[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 29/06 (2006.01)
H04L 12/24 (2006.01)

[12] 发明专利说明书

专利号 ZL 200610057795.5

[45] 授权公告日 2009 年 9 月 23 日

[11] 授权公告号 CN 100544362C

[22] 申请日 2006.2.27
[21] 申请号 200610057795.5
[30] 优先权
[32] 2005. 6. 9 [33] JP [31] 2005 - 169403
[73] 专利权人 株式会社日立制作所
地址 日本东京都
[72] 发明人 加藤崇利 常广隆司 幡野富久
[56] 参考文献
CN 1141653C 2004.3.10
CN 1303054A 2001.7.11
JP2005 - 12775A 2005.1.13
CN 1503525A 2004.6.9
审查员 张 玉

[74] 专利代理机构 北京银龙知识产权代理有限公司
代理人 许 静

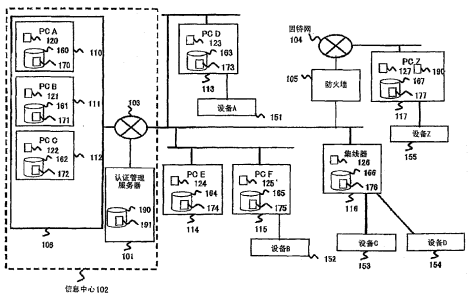
权利要求书 4 页 说明书 32 页 附图 15 页

[54] 发明名称

设备管理系统

[57] 摘要

本发明的目的是，在服务器客户机方式的系统中，不损失使用者的便利性、提供具有安全地共享设备的功能的设备管理系统。 设备连接到使用者使用的终端或者在网络上连接的集线器上。 通过在终端等上安装的具有设备驱动程序功能和通信功能的设备管理管理程序、在服务器上安装的具有设备驱动程序功能和通信功能的虚拟设备管理程序、和管理设备的访问权限的认证服务器，管理对设备的访问，同时能够和虚拟地把设备直接连接在服务器上同样使用该设备。



1. 一种设备管理系统，它用于在用网络连接执行应用程序的服务器、对所述服务器给出上述应用程序的执行的指示并从该服务器接收执行结果的客户机和认证所述客户机的认证服务器的系统中，从所述服务器控制在所述客户机上连接的设备，其特征在于，

所述客户机，具有收发在该客户机上连接的设备的设备驱动程序和数据的同时在和所述服务器之间收发该数据的设备管理单元；

所述认证服务器，具有管理该设备管理系统内的各设备的使用权限的设备信息保存单元；

所述服务器，具有遵照在所述设备信息保存单元中保存的所述使用权限，控制在该服务器内动作的应用和所述设备管理单元之间通过所述网络进行的数据的收发的虚拟设备管理单元。

2. 根据权利要求 1 所述的设备管理系统，其特征在于，

所述设备管理单元，在连接了所述设备时，向所述认证服务器发送作为确定该设备的信息的设备信息，

所述认证服务器，进一步具有保存预先设定的所述各设备的使用权限的策略保存单元，

当接收到所述设备信息时，遵照在所述策略保存单元中保存的信息，在所述设备信息保存单元中登录由所述接收到的设备信息确定的设备的使用权限。

3. 根据权利要求 1 所述的设备管理系统，其特征在于，

所述客户机向所述服务器发送访问请求，

当所述服务器接收到所述访问请求时，该服务器具有的虚拟设备管理单元，参照所述设备信息保存单元，在和客户机装置具有的设备管理单元之间形成通信路径，由此来执行控制，所述客户机装置连接所述访问请求的发送源的客户机的使用者具有使用权限的设备。

4. 根据权利要求 3 所述的设备管理系统，其特征在于，

所述虚拟设备管理单元，当所述服务器接收到访问请求时，在参照所述

设备信息保存单元前，向所述认证服务器发送更新该设备信息保存单元的信息的更新指示，

所述认证服务器，一旦接收所述更新指示，对于在所述网络上连接的客户机，指示与所述设备信息一起获取作为表示该设备的现在的使用状况的信息的设备状态信息，遵照对于指示返回的所述设备信息以及所述设备状态信息，更新所述设备信息保存单元的信息，

在所述客户机接收到获取所述设备信息以及所述设备状态信息的指示时，该客户机具有的所述设备管理单元，取得在该客户机上连接的设备的所述设备信息以及所述设备状态信息，向所述认证服务器返送。

5. 根据权利要求 4 所述的设备管理系统，其特征在于，

所述设备信息保存单元，对于各设备还保存是否需要排他控制以及各设备的现在的使用状况，

所述虚拟设备管理单元，在所述服务器接收到访问请求时，在该使用请求的请求源具有使用权限的设备是需要所述排他控制的设备、表示所述使用状况是由其他使用者占有的场合，在把所述使用状况更新为表示该占有结束后，在和连接该设备的客户机的所述设备管理单元之间形成通信路径。

6. 根据权利要求 3 所述的设备管理系统，其特征在于，

所述客户机具有用户接口，

通过该用户接口，将从用户输入的确定用户的信息以及认证号码作为访问请求来接收，向所述服务器发送。

7. 根据权利要求 3 所述的设备管理系统，其特征在于，

所述客户机，与所述设备信息一起，向所述服务器发送作为使用该设备的请求的设备使用请求，

所述虚拟设备管理单元，进一步具有：

在装备该虚拟设备管理单元的服务器接收到访问请求时，通过所述通信路径向连接该设备的客户机具有的设备管理单元发送确认由该访问请求确定的设备的动作的动作确认指示的动作确认指示单元；

监视使用所述通信路径的通信是否正常进行的通信状态监视单元；和

在对于所述动作确认指示的返回信息，表示动作状态不正常的场合，或

者在所述通信状态确认单元中、通过所述监视检测出所述通信未正常运行的场合，向所述认证服务器通知该意思的不正确通知单元。

8. 根据权利要求 7 所述的设备管理系统，其特征在于，

所述设备管理单元，进一步具有：

在所述通信路径形成后，监视通过所述通信路径的通信状态以及装备该设备管理单元的客户机上连接的设备的动作状态的监视单元；和

在通过所述监视检测出是不正确状态的场合，向所述认证服务器通知该意思的第二不正确通知单元。

9. 根据权利要求 7 所述的设备管理系统，其特征在于，

所述认证服务器，在从所述通知单元或者所述第二不正确通知单元接收到意思是不正确状态的通知的场合，从所述设备信息保存单元中删除处于该不正确状态中的设备以及处于不正确状态的通信路径作为通信对象的设备。

10. 根据权利要求 1 所述的设备管理系统，其特征在于，

所述设备管理单元、所述虚拟设备管理单元以及所述认证服务器，分别具有作为日志记录收发的数据以及事件的日志保存单元，

所述认证服务器，还具有收集并显示在自身的日志保存单元中记录的日志、在所述设备管理单元的日志保存单元中记录的日志、和在所述虚拟设备管理单元的日志保存单元中记录的日志的显示单元。

11. 根据权利要求 10 所述的设备管理系统，其特征在于，

所述认证服务器，在从所述通知单元或者所述第二不正确通知单元接收到意思是不正确状态的通知的场合，在所述认证服务器的日志保存单元中保存该通知。

12. 根据权利要求 2 所述的设备管理系统，其特征在于，

所述虚拟设备管理单元，进一步具有显示在现时刻在该设备管理系统中可使用的设备的所述设备信息的第二显示单元。

13. 根据权利要求 1 所述的设备管理系统，其特征在于，

进一步具有装备连接所述网络的接口的第二设备，

所述设备，具有：

在和所述服务器之间进行数据的收发的第二设备管理单元；和

在该设备连接到所述网络上时、向所述认证服务器发送该设备的所述设备信息的设备连接单元。

14. 根据权利要求 13 所述的设备管理系统，其特征在于，

所述第二设备，进一步具有取得认证该设备的使用者的信息、向所述认证服务器发送的认证单元。

15. 一种客户机，是在用网络连接执行应用程序的服务器、对所述服务器给出所述应用程序的执行的指示并从该服务器接收执行结果的客户机、和认证所述客户机的认证服务器的系统中、从所述服务器控制在所述客户机上连接的设备的设备管理系统中的所述客户机，其特征在于，

具有在收发在该客户机上连接的设备的设备驱动程序和数据的同时在和所述服务器之间收发该数据的设备管理单元。

16. 根据权利要求 15 所述的客户机，其特征在于，

所述设备管理单元，在向所述客户机连接设备时，或者从所述认证服务器接收到指示时，向所述认证服务器发送确定该连接的设备的设备信息。

17. 根据权利要求 16 所述的客户机，其特征在于，

所述设备管理单元，在从所述认证服务器接收到指示时，与所述设备信息一起，还返回表示该设备的使用状况的设备状态信息。

18. 一种服务器，是在用网络连接执行应用程序的服务器、对所述服务器给出所述应用程序的执行的指示并从该服务器接收执行结果的客户机和认证所述客户机的认证服务器的系统中，从所述服务器控制在所述客户机上连接的设备的设备管理系统中的所述服务器，其特征在于，具有：

根据在所述认证服务器中保存的所述设备管理系统内的各设备的使用权限、在和所述客户机之间形成通信路径的通信路径形成单元；

执行在该服务器内运行的应用程序和为使在所述客户机上连接的设备动作的数据的收发的设备驱动程序单元；和

通过在所述通信路径形成单元中形成的通信路径，与所述客户机收发所述设备驱动程序单元收发的数据的通信单元。

设备管理系统

技术领域

本发明涉及管理对通过网络连接在服务器上的设备的访问的技术。特别是，涉及在和设备直接连接在服务器上的场合同样地可虚拟地使用该设备的系统中，能够安全而且简便地远距离操作的技术。

