

(11) 特許出願公開番号

特開2008-210213

(P2008-210213A)

(43) 公開日 平成20年9月11日(2008.9.11)

|                                |               |             |
|--------------------------------|---------------|-------------|
| (51) Int. Cl.                  | F I           | テーマコード (参考) |
| <b>G 0 6 F 11/28 (2006.01)</b> | G 0 6 F 11/28 | 3 1 0 A     |
| <b>G 0 6 F 11/34 (2006.01)</b> | G 0 6 F 11/34 | L           |

審査請求 有 請求項の数 6 O L (全 12 頁)

(21) 出願番号 特願2007-47035 (P2007-47035)  
(22) 出願日 平成19年2月27日 (2007. 2. 27)

(特許庁注：以下のものは登録商標)

## 1. Linux

(71) 出願人 000004237  
日本電気株式会社  
東京都港区芝五丁目7番1号

(74) 代理人 100088959  
弁理士 境 廣巳

(72) 発明者 鈴木 和明  
東京都港区芝五丁目7番1号 日本電気株  
式会社内

Fターム(参考) 5B042 GA10 HH30 MA08 MA10 MA13  
MC21 MC40 NN04 NN05

(54) 【発明の名称】 プロセス動作表示装置及びプロセス動作表示方法並びにプログラム

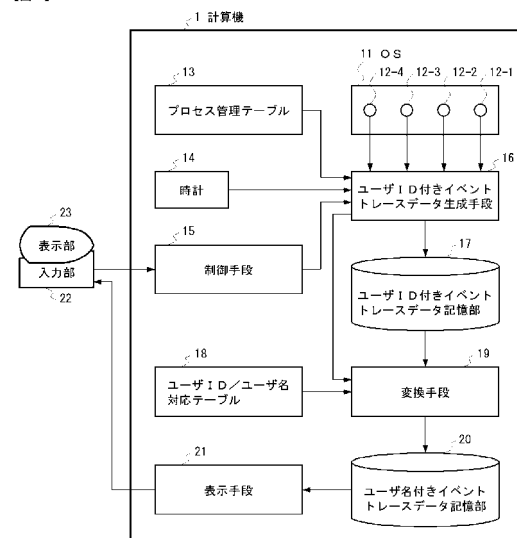
(57) 【要約】

【課題】誰がどのプロセスを実行したのかを容易に把握できるようにする。

【解決手段】グループ12-1,12-2が、プロセスの実行開始、実行終了に関するイベントを検出し、検出したイベントに関連するプロセスのプロセスIDを含んだイベントトレースデータを出力し、ユーザID付きイベントトレースデータ生成手段16が、イベントトレースデータにプロセスを実行したユーザのユーザIDを付加したユーザID付きイベントトレースデータを生成し、変換手段19が、ユーザID付きイベントトレースデータ中のユーザIDを対応するユーザ名で置き換えたユーザ名付きイベントトレースデータを生成する。表示手段21は、変換手段19で生成されたユーザID付きイベントトレースデータに基づいて、実行されたプロセスのプロセスIDと、プロセスを実行したユーザのユーザ名とを一体不可分な組として表示部23に表示する。

【選択図】 図1

【圖 1】



## 【特許請求の範囲】

## 【請求項 1】

プロセスの実行開始、実行終了に関するイベントを検出し、該検出したイベントに関連するプロセスのプロセスIDを含んだイベントトレースデータを出力するイベントトレースデータ出力手段と、

プロセスのプロセスIDと、該プロセスIDのプロセスを実行したユーザのユーザIDとが対応付けて登録されるプロセス管理テーブルと、

前記イベントトレースデータ出力手段から出力されたイベントトレースデータと、前記プロセス管理テーブルに登録されているユーザIDの内の、前記イベントトレースデータに含まれているプロセスIDに対応するユーザIDとの対からなるユーザID付きイベントトレースデータを生成するユーザID付きイベントトレースデータ生成手段と、

該ユーザID付きイベントトレースデータ生成手段で生成されたユーザID付きイベントトレースデータに基づいて、実行されたプロセスのプロセスIDと該プロセスを実行したユーザのユーザIDとを一体不可分な組として表示装置に表示する表示手段とを備えたことを特徴とするプロセス動作表示装置。

## 【請求項 2】

請求項 1 記載のプロセス動作表示装置において、

ユーザIDと、該ユーザIDによって特定されるユーザのユーザ名とが対応付けて登録された対応テーブルと、

該対応テーブルを参照して、前記ユーザID付きイベントトレースデータ生成手段で生成されたユーザID付きイベントトレースデータを、ユーザIDの代わりにユーザ名を含んだユーザ名付きイベントトレースデータに変換する変換手段とを備え、且つ、

前記表示手段が、前記ユーザID付きイベントトレースデータの代わりに、前記変換手段で生成されたユーザ名付きイベントトレースデータに基づいて、実行されたプロセスのプロセスIDと、該プロセスを実行したユーザのユーザ名とを一体不可分な組として前記表示装置に表示することを特徴とするプロセス動作表示装置。

