(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5098821号
(P5098821)
(45)発行日　平成24年12月12日(2012.12.12)　(24)登録日　平成24年10月5日(2012.10.5)

(51)Int.Cl.　F I
G06F 13/00 (2006.01)　G06F 13/00　351N

請求項の数 5　(全 14 頁)

(21)出願番号　特願2008-144062(P2008-144062)
(22)出願日　平成20年6月2日(2008.6.2)
(65)公開番号　特開2009-289221(P2009-289221A)
(43)公開日　平成21年12月10日(2009.12.10)
審査請求日　平成23年2月17日(2011.2.17)

(73)特許権者　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(74)代理人　100094662
弁理士　穂坂　和雄
(74)代理人　100111822
弁理士　渡部　章彦
(74)代理人　100119161
弁理士　重久　啓子
(72)発明者　森山　晃一
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

最終頁に続く

(54)【発明の名称】監視対象システムの障害等の予兆を検出する監視装置及び監視方法

(57)【特許請求の範囲】
【請求項１】
大規模コンピュータシステムやネットワークシステム等の監視対象システムの障害等の予兆を検出する監視装置であって，
監視対象システムの性能を表す時系列データを一定周期で抽出して過去の時系列データとして格納する手段と，
前記時系列データが，各部の使用率，抽出間隔，異常値検出回数，知識データ選定条件，オフラインデータ選定条件を含む予め選定条件格納部に格納された選定条件に適合すると過去のメタデータとして前記時系列データと関連付けて過去のメタデータ格納手段に格納する第１のメタデータ化手段と，
監視対象システムからのリアルタイムの性能を表す時系列データについて上記選定条件とは別に設定された選定条件に適合するとリアルタイムのメタデータを生成する第２のメタデータ化手段と，
前記リアルタイムのメタデータと前記過去のメタデータ格納手段のメタデータとを照合し，前記照合において予め設定された所定の一致度が得られると当該メタデータに関連付けられた前記過去の時系列データを参照して設定された時系列データの今後の変化を検出して出力する照合予兆検出手段と，
を備えることを特徴とする監視対象システムの障害等の予兆を検出する監視装置。
【請求項２】
請求項１において，

前記照合予兆検出手段は，前記所定の一致度が得られたメタデータに関連付けられた前記過去の時系列データにおいて異常が発生するか判別して，異常が検出されると，異常に対する対処手順を前記関連付けられた過去のメタデータから読み出して保守端末に表示して対処を促すことを特徴とする監視対象システムの障害等の予兆を検出する監視装置。

【請求項３】

請求項１において，

前記照合予兆検出手段は，前記照合において予め設定された所定の一致度が複数の過去のメタデータについて得られると，該複数の過去のメタデータに関連付けられた各時系列データを参照して最も最近に発生した時系列データの今後の変化を検出して出力することを特徴とする監視対象システムの障害等の予兆を検出する監視装置。

【請求項４】

大規模コンピュータシステムやネットワークシステム等の監視対象システムの監視方法において，

前記監視対象システムの状態を表す時系列データの値や変化の特徴を，各部の使用率，抽出間隔，異常値検出回数，知識データ選定条件，オフラインデータ選定条件を含む選定条件として予め設定し，前記選定条件に従って監視対象の時系列データをメタデータ化して過去のメタデータとして過去の時系列データと関連付けて格納し，

前記監視対象システムのリアルタイムの状態を表す時系列データについて予め設定した値や変化の特徴を選定条件としてメタデータを生成し，

前記生成したリアルタイムのメタデータと前記過去のメタデータとを照合して，予め設定した程度の一致度が得られると当該過去のメタデータ及び関連付けられた過去の時系列データを参照して，その時点以降に発生したデータの変化やイベントを予兆として検出して出力する，

ことを特徴とする監視対象システムの障害等の予兆を検出する監視方法。

【請求項５】

請求項４において，

前記過去のメタデータとして，障害時における保守者が対応すべき操作内容を関連付けて保持し，障害の予兆が出力される時に前記保持された操作内容を出力することを特徴とする監視対象システムの障害等の予兆を検出する監視方法。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は大規模コンピュータシステムやネットワークシステム等の監視対象システムの障害等の予兆を検出する監視装置及び監視方法に関する。

【背景技術】

【０００２】

大規模コンピュータシステム，ネットワークシステムにおける障害対応や規制措置等の保守操作は，構成する各装置による異常状態検出時の通知や，保守者による状態監視での，経験に基づく状況判断により実施される方法が一般的に行われている。

【０００３】

これらのシステムの常時監視により，システムのサービス継続の阻害となる障害を検出し，保守操作を行うことは極めて重要であり，更に障害に至る以前にその予兆をできるだけ早く正確に検出し，障害の防止対策を迅速に行うことが求められている。

【０００４】

事前に異常を検知する技術として，過去に異常のあった日時を過去のトラヒックデータの蓄積結果より特定し，同様のトラヒックデータの変動が予見される日時に対して予め規制制御する技術がある（特許文献１参照）。しかし，この技術では時間帯などと因果関係のない突発的な異常について予期することはできない。

【０００５】

他の方法として，過去のネットワーク監視データを統計処理し，検出対象となる統計的

な振る舞いを定め，それに基づいて管理対象の情報を絞り込んで監視を行い，連続量情報の統計的な振る舞いを検出すると異常が発生する予兆を発見したとみなして，監視ルールを参照して監視情報収集部に対して関連する複数の監視情報を収集するよう指示し，監視情報判定部でその値を判定することにより障害の原因を特定する技術（特許文献２参照）があるが，この技術ではバースト的なトラヒック増減や障害によるリソース使用量の急増は検出が可能ではあるが，正常値の範囲内で発生するゆらぎ等の予兆として捕捉すべき傾向を検出することはできない。

