[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
G06F 3/00
G06F 11/00 G06F 13/14
H04M 1/64

[12] 发明专利申请公开说明书

[21] 申请号 02800108.7

[43] 公开日 2003 年 11 月 12 日

[11] 公开号 CN 1455892A

[22] 申请日 2002.1.16 [21] 申请号 02800108.7
[30] 优先权
[32] 2001. 1.16 [33] US [31] 09/760,999
[86] 国际申请 PCT/US02/01335 2002.1.16
[87] 国际公布 WO02/057895 英 2002.7.25
[85] 进入国家阶段日期 2002.9.16
[71] 申请人 通用电气公司
地址 美国纽约州
[72] 发明人 J·A·巴内特 B·J·维维尔
K·S·阿古尔 M·M·科恩菲因
O·R·奥克索伊 B·O·威廉斯
J·塞巴斯蒂安 D·T·梅林

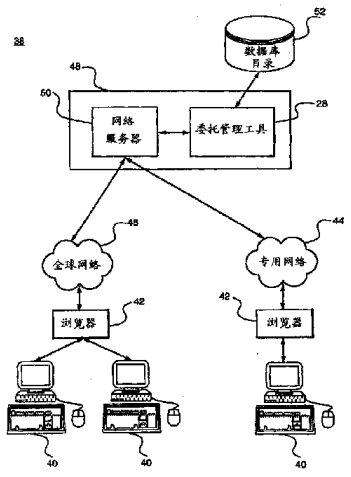
[74] 专利代理机构 中国专利代理(香港)有限公司
代理人 吴立明 张志醒

权利要求书 4 页 说明书 12 页 附图 6 页

[54] 发明名称 使用属性许可委托管理在一个数据库目录中的信息

[57] 摘要

一个委托管理工具(28)，用于使用属性许可来管理在一个数据库目录(52)中的信息。 该委托管理工具(28)允许一个管理员形成具有用户属性许可的管理域和子域，其中该用户属性许可定义了一个管理员能和不能在一个用户属性上执行的管理操作。 此外，委托管理工具(28)还允许一个管理员定义用于分配给该用户属性的有限值。



ISSN1008-4274

1.一种用于管理一个用户团体的方法，包含:

为在该用户团体中的每个用户定义一组用户属性；以及

标识一个用于管理每一个用户属性的许可级别。

2.如权利要求 1 所述的方法，其特征在于：每个许可级别定义了一个管理员能和不能在一个用户属性上执行的管理操作。

3.如权利要求 1 所述的方法，进一步包含：定义一个管理员能够为用户属性分配的有限值。

4.一种用于管理与一个用户团体有关的用户信息的方法，包含:

为在该用户团体中的每个用户从用户信息中定义一组用户属性;

标识一个用于管理每一个用户属性的许可级别；以及

依据每一个许可级别管理这些用户属性。

5.如权利要求 4 所述的方法，其特征在于：每个许可级别定义了一个管理员能和不能在一个用户属性上执行的操作。

6.如权利要求 4 所述的方法，进一步包含：定义一个管理员能够为任何一个用户属性分配的有限值。

7.一种用于允许一个管理员控制一个用户团体的管理的方法，包含:

向管理员提供与该用户团体有关的用户信息;

提示管理员为在该用户团体中的每个用户定义一组用户属性;

提示管理员为每一个用户属性标识一个许可级别；以及

使用该被标识的许可级别来控制用户信息的管理。

8.如权利要求 7 所述的方法，其特征在于：每个许可级别都定义了该管理员能和不能在一个用户属性上执行的操作。

9.如权利要求 8 所述的方法，进一步包含：提示管理员定义该管理员能够为任何一个用户属性分配的有限值。

10.一种用于管理与一个用户团体有关的用户信息的用户团体管理工具，包含:

一个把该用户团体定义成为至少一个管理域的域定义组件，该域定义组件包含：一个从该用户团体中指定至少一个任意用户组的用户组指定组件，和一个为该至少一个任意用户组定义一组可允许的用户属性的用户属性定义组件；以及

一个信息管理组件，根据可允许的用户属性管理与该管理域有关的用户信息。

11. 如权利要求 10 所述的工具，其特征在于：用户属性定义组件包含一个属性许可组件，它为每一个用户属性指定一个许可级别。

12. 如权利要求 11 所述的工具，其特征在于：每个许可级别都定义了一个管理员能和不能在一个用户属性上执行的操作。

13. 如权利要求 10 所述的工具，其特征在于：用户属性定义组件包含一个属性有限值组件，它定义了一个管理员能够为任何一个用户属性分配的有限值。

14. 如权利要求 10 所述的工具，进一步包含一个管理特权组件，它授予用于该管理域的管理特权。

15. 如权利要求 14 所述的工具，其特征在于：管理特权组件委托被授予的、用于该管理域的管理特权。

16. 一个用于管理与一个用户团体有关的用户信息的系统，包含：

一个包含有多个用户信息的数据库目录；

一个用户团体管理工具，管理在该数据库目录中的多个用户信息；该用户团体管理工具包含：一个把该用户团体定义成为至少一个管理域的域定义组件，该域定义组件包含：一个从该用户团体中指定至少一个任意用户组的用户组指定组件，和一个为该至少一个任意用户组定义一组可允许的用户属性的用户属性定义组件；以及一个信息管理组件，它根据该可允许的用户属性管理与该管理域有关的用户信息；以及

一个第一计算单元，被配置为服务于该用户团体管理工具和该数据库目录。

17. 如权利要求 16 所述的系统，进一步包含一个第二计算单元，其被配置来执行经由一个网络按第一计算单元服务的用户团体管理工具。

18. 如权利要求 16 所述的系统，其特征在于：用户属性定义组件包含一个属性许可组件，它为每一个用户属性指定一个许可级别。

19. 如权利要求 18 所述的系统，其特征在于：每个许可级别定义了一个管理员能和不能在一个用户属性上执行的操作。

20. 如权利要求 16 所述的系统，其特征在于：用户属性定义组件

包含一个属性有限值组件，它定义了一个管理员能够为任何一个用户属性分配的有限值。

21. 一种用于提供一个用户团体的管理的用户团体管理工具，包含:

用于把该用户团体定义到至少一个管理域中的装置，该管理域定义装置包含：用于从该用户团体中指定至少一个任意用户组的装置，以及用于为该至少一个任意用户组定义一组可允许的用户属性的装置；以及

用于根据该可允许的用户属性管理与该管理域有关的用户信息的装置。

22. 如权利要求 21 所述的工具，其特征在于：用户属性定义装置包含用于为每一个用户属性指定一个许可级别的装置。

23. 如权利要求 22 所述的工具，其特征在于：每个许可级别都定义了一个管理员能和不能在一个用户属性上执行的操作。

24. 如权利要求 21 所述的工具，其特征在于：用户属性定义装置包含用于定义一个管理员能够为任何一个用户属性分配的有限值的装置。

25. 一种存储了用于指示一个计算机系统管理一个用户团体的计算机指令的计算机可读介质，该计算机指令包含:

为在该用户团体中的每个用户定义一组用户属性；以及

标识一个用于管理每一个用户属性的许可级别。

26. 如权利要求 25 所述的计算机可读介质，其特征在于：每个许可级别都定义了一个管理员能和不能在一个用户属性上执行的操作。

27. 如权利要求 25 所述的计算机可读介质，进一步包含：用于定义一个管理员能够为任何一个用户属性分配的有限值的指令。

28. 一种存储了用于指示一个计算机系统允许一个管理员控制管理一个用户团体的计算机指令的计算机可读介质，该计算机指令包含:

向管理员提供与该用户团体有关的用户信息;

提示管理员为在该用户团体中的每一个用户定义一组用户属性;

提示管理员为每一个用户属性标识一个许可级别；以及

使用该被标识的许可级别以控制用户信息的管理。

29.如权利要求 28 所述的计算机可读介质，其特征在于：每个许可级别都定义了该管理员能和不能在一个用户属性上执行的操作。

30.如权利要求 28 所述的计算机可读介质，进一步包含：用于提示管理员定义该管理员能够为任何一个用户属性分配的有限值的指令。

使用属性许可委托管理在一个数据库目录中的信息

发明背景技术

这个公开通常涉及基于团体的计算机服务，尤其涉及使用属性许可管理基于团体的计算机服务。

通常，一个团体是一组通常共享一个共同利益的人。随着 Internet 和电子商务的出现，许多公司正通过内部网和外部网为雇员、供应商、合伙人和客户形成团体。该团体使得让雇员、供应商、合伙人和客户一起工作变得更容易和较为便宜。在计算机服务的环境中，这些人被认为是计算机用户或者简单地被认为是用户。有关该团体中每一个用户的信息被保存在大量的目录和数据库中。该信息可以包含诸如用户的姓名、位置、电话号码、机构、登录标识、口令等条目。其它信息可以包含该用户对诸如应用程序和内容之类的资源的存取特权。该目录还可以存储与在支持该团体的网络中的物理设备（例如，个人计算机、服务器、打印机、路由器、通信服务器等）有关的信息。附加信息可以包含每一个物理设备可得到的服务（例如，操作系统、应用程序、共享文件系统、打印队列等）。所有上述信息通常被称为基于团体的计算机服务。

随着该团体在规模和复杂程度方面的增长，这些基于团体的计算机服务的管理（即，创建、维护、修改、更新、和停用）变得困难了。在很多情况下，除非一个团体被细分成更多可管理的子团体，否则管理就变为一个几乎不可能完成的任务。随着这些子团体的创建，通过分配不同的个人去管理子团体、使用共享管理该团体职责的一个管理员队伍变得是所期望的。这种类型的管理被称为委托管理。

当前可用的、便于委托管理的管理工具确实具有它们的缺点。例如，这些工具没有提供限制一个管理员能够在用户信息上执行什么类型操作的性能。一个普遍的例子包含：允许一个管理员重置一个用户的口令，但是不允许管理员查看一个已有的口令。在这个例子中，一种类型的操作（设置一个新口令）在另一个操作（查看已有口令）未被允许时是被允许的。提供最小允许的许可（或操作）以便尽可能地

保护数据是重要的。此外，当前可用的管理工具没有提供限制一个管理员能够分配给与用户信息有关的数据字段的值的性能。例如，在一个用户目录内经常有用于存储用户访问许可（它准许访问基于网络的应用程序）的数据字段。通常，这些数据字段值包含一个允许值的列表（一个枚举列表），而且只有来自于那个列表的值应该被输入。通过把值仅仅限制为在那个枚举列表内的那些值，能够限制错误和印刷上的误差。

因此，需要有一个这样的管理工具，该工具提供了限制一个管理员能够在用户信息上执行什么类型操作的性能，从而使一个管理员被约束在他或她能够做的范围内。此外，还需要有一个这样的管理工具，其提供了限制一个管理员能够分配给用户信息的值的性能，以便限制能够被输入的数据值并且确保数据的正确性。

发明概述

在这个公开的一个实施例中，有一种存储了用于指示一个计算机系统管理一个用户团体的指令的方法、系统和计算机可读介质。在这个实施例中，为在该用户团体中的每个用户定义一组用户属性。然后标识一个用于管理每一个用户属性的许可级别。

在这个公开的第二实施例中，有一种系统、方法和计算机可读介质，其存储了用于指示一个计算机系统允许一个管理员控制一个用户团体的管理的指令。在这个实施例中，与该用户团体有关的用户信息被提供给一个管理员。管理员被提示为在该用户团体中的每个用户定义一组用户属性。管理员被提示为每一个用户属性标识一个许可级别。被标识的许可级别被用来控制用户信息的管理。

在另一个实施例中，有一种用于管理与一个用户团体有关的用户信息的用户团体管理工具。在该用户团体管理工具中有一个域定义组件，它把该用户团体定义到至少一个管理域中。该域定义组件包含：一个从该用户团体中指定至少一个任意用户组的用户组指定组件，和一个为该至少一个任意用户组定义一组可允许的用户属性的用户属性定义组件。一个信息管理组件根据可允许的用户属性管理与该管理域有关的用户信息。

在还有另一个实施例中，有一个用于管理与一个用户团体有关的

用户信息的系统。这个系统包含一个包含有多个用户信息的数据库目录。一个用户团体管理工具管理在该数据库目录中的多个用户信息。该用户团体管理工具包含一个域定义组件，它把该用户团体定义到至少一个管理域中。该域定义组件包含：一个从该用户团体中指定至少一个任意用户组的用户组指定组件和一个为该至少一个任意用户组定义一组可允许的用户属性的用户属性定义组件。一个信息管理组件根据可允许的用户属性管理与该管理域有关的用户信息。一个计算单元被配置为服务于该用户团体管理工具和该数据库目录。

附图简要说明

图 1 显示了一个用户团体示例的一个示意图；

图 2 显示了如图 1 所示的用户团体的委托管理的一个示例；

图 3 显示了一个通用计算机系统的一个示意图，在该通用计算机系统中运行这样一个委托管理工具，其创建用于管理与一个用户团体有关的信息的用户属性许可；

图 4 显示了委托管理工具的一个最高级组件体系结构框图，其中该委托管理工具创建用于管理信息的用户属性许可，并且在如图 3 所示的计算机系统上运行；

图 5 显示了这样一个系统的体系结构框图，该系统用于实现如图 4 所示的、创建用户属性许可的委托管理工具；以及

图 6 显示了利用如图 4 所示的委托管理工具、为创建一个具有用户属性许可的管理域而执行的动作的一个流程图。

本发明的详细说明

图 1 显示了从一个医疗服务供应商接收一个服务团体的一个用户团体实例的一个示意图。在图 1 中显示的例子是一个用户团体的概念的说明，而不打算限制这个公开。在图 1 中，保健供应商 A - D 是从医疗服务供应商 X 接收基于计算机的服务的团体。这种基于计算机的服务的例子可以包含医学信息、定购医药用品的能力、调度患者预约的能力、为患者服务存档要求的能力。用于这个方案的、基于计算机服务的其它说明性例子可以包含基准信息、保健统计以及对可下载软件的访问。保健供应商还可能想要向他们的客户、合伙人、厂家、供

