(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2009-217382
(P2009-217382A)
(43)公開日　平成21年9月24日(2009.9.24)

(51)Int.Cl.		F I		テーマコード（参考）
G06F 11/34	(2006.01)	G06F 11/34	S	5B042
G06F 11/30	(2006.01)	G06F 11/30		

審査請求 未請求　請求項の数 11　ＯＬ　（全 22 頁）

(21)出願番号　特願2008-58441 (P2008-58441)
(22)出願日　平成20年3月7日 (2008.3.7)

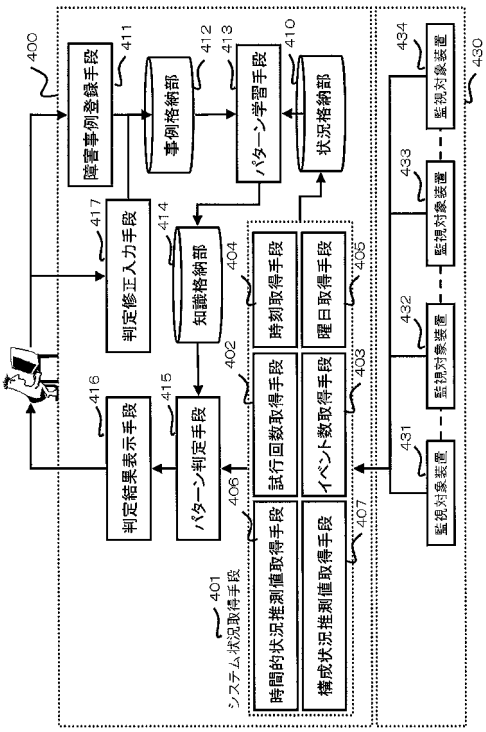
（出願人による申告）平成１９年度、総務省、「ユビキタスネットワーク制御・管理技術の研究開発」委託研究、産業技術力強化法第１９条の適用を受ける特許出願

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(74)代理人　100077827
弁理士　鈴木　弘男
(72)発明者　中台　慎二
東京都港区芝五丁目７番１号　日本電気株式会社内

Ｆターム(参考)　5B042 JJ15　JJ17　JJ29　KK13　KK14　MC15

(54)【発明の名称】障害分析システム、障害分析方法、障害分析サーバおよび障害分析プログラム

(57)【要約】
【課題】システムにおける障害を検出し、障害の種類または場所を保守運用者に提示する運用管理システムの中で、事例を登録してルールや閾値が学習されるような障害分析システムにおいては、障害検出の精度が悪く、本来検出されるべき障害とは異なる種類または場所の障害が検出されていた。
【解決手段】障害の種類や場所を学習する際に用いる特徴空間を、監視対象装置の異常度を示す値と、監視対象装置に関する状況情報と、を含めることで、障害を分類する超平面を生成する際に、障害の種類や場所、あるいは正常であるといったラベルがついた事例間が、特徴空間内で距離を持つことができ、障害を高い精度で検出し分類できる超平面を生成することができるようになる。
【選択図】図４



【特許請求の範囲】
【請求項１】
監視対象装置の異常度を示す複数の指標値を含むシステム情報を前記システム情報の識別情報とともに順次出力する監視対象装置から、前記システム情報および前記システム情報の識別情報を順次受信するシステム情報受信手段と、
前記システム情報受信手段が受信した前記各システム情報を所定の判定基準と比較し、比較の結果に基づいて前記各システム情報を種別毎に分類する種別判定手段と、
前記各システム情報の識別情報と、前記各システム情報が分類された各種別を示す情報と、を対応付けて出力する判定結果出力部と、
前記各システム情報の識別情報についてそれぞれ真の種別を示す情報の入力を受ける障害事例登録手段と、
前記各システム情報の識別情報を前記真の種別と対応付けて記憶する事例格納部と、
前記システム情報受信手段が受信した各システム情報と、前記各システム情報の識別情報に対応付けて記憶されている真の種別を示す情報と、に基づいて前記判定基準を更新するパターン学習手段と、
を備え、
前記種別判定手段は、前記各システム情報に前記監視対象装置の異常度とは関係のない指標値を含めて前記判定基準と比較することにより、前記各システム情報を種別毎に分類する、情報処理装置。
【請求項２】
請求項１に記載の情報処理装置であって、
前記監視対象装置の異常度とは関係のない指標値には、前記監視対象装置が前記監視対象装置と接続される他の装置に所定の期間にデータを送信した回数を示す送信回数情報を含める、情報処理装置。
【請求項３】
請求項１に記載の情報処理装置であって、
前記監視対象装置の異常度とは関係のない指標値には、時刻を示す時刻情報を含める、情報処理装置。
【請求項４】
請求項１に記載の情報処理装置であって、
前記監視対象装置の異常度とは関係のない指標値には、曜日を示す曜日情報を含める、情報処理装置。
【請求項５】
請求項１に記載の情報処理装置であって、
前記情報処理装置は、前記システム情報受信部が受信したシステム情報に含まれる指標値に基づいて、前記指標値の現在の予測値を算出する時間的状況推測値算出手段を備え、
前記監視対象装置の異常度とは関係のない指標値には、前記時間的状況推測値算出手段が算出した前記予測値を含める、情報処理装置。
【請求項６】
請求項１に記載の情報処理装置であって、
前記情報処理装置は、第１の監視対象装置と第２の監視対象装置とそれぞれ通信可能に接続され、
前記事例格納部は、前記監視対象装置毎に前記各システム情報の識別情報を前記真の種別と対応付けて記憶し、
前記第１の監視対象装置の各指標値と前記第２の監視対象装置の各指標値との関係を算出する構成状況推測値算出手段を備え、
前記構成状況推測値算出手段は、前記第１の監視対象装置の各指標値と前記算出された関係とに基づいて、前記第２の監視対象装置の各指標値の予測値を求め、
前記種別判定手段は、前記求めた予測値を前記判定基準と比較することで前記第２の監視対象装置の各システム情報を種別毎に分類する、情報処理装置。

【請求項７】
請求項1に記載の情報処理装置であって、
前記監視対象装置の異常度とは関係のない指標値には、前記監視対象装置において所定の期間に発生したイベントの回数を示すイベント回数情報を含める、情報処理装置。
【請求項８】
請求項１に記載の情報処理装置であって、
前記真の種別を示す情報は、前記監視対象装置が正常であるか異常であるかを示す情報である、情報処理装置。
【請求項９】
請求項１に記載の情報処理装置であって、
前記障害事例登録手段は、前記真の種別を示す情報を、オペレータにより操作される端末から受信する、情報処理装置。
【請求項１０】
情報処理装置の制御方法であって、
前記情報処理装置が、監視対象装置の異常度を示す複数の指標値を含むシステム情報を前記システム情報の識別情報とともに順次出力する監視対象装置から、前記システム情報および前記システム情報の識別情報を順次受信し、
前記情報処理装置が、受信した前記各システム情報を所定の判定基準と比較し、比較の結果に基づいて前記各システム情報を種別毎に分類し、
前記情報処理装置が、前記各システム情報の識別情報と、前記各システム情報が分類された各種別を示す情報と、を対応付けて出力し、
前記情報処理装置が、前記各システム情報の識別情報についてそれぞれ真の種別を示す情報の入力を受け、
前記情報処理装置が、前記各システム情報の識別情報を前記真の種別と対応付けて記憶し、
前記情報処理装置が、受信した各システム情報と、前記各システム情報の識別情報に対応付けて記憶されている真の種別を示す情報と、に基づいて前記判定基準を更新し、
前記情報処理装置が、前記各システム情報に前記監視対象装置の異常度とは関係のない指標値を含めて前記判定基準と比較することにより、前記各システム情報を種別毎に分類する、情報処理装置の制御方法。
【請求項１１】
情報処理装置の制御プログラムであって、
前記情報処理装置に、
監視対象装置の異常度を示す複数の指標値を含むシステム情報を前記システム情報の識別情報とともに順次出力する監視対象装置から、前記システム情報および前記システム情報の識別情報を順次受信する処理と、
受信した前記各システム情報を所定の判定基準と比較し、比較の結果に基づいて前記各システム情報を種別毎に分類する処理と、
前記各システム情報の識別情報と、前記各システム情報が分類された各種別を示す情報と、を対応付けて出力する処理と、
前記各システム情報の識別情報についてそれぞれ真の種別を示す情報の入力を受ける処理と、
前記各システム情報の識別情報を前記真の種別と対応付けて記憶する処理と、
受信した各システム情報と、前記各システム情報の識別情報に対応付けて記憶されている真の種別を示す情報と、に基づいて前記判定基準を更新する処理と、
前記各システム情報に前記監視対象装置の異常度とは関係のない指標値を含めて前記判定基準と比較することにより、前記各システム情報を種別毎に分類する処理と、
を実行させる情報処理装置の制御プログラム。
【発明の詳細な説明】
【技術分野】

