

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第5444673号  
(P5444673)

(45) 発行日 平成26年3月19日(2014.3.19)

(24) 登録日 平成26年1月10日(2014.1.10)

(51) Int.Cl.		F I			
<b>G06F 11/30</b>	<b>(2006.01)</b>	G06F 11/30			E
<b>G06F 11/32</b>	<b>(2006.01)</b>	G06F 11/32			E
<b>G06F 11/34</b>	<b>(2006.01)</b>	G06F 11/34			H

請求項の数 4 (全 22 頁)

(21) 出願番号	特願2008-252006 (P2008-252006)	(73) 特許権者	000005223
(22) 出願日	平成20年9月30日 (2008.9.30)		富士通株式会社
(65) 公開番号	特開2010-86099 (P2010-86099A)		神奈川県川崎市中原区上小田中4丁目1番1号
(43) 公開日	平成22年4月15日 (2010.4.15)	(74) 代理人	100074099
審査請求日	平成23年7月8日 (2011.7.8)		弁理士 大菅 義之
		(74) 代理人	100133570
			弁理士 ▲徳▼永 民雄
		(72) 発明者	田中 正雄
			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	多胡 滋

最終頁に続く

(54) 【発明の名称】 ログ管理方法、ログ管理装置、ログ管理装置を備えた情報処理装置、及びプログラム

(57) 【特許請求の範囲】

【請求項1】

情報処理装置を構成する部品、及び実行中のプログラムを監視対象として監視することで該情報処理装置が出力するログを該情報処理装置、及び別の情報処理装置の一方により管理する方法において、

前記ログを前記情報処理装置に存在する前記監視対象毎に分類する分類ステップと、

前記監視対象をハードウェア及びソフトウェアのカテゴリに分け、互いに異なるカテゴリに属する監視対象間で動作に関連性が存在すると見なす監視対象の組み合わせを示す関連付け定義情報を参照して、前記分類ステップでログを分類した監視対象のなかで該関連付け定義情報に示されている組み合わせを特定する特定ステップと、

前記特定ステップで特定した前記組み合わせに基づいて、前記分類ステップで前記監視対象毎に分類したログを対応付けて表示装置上に出力する出力ステップと、

前記監視対象毎に、一定時間内に出力されたログを解析して、該ログが出力された監視対象の状態を判断する解析ステップと、

前記ログが出力された前記監視対象の順序、及び該監視対象が属するカテゴリを基に、前記組み合わせを前記関連付け定義情報として登録することにより、該関連付け定義情報を更新する更新ステップと、を含み、

前記出力ステップでは、前記解析ステップでの判断結果を共に出力し、前記特定ステップで特定した前記組み合わせ毎に、前記分類ステップで前記監視対象毎に分類したログを示すシンボルを時系列に沿って配置した形で出力させる、

ことを特徴とするログ管理方法。

【請求項 2】

情報処理装置を構成する部品、及び実行中のプログラムを監視対象として監視することで該情報処理装置から出力されるログを管理する装置において、

前記ログを前記情報処理装置に存在する前記監視対象毎に分類する分類手段と、

前記監視対象をハードウェア及びソフトウェアのカテゴリに分け、互いに異なるカテゴリに属する監視対象間で動作に関連性が存在すると見なす監視対象の組み合わせを示す関連付け定義情報を記憶した情報記憶手段と、

前記情報記憶手段に記憶された前記関連付け定義情報を参照して、前記分類手段がログを分類した監視対象のなかで該関連付け定義情報に示されている組み合わせを特定する特定手段と、

10

前記特定手段が特定した前記組み合わせに基づいて、前記分類手段が前記監視対象毎に分類したログを対応付けて表示装置上へ出力する出力手段と、

前記監視対象毎に、一定時間内に出力されたログを解析して、該ログが出力された監視対象の状態を判断する解析手段と、

前記ログが出力された前記監視対象の順序、及び該監視対象が属するカテゴリを基に、前記組み合わせを前記関連付け定義情報として登録することにより、該関連付け定義情報を更新する更新手段と、を具備し、

前記出力手段は、前記解析手段による判断結果を共に出力でき、前記特定手段が特定した前記組み合わせ毎に、前記分類手段が前記監視対象毎に分類したログを示すシンボルを時系列に沿って配置した形で出力させる、

20

ことを特徴とするログ管理装置。

【請求項 3】

請求項 2 記載のログ管理装置を備えている、

ことを特徴とする情報処理装置。

【請求項 4】

情報処理装置を構成する部品、及び実行中のプログラムを監視対象として監視することで該情報処理装置が出力するログを管理するログ管理装置として用いられるコンピュータに、

前記ログを前記情報処理装置に存在する前記監視対象毎に分類する分類機能と、

30

記憶手段に記憶された、前記監視対象をハードウェア及びソフトウェアのカテゴリに分け、互いに異なるカテゴリに属する監視対象間で動作に関連性が存在すると見なす監視対象の組み合わせを示す関連付け定義情報を参照して、前記分類機能によりログを分類した監視対象のなかで該関連付け定義情報に示されている組み合わせを特定する特定機能と、

前記特定機能により特定した前記組み合わせに基づいて、前記分類機能により前記監視対象毎に分類したログを対応付けて表示装置上へ出力する出力機能と、

前記監視対象毎に、一定時間内に出力されたログを解析して、該ログが出力された監視対象の状態を判断する解析機能と、

前記ログが出力された前記監視対象の順序、及び該監視対象が属するカテゴリを基に、前記組み合わせを前記関連付け定義情報として登録することにより、該関連付け定義情報を更新する更新機能と、を実現させ、

40

前記出力機能は、前記解析機能による判断結果を共に出力でき、前記特定機能により特定した前記組み合わせ毎に、前記分類機能により前記監視対象毎に分類したログを示すシンボルを時系列に沿って配置した形で出力させる、

ことを特徴とするプログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、情報処理装置（コンピュータ）に存在する監視対象、つまり情報処理装置を構成する部品、及び実行中のプログラムを監視することで出力されるログを管理する技術

50

に関する。

【背景技術】

【0002】

従来、サーバ等の情報処理装置では、そのシステムを構成するコンピュータのハードウェアやソフトウェア等の構成要素をそれぞれ監視対象としてログ（又はログメッセージ）を記録することが行われている。そのログは、情報処理装置の動作、状態、或いは操作状況などの事象の時間的推移を示す情報となる。通信ネットワークを介してサービスを提供するシステムを構成するサーバでは、登録したユーザのログオンやログオフ、警告、異常又は故障発生の状態等のシステムに関する様々な事象が記録される。このようなことからログは、障害発生時の原因追及や不正アクセスの痕跡探し、システムの稼働統計をとる等の目的で利用される。

10

【0003】

図16は、従来のログ管理装置の動作を説明する図である。そのログ管理装置110は、通信ネットワークを介してサービスを提供するサーバ100に搭載されたものである。例えば、ログ管理装置110として動作させる機能を搭載したソフトウェアによって実現されている。

【0004】

サーバ100を構成するCPU（中央演算処理装置）、メモリ、システムコントローラ、ハードディスク装置（HDD）、ホストバスアダプタ等のハードウェア群101、及びオペレーティングシステム（OS）102上で動作するソフトウェア（アプリケーション・プログラム等）は、ログをとる監視対象となる。OS102は、各ソフトウェアの動作を監視し、各種イベントが発生、或いは状態の変化が発生した場合に、その内容を示すログをログ管理装置110に出力する。また、OS102は、ハードウェア群101を構成する各ハードウェアの動作を監視し、何らかの異常が発生しそうな場合や何らかの異常が発生した場合に、その旨（警告や異常）をイベント検知部103に通知する。その通知に回答して、イベント検知部103は発生した異常、及びその異常が発生したハードウェアを示すログをログ管理装置110に出力する。ログ管理装置110は、そのようにしてOS102、或いはイベント検知部103から出力されるログをログファイル104に格納する。

20

【0005】

そのログファイル104は、例えばサーバ100がハードウェア群101の一つとして搭載した不揮発性の記憶装置（例えばハードディスク装置）等に格納される。イベント検知部103は、例えばOS102に搭載された1ソフトウェアにより実現される。

30

【0006】

図17は、従来のログ管理装置110によりログファイル104に格納されるログを説明する図である。

図17は、ハードウェア群101を構成する部品HA及びHBにログを出力すべき異常、或いは故障が発生し、OS102上で動作するソフトウェア（図中「ソフト」と表記）SA、SB及びSCにログを出力すべき異常、或いはイベントが発生した場合を例にとって、出力されるログを示している。例えばソフトウェアSAで異常が発生したことでログ管理装置110に出力されたログは「ソフトSA異常」と表記している。イベント検知部103は、OS102の一部との想定から示していない。図17に示すようにログは、監視対象がログを出力すべき状態となれば随時、出力される。それにより、時系列で様々な種別/監視対象のログが入り交じった状態でログファイル104に格納される。

