

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第5126698号  
(P5126698)

(45) 発行日 平成25年1月23日(2013.1.23)

(24) 登録日 平成24年11月9日(2012.11.9)

(51) Int.Cl.		F I			
<b>G06F 11/30</b>	<b>(2006.01)</b>	G06F 11/30		A	
<b>G06F 11/34</b>	<b>(2006.01)</b>	G06F 11/34		L	
		G06F 11/34		S	

請求項の数 16 (全 56 頁)

(21) 出願番号	特願2009-503974 (P2009-503974)	(73) 特許権者	000004237
(86) (22) 出願日	平成20年3月4日(2008.3.4)		日本電気株式会社
(86) 国際出願番号	PCT/JP2008/053830		東京都港区芝五丁目7番1号
(87) 国際公開番号	W02008/111428	(74) 代理人	100130029
(87) 国際公開日	平成20年9月18日(2008.9.18)		弁理士 永井 道雄
審査請求日	平成23年2月10日(2011.2.10)	(74) 代理人	100166338
(31) 優先権主張番号	特願2007-64678 (P2007-64678)		弁理士 関口 正夫
(32) 優先日	平成19年3月14日(2007.3.14)	(74) 代理人	100152054
(33) 優先権主張国	日本国(JP)		弁理士 仲野 孝雅
		(72) 発明者	加藤 清志
			日本国東京都港区芝五丁目7番1号 日本電気株式会社内
		審査官	多胡 滋

最終頁に続く

(54) 【発明の名称】 運用管理装置、運用管理方法および運用管理プログラム

(57) 【特許請求の範囲】

【請求項1】

管理対象システムの状態を表す属性の名称とその属性値とを対応付けたイベントデータが、定められた条件に合致したときに処理を行う運用管理装置であって、

実行する処理を定めた運用ルール情報を記憶するルール記憶手段と、

運用ルール情報毎に定められた条件となる情報であって、属性と属性値とを対応づけた情報であり、属性値の一部が過去のイベントデータから推測される参考値として記述されることがあり、また、属性値の一部が変数として記述されることがある個別フィルタ情報を記憶する個別フィルタ情報記憶手段と、

個別フィルタ情報で変数として記述された属性値に管理対象システムで生成されたイベントデータの属性値を代入したデータである予測イベントデータを記憶する予測イベントデータ記憶手段と、

生成されたイベントデータと、当該イベントデータに合致する個別フィルタ情報から生成された予測イベントデータと、運用ルール情報に対応する個別フィルタ情報の集合であるグループであってイベントデータに合致する個別フィルタ情報が属するグループとを対応付けた情報である予測イベント一覧を記憶する予測イベント一覧記憶手段と、

運用ルール情報と、運用ルール情報が定める条件となる各個別フィルタ情報と、前記各個別フィルタ情報が属するグループと、個別フィルタ情報から生成された予測イベントデータとを対応付けた情報である予測イベント対応表を記憶する予測イベント対応表記憶手段と、

10

20

新たに生成されたイベントデータの属性値が、既に存在する予測イベントデータの参考値以外の属性値と合致している場合にイベントデータと予測イベントデータとが合致すると判定し、新たに生成されたイベントデータの属性値が、既に存在する予測イベントデータの参考値以外の属性値と合致していない場合にイベントデータと予測イベントデータとが合致しないと判定する予測イベントデータ合致判定手段と、

イベントデータと予測イベントデータとが合致しないと判定された場合に、参考値以外の属性値がイベントデータの属性値と合致する個別フィルタ情報を特定する個別フィルタ情報特定手段と、

個別フィルタ情報の特定に成功した場合に、当該個別フィルタ情報が属するグループに属する各個別フィルタ情報の変数にイベントデータの属性値を代入して、前記各個別フィルタ情報毎に予測イベントデータを生成し、予測イベントデータ記憶手段に予測イベントデータを記憶させ、イベントデータと予測イベントデータとイベントデータに合致する個別フィルタ情報が属するグループとの対応関係を示す情報を予測イベント一覧記憶手段に記憶させ、生成された予測イベントデータとその予測イベントデータの生成に用いられた個別フィルタ情報のグループと、当該グループに属する各個別フィルタ情報と、前記各個別フィルタ情報を条件とする運用ルール情報との対応関係を示す情報を予測イベント対応表記憶手段に記憶させる予測イベントデータ生成手段と、

予測イベントデータ生成手段が予測イベントデータを生成した後に、当該予測イベントデータを生成するために用いたイベントデータに合致する個別フィルタ情報が属するグループと予測イベント一覧で対応付けられた各イベントデータが、前記グループに対応する運用ルール情報の個別フィルタ情報を満足しているか否かを判定し、満足している場合に運用ルール情報が定める処理を実行するルール判定手段とを備えた

ことを特徴とする運用管理装置。

#### 【請求項 2】

イベントデータと予測イベントデータとが合致すると判定された場合に、予測イベントデータに含まれる参考値がイベントデータの属性値に合致するか否かを判定する参考値合致判定手段と、

イベントデータと予測イベントデータとが合致すると判定され予測イベントデータに含まれる参考値がイベントデータの属性値に合致しないと判定された場合に、運用ルール情報およびイベントデータを表示するとともに参考値と合致しない属性値を表示し、運用ルール情報の条件を変更するか否かの指示が入力されるユーザインタフェース手段と、

運用ルール情報の条件を変更しない旨の指示が入力された場合に、イベントデータの属性値と予測イベントデータの参考値とが一致していなかった属性の参考値を個別フィルタ情報から削除し、運用ルール情報の条件を変更する旨の指示が入力された場合に、イベントデータの属性値と予測イベントデータの参考値とが一致していなかった属性であって前記予測イベントデータの生成に用いた個別フィルタ情報が属するグループの個別フィルタ情報の属性の属性値を変数を用いた属性値に書き換え、イベントデータの属性値と合致していなかった予測イベントデータの参考値を参考値でない属性値に書き換える修正手段とを備えた

請求項 1 に記載の運用管理装置。

#### 【請求項 3】

予め発生順序が決まっている複数イベントデータに合致する複数の個別フィルタ情報を保持し、前記複数の個別フィルタ情報を順番を指定して予測イベントデータ生成手段に通知するジョブ管理手段を備え、

予測イベントデータ生成手段は、前記複数の個別フィルタ情報の集合を 1 つのグループとして、当該グループと前記複数の個別フィルタ情報とを対応付けた情報を予測イベント対応表記憶手段に記憶させ、ジョブ管理手段が通知した個別フィルタ情報と、当該個別フィルタ情報に合致するイベントデータから予測フィルタ情報を生成した場合に、前記個別フィルタ情報の次の個別フィルタ情報の変数に前記イベントデータの属性値を代入した予測イベントデータを生成し、生成した予測イベントデータを、グループと複数の個別フィ

10

20

30

40

50

ルタ情報とを対応付けた前記情報に追加する

請求項 1 または請求項 2 に記載の運用管理装置。

【請求項 4】

予測イベント対応表記憶手段で運用ルール情報に対応付けられた予測イベントデータが存在する場合に、当該予測イベントデータを管理対象システムに通知することによって、管理対象システムが生成したイベントデータのうち前記予測イベントデータに合致するイベントデータを優先的に通知することを管理対象システムに要求する優先イベントデータ要求手段を備えた

請求項 1 から請求項 3 のうちのいずれか 1 項に記載の運用管理装置。

【請求項 5】

属性と参考値でない属性値とを対応付けた情報であるフィルタ情報を記憶するフィルタ情報記憶手段と、

過去に生成されたイベントデータであって運用ルール情報が指定するフィルタ情報に合致するイベントデータから推測される属性値を参考値として前記フィルタ情報に付加することで個別フィルタ情報を生成する個別フィルタ情報生成手段とを備えた

請求項 1 から請求項 4 のうちのいずれか 1 項に記載の運用管理装置。

【請求項 6】

管理対象システムの状態を表す属性の名称とその属性値とを対応付けたイベントデータが定められた条件に合致したときに処理を行う運用管理装置であって、

実行する処理を定めた運用ルール情報を記憶するルール記憶手段と、

運用ルール情報毎に定められた条件となる情報であって、属性と属性値とを対応づけた情報であり、属性値の一部が過去のイベントデータから推測される参考値として記述されることがあり、また、属性値の一部が変数として記述されることがある個別フィルタ情報を記憶する個別フィルタ情報記憶手段と、

個別フィルタ情報で変数として記述された属性値に管理対象システムで生成されたイベントデータの属性値を代入したデータである予測イベントデータを記憶する予測イベントデータ記憶手段と、

生成されたイベントデータと、当該イベントデータに合致する個別フィルタ情報から生成された予測イベントデータと、運用ルール情報に対応する個別フィルタ情報の集合であるグループであってイベントデータに合致する個別フィルタ情報が属するグループとを対応付けた情報である予測イベント一覧を記憶する予測イベント一覧記憶手段と、

運用ルール情報と、運用ルール情報が定める条件となる各個別フィルタ情報と、前記各個別フィルタ情報が属するグループと、個別フィルタ情報から生成された予測イベントデータとを対応付けた情報である予測イベント対応表を記憶する予測イベント対応表記憶手段とを備えた運用管理装置に適用される運用管理方法であって、

予測イベントデータ合致判定手段が、新たに生成されたイベントデータの属性値が、既に存在する予測イベントデータの参考値以外の属性値と合致している場合にイベントデータと予測イベントデータとが合致すると判定し、新たに生成されたイベントデータの属性値が、既に存在する予測イベントデータの参考値以外の属性値と合致していない場合にイベントデータと予測イベントデータとが合致しないと判定し、

個別フィルタ情報特定手段が、イベントデータと予測イベントデータとが合致しないと判定された場合に、参考値以外の属性値がイベントデータの属性値と合致する個別フィルタ情報を特定し、

予測イベントデータ生成手段が、個別フィルタ情報の特定に成功した場合に、当該個別フィルタ情報が属するグループに属する各個別フィルタ情報の変数にイベントデータの属性値を代入して、前記各個別フィルタ情報毎に予測イベントデータを生成し、予測イベントデータ記憶手段に予測イベントデータを記憶させ、イベントデータと予測イベントデータとイベントデータに合致する個別フィルタ情報が属するグループとの対応関係を示す情報を予測イベント一覧記憶手段に記憶させ、生成された予測イベントデータとその予測イベントデータの生成に用いられた個別フィルタ情報のグループと、当該グループに属する

10

20

30

40

50

各個別フィルタ情報と、前記各個別フィルタ情報を条件とする運用ルール情報との対応関係を示す情報を予測イベント対応表記憶手段に記憶させ、

予測イベントデータ生成手段が予測イベントデータを生成した後に、ルール判定手段が、当該予測イベントデータを生成するために用いたイベントデータに合致する個別フィルタ情報が属するグループと予測イベント一覧で対応付けられた各イベントデータが、前記グループに対応する運用ルール情報の個別フィルタ情報を満足しているか否かを判定し、満足している場合に運用ルール情報が定める処理を実行する

ことを特徴とする運用管理方法。

【請求項 7】

参考値合致判定手段が、イベントデータと予測イベントデータとが合致すると判定された場合に、予測イベントデータに含まれる参考値がイベントデータの属性値に合致するか否かを判定し、

ユーザインタフェース手段が、イベントデータと予測イベントデータとが合致すると判定され予測イベントデータに含まれる参考値がイベントデータの属性値に合致しないと判定された場合に、運用ルール情報およびイベントデータを表示するとともに参考値と合致しない属性値を表示し、運用ルール情報の条件を変更するか否かの指示が入力され、

修正手段が、運用ルール情報の条件を変更しない旨の指示が入力された場合に、イベントデータの属性値と予測イベントデータの参考値とが一致していなかった属性の参考値を個別フィルタ情報から削除し、運用ルール情報の条件を変更する旨の指示が入力された場合に、イベントデータの属性値と予測イベントデータの参考値とが一致していなかった属性であって前記予測イベントデータの生成に用いた個別フィルタ情報が属するグループの個別フィルタ情報の属性の属性値を変数を用いた属性値に書き換え、イベントデータの属性値と合致していなかった予測イベントデータの参考値を参考値でない属性値に書き換える

請求項 6 に記載の運用管理方法。

【請求項 8】

ジョブ管理手段が、予め発生順序が決まっている複数イベントデータに合致する複数の個別フィルタ情報を保持し、前記複数の個別フィルタ情報を順番を指定して予測イベントデータ生成手段に通知し、

予測イベントデータ生成手段が、前記複数の個別フィルタ情報の集合を 1 つのグループとして、当該グループと前記複数の個別フィルタ情報とを対応付けた情報を予測イベント対応表記憶手段に記憶させ、ジョブ管理手段が通知した個別フィルタ情報と、当該個別フィルタ情報に合致するイベントデータから予測フィルタ情報を生成した場合に、前記個別フィルタ情報の次の個別フィルタ情報の変数に前記イベントデータの属性値を代入した予測イベントデータを生成し、生成した予測イベントデータを、グループと複数の個別フィルタ情報とを対応付けた前記情報に追加する

請求項 6 または請求項 7 に記載の運用管理方法。

【請求項 9】

優先イベントデータ要求手段が、予測イベント対応表記憶手段で運用ルール情報に対応付けられた予測イベントデータが存在する場合に、当該予測イベントデータを管理対象システムに通知することによって、管理対象システムが生成したイベントデータのうち前記予測イベントデータに合致するイベントデータを優先的に通知することを管理対象システムに要求する

請求項 6 から請求項 8 のうちのいずれか 1 項に記載の運用管理方法。

【請求項 10】

管理対象システムの状態を表す属性の名称とその属性値とを対応付けたイベントデータが定められた条件に合致したときに処理を行うコンピュータであって、

実行する処理を定めた運用ルール情報を記憶するルール記憶手段と、

運用ルール情報毎に定められた条件となる情報であって、属性と属性値とを対応づけた情報であり、属性値の一部が過去のイベントデータから推測される参考値として記述され

10

20

30

40

50

ることがあり、また、属性値の一部が変数として記述されることがある個別フィルタ情報を記憶する個別フィルタ情報記憶手段と、

個別フィルタ情報で変数として記述された属性値に管理対象システムで生成されたイベントデータの属性値を代入したデータである予測イベントデータを記憶する予測イベントデータ記憶手段と、

生成されたイベントデータと、当該イベントデータに合致する個別フィルタ情報から生成された予測イベントデータと、運用ルール情報に対応する個別フィルタ情報の集合であるグループであってイベントデータに合致する個別フィルタ情報が属するグループとを対応付けた情報である予測イベント一覧を記憶する予測イベント一覧記憶手段と、

運用ルール情報と、運用ルール情報が定める条件となる各個別フィルタ情報と、前記各個別フィルタ情報が属するグループと、個別フィルタ情報から生成された予測イベントデータとを対応付けた情報である予測イベント対応表を記憶する予測イベント対応表記憶手段とを備えたコンピュータに搭載される運用管理プログラムであって、

コンピュータに、

新たに生成されたイベントデータの属性値が、既に存在する予測イベントデータの参考値以外の属性値と合致している場合にイベントデータと予測イベントデータとが合致すると判定し、新たに生成されたイベントデータの属性値が、既に存在する予測イベントデータの参考値以外の属性値と合致していない場合にイベントデータと予測イベントデータとが合致しないと判定する予測イベントデータ合致判定処理、

イベントデータと予測イベントデータとが合致しないと判定された場合に、参考値以外の属性値がイベントデータの属性値と合致する個別フィルタ情報を特定する個別フィルタ情報特定処理、

個別フィルタ情報の特定に成功した場合に、当該個別フィルタ情報が属するグループに属する各個別フィルタ情報の変数にイベントデータの属性値を代入して、前記各個別フィルタ情報毎に予測イベントデータを生成し、予測イベントデータ記憶手段に予測イベントデータを記憶させ、イベントデータと予測イベントデータとイベントデータに合致する個別フィルタ情報が属するグループとの対応関係を示す情報を予測イベント一覧記憶手段に記憶させ、生成された予測イベントデータとその予測イベントデータの生成に用いられた個別フィルタ情報のグループと、当該グループに属する各個別フィルタ情報と、前記各個別フィルタ情報を条件とする運用ルール情報との対応関係を示す情報を予測イベント対応表記憶手段に記憶させる予測イベントデータ生成処理、および

予測イベントデータ生成処理で予測イベントデータを生成した後に、当該予測イベントデータを生成するために用いたイベントデータに合致する個別フィルタ情報が属するグループと予測イベント一覧で対応付けられた各イベントデータが、前記グループに対応する運用ルール情報の個別フィルタ情報を満足しているか否かを判定し、満足している場合に運用ルール情報が定める処理を実行するルール判定処理

を実行させるための運用管理プログラム。

#### 【請求項 11】

コンピュータに、

イベントデータと予測イベントデータとが合致すると判定された場合に、予測イベントデータに含まれる参考値がイベントデータの属性値に合致するか否かを判定する参考値合致判定処理、

イベントデータと予測イベントデータとが合致すると判定され予測イベントデータに含まれる参考値がイベントデータの属性値に合致しないと判定された場合に、運用ルール情報およびイベントデータを表示するとともに参考値と合致しない属性値を表示する表示処理、

運用ルール情報の条件を変更しない旨の指示が入力された場合に、イベントデータの属性値と予測イベントデータの参考値とが一致していなかった属性の参考値を個別フィルタ情報から削除し、運用ルール情報の条件を変更する旨の指示が入力された場合に、イベントデータの属性値と予測イベントデータの参考値とが一致していなかった属性であって前

10

20

30

40

50

記予測イベントデータの生成に用いた個別フィルタ情報が属するグループの個別フィルタ情報の属性の属性値を変数を用いた属性値に書き換え、イベントデータの属性値と合致していなかった予測イベントデータの参考値を参考値でない属性値に書き換える修正処理を実行させる請求項 10 に記載の運用管理プログラム。

【請求項 12】

コンピュータに、

予め発生順序が決まっている複数イベントデータに合致する複数の個別フィルタ情報であって順番が定められている個別フィルタ情報の集合を1つのグループとして、当該グループと前記複数の個別フィルタ情報とを対応付けた情報を予測イベント対応表記憶手段に記憶させる処理を実行させ、

10

予測イベントデータ生成処理で、前記順番が定められている個別フィルタ情報と、当該個別フィルタ情報に合致するイベントデータから予測フィルタ情報を生成した場合に、前記個別フィルタ情報の次の個別フィルタ情報の変数に前記イベントデータの属性値を代入した予測イベントデータを生成し、生成した予測イベントデータを、グループと複数の個別フィルタ情報とを対応付けた前記情報に追加する処理を実行させる

請求項 10 または請求項 11 に記載の運用管理プログラム。

【請求項 13】

コンピュータに、

予測イベント対応表記憶手段で運用ルール情報に対応付けられた予測イベントデータが存在する場合に、当該予測イベントデータを管理対象システムに通知することによって、管理対象システムが生成したイベントデータのうち前記予測イベントデータに合致するイベントデータを優先的に通知することを管理対象システムに要求する優先イベントデータ要求処理を実行させる

20

請求項 10 から請求項 12 のうちのいずれか 1 項に記載の運用管理プログラム。

【請求項 14】

管理対象システムの状態を表す属性とその属性値とを対応付けたイベントデータに応じて処理を行う運用管理装置であって、

生成された前記イベントデータの属性値が、予め設定された予測イベントデータの参考値以外の属性値と合致している場合に、予め設定された個別フィルタ情報のグループに対応付けられた複数の個別フィルタ情報から、前記イベントデータの属性値と合致する属性値を持つ個別フィルタ情報を特定する手段と、

30

特定された前記個別フィルタ情報の属するグループに対応付けられた複数の個別フィルタ情報の変数に前記イベントデータの属性値を加えて、前記複数の個別フィルタ情報毎に予測イベントデータを生成する手段と、

前記予測イベントデータ生成に用いた前記イベントデータに合致する前記個別フィルタ情報のグループと予め対応付けられた複数のイベントデータが、前記個別フィルタ情報のグループと予め対応付けられた運用ルール情報の条件を満足しているか否かを判定し、満足している場合に前記運用ルール情報に従い処理を実行する手段と、を備えたことを特徴とする運用管理装置。

【請求項 15】

40

管理対象システムの状態を表す属性とその属性値とを対応付けたイベントデータに応じて処理を行う運用管理装置の動作方法であって、

生成された前記イベントデータの属性値が、予め設定された予測イベントデータの参考値以外の属性値と合致している場合に、予め設定された個別フィルタ情報のグループに対応付けられた複数の個別フィルタ情報から、前記イベントデータの属性値と合致する属性値を持つ個別フィルタ情報を特定し、

特定された前記個別フィルタ情報の属するグループに対応付けられた複数の個別フィルタ情報の変数に前記イベントデータの属性値を加えて、前記複数の個別フィルタ情報毎に予測イベントデータを生成し、

前記予測イベントデータ生成に用いた前記イベントデータに合致する前記個別フィルタ

50

情報のグループと予め対応付けられた複数のイベントデータが、前記個別フィルタ情報のグループと予め対応付けられた運用ルール情報の条件を満足しているか否かを判定し、満足している場合に前記運用ルール情報に従い処理を実行することを特徴とする運用管理方法。

【請求項 16】

管理対象システムの状態を表す属性とその属性値とを対応付けたイベントデータに応じて処理を行う運用管理装置の動作プログラムであって、

コンピュータに、

生成された前記イベントデータの属性値が、予め設定された予測イベントデータの参考値以外の属性値と合致している場合に、予め設定された個別フィルタ情報のグループに対応付けられた複数の個別フィルタ情報から、前記イベントデータの属性値と合致する属性値を持つ個別フィルタ情報を特定する処理と、

10

特定された前記個別フィルタ情報の属するグループに対応付けられた複数の個別フィルタ情報の変数に前記イベントデータの属性値を加えて、前記複数の個別フィルタ情報毎に予測イベントデータを生成する処理と、

前記予測イベントデータ生成に用いた前記イベントデータに合致する前記個別フィルタ情報のグループと予め対応付けられた複数のイベントデータが、前記個別フィルタ情報のグループと予め対応付けられた運用ルール情報の条件を満足しているか否かを判定し、満足している場合に前記運用ルール情報に従い処理を実行する処理と、

を実行させるための運用管理プログラム。

20

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、WEBサービスや業務サービスといった情報通信サービスを提供するサービスシステムのシステム状態の分析を行う運用管理装置、運用管理方法および運用管理プログラムに関し、特に、サービスシステムの信頼性を高めたり、運用管理装置を操作する者の操作負担を軽減したりすることができる運用管理装置、運用管理方法および運用管理プログラムに関する。

【背景技術】

【0002】

WEBサービスのような情報通信サービスの社会インフラとしての重要性が高まるにつれて、そのサービスを提供する装置（以下、サービスシステムと記す。）の安定稼働が重要となっている。このようなサービスシステムの運用管理は、従来管理者が手作業で行っていた。しかし、サービスシステムが大規模・複雑化するにつれて、管理者に要求される知識および操作の面での負担が飛躍的に増大し、判断ミスや操作ミスによるサービス停止といった問題も発生している。