【０００１】
本発明はシステム障害分析システム、障害分析方法、障害分析サーバおよび障害分析プログラムに関し、特にルールや閾値を設定することなく、システム障害を検出し分類できるシステム障害分析システム、障害分析方法、障害分析サーバおよび障害分析プログラムに関する。
【背景技術】
【０００２】
従来の障害分析システムの一例が、特許文献１に記載されている。図１に示すように、この従来の障害分析システム１００は、動作測定記録（ＯＭ）転送ユニットや障害記録転送ユニットといった異常呼量監視手段と、閾値判定手段と、判定結果表示手段とから構成されている。
【０００３】
また、他の従来の障害分析システムの一例が、非特許文献１に記載されている。図２に示すように、この従来の障害分析システム２００は、監視対象装置２３１～２３４からなる監視対象システム２３０を管理するために、異常度監視手段２０１と、異常度格納部２１０と、障害事例登録手段２１１と、事例格納部２１２と、パターン学習手段２１３と、知識格納部２１４と、パターン判定手段２１５と、判定結果表示手段２１６と、判定修正入力手段２１７とから構成されている。
【０００４】
パターン学習手段２１３は、Ｓｕｐｐｏｒｔ　Ｖｅｃｔｏｒ　Ｍａｃｈｉｎｅ（ＳＶＭ）というパターン識別器を用いて行われるパターン学習によって知識情報を生成する。
【０００５】
このＳＶＭは、非特許文献２に詳しい。一般に、パターン学習においては、まず、多次元の変数から一次元のクラス（パターン）を推定する。この多次元の変数として用いる変数を特徴と呼ぶ。またｄ個からなる特徴が張るｄ次元空間を特徴空間R^dと呼ぶ。また、入力変数を、この特徴空間における特徴変数ｘ（$\in R^d$）とし、出力変数をクラスｙ（$\in \{1, -1\}$）とすると、特徴空間内でｘがある領域を超えるとｙが変化する。このような変化を生む領域の境界を超平面と呼ぶ。
【０００６】
この超平面は、ｎ個の入力値x_i（ｉ＝１，２，．．．，ｎ）に対する出力値y_iが与えられると、パターン学習により生成することができる。パターン学習の際、出力値ｙの異なる入力値間の距離をマージンと呼ぶ。
【０００７】
パターン学習手段２１３にて得られる知識情報とは、この障害を検出し分類するための閾値であり、異常度の組み合わせからなる特徴空間においては、複数のクラスを分類する超平面となる。
【０００８】
【特許文献１】特許第３５８１９３４号公報
【非特許文献１】JING WU, JIAN-GUO ZHOU, PU-LIUYAN, MING WU、「A STUDY ON NETWORK FAULT KNOWLEDGE ACQUISITION BASED ON SUPPORTVECTOR MACHINE」、Proceedings of the Fourth International Conference on MachineLearning and Cybernetics, Guangzhou, 18-21 August 2005
【非特許文献２】麻生英樹，津田宏治，村田昇,「パターン認識と学習の統計学」、岩波書店,pp.107-123，2005
【発明の開示】
【発明が解決しようとする課題】
【０００９】
特許文献１に記載の構成を有する従来の障害分析システムはつぎのように動作する。
【００１０】
異常呼量監視手段１０１が、監視対象装置から異常の発生を示すログの有無を監視し、

存在する場合は異常の種別に応じて、時間当たりのトラフィック量である呼量をカウントする。閾値判定手段１１５は、一定時間内の呼量が所定の閾値以上になると、判定結果表示手段１１６を通じて、保守運用者にその異常を障害として通知する。

【００１１】

このような動作により、この従来の障害分析システムでは、自動で障害を検出することができる。

【００１２】

また、非特許文献１に記載の構成を有する従来の障害分析システムはつぎのように動作する。

【００１３】

すなわち、監視対象装置２３１～２３４に対する監視結果から、装置や回線単位の故障の可能性を表す指標である異常度を収集する。

【００１４】

異常度の例は、図３の３０１～３１３のように、リンクが落ちているか否か、エラー率、輻輳率、棄却率、利用率といった値である。

【００１５】

得られた異常度の組み合わせを、パターン判定手段２１５は知識格納部２１４に格納された知識情報を用いて、監視対象システム２３０において障害が発生したか否か判定し、判定結果表示手段２１６を通して、判定結果を保守運用者に提示する。

【００１６】

知識格納部２１４に格納される知識情報は、以下の手順で生成される。

【００１７】

まず、保守運用者が障害事例登録手段２１１を用いて、過去の障害事例を事例格納部２１２に登録する。

【００１８】

パターン学習手段２１３は、事例格納部２１２に格納されている障害事例と、異常度格納部２１０に格納された異常度の組み合わせとから知識情報を生成し、知識格納部２１４に格納する。ここで、障害事例とは、いつどこでどのような障害が発生したかを表す情報である。

【００１９】

前記判定結果表示手段２１６が保守運用者に対して示した障害判定結果が、実際には障害ではなかった場合には、判定修正入力手段２１７を用いて、事例格納部２１２に入力される。

【００２０】

このような動作により、この従来の障害分析システムでは、前記従来の障害分析システムとは異なり、障害検出および分類のための閾値を設定することなく、障害を検出することができる。

【００２１】

しかしながら、上述の従来例では、障害の影響が異常度を示す変数には表れず、例えば装置間通信における所定の期間にデータを送信した回数といった異常度を示す変数ではない変数に表れるような障害は、保守運用者が障害事例を登録しても、障害の検出やその障害の分類ができない、あるいは検出の精度が悪い。

【００２２】

本発明は上記課題を鑑みてなされたものであって、その目的の１つは、障害による影響が異常度を示す変数に表れず、異常度を示す変数ではない変数に表れるような障害も検出でき、または分類できる障害分析システムを提供することにある。

【課題を解決するための手段】

【００２３】

本発明による情報処理装置の好ましい一態様は、監視対象装置の異常度を示す複数の指標値を含むシステム情報を前記システム情報の識別情報とともに順次出力する監視対象装

置から、前記システム情報および前記システム情報の識別情報を順次受信するシステム情報受信手段と、前記システム情報受信手段が受信した前記各システム情報を所定の判定基準と比較し、比較の結果に基づいて前記各システム情報を種別毎に分類する種別判定手段と、前記各システム情報の識別情報と、前記各システム情報が分類された各種別を示す情報と、を対応付けて出力する判定結果出力部と、前記各システム情報の識別情報についてそれぞれ真の種別を示す情報の入力を受ける障害事例登録手段と、前記各システム情報の識別情報を前記真の種別と対応付けて記憶する事例格納部と、前記システム情報受信手段が受信した各システム情報と、前記各システム情報の識別情報に対応付けて記憶されている真の種別を示す情報と、に基づいて前記判定基準を更新するパターン学習手段と、を備え、前記種別判定手段は、前記各システム情報に前記監視対象装置の異常度とは関係のない指標値を含めて前記判定基準と比較することにより、前記各システム情報を種別毎に分類する。

【００２４】

本発明による情報処理装置の制御方法の好ましい一態様は、前記情報処理装置が、監視対象装置の異常度を示す複数の指標値を含むシステム情報を前記システム情報の識別情報とともに順次出力する監視対象装置から、前記システム情報および前記システム情報の識別情報を順次受信し、前記情報処理装置が、受信した前記各システム情報を所定の判定基準と比較し、比較の結果に基づいて前記各システム情報を種別毎に分類し、前記情報処理装置が、前記各システム情報の識別情報と、前記各システム情報が分類された各種別を示す情報と、を対応付けて出力し、前記情報処理装置が、前記各システム情報の識別情報についてそれぞれ真の種別を示す情報の入力を受け、前記情報処理装置が、前記各システム情報の識別情報を前記真の種別と対応付けて記憶し、前記情報処理装置が、受信した各システム情報と、前記各システム情報の識別情報に対応付けて記憶されている真の種別を示す情報と、に基づいて前記判定基準を更新し、前記情報処理装置が、前記各システム情報に前記監視対象装置の異常度とは関係のない指標値を含めて前記判定基準と比較することにより、前記各システム情報を種別毎に分類する。

【００２５】

本発明による情報処理装置の制御プログラムの好ましい一態様は、前記情報処理装置に、監視対象装置の異常度を示す複数の指標値を含むシステム情報を前記システム情報の識別情報とともに順次出力する監視対象装置から、前記システム情報および前記システム情報の識別情報を順次受信する処理と、受信した前記各システム情報を所定の判定基準と比較し、比較の結果に基づいて前記各システム情報を種別毎に分類する処理と、前記各システム情報の識別情報と、前記各システム情報が分類された各種別を示す情報と、を対応付けて出力する処理と、前記各システム情報の識別情報についてそれぞれ真の種別を示す情報の入力を受ける処理と、前記各システム情報の識別情報を前記真の種別と対応付けて記憶する処理と、受信した各システム情報と、前記各システム情報の識別情報に対応付けて記憶されている真の種別を示す情報と、に基づいて前記判定基準を更新する処理と、前記各システム情報に前記監視対象装置の異常度とは関係のない指標値を含めて前記判定基準と比較することにより、前記各システム情報を種別毎に分類する処理と、を実行させる。

