

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2020-149250

(P2020-149250A)

(43) 公開日 令和2年9月17日(2020.9.17)

(51) Int.Cl.		F I				テーマコード (参考)
G 0 6 F	11/07	(2006.01)	G 0 6 F	11/07	1 8 1	5 B 0 4 2
G 0 6 F	16/30	(2019.01)	G 0 6 F	16/30		
G 0 6 F	16/38	(2019.01)	G 0 6 F	16/38		
G 0 6 F	16/335	(2019.01)	G 0 6 F	16/335		

審査請求 未請求 請求項の数 7 O L (全 23 頁)

(21) 出願番号	特願2019-45267 (P2019-45267)	(71) 出願人	000005223
(22) 出願日	平成31年3月12日 (2019.3.12)		富士通株式会社
			神奈川県川崎市中原区上小田中4丁目1番1号
		(74) 代理人	110002147
			特許業務法人酒井国際特許事務所
		(72) 発明者	齋藤 悠司
			神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内
		(72) 発明者	内海 哲哉
			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	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

最終頁に続く

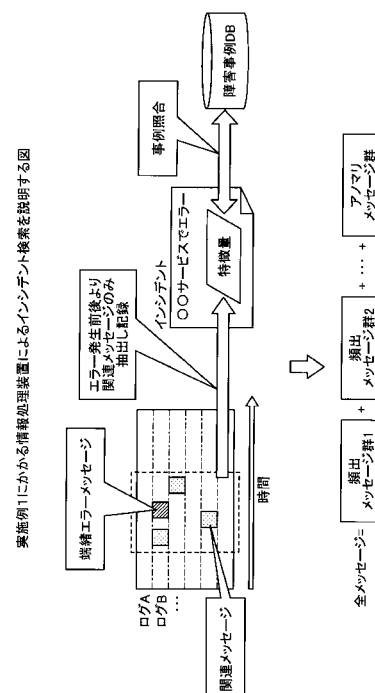
(54) 【発明の名称】 出力プログラム、出力方法および情報処理装置

(57) 【要約】

【課題】 出現頻度の低いエラーメッセージを有効利用したインシデント検索を実行することを課題とする。

【解決手段】 情報処理装置は、過去に発生したメッセージ群に含まれる各メッセージの出現頻度に基づいて、頻出メッセージ群を生成する。情報処理装置は、エラーメッセージの発生に応じて、蓄積されるメッセージ群の中からエラーメッセージの前後所定時間分のメッセージ群をエラー周辺ログとして抽出する。情報処理装置は、エラー周辺ログと頻出メッセージ群の関連度合に基づいて、エラーメッセージが頻出メッセージ群に含まれるか否かを判定する。情報処理装置は、判定結果に応じて、頻出メッセージ群、または、エラー周辺ログのうち頻出メッセージ群に含まれないメッセージを、エラーメッセージに関連付けられる関連メッセージとして出力する。

【選択図】 図2



【特許請求の範囲】**【請求項 1】**

コンピュータに、

過去に発生したメッセージ群に含まれる各メッセージの出現頻度に基づいて、頻出メッセージ群を生成し、

エラーメッセージの発生に応じて、蓄積されるメッセージ群の中から前記エラーメッセージの前後所定時間分のメッセージ群をエラー周辺ログとして抽出し、

前記エラー周辺ログと前記頻出メッセージ群の関連度合に基づいて、前記エラーメッセージが前記頻出メッセージ群に含まれるか否かを判定し、

判定結果に応じて、前記頻出メッセージ群、または、前記エラー周辺ログのうち前記頻出メッセージ群に含まれないメッセージを、前記エラーメッセージに関連付けられる関連メッセージとして出力する

10

処理を実行させることを特徴とする出力プログラム。

【請求項 2】

前記エラー周辺ログのうち前記頻出メッセージ群では表現できないメッセージ群を、前記エラー周辺ログのうち前記頻出メッセージ群に含まれないメッセージであるアノマリメッセージ群として抽出する処理を前記コンピュータに実行させ、

前記出力する処理は、前記エラーメッセージが前記頻出メッセージ群に含まれる場合、前記頻出メッセージ群を前記関連メッセージとして出力し、前記エラーメッセージが前記頻出メッセージ群に含まれない場合、前記アノマリメッセージ群を前記関連メッセージとして出力することを特徴とする請求項 1 に記載の出力プログラム。

20

【請求項 3】

前記生成する処理は、前記過去に発生したメッセージ群である観測メッセージ群に含まれる各メッセージを形式ごとに分類し、分類した各メッセージの形式の出現回数を集計して、観測データ行列を生成し、前記観測データ行列から前記頻出メッセージ群を生成することを特徴とする請求項 2 に記載の出力プログラム。

【請求項 4】

前記抽出する処理は、前記観測メッセージ群に含まれる各メッセージの形式ごとに前記エラー周辺ログを分類し、分類した各メッセージ形式の出現回数を集計して、エラー周辺の観測データ行列を生成し、

30

前記判定する処理は、前記エラー周辺の観測データ行列に含まれる前記頻出メッセージ群を抽出するとともに、前記エラー周辺の観測データ行列から前記頻出メッセージ群を除く前記アノマリメッセージ群を抽出し、前記エラーメッセージが発生した時間帯に前記頻出メッセージ群が発生しているかを判定することを特徴とする請求項 3 に記載の出力プログラム。

【請求項 5】

前記出力する処理は、前記エラーメッセージが発生した時間帯に前記頻出メッセージ群が発生している場合、前記頻出メッセージ群を前記関連メッセージとして出力し、前記エラーメッセージが発生した時間帯に前記頻出メッセージ群が発生していない場合、前記アノマリメッセージ群を前記関連メッセージとして出力することを特徴とする請求項 4 に記載の出力プログラム。

40

【請求項 6】

コンピュータが、

過去に発生したメッセージ群に含まれる各メッセージの出現頻度に基づいて、頻出メッセージ群を生成し、

エラーメッセージの発生に応じて、蓄積されるメッセージ群の中から前記エラーメッセージの前後所定時間分のメッセージ群をエラー周辺ログとして抽出し、

前記エラー周辺ログと前記頻出メッセージ群の関連度合に基づいて、前記エラーメッセージが前記頻出メッセージ群に含まれるか否かを判定し、

判定結果に応じて、前記頻出メッセージ群、または、前記エラー周辺ログのうち前記頻

50

出メッセージ群に含まれないメッセージを、前記エラーメッセージに関連付けられる関連メッセージとして出力する

処理を実行することを特徴とする出力方法。

【請求項 7】

過去に発生したメッセージ群に含まれる各メッセージの出現頻度に基づいて、頻出メッセージ群を生成する生成部と、

エラーメッセージの発生に応じて、蓄積されるメッセージ群の中から前記エラーメッセージの前後所定時間分のメッセージ群をエラー周辺ログとして抽出する抽出部と、

前記エラー周辺ログと前記頻出メッセージ群の関連度合に基づいて、前記エラーメッセージが前記頻出メッセージ群に含まれるか否かを判定する判定部と、

判定結果に応じて、前記頻出メッセージ群、または、前記エラー周辺ログのうち前記頻出メッセージ群に含まれないメッセージを、前記エラーメッセージに関連付けられる関連メッセージとして出力する出力部と

を有することを特徴とする情報処理装置。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、出力プログラム、出力方法および情報処理装置に関する。

【背景技術】

【0002】

ICT (Information and Communication Technology) システムにおけるインシデント対応では、インシデント発生時に過去に発生済みであるか否かを判別する既知障害判別を実行し、発生していれば過去の対処方法などの再利用が行われる。

【0003】

この既知障害判別は、過去のインシデント対応記録を保持した障害事例DBを検索することで行われる。その際、インシデントの端緒となったエラーメッセージをキーワードとして検索することが多いが、端緒となったエラーメッセージのみによる障害事例DBの検索では、エラーメッセージの内容は同一であるが、原因や対策が異なる事象が誤って検索される場合がある。このため、近年では、対象のエラーメッセージと過去に頻繁に一緒に出現した頻出メッセージ群を特定しておき、頻出メッセージ群をインシデントの検索に利用することで、誤検索を抑制する技術が利用されている。

【先行技術文献】

【特許文献】

【0004】

【特許文献 1】特開 2006-4346 号公報

【特許文献 2】特開 2017-72882 号公報

【非特許文献】

【0005】

【非特許文献 1】Y. Watanabe, H. Otsuka, M. Sonoda, S. Kikuchi and Y. Matsumoto, "Online failure prediction in cloud datacenters by real-time message pattern learning", 4th IEEE International Conference on Cloud Computing Technology and Science Proceedings, Taipei, 2012, pp.504-511.

