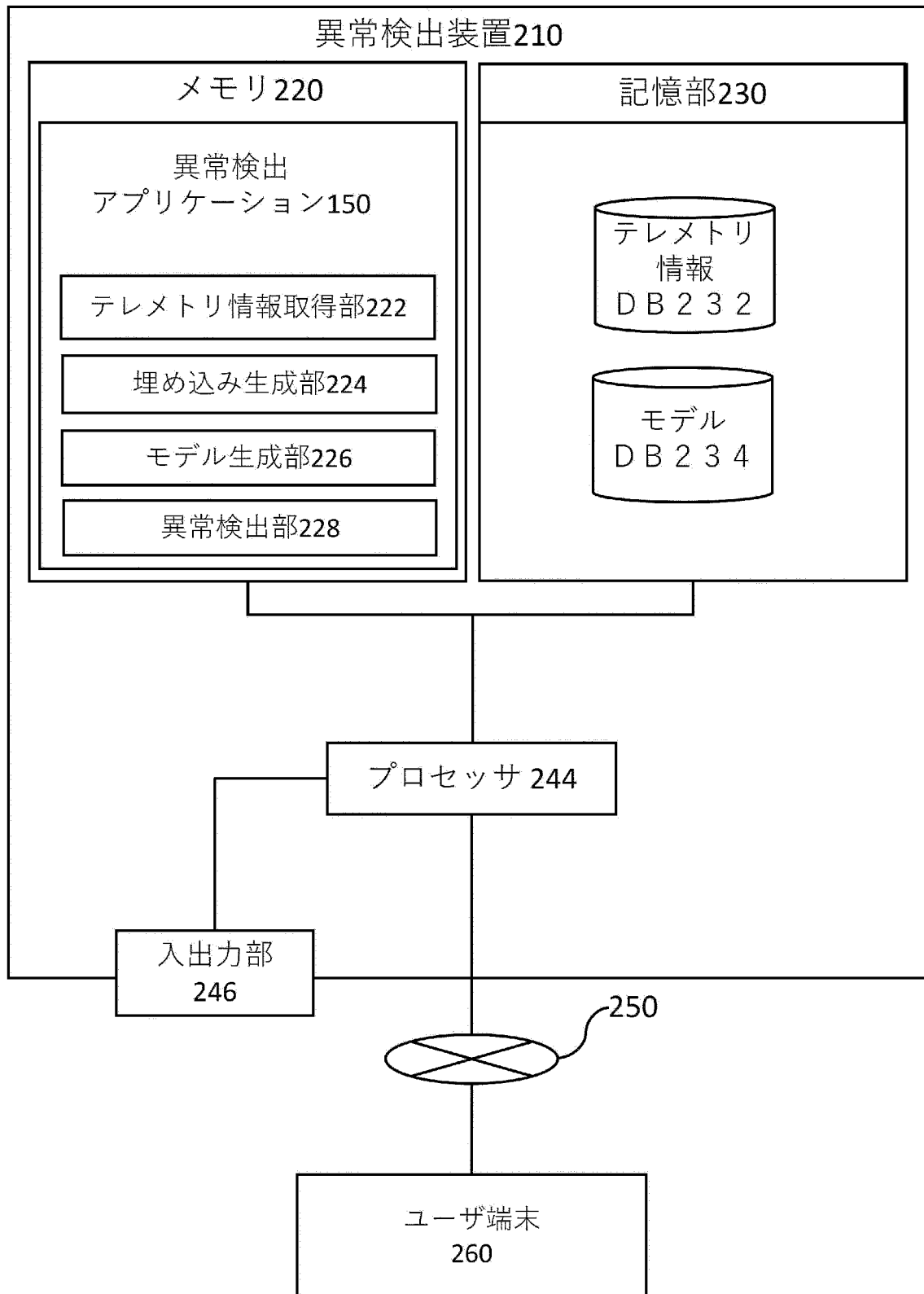
[図1]

図 1



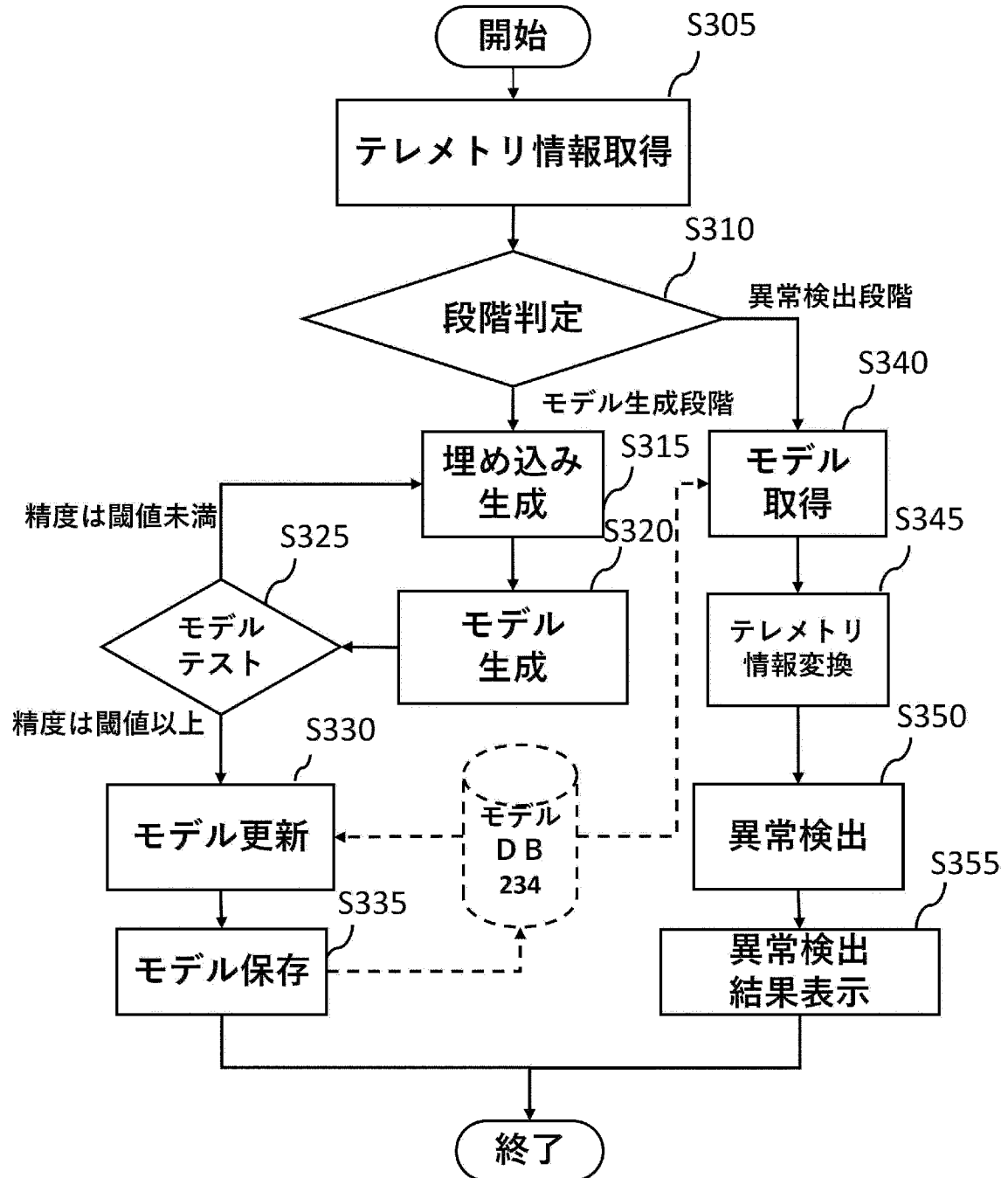
[図2]