背景技术

在通过因特网或者企业内的内部网等网络进行通信时，每人可利用的的数据传送频带正在宽频带化。莫说是从企业内部的设备对外部的服务器的访问，从家庭或饭店、热点（注册商标）对企业内部的设备以数 Mbps～数十 Mbps 的频带的访问也成为可能。在从家庭或者街上利用因特网的场合，即使可永远在线价格也不贵。

另外，个人计算机（PC）或者 PDA、便携电话等信息设备的低价格化不断发展，给大部分从业人员配备信息终端进行业务处理的企业日增。多数企业，为迅速处理业务，已经许可在出差地点或者自己家、移动中等办公室外的场所利用信息设备，访问企业内的 PC 或者服务器等设备。

这样的访问称为远程访问功能，在公司内设置具有进行加密通信的虚拟专用网络（VPN）功能的服务器，通过该服务器，在和办公室外的信息设备的通信中，进行加密中途路径上的通信等的管理。随着从办公室外来的远程访问变成普通的事情，不仅从办公室外对邮件服务器或者 WEB 服务器进行访问，执行部分业务，而且身处在办公室内时执行的业务的大部分也正在转移为远距离执行的业务形式。

作为为导入这样的业务形式的方法，可以举出称为服务器客户机方式的系统运用的方式。服务器客户机方式的系统，称为网络计算系统或者基于服务器的计算等，在服务器侧存储主要的程序或数据，从 PC 或瘦客户机那样的客户机侧进行操作。在服务器客户机方式中，因为运算处理或者数据的存储主要在服务器侧执行，所以在瘦客户机那样的客户机侧，减少了各自进行

OS 或者业务中使用的应用程序的版本升级或故障确定、病毒对策或病毒清除的必要性或频度，可以减低整体的管理成本，增加安全性（例如参照特开 2005—12775 号公报）。

发明内容

在服务器客户机方式中，也可以把服务器和客户机设置在物理上分开的场所。

在这样的服务器客户机方式中，作为使用者在服务器上使用在 CD—ROM 驱动器或打印机等信息设备上连接的外围设备（下面，在本说明书中称为设备）的方法，有在服务器上直接连接该设备加以利用的方法。在这种场合，即使在客户机侧不安装该设备的驱动程序，客户机通过服务器侧的驱动程序也能使用该设备。另外，也可以由多个客户机共享该设备。但是，在这种场合，因为在客户机侧的操作环境中没有在服务器上直接连接的设备（例如 CD—ROM）的驱动程序，所以不能执行取出 CD—ROM 等的操作。

另外，有在内部网等网络上作为共享设备配置相应设备，在客户机侧安装该设备的驱动程序，通过该驱动程序使用相应设备的方法。在这种场合，在把 CD—ROM 插入 CD—ROM 驱动器上后，如不采取访问限制等措施，则存在由保存该设备的驱动程序的第三者不正当访问的可能性，存在安全方面的问题。特别是在服务器存在于网络上的场合，因为在服务器上虚拟连接多个客户机可使用的共享设备，带有安全风险，所以需要认证或加密等充分提高安全性的措施。

另外，如果是像 CD—ROM 驱动器那样普通的设备，则各个客户机有驱动程序，而服务器以及客户机的 OS 提供进行设备共享的功能的可能性很高，所以在本方法中有可能进行设备的共享。但是，在需要具有特别功能的驱动程序的特殊设备的场合，需要为共享相应设备的专用功能，因为一般在 OS 中多数不提供这样的功能，所以难于实现在客户机侧具有设备的驱动程序的结构中的设备的共享。

本发明是鉴于上述情况提出的，其目的是，在服务器客户机方式中共享设备的场合，不损失使用者的方便性，可提高系统内的安全性。

因此，本发明，管理使在网络上连接的设备虚拟地在服务器上动作的场

合的访问权限。

具体说，是在用网络连接执行应用程序的服务器、向所述服务器给出执行应用程序的指示并从该服务器接收执行结果的客户机、和认证所述客户机的认证服务器的系统中，从所述服务器控制在所述客户机上连接的设备的设备管理系统，其特征为，

所述客户机，具有在收发在该客户机上连接的设备的设备驱动程序和数据的同时在和所述服务器间收发该数据的设备管理单元；

所述认证服务器，具有管理该设备管理系统内的各设备的使用权限的设备信息保存单元；

所述服务器，具有遵照在所述设备信息保存单元中保存的所述使用权限、控制在该服务器中动作的应用程序、和设备管理单元之间通过所述网络执行的数据的收发的虚拟设备管理单元。

根据本发明，在服务器客户机方式中共享设备的场合，能够不损失使用者的方便性、提高系统内的安全性。

附图说明

图 1 是第一实施形态的管理系统的框图；

图 2 是第一实施形态的策略表的一例；

图 3 是表示第一实施形态的设备信息表的一例的图；

图 4 是第一实施形态的认证管理服务器保存的使用者信息数据库的一例；

图 5 是第一实施形态的刀片服务器保存的 PC 使用管理表的一例；

图 6 是第一实施形态的设备共享处理的处理流程；

图 7 是第一实施形态的设备共享处理结束时的处理流程；

图 8 是用于说明第一实施形态的设备管理管理程序、虚拟设备管理程序的动作的图；

图 9 是说明第一实施形态的设备使用时的动作的流程；

图 10 是说明第一实施形态的设备使用时的动作的流程；

图 11 是通过管理应用程序显示的日志管理画面的一例；

图 12 是第一实施形态的虚拟设备管理程序的设备管理画面的一例；

图 13 是第二实施形态的管理系统的框图；

图 14 是第三实施形态的管理系统的框图；

图 15 是第一实施形态的 PC—A 的硬件结构图。

具体实施方式

下面参照附图详细说明本发明的实施形态。

<<第一实施形态>>

以下使用附图说明本发明的设备管理系统的第一实施形态。

图 1 是本实施形态的设备管理系统的详细的框图。本实施形态的设备管理系统，装备：具有认证服务器 101、网络 103、刀片服务器 106 的信息中心 102；和在该信息中心的网络 103 上连接的 PC 等客户机装置。

信息中心 102，是在管理信息设备的中心中限制通常的房间出入、管理监视设置的设备的区域。信息中心的设置场所不加限定。例如，可以设置在使用者使用客户机装置等终端的场所，也可以设置在离开的场所。在使用者在办公室等处使用终端的场合，信息中心 102 也可以设置在管理使用者的企业团体的建筑物内。在使用者是一般消费者、从自己家或饭店、街头等使用服务提供企业的服务的场合，信息中心 102 也可以设置在因特网服务提供商或服务器出租企业、应用服务提供商等管理的建筑物内。另外，也可以是在使用者自己家或者在办公室的一角集中服务器的区域。

认证管理服务器 101，是执行设备或使用者的认证和管理的设备，由信息中心 102 的管理者管理。有关认证管理服务器 101 为实现这点而保存的各种数据，后面叙述。认证管理服务器 101，使用具有通信接口、CPU 以及存储器的信息处理装置实现，通过 CPU 执行在存储器中存储的程序实现各种功能。此外，实现各功能的程序，也可以通过存储介质、或者包含载波、数字信号、通信线的通信介质，从其他装置取得。

刀片服务器 106，是在内部具有多个服务器或者 PC 的设备，具有连接未图示的电源、内部设备和网络 103 的接口功能、管理装置等。在本实施形态中，举例说明内部具有 PC—A110、PC—B111、PC—C112 的情况。当然，刀片服务器 106 的结构不限于此，可安装或拆除这些以外的 PC 或服务器。

网络 103 相互连接认证管理服务器 101、PC—A110、PC—B111、PC—

C112 等。在本实施形态中，以下对于使用 TCP/IP 协议进行通信的网络进行说明。当然也可以是遵照这以外的协议进行通信的网络。

此外，在本实施形态中，PC—A110、PC—B111、PC—C112，被构成在刀片服务器 106 内，但是也可以不设置在刀片服务器 106 内部甚至不设置在信息中心 102 内而在网络 103 上存在。PC—A110、PC—B111、PC—C112，作为 PC 记载，但是无论是服务器，工作站还是内置设备，只要是在存储器和 CPU 上执行在存储介质中存储的 OS 或应用程序的信息设备，就不加以限定。

图 15 是 PC—A110 的硬件结构图。PC—A110 具有硬盘驱动器或闪烁存储器等存储设备 160、存储器 110a、CPU110b 和作为用于通信的接口的通信接口 103c。在 PC—A110 中，通过由 CPU 执行读入存储器的程序，就能实现各处理部。此外，各程序也可以通过存储介质或者通信介质从其他装置取得。此外，所谓通信介质，包含载波、数字信号、通信线。

PC—A110 遵照使用者的指示执行运算。运算结果在 PC—A110 或者刀片服务器 106 上连接的未图示的显示器上显示。在存储设备 160 内，由管理者安装虚拟设备管理程序 120。一起动 PC—A110，就从存储设备 160 把 OS 读入存储器 110b，在由 CPU110a 执行而成为可使用状态后，虚拟设备管理程序 120 被读入存储器 110b，由 CPU110a 执行后虚拟设备变得可以使用。