【非特許文献 2】東羅翔太郎, 豊田真智子, 中村吉孝, "Convolutional NMFにおける時間フレームの間隔変化に関する一考察", NTTソフトウェアイノベーションセンタ, DEIM Forum 2015 F8-1.

【非特許文献 3】Wang, Wenwu and Cichocki, Andrzej and Chambers, Jonathon A, "A multiplicative algorithm for convolutional non-negative matrix factorization based on squared Euclidean distance", IEEE Transactions on Signal Processing, vol157, No.7, p2858-2864, 2009.

【発明の概要】

【発明が解決しようとする課題】

【0006】

しかしながら、上記技術では、頻出メッセージ群に含まれない、新規のエラーメッセージや出現頻度の低いエラーメッセージをインシデント検索に利用できないので、有効な対処方法が検索できるとはいえない。

【0007】

一つの側面では、出現頻度の低いエラーメッセージを有効利用したインシデント検索を実行することができる出力プログラム、出力方法および情報処理装置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】

【0008】

第1の案では、出力プログラムは、コンピュータに、過去に発生したメッセージ群に含まれる各メッセージの出現頻度に基づいて、頻出メッセージ群を生成する処理を実行させる。出力プログラムは、コンピュータに、エラーメッセージの発生に応じて、蓄積されるメッセージ群の中から前記エラーメッセージの前後所定時間分のメッセージ群をエラー周辺ログとして抽出する処理を実行させる。出力プログラムは、コンピュータに、前記エラー周辺ログと前記頻出メッセージ群の関連度合に基づいて、前記エラーメッセージが前記頻出メッセージ群に含まれるか否かを判定する処理を実行させる。出力プログラムは、コンピュータに、判定結果に応じて、前記頻出メッセージ群、または、前記エラー周辺ログのうち前記頻出メッセージ群に含まれないメッセージを、前記エラーメッセージに関連付けられる関連メッセージとして出力する処理を実行させる。

【発明の効果】

【0009】

一実施形態によれば、出現頻度の低いエラーメッセージを有効利用したインシデント検索を実行することができる。

【図面の簡単な説明】

【0010】

【図1】図1は、実施例1にかかるインシデント検索システムの全体構成を説明する図である。

【図2】図2は、実施例1にかかる情報処理装置によるインシデント検索を説明する図である。

【図3】図3は、実施例1にかかる情報処理装置の機能構成を示す機能ブロック図である。

【図4】図4は、障害事例DBに記憶される情報の例を示す図である。

【図5】図5は、利用するログメッセージを説明する図である。

【図6】図6は、学習手法を説明する図である。

【図7】図7は、学習手法の定義一覧を示す図である。

【図8】図8は、学習用ログの分類結果を示す図である。

【図9】図9は、観測データ行列の作成を説明する図である。

【図10】図10は、頻出メッセージ群の学習結果を示す図である。

【図11】図11は、エラー周辺ログの抽出を説明する図である。

【図12】図12は、エラー周辺ログに対する観測データ行列を説明する図である。

【図13】図13は、重み係数行列の算出結果の例を示す図である。

【図14】図14は、アノマリメッセージ群の抽出を説明する図である。

【図15】図15は、メッセージの判別を説明する図である。

【図16】図16は、関連メッセージ群を説明する図である。

【図17】図17は、学習フェーズの処理の流れを示すフローチャートである。

【図18】図18は、抽出フェーズの処理の流れを示すフローチャートである。

【図19】図19は、多点障害の問題点を説明する図である。

【図20】図20は、実施例2にかかる学習用ログの分類結果を示す図である。

10

20

30

40

50

【図 2 1】図 2 1 は、実施例 2 にかかる観測データ行列の作成を説明する図である。

【図 2 2】図 2 2 は、実施例 2 にかかる頻出メッセージ群の学習結果を説明する図である。

【図 2 3】図 2 3 は、実施例 2 にかかるエラー周辺ログの抽出を説明する図である。

【図 2 4】図 2 4 は、実施例 2 にかかるエラー周辺ログに対する観測データ行列を説明する図である。

【図 2 5】図 2 5 は、実施例 2 にかかる重み係数行列の算出結果の例を示す図である。

【図 2 6】図 2 6 は、実施例 2 にかかるアノマリメッセージ群の抽出を説明する図である。

【図 2 7】図 2 7 は、実施例 2 にかかるメッセージの判別例 1 を説明する図である。

10

【図 2 8】図 2 8 は、実施例 2 にかかるメッセージの判別例 2 を説明する図である。

【図 2 9】図 2 9 は、実施例 2 にかかる出力結果を説明する図である。

【図 3 0】図 3 0 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】

【0011】

以下に、本願の開示する出力プログラム、出力方法および情報処理装置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。また、各実施例は、矛盾のない範囲内で適宜組み合わせることができる。

【実施例 1】

【0012】

20

〔全体構成〕

図 1 は、実施例 1 にかかるインシデント検索システムの全体構成を説明する図である。図 1 に示すように、このシステムは、情報処理装置 10 と複数のユーザ端末 50 とがネットワーク N を介して相互に通信可能に接続される。なお、ネットワーク N には、有線や無線を問わず、インターネットや専用線などの各種通信網を採用することができる。

【0013】

情報処理装置 10 は、過去のインシデント対応記録を保持した障害事例 DB を保持し、各ユーザ端末からの検索要求に応じて、過去の対処内容を応答するコンピュータ装置の一例である。

【0014】

30

各ユーザ端末 50 は、システム管理者などが利用するコンピュータ装置の一例であり、システム障害などの発生時に、エラーメッセージなどを検索条件とする検索要求を情報処理装置 10 に送信する。そして、各ユーザ端末 50 は、検索要求に対応する対処内容を取得する。このようにして、システム管理者は、障害発生時に、過去に対応された対処内容を取得して、障害対応を行う。

【0015】

このような情報処理装置 10 が、各ユーザ端末 50 から検索要求に応じて実行するインシデント検索について説明する。図 2 は、実施例 1 にかかる情報処理装置 10 によるインシデント検索を説明する図である。図 2 に示すように、情報処理装置 10 は、対象システムのログメッセージ（以下では単に「ログ」と記載する場合がある）を出力順の時系列で収集する。

40

【0016】

そして、情報処理装置 10 は、システム障害「〇〇サービスでエラー」が発生すると、システム障害の端緒となったエラーメッセージである端緒エラーメッセージを特定する。すると、情報処理装置 10 は、端緒エラーメッセージの発生前後から、端緒エラーメッセージ周辺の関連メッセージを自動的に選別して収集する。そして、情報処理装置 10 は、関連メッセージを特徴量として、システム障害「〇〇サービスでエラー」に対応付けることでインシデントの特徴づけを行い、障害事例の事例照合に利用する。

【0017】

ここで、情報処理装置 10 は、全ログメッセージをよく一緒に出現する頻出メッセージ

50

群と、これまで出現頻度の低いアノマリメッセージ群とに分解する。なお、頻出メッセージの例としては、定期サーバの再起動や定期バックアップなどである。そして、情報処理装置 10 は、エラーを含むメッセージ群を関連メッセージ群として抽出する。具体的には、過去に頻繁に発生しているエラーは、頻出メッセージ群に含まれ、新規または頻繁ではないエラーは、アノマリメッセージ群に含まれることとなる。