図 2 異常検出システム200



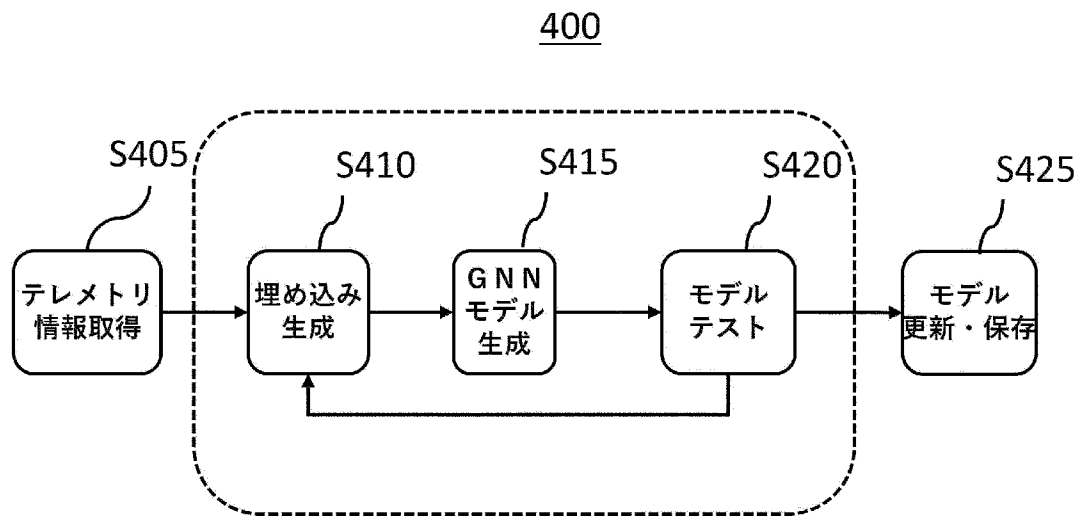
[図3]

図 3



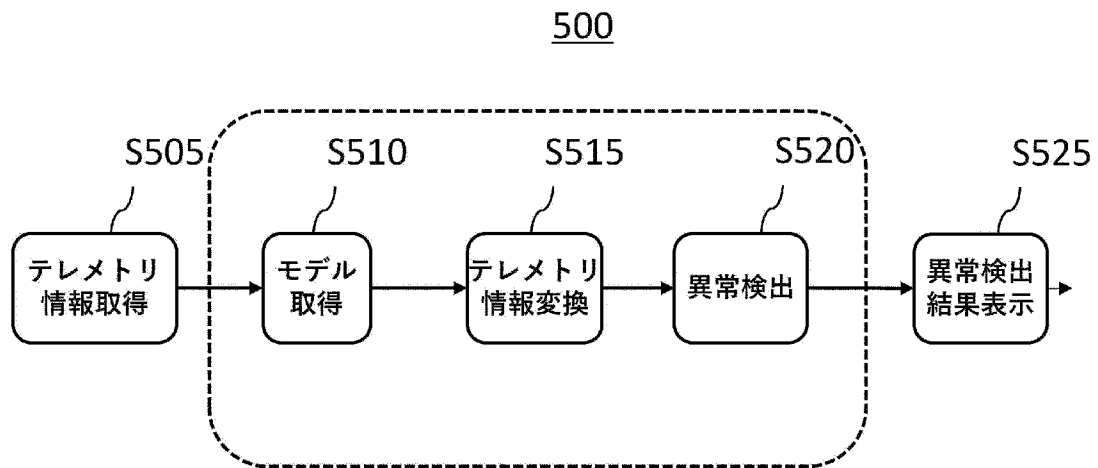
[図4]