40

【0007】

図18は、ログファイル104に格納されたログの内容を示す図である。図18に示すように各ログは、それが出力された月日、時刻、監視対象、種別、及び要因の各データを備えた構成となっている。種別とは、ログを出力させる原因に相当し、具体的には異常、イベント、或いは故障等である。要因は、その種別となる原因が発生したと判断した理由に相当する。

50

【特許文献1】特開2005-141663号公報

【特許文献2】特開2006-302170号公報

【特許文献3】特開2004-206166号公報

【発明の開示】

【発明が解決しようとする課題】

【0008】

ログは、障害に対応するための有用な情報である。しかし、そのログは、時系列で様々な種別/監視対象のログが入り交じった状態でログファイル104に格納される。このため、ログの解析に膨大な時間と労力を必要としていた。

【0009】

従来のログ管理装置のなかには、ログの解析をより容易に行えるように、ログファイルに収集したログのなかから検索条件を満たすログを抽出して出力するものがある（特許文献1）。

【0010】

検索条件を設定可能なログ管理装置では、適切な検索条件を設定することにより、解析に必要なログを抽出させることができる。しかし、解析に必要なログのみを抽出できるとは限らない。解析に不必要なログが存在する、解析に必要なログが抜けている、といったことが発生するのが普通である。また、適切な検索条件を設定するためには、ある程度の知識や経験が必要である。このようなことから、保守要員がログ解析をより容易に行えるように支援するためには、検索以外の手法も重視すべきと考えられる。

【0011】

本発明は、解析をより容易に行えるようにログを出力することにより、障害への対応を支援するための技術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】

【0012】

本発明を適用した1システムでは、情報処理装置を構成する部品、及び実行中のプログラムを監視対象として監視することでその情報処理装置が出力するログを監視対象毎に分類し、監視対象をハードウェア及びソフトウェアのカテゴリに分け、互いに異なるカテゴリに属する監視対象間で動作に関連性が存在すると見なす監視対象の組み合わせを示す関連付け定義情報を参照して、ログを分類した監視対象のなかで関連付け定義情報に示されている組み合わせを特定し、特定した組み合わせに基づいて、監視対象毎に整理したログを対応付けて表示装置上へ出力し、監視対象毎に、一定時間内に出力されたログを解析して、該ログが出力された監視対象の状態を判断し、ログが出力された監視対象の順序、及び該監視対象が属するカテゴリを基に、組み合わせを関連付け定義情報として登録することにより、該関連付け定義情報を更新する。監視対象の状態の判断結果は共に出力し、監視対象毎に分類したログは、特定した組み合わせ毎に、そのログを示すシンボルを時系列に沿って配置した形で出力させる。

【0013】

情報処理装置（コンピュータ）を構成するハードウェアである部品は、その情報処理装置上で実行されるプログラム（ソフトウェア）の制御で動作する。このことから、プログラムが動作させる部品が正常に動作しない、或いは部品を動作させるプログラムに不具合が存在するような場合、監視対象をソフトウェア、及びハードウェアのカテゴリに分ければ、一方のカテゴリに属する監視対象のログの出力により、他方のカテゴリに属し、その監視対象に係る別の監視対象のログが出力されるという、ログ出力上の動作の関連性（依存関係）が成立する。

【0014】

この関連性（依存関係）に着目し、管理対象別に分類したログを対応付けて出力（表示）させる。障害を発生させる原因となった監視対象、及びその監視対象との間に依存関係が存在する監視対象では、比較的の高い頻度でログが出力される。このため保守要員にとっては、障害を発生させる原因として考えられる監視対象の絞り込み（初期切り分け）は

10

20

30

40

50

より容易に行えるようになる。従って、障害への対応自体もより容易に行えるようになる。ログが出力された監視対象の状態の判断結果の表示により、障害への事前対応もより容易に行えるようになる。

【発明の効果】

【0015】

本発明を適用した場合には、障害への対応をより容易に行えるように支援することができる。

【発明を実施するための最良の形態】

【0016】

以下、実施形態の例について、図面を参照しながら詳細に説明する。

図1は、本実施形態によるログ管理装置の構成を示す図である。そのログ管理装置20は、通信ネットワークを介してサービスを提供するサーバ10に、そのサーバ10に存在する監視対象の監視によって得られるログを管理するために搭載されたものである。例えば、ログ管理装置20として動作させる機能を搭載したプログラム（以降「ログ管理ソフト」）によって実現される。

【0017】

サーバ10は、CPU（中央演算処理装置）、メモリ、システムコントローラ、ハードディスク装置（HDD）、ホストバスアダプタ等のハードウェア群11によって構成され、オペレーティングシステム（OS）12上で動作するソフトウェア（ミドルウェアやアプリケーション・プログラム等）が搭載されている。ハードウェア群11を構成するCPU（中央演算処理装置）、メモリ、システムコントローラ、ハードディスク装置（HDD）、ホストバスアダプタ等の各ハードウェア、及びミドルウェアやアプリケーション・プログラム等の各ソフトウェアは、ログをとる監視対象となる。OS12は、実行中の各ソフトウェアの動作を監視し、各種イベントが発生、或いは状態の変化が発生した場合に、その内容を示すログをログ管理装置20に出力する。また、OS12は、ハードウェア群11を構成する各ハードウェアの動作を監視し、何らかの異常、或いは故障が発生した場合に、その旨をイベント検知部13に通知する。その通知にตอบสนองして、イベント通知部13は発生した事象（警告、異常、或いは故障）及びその事象が発生したハードウェアを示すログをログ管理装置20に出力する。ログ管理装置20は、そのようにしてOS12、或いはイベント検知部13から出力されるログを所定のログファイル16に格納する。

【0018】

ログ管理装置20は、構成認識部21、ログ分類部22、及び二次元表示部23を備えた機能構成であり、ログファイル16以外のデータとしては、構成テーブル群24、関連付け定義情報25、及び分類ログテーブル群26を管理する。それらのデータは、例えばハードディスク装置に保存され、必要に応じてメモリに読み出される。

【0019】

サーバ10は、ハードウェア構成情報14、及びソフトウェア構成情報15を管理している。ハードウェア構成情報14は、サーバ10を構成するハードウェア毎に、つまりハードウェア群11を構成するCPU（中央演算処理装置）、メモリ、システムコントローラ、ハードディスク装置（HDD）、ホストバスアダプタ等のハードウェア毎に、そのハードウェアについての情報をまとめたものである。ソフトウェア構成情報15は、サーバ10が実行するソフトウェア毎に、そのソフトウェアについての情報をまとめたものである。構成情報14或いは15に情報が格納されたハードウェア、及びソフトウェアは、ログを出力する監視対象となる。

【0020】

構成認識部21は、ハードウェア構成情報14、及びソフトウェア構成情報15を参照して、ハード構成テーブル24a（図2）、及びソフト構成テーブル24b（図3）を構成テーブル群24として生成する。各構成テーブル24a及び24bは、例えばハードウェア構成情報14及びソフトウェア構成情報15にそれぞれ格納されている情報を抽出し

10

20

30

40

50

て格納する形で生成したものである。

【 0 0 2 1 】

図 2 は、ハード構成テーブル 2 4 a のデータ構成を示す図である。図 3 は、ソフト構成テーブル 2 4 b のデータ構成を示す図である。

図 2 に示すように、ハード構成テーブル 2 4 a には、CPU (中央演算処理装置)、メモリ、システムコントローラ、ハードディスク装置 (HDD)、ホストバスアダプタ等のハードウェア毎に、当該ハードウェアの部品名、搭載位置、状態、及びキーワードの各データが格納されている。キーワードとしては、ハードウェアを示す表現として考えられるものが一つ以上まとめられている。

【 0 0 2 2 】

以降は、「ハードウェア」「ソフトウェア」はそれぞれカテゴリを指す意味で用いる。ハードウェアに属するものは「部品」と表記し、ソフトウェアに属するものは省略形の「ソフト」と表記することとする。

【 0 0 2 3 】

一方のソフト構成テーブル 2 4 b には、図 3 に示すように、ソフトウェアの名称 (図中「ソフト名」と表記)、カテゴリ、及び詳細情報の各データがソフトウェア毎に格納されている。カテゴリとは、対応するソフトウェアの種類、或いは搭載された形態に相当するものである。例えば「system」は OS 1 2 に搭載されたソフトウェアであることを表し、「application」はアプリケーション・プログラムであることを表している。詳細情報は、ソフトウェアの機能、或いは用途等についての情報である。

