(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4980581号
(P4980581)

(45)発行日　平成24年7月18日(2012.7.18)　(24)登録日　平成24年4月27日(2012.4.27)

(51)Int.Cl.　　F I
G06F 15/00 (2006.01)　　G06F 15/00　470
G06F 11/34 (2006.01)　　G06F 11/34　S

請求項の数 13　(全 24 頁)

(21)出願番号　特願2005-114821 (P2005-114821)
(22)出願日　平成17年4月12日 (2005.4.12)
(65)公開番号　特開2005-327261 (P2005-327261A)
(43)公開日　平成17年11月24日 (2005.11.24)
審査請求日　平成20年4月2日 (2008.4.2)
(31)優先権主張番号　特願2004-122074 (P2004-122074)
(32)優先日　平成16年4月16日 (2004.4.16)
(33)優先権主張国　日本国(JP)

(73)特許権者　000191076
新日鉄ソリューションズ株式会社
東京都中央区新川２丁目２０番１５号
(74)代理人　100090273
弁理士　國分　孝悦
(72)発明者　坂井　良文
東京都中央区新川二丁目２０番１５号　新日鉄ソリューションズ株式会社内
(72)発明者　池田　佳隆
東京都中央区新川二丁目２０番１５号　新日鉄ソリューションズ株式会社内
(72)発明者　進藤　朋和
東京都中央区新川二丁目２０番１５号　新日鉄ソリューションズ株式会社内

最終頁に続く

(54)【発明の名称】性能監視装置、性能監視方法及びプログラム

(57)【特許請求の範囲】
【請求項１】
複数の情報処理装置が協調して動作する情報処理システムの性能を監視する性能監視装置であって、
前記複数の情報処理装置の稼働状況、及び、前記複数の情報処理装置間を接続する各通信回線のデータ通信状況を監視する監視手段と、
前記複数の情報処理装置のうちの一の情報処理装置の稼働状況に関する監視データと他の情報処理装置の稼働状況に関する監視データとの相関関係、前記複数の情報処理装置間を接続する各通信回線のうちの一の通信回線のデータ通信状況に関する監視データと他の通信回線のデータ通信状況に関する監視データとの相関関係、又は、前記複数の情報処理装置のうちの一の情報処理装置の稼働状況に関する監視データと当該情報処理装置と他の情報処理装置とを接続する通信回線のデータ通信状況に関する監視データとの相関関係に基づいて、前記情報処理システムに現在発生している障害を検知、又は、前記情報処理システムに将来障害が発生する可能性を予測する障害検知／予測手段とを有することを特徴とする性能監視装置。
【請求項２】
前記監視手段による監視データを蓄積する監視データ蓄積手段と、
前記監視データ蓄積手段から複数種類の監視データを読み出し、前記複数種類の監視データの相関関係を算出する相関関係算出手段とを更に有し、
前記障害検知／予測手段は、前記相関関係算出手段により算出される前記複数種類の監

視データの相関関係と、前記監視手段によって得られる現在の前記複数種類の監視データとに基づいて、前記情報処理システムに現在発生している障害を検知することを特徴とする請求項１に記載の性能監視装置。

【請求項３】

前記監視手段による監視データを蓄積する監視データ蓄積手段と、

前記監視データ蓄積手段から前記複数種類の監視データを読み出し、前記複数種類の監視データの相関関係を算出する相関関係算出手段とを更に有し、

前記障害検知／予測手段は、前記相関関係算出手段により算出される前記複数種類の監視データの相関関係と、前記監視手段によって現在までに得られた前記複数種類の監視データの推移とに基づいて、前記情報処理システムに将来障害が発生する可能性のあることを予測することを特徴とする請求項１に記載の性能監視装置。

【請求項４】

前記相関関係算出手段は、前記監視データ蓄積手段から読み出した前記複数種類の監視データに基づいて、前記情報処理システムの正常稼働時及び異常稼働時の少なくとも何れか一方の相関関係を算出し、前記障害検知／予測手段は、前記正常稼働時の相関関係又は前記異常稼働時の相関関係を用いて、前記情報処理システムに現在発生している障害を検知、又は、前記情報処理システムに将来障害が発生する可能性を予測することを特徴とする請求項２又は３に記載の性能監視装置。

【請求項５】

前記障害検知／予測手段は、前記情報処理システムに現在発生している障害を検知、又は、前記情報処理システムに将来障害が発生する可能性を予測したときに用いた相関関係の種類から、前記情報処理システムに現在発生している障害の原因又は前記情報処理システムに将来発生する可能性のある障害の原因を判別することを特徴とする請求項２乃至４の何れか１項に記載の性能監視装置。

【請求項６】

前記障害検知／予測手段により検知又は予測された前記情報処理システムに現在発生している発生した障害又は前記情報処理システムに将来障害が発生する可能性を報知する報知手段を更に有することを特徴とする請求項１乃至４の何れか１項に記載の性能監視装置。

【請求項７】

前記障害検知／予測手段により検知又は予測された前記情報処理システムに現在発生している障害又は前記情報処理システムに将来障害が発生する可能性と、同じく前記障害検知／予測手段によって判別された障害の原因とを報知する報知手段を更に有することを特徴とする請求項５に記載の性能監視装置。

【請求項８】

前記複数の情報処理装置が協調して動作する情報処理システムの情報処理装置及び前記複数の情報処理装置間の関連性に関する構成情報を格納する構成情報記憶手段と、前記格納された構成情報のうち前記監視手段で監視対象とする範囲を特定するための監視対象指定手段とを更に備え、

前記監視手段は、前記監視対象指定手段で特定された範囲について監視することを特徴とする請求項１乃至７の何れか１項に記載の性能監視装置。

【請求項９】

監視対象の前記情報処理装置、情報処理装置間を接続する各通信回線、前記情報処理装置を取り巻く環境のうち、少なくとも１つに発生した事象に関するイベントデータを格納するイベントデータ格納手段を更に備え、

前記監視手段は、前記情報処理装置の稼働状況及び前記複数の情報処理装置間を接続する各通信回線のデータ通信状況に加え、前記イベントデータを取得し、前記イベントデータ格納手段に格納することを特徴とする請求項１乃至８の何れか１項に記載の性能監視装置。

【請求項１０】

前記監視手段が取得した監視データを基に、イベントデータを生成するイベントデータ生成手段を更に備え、

前記イベントデータ生成手段は、生成したイベントデータを、前記イベントデータ格納手段に格納することを特徴とする請求項１乃至９の何れか１項に記載の性能監視装置。

【請求項１１】

前記障害検知／予測手段は、前記イベントデータ格納手段に格納されたイベントデータに関連する相関関係に基づいて前記情報処理システムに将来障害が発生する可能性を予測することを特徴とする請求項９又は１０に記載の性能監視装置。

【請求項１２】

複数の情報処理装置が協調して動作する情報処理システムの性能を監視する性能監視装置による性能監視方法であって、

前記複数の情報処理装置の稼働状況、及び、前記複数の情報処理装置間を接続する各通信回線のデータ通信状況を監視する監視ステップと、

前記複数の情報処理装置のうちの一の情報処理装置の稼働状況に関する監視データと他の情報処理装置の稼働状況に関する監視データとの相関関係、前記複数の情報処理装置間を接続する各通信回線のうちの一の通信回線のデータ通信状況に関する監視データと他の通信回線のデータ通信状況に関する監視データとの相関関係、又は、前記複数の情報処理装置のうちの一の情報処理装置の稼働状況に関する監視データと当該情報処理装置と他の情報処理装置とを接続する通信回線のデータ通信状況に関する監視データとの相関関係に基づいて、前記情報処理システムに現在発生している障害を検知、又は、前記情報処理システムに将来障害が発生する可能性を予測する障害検知／予測ステップとを有することを特徴とする性能監視方法。

【請求項１３】

請求項１２に記載の性能監視方法をコンピュータに実行させるためのプログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、複数の情報処理装置が協動して動作する情報処理システムの稼働を監視し、情報処理システムの障害発生を検知又は予測する性能監視装置、性能監視方法及びプログラムに関するものである。

【背景技術】

【０００２】

従来、装置の障害を監視する手法、或いは運用管理を行う手法が提案されている。例えば、特許文献１には、障害発生予測アルゴリズムと障害検出用のパラメータを格納したテーブルをメモリに格納しておき、また、顧客名・製品名・モデル番号・保守履歴・障害履歴などをデータベースに格納しておき、障害発生予測アルゴリズムを用いてデータベースに格納しておき、障害発生予測アルゴリズムを用いてデータベースに格納された各情報が、障害発生条件を満たせば通知メールを発信するシステムが開示されている。また、特許文献２には、ハードウェア状態・プログラムの稼働状況を能動的に採取して解析を行い、運用支障をきたす危険がある場合には障害を回避する指示を与えるための装置が開示されている。

【０００３】

【特許文献１】特開２００１－８４２７６号公報

【特許文献２】特開平９－３１１７３３号公報

【発明の開示】

【発明が解決しようとする課題】

【０００４】

特許文献１に開示される発明は、特定の装置の監視をして障害発生を予測するものであるが、監視対象が装置自体のみであることを想定している。例えば、ウェブサーバ、アプリケーションサーバ及びデータベースサーバから成る３層構造のウェブシステムなど、複

数の機能が協調して動作しているシステムの場合、装置間における処理の負荷分散やトランザクション発生数に対してメモリ等のリソースが不足している等、様々な原因による障害が予測されるが、特許文献１に開示される発明は、その点については全く考慮されていない。

【０００５】

また、特許文献２に開示される発明は、知識ベース格納装置に格納された採取すべきハードウェア／ソフトウェアの稼働情報に基づいて、情報採取手段が情報を採取し、採取された情報を用いて経験則から対処すべき指示を出力するものである。特許文献２に開示された発明の場合も、監視対象はコンピュータ自体のみであり、複数のコンピュータが協調して動作しているようなシステムで発生し得る上記の障害については何ら説明がなされていない。