## 【請求項 3】

プロセスのプロセスIDと、該プロセスIDのプロセスを実行したユーザのユーザIDとが対応付けて登録されるプロセス管理テーブルを備えたコンピュータによるプロセス動作表示方法であって、

前記コンピュータが、プロセスの実行開始、実行終了に関するイベントを検出し、該検出したイベントに関連するプロセスのプロセスIDを含んだイベントトレースデータを出力するイベントトレースデータ出力ステップと、

前記コンピュータが、前記イベントトレースデータ出力ステップで出力されたイベントトレースデータと、前記プロセス管理テーブルに登録されているユーザIDの内の、前記イベントトレースデータに含まれているプロセスIDに対応するユーザIDとの対からなるユーザID付きイベントトレースデータを生成するユーザID付きイベントトレースデータ生成ステップと、

前記コンピュータが、前記ユーザID付きイベントトレースデータ生成ステップで生成されたユーザID付きイベントトレースデータに基づいて、実行されたプロセスのプロセスIDと該プロセスを実行したユーザのユーザIDとを一体不可分な組として表示装置に表示する表示ステップとを含むことを特徴とするプロセス動作表示方法。

## 【請求項 4】

請求項 3 記載のプロセス動作表示方法において、

前記コンピュータが、ユーザIDと、該ユーザIDによって特定されるユーザのユーザ名とが対応付けて登録された対応テーブルを備え、且つ、

前記コンピュータが、該対応テーブルを参照して、前記ユーザID付きイベントトレースデータ生成ステップで生成されたユーザID付きイベントトレースデータを、ユーザIDの代わりにユーザ名を含んだユーザ名付きイベントトレースデータに変換する変換ステップを含み、

10

20

30

40

50

前記表示ステップでは、前記ユーザID付きイベントトレースデータの代わりに、前記変換ステップで生成されたユーザ名付きイベントトレースデータに基づいて、前記実行されたプロセスのプロセスIDと、該プロセスを実行したユーザのユーザ名とを一体不可分な組として前記表示装置に表示することを特徴とするプロセス動作表示方法。

【請求項 5】

プロセスのプロセスIDと、該プロセスIDのプロセスを実行したユーザのユーザIDとが対応付けて登録されるプロセス管理テーブルを備えたコンピュータを、

プロセスの実行開始、実行終了に関するイベントを検出し、該検出したイベントに関連するプロセスのプロセスIDを含んだイベントトレースデータを出力するイベントトレースデータ出力手段、

前記イベントトレースデータ出力手段から出力されたイベントトレースデータと、前記プロセス管理テーブルに登録されているユーザIDの内の、前記イベントトレースデータに含まれているプロセスIDに対応するユーザIDとの対からなるユーザID付きイベントトレースデータを生成するユーザID付きイベントトレースデータ生成手段、

該ユーザID付きイベントトレースデータ生成手段で生成されたユーザID付きイベントトレースデータに基づいて、実行されたプロセスのプロセスIDと該プロセスを実行したユーザのユーザIDとを一体不可分な組として表示装置に表示する表示手段とをして機能させるためのプログラム。

【請求項 6】

請求項 5 記載のプログラムにおいて、

前記コンピュータが、ユーザIDと、該ユーザIDによって特定されるユーザのユーザ名とが対応付けて登録された対応テーブルを備え、且つ、

前記コンピュータを、前記対応テーブルを参照して、前記ユーザID付きイベントトレースデータ生成手段で生成されたユーザID付きイベントトレースデータを、ユーザIDの代わりにユーザ名を含んだユーザ名付きイベントトレースデータに変換する変換手段として機能させ、

前記表示手段が、前記ユーザID付きイベントトレースデータの代わりに前記変換手段で生成されたユーザ名付きイベントトレースデータに基づいて、前記計算機上で実行されたプロセスのプロセスIDと、該プロセスを実行したユーザのユーザ名とを一体不可分な組として前記表示装置に表示することを特徴とするプログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、計算機上で実行されたプロセスの動作状況を表示するプロセス動作表示技術に関し、特に、プロセスを実行したユーザを把握することができるプロセス動作表示技術に関する。

【背景技術】

【0002】

従来から計算機上で実行されたプロセスの動作状況を表示するプロセス動作表示装置としては種々のものが知られている（例えば、特許文献 1、2 参照）。

【0003】

特許文献 1、2 に記載されているプロセス動作表示装置では、次のようにして計算機上で実行されたプロセスの動作状況を表示するようにしている。計算機のオペレーティングシステムの所定箇所にプロセス切り替えイベント検出用のプローブを埋め込んでおく（プロセスのResumを検出するプローブと、プロセスのSaveを検出するプローブとを埋め込んでおく）。各プローブは、その実行時に、イベント種別（Save或いはResum）と、Save或いはResumされたプロセスのプロセスIDとを含んだイベントトレースデータを出力する。このイベントトレースデータは、記憶装置に発生順に記録され、表示手段が、記憶装置の記憶内容に基づいて、実行された各プロセスを実行順に表示する。なお、特許文献 1、2 においては、オペレーティングシステムの所定箇所にプロセス間通信イベント検出用のブ