図 4



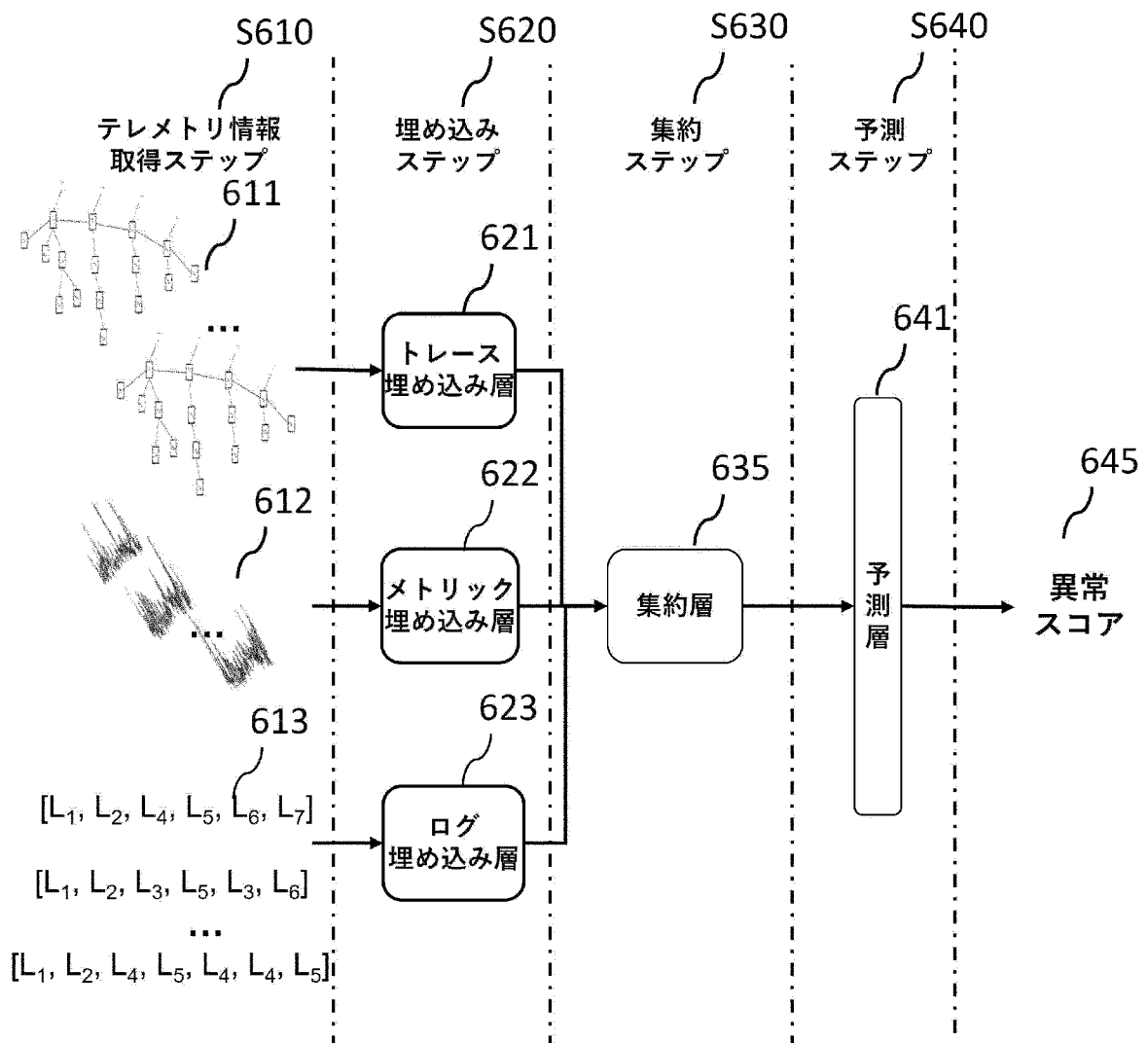
[図5]

図 5



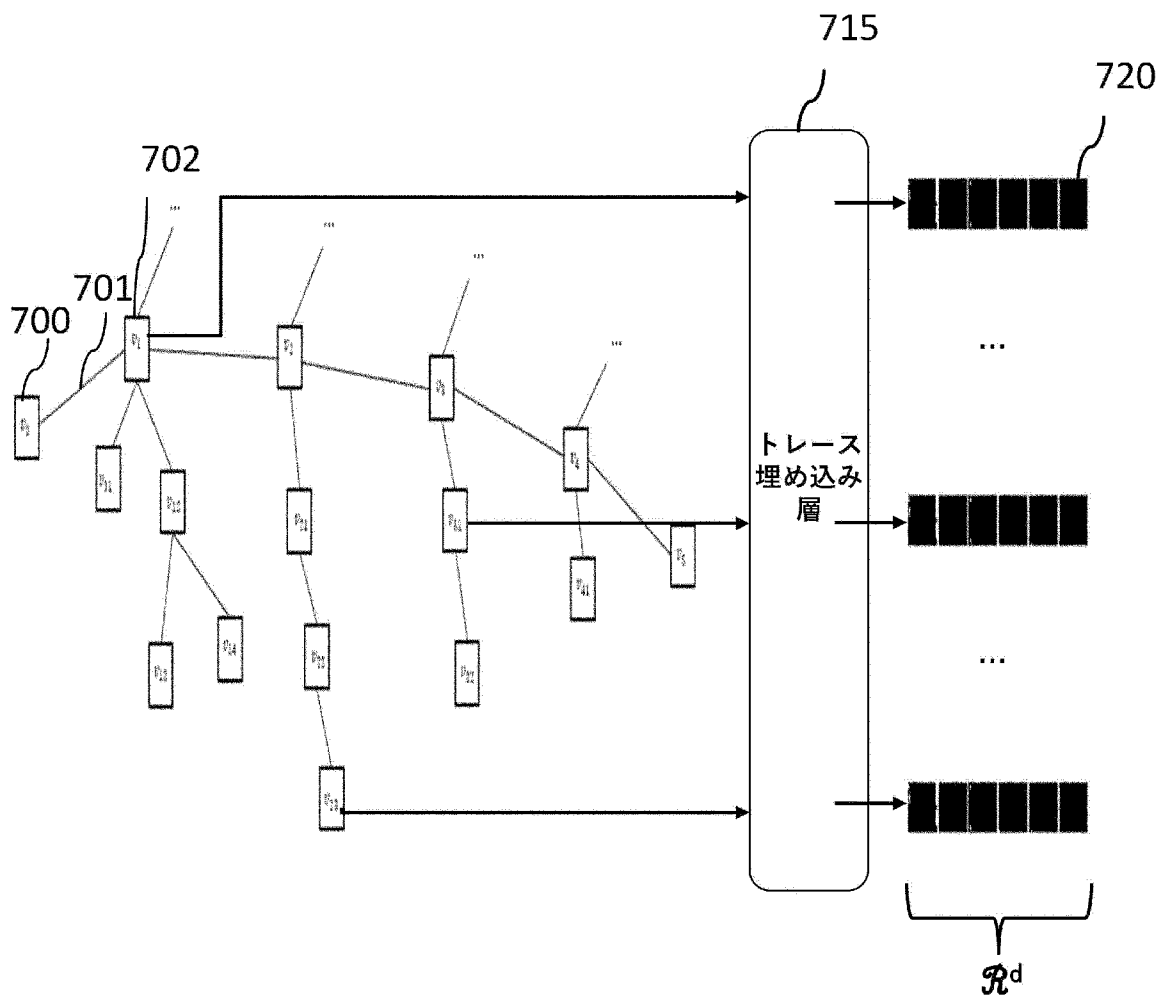
[図6]