【0018】

つまり、情報処理装置 10 は、発生頻度が少ないエラーであっても、当該エラーに関連する関連メッセージ群を生成して、当該エラーの特徴量として管理することができる。この結果、情報処理装置 10 は、アノマリメッセージ群に該当するログもインシデント検索に利用することができるので、出現頻度の低いエラーメッセージを有効利用したインシデント検索を実行することができる。

10

【0019】

〔機能構成〕

図 3 は、実施例 1 にかかる情報処理装置 10 の機能構成を示す機能ブロック図である。図 3 に示すように、情報処理装置 10 は、通信部 11、記憶部 12、制御部 20 を有する。

【0020】

通信部 11 は、他の装置との間の通信を制御する処理部であり、例えば通信インタフェースなどである。例えば、通信部 11 は、対象システムのログメッセージの一覧を受信し、ユーザ端末 50 から各種要求やデータを受信し、ユーザ端末 50 に各種情報などを送信する。

20

【0021】

記憶部 12 は、データや制御部 20 が実行する各種プログラムなどを記憶する記憶装置の一例であり、例えばメモリやハードディスクなどである。この記憶部 12 は、障害事例 DB 13 を記憶する。

【0022】

障害事例 DB 13 は、過去のインシデント対応記録を記憶するデータベースである。具体的には、障害事例 DB 13 は、障害発生時の対処内容を記憶する。図 4 は、障害事例 DB 13 に記憶される情報の例を示す図である。図 4 に示すように、障害事例 DB 13 は、「メッセージ群、対処方法」を対応付けて記憶する。

30

【0023】

ここで記憶される「メッセージ群」は、障害発生時に出力されたメッセージを示し、「対処方法」は、障害に対して実行された対処内容を示す。図 4 の例では、「〇〇でエラー」と「××サービス停止」のメッセージが両方出力されたときの障害に対して、「再起動後に××サービス起動」の対処が行われたことを示す。なお、障害事例 DB 13 が記憶する情報は、障害内容などをさらに対応付けることもでき、任意に変更することができる。また、ここで記憶される情報は、管理者などが格納することもでき、公知の手法を用いて情報処理装置 10 が自動で生成することもできる。

【0024】

制御部 20 は、情報処理装置 10 全体を司る処理部であり、例えばプロセッサなどである。この制御部 20 は、学習処理部 30、抽出処理部 40 を有する。なお、学習処理部 30、抽出処理部 40 は、プロセッサが有する電子回路の一例やプロセッサが実行するプロセスの一例である。

40

【0025】

ここで、学習処理部 30 や抽出処理部 40 で利用するログメッセージについて説明する。図 5 は、利用するログメッセージを説明する図である。図 5 に示すように、出力順に時系列で保存されるログメッセージにおいて、学習処理部 30 は、エラー発生前の一定期間のログを学習用ログとして利用する。また、抽出処理部 40 は、学習用ログとは異なり、エラーメッセージを含むエラーメッセージ周辺時刻のログを、エラー周辺ログとして利用する。

50

【0026】

また、本実施例では、例えば「NTTソフトウェアイノベーションセンタ、Convolutional NMFにおける時間フレームの間隔変化に関する一考察、DEIM2015」に示されるように、NMF (Non-negative Matrix Factorization) を拡張した畳込み非負値行列因子分解 (CNMF) を利用することができる。図6は、学習手法を説明する図である。図6に示すように、本実施例では、問題を行列分解として定式化し、頻出メッセージ群を基底として抽出する。例えば、観測データ行列の時間枠において、各ログ ($L_1 \sim L_N$) の出現数を計数する。そして、観測データ行列から基底行列を抽出する際に、基底行列に幅 T を持たせるように処理して、頻出メッセージ群を基底として抽出する。

【0027】

10

また、CNMFで使用する定義一覧を図7に示す。図7は、学習手法の定義一覧を示す図である。図7に示すように、本実施例で使用する記号として、学習用ログの観測データ行列、学習用ログの重み係数行列、エラー周辺ログの観測データ行列、エラー周辺ログの重み係数行列、基底行列 (頻出メッセージ群)、アノマリメッセージ行列、頻出メッセージ群の最大数、メッセージ形式数、観測データ行列の時間枠の幅、基底行列の時間幅を定義する。また、本実施例においては、観測データ行列の時間枠の幅を T_M 、頻出メッセージ群の最大数を K 、基底行列の時間幅を T とする。

【0028】

図3に戻り、学習処理部30は、分類部31、作成部32、学習部33を有し、頻出メッセージ群の学習処理を実行する処理部である。すなわち、学習処理部30は、学習フェーズを実行する。

20

【0029】

分類部31は、学習用ログから形式が類似するメッセージ进行分类する処理部である。具体的には、分類部31は、ログメッセージの一覧から図5に示す学習用ログに該当するログメッセージを取得し、メッセージに含まれるIP (Internet Protocol) アドレスやホスト名などのパラメータ部分を除外したメッセージ形式ごとに分類して、作成部32に出力する。

【0030】

図8は、学習用ログの分類結果を示す図である。図8に示すように、分類部31は、「DBでエラー」にメッセージ形式ID「1」を割当てて分類し、「IP: *でバックアップを開始します」にメッセージ形式ID「2」を割当てて分類し、「IP: *でバックアップを完了しました」にメッセージ形式ID「3」を割当てて分類する。また、分類部31は、「Aサービス起動」にメッセージ形式ID「4」を割当てて分類し、「Bサービス起動」にメッセージ形式ID「5」を割当てて分類する。

30

【0031】

作成部32は、分類部31による分類結果を用いて、学習用の観測データ行列を作成する処理部である。具体的には、作成部32は、分類されたメッセージ形式ごとの出現回数を集計し、集計結果に基づき観測データ行列 Y を作成して、学習部33に出力する。

【0032】

図9は、観測データ行列の作成を説明する図である。図9に示すように、作成部32は、メッセージ形式ID「1」から「5」のそれぞれが割当てられた「DBでエラー」などの各メッセージの出現回数を、「1/1 00:00:00~00:10:00」などの各時間帯で計数する。図9の例では、メッセージ形式ID「1」のメッセージ「DBでエラー」は、時間帯「1/1 00:00:00~00:10:00」では出現回数「0」、時間帯「1/1 00:10:00~00:20:00」では出現回数「0」、時間帯「1/1 01:00:00~01:10:00」では出現回数「1」であることを示す。このようにして、作成部32は、各メッセージの集計結果を観測データ行列 Y として作成する。

40

【0033】

学習部33は、作成部32による観測データ行列の作成結果から頻出メッセージ群を学習する処理部である。例えば、学習部33は、基底行列の時間幅 T を2、頻出メッセージ

50

群数 K を 2 とし、上述した CNMF により、頻出メッセージ群（基底行列 H_t ）を学習する。

【0034】

図 10 は、頻出メッセージ群の学習結果を示す図である。図 10 に示すように、学習部 33 は、図 9 に示した観測データ行列 Y に対して CNMF を実行することで、頻出メッセージ群として、バックアップメッセージ群とサービス起動メッセージ群を抽出して、抽出処理部 40 に出力する。

【0035】

なお、バックアップメッセージ群は、図 8 や図 9 に示すメッセージ形式「ID」が「2」である「IP：＊でバックを開始します」と、メッセージ形式 ID が「3」である「IP：＊でバックアップを完了しました」とを含むメッセージ群である。また、サービス起動メッセージ群は、図 8 や図 9 に示すメッセージ形式「ID」が「4」である「A サービス起動」と、メッセージ形式 ID が「5」である「B サービス起動」とを含むメッセージ群である。

【0036】

抽出処理部 40 は、ログ抽出部 41、行列作成部 42、メッセージ抽出部 43、判別部 44、出力部 45 を有し、エラーメッセージに関連する関連メッセージ群の抽出を実行する処理部である。

【0037】

ログ抽出部 41 は、エラーログに関連するログ抽出を行うために、エラーログの周辺ログを抽出する処理部である。具体的には、ログ抽出部 41 は、ログメッセージの一覧から図 5 に示すエラー周辺用ログに該当するログメッセージを取得して、行列作成部 42 に出力する。

