

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第5621937号
(P5621937)

(45) 発行日 平成26年11月12日(2014.11.12)

(24) 登録日 平成26年10月3日(2014.10.3)

(51) Int.Cl. F I
G06F 11/34 (2006.01) G O 6 F 11/34 S
G06F 11/32 (2006.01) G O 6 F 11/32 J

請求項の数 21 (全 17 頁)

<p>(21) 出願番号 特願2013-529952 (P2013-529952) (86) (22) 出願日 平成24年7月31日 (2012.7.31) (86) 国際出願番号 PCT/JP2012/069931 (87) 国際公開番号 W02013/027562 (87) 国際公開日 平成25年2月28日 (2013.2.28) 審査請求日 平成26年2月19日 (2014.2.19) (31) 優先権主張番号 特願2011-182261 (P2011-182261) (32) 優先日 平成23年8月24日 (2011.8.24) (33) 優先権主張国 日本国(JP)</p>	<p>(73) 特許権者 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 100109313 弁理士 机 昌彦 (74) 代理人 100124154 弁理士 下坂 直樹 (72) 発明者 長谷川 英男 東京都港区芝五丁目7番1号 日本電気株式会社内 審査官 多賀 実</p>
---	--

最終頁に続く

(54) 【発明の名称】 運用管理装置、運用管理方法、及びプログラム

(57) 【特許請求の範囲】

【請求項 1】

システムにおける複数メトリックの計測値をそれぞれ時系列に収集するメトリック収集手段と、

前記複数メトリックの計測値の各々の各時刻における異常の継続度合いを示す継続度をもとに、当該メトリックの異常スコアを算出し、出力する異常スコア算出手段と、
を備え、

前記異常スコア算出手段は、前記異常スコアに応じて、所定の図形の大きさ、及び、表示手段の表示画面上の位置を決定し、当該図形を、当該大きさで、当該位置に表示する運用管理装置。

【請求項 2】

前記異常スコア算出手段は、前記異常スコアに応じて大きくなる概略円形の図形の大きさ、及び、前記異常スコアに応じて高くなる、所定の垂直軸上の設定された基準点からの高さを決定し、当該図形を、当該大きさで、当該基準点からの高さに表示する
 請求項 1 に記載の運用管理装置。

【請求項 3】

前記異常スコア算出手段は、前記異常の検出の開始時刻が同一である前記メトリックからなるグループを生成し、当該グループに含まれる前記メトリックの異常スコアの合計値を当該グループの異常スコアとして算出し、出力する
 請求項 1 または 2 に記載の運用管理装置。

【請求項 4】

システムにおける複数メトリックの計測値をそれぞれ時系列に収集するメトリック収集手段と、

前記複数メトリックの計測値の各々の各時刻における異常の継続度合いを示す継続度をもとに、当該メトリックの異常スコアを算出し、出力する異常スコア算出手段と、
を備え、

前記異常スコア算出手段は、前記異常の検出の開始時刻が同一である前記メトリックからなるグループを生成し、当該グループに含まれる前記メトリックの異常スコアの合計値を当該グループの異常スコアとして算出し、出力する

運用管理装置。

10

【請求項 5】

前記異常スコア算出手段は、前記複数メトリックの計測値の各々の各時刻における異常の度合いを示す異常度と前記継続度とをもとに、当該メトリックの前記異常スコアを算出する

請求項 1 乃至 4 のいずれかに記載の運用管理装置。

【請求項 6】

さらに、前記複数のメトリックの内の異なる 2 つのメトリック間の相関関係を示す相関関数を 1 以上含む相関モデルを記憶する相関モデル記憶手段を含み、

前記異常度は、前記複数メトリックの計測値の各々を前記相関関数に適用したときの変換誤差をもとに算出される

請求項 5 に記載の運用管理装置。

20

【請求項 7】

前記継続度は、各時刻以前の所定期間における、前記異常が検出された期間の割合である

請求項 1 乃至 6 のいずれかに記載の運用管理装置。

【請求項 8】

システムにおける複数メトリックの計測値をそれぞれ時系列に収集し、

前記複数メトリックの計測値の各々の各時刻における異常の継続度合いを示す継続度をもとに、当該メトリックの異常スコアを算出し、出力する

運用管理方法であって、

前記異常スコアを出力する場合、前記異常スコアに応じて、所定の図形の大きさ、及び、表示手段の表示画面上の位置を決定し、当該図形を、当該大きさで、当該位置に表示する

運用管理方法。

30

【請求項 9】

前記異常スコアを出力する場合、前記異常スコアに応じて大きくなる概略円形の図形の大きさ、及び、前記異常スコアに応じて高くなる、所定の垂直軸上の設定された基準点からの高さを決定し、当該図形を、当該大きさで、当該基準点からの高さに表示する

請求項 8 に記載の運用管理方法。

【請求項 10】

前記異常スコアを出力する場合、前記異常の検出の開始時刻が同一である前記メトリックからなるグループを生成し、当該グループに含まれる前記メトリックの異常スコアの合計値を当該グループの異常スコアとして算出し、出力する

請求項 8 または 9 に記載の運用管理方法。

40

【請求項 11】

システムにおける複数メトリックの計測値をそれぞれ時系列に収集し、

前記複数メトリックの計測値の各々の各時刻における異常の継続度合いを示す継続度をもとに、当該メトリックの異常スコアを算出し、出力する

運用管理方法であって、

前記異常スコアを出力する場合、前記異常の検出の開始時刻が同一である前記メトリッ

50

クからなるグループを生成し、当該グループに含まれる前記メトリックの異常スコアの合計値を当該グループの異常スコアとして算出し、出力する
運用管理方法。

【請求項 1 2】

前記異常スコアを算出する場合、前記複数メトリックの計測値の各々の各時刻における異常の度合いを示す異常度と前記継続度とをもとに、当該メトリックの前記異常スコアを算出する

請求項 8 乃至 1 1 のいずれかに記載の運用管理方法。

【請求項 1 3】

さらに、前記複数のメトリックの内の異なる 2 つのメトリック間の相関関係を示す相関関数を 1 以上含む相関モデルを記憶し、

前記異常度は、前記複数メトリックの計測値の各々を前記相関関数に適用したときの変換誤差をもとに算出される

請求項 1 2 に記載の運用管理方法。

【請求項 1 4】

前記継続度は、各時刻以前の所定期間における、前記異常が検出された期間の割合である

請求項 8 乃至 1 3 のいずれかに記載の運用管理方法。

【請求項 1 5】

コンピュータに、

システムにおける複数メトリックの計測値をそれぞれ時系列に収集し、

前記複数メトリックの計測値の各々の各時刻における異常の継続度合いを示す継続度をもとに、当該メトリックの異常スコアを算出し、出力する

処理を実行させるプログラムであって、

前記異常スコアを出力する場合、前記異常スコアに応じて、所定の図形の大きさ、及び、表示手段の表示画面上の位置を決定し、当該図形を、当該大きさで、当該位置に表示する

処理を実行させるプログラム。

【請求項 1 6】

前記異常スコアを出力する場合、前記異常スコアに応じて大きくなる概略円形の図形の大きさ、及び、前記異常スコアに応じて高くなる、所定の垂直軸上の設定された基準点からの高さを決定し、当該図形を、当該大きさで、当該基準点からの高さに表示する