図 6



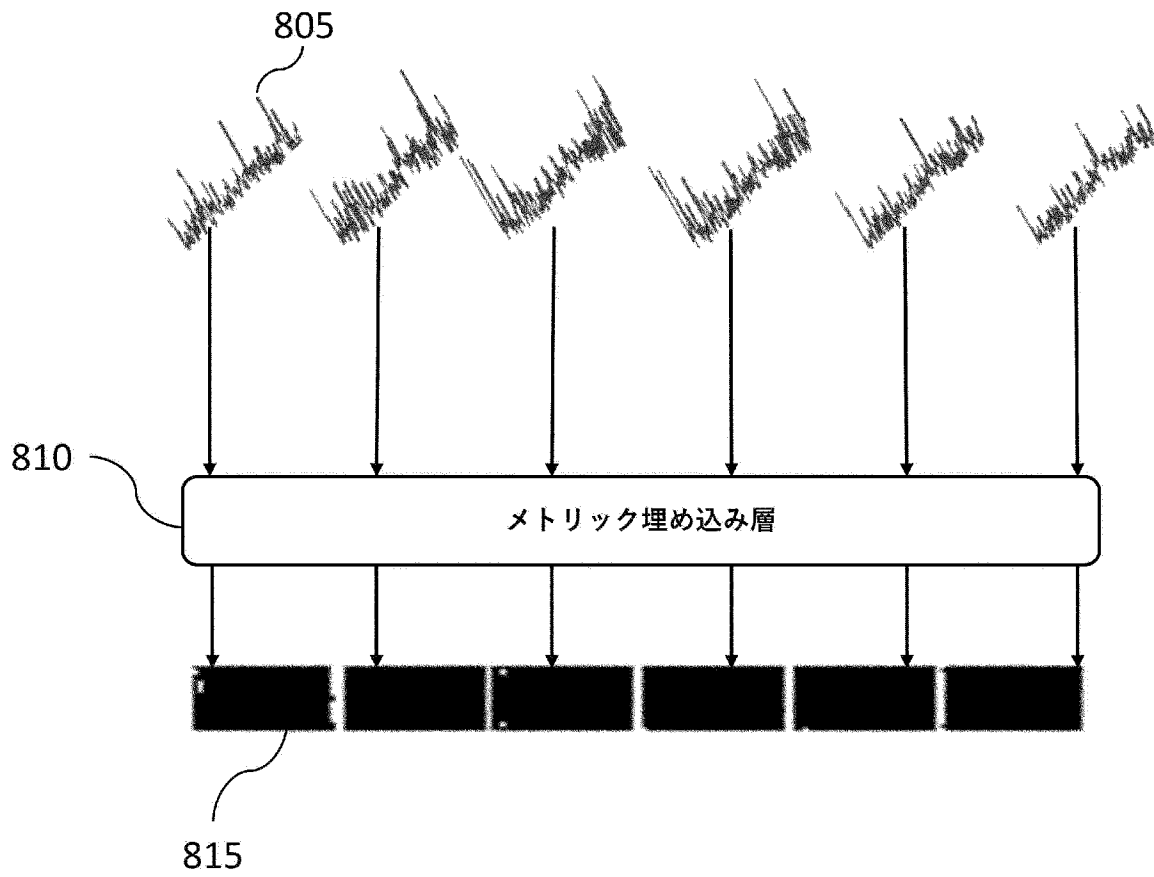
[図7]

図 7



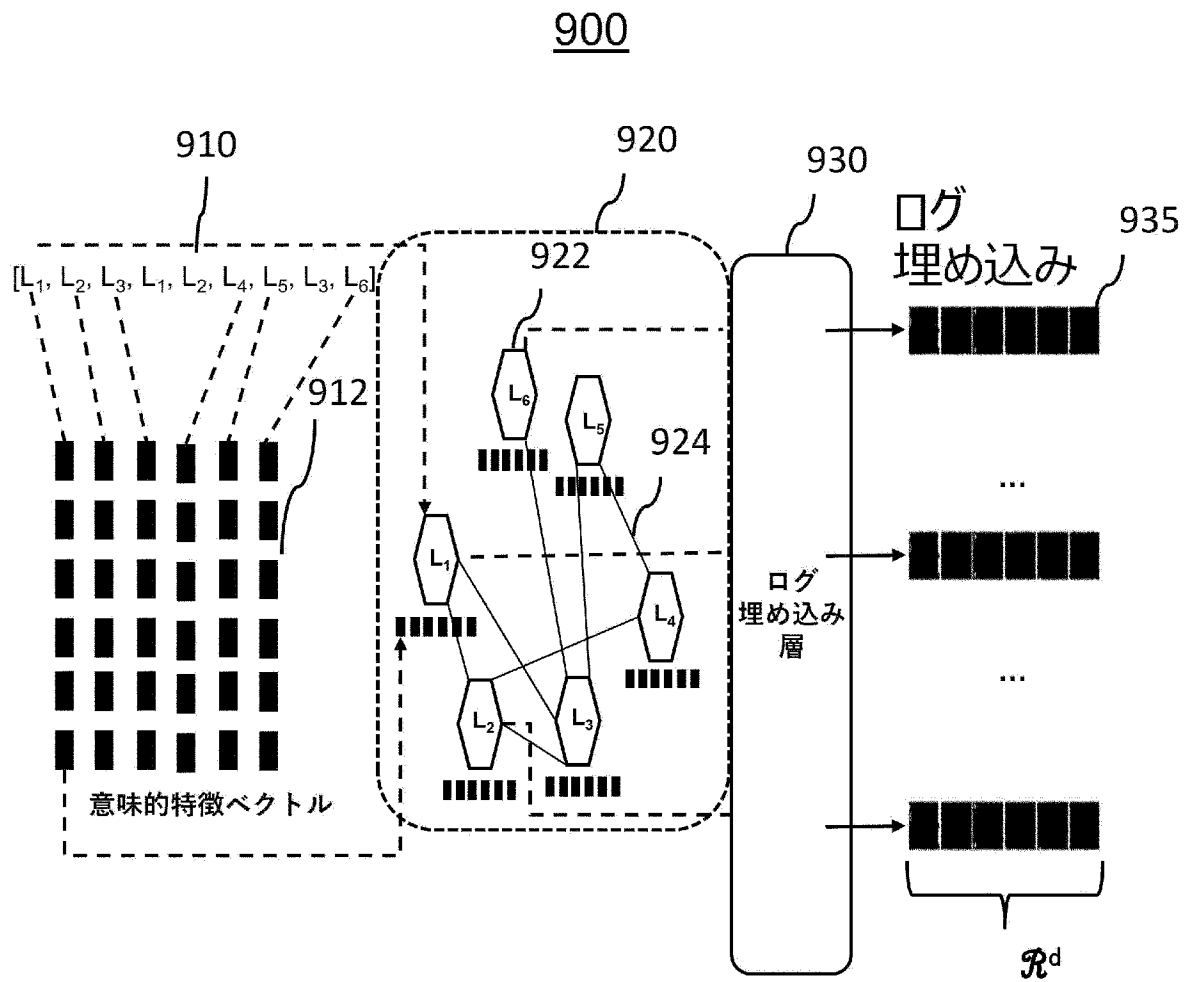
[図8]

