

(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2004-532438

(P2004-532438A)

(43) 公表日 平成16年10月21日(2004.10.21)

(51) Int.Cl.⁷

G06F 12/14

F I

G06F 12/14 520A

テーマコード (参考)

5B017

審査請求 未請求 予備審査請求 未請求 (全 54 頁)

(21) 出願番号 特願2002-558172 (P2002-558172)
 (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/US2002/001330
 (87) 国際公開番号 W02002/057956
 (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 09/760,998
 (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

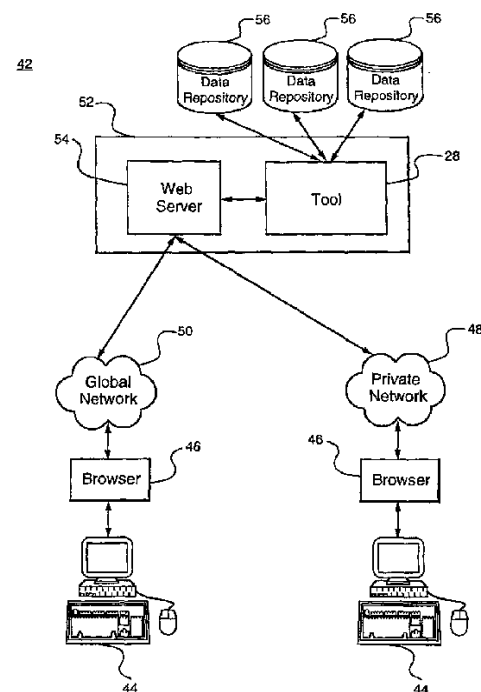
最終頁に続く

(54) 【発明の名称】 管理するコミュニティの確立と保守

(57) 【要約】

【課題】 管理するコミュニティの確立し保守する方法と提供する。

【解決手段】 管理するコミュニティ確立と保守。管理ツール (28) が様々な構造化された個別のディレクトリとデータベース (56) に存在する情報をもつコミュニティを管理することを可能にする方法とツールが開示される。さらに、本開示では、管理ツールが、幅広い範囲のディレクトリとデータベース (56) から管理される情報を確立することを可能にする方法とツール (28) について説明しているが、その中には、管理される情報と管理されない情報を規定し、管理する新しい情報を見つける (32) ことが含まれる。



【特許請求の範囲】**【請求項 1】**

データ収集を管理するために必要な情報を確立する方法であって、
データ収集に関するデータを含む少なくとも 1 つのデータレポジトリを識別する工程と、
前記少なくとも 1 つのデータレポジトリ内のデータ構造を見つける工程と、
データオブジェクトと前記オブジェクトの属性を選択して、見つけられた構造から管理する工程と、
選択された属性を管理するためのアクセス許可を規定する工程を備える方法。

【請求項 2】

前記少なくとも 1 つのデータレポジトリを識別する工程は、様々な構造をもつデータレポジトリから選択することを備える、請求項 1 の方法。 10

【請求項 3】

構造を見つける前記工程は、前記少なくとも 1 つのデータレポジトリ内に存在するデータオブジェクトと属性を確認することを備える、請求項 1 の方法。

【請求項 4】

非管理の属性を識別する工程をさらに備える、請求項 1 の方法。

【請求項 5】

アクセス許可を規定する前記工程は、前記選択された属性に関して実行できるかもしくはできないオペレーションを確認することを備える、請求項 1 の方法。

【請求項 6】

アクセス許可を規定する前記工程は、前記選択された属性の一部に対する限定値を特定することを備える、請求項 1 の方法。 20

【請求項 7】

選択されたデータオブジェクトと属性と規定されたアクセス許可のうちの少なくとも 1 つを変更する工程をさらに備える、請求項 1 の方法。

【請求項 8】

次の時間に、前記少なくとも 1 つのデータレポジトリ内のデータ構造に関する情報を再発見する工程をさらに備える、請求項 1 の方法。

【請求項 9】

コミュニティを管理するために必要な情報を確立する方法であって、 30
前記コミュニティに関するデータを含む少なくとも 1 つのデータレポジトリを識別する工程と、
前記少なくとも 1 つのデータレポジトリ内のデータ構造を見つける工程と、
データオブジェクトと前記オブジェクトの属性を選択して、見つけられた構造から管理する工程と、
選択された属性を管理するためのアクセス許可を規定する工程を備える方法。

【請求項 10】

少なくとも 1 つのデータレポジトリを識別する前記工程は、前記少なくとも 1 つのデータレポジトリに記憶されるデータをアクセスするための接続情報を特定することを備える、請求項 9 の方法。 40

【請求項 11】

構造を見つける前記工程は、前記少なくとも 1 つのデータレポジトリ内に存在するデータオブジェクトと属性を確認することを備える、請求項 1 の方法。

【請求項 12】

非管理の属性を識別する工程をさらに備える、請求項 1 の方法。

【請求項 13】

アクセス許可を規定する前記工程は、選択された属性に関して実行できる、もしくは、できないオペレーションを確認することを備える、請求項 1 の方法。

【請求項 14】

アクセス許可を規定する前記工程は、選択された属性の一部に対する限定値を特定するこ 50

とを備える、請求項 1 の方法。

【請求項 15】

選択されたデータオブジェクトと属性と規定されたアクセス許可のうちの少なくとも 1 つを変更する工程をさらに備える、請求項 1 の方法。

【請求項 16】

次の時間に、前記少なくとも 1 つのデータレポジトリ内のデータ構造に関する情報を再発見する工程をさらに備える、請求項 1 の方法。

【請求項 17】

情報を再発見する前記工程は、前記少なくとも 1 つのデータレポジトリ内に存在するデータオブジェクトと属性を確認することを備える、請求項 16 の方法。

10

【請求項 18】

管理する新しいデータオブジェクトと属性を選択する工程をさらに備える、請求項 17 の方法。

【請求項 19】

コミュニティを管理するために必要な情報を管理者が確立できるようにする方法であって、

前記コミュニティに関するデータを含む少なくとも 1 つのデータレポジトリを識別する工程と、

前記少なくとも 1 つのデータレポジトリ内のデータ構造を見つける工程と、

見つめられた構造からオブジェクト内のデータオブジェクトと属性を選択するように前記管理者を促す工程と、

20

選択された属性を管理するためのアクセス許可を規定するように前記管理者を促す工程を備える方法。

【請求項 20】

少なくとも 1 つのデータレポジトリを識別する前記工程は、前記少なくとも 1 つのデータレポジトリ内に記憶されたデータをアクセスするための接続情報を特定することを備える、請求項 19 の方法。

【請求項 21】

前記構造を見つける前記工程は、前記少なくとも 1 つのデータレポジトリ内に存在するデータオブジェクトと属性を確認することを備える、請求項 19 の方法。

30

【請求項 22】

非管理の属性を識別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 19 の方法。

【請求項 23】

選択されたデータオブジェクトと属性と規定されたアクセス許可のうちの少なくとも 1 つを変更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 19 の方法。

【請求項 24】

次の時間に、前記少なくとも 1 つのデータレポジトリ内のデータ構造に関する情報を見つけるように前記管理者を促す工程をさらに備える、請求項 19 の方法。

【請求項 25】

40

管理ツールを支援するようにコミュニティを構成する方法であって、

前記コミュニティに関するデータを含む少なくとも 1 つのデータレポジトリを識別する工程と、

前記少なくとも 1 つのデータレポジトリ内のデータ構造を見つける工程と、

見つめられた構造から前記オブジェクト内のデータオブジェクトと属性を選択する工程と、

選択された属性を管理するためのアクセス許可を規定する工程と、

前記管理ツールを利用して、選択されたデータオブジェクトと属性と規定されたアクセス許可に基づいて前記コミュニティを管理する工程を備える方法。

【請求項 26】

50

少なくとも1つのデータレポジトリを識別する前記工程は、前記少なくとも1つのデータレポジトリに格納されたデータをアクセスするための接続情報を特定することを備える、請求項25の方法。

【請求項27】

少なくとも1つのデータレポジトリを識別する前記工程は、様々な構造をもつデータレポジトリから選択することを備える、請求項25の方法。

【請求項28】

管理される属性を識別する工程をさらに備える、請求項25の方法。

【請求項29】

アクセス許可を規定する前記工程は、選択された属性に関して実行できるかもしくはできないオペレーションを確認することを備える、請求項25の方法。 10

【請求項30】

アクセス許可を規定する前記工程は、選択された属性の一部に対する限定値を特定することを備える、請求項25の方法。

【請求項31】

選択されたデータオブジェクトと属性と規定されたアクセス許可のうちの少なくとも1つを変更する工程をさらに備える、請求項25の方法。

【請求項32】

次の時間に、前記少なくとも1つのデータレポジトリ内のデータ構造に関する情報を再発見する工程をさらに備える、請求項25の方法。 20

【請求項33】

コミュニティを管理するために必要な情報を確立するためのツールであって、前記コミュニティに関するデータを含む少なくとも1つのデータレポジトリを識別するデータレポジトリ識別子コンポーネントと、前記少なくとも1つのデータレポジトリ内のデータ構造を見つけるデータ構造発見コンポーネントと、前記データ構造発見コンポーネントによって見つけられた構造に基づいて、オブジェクト内のデータオブジェクトと属性を選択するデータ選択コンポーネントと、前記データ選択コンポーネントによって選択された属性を管理するためのアクセス許可を規定するアクセス許可コンポーネントを備えるツール。 30

【請求項34】

前記データレポジトリ識別子コンポーネントは、前記少なくとも1つのデータレポジトリに記憶されたデータをアクセスするための接続情報を特定する、請求項33のツール。

【請求項35】

前記データレポジトリ識別子コンポーネントは、様々な構造をもつデータレポジトリから選択する、請求項33のツール。

【請求項36】

前記データ構造発見コンポーネントは、前記少なくとも1つのデータレポジトリ内に存在するデータオブジェクトと属性を確認する、請求項33のツール。

【請求項37】

前記データ選択コンポーネントは、管理される属性を識別する、請求項33のツール。 40

【請求項38】

前記アクセス許可コンポーネントは、選択された属性に関して実行できるかもしくはできないオペレーションを確認する、請求項33のツール。

【請求項39】

前記アクセス許可コンポーネントは、選択された属性の一部に対する限定値を特定する、請求項33のツール。

【請求項40】

選択されたデータオブジェクトと属性と規定されたアクセス許可のうちの少なくとも1つを変更する変更コンポーネントをさらに備える、請求項33のツール。 50

【請求項 4 1】

次の時間に、前記少なくとも 1 つのデータレポジトリ内のデータ構造に関する情報を再発見する再発見情報コンポーネントをさらに備える、請求項 3 3 のツール。

【請求項 4 2】

コミュニティを管理するために必要な情報を確立するためのツールであって、前記コミュニティに関するデータを含む少なくとも 1 つのデータレポジトリを識別する手段と、

前記少なくとも 1 つのデータレポジトリ内のデータ構造を見つける手段と、

前記見つける手段によって見つけられた前記構造に基づいて前記オブジェクト内のデータオブジェクトと属性を選択する手段と、

前記選択する手段によって選択された属性を管理するためのアクセス許可を規定する手段を備えるツール。

10

【請求項 4 3】

前記識別する手段は、様々な構造をもつデータレポジトリから選択する、請求項 4 2 のツール。

【請求項 4 4】

前記見つける手段は、前記少なくとも 1 つのデータレポジトリ内に存在するデータオブジェクトと属性を確認する、請求項 4 2 のツール。

【請求項 4 5】

前記選択する手段は非管理の属性を識別する、請求項 4 2 のツール。

20

【請求項 4 6】

前記選択されたデータオブジェクトと属性と規定されたアクセス許可のうちの少なくとも 1 つを変更する手段をさらに備える、請求項 4 2 のツール。

【請求項 4 7】

次の時間に、前記少なくとも 1 つのデータレポジトリ内のデータ構造に関する情報を再発見する手段をさらに備える、請求項 4 2 のツール。

【請求項 4 8】

コミュニティを管理するために必要な情報を確立するシステムであって、

複数のコミュニティ情報を備える少なくとも 1 つのデータレポジトリと、

前記少なくとも 1 つのデータレポジトリ内の情報を確立して前記コミュニティを管理するツールであって、前記コミュニティに関するデータを含む少なくとも 1 つのデータレポジトリを識別するデータレポジトリ識別子コンポーネントと、前記少なくとも 1 つのデータレポジトリ内のデータ構造を見つけるデータ構造発見コンポーネントと、前記データ構造発見コンポーネントによって見つけられた構造に基づいてオブジェクト内のデータオブジェクトと属性を選択するデータ選択コンポーネントと、前記データ選択コンポーネントによって選択された属性を管理するためのアクセス許可を規定するアクセス許可コンポーネントを備える、当該ツールと、