【０００６】

具体的には，図９に示す監視対象のデータが推移するパターンの例について説明すると，時刻(t-z) ～時刻(t-z)+n のデータの推移があらわれた後，時刻ｔ＋１に異常が発生した場合，閾値や統計情報の検出手段によっては時刻(t-z) ～時刻(t-z)+n のデータの推移はｔｈ１で示す通常値の平均的な値（正常値）の範囲内とみなされて，異常の可能性を検出することはできない。異常を検出する閾値であるｔｈ２を超えないと異常を感知することができないため，時刻ｔ＋１になって異常を検出することになり平均的な値ｔｈ１の状態では時刻ｔ＋１に発生する異常の予兆として検出することができない。

【特許文献１】特開２００１－２８６２８号公報

【特許文献２】特開２００５－２８５０４０号公報

【発明の開示】

【発明が解決しようとする課題】

【０００７】

上記したように従来の特許文献１や特許文献２の方法では，トラフィックの異常や障害の発生を検出する手段としては有効であるが，それらの方法では図９に示すように異常判断の閾値の範囲内（正常動作と判断される範囲）で発生するゆらぎや発生するパターンに対して適用しても異常や障害を検出することができない。すなわち，従来は予め型が決められた予兆検出手段（閾値や平均値による検出）を用いているが，従来の各リソース（装置構成）毎に設定した閾値などによる検出手段では，設定する値が低ければ誤検知が発生し，高ければ検出した直後に障害に至ってしまうなど，適切な設定が難しいため，障害に至る予兆を的確に捉えることはできなかった。

【０００８】

一方，予兆に対する保守作業については，従来，保守者の経験やスキルに依存しており，正確で迅速な障害防止対策をすることは難しかった。

【０００９】

本発明は監視対象の時系列データの値が異常を表す閾値を超えることが無くても，大規模コンピュータシステムやネットワークシステム等の監視対象システムの障害等の予兆を検出する監視装置及び監視方法を提供することを目的とする。

【課題を解決するための手段】

【００１０】

この発明では単一点での異常値判定ではなく，時系列の監視データに対する値の変化の特徴をリアルタイムにデータ化し，その特徴点が過去に似たような推移があったかを検出することにより，異常を表す閾値に依存せずに予兆を検出するものである。

【００１１】

なお，以下の説明で選定条件（またはポリシールール）は，監視対象の時系列データの値の変化や，パターンの特徴を表すデータや，障害情報，オペレーション（保守者による運用操作），システムイベント（故障やアラーム等の発生）等が含まれ，この選定条件に含まれた特徴を表すデータに従ってメタデータが生成される。また，時系列データは，監視対象システムである大規模コンピュータシステムやネットワークシステムから一定周期で取得するトラヒックや状態（リソース使用量や性能情報等）に関する値を指し，例えば，ＣＰＵ使用率，ＤＩＳＫ入出力回数，空き容量，メモリ使用等のサーバの性能やリソースを判断できるデータや，回線使用率，パケット破棄率，エラーパケット数等のネットワーク性能等を判断するためのデータ等の定期的に取得できる時系列のデータを意味する。

また，メタデータは，監視対象システムから上記選定条件に従って生成したデータ及びシステムから発生したデータや，保守端末からの操作により発生したデータも含まれる。なお，システムから発生したデータは，障害情報，システムイベント（故障やアラーム等の発生）が含まれ，保守端点からの操作により発生したデータは，オペレーション（保守者による運用操作）が含まれる。

【００１２】

この大規模コンピュータシステムやネットワークシステム等の監視対象システムの障害等の予兆を検出する監視装置は，監視対象システムの性能を表す時系列データを一定周期で抽出して過去の時系列データとして格納する手段と，前記時系列データが，設定された数値や変化のパターンを表す特徴データや，障害発生等のイベントを含むトリガデータ等で構成する予め格納部に格納された選定条件に従って過去のメタデータを生成して過去の時系列データと関連付けて過去のメタデータ格納手段に格納する第１のメタデータ化手段を備える。一方，監視対象システムからのリアルタイムの状態を表す時系列データについて上記選定条件とは別に設定することができる選定条件に従ってリアルタイムのメタデータを生成する第２のメタデータ化手段を備える。そのリアルタイムのメタデータと過去のメタデータ格納手段のメタデータとを照合し，予め設定された所定の一致度が得られると当該メタデータに関連付けられた過去の時系列データを参照して設定された時系列データの今後の変化を照合予兆検出手段により検出して出力するよう構成する。

【００１３】

更に，上記の照合予兆検出手段は，所定の一致度が得られたメタデータに関連付けられた過去の時系列データにおいて異常が発生するか判別して，異常が検出されると，異常に対する対処手順を関連付けられた過去のメタデータから読み出して保守端末に表示して対処を促すように構成することができる。また，照合予兆検出手段は，照合において予め設定された所定の一致度が複数の過去のメタデータについて得られると，該複数の過去のメタデータに関連付けられた各時系列データを参照して最近に発生した時系列データの今後の変化を検出して出力するように構成することができる。

【００１４】

また，この監視装置の原理による監視対象システムの監視方法として，監視対象システムの状態を表す時系列データの値や変化の特徴を選定条件として予め設定し，前記選定条件に従って監視対象の時系列データをメタデータ化して過去のメタデータとして過去の時系列データと関連付けて格納し，監視対象システムのリアルタイムの状態を表す時系列データについて予め設定した値や変化の特徴を選定条件としてメタデータを生成し，生成したリアルタイムのメタデータと過去のメタデータと照合して，予め設定した程度の一致度が得られると当該過去のメタデータ及び関連付けられた過去の時系列データを参照して，その時点以降に発生したデータの変化やイベントを予兆として検出して出力するよう構成することができる。