図 8



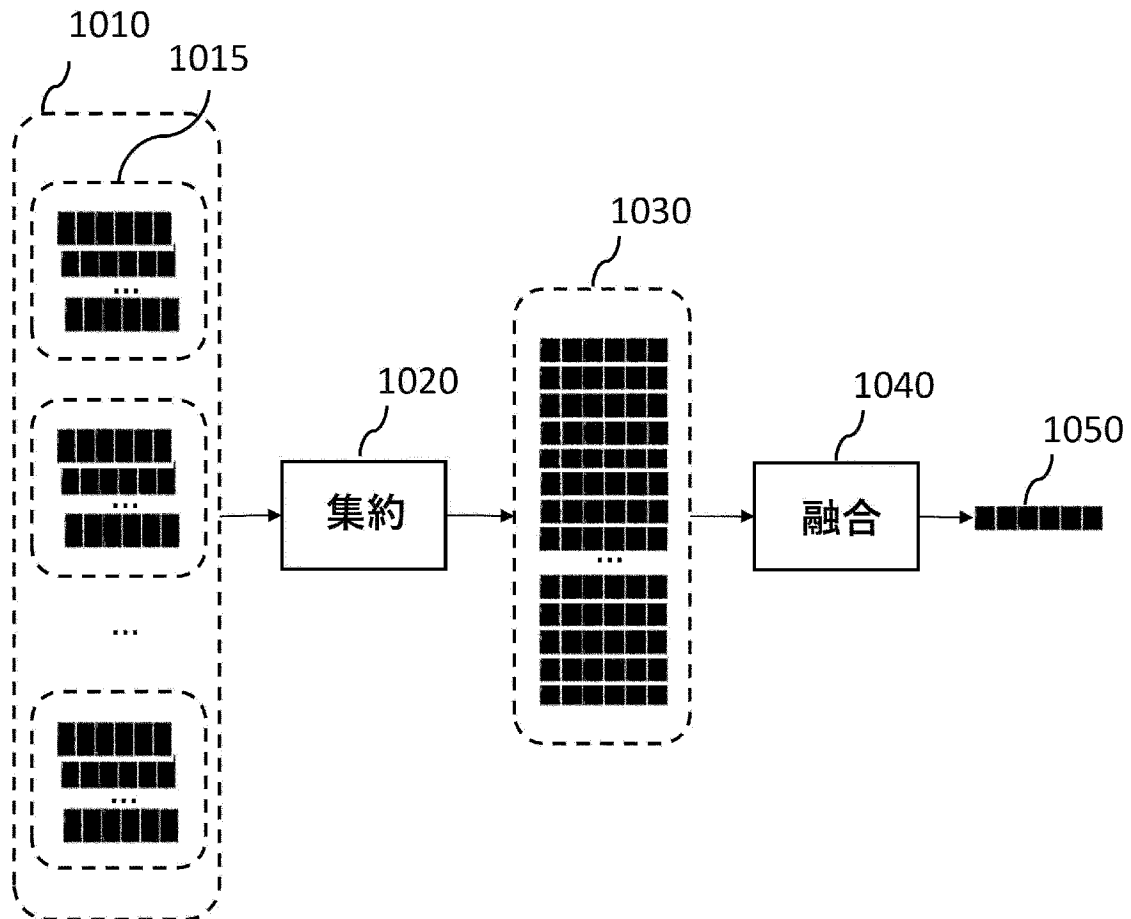
[図9]

図 9



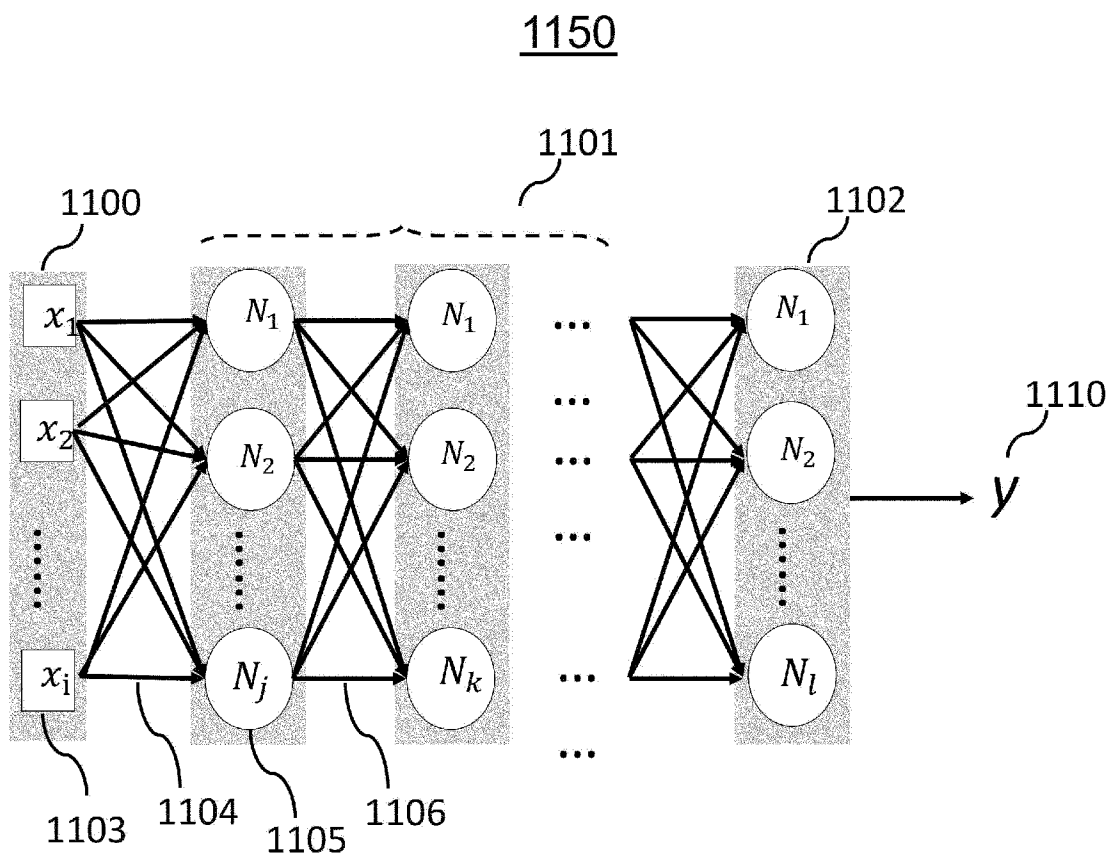
[図10]

