

明 細 書

発明の名称： 監視システム、監視方法、及びプログラム

技術分野

[0001] 本開示は、監視システム、監視方法、及びプログラムに関する。

背景技術

[0002] 従来、サービスにおける異常の検知、復旧、又は分析といった種々の目的のために、監視対象となる装置の状態に関する状態データが解析されている。例えば、特許文献1には、ある装置の状態データが示す時系列的な状態の変化と、当該装置の実際の稼働状態と、の関係が学習されたモデルに基づいて、当該装置の異常の有無を判定するシステムが記載されている。特許文献2には、過去における装置のメモリ使用量の履歴と、現在における当該装置のメモリ使用量と、に基づいて、将来的な当該装置のメモリ使用量が閾値を超えるか否かを推定するシステムが記載されている。例えば、特許文献3には、システムに障害（異常の一例）が発生した場合に、当該システムにおける装置の状態に関する状態データと、当該システムに発生した障害を復旧するための復旧手順と、の関連度を計算する計算モデルに基づいて、当該システムに発生した障害を復旧させるために有効な復旧手順を特定することが記載されている。

先行技術文献

特許文献

[0003] 特許文献1：国際公開2017／169949号公報

特許文献2：特表2022－511938号公報

特許文献3：特開2021－015321号公報

発明の概要

発明が解決しようとする課題

[0004] 上記のような技術では、サービスにおける監視対象となる装置の状態に関する状態データに基づいて、サービスにおける異常に関する処理を実行する

ことが求められている。

- [0005] 本開示の目的の1つは、サービスにおける監視対象となる装置の状態に関する状態データに基づいて、サービスにおける異常に関する処理を実行することである。

課題を解決するための手段

- [0006] 本開示に係る監視システムは、サービスにおける監視対象となる装置の状態に関する状態データを取得する状態データ取得部を含み、前記状態データに基づいて、前記サービスにおける異常に関する処理を実行する。

発明の効果

- [0007] 本開示によれば、サービスにおける監視対象となる装置の状態に関する状態データに基づいて、サービスにおける異常に関する処理を実行できる。

図面の簡単な説明

- [0008] [図1]監視システムのハードウェア構成の一例を示す図である。
[図2]通信サービスで異常が発生していない場合の通信装置の時系列的な通信量の変化の一例を示す図である。
[図3]通信サービスで異常が検知された場合の通信装置の時系列的な通信量の変化の一例を示す図である。
[図4]管理者端末に表示される通知の一例を示す図である。
[図5]監視システムで実現される機能の一例を示す図である。
[図6]状態データベースの一例を示す図である。
[図7]期間設定部により設定される期間の一例を示す図である。
[図8]監視システムで実行される処理の一例を示す図である。
[図9]変形例1-1の監視システムで実現される機能の一例を示す図である。
[図10]通信サービスで異常が検知された場合の通信装置の時系列的な通信量の変化の一例を示す図である。
[図11]管理者端末に表示される通知の一例を示す図である。
[図12]監視システムで実現される機能の一例を示す図である。
[図13]状態データベースの一例を示す図である。

[図14]クラスタリングの実行結果の一例を示す図である。

[図15]監視システムで実行される処理の一例を示す図である。

[図16]変形例の監視システムで実現される機能の一例を示す図である。

発明を実施するための形態

[0009] [1. 第1実施形態]

本開示に係る監視システムの実施形態の一例である第1実施形態を説明する。第1実施形態では、サービスにおける異常に関する処理の一例を説明する。従来の技術では、種々の装置の種々の状態データが存在するので、サービスの提供者が、サービスにおける異常に関係のある状態データを特定できれば、サービスにおける異常の検知、復旧、又は分析といった種々の目的で利用できる。非常に有用である。しかしながら、従来の技術は、装置の状態に関する種々の状態データの中から、どの状態データが異常に関係しているかを特定することはできない。そこで、第1実施形態の監視システムは、サービスにおける異常に状態データが関係するか否かを判定する。

[0010] [1-1. 監視システムのハードウェア構成]

図1は、監視システムのハードウェア構成の一例を示す図である。例えば、監視システム1は、サーバ10、通信装置20、ユーザ端末30、及び管理者端末40を含む。サーバ10、通信装置20、ユーザ端末30、及び管理者端末40の各々は、ネットワークNに接続可能である。例えば、ネットワークNは、インターネット、公衆通信回線、又はLANである。

[0011] サーバ10は、サーバコンピュータである。本実施形態では、通信事業者がサーバ10を管理する場合を例に挙げる。例えば、サーバ10は、制御部11、記憶部12、及び通信部13を含む。制御部11は、少なくとも1つのプロセッサを含む。記憶部12は、RAM等の揮発性メモリと、フラッシュメモリ等の不揮発性メモリと、の少なくとも一方を含む。通信部13は、有線通信用の通信インタフェースと、無線通信用の通信インタフェースと、の少なくとも一方を含む。

[0012] 通信装置20は、他の装置と通信を行う装置である。例えば、通信装置2

0は、通信事業者が管理する装置である。通信装置20は、無線通信用の装置であってもよいし、有線通信用の装置であってもよい。通信装置20は、ユーザによる通話及びデータ通信の少なくとも一方を中継する。例えば、通信装置20は、公衆通信回線の基地局、構内交換機、無線LANのアクセスポイント、ルーター、ハブ、リピータ、モデム、又は仮想化技術で利用されるサーバコンピュータである。通信装置20は、完全仮想化クラウドネイティブモバイルネットワークをユーザに提供する通信事業者の装置であってもよい。

[0013] ユーザ端末30は、通信サービスを利用するユーザのコンピュータである。例えば、ユーザ端末30は、スマートフォン、タブレット、パーソナルコンピュータ、又はウェアラブル端末である。例えば、ユーザ端末30は、制御部31、記憶部32、通信部33、操作部34、及び表示部35を含む。制御部31、記憶部32、及び通信部33のハードウェア構成は、それぞれ制御部11、記憶部12、及び通信部13と同様であってよい。操作部34は、タッチパネル又はマウス等の入力デバイスである。表示部35は、液晶又は有機EL等のディスプレイである。

[0014] 管理者端末40は、通信サービスにおける管理者のコンピュータである。例えば、管理者端末40は、スマートフォン、タブレット、パーソナルコンピュータ、又はウェアラブル端末である。例えば、管理者端末40は、制御部41、記憶部42、通信部43、操作部44、及び表示部45を含む。制御部41、記憶部42、通信部43、操作部44、及び表示部45のハードウェア構成は、それぞれ制御部11、記憶部12、通信部13、操作部34、及び表示部35と同様であってよい。

[0015] なお、記憶部12、32、42に記憶されるプログラムは、ネットワークNを介して供給されてもよい。また、各コンピュータには、コンピュータ読み取り可能な情報記憶媒体を読み取る読取部（例えば、メモリカードスロット）と、外部機器とデータの入出力をするための入出力部（例えば、USBポート）と、の少なくとも一方が含まれてもよい。例えば、情報記憶媒体に

記憶されたプログラムが、読取部及び入出力部の少なくとも一方を介して供給されてもよい。

[0016] また、監視システム1は、少なくとも1つのコンピュータを含めばよく、図1の例に限られない。例えば、監視システム1は、通信装置20、ユーザ端末30、及び管理者端末40の少なくとも1つを含まなくてもよい。この場合、当該少なくとも1つは、監視システム1の外部に存在する。監視システム1は、サーバ10だけを含んでもよい。監視システム1は、サーバ10と、図1に示さない他のコンピュータと、を含んでもよい。監視システム1は、管理者端末40だけを含んでもよい。監視システム1は、管理者端末40と、図1に示さない他のコンピュータと、を含んでもよい。

[0017] [1-2. 監視システムの概要]

本実施形態では、通信装置20が、コンテナ化されたネットワーク機能であるCNF (Containerized Network Function) を有するサーバコンピュータである場合を例に挙げる。更に、ユーザ端末30がスマートフォンである場合を例に挙げる。通信装置20は、多数のユーザ端末30の通信を中継する。例えば、通信装置20が処理すべき通信量が、当該通信装置20が処理可能な通信量に達すると、通信サービスで異常が発生する可能性がある。通信量は、bps等の公知の指標によって表現可能である。

[0018] 例えば、通信サービスで異常が発生すると、管理者は、異常の要因となった通信装置20を特定して復旧作業を行う。しかしながら、通信サービスでは、多数の通信装置20が存在し、種々の異常が発生しうるので、管理者が、異常の要因となった通信装置20を特定するのが難しいことがある。このとき、異常の要因となった通信装置20は、それ以上の通信を処理しきれないので、通信量が飽和する場合がある。

[0019] 通信量が飽和するとは、通信量が正の状態であり（通信量が0ではない状態であり）、かつ、通信量が増加しない又は略増加しないことである。通信量が増加しないとは、通信量の変化量が0のことである。通信量が略増加しないとは、通信量の変化量が閾値未満であることである。飽和の具体的な判

定方法は、後述する。通信量は、上限値が定められていてもよいが、管理者が定めた上限値よりも多くの通信量を通信装置 20 が処理可能な場合や、管理者が定めた上限値よりも低い通信量しか通信装置 20 が処理できない場合もあり、さらには、管理者自身、通信装置 20 の上限値を知らない場合もあるので、本実施形態では、通信量の上限値が定められていないものとする。このため、通信装置 20 の通信量が一定程度に達したとしても、異常が検知されるわけではないものとする。

[0020] 図 2 は、通信サービスで異常が発生していない場合の通信装置 20 の時系列的な通信量の変化の一例を示す図である。図 2 の横軸は、時間を示す軸である。図 2 の縦軸は、通信量を示す軸である。図 2 の例では、通信事業者の施設に配置された 3 台の通信装置 20 A ~ 20 C の各々の通信量の変化が示されている。以降、通信装置 20 A ~ 20 C を区別しない時は、単に通信装置 20 という。図 2 のように、通信サービスで異常が発生していない場合には、各通信装置 20 の通信量は、飽和していない。即ち、各通信装置 20 の通信量は、原則として、常に変化している。

[0021] 図 3 は、通信サービスで異常が検知された場合の通信装置 20 の時系列的な通信量の変化の一例を示す図である。図 3 の例では、時点 t_{00} から時点 t_{01} までの期間において、通信装置 20 C の通信量が飽和している。当該期間では、通信装置 20 C は、それ以上の通信を処理できないので、ある特定のエリアで通信装置 20 C に接続を試みたユーザ端末 30 が、通信サービスを利用できない可能性がある。このような場合に、ユーザは、通信サービスのコールセンターに連絡し、通信サービスを利用できないことを伝えることがある。

[0022] 例えば、管理者は、複数のユーザからの問い合わせを受けて、異常が発生していることを把握する。この時点では、管理者は、どの通信装置 20 が異常の要因であるかを特定しておらず、その後、時点 t_{01} が訪れて通信装置 20 C の通信量が下がり、異常が自然解消したものとする。更に、管理者は、ユーザからの問い合わせを受けなくなった場合に、異常が解消したことを

特定したものとする。時点 t_{01} が訪れると、ユーザ端末 30 が通信サービスを利用できるようになるので、異常が発生していた期間と、通信装置 20C の通信量と、の間には相関関係がある。なお、本実施形態では、飽和開始タイミングから飽和終了タイミングまでの期間を異常が発生していた期間の一例として取り扱うが、飽和開始タイミングから飽和が終了していない現時点までの期間を異常が発生していた期間の一例として取り扱ってもよい。例えば、飽和開始タイミングから、管理者が指定した時点までの期間を異常が発生していた期間の一例として取り扱ってもよい。

[0023] 例えば、サーバ 10 は、異常が発生して解消した後に、通信装置 20A～20C の各々の通信量を解析する。サーバ 10 は、異常が発生していた期間において、通信装置 20C の通信量が飽和していたことを特定する。サーバ 10 は、今回発生した異常の特徴と、通信装置 20C の通信量が当該異常に関係していることと、を関連付けて記憶しておく。サーバ 10 は、同様の異常が再び発生した場合に、管理者端末 40 に対し、通信装置 20C の状態をチェックすることを促す通知を送信する。

[0024] 図 4 は、管理者端末 40 に表示される通知の一例を示す図である。例えば、管理者が、管理者端末 40 にインストールされたメンテナンス用のツールを起動すると、サーバ 10 から受信した通知を示す管理者画面 SC が表示部 45 に表示される。管理者画面 SC には、過去に同様の異常が検知された場合に通信装置 20C の通信量が飽和したので、今回も通信装置 20C の状態をチェックすることを示すメッセージが表示される。

[0025] 例えば、過去に通信装置 20C の通信量が飽和した場合に、通信サービスのコールセンターが、ある特定のエリア X から通信サービスを利用しようとしたユーザからの問い合わせを受けたとする。現時点で、コールセンターが、同じエリア X から通信サービスを利用しようとしたユーザからの問い合わせを受けた場合に、エリア X における通信サービスで異常が発生したことが検知される。この場合、サーバ 10 は、管理者端末 40 に対し、通信装置 20C の状態を確認することを促す管理者画面 SC の表示データを送信する。

[0026] 例えば、管理者端末40は、管理者画面SCの表示データを受信すると、通信装置20Cの状態を確認することを促すメッセージを含む管理者画面SCを表示部45に表示させる。管理者画面SCには、現在の通信装置20Cの通信量を示すグラフが表示されてもよいし、過去に同様の異常が発生した時の通信装置20Cの通信量を示すグラフが表示されてもよい。管理者は、管理者画面SCを確認し、通信装置20Cのメンテナンスを行う。通信装置20Cのメンテナンス自体は、公知の方法で行われてもよい。

[0027] 以上のように、監視システム1は、通信サービスで異常が発生して復旧した場合に、通信装置20の通信量が飽和していたか否かを判定する。監視システム1は、通信装置20の通信量が飽和していたか否かの判定結果に基づいて、通信サービスにおける異常に、通信装置20の通信量が関係するか否かを判定する。例えば、同様の異常が再び発生した場合に、管理者が、異常の要因となった通信装置20を特定しやすくなり、迅速に復旧作業を行うことができるようになる。以降、本実施形態の詳細を説明する。

[0028] [1-3. 監視システムで実現される機能]

図5は、監視システム1で実現される機能の一例を示す図である。図5では、サーバ10で実現される機能と、管理者端末40で実現される機能と、が示されている。通信装置20及びユーザ端末30の各々の機能は、公知の通信サービスにおける機能と同様のため、図5では省略する。例えば、通信装置20は、サーバ10に対し、後述の状態データ又はその一部の情報を送信する機能を有する。ユーザ端末30は、ユーザが通信サービスを利用するための機能を有する。

[0029] [1-3-1. サーバで実現される機能]

例えば、サーバ10は、データ記憶部100、状態データ取得部101、期間設定部102、正規化実行部103、飽和判定部104、関係判定部105、及び復旧処理実行部106を含む。データ記憶部100は、記憶部12により実現される。状態データ取得部101、期間設定部102、正規化実行部103、飽和判定部104、関係判定部105、及び復旧処理実行部

106は、制御部11により実現される。

[0030] [データ記憶部]

データ記憶部100は、通信サービスに関するデータを記憶する。例えば、データ記憶部100は、状態データベースDBを記憶する。

[0031] 図6は、状態データベースDBの一例を示す図である。状態データベースDBは、複数の通信装置20の各々の状態データが格納されたデータベースである。例えば、状態データベースDBには、複数の通信装置20の各々の識別情報と、当該通信装置20の状態を示す状態データと、が格納される。状態データベースDBには、他のデータが格納されてもよい。例えば、状態データベースDBには、飽和判定部の判定結果を示す情報、又は、関係判定部の判定結果を示す情報が格納されてもよい。

[0032] 通信装置20の識別情報は、任意の情報であってもよく、例えば、IPアドレス、装置名、又はMACアドレスであってもよい。状態データは、ある一時点における通信装置20のピンポイントの状態を示してもよいが、本実施形態では、状態データは、通信装置20の時系列的な状態の変化に関するデータである。通信装置20の状態は、通信装置20の負荷ということもできる。通信装置20の状態は、ハードウェア的な状態を意味してもよいし、ソフトウェア的な状態を意味してもよい。

[0033] 本実施形態では、通信装置20の通信量が通信装置20の状態に相当する場合を例に挙げるが、通信装置20の他の状態が通信装置20の状態に相当してもよい。他の状態としては、通信装置20のリソースの消費量、サービスに対するリクエストの処理時間（レスポンスタイム）、又はリクエストに対して返されたエラーの数であってもよい。状態データは、ゴールデンシグナルメトリクスと呼ばれる指標であってもよいし、公知のベンチマークテストで利用されるその他の指標であってもよい。例えば、状態データは、CPU使用量、メモリ使用量、電力消費量、通信速度、温度、又はこれらの組み合わせであってもよい。

[0034] なお、状態データは、通信サービス又は他のサービスにおける業績に関す

る状態を示してもよい。他のサービスは、ユーザが通信サービスを介して利用するサービスであり、例えば、電子商取引サービス、旅行予約サービス、決済サービス、又は金融サービスである。例えば、状態データは、通信装置20に接続中（通信サービス又は他のサービスにログイン中）のユーザの数、ユーザが通信装置20を経由して実行した決済、又はユーザが通信装置20を経由して行った注文であってもよい。決済数、決済額、注文数、及び注文額が増えるほど、通信装置20の負荷が高まるので、決済数、決済額、注文数、及び注文額も、通信装置20の状態に相当する。