应商等提供基于计算机的服务。在图 1 中，保健供应商 B 提供从医疗服务供应商 X 建立的、基于计算机的服务到一个和它具有一种关系的本地诊所和本地医院。该基于计算机的服务还能够被提供给他们的雇员。在图 1 中，基于计算机的服务被提供给在该本地医院中的各个部门，诸如心脏病科、放射科、肠胃病科、医学研究机构等。基于计算机服务的类似分配类型能够为其他保健供应商（即，保健供应商 A、 C 和 D）提供。

医疗服务供应商 X 在一个数据库目录中存储有关在该团体中每一个用户的信息。该信息可以包含诸如用户的姓名、位置、电话号码、机构、登录标识、口令等条目。其它信息可以包含该用户对由医疗服务供应商X提供的某些资源、诸如应用程序和内容的存取特权。医疗服务供应商的数据库目录还可以存储与在支持该团体的网络中的物理设备（例如，个人计算机、服务器、打印机、路由器、通信服务器等）有关的信息。保存在该数据库目录中的附加信息可以包含每一个物理设备可得到的服务（例如，操作系统、应用程序、共享文件系统、打印队列等）。

由于如图 1 所示的用户团体能够是相当大和复杂的，所以细分和委托管理这些团体是所期望的。图 2 显示了如图 1 所示的用户团体的委托管理的一个例子。在这个例子中，有一个用于每个团体、负责管理各种动作的管理员，这些动作包含但是不局限于：修改用户信息、更新对某些资源的许可、停用用户账号、创建用户帐号、以及维护用户帐号。例如，超级管理员管理用于医疗服务供应商 X 的动作；管理员 A 管理用于与保健供应商 B 有关的本地诊所和本地医院的心脏病科的动作；管理员 B 管理用于保健供应商 A 和 B 的动作；管理员 C 管理用于保健供应商 D 的动作；管理员 D 管理用于与保健供应商 B 有关的本地医院、与保健供应商 B 有关的本地医院的医学研究部门的动作、以及用于保健供应商 C 的动作；管理员 E 管理用于与保健供应商 B 有关的本地医院中的心脏病科和放射科的动作；以及管理员 F 管理用于与保健供应商 B 有关的本地医院中的肠胃病科的动作。管理员 A － F 管理动作的范围完全取决于他们具有的权限类型。用于这个示例的其它形式委托管理对于本领域技术人员来说将可能是显而易见的。

为了说明这个公开提供的委托管理，在图 2 的用户团体中的每一

块（即，医疗服务供应商X、保健供应商A－D、本地诊所、本地医院、心脏病科、放射科、肠胃病科、医学研究机构）都表示一个管理域。一个管理域是一个包含一组用户、一组能够被修改的用户属性、以及一组用于那些数据字段的允许值的管理对象，一个管理员在该管理对象上具有权限。用户属性的可能示例可以包含但不局限于：雇主、角色或者工作说明、已经被授予访问许可的资源、地址、以及使用的设备。通常，一个管理员的权限可以包含编辑权限和／或委托权限。当一个管理员可以编辑用户的某些属性时，他或她在该管理域内具有编辑权限。当他或她可以定义用户的一个子集并且标识用于修改的属性时，一个管理员在该管理域内具有委托权限，以便创建一个管理子域。把该管理子域分配给一个人就是那个域的委托。创建一个管理子域并且把那个域分配给一个用户的能力是委托权限。尽管在这个公开中描述的权限通常涉及编辑权限和委托权限，但是本领域普通技术人员将会意识到：诸如查看、修改、删除、临时委托、以及类似操作之类的、但是在可视数据范围上具有限制的其它权限类型同样是可能的。能够在除委托和编辑权限之外、代替委托和编辑权限、或者结合委托和编辑权限一起使用这些权限例子。

如上所述，能够创建用户属性许可来限制一个管理员能和不能执行什么类型的操作是所希望的。例如，在图 2 中，一个管理员可以仅仅需要许可来修改与该用户有关的单个数据字段。这样的一个例子能够是一个公司的工薪管理部门；工薪管理应当仅仅被允许修改一个雇员的薪金数据字段。

此外，能够限制用户属性的值为允许值的一个子集是所希望的。例如，在图 2 中，一个管理员可以负责管理用户对一个应用程序的访问。用户目录可以包含一个用于定义用户可以访问的所有应用程序的数据字段。然而，管理员仅仅负责单个应用程序；因此，管理员应当仅仅被允许为任一用户设置用于那个应用程序的单个值。

作为一个例子，以上描述的、用于创建用于管理与一个用户团体有关的信息的用户属性许可的委托管理性能能够以软件实现。图 3 显示了一个通用计算机系统 10 的一个示意图，在该通用计算机系统中运行这样一个委托管理工具，其创建用于管理信息的用户属性许可。计算机系统 10 通常包含至少一个处理器 12、一个存储器 14、输入／输

出设备、以及连接该处理器、存储器和输入／输出设备的数据通道（例如，总线）16。处理器 12 从存储器 14 接收指令和数据并且执行各种计算。处理器 12 包含一个执行算术和逻辑操作的算术逻辑单元（ALU），以及一个从存储器 14 中提取指令并且解码和执行它们、并在必要时访问 ALU 的控制单元。存储器 14 通常包含一个随机存取存储器（RAM）和一个只读存储器（ROM）；然而，可能有其它类型的存储器，诸如可编程序只读存储器（PROM）、可擦可编程序只读存储器（EPROM）和电可擦可编程只读存储器（EEPROM）。此外，存储器 14 最好包含一个在处理器 12 上执行的操作系统。操作系统执行包括识别输入、发送输出到输出设备、跟踪文件和目录、以及控制各种外围设备在内的基本任务。

输入／输出设备可以包含输入数据与指令到计算机系统 10 中的一个键盘 18 和一个鼠标 20。此外，一个显示器 22 可以用来允许一个用户看到计算机已经完成了什么。其它输出设备可以包含一台打印机、绘图仪、合成器和扬声器。一个诸如一个电话或者电缆调制解调器的通信设备 24 或者一个诸如一个 Ethernet 适配器、局域网（LAN）适配器、综合业务数字网络（ISDN）适配器、或者数字用户路（Digital Subscriber Line，DSL）适配器的网卡，允许计算机系统 10 访问在一个诸如一个 LAN 或者一个广域网（WAN）的网络上的其它计算机和资源。一个大容量存储设备 26 可以用来允许计算机系统 10 永久地保持大量数据。该大容量存储设备可以包含所有类型的磁盘驱动器、诸如软盘、硬盘和光盘、及磁带驱动器，它能够读和写数据到一个包含数字录音带（DAT）、数字线性带（DLT）、或者其它磁性编码介质的磁带上面。以上描述的计算机系统 10 能够采取手提式数字计算机、个人数字助理计算机、笔记本计算机、个人计算机、工作站、小型计算机、大型计算机或者巨型计算机的形式。

图 4 显示了一个委托管理工具 28 的一个最高级组件体系结构框图，其中该委托管理工具能够创建用于管理信息的用户属性许可并且在如图 3 所示的计算机系统 10 上运行。委托管理工具 28 包含一个域定义组件 30，它把一个用户团体定义到至少一个管理域中。域定义组件 30 包含一个用户组指定组件 31，它允许一个管理员从一个用户团体中指定至少一个任意用户组。用户组指定组件 31 通过由管理员构造的