【 0 0 2 4 】

構成認識部 2 1 は、ハード構成テーブル 2 4 a 及びソフト構成テーブル 2 4 b から構成される構成テーブル群 2 4 の他に、関連付け定義情報 2 5 を作成する。その関連付け定義情報 2 5 は、図 4 に示すように、異なるカテゴリに属する監視対象間の関連付けを定義したものである。図 4 に示す例では、部品名が「部品 H A」の部品はソフト名が「ソフト S A」のソフトウェアと関連付けられている。部品名が「部品 H B」の部品はソフト名が「ソフト S B」のソフトウェアと関連付けられている。ソフト名が「ソフト S C」のソフトウェアには部品が関連付けられていない状態である。

【 0 0 2 5 】

例えばソフトウェアを実行する場合、当該ソフトウェアの実行に際して必要なハードウェアを動作させる。このため、ある部品に異常、或いは故障等の正常に動作しない事象が発生すると、その事象はその部品を動作させるソフトウェアに影響を及ぼす。或いは、ソフトウェアの不具合によってハードウェアが正常に動作しない場合もある。このことは、例えばある部品のログが出力されると、その部品を動作させるソフトウェアのログも出力されるという、互いに異なるカテゴリに属する監視対象間にログ出力上の動作の関連性 (依存関係) が存在することを意味する。このことから本実施形態では、保守要員がログ解析を行った場合に、その関連性が存在する、或いはその関連性が存在すると推量される監視対象の組み合わせを関連付け定義情報 2 5 中で定義し、ログ出力に利用するようにしている。

【 0 0 2 6 】

監視対象の組み合わせの定義、つまり関連付け定義情報 2 5 の作成、及び更新は、構成認識部 2 1 が行う。構成認識部 2 1 は、ハード構成テーブル 2 4 a 及びソフト構成テーブル 2 4 b を参照して、ハードウェアを構成する部品とソフトウェア間の関連付け定義情報 2 5 を作成する。その作成は、ハード構成テーブル 2 4 a に部品毎に格納されたキーワード、及びソフト構成テーブル 2 4 b のソフトウェア毎に格納された詳細情報を参照して行う。その参照により、キーワード、詳細情報からログ出力上の関連性を有すると考えられる監視対象の組み合わせを抽出して、その組み合わせ情報を格納した関連付け定義情報 2 5 を作成する。

【 0 0 2 7 】

ハードウェア構成情報 1 4 及びソフトウェア構成情報 1 5 は共に、システム構成の変更

10

20

30

40

50

等により更新される可能性がある。このことから構成認識部 2 1 は、状況に応じて、ハード構成テーブル 2 4 a、ソフト構成テーブル 2 4 b、及び関連付け定義情報 2 5 のうちの何れかの更新を行う。

【 0 0 2 8 】

図 5 は、関連付け定義情報 2 5 の更新方法を説明する図である。

ログファイル 1 6 には、時系列で部品又はソフトウェアに関するログが格納される。各ログは、それが出力された月日、時刻、監視対象、種別、及び要因の各データを備えた構成となっている。上述したように、ある部品に異常、或いは故障が発生すると、その事象はその部品を動作させるソフトに影響を及ぼす。このことから、ある部品に発生した事象は、その事象によるログが出力された後、その部品を動作させるソフトのログを出力させる。本実施形態では、このことに着目し、ハードウェアに属する監視対象のログに続けて、ソフトウェアに属する監視対象のログが一つ以上、連続する同一パターンが複数回、繰り返された場合、それらの監視対象間には関連性が存在すると見なし、それらの監視対象を関連付け定義情報 2 5 に登録するようにしている。図 5 に示す例は、部品 H G のログの後にソフト S H のログが続くパターンが繰り返されたことから、部品 H G とソフト S H の組み合わせを関連付け定義情報 2 5 に新たに登録する場合のものである。

10

【 0 0 2 9 】

ログ分類部 2 2 は、OS 1 2、或いはイベント検知部 1 3 から出力されたログをログファイル 1 6 に格納する。またログは、構成テーブル群 2 4 に登録された監視対象毎に用意したテーブル（分類ログテーブル）のなかで対応するテーブルに格納する。このことから分類ログテーブル群 2 6 は、監視対象毎に用意した分類ログテーブルから構成される。監視対象毎に異なる分類ログテーブルにログを格納することにより、ログは監視対象別に整理・分類される。

20

【 0 0 3 0 】

二次元表示部 2 3 は、関連付け定義情報 2 5 を参照して、互いに異なるカテゴリに属する監視対象を関連させ、ログを二次元表示させる。図 6 は、ログの関連付け方法を説明する図であり、図 7 は、ログ表示例を示す図である。

【 0 0 3 1 】

図 6 に示すように、各分類ログテーブルから読み出されたログは関連付け定義情報 2 5 に従ってまとめられ、図 7 に示すようにログ表示は、関連付けられたカテゴリの異なる監視対象の組み合わせ毎に、ログの内容を示すシンボルを時系列に沿って配置する形で行われる。ここではシンボルとして、例えば、警告（警告を行った動作により出力されたログ）を示す「W」、異常（異常の発生により出力されたログ）を示す「E」、及び構成テーブル群 2 4 に登録されていない監視対象により出力されたログ（図中「未知メッセージ」と表記）を示す「U」のみを表記している。図 7 では、縦軸に監視対象、横軸に時間をとったグラフによる二次元表示としているが、縦軸と横軸を逆にした二次元表示としても良い。

30

【 0 0 3 2 】

図 7 に示すように、何らかの障害が発生した監視対象、及びその監視対象と関連性を有する別カテゴリの監視対象では、高い頻度でログが出力される。それらの監視対象のログはまとめた形で表示される。このため、障害に対応する保守要員にとっては、障害が発生している可能性が考えられる監視対象（被疑箇所）の絞り込み（初期切り分け）を容易に行えるようになる。被疑箇所を見落とすようなことは発生し難くなる。また監視対象毎に時系列にログを配置することから、障害が発生する監視対象、その障害が発生し易い時間帯等の把握も容易に行うことができる。このようなことから保守要員は、障害への適切な対応、及び解析をより容易、且つ迅速に行えることとなる。

40

【 0 0 3 3 】

本実施形態では、各分類ログテーブルを検索し、一定時間内に同一の要因によるワーニング（警告）又はエラー（異常、或いは故障等）を示すログが一定回数以上、記録された場合、その分類ログテーブルに対応する監視対象は故障しているの見なし、その旨を警告

50

表示するようにしている。その警告表示により、被疑箇所の見落としはより防止することができ、事前対応もより容易に行えるようになる。その警告表示は、シンボルの表示色を変更することで行っている。

#### 【 0 0 3 4 】

図 8 は、故障の判断方法を説明する図である。

図 8 に示す分類ログテーブルでは、「 c c c c 」を要因とする異常によるログが一定時間内に 3 回記録されている。本実施形態では、一定時間内に同一の要因によるログを検索し、そのログが 3 回以上記録されたことを条件に、分類ログテーブルに対応する監視対象が故障しているか否かの判断を行うようにしている。故障していると判断した場合、その旨はシンボルの表示色を変更することで示すようにしている。図 7 では、表示色を変えているシンボルは、「エラー集中 故障表示」と表記した破線で囲うことで示している。その破線で囲まれたシンボルは、部品 H A 及びソフト S A で交互に繰り返されている「 W 」と「 E 」である。

10

#### 【 0 0 3 5 】

また、本実施形態では、分類ログテーブル毎に、統計情報を保持するようにしている。その統計情報は、同一の要因によるログが記録された回数のカウント結果（カウント値）を含むものである。新たにログが記録された場合、その統計情報、つまり対応するカウント値を更新するようにしている。カウント値は、例えば予め定めた時間帯で分けて、保持するようにしている。これは、サーバ 1 0 の負荷の重さや提供するサービスは、時間帯によって異なることが多い傾向があるためである。

20

#### 【 0 0 3 6 】

監視対象に何らかの不具合が存在する場合、同じ要因によるログが出力される頻度が高くなる。通常、不具合を放置した場合には、当該不具合が他のハードウェア又はソフトウェアに伝播することにより、データや状態等の整合性が取れなくなり、最終的にはシステム・パニックを引き起こす結果となる。このことから統計情報、つまり同じ要因によるログのカウント値は、今後、致命的なエラーが発生する可能性の判断に用いる。致命的なエラー（障害）が発生する可能性が高いと判断した場合、その可能性（エラー予兆）を警告表示するようにしている。その警告表示により、事前対応がより容易に行えるように支援する。

