

(19) 日本国特許庁(JP)

(12) 公表特許公報(A)

(11) 特許出願公表番号

特表2004-523826

(P2004-523826A)

(43) 公表日 平成16年8月5日(2004.8.5)

(51) Int.Cl.⁷

G06F 12/00

G06F 12/14

F I

G06F 12/00 537M

G06F 12/14 310K

テーマコード (参考)

5B017

5B082

審査請求 未請求 予備審査請求 未請求 (全 46 頁)

(21) 出願番号 特願2002-558113 (P2002-558113)
 (86) (22) 出願日 平成14年1月16日 (2002.1.16)
 (85) 翻訳文提出日 平成15年7月16日 (2003.7.16)
 (86) 国際出願番号 PCT/US2002/001335
 (87) 国際公開番号 W02002/057895
 (87) 国際公開日 平成14年7月25日 (2002.7.25)
 (31) 優先権主張番号 09/760,999
 (32) 優先日 平成13年1月16日 (2001.1.16)
 (33) 優先権主張国 米国 (US)

(71) 出願人 390041542
 ゼネラル・エレクトリック・カンパニイ
 GENERAL ELECTRIC CO
 MPANY
 アメリカ合衆国、ニューヨーク州、スケネ
 クタデイ、リバーロード、1 番
 (74) 代理人 100093908
 弁理士 松本 研一
 (74) 代理人 100105588
 弁理士 小倉 博
 (74) 代理人 100106541
 弁理士 伊藤 信和

最終頁に続く

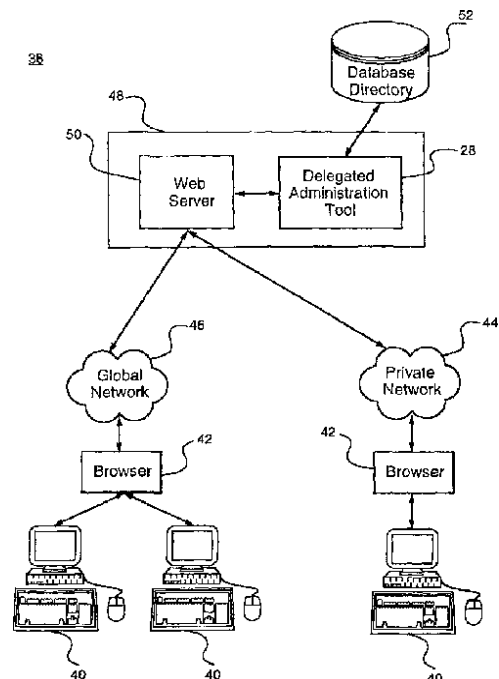
(54) 【発明の名称】 属性許可を用いたデータベースディレクトリの情報の委託管理

(57) 【要約】

【課題】 データベースディレクトリの情報の委託管理方法を提供する。

【解決手段】 属性許可を利用してデータベースディレクトリ (52) 内の情報を管理する委託管理ツール (28)。委託管理ツール28によって、管理者は、ユーザ属性で実行できる、また、実行できない管理オペレーションを規定するユーザ属性許可をもつ管理領域とサブ領域を形成することができる。また、委託管理ツール (28) によって、管理者は、ユーザ属性に割り当てるための限定値を規定することができる。

【選択図】 図5



【特許請求の範囲】**【請求項 1】**

ユーザコミュニティを管理する方法であって、
前記ユーザコミュニティ内の各ユーザに対する一連のユーザ属性を規定する工程と、
前記ユーザ属性の各々を管理する許可レベルを特定する工程を備える方法。

【請求項 2】

各許可レベルは、特定のユーザ属性で管理者が実施可能な管理オペレーションと実施不可能な管理オペレーションを規定するものである、請求項 1 の方法。

【請求項 3】

管理者が前記ユーザ属性に割り当て可能な限定値を規定する工程をさらに備える、請求項 10 1 の方法。

【請求項 4】

ユーザコミュニティに関するユーザ情報を管理する方法であって、
前記ユーザコミュニティの各ユーザのユーザ情報から一連のユーザ属性を規定する工程と、
前記ユーザ属性の各々に対する許可レベルを特定する工程と、
前記許可レベルの各々に基づいて前記ユーザ属性を管理する工程を備える方法。

【請求項 5】

各許可レベルは、管理者が特定のユーザ属性で実施可能なオペレーションと実施不可能なオペレーションを規定するものである、請求項 4 の方法。 20

【請求項 6】

管理者が前記ユーザ属性のいずれかに割り当て可能な限定値を規定する工程をさらに備える、請求項 4 の方法。

【請求項 7】

管理者がユーザコミュニティの管理を制御することができる方法であって、
前記ユーザコミュニティに関するユーザ情報を前記管理者に提供する工程と、
前記ユーザコミュニティ内の各ユーザのためにの一連のユーザ属性を規定するように前記管理者に促す工程と、
前記ユーザ属性の各々に対する許可レベルを特定するように前記管理者を促す工程と、
特定された許可レベルを利用して、前記ユーザ情報の管理を制御する工程を備える方法。 30

【請求項 8】

各許可レベルは、前記管理者がユーザ属性に関して実施可能なオペレーションと実施不可能なオペレーションを規定するものである、請求項 7 の方法。

【請求項 9】

前記管理者が前記ユーザ属性のいずれかに対して割り当て可能な限定値を規定するように前記管理者を促す工程をさらに備える、請求項 7 の方法。

【請求項 10】

ユーザコミュニティに関するユーザ情報を管理するためのユーザコミュニティ管理ツールであって、
前記ユーザコミュニティを少なくとも 1 つの管理領域に規定する領域規定コンポーネント 40
であって、前記ユーザコミュニティから少なくとも 1 つの任意のユーザグループを特定するユーザグループ特定コンポーネントと、前記少なくとも 1 つの任意のユーザグループに対して許容可能な一連のユーザ属性を規定するユーザ属性規定コンポーネントを備える、当該領域規定コンポーネントと、
前記許容可能なユーザ属性に基づいて前記管理領域に関するユーザ情報を管理する情報管理コンポーネントを備える、ユーザコミュニティ管理ツール。

【請求項 11】

前記ユーザ属性規定コンポーネントは、前記ユーザ属性の各々に対する許可レベルを特定する属性許可コンポーネントを備える、請求項 10 のツール。

【請求項 12】

各許可レベルは、管理者が特定のユーザ属性に関して実施可能なオペレーションと実施不可能なオペレーションを規定するものである、請求項 11 のツール。

【請求項 13】

前記ユーザ属性規定コンポーネントは、管理者が前記ユーザ属性のうちのいずれかに割り当て可能な限定値を規定する属性限定値コンポーネントを備える、請求項 10 のツール。

【請求項 14】

前記管理領域に対する管理特権を付与する管理特権コンポーネントをさらに備える、請求項 10 のツール。

【請求項 15】

前記管理特権コンポーネントは、前記管理領域に対して、付与された管理特権を委託する、請求項 14 のツール。 10

【請求項 16】

ユーザコミュニティに関するユーザ情報を管理するシステムであって、複数のユーザ情報を含むデータベースディレクトリと、前記データベースディレクトリ内の前記複数のユーザ情報を管理するユーザコミュニティ管理ツールであって、前記ユーザコミュニティ管理ツールは、前記ユーザコミュニティを少なくとも 1 つの管理領域に規定する領域規定コンポーネントを備え、前記領域規定コンポーネントは、前記ユーザコミュニティから少なくとも 1 つの任意のユーザグループを特定するユーザグループ特定コンポーネントと、前記少なくとも 1 つの任意のユーザグループに対する許容可能な一連のユーザ属性を規定するユーザ属性規定コンポーネントと、前記許容可能なユーザ属性に基づいて前記管理領域に関連するユーザ情報を管理する情報管理コンポーネントを備える、当該ユーザコミュニティ管理ツールと、前記ユーザコミュニティ管理ツールと前記データベースディレクトリを提供するように構成された第 1 の計算部を備えるシステム。 20

【請求項 17】

ネットワークを介して前記第 1 の計算部から提供されたユーザコミュニティ管理ツールを実行するように構成された第 2 の計算部をさらに備える、請求項 16 のシステム。

【請求項 18】

前記ユーザ属性規定コンポーネントは、前記ユーザ属性の各々に対する許可レベルを特定する属性許可コンポーネントを備える、請求項 16 のシステム。 30

【請求項 19】

各許可レベルは、管理者が特定のユーザ属性に関して実施可能なオペレーションと実施不可能なオペレーションを規定するものである、請求項 18 のシステム。

【請求項 20】

前記ユーザ属性規定コンポーネントは、管理者が前記ユーザ属性に割り当て可能な限定値を規定する属性限定値コンポーネントを備える、請求項 16 のシステム。

【請求項 21】

ユーザコミュニティの管理を可能にするユーザコミュニティ管理ツールであって、前記ユーザコミュニティを少なくとも 1 つの管理領域に規定する手段であって、前記ユーザコミュニティから少なくとも 1 つの任意のユーザグループを特定する手段と、前記少なくとも 1 つの任意のユーザグループに対して許容可能な一連のユーザ属性を規定する手段を含む、当該管理領域に規定する手段と、前記許容可能なユーザ属性に基づいて前記管理領域に関連するユーザ情報を管理する手段を備えるユーザコミュニティ管理ツール。 40

【請求項 22】

前記ユーザ属性規定手段は、前記ユーザ属性の各々に対する許可レベルを特定する手段を含む、請求項 21 のツール。

【請求項 23】

各許可レベルは、管理者がユーザ属性に関して実施可能なオペレーションと実施不可能なオペレーションを規定するものである、請求項 22 のツール。 50

【請求項 2 4】

前記ユーザ属性規定手段は、管理者が前記ユーザ属性に割り当て可能な限定値を規定する手段を含む、請求項 2 1 のツール。

【請求項 2 5】

ユーザコミュニティを管理するようにコンピュータシステムを指示するコンピュータ命令を記憶するコンピュータ読取可能媒体であって、前記コンピュータ命令は、前記ユーザコミュニティ内の各ユーザに対して一連のユーザ属性を規定し、前記ユーザ属性の各々を管理するための許可レベルを特定することを備える、コンピュータ読取可能媒体。

【請求項 2 6】

各許可レベルは、管理者が特定のユーザ属性に関して実施可能なオペレーションと実施不可能なオペレーションを規定するものである、請求項 2 5 のコンピュータ読取可能媒体。

【請求項 2 7】

管理者が前記ユーザ属性に割り当て可能な限定値を規定する命令をさらに備える、請求項 2 5 のコンピュータ読取可能媒体。

【請求項 2 8】

管理者がユーザコミュニティの管理を制御できるようにコンピュータシステムを指示するコンピュータ命令を記憶するコンピュータ読取可能媒体であって、前記コンピュータ命令は、

前記ユーザコミュニティに関するユーザ情報を前記管理者に提供し、

前記ユーザコミュニティ内の各ユーザに対する一連のユーザ属性を規定するように前記管理者に促し、

前記ユーザ属性の各々に対する許可レベルを特定するように前記管理者を促し、

特定された許可レベルを利用して前記ユーザ情報の管理を制御することを含む、コンピュータ読取可能媒体。

【請求項 2 9】

各許可レベルは、前記管理者がユーザ属性に関して実施可能なオペレーションと実施不可能なオペレーションを規定するものである、請求項 2 8 のコンピュータ読取可能媒体。

【請求項 3 0】

前記ユーザ属性に割り当て可能な限定値を規定するように前記管理者を促す命令をさらに含む、請求項 2 8 のコンピュータ読取可能媒体。

【発明の詳細な説明】

【技術分野】

【0 0 0 1】

本開示は一般的にコミュニティベースのコンピュータサービスに関し、特に、属性許可を使ったコミュニティベースのコンピュータサービスの管理に関する。

【背景技術】

【0 0 0 2】

一般にコミュニティとは、通常、共通の活動を共有する人々の集まりである。インターネットと電子商取引の出現により、多くの企業が、イントラネットやエキストラネットを介して例えば従業員やサプライヤやパートナーや顧客といったコミュニティを形成している。コミュニティによって、従業員とサプライヤとパートナーと顧客は簡単に低コストで協同作業することができる。コンピュータサービスの分野では、そのような人々はコンピュータユーザもしくは単にユーザとして知られている。コミュニティ内の各ユーザに関する情報は、広範囲に渡るディレクトリやデータベースに格納されている。この情報には、ユーザの名前や所在地や電話番号や組織名やログイン ID やパスワードなどの項目が含まれることがある。その他の情報には、アプリケーションやコンテンツといったリソースへのユーザのアクセス特権が含まれることもある。またディレクトリには、コミュニティをサポートするネットワーク内の物理的装置（例えば、パーソナルコンピュータやサーバやプリンタやルータやコミュニケーションサーバなど）に関する情報を格納することができる。その