[0035] 本実施形態では、状態データには、通信装置20の時系列的な状態の変化が示されている。例えば、状態データは、通信装置20の状態が取得された日時と、当該日時における通信装置20の状態を示す数値と、を含む。通信装置20の状態は、数値ではなく、文字等の他の形式で表現されてもよい。本実施形態では、通信装置20の通信量が通信装置20の状態に相当するので、状態データは、通信装置20の通信量が取得された日時と、当該日時における通信装置20の通信量と、を含む。

[0036] なお、データ記憶部100に記憶されるデータは、状態データベースDBに限られない。データ記憶部100は、通信サービスに関する何らかのデータを記憶すればよい。例えば、データ記憶部100は、飽和判定部104の判定結果を示すデータを記憶してもよい。データ記憶部100は、関係判定部105の判定結果を示すデータを記憶してもよい。データ記憶部100は、管理者端末40に管理者画面SCを表示させるために必要なデータを記憶してもよい。データ記憶部100は、後述の処理で利用される各種閾値を記憶してもよい。閾値は、管理者が指定してもよいし、機械学習の手法や統計的な手法に基づいて決定されてもよい。

[0037] [状態データ取得部]

状態データ取得部101は、状態データを取得する。例えば、状態データ取得部101は、複数の通信装置20の各々に対し、定期的（例えば、1秒～30秒程度、又は、1分～5分程度）に、当該通信装置20の状態を要求

する。通信装置２０は、サーバ１０から、状態データ取得部１０１の要求を受信すると、サーバ１０に対し、自身の識別情報と、自身の状態を示す情報と、を送信する。状態データ取得部１０１は、当該通信装置２０の識別情報に関連付けられた状態データに、現在の日時と、通信装置２０から受信した情報と、を追加する。

[0038] なお、通信装置２０は、ある程度の期間の状態データを蓄積して、サーバ１０に対し、一度に状態データを送信してもよい。この場合、状態データ取得部１０１は、通信装置２０から、一度に状態データを取得して状態データベースＤＢに格納する。他にも例えば、状態データ取得部１０１は、定期的ではなく不定期的に、通信装置２０から状態データを取得してもよい。状態データ取得部１０１は、管理者が指示したタイミングで、通信装置２０から状態データを取得してもよい。

[0039] 通信装置２０は、通信サービスにおける監視対象となる装置の一例である。監視対象となる装置は、任意の装置であってよく、通信装置２０に限られない。本実施形態で通信装置２０と記載した箇所は、監視対象となる他の装置に読み替えることができる。他の装置は、通信サービスで利用されている装置であればよく、例えば、サーバ１０、サーバ１０以外の他のコンピュータ、サーバ１０及び他のコンピュータに含まれるＣＰＵ・メモリ・ネットワークカード等の部品、バッテリー、アンテナ、通信ケーブル、又はセンサであってもよい。

[0040] 本実施形態では、状態データ取得部１０１は、異常が検知された場合に、状態データを取得する。異常が検知された場合に取得される状態データは、異常が発生してから解消するまでの期間の全部又は一部における状態を示す。以降、この期間を異常期間という。状態データは、異常期間の全部又は一部だけではなく、異常期間以外の他の期間における状態も示してもよい。状態データ取得部１０１は、異常が発生してから解消するまでの間に、状態データを取得してもよいし、異常が解消した後に、事後的に状態データを取得してもよい。

[0041] 本実施形態では、状態データには、あるピンポイントのタイミングにおける状態が示されるのではなく、状態データには、ある程度の長さを有する期間における状態が示される。例えば、状態データ取得部101は、期間設定部102により設定された期間における装置の時系列的な状態の変化に関する状態データを取得する。本実施形態では、後述の期間設定部102により飽和期間、基準期間、及び異常期間といった3つの期間が設定されるので、状態データ取得部101は、飽和期間、基準期間、及び異常期間の各々における通信装置20の状態を示す状態データを取得する。

[0042] なお、状態データ取得部101は、飽和期間、基準期間、及び異常期間以外の他の期間における通信装置20の状態を示す状態データを取得してもよい。例えば、状態データ取得部101は、飽和期間よりも前における通信装置20の状態を示す状態データを取得してもよい。状態データ取得部101は、基準期間及び異常期間よりも後における通信装置20の状態を示す状態データを取得してもよい。状態データ取得部101は、異常が発生した異常発生タイミングに関係なく、通信装置20の状態を示す状態データを取得してもよい。状態データ取得部101は、状態データベースDBに格納された状態データを、任意のタイミングで取得可能である。

[0043] [期間設定部]

期間設定部102は、状態データに関する期間を設定する。状態データに関する期間とは、後述の関係判定部105の判定で利用される期間である。状態データに状態が示された全ての期間が後述の関係判定部105の判定で利用されてもよいが、本実施形態では、状態データに状態が示された一部の期間だけが後述の関係判定部105の判定で利用されるものとする。期間を設定するとは、期間の開始時点及び終了時点を決定することである。

[0044] 図7は、期間設定部102により設定される期間の一例を示す図である。本実施形態では、期間設定部102が、飽和期間T1、基準期間T2、及び異常期間T3といった3つの期間を設定する場合を例に挙げる。図7のタイムウィンドウWは、状態データのうち、関係判定部105等の処理で利用さ

れる期間である。図7の例では、基準期間T2及び異常期間T3を合わせた期間がタイムウィンドウWになる。

[0045] 例えば、期間設定部102は、飽和期間T1、基準期間T2、及び異常期間T3のうちの何れか1つ又は2つだけを設定してもよい。即ち、期間設定部102は、飽和期間T1だけ、基準期間T2だけ、異常期間T3だけ、飽和期間T1及び基準期間T2だけ、飽和期間T1及び異常期間T3だけ、又は、基準期間T2及び異常期間T3だけを設定してもよい。期間設定部102は、飽和期間T1、基準期間T2、及び異常期間T3を設定せずに、タイムウィンドウWだけを設定してもよい。

[0046] 例えば、期間設定部102は、飽和判定部104の判定結果に基づいて、状態データに関する飽和期間T1を設定する。図7の例では、期間設定部102は、状態データが示す状態が飽和を開始した飽和開始タイミングt1から、状態データが示す状態が飽和を終了した飽和終了タイミングt2までの期間を、飽和期間T1として設定する。飽和開始タイミングt1は、状態データに状態が示された日時のうち、飽和判定部104が飽和を開始したと判定した日時である。飽和終了タイミングt2は、状態データに状態が示された日時のうち、飽和判定部104が飽和を終了したと判定した日時である。なお、期間設定部102は、飽和開始タイミングt1から飽和が終了していない（飽和が継続している）現在のタイミングまでの期間を飽和期間T1として設定してもよい。例えば、期間設定部102は、飽和開始タイミングt1から、管理者が指定した時点までの期間を飽和期間T1として設定してもよい。

[0047] 例えば、期間設定部102は、異常が検知された場合に、異常が発生した異常発生タイミングt3に基づいて、状態データに関する基準期間T2及び異常期間T3を設定する。本実施形態では、異常が検知された場合に、管理者が、管理者端末40から、異常が発生したことを示す異常発生操作を行う。例えば、管理者は、ユーザから、異常が発生したことを示す問い合わせを受け付けると、異常発生操作を行う。

- [0048] 例えば、サーバ10は、管理者端末40から、異常発生操作を示す異常発生データを受信したか否かを判定することによって、異常が発生したか否かを判定する。サーバ10は、管理者端末40から異常発生データを受信しない場合には、異常が発生したと判定しない。管理者端末40から異常発生データを受信した場合に、異常が発生したと判定する。サーバ10が異常発生データを受信したタイミングが異常発生タイミングt3である。
- [0049] なお、管理者は、ユーザからの問い合わせではなく、他の判断要素に基づいて、異常発生操作を行ってもよい。例えば、管理者は、管理者画面SC又はその他の画面で、通信装置20の状態データを目視で確認して異常発生操作を行ってもよい。異常の発生を推定するプログラムの実行結果が管理者画面SC又はその他の画面に表示される場合、管理者は、当該実行結果を目視で確認して異常発生操作を行ってもよい。
- [0050] また、サーバ10が異常の発生を検知する方法自体は、任意の方法であってよく、管理者による異常発生操作に限られない。例えば、サーバ10は、異常の発生を検知するための異常検知プログラムの実行結果に基づいて、異常の発生を検知してもよい。異常検知プログラムは、状態データに基づいて、異常が発生したか否かを判定する。例えば、異常検知プログラムは、状態データが示す状態が基準範囲を超えた場合に、異常が発生したと判定する。
- [0051] 例えば、異常検知プログラムは、状態データが示す状態が基準範囲を超えた状態が所定時間以上継続した場合に、異常が発生したと判定してもよい。異常検知プログラムは、状態データが示す状態が基準範囲を超えた回数又は頻度が閾値以上になった場合に、異常が発生したと判定してもよい。この場合、異常検知プログラムが異常と判定したタイミングが異常発生タイミングt3である。
- [0052] 図7の例では、期間設定部102は、基準期間T2の基準となる基準タイミングt4から、異常が発生した異常発生タイミングt3までの期間を、基準期間T2として設定する。例えば、基準タイミングt4は、異常発生タイミングt3の所定時間だけ前のタイミングである。基準タイミングt4は、

現時点の所定時間だけ前のタイミングであってもよいし、管理者が指定したタイミングであってもよい。

[0053] 例えば、期間設定部 102 は、異常発生タイミング t_3 から、異常が解消した異常解消タイミング t_5 までの期間を、異常期間 T_3 として設定する。異常解消タイミング t_5 は、異常が解消したと判定されたタイミングである。本実施形態では、異常が解消した場合に、管理者が、管理者端末 40 から、異常が解消したことを示す異常解消操作を行う。例えば、管理者は、ユーザから、異常が発生したことを示す問い合わせを受け付けなくなると、異常解消操作を行う。

[0054] 例えば、サーバ 10 は、管理者端末 40 から、異常解消操作を示す異常解消データを受信したか否かを判定することによって、異常が解消したか否かを判定する。サーバ 10 は、管理者端末 40 から異常解消データを受信しない場合には、異常が解消したと判定しない。管理者端末 40 から異常解消データを受信した場合に、異常が解消したと判定する。サーバ 10 が異常解消データを受信したタイミングが異常解消タイミング t_5 である。

[0055] なお、管理者は、ユーザからの問い合わせではなく、他の判断要素に基づいて、異常解消操作を行ってもよい。例えば、管理者は、管理者画面 SC 又はその他の画面で、通信装置 20 の状態データを目視で確認して異常解消操作を行ってもよい。異常の解消を推定するプログラムの実行結果が管理者画面 SC 又はその他の画面に表示される場合、管理者は、当該実行結果を目視で確認して異常解消操作を行ってもよい。

[0056] また、サーバ 10 が異常の解消を検知する方法自体は、任意の方法であってもよく、管理者による異常解消操作に限られない。例えば、サーバ 10 は、異常の解消を検知するための異常解消プログラムの実行結果に基づいて、異常の解消を検知してもよい。異常解消プログラムは、状態データに基づいて、異常が解消したか否かを判定する。例えば、異常解消プログラムは、状態データが示す状態が基準範囲に収まった場合に、異常が解消したと判定する。

[0057] 例えば、異常解消プログラムは、状態データが示す状態が基準範囲に収まった状態が所定時間以上継続した場合に、異常が解消したと判定してもよい。異常解消プログラムは、状態データが示す状態が基準範囲に収まった回数又は頻度が閾値以上になった場合に、異常が解消したと判定してもよい。この場合、異常解消プログラムが異常解消と判定したタイミングが異常解消タイミング t_5 である。

[0058] [正規化実行部]

正規化実行部 103 は、状態データに関する正規化を実行する。例えば、正規化実行部 103 は、複数の通信装置 20 の各々の状態データに基づいて、正規化を実行する。正規化実行部 103 は、複数の通信装置 20 の各々の状態データが示す状態の数値が、ある一定の範囲内に収まるように、正規化を実行する。正規化実行部 103 は、公知の正規化手法に基づいて、正規化を実行すればよい。例えば、正規化手法は、 z スコア正規化手法、又は、最小－最大正規化手法であってもよい。

[0059] [飽和判定部]

飽和判定部 104 は、状態データに基づいて、通信装置 20 の時系列的な状態が飽和しているか否かを判定する。飽和とは、状態データが示す状態の変化量が閾値未満になること、又は、当該変化量が当該閾値未満の状態が所定時間以上継続することである。通信量のように、原則として上限値が存在しない場合、通信量が増加すれば、変化量は、主に増加量を意味する。そのため、ある期間で変化量の合計が増加した後に、状態データが示す状態の増加量が閾値未満になること、又は、当該増加量が当該閾値未満の状態が所定時間以上継続することが、飽和に相当する。変化量は、ある一定程度の期間における積算値であってもよいし、ある時点と次の時点の変化量であってもよい。変化量は、通信量の減少量を意味してもよい。つまり、飽和判定部 104 は、状態データが示す当該変化量そのものの時系列的な変化に基づいて、当該飽和の判定を行う。

[0060] 例えば、飽和判定部 104 は、状態データが示す状態の増加量が閾値以上

の状態から、当該増加量が閾値未満の状態、又は、当該増加量が閾値未満の状態が所定時間以上継続した状態になった場合に、通信装置 20 の時系列的な状態が飽和していると判定する。飽和判定部 104 は、状態データが示す状態の増加量が閾値未満の状態、又は、当該増加量が閾値未満の状態が所定時間以上継続した状態になったとしても、その前において、当該増加量が閾値未満の状態であれば、通信装置 20 の時系列的な状態が飽和していないと判定する。例えば、飽和判定部 104 は、状態データが示す状態が閾値以上であり、かつ、当該状態の増加量が閾値未満の状態、又は、当該増加量が閾値未満の状態が所定時間以上継続した状態になった場合に、通信装置 20 の時系列的な状態が飽和していると判定してもよい。飽和判定部 104 は、状態データが示す状態の増加量が閾値未満の状態、又は、当該増加量が閾値未満の状態が所定時間以上継続した状態になったとしても、当該状態が閾値未満であれば、通信装置 20 の時系列的な状態が飽和していないと判定する。

[0061] 例えば、飽和判定部 104 は、複数の通信装置 20 の各々の状態データと、予め定められた閾値と、に基づいて、当該通信装置 20 の時系列的な状態が飽和しているか否かを判定する。別の言い方をすれば、飽和判定部 104 は、通信装置 20 の状態データごとに、予め定められた閾値に基づいて、当該状態データが示す時系列的な状態が飽和しているか否かを判定する。飽和判定部 104 が飽和を判定する際に参照される閾値は、管理者が指定してもよいし、過去の異常の傾向から計算されてもよい。閾値は、機械学習の手法を利用したモデルに基づいて決定されてもよい。

[0062] なお、飽和判定部 104 は、閾値を利用せずに、機械学習の手法を利用したモデルに基づいて、通信装置 20 の状態が飽和しているか否かを判定してもよい。この場合、モデルには、訓練用の状態データが示す時系列的な状態の変化を入力とし、当該状態が飽和しているか否かを示すラベルを出力とする訓練データが学習されている。飽和判定部 104 は、学習済みのモデルに判定対象の状態データを入力し、モデルから出力されたラベルに基づいて、通信装置 20 の状態が飽和しているか否かを判定してもよい。

- [0063] 例えば、飽和判定部 104 は、ある通信装置 20 の状態データが示す変化量が閾値以上であるか否かを判定することによって、当該通信装置 20 の時系列的な状態が飽和しているか否かを判定する。飽和判定部 104 は、ある通信装置 20 の状態データが示す変化量が閾値以上であると判定された場合には、当該通信装置 20 の時系列的な状態が飽和していると判定しない。飽和判定部 104 は、ある通信装置 20 の状態データが示す変化量が閾値未満であると判定された場合には、当該通信装置 20 の時系列的な状態が飽和していると判定する。
- [0064] 例えば、飽和判定部 104 は、ある通信装置 20 の状態データが示す変化量が閾値未満である状態が所定時間以上継続しているか否かを判定することによって、当該通信装置 20 の時系列的な状態が飽和しているか否かを判定する。飽和判定部 104 は、ある通信装置 20 の状態データが示す変化量が閾値未満である状態が所定時間以上継続していないと判定された場合には、当該通信装置 20 の時系列的な状態が飽和していると判定しない。飽和判定部 104 は、ある通信装置 20 の状態データが示す変化量が閾値未満である状態が所定時間以上継続していると判定された場合には、当該通信装置 20 の時系列的な状態が飽和していると判定する。
- [0065] 本実施形態では、飽和判定部 104 は、異常が検知された場合に、通信装置 20 の状態データに基づいて、当該通信装置 20 の状態が飽和しているか否かを判定する。即ち、飽和判定部 104 は、異常が発生した後に、通信装置 20 の状態データに基づいて、当該通信装置 20 の状態が飽和しているか否かを判定する。例えば、飽和判定部 104 は、正規化が実行された状態データに基づいて、通信装置 20 の状態が飽和しているか否かを判定する。飽和判定部 104 は、正規化が実行された状態データが示す状態に基づいて、通信装置 20 の状態が飽和しているか否かを判定する。
- [0066] なお、本実施形態では、飽和判定部 104 は、状態データが示す状態のうち、タイムウィンドウ W 内の状態に基づいて、当該状態が飽和しているか否かを判定する場合を説明する。飽和判定部 104 は、タイムウィンドウ W に

関係なく、状態データが示す状態が飽和しているか否かを判定してもよい。例えば、飽和判定部 104 は、状態データが示す状態のうち、基準期間 T2 内の状態に基づいて、当該状態が飽和しているか否かを判定してもよい。飽和判定部 104 は、状態データが示す状態のうち、異常期間 T3 内の状態に基づいて、当該状態が飽和しているか否かを判定してもよい。飽和判定部 104 は、状態データが示す全期間の状態に基づいて、当該状態が飽和しているか否かを判定してもよい。