#### 【 0 0 3 7 】

図 9 は、エラー予兆の判断方法を説明する図である。

図 9 において、分類ログテーブルの右側に上から「 1 1 1 1 2 2 3 . . . 」と表記した数字は、同じ要因によるログのカウント値を示している。本実施形態では、エラー予兆の警告を行うべきか否かを判断するうえでの閾値を 3 とすることにより、カウント値が 3 以上となっているログの監視対象はエラー予兆の警告を行うべきと見なすようにしている。エラー予兆を警告すべきとする監視対象は、ログのシンボルの表示色を変更することで示すようにしている。図 7 では、エラー予兆の警告のために表示色を変えているシンボルは、「エラー予兆」と表記した破線で囲うことで示している。その破線で囲まれたシンボルは、部品 H B で 3 つの「 W 」の後に位置する「 E 」である。

30

#### 【 0 0 3 8 】

上述したように本実施形態によるログ管理装置は、サーバ 1 0 がログ管理ソフトを実行することで実現される。以降は、構成認識部 2 1、ログ分類部 2 2 及び二次元表示部 2 3 を実現させるために実行される処理について、図 1 0 ~ 図 1 4 に示すフローチャートを参照して詳細に説明する。

40

#### 【 0 0 3 9 】

図 1 0 は、関連付け定義情報作成処理のフローチャートである。この作成処理は、構成テーブル群 2 4（ハード構成テーブル 2 4 a、及びソフト構成テーブル 2 4 b）、及び関連付け定義情報 2 5 を作成するために実行される処理である。その実行は、例えばログ管理ソフトの起動後、構成テーブル群 2 4、及び関連付け定義情報 2 5 が存在しないことが確認されたことが契機とされる。始めに図 1 0 を参照して、この作成処理について詳細に

50



説明する。

【 0 0 4 0 】

先ず、ステップ S 1 では、ハードウェア構成情報 1 4 を参照する。続くステップ S 2 では、その構成情報 1 4 に登録されている部品の情報を抽出する。次のステップ S 3 では、ハードディスク装置等の不揮発性の記憶装置にハード構成テーブル 2 4 a を作成し、抽出した情報を格納する。その次のステップ S 4 では、情報を格納した部品毎に、状態として正常に動作していることを示す「normal」を格納する。また、部品毎に、搭載位置の情報や他の項目の情報からキーワードを生成し格納する。そのようにして、図 2 に示すような内容のハード構成テーブル 2 4 a を作成する。

【 0 0 4 1 】

ステップ S 4 に続くステップ S 5 では、ソフトウェア構成情報 1 5 を参照する。次のステップ S 6 では、その構成情報 1 5 に登録されているソフトの情報を抽出し、抽出した情報を格納した図 3 に示すようなソフト構成テーブル 2 4 b を作成する。その後はステップ S 7 に移行する。

【 0 0 4 2 】

ステップ S 7 では、ハード構成テーブル 2 4 a に登録された部品のキーワードを抽出し、そのキーワードを用いて、ソフト構成テーブル 2 4 b の詳細情報を対象とした検索を行う。続くステップ S 8 では、キーワードを含む詳細情報が存在するか否かを判定する。検索の結果、キーワードを含む詳細情報を抽出できた場合、判定は Yes となってステップ S 9 に移行する。そうでない場合には、判定は No となってステップ S 1 0 に移行する。

【 0 0 4 3 】

ステップ S 9 では、検索に用いたキーワードを有する部品、及びそのキーワードを含む詳細情報を有するソフトを示す組み合わせを関連付け定義情報 2 5 に反映させ、その組み合わせを示す情報を格納する。次のステップ S 1 0 では、検索に用いたキーワードを有する部品はハード構成テーブル 2 4 a の最後のものか否かを判定する。キーワード検索の対象となる部品が他に存在しない場合、判定は Yes となり、ここで関連付け定義情報作成処理を終了する。そうでない場合には、判定は No となって上記ステップ S 7 に戻る。それにより、別の部品のキーワードを用いた検索を行う。

【 0 0 4 4 】

例えば部品 H A のキーワードの一つである「CPU」はソフト S A の詳細情報中に存在している。部品 H B のキーワードである「MEM」「mem」等は、ソフト S B の詳細情報中の「Memory」に対応すると見なされる（図 2 及び図 3）。これらのことから、部品 H A とソフト S A、部品 H B とソフト S B、の 2 つの組み合わせは関連付け定義情報 2 5 に登録されることとなる。

【 0 0 4 5 】

図 1 1 は、構成テーブル更新処理のフローチャートである。この更新処理は、ハードウェア構成情報 1 4、或いはソフトウェア構成情報 1 5 の更新に合わせて、ハード構成テーブル 2 4 a、或いはソフト構成テーブル 2 4 b を更新するための処理である。例えばログ管理ソフトの起動後、無条件で一度、実行される。次に図 1 1 を参照して、この更新処理について詳細に説明する。

【 0 0 4 6 】

先ず、ステップ S 2 1 では、ハードウェア構成情報 1 4 を参照する。次のステップ S 2 2 では、ハード構成テーブル 2 4 a を参照する。その後に移行するステップ S 2 3 では、ハードウェア構成情報 1 4 及びハード構成テーブル 2 4 a 間での差分判定、つまりそれらのうちの一方にのみ登録されている部品の存在を判定する。そのような部品が存在していない場合、差分なしと判定し、ステップ S 2 5 に移行する。そうでない場合には、差分ありと判定して、ステップ S 2 4 に移行し、ハードウェア構成情報 1 4 と登録された部品が同じとなるようにハード構成テーブル 2 4 a を更新する。その更新後に上記ステップ S 2 5 に移行する。

【 0 0 4 7 】

10

20

30

40

50

ステップS 2 5では、ソフトウェア構成情報1 5を参照する。次のステップS 2 6では、ソフト構成テーブル2 4 bを参照する。その後に移行するステップS 2 7では、ソフトウェア構成情報1 5及びソフト構成テーブル2 4 b間での差分判定、つまりそれらのうちの一方にのみ登録されているソフトの存在を判定する。そのようなソフトが存在していない場合、差分なしと判定し、ここで構成テーブル更新処理を終了する。そうでない場合には、差分ありと判定して、ステップS 2 8に移行し、ソフトウェア構成情報1 5と登録されたソフトが同じとなるようにソフト構成テーブル2 4 bを更新する。その更新後、この構成テーブル更新処理を終了する。

【0 0 4 8】

図1 2は、関連付け定義情報更新処理のフローチャートである。この更新処理は、ログファイル1 6に記録されたログを参照して、関連付け定義情報2 5を更新するための処理である。例えばログ管理ソフトの起動後に、或いは一定時間間隔で実行される。次に図1 2を参照して、この更新処理について詳細に説明する。関連付け定義情報2 5の更新は、図5に示す方法で行われる。

【0 0 4 9】

まず、ステップS 4 1では、記録されたログをキーにしてログファイル1 6を検索する。続くステップS 4 2では、その検索により、複数行に渡り同一パターンのログ(メッセージ)が有るか否かを検出する、すなわち、同じ順序で複数の異なる監視対象のログが連続し、且つそれらが属するカテゴリが全て同じでない同一パターンが複数あるか否かのチェックを行う。次のステップS 4 3では、そのチェックにより、同一パターンが複数有ったか否かを判定する。同一パターンが複数有った場合、判定はYesとなってステップS 4 4に移行する。そうでない場合には、判定はNoとなり、ここで関連付け定義情報更新処理を終了する。

【0 0 5 0】

ステップS 4 4では、同一パターン、つまり複数行のログ(メッセージ)を単一のログに分解する。次のステップS 4 5では、ハードウェアに属する監視対象のログを抽出し、ハード構成テーブル2 4 aを参照して、その監視対象である部品を特定する。続くステップS 4 6では、ソフトウェアに属する監視対象のログを抽出し、ソフト構成テーブル2 4 bを参照して、その監視対象であるソフトを特定する。その特定後はステップS 4 7に移行する。

【0 0 5 1】

ステップS 4 7では、ステップS 4 6及びS 4 7でそれぞれ特定した監視対象の組み合わせが既に関連付け定義情報2 5に存在するか否かを判定する。その組み合わせが既に登録されていた場合、判定はYesとなり、ここで関連付け定義情報更新処理を終了する。そうでない場合には、判定はNoとなってステップS 4 9に移行し、その組み合わせを関連付け定義情報2 5に反映させる。その後、関連付け定義情報更新処理を終了する。

【0 0 5 2】

上記図1 0～図1 2に示す各処理を実行することにより、構成テーブル群2 4及び関連付け定義情報2 5の作成、及び更新が必要に応じて行われる。このことから、構成認識部2 1が実現される。

