

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第6160064号
(P6160064)

(45) 発行日 平成29年7月12日 (2017. 7. 12)

(24) 登録日 平成29年6月23日 (2017. 6. 23)

(51) Int. Cl.	F 1
GO 6 F 11/30 (2006. 01)	GO 6 F 11/30 1 5 1
GO 6 F 11/34 (2006. 01)	GO 6 F 11/30 1 7 2
	GO 6 F 11/34 1 5 2

請求項の数 7 (全 28 頁)

(21) 出願番号	特願2012-253731 (P2012-253731)	(73) 特許権者	000005223
(22) 出願日	平成24年11月19日 (2012. 11. 19)		富士通株式会社
(65) 公開番号	特開2014-102661 (P2014-102661A)		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26年6月5日 (2014. 6. 5)	(74) 代理人	100089118
審査請求日	平成27年7月6日 (2015. 7. 6)		弁理士 酒井 宏明
		(72) 発明者	渡辺 幸洋
			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	大塚 浩
			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	松本 安英
			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】 適用判定プログラム、障害検出装置および適用判定方法

(57) 【特許請求の範囲】

【請求項 1】

コンピュータに、

第1のシステム構成において障害の予兆検出に用いられる障害予兆パターンを、前記第1のシステム構成において過去に発生した障害事象に基づいて生成し、

前記第1のシステム構成から第2のシステム構成へシステム構成が遷移する際に、前記システム構成の時間的連続性に着目した、前記システム構成に依存しない構成要素の変更回数と、前記システム構成の空間的連続性に着目した、前記システム構成の変更履歴に依存しない構成要素の差分数とを算出し、

生成された前記障害予兆パターンを用いて前記障害の予兆が検出された場合に、前記構成要素の変更回数および前記構成要素の差分数を座標とする点と前記座標の原点との距離である差分距離が閾値以下か否かを判定し、

前記差分距離が前記閾値以下である場合に、前記障害予兆パターンが有効と判定し、前記障害の予兆を通知する

処理を実行させることを特徴とする適用判定プログラム。

【請求項 2】

前記算出する処理は、さらに、前記第1のシステム構成時におけるシステムの負荷量と前記第2のシステム構成時におけるシステムの負荷量との比である負荷量比を算出し、

前記判定する処理は、前記構成要素の変更回数と前記構成要素の差分数と前記負荷量比とを座標とする点と前記座標の原点との距離である差分距離が閾値以下か否かを判定し、

10

20

前記通知する処理は、前記差分距離が前記閾値以下である場合に、前記障害予兆パターンが有効と判定し、前記障害の予兆を通知することを特徴とする請求項 1 に記載の適用判定プログラム。

【請求項 3】

前記算出する処理は、さらに、前記第 1 のシステム構成時におけるシステムの負荷の傾向を示す負荷パターンと前記第 2 のシステム構成時におけるシステムの負荷傾向を示す負荷パターンとの差である負荷パターン差を算出し、

前記判定する処理は、前記構成要素の変更回数と前記構成要素の差分数と前記負荷パターン差とを座標とする点と前記座標の原点との距離である差分距離が閾値以下か否かを判定し、

10

前記通知する処理は、前記差分距離が前記閾値以下である場合に、前記障害予兆パターンが有効と判定し、前記障害の予兆を通知することを特徴とする請求項 1 または 2 に記載の適用判定プログラム。

【請求項 4】

前記算出する処理は、前記構成要素の変更回数と前記構成要素の差分数とさらに、前記第 1 のシステム構成時におけるシステムの負荷量と前記第 2 のシステム構成時におけるシステムの負荷量との比である負荷量比または前記第 1 のシステム構成時におけるシステムの負荷の傾向を示す負荷パターンと前記第 2 のシステム構成時におけるシステムの負荷の傾向を示す負荷パターンとの差である負荷パターン差のうち、少なくとも 1 つを算出し、

前記判定する処理は、前記構成要素の変更回数と前記構成要素の差分数と前記負荷量比とを座標とする点と前記座標の原点との距離である差分距離が閾値以下か否か、または、前記構成要素の変更回数と前記構成要素の差分数と前記負荷パターン差とを座標とする点と前記座標の原点との距離である差分距離が閾値以下か否かを判定し、

20

前記通知する処理は、前記差分距離が前記閾値以下である場合に、前記障害予兆パターンが有効と判定し、前記障害の予兆を通知することを特徴とする請求項 1 に記載の適用判定プログラム。

【請求項 5】

前記障害予兆パターンを用いて障害の予兆を検出し、

前記障害の予兆が検出された後に、実際に障害が発生したか否かを判定し、

判定した結果に基づいて、前記閾値を決定する処理を前記コンピュータにさらに実行させることを特徴とする請求項 1 から 4 のいずれか一つに記載の適用判定プログラム。

30

【請求項 6】

第 1 のシステム構成において障害の予兆検出に用いられる障害予兆パターンを、前記第 1 のシステム構成において過去に発生した障害事象に基づいて生成する生成部と、

前記第 1 のシステム構成から第 2 のシステム構成へシステム構成が遷移する際に、前記システム構成の時間的連続性に着目した、前記システム構成に依存しない構成要素の変更回数と、前記システム構成の空間的連続性に着目した、前記システム構成の変更履歴に依存しない構成要素の差分数とを算出する算出部と、

前記生成部によって生成された前記障害予兆パターンを用いて前記障害の予兆が検出された場合に、前記構成要素の変更回数および前記構成要素の差分数を座標とする点と前記座標の原点との距離である差分距離が閾値以下か否かを判定し、前記差分距離が前記閾値以下である場合に、前記障害予兆パターンが有効と判定し、前記障害の予兆を通知する判定部と

40

を有することを特徴とする障害検出装置。

【請求項 7】

コンピュータが、

第 1 のシステム構成において障害の予兆検出に用いられる障害予兆パターンを、前記第 1 のシステム構成において過去に発生した障害事象に基づいて生成し、

前記第 1 のシステム構成から第 2 のシステム構成へシステム構成が遷移する際に、前記システム構成の時間的連続性に着目した、前記システム構成に依存しない構成要素の変更

50

回数と、前記システム構成の空間的連続性に着目した、前記システム構成の変更履歴に依存しない構成要素の差分数とを算出し、

生成された前記障害予兆パターンを用いて前記障害の予兆が検出された場合に、前記構成要素の変更回数および前記構成要素の差分数を座標とする点と前記座標の原点との距離である差分距離が閾値以下か否かを判定し、

前記差分距離が前記閾値以下である場合に、前記障害予兆パターンが有効と判定し、前記障害の予兆を通知する

処理を含んだことを特徴とする適用判定方法。

【発明の詳細な説明】

【技術分野】

10

【0001】

本発明は、適用判定プログラム、障害検出装置および適用判定方法に関する。

【背景技術】

【0002】

情報処理システムで発生する障害を検出する方法として、障害の予兆を示す障害予兆パターンを用いる障害検出装置が知られている。例えば、障害検出装置は、過去のログと障害発生情報とから、障害が起こる共起確率が高いメッセージの組み合わせを抽出する。そして、障害検出装置は、情報処理システムにおいて障害予兆パターンと同じ組み合わせのメッセージが出力された場合に、障害が発生する可能性があるかと判定する。

【0003】

20

また、障害の検出に用いる障害判定ルールを他のシステム等に流用する際に、情報処理システムを構成する構成要素ごとに流用可否の基準を設ける手法が知られている。例えば、OS (Operating System) の監視項目が閾値以上一致している場合やOSのバージョンが一致している場合に、障害判定ルールを流用すると判定する。

【先行技術文献】

【特許文献】

【0004】

【特許文献1】特開2009-176203号公報

【特許文献2】特開2012-3713号公報

【発明の概要】

30

【発明が解決しようとする課題】

【0005】

しかしながら、上記の技術では、共起確率に基づいて障害予兆パターンが生成されるので、システム構成の変化が当該パターンに与える影響度が明確ではなく、障害予兆パターンの適用が妥当か否かを判定できないという問題がある。

【0006】

例えば、クラウドシステムは、システムを構成する構成要素も多く、システム構成も頻繁に変わる。したがって、システム構成が変更されるたびに障害予兆パターンを学習すると、学習時間が短くなるので、生成される障害予兆パターンの信頼性も低下する。

【0007】

40

また、構成要素ごとに基準を設ける手法を障害予兆パターンに適用した場合、構成要素ごとに基準を作成し、システム構成が変わるたびに基準に応じて障害予兆パターンを変更することになる。したがって、この手法は、作業負担も多くなり、クラウドシステムには適さない。

【0008】

このように、上記の技術では、特定の情報処理システムに適用される障害予兆パターンが有効なパターンであるか否かを判定できないので、有効ではない障害予兆パターンが適用されてしまい、障害の予兆を見逃すことが発生する。

【0009】

1つの側面では、障害の予兆を検出する際に用いる障害予兆パターンの有効性を判定す

50

ることができる適用判定プログラム、障害検出装置および適用判定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】

第1の案では、コンピュータに、第1のシステム構成において障害の予兆検出に用いられる障害予兆パターンを、前記第1のシステム構成において過去に発生した障害事象に基づいて生成する処理を実行させる。コンピュータに、前記第1のシステム構成から第2のシステム構成へシステム構成が遷移する際に、システムを構成する構成要素の変更が実行された累積回数である変更回数を用いて、システム構成間の差を示す差分情報を算出する処理を実行させる。コンピュータに、算出した前記差分情報に応じて、前記第2のシステム構成における障害の予兆検出への前記障害予兆パターンの適用可否を判定する処理を実行させる。

10

【発明の効果】

【0011】

本発明の1実施態様によれば、障害の予兆を検出する際に用いる障害予兆パターンの有効性を判定することができる。

【図面の簡単な説明】

【0012】

【図1】図1は、実施例1に係るシステムの全体構成例を示す図である。

【図2】図2は、実施例1に係る障害検出装置の機能構成を示す機能ブロック図である。

20

【図3】図3は、構成情報DBに記憶される情報の例を示す図である。

【図4】図4は、構成要素の関係性を説明する図である。

【図5】図5は、構成変更情報DBに記憶される情報の例を示す図である。

【図6】図6は、管理メッセージDBに記憶される情報の例を示す図である。

【図7】図7は、障害情報DBに記憶される情報の例を示す図である。

【図8】図8は、障害予兆パターンDBに記憶される情報の例を示す図である。

【図9】図9は、障害予兆記録DBに記憶される情報の例を示す図である。

【図10】図10は、障害予兆パターンの学習を説明する図である。

【図11】図11は、構成情報の遷移を説明する図である。

【図12】図12は、障害予兆パターンの有効範囲を説明する図である。

30

【図13】図13は、障害予兆検出時の構成情報例を示す図である。

【図14】図14は、構成の変更回数を説明する図である。

【図15】図15は、構成の差分数を説明する図である。

【図16】図16は、判定基準を説明する図である。

【図17】図17は、閾値の学習を説明する図である。

【図18】図18は、障害予兆学習処理の流れを示すフローチャートである。

【図19】図19は、障害予兆検出処理の流れを示すフローチャートである。

【図20】図20は、予兆通報判定処理の流れを示すフローチャートである。

【図21】図21は、構成差分算出処理の流れを示すフローチャートである。

【図22】図22は、閾値学習処理の流れを示すフローチャートである。

40

【図23】図23は、負荷量を説明する図である。

【図24】図24は、負荷パターンを説明する図である。

【図25】図25は、ハードウェア構成例を説明する図である。

【発明を実施するための形態】

【0013】

以下に、本願の開示する適用判定プログラム、障害検出装置および適用判定方法の実施例を図面に基づいて詳細に説明する。なお、この実施例によりこの発明が限定されるものではない。