処理を実行させる請求項 1 5 に記載のプログラム。

【請求項 1 7】

前記異常スコアを出力する場合、前記異常の検出の開始時刻が同一である前記メトリックからなるグループを生成し、当該グループに含まれる前記メトリックの異常スコアの合計値を当該グループの異常スコアとして算出し、出力する

処理を実行させる請求項 1 5 または 1 6 に記載のプログラム。

【請求項 1 8】

コンピュータに、

システムにおける複数メトリックの計測値をそれぞれ時系列に収集し、

前記複数メトリックの計測値の各々の各時刻における異常の継続度合いを示す継続度をもとに、当該メトリックの異常スコアを算出し、出力する

処理を実行させるプログラムであって、

前記異常スコアを出力する場合、前記異常の検出の開始時刻が同一である前記メトリックからなるグループを生成し、当該グループに含まれる前記メトリックの異常スコアの合計値を当該グループの異常スコアとして算出し、出力する

処理を実行させるプログラム。

【請求項 1 9】

前記異常スコアを算出する場合、前記複数メトリックの計測値の各々の各時刻における

10

20

30

40

50

異常の度合いを示す異常度と前記継続度とをもとに、当該メトリックの前記異常スコアを算出する処理を実行させる請求項 15 乃至 18 のいずれかに記載のプログラム。

【請求項 20】

さらに、前記複数のメトリックの内の異なる 2 つのメトリック間の相関関係を示す相関関数を 1 以上含む相関モデルを記憶する処理を実行させ、

前記異常度は、前記複数メトリックの計測値の各々を前記相関関数に適用したときの変換誤差をもとに算出される

請求項 19 に記載のプログラム。

【請求項 21】

前記継続度は、各時刻以前の所定期間における、前記異常が検出された期間の割合である

10

請求項 15 乃至 20 のいずれかに記載のプログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、運用管理装置、運用管理方法、及びプログラムに関し、特にシステムの異常を検出する運用管理装置、運用管理方法、及びプログラムに関する。

【背景技術】

【0002】

IT (Information Technology) システムでは、管理者がシステムを監視し、システムに異常が発生したと認められる場合には、検出された異常に優先順位をつけて対処することにより、システム停止などの致命的な状態を回避する。

20

このような IT システムの異常を検出する運用管理システムの一例が、特許文献 1 及び 2 に記載されている。特許文献 1 及び 2 に記載の運用管理システムは、システムの複数のメトリック（性能指標）の計測値をもとに、メトリックの組み合わせの各々に対して相関関係を検出し、相関モデルを生成する。そして、この運用管理システムは、生成された相関モデルを用いて、入力されたメトリックの計測値に対して相関関係の破壊が発生しているかどうかを判定し、システムの異常を検出する。

この運用管理システムでは、管理者がシステムの異常有無を判別するため、相関破壊数の時間経過を示すグラフを出力する。また、ある時刻における異常の詳細として、異常が検出されたメトリック（異常メトリック）のリストを、異常スコアとともに出力する。

30

なお、関連技術として、特許文献 3 には、システムのリソース項目の中から、統計手法を用いて監視項目、及び、閾値を検出する監視装置が開示されている。

【先行技術文献】

【特許文献】

【0003】

【特許文献 1】特開 2009 - 199533 号公報

【特許文献 2】特開 2010 - 186310 号公報

【特許文献 3】特開 2003 - 263342 号公報

【発明の概要】

40

【発明が解決しようとする課題】

【0004】

上述の特許文献 1 及び 2 に記載の運用管理システムでは、システムの規模が大きくなるとメトリックの数が増え、異常メトリックも大量に提示される。異常メトリックには、バックグラウンド処理等に起因した短時間で終了する異常のように、本来管理者が注目する必要がない重要度（緊急度）の低い異常が発生しているメトリックも含まれるが、このように大量の異常メトリックが発生した場合、長時間継続して発生している異常のように、重要度（緊急度）の高い異常が発生しているメトリックを把握することが難しくなるという問題がある。

本発明の目的は、上述の課題を解決し、システムにおける継続性のある異常が発生して

50

いるメトリックを容易に把握できる運用管理装置、運用管理方法、及びプログラムを提供することである。

【課題を解決するための手段】

【0005】

本発明の一態様における運用管理装置は、システムにおける複数メトリックの計測値をそれぞれ時系列に収集するメトリック収集手段と、前記複数メトリックの計測値の各々の各時刻における異常の継続度合いを示す継続度をもとに、当該メトリックの異常スコアを算出し、出力する異常スコア算出手段と、を含む。

本発明の一態様における運用管理方法は、システムにおける複数メトリックの計測値をそれぞれ時系列に収集し、前記複数メトリックの計測値の各々の各時刻における異常の継続度合いを示す継続度をもとに、当該メトリックの異常スコアを算出し、出力する。

10

本発明の一態様におけるコンピュータが読み取り可能な記録媒体は、コンピュータに、システムにおける複数メトリックの計測値をそれぞれ時系列に収集し、前記複数メトリックの計測値の各々の各時刻における異常の継続度合いを示す継続度をもとに、当該メトリックの異常スコアを算出し、出力する処理を実行させるプログラムを格納する。

【発明の効果】

【0006】

本発明の効果は、システムにおける継続性のあるメトリックの異常を容易に把握できることである。

【図面の簡単な説明】

20

【0007】

【図1】本発明の第1の実施の形態の特徴的な構成を示すブロック図である。

【図2】本発明の第1の実施の形態における運用管理装置100を適用した運用管理システムの構成を示すブロック図である。

【図3】本発明の第1の実施の形態における運用管理装置100の処理を示すフローチャートである

【図4】本発明の第1の実施の形態における性能系列情報121の例を示す図である。

【図5】本発明の第1の実施の形態における相関モデル122の例を示す図である。

【図6】本発明の第1の実施の形態における残差の例を示す図である。

【図7】本発明の第1の実施の形態における相関変化情報123の例を示す図である。

30

【図8】本発明の第1の実施の形態における異常スコアの算出過程を示す図である。

【図9】本発明の第1の実施の形態における異常スコアの算出結果を示す図である。

【図10】本発明の第1の実施の形態における解析結果130の例を示す図である。

【図11】本発明の第2の実施の形態における運用管理装置100の処理を示すフローチャートである。

【図12】本発明の第2の実施の形態におけるグループ異常スコアの算出結果を示す図である。

【図13】本発明の第2の実施の形態における解析結果140の例を示す図である。

【発明を実施するための形態】

【0008】

40

(第1の実施の形態)