【0 0 5 3】

図1 3は、ログ分類処理のフローチャートである。この分類処理は、OS 1 2或いはイベント検知部1 3から出力されたログをログファイル1 6に記録し、対応する分類ログテーブルに格納するための処理である。例えばOS 1 2或いはイベント検知部1 3からのログの出力を契機に実行される。ログ分類部2 2は、この分類処理を実行することで実現される。次に図1 3を参照して、この分類処理について詳細に説明する。

【0 0 5 4】

まず、ステップS 6 1では、OS 1 2或いはイベント検知部1 3から通知されたログを入力する。次のステップS 6 2では、入力したログを内部バッファに格納する。その次のステップS 6 3では、内部バッファに格納したログ(図中「イベント情報」と表記)を口

10

20

30

40

50

グファイル 16 に記録する。その後はステップ S 64 に移行する。

【0055】

ステップ S 64 では、ログに対応する構成テーブルを参照する。続くステップ S 65 では、ログが出力された監視対象（図中「イベント」と表記）が構成テーブルに含まれているか否かのチェックを行う。次のステップ S 66 では、その監視対象が構成テーブルに含まれているか否かを判定する。その監視対象が構成テーブルに登録されている場合、判定は Yes となってステップ S 67 に移行する。そうでない場合には、判定は No となってステップ S 71 に移行する。

【0056】

ステップ S 67 では、ログを格納する分類ログテーブルを決定する。続くステップ S 68 10  
8 では、決定したテーブルにログを格納する。その後は、ステップ S 69 で内部バッファを消去してから、ログ分類処理を終了する。

【0057】

一方、ステップ S 70 では、内部バッファに格納したログは構成テーブル（構成テーブル群 24）には登録されていない未知の監視対象のものとして特定する。次のステップ S 71  
では、このログが出力された監視対象に対応する構成テーブルに登録する更新を行い、そのログを格納するための分類ログテーブルを作成する。その作成後は上記ステップ S 68  
に移行し、作成した分類ログテーブルにログを格納する。

【0058】

未知の監視対象から出力された最初のログは、図 7 に示すように「U」で表すようにし  
ている。その最初のログであることは、例えば種別としてその旨を示すデータを書き込む  
ことで常に特定することができる。

【0059】

本実施形態では、構成テーブル群 24 を参照し、登録されている監視対象毎に分類ログ  
テーブルを作成するようになっている。しかし、各分類ログテーブルに格納したログは関  
連付け定義情報 25 に従ってまとめる形で表示する。このことから作成する分類ログテ  
ーブルは、関連付け定義情報 25 に組み合わせとして登録された監視対象用のみとしても良  
い。

【0060】

図 14 は、二次元表示処理のフローチャートである。この表示処理は、図 7 に示すよう  
にログを二次元表示するための処理である。例えばログの出力を保守要員等に指示された  
ことを契機に実行される。二次元表示部 23 は、この表示処理を実行することで実現され  
る。最後に図 14 を参照して、この表示処理について詳細に説明する。

【0061】

まず、ステップ S 81 では、分類ログテーブル群 26 を参照し、続くステップ S 82 30  
では、そのなかの一つを選択する。次のステップ S 83 では、前に選択した分類ログテ  
ーブルは最後か否かを判定する。今回、選択する対象となる分類ログテーブルが存在しない場  
合、判定は Yes となり、ここで二次元表示処理を終了する。そうでない場合には、判定  
は No となってステップ S 84 に移行する。

【0062】

ログは、時系列で出力する。このことから、ステップ S 84 ~ S 88 40  
では、分類ログテ  
ーブルの先頭から（早く記録されたほうから）ログを順次、読み込み、そのログを示すシ  
ンボルを配置していくための処理が行われる。

【0063】

まず、ステップ S 84 では、1 行（に記録されたログ）を読み込む。続くステップ S 8  
5 では、ログをその種別に対応するシンボルに変換する。次のステップ S 86 では、月日  
、及び時刻を抽出して時間を認識する。その次のステップ S 87 では、シンボルを認識し  
た時間で決定される位置にプロットする。その後はステップ S 88 に移行して、そのよう  
にしてシンボルの配置を決定したログは最後の行に記録されていたか否かを判定する。そ  
のログが最後の行に記録されていた場合、判定は Yes となってステップ S 89 に移行す  
50

る。そうでない場合には、判定はNoとなって上記ステップS 8 4に戻る。

【0064】

ステップS 8 9では、一定時間内に一定回数以上の同じ要因の異常により出力されたログが有るか否かを判定する(図8)。そのようなログが有った場合、判定はYesとなり、ステップS 9 0で故障を警告表示するための表示変更、つまりシンボルの表示色の変更を行ってからステップS 9 1に移行する。そうでない場合には、判定はNoとなってそのステップS 9 1に移行する。

【0065】

ステップS 9 1では、同じ要因の異常により出力されたログのなかでカウント値が閾値を越えているものがあるか否かを判定する(図9)。そのようなログが有った場合、判定はYesとなり、ステップS 9 2でエラー予兆を警告表示するための表示変更、つまりシンボルの表示色の変更を行ってから、上記ステップS 8 2に戻る。そうでない場合には、判定はNoとなり、そのステップS 8 2に戻る。

【0066】

ステップS 8 2での分類ログテーブルの選択は、関連付け定義情報25を参照して行われる。それにより、関連付け定義情報25で登録された組み合わせの一方を選択した後は、次にその組み合わせで残った方を選択する。そのような選択を行うことにより、図7に示すように、関連付け定義情報25に登録された組み合わせ毎に監視対象のログをまとめる形で表示するようにしている。

【0067】

なお、本実施形態は、監視対象を搭載したコンピュータであるサーバ10上で実現されているが、外部装置として、或いは外部装置上に実現させても良い。また、出力されたログは対応する分類ログテーブルに格納することで予め整理するようにしているが、ログの出力時に、ログファイル16に記録されたログを対象に整理を行うようにしても良い。

【0068】

図15は、ハードウェア構成の実施形態の一例を示す図である。ここで図15を参照して、本実施形態によるログ管理装置として適用可能なコンピュータ(情報処理装置)の構成について具体的に説明する。

【0069】

図15に示すコンピュータは、CPU61、メモリ62、入力装置63、出力装置64、外部記憶装置65、媒体駆動装置66、及びネットワーク接続装置67を有し、これらがバス68によって互いに接続された構成となっている。同図に示す構成は一例であり、これに限定されるものではない。

【0070】

CPU61は、当該コンピュータ全体の制御を行う。

メモリ62は、プログラム実行、データ更新等の際に、外部記憶装置65(あるいは可搬型の記録媒体M)に記憶されているプログラムあるいはデータを一時的に格納するRAM等のメモリである。CPU61は、プログラムをメモリ62に読み出して実行することにより、全体の制御を行う。

【0071】

入力装置63は、例えば、キーボード、マウス等の操作装置と接続されたインターフェースである。操作装置に対するユーザの操作を検出し、その検出結果をCPU61に通知する。

【0072】

出力装置64は、例えば表示装置と接続された表示制御装置である。ネットワーク接続装置67は、例えばイントラネットやインターネット等の通信ネットワークを介して、外部装置と通信を行うためのものである。外部記憶装置65は、例えばハードディスク装置である。主に各種データやプログラムの保存に用いられる。

【0073】

媒体駆動装置66は、光ディスクや光磁気ディスク等の可搬型の記録媒体Mにアクセス

10

20

30

40

50

するものである。

上述の構成では、ログ管理ソフトは外部記憶装置 65、若しくは記録媒体 M にアクセスするか、或いはネットワーク接続装置 67 を介して取得される。そのようにして取得可能なログ管理装置を CPU 61 に実行させることにより、本実施形態によるログ管理装置 20 は実現される。

【 0074 】

構成テーブル群 24、関連付け定義情報 25、及び分類ログテーブル群 26 は、例えば外部記憶装置 65 に保存され、必要に応じてメモリ 62 に読み出される。ログファイル 16、ハードウェア構成情報 14、及びソフトウェア構成情報 15 は、例えば外部記憶装置 65 に保存される。ログ出力（表示）は、例えば出力装置 64、或いはネットワーク接続装置 67 を介して行われる。そのログ出力は、媒体駆動装置 66 を介して記録媒体 M にデータを記録することで行わせることもできる。このことからログ管理装置 20 は、ログを出力するサーバ 20（情報処理装置）とは異なる情報処理装置に搭載しても良い。ログ管理装置 20 にログを管理させる情報処理装置は複数台であっても良い。

10

【 0075 】

以上の変形例を含む実施形態に関し、更に以下の付記を開示する。

（付記 1）

情報処理装置を構成する部品、及び実行中のプログラムを監視対象として監視することで該情報処理装置が出力するログを該情報処理装置、及び別の情報処理装置の一方により管理する方法において、