図 10

1000

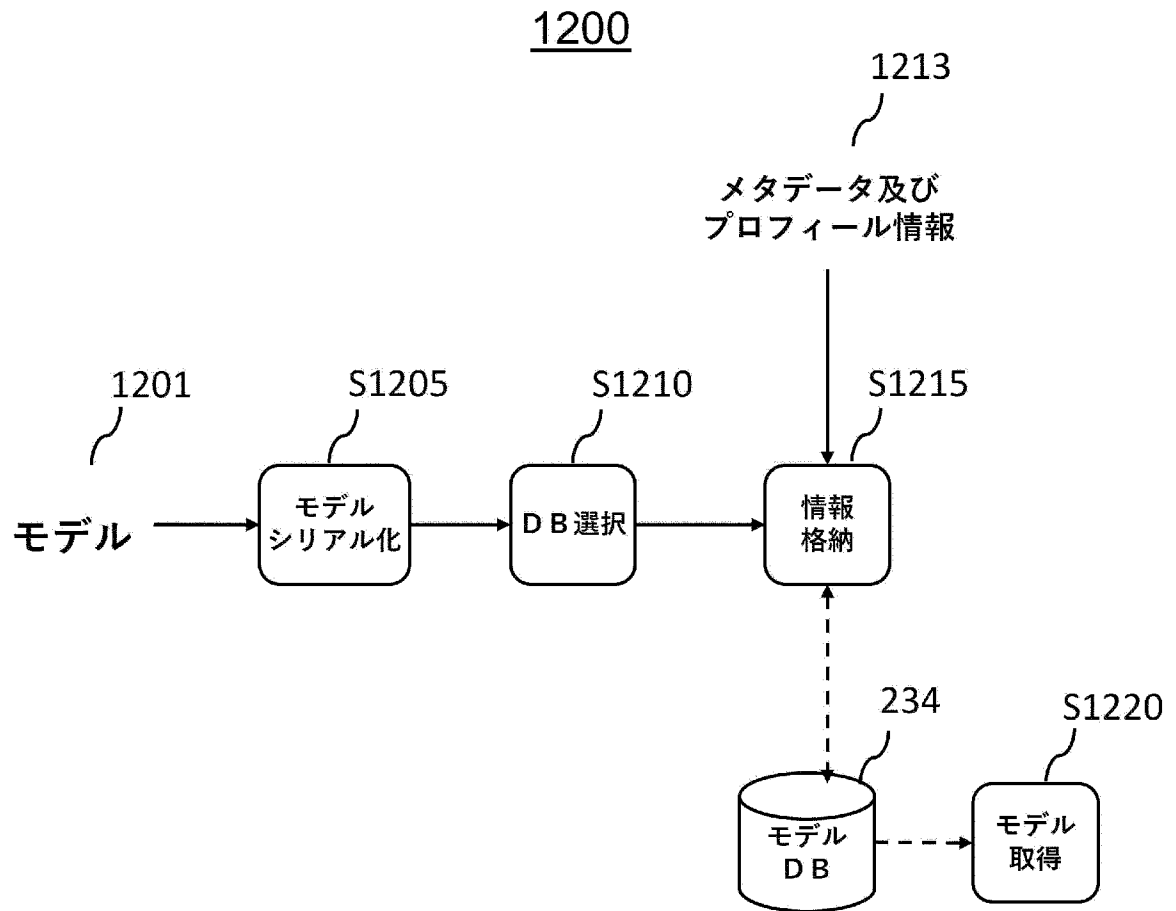
[図11]

図 1 1



[図12]

図 1 2



[図13]

