(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2006 年7 月6 日 (06.07.2006)

PCT

(10) 国際公開番号
WO 2006/070477 A1

(51) 国際特許分類[7]: G06F 12/00, 17/30

(21) 国際出願番号: PCT/JP2004/019649

(22) 国際出願日: 2004 年12 月28 日 (28.12.2004)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(71) 出願人 (米国を除く全ての指定国について): 富士通株式会社 (FUJITSU LIMITED) [JP/JP]; 〒2118588 神奈川県川崎市中原区上小田中４丁目１番１号 Kanagawa (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 烏谷 彰 (KARASUDANI, Akira) [JP/JP]; 〒2118588 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 Kanagawa (JP). 松田 高弘 (MATSUDA, Takahiro) [JP/JP]; 〒2118588 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 Kanagawa (JP). 森原 隆 (MORIHARA, Takashi) [JP/JP]; 〒2118588 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 Kanagawa (JP).

(74) 代理人: 大菅 義之 (OSUGA, Yoshiyuki); 〒1020084 東京都千代田区二番町８番地２０，二番町ビル３Ｆ Tokyo (JP).

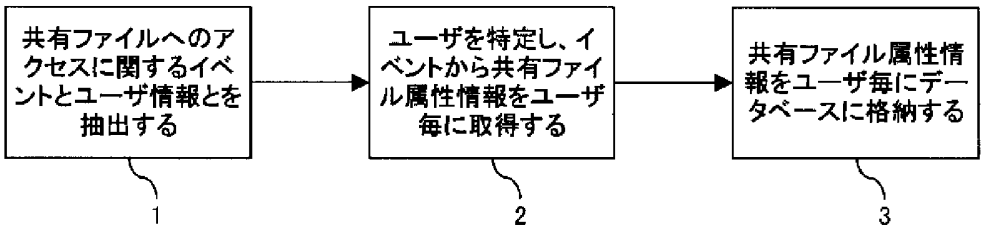
(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU,

[続葉有]

(54) Title: FILE ATTRIBUTE INFORMATION MANAGEMENT PROGRAM, MANAGEMENT METHOD, AND MANAGEMENT DEVICE

(54) 発明の名称: ファイル属性情報管理プログラム、管理方法、および管理装置



1 EXTRACT EVENT ON ACCESS TO SHARED FILE AND USER INFORMATION
2 SPECIFY USER, AND ACQUIRE SHARED FILE ATTRIBUTE INFORMATION FOR EACH USER FROM EVENT
3 STORE SHARED FILE ATTRIBUTE INFORMATION FOR EACH USER IN DATABASE

(57) Abstract: In a system provided with a shared file shared by a plurality of users, a program contemplates to facilitate a file retrieval according to stored contents corresponding to the past file accesses of the users and to take loads off the information managements of the users. The program causes a computer to execute procedures to monitor the accesses of users to the shared file and to extract an event on the access and information on the user having made the access, procedures to specify the user with the extracted result and to acquire the attribute information of the shared file for each user from the event, and a procedure to store the acquired attribute information for each user in a database.

(57) 要約: 複数のユーザによって共有される共有ファイルを備えるシステムにおいて、ユーザの過去のファイルアクセスに対応する記憶内容に合ったファイル検索を容易とし、ユーザの情報管理の負担を軽減させることを目的とする。本発明のプログラムは、ユーザによる共有ファイルへのアクセスを監視し、アクセスに関するイベントとアクセスを行ったユーザの情報とを抽出する手順と、該抽出結果を用いてユーザを特定し、イベントから共有ファイルの属性情報をユーザ毎に取得する手順と、取得された属性情報をユーザ毎にデータベースに格納する手順とを計算機に実行させる。

WO 2006/070477 A1

IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

明 細 書

ファイル属性情報管理プログラム、管理方法、および管理装置

技術分野

[0001] 本発明はファイルの管理方式に係り、さらに詳しくは複数のユーザで共有される共有ファイルを用いるファイルシステムにおいて、その共有ファイルの属性情報をユーザ毎に管理することによって、例えばユーザによるファイル検索を容易とし、ユーザによる情報管理の負担を軽減させることができるファイル属性情報管理プログラム、管理方法、および管理装置に関する。

背景技術

[0002] PCやPDAなどの情報機器やインターネットなどのネットワーク環境の普及が進み、ユーザは簡単に文書や画像などを作成、編集したり、様々な情報にアクセスしたりできるようになった。ネットワークを介したユーザ同士のファイルの共有も広く行われている。

[0003] しかしながら、扱える情報が増えた反面、ユーザがその情報を管理する負担も大きくなっている。現在では多くのユーザが自分のPCの中に大量の情報(ファイル)を保存しているが、既存の情報管理方法では、そのファイルの内容さえ充分に把握することが困難になっている。ユーザが情報処理に専念できるように情報管理の負担を軽減する仕組みが求められている。

[0004] 大量のファイルをユーザが管理するために以下のような技術が用いられている。その第1は階層ディレクトリを持つファイルシステムである。このシステムではファイルは階層構造をもったディレクトリとして分類、管理される。ディレクトリの構造やファイルの分類規則を全て把握している場合にはユーザは簡単にファイルを探すことができる。しかしながらディレクトリの数が増えてくると、ユーザがディレクトリの構造を把握しつづけるのは難しくなる。ユーザが情報を分類する基準も時間とともに変わる可能性もあり、分類規則を首尾一貫した状態に保つことも困難であるという問題点もある。

[0005] ファイル管理のための第2の技術は情報検索システムの利用である。このシステムでは、ファイルはその内容や属性情報を用いて検索される。ユーザが指定したキーワ

ードや、アクセス日時などの検索条件を満たすファイルが探索され、ユーザに提示される。ユーザが指定した検索条件に相当する情報がシステム内に保存されていれば、その条件を満たすファイルを提示することができる。

[0006] しかしながら一般的にファイルシステムやデータベースなどに保存されているファイルの属性情報は、最新のアクセス日時や、ファイルのサイズ、ファイルの種類など予め定められたものに限られることが多い。ユーザがファイルを探す時に思い浮かべる、ファイルを扱った時の状況やエピソード、例えばそのファイルと同時に参照した別のファイル名など、ユーザの記憶に残っている情報を検索条件に利用することは困難である。

[0007] またユーザは検索で得られたファイルの中からさらにユーザの要求に合うファイルを見つけ出す必要がある。ユーザの要求に合うファイルが見つからなかった場合には、見つかるまで何度も条件を変えて検索しなおさなければならないという問題点もあった。

[0008] このようにファイルや文書など、複数のユーザによって共有される資源の管理方法に関する従来技術として以下の文献がある。

特許文献1:特開平8−292910号公報 「資源管理装置および資源管理方法」

特許文献2:特開平9−62658号公報 「文書間リンク処理システム」

特許文献3:特開2001−350795(P2001−350795A)号 「文書管理システム」

特許文献4:国際公開WO2004／031956A1号 「関連情報管理方法、プログラム及び装置」

[0009] 特許文献1には、複数の計算機システムがネットワークで結ばれたネットワーク情報システムにおける資源管理方式として、個々のユーザのアクセス方法の嗜好や意図を反映した、ユーザ毎に局所的な資源アクセスのための名前空間を提供する、柔軟性の高い分散システムを実現することができる資源管理装置、および資源管理方法が開示されている。

[0010] 特許文献2には、ユーザの操作や文書アクセス要求からユーザ毎の利用履歴を記憶し、その利用履歴と文書間の関連付けの規則から文書間に自動的にリンクを張り、リンクを張るためのユーザの手間を省き、ミスを防止することができる文書間リンク処

理システムが開示されている。

[0011] 特許文献3は、特許文献2と同様に文書間のリンクに関する発明であるが、文書単位、およびユーザ単位に文書間の関連付け条件を記憶させることによって、リンクのメンテナンスを行う必要がなく、文書に関連する最新の情報をいつでも取得することを可能とする文書管理システムを開示しており、アクセスをしているユーザをシステムが認識することにより、ユーザ番号を特定してユーザ毎に関連文書の検索を行うことを可能としている。

[0012] しかしながらこれら3つの特許文献においては、計算機システムにおける資源管理のための技術や、文書間の関連付けのための文書間リンクの管理が対象となっており、本発明が対象とするようなファイルの属性情報をユーザのアクセス処理に対応して抽出し、その属性情報をファイルに対応させて記憶し、ファイルの検索に利用することはできないという問題点があった。

[0013] 特許文献4にはファイルの属性情報を自動生成する技術が開示されている。例えばユーザのファイル操作を分析し、同時に参照したファイルや同時にコピーしたファイルの名前などを抽出し、ユーザがファイルを検索するときに思い浮かべる、ファイルを扱ったときの状況などを検索条件として利用できるようにファイルの属性情報として記録する関連情報管理方式が開示されている。

[0014] しかしながらこの技術においては、ファイル管理のベースとして従来のファイルシステムが利用されており、ファイルの属性情報は1つのファイルに対して1系統しか許されないのが一般的である。複数のユーザがファイルを共有している場合、ファイルの属性情報はユーザ毎に記憶されることはなく、他のユーザの処理によって上書きされてしまう可能性がある。そこでユーザがファイルを検索する場合に属性情報を用いても、その属性情報自体が他のユーザによって上書きされている場合には、ユーザが探したいファイルを見つけることができない可能性がある。ユーザが自分の記憶に基づいて指定した検索条件と、実際に記録されている属性情報とが合致しないためである。

[0015] 例えばあるユーザAがファイルαを更新した後に他のユーザBが同じファイルを更新したとする。ユーザがファイルを更新すると、そのファイルの属性情報としての最新

ファイル更新時間が上書き変更される。この例ではファイルαに対する最新ファイル更新時間はユーザBがファイルを更新した時間となる。しかしながらユーザAがファイルを検索する場合には、自分がファイルを更新した時間を条件として検索を行うため、ファイルαを見つけることはできないことになる。

発明の開示

[0016] 本発明の目的は、複数のユーザによって共有されるファイルの属性情報をユーザ毎に保存可能とすることによって、ユーザの過去のファイルアクセスに対応する記憶内容にあったファイル検索を容易とし、ユーザの情報管理の負担を軽減させることである。

[0017] 本発明のファイル属性情報管理プログラムは、複数のユーザによって共有される共有ファイルの属性情報を管理する計算機によって使用されるプログラムであり、ユーザによる共有ファイルへのアクセスを監視し、アクセスに関するイベントとアクセスを行ったユーザの情報とを抽出するアクセス監視手順と、アクセス監視手順の抽出結果を用いてアクセスを行ったユーザを特定し、アクセスに関するイベントから共有ファイル属性情報をユーザ毎に取得する属性情報抽出手順とを計算機に実行させるためのものであり、また属性情報抽出手順によって取得された共有ファイル属性情報を、ユーザ毎にデータベースに格納する属性情報管理手順をさらに計算機に実行させるものである。また本発明においてはこのようなプログラムを格納した計算機読出し可能可搬型記憶媒体が用いられる。

[0018] 発明の実施の形態においては、本発明のプログラムはデータベースに格納されている共有ファイル属性情報に対してアクセス可能なユーザを示すアクセス制御リストを設定する手順と、共有ファイル属性情報へのアクセスを要求するユーザがそのアクセス制御リストの内容を満足するかを判定する判定手順とをさらに計算機に実行させることもできる。さらに実施の形態においては、ユーザからの共有ファイル属性情報の出力要求に応じてそのユーザを特定し、特定されたユーザがアクセス制御リストの内容を満足することが前記判定手順によって判定された時、要求された共有ファイル属性情報をユーザ側に出力する手順をさらに計算機に実行させることもできる。

[0019] また実施の形態において本発明のプログラムは、ユーザからのアクセス制御リスト設

定／変更の要求に応じて、アクセス制御リストの内容が格納されているメモリの記憶内容の設定／変更を行う手順をさらに計算機に実行させることもでき、あるいはユーザからの要求に応じて共有ファイル属性情報に対して設定されているアクセス制御リストの変更を行う手順をさらに計算機に実行させることもできる。

[0020] 本発明のファイル属性情報管理方法は、複数のユーザによって共有される共有ファイルの属性情報を管理する方法であって、ユーザによる共有ファイルへのアクセスを監視し、アクセスに関するイベントとアクセスを行ったユーザの情報とを抽出し、その抽出結果を用いてアクセスを行ったユーザを特定し、アクセスに関するイベントから共有ファイルの属性情報をユーザ毎に取得する方法が用いられる。

[0021] 発明の実施の形態においては、本発明のファイル属性情報管理方法は前述の管理プログラムと同様に、取得された属性情報をユーザ毎にデータベースに格納することもでき、またこの共有ファイル属性情報に対するアクセス制御リストを設定し、アクセスを要求するユーザがアクセス制御リストの内容を満足するかを判定することもでき、あるいはユーザからの共有ファイル属性情報の出力要求に応じて要求された共有ファイル属性情報をユーザ側に出力することもできる。

[0022] 本発明のファイルアクセス属性情報管理装置は、ユーザによる共有ファイルへのアクセスを監視し、アクセスに関するイベントとアクセスを行ったユーザの情報とを抽出するアクセス監視手段と、アクセス監視手段の出力を用いてアクセスを行ったユーザを特定し、アクセスに関するイベントから共有ファイルの属性情報をユーザ毎に取得する属性情報抽出手段とを備える。

