(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2006-4346
(P2006-4346A)
(43)公開日　平成18年1月5日(2006.1.5)

| (51)Int.Cl. | | F I | | | テーマコード（参考） |
|---|---|---|---|---|---|
| G06F 11/34 | (2006.01) | G06F | 11/34 | L | 5B042 |
| G06F 15/00 | (2006.01) | G06F | 15/00 | 320K | 5B085 |
| | | | | | 5B185 |

審査請求 未請求　請求項の数 10　ＯＬ　（全 30 頁）

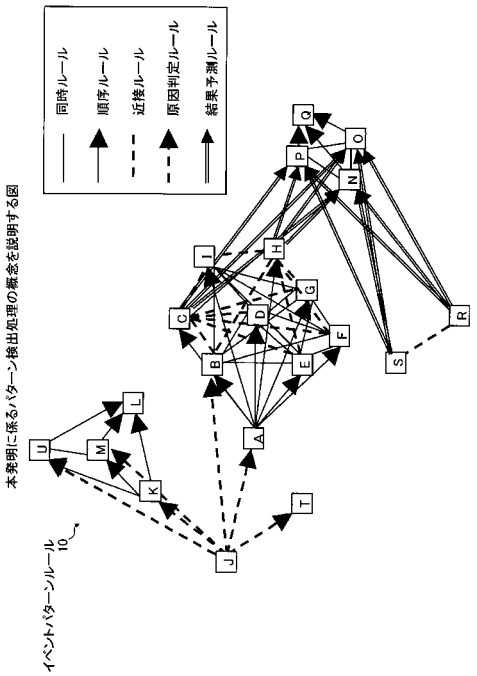
(21)出願番号　特願2004-182520 (P2004-182520)
(22)出願日　平成16年6月21日 (2004.6.21)

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(74)代理人　100089118
弁理士　酒井　宏明
(72)発明者　小林　健一
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　湯上　伸弘
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

Ｆターム(参考)　5B042 GA12 JJ06 JJ19 JJ29 KK13 LA13 MA14 MB04 MC15 MC40
5B085 AC14 AC16 BG02
5B185 AC14 AC16 BG02

(54)【発明の名称】パターン検出プログラム

(57)【要約】
【課題】生起したイベントに係る情報を記憶したイベントデータからイベントの生起パターンを検出する際に、イベントログからイベントの生起パターンについての詳細な情報を抽出すること。
【解決手段】同時ルール、順序ルール、近接ルール、原因判定ルール、および、結果予測ルールなどの、イベント間において定義される複数種類の関係に係る情報に基づいて、イベントログからイベントの生起パターンを検出し、検出されたイベントの生起パターンを出力する。
【選択図】　図１



【特許請求の範囲】
【請求項１】
生起したイベントに係る情報を記憶したイベントデータからイベントの生起パターンを検出する処理をコンピュータに実行させるパターン検出プログラムであって、
イベント間において定義される複数種類の関係に係る情報に基づいて、前記イベントデータからイベントの生起パターンを検出する検出手順と、
前記検出手順により検出されたイベントの生起パターンを出力する出力手順と、
をコンピュータに実行させることを特徴とするパターン検出プログラム。
【請求項２】
前記複数種類の関係に係る情報は、イベントの生起時刻およびイベントの生起確率に基づいて定義された情報であることを特徴とする請求項１に記載のパターン検出プログラム。
【請求項３】
前記検出手順は、関係の有無を判定するイベント間の生起時刻の範囲に係る設定値を、生起パターンの検出結果に基づいて設定することを特徴とする請求項２に記載のパターン検出プログラム。
【請求項４】
前記検出手順は、関係の有無を判定するイベント間の生起確率に係る設定値を、生起パターンの検出結果に基づいて設定することを特徴とする請求項２または３に記載のパターン検出プログラム。
【請求項５】
前記検出手順は、前記イベントの生起パターンの検出結果を評価する評価関数に基づいて、関係の有無を判定するイベント間の生起時刻の範囲に係る設定値、または、関係の有無を判定するイベント間の生起確率に係る設定値を設定することを特徴とする請求項２、３または４に記載のパターン検出プログラム。
【請求項６】
前記複数種類の関係に係る情報は、２つのイベントが生起した生起時刻の差の大小に応じて異なる種類の関係を定義した情報を含んだことを特徴とする請求項１～５のいずれか１つに記載のパターン検出プログラム。
【請求項７】
前記検出手順は、２つのイベントから構成される生起パターンを結合することにより、３つ以上のイベントから構成される生起パターンを検出することを特徴とする請求項１～６のいずれか１つに記載のパターン検出プログラム。
【請求項８】
前記検出手順は、生起パターンの結合の可否を判定する結合条件に基づいて、生起パターンの結合を実行するか否かを判定することを特徴とする請求項７に記載のパターン検出プログラム。
【請求項９】
前記検出手順は、結合された生起パターンに含まれる部分が所定の基準を満足しているか否かを判定し、所定の基準を満足しない部分を生起パターンから削除することを特徴とする請求項７または８に記載のパターン検出プログラム。
【請求項１０】
前記出力手順は、生起パターンに含まれるイベント間の関係に係る情報に基づいて、前記検出手順により検出された生起パターンに含まれるイベント間の関係を統合し、イベント間の関係が統合された生起パターンを出力することを特徴とする請求項１～９のいずれか１つに記載のパターン検出プログラム。

【発明の詳細な説明】
【技術分野】

【０００１】
この発明は、生起したイベントに係る情報を記憶したイベントデータからイベントの生起パターンを検出する処理をコンピュータに実行させるパターン検出プログラムに関し、特に、イベントデータからイベントの生起パターンについての詳細な情報を抽出することができるパターン検出プログラムに関する。
【背景技術】
【０００２】
近年、銀行などの勘定系システムに対する不正なトランザクション、インターネット上のウェブサイトに対する不正なアクセス、あるいは、ネットワークシステムの障害の予兆などのさまざまなイベントの生起状況を分析して、事故やトラブルを事前に回避することができるイベント分析システムが開発されるようになってきている。
【０００３】
図１６は、イベントの生起パターンを分析するイベント分析システム２の一例を示す図であり、図１７は、生起したイベントを記録したイベントログの一例を示す図である。図１６に示すように、このイベント分析システム２は、イベントログを顧客システム１から取得して、障害が発生する際に顕著に見られるイベントの生起パターンを検出し、ノウハウとして蓄積する。
【０００４】
イベントログとは、図１７に示すように、顧客システム１に生起したエラーなどのイベントの情報が書き込まれたログである。具体的には、このイベントログには、イベントの生起時刻、イベントの種別、その他の付加情報などが記録される。
【０００５】
そして、イベント分析システム２は、顧客システム１のイベントログを分析し、検出したイベントの生起パターンがイベントログ中に含まれているか否かをパターンマッチングにより監視して障害の発生状況を診断する。顧客システム１の管理者は、イベント分析システム２により診断された結果に基づいて、顧客システム１に発生する障害に適切に対処することができる。
【０００６】
従来、上述したようなイベントの生起パターンを検出する方法がいくつか知られている。たとえば、イベントログの中から高い頻度で発生するイベントの生起パターンを検出するアプリオリと呼ばれるアルゴリズムが開発されている（非特許文献１参照）。
【０００７】
図１８は、アプリオリアルゴリズムによるイベントの生起パターンの検出処理を説明する図である。図１８のＡからＤは個々のイベントを表しており、ＡＢ、ＡＢＣまたはＡＢＣＤなどは複数のイベントのまとまりを表している。
【０００８】
アプリオリアルゴリズムでは、個々のイベントを結合してイベントの生起パターンの候補を生成するとともに、生起頻度の低いイベントのパターンを除外して、生起頻度の高いイベントの生起パターンのみを検出する。そのため、生起頻度が低いが、重大な事故やトラブルにつながるようなイベントの生起パターンを検出することが難しい。
【０００９】
このようなアプリオアルゴリズムの欠点を克服するため、因果関係が有りそうなイベントの生起パターンを検出した後、その生起パターンに含まれるイベント間に因果関係が有るか否かを統計的な手法を用いて判定することにより、生起頻度は低いものの、関連性が高いと考えられるイベントの生起パターンを検出する因果関係検出装置が開示されている（特許文献１参照）。
【００１０】
また、生起頻度に基づいてイベントの生起パターンを検出するのではなく、条件付き確率を算出することにより、関連性が高いと考えられるイベントの生起パターンを検出する方法も提案されている（非特許文献２参照）。

【００１１】
【特許文献１】特開平１０－１３４０８６号公報
【非特許文献１】R. Agrawal, R. Srikant, "Fast Algorithms for Mining Association Rules", Proceedings of the 20th International Conference on Very Large Databases, Santiago, Chile, Sept. 1994.
【非特許文献２】S. Ma, J. Hellerstein, "Mining Mutually Dependent Patterns", 2001 IEEE International Conference on Data Mining, San Jose, California, Nov. 29 - Dec. 2, 2001.
【発明の開示】
【発明が解決しようとする課題】
【００１２】
しかしながら、上述した従来技術は、イベントログから高い頻度で生起するイベントの集合、あるいは、関連性が高いイベントの集合を生起パターンとして検出するのみであり、さらに詳細な情報をイベントログから抽出し、管理者が事故やトラブルを事前に回避する作業を強力に支援することが難しかった。
【００１３】
具体的には、管理者が従来技術により得られる情報は、あるイベントが生起した場合にそれに応じて生起する可能性の高いイベントの情報であり、管理者がより適切に事故やトラブルに対処することができるようにするために、イベントの生起パターンに対するさらに詳細な情報を提供することが難しいという問題があった。
【００１４】
この発明は、上述した従来技術による問題点を解消するためになされたものであり、生起したイベントの情報を記憶したイベントデータから、イベントの生起パターンについての詳細な情報を抽出することができるパターン検出プログラムを提供することを目的とする。
【課題を解決するための手段】
【００１５】
上述した課題を解決し、目的を達成するため、本発明は、生起したイベントに係る情報を記憶したイベントデータからイベントの生起パターンを検出する処理をコンピュータに実行させるパターン検出プログラムであって、イベント間において定義される複数種類の関係に係る情報に基づいて、前記イベントデータからイベントの生起パターンを検出する検出手順と、前記検出手順により検出されたイベントの生起パターンを出力する出力手順と、をコンピュータに実行させることを特徴とする。
【００１６】
また、本発明は、前記複数種類の関係に係る情報は、イベントの生起時刻およびイベントの生起確率に基づいて定義された情報であることを特徴とする。
【００１７】
また、本発明は、前記検出手順は、関係の有無を判定するイベント間の生起時刻の範囲に係る設定値を、生起パターンの検出結果に基づいて設定することを特徴とする。
【００１８】
また、本発明は、前記検出手順は、関係の有無を判定するイベント間の生起確率に係る設定値を、生起パターンの検出結果に基づいて設定することを特徴とする。
【００１９】
また、本発明は、前記検出手順は、前記イベントの生起パターンの検出結果を評価する評価関数に基づいて、関係の有無を判定するイベント間の生起時刻の範囲に係る設定値、または、関係の有無を判定するイベント間の生起確率に係る設定値を設定することを特徴とする。
【００２０】
また、本発明は、前記複数種類の関係に係る情報は、２つのイベントが生起した生起時刻の差の大小に応じて異なる種類の関係を定義した情報を含んだことを特徴とする。

【００２１】
また、本発明は、前記検出手順は、２つのイベントから構成される生起パターンを結合することにより、３つ以上のイベントから構成される生起パターンを検出することを特徴とする。
【００２２】
また、本発明は、前記検出手順は、生起パターンの結合の可否を判定する結合条件に基づいて、生起パターンの結合を実行するか否かを判定することを特徴とする。
【００２３】
また、本発明は、前記検出手順は、結合された生起パターンに含まれる部分が所定の基準を満足しているか否かを判定し、所定の基準を満足しない部分を生起パターンから削除することを特徴とする。
【００２４】
また、本発明は、前記検出手順は、生起パターンに含まれるイベント間の結合可能な関係に係る情報に基づいて、結合する生起パターンの組み合わせを選択することを特徴とする。
【００２５】
また、本発明は、前記出力手順は、生起パターンに含まれるイベント間の関係に係る情報に基づいて、前記検出手順により検出された生起パターンに含まれるイベント間の関係を統合し、イベント間の関係が統合された生起パターンを出力することを特徴とする。
【００２６】
また、本発明は、生起したイベントに係る情報を記憶したイベントデータからイベントの生起パターンを検出するパターン検出装置であって、イベント間において定義される複数種類の関係に係る情報に基づいて、前記イベントデータからイベントの生起パターンを検出する検出手段と、前記検出手段により検出されたイベントの生起パターンを出力する出力手段と、を備えたことを特徴とする。
【００２７】
また、本発明は、生起したイベントに係る情報を記憶したイベントデータからイベントの生起パターンを検出するパターン検出方法であって、イベント間において定義される複数種類の関係に係る情報に基づいて、前記イベントデータからイベントの生起パターンを検出する検出工程と、前記検出工程により検出されたイベントの生起パターンを出力する出力工程と、を含んだことを特徴とする。
【発明の効果】
【００２８】
本発明によれば、イベント間において定義される複数種類の関係に係る情報に基づいて、イベントデータからイベントの生起パターンを検出し、検出されたイベントの生起パターンを出力することとしたので、生起したイベントの情報を記憶したイベントデータから、イベントの生起パターンについての詳細な情報を抽出することができるという効果を奏する。
【００２９】
また、本発明によれば、複数種類の関係に係る情報は、イベントの生起時刻およびイベントの生起確率に基づいて定義された情報であることとしたので、イベント間の関係をイベントの生起時刻およびイベントの生起確率に基づいて柔軟に設定し、イベントの生起パターンについての詳細な情報を抽出することができるという効果を奏する。
【００３０】
また、本発明によれば、関係の有無を判定するイベント間の生起時刻の範囲に係る設定値を、生起パターンの検出結果に基づいて設定することとしたので、適切な設定値を自動的に設定することにより、イベント間における関係の有無を精度よく判定することができるという効果を奏する。
【００３１】
また、本発明によれば、関係の有無を判定するイベント間の生起確率に係る設定値を、