一个查询规则来查询一个包含用户信息的数据库目录形成至少一个任意用户组。该查询规则定义在该至少一个任意用户组内的用户。例如，参见图 2，一个管理员能够使用用户组指定组件 31 以从包含是放射学家的用户的一个组、包含由保健供应商 B 雇用的用户的第二组、以及包含位于 Wisconsin 的用户的第三组中形成一个管理域。

被指定的每个任意用户组都具有与它的每一个用户有关的属性和用于这些属性的允许值。一个用户属性定义组件 33 允许一个管理员为该至少一个任意用户组定义一组许可的用户属性。具体地，被定义的这组许可用户属性包含一个管理员能够对其起作用的属性。用户属性定义组件 33 包含一个属性许可组件 34，它允许一个管理员为每一个用户属性指定一个许可级别。许可级别与在一个域内定义的属性的管理有关。这允许不同的管理员在管理同一数据时具有不同的许可。尤其是，许可级别指示了什么类型的操作能不能在与该至少一个任意用户组有关的属性上执行。一个管理员能够在用户属性上执行的某些操作包含查看、编辑和删除。这些管理操作仅仅说明了能够在该属性上执行的几个操作，而且没有穷举其它的可能性。能够在该属性上执行的某些其它管理操作的例子是在一个特定时期内进行编辑和重置数据字段为缺省值。一个管理员能够使用属性许可组件 34 来选择这些操作中的任何一个以限制能和不能对该属性进行什么操作。用于该属性的许可选择被留给设置管理域的用户。仅仅选择上述操作中的一个或者这些操作的任何组合是可能的。

再次参见图 2，作为例子，一个管理员能够为包含在 Wisconsin 州中、由保健供应商 B 雇用的放射学家的管理域使用属性许可组件 34，以定义什么类型的操作能和不能在某些属性上形成。例如，能够定义防止一个管理员编辑、查看和删除一个诸如一个放射学家的薪金的属性的许可，同时能够准许编辑和查看一个放射学家被授权使用什么类型的诊断软件工具。能够被定义的另一个许可是：允许一个管理员编辑、查看、和删除一般的、诸如放射学家的姓名、地址、电子邮件地址、电话号码等的用户信息。

用户属性定义组件 33 还包含一个属性有限值组件 35，它允许一个管理员指定能够分配给用户属性的某些值。某些用户属性将具有类似的有限值。此外，有可能跨越多个用户目录使用一组指定的有限属性。

再次参见图 2，作为一个例子，一个管理员能够为包含在 Wisconsin 州中、由保健供应商 B 雇用的放射学家的管理域使用属性有限值组件 35，以定义一个管理员能够为一个用户属性分配什么值。例如，就“工作的州”用户属性而言，值能够被限制在 50 个可能值的一个中，其中这些值被限制为两个字母缩写（例如，WI、NY 等）。在另一种情况下，属性有限值组件 35 能被用来限制用于一个诸如“许可授权”的用户属性的值，其中一个管理员把值分配给不同的应用。在这样一种情况下，每个管理员可以被允许设置与一个特定应用有关的值、而不是与其它应用有关的值。例如，在图 2 中，本地医院管理员（管理员 D）可以限制管理员 E 可执行的操作仅仅是分别为在放射科和心脏病科中的用户设置放射和心脏病应用许可。

委托管理工具 28 还包含一个管理特权组件 32。管理特权组件 32 允许一个管理员为他或她对其具有权限的一个管理域或者管理子域授予管理特权。授予的管理特权可以包含委托权限和编辑权限中的至少一个。如上所述，授予其它类型的权限、诸如查看、修改、删除、暂时委托等也是可能的。能够在除委托和编辑权限之外、代替委托和编辑权限、或者结合委托和编辑权限一起使用这些权限的示例。

管理特权组件 32 还允许一个管理员定义：在他或她操作的和对其具有权限的一个管理域或者子域中的哪些用户将具有该授予的管理特权。更具体地说，一个管理员能够使用这个组件以通过把委托权限、编辑权限或者其它类型分配给一个特定用户来为他们的操作域定义各个管理员。具有委托权限的管理员还能够使用域定义组件 30（即，用户组指定组件 31 和用户属性定义组件 33)以从一个附加的用户组中为它们的操作域形成子域，并且为用户属性的一个子集分配某些属性许可和值。管理员还能够使用管理特权组件 32 为他们已经定义的那个特定子域授予权限。

委托管理工具 28 还包含一个信息管理组件 36，它依据委托的管理特权管理与每一个管理域有关的信息。取决于委托的权限类型和与每一个用户属性有关的许可级别，一个管理员能够使用信息管理组件 36 来执行包含但不局限于编辑、查看或者删除用于一个域中的一个用户的特定属性的操作。信息管理组件 36 不局限于这些功能，而且可以执行其它诸如生成报告（例如，关于在一个域内的所有用户的报告）、

分析数据（例如，确定某些类型的数据如何频繁地改变）、执行统计分析或者允许用户在某些属性（例如电话号码、电子邮件地址、口令等）上执行自我管理之类的功能。

委托管理工具 28 不局限于一个软件实现。例如，域定义组件 30（即，用户组指定组件 31 和包含属性许可组件 34 以及属性有限值组件 35 的用户属性定义组件 33）、管理特权组件 32 和信息管理组件 36 可以采取硬件或者固件或者软件、硬件和固件的组合的形式。

此外，委托管理工具 28 不局限于域定义组件 30（即，用户组指定组件 31 和包含属性许可组件 34 以及属性有限值组件 35 的用户属性定义组件 33）、管理特权组件 32 和信息管理组件 36。本领域技术人员将会意识到，委托管理工具 28 可能具有其它组件。例如，委托管理工具 28 还可以包含一个工作流程组件，它管理有关用户创建和管理的过程。此外，委托管理工具 28 还可以包含一个报告组件，它报告使用统计、误差状况等。那里还可以有一个事务管理组件，它使用两阶段的提交／反转。委托管理工具 28 能够包含的另一个组件是一个用于查看与管理域的分级有关的信息的浏览组件。

图 5 显示了一个用于实现如图 4 所示的委托管理工具的系统 38 的一个体系结构框图。图 5 显示了访问委托管理工具 28 的几种方式。一个计算单元 40 允许一个管理员访问委托管理工具 28。该管理员能够是超级管理员或者具有委托权限、编辑权限或者其它类型权限的管理员。此外，在该域中的用户可以通过一个计算单元 40 访问委托管理工具 28 来执行某些基本的自我管理。计算单元 40 能够采取手提式数字计算机、个人数字助理计算机、笔记本计算机、个人计算机、或工作站的形式。管理员和用户使用一个诸如 Microsoft INTERNET EXPLORER 或 Netscape NAVIGATOR 之类的网络浏览器 42 以在计算单元 40 上定位和显示委托管理工具 28。一个诸如一个电子或无线网络的通信网络连接计算单元 40 到委托管理工具 28。图 5 显示了计算单元 40 可以通过一个诸如一个外部网或内部网的专用网络 44、或一个诸如一个 WAN（例如，国际互连网）的全球网络 46 连接到委托管理工具 28。如图 5 所示，委托管理工具 28 驻留在一个服务器 48 中，该服务器 48 包含一个服务于委托管理工具 28 和一个数据库目录 52（或多个目录）的网络服务器 50，该数据库目录包含用于在形成团体的所有域中的用户的各