【0038】

図 11 は、エラー周辺ログの抽出を説明する図である。図 11 に示すように、ログ抽出部 41 は、全ログメッセージから、エラーメッセージ発生の前後 60 分をエラー周辺ログとして抽出する。図 11 の例では、「2/1 00:30:00」にエラーメッセージ「DBでエラー」が発生しているので、「2/1 00:30:00」の 60 分前である「1/31 23:30:00」に発生した「XXXXXXXX」から、「2/1 00:30:00」の 60 分後である「2/1 01:30:00」に発生した「YYYYYY」までがエラー周辺ログとして抽出される。

【0039】

行列作成部 42 は、学習処理部 30 による学習フェーズにより分類されたメッセージ形式ごとに出現回数を計数し、エラー周辺用の観測データ行列を作成する処理部である。具体的には、行列作成部 42 は、図 9 に示すメッセージ形式 ID ごとにエラー周辺ログを分類する。そして、行列作成部 42 は、分類されたメッセージ形式ごとの出現回数を集計し、CNMF により観測データ行列 Y を作成して、メッセージ抽出部 43 に出力する。

【0040】

図 12 は、エラー周辺ログに対する観測データ行列を説明する図である。図 12 に示すように、行列作成部 42 は、ログ抽出部 41 で抽出されたエラー周辺ログを、学習処理部 30 で分類されたメッセージ形式 ID「1」から「5」のそれぞれのメッセージに分類する。そして、行列作成部 42 は、分類された各メッセージ形式の各時間帯の出現回数を、学習処理部 30 と同様の手法により集計する。このようにして、行列作成部 42 は、エラー周辺ログから観測データ行列 Y' を作成する。

【0041】

メッセージ抽出部 43 は、学習処理部 30 による学習フェーズにて学習された基底行列を用いて、行列作成部 42 により作成された観測データ行列に含まれる頻出メッセージ群を抽出する処理部である。例えば、メッセージ抽出部 43 は、「Wang, Wenwu and Cichocki, Andrzej and Chambers, Jonathon A, "A multiplicative algorithm for convolutive non-negative matrix factorization based on squared Euclidean distance", IEEE Transactions on Signal Processing, vol57, No.7, p2858-28

10

20

30

40

50

64, 2009」に示される技術を用いることができる。具体的には、メッセージ抽出部 43 は、学習処理部 30 により学習された基底行列 H_t と観測データ行列 Y' とを用いて、式 (1) により頻出メッセージ群を抽出する。

【0042】

【数 1】

$$U'^* = \arg \min_{U'} \left\| Y' - \sum_{t=0}^{T-1} H_t U'^{t \rightarrow} \right\|_2^2, U' > 0 \quad \cdots \text{式(1)}$$

($\|\cdot\|_2$ は L2 ノルムを表す)

10

【0043】

重み係数行列 U' は、頻出メッセージ群のうちエラー周辺ログに含まれるものを表すことから、式 (1) を最小化する重み行列 U' を求めることで、エラー周辺メッセージから作成された観測データ行列 Y' に含まれる頻出メッセージ群を抽出することができる。図 13 は、重み係数行列の算出結果の例を示す図である。本実施例では、図 13 に示すように、頻出メッセージ群のうちバックアップメッセージ群について、時間帯「2/1 00:00:00~00:10:00」に「1」が設定されたとする。

【0044】

また、メッセージ抽出部 43 は、頻出メッセージ群では表現できない観測データ行列 Y' をアノマリメッセージ群として抽出する。例えば、メッセージ抽出部 43 は、式 (2) を用いて、観測データ行列 Y' のうち基底行列 H_t の組み合わせで表現できないメッセージ群を、アノマリメッセージ行列として算出する。

20

【0045】

【数 2】

$$A = Y' - \sum_{t=0}^{T-1} H_t U'^{t \rightarrow} \quad \cdots \text{式(2)}$$

【0046】

そして、メッセージ抽出部 43 は、算出されたアノマリメッセージ行列の要素のうち 0 より大きい要素値が設定されたメッセージ形式を、アノマリメッセージ群として抽出する。図 14 は、アノマリメッセージ群の抽出を説明する図である。図 14 に示すように、メッセージ抽出部 43 は、学習処理部 30 で分類されたメッセージ形式 ID「1」から「5」のそれぞれのメッセージに対する算出結果をアノマリメッセージ行列 A として算出する。そして、メッセージ抽出部 43 は、要素値が 0 より大きい「1」が設定される、「2/1 00:30:00 DBでエラー」と「2/1 00:30:00 Aサービス起動」とを、アノマリメッセージ群として抽出する。

30

【0047】

図 3 に戻り、判別部 44 は、エラーメッセージと関連する関連メッセージの判別を実行する処理部である。具体的には、判別部 44 は、対象エラーメッセージを含む頻出メッセージ群を特定して関連メッセージ群とするとともに、頻出メッセージ群が特定されなかった場合に、アノマリメッセージ群を関連メッセージ群として抽出する。

40

【0048】

図 15 は、メッセージの判別を説明する図である。図 15 に示すように、判別部 44 は、図 11 に示した「2/1 00:30:00」の対象のエラーメッセージ「DBでエラー」の時間帯と、重み係数行列 U' とを比較し、エラーメッセージの発生時間帯「2/1 00:30:00」を含む時間帯「00:30:00~00:40:00」に頻出メッセージ群の出現がないので、関連メッセージ群を特定できないと判別する。

【0049】

そして、判別部 44 は、頻出メッセージ群の出現がないことから、アノマリメッセージ群を関連メッセージ群と判別する。図 16 は、関連メッセージ群を説明する図である。図

50

16に示すように、判別部44は、図14で抽出したアノマリメッセージ群を関連メッセージと判別するが、このとき対象エラー「DBでエラー」を除外した「2/1 00:30:00 Aサービス起動」のみを関連メッセージ群とする。

【0050】

出力部45は、判別部44による判別結果を出力する処理部である。例えば、出力部45は、対象のエラーメッセージ「2/1 00:30:00 DBでエラー」と関連メッセージ「2/1 00:30:00 Aサービス起動」とを対応付けて、ディスプレイに表示したり、管理者端末に送信したりする。

【0051】

この結果、管理者などは、エラーメッセージ「DBでエラー」が発生して対処が完了すると、エラーメッセージ「DBでエラー」と関連メッセージ「Aサービス起動」と対処内容とを対応付けて、障害事例DB13に登録することができる。また、管理者は、次にエラーメッセージ「DBでエラー」が発生したときに、「DBでエラー」と「Aサービス起動」と検索条件として、障害事例DB13を検索することで、過去の対処方法を取得することもできる。

【0052】

[学習フェーズの流れ]

図17は、学習フェーズの処理の流れを示すフローチャートである。図17に示すように、学習処理部30の分類部31は、1週間ごとのように定期的に、または、ログメッセージが一定値以上増加した場合に、処理開始と判定し（S101:Yes）、ログメッセージを取得して、ログメッセージから学習用ログを取得する（S102）。

【0053】

続いて、分類部31は、学習用ログをメッセージ形式で分類する（S103）。そして、作成部32は、分類結果を用いて、学習用ログの観測データ行列を生成する（S104）。その後、学習部33は、観測データ行列を用いて、学習用ログの頻出メッセージ群の学習を実行する（S105）。

【0054】

[抽出フェーズの流れ]

図18は、抽出フェーズの処理の流れを示すフローチャートである。図18に示すように、抽出処理部40のログ抽出部41は、エラーがメッセージを検出すると、処理開始と判定し（S201:Yes）、ログメッセージからエラー周辺ログを抽出する（S202）。

【0055】

続いて、行列作成部42は、エラー周辺ログの観測データ行列を生成する（S203）。そして、メッセージ抽出部43は、エラー周辺ログ中に出現する頻出メッセージ群を抽出し（S204）、エラー周辺ログ中のアノマリメッセージ群を抽出する（S205）。