生起パターンの検出結果に基づいて設定することとしたので、適切な設定値を自動的に設定することにより、イベント間における関係の有無を精度よく判定することができるという効果を奏する。

【００３２】

また、本発明によれば、イベントの生起パターンの検出結果を評価する評価関数に基づいて、関係の有無を判定するイベント間の生起時刻の範囲に係る設定値、または、関係の有無を判定するイベント間の生起確率に係る設定値を設定することとしたので、評価が高い生起パターンを検出するのに適切な設定値を自動的に設定することができるという効果を奏する。

【００３３】

また、本発明によれば、複数種類の関係に係る情報は、２つのイベントが生起した生起時刻の差の大小に応じて異なる種類の関係を定義した情報を含んだこととしたので、生起パターンについてより詳細な情報を抽出することができるという効果を奏する。

【００３４】

また、本発明によれば、２つのイベントから構成される生起パターンを結合することにより、３つ以上のイベントから構成される生起パターンを検出することとしたので、３つ以上のイベントからなる生起パターンを効率的に検出することができるという効果を奏する。

【００３５】

また、本発明によれば、生起パターンの結合の可否を判定する結合条件に基づいて、生起パターンの結合を実行するか否かを判定することとしたので、所定の条件を満足する生起パターンのみを検出することができるという効果を奏する。

【００３６】

また、本発明によれば、結合された生起パターンに含まれる部分が所定の基準を満足しているか否かを判定し、所定の基準を満足しない部分を生起パターンから削除することとしたので、所定の基準を満足する生起パターンのみを検出することができるという効果を奏する。

【００３７】

また、本発明によれば、生起パターンに含まれるイベント間の結合可能な関係に係る情報に基づいて、結合する生起パターンの組み合わせを選択することとしたので、結合可能な生起パターンの組み合わせを効率的に探索し、生起パターンを結合することができるという効果を奏する。

【００３８】

また、本発明によれば、生起パターンに含まれるイベント間の関係に係る情報に基づいて、検出された生起パターンに含まれるイベント間の関係を統合し、イベント間の関係が統合された生起パターンを出力することとしたので、複雑なイベント間の関係を簡略化して、利用者が理解しやすい情報を提供することができるという効果を奏する。

【発明を実施するための最良の形態】

【００３９】

以下に添付図面を参照して、本発明に係るパターン検出プログラムの好適な実施例を詳細に説明する。

【実施例１】

【００４０】

まず、本発明に係るパターン検出処理の概念について説明する。図１は、本発明に係るパターン検出処理の概念を説明する図である。図１に示すように、本発明では、あるシステムに生起したイベントを記録したイベントログから、イベントパターンルール１０が生成される。

【００４１】

イベントパターンルール１０とは、イベントログから何らかの関係を有すると考えられるイベントが抽出されたイベントの生起パターンである。このイベントパターンルール１

０は、イベントログに記録されたイベント集合との間で照合され、システム障害などの発生を事前に検出するのに用いられる。このパターン検出処理の実行により、システムの管理作業を効率的に支援することができるようになる。

【００４２】

図１において、イベントパターンルール１０は、ノード（頂点）Ａ～Ｔと、ノードＡ～Ｔを他のノードＡ～Ｔと結合しているエッジ（辺）とから構成されている。ノードＡ～Ｔは、それぞれ生起したイベントを示している。

【００４３】

エッジは、ノードＡ～Ｔ間の結合関係を示すものであり、同時ルール、順序ルール、近接ルール、原因判定ルールおよび結果予測ルールの種類がある。また、同時ルールおよび近接ルールは方向のない無向エッジで表現され、順序ルール、原因判定ルールおよび結果予測ルールは方向がある有向エッジで表現される。

【００４４】

同時ルールは、実線で示されている関係であり、実線で結合されたイベントどうしが同時に生起することを意味する。順序ルールは、実線の矢印で示されている関係であり、矢印の方向にイベントが順番に生起することを意味する。近接ルールは、点線で示されている関係であり、点線で結合された各イベントの生起時刻が近いことを意味する。

【００４５】

原因判定ルールは、点線の矢印で示されている関係であり、矢印の先のイベントが生起する前に、矢印の元のイベントが生起することを意味する。結果予測ルールは、二重線の矢印で示されている関係であり、矢印の元のイベントが生起した場合に矢印の先のイベントが生起することを意味する。

【００４６】

このように、本発明では、同時ルール、順序ルール、近接ルール、結果予測ルールおよび原因判定ルールの複数のイベント間の関係を用いて、イベントログからイベントパターンルールを生成することとしているので、イベントの生起パターンにおけるイベント間の関係に係る詳細な情報をイベントログから抽出することができる。

【００４７】

この他、このパターン検出処理には、アプリオリアルゴリズムでは検出できなかった低頻度で生起するイベントの生起パターンを検出することができる、従来検出することが困難であった生起パターンを容易に検出できる、３つ以上のイベントを含んだ生起パターンを高速に検出することができるなどの長所がある。以下では、このような長所を有するパターン検出処理の特徴について、詳細に説明していく。

【００４８】

つぎに、本明細書で用いられる用語の詳細な説明をおこなう。「イベント」とは、顧客システムに生起した事象であり、生起時刻、イベント種別、属性の情報が対応付けられている。ここで、生起時刻は、イベントが生起した時刻である。イベント種別は、生起するイベントの種類を識別する識別情報である。属性は、イベントに係るその他の付加的な情報である。このようなイベントの情報を蓄積したものが「イベントログ」である。

【００４９】

「時間制約条件」とは、ほぼ共起するイベントを定義する条件である。具体的には、「時間制約条件」とは、あるイベントの生起時刻ｔ１と別のイベントの生起時刻ｔ２とが、近いか否かを判定する際に用いられる条件である。これを数式で表すと、

$$t1+ts \leqq t2 \leqq t1+te$$

となる。

【００５０】

ここで、ｔｓおよびｔｅは、２つのイベント間の生起時刻の近さを定義する所定の時間である。たとえば、２つのイベントが３００秒以内に発生する場合には、ｔｓ＝－３００秒、ｔｅ＝３００秒となる。以降、上記数式で示される時間制約条件を、Ｆｔ（ｔ１，ｔ２）と表すこととする。

【００５１】
「共起確率条件」とは、時間制約条件とともに、ほぼ共起するイベントを定義する条件である。具体的には、種別がｃ１である任意のイベントが時刻ｔ１に生起したとき、種別がｃ２である任意のイベントが、時間制約条件Ｆｔ（ｔ１，ｔ２）を満足する時刻ｔ２に生起する確率を、種別がｃ１であるイベントと種別がｃ２であるイベントとの共起確率と呼び、これをＰ（ｃ１，ｃ２）で表す。
【００５２】
そして、「共起確率条件」は、数式を用いて、
Ｐ（ｃ１，ｃ２）≧ｍｉｎｃｏｎｆ
と定義される。ここで、ｍｉｎｃｏｎｆは、０≦ｍｉｎｃｏｎｆ≦１の定数であり、これを最小確信度と呼ぶ。
【００５３】
種別ｃ１のイベントと種別ｃ２のイベントとが「ほぼ共起する」とは、「時間制約条件」および「共起確率条件」の両方を、種別ｃ１のイベントと種別ｃ２のイベントとが満足する場合のことである。以下では、種別ｃ１のイベントと種別ｃ２のイベントとの間の共起確率を、
Ｐ（ｃ１，ｃ２，Ｆｔ）
で表すこととする。
【００５４】
ここで、種別ｃ１のイベントが生起した回数をＮ（ｃ１）とし、種別ｃ１のイベントが生起した場合に、種別ｃ２のイベントが、Ｆｔ（ｔ１，ｔ２）の時間制約条件を満足する時刻ｔ２に生起した回数をＮ（ｃ１，ｃ２，Ｆｔ）とすると、共起確率Ｐ（ｃ１，ｃ２，Ｆｔ）は、
Ｐ（ｃ１，ｃ２，Ｆｔ）＝Ｎ（ｃ１，ｃ２，Ｆｔ）／Ｎ（ｃ１）
と表される。
【００５５】
また、時間制約条件Ｆｔ（ｔ１，ｔ２）は、ｔｓおよびｔｅで定義されるので、共起確率Ｐ（ｃ１，ｃ２，Ｆｔ）は、
Ｐ（ｃ１，ｃ２，Ｆｔ）
＝Ｎ（ｃ１，ｃ２，Ｆｔ）／Ｎ（ｃ１）
＝Ｎ（ｃ１，ｃ２，ｔｓ，ｔｅ）／Ｎ（ｃ１）
＝Ｐ（ｃ１，ｃ２，ｔｓ，ｔｅ）
と表すこともできる。
【００５６】
共起確率Ｐ（ｃ１，ｃ２，Ｆｔ）を用いて「ほぼ共起する」イベントの生起パターンを検出する際、種別ｃ１のイベントが発生した回数Ｎ（ｃ１）が極端に小さいと、計算された共起確率Ｐ（ｃ１，ｃ２，Ｆｔ）の信頼性が低くなる。そのため、
Ｎ（ｃ１）＜ｍｉｎｓｕｐ
となる種別ｃ１のイベントに係る生起パターンは除外することとする。ここで、ｍｉｎｓｕｐは、所定の閾値である。
【００５７】
つぎに、はじめに説明した「同時ルール」、「順序ルール」、「近接ルール」、「原因判定ルール」および「結果予測ルール」のイベント間の関係をさらに詳細に説明する。以下では、ｗを、イベントどうしが関連をもつとみなすことができる時間間隔の限度値とし、ｅを、イベントが発生した時刻の測定誤差や時刻の測定精度を考慮した、時刻のずれの許容限度値とする。なお、ｗおよびｅには、０＜ｅ＜ｗという関係がある。
【００５８】
「同時ルール」とは、同時に起きる種別ｃ１のイベントと種別ｃ２のイベントとの間の関係を示すものである。数式を用いると、この同時ルールは、
Ｐ（ｃ１，ｃ２，－ｅ，ｅ）≧ｍｉｎｃｏｎｆ，