种信息。然而，委托管理工具不是必须与服务器 48 一起驻留的。如果希望的话，系统 38 可以具有允许对访问委托管理工具 28 的用户进行验证和访问控制的功能。验证和访问控制都能够在网络服务器级别由委托管理工具 28 它自己、或是市场上可买到的诸如 Netegrity SITEMINDER 的程序包来处理。

如上所述，在数据库目录 52 中的信息可以包含诸如用户的姓名、位置、电话号码、机构、登录标识、口令等之类的信息。其它信息可以包含该用户对诸如应用程序和内容之类的某些资源的存取特权。数据库目录 52 还可以存储与在支持团体的网络中的物理设备（例如，个人计算机、服务器、打印机、路由器、通信服务器等）有关的信息。存储在该数据库目录 52 中的附加信息可以包含每一个物理设备可得到的服务（例如，操作系统、应用程序、共享文件系统、打印队列等）。数据库目录 52 能够采取一个轻型目录访问协议(LDAP)数据库的形式；然而，能够和委托管理工具 28 一起使用具有其它类型模式的其它目录类型数据库，这包含关系数据库、面向对象的数据库、平面文件、或其它数据管理系统。

使用如图 5 所示的系统 38，一个诸如一个超级管理员或一个具有委托或编辑权限的管理员的管理员能够使用委托管理工具 28 来创建用户属性许可。此外，团体中的用户能够使用委托管理工具 28 来限制用户属性值为允许值的一个子集。图 6 显示了这样一个流程图，它描述了利用委托管理工具 28 为创建一个具有用户属性许可的管理域而执行的动作。为了创建一个管理域，用户必须是一个超级管理员或者一个具有委托权限的管理员。在块 54，超级管理员或具有委托权限的管理员注册。注册动作能够包含输入身份和安全信息（例如，一个有效的用户名和口令）。在 56 处委托管理工具验证该用户名和口令。然后在 58 处，委托管理工具确定该用户是否具有许可以创建一个管理域(即，该用户是一个超级管理员或具有委托权限的管理员）。如果用户没有被验证或不具有许可以创建一个管理域，则该用户不被允许创建一个域。

在 60 处，用户标识能够为该管理域处理的一个属性子集。如上所述，属性可以包含任何数据，它描述了有关一个用户的信息（例如，雇主、工作说明、已经被授予访问许可的资源、地址、使用的设备等）。

接下来，在62处，用户标识定义了一个管理员能和不能在该域中的每一个属性上执行什么类型操作（例如，编辑、查看、删除、等）的许可。然后在64处，用户标识将具有与此相关的有限值的属性。一个属性是否被指定为一个有限值组件的确定由用户进行判断。在66处，用户为已经被标识为具有有限值的属性分配可允许的值。通常，能够预先由一个超级管理员创建用于任何域的有限值属性和允许值的一个列表。因此，当一个具有委托权限的管理员想要创建一个管理域时，标识有限值属性和分配允许值的动作通过从由超级管理员创建的列表中进行选择来执行。例如，考虑一个标识了一个用户位置的“国家”属性。超级管理员能够把“国家”属性限制为国家缩写的一个有限集合。例如，为了表示国家美国、加拿大和墨西哥，超级管理员能够分别定义一组诸如USA、CAN或者MEX的值。因此，正创建一个管理域的一个用户然后能选择这些将和“国家”属性一起使用的有限值。

接下来，用户指定能够被管理的至少一个任意用户组，其中在该组中的每个用户的特征在于在一个管理员能够如何管理这些属性上具有许可的相同属性。特别是，该至少一个任意用户组是在68处通过构造一个查询规则从数据库目录中指定的。该查询的结果定义了在该团体或者域中的用户组成员。在已经构造了该查询规则之后，在70处形成该团体或者域。接下来，在72处，用用于该新创建的管理域的数据来更新该数据库目录。如果一个具有委托权限的管理员想要从他们的操作域中创建另一个域，则重复块 58 - 72。否则，每当一个超级管理员或者一个具有委托权限的管理员希望创建用于他们的操作域的一个管理域时，就重复块54到72。

这个公开中的上述流程图显示了委托管理工具的功能与操作。在这一点上，每块都表示代码的一个模块、段、或部分，它包含用于实现指定的逻辑功能的一条或多条可执行指令。也应注意到，在某些可选择的实现中，在这些块中标注的功能可能没有以附图中标注的顺序出现，或是，例如实际上可能实质同时或以相反顺序被执行，这取决于所涉及的功能。此外，本领域技术人员将会意识到可以增加附加的块。此外，这些功能能够以诸如C++或JAVA之类的编程语言来实现；当然，也能够使用其它语言。

以上描述的委托管理工具包含用于实现逻辑功能的可执行指令的

一个有序列表。该有序列表能够被包含在任何计算机可读介质中，用于由一个基于计算机的系统使用或与之结合使用，其中该基于计算机的系统能够检索这些指令并且执行它们。在这个申请的上下文中，计算机可读介质能够是任何能够包含、存储、传递、传送、传输或输送这些指令的装置。计算机可读介质能够是一个电子的、磁的、光的、电磁的、红外的系统、装置或设备。计算机可读介质的一个说明性、但是未穷举的列表能够包含：具有一条或多条导线的一个电连接（电子的）、一个便携式计算机磁盘（磁的）、一个随机存取存储器（RAM）（磁的）、一个只读存储器（ROM）（磁的）、一个可擦可编程序只读存储器（EPROM或闪速存储器）（磁的）、一个光学纤维（光的）、和一个便携式光盘只读存储器（CDROM）（光的）。

注意到，计算机可读介质可以包含在其上打印这些指令的纸件或另一种适当的介质。例如，这些指令能够经由该纸件或其它介质的光学扫描被电子地获取，然后必要时以一种适当的方式被编译、解释或处理，然后被存储在一个计算机存储器中。

显然已经依据这个发明提供了一种委托管理工具。虽然已经结合本发明的一个最佳实施例对它进行了详细的显示和描述，但是应当明白，在没有背离本发明的范围的情况下能够由本领域技术人员进行变体和修改。