10

20

30

40

50

他の情報には、各物理的装置から使用可能なサービス（例えば、オペレーティングシステムやアプリケーションや共有ファイルシステムや印刷キューなど）が含まれていてもよい。一般的に、上記の全情報がコミュニティベースのコンピュータサービスとして知られている。

【0003】

このようなコミュニティベースのコンピュータサービスの管理（即ち、生成と保守と修正と更新とディスエーブル化）は、コミュニティが大規模になり複雑になるにつれて困難になる。多くの場合、管理は、コミュニティをより管理しやすいサブコミュニティに細分しない限りほとんど実施不可能なタスクである。こうしたサブコミュニティを生成した場合、サブコミュニティの管理に個別の人を割り当て、コミュニティ管理を分担する管理者チームを活用することが望ましくなる。このような管理を委託管理と呼ぶ。 10

【0004】

委託管理を容易にする現在使用可能な管理ツールには欠点がある。このようなツールには、例えば、ユーザ情報に対して管理者がどのようなオペレーションを行えるかを限定する機能が備わっていない。一般的な例を1つ挙げると、管理者はユーザのパスワードをリセットできるが、既存のパスワードを閲覧することはできない場合がある。この例では、ある種のオペレーション（新しいパスワードを設定すること）はできるが、別のオペレーション（既存のパスワードを閲覧すること）は行なえない。データを可能な限り保護するためには、最低限の許可（即ち、オペレーション）を与えることが重要である。また、現在利用可能な管理ツールでは、ユーザ情報に関するデータフィールドに対して管理者の割り 20
当て可能な値を限定する機能が備わっていない。例えば、ユーザディレクトリ内には、（ウェブベースのアプリケーションへのアクセスを許可する）ユーザアクセス許可を記憶するために使用されるデータフィールドがある場合が多い。一般に、このようなデータフィールド値は、許容値のリスト（列挙リスト）からなり、そのリストからの値のみが入力されるはずである。そのような列挙リスト内の値だけに値を制限することによって、間違いや入力エラーを抑えることができる。

【発明の開示】

【発明が解決しようとする課題】

【0005】

従って、ユーザ情報に対して管理者がどのようなオペレーションを行うことができるかを 30
限定する機能を提供することによって、管理者が行えることを制限できる管理ツールが必要である。また、入力可能なデータ値を限定すると共にそのデータの正確さを保証するために管理者がユーザ情報に対して割り当て可能な値を限定する機能を提供する管理ツールも求められている。

【課題を解決するための手段】

【0006】

本開示の一実施形態には、ユーザコミュニティを管理するようにコンピュータシステムを指示する方法とシステムと、その命令を記憶するコンピュータ読取可能媒体がある。本実施形態では、ユーザコミュニティ内の各ユーザに対する一連のユーザ属性が規定される。次に、各ユーザ属性を管理するための許可レベルが特定される。 40

【0007】

本開示の第2の実施形態には、管理者がユーザコミュニティの管理を制御できるようにコンピュータシステムを指示するシステムと方法と、その命令を記憶するコンピュータ読取可能媒体がある。本実施形態では、ユーザコミュニティに関するユーザ情報が管理者に提供される。管理者は、ユーザコミュニティ内の各ユーザに対する一連のユーザ属性を規定するよう促される。管理者は、各ユーザ属性に対する許可レベルを特定するよう促される。特定された許可レベルは、ユーザ情報の管理を制御するために使用される。

【0008】

その他の一実施形態には、ユーザコミュニティに関するユーザ情報を管理するユーザコミュニティ管理ツールがある。ユーザコミュニティ管理ツールには、ユーザコミュニティを 50

少なくとも1つの管理領域に規定する領域規定コンポーネントがある。領域規定コンポーネントは、ユーザコミュニティから少なくとも1つの任意のユーザグループを特定するユーザグループ特定コンポーネントと、少なくとも1つの任意のユーザグループに対して許容できる一連のユーザ属性を規定するユーザ属性規定コンポーネントを備える。情報管理コンポーネントは、許容可能なユーザ属性に基づいて管理領域に関するユーザ情報を管理する。

【0009】

その他の実施形態には、ユーザコミュニティに関するユーザ情報を管理するシステムがある。このシステムは、複数のユーザ情報を格納するデータベースディレクトリを備える。ユーザコミュニティ管理ツールは、データベースディレクトリ内の複数のユーザ情報を管理する。ユーザコミュニティ管理ツールは、ユーザコミュニティを少なくとも1つの管理領域に規定する領域規定コンポーネントを備える。領域規定コンポーネントは、ユーザコミュニティから少なくとも1つの任意のユーザグループを特定するユーザグループ特定コンポーネントと、少なくとも1つの任意のユーザグループに対して許容可能なユーザ属性のセットを規定するユーザ属性規定コンポーネントを備える。情報管理コンポーネントは、許容可能なユーザ属性に基づいて管理領域に関するユーザ情報を管理する。計算部は、ユーザコミュニティ管理ツールとデータベースディレクトリを提供するように構成される。

10

【発明を実施するための最良の形態】

【0010】

図1は、医療サービスプロバイダからコミュニティサービスを受けるユーザコミュニティの一例を示す概略図である。図1に示された例は、ユーザコミュニティの概念の例示したものであって、本開示を限定するものではない。図1では、健康管理プロバイダA～Dは、医療サービスプロバイダXからのコンピュータによるサービスを受けるコミュニティである。このようなコンピュータサービスの例には、医療情報と、医療用補給品の注文と、患者の予約と、患者用サービスの請求が含まれていてもよい。この場合のコンピュータサービスにおけるその他の例には、ベンチマーク情報と健康管理統計データと、ダウンロード可能なソフトウェアへのアクセスが含まれることもある。また、健康管理プロバイダは、コンピュータによるサービスを、顧客やパートナやベンダやサプライヤなどにも提供したいかもしれない。図1では、健康管理プロバイダBは、医療サービスプロバイダXによって確立されたコンピュータサービスを、関係のある地域の診療所と地域の病院に提供する。このコンピュータサービスは、従業員にも提供することができる。図1では、コンピュータサービスは、心臓や放射線や胃腸病や医療研究などの地域の病院内の様々な医療科に提供される。他の健康管理プロバイダ（即ち、健康管理プロバイダA、C、D）に対しても同様なコンピュータサービスの配信を行うことができる。

20

30

【0011】

医療サービスプロバイダXは、コミュニティ内の各ユーザに関する情報をデータベースのディレクトリに記憶する。この情報には、ユーザの名前や所在地や電話番号や組織名やログインIDやパスワードなどの項目が含まれてもよい。さらに別の情報には、医療サービスプロバイダXが提供する、アプリケーションやコンテンツなどのリソースに対するユーザのアクセス特権が含まれてもよい。医療サービスプロバイダのデータベースディレクトリには、コミュニティをサポートするネットワーク内の物理的な装置（例えば、パーソナルコンピュータやサーバやプリンタやルータや通信サーバなど）に関する情報を格納することもできる。データベースディレクトリに格納されるその他の情報には、各物理的装置から利用可能なサービス（例えば、オペレーティングシステムやアプリケーションや共有ファイルシステムや印刷待ち行列など）が含まれていてもよい。

40

【0012】

図1に示されたユーザコミュニティはかなり大規模で複雑である可能性があるので、このようなコミュニティの管理を分割して委託することが望ましい。図2は、図1に示されたユーザコミュニティの委託管理の一例を示したものである。この例では、各コミュニティ

50

毎に様々なアクティビティ管理を担当する管理者がいる。アクティビティには、これに限定されることはないが、ユーザ情報の修正と、リソースへの許可更新と、ユーザアカウントのディスエーブル化と、ユーザアカウントの生成と、ユーザアカウントの管理が含まれる。例えば、上級管理者が医療サービスプロバイダXに関するアクティビティを管理し、管理者Aが健康管理プロバイダBと関連する地域診療所と地域の病院の心臓科に関するアクティビティを管理し、管理者Bが健康管理プロバイダA、Bに関するアクティビティを管理し、管理者Cが健康管理プロバイダDに関するアクティビティを管理し、管理者Dが健康管理プロバイダBと関連する地域の病院に関するアクティビティと、健康管理プロバイダBと関連する地域の病院の医療研究科に関するアクティビティと、健康管理プロバイダCに関するアクティビティを管理し、管理者Eが健康管理プロバイダBと関連する地域の病院の心臓科と放射線科に関するアクティビティを管理し、管理者Fが健康管理プロバイダBと関連する地域の病院の胃腸病科に関するアクティビティを管理する。管理者A～Fが管理するアクティビティの範囲は、管理者らが持つ権限の種類によって完全に決まる。当業者にとって明らかなことであるが、この例の委託管理は他の形態を採ることも可能である。

【0013】

本開示で提供される委託管理を説明するために、図2のユーザコミュニティ内の各ブロック（即ち、医療サービスプロバイダX、健康管理プロバイダA～D、地域の診療所、地域の病院、心臓科、放射線科、胃腸病科、医療研究科）は、管理領域を表わしている。管理領域は、管理される対象であり、対象には、一連のユーザのと、一連の修正可能なユーザ属性と、管理者権限のあるデータフィールドに対する許容可能な一連の値が含まれる。ユーザ属性の例には、これに限定されることはないが、雇用主と、任務／職務内容と、アクセス許可が付与されているリソースと、アドレスと、使用装置が含まれていてもよい。一般的に、管理者の権限には編集権限や委託権限が含まれていてもよい。管理者が特定のユーザの属性を編集する場合には、管理領域内の編集権限をもっている。管理者がサブ管理領域を生成するためにユーザのサブセットを規定し、修正する属性を特定する際は、管理者は管理領域内での委託権限を持っている。サブ管理領域を特定の者に割り当てることが、領域の委託である。サブ管理領域を生成してその領域をユーザに割り当てることができることが、委託権限である。本開示で説明した権限は一般的に編集権限と委託権限に関するものであるが、閲覧可能なデータ範囲に制限はあるものの、閲覧や修正や削除や一時的な委託やそれと同様のオペレーションなどのその他の種類の権限もあり得ることを当業者であれば理解することができる。さらに、このような例の権限を、委託権限と編集権限の代わりに利用したり、委託権限と編集権限と組合せて利用することもできる。

【0014】

上で触れたように、管理者がどのようなオペレーションを行え、どのようなオペレーションを行えないかを限定するユーザ属性許可を生成することが望ましい。例えば図2では、管理者は、ユーザに関する1つのデータフィールドを修正するための許可だけを必要としているかもしれない。この例として企業の給与部門をあげることができる。給与部門は、従業員の給与データのフィールドだけの修正が許されているべきである。

【0015】

さらに、ユーザ属性値を許容可能なサブセット値に限定することが望ましい。図2では、例えば、管理者は、ある1つの用途に対するユーザアクセス管理を担当している場合がある。そのユーザディレクトリには、ユーザがアクセス可能な全用途を規定するためのデータフィールドが含まれていてもよい。しかし、管理者は、1つの用途しか担当していないため、管理者は、ユーザに対してその用途に対して一つの値だけを設定することができるべきである。

【0016】

一例として、ユーザコミュニティに関する情報を管理するためにユーザ属性許可を生成する上述の委託管理の機能をソフトウェアで実施することができる。図3は、情報を管理するためにユーザ属性許可を生成する委託管理ツールが動作する汎用のコンピュータシステ

10

20

30

40

50

ム 10 の概略図を示したものである。一般的に、コンピュータシステム 10 は、少なくとも 1 個のプロセッサ 12 とメモリ 14 と入出力装置と、プロセッサとメモリと入出力装置を接続するデータ経路（例えば、バス）16 を備える。プロセッサ 12 は、メモリ 14 から命令とデータを受けとり、様々な計算を行なう。プロセッサ 12 は、算術論理演算を行なう論理演算装置（ALU）と、メモリ 14 から命令を抽出しその命令を解読し実行して、必要な時に ALU を呼び出す制御ユニットを備える。一般的に、メモリ 14 には、ランダムアクセスメモリ（RAM）とリードオンリメモリ（ROM）が含まれるが、プログラマブル読取専用メモリ（PROM）や消去可能プログラマブル読取専用メモリ（EPROM）や電気消去可能読取専用メモリ（EEPROM）などのその他の種類のメモリであってもよい。また、メモリ 14 には、プロセッサ 12 で実行するオペレーティングシステム 10 が含まれていることが好ましい。このオペレーティングシステムは、入力情報を認識し、出力情報を出力装置に送り、ファイルとディレクトリを管理し、様々な周辺装置を制御することを含む基本的なタスクを実行する。