次に、本発明の第1の実施の形態について説明する。

はじめに、本発明の第1の実施の形態の構成について説明する。図2は、本発明の第1の実施の形態における運用管理装置100を適用した運用管理システムの構成を示すブロック図である。

図2を参照すると、本発明の第1の実施の形態における運用管理システムは、運用管理装置100、1以上の被監視装置200、及び、監視端末300を含む。運用管理装置100と被監視装置200は、ネットワークにより接続される。また、運用管理装置100と監視端末300も、ネットワークにより接続される。

被監視装置200は、WebサーバやDatabaseサーバ等、システムを構成する

50

装置である。被監視装置 200 の各々は、監視エージェント 201 を含む。

被監視装置 200 の監視エージェント 201 は、被監視装置 200 の複数種目の性能値の実測データ（計測値）を一定間隔毎に計測し、運用管理装置 100 へ送信する。性能値の種目として、例えば、CPU（Central Processing Unit）使用率、メモリ使用率、ディスクアクセス頻度等、コンピュータリソースの使用率や使用量用いられる。

ここで、被監視装置 200 と性能値の種目の組をメトリック（性能指標）とし、同一時刻に計測された複数のメトリックの値の組を性能情報とする。メトリックは、整数や小数の数値より表される。また、メトリックは、特許文献 1 における要素に相当する。

運用管理装置 100 は、監視対象である被監視装置 200 から収集した性能情報をもとに、被監視装置 200 についての相関モデル 122 を生成し、生成した相関モデル 122 を用いて、被監視装置 200 の障害や異常の検出を行う。

運用管理装置 100 は、メトリック収集部 101、相関モデル生成部 102、相関変化分析部 103、異常スコア算出部 104、メトリック記憶部 111、相関モデル記憶部 112、及び、相関変化記憶部 113 を含む。

メトリック収集部 101 は、被監視装置 200 から性能情報を収集し、その時系列変化を性能系列情報 121 としてメトリック記憶部 111 に保存する。

相関モデル生成部 102 は、性能系列情報 121 をもとに、被監視装置 200 により構成されるシステムの相関モデル 122 を生成する。

相関モデル記憶部 112 は、相関モデル生成部 102 が生成した相関モデル 122 を記憶する。

相関変化分析部 103 は、特許文献 1 と同様に、新たに入力された性能情報について、相関モデル 122 に含まれる各メトリックの組み合わせに対する相関関係の異常を検出する。

相関変化記憶部 113 は、相関変化分析部 103 による相関関係の異常の検出結果を相関変化情報 123 として記憶する。

異常スコア算出部 104 は、相関変化情報 123 をもとに、各メトリックの異常スコアを算出し、監視端末 300 へ出力する。

監視端末 300 は、運用管理装置 100 が、管理者等から被監視装置 200 の障害や異常の検出指示を受け付け、その検出結果を出力するための端末である。監視端末 300 は、表示部 301 を含む。

監視端末 300 の表示部 301 は、例えば、ディスプレイ等の表示デバイスであり、運用管理装置 100 により出力された異常スコアを、表示画面により、管理者等に出力（表示）する。

なお、運用管理装置 100 は、CPU とプログラムを記憶した記憶媒体を含み、プログラムに基づく制御によって動作するコンピュータであってもよい。また、メトリック記憶部 111、相関モデル記憶部 112、及び、相関変化記憶部 113 は、それぞれ個別の記憶媒体でも、一つの記憶媒体によって構成されてもよい。

次に、本発明の第 1 の実施の形態における運用管理装置 100 の動作について説明する。

図 3 は、本発明の第 1 の実施の形態における運用管理装置 100 の処理を示すフローチャートである。

はじめに、運用管理装置 100 のメトリック収集部 101 は、被監視装置 200 上の監視エージェント 201 により計測された性能情報を収集し、メトリック記憶部 111 に保存する（ステップ S101）。

図 4 は、本発明の第 1 の実施の形態における性能系列情報 121 の例を示す図である。図 4 の例では、性能系列情報 121 は、メトリック x_{1} 、 x_{2} 、 x_{3} ...（以下、 x_{n} に続く文字は、添え字を示す）の計測値の時系列変化を含む。

例えば、メトリック収集部 101 は、図 4 の性能系列情報 121 を保存する。

次に、相関モデル生成部 102 は、メトリック記憶部 111 の性能系列情報 121 を参

10

20

30

40

50

照し、管理者等により指定された、所定のモデル化期間の性能情報をもとに、相関モデル 1 2 2 を生成し、相関モデル記憶部 1 1 2 に保存する（ステップ S 1 0 2）。

ここで、相関モデル 1 2 2 は、複数のメトリックの内の 2 つのメトリックの全組み合わせの各々についての、相関関数（または、変換関数）と閾値とを含む。

相関関数は、各メトリックの組み合わせについて、所定のモデル化期間（ t_s t t_e 、 t は時刻）の計測値の時系列データに対して成り立つ相関関係を、所定の近似式で記述したものである。メトリック x_i からメトリック x_j への相関関係についての相関関数を f_i, j とした場合、メトリックの組み合わせの内の一方のメトリック x_j の推定値は、他方のメトリック x_i の計測値から、相関関数 f_i, j を用いて、数 1 式のように表される。

【数 1】

$$x_j(t) \text{ の推定値} = f_{i,j}(x_i(t, t-1, t-2, \dots))$$

相関モデル生成部 1 0 2 は、所定のモデル化期間の性能系列情報 1 2 1 に基づいて、各メトリックの組み合わせについて、相関関数の係数を決定する。相関関数の係数は、特許文献 1 と同様に、上述のメトリックの計測値の時系列に対する、システム同定処理によって決定される。

閾値は、各メトリックの組み合わせについて、所定のモデル化期間における、相関関数による残差（変換誤差、または、予測誤差）の最大値である。ここで、残差は、相関関数を用いて算出されたメトリックの推定値と、当該メトリックの計測値との差分の絶対値である。

メトリック x_i からメトリック x_j への相関関係についての閾値 Th_i, j 、残差 $d_i, j(t)$ は、数 2 式により表現される。

【数 2】

$$Th_{i,j} = \max_{t_s \leq t \leq t_e} (d_{i,j}(t))$$

$$d_{i,j}(t) = \text{abs}(x_j(t) - f_{i,j}(x_i(t, t-1, t-2, \dots)))$$

なお、 $\text{abs}()$ は、括弧内の値の絶対値を示す。

ここで、被監視装置 2 0 0 が正常である限り、残差 $d_i, j(t)$ の値は極めて小さく、閾値 Th_i, j を超えないものと仮定する。

相関モデル生成部 1 0 2 は、特許文献 1 と同様に、所定のモデル化期間の残差をもとに、各メトリックの組み合わせについて、相関関数の重みを算出し、重みが所定値以上の相関関数とその閾値の集合を相関モデル 1 2 2 としてもよい。