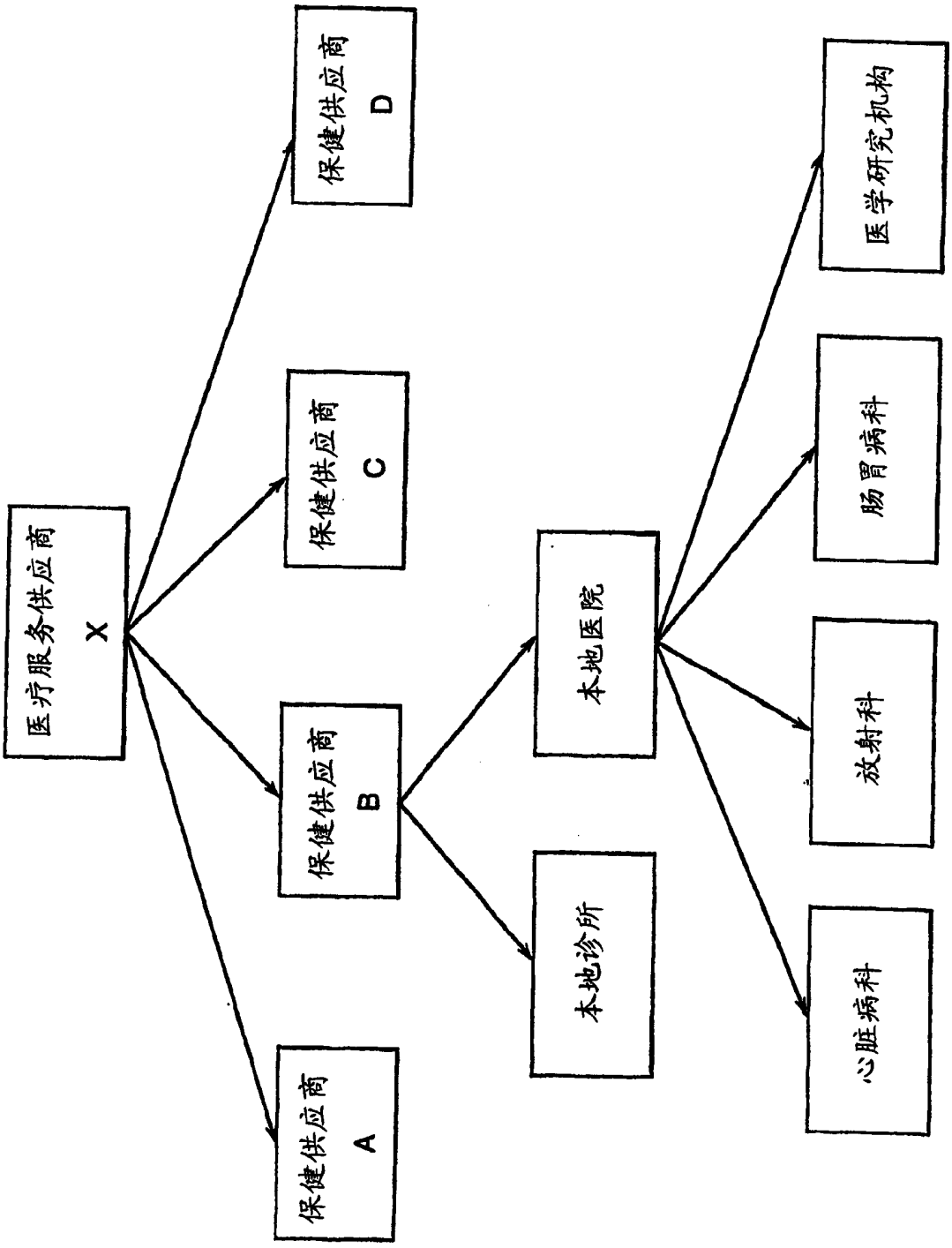

医疗服务供应商
X
保健供应商
A
保健供应商
B
保健供应商
C
保健供应商
D
本地诊所
本地医院
心脏病科
放射科
肠胃病科
医学研究机构

图 1

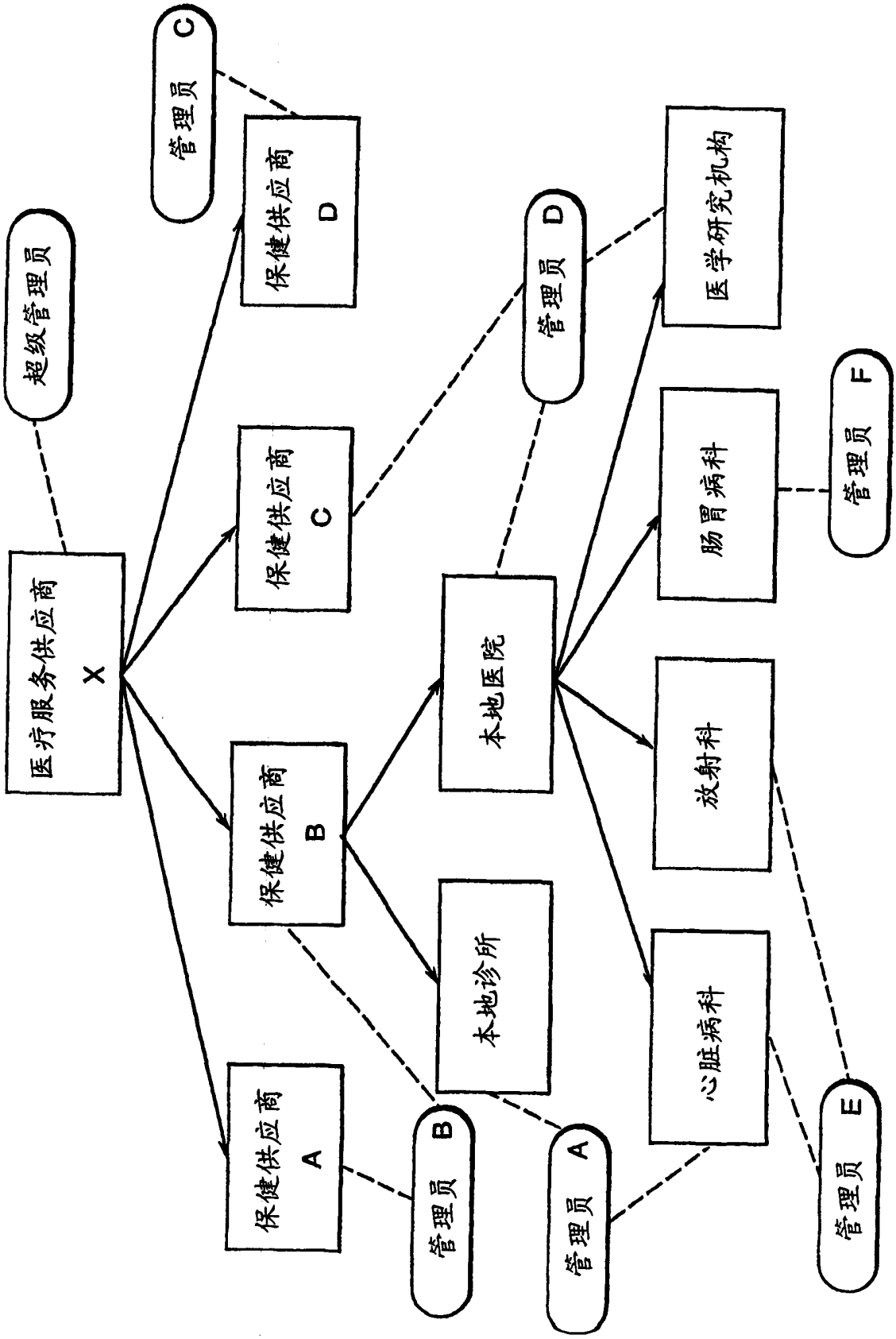

超级管理员
医疗服务供应商
X
管理员 C
保健供应商
D
保健供应商
C
保健供应商
B
保健供应商
A
本地医院
本地诊所
管理员 D
医学研究机构
肠胃病科
管理员 F
放射科
心脏病科
管理员 E
管理员 B
管理员 A