30

【0003】

このため、ハードウェアあるいはソフトウェアを一元的に状態監視し制御する統合運用管理システムでは、複数の機器から収集したイベントデータ（状態通知）に基づいて異常状態の組み合わせ等の分析を自動的に行い、大局的な問題点や原因を推定して管理者に通知し、対処支援を行うことができる。

40

【0004】

関連技術の運用管理装置の例が、特許文献1に記載されている。

【0005】

関連技術の運用管理装置は、順次発生するイベントデータの組み合わせを条件として指定して条件に応じた対処等を定めた運用ルール情報を保持している。イベントデータは、サービスシステムの状態を表すデータである。運用管理装置は、発生したイベントデータが運用ルール情報で指定されている条件を満たしているときに、その運用ルール情報に従って対処等を行う。

【0006】

50

このようにして運用管理装置は、予め想定されるサービスシステムの異常状態の監視や対処を行う。このような運用管理装置を用いることで、多数の機器を手動で監視し対処する場合に比べて、管理者の作業負担が大幅に軽減される。運用ルール情報に従って自動的に対処等が行われることによって、管理者の経験や能力に依らず一定の監視および対処を行うことができ、運用管理品質が向上する。

【0007】

図25は、一般的に知られている関連技術の運用管理装置の構成を示すブロック図である。図25に例示する運用管理装置41は、イベントデータ取得手段2と、イベント蓄積手段7と、イベント分析手段4と、判定条件蓄積手段3と、ユーザ対話手段5と、制御手段6とを備えている。また、運用管理装置41は、サービスシステム1と接続されている。運用管理装置41とサービスシステム1は、通信回線あるいは通信ネットワークを介して接続されていてもよい。また、運用管理装置41とサービスシステム1とが1つの装置として構成されていてもよい。

10

【0008】

サービスシステム1は、WEBサービスや業務サービスといった情報通信サービスを提供する情報処理装置等である。例えば、サービスシステム1は、端末(図示せず。)からの要求に応じてWebページを端末に送信したり、端末からの要求に応じて業務処理を実行したりする。サービスシステム1が提供する業務サービスは特に限定されない。

【0009】

サービスシステム1は、イベントデータを生成するイベントデータ生成手段71を備える。イベントデータは、サービスシステム1の状態を表す情報である。例えば、イベントデータは、サービスシステム1が備えるハードウェアやサービスシステム1に搭載されたソフトウェアの状態や、サービスシステム1が実行した処理の結果等を表す。

20

【0010】

イベントデータ生成手段71は、ハードウェアやソフトウェアの状態を監視し、その状態を表す情報をイベントデータとして生成する。また、イベントデータ生成手段71は生成したイベントデータを運用管理装置41に送信する。なお、個々のイベントデータが表しているサービスシステム1の状態をイベントと記す。

【0011】

イベント蓄積手段7は、サービスシステム1の動作状態の変化に従って順次生成されるイベントデータを記憶する記憶装置である。

30

【0012】

イベントデータ取得手段2は、イベントデータ生成手段71が順次生成して送信したイベントデータを受信し、受信したイベントデータをイベント蓄積手段7に記憶させる。また、イベントデータ取得手段2は、サービスシステム1から新たにイベントデータを受信した場合、そのイベントデータをイベント分析手段4に出力する。

【0013】

判定条件蓄積手段3は、運用ルール情報を記憶する記憶装置である。運用ルール情報には、多数のイベントデータからイベントデータを抽出するための条件が定められている。

【0014】

イベント分析手段4は、運用ルール情報を参照して、条件に合致するイベントデータを抽出する。なお、抽出すべきイベントデータは、管理者が監視したいと考えるイベントデータであり、どのようなイベントデータを抽出すべきかは、予め管理者によって定められる。抽出すべきイベントデータとして、例えば、障害の予兆となる状態を示すイベントデータ、障害の発生を示すイベントデータ、定期的に確認すべき項目を示すイベントデータ等がある。そして、予め抽出すべきイベントデータとして定められたイベントデータを抽出するための条件が管理者によって決定され、その条件を表した運用ルール情報が管理者によって作成される。判定条件蓄積手段3は、この運用ルール情報を記憶する。

40

【0015】

イベント分析手段4は、イベントデータ取得手段2からイベントデータが入力されると

50

、判定条件蓄積手段3に記憶された運用ルール情報を参照して、運用ルール情報に定められた条件に合致するイベントデータであるか否かを判定する。また、運用ルール情報には、条件に合致するイベントデータが存在する場合に実行すべき処理が記述されている場合がある。ただし、運用ルール情報にそのような処理が記述されていない場合もある。

【0016】

イベント分析手段4は、分析結果(判定結果)をユーザ対話手段5に出力する。このとき、イベント分析手段4は、条件に合致すると判定されたイベントデータおよびその判定に用いた運用ルール情報も併せて、ユーザ対話手段5に出力する。

【0017】

ユーザ対話手段5は、例えば、キーボードやマウス等の入力デバイスとディスプレイ装置とを含み、サービスシステム1の管理者に情報を表示したり、または、管理者からの操作を受け付ける。

【0018】

ユーザ対話手段5は、例えば、イベント分析手段4による分析結果、条件に合致すると判定されたイベントデータおよびその判定に用いた運用ルール情報を表示する。ユーザ対話手段5は、管理者による対話入力に従って、判定条件蓄積手段3に記憶された運用ルール情報を修正する。また、ユーザ対話手段5は、管理者による対話入力に応じて、サービスシステム1に対する制御指示を制御手段6に出力する。

【0019】

制御手段6は、ユーザ対話手段5からの制御指示に基づいて、サービスシステム1を制御する。

【0020】

次に、イベントデータについて説明する。図26は、図25に例示する従来の運用管理装置41がサービスシステム1から受信して記憶するイベントデータの例を示す説明図である。図26(b)はイベントデータの例を示し、図26(a)は、サービスシステム1の状態変化に伴って順次収集されるイベントデータの一覧を示すデータ(以下、イベントリストと記す。)を示す。

【0021】

図26に示す例では、個々のイベントデータは、収集されたイベントデータを一意に識別するための番号と、イベントデータの種類を表す情報と、発生日時と、発生元のハードウェアあるいはソフトウェアを示す情報と、イベントデータの形式を示すIDと、イベント発生に関わるユーザ名と、イベントの補足説明文とを含む。イベントデータに他の情報が含まれていてもよい。図26に例示するイベントリスト100は、各イベントデータから上記の情報(番号等の各情報)を抽出して列挙した情報である。なお、イベントデータには番号が含まれていなくてもよいが、以下の説明では、便宜的に番号が含まれている場合を例にして説明する。イベントデータを一意に識別する番号は、イベント取得手段2が受信したイベントデータに付加する。

【0022】

図26(b)に例示するイベントデータ101は、イベントリスト110に示す各イベントデータのうち、番号がE9005であるイベントデータの記述例を示す。本例では、イベントデータ101が、TYPE(種類)やSERVERといったサービスシステムの状態を表す属性の名称とその値(属性値)がイコール記号(=)で連結されたテキストファイルである場合を示している。

【0023】

イベントリスト100は、イベントデータに含まれる各属性の名称およびその値の記述を解釈して生成される。すなわち、イベントリストを生成する場合には、イベント取得手段2が、受信したイベントデータからTYPE(種類)やSERVERの各属性値の値を抽出し、1つのイベントデータから抽出したTYPE(種類)等の各属性値の値を対応付け、イベントデータ毎にイベントリスト100に追加していけばよい。

【0024】

10

20

30

40

50

図 2 6 に示す例では、イベントデータの T Y P E 属性からイベントリストにおける種類を生成し、イベントデータの D A T E 1 (日付)と T I M E 1 (時刻)からイベントリストにおける日時の項目を生成し、イベントデータの S E R V E R と S O U R C E からイベントリストにおける発生元の項目を生成する。同様に、イベントデータの U S E R からイベントリストにおけるユーザを生成する。

【 0 0 2 5 】

なお、図 2 6 では、イベントデータ 1 0 1 の T Y P E 属性として記述されている “ I N F O R M A T I O N ” からイベントリストにおける「情報」という文字列を導出してイベントリストに含めている。このようなイベントデータ 1 0 1 に含まれる各属性の属性値に対応する文字列を予め決めておき、その文字列をイベントリストに含めてもよい。

10

【 0 0 2 6 】

なお、図 2 6 では、コンピュータの状態を示す一般的な項目を示すイベントデータを例示しているが、イベントデータは他の情報を含んでいてもよい。イベントデータは、属性と、その属性の値とを対応させてサービスシステム 1 の状態を表す。また、イベントデータは、テキスト形式のデータであってもバイナリ形式のデータであってもよい。

【 0 0 2 7 】

イベントデータ取得手段 2 は、受信した全てのイベントデータを図 2 6 ( b ) に例示するようなイベント毎のファイルとしてイベント蓄積手段 7 に記憶させてもよい。また、受信した全てのイベントデータから、図 2 6 ( a ) に例示する表形式のイベントリストを生成し、各イベントデータをイベントリストの形式でイベント蓄積手段 7 に記憶させてもよい。以下の説明では、イベントデータ取得手段 2 が各イベントデータをイベントリストの形式でイベント蓄積手段 7 に記憶させる場合を例にして説明する。

20

【 0 0 2 8 】

図 2 7 は、判定条件蓄積手段 3 に記憶される運用ルール情報およびフィルタ情報の例を示す説明図である。図 2 7 ( a ) は運用ルール情報の例を示し、図 2 7 ( b ) はフィルタ情報の例を示している。フィルタ情報は、イベント分析手段 4 が抽出すべきイベントデータの条件を表す情報である。

【 0 0 2 9 】

ただし、イベント分析手段 4 がイベントデータを抽出する条件は、1つのフィルタ情報だけによって定めるとは限らず、条件が複数のフィルタ情報によって定められる場合もある。イベント分析手段 4 がイベントデータを抽出する条件は、運用ルール情報内で、1つまたは複数のフィルタ情報の組み合わせとして記述される。運用ルール情報において、イベントデータを抽出する条件として記述された1つまたは複数のフィルタ情報の組み合わせを組み合わせ条件と記す。

30

【 0 0 3 0 】

なお、運用ルール情報内に1つまたは複数のフィルタ情報の組み合わせを直接記述してもよいが、ここでは、運用ルール情報に組み合わせ条件としてフィルタ情報の識別情報が記述される場合を例にして説明する。なお、フィルタ情報は予め管理者に作成され、判定条件蓄積手段 3 に記憶される。

【 0 0 3 1 】

フィルタ情報は、イベントデータと同様に “ S O U R C E ” 等の属性と、属性の値とが含まれている。ただし、フィルタ情報に含まれる全ての属性に、属性の値が定められているとは限らない。

40

【 0 0 3 2 】

図 2 7 ( b ) に例示するフィルタ情報 2 0 2 では、“ S O U R C E ” というソフトウェアを表す属性の属性値が “ B I Z A P ” という業務ソフトウェアであり、“ E V E N T I D ” というイベントデータの形式の I D を表す属性の属性値が “ 8 0 0 0 ” であり、他の属性には属性値が定められていない。フィルタ情報で定めている属性の値がいずれも、イベントデータに含まれているその属性の値と一致している場合、イベント分析手段 4 は、イベントデータが、フィルタ情報が示す条件を満足していると判定する。

50

## 【 0 0 3 3 】

図 2 7 ( a ) に例示するように、運用ルール群 ( 運用ルール情報の集合 ) 2 0 0 に属する各運用ルール情報は、運用ルール情報を識別する番号と、組み合わせ条件と、イベントデータが条件に合致したと判定された場合に実行する処理内容と、運用ルールの説明文を含む。

## 【 0 0 3 4 】

例えば、図 2 7 ( a ) に例示する運用ルール群 2 0 0 のうち、番号が R 0 1 2 0 である運用ルール情報は、イベントデータと条件 F 0 0 1 1 ( 図 2 7 に示すフィルタ情報 2 0 1 参照。 ) および条件 F 0 0 1 2 ( フィルタ情報 2 0 2 参照。 ) との判定結果が共に真であれば、すなわち、イベントデータが条件 F 0 0 1 1、F 0 0 1 2 の双方に合致していれば、対処として `M i g ( $ F 0 0 1 2 . S O U R C E , $ S V ( N O U P D A T E ) )` というコマンドを実行することを示している。

10

## 【 0 0 3 5 】

ここで例示した運用ルール情報 R 0 1 2 0 は、サービスシステム 1 に含まれるコンピュータで、ソフトウェアの自動アップデートが行われた後に業務ソフトウェアが異常となった場合に生成されるイベントデータを検出するためのルールである。そして、この運用ルール情報 R 0 1 2 0 には、アップデートが行われていない別のコンピュータへ業務ソフトウェアを移動させるというコマンドも記述されている。

## 【 0 0 3 6 】

フィルタ情報 2 0 1 で示される条件 F 0 0 1 1 は、『イベントデータ内の S O U R C E 属性値が「 u p d a t e r 」であり、かつ、E V E N T I D 属性値が 4 0 0 1 である』という条件である。従って、イベント分析手段 4 は、そのようなイベントデータを検出した場合に、そのイベントデータは条件 F 0 0 1 1 に合致すると判定する ( 条件 F 0 0 1 1 との判定が真になる。 ) 。

20

## 【 0 0 3 7 】

条件 F 0 0 1 に合致するイベントデータの例として、図 2 6 に示すイベントデータ E 9 0 0 2 が挙げられる。また、図 2 7 に示す条件 F 0 0 1 2 は、『イベントデータ内の S O U R C E が「 B I Z A P 」であり E V E N T I D が「 8 0 0 0 」である』という条件である。例えば、図 2 6 に例示するイベントデータ E 9 0 0 4 がこの条件に合致する。従って、イベント分析手段 4 は、例えば図 2 6 に示すイベントデータ E 9 0 0 4 がイベントデータ取得手段 2 から入力された場合に、そのイベントデータは条件 F 0 0 1 2 に合致すると判定する ( 条件 F 0 0 1 2 との判定が真になる。 ) 。

30

## 【 0 0 3 8 】

ここで述べた条件 F 0 0 1 1 は、ソフトウェアのアップデートが行われたことを示すイベントデータを抽出するための条件である。また、条件 F 0 0 1 2 は、B I Z A P という業務ソフトウェアがエラーとなったことを示すイベントデータを抽出するための条件である。

## 【 0 0 3 9 】

また、条件 F 0 0 1 1、F 0 0 1 2 を組み合わせ条件とする運用ルール情報 R 0 1 2 0 ( 図 2 7 ( a ) 参照。 ) に記述される対処は、条件 F 0 0 1 2 に合致したイベントデータの S O U R C E 属性値に記述される業務ソフトウェア ( \$ F 0 0 1 2 . S O U R C E ) を、アップデートが行われていないことを示す N O U P D A T E の属性値を持つコンピュータ ( \$ S V ( N O U P D A T E ) ) に移動 ( M i g ( ) ) することを示している。

40

## 【 0 0 4 0 】

ここで、\$ 記号から始まる文字列は変数であり、イベント分析手段 4 で運用ルール情報が判定される際に、実際のイベントデータあるいは別途与えられた処理関数によって値が確定する情報であることを示す。別途与えられた処理関数によって決定する値とは、イベントデータ以外によって決定される値であり、例えば、「現在時刻」が該当する。以下、\$ 記号は変数を示すものとして説明する。

## 【 0 0 4 1 】

50

同様に、運用ルール情報 R 0 1 3 0 は、ジョブ異常を検出する図示しないフィルタ情報である F 0 0 1 3 とイベントデータとが合致したときに、対処として、MailTo (operator) というコマンドを実行することを示す。“MailTo (operator)” は、管理者へのメール通報を行うコマンドである。

【 0 0 4 2 】

このように運用ルール情報は、イベントデータが組み合わせ条件に合致すると判定した場合に、実行すべき対処を示している。

【 0 0 4 3 】

なお、図 2 7 ( a ) では、運用ルール情報として if - then 形式で記述される一般的なルールを例として挙げている。運用ルール情報は、このようなルールに限定されるものではない。例えば、組み合わせ情報としてフィルタ情報を記述するのではなく、正規表現等の一般的な構造解析手法を用いて情報を抽出するものであってもよい。

10

【 0 0 4 4 】

また、サービスシステム 1 の状態監視のみを行う場合には、対処が管理者通報や画面表示に固定されるため、対処の項目が省略される場合もある。さらに、能力の高い管理者のみを想定する場合には、理解促進のための説明文がない場合もある。いずれの場合でも、サービスシステム 1 の状態を表すイベントデータの分析を行えるものであればよい。すなわち、イベントデータが条件に合致しているか否か判定を判定し、合致するイベントデータを抽出することができるものであればよい。

【 0 0 4 5 】

20

以下、運用ルール情報において、イベントデータを抽出する条件をイベントデータで表す場合を例にして説明する。

【 0 0 4 6 】

また、イベント分析手段 4 は、内部メモリを有し、そのメモリに、個々のフィルタ情報を識別する番号 ( フィルタ番号 ) 毎に、そのフィルタ番号を組み合わせ情報として記述している運用ルール情報の番号とを対応付けた情報 ( 以下、分析状態表と記す。 ) を記憶する。

【 0 0 4 7 】

また、フィルタ番号が示すフィルタ情報に合致するイベントデータがイベント分析手段 4 に入力された場合、イベント分析手段 4 は、そのイベントデータの番号をフィルタ情報に対応付けて分析状態表に追加する。

30

【 0 0 4 8 】

図 2 8 は、イベント分析手段 4 が内部メモリ等に保持する分析状態表の例を示す。図 2 8 では、図 2 6 に示すイベントデータが順次イベント分析手段 4 に入力されイベント分析手段 4 が分析 ( イベントデータと条件とが合致するか否かの判定処理 ) を行っていったときの分析状態表の変化の例を示している。

【 0 0 4 9 】

図 2 8 に示すように、分析状態表では、運用ルール群 2 0 0 の組み合わせ条件として記述されている個々のフィルタ情報の番号と、そのフィルタ情報の番号を記述した運用ルール情報の番号とが、フィルタ情報の番号毎に対応付けて列挙されている。また、フィルタ情報と合致したイベントデータが存在する場合には、そのイベントデータの番号もフィルタ情報に対応付けて分析状態表に追加される。なお、図 2 7 に示す運用ルール群 2 0 0 では個々の運用ルール情報からフィルタ情報を探索することができる。

40

【 0 0 5 0 】

一方、図 2 8 に示す分析状態表は、フィルタ情報の番号をすべて列挙した情報であり、フィルタ情報から運用ルールを特定するために用いられる。例えば、図 2 8 に示す分析状態表 3 0 1 のフィルタ番号 F 0 0 1 1 の行を参照すると、このフィルタ情報は、図 2 7 に示す運用ルール群 2 0 0 における番号 R 0 1 2 0 のルールと対応付けられている。

【 0 0 5 1 】

従って、フィルタ番号 F 0 0 1 1 を組み合わせ条件として記述している運用ルール情報

50

R 0 1 2 0を検索することができる。また、図 2 8 に示す分析状態表 3 0 1 のフィルタ番号 F 0 0 1 1 の行では、イベントデータ E 9 0 0 2 が対応付けられている。従って、フィルタ番号 F 0 0 1 1 のフィルタ情報に合致するイベントデータとしてイベントデータ E 9 0 0 2 が存在することを示している。

【 0 0 5 2 】

イベント分析手段 4 は、イベントデータ取得手段 2 からイベントデータ E 9 0 0 2 が入力された時点で、表の上から順にフィルタ情報とマッチングを行う。すなわち、イベントデータがフィルタ情報に合致しているか否かを、分析状態表に記述されたフィルタ番号毎に判定していく。イベントデータがフィルタ情報と合致していると判定したならば、イベント分析手段 4 は、そのイベントデータの番号を、合致していると判定したフィルタ情報の番号に対応付けて分析状態表に記述する。分析状態表に記述されたイベントデータの番号から、対応する運用ルール情報の組み合わせ条件に合致するか否かの判定対象となるイベントデータを特定することができる。

10

【 0 0 5 3 】

図 2 9 は、図 2 5 に例示する従来の運用管理装置のイベント分析手段 4 の動作の例を示すフローチャートである。以下、図 2 5 から図 2 9 を参照して、従来の運用管理装置の動作を説明する。

【 0 0 5 4 】

予め、ユーザ対話手段 5 には、管理者から運用ルール群およびフィルタ情報が入力される。そして、ユーザ対話手段 5 は、その運用ルール群およびフィルタ情報を判定条件蓄積手段 3 に記憶させる。ここでは、図 2 7 ( a ) に示す運用ルール群 2 0 0 と、図 2 7 ( b ) に示すフィルタ情報 2 0 1、2 0 2 を含むフィルタ情報の集合が判定条件蓄積手段 3 に記憶されている場合を例にして説明する。

20

【 0 0 5 5 】

サービスシステム 1 のイベントデータ生成手段 7 1 は、順次サービスシステム 1 の動作状態を検出してイベントデータを生成し、イベントデータを運用管理装置 4 1 に送信する。イベントデータ取得手段 2 は、サービスシステム 1 からイベントデータを受信すると、そのイベントデータをイベント蓄積手段 7 に記憶させ、また、そのイベントデータをイベント分析手段 4 に出力する。

【 0 0 5 6 】

イベント分析手段 4 は、イベントデータ取得手段 2 からイベントデータを入力され、イベントデータの入力がない場合には、イベントデータの入力を待つ (ステップ S 7 0 1 )。

30

【 0 0 5 7 】

イベントデータ取得手段 2 からイベントデータが入力されると (ステップ S 7 0 1 の Y e s )、イベント分析手段 4 は例えば以下に示すように、運用ルール群 2 0 0 に含まれる運用ルール情報で組み合わせ条件とされたフィルタ情報とそのイベントデータとが合致するか否かを判定する。

【 0 0 5 8 】

イベント分析手段 4 は、図 2 8 に例示する分析状態表を参照して、分析状態表にフィルタ番号が列挙されているフィルタ情報のうち、イベントデータと合致しているか否かの判定が行われていないフィルタ情報の有無を判定する (ステップ S 7 0 2 )。イベントデータと合致しているか否かの判定が行われていないフィルタ情報が存在しているならば (ステップ S 7 0 2 の Y e s )、イベント分析手段 4 は、そのフィルタ情報のうちの 1 つとイベントデータとが合致するか否かを判定する (ステップ S 7 0 3 )。

40

【 0 0 5 9 】

ステップ S 7 0 3 における判定結果がフィルタ情報とイベントデータとが合致していないという判定結果であれば (ステップ S 7 0 4 の N o )、ステップ S 7 0 2 に移行し、ステップ S 7 0 2 以降の動作を繰り返す。イベントデータと合致しているか否かの判定が行われていないフィルタ情報が存在していなければ (ステップ S 7 0 2 の N o )、ステップ