【発明の効果】

【００１５】

本発明によればシステムへのトラヒックや性能データ等の監視データに対して選定条件（またはポリシールールという）に従い，傾向やイベント等の特徴や，保守者が行ったオペレーション，障害や保守作業イベント等を監視データに関係付けてメタデータとして保持し，リアルタイムのトラヒックや性能データ等のメタデータに対して選定条件に従って照合（マッチング）を行うことで，将来の監視データを予測及び将来起こりうる事象を迅速且つ正確に予兆し，起こりうるイベントやそのイベントに対する過去行った保守オペレーションを保守者へ通知することができる。

【００１６】

そして，単一点での異常値判定ではなく，特徴点の取得観点を選定条件（ポリシールール）として監視対象データ毎に設定できるようにすることで，取得データの種別や状況変化に柔軟に対応できるようにする。

【００１７】

また，過去の障害トラブルなどのイベント，障害防止対策として実施したオペレーションなどをそのメタデータに関連付けることで照合された過去データから必要なオペレーションを正確に抽出することを可能とする。

【発明を実施するための最良の形態】

【００１８】

図１は本発明に係るシステムの実施例の構成を示す。図中，１は監視装置，１０は監視対象システムからリアルタイムに収集する時系列データから指定されたメタデータを作成すると共に過去のメタデータと照合することで障害等の予兆を検出する処理部，１０ａは監視対象システム２のトラヒックや処理量等のシステムの状態を表す時系列データに対して予め設定されたデータの変化の傾向や，障害や保守作業のイベント等を関連付けて格納する過去データ用の第１のメタデータ化手段，１０ｂはリアルタイムの監視のための第２のメタデータ化手段，１０ｃはリアルタイムの時系列データから第２の選定条件格納部１１ｂの選定条件に従って生成されたリアルタイムのメタデータと，過去のメタデータ格納部１３ｂのメタデータとを照合して一致度が予め設定された値以上である過去のメタデータを検出すると，そのメタデータに対して一定時間内に障害が発生するか過去の時系列データ格納部１２ｂのデータから障害発生，障害時の規制等の対処内容等の予兆を出力する照合予兆検出手段である。

【００１９】

１１ａは監視対象システムのトラヒックや性能に関するデータや，回線使用率，パケット破棄率，エラーパケット数等のデータ等を定期的に取得した時系列データに対して，障害とは言えない（障害と判断される閾値を超えない）レベルであるが，平均値を超える値の発生回数や，変化のパターン等の過去のデータとの照合で障害等の予兆として検出できる設定データ，監視対象システムからの障害等のイベントデータ，保守端末１４からの作業内容（障害等の異常時における保守者のオペレーション）等を含む各種の選定条件（ポリシールールと呼ぶ場合がある）が格納された第１の選定条件格納部，１１ｂは監視対象システムのリアルタイムの時系列データから保守端末１４に対して障害発生の予兆を検出するためのメタデータを生成するための各種の選定条件（第１の選定条件格納部１１ａと同じ場合もあるが一部異なる条件を設定可能）が設定された第２の選定条件格納部，１２ａは監視対象システムから入力するトラヒック，ＣＰＵ使用率等のシステムの性能を表す予め設定された周期で抽出された複数種の時系列データを，障害等のシステムイベント情報（保守者が入力した情報を含む）とそれぞれの時間情報と共に格納される時系列データ格納部である。

【００２０】

１３ａは上記過去データ用の第１のメタデータ化手段１０ａにより生成したメタデータを格納したメタデータ格納部，１３ｂはメタデータ格納部１３ａに格納した過去の時系列データにより生成したメタデータが格納された過去のメタデータ格納部，１４は保守者が監視対象システム２に対して入力する操作指示（オペレーション）や，監視対象システム２から発生した障害やアラームを保守者に知らせるために出力（表示）が行われると共に，監視装置１からの障害等の予兆検出に応じて表示を行う保守端末，２は大規模コンピュータシステムやネットワークシステム等の監視対象システム，２０－１～２０－３は監視対象システム２の構成要素であるノード（コンピュータ，端末等）である。なお，図１の構成では時系列データ格納部１２ｂを時系列データ格納部１２ａと別に設けているが，監視対象システム２からのシステムの性能を表すリアルタイムの時系列データを格納するのと同時に，時系列データ格納部１２ａに格納された過去の時系列データを照合予兆検出手段１０ｃにおける照合のためにアクセス可能な構成を備えるようにすれば，過去の時系列データ格納部１２ｂを時系列データ格納部１２ａとは別に設ける必要がないが，図１の例では時系列データ格納部１２ａに格納したデータを過去データとして過去の時系列データ格納部１２ｂに適時に複写して照合に使用する。