【０００６】

以上のように、従来の監視・運用管理システムは個々のコンピュータを監視すること自体はできたものの、今日のような複数のコンピュータが協調して動作し、協調して動作することによる複雑化した障害発生の予測は想定されておらず、複雑なコンピュータシステムを対象とする監視においては、障害の検出・予測や原因の切りわけが難しい、あるいは手間がかかる場合が多かった。

【０００７】

従って、本発明の目的は、例えば、情報処理装置間における処理の負荷分散やトランザクション発生数に対してメモリ等のリソースが不足している等、複数の情報処理装置が協調して動作する情報処理システムに発生し得る複雑化した障害を精度よく検知又は予測可能とすることにある。

【課題を解決するための手段】

【０００８】

本発明の性能監視装置は、複数の情報処理装置が協調して動作する情報処理システムの性能を監視する性能監視装置であって、前記複数の情報処理装置の稼働状況、及び、前記複数の情報処理装置間を接続する各通信回線のデータ通信状況を監視する監視手段と、前記複数の情報処理装置のうちの一の情報処理装置の稼働状況に関する監視データと他の情報処理装置の稼働状況に関する監視データとの相関関係、前記複数の情報処理装置間を接続する各通信回線のうちの一の通信回線のデータ通信状況に関する監視データと他の通信回線のデータ通信状況に関する監視データとの相関関係、又は、前記複数の情報処理装置のうちの一の情報処理装置の稼働状況に関する監視データと当該情報処理装置と他の情報処理装置とを接続する通信回線のデータ通信状況に関する監視データとの相関関係に基づいて、前記情報処理システムに現在発生している障害を検知、又は、前記情報処理システムに将来障害が発生する可能性を予測する障害検知／予測手段とを有することを特徴とする。

【０００９】

本発明の性能監視方法は、複数の情報処理装置が協調して動作する情報処理システムの性能を監視する性能監視装置による性能監視方法であって、前記複数の情報処理装置の稼働状況、及び、前記複数の情報処理装置間を接続する各通信回線のデータ通信状況を監視する監視ステップと、前記複数の情報処理装置のうちの一の情報処理装置の稼働状況に関する監視データと他の情報処理装置の稼働状況に関する監視データとの相関関係、前記複数の情報処理装置間を接続する各通信回線のうちの一の通信回線のデータ通信状況に関する監視データと他の通信回線のデータ通信状況に関する監視データとの相関関係、又は、前記複数の情報処理装置のうちの一の情報処理装置の稼働状況に関する監視データと当該情報処理装置と他の情報処理装置とを接続する通信回線のデータ通信状況に関する監視データとの相関関係に基づいて、前記情報処理システムに現在発生している障害を検知、又は、前記情報処理システムに将来障害が発生する可能性を予測する障害検知／予測ステップとを有することを特徴とする。

【００１０】

本発明のプログラムは、前記性能監視方法をコンピュータに実行させることを特徴とする。

【発明の効果】

【００１１】

本発明によれば、情報処理システムを構成する複数の情報処理装置の稼働状況、及び、当該複数の情報処理装置を接続する各通信監視のデータ通信状況を監視することにより、例えば、情報処理装置間における処理が正常に動作している場合、発生するトランザクション量に対して本来使うべきリソースよりも多いあるいは少ないリソースしか使用できていないことから、障害の発生を検出、予測したり、その現象がどのサーバでおきているかを検出することによって、複数の情報処理装置からなるシステムのどの部分で障害がおきているかを知ることができ、複数の情報処理装置が協調して動作する情報処理システムに発生し得る複雑化した障害を精度よく検知又は予測することが可能となる。

【発明を実施するための最良の形態】

【００１２】

以下、本発明を適用した好適な第一の実施形態を、添付図面を参照しながら詳細に説明する。

【００１３】

図１は、本発明の第一の実施形態に係る性能監視システムの構成を概略的に示した図である。図１において、本実施形態の性能監視システムは、性能監視装置１０、Ｗｅｂサーバ１１、ＡＰ（アプリケーション）サーバ１２、及び、ＤＢ（データベース）サーバ１３により構成されている。性能監視装置１０は、Ｗｅｂサーバ１１、ＡＰサーバ１２及びＤＢサーバ１３から構成される情報処理システムとＬＡＮ（Local Area Network）等の通信回線で接続され、この通信回線を介して各サーバの状態を監視することが可能である。

【００１４】

本実施形態の性能監視装置１０は、蓄積サーバ１０１と分析サーバ１０２によって構成され、蓄積サーバ１０１は、各サーバに対する監視により夫々のＣＰＵやメモリ等のリソースの使用量、使用率を示すリソース使用状況データ及び処理履歴を示すログデータ等を取得するとともに、Ｗｅｂサーバ１１、ＡＰサーバ１２及びＤＢサーバ１３間を接続する各通信回線で通信されるトランザクションのスループット、処理名等を示すトランザクションデータを取得し、夫々を監視データとして内部に蓄積する。また、サーバに対する監視或いは通信回線に対する監視いずれからも取得できる情報として、ある処理命令に対する応答時間なども蓄積する。分析サーバ１０２は、蓄積サーバ１０１に蓄積された監視データに基づいて、情報処理システムに現在発生している障害を検知、又は、情報処理システムに将来発生する可能性のある障害を予測する。

【００１５】

このように、本実施形態では、性能監視装置１０の監視対象を複数の装置夫々の稼働状況、装置間を接続する各通信回線のデータ通信状況としていることにより、複数の情報処理装置が協動して動作する情報処理システムに発生する障害の検知又は予測を精度よく行うことが可能となる。

【００１６】

図２は、性能監視装置１０（蓄積サーバ１０１、分析サーバ１０２）内のコンピュータシステムのハードウェア構成を概略的に示した図である。

図２に示すように、上記コンピュータシステム１２００は、ＣＰＵ１２０１、ＲＯＭ１２０２、ＲＡＭ１２０３、キーボード（ＫＢ）１２０９のキーボードコントローラ（ＫＢＣ）１２０５、表示部としてのＣＲＴディスプレイ（ＣＲＴ）１２１０のＣＲＴコントローラ（ＣＲＴＣ）１２０６、ハードディスク（ＨＤ）１２１１及びフレキシブルディスク（ＦＤ）１２１２のディスクコントローラ（ＤＫＣ）１２０７、並びに、ネットワーク１２２０との接続のためのネットワークインタフェースカード（ＮＩＣ）１２０８が、システムバス１２０４を介して互いに通信可能に接続された構成としている。

【００１７】

ＣＰＵ１２０１は、ＲＯＭ１２０２或いはＨＤ１２１１等から情報を読み出すソフトウェアを実行することで、システムバス１２０４に接続された各構成部を統括的に制御し、後述する図４及び図５に示す処理等を実行する。

【００１８】

ＲＡＭ１２０３は、ＣＰＵ１２０１の主メモリ或いはワークエリア等として機能する。ＫＢＣ１２０５は、ＫＢ１２０９や図示していないポインティングデバイス等からの指示入力を制御する。ＣＲＴＣ１２０６は、ＣＲＴ１２１０の表示を制御する。ＤＫＣ１２０７は、ブートプログラム、種々のアプリケーション、編集ファイル、ユーザファイル及びネットワーク管理プログラムへのアクセスを制御する。ＮＩＣ１２０８は、Ｗｅｂサーバ１１、ＡＰサーバ１２、ＤＢサーバ１３及び各サーバ間を接続する通信回線と本性能監視装置１０間のデータの送受信を制御する。

【００１９】

図３は、性能監視装置１０（蓄積サーバ１０１及び分析サーバ１０２）の機能構成を示すブロック図である。

性能監視装置１０は、監視データ取得部１００１、監視データ記憶部１００２、異常検出部１００３、相関関係抽出部１００４、相関関係記憶部１００５、障害検知／予測部１００６及び報知部１００７により構成される。監視データ取得部１００１は、例えばＣＰＵ１２０１、ＲＯＭ１２０２内のプログラム及びＮＩＣ１２０８により構成され、異常検出部１００３、相関関係抽出部１００４及び障害検知／予測部１００６は、例えばＣＰＵ１２０１及びＲＯＭ１２０２内のプログラムにより構成され、監視データ記憶部１００１及び相関関係記憶部１００４は、例えばＲＡＭ１２０３やＨＤ１２１１の記録媒体により構成され、報知部１００７は、例えばＣＰＵ１２０１、ＣＲＴＣ１２０６及びＣＲＴ１２１０によって構成される。

【００２０】

監視データ取得部１００１は、Ｗｅｂサーバ１１、ＡＰサーバ１２及びＤＢサーバ１３からリソース使用状況データ及びログデータ、上記サーバ間を接続する通信回線からトランザクションデータ等を取得する。図示していないが、ＡＰサーバ１２やＤＢサーバ１３のログデータは、ＡＰサーバ１２やＤＢサーバ１３内に保存されていたり、或いは別途設けられるログ保存用サーバに保存されていたりするが、監視データ取得部１００１は、通信回線を介してｆｔｐなどによりこのログデータを取得する。なお、ＡＰサーバ１２やＤＢサーバ１３がログデータを送信する機能を設けていれば、監視データ取得部１００１はログデータを受動的に取得するという方法をとっても良い。監視データ記憶部１００２は、監視データ取得部１００１によってこれまで取得された監視データを蓄積する。

【００２１】

異常検出部１００３は、監視データ記憶部１００２から監視データを読み込み、読み込んだ監視データに基づいて情報処理システムの異常を検出する。相関関係抽出部１００４は、監視データ記憶部１００２から２種類の監視データを読み込み、その相関関係を求める。この相関関係の詳細については後述するが、相関関係抽出部１００４では、情報処理システムが正常に稼働しているときの相関関係や、情報処理システムに異常が発生したときの相関関係が求められる。なお、１組の監視データに基づいて作成される相関関係は、正常時も異常時も複数あって良い。相関関係記憶部１００５は、相関関係抽出部１００４によって求められた相関関係をそれぞれにＩＤを付与して記憶する。