[0023] 以上のように本発明によれば、複数のユーザによって共有される共有ファイルの属性情報をユーザ毎に取得し、その共有ファイル属性情報をユーザ毎にデータベースに格納することによって、ユーザによるファイルアクセスを容易にすることができる。

図面の簡単な説明

[0024] [図1]本発明のファイル属性情報管理プログラムの機能的な原理ブロック図である。

[図2]本発明の共有ファイル属性情報管理方式が用いられるファイル共有システムの構成例のブロック図である。

[図3]ファイル共有サーバの構成例のブロック図である。

[図4]ファイル共有サーバの機能的な詳細構成を示すブロック図である。

[図5]ファイルアクセス監視部による処理の詳細フローチャートである。

[図6]ファイルアクセスイベントとユーザ情報の検出結果の例を示す図である。

[図7]属性情報抽出部による処理の詳細フローチャートである。

[図8]図7において同時参照ファイルのファイル名を属性情報として抽出する処理の詳細フローチャートである。

[図9]図7において同時コピーファイルのファイル名を属性情報として抽出する処理の詳細フローチャートである。

[図10]属性情報管理部による処理の詳細フローチャートである。

[図11]共有ファイル属性情報の例を示す図である。

[図12]アクセス制御リストの例を示す図である。

[図13]属性情報出力処理の詳細フローチャートである。

[図14]ファイル検索処理の詳細フローチャートである。

[図15]アクセス制御リストの設定／変更処理の詳細フローチャートである。

[図16]アクセス制御リスト取得処理の詳細フローチャートである。

[図17]ファイル属性情報とアクセス制御リストのリンクを説明する図である。

[図18]本発明におけるプログラムのコンピュータへのローディングを説明する図である。

発明を実施するための最良の形態

[0025] 図1は本発明のファイル属性情報管理プログラムの原理的な機能ブロック図である。同図は複数のユーザによって共有される共有ファイルの属性情報を管理する計算機によって用いられるプログラムの原理的な機能ブロック図である。

[0026] 図1においてまず1で、ユーザによる共有ファイルへのアクセスに関するイベントとアクセスを行ったユーザの情報とが抽出され、2でそのユーザ情報からそのユーザが特定され、アクセスに関するイベントから共有ファイル属性情報がユーザ毎に取得され、3でその共有ファイル属性情報がユーザ毎にデータベースに格納される。これによってユーザ毎のファイル属性情報は、他のユーザの同一ファイルへのアクセスによっても上書き消去されることはなく、各ユーザは自分の過去のファイルアクセスの記憶

内容にしたがってファイルの検索を行うことが可能となる。

[0027] 図2は、本発明の共有ファイル属性情報管理方式が用いられるファイル共有システムの構成ブロック図である。同図においてシステムは、複数のクライアント(端末)10、ファイル共有サーバ11、およびこれらを相互に接続するネットワーク12によって構成されている。ファイル共有サーバ11に対しては同時に複数のクライアント10との間での通信がネットワーク12を介して実現可能である。ファイル共有サーバ11とクライアント(端末)10とは同一の計算機の内部に実現されることもできる。共有ファイルのユーザは、クライアント(端末)10からファイル共有サーバ11によって管理される共有ファイルにアクセスすることができる。

[0028] 図3は、ファイル共有サーバのハードウェア構成例の説明図である。同図においてファイル共有サーバ11には、ネットワーク12、共有ファイルなどを格納する外部記憶装置13、および本発明とは直接の関係がないユーザインタフェース14が接続されている。ファイル共有サーバ11は、処理を実行するCPU20、プログラムなどを格納するROM21、プログラムの実行時におけるデータなどを格納するRAM22、入出力装置などを接続するためのI／O23、およびこれらが接続されるバス24から構成され、I／O23にはネットワーク12、外部記憶装置13、およびユーザインタフェース14が接続される。

[0029] 図4は、ファイル共有サーバの機能的な構成ブロック図である。同図においてファイル共有サーバ11は、複数のクライアント10とローカルエリアネットワークLAN26によって接続されているものとし、その内部にファイルアクセス監視部30、属性情報抽出部31、属性情報管理部32、属性情報出力部33、ACL設定および取得部34を備えている。なおここでは、ファイル共有サーバ11内で本発明に直接関連のある機能ブロックのみを示しており、例えばファイル共有サーバ11の内部で図3の外部記憶装置13に格納されている共有ファイル自体を管理する共有ファイル管理部などは省略されている。なおこの共有ファイル管理部はファイル共有サーバ11の内部に備えられてもよく、あるいはファイル共有サーバ11の外部で外部記憶装置13に対するアクセス専用のコンピュータの内部に備えられることもできる。

[0030] ファイルアクセス監視部30は、前述のように図示しない共有ファイル管理部を介し

たユーザによる共有ファイルへのアクセスを監視するものであり、ユーザによるクライアント端末10を用いた共有ファイルへのアクセス処理としてのファイルやフォルダのオープン、クローズ、リード、ライト、名前変更、および削除などすべてのアクセス処理が監視される。ただし、システムの設計時にディレクトリに関する処理を除外するなど、一部のアクセス処理に限定することも可能である。

[0031] 属性情報抽出部31は、ファイルアクセス監視部30による監視結果を分析し、ユーザ特定部35によって同定されるユーザごとに属性情報の抽出を行う。属性情報の種類としては、ファイルのアクセス時刻、更新時刻、ファイル名が変更された場合の古いファイルの名前、あるファイルと同時に参照したファイルのファイル名などが抽出される。ユーザ特定部35は、共有ファイルにアクセスしたユーザを識別するための情報、すなわち名前、ユーザID、クライアント名などを用いてユーザの同定を行う。なおファイルアクセス監視部30と属性情報抽出部31は基本的にファイル共有サーバ11の内部で、ユーザからは見えない処理を行うものであり、ファイル共有サーバ11の枠との間の矢印は省略されている。

[0032] 属性情報管理部32は、属性情報データベースを基本的な構成要素とするものであり、属性情報抽出部31によって抽出された属性情報、およびユーザIDなどを用いてユーザ毎にファイルの属性情報を管理するものである。属性情報としては、最新の情報だけでなく、過去の全ての情報、すなわち全てのファイルアクセス時刻や更新時刻を記録しておくこともできる。

[0033] 属性情報データベース38の内容としては、ファイル毎、例えばファイルAに対してユーザ毎に属性1から属性5．．、例えばアクセス時刻、更新時刻などの属性データが記録される。属性情報管理部32によって管理される情報としては、この属性情報データベース38の他に、アクセスコントロールリストACL36がある。ACL36は、後述するように各ユーザの属性情報に対応してその属性情報にアクセスできるユーザを定義するものであり、属性情報管理部32の内部のACL判定部37は、このACL36の内容を用いて各ユーザが参照できる属性情報の範囲を管理するものである。

[0034] 属性情報出力部33は、ユーザからの要求に応じてファイルの属性情報やユーザの指定条件を満たすファイルの検索結果をユーザに対して出力するものである。クライ

アント(端末)10からユーザの要求、例えばユーザが指定するファイルの属性情報の参照要求や、ユーザの指定条件を満たす属性情報を持つファイルの検索要求を受け取った時、ユーザ特定部35によってユーザを識別する情報を用いてユーザの同定が行われる。属性情報出力部31は同定したユーザ名などのユーザ情報とユーザの要求とを属性情報管理部32に伝達する。

[0035] 属性情報管理部32は、ACL36の内容に基づいて、例えばユーザがファイルの属性情報を参照できるか否かを判断し、その判断に対応した結果を属性情報出力部33に返す。属性情報出力部33は、この応答を受け取り、属性情報を整形したり、エラー情報を生成してクライアント10側に返す。

[0036] ACL設定および取得部34は、ユーザの要求に応じてACL36の内容を取得してユーザに返したり、ユーザの要求に応じてファイルの属性情報に対してACLの設定を行う。ACLの内容によって、ユーザが属性情報を公開する条件(公開できるユーザやクライアント、公開できないユーザやクライアントなど)の定義が行われる。

[0037] なお図4において属性情報抽出部31と属性情報出力部33などをそれぞれ複数設け、例えば各属性情報抽出部は1人のユーザに対応して属性情報を抽出して属性情報管理部に送ることも、また属性情報出力部33が対応するユーザに属性情報を出力することもできるものとする。

[0038] 図5は、ファイルアクセス監視部による処理の詳細フローチャートである。ファイルアクセス監視部30は、前述のようにユーザの共有ファイルへのアクセスを監視し、その結果を属性情報抽出部31に伝えるものである。図5において処理が開始されると、まずステップS1でファイルアクセスのイベントがあったか否かが判定される。すなわちユーザから共有ファイルへのアクセスがあると、ファイルのオープンやクローズ、ファイルのリードやライトなど、個々のファイルアクセス処理がイベントとして検出される。ステップS1でイベントが検出されない場合には、ステップS1の処理が続けられる。

[0039] イベントが検出された場合には、ステップS2でこのイベントがファイル属性情報の抽出に有用なイベントであるか否かが判定される。例えばユーザの共有ファイルへのアクセスに先立ち、クライアント10のOSやアプリケーションがファイルのステータスを確認する目的でファイルにアクセスするような場合がある。このようにユーザの記憶に残

らないバックグラウンドで行われたファイルアクセス処理に対応するイベントは、ユーザの記憶にそったファイル属性情報の抽出やファイルの検索には利用できないため、有用なイベントでないものとしてステップS1以降の処理が繰り返される。

[0040] ここで属性情報の抽出に有用なイベントとしては、例えばファイルのオープン／クローズ、ファイルのリード／ライト、ファイル名やディレクトリ名の変更、ファイルの移動、ファイルの削除、ディレクトリのオープン／クローズ、ディレクトリの作成、ディレクトリの削除などがある。

[0041] このような有用なイベントが検出されると、ステップS3でファイルにアクセスしたユーザを特定するためにユーザ名、ユーザID、クライアント名などの情報が取得され、ステップS4でファイルアクセスのイベントの種類とユーザに関する情報が属性情報抽出部31に伝達され、このイベントに対応する処理が終了する。図5の処理は、実際には、例えばシステムの起動時にスタートし、1つのイベントに対してステップS4で終了するが、さらに次のイベントに対応する属性情報を抽出するために、ステップS1からS4までの処理がシステムの動作中には無限に繰り返されることになる。

[0042] 図6はファイルアクセス監視部30によって検出されたファイルアクセスのイベントと、ユーザ情報の例の説明図である。同図において処理対象特定IDは、例えばファイルディスクリプタ番号であり、どのユーザのどのファイルへの処理に関するものかを特定するものである。ファイルディスクリプタ番号は、例えばファイル共有サーバ11が自動的につける番号であり、例えばユーザAがファイルαにアクセスするとそれに対応する番号が付けられ、同じファイルに対してユーザBがアクセスすると異なる番号が付けられる。同時に同じファイルディスクリプタ番号が用いられることはないが、別の日などに同じ番号がつかわれる可能性はある。

[0043] イベントの情報としては、イベントの種類や、そのイベントの種類に対応するパラメータがある。このパラメータも属性情報抽出部31に与えられ、属性情報の抽出に利用される。そのパラメータとしては、ファイル共有サーバ側で、例えばローカルに付加されるファイル名や、ユーザから認知することが可能なファイル名、処理の開始時刻、完了時刻などがある。ユーザ情報としては、ユーザ名、またはID、およびクライアント10の名称、またはIDがある。

[0044] 図6において、例えば一番上の2つの行のイベントと、最後の行のイベントに対応する処理対象特定ID、例えばファイルディスクリプタ番号は全て28であり、ユーザ名は3328、クライアント名はクライアントAでそれぞれ同一である。そこで同一のファイルのオープン、リード、およびクローズの処理が1人のユーザによって行われたことになり、この3つのイベントを1つの組としてこの1組のイベントに対応するファイルアクセスに対する属性情報が抽出される。なお、イベント種類の中でunlinkは、ファイルの削除を示す。

[0045] 図7は、属性情報抽出部31による処理の詳細フローチャートである。同図において処理が開始されると、まずステップS10でファイルアクセス監視部30からのイベントとユーザ情報が受信されたか否かが判定され、まだ受信されていない場合には、その処理が繰り返される。受信した場合にはステップS11でユーザ情報からユーザがユニークに特定される。ユーザ情報は前述のように、例えばユーザ名、IDなどであるが、クライアント10やファイル共有サーバ11が設置されたネットワーク環境によっては変化する可能性がある。クライアント10側からユーザ名やIDが送られてきたり、IPアドレスやMACアドレスなどが送られてきたりする可能性があり、このような様々な情報からユーザ特定部35によってユーザの同定が行われる。

[0046] 続いてステップS12で同一ユーザからのイベントの受信が行われる。ここでは簡単のために図4の属性情報抽出部31と属性情報出力部33が前述のようにそれぞれ複数存在し、それぞれの属性情報抽出部31や属性情報出力部33が1人のユーザに対応してファイルの属性情報を抽出したり、属性情報の出力を行うものとする。そこでステップS12以降では、ステップS11で特定されたユーザからのファイルアクセスに関するイベントが受信され、そのイベントに対応して属性情報の抽出が行われるものとする。