図 5 は、本発明の第 1 の実施の形態における相関モデル 1 2 2 の例を示す図である。図 5 の例では、相関モデル 1 2 2 は、メトリック x_1 、 x_2 、 x_3 、... の間の相関関数と閾値を含む。

例えば、相関モデル生成部 1 0 2 は、図 4 の性能系列情報 1 2 1 をもとに、図 5 に示すような相関モデル 1 2 2 を生成する。

次に、相関変化分析部 1 0 3 は、各時刻において、メトリック収集部 1 0 1 により新たに収集された性能情報に対して、相関モデル 1 2 2 に含まれる相関関係の異常を検出し、相関変化情報 1 2 3 を相関変化記憶部 1 1 3 に保存する（ステップ S 1 0 3）。

ここで、相関変化分析部 1 0 3 は、特許文献 1 と同様に、新たに入力された性能情報について、相関モデル 1 2 2 に含まれる各相関関係に関し、異常（相関破壊）の有無を判定する。

相関関係の異常の度合いを示す異常度は、新たに入力された性能情報と相関モデル 1 2 2 とを用いて算出される残差により示される。相関変化分析部 1 0 3 は、残差、及び、閾値を用いて、メトリック x_i からメトリック x_j への相関関係についての異常の有無を、数 3 式により判定する。

10

20

30

40

50

【数 3】

$$d_{i,j}(t)/Th_{i,j} \geq 1 \quad \dots \quad \text{異常あり}$$

$$d_{i,j}(t)/Th_{i,j} < 1 \quad \dots \quad \text{異常なし}$$

図 6 は、本発明の第 1 の実施の形態における残差の例を示す図である。図 6 の例では、メトリック x_{j} の推定値と計測値に関する残差の閾値に対する割合が 1 を超えている場合、メトリック x_{i} からメトリック x_{j} への相関関係に異常があると判定されている。

図 7 は、本発明の第 1 の実施の形態における相関変化情報 1 2 3 の例を示す図である。相関変化情報 1 2 3 は、各メトリックの組み合わせについて、各時刻における残差の閾値に対する割合 ($d_{i,j}(t)/Th_{i,j}$)、及び、異常の有無を含む。

例えば、相関モデル生成部 1 0 2 は、新たに収集された性能情報に対して、図 5 に示す相関モデル 1 2 2 に含まれる相関関係の異常を検出し、図 7 のような相関変化情報 1 2 3 を保存する。

次に、異常スコア算出部 1 0 4 は、各時刻において、相関変化情報 1 2 3 をもとに、各メトリックの異常スコアを算出する (ステップ S 1 0 4)。

ここで、異常スコアは、各メトリックに関する相関関係の異常の度合い (残差)、及び、異常の継続度合いをもとに算出される。異常スコア算出部 1 0 4 は、メトリック x_{i} の異常スコア $S_{i}(t)$ を、数 4 式により算出する。

【数 4】

$$S_i(t) = \text{average}(s_{i,j}(t))$$

$$s_{i,j}(t) = d_{i,j}(t)/Th_{i,j} \times \text{step}(d_{i,j}(t)/Th_{i,j}) \times c_{i,j}(t)$$

$$\text{step}(y) = \begin{cases} 1 & \text{if}(y \geq 1) \\ 0 & \text{else} \end{cases}$$

ここで、 $\text{average}_{i}()$ は、メトリック x_{i} から相関関係がある他のメトリックとの間の相関関係のすべてに対して括弧内の値を算出し、その平均値を求めることを示す。例えば、メトリック x_{1} から x_{2} 、 x_{3} 、 x_{4} との間に相関関係がある場合、括弧内の値の、これらの相関関係についての平均値が算出される。

また、 $c_{i,j}(t)$ は、異常の継続度合いを示す異常継続度であり、時刻 t 以前の所定期間において、相関関係に異常が検出された期間の割合を示す。

$\text{step}(y)$ は、ステップ関数であり、数 3 式により算出される残差の閾値に対する割合が 1 未満、すなわち、相関関係が正常な場合、0 である。したがって、メトリック x_{i} から相関関係がある他のメトリックとの間の相関関係のすべてが正常な場合、異常スコア $S_{i}(t)$ は 0 である。

図 8 は、本発明の第 1 の実施の形態における異常スコアの算出過程を示す図である。図 9 は、本発明の第 1 の実施の形態における異常スコアの算出結果を示す図である。

例えば、異常スコア算出部 1 0 4 は、各時刻において、図 7 の相関変化情報 1 2 3 をもとに、図 8 のように異常継続度を算出し、図 9 のように異常スコアを算出する。

図 9 の異常スコアの算出結果では、例えば、時刻 1 2 : 3 0 において、メトリック x_{1} の異常スコアが、メトリック x_{2} 、 x_{3} の異常スコアよりも大きく、メトリック x_{1} の異常度が大きい、あるいは、異常が継続している可能性が高いことを示している。

次に、異常スコア算出部 1 0 4 は、各時刻において、各メトリックの異常スコアを含む解析結果 1 3 0 を生成し、監視装置 3 0 0 に出力する (ステップ S 1 0 5)。監視端末 3 0 0 の表示部 3 0 1 は、解析結果 1 3 0 を管理者等に表示する。

図 1 0 は、本発明の第 1 の実施の形態における解析結果 1 3 0 の例を示す図である。図 1 0 の例では、解析結果 1 3 0 は、異常相関率表示部 1 3 1、異常相関表示部 1 3 2、及

10

20

30

40

50

び、異常スコア表示部 133 を含む。

例えば、異常スコア算出部 104 は、図 10 の解析結果 130 を監視端末 300 に送信する。

異常相関率表示部 131 は、相関モデル 122 に含まれる相関関係の内、異常と判定された相関関係の割合の経時変化を示す。管理者等は、異常相関率表示部 131 を参照し、被監視装置 200 において、相関関係の異常が多発した時刻を把握することができる。

異常相関表示部 132 は、相関モデル 122 上で異常と判定された相関関係を示す。異常相関表示部 132 では、相関モデル 122 の各メトリックが、当該メトリックの識別子（名前）とともに円で示され、異常と判定された相関関係は、円と円を結ぶ実線で示される。異常相関表示部 132 は、例えば、異常相関率表示部 131 上で管理者等により指定された時刻に関して、異常と判定された相関関係を表示する。また、異常相関表示部 132 は、新たな性能情報が収集される度に、最新の収集時刻に関して、異常と判定された相関関係を表示してもよい。管理者等は、異常相関表示部 132 を参照し、被監視装置 200 において、異常が集中するメトリックを把握することができる。