30

前記ツールを提供するように構成される第 1 の計算部を備えるシステム。

【請求項 4 9】

ネットワークを介して前記第 1 の計算部から提供される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 4 8 のシステム。

40

【請求項 5 0】

前記データレポジトリ識別子コンポーネントは、前記少なくとも 1 つのデータレポジトリに記憶されたデータをアクセスするための接続情報を特定する、請求項 4 8 のシステム。

【請求項 5 1】

前記データレポジトリ識別子コンポーネントは、様々な構造をもつデータレポジトリから選択する、請求項 4 8 のシステム。

【請求項 5 2】

前記データ構造発見コンポーネントは、前記少なくとも 1 つのデータレポジトリ内に存在するデータオブジェクトと属性を確認する、請求項 4 8 のシステム。

50

【請求項 5 3】

前記データ選択コンポーネントは、非管理の属性を識別する、請求項 4 8 のシステム。

【請求項 5 4】

前記アクセス許可コンポーネントは、選択された属性に関して実行できるかもしくはできないオペレーションを確認する、請求項 4 8 のシステム。

【請求項 5 5】

前記アクセス許可コンポーネントは、選択された属性の一部に対する限定値を特定する、請求項 4 8 のシステム。

【請求項 5 6】

前記ツールは、前記選択されたデータオブジェクトと属性と規定されたアクセス許可のうちの少なくとも 1 つを変更する変更コンポーネントをさらに備える、請求項 4 8 のシステム。 10

【請求項 5 7】

前記ツールは、次の時間に、前記少なくとも 1 つのデータレポジトリ内のデータ構造に関する情報を再発見する再発見情報コンポーネントをさらに備える、請求項 4 8 のシステム。

【請求項 5 8】

コミュニティを管理するために必要な情報を確立するようにコンピュータシステムを命令するコンピュータインストラクションを記憶するコンピュータ読取可能媒体であって、前記コンピュータインストラクションは、 20

前記コミュニティに関するデータを含む少なくとも 1 つのデータレポジトリを識別する工程と、

前記少なくとも 1 つのデータレポジトリ内のデータ構造を見つける工程と、

データオブジェクトと前記オブジェクトの属性を選択して、見つけられた構造から管理する工程と、

前記選択された属性を管理するためのアクセス許可を規定する工程を備える、コンピュータ読取可能媒体。

【請求項 5 9】

少なくとも 1 つのデータレポジトリを識別する前記工程は、前記少なくとも 1 つのデータレポジトリに記憶されたデータをアクセスするための接続情報を特定するインストラクションを備える、請求項 5 8 のコンピュータ読取可能媒体。 30

【請求項 6 0】

構造を見つける前記工程は、前記少なくとも 1 つのデータレポジトリ内に存在するデータオブジェクトと属性を確認するインストラクションを備える、請求項 5 8 のコンピュータ読取可能媒体。

【請求項 6 1】

非管理の属性を識別するインストラクションをさらに備える、請求項 5 8 のコンピュータ読取可能媒体。

【請求項 6 2】

アクセス許可を規定する前記工程は、選択された属性に関して実行できるかもしくはできないオペレーションを確認するインストラクションを備える、請求項 5 8 のコンピュータ読取可能媒体。 40

【請求項 6 3】

アクセス許可を規定する前記工程は、前記選択された属性の一部に対する限定値を特定するインストラクションを備える、請求項 5 8 のコンピュータ読取可能媒体。

【請求項 6 4】

選択されたデータオブジェクトと属性と規定されたアクセス許可のうちの少なくとも 1 つを変更するインストラクションをさらに備える、請求項 5 8 のコンピュータ読取可能媒体。を備える、請求項 5 8 のコンピュータ読取可能媒体。

【請求項 6 5】

次の時間に、前記少なくとも1つのデータレポジトリ内のデータ構造に関する情報を再発見するインストラクションをさらに備える、請求項58のコンピュータ読取可能媒体。

【請求項66】

情報を再発見する前記工程は、前記少なくとも1つのデータレポジトリ内に存在するデータオブジェクトと属性を確認するインストラクションを備える、請求項65のコンピュータ読取可能媒体。

【請求項67】

新しいデータオブジェクトと属性を選択して管理するインストラクションをさらに備える、請求項66のコンピュータ読取可能媒体。

【請求項68】

管理者がコミュニティを管理するために必要な情報を確立できるようにコンピュータシステムを命令するコンピュータインストラクションを記憶するコンピュータ読取可能媒体であって、前記コンピュータインストラクションは、
前記コミュニティに関するデータを含む少なくとも1つのデータレポジトリを識別する工程と、

前記少なくとも1つのデータレポジトリ内のデータ構造を見つける工程と、
見つめられた構造からデータオブジェクトと前記オブジェクトの属性を選択するように前記管理者を促す工程と、
選択された属性を管理するためのアクセス許可を規定するように前記管理者を促す工程を備える、コンピュータ読取可能媒体。

【請求項69】

少なくとも1つのデータレポジトリを識別する前記工程は、前記少なくとも1つのデータレポジトリに記憶されたデータをアクセスするための接続情報を特定するインストラクションを備える、請求項68のコンピュータ読取可能媒体。

【請求項70】

構造を見つける前記工程は、前記少なくとも1つのデータレポジトリに存在するデータオブジェクトと属性を確認するインストラクションを備える、請求項68のコンピュータ読取可能媒体。

【請求項71】

非管理の属性を識別するように前記管理者を促すインストラクションをさらに備える、請求項68のコンピュータ読取可能媒体。

【請求項72】

前記選択されたデータオブジェクトと属性と規定されたアクセス許可のうちの少なくとも1つを変更するように前記管理者を促すインストラクションをさらに備える、請求項68のコンピュータ読取可能媒体。

【請求項73】

次の時間に、前記少なくとも1つのデータレポジトリ内の前記データ構造に関する情報を再発見するように前記管理者を促すインストラクションをさらに備える、請求項68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】

【0001】

本開示は一般的にコミュニティに関し、特に、コミュニティを管理するために必要な情報を確立して保守することに関する。

【背景技術】

【0002】

一般的に、コミュニティは概して共通の利益を共有する人のグループである。インターネットと電子商取引の到来によって、多くの会社では従業員とサプライヤとパートナーとクライアントのためにイントラネットとエクストラネットを介してコミュニティを形成する。コミュニティは、従業員とサプライヤとパートナーとクライアントが一緒に働くことを

10

20

30

40

50

容易にし、また、費用がかからないようにするものである。コンピュータサービス環境では、これらの人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の情報は、幅広い範囲のディレクトリとデータベースに格納される。情報には、ユーザ名や住所や電話番号や組織やログイン識別子やパスワードなどの項目が含まれていてもよい。その他の情報には、アプリケーションと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いてもよい。また、ディレクトリとデータベースには、コミュニティを支援するネットワーク内の物理デバイス（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）の情報を記憶することができる。さらに別の情報には、各物理デバイスにとって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プリントキューなど）が含まれていてもよい。 10

【0003】

一般的に、管理ツールはコミュニティに関する全情報を管理する。ほとんどの管理ツールが直面する問題は、情報を記憶するディレクトリやデータベースが互いに大きく異なる構造をもつことである。最も商業的に入手可能な管理ツールには、広範囲に渡るディレクトリとデータベースに記憶される情報を管理する能力がない。このため、様々なディレクトリとデータベースに情報を記憶するコミュニティの管理者は1つ以上の管理ツールを使って情報を管理することが多い。何故ならば、1つのツールだけでは、構造とコンテンツが異なる情報を探し、識別し、特徴づけることができないからである。例えば、組織では、組織がライセンスを与えたソフトウェアに関する軽量ディレクトリアクセスプロトコル（L D A P）のディレクトリと情報などの、ディレクトリ内のカスタマ情報をデータベースに格納するとしたならば、情報の構造とコンテンツは異なるので、管理者は1つ以上の管理ツールを利用することによって両方のコミュニティを管理することができる。従って、様々な構造化された個別のディレクトリとデータベースに情報が存在する様々なコミュニティを管理ツールが管理できる方法が必要である。 20

【発明の開示】

【発明が解決しようとする課題】

【0004】

幅広い範囲のディレクトリとデータベースに記憶されているコミュニティ情報に関するその他の問題は、ディレクトリとデータベースから管理される情報を現在利用可能な管理ツールで確立することが困難なことである。一般的に、ディレクトリとデータベースに格納されたデータには幅広く様々な情報が含まれている。（例えば、名前や住所などの）データの一部はユーザによって管理され、（例えば、ユーザやリソースの特徴などの）データの一部は管理者によって管理される。一般的に、その他にも、管理者によって管理される必要のないユーザに自動的に関わることの多いデータが多く存在する。管理者によって管理される必要のないその他のデータには、ディレクトリとデータベース内で未使用か、もしくは、自動的に更新されるデータフィールドが含まれる。コミュニティを管理するために、管理されるディレクトリやデータベースのデータのサブセットを切り出して、その残りを明示的に無視することが望ましい。また、ディレクトリとデータベースの構造が変化すると、その変化を見つけて新しいデータ要素を管理するか否かを決定することが望ましい。従って、ディレクトリとデータベースから管理される情報を管理ツールで確立できる方法が必要であるが、これには、管理される情報と管理されない情報を規定して、管理する新しい情報を見つけることが含まれる。 30 40

【課題を解決するための手段】

【0005】

本開示の一実施形態には、コミュニティを管理するために必要な情報を確立する方法とシステムと、それを実行するようにコンピュータシステムに命令するインストラクションを記憶するコンピュータ読取可能媒体がある。本実施形態によれば、コミュニティに関連するデータを含む少なくとも1つのデータレポジトリが識別される。少なくとも1つのデータレポジトリのデータ構造が見つけられる。見つけられた管理構造からデータオブジェク 50

トとオブジェクトの属性が選択される。選択された属性を管理するためのアクセス許可が規定される。

【0006】

本開示の第2の実施形態によれば、コミュニティを管理するために必要な情報を管理者に確立させるシステムと方法と、それを実行するようにコンピュータシステムを命令するインストラクション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、コミュニティに関連するデータを含む少なくとも1つのデータレポジトリが識別される。少なくとも1つのデータレポジトリのデータ構造が見つけられる。管理者は、見つけられた構造からデータオブジェクトとオブジェクトの属性を選択して、選択された属性を管理するためのアクセス許可を規定するように促される。その他の一実施形態によれば、コミュニティを管理するために必要な情報を確立するツールがある。ツールは、コミュニティに関連するデータを含む少なくとも1つのデータレポジトリを識別するデータレポジトリ識別子コンポーネントを備える。データ構造発見コンポーネントは、少なくとも1つのデータレポジトリ内のデータ構造を見つける。データ選択コンポーネントは、データ構造発見コンポーネントによって見つけられた構造に基づいてデータオブジェクトとオブジェクトの属性を選択する。アクセス許可コンポーネントは、データ選択コンポーネントによって選択された属性を管理するためのアクセス許可を規定する。

10

【0007】

さらに別の一実施形態によれば、コミュニティを管理するために必要な情報を確立するシステムがある。本システムは、複数のコミュニティ情報を含む少なくとも1つのデータレポジトリを備える。ツールは、少なくとも1つのデータレポジトリの情報を確立することによってコミュニティを管理する。ツールは、コミュニティに関連するデータを含む少なくとも1つのデータレポジトリを識別するデータレポジトリ識別子コンポーネントを備える。データ構造発見コンポーネントは、少なくとも1つのデータレポジトリ内のデータ構造を見つける。データ選択コンポーネントは、データ構造発見コンポーネントによって見つけられた構造に基づいてデータオブジェクトとオブジェクトの属性を選択する。アクセス許可コンポーネントは、データ選択コンポーネントによって選択された属性を管理するためのアクセス許可を規定する。計算部は、ツールを提供するように構成される。