[0047] その後ステップS13で属性情報抽出に十分なイベント情報が集まったか否かが判定され、まだ集まっていない場合には、ステップS12以降の処理が繰り返される。ここでこの十分なイベント情報が集まったか否かの判断は属性情報ごとに異なり、例えば前述のようにファイルのオープンからクローズまでのイベントが検出されることによって十分なイベント情報が集まったと判定する場合もあり、あるいは同時に、例えば1つの

フォルダに複数のファイルがコピーされ、ファイルのファイル名を属性情報として抽出する場合には、それに対応した判定が必要となる。そのような例は図8、および図9で後述する。

[0048] ステップS13で十分なイベント情報が集まったと判定されると、ステップS14で属性情報の抽出が行われ、ステップS15で属性情報抽出に使用されたイベント情報が破棄され、ステップS16で抽出された属性情報とユーザ名の情報が属性情報管理部32に伝達され、例えば前述のようなファイルオープンからファイルクローズまでの1組のイベント情報に対応する属性情報の抽出処理が終了する。なおこの属性情報抽出処理も、例えばシステムの起動時にスタートし、1組のイベントに対応する属性情報の抽出が終わると、システム動作中はステップS10以降の処理が無限に繰り返されることになる。なお、例えば属性情報抽出部31が1つしか存在しない場合には、その処理としてステップS12は実行されず、ステップS13で十分なイベント情報が集まっていないときにはステップS10に戻り、イベント情報がユーザ毎に区分されて、ステップS13からステップS16が実行される。

[0049] 図7で説明したように属性情報を抽出する前に十分なイベント情報が集まったかの判定が行われる。例えばファイルオープンのイベントだけを受け取っても、そのファイルに対するアクセスが内容の読み取りだけなのか、これから更新を行うのかは不明である。内容が読み取られるだけの場合には、属性情報としてアクセス時刻が抽出されるが、更新される場合にはアクセス時刻だけでなく、更新時刻も抽出する必要がある。このような判断を行うためには、ファイルオープンのイベントを受け取った後にそれに続くイベントがリードやライトなのかを確認する必要があり、また最終的にはそのファイルのクローズのイベントを検出する必要がある。図8はこのようにファイルのオープンからクローズまでのイベントを検出し、それによって十分なイベント情報が集まったと判定して属性情報を抽出する場合の、図7のステップS12からS14に対応する詳細処理のフローチャートである。

[0050] すなわちユーザがあるクライアント10を用いてファイルAを開くと、オープンのイベントが発生する。ファイルAを閉じた時点で生ずるクローズのイベントが起きるまでに、同じユーザが同じクライアント10を用いて他のファイル(B)を開くと、そのファイルに対

応するオープンのイベントが生じる。これによってファイルAとファイルBが同時に参照されたことを知ることができ、その結果が属性情報として抽出される。ファイルを同時に参照したか否かは相互的な関係であり、ファイルAの属性情報としてファイルBのファイル名を抽出すると同時に、ファイルBの属性情報としてファイルAのファイル名の抽出が必要となる。

[0051] すなわち図8において処理が開始されると、ステップS20でファイルAに対するオープンのイベントが検出され、ステップS21でファイルAに対するクローズのイベントが検出されたか否かが判定され、まだ検出されていない場合には、ステップS22でファイルA以外のファイルのオープンのイベントが検出されたか否かが判定され、検出された場合にはステップS23でそのファイルの名前が取得されて保持された後に、また検出されていない場合にはただちにステップS12の同一ユーザからのイベント受信の処理が行われ、ステップS21以降の処理が繰り返される。

[0052] ステップS21でファイルAに対するクローズのイベントが検出された時には、ステップS24で保持されているファイル名がファイルAに対する属性情報として抽出され、ステップS25で保持されていたファイルの属性情報としてファイルAのファイル名が抽出されて処理を終了する。すなわち図7のステップS13の処理は図8では基本的にステップS21の処理に相当するが、十分なイベント情報が集まっていない場合にはステップS22、S23の処理が行われた後に、ステップS12の同一ユーザからのイベント受信の処理が行われることになる。

[0053] 図8では同時に参照したファイルが、ユーザ側から見て関連性が高いファイルと見なされていると考えられるために、それらのファイル名が属性情報として抽出される。ファイルアクセス監視部からは繰返しファイルのオープンやクローズのイベントが伝えられることになるが、それらのイベントを個別に扱うことなく、最初のファイル、ここではファイルAのクローズが生ずるまで待ち、その間に生じたイベントをすべて分析することによって同時に参照されたファイルのファイル名が属性情報として抽出される。

[0054] 図9は、ファイルの同時コピーに対応する属性情報抽出時の、図7のステップS12からS14に相当する処理の詳細フローチャートである。ここではあるフォルダから別のフォルダに同時に、すなわち連続的に複数のファイルのコピーが行われた場合、そ

のファイル名を属性情報として抽出する処理が行われる。ユーザがクライアント10を用いて複数のファイルを同時にコピーする場合には、次々にファイルを開いて内容を読み出し、その内容を別のフォルダにファイルとして書き込む動作が行われる。この処理が予め定められた時間内に繰返し次々と行われた場合には同時にコピーが行われたものと判断し、そのコピーが行われたファイルの名前をファイルの属性情報として抽出する処理が行われる。

[0055] 図9において処理が開始されると、まずステップS28で予め定められた時間内で次のファイルのコピー処理が始まったか否かが判定される。ただし、一度目のコピー処理の場合にはこの判定は行われない。その時間内に処理が始まった場合にはステップS29でコピー元のファイルのオープン、ステップS30でコピー先のファイルのオープンが検出され、ステップS31でコピー先のフォルダ名が抽出されて、例えばバッファに保持される。

[0056] 続いてステップS32でコピー元のファイルに対するリードのイベントが検出され、ステップS33でコピー先のファイルへのライトのイベントが検出され、ステップS34でコピー元のファイルのクローズのイベントが検出され、ステップS35でコピー先のファイルのクローズが検出され、ステップS36でコピー先のフォルダ名がその前のコピー処理におけると同じフォルダ名か否かが判定される。一度目のコピー処理に対してはこの判定は行われず、ステップS29からS35までの処理だけが行われる。なおステップS28からS35の処理では前述と同様に同一ユーザからのイベント受信の処理が含まれるものとし、その受信結果に対応して判定や検出が行われる。

[0057] ステップS36の判定結果が同じフォルダ名である場合にはステップS37で同時コピーが行われたものとしてそのファイルのファイル名がバッファに保持された後にステップS28以降の処理が繰り返される。そしてステップS28で次のファイルのコピー処理が予め定められた時間内に始まらなかったと判定された場合、およびステップS36でコピー先のフォルダ名が前のコピー処理におけると同じフォルダ名でないと判定されると、ステップS38で保持されていたファイルのファイル名がそれぞれのファイルの属性情報、すなわち同時にコピーが行われたファイルのそれぞれに対する属性情報として抽出されて処理を終了する。

[0058] 図10は、属性情報管理部32による処理の詳細フローチャートである。同図において処理が開始されると、まずステップS40で属性情報抽出部31から属性情報とユーザ名などの情報を受信したか否かが判定され、まだ受信していない場合にはその処理が続行される。受信した場合にはステップS31で属性情報がユーザ毎にデータベースに登録され、ステップS42で登録された属性情報に対して各ユーザに対するデフォルトのアクセスコントロールリストが設定されて、受信した属性情報とユーザ情報に対する処理が終了する。図10の処理はシステムの動作中は無限に繰り返される。なおここでは登録された属性情報に、例えば各ユーザ毎に異なるデフォルトのACLが設定されるものとしたが、このデフォルトのACLは、システムによって設定されたデフォルトのものでも良く、ユーザによって指定されたデフォルトのものでも良い。

[0059] 図11は、ファイルBに対する属性情報の例である。この属性情報の各行は、図7においてステップS13で十分なイベント情報が集まったと判定された後に、1組のイベントに対応して抽出された属性情報を示すものである。

[0060] 図11では、ファイルBの属性情報がアクセス日時の古いものが下になるように配置されている。最も下の行の属性情報においては、アクセス日時、更新日時、作成日時が同一であり、この時点でファイルBの作成そのものが行われたことが示されている。例えばその上の行の属性情報としては、ユーザTarouがファイルBにアクセスし、同時にファイルAとファイルDとを参照したことが示されている。なお“削除したか”の欄には、ファイルが削除された場合に、そのことをユーザに知らせるためのフラグが設定される。

[0061] 図12は、ユーザTarouに対するアクセスコントロールリストの例である。このユーザに対しては2種類のACLが図4の属性情報管理部32の内部のACL36に登録されているが、上のACL(Tarou−1)はデフォルトのACLであり、これに対して下のACL(Tarou−2)は後述するようにユーザTarouによって設定されたデフォルトと異なるACLである。下のACLでは属性情報に対する参照を許可するユーザとしてTarouとHanakoとが指定され、参照を拒否するユーザとしては許可するユーザ以外の全てのユーザが指定され、属性情報を変更できるユーザとしてはTarouのみが指定されている。図11の下から2番目の属性情報に対してはこのACLが指定されているが、こ

の指定は図10のステップS42でデフォルトのACLが設定された後に、後述するようにユーザ側からのACL設定要求に対応して、ACLの変更が行われたことを示している。

[0062] 図13は、ユーザからの要求による属性情報出力処理の詳細フローチャートである。この処理は図4の属性情報出力部33と属性情報管理部32とによって実現される。処理が開始されると、まずステップS45で属性情報出力部33によって、クライアントからの属性情報の参照や検索の要求とユーザ情報の受信が行われた否かが判定され、行われていない場合にはこの処理が繰り返される。受信した場合にはステップS46でユーザ特定部35によってユーザ情報からユーザがユニークに特定され、ステップS47で属性情報管理部32に対してクライアント側、すなわちユーザの要求とユーザ名などのユーザ情報が伝達される。

[0063] 属性情報管理部32側では、ステップS48で属性情報出力部33からの出力要求やユーザ情報を受信したか否かが判定され、まだ受信していない場合にはこの処理が繰り返される。受信した場合にはステップS49で、そのユーザが参照したい属性情報に対応するアクセスコントロールリストの内容に対応して、図11、および図12からそのユーザが参照を許可されたユーザであるか否かが判定され、参照が許可される場合にはステップS50で属性情報が属性情報出力部33に伝達され、ステップS51で属性情報出力部33からクライアント側に属性情報が出力されて処理を終了する。

[0064] これに対してステップS49で属性情報参照、あるいは検索の要求を行ったユーザが参照が許可されるユーザでない場合には、ステップS52で属性情報を出力できないことが属性情報管理部32から属性情報出力部33に伝達され、ステップS53で属性情報出力部33からクライアント10側にエラーが出力されて処理を終了する。なお図13の処理も図7と同様に、例えばシステムの起動時にスタートし、ユーザからの要求に対してステップS51、またはステップS53の処理によって一旦処理を終了するが、ステップS45の受信検出からの処理がシステムの動作中は常に繰り返されることになる。

[0065] 図14は、ユーザからの要求によるファイル属性情報を用いたファイル検索処理の詳細フローチャートである。本実施形態では、ユーザが自分の過去の共有ファイルへ

のアクセス時に抽出されたと考えられる共有ファイルのメタデータとしてのファイル属性情報を用いてファイル検索を行うことができる点に大きな特徴があるが、図14ではユーザから与えられる検索条件に対応して検索条件に合致する属性情報に対してそのユーザがアクセスできるかどうかを判定し、アクセスできる属性情報に対応するファイルのみを抽出して検索結果をユーザ側に戻す処理が行われる。

[0066] 図14において処理が開始されると、まずステップS56でクライアント10側からのユーザによるファイルの検索要求とそのユーザのユーザ情報が受信されたか否かが属性情報出力部33によって判定され、まだ受信していない場合にはこの処理が繰り返される。受信した場合にはステップS46でユーザ特定部35によってユーザがユニークに特定され、ステップS47で属性情報管理部32に対してユーザからの検索要求とユーザ名などの情報が伝達される。

[0067] 属性情報管理部32側では、ステップS48で属性情報出力部33からのユーザの要求とユーザ情報が受信されたか否かが判定され、まだ受信していない場合にはこの処理が繰り返される。受信した場合にはステップS57で指定された検索条件を満たすファイルが検索され、ステップS58で検索されたファイルの中で検索条件に合致する属性情報へのアクセス許可があるファイルのみが抽出される。このアクセス許可の有無の判定はACL36を用いてACL判定部37によって行われる。そしてステップS59ではその抽出されたファイルのみが属性情報出力部33に伝達され、ステップS60で属性情報出力部33からクライアント10側に抽出されたファイルが出力されて処理を終了する。なお図14の処理も図13と同様にステップS56の受信検出以後が常に行われる形式で実行される。

[0068] 図15は、アクセスコントロールリストACLの設定、および変更処理の詳細フローチャートである。この処理は図4のACL設定および取得部34と、属性情報管理部32とによって実行される。図15において処理が開始されると、ステップS61でクライアント10側からのACLの設定、または変更の要求とユーザ情報が受信されたか否かがACL設定および取得部34によって判定される。まだ受信していない場合にはこの処理が繰り返される。受信した場合にはステップS62でユーザ特定部35によってユーザがユニークに特定され、ステップS63で属性情報管理部32に対してユーザからの要求