这里所说的虚拟设备，是把在 PC—A110 上通过网络 103 连接的设备仿佛是直接连接在 PC—A110 上的设备那样可使用的机构。通过本机构，连接位于分离场所的设备，变得和在 PC—A110 上物理连接的设备同样可以使用。

虚拟设备管理程序 120，是控制为进行和在 PC—A110 上通过网络 103 连接的设备 A151 之间的数据的收发的软件。用于实现虚拟地和在服务器上直接连接的场合同样可使用设备 A151 的功能。关于其细节，和后述的设备管理管理程序 123 一起在后面说明。

另外，在存储设备 160 中，把虚拟设备管理程序 120 收发的数据以及在虚拟设备管理程序 120 中发生的事件作为日志 170 存储。有关日至 170 的细节后述。

PC—B111 以及 PC—C112 有和 PC—A110 同样的结构。在内部分别具有

存储设备 161、162，同时安装虚拟设备管理程序 121、122，起动后动作。以后，在不需要特别区分 PC—A110、PC—B111、PC—C112 的场合，以 PC—A110 为代表加以说明。

此外，存储设备 160～162，也可以不在刀片服务器 106 内存在，而在网络 103 上存在。

下面，作为客户机装置说明在网络 103 上连接的设备。

在本实施形态中，作为客户机装置，举例说明装备 PC—D113、PC—E114、PC—F115、集线器 116、防火墙 105 以及通过因特网 104 连接的 PC—Z117 的情况。另外，举例说明在 PC—D113 上连接设备 A151、在 PC—F115 上连接设备 B152、在集线器 116 上连接设备 C153 以及设备 D154、在 PC—Z117 上连接设备 Z155 的情况。各客户机装置以及设备的连接结构不限于此。

PC—D113，是遵照使用者的指示进行运算，根据需要使用设备，向使用者提示运算结果的信息处理装置。硬件结构、各处理部的实现方法和上述 PC—A110 基本相同。PC—D113，通过未图示的网络接口连接到网络 103 上。PC—D113，具有硬盘驱动器或闪光存储器等存储设备 163 以及未图示的存储器以及 CPU，根据使用者的指示进行运算。运算结果在 PC—D113 上连接的未图示的显示器上显示。从使用者来的指示，通过未图示的键盘或鼠标这样的用户接口向 PC—D113 发送。

另外，PC—D113，在存储设备 163 内安装设备管理管理程序 123。一起动 PC—D113，就从存储设备 163 把 OS 读入存储器 110b，通过 CPU 执行而成为可使用状态后，设备管理管理程序 123 被读入存储器，通过 CPU 执行，连接的设备 A151 在 PC—A110 上作为虚拟设备变得可以使用。另外，在存储设备 163 上，把设备管理管理程序 123 收发的数据等作为日志 173 存储。有关日志 173 的细节，后述。

设备管理管理程序 123，是 PC—D113 为把设备 A151 作为刀片服务器 106 的 PC—A110 的虚拟设备使用的软件。其细节和虚拟设备管理程序 120 一起，后述。

PC—E114、PC—F115、PC—Z117 具有基本与 PC—D113 相同的结构，分别具有存储设备 164、165、167。另外，实现设备管理管理程序 124、125、

127。另外，在各存储器中分别存储日志 174、175、177。

再有，集线器 116 是从 PC—D113 去掉显示画面等的一般功能的一部分的设备。亦即，通过未图示的网络接口连接因特网，具有硬盘驱动器或闪光存储器等存储设备 166 以及未图示的存储器及 CPU，进行运算。硬件结构、各处理部的实现方法，基本和 PC—A110 相同。在实现设备管理管理程序 126 的同时，在存储设备 166 中保存日志 167。以后，在不需要特别区分 PC—D113、PC—E114、PC—F115、PC—Z117、集线器 116 的场合，以 PC—D113 为代表进行说明。

设备 A151，是在信息设备上连接的例如 CD—ROM 或打印机等的外围设备。设备 A151，通过设备连接用的接口和 PC—D113 连接。设备连接用的接口，例如可以考虑为在 PC 上连接通用串行总线（USB）、无线 USB、近距离无线通信接口、红外线通信接口、串行端口接口、并行端口接口、IEEE1394 接口、PS/2 接口（注册商标）、音频接口这样的设备。在本实施形态中，举例说明接口是 USB 的情况，但是接口不限于此。

另外，设备 A151，通过在连接的 PC—D113 中安装的设备管理管理程序 123 作为虚拟设备在本系统中使用。以后，把设备管理管理程序 123 称为管理设备 A151 的设备管理管理程序。

另外，在各 PC 以及总线上连接的设备 B152、C153、D154 也是和设备 A151 同样的外围设备，在本实施形态中，作为一例通过 USB 接口连接 PC 或者集线器。以后在不需要特别区分设备 A151、设备 B152、设备 C153、设备 D154 的场合，以设备 A151 为代表进行说明。

下面就其认证管理服务器 101 保存的策略表 1400、设备管理表 200 以及使用者信息数据库 300 进行说明。认证管理服务器 101，和虚拟设备管理程序 120 和设备管理管理程序 123 一起控制对各设备的访问。

策略表 1400 登录关于本系统内管理者管理的设备的访问策略。例如，登录每个设备的使用权限、对应连接设备的客户机装置的使用权限等。本表预先由管理者等设定。策略表 1400，可由系统的管理者自由变更。另外，通过不设定策略表 1400，也可以将系统构成为不能自动变更设备信息表 200 上的规则，而仅能用手工变更。管理者遵照自己管理的系统中要决定的策略构成

策略表 1400。

图 2 表示策略表 1400 的一例。如该图所示，策略表 1400，对于每一策略，记录策略号码 1401、设备名 1402、连接应用程序的地址 1403、连接应用程序的网络接口 ID1404、销售商 ID1405、产品 ID1406、序列号 1407、设备类别 1408、排他控制 1409、可否使用 1410、可使用 ID1411。当然，也可以记录其他项目。

策略号码 1401，是由管理者在策略表 1401 内登录策略信息时自动赋予各策略的识别号码。在增减在本系统上可使用的机器或设备时，遵照在策略表 1400 中登录的策略生成后述的设备信息表 200 的记录。在系统上增减适用于多个策略的机器或设备时，按照预定的优先顺序使用策略。

设备名 1402、连接应用程序的地址 1403、连接应用程序的网络接口 ID1404、销售商 ID1405、产品 ID1406、序列号 1407、设备类别 1408，和在后述的设备信息表 200 中记载的内容相同，表示机器或者设备的信息。管理者设定各自的相应每一个策略的设备名、连接应用程序的地址、连接应用程序的网络接口 ID、销售商 ID、产品 ID、序列号、设备类别的条件。有关它们的细节，在对设备信息表 200 的说明中加以说明。

排他控制 1409，是在使用者使用设备时定义是否禁止别的使用者使用的值。可设定“必须”、“可能”、“不要”、或“不定义（*）”。在“不定义（*）”的场合，基本上和不要相同对待，但是也可以对设备的每一类别、分类自动设定构成。这里，所谓分类，例如是键盘、存储设备等在同一设备驱动程序（分类驱动程序）下动作的设备类别。

可否使用 1410 表示在执行设备的使用许可时的认证管理服务器 101 的举动，可设定为“可能”、“禁止”、或“警告”。设定为“可能”的策略，是自动使在后述的可使用 ID1411 中记载的使用者可使用该机器或设备的策略。设定为“禁止”的策略，是自动使在后述的可使用 ID1411 中记载的使用者不可使用该机器或设备的策略。设定为“警告”的策略，是在对后述的可使用 ID1411 中记载的使用者显示警告后自动可使用该机器或设备的策略。警告显示可对每一策略设定。

此外，图中的*标记是不定义的意思，管理认证服务器 101 进行记述内容

和实际信息的匹配。

例如，在图 2 中策略号码 1401 是 1 的策略，是设备名 1402、连接应用程序的地址 1403、连接应用程序的网络接口 ID1404、序列号 1407、设备类别 1408 不定义的策略。亦即在有关于销售商 ID1405 是“1001”、产品 ID1406 是“1001”的设备的策略的询问的场合，与其设备名、连接应用程序的地址、连接应用程序的网络接口 ID、序列号、设备类别无关，在设备信息表 200 中记录排他控制 1409 是“不要”、可否使用 1410 是“可能”、可使用 ID1411 是 20000001、20000010 等。

另外，策略号码 1401 是 2 的策略，是仅对由销售商 ID 是“1105”、设备类别以“B Ltd.”开始的设备，自动地把排他控制设定为“必须”、把可使用 ID 设定为 20000011 的策略。

然后，策略号码 1401 是 3 的策略，是对于连接应用程序的地址 1403 是 192.168.1.1、连接应用程序的网络接口 ID1404 是“00：00：00：00：00：01”的客户机装置上连接的设备，自动地把排他控制 1409 设定为“不定义”、关于可否使用 1410 是置成“警告”显示后对所有用户设定为可使用的策略。

另外，策略号码 1401 是 n 的策略，是对于所有的设备设定禁止使用的策略。亦即，在存在对未在策略表 1400 中登录的设备的登录的委托的场合，认证管理服务器 101，参照策略号码 1401 是 n 的栏，在设备信息表 200 中把排他控制 1409 设定为“不要”、把可否使用 1410 设定为“禁止”。