20

【発明を実施するための最良の形態】

【0008】

本開示では、現在利用可能な管理ツールを使って幅広い範囲のディレクトリとデータベースに記憶されたコミュニティ情報の管理に関する問題を克服する方法を説明する。特に、本方法は、管理されるコミュニティの生成と構築とその次の変更を容易にすることによって、現在利用可能な管理ツールは、コミュニティに関する構造と情報のコンテンツに無関係に、コミュニティを管理することができる。本方法では、管理されるコミュニティを構築することには、潜在的に管理されるコミュニティに関連する、ディレクトリとデータベースなどのデータレポジトリに記憶された情報やデータを見つけることが含まれる。また、構築には、管理される特定のデータ要素や属性と非管理の属性を識別するために行うユーザとの相互作用が含まれる。また、構築の際に利用されるプロセスをその次の変更の際に利用したり、管理されるコミュニティを更新することもできる。管理されるコミュニティの生成と構築と変更の際に利用される同じプロセスを使って、複数の個別のコミュニティを管理することができる。

30

40

【0009】

一例では、管理されるコミュニティを作成し構築し変更する方法をソフトウェアで実施することができる。図1は、コミュニティを管理するために必要な情報を確立するツールを実施する汎用コンピュータシステム10の図を示す。一般的に、コンピュータシステム10は、少なくとも1つのプロセッサ12とメモリ14と入出力デバイスと、プロセッサとメモリと入出力デバイス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からインストラクションとデータを受け入れて様々な計算を実行する。プロセッサ12には、算術論理オペレーションを実行する演算論理回路（ALU）と

50

、メモリ14からインストラクションを抽出しデコードして実行する制御部が含まれており、必要に応じてALUを利用する。一般的に、メモリ14には、ランダムアクセスメモリ(RAM)と読出専用メモリ(ROM)が含まれるが、プログラマブル読出専用メモリ(PROM)と消去可能プログラマブル読出専用メモリ(EPROM)と電氣的消去可能プログラマブル読出専用メモリ(EEPROM)などのその他の種類のメモリでもよい。また、メモリ14は、プロセッサ12で実行されるオペレーティングシステムを含むことが好ましい。オペレーティングシステムは、入力情報を認識する基本タスクを実行して、出力装置に出力情報を送り、ファイルとディレクトリを追跡して様々な周辺装置を制御する。

【0010】

入出力デバイスは、データとインストラクションをコンピュータシステム10入力するキーボード18とマウス20を備えていてもよい。また、ユーザは、ディスプレイ22を利用することによってコンピュータの遂行結果を見ることができる。その他の出力装置には、プリンタとプロッタとシンセサイザとスピーカが含まれていてもよい。電話やケーブルモデムなどの通信デバイス24や、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)アダプタや統合デジタル通信網(ISDN)アダプタやデジタル加入者ライン(DSL)アダプタなどのネットワークカードは、コンピュータシステム10が、LANやワイドエリアネットワーク(WAN)などのネットワーク上のその他のコンピュータとリソースをアクセスすることを可能にするものである。大容量記憶装置26を利用することによって、コンピュータシステム10は大量のデータを永久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)とハードディスクと光ディスクなどの全ての種類のディスクドライブと、デジタルオーディオテープ(DAT)やデジタルリニヤテープ(DLT)やその他の磁氣的符号化媒体を含むテープに対してデータの読み書きを行うことができるテープドライブが含まれる。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の形態をとることができる。

【0011】

図2は、コミュニティを管理するために必要な情報を確立し、図1に示されるコンピュータシステム10で動作するツール28のトップレベルのコンポーネントアーキテクチャ図を示す。一般的に、トップレベルの管理者は、ツール28を利用するが、本開示では上級管理者と呼ばれる。上級管理者が一般的に実行する機能の一部には、本開示で記述されたソフトウェアツールをインストールし、1つ以上のデータレポジトリとリンクするようなインストールを構築し、管理されるデータを識別し、自己管理されるデータを識別し、以前に選択されたデータの管理に、選択されたユーザを割り当てることが含まれる。ツール28は、ユーザコミュニティに関連するデータを含む少なくとも1つのデータレポジトリを識別するデータレポジトリ識別子コンポーネント30を備える。データレポジトリ識別子コンポーネント30が識別する少なくとも1つのデータレポジトリには、様々な構造をもつ複数のレポジトリが含まれていてもよい。また、データレポジトリ識別子コンポーネント30は、少なくとも1つのデータレポジトリに記憶されたデータをアクセスするための接続情報を調べる。接続情報例には、これに限定されることはないが、少なくとも1つのデータレポジトリと、少なくとも1つのレポジトリとインターフェイスするポートと、少なくとも1つのレポジトリに対するログイン識別子と、少なくとも1つのレポジトリをアクセスするためのパスワードのためのアクセスを提供するサーバが含まれる。

【0012】

データ構造発見コンポーネント32は、少なくとも1つのデータレポジトリ内のデータ構造を見つける。特に、データ構造発見コンポーネント32は、少なくとも1つのデータレポジトリに存在するデータオブジェクトと属性を確認する。一般的に、少なくとも1つのデータレポジトリ内でデータオブジェクトがどのように定義されているかを最初に調べる

10

20

30

40

50

ために、標準データベースに関する問い合わせが実行される。上級管理者が、管理されたユーザを含むデータオブジェクトを選択した後で、どの属性がオブジェクトに関連するの
かを確認するためにさらに別の問い合わせがなされる。

【0013】

上級管理者はデータ選択コンポーネント34を利用して、データ構造発見コンポーネント
32によって見つけられたデータオブジェクトと属性を選択することができる。特に、上
級管理者は、見つけられたオブジェクトと属性のどれを管理すべきかを決定する。見つけ
られたオブジェクトとクラスの全てを管理する必要はない。どのオブジェクトと属性をコ
ミュニティ内で管理すべきかを選ぶことは上級管理者の裁量に任せられる。一般的に、そ
の選択はコミュニティ毎に異なるものである。また、上級管理者はデータ選択コンポーネ
ント34を利用して、管理されるユーザコミュニティ内で未使用であることがわかったオ
ブジェクトと属性を識別することができる。例えば、ツール28を実施するために使われ
、例えば、システム状態を把握したりシステムの事象の日時を追跡するための属性は、コ
ミュニティの管理者によって変更されるべきではない。管理すべきでないその他の属性例
には、編集すべきでなかったり直接閲覧されるべきでない内部生成されたデータや、単に
未使用であるか決して変更されることのないデータフィールドが含まれる。そのような属
性に対して、上級管理者はデータ選択コンポーネント34を利用してそれらの属性を識別
するので、それらはコミュニティ内で管理されることはない。

10

【0014】

上級管理者はアクセス許可コンポーネント36を利用して、データ選択コンポーネント3
4によって選択された属性を管理するためのアクセス許可を規定することができる。上級
管理者によって規定されるアクセス許可とは、特定のコミュニティの管理者が特定の属性
に関してどのような役割を果たすことができるのかを決定するものであって、特に、ア
クセス許可は、コミュニティで規定された属性に関して管理者が実行できるかもしくはでき
ないオペレーションの種類が何であるかを規定するものである。上級管理者が受け入れる
ことのできるオペレーションの中には、属性を閲覧したり編集したり削除することが含ま
れる。これらの管理オペレーションは、上級管理者がアクセス許可を受け入れることが
できる幾つかのオペレーションだけの説明に役立つものであって、その他の可能性を網羅す
るものではない。受け入れ可能なその他の管理オペレーションの例には、特定の期間編集
したり、データフィールドをデフォルト値にリセットすることがある。一般的に、上級
管理者は、属性に対してできることとできないことを限定するために、アクセス許可コン
ポーネント36を利用してこれらのオペレーションに対するアクセス許可を受け入れるか
、もしくは拒否することができる。属性に対するアクセス許可の選択は上級管理者に任せ
られる。尚、上述のオペレーションのうちの1つや、オペレーションの組み合わせに対す
るアクセス許可を受け入れることは可能である。

20

30

【0015】

また、アクセス許可コンポーネント36によって、上級管理者は、選択された属性の一部
に対して限定値を与えることができる。例えば、ユーザが雇用されている州に関するデー
タ（例えば、雇用の州）を含む属性に対する値は、50個の値のうちの1つに限定するこ
とができる。ここで、その値は2文字略語（例えば、W IやN Yなど）に限定される。1
つの属性に対して値を限定できるその他の例には、ユーザが利用できるアプリケーション
をリストする属性がある。この例では、このアプリケーション属性の値を、C a t a l o
gやA u c t i o nやE m a i lやC h a tやW e bなどの特定の名前に限定してもよい
。さらに、ユーザ属性の一部が同様の限定値をもつことも可能である。さらに、複数のデ
ータレポジトリに対する特定の限定属性のセットを用いてもよい。

40

【0016】

変更コンポーネント38によって、上級管理者は、コミュニティの初期構成を変更したり
更新することができる。特に、上級管理者は、変更コンポーネント38を利用して、サー
バとポートとログイン識別子とパスワード情報などの少なくとも1つのデータレポジトリ
に対する接続情報を変更することができる。また、管理のために以前に選択したデータオ

50

プロジェクトと属性を変更することができる。また、これには、管理されるコミュニティで未使用と識別された属性を変更することが含まれる。さらに、変更コンポーネント38を利用して、属性に対して規定されたアクセス許可と、属性に特定された限定値を変更することもできる。

【0017】

再発見情報コンポーネント40によって、上級管理者は、コミュニティの活動後の時間で少なくとも1つのデータレポジトリ内のデータ構造に関する情報を見つけることができる。一般的に、初期的な発見の後に、少なくとも1つのデータレポジトリはさらに別の規定された属性をもつことがあるので、再発見が必要となる場合がある。例えば、古いレポジトリの一部には、Eメールアドレスやファックス番号や個人ホームページのリファレンスを記憶する属性がない場合がある。これらの属性が少なくとも1つのレポジトリに追加される場合は、この情報を再発見して管理属性に入れることが必要となる。また、レポジトリを正確に見るためには、基礎的なデータレポジトリが変更されたときはいつでも再発見することが望ましい。

10

【0018】

オブジェクトクラスと属性を再発見するために、再発見情報コンポーネント40は、オブジェクトクラスと属性を求めて少なくとも1つのデータレポジトリをサーチする。上級管理者は再発見情報コンポーネント40を利用して、管理するさらに別のオブジェクトと属性を選択することができる。新しい属性がコミュニティの管理に役立たない場合は、上級管理者は、それを非管理として識別する。次に、上級管理者は、選択された新しい属性と、属性に対して指定されるべき限定値に対するアクセス許可を決定する。

20

【0019】

ツール28は、ソフトウェアによる実施に限定されることはない。例えば、データレポジトリ識別子コンポーネント30とデータ構造発見コンポーネント32とデータ選択コンポーネント34とアクセス許可コンポーネント36と変更コンポーネント38と再発見情報コンポーネント40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み合わせの形態をとってもよい。

【0020】

さらに、ツール28は、データレポジトリ識別子コンポーネント30とデータ構造発見コンポーネント32とデータ選択コンポーネント34とアクセス許可コンポーネント36と変更コンポーネント38と再発見情報コンポーネント40に限定されることはない。当業者であれば、ツール28がその他のコンポーネントを備えてもよいことを理解することができる。例えば、ツール28には、ユーザの生成と管理に関するプロセスを管理するワークフローコンポーネントがさらに含まれていてもよい。また、ツール28には、利用統計やエラー状態などを含む報告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。ツール28が備えることができるその他のコンポーネントには、コミュニティ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

【0021】

図3は、図2に示されるツールを実現するためのシステム42のアーキテクチャ図を示す。図3は、ツール28をアクセスするために幾つかの方法があることを示す。計算部44によって、上級管理者はツール28をアクセスすることができる。計算部44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の形態をとることができる。上級管理者は、Microsoft INTERNET EXPLORERやNetscape NAVIGATORなどのウェブブラウザ46を利用して、計算部44で管理ツール28を探して表示することができる。電子もしくは無線のネットワークなどの通信ネットワークは、計算部44をツール28に接続するものである。図3は、イクストラネットやイントラネットなどの個人ネットワーク48や、WAN（例えば、インターネット）などのグローバルネットワーク50を介して計算部44をツール28に接続するこ