【００２２】

障害検知／予測部１００６は、情報処理システムに現在発生している障害の検知、又は、情報処理システムに将来発生する可能性のある障害の予測を行う。即ち、障害検知／予測部１００６は、情報処理システムが正常に稼働しているときの上記２種類の監視データの相関関係と、監視データ記憶部１００２に蓄積される最新の上記２種類の監視データとを比較することにより、情報処理システムに現在発生している障害を検知したり、情報処理システムに異常が発生したときの上記２種類の監視データの相関関係と、最近得られた上記２種類の監視データの相関関係との類似性から情報処理システムに将来発生する可能

性のある障害を予測する。

【００２３】

報知部１００７は、障害検知／予測部１００６により障害発生が検知された場合、又は、障害発生が予測された場合にそれらの内容を報知する。本実施形態の報知方法としては、報知部１００７が画面表示により検知内容又は予測内容をオペレータに報知するが、他の実施形態として、電子メール等による報知方法でもよい。

【００２４】

尚、本実施形態においては、監視データ取得部１００１及び監視データ記憶部１００２が蓄積サーバ１０１内の構成、異常検出部１００３、相関関係抽出部１００４、相関関係記憶部１００５、障害検知／予測部１００６及び報知部１００７が分析サーバ１０２内の構成であることを想定しているが、他の実施形態として、性能監視装置１０の構成を蓄積サーバ１０１及び分析サーバ１０２の二つのサーバに分けることなく、一つのサーバ内に集約した構成としてもよい。

【００２５】

次に、性能監視装置１０の動作について図４及び図５のフローチャートを用いて詳細に説明する。本発明を適用した第一の実施形態における性能監視システムでは、大きく分けて次の５つの処理がある。（１）監視データ取得部１００１が取得した監視データを監視データ記憶部１００２に記憶させる処理。（２）監視データ記憶部１００２から読み込んだデータに基づいて相関関係を求める（生成する）処理。（３）相関関係抽出部１００４が求めた相関関係を相関関係記憶部１００５に記憶させる処理。この（１）～（３）の処理は監視目的に応じてバッチ処理或いはリアルタイム処理で行われる。更に、（４）監視データと相関関係或いは相関関係どうしを比較する処理。そして（５）監視データと相関関係から異常検知する処理などがある。図４は、監視データ取得部１００１、異常検出部１００３及び相関関係抽出部１００４の動作を示すフローチャートであり、図５は、障害検知／予測部１００６の動作を示すフローチャートである。

【００２６】

なお、監視データ記憶部１００２に（１）で蓄積された各種データは、その後の各処理で用いられた後も原則として消去せずに残しておくことが好ましい。例えば後述する第二の実施形態で説明する通り、システムの構成が変更されたときなどに、過去データとの比較を行う上で、多くのデータが使用できるという利点がある。

【００２７】

先ず、図４を参照しながら、監視データ取得部１００１、異常検出部１００３及び相関関係抽出部１００４の動作について説明する。図４では、上述した（１）や（３）の記憶させる処理と他の処理とを並行して説明するが、必ずしも並行して行う必要はない。まず最初に監視データ取得部１００１は、Ｗｅｂサーバ１１、ＡＰサーバ１２、ＤＢサーバ１３及び各サーバを接続する通信回線の監視データを取得し、取得した監視データを監視データ記憶部１００２に蓄積させていく（ステップＳ４０１、Ｓ４０２）。

【００２８】

続いて、異常検出部１００３は、監視データ記憶部１００２から２種類の監視データを読み込んだ後、それらの２種類の監視データに対応する正常時の相関関係を相関関係記憶部１００５から読み込み、監視データ記憶部１００２から読み込んだ当該２種類の監視データと、相関関係記憶部１００５から読み込んだ正常時の相関関係とを比較することにより情報処理システムの異常を検出する（ステップＳ４０３）。これは監視目的に応じて任意の周期で監視データと相関関係を読み込んで比較処理する。なお、ここで異常検出部１００３によって監視データ記憶部１００２から読み込まれる２種類の監視データは、監視データ取得部１００１によって同時に取得されたデータであることが前提である。また、ここで異常検出部１００３によって用いられる正常時の相関関係とは、当該２種類の監視データに関して一つ前のステップＳ４０６の処理で求められた正常時の相関関係である。

【００２９】

情報処理システムの異常が検出された場合、相関関係抽出部１００４は、監視データ記

憶部１００２から読み込んだ過去の当該２種類の監視データから当該２種類の監視データの相関関係を算出する（ステップＳ４０３／ＹＥＳ、Ｓ４０４）。続いて、相関関係抽出部１００４は、算出した相関関係を異常時の相関関係として相関関係記憶部１００５に相関関係ＩＤと共に記憶させる（ステップＳ４０７）。このとき、相関関係記憶部１００５内においては、当該２種類の監視データについて、一つ前のステップＳ４０４の処理において求められた異常時の相関関係が今回のステップＳ４０４の処理において求められた異常時の相関関係に更新される。従って、本実施形態では、情報処理システムの稼働に追従して常に新しい異常時の相関関係を、後述のステップＳ５０５におけるエラー予測処理に用いることが可能となる。

【００３０】

一方、ステップＳ４０３において異常が検出されなかった場合、相関関係抽出部１００４は、当該２種類の監視データの取得開始から所定時間が経過したか否かを判断する（ステップＳ４０３／ＮＯ、Ｓ４０５）。

【００３１】

当該２種類の監視データの取得開始から所定時間が経過している場合、相関関係抽出部１００４は、取得開始から所定時間が経過するまでに監視データ記憶部１００２から読み込んだ当該２種類の監視データから当該２種類の監視データの相関関係を算出し、正常時の相関関係として相関関係記憶部１００５に相関関係ＩＤと共に記憶させる（ステップＳ４０５／ＹＥＳ、ステップＳ４０６、Ｓ４０７）。このとき、相関関係記憶部１００５内においては、当該２種類の監視データに関し、一つ前のステップＳ４０６の処理において求められた正常時の相関関係が今回のステップＳ４０６の処理において求められた正常時の相関関係に更新される。従って、本実施形態では、情報処理システムの稼働に追従して常に新しい正常時の相関関係を、後述のステップＳ５０３におけるエラー検知処理に用いることが可能となる。

【００３２】

ステップＳ４０５において、当該監視データの取得開始から所定時間が経過していない場合には、ステップＳ４０１の監視データの取得処理に戻る。以上のように、本実施形態では監視対象のシステムに特に異常がない限り常に正常時としての相関関係が蓄積されていき、異常が発生したときには、異常時の相関関係が新たに生成され蓄積されていく。

【００３３】

次に、図５を参照しながら、障害検知／予測部１００６の動作について説明する。障害検知／予測部１００６は、監視データ記憶部１００２から２種類の監視データを読み込む（ステップＳ５０１）。なお、ここで読み込まれる２種類の監視データは、監視データ取得部１００１によって同時に取得されたデータであり、監視データ記憶部１００２において記憶される当該２種類の監視データのうち最新のデータであることが前提である。そして、監視データ記憶部１００２から監視データを読み込む周期は監視目的に応じて任意に設定できるが、障害検知という目的からすればできるだけリアルタイム性が求められる。従って監視データ取得部１００１がデータを取得して監視データ記憶部１００２に記憶されたらすぐに読み込むよう設定することが好ましい。

【００３４】

続いて、障害検知／予測部１００６は、当該２種類の監視データと、相関関係記憶部１００５に記憶される当該２種類の監視データに対応する正常時の相関関係とを比較し、その比較結果に基づいて情報処理システムにエラー（異常）が発生したか否かを判断する（ステップＳ５０２、Ｓ５０３）。

【００３５】

ステップＳ５０３において、障害検知／予測部１００６が情報処理システムにエラーが発生したと判断した場合、報知部１００７はその内容をオペレータに対して報知する（ステップＳ５０３／ＹＥＳ、Ｓ５０６）。

【００３６】

一方、障害検知／予測部１００６は、ステップＳ５０３において情報処理システムにエ

ラーが発生したと判断しなかった場合には、所定回数前のステップＳ５０１の処理から今回のステップＳ５０１の処理までに得られた複数の当該２種類の監視データに基づいて、当該２種類の監視データの相関関係を求め、この相関関係と相関関係記憶部１００５に蓄積されている当該２種類の監視データの過去の相関関係とを用いてエラーが発生する可能性があるか否かを予測をする（ステップＳ５０３／ＮＯ、Ｓ５０４、Ｓ５０５）。

【００３７】

ステップＳ５０５において、障害検知／予測部１００６が情報処理システムに将来エラーが発生する可能性があると判断した場合、報知部１００７はその内容をオペレータに対して報知する（ステップＳ５０５／ＹＥＳ、Ｓ５０７）。

【００３８】

一方、障害検知／予測部１００６が上記２つの相関関係が類似していないと判断した場合、処理はステップＳ５０１の監視データの読み込みに戻る（ステップＳ５０５／ＮＯ、Ｓ５０１）。

【００３９】

ここで、ステップＳ５０３におけるエラー検知処理について図６を用いて具体的に説明する。　図６では、上記２種類の監視データとしてトランザクションデータとリソース使用状況データとが用いられ、トランザクションデータにより示されるスループット、リソース使用状況データにより示されるディスクＩ／Ｏ量から算出された相関関係６０１を示している。なお、図６中の「×」印は、上記２種類の監視データで示されるスループット、ディスクＩ／Ｏ量の関係からプロットされる点であり、上記２種類の監視データ毎に対応する点として、１２個の点がプロットされている。また、ハッチングされた範囲領域６０４は、正常時の相関関係６０１を基準としたときに正常とみなす範囲であり、相関関係に応じて予め定められている。なお、図６においては、相関関係６０１と平行して範囲領域６０４が設定されているが、必ずしも相関関係を中心とした一定幅で領域を設定する必要はない。