【００２１】

選定条件格納部（図１の第１の選定条件格納部１１ａと第２の選定条件格納部１１ｂ）

に設定される選定条件（ポリシールール）の種類には，次のようなものがある。

【００２２】

(1) 時系列データ選定条件・・・時系列データの種類（監視対象システムから取出す性能を表すデータの種類）

(2) 抽出データ選定条件・・・メタデータとして保持するデータの抽出間隔（サンプリング間隔）

(3) 特徴データ選定条件・・・データ列に対する特徴を表現するための評価観点

(4) トリガデータ選定条件・・・メタデータ化とするシステム上に発生する各種イベント（故障やアラーム等）

(5) 知識データ選定条件・・・メタデータ化とする保守作業や障害対象の内容

(6) オフラインデータ選定条件・・・オフラインでメタデータ化する場合の投入形式の定義

図２に各部に格納されるデータの具体例を示す。図２のＡ．は選定条件格納部（図１の１１ａ，１１ｂ）に設定される選定条件のデータ構成であり，選定条件が１１０～１１６の各種類に分類されている例を示す。１１０は時系列データ選定条件でありａ１～ａ３が設定されており，ａ１はＣＰＵ使用率，ａ２はメモリ使用率，ａ３は回線使用率である。１１１は抽出データ選定条件であり，ｂ１～ｂ３としてそれぞれ１分，１０分，６０分の抽出間隔が設定されている。１１２は特徴データ選定条件であり，ｃ１～ｃ７の各特徴データが設定されおり，ｃ１はｔポイント（抽出間隔がｔ個分の時間）内での異常値検出回数，ｃ２はｔポイント内での平均値±３０％内の回数，ｃ３は最大異常値連続検出回数，ｃ４は増減パターン列（特徴となる増減パターン列），ｃ５は５を１単位とした場合の正規化値（元の数値を５で除算した時の商），ｃ６は５を１単位とした場合の増減正規化値，ｃ７は異常値検出回数（ｔポイント内）である。１１３はトリガデータ選定条件であり，この例ではｄ１として，システムイベント（障害やアラーム等）が設定されている。１１４は知識データ選定条件であり，ｅ１として異常復旧手順，ｅ２として障害解析手順が設定されている。１１５はオフラインデータ選定条件であり，保守者がオフラインで保守端末（図１の１４）から直接設定したメタデータであり，この例ではｆ１～ｆ４としてそれぞれ日付データとメタデータの組合せで構成される。１１６は一致度を表し，このデータは上記図１の照合予兆検出手段１０ｃにおける照合において，過去データ（実績データ）とリアルタイムデータとの一致度の程度を表し，ｇ１は特徴データ選定条件の５０％の一致度が要求される場合であり，ｇ２は特徴データ選定条件の１００％の一致度が要求されることを表す。

【００２３】

図２のＢ．は時系列データ格納部のデータ構成例であり，この例はＣＰＵ使用率のデータだけを示すが，他にメモリ使用率，回線使用率，トラヒック等の各種の時系列データを格納することができる。Ｂ．の例では，計測時間の抽出周期毎のＣＰＵ使用率を表す時系列データ１２０が設定され，この例では抽出周期が１分毎（15:11:50は１５時１１分５０秒を表し，15:12:50，15:13:50，15:14:50・・・の各時点）の場合であり，図２のＡ．に示す抽出データ選定条件のｂ１に設定された抽出周期である。Ｃ．はメタデータ格納部に格納されるデータ構成例であり，各種の抽出された時系列データに対するメタデータ１３０が格納され，各抽出データ毎（時系列データの種別及び抽出周期別）にメタデータが作成される。Ｃ．に示す例では，抽出データとして上記Ｂ．に示す１分周期で抽出されたＣＰＵ使用率を表す時系列データに対して，特徴データ選定条件として図２のＡ．の選定条件の中の特徴データ選定条件１１２の中の異常値検出回数ｃ１と最大異常値連続検出回数ｃ３に適合したメタデータであり，トリガデータ選定条件１１３のシステムイベントｄ１及び知識データ選定条件１１４の中の異常復旧手順ｅ１の各選定条件を満たして選定されたメタデータが格納されている。

【００２４】

図３は時系列データ収集とメタデータ格納の処理フローである。図４は時系列データからメタデータ生成の仕組みと時系列データの変動パターン例を示し，Ａ．のａ～ｄは時系

列データ入力，障害情報入力，オペレーション入力及びシステムイベント入力という監視対象システムから出力または保守端末からシステムへ入力されるデータを表し，このデータが第１の選定条件格納部１１ａに設定された条件に適合するとメタデータ格納部１３ａに格納され，時系列データは時系列データ格納部１２ａに格納され，図４のＢ．は時系列データの変化の例を示し，平均値に対する±３０％の変動のライン，時間ｔ０の一定時間後の時間ｔ１にトラヒックが増加してサーバＡの輻輳が発生し，時間ｔ２にトラヒック入量規制が実行され，時間ｔ３に入量規制解除が実行されている例を示す。

【００２５】

図３のフローチャートを図２及び図４を参照しながら説明する。最初に選定条件を読込む（図３のＳ１）。この場合，図１の第１の選定条件格納部１１ａから処理部１０の第１のメタデータ化手段１０ａに読込まれる。続いて時系列データを収集し（図３のＳ２），収集された時系列データに対してデータの種類（例えば，ＣＰＵ使用率）に対して設定された選定条件に従いメタデータ化を行う（同Ｓ３）。この場合，入力された時系列データについて，選定条件として設定された条件を満たすか判定し，満たす場合はそれをメタデータとして格納する。図２に示す例では時系列データの入力に対してＡ．に示す選定条件１１ａと照合して，Ｃ．に示すメタデータが生成される。

【００２６】

この時の時系列データとそれに関するメタデータとを関連付け（時間情報を共通データとして持つ），データベース（図１～図４の時系列データ格納部１２とメタデータ格納部１３ａに対応）に格納し（図３のＳ４），次に新しい収集データが存在するか判別し（同Ｓ５），存在する場合はステップＳ３に戻り，同様の処理（Ｓ４，Ｓ５）が実行され，存在しないと終了する。

【００２７】

このようにして監視対象システム２からの時系列データとその時系列データについて選定条件を満たしたメタデータが，時間情報を共通データとして紐付け（関連付け）られ，メタデータ格納部１３ａに過去データ（実績）として格納され，そのメタデータ格納部１３ａに格納されたメタデータに対応した過去の時系列データが時系列データ格納部１２に格納され，各格納部１２，１３ａのデータは監視装置１において後述する監視の処理フロー（図６）において利用される。なお，メタデータ格納部１３ａには，特徴データだけでなく，実際に過去において発生（実行）したトリガデータ（障害等のシステムイベント），知識データ（障害復旧手順等），オフラインデータ（操作者が実行した操作，処理等）等の実績データも含まれ，時系列データ格納部１２ａには図４のＢ．に示すＣＰＵ使用率等の変動パターンとイベント（イベントはメタデータだけに含まれる）のデータ（障害発生等）が格納される。