かつ、
Ｐ（ｃ２，ｃ１，－ｅ，ｅ）≧ｍｉｎｃｏｎｆ
を満足するイベント間の関係として表される。
【００５９】
「順序ルール」とは、順番に起きる種別ｃ１のイベントと種別ｃ２のイベントとの間の関係を示すものである。数式を用いると、この順序ルールは、同時ルールの条件を満足しないイベントのうち、
Ｐ（ｃ１，ｃ２，－ｅ，ｗ）≧ｍｉｎｃｏｎｆ，
かつ、
Ｐ（ｃ２，ｃ１，－ｗ，ｅ）≧ｍｉｎｃｏｎｆ
を満足するイベント間の関係として表される。
【００６０】
「近接ルール」とは、順番に関係なく、近い時刻に発生する種別ｃ１のイベントと種別ｃ２のイベントとの間の関係を示すものである。数式を用いると、この近接ルールは、順序ルールの条件を満足しないイベントのうち、
Ｐ（ｃ１，ｃ２，－ｗ，ｗ）≧ｍｉｎｃｏｎｆ，
かつ、
Ｐ（ｃ２，ｃ１，－ｗ，ｗ）≧ｍｉｎｃｏｎｆ
を満足するイベント間の関係として表される。
【００６１】
「原因判定ルール」とは、種別ｃ２のイベントが発生する前に、種別ｃ１のイベントが発生するイベント間の関係を示すものである。数式を用いると、この原因判定ルールは、順序ルールの条件を満足しないイベントのうち、
Ｐ（ｃ２，ｃ１，－ｗ，ｅ）≧ｍｉｎｃｏｎｆ
を満足するイベント間の関係として表される。
【００６２】
「結果予測ルール」とは、種別ｃ１のイベントが発生した場合に、種別ｃ２のイベントが発生するイベント間の関係を示すものである。数式を用いると、この結果予測ルールは、順序ルールの条件を満足しないイベントのうち、
Ｐ（ｃ１，ｃ２，－ｅ，ｗ）≧ｍｉｎｃｏｎｆ
を満足するイベント間の関係として表される。
【００６３】
本発明に係るパターン検出処理では、種別ｃ１のイベントと種別ｃ２のイベントの組（ｃ１，ｃ２）が、上述した同時ルール、順序ルール、近接ルール、原因判定ルール、あるいは、結果予測ルールのいずれかを満足する場合に、そのイベントの組（ｃ１，ｃ２）が所定の結合関係を満足するペアルールとして抽出される。
【００６４】
つぎに、本発明に係るパターン検出装置の機能的構成について説明する。図２は、本発明に係るパターン検出装置２１の機能的構成を示す図である。図２に示すように、このパターン検出装置２１は、顧客システム２０とインターネット２２を介して接続されている。
【００６５】
顧客システム２０は、イベントログの解析により、障害の発生を予測あるいは検知する対象となるシステムである。この顧客システム２０は、発生したイベントの情報をイベントログとして記録し、パターン検出装置２１に送信する。
【００６６】
パターン検出装置２１は、顧客システム２０から受信したイベントログから、障害が発生する予兆と考えられるイベントの生起パターンをイベントパターンルールとして検出し、顧客システム２０の管理作業を支援する装置である。このパターン検出装置２１は、インターフェース部２１０、入力部２１１、表示部２１２、記憶部２１３および制御部２１

４を有する。
【００６７】
インターフェース部２１０は、インターネット２２を介して、顧客システム２０との間でデータの授受をおこなうネットワークインターフェースである。入力部２１１は、キーボードやマウスなどの入力デバイスである。表示部２１２は、ディスプレイなどの表示デバイスである。
【００６８】
記憶部２１３は、ハードディスク装置などの記憶デバイスである。この記憶部２１３は、イベントログ２１３ａ、関係定義データ２１３ｂおよびイベントパターンルール２１３ｃを記憶している。
【００６９】
イベントログ２１３ａは、顧客システム２０において発生したイベントの情報を蓄積したログであり、顧客システム２０から受信したものである。関係定義データ２１３ｂは、同時ルール、順序ルール、近接ルール、原因判定ルールおよび結果予測ルールのイベント間の関係を定義する定義式、ｗやｅ、ｍｉｎｃｏｎｆなどの各種設定値を記憶したデータである。イベントパターンルール２１３ｃは、検出されたイベントパターンルールを記憶したデータである。
【００７０】
制御部２１４は、パターン検出装置２１を全体制御する制御部である。この制御部２１４は、イベントログ管理部２１４ａ、関係定義データ管理部２１４ｂ、確率算出部２１４ｃ、ペアルール生成部２１４ｄ、複合ルール生成部２１４ｅ、ルール簡略化部２１４ｆおよびルール管理部２１４ｇを有する。
【００７１】
イベントログ管理部２１４ａは、顧客システム２０からイベントログを取得して、記憶部２１３にイベントログ２１３ａとして記憶する処理をおこなう。また、イベントログ管理部２１４ａは、イベントパターンルールが検出された場合に、顧客システム２０から取得したイベントログ内にイベントパターンルールとマッチするパターンが生起しているか否かを検出し、同様のパターンが検出された場合には、警告メッセージを出力するなどの処理をおこなう。
【００７２】
関係定義データ管理部２１４ｂは、同時ルール、順序ルール、近接ルール、原因判定ルールおよび結果予測ルールのイベント間の関係を定義する定義式、ｗやｅ、ｍｉｎｃｏｎｆなどの各種設定値の入力を顧客システム２０の管理者から受け付けて、関係定義データ２１３ｂとして記憶部２１３に記憶する。
【００７３】
確率算出部２１４ｃは、イベント間の関係を規定する共起確率Ｐ（ｃ１，ｃ２，ｔｓ，ｔｅ）を算出する。具体的には、確率算出部２１４ｃは、種別ｃ１のイベントが生起した数Ｎ（ｃ１）、および、種別ｃ１であるイベントが生起した場合に種別ｃ２であるイベントが生起した数Ｎ（ｃ１，ｃ２，ｔｓ，ｔｅ）を算出することにより、共起確率Ｐ（ｃ１，ｃ２，ｔｓ，ｔｅ）を算出する。
【００７４】
ペアルール生成部２１４ｄは、確率算出部２１４ｃにより算出された共起確率Ｐ（ｃ１，ｃ２，ｔｓ，ｔｅ）の情報を基にして、所定の関係を有するイベントの組をペアルールとしてイベントログから抽出する処理をおこなう。
【００７５】
具体的には、ペアルール生成部２１４ｄは、イベントログから任意の２つのイベントの組を取得して、取得したイベントの組が、同時ルール、順序ルール、近接ルール、原因判定ルール、あるいは、結果予測ルールのいずれかの条件に当てはまるか否かを調べ、いずれかの条件を満足した場合に、当該条件に対応するペアルールとしてイベントの組を抽出する。ペアルール生成部２１４ｄは、この処理を未調査のイベントの組がなくなるまで継

続する。

【００７６】

複合ルール生成部２１４ｅは、ペアルール生成部２１４ｄにより生成されたペアルールを結合し、３つ以上のイベントの組からなるイベントパターンルールを生成する。具体的には、複合ルール生成部２１４ｅは、ペアルールＡに含まれるイベントおよびペアルールＢに含まれるイベントとの和集合と、ペアルールＡの２つのイベント間の関係とペアルールＢの２つのイベント間の関係との和集合とにより構成されるルールを生成する。

【００７７】

そして、複合ルール生成部２１４ｅは、結合可能なペアルールあるいはルールがなくなるまで、ペアルールあるいはルールを結合し、図１に示したような３つ以上のイベントが結合されたイベントパターンルールを生成する。

【００７８】

ペアルールあるいはルールの結合は、図１に一例を示したように、同時ルールと順序ルールの結合など、異なる関係を有するペアルールあるいはルール間でもおこなわれる。また、他のペアルールと結合ができないペアルールは、複合ルール生成部２１４ｅにより、２つのイベントからなるイベントパターンルールとして設定される。

【００７９】

ルール簡略化部２１４ｆは、複合ルール生成部２１４ｅにより生成されたイベントパターンルールを、人が理解しやすいように簡略化する処理をおこなう。具体的には、ルール簡略化部２１４ｆは、イベントパターンルールに含まれるイベントをノードで表し、イベント間の関係をエッジで表したグラフを生成する。

【００８０】

そして、ルール簡略化部２１４ｆは、複数のノードからなる強連結成分を抽出し、強連結成分を１つのノードに統合する処理をおこなう。ここで、強連結成分とは、グラフのエッジを辿った場合に互いに到達可能であるノードの集合のことである。

【００８１】

図３は、イベントパターンルールの簡略化処理を説明する図である。図３は、図１のイベントパターンルール１０が簡略化されたものである。図３に示すように、ルール簡略化部２１４ｆは、同時ルール（図１の実線）の関係で結合されているノードどうしを強連結成分として抽出し、一つに統合する処理をおこなう。たとえば、図１のノードＢ、ノードＤ、ノードＥ、ノードＦ、ノードＧおよびノードＩは、強連結成分あるので、図３に示すように１つにまとめられる。

【００８２】

また、ルール簡略化部２１４ｆは、イベントパターンルールに含まれる順序ルールで連結されたノードの集合に対して、推移縮約を適用する。推移縮約とは、ノードＡから出発してノードＢに到達する経路が複数ある場合に、それらの経路のどのノードからもノードＢに到達できるような１つの経路で複数の経路を置き換え、経路を統合する処理である。

【００８３】

図１の例では、ノードＫとノードＭ、ノードＭとノードＬおよびノードＫとノードＬとは、順序ルールの関係にあり、ノードＫからノードＬに直接至る経路と、ノードＫ、ノードＭ、ノードＬと辿る経路とがあるが、図３に示すように、２つの経路のどのノードからもノードＬに到達できる１つの経路、すなわちこの場合は、ノードＫ、ノードＭ、ノードＬと辿る経路に２つの経路が統合される。

【００８４】

推移縮約を適用することにより、順序ルールにより示されるイベントの生起順序の情報を、経路の途中のイベントについても省略せずに、イベントパターンルールを簡略化することができる。

【００８５】

その後、ルール簡略化部２１４ｆは、同時ルールおよび順序ルールの結合関係が簡略化されたイベントパターンルールに、簡略化処理が適用されなかった順序ルールの関係、近

接ルールの関係、原因判定ルールの関係、および、結果予測ルールの関係を追加し、最終的なイベントパターンルールを生成する。

【００８６】

このイベントパターンルールの簡略化処理は、イベントパターンルールに含まれるイベントの数が大きくなるほど効果的なものとなる。図４は、イベントパターンルールの簡略化処理の効果を説明する図である。

【００８７】

図４の簡略化処理前のイベントパターンルール４０に示すように、イベントパターンルールに含まれるイベントの数が大きい場合には、各イベント間の関係を把握することが困難であるが、簡略化処理後のイベントパターンルール４１に示すように、簡略化処理がなされた後は、顧客システム２０の管理者は有益なルールや、以前認知していなかった新たなイベントの生起パターンを把握して、その知識を顧客システム２０の管理作業に生かすことができるようになる。

【００８８】

図２の説明に戻ると、ルール管理部２１４ｇは、複合ルール生成部２１４ｅにより生成されたイベントパターンルール、あるいは、ルール簡略化部２１４ｆにより簡略化されたイベントパターンルールを記憶部２１３に記憶し、また、表示部２１２などに出力する処理をおこなう。

【００８９】

図３に示したようなイベントパターンルールを表示部２１２に出力する際には、ルール管理部２１４ｇは、マグネティックスプリングモデルなどによるグラフ描画法によりイベントパターンルールを出力する。

【００９０】

つぎに、実施例１に係るパターン検出処理の処理手順について説明する。図５は、実施例１に係るパターン検出処理の処理手順を示すフローチャートである。図５に示すように、まず、パターン検出装置２１の確率算出部２１４ｃは、記憶部２１３に記憶されたイベントログ２１３ａおよび関係定義データ２１３ｂを読み込み（ステップＳ１０１）、読み込んだイベントログ２１３ａからイベントの共起確率Ｐ（ｃ１，ｃ２，ｔｓ，ｔｅ）を算出する（ステップＳ１０２）。

【００９１】

続いて、ペアルール算出部２１４ｄは、確率算出部２１４ｃにより算出された共起確率Ｐ（ｃ１，ｃ２，ｔｓ，ｔｅ）と、関係定義データ２１３ｂとから、ペアルールを生成する処理をおこなう（ステップＳ１０３）。

【００９２】

その後、複合ルール生成部２１４ｅは、結合可能なペアルールを結合してイベントパターンルールを生成し（ステップＳ１０４）、さらに、ルール簡略化部２１４ｆは、複合ルール生成部２１４ｅにより生成されたイベントパターンルールを簡略化する処理をおこなう（ステップＳ１０５）。

【００９３】

そして、ルール管理部２１４ｇは、イベントパターンルールを記憶部２１３に記憶し、また、表示部２１２に出力する処理をおこない（ステップＳ１０６）、このパターン検出処理を終了する。

【００９４】

つぎに、図５に示したパターン検出処理のステップＳ１０２において、確率算出部２１４ｃが共起確率Ｐ（ｃ１，ｃ２，ｔｓ，ｔｅ）の算出に用いるイベントの発生回数Ｎ（ｃ１）およびＮ（ｃ１，ｃ２，ｔｓ，ｔｅ）の算出処理の処理手順について説明する。図６は、イベントの発生回数Ｎ（ｃ１）およびＮ（ｃ１，ｃ２，ｔｓ，ｔｅ）の算出処理の処理手順を示すフローチャートである。

【００９５】

図６に示すように、まず、パターン検出装置２１の確率算出部２１４ｃは、イベントロ

グ内に含まれるイベントを生起時刻順に並べ替える処理をおこなう（ステップＳ２０１）。そして、確率算出部２１４ｃは、探索マーカを、並べ替えたイベントログの先頭のイベントを指すよう設定し（ステップＳ２０２）、さらに、イベントの生起数をカウントするカウンタの値を０に初期化する（ステップＳ２０３）。

【００９６】

続いて、確率算出部２１４ｃは、イベントログの先頭のイベントを選択し（ステップＳ２０４）、選択したイベントの種別をｃ１、生起時刻をｔ１に設定する（ステップＳ２０５）。その後、確率算出部２１４ｃは、種別ｃ１のイベントの生起数カウンタに１を加算する処理をおこなう（ステップＳ２０６）。この生起数カウンタの値が、Ｎ（ｃ１）の値となる。