10

20

30

40

50

ローブも埋め込んでおき、プロセス間通信も表示できるようにしている。

【0004】

【特許文献1】特開2003-157185号公報

【特許文献2】特開2004-5198号公報

【発明の開示】

【発明が解決しようとする課題】

【0005】

特許文献1、2によれば計算機上で実行されたプロセスを時系列に並べて表示したり、各プロセス間で行われたプロセス間通信を表示することができるので、プロセスの動作状況が容易に理解可能となる。しかし、特許文献1、2に記載されているプロセス動作表示装置は、計算機の性能分析を目的としているため、プロセスを実行したユーザに関する情報は全く表示されない。このため、特許文献1に記載されている従来の技術によっては、プロセスを誰が実行したのかを把握することができない。また、Linux Trace Tool、Linux Kernel State Tracerといった特許文献1、2と同様の計算機の動作表示装置においても、プロセスを実行したユーザに関する情報は全く表示されない。

【0006】

〔発明の目的〕

そこで、本発明の目的は、誰がどのプロセスを実行したのかを容易に把握できるようにすることにある。

【課題を解決するための手段】

【0007】

本発明にかかる第1のプロセス動作表示装置は、

プロセスの実行開始、実行終了に関するイベントを検出し、該検出したイベントに関連するプロセスのプロセスIDを含んだイベントトレースデータを出力するイベントトレースデータ出力手段と、

プロセスのプロセスIDと、該プロセスIDのプロセスを実行したユーザのユーザIDとが対応付けて登録されるプロセス管理テーブルと、

前記イベントトレースデータ出力手段から出力されたイベントトレースデータと、前記プロセス管理テーブルに登録されているユーザIDの内の、前記イベントトレースデータに含まれているプロセスIDに対応するユーザIDとの対からなるユーザID付きイベントトレースデータを生成するユーザID付きイベントトレースデータ生成手段と、

該ユーザID付きイベントトレースデータ生成手段で生成されたユーザID付きイベントトレースデータに基づいて、実行されたプロセスのプロセスIDと該プロセスを実行したユーザのユーザIDとを一体不可分な組として表示装置に表示する表示手段とを備えたことを特徴とする。

【0008】

本発明にかかる第2のプロセス動作表示装置は、第1のプロセス動作表示装置において、

ユーザIDと、該ユーザIDによって特定されるユーザのユーザ名とが対応付けて登録された対応テーブルと、

該対応テーブルを参照して、前記ユーザID付きイベントトレースデータ生成手段で生成されたユーザID付きイベントトレースデータを、ユーザIDの代わりにユーザ名を含んだユーザ名付きイベントトレースデータに変換する変換手段とを備え、且つ、

前記表示手段が、前記ユーザID付きイベントトレースデータの代わりに、前記変換手段で生成されたユーザ名付きイベントトレースデータに基づいて、実行されたプロセスのプロセスIDと、該プロセスを実行したユーザのユーザ名とを一体不可分な組として前記表示装置に表示することを特徴とする。

【0009】

本発明にかかる第1のプロセス動作表示方法は、

プロセスのプロセスIDと、該プロセスIDのプロセスを実行したユーザのユーザIDとが対

応付けて登録されるプロセス管理テーブルを備えたコンピュータによるプロセス動作表示方法であって、

前記コンピュータが、プロセスの実行開始、実行終了に関するイベントを検出し、該検出したイベントに関連するプロセスのプロセスIDを含んだイベントトレースデータを出力するイベントトレースデータ出力ステップと、

前記コンピュータが、前記イベントトレースデータ出力ステップで出力されたイベントトレースデータと、前記プロセス管理テーブルに登録されているユーザIDの内の、前記イベントトレースデータに含まれているプロセスIDに対応するユーザIDとの対からなるユーザID付きイベントトレースデータを生成するユーザID付きイベントトレースデータ生成ステップと、

前記コンピュータが、前記ユーザID付きイベントトレースデータ生成ステップで生成されたユーザID付きイベントトレースデータに基づいて、実行されたプロセスのプロセスIDと該プロセスを実行したユーザのユーザIDとを一体不可分な組として表示装置に表示する表示ステップとを含むことを特徴とする。

#### 【0010】

本発明にかかる第2のプロセス動作表示方法は、第1のプロセス動作表示方法において、

前記コンピュータが、ユーザIDと、該ユーザIDによって特定されるユーザのユーザ名とが対応付けて登録された対応テーブルを備え、且つ、

前記コンピュータが、該対応テーブルを参照して、前記ユーザID付きイベントトレースデータ生成ステップで生成されたユーザID付きイベントトレースデータを、ユーザIDの代わりにユーザ名を含んだユーザ名付きイベントトレースデータに変換する変換ステップを含み、

前記表示ステップでは、前記ユーザID付きイベントトレースデータの代わりに、前記変換ステップで生成されたユーザ名付きイベントトレースデータに基づいて、前記実行されたプロセスのプロセスIDと、該プロセスを実行したユーザのユーザ名とを一体不可分な組として前記表示装置に表示することを特徴とする。