50

S 7 0 1 に移行して新たなイベントデータの入力を待つ。

【 0 0 6 0 】

ステップ S 7 0 3 における判定結果がフィルタ情報とイベントデータとが合致しているという判定結果であれば（ステップ S 7 0 4 の Y e s ）、イベント分析手段 4 は、その入力されたイベントデータの番号を、合致すると判定されたフィルタ情報のフィルタ番号に対応付けて分析状態表に記録する（ステップ S 7 0 5 ）。

【 0 0 6 1 】

例えば、イベントデータ取得手段 2 から図 2 6 ( a ) に示すイベントデータイベントデータ E 9 0 0 2 が入力され、そのイベントデータ E 9 0 0 2 がフィルタ番号 F 0 0 1 1 で示されるフィルタ情報 2 0 1 と合致すると判定された場合、分析状態表においてフィルタ番号 F 0 0 1 1 に対応させて E 9 0 0 2 を記録する（ステップ S 7 0 5 ）。

10

【 0 0 6 2 】

さらに、イベント分析手段 4 は、イベントデータと合致しているフィルタ情報のフィルタ番号から運用ルール情報を特定し、イベントデータがその運用ルール情報の組み合わせ条件を満足しているか否かを判定する（ステップ S 7 0 6 ）。

【 0 0 6 3 】

ステップ S 7 0 6 における判定結果がイベントデータは組み合わせ条件を満足していないという判定結果であれば（ステップ S 7 0 7 の N o ）、ステップ S 7 0 1 に移行して新たなイベントデータの入力を待つ。一方、ステップ S 7 0 6 における判定結果がイベントデータは組み合わせ条件を満足しているという判定結果であれば（ステップ S 7 0 7 の Y e s ）、イベント分析手段 4 は、ステップ S 7 0 6 で特定された運用ルール情報で指定された対処を実行する（ステップ S 7 0 8 ）。

20

【 0 0 6 4 】

例えば、上記の例のようにステップ S 7 0 5 の処理を行った場合、イベント分析手段 4 は、分析状態表 3 0 1 から、フィルタ番号 F 0 0 1 1 に対応するルール番号である R 0 1 2 0 を特定し、イベントデータがその運用ルール情報の組み合わせ条件である「 F 0 0 1 1 AND F 0 0 1 2 」を満足するか否かを判定する（ステップ S 7 0 6 ）。

【 0 0 6 5 】

イベントデータ E 9 0 0 2 がイベント分析手段 4 に入力されたときの分析状態表 3 0 1 を参照すると、F 0 0 1 1 には対応するイベントデータが記録されているため真であるが、F 0 0 1 2 には対応するイベントデータが記録されていないため偽となり、運用ルール情報 R 0 1 2 0 の組み合わせ条件は偽である。すなわち、イベントデータ E 9 0 0 2 は運用ルール情報 R 0 1 2 0 の組み合わせ条件の組み合わせ条件を満足しない（ステップ S 7 0 7 の N o ）。

30

【 0 0 6 6 】

例示した上記の動作の後、イベント分析手段 4 にイベントデータ E 9 0 0 3 （図 2 6 参照。）が入力されると（ステップ S 7 0 1 の Y e s ）、イベント分析手段 4 は、そのイベントデータ E 9 0 0 3 と合致するフィルタ情報を特定する（ステップ S 7 0 2 ~ S 7 0 4 ）。

40

【 0 0 6 7 】

続いて、イベント分析手段 4 は、F 0 0 1 0 に対応する運用ルール情報 R 0 1 1 0 を特定し、イベントデータ E 9 0 0 3 がその運用ルール情報の組み合わせ条件を満足するか否かを判定する（ステップ S 7 0 6 ）。

50

## 【 0 0 6 8 】

従って、運用ルール情報の対処を実行することになるが（ステップ S 7 0 8）、運用ルール情報 R 0 1 1 0 には該当する対処が記述されていないので（図 2 7（a）参照。）何も処理を行わない。

## 【 0 0 6 9 】

次に、運用ルール情報の条件判定が完了したことから、分析状態表から対応イベント（ここでは E 9 0 0 3）を削除し（ステップ 7 0 9）、ステップ S 7 0 1 に移行する。この時点での分析状態表は、図 2 8 に示す分析状態表 3 0 1 と同様である。

## 【 0 0 7 0 】

さらに、同様にしてイベント分析手段 4 にイベントデータ E 9 0 0 4 が入力され、そのイベントデータとフィルタ番号 F 0 0 1 2 のフィルタ情報とが合致すると判定すると（ステップ S 7 0 1 ~ S 7 0 4）、イベント分析手段 4 は、分析状態表に対応イベントとして E 9 0 0 4 を記録する（ステップ S 7 0 5）。すなわち、F 0 0 1 2 に対応させてイベントデータの番号 E 9 0 0 4 を記憶する。

## 【 0 0 7 1 】

この結果、分析状態表 3 0 1 は、図 2 8 に示す分析状態表 3 0 2 の状態になる。さらに、イベント分析手段 4 は、F 0 0 1 2 に対応する運用ルール情報 R 0 1 2 0 を特定し、イベントデータ E 9 0 0 3 がその運用ルール情報の組み合わせ条件を満足するか否かを判定する（ステップ S 7 0 6）。このとき、分析状態表 3 0 2（図 2 8 参照。）では F 0 0 1 1 と F 0 0 1 2 の両方に対応イベントが存在することから条件判定が真となる（ステップ 7 0 7 の Y e s）。

## 【 0 0 7 2 】

よって、イベント分析手段 4 は、ユーザ対話手段 5 および制御手段 6 を介してサービスシステム 1 に対して対処を実行し（ステップ S 7 0 8）、運用ルール情報 R 0 1 2 0 に対応する対応イベント（E 9 0 0 2, E 9 0 0 4）を削除する（ステップ S 7 0 9）。この結果、分析状態表 3 0 2 は、図 2 8 に示す分析状態表 3 0 3 の状態になる。

## 【 0 0 7 3 】

図 2 6（a）に示すイベントデータ E 9 0 0 5 は、このようにして行われた対処の結果を示すイベントデータであり、運用ルール情報 R 0 1 1 0 の組み合わせ条件に合致するものとする。

## 【 0 0 7 4 】

イベント分析手段 4 は、イベントデータのうち、運用ルール情報の組み合わせ条件に合致したイベントデータからなるリストを作成して、イベント蓄積手段 1 に記憶させる態様もある。このリストは、図 2 6（a）に示すイベントリストと同様のフォーマットのリストとして作成される。

## 【 0 0 7 5 】

このようにして運用ルール情報の組み合わせ条件に合致したイベントデータのリストを作成した場合、ユーザ対話手段 5 は、そのリストをユーザ対場手段 5 を介して管理者に提示する。管理者は、このリストの中のイベントデータ E 9 0 0 5 を参照することで、異常に自動的に対処が行われたことを知ることができる。

## 【 0 0 7 6 】

また、運用ルール情報として対処を指定していない異常を発見した場合等、ユーザ対話手段 5 を介して制御手段 6 に制御指示を行い、手動で対処を行うことができる。なお、イベントデータ取得手段 2 が受信したイベントデータは全てファイル毎にあるいはイベントリストとしてイベント蓄積手段 1 に記憶されている。これらのイベントデータ（イベントリスト）をユーザ対話手段 5 に表示させることで、管理者により詳細な情報を確認させることができる。

## 【 0 0 7 7 】

このように、図 2 5 に示す関連技術の運用管理装置では、順次発生するイベントデータを抽出するための組み合わせ条件を運用ルール情報で指定することによって、予め想定さ

10

20

30

40

50

れるサービスシステム 1 の異常状態の監視および対処を行うことができる。そして、多数の機器を手動で監視し対処する場合に比べて、大幅に作業負担が軽減される。また、自動化によって、管理者の経験や能力に依らず一定の監視および対処を行うことができ、運用管理品質が向上する。

【 0 0 7 8 】

また、特許文献 2 には、情報処理システムに将来障害が発生する可能性を予測するステップを含む性能監視方法が記載されている。

【 0 0 7 9 】

【特許文献 1】特開 2 0 0 6 - 2 4 4 4 0 4 号公報

【特許文献 2】特開 2 0 0 5 - 3 2 7 2 6 1 号公報 ( 段落 0 0 0 9 )

10

【発明の開示】

【発明が解決しようとする課題】

【 0 0 8 0 】

関連技術の運用管理装置では、イベント分析手段 4 は、入力されたイベントデータの中から、運用ルール情報の組み合わせ条件に合致するイベントデータを抽出する。組み合わせ条件は、フィルタ情報の組み合わせとして記述されるので、予め発生する時間順序が判明しているイベントデータに対しても、時系列とは関係なく、各フィルタ情報と合致しているか否かの判定を行うことになる。

【 0 0 8 1 】

イベント分析手段 4 に入力されたイベントデータがどのフィルタ情報に合致するかを判定するために、すべてのフィルタ情報とマッチングする必要があるため、処理負荷が大きいという問題があった。

20

【 0 0 8 2 】

例えば、前述した運用ルール情報 R 0 1 2 0 の組み合わせ条件は、F 0 0 1 1 および F 0 0 1 2 である。F 0 0 1 1 に合致するイベントデータが発生し、F 0 0 1 2 に合致するイベントデータがその後に発生することがわかっている場合であっても、各イベント毎に全てのフィルタ情報のマッチングを行う。このため、イベントデータ E 9 0 0 4 が発生した時点で、分析状態表 3 0 2 で示す対応 ( E 9 0 0 4 と F 0 0 1 2 との対応 ) を見つけるためには、既に E 9 0 0 2 と合致するフィルタ情報 F 0 0 1 1 とのマッチングも含めて、順次マッチングを繰り返す必要があった。

30

【 0 0 8 3 】

特に、サービスシステムが多数の機器で構成される大規模環境では、人手での運用管理が難しいため、運用管理装置による運用管理の自動化が最も望まれている。しかし、関連技術の運用管理装置では、このような環境では、運用ルール情報の数も、その条件として指定されるフィルタ情報の組合せも多くなり、飛躍的に処理負荷が増大するため、適用が困難であるという問題があった。

【 0 0 8 4 】

さらに、この関連技術の運用管理装置では、運用ルール情報の組み合わせ条件として複数のフィルタ条件を指定し、それらに合致する複数のイベントデータを検出したときに対処を行う。この場合、個々のイベントデータを特定するためのフィルタ条件と、発生元の関係や時間順序等のサービスシステムの特性に依存する環境依存のフィルタ条件を区別することができない。

40

【 0 0 8 5 】

前述の例では、イベントデータ E 9 0 0 2 とイベントデータ E 9 0 0 4 の発生元が S V 3 で同じである ( 図 2 6 ( a ) 参照 ) 。これらの発生元が異なっていたとしても、運用ルール情報 R 0 1 2 0 の条件は真となる。これは、例示したフィルタ情報に発生元の S E R V E R を特定する記述がないためである ( 図 2 7 ( b ) 参照 ) 。

【 0 0 8 6 】

仮に発生元を特定する記述をフィルタ情報に追加するとしても、発生元が同じ場合に限定すれば良いのか、異なっても一定の条件で真になるようにすれば良いのかは、サー

50

ビスシステム1の特性に依存する。例えば、運用ルール情報R0120を設定した主旨を考慮すれば、業務ソフトウェアが稼動するコンピュータでアップデートが行われた場合を特定することになるが、独立したコンピュータで実現されたシステムであれば、発生元が同じ場合のみに限定することになり、複数のコンピュータが付加分散等で連携する場合は、連携するコンピュータかどうかで区別することになる。

【0087】

このように、環境依存の条件とほとんど環境に依存しない(不変とみなせる)条件を区別することができないため、結果的に、実際に発生するイベントデータの系列に合わせてフィルタ情報に環境依存の条件を多数記述する必要がある。このため、条件記述が複雑で判読性が低下することから、管理者が適切に運用ルール情報を設定することが難しくなるという問題があった。また、類似する他のシステムへの適用が困難となり、個々のサービスシステム毎に管理者が調整する作業が多くなるという問題があった。

10

【0088】

また、例えば、ある運用ルール情報Pの組み合わせ条件ではフィルタ情報A、Bが指定され、他の運用ルール情報Qの組み合わせ条件ではフィルタ情報A、Cが指定されていたとする。そして、運用ルール情報Pでは、フィルタ情報A、Bに合致する各イベントデータとして、発生元サーバが同一であるイベントデータを抽出し、運用ルール情報Qでは、フィルタ情報A、Cに合致する各イベントデータとして、発生元サーバが同一であるか否かを問わないイベントデータを抽出するとする。この場合、フィルタ情報Aの記述が複雑になり、フィルタ情報の判読性が低下する。

20

【0089】

以上に説明したように、関連技術の運用管理装置では、処理負荷が大きいため大規模環境に適用できないという問題があった。また、環境依存の記述が多くなるため、適切に運用ルール情報を設定できないという問題があった。

【0090】

そして、発生したイベントデータがどのフィルタ条件に合致するかを判定するために、すべてのフィルタ情報とマッチングする必要があるため、処理負荷が大きいためという問題があった。特に、サービスシステムが多数の機器で構成される大規模環境では、運用ルール情報の数も、その条件として指定されるフィルタ情報の組み合わせも多くなり、飛躍的に処理負荷が増大するという問題があった。

30

【0091】

さらに、実際に発生するイベントデータの系列に合わせてフィルタ情報に環境依存の条件を多数記述する必要があるため、条件記述が複雑で判読性が低下することから、管理者が適切に運用ルール情報を設定することが難しくなるという問題があった。

【0092】

そこで、本発明は、イベントデータと条件とが合致するか否かの判定を行う際の処理負荷を軽減してイベントデータの分析を迅速に行うことができる運用管理装置、運用管理方法および運用管理プログラムを提供することを目的とする。また、個々のイベントデータを特定するための条件と、サービスシステムの特性に依存する条件を区別し、管理者が運用ルール情報を容易に理解でき適切に設定できる運用管理装置、運用管理方法および運用管理プログラムを提供することを目的とする。

40

【課題を解決するための手段】

【0093】

本発明の運用管理装置は、管理対象システムの状態を表す属性の名称とその属性値とを対応付けたイベントデータが定められた条件に合致したときに処理を行う運用管理装置であって、次のルール記憶手段、個別フィルタ情報記憶手段、予測イベント一覧記憶手段、予測イベント対応表記憶手段、個別フィルタ情報特定手段、予測イベントデータ生成手段、およびルール判定手段を有する。

【0094】

ルール記憶手段は、実行する処理を定めた運用ルール情報を記憶する。

50

## 【0095】

個別フィルタ情報記憶手段は、運用ルール情報毎に定められた条件となる情報であって、属性と属性値とを対応づけた情報であり、属性値の一部が過去のイベントデータから推測される参考値として記述されることがあり、また、属性値の一部が変数として記述されることがある個別フィルタ情報を記憶する。

## 【0096】

予測イベント一覧記憶手段は、個別フィルタ情報で変数として記述された属性値に管理対象システムで生成されたイベントデータの属性値を代入したデータである予測イベントデータを記憶する予測イベントデータ記憶手段と、生成されたイベントデータと、当該イベントデータに合致する個別フィルタ情報から生成された予測イベントデータと、運用ルールの情報に対応する個別フィルタ情報の集合であるグループであってイベントデータに合致する個別フィルタ情報が属するグループとを対応付けた情報である予測イベント一覧を記憶する。

10

## 【0097】

予測イベント対応表記憶手段は、運用ルール情報と、運用ルール情報が定める条件となる各個別フィルタ情報と、その各個別フィルタ情報が属するグループと、個別フィルタ情報から生成された予測イベントデータとを対応付けた情報である予測イベント対応表を記憶する。

## 【0098】

予測イベントデータ合致判定手段は、新たに生成されたイベントデータの属性値が、既に存在する予測イベントデータの参考値以外の属性値と合致している場合にイベントデータと予測イベントデータとが合致すると判定し、新たに生成されたイベントデータの属性値が、既に存在する予測イベントデータの参考値以外の属性値と合致していない場合にイベントデータと予測イベントデータとが合致しないと判定する。

20

## 【0099】

個別フィルタ情報特定手段は、イベントデータと予測イベントデータとが合致しないと判定された場合に、参考値以外の属性値がイベントデータの属性値と合致する個別フィルタ情報を特定する。

## 【0100】

予測イベントデータ生成手段は、個別フィルタ情報の特定に成功した場合に、当該個別フィルタ情報が属するグループに属する各個別フィルタ情報の変数にイベントデータの属性値を代入して、その各個別フィルタ情報毎に予測イベントデータを生成し、予測イベントデータ記憶手段に予測イベントデータを記憶させ、イベントデータと予測イベントデータとイベントデータに合致する個別フィルタ情報が属するグループとの対応関係を示す情報を予測イベント一覧記憶手段に記憶させ、生成された予測イベントデータとその予測イベントデータの生成に用いられた個別フィルタ情報のグループと、当該グループに属する各個別フィルタ情報と、その各個別フィルタ情報を条件とする運用ルール情報との対応関係を示す情報を予測イベント対応表記憶手段に記憶させる。

30

## 【0101】

ルール判定手段は、予測イベントデータ生成手段が予測イベントデータを生成した後に、当該予測イベントデータを生成するために用いたイベントデータに合致する個別フィルタ情報が属するグループと予測イベント一覧で対応付けられた各イベントデータが、そのグループに対応する運用ルール情報の個別フィルタ情報を満足しているか否かを判定し、満足している場合に運用ルール情報が定める処理を実行する。

40

## 【発明の効果】

## 【0102】

本発明では、運用ルール情報毎に定められた条件となる情報であって、属性と属性値とを対応づけた情報であり、属性値の一部が過去のイベントデータから推測される参考値として記述されることがあり、また、属性値の一部が変数として記述されることがある個別フィルタ情報を用いるとともに、個別フィルタ情報で変数として記述された属性値に管理

50

対象システムで生成されたイベントデータの属性値を代入したデータである予測イベントデータを用いる。そして、上述のような予測イベント一覧記憶手段、予測イベント対応表記憶手段、予測イベントデータ合致判定手段を備える。従って、環境に適合したルール条件を定めることができ、ルール判定の精度を高めることができる。

【0103】

また、予測イベントデータ合致判定手段は、イベントデータと、実際に発生するイベントデータと形式が似た予測イベントデータとが合致するか否かを判定するため、複数のイベントデータ間の関連記述がし易く、予め発生が予想されるイベントデータを優先的に処理することができる。そのため、条件式の全比較が必要な関連技術の運用管理装置に比べて、大幅に処理速度を向上できる。この結果、大規模環境等、ルール条件の多い環境にも適用することができる。

10

【0104】

さらにまた、相関関係等の環境依存条件を具体的な値に展開した予測イベントデータを生成することで、例えば、機器構成やソフトウェア挙動に変化があった場合等に、予測された値との差異が検出され、管理者に提示し対処を促すことができる。この結果、環境変化に追従して運用ルール情報を洗練していく作業を支援することができ、効率的な運用を実現できる。

【図面の簡単な説明】

【0105】

【図1】本発明の第1の実施の形態に係る運用管理装置の構成を示すブロック図である。

20

【図2】第1の実施の形態における予測イベントデータを生成する動作のフローチャートである。

【図3】第1の実施の形態における個別フィルタ情報の例を示す説明図である。

【図4】第1の実施の形態における予測イベントデータの例を示す説明図である。

【図5】図2に示すステップS713の処理経過の例を示すフローチャートである。

【図6】図5に示すステップS601で抽出されたイベントデータの例を示す説明図である。

【図7】第1の実施の形態におけるイベントデータの例を示す説明図である。

【図8】第1の実施の形態における予測イベント対応表の例を示す説明図である。

【図9】第1の実施の形態におけるフィルター一覧を示す説明図である。

30

【図10】第1の実施の形態における予測イベント一覧を示す説明図である。

【図11】図2に示すステップS714の動作を示すフローチャートである。

【図12】第1の実施の形態におけるユーザ対話手段が表示する画面の例を示す説明図である。

【図13】第1の実施の形態における予測イベント対応表の遷移の例を示す説明図である。

【図14】第1の実施の形態における予測イベント一覧の遷移の例を示す説明図である。

【図15】第1の実施の形態における個別フィルタ情報の例を示す説明図である。

【図16】第1の実施の形態における修正されたフィルタ情報の例を示す説明図である。

【図17】第1の実施の形態における修正された個別フィルタ情報の例を示す説明図である。

40

【図18】第1の実施の形態における修正された予測イベントデータの例を示す説明図である。

【図19】本発明の第2の実施の形態に係る運用管理装置の構成を示すブロック図である。

【図20】第2の実施の形態におけるイベントデータの例を示す説明図である。

【図21】第2の実施の形態における予測イベント対応表の遷移の例を示す説明図である。

【図22】第2の実施の形態における予測イベント一覧の遷移の例を示す説明図である。

【図23】第2の実施の形態における予測イベント一覧の遷移の例を示す説明図である。

50

【図 2 4】本発明の第 3 の実施の形態に係る運用管理装置の構成を示すブロック図である。

【図 2 5】関連技術の運用管理装置の構成例を示すブロック図である。

【図 2 6】( a ) および ( b ) は、関連技術におけるイベントデータの例を示す説明図である。

【図 2 7】( a ) および ( b ) は、関連技術における運用ルール情報およびフィルタ情報の例を示す説明図である。

【図 2 8】関連技術における分析状態表の例を示す説明図である。

【図 2 9】関連技術の運用管理装置の動作の例を示すフローチャートである。

【符号の説明】

10

【 0 1 0 6 】

- 2 イベントデータ取得手段
- 3 判定条件蓄積手段
- 4 イベント分析手段
- 5 ユーザ対話手段
- 6 制御手段
- 7 イベント蓄積手段
- 8 予測イベント蓄積手段
- 9 予測イベント管理手段
- 1 0 予測イベント分析手段
- 1 1 ジョブ管理手段
- 3 1 運用管理装置

20

【発明を実施するための最良の形態】

【 0 1 0 7 】

以下、本発明の実施の形態に係る運用管理装置、運用管理方法および運用管理プログラムについて、図面を参照して説明する。

【 0 1 0 8 】

( 第 1 の実施の形態 )

図 1 は、本発明の第 1 の実施の形態に係る運用管理装置の構成を示すブロック図である。図 2 5 に示す関連技術の運用管理装置 4 1 の構成要素と同様の構成要素については、図 2 5 と同一の符号を付し説明を省略する。

30

【 0 1 0 9 】

図 1 に示す本実施の形態の運用管理装置 3 1 は、図 2 5 に示す関連技術の運用管理装置が備えるイベントデータ取得手段 2、イベント蓄積手段 7、イベント分析手段 4、判定条件蓄積手段 3、ユーザ対話手段 5、制御手段 6 に加えて、予測イベント蓄積手段 8 と、予測イベント管理手段 9 と、予測イベント分析手段 1 0 とを備える。