40

50

とができることを示す。図 3 に示されているように、ツール 28 は、ツール 28 と、コミュニティに関する様々な情報を含むデータレポジトリ 56（もしくは、複数のレポジトリ）を提供するウェブサーバ 54 を備えるサーバ 52 に存在する。しかしながら、ツールはサーバ 52 と共存する必要はない。必要に応じて、システム 42 は、ツール 28 をアクセスするための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。ツール 28 自体によって、もしくは、Netegrity S I T E M 1 N D E R などの市販のパッケージによって、ウェブサーバレベルで認証とアクセス制御の両方を処理することができる。

【0022】

上述のデータレポジトリもしくは複数のレポジトリ 56 の情報には、名前や住所や電話番号や組織やログイン識別子やパスワードなどの、コミュニティのユーザに関するコミュニティ情報が含まれる。その他の情報には、アプリケーションとコンテンツなどの特定のリソースに対するユーザのアクセス特権が含まれていてもよい。また、データレポジトリもしくは複数のレポジトリ 56 は、コミュニティを支援するネットワーク内の物理デバイス（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することができる。データレポジトリもしくは複数のレポジトリ 56 に記憶されたさらに別の情報には、各物理デバイスにとって利用可能なサービス（例えば、オペレーティングシステム、アプリケーション、共有ファイルシステム、プリントキューなど）が含まれていてもよい。データレポジトリやレポジトリ 56 には、データを格納するための様々な構造をもつディレクトリとデータベースなどのレポジトリが含まれていてもよい。データレポジトリの例には、これに限定されることはないが、L D A P ディレクトリとリレーショナルデータベースとオブジェクト指向データベースと平ファイルとデータ管理システムと、その他の種類のスキーマをもつその他のディレクトリ型データベースがある。

【0023】

図 3 に示されるシステム 42 を利用して、上級管理者などの管理者はツール 28 を利用して、ユーザコミュニティなどのコミュニティを確立し維持することができる。図 4 は、ツール 28 を利用してコミュニティ管理を初期的に構築するように実施される処理を説明するフローチャートを示す。ブロック 58 では、上級管理者がサインインする。サインインの行為には、アイデンティティとセキュリティ情報（例えば、有効なユーザ名前とパスワード）を入力することが含まれていてもよい。60 では、ツールはユーザ名前とパスワードを認証する。次に、62 では、ツールは、コミュニティを構築するための許可をユーザが受けている（即ち、ユーザは上級管理者である）かどうかを確認する。ユーザが認証されていないか、もしくはコミュニティを構築するための許可を受けていない場合は、ユーザはコミュニティを構築することができない。

【0024】

64 では、上級管理者はツールをインストールし、コミュニティ情報を含む少なくとも 1 つのデータレポジトリを識別する。このインストールでは、上級管理者は、サーバとポートの情報などの少なくとも 1 つのデータレポジトリ内に格納されたデータをアクセスするための接続情報と、少なくとも 1 つのレポジトリをアクセスするための識別子とパスワードを入力する。尚、少なくとも 1 つのデータレポジトリが既に存在する可能性があり、この場合には、上級管理者が単に接続情報をツールに提供する必要がある。次に、66 では、そのスキーマを見つけるために、ツールは少なくとも 1 つのデータレポジトリに接続される。上述したが、この発見段階では、ツールはどのデータオブジェクトと属性が少なくとも 1 つのデータレポジトリ内に存在するかを知る。まず、68 では、少なくとも 1 つのデータレポジトリ内のデータオブジェクトが発見される。次に、70 では、上級管理者は、管理されるユーザを編成するデータオブジェクトを選択する。72 では、データ選択コンポーネントを利用して、選択されたデータオブジェクトの属性を知ることができる。次に、74 では、データ選択コンポーネントを利用して、非管理の属性を識別することができる。

10

20

30

40

50

【0025】

76では、上級管理者は、ユーザによって自己管理可能な属性を選択する。上述したように、自己管理可能な一部の属性にはユーザ名や住所や電話番号などが含まれていてもよい。次に、78では、上級管理者はアクセス許可コンポーネントを利用して、アクセス許可を規定して、自己管理のために選択された属性に対してユーザができることを規定することができる。80では、上級管理者はデータ選択コンポーネントを利用して、管理者によって管理される属性を選択し、82では、アクセス許可コンポーネントによって、選択された属性に関して管理者が（例えば、編集や閲覧や削除などの）行為をどのように行え、また、行えないのかを規定することができる。

【0026】

次に、84では、上級管理者は属性を識別するが、その属性はその属性に関する限定値をもつ。また、このブロックでは、上級管理者は、識別されて限定値をもつ属性に許容可能な値を割り当てる。次に、86では、初期的な全構築データを退避する。コミュニティが構築されると、管理ツールはコミュニティを管理することができる。特に、管理ツールを利用して、様々な領域とサブ領域とを設定し、これらの領域を管理するための権限を与えることができる。

【0027】

図5は、ツール28を利用して既存の構成を変更するためになされる処理を説明するフローチャートを示す。ブロック88では、上級管理者は、アイデンティティとセキュリティ情報（例えば、有効なユーザ名とパスワード）を入力することによってサインインする。90では、ツールはユーザ名とパスワードを認証し、92では、ユーザが既存の構成を変更するための許可を受けているか（即ち、ユーザは上級管理者である）どうかを確認する。ユーザが認証されていないか、もしくは、コミュニティを構成するための許可を受けていない場合は、ユーザは既存の構成を変更することができない。94では、上級管理者は、変更したい特定の構成を選択する。次に、96では、ツールは、選択した構成を分析して構築データを獲得し、上級管理者に提供する。次に、98では、上級管理者は構成に対する変更を行う。この変更には、オブジェクトや属性やアクセス許可や限定値属性や接続情報などを変更したり追加したり削除することが含まれていてもよい。変更によって非管理として指定された属性に影響が及ぶ場合は、その変更に注釈がつけられる。変更後の100では、変更された構築データが更新される。

【0028】

図6は、ツール28を利用して少なくとも1つのデータレポジトリの再発見時に行われる処理を説明するフローチャートを示す。ブロック102では、上級管理者は、アイデンティティとセキュリティ情報（例えば、有効なユーザ名前とパスワード）を入力することによってサインインする。104では、ツールはユーザ名前とパスワードを認証して、106では、ユーザがデータを再発見するための許可を受けている（即ち、ユーザは上級管理者である）かどうかを確認する。ユーザが認証されていないか、もしくは、データを再発見するための許可を受けていない場合は、ユーザはそれを行うことができない。108では、上級管理者は、再発見するための少なくとも1つのデータレポジトリを選択する。110では、ツールは、少なくとも1つのデータレポジトリを這うように進んで、少なくとも1つのデータレポジトリ内のデータオブジェクトと属性を見つけ、112では、その結果を上級管理者に提供する。次に、114では、図5で説明されたように、上級管理者は構成を変更する。変更後の116では、変更された構築データが更新される。基本的に、再発見プロセスによって、上級管理者は、（例えば、データオブジェクトの発見やオブジェクトの選択や属性の発見や属性の選択などの）初期的構成で実行される同じステップを実行することになる。

【0029】

図7は、ツール28を利用してアクセス許可と限定値属性を構成するように実行される処理を説明するフローチャートを示す。上述したように、上級管理者は、初期の構築時や構成の変更時にアクセス許可と限定値属性を構築することができる。ブロック118では、

10

20

30

40

50

上級管理者は、アイデンティティとセキュリティ情報（例えば、有効なユーザ名とパスワード）を入力することによってサインインする。120では、ツールはユーザ名とパスワードを認証し、122では、ユーザがアクセス許可と限定値属性を設定するための許可を受けている（即ち、ユーザは上級管理者である）かどうかを確認する。ユーザが認証されていないか、もしくは、アクセス許可と限定値属性を設定するための許可を受けていない場合は、ユーザはそれを行うことはできない。124では、ツールは、構築時に上級管理者によって選択された属性を得る。次に、126では、上級管理者は、各属性に関してどの種類のオペレーション（例えば、編集や閲覧や削除など）を管理者ができる、もしくはできないのかを規定するアクセス許可を識別する。次に、128では、上級管理者は、限定値をもつ属性を識別することができる。130では、上級管理者は、識別されて限定をもつ属性に許容可能な値が割り当てられる。次に、132ではその選択が更新される。 10

【0030】

本開示の上述のフローチャートは、ツールの機能とオペレーションを示すものである。この点で、各ブロックは特定の論理機能を実現するための1つ以上の実行可能なインストラクションを備えるモジュールやセグメントやコードの一部を表す。また、さらに別の実施形態では、ブロック内に記載された機能は、図で示されている順序とは別の順序で発生してもよい、例えば、実際に、関連する機能に基づいてほぼ同時にか、もしくは、逆順に実行してもよいことに注目されたい。また、当業者であれば、さらに別のブロックを追加してもよいことを理解することができる。さらに、C++やJ A V A（商標）などのプログラミング言語でその機能を実現してもよいが、その他の言語を使うことも可能である。 20

【0031】

上述のツールは、論理機能を実現するための実行可能なインストラクションの順序リストを備えている。順序リストは、インストラクションを取り込んで実行するコンピュータシステムによってか、もしくは、それと接続して使用するコンピュータ読取可能媒体で実現することができる。本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、インストラクションを含み記憶し送り伝達しトランスポートすることができる手段でよい。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によるシステムや装置やデバイスでよい。網羅的なものではないが説明に役立つコンピュータ読取可能媒体のリストには、1つ以上の電線と携帯型コンピュータディスク（磁気）とランダムアクセスメモリ（R A M）（磁気）と読出専用メモリ（R U M）（磁気）と消去可能プログラマブル読出専用メモリ（E P R O Mやフラッシュメモリ）（磁気）や光ファイバー（光学）や携帯型コンパクトディスク読出専用メモリ（C D R O M）（光学）を備える電気接続（電子）が含まれていてもよい。 30

【0032】

尚、コンピュータ読取可能媒体は、インストラクションが印刷される紙やその他の適切な媒体を備えていてもよい。例えば、インストラクションを、紙やその他の媒体を光学スキャンすることによって電子的に獲得し、次にコンパイルし、解釈するか、さもなければ、必要に応じて適切な方法で処理し、次に、コンピュータメモリに記憶させてもよい。

【0033】

本発明に基づいて、管理されるコミュニティを確立して維持するツールが提供されたことは明らかである。特に、好適な実施形態と共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修正や変更を行うことができることを理解することができる。 40

【図面の簡単な説明】

【0034】

【図1】図1は、コミュニティを管理するために必要な情報を確立するツールが動作する汎用コンピュータシステムの図を示す。

【図2】図2は、コミュニティを管理するために必要な情報を確立し、図1で示されるコンピュータシステムで実行されるツールのトップレベルのコンポーネントのアーキテクチャ図を示す。 50

【図 3】図 3 は、コミュニティを管理するために必要な情報を確立して保守するツールを実施するシステムのアーキテクチャ図を示す。

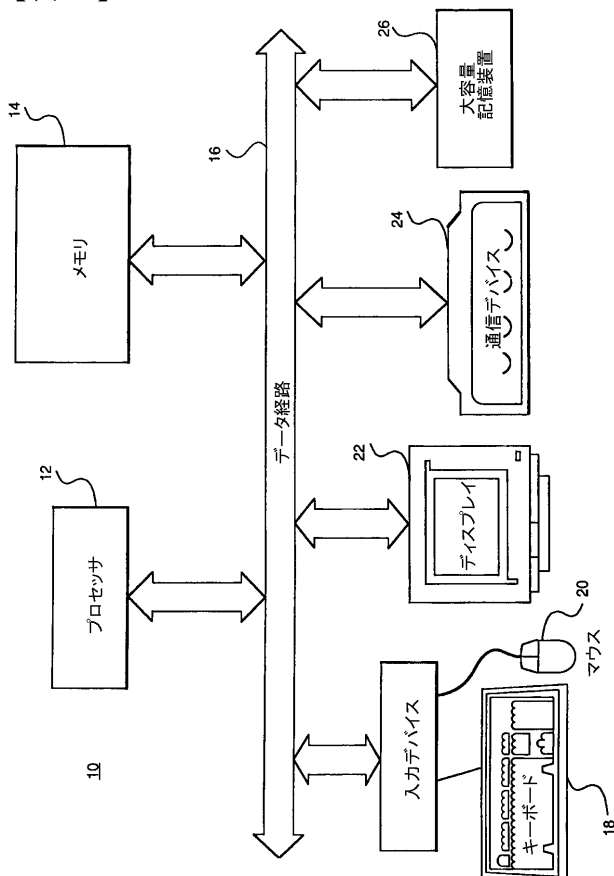
【図 4】図 4 は、図 2 で示されるツールを使ってコミュニティの管理を初期的に構成するように実行される処理を記述したフローチャートを示す。