下面说明设备信息表 200。设备信息表 200，用于管理为管理在本系统上连接的各设备的访问的必要的信息。登录的各记录，由设备管理管理程序 123，遵照在和使自身管理的设备变得可在本系统内共享的请求（下面称设备连接请求）一起发送的、特别指定设备的各种信息（下面称设备信息）上加上在策略表 1400 中登录的策略来生成。虚拟设备管理程序 120 使用设备信息表 200，控制各设备可否使用。

在由设备管理管理程序 123 连接或者取下设备时，作为设备信息，至少发送在网络 103 上特别指定发送源的客户机装置的信息（在本实施形态中是 IP 地址和 MAC 地址）、特别指定该设备的信息（在本实施形态中是销售商 ID、产品 ID 和序列号）和表示是连接还是卸下的信息。认证管理服务器 101，遵

照策略表 1400，生成记录，在设备信息表 200 中登录。

另外，在客户机装置自身从网络 103 被切离的场合，向认证管理服务器 101 发送特别指定该客户机装置的信息和表示切离的信息。

认证管理服务器 101，例如在增减设备时、在切离客户机装置时、增减使用系统的使用者时、变更网络结构时、认证管理服务器 101 管理的系统的结构有变更时、策略表 1400 的记录有变更时、从管理者接收设备信息表 200 的更新的指示时，更新设备信息表 200。另外，如后述，关于状态，每隔规定期间进行更新。

图 3 是表示设备信息表 200 的一例的图。如本图所示，设备信息表 200，具有：设备 ID201、设备名 202、连接应用程序的地址 203、连接应用程序的网络接口 ID204、销售商 ID205、产品 ID206、序列号 207、设备类别 208、排他控制 209、状态 210、可使用 ID211、使用用户 ID212。

设备 ID201，用于唯一识别管理的各设备，在每次有新登录请求时自动形成。另外，是每当认证管理服务器 101 或设备管理管理程序 123 的起动或结束、设备插拔等时可能变更的临时 ID。

设备名 202，是为容易调用设备的名称，预先由管理者或使用者设定。在管理者设定的场合，在策略表 1400 内登录好设备名，在生成设备信息表 200 的记录时，从策略表 1400 中抽出进行登录。另一方面，在使用者设定的场合，在设备信息中包含，通知认证管理服务器 101。

连接应用的地址 203，记录连接设备的客户机装置（在设备 A151 的例子中是 PC—D113）的 IP 地址。作为设备信息通知它们。这些地址，在上述客户机装置在子网络间进行移动等场合，即使在使用中也有可能适宜变更。

网络接口 ID204，记录表示连接设备的客户机装置（在设备 A151 的例子中是 PC—D113）的网络接口的 ID 的号码。如本实施形态在网络使用 TCP/IP 协议的场合，作为网络接口 ID 可使用 MAC 地址。网络接口 ID204，和连接应用的地址不同，是设备中固有的，设备不变更的话，不能变更。

销售商 ID205、产品 ID206、序列号 207，是预先给设备自身赋予的设备的识别号码，在客户机装置（在设备 A151 的例子中是 PC—D113）上连接设备时，作为设备信息被取得。这些信息，作为设备信息从客户机装置向认证

管理服务器 101 发送。各设备，通过销售商 ID、产品 ID、序列号的组进行识别。销售商 ID 以及产品 ID 是唯一赋予每一销售商以及产品的 ID。另外，顺序号是给每一产品个别赋予的号码。

设备类别 208 是为使用者理解由销售商或管理者赋予的名称。在销售商赋予的场合，从说明符那样的设备信息中抽出，包含在设备信息中进行通知。另一方面，在由管理者赋予的场合，预先登录在策略表 1400 中。

排他控制 209，是在使用者使用设备时表示是否禁止别的使用者使用的定义信息。在排他控制 209 是“必须”的场合，对于设备的使用执行排他控制，从设备的使用开始到使用者结束使用，该设备禁止由别的使用者访问。在排他控制 209 为“可能”的场合，仅在正向设备进行收发信息期间该设备禁止由别的使用者使用。在排他控制 209 为“不要”的场合，不执行排他控制。本信息从策略表 1400 中抽出登录。

状态 210 是表示设备的使用情况的信息。本信息，由认证管理服务器 101 每隔规定时间对各连接客户机装置进行轮询取得。在状态 210 为“占用中”的场合，表示使用者一边执行排他处理、一边使用该设备的状态。在状态 210 为“使用中”的场合，表示使用者不执行排他处理、而使用该设备的状态。在状态 210 为“通信中”的场合，表示使用者仅在进行通信期间使用排他控制、通信一结束就迅速解除占用状态的情况。在状态 210 为“不明”的场合，例如，表示没有对认证管理服务器 101 的通知，设备管理管理程序 123 成为不能通信的状态。在状态 210 为“不明”状态的场合，经过一定时间后，认证管理服务器 101 进行控制，以使相应的设备管理管理程序 123 停止和安装该设备管理管理程序 123 的 PC—D113 上连接的设备 A151 停止。在状态 210 为“切断”的场合，表示虚拟设备管理程序 120 能和设备管理管理程序 123 进行通信、但是设备管理管理程序 123 不能和该设备 A151 的之间的通信的状态。另外，在状态 210 为“未使用”的场合，表示哪个客户机都未使用的状态。

可使用 ID211，记录许可对该设备连接的使用者或者组的 ID。本信息从策略表 1400 中抽出。在许可多个使用者或组对该设备连接的场合，登录全部许可的使用者或组的 ID。可使用 ID211，也可以是未定义、即未登录任何 ID

的状态。在未定义的场合，任何使用者或组都许可连接。

使用用户 ID212，记录现在正在使用该设备的使用者的 ID。本信息由认证管理服务器 101 每隔规定时间对各连接设备进行轮询取得。

下面说明认证管理服务器 101 保存的使用者信息数据库 300。本数据库 300，用于在使用者从在网络 103 上连接的、信息中心 102 以外的设备请求向信息中心 102 内的设备连接的场合，判定（认证）请求连接的使用者是否持有可许可的使用者权限。本数据库预先由管理者登录。

图 4 是认证管理服务器 101 保存的使用者信息数据库 300 的一例。如本图所示，在使用者信息数据库 300 中，对于每一用户登录使用者 ID301、使用者姓名 302、所属组 303、证书 304、有效期间 305、证书认证许可 306、Hash 加密方式 307、口令 308、可否口令认证 309 各项目。

使用者 ID301 是用于识别使用者的 ID，预先赋予每一使用者。如使用者的使用权利不变，则一般不变。使用者姓名 302 是表示使用者的名称的字符串。使用者姓名 302，在显示使用信息时使用。所属组 303 是表示使用者所属的组的信息。在本实施形态中，各种使用权限以组单位分配。所属组 303 表示相应于给予各使用者的权限的组。一个使用者可以属于多个组，即在所属组 303 中可以登录多个组。另外，所属组 303 也可以未定义。在未定义的场合，对于该使用者不给予任何使用权限。

证书 304，是指定在使用者认证中使用的公开密钥证书的信息。作为证书 304 记录的公开密钥证书，需要在认证管理服务器中能够验证其有效性。例如也可以构成为在认证管理服务器 101 中持有认证局，该认证局进行发行。

有效期间 305，是使用者持有使用刀片服务器 106 内的 PC 或设备的权利的期间。在有效期间 305 未定义的场合，使用者没有使用 PC 的权利。有效期间除使用年、月、日等的期间的设定外，也可以设定每周星期一、每日从 8 时 45 分到 17 时 15 分这样的期间。有效期间 305 可以和在证书 304 中表示的公开密钥证书的有效期限独立设定。

证书认证许可 306，是表示可否认可证书认证的信息。Hash 加密方式 307，记载使用认可的公开密钥基础设施进行认证的场合的 Hash 加密的方式。在 Hash 加密方式 307 未定义的场合，对于由认证管理服务器 101 进行的 Hash

加密方式无限制。即使在这一场合，在未在客户机（使用者使用的 PC 等）安装的方式也不能进行认证。口令 308，是在使用口令进行认证的场合的口令。作为口令 308 登录 Hash 值或者执行加密等时的信息。可否口令认证 309，是表示可否使用口令进行认证的信息。

刀片服务器 106 在认证管理服务器 101 中确认认证信息后得到认证，这是经历使用基于使用者信息数据库 300 的口令或公开密钥基础设施的认证后，使用者取得可以使用刀片服务器 106 内的 PC 的权限的情况。

在本实施形态中，认证用两阶段进行，1) 来访问的使用者是否有对刀片服务器 106 的访问权限，2) 在分配刀片服务器 106 内的 PC—A110 后，是否是具有使用该 PC—A110 的资源（程序或虚拟设备）的权限的人。在哪一场合使用者都向刀片服务器 106 或者 PC—A110 发送至少包含使用者认证用信息的认证请求，接收认证请求的刀片服务器 106 或者 PC—A110，访问认证管理服务器 101，核对在使用者信息数据库 300 中登录的记录，进行认证。这里，所谓使用者认证信息，指使用者 ID 以及口令，或者对应在每一使用者中登录的公开密钥信息的署名。

下面说明在信息中心 102 内的各 PC 的使用状况的管理中使用的 PC 使用管理表 400。图 5 是刀片服务器 106 保存的 PC 使用管理表 400 的一例。