【0056】

その後、判別部44は、頻出メッセージ群がエラーメッセージを含むか否かを判定する（S206）。そして、判別部44は、頻出メッセージ群がエラーメッセージを含む場合（S206:Yes）、頻出メッセージ群を関連メッセージ群と決定し（S207）、頻出メッセージ群がエラーメッセージを含まない場合（S206:No）、アノマリメッセージ群を関連メッセージ群と決定する（S208）。

【0057】

[効果]

上述したように、情報処理装置10は、図5に示した全メッセージを、エラーメッセージを含まない頻出メッセージ群と、エラーメッセージを含むアノマリメッセージ群とに分類することができる。したがって、情報処理装置10は、頻出メッセージ群に含まれない、新規のエラーメッセージや出現頻度の低いエラーメッセージも、エラーメッセージと関連する関連メッセージ群として対応付けることができる。このため、情報処理装置10は、既知の障害判別において、新規または過去に出現頻度の低いエラーメッセージであって

10

20

30

40

50

も、インシデント検索に利用することができるので、誤検索を抑制し、検索精度を向上させることができる。

【実施例 2】

【0058】

ところで、頻出メッセージ群だけを関連メッセージとして対応付ける一般技術では、同時に複数の障害が発生した場合（多点障害）、メッセージ全体からどのメッセージがどの障害に関連するメッセージであるかを特定できない場合がある。

【0059】

図 19 は、多点障害の問題点を説明する図である。図 19 には、障害 1、障害 2、障害 3 の 3 つの多点障害が発生した例を示している。実施例 1 のようなアノマリメッセージ群を利用しない場合、各障害を頻出メッセージ群と対応付けることになる。例えば、頻出メッセージ群として障害 1 エラーの関連メッセージを特定し、頻出メッセージ群として障害 2 エラーの関連メッセージを特定できたとしても、障害 3 エラーが新規エラーや出現頻度の低いエラーであった場合、頻出メッセージ群が存在しないことから、関連メッセージ群を特定できないことがある。

【0060】

この結果、障害 3 のエラー情報を障害事例として登録することができず、次に障害 3 と同様の障害が発生しても、その対処方法を共有することもできない。したがって、システムの信頼性の低下にもつながる。

【0061】

そこで、実施例 2 では、実施例 1 で説明したアノマリメッセージ群を関連メッセージ群として抽出することで、同時に複数の障害が発生した場合（多点障害）に、メッセージ全体を各障害に対応する関連メッセージ群に分解する例を説明する。なお、機能構成や学習手法などは、実施例 1 と同様なので、詳細な説明は省略する。

【0062】

〔学習フェーズ〕

まず、学習処理部 30 は、実施例 1 と同様の手法を用いて、学習用ログから形式が類似するメッセージを分類する。図 20 は、実施例 2 にかかる学習用ログの分類結果を示す図である。図 20 に示すように、学習処理部 30 は、「DB でエラー」にメッセージ形式 ID「1」を割当てて分類し、「IP：*でバックアップを開始します」にメッセージ形式 ID「2」を割当てて分類し、「IP：*でバックアップを完了しました」にメッセージ形式 ID「3」を割当てて分類する。また、分類部 31 は、「A サービス起動」にメッセージ形式 ID「4」を割当てて分類し、「B サービス起動」にメッセージ形式 ID「5」を割当てて分類する。

【0063】

実施例 1 と異なる点は、実施例 1 の図 8 では、1 つの DB エラーが発生している例であったのに対して、実施例 2 の図 20 では、2 つの DB エラーが発生している点である。すなわち、図 20 は、多点障害が発生している。

【0064】

次に、学習処理部 30 は、実施例 1 と同様の手法を用いて、分類結果から学習用の観測データ行列を作成する。図 21 は、実施例 2 にかかる観測データ行列の作成を説明する図である。図 21 に示すように、学習処理部 30 は、メッセージ形式 ID「1」から「5」のそれぞれが割当てられた「DB でエラー」などの各メッセージの出現回数を、「1/1 00:00:00~00:10:00」などの各時間帯で計数する。図 21 の例では、実施例 1 と異なり、メッセージ形式 ID「1」のメッセージ「DB でエラー」が、時間帯「1/1 00:00:00~00:10:00」と、時間帯「1/1 01:00:00~01:10:00」との両方で発生している。このようにして、学習処理部 30 は、各メッセージの集計結果を観測データ行列 Y として作成する。

【0065】

続いて、学習処理部 30 は、実施例 1 と同様の CNMF により、観測データ行列の作成結果から頻出メッセージ群を学習する。図 22 は、実施例 2 にかかる頻出メッセージ群の

10

20

30

40

50

学習結果を説明する図である。図 2 2 に示すように、学習処理部 3 0 は、図 2 1 に示した観測データ行列 Y に対して CNMF を実行することで、頻出メッセージ群として、バックアップメッセージ群とサービス起動メッセージ群を抽出する。

【0066】

なお、実施例 1 と異なり、バックアップメッセージ群は、メッセージ形式「ID」が「2」である「IP：*でバックを開始します」と、メッセージ形式 ID が「3」である「IP：*でバックアップを完了しました」に加えて、メッセージ形式「ID」が「1」である「DBでエラー」を含むメッセージ群である。サービス起動メッセージ群については、実施例 1 と同様である。

【0067】

[抽出フェーズ]

まず、抽出処理部 4 0 は、エラーログに関連するログ抽出を行うために、ログメッセージの一覧からエラー周辺ログを抽出する。図 2 3 は、実施例 2 にかかるエラー周辺ログの抽出を説明する図である。ここでは、対象のエラーメッセージが 2 つ発生しており、1 番目のエラーの 6 0 分前から 2 番目のエラーの 6 0 分後までをエラー周辺ログとして抽出する。

【0068】

図 2 2 の例では、抽出処理部 4 0 は、「2/1 00:00:01」に 1 番目のエラーメッセージ 1 「DBでエラー」が発生しているので、「2/1 00:00:01」の 6 0 分前である「1/3 1 23:30:01」に発生した「XXXXX」をエラー周辺ログの開始とする。また、抽出処理部 4 0 は、「2/1 00:30:00」に 2 番目のエラーメッセージ 2 「DBでエラー」が発生しているので、「2/1 00:30:00」の 6 0 分後である「2/1 01:30:00」に発生した「YYYYY」をエラー周辺ログの最後とする。

【0069】

続いて、抽出処理部 4 0 は、学習フェーズにより分類されたメッセージ形式ごとに出現回数を計数し、エラー周辺用の観測データ行列を作成する。図 2 4 は、実施例 2 にかかるエラー周辺ログに対する観測データ行列を説明する図である。図 2 4 に示すように、抽出処理部 4 0 は、抽出されたエラー周辺ログを、学習処理部 3 0 で分類されたメッセージ形式 ID 「1」から「5」のそれぞれのメッセージに分類する。そして、抽出処理部 4 0 は、分類された各メッセージ形式の各時間帯の出現回数を、学習処理部 3 0 と同様の手法により集計する。実施例 1 とは異なり、時間帯「2/1 00:00:00~00:10:00」において、メッセージ形式 ID 「1」のメッセージ形式「DBでエラー」がカウントされている。このようにして、抽出処理部 4 0 は、エラー周辺ログから観測データ行列 Y ' を作成する。

【0070】

次に、抽出処理部 4 0 は、学習フェーズにて学習された基底行列 H_t を用いて、実施例 1 と同様の式 (1) により、観測データ行列 Y ' に含まれる頻出メッセージ群を抽出する。図 2 5 は、実施例 2 にかかる重み係数行列の算出結果の例を示す図である。ここで、抽出処理部 4 0 は、頻出メッセージ群のうちエラー周辺ログに含まれるものを表す重み係数行列 U ' を算出する。図 2 5 に示すように、重み係数行列 U ' は、実施例 2 においても実施例 1 と同様、バックアップメッセージ群について、時間帯「2/1 00:00:00~00:10:00」に「1」が設定されたとする。