【００２８】

図５はオフラインのメタデータ設定の処理フローであり，保守端末１４からの操作により実行される。最初に現状の選定条件（ポリシールール）として定義されている内容を全て表示し（図５のＳ１），保守端末よりメタデータとして登録したいデータの読み込み（保守作業等の作業手順，システムイベント，システム状況等）を行う（同Ｓ２）。選定条件（オフライン登録形式定義）に従い，登録されたデータからメタデータとして保持するデータを抽出し（図５のＳ３），抽出されたメタデータを時系列データと時間（日付）により紐付け（関係付け）し，データベースへ格納する（同Ｓ４）。このようにして，異常発生後の対処手順や障害発生前に発生するように予兆現象などの監視時系列データの特徴，時系列データに現れないサービスイベントや保守イベントなどを，保存されているオンラインで作成されるメタデータに対してオフライン作業として追加することが可能となる。

【００２９】

図６は監視対象システムのリアルタイムの監視の処理フローであり，図７は照合によるリアルタイムの予兆検出動作の説明図である。図７のＡ．はリアルタイムの時系列データ，Ｂ．は過去のメタデータとリアルタイムのメタデータとの照合を取る動作を示し，Ｃ．

は一定程度以上の一致が得られた（マッチングした）場合の現在から後に発生するパターン（過去の時系列データから得たパターン）を示し，Ｄ．は一致が得られたデータが複数パターン検出された場合の複数のパターンを表す。

【００３０】

図６において，最初に選定条件（ポリシールール）を読み込む（図６のＳ１）。この時の選定条件は図１の第２の選定条件格納部１１ｂに格納されたリアルタイムの監視に使用する選定条件であり，上記図３の処理フローの過去データ（実績データ）を収集する時に参照される選定条件（図１の第１の選定条件格納部１１ａ）と同じでもよいが，異なったもの（一部を選択可能）でも良い。監視装置（図１の１）の監視対象システム（図１の２）を構成する装置から情報収集を行う（図６のＳ２）。次にリアルタイムの時系列データ（図７のＡ．に例として示す）に対して選定条件（図１の第２の選定条件格納部１１ｂ）に従ってメタデータ化され，得られたメタデータと過去データのメタデータ（図１の過去のメタデータ格納部１３ｂ）を照合する（図６のＳ３）。この様子は図７のＢ．に示される。

【００３１】

照合による一致度を算出する（図６のＳ４）。この場合，一致度として６０％，４０％等の数値が得られる。複数の過去データに対して一致度の数値によりソート（降順）する（図６のＳ５）。これにより一致度の異なる複数の過去データが検出されても一致度の高いものから順に並べられる。次に予め設定された一定値以上の一致度を持つ対象過去データがあるか判別し（図６のＳ６），一定値以上の一致度を持つ対象過去データが無いとステップＳ３に戻り，該当する対象過去データがあった場合は選択された過去データ（一定値以上の一致度を持つ）に対して，今後発生しうるデータ状況を表示する（同Ｓ７）。このデータ状況の表示は一定値以上の一致度を持つ過去データの時間情報の後に発生したデータ状況を当該一致度を持つ過去の時系列データ（時系列データ格納部１２に格納）の中から選択して表示する。図７のＣ．は，一致度が一定値以上であった現在までの過去データについて，現在より後に発生し得る過去データの例が表示されている。

【００３２】

次に上記ステップＳ７で選択された過去データにおいて異常が発生しうるか判別する（図６のＳ８）。この判別は，選択された一定値以上の一致度を持つ過去のメタデータ（図１のメタデータ格納部１３ｂ）の発生時刻（時点ｔ）に対応する過去の時系列データ（図１の時系列データ格納部１２ｂ）を見てその一定時間内（時点ｔ＋ｘ内）に性能データに異常が発生しているかを検出するものである。

【００３３】

現在から一定時間内に異常が発生しないと判別されると，ステップＳ３に戻り，現状の情報のメタデータと過去点のメタデータの比較の処理を引き続き行い，異常が発生し得ると判別されると，発生され得る（予兆される）と判別された異常に対してメタデータから対処手順を読み込む（図６のＳ９）。この対処手順は図２の例で示すと，Ｃ．に示すメタデータの中では「（ｅ１）異常復旧手順」として示されて，上記図２のＡ．に示す知識データ選定条件１１４の中の異常復旧手順に適合したデータとして格納されている。次にこの対処手順について選定条件に異常時の自動対処（フラグ）がオンであるか判別する（図６のＳ１０）。図２のＡ．の例では知識データ選定条件１１４の中の障害復旧手順に対して「自動対処フラグ」が「１」（オンを表す）に設定されている。

【００３４】

自動対処のフラグがオンに設定されてない場合は，異常内容及び対処内容を表示（図１の保守端末１４に表示）し（図６のＳ１１），保守者が対処内容（結果）を確認できるようにする。図７のＤ．は異常内容（予兆）及び対処内容を保守端末に表示した例を示し，現在時間ｔ０に対し一定時間後のｔ１にサーバＡの輻輳発生があり，ｔ２にトラヒック入量規制の対処が実行され，ｔ３に入量規制解除が実行されていることが表示される。なおこの例では，点線で示す別の過去データ（一致度が一定値以上の別のデータ）が存在し，複数のデータが同時に表示されている。