とユーザ情報が伝達される。

[0069] 属性情報管理部32では、ステップS64でACL設定および取得部34からユーザの要求とユーザ情報を受信したか否かが判定され、まだ受信していない場合にはこの処理が繰り返される。受信した場合にはステップS65でユーザが変更の対象とする属性情報のACLに対応して、ACLの内容を変更可能なユーザであるか否かが、図11、図12の内容を用いて判定される。ユーザがACLの変更要求を行う場合にはユーザはACLの内容を知る必要があるが、このユーザによるACLの取得については図16で説明する。

[0070] ユーザがACLを変更可能なユーザである場合には、ステップS66で新しいACLの設定か否かが判定され、その設定である場合にはステップS67で新しいACLが登録された後に、新しい設定でない場合には直ちにステップS68の処理に移行する。ステップS68ではユーザの要求に対応して属性情報に対するACLの変更が行われ、その結果がACL設定および取得部34に返され、ステップS69で変更結果がクライアント側に出力されてユーザからの要求に対応する処理が終了する。

[0071] ステップS65でユーザがACLを変更可能でない場合には、ステップS70でACLを変更できないことが属性情報管理部32からACL設定および取得部34に通知され、ステップS71でクライアント側にエラーが出力されてユーザ要求に対する処理を終了する。

[0072] 前述のように例えばユーザがACLの内容を変更する場合には、ユーザは図12に示すようなACLの設定内容を取得し、その内容を変更したり、図11の属性情報に対して設定すべきACLの変更を行う。個々のACLの指定にあたってはACLのIDとして、ユニークに定められた、図12に示されているACL名や数値が用いられる。

[0073] 図16はACL取得処理の詳細フローチャートである。同図において処理が開始されると、まずステップS75でACL設定および取得部34によって、クライアント10側からユーザによるACLの取得要求とユーザ情報を受信したか否かが判定され、まだ受信していない場合にはこの処理が繰り返される。受信した場合にはステップS76でユーザがユニークに特定され、ステップS77で属性情報管理部32に対してACL取得要求とユーザ情報が伝達される。

[0074] 属性情報管理部32側ではステップS78で、ACL設定および取得部からのユーザの要求とユーザ情報が受信されたか否かが判定され、受信していない場合にはその処理が繰り返される。受信した場合にはステップS79でACL36の内容を用いてそのユーザのACLをACL設定および取得部34に伝達し、ACL設定および取得部34側ではステップS80でクライアント10側にそのACLを出力して処理を終了する。なお図15、および図16においてもステップS61、ステップS75の受信検出処理以降が常に実行される。

[0075] 図17は、図11で説明したようなファイルの属性情報と、図12で説明したようなACLとのリンクの説明図である。前述のように属性情報抽出部31によって属性情報が抽出されると、属性情報管理部32によって属性情報データベースに対してその属性情報に対応するACLとしてそのユーザのデフォルトのACLが設定される。図12ではTarouに対する属性情報の登録時には、Tarou−1のACLが設定される。デフォルトのACLとしては、前述のようにシステムによって設定されたものを用いることもでき、あるいは各ユーザによって図15の処理によって設定されたものを用いることもできる。

[0076] その後図16で説明したように属性情報に設定されたACLを変更することもできる。またACLそのものの内容の変更や、新しいACLの登録も可能であり、図11の上から3行目と4行目などの属性情報に対しては、最初に設定されたデフォルトのACLがその後デフォルトでないTarou−2に変更されている。ユーザから属性情報出力部33を介してファイル属性情報に対するアクセスの依頼があると、属性情報管理部32では属性情報に対して設定されたACLのIDを調べ、そのIDが示すACLの内容の確認を行う。その結果によってアクセス依頼を行ったユーザにその属性情報へアクセス権があると判定すると、そのファイル属性情報へのアクセスが許可される。

[0077] 以上において本発明のファイル属性情報管理プログラムなどについてその詳細を説明したが、このプログラムは当然一般的なコンピュータシステムによって実行されることが可能である。図18はそのようなコンピュータシステム、すなわちハードウェア環境の構成ブロック図である。

[0078] 図18においてコンピュータシステムは中央処理装置(CPU)50、リードオンリメモリ(ROM)51、ランダムアクセスメモリ(RAM)52、通信インタフェース53、記憶装置54

、入出力装置55、可搬型記憶媒体の読取り装置56、およびこれらの全てが接続されたバス57によって構成されている。

[0079] 記憶装置54としてはハードディスク、磁気ディスクなど様々な形式の記憶装置を使用することができ、このような記憶装置54、またはROM51に図5、図7ー図10、図13ー図16などのフローチャートに示されたプログラムや、本発明の請求の範囲のプログラムなどが格納され、そのようなプログラムがCPU50によって実行されることにより、本実施形態におけるファイル属性情報のユーザ毎の管理、属性情報を用いたファイル検索、アクセスコントロールリストによる管理などが可能となる。

[0080] このようなプログラムは、プログラム提供者58からネットワーク59、および通信インタフェース53を介して、例えば記憶装置54に格納されることも、また市販され、流通している可搬型記憶媒体60に格納され、読取り装置56にセットされて、CPU50によって実行されることも可能である。可搬型記憶媒体60としてはCD−ROM、フレキシブルディスク、光ディスク、光磁気ディスク、DVDなど様々な形式の記憶媒体を使用することができ、このような記憶媒体に格納されたプログラムが読取り装置56によって読取られることにより、本実施形態におけるユーザ毎のファイル属性情報の管理などが可能となる。

[0081] 以上詳細に説明したように本発明によれば、ファイル共有サーバにおいてユーザ毎にファイルの属性情報を抽出し、管理することにより、他のユーザの処理によって自分のファイル処理によって生成されたファイル属性情報が上書きされて消えてしまうことが防止される。そこでユーザは自分が共有ファイルにアクセスした時間や更新した時間、自分の覚えているファイル名など、自分の持っている記憶内容に沿った検索条件を用いてファイルを探すことが可能になり、共有ファイルを用いた情報処理の効率向上に寄与するところが大きい。

[0082] また他のユーザのファイル処理によって生成されたファイル属性情報を参照することによって自分の情報管理に利用することもできる。例えば他のユーザがあるファイルと同時に参照したファイル、すなわちそのユーザがそのファイルと関連が深いと考えている他のファイルを参照することによって自分の仕事に役立てることが可能となる。

[0083] さらに属性情報毎にアクセスコントロールリストACLが設定されるために、ユーザは自分のファイル属性情報を公開してよい他のユーザの範囲などを設定することができ、他人に公開したくない属性情報に対する他人のアクセスを制限することが可能となる。

産業上の利用可能性

[0084] 本発明は、共有ファイル利用システムに対するファイル属性情報管理プログラムを格納した記憶媒体の販売産業や、そのようなプログラムを用いるファイル属性情報管理装置の製造産業などは当然のこととして、複数のユーザによって共有されるファイルシステムを利用する全ての産業において利用可能である。

請求の範囲

[1] 複数のユーザによって共有されるファイルの属性情報を管理する計算機によって用いられるプログラムであって、

ユーザによる前記共有ファイルへのアクセスを監視し、アクセスに関するイベントとアクセスを行ったユーザの情報とを抽出するアクセス監視手順と、

該アクセス監視手順による抽出結果を用いてアクセスを行ったユーザを特定し、アクセスに関するイベントから共有ファイルの属性情報をユーザ毎に取得する属性情報抽出手順とを計算機に実行させることを特徴とするファイル属性情報管理プログラム。

[2] 前記属性情報抽出手順によって取得された共有ファイル属性情報をユーザ毎にデータベースに格納する属性情報管理手順をさらに計算機に実行させることを特徴とする請求項1記載のファイル属性情報管理プログラム。

[3] 前記データベースに格納されている共有ファイル属性情報に対してアクセス可能なユーザを示すアクセス制御リストを設定する手順と、

該共有ファイル属性情報へのアクセスを要求するユーザが該アクセス制御リストの内容を満足するかを判定する判定手順とをさらに計算機に実行させることを特徴とする請求項2記載のファイル属性情報管理装置。

[4] ユーザからの共有ファイル属性情報の出力要求に応じて、該ユーザを特定し、該特定されたユーザが前記アクセス制御リストの内容を満足することが前記判定手順によって判定された時、該要求された共有ファイル属性情報をユーザ側に出力する手順をさらに計算機に実行させることを特徴とする請求項3記載のファイル属性情報管理プログラム。

[5] ユーザからのアクセス制御リスト設定／変更の要求に応じて、前記アクセス制御リストの内容が格納されているメモリの記憶内容の設定／変更を行う手順をさらに計算機に実行させることを特徴とする請求項3記載のファイル属性情報管理プログラム。

[6] ユーザからの要求に応じて、共有ファイル属性情報に対して設定されているアクセス制御リストの変更を行う手順をさらに計算機に実行させることを特徴とする請求項3記載のファイル属性情報管理プログラム。

[7] 複数のユーザによって共有されるファイルの属性情報を管理する方法であって、

ユーザによる前記共有ファイルへのアクセスを監視し、アクセスに関するイベントとアクセスを行ったユーザの情報とを抽出し、

該抽出結果を用いてアクセスを行ったユーザを特定し、アクセスに関するイベントから共有ファイルの属性情報をユーザ毎に取得することを特徴とするファイル属性情報管理方法。

[8] 前記取得された共有ファイル属性情報をさらにユーザ毎にデータベースに格納することを特徴とする請求項7記載のファイル属性情報管理方法。

[9] 前記データベースに格納されている共有ファイル属性情報に対して、さらにアクセス可能なユーザを示すアクセス制御リストを設定し、

該共有ファイル属性情報へのアクセスを要求するユーザが該アクセス制御リストの内容を満足するかを判定することを特徴とする請求項8記載のファイル属性情報管理方法。

[10] ユーザからの共有ファイル属性情報の出力要求に応じて、さらに該ユーザを特定し、該特定されたユーザが前記アクセス制御リストの内容を満足することが判定された時、該要求された共有ファイル属性情報をユーザ側に出力することを特徴とする請求項9記載のファイル属性情報管理方法。

[11] 複数のユーザによって共有されるファイルの属性情報を管理する計算機によって用いられる記憶媒体であって、

ユーザによる前記共有ファイルへのアクセスを監視し、アクセスに関するイベントとアクセスを行ったユーザの情報とを抽出するアクセス監視ステップと、

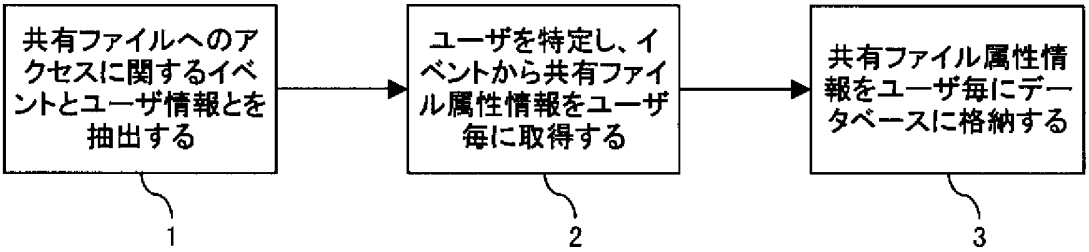
該アクセス監視ステップによる抽出結果を用いてアクセスを行ったユーザを特定し、アクセスに関するイベントから共有ファイルの属性情報をユーザ毎に取得する属性情報抽出ステップとを計算機に実行させるためのファイル属性情報管理プログラムを格納した計算機読み出し可能可搬型記憶媒体。

[12] 複数のユーザによって共有されるファイルの属性情報を管理する装置であって、

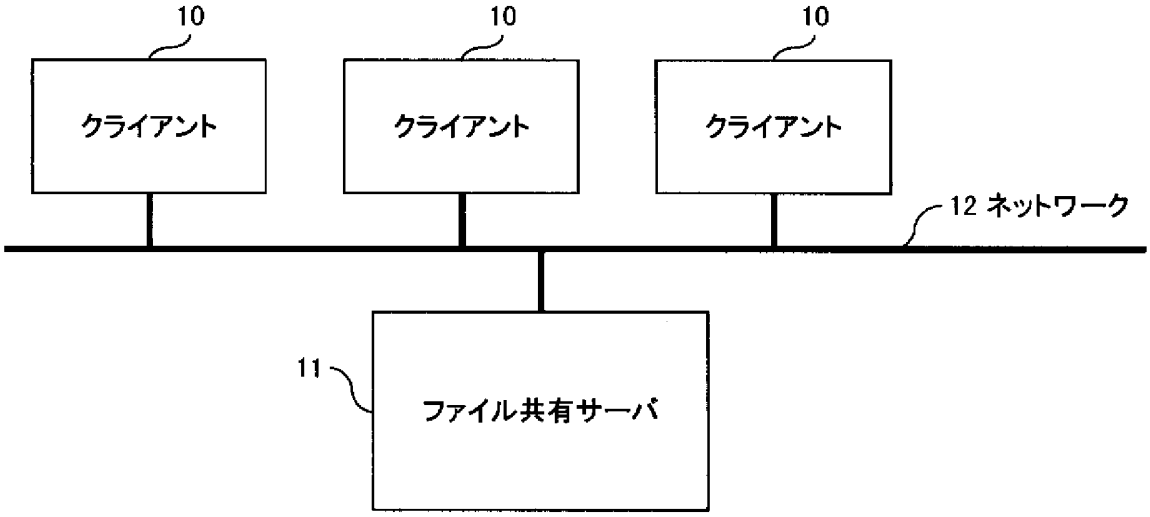
ユーザによる前記共有ファイルへのアクセスを監視し、アクセスに関するイベントとアクセスを行ったユーザの情報とを抽出するアクセス監視手段と、