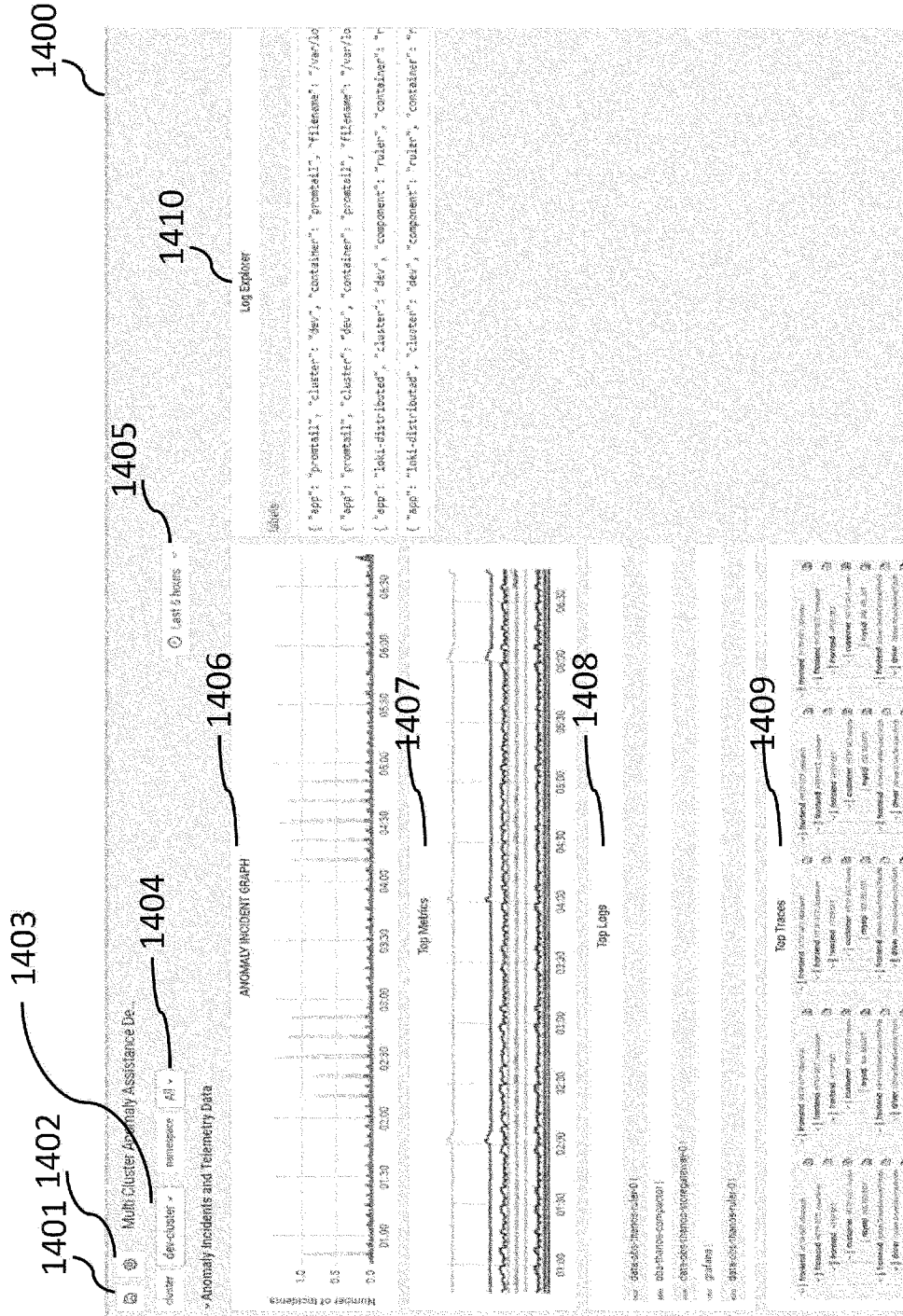
図 1 3

1300

	1301	1302	1303	1304	1305	1306	1307	1308
	モデル ID	作成 日時	モデル アーキ テク チャ	メト リック 統計	デー タ カバ レッジ	バ ー ジ ョ ン	プロ ジェ クト ID	シリアル 形式
1309	(PK, TEXT- INT)	(DATE TIME)	(TEXT)	(TEXT)	(DATE TIME- DATE TIME)	(TE XT)	(TEXT)	(VARBINA RY)
1310	grad- 0001	2023/ 01/01	aen- gnn- shap	acc- 9758- auc- 8918	2022/10 /01- 2022/12 /31	v0. 1	proj- 236e- 8	(VARBINA RY)

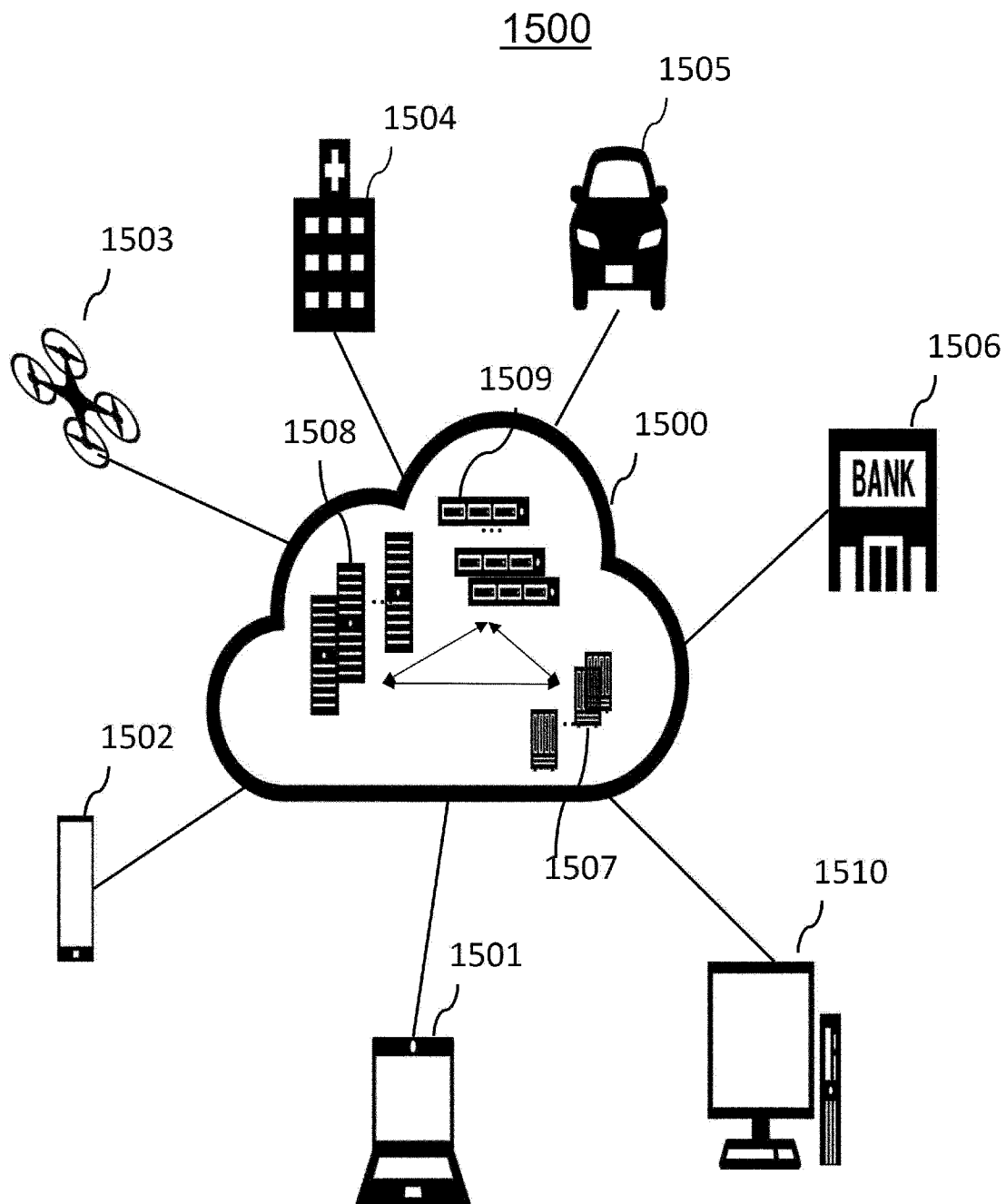
[図14]