【図 5】図 5 は、図 2 で示されるツールを使って既存の構成を変更するように実行される処理を記述したフローチャートを示す。

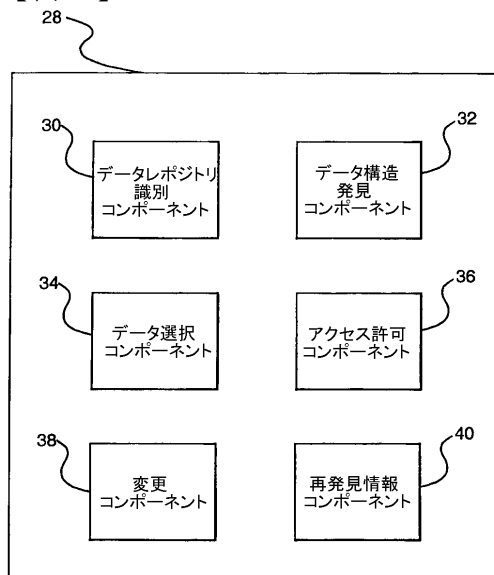
【図 6】図 6 は、図 2 で示されるツールを使って少なくとも 1 つのデータレポジトリ内のデータを再発見するように実行される処理を記述したフローチャートを示す。

【図 7】図 7 は、図 2 で示されるツールを使ってアクセス許可と限定値属性を構成するように実行される処理を記述したフローチャートを示す。

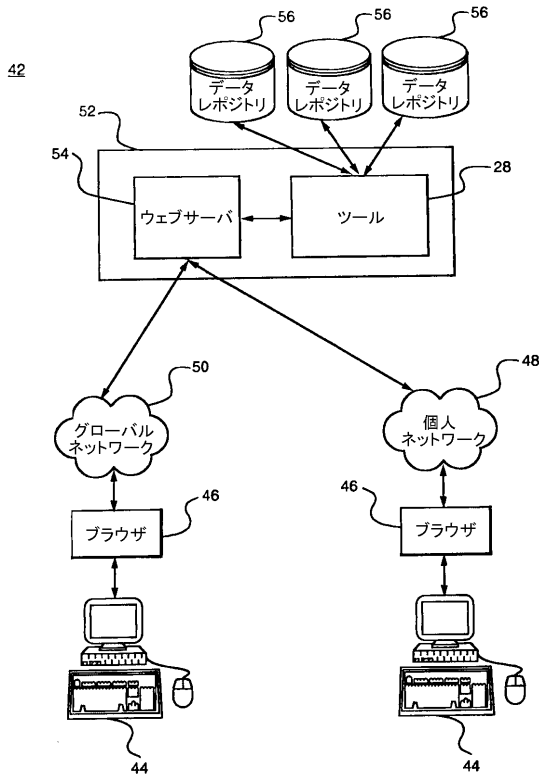
【図 1】



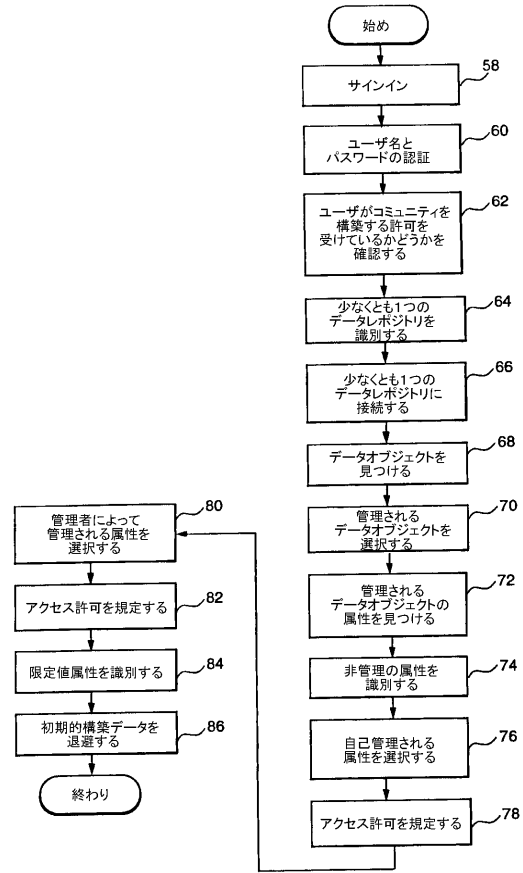
【図 2】



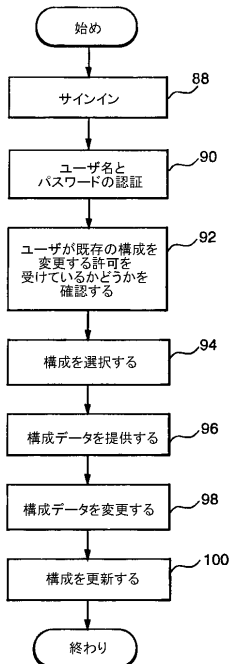
【図 3】



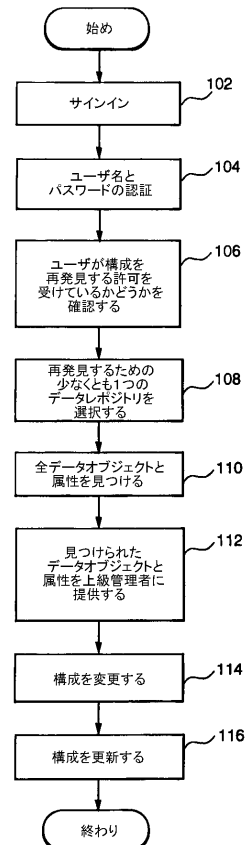
【図 4】



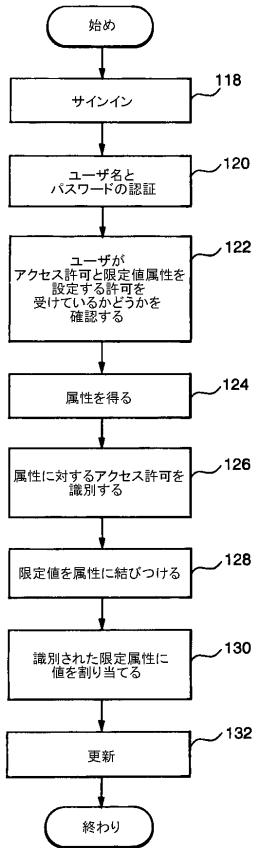
【図 5】



【図 6】



【図 7】



【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 02/057956 A1

(51) International Patent Classification: G06F 17/30

(21) International Application Number: PCT/US02/01330

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

(25) Filing Language: English

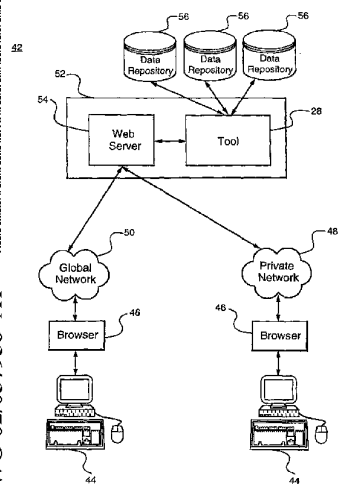
(26) Publication Language: English

(30) Priority Data: 09/760,998 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 Finnis Road,
Pattersonville, NY 12137 (US). VIVIER, Barbara, Jean;2577 Rosendale Road, Schenectady, NY 12309 (US). AG-
GOUR, Kareem, Sherif; 1506 Union Street, Apartment
3, Schenectady, NY 12309 (US). KORNFEIN, Mark,
Mitchell; 17 Omega Terrace, Latham, NY 12110 (US).
OSKOY, Osman, Rifki; 30 Grissom Drive, Clifton Park,
NY 12065 (US). WILLIAMS, Bassel, Omari; 185 Van
Rensselaer Boulevard, Bldg 26, Apt. 1A, Albany, NY
12204 (US).(74) Agents: CHASKIN, Jay, L. et al.; General Electric Com-
pany, 3135 Easton Turnpike WC3, Fairfield, CT 06431
(US).(81) Designated States (national): AE, AG, AL, AM, AT, AU,
AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU,
CZ, DE, DK, DM, DZ, 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, NO, NZ, OM, PI, PL, PT, RO, RU, SD, SE, SG,

[Continued on next page]

(54) Title: ESTABLISHMENT AND MAINTENANCE OF A MANAGED COMMUNITY



(57) Abstract: Establishment and maintenance of a managed community. In this disclosure there is an approach and tool that enables an administration tool (28) to manage communities whose information resides in separate and differently structured directories and databases (56). In addition, this disclosure describes an approach and tool (28) that enables an administration tool to establish information to be managed from the broad range of directories and databases (56), which includes defining information that is to be managed and information that is not to be managed and the discovering (32) of new information to manage.

WO 02/057956 A1

WO 02/057956 A1



SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN,
YU, ZA, ZM, ZW.

Published:
— with international search report

(84) **Designated States (regional):** ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SI, 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, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

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 02/057956

PCT/US02/01330

ESTABLISHMENT AND MAINTENANCE OF A MANAGED COMMUNITY

BACKGROUND OF THE INVENTION

This disclosure relates generally to a community and more particularly to establishing and maintaining information needed to manage a community.

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 and databases 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.

An administration tool typically manages all of the information associated with the community. A problem facing most administration tools is that the directories or databases that store the information can have structures that vary significantly from each other. Most commercially available administration tools do not have the capability to manage information stored in a broad range of directories and databases. Consequently, administrators of communities that store information in different directories and databases often have to use more than one administration tool to manage the information because a single tool is unable to locate, identify and characterize information that varies in structure and content. For example, suppose that an organization stores customer information in a directory such as a lightweight directory access protocol (LDAP) directory and information on software that the

WO 02/057956

PCT/US02/01330

organization licenses in a database; an administrator would have to use more than one administration tool to manage both communities because the information varies in structure and content. Therefore, there is a need for an approach that can enable an administration tool to manage different communities whose information resides in separate and differently structured directories and databases.

Another problem with having community information stored in a broad range of directories and databases is that it is difficult for currently available administration tools to establish information to be managed from the directories and databases. Generally, data stored in directories and databases include a wide variety of information. Some of the data (e.g., name, address, etc.) are managed by a user, while some data (e.g., user and resource characteristics) are managed by an administrator. Typically, there is a great deal of other data that are often automatically associated with a user that do not have to be managed by an administrator. Other data that do not have to be managed by an administrator include unused or automatically updated data fields in the directories and databases. In order to manage a community, it is desirable to carve out a subset of the directory or database data to be managed and to explicitly ignore the rest. Also, as directories and databases change in structure, it is desirable to discover those changes and to decide whether or not to manage any new data elements. Therefore, there is a need for an approach that can enable an administration tool to establish information to be managed from the directories and databases, which includes defining information that is to be managed and information that is not to be managed and the discovering of new information to manage.

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 establish information needed to manage a community. In this embodiment, at least one data repository containing data related to the community is identified. The structure of the data within the at least one data repository is discovered. Data objects and attributes within the objects are selected from the discovered structure for managing. Access permissions for managing the selected attributes are defined.

WO 02/057956

PCT/US02/01330

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 establish information needed to manage a community. In this embodiment, at least one data repository containing data related to the community is identified. The structure of the data within the at least one data repository is discovered. The administrator is prompted to select data objects and attributes within the objects from the discovered structure and to define access permissions for managing the selected attributes.