【００３５】
上記ステップＳ１０で自動対処フラグがオンに設定されていると判別されると，自動処理が実行されるが，対象が複数存在するか判別する（図６のＳ１２）。これは上記ステップＳ５において一致度が一定値以上の過去データが複数あるか判別するもので，複数存在する場合は選定条件に従い，最適なパターンを選択する（同Ｓ１３）。この時，日付情報により最も近いものを最適パターンとして選択する。その場合，選定条件（ポリシールール）に最新日付情報とする定義がなされているものとし，デフォルトを最新日付とすることができる。
【００３６】
ステップＳ１２で対象が複数存在しない場合及びステップＳ１３で選択されると，異常内容を表示して対処処理（自動処理の内容）を実行し（図６のＳ１４），処理を終了する。
【００３７】
上記ステップＳ８で判別される過去データには，監視を強化すべき状態であることや，保守者によるシステムへのアクション（設定，制御等のオペレーション）の発火条件等をを過去の時系列データに記録しておくことにより，それらのデータを一定以上の一致度を持つ場合に出力することができる。
【００３８】
図８は監視対象データのメタデータ化の例を示し，図８の(1) は時系列データの例であり，計測単位時間として１分（抽出間隔）を用い，監視対象システムの特性を表す測定データの一つとしてトラヒック量を収集した例である。図８の(2) は，(1) に示す時系列データ（測定データ）に対して選定条件の例１として，図２のＡ．の特徴データ選定条件１１２の中のｃ５に示す「５」を１単位とした場合の正規化値である。また，図８の(3) は(1) に示す時系列の測定データに対して選定条件の例２として，図２のＡ．の特徴データ選定条件１１２の中のｃ６に示す「５」を１単位とした場合の１単位以上の増減正規化値である。更に，図８の(4) は(1) に示す時系列の測定データに対して選定条件として，「５」を１単位として，２単位を超える測定データの正規化値である。(2) ～(4) の各正規化値における警報発生の条件が設定されている。
【００３９】
（付記１）　大規模コンピュータシステムやネットワークシステム等の監視対象システムの障害等の予兆を検出する監視装置であって，監視対象システムの性能を表す時系列データを一定周期で抽出して過去の時系列データとして格納する手段と，前記時系列データが，設定された数値や変化のパターンを表す特徴データや，障害発生等のイベントやトリガデータを含む予め格納部に格納された選定条件に適合すると過去のメタデータとして前記時系列データと関連付けて過去のメタデータ格納手段に格納する第１のメタデータ化手段と，監視対象システムからのリアルタイムの性能を表す時系列データについて上記選定条件とは別に設定された選定条件に適合するとリアルタイムのメタデータを生成する第２のメタデータ化手段と，前記リアルタイムのメタデータと前記過去のメタデータ格納手段のメタデータとを照合し，前記照合において予め設定された所定の一致度が得られると当該メタデータに関連付けられた前記過去の時系列データを参照して設定された時系列データの今後の変化を検出して出力する照合予兆検出手段と，を備えることを特徴とする監視対象システムの障害等の予兆を検出する監視装置。
【００４０】
（付記２）　付記１において，前記照合予兆検出手段は，前記所定の一致度が得られたメタデータに関連付けられた前記過去の時系列データにおいて異常が発生するか判別して，異常が検出されると，異常に対する対処手順を前記関連付けられた過去のメタデータから読み出して保守端末に表示して対処を促すことを特徴とする監視対象システムの障害等の予兆を検出する監視装置。
【００４１】
（付記３）　付記１において，前記照合予兆検出手段は，前記照合において予め設定さ

れた所定の一致度が複数の過去のメタデータについて得られると，該複数の過去のメタデータに関連付けられた各時系列データを参照して最も最近に発生した時系列データの今後の変化を検出して出力することを特徴とする監視対象システムの障害等の予兆を検出する監視装置。

【００４２】

（付記４）　付記１において，前記選定条件のデータとして，時系列データの抽出周期，知識データとして異常復旧手順，障害解析手順，オフラインデータとして操作端末からの日付とイベントの情報を設定し，前記第１と第２のメタデータ化手段は，前記各選定条件に設定されたオフライン設定データを含めてメタデータ化することを特徴とする監視対象システムの障害等の予兆を検出する監視装置。

【００４３】

（付記５）　大規模コンピュータシステムやネットワークシステム等の監視対象システムの監視方法において，前記監視対象システムの状態を表す時系列データの値や変化の特徴を選定条件として予め設定し，前記選定条件に従って監視対象の時系列データをメタデータ化して過去のメタデータとして過去の時系列データと関連付けて格納し，前記監視対象システムのリアルタイムの状態を表す時系列データについて予め設定した値や変化の特徴を選定条件としてメタデータを生成し，前記生成したリアルタイムのメタデータと前記過去のメタデータと照合して，予め設定した程度の一致度が得られると当該過去のメタデータ及び関連付けられた過去の時系列データを参照して，その時点以降に発生したデータの変化やイベントを予兆として検出して出力する，ことを特徴とする監視対象システムの障害等の予兆を検出する監視方法。

【００４４】

（付記６）　付記５において，前記選定条件は，監視対象システムの監視対象データ毎に設定することを特徴とする監視対象システムの障害等の予兆を検出する監視方法。

【００４５】

（付記７）　付記５において，前記過去のメタデータとして，障害時における保守者が対応すべき操作内容を関連付けて保持し，障害の予兆が出力される時に前記保持された操作内容を出力することを特徴とする監視対象システムの障害等の予兆を検出する監視方法。