【実施例1】

【0014】

50

[全体構成]

図1は、実施例1に係るシステムの全体構成例を示す図である。図1に示すように、このシステムは、複数のクライアント端末1とデータセンタ2と、C M D B (Configuration Management Database) 5と障害検出装置10とを有し、クラウドシステムによるサービスをクライアント端末1に提供するシステムである。

【0015】

各クライアント端末1は、データセンタ2にアクセスしてクラウドシステムを利用し、サービスの提供を受ける端末である。データセンタ2には、複数の物理サーバが設置され、複数の仮想マシンが動作し、複数の仮想マシンによって顧客ごとに情報処理システムを構築する。各情報処理システムは、同じテンプレートから生成され、各顧客にサービスを提供する。

10

【0016】

C M D B 5は、データセンタ2で提供される情報処理システムの構成を統合管理するデータベースである。C M D B 5は、各情報処理システムが有する構成要素 (CI: Configuration Item)、各構成要素の属性、各構成要素が他の情報処理システムの構成要素との間で有する関係性などを関連付けて管理する。

【0017】

障害検出装置10は、C M D B 5を用いて、データセンタ2で提供される情報処理システムで発生する障害の予兆を検出するサーバである。このような状態において、障害検出装置10は、第1のシステム構成において障害の予兆検出に用いられる障害予兆パターンを、第1のシステム構成において過去に発生した障害事象に基づいて生成する。そして、障害検出装置10は、第1のシステム構成から第2のシステム構成へシステム構成が遷移する際に、システムを構成する構成要素の変更が実行された累積回数である変更回数を用いて、システム構成間の差を示す差分情報を算出する。その後、障害検出装置10は、算出した差分情報に応じて、第2のシステム構成における障害の予兆検出への障害予兆パターンの適用可否を判定する。

20

【0018】

このように、障害検出装置10は、障害予兆パターンを学習した時のシステム構成と、当該パターンが適用されるシステム構成との異なり具合を定量化し、学習時と異なるシステムへの適用可否を判定することで、障害予兆パターンの有効性を判定することができる。

30

【0019】

[障害検出装置の構成]

図2は、実施例1に係る障害検出装置の機能構成を示す機能ブロック図である。なお、図1に示したクライアント端末1は一般的なコンピュータと同様の機能構成を有するので、詳細な説明は省略する。同様に、データセンタ2が有する物理サーバの機能構成についても、一般的なサーバと同様の構成を有するので、詳細な説明は省略する。

【0020】

図2に示すように、障害検出装置10は、通信処理部11、記憶部12、制御部20を有する。ここで、通信処理部11は、ネットワークインターフェースカードなどであり、記憶部12は、メモリなどの記憶装置であり、制御部20は、C P U (Central Processing Unit) などのプロセッサである。

40

【0021】

通信処理部11は、他の装置との間の通信を制御する処理部である。例えば、通信処理部11は、データセンタ2からログメッセージを受信する。また、通信処理部11は、図示しない管理装置に障害の発生や障害の予兆を通知する。また、通信処理部11は、データセンタ2内の情報処理システムを構成する構成要素の変更や、発生した障害情報などを管理装置などから受け付ける。

【0022】

記憶部12は、構成情報D B 13、構成変更情報D B 14、管理メッセージD B 15、

50

障害情報DB16、障害予兆パターンDB17、障害予兆記録DB18を保持する。

【0023】

構成情報DB13は、データセンタ2内の情報処理システムの構成情報を記憶する。具体的には、構成情報DB13は、情報処理システムごとに、情報処理システムを構成する構成要素と、各構成要素間の関係性を記憶する。この構成情報DB13は、CMD B5そのものであってもよく、CMD B5から取得したデータを記憶する記憶部であってもよい。図3は、構成情報DBに記憶される情報の例を示す図である。なお、図3には、一例としてXML (Extensible Markup Language) 形式で構成情報を管理する例を図示したが、これに限定されるものではなく、他の形式であってもよい。

【0024】

図3に示すように、構成情報DB13は、構成要素の情報を管理する「CIs」と、構成要素間の関係性を示す「Relations」とを記憶する。ここで設定される情報は、管理者等によって変更される。「CIs」は、「CI id」と「item」と「type」と「ip」等を含むレコードで構成要素を定義して管理する。「CI id」には、構成要素を識別する識別子が設定される。「item」には、構成要素の情報処理システム上での役割が設定される。「type」は、構成要素の名称等が設定される。「ip」は、構成要素に割当てたアドレスが設定される。

【0025】

例えば、図3の「CIs」の1行目は、「type=PC1」の構成要素が、情報処理システム上で「Pc」として動作し、「CI id=0S0IW3SH」で識別されることを定義する。同様に、図3の「CIs」の3行目は、「type=OS (A)」の構成要素が、情報処理システム上で「Os」として動作し、「CI id=H38FHZ0S」で識別されるとともに、「ip=192.168.1.10」が設定されることを定義する。また、図3の「CIs」の5行目は、「type=AP1」の構成要素が、情報処理システム上で「APP」すなわちアプリケーションとして動作し、「CI id=2H9JIIHY」で識別されることを定義する。また、図3の「CIs」の7行目は、「type=table__a」の構成要素が、情報処理システム上で「Instance」すなわち記憶部として動作し、「CI id=HREIO928」で識別されることを定義する。

【0026】

また、「Relations」は、「Relations id」、「src」、「dst」、「type」等を含むレコードで構成要素間の関係性を定義する。「Relations id」には、関係性を識別する識別子が設定される。「src」には、関係元の構成要素の識別子が設定され、「dst」には、関係先の構成要素の識別子が設定される。「tyep」には、関係性を特定する情報が設定される。

【0027】

図3の「Relations」の1行目は、「src」側の「CI id=0S0IW3SH」である「PC1」が、「dst」側の「CI id=H38FHZ0S」である「OS (A)」を保持していることを定義する。「type」に設定される「Has」は、関係元が関係先を保持している関係、すなわち、関係先が関係元で動作している関係を示す。また、「InstalledOn」は、関係先が関係元にインストールされている関係を示す。「ConnectedTo」は、関係元と関係先とが相互に接続されている関係を示す。「Use」は、関係元が関係先を使用や参照する関係を示す。「DeployedOn」は、関係元が関係先を利用可能にする関係、すなわち、関係元を用いて関係先を利用する関係を示す。

【0028】

ここで、図3で説明した構成要素の関係性を図4に図示する。図4は、構成要素の関係性を説明する図である。図4では、四角が構成要素で、矢印が関係性を示す。図4に示すように、構成要素「PC1」が構成要素「OS (A)」を保持し、構成要素「OS (A)」が構成要素「AP1」を保持し、構成要素「AP1」が構成要素「table__a」を保持する。また、構成要素「table__a」が構成要素「AP1」で利用可能に制御され、構成要素「AP1」が構成要素「OS (A)」にインストールされ、構成要素「OS (A)」が構成要素「PC1」にインストールされている。

10

20

30

40

50

【0029】

同様に、構成要素「PC2」が構成要素「OS (B)」を保持し、構成要素「OS (B)」が構成要素「AP2」を保持し、構成要素「AP2」が構成要素「servlet__a」を保持する。また、構成要素「servlet__a」が構成要素「AP2」で利用可能に制御され、構成要素「AP2」が構成要素「OS (B)」にインストールされ、構成要素「OS (B)」が構成要素「PC2」にインストールされている。また、構成要素「OS (A)」と構成要素「OS (B)」とが接続されており、構成要素「servlet__a」が構成要素「table__a」を参照している。

【0030】

また、図4に示した全構成要素で1つの情報処理システムとして動作し、テナントとして顧客にサービスを提供する。なお、「PC1」と「OS (A)」と「AP1」と「table__a」とがテナント1として顧客にサービスを提供し、「PC2」と「OS (B)」と「AP2」と「servlet__a」とがテナント2として顧客にサービスを提供するようにすることもできる。

10

【0031】

図2に戻り、構成変更情報DB14は、情報処理システムの構成変更を記憶する。ここで記憶される情報は、後述する構成変更学習部21によって更新されてもよく、管理者等によって更新されてもよい。図5は、構成変更情報DBに記憶される情報の例を示す図である。

【0032】

図5に示すように、構成変更情報DB14は、「時刻、変更種別、対象、パラメータ」を記憶する。「時刻」は、構成変更が実行された日時を示す。「変更種別」は、変更された内容を示し、削除された場合には「DEL」、追加された場合には「ADD」、設定変更された場合には「MOD」が設定される。「対象」は、変更された構成要素を示す。「パラメータ」は、変更されたパラメータを示す。なお、構成変更情報DB14は、これらの情報以外にも、例えば変更が実行された情報処理システムやテナントを特定する情報等を記憶してもよい。

20

【0033】

図5の場合、「日本標準時の2012年3月13日10:31:02」に、構成要素「2H9JIIHY」が情報処理システムから削除されたことを示す。また、「日本標準時の2012年3月13日10:35:28」に、構成要素「220GEANA」が情報処理システムに追加されたことを示す。また、「日本標準時の2012年3月25日21:00:18」に、構成要素「93H6SK8A」の設定として「OSのバージョン」が「SP3」に変更されたことを示す。

30

【0034】

管理メッセージDB15は、情報処理システムの各構成要素等から出力されるログメッセージを記憶する。ここで記憶される情報は、後述するメッセージ収集部22によって更新されてもよく、管理者等によって更新されてもよい。図6は、管理メッセージDBに記憶される情報の例を示す図である。

【0035】

図6に示すように、管理メッセージDB15は、フィールド15aから15eで構成される各メッセージを記憶する。時刻フィールド15aには、ログメッセージが出力された日時が出力される。ホスト名フィールド15bには、ログメッセージを出力した構成要素のホスト名が出力される。モジュール名フィールド15cには、ログメッセージを出力したモジュール名が出力される。メッセージ種別フィールド15dには、ログメッセージの種別を識別するメッセージIDが出力される。メッセージフィールド15eには、出力されたログメッセージの詳細な内容が出力される。

40

【0036】

ホスト名フィールド15bと、モジュール名フィールド15cとを用いて、構成情報を特定することができる。具体的には、図6のホスト名フィールド15bが図3の「item」に対応し、図6のモジュール名フィールド15cが図3の「type」に対応する。