【発明の効果】

【００２６】

本発明の効果は、障害の影響が異常度を示す変数には表れず、異常度を示す変数ではない変数に表れるような障害も検出しその障害を分類できる障害分析システムを提供できることにある。

【発明を実施するための最良の形態】

【００２７】

次に、発明を実施するための最良の形態について図面を参照して詳細に説明する。

【００２８】

図４を参照すると、本発明の第１の実施の形態は、監視対象装置４３１～４３４を備えるシステム４３０と通信可能に接続されている、プログラム制御により動作するコンピュ

ータ（中央処理装置とプロセッサとデータ処理装置とを少なくとも備える）４００である。

【００２９】

コンピュータ４００は、障害事例登録手段４１１と、事例格納部４１２と、システム状況取得手段４０１と、状況格納部４１０と、パターン学習手段４１３と、知識格納部４１４と、パターン判定手段４１５と、判定結果表示手段４１６と、判定修正入力手段４１７を含む。

【００３０】

障害事例登録手段４１１は事例格納部４１２と接続し、事例格納部４１２は障害事例登録手段４１１とパターン学習手段４１３とそれぞれ接続し、パターン学習手段４１３は状況格納部４１０と知識格納部４１４とそれぞれ接続し、状況格納部４１０はパターン学習手段４１３とシステム状況取得手段４０１とそれぞれ接続し、知識格納部４１４は、パターン学習手段４１３とパターン判定部４１５とそれぞれ接続し、システム状況取得手段４０１は、状況格納部４１０とパターン判定手段４１４とそれぞれ接続し、パターン判定手段４１５は、知識格納部４１４とシステム状況取得手段４０１と判定結果表示手段４１６とそれぞれ接続し、判定結果表示手段４１６はパターン判定手段４１５と接続している。

【００３１】

本明細書において、知識情報、閾値、境界面および超平面は同一のものを指し、特許請求の範囲に記載の判定基準に相当する。また本明細書では、特徴は特許請求の範囲に記載の指標値に相当する。

【００３２】

これらの手段はそれぞれ概略つぎのように動作する。

【００３３】

障害事例登録手段４１１は、保守運用者（特許請求の範囲に記載のオペレータに相当する）が使用する図示しない端末から、障害発生時間と場所との入力を受け付ける。この障害発生時間と場所との組を事例と呼ぶ。

【００３４】

事例とは、前記の障害発生時間と場所とが、あるいは正常であった時間と場所とが、対応付けられている情報である。ここで、事例として記憶されている時間と場所とはともに、期間や範囲のように広がりを持っていても良い。また、事例には実際に障害であった場合の事例を示す障害事例と実際には正常であった場合の事例を示す正常事例とがある。障害事例には障害発生時間と場所とが、正常事例には正常であった時間と場所とが含まれている。また、事例には事例の種類（クラス、パターンに相当する。また、特許請求の範囲に記載の真の種別に相当する）が含まれていてもよい。事例の種類とは、当該事例が正常であることを示す情報または障害の種類を含む情報である。この場合、障害事例には障害発生時間と場所と障害の種類とが、正常事例には正常であった時間と場所と当該事例が正常であることを示す情報とが、含まれている。あるいは、事例の種類は、事例とは独立した情報として構成されていてもよい。本明細書では事例に、事例の種類を含まないものとして考える。もちろん、事例に事例の種類を含んでいてもよい。

【００３５】

障害事例登録手段４１１は、事例とともに、当該事例の種類の入力を受け付けてもよい。場所とは、各監視対象装置を識別する識別子であってもよいし、回線名、住所などのように障害発生の箇所を特定できるものであればよい。障害発生時間と場所とは特許請求の範囲に記載のシステム情報（状況情報）の識別情報に含まれるものである。また本明細書では、システム情報の識別情報は事例に相当する。

【００３６】

なお、システム情報の識別情報はシステム情報が識別できる情報を含んでいればよく、一意に付される識別子などを含んでいればよい。

【００３７】

事例格納部４１２は、障害事例登録手段４１１または後述の判定修正入力手段４１７か

ら事例を受け取り、受け取った事例を図１６のように格納する。図１６を参照すると、事例番号と時刻と場所とパターンとを対応付けて記憶している。事例番号、時刻および場所はシステム情報の識別情報であり、パターンは事例の種類である。なお、事例番号、時刻、場所はそれぞれ必須ではなく、システム情報を識別できる情報が少なくとも１つあればよい。

【００３８】

システム状況取得手段４０１（特許請求の範囲の記載のシステム情報受信部に相当する）は、監視対象システム４３０における監視対象装置４３１～４３４から当該監視対象装置におけるシステム情報（状況情報）を取得する。このシステム情報には、異常度だけではなく、当該監視対象装置における状況情報も含む。システム状況取得手段４０１は、取得したシステム情報を状況格納部４１０に格納する。

【００３９】

状況情報とは、異常度とは異なり、その値の大小が障害の可能性を表さない値である。例えば、装置が他の装置と所定の期間にデータを送信した回数は、その値が大きくても、故障の可能性を示すものではない。本明細書では、異常度は、特許請求の範囲に記載の監視対象装置の異常度を示す複数の指標値に相当する。また、状況情報は、監視対象装置の異常度とは関係のない指標値に相当する。また、異常度と状況情報とを含む情報（システム情報を呼ぶ）は特許請求の範囲に記載のシステム情報に相当する。

【００４０】

システム状況取得手段４０１は、取得したシステム情報を状況格納部４１０に格納する。パターン学習手段４１３がパターン学習を行う際に用いる特徴空間の基底となる特徴は、これらのシステム情報に含まれる。

【００４１】

また、このシステム状況取得手段４０１は、試行回数取得手段４０２、イベント数取得手段４０３、時刻取得手段４０４、曜日取得手段４０５、時間的状況推測値取得手段４０６、構成状況推測値取得手段４０７を備える。システム状況取得手段４０１は、試行回数取得手段４０２、イベント数取得手段４０３、時刻取得手段４０４、曜日取得手段４０５、時間的状況推測値取得手段４０６、構成状況推測値取得手段４０７に受け取ったシステム情報を渡す。試行回数取得手段４０２、イベント数取得手段４０３、時刻取得手段４０４、曜日取得手段４０５、時間的状況推測値取得手段４０６、構成状況推測値取得手段４０７は受け取ったシステム情報を基に各処理を行い、出力結果をパターン判定手段４１５に渡す。

【００４２】

試行回数取得手段４０２は、監視対象装置４３１～４３４が、当該監視対象装置に接続されるその他の装置に所定の期間にデータを送信した回数を示す送信回数情報を取得する。取得方法は、例えばシステム情報に含まれる送信回数情報を抽出することによって行ってもよい。そして、試行回数取得手段４０２は、取得した送信回数情報をパターン判定手段４１５に渡す。

【００４３】

イベント数取得手段４０３は、監視対象装置４３１～４３４において発生した所定の期間のイベント数を取得する。例えば、当該監視対象装置における所定の期間の起動回数などである。取得方法は、例えばシステム情報に含まれる前述の起動回数などを示す情報を抽出することによって行ってもよい。そして、試行回数取得手段４０２は、取得したイベント数を示す情報をパターン判定手段４１５に渡す。

【００４４】

時刻取得手段４０４は、その事例が発生した時刻、あるいは監視を行った時刻を示す時刻情報を取得する。取得方法は、例えばシステム情報に含まれる時刻情報を抽出することによって行ってもよいし、時刻取得手段４０４が計測する現在の時刻を時刻情報として取得してもよい。そして時刻取得手段４０４は、取得した時刻情報をパターン判定手段４１５に渡す。