[0067] [関係判定部]

関係判定部 105 は、飽和判定部 104 の判定結果に基づいて、通信サービスにおける異常に状態データが関係するか否かを判定する。異常に状態データが関係するとは、異常と、状態データと、の間に相関関係があることである。異常が発生すると、状態データが示す状態が飽和する場合には、異常が状態データに關係する。異常が検知された場合に、状態データが示す状態が必ず飽和する必要はなく、異常と、状態データと、の間にある程度の相関関係があればよい。例えば、異常が n (n は、自然数) 回発生した場合に、状態データが示す状態が飽和になっている回数が k (k は、 n 以下の自然数) 回以上である場合には、異常に状態データが関係する。ただし、 k は、 n の所定割合 (例えば、70%) 以上であるものとする。

[0068] 本実施形態では、関係判定部 105 は、異常が検知された場合に、異常に状態データが関係するか否かを判定する。即ち、関係判定部 105 は、異常が発生した後に、異常に状態データが関係するか否かを判定する。関係判定部 105 は、異常が解消する前に (即ち、異常期間 T3 中に)、異常に状態データが関係するか否かを判定してもよいが、本実施形態では、関係判定部 105 は、異常が解消した後に、異常に状態データが関係するか否かを判定する場合を例に挙げる。

[0069] 例えば、関係判定部 105 は、状態データに変化が示された期間のうち、状態が飽和していると判定された飽和期間 T1 に基づいて、異常に状態データが関係するか否かを判定する。状態データに変化が示された期間とは、状

態データが含むタイムスタンプの期間である。飽和期間 T_1 は、飽和判定部104により通信装置20の状態が飽和していると判定された期間である。即ち、飽和期間 T_1 は、状態データが示す状態の変化量が閾値未満の期間、又は、状態データが示す状態の変化量が閾値未満の状態が継続している期間である。

[0070] 例えば、関係判定部105は、状態データに変化が示された期間のうち、異常が発生している異常期間 T_3 と、状態が飽和していると判定された飽和期間 T_1 と、の一致度に基づいて、異常に状態データが関係するか否かを判定してもよい。ここでの一致度とは、飽和期間 T_1 及び異常期間 T_3 が重複する重複期間の長さ又は割合である。飽和期間 T_1 及び異常期間 T_3 が一致するほど、重複期間が長く又は重複期間の割合が高くなる。例えば、関係判定部105は、飽和期間 T_1 及び異常期間 T_3 が重複する重複期間を計算し、当該重複期間に基づいて、異常に状態データが関係するか否かを判定する。

[0071] 例えば、関係判定部105は、重複期間の長さが閾値未満である場合には、異常に状態データが関係するとは判定せず、重複期間の長さが閾値以上である場合には、異常に状態データが関係すると判定する。閾値は、予め定められていてもよいし、飽和期間 T_1 及び異常期間 T_3 の少なくとも一方の長さに基づいて定められてもよい。例えば、関係判定部105は、重複期間が、飽和期間 T_1 及び異常期間 T_3 の少なくとも一方の所定割合（例えば、8割）未満であれば、異常に状態データが関係しないと判定し、重複期間が当該所定割合以上であれば、異常に状態データが関係すると判定してもよい。

[0072] なお、関係判定部105が、飽和期間 T_1 に基づいて、異常に状態データが関係するか否かを判定する方法は、重複期間に基づく方法に限られない。例えば、関係判定部105は、飽和期間 T_1 が異常発生タイミング t_3 を含むか否かを判定することによって、異常に状態データが関係するか否かを判定してもよい。この場合、関係判定部105は、飽和期間 T_1 が異常発生タイミング t_3 を含まない場合には、異常に状態データが関係しないと判定し

、飽和期間T 1が異常発生タイミングt 3を含む場合に、異常に状態データが関係すると判定してもよい。

[0073] 他にも例えば、関係判定部105は、飽和期間T 1の長さが閾値以上であるか否かを判定することによって、異常に状態データが関係するか否かを判定してもよい。関係判定部105は、飽和期間T 1の長さが閾値未満である場合には、異常に状態データが関係しないと判定し、飽和期間T 1の長さが閾値以上である場合に、異常に状態データが関係すると判定してもよい。

[0074] 例えば、関係判定部105は、状態データに変化が示された期間のうち、異常が発生している異常期間T 3よりも前の他の期間における状態の最高値に基づいて、異常に状態データが関係するか否かを判定してもよい。他の期間は、異常期間T 3よりも前の期間であればよい。本実施形態では、基準期間T 2が他の期間に相当する場合を例に挙げる。他の期間は、異常期間T 3の直前でもよいし、異常期間T 3の直前ではないが、異常期間T 3からある程度前の期間であってもよい。他の期間は、基準期間T 2よりも前の期間であってもよい。なお、異常期間T 3は、異常発生タイミングt 3から多少離れたタイミングを含んでもよい。最高値は、ある期間内における通信量の最大値である。

[0075] 例えば、関係判定部105は、他の期間（本実施形態では、基準期間T 2）における状態の最高値と、他の期間よりも前の期間における状態の最高値と、に基づいて、異常に状態データが関係するか否かを判定してもよい。他の期間よりも前の期間は、基準期間T 2よりも前の期間である。例えば、他の期間よりも前の期間は、基準期間T 2よりも前の全期間であってもよいし、基準期間T 2よりも前の一部の期間であってもよい。最高値は、時系列的な変化のピークとなる値である。関係判定部105は、状態データベースD Bを参照し、他の期間における最高値と、他の期間よりも前の期間における状態の最高値と、を取得する。

[0076] 例えば、関係判定部105は、他の期間（本実施形態では、基準期間T 2）における状態の最高値が、他の期間よりも前の期間における状態の最高値

未満であるか否かを判定する。関係判定部 105 は、他の期間（本実施形態では、基準期間 T2）における状態の最高値が、他の期間よりも前の期間における状態の最高値以上である場合には、異常に状態データが関係しないと判定し、他の期間（本実施形態では、基準期間 T2）における状態の最高値が、他の期間よりも前の期間における状態の最高値未満である場合に、異常に状態データが関係すると判定する。

[0077] 例えば、関係判定部 105 は、状態データに変化が示された期間のうち、異常が発生している異常期間 T3 における状態データが示す状態の最高値に基づいて、異常に状態データが関係するか否かを判定してもよい。関係判定部 105 は、異常期間 T3 における状態データが示す状態のうち、最高値を取得する。関係判定部 105 は、最高値が閾値未満であると判定された場合には、異常に状態データが関係するとは判定せず、最高値が閾値以上であると判定された場合に、異常に状態データが関係すると判定する。

[0078] 例えば、関係判定部 105 は、状態データに変化が示された期間のうち、状態が飽和している飽和期間 T1 と、異常が発生している異常期間 T3 よりも前の他の期間と、の各々における状態の変化量に基づいて、異常に状態データが関係するか否かを判定してもよい。先述したように、基準期間 T2 は、他の期間の一例である。関係判定部 105 は、飽和期間 T1 における状態の変化量と、他の期間における状態の変化量と、の差が閾値以上であるか否かを判定する。関係判定部 105 は、当該差が閾値未満であると判定された場合には、異常に状態データが関係するとは判定せず、当該差が閾値以上であると判定された場合に、異常に状態データが関係すると判定する。

[0079] なお、関係判定部 105 は、上記説明した判定方法以外の他の判定方法に基づいて、異常に状態データが関係するか否かを判定してもよい。例えば、関係判定部 105 は、異常期間 T3 において状態データが示す状態が飽和しているが、異常が発生していない期間でも当該状態が飽和している場合には、定常的に飽和が発生する状態データなので、異常に状態データが関係しないと判定してもよい。一方、関係判定部 105 は、異常が発生していない期

間では状態データが示す状態が飽和していないが、異常期間 T 3 において状態データが示す状態が飽和している場合には、異常期間 T 3 にだけ飽和が発生するので、異常に状態データが関係しないと判定してもよい。

[0080] [復旧処理実行部]

復旧処理実行部 106 は、異常が検知された場合に、異常に関係すると判定された状態データに基づいて、異常の復旧に関する復旧処理を実行する。復旧処理は、発生した異常に関係する何らかの処理であればよい。本実施形態では、異常に関係する状態データを管理者画面 SC に表示させる処理が復旧処理に相当する。復旧処理は、他の処理であってもよく、例えば、予め用意された復旧のためのプログラムを実行する処理、又は、管理者に電子メール等の通知を送信する処理であってもよい。

[0081] 例えば、復旧処理実行部 106 は、異常が検知された場合に、管理者端末 40 に対し、管理者画面 SC の表示データを送信することによって、管理者端末 40 に管理者画面 SC を表示させる。復旧処理実行部 106 は、異常が検知された場合に、異常と関係する状態データを示す画像を、管理者画面 SC に表示させる。図 4 の例では、ある異常が発生した場合に、復旧処理実行部 106 は、過去に同じ以上が発生した場合に関係判定部 105 により判定された状態データが示す状態を、管理者画面 SC に表示させる。復旧処理実行部 106 は、ある異常が発生して当該異常と関係する状態データが特定された場合に、同じ異常が発生すると、当該異常と関係する状態データに基づいて、復旧処理を実行する。

[0082] [1-3-2. 管理者端末で実現される機能]

例えば、管理者端末 40 は、データ記憶部 400、操作受付部 401、及び表示制御部 402 を含む。データ記憶部 400 は、記憶部 42 を主として実現される。操作受付部 401 及び表示制御部 402 は、制御部 41 を主として実現される。

[0083] [データ記憶部]

データ記憶部 400 は、管理者の業務に必要なデータを記憶する。例えば

、データ記憶部400は、管理者画面SCを表示するために必要なデータを記憶する。データ記憶部400は、管理者の業務に必要なメンテナンスツールを記憶してもよい。メンテナンスツール自体は、公知のツールであってよく、例えば、ハードウェア及びソフトウェアの少なくとも一方の状態を監視可能なツールであればよい。

[0084] [操作受付部]

操作受付部401は、管理者による各種操作を受け付ける。例えば、操作受付部401は、管理者画面SCに対する操作を受け付ける。

[0085] [表示制御部]

表示制御部402は、各種画面を表示部45に表示させる。例えば、表示制御部402は、管理者画面SCを表示部45に表示させる。

[0086] [1-4. 監視システムで実行される処理]

図8は、監視システム1で実行される処理の一例を示す図である。制御部11、41が、それぞれ記憶部12、42に記憶されたプログラムを実行することによって、図8の処理が実行される。

[0087] 図8のように、サーバ10は、複数の通信装置20の各々と通信し、状態データを取得して状態データベースDBに格納する(S1)。異常が発生すると、管理者端末40は、管理者による異常発生操作を受け付ける(S2)。管理者端末40は、サーバ10に対し、異常発生操作が行われたことを示す異常発生データを送信する(S3)。サーバ10は、管理者端末40から、異常発生データを受信する(S4)。サーバ10は、異常発生データを受信したタイミングを、異常が発生した異常発生タイミングt3として記憶部12に記録する(S5)。なお、管理者が異常発生タイミングt3を指定してもよい。この場合、サーバ10は、管理者が指定した異常発生タイミングt3を記憶部12に記録する。

[0088] 異常が解消すると、管理者端末40は、管理者による異常解消操作を受け付ける(S6)。管理者端末40は、サーバ10に対し、異常解消操作が行われたことを示す異常解消データを送信する(S7)。サーバ10は、管理

者端末40から、異常解消データを受信する(S8)。サーバ10は、異常解消データを受信したタイミングを、異常が解消した異常解消タイミングt5として記憶部12に記録する(S9)。なお、管理者が異常解消タイミングt5を指定してもよい。この場合、サーバ10は、管理者が指定した異常解消タイミングt5を記憶部12に記録する。

[0089] サーバ10は、異常発生タイミングt3の所定時間前である基準タイミングt4から異常発生タイミングt3までの期間を、基準期間T2として設定する(S10)。サーバ10は、異常発生タイミングt3から異常解消タイミングt5までの期間を、異常期間T3として設定する(S11)。サーバ10は、状態データベースDBを参照し、異常発生タイミングt3を含む期間の状態データを、判定対象の状態データとして取得する(S12)。判定対象の状態データは、S13以降の処理の対象となる状態データである。以降の処理は、状態データごとに実行される。

[0090] サーバ10は、判定対象の状態データを正規化する(S13)。S13では、サーバ10は、正規化以外にも、判定対象の状態データに対し、標準化処理又は平滑化処理等の前処理を実行してもよい。他にも例えば、サーバ10は、判定対象の状態データが示す状態が所定の閾値未満である場合には、S14以降の処理を実行しないようにしてもよい。

[0091] サーバ10は、正規化が実行された判定対象の状態データが示す状態が飽和しているか否かを判定する(S14)。S14では、サーバ10は、状態データが示す状態の時系列的な変化量を計算する。サーバ10は、時系列的な変化量が閾値未満の状態が継続している場合に、状態データが示す状態が飽和していると判定する。サーバ10は、時系列的な変化量が閾値以上である場合、又は、時系列的な変化量が閾値未満の状態が継続していない場合に、状態データが示す状態が飽和していないと判定する。

[0092] S14において、判定対象の状態データが示す状態が飽和していると判定されない場合(S14:N)、サーバ10は、判定対象の状態データが異常に関係ないと判定し(S15)、S21の処理に移行する。S14において

、判定対象の状態データが示す状態が飽和していると判定された場合（S 1 4 : Y）、サーバ 1 0 は、飽和開始タイミング t_1 から飽和終了タイミング t_2 までの期間を、飽和期間 T 1 として設定する（S 1 6）。

[0093] サーバ 1 0 は、判定対象の状態データの基準期間 T 2 における最高値である第 1 最高値が、当該状態データの基準期間 T 2 よりも過去の期間における最高値である第 2 最高値以上であるか否かを判定する（S 1 7）。S 1 7 において、第 1 最高値が第 2 最高値以上であると判定された場合（S 1 7 : Y）、サーバ 1 0 は、S 1 5 に移行し、判定対象の状態データが異常に関係ないと判定する。

[0094] S 1 7 において、第 1 最高値が第 2 最高値未満であると判定された場合（S 1 7 : N）、サーバ 1 0 は、判定対象の状態データの異常期間 T 3 における第 3 最高値が、第 1 最高値又は第 2 最高値以上であるか否かを判定する（S 1 8）。ここでは、サーバ 1 0 が、第 3 最高値と、第 1 最高値又は第 2 最高値と、を比較する場合（即ち、第 1 最高値又は第 2 最高値の何れか一方だけが比較対象になる場合）を説明するが、サーバ 1 0 が、第 3 最高値と、第 1 最高値及び第 2 最高値と、を比較してもよい。

[0095] S 1 8 において、異常期間 T 3 における最高値が第 1 最高値又は第 2 最高値未満であると判定された場合（S 1 8 : N）、サーバ 1 0 は、S 1 5 に移行し、判定対象の状態データが異常に関係ないと判定する。S 1 8 において、異常期間 T 3 における最高値である第 3 最高値が第 1 最高値又は第 2 最高値以上であると判定された場合（S 1 8 : Y）、サーバ 1 0 は、飽和期間 T 1 及び異常期間 T 3 の一致度が閾値以上であるか否かを判定する（S 1 9）。S 1 9 において、飽和期間 T 1 及び異常期間 T 3 の一致度が閾値未満であると判定された場合（S 1 9 : N）、サーバ 1 0 は、S 1 5 に移行し、判定対象の状態データが異常に関係ないと判定する。

[0096] S 1 9 において、飽和期間 T 1 及び異常期間 T 3 の一致度が閾値以上であると判定された場合（S 1 9 : Y）、サーバ 1 0 は、判定対象の状態データを、異常に関係のある状態データの候補として記憶部 1 2 に記録する（S 2

0)。サーバ10は、全ての状態データが判定対象になったか否かを判定する(S21)。S21において、まだ判定対象になっていない状態データが存在する場合(S21:N)、S12の処理に戻り、次の判定対象の状態データに対する処理が実行される。

[0097] S21において、全ての状態データを判定したと判定された場合(S21:Y)、サーバ10は、S20で候補として記録された状態データの中から、異常に関係ある状態データとして判定し(S22)、本処理は終了する。S22では、サーバ10は、S20で候補として記録された状態データの各々の飽和期間T1及び基準期間T2における変化量等に基づいて、当該状態データと異常との関係度合いを示す特徴量を計算し、当該特徴量が高い順に所定数の状態データを、異常に関係ある状態データとして判定する。なお、S22の処理が実行されずに、S20で候補として記録された状態データが、そのまま異常に関係ある状態データとして判定されてもよい。

[0098] [1-5. 実施形態のまとめ]

本実施形態の監視システム1は、通信装置20の時系列的な状態の変化に関する状態データに基づいて、通信装置20の状態が飽和しているか否かを判定する。監視システム1は、当該判定結果に基づいて、通信サービスにおける異常に状態データが関係するか否かを判定する。これにより、監視システム1は、通信サービスにおける異常に状態データが関係するか否かを判定できる。その結果、例えば、監視システム1は、異常の復旧を早めることができる。他にも例えば、監視システム1は、異常を迅速に検知したり、異常の要因を分析したりするといったことも可能になる。