【0037】

障害情報DB16は、発生した障害の情報を記憶する。ここで記憶される情報は、管理

50

者等によって更新されてもよく、制御部20が管理者端末から取得して更新してもよい。図7は、障害情報DBに記憶される情報の例を示す図である。なお、図7には、一例としてXML形式で障害情報を管理する例を図示したが、これに限定されるものではなく、他の形式であってもよい。

【0038】

図7に示すように、障害情報DB16は、「Trouble uid」と「type」と「date」と「title」等を含むレコードで障害情報を記憶する。「Trouble uid」は、障害情報を識別する識別子である。「type」は、障害の種別を特定する情報である。「date」は、障害が発生した日時である。「title」は、障害の内容である。

【0039】

図7を例にして説明すると、「Web Down」の障害を示す「T001」が「日本標準時の2012年3月13日の10:51:02」に発生し、この障害が「201203130001」で識別されることを示す。また、「Web Down」の障害を示す「T001」が「日本標準時の2014年4月12日の16:31:08」にも発生し、この障害が「201204120001」で識別されることを示す。同様に、「DB Slow Down」の障害を示す「T003」が「日本標準時の2012年3月18日の03:25:22」に発生し、この障害が「201203180025」で識別されることを示す。

【0040】

障害予兆パターンDB17は、障害の予兆を特定するログメッセージのパターンである障害予兆パターンと、当該パターンが生成されたときの構成情報とを対応付けて記憶する。ここで記憶される情報は、後述する障害予兆学習部23によって更新される。図8は、障害予兆パターンDBに記憶される情報の例を示す図である。図8に示すように、障害予兆パターンDB17は、障害予兆パターン17aと、学習時の構成情報17bとを対応付けて記憶する。

【0041】

障害予兆パターン17aは、「障害、メッセージパターン、発生総数、障害前発生数、共起確率」で構成される。「障害」は、障害の種別を特定する情報であり、図7に示した「type」に対応する。「メッセージパターン」は、障害が実際に検出される前に発生するメッセージの組み合わせであり、図6に示したメッセージ種別フィールド15dに出力された識別子の組み合わせである。「発生総数」は、当該メッセージパターンが発生した回数である。「障害前発生数」は、当該メッセージパターンが発生した後に、障害が実際に検出された回数である。「共起確率」は、メッセージパターンが発生した際に障害が発生する確率であり、障害前発生数/発生総数で算出された値である。

【0042】

図8の場合、障害予兆パターン「0005、0007、0012」は、今までに572回発生し、そのうち534回で実際に障害「T001」が発生しており、当該パターンが発生した際に障害「T001」が起こる共起確率が「0.93」であることを示している。同様に、障害予兆パターン「0005、0007、0012」は、今までに572回発生し、そのうち501回で実際に障害「T002」が発生しており、当該パターンが発生した際に障害「T002」が起こる共起確率が「0.88」であることを示している。また、障害予兆パターン「0008、0036、0041、0108」は、今までに72回発生し、そのうち62回で実際に障害「T001」が発生しており、当該パターンが発生した際に障害「T001」が起こる共起確率が「0.86」であることを示している。

【0043】

学習時の構成情報17bは、障害予兆パターンごとに「学習時刻、構成情報（時刻、メッセージ種別ID、メッセージ発信CI）」を対応付けて記憶する。図8に示した学習時の構成情報17bの「パターン」は、障害予兆パターンに該当し、「学習時刻」は、障害予兆パターンを学習したときの時刻である。また、構成情報内の「時刻」は、メッセージが発信された時刻である。「メッセージ種別ID」は、発信されたメッセージの識別子であり、図6に示したメッセージ種別フィールド15dに出力された識別子に該当する。「メッセージ発信CI」は、メッセージを発信した構成要素であり、図3に示した「CI id」に対応する。

10

20

30

40

50

【0044】

図8の場合、障害予兆パターン「0005、0007、0012」を学習した日時が「日本標準時の2012年3月8日10:20:00」である。このときに、構成要素「029KKZHE」がメッセージ「0005」を出力し、構成要素「029KKZHE」と構成要素「2H9JIIHY」とがメッセージ「0007」を出力し、構成要素「0S0IW3SH」がメッセージ「0012」を出力したことを示す。

【0045】

障害予兆記録DB18は、検出された障害予兆を記憶する。ここで記憶される情報は、予兆通報判定部26等によって更新される。図9は、障害予兆記録DBに記憶される情報の例を示す図である。図9に示すように、障害予兆記録DB18は、「時刻、障害種別、検出パターン、検出構成、共起確率、構成変更量」を記憶する。

10

【0046】

「時刻」は、障害の予兆が検出された時刻である。「障害種別」は、予兆があるとして検出された障害を識別する識別子であり、図8の「障害」に対応する。「検出パターン」は、検出された障害予兆パターンであり、図8の「メッセージパターン」に対応する。「検出構成」は、障害予兆が検出されたときのシステム構成であり、構成要素「Ci id」の組み合わせである。「共起確率」は、検出された障害予兆パターンが「障害種別」の障害を共起させる確率であり、図8の「共起確率」に対応する。「構成変更量」は、検出された障害予兆パターンの学習時の構成情報と、当該障害予兆パターンの検出時の構成情報との異なり具合を示す情報であり、後述する構成差分算出部25によって算出される。

【0047】

20

図9の場合、「日本標準時の2012年4月12日の16:16:00」に、障害「T001」の共起確率が「0.93」である障害予兆パターン「0005、0007、0012」が検出されたことを示す。さらに、この障害予兆パターン「0005、0007、0012」を検出したときのシステム構成が「0S0IW3SH、029KKZHE、000GEANA」であり、この検出時の構成情報と当該障害予兆パターンの学習時の構成情報との構成変更量が「10、2」であることを示す。

【0048】

図2に戻り、制御部20は、構成変更学習部21、メッセージ収集部22、障害予兆学習部23、障害予兆検出部24、構成差分算出部25、予兆通報判定部26、閾値学習部27を有し、これらによって障害予兆の検出を実行する処理部である。

【0049】

30

構成変更学習部21は、情報処理システムのシステム構成の変更を検出して構成変更情報DB14を更新し、構成情報の変更を学習する処理部である。具体的には、構成変更学習部21は、構成情報DB13を監視し、構成情報DB13が更新されたことを検出すると、更新された内容を構成変更情報DB14に格納する。

【0050】

例えば、「2012年5月12日11:00:00」にテナント1の「H38FHZ0S」のOSが「OS(A)」から「OS(C)」に変更されたとする。この場合、構成変更学習部21は、「時刻(2012-05-12T11:00:00-09:00)、変更種別(MOD)、対象(H38FHZ0S)、パラメータ(TARGET=OS、VALUE=OS(C))」を構成変更情報DB14に格納する。

【0051】

40

メッセージ収集部22は、データセンタ2内の情報処理システムから出力されたログメッセージを各情報処理システムから収集して、収集したメッセージを管理メッセージDB15に格納する処理部である。

【0052】

障害予兆学習部23は、障害の予兆を示すログメッセージのパターンである障害予兆パターンを、過去に発生した障害事象に基づいて生成し、所定の間隔で学習する処理部である。具体的には、障害予兆学習部23は、障害予兆パターンの生成、障害予兆パターンの抽出、障害予兆パターンの共起確率の学習などを定期的に実行して、障害予兆パターンDB17を更新する処理部である。

【0053】

50

例えば、障害予兆学習部 2 3 は、過去一定期間のログメッセージを管理メッセージ DB 1 5 から抽出し、抽出したログメッセージ群からメッセージパターンを生成する。また、障害予兆学習部 2 3 は、生成した各メッセージパターンを構成するメッセージを出力した構成要素を特定する。そして、障害予兆学習部 2 3 は、生成したメッセージパターンの組み合わせが障害予兆パターン DB 1 7 に記憶されている場合に、「発生総数」をインクリメントし、記憶されていない場合には、新たにエントリを生成する。

【0054】

その後、障害予兆学習部 2 3 は、メッセージの発生時刻から所定時間内に障害が発生している場合には、当該障害を特定する識別子とメッセージパターンと組み合わせに該当する「障害前発生数」をインクリメントした後、共起確率を更新する。一方、障害予兆学習部 2 3 は、障害が発生していない場合には、当該障害を特定する識別子とメッセージパターンと組み合わせに該当する「障害前発生数」をインクリメントすることなく、共起確率を更新する。

10

【0055】

ここで、図 10 を用いて具体的に説明する。図 10 は、障害予兆パターンの学習を説明する図である。図 10 に示すように、障害予兆学習部 2 3 は、任意に設定された学習タイミングに到達すると、障害予兆学習期間（P 分間）内の W 分の間に出力されたメッセージを管理メッセージ DB 1 5 から抽出する。なお、P 分は任意に設定してもよく、障害発生時刻（S 分）を基準として、S 分から所定時間前までと設定してもよい。続いて、障害予兆学習部 2 3 は、各メッセージのメッセージ種別フィールド 1 5 d を参照し、W 分の間に、「0005、0007、0012」の組み合わせを抽出したとする。

20

【0056】

すると、障害予兆学習部 2 3 は、障害予兆パターン DB 1 7 を参照し、「障害」に関係なく「0005、0007、0012」に対応する「発生回数」をインクリメントする。図 8 の例では、障害予兆学習部 2 3 は、「0005、0007、0012」に対応する「T001」と「T002」の両方の「発生回数」とをインクリメントする。また、障害予兆学習部 2 3 は、抽出したメッセージパターン「0005、0007、0012」の各メッセージについて、ホスト名フィールド 1 5 b とモジュール名フィールド 1 5 c とから構成情報 DB 1 3 に記憶される「item」と「type」とを特定し、これらに対応する「CI id」を特定する。その後、障害予兆学習部 2 3 は、抽出したメッセージパターン「0005、0007、0012」と、特定した「CI id」とを対応付けて、学習時の構成情報 1 7 b として障害予兆パターン DB 1 7 に格納する。

30

【0057】

その後、障害予兆学習部 2 3 は、障害情報 DB 1 6 を参照し、W 分後から P 分までの間に障害「T001」が発生していれば、「T001」と「0005、0007、0012」との組に対応する「障害前発生数」をインクリメントする。一方、障害予兆学習部 2 3 は、障害情報 DB 1 6 を参照し、W 分後から P 分までの間に障害「T002」が発生していれば、「T002」と「0005、0007、0012」との組に対応する「障害前発生数」をインクリメントする。その後、障害予兆学習部 2 3 は、現時点で格納されている、更新済みの「発生総数」および「障害前発生数」を用いて共起確率を算出して更新する。

40

【0058】

図 2 に戻り、障害予兆検出部 2 4 は、障害予兆パターン DB 1 7 に記憶される障害予兆パターンを用いて、障害の予兆を検出する処理部である。具体的には、障害予兆検出部 2 4 は、管理メッセージ DB 1 5 に随時格納されるログメッセージを監視し、障害予兆パターン DB 1 7 に記憶される障害予兆パターンと同じパターンの発生を検出した場合に、障害の予兆を検出する。そして、障害予兆検出部 2 4 は、検出した障害の予兆や障害予兆パターンを構成差分算出部 2 5 や予兆通報判定部 2 6 に通知する。