【図面の簡単な説明】

【００４６】

【図１】本発明に係るシステムの実施例の構成を示す図である。

【図２】各部に格納されるデータの具体例を示す図である。

【図３】時系列データ収集とメタデータ格納の処理フローである。

【図４】時系列データからメタデータ生成の仕組みと時系列データの変動パターン例を示す図である。

【図５】オフラインのメタデータ設定の処理フローを示す図である。

【図６】監視対象システムのリアルタイムの監視の処理フローを示す図である。

【図７】照合によるリアルタイムの予兆検出動作の説明図である。

【図８】監視対象データのメタデータ化の例を示す図である。

【図９】監視対象のデータが推移するパターンの例を示す図である。

【符号の説明】

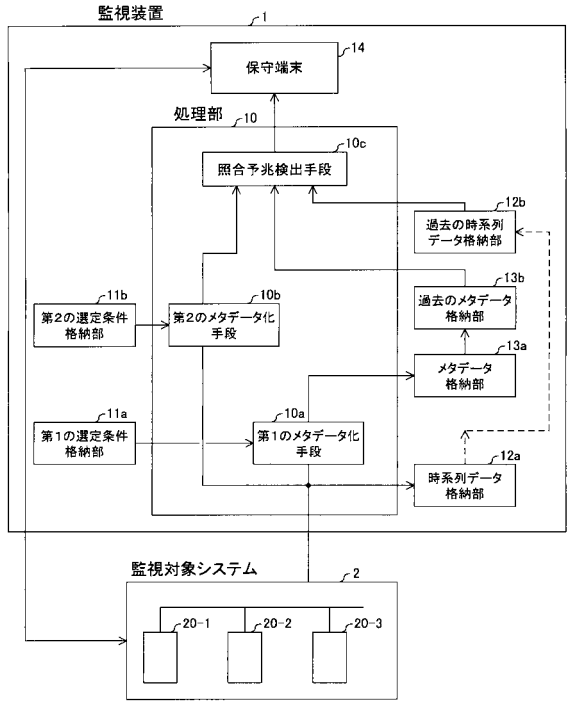
【００４７】

１　　監視装置
１０　　処理部
１０ａ　　第１のメタデータ化手段
１０ｂ　　第２のメタデータ化手段
１０ｃ　　照合予兆検出手段
１１ａ　　第１の選定条件格納部
１１ｂ　　第２の選定条件格納部

１２ａ　　時系列データ格納部
１３ａ　　メタデータ格納部
１３ｂ　　過去のメタデータ格納部
１４　　保守端末
２　　監視対象システム
２０－１～２０－３　　ノード