異常スコア表示部 133 は、各メトリックの異常スコアを示す。各メトリックは、所定の矩形領域内に、当該メトリックの識別子とともに円で示され、異常スコアが大きいほど、円の大きさ（半径）は大きくなる。また、異常スコアが大きいほど、円は、矩形領域の上部に表示される。

異常スコア算出部 104 は、このように、異常スコアに応じて大きくなる円の大きさ、及び、前記異常スコアに応じて高くなる、矩形領域の底辺に対する垂直軸上の底辺からの高さを決定し、当該円が、当該大きさで、当該高さに表示されるように、異常スコア表示部 133 として表示されるデータを生成する。

異常スコア表示部 133 は、例えば、異常相関率表示部 131 上で管理者等により指定された時刻に関して、異常スコアを表示してもよい。また、異常スコア表示部 133 は、新たな性能情報が収集される度に、最新の収集時刻に関して、異常スコアを表示してもよい。

また、異常スコアは、数 4 式に示したように、相関関係の異常度（残差）に異常継続度を乗じることにより算出される。異常継続度は、異常スコアを算出する時刻以前の所定期間において、異常が検出された期間の割合であるため、異常の発生が続くと、時間の経過とともに異常スコアが次第に大きくなり、異常の発生が止まると、時間の経過とともに異常スコアが次第に小さくなる。このため、異常スコア表示部 133 では、メトリックに関する異常の発生が続くと、当該メトリックの円が次第に大きくなりつつ矩形領域の中を上昇し、異常の発生が止まると、当該メトリックの円が次第に小さくなりつつ矩形領域の中を下降する。すなわち、異常スコア表示部 133 では、各メトリックの異常スコアが、風船や泡のような浮力を得た物体の移動と同様な移動で表示される。なお、矩形領域中の円の上昇、下降は、よく知られるアルキメデスの原理に従っていてもよい。

図 10 の解析結果 130 では、時刻 12:30 において、メトリック x__1 を示す円が、他のメトリックの円より大きく、上部に表示されている。これにより、管理者等は、メトリック x__1 の異常度が大きい、あるいは、異常が継続している可能性が高いことを容易に把握することができる。

また、図 9 の異常スコアの算出結果では、メトリック x__1 の異常は、時刻 12:20 から時刻 12:40 の間継続し、異常スコアは時刻 12:30 において最大となる。この場合、異常スコア表示部 133 では、メトリック x__1 を示す円が、時刻 12:20 から時刻 12:30 に大きくなりつつ上昇し、時刻 12:30 から時刻 12:40 に小さくなりつつ下降する。これにより、管理者等は、メトリック x__1 の異常の継続が開始された、あるいは、継続が停止した可能性を容易に把握することができる。

以上により、本発明の第 1 の実施の形態の動作が完了する。

次に、本発明の第 1 の実施の形態の特徴的な構成を説明する。図 1 は、本発明の第 1 の実施の形態の特徴的な構成を示すブロック図である。

図 1 を参照すると、本発明の第 1 の実施の形態の運用管理装置 100 は、メトリック収

10

20

30

40

50

集部 101 と異常スコア算出部 104 とを含む。

ここで、メトリック収集部 101 は、システムにおける複数メトリックの計測値をそれぞれ時系列に収集する。また、異常スコア算出部 104 は、複数メトリックの計測値の各々の各時刻における異常の継続度合いを示す継続度をもとに、当該メトリックの異常スコアを算出し、出力する。

次に、本発明の第 1 の実施の形態の効果を記載する。

特許文献 1 に記載された技術では、ある時刻におけるメトリック x_{i} の異常スコアは、メトリック x_{i} から他のメトリックへの相関関係の内、当該時刻において異常と判定された相関関係の数をもとに算出され、異常メトリックのリストが異常スコアとともに表示される。管理者等は、異常メトリックのリストをもとに、異常スコアの高いメトリックの異常に対する対処を優先的に行う。この場合、管理者等は、当該メトリックの異常が継続的であるか、一時的であるかを把握できないため、当該メトリックの異常が一時的であっても優先的に対処する可能性がある。また、管理者等は、当該メトリックの異常が継続的であるか、一時的であるかを把握するために、例えば、異常メトリックのリストを、当該時刻の前後の時刻と比較する必要がある。

10

本発明の本発明の第 1 の実施の形態によれば、システムにおける継続性のあるメトリックの異常を容易に把握できる。その理由は、異常スコア算出部 104 が、メトリックの各時刻における異常の継続度合いを示す継続度をもとに、当該メトリックの異常スコアを算出するためである。また、異常スコア算出部 104 が、各メトリックの異常スコアを、異常スコアに応じた大きさ、及び、表示位置を有する図形で表示するためである。

20

これにより、管理者等は、継続的に発生しているメトリックの異常に対する対処を優先的に行うことができ、特許文献 1 の技術のみを用いる場合に比べ、システムの安定的な運用が期待できる。

また、これにより、管理者等は、メトリックの異常が継続的であるかどうかを調べるために、各時刻における異常メトリックのリストを比較する必要はなく、継続的な異常の把握における管理者等の負担軽減や、見逃しの防止が期待できる。

また、本発明の第 1 の実施の形態によれば、メトリックの異常の継続が開始された、あるいは、停止したことを容易に把握できる。その理由は、上述のように、異常スコア算出部 104 が、各メトリックの異常スコアを、異常スコアに応じた大きさ、及び、表示位置を有する図形で表示するためである。

30

(第 2 の実施の形態)

次に、本発明の第 2 の実施の形態について説明する。

本発明の第 2 の実施の形態においては、異常スコア算出部 104 が、異常検出の開始時刻が同一であるメトリックをグループ化する点において、本発明の第 1 の実施の形態と異なる。

本発明の第 2 の実施の形態の構成は、本発明の第 1 の実施の形態と同様となる。

次に、本発明の第 2 の実施の形態における運用管理装置 100 の動作について説明する。

図 11 は、本発明の第 2 の実施の形態における運用管理装置 100 の処理を示すフローチャートである。ここで、メトリック収集部 101 が性能情報を収集してから、異常スコア算出部 104 が、各メトリックの異常スコアを算出するまでの動作 (ステップ S201 ~ S204) は、本発明の第 1 の実施の形態の動作 (ステップ S101 ~ S104) と同様となる。

40

異常スコア算出部 104 は、上述のステップ S104 で、算出された各メトリックの異常スコアを参照し、異常検出の開始時刻が同一であるメトリックをグループ化する (ステップ S205)。ここで、異常検出の開始時刻が同一であるメトリックとは、異常スコアが 0 から 0 より大きい値に変わった時刻が同一のメトリックである。そして、異常スコア算出部 104 は、グループ化されたメトリックの異常スコアを合計することにより、各グループの異常スコアであるグループ異常スコアを算出する (ステップ S206)。