[0099] また、監視システム1は、異常が検知された場合に、状態データの取得、通信装置20の状態が飽和しているか否かの判定、及び異常に状態データが関係するか否かの判定を実行する。監視システム1は、異常が検知された場合に、異常に関係すると判定された状態データに基づいて、復旧処理を実行する。これにより、監視システム1は、異常が検知された場合の復旧を早めることができる。

- [0100] また、監視システム 1 は、異常が検知された場合に、異常が発生した異常発生タイミング t_3 に基づいて、状態データに関する期間を設定する、監視システム 1 は、期間における通信装置 20 の時系列的な状態の変化に関する状態データを取得する。これにより、監視システム 1 は、異常に関係のある期間における状態データに基づいて、異常に状態データが関係するか否かを判定できるので、判定精度が高まる。監視システム 1 は、異常に関係する状態データを精度よく特定することによって、異常の復旧を早めることができる。
- [0101] また、監視システム 1 は、正規化が実行された状態データに基づいて、状態が飽和しているか否かを判定する。これにより、監視システム 1 は、通信装置 20 ごとに通信量が変化する範囲が変わったとしても、その範囲を正規化によって吸収できるので、異常に状態データが関係するか否かの判定精度を高めることができる。
- [0102] また、監視システム 1 は、状態データに変化が示された期間のうち、状態が飽和していると判定された飽和期間 T_1 に基づいて、異常に状態データが関係するか否かを判定する。これにより、監視システム 1 は、飽和期間 T_1 といった異常に直結する可能性が高い期間を利用して異常に状態データが関係するか否かを判定できるので、異常に状態データが関係するか否かの判定精度を高めることができる。
- [0103] また、監視システム 1 は、状態データに変化が示された期間のうち、異常が発生している異常期間 T_3 よりも前の他の期間における状態の最高値に基づいて、異常に状態データが関係するか否かを判定する。これにより、監視システム 1 は、例えば、異常が発生していない時から定常的に通信量が高くなるか否かを考慮したうえで、異常に状態データが関係するか否かを判定できるので、異常に状態データが関係するか否かの判定精度を高めることができる。
- [0104] また、監視システム 1 は、異常期間 T_3 よりも前の他の期間における状態の最高値と、他の期間よりも前の期間における状態の最高値と、に基づいて

、異常に状態データが関係するか否かを判定する。これにより、監視システム 1 は、例えば、異常が発生していない時から定常的に通信量が高くなるか否かを考慮したうえで、異常に状態データが関係するか否かを判定できるので、異常に状態データが関係するか否かの判定精度を高めることができる。

[0105] また、監視システム 1 は、状態データに変化が示された期間のうち、異常が発生している異常期間 T 3 における状態データが示す状態の最高値に基づいて、異常に状態データが関係するか否かを判定する。状態データが示す状態が飽和していたとしても、あまり高い値でなければ当該状態が異常に関係しない可能性があるので、監視システム 1 は、異常期間 T 3 における状態データが示す状態の最高値を考慮して異常に状態データが関係するか否かを判定することによって、異常に状態データが関係するか否かの判定精度を高めることができる。

[0106] また、監視システム 1 は、状態データに変化が示された期間のうち、異常が発生している異常期間 T 3 と、状態が飽和していると判定された飽和期間 T 1 と、の一致度に基づいて、異常に状態データが関係するか否かを判定する。飽和期間 T 1 及び異常期間 T 3 の一致度が高いほど、異常に状態データが関係している度合いが高いと考えられるので、監視システム 1 は、一致度を利用することによって、異常に状態データが関係するか否かの判定精度を高めることができる。

[0107] また、監視システム 1 は、状態データに変化が示された期間のうち、状態が飽和している飽和期間 T 1 と、異常が発生している異常期間 T 3 よりも前の他の期間と、の各々における状態の変化量に基づいて、異常に状態データが関係するか否かを判定する。これにより、監視システム 1 は、ある状態データが示す状態が飽和していたとしても、定常的に飽和しやすい状態なのかを考慮したうえで、異常に状態データが関係するか否かを判定できるので、異常に状態データが関係するか否かの判定精度を高めることができる。

[0108] [1-6. 変形例]

本開示は、以上に説明した実施形態に限定されるものではない。本開示の

趣旨を逸脱しない範囲で、適宜変更可能である。

[0109] [1-6-1. 変形例1-1]

図9は、変形例1-1の監視システム1で実現される機能の一例を示す図である。変形例1-1の監視システム1は、検知処理実行部107を含む。検知処理実行部107は、制御部11により実現される。例えば、実施形態では、異常が検知された場合に一連の処理が実行される場合を説明したが、一連の処理は、異常が検知される前に実行されてもよい。変形例1-1では、飽和判定部104の判定結果が異常の検知に利用される場合を説明する。なお、変形例1-1では、状態データのうち、一連の処理で利用される期間（図7のタイムウィンドウWに相当する期間）は、現時点の所定期間（例えば、15分程度）だけ前の時点から現時点までの期間とする。

[0110] 変形例1-1の状態データ取得部101は、異常が検知される前に、状態データを取得する。状態データ取得部101による状態データの取得方法は、実施形態と同様である。状態データ取得部101は、通信サービスの稼働中にリアルタイムで状態データを取得する。状態データ取得部101は、異常の発生有無に関係なく、状態データを取得する。変形例1-1の飽和判定部104は、異常が検知される前に、状態データに基づいて、状態が飽和しているか否かを判定する。飽和判定部104による飽和の判定方法も、実施形態と同様である。飽和判定部104は、異常の発生有無に関係なく、状態データが示す状態が飽和しているか否かを判定する。

[0111] 変形例1-1の関係判定部105は、異常が検知される前に、異常に状態データが関係するか否かを判定する。関係判定部105は、異常の発生有無に関係なく、状態データが示す状態が異常に関係するか否かを判定する。例えば、関係判定部105は、状態データが示す状態が飽和していないと判定された場合には、当該状態が異常に関係しないと判定し、状態データが示す状態が飽和していると判定された場合には、当該状態が異常に関係すると判定する。

[0112] 検知処理実行部107は、異常に関係すると判定された状態データに基づ

いて、異常の検知に関する検知処理を実行する。検知処理は、発生した異常を検知する何らかの処理であればよい。変形例 1-1 では、異常の発生を管理者画面 S C に表示させる処理が検知処理に相当する。例えば、検知処理実行部 107 は、異常が検知された場合に、異常が検知されたことを示す画像を、管理者画面 S C に表示させる。検知処理実行部 107 は、管理者に対し、電子メール等の手段を利用して通知を送信することによって、検知処理を実行してもよい。

[0113] 変形例 1-1 の監視システム 1 は、異常が検知される前に、状態データの取得、通信装置 20 の状態が飽和しているか否かの判定、及び異常に状態データが関係するか否かの判定を実行する。監視システム 1 は、異常に關係すると判定された状態データに基づいて、異常の検知に関する検知処理を実行する。これにより、監視システム 1 は、迅速に異常を検知できる。

[0114] [1-6-2. 変形例 1-2]

例えば、監視システム 1 は、通信サービス以外の他のサービスにも適用可能である。例えば、監視システム 1 は、電子商取引サービス、旅行予約サービス、金融サービス、決済サービス、オンラインフリーマーケットサービス、又は動画配信サービスといった他のサービスにおける異常に、当該他のサービスにおける装置の状態データが関係するか否かを判定してもよい。

[0115] 例えば、監視システム 1 は、複数のサービスの各々における異常に、当該サービス又は他のサービスにおける装置の状態データが関係するか否かを判定してもよい。監視システム 1 は、クラウドインフラストラクチャ又はクラウドプラットフォームにおけるテナントと読み換えられる。監視システム 1 は、ソフトウェア構成又はハードウェア構成を含むオフリングサービス群から選択される複数のオフリングサービスによって構成される。

[0116] 変形例 1-2 の状態データ取得部 101 は、複数のサービスの各々における装置の状態データを取得する。状態データ取得部 101 が個々のサービスにおける装置の状態データを取得する処理は、実施形態と同様であってよい。状態データ取得部 101 は、複数のサービスの各々の装置と通信し、当該

装置の状態データを取得する。

[0117] 変形例 1-2 の飽和判定部 104 は、複数のサービスの各々における装置の状態データに基づいて、当該装置が飽和しているか否かを判定する。飽和判定部 104 が個々のサービスにおける装置の状態データに基づいて飽和を判定する処理は、実施形態と同様であってよい。

[0118] 変形例 1-2 の関係判定部 105 は、飽和判定部 104 の判定結果に基づいて、複数のサービスの各々における異常に状態データが関係するか否かを判定する。関係判定部 105 が個々のサービスにおける異常に状態データが関係するか否かを判定する処理は、実施形態と同様であってよい。

[0119] 変形例 1-2 の監視システム 1 は、複数のサービスの各々における装置の状態データを取得する。監視システム 1 は、複数のサービスの各々における装置の状態データに基づいて、装置が飽和しているか否かを判定する。監視システム 1 は、当該判定結果に基づいて、複数のサービスの各々における異常に状態データが関係するか否かを判定する。これにより、監視システム 1 は、複数のサービスの各々の異常に対応できる。

[0120] [1-6-3. その他の変形例]

例えば、上記変形例を組み合わせてもよい。

[0121] 例えば、実施形態では、サーバ 10 で主な処理が実行される場合を説明したが、サーバ 10 で実行されるものとして説明した処理は、管理者端末 40 又は他のコンピュータで実行されてもよいし、複数のコンピュータで分担されてもよい。

[0122] [2. 第 2 実施形態]

本開示に係る監視システム 1 の別実施形態の一例である第 2 実施形態を説明する。第 2 実施形態では、サービスにおける異常に関する処理の一例を説明する。従来の技術は、システムにおける種々の装置のうち、予め定められた装置の状態に基づいて復旧手順を特定することしかできない。システムに発生した異常には、種々の装置が関係していることがある。複数の装置の各々の状態データが密接に関連していたとしても、従来の技術は、これらの関

連性を特定できない。そこで、第2実施形態の監視システム1は、サービスにおける監視対象となる装置の状態に関する状態データの関連性を特定する。

[0123] [2-1. 第2実施形態の監視システムのハードウェア構成]

第2実施形態の監視システム1のハードウェア構成は、第1実施形態と同様であってよい。

[0124] [2-2. 監視システムの概要]

本実施形態では、通信装置20が、コンテナ化されたネットワーク機能であるCNF (Containerized Network Function) を有するサーバコンピュータである場合を例に挙げる。更に、ユーザ端末30がスマートフォンである場合を例に挙げる。通信装置20は、多数のユーザ端末30の通信を中継する。例えば、通信装置20が処理すべき通信量が、当該通信装置20が処理可能な通信量に達すると、通信サービスで異常が発生する可能性がある。通信量は、bps等の公知の指標によって表現可能である。

[0125] 例えば、通信サービスで異常が発生すると、管理者は、異常に関係する通信装置20を特定して復旧作業を行う。しかしながら、通信サービスでは、ある1つの通信装置20だけではなく、複数の通信装置20が異常に関係することがある。例えば、特定のエリアで通信サービスの異常が発生した場合に、管理者が異常の要因として特定した通信装置20以外にも、当該通信装置20と関連性のある他の通信装置20が異常に関係している可能性がある。管理者が、異常に関係する全ての通信装置20を自力で特定するのは難しい。

[0126] 例えば、通信装置20が処理する通信量が閾値以上になった場合に異常を検知することも考えられるが、管理者が定めた上限値よりも多くの通信量を通信装置20が処理可能な場合や、管理者が定めた上限値よりも低い通信量しか通信装置20が処理できない場合もある。更に、管理者自身、通信装置20の上限値を知らない場合もあるので、本実施形態では、異常と判定するための通信量の上限値が定められていない。このため、通信装置20の通信

量が一定程度に達したとしても、必ずしも異常に該当するとは限らない。

[0127] 本実施形態では、サーバ10は、通信サービスにおいて発生した異常に係る通信装置20の通信量と似た特徴を有する他の通信装置20の通信量を特定する。例えば、異常に係る通信装置20は、管理者による分析によって特定される。後述の変形例のように、異常に係る通信装置20は、通信量の飽和によって特定されてもよい。上記他の通信装置20は、異常と関係している可能性があるので、上記他の通信装置20を特定することは、異常の検知や復旧等に有用である。

[0128] 図10は、通信サービスで異常が検知された場合の通信装置20の時系列的な通信量の変化の一例を示す図である。図10の横軸は、時間軸である。図10の縦軸は、通信量を示す軸である。図10の例では、通信事業者の施設に配置された5台の通信装置20A～20Eの各々の通信量の変化が示されている。以降、通信装置20A～20Eを区別しない時は、単に通信装置20という。

[0129] 図10の例では、ある特定の時点で、通信装置20Aの通信量が急激に増加する。その後、通信装置20Aは、ある一定量以上の通信を処理できなくなり、通信量が飽和する。この場合、ある特定のエリアで通信装置20Aに接続を試みたユーザ端末30が、通信サービスを利用できなくなる。即ち、当該エリアにおける通信サービスに異常が発生する。ユーザは、通信サービスのコールセンターに連絡し、通信サービスを利用できないことを伝えることがある。

[0130] 例えば、管理者は、複数のユーザからの問い合わせを受けて、異常が発生していることを把握する。この時点では、管理者は、どの通信装置20が異常の要因であるかを特定しておらず、その後、通信装置20Aの通信量が下がり、異常が自然復旧したとする。更に、管理者は、ユーザからの問い合わせを受けなくなり、異常が自然復旧したことを把握する。異常が自然復旧すると、ユーザ端末30が通信装置20Aを介して通信サービスを利用できるようになる。

- [0131] 例えば、管理者は、ある特定のエリアで発生した異常が発生して解消した後、通信装置20A～20Eの各々の通信量を解析する。管理者は、当該異常が発生していた期間において、通信装置20Aの通信量が急激に増加して飽和していたことを特定する。管理者は、管理者端末40に対し、上記エリアで発生した異常に、通信装置20Aの通信量が関係することを示す情報を入力する。管理者端末40は、サーバ10に対し、当該情報をアップロードする。サーバ10は、上記エリアと、通信装置20Aの通信量が当該エリアの異常に関係していることと、を関連付けて記憶する。
- [0132] 例えば、サーバ10は、通信装置20A～20Eの各々をクラスタリングすることによって、通信装置20B～20Eの各々の状態データの中から、通信装置20Aの状態データと関連性のある状態データがあるか否かを判定する。図10の例であれば、クラスタリングによって、通信装置20Aの通信量の特徴と、通信装置20Eの通信量の特徴と、が似ていることが特定される。
- [0133] 例えば、サーバ10は、あるエリアにおける異常に、管理者が指定した通信装置20Aだけではなく、クラスタリングによって特定された通信装置20Eも関係していることを記憶部12に記録する。サーバ10は、当該エリアで再び異常が発生した場合に、管理者端末40に対し、通信装置20Aだけではなく、通信装置20Eの状態もチェックすることを促す通知を送信する。
- [0134] 図11は、管理者端末40に表示される通知の一例を示す図である。例えば、過去に通信装置20Aの通信量に異常が見られた場合に、通信サービスのコールセンターが、ある特定のエリアXから通信サービスを利用しようとしたユーザからの問い合わせを受けたとする。現時点で、コールセンターが、同じエリアXで通信サービスを利用しようとしたユーザからの問い合わせを受けた場合に、エリアXにおける通信サービスで異常が発生したことが検知される。この場合、サーバ10は、管理者端末40に対し、管理者が指定した通信装置20Aと、クラスタリングによって特定された通信装置20E

と、を確認することを促す管理者画面ＳＣの表示データを送信する。

[0135] 例えば、管理者端末４０は、管理者画面ＳＣの表示データを受信すると、通信装置２０Ａの通信量と、通信装置２０Ａの通信量と関連性のある通信装置２０Ｅの通信量と、を確認することを促すメッセージが表示される。管理者画面ＳＣには、現在の通信装置２０Ａ、２０Ｅの各々の通信量を示すグラフが表示されてもよいし、過去に同様の異常が発生した時の通信装置２０Ａ、２０Ｅの各々の通信量を示すグラフが表示されてもよい。管理者は、管理者画面ＳＣを確認し、通信装置２０Ａ、２０Ｅのメンテナンスを行う。通信装置２０Ａ、２０Ｅの各々のメンテナンス自体は、公知の方法で行われてもよい。

[0136] 以上のように、監視システム１は、通信サービスで異常が発生した場合に、異常と関係がある通信装置２０Ａと関連性のある通信装置２０Ｅを、クラスタリングによって特定する。例えば、監視システム１は、同様の異常が再び発生した場合に、管理者が、異常の要因となった通信装置２０を特定しやすくなるので、迅速に復旧作業を行うことができる。以降、監視システム１の詳細を説明する。

[0137] [２－３．監視システムで実現される機能]

図１２は、監視システム１で実現される機能の一例を示す図である。図１２では、サーバ１０で実現される機能と、管理者端末４０で実現される機能と、が示されている。通信装置２０及びユーザ端末３０の各々の機能は、公知の通信サービスにおける機能と同様のため、図１２では省略する。例えば、通信装置２０は、サーバ１０に対し、後述の状態データ又はその一部の情報を送信する機能を有する。ユーザ端末３０は、ユーザが通信サービスを利用するための機能を有する。

[0138] [２－３－１．サーバで実現される機能]

例えば、サーバ１０は、データ記憶部１００、状態データ取得部１０１、クラスタリング実行部１０８、関連データ特定部１０９、及び復旧処理実行部１０６を含む。データ記憶部１００は、記憶部１２により実現される。状

態データ取得部 101、クラスタリング実行部 108、関連データ特定部 109、及び復旧処理実行部 106 は、制御部 11 により実現される。

[0139] [データ記憶部]