【００４５】
曜日取得手段４０５は、その事例が発生した曜日、あるいは監視を行った曜日を示す曜日情報を取得する。取得方法は、例えばシステム情報に含まれる曜日情報を抽出することによって行ってもよいし、曜日取得手段４０５が計測する現在の曜日を曜日情報として取得してもよい。そして曜日取得手段４０５は、取得した曜日情報をパターン判定手段４１５に渡す。
【００４６】
時間的状況推測値取得手段４０６は、図示しない時間的状況推測値算出手段を含む。時間的状況推測値算出手段は各監視対象装置が過去に送信し、後述の状況格納部４１０に記憶されているシステム情報に基づいて現在の当該監視対象装置のシステム情報の予測値を算出する。そして、時間的状況推測値取得手段４０６は、算出したシステム情報の予測値をパターン判定部４１５に渡す。
【００４７】
例えば、過去数日の同時刻の平均値を用いることで、その監視対象装置の状況またはコンテキストを含んだ情報を取得することができる。
【００４８】
構成状況推測値取得手段４０７は、図示しない構成状況推測値算出手段を含む。構成状況推測値算出手段は当該監視対象装置のシステム情報とあるほかの監視対象装置のシステム情報との関係を求め、当該ほかの監視対象装置の現在のシステム情報を用いて、当該監視対象装置のシステム情報を算出する。例えば、監視対象装置４３１の観測値ａと監視対象装置４３２の観測値ｂとの間にｂ＝２ａの関係が定常的に成り立っているときに、監視対象装置４３１の値ａから推測される監視対象装置４３２の値２ａが、ここで取得される。ｂ＝２ａの関係は後述の状況格納部４１０に記憶されている過去の当該監視対象装置のシステム情報および当該ほかの監視対象装置の現在のシステム情報から算出する。例えば、当該監視対象装置と当該ほかの監視対象装置との間に定常的に成り立っている数式モデル（例えばＡＲＸモデル（autoregressive model with exogenous input））をもとに算出してもよい。そして、構成状況推測値取得手段４０７は、算出したシステム情報の予測値をパターン判定部４１５に渡す。
【００４９】
状況格納部４１０は、図１８に示すように、過去にシステム状況取得手段４０１が受信したシステム情報に含まれる異常度または状況情報を示す特徴と、時刻と、場所と値と、を対応付けて記憶している。また、例えば時間と場所で識別できるシステム情報を返すことができるように格納してもよい。
【００５０】
パターン学習手段４１３（特許請求の範囲に記載のパターン学習部に相当する）は、保守運用者から障害事例登録手段４１１あるいは判定修正入力手段４１７に対して入力があったタイミングで、あるいは定期的に、事例格納部４１２に格納された各事例に対応付けられているシステム情報を状況格納部４１０から読み出す。読み出された各システム情報に含まれる各特徴でパターン学習手段４１３が用いる特徴空間を構成している。
【００５１】
すなわち、事例を基に読み出されるシステム情報に含まれる異常度または状況情報は、この特徴空間における特徴ベクトルを表している。
【００５２】
図１７は、パターン学習手段４１３内にて格納するデータ構造を示す図である。図１７において、１９０１および１９０２は異常度に関するものであり、１９０３～１９０９はシステム情報に関するものである。
【００５３】
また、パターン学習手段４１３は、読み出されたシステム情報を基に障害を検出し分類するための閾値（超平面）を生成し、知識格納部４１４に格納する。
【００５４】

知識格納部４１４は、パターン学習手段４１３によって生成された閾値を格納する。

【００５５】

パターン判定手段４１５（特許請求の範囲に記載の種別判定手段に相当する）は、システム状況取得手段４０１からシステム情報を受信する。そしてパターン判定手段４１５は、知識格納部４１４に格納された閾値を読み出して、受信したシステム情報が、障害であるか、あるいは正常であるかを示しているかを判定する。さらに障害であると判定された場合はどのような障害であるかを判定し、システム情報の識別情報と判定結果とを判定結果表示手段４１６に渡す。

【００５６】

判定結果表示手段４１６（特許請求の範囲に記載の判定結果出力部に相当する）は、前記パターン判定手段４１５から受け取った判定結果（パターン、事例の種類、特許請求の範囲に記載の種別に相当する）とシステム情報の識別情報（事例）とを保守運用者に対して表示する。

【００５７】

判定修正入力手段４１７は、前記判定結果表示手段４１６が保守運用者に対して提示した判定結果（パターン、事例の種類、特許請求の範囲に記載の種別に相当する）が間違いであった場合に、保守運用者が正しいと考える事例の種類（特許請求の範囲に記載の真の種別に相当する）と事例とを事例格納部４１２に登録する。例えば、時間と場所（事例）に加え、事例の種類（真の種別）などを、事例格納部４１２に追加する、あるいは事例格納部４１２に格納されている事例を保守運用者が正しいと考える事例に修正してもよい。

【００５８】

次に、図５、図６及び図７のフローチャートを参照して本実施の形態の全体の動作について詳細に説明する。

【００５９】

まず、システム状況取得手段４０１が監視対象システム４３０からシステム情報（異常度および状況情報を含む情報）を取得し、取得したシステム情報をパターン判定手段４１５に渡す（図５の５０１）。

【００６０】

パターン判定手段４１５が知識格納部４１４に含まれる閾値（超平面）を用いて、前記システム状況取得手段から受け取ったシステム情報から、監視対象システム４３０における事例の種類を判定し、判定結果（事例の種類、種別）と当該システム情報の識別情報（事例）とを判定結果表示手段４１６に渡す（図５の５０２）。

【００６１】

次に、図５の５０２においてパターン判定手段４１５が障害であると判定した場合には、判定結果表示手段４１６は、パターン判定手段４１５から受け取った判定されたパターン（種別）とシステム情報の識別情報（事例）とを保守運用者に表示する。（図５の５０３）。

【００６２】

次に、保守運用者は、障害事例登録手段４１１、あるいは判定修正手段４１７に対して、事例および真の種別として障害発生時間または正常である時間、場所、事例の種類を入力する。障害事例登録手段４１１、あるいは判定修正手段４１７は入力された事例を事例格納部４１２に格納する（図６の６０１）。

【００６３】

次にパターン学習手段４１３は、パターン学習により障害判定を行うための閾値を生成する（図６の６０２）。このステップは、別途保守運用者からの指示により実行されても良い。

【００６４】

事例から障害判定を行うための閾値を生成するために、パターン学習手段４１３は、事例格納部４１２に含まれる全ての事例について、状況格納部４１０から当該事例に含まれる時間または場所に対応付けられているシステム情報を取得する（図７の７０１、７０２

）。パターン学習手段４１３は、事例格納部４１２から得られた各事例に対応付けられている各システム情報に含まれる異常度および状況情報から構成される特徴ベクトルを用いて、各システム情報について、各システム情報の事例の種類というパターンに分類するための超平面を学習し（図７の７０３）超平面を生成する。

【００６５】

パターン学習部４１３は学習し生成した超平面を知識格納部４１４に格納し、前記パターン判定手段４１５は、知識格納部４１４に格納された超平面を用いてシステム状況取得手段４０１から受け取った各システム情報についてパターンを分類する（図７の７０４）。

【００６６】

次に、本実施の形態の効果について説明する。

【００６７】

本実施の形態では、監視対象装置に関する状況情報を含むシステム情報を取得し、これをパターン学習手段における特徴空間に含めるように構成されているため、保守運用者が事例の種類と事例とを登録した場合に、より精度の良い障害検出および分類を自動で行うことができる。その理由は、異常度を示す変数ではない変数も特徴空間に含めることで、特徴空間において、従来は分類できなかった、障害事例と正常事例とを分類する超平面が生成できる、あるいは生成される超平面が持つマージンが大きくなるためである。

【００６８】

また、本実施の形態では、障害の影響が異常度としては表れるものの、他の異なる種類の障害も同じ異常度として表れるようなシステムにおいても、保守運用者が障害事例を登録して異なる障害として検出できる。その理由は、試行回数といった変数も特徴空間に含めることで、異なる障害を分類するような超平面を特徴空間に生成できる、あるいは生成できる超平面のマージンが大きくなるためである。

【００６９】

また、本実施の形態では、ユーザがシステムを利用する回数が変化するようなシステムの障害を分析し、さらに特徴空間には、システムの異常度を示す変数に呼損率や失敗率などが含まれている場合、システムの利用回数が少ない時間帯でも、障害検出の精度を高くできる。その理由は、試行回数を特徴空間に含めることで、試行回数が少なく、かつ失敗率が高い空間と、試行回数が多く、かつ失敗率の低い空間とを分離する超平面を生成することができる点にある。

【００７０】

また、本実施の形態では、単一の監視対象装置の異常度だけでは根本的な障害を発見できず、複数の監視対象装置が影響しあうようなシステムにおいても、保守運用者が障害事例を登録して、障害検出の精度を高くすることができる。その理由は、当該監視対象装置の構成状況から推測される値を特徴空間に含めることで、定常的に監視対象装置間で成り立っていた関係が崩れた上で、当該監視対象装置のみが異常度が上昇していることを示す空間と、その関係を保ちながら、他の監視対象装置も共に異常度が上昇していることを示す空間とを分類するような超平面を、特徴空間に生成できる、あるいは生成できる超平面のマージンが大きくなるためである。

【実施例】

【００７１】

次に、具体的な実施例を用いて本発明を実施するための第１の最良の形態の動作を説明する。

【００７２】

図８に示すように、監視対象システム４３０には、監視対象装置１００１が存在し、他の装置１００２との接続において、監視対象装置１００１からの接続要求の単位時間あたりの試行回数が、１０１１に示されるような変化であり、その試行の呼損率が１０１２に示されるような変化であるとする。