在 PC 使用管理表 400 中，对于信息中心 102 内的各 PC 的每一个，登录 PC 名 401、网络名 402、IP 地址 403、MAC 地址 404、使用源终端 405、使用源网络名 406、使用源 IP 地址 407、使用源 MAC 地址 408、使用者 ID409、状态 410、连接开始时刻 411、连接结束时刻 412、动作确认时刻 413。

PC 名 401，是识别信息中心 102 内的 PC 的 PC 的名称。其由管理者无重复地预先确定登录。网络名 402 是在网络上识别 PC 时使用的名称。其由管理者无重复地预先确定登录。对于各 PC，对于网络名 402 和 PC 名 401 可以赋予相同的名称，也可以赋予不同的名称。

IP 地址 403 是赋予各 PC 的 IP 地址。MAC 地址 404 是在各 PC 上的网络接口中唯一确定的地址。

使用源终端 405 是在现时刻远距离操作信息中心 102 内的 PC 的客户机装置的名称，该名称也由管理者无重复地预先确定登录。管理者可以自由地

设定、变更名称。在不通过客户机装置使用该信息中心 102 内的 PC 的场合，使用源终端 405 成为未定义。使用源网络名 406 是在网络 103 上识别使用源时使用的名称。由管理者无重复地预先确定登录。此外，使用源终端 405 以及使用源网络名也可以是相同的名称。

使用源 IP 地址 407 是客户机装置的 IP 地址。使用源 MAC 地址 408 是在客户机装置的网络接口中唯一确定的地址。

使用者 ID409，是使用客户机装置的使用者的使用者 ID。在不使用客户机装置的场合，使用者 ID409 成为未定义。

状态 410 是表示该 PC 是否运行的信息。在状态 410 中记录的信息中，有“运行中”、“确认中”、“待机中”3 种。状态 410 是“运行中”的 PC，表示正由具有在使用者 ID409 中登录的 ID 的使用者通过在使用源终端 405 中指定的客户机装置使用。状态 410 是“确认中”的场合，表示在认证管理服务器 101 中正进行客户机装置是否正使用 PC 的确认的状态，或者确认未结束的状态。状态 410 是“待机中”的 PC，表示客户机装置等待使用 PC 的状态，亦即客户机装置是未使用 PC 的状态。

连接开始时刻 411，表示由使用者 ID409 指定的使用者通过由使用源终端 405 指定的客户机装置开始 PC 的操作的时刻。连接结束时刻 412 表示结束由使用者 ID409 指定的使用者通过由使用源终端 405 指定的客户机装置执行的 PC 的操作的时刻。动作确认时刻 413，表示由虚拟设备管理程序 120 对认证管理服务器 101 在发生了信道的生成、拆除等时执行的通信的最终时刻。

刀片服务器 106，每当构成的各 PC 的使用状况有变更时更新本数据库。

下面，就其在本实施形态的设备管理系统中设定设备为可共享的状态、在设定后进行共享设备的处理（以后称设备共享处理）进行说明。这里，以使用者使用客户机装置是 PC—D113、远距离操作信息中心 102 内构成刀片服务器 106 的设备中的 PC—A110、可共享在 PC—D113 上正连接的设备 A151 的场合为例加以说明。不用说，即使是其他使用者终端、构成其他刀片服务器 106 的机器、其他设备，设备共享处理的步骤也都相同。

图 6 是上述例子中的设备共享处理的处理流程。

使用者给 PC—D113 进行起动指示（501）。接收来自使用者的起动指示

的 PC—D113 从存储设备 163 加载 OS 或应用并起动（502）。这里，OS 或应用，也可以从网络上存在的存储设备加载。此时，设备管理管理程序 123 也被起动。

在步骤 502 起动的设备管理管理程序 123，取得在 PC—D113 上连接的设备 A151 的信息（503）。连接的设备的信息的取得，通过在起动时对应来自主机（在本实施形态中是 PC—D113）侧的请求从设备侧向主机发送作为关于设备全体的信息的数据的说明符的信息来执行（504）。在说明符中，例如包含表示设备的类别的代码、设备的大类的代码、该设备的制造销售商的 ID、产品 ID、序列号等。在 PC—D113 中根据在步骤 503 取得的信息数据读入驱动设备 A151 的设备驱动程序，进行动作。设备管理管理程序 123，通过实现管理的设备（这里是设备 A151）的驱动程序或者过滤驱动程序的功能，把本设备置成在本系统内可共享的状态，控制向该设备收发的信息。

设备管理管理程序 123，在确认在 PC—D113 上连接的设备 A151 的动作后，和设备连接请求一起向认证管理服务器 101 发送从在步骤 503 取得的设备 A151 的设备的信息中抽出的设备信息（504）。在认证管理服务器 101 中，接收设备连接请求以及设备信息后，与策略表 1400 内的数据对照，在设备信息管理表 200 中登录关于有设备连接请求的设备的策略。

另一方面，PC—D113 的起动结束后，PC—D113 在显示器上显示起动结束的旨意（506）。使用者确认起动结束后，指示开始构成信息中心 102 内的刀片服务器 106 的 PC 的使用。在本实施形态中，使用开始的指示是使用者的 ID 以及口令的输入。

PC—D113，从使用者接收开始使用的指示后（507），作为使用刀片服务器 106 的请求（以后称服务器使用开始请求），向刀片服务器 106 发送接收的使用者认证用信息（508）。

刀片服务器 106，在接收服务器使用开始请求后，执行使用者是否具有适当使用刀片服务器 106 的权限的认证（509）。具体说，刀片服务器 106，向认证管理服务器 101 发送在使用开始请求中包含的使用者 ID 以及口令，委托认证（510）。在认证管理服务器 101 中，把接收到的使用者认证用信息与使用者信息数据库进行核对，进行认证，向刀片服务器 106 返回结果。这里，

认证使用者是否对刀片服务器 106 具有访问权限。

刀片服务器 106，在接收从认证管理服务器 101 返回认证成功的信息的场合，刀片服务器 106，判定为来访的使用者许可使用刀片服务器 106，从构成刀片服务器 106 的 PC 中决定该使用者要使用的 PC。PC，是对应使用顺序被适当分配，还是预先给使用者一对一分配，抑或对应给使用者分配的某种权限进行分配，任何一种形态均可。取何种形态由管理者决定。这里，对刀片服务器 106 给来访问的使用者分配 PC—A110 的情况进行说明。在分配其他 PC 的场合，处理也相同。

刀片服务器 106，在决定分配给 PC—D113 的 PC 为 PC—A110 后，执行 PC—A110 的起动状况的确认（511）。在未起动 PC—A110 的场合，向 PC—A110 发送起动 PC—A110 的请求（512）。遵照发送的请求 PC—A110 起动后（513），PC—A110 向刀片服务器 106 通知表示起动结束的信息。此外，在 PC—A110 已经起动的场合，例如 PC—A110 是具有服务器功能、多人可同时使用的环境且总是通电的场合等，不需要来自步骤 512 的 PC 的起动操作。

此外，PC 的运行状况，通过访问 PC 使用管理表 400、确认相应的 PC 名 401 的状态 410 来进行。起动后，把分配的客户机装置作为相应的 PC 名 401 的使用源终端 405 追记。

另一方面， PC—A110 一起动，在 PC—A110 内的安装的虚拟设备管理程序 120 就确认可使用的设备（515）。具体说，虚拟设备管理程序 120，向认证管理服务器 101 发送虚拟设备管理程序 120 运行的 PC（这里是 PC—A110）可使用的设备的调查的请求（以下称可使用设备调查请求）（516）。

接收可使用设备调查请求的认证管理服务器 101，执行设备的调查和确认（517）。具体说，接收可使用设备调查请求的认证管理服务器 101，首先，确认是否新登录了新的设备，并执行已经保存的设备信息表 200 的更新（518）。认证管理服务器 101，接收可使用设备调查请求，对于在此刻在设备信息表 200 中登录的各设备，向在该设备上连接的各 PC 或者集线器等的客户机装置的设备管理管理程序，进行已登录的设备是否依然可以使用的询问（519）。

从认证管理服务器 101 接收到的询问的各客户机装置的设备管理管理程

序，向认证管理服务器 101 返回接收到现时刻的询问的设备的可否使用（520）。此外，各设备管理管理程序，作为表示可否使用的信息，在该设备已经被切断的场合，返回被切断的信息；在正连接的场合，返回各设备的“占用中”、“使用中”、“通信中”这样的现在的状态。认证管理服务器 101 使用从各设备管理管理程序接收的信息，更新设备信息表 200。在接收被切断的信息的场合，删除关于该设备的记录。

然后，认证管理服务器 101，把在设备信息表 200 中登录的设备作为现时刻可使用的设备，向发出询问的虚拟设备管理程序 120 发送（521）。

接着，虚拟设备管理程序 120，根据设备信息表 200 的信息，执行共享设备的处理。在现时刻，虚拟设备管理程序 120，因为是未进行使用者的认证的状态，所以在进行可使用的设备的检查时在信息表中对于有可使用 ID 的限制的设备，不能进行共享处理。因此，虚拟设备管理程序 120，抽出在设备信息表 200 中登录的设备且可使用 ID211 是未定义的设备，在和这些可使用的设备之间，进行生成信道等的通信准备（522，523）。

此外，也可以构成为：认证管理服务器 101，在从虚拟设备管理程序 120 接收可使用设备调查请求的场合（516），不执行对各设备管理管理程序 123 的询问，抽出在该时刻在设备信息表 200 中登录的设备且可使用 ID211 是未定义的设备，向发出询问的虚拟设备管理程序 120 返回（521）。在这一场合，不执行步骤 517～520 的处理。