In another embodiment, there is a tool for establishing information needed to manage a community. The tool comprises a data repository identification component that identifies at least one data repository containing data related to the community. A data structure discovery component discovers the structure of the data within the at least one data repository. A data selection component selects data objects and attributes within the objects according to the structure discovered by the data structure discovery component. An access permissions component defines access permissions for managing the attributes selected by the data selection component.

In still another embodiment, there is a system for establishing information needed to manage a community. This system comprises at least one data repository containing a plurality of community information. A tool establishes information in the at least one data repository to manage the community. The tool comprises a data repository identification component that identifies the least one data repository containing data related to the community. A data structure discovery component discovers the structure of the data within the at least one data repository. A data selection component selects data objects and attributes within the objects according to the structure discovered by the data structure discovery component. An access permissions component defines access permissions for the managing attributes selected by the data selection component. A computing unit is configured to serve the tool.

BRIEF DESCRIPTION OF THE DRAWINGS

WO 02/057956

PCT/US02/01330

Fig. 1 shows a schematic of a general-purpose computer system in which a tool that establishes information needed to manage a community operates;

Fig. 2 shows a top-level component architecture diagram of a tool that establishes information needed to manage a community and that operates on the computer system shown in Fig. 1;

Fig. 3 shows an architectural diagram of a system for implementing the tool that establishes and maintains information needed to manage a community;

Fig. 4 shows a flow chart describing the acts performed to initially configure administration of a community with the tool shown in Fig. 2;

Fig. 5 shows a flow chart describing the acts performed to modify an existing configuration with the tool shown in Fig. 2;

Fig. 6 shows a flow chart describing the acts performed to rediscover data within the at least one data repository with the tool shown in Fig. 2; and

Fig. 7 shows a flow chart describing the acts performed to configure access permissions and restricted value attributes with the tool shown in Fig. 2.

DETAILED DESCRIPTION OF THE INVENTION

In this disclosure, there is a description of an approach that overcomes the problems associated with managing community information stored in a broad range of directories and databases with currently available administrative tools. In particular, this approach facilitates the creation, configuration and subsequent modification of a managed community so that currently available administrative tools can manage the community without regard to the structure and content of information associated with the community. In this approach, the configuration of the managed community includes discovering information or data associated with the community that are stored in data repositories such as directories and databases and that are to be potentially managed. The configuration also includes user interaction to identify specific data elements or attributes that are to be managed and attributes that are not to

WO 02/057956

PCT/US02/01330

be managed. The processes used in the configuration can also be used in subsequent modifications or updates to the managed community. The same processes used in the creation, configuration and modification of a managed community can be used to manage multiple independent communities.

As an example, this approach for creating, configuring and modifying a managed community can be implemented in software. Fig. 1 shows a schematic of a general-purpose computer system 10 in which a tool that establishes information needed to manage a community 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 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

WO 02/057956

PCT/US02/01330

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. 2 shows a top-level component architecture diagram of a tool 28 that establishes information needed to manage a community and that operates on the computer system 10 shown in Fig. 1. Generally, a top-level administrator uses the tool 28 and in this disclosure is referred to as a SuperAdministrator. Some functions that the SuperAdministrator typically performs comprise installing the software tool described in this disclosure, configuring the installation to connect to one or more data repositories, identifying the data to be managed, identifying data to be self-managed and assigning selected users to manage the data previously selected. The tool 28 comprises a data repository identification component 30 that identifies at least one data repository containing data related to the user community. The at least one data repository that the data repository identification component 30 identifies may comprise a multiple of repositories that have different structures. The data repository identification component 30 also determines connection information for accessing data stored within the at least one data repository. Examples of connection information include but are not limited to the server that provides access to the at least one data repository, the port that interfaces with the at least one repository, a login identification for the at least one repository and the password for accessing the at least one repository.

A data structure discovery component 32 discovers the structure of the data within the at least one data repository. In particular, the data structure discovery component 32 determines the data objects and attributes that exist within the at least one data repository. Typically, standard database queries are performed to first determine what data objects are defined within the at least one data repository. After the

WO 02/057956

PCT/US02/01330

SuperAdministrator selects those data objects that comprise a managed user, then further queries are made to find out which attributes are associated with those objects.

The SuperAdministrator uses a data selection component 34 to select data objects and attributes discovered by the data structure discovery component 32. In particular, the SuperAdministrator decides which objects and attributes that were discovered shall be managed. Not all of the objects and classes that are discovered need to be managed. The selection of which objects and attributes are to be managed within the community is left to the discretion of the SuperAdministrator. Typically, the selection will vary from one community to a next. The SuperAdministrator also uses the data selection component 34 to identify attributes from the discovered objects and attributes that are unused within the managed user community. For example, attributes such as those that capture the state of the system that is used to implement the tool 28 and those that track times and dates of events in the system should not be altered by an administrator of the community. Other examples of attributes that should not be managed include internally generated data that should not be edited or viewed directly or data fields that are simply unused or are never changing. For such attributes, the SuperAdministrator uses the data selection component 34 to identify these attributes so that they will not be managed within community.

The SuperAdministrator uses an access permissions component 36 to define access permissions for managing the attributes selected by the data selection component 34. The access permissions defined by the SuperAdministrator determine how an administrator for a particular community can act upon certain attributes. In particular, the access permissions define what types of operations an administrator can and cannot perform on the attributes defined in a community. Some operations that the SuperAdministrator can grant include viewing, editing and deleting the attributes. These administrative operations are illustrative of only a few operations that the SuperAdministrator can grant access permission to and are not exhaustive of other possibilities. Examples of some other administrative operations that can be granted are editing during a particular time period and resetting data fields to default values. In general, the SuperAdministrator can use the access permissions component 36 to grant or deny access permission for any of these operations in order to restrict what

WO 02/057956

PCT/US02/01330

can and cannot be done to the attributes. Selection of access permissions for the attributes is left to the SuperAdministrator. Note that it is possible to grant access permission for just one of the above operations or any combination of the operations.

The access permissions component 36 also allows the SuperAdministrator to specify restricted values for some of the selected attributes. For example, for an attribute that contains data on the state that a user is employed (e.g., State of Employment), values can be restricted to one of 50 possible values, wherein the values are limited to two letter abbreviations (e.g., WI, NY, etc.). Another example where values can be restricted for an attribute, is for an attribute that lists applications that a user has access to. In this example, values for this application attribute may be restricted to specific names such as Catalog, Auction, Email, Chat, Web, etc. In addition, it is possible that some user attributes will have similar restricted values. Furthermore, it is possible to use a set of specified restricted attributes across a multiple of data repositories.

A modification component 38 allows the SuperAdministrator to make modifications or updates to the initial configuration of the community. In particular, the SuperAdministrator can use the modification component 38 to make changes to connection information for the at least one data repository such as server, port, login identification and password information. Also, modifications can be made to the data objects and attributes that were selected earlier for managing. This also includes making modifications to the attributes that were identified as unused within the managed community. Furthermore, the modification component 38 can be used to make modifications to the access permissions defined for the attributes, as well as the restricted values that were specified for the attributes.

A rediscovery information component 40 enables the SuperAdministrator to rediscover information about the structure of the data within the at least one data repository at a subsequent time after the community is up and running. Generally, after the initial discovery, the at least one data repository may have had additional attributes defined and thus might necessitate a rediscovery. For example, some older repositories may not contain attributes to store e-mail addresses or fax numbers or

WO 02/057956

PCT/US02/01330

personal home page references. If those attributes are added to the at least one repository, then it is desirable to perform a rediscovery of this information and include them as managed attributes. Also, it may be desirable to perform a rediscovery anytime that changes have been made to the underlying data repository in order to have an accurate view of the repository.

To rediscover object classes and attributes, the rediscovery information component 40 searches the at least one data repository for the object classes and attributes. The SuperAdministrator uses the rediscovery information component 40 to select additional objects and attributes to be managed. If any of the new attributes are useless to the managing of the community, then the SuperAdministrator identifies them as unmanaged. The SuperAdministrator then determines the access permissions for the new attributes that were selected, as well as any restricted values that should be designated for the attributes.

The tool 28 is not limited to a software implementation. For instance, the data repository identification component 30, data structure discovery component 32, data selection component 34, access permissions component 36, modification component 38 and rediscovery information component 40 may take the form of hardware or firmware or combinations of software, hardware, and firmware.

In addition, the tool 28 is not limited to the data repository identification component 30, data structure discovery component 32, data selection component 34, access permissions component 36, modification component 38 and rediscovery information component 40. One of ordinary skill in the art will recognize that the tool 28 may have other components. For example, the tool 28 could also include a workflow component that manages processes surrounding user creation and administration. Also, the 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 tool 28 could include is a browsing component for viewing information associated with the community.

WO 02/057956

PCT/US02/01330

Fig. 3 shows an architectural diagram of a system 42 for implementing the tool shown in Fig. 2. Fig. 3 shows that there are several ways of accessing the tool 28. A computing unit 44 allows the SuperAdministrator to access the tool 28. The computing unit 44 can take the form of a hand-held digital computer, personal digital assistant computer, notebook computer, personal computer or workstation. The SuperAdministrator uses a web browser 46 such as Microsoft INTERNET EXPLORER or Netscape NAVIGATOR to locate and display the administration tool 28 on the computing unit 44. A communication network such as an electronic or wireless network connects the computing unit 44 to the tool 28. Fig. 3 shows that the computing units 44 may connect to the tool 28 through a private network 48 such as an extranet or intranet or a global network 50 such as a WAN (e.g., Internet). As shown in Fig. 3, the tool 28 resides in a server 52, which comprises a web server 54 that serves the tool 28 and a data repository 56 (or repositories) that contains the various information associated with the community. However, the tool does not have to be co-resident with the server 52. If desired, the system 42 may have functionality that enables authentication and access control of users accessing the tool 28. Both authentication and access control can be handled at the web server level by the tool 28 itself, or by commercially available packages such as Netegrity SITEMINDER.

The information in the data repository or repositories 56 as mentioned above may comprise community information on users in the community such as their 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 data repository or repositories 56 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 data repository or repositories 56 may comprise the services (e.g., operating systems, applications, shared-file systems, print queues, etc.) available to each of the physical devices. The data repository or repositories 56 may comprise repositories such as directories and databases that have different structures for storing data. Examples of possible data repositories include but are not limited to LDAP directories, relational databases, object-oriented databases, flat files,

WO 02/057956

PCT/US02/01330

data management systems and other directory type databases with other types of schema.

Using the system 42 shown in Fig. 3, an administrator such as the SuperAdministrator can use the tool 28 to establish and maintain a community such as a user community. Fig. 4 shows a flow chart describing the acts performed to initially configure administration of a community with the tool 28. At block 58, the SuperAdministrator signs in. The sign-in act can include entering identity and security information (e.g., a valid username and password). The tool validates the username and password at 60. The tool then determines if the user has permission (i.e., the user is a SuperAdministrator) to configure a community at 62. If the user is not authenticated or does not have permission to configure a community, then the user is not allowed to configure a community.

At 64, the SuperAdministrator installs the tool and identifies the at least one data repository that contains community information. In the installation, the SuperAdministrator inputs connection information for accessing data stored within the at least one data repository such as server and port information, the identification and password for accessing the at least one repository. Note that the at least one data repository may already exist; in this case the SuperAdministrator simply needs to provide the connection information to the tool. Next, the tool connects to the at least one data repository at 66 to discover the schema. As mentioned above, during this discovery phase, the tool learns what data objects and attributes exist within the at least one data repository. First, at 68, the data objects in the at least one data repository are discovered. Next, the SuperAdministrator selects data objects at 70 that will make up a managed user. The data selection component is then used at 72 to discover attributes on those selected data objects. Next, the data selection component is used to identify attributes that are not managed at 74.

At 76, the SuperAdministrator selects attributes that will be self-administered by a user. As mentioned above, some attributes that can be self-administered may include the user's name, address, telephone number, etc. Next, the SuperAdministrator uses the access permissions component to define access permissions at 78 to define what

WO 02/057956

PCT/US02/01330

acts a user can do to the attributes selected for self-administration. At 80, the SuperAdministrator uses the data selection component to select attributes to be managed by administrators and the access permissions component to define how the administrators can and cannot act (e.g., edit, view, delete, etc.) upon the selected attributes at 82.