20

前記ログを前記情報処理装置に存在する前記監視対象毎に分類する分類ステップと、  
前記監視対象をハードウェア及びソフトウェアのカテゴリに分け、互いに異なるカテゴリに属する監視対象間で動作に関連性が存在すると見なす監視対象の組み合わせを示す関連付け定義情報を参照して、前記分類ステップでログを分類した監視対象のなかで該関連付け定義情報に示されている組み合わせを特定する特定ステップと、

前記特定ステップで特定した前記組み合わせに基づいて、前記分類ステップで前記監視対象毎に分類したログを対応付けて表示装置上に出力する出力ステップと、

を含むことを特徴とするログ管理方法。

（付記 2）

前記ログが出力された前記監視対象の順序、及び該監視対象が属するカテゴリを基に、前記組み合わせを前記関連付け定義情報として登録することにより、該関連付け定義情報を更新する更新ステップ、

30

を更に含むことを特徴とする付記 1 記載のログ管理方法。

（付記 3）

前記更新ステップでは、前記ログが出力される前記監視対象の順序を監視することにより、互いに異なるカテゴリに属する複数の監視対象のログが連続する同一のパターンが複数回、繰り返された場合に、該同一のパターンを構成するログが出力された複数の監視対象の組み合わせを前記関連付け定義情報として登録する、

ことを特徴とする付記 2 記載のログ管理方法。

（付記 4）

40

前記出力ステップでは、前記特定ステップで特定した前記組み合わせ毎に、前記分類ステップで前記監視対象毎に分類したログを示すシンボルを時系列に沿って配置した形で表示出力させる、

ことを特徴とする付記 1 記載のログ管理方法。

（付記 5）

前記監視対象毎に、一定時間内に出力されたログを解析して、該ログが出力された監視対象の状態を判断する解析ステップを更に含み、

前記出力ステップでは、前記解析ステップでの判断結果を共に出力する、

ことを特徴とする付記 4 記載のログ管理方法。

（付記 6）

50

前記分類ステップでは、前記監視対象毎に、該監視対象により出力されたログを格納するテーブルを作成することにより分類する、  
ことを特徴とする付記 2 記載のログ管理方法。

(付記 7)

情報処理装置を構成する部品、及び実行中のプログラムを監視対象として監視することで該情報処理装置から出力されるログを管理する装置において、

前記ログを前記情報処理装置に存在する前記監視対象毎に分類する分類手段と、

前記監視対象をハードウェア及びソフトウェアのカテゴリに分け、互いに異なるカテゴリに属する監視対象間で動作に関連性が存在すると見なす監視対象の組み合わせを示す関連付け定義情報を記憶した情報記憶手段と、

前記情報記憶手段に記憶された前記関連付け定義情報を参照して、前記分類ステップでログを分類した監視対象のなかで該関連付け定義情報に示されている組み合わせを特定する特定手段と、

前記特定手段が特定した前記組み合わせに基づいて、前記分類手段が前記監視対象毎に分類したログを対応付けて表示装置上に出力する出力手段と、

を具備することを特徴とするログ管理装置。

(付記 8)

付記 7 記載のログ管理装置を備えている、

ことを特徴とする情報処理装置。

(付記 9)

情報処理装置を構成する部品、及び実行中のプログラムを監視対象として監視することで該情報処理装置が出力するログを管理するログ管理装置として用いられるコンピュータに、

前記ログを前記情報処理装置に存在する前記監視対象毎に分類する分類機能と、

記憶手段に記憶された、前記監視対象をハードウェア及びソフトウェアのカテゴリに分け、互いに異なるカテゴリに属する監視対象間で動作に関連性が存在すると見なす監視対象の組み合わせを示す関連付け定義情報を参照して、前記分類機能によりログを分類した監視対象のなかで該関連付け定義情報に示されている組み合わせを特定する特定機能と、

前記特定機能により特定した前記組み合わせに基づいて、前記分類機能により前記監視対象毎に分類したログを対応付けて表示装置上に出力する出力機能と、

を実現させるためのプログラム。

【図面の簡単な説明】

【0076】

【図 1】本実施形態によるログ管理装置の構成を示す図である。

【図 2】ハード構成テーブルのデータ構成を示す図である。

【図 3】ソフト構成テーブルのデータ構成を示す図である。

【図 4】関連付け定義情報のデータ構成を示す図である。

【図 5】関連付け定義情報の更新方法を説明する図である。

【図 6】ログの関連付け方法を説明する図である。

【図 7】ログ表示例を示す図である。

【図 8】故障の判断方法を説明する図である。

【図 9】エラー予兆の判断方法を説明する図である。

【図 10】関連付け定義情報作成処理のフローチャートである。

【図 11】構成テーブル更新処理のフローチャートである。

【図 12】関連付け定義情報更新処理のフローチャートである。

【図 13】ログ分類処理のフローチャートである。

【図 14】二次元表示処理のフローチャートである。

【図 15】ハードウェア構成の実施形態の一例を示す図である。

【図 16】従来のログ管理装置の動作を説明する図である。

【図 17】従来のログ管理装置によりログファイルに格納されるログを説明する図である

10

20

30

40

50

。 【図18】 ログファイルに格納されたログの内容を示す図である。

【符号の説明】

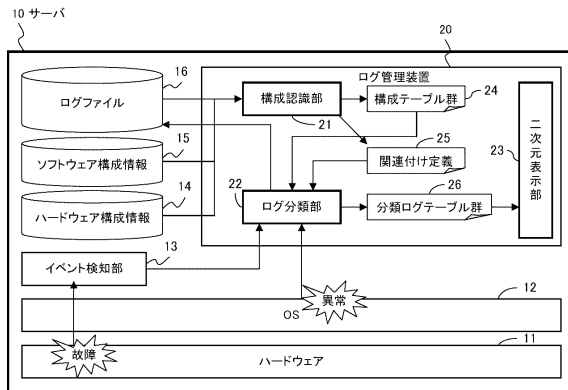
【0077】

- 10 サーバ
- 11 ハードウェア群
- 12 OS
- 13 イベント検知部
- 14 ハードウェア構成情報
- 15 ソフトウェア構成情報
- 16 ログファイル
- 20 ログ管理装置
- 21 構成認識部
- 22 ログ分類部
- 23 二次元表示部
- 24 構成テーブル群
- 25 関連付け定義
- 26 分類ログテーブル群

【図1】

【図2】

本実施形態による  
ログ管理装置の構成を示す図



ハード構成テーブルの  
データ構成を示す図

部品	搭載位置	状態	キーワード
部品HA	CPU-SLOT#0	normal	CPU.cpu,Cpu
部品HB	MEM-SLOT#0	normal	MEM.mem,Mem
部品HC	MEM-SLOT#1	normal	MEM.mem,Mem
部品HD	MEM-SLOT#2	normal	MEM.mem,Mem
部品HE	MEM-SLOT#3	normal	MEM.mem,Mem
部品HF	PCI-SLOT#0	normal	PCI.pci
部品HG	PCI-SLOT#1	normal	PCI.pci
部品HH	PCI-SLOT#2	normal	PCI.pci
:			

【図3】

ソフト構成テーブルのデータ構成を示す図

ソフト名	カテゴリ	詳細情報
ソフトSA	system	CPU patrol diagnosis
ソフトSB	system	Memory driver
ソフトSC	application	Web Browser
ソフトSD	system	Core Kernel software
ソフトSE	application	Header files
ソフトSF	system	Drivers for the PCI bus
ソフトSG	system	PCI Ethernet Driver
:		

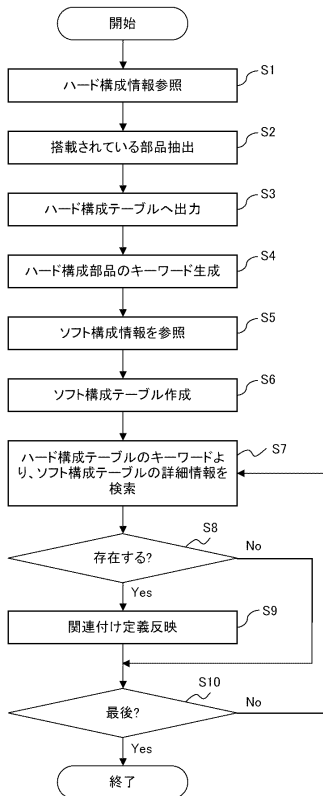
【図4】

関連付け定義情報のデータ構成を示す図

部品	関連ソフト
部品HA	ソフトSA
部品HB	ソフトSB
—	ソフトSC
部品HF	ソフトSF、ソフトSG
:	