【００４０】

相関関係抽出部１００４は、上記１２個の点の近似式（図６中の直線に相当）を求める。ここで求められる近似式がスループットとディスクＩ／Ｏ量との相関関係６０１である。この相関関係６０１がステップＳ４０６において求められる正常時の相関関係であるとすると、ステップＳ５０１において読み込まれる２種類の監視データに対応して（当該２種類の監視データにより示されるスループット、ディスクＩ／Ｏ量に対応して）プロットされる点が図６中の６０２である場合、即ち、相関関係６０１を基準とする所定幅の範囲領域６０４外であって、当該範囲領域６０４の上方にステップＳ５０１にて読み込まれる２種類の監視データがプロットされるような場合、障害検知／予測部１００６は、正常時の相関関係６０１を基準にして、現在、スループットに対してディスクＩ／Ｏ量が多過ぎると判断し、ディスクＩ／Ｏ量の多さを原因とした情報処理システムのエラーを検知することができる。報知部１００７は、画面表示によりオペレータに対してシステムのエラーとその原因（スループットに対してディスクＩ／Ｏ量が多過ぎる）とを報知する。

【００４１】

また、ステップＳ５０１において読み込まれた２種類の監視データに対応して（当該２種類の監視データにより示されるスループット、ディスクＩ／Ｏ量に対応して）プロットされる点が図６中の６０３である場合、即ち、相関関係６０１を基準とした所定幅の範囲領域６０４外であって、当該範囲領域６０４の下方にステップＳ５０１にて読み込まれる２種類の監視データがプロットされるような場合、障害検知／予測部１００６は、正常時の相関関係６０１を基準にして、現在、ディスクＩ／Ｏ量に対してスループットが高過ぎると判断し、スループットの高さを原因とした情報処理システムのエラーを検知することができる。報知部１００７は、画面表示によりオペレータに対してシステムのエラーとその原因（ディスクＩ／Ｏ量に対してスループットが高過ぎる）とを報知する。

【００４２】

なお、上述した実施形態では、どのような処理に対するスループットであるかの内容は

限定していない。したがって、特定の処理に関するスループットであってもよいし、或いは、いくつかの処理を足し合わせたスループットでも良い。例えば処理ａ、処理ｂ、処理ｃ毎にスループットとディスクのＩ／Ｏ量との相関関係を求めておき、これら３つの相関関係の足し合わせた量を、当該スループットにおける基準のディスクＩ／Ｏ量として扱うようにしても良い。

【００４３】

また、本実施形態の性能監視システムは、複数のサーバを監視していることを特徴としているので、オペレータに対しては、どのサーバの挙動に基づいてエラーを検知したかを含めてシステムのエラーとその原因を報知するようにする。

【００４４】

本実施形態では、監視データ取得部１００１によって取得される監視データに基づいて他にも様々なエラー検知を行うことが可能である。例えば、或るサーバへのトランザクションを監視して得られるトランザクションデータと、当該サーバのリソース使用状況データとを用い、トランザクションデータにより示されるスループット、リソース使用状況データにより示されるＣＰＵ使用率に基づいて、当該サーバのスループットが高くなっているにも拘わらずＣＰＵ使用率が低い、又は、当該サーバのスループットが低いにも拘わらずＣＰＵ使用率が高いことを情報処理システムのエラー原因として判断することができる。

【００４５】

また、異なる２つのサーバのリソース使用状況データに基づいて次のようなエラー原因を把握することが可能となる。例えば、正常な稼働状態では、Ｗｅｂサーバ１１とＡＰサーバ１２とのＣＰＵ使用率はＮ：Ｍであるはずなのに、Ｗｅｂサーバ１１から得られるリソース使用状況データにより示されるＣＰＵ使用率、ＡＰサーバ１２から得られるリソース使用状況データにより示されるＣＰＵ使用率に基づいて、Ｗｅｂサーバ１１の使用率のみが高い場合には、情報処理システムのエラー原因がＡＰサーバ１２における障害発生であることが判断できる。

【００４６】

また、或るサーバのリソース使用状況データとログデータとに基づいて次のようなエラー原因を把握することが可能となる。例えば、リソース使用状況データにより示されるＣＰＵ使用率、ログデータから判断される処理１の発生頻度に基づいて、当該サーバのＣＰＵ利用率が異常に高い値をとる時間帯で通常より処理１の発生頻度が高くなっている場合には、情報処理システムのエラー原因が、その時間帯において当該サーバ内の処理１の発生頻度が高くなっていることであることが判断できる。

【００４７】

さらに、異なる２つのサーバのログデータに基づいて次のようなエラー原因を把握することが可能となる。例えば、Ｗｅｂサーバ１１のログデータから判断されるＷｅｂサーバ１１のスループット、ＡＰサーバ１２のログデータから判断されるＡＰサーバ１２のスループットに基づいて、Ｗｅｂサーバ１１のスループットが増加傾向であるのに拘わらずＡＰサーバ１２のスループットが増加しない場合には、ＡＰサーバ１２に問題があるため、ＡＰサーバ１２を利用する処理が滞っており、Ｗｅｂサーバ１１のみを利用する処理の比率が増えているということを検出できる。

【００４８】

次に、図５のステップＳ５０５のエラー予測処理を図７を用いて具体的に説明する。

図７は、異なるサーバ（ここでは、Ｗｅｂサーバ１１とＡＰサーバ１２）のログデータを用い、それらのログデータにより判断されるＷｅｂサーバ１１の処理１のスループット、ＡＰサーバ１２の処理２のスループットに基づいて算出された相関関係を示している。範囲領域７０１は、Ｗｅｂサーバ１１の処理１の発生数に対してＡＰサーバ１２の処理２の発生数が正常時に求められたときの正常とみなされる範囲を示している。

【００４９】

図７においては、相関関係７０２として、相関関係１００５に蓄積されている過去の相

関関係として、７０２（ａ）と７０２（ｂ）がある。そして、所定回数前のステップＳ５０１の処理から今回のステップＳ５０１の処理までに得られたＷｅｂサーバ１１とＡＰサーバ１２のログデータに基づいて、相関関係抽出部１００４が求めた相関関係７０２（ｃ）も示されている。時系列的に見たときに、最初に求めた相関関係が７０２（ａ）、次が７０２（ｂ）、最新のデータが７０２（ｃ）であるとする。更に、相関関係７０３（ｄ）は監視対象システムの今後予想される相関関係を示している。なお、図をわかりやすくするために、図７においては範囲領域７０１に対応する相関関係の線は表示していない。

【００５０】

ステップ５０４では、監視対象システムの過去の動向と現在の状況を相関関係７０２（ａ）～７０２（ｃ）に基づいて、つまり、ある監視対象のシステムを定期的に監視したときのデータを用いてエラーを予測する。

【００５１】

障害検知／予測部１００６は、ステップＳ５０５において、相関関係７０２の時系列に伴う推移を判定し、相関関係が正常時の範囲領域７０１からはずれそうな場合、情報処理システムに将来異常が発生する可能性があると予測する。この時、必要に応じて、将来の相関関係７０２（ｄ）を生成する。尚、本実施例では、最新の監視データから作成された相関関係が、正常時の相関関係の範囲領域７０１から外れそうであることを判断の基準としているが、例えば、最新の監視データから作成された相関関係が異常時の相関関係に類似した相関関係になりつつあることを判断基準としても良いし、或いは、領域範囲に入るか否かで判断するのではなく、正常時・異常時の相関関係の傾きなどで判断しても良い。

【００５２】

障害検知／予測部１００６による上記の予測内容は、報知部１００７によってオペレータに対して報知される。

【００５３】

また、本実施形態においては、本情報処理システムに類似した構成の情報処理システムを新規に設置する場合、本情報処理システムの相関関係記憶部１００５で記憶された正常時及び異常時の相関関係を、新規の情報処理システム内の相関関係記憶部に記憶させることにより、新規の情報処理システムにおいて適切なエラー検知処理、エラー予測処理を同様に行うこともできる。ここで性能監視装置１０は、図１に示す情報処理システムに限られず様々な構成の情報処理システムを監視対象とすることができるため、流用できる相関関係は上述した例に限られないことは勿論である。

【００５４】

以上のように、本実施形態によれば、障害検知又は予測時に用いた２種類の監視データの種類によって、当該障害の原因まで追求することが可能となる。尚、本実施形態では、２種類の監視データの相関関係を用いているが、本発明に適用可能な相関関係は２種類の監視データから算出されるものに限られず、更に多種類の監視データの相関関係であってもよい。

【００５５】

また、説明の便宜上、異常検出部１００３と障害検知／予測部１００６とは別の構成で行うよう説明したが、いずれも、監視データ記憶部１００２から読み込んだ監視データと、相関関係記憶部１００５から読み込んだ相関関係とを比較するという処理については、共通のソフトウェア／ハードウェアを用いてもよい。

【００５６】

次に、本実施形態の他の処理の例について説明する。Ｗｅｂサーバ１１における処理１の発生回数とＡＰサーバ１２における処理２の発生回数間の基準比率を予め設定しておき、現在の当該２種類の監視データ間の比率が基準比率から離れていく傾向にある場合にエラーを予測することも可能である。例えば基準比率が１：１で設定されているにもかかわらず、時間経過と共にその比率が１：１．１、１：１．２、１：１．３、・・・などと基準から離れていく傾向が見られた場合に検知して、オペレータに報知する。

