(19)日本国特許庁(JP)

# (12)特許公報(B2)

(11)特許番号
特許第7207009号
(P7207009)

(45)発行日　令和5年1月18日(2023.1.18)

(24)登録日　令和5年1月10日(2023.1.10)

| (51)国際特許分類 | | | FI | | |
|---|---|---|---|---|---|
| *G06F* | *11/07* | *(2006.01)* | G06F | 11/07 | 160 |
| *G06F* | *16/35* | *(2019.01)* | G06F | 11/07 | 140A |
| *H04L* | *67/00* | *(2022.01)* | G06F | 16/35 | |
| | | | H04L | 67/00 | |

請求項の数　6　（全15頁）

(21)出願番号　特願2019-33254(P2019-33254)
(22)出願日　平成31年2月26日(2019.2.26)
(65)公開番号　特開2020-140250(P2020-140250A)
(43)公開日　令和2年9月3日(2020.9.3)
審査請求日　令和3年5月31日(2021.5.31)

(73)特許権者　000004226
日本電信電話株式会社
東京都千代田区大手町一丁目５番１号
(74)代理人　110002147
弁理士法人酒井国際特許事務所
(72)発明者　東羅 翔太郎
東京都千代田区大手町一丁目５番１号
日本電信電話株式会社内
(72)発明者　外山 将司
東京都千代田区大手町一丁目５番１号
日本電信電話株式会社内
(72)発明者　豊田 真智子
東京都千代田区大手町一丁目５番１号
日本電信電話株式会社内
審査官　甲斐 哲雄

最終頁に続く

(54)【発明の名称】　異常検知装置、異常検知方法および異常検知プログラム

(57)【特許請求の範囲】

【請求項１】

システムから出力されたテキストログに含まれる各メッセージの種別を表す各メッセージの部分文字列と、メッセージの種別ごとに設定されたＩＤとが対応付けられた辞書情報を記憶する記憶部と、

前記システムから出力されたテキストログに含まれるメッセージを取得すると、前記記憶部に記憶された辞書情報を参照し、前記テキストログに含まれるメッセージを種別ごとに分類し、分類した各メッセージにＩＤを付与する分類部と、

前記分類部によってメッセージに付与されたＩＤに基づいて、異常を検知する検知部とを有し、

前記分類部は、分類されたメッセージのうち、前記記憶部の辞書情報の中に該当するメッセージの種別が存在しなかったメッセージには、新規ＩＤを付与するとともに、当該新規ＩＤおよび当該メッセージを基に前記辞書情報を前記記憶部に追加し、

前記検知部は、前記分類部によって分類されたメッセージのうち、前記記憶部の辞書情報の中に該当するメッセージの種別が存在しなかったメッセージの種別の件数が所定の閾値を超えている場合には、異常を検知することを特徴とする異常検知装置。

【請求項２】

前記検知部は、前記分類部によって前記メッセージが分類された結果から、前記メッセージに付与されたＩＤの単位時間あたりの頻度をＩＤごとに集計し、任意の単位時間の頻度と他の単位時間の頻度とを比較し、各単位時間のＩＤごとの異常度を検知することを特

徴とする請求項１に記載の異常検知装置。
【請求項３】
前記分類部は、前記メッセージを所定の区切り文字で分割して単語群を抽出し、各単語を文字種によってパラメータまたは非パラメータに分類し、前記記憶部に記憶された辞書情報の種別群の中で、非パラメータと分類された箇所の単語が一致する種別が存在する場合には、該種別に対応するＩＤを前記メッセージに付与し、非パラメータと分類された箇所の単語が一致する種別が存在しない場合には、前記メッセージに新規ＩＤを付与することを特徴とする請求項１または２に記載の異常検知装置。
【請求項４】
前記分類部によって付与されたＩＤを含むメッセージに関する情報を通知する通知部をさらに有することを特徴とする請求項１～３のいずれか一つに記載の異常検知装置。
【請求項５】
異常検知装置によって実行される異常検知方法であって、
前記異常検知装置は、システムから出力されたテキストログに含まれる各メッセージの種別を表す各メッセージの部分文字列と、メッセージの種別ごとに設定されたＩＤとが対応付けられた辞書情報を記憶する記憶部を有し、
前記システムから出力されたテキストログに含まれるメッセージを取得すると、前記記憶部に記憶された辞書情報を参照し、前記テキストログに含まれるメッセージを種別ごとに分類し、分類した各メッセージにＩＤを付与する分類工程と、
前記分類工程によってメッセージに付与されたＩＤに基づいて、異常を検知する検知工程と
を含み、
前記分類工程は、分類されたメッセージのうち、前記記憶部の辞書情報の中に該当するメッセージの種別が存在しなかったメッセージには、新規ＩＤを付与するとともに、当該新規ＩＤおよび当該メッセージを基に前記辞書情報を前記記憶部に追加し、
前記検知工程は、前記分類工程によって分類されたメッセージのうち、前記記憶部の辞書情報の中に該当するメッセージの種別が存在しなかったメッセージの種別の件数が所定の閾値を超えている場合には、異常を検知することを特徴とする異常検知方法。
【請求項６】
システムから出力されたテキストログに含まれるメッセージを取得すると、前記システムから出力されたテキストログに含まれる各メッセージの種別を表す各メッセージの部分文字列とメッセージの種別ごとに設定されたＩＤとが対応付けられた辞書情報を記憶する記憶部に記憶された前記辞書情報を参照し、前記テキストログに含まれるメッセージを種別ごとに分類し、分類した各メッセージにＩＤを付与する分類ステップと、
前記分類ステップによってメッセージに付与されたＩＤに基づいて、異常を検知する検知ステップと
をコンピュータに実行させ、
前記分類ステップは、分類されたメッセージのうち、前記記憶部の辞書情報の中に該当するメッセージの種別が存在しなかったメッセージには、新規ＩＤを付与するとともに、当該新規ＩＤおよび当該メッセージを基に前記辞書情報を前記記憶部に追加し、
前記検知ステップは、前記分類ステップによって分類されたメッセージのうち、前記記憶部の辞書情報の中に該当するメッセージの種別が存在しなかったメッセージの種別の件数が所定の閾値を超えている場合には、異常を検知することを特徴とする異常検知プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、異常検知装置、異常検知方法および異常検知プログラムに関する。
【背景技術】
【０００２】