#### 【0011】

本発明にかかる第1のプログラムは、

プロセスのプロセスIDと、該プロセスIDのプロセスを実行したユーザのユーザIDとが対応付けて登録されるプロセス管理テーブルを備えたコンピュータを、

プロセスの実行開始、実行終了に関するイベントを検出し、該検出したイベントに関連するプロセスのプロセスIDを含んだイベントトレースデータを出力するイベントトレースデータ出力手段、

前記イベントトレースデータ出力手段から出力されたイベントトレースデータと、前記プロセス管理テーブルに登録されているユーザIDの内の、前記イベントトレースデータに含まれているプロセスIDに対応するユーザIDとの対からなるユーザID付きイベントトレースデータを生成するユーザID付きイベントトレースデータ生成手段、

該ユーザID付きイベントトレースデータ生成手段で生成されたユーザID付きイベントトレースデータに基づいて、実行されたプロセスのプロセスIDと該プロセスを実行したユーザのユーザIDとを一体不可分な組として表示装置に表示する表示手段とをして機能させる。

#### 【0012】

本発明にかかる第2のプログラムは、第1のプログラムにおいて、

前記コンピュータが、ユーザIDと、該ユーザIDによって特定されるユーザのユーザ名とが対応付けて登録された対応テーブルを備え、且つ、

前記コンピュータを、前記対応テーブルを参照して、前記ユーザID付きイベントトレースデータ生成手段で生成されたユーザID付きイベントトレースデータを、ユーザIDの代わりにユーザ名を含んだユーザ名付きイベントトレースデータに変換する変換手段として機能させ、

10

20

30

40

50

前記表示手段が、前記ユーザID付きイベントトレースデータの代わりに前記変換手段で生成されたユーザ名付きイベントトレースデータに基づいて、前記計算機上で実行されたプロセスのプロセスIDと、該プロセスを実行したユーザのユーザ名とを一体不可分な組として前記表示装置に表示することを特徴とする。

#### 【0013】

〔作用〕

イベントトレースデータ出力手段が、プロセスの実行開始、実行終了に関するイベントを検出し、該検出したイベントに関連するプロセスのプロセスIDを含んだイベントトレースデータを出力する。ユーザID付きイベントトレースデータ生成手段では、イベントトレースデータ出力手段から出力されたイベントトレースデータと、プロセス管理テーブルに登録されているユーザIDの内の、上記イベントトレースデータに含まれているプロセスIDに対応するユーザIDとの対からなるユーザID付きイベントトレースデータを生成する。表示手段は、ユーザID付きイベントトレースデータ生成手段で生成されたユーザID付きイベントトレースデータに基づいて、実行されたプロセスのプロセスIDと、プロセスを実行したユーザのユーザIDとを一体不可分な組として表示装置に表示する。

#### 【発明の効果】

#### 【0014】

本発明によれば、誰がどのプロセスを実行したのかを把握することが可能になる。その理由は、イベントトレースデータ出力手段から出力されたイベントトレースデータと、プロセス管理テーブルに登録されているユーザIDの内の、イベントトレースデータに含まれているプロセスIDに対応するユーザIDとの対からなるユーザID付きイベントトレースデータを生成するユーザID付きイベントトレースデータ生成手段と、ユーザID付きイベントトレースデータ生成手段で生成されたユーザID付きイベントトレースデータに基づいて、実行されたプロセスのプロセスIDと、プロセスを実行したユーザのユーザIDとを一体不可分な組として表示装置に表示する表示手段とを備えているからである。

#### 【発明を実施するための最良の形態】

#### 【0015】

次に、本発明を実施するための最良の形態について図面を参照して詳細に説明する。

#### 【0016】

〔実施の形態の構成の説明〕

図1を参照すると、本実施の形態は、計算機1上のオペレーティングシステム(OS)11に埋め込まれたプローブ12-1～12-4と、プロセス管理テーブル13と、時計14と、制御手段15と、ユーザID付きイベントトレースデータ生成手段16と、ユーザID付きイベントトレースデータ記憶部17と、ユーザID/ユーザ名対応テーブル18と、変換手段19と、ユーザ名付きイベントトレースデータ記憶部20と、表示手段21と、キーボード等の入力部22と、LCD等の表示部23とから構成されている。

#### 【0017】

プローブ12-1、12-2は、プロセス切り替えイベント検出用のプローブである。プローブ12-1は、その実行時に、イベント種別「プロセスのResum」と「ResumしたプロセスのプロセスID」とを含んだイベントトレースデータを出力する。プローブ12-2は、その実行時に、イベント種別「プロセスのSave」と「SaveしたプロセスのプロセスID」とを含んだイベントトレースデータを出力する。

#### 【0018】

プローブ12-3、12-4は、プロセス間通信イベント検出用のプローブである。プローブ12-3は、その実行時にイベント種別「Send（プロセス間通信の送信）」と「通信路番号」とを含むイベントトレースデータを出力する。プローブ12-4は、その実行時にイベント種別「Receive（プロセス間通信の受信）」と「通信路番号」とを含んだイベントトレースデータを出力する。