データ記憶部 100 は、通信サービスに関するデータを記憶する。例えば、データ記憶部 100 は、状態データベース DB を記憶する。

[0140] 図 13 は、状態データベース DB の一例を示す図である。状態データベース DB は、複数の通信装置 20 の各々の状態データが格納されたデータベースである。例えば、状態データベース DB には、複数の通信装置 20 の各々を識別可能な装置識別情報、当該通信装置 20 の状態を示す状態データ、後述の異常要因データに該当するか否かを識別可能な異常要因識別情報、及び後述の関連データに該当するか否かを識別可能な関連識別情報が格納される。状態データベース DB には、他のデータが格納されてもよい。例えば、状態データベース DB には、通信装置 20 が配置された場所等を示す情報が格納されてもよい。

[0141] 通信装置 20 の識別情報は、任意の情報であってよく、例えば、IP アドレス、装置名、又は MAC アドレスであってもよい。状態データは、本実施形態では、状態データは、通信装置 20 の時系列的な状態の変化に関するデータである。通信装置 20 の状態は、通信装置 20 の負荷ということもできる。通信装置 20 の状態は、ハードウェア的な状態を意味してもよいし、ソフトウェア的な状態を意味してもよい。

[0142] 本実施形態では、通信装置 20 の通信量が通信装置 20 の状態に相当する場合を例に挙げるが、通信装置 20 の他の状態が通信装置 20 の状態に相当してもよい。他の状態としては、通信装置 20 のリソースの消費量、サービスに対するリクエストの処理時間（レスポンスタイム）、又はリクエストに対して返されたエラーの数であってもよい。状態データは、ゴールデンシグナルメトリクスと呼ばれる指標であってもよいし、公知のベンチマークテストで利用されるその他の指標であってもよい。例えば、状態データは、CPU 使用量、メモリ使用量、電力消費量、通信速度、温度、又はこれらの組み

合わせであってもよい。

[0143] なお、状態データは、通信サービス又は他のサービスにおける業績に関する状態を示してもよい。他のサービスは、ユーザが通信サービスを介して利用するサービスであり、例えば、電子商取引サービス、旅行予約サービス、決済サービス、又は金融サービスである。例えば、状態データは、通信装置20に接続中（通信サービス又は他のサービスにログイン中）のユーザの数、ユーザが通信装置20を経由して実行した決済、又はユーザが通信装置20を経由して行った注文であってもよい。決済数、決済額、注文数、及び注文額が増えるほど、通信装置20の負荷が高まるので、決済数、決済額、注文数、及び注文額も、通信装置20の状態に相当する。

[0144] 本実施形態では、複数の通信装置20の各々の状態データは、通信装置20の時系列的な状態の変化を示す。例えば、状態データは、通信装置20の状態が取得された日時と、当該日時における通信装置20の状態を示す数値と、を含む。通信装置20の状態は、数値ではなく、文字等の他の形式で表現されてもよい。本実施形態では、通信装置20の通信量が通信装置20の状態に相当するので、状態データは、通信装置20の通信量が取得された日時と、当該日時における通信装置20の通信量と、を含む。

[0145] なお、複数の通信装置20の各々の状態データは、通信装置20の時系列的な状態の変化ではなく、あるピンポイント（1時点）における状態を示してもよい。例えば、ある状態データは、時系列的な状態の変化を示し、他の状態データは、あるピンポイントにおける状態を示してもよい。あるピンポイントにおける状態を示す状態データが多数集まることによって、多数の状態データの全体として、時系列的な状態の変化が示されてもよい。

[0146] また、データ記憶部100に記憶されるデータは、状態データベースDBに限られない。データ記憶部100は、通信サービスに関する何らかのデータを記憶すればよい。例えば、データ記憶部100は、管理者端末40に管理者画面SCを表示させるために必要なデータを記憶してもよい。データ記憶部100は、後述の処理で利用される各種閾値を記憶してもよい。閾値は

、管理者が指定してもよいし、機械学習の手法や統計的な手法に基づいて決定されてもよい。

[0147] [状態データ取得部]

状態データ取得部101は、通信サービスにおける監視対象となる複数の通信装置20の各々の状態に関する状態データを取得する。例えば、状態データ取得部101は、複数の通信装置20の各々に対し、定期的（例えば、1秒～30秒程度、又は、1分～5分程度）に、当該通信装置20の状態を要求する。通信装置20は、サーバ10から、状態データ取得部101の要求を受信すると、サーバ10に対し、自身の装置識別情報と、自身の状態を示す情報と、を送信する。状態データ取得部101は、当該通信装置20の装置識別情報に関連付けられた状態データに、現在の日時と、通信装置20から受信した情報と、を追加する。

[0148] なお、通信装置20は、ある程度の期間の状態データを蓄積して、サーバ10に対し、一度に状態データを送信してもよい。この場合、状態データ取得部101は、通信装置20から、一度に状態データを取得して状態データベースDBに格納する。他にも例えば、状態データ取得部101は、定期的ではなく不定期的に、通信装置20から状態データを取得してもよい。状態データ取得部101は、管理者が指示したタイミングで、通信装置20から状態データを取得してもよい。

[0149] 通信装置20は、通信サービスにおける監視対象となる装置の一例である。監視対象となる装置は、任意の装置であってよく、通信装置20に限られない。本実施形態で通信装置20と記載した箇所は、監視対象となる他の装置に読み替えることができる。他の装置は、通信サービスで利用されている装置であればよく、例えば、サーバ10、サーバ10以外の他のコンピュータ、サーバ10及び他のコンピュータに含まれるCPU・メモリ・ネットワークカード等の部品、バッテリー、アンテナ、通信ケーブル、又はセンサであってもよい。

[0150] 本実施形態では、状態データ取得部101は、異常が検知された場合に、

状態データを取得する。異常が検知された場合に取得される状態データは、異常が発生してから解消するまでの期間の全部又は一部における状態を示す。以降、この期間を異常期間という。状態データは、異常期間の全部又は一部だけではなく、異常期間以外の他の期間における状態も示してもよい。状態データ取得部101は、異常が発生してから解消するまでの間に、状態データを取得してもよいし、異常が解消した後に、事後的に状態データを取得してもよい。

[0151] 本実施形態では、状態データには、あるピンポイントのタイミングにおける状態が示されるのではなく、状態データには、ある程度の長さを有する期間における状態が示される。状態データ取得部101は、過去の全期間における状態を示す状態データを取得してもよいが、本実施形態では、過去の一部の期間における状態を示す状態データを取得するものとする。例えば、状態データ取得部101は、異常が検知された時点を含む期間における装置の時系列的な状態の変化に関する状態データを取得する。

[0152] [クラスタリング実行部]

クラスタリング実行部108は、複数の通信装置20の各々の状態データに関するクラスタリングを実行する。クラスタリングは、互いに似た特徴を有する状態データを特定する処理である。クラスタリングは、グルーピングと呼ばれることもある。クラスタリング実行部108は、互いに似た特徴を有する状態データが同じクラスに属するように、クラスタリングを実行する。あるクラスに属する複数の状態データの各々は、互いに似た特徴を示す。クラスの数、は、予め定められていてもよいし、特に定められていなくてもよい。

[0153] クラスタリングの手法自体は、公知の手法であってよい。例えば、クラスタリング実行部108は、k-means、階層的クラスタリング、密度ベースクラスタリング、ガウス混合モデル、又はスペクトラルクラスタリングに基づいて、クラスタリングを実行してもよい。他にも例えば、クラスタリング実行部108は、機械学習の手法を利用して作成された機械学習モデル

に基づいて、クラスタリングを実行してもよい。機械学習モデルも、公知の方法で作成されたモデルであってよい。例えば、クラスタリング実行部 108 は、RNN (Recurrent Neural Network)、LSTM (Long Short Term Memory)、又はTransformerベース等のモデルに対し、複数の通信装置 20 の各々の状態データを入力することによって、クラスタリングを実行してもよい。

[0154] 図 14 は、クラスタリングの実行結果の一例を示す図である。図 14 では、多数の通信装置 20 の各々の状態データが特徴量化されたベクトル空間が示されている。図 14 の白丸は、後述の異常関係データである。図 14 の黒丸は、異常関係データ以外の他の状態データである。図 14 の丸同士が近いことは、特徴が似ていることを意味する。本実施形態では、時系列的な状態の変化が状態データに示されているので、クラスタリング実行部 108 は、複数の通信装置 20 の各々の状態データが示す時系列的な状態の変化に基づいて、クラスタリングを実行する。例えば、クラスタリング実行部 108 は、個々の状態データが示す波形の特徴量を計算する。

[0155] 例えば、クラスタリング実行部 108 は、状態データの時間領域における特徴量を計算する。クラスタリング実行部 108 は、ある状態データが示す時系列的な状態の変化の平均値、分散、標準偏差、最小値、最大値、立ち上がりのタイミング、変化量の平均値、変化量の最大値、変化量の最小値、又はこれらの組み合わせを、当該状態データの時間領域における特徴量として計算する。クラスタリング実行部 108 は、ある状態データが示す状態が飽和した期間、その時の通信量、飽和の頻度、又はこれらの組み合わせを、当該状態データの時間領域における特徴量として計算してもよい。クラスタリング実行部 108 は、時間領域ではなく、状態データの周波数領域における特徴量を計算してもよい。

[0156] 例えば、クラスタリング実行部 108 は、複数の状態データの各々の特徴量に基づいて、互いに特徴量が近い状態データ同士が同じクラスに属するように、クラスタリングを実行する。機械学習モデルが利用される場合、状

態データの特徴量は、埋め込み表現と呼ばれることもある。クラスタリングの実質的な処理は、機械学習モデルの内部で実行される。クラスタリング実行部108は、複数の状態データの各々を機械学習モデルに入力し、機械学習モデルからの出力を取得することによって、クラスタリングを実行する。例えば、機械学習モデルの出力は、複数の状態データの各々と、当該状態データが属するクラスタと、の関係を示すデータである。クラスタリングは、教師無し学習の手法が利用されてもよい。クラスタリング実行部108は、状態データが示す波形を画像として捉えて、画像の類否を判定する手法に基づいて、クラスタリングを実行してもよい。

[0157] 本実施形態では、クラスタリング実行部108は、異常が検知された場合に、複数の装置の各々の状態データに基づいて、クラスタリングを実行する。例えば、クラスタリング実行部108は、サーバ10が異常を検知した場合に自動的にクラスタリングを実行してもよいし、通信サービスの管理者が管理者端末40で所定の操作を行った場合にクラスタリングを実行してもよい。クラスタリング実行部108は、異常が検知された後に、クラスタリングを実行すればよい。異常が検知される前にクラスタリングが実行される例は、後述の変形例2-1で説明する。

[0158] 図14の例では、4つの異常関係データが管理者によって指定されており、クラスタリング実行部108は、クラスタリングによって、クラスタC1~C4の4つを特定する。例えば、クラスタC1の中の白丸（異常関係データ）は、図10及び図11の例における通信装置20Aの状態データである。クラスタC1の中の黒丸の1つは、図10及び図11の例における通信装置20Eの状態データである。他のクラスタC2~C4の各々における白丸は、通信装置20Aが異常の要因となるエリアX以外の他のエリアにおける異常の要因となった通信装置20の状態データである。他のエリアについても、当該通信装置20と関連性のある他の通信装置20の状態データが、クラスタリングによって特定される。なお、クラスタC1~C4の各々に属する状態データの数は、互いに同じであってもよいし異なってもよい。

[0159] [関連データ特定部]

関連データ特定部109は、クラスタリングの実行結果に基づいて、サービスにおける異常の要因に関する状態データである異常要因データと関連性のある他の状態データである関連データを特定する。本実施形態では、管理者が、どの通信装置20の状態データが異常要因データに相当するかを指定するものとする。サーバ10は、管理者端末40から、管理者が異常要因データとして指定した通信装置20の状態データを示す情報を受信すると、状態データベースDBのうち、当該通信装置20の装置識別情報に関連付けられた異常要因識別情報を更新する。図13の例であれば、サーバ10は、通信装置20Aの状態データが、エリアXの異常の要因に関する異常要因データであることを示すように、通信装置20Aの異常要因識別情報を更新する。

[0160] 関連データは、クラスタリングによって、異常要因データと似た特徴を有することが特定された状態データである。別の言い方をすれば、関連データは、異常要因データと同じクラスタに属する状態データである。関連データ特定部109は、1つの異常要因データに対し、少なくとも1つの関連データを特定する。異常要因データと似た特徴を有する状態データが存在しなければ、関連データ特定部109は、関連データを1つも特定しないこともある。関連データ特定部109は、状態データベースDBのうち、関連データとして特定された通信装置20の状態データに関連付けられた関連情報を更新する。図13の例であれば、関連データ特定部109は、通信装置20Eの状態データを関連データとして特定するので、通信装置20Eの状態データに関連付けられた関連情報を更新する。

[0161] なお、関連データ特定部109は、異常要因データとは同じクラスタに属していなくても、多少似た特徴を有している状態データであれば、関連データとして特定してもよい。例えば、関連データ特定部109は、異常要因データとは同じクラスタに属していないが、特徴量の違い（図14の例であれば、ベクトル空間における距離）が閾値未満である状態データを、関連デー

タとして特定してもよい。また、関連データ特定部 109 は、特徴量の違いを計算する場合、より特徴のあるデータポイント区間に重み（ウェイトパラメータ）をかけることで、より特徴のあるデータに近い関連データを特定することが可能となる。逆に、関連データ特定部 109 は、異常要因データと同じクラスに属する状態データだったとしても、関連データとして特定しなくてもよい。例えば、関連データ特定部 109 は、異常要因データと同じクラスに属する複数の状態データのうち、異常要因データの特徴量との差が小さい順に所定数の状態データを、関連データとして特定してもよい。

[0162] 本実施形態では、関連データ特定部 109 は、異常が検知された場合に、関連データを特定する。例えば、関連データ特定部 109 は、サーバ 10 が異常を検知した場合に自動的に関連データを特定してもよいし、通信サービスの管理者が管理者端末 40 で所定の操作を行った場合に関連データを特定してもよい。関連データ特定部 109 は、異常が検知された後に、関連データを特定すればよい。異常が検知される前に関連データが特定される例は、後述の変形例 2-1 で説明する。

[0163] [復旧処理実行部]

復旧処理実行部 106 は、異常が検知された場合に、異常要因データと、関連データと、に基づいて、異常の復旧に関する復旧処理を実行する。復旧処理は、発生した異常に関係する何らかの処理であればよい。本実施形態では、異常に関係する状態データを管理者画面 SC に表示させる処理が復旧処理に相当する。復旧処理は、他の処理であってもよく、例えば、予め用意された復旧のためのプログラムを実行する処理、又は、管理者に電子メール等の通知を送信する処理であってもよい。

[0164] 例えば、復旧処理実行部 106 は、異常が検知された場合に、異常要因データと、関連データと、に基づいて、管理者端末 40 に対し、管理者画面 SC の表示データを送信することによって、管理者端末 40 に管理者画面 SC を表示させる。復旧処理実行部 106 は、異常が検知された場合に、異常要因データと、関連データと、の各々を示す画像を、管理者画面 SC に表示さ

せる。

[0165] 図 1 2 の例では、ある異常が発生した場合に、復旧処理実行部 1 0 6 は、過去に同じ以上が発生した場合に関連データ特定部 1 0 9 により判定された状態データが示す状態を、管理者画面 S C に表示させる。復旧処理実行部 1 0 6 は、ある異常が発生して当該異常と関係する状態データが特定された場合に、同じ異常が発生すると、当該異常と関係する状態データに基づいて、復旧処理を実行する。

[0166] 図 1 3 の状態データベース D B の例であれば、復旧処理実行部 1 0 6 は、エリア X で異常が発生した場合に、状態データベース D B の異常要因識別情報を参照し、通信装置 2 0 A の状態データが、当該異常の要因である異常要因データであることを特定する。更に、復旧処理実行部 1 0 6 は、状態データベース D B の関連識別情報を参照し、通信装置 2 0 E の状態データが、関連データであることを特定する。復旧処理実行部 1 0 6 は、当該特定された異常要因データ及び関連データに基づいて、管理者画面 S C の表示データを生成して管理者端末 4 0 に送信する。

[0167] [2 - 3 - 2 . 管理者端末で実現される機能]

例えば、管理者端末 4 0 は、データ記憶部 4 0 0 、操作受付部 4 0 1 、及び表示制御部 4 0 2 を含む。データ記憶部 4 0 0 は、記憶部 4 2 を主として実現される。操作受付部 4 0 1 及び表示制御部 4 0 2 は、制御部 4 1 を主として実現される。

[0168] [データ記憶部]

データ記憶部 4 0 0 は、管理者の業務に必要なデータを記憶する。例えば、データ記憶部 4 0 0 は、管理者画面 S C を表示するために必要なデータを記憶する。データ記憶部 4 0 0 は、管理者の業務に必要なメンテナンスツールを記憶してもよい。メンテナンスツール自体は、公知のツールであってよく、例えば、ハードウェア及びソフトウェアの少なくとも一方の状態を監視可能なツールであればよい。

[0169] [操作受付部]

操作受付部４０１は、管理者による各種操作を受け付ける。例えば、操作受付部４０１は、管理者画面ＳＣに対する操作を受け付ける。

[0170] 〔表示制御部〕

表示制御部４０２は、各種画面を表示部４５に表示させる。例えば、表示制御部４０２は、管理者画面ＳＣを表示部４５に表示させる。

[0171] 〔２－４．監視システムで実行される処理〕

図１５は、監視システム１で実行される処理の一例を示す図である。制御部１１、４１が、それぞれ記憶部１２、４２に記憶されたプログラムを実行することによって、図１５の処理が実行される。