【0017】

入出力装置には、コンピュータシステム 10 にデータと命令を入力するキーボード 18 とマウス 20 が含まれてもよい。また、ユーザは、ディスプレイ 22 を使ってコンピュータの実行内容を見ることができる。その他の出力装置としては、プリンタと、プロッタと、シンセサイザと、スピーカがあってもよい。イーサネットアダプタ（イーサネットは商標）やローカルエリアネットワーク（LAN）アダプタや統合サービスデジタル網（ISDN）アダプタやデジタル加入者回線（DSL）アダプタなどのネットワークカードやケーブルモデムや電話などの通信デバイス 24 によって、コンピュータシステム 10 は、LAN または広域ネットワーク（WAN）などのネットワーク上の他のコンピュータとリソースを利用することができる。コンピュータシステム 10 は、大容量記憶装置 26 を利用することによって大量のデータを永続的に保持することができる。大容量記憶装置には、フロッピーディスク（商標）やハードディスクや光ディスクなどの全ての種類のディスクドライブ、ならびに、デジタルオーディオテープ（DAT）やデジタルリニアテープ（DLT）や他の磁気符号化媒体が含まれていてもよいテープ上でデータの読み書きが可能なテープドライブが含まれてもよい。上述のコンピュータシステム 10 は、ハンドヘルドデジタルコンピュータや携帯情報端末やノートブックコンピュータやパーソナルコンピュータやワークステーションやミニコンピュータやメインフレームコンピュータやスーパーコンピュータかのいずれかの形態を採ることができる。

【0018】

図 4 は、図 3 に示されたコンピュータシステム 10 で動作し、情報を管理するためにユーザ属性許可を生成できる委託管理ツール 28 の最上位レベル・コンポーネントの構成を示した図である。委託管理ツール 28 は、ユーザコミュニティを規定して少なくとも 1 つの管理領域とする領域規定コンポーネント 30 を備える。領域規定コンポーネント 30 には、管理者がユーザコミュニティから少なくとも 1 つの任意のユーザグループを特定できるユーザグループ特定コンポーネント 31 が含まれる。ユーザグループ特定コンポーネント 31 は、管理者が構築した問合せ規則によって少なくとも 1 つの任意のユーザグループを形成し、ユーザ情報を含むデータベースディレクトリについての問合せを行うことができる。この問合せ規則によって、少なくとも 1 つの任意のユーザグループのユーザを規定する。例えば、図 2 を参照すると、管理者は、ユーザグループ特定コンポーネント 31 を使って、放射線専門医であるユーザから成る 1 つのグループと、健康管理プロバイダ B が雇用しているユーザから成る第 2 のグループと、ウィスコンシン州にいるユーザから成る第 3 のグループから 1 つの管理領域を形成することができる。

【0019】

特定された任意の各ユーザグループは、各ユーザに関する属性と、それらの属性に対する許容値を備える。ユーザ属性規定コンポーネント 33 によって、管理者は、少なくとも 1 つの任意のユーザグループに対して許容可能な一連のユーザ属性を規定することが可能になる。特に、規定された許容可能な一連のユーザ属性には、管理者がオペレーション可能

な属性が含まれる。ユーザ属性規定コンポーネント 33 には、管理者がユーザ属性ごとに許可レベルを特定できる属性許可コンポーネント 34 が含まれる。この許可レベルは、領域内で規定された属性の管理に関連する。これによって、同一のデータを管理する際に、様々な管理者が様々な許可を持つことが可能になる。特に、この許可レベルは、少なくとも 1 つの任意のユーザグループに関する属性に対してどのようなオペレーションが行えて、行えないのかを示すものである。管理者がユーザ属性に対して実施可能なオペレーションの中には、閲覧と編集と削除が含まれる。これらの管理オペレーションは、属性に対して実施可能なほんの少数のオペレーションを例示したものであり、その他の可能性を網羅するものではない。属性に対して実施可能なその他の例の管理オペレーションには、特定の期間での編集や、データフィールドをリセットしてデフォルト値にすることがある。管理者は属性許可コンポーネント 34 を利用し、これらのオペレーションのうちのいずれかを選択して、属性に対して何ができて何ができないのかを限定することができる。属性に対する許可を選択することは、管理領域を設定するユーザに任せられる。上のオペレーションのうちの 1 つだけ、もしくは、上のオペレーションの組み合わせを選択することができる。

【0020】

一例として図 2 を再び参照すると、管理者は、ウィスコンシン州にある健康管理プロバイダ B が雇用する放射線専門医を含む管理領域に対する属性許可コンポーネント 34 を利用して、特定の属性に対してどのような種類のオペレーションが可能であって、どのようなオペレーションはできないのかを規定することができる。例えば、放射線専門医の給与などの属性に対する管理者の編集、閲覧、削除の禁止を許可することを規定するが、利用資格のある放射線専門医が使えるのはどの種類の診断用ソフトウェアツールであるかを編集し閲覧するための許可を与えることができる。規定できるその他の許可には、放射線専門医の名前や住所や電子メールのアドレスや電話番号などの一般的なユーザ情報を管理者が編集、閲覧、削除できるという許可がある。

【0021】

また、ユーザ属性規定コンポーネント 33 には、ユーザ属性に割り当て可能な特定の値を管理者が特定できる属性限定値コンポーネント 35 が含まれる。ユーザ属性のうちの一部のものは、同様の限定値をもつことが可能である。また、複数のユーザディレクトリにわたって、特定された一連の限定値を利用することができる。一例として図 2 を再び参照すると、管理者は、ウィスコンシン州にある健康管理プロバイダ B が雇用する放射線専門医を含む管理領域に対して属性限定値コンポーネント 35 を利用して、管理者がどんな値をユーザ属性に割り当て可能かを規定することができる。例えば、「雇用の州」というユーザ属性の場合、その値は 2 文字の略語（例えば、WI や NY など）に限定され、その値を 50 個の可能な値のうちの 1 つに限定することができる。別のシナリオでは、属性限定値コンポーネント 35 を使って、管理者は、様々な用途に値を割り当てる「許可の認定」などのユーザ属性の値を限定することができる。そのようなシナリオでは、各管理者は、特定の用途に関連する値の設定は許可されるが、その他の用途に関する値については許可されない。例えば、図 2 では、地域の病院の管理者（管理者 D）は、放射線科と心臓科のユーザに対して放射線と心臓病のアプリケーションに対する許可を設定することだけを管理者 E が行なえるように限定することができる。

【0022】

また、委託管理ツール 28 は管理特権コンポーネント 32 を備える。管理特権コンポーネント 32 によって、管理者は、権限をもつ管理領域やサブ管理領域に対する管理特権を付与することができる。付与された管理特権には、委託権限と編集権限のうちの少なくとも 1 つが含まれていてもよい。上述したように、閲覧や修正や削除や一時的委託などのその他の種類の権限を付与することも可能である。このような例の権限を、委託権限と編集権限と共に用いるか、委託権限と編集権限の代わりに用いるか、もしくはそれらの権限と組み合わせて用いることができる。

【0023】

また、管理特権コンポーネント 3 2 によって、管理者は、権限をもってオペレーションを行う管理領域やサブ領域内のどのユーザが付与された管理特権をもつことができるのかを規定することができる。特に、管理者は、このコンポーネントを使って委託権限や編集権限やその他の種類の権限を特定のユーザに割り当てて、オペレーション領域に対する様々な管理者を定めることができる。また、委託権限をもつ管理者は領域規定コンポーネント 3 0（即ち、ユーザグループ特定コンポーネント 3 1 とユーザ属性規定コンポーネント 3 3）を利用して、さらに別のユーザグループからサブ領域をオペレーション領域として形成し、一連のユーザ属性のサブセットに対する特定の属性の許可と値を割り当てることができる。また、管理者は管理特権コンポーネント 3 2 を利用して、すでに規定した特定のサブ領域に対する権限を与えることができる。

10

【0024】

また、委託管理ツール 2 8 は、委託された管理特権に従って、各管理領域に関する情報を管理する情報管理コンポーネント 3 6 を備える。管理者は情報管理コンポーネント 3 6 を使って、委託された権限の種類と各ユーザ属性に関する許可レベルに応じて、これに限定されることはないが、領域内のユーザのための特定の属性の編集や閲覧や削除を含むオペレーションを実施することができる。情報管理コンポーネント 3 6 はこれらの機能に限定されず、レポート（例えば、領域内の全ユーザに関するレポート）の作成やデータ分析（例えば、一部の種類のデータの変更頻度を調査する）や統計的分析や特定の属性（例えば、電話番号や電子メールアドレスやパスワードなどの）の自己管理をユーザにやらせるなどのその他の機能を実行することが可能である。

20

【0025】

委託管理ツール 2 8 は、ソフトウェアでの実施に限定されることはない。例えば、領域規定コンポーネント 3 0（即ち、ユーザグループ特定コンポーネント 3 1 と、属性許可コンポーネント 3 4 と属性限定値コンポーネント 3 5 を含むユーザ属性規定コンポーネント 3 3）と、管理特権コンポーネント 3 2 と、情報管理コンポーネント 3 6 は、ハードウェアやファームウェアや、ソフトウェアとハードウェアとファームウェアの組合せの形態を採ることができる。

【0026】

さらに、委託管理ツール 2 8 は、領域規定コンポーネント 3 0（即ち、ユーザグループ特定コンポーネント 3 1、および、属性許可コンポーネント 3 4 と属性限定値コンポーネント 3 5 を含むユーザ属性規定コンポーネント 3 3）と、管理特権コンポーネント 3 2 と、情報管理コンポーネント 3 6 に限定されるものではない。当業者であれば、委託管理ツール 2 8 がその他のコンポーネントを備えていてもよいことを理解することができる。例えば、委託管理ツール 2 8 には、ユーザの生成と管理に関わるプロセスを管理するワークフローコンポーネントも含まれていてもよい。また、委託管理ツール 2 8 には、利用統計やエラー状態などをレポートするレポートングコンポーネントが含まれていてもよい。また、2 相コミット／ロールバックを利用してトランザクションを実行するトランザクション管理コンポーネントがあってもよい。委託管理ツール 2 8 が備えることができるさらに別のコンポーネントには、管理領域の階層に関する情報を閲覧するためのブラウジングコンポーネントがある。

30

40

【0027】

図 5 は、図 4 に示された委託管理ツールを実装したシステム 3 8 の構成図を示したものである。図 5 には、委託管理ツール 2 8 をアクセスするための複数の方法が示されている。計算部 4 0 によって、管理者は委託管理ツール 2 8 をアクセスすることができる。管理者とは、上級管理者や、委託権限や編集権限やその他の種類の権限をもつ管理者である。また、領域内のユーザは計算部 4 0 を介して委託管理ツール 2 8 をアクセスして、基本的な自己管理の一部を行なうことができる。計算部 4 0 は、ハンドヘルドデジタルコンピュータやパーソナルデジタルアシスタントコンピュータやノートブックコンピュータやパーソナルコンピュータやワークステーションか、のいずれかの形態を採ることができる。管理者とユーザは、Microsoft INTERNET EXPLORER や Netscape

50

p e N A V I G A T O Rなどのウェブブラウザ42を利用して委託管理ツール28を突き止めて、計算部40に表示する。計算部40は、電子ネットワークや無線ネットワークなどの通信ネットワークを介して委託管理ツール28に接続される。図5には、計算部40が、エキストラネットやイントラネットなどの専用ネットワーク44やWAN（例えば、インターネット）などの広域ネットワーク46を介して委託管理ツール28に接続できることが示されている。図5に示されているように、委託管理ツール28はサーバ48内に存在し、サーバ48は、委託管理ツール28を提供するウェブサーバ50と、コミュニティを形成する領域内の全ユーザに関する様々な情報を格納するデータベースディレクトリ52（もしくは複数のデータベースディレクトリ）を備えるものである。しかしながら、委託管理ツールはサーバ48と共存する必要はない。システム38は、必要に応じて、委託管理ツール28をアクセスするユーザの認証とアクセス制御を可能にする機能を備えていてもよい。委託管理ツール28自体、もしくはN e t e g r i t y S I T E M I N D E Rなどの市販パッケージによって、認証とアクセス制御の両方のオペレーションをウェブサーバレベルで実行することができる。