【００７３】

この時系列データは、ある時刻において障害が発生しているものとするが１０１２に示すように、呼損率には表れていない。試行回数の低下となって表れているが、試行回数の多寡自体は障害とは言えない。

【００７４】

ここで、保守運用者が障害事例登録手段４１１を用いて、図８の障害期間を障害事例として登録し、それ以外の正常である期間を正常事例として登録したとすると、システム状況取得手段４０１における試行回数取得手段４０２が存在しなく、試行回数を特徴空間に含めない場合は、図９に示すように、正常事例１１０１も、障害事例１１０２も特徴空間において近傍の領域に分布するため、それらを分離する超平面の生成は困難である、あるいは精度の低い境界面しか生成できない。

【００７５】

それに対して、特徴空間に試行回数１１１３も含めた場合は、正常事例と障害事例とを分離する超平面１１１５を生成することができる。

【００７６】

ただし、ここで深夜時間帯など本来正常な時間帯にも、試行回数１１１３が低くなるため、正常事例１１１６のような障害事例に紛れ込んでしまうことがある。これはすなわち、深夜時間帯になると障害として検知してしまうことと対応する。

【００７７】

このため別の特徴として、試行回数１１１７以外に時間帯１１１８を特徴空間に含めても良い。このようにすることで、深夜時間帯に試行回数が少なくなっている事例と、昼間に試行回数が少なくなっている事例を高精度に分離する超平面を生成することができる。

【００７８】

あるいは、試行回数１１１９以外に、この試行回数の時間的状況推測値１０１３（１１２０）を用いても良い。

【００７９】

これにより、過去の正常な期間の監視対象のデータから推測される現在の試行回数が大きいときに、試行回数が小さいと障害であると判定するようになり、逆に推測される現在の試行回数が小さい時に、試行回数が小さいときには、正常であると判定されるようになる。

【００８０】

次に、具体的な実施例を用いて本発明を実施するための第２の最良の形態の動作を説明する。

【００８１】

図１０に示すように、監視対象システム４３０には、監視対象装置１２０１が存在し、他の装置１２０２との接続において、接続要求が失敗した際に再送されるような状態での障害と、再送されないような状態での障害とがあるとする。

【００８２】

前者の障害では試行１２１１～１２１３のように、一定回数の試行を繰り返すため、単位時間あたりの試行回数の時間変化１２０４は上昇し、単位時間あたりの呼損率１２０３も上昇する。

【００８３】

これに対して、監視対象装置１２３１と他の装置１２３２との接続で、後者の障害では試行１２４１で失敗すると再試行が行われないため、試行回数の時間変化１２３４は変わらず、呼損率１２３３のみが劣化する。

【００８４】

ここで、保守運用者が障害事例登録手段４１１を用いて、図１０の障害期間を障害事例として登録し、それ以外の正常である期間を正常事例として登録したとすると、システム状況取得手段４０１における試行回数取得手段４０２が存在しなく、試行回数を特徴空間に含めない場合は、図１１に示すように、障害パターン１の事例１３１１も、障害パターン２の事例１３１２も特徴空間において近傍の領域に分布するため、それらを分離する超

平面の生成は困難である、あるいは精度の低い超平面しか生成できない。
【００８５】
それに対して、特徴空間に試行回数１３２２も含めた場合は、障害パターン１の事例１３１１と障害パターン２の事例１３１２とを分離する超平面１３２３を生成することができる。
【００８６】
次に、具体的な実施例を用いて本発明を実施するための第３の最良の形態の動作を説明する。
【００８７】
図１２に示すように、監視対象システム４３０には、監視対象装置１４０１が存在し、他の装置１４０２との接続において、単位時間あたりの試行回数の時間変化１４０３に対して、単位時間あたりの呼損率１４０４があるとする。
【００８８】
ここで、保守運用者が事例登録手段４１１を用いて、障害事例と、図１２の期間を正常事例として登録したとすると、システム状況取得手段における試行回数取得手段４０２が存在しなく、試行回数を特徴空間に含めない場合は、図１３に示すように、正常事例１５０４も障害と判定するような超平面が生成されてしまうが、特徴空間に試行回数１５１２も含めた場合は、試行回数が少ないときに呼が落ちて呼損率が高くなるような事例１５１４と、実際の障害である事例との間に、両者を分離しやすい超平面を生成することができる。
【００８９】
次に、具体的な実施例を用いて本発明を実施するための第４の最良の形態の動作を説明する。
【００９０】
図１４に示すように、監視対象システム４３０には、監視対象装置としてＡｐｐサーバ１６０１が存在し、その異常度としてＣＰＵ利用率が監視により取得され、また別の監視対象装置としてＷｅｂサーバ１６０４が存在し、その異常度としてＣＰＵ利用率が監視により取得され、前者の時系列データとして１６０５が得られるとする。
【００９１】
また、ＷｅｂサーバとＡｐｐサーバの間には定常的な数理的な関係が成り立っており、Ｗｅｂサーバ１６０４から得られた値から推測されるＡｐｐサーバの値の時系列データとして１６０６が得られるとする。
【００９２】
ここで、保守運用者が障害事例登録手段４１１を用いて、図１４の１６０７の期間を障害事例として登録し、それ以外の期間のデータを正常事例として登録したとすると、システム状況取得手段における試行回数取得手段４０２が存在しなく、構成状況推測値を特徴空間に含めない場合は、図１５に示すように、当該装置の障害事例１７０４と正常事例１７０３とを分離するような超平面が生成されない、あるいは分類精度の低い超平面しか生成できないが、特徴空間に構成状況推測値も含めた場合は、関連する装置が正常であるにも関わらず、当該装置のみの異常度のみが高いことを表す空間と、当該装置も、他の関連する装置も共に異常度が高くなっていることを表す空間とを分離しやすい超平面を生成することができる。
【産業上の利用可能性】
【００９３】
本発明によれば、コンピュータシステムやネットワークシステムを運用管理するといった用途に適用できる。
【図面の簡単な説明】
【００９４】
【図１】従来の第１の発明を示すブロック図である。
【図２】従来の第２の発明を示すブロック図である。

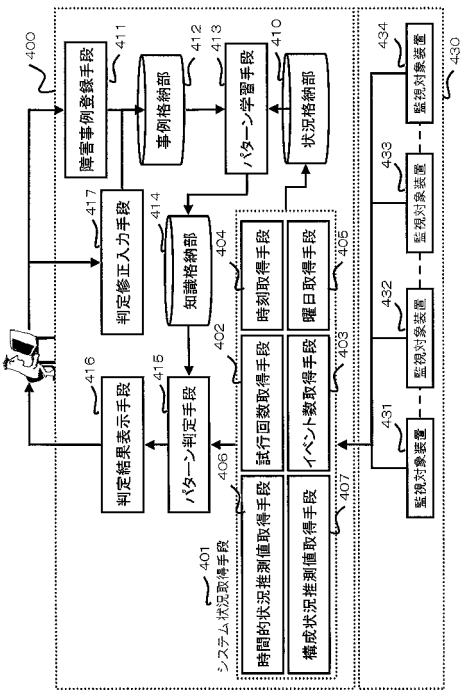
【図３】従来の第２の発明で用いられる特徴空間を示す表である。
【図４】本発明を実施するための最良の形態の構成を示すブロック図である。
【図５】本発明を実施するための最良の形態の動作を示す流れ図である。
【図６】本発明を実施するための最良の形態の動作を示す流れ図である。
【図７】本発明を実施するための最良の形態の動作を示す流れ図である。
【図８】本発明を実施するための最良の形態の動作の具体例を示す監視対象の構成図である。
【図９】本発明を実施するための最良の形態の動作の具体例を示す特徴空間である。
【図１０】本発明を実施するための最良の形態の動作の具体例を示す監視対象の構成図である。
【図１１】本発明を実施するための最良の形態の動作の具体例を示す特徴空間である。
【図１２】本発明を実施するための最良の形態の動作の具体例を示す監視対象の構成図である。
【図１３】本発明を実施するための最良の形態の動作の具体例を示す特徴空間である。
【図１４】本発明を実施するための最良の形態の動作の具体例を示す監視対象の構成図である。
【図１５】本発明を実施するための最良の形態の動作の具体例を示す特徴空間である。
【図１６】事例格納部４１２に格納するデータ構造を示す図である。
【図１７】パターン学習手段４１３内にて格納するデータ構造を示す図である。
【図１８】状況格納部４１０に格納するデータ構造を示す図である。
【符号の説明】
【００９５】
１００、２００、４００　コンピュータ
４０１　システム状況取得手段
４０２　試行回数取得手段
４０３　イベント数取得手段
４０４　時刻取得手段
４０５　曜日取得手段
４０６　時間的状況推測値取得手段
４０７　構成状況推測値取得手段
４１０　状況格納部
４１１　障害事例登録手段
４１２　事例格納部
４１３　パターン学習手段
４１４　知識格納部
４１５　パターン判定手段
４１６　判定結果表示手段
４１７　判定修正入力手段
４３１、４３２、４３３、４３４　監視対象装置