従来、サーバシステムやネットワークシステムにおける異常検知や状態分析のために、ｓｙｓｌｏｇやＭＩＢ（Management Information Base）情報等のテキストログを用いたシステムの監視が行われている。

【０００３】

例えば、システムに障害が発生した際に、人手によって特定のキーワードでテキストログを検索し、当該キーワードを含んだメッセージをクリティカルなメッセージとして抽出することが行われている。

【先行技術文献】

【特許文献】

【０００４】

【文献】特開２０１４－１５３７２３号公報
特開２０１５－３６８９１号公報

【発明の概要】

【発明が解決しようとする課題】

【０００５】

しかしながら、従来のブラックリストによる監視では、既知の異常を検知することはできても、未知の異常を検知することはできないという課題があった。

【課題を解決するための手段】

【０００６】

上述した課題を解決し、目的を達成するために、本発明の異常検知装置は、システムから出力されたテキストログに含まれる各メッセージの種別を表す各メッセージの部分文字列と、メッセージの種別ごとに設定されたＩＤとが対応付けられた辞書情報を記憶する記憶部と、前記システムから出力されたテキストログに含まれるメッセージを取得すると、前記記憶部に記憶された辞書情報を参照し、前記テキストログに含まれるメッセージを種別ごとに分類し、分類した各メッセージにＩＤを付与する分類部と、前記分類部によってメッセージに付与されたＩＤに基づいて、異常を検知する検知部とを有することを特徴とする。

【０００７】

また、本発明の異常検知方法は、異常検知装置によって実行される異常検知方法であって、前記異常検知装置は、システムから出力されたテキストログに含まれる各メッセージの種別を表す各メッセージの部分文字列と、メッセージの種別ごとに設定されたＩＤとが対応付けられた辞書情報を記憶する記憶部を有し、前記システムから出力されたテキストログに含まれるメッセージを取得すると、前記記憶部に記憶された辞書情報を参照し、前記テキストログに含まれるメッセージを種別ごとに分類し、分類した各メッセージにＩＤを付与する分類工程と、前記分類工程によってメッセージに付与されたＩＤに基づいて、異常を検知する検知工程とを含むことを特徴とする。

【０００８】

また、本発明の異常検知プログラムは、システムから出力されたテキストログに含まれるメッセージを取得すると、前記システムから出力されたテキストログに含まれる各メッセージの種別を表す各メッセージの部分文字列とメッセージの種別ごとに設定されたＩＤとが対応付けられた辞書情報を記憶する記憶部に記憶された前記辞書情報を参照し、前記テキストログに含まれるメッセージを種別ごとに分類し、分類した各メッセージにＩＤを付与する分類ステップと、前記分類ステップによってメッセージに付与されたＩＤに基づいて、異常を検知する検知ステップとをコンピュータに実行させることを特徴とする。

【発明の効果】

【０００９】

本発明によれば、未知の異常を検知することができるという効果を奏する。

【図面の簡単な説明】

【００１０】

【図１】図１は、第１の実施形態に係る異常検知装置の構成例を示すブロック図である。

【図２】図２は、テキストログの一例を示す図である。
【図３】図３は、辞書情報のデータ構成の一例を示す図である。
【図４】図４は、テンプレートの作成について説明するための図である。
【図５】図５は、ＩＤ付与処理を説明する図である。
【図６】図６は、ログを集約してＩＤを付与する一連の流れの一例を説明する図である。
【図７】図７は、システムが安定して運用されている場合の新規テンプレート数の推移を示す図である。
【図８】図８は、未知の事象が発生している場合の新規テンプレート数の推移を示す図である。
【図９】図９は、単位時間当たりの新規テンプレート数を監視することで未知異常を発見する一連の処理の流れを説明する図である。
【図１０】図１０は、ＩＤごとの出現頻度の相対的な変化から異常度を算出する処理を説明する図である。
【図１１】図１１は、第１の実施形態に係る異常検知装置における処理の流れの一例を示すフローチャートである。
【図１２】図１２は、異常検知プログラムを実行するコンピュータを示す図である。
【発明を実施するための形態】
【００１１】
以下に、本願に係る異常検知装置、異常検知方法および異常検知プログラムの実施の形態を図面に基づいて詳細に説明する。なお、この実施の形態により本願に係る異常検知装置、異常検知方法および異常検知プログラムが限定されるものではない。
【００１２】
［第１の実施形態］
以下の実施の形態では、第１の実施形態に係る異常検知装置１０の構成、異常検知装置１０の処理の流れを順に説明し、最後に第１の実施形態による効果を説明する。
【００１３】
［異常検知装置の構成］
まず、図１を用いて、本実施形態の異常検知装置１０の構成例を説明する。図１は、第１の実施形態に係る異常検知装置の構成例を示すブロック図である。図１に示すように、異常検知装置１０は、入力部１１、出力部１２、通信部１３、記憶部１４及び制御部１５を有する。
【００１４】
入力部１１は、ユーザからのデータの入力を受け付ける。入力部１１は、例えば、マウスやキーボード等の入力装置である。出力部１２は、画面の表示等により、データを出力する。出力部１２は、例えば、ディスプレイ等の表示装置である。通信部１３は、ネットワークを介して、他の装置との間でデータ通信を行う。例えば、通信部１３はＮＩＣ（Network Interface Card）である。
【００１５】
記憶部１４は、ＨＤＤ（Hard Disk Drive）、ＳＳＤ（Solid State Drive）、光ディスク等の記憶装置である。なお、記憶部１４は、ＲＡＭ（Random Access Memory）、フラッシュメモリ、ＮＶＳＲＡＭ（Non Volatile Static Random Access Memory）等のデータを書き換え可能な半導体メモリであってもよい。記憶部１４は、異常検知装置１０で実行されるＯＳ（Operating System）や各種プログラムを記憶する。さらに、記憶部１４は、プログラムの実行で用いられる各種情報を記憶する。
【００１６】
また、記憶部１４は、出力ログ情報１４１及び辞書情報１４２を記憶する。記憶部１４は、システムから出力されたテキストログに含まれる各メッセージの種別を表す各メッセージの部分文字列と、メッセージの種別ごとに設定されたＩＤとが対応付けられた辞書情報１４２を記憶する。
【００１７】