【0059】

例えば、障害予兆検出部 2 4 は、管理メッセージ DB 1 5 に「0005、0007、0012」のパターンが検出された場合に、障害「T001」と「T002」の障害の予兆を検出し、構成差分算出部 2 5 や予兆通報判定部 2 6 に通知する。このとき、障害予兆検出部 2 4 は、障害予兆

50

パターンと一致したメッセージを出力した構成要素を、障害予兆学習部 2 3 と同様の手法で特定して、構成差分算出部 2 5 や予兆通報判定部 2 6 に通知する。

【0060】

構成差分算出部 2 5 は、障害予兆パターン学習時のシステム構成と障害の予兆検出時のシステム構成との間で構成が異なることを特徴づける複数の指標を用いて、システム構成間の差を示す差分距離を算出する処理部である。

【0061】

例えば、構成差分算出部 2 5 は、障害予兆パターン学習時の構成情報から障害の予兆検出時の構成情報へ構成が遷移する際に、構成要素の変更が実行された累積回数である変更回数を算出する。また、構成差分算出部 2 5 は、障害予兆パターン学習時の構成要素と障害の予兆検出時の構成要素とで相違する構成要素の数である差分数を算出する。そして、構成差分算出部 2 5 は、変更回数と差分数とを用いて、学習時と検出時との構成情報の差分距離を算出する。なお、構成差分算出部 2 5 は、適用されている障害予兆パターンの学習時間を保持しておき、当該学習時間に対応する学習時の構成情報を障害予兆パターン DB 1 7 から特定する。このようにすることで、構成差分算出部 2 5 は、最新の障害予兆パターンが未適用であっても、学習時と検出時との構成情報の差分距離を正確に算出することができる。

【0062】

具体的には、構成差分算出部 2 5 は、障害の予兆が検出されたことが障害予兆検出部 2 4 から通知されると、障害予兆パターン DB 1 7 から検出された予兆に対応するエントリを抽出し、予兆が検出された障害に対応するエントリを障害予兆記録 DB 1 8 に生成する。このとき、構成差分算出部 2 5 は、予兆検出時の構成情報を障害予兆検出部 2 4 から受信して、障害予兆記録 DB 1 8 に生成したエントリの「検出構成」に格納する。そして、構成差分算出部 2 5 は、検出された障害予兆パターンの学習時の構成情報を障害予兆パターン DB 1 7 から取得し、学習時の構成情報と検出時の構成情報とからシステム構成間の構成変更量を算出する。その後、構成差分算出部 2 5 は、障害予兆記録 DB 1 8 に生成したエントリの「構成変更量」に、算出した構成変更量を格納する。

【0063】

ここで、構成情報の遷移について説明する。図 1 1 は、構成情報の遷移を説明する図である。図 1 1 に示すように、システム A 1 に着目にした場合、A 1 の構成は時間によって一部ずつ更新されていく。これを時間的連続性と呼ぶ。また、クラウドシステムは、同じテンプレートから複数のシステムを生成されるので、同じ時間帯で、完全に均一ではなく部分的に異なる他のシステムが存在する。これを空間的連続性と呼ぶ。

【0064】

この時間的連続性に着目して算出した変更量が上記「変更回数」であり、空間的連続性に着目して算出した変更量が上記「差分数」である。つまり、「変更回数」は、変更の回数のみで算出され、変更の内容や変更の結果、システム構成がどのようにかわったかは見ていない値であり、システム構成に依存しない特徴量である。また、「差分数」は、システム構成同士の差分のみで算出され、システム構成が過去に何度の変更を経て現在の構成になったか見ておらず、システム変更履歴に依存しない特徴量である。このように、構成差分算出部 2 5 は、互いに関連性のない、独立した特徴量を用いて、学習時と検出時の構成情報の構成変更量を算出する。

【0065】

予兆通報判定部 2 6 は、検出された予兆が妥当であるか否かを判定する処理部である。具体的には、予兆通報判定部 2 6 は、構成差分算出部 2 5 により算出された構成変更量が閾値未満の場合には、適用される障害予兆パターンが有効であると判定し、当該障害予兆パターンを用いて検出された障害の予兆を管理者等に通報する。

【0066】

例えば、図 9 を例にすると、予兆通報判定部 2 6 は、図 9 の 1 行目の障害予兆パターン「0005、0007、0012」と一致するとして検出された障害の予兆について、構成変更量「10

10

20

30

40

50

、2」を障害予兆記録DB18から取得する。そして、予兆通報判定部26は、構成変更量「10、2」によって特定される差分距離が閾値未満であれば、障害「T001」が発生する可能性があることを管理者等に通報する。このとき、予兆通報判定部26は、構成変更量「10、2」によって特定される差分距離が閾値未満であっても、共起確率が所定値未満であれば、通報しないように制御することもできる。

【0067】

ここで、障害予兆の有効範囲を説明する。図12は、障害予兆パターンの有効範囲を説明する図である。図12に示すように、障害予兆パターンを学習したときから、図11と同様、システムの構成は、時間軸および空間軸で変更されていく。具体的には、システムAは、時間とともにソフトウェアのバージョンアップなどのマイナーチェンジが実行されるので、A1、A2、A3、A4と構成変更が実行される。この場合に、システムAがA1に構成変更されたタイミングで障害検出パターンが学習されて、構成変更が短時間で発生したとすると、この障害検出パターンを用いてA1、A2、A3、A4の各々で障害予兆の検出が実行される。

10

【0068】

一方で、クラウドシステムの特性上、システムAと似た構成のシステムB1、C1、D1が同時期に存在する。この場合も、システムAがA1に構成変更されたタイミングで学習された障害検出パターンを用いて、同時期に存在するB1、C1、D1の各々で障害予兆の検出が実行される。

【0069】

20

このように、あるタイミングで学習された障害予兆パターンが、時間的または空間的に異なるシステム、すなわち、構成が異なるシステムで利用される。一方、障害予兆パターンは、共起確率に基づいて生成されるので、システム構成の変化が当該パターンに与える影響度が明確ではない。そこで、予兆通報判定部26は、構成差分算出部25により算出された構成変更量を用いて、適用される障害予兆パターンの有効性を判定する。つまり、予兆通報判定部26は、学習された障害予兆パターンがどの時間、どの空間まで有効であるかを定量的に判定する。そして、予兆通報判定部26は、有効ではないと判定された場合には、共起確率が高くても、誤検出の可能性が高いとして、検出された障害の予兆を通報しないように制御する。

【0070】

30

閾値学習部27は、障害の予兆が検出された後に、実際に障害が発生したか否かを判定し、判定した結果に基づいて、障害予兆パターンの適用可否を判定する差分距離の閾値を決定する。つまり、閾値学習部27は、障害予兆パターンを用いて検出された複数の障害予兆各々が正解なのか誤検出なのかを統計的に判断し、予兆通報判定部26が障害予兆パターンの有効性の判定に用いる閾値を更新する。

【0071】

[有効性判定の具体例]

次に、図13から図16を用いて、適用される障害予兆パターンの有効性を判定する具体例を説明する。図13は、障害予兆検出時の構成情報例を示す図である。図14は、構成の変更回数を説明する図である。図15は、構成の差分数を説明する図である。図16は、判定基準を説明する図である。なお、ここでは、障害検出パターンとして「0005、0007、0012」が検出され、学習時の構成が図8に示す「0S0IW3SH、2H9JIIHY、029KKZHE」であるものとする。

40

【0072】

まず、障害予兆検出部24は、管理メッセージDB15に格納されるログメッセージから障害検出パターン「0005、0007、0012」と一致するメッセージが発生したことを検出する。すると、障害予兆検出部24は、障害検出パターン「0005、0007、0012」を出力した構成要素を抽出する。具体的には、障害予兆検出部24は、障害検出パターン「0005、0007、0012」を検出した時刻、メッセージ種別ID、メッセージ発信CIを、検出したメッセージから抽出し、図13に示す構成情報を生成する。なお、障害予兆検出部24は、図

50

6に示したメッセージ種別フィールド15dから「メッセージ種別ID」を抽出する。また、障害予兆検出部24は、図6に示したホスト名フィールド15bとモジュール名フィールド15cとから、図3に示した「item」と「type」とを特定し、これらに対応する「CI id」を「メッセージ発信CI」として抽出する。

【0073】

また、障害予兆検出部24は、検出された障害の予兆に関する情報が格納されるエントリを障害予兆記録DB18に生成する。具体的には、障害予兆検出部24は、障害予兆パターンDB17から、障害検出パターン「0005、0007、0012」、「障害」、「共起確率」を抽出し、それぞれを「検出パターン、障害種別、共起確率」とするレコードを障害予兆記録DB18に生成する。また、障害予兆検出部24は、生成したエントリの「時刻」に

10

【0074】

その後、構成差分算出部25は、障害予兆記録DB18に格納されたエントリから検出パターン「0005、0007、0012」を特定し、特定した検出パターンに対応する構成情報「OS0IW3SH、029KKZHE、220GEANA」および「学習時刻」を障害予兆パターンDB17から抽出する。すなわち、構成差分算出部25は、検出されたメッセージパターン「0005、0007、0012」の学習時の構成情報を抽出する。

【0075】

続いて、構成差分算出部25は、構成変更情報DB14を参照し、「学習時刻」より後の時間で構成変更が実行された回数を計数する。つまり、構成差分算出部25は、学習時から検出時までの構成変更の回数を計数する。

20

【0076】

具体的には、構成差分算出部25は、構成変更情報DB14を参照することで、図14に示すように「OS0IW3SH」が学習時から検出時まで4回設定変更されたことを検出する。同様に、構成差分算出部25は、学習時の「2H9JIIHY」が1回設定変更された後に削除されたことを検出し、学習時の「029KKZHE」が検出時まで2回設定変更されたことを検出する。同様に、構成差分算出部25は、学習時にはなかった「220GEANA」が学習時以降に追加された後に1回設定変更されたことを検出する。以上から、構成差分算出部25は、学習時から検出時まで10回の構成変更があったことを検出する。すなわち、構成差分算出部25は、変更が実行された累積回数である変更回数として10を算出する。

30

【0077】

さらに、構成差分算出部25は、構成変更情報DB14を参照し、学習時の構成要素の種類と、検出時の構成要素の種類の相違数を計数する。つまり、構成差分算出部25は、学習時と検出時とで構成要素が相違する数を計数する。