図 14



[図15]

図 15



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2024/021994

A. CLASSIFICATION OF SUBJECT MATTER G06F 11/07 (2006.01)i; G06F 11/34 (2006.01)i; G06N 20/00 (2019.01)i FI: G06F11/07 151; G06N20/00 130; G06F11/34 147 According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) G06F11/07; G06F11/34; G06N20/00 Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Published examined utility model applications of Japan 1922-1996 Published unexamined utility model applications of Japan 1971-2024 Registered utility model specifications of Japan 1996-2024 Published registered utility model applications of Japan 1994-2024 Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	BOGATINOVSKI, Jasmin et al. Multi-Source Anomaly Detection in Distributed IT Systems. [online]. 13 January 2021, [retrieved on 22 July 2024], Internet<URL:https://arxiv.org/pdf/2101.04977> particularly, "1 Introduction", "3 Multimodal approach for anomaly detection from heterogeneous data", "5 Conclusion", fig. 2	1, 5-11
A		2-4, 12
Y	US 2022/0172067 A1 (INTERNATIONAL BUSINESS MACHINES CORP.) 02 June 2022 (2022-06-02) paragraphs [0049], [0050], [0059]-[0065], fig. 4, 5, 10, 11	1, 5-11
Y	WO 2022/111154 A1 (INTERNATIONAL BUSINESS MACHINES CORP.) 02 June 2022 (2022-06-02) paragraphs [0059]-[0079], [0128]	1, 5-11
☒ Further documents are listed in the continuation of Box C. ☒ See patent family annex.		
* Special categories of cited documents: “A” document defining the general state of the art which is not considered to be of particular relevance “D” document cited by the applicant in the international application “E” earlier application or patent but published on or after the international filing date “L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) “O” document referring to an oral disclosure, use, exhibition or other means “P” document published prior to the international filing date but later than the priority date claimed “T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention “X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone “Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art “&” document member of the same patent family		
Date of the actual completion of the international search 19 July 2024		Date of mailing of the international search report 13 August 2024
Name and mailing address of the ISA/JP Japan Patent Office (ISA/JP) 3-4-3 Kasumigaseki, Chiyoda-ku, Tokyo 100-8915 Japan		Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2024/021994

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2020/0364612 A1 (VISA INTERNATIONAL SERVICE ASSOCIATION) 19 November 2020 (2020-11-19) paragraph [0090]	6, 7, 10, 11

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/JP2024/021994

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
US	2022/0172067	A1	02 June 2022	(Family: none)	
WO	2022/111154	A1	02 June 2022	(Family: none)	
US	2020/0364612	A1	19 November 2020	(Family: none)	

A. 発明の属する分野の分類（国際特許分類（IPC））
G06F 11/07(2006.01)i; G06F 11/34(2006.01)i; G06N 20/00(2019.01)i
FI: G06F11/07 151; G06N20/00 130; G06F11/34 147

B. 調査を行った分野
調査を行った最小限資料（国際特許分類（IPC））
G06F11/07; G06F11/34; G06N20/00
最小限資料以外の資料で調査を行った分野に含まれるもの
日本国実用新案公報 1922-1996年
日本国公開実用新案公報 1971-2024年
日本国実用新案登録公報 1996-2024年
日本国登録実用新案公報 1994-2024年
国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
Y	BOGATINOVSKI, Jasmin ほか, Multi-Source Anomaly Detection in Distributed IT Systems, [online], 2021.01.13, [検索日 2024.07.22]、インターネット<URL : https://arxiv.org/pdf/2101.04977 > 特に、「1 Introduction」、「3 Multimodal approach for anomaly detection from heterogeneous data」、「5 Conclusion」Fig. 2	1,5-11
A		2-4,12
Y	US 2022/0172067 A1 (INTERNATIONAL BUSINESS MACHINES CORPORATION) 02.06.2022 (2022-06-02) 段落0049, 0050, 0059-0065, FIGs. 4, 5, 10, 11	1,5-11
Y	WO 2022/111154 A1 (INTERNATIONAL BUSINESS MACHINES CORPORATION) 02.06.2022 (2022-06-02) 段落0059-0079, 0128	1,5-11
Y	US 2020/0364612 A1 (VISA INTERNATIONAL SERVICE ASSOCIATION) 19.11.2020 (2020-11-19) 段落0090	6,7,10,11

☐ C欄の続きにも文献が列挙されている。☒ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー
“A” 特に関連のある文献ではなく、一般的技术水準を示すもの
“D” 国際出願で出願人が先行技術文献として記載した文献
“E” 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
“I” 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
“O” 口頭による開示、使用、展示等に言及する文献
“P” 国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献

“T” 国際出願日又は優先日後に公表された文献であって出願と抵触するものではなく、発明の原理又は理論の理解のために引用するもの
“X” 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
“Y” 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
“&” 同一パテントファミリー文献

国際調査を完了した日
19.07.2024

国際調査報告の発送日
13.08.2024

名称及びあて先
日本国特許庁(ISA/JP)
〒100-8915
日本国
東京都千代田区霞が関三丁目4番3号

権限のある職員（特許庁審査官）

久々宇 篤志 5B 4678

電話番号 03-3581-1101 内線 3529

国際調査報告
パテントファミリーに関する情報

国際出願番号
PCT/JP2024/021994

引用文献			公表日	パテントファミリー文献	公表日
US	2022/0172067	A1	02.06.2022	(ファミリーなし)	
WO	2022/111154	A1	02.06.2022	(ファミリーなし)	
US	2020/0364612	A1	19.11.2020	(ファミリーなし)	