【図３】

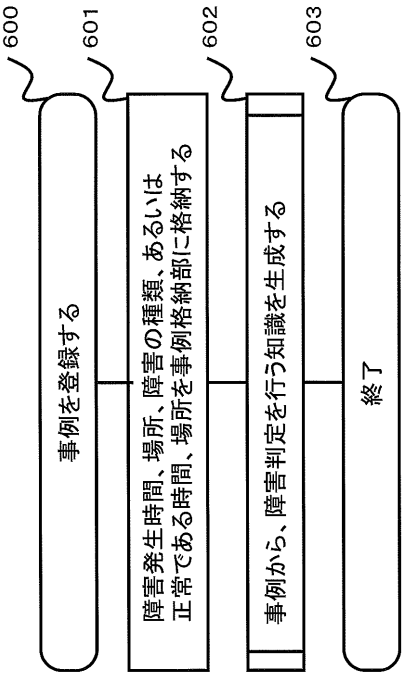
300

	異常度	値
301	インターフェース管理状態	1: up, 2: down
302	リンクプロトコル状態	1: up, 2: down
303	インターフェース稼動状態	1: up, 2: down
304	CRC エラー率	0-100%
305	輻輳率	0-100%
306	遅れ輻輳率	0-100%
307	入力パケット棄却率	0-100%
308	出力パケット棄却率	0-100%
309	総パケット棄却率	0-100%
310	入力キュー利用率	0-100%
311	出力キュー利用率	0-100%
312	平均入力インターフェース利用率	0-100%
313	平均出力インターフェース利用率	0-100%

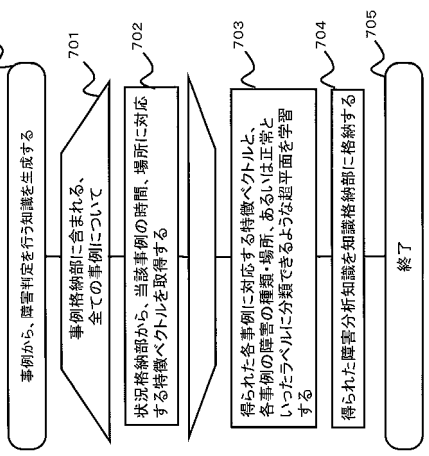
【図４】



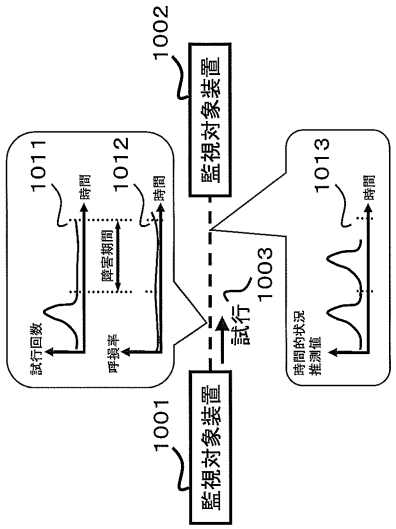
【図６】



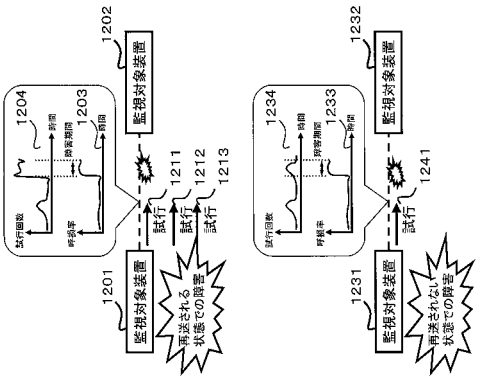
【図７】



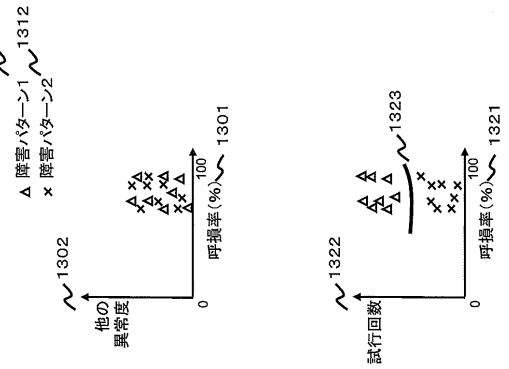
【図８】



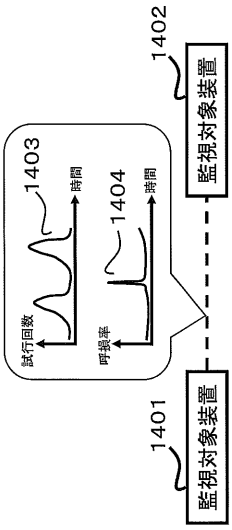
【図１０】



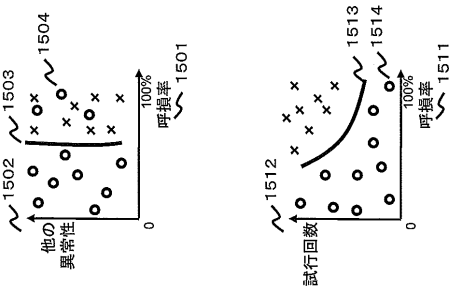
【図１１】



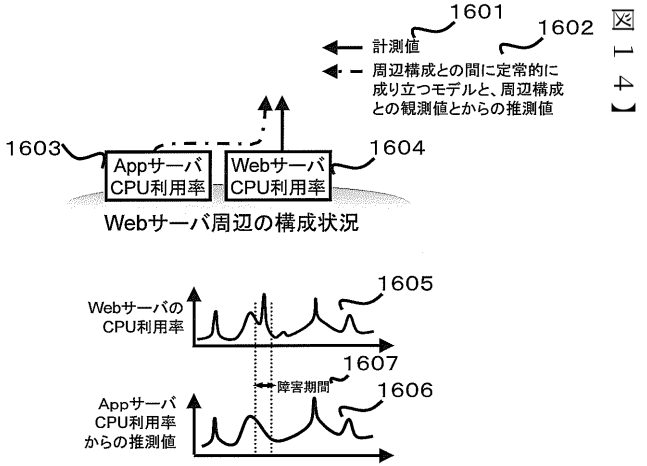
【図１２】



【図１３】



【図１４】



【図１５】

• 事例格納部412のテーブル　1800

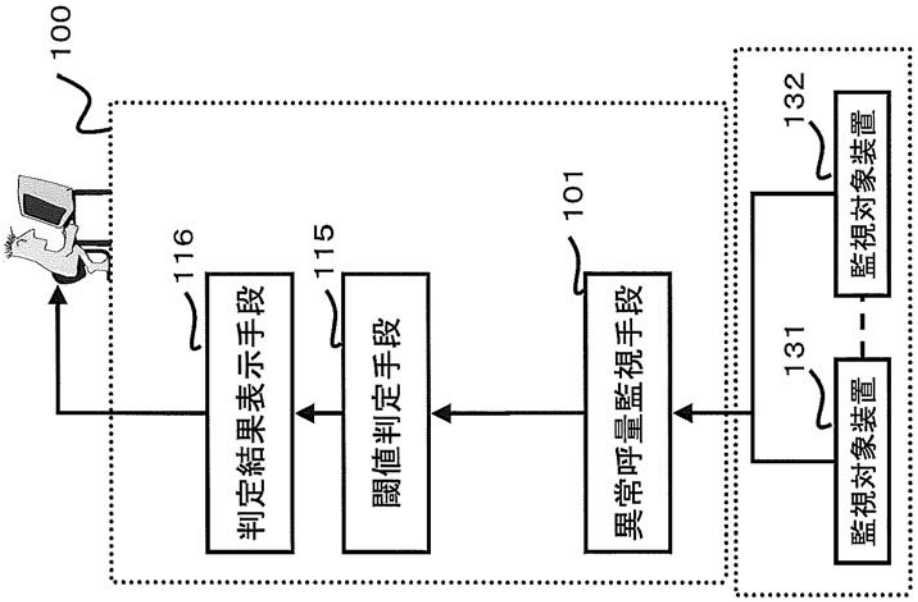
事例番号	時刻	場所	パターン	
1	08/01/11 08:22:16	監視対象装置431	障害1	1802
2	08/01/16 09:49:23	監視対象装置433	障害1	1801
3	08/01/17 20:17:37	通信網{監視対象装置431,監視対象装置432}	障害2	1803
4	08/01/21 13:32:41	監視対象装置433	障害1	1804
5	08/01/24 17:51:16	監視対象装置431	正常	1805
6	08/02/02 19:46:27	監視対象装置432	障害3	1806