【0078】

具体的には、構成差分算出部25は、学習時の構成情報「OS0IW3SH、2H9JIIHY、029KKZHE」の各構成要素について、構成情報DB13を参照して、「CI id」を「type」に変換する。つまり、構成差分算出部25は、「OS0IW3SH」を「PC1」、「2H9JIIHY」を「OS(A)」、「029KKZHE」を「AP2」に変換する。同様に、構成差分算出部25は、検出時の構成情報「OS0IW3SH、029KKZHE、220GEANA」の各構成要素について、「OS0IW3SH」を「PC1」、「029KKZHE」を「AP2」、「220GEANA」を「OS(B)」に変換する。そして、構成差分算出部25は、学習時の構成情報「PC1、OS(A)、AP2」と検出時の構成情報「PC1、AP2、OS(B)」とを比較し、一致する構成要素の数が「2個」とであると特定する。すなわち、構成差分算出部25は、相違する構成要素の差分数として2を算出する。

40

【0079】

その後、構成差分算出部25は、障害予兆記録DB18に生成したレコードの「構成変更量」に、時間軸の構成差分である変更回数「10」と空間軸の構成差分である差分数「2」とを格納する。続いて、予兆通報判定部26は、構成変更量「10、2」に基づいて、検出された予兆の精度すなわち障害予兆パターンの有効性を判定する。具体的には、予

50

兆通報判定部26は、図16に示すように、横軸を変更回数、縦軸を差分数として、構成変更量「10、2」をプロットする。このとき、プロットされた構成変更量「10、2」で特定される点と、原点(0、0)とを結ぶ直線の長さが、差分距離として表される。そして、予兆通報判定部26は、この差分距離が閾値の範囲内である場合に、検出された障害予兆パターンは有効であると判定し、予兆を通報する。一方で、予兆通報判定部26は、この差分距離が閾値の範囲外である場合に、検出された障害予兆パターンは有効ではないと判定し、予兆を通報しないように制御する。

【0080】

[閾値学習の具体例]

次に、予兆通報判定部26が予兆の有効性を判定する際に用いる閾値の学習例を説明する。図17は、閾値の学習を説明する図である。図17に示すように、閾値学習部27は、横軸を変更回数、縦軸を差分数として、障害予兆記録DB18に記憶される各レコードの「構成変更量」をプロットする。そして、閾値学習部27は、予兆を有効と判定したか無効と判定したかによって、プロットした各構成変更量を「正解群」と「誤検出群」とにグループ分けする。その後、閾値学習部27は、プロットした状態から「正解群」が多く含まれるように境界を決定し、決定した境界を新たな閾値とする。なお、境界の決定手法は、マハラノビス距離などの統計学の様々な手法を用いることができる。

【0081】

[処理の流れ]

続いて、障害検出装置10が実行する処理の流れについて説明する。ここでは、障害予兆学習処理、障害予兆検出処理、予報通報判定処理、構成差分算出処理、閾値学習処理について説明する。

【0082】

(障害予兆学習処理)

図18は、障害予兆学習処理の流れを示すフローチャートである。この処理は定期的に行われる。図18に示すように、障害予兆学習部23は、学習タイミングに到達すると、管理メッセージDB15から過去一定期間(W分)のメッセージを抽出し、様々なパターンを生成する(S101)。

【0083】

続いて、障害予兆学習部23は、生成した各パターンについて、構成情報DB13や管理メッセージDB15を参照し、各パターンを構成するメッセージの発信元のCI(構成要素)を抽出する(S102)。

【0084】

そして、障害予兆学習部23は、生成した各パターンのうち、障害予兆パターンDB17の障害予兆パターン17aに記憶される障害予兆パターンと一致するパターンについては、該当する障害予兆パターンの「発生総数」を更新する(S103)。具体的には、障害予兆学習部23は、当該パターンに対応するエントリの「発生総数」をインクリメントする。このとき、障害予兆学習部23は、障害予兆パターンDB17に記憶される障害予兆パターン17aと一致しないパターンについては、新たなエントリを障害予兆パターンDB17に生成する。

【0085】

その後、障害予兆学習部23は、管理メッセージDB15から抽出したメッセージ群の時刻から一定期間(P分)以内の障害を、障害情報DB16から取り出す(S104)。そして、障害予兆学習部23は、障害予兆パターンDB17の障害予兆パターン17aに記憶される各エントリの「障害」と一致する障害が発生している場合には、当該エントリの「障害」に対応する「障害前発生数」を更新する(S105)。

【0086】

さらに、障害予兆学習部23は、障害予兆パターンDB17の障害予兆パターン17aに記憶される各エントリに対応付けられる学習時の構成情報17bを、S102で抽出した構成要素を組み合わせた構成情報で更新する(S106)。その後、障害予兆学習部2

10

20

30

40

50

3は、障害予兆パターンDB17の障害予兆パターン17aの各エントリについて、共起確率を再計算して更新する(S107)。その後は、S101に戻って以降の処理が繰り返される。

【0087】

(障害予兆検出処理)

図19は、障害予兆検出処理の流れを示すフローチャートである。この処理は定期的に行われる。図19に示すように、障害予兆検出部24は、管理メッセージDB15から最新一定時間(W分)のメッセージを抽出して、様々なパターンを生成する(S201)。

【0088】

10

続いて、障害予兆検出部24は、生成した各パターンについて、構成情報DB13や管理メッセージDB15を参照し、各パターンを構成するメッセージの発信元のCI(構成要素)を抽出する(S202)。

【0089】

その後、障害予兆検出部24は、生成した各パターンのうち、障害予兆パターンDB17の障害予兆パターン17aに記憶される障害予兆パターンと一致するパターンを検索する(S203)。

【0090】

そして、障害予兆検出部24は、一致するパターンが検索された場合(S204:Yes)、一致したパターンと当該パターンの構成要素等を用いて、障害予兆記録DB18にエントリを生成する(S205)。その後、障害予兆検出部24は、予兆通報判定部26に予兆通報判定処理の実行を依頼した後(S206)、S201以降を繰り返す。なお、障害予兆検出部24は、一致するパターンが検索されなかった場合も(S204:No)、S201以降を繰り返す。

20

【0091】

(予兆通報判定処理)

図20は、予兆通報判定処理の流れを示すフローチャートである。図20に示すように、予兆通報判定部26は、障害予兆検出部24から処理の実行開始が依頼されると(S301:Yes)、障害予兆検出部24によって障害予兆記録DB18に格納されたエントリ、すなわち、障害予兆通報の内容を取得する(S302)。

30

【0092】

その後、予兆通報判定部26は、構成差分算出部25に構成差分算出処理の開始を依頼する(S303)。このとき、予兆通報判定部26は、S302で取得した障害予兆通報の内容を構成差分算出部25に出力してもよい。

【0093】

そして、予兆通報判定部26は、構成差分算出部25から構成差分算出処理の算出結果を取得し(S304)、取得した算出結果である構成変更量と閾値とを比較する(S305)。

【0094】

予兆通報判定部26は、構成変更量が閾値以下であると判定した場合(S306:Yes)、予兆を通報する(S307)。一方、予兆通報判定部26は、構成変更量が閾値より大きいと判定した場合(S306:No)、処理を終了する。

40

【0095】

(構成差分算出処理)

図21は、構成差分算出処理の流れを示すフローチャートである。図21に示すように、構成差分算出部25は、予兆通報判定部26から処理の実行開始が依頼されると(S401:Yes)、障害予兆検出部24によって障害予兆記録DB18に格納されたエントリ、すなわち、障害予兆通報の内容を取得する(S402)。

【0096】

そして、構成差分算出部25は、S402で取得した障害予兆通報の内容から予兆検出

50

時の構成情報を取得する（S403）。具体的には、構成差分算出部25は、障害予兆パターンの各メッセージの出力元の構成要素を抽出する。

【0097】

続いて、構成差分算出部25は、障害予兆に該当するパターンの学習時の構成情報を取得する（S404）。具体的には、構成差分算出部25は、検出されたパターンに対応するエントリを障害予兆パターンDB17から検索し、検索された障害予兆パターンに対応付けられる学習時の構成情報を特定する。さらに、構成差分算出部25は、特定した構成情報を構成する構成要素「メッセージ発信CI」を取得する。

【0098】

その後、構成差分算出部25は、構成変更量を算出し（S405）、その算出結果を予兆通報判定部26に応答する（S406）。具体的には、構成差分算出部25は、学習時から検出時までの構成要素の変更が実行された累積回数である変更回数と、学習時と検出時とで構成要素が相違する数を示す差分数とを算出する。また、構成差分算出部25は、算出した構成変更量（変更回数、差分数）を、障害予兆記録DB18の該当するエントリに格納してもよい。

【0099】

（閾値学習処理）

図22は、閾値学習処理の流れを示すフローチャートである。この処理は定期的に行われる。図22に示すように、閾値学習部27は、閾値の学習タイミングに到達すると、障害予兆記録DB18から、1種類の障害について予兆通報を抽出する（S501）。具体的には、閾値学習部27は、障害予兆記録DB18から、「障害種別」が一致するエントリを取得する。

【0100】

続いて、閾値学習部27は、抽出した予兆通報について、予兆が正解であったか誤検出であったかを判定する（S502）。具体的には、閾値学習部27は、抽出した予兆通報が検出された時刻から所定時間が経過するまでに、当該予兆通報に対応する「障害」が発生したか否かを判定する。

【0101】

その後、閾値学習部27は、各予兆通報の判定した結果から正解群と誤検出群の構成変更量について、マハラノビス距離を算出する（S503）。そして、閾値学習部27は、マハラノビス距離の算出結果から閾値となる判別式を求め（S504）、閾値を更新する（S505）。その後は、S501に戻って以降の処理が繰り返される。

【0102】

このように、実施例1に係る障害検出装置10は、互いに独立する指標を用いて、学習時の構成と検出時の構成との異なり具合を定量化し、使用される障害検出パターンの有効性を判定することができる。したがって、障害検出装置10は、システム構成がどの程度変わると学習した障害予兆パターンが使用できなくなるのかを定量的に評価することができる。

【0103】

また、障害検出装置10は、実際に障害の予兆が検出された場合に、当該予兆に対応する障害予兆パターンの有効性を判定することができるので、検出された予兆の信頼性を判定することができる。つまり、障害検出装置10は、信頼性の低い予兆、すなわち、構成変更量が閾値より大きい障害予兆パターンで検出された予兆については、管理者等への通報を抑制できる。したがって、障害検出装置10は、適用が妥当ではない障害予兆パターンによって検出される、予兆の誤検出を抑制することができる。

【0104】

また、障害検出装置10は、予兆の検出と障害の実績とから、障害予兆パターンの有効性を判定する基準を更新することができるので、実績を考慮した基準で有効性を判定することができ、判定精度を向上させることができる。

【実施例2】

【0105】

実施例1では、構成変更量（変更回数、差分数）を用いて、学習時と検出時との構成情報の差分距離を算出する例を説明したが、差分距離の算出には他の指標を用いることもできる。そこで、実施例2では、構成変更量の1つとして負荷量を用いる例と、負荷パターンを用いる例とを説明する。