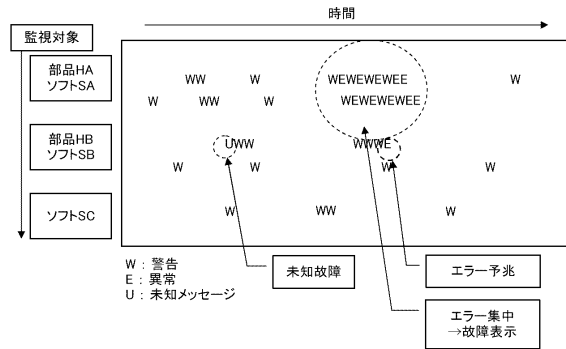
【図10】

関連付け定義情報作成処理のフローチャート



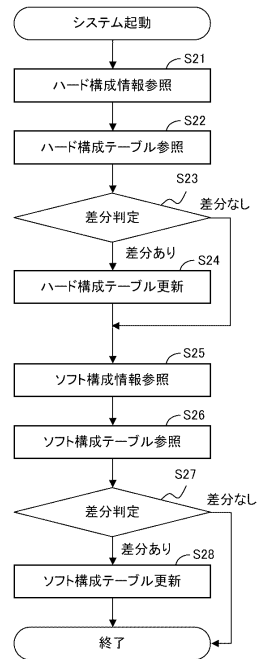
【図7】

ログ表示例を示す図



【図11】

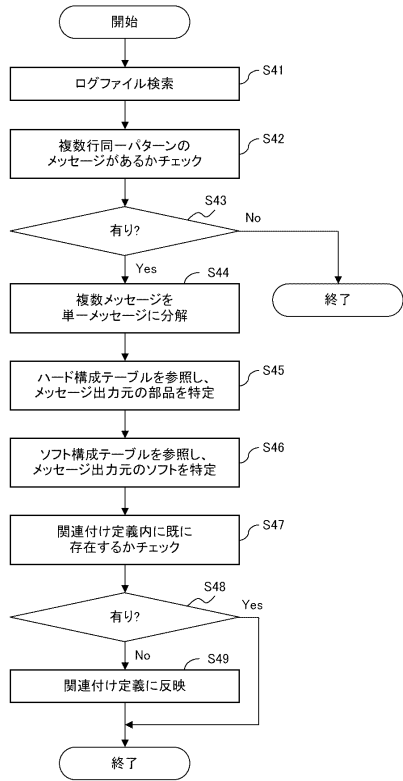
構成テーブル更新処理のフローチャート





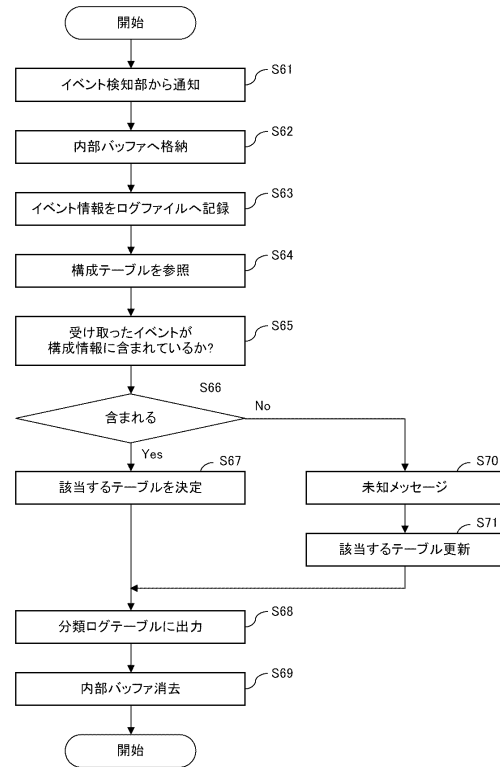
【図12】

関連付け定義情報更新処理のフローチャート



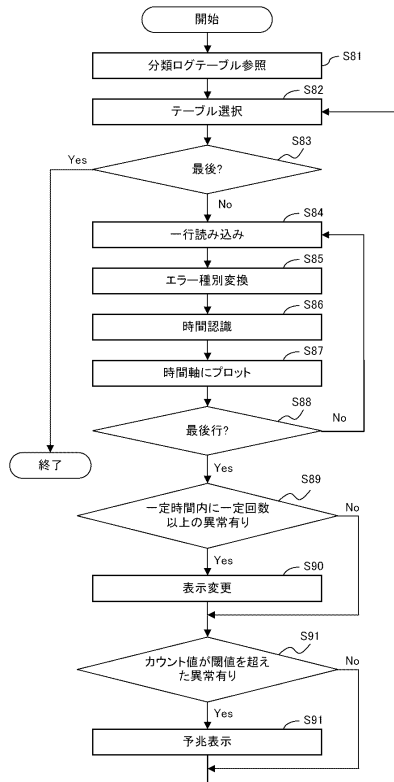
【図13】

ログ分類処理のフローチャート



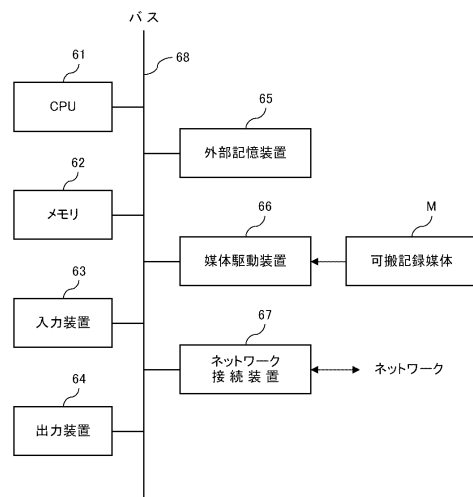
【図14】

二次元表示処理のフローチャート



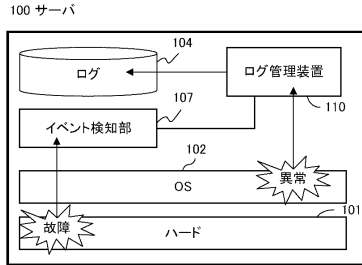
【図15】

ハードウェア構成の実施形態の一例を示す図



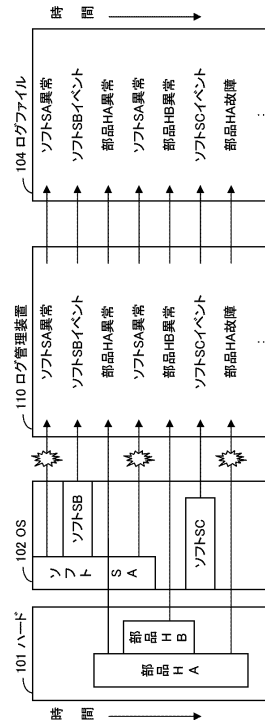
【図16】

従来のログ管理装置の動作を説明する図



【図17】

従来のログ管理装置によりログファイルに格納されるログを説明する図



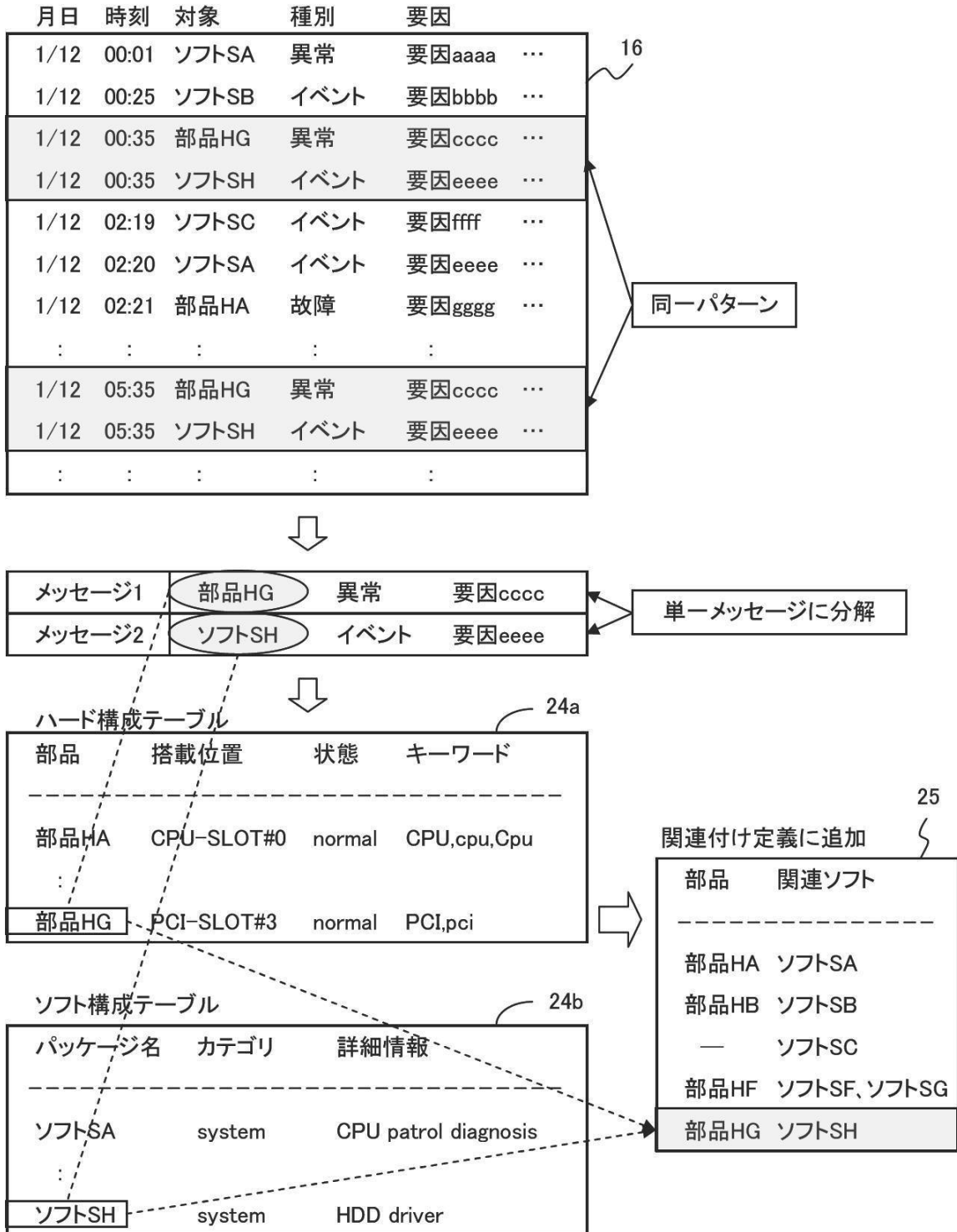
【図18】

ログファイルに格納されたログの内容を示す図

月日	時刻	対策	種別	要因