#### 【0019】

なお、各プローブ12-1～12-4が出力するイベントトレースデータの形式は、上

記した例に限られるものではなく、プロセスの動作を特徴付けることができるものであれば良い。また、プローブの種類も上記した例に限られるものではなく、アプリケーションプログラムに埋め込まれたプローブなどを使用しても良い。

#### 【0020】

プロセス管理テーブル13には、プロセスIDと、そのプロセスIDのプロセスを実行したユーザのユーザIDとが対応付けて登録される。図2にプロセス管理テーブル13の内容例を示す。同図の例は、プロセスID「sshd」のプロセスをユーザID「1234」のユーザが実行し、プロセスID「bash」のプロセスをユーザID「9876」のユーザが実行していることを示している。

#### 【0021】

時計14は、現在時刻を表示する。

#### 【0022】

制御手段15は、入力部22を介してユーザからイベントトレースデータの記録開始が指示されることによりユーザID付きイベントトレースデータ生成手段16に対して起動指示を入力し、記録終了が指示されることによりユーザID付きイベントトレースデータ生成手段16に対して終了指示を出力する。

#### 【0023】

ユーザID付きイベントトレースデータ生成手段16は、次のような機能を有する。

#### 【0024】

・プロセスIDを含むイベントトレースデータが入力された場合、時計14から現在時刻を入力すると共に、プロセス管理テーブル13から上記イベントトレースデータに含まれているプロセスIDに対応するユーザIDを検索し、上記イベントトレースデータと、上記現在時刻と、上記ユーザIDとからなるユーザID付きイベントトレースデータを生成してユーザID付きイベントトレースデータ記憶部17に格納する。図3にユーザID付きイベントトレースデータの一例を示す。同図の例は、プロセスID「sshd」のプロセスがユーザID「1234」のユーザによって「0時0分0秒」に「Resum」されたことを示している。

#### 【0025】

・プロセスIDを含まないイベントトレースデータが入力された場合、時計14から現在時刻を入力し、上記イベントトレースデータと上記現在時刻とを対応付けてユーザID付きイベントトレースデータ記憶部17に格納する。

#### 【0026】

・制御手段15から終了指示が入力されたとき、変換手段19を起動する。

#### 【0027】

ユーザID／ユーザ名対応テーブル18には、ユーザIDと、そのユーザIDによって特定されるユーザのユーザ名とが対応付けて登録されている。即ち、ユーザID／ユーザ名対応テーブル18は、マシンリーダブルな表現形式をとるユーザIDと、ヒューマンリーダブルな表現形式をとるユーザ名とを対応付けるためのテーブルである。図4はユーザID／ユーザ名対応テーブル18の内容例を示した図である。同図の例は、ユーザID「1234」によって特定されるユーザのユーザ名が「foo」、ユーザID「9876」によって特定されるユーザのユーザ名が「bar」であることを示している。

#### 【0028】

変換手段19は、ユーザID付きイベントトレースデータ記憶部17に格納されているデータを順次入力し、入力したデータがユーザID付きイベントトレースデータであった場合には、ユーザID／ユーザ名対応テーブル18を参照して、ユーザID付きイベントトレースデータ中のユーザIDに対応するユーザ名で置き換え、置き換え後のデータ（ユーザ名付きイベントトレースデータ）をユーザ名付きイベントトレースデータ記憶部20に格納する。また、読み込んだデータが、ユーザID付きイベントトレースデータでなかった場合は、そのデータをそのままユーザ名付きイベントトレースデータ記憶部20に格納する。

#### 【0029】

表示手段21は、ユーザ名付きイベントトレースデータ記憶部20の内容に基づいて、

10

20

30

40

50

表示部 2 3 上に、プロセス名とそのプロセスを実行したユーザのユーザ名とを一体不可分な組として表示すると共に、プロセスの動作状況を表示する。図 5 に表示手段 2 1 による表示例を示す。この例は、ユーザ名「foo」のユーザによって実行されたプロセスID「sshd」と、ユーザ名「bar」のユーザによって実行されたプロセスID「bash」のプロセスとがプロセス間通信を行っていることを示している。また、この例では、プロセスをResum、Saveした時刻も表示している。

#### 【0030】

なお、制御手段 1 5、ユーザID付きイベントトレースデータ生成手段 1 6、変換手段 1 9、表示手段 2 1 は C P U (コンピュータ) によって実現可能であり、C P U によって実現する場合は、例えば、次のようにする。C P U を制御手段 1 5、ユーザID付きイベント  
10  
トレースデータ生成手段 1 6、変換手段 1 9、表示手段 2 1 として機能させるためのプログラムを記録したディスク、半導体メモリ、その他の記録媒体を用意し、C P U に上記プログラムを読み取らせる。C P U は、読み取ったプログラムに従って自身の動作を制御することにより、自 C P U 上に制御手段 1 5、ユーザID付きイベントトレースデータ生成手段 1 6、変換手段 1 9、表示手段 2 1 を実現する。