The SuperAdministrator then identifies attributes that will have restricted values associated therewith at 84. At this block, the SuperAdministrator also assigns allowable values for the attributes that have been identified to have restricted values. All of the initial configuration data are then saved at 86. Once the community has been configured, then an administration tool can administer the community. In particular, the administration tool can be used to set up various domains and sub-domains and grant authority to manage these domains.

Fig. 5 shows a flow chart describing the acts performed to modify an existing configuration with the tool 28. At block 88, the SuperAdministrator signs in by entering his or her identity and security information (e.g., a valid username and password). The tool validates the username and password at 90 and determines if the user has permission (i.e., the user is a SuperAdministrator) to modify an existing configuration at 92. If the user is not authenticated or does not have permission to configure a community, then the user is not allowed to modify an existing configuration. At 94, the SuperAdministrator selects a particular configuration that he or she would like to modify. The tool then parses the configuration selection, obtains the configuration data and presents it to the SuperAdministrator at 96. Then the SuperAdministrator makes the modifications to the configuration at 98. The modifications could include modifying, adding or removing objects, attributes, access permissions, restricted value attributes, connection information, etc. If any modifications affect the attributes that were designated as unmanaged, then such changes are noted. After making the modifications, the modified configuration data is then updated at 100.

Fig. 6 shows a flow chart describing the acts performed during rediscovery of the at least one data repository with the tool 28. At block 102, the SuperAdministrator signs

WO 02/057956

PCT/US02/01330

in by entering his or her identity and security information (e.g., a valid username and password). The tool validates the username and password at 104 and determines if the user has permission (i.e., the user is a SuperAdministrator) to rediscover data at 106. If the user is not authenticated or does not have permission to rediscover data, then the user is not allowed to do so. At 108, the SuperAdministrator selects at least one data repository to rediscover. The tool crawls the at least one data repository and finds all data objects and attributes in the at least one data repository at 110 and presents the results to the SuperAdministrator at 112. Then the SuperAdministrator makes any modifications to the configuration at 114 in the manner described with Fig. 5. After making any modifications, the modified configuration data are then updated at 116. Basically, the rediscovery process causes the SuperAdministrator to perform the same steps performed in the initial configuration (e.g., discovering data objects, selecting objects, discovering attributes, selecting attributes, etc.).

Fig. 7 shows a flow chart describing the acts performed to configure access permissions and restricted value attributes with the tool 28. As mentioned above, the SuperAdministrator can configure access permissions and restricted value attributes during initial configuration or modification of the configuration. At block 118, the SuperAdministrator signs in by entering his or her identity and security information (e.g., a valid username and password). The tool validates the username and password at 120 and determines if the user has permission (i.e., the user is a SuperAdministrator) to set access permissions and restricted value attributes at 122. If the user is not authenticated or does not have permission to set access permissions and restricted value attributes, then the user is not allowed to do so. At 124, the tool obtains the attributes selected by the SuperAdministrator during the configuration. Then the SuperAdministrator identifies access permissions defining what type of operations (e.g., edit, view, delete, etc.) an administrator can and cannot perform on each of the attributes at 126. The SuperAdministrator then identifies attributes that will have restricted values associated therewith at 128. At 130, the SuperAdministrator assigns allowable values for the attributes that have been identified to have restricted values. The selections are then updated at 132.

WO 02/057956

PCT/US02/01330

The foregoing flow charts of this disclosure show the functionality and operation of the 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 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 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 tool that establishes and maintains a managed community. While the invention has been

WO 02/057956

PCT/US02/01330

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 02/057956

PCT/US02/01330

WHAT IS CLAIMED IS:

1. A method for establishing information needed to manage a collection of data, comprising:

identifying at least one data repository containing data related to the collection of data;

discovering the structure of the data within the at least one data repository;

selecting data objects and attributes within the objects to manage from the discovered structure; and

defining access permissions for managing the selected attributes.
2. The method according to claim 1, wherein the identifying of the at least one data repository comprises selecting from data repositories having different structures.
3. The method according to claim 1, wherein the discovering of the structure comprises determining the data objects and attributes that exist within the at least one data repository.
4. The method according to claim 1, further comprising identifying attributes that are unmanaged.
5. The method according to claim 1, wherein the defining of access permissions comprises determining operations that can and cannot be performed on the selected attributes.
6. The method according to claim 1, wherein the defining of access permissions comprises specifying restricted values for some of the selected attributes.
7. The method according to claim 1, further comprising modifying at least one of the selected data objects and attributes and the defined access permissions.
8. The method according to claim 1, further comprising rediscovering information about the structure of the data within the at least one data repository at a subsequent time.

WO 02/057956

PCT/US02/01330

9. A method for establishing information needed to manage a community, comprising:

identifying at least one data repository containing data related to the community;

discovering the structure of the data within the at least one data repository;

selecting data objects and attributes within the objects to manage from the discovered structure; and

defining access permissions for managing the selected attributes.

10. The method according to claim 9, wherein the identifying of at least one data repository comprises specifying connection information for accessing data stored within the at least one data repository.

11. The method according to claim 9, wherein the discovering of the structure comprises determining the data objects and attributes that exist within the at least one data repository.

12. The method according to claim 9, further comprising identifying attributes that are unmanaged.

13. The method according to claim 9, wherein the defining of access permissions comprises determining operations that can and cannot be performed on the selected attributes.

14. The method according to claim 9, wherein the defining of access permissions comprises specifying restricted values for some of the selected attributes.

15. The method according to claim 9, further comprising modifying at least one of the selected data objects and attributes and the defined access permissions.

16. The method according to claim 9, further comprising rediscovering information about the structure of the data within the at least one data repository at a subsequent time.

WO 02/057956

PCT/US02/01330

17. The method according to claim 16, wherein the rediscovering of information comprises determining the data objects and attributes that exist within the at least one data repository.

18. The method according to claim 17, further comprising selecting new data objects and attributes to manage.

19. A method for enabling an administrator to establish information needed to manage a community, comprising:

identifying at least one data repository containing data related to the community;

discovering the structure of the data within the at least one data repository;

prompting the administrator to select data objects and attributes within the objects from the discovered structure; and

prompting the administrator to define access permissions for managing the selected attributes.

20. The method according to claim 19, wherein the identifying of at least one data repository comprises specifying connection information for accessing data stored within the at least one data repository.

21. The method according to claim 19, wherein the discovering of the structure comprises determining the data objects and attributes that exist within the at least one data repository.

22. The method according to claim 19, further comprising prompting the administrator to identify attributes that are unmanaged.

23. The method according to claim 19, further comprising prompting the administrator to modify at least one of the selected data objects and attributes and the defined access permissions.

WO 02/057956

PCT/US02/01330

24. The method according to claim 19, further comprising prompting the administrator to rediscover information about the structure of the data within the at least one data repository at a subsequent time.

25. A method for configuring a community to support an administrative tool, comprising:

identifying at least one data repository containing data related to the community;

discovering the structure of the data within the at least one data repository;

selecting data objects and attributes within the objects from the discovered structure;

defining access permissions for managing the selected attributes; and

using the administrative tool to manage the community according to the selected data objects and attributes and defined access permissions.

26. The method according to claim 25, wherein the identifying of at least one data repository comprises specifying connection information for accessing data stored within the at least one data repository.

27. The method according to claim 25, wherein the identifying of at least one data repository comprises selecting from data repositories having different structures.

28. The method according to claim 25, further comprising identifying attributes that are unmanaged.

29. The method according to claim 25, wherein the defining of access permissions comprises determining operations that can and cannot be performed on the selected attributes.

30. The method according to claim 25, wherein the defining of access permissions comprises specifying restricted values for some of the selected attributes.

31. The method according to claim 25, further comprising modifying at least one of the selected data objects and attributes and the defined access permissions.

WO 02/057956

PCT/US02/01330

32. The method according to claim 25, further comprising rediscovering information about the structure of the data within the at least one data repository at a subsequent time.

33. A tool for establishing information needed to manage a community, comprising:

a data repository identification component that identifies at least one data repository containing data related to the community;

a data structure discovery component that discovers the structure of the data within the at least one data repository;

a data selection component that selects data objects and attributes within the objects according to the structure discovered by the data structure discovery component; and

an access permissions component that defines access permissions for managing the attributes selected by the data selection component.

34. The tool according to claim 33, wherein the data repository identification component specifies connection information for accessing data stored within the at least one data repository.

35. The tool according to claim 33, wherein the data repository identification component selects from data repositories having different structures.

36. The tool according to claim 33, wherein the data structure discovery component determines the data objects and attributes that exist within the at least one data repository.

37. The tool according to claim 33, wherein the data selection component identifies attributes that are unmanaged.

38. The tool according to claim 33, wherein the access permissions component determines operations that can and cannot be performed on the selected attributes.

39. The tool according to claim 33, wherein the access permissions component specifies restricted values for some of the selected attributes.

WO 02/057956

PCT/US02/01330

40. The tool according to claim 33, further comprising a modification component that modifies at least one of the selected data objects and attributes and the defined access permissions.

41. The tool according to claim 33, further comprising a rediscovery information component that rediscovers information about the structure of the data within the at least one data repository at a subsequent time.

42. A tool for establishing information needed to manage a community, comprising:
means for identifying at least one data repository containing data related to the community;
means for discovering the structure of the data within the at least one data repository;
means for selecting data objects and attributes within the objects according to the structure discovered by the discovering means; and
means for defining access permissions for the managing attributes selected by the selecting means.

43. The tool according to claim 42, wherein the identifying means selects from data repositories having different structures.

44. The tool according to claim 42, wherein the discovering means determines the data objects and attributes that exist within the at least one data repository.

45. The tool according to claim 42, wherein the selecting means identifies attributes that are unmanaged.

46. The tool according to claim 42, further comprising means for modifying at least one of the selected data objects and attributes and the defined access permissions.

47. The tool according to claim 42, further comprising means for rediscovering information about the structure of the data within the at least one data repository at a subsequent time.

WO 02/057956

PCT/US02/01330

48. A system for establishing information needed to manage a community, comprising:

at least one data repository containing a plurality of community information;

a tool to establish information in the at least one data repository to manage the community; the tool comprising a data repository identification component that identifies the least one data repository containing data related to the community; a data structure discovery component that discovers the structure of the data within the at least one data repository; a data selection component that selects data objects and attributes within the objects according to the structure discovered by the data structure discovery component; and an access permissions component that defines access permissions for managing the attributes selected by the data selection component; and

a first computing unit configured to serve the tool.

49. The system according to claim 48, further comprising a second computing unit configured to execute the tool served from the first computing unit over a network.

50. The system according to claim 48, wherein the data repository identification component specifies connection information for accessing data stored within the at least one data repository.

51. The system according to claim 48, wherein the data repository identification component selects from data repositories having different structures.

52. The system according to claim 48, wherein the data structure discovery component determines the data objects and attributes that exist within the at least one data repository.

53. The system according to claim 48, wherein the data selection component identifies attributes that are unmanaged.

54. The system according to claim 48, wherein the access permissions component determines operations that can and cannot be performed on the selected attributes.

WO 02/057956

PCT/US02/01330

55. The system according to claim 48, wherein the access permissions component specifies restricted values for some of the selected attributes.

56. The system according to claim 48, wherein the tool further comprises a modification component that modifies at least one of the selected data objects and attributes and the defined access permissions.

57. The system according to claim 48, wherein the tool further comprises a rediscovery information component that rediscovers information about the structure of the data within the at least one data repository at a subsequent time.

58. A computer-readable medium storing computer instructions for instructing a computer system to establish information needed to manage a community, the computer instructions comprising:

identifying at least one data repository containing data related to the community;

discovering the structure of the data within the at least one data repository;

selecting data objects and attributes within the objects to manage from the discovered structure; and

defining access permissions for managing the selected attributes.

59. The computer-readable medium according to claim 58, wherein the identifying of at least one data repository comprises instructions for specifying connection information for accessing data stored within the at least one data repository.

60. The computer-readable medium according to claim 58, wherein the discovering of the structure comprises instructions for determining the data objects and attributes that exist within the at least one data repository.