【 0 1 1 0 】

予測イベント蓄積手段 8 は、判定条件蓄積手段 3 に蓄積される運用ルール情報毎に管理されたフィルタ情報である個別フィルタ情報と、将来発生が期待されるイベントデータを示す予測イベントデータとを記憶する記憶装置である。ここで、運用ルール情報毎に管理されるとは、個々の運用ルール情報毎に用意されるということを意味する。

40

【 0 1 1 1 】

例えば、関連技術の運用管理装置において、1つのフィルタ情報は、複数の運用ルール情報の組み合わせ情報として指定されることがあった。本実施の形態における個別フィルタ情報は、1つの運用管理情報にのみ対応する。個別フィルタ情報は、後述の予測イベント対応表(図 8 参照。)に示すように、運用ルール情報に対応付けられている。

【 0 1 1 2 】

図 8 に示す例では、例えば、運用ルール情報 R 0 1 2 0 に個別フィルタ情報 F 1 0 1 1、F 1 0 1 2 が対応付けられている。個別フィルタ情報 F 1 0 1 1、F 1 0 1 2 はそれぞれ運用ルール情報 R 0 1 2 0 のみに対応し、他の運用ルール情報には対応付けられていな

50

い。また、個別フィルタ情報および予測イベントデータの例については後述する。

【0113】

予測イベント管理手段9は、判定条件蓄積手段3に蓄積される各々の運用ルール情報の組み合わせ条件で指定されるフィルタ情報と、イベント蓄積手段7に蓄積される過去のイベントデータの履歴とから個別フィルタ情報を生成して、個別フィルタ情報を予測イベント蓄積手段8に記憶させる。個別フィルタ情報を生成する動作の例については後述する。

【0114】

なお、運用ルール情報の組み合わせ条件で指定されるフィルタ情報は、関連技術の運用管理装置におけるフィルタ情報と同様の情報である。予測イベント管理手段9がフィルタ情報から個別フィルタ情報を生成するのではなく、管理者によってユーザ対話手段5を介して予測イベント管理手段9に個別フィルタ情報が入力され、予測イベント管理手段9が管理者によって入力された個別フィルタ情報を予測イベント蓄積手段8に記憶させてもよい。

10

【0115】

また、予測イベント管理手段9が個別フィルタ情報を生成する際に、個別フィルタ情報をユーザ対話手段5に表示させ、管理者に修正された場合には修正された個別フィルタ情報を予測イベント蓄積手段8に記憶させる態様であってもよい。このように、予測イベント管理手段9が管理者と対話的に個別フィルタ情報を生成してもよい。

【0116】

予測イベント分析手段10には、イベントデータ取得手段2からイベントデータが入力される。予測イベント分析手段10は、予測イベント蓄積手段8に蓄積される個別フィルタ情報から予測イベントデータを生成して予測イベント蓄積手段8に記憶させる。

20

【0117】

また、予測イベント分析手段10は、入力されたイベントデータが予測イベントデータ、個別フィルタ情報に合致するか否かを判定する処理を行う。また、その判定結果をイベント分析手段4に出力する。入力されたイベントデータが予測イベントデータ、個別フィルタ情報に合致するか否かを判定する処理は、後述のステップS721、S723の処理であり、処理の詳細については後で述べる。

【0118】

さらに、イベント分析手段4は、図25を用いて説明した機能に加えて、予測イベント分析手段10から判定結果が入力され、合致したイベントデータに対応する運用ルール情報の判定を行う機能も有する。この判定処理は、後述のステップS726の処理であり、処理の詳細については後で述べる。また、イベント分析手段4は、予測イベントまたは個別フィルタに含まれる推測された属性値がイベントデータと一致しない場合にユーザ対話手段5を介して管理者に確認を促す機能も有する。

30

【0119】

図2は、本実施の形態の運用管理装置が予測イベントデータを生成する動作のフローチャートである。以下、図3および図4を用いて個別フィルタ情報および予測イベントデータを説明した上で、本発明の動作について説明する。

【0120】

図3は、本実施の形態の運用管理装置で用いられる個別フィルタ情報の例を示す説明図である。個別フィルタ情報は、フィルタ情報に含まれる属性のうち属性値が定められていない属性に対して参考値を追加した情報である。参考値とは、過去にサービスシステム1から受信したイベントデータから推測される属性値である。以下の説明では、参考値となる属性値は“ [ ”および“ ] ”という括弧の記号で囲んで表すこととする。フィルタ情報の複数の属性に対して参考値を付加して個別フィルタ情報を生成してもよい。

40

【0121】

図3に示す個別フィルタ情報211は、図27(b)に示すフィルタ情報201のTIME1(イベントデータ発生時刻)の属性およびSERVERの属性に対して参考値を追加して得られた個別フィルタ情報の例を示している。同様に、図3に示す個別フィルタ情

50

報 2 1 2 は、図 2 7 ( b ) に示すフィルタ情報の T I M E 1 の属性および S O U R C E の属性に対して参考値を追加して得られた個別フィルタ情報の例を示している。

【 0 1 2 2 】

また、個別フィルタ情報に対しては、個別フィルタ情報を一意に識別するための番号が付与される。例えば、個別フィルタ情報 2 1 1 では、他の個別フィルタ情報やフィルタ情報と区別するために、F 1 0 1 1 という番号が記述されている。本例では、図 2 7 ( b ) のフィルタ情報 2 0 1 から図 3 の個別フィルタ情報 2 1 1 を生成するとき、番号を F 1 0 1 1 に変更している。

【 0 1 2 3 】

参考値は、例えば、変数を用いて記述される。本例では、変数を \$ 記号から始まる文字列で表している。図 3 に示す例では “ \$ F 0 1 ” や “ \$ F 0 2 ” 等の変数で参考値が記述されている。また、複数のイベントデータがそれぞれ異なる個別フィルタ情報に合致していることを表す際に、その複数のイベントデータの属性値に相関性があるという条件も含めて表現しなければならない場合がある。その場合には、複数の個別フィルタ情報で同一の変数（変数でなくてもよい。）を記述していればよい。

10

【 0 1 2 4 】

図 3 に示す変数 “ \$ F 0 1 ” および “ \$ F 0 2 ” は、個別フィルタ情報 2 1 1、2 1 2 それぞれで用いられている。また、図 3 に示す “ P E R I O D ( \$ F 0 1 , \* ) ” は、変数 \$ F 0 1 から一定期間内であることを表している。また、複数の個別フィルタ情報において参考値として共通の変数を用いて、その変数で表された参考値も含めて複数のイベントデータが個々の個別フィルタ情報にそれぞれ合致している場合、イベントデータに相関があるという。また、異なる個別フィルタ情報間で共通の変数を用いて表された参考値を相関情報と記す。図 3 に示す例では、\$ F 0 1、\$ F 0 2、P E R I O D ( \$ F 0 1 , \* ) がそれぞれ相関情報に該当する。

20

【 0 1 2 5 】

また、参考値は、変数ではなく、具体的な値であってもよい。例えば、個別フィルタ情報に、[ S V 4 ] 等の変数を用いない参考値が付加されていてもよい。そして、そのような具体的な値を用いた参考値を複数の個別フィルタ情報に記述して相関性を表してもよい。

【 0 1 2 6 】

図 4 は、本実施の形態の運用管理装置が生成する予測イベントデータの例を示す説明図である。予測イベントデータは、個別フィルタ情報に記述された変数を、検出されたイベントデータの属性値で置き換えた情報である。図 4 に示す予測イベントデータ 2 2 1、2 2 2 は、それぞれ図 3 に示す個別フィルタ情報 2 1 1、2 1 2 の変数をイベントデータ内の属性値で置き換えた情報である。

30

【 0 1 2 7 】

また、予測イベントデータを生成する際にも、予測イベントデータを識別する番号が予測イベントデータに記述される。例えば、図 4 に示す予測イベントデータでは、他の情報と区別するために F 1 1 1 1 という番号が記述されている。本例では、図 3 の個別フィルタ情報 2 1 1 から図 4 の予測イベントデータ 2 2 1 を生成するとき、番号を F 1 1 1 1 に変更している。

40

【 0 1 2 8 】

以下、図 2 7、図 1、図 2、図 3、図 4 を参照して、本実施の形態における予測イベントデータ生成の動作を説明する。

【 0 1 2 9 】

まず、管理者によって、ユーザ対話手段 5 に運用ルール情報の修正指示が入力され、ユーザ対話手段 5 は、修正指示に従い（すなわち管理者に操作に従い）、判定条件蓄積手段 3 に記憶された運用ルール情報を修正する（ステップ S 7 1 1）。

【 0 1 3 0 】

ステップ S 7 1 1 では、新たな運用ルール情報がユーザ対話手段 5 に入力され、ユーザ

50

対話手段 5 がその運用ルール情報を判定条件蓄積手段 3 に記憶させてもよい。ここでは、判定条件蓄積手段 3 に記憶されていた運用ルール情報 R 0 1 2 0 の組み合わせ条件が、図 2 7 ( a ) に例示するように “ F 0 0 1 1 AND F 0 0 1 2 ” に修正されたとする。

【 0 1 3 1 】

続いて、予測イベント管理手段 9 は、入力された運用ルール情報（修正された運用ルール情報）の組み合わせ条件が示すフィルタ情報 2 0 1 およびフィルタ情報 2 0 2 を判定条件蓄積手段 3 から読み出し、個別フィルタ情報として予測イベント蓄積手段 8 に記憶させる（ステップ S 7 1 2）。この時点では、予測イベント蓄積手段 8 に記憶された個別フィルタ情報は、判定条件蓄積手段 3 に記憶されたフィルタ情報と同一である。

【 0 1 3 2 】

続くステップ S 7 1 3 において、予測イベント蓄積手段 8 に記憶された個別フィルタ情報に参考値を追加する。なお、ステップ S 1 2 および後述のステップ S 1 3 の動作は、運用ルール情報毎に行う。

【 0 1 3 3 】

ステップ S 7 1 2 の後、予測イベント管理手段 9 は、イベント蓄積手段 7 からイベントデータを読み出し、個別フィルタ情報に合致する過去のイベントデータの特性に基づいて参考値を追加する（ステップ 7 1 3）。

【 0 1 3 4 】

図 2 7 ( b ) に示すフィルタ情報の属性値は、イベントデータがフィルタ情報と合致すると判定されるために、イベントデータの属性値が必ず一致しなければならない値である。一方、個別フィルタ情報に含まれる参考値は、サービスシステム 1 の使用環境で過去に発生したイベントデータによく現れていたことを示すものであり、一致する可能性が高い値を示す。

【 0 1 3 5 】

ステップ S 7 1 3 における参考値の導出は、過去のイベントデータを統計的に解析する一般的な手法により実現できる。以下、予測イベント管理手段 9 がステップ S 7 1 3 において参考値を導出する動作について説明する。なお、以下に示す参考値の導出動作は一例であり、他の動作で参考値を導出してよい。

【 0 1 3 6 】

図 5 は、ステップ S 7 1 2 で予測イベント蓄積手段 8 に記憶された個別フィルタ情報に参考値を追加するステップ S 7 1 3 の処理経過の例を示すフローチャートである。予測イベント管理手段 9 は、イベント蓄積手段 7 に記憶されている過去のイベントデータから、ステップ S 7 1 1 で判定条件蓄積手段 3 に記憶された運用ルール情報の組み合わせ条件に合致する各イベントデータを抽出する（ステップ S 6 0 1）。

【 0 1 3 7 】

例えば、ステップ S 7 1 1 で、図 2 7 ( a ) に例示する運用ルール情報 R 0 1 2 0 が判定条件蓄積手段 3 に記憶された場合、予測イベント管理手段 9 は、イベント蓄積手段 7 に記憶されている過去のイベントデータから、運用ルール情報 R 0 1 2 0 の組み合わせ条件として指定されたフィルタ情報 2 0 1 およびフィルタ 2 0 2（図 2 7 ( b ) 参照。）に合致するイベントデータを抽出する。このとき、予測イベント管理手段 9 は、組み合わせ条件で指定された各フィルタ情報毎に合致するイベントデータの検索に成功した時点で、その各フィルタ条件に合致するイベントデータの集合を抽出する。

【 0 1 3 8 】

図 6 は、このようにステップ S 6 0 1 で抽出されたイベントデータの例を示す説明図である。

【 0 1 3 9 】

図 6 に示す例では、運用ルール情報 R 0 1 2 0 の組み合わせ条件で指定されたフィルタ情報 2 0 1、2 0 2（図 2 7 参照。）に合致するイベントデータ E 8 0 1 0、E 8 0 2 0 が抽出されていることを示している。このイベントデータ E 8 0 1 0、E 8 0 2 0 は、2 0 0 6 年 6 月 2 9 日の時点で生成されていたイベントデータである。予測イベント管理手

10

20

30

40

50

段 9 は、フィルタ情報 201、202 に合致するイベントデータ E8010、E8020 を検索した時点で、そのイベントデータ E8010、E8020 の集合を抽出する。

【0140】

同様に、図 6 に示す例では、フィルタ情報 201、202 (図 27 参照。) に合致するイベントデータ E8030、E8040 が抽出されていることを示している。このイベントデータ E8030、E8040 は、2006 年 10 月 2 日の時点で生成されていたイベントデータである。予測イベント管理手段 9 は、フィルタ情報 201、202 に合致するイベントデータ E8030、E8040 を検索した時点で、そのイベントデータ E8030、E8040 の集合を抽出する。

【0141】

これらのイベントデータは、月末にパッチの適用が行われた後に次の業務を開始したときに異常が発生したことを示している。イベントデータ E8010、E8020 は、6 月末に管理者が手動でパッチ適用を実行して異常が発生したことを示している。イベントデータ E8030、E8040 は、9 月末に自動でパッチ適用が実行されて異常が発生したことを示している。

【0142】

ステップ S601 の後、予測イベント管理手段 9 は、同種のイベントデータに共通する属性値を抽出する (ステップ S602)。ここで、「同種のイベントデータ」とは、ステップ S601 で抽出されたイベントデータのうち、同一のフィルタ情報に合致すると判定されたイベントデータである。

【0143】

例えば、図 6 に示す例では、イベントデータ E8010、E8030 は、いずれも図 27 (b) に示すフィルタ情報 201 に合致していると判定されているので同種のイベントデータに該当する。同様に、イベントデータ E8020、E8040 は、いずれもフィルタ情報 202 (図 27 (b) 参照。) に合致していると判定されているので、同種のイベントデータに該当する。

【0144】

予測イベント管理手段 9 は、同種のイベントデータ E8010、E8030 から、共通する属性値を抽出する。すなわち、発生元を示す SOURCE の「updater」と EVENTID の「4001」を抽出する。ただし、これらの属性値は、すでにフィルタ情報 201 に記述されている値であり、参考値として追加される属性値ではない。

【0145】

同様に、予測イベント管理手段 9 は、同種のイベントデータ E8020、E8040 から、共通する属性値「BIZAP」、「8000」を抽出するが、これらもフィルタ情報 202 に記述された値であり、参考値として追加される値ではない。

【0146】

続いて、予測イベント管理手段 9 は、組み合わせ条件となるフィルタ情報 201、202 に合致するものとして抽出されたイベントデータの集合毎に、イベントデータ間の相関性を特定する (ステップ S603)。すなわち、予測イベント管理手段 9 は、組み合わせ条件との 1 回の条件判定で合致すると判定されたイベントデータの組毎に、イベントデータ間の相関性を特定する。

【0147】

予測イベント管理手段 9 は、まず、イベントデータ E8010、E8020 の属性値を比較して、相関性を特定する。予測イベント管理手段 9 は、この 2 つのイベントデータ E8010、E8020 の属性値をそれぞれ比較し、一致する属性値および発生日時の順番を特定する。すると、以下の比較結果 (比較結果 1 とする。) が得られる。

【0148】

- ・種類が「不明」で一致
- ・日付が「2006 / 6 / 29」で一致
- ・時刻は、E8010の方が先に発生

10

20

30

40

50

- ・発生元のサーバが「S V 2」で一致
- ・ユーザが「root」で一致・説明の最初の文字列が「手動：」で一致

## 【0149】

イベントデータE8010、E8020の属性値の比較により、以上の5つの相関関係が判明し、この比較結果が参考値の候補となる。

## 【0150】

同様に、予測イベント管理手段9は、イベントデータE8030、E8040の属性値を比較して相関性を特定する。すると、以下の比較結果（比較結果2とする。）が得られる。

## 【0151】

- ・時刻は、E8030の方が先に発生
- ・発生元のサーバが「S V 3」で一致

## 【0152】

イベントデータE8030、E8040の属性値の比較により、以上の2つの相関関係が判明する。

## 【0153】

予測イベント管理手段9は、イベントデータの集合毎の比較結果として得た相関関係から共通する相関関係を特定する。本例では、比較結果1、2において、以下の相関関係が共通している。

## 【0154】

- ・時刻は、フィルタ情報201に合致するイベントの方が先に発生
- ・発生元のサーバが一致

## 【0155】

予測イベント管理手段9は、共通していた相関関係を参考値として個別フィルタ情報に追加する（ステップS604）。また、同種のイベントデータに共通する属性値であってフィルタ情報に記述されていない属性値をステップS602で抽出していた場合には、予測イベント管理手段9は、その属性値を相関値として個別フィルタ情報に追加する。

## 【0156】

ステップS604において、共通していた相関関係を参考値として個別フィルタ情報に追加する場合、予測イベント管理手段9は、一致する事項（上記の例ではサーバ）に関しては、共通の変数を用いて表した参考値を各個別フィルタ情報に追加すればよい。また、時間の前後関係を表す場合には、例えば、個別フィルタ情報間で共通の変数を用い、さらに、上述のPERIOD等の所定の表現を用いた参考値をフィルタ情報に追加すればよい。ここでは、PERIODという表現を用いた場合を例示したが、参考値として、変数と他の計算式の組み合わせで示される式を追加してもよい。また、変数のみを参考値として追加してもよい。

## 【0157】

図3は、このようにして生成された個別フィルタ情報の例であり、“[ ”と” ]”で囲まれた記述が参考値を示す。\$F01や\$F02は変数を表し、個別フィルタ情報211と個別フィルタ情報212の間で一致する情報であることを示す。この例では、この運用ルール情報の組み合わせ条件に合致すると判定される2つのイベントデータでは、SERVER属性の値が一致し、発生時刻は個別フィルタ情報212に合致するイベントデータが後（PERIOD（\$F01、\*）は\$F01以降の期間を示す処理関数）になることを示す。

## 【0158】

図6で説明したように、この実行環境では、過去の例から手動で実行される場合と自動で実行される場合とがあり、それぞれで属性値や説明に違いが発生する。また、これまでの実績では、異常は、同じサーバからのイベントデータとなっている。図3に示す参考値では、このような実行環境に依存する条件が適切に設定されている。

## 【0159】

10

20

30

40

50

なお、上記の参考値の生成方法の説明では、属性値が完全に一致する場合と、属性値の順序関係が判明した場合という簡単な例で説明したが、この例に限定されるものではない。参考値の導出は、一般に知られている情報の構造解析手法やマイニング手法を利用して参考値を推定することによって行ってもよい。

【 0 1 6 0 】

上記の例示した手法以外の手法であっても、過去のイベントデータが有する特徴から出現確率の高い属性値の候補あるいは相関関係が決定できるものであれば、本発明の個別フィルタ情報に参考値として記述することができ、実行環境に依存した条件として利用できるものである。また、管理者が個別フィルタ情報を生成し、ユーザ対話手段 5 を介して予測イベント管理手段 9 にその個別フィルタ情報が入力され、予測イベント管理手段 9 がその個別フィルタ情報を予測イベント蓄積手段 8 に記憶させてもよい。

10

【 0 1 6 1 】

また、予測イベント管理手段 9 は、個別フィルタ情報を他の情報と区別して一意を表す番号を識別情報として個別フィルタ情報に記述する。図 3 に示す例では、個別フィルタ 2 1 1、2 1 2 にそれぞれ番号 F 1 0 1 1、F 1 0 1 2 が記述されている。

【 0 1 6 2 】

以上のように個別フィルタ情報に参考値を追加する処理を行った後、イベントデータ取得手段 2 が新たにイベントデータを受信してそのイベントデータを予測イベント分析手段 1 0 に出力した場合、予測イベント分析手段 1 0 は、そのイベントデータと予測イベント蓄積手段 8 に記憶された個別フィルタ情報とのマッチングを行う。そして、イベントデータが個別フィルタ情報に合致する場合には、予測イベント分析手段 1 0 は、個別フィルタ情報の参考値をイベントデータの属性値に置き換えた情報を個別フィルタ情報とは別に生成する（ステップ S 1 4）。この情報が予測イベントデータである。

20

【 0 1 6 3 】

例えば、ステップ S 7 1 3 で、図 3 に例示する個別フィルタ情報 2 1 1、2 1 2 が予測イベント蓄積手段 8 に記憶されたとする。その状態で、イベントデータ取得手段 2 が予測イベント分析手段 1 0 に対して、個別フィルタ情報 2 1 1 に合致するイベントデータを出力したとする。すると、予測イベント分析手段 1 0 は、そのイベントデータに含まれる属性値で参考値の値を書き換えた予測イベントデータを生成する（ステップ S 7 1 4）。

【 0 1 6 4 】

図 4 に示す予測イベントデータ 2 2 1 は、このようにして生成された予測イベントデータである。また、このとき参考値に含まれる変数をイベントデータの属性値に置き換えたならば、その変数を記述した他の個別フィルタ情報においても、その変数を属性値に置き換えた予測イベントデータを生成する。

30

【 0 1 6 5 】

本例では、個別フィルタ情報 2 1 2（図 3 参照。）の変数を置き換えた予測イベントデータ 2 2 2（図 4 参照。）を生成する。予測イベントデータ 2 2 1 は、既に発生したイベントデータに対応するものであるが、予測イベントデータ 2 2 2 は、まだ発生していないイベントデータを示している。図 4 に示す予測イベントデータは、SERVER が「SV 4」であるイベントデータが入力される可能性が高いことを示している。ステップ S 7 1 4 の動作の詳細は、図 1 1 を用いて後述する。

40

【 0 1 6 6 】

以下、図 7 に例示するイベントデータがサービスシステム 1 から送られる場合を例にして説明する。図 7 に例示するイベントリスト 1 1 0 では、番号が E 9 0 0 2 であるイベントデータの発生元が SV 4 である点で、図 2 6 に示すイベントリスト 1 0 0 と異なる。また、図 7 に例示するイベントリスト 1 2 0 は、イベントリスト 1 1 0 が生成された状態からさらに時間が経過して E 9 0 0 5 ~ E 9 0 0 8 のイベントデータが追加されたイベントリストである。

【 0 1 6 7 】

図 8 は、本発明の運用管理装置が用いる予測イベント対応表の例を示す説明図である。

50

予測イベント対応表は、運用ルール情報と、個別フィルタ情報と、予測イベントデータとの対応関係を示す情報である。また、1つの運用ルール情報に対応する個別フィルタ情報のグループには、運用ルール情報の番号と一対一に対応するグループの番号が割り当てられる。この割り当ては、例えば、予測イベント管理手段9が行う。