此外，信道的生成，通过虚拟设备管理程序 120，在和连接在步骤 521 作为可使用设备接收的各设备的客户机装置装备的设备管理管理程序之间，根据相互的 IP 地址和由认证管理服务器 101 给的信息，进行相互认证、密钥交换，形成加密通信路径来进行（523）。

作为相互认证的方法的一例，可以举出：认证管理服务器 101，对于设备管理管理程序 123 在设备信息收发时，另外对于虚拟设备管理程序 120 返回使用设备时，分别安全地发送预共享密钥（事前共享密钥），以该事前共享密钥为基础进行认证的方式。不过相互认证的方式不特别限定本方法，只要执行信道的生成的对手能够确认是特定的设备管理管理程序和虚拟设备管理程序即可。

相互认证结束后，在虚拟设备管理程序 120 和设备管理管理程序之间，交换用于交换 ID 信息以及数据的加密用的密钥。以后，使用在这里交换的加密用的密钥，设备管理管理程序和虚拟设备管理程序 120 进行通信。因此，对于第三者就不可能窃听交换 ID 信息以及数据的通信。该加密用的密钥，可以是固定值，也可以是每使用一次或者按一定期间舍弃，并生成新的加密用的密钥。

在本实施形态中，在这样在虚拟设备管理程序 120 和设备管理管理程序 123 之间生成信道的场合，该设备管理管理程序 123 管理的设备就成为了可共享的状态。通过这样的第三者不能窃听的通信路径（信道），PC—A110，和在 PC—A110 上直接连接设备 A151 的场合相同，能够控制设备 A151。

即，在本实施形态中，所谓“设备的共享”，是 PC—A110 能够和在其上直接连接设备 A151 的场合相同地 PC—A110 进行处理那样进行动作。例如，在对于在 PC—D113 上连接的设备 A151 实现了“设备的共享”的场合，从设备 A151 通过设备管理管理程序 123、虚拟设备管理程序 120，PC—A110 能够读出或者重设在设备 A151 内设定的通信方式或者说明符。

此外，在 PC—A110 中，在过去未使用设备 A151 的场合，安装必要的设备驱动程序。一般，在进行设备的共享时，PC—A110 上运行的操作系统自动识别新追加的设备，执行对该设备的运行必要的设备驱动程序的安装作业。这样的安装作业，在 PC—A110 上最初使用的设备在 PC—A110 和其他机器之间被共享时发生，如是在过去使用的设备，则因为在 PC—A110 上已经安装有必要的驱动程序，所以不发生。

此外，在 PC—A110 上运行的操作系统不具有如上述自动识别设备、执行必要的设备驱动程序的安装的功能的场合，管理者或者使用者手工进行设备驱动程序的安装，变更 PC—A110 的设定，使设备变得可以使用。

另外，在多个使用者共享设备 A151 的场合，有时各使用者分别独立地指示复位或者进行通信。在这样的场合，设备管理管理程序 123，构成为或变更为不接收复位那样的步骤，或代之为发送已由设备 A151 取得的、在设备管理管理程序 123 内保存的信息。具体说，对于来自虚拟设备管理程序 120 的特定的通信，进行预定的应答。

此外，把这里生成的信道的信息，向认证管理服务器 101 发送（591），在认证管理服务器 101 中，使用接收的信息，更新设备信息表 200（592）。

通过以上的处理，PC—A110 就可由 PC—D113 的使用者使用。

接着，使用者通过 PC—D113 请求使用 PC—A110。即 PC—D113 在从使用者接收使用 PC—A110 的指示后，PC—D113 生成使用 PC 的请求（以后称 PC 使用请求），将其向 PC—A110 发送（524）。在该 PC 使用请求中，包含指定使用者的信息，例如使用者 ID、口令等。

PC—A110，接收 PC 使用者请求，进行登录处理（525）。登录处理，首先，PC—A110 向认证管理服务器 101 发送指定在使用者请求中包含的使用者的信息。认证管理服务器 101，对比接收的指定使用者的信息和在使用者信息数据库 300 中存储的信息，执行使用者的认证，向 PC—A110 返回结果。此外，也可以构成为：预先在使用者信息数据库 300 中的项目中，PC—A110 也只保存登录时的使用者认证所必要的项目，在 PC—A110 上进行登录时的认证。

接着，虚拟设备管理程序 120 进行可使用设备的检查。这里，虚拟设备管理程序 120，抽出对于登录的使用者的可使用设备。抽出可使用设备的步骤，基本和在上述 516 中说明的相同。在询问时也可以将登录的使用者的 ID 向认证管理服务器 101 发送，仅接收把该使用者的 ID 作为可使用 ID 登录的使用者 ID 的返回信息。

认证管理服务器 101 和上述处理相同，对于在设备信息表 200 中登录的全体设备，向连接该设备的客户机装置的设备管理管理程序询问最新的信息，接收返回信息、更新设备信息表 200 后，向发出询问的虚拟设备管理程序 120 返回（529～532）。此外，和上述同样，认证管理服务器 101 也可以构成为：对应可使用设备调查请求，参照设备信息表 200，向发出询问的虚拟设备管理程序 120 返回现时作为该使用者可使用的设备登录的设备（532）。

在初次进行可使用设备的检查时（516～523），因为未指定使用者，所以对于可使用 ID 被限定的设备，不能设定共享处理即通信路径。但是，在使用者登录（525）后，在可使用 ID 中存在使用者的 ID 或者使用者所属组的 ID 的设备就变得可以使用。因此，在该时刻在与新成为可使用的设备之间，和

上述相同，开设通信路径（信道）（533～534）。

此外，也可以构成为：在和可使用设备的通信准备（533）的阶段，在PC—A110 的画面上、在 PC—D113 或者信息中心 102 内的管理者能够确认的画面上，显示可使用设备的一览表。在这种场合，在这些画面上，就显示现在正被共享的设备和可连接的设备等的列表。虚拟设备管理程序 120 保存的在前次结束时刻在设备共享列表中存在的、现在可使用的设备可以没有使用者的指示来进行信道的生成，即可以进行设备的共享。可以构成为：能够通过管理者或者使用者设定是否没有使用者的指示来进行关于可执行设备共享的设备的共享设定。

生成的信道信息，向认证管理服务器 101 发送（593）。在认证管理服务器 101 中，根据接收的信道的信息更新设备信息表 200（594）。其后，开始使用 PC—A110（535）。

这里，可使用设备的检查、可使用设备调查请求、设备的调查和确认、设备使用可否询问、设备信息取得、设备信息发送可使用设备返回（526～534）、信道生成信息的发送 593、以及表的更新 594，在 PC 的使用（535）的中间被适当重复执行，认证管理服务器 101 拥有的设备信息表总是不断更新为最新的状态。

这里，希望定期执行使用者登录后的由虚拟设备管理程序 120 进行的可使用设备的检查。虚拟设备管理程序 120，定期确认设备信息表 200，确认由于状态的变更引起的可否共享的变化。

另一方面，设备信息表 200，通过设备管理管理程序 123，每当发生设备的连接状况的变化、状态的变化等关于设备的状态的变化时，向认证管理服务器 101 通知，连同表示变化后的信息一起更新。

经过以上的处理，通过设备管理管理程序 123 和虚拟设备管理程序 120 动作、进行通信，设备 A151，就能够作为 PC—A110 的设备动作。即对于设备 A151 实现设备的共享。

下面说明本实施形态的设备管理系统中的设备共享结束时的处理。图 7 是本实施形态的设备共享处理结束时的处理流程。

如本图所示，使用者使用 PC—D113 远距离操作 PC—A110，结束设备

A151 的使用后，对其他使用者释放设备 A151。

使用者，对 PC—D113 进行设备使用结束指示（601）。PC—D113，在接收使用者发出的设备使用结束的指示后，向虚拟设备管理程序 120 发送设备使用结束的请求（以下称设备使用结束请求）（602）。虚拟设备管理程序 120，接收设备使用结束请求后，执行使用结束设备的检查（603）。具体说，虚拟设备管理程序 120 判断在 PC—A110 上是否可以结束设备的使用。

例如，在 PC—A110 上的应用或者其他的客户机装置正在使用设备使用结束请求的对象设备的场合，不能终止使用。在这一场合，在这些应用或者其他的客户机装置结束设备使用结束请求的对象设备的使用前等待结束处理。在这一场合，向 PC—D113 通知不能结束指示的设备的旨意。PC—D113 通过显示向使用者通知接收到的通知。

此外，该通知不一定进行，例如也可以构成为仅在待机规定时间以上后还不能执行结束使用的场合进行通知。当然，在使用结束设备的检查（603）中，在可结束使用的场合，连同指定设备的信息向认证管理服务器 101 执行作为结束该设备使用的意思的通知的使用结束设备的信息发送（604）。

接着，认证管理服务器 101，接收使用结束设备发送信息，进行设备的调查和确认（605）。具体说，向发出设备使用结束请求的设备管理管理程序 123、执行作为表示指示的设备的使用结束了的信息的设备释放信息发送（606）。

设备管理管理程序 123，执行设备的调查和确认（607）。这里，进行调查有无从设备来的应答等的调查。如果没有应答，把设备信息表 200 的该设备的状态置为“不用”。