#### 【0031】

〔実施の形態の動作の説明〕

次に、本実施の形態の動作について詳細に説明する。

#### 【0032】

オペレーティングシステム 1 1 に埋め込まれている各プローブ 1 2 - 1 ~ 1 2 - 4 は、その実行時にイベントトレースデータを出力する。本実施の形態では、プローブ 1 2 - 1 は、イベント種別「Resum」と「ResumしたプロセスのプロセスID」とを含んだイベント  
20  
トレースデータを出力し、プローブ 1 2 - 2 は、イベント種別「Save」と「SaveしたプロセスのプロセスID」とを含んだイベントトレースデータを出力する。また、プローブ 1 2 - 3 は、イベント種別「Send」と「通信路番号」とを含むイベントトレースデータを出力し、プローブ 1 2 - 4 は、イベント種別「Receive」と「通信路番号」とを含んだイベント  
トレースデータを出力する。

#### 【0033】

ユーザは、イベントトレースデータの記録を開始する場合、入力部 2 2 から制御手段 1 5 に対して記録開始指示を入力する。これにより、制御手段 1 5 は、ユーザID付きイベント  
30  
トレースデータ生成手段 1 6 に対して起動指示を出力する。

#### 【0034】

ユーザID付きイベントトレースデータ生成手段 1 6 は、起動指示が入力されると、図 6 のフローチャートに示す処理を開始する。起動後、プローブ 1 2 - 1 ~ 1 2 - 4 からイベント  
トレースデータが入力されると (ステップ S 6 1 が Y E S)、ユーザID付きイベント  
トレースデータ生成手段 1 6 は、上記イベントトレースデータにプロセスIDが含まれている  
か否かを判定する (ステップ S 6 2)。

#### 【0035】

そして、プロセスIDが含まれていると判定した場合 (ステップ S 6 2 が Y E S) は、プロセス管理テーブル 1 3 から上記プロセスIDに対応付けて登録されているユーザIDを検索  
40  
し (ステップ S 6 3)、更に、時計 1 4 から現在時刻を入力する (ステップ S 6 4)。その後、イベントトレースデータ、ステップ S 6 3 で検索したユーザID及びステップ S 6 4 で入力した現在時刻を含むユーザID付きイベントトレースデータを生成してユーザID付き  
イベントトレースデータ記憶部 1 7 に登録する (ステップ S 6 5)。例えば、イベント  
トレースデータに含まれているプロセスIDが「sshd」、現在時刻が「00:00:00」、プロセス  
管理テーブル 1 3 の内容が図 2 に示すものであるとすると、図 3 に示すようなユーザID  
付きイベントトレースデータが生成され、ユーザID付きイベントトレースデータ記憶部 1 7  
に登録されることになる。

#### 【0036】

これに対して、プロセスIDが含まれていないと判定した場合 (ステップ S 6 2 が N O)

10

20

30

40

50



は、時計 14 から現在時刻を入力し（ステップ S 66）、その後、イベントトレースデータとステップ S 66 で入力した現在時刻とを対応付けてユーザID付きイベントトレースデータ記憶部 17 に登録する（ステップ S 67）。

【0037】

ユーザID付きイベントトレースデータ生成手段 16 は、イベントトレースデータが入力される毎に、上記した処理を行う。

【0038】

ユーザは、イベントトレースデータの記録を終了する場合、入力部 22 から制御手段 15 に対して、イベントトレースデータの記録終了を指示を入力する。これにより、制御手段 15 は、ユーザID付きイベントトレースデータ生成手段 16 に対して終了指示を出力する。

10

【0039】

ユーザID付きイベントトレースデータ生成手段 16 は、制御手段 15 から終了指示が入力されると（ステップ S 68 が YES）、変換手段 19 を起動した後（ステップ S 69）、その処理を終了する。

【0040】

変換手段 19 は、起動されると、図 7 のフローチャートに示すように、ユーザID付きイベントトレースデータ記憶部 17 に登録されているデータの 1 つを入力し（ステップ S 71）、そのデータにユーザIDが含まれているか否かを判定する（ステップ S 73）。即ち、入力したデータがユーザID付きイベントトレースデータであるか否かを判定する。

20

【0041】

そして、ユーザIDが含まれていると判定した場合（ステップ S 73 が YES）は、ユーザID／ユーザ名対応テーブル 18 から上記ユーザIDに対応付けて登録されているユーザ名を検索し（ステップ S 74）、更に、入力したイベントトレースデータ中のユーザIDをステップ S 74 で検索したユーザ名に変換し（ステップ S 75）、変換後のデータ（ユーザ名付きイベントトレースデータ）を、ユーザ名付きイベントトレースデータ記憶部 20 に登録する（ステップ S 76）。例えば、図 2 に示すユーザID付きイベントトレースデータを入力した場合には、図 8 に示すようなユーザ名付きイベントトレースデータが生成されることになる。