【００９７】

そして、確率算出部２１４ｃは、生起時刻がｔ１＋ｔｓ以降となるイベントを探索マーカが指すまで探索マーカを進めた後（ステップＳ２０７）、探索マーカが指しているイベントの種別をｃ２、生起時刻をｔ２に設定する処理をおこなう（ステップＳ２０８）。ここで、ｔｓは、時間制約条件ｔ１＋ｔｓ≦ｔ２≦ｔ１＋ｔｅにおける閾値ｔｓである。

【００９８】

その後、確率算出部２１４ｃは、ｔ２がｔ１＋ｔｅよりも大きいか否かを調べる（ステップＳ２０９）。ここで、ｔｅは、時間制約条件ｔ１＋ｔｓ≦ｔ２≦ｔ１＋ｔｅにおける閾値ｔｅである。

【００９９】

そして、ｔ２がｔ１＋ｔｅよりも大きくない場合には（ステップＳ２０９，Ｎｏ）、確率算出部２１４ｃは、種別ｃ１および種別ｃ２のイベントの組の生起数カウンタに１を加算し（ステップＳ２１０）、探索マーカをつぎのイベントを指すよう１つ進めて（ステップＳ２１１）、ステップＳ２０８に移行し、それ以後の処理を継続する。このイベントの組の生起数カウンタの値が、Ｎ（ｃ１，ｃ２，ｔｓ，ｔｅ）の値となる。

【０１００】

ｔ２がｔ１＋ｔｅよりも大きい場合には（ステップＳ２０９，Ｙｅｓ）、確率算出部２１４ｃは、選択するつぎのイベントがイベントログ内にあるか否かを調べ（ステップＳ２１２）、つぎのイベントがある場合には（ステップＳ２１２，Ｙｅｓ）、つぎのイベントを選択し（ステップＳ２１３）、ステップＳ２０５に移行して、それ以後の処理を継続する。

【０１０１】

イベントログ内に選択するつぎのイベントがない場合には（ステップＳ２１２，Ｎｏ）、そのままこのイベントの発生回数Ｎ（ｃ１）およびＮ（ｃ１，ｃ２，ｔｓ，ｔｅ）の算出処理を終了する。

【０１０２】

上記発生回数Ｎ（ｃ１）およびＮ（ｃ１，ｃ２，ｔｓ，ｔｅ）の算出処理の算出結果を用いて、確率算出部２１４ｃは、生起確率Ｐ（ｃ１，ｃ２，ｔｓ，ｔｅ）の値を、

Ｐ（ｃ１，ｃ２，ｔｓ，ｔｅ）

＝Ｎ（ｃ１，ｃ２，ｔｓ，ｔｅ）／Ｎ（ｃ１）

の式により算出する。

【０１０３】

つぎに、図５に示したパターン検出処理のステップＳ１０４において、複合ルール生成部２１４ｅがペアルールを結合することによりイベントパターンルールを生成する処理の処理手順について説明する。図７は、ペアルールの結合によりイベントパターンルールを生成する処理の処理手順を示すフローチャートである。

【０１０４】

図７に示すように、まず、パターン検出装置２１の複合ルール生成部２１４ｅは、ルールを登録する候補リストにすべてのペアルールを登録する（ステップＳ３０１）。そして、複合ルール生成部２１４ｅは、生成されたイベントパターンルールを登録する確定リス

トを空にして初期化する（ステップＳ３０２）。

【０１０５】

続いて、複合ルール生成部２１４ｅは、候補リストからルール（ペアルールを含む）をルールＡとして取り出す処理を実行し（ステップＳ３０３）、ルールＡが取り出せたか否かを調べる（ステップＳ３０４）。ルールＡが取り出せなかった場合には（ステップＳ３０４，Ｎｏ）、複合ルール生成部２１４ｅは、確定リストに登録されたルールを出力し（ステップＳ３１０）、イベントパターンルールを生成する処理を終了する。

【０１０６】

ルールＡが取り出せた場合には（ステップＳ３０４，Ｙｅｓ）、複合ルール生成部２１４ｅは、候補リストの中からルールＡと共通するイベントを含むルールをルールＢとして取り出す処理を実行し（ステップＳ３０５）、ルールＢを取り出せたか否かを調べる（ステップＳ３０６）。

【０１０７】

ルールＢを取り出せなかった場合には（ステップＳ３０６，Ｎｏ）、複合ルール生成部２１４ｅは、ルールＡを確定リストに登録し（ステップＳ３０９）、ステップＳ３０３に移行して、それ以後の処理を継続する。

【０１０８】

ルールＢを取り出せた場合には（ステップＳ３０６，Ｙｅｓ）、複合ルール生成部２１４ｅは、ルールＡとルールＢとを結合したルールを生成し（ステップＳ３０７）、生成したルールを候補リストに登録する（ステップＳ３０８）。そして、ステップＳ３０３に移行して、それ以後の処理を継続する。

【０１０９】

つぎに、図５に示したパターン検出処理のステップＳ１０５において、ルール簡略化部２１４ｆがイベントパターンルールを簡略化する処理の処理手順について説明する。図８は、イベントパターンルールを簡略化する処理の処理手順を示すフローチャートである。

【０１１０】

図８に示すように、まず、パターン検出装置２１のルール簡略化部２１４ｆは、複合ルール生成部２１４ｅにより生成されたイベントパターンルールにおける順序ルールおよび同時ルールの情報を取得する（ステップＳ４０１）。そして、ルール簡略化部２１４ｆは、順序ルールおよび同時ルールに含まれる各イベントに対応するノードをグラフに設定する（ステップＳ４０２）。

【０１１１】

その後、ルール簡略化部２１４ｆは、あるイベントＡから他のイベントＢへの順序を有する順序ルールに対して、イベントＡに対応するノードＡからイベントＢに対応するノードＢへの向きを有する有向エッジを生成する（ステップＳ４０３）。さらに、ルール簡略化部２１４ｆは、イベントＡおよびイベントＢ間の同時ルールに対して、ノードＡからノードＢへ、および、ノードＢからノードＡへの向きを有する２本の有向エッジを生成する（ステップＳ４０４）。

【０１１２】

続いて、ルール簡略化部２１４ｆは、順序ルールおよび同時ルールが有向エッジを用いて表されたグラフの強連結成分を求める処理をおこない（ステップＳ４０５）、得られた強連結成分を強連結成分ごとに１つのノードに統合する処理をおこなう（ステップＳ４０６）。

【０１１３】

さらに、ルール簡略化部２１４ｆは、グラフの推移縮約を実行し、ノードＡからノードＢに到達する経路が複数ある場合に、それらの経路のどのノードからもノードＢに到達できるような１つの経路で複数の経路を置き換え、経路を統合する処理をおこなう（ステップＳ４０７）。なお、推移縮約が適用されなかった順序ルールについては、そのまま有向エッジの設定を保持する。

【０１１４】

その後、ルール簡略化部２１４ｆは、順序ルールおよび同時ルール以外のルール、すなわち、近接ルール、原因判定ルール、および、結果予測ルールを追加し（ステップＳ４０８）、イベントパターンルールを簡略化する処理を終了する。

【０１１５】

上述してきたように、本実施例１では、同時ルール、順序ルール、近接ルール、原因判定ルール、および、結果予測ルールなどの、イベント間において定義される複数種類の関係に係る情報に基づいて、確率算出部２１４ｃおよびペアルール生成部２１４ｄが、イベントログからイベントパターンルールを検出し、検出されたイベントパターンルールを出力することとしたので、イベントログから、イベントの生起パターンについての詳細な情報を抽出することができる。

【０１１６】

また、本実施例１では、上記複数種類の関係に係る情報は、イベントの生起時刻およびイベントの生起確率に基づいて定義された情報であることとしたので、イベント間の関係をイベントの生起時刻およびイベントの生起確率に基づいて柔軟に設定し、イベントの生起パターンについての詳細な情報を抽出することができる。

【０１１７】

また、本実施例１では、複数種類の関係に係る情報は、２つのイベントが生起した生起時刻の差の大小に応じて、イベント間の関係を同時ルールと近接ルールとに分けて定義した情報を含んだこととしたので、生起パターンについてより詳細な情報を抽出することができる。

【０１１８】

また、本実施例１では、複合ルール生成部２１４ｅが、２つのイベントから構成されるペアルールを結合することにより、３つ以上のイベントから構成されるイベントパターンルールを検出することとしたので、３つ以上のイベントからなる生起パターンを効率的に検出することができる。

【０１１９】

また、本実施例１では、ルール簡略化部２１４ｆが、イベントパターンルールに含まれるイベント間の関係に係る情報に基づいて、検出されたイベントパターンルールに含まれるイベント間の関係を統合し、イベント間の関係が統合されたイベントパターンルールを出力することとしたので、複雑なイベント間の関係を簡略化して、顧客システム２０の管理者が理解しやすい情報を提供することができる。

【実施例２】

【０１２０】

ところで、実施例１では、ペアルールを結合することによりイベントパターンルールを生成することとしたが、ペアルールの結合が有効なものか否かを判定し、有効なペアルールの結合から構成されるイベントパターンルールのみを出力するようにしてもよい。そこで、本実施例２では、ペアルールの結合が有効なものか否かを判定する場合について説明する。

【０１２１】

本実施例２に係るパターン検出処理においては、図２に示したパターン検出装置２１の複合ルール生成部２１４ｅが、ルールの結合前にあらかじめ定めた結合条件に基づいて、ルールの結合が有効であるか否かを判定し、有効であると判定された場合に、ルールの結合を実行する。

【０１２２】

たとえば、種別Ａのイベントおよび種別Ｂのイベントからなるペアルール（Ａ，Ｂ）、種別Ｂのイベントおよび種別Ｃのイベントからなるペアルール（Ｂ，Ｃ）、種別Ｃのイベントおよび種別Ｄのイベントからなるペアルール（Ｃ，Ｄ）、および、種別Ｄのイベントおよび種別Ｅのイベントからなるペアルール（Ｄ，Ｅ）があり、これらのペアルールが最小確信度ｍｉｎｃｏｎｆが０．９という条件で生成されているものとする。

【０１２３】

そして、これらのペアルールが結合され、（Ａ，Ｂ，Ｃ，Ｄ，Ｅ）という５つのイベントから構成されるルールが生成されると、イベントＡとイベントＥとの間の共起確率は
$0.9^4 = 0.6561$
と小さくなってしまい、ルールの有効性が低くなる。

【０１２４】

そのため、「結合時の共起確率が０．７以上」という結合条件をあらかじめ定めておき、この結合条件を満足するルールのみを結合する。この場合、図７のステップＳ３０５は、つぎのように変更される。「候補リストからルールＡと共通するイベントを含み、かつ、ルールＡと所定の結合条件を満足するルールをルールＢとして取り出す処理を実行する。」

【０１２５】

このように、結合条件を満足するルール間でのみ結合をおこなうことにより、顧客システム２０の管理者に有用なイベントパターンルールのみを抽出することができるようになる。

【０１２６】

なお、上記処理では、結合条件を満足するルール間でのみ結合を実行することとしたが、ルールの結合処理の実行後、規定を満足しないイベントパターンルールの部分を削除することとしてもよい。

【０１２７】

図９は、イベントパターンルールから規定違反のルール部分を削除する処理の処理手順を示すフローチャートである。この処理は、図７のステップＳ３１０の代わりにおこなわれる処理である。

【０１２８】

図９に示すように、まず、図２に示したパターン検出装置２１の複合ルール生成部２１４ｅは、確定リストからルールをルールＣとして取り出す処理を実行し（ステップＳ５０１）、ルールＣが取り出せたか否かを調べる（ステップＳ５０２）。

【０１２９】

ルールＣが取り出せなかった場合には（ステップＳ５０２，Ｎｏ）、複合ルール生成部２１４ｅは、確定リストに登録されたルールを出力し（ステップＳ５０３）、規定違反のルール部分を削除する処理を終了する。

【０１３０】

ルールＣが取り出せた場合には（ステップＳ５０２，Ｙｅｓ）、複合ルール生成部２１４ｅは、ルールＣが規定違反か否かを調べ（ステップＳ５０４）、規定違反でない場合には（ステップＳ５０４，Ｎｏ）、確定リストからつぎのルールをルールＣとして取り出す処理を実行し（ステップＳ５１０）、ステップＳ５０２に移行して、それ以後の処理を継続する。

【０１３１】

ルールＣが規定違反である場合には（ステップＳ５０４，Ｙｅｓ）、複合ルール生成部２１４ｅは、ルールＣに含まれ、関係を有する２つのイベントのうち、削除すべき２つのイベントを選択する（ステップＳ５０５）。具体的には、複合ルール生成部２１４ｅは、ルールＣからルールＣに含まれる２つのイベントを削除する場合に、ルールＣの規定違反の度合いが最も小さくなるものを削除する。