【0028】

上述のデータベースディレクトリ52内の情報には、ユーザの名前や所在地や電話番号や組織名やログインIDやパスワードなどの情報が含まれていてもよい。その他の情報には、アプリケーションやコンテンツなどのリソースへのユーザアクセス特権が含まれていてもよい。データベースディレクトリ52には、コミュニティを支援するための、ネットワーク内の物理的装置（例えば、パーソナルコンピュータやサーバやプリンタやルータや通信サーバなど）に関する情報を記憶してもよい。データベースディレクトリ52に記憶されるその他の情報には、各物理的装置が利用可能なサービス（例えば、オペレーティングシステムやアプリケーションや共有ファイルシステムや印刷キューなど）が含まれていてもよい。データベースディレクトリ52は、軽量ディレクトリアクセスプロトコル（LDAP）データベースの形態を採ることができる。しかしながら、その他の種類のスキーマを備えるその他のディレクトリ型データベースを、リレーショナルデータベースやオブジェクト指向データベースや平ファイルやその他のデータ管理システムを含む委託管理ツール28と共に利用することもできる。

【0029】

図5に示されたシステム38を利用することによって、委託権限や編集権限をもつ管理者や上級管理者などの管理者は委託管理ツール28を使ってユーザ属性許可を生成することができる。また、コミュニティのユーザは委託管理ツール28を使って、ユーザ属性値を許容値のサブセットに限定することができる。図6は、委託管理ツール28を用いてユーザ属性許可をもつ管理領域を生成するために行なわれる処理を説明するためのフローチャートを示す。管理領域を生成するためには、ユーザは上級管理者か、もしくは委託権限をもつ管理者でなければならない。ブロック54では、上級管理者か、もしくは委託権限をもつ管理者がサインインする。サインインするオペレーションには、識別情報とセキュリティ情報（例えば、有効なユーザ名やパスワード）の入力が含まれる。56では、委託管理ツールによってユーザ名とパスワードが認証される。次いで58では、委託管理ツールによって、ユーザが管理領域を生成するための許可をもっている（例えば、ユーザが上級管理者や委託権限をもつ管理者である）かどうか判断される。ユーザが認証されていないか、もしくは管理領域を生成する許可をもっていない場合には、そのユーザは領域を生成することはできない。

【0030】

60では、ユーザは管理領域に対して扱える属性のサブセットを特定する。上述したように、属性には、ユーザに関する情報を記述するデータ（例えば、雇用主や職務内容やアクセス許可が付与されているリソースやアドレスや使用装置など）が含まれていてもよい。次に62では、ユーザは、管理者が領域内の各属性に対してどのようなオペレーション（例えば、編集や閲覧や削除など）を実行できて、どのようなオペレーションが実行できないかを規定するための許可を特定する。次に64では、ユーザは、それに関連する限定値

をもつことができる属性を特定する。限定値の要素として属性が特定されるかどうかの判断はユーザの裁量に委ねられる。66では、ユーザは、限定値をもつと特定された属性に対して許容値を割り当てる。一般的に、上級管理者は、領域に対する限定値の属性と許容値のリストを事前に作成することができる。従って、委託権限をもつ管理者が管理領域を生成したい時に、上級管理者によって作成されたリストから選択することによって限定値の属性を特定して許容値を割り当てる作業が実施される。例えば、ユーザの所在地を特定する「国」属性を考えてみよう。上級管理者は、「国」属性を、限定された一連の国の略語に限定することができる。例えば、上級管理者は、米国やカナダやメキシコなどの国を表わすために、USAやCANやMEXなどの一連の値をそれぞれ規定することができる。従って、管理領域を生成するユーザは、「国」属性と共に使われるこれらの限定値を選択することができる。 10

【0031】

次に、ユーザは、管理可能な少なくとも1つのユーザグループを特定する。尚、そのグループ内の各ユーザは、管理者がこれらの属性を管理する方法に関する同じ許可属性で特徴づけられる。特に68では、問合せ規則を構築することによってデータベースディレクトリから少なくとも1つの任意のユーザグループが特定される。その問合せの結果、コミュニティ、即ち領域内のユーザグループのメンバーが決まる。問合せ規則の構築後に、70では、コミュニティ、即ち領域が形成される。次に72では、データベースディレクトリは、新規に生成された管理領域に関するデータで更新される。委託権限をもつ管理者がオペレーション領域とは別の領域を生成したい場合は、ブロック58～72が繰返される。 20
さもなければ、上級管理者や、委託特権をもつ管理者がオペレーション領域に対して管理領域を生成したい場合はブロック54～72が常に繰返される。

【0032】

本開示の上述したフローチャートには、委託管理ツールの機能と動作が示されている。この点に関して、各ブロックは、特定の論理機能を実施するための1つまたは複数の実行可能命令を含むモジュールやセグメントやコードの一部を表わすものである。さらに別の実装形態では、ブロック内に記載された機能は図に記載された順序通りでなくてもよく、実際には、例えば、関係する機能に依存してほぼ同時かもしくは逆順に実行してもよいことに留意されたい。また、当業者であれば、ブロックを追加できることを理解することができる。さらに、そのような機能は、C++やJAVA（商標）などのプログラミング言語 30
で実現可能であるが、その他の言語を利用してもよい。

【0033】

上述の委託管理ツールは、論理機能を実施するための実行可能な命令の順序リストを備えている。順序リストは、どのようなコンピュータ読取可能媒体でも実現することができる。命令を取出して実行するコンピュータシステムによってか、もしくは、それに接続することによって利用可能となる。このアプリケーション環境では、コンピュータ読取可能媒体は、命令を格納したり記録したり通信したり伝搬したり転送したりトランスポートする手段であればどのようなものでもよい。コンピュータ読取可能媒体は、電子的か磁気的か光学的か電磁気的か赤外線システムや装置やデバイスであってもよい。コンピュータ読取可能媒体の例には、1本または複数の電線による電気（電子）接続と、携帯型コンピュータ用ディスク（磁気）と、ランダムアクセスメモリ（RAM）（磁気）と、リードオンリメモリ（ROM）（磁気）と、消去可能プログラマブル読取専用メモリ（EPROMまたはフラッシュメモリ）（磁気）と、光ファイバ（光学）と、再生専用携帯型コンパクトディスク（CDROM）（光学）が含まれていてもよいが、これらは全てを網羅して 40
いるものではない。

【0034】

コンピュータ読取可能媒体には、命令を印刷する紙やその他の適切な媒体が含まれてもよいことに留意されたい。例えば、命令は、紙やその他の媒体を光学的に走査することによって電氣的に入手することができ、必要に応じて、適切な方法でコンパイルしたり解釈したり処理して、コンピュータのメモリに記憶させることができる。 50

【0035】

本発明の委託管理ツールが実現可能であることは明らかである。好適な実施形態に関連して特に本発明を図示し説明したが、当業者であれば、本発明の範囲から逸脱することなく変更や修正を実施できることを理解することができる。

【図面の簡単な説明】

【0036】

【図1】 図1は、ユーザコミュニティの一例の模式図である。

【図2】 図2は、図1に示されたユーザコミュニティの委託管理の一例を示す。

【図3】 図3は、ユーザコミュニティに関する情報を管理するためのユーザ属性許可を生成する委託管理ツールが動作する汎用コンピュータシステムの模式図である。

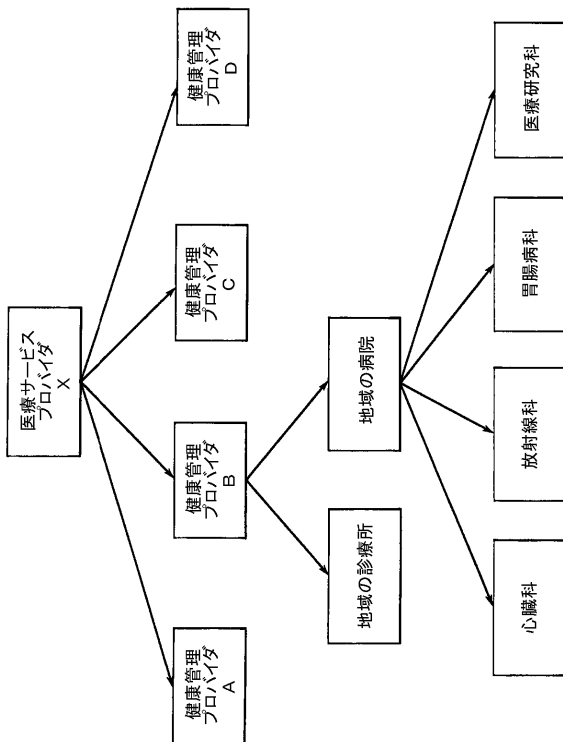
10

【図4】 図4は、情報管理のためのユーザ属性許可を生成するものであって、図3に示されたコンピュータシステムで動作する委託管理ツールのトップレベルコンポーネントの構成図を示す。

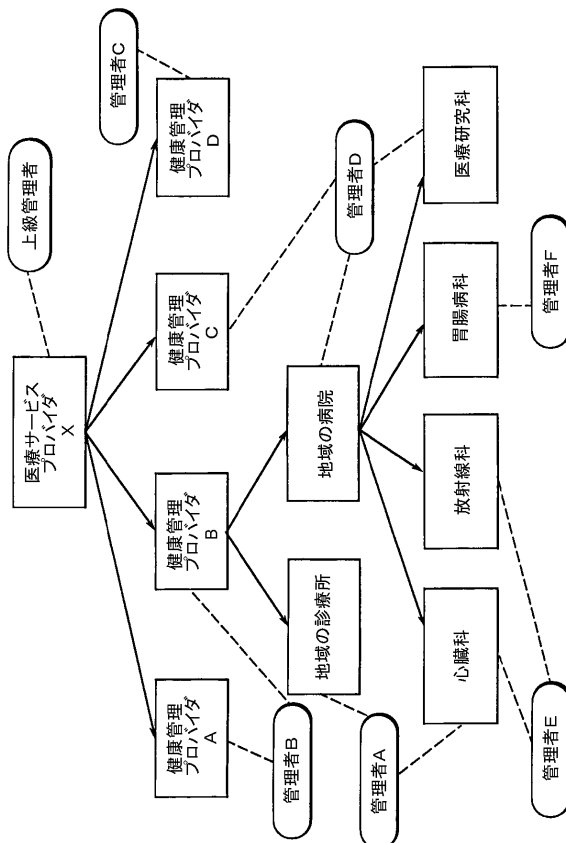
【図5】 図5は、図4に示されたユーザ属性許可を生成する委託管理ツールを実装したシステムの構成図を示す。