【0168】

予測イベント対応表では、具体的には、上記のグループを識別する番号と、そのグループの番号に対応する運用ルール情報の番号と、個別フィルタ情報の組み合わせ（フィルタ系列と呼ぶことにする。）と、予測イベントデータの生成状況を示す監視状況とが対応付けられている。

【0169】

図8に示す予測イベント対応表401、402、403は、それぞれ、図7に示すイベントデータE9001、E9003、E9003が検出された時点での予測イベント対応表を示している。イベントデータE9001～E9003の検出に伴い、図8に示すように予測イベント対応表の内容は遷移する。

【0170】

グループの番号と、運用ルール情報の番号と、フィルタ系列との対応関係は、運用ルール情報が修正されなければ変化しない。予測イベント対応表におけるグループの番号と、運用ルール情報の番号と、フィルタ系列との対応関係を示す部分は、ステップS713で運用ルール情報に対応する個別フィルタ情報を作成した後に、予測イベント管理手段9がグループの番号を新たに割り当てて作成し、運用管理装置の記憶装置（予測イベント対応表記憶手段）に記憶させておけばよい。ただし、他のタイミングで作成してもよい。また、監視状況の部分はイベントデータの入力に応じて書き換えられる。

【0171】

図9は、本発明の運用管理装置が用いるフィルタ一覧を示す説明図である。フィルタ一覧は、各個別フィルタ情報の番号毎に、個別フィルタ情報が属するフィルタ系列（グループ）の番号を対応付けた情報である。また、図9に示す個別フィルタ情報210は、フィルタ一覧で列挙される個別フィルタ情報の一例を示す。

【0172】

なお、図9に示す個別フィルタ情報210には参考値が付加されていないが、付加すべき参考値が存在しない場合には、個別フィルタ情報と、フィルタ情報は番号以外が共通の情報となる。フィルタ一覧では、個別フィルタ情報が列挙され、それぞれの個別フィルタ情報に対応するグループの番号が記述される。

【0173】

個別フィルタ情報に合致するイベントデータを予測イベント分析手段10が検出した場合、予測イベント分析手段10は、その個別フィルタ情報に対応するグループの番号をフィルタ一覧から特定することができ、さらにその番号に対応する運用ルール情報や予測イベントデータを予測イベント対応表（図8参照。）を参照して特定することができる。

【0174】

さらに、運用ルール情報の番号から、図27(a)に示す運用ルール情報に含まれる対処内容を特定することができる。フィルタ一覧は、例えば、ステップS713で運用ルール情報に対応する個別フィルタ情報を作成した後に、予測イベント管理手段9が作成し、運用管理装置の記憶装置に記憶させておけばよい。フィルタ一覧の作成タイミングは、他のタイミングであってもよい。

【0175】

図10は、本発明の運用管理装置が用いる予測イベント一覧を示す説明図である。予測イベント一覧は、予測イベントデータを識別する番号と、予測イベントデータに対応するグループの番号と、予測イベントデータに合致したイベントデータの番号と、対応する運用ルール情報の各個別フィルタ情報が示す条件の判定が完了しているか否かを示す情報とを含む。

【0176】

10

20

30

40

50

図10に示す予測イベント一覧321、322、323は、それぞれイベントデータE9001、E9002、E9003が検出された場合の予測イベント一覧を示し、それぞれ図8に示す予測イベント対応表401、402、403と対応している。例えば、予測イベント対応表が図8に示す予測イベント対応表401のようになっている場合、予測イベント一覧は図10に示す予測イベント一覧321のようになっている。予測イベント一覧は、運用管理装置が備える記憶装置(予測イベント一覧記憶手段)に記憶される。

【0177】

図11は、上述のステップS714の動作を示すフローチャートである。また、図12は、ユーザ対話手段5が表示する画面の例を示す説明図である。

【0178】

図2を用いて説明した通り、管理者からユーザ対話手段5に運用ルール情報R0120(図27参照。)が入力されると、ユーザ対話手段5は、その運用ルール情報R0120を判定条件蓄積手段3に記憶される。すると、予測イベント管理手段9は図3に例示する個別フィルタ情報を生成し予測イベント蓄積手段8に記憶させる(ステップS711~S713)。運用ルール情報R0110、運用ルール情報R0130に対応する個別フィルタ情報も同様にして生成される。

【0179】

予測イベント管理手段9は、運用ルール情報毎にグループ番号を割り当て、個々の個別フィルタ情報の番号と、個別フィルタ情報に対応する運用ルール情報に対して割り当てたグループの番号とを対応付けたフィルタ一覧311(図9参照。)を生成する。

【0180】

次に、図7に示すイベントデータが順次発生する場合を例にして説明する。サービスシステム1が動作状態に応じたイベントデータE9001を生成し、イベントデータ取得手段2がそのイベントデータを受信すると、イベントデータ取得手段2はそのイベントデータを予測イベント分析手段10に出力する。予測イベント分析手段10は、イベントデータ取得手段2からイベントデータが入力されると、ステップS14の処理を行う。具体的には、図11に示す動作を行う。

【0181】

まず、予測イベント分析手段10は、イベントデータ取得手段2から入力されたイベントデータE9001と、予測イベントデータとのマッチングを行う(ステップS721)。ステップS721では、予測イベントデータに含まれる参考値以外の属性値と、入力されたイベントデータに含まれる属性値とが一致するか否かを判定する。

【0182】

また、予測イベントデータの属性値として参考値でない変数がある場合には、その参考値でない変数とイベントデータの属性値との合致判定は行わなくてよい。ただし、予測イベントデータが生成されていない場合には、イベントデータと予測イベントデータは一致しないことになる(ステップS722のNo)。ここでは、予測イベントデータが存在していない状態から説明する。従って、イベントデータと予測イベントデータは一致しないことになり、ステップS723に移行する。

【0183】

ステップS723では、入力されたイベントデータE9001と個別フィルタ情報とのマッチング(フィルタ判定処理)を行う。具体的には、予測イベント分析手段10は、フィルタ一覧311(図9参照。)に列挙される個別フィルタ情報を1つずつ予測イベント蓄積手段8から読み込み、イベントデータと個別フィルタ情報とが合致するか否かを判定する。

【0184】

予測イベント分析手段10は、個別フィルタ情報に含まれる参考値以外の属性値が全てイベントデータに含まれる属性値と一致していれば合致すると判定し、そうでなければ合致しないと判定する。合致しなければ、次の個別フィルタ情報を1つ読み込み同様に、イベントデータと合致するか否かを判定する。

10

20

30

40

50

## 【 0 1 8 5 】

予測イベント分析手段 1 0 は、イベントデータと個別フィルタ情報とが合致するか、あるいは、イベントデータと合致するか否かを判定していない個別フィルタ情報が存在しなくなるまで、上記の動作を繰り返す。この繰り返し処理は、図 2 9 に示すステップ S 7 0 2 ~ S 7 0 4 の繰り返し処理と同様である。

## 【 0 1 8 6 】

本例では、予測イベント分析手段 1 0 は、イベントデータ E 9 0 0 1 と番号が F 1 0 1 0 である個別フィルタ情報 2 1 0 ( 図 9 参照。 ) とが合致すると判定し ( ステップ S 7 2 3 およびステップ S 7 2 4 の Y e s )、ステップ S 7 2 5 に移行する。

## 【 0 1 8 7 】

ステップ S 7 2 5 において予測イベント分析手段 1 0 は、フィルター一覧 3 1 1 を参照し、イベントデータと合致すると判定した個別フィルタ情報の番号に対応するグループの番号 ( 本例では G 0 1 1 0。図 9 参照。 ) を抽出する。そして、予測イベント分析手段 1 0 は、そのグループの番号に対応する新たな予測イベントデータを生成する ( ステップ S 7 2 5 )。

10

## 【 0 1 8 8 】

ステップ 7 2 3 でイベントデータと合致すると判定された個別フィルタ情報がある場合、その個別フィルタ情報は、運用ルール情報の組み合わせ条件となる複数のフィルタ情報から生成された個別フィルタ情報のうちの一つの個別フィルタ情報である。すなわち、ステップ S 7 2 3 からステップ S 7 2 5 に移行したということは、運用ルール情報に対応する個別フィルタ情報のいずれかに合致する最初のイベントデータが入力されていたという状況に該当する。

20

## 【 0 1 8 9 】

このように、ステップ S 7 2 3 からステップ S 7 2 5 に移行した場合、予測イベント分析手段 1 0 は、個別フィルタ情報の変数に、入力されたイベントデータの属性値を代入し、識別情報となる番号を付与した予測イベントデータを生成する。

## 【 0 1 9 0 】

そして、ステップ 7 2 3 でイベントデータと合致すると判定された個別フィルタ情報と同じグループに属する他の個別フィルタ情報があり、その個別フィルタ情報に上記の変数と同一の変数が含まれていれば、その変数にイベントデータの値を代入した予測イベントデータも生成する。

30

## 【 0 1 9 1 】

そして、予測イベント分析手段 1 0 は、予測イベント対応表の監視状況を示す情報として、個別フィルタ情報の番号に対応付けて個別フィルタ情報の番号を予測イベント対応表に記述する ( 図 8 に示す予測イベント対応表 4 0 1 参照。 )。

## 【 0 1 9 2 】

さらに、予測イベント分析手段 1 0 は、予測イベントデータの番号 ( ここでは F 1 1 1 0 とする。 ) と、グループの番号と、イベントデータの番号 ( ここでは E 9 0 0 1 ) とを対応付けた予測イベント一覧を作成する ( 図 1 0 に示す予測イベント一覧 3 2 1 参照。ただし、「済」という情報はこの時点では付加されていない。 )。

40

## 【 0 1 9 3 】

また、予測イベント分析手段 1 0 は、予測イベント対応表 4 0 1 ( 図 8 参照。 ) から、グループの番号に対応する運用ルール情報の番号 R 0 1 1 0 を特定し、その番号の運用ルール情報、イベントデータ、および運用ルール情報に対応する個別フィルタ情報をイベント分析手段 4 に出力する。このとき、予測イベント分析手段 1 0 は、イベントデータとして、運用ルール情報に対応するグループ番号を特定し、さらに予測イベント一覧においてそのグループ番号に対応付けられている各イベントデータをイベント分析手段 4 に出力する。

## 【 0 1 9 4 】

イベント分析手段 4 は、予測イベント分析手段 1 0 から入力された運用ルール情報の条

50

件とイベントデータとが合致するか否かを判定する（ステップS726）。すなわち、予測イベント分析手段10から入力された運用ルール情報に対応する各個別フィルタ情報とイベントデータとが合致するか否かを判定する。

**【0195】**

本例では、運用ルール情報に対応する個別フィルタ情報が1つだけであり、その個別フィルタ情報（F1010）はイベントデータE9001に合致するので、運用ルール情報の条件とイベントデータとが合致すると判定されることになる。しかし、運用ルール情報R0110（図27参照）は、対処を指定していないので、対処は実行されない。

**【0196】**

この場合、イベント分析手段4は、「何も行わない」という処理をユーザ対話手段5を介して管理者に提示するとともに制御手段6に通知する。ユーザ対話手段5は、同時にこの対処の結果（「何も行わない」という表示を完了したこと）を予測イベント管理手段9に通知する。すると、予測イベント管理手段9は、対処が完了したことから図10の予測イベント一覧321の判定項目に「済」を記述し、ステップ721へ戻る。

**【0197】**

同様に、サービスシステム1が図7に示すイベントデータE9002を生成し運用管理装置に送信してイベントデータ取得手段2がそのイベントデータを受信した結果、予測イベント分析手段10にイベントデータ取得手段2からイベントデータE9002が入力されたとする。すると、既に説明した場合と同様に、予測イベント分析手段10は、そのイベントデータE9002と予測イベントデータとのマッチングを行う（ステップS721）。

**【0198】**

この時点で、図10に示す予測イベント一覧321に示すように、番号がF1110の予測イベントデータが存在するが、対応するイベントデータと運用ルール情報の条件との判定が行われたことを示す「済」という情報が付加されているので、番号がF1110の予測イベントデータは、ステップS721でのマッチングの対象にならない。よって、ここでは、イベントデータE9002と予測イベントデータとが一致しないと判定し（ステップS722のNo）、ステップS723に移行する。

**【0199】**

予測イベント分析手段10は、イベントデータE9002と、図3に示す個別フィルタ情報211（番号F1011）とが合致すると判定し（ステップS723、ステップS724のYes）、ステップS725に移行する。ステップS725において予測イベント分析手段10は、フィルター一覧311を参照し、イベントデータと合致すると判定した個別フィルタ情報の番号に対応するグループの番号（本例ではG0120。図9参照）を抽出する。そして、予測イベント分析手段10は、そのグループの番号に対応する新たな予測イベントデータを生成する（ステップS725）。

**【0200】**

ここでは、ステップS723からステップS725に移行しているので、予測イベント分析手段10は、個別フィルタ情報の変数に、入力されたイベントデータの属性値を代入し、識別情報となる番号を付与した予測イベントデータを生成する。すなわち、イベントデータE9002と合致する個別フィルタ情報211（番号F1011）の変数に、イベントデータE9002の属性値を代入した予測イベントデータを生成する。

**【0201】**

具体的には、個別フィルタ情報211（番号F1011）の変数（図3参照。）に、イベントデータE9002のTIME1およびSERVERの属性値を代入した予測イベントデータ（図4に示す番号F1111の予測イベントデータ）を生成する。予測イベント分析手段10は、予測イベントデータを他の情報と区別するために識別情報となる番号（ここではF1111）を付与する。

**【0202】**

そして、ステップ723でイベントデータと合致すると判定された個別フィルタ情報と

10

20

30

40

50

同じグループに属する他の個別フィルタ情報（図3に示す番号がF1012の個別フィルタ情報）があり、その個別フィルタ情報に同一の変数が含まれている。

【0203】

従って、予測イベント分析手段10は、その個別フィルタ情報（番号F1012）の変数にイベントデータE9002の属性値を代入した予測イベントデータも生成する。具体的には、個別フィルタ情報212（番号F1012）の変数（図3参照。）に、イベントデータE9002のTIME1およびSERVERの属性値を代入した予測イベントデータ（図4に示す番号F1112の予測イベントデータ）を生成する。

【0204】

また、予測イベント分析手段10は、予測イベントデータの番号（ここではF1110とする。）と、グループの番号と、イベントデータの番号とを対応付けた情報を予測イベント一覧に追加する。

【0205】

この結果、図10に示す予測イベント一覧322が得られる。番号F1111と、グループ番号G0120と、イベントデータE9002とを対応付けた情報が追加されている。また、番号F1112の予測イベントデータは、イベントデータE9002に合致する個別フィルタ情報と同じグループの個別フィルタ情報から生成されているので、対応するイベントデータはこの時点で存在していない（図10に示す予測イベント一覧322参照。）。

【0206】

また、予測イベント分析手段10は、生成した予測イベントデータの番号（F1111、F1112）を、グループ番号120に対応付けて予測イベント対応表の「監視状況」に記述する（図8に示す予測イベント対応表402参照。）。

【0207】

予測イベント分析手段10は、予測イベント対応表402（図8参照。）から、グループの番号に対応する運用ルール情報の番号R0120を特定し、その番号の運用ルール情報、イベントデータ、および運用ルール情報に対応する個別フィルタ情報をイベント分析手段4に出力する。

【0208】

イベント分析手段4は、予測イベント分析手段10から入力された運用ルール情報に対応する各個別フィルタ情報とイベントデータとが合致するか否かを判定する（ステップS726）。ここでは、図3に示す個別フィルタ情報212（番号F1012）に合致するイベントデータが揃っていないので、番号R0120の運用ルール情報の条件は満たされていないと判定する。その後、予測イベント分析手段10は、新たなイベントデータの入力を待つ。

【0209】

さらに、イベントデータE9003（図7参照。）が予測イベント分析手段10に入力された場合には、イベントデータE9001が入力されたときと同様の動作を行う。すると、新たな予測イベントデータ（番号F1210とする。）が生成され、また、ステップS726のルール判定処理が行われる。また、この結果、図8に示す予測イベント対応表403および図10に示す予測イベント一覧323が得られる。

【0210】

ここで、続いてイベントデータE9004が発生した場合を例として、管理者によるフィルタ情報修正時の動作について説明する。イベントデータE9004（図7参照。）は、SERVER属性の値を除いて、図4に示す予測イベント情報222と合致する。予測イベントデータ222におけるSERVER属性は参考値であり、「SV4」を想定しているが、実際に発生したイベントデータE9004では「SV3」となっている。

【0211】

関連技術の運用管理装置の説明で用いた図26のイベントリスト100では、発生元が同じ「SV3」というコンピュータであったが、図7に示すイベントリスト110では、

10

20

30

40

50

「SV3」と「SV4」という2つの発生元がある。これは、例えば、「SV3」のみで運用していたシステムに「SV4」を追加した場合に相当する。関連技術の運用管理装置では、このように機器の種類が増えた場合、その環境変化に合わせてフィルタ情報を修正しなければ管理者の望む動作が得られないことになる。

【0212】

図10に示す予測イベント一覧323の状態、イベントデータE9004が予測イベント分析手段10に入力されると、予測イベント分析手段10がイベントデータE9004と予測イベントデータとのマッチングを行う(ステップS721)。

【0213】

図13は予測イベント対応表の遷移の例を示す説明図であり、図14は予測イベント一覧の遷移の例を示す説明図である。図13に示す予測イベント対応表404~406は、それぞれ図14に示す予測イベント一覧324~326に対応している。上記のように、予測イベント分析手段10が、イベントデータE9004と予測イベントデータとが合致しているか否かを判定する処理(ステップS721)では、イベントデータE9004と図4に示す予測イベントデータ(番号F1112)とが合致すると判定する(ステップS722のYes)。

10

【0214】

また、イベントデータと予測イベントデータとが合致したと判定したとき、予測イベント分析手段10は、予測イベントデータ(番号F1112)に合致するイベントデータの番号を予測イベント一覧に記述する。この結果、図10に示す予測イベント一覧323が、図14に示す予測イベント一覧324に遷移する。このときの予測イベント対応表は、図13に示す予測イベント対応表404である。

20

【0215】

イベントデータと予測イベントデータとが合致した場合、ステップS727に移行し、予測イベント分析手段10は、イベントデータの属性値と予測イベントデータの参考値が合致しているか否かを判定する(ステップS727)。イベントデータの属性値と予測イベントデータの参考値が合致していれば(ステップS727のYes)、ステップS725に移行する。イベントデータの属性値と予測イベントデータの参考値が合致していなければ(ステップS727のNo)、ステップS721で予測イベントデータと合致したイベントデータおよび、参考値とイベントデータの属性値との比較情報(比較結果)をイベント分析手段4に出力する。

30

【0216】

イベント分析手段4は、ユーザ対話手段5を介して管理者にイベントデータ、参考値とイベントデータの属性値との比較結果を提示する(ステップS728)。図12の画面901は、このようにして出力された画面の例である。画面901は、参考値が一致しないことを示すメッセージ表示欄902と、運用ルール情報および個別フィルタ情報の概要を参考値と共に示すツリー表示欄903と、現在のイベントデータの内容および項目毎のマッチング結果を示すデータ表示欄904と、管理者による入力を受け取るボタン905、906とを含む。

【0217】

40

図12に例示する画面では、ツリー表示欄903で、参考値である「SV4」がイベントデータの属性値と異なっていることを示す「」印を提示し、データ表示欄904で、項目毎の比較結果を、、、xで表している。は、一致していることを表し、は参考値と一致していないことを表している。管理者はこの画面を参照して、イベントデータE9004を合致するルールとして運用ルール情報を受け入れるか、または、フィルタ情報を変更して再判定を行うかを選択することができる。ボタン906は、フィルタ情報を変更することを指示するボタンであり、ボタン905は、フィルタ情報を変更しないことを指示するボタンである。

【0218】

イベントデータと予測イベントデータとでSERVERの属性値が異なっても両者

50

が合致していると判断してよい場合として、同じ機器が複数の別名を持つ場合や、複数の機器が連携しているため業務ソフトウェアへの影響がある場合等が考えられる。

【0219】

この場合、管理者が画面901で例示した「このイベントで判定」のボタン905を押下すると、予測イベント管理手段9は、フィルタ情報の変更を行わないという指示が入力されたと判定し(ステップS729のNo)、ステップS725に移行する。ステップS725では、予測イベント分析手段10は予測イベントデータの生成を行う(ステップ725)。

【0220】

ここで、ステップS723を経ずに、ステップS727の判定を行ってから、ステップS75に以降しているということは、運用ルール情報に対応する個別フィルタ情報のいずれかに合致する2番目以降のイベントデータが入力されているということである。このとき、運用ルール情報に対応する個別フィルタ情報のいずれかに合致するイベントデータが入力されてステップS723を経てステップS725に移行したときに、その最初のイベントデータの属性値が、同じグループに属する各個別フィルタ情報に入力されて各個別フィルタ情報に対応する予測イベントデータが作成されている。

10

【0221】

従って、ステップS723を経ずに、ステップS727を経て、ステップS725に移行した場合、予測イベント分析手段10は、個別フィルタ情報の参考値にイベントデータの属性値を代入して予測イベントデータを生成する動作を行わなくてよい。

20

【0222】

ステップS725では、予測イベント分析手段10は、既に説明したように、運用ルール情報、イベントデータ、および運用ルール情報に対応する個別フィルタ情報をイベント分析手段4に出力する処理も行う。

【0223】

この後、イベント分析手段4は、S726の判定処理を行うが、運用ルール情報の条件が満たされると判定され、運用ルール情報の対処が実行されるのは、運用ルール情報に対応する個別フィルタ情報のいずれかに合致する最後のイベントデータが入力されて(すなわち、各個別フィルタに合致するイベントデータが入力済みとなって)ステップS727からステップS725、S726に移行した場合(運用ルール情報に対応する個別フィルタが1つしかない場合にはステップS723からステップS725、S726に移行した場合)である。

30

【0224】

また、フィルタ情報を変更しないという指示を入力するためのボタン905が押下されたということは、運用ルール情報R0120の判定にイベントデータE9004を用いたということである。このことから、運用ルール情報の満たすための条件として推定されていたイベントデータSERVER属性も一致しているという条件は満たす必要がないことになる。

【0225】

よって、予測イベント管理手段9は、運用ルール情報R0120に対応する個別フィルタ情報を特定し、その個別フィルタ情報からイベントデータのSERVER属性が一致するという条件を表す参考値を削除する。なお、予測イベント対応表で運用ルール情報と個別フィルタ情報とが対応付けられているので、予測イベント対応表を参照することで運用ルール情報に対応する個別フィルタ情報を特定できる。