【０１３２】

その後、複合ルール生成部２１４ｅは、選択された２つのイベントをルールＣから削除してルールＤを生成し（ステップＳ５０６）、ルールＤが規定違反か否かを調べる処理をおこなう（ステップＳ５０７）。

【０１３３】

ルールＤが規定違反でない場合には（ステップＳ５０７，Ｎｏ）、複合ルール生成部２１４ｅは、ルールＤを出力し（ステップＳ５０８）、ステップＳ５１０に移行して、それ以後の処理を継続する。ルールＤが規定違反である場合には（ステップＳ５０７，Ｙｅｓ

）、複合ルール生成部２１４ｅは、ルールＤを確定リストに登録し（ステップＳ５０９）、ステップＳ５１０に移行して、それ以後の処理を継続する。

【０１３４】

このように、規定を満足しないイベントパターンルールの部分を削除することにより、顧客システム２０の管理者に有用なイベントパターンルールのみを抽出することができるようになる。

【０１３５】

なお、上述したように、結合条件や規定に基づいてルールの結合が有効なものか否かを判定する場合には、結合条件や規定の設定により判定に要する計算量が大きくなり、実用上問題となる場合がある。そのため、所定の関係を有するルールと結合可能なルールの関係の情報をあらかじめ記憶しておき、その情報に基づいてルールどうしの結合を実行することとしてもよい。

【０１３６】

図１０は、所定の関係を有するルールと結合可能なルールの関係を記憶した結合表の一例を示す図である。図１０に示すように、この例では、同時ルール、順序ルールおよび近接ルールの結合関係を有するルールどうしは結合が可能となるよう設定されている。

【０１３７】

しかし、結果予測ルールの関係を有するルールは、同時ルール、順序ルール、近接ルールおよび結果予測ルールの関係を有するルールとの間での結合は可能であるものの、原因判定ルールとの間の結合は禁止されている。

【０１３８】

同様に、原因判定ルールの関係を有するルールは、同時ルール、順序ルール、近接ルールおよび原因判定ルールの関係を有するルールとの間での結合は可能であるものの、結果予測ルールとの間の結合は禁止されている。

【０１３９】

このように、結合可能なルールの関係の情報をあらかじめ記憶しておき、その情報に基づいて、結合するルールの候補を限定することにより、ルールの結合を高速に実行することができる。

【０１４０】

上述してきたように、本実施例２では、複合ルール生成部２１４ｅが、ルールの結合の可否を判定する結合条件に基づいて、ルールの結合を実行するか否かを判定することとしたので、所定の条件を満足するイベントパターンルールのみを検出することができる。

【０１４１】

また、本実施例２では、複合ルール生成部２１４ｅが、結合されたイベントパターンルールに含まれる部分が規定を満足しているか否かを判定し、規定を満足しない部分をイベントパターンルールから削除することとしたので、規定を満足するイベントパターンルールのみを検出することができる。

【０１４２】

また、本実施例２では、複合ルール生成部２１４ｅが、ルールに含まれるイベント間の結合可能な関係に係る情報に基づいて、結合するルールの組み合わせを選択することとしたので、結合可能なルールの組み合わせを効率的に探索し、ルールを結合することができる。

【実施例３】

【０１４３】

ところで、上記実施例１および２では、時間制約条件Ｆｔ（ｔ１，ｔ２）において、２つのイベント間の生起時刻の近さを定義する時間ｔｓおよびｔｅをあらかじめ設定しておくこととしたが、実際のイベントログの分析においては、イベント間で関係が見出される生起時刻の範囲が不明である場合が多いため、時間ｔｓおよびｔｅをあらかじめ設定することが難しい場合がある。そこで、本実施例３では、イベント間に関係が見出される時間間隔をあらかじめ設定しておくのではなく、適切な時間間隔を自動的に設定する場合につ

いて説明する。

【０１４４】

実施例３では、時間制約条件Ｆｔ（ｔ１，ｔ２）を

ｔ１－ｗ≦ｔ２≦ｔ１

と定義する。ここで、ｗは、イベント間に関係が見出される時間間隔を決定する閾値であり、以下に説明するような方法で自動的に設定される値である。この場合、共起確率Ｐ（ｃ１，ｃ２，ｔｓ，ｔｅ）はＰ（ｃ１，ｃ２，－ｗ，０）と表される。

【０１４５】

本実施例３に係るパターン検出処理においては、図２に示したパターン検出装置２１の確率算出部２１４ｃが、

Ｐ（ｃ１，ｃ２，－ｗ，０）≧ｍｉｎｃｏｎｆ

となる閾値ｗを求めることにより、イベント間に関係が見出される適切な時間間隔を決定する。

【０１４６】

まず、確率算出部２１４ｃが共起確率Ｐ（ｃ１，ｃ２，－ｗ，０）の算出に用いるイベントの発生回数Ｎ（ｃ１）およびＮ（ｃ１，ｃ２，－ｗ，０）の算出処理の処理手順について説明する。図１１は、イベントの発生回数Ｎ（ｃ１）およびＮ（ｃ１，ｃ２，－ｗ，０）の算出処理の処理手順を示すフローチャートである。

【０１４７】

なお、イベントの発生回数Ｎ（ｃ１）およびＮ（ｃ１，ｃ２，－ｗ，０）を算出する前に、閾値ｗの候補値をいくつか設定しておく。設定された候補値を小さい順に、ｗ１、ｗ２、・・・、ｗＮとし、候補値の個数をＮｗとする。ここで、ｗＮは、無限大の時間を表す。また、２倍ずつ増加するような候補値を２０個ほど用意すると、イベント間の関係を見い出す時間間隔のほとんどに対応することができるようになり好ましい。

【０１４８】

図１１に示すように、まず、確率算出部２１４ｃは、イベントログ内に含まれるイベントを生起時刻順に並べ替える処理をおこなう（ステップＳ６０１）。そして、確率算出部２１４ｃは、探索マーカを、並べ替えたイベントログの先頭のイベントを指すよう設定し（ステップＳ６０２）、さらに、イベントの生起数をカウントするカウンタの値を０に初期化する（ステップＳ６０３）。

【０１４９】

続いて、確率算出部２１４ｃは、イベントの生起時刻を記憶する生起時刻テーブルを用意する（ステップＳ６０４）。ここで、生起時刻テーブルは、イベントの種別の数だけイベントを登録する記憶領域を有している。そして、この時点では、生起時刻テーブルには何も登録されておらず、以下に説明する処理により、生起時刻が新しいイベントから順次登録されていく。

【０１５０】

その後、確率算出部２１４ｃは、イベントログの先頭のイベントを選択し（ステップＳ６０５）、選択したイベントの種別をｃ１、生起時刻をｔ１に設定する（ステップＳ６０６）。そして、確率算出部２１４ｃは、種別ｃ１のイベントの生起数カウンタに１を加算する（ステップＳ６０７）。この生起数カウンタの値が、Ｎ（ｃ１）の値となる。

【０１５１】

続いて、確率算出部２１４ｃは、種別ｃ１のイベントの直前に生起したイベントを生起時刻テーブルから検索する（ステップＳ６０８）。そして、確率算出部２１４ｃは、種別ｃ１のイベントの直前に生起したイベントがあったか否かを調べ（ステップＳ６０９）、イベントがなかった場合には（ステップＳ６０９，Ｎｏ）、種別ｃ１のイベントの生起時刻ｔ１を生起時刻テーブルに登録する処理をおこなう（ステップＳ６１５）。

【０１５２】

種別ｃ１のイベントの直前に生起したイベントがあった場合には（ステップＳ６０９，Ｙｅｓ）、確率算出部２１４ｃは、検索されたイベントの種別をｃ２、生起時刻をｔ２に

設定する処理をおこなう（ステップＳ６１０）。

【０１５３】

そして、確率算出部２１４ｃは、ｔ２－ｔ１よりも値が大きい閾値ｗｘ（ｘ＝１、２、・・・、Ｎ）のうち、最小のものを抽出する（ステップＳ６１１）。そして、確率算出部２１４ｃは、ｗｘに対する種別ｃ１および種別ｃ２のイベントの組の生起数カウンタに１を加算する（ステップＳ６１２）。このイベントの組の生起数カウンタの値が、Ｎ（ｃ１，ｃ２，－ｗｘ，０）の値となる。

【０１５４】

続いて、確率算出部２１４ｃは、生起時刻テーブルから種別ｃ２のイベントの前に生起したイベントを検索し（ステップＳ６１３）、イベントがあったか否かを調べる（ステップＳ６１４）。そして、イベントがあった場合には（ステップＳ６１４，Ｙｅｓ）、確率算出部２１４ｃは、ステップＳ６１０に移行して、それ以後の処理を継続する。

【０１５５】

つぎのイベントがなかった場合には（ステップＳ６１４，Ｎｏ）、確率算出部２１４ｃは、種別ｃ１のイベントの生起時刻ｔ１を生起時刻テーブルに登録し（ステップＳ６１５）、イベントログからつぎのイベントを選択する処理をおこなう（ステップＳ６１６）。

【０１５６】

そして、確率算出部２１４ｃは、検索の結果、つぎのイベントがあったか否かを調べ（ステップＳ６１７）、つぎのイベントがあった場合には（ステップＳ６１７，Ｙｅｓ）、ステップＳ６０６に移行して、それ以後の処理を継続する。つぎのイベントがなかった場合には（ステップＳ６１７，Ｎｏ）、イベントの発生回数Ｎ（ｃ１）およびＮ（ｃ１，ｃ２，－ｗｘ，０）の算出処理を終了する。

【０１５７】

その後、確率算出部２１４ｃは、発生回数Ｎ（ｃ１）およびＮ（ｃ１，ｃ２，－ｗｘ，０）の算出結果を用いて、生起確率Ｐ（ｃ１，ｃ２，－ｗｘ，０）の値を、

Ｐ（ｃ１，ｃ２，－ｗｘ，０）

＝Ｎ（ｃ１，ｃ２，－ｗｘ，０）／Ｎ（ｃ１）

の式により算出する。

【０１５８】

そして、確率算出部２１４ｃは、各種別のイベントについて、

Ｐ（ｃ１，ｃ２，－ｗｘ，０）≧ｍｉｎｃｏｎｆ

となる最小のｗｘを選択し、選択されたｗｘの値を時間制約条件Ｆｔ（ｔ１，ｔ２）の閾値ｗとして設定する処理をおこなう。ここで、ｗｘが無限大であった場合には（ｗｘ＝ｗＮ）、イベント間に関係が見出される適切な時間間隔がなかったことを意味する。

【０１５９】

なお、実際にはイベント間の関係を見いだすための時間間隔が長くなるほど、イベント間の共起確率Ｐ（ｃ１，ｃ２，－ｗｘ，０）が大きくなり、本来無関係なイベント間に共起性があるように判定される危険がある。そのため、以下に説明するような方法で、無効なイベント間の関係を棄却する処理をおこなう。

【０１６０】

まず、種別ｃ１のイベントの生起と種別ｃ２のイベントの生起とが独立であると仮定した場合に、

ｔ１－ｗ≦ｔ２≦ｔ１

である時間範囲に種別ｃ２のイベントが生起する確率をＰ’（ｃ２，ｗ）とする。ここで、ｔ１は、種別ｃ１のイベントの生起時刻であり、ｔ２は、種別ｃ２のイベントの生起時刻である。