記憶部１４は、システムから出力されたテキストログを出力ログ情報１４ａとして記憶する。ここで、テキストログは、例えば、計算機システムを構成するサーバマシン、パーソナルコンピュータ、ストレージ等から出力される。また、テキストログは、例えば、ネットワークシステムを構成するルータ、ファイアウォール、ロードバランサ、光伝送装置、光伝送中継器等から出力される。また、出力されるテキストログは、システム全体に関するものであってもよいし、システムを構成する装置に関するものであってもよい。さらに、テキストログは、計算機システムやネットワークシステムが仮想化された環境において出力されたものであってもよい。

【００１８】

テキストログは、例えば、ＯＳのシスログ、アプリケーション及びデータベースの実行ログ、エラーログ、操作ログ、ネットワーク機器から得られるＭＩＢ情報、監視システムのアラート、行動ログ、動作状態ログ等である。なお、テキストログは上記のものに限定されるものではなく、どのようなものであってもよい。

【００１９】

図２は、テキストログの一例を示す図である。図２に示すように、テキストログの各レコードは、メッセージとメッセージに付された発生日時とを含む。例えば、テキストログの１行目のレコードは、メッセージ「LINK-UP Interface 1/0/17」と、発生日時「2015/05/18T14:56」とを含む。なお、メッセージには、ホストやログレベルといった付加情報を含んでも構わない。

【００２０】

記憶部１４は、テキストログのメッセージを分類するためのデータを辞書情報１４ｂとして記憶する。図３は、辞書情報のデータ構成の一例を示す図である。図３に示すように、辞書情報１４ｂは、ＩＤ及び単語シーケンスで構成されるテンプレートを含む。つまり、テンプレートは、テンプレートＩＤ、単語シーケンスから構成される。ＩＤは、テキストログのメッセージが分類される種別を識別するための情報である。単語シーケンスは、テキストログのメッセージの分類に用いられる文字列である。例えば、ＩＤが「１」である種別にメッセージが分類されるか否かは、単語シーケンス「LINK-UP Interface *」を用いて判定される。なお、辞書情報１４ｂを用いたメッセージの分類は分類部１５ａによって行われる。分類部１５ａの具体的な処理については後述する。

【００２１】

制御部１５は、異常検知装置１０全体を制御する。制御部１５は、例えば、ＣＰＵ（Central Processing Unit）、ＭＰＵ（Micro Processing Unit）等の電子回路や、ＡＳＩＣ（Application Specific Integrated Circuit）、ＦＰＧＡ（Field Programmable Gate Array）等の集積回路である。また、制御部１５は、各種の処理手順を規定したプログラムや制御データを格納するための内部メモリを有し、内部メモリを用いて各処理を実行する。また、制御部１５は、各種のプログラムが動作することにより各種の処理部として機能する。例えば、制御部１５は、分類部１５ａ、検知部１５ｂおよび通知部１５ｃを有する。

【００２２】

分類部１５ａは、システムから出力されたテキストログに含まれるメッセージを取得すると、記憶部１４に記憶された辞書情報を参照し、テキストログに含まれるメッセージを種別ごとに分類し、分類した各メッセージにＩＤを付与する。前述の通り、分類部１５ａは、辞書情報１４ｂを用いて分類を行う。

【００２３】

ここで、辞書情報１４ｂは、分類部１５ａによって作成されてもよい。例えば、分類部１５ａは、メッセージからパラメータを削除することで得られる文字列を基にテンプレートを作成することができる。ここで、図４を用いて、テキストログに基づいたテンプレートの作成方法について説明する。図４は、テンプレートの作成について説明するための図である。テンプレートは、テンプレートＩＤ、単語シーケンスから構成される。

【００２４】

分類部１５ａは、メッセージを所定の区切り文字で分割して単語群を抽出し、各単語を文字種によってパラメータまたは非パラメータに分類し、記憶部１４に記憶された辞書情報のテンプレート群のそれぞれの単語シーケンスと比較し、上記メッセージ中の非パラメータと分類された箇所の単語がすべて一致するテンプレートが存在する場合には、該テンプレートのＩＤをメッセージに付与する。