图 2

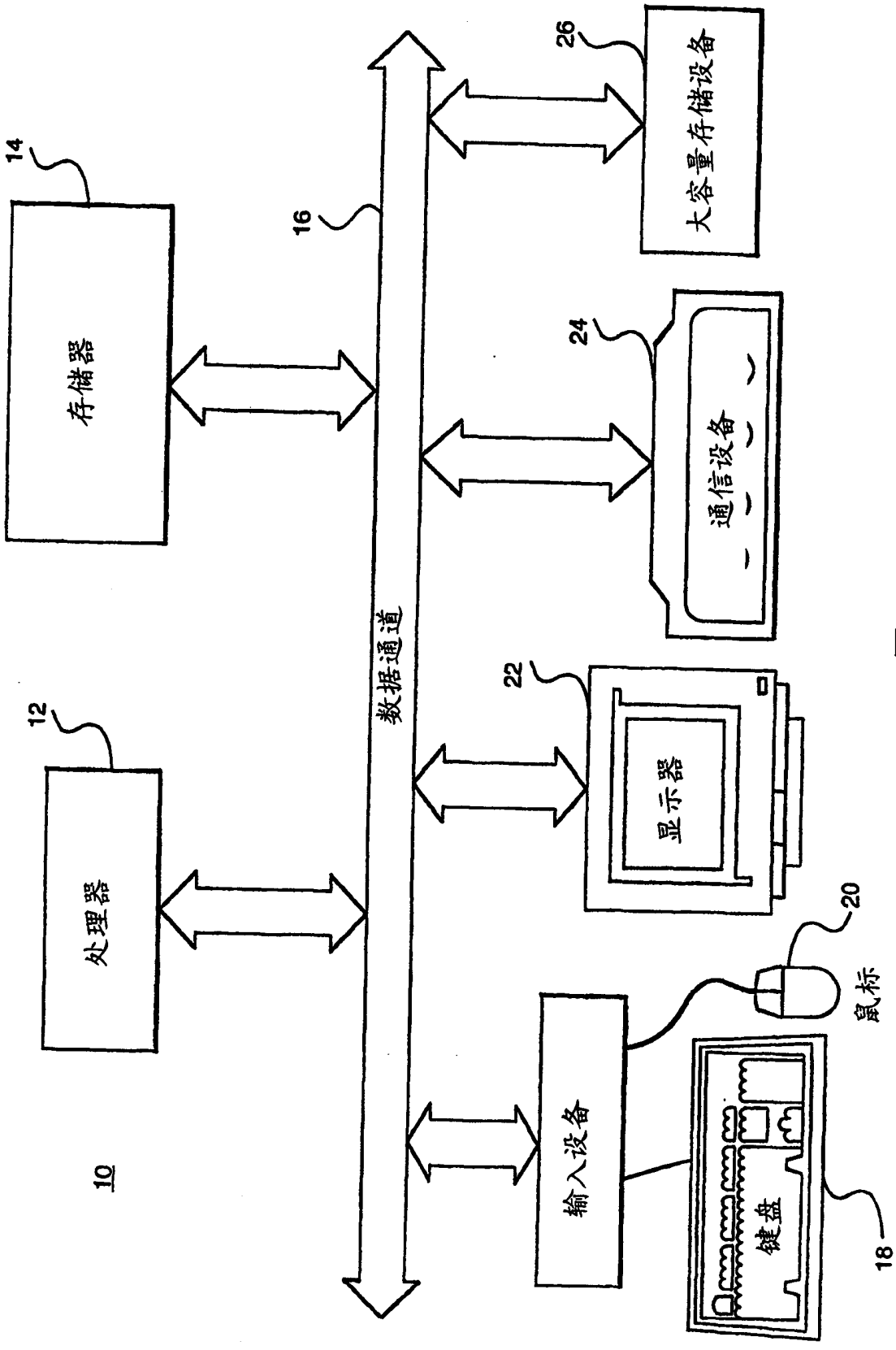

10
处理器
12
存储器
14
数据通道
16
大容量存储设备
26
通信设备
24
显示器
22
输入设备
鼠标
20
键盘
18

图 3

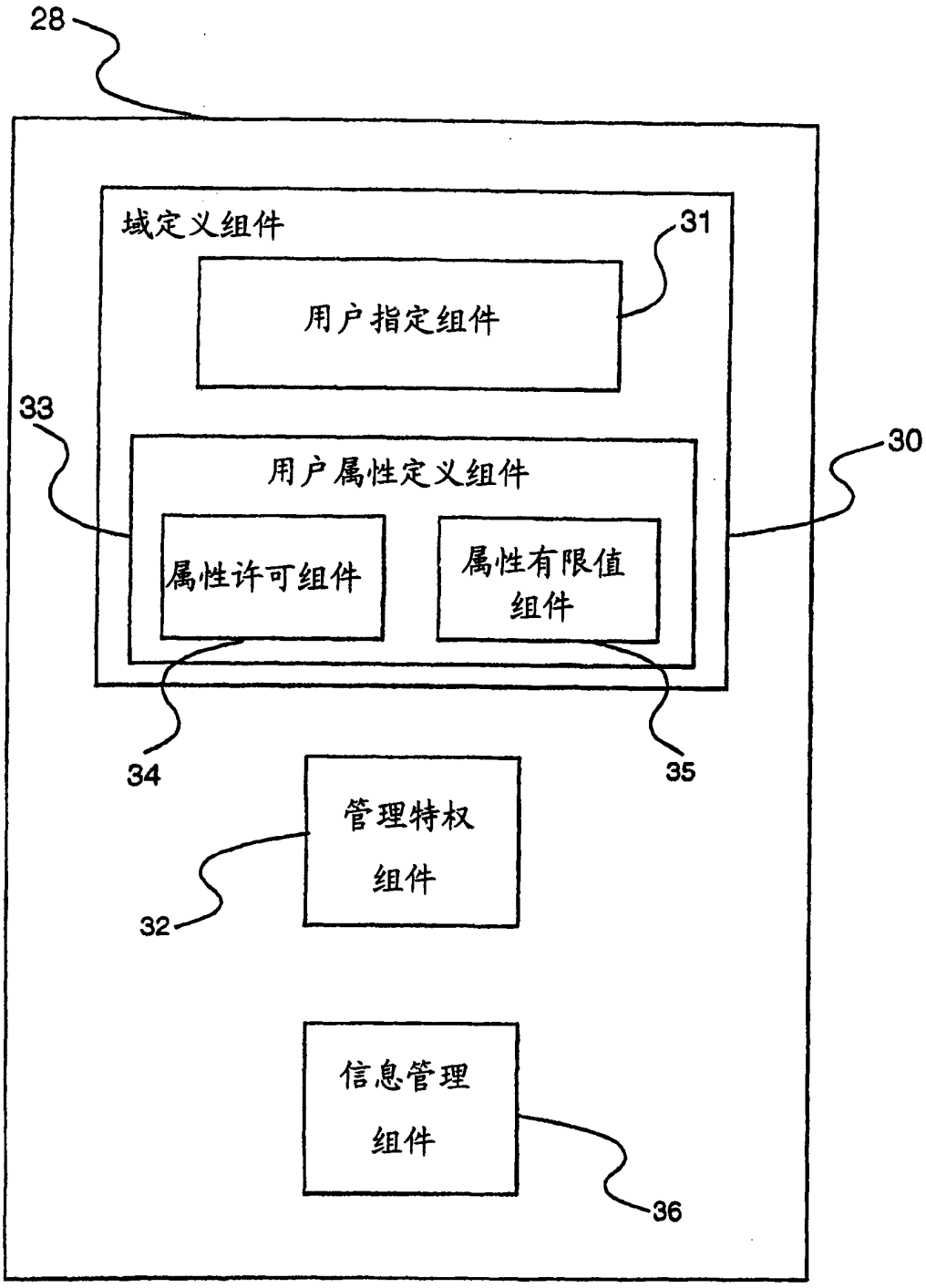

28
域定义组件
31
用户指定组件
33
用户属性定义组件
30
属性许可组件
属性有限值组件
34
35
管理特权组件
32
信息管理组件
36

图 4

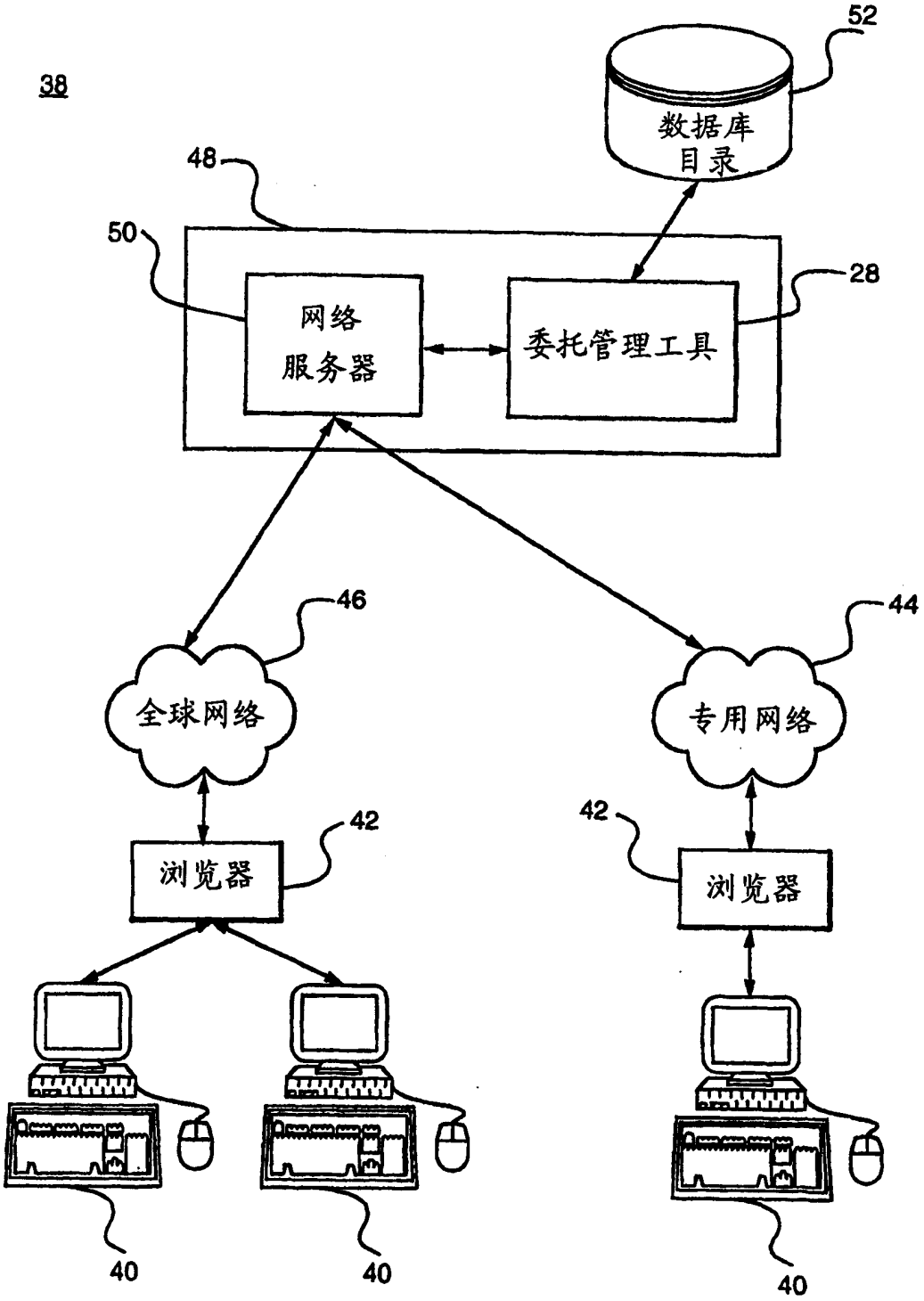