【図１８】

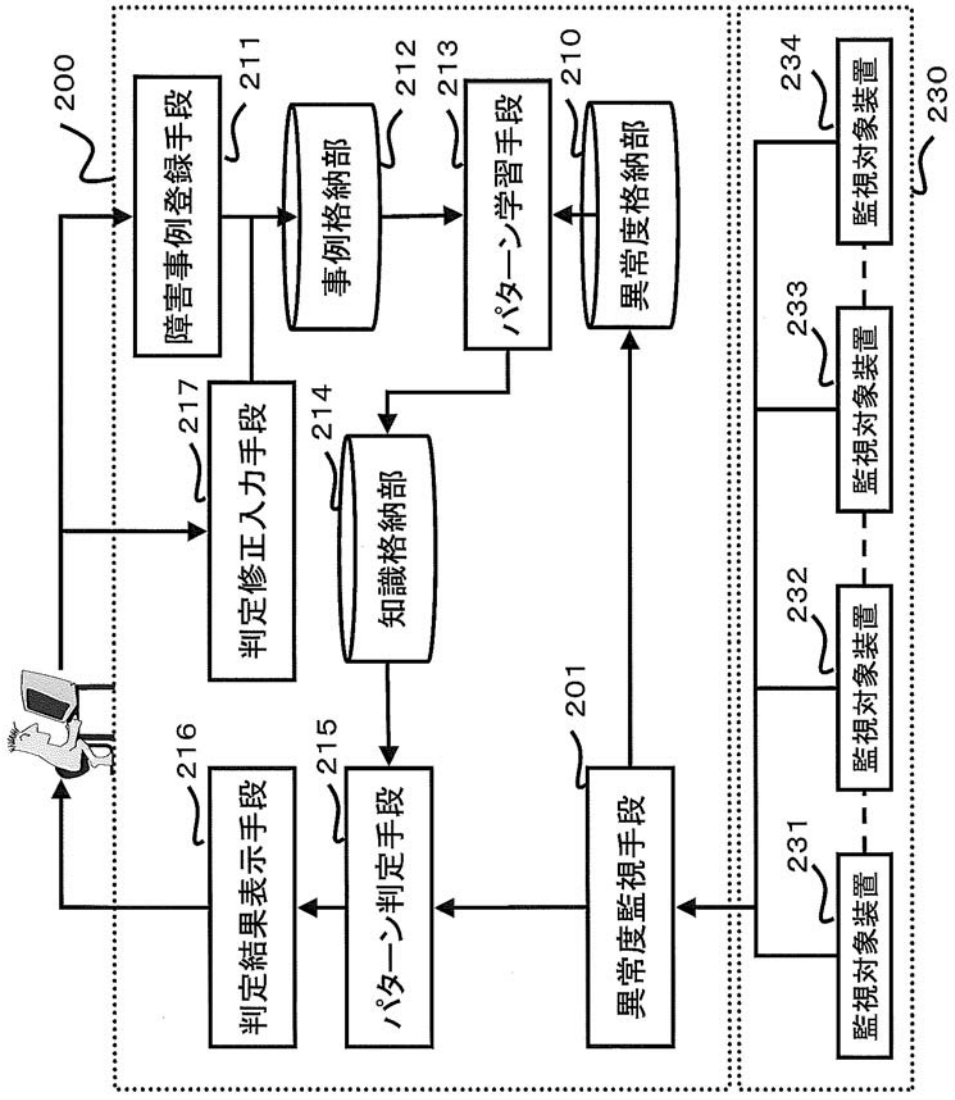
状況格納部410に格納されたテーブル　2000

特徴	時刻	場所	値	
通信Aの呼損率	08/01/11 08:15:00	監視対象装置431	1	2001
CPU利用率	08/01/11 08:15:00	監視対象装置431	60	2002
通信Aの試行回数	08/01/11 08:15:00	監視対象装置431	15	2003
通信Aの呼損率　の過去データからの推測値	08/01/11 08:15:00	監視対象装置431	0	2004
通信Aの呼損率　の隣接装置の現在値からの推測値	08/01/11 08:15:00	監視対象装置431	0	2005
CPU利用率　の過去データからの推測値	08/01/11 08:15:00	監視対象装置431	50	2006
CPU利用率　の隣接装置の現在値からの推測値	08/01/11 08:15:00	監視対象装置431	42	2007
通信Aの呼損率	08/01/11 08:15:00	監視対象装置432	3	2008
CPU利用率	08/01/11 08:15:00	監視対象装置432	70	2009
通信Aの試行回数	08/01/11 08:15:00	監視対象装置432	20	2010
通信Aの呼損率　の過去データからの推測値	08/01/11 08:15:00	監視対象装置432	8	2011
通信Aの呼損率　の隣接装置の現在値からの推測値	08/01/11 08:15:00	監視対象装置432	1	2012
CPU利用率　の過去データからの推測値	08/01/11 08:15:00	監視対象装置432	60	2013
CPU利用率　の隣接装置の現在値からの推測値	08/01/11 08:15:00	監視対象装置432	50	2014
...				2015
通信Aの呼損率	08/01/11 08:30:00	監視対象装置431	2	2016
CPU利用率	08/01/11 08:30:00	監視対象装置431	65	2017
通信Aの試行回数	08/01/11 08:30:00	監視対象装置431	25	2018
通信Aの呼損率　の過去データからの推測値	08/01/11 08:30:00	監視対象装置431	1	2019
通信Aの呼損率　の隣接装置の現在値からの推測値	08/01/11 08:30:00	監視対象装置431	1	2020
CPU利用率　の過去データからの推測値	08/01/11 08:30:00	監視対象装置431	55	2021
CPU利用率　の隣接装置の現在値からの推測値	08/01/11 08:30:00	監視対象装置431	45	2022