【００２５】

また、分類部１５ａは、メッセージの分類を行う際に、記憶部１４に記憶された辞書情報のテンプレート群の中に、非パラメータと分類された箇所の単語がすべて一致する単語シーケンスを持つテンプレートが存在しない場合には、当該メッセージを基にした単語シーケンスを持つ新たなテンプレートを作成し、新規ＩＤを付与した新しいテンプレートを生成しても良い。

【００２６】

図４に示すように、分類部１５ａは、例えば、「数値と記号」で構成される単語をパラメータとみなし、メッセージからパラメータを削除した文字列を単語シーケンスとすることができる。この場合、分類部１５ａは、図２のテキストログに含まれるメッセージ「LINK-UP Interface 1/0/17」、又はメッセージ「LINK-UP Interface 0/0/0」から、「LINK-UP Interface」という単語シーケンスを作成する。さらに、分類部１５ａは、作成した単語シーケンスとＩＤとを持つテンプレートとして生成し、記憶部１４の辞書情報１４ｂに追加する。このとき、分類部１５ａは、パラメータを削除した部分に「*」等のワイルドカードを追加してもよい。

【００２７】

なお、分類部１５ａがパラメータとみなす単語は上記の例に限られない。分類部１５ａは、例えば、「数字を含む単語」を全てパラメータとみなしてもよいし、「数字とアルファベットで構成される単語」は非パラメータとみなしてもよいし、「アルファベットのみで構成される単語」だけを非パラメータとしてもよい。

【００２８】

また、パラメータ／非パラメータの判断基準は文字種に限らずルールベースで作成しても良い。具体的には、「IPアドレスのルールに従う単語」をパラメータとみなしてもよい。さらに、単語の枠を超えて、前記「所定の区切り文字」を含む文字列についてパラメータ／非パラメータと判定しても良い。

【００２９】

また、本実施形態において、辞書情報１４ｂのテンプレートは、分類部１５ａによって作成されたものである必要はなく、あらかじめユーザにより作成されたものや、異常検知装置１０以外の装置によって自動的に作成されたものであってもよい。

【００３０】

ここで、図５を用いて、分類部１５ａによるＩＤ付与処理を説明する。図５はG、ＩＤ付与処理を説明する図である。分類部１５ａは、辞書情報１４ｂ中の各テンプレートの単語シーケンスとテキストログのメッセージと比較することにより、メッセージの分類を行う。このとき、分類部１５ａは、単語シーケンスがメッセージに完全一致する場合、又は、部分一致する場合に、テンプレートがメッセージに一致すると判定する。そして、分類部１５ａは、メッセージに対し、一致すると判定されたテンプレートのＩＤを付与する。

【００３１】

例えば、図３のＩＤが「１」であるテンプレートの単語シーケンス「LINK-UP Interface *」が、図２のテキストログの１行目のメッセージ「LINK-UP Interface 1/0/17」に部分一致するため、分類部１５ａはテンプレートの単語シーケンス「LINK-UP Interface *」がメッセージ「LINK-UP Interface 1/0/17」に一致すると判定し、メッセージ「LINK-UP Interface 1/0/17」にＩＤ「１」を付与する。

【００３２】

また、分類部１５ａは、メッセージに一致する単語シーケンスを持つテンプレートが辞書情報１４ｂに存在しない場合には、まだ付与されていない新規ＩＤを付与するとともに

、メッセージをもとに新たなテンプレートを辞書情報１４ｂに追加する。
【００３３】
分類部１５ａは、メッセージの分類及びＩＤの付与を行うことで、分類済みテキストログを作成する。図２に示すように、分類済みテキストログの各レコードは、メッセージのＩＤ及び発生日時を含む。例えば、分類済みテキストログの１行目のレコードは、メッセージ「LINK-UP Interface 1/0/17」に付与されたＩＤ「１」と、発生日時「2015/05/18T14:56」とを含む。
【００３４】
次に、図６を用いて、ログを集約してＩＤを付与する一連の流れの一例を説明する。図６は、ログを集約してＩＤを付与する一連の流れの一例を説明する図である。図６に例示するように、分類部１５ａは、ファイルログやリアルタイムログ等のフォーマットの異なる種々のログをそれぞれの形式に従ってフォーマット変換する。ここで、例えば、分類部１５ａは、リアルタイムログについて、時刻の入れ替わりを防ぐため、ログを受け取った時刻を付与した後に、フォーマットを変換する。フォーマット変換済みログメッセージは、日時やメッセージ本文、その他の情報を含むものとする。
【００３５】
そして、分類部１５ａは、辞書情報のテンプレートを参照してメッセージにＩＤを付与し、ＩＤ化されたログメッセージを出力する。また、分類部１５ａは、新規のＩＤを付与した場合には、新しいテンプレートを追加するように辞書情報を更新する。
【００３６】
図１の説明に戻って、検知部１５ｂは、分類部１５ａによってメッセージに付与されたＩＤに基づいて、異常を検知する。例えば、検知部１５ｂは、分類部１５ａによって分類されたメッセージのうち、記憶部１４の辞書情報の中に該当するメッセージの種別が存在しなかったメッセージの種別の件数が所定の閾値を超えている場合には、異常を検知する。
【００３７】
ここで、図７および図８を用いて、新規テンプレート数の推移について説明する。図７は、システムが安定して運用されている場合の新規テンプレート数の推移を示す図である。図８は、未知の事象が発生している場合の新規テンプレート数の推移を示す図である。図７に例示するように、システムが安定して運用されていれば、初期段階においてある程度の期間は未知のログが出現するが、未知のログの出現頻度は減少していく。そして、図８に例示するように、システムにおいて障害やメンテナンス等の未知の事象が発生している場合には、所定の期間において未知のログが大量に出現する。
【００３８】
検知部１５ｂは、このような未知の事象が発生していることを検知するため、所定の期間における新規ＩＤの付与数が所定の閾値を超えるか判定する。例えば、図８の例では、検知部１５ｂは、１日ごとの新規ＩＤの付与数を計数し、１日の新規ＩＤの付与数が閾値２５０を超えているかを監視する。そして、検知部１５ｂは、１日の新規ＩＤの付与数が閾値「２５０」を超えている場合に、異常を検知する。なお、閾値は、任意に設定変更可能であるものとする。
【００３９】
図１の説明に戻って、通知部１５ｃは、分類部１５ａによって付与されたＩＤを含むメッセージに関する情報を通知する。例えば、通知部１５ｃは、新規ＩＤリストを外部の端末装置に通知するようにしてもよい。また、例えば、通知部１５ｃは、検知部１５ｂによって異常が検知された場合には、外部の端末装置にアラートを通知するようにしてもよい。また、例えば、通知部１５ｃは、外部の端末装置からの要求に応じて、辞書情報やＩＤのヒートマップを表示するようにしてもよい。
【００４０】
ここで、図９を用いて、単位時間当たりの新規ＩＤ付与数を監視することで未知異常を発見する一連の処理の流れを説明する。図９は、単位時間当たりの新規ＩＤ付与数を監視することで未知異常を発見する一連の処理の流れを説明する図である。図９に例示するよ