【図6】 図6は、図4に示された委託管理ツールを利用してユーザ属性許可をもつ管理領域を生成するための処理のフローチャートを示す。

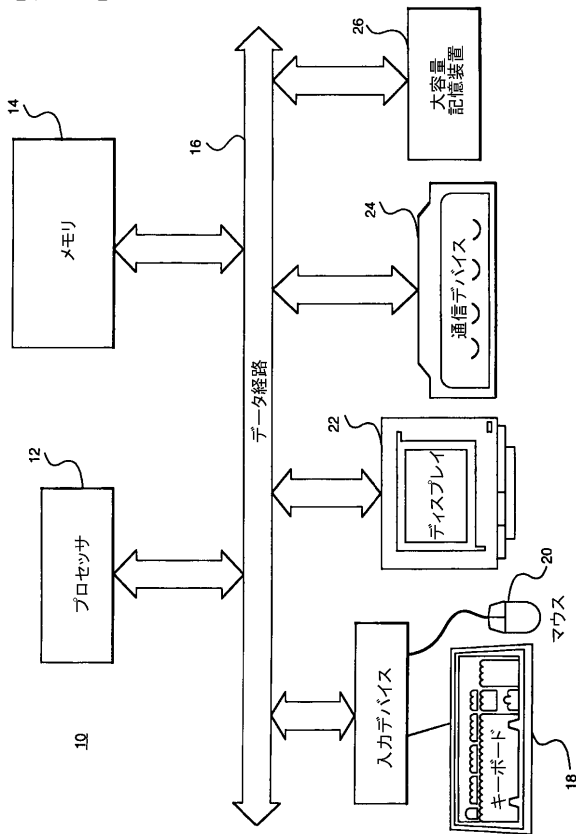
【図1】



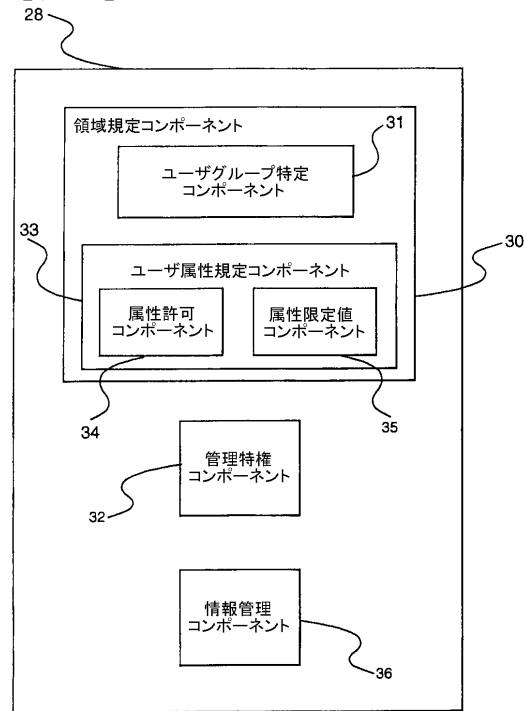
【図2】



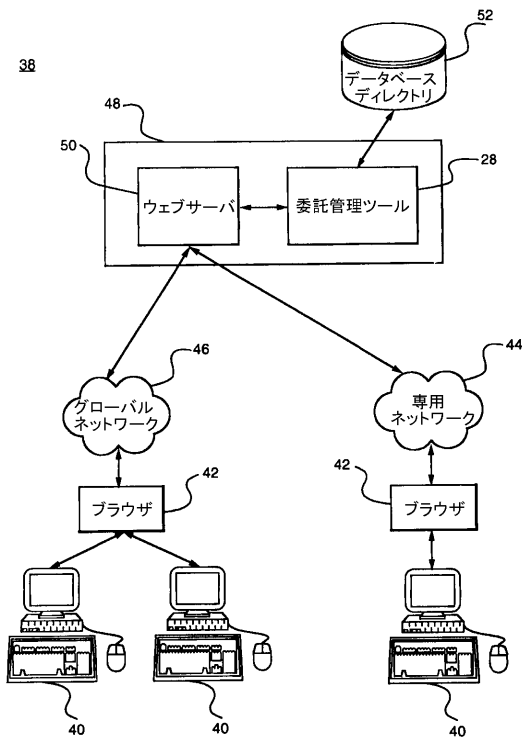
【図 3】



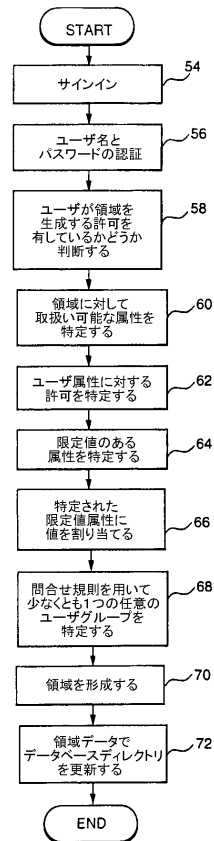
【図 4】



【図 5】



【図 6】



【国際公開パンフレット】

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau(43) International Publication Date
25 July 2002 (25.07.2002)

PCT

(10) International Publication Number
WO 02/057895 A1(51) International Patent Classification: G06F 3/00,
11/00, 13/14, H04M 1/64

(21) International Application Number: PCT/US02/01335

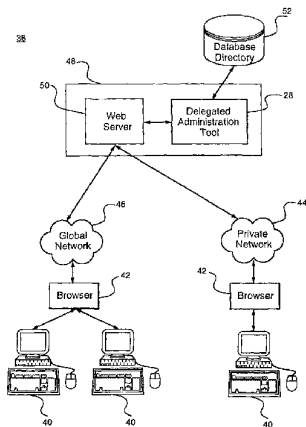
(22) International Filing Date: 16 January 2002 (16.01.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/760,999 16 January 2001 (16.01.2001) US(71) Applicant: GENERAL ELECTRIC COMPANY
[US/US], 1 River Road, Schenectady, NY 12345 (US).(72) Inventors: BARNETT, Janet, Arlie; 2240 Ennis Road,
Pattersonville, NY 12137 (US); VIVIER, Barbara, Jean;
2572 Rosendale Road, Schenectady, NY 12309 (US); AG-
GOUR, Kareem, Sherif; 1506 Union Street, Apartment3, Schenectady, NY 12309 (US); KORNFEIN, Mark,
Mitchell; 17 Omega Terrace, Latham, NY 12110 (US);
OKSOY, Osman, Rifki; 30 Grissom Drive, Clifton Park,
NY 12065 (US); WILLIAMS, Bassel, Omari; 185 Van
Rensselaer Boulevard, Building 26, Apt. 1A, Albany, NY
12204 (US); SEBASTIAN, Jose; 2414 Springdale Road,
Apartment 112, Waukesha, WI (US); MEHRING, David,
Thomas; W238 N6972 Gale Drive, Sussex, WI 53089
(US).(74) Agents: CHASKIN, Jay, L. et al.; General Electric Com-
pany, 3135 Easton Turnpike w3c, Fairfield, CT 06431 (US).(81) Designated States (national): AE, AG, AL, AM, AT, AU,
AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ,
DE, DK, DM, DZ, EE, 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,
NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM,
TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

[Continued on next page]

(54) Title: DELEGATED ADMINISTRATION OF INFORMATION IN A DATABASE DIRECTORY USING ATTRIBUTE PER-
MISSIONS

(57) Abstract: A delegated administrative tool (28) for administering information in a database directory (52) using attribute permissions. The delegated administrative tool (28) enables an administrator to form administrative domains and sub-domains having user attribute permissions that define administrative operations that an administrator can and cannot perform on a user attribute. Also, the delegated administrative tool (28) enables an administrator to define restricted values for assigning to the user attributes.

WO 02/057895 A1

WO 02/057895 A1



(84) **Designated States** (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CI, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— with international search report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WO 02/057895

PCT/US02/01335

DELEGATED ADMINISTRATION OF INFORMATION IN A DATABASE
DIRECTORY USING ATTRIBUTE PERMISSIONS

BACKGROUND OF THE INVENTION

This disclosure relates generally to community-based computer services and more particularly to administration of community-based computer services using attribute permissions.

Generally, a community is a group of people who typically share a common interest. With the advent of the Internet and e-commerce, many companies are forming communities through intranets and extranets, for employees, suppliers, partners and clients. The communities make it easier and less expensive for the employees, suppliers, partners and clients to work together. In the context of computer services, these people are known as computer users or simply users. Information on each of the users in the communities is stored in a broad range of directories and databases. The information may comprise items such as the user's name, location, telephone number, organization, login identification, password, etc. Other information may comprise the user's access privileges to resources such as applications and content. The directories may also store information on the physical devices (e.g., personal computers, servers, printers, routers, communication servers, etc.) in the networks that support the communities. Additional information may comprise the services (e.g., operating systems, applications, shared-file systems, print queues, etc.) available to each of the physical devices. All of the above information is generally known as community-based computer services.

The administration (i.e., the creation, maintenance, modification, updating and disabling) of these community-based computer services becomes difficult as the communities grow in size and complexity. In many cases, administration becomes an almost impossible task, unless a community is subdivided into more manageable sub-communities. With the creation of these sub-communities, it becomes desirable to use a team of administrators who share responsibilities for administering the community by assigning different individuals to administer the sub-communities. This type of administration is referred to as delegated administration.

WO 02/057895

PCT/US02/01335

Currently available administration tools that facilitate delegated administration do have their drawbacks. For instance, these tools do not provide the capability to restrict what types of operations an administrator can perform on the user information. One common example includes allowing an administrator to reset a user's password, but not allowing the administrator to view an existing password. In this example, one type of operation (setting a new password) is allowed while another (viewing the existing password) is not. It is important to provide the minimum allowable permissions (or operations) in order to protect the data as much as possible. Also, the currently available administration tools do not provide the capability to restrict values that an administrator can assign to data fields associated with the user information. For example, there are often data fields within a user directory that are used to store user access permissions (which grant access to web-based applications). Typically, these data field values consist of a list of allowable values (an enumerated list), and only values from that list should be entered. By restricting values to only those within that enumerated list, mistakes and typographic errors can be limited.

Therefore, there is a need for an administration tool that provides the capability to restrict what types of operations an administrator can perform on the user information so that an administrator is constrained in what he or she can do. Also, there is a need for an administration tool that provides the capability to restrict values that an administrator can assign to user information in order to both limit the data values that can be entered, as well as ensure correctness of the data.

BRIEF SUMMARY OF THE INVENTION

In one embodiment of this disclosure, there is a method, system and computer readable medium that stores instructions for instructing a computer system, to manage a user community. In this embodiment, a set of user attributes are defined for each user in the user community. A permission level for managing each of the user attributes is then identified.

In a second embodiment of this disclosure, there is a system, method and computer readable medium that stores instructions for instructing a computer system, to enable an administrator to control administration of a user community. In this embodiment,

WO 02/057895

PCT/US02/01335

user information associated with the user community is provided to an administrator. The administrator is prompted to define a set of user attributes for each user in the user community. The administrator is prompted to identify a permission level for each of the user attributes. The identified permission levels are used to control administration of the user information.

In another embodiment, there is a user community administration tool for managing user information associated with a user community. In the user community administration tool there is a domain definition component that defines the user community into at least one administrative domain. The domain definition component comprises a user group specifying component that specifies at least one arbitrary group of users from the user community and a user attribute definition component that defines a set of permissible user attributes for the at least one arbitrary group of users. An information management component manages the user information associated with the administrative domain in accordance with the permissible user attributes.

In still another embodiment, there is a system for managing user information associated with a user community. This system comprises a database directory that contains a plurality of user information. A user community administration tool manages the plurality of user information in the database directory. The user community administration tool comprises a domain definition component that defines the user community into at least one administrative domain. The domain definition component comprises a user group specifying component that specifies at least one arbitrary group of users from the user community and a user attribute definition component that defines a set of permissible user attributes for the at least one arbitrary group of users. An information management component manages the user information associated with the administrative domain in accordance with the permissible user attributes. A computing unit is configured to serve the user community administration tool and the database directory.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 shows a schematic of an example of a user community;

WO 02/057895

PCT/US02/01335

Fig. 2 shows an example of delegated administration of the user community shown in Fig. 1;

Fig. 3 shows a schematic of a general-purpose computer system in which a delegated administration tool that creates user attribute permissions for managing information associated with a user community operates;

Fig. 4 shows a top-level component architecture diagram of the delegated administration tool that creates user attribute permissions for managing information and that operates on the computer system shown in Fig. 3;

Fig. 5 shows an architectural diagram of a system for implementing the delegated administration tool that creates user attribute permissions shown in Fig. 4; and

Fig. 6 shows a flow chart of the acts performed to create an administrative domain having user attribute permissions with the delegated administration tool shown in Fig. 4.

DETAILED DESCRIPTION OF THE INVENTION

Fig. 1 shows a schematic of an example of a user community receiving a community of services from a medical services provider. The example shown in Fig. 1 is illustrative of the concept of a user community and is not meant to limit this disclosure. In Fig. 1, Healthcare Providers A-D are communities that receive computer-based services from Medical Services Provider X. Examples of such computer-based services may comprise medical information, the ability to order medical supplies, the ability to schedule patient appointments, the ability to file claims for patient services. Other illustrative examples of computer-based services for this scenario may comprise benchmarking information, healthcare statistics and access to downloadable software. The healthcare providers may also want to provide the computer-based services to their clients, partners, vendors, suppliers, etc. In Fig. 1, Healthcare Provider B provides the computer-based services established from Medical Services Provider X to a Local Clinic and Local Hospital with which it has a relationship. The computer-based services can also be provided to their employees. In Fig. 1, the computer-based services are provided to the various departments in the

WO 02/057895

PCT/US02/01335

Local Hospital such as Cardiology, Radiology, Gastroenterology, Medical Research, etc. Similar types of distribution of the computer-based services can be provided for the other healthcare providers (i.e., Healthcare Providers A, C and D).