【0042】

これに対して、ユーザIDが含まれていないと判定した場合（ステップ S 73 が NO）は、ステップ S 71 で入力したデータをそのままユーザ名付きイベントトレースデータ記憶部 20 に登録する（ステップ S 76）。

30

【0043】

変換手段 19 は、上記した処理を未入力のデータがなくなるまで繰り返し行い、未入力のデータがなくなると（ステップ S 72 が YES）、表示手段 21 を起動し（ステップ S 77）、その後、処理を終了する。

【0044】

表示手段 21 は、起動されると、ユーザ名イベントトレースデータ記憶部 20 の内容に基づいて、表示部 23 に図 5 に示すような表示を行う。即ち、実行されたプロセスのプロセスIDと、そのプロセスを実行したユーザのユーザ名とを一体不可分な組として表示すると共に、プロセスの動作状況を表示する。

40

【0045】

なお、上述した説明では、表示手段 21 が、ユーザ名付きイベントトレースデータ記憶部 20 の内容に基づいて、表示部 23 上に、実行されたプロセスのプロセスIDと、そのプロセスを実行したユーザのユーザ名との一体不可分な組およびプロセスの動作状況を表示するようにしたが、表示手段 21 が、ユーザID付きイベントトレースデータ記憶部 17 の内容に基づいて、表示部 23 上に、実行されたプロセスのプロセスIDと、そのプロセスを実行したユーザのユーザIDとの一体不可分な組およびプロセスの動作状況を表示するようにしても良い。この場合には、変換手段 19 及びユーザ名付きイベントトレースデータ記

50

憶部 20 は、不要となる。

【0046】

〔実施の形態の効果〕

本実施の形態によれば、誰がどのプロセスを実行したのかを把握することが可能になる。その理由は、オペレーティングシステム 11 から出力されたイベントトレースデータと、プロセス管理テーブル 13 に登録されているユーザIDの内の、イベントトレースデータに含まれているプロセスIDに対応するユーザIDとの対からなるユーザID付きイベントトレースデータを生成するユーザID付きイベントトレースデータ生成手段 16 と、ユーザID／ユーザ名対応テーブル 18 を参照して、ユーザID付きイベントトレースデータ生成手段 16 で生成されたユーザID付きイベントトレースデータを、ユーザIDの代わりにユーザ名を含んだユーザ名付きイベントトレースデータに変換する変換手段 19 と、変換手段 19 で生成されたユーザ名付きイベントトレースデータに基づいて、前記計算機上で実行されたプロセスのプロセスIDと、該プロセスを実行したユーザのユーザ名とを一体不可分な組として表示部 23 に表示する表示手段 21 とを備えているからである。

10

【産業上の利用可能性】

【0047】

企業内の計算機において、誰がどのようなプロセスを実行したのかを管理したい場合に適用すると有効である。

【図面の簡単な説明】

【0048】

20

【図 1】本発明の実施の形態の構成例を示すブロック図である。

【図 2】プロセス管理テーブル 13 の内容例を示す図である。

【図 3】ユーザID付きイベントトレースデータの一例を示す図である。

【図 4】ユーザID／ユーザ名対応テーブル 18 の内容例を示す図である。

【図 5】表示手段 21 による表示の一例を示す図である。

【図 6】ユーザID付きイベントトレースデータ生成手段 16 の処理例を示すフローチャートである。

【図 7】変換手段 19 の処理例を示すフローチャートである。

【図 8】ユーザ名付きイベントトレースデータの一例を示す図である。

【符号の説明】

30

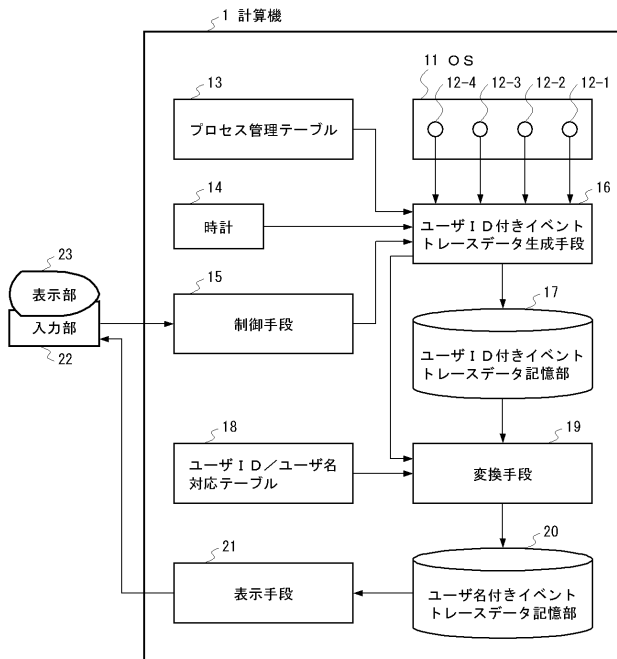
【0049】

- 1 … 計算機
- 11 … オペレーティングシステム (OS)
- 12 - 1 ~ 12 - 4 … プロープ
- 13 … プロセス管理テーブル
- 14 … 時計
- 15 … 制御手段
- 16 … ユーザID付きイベントトレースデータ生成手段
- 17 … ユーザID付きイベントトレースデータ記憶部
- 18 … ユーザID／ユーザ名対応テーブル
- 19 … 変換手段
- 20 … ユーザ名付きイベントトレースデータ記憶部
- 21 … 表示手段
- 22 … 入力部
- 23 … 表示部