【0071】

続いて、抽出処理部 4 0 は、式 (2) を用いて、観測データ行列 Y ' のうち基底行列 H_t の組み合わせで表現できないメッセージ群を、アノマリメッセージ行列として算出する。図 2 6 は、実施例 2 にかかるアノマリメッセージ群の抽出を説明する図である。図 2 6 に示すように、抽出処理部 4 0 は、学習フェーズで分類されたメッセージ形式 ID 「1」から「5」のそれぞれのメッセージに対する算出結果をアノマリメッセージ行列 A として算出する。そして、抽出処理部 4 0 は、行列の要素値が 0 より大きい「1」が設定される、「2/1 00:30:00 DBでエラー」と「2/1 00:30:00 A サービス起動」とを、アノマリメッセージ群として抽出する。

10

20

30

40

50

【0072】

その後、抽出処理部40は、エラーメッセージと関連する関連メッセージの判別を実行する。図27は、実施例2にかかるメッセージの判別例1を説明する図であり、図28は、実施例2にかかるメッセージの判別例2を説明する図である。

【0073】

具体的には、図27に示すように、抽出処理部40は、図23に示した対象のエラーメッセージ1「DBでエラー」の時間帯「2/1 00:00:01」と、重み係数行列U'とを比較し、エラーメッセージの発生時間を含む時間帯「2/1 00:00:00～ 00:10:00」に頻出メッセージ群である「バックアップメッセージ群」が出現しているので、関連メッセージ群を特定できると判別する。

10

【0074】

すなわち、抽出処理部40は、エラーメッセージ1「DBでエラー」の関連メッセージ群を「バックアップメッセージ群」と決定する。より詳細には、抽出処理部40は、「2/1 00:00:01」の対象エラーメッセージ1「DBでエラー」の関連メッセージ群として、図23のエラー周辺ログを参照し、「2/1 00:00:00」から「2/1 00:10:00」の間に出現したバックアップメッセージ群である、「2/1 00:00:05」のメッセージ「IP:192.168.0.1でバックアップを開始します」と「2/1 00:10:00」のメッセージ「IP:192.168.0.1でバックアップを完了しました」とを決定する。

【0075】

また、図28に示すように、抽出処理部40は、図23に示した対象のエラーメッセージ2「DBでエラー」の時間帯「2/1 00:30:00」と、重み係数行列U'とを比較し、エラーメッセージの発生時間を時間帯「2/1 00:30:00～00:40:00」に頻出メッセージ群が出現していないので、関連メッセージ群を特定できないと判別する。

20

【0076】

すなわち、抽出処理部40は、エラーメッセージ2「DBでエラー」の関連メッセージ群を「アノマリメッセージ群」と決定する。より詳細には、抽出処理部40は、図26で抽出したアノマリメッセージ群である「2/1 00:30:00」の「DBでエラー」と「2/1 00:30:00」の「Aサービス起動」のうち、対象エラー「DBでエラー」を除外した「2/1 00:30:00」の「Aサービス起動」のみを関連メッセージ群とする。

【0077】

そして、抽出処理部40は、各エラーメッセージに対する関連メッセージ群の判別結果を出力する。図29は、実施例2にかかる出力結果を説明する図である。図29に示すように、抽出処理部40は、「2/1 00:00:01」の対象エラーメッセージ1「DBでエラー」に対応付けて、関連メッセージ群として、「2/1 00:00:05, IP:192.168.0.1でバックアップを開始します」と「2/1 00:10:00, IP:192.168.0.1でバックアップを完了しました」とを出力する。同様に、抽出処理部40は、「2/1 00:30:00」の対象エラーメッセージ2「DBでエラー」に対応付けて、関連メッセージ群として、「2/1 00:30:00, Aサービス起動」を出力する。

30

【0078】

[効果]

上述したように、情報処理装置10は、図23に示した2つのエラーメッセージを含む全メッセージを、エラーメッセージ1を含む頻出メッセージ群と、エラーメッセージ2を含むアノマリメッセージ群とに分類することができる。したがって、情報処理装置10は、出現頻度の少ないエラーのエラーメッセージを含む多点障害発生時に、各エラーメッセージと関連する関連メッセージ群を特定して対応付けることができる。

40

【実施例3】

【0079】

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。

【0080】

50

〔数値等〕

上記実施例で用いた数値、メッセージ内容、時間幅などはあくまで一例であり、例示したものや図示したものに限定されず、任意に変更することができる。また、2つのエラーメッセージが発生した多点障害を例にして説明したが、これに限定されず、3つ以上の多点障害であっても同様に処理することができる。

【0081】

また、上記情報処理装置10は、課金システム、受発注システム、銀行系システムなど、様々なシステムのインシデント管理に適用することができる。また、上記実施例では、エラーメッセージが発生したタイミングで抽出フェーズを実行する例を説明したが、これに限定されるものではない。例えば、エラーメッセージが数回発生したタイミング、情報処理装置10がユーザ端末50からエラーメッセージを含む検索要求を受信したタイミングなどで実行することもできる。

【0082】

また、頻出メッセージ群の抽出やアノマリメッセージ行列の抽出は、式(1)や式(2)の手法に限らず、公知の手法を採用することができる。

【0083】

〔システム〕

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。

【0084】

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な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。例えば、学習処理部30と抽出処理部40とを別々の装置で実現することもできる。

【0085】

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。

【0086】

〔ハードウェア〕

図30は、ハードウェア構成例を説明する図である。図30に示すように、情報処理装置10は、通信装置10a、HDD(Hard Disk Drive)10b、メモリ10c、プロセッサ10dを有する。また、図30に示した各部は、バス等で相互に接続される。

【0087】

通信装置10aは、ネットワークインタフェースカードなどであり、他のサーバとの通信を行う。HDD10bは、図3に示した機能を動作させるプログラムやDBを記憶する。

【0088】

プロセッサ10dは、図3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HDD10b等から読み出してメモリ10cに展開することで、図3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、情報処理装置10が有する各処理部と同様の機能を実行する。具体的には、プロセッサ10dは、学習処理部30と抽出処理部40等と同様の機能を有するプログラムをHDD10b等から読み出す。そして、プロセッサ10dは、学習処理部30と抽出処理部40等と同様の処理を実行するプロセスを実行する。

【0089】

このように情報処理装置10は、プログラムを読み出して実行することでインシデント管理方法を実行する情報処理装置として動作する。また、情報処理装置10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

10

20

30

40

50

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、情報処理装置 10 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。

【符号の説明】

【0090】

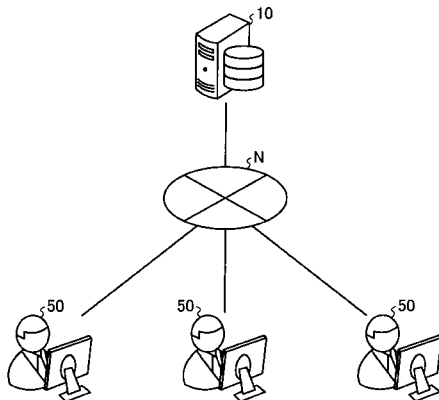
- 10 情報処理装置
- 11 通信部
- 12 記憶部
- 13 障害事例DB
- 20 制御部
- 30 学習処理部
- 31 分類部
- 32 作成部
- 33 学習部
- 40 抽出処理部
- 41 ログ抽出部
- 42 行列作成部
- 43 メッセージ抽出部
- 44 判別部
- 45 出力部