另一方面，在从设备得到通常的应答的场合，设备管理管理程序 123 废弃在和虚拟设备管理程序 120 之间确立的信道（608）。在信道废弃成功的场合，向认证管理服务器 101 发送为表示已结束信道废弃的信息的信道废弃信息（609）。

认证管理服务器 101，接收信道废弃信息，进行设备信息表 200 的更新（610）。亦即，在该时刻，认证管理服务器 101，对于信道被废弃的设备，变更设备信息表 200 的状态 210，例如从“占用中”、“使用中”、“通信中”

变更为“未使用”。

认证管理服务器101、设备管理管理程序123以及虚拟设备管理程序120，使用图6以及图7说明的一系列动作中发送的或者接收的数据，分别作为日志191、173、170，在存储设备190、163、160中记录。

下面说明在图6的处理结束而变成在设备A151成为可共享、能作为PC—A110的设备动作后的、设备管理管理程序123和虚拟设备管理程序120之间的数据的收发控制的细节。

图8是用于说明设备管理管理程序123以及虚拟设备管理程序120、和PC—A110以及PC—D113的设备驱动程序以及应用的关系（软件堆栈）的图。

在从在PC—D113上运行的应用1211操作在PC—D113上连接的设备A151、进行命令收发的场合，通常，需要通过设备驱动程序接口1212，经由多个驱动程序1213～1215。这里驱动程序1213、驱动程序1214，是在驱动程序1215上连接的连接接口的驱动程序等，驱动程序1213是最上位的驱动程序，驱动程序1214、驱动程序1215顺次成为下位的设备单位的驱动程序。

设备管理管理程序123，具有过滤驱动程序1210。过滤驱动程序1210作为驱动程序1213～1215的上位过滤驱动程序（上过滤驱动程序）或者下位滤波器驱动程序（下过滤驱动程序）动作，在图示箭头的路径上使用驱动程序1213～1215进行和设备A151的数据的收发。亦即，过滤驱动程序1210通过设备A151和驱动程序1215以及驱动程序1214进行数据的收发。

此外，过滤驱动程序1210作为过滤驱动程序记载，但是也可以具有驱动程序1213～1215的功能的一部分或者全部，在这种场合作为一种设备驱动程序动作。

设备管理管理程序123和虚拟设备管理程序120，在设备管理管理程序123装备的通信模块1209和虚拟设备管理程序120装备的通信模块1206之间，经由网络103进行数据的收发，这样来进行通信。

虚拟设备管理程序120具有设备驱动程序1205，设备驱动程序1205执行在PC—A110内运行的应用1200等和设备A151之间进行数据收发时的信息的交换。

在应用1200和设备驱动程序1205之间的数据的收发，如图示箭头那样

可以由应用 1200 直接进行，或者通过设备驱动程序接口 1201 进行，抑或通过驱动程序 1202～1204 进行。

GUI1207 以及 1208，分别是虚拟设备管理程序 120 以及设备管理管理程序 123 的图形用户接口，起向用户提供信息或者接收从用户输入的信息的作用。

如上所述，虚拟设备管理程序 120，成为从 PC—A110 内的应用进行对在本实施形态的设备管理系统内存在的设备的数据的收发的入口。虚拟设备管理程序 120，在内部具有设备驱动程序 1205 和通信模块 1206，具有通过网络 103 和设备管理管理程序 123 以及认证管理服务器 101 进行通信的功能。

另外，设备管理管理程序 123，成为从在 PC—D113 上连接的设备 A151 与在本实施形态的设备管理系统内存在的 PC 等进行数据的收发的入口。设备管理管理程序 123，在内部具有过滤驱动程序 1210 和通信模块 1209，具有通过网络 103 和虚拟设备管理程序 120 以及认证管理服务器 101 进行通信的功能。

下面说明图 6 所示的信道的生成（523 以及 534）结束、虚拟设备管理程序 120 变得能够控制设备 A151 后，对于虚拟设备管理程序 120 给出使用设备 A151 的命令时的动作。图 9 是说明在本实施形态的设备管理系统中设备使用时的、设备管理管理程序 123 以及虚拟设备管理程序 120 的动作的流程。这里，对于从虚拟设备管理程序 120 侧进行触发的场合的处理进行说明。

在图 6 所示的信道的生成（523 以及 534）结束、虚拟设备管理程序 120 变得能够控制设备 A151 后，如果给虚拟设备管理程序 120 提供使用设备 A151 的命令（开始 700），则虚拟设备管理程序 120，确认设备 A151 是否在运行（701）。具体说，虚拟设备管理程序 120 向设备管理管理程序 123 发送规定的命令，询问可否取得设备 A151 的状态，是否是可通信的状态。或者确认是否是已确保通信路径的状态。然后，根据从设备管理管理程序 123 返回的信息内容进行判断。

在未运行的场合，向认证管理服务器 101 通知设备 A151 处于不正确的状态，认证管理服务器 101 以及虚拟设备管理程序 120 各自在日志 191、170 中记载（702）。虚拟设备管理程序 120，在结束向日志 170 的记载后，非正

常结束对于给予的命令的处理（716）。此时虚拟设备管理程序 120 也可以向使用者通知表示不正确结束的错误消息。进而，也可以构成为在接收到处于不正确状态的通知时自动进行和设备 A151 的通信的结束处理。另外，也可以构成为多次执行动作确认，在即使多次执行后仍继续通知不正确状态的场合，前进到 702。

另一方面，在步骤 701 确认设备 A151 运行的场合，虚拟设备管理程序 120 根据需要向认证管理服务器 101 以及设备管理管理程序 123 执行用于生存确认的通知（703）。通过本处理，认证管理服务器 101 以及设备管理管理程序 123 就能够确认和设备 A151 的信道已经建立了。

接着，虚拟设备管理程序 120 判别是否收到成为使用设备 A151 的触发的指示（例如从 PC—A110）。在判定为没有触发的指示的场合，返回步骤 701。

另一方面，在判定为有触发的指示的场合，在虚拟设备管理程序 120 中，生成遵照设备接口协议的事务（705）。然后，生成的事务被变换为网络协议中规定的协议，向设备管理管理程序 123 发送（706）。

接着，虚拟设备管理程序 120，判断事务（数据）是否正确到达设备管理管理程序 123，在未正确到达的场合判断其次数是否未超过预先指定的次数。

具体说，首先，虚拟设备管理程序 120，判别数据未正确到达设备管理管理程序 123 的次数是否达到指定次数（707）。

在达到指定次数的场合，虚拟设备管理程序 120，判断为通信处于不正确的状态，将此向认证管理服务器 101 通知，同时在日志 170 中记载。也可以构成为在认证管理服务器 101 的日志 191 中也记录通信处于不正确的状态的信息。虚拟设备管理程序 120，在向日志 170 的记载结束后，非正常结束（709）。虚拟设备管理程序 120 可以将错误通知使用者，也可以自动进入和设备 A151 的通信的结束处理。

另一方面，在步骤 707 中在次数未达到指定次数的场合，虚拟设备管理程序 120 执行数据是否正确到达设备管理管理程序 123 的检查（710）。具体说，在根据对于发送的数据的响应，判断为不正确的场合，或者，在到规定的时刻没有响应的场合，判断为未正确到达。然后，在判断为未正确到达的

场合，未正确到达次数加 1，返回步骤 707。

在步骤 710 中在数据正确到达的场合，虚拟设备管理程序 120，确认是否有未发送的事务（711）。然后，在存在未发送的事务的场合，返回步骤 706 ，重复处理。

在没有未发送的事务的场合，虚拟设备管理程序 120，进行是否有应该接收的事务的检查（712）。这点通过在设定两者间的通信线路时预先确定的数据量的数据的发送是否结束来判断。

在有应该接收的事务的场合，虚拟设备管理程序 120，把接收的数据变换为设备接口协议（713）。接着向设备驱动程序发送抽出的数据（714），返回步骤 712。

另一方面，在步骤 712 中在没有应该接收的事务的场合，虚拟设备管理程序 120 结束处理（715）。

此外，在上述处理中，在处理不正确终止的场合（步骤 716，709），认证管理服务器 101、设备管理管理程序 123 以及虚拟设备管理程序 120，在处理不正确终止的时刻，适当再确认可使用的设备，更新认证管理服务器 101 内的信息管理表 200。即虚拟设备管理程序 120 如能再确认设备的话，则再次进行正常的通信。如可能生成信道的话则生成，把设备信息表 200 的状态置为“占用中”、“通信中”、“使用中”。

下面说明在图 6 所示的信道的生成（523 以及 534）结束、设备管理管理程序 123 变得能够控制设备 A151 后，设备 A151 对于设备管理管理程序 123 发送信息的场合的动作。图 10 是说明在本实施形态的设备管理系统中设备使用时的、设备管理管理程序 123 以及虚拟设备管理程序 120 的动作的流程。这里，对于从设备 A151 侧进行触发的场合的处理进行说明。

在图 6 所示的信道的生成（523 以及 534）结束、设备管理管理程序 123 变得能够控制设备 A151 后，设备 A151 向设备管理管理程序 123 发送信息后（开始 800），设备管理管理程序 123 确认设备 A151 是否运行（801）。运行确认，同图 9 的处理。

在不运行的场合，向认证管理服务器 101 通知设备 A151 处于不正确状态，认证服务器 101 以及设备管理管理程序 123 各自在日志 191、173 中记载