該アクセス監視手段による抽出結果を用いてアクセスを行ったユーザを特定し、アクセスに関するイベントから共有ファイルの属性情報をユーザ毎に取得する属性情報抽出手段とを備えることを特徴とするファイル属性情報管理装置。

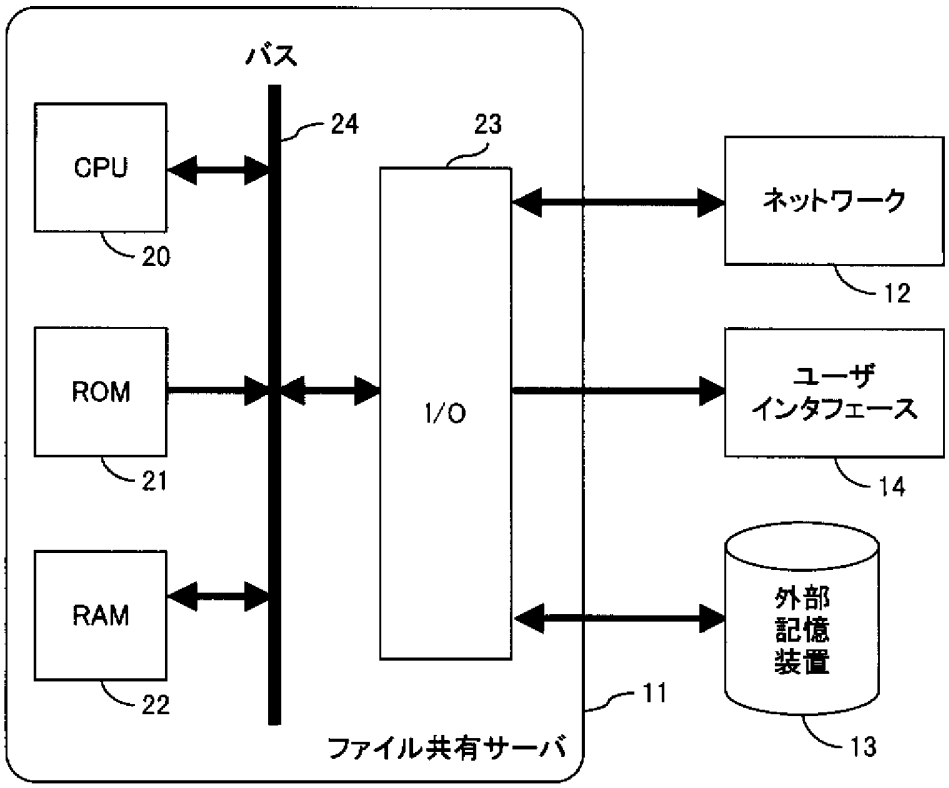
[図1]


共有ファイルへのアクセスに関するイベントとユーザ情報とを抽出する
1
ユーザを特定し、イベントから共有ファイル属性情報をユーザ毎に取得する
2
共有ファイル属性情報をユーザ毎にデータベースに格納する
3

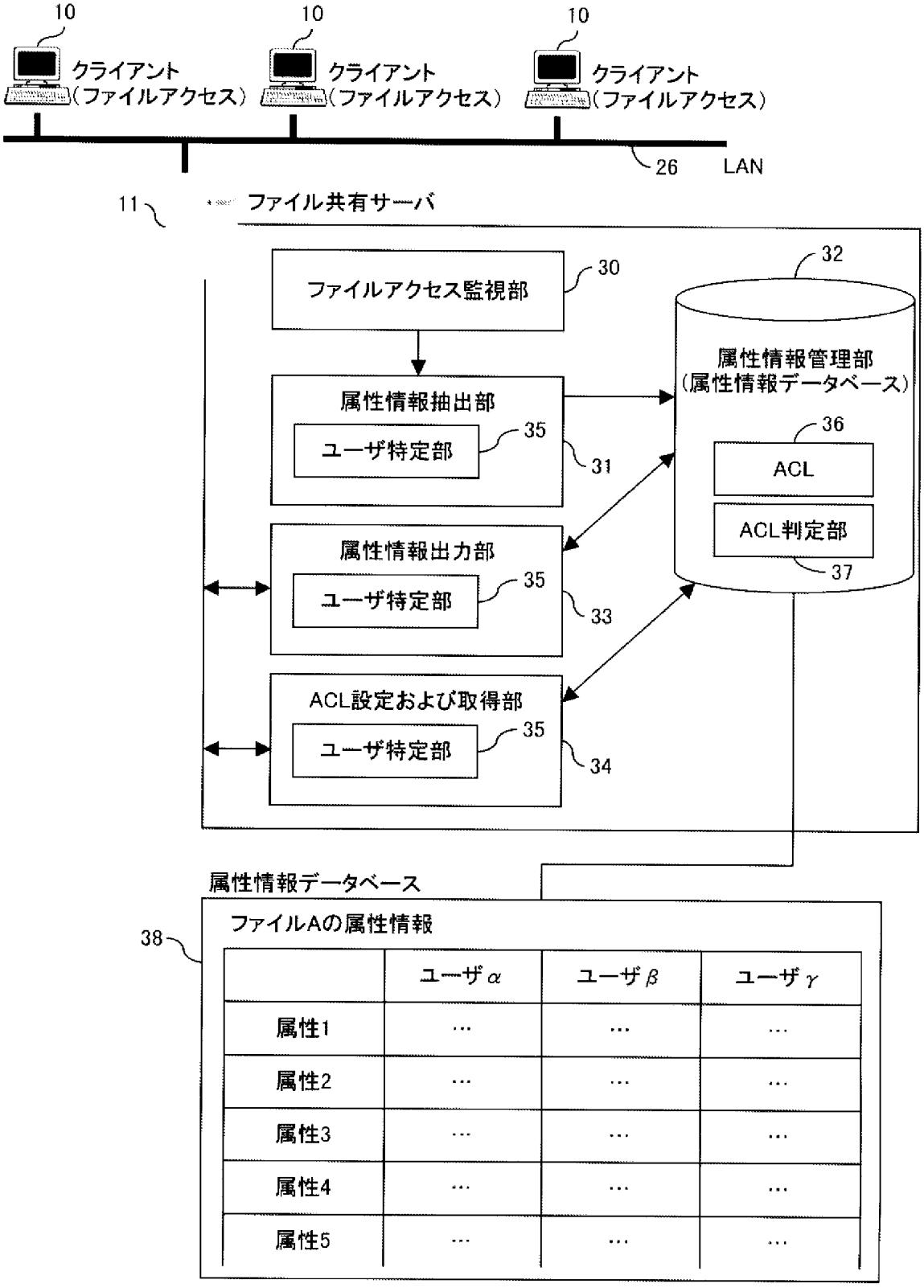
[図2]


10
クライアント
10
クライアント
10
クライアント
12 ネットワーク
11
ファイル共有サーバ

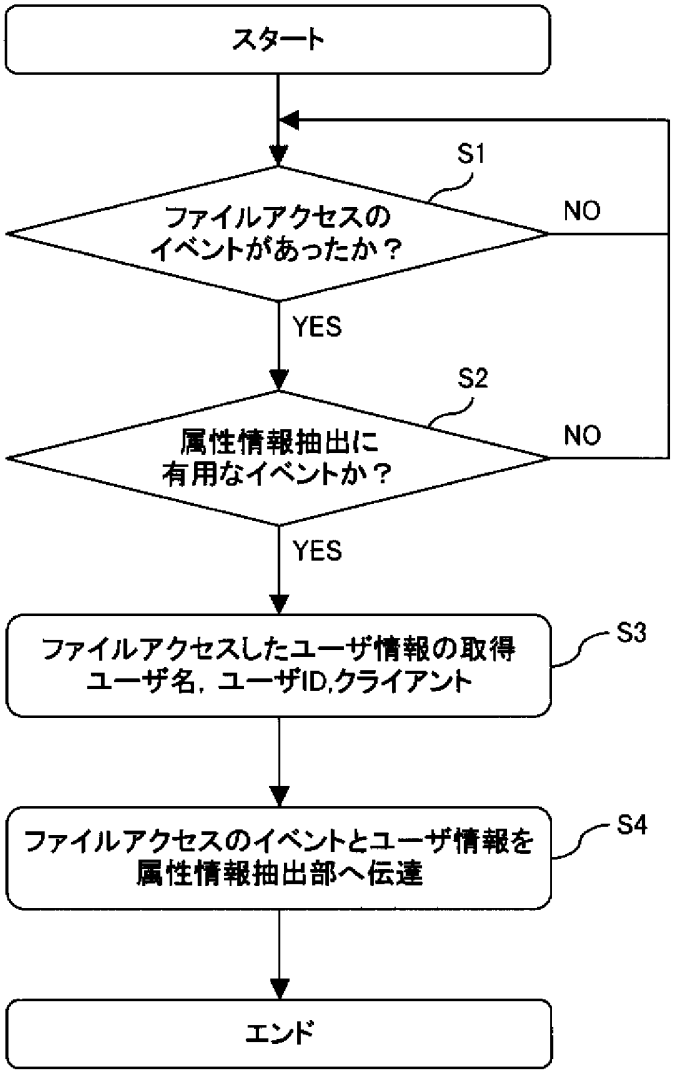
[図3]


バス
24
23
CPU
20
ROM
21
RAM
22
I/O
ネットワーク
12
ユーザ
インタフェース
14
外部
記憶
装置
13
11
ファイル共有サーバ

[図4]


10
クライアント
(ファイルアクセス)
10
クライアント
(ファイルアクセス)
10
クライアント
(ファイルアクセス)
26
LAN
11
ファイル共有サーバ
ファイルアクセス監視部
30
32
属性情報管理部
(属性情報データベース)
属性情報抽出部
ユーザ特定部
35
31
36
ACL
ACL判定部
37
属性情報出力部
ユーザ特定部
35
33
ACL設定および取得部
ユーザ特定部
35
34
属性情報データベース
38
ファイルAの属性情報
ユーザα
ユーザβ
ユーザγ
属性1
属性2
属性3
属性4
属性5

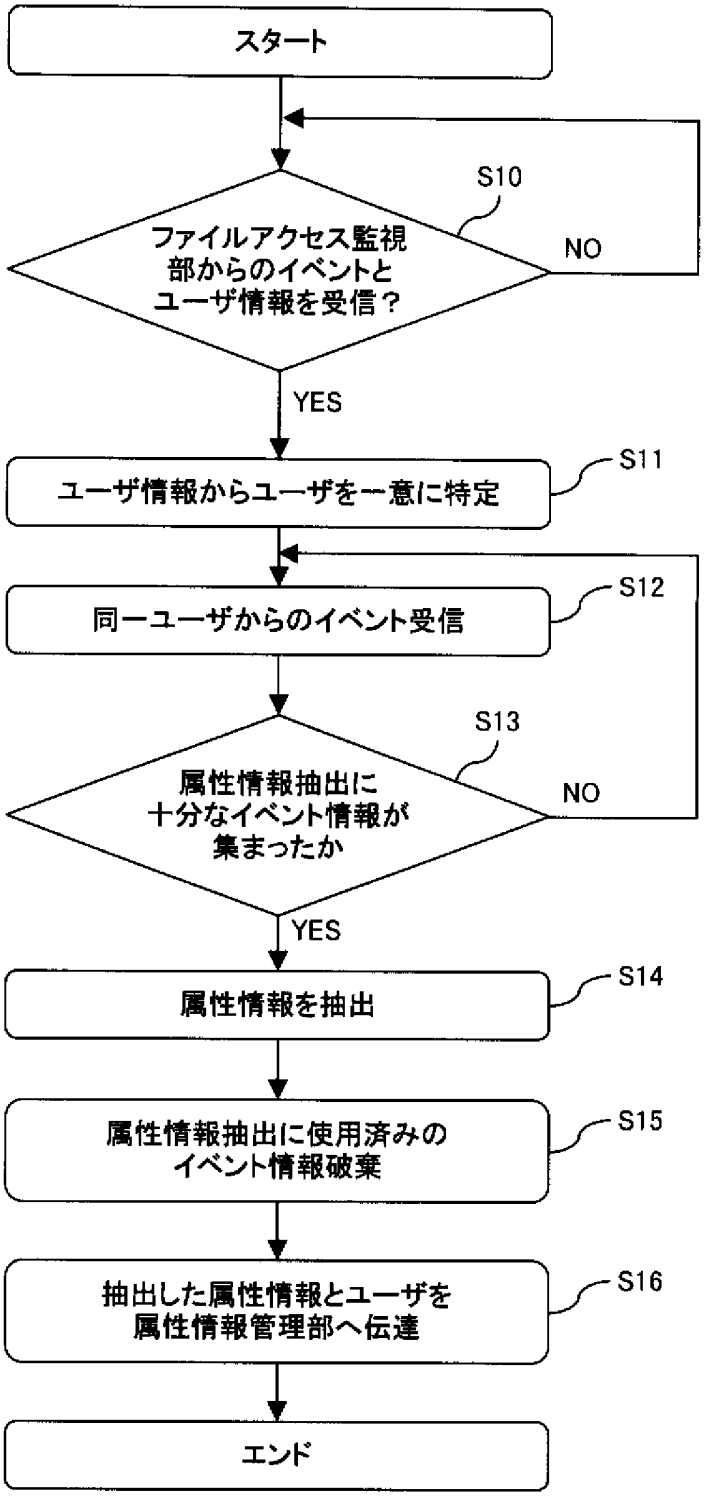
[図5]