図 12 は、本発明の第 2 の実施の形態におけるグループ異常スコアの算出結果を示す図

50

である。

例えば、異常スコア算出部 104 は、各時刻において、図 9 の異常スコアをもとに、図 12 のグループ異常スコアを算出する。

この場合、異常スコア算出部 104 は、時刻 12 : 20 の異常スコアをもとに、当該時刻に異常検出が開始されたメトリック x_{11} のみからなるグループ A を生成する。グループ A は、時刻 12 : 40 まで継続する。また、異常スコア算出部 104 は、時刻 12 : 30 の異常スコアをもとに、当該時刻に異常検出が開始されたメトリック x_{12} と x_{13} からなるグループ B を生成する。グループ B は、時刻 12 : 30 で終了する。そして、異常スコア算出部 104 は、各グループに含まれるメトリックの異常スコアをもとに、図 12 のようにグループ異常スコアを算出する。

10

図 12 のグループ異常スコアの算出結果では、メトリック x_{12} の異常検出開始時刻と x_{13} の異常検出開始時刻とが同一であり、メトリック x_{12} の異常と x_{13} の異常とは、共通の異常事象に起因した異常の可能性があり、関連性が高いことを示している。また、メトリック x_{11} の異常検出開始時刻とメトリック x_{12} 、 x_{13} の異常検出開始時刻とは異なることを示している。

異常スコア算出部 104 は、各時刻において、各グループのグループ異常スコアを含む解析結果 140 を生成し、監視装置 300 に出力する (ステップ S207)。

図 13 は、本発明の第 2 の実施の形態における解析結果 140 の例を示す図である。図 13 の例では、解析結果 140 は、異常相関率表示部 141、異常相関表示部 142、及び、異常スコア表示部 143 を含む。

20

異常相関率表示部 141、異常相関表示部 142 は、本発明の第 1 の実施の形態の異常相関率表示部 131、異常相関表示部 132 と同様に、それぞれ、異常と判定された相関関係の割合、相関モデル 122 上での異常と判定された相関関係を示す。

異常スコア表示部 143 は、各グループのグループ異常スコアを示す。各グループは、所定の矩形領域内に、当該グループに含まれるメトリックの識別子とともに円で示され、本発明の第 1 の実施の形態と同様に、異常スコアが大きいほど、円の大きさは大きくなり、矩形領域の上部に表示される。

本発明の第 1 の実施の形態における、図 10 の解析結果 130 では、時刻 12 : 30 において、メトリック x_{12} 、 x_{13} は、それぞれ異常の継続性がなく、異常スコアがメトリック x_{11} に比べて低いため、メトリック x_{12} 、 x_{13} を示す円は、それぞれ、異常スコア表示部 133 の下部に小さく表示される。

30

一方、本発明の第 2 の実施の形態における、図 13 の解析結果 140 では、時刻 12 : 30 において、メトリック x_{11} からなるグループを示す円と同様に、メトリック x_{12} 、 x_{13} からなるグループを示す円が、他のグループの円より大きく、異常スコア表示部 143 の上部に表示される。

これにより、管理者等は、メトリック x_{12} 、 x_{13} の関連性が高いことと、それらの異常度の総和が大きい、あるいは、それらの異常が継続している可能性が高いこととを容易に把握することができる。

以上により、本発明の第 2 の実施の形態の動作が完了する。

次に、本発明の第 2 の実施の形態の効果を記載する。

40

ある一つの異常事象により複数のメトリックが異常な値となった場合、当該複数のメトリックの異常が同じ時刻に発生することがある。特許文献 1 の技術では、管理者等は、このような異常事象を把握するために、例えば、異常メトリックのリストの時間的な変化をもとに、異常メトリック間の時間的な関連性を確認し、同じ時刻に発生する異常メトリックを抽出する必要がある。また、異常事象を特定するために、異常が発生した相関関係に関してシグネチャマッチングを適用する方法も提案されている。しかしながら、未知の異常事象に対しては、相関関係に関するシグネチャの蓄積が無く、シグネチャマッチングを適用することはできない。

本発明の本発明の第 2 の実施の形態によれば、同じ時刻に発生する異常メトリックを容易に把握できる。その理由は、異常スコア算出部 104 が、異常検出の開始時刻が同一で

50

あるメトリックをグループ化し、各グループのグループ異常スコアを算出するためである。

これにより、管理者等は、共通の異常事象に起因した異常を、迅速に把握でき、システムのより安定的な運用が期待できる。

以上、実施の形態を参照して本願発明を説明したが、本願発明は上記実施の形態に限定されない。本願発明の構成や詳細には、本願発明のスコープ内で当業者が理解し得る様々な変更をすることができる。

例えば、本発明の実施の形態では、システムにおける性能指標をメトリックとし、メトリックの異常スコアを算出しているが、これに限らず、メトリックは、システムにおけるクライアントコンピュータからの要求量や、システムを介して単位時間あたりに処理される貨物の数等、システムに関して時系列で表される指標であれば、どのような指標でもよい。

また、本発明の実施の形態では、メトリックの異常度合いとして、当該メトリックに関する相関関係の異常（相関破壊）の度合いを用いているが、これに限らず、メトリックの異常度合いは、メトリックの値の所定の閾値に対する超過（閾値異常）の度合い等、他の異常度を用いてもよい。

また、本発明の実施の形態では、相関モデル122における閾値を、各メトリックの組み合わせについて、相関関数による残差の最大値をもとに算出しているが、閾値は、各メトリックの組み合わせについて定義された所定値、または、相関モデル122について定義された所定値でもよい。

また、本発明の実施の形態では、異常スコアを数4式により算出しているが、異常スコアが、メトリックの異常の継続度合いに応じて増加するのであれば、他の数式を用いて異常スコアを算出してもよい。例えば、数4式において、メトリックに関する相関関係の異常度（残差）を用いずに、当該メトリックに関する相関関係の異常継続度のみを用いて、異常スコアを算出してもよい。

また、本発明の実施の形態では、解析結果130、140において、異常スコアの大きさをメトリックを表す円の大きさ、及び、所定の矩形領域内での当該円が表示される高さで示しているが、これに限らず、異常スコアの大きさを示すことができれば、他の形状の図形や、他の表示位置により示してもよい。例えば、異常スコアの大きさを楕円や球等、円以外の図形の大きさにより表示してもよい。また、異常スコアの大きさを、円や台形等、矩形以外の所定の形状において定義された垂直軸上の所定の基準点からの高さで示してもよい。

また、異常スコアの大きさを、地平面に対する垂直軸上の、所定の基準点からの高さで示してもよい。この場合、表示部301が地平面に対して傾いて配置されていても、各メトリックを表す図形は、異常スコアに応じて、地平面に対して垂直方向に上昇または下降する。すなわち、各メトリックを表す図形の移動は、実際の浮力を得た物体の移動により近くなる。これにより、管理者等は、各メトリックの異常スコアの変化を、より容易に把握することができる。