[0172] 図１５のように、サーバ１０は、複数の通信装置２０の各々と通信し、状態データを取得して状態データベースＤＢに格納する（Ｓ１００）。Ｓ１００の処理は、定期的に実行される。異常が発生すると、管理者端末４０は、管理者による異常発生操作を受け付ける（Ｓ１０１）。管理者端末４０は、サーバ１０に対し、異常発生操作が行われたことを示す異常発生データを送信する（Ｓ１０２）。サーバ１０は、管理者端末４０から、異常発生データを受信する（Ｓ１０３）。サーバ１０は、異常発生データを受信したタイミングを、異常が発生した異常発生タイミングとして記憶部１２に記録する（Ｓ１０４）。なお、管理者が異常発生タイミングを指定してもよい。この場合、サーバ１０は、管理者が指定した異常発生タイミングを記憶部１２に記録する。

[0173] 異常が解消すると、管理者端末４０は、管理者による異常解消操作を受け付ける（Ｓ１０５）。管理者端末４０は、サーバ１０に対し、異常解消操作が行われたことを示す異常解消データを送信する（Ｓ１０６）。サーバ１０は、管理者端末４０から、異常解消データを受信する（Ｓ１０７）。サーバ１０は、異常解消データを受信したタイミングを、異常が解消した異常解消タイミングとして記憶部１２に記録する（Ｓ１０８）。なお、管理者が異常解消タイミングを指定してもよい。この場合、サーバ１０は、管理者が指定した異常解消タイミングを記憶部１２に記録する。

[0174] 管理者は、複数の通信装置 20 の各々の状態データを分析し、異常要因データを特定する。管理者端末 40 は、管理者が異常要因データを指定すると、サーバ 10 に対し、異常要因データを識別可能な異常要因識別情報を送信する (S109)。図 10 等の例であれば、管理者端末 40 は、サーバ 10 に対し、通信装置 20A の状態データが異常要因データであることを示す異常要因識別情報を送信する。

[0175] サーバ 10 は、管理者端末 40 から異常要因識別情報を受信すると (S110)、状態データベース DB を更新する (S111)。図 13 の例であれば、サーバ 10 は、状態データベース DB のうち、通信装置 20A の装置識別情報に関連付けられた異常要因識別情報を更新する。サーバ 10 は、複数の通信装置 20 の各々の状態データに基づいて、クラスタリングを実行する (S112)。サーバ 10 は、クラスタリングの実行結果に基づいて、異常要因データと関連性のある関連データを特定し (S113)、本処理は終了する。以降、同様の異常が発生した場合には、サーバ 10 は、異常要因データと、関連データと、に基づいて、復旧処理を実行する。

[0176] [2-5. 実施形態のまとめ]

本実施形態の監視システム 1 は、複数の通信装置 20 の各々の状態に関する状態データを取得する。監視システム 1 は、複数の通信装置 20 の各々の状態データに関するクラスタリングを実行する。監視システム 1 は、クラスタリングの実行結果に基づいて、関連データを特定するので、通信装置 20 の状態データの関連性を特定できる。例えば、監視システム 1 は、管理者が関連データの存在に気付けなかったとしても、クラスタリングによって関連データを特定できるので、管理者が異常発生時の復旧を迅速に行うことができる。監視システム 1 は、管理者の業務を支援できる。

[0177] また、監視システム 1 は、異常が検知された場合に、複数の通信装置 20 の各々の状態データを取得する。監視システム 1 は、異常が検知された場合に、複数の通信装置 20 の各々の状態データに基づいて、クラスタリングを実行する。監視システム 1 は、異常が検知された場合に、関連データを特定

する。監視システム 1 は、異常が検知された場合に、異常要因データと、関連データと、に基づいて、復旧処理を実行する。監視システム 1 は、復旧処理によって、通信サービスにおける異常を迅速に復旧できる。例えば、監視システム 1 は、似た異常が再び発生した場合に、管理者に異常要因データ及び関連データをチェックさせることができるので、管理者の業務を効果的に支援できる。

[0178] また、監視システム 1 は、監視システム 1 は、複数の通信装置 20 の各々の状態データが示す時系列的な状態の変化に基づいて、クラスタリングを実行する。監視システム 1 は、通信装置 20 の状態の時系列的な変化から、状態データの関連性を特定できる。例えば、監視システム 1 は、異常要因データと時系列的な特徴が似た状態データを、関連データとして特定することによって、状態データの時系列的な変化に基づいて、より精度のたかい復旧処理を実行できる。

[0179] [2-6. 変形例]

本開示は、以上に説明した実施形態に限定されない。本開示は、本開示の趣旨を逸脱しない範囲で、適宜変更可能である。

[0180] 図 16 は、変形例の監視システム 1 で実現される機能の一例を示す図である。変形例の監視システム 1 は、検知処理実行部 110、飽和判定部 104、及び異常要因データ特定部 111 を含む。検知処理実行部 110、飽和判定部 104、及び異常要因データ特定部 111 は、制御部 11 により実現される。

[0181] [2-6-1. 変形例 2-1]

例えば、実施形態では、異常が検知された場合に一連の処理が実行される場合を説明したが、一連の処理は、異常が検知される前に実行されてもよい。変形例 2-1 では、関連データ特定部 109 により特定された関連データが、実施形態のような異常の復旧ではなく、異常の検知に利用される場合を説明する。

[0182] 変形例 2-1 の状態データ取得部 101 は、異常が検知される前に、複数

の通信装置 20 の各々の状態データを取得する。状態データ取得部 101 による状態データの取得方法は、実施形態と同様である。状態データ取得部 101 は、通信サービスの稼働中にリアルタイムで状態データを取得する。状態データ取得部 101 は、異常の発生有無に関係なく、状態データを取得する。例えば、実際には異常が発生していたとしても、監視システム 1 で異常が検知される前であれば、上記「異常が検知される前」に相当する。

[0183] 変形例 2-1 のクラスタリング実行部 108 は、異常が検知される前に、複数の通信装置 20 の各々の状態データに基づいて、クラスタリングを実行する。クラスタリングの実行方法も、実施形態と同様である。クラスタリング実行部 108 は、異常の発生有無に関係なく、クラスタリングを実行する。変形例 2-1 の関連データ特定部 109 は、異常が検知される前に、関連データを特定する。関連データの特定方法も、実施形態と同様である。関連データ特定部 109 は、異常の発生有無に関係なく、関連データを特定する。

[0184] 監視システム 1 は、検知処理実行部 110 を含む。検知処理実行部 110 は、異常要因データと、関連データと、に基づいて、異常の検知に関する検知処理を実行する。検知処理は、発生した異常を検知する何らかの処理であればよい。変形例 2-1 では、異常の発生を管理者画面 SC に表示させる処理が検知処理に相当する。例えば、検知処理実行部 110 は、異常が検知された場合に、異常が検知されたことを示す画像を、管理者画面 SC に表示させる。検知処理実行部 110 は、管理者に対し、電子メール等の手段を利用して通知を送信することによって、検知処理を実行してもよい。

[0185] 変形例 2-1 では、異常要因データと、関連データと、の各々に、異常が発生したか否かを示す基準が関連付けられているものとする。当該基準は、過去に発生した異常に基づいて定められるものとする。例えば、何らかの閾値であってもよいし、後述の変形例 2-2 のように飽和が発生したか否かであってもよい。検知処理実行部 110 は、異常要因データと、関連データと、の各々が当該基準を満たしたか否かを判定する。

[0186] 例えば、検知処理実行部 110 は、異常要因データと、関連データと、の少なくとも一方が当該基準を満たしたと判定した場合に、検知処理を実行する。なお、検知処理実行部 110 は、異常要因データと、関連データと、の両方が上記基準を満たしたと判定した場合に検知処理を実行してもよい。検知処理実行部 110 は、異常要因データ又は関連データの何れか一方のみが上記基準を満たしたと判定した場合に検知処理を実行してもよい。

[0187] 変形例 2-1 の監視システム 1 は、異常が検知される前に、複数の通信装置 20 の各々の状態データの取得、クラスタリングの実行、及び関連データの特定を行う。監視システム 1 は、異常要因データと、関連データと、に基づいて、異常の検知に関する検知処理を実行する。これにより、監視システム 1 は、迅速に異常を検知できる。

[0188] [2-6-2. 変形例 2-2]

例えば、実施形態では、管理者が状態データを分析して異常要因データを指定する場合を例に挙げた。状態データは、監視システムによって分析されて、異常要因データとして分類されてもよい。例えば、通信サービスでは、多数の通信装置 20 が存在し、種々の異常が発生しうるので、管理者が、異常の要因となった通信装置 20 を特定するのが難しいことがある。このとき、異常の要因となった通信装置 20 は、それ以上の通信を処理しきれないので、通信量が飽和する場合がある。

[0189] 通信量が飽和するとは、通信量が正の状態であり（通信量が 0 ではない状態であり）、かつ、通信量が変化しない又は略変化しないことである。通信量が変化しないとは、通信量の変化量が 0 のことである。通信量が略変化しないとは、通信量の変化量が閾値未満であることである。飽和の具体的な判定方法は、後述する。通信量は、上限値が定められていてもよいが、管理者が定めた上限値よりも多くの通信量を通信装置 20 が処理可能な場合や、管理者が定めた上限値よりも低い通信量しか通信装置 20 が処理できない場合もあり、さらには、管理者自身、通信装置 20 の上限値を知らない場合もあるので、通信量の上限値が定められていないものとする。このため、通信装

置 20 の通信量が一定程度に達したとしても、異常が検知されるわけではないものとする。

[0190] 図 10 の例であれば、通信装置 20 A の通信量が急激に増加した後に、通信装置 20 A の通信量が飽和している。当該期間では、通信装置 20 A は、それ以上の通信を処理できないので、ある特定のエリアで通信装置 20 A に接続を試みたユーザ端末 30 が、通信サービスを利用できない可能性がある。なお、変形例 2-2 では、飽和開始タイミングから飽和終了タイミングまでの期間を異常が発生していた期間の一例として取り扱うが、飽和開始タイミングから飽和が終了していない現時点までの期間を異常が発生していた期間の一例として取り扱ってもよい。例えば、飽和開始タイミングから、管理者が指定した時点までの期間を異常が発生していた期間の一例として取り扱ってもよい。

[0191] 変形例 2-2 の監視システム 1 は、飽和判定部 104 及び異常要因データ特定部 111 を含む。飽和判定部 104 は、複数の通信装置 20 の各々の状態データに基づいて、当該通信装置 20 の状態データが示す状態が飽和しているか否かを判定する。飽和判定部 104 が判定する飽和は、状態データが示す状態の変化量が閾値未満になること、又は、当該変化量が当該閾値未満の状態が所定時間以上継続することである。通信量のように、原則として上限値が存在しない場合、通信量が増加すれば、変化量は、主に増加量を意味する。そのため、ある期間で変化量の合計が増加した後に、状態データが示す状態の増加量が閾値未満になること、又は、当該増加量が当該閾値未満の状態が所定時間以上継続することが、飽和に相当する。変化量は、ある一定程度の期間における積算値であってもよいし、ある時点と次の時点の変化量であってもよい。変化量は、通信量の減少量を意味してもよい。つまり、飽和判定部 104 は、状態データが示す当該変化量そのものの時系列的な変化に基づいて、当該飽和の判定を行う。

[0192] 例えば、飽和判定部 104 は、状態データが示す状態の増加量が閾値以上の状態から、当該増加量が閾値未満の状態、又は、当該増加量が閾値未満の

状態が所定時間以上継続した状態になった場合に、通信装置 20 の時系列的な状態が飽和していると判定する。飽和判定部 104 は、状態データが示す状態の増加量が閾値未満の状態、又は、当該増加量が閾値未満の状態が所定時間以上継続した状態になったとしても、その前において、当該増加量が閾値未満の状態であれば、通信装置 20 の時系列的な状態が飽和していないと判定する。例えば、飽和判定部 104 は、状態データが示す状態が閾値以上であり、かつ、当該状態の増加量が閾値未満の状態、又は、当該増加量が閾値未満の状態が所定時間以上継続した状態になった場合に、通信装置 20 の時系列的な状態が飽和していると判定してもよい。飽和判定部 104 は、状態データが示す状態の増加量が閾値未満の状態、又は、当該増加量が閾値未満の状態が所定時間以上継続した状態になったとしても、当該状態が閾値未満であれば、通信装置 20 の時系列的な状態が飽和していないと判定する。

[0193] 例えば、飽和判定部 104 は、複数の通信装置 20 の各々の状態データと、予め定められた閾値と、に基づいて、当該通信装置 20 の時系列的な状態が飽和しているか否かを判定する。別の言い方をすれば、飽和判定部 104 は、通信装置 20 の状態データごとに、予め定められた閾値に基づいて、当該状態データが示す時系列的な状態が飽和しているか否かを判定する。飽和判定部 104 が飽和を判定する際に参照される閾値は、管理者が指定してもよいし、過去の異常の傾向から計算されてもよい。閾値は、機械学習の手法を利用したモデルに基づいて決定されてもよい。

[0194] なお、飽和判定部 104 は、閾値を利用せずに、機械学習の手法を利用したモデルに基づいて、通信装置 20 の状態が飽和しているか否かを判定してもよい。この場合、モデルには、訓練用の状態データが示す時系列的な状態の変化を入力とし、当該状態が飽和しているか否かを示すラベルを出力とする訓練データが学習されている。飽和判定部 104 は、学習済みのモデルに判定対象の状態データを入力し、モデルから出力されたラベルに基づいて、通信装置 20 の状態が飽和しているか否かを判定してもよい。

[0195] 例えば、飽和判定部 104 は、ある通信装置 20 の状態データが示す変化

量が閾値以上であるか否かを判定することによって、当該通信装置 20 の時系列的な状態が飽和しているか否かを判定する。飽和判定部 104 は、ある通信装置 20 の状態データが示す変化量が閾値以上であると判定された場合には、当該通信装置 20 の時系列的な状態が飽和していると判定しない。飽和判定部 104 は、ある通信装置 20 の状態データが示す変化量が閾値未満であると判定された場合には、当該通信装置 20 の時系列的な状態が飽和していると判定する。

[0196] 例えば、飽和判定部 104 は、ある通信装置 20 の状態データが示す変化量が閾値未満である状態が所定時間以上継続しているか否かを判定することによって、当該通信装置 20 の時系列的な状態が飽和しているか否かを判定する。飽和判定部 104 は、ある通信装置 20 の状態データが示す変化量が閾値未満である状態が所定時間以上継続していないと判定された場合には、当該通信装置 20 の時系列的な状態が飽和していると判定しない。飽和判定部 104 は、ある通信装置 20 の状態データが示す変化量が閾値未満である状態が所定時間以上継続していると判定された場合には、当該通信装置 20 の時系列的な状態が飽和していると判定する。

[0197] 例えば、飽和判定部 104 は、異常が検知された場合に、通信装置 20 の状態データに基づいて、当該通信装置 20 の状態が飽和しているか否かを判定する。即ち、飽和判定部 104 は、異常が発生した後に、通信装置 20 の状態データに基づいて、当該通信装置 20 の状態が飽和しているか否かを判定する。例えば、飽和判定部 104 は、正規化が実行された状態データに基づいて、通信装置 20 の状態が飽和しているか否かを判定する。飽和判定部 104 は、正規化が実行された状態データが示す状態に基づいて、通信装置 20 の状態が飽和しているか否かを判定する。

[0198] なお、飽和判定部 104 は、状態データが示す状態のうち、所定のタイムウィンドウ内の状態に基づいて、当該状態が飽和しているか否かを判定してもよい。飽和判定部 104 は、タイムウィンドウに関係なく、状態データが示す状態が飽和しているか否かを判定してもよい。例えば、飽和判定部 10

4 は、状態データが示す状態のうち、基準期間内の状態に基づいて、当該状態が飽和しているか否かを判定してもよい。飽和判定部 104 は、状態データが示す状態のうち、異常が発生している異常期間内の状態に基づいて、当該状態が飽和しているか否かを判定してもよい。飽和判定部 104 は、状態データが示す全期間の状態に基づいて、当該状態が飽和しているか否かを判定してもよい。

[0199] 異常要因データ特定部 111 は、複数の通信装置 20 の各々の状態データのうち、当該通信装置 20 の状態が飽和していると判定された状態データを、異常要因データとして特定する。図 10 の例であれば、通信装置 20A の状態が飽和の傾向を示しているので、異常要因データ特定部 111 は、通信装置 20A の状態データを、異常要因データとして特定する。異常要因データが特定された後の処理は、実施形態と同様である。

[0200] 変形例 2-2 の監視システム 1 は、複数の通信装置 20 の各々の状態データに基づいて、当該通信装置 20 の状態が飽和しているか否かを判定する。監視システム 1 は、複数の通信装置 20 の各々の状態データのうち、状態が飽和していると判定された状態データを、異常要因データとして特定する。これにより、監視システム 1 は、通信サービスにおける異常に状態データが関係するか否かを判定できる。その結果、例えば、監視システム 1 は、異常の復旧を早めることができる。他にも例えば、監視システム 1 は、異常を迅速に検知したり、異常の要因を分析したりするといったことも可能になる。

[0201] [2-6-3. 変形例 2-3]