61. The computer-readable medium according to claim 58, further comprising instructions for identifying attributes that are unmanaged.

WO 02/057956

PCT/US02/01330

62. The computer-readable medium according to claim 58, wherein the defining of access permissions comprises instructions for determining operations that can and cannot be performed on the selected attributes.

63. The computer-readable medium according to claim 58, wherein the defining of access permissions comprises instructions for specifying restricted values for some of the selected attributes.

64. The computer-readable medium according to claim 58, further comprising instructions for modifying at least one of the selected data objects and attributes and the defined access permissions.

65. The computer-readable medium according to claim 58, further comprising instructions for rediscovering information about the structure of the data within the at least one data repository at a subsequent time.

66. The computer-readable medium according to claim 65, wherein the rediscovering of information comprises instructions for determining the data objects and attributes that exist within the at least one data repository.

67. The computer-readable medium according to claim 66, further comprising instructions for selecting new data objects and attributes to manage.

68. A computer-readable medium storing computer instructions for instructing a computer system to enable an administrator to establish information needed to manage a community, the computer instructions comprising:

identifying at least one data repository containing data related to the community;

discovering the structure of the data within the at least one data repository;

prompting the administrator to select data objects and attributes within the objects from the discovered structure; and

prompting the administrator to define access permissions for managing the selected attributes.

WO 02/057956

PCT/US02/01330

69. The computer-readable medium according to claim 68, wherein the identifying of at least one data repository comprises instructions for specifying connection information for accessing data stored within the at least one data repository.

70. The computer-readable medium according to claim 68, wherein the discovering of the structure comprises instructions for determining the data objects and attributes that exist within the at least one data repository.

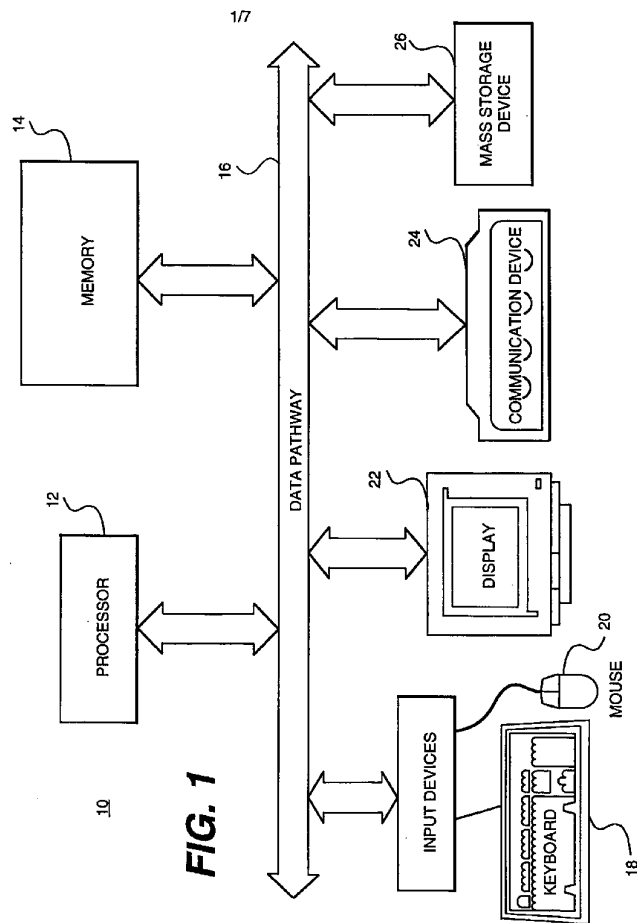
71. The computer-readable medium according to claim 68, further comprising instructions for prompting the administrator to identify attributes that are unmanaged.

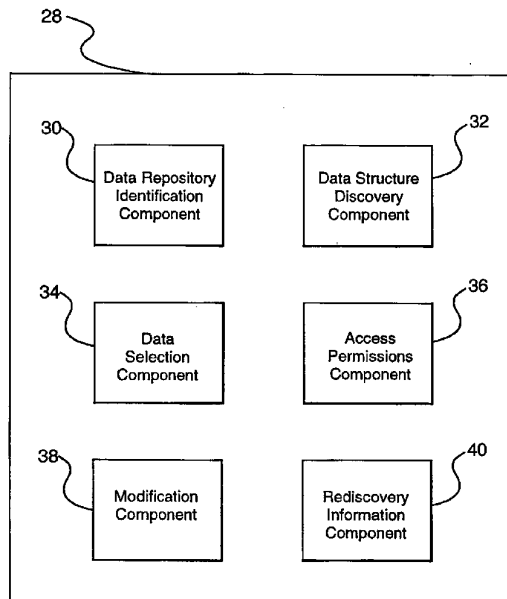
72. The computer-readable medium according to claim 68, further comprising instructions for prompting the administrator to modify at least one of the selected data objects and attributes and the defined access permissions.

73. The computer-readable medium according to claim 68, further comprising instructions for prompting the administrator to rediscover information about the structure of the data within the at least one data repository at a subsequent time.

WO 02/057956

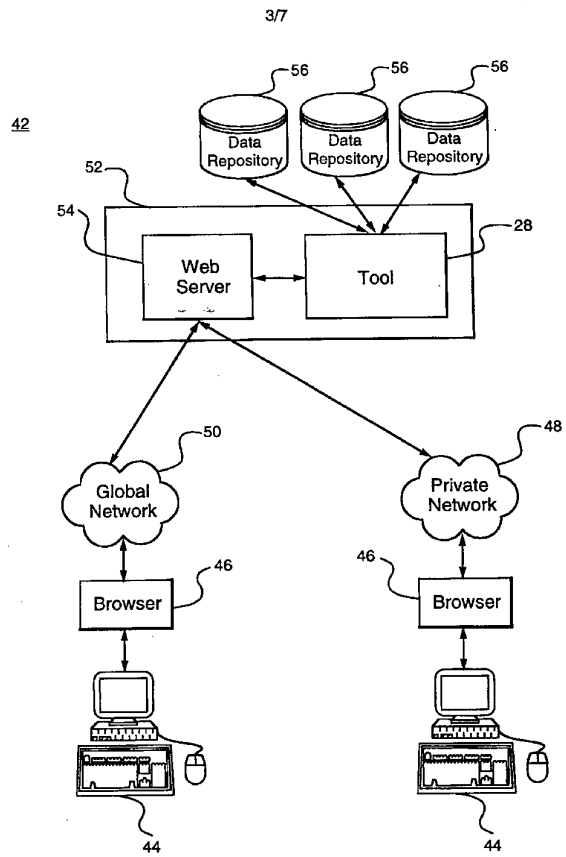
PCT/US02/01330



**FIG. 2**

WO 02/057956

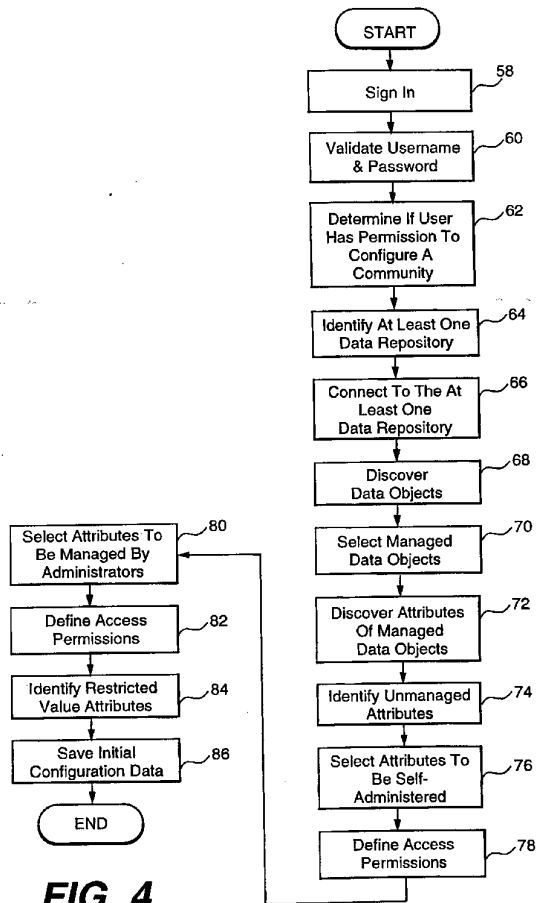
PCT/US02/01330

**FIG. 3**

WO 02/057956

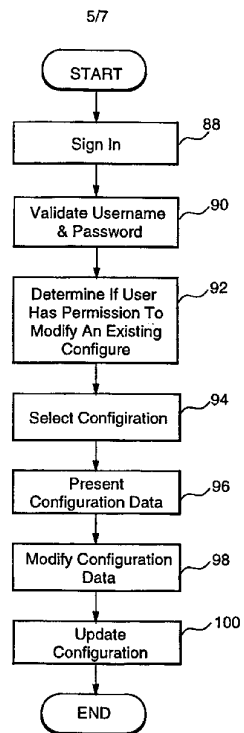
PCT/US02/01330

4/7

**FIG. 4**

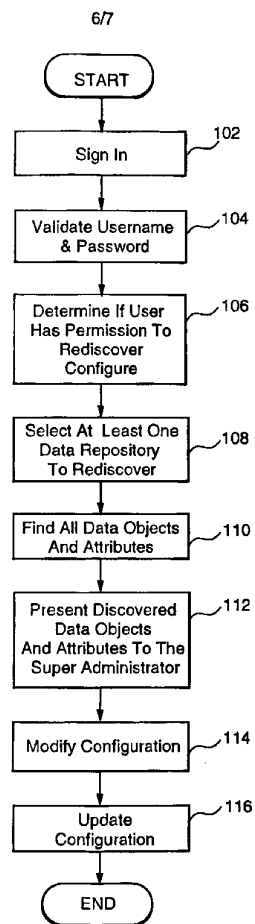
WO 02/057956

PCT/US02/01330

**FIG. 5**

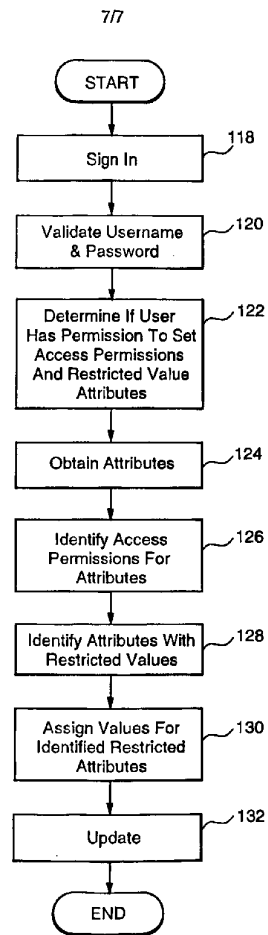
WO 02/057956

PCT/US02/01330

**FIG. 6**

WO 02/057956

PCT/US02/01330

**FIG. 7**

【国際調査報告】

INTERNATIONAL SEARCH REPORT		International application No. PCT/US02/01330
A. CLASSIFICATION OF SUBJECT MATTER IPC(7) : G06F, 17/30 US CL : 707/3, 10, 9 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. : 707/3, 10, 9 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) WEST, DIALOG, CAS ONLINE, IEEE, NPL		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,996,007 A (KLUG et al.), 30 November 1999, see entire document.	1-72
Y	US 6,038,560 A (WICAL) 14 March 2000, see entire document.	1-72
Y	US 6,029,161 A (LANG et al.) 22 February 2000, see entire document.	1-72
☐ 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 document 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 reasons (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 03 APRIL 2002		Date of mailing of the international search report 13 APRIL 2002
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230		Authorized officer JEAN M. CORRIEU Telephone No. (703) 306-3035

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,CO,CR,CU,CZ,DE,DK,DM,DZ,EC,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,OM,PH,P L,PT,RO,RU,SD,SE,SG,SI,SK,SL,TJ,TM,TN,TR,TT,TZ,UA,UG,UZ,VN,YU,ZA,ZM,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 オスコイ, 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、ビーエル・ディージャー・2 6、バン・レンスラー・ブルヴァール、1 8 5 番

Fターム(参考) 5B017 AA02 AA03 BA06 CA16