【0106】

（負荷量）

図23は、負荷量を説明する図である。図23は、該当システムの負荷量が時間によって変化する例を図示し、縦軸が負荷、横軸が時間である。図23に示す負荷量は、単位時間当たりの処理数、利用者の同時接続数など、システムに対する外部からの負荷量である。なお、単位時間当たりの処理数としては、例えば1日あたりのページ閲覧数などが該当し、利用者の同時接続数としては、ある時刻に接続しているユーザ数などが該当する。

10

【0107】

図23に示すように、時間が経過するに連れてシステムの構成が変更されると、システムの負荷量も変化する。つまり、学習時「 t_0 」時の負荷量「 $F(t_0)$ 」と、検出時「 t_1 」の負荷量「 $F(t_1)$ 」とが異なっていれば、システムの変更が行われている可能性が高い。そこで、この例では、 $F(t_0)$ と $F(t_1)$ との比を算出し、算出した負荷量の比を構成変更量として用いる。具体的には、構成差分算出部25は、負荷量の比「 D 」を「 $D = |F(t_1) - F(t_0)| / F(t_0)$ 」と算出する。

20

【0108】

このように、障害検出装置10は、実施例1で説明した構成変更量の1つ、または、3つ目の構成変更量として、負荷量の比を用いることもできる。この結果、システムの内部構成に直接的には依存しない、システムの外部からの影響を客観的に用いることができるので、判定精度の向上が期待できる。

【0109】

（負荷パターン）

図24は、負荷パターンを説明する図である。図24は、該当システムがユーザに対してサービス等を提供することで発生する負荷の変化を図示し、縦軸が負荷、横軸が時間である。つまり、負荷パターンは、該当システムを所有するテナントの業務パターンである。

30

【0110】

ここでは、負荷のピーク周期 t と、負荷のピーク時の値であるピーク負荷 l_p と、平均負荷 l_a とを用いて負荷パターン L を $L(t, l_p, l_a)$ と定義する。なお、学習時の負荷パターンは、 $L_0(t_0, l_{p0}, l_{a0})$ と定義でき、検出時の負荷パターンは、 $L_1(t_1, l_{p1}, l_{a1})$ と定義できる。

【0111】

そして、学習時のシステムの負荷パターンと、検出時のシステムの負荷パターンとの差分 D は、「 $D = (|t_1 - t_0| / t_0) + (|l_{p1} - l_{p0}| / l_{p0}) + (|l_{a1} - l_{a0}| / l_{a0})$ 」と算出することができる。

【0112】

40

学習時のテナントと検出時のテナントとが同一であれば、利用方法や業務の負荷パターンが類似すると考えられる。したがって、負荷パターンの差分「 D 」は0に近いほど、学習した障害予兆パターンの有効性は高い。一方、学習時のテナントと検出時のテナントとが異なれば、利用方法や業務の負荷パターンが異なると考えられる。したがって、負荷パターンの差分「 D 」は、例えば30のように大きな値ほど、学習した障害予兆パターンの有効性は低い。

【0113】

このように、障害検出装置10は、実施例1で説明した構成変更量の1つ、または、3つ目の構成変更量として、負荷パターンの差分を用いることもできる。この結果、システムの内部構成に直接的には依存しない、システムの負荷状態の変化を客観的に用いること

50

ができるので、判定精度の向上が期待できる。

【実施例 3】

【0114】

さて、これまで本発明の実施例について説明したが、本発明は上述した実施例以外にも、種々の異なる形態にて実施されてよいものである。そこで、以下に異なる実施例を説明する。

【0115】

(適用システム)

実施例 1 や実施例 2 で説明した障害予兆パターンの適用判定方法は、学習時と検出時と同じシステムであってもよく、異なるシステムであっても同様に処理することができる。上述したように、クラウドシステムは、同じテンプレートを用いて複数のシステムから構成されることが多い。このため、システム A で障害予兆パターンを学習し、システム B に当該障害予兆パターンを適用することもある。つまり、障害予兆パターン学習時は、システム A とシステム B とは同様の構成であり、時間経過とともに、各々でシステム構成の変更が行われる。

10

【0116】

したがって、障害検出装置 10 は、システム A で学習された障害予兆パターンをシステム B に適用し、システム B における構成変更を管理する。そして、障害検出装置 10 は、システム B で障害の予兆が検出された場合に、学習時のシステム A と現在のシステム B との差分数と、学習時のシステム A から現在のシステム B に変更されるまでの変更回数とを算出する。こうして、障害検出装置 10 は、当該障害予兆パターンの適用が有効か否かをでき、各実施例と同様の効果を得ることができる。

20

【0117】

(指標の組み合わせ)

実施例 1 では、変更回数と差分数とを用いて差分距離を算出する例を説明し、実施例 2 では、負荷量比または負荷パターンの比を用いる例を説明したが、これらは任意に組み合わせることができる。例えば、変更回数と負荷パターンの比とを用いる場合には、横軸を変更回数、縦軸を負荷パターンの比として、構成変更量をプロットし、差分距離が閾以下か否かを判定することもできる。また、変更回数、差分数、負荷量比、負荷パターンを用いた四次元で差分距離が閾以下か否かを判定することもできる。なお、負荷量比や負荷パターンを用いる場合には、これらを用いることを予め決定しておき、学習時から負荷量比や負荷パターンを計測する。

30

【0118】

(共起確率)

実施例 1 等で示した障害予兆パターン DB 17 は、共起確率が所定値以上のパターンを記憶するようにすることもできる。このような状態で、障害検出装置 10 は、障害予兆を検出した場合に、障害予兆パターンの有効性を判定する。この結果、障害検出装置 10 は、共起確率が高い障害予兆パターンで障害の予兆が検出され、障害予兆パターンが有効ではない場合には、信頼性の低い予兆が検出されたとして、予兆の通報を抑制することができる。

40

【0119】

障害予兆パターン DB 17 は、共起確率が低いパターンを記憶してもよい。このような状態で、障害検出装置 10 は、障害予兆を検出した場合に、障害予兆パターンの有効性を判定する。この結果、障害検出装置 10 は、学習時と検出時のシステム構成の違いによっては、共起確率が低く信頼性の低い障害予兆パターンで障害の予兆が検出されるが、障害予兆パターンを有効であると判定する場合もある。この場合、障害検出装置 10 は、信頼性の高い予兆が検出されたとして、予兆の通報を実行することができる。

【0120】

(システム)

また、本実施例において説明した各処理のうち、自動的におこなわれるものとして説明

50

した処理の全部または一部を手動的におこなうこともできる。あるいは、手動的におこなわれるものとして説明した処理の全部または一部を公知の方法で自動的におこなうこともできる。この他、上記文書中や図面中で示した処理手順、制御手順、具体的名称、各種のデータやパラメータを含む情報については、特記する場合を除いて任意に変更することができる。

【0121】

また、図示した各装置の各構成要素は機能概念的なものであり、必ずしも物理的に図示の如く構成されていることを要しない。すなわち、各装置の分散や統合の具体的形態は図示のものに限られない。つまり、その全部または一部を、各種の負荷や使用状況などに応じて、任意の単位で機能的または物理的に分散・統合して構成することができる。さらに、各装置にて行なわれる各処理機能は、その全部または任意の一部が、CPUおよび当該CPUにて解析実行されるプログラムにて実現され、あるいは、ワイヤードロジックによるハードウェアとして実現され得る。

【0122】

(ハードウェア)

図25は、ハードウェア構成例を示す図である。ここで示したハードウェア構成は、障害検出装置10のハードウェア構成である。図25に示すように、コンピュータ100は、CPU101、メモリ102、HDD(Hard Disk Drive)103、通信インタフェース104、入力装置105、表示装置106を有する。また、図25に示した各部は、バス100aで相互に接続される。

【0123】

入力装置105は、例えばキーボードなどであり、表示装置106は、例えばディスプレイなどであり、通信インタフェース104は、例えばNIC(Network Interface Card)などである。HDD103は、図2等に示した機能を実行するプログラムや図2に示した各DBを記憶する。記録媒体の例としてHDD103を例に挙げたが、ROM(Read Only Memory)、RAM、CD-ROM等の他のコンピュータが読み取り可能な記録媒体に各種プログラムを格納しておき、コンピュータに読み取らせることとしてもよい。なお、記録媒体を遠隔地に配置し、コンピュータが、その記憶媒体にアクセスすることでプログラムを取得して利用してもよい。また、その際、取得したプログラムをそのコンピュータ自身の記録媒体に格納して用いてもよい。

【0124】

CPU101は、図2に示した各処理部と同様の処理を実行するプログラムをHDD103等から読み出してメモリ102に展開することで、図2等で説明した各機能を実行するプロセスを動作させる。すなわち、このプロセスは、障害検出装置10が有する各処理と同様の機能を実行する。具体的には、CPU101は、構成変更学習部21、メッセージ収集部22、障害予兆学習部23、障害予兆検出部24、構成差分算出部25、予兆通報判定部26、閾値学習部27と同様の機能を有するプログラムをHDD103等から読み出す。そして、CPU101は、各処理部と同様の処理を実行するプロセスを実行する。このようにコンピュータ100は、プログラムを読み出して実行することで適用判定方法を実行する情報処理装置として動作する。

【0125】

また、コンピュータ100は、媒体読取装置によって記録媒体から上記プログラムを読み出し、読み出された上記プログラムを実行することで上記した実施例と同様の機能を実現することもできる。なお、この他の実施例でいうプログラムは、コンピュータ100によって実行されることに限定されるものではない。例えば、他のコンピュータまたはサーバがプログラムを実行する場合や、これらが協働してプログラムを実行するような場合にも、本発明を同様に適用することができる。

【0126】

以上の各実施例を含む実施形態に関し、さらに以下の付記を開示する。

【0127】

(付記 1) コンピュータに、

第 1 のシステム構成において障害の予兆検出に用いられる障害予兆パターンを、前記第 1 のシステム構成において過去に発生した障害事象に基づいて生成し、

前記第 1 のシステム構成から第 2 のシステム構成へシステム構成が遷移する際に、システムを構成する構成要素の変更が実行された累積回数である変更回数を用いて、システム構成間の差を示す差分情報を算出し、

算出した前記差分情報に応じて、前記第 2 のシステム構成における障害の予兆検出への前記障害予兆パターンの適用可否を判定する

処理を実行させることを特徴とする適用判定プログラム。

【0128】

10

(付記 2) 前記差分情報を算出する処理は、前記第 1 のシステム構成を構成する構成要素と前記第 2 のシステム構成を構成する構成要素とで相違する構成要素の数である差分数をさらに用いて、前記差分情報を算出することを特徴とする付記 1 に記載の適用判定プログラム。

【0129】

(付記 3) 前記差分情報を算出する処理は、さらに、前記第 1 のシステム構成時におけるシステムの負荷量と前記第 2 のシステム構成時におけるシステムの負荷量との比である負荷量比を用いて、前記差分情報を算出することを特徴とする付記 2 に記載の適用判定プログラム。

【0130】

20

(付記 4) 前記差分情報を算出する処理は、さらに、前記第 1 のシステム構成時におけるシステムの負荷の傾向を示す負荷パターンと前記第 2 のシステム構成時におけるシステムの負荷傾向を示す負荷パターンとの差である負荷パターン差を用いて、前記差分情報を算出することを特徴とする付記 2 または 3 に記載の適用判定プログラム。