うに、異常検知装置１０は、異常が発生したシステムから出力された新規ログについて、記憶部１４に記憶された辞書情報１４ｂを参照し、辞書情報に登録されていないテキストログのメッセージには新規ＩＤを付与する。そして、異常検知装置１０は、新規ＩＤリストを外部の端末装置に通知する。

【００４１】

また、異常検知装置１０では、時刻毎の新規ＩＤ数と辞書を常時可視化できるようにし、何かあったときに迅速に原因特定し、新たな監視項目にすることができる。また、異常検知装置１０は、所定の期間における新規ＩＤ数が所定の閾値を超えたときにはアラートを外部の端末装置に通知する。このように、異常検知装置１０では、単位時間あたりの新規ＩＤ付与数を監視することで未知異常を早期に発見することができ、ユーザ申告前のトラブル対処を行うことができる。

【００４２】

つまり、正常時のログが辞書情報１４ｂに登録されていれば異常時のログは新規ＩＤが付与されるという前提のもと、異常検知装置１０は、辞書情報にないログには新規ＩＤを付与し、新規ＩＤの増加数から未知の異常を検知することが可能である。

【００４３】

また、異常検知装置１０では、端末装置からの要求に応じて、辞書ビューアやＩＤのヒートマップを表示するようにしてもよく、辞書ビューアやログヒートマップとして可視化することで、迅速に内容を確認することが可能である。

【００４４】

また、上記の説明では、異常検知装置１０の検知部１５ｂが、所定の期間における新規ＩＤ数が所定の閾値を超えたときに異常を検知する場合を説明したが、これに限定されるものではない。例えば、検知部１５ｂは、分類部１５ａによってメッセージが分類された結果から、メッセージに付与されたＩＤの単位時間（例えば、１日）あたりの付与回数をＩＤごとに集計し、任意の単位時間の付与回数と他の単位時間の付与回数とを比較し、各単位時間のＩＤごとの異常度を検知するようにしてもよい。

【００４５】

ここで、図１０を用いて、ＩＤごとの出現頻度の相対的な変化から異常度を算出する処理について説明する。図１０は、ＩＤごとの出現頻度の相対的な変化から異常度を算出する処理を説明する図である。例えば、検知部１５ｂは、毎日、１日ごとの集計値を過去５日分算出し、ＴＦ－ＩＤＦ値を計算すると、直近５日間と比べて１日あたりの頻度が多いＩＤを見付けることができる。図１０の左側においては、「１」～「７」のＩＤについて、５日間（４日前、３日前、２日前、昨日、今日）における１日ごとの付与数の和がそれぞれ表示されている。

【００４６】

例えば、検知部１５ｂは、図１０に例示する式を用いて、各ＩＤの１日ごとのＴＦ－ＩＤＦ値を計算する。具体例を挙げて説明すると、検知部１５ｂは、例えば、ＩＤ「４」の「昨日」について、「５×ｌｏｇ$_{10}$（５／１）」を計算し、ＴＦ－ＩＤＦ値として約「３．５」となる。

【００４７】

そして、検知部１５ｂは、計算したＴＦ－ＩＤＦ値を異常度とし、異常度が所定の閾値（例えば、０．７）以上であるＩＤが存在する場合には、異常を検知するようにしてもよい。

【００４８】

［異常検知装置の処理手順］

次に、図１１を用いて、第１の実施形態に係る異常検知装置１０による処理手順の例を説明する。図１１は、第１の実施形態に係る異常検知装置における処理の流れの一例を示すシーケンス図である。なお、図１１の例では、新規ＩＤが付与されるたびに、新規ＩＤリストを通知し、異常を検知する場合の処理例を説明するが、新規ＩＤリストを通知する処理や異常を検知する処理を行うタイミングはこれに限定されるものではなく、どのよう