【０１６１】

種別ｃ２のイベントが生起する確率をこのように定義すると、種別ｃ１のイベントと種別ｃ２のイベントとの間に相関関係があることは、

Ｐ（ｃ１，ｃ２，－ｗ，０）＞Ｐ’（ｃ２，ｗ）

と表される。
【０１６２】
ここで、生起確率Ｐ’（ｃ２，ｗ）は、イベントの生起時刻の分布モデルを与えることにより決定される。ここでは、種別ｃ２のイベントの生起時刻は、一様に分布すると仮定する。すなわち、イベントログにイベントが記録された期間をＴとすると、種別ｃ２のイベントの時間密度ｄ（ｃ２）は、
ｄ（ｃ２）＝Ｎ（ｃ２）／Ｔ
となる。ここで、Ｎ（ｃ２）は、種別ｃ２のイベントが期間Ｔ内に生起した数である。
【０１６３】
したがって、生起確率Ｐ’（ｃ２，ｗ）は、
Ｐ’（ｃ２，ｗ）＝ｄ（ｃ２）×ｗ＝Ｎ（ｃ２）×ｗ／Ｔ
により算出することができる。
【０１６４】
確率算出部２１４ｃは、このようにして算出した生起確率Ｐ’（ｃ２，ｗ）を用いて、共起関係にないイベント間の組み合わせを棄却する。具体的には、確率算出部２１４ｃは、
Ｐ（ｃ１，ｃ２，－ｗ，０）＞θ×Ｐ’（ｃ２，ｗ）
を満足しない種別ｃ１のイベントおよび種別ｃ２のイベントの組み合わせを棄却する。ここで、θは、種別ｃ１のイベントおよび種別ｃ２のイベントの相関の強さを表す１以上の実数である。
【０１６５】
以上説明してきたように、本実施例３では、確率算出部２１４ｃが、関係の有無を判定するイベント間の生起時刻の範囲に係る設定値ｗを、さまざまな候補値ｗｘに対して共起確率Ｐ（ｃ１，ｃ２，－ｗ，０）が最小確信度ｍｉｎｃｏｎｆ以上となるイベントの生起パターンを検出した結果に基づいて設定することとしたので、適切な設定値ｗを自動的に設定することにより、イベント間における関係の有無を精度よく判定することができる。
【実施例４】
【０１６６】
ところで、上記実施例１、２および３では、共起確率条件において、最小確信度ｍｉｎｃｏｎｆをあらかじめ設定しておくこととしたが、イベント間における関係の有無を判定するのに用いられる最小確信度ｍｉｎｃｏｎｆをあらかじめ適切に設定するのは難しい。そこで、本実施例４では、最小確信度ｍｉｎｃｏｎｆをあらかじめ設定しておくのではなく、適切な最小確信度ｍｉｎｃｏｎｆを自動的に設定する場合について説明する。
【０１６７】
図１２は、最小確信度ｍｉｎｃｏｎｆの自動設定によるパターン検出処理の処理手順を示すフローチャートである。図１２に示すように、まず、図２に示したパターン検出装置２１の確率算出部２１４ｃは、記憶部２１３に記憶されたイベントログ２１３ａおよび関係定義データ２１３ｂを読み込む（ステップＳ７０１）。
【０１６８】
そして、確率算出部２１４ｃは、読み込んだイベントログ２１３ａからイベントの共起確率Ｐ（ｃ１，ｃ２，ｔｓ，ｔｅ）を算出し（ステップＳ７０２）、ペアルール算出部２１４ｃは、確率算出部２１４ｃにより算出された共起確率Ｐ（ｃ１，ｃ２，ｔｓ，ｔｅ）と、関係定義データ２１３ｂとから、ペアルールを生成する処理をおこなう（ステップＳ７０３）。
【０１６９】
その後、複合ルール生成部２１４ｅは、結合可能なペアルールを結合してイベントパターンルールを生成する（ステップＳ７０４）。そして、複合ルール生成部２１４ｅは、生成したイベントパターンルールの総数を算出し（ステップＳ７０５）、その総数が所定値Ｎｒ以下であるか否かを調べる（ステップＳ７０６）。
【０１７０】

総数が所定値Ｎｒ以下である場合には（ステップＳ７０６，Ｙｅｓ）、確率算出部２１４ｃは、最小確信度ｍｉｎｃｏｎｆが所定量小さくなるよう再設定する（ステップＳ７０７）。そして、再設定された最小確信度ｍｉｎｃｏｎｆに基づいて、ステップＳ７０３以降の処理を継続する。

【０１７１】

イベントパターンルールの総数が所定値Ｎｒより多い場合には（ステップＳ７０６，Ｎｏ）、ルール簡略化部２１４ｆは、複合ルール生成部２１４ｅにより生成されたイベントパターンルールを簡略化する処理をおこなう（ステップＳ７０８）。

【０１７２】

そして、ルール管理部２１４ｇは、イベントパターンルールを記憶部２１３に記憶し、また、表示部２１２に出力する処理をおこない（ステップＳ７０９）、最小確信度ｍｉｎｃｏｎｆの自動設定によるパターン検出処理を終了する。

【０１７３】

上述してきたように、本実施例４では、確率算出部２１４ｃが、関係の有無を判定するイベント間の生起確率に係る設定値である最小確信度ｍｉｎｃｏｎｆを、イベントパターンルールを検出した結果えられたイベントパターンルールの総数Ｎｒに基づいて設定することとしたので、適切な設定値ｍｉｎｃｏｎｆを自動的に設定することにより、イベント間における関係の有無を精度よく判定することができる。

【実施例５】

【０１７４】

ところで、上記実施例３および４では、時間制約条件におけるイベント間の生起時刻の近さを定義する閾値、および、共起確率条件における最小確信度を自動的に設定する場合について説明したが、このようなパラメータのうち、適切なイベントパターンルールを検出するために重要なパラメータはどれであり、どのパラメータを再設定すべきかを判定することは難しい。そこで、本実施例５では、適切なイベントパターンルールを検出するために効果が高いパラメータを自動的に選択し、その値を設定する場合について説明する。

【０１７５】

まず、検出されたイベントパターンルールを評価する評価関数について説明する。本実施例５では、イベントパターンルールを、評価関数

Ｅ＝（ｍｉｎｃｏｎｆ－０．７）×Ｎａ

により評価する。

【０１７６】

評価関数Ｅにおいて、ｍｉｎｃｏｎｆは、共起確率条件における最小確信度であり、Ｎａは、イベントパターンルールに対して簡略化処理を実行した結果得られたグラフのエッジの総本数である。ここでは、最小確信度ｍｉｎｃｏｎｆ、および、エッジの総本数Ｎａが大きいイベントパターンルールが高い評価となるように設定されている。

【０１７７】

図１３は、適切なイベントパターンルールを検出するのに有効なパラメータの設定処理の処理手順を示すフローチャートである。このパラメータの設定処理は、図２に示したパターン検出装置２１の関係定義データ管理部２１４ｂによりおこなわれる。また、評価関数の情報は、記憶部２１３に関係定義データ２１３ｂとして記憶されている。

【０１７８】

図１３に示すように、まず、関係定義データ管理部２１４ｂは、関係定義データ２１３ｂから評価関数の情報を読み出す（ステップＳ８０１）。そして、関係定義データ管理部２１４ｂは、時間制約条件Ｆｔのパラメータｔｓおよびｔｅの変化分に対する評価関数の値の変化分を求める（ステップＳ８０２）。評価関数の値は、図５に示したようなイベントパターンルールの検出処理を実行することにより算出される。

【０１７９】

続いて、関係定義データ管理部２１４ｂは、共起確率条件のパラメータである最小確信度ｍｉｎｃｏｎｆの変化分に対する評価関数の値の変化分を求める（ステップＳ８０３）

。そして、さらに、関係定義データ管理部２１４ｂは、イベント生起数のパラメータｍｉｎｓｕｐの変化分に対する評価関数の値の変化分を求める（ステップＳ８０４）。

【０１８０】

その後、関係定義データ管理部２１４ｂは、時間制約条件Ｆｔのパラメータｔｓおよびｔｅ、共起確率条件のパラメータである最小確信度ｍｉｎｃｏｎｆ、イベントの生起数のパラメータｍｉｎｓｕｐのうち、評価関数の値を増加させる効果が最も大きいパラメータの値を変更する処理をおこなう（ステップＳ８０５）。

【０１８１】

そして、関係定義データ管理部２１４ｂは、評価関数の値が増加したか否かを調べ（ステップＳ８０６）、増加した場合には（ステップＳ８０６，Ｙｅｓ）、ステップＳ８０２に移行して、それ以後の処理を継続する。評価関数の値が増加しなかった場合は（ステップＳ８０７，Ｎｏ）、このパラメータの設定処理を終了する。

【０１８２】

上述してきたように、本実施例５では、関係定義データ管理部２１４ｂが、イベントパターンルールの検出結果を評価する評価関数Ｅに基づいて、イベント間の生起時刻の時間差に係る閾値ｔｓおよびｔｅ、イベントの共起確率に係る最小確信度ｍｉｎｃｏｎｆ、または、イベントの生起数のパラメータｍｉｎｓｕｐを設定することとしたので、評価が高いイベントパターンルールを検出するのに適切なパラメータを自動的に設定することができる。

【０１８３】

ところで、上記実施例１～５で説明したパターン検出装置およびパターン検出方法は、あらかじめ用意されたプログラムをパーソナル・コンピュータやワークステーションなどのコンピュータシステムで実行することによって実現することができる。そこで、以下では、上記実施例１～５で説明したパターン検出装置（パターン検出方法）と同様の機能を有するパターン検出プログラムを実行するコンピュータシステムについて説明する。

【０１８４】

図１４は、本発明に係るコンピュータシステム１００の構成を示すシステム構成図であり、図１５は、図１４に示したコンピュータシステム１００における本体部１０１の構成を示すブロック図である。

【０１８５】

図１４に示すように、本発明に係るコンピュータシステム１００は、本体部１０１と、本体部１０１からの指示によって表示画面１０２ａに画像などの情報を表示するためのディスプレイ１０２と、このコンピュータシステム１００に種々の情報を入力するためのキーボード１０３と、ディスプレイ１０２の表示画面１０２ａ上の任意の位置を指定するためのマウス１０４とを備える。

【０１８６】

また、このコンピュータシステム１００における本体部１０１は、図１５に示すように、ＣＰＵ１２１と、ＲＡＭ１２２と、ＲＯＭ１２３と、ハードディスクドライブ（ＨＤＤ）１２４と、ＣＤ－ＲＯＭ１０９を受け入れるＣＤ－ＲＯＭドライブ１２５と、フレキシブルディスク（ＦＤ）１０８を受け入れるＦＤドライブ１２６と、ディスプレイ１０２、キーボード１０３並びにマウス１０４を接続するＩ／Ｏインターフェース１２７と、ローカルエリアネットワークまたはワイドエリアネットワーク（ＬＡＮ／ＷＡＮ）１０６に接続するＬＡＮインターフェース１２８とを備える。

【０１８７】

さらに、このコンピュータシステム１００には、インターネットなどの公衆回線１０７に接続するためのモデム１０５が接続されるとともに、ＬＡＮインターフェース１２８およびＬＡＮ／ＷＡＮ１０６を介して、他のコンピュータシステム（ＰＣ）１１１、サーバ１１２並びにプリンタ１１３などが接続される。

【０１８８】

そして、このコンピュータシステム１００は、所定の記録媒体に記録されたパターン検

出プログラムを読み出して実行することでパターン検出装置（パターン検出方法）を実現する。

【０１８９】

ここで、所定の記録媒体とは、フレキシブルディスク（ＦＤ）１０８、ＣＤ－ＲＯＭ１０９、ＭＯディスク、ＤＶＤディスク、光磁気ディスク、ＩＣカードなどの「可搬用の物理媒体」の他に、コンピュータシステム１００の内外に備えられるハードディスクドライブ（ＨＤＤ）１２４や、ＲＡＭ１２２、ＲＯＭ１２３などの「固定用の物理媒体」、さらに、モデム１０５を介して接続される公衆回線１０７や、他のコンピュータシステム１１１並びにサーバ１１２が接続されるＬＡＮ／ＷＡＮ１０６などのように、プログラムの送信に際して短期にプログラムを保持する「通信媒体」など、コンピュータシステム１００によって読み取り可能なパターン検出プログラムを記録する、あらゆる記録媒体を含むものである。

【０１９０】

すなわち、パターン検出プログラムは、上記した「可搬用の物理媒体」、「固定用の物理媒体」、「通信媒体」などの記録媒体に、コンピュータ読み取り可能に記録されるものであり、コンピュータシステム１００は、このような記録媒体からパターン検出プログラムを読み出して実行することでパターン検出装置およびパターン検出方法を実現する。

【０１９１】

なお、パターン検出プログラムは、コンピュータシステム１００によって実行されることに限定されるものではなく、他のコンピュータシステム１１１またはサーバ１１２がパターン検出プログラムを実行する場合や、これらが協働してパターン検出プログラムを実行するような場合にも、本発明を同様に適用することができる。

【０１９２】

さて、これまで本発明の実施例について説明したが、本発明は上述した実施例以外にも、特許請求の範囲に記載した技術的思想の範囲内において種々の異なる実施例にて実施されてもよいものである。

【０１９３】

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

【０１９４】

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ように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。

【０１９５】

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。

【０１９６】

（付記１）生起したイベントに係る情報を記憶したイベントデータからイベントの生起パターンを検出する処理をコンピュータに実行させるパターン検出プログラムであって、

イベント間において定義される複数種類の関係に係る情報に基づいて、前記イベントデータからイベントの生起パターンを検出する検出手順と、

前記検出手順により検出されたイベントの生起パターンを出力する出力手順と、

をコンピュータに実行させることを特徴とするパターン検出プログラム。

【０１９７】

（付記２）前記複数種類の関係に係る情報は、イベントの生起時刻およびイベントの生起確率に基づいて定義された情報であることを特徴とする付記１に記載のパターン検出プログラム。

【０１９８】

（付記３）前記検出手順は、関係の有無を判定するイベント間の生起時刻の範囲に係る設定値を、生起パターンの検出結果に基づいて設定することを特徴とする付記２に記載のパターン検出プログラム。

【０１９９】

（付記４）前記検出手順は、関係の有無を判定するイベント間の生起確率に係る設定値を、生起パターンの検出結果に基づいて設定することを特徴とする付記２または３に記載のパターン検出プログラム。