【0131】

(付記 5) 前記差分情報を算出する処理は、前記変更回数とさらに、前記第 1 のシステム構成を構成する構成要素と前記第 2 のシステム構成を構成する構成要素とで相違する構成要素の数である差分数と、前記第 1 のシステム構成時におけるシステムの負荷量と前記第 2 のシステム構成時におけるシステムの負荷量との比である負荷量比と、前記第 1 のシステム構成時におけるシステムの負荷の傾向を示す負荷パターンと前記第 2 のシステム構成時におけるシステムの負荷の傾向を示す負荷パターンとの差である負荷パターン差とのうち、少なくとも 1 つを用いて、前記差分距離を算出することを特徴とする付記 1 に記載の適用判定プログラム。

30

【0132】

(付記 6) 前記生成した障害予兆パターンを用いて障害の予兆を検出する処理を前記コンピュータにさらに実行させ、

前記差分情報を算出する処理は、前記障害の予兆が検出された際のシステム構成を前記第 2 のシステム構成として抽出し、前記システム構成間の差分情報を算出することを特徴とする付記 1 から 5 のいずれか一つに記載の適用判定プログラム。

【0133】

40

(付記 7) 前記障害予兆パターンを用いて障害の予兆を検出し、

前記障害の予兆が検出された後に、実際に障害が発生したか否か判定し、

判定した結果に基づいて、前記第 2 のシステム構成への前記障害予兆パターンの適用可否を判定する前記差分情報の閾値を決定する処理を前記コンピュータにさらに実行させることを特徴とする付記 1 から 6 のいずれか一つに記載の適用判定プログラム。

【0134】

(付記 8) 第 1 のシステム構成において障害の予兆検出に用いられる障害予兆パターンを、前記第 1 のシステム構成において過去に発生した障害事象に基づいて生成する生成部と、

前記第 1 のシステム構成から第 2 のシステム構成へシステム構成が遷移する際に、シス

50

テムを構成する構成要素の変更が実行された累積回数である変更回数を用いて、システム構成間の差を示す差分情報を算出する算出部と、

前記算出部によって算出された前記差分情報に応じて、前記第2のシステム構成における障害の予兆検出への前記障害予兆パターンの適用可否を判定する判定部と

を有することを特徴とする障害検出装置。

【0135】

(付記9) コンピュータが、

第1のシステム構成において障害の予兆検出に用いられる障害予兆パターンを、前記第1のシステム構成において過去に発生した障害事象に基づいて生成し、

前記第1のシステム構成から第2のシステム構成へシステム構成が遷移する際に、システムを構成する構成要素の変更が実行された累積回数である変更回数を用いて、システム構成間の差を示す差分情報を算出し、

算出した前記差分情報に応じて、前記第2のシステム構成における障害の予兆検出への前記障害予兆パターンの適用可否を判定する

処理を含んだことを特徴とする適用判定方法。

【0136】

(付記10) メモリと、

前記メモリに接続されるプロセッサと、を有し、

前記プロセッサは、

第1のシステム構成において障害の予兆検出に用いられる障害予兆パターンを、前記第1のシステム構成において過去に発生した障害事象に基づいて生成し、

前記第1のシステム構成から第2のシステム構成へシステム構成が遷移する際に、システムを構成する構成要素の変更が実行された累積回数である変更回数を用いて、システム構成間の差を示す差分情報を算出し、

算出した前記差分情報に応じて、前記第2のシステム構成における障害の予兆検出への前記障害予兆パターンの適用可否を判定する

処理を実行することを特徴とする障害検出装置。

【0137】

(付記11) 第1のシステム構成において障害の予兆検出に用いられる障害予兆パターンを、前記第1のシステム構成において過去に発生した障害事象に基づいて生成し、

前記第1のシステム構成から第2のシステム構成へシステム構成が遷移する際に、システムを構成する構成要素の変更が実行された累積回数である変更回数を用いて、システム構成間の差を示す差分情報を算出し、

算出した前記差分情報に応じて、前記第2のシステム構成における障害の予兆検出への前記障害予兆パターンの適用可否を判定する処理をコンピュータに実行させる適用判定プログラムを記憶する、コンピュータ読み取り可能な記憶媒体。

【符号の説明】

【0138】

1 クライアント端末

2 データセンタ

5 C M D B

10 障害検出装置

11 通信処理部

12 記憶部

13 構成情報 D B

14 構成変更情報 D B

15 管理メッセージ D B

16 障害情報 D B

17 障害予兆パターン D B

18 障害予兆記録 D B

10

20

30

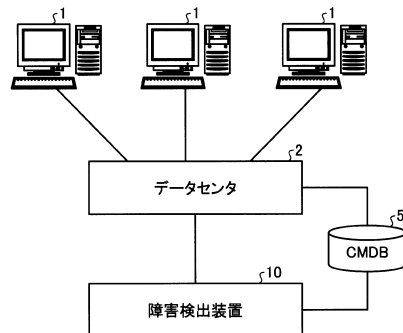
40

50

- 20 制御部
- 21 構成変更学習部
- 22 メッセージ収集部
- 23 障害予兆学習部
- 24 障害予兆検出部
- 25 構成差分算出部
- 26 予兆通報判定部
- 27 閾値学習部

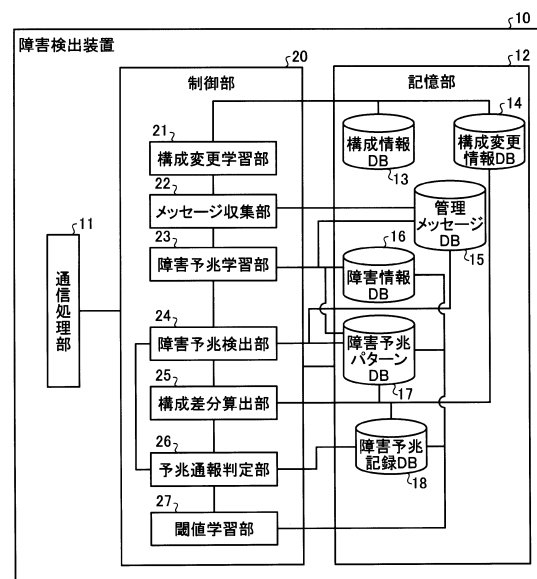
【図1】

実施例1に係るシステムの全体構成例を示す図



【図2】

実施例1に係る障害検出装置の機能構成を示す機能ブロック図



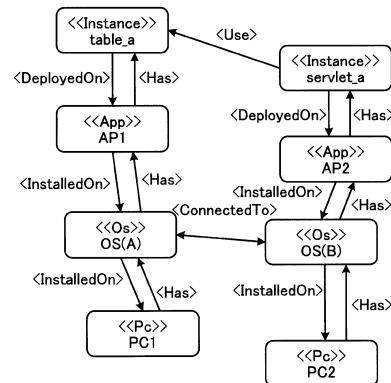
【図 3】

構成情報DBに記憶される情報の例を示す図

```
<cmdb>
<Cls>
  <Cl id="OS0IW3SH" item="Pc" type="PC1"/>
  <Cl id="SS9IHKER" item="Pe" type="PC2"/>
  <Cl id="H38FHZOS" item="Os" type="OS(A)" ip="192.168.1.10"/>
  <Cl id="93H6SK8A" item="Os" type="OS(B)" ip="192.168.1.11"/>
  <Cl id="2H9JIJHY" item="App" type="AP1"/>
  <Cl id="029KZKZE" item="App" type="AP2"/>
  <Cl id="HREIO928" item="Instance" type="table_a"/>
  <Cl id="5198IKSH" item="Instance" type="servlet_a"/>
</Cls>
<Relations>
  <Relation id="02LOILJM" src="OS0IW3SH" dst="H38FHZOS" type="Has"/>
  <Relation id="JREHA98H" src="H38FHZOS" dst="OS0IW3SH" type="InstalledOn"/>
  <Relation id="GK92E0KA" src="SS9IHKER" dst="93H6SK8A" type="Has"/>
  <Relation id="H4K9328UJ" src="93H6SK8A" dst="SS9IHKER" type="InstalledOn"/>
  <Relation id="J919W04I" src="H38FHZOS" dst="93H6SK8A" type="ConnectedTo"/>
  <Relation id="TEJUBGG0" src="H38FHZOS" dst="029KZKZE" type="Has"/>
  <Relation id="49AOZKAW" src="029KZKZE" dst="H38FHZOS" type="InstalledOn"/>
  <Relation id="G09RSIKS" src="93H6SK8A" dst="2H9JIJHY" type="Has"/>
  <Relation id="63870DH9" src="2H9JIJHY" dst="HREIO928" type="InstalledOn"/>
  <Relation id="23KD99HU" src="HREIO928" dst="HREIO928" type="Has"/>
  <Relation id="87EUDHWE" src="HREIO928" dst="029KZKZE" type="DeployedOn"/>
  <Relation id="MJUYEGC3" src="2H9JIJHY" dst="5198IKSH" type="Has"/>
  <Relation id="2YDIB98A" src="5198IKSH" dst="2H9JIJHY" type="DeployedOn"/>
  <Relation id="YIRUETWG" src="5198IKSH" dst="HREIO928" type="Use"/>
</Relations>
</cmdb>
```

【図 4】

構成要素の関係性を説明する図



【図 5】

構成変更情報DBに記憶される情報の例を示す図

時刻	変更種別	対象	パラメータ
2012-03-13T10:31:02-09:00	DEL	2H9JIIHY	
2012-03-13T10:35:28-09:00	ADD	22OGEANA	
2012-03-25T21:00:18-09:00	MOD	93H6SK8A	TARGET=OS_VERSION VALUE=SP3
⋮	⋮	⋮	⋮

【図 6】

管理メッセージDBに記憶される情報の例を示す図

[illegible]

【图 7】

障害情報DBに記憶される情報の例を示す図

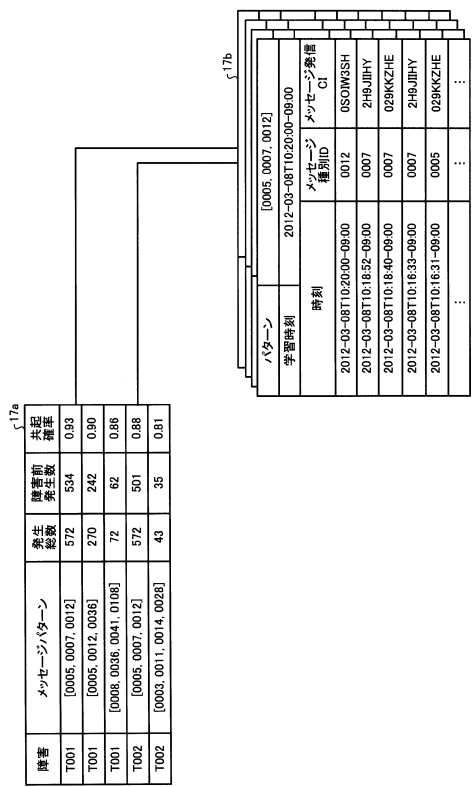
```

<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<Troubles>
  <Trouble uid="201203130001" type="T001" date="2012-03-13T10:51:02-09:00" title="Web Down." />
  <Trouble uid="201203130009" type="T002" date="2012-03-16T20:16:51-09:00" title="HDD Fault" />
  <Trouble uid="201203160001" type="T003" date="2012-03-18T03:25:22-09:00" title="DB Slow Down" />
  <Trouble uid="201203160002" type="T004" date="2012-03-18T03:26:00-09:00" title="Web Slow Down" />
  <Trouble uid="201204120025" type="T001" date="2012-04-12T16:31:08-09:00" title="Web Down." />
  <Trouble uid="201204120026" type="T002" date="2012-04-12T22:51:37-09:00" title="HDD Fault" />
</Troubles>