40

【図 1】

【図 1】



【図 2】

【図 2】

13 プロセス管理テーブル

| プロセス ID | ユーザ ID |
|---------|--------|
| sshd    | 1234   |
| bash    | 9876   |
| ⋮       | ⋮      |

【図 3】

【図 3】

ユーザ ID 付きイベントトレースデータ

| ユーザ ID | 時刻       | イベントトレースデータ |       |
|--------|----------|-------------|-------|
| 1234   | 00:00:00 | sshd        | Resum |

【図 4】

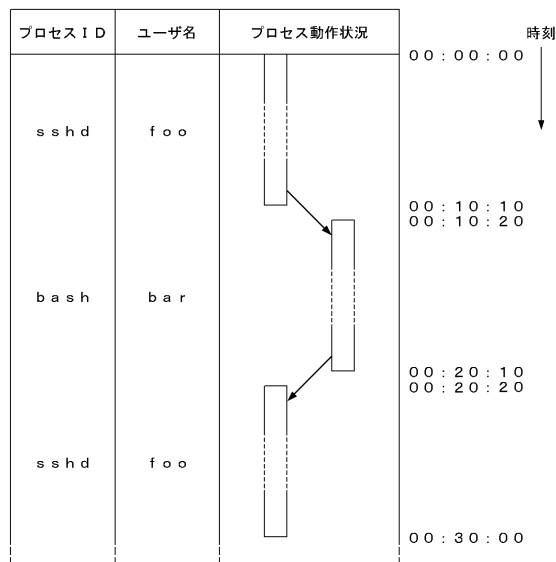
【図 4】

18 ユーザ ID/ユーザ名対応テーブル

| ユーザ ID | ユーザ名 |
|--------|------|
| 1234   | foo  |
| 9876   | bar  |
| ⋮      | ⋮    |

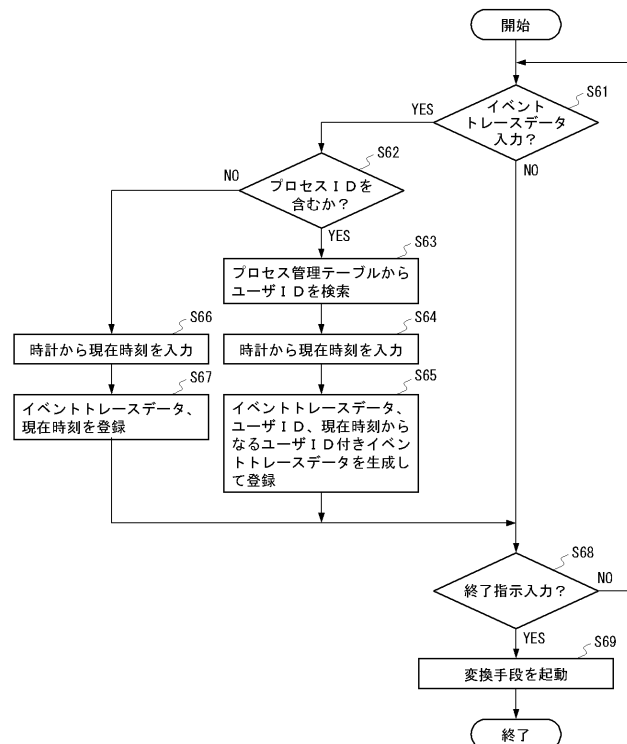
【図 5】

【図 5】



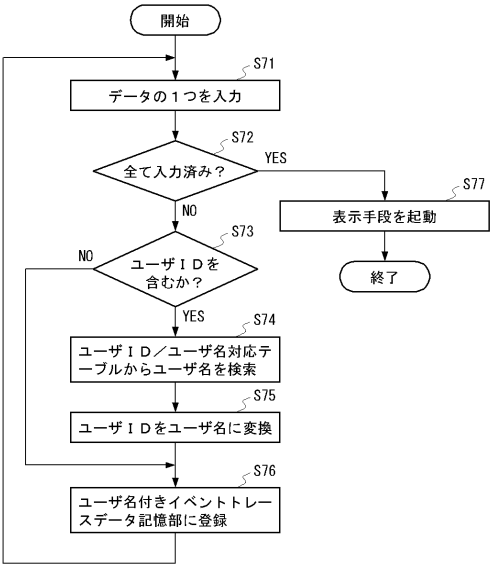
【図 6】

【図 6】



【図 7】

【図7】



【図 8】

【図8】

ユーザ名付きイベントトレースデータ

| ユーザ名  | 時刻       | イベントトレースデータ |           |
|-------|----------|-------------|-----------|
| f o o | 00:00:00 | s s h d     | R e s u m |