【００５７】

さらに、２種類の監視データから得られる１つの相関関係情報に基づいても異常検知をすることができる。図８は、スループットデータに対する応答時間との相関関係を示す例である。この図においては、スループットが高くなるにつれて応答時間が長くなっており、スループットがある量を超えると急激に応答時間が悪化することがわかる。応答時間が悪化する点をエラーとして検知することにより、レスポンス悪化に対してオペレータは早期に対策をとることが可能となる。具体的には、このような相関関係を相関関係記憶部１００５に記憶しておき、性能監視装置１０は監視データがこのような相関関係の極点に差し掛かったことを検知した場合にエラーと判断してオペレータに報知する。

【００５８】

このように、本実施形態では相関関係の時間経過による変化を捉え、相関関係の傾きの変化、相関関係のX軸やY軸方向へのシフトなどが許容されていない場合には、これらの状況を元にエラーを報知するものである。但しこれに限るものではなく、ある時刻断面で正常時の相関関係と比較してエラー予測しても良い。

【００５９】

なお、上述した実施形態では、性能監視装置１０によって取得される監視データとしてリソース使用状況データ、トランザクションデータ及びログデータを例として挙げたが、本発明に適用可能な監視データはこれらに限られず、Ｗｅｂサーバ１１、ＡＰサーバ１２及びＤＢサーバ１３の稼働状況を特定可能なデータは全て性能監視装置１０の採取対象とすることができ、同様の動作によるエラー検知処理、エラー予測処理が可能である。さらに、上記実施形態では、性能監視装置１０の監視対象となる情報処理システムの構成を、図１に示すＷｅｂサーバ１１、ＡＰサーバ１２及びＤＢサーバ１３から成る情報処理システムとしているが、他の構成の情報処理システムも本発明の性能監視装置の監視対象となり得ることは勿論である。

【００６０】

上述した実施形態では、１つのＷｅｂサーバ１１と１つのＡＰサーバ１２と１つのＤＢサーバ１３とで構成されたシステムを１つの性能監視装置１０で監視するという例で説明したが、これらは必ずしも１つずつである必要はない。性能監視装置１０は、ネットワーク上に接続されたサーバや通信回線を監視できるものであるため、１つの性能監視装置１０で２組以上のＷｅｂサーバ１１とＡＰサーバ１２とＤＢサーバ１３とで構成されたシステムを監視することも可能である。

【００６１】

また、Ｗｅｂサーバ１１とＡＰサーバ１２とＤＢサーバ１３の数も１：１：１である必要はなく、Ｍ：Ｎ：Ｌというようにそれぞれが複数備えられたシステムであっても良い。１例を挙げると、図９のように、６台のＷｅｂサーバ１１がそれぞれ３台ずつ２台のＡＰサーバ１２と接続され、この２台のＡＰサーバ１２が１台のＤＢサーバ１３と接続されている。このとき性能監視装置１０は個々のサーバや通信回線を監視し、その挙動からきめ細かにエラー検知をすることができるようになる。また、必要に応じて１台のＡＰサーバ１２に接続されている３台のＷｅｂサーバ１１との通信については、取りまとめて１つのＷｅｂサーバ１１とみなして監視することもできる。この場合、システム構成情報を性能監視装置１０に格納しておき、任意に監視対象を設定できるようにすることが好ましい。

【００６２】

次に、本発明を適用した好適な第二の実施形態を説明する。上述したように、監視対象となるシステムについて、システム構成情報を性能監視装置１０に格納しておき、任意に監視対象を設定できるようにすることが好ましい。そこで第二の実施形態では、第一の実施形態の機能構成に加え、監視対象となるシステムのシステム構成情報を更に管理することで、より多様な監視と障害予測を行えるように工夫している。

【００６３】

図１０は、第二の実施形態に係る性能監視システムの構成を概略的に示した図である。以下、図面を参照しながら詳細に説明するが、第一の実施形態と同一の機能については説明を省略する。図１０は、図９で示した６台のＷｅｂサーバ１１と２台のＡＰサーバ１２

と１台のＤＢサーバ１３とから構成されたシステムの性能監視を行うための構成であり、第一の実施形態と同様に、蓄積サーバ１０１と分析サーバ１０２から構成される性能監視装置１０が通信回線から取得できる情報を収集蓄積し、分析する。第二の実施形態では更に、構成情報管理装置２０が備わっており、性能監視装置１０に接続されている。なお、以下の説明では構成情報管理装置２０は性能監視装置１０と別の装置として構成した例を説明するが、これは１台のコンピュータで構成しても良い。

【００６４】

構成情報管理装置２０は、監視対象となるシステム全体の構成にかかわる情報を格納しておくものである。具体的には、各機能のサーバの数やハードウェア属性、ネットワーク構成、ネットワーク属性、ソフトウェアやファームウェアなど、情報処理装置自体の情報と各情報処理装置間の関連性を示す情報をデータベースに格納している。なお、以下では説明を簡単にするために、ハードウェアに関する構成情報を扱う例とする。例えば、図９で示した全体構成について、ＩＤを付与して格納しておく。新たにサーバが追加されたなど監視対象のシステムの構成が変更された場合には、新たな構成情報として別途ＩＤが付与されて構成情報管理装置２０に格納される。なお、構成情報管理装置２０は、単体コンピュータで構成するには、図２に示したようなコンピュータの基本的な機能を有することになる。

【００６５】

図１１は第二の実施形態に用いる性能監視装置１０と構成情報管理装置２０の構成を詳細に説明する図である。性能監視装置１０は、第一の実施形態で説明した機能に加え、システム構成全体の中で、監視対象とする範囲を指定するための監視対象指定部１００８と、指定された監視対象範囲を記憶しておくための監視対象範囲データを監視データ記憶部１００２に備えている。

【００６６】

後述するように、第二の実施形態においては、複数のハードウェアで構成されたシステムの全体構成が構成情報管理装置２０に構成情報ＩＤが付与されて記憶される。これに対して、監視対象は記憶されているシステムの全体構成の内任意の範囲を指定することができるようになっている。例えば図９において６台のＷｅｂサーバ１１と２台のＡＰサーバ１２と１台のＤＢサーバ１３の合計９台のコンピュータで構成されているシステムについて、システム全体を監視対象とすることもでき、或はその内の何台かだけを監視対象とすることもできる。そのために監視対象指定部１００８は監視対象を特定するための情報をオペレータから受付ける機能を持っている。具体的には、オペレータのキーボードやマウス操作等で範囲指定の情報を受け取る。

【００６７】

監視対象指定部１００８で受け取った範囲指定の情報は、監視データ記憶部１００２に監視対象範囲データとして監視対象ＩＤが付与されて記憶される。監視データ所得部１００１は、Ｗｅｂサーバ１１、ＡＰサーバ１２及びＤＢサーバ１３からリソース使用状況データ及びログデータ、上記サーバ間を接続する通信回線からトランザクションデータ等を取得する際に、監視対象範囲データを参照し、指定されている範囲の情報だけを取得する。なお、監視データ所得部１００１が能動的に監視データを取得する場合には、指定されているサーバ等にアクセスしてログデータ等を取得し、受動的に監視データを取得する場合には、受信したログデータ等の内、監視対象範囲として指定されているサーバ等のデータだけを選別（フィルタリング）して取得する。

【００６８】

構成情報管理装置２０は、構成情報を入力して登録するための構成情報登録部２００１と、入力された構成情報を記憶するための構成情報記憶部２００２、そして性能監視装置１０からの要求に応じて構成情報記憶部２００２に記憶された構成情報を抽出し、性能監視装置１０に送信するための構成情報抽出部２００３から構成される。

【００６９】

構成情報登録部２００１は、キーボードやマウスなどでありオペレータが入力する情報

を受け付ける機能である。例えば図９であればオペレータは、監視対象としたいシステムの全体構成として、６台のＷｅｂサーバと２台のＡＰサーバと１台のＤＢサーバなど、ハードウェアの数量に関する情報と、各ハードウェアがそれぞれどのような形態で接続されているか、接続するためのネットワークはどれほどの転送レートを持ったものであるか、各ハードウェア・ソフトウェアのスペックはどのようなものであるか等を入力する。各ハードウェア・ソフトウェアのスペックとしては、単に購入時のスペックだけではなく、ファームウェアやソフトウェアのバージョンなども登録しておくと良い。なお、オペレータからの入力だけでなく、ネットワークを介してコンピュータが取得できるシステムの構成情報は、自動的に取得しても良い。

【００７０】

構成情報記憶部２００２は、構成情報登録部２００１で受け付けた情報を監視対象システム毎に格納するものである。構成情報には、構成情報ＩＤ以外にも構成情報を受け付けた記憶日時情報等の属性情報も付加されて記憶される。

【００７１】

構成情報抽出部２００３は、構成情報記憶部２００２に格納されている構成情報を、性能監視装置１０やオペレータからの指示に基づいて抽出する機能である。後述するように、第二の実施形態では、システムの構成に応じて性能を監視したり異常を検出するため、監視対象のシステムと正常時のシステムの挙動とから相関関係を求める必要がある。そこで、性能監視装置１０は必要に応じて構成情報を構成情報記憶部２００２から読み出して相関関係のデータ等を作成する。

【００７２】

ここで、相関関係記憶部１００５内の相関関係は、相関関係を求めた環境毎に記憶される。例えばサーバが１０台の時と、１１台の時とではシステムの挙動は異なってくる。従ってサーバが１０台の時の相関関係と１１台になったときの相関関係は別に求めてそれぞれに相関関係ＩＤを付与して記憶する。そして、当該相関関係を求めた際の監視対象ＩＤ及び／又は構成情報ＩＤとをリンクさせておく。リンクはリレーショナルデータベース等で管理することで容易に設定できる。このような、ＩＤで関連付けられた各情報は別途履歴情報として格納しておいても良い。当然ながら、１つの監視対象に対して複数の相関関係が生成されるので、相関関係ＩＤと監視対象ＩＤとは複数対複数の関係でリンクが形成される。構成情報ＩＤも同様である。