なタイミングであってもよい。

【００４９】

図１１に例示するように、異常検知装置１０の分類部１５ａは、ログメッセージを受け付けると（ステップＳ１０１肯定）、メッセージを所定の区切り文字で分割して単語群を抽出する（ステップＳ１０２）。そして、分割部１５ａは、各単語を文字種によってパラメータまたは非パラメータに分類し、記憶部１４に記憶された辞書情報のテンプレート群のそれぞれの単語シーケンスと比較し、上記メッセージ中の非パラメータと分類された箇所の単語がすべて一致するテンプレートが存在する場合には、該テンプレートのＩＤをメッセージに付与する（ステップＳ１０３）。

【００５０】

そして、分類部１５ａは、ステップＳ１０３において新規ＩＤを付与したか判定する（ステップＳ１０４）。この結果、分類部１５ａは、新規ＩＤを付与したと判定しなかった場合には（ステップＳ１０４否定）、そのまま処理を終了する。また、分類部１５ａは、新規ＩＤを付与したと判定した場合には（ステップＳ１０４肯定）、記憶部１４の辞書情報１４ｂに新しいテンプレートを追加する（ステップＳ１０５）。

【００５１】

続いて、通知部１５ｃは、新規ＩＤリストを通知する（ステップＳ１０６）。そして、検知部１５ｂは、単位時間あたりの新規テンプレート数が閾値を超えるか判定する（ステップＳ１０７）。この結果、検知部１５ｂは、単位時間あたりの新規テンプレート数が所定数を超えていない場合には（ステップＳ１０７否定）、そのまま処理を終了する。また、検知部１５ｂは、単位時間あたりの新規テンプレート数が超えている場合には（ステップＳ１０７肯定）、異常を検知する（ステップＳ１０８）。

【００５２】

［第１の実施形態の効果］

第１の実施形態に係る異常検知装置１０は、過去にシステムから出力されたテキストログに含まれるメッセージと、メッセージの種別ごとに設定されたＩＤとが対応付けられた辞書情報１４ｂを記憶する記憶部１４を有する。異常検知装置１０は、システムから出力されたテキストログに含まれるメッセージを取得すると、記憶部１４に記憶された辞書情報１４ｂを参照し、テキストログに含まれるメッセージを種別ごとに分類し、分類した各メッセージにＩＤを付与し、メッセージに付与されたＩＤに基づいて、異常を検知する。このため、異常検知装置１０では、未知の異常を検知することが可能である。

【００５３】

また、第１の実施形態に係る異常検知装置１０は、メッセージに付与されたＩＤのうち、所定の期間における新規ＩＤの付与数が所定の閾値を超えている場合には、異常を検知するので、単位時間あたりの新規ＩＤ付与数を監視することで未知異常を早期に検知することが可能である。

【００５４】

また、第１の実施形態に係る異常検知装置１０は、ＩＤを含むメッセージに関する情報を通知することで、例えば、時刻ごとの新規ＩＤ数の変化をユーザが常時監視することが可能である。

【００５５】

また、第１の実施形態に係る異常検知装置１０は、前記メッセージに付与されたＩＤの単位時間あたりの頻度をＩＤごとに集計し、任意の単位時間の頻度と他の単位時間の頻度とを比較し、各単位時間のＩＤごとの異常度を検知することで、過去に観測されたことがあるＩＤのログについても異常を検知することが出来る。

【００５６】

また、第１の実施形態に係る異常検知装置１０は、分類部１５ａが、メッセージを所定の区切り文字で分割して単語群を抽出し、各単語を文字種によってパラメータまたは非パラメータに分類し、記憶部１４に記憶された辞書情報のテンプレート群のそれぞれの単語シーケンスと比較し、上記メッセージ中の非パラメータと分類された箇所の単語がすべて

一致するテンプレートが存在する場合には、該テンプレートのＩＤをメッセージに付与することで、分類方法について事前に詳細な設定を行わずにシステムのログメッセージを分類することが可能である。

【００５７】

（システム構成等）

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・統合の具体的形態は図示のものに限られず、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。

【００５８】

また、本実施の形態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、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。

【００５９】

（プログラム）

また、上記実施形態において説明した異常検知装置が実行する処理をコンピュータが実行可能な言語で記述したプログラムを作成することもできる。例えば、実施形態に係る異常検知装置１０が実行する処理をコンピュータが実行可能な言語で記述した異常検知プログラムを作成することもできる。この場合、コンピュータが異常検知プログラムを実行することにより、上記実施形態と同様の効果を得ることができる。さらに、かかる異常検知プログラムをコンピュータ読み取り可能な記録媒体に記録して、この記録媒体に記録された異常検知プログラムをコンピュータに読み込ませて実行することにより上記実施形態と同様の処理を実現してもよい。

【００６０】

図１２は、異常検知プログラムを実行するコンピュータを示す図である。図１２に例示するように、コンピュータ１０００は、例えば、メモリ１０１０と、ＣＰＵ１０２０と、ハードディスクドライブインタフェース１０３０と、ディスクドライブインタフェース１０４０と、シリアルポートインタフェース１０５０と、ビデオアダプタ１０６０と、ネットワークインタフェース１０７０とを有し、これらの各部はバス１０８０によって接続される。

【００６１】

メモリ１０１０は、図１２に例示するように、ＲＯＭ（Read Only Memory）１０１１及びＲＡＭ１０１２を含む。ＲＯＭ１０１１は、例えば、ＢＩＯＳ（Basic Input Output System）等のブートプログラムを記憶する。ハードディスクドライブインタフェース１０３０は、図１２に例示するように、ハードディスクドライブ１０９０に接続される。ディスクドライブインタフェース１０４０は、図１２に例示するように、ディスクドライブ１１００に接続される。例えば磁気ディスクや光ディスク等の着脱可能な記憶媒体が、ディスクドライブ１１００に挿入される。シリアルポートインタフェース１０５０は、図１２に例示するように、例えばマウス１１１０、キーボード１１２０に接続される。ビデオアダプタ１０６０は、図１２に例示するように、例えばディスプレイ１１３０に接続される。