40

【0226】

この場合、予測イベント管理手段9は、運用ルール情報R0120に対応する個別フィルタ情報(番号F1011、F1012。図3参照。)からそれぞれ、SERVER属性が一致するという条件を表す参考値[ \$ F 0 2 ]を削除して、図15に示す個別フィルタ情報211、212(番号F1011、F1012)を再生成し、予測イベント蓄積手段8に記憶させる。この結果、イベントデータの属性値と参考値との不一致が解消したこと

50

になる。

【 0 2 2 7 】

なお、フィルタ情報を変更しないという指示を入力するためのボタン 9 0 5 が押下された場合 (ステップ S 7 2 9 の N o )、予測イベント管理手段 9 は個別フィルタ情報の変更を行うがこの処理は図 1 1 において省略している。また、変更されるのは個別フィルタ情報であって、フィルタ情報ではない。

【 0 2 2 8 】

ステップ S 7 2 5 の後、イベント分析手段 4 は、ルール判定処理を行う (ステップ S 7 2 6 )。すなわち、予測イベント分析手段 1 0 から入力された運用ルール情報に対応する各個別フィルタ情報とイベントデータとが合致するか否かを判定する。ここではイベントデータは、運用ルール R 0 1 2 0 の条件 (運用ルール R 0 1 2 0 の個別フィルタ情報) を満足するので対処が実行される。

10

【 0 2 2 9 】

また、イベントデータと予測イベントデータとで S E R V E R の属性値が同一である必要がある場合、管理者は、図 1 2 に例示した「条件を変更する」のボタン 9 0 6 を押下する。ボタン 9 0 6 が押下されると、予測イベント管理手段 9 は、フィルタ情報の変更を行うという指示が入力されたと判定し (ステップ S 7 9 2 の Y e s )、参考値とイベントデータの属性値が一致しなければならないことを反映するように、判定条件蓄積手段 3 に記憶されているフィルタ情報 (ここでは運用ルール情報 R 0 1 2 0 のフィルタ情報) を修正する。

20

【 0 2 3 0 】

具体的には、運用ルール情報 R 0 1 2 0 の組み合わせ条件として指定されている各フィルタ情報の S E R V E R 属性の属性値として共通の変数を記述する。この変数は参考値としない。本例では、“ [ ] ” という括弧で囲まずに変数を記述する。図 1 6 は、このようにして修正されたフィルタ情報を示す。

【 0 2 3 1 】

予測イベント管理手段 9 は、運用ルール情報 R 0 1 2 0 で指定された各フィルタ情報 2 0 1、2 0 2 (図 2 7 ( b ) 参照。) の S E R V E R 属性の属性値として共通の変数「 \$ S V 」を追加記述し、図 1 6 に示すフィルタ情報 2 0 1、2 0 2 を判定条件蓄積手段 3 に記憶させる。

30

【 0 2 3 2 】

この結果、各フィルタ条件 2 0 1、2 0 2 に合致するイベントデータの S E R V E R 属性の属性値が同じであることが、運用ルール情報 R 0 1 2 0 の条件として追加されたことになる。また、予測イベント管理手段 9 は、フィルタ情報が変更したことに伴い、そのフィルタ情報から生成された個別フィルタ情報、およびその個別フィルタ情報から生成された予測イベントデータに対しても、フィルタ情報に対する修正と同様の修正を行う (ステップ S 7 3 0 )。

【 0 2 3 3 】

本例では、予測イベント管理手段 9 は、図 3 個別フィルタ情報 2 1 1、2 1 2 の S E R V E R 属性をそれぞれ参考値である [ \$ F 0 2 ] から、参考値でない同一の変数 \$ S V に修正する。図 1 7 に示す個別フィルタ情報 2 1 3、2 1 4 は、このように修正された個別フィルタ情報を示している。

40

【 0 2 3 4 】

また、予測イベント管理手段 9 は、図 4 に示す各予測イベントデータの S E R V E R 属性を参考値から、参考値でない属性値に修正する。本例では、参考値を示す “ [ ] ” を削除することによって参考値 [ S V 4 ] を、参考値でない属性値 S V 4 に修正する。図 1 8 に示す予測イベントデータ 2 1 3、2 1 4 は、このように修正された予測イベントデータを示している。

【 0 2 3 5 】

以上のようにフィルタ情報、個別フィルタ情報および予測イベントデータを修正した後

50

、ステップS721に戻り、予測イベント分析手段10は、入力されたイベントデータE9004に対して再度ステップS721以降の処理を行う。

【0236】

すると、予測イベント分析手段10は、発生元（すなわちSERVER属性）がSV3として記述されたイベントデータE9004と、SERVER属性がSV4（参考値ではない。）である予測イベントデータ224（図18参照。）とが合致しないと判定する（ステップS721、ステップS722のNo）。すなわち、イベントデータE9004は、既に入力されているイベントデータE9002とは関連しないイベントデータとして扱われることになる。

【0237】

続いて、ステップS723の処理を行い、ステップS725に移行する。ステップS723からステップS725に移行しているため、予測イベント分析手段10は、個別フィルタ情報の変数に、入力されたイベントデータの属性値を代入し、識別情報となる番号を付与した予測イベントデータを生成する。すなわち、図4に示す予測イベントデータ221、222（番号F1111、F1112）を生成した動作と同様の動作で、予測イベントデータを生成する。

【0238】

なお、ステップS730で、個別フィルタ情報が修正されているので、新たな予測イベントデータが生成される。ここで、番号F1211の予測イベントデータと番号F1212の予測イベントデータが生成されたとする。

【0239】

また、予測イベント分析手段10は、予測イベント一覧322（図10参照）を得る動作と同様にして同様にして、図14に示す予測イベント一覧324に情報を追加して、図14に示す予測イベント一覧325を生成する。予測イベント一覧325では、E9004とF1212が対応付けられていて、イベントデータE9004に合致する個別フィルタ情報から予測イベントデータF1212が生成され、その個別フィルタ情報と同じグループの個別フィルタ情報から予測イベントデータF1211が生成されていることを表している。

【0240】

また、予測イベント分析手段10は、予測イベント対応表のルール番号R0120に対応する監視状況として、F1211、F1212を追加する。この結果、予測イベント対応表404（図13参照。）は、予測イベント対応表405（図13参照。）に遷移する。なお、F1211とF1212は、TIME1属性の参考値によって、F1211が先に発生することが期待されている。既にF1212が先に発生した状態で、F1211に合致するイベントデータが後で発生すると、同様に参考値との不一致がある場合の処理が行われることになる。

【0241】

このようにして、新たなイベントが発生する度に、予測イベントデータの生成やマッチングが行われる。図7のイベントリスト120は、さらにイベントデータが生成された例である。イベントデータE9005が予測イベント分析手段10に入力されると、図14に示す予測イベント一覧325は予測イベント一覧326に遷移する。なお、このとき、図13に示す予測イベント対応表405は、予測イベント対応表406に遷移する。

【0242】

予測イベント一覧326に示すように、イベントデータE9005は、F1112に合致し、運用ルール情報R0120の判定が真となって、「SV4」での対処が行われる。この対処の結果がイベントデータE9006（図7参照。）である。さらに、イベントデータE9007が、予測イベントデータF1211に対応するため、同様に「SV3」での対処が行われ、結果がイベントデータE9008で示される。

【0243】

このように、本実施の形態によれば、管理者が汎用的な論理によって運用ルール情報を

10

20

30

40

50

作成した場合に、その条件に過去の履歴から実行環境に依存する条件が自動的に付与された予測イベントデータが生成される。環境依存の条件（例えば、イベントデータの発生元のサーバが同一である等の条件）によって環境に適合するように変数で記述されたルール条件となるため、ルール判定の精度を高めることができる。

【0244】

また、環境依存の条件設定が自動化され、管理者が指定する条件が分離されているため、条件記述が複雑になることがなく、類似環境に運用ルール情報を適用しやすい。この結果、管理者が運用ルール情報を扱う場合の作業負担が大幅に減少し、適用範囲が拡大するという効果がある。

【0245】

さらに、本実施の形態によれば、発生したイベントデータに応じて予測イベントデータが生成される。論理的な条件式による判定ではなく、実際に発生するイベントデータと形式が似た予測イベントデータとのマッチングによって判定されるため、複数のイベントデータ間の相関記述がし易く、予め発生が予想されるイベントデータを優先的に処理することができるため、条件式の全比較が必要な関連技術の運用管理装置に比べて、大幅に処理速度を向上できる。この結果、大規模環境等、ルール条件の多い環境にも適用可能である。

【0246】

さらにまた、相関関係等の環境依存条件を具体的な値に展開した予測イベントデータを生成することで、例えば、機器構成やソフトウェア挙動に変化があった場合等に、予測された値との差異が検出され、管理者に提示し対処を促すことができる。この結果、環境変化に追従して運用ルール情報を洗練していく作業を支援することができ、効率的な運用を実現できる。

【0247】

なお、本実施の形態では、フィルタ情報が異なる運用ルール情報を例として動作を説明したが、その例に固定されるものではなく、複数ルールで共通のフィルタ情報を指定されるものであっても良い。この場合でも、共通するフィルタ情報から運用ルール情報毎の個別フィルタ情報が生成されて、予測イベントデータを生成することができる。

【0248】

また、本実施の形態では、過去のイベントデータから参考値を生成する例で説明したが、その例に固定されるものではなく、一般に知られている特長分析の技術を用いて他の種類の情報から生成するものであっても、管理者によって直接入力されるものであっても良い。いずれの場合においても、発生するイベントデータと同様の系列を持つ予測イベントデータを生成し、そのイベントデータ間の相関や参考値が指定できるものであれば、同様の効果が得られるものである。

【0249】

なお、予測イベント一覧や予測イベント対応表を変更するタイミングは、第1の実施の形態で説明したタイミングに限定されない。

【0250】

（第2の実施の形態）

図19は、本発明の第2の実施の形態を示すブロック図である。図1に示す第1の実施の形態の運用管理装置31と同様の構成要素については、図1と同一の符号を付し説明を省略する。

【0251】

第2の実施の形態の運用管理装置31は、図1に示す第1の実施の形態の運用管理装置が備えるイベントデータ取得手段2、イベント蓄積手段7、イベント分析手段4、判定条件蓄積手段3、ユーザ対話手段5、制御手段6、予測イベント蓄積手段8、予測イベント管理手段9、予測イベント分析手段10に加えて、ジョブ管理手段11を備える。

【0252】

ジョブ管理手段11は、定期的な処理の実行や条件分岐等の手順を有する処理の実行計

10

20

30

40

50

画に従って制御手段に指示を行うとともに、処理の実行に伴って発生するイベントデータの予定を予測イベント管理手段 9 に通知する。

【 0 2 5 3 】

ジョブ管理手段 1 1 は、制御手段 6 に対し、サービスシステム 1 に処理を実行させる指示を、予め定められたタイミングで出力する。制御手段 6 は、この指示がジョブ管理手段 1 1 から入力されると、サービスシステム 1 に処理を実行させる。サービスシステム 1 のイベントデータ生成手段 7 1 は、処理の実行に伴ってイベントデータを順次生成し、運用管理装置 3 1 に送信する。

【 0 2 5 4 】

また、ジョブ管理手段 1 1 は、サービスシステム 1 による処理の実行に伴ってサービスシステム 1 から順次送信されるイベントデータに合致する個別フィルタ情報を予め記憶しておく。そして、ジョブ管理手段 1 1 は、処理の実行に伴って発生するイベントデータの予定を表す情報として、その個別フィルタ情報を予測イベント管理手段 9 に出力する。このとき、ジョブ管理手段 1 1 は、発生するイベントデータの順番にあわせて、各イベントデータに合致する個別フィルタ情報の順番を指定して個別フィルタ情報を予測イベント管理手段 9 に出力する。

10

【 0 2 5 5 】

なお、ジョブ管理手段 1 1 は、予測イベント管理手段 9 に出力する個別フィルタ情報およびその順番の情報を予め記憶する。ジョブ管理手段 1 1 が制御手段 6 に指示を出力することでサービスシステム 1 が実行する処理は予め決まっているので、どのようなイベントデータが順次発生するのかも予めわかっている。

20

【 0 2 5 6 】

従って、管理者がその各イベントデータに合致する個別フィルタ情報を作成して順番を指定してジョブ管理手段 1 1 に入力し、ジョブ管理手段 1 1 が各個別フィルタ情報および順番を記憶しておけばよい。

【 0 2 5 7 】

ジョブ管理手段 1 1 は、例えば、サービスシステム 1 に処理を実行させる時刻を予め記憶し、その時刻になったときに、処理の実行に伴って生成される各イベントデータに対応する各個別フィルタ情報およびその順番を予測イベント管理手段 9 に出力すればよい。

【 0 2 5 8 】

予測イベント管理手段 9 は、第 1 の実施の形態で説明した処理に加えて、ジョブ管理手段 1 1 から受け取ったイベントデータの予定（すなわち順番が指定された個別フィルタ情報）に従って、予測イベントデータを生成する機能を新たに有する。

30

【 0 2 5 9 】

以下、図 2 0 に示すイベントリスト 1 3 0 に含まれる各イベントデータがサービスシステム 1 から送られる場合を例にして説明する。図 2 0 に示すイベントデータ E 9 0 0 1、E 9 0 0 2、E 9 0 0 3 は、図 7 に示すイベントデータ E 9 0 0 1、E 9 0 0 2、E 9 0 0 3 と同様である。また、図 2 0 に示すイベントデータ E 2 0 0 1、E 2 0 0 2、E 2 0 0 3 は、ジョブの実行に伴って順次生成されるイベントデータである。ただし、E 2 0 0 3 は、ジョブ実行時にエラーが生じた場合に生成されるイベントデータである。

40

【 0 2 6 0 】

図 2 1 は、本実施の形態における予測イベント対応表の遷移の例を示す説明図である。図 2 2 および図 2 3 は、本実施の形態における予測イベント一覧の遷移の例を示す説明図である。

【 0 2 6 1 】

以下、本実施の形態における運用管理装置の動作を説明する。

【 0 2 6 2 】

ジョブ管理手段 1 1 は、所定のタイミング（例えば予め定められた日時）になると、制御手段 6 に対し、サービスシステム 1 に処理を実行させる指示を出力する。また、このとき、ジョブ管理手段 1 1 は、サービスシステム 1 が処理の実行に伴い生成する各イベント

50

データに合致する個別フィルタ情報を、順番を指定して予測イベント管理手段 9 に出力する。

【 0 2 6 3 】

制御手段 6 は、ジョブ管理手段 1 1 からの指示に従ってサービスシステム 1 に処理を実行させる。すると、サービスシステム 1 はその処理の実行に伴いイベントデータを順次生成して運用管理装置 3 1 に送信する。例えば、サービスシステム 1 は、その処理に含まれる個々の処理ステップの成否を示すイベントデータを順次生成して運用管理装置 3 1 に送信する。

【 0 2 6 4 】

その結果、運用管理装置 3 1 には、図 2 0 に示すように、サービスシステム 1 が提供する業務サービスのイベントデータ（例えば、E 9 0 0 1、E 9 0 0 2、E 9 0 0 3）に混じって、ジョブ管理手段 1 1 の指示に起因して実行した処理（ジョブ）のイベントデータ（図 2 0 に示す E 2 0 0 1、E 2 0 0 2、E 2 0 0 3）も送信される。例えば、図 2 0 に示すイベントデータ E 2 0 0 1 は、「S V 3」というコンピュータ上の j o b というソフトウェア機能が「J O B 1」という処理の実行に成功したことを示す。

10

【 0 2 6 5 】

また、予測イベント管理手段 9 は、このようなイベントデータの発生予定をジョブ管理手段 1 1 から個別フィルタ情報として受け取り、予測イベント蓄積手段 8 に記憶させる。そして、その個別フィルタの集合を 1 つのグループとして、グループ番号を割り当てる。

【 0 2 6 6 】

そして、予測イベント管理手段 9 は、ジョブ管理手段 1 1 から入力された個別フィルタ情報をフィルタ系列として個々の個別フィルタ情報の番号（本例では F 2 0 0 1、F 2 0 0 2、F 2 0 0 3 とする。）と、割り当てたグループの番号（G 0 2 0 0 とする。）とを対応付けて予測イベント対応表に追加する。

20

【 0 2 6 7 】

このとき、運用ルール情報の番号は対応付けない。個別フィルタ情報の順番は、F 2 0 0 1、F 2 0 0 2、F 2 0 0 3 の順であるものとする。図 2 1 に示す予測イベント 4 1 0 において、G 0 2 0 0 は上述のグループの番号であり、対応するルール番号はなく、フィルタ系列としてイベントデータの発生予定を示す個別フィルタ情報 F 2 0 0 1、F 2 0 0 2、F 2 0 0 3 が設定されている。

30

【 0 2 6 8 】

この例では、F 2 0 0 1、F 2 0 0 2、F 2 0 0 3 のフィルタ系列は、ジョブが成功した場合に順次発生するイベントデータに合致する個別フィルタ情報である。イベントデータ E 2 0 0 3 は、ジョブがエラーになったときに生成されるイベントデータであり、その場合、管理者へのメール通知を行うという対象を定めた運用ルール情報 R 0 1 3 0 が適用され、図 2 7 に示すように管理者へのメール通報を行う対処が実行される。従って、ジョブ成功時のイベントデータに対応する個別フィルタ情報 F 2 0 0 3 は、イベントデータ E 2 0 0 3 とは合致しない。

【 0 2 6 9 】

図 2 3 に示すイベントデータ E 9 0 0 1 が生成され、予測イベント分析手段 1 0 に入力されると、予測イベント分析手段 1 0 は、ステップ S 7 2 1 以降の処理を行う。イベントデータ E 9 0 0 1 が入力されたときに、イベントデータ E 9 0 0 1 と合致する予測イベントデータは存在せず、また、イベントデータ E 9 0 0 1 と合致する個別フィルタ F 2 0 0 1 は、ジョブ管理手段 1 1 から予測イベント管理手段 9 に送られ、予測イベント蓄積手段 8 に記憶されている。

40

【 0 2 7 0 】

従って、ステップ S 7 2 1 からステップ S 7 2 3 を経てステップ S 7 2 5 の処理を行う。予測イベント分析手段 1 0 は、予測イベントデータとして、F 2 1 0 1 と F 2 1 0 2 を生成する。ここでは、入力されたイベントデータが E 2 0 0 1 であり、予測イベント分析手段 1 0 は、そのイベントデータに続く次のイベントデータに対応する予測イベントデー

50

タも生成する。その予測イベントデータが F 2 1 0 2 である。

【 0 2 7 1 】

次のイベントデータに対応する予測イベントデータは、同じグループ内の次の個別フィルタ情報を用いて、第 1 の実施の形態と同様に作成すればよい。この個別フィルタ情報はジョブ管理手段 1 1 が出力した個別フィルタ情報であり、順番も指定されているので、次のイベントデータに対応する次の個別フィルタ情報を特定して予測イベントデータを生成することができる。

【 0 2 7 2 】

予測イベント分析手段 1 0 は、イベントデータ E 2 0 0 1 と、グループ番号 G 0 2 0 0 と、E 2 0 0 1 から生成した予測イベントデータ F 2 1 0 1 とを対応付けた情報を予測イベント一覧に追加する。また、グループ番号 G 0 2 0 0 と、F 2 1 0 2 とを対応付けた情報を予測イベント一覧に追加する。E 2 0 0 1 に続くイベントデータはまだ入力されていないので、F 2 1 0 2 に対応するイベントデータはこの時点ではない。図 2 2 に示す予測イベント一覧 3 3 1 は、この状態の予測イベント一覧を表している。

10

【 0 2 7 3 】

また、予測イベント分析手段 1 0 は、生成した予測イベントデータ F 2 1 0 1、F 2 1 0 2 を、グループ番号 G 0 2 0 0 およびフィルタ系列 F 2 0 0 1、F 2 0 0 2、F 2 0 0 3 に対応付けて、予測イベント対応表の監視状況に記述する。

【 0 2 7 4 】

図 2 1 に示す予測イベント対応表 4 1 0 は、この状態の予測イベント対応表を表している。ジョブ実行に関するイベントデータは順次発生するものであるため、ジョブに関する 1 つのイベントデータが入力された場合、予測イベント分析手段 1 0 は、次のイベントに対応する予測イベントデータを生成し、予測イベント対応表 4 1 0 に記述する（図 2 1 に示す予測イベント対応表 4 1 0 参照。）。

20

【 0 2 7 5 】

同様に、イベントデータ E 9 0 0 2 およびイベントデータ E 2 0 0 2 が生成され予測イベント分析手段 1 0 に入力されると、ステップ S 7 2 1 以降の処理を行い、図 2 2 に示す予測イベント一覧 3 3 2 を導出する。すなわち、E 9 0 0 2 と、グループ番号 G 0 1 2 0 と、新たに生成した予測イベントデータ F 1 1 1 1 とを対応付けた情報、および新たな予測イベントデータ F 1 1 1 2 とグループ番号 G 0 1 2 0 とを対応付けた情報を予測イベント一覧に追加する。この動作は第 1 の実施の形態と同様である。

30

【 0 2 7 6 】

また、イベントデータ E 2 0 0 2 と、グループ番号 G 0 2 0 0 と、新たに生成した予測イベントデータ F 2 1 0 2 とを対応付けた情報を予測イベント一覧に追加する。さらに、次のイベントデータに対応する予測イベントデータも作成し（F 2 1 0 3 とする。）、F 2 1 0 3 とグループ番号 G 0 2 0 0 とを対応付けた情報を予測イベント一覧に追加する（図 2 2 に示す予測イベント一覧 3 3 2 ）。

【 0 2 7 7 】

イベントデータ E 2 0 0 3 が発生せず（すなわちエラーが発生せず）、正常に終了した場合のイベントデータが予測イベント分析手段 1 0 に入力された場合もステップ S 7 2 1 以降の処理を行い、予測イベント分析手段 1 0 は、そのイベントデータを予測イベント一覧 3 3 2 において、F 2 1 0 3 および G 0 2 0 0 に対応付けて記述し、G 0 2 0 0 に対応する各予測イベントデータに関する処理が終わったことを示す情報（本例では「済」）を記述する。

40

【 0 2 7 8 】

また、ジョブが正常に終了せず、ジョブの異常終了を示すイベントデータ E 2 0 0 3 が生成されて、予測イベント分析手段 1 0 に入力されたとする。予測イベント分析手段 1 0 は、ステップ S 7 2 1 以降の処理を行う。この場合、ステップ S 7 2 1 からステップ S 7 2 3 に以降し、正常終了時の個別フィルタ情報 F 2 0 0 1、F 2 0 0 2、F 2 0 0 3 のグループとは合致せず、他の個別フィルタ情報（F 1 0 1 3 とする。）と合致し、ステップ

50

S 7 2 5 に移行する。

【 0 2 7 9 】

予測イベント分析手段 1 0 は、予測イベントデータ ( F 1 1 1 3 とする。 ) を生成し、 F 1 1 1 3、 G 0 1 3 0、 E 2 0 0 3 を対応付けた情報を予測イベント一覧に追加する ( 図 2 3 に示す予測イベント一覧 3 3 3 )。既に説明したように、 E 2 0 0 3 発生時には、ルール R 0 1 3 0 が適用されるものであり、個別フィルタ情報 F 1 0 1 3 は、 R 0 1 3 0 に対応付けられているものとする。