【００７３】

次に、図１２を参照しながら性能監視装置１０と構成情報管理装置２０の動作を説明する。第二の実施形態では、図４を用いて説明した第一の実施形態による監視と相関関係抽出の処理自体は同じであるが、この監視処理に先立って監視対象の範囲を特定する処理が行われる。まず最初に、構成情報登録部２００１は、オペレータ又はコンピュータにより入力されるシステムの全体構成に拘る情報を受信して構成情報記憶部２００２に転送する（ステップＳ１２０１）。システムの全体構成に拘る情報を受信した構成情報記憶部２００２は、構成情報にＩＤを付与して順次情報を記憶していく。この時、上述のように受信した日時情報も一緒に記憶される（ステップＳ１２０２）。

【００７４】

続いて、構成情報記憶部２００２に記憶されたシステムの全体構造の内、監視対象としたい範囲に関する情報をオペレータが入力し、入力された情報を監視対象指定部１００８が受付ける（ステップＳ１２０３）。範囲指定方法の一例としては、対象となる複数のサーバのＩＰアドレスなど一意にハードウェアを特定することが挙げられる。そして受付けられた情報に基づいて、監視データ取得部１００１は構成情報抽出部２００３に抽出指示し、構成情報抽出部２００３が構成情報記憶部２００２からシステムに関する情報を抽出して監視データ取得部１００１に返送する（ステップＳ１２０４）。

【００７５】

例えば、図９において、ＤＢサーバ以外の８台のサーバを監視対象とするようオペレータからの指示を監視対象指定部１００８が受けると、監視データ取得部１００１はその情

報を構成情報抽出部２００３に抽出条件として送信し、構成情報抽出部２００３は８台のＩＰアドレス等を用いてサーバを特定する。特定された対象となる複数のサーバのＩＰアドレスは監視データ取得部１００１に送信され、監視データ取得部１００１は監視データ記憶部１００２に監視対象範囲データとして監視対象ＩＤを付与して記憶する（Ｓ１２０５）。

【００７６】

監視データ取得部１００１は監視処理を行う際に、監視データ記憶部１００２に記憶された監視対象範囲データで特定されるハードウェア群に関する監視データを取得する。以下は図４や図５を用いて説明した第一の実施形態と同様に処理が行われる。この時、監視対象ＩＤと対応する相関関係ＩＤとに基づいて比較に用いられる相関関係が抽出され各処理が行われる。なお、図１２のステップＳ１２０１からステップＳ１２０５に於ける処理はシステムの構成が変更された度、または監視対象範囲が変更される度に行われる。

【００７７】

以上説明したように、本発明を適用した第二の実施形態では、監視対象とするハードウェア構成とソフトウェア構成を特定する情報を更に備えることにより、システム全体の中の特定部位だけの監視を行たいなど、目的に応じた監視対象の範囲を監視することが可能となる。なお、上述した実施形態では１つのシステムについて性能監視装置１０と構成情報管理装置２０がひとつずつ備わっている例を示したが、本発明はこれにとどまらず例えば、ＡＳＰ（アプリケーションサービスプロバイダ）サービス等の形態にも応用できる。つまり、監視対象となるシステムが複数存在し、それら個々のシステム内の特定範囲だけを監視対象とすることができる。その場合、システム毎に構成情報を記憶し、システム毎に監視対象範囲データを持てば良い。

【００７８】

また、別の形態として、１つのシステムの中で、目的に応じて複数の監視対象範囲を設定しても良い。例えばサーバＡ～サーバＪまでの１０台のサーバで構成されたシステム全体の内、１つ目の監視対象範囲がサーバＡ～サーバＥの５台、２つ目の監視対象範囲がサーバＦ～サーバＨの３台という範囲を指定しても良い。更には、１つ目の監視対象範囲がサーバＡ～サーバＧの７台、２つ目の監視対象範囲がサーバＣ～サーバＪの８台など、１つのサーバが複数の監視対象として指定されても良い。いずれの場合も、監視データ取得部１００１は監視処理を行う際に、監視データ記憶部１００２に記憶された監視対象範囲データを参照して監視対象のサーバを特定し、必要な監視データを取得するという処理が行われる。

【００７９】

次に、本発明を適用した好適な第三の実施形態を説明する。上述した第一の実施形態と第二の実施形態では、何れもリソース使用状況データ、ログデータ、トランザクションデータなど、コンピュータの稼働状況を収集していた。これに対して第三の実施形態では、更に、コンピュータ稼働状況以外の情報をも収集して相関関係を求めるようにしている。

【００８０】

コンピュータシステムは、様々な理由により、ハードウェア構成やソフトウェア構成が変更される。これらの変更によりコンピュータシステムの性能が変化する。また、コンピュータシステムを取りまく環境の変化によってもコンピュータシステムの性能は変化する。本実施形態においては、これらの変化を捉えて監視データのひとつとして扱うことを特徴としている。これを特に「イベントデータ」と称することとする。「イベントデータ」は、稼働状況を含めて監視したい対象システムの内外で発生する事象に関するデータである。例えば、内部で発生する事象としては、エラーの発生、コンピュータに組み込まれるＣＰＵの数量が増加したなどのシステムの変更がある。また外部的な事象としては、温度の変化や地震や衝撃による揺れの発生などがある。そしてイベントの内容によってはコンピュータの演算性能が低下してスループットが低下するなどの変化が発生する。そこで、例えば、監視データ取得部１００１がイベントデータをキャッチしたときに、イベントに応じて分析や異常検知などの処理を行うようにする。

【００８１】
図１３は、第三の実施形態に係る性能監視システムの構成を概略的に示した図である。第三の実施形態でも基本的な情報処理は第一の実施形態及び第二の実施形態と同様であるが、本実施形態の特徴をわかりやすく説明するための構成のみを表示している。従って、同じ処理については説明を省略する。第三の実施形態の特徴のひとつとして入力データソースが「Ｗｅｂサーバ」「ＡＰサーバ」「ＤＢサーバ」等の監視対象装置に加え、「運用管理ツール」「ユーザ入力」が含まれている点がある。そして監視データ記憶部１００２に記憶されているデータについて、監視データに関するもの１００２と、イベントデータに関するもの１００２'とを分けて示している。
【００８２】
イベントデータは、監視対象システムから発せられる信号をそのまま利用したり、図示しない運用管理ツールから受信したり、或いは人間により入力されるデータがある。なお、運用管理ツールはシステムのハードウェアやソフトウェアを管理するものであって、それぞれのハードウェアがどのような構成を持っており、どのようなバージョンのソフトウェアがインストールされているかどうか等の情報を管理している。
【００８３】
さらに、イベントデータは後述するように、監視対象システムから受信したログデータなどを元に生成されるものもある。いずれにしても、イベントデータもそれぞれイベントデータＩＤが付与されて監視データ記憶部１００２の所定の場所に格納される。
【００８４】
次に、第三の実施形態におけるデータの流れを説明する。監視データ取得部１００１を介して受信した各データは、それぞれデータの種類に応じて、記憶部に格納される。まず監視対象システムの構成に関するデータは、第二の実施形態で説明したように構成情報管理装置２０の構成情報記憶部２００２に記憶される。監視対象システムから受信したログデータやスループットなどの監視データは、監視データ記憶部１００２に格納され、同様に監視データ取得部１００１を介して受信したイベントデータも監視データ記憶部１００２'に格納される。
【００８５】
監視データ記憶部１００２に格納された監視データからは、何らかのイベントに関する情報を引き出すこともできる。例えば監視対象のサーバがダウンすると、監視データが受信されなくなる。つまり、定期的に受信できていた監視データが監視データ記憶部１００２に記憶されなくなった時点を感知できれば監視対象のサーバがダウンしたというエラー（障害）に関するイベントを抽出することができる。また、CPU使用率が１０分程度にわたって９０％を越えているような場合は過負荷とみなすことができるので、システムの稼働状況に関するイベントを抽出することができる。
【００８６】
そこで、第三の実施形態では、イベントデータ生成部１００９を設けて、監視データをもとにイベントデータを生成している。イベントデータ生成部１００９は、監視データ記憶部１００２に格納された監視データについて、図示しないルール記憶部に記憶されているイベントデータ生成ルールに基づいてイベントデータを生成する。イベントデータ生成ルールには、どのようなタイミングで、どのデータを用いて、どのようなイベントデータを生成すかどうかが定義されている。上述したエラーに関するイベントの例では、「常に」「監視データ」を抽出して「監視データが一定時間受信できなければ"サーバダウン"」というイベントデータ生成ルールに従ってルール生成処理が行われる。また、稼働状況に関するイベントの例では、「常に」「CPU使用率」を抽出して「９０％異常が１０分続いたら"過負荷"」というイベントデータ生成ルールに従ってルール生成処理が行われる。そして、イベントデータＩＤを付与した上で監視データ記憶部１００２'に格納する。
【００８７】
このように、第三の実施形態では、監視対象のシステムに発生するあらゆる事象について、監視対象システムから発せられる信号、図示しない運用管理ツールから受信した信号

、人間により入力される情報、或いはイベントデータ生成部１００９で生成されたデータを、イベントデータとして監視データ記憶部１００２に格納する。

【００８８】

相関関係抽出部１００４は、監視データ記憶部１００２及び構成情報記憶部２００２に記憶された各情報を用いて相関関係を求め、相関関係１００５に記憶しておく。

【００８９】

次に、イベントデータを用いた処理について説明する。第一の実施形態や第二の実施形態では、（２）監視データ記憶部１００２から読み込んだデータに基づいて相関関係を求める（生成する）処理、（４）監視データと相関関係或いは相関関係どうしを比較する処理、（５）監視データと１つの相関関係から異常検知する処理を行ったが、本実施形態では更に（６）監視データと、イベントデータをきっかけとして生成した相関関係とを比較する。