スタート
S1
ファイルアクセスの
イベントがあったか？
NO
YES
S2
属性情報抽出に
有用なイベントか？
NO
YES
ファイルアクセスしたユーザ情報の取得
ユーザ名，ユーザID,クライアント
S3
ファイルアクセスのイベントとユーザ情報を
属性情報抽出部へ伝達
S4
エンド

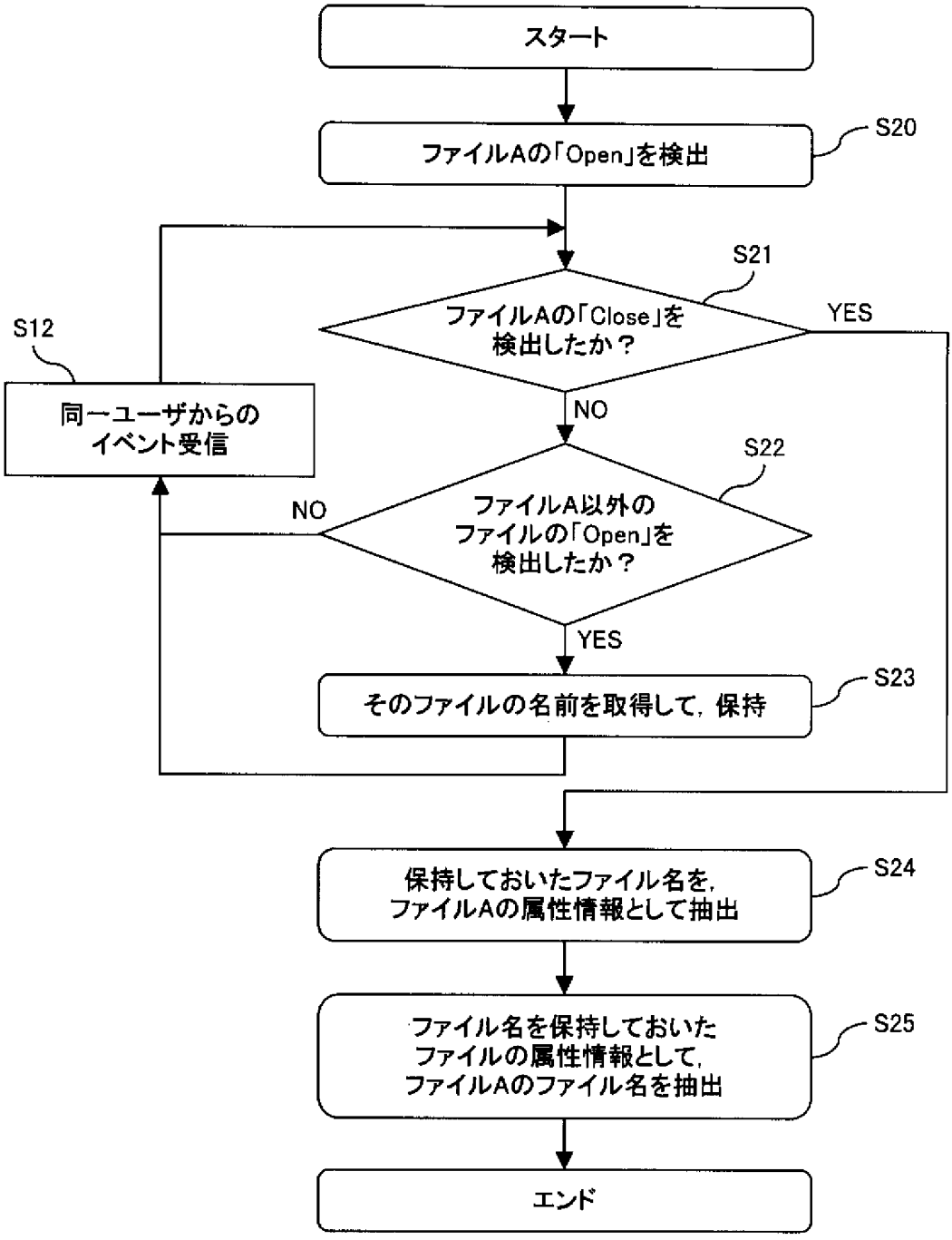
[図6]

処理対象特定ID	イベント種類	ユーザ名 or ID	クライアント名 or ID	イベント種類毎のパラメータ
28	Open	3328	Client A	ファイル名A, 処理開始時間など
28	Read	3328	Client A	無し
29	Open	3328	Client A	ファイル名B, 処理開始時間など
29	Write	3328	Client A	無し
30	Mkdir	3429	Client B	フォルダ名C, 処理完了時間など
29	Close	3328	Client A	処理完了時間など
31	unlink	3429	Client B	ファイル名D, 処理開始時間など
32	Rename	3429	Client B	旧ファイル名B', 新ファイル名B, 処理開始時間など
28	Close	3328	Client A	処理完了時間など
…	…	…	…	…

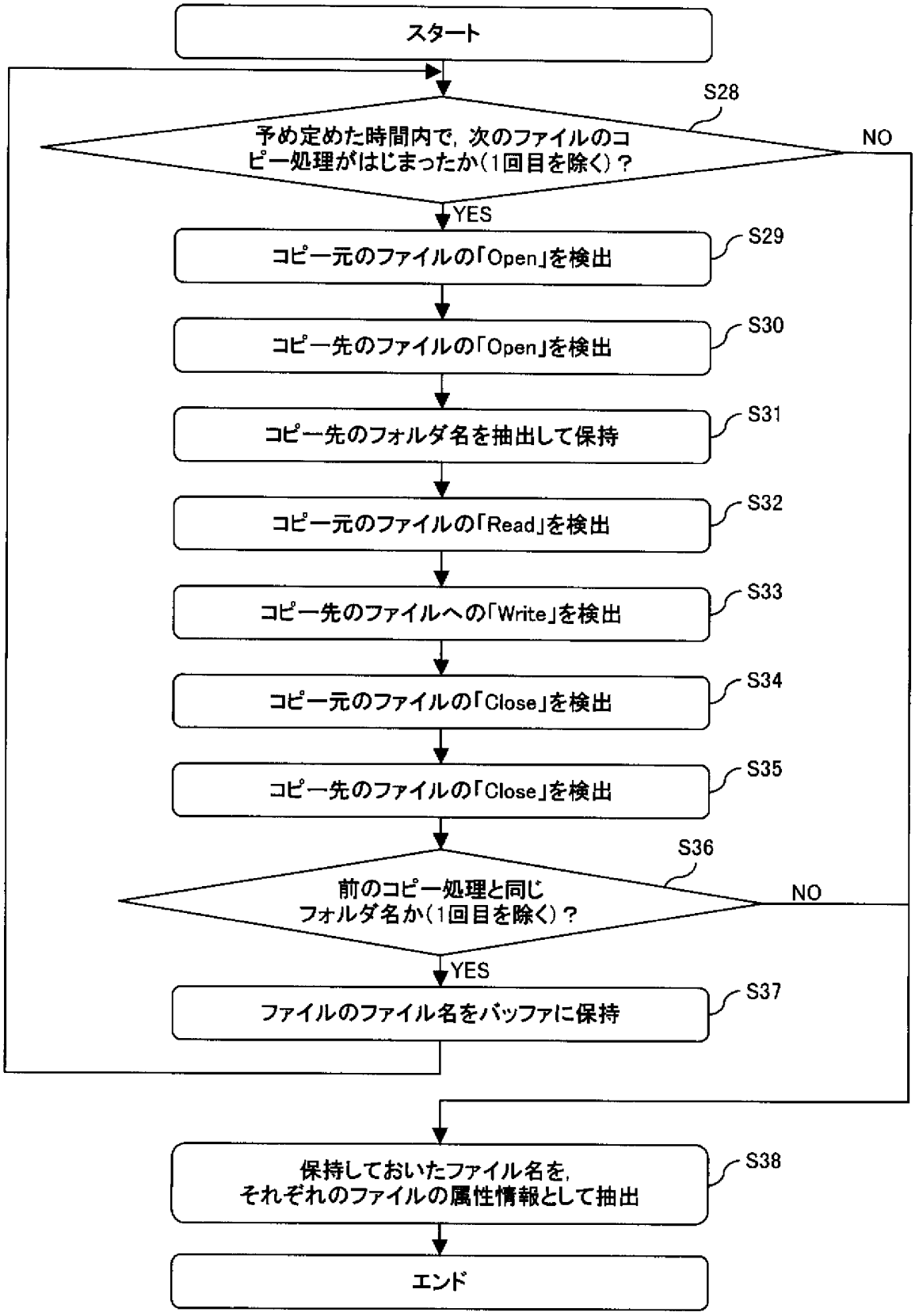
[図7]


スタート
S10
ファイルアクセス監視部からのイベントとユーザ情報を受信？
NO
YES
S11
ユーザ情報からユーザを一意に特定
S12
同一ユーザからのイベント受信
S13
属性情報抽出に十分なイベント情報が集まったか
NO
YES
S14
属性情報を抽出
S15
属性情報抽出に使用済みのイベント情報破棄
S16
抽出した属性情報とユーザを属性情報管理部へ伝達
エンド

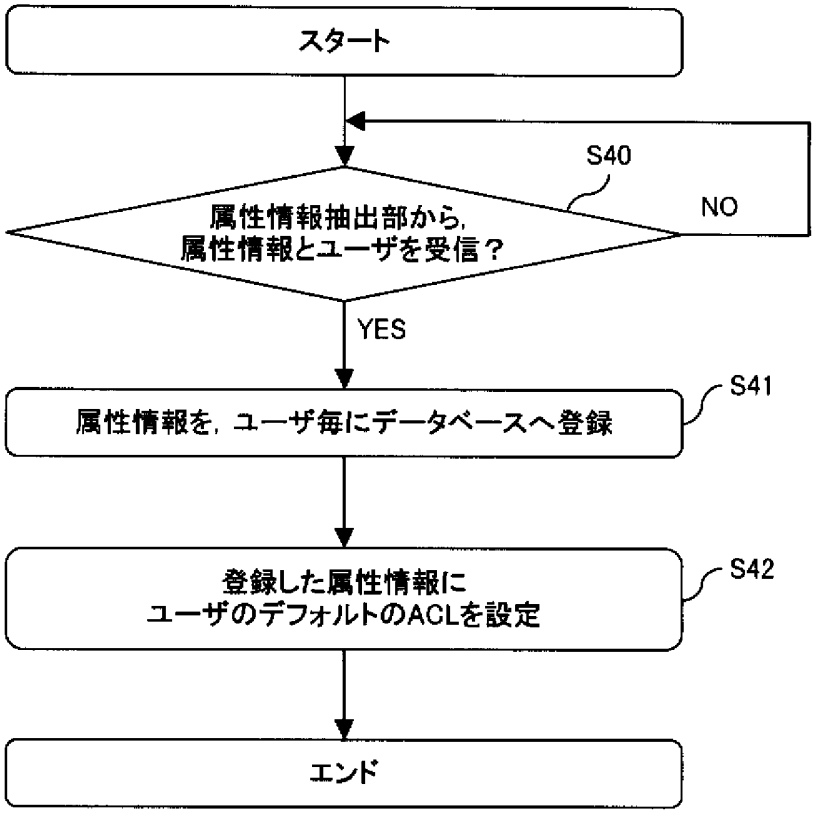
[図8]


スタート
ファイルAの「Open」を検出
S20
S21
ファイルAの「Close」を検出したか？
YES
NO
S12
同一ユーザからのイベント受信
S22
NO
ファイルA以外のファイルの「Open」を検出したか？
YES
そのファイルの名前を取得して，保持
S23
保持しておいたファイル名を，ファイルAの属性情報として抽出
S24
ファイル名を保持しておいたファイルの属性情報として，ファイルAのファイル名を抽出
S25
エンド

[図9]


スタート
S28
予め定めた時間内で，次のファイルのコピー処理がはじまったか(1回目を除く)？
NO
YES
S29
コピー元のファイルの「Open」を検出
S30
コピー先のファイルの「Open」を検出
S31
コピー先のフォルダ名を抽出して保持
S32
コピー元のファイルの「Read」を検出
S33
コピー先のファイルへの「Write」を検出
S34
コピー元のファイルの「Close」を検出
S35
コピー先のファイルの「Close」を検出
S36
前のコピー処理と同じフォルダ名か(1回目を除く)？
NO
YES
S37
ファイルのファイル名をバッファに保持
S38
保持しておいたファイル名を，それぞれのファイルの属性情報として抽出
エンド

[図10]


スタート
S40
属性情報抽出部から，
属性情報とユーザを受信？
NO
YES
S41
属性情報を，ユーザ毎にデータベースへ登録
S42
登録した属性情報に
ユーザのデフォルトのACLを設定
エンド