【 0 2 8 0 】

予測イベント分析手段 1 0 は、 G 0 1 3 0、 R 0 1 3 0、 F 1 0 1 3 に対応する情報として、生成した予測イベントデータの番号 F 1 1 1 3 を予測イベント対応表に追加する ( 図 2 1 に示す予測イベント対応表 4 1 1 参照。 )。 10

【 0 2 8 1 】

この後、ステップ S 7 2 6 に以降し、さらに運用ルール情報 R 0 1 3 0 の対処が実行される。すなわち、管理者へのメール通知が行われる。この通知を受けた管理者は、異常終了としてジョブを中断してもよい。あるいは、サービスシステム 1 を復旧させてもよい。

【 0 2 8 2 】

予測イベント管理手段 9 は、ユーザ対話手段 5 を介して、ジョブを終了する旨の情報が入力された場合、ジョブ管理手段 1 1 から入力された個別フィルタ情報をフィルタ系列としている情報を予測イベント対応表から削除する。 20

【 0 2 8 3 】

本例では、予測イベント対応表 4 1 1 ( 図 2 1 参照。 ) から G 0 2 0 0 と、 F 2 0 0 1、 F 2 0 0 2、 F 2 0 0 3 と、 F 2 1 0 1、 F 2 1 0 2 を対応付けた情報を削除する。図 2 1 に示す予測イベント対応表 4 1 2 は、このときの予測イベント対応表を表している。また、予測イベント管理手段 9 は、そのグループ番号 G 0 2 0 0 に対応付けられた情報を予測イベント一覧から削除する。この結果得られる予測イベント一覧は、図 2 3 に示す予測イベント一覧 3 3 4 である。

【 0 2 8 4 】

また、管理者がサービスシステム 1 を復旧させ、正常に終了したときのイベントデータが運用管理装置に送信する。このイベントデータが予測イベント分析手段 1 0 に入力されると、ステップ S 7 2 1 以降の処理を行う。この結果、予測イベント分析手段 1 0 は、そのイベントデータを予測イベント一覧 3 3 3 において、 F 2 1 0 3 および G 0 2 0 0 に対応付けて記述し、 G 0 2 0 0 に対応する各予測イベントデータに関する処理が終わったことを示す情報 ( 本例では「済」 ) を記述する。 30

【 0 2 8 5 】

なお、本例では、ジョブの異常終了を示すイベントデータ E 2 0 0 3 に応じた運用ルール情報 R 0 1 3 0 で、管理者へのメール通知を定めた例を示したが、異常終了を示すイベントデータ E 2 0 0 3 に応じた運用ルール情報 R 0 1 3 0 において、ジョブ管理手段 1 1 から入力された個別フィルタ情報に基づいて生成した情報 ( 本例では、グループ番号 G 0 2 0 0 に対応する情報 ) を、予測イベント対応表や予測イベント一覧から削除するコマンドを定めていてもよい。 40

【 0 2 8 6 】

また、サービスシステム 1 がジョブ終了の通知を予測イベント管理手段 9 に送信し、予測イベント管理手段 9 は、その通知を受信したときにそのジョブに関連する情報 ( 本例では、グループ番号 G 0 2 0 0 に対応する情報 ) を、予測イベント対応表や予測イベント一覧から削除してもよい。

【 0 2 8 7 】

以上のように、本実施の形態によれば、ジョブ実行に伴って計画的に発生が予想されるイベントデータを予測イベントデータとマッピングして迅速に処理することができるため、ジョブ実行に伴い多数のイベントデータが発生しても、他の運用ルール情報の条件判定に影響を与えることがない。 50

## 【0288】

ジョブは、日時指定等によって計画的に行われるものであり、ジョブに対応するイベントデータの発生日時や系列も予め定められている。しかしながら、曜日によって実行時間をシフトしたり、エラーになった場合の処理等様々な手順が規定されているため、そのようなジョブの手順をすべて理解できないと発生するイベントデータの系列を予測することができない。また、複雑な手順に対応するルール条件として正確に記述することも難しい。

## 【0289】

関連技術の運用管理装置では、他のルール条件と同様に記述して処理していたため、多数の正常イベントによって処理負荷が増大したり、他の条件と合致してしまって誤判定となったりするような問題があった。これに対して、本実施の形態の運用管理装置は、運用ルール情報の条件から予測イベントデータを生成してマッチングする方法であるため、論理条件式の判定ではなく、順次発生するイベントデータの系列として、ジョブ実行のイベントデータを効率的に処理することができる。

10

## 【0290】

(第3の実施の形態)

図24は、本発明の第3の実施の形態を示すブロック図である。第1の実施の形態、第2の実施の形態の運用管理装置31と同様の構成要素については、図1および図19と同一の符号を付し説明を省略する。以下、図24、図21を用いて、本発明の第3の実施の形態を説明する。

20

## 【0291】

本実施の形態の運用管理装置は、サービスシステムに対して、優先的に送信すべきイベントデータを指示する。このような指示を行う運用管理装置をマネージャ装置30と記す。また、このような指示を受ける装置をエージェント装置20と記す。エージェント装置20は、サービスシステム1を含む。

## 【0292】

また、サービスシステム1は、イベントデータ生成手段71の他に、マネージャ装置(運用管理装置)30からの指示に応じて優先的に送信すべきイベントデータを優先的に送信する通信制御手段12を備える。エージェント装置20と、マネージャ装置30とは、通信回線あるいは通信ネットワークを介して接続される。

30

## 【0293】

通信制御手段12は、イベントデータ取得手段2へのイベントデータの送信および制御手段6からの制御指示の受信を行うとともに、予測イベント管理手段9の指示を受けて、イベントデータの送受信の速度あるいは順序を変更する。イベントデータの送受信の速度あるいは順序を変更するとは、例えば、予測イベント管理手段9が指示した条件に合致するイベントデータがイベントデータ生成手段71によって生成されたならば、直ちにそのイベントデータを運用管理装置30に送信し、その他のイベントデータ(指示された条件に合致しないイベントデータ)は、一定時間間隔毎にまとめて送信することである。

## 【0294】

予測イベント管理手段9は、第2の実施の形態の機能に加えて、予測イベントデータの生成状況に応じて、優先的に受信するイベントデータを指定する情報をサービスシステム1の通信制御手段12に送信する。

40

## 【0295】

本実施の形態の運用管理装置が備える各手段の動作は、第1の実施の形態や第2の実施の形態と同様である。ただし、予測イベント管理手段9が、通信制御手段12に対して、受信するイベントデータの優先度を制御する。運用管理装置が優先的に受信すべきイベントデータは、運用管理装置の予測イベント管理手段9が生成した予測イベントデータに合致するイベントデータである。

## 【0296】

ただし、ジョブ実行に伴う正常なイベントとして生成された予測イベントデータに合致

50

するイベントデータは、特に急いで受信する必要はない。生成された予測イベントデータは、予測イベント対応表に記述されている（図21に示す予測イベント対応表の「監視状況」参照。）。

【0297】

予測イベント対応表に記述された予測イベントデータのうち、対応するルール番号の記述がない予測イベントデータは、ジョブ実行に伴う正常なイベントとして生成された予測イベントデータであり、そのようなイベントデータに合致するイベントデータは、急いで受信する必要はない。

【0298】

一方、予測イベント対応表に記述された予測イベントデータのうち、対応するルール番号の記述がある予測イベントデータに合致するイベントデータは、優先的に受信すべきイベントデータである。予測イベント管理手段9は、予測イベント対応表に、ルール番号に対応付けられた予測イベントデータの番号が記述されている場合には、その番号によって特定される予測イベントデータをサービスシステム1に送信することによって、その予測イベントデータに合致するイベントデータを優先的に送信することを要求する。

10

【0299】

サービスシステム1が備える通信制御手段12は、予測イベント管理手段9から予測イベントデータを受信する。そして、通信制御手段12は、イベントデータ生成手段71がイベントデータを生成したときに、そのイベントデータと受信した予測イベントデータとが合致するか否かを判定する。このとき、予測イベントデータに含まれる参考値以外の属性値とイベントデータの属性値とが合致していれば、両者は合致すると判定すればよい。

20

【0300】

通信制御手段12は、予測イベントデータに合致するイベントデータは、直ちに運用管理装置に送信する。一方、予測イベントデータに合致していないイベントデータは、保持しておく。そして、通信制御手段12は、一定期間毎に（例えば10分ごとに）、保持しているイベントデータを運用管理装置に送信する。

【0301】

通信制御手段12が送信したイベントデータは、イベントデータ取得手段2に受信される。イベントデータ取得手段2がイベントデータを受信した後の動作は、第1の実施の形態あるいは第2の実施の形態と同様である。

30

【0302】

通信ネットワークを介して情報を収集する関連技術の運用管理装置では、多数のイベントを頻繁に受信すると通信帯域が圧迫されてイベントデータの欠落が発生する場合があります。逆にイベントデータの受信間隔を長くしていると負荷は低減するものの、分析に遅れが出て障害が発生するといった問題があった。

【0303】

また、条件判定の結果に応じてイベントデータの送信タイミングを制御する従来の運用管理装置では、条件判定が論理条件式で行われるため、送信タイミングを制御するエージェント装置側でも論理条件式の判定が必要となり、処理負荷が増大するという問題があった。

40

【0304】

これに対して、本実施の形態の運用管理装置では、条件を予測イベントデータに展開してマッチングする方式であるため、イベントデータ単位のフィルタ（イベントデータを指定する条件となる予測イベントデータ）をそのままエージェント装置に指定することができ、処理負荷を増加させず、分析に適した送信制御を行うことができる。

【0305】

以上、本発明の実施の形態について説明したが、本発明は以上の実施の形態にのみ限定されず、その他各種の付加変更が可能である。また、本発明の運用管理装置が備える各手段は、その有する機能をハードウェア的に実現することは勿論、コンピュータとプログラムとで実現することができる。プログラムは、磁気ディスクや半導体メモリ等のコンピュ

50

ータ可読記録媒体に記録されて提供され、コンピュータの立ち上げ時等にコンピュータに読み取られ、そのコンピュータの動作を制御することにより、そのコンピュータを前述した各実施の形態における各手段として機能させる。

【0306】

(第4の実施の形態)

本発明の第4の実施の形態に係る運用管理装置は、管理対象システムの状態を表す属性の名称とその属性値とを対応付けたイベントデータが定められた条件に合致したときに処理を行うもので、以下のルール記憶手段、個別フィルタ情報記憶手段、予測イベント一覧記憶手段、予測イベント対応表記憶手段、予測イベントデータ合致判定手段、個別フィルタ情報特定手段、予測イベントデータ生成手段、およびルール判定手段を有する。

10

【0307】

ルール記憶手段(例えば、判定条件蓄積手段3)は、実行する処理を定めた運用ルール情報を記憶する。

【0308】

個別フィルタ情報記憶手段(例えば、予測イベント蓄積手段8)は、運用ルール情報毎に定められた条件となる情報であって、属性と属性値とを対応づけた情報であり、属性値の一部が過去のイベントデータから推測される参考値として記述されることがあり、また、属性値の一部が変数として記述されることがある個別フィルタ情報を記憶する。

【0309】

予測イベントデータ記憶手段(例えば、予測イベント蓄積手段8)は、個別フィルタ情報で変数として記述された属性値に管理対象システムで生成されたイベントデータの属性値を代入したデータである予測イベントデータを記憶する。

20

【0310】

予測イベント一覧記憶手段は、生成されたイベントデータと、当該イベントデータに合致する個別フィルタ情報から生成された予測イベントデータと、運用ルール情報に対応する個別フィルタ情報の集合であるグループであってイベントデータに合致する個別フィルタ情報が属するグループとを対応付けた情報である予測イベント一覧を記憶する。

【0311】

予測イベント対応表記憶手段は、運用ルール情報と、運用ルール情報が定める条件となる各個別フィルタ情報と、その各個別フィルタ情報が属するグループと、個別フィルタ情報から生成された予測イベントデータとを対応付けた情報である予測イベント対応表を記憶する。

30

【0312】

予測イベントデータ合致判定手段(例えば、ステップS721の処理を行う予測イベント分析手段10)は、新たに生成されたイベントデータの属性値が、既に存在する予測イベントデータの参考値以外の属性値と合致している場合にイベントデータと予測イベントデータとが合致すると判定し、新たに生成されたイベントデータの属性値が、既に存在する予測イベントデータの参考値以外の属性値と合致していない場合にイベントデータと予測イベントデータとが合致しないと判定する。

【0313】

個別フィルタ情報特定手段(例えば、ステップS723の処理を行う予測イベント分析手段10)は、イベントデータと予測イベントデータとが合致しないと判定された場合に、参考値以外の属性値がイベントデータの属性値と合致する個別フィルタ情報を特定する。

40

【0314】

予測イベントデータ生成手段(例えば、ステップS725の処理を行う予測イベント分析手段10)は、個別フィルタ情報の特定に成功した場合に、当該個別フィルタ情報が属するグループに属する各個別フィルタ情報の変数にイベントデータの属性値を代入して、その各個別フィルタ情報毎に予測イベントデータを生成し、予測イベントデータ記憶手段に予測イベントデータを記憶させ、イベントデータと予測イベントデータとイベントデー

50

タに合致する個別フィルタ情報が属するグループとの対応関係を示す情報を予測イベント一覧記憶手段に記憶させ、生成された予測イベントデータとその予測イベントデータの生成に用いられた個別フィルタ情報のグループと、当該グループに属する各個別フィルタ情報と、その各個別フィルタ情報を条件とする運用ルール情報との対応関係を示す情報を予測イベント対応表記憶手段に記憶させる。

**【 0 3 1 5 】**

ルール判定手段（例えば、ステップ S 7 2 6 の処理を行うイベント分析手段 4）は、予測イベントデータ生成手段が予測イベントデータを生成した後に、当該予測イベントデータを生成するために用いたイベントデータに合致する個別フィルタ情報が属するグループと予測イベント一覧で対応付けられた各イベントデータが、そのグループに対応する運用

10

**【 0 3 1 6 】**

本実施の形態の上記構成において、次の参考値合致判定手段、ユーザインタフェース手段、および修正手段を備えてもよい。

**【 0 3 1 7 】**

参考値合致判定手段（例えば、ステップ S 7 2 5 の処理を行う予測イベント分析手段 10）は、イベントデータと予測イベントデータとが合致すると判定された場合に、予測イベントデータに含まれる参考値がイベントデータの属性値に合致するか否かを判定する。

**【 0 3 1 8 】**

ユーザインタフェース手段（例えば、ステップ S 7 2 8 の処理を行うイベント分析手段 4 およびユーザ対話手段 5）は、イベントデータと予測イベントデータとが合致すると判定され予測イベントデータに含まれる参考値がイベントデータの属性値に合致しないと判定された場合に、運用ルール情報およびイベントデータを表示するとともに参考値と合致しない属性値を表示し、運用ルール情報の条件を変更するか否かの指示が入力される。

20

**【 0 3 1 9 】**

修正手段（例えば、予測イベント管理手段 9）は、運用ルール情報の条件を変更しない旨の指示が入力された場合に、イベントデータの属性値と予測イベントデータの参考値とが一致していなかった属性の参考値を個別フィルタ情報から削除し、運用ルール情報の条件を変更する旨の指示が入力された場合に、イベントデータの属性値と予測イベントデータの参考値とが一致していなかった属性であってその予測イベントデータの生成に用いた個別フィルタ情報が属するグループの個別フィルタ情報の属性の属性値を変数を用いた属性値に書き換え、イベントデータの属性値と合致していなかった予測イベントデータの参考値を参考値でない属性値に書き換える。

30

**【 0 3 2 0 】**

本実施の形態の上記構成において、次のジョブ管理手段を備えてもよい。

ジョブ管理手段（例えば、ジョブ管理手段 11）は、予め発生順序が決まっている複数イベントデータに合致する複数の個別フィルタ情報を保持し、その複数の個別フィルタ情報を順番を指定して予測イベントデータ生成手段に通知する。

**【 0 3 2 1 】**

この場合、予測イベントデータ生成手段が、その複数の個別フィルタ情報の集合を 1 つのグループとして、当該グループとその複数の個別フィルタ情報とを対応付けた情報を予測イベント対応表記憶手段に記憶させ、ジョブ管理手段が通知した個別フィルタ情報と、当該個別フィルタ情報に合致するイベントデータから予測フィルタ情報を生成した場合に、その個別フィルタ情報の次の個別フィルタ情報の変数にそのイベントデータの属性値を代入した予測イベントデータを生成し、生成した予測イベントデータを、グループと複数の個別フィルタ情報とを対応付けた情報に追加する。

40

**【 0 3 2 2 】**

上記構成によれば、計画的に発生が予想されるイベントデータを予測イベントデータとマッピングして迅速に処理することができるため、管理対象システムの動作に伴い多数の

50

イベントデータが発生しても、他の運用ルール情報の条件判定に影響を与えない。

【0323】

本実施の形態の上記構成において、次の優先イベントデータ要求手段を備えてもよい。

【0324】

優先イベントデータ要求手段（例えば、予測イベント管理手段9）は、予測イベント対応表記憶手段で運用ルール情報に対応付けられた予測イベントデータが存在する場合に、当該予測イベントデータを管理対象システムに通知することによって、管理対象システムが生成したイベントデータのうちその予測イベントデータに合致するイベントデータを優先的に通知することを管理対象システムに要求する。

10

【0325】

上記構成によれば、イベントデータ単位の条件となる予測イベントデータを管理対象システムに指定して、処理負荷を増加させず、分析に適した送信制御を管理対象システムに対して行うことができる。

【0326】

本実施の形態の上記構成において、次の個別フィルタ情報生成手段を備えてもよい。

【0327】

個別フィルタ情報生成手段（例えば、ステップS712、S713の処理を行う予測イベント管理手段9）は、属性と参考値でない属性値とを対応付けた情報であるフィルタ情報を記憶するフィルタ情報記憶手段（例えば、判定条件蓄積手段3）と、過去に生成されたイベントデータであって運用ルール情報が指定するフィルタ情報に合致するイベントデータから推測される属性値を参考値としてそのフィルタ情報に付加することで個別フィルタ情報を生成する。

20

【0328】

上記構成によれば、個別フィルタ情報を生成するために用いるフィルタ情報の記述が複雑にならない。さらに、運用ルール情報を類似環境に適用する場合にも、同様にして共通的な記述であるフィルタ情報から適用先の環境に応じた個別フィルタ情報が生成される。その結果、管理者が運用ルール情報を扱う場合の作業負担が大幅に減少し、適用範囲を拡大し易くなる。

【0329】

（第5の実施の形態）

本発明の第5の実施の形態に係る運用管理方法は、管理対象システムの状態を表す属性の名称とその属性値とを対応付けたイベントデータが定められた条件に合致したときに処理を行う運用管理装置に適用される。

30

【0330】

運用管理装置は、以下のルール記憶手段、個別フィルタ情報記憶手段、予測イベントデータ記憶手段、予測イベント一覧記憶手段、および予測イベント対応表記憶手段を備える。

【0331】

ルール記憶手段（例えば、判定条件蓄積手段3）は、実行する処理を定めた運用ルール情報を記憶する。

40

【0332】

個別フィルタ情報記憶手段（例えば、予測イベント蓄積手段8）は、運用ルール情報毎に定められた条件となる情報であって、属性と属性値とを対応づけた情報であり、属性値の一部が過去のイベントデータから推測される参考値として記述されることがあり、また、属性値の一部が変数として記述されることがある個別フィルタ情報を記憶する。

【0333】

予測イベントデータ記憶手段（例えば、予測イベント蓄積手段8）は、個別フィルタ情報で変数として記述された属性値に管理対象システムで生成されたイベントデータの属性値を代入したデータである予測イベントデータを記憶する。

50

## 【0334】

予測イベント一覧記憶手段は、生成されたイベントデータと、当該イベントデータに合致する個別フィルタ情報から生成された予測イベントデータと、運用ルール情報に対応する個別フィルタ情報の集合であるグループであってイベントデータに合致する個別フィルタ情報が属するグループとを対応付けた情報である予測イベント一覧を記憶する。

## 【0335】

予測イベント対応表記憶手段は、運用ルール情報と、運用ルール情報が定める条件となる各個別フィルタ情報と、その各個別フィルタ情報が属するグループと、個別フィルタ情報から生成された予測イベントデータとを対応付けた情報である予測イベント対応表を記憶する。

10

## 【0336】

上記構成の運用管理装置に適用される運用管理方法は、以下の動作を行う。

## 【0337】

まず、予測イベントデータ合致判定手段（例えば、予測イベント分析手段10）が、新たに生成されたイベントデータの属性値が、既に存在する予測イベントデータの参考値以外の属性値と合致している場合にイベントデータと予測イベントデータとが合致すると判定し、新たに生成されたイベントデータの属性値が、既に存在する予測イベントデータの参考値以外の属性値と合致していない場合にイベントデータと予測イベントデータとが合致しないと判定する。

## 【0338】

次に、個別フィルタ情報特定手段（例えば、予測イベント分析手段10）が、イベントデータと予測イベントデータとが合致しないと判定された場合に、参考値以外の属性値がイベントデータの属性値と合致する個別フィルタ情報を特定する。

20

## 【0339】

次に、予測イベントデータ生成手段（例えば、予測イベント分析手段10）が、個別フィルタ情報の特定に成功した場合に、当該個別フィルタ情報が属するグループに属する各個別フィルタ情報の変数にイベントデータの属性値を代入して、その各個別フィルタ情報毎に予測イベントデータを生成し、予測イベントデータ記憶手段に予測イベントデータを記憶させ、イベントデータと予測イベントデータとイベントデータに合致する個別フィルタ情報が属するグループとの対応関係を示す情報を予測イベント一覧記憶手段に記憶させ、生成された予測イベントデータとその予測イベントデータの生成に用いられた個別フィルタ情報のグループと、当該グループに属する各個別フィルタ情報と、その各個別フィルタ情報を条件とする運用ルール情報との対応関係を示す情報を予測イベント対応表記憶手段に記憶させる。

30

## 【0340】

次に、予測イベントデータ生成手段が予測イベントデータを生成した後に、ルール判定手段（例えば、イベント分析手段4）が、当該予測イベントデータを生成するために用いたイベントデータに合致する個別フィルタ情報が属するグループと予測イベント一覧で対応付けられた各イベントデータが、そのグループに対応する運用ルール情報の個別フィルタ情報を満足しているか否かを判定し、満足している場合に運用ルール情報が定める処理を実行する。

40

## 【0341】

本実施の形態の上記構成において、次の動作を行ってもよい。

## 【0342】

まず、参考値合致判定手段（例えば、予測イベント分析手段10）が、イベントデータと予測イベントデータとが合致すると判定された場合に、予測イベントデータに含まれる参考値がイベントデータの属性値に合致するか否かを判定する。