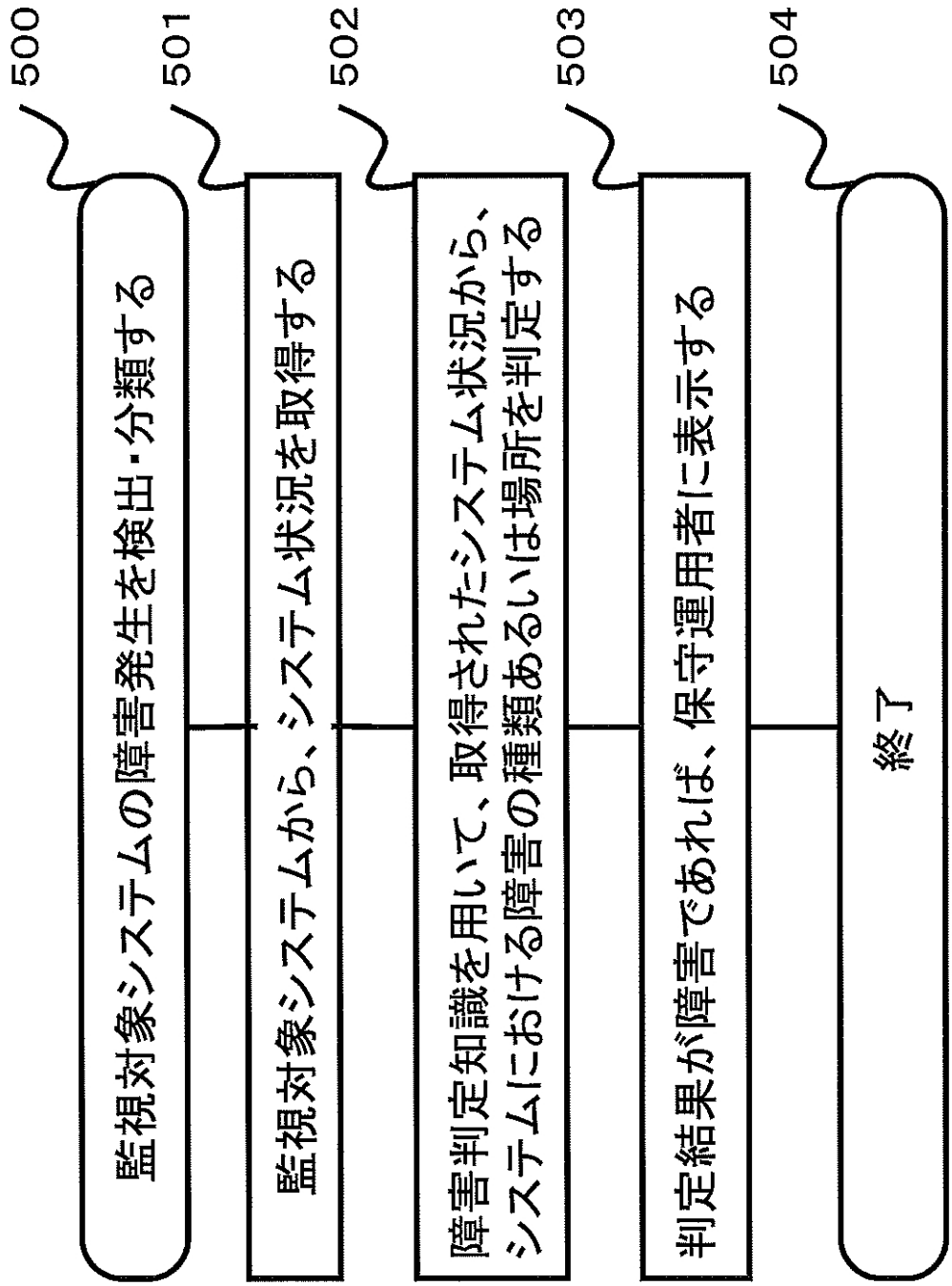
【図１】


100
116
判定結果表示手段
115
閾値判定手段
101
異常呼量監視手段
132
監視対象装置
131
監視対象装置

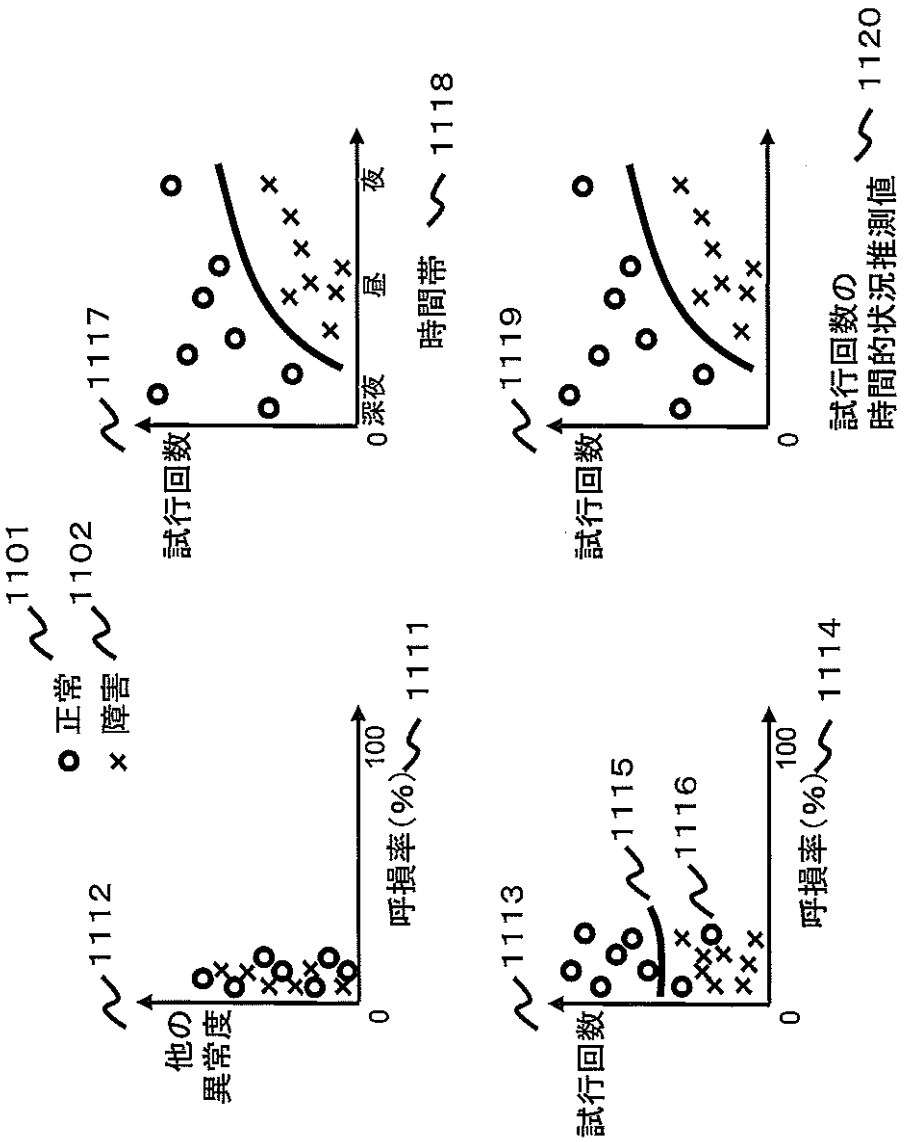
【図２】


200
障害事例登録手段
211
事例格納部
212
213
パターン学習手段
210
異常度格納部
234
監視対象装置
230
233
監視対象装置
217
判定修正入力手段
214
知識格納部
232
監視対象装置
201
216
判定結果表示手段
215
パターン判定手段
異常度監視手段
231
監視対象装置

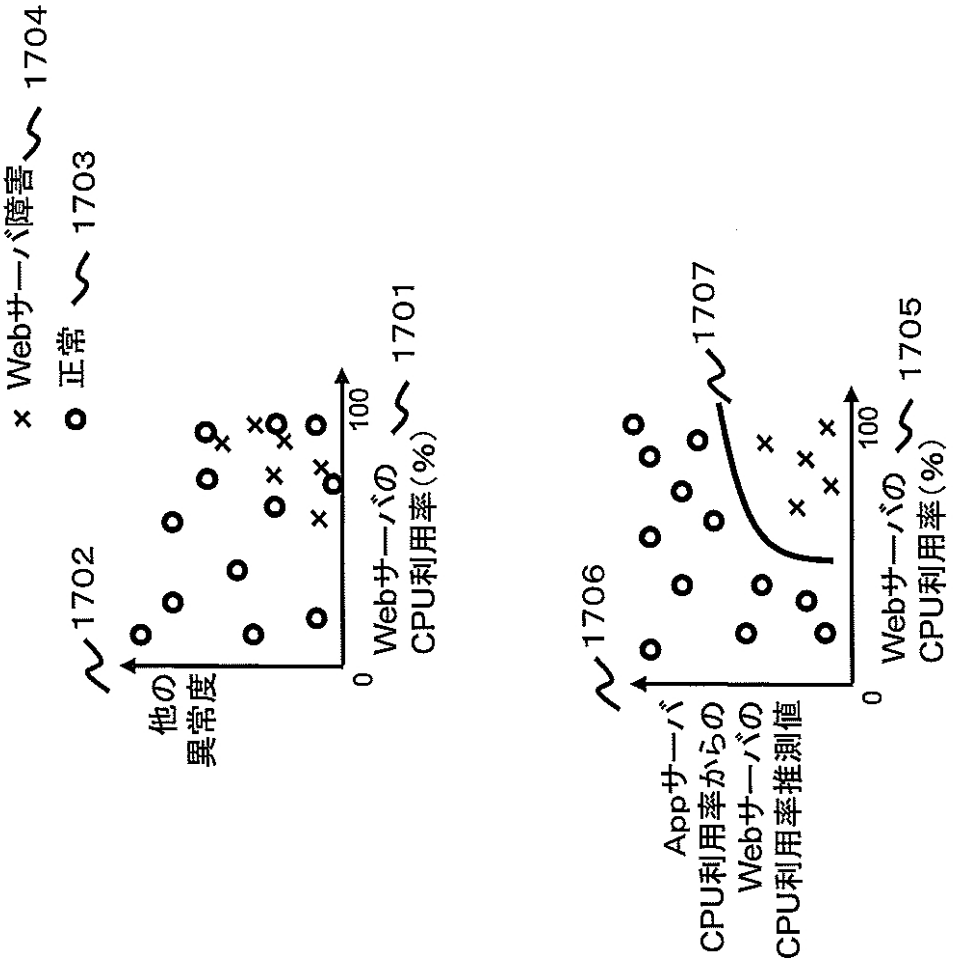
【図５】


500
監視対象システムの障害発生を検出・分類する
501
監視対象システムから、システム状況を取得する
502
障害判定知識を用いて、取得されたシステム状況から、システムにおける障害の種類あるいは場所を判定する
503
判定結果が障害であれば、保守運用者に表示する
504
終了

【図９】


1101
正常
1102
障害
1117
試行回数
深夜
昼
夜
時間帯
1118
1112
他の異常度
0
100
呼損率(%)
1111
1119
試行回数
0
試行回数の時間的状況推測値
1120
1113
試行回数
1115
1116
0
100
呼損率(%)
1114

【図１５】


× Webサーバ障害 1704
o 正常 1703
1702
他の異常度
0
100
Webサーバの CPU利用率(%) 1701
1706
Appサーバ CPU利用率からの Webサーバの CPU利用率推測値
1707
0
100
Webサーバの CPU利用率(%) 1705

【図１７】

パターン学習手段413に格納