【００９０】

監視データと、イベントデータをきっかけとして生成した相関関係とを比較する処理（６）の例として、ここでは上述した監視データとサーバダウンというイベントデータとの相関関係を用いた一連の分析処理を説明する。監視データとしては、「ディスクＩ／Ｏ」と「サーバのスループット」を監視しているものとする。

【００９１】

まず、監視対象のシステムについて「ディスクＩ／Ｏ」と「サーバのスループット」を継続的に測定し、測定されたデータは監視データ取得部１００１で取得され、監視データ記憶部１００２に「ディスクＩ／Ｏ」と「サーバのスループット」として逐次記憶される。イベントデータ生成部１００９は常に監視データを抽出し続け、もし監視データが一定時間受信できなければ"サーバダウン"とみなして"サーバダウン"というイベントデータを生成した上で監視データ記憶部１００２'に記憶する。

【００９２】

次に相関関係抽出部１００４は、監視データ記憶部１００２に記憶されたディスク「ディスクＩ／Ｏ」と「サーバのスループット」と、監視データ記憶部１００２'に記憶された"サーバダウン"のイベントデータに基づいて相関関係を抽出し、相関関係記憶部１００５に記憶する。具体的には、監視データ記憶部１００２に記憶された「ディスクＩ／Ｏ」と「サーバのスループット」の監視データが急増した直後に監視データが一定時間受信できなくなっていれば、「ディスクＩ／Ｏ」と「サーバの処理数」に基づいて図１４に示したような相関関係を求めた上で、更に、「ディスクＩ／Ｏ」または「サーバのスループット」がある一定値を超えたときに"サーバダウン"が発生したという情報を生成する。図１４では、ハッチングした領域が過去に"サーバダウン"発生した時の「ディスクＩ／Ｏ」と「サーバのスループット」との関係を示す部分である。

【００９３】

次に、障害検知／予測部１００６は、監視データ記憶部１００２に逐次記憶される「ディスクＩ／Ｏ」と「サーバのスループット」の監視データについて読み出し、そのデータが図１４に示した相関関係の正常値にあるのか、それとも"サーバダウン"が発生する可能性にあるのか（障害予測）、或は"サーバダウン"が発生したのか（障害検知）を判別する。そして、障害予測または障害検知と判断した場合には、「"サーバダウン"が発生する可能性がある」「"サーバダウン"が発生した」等のメッセージを報知部１００７に表示する。

【００９４】

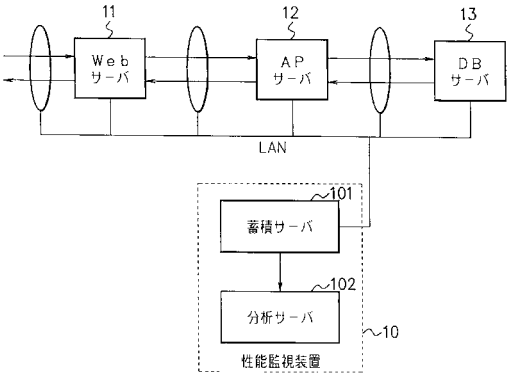
なお、先に示した稼働状況に関するイベントの例では、生成された"過負荷"というイベントデータに基づいて、次のような相関関係の比較をすることができる。一般的にはスループットが上昇したときにCPUの処理が増加して負荷が高くなる。それに対して、スループットが高くなっているにもかかわらず、CPU負荷が高くなっていない状態は異常と考えられる。そこで、CPU使用率とスループットとの相関関係について、正常時の相関関係と"過負荷"というイベントが発生した時の相関関係を比較し、障害を判断する。

【００９５】
以上のように、第三の実施形態では、監視対象のシステムの内外に発生するあらゆる事象をイベントデータとして抽出し、抽出したイベントデータと監視データとを用いて相関関係を抽出している。なお、上記実施形態では単にイベントデータと監視データとを用いた分析処理について説明したが、第二の実施形態で説明したような構成情報まで含めたデータを用いて相関関係を求めることでより詳細な異常検知をすることも可能となる。
【００９６】
なお、上述した各実施形態では、予め相関関係を求めるには図示しないルール記憶部に記憶された相関関係抽出ルールに基づいて相関関係が抽出される。この相関関係抽出ルールは予めユーザによって登録されているものであるが、記憶された監視データやイベントデータを元に、どのような相関関係を抽出すればよいかを自動的に推測し、相関関係抽出ルール自体を自動生成するようにしても良い。つまり、監視データやイベントデータを蓄積しつづけておき、エラー等が発生しない状況を正常値とし、この正常値を外れた何らかの監視データがあった場合に相関関係抽出ルール生成機能が働き、それらデータから新たな相関関係ルールを生成するなどしても良い。
【００９７】
以上詳細に説明したとおり、本発明では、第一の実施形態および第二の実施形態のように、システムの稼動状況に関する量的な複数種類の情報から相関関係を求める方法、そして、第三の実施形態のように、システムの稼動状況に関する量的な情報とシステムに対して発生したイベント情報とから相関関係を求める。このようにして求めた相関関係は相関関係記憶部１００５に記憶され、監視データはこの相関関係と比較されて障害の検知や予測が行われる。
【００９８】
ところで、本発明の目的は、前述した実施形態の機能を実現するソフトウェアのプログラムコードを記録した記憶媒体を、システム或いは装置に供給し、そのシステム或いは装置のコンピュータ（またはＣＰＵやＭＰＵ）が記憶媒体に格納されたプログラムコードを読み出し実行することによっても、達成されることは言うまでもない。
【００９９】
この場合、記憶媒体から読み出されたプログラムコード自体が前述した実施形態の機能を実現することになり、プログラムコード自体及びそのプログラムコードを記憶した記憶媒体は本発明を構成することになる。
【０１００】
プログラムコードを供給するための記憶媒体としては、例えば、フレキシブルディスク、ハードディスク、光ディスク、光磁気ディスク、ＣＤ－ＲＯＭ、ＣＤ－Ｒ、磁気テープ、不揮発性のメモリカード、ＲＯＭ等を用いることができる。
【０１０１】
また、コンピュータが読み出したプログラムコードを実行することにより、前述した実施形態の機能が実現されるだけでなく、そのプログラムコードの指示に基づき、コンピュータ上で稼動しているＯＳ(基本システム或いはオペレーティングシステム)などが実際の処理の一部又は全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。
【０１０２】
さらに、記憶媒体から読み出されたプログラムコードが、コンピュータに挿入された機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに書込まれた後、そのプログラムコードの指示に基づき、その機能拡張ボードや機能拡張ユニットに備わるＣＰＵ等が実際の処理の一部又は全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。
【図面の簡単な説明】
【０１０３】
【図１】本発明の第一の実施形態に係る性能監視システムの構成を概略的に示す図である

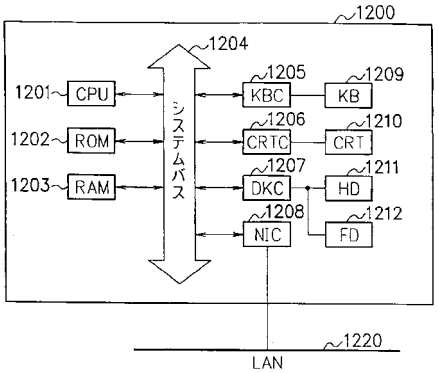
。
【図２】性能監視装置内のコンピュータシステムのハードウェア構成を概略的に示す図である。
【図３】性能監視装置の機能構成を示すブロック図である。
【図４】監視データ取得部、異常検出部及び相関関係抽出部の動作を示すフローチャートである。
【図５】障害検知／予測部の動作を示すフローチャートである。
【図６】図５のステップＳ５０３におけるエラー検知処理を具体的に説明するための図である。
【図７】図５のステップＳ５０５におけるエラー予測処理を具体的に説明するための図である。
【図８】スループットデータに対する応答時間との相関関係を示す図である。
【図９】本発明を適用可能な性能監視システムの他の構成例を示す図である。
【図１０】本発明の第二の実施形態に係る性能監視システムの構成を概略的に示す図である。
【図１１】性能監視装置内のコンピュータシステムのハードウェア構成を概略的に示す図である。
【図１２】構成情報の登録と抽出処理を示すフローチャートである。
【図１３】性能監視装置内のコンピュータシステムのハードウェア構成を概略的に示す図である。
【図１４】本発明の第三の実施形態における相関関係を示す図である。
【符号の説明】
【０１０４】
１０：性能監視装置
１１：Ｗｅｂサーバ
１２：ＡＰサーバ
１３：ＤＢサーバ
２０：構成情報管理装置
１０１：蓄積サーバ
１０２：分析サーバ
１００１：監視データ取得部
１００２：監視データ記憶部
１００３：異常検出部
１００４：相関関係抽出部
１００５：相関関係記憶部
１００６：障害検知／予測部
１００７：報知部
１００８：監視対象指定部
１００９：イベントデータ生成部
１２００：コンピュータシステム
１２０１：ＣＰＵ
１２０２：ＲＯＭ
１２０３：ＲＡＭ
１２０４：システムバス
１２０５：キーボードコントローラ（ＫＢＣ）
１２０６：ＣＲＴコントローラ（ＣＲＴＣ）
１２０７：ディスクコントローラ（ＤＫＣ）
１２０８：ネットワークインタフェースカード（ＮＩＣ）
１２０９：キーボード（ＫＢ）
１２１０：ＣＲＴディスプレイ（ＣＲＴ）

１２１１：ハードディスク（ＨＤ）
１２１２：フレキシブルディスク（ＦＤ）
１２２０：ＬＡＮ
２００１：構成情報登録部
２００２：構成情報記憶部
２００３：構成情報抽出部