Medical Services Provider X stores information on each of the users in the community in a database directory. The information may comprise items such as the user's name, location, telephone number, organization, login identification, password, etc. Other information may comprise the user's access privileges to certain resources provided by Medical Services Provider X such as applications and content. The database directory of Medical Services Provider may also store information on the physical devices (e.g., personal computers, servers, printers, routers, communication servers, etc.) in the networks that support the communities. Additional information stored in the database directory may comprise the services (e.g., operating systems, applications, shared-file systems, print queues, etc.) available to each of the physical devices.

Since the user community shown in Fig. 1 can be quite large and complex, it is desirable to subdivide and delegate administration of these communities. Fig. 2 shows an example of delegated administration of the user community shown in Fig. 1. In this example, there is an administrator for each community that is responsible for managing a variety of activities that include but are not limited to modifying user information, updating permissions to certain resources, disabling user accounts, creating user accounts and maintaining user accounts. For instance, the SuperAdministrator manages the activities for Medical Services Provider X; Administrator A manages the activities for the Local Clinic associated with Healthcare Provider B and the Cardiology department of the Local Hospital; Administrator B manages the activities for Healthcare Providers A and B; Administrator C manages the activities for Healthcare Provider D; Administrator D manages the activities for the Local Hospital associated with Healthcare Provider B, the Medical Research departments for the Local Hospital associated with Healthcare Provider B, as well as the activities for Healthcare Provider C; Administrator E manages the activities for the Cardiology and Radiology departments of the Local Hospital associated with Healthcare Provider B; and Administrator F manages the

WO 02/057895

PCT/US02/01335

activities for the Gastroenterology department of the Local Hospital associated with Healthcare Provider B. The extent to which Administrators A-F manage activities depends entirely on the type of authority that they have. Other forms of delegated administration for this example are possible as will be apparent to people skilled in the art.

For purposes of explaining the delegated administration provided with this disclosure, each block (i.e., Medical Services Provider X, Healthcare Providers A-D, Local Clinic, Local Hospital, Cardiology, Radiology, Gastroenterology, Medical Research) in the user community of Fig. 2 represents an administrative domain. An administrative domain is a managed object that comprises a set of users, a set of user attributes which can be modified, and a set of allowable values for those data fields over which an administrator has authority. Possible examples of user attributes may include but are not limited to employer, role or job description, resources that permission has been granted to access, address and equipment used. Generally, an administrator's authority may comprise edit authority and/or delegation authority. An administrator has edit authority within the administrative domain when he or she may edit certain attributes of the users. An administrator has delegation authority within the administrative domain when he or she may define a subset of the users and identify attributes for modification, in order to create an administrative sub-domain. The assignment of the administrative sub-domain to a person is the delegation of that domain. The ability to create an administrative sub-domain and to assign that domain to a user is delegation authority. Although the authority described in this disclosure relates generally to edit authority and delegation authority, one of ordinary skill in the art will recognize that other types of authority such as view, modify, delete, temporary delegation, as well as similar operations, but with limitations on the extent of viewable data, are possible as well. These examples of authority can be used in addition to, in place of, or in combination with the delegation and edit authority.

As mentioned above, it is desirable to be able to create user attribute permissions to restrict what types of operations an administrator can and cannot perform. For example, in Fig. 2, an administrator may only require permission to modify a single

WO 02/057895

PCT/US02/01335

data field associated with the user. An example of this could be a company's payroll department; payroll should only be allowed to modify an employee's salary data field.

In addition, it is desirable to be able to restrict values of the user attributes to a subset of allowable values. For example, in Fig. 2, an administrator may be responsible for managing user access to one application. The user directory may contain a data field for defining all applications that the user may access. However, the administrator is only responsible for a single application; consequently, the administrator should only be allowed to set a single value for that application for any user.

As an example, the above-described delegated administration capabilities for creating user attribute permissions for managing information associated with a user community can be implemented in software. Fig. 3 shows a schematic of a general-purpose computer system 10 in which a delegated administration tool that creates user attribute permissions for managing information operates. The computer system 10 generally comprises at least one processor 12, a memory 14, input/output devices, and data pathways (e.g., buses) 16 connecting the processor, memory and input/output devices. The processor 12 accepts instructions and data from the memory 14 and performs various calculations. The processor 12 includes an arithmetic logic unit (ALU) that performs arithmetic and logical operations and a control unit that extracts instructions from memory 14 and decodes and executes them, calling on the ALU when necessary. The memory 14 generally includes a random-access memory (RAM) and a read-only memory (ROM); however, there may be other types of memory such as programmable read-only memory (PROM), erasable programmable read-only memory (EPROM) and electrically erasable programmable read-only memory (EEPROM). Also, the memory 14 preferably contains an operating system, which executes on the processor 12. The operating system performs basic tasks that include recognizing input, sending output to output devices, keeping track of files and directories and controlling various peripheral devices.

The input/output devices may comprise a keyboard 18 and a mouse 20 that enter data and instructions into the computer system 10. Also, a display 22 may be used to allow a user to see what the computer has accomplished. Other output devices may include

WO 02/057895

PCT/US02/01335

a printer, plotter, synthesizer and speakers. A communication device 24 such as a telephone or cable modem or a network card such as an Ethernet adapter, local area network (LAN) adapter, integrated services digital network (ISDN) adapter, or Digital Subscriber Line (DSL) adapter, that enables the computer system 10 to access other computers and resources on a network such as a LAN or a wide area network (WAN). A mass storage device 26 may be used to allow the computer system 10 to permanently retain large amounts of data. The mass storage device may include all types of disk drives such as floppy disks, hard disks and optical disks, as well as tape drives that can read and write data onto a tape that could include digital audio tapes (DAT), digital linear tapes (DLT), or other magnetically coded media. The above-described computer system 10 can take the form of a hand-held digital computer, personal digital assistant computer, notebook computer, personal computer, workstation, mini-computer, mainframe computer or supercomputer.

Fig. 4 shows a top-level component architecture diagram of a delegated administration tool 28 that can create user attribute permissions for managing information and that operates on the computer system 10 shown in Fig. 3. The delegated administration tool 28 comprises a domain definition component 30 that defines a user community into at least one administrative domain. The domain definition component 30 comprises a user group specifying component 31 that enables an administrator to specify at least one arbitrary group of users from a user community. The user group specifying component 31 forms the at least one arbitrary group of users through a query rule constructed by the administrator to query a database directory containing user information. The query rule defines the users within the at least one arbitrary group of users. For example, referring to Fig. 2, an administrator can use the user group specifying component 31 to form an administrative domain from one group that comprises users that are radiologists, a second group that comprises users that are employed by Healthcare Provider B, and a third group that comprises users that are located in Wisconsin.

Each arbitrary group of users that is specified has attributes associated with each of its users and allowable values for these attributes. A user attribute definition component 33 enables an administrator to define a set of permissible user attributes for the at least

WO 02/057895

PCT/US02/01335

one arbitrary group of users. Specifically, the defined set of permissible user attributes contains the attributes that an administrator can act upon. The user attribute definition component 33 comprises an attribute permission component 34 that enables an administrator to specify a permission level for each of the user attributes. The permission level is associated with management of attributes as defined within a domain. This allows different administrators to have different permissions when managing the same data. In particular, the permission level is indicative of what types of operations can and cannot be performed on the attributes associated with the at least one arbitrary group of users. Some operations that an administrator can perform on user attributes comprise viewing, editing and deleting. These administrative operations are illustrative of only a few operations that can be performed on the attributes and are not exhaustive of other possibilities. Examples of some other administrative operations that can be performed on the attributes are editing during a particular time period and resetting data fields to default values. An administrator can use the attribute permission component 34 to select any of these operations to restrict what can and cannot be done to the attributes. Selection of permissions for the attributes is left to the user that is setting up the administrative domain. It is possible to select just one of the above operations or any combination of the operations.

Referring again to Fig. 2 as example, an administrator can use the attribute permission component 34 for the administrative domain that comprises radiologists that are employed by Healthcare Provider B in the state of Wisconsin to define what types of operations can and cannot be formed on certain attributes. For example, permission to prevent an administrator from editing, viewing and deleting an attribute such as a radiologist's salary can be defined, while permission can be granted to edit and view what type of diagnostic software tools that a radiologist is licensed to use. Another permission that can be defined is to permit an administrator to edit, view, and delete general user information such as the radiologist's name, address, e-mail address, phone number, etc.

The user attribute definition component 33 also comprises an attribute restricted value component 35 that enables an administrator to specify certain values that can be assigned to user attributes. It is possible that some user attributes will have similar

WO 02/057895

PCT/US02/01335

restricted values. Also, it is possible to use a set of specified restricted attributes across a multiple of user directories. Referring again to Fig. 2 as an example, an administrator can use the attribute restricted value component 35 for the administrative domain that comprises radiologists that are employed by Healthcare Provider B in the state of Wisconsin to define what values an administrator can assign for a user attribute. For example, for the "State of Employment" user attribute, values can be restricted to one of 50 possible values, wherein the values are limited to two letter abbreviations (e.g., WI, NY, etc.). In another scenario, the attribute restricted value component 35 could be used to restrict values for a user attribute such as "Permissions Authorization", where an administrator assigns values to different applications. In such a scenario, each administrator may have permission to set values associated with a particular application, but not values associated with other applications. For example, in Fig. 2, the local hospital administrator (Administrator D) may limit what Administrator E may do to only setting Radiology and Cardiology applications permissions for users in the Radiology and Cardiology departments, respectively.

The delegated administration tool 28 also comprises an administrative privileges component 32. The administrative privileges component 32 enables an administrator to grant administrative privileges for an administrative domain or administrative sub-domain that he or she has authority for. The granted administrative privileges may comprise at least one of delegation authority and edit authority. As mentioned above, it is also possible to grant other types of authority such as view, modify, delete, temporary delegation, etc. These examples of authority can be used in addition to, in place of, or in combination with the delegation and edit authority.

The administrative privileges component 32 also enables an administrator to define which users in an administrative domain or sub-domain that he or she operates and has authority for will have the granted administrative privileges. More specifically, an administrator can use this component to define various administrators for their operational domain by assigning delegation authority, edit authority or other types to a particular user. Administrators with delegation authority can also use the domain definition component 30 (i.e., the user group specifying component 31 and user

WO 02/057895

PCT/US02/01335

attribute definition component 33) to form sub-domains from an additional group of users for their operational domain and assign certain attribute permissions and values for a subset of user attributes. The administrator can also use the administrative privileges component 32 to grant authority for that particular sub-domain that they have defined.

The delegated administration tool 28 also comprises an information management component 36 that manages information associated with each of the administrative domains in accordance with the delegated administrative privileges. Depending on the type of authority delegated and the permission level associated with each of the user attributes, an administrator can use the information management component 36 to perform operations including but not limited to editing, viewing or deleting specific attributes for a user in a domain. The information management component 36 is not limited to these functions and may perform other functions such as generating reports (e.g., reports on all users within a domain), analyzing data (e.g., determining how frequently some types of data change), performing statistical analysis or allowing users to perform self-administration on certain attributes (e.g., phone number, e-mail address, passwords, etc.).

The delegated administration tool 28 is not limited to a software implementation. For instance, the domain definition component 30 (i.e., the user group specifying component 31 and user attribute definition component 33 which includes the attribute permissions component 34 and attribute restricted value component 35), administrative privileges component 32 and information management component 36 may take the form of hardware or firmware or combinations of software, hardware, and firmware.

In addition, the delegated administration tool 28 is not limited to the domain definition component 30 (i.e., the user group specifying component 31 and user attribute definition component 33 which includes the attribute permissions component 34 and attribute restricted value component 35), administrative privileges component 32 and information management component 36. One of ordinary skill in the art will recognize that the delegated administration tool 28 may have other components. For

WO 02/057895

PCT/US02/01335

example, the delegated administration tool 28 could also include a workflow component that manages processes surrounding user creation and administration. Also, the delegated administration tool 28 could include a reporting component that reports usage statistics, error conditions, etc. There could also be a transactional management component that performs transactions using 2-phase commit/rollback. Still another component that the delegated administration tool 28 could include is a browsing component for viewing information associated with the hierarchy of administrative domains.