この出願は、2011年8月24日に提出された日本出願特願2011-182261を基礎とする優先権を主張し、その開示の全てをここに取り込む。

【符号の説明】

【0009】

- 100 運用管理装置
- 101 メトリック収集部
- 102 相関モデル生成部
- 103 相関変化分析部
- 104 異常スコア算出部
- 111 メトリック記憶部
- 112 相関モデル記憶部
- 113 相関変化記憶部

10

20

30

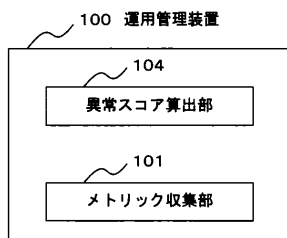
40

50

- 1 2 1 性能系列情報
- 1 2 2 相関モデル
- 1 2 3 相関変化情報
- 1 3 0 解析結果
- 1 3 1 異常相関率表示部
- 1 3 2 異常相関表示部
- 1 3 3 異常スコア表示部
- 1 4 0 解析結果
- 1 4 1 異常相関率表示部
- 1 4 2 異常相関表示部
- 1 4 3 異常スコア表示部
- 2 0 0 被監視装置
- 2 0 1 監視エージェント
- 3 0 0 監視端末

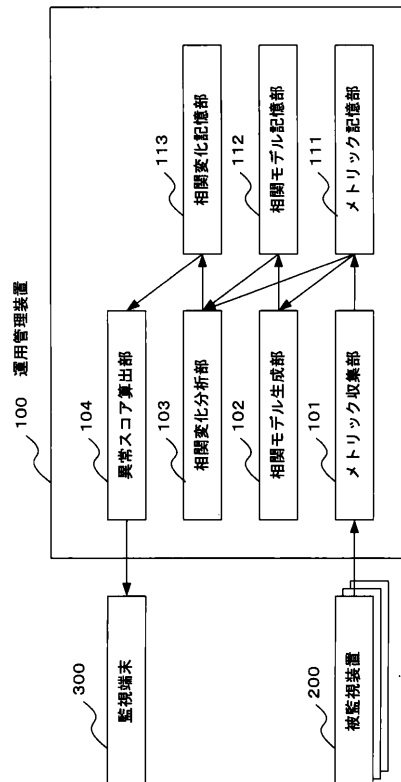
【図1】

図1



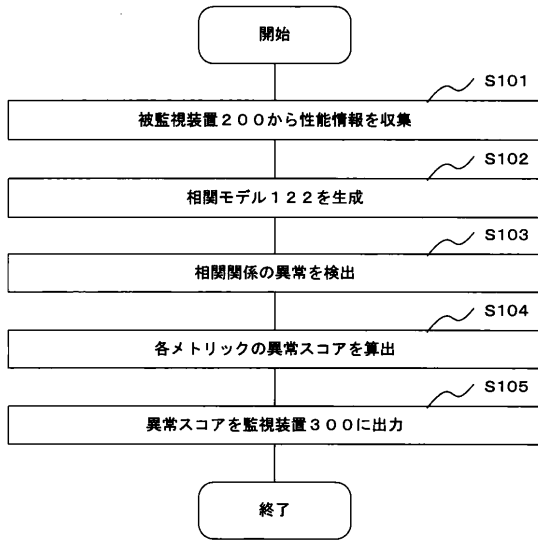
【図2】

図2



【 図 3 】

図3



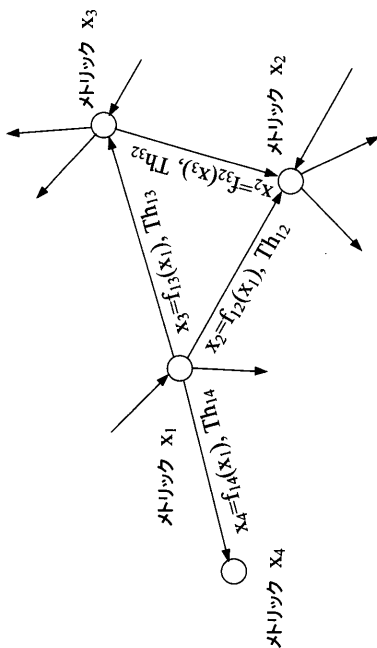
【 図 4 】

図4

時刻	メトリック x_1	メトリック x_2	メトリック x_3	...
2011/8/1 10:00	15	300	32	..
2011/8/1 10:10	18	361	35	..
2011/8/1 10:20	22	425	41	..
2011/8/1 10:30	20	398	40	..
..

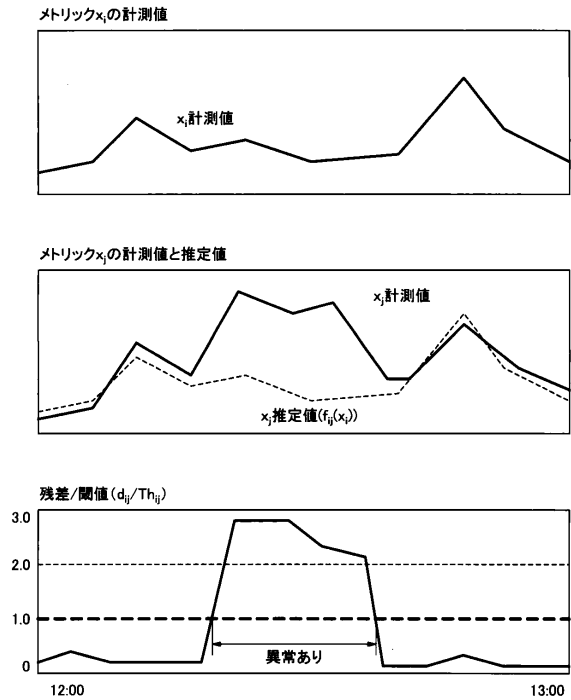
【 図 5 】

図5



【 図 6 】

図6



【 図 7 】

図 7

時刻		11:50	12:00	12:10	12:20	12:30	12:40	12:50
相関関係 X ₁ to X ₂	残差/閾値(d ₁₂ /Th ₁₂)	1.2	0.3	0.5	2.8	2.5	2.4	0.3
	異常有無	yes	no	no	yes	yes	yes	no
相関関係 X ₁ to X ₃	残差/閾値(d ₁₃ /Th ₁₃)	0.0	0.0	0.4	0.0	8.5	0.6	0.3
	異常有無	no	no	no	no	yes	no	no
相関関係 X ₁ to X ₄	残差/閾値(d ₁₄ /Th ₁₄)	0.0	0.0	0.0	0.0	0.6	0.0	0.0
	異常有無	no	no	no	no	no	no	no
:	:	:	:	:	:	:	:	:

【 図 9 】

図 9

時刻	11:50	12:00	12:10	12:20	12:30	12:40	12:50
メトリック X ₁	0.30	0.00	0.00	0.30	0.40	0.20	0.00
メトリック X ₂	0.00	0.00	0.00	0.00	0.23	0.00	0.00
メトリック X ₃	0.00	0.00	0.00	0.00	0.20	0.00	0.00