38
52
数据库
目录
48
50
网络
服务器
委托管理工具
28
46
44
全球网络
专用网络
42
浏览器
42
浏览器
40
40
40

图 5

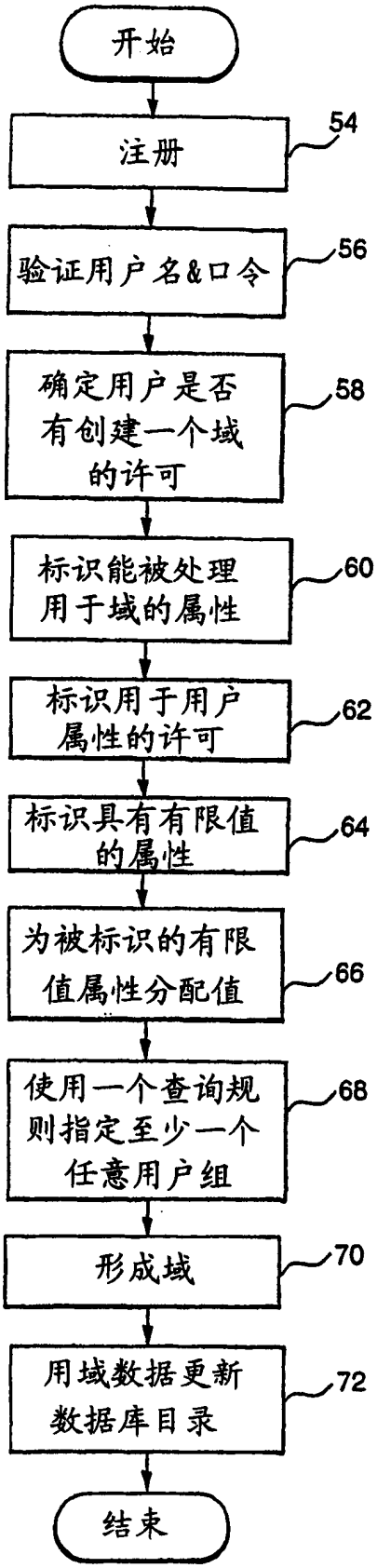

开始
注册
54
验证用户名&口令
56
确定用户是否有创建一个域的许可
58
标识能被处理用于域的属性
60
标识用于用户属性的许可
62
标识具有有限值的属性
64
为被标识的有限值属性分配值
66
使用一个查询规则指定至少一个任意用户组
68
形成域
70
用域数据更新数据库目录
72
结束

图 6