```

【図 8】

障害予兆パターンDBに記憶される情報の例を示す図



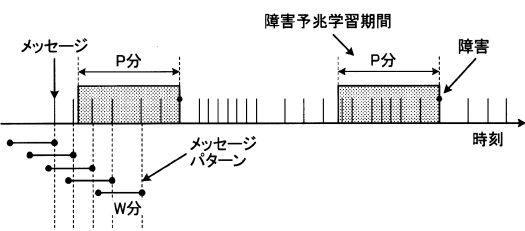
【図 9】

障害予兆記録DBに記憶される情報の例を示す図

時刻	障害種別	検出パターン	検出構成	共起確率	構成変更量 (変更回数、 差分)
2012-04-12T16:16:00-09:00	T001	[0005, 0007, 0012]	OSOW3SH 029KKZHE 2Z0GEANA	0.93	(10, 2)
2012-04-12T16:16:00-09:00	T002	[0005, 0007, 0012]	::	0.88	::
2012-04-12T16:38:40-09:00	T001	[0008, 0036, 0041, 0108]	::	0.86	::
2012-04-12T16:49:28-09:00	T003	[00027, 0066, 0091, 0101]	::	0.88	::
2012-04-12T16:50:32-09:00	T001	[0005, 0012, 0036]	::	0.90	::

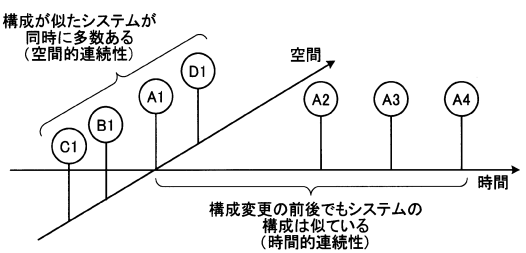
【図 10】

障害予兆パターンの学習を説明する図



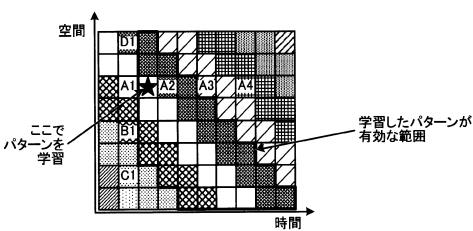
【図 11】

構成情報の遷移を説明する図



【図 12】

障害予兆パターンの有効範囲を説明する図



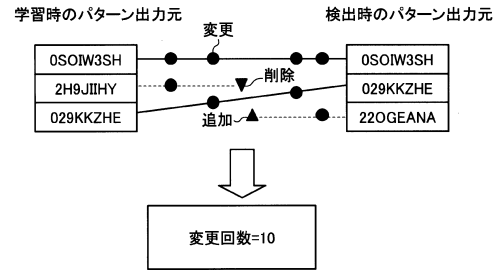
【図 13】

障害予兆検出時の構成情報例を示す図

パターン	[0005, 0007, 0012]	
検出時刻	2012-04-12T16:16:00-09:00	
時刻	メッセージ 種別ID	メッセージ 発信CI
2012-04-12T16:16:00-09:00	0012	0SOIW3SH
2012-04-12T16:15:40-09:00	0007	029KKZHE
2012-04-12T16:14:38-09:00	0007	22OGEANA
2012-04-12T16:14:31-09:00	0005	029KKZHE
⋮	⋮	⋮

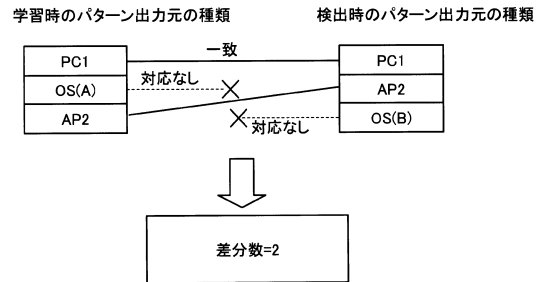
【図 14】

構成の変更回数を説明する図



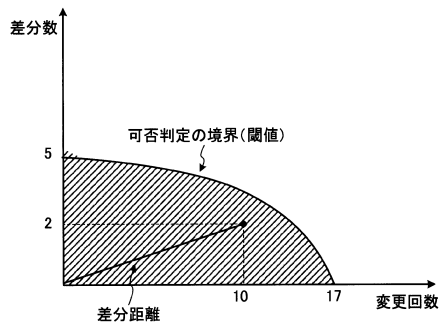
【図 15】

構成の差分数を説明する図



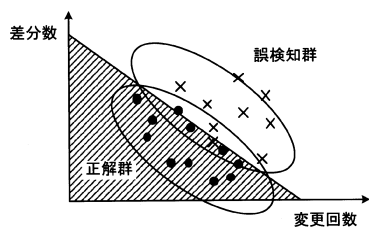
【図 16】

判定基準を説明する図



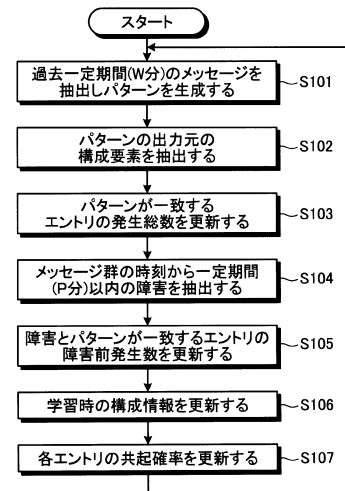
【図 17】

閾値の学習を説明する図



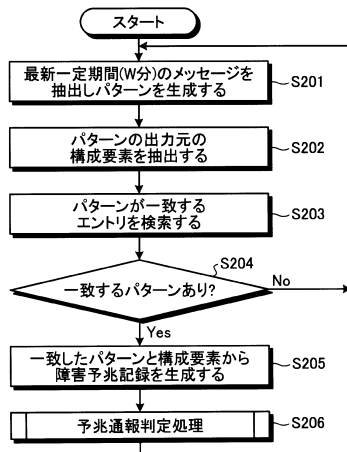
【図 18】

障害予兆学習処理の流れを示すフローチャート



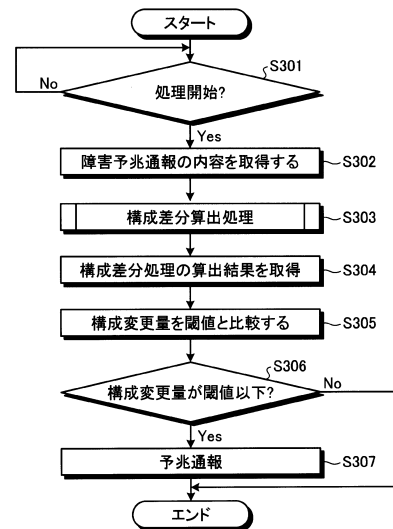
【図 19】

障害予兆検出処理の流れを示すフローチャート



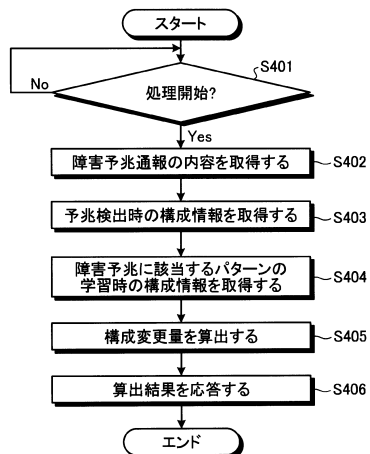
【図 20】

予兆通報判定処理の流れを示すフローチャート



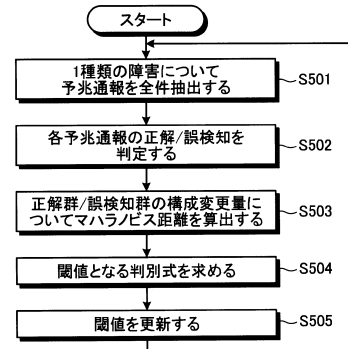
【図 21】

構成差分算出処理の流れを示すフローチャート



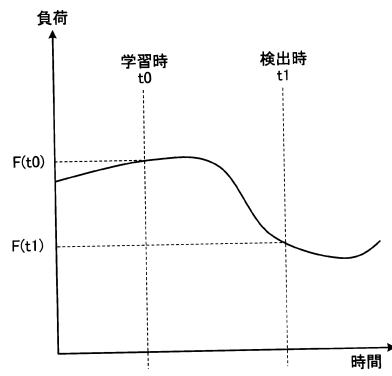
【図 22】

閾値学習処理の流れを示すフローチャート



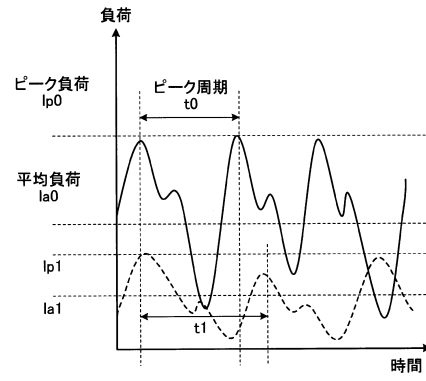
【図 2 3】

負荷量を説明する図



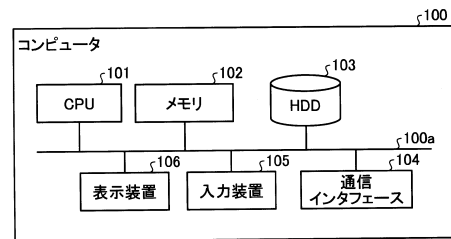
【図 2 4】

負荷パターンを説明する図



【図 2 5】

ハードウェア構成例を説明する図



フロントページの続き

審査官 多胡 滋

- (56)参考文献 国際公開第2011/125138 (WO, A1)
特表2009-533739 (JP, A)
特開2009-193153 (JP, A)
国際公開第2012/067031 (WO, A1)
特開2009-176203 (JP, A)
特開2010-231825 (JP, A)

- (58)調査した分野(Int.Cl., DB名)
G06F 11/30
G06F 11/34