【０２００】

（付記５）前記検出手順は、前記イベントの生起パターンの検出結果を評価する評価関数に基づいて、関係の有無を判定するイベント間の生起時刻の範囲に係る設定値、または、関係の有無を判定するイベント間の生起確率に係る設定値を設定することを特徴とする付記２、３または４に記載のパターン検出プログラム。

【０２０１】

（付記６）前記複数種類の関係に係る情報は、２つのイベントが生起した生起時刻の差の大小に応じて異なる種類の関係を定義した情報を含んだことを特徴とする付記１～５のいずれか１つに記載のパターン検出プログラム。

【０２０２】

（付記７）前記検出手順は、２つのイベントから構成される生起パターンを結合することにより、３つ以上のイベントから構成される生起パターンを検出することを特徴とする付記１～６のいずれか１つに記載のパターン検出プログラム。

【０２０３】

（付記８）前記検出手順は、生起パターンの結合の可否を判定する結合条件に基づいて、生起パターンの結合を実行するか否かを判定することを特徴とする付記７に記載のパターン検出プログラム。

【０２０４】

（付記９）前記検出手順は、結合された生起パターンに含まれる部分が所定の基準を満足しているか否かを判定し、所定の基準を満足しない部分を生起パターンから削除することを特徴とする付記７または８に記載のパターン検出プログラム。

【０２０５】

（付記１０）前記検出手順は、生起パターンに含まれるイベント間の結合可能な関係に係る情報に基づいて、結合する生起パターンの組み合わせを選択することを特徴とする付記７、８または９に記載のパターン検出プログラム。

【０２０６】

（付記１１）前記出力手順は、生起パターンに含まれるイベント間の関係に係る情報に基づいて、前記検出手順により検出された生起パターンに含まれるイベント間の関係を統合し、イベント間の関係が統合された生起パターンを出力することを特徴とする付記１～１０のいずれか１つに記載のパターン検出プログラム。

【０２０７】

（付記１２）生起したイベントに係る情報を記憶したイベントデータからイベントの生起パターンを検出するパターン検出装置であって、

イベント間において定義される複数種類の関係に係る情報に基づいて、前記イベントデータからイベントの生起パターンを検出する検出手段と、

前記検出手段により検出されたイベントの生起パターンを出力する出力手段と、

を備えたことを特徴とするパターン検出装置。

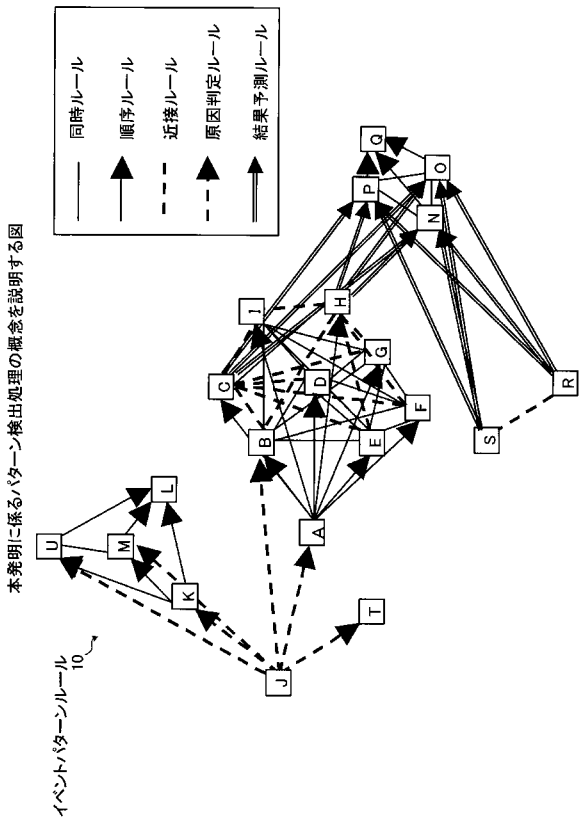
【０２０８】

（付記１３）生起したイベントに係る情報を記憶したイベントデータからイベントの生起

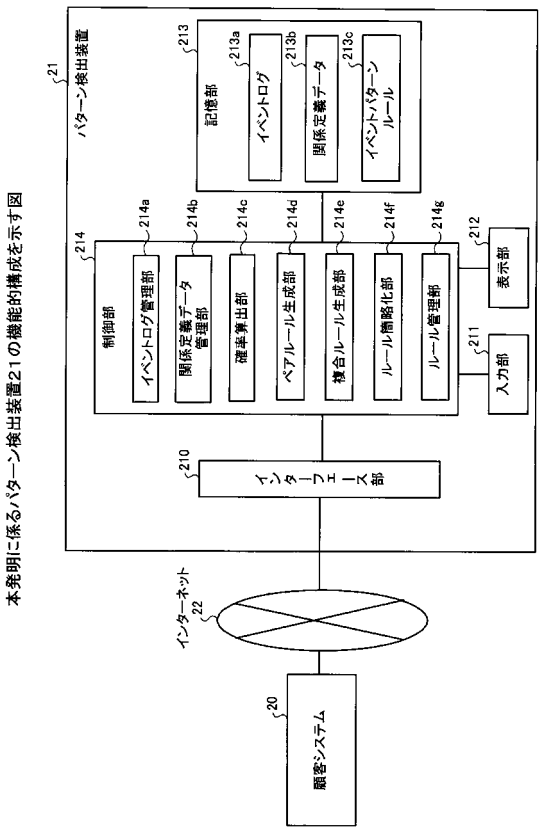
パターンを検出するパターン検出方法であって、
イベント間において定義される複数種類の関係に係る情報に基づいて、前記イベントデータからイベントの生起パターンを検出する検出工程と、
前記検出工程により検出されたイベントの生起パターンを出力する出力工程と、
を含んだことを特徴とするパターン検出方法。
【産業上の利用可能性】
【０２０９】
以上のように、本発明にかかるパターン検出プログラムは、生起したイベントの情報を記憶したイベントデータから、イベントの生起パターンについての詳細な情報を抽出することが必要なパターン検出システムに有用である。
【図面の簡単な説明】
【０２１０】
【図１】本発明に係るパターン検出処理の概念を説明する図である。
【図２】本発明に係るパターン検出装置２１の機能的構成を示す図である。
【図３】イベントパターンルールの簡略化処理を説明する図である。
【図４】イベントパターンルールの簡略化処理の効果を説明する図である。
【図５】実施例１に係るパターン検出処理の処理手順を示すフローチャートである。
【図６】イベントの発生回数Ｎ（ｃ１）およびＮ（ｃ１，ｃ２，ｔｓ，ｔｅ）の算出処理の処理手順を示すフローチャートである。
【図７】ペアルールの結合によりイベントパターンルールを生成する処理の処理手順を示すフローチャートである。
【図８】イベントパターンルールを簡略化する処理の処理手順を示すフローチャートである。
【図９】イベントパターンルールから規定違反のルール部分を削除する処理の処理手順を示すフローチャートである。
【図１０】所定の関係を有するルールと結合可能なルールの関係を記憶した結合表の一例を示す図である。
【図１１】イベントの発生回数Ｎ（ｃ１）およびＮ（ｃ１，ｃ２，－ｗ，０）の算出処理の処理手順を示すフローチャートである。
【図１２】最小確信度ｍｉｎｃｏｎｆの自動設定によるパターン検出処理の処理手順を示すフローチャートである。
【図１３】適切なイベントパターンルールを検出するのに有効なパラメータの設定処理の処理手順を示すフローチャートである。
【図１４】本発明に係るコンピュータシステム１００の構成を示すシステム構成図である。
【図１５】図１４に示したコンピュータシステム１００における本体部１０１の構成を示すブロック図である。
【図１６】イベントの生起パターンを分析するイベント分析システム２の一例を示す図である。
【図１７】生起したイベントを記録したイベントログの一例を示す図である。
【図１８】アプリオリアルゴリズムによるイベントの生起パターンの検出処理を説明する図である。
【符号の説明】
【０２１１】
１，２０　顧客システム
２　イベント分析システム
１０　イベントパターンルール
２１　パターン検出装置
２１０　インターフェース部
２１１　入力部

２１２　表示部
２１３　記憶部
２１３ａ　イベントログ
２１３ｂ　関係定義データ
２１３ｃ　イベントパターンルール
２１４　制御部
２１４ａ　イベントログ管理部
２１４ｂ　関係定義データ管理部
２１４ｃ　確率算出部
２１４ｄ　ペアルール生成部
２１４ｅ　複合ルール生成部
２１４ｆ　ルール簡略化部
２１４ｇ　ルール管理部
２２　インターネット
４０　簡略化処理前のイベントパターンルール
４１　簡略化処理後のイベントパターンルール