例えば、複数の通信装置 20 の各々の状態データは、当該通信装置 20 が管理する時間に基づいて生成される。複数の通信装置 20 の各々が管理する時間は、互いにずれていることがある。この場合、複数の通信装置 20 の各々の状態データの互いの時間軸がずれていることがある。このため、クラスタリング実行部 108 は、複数の通信装置 20 の各々の状態データの時間軸を揃えてから、当該時間軸が揃えられた当該状態データに基づいて、クラスタリングを実行してもよい。

[0202] 例えば、クラスタリング実行部108は、複数の通信装置20の各々から、当該通信装置20が管理する現在の時間を取得する。クラスタリング実行部108は、通信装置20ごとに、サーバ10が管理する現在の時間と、当該通信装置20が管理する現在の時間と、のずれを計算する。クラスタリング実行部108は、通信装置20ごとに、当該ずれが閾値よりも小さくなるように（例えば、当該ずれが0になるように）、当該通信装置20の時間軸をずらすことによって、複数の通信装置20の各々の時間軸を揃える。

[0203] 例えば、クラスタリング実行部108は、通信装置20Aが管理する時間が、サーバ10が管理する時間よりも15秒進んでいることを特定したとする。この場合、クラスタリング実行部108は、通信装置20Aの状態データが示す時間軸を、全体的に15秒遅れるように変更する。他にも例えば、クラスタリング実行部108は、通信装置20Bが管理する時間が、サーバ10が管理する時間よりも20秒遅れていることを特定したとする。この場合、クラスタリング実行部108は、通信装置20Bの状態データが示す時間軸を、全体的に20秒早まるように変更する。

[0204] なお、変形例2-3では、サーバ10が管理する時間が基準になる場合を例に挙げたが、クラスタリング実行部108は、複数の通信装置20の何れかが管理する時間を基準としてもよい。例えば、クラスタリング実行部108は、通信装置20Aが管理する時間を基準としてもよい。この場合、クラスタリング実行部108は、通信装置20Bが管理する時間が、通信装置20Aが管理する時間よりも32秒進んでいることを特定したとすると、通信装置20Bの状態データが示す時間軸を、全体的に32秒遅れるように変更する。クラスタリング実行部108は、通信装置20Cが管理する時間が、通信装置20Aが管理する時間よりも26秒遅れていることを特定したとすると、通信装置20Cの状態データが示す時間軸を、全体的に26秒早まるように変更する。クラスタリング実行部108は、通信装置20Aの時間軸は変更しない。

[0205] 変形例2-3の監視システム1は、複数の通信装置20の各々の状態デー

タの時間軸を揃えてから、当該時間軸が揃えられた当該状態データに基づいて、クラスタリングを実行する。複数の通信装置20の各々の状態データの時間軸がずれている場合には、本来は互いに似た特徴を有する状態データだったとしても、状態データ上の時間軸のずれによって、互いに似た特徴を有しないと判定される可能性がある。この点、監視システム1は、複数の通信装置20の各々の状態データの時間軸を揃えることによって、関連データを特定する精度を高めることができる。

[0206] [2-6-4. 変形例2-4]

例えば、通信装置20Aの状態データと、通信装置20Bの状態データと、の間に関連性があったとしても、通信装置20Aの通信量が急激に上がった30秒後に、通信装置20Bの通信量が急激に上がるといったように、これらの関連性の間にタイムラグが発生することがある。この場合、同じ時点の通信量同士がクラスタリングで比較されると、特徴としては似ていないと判定されることがある。クラスタリング実行部108が、通信装置20Bの状態データが示す波形を全体的に30秒ずつ早めたうえで、通信装置20Aの状態データと比較すると、全体的な波形の特徴が似ていることを特定しやすくなる。このため、クラスタリング実行部108は、複数の通信装置20の各々の状態データの時間軸をずらしてから、当該時間軸がずらされた当該状態データに基づいて、クラスタリングを実行してもよい。

[0207] 変形例2-4では、時間軸をどの程度ずらすかを示すずらし量は、予め決められているものとする。更に、時間軸のずらし量として、複数のずらし量が定められているものとする。例えば、10秒、20秒、30秒、40秒、50秒、及び60秒といった6つのずらし量が定められているものとする。上記の例において、通信装置20Aの状態データが異常要因データだったとすると、クラスタリング実行部108は、通信装置20Bの状態データの時間軸を、10秒だけ早めたうえでクラスタリングを実行する。更に、クラスタリング実行部108は、通信装置20Bの状態データの時間軸を、10秒だけ遅くしたうえでクラスタリングを実行する。

- [0208] 以降同様に、クラスタリング実行部108は、通信装置20Bの状態データの時間軸を、20秒、30秒、40秒、50秒、及び60秒の各々だけ早めたうえでクラスタリングを実行する。更に、クラスタリング実行部108は、通信装置20Bの状態データの時間軸を、20秒、30秒、40秒、50秒、及び60秒の各々だけ遅くしたうえでクラスタリングを実行する。クラスタリング実行部108は、通信装置20C等の以外の他の通信装置20も同様にして、状態データの時間軸を、予め定められたずらし量だけ早めた又は遅くしたうえで、クラスタリングを実行する。
- [0209] 変形例2-4の関連データ特定部109は、上記のように時間軸がずらされたうえで実行されたクラスタリングの実行結果に基づいて、関連データを特定する。例えば、関連データ特定部109は、複数の上記ずらし量の何れかに基づくクラスタリングにより、異常要因データと同じクラスに分類された状態データを、関連データとして特定する。関連データ特定部109は、複数の上記ずらし量の各々に基づくクラスタリングのうち、基準数以上のクラスタリングにより、異常要因データと同じクラスに分類された状態データを、関連データとして特定してもよい。
- [0210] 上記の例であれば、クラスタリング実行部108は、通信装置20Bの状態データの時間軸を全体的に30秒早めるようにずらした場合の処理によって、通信装置20Aの状態データと、通信装置20Bの状態データと、が似ていることを特定する。このため、先述したようなタイムラグが存在したとしても、クラスタリング実行部108は、通信装置20Aの状態データと、通信装置20Bの状態データと、を同じクラスに分類できる。クラスタリング実行部108は、上記複数のずらし量のうちの少なくとも1つについて、互いに類似すると判定した状態データ同士を、同じクラスに分類する。
- [0211] 変形例2-4の監視システム1は、複数の通信装置20の各々の状態データの時間軸をずらしてから、当該時間軸がずらされた当該状態データに基づいて、クラスタリングを実行する。監視システム1は、互いに関連性のある異常要因データ及び関連データの間にタイムラグがあったとしても、あえて

時間軸をずらすことによって、タイムラグを吸収し、異常要因データと関連性のある関連データを特定できる。

[0212] [2-6-5. 変形例2-5]

例えば、変形例2-4において、クラスタリング実行部108は、複数の通信装置20の各々の状態データが示す時系列的な状態の変化のうちの一部の期間に基づいて、時間軸のずらし量を決定し、当該決定されたずらし量に基づいて、複数の通信装置20の各々の状態データの時間軸をずらしてもよい。変形例2-5では、クラスタリング実行部108は、複数のずらし量の何れを利用するかを、状態データが示す期間のうちの一部だけを利用して決定する。

[0213] 例えば、クラスタリング実行部108は、異常要因データが示す特徴的な期間を、上記一部の期間として決定する。当該期間を決定するための基準となる特徴は、予め定められているものとする。図10の例であれば、通信装置20Aの状態データが異常要因データに相当する。更に、通信装置20Aの通信量が急激に上がったタイミングが異常の特徴を示す場合には、クラスタリング実行部108は、当該タイミングを含む期間を、上記一部の期間として決定する。当該期間は、管理者が手動で指定してもよい。

[0214] 例えば、クラスタリング実行部108は、複数のずらし量の各々について、通信装置20Aの状態データのうちの上記一部の期間の状態変化と、他の通信装置20の状態データのうちの上記一部の期間の状態変化と、を比較する。クラスタリング実行部108は、複数のずらし量のうち、最も状態変化の差が小さいずらし量を、時間軸のずらし量として決定する。クラスタリング実行部108は、当該決定されたずらし量に基づいて、変形例2-4で説明した処理を実行し、クラスタリングを実行する。ずらし量に基づくクラスタリングは、変形例2-4と同様であってよい。

[0215] 変形例2-5の監視システム1は、複数の通信装置20の各々の状態データが示す時系列的な状態の変化のうちの一部の期間に基づいて、時間軸のずらし量を決定し、当該決定されたずらし量に基づいて、複数の通信装置20

の各々の状態データの時間軸をずらす。監視システム 1 は、互いに関連性のある異常要因データ及び関連データの間にタイムラグがあったとしても、最適なずらし量で時間軸をずらすことによって、タイムラグを吸収し、異常要因データと関連性のある関連データを特定できる。監視システム 1 は、不要なずらし量に基づく処理を実行しなくて済むので、処理負荷を軽減できる。

[0216] [2-6-6. 変形例 2-6]

例えば、クラスタリング実行部 108 は、複数の通信装置 20 の各々の状態データが示す値の差を計算し、当該計算された差に基づいて、クラスタリングを実行してもよい。図 10 を例に挙げると、クラスタリング実行部 108 は、通信装置 20A の状態データである異常要因データと、通信装置 20B~20E の各々の状態データと、の差を計算する。当該差は、マハラノビス距離等の公知の指標が利用されてよい。クラスタリング実行部 108 は、当該差の変化量が閾値未満の状態データを、異常要因データと同じクラスタに分類する。

[0217] 図 10 の例では、通信装置 20A の状態データである異常要因データと、通信装置 20E の状態データと、の差がある一定範囲に収まった状態が継続しているので、クラスタリング実行部 108 は、異常要因データと、通信装置 20E の状態データと、を同じクラスタに分類する。即ち、クラスタリング実行部 108 は、異常要因データとの差がある程度存在したとしても、当該差が一定範囲に収まっている状態データであれば、異常要因データと同じクラスタに当該状態データを分類する。なお、クラスタリング実行部 108 は、変化量ではなく、当該差だけに基づいて、クラスタリングを実行してもよい。クラスタリングが実行された後の処理は、実施形態で説明した通りである。

[0218] 変形例 2-6 の監視システム 1 は、複数の通信装置 20 の各々の状態データが示す値の差を計算し、当該計算された差に基づいて、クラスタリングを実行する。これにより、監視システム 1 は、複数の通信装置 20 の各々の状態データが示す差に着目したクラスタリングを実行し、クラスタリングの精

度を高めることができる。

[0219] [2-6-7. 変形例2-7]

例えば、通信装置20によっては、強制的な再起動やシャットダウン等のいわゆるノードダウンによって、状態データの一部が取得されないことがある、この場合に、状態データ取得部101は、複数の通信装置20のうち、状態データの一部が取得されなかった通信装置20の当該全部又は当該一部が所定の値を示すように、状態データを取得してもよい。所定の値は、予め管理者が指定した値であってもよいし、その場で動的に計算されてもよい。

[0220] 図10の例において、通信装置20Bの状態データのうちの一部分が、通信装置20Bの強制的な再起動によって欠損していたとする。この場合、状態データ取得部101は、状態データのうち、欠損していなかった部分の平均値で、欠損した部分を埋めてもよい。状態データ取得部101は、状態データのうち、欠損した部分を、管理者が指定した値で埋めてもよい。当該部分を埋めることは、パディングと呼ばれることもある。欠損した部分を埋める方法自体は、公知のパディングの方法を利用可能である。

[0221] 変形例2-7の監視システム1は、複数の通信装置20のうち、状態データの一部が取得されなかった通信装置20の当該全部又は当該一部が所定の値を示すように、状態データを取得する。これにより、監視システム1は、状態データの一部が欠損していたとしても、クラスタリングを実行できる。

[0222] [2-6-8. 変形例2-8]

例えば、クラスタリング実行部108は、複数の通信装置20の各々の状態データと、当該状態データに関連付けられた属性と、に基づいて、クラスタリングを実行してもよい。属性は、何らかの観点で状態データを分類可能な情報であればよく、変形例2-8では、複数の通信装置20の各々が配置された場所を示す場合を例に挙げる。場所は、市町村といったある程度広い範囲であってもよいし、通信装置20がある建物、部屋、又はラックといったある程度狭い範囲であってもよい。属性は、通信装置20が配置された場所に限られず、例えば、通信装置20の性能、役割、又は種類であってもよい。

い。属性は、状態データが意味する内容、又は、状態データのサンプリング周期等の取得条件であってもよい。通信装置20の属性を示すデータは、データ記憶部100に予め記憶されているものとする。

[0223] 例えば、クラスタリング実行部108は、複数の通信装置20の各々の状態データと、当該状態データに関連付けられた場所と、に基づいて、クラスタリングを実行する。クラスタリング実行部108は、同じ場所に配置された複数の通信装置20の各々の状態データに基づいて、クラスタリングを実行する。クラスタリング実行部108は、複数の通信装置20の各々の状態データ同士の特徴が似ていたとしても、異なる場所に配置された通信装置20であれば、同じクラスタには属さないようにする。クラスタリング実行部108は、あくまで同じ場所に配置された複数の通信装置20の中で、クラスタリングを実行する。

[0224] なお、場所以外の属性が利用される場合のクラスタリングも、上記と同様の方法で実行されてよい。例えば、クラスタリング実行部108は、同じ属性が関連付けられた複数の通信装置20の各々の状態データに基づいて、クラスタリングを実行する。クラスタリング実行部108は、複数の通信装置20の各々の状態データ同士の特徴が似ていたとしても、異なる属性が関連付けられた通信装置20の状態データであれば、同じクラスタには属さないようにする。クラスタリング実行部108は、あくまで同じ属性が状態データに関連付けられた複数の通信装置20の中で、クラスタリングを実行する。クラスタリングが実行された後の処理は、実施形態と同様である。

[0225] 変形例2-8の監視システム1は、複数の通信装置20の各々の状態データと、当該状態データに関連付けられた属性と、に基づいて、クラスタリングを実行する。これにより、監視システム1は、状態データの属性を考慮したクラスタリングを実行できるので、クラスタリングの精度を高めることができる。例えば、監視システム1は、同じ属性が状態データに関連付けられた複数の通信装置20の中でクラスタリングを実行することで、状態データ同士の関連性を精度よく特定できる。

[0226] また、監視システム 1 は、複数の通信装置 20 の各々の状態データと、当該状態データに関連付けられた場所と、に基づいて、クラスタリングを実行する。これにより、監視システム 1 は、通信装置 20 が配置された場所を考慮したクラスタリングを実行できるので、クラスタリングの精度を高めることができる。例えば、監視システム 1 は、同じ場所に配置された複数の通信装置 20 の中でクラスタリングを実行することで、状態データ同士の関連性を精度よく特定できる。

[0227] [2-6-9. 変形例 2-9]

例えば、変形例 2-9 において、クラスタリング実行部 108 は、複数の通信装置 20 の各々の状態データに基づく時系列データを所定時間間隔で平均化してよい。例えば、状態データが 1 個 / 1 秒の頻度で取得される場合、状態データの数量は 3600 個 / 60 分となる。当該状態データを 1 分間隔で平均化すると、3600 個 / 60 分の状態データは 60 個に削減される。変形例 2-9 のクラスタリング実行部 108 は、事前に状態データの平均化を行うことによって、平均化前の時系列データと類似する軽量の時系列データを作成することができ、クラスタリングの処理負荷を軽減できる。

[0228] [2-6-10. その他の変形例]

例えば、上記変形例を組み合わせてもよい。

[0229] 例えば、監視システム 1 は、SNS の投稿に基づいて、サービスにおける異常を検知してもよい。この場合、監視システム 1 は、SNS の投稿に関する投稿データを取得する。投稿データは、テキスト、画像、動画、ハッシュタグ、又はこれらの組み合わせであってもよい。監視システム 1 は、監視対象となるサービスの名前を含む投稿の数に基づいて、異常を検知する。監視システム 1 は、当該投稿の数が閾値以上になった場合に、異常を検知する。関連データ特定部 109 は、SNS における投稿データと、通信装置 20 の状態データと、の関連性を特定してもよい。例えば、関連データ特定部 109 は、SNS における投稿の数が増えたタイミングと、通信装置 20 の状態データが示す負荷が増加したタイミングと、の間に相関関係がある場合に、

SNSにおける投稿データと、通信装置20の状態データと、の間に関連性があることを特定してもよい。

[0230] 例えば、監視システム1は、通信サービス以外の他のサービスにも適用可能である。例えば、監視システム1は、電子商取引サービス、旅行予約サービス、金融サービス、決済サービス、オンラインフリーマーケットサービス、又は動画配信サービスといった他のサービスにおける異常の要因となる異常要因データと関連性のある関連データを特定してもよい。監視対象となる装置は、これらのサービスで利用される装置であればよく、実施形態のような通信装置に限られない。例えば、監視対象となる装置は、サーバコンピュータ、パーソナルコンピュータ、タブレット、電源装置、プリンタ、スキャナ、又はその他の装置であってもよい。

[0231] 例えば、実施形態では、サーバ10で主な処理が実行される場合を説明したが、サーバ10で実行されるものとして説明した処理は、管理者端末40又は他のコンピュータで実行されてもよいし、複数のコンピュータで分担されてもよい。

[0232] [3. 付記]

例えば、監視システムは、下記のような構成も可能である。

[0233] [3-1. 第1実施形態に係る付記]

(1-1)

サービスにおける監視対象となる装置の時系列的な状態の変化に関する状態データを取得する状態データ取得部と、

前記状態データに基づいて、前記状態が飽和しているか否かを判定する飽和判定部と、

前記飽和判定部の判定結果に基づいて、前記サービスにおける異常に前記状態データが関係するか否かを判定する関係判定部と、

を含む監視システム。

(1-2)