【００６２】

ここで、図１２に例示するように、ハードディスクドライブ１０９０は、例えば、ＯＳ１０９１、アプリケーションプログラム１０９２、プログラムモジュール１０９３、プロ

グラムデータ１０９４を記憶する。すなわち、上記の、異常検知プログラムは、コンピュータ１０００によって実行される指令が記述されたプログラムモジュールとして、例えばハードディスクドライブ１０９０に記憶される。

【００６３】

また、上記実施形態で説明した各種データは、プログラムデータとして、例えばメモリ１０１０やハードディスクドライブ１０９０に記憶される。そして、ＣＰＵ１０２０が、メモリ１０１０やハードディスクドライブ１０９０に記憶されたプログラムモジュール１０９３やプログラムデータ１０９４を必要に応じてＲＡＭ１０１２に読み出し、各種処理手順を実行する。

【００６４】

なお、異常検知プログラムに係るプログラムモジュール１０９３やプログラムデータ１０９４は、ハードディスクドライブ１０９０に記憶される場合に限られず、例えば着脱可能な記憶媒体に記憶され、ディスクドライブ等を介してＣＰＵ１０２０によって読み出されてもよい。あるいは、異常検知プログラムに係るプログラムモジュール１０９３やプログラムデータ１０９４は、ネットワーク（ＬＡＮ（Local Area Network）、ＷＡＮ（Wide Area Network）等）を介して接続された他のコンピュータに記憶され、ネットワークインタフェース１０７０を介してＣＰＵ１０２０によって読み出されてもよい。

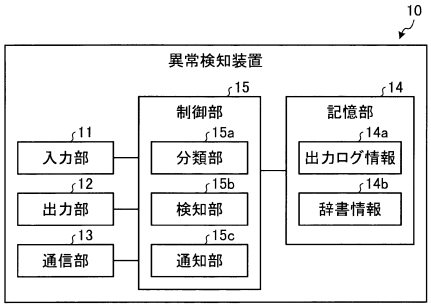
【符号の説明】

【００６５】

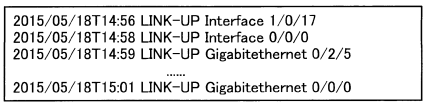
１０　異常検知装置
１１　入力部
１２　出力部
１３　通信部
１４　記憶部
１４ａ　出力ログ情報
１４ｂ　辞書情報
１５　制御部
１５ａ　分類部
１５ｂ　検知部
１５ｃ　通知部

【図面】

【図１】



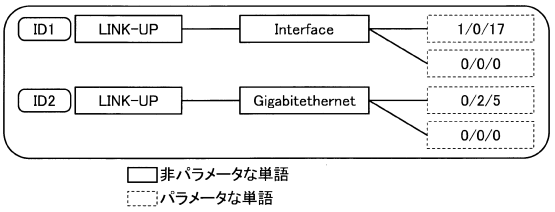

【図２】



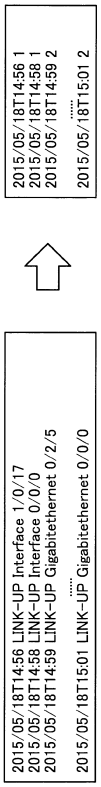

【図３】

| ID | 単語シーケンス |
|---|---|
| 1 | LINK-UP Interface * |
| 2 | LINK-UP Gigabitethernet * |
| | |

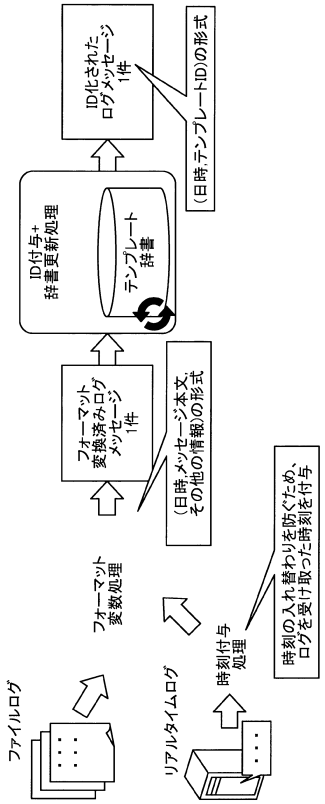
【図４】



【図５】


2015/05/18T14:56 LINK-UP Interface 1/0/17
2015/05/18T14:58 LINK-UP Interface 0/0/0
2015/05/18T14:59 LINK-UP Gigabitethernet 0/2/5
……
2015/05/18T15:01 LINK-UP Gigabitethernet 0/0/0
2015/05/18T14:56 1
2015/05/18T14:58 1
2015/05/18T14:59 2
……
2015/05/18T15:01 2