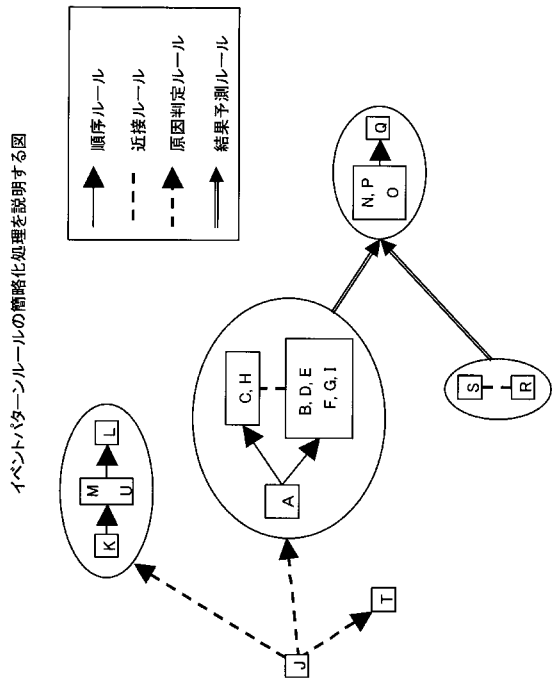
【図１】




【図２】

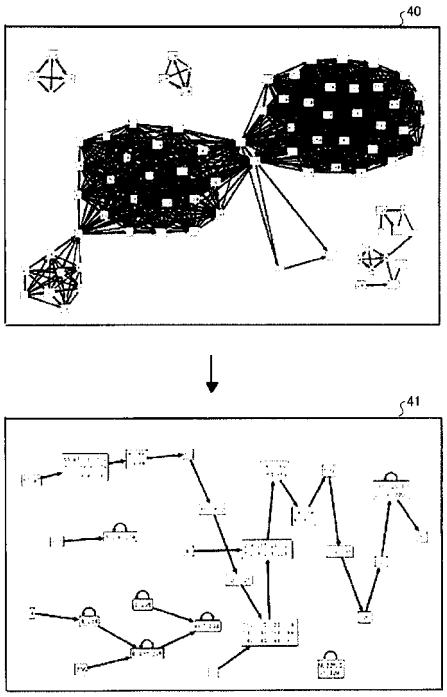


【図３】



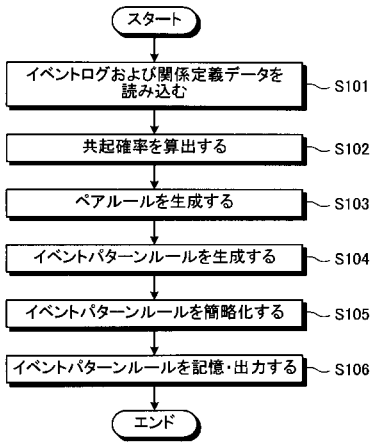

【図４】

イベントパターンルールの簡略化処理の効果を説明する図



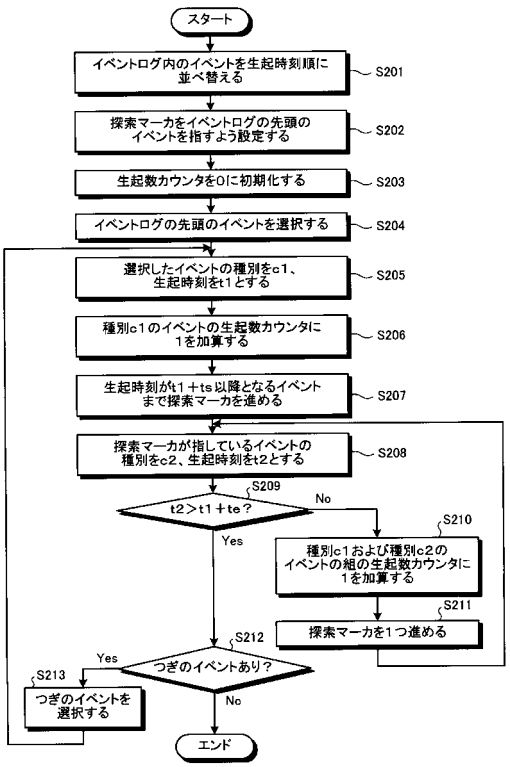

【図５】

実施例1に係るパターン検出処理の処理手順を示すフローチャート



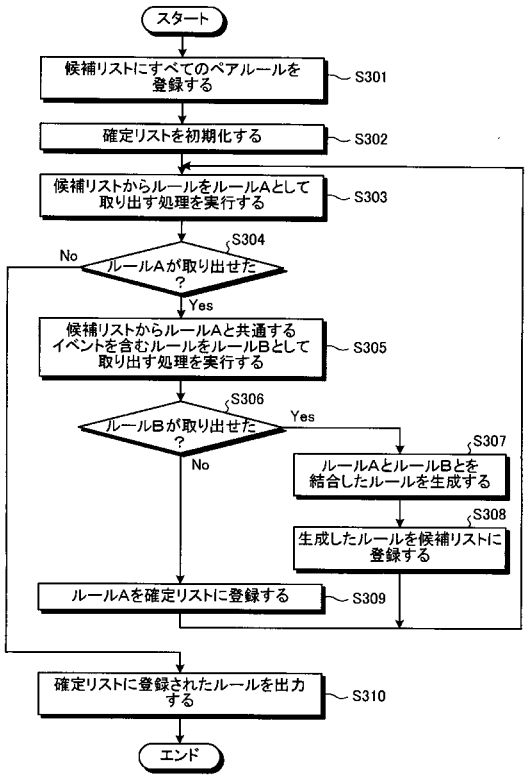

【図６】

イベントの発生回数N(c1)およびN(c1,c2,ts,te)の算出処理の処理手順を示すフローチャート



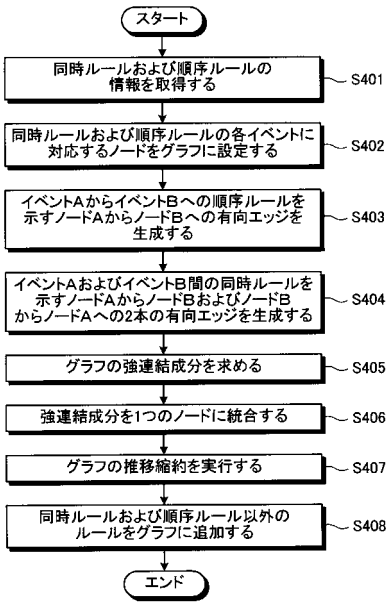
【図７】

ペアルールの結合によりイベントパターンルールを生成する処理の処理手順を示すフローチャート



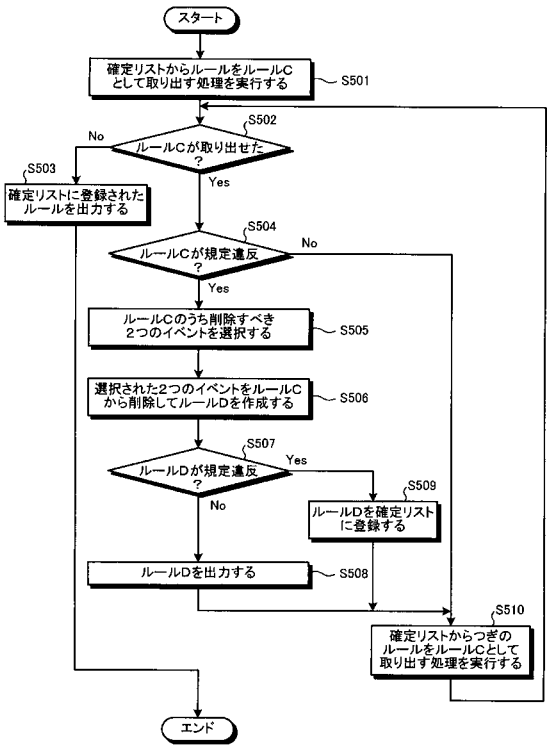

【図８】

イベントパターンルールを簡略化する処理の処理手順を示すフローチャート




【図９】

イベントパターンルールから規定違反のルール部分を削除する処理の処理手順を示すフローチャート



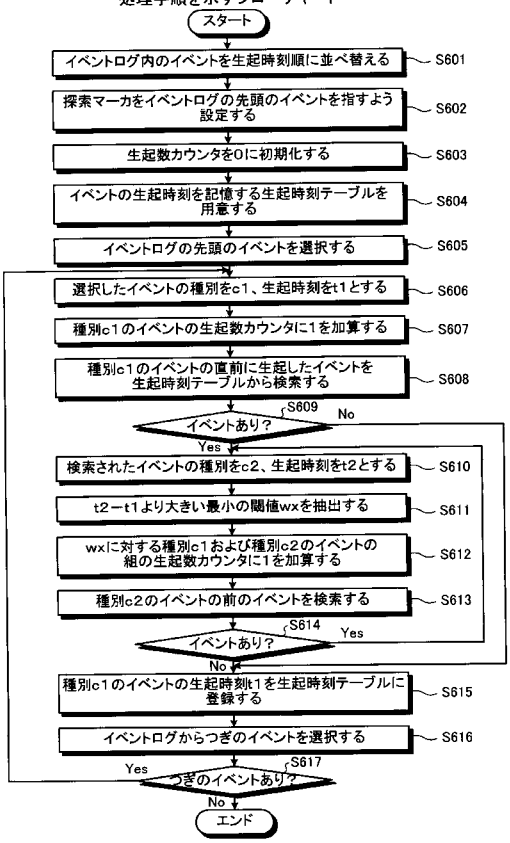

【図１０】

所定の関係を有するルールと結合可能なルールの関係を記憶した結合表の一例を示す図

| | 同時ルール | 順序ルール | 近接ルール | 結果予測ルール | 原因判定ルール |
|---|---|---|---|---|---|
| 同時ルール | ○ | ○ | ○ | ○ | ○ |
| 順序ルール | ○ | ○ | ○ | ○ | ○ |
| 近接ルール | ○ | ○ | ○ | ○ | ○ |
| 結果予測ルール | ○ | ○ | ○ | ○ | × |
| 原因判定ルール | ○ | ○ | ○ | × | ○ |

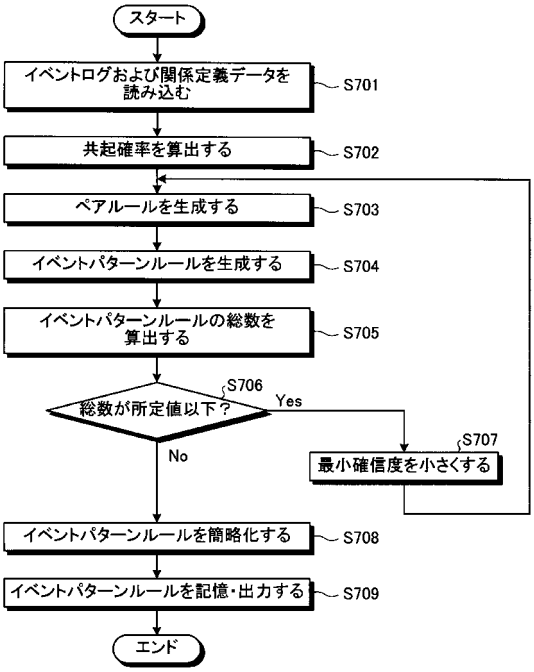
【図１１】

イベントの発生回数N(c1)およびN(c1, c2, −w, 0)の算出処理の処理手順を示すフローチャート



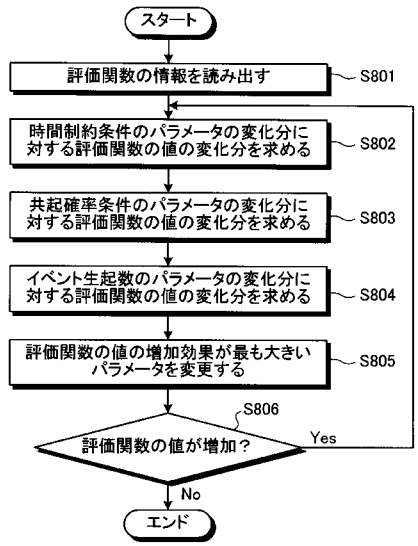

【図１２】

最小確信度minconfの自動設定によるパターン検出処理の処理手順を示すフローチャート



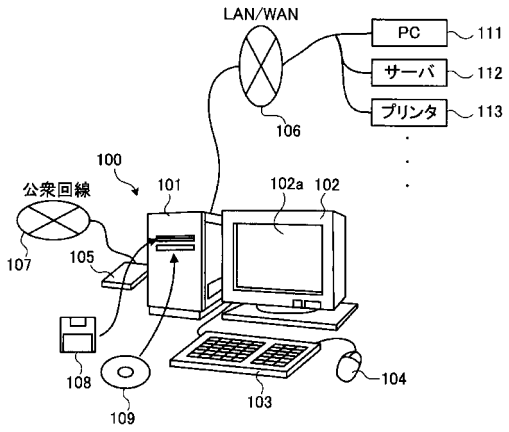

【図１３】

適切なイベントパターンルールを検出するのに有効なパラメータの設定処理の処理手順を示すフローチャート

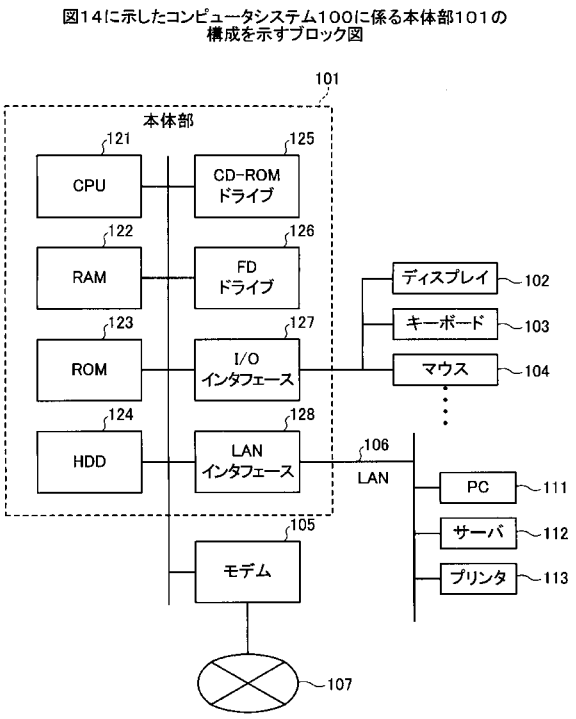



【図１４】

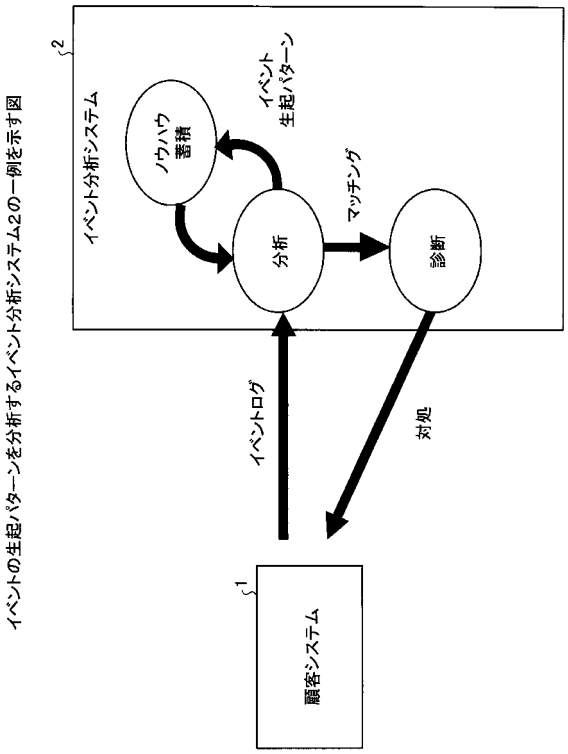
本発明に係るコンピュータシステム100の構成を示すシステム構成図



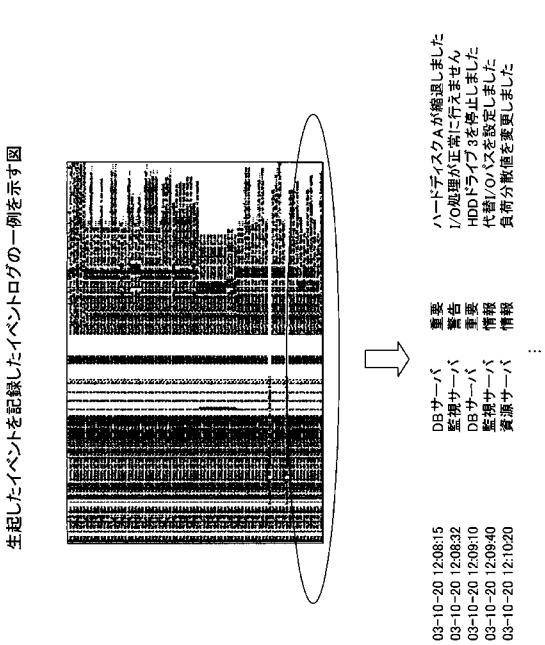
【図１５】




【図１６】




【図１７】




【図１８】