前記状態データ取得部は、前記異常が検知された場合に、前記状態データ

を取得し、

前記飽和判定部は、前記異常が検知された場合に、前記状態データに基づいて、前記状態が飽和しているか否かを判定し、

前記関係判定部は、前記異常が検知された場合に、前記異常に前記状態データが関係するか否かを判定し、

前記監視システムは、前記異常が検知された場合に、前記異常に関係すると判定された前記状態データに基づいて、前記異常の復旧に関する復旧処理を実行する復旧処理実行部を更に含む、

(1-1)に記載の監視システム。

(1-3)

前記状態データ取得部は、前記異常が検知される前に、前記状態データを取得し、

前記飽和判定部は、前記異常が検知される前に、前記状態データに基づいて、前記状態が飽和しているか否かを判定し、

前記関係判定部は、前記異常が検知される前に、前記異常に前記状態データが関係するか否かを判定し、

前記監視システムは、前記異常に関係すると判定された前記状態データに基づいて、前記異常の検知に関する検知処理を実行する検知処理実行部を更に含む、

(1-1)又は(1-2)に記載の監視システム。

(1-4)

前記状態データ取得部は、複数の前記サービスの各々における前記装置の前記状態データを取得し、

前記飽和判定部は、前記複数のサービスの各々における前記装置の前記状態データに基づいて、前記装置が飽和しているか否かを判定し、

前記関係判定部は、前記飽和判定部の判定結果に基づいて、前記複数のサービスの各々における前記異常に前記状態データが関係するか否かを判定する、

(1-1) ~ (1-3) の何れかに記載の監視システム。

(1-5)

前記監視システムは、前記異常が検知された場合に、前記異常が発生した異常発生タイミングに基づいて、前記状態データに関する期間を設定する期間設定部を更に含み、

前記状態データ取得部は、前記期間における前記装置の時系列的な状態の変化に関する前記状態データを取得する、

(1-1) ~ (1-4) の何れかに記載の監視システム。

(1-6)

前記監視システムは、前記状態データに関する正規化を実行する正規化実行部を更に含み、

前記飽和判定部は、前記正規化が実行された前記状態データに基づいて、前記状態が飽和しているか否かを判定する、

(1-1) ~ (1-5) の何れかに記載の監視システム。

(1-7)

前記関係判定部は、前記状態データに前記変化が示された期間のうち、前記状態が飽和していると判定された飽和期間に基づいて、前記異常に前記状態データが関係するか否かを判定する、

(1-1) ~ (1-6) の何れかに記載の監視システム。

(1-8)

前記関係判定部は、前記状態データに前記変化が示された期間のうち、前記異常が発生している異常期間よりも前の他の期間における前記状態の最高値に基づいて、前記異常に前記状態データが関係するか否かを判定する、

(1-1) ~ (1-7) の何れかに記載の監視システム。

(1-9)

前記他の期間は、前記異常期間よりも前の期間であり、

前記関係判定部は、前記他の期間における前記状態の最高値と、前記他の期間よりも前の期間における前記状態の最高値と、に基づいて、前記異常に

前記状態データが関係するか否かを判定する、

(1-8)に記載の監視システム。

(1-10)

前記関係判定部は、前記状態データに前記変化が示された期間のうち、前記異常が発生している異常期間における前記状態データが示す前記状態の最高値に基づいて、前記異常に前記状態データが関係するか否かを判定する、

(1-1)～(1-9)の何れかに記載の監視システム。

(1-11)

前記関係判定部は、前記状態データに前記変化が示された期間のうち、前記異常が発生している異常期間と、前記状態が飽和していると判定された飽和期間と、の一致度に基づいて、前記異常に前記状態データが関係するか否かを判定する、

(1-1)～(1-10)の何れかに記載の監視システム。

(1-12)

前記関係判定部は、前記状態データに前記変化が示された期間のうち、前記状態が飽和している飽和期間と、前記異常が発生している異常期間よりも前の他の期間と、の各々における前記状態の変化量に基づいて、前記異常に前記状態データが関係するか否かを判定する、

(1-1)～(1-11)の何れかに記載の監視システム。

[0234] [3-2. 第2実施形態に係る付記]

(2-1)

サービスにおける監視対象となる複数の装置の各々の状態に関する状態データを取得する状態データ取得部と、

前記複数の装置の各々の前記状態データに関するクラスタリングを実行するクラスタリング実行部と、

前記クラスタリングの実行結果に基づいて、前記サービスにおける異常の要因に関する前記状態データである異常要因データと関連性のある他の前記状態データである関連データを特定する関連データ特定部と、

を含む監視システム。

(2-2)

前記状態データ取得部は、前記異常が検知された場合に、前記複数の装置の各々の前記状態データを取得し、

前記クラスタリング実行部は、前記異常が検知された場合に、前記複数の装置の各々の前記状態データに基づいて、前記クラスタリングを実行し、

前記関連データ特定部は、前記異常が検知された場合に、前記関連データを特定し、

前記監視システムは、前記異常が検知された場合に、前記異常要因データと、前記関連データと、に基づいて、前記異常の復旧に関する復旧処理を実行する復旧処理実行部を更に含む、

(2-1)に記載の監視システム。

(2-3)

前記状態データ取得部は、前記異常が検知される前に、前記複数の装置の各々の前記状態データを取得し、

前記クラスタリング実行部は、前記異常が検知される前に、前記複数の装置の各々の前記状態データに基づいて、前記クラスタリングを実行し、

前記関連データ特定部は、前記異常が検知される前に、前記関連データを特定し、

前記監視システムは、前記異常要因データと、前記関連データと、に基づいて、前記異常の検知に関する検知処理を実行する検知処理実行部を更に含む、

(2-1)又は(2-2)に記載の監視システム。

(2-4)

前記複数の装置の各々の前記状態データは、当該装置の時系列的な前記状態の変化を示し、

前記クラスタリング実行部は、前記複数の装置の各々の前記状態データが示す時系列的な前記状態の変化に基づいて、前記クラスタリングを実行する

、

(2-1) ~ (2-3) の何れかに記載の監視システム。

(2-5)

前記監視システムは、

前記複数の装置の各々の前記状態データに基づいて、当該前記状態データが示す前記状態が飽和しているか否かを判定する飽和判定部と、

前記複数の装置の各々の前記状態データのうち、前記状態が飽和していると判定された前記状態データを、前記異常要因データとして特定する異常要因データ特定部と、

を更に含む(2-4)に記載の監視システム。

(2-6)

前記クラスタリング実行部は、前記複数の装置の各々の前記状態データの時間軸を揃えてから、当該時間軸が揃えられた当該状態データに基づいて、前記クラスタリングを実行する、

(2-4) 又は(2-5)に記載の監視システム。

(2-7)

前記クラスタリング実行部は、前記複数の装置の各々の前記状態データの時間軸をずらしてから、当該時間軸がずらされた当該状態データに基づいて、前記クラスタリングを実行する、

(2-4) ~ (2-6) の何れかに記載の監視システム。

(2-8)

前記クラスタリング実行部は、前記複数の装置の各々の前記状態データが示す時系列的な前記状態の変化のうちの一部の期間に基づいて、前記時間軸のずらし量を決定し、当該決定されたずらし量に基づいて、前記複数の装置の各々の前記状態データの時間軸をずらす、

(2-7)に記載の監視システム。

(2-9)

前記クラスタリング実行部は、前記複数の装置の各々の前記状態データが

示す値の差を計算し、当該計算された差に基づいて、前記クラスタリングを実行する、

(2-1) ~ (2-8) の何れかに記載の監視システム。

(2-10)

前記状態データ取得部は、前記複数の装置のうち、前記状態データの一部が取得されなかった前記装置の当該全部又は当該一部が所定の値を示すように、前記状態データを取得する、

(2-1) ~ (2-9) の何れかに記載の監視システム。

(2-11)

前記クラスタリング実行部は、前記複数の装置の各々の前記状態データと、当該状態データに関連付けられた属性と、に基づいて、前記クラスタリングを実行する、

(2-1) ~ (2-10) の何れかに記載の監視システム。

(2-12)

前記属性は、前記複数の装置の各々が配置された場所を示し、
前記クラスタリング実行部は、前記複数の装置の各々の前記状態データと、当該状態データに関連付けられた前記場所と、に基づいて、前記クラスタリングを実行する、

(2-11) に記載の監視システム。

請求の範囲

- [請求項1] サービスにおける監視対象となる装置の状態に関する状態データを取得する状態データ取得部を含み、
前記状態データに基づいて、前記サービスにおける異常に関する処理を実行する、
監視システム。
- [請求項2] 前記状態データ取得部は、前記装置の時系列的な状態の変化に関する前記状態データを取得し、
前記監視システムは、
前記状態データに基づいて、前記状態が飽和しているか否かを判定する飽和判定部と、
前記飽和判定部の判定結果に基づいて、前記サービスにおける異常に前記状態データが関係するか否かを判定する関係判定部と、
を更に含む請求項1に記載の監視システム。
- [請求項3] 前記状態データ取得部は、前記異常が検知された場合に、前記状態データを取得し、
前記飽和判定部は、前記異常が検知された場合に、前記状態データに基づいて、前記状態が飽和しているか否かを判定し、
前記関係判定部は、前記異常が検知された場合に、前記異常に前記状態データが関係するか否かを判定し、
前記監視システムは、前記異常が検知された場合に、前記異常に関係すると判定された前記状態データに基づいて、前記異常の復旧に関する復旧処理を実行する復旧処理実行部を更に含む、
請求項2に記載の監視システム。
- [請求項4] 前記状態データ取得部は、前記異常が検知される前に、前記状態データを取得し、
前記飽和判定部は、前記異常が検知される前に、前記状態データに基づいて、前記状態が飽和しているか否かを判定し、

前記関係判定部は、前記異常が検知される前に、前記異常に前記状態データが関係するか否かを判定し、

前記監視システムは、前記異常に関係すると判定された前記状態データに基づいて、前記異常の検知に関する検知処理を実行する検知処理実行部を更に含む、

請求項 2 又は 3 に記載の監視システム。

[請求項5] 前記状態データ取得部は、複数の前記サービスの各々における前記装置の前記状態データを取得し、

前記飽和判定部は、前記複数のサービスの各々における前記装置の前記状態データに基づいて、前記装置が飽和しているか否かを判定し、

前記関係判定部は、前記飽和判定部の判定結果に基づいて、前記複数のサービスの各々における前記異常に前記状態データが関係するか否かを判定する、

請求項 2 又は 3 に記載の監視システム。

[請求項6] 前記監視システムは、前記異常が検知された場合に、前記異常が発生した異常発生タイミングに基づいて、前記状態データに関する期間を設定する期間設定部を更に含む、

前記状態データ取得部は、前記期間における前記装置の時系列的な状態の変化に関する前記状態データを取得する、

請求項 2 又は 3 に記載の監視システム。

[請求項7] 前記監視システムは、前記状態データに関する正規化を実行する正規化実行部を更に含む、

前記飽和判定部は、前記正規化が実行された前記状態データに基づいて、前記状態が飽和しているか否かを判定する、

請求項 2 又は 3 に記載の監視システム。

[請求項8] 前記関係判定部は、前記状態データに前記変化が示された期間のうち、前記状態が飽和していると判定された飽和期間に基づいて、前記

異常に前記状態データが関係するか否かを判定する、

請求項 2 又は 3 に記載の監視システム。

[請求項9] 前記関係判定部は、前記状態データに前記変化が示された期間のうち、前記異常が発生している異常期間よりも前の他の期間における前記状態の最高値に基づいて、前記異常に前記状態データが関係するか否かを判定する、

請求項 2 又は 3 に記載の監視システム。

[請求項10] 前記他の期間は、前記異常期間よりも前の期間であり、
前記関係判定部は、前記他の期間における前記状態の最高値と、前記他の期間よりも前の期間における前記状態の最高値と、に基づいて、前記異常に前記状態データが関係するか否かを判定する、

請求項 7 に記載の監視システム。

[請求項11] 前記関係判定部は、前記状態データに前記変化が示された期間のうち、前記異常が発生している異常期間における前記状態データが示す前記状態の最高値に基づいて、前記異常に前記状態データが関係するか否かを判定する、

請求項 2 又は 3 に記載の監視システム。

[請求項12] 前記関係判定部は、前記状態データに前記変化が示された期間のうち、前記異常が発生している異常期間と、前記状態が飽和していると判定された飽和期間と、の一致度に基づいて、前記異常に前記状態データが関係するか否かを判定する、

請求項 2 又は 3 に記載の監視システム。

[請求項13] 前記関係判定部は、前記状態データに前記変化が示された期間のうち、前記状態が飽和している飽和期間と、前記異常が発生している異常期間よりも前の他の期間と、の各々における前記状態の変化量に基づいて、前記異常に前記状態データが関係するか否かを判定する、

請求項 2 又は 3 に記載の監視システム。

[請求項14] 前記状態データ取得部は、複数の前記装置の各々の状態に関する前

記状態データを取得し、

前記監視システムは、

前記複数の装置の各々の前記状態データに関するクラスタリングを
実行するクラスタリング実行部と、

前記クラスタリングの実行結果に基づいて、前記サービスにおける
異常の要因に関する前記状態データである異常要因データと関連性の
ある他の前記状態データである関連データを特定する関連データ特定
部と、

を更に含む請求項 1 に記載の監視システム。

[請求項15]

前記状態データ取得部は、前記異常が検知された場合に、前記複数の
装置の各々の前記状態データを取得し、

前記クラスタリング実行部は、前記異常が検知された場合に、前記
複数の装置の各々の前記状態データに基づいて、前記クラスタリング
を実行し、

前記関連データ特定部は、前記異常が検知された場合に、前記関連
データを特定し、

前記監視システムは、前記異常が検知された場合に、前記異常要因
データと、前記関連データと、に基づいて、前記異常の復旧に関する
復旧処理を実行する復旧処理実行部を更に含む、

請求項 1 4 に記載の監視システム。

[請求項16]

前記状態データ取得部は、前記異常が検知される前に、前記複数の
装置の各々の前記状態データを取得し、

前記クラスタリング実行部は、前記異常が検知される前に、前記複
数の装置の各々の前記状態データに基づいて、前記クラスタリングを
実行し、

前記関連データ特定部は、前記異常が検知される前に、前記関連デ
ータを特定し、

前記監視システムは、前記異常要因データと、前記関連データと、

に基づいて、前記異常の検知に関する検知処理を実行する検知処理実行部を更に含む、

請求項 1 4 又は 1 5 に記載の監視システム。

[請求項17] 前記複数の装置の各々の前記状態データは、当該装置の時系列的な前記状態の変化を示し、

前記クラスタリング実行部は、前記複数の装置の各々の前記状態データが示す時系列的な前記状態の変化に基づいて、前記クラスタリングを実行する、

請求項 1 4 又は 1 5 に記載の監視システム。

[請求項18] 前記監視システムは、

前記複数の装置の各々の前記状態データに基づいて、当該前記状態データが示す前記状態が飽和しているか否かを判定する飽和判定部と、

前記複数の装置の各々の前記状態データのうち、前記状態が飽和していると判定された前記状態データを、前記異常要因データとして特定する異常要因データ特定部と、

を更に含む請求項 1 7 に記載の監視システム。

[請求項19] 前記クラスタリング実行部は、前記複数の装置の各々の前記状態データの時間軸を揃えてから、当該時間軸が揃えられた当該状態データに基づいて、前記クラスタリングを実行する、

請求項 1 7 に記載の監視システム。

[請求項20] 前記クラスタリング実行部は、前記複数の装置の各々の前記状態データの時間軸をずらしてから、当該時間軸がずらされた当該状態データに基づいて、前記クラスタリングを実行する、

請求項 1 7 に記載の監視システム。

[請求項21] 前記クラスタリング実行部は、前記複数の装置の各々の前記状態データが示す時系列的な前記状態の変化のうちの一部の期間に基づいて、前記時間軸のずらし量を決定し、当該決定されたずらし量に基づい

て、前記複数の装置の各々の前記状態データの時間軸をずらす、
請求項 20 に記載の監視システム。

[請求項22] 前記クラスタリング実行部は、前記複数の装置の各々の前記状態データが示す値の差を計算し、当該計算された差に基づいて、前記クラスタリングを実行する、

請求項 14 又は 15 に記載の監視システム。

[請求項23] 前記状態データ取得部は、前記複数の装置のうち、前記状態データの一部が取得されなかった前記装置の当該全部又は当該一部が所定の値を示すように、前記状態データを取得する、

請求項 14 又は 15 に記載の監視システム。

[請求項24] 前記クラスタリング実行部は、前記複数の装置の各々の前記状態データと、当該状態データに関連付けられた属性と、に基づいて、前記クラスタリングを実行する、

請求項 14 又は 15 に記載の監視システム。

[請求項25] 前記属性は、前記複数の装置の各々が配置された場所を示し、
前記クラスタリング実行部は、前記複数の装置の各々の前記状態データと、当該状態データに関連付けられた前記場所と、に基づいて、前記クラスタリングを実行する、

請求項 24 に記載の監視システム。

[請求項26] サービスにおける監視対象となる装置の状態に関する状態データを取得する状態データ取得ステップを含み、

前記状態データに基づいて、前記サービスにおける異常に関する処理を実行する、

監視方法。

[請求項27] サービスにおける監視対象となる装置の状態に関する状態データを取得する状態データ取得部としてコンピュータを機能させ、

前記コンピュータに、前記状態データに基づいて、前記サービスにおける異常に関する処理を実行させる、

プログラム。