Fig. 5 shows an architectural diagram of a system 38 for implementing the delegated administration tool shown in Fig. 4. Fig. 5 shows that there are several ways of accessing the delegated administration tool 28. A computing unit 40 allows an administrator to access the delegated administration tool 28. The administrator could be the SuperAdministrator or administrators with delegation authority, edit authority or other types of authority. Also, users in the domain may access the delegated administration tool 28 through a computing unit 40 to perform some basic self-administration. The computing unit 40 can take the form of a hand-held digital assistant computer, personal digital assistant computer, notebook computer, personal computer or workstation. The administrators and users use a web browser 42 such as Microsoft INTERNET EXPLORER or Netscape NAVIGATOR to locate and display the delegated administration tool 28 on the computing unit 40. A communication network such as an electronic or wireless network connects the computing unit 40 to the delegated administration tool 28. Fig. 5 shows that the computing units 40 may connect to the delegated administration tool 28 through a private network 44 such as an extranet or intranet or a global network 46 such as a WAN (e.g., Internet). As shown in Fig. 5, the delegated administration tool 28 resides in a server 48, which comprises a web server 50 that serves the delegated administration tool 28 and a database directory 52 (or directories) that contains the various information for the users in all of the domains that form the community. However, the delegated administration tool does not have to be co-resident with the server 48. If desired, the system 38 may have functionality that enables authentication and access control of users accessing the delegated administration tool 28. Both authentication and access

WO 02/057895

PCT/US02/01335

control can be handled at the web server level by the delegated administration tool 28 itself, or by commercially available packages such as Netegrity SITEMINDER.

The information in the database directory 52 as mentioned above may comprise information such as the user's name, location, telephone number, organization, login identification, password, etc. Other information may comprise the user's access privileges to certain resources such as applications and content. The database directory 52 may also store information on the physical devices (e.g., personal computers, servers, printers, routers, communication servers, etc.) in the networks that support the communities. Additional information stored in the database directory 52 may comprise the services (e.g., operating systems, applications, shared-file systems, print queues, etc.) available to each of the physical devices. The database directory 52 can take the form of a lightweight directory access protocol (LDAP) database; however, other directory type databases with other types of schema can be used with the delegated administration tool 28, including relational databases, object-oriented databases, flat files, or other data management systems.

Using the system 38 shown in Fig. 5, an administrator such as a SuperAdministrator or an administrator with delegation or edit authority can use the delegated administration tool 28 to create user attribute permissions. Also, users of the community can use the delegated administration tool 28 to restrict user attribute values to a subset of allowable values. Fig. 6 shows a flow chart describing the acts performed to create an administrative domain having user attribute permissions with the delegated administration tool 28. To create an administrative domain, the user must be either a SuperAdministrator or an administrator having delegation authority. At block 54, the SuperAdministrator or administrator with delegation authority signs in. The sign-in act can include entering identity and security information (e.g., a valid username and password). The delegated administration tool validates the username and password at 56. The delegated administration tool then determines if the user has permission (i.e., the user is a SuperAdministrator or administrator with delegation authority) to create an administrative domain at 58. If the user is not authenticated or does not have permission to create an administrative domain, then the user is not allowed to create a domain.

WO 02/057895

PCT/US02/01335

At 60, the user identifies a subset of attributes that can be handled for the administrative domain. As mentioned above, attributes may comprise any data, which describe information about a user (e.g., employer, job description, resources that permission has been granted to access, address, equipment used, etc.). Next, the user identifies permissions that define what type of operations (e.g., edit, view, delete, etc.) an administrator can and cannot perform on each of the attributes in the domain at 62. The user then identifies attributes that will have restricted values associated therewith at 64. The determination of whether an attribute is designated as a restricted value component is left to the discretion of the user. At 66, the user assigns allowable values for the attributes that have been identified to have restricted values. Generally, a list of the restricted value attributes and allowable values for any domain can be created beforehand by a SuperAdministrator. Therefore, when an administrator with delegation authority wants to create an administrative domain, the acts of identifying restricted value attributes and assigning allowable values is performed by making selections from the list created by the SuperAdministrator. For example, consider a "country" attribute that identifies the location of a user. The SuperAdministrator can restrict the "country" attribute to a limited set of country abbreviations. For instance, in order to represent the countries United States, Canada and Mexico, the SuperAdministrator can define a set of values such as USA, CAN or MEX, respectively. Thus, a user that is creating an administrative domain can then select these restricted values to be used with the "country" attribute.

Next, the user specifies at least one arbitrary group of users that can be administered, where each user in the group is characterized by the same attributes that have permissions on how an administrator can manage these attributes. In particular, the at least one arbitrary group of users are specified from the database directory by constructing a query rule at 68. The results of the query define the members of the groups of users in the community or domain. After the query rule has been constructed, the community or domain is formed at 70. Next, the database directory is updated at 72 with the data for the newly created administrative domain. If an administrator with delegation authority wants to create another domain from their operational domain, then blocks 58-72 are repeated. Otherwise, any time a

WO 02/057895

PCT/US02/01335

SuperAdministrator or an administrator with delegation authority desires to create an administrative domain for their operational domain, then blocks 54 through 72 are repeated.

The foregoing flow charts of this disclosure show the functionality and operation of the delegated administration tool. In this regard, each block represents a module, segment, or portion of code, which comprises one or more executable instructions for implementing the specified logical function(s). It should also be noted that in some alternative implementations, the functions noted in the blocks may occur out of the order noted in the figures or, for example, may in fact be executed substantially concurrently or in the reverse order, depending upon the functionality involved. Also, one of ordinary skill in the art will recognize that additional blocks may be added. Furthermore, the functions can be implemented in programming languages such as C++ or JAVA; however, other languages can be used.

The above-described delegated administration tool comprises an ordered listing of executable instructions for implementing logical functions. The ordered listing can be embodied in any computer-readable medium for use by or in connection with a computer-based system that can retrieve the instructions and execute them. In the context of this application, the computer-readable medium can be any means that can contain, store, communicate, propagate, transmit or transport the instructions. The computer readable medium can be an electronic, a magnetic, an optical, an electromagnetic, or an infrared system, apparatus, or device. An illustrative, but non-exhaustive list of computer-readable mediums can include an electrical connection (electronic) having one or more wires, a portable computer diskette (magnetic), a random access memory (RAM) (magnetic), a read-only memory (ROM) (magnetic), an erasable programmable read-only memory (EPROM or Flash memory) (magnetic), an optical fiber (optical), and a portable compact disc read-only memory (CDROM) (optical).

Note that the computer readable medium may comprise paper or another suitable medium upon which the instructions are printed. For instance, the instructions can be electronically captured via optical scanning of the paper or other medium, then

WO 02/057895

PCT/US02/01335

compiled, interpreted or otherwise processed in a suitable manner if necessary, and then stored in a computer memory.

It is apparent that there has been provided in accordance with this invention, a delegated administration tool. While the invention has been particularly shown and described in conjunction with a preferred embodiment thereof, it will be appreciated that variations and modifications can be effected by a person of ordinary skill in the art without departing from the scope of the invention.

WO 02/057895

PCT/US02/01335

WHAT IS CLAIMED IS:

1. A method for managing a user community, comprising:

defining a set of user attributes for each user in the user community; and

identifying a permission level for managing each of the user attributes.
2. The method according to claim 1, wherein each permission level defines administrative operations that an administrator can and cannot perform on a user attribute.
3. The method according to claim 1, further comprising defining restricted values that an administrator can assign for the user attributes.
4. A method for managing user information associated with a user community, comprising:

defining a set of user attributes from the user information for each user the user community;

identifying a permission level for each of the user attributes; and

managing the user attributes according to each of the permission levels.
5. The method according to claim 4, wherein each permission level defines operations that an administrator can and cannot be perform on a user attribute.
6. The method according to claim 4, further comprising defining restricted values that an administrator can assign for any of the user attributes.
7. A method for enabling an administrator to control administration of a user community, comprising:

providing user information associated with the user community to the administrator;

prompting the administrator to define a set of user attributes for each user in the user community;

WO 02/057895

PCT/US02/01335

prompting the administrator to identify a permission level for each of the user attributes; and

using the identified permission levels to control administration of the user information.

8. The method according to claim 7, wherein each permission level defines operations that the administrator can and cannot perform on a user attribute.

9. The method according to claim 8, further comprising prompting the administrator to define restricted values that the administrator can assign for any of the user attributes.

10. A user community administration tool for managing user information associated with a user community, comprising:

a domain definition component that defines the user community into at least one administrative domain, the domain definition component comprising a user group specifying component that specifies at least one arbitrary group of users from the user community and a user attribute definition component that defines a set of permissible user attributes for the at least one arbitrary group of users; and

an information management component that manages the user information associated with the administrative domain in accordance with the permissible user attributes.

11. The tool according to claim 10, wherein the user attribute definition component comprises an attribute permission component that specifies a permission level for each of the user attributes.

12. The tool according to claim 11, wherein each permission level defines operations that an administrator can and cannot perform on a user attribute.

13. The tool according to claim 10, wherein the user attribute definition component comprises an attribute restricted value component that defines restricted values that an administrator can assign for any of the user attributes.

WO 02/057895

PCT/US02/01335

14. The tool according to claim 10, further comprising an administrative privileges component that grants administrative privileges for the administrative domain.

15. The tool according to claim 14, wherein the administrative privileges component delegates the granted administrative privileges for the administrative domain.

16. A system for managing user information associated with a user community, comprising:

a database directory containing a plurality of user information;

a user community administration tool to manage the plurality of user information in the database directory; the user community administration tool comprising a domain definition component that defines the user community into at least one administrative domain, the domain definition component comprising a user group specifying component that specifies at least one arbitrary group of users from the user community and a user attribute definition component that defines a set of permissible user attributes for the at least one arbitrary group of users; and an information management component that manages the user information associated with the administrative domain in accordance with the permissible user attributes; and

a first computing unit configured to serve the user community administration tool and the database directory.

17. The system according to claim 16, further comprising a second computing unit configured to execute the user community administration tool served from the first computing unit over a network.

18. The system according to claim 16, wherein the user attribute definition component comprises an attribute permission component that specifies a permission level for each of the user attributes.

19. The system according to claim 18, wherein each permission level defines operations that an administrator can and cannot perform on a user attribute.

WO 02/057895

PCT/US02/01335

20. The system according to claim 16, wherein the user attribute definition component comprises an attribute restricted value component that defines restricted values that an administrator can assign for any of the user attributes.

21. A user community administration tool for providing administration of a user community, comprising:

means for defining the user community into at least one administrative domain, the administrative domain definition means comprising means for specifying at least one arbitrary group of users from the user community and means for defining a set of permissible user attributes for the at least one arbitrary group of users; and

means for managing the user information associated with the administrative domain in accordance with the permissible user attributes.

22. The tool according to claim 21, wherein the user attribute definition means comprises means for specifying a permission level for each of the user attributes.

23. The tool according to claim 22, wherein each permission level defines operations that an administrator can and cannot perform on a user attribute.

24. The tool according to claim 21, wherein the user attribute definition means comprises means for defining restricted values that an administrator can assign for any of the user attributes.

25. A computer-readable medium storing computer instructions for instructing a computer system to manage a user community, the computer instructions comprising:

defining a set of user attributes for each user in the user community; and

identifying a permission level for managing each of the user attributes.

26. The computer-readable medium according to claim 25, wherein each permission level defines operations that an administrator can and cannot perform on a user attribute.

WO 02/057895

PCT/US02/01335

27. The computer-readable medium according to claim 25, further comprising instructions for defining restricted values that an administrator can assign for any of the user attributes.