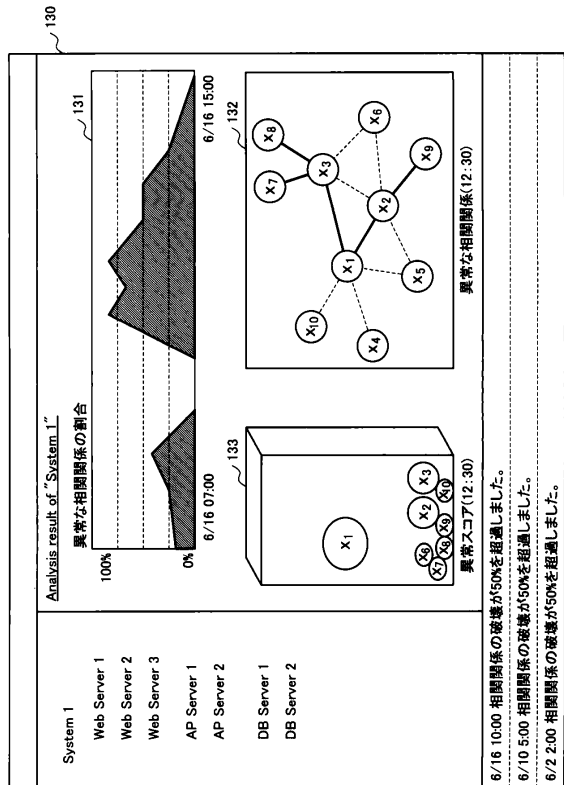
【 図 8 】

図 8

時刻		11:50	12:00	12:10	12:20	12:30	12:40	12:50
相関関係 X ₁ to X ₂	残差/閾値(d ₁₂ /Th ₁₂)	1.2	0.3	0.5	2.8	2.5	2.4	0.3
	異常有無	yes	no	no	yes	yes	yes	no
	異常継続度(C ₁₂)	1.00	0.83	0.67	0.67	0.67	0.67	0.5
相関関係 X ₁ to X ₃	S ₁₂	1.2	0.0	0.0	1.8	1.7	1.6	0.0
	残差/閾値(d ₁₃ /Th ₁₃)	0.0	0.0	0.4	0.0	8.5	0.6	0.3
	異常有無	no	no	no	no	yes	no	no
相関関係 X ₁ to X ₄	異常継続度(C ₁₃)	0.0	0.0	0.0	0.0	0.17	0.17	0.17
	S ₁₃	0.0	0.0	0.0	0.0	1.4	0.0	0.0
	残差/閾値(d ₁₄ /Th ₁₄)	0.0	0.0	0.0	0.0	0.6	0.0	0.0
相関関係 X ₁ to X ₄	異常有無	no	no	no	no	no	no	no
	異常継続度(C ₁₄)	0.0	0.0	0.0	0.0	0.0	0.0	0.0
	S ₁₄	0.0	0.0	0.0	0.0	0.0	0.0	0.0
:	:	:	:	:	:	:	:	:

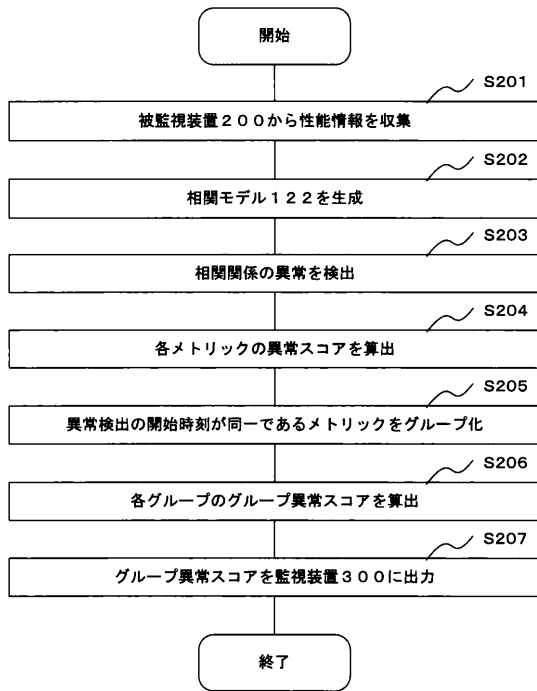
【 図 10 】

図 10



【 図 1 1 】

図11



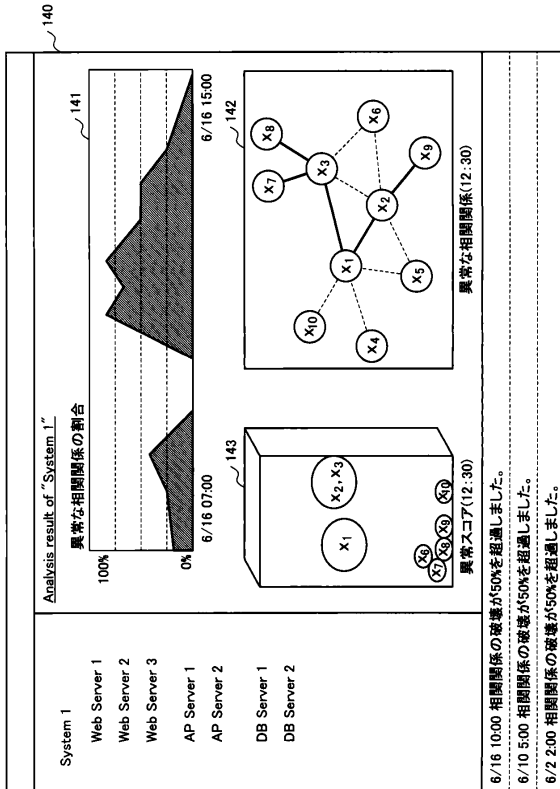
【 図 1 2 】

図12

時刻	12:00	12:10	12:20	12:30	12:40	12:50
グループA			X ₁	X ₁	X ₁	
異常スコア			0.30	0.40	0.20	
グループB				X ₂ X ₃		
異常スコア				0.43		

【 図 1 3 】

図13



フロントページの続き

(56)参考文献 国際公開第2010/032701(WO, A1)

特開2009-076056(JP, A)

特開2011-230634(JP, A)

特開平06-243064(JP, A)

特開2002-132340(JP, A)

国際公開第2011/065196(WO, A1)

特開2005-101854(JP, A)

目黒裕章他, 異常の継続性を考慮したネットワーク異常検出方式, 電子情報通信学会2007年
総合大会講演論文集 通信2, 日本, 社団法人電子情報通信学会, 2007年 3月 7日, p
. 160

(58)調査した分野(Int.Cl., DB名)

G06F 3/048

G06F 3/14

G06F 11/32

G06F 11/34

G05B 23/02