10

20

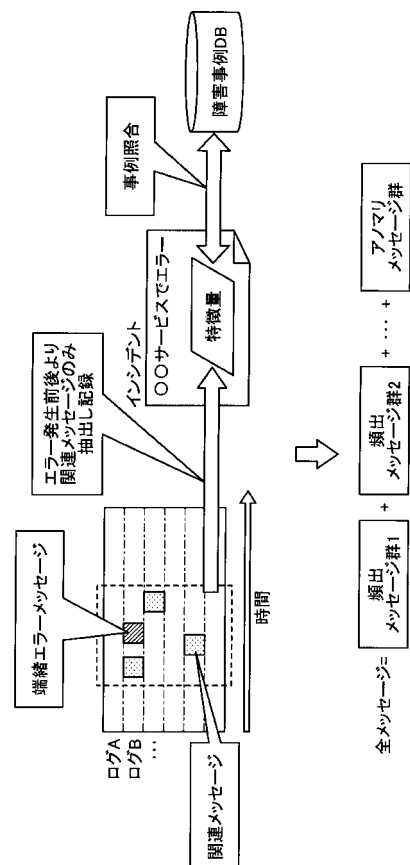
【図 1】

実施例 1 にかかるインシデント検索システムの全体構成を説明する図



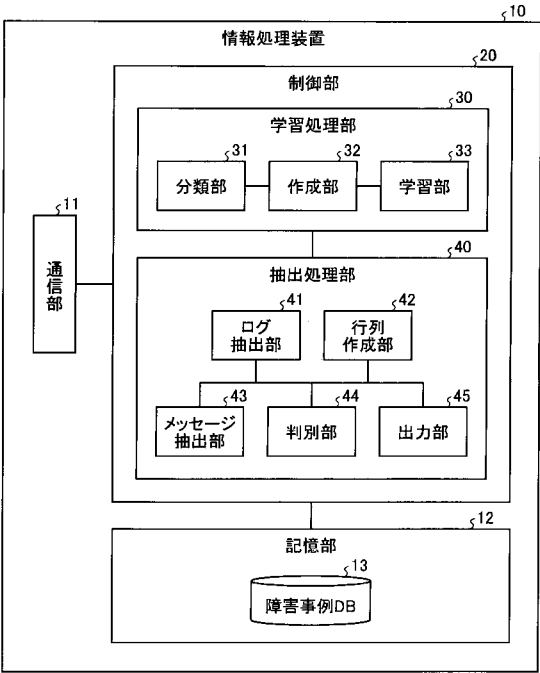
【図 2】

実施例 1 にかかる情報処理装置によるインシデント検索を説明する図



【図 3】

実施例1にかかる情報処理装置の機能構成を示す機能ブロック図



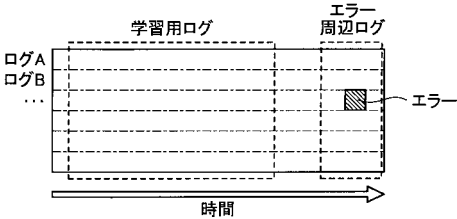
【図 4】

障害事例DBに記憶される情報の例を示す図

メッセージ群	対処方法
〇〇でエラー ××サービス停止	再起動後に××サービス起動
...	...

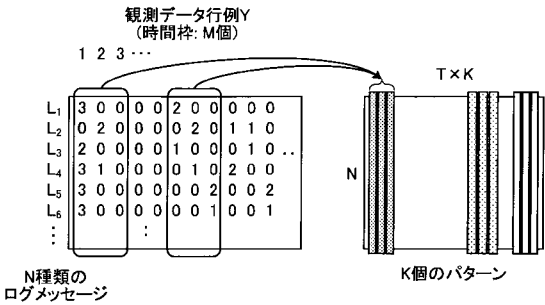
【図 5】

利用するログメッセージを説明する図



【図 6】

学習手法を説明する図



【図 7】

学習手法の定義一覧を示す図

記号の意味	
■	学習用ログの観測データ行列: Y
■	学習用ログの重み係数行列: U
■	エラー周辺ログの観測データ行列: Y'
■	エラー周辺ログの重み係数行列: U'
■	基底行列(頻出メッセージ群): $H_k \in \mathbb{R}^{N \times K}$
■	アノマリメッセージ行列: $A \in \mathbb{R}^{N \times M}$
■	頻出メッセージ群の最大数: K
■	メッセージ形式数: N
■	観測データ行列時間枠の幅: T_M
■	基底行列の時間幅: T
事前定義情報	
■	観測データ行列時間枠の幅: T_M
■	頻出メッセージ群の最大数: K
■	基底行列の時間幅: T

【図 8】

学習用ログの分類結果を示す図

学習用ログ		メッセージ形式ID
時刻	メッセージ	
	...	
1/1 00:00:05	IP:192.168.0.1でバックアップを開始します	2
1/1 00:10:00	IP:192.168.0.1でバックアップを完了しました	3
	...	
1/1 01:00:01	DBでエラー	1
1/1 01:00:05	IP:192.168.0.2でバックアップを開始します	2
1/1 01:10:00	IP:192.168.0.2でバックアップを完了しました	3
	...	
1/2 05:00:00	Aサービス起動	4
1/2 05:00:00	Bサービス起動	5
1/2 05:30:00	Aサービス起動	4
1/2 05:30:00	Bサービス起動	5
	...	

【図 9】

対象ログ:学習用ログ		観測データ行列の作成を説明する図									
メッセージ形式ID	メッセージ形式	観測データ行列Y									
1	DBでエラー	1/1 00:00:00	1/1 00:10:00	1/1 01:00:00	1/1 01:10:00	1/1 01:00:00	1/1 01:10:00	1/1 01:00:00	1/1 01:10:00	1/1 01:00:00	1/1 01:10:00
2	IP*でバックアップを開始します	0	0	0	0	0	0	0	0	0	0
3	IP*でバックアップを完了しました	1	0	0	1	0	1	0	0	0	0
4	Aサービス起動	0	0	0	0	0	0	0	0	1	1
5	Bサービス起動	0	0	0	0	0	0	0	0	1	1
...	...	...	...	...	...	...	...	...	...	...	...

【図 10】

頻出メッセージ群の学習結果を示す図

バックアップメッセージ群:			サービス起動メッセージ群:		
メッセージ形式ID			メッセージ形式ID		
1	0	0	1	0	0
2	1	0	2	0	0
3	0	1	3	0	0
4	0	0	4	1	0
5	0	0	5	1	0
...			...		

【図 11】

エラー周辺ログの抽出を説明する図

対象ログ:エラー周辺ログ	
時刻	メッセージ
	...
1/31 23:30:01	XXXXXX
2/1 00:00:05	IP:192.168.0.1でバックアップを開始します
2/1 00:10:00	IP:192.168.0.1でバックアップを完了しました
	...
2/1 00:30:00	DBでエラー
2/1 00:32:00	Aサービス起動
2/1 01:30:00	YYYYYY
	...

【図 1 2】

エラー周辺ログに対する観測データ行列を説明する図

対象ログ:エラー周辺ログ		観測データ行列Y'				
メッセージ形式ID	メッセージ形式	...	2/1 00:00:00	2/1 00:10:00	2/1 00:30:00	...
1	DBでエラー		0	0	1	
2	IP*でバックアップを開始します	...	1	0	0	...
3	IP*でバックアップを完了しました		0	1	0	
4	Aサービス起動		0	0	1	
5	Bサービス起動		0	0	0	
...						

【図 1 3】

重み係数行列の算出結果の例を示す図

対象ログ:エラー周辺ログ					
メッセージ群	2/1 00:00:00	2/1 00:10:00	...	2/1 00:30:00	...
バックアップメッセージ群	1	0		0	
サービス起動メッセージ群	0	0	...	0	...

重み係数行列U'

【図 1 4】

アノマリメッセージ群の抽出を説明する図

対象ログ:エラー周辺ログ		アノマリメッセージ行列A				
メッセージ形式ID	メッセージ形式	2/1 00:00:00	2/1 00:10:00	2/1 00:30:00	...	...
1	DBでエラー	0	0	1		
2	IP*でバックアップを開始します	0	0	0		
3	IP*でバックアップを完了しました	0	0	0		
4	Aサービス起動	0	0	1		
5	Bサービス起動	0	0	0		
...						