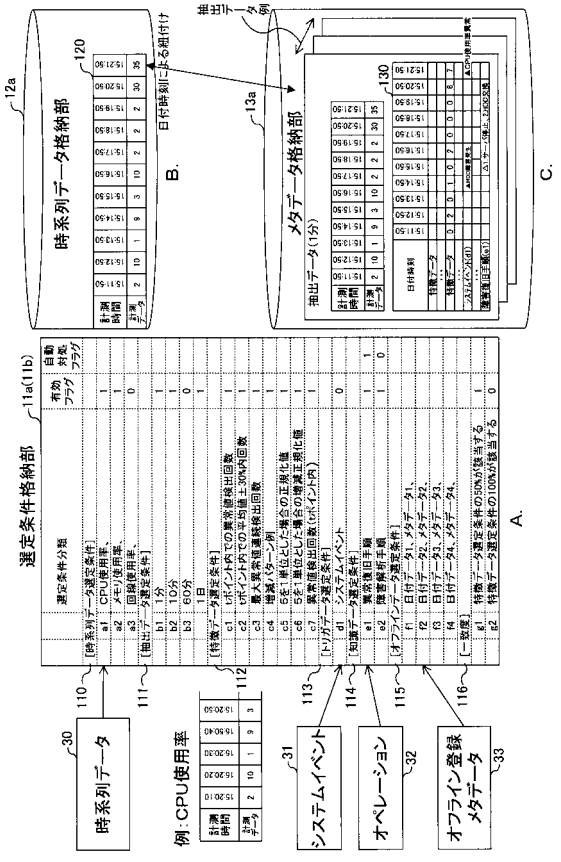
【図１】

本発明に係るシステムの実施例の構成



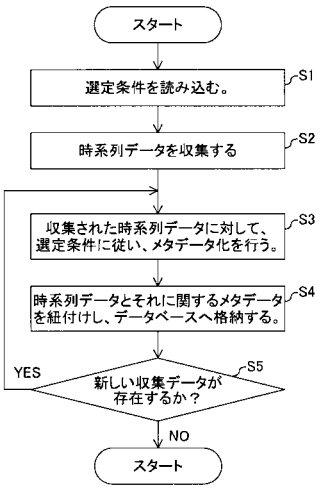
【図２】

各部に格納されるデータの具体例



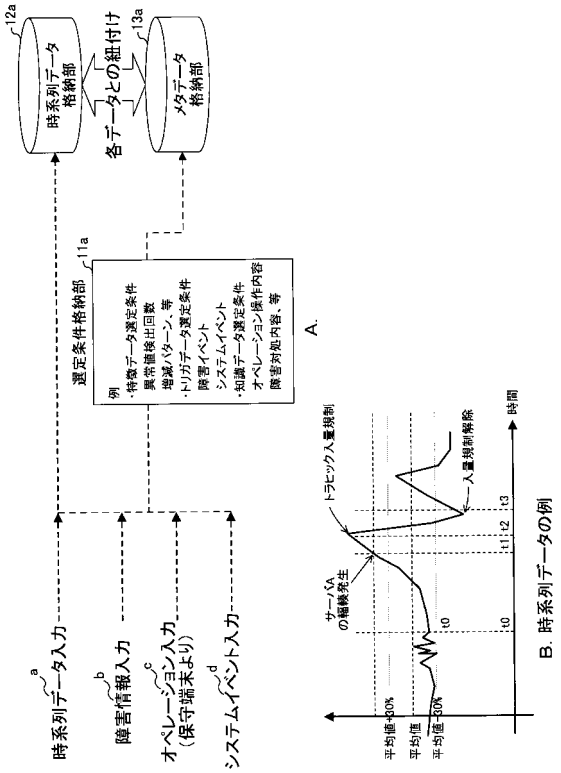
【図３】

時系列データ収集とメタデータ格納の処理フロー



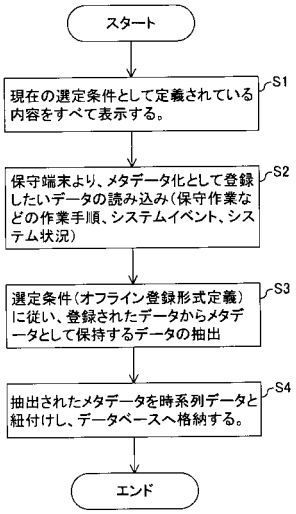
【図４】

時系列データからメタデータ生成の仕組みと時系列データの変動パターン例



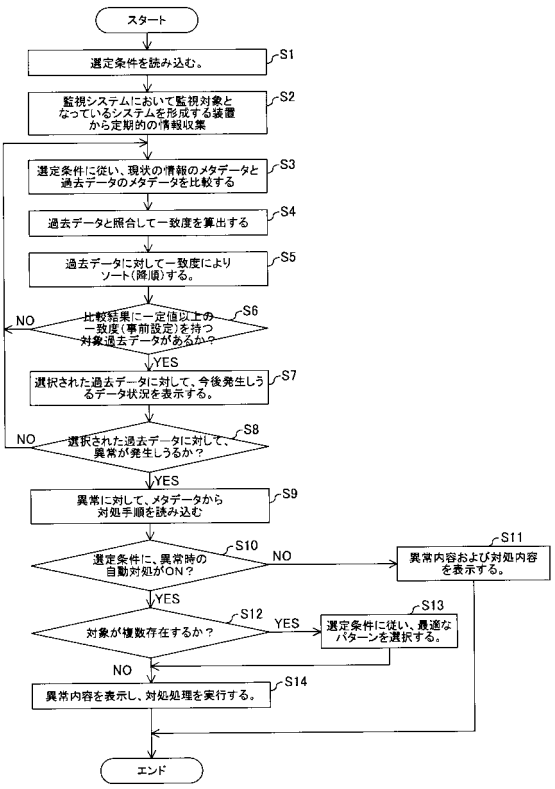
【図５】

オフラインのメタデータ設定の処理フロー



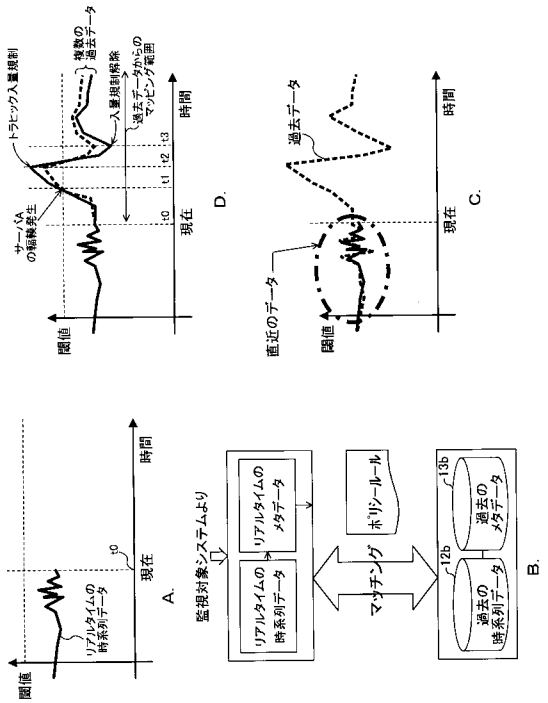
【図６】

監視対象システムのリアルタイムの監視の処理フロー



【図７】

照合によるリアルタイムの予兆検出動作の説明図



【図８】

監視対象データのメタデータ化の例

(1)

計測単位時間	00:00:00	00:01:00	00:02:00	00:03:00	00:04:00	00:05:00	00:06:00	00:07:00	00:08:00	00:09:00
計測データ	2	10	1	9	3	10	2	2	2	30

(2)

ポリシールール例1	5を1単位として、測定データを正規化する。									
メタデータ例1	0	2	0	1	0	2	0	0	0	6
	▲警報発火条件設定									

(3)

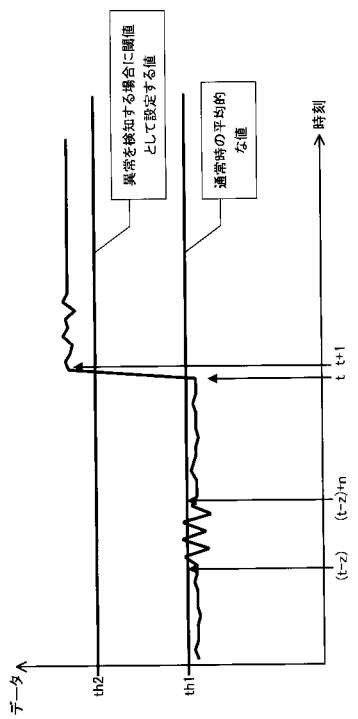
ポリシールール例2	5を1単位として、1単位以上の増減を正規化する。									
メタデータ例2	0	+2	-2	+1	-1	+2	-2	0	0	+6
	▲警報発火条件設定									

(4)

ポリシールール例3	5を1単位として、2単位を超える測定データを正規化する。									
メタデータ例3	0	2	0	0	0	2	0	0	0	6
	▲警報発火条件設定									

【図９】

監視対象のデータが推移するパターンの例



フロントページの続き

(72)発明者　来海　清
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　今村　哲朗
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　中山　幸司
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　澁谷　仁
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　吉沢　誠
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　吉田　直宏
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

審査官　木村　雅也

(56)参考文献　特開平１０－０４９２１９（ＪＰ，Ａ）
特表２００５－５２３５２６（ＪＰ，Ａ）
特開２００１－０２８６２８（ＪＰ，Ａ）
特開２００５－２８５０４０（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　１３／００