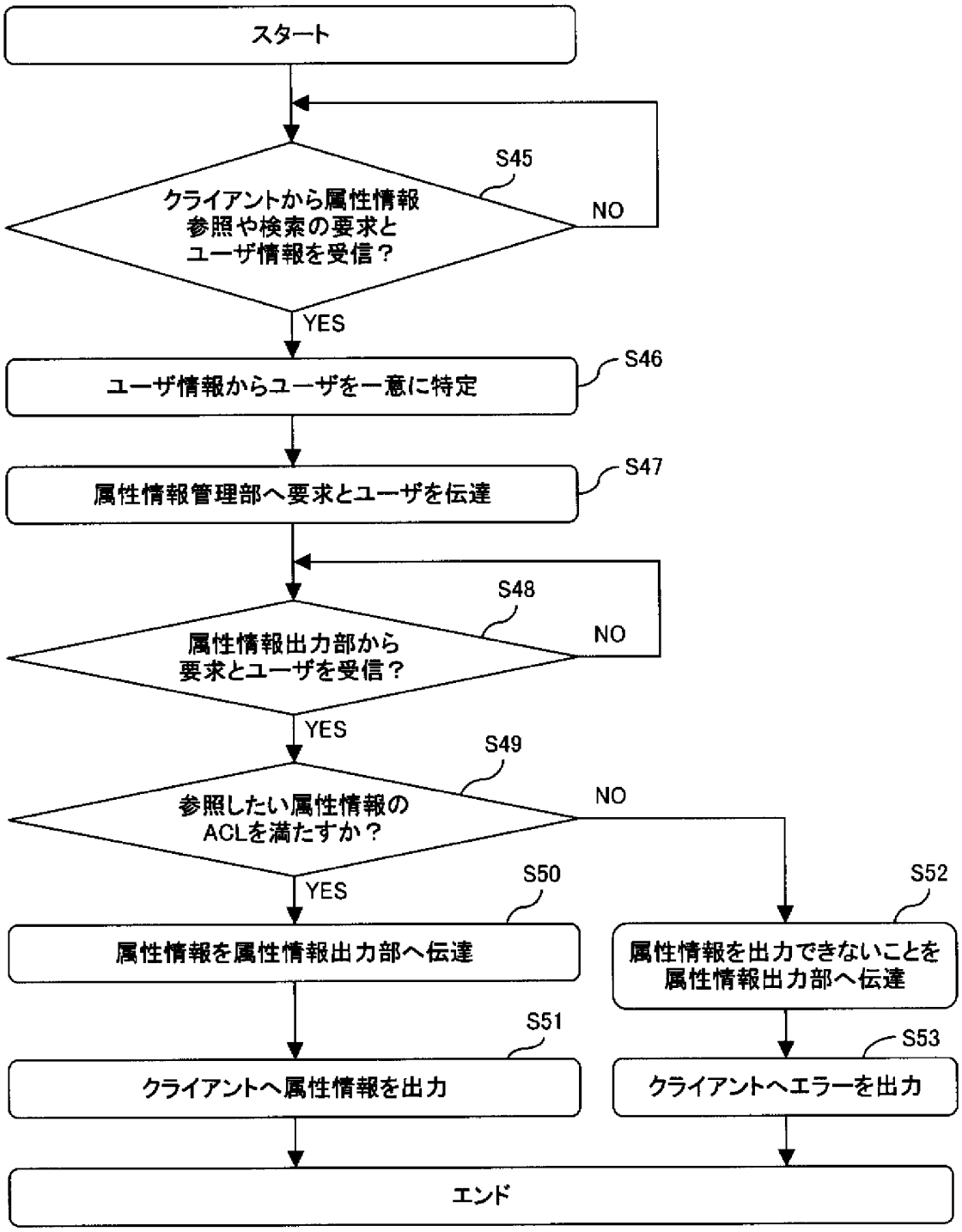
[図11]

ユーザ	各アクセス日時	各更新日時	作成日時	古いファイル名	同時参照ファイル	削除したか	…	ACL ID
…	…	…	…	…	…	…	…	…
Tarou	2004/08/30 22:59	-	-	ファイルB'-	-	-		Tarou-1
Tarou	2004/08/30 21:59	2004/08/30 21:59	-	-	ファイルA	-		Tarou-1
Tarou	2004/08/30 20:50	-	-	-	-	-		Tarou-2
Tarou	2004/08/30 20:30	-	-	-	-	-		Tarou-2
Akira	2004/08/24 17:15	2004/08/24 17:15	-	-	ファイルA	-		Akira-1
Akira	2004/08/15 11:00	-	-	-	-	-		Akira-2
Hanako	2004/08/15 10:00	2004/08/15 10:00	-	-	-	-		Hanako-1
Tarou	2004/08/13 10:00	-	-	-	ファイルA ファイルD	-		Tarou-2
Akira	2004/08/10 11:12	2004/08/10 11:12	2004/08/10 11:12	-	-	-		Akira-1

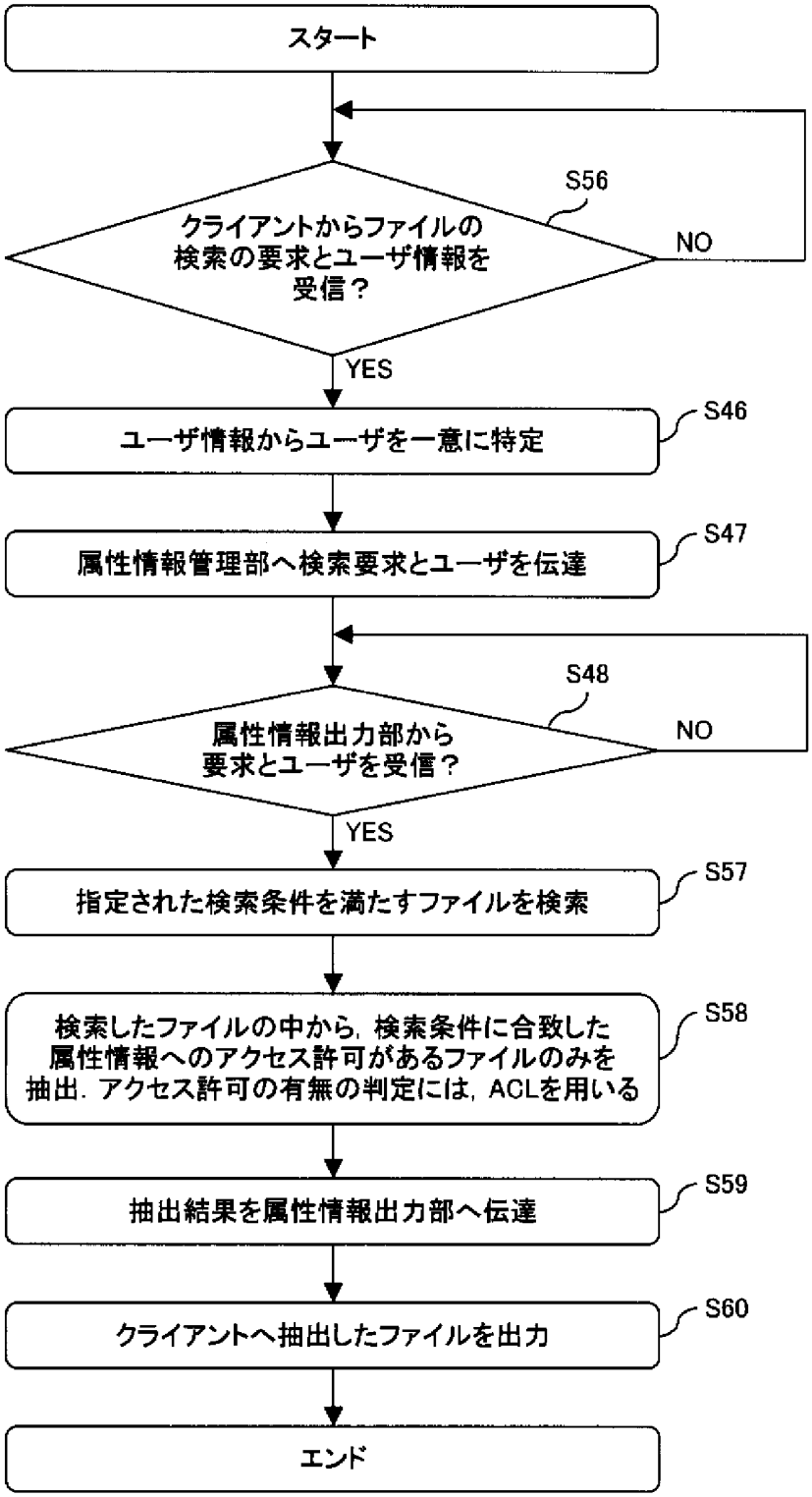
[図12]

ACL名	参照を許可するユーザ	参照を拒否するユーザ	変更可能なユーザ	デフォルトかどうかのフラグ
Tarou-1	all	none	all	1(デフォルト)
Tarou-2	Tarou Hanako	all	Tarou	0
…	…	…	…	…

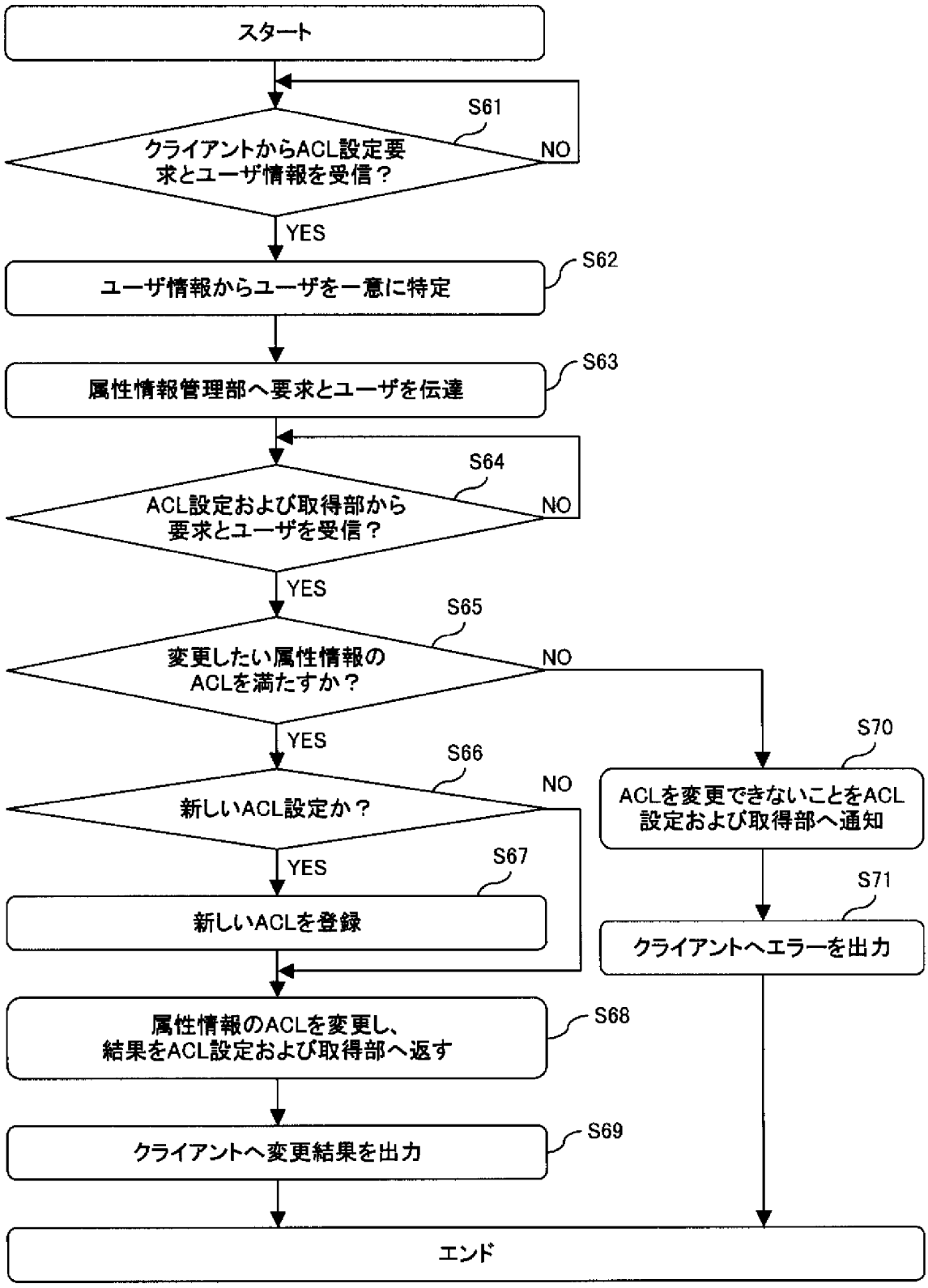
[図13]


スタート
S45
クライアントから属性情報
参照や検索の要求と
ユーザ情報を受信？
NO
YES
S46
ユーザ情報からユーザを一意に特定
S47
属性情報管理部へ要求とユーザを伝達
S48
属性情報出力部から
要求とユーザを受信？
NO
YES
S49
参照したい属性情報の
ACLを満たすか？
NO
YES
S50
属性情報を属性情報出力部へ伝達
S51
クライアントへ属性情報を出力
S52
属性情報を出力できないことを
属性情報出力部へ伝達
S53
クライアントへエラーを出力
エンド