## 【0343】

次に、ユーザインタフェース手段（例えば、イベント分析手段4およびユーザ対話手段5）が、イベントデータと予測イベントデータとが合致すると判定され予測イベントデー

50

タに含まれる参考値がイベントデータの属性値に合致しないと判定された場合に、運用ルール情報およびイベントデータを表示するとともに参考値と合致しない属性値を表示し、運用ルール情報の条件を変更するか否かの指示が入力される。

【 0 3 4 4 】

次に、修正手段（例えば、予測イベント管理手段 9）が、運用ルール情報の条件を変更しない旨の指示が入力された場合に、イベントデータの属性値と予測イベントデータの参考値とが一致していなかった属性の参考値を個別フィルタ情報から削除し、運用ルール情報の条件を変更する旨の指示が入力された場合に、イベントデータの属性値と予測イベントデータの参考値とが一致していなかった属性であってその予測イベントデータの生成に用いた個別フィルタ情報が属するグループの個別フィルタ情報の属性の属性値を変数を用いた属性値に書き換え、イベントデータの属性値と合致していなかった予測イベントデータの参考値を参考値でない属性値に書き換える。

10

【 0 3 4 5 】

本実施の形態の上記構成において、次の動作を行ってもよい。

【 0 3 4 6 】

まず、ジョブ管理手段（例えば、ジョブ管理手段 11）が、予め発生順序が決まっている複数イベントデータに合致する複数の個別フィルタ情報を保持し、その複数の個別フィルタ情報を順番を指定して予測イベントデータ生成手段に通知する。

【 0 3 4 7 】

次に、予測イベントデータ生成手段が、その複数の個別フィルタ情報の集合を 1 つのグループとして、当該グループとその複数の個別フィルタ情報とを対応付けた情報を予測イベント対応表記憶手段に記憶させ、ジョブ管理手段が通知した個別フィルタ情報と、当該個別フィルタ情報に合致するイベントデータから予測フィルタ情報を生成した場合に、その個別フィルタ情報の次の個別フィルタ情報の変数にそのイベントデータの属性値を代入した予測イベントデータを生成し、生成した予測イベントデータを、グループと複数の個別フィルタ情報とを対応付けた情報に追加する。

20

【 0 3 4 8 】

本実施の形態の上記構成において、次の動作を行ってもよい。

【 0 3 4 9 】

優先イベントデータ要求手段（例えば、予測イベント管理手段 9）が、予測イベント対応表記憶手段で運用ルール情報に対応付けられた予測イベントデータが存在する場合に、当該予測イベントデータを管理対象システムに通知することによって、管理対象システムが生成したイベントデータのうちその予測イベントデータに合致するイベントデータを優先的に通知することを管理対象システムに要求する。

30

【 0 3 5 0 】

（第 6 の実施の形態）

本発明の第 6 の実施の形態に係る運用管理プログラムは、管理対象システムの状態を表す属性の名称とその属性値とを対応付けたイベントデータが定められた条件に合致したときに処理を行うコンピュータに搭載される。

【 0 3 5 1 】

コンピュータは、以下のルール記憶手段、個別フィルタ情報記憶手段、予測イベントデータ記憶手段、予測イベント一覧記憶手段、および予測イベント対応表記憶手段を備える。

40

【 0 3 5 2 】

ルール記憶手段（例えば、判定条件蓄積手段 3）は、実行する処理を定めた運用ルール情報を記憶する。

【 0 3 5 3 】

個別フィルタ情報記憶手段（例えば、予測イベント蓄積手段 8）は、運用ルール情報毎に定められた条件となる情報であって、属性と属性値とを対応づけた情報であり、属性値の一部が過去のイベントデータから推測される参考値として記述されることがあり、また

50

、属性値の一部が変数として記述されることがある個別フィルタ情報を記憶する。

【0354】

予測イベントデータ記憶手段（例えば、予測イベント蓄積手段8）は、個別フィルタ情報で変数として記述された属性値に管理対象システムで生成されたイベントデータの属性値を代入したデータである予測イベントデータを記憶する。

【0355】

予測イベント一覧記憶手段は、生成されたイベントデータと、当該イベントデータに合致する個別フィルタ情報から生成された予測イベントデータと、運用ルール情報に対応する個別フィルタ情報の集合であるグループであってイベントデータに合致する個別フィルタ情報が属するグループとを対応付けた情報である予測イベント一覧を記憶する。

10

【0356】

予測イベント対応表記憶手段は、運用ルール情報と、運用ルール情報が定める条件となる各個別フィルタ情報と、その各個別フィルタ情報が属するグループと、個別フィルタ情報から生成された予測イベントデータとを対応付けた情報である予測イベント対応表を記憶する。

【0357】

上記構成のコンピュータに搭載される運用管理プログラムは、コンピュータに、次の予測イベントデータ合致判定処理、個別フィルタ情報特定処理、予測イベントデータ生成処理、およびルール判定処理を実行させる。

【0358】

予測イベントデータ合致判定処理は、新たに生成されたイベントデータの属性値が、既に存在する予測イベントデータの参考値以外の属性値と合致している場合にイベントデータと予測イベントデータとが合致すると判定し、新たに生成されたイベントデータの属性値が、既に存在する予測イベントデータの参考値以外の属性値と合致していない場合にイベントデータと予測イベントデータとが合致しないと判定する。

20

【0359】

個別フィルタ情報特定処理は、イベントデータと予測イベントデータとが合致しないと判定された場合に、参考値以外の属性値がイベントデータの属性値と合致する個別フィルタ情報を特定する。

【0360】

予測イベントデータ生成処理は、個別フィルタ情報の特定に成功した場合に、当該個別フィルタ情報が属するグループに属する各個別フィルタ情報の変数にイベントデータの属性値を代入して、その各個別フィルタ情報毎に予測イベントデータを生成し、予測イベントデータ記憶手段に予測イベントデータを記憶させ、イベントデータと予測イベントデータとイベントデータに合致する個別フィルタ情報が属するグループとの対応関係を示す情報を予測イベント一覧記憶手段に記憶させ、生成された予測イベントデータとその予測イベントデータの生成に用いられた個別フィルタ情報のグループと、当該グループに属する各個別フィルタ情報と、その各個別フィルタ情報を条件とする運用ルール情報との対応関係を示す情報を予測イベント対応表記憶手段に記憶させる。

30

【0361】

ルール判定処理は、予測イベントデータ生成処理で予測イベントデータを生成した後に、当該予測イベントデータを生成するために用いたイベントデータに合致する個別フィルタ情報が属するグループと予測イベント一覧で対応付けられた各イベントデータが、そのグループに対応する運用ルール情報の個別フィルタ情報を満足しているか否かを判定し、満足している場合に運用ルール情報が定める処理を実行する。

40

【0362】

本実施の形態の上記構成において、コンピュータに、次の参考値合致判定処理、表示処理、および修正処理を実行させてもよい。

【0363】

参考値合致判定処理は、イベントデータと予測イベントデータとが合致すると判定され

50

た場合に、予測イベントデータに含まれる参考値がイベントデータの属性値に合致するかどうかを判定する。

【0364】

表示処理は、イベントデータと予測イベントデータとが合致すると判定され予測イベントデータに含まれる参考値がイベントデータの属性値に合致しないと判定された場合に、運用ルール情報およびイベントデータを表示するとともに参考値と合致しない属性値を表示する。

【0365】

修正処理は、運用ルール情報の条件を変更しない旨の指示が入力された場合に、イベントデータの属性値と予測イベントデータの参考値とが一致していなかった属性の参考値を個別フィルタ情報から削除し、運用ルール情報の条件を変更する旨の指示が入力された場合に、イベントデータの属性値と予測イベントデータの参考値とが一致していなかった属性であってその予測イベントデータの生成に用いた個別フィルタ情報が属するグループの個別フィルタ情報の属性の属性値を変数を用いた属性値に書き換え、イベントデータの属性値と合致していなかった予測イベントデータの参考値を参考値でない属性値に書き換える。

10

【0366】

本実施の形態の上記構成において、コンピュータに、次の処理を実行させてもよい。

【0367】

この処理は、予め発生順序が決まっている複数イベントデータに合致する複数の個別フィルタ情報であって順番が定められている個別フィルタ情報の集合を1つのグループとして、当該グループとその複数の個別フィルタ情報とを対応付けた情報を予測イベント対応表記憶手段に記憶させる処理を実行させ、予測イベントデータ生成処理で、順番が定められている個別フィルタ情報と、当該個別フィルタ情報に合致するイベントデータから予測フィルタ情報を生成した場合に、その個別フィルタ情報の次の個別フィルタ情報の変数にそのイベントデータの属性値を代入した予測イベントデータを生成し、生成した予測イベントデータを、グループと複数の個別フィルタ情報とを対応付けた情報に追加する。

20

【0368】

本実施の形態の上記構成において、コンピュータに、次の優先イベントデータ要求処理を実行させてもよい。

30

【0369】

優先イベントデータ要求処理は、コンピュータに、予測イベント対応表記憶手段で運用ルール情報に対応付けられた予測イベントデータが存在する場合に、当該予測イベントデータを管理対象システムに通知することによって、管理対象システムが生成したイベントデータのうちその予測イベントデータに合致するイベントデータを優先的に通知することを管理対象システムに要求する。

【0370】

この出願は、2007年3月14日に出願された日本出願特願2007-064678号を基礎とする優先権を主張し、その開示の全てをここに取り込む。

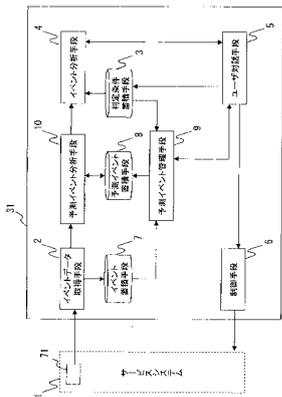
【産業上の利用可能性】

40

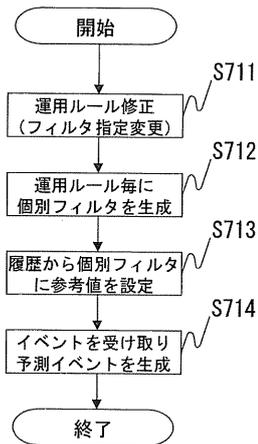
【0371】

本発明は、管理対象となるシステムの状態を表すイベントデータが条件に合致する場合に対処を実施する運用管理装置に好適に適用される。

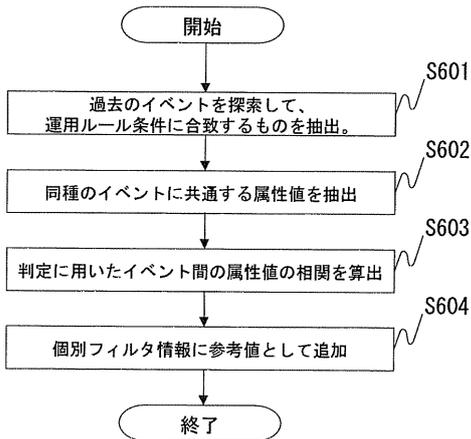
【図1】



【図2】



【図5】



【図3】

[RULE FILTER] NUMBER = F1011 TYPE = DATE1 = TIME1 = [\$F01] SERVER = [\$F02] SOURCE = updater EVENTID = 4001 USER = DESCRIPTION =	[RULE FILTER] NUMBER = F1012 TYPE = DATE1 = TIME1 = [PERIOD(\$F01, *)] SERVER = [\$F02] SOURCE = BIZAP EVENTID = 8000 USER = DESCRIPTION =
--	---

211 :個別フィルタ情報      212 :個別フィルタ情報

【図4】

[RULE FILTER] NUMBER = F1111 TYPE = DATE1 = TIME1 = [03:00:10] SERVER = [SV4] SOURCE = updater EVENTID = 4001 USER = DESCRIPTION =	[RULE FILTER] NUMBER = F1112 TYPE = DATE1 = TIME1 = [PERIOD(03:00:10, *)] SERVER = [SV4] SOURCE = BIZAP EVENTID = 8000 USER = DESCRIPTION =
---	--

221 :予測イベントデータ      222 :予測イベントデータ

【図6】

番号	種別	日時	発生源	ID	ユーザ	説明
E8010	不明	2006/06/29-06:00:12	SV2.updater	4001	root	手動:バッチが適用されました。
E8020	不明	2006/06/29-07:08:33	SV2.BIZAP	8000	root	手動:マスタの応答がありません。
E8030	警告	2006/09/30-03:00:25	SV3.updater	4001	N/A	バッチが適用されました。
E8040	情報	2006/10/02-08:02:30	SV3.BIZAP	8000	admin	業務を開始しました。

101 :イベントリスト

【図7】

番号	種類	日時	発生元	ID	ユーザ	説明
E9001	情報	2006/10/30-23:05:30	SV3.agent	0033	admin	業務を停止しました。
E9002	警告	2006/10/31-03:00:10	SV4.updater	4001	N/A	パッチが適用されました。
E9003	情報	2006/10/31-08:00:10	SV3.agent	0032	admin	業務を開始しました。
E9004	異常	2006/10/31-08:02:30	SV3.BIZAP	8000	SYSTEM	マスタの応答がありません。

110: イベントリスト

番号	種類	日時	発生元	ID	ユーザ	説明
E9001	情報	2006/10/30-23:05:30	SV3.agent	0033	admin	業務を停止しました。
E9002	警告	2006/10/31-03:00:10	SV4.updater	4001	N/A	パッチが適用されました。
E9003	情報	2006/10/31-08:00:10	SV3.agent	0032	admin	業務を開始しました。
E9004	異常	2006/10/31-08:02:30	SV3.BIZAP	8000	SYSTEM	マスタの応答がありません。
E9005	異常	2006/10/31-08:10:00	SV4.BIZAP	8000	SYSTEM	マスタの応答がありません。
E9006	情報	2006/10/31-08:10:33	SV4.agent	0132	admin	業務APを移動します。
E9007	警告	2006/10/31-08:11:30	SV3.agent	4001	N/A	パッチが適用されました。
E9008	情報	2006/10/31-08:12:00	SV3.agent	0132	admin	業務APを移動します。

120: イベントリスト

【図8】

番号	ルール番号	フィルタ系列	監視状況
G010	R0110	F1010	F1110
G020	R0120	F1011 F1012	
G030	R0130	F1013	

401: 予測イベント対応表

番号	ルール番号	フィルタ系列	監視状況
G010	R0110	F1010	F1111 F1112
G020	R0120	F1011 F1012	
G030	R0130	F1013	

402: 予測イベント対応表

番号	ルール番号	フィルタ系列	監視状況
G010	R0110	F1010	F1210
G020	R0120	F1011 F1012	F1111 F1112
G030	R0130	F1013	

403: 予測イベント対応表

【図9】

番号	グループ番号
F1010	G0110
F1011	G0120
F1012	G0120
F1013	G0130

311: フィルター一覧

[EVENT FILTER]  
 NUMBER = F1010  
 TYPE =  
 DATE1 =  
 TIME1 =  
 SERVER =  
 SOURCE = agent  
 EVENTID =  
 USER =  
 DESCRIPTION =

210: 個別フィルタ情報

【図10】

判定	番号	グループ番号	対応イベント
済	F1110	G0110	E9001

321: 予測イベント一覧

判定	番号	グループ番号	対応イベント
済	F1110	G0110	E9001
	F1111	G0120	E9002
	F1112	G0120	

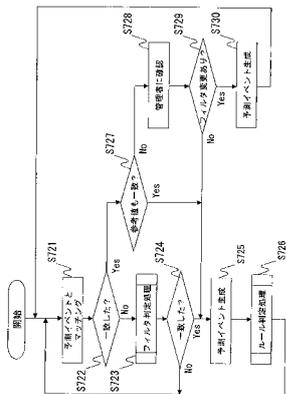
322: 予測イベント一覧

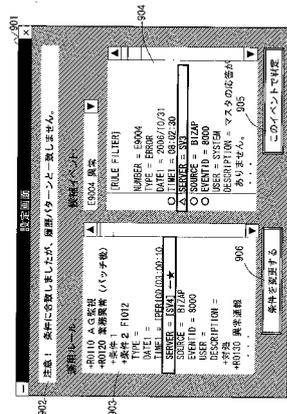
判定	番号	グループ番号	対応イベント
済	F1110	G0110	E9001
済	F1210	G0110	E9003
	F1111	G0120	E9002
	F1112	G0120	

323: 予測イベント一覧

【 1 1 】



【 1 2 】



【 1 4 】

予測イベント	予測イベント	予測イベント
234	235	236
...	...	...

【 1 5 】

[RULE FILTER] NUMBER = F1011 TYPE = DATE1 = TIME1 = [\$F01] SERVER = SOURCE = updater EVENTID = 4001 USER = DESCRIPTION =	[RULE FILTER] NUMBER = F1012 TYPE = DATE1 = TIME1 = [PERIOD(\$F01, *)] SERVER = SOURCE = BIZAP EVENTID = 8000 USER = DESCRIPTION =
--	---

211 : 個別フィルタ情報

212 : 個別フィルタ情報

【 1 3 】

番号	ルール番号	フィルタ系列	監視状況
...	...	...	...
...	G0110	F1010	F1111 F1112
...	G0120	F1011 F1012	...
...	G0130	F1013	...

404 : 予測イベント対応表

番号	ルール番号	フィルタ系列	監視状況
...	...	...	...
...	G0110	F1010	F2111 F2112 F1211 F1212
...	G0120	F1011 F1012	...
...	G0130	F1013	...

405 : 予測イベント対応表

番号	ルール番号	フィルタ系列	監視状況
...	...	...	...
...	G0110	F1010	F2111 F2112
...	G0120	F1011 F1012	...
...	G0130	F1013	...

406 : 予測イベント対応表

【 1 6 】

[RULE FILTER] NUMBER = F001 TYPE = DATE1 = TIME1 = SERVER = SVV SOURCE = updater EVENTID = 4001 USER = DESCRIPTION =	[RULE FILTER] NUMBER = F0012 TYPE = DATE1 = TIME1 = SERVER = SVV SOURCE = BIZAP EVENTID = 8000 USER = DESCRIPTION =
---	--

203 : フィルタ情報      204 : フィルタ情報

【 1 7 】

[RULE FILTER] NUMBER = F001 TYPE = DATE1 = TIME1 = [\$F01] SERVER = SVV SOURCE = updater EVENTID = 4001 USER = DESCRIPTION =	[RULE FILTER] NUMBER = F0012 TYPE = DATE1 = TIME1 = [PERIOD(\$F01, *)] SERVER = SVV SOURCE = BIZAP EVENTID = 8000 USER = DESCRIPTION =
---	---

213 : 個別フィルタ情報      214 : 個別フィルタ情報

【 1 8 】

[RULE FILTER] NUMBER = F1111 TYPE = DATE1 = TIME1 = [00:00:00] SERVER = SV4 SOURCE = updater EVENTID = 4001 USER = DESCRIPTION =	[RULE FILTER] NUMBER = F1112 TYPE = DATE1 = TIME1 = [PERIOD(\$F01, *)] SERVER = SV4 SOURCE = BIZAP EVENTID = 8000 USER = DESCRIPTION =
---	---

223 : 予測イベントデータ      224 : 予測イベントデータ



【図23】

判定	番号	グループ番号	対応イベント
済	F110	G0110	E9001
済	F113	G0130	E2003
	F2101	G0200	E2001
	F2102	G0200	E2002
	F2103	G0200	E9002
	F1111	G0120	E9002
	F1112	G0120	E9002

333:予測イベント一覧

334:予測イベント一覧

【図26】

番号	種類	日時	発生源	ID	ユーザ	説明
E9001	情報	2006/10/30-23:05:30	SV3_agent	0033	admin	業務を停止しました。
E9002	警告	2006/10/31-03:00:10	SV3_updater	4001	N/A	パッチが適用されました。
E9003	情報	2006/10/31-08:00:10	SV3_agent	0032	admin	業務を開始しました。
E9004	異常	2006/10/31-08:02:30	SV3_BIZAP	8000	SYSTEM	マスタの応答がありません。
E9005	情報	2006/10/31-08:05:40	SV3_agent	0132	admin	業務APを移動します。

100:イベントリスト

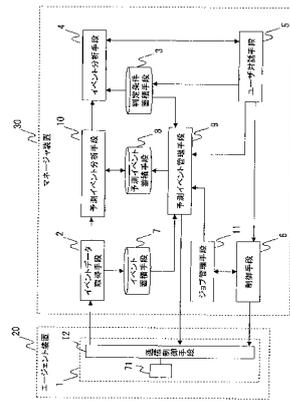
101:イベントデータ

```

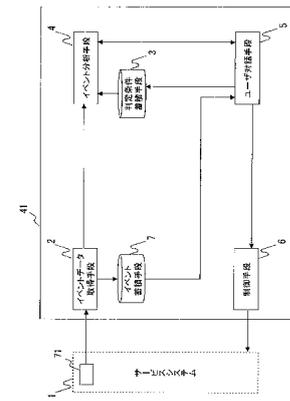
[EVENT DATA]
NUMBER = E9005
TYPE = INFORMATION
DATEI = 2006/10/31
TIMEI = 08:05:40
SERVER = SV3
SOURCE = agent
EVENTID = 0132
USER = admin
DESCRIPTION = 業務APを移動します。
詳細は以下の通り。
対応ルール番号: R0120
検知した条件: E9002, E9004
対処の予定: N/A(BIZAP, SV4)

```

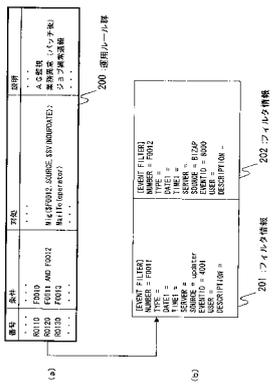
【図24】



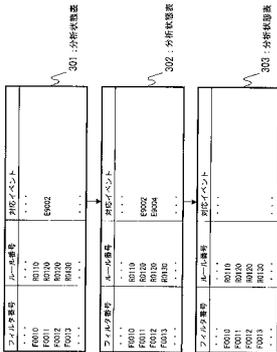
【図25】



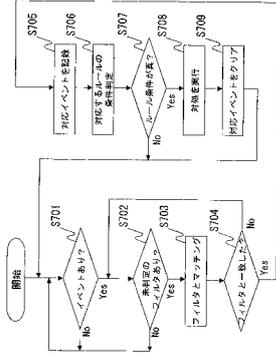
【図27】



【図28】



【 図 29 】



---

フロントページの続き

- (56)参考文献 特開2002-318710(JP,A)  
特開2005-141466(JP,A)  
特開2005-182647(JP,A)  
特開2006-004346(JP,A)  
特開2006-244404(JP,A)  
特開2006-318071(JP,A)  
特開2006-338305(JP,A)

(58)調査した分野(Int.Cl., DB名)

G06F 11/30

G06F 11/34