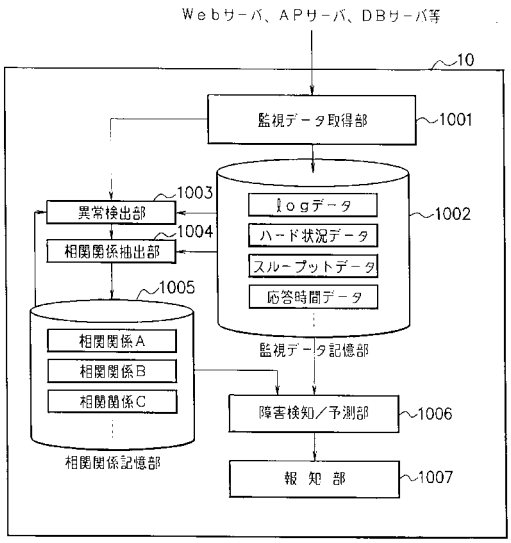
【図１】



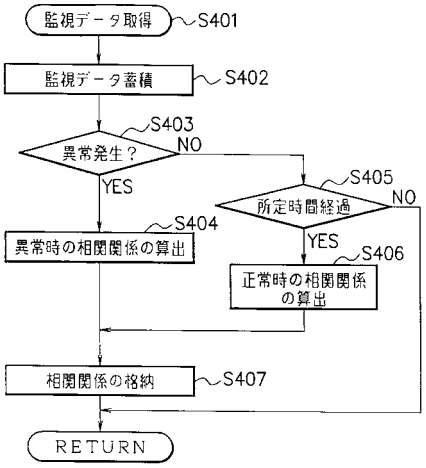
【図２】



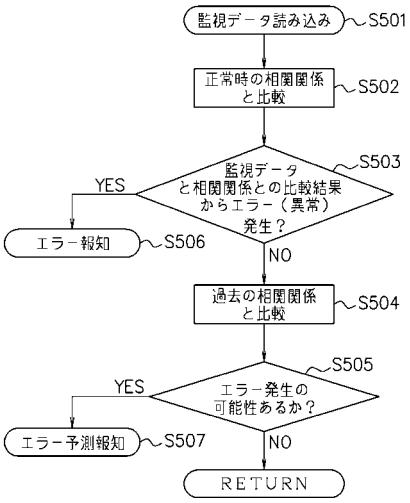
【図３】


Webサーバ、APサーバ、DBサーバ等
10
監視データ取得部
1001
異常検出部
1003
相関関係抽出部
1004
1005
相関関係A
相関関係B
相関関係C
相関関係記憶部
1002
logデータ
ハード状況データ
スループットデータ
応答時間データ
監視データ記憶部
障害検知／予測部
1006
報知部
1007

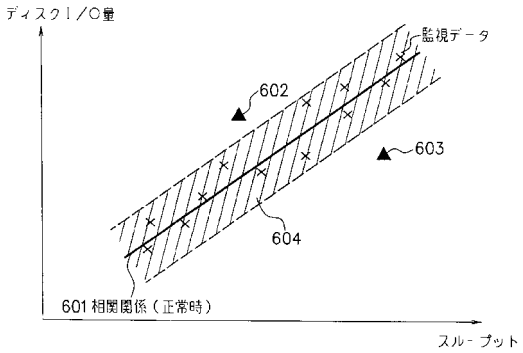
【図４】


監視データ取得
S401
監視データ蓄積
S402
S403
異常発生？
NO
YES
S405
所定時間経過
NO
YES
S404
異常時の相関関係の算出
S406
正常時の相関関係の算出
相関関係の格納
S407
RETURN

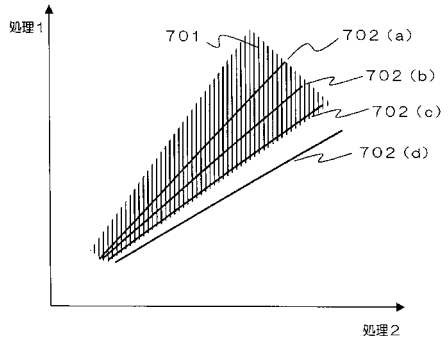
【図５】


監視データ読み込み
S501
正常時の相関関係と比較
S502
S503
監視データと相関関係との比較結果からエラー（異常）発生？
YES
エラー報知
S506
NO
過去の相関関係と比較
S504
S505
エラー発生の可能性あるか？
YES
エラー予測報知
S507
NO
RETURN

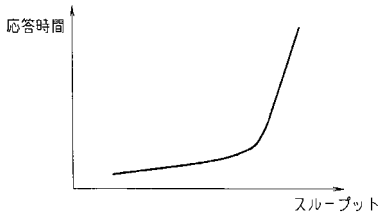
【図６】


ディスクI／O量
監視データ
602
603
604
601 相関関係（正常時）
スループット

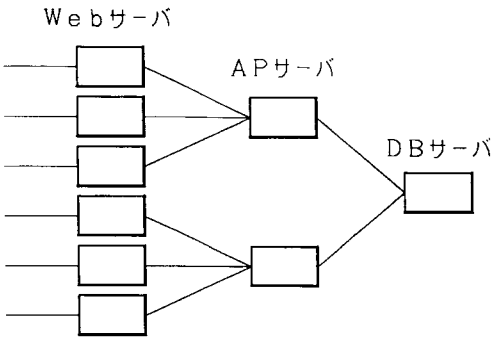
【図７】


処理1
701
702（a）
702（b）
702（c）
702（d）
処理2

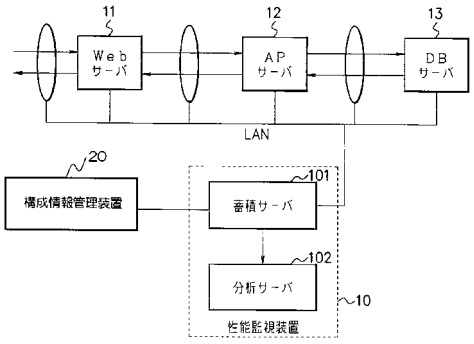
【図８】


応答時間
スループット

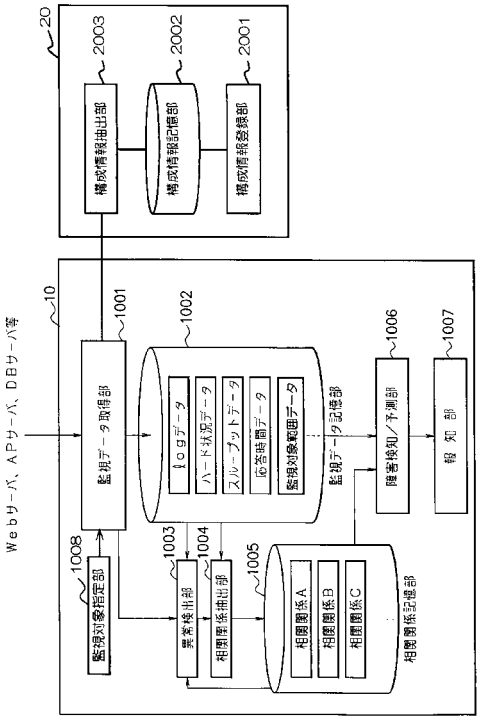
【図９】


Webサーバ
APサーバ
DBサーバ

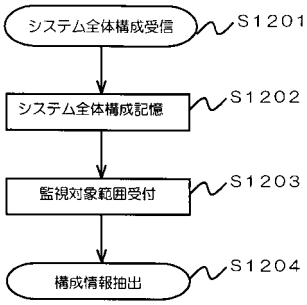
【図１０】


11
12
13
Web サーバ
AP サーバ
DB サーバ
LAN
20
構成情報管理装置
101
蓄積サーバ
102
分析サーバ
10
性能監視装置

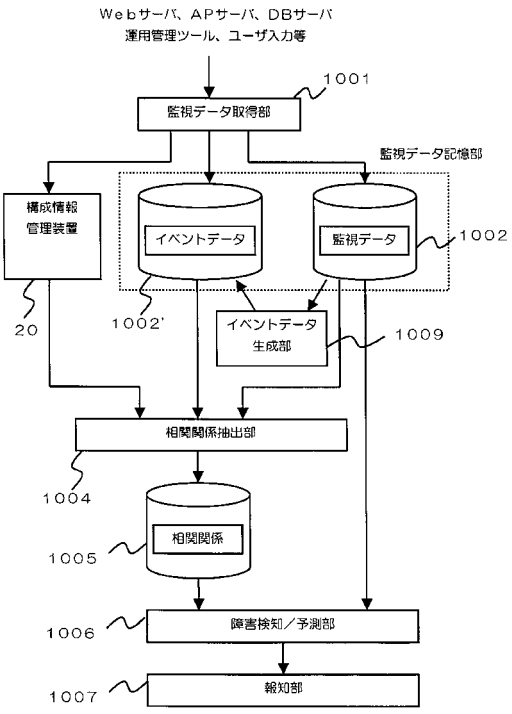
【図１１】



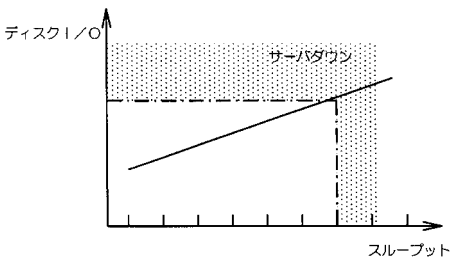
【図１２】



【図１３】



【図１４】



フロントページの続き

(72)発明者　横山　雄一
東京都中央区新川二丁目２０番１５号　新日鉄ソリューションズ株式会社内

審査官　漆原　孝治

(56)参考文献　特開平１０－０４９２１９（ＪＰ，Ａ）
特開平０７－１６８６１９（ＪＰ，Ａ）
特開平１１－０８８３９９（ＪＰ，Ａ）
特開平１１－３０８２２１（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　１５／００
Ｇ０６Ｆ　１１／３４