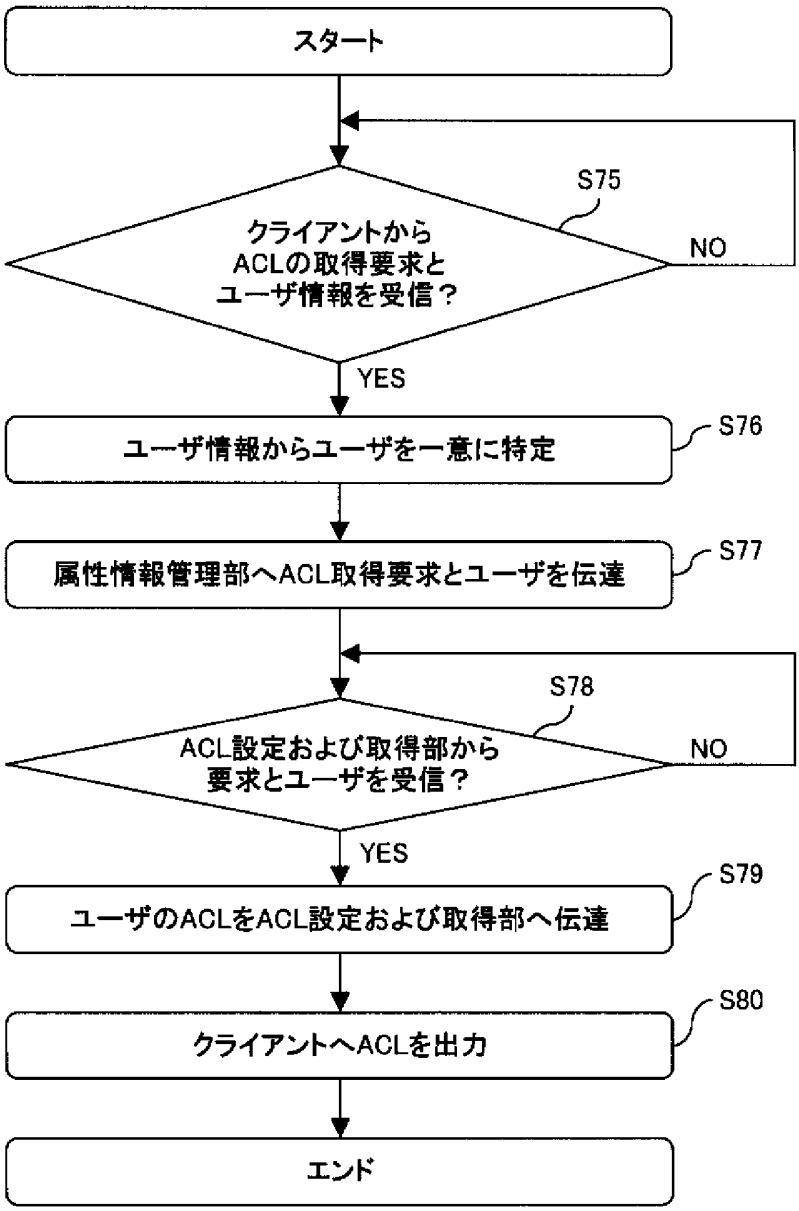
[図14]


スタート
S56
クライアントからファイルの
検索の要求とユーザ情報を
受信？
NO
YES
S46
ユーザ情報からユーザを一意に特定
S47
属性情報管理部へ検索要求とユーザを伝達
S48
属性情報出力部から
要求とユーザを受信？
NO
YES
S57
指定された検索条件を満たすファイルを検索
S58
検索したファイルの中から，検索条件に合致した
属性情報へのアクセス許可があるファイルのみを
抽出．アクセス許可の有無の判定には，ACLを用いる
S59
抽出結果を属性情報出力部へ伝達
S60
クライアントへ抽出したファイルを出力
エンド

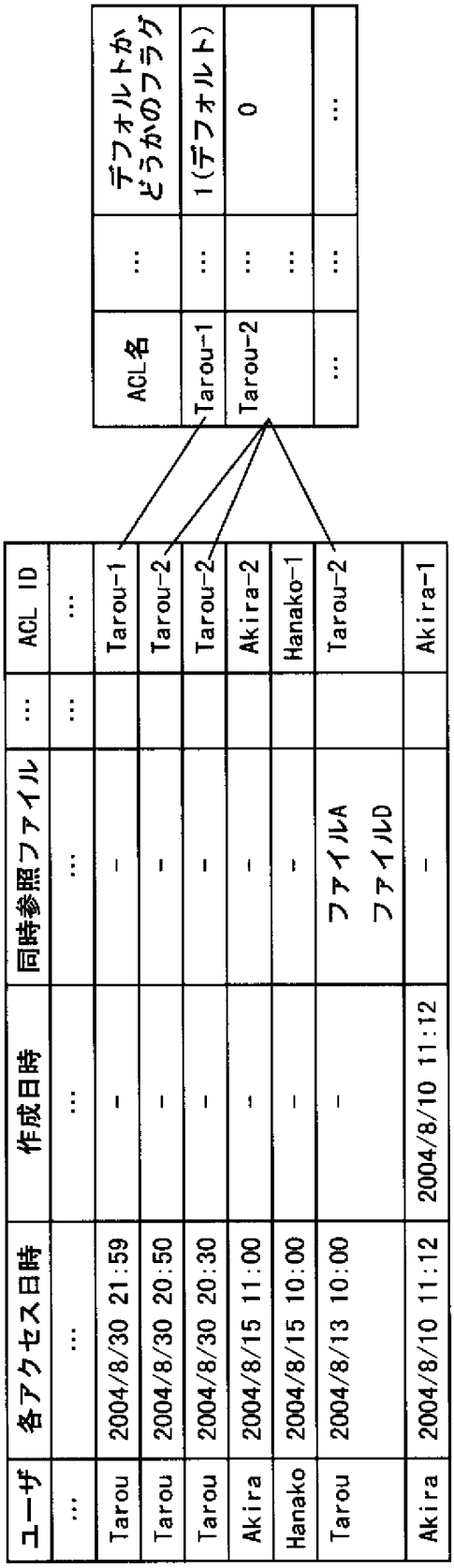
[図15]


スタート
S61
クライアントからACL設定要求とユーザ情報を受信？
NO
YES
S62
ユーザ情報からユーザを一意に特定
S63
属性情報管理部へ要求とユーザを伝達
S64
ACL設定および取得部から要求とユーザを受信？
NO
YES
S65
変更したい属性情報のACLを満たすか？
NO
YES
S66
新しいACL設定か？
NO
YES
S67
新しいACLを登録
S68
属性情報のACLを変更し、結果をACL設定および取得部へ返す
S69
クライアントへ変更結果を出力
S70
ACLを変更できないことをACL設定および取得部へ通知
S71
クライアントへエラーを出力
エンド

[図16]


スタート
S75
クライアントから
ACLの取得要求と
ユーザ情報を受信？
NO
YES
ユーザ情報からユーザを一意に特定
S76
属性情報管理部へACL取得要求とユーザを伝達
S77
S78
ACL設定および取得部から
要求とユーザを受信？
NO
YES
ユーザのACLをACL設定および取得部へ伝達
S79
クライアントへACLを出力
S80
エンド

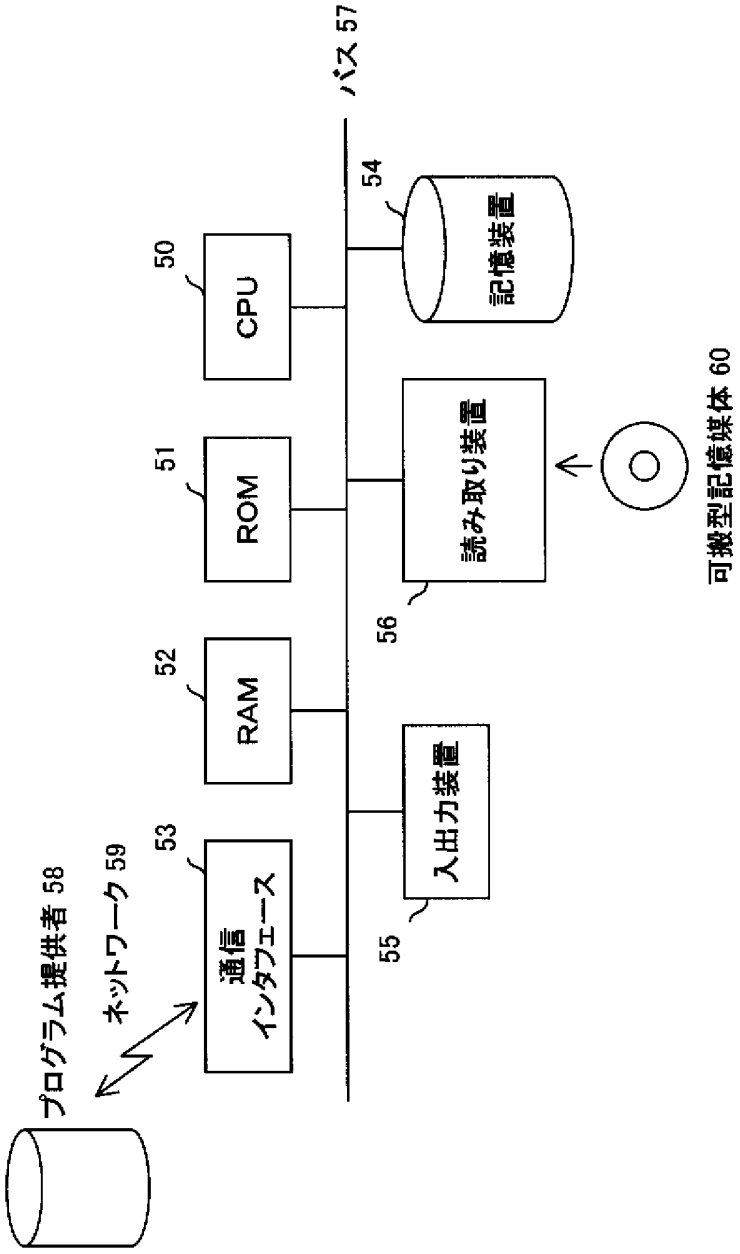
[図17]



ユーザ	各アクセス日時	作成日時	同時参照ファイル	…	ACL ID
…	…	…	…	…	…
Tarou	2004/8/30 21:59	–	–		Tarou-1
Tarou	2004/8/30 20:50	–	–		Tarou-2
Tarou	2004/8/30 20:30	–	–		Tarou-2
Akira	2004/8/15 11:00	–	–		Akira-2
Hanako	2004/8/15 10:00	–	–		Hanako-1
Tarou	2004/8/13 10:00	–	ファイルA ファイルD		Tarou-2
Akira	2004/8/10 11:12	2004/8/10 11:12	–		Akira-1

ACL名	…	デフォルトかどうかのフラグ
Tarou-1	…	1(デフォルト)
Tarou-2	…	0
…	…	…

[図18]


バス 57
CPU
50
ROM
51
RAM
52
通信
インタフェース
53
入出力装置
55
読み取り装置
56
記憶装置
54
可搬型記憶媒体 60
ネットワーク 59
プログラム提供者 58

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/019649

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G06F12/00, G06F17/30

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G06F12/00, G06F17/30

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2005
Kokai Jitsuyo Shinan Koho 1971-2005 Toroku Jitsuyo Shinan Koho 1994-2005

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP 2000-172696 A (Toshiba Corp.), 23 June, 2000 (23.06.00), Abstract; Par Nos. [0005], [0016] to [0017]; Fig. 2 (Family: none)	1-12
A	JP 6-342451 A (NEC Corp.), 13 December, 1994 (13.12.94), Par Nos. [0008] to [0009] (Family: none)	1-12
A	WO 2002/065295 A1 (TDK Corp.), 22 August, 2002 (22.08.02), Abstract & JP 2002-244902 A	1-12

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is notconsidered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
28 January, 2005 (28.01.05)	15 February, 2005 (15.02.05)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

国際調査報告

国際出願番号　PCT／JP2004／019649

A.　発明の属する分野の分類（国際特許分類（IPC））

Int.Cl[7]　G06F12/00,　G06F17/30

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int.Cl[7]　G06F12/00,　G06F17/30

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922－1996年
日本国公開実用新案公報	1971－2005年
日本国実用新案登録公報	1996－2005年
日本国登録実用新案公報	1994－2005年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X	JP　2000－172696　A（株式会社東芝） 2000.06.23，要約，段落【0005】， 段落【0016】－【0017】，第2図（ファミリーなし）	1－12
A	JP　6－342451　A（日本電気株式会社） 1994.12.13，段落【0008】－【0009】 （ファミリーなし）	1－12

☒ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日 28.01.2005	国際調査報告の発送日 15.2.2005
国際調査機関の名称及びあて先 日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官（権限のある職員） 平井　誠　5N　9071 電話番号　03－3581－1101　内線　3585

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００４／０１９６４９

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ａ	ＷＯ　２００２／０６５２９５　Ａ１ （ティーディーケイ株式会社）２００２．０８．２２，　要約 ＆　ＪＰ　２００２－２４４９０２　Ａ	１－１２