アノマリメッセージ群:

2/1 00:30:00「DBでエラー」
2/1 00:30:00「Aサービス起動」

【図 1 5】

メッセージの判別を説明する図

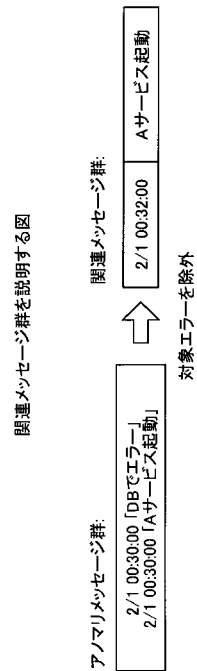
対象エラーメッセージ: 2/1 00:30:00 DBでエラー



重み係数行列U'

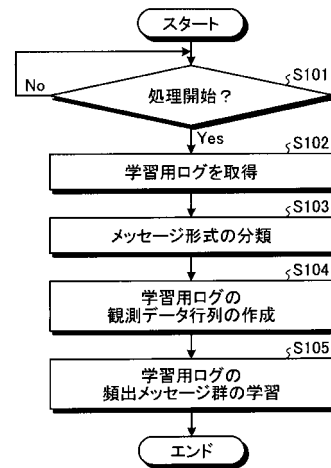
メッセージ群	2/1 00:00:00	2/1 00:10:00	...	2/1 00:30:00	...
バックアップメッセージ群	1	0		0	
サービス起動メッセージ群	0	0	...	0	...

【図 16】



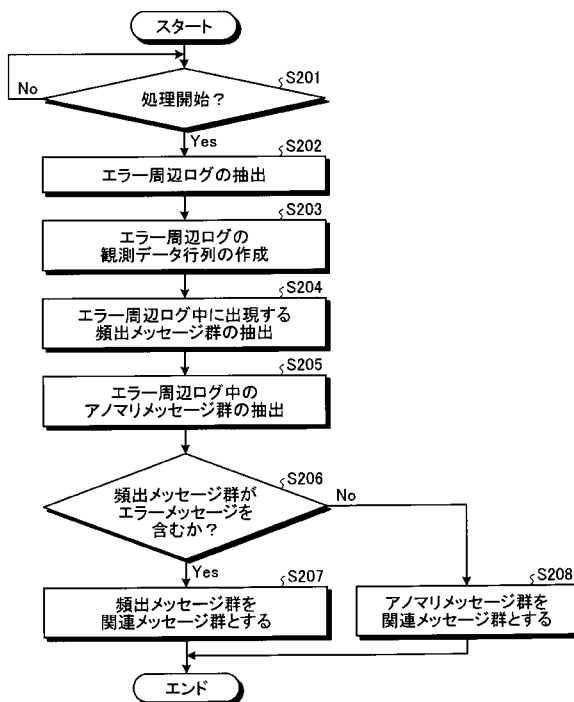
【図 17】

学習フェーズの処理の流れを示すフローチャート



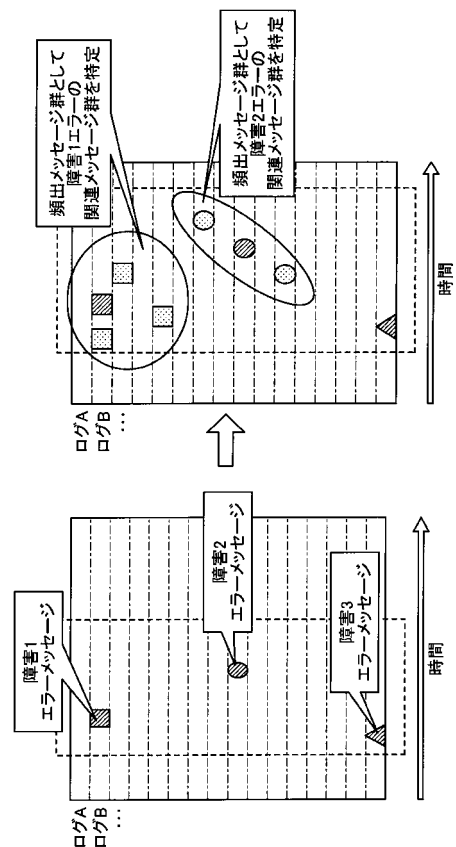
【図 18】

抽出フェーズの処理の流れを示すフローチャート



【図 19】

多点障害の問題点を説明する図



【図 20】

実施例2にかかる学習用ログの分類結果を示す図

対象ログ:学習用ログ		
学習用ログ		メッセージ形式ID
時刻	メッセージ	
	...	
1/1 00:00:01	DBでエラー	1
1/1 00:00:05	IP:192.168.0.1でバックアップを開始します	2
1/1 00:10:00	IP:192.168.0.1でバックアップを完了しました	3
	...	
1/1 01:00:01	DBでエラー	1
1/1 01:00:05	IP:192.168.0.2でバックアップを開始します	2
1/1 01:10:00	IP:192.168.0.2でバックアップを完了しました	3
	...	
1/2 05:00:00	Aサービス起動	4
1/2 05:00:00	Bサービス起動	5
1/2 05:30:00	Aサービス起動	4
1/2 05:30:00	Bサービス起動	5
	...	

【図 21】

実施例2にかかる観測データ行列の作成を説明する図

対象ログ:学習用ログ		1/1 00:00:00~00:10:00における出現回数											
メッセージ形式ID	メッセージ形式	1/1 00:00:00	1/1 00:10:00	...	1/1 01:00:00	1/1 01:10:00	1/1 01:00:00	1/1 01:10:00	...	1/1 05:00:00	1/1 05:30:00	...	1/1 05:30:00
1	DBでエラー	1	0	0	1	0	1	0	0	0	0	0	0
2	IP*でバックアップを開始します	1	0	...	1	0	...	0	...	0	0	...	0
3	IP*でバックアップを完了しました	0	1	0	0	1	0	0	0	0	0	0	0
4	Aサービス起動	0	0	0	0	0	0	0	0	1	1	0	1
5	Bサービス起動	0	0	0	0	0	0	0	0	1	1	0	1
...													

【図 22】

実施例2にかかる頻出メッセージ群の学習結果を説明する図

バックアップメッセージ群:			サービス起動メッセージ群:		
メッセージ形式ID			メッセージ形式ID		
1	1	0	1	0	0
2	1	0	2	0	0
3	0	1	3	0	0
4	0	0	4	1	0
5	0	0	5	1	0
...			...		

【図 23】

実施例2にかかるエラー周辺ログの抽出を説明する図

対象ログ:エラー周辺ログ	
時刻	メッセージ
	...
1/31 23:00:01	XXXXXX
2/1 00:00:01	DBでエラー
2/1 00:00:05	IP:192.168.0.1でバックアップを開始します
2/1 00:10:00	IP:192.168.0.1でバックアップを完了しました
	...
2/1 00:30:00	DBでエラー
2/1 00:32:00	Aサービス起動
2/1 01:30:00	YYYYYY
	...

【図 2 8】

実施例2にかかるメッセージの判別例2を説明する図

対象エラーメッセージ2: 2/1 00:30:00 DBでエラー

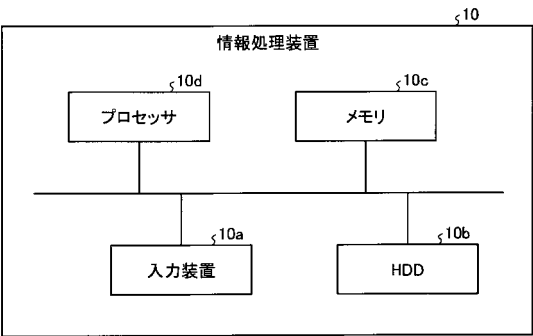
重み係数行列U'

メッセージ群	2/1 00:00:00	2/1 00:10:00	...	2/1 00:30:00	...
バックアップ メッセージ群	1	0		0	
サービス起動 メッセージ群	0	0	...	0	...

頻出メッセージ群の出現なし

【図 3 0】

ハードウェア構成例を説明する図



【図 2 9】

実施例2にかかる出力結果を説明する図

■出力結果

■対象エラーメッセージ1: 2/1 00:00:01 DBでエラー

関連メッセージ群

2/1 00:00:05	IP:192.168.0.1でバックアップを開始します
2/1 00:10:00	IP:192.168.0.1でバックアップを完了しました

■対象エラーメッセージ2: 2/1 00:30:00 DBでエラー

関連メッセージ群

2/1 00:32:00	Aサービス起動
--------------	---------

フロントページの続き

Fターム(参考) 5B042 MA08 MA10 MA11 MA14 MC23 MC35 MC40