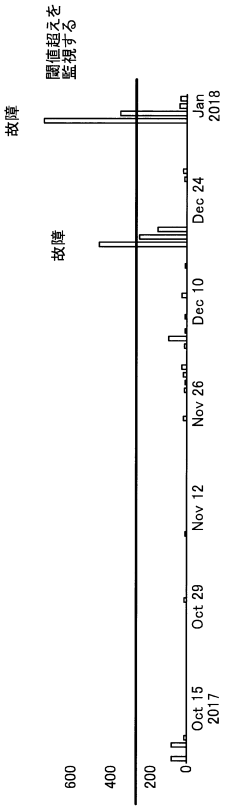
【図６】


ファイルログ
リアルタイムログ
フォーマット
変数処理
時刻付与
処理
時刻の入れ替わりを防ぐため、
ログを受け取った時刻を付与
(日時,メッセージ本文,
その他の情報)の形式
フォーマット
変換済みログ
メッセージ
1件
ID付与+
辞書更新処理
テンプレート
辞書
ID化された
ログメッセージ
1件
(日時,テンプレートID)の形式

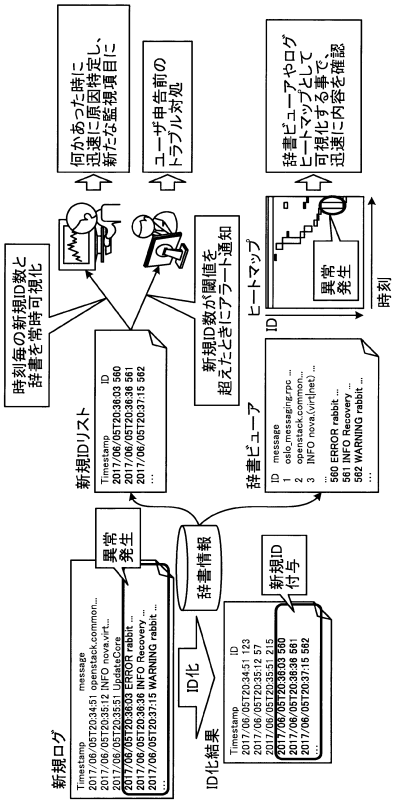
【図７】


200
100
0
Apr 15
2018
Apr 29
May 13
May 27
Jun 10
Jun 24
Jul 8
Jul 2

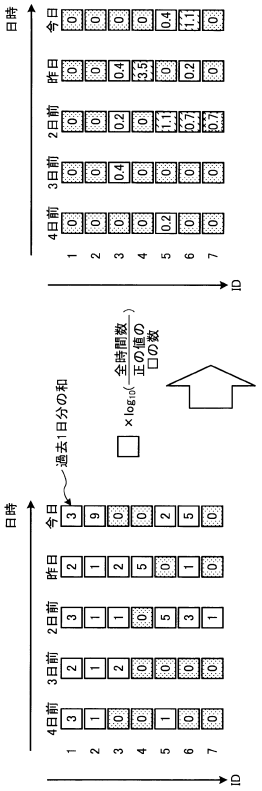
【図８】


閾値超えを
監視する
故障
故障
600
400
200
0
Oct 15
2017
Oct 29
Nov 12
Nov 26
Dec 10
Dec 24
Jan
2018

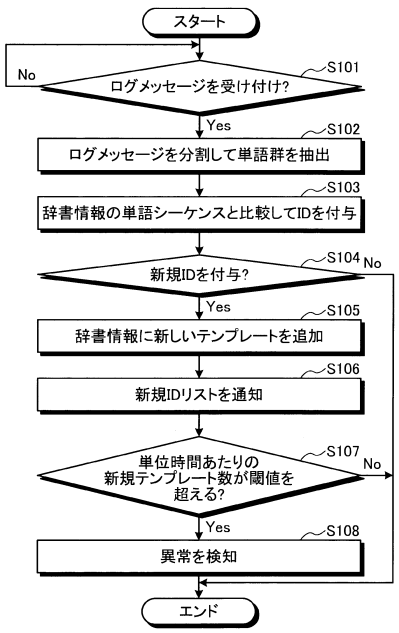
【図９】



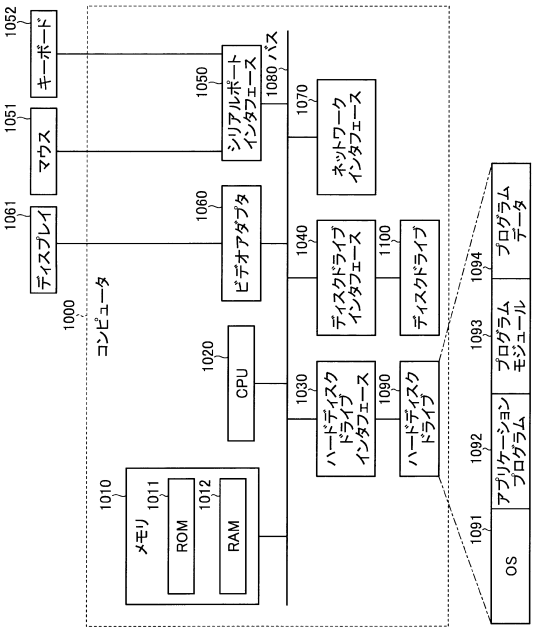

【図１０】




【図１１】




【図１２】



フロントページの続き

(56)参考文献 国際公開第２０１７／０８１８６５（WO，Ａ１）
特開２００４－３１８５５２（ＪＰ，Ａ）
高田 哲司，見えログ：情報視覚化とテキストマイニングを用いたログ情報ブラウザ，情報処理学会論文誌，日本，社団法人情報処理学会，2000年12月15日，第４１巻，第１２号，pp. 3265-3275，ISSN:0387-5806

(58)調査した分野 (Int.Cl.，ＤＢ名)
Ｇ０６Ｆ １１／０７
Ｇ０６Ｆ １６／００－１６／９５８
Ｈ０４Ｌ ６７／００