28. A computer-readable medium storing computer instructions for instructing a computer system to enable an administrator to control administration of a user community, the computer instructions comprising:

providing user information associated with the user community to the administrator;

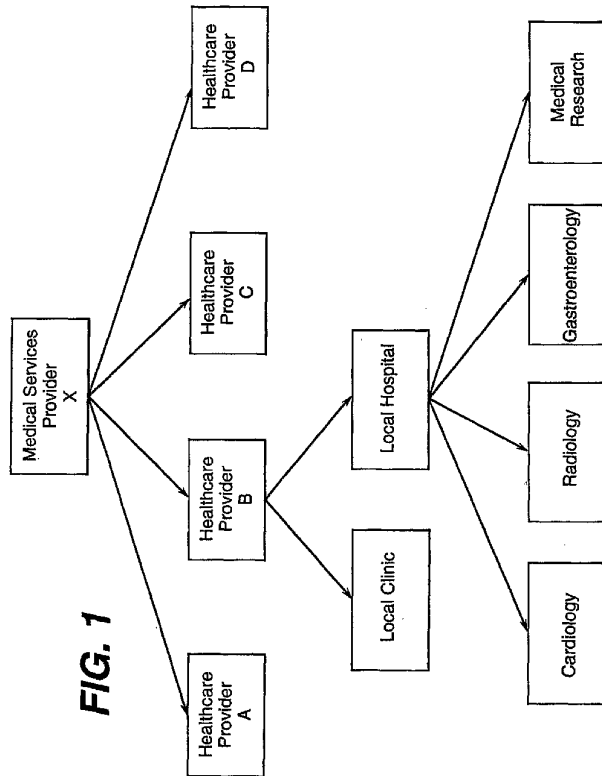
prompting the administrator to define a set of user attributes for each of the users in the user community;

prompting the administrator to identify a permission level for each of the user attributes; and

using the identified permission levels to control administration of the user information.

29. The computer-readable medium according to claim 28, wherein each permission level defines operations that the administrator can and cannot perform on a user attribute.

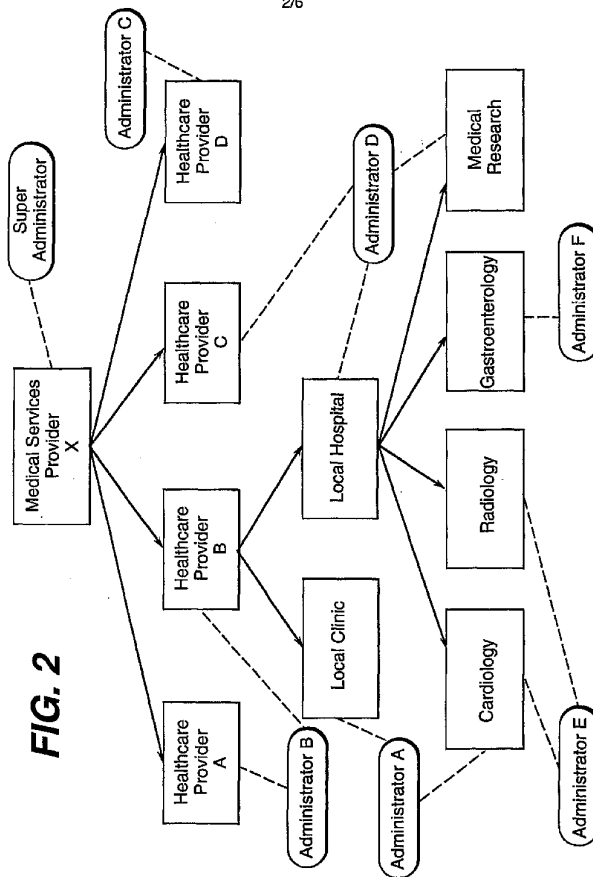
30. The computer-readable medium according to claim 28, further comprising instructions for prompting the administrator to define restricted values that the administrator can assign for any of the user attributes.



WO 02/057895

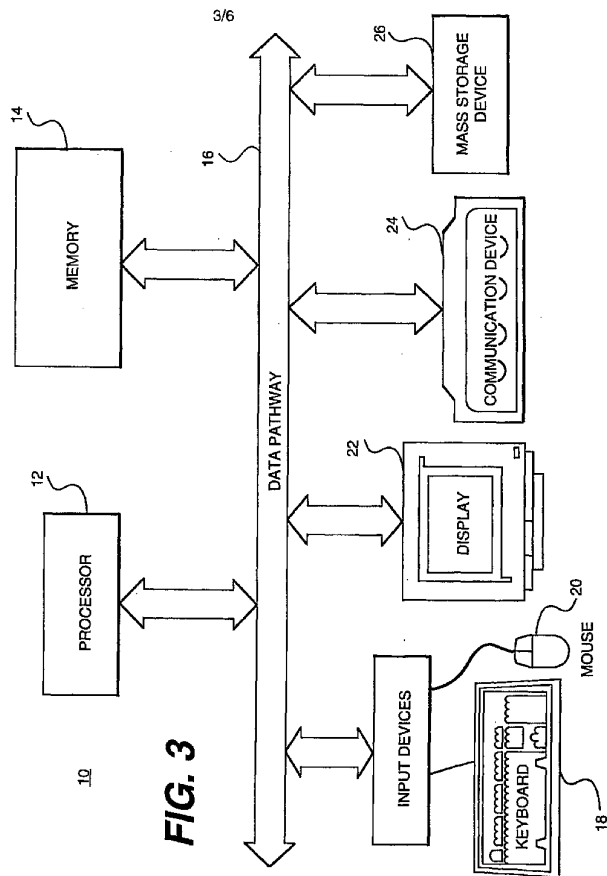
PCT/US02/01335

2/6



WO 02/057895

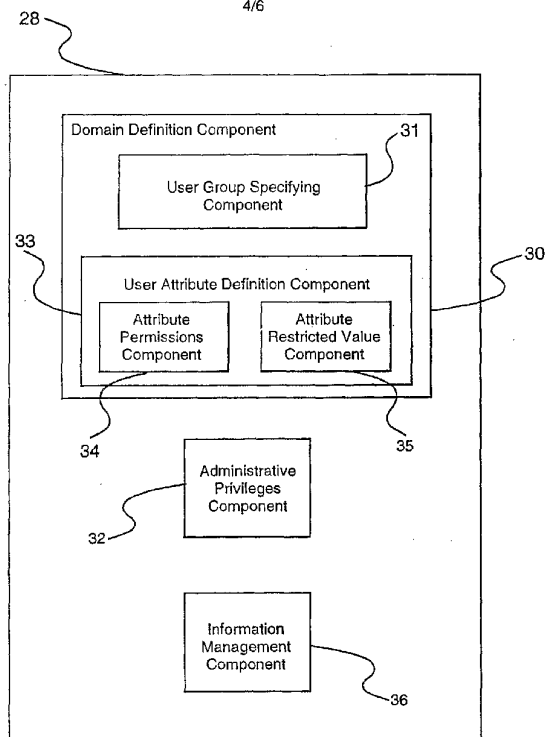
PCT/US02/01335



WO 02/057895

PCT/US02/01335

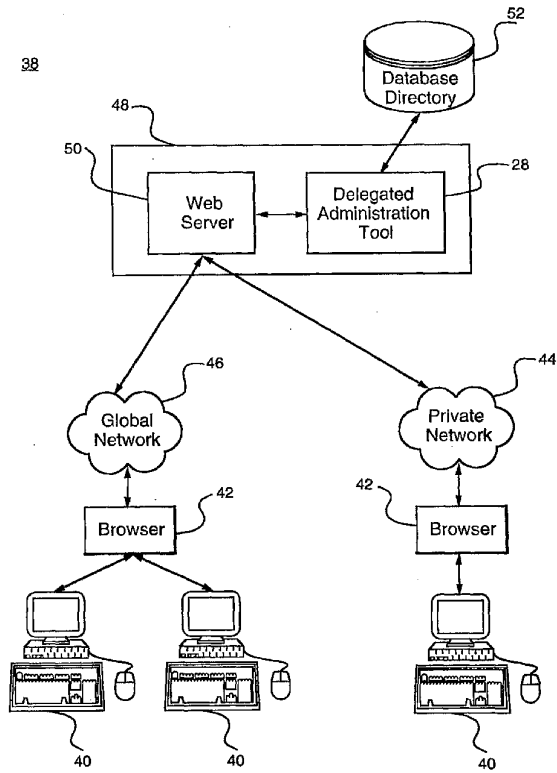
4/6

**FIG. 4**

WO 02/057895

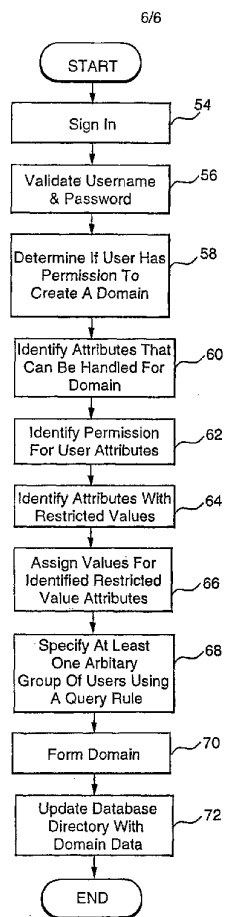
PCT/US02/01335

5/6

**FIG. 5**

WO 02/057895

PCT/US02/01335

**FIG. 6**

【国際調査報告】

INTERNATIONAL SEARCH REPORT		International application No. PCT/US02/01335
A. CLASSIFICATION OF SUBJECT MATTER IPC(7) : G06F 3/00, 11/00, 13/14; H04M 1/64 US CL : 713/201; 348/853; 710/36; 379/88.13 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) U.S. : 713/201; 348/853; 710/36; 379/88.13 Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) Please See Continuation Sheet		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y, E	US 2002/0030703 A1 (ROBERTSON et al) 14 March 2002, see whole document.	1-30
Y	US 5,968,177 A (BATTEN-CAREW et al) 19 October 1999, see whole document.	1-30
Y	US 6,031,895 A (COHN et al) 29 February 2000, see whole document.	1-30
Y	US 6,151,643 A (CHENG et al) 21 November 2000, see whole document.	1-30
☐ 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 not considered to be of particular relevance "E" earlier application or patent 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 "Z" document member of the same patent family		
Date of the actual completion of the international search 02 April 2002 (02.04.2002)		Date of mailing of the international search report 02 April 2002
Name and mailing address of the ISA/US Comptroller of Patents and Trademarks Box PCT Washington, D.C. 20531 Facsimile No. (703)305-3230		Authorized officer Ayaz R. Sheikh James R. Matthews Telephone No. 703-305-9648

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US02/01335

Continuation of B. FIELDS SEARCHED Item 3:

East search terms:

service provider, client/server, user attributes, user profile, database directory, administrator, administration, attribute permission.

フロントページの続き

(81)指定国 AP(GH,GM,KE,LS,MW,MZ,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT, BE,CH,CY,DE,DK,ES,FI,FR,GB,GR,IE,IT,LU,MC,NL,PT,SE,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN, TD,TG),AE,AG,AL,AM,AT,AU,AZ,BA,BB,BG,BR,BY,BZ,CA,CH,CN,CR,CU,CZ,DE,DK,DM,DZ,EE,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,NO,NZ,PL,PT,RO,RU,SD, SE,SG,SI,SK,SL,TJ,TM,TR,TT,TZ,UA,UG,UZ,VN,YU,ZA,ZW

(72)発明者 バーネット, ジャネット・アーリー

アメリカ合衆国、1 2 1 3 7、ニューヨーク州、パターソンビル、エニス・ロード、2 2 4 0 番

(72)発明者 ビビエ, バーバラ・ジーン

アメリカ合衆国、1 2 3 0 9、ニューヨーク州、スケネクタデイ、ローセンドール・ロード、2 5 7 2 番

(72)発明者 アグール, カリーム・シェリフ

アメリカ合衆国、1 2 3 0 9、ニューヨーク州、スケネクタデイ、アパートメント・3、ユニオン・ストリート、1 5 0 6 番

(72)発明者 コーンファイン, マーク・ミッチェル

アメリカ合衆国、1 2 1 1 0、ニューヨーク州、ラザム、オメガ・テラス、1 7 番

(72)発明者 オクソイ, オスマン・リフキ

アメリカ合衆国、1 2 0 6 5、ニューヨーク州、クリフトン・パーク、グリソム・ドライブ、3 0 番

(72)発明者 ウィリアムズ, バセル・オマリ

アメリカ合衆国、1 2 2 0 4、ニューヨーク州、オールバニ、エーピーティー・1エー、ビルディング・2 6、バン・レンスラー・ブルヴァール、1 8 5 番

(72)発明者 セバスチャン, ホセ

アメリカ合衆国、ウィスコンシン州、ウォーキシャ、アパートメント・1 1 2、スプリングデール・ロード、2 4 1 4 番

(72)発明者 メーリング, デビッド・トマス

アメリカ合衆国、5 3 0 8 9、ウィスコンシン州、サセックス、ゲール・ドライブ、ダブリュー 2 3 8・エヌ 6 9 7 2 番

Fターム(参考) 5B017 BA06 CA16

5B082 EA11 GA13