1/12	00:01	ソフトSA	異常	要因 aaaa ...
1/12	00:25	ソフトSB	イベント	要因 bbbb ...
1/12	00:35	部品HA	異常	要因 cccc ...
1/12	00:36	ソフトSA	異常	要因 dddd ...
1/12	01:53	部品HB	異常	要因 eeee ...
1/12	02:19	ソフトSC	イベント	要因 ffff ...
1/12	02:21	部品HA	故障	要因 gggg ...
:	:	:	:	:
1/25	05:42	ソフトSA	異常	要因 zzzz ...

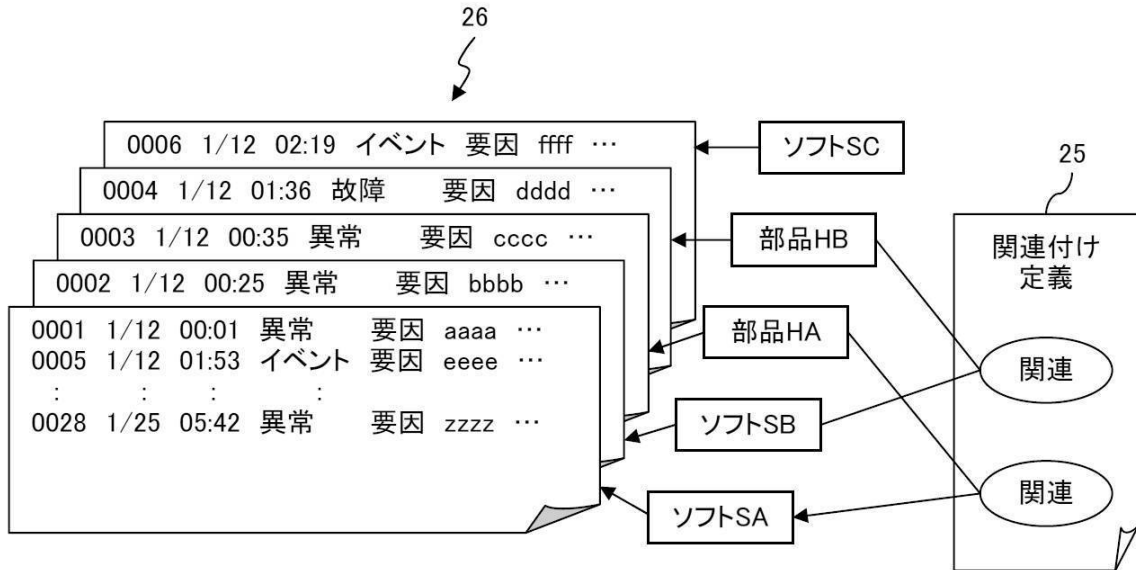
【図5】

### 関連付け定義情報の更新方法を説明する図



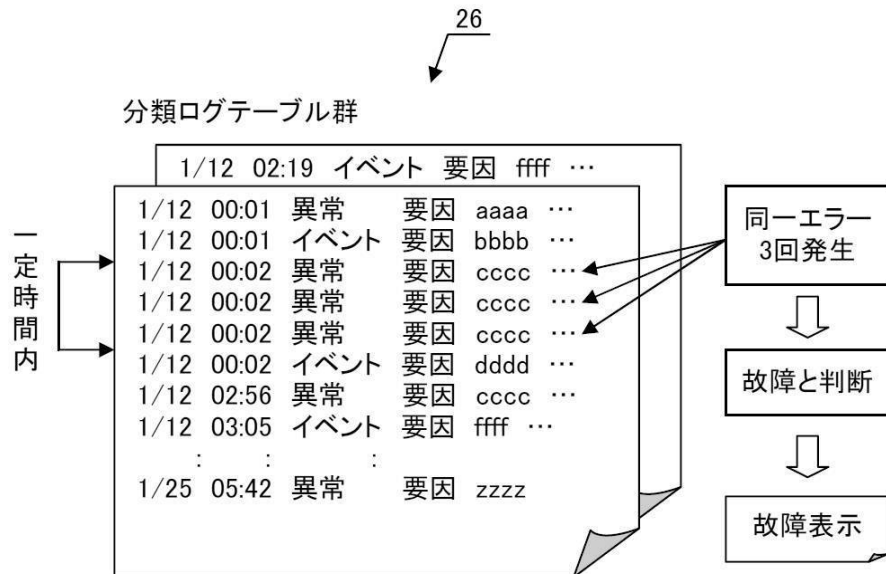
【図6】

### ログの関連付け方法を説明する図



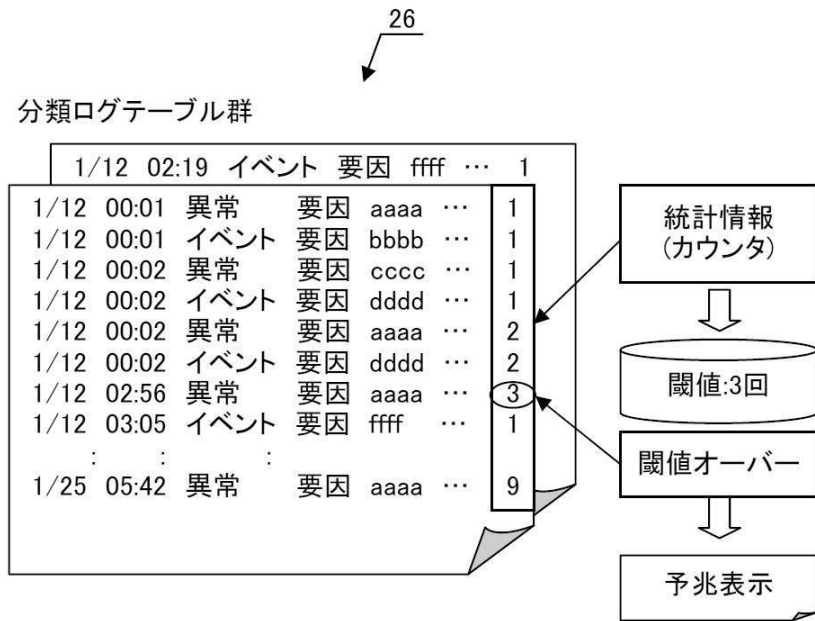
【図8】

### 故障の判断方法を説明する図



【図9】

### エラー予兆の判断方法を説明する図



---

フロントページの続き

- (56)参考文献 特開2001-256032(JP,A)  
特開2008-065668(JP,A)  
特開2008-140248(JP,A)  
特開2003-091434(JP,A)

(58)調査した分野(Int.Cl., DB名)

G06F 11/30  
G06F 11/32  
G06F 11/34