（802）。设备管理管理程序 123，在结束向日志 173 的记载后，进行不正确终止（816）。此时，设备管理管理程序 123 也可以向使用者通知表示不正确终止的错误消息。再有，也可以构成为在接收处于不正确状态的通知时，自动执行和设备 A151 的通信的结束处理。另外，也可以构成为多次执行运行确认，在即使多次执行仍继续通知不正确状态的场合前进到 802。

另一方面，在步骤 801 中在确认设备 A151 运行的场合，设备管理管理程序 123 根据需要向认证管理服务器 101 以及虚拟设备管理程序 120 进行为生存确认的通知（803）。通过本处理，认证管理服务器 101 以及虚拟设备管理程序 120 就能够确认和设备 A151 的信道已经建立。

接着，设备管理管理程序 123，判别是否接收到成为使用设备 A151 的触发的指示（例如来自 PC—A100）（804）。在判定为没有成为触发的指示的场合，返回到步骤 801。

另一方面，在判定为有成为触发的指示的场合，在设备管理管理程序 123 中，生成遵照设备接口协议的事务（805）。然后，生成的事务变换为用网络协议定义的包，向虚拟设备管理程序 120 发送（806）。

接着，设备管理管理程序 123，判断事务（数据）是否正确到达虚拟设备管理程序 12，在未正确到达的场合，判断其次数是否未超过预先指定的次数。

具体说，首先，设备管理管理程序 123 判别数据未正确到达虚拟设备管理程序 120 的次数是否达到预先指定的次数（807）。

在达到指定次数的场合，设备管理管理程序 123，判断通信处于不正确状态，将此通知认证管理服务器 101，同时在日志 713 内记录。也可以构成为把通信处于不正确状态的信息也在认证管理服务器 101 的日志 191 中记录。设备管理管理程序 123，在向日志 173 的记载结束后，进行不正确结束（809）。设备管理管理程序 123，可以向使用者通知错误，也可以自动进入和设备 A151 的通信的结束处理。

另一方面，在步骤 807 中在次数未达到指定次数的场合，设备管理管理程序 123 进行数据是否正确到达虚拟设备管理程序 120 的检查（810）。这里，在判断为未正确到达的场合，在未正确到达次数上加 1，返回步骤 807。

在步骤 810 在数据正确到达的场合，设备管理管理程序 123 执行是否还有未发送的事务的检查（811）。

然后，在还有未发送的事务的场合，返回步骤 806，重复处理。

在没有未发送的事务的场合，设备管理管理程序 123 进行是否有应该接收的事务的检查（812）。

在有应该接收的事务的场合，设备管理管理程序 123 把接收的数据变换为设备接口协议（813）。然后向设备驱动程序发送抽出的数据（814），返回步骤 812。

另一方面，在步骤 812 在没有应该接收的事务的场合，设备管理管理程序 123 结束处理（815）。

此外，在上述处理中，在处理不正确结束的场合（步骤 816，809），认证管理服务器 101、设备管理管理程序 123 以及虚拟设备管理程序 120，在处理不正确结束的时刻，适当地进行可使用设备的再确认，更新认证管理服务器 101 内的设备信息管理表 200。亦即，设备管理管理程序 123，如设备能够再确认，则再次进行正常的通信，如可能生成信道则生成信道，把设备信息管理表 200 的状态置为“占用中”、“通信中”、“使用中”。

通过以上的动作，由认证管理服务器 101 以及虚拟设备管理程序 120 以及设备管理管理程序 123 积蓄的日志 191、170、173，由网络管理者通过在认证管理服务器 101 或者其他管理设备上安装的管理应用显示。

图 11 表示通过管理应用显示的日志管理画面的一例。本图所示的管理日志，是认证管理服务器 101 收集认证管理服务器 101、虚拟设备管理程序 120 以及设备管理管理程序 123 内保存的日志 191、170、173，显示在自身的存储设备 190 或者存储器中积蓄的内容的日志。

用于该显示的应用（管理应用），也可以位于认证管理服务器 101 以外。在这种场合，接收来自认证管理服务器 101 的许诺进行显示。在存在多个信息中心 102 以及刀片服务器 106 的结构中，管理应用也可以从认证管理服务器 101 以外的认证管理服务器及其管理的应用收集日志，显示合并了收集的日志的内容。

设备管理画面 1000 是用于进行管理应用显示的设备的管理的画面。在设

备管理画面 1000 中，显示积蓄的各日志 191、170、173 的号码 1001、时刻 1002、设备 ID1003、设备名 1004、地址（源）1005、网络接口 ID（源）1006、应用 ID1007、地址（主机）1008、网络接口 ID（主机）1009、应用 ID1010、销售商 ID1011、产品 ID1012、序号 1013、设备名 1014、使用用户 ID1015、信息 1016、备注 1017 各项。

号码 1001 是用于管理日志的号码，每次积蓄日志时自动赋予。时刻 1002 是记录日志的日期时间。信息 1016 详细表示在日志 170、173、191 中作为日志记录的事件的内容。

地址（源）1005、地址（主机）1008 表示源以及主机（目的地）的地址。网络接口 ID（源）1006 以及网络接口 ID（主机）1009 表示源以及主机（目的地）的网络接口 ID。在备注 1017 内显示未在信息 1016 中显示的信息，例如提醒管理者注意的信息、补充信息 1016 的信息。

其他项目与使用图 2～4 说明的信息表 200、使用者信息数据库 300、PC 使用管理表 400 的同名的项目相同。

另外，认证管理服务器 101 装载具有检索在设备管理画面 1000 中显示的各信息的功能的管理应用。通过管理应用显示在设备管理画面 1000 中表示的信息，可以即时掌握哪个机器或设备处于何种状态，提高系统整体的方便性。例如，通过只检索在发生不正确认证场合的信息加以显示、监视，能够发现不正当的访问，采取对策。另外通过适当地只检索在不能使用设备的场合的信息加以显示、监视，可以早期发现系统内发生的故障，进行应对。再有，与由管理应用将日志整体做成一览表相比，使显示易于观看，这样可以减少管理者的操作失误。由此，可以得到提高系统整体安全性这样的效果。

下面说明虚拟设备管理程序 120 生成、显示的设备管理画面的细节。图 12 是虚拟设备管理程序 120 的设备管理画面的一例。

如本图所示，设备管理画面 900，具有：认证管理服务器显示部 901；连接 PC 集线器显示部 902、905、908、911；设备显示部 903、906、909、912；和连接切断指示部 904、907、910、913。

虚拟设备管理程序 120 一被起动，就向预先指定的认证管理服务器 101 发送请求，以便取得可使用的设备信息。

在认证管理服务器 101 中，在对使用者的认证成功后，从设备管理管理程序 123 向虚拟设备管理程序 120 发送设备管理信息。遵照接收的设备管理信息，虚拟设备管理程序 120 管理可使用的设备的信息等。

在图 12 中在认证管理服务器显示部 901 中，显示虚拟设备管理程序 120 正通信的认证管理服务器 101。在图 12 所示的例子中，显示虚拟设备管理程序在和认证管理服务器 101 通信成功的情况。这里，显示为 192.168.0.1 的是认证管理服务器 101 的地址。

在状态 920 中，表示认证管理服务器 101 的状态。这里，作为状态显示可使用的用户 ID 为何值，使用者名为何人等。在图 12 的例子中显示用户 A 被认证的情况。

在连接 PC 集线器显示部 902、905、908、911，显示正连接的 PC、集线器的信息。另外，使用者现在使用中的设备用不同颜色显示。

在设备显示部 903、906、909、912 中，显示设备的名称或状态、使用者 ID 等信息，使容易理解地显示使用者可使用哪个设备这样的信息。

在连接切断指示部 904、907、910、913 中，显示使用者能够给出指示的选择设备的使用或专用、停止使用、预定等的可供选择的选项。虚拟设备管理程序 120，通过接收预定按钮的按下，进行对现在他人正使用的设备的预定。然后，在该设备成为可使用的场合，向认证管理服务器 101 或者设备管理管理程序 123 进行已成为可使用的意思的通知。接收通知的设备管理管理程序 123 向使用者进行已成为可使用的意思的通知。在图 12 的例子中，使用者可使用的设备用影线表示，另外，使用者可执行的操作用粗体字按钮表示，并考虑到易于操作。

以上对于使用 PC—D113 使用刀片服务器 106 内的 PC—A110 的服务器客户机方式进行了说明。

和已经说明的例子同样，可以从在网络 103 以及因特网 104 上连接的客户机装置使用刀片服务器 106 内的任何一个 PC，还可以使用设备 A151～设备 Z155。

这里，集线器 116，不具有作为 PC 的功能，而是在内部具有管理管理程序 126 以及存储设备 176 的内置设备。在使用如 PC—E114 那样不连接设备

的 PC 的场合，和 PC—D113 同样，也能使用在其他 PC 等上连接的设备。另外，如集线器 116 那样连接多台设备时也同样。

再有，在使用经由因特网 104 以及防火墙 105 的 PC—Z117 来使用网络 103 上的 PC 或设备的场合也基本上是同样的。但是，在该场合，希望 PC—Z117 在内部具有加密因特网 104 上的通信的加密应用 190、加密后来进行通信。

如上所述，本实施形态所示的设备管理系统，关于被管理的设备、通过虚拟设备管理程序 120 和设备管理管理程序 123 和认证管理服务器 101、经由客户机装置管理在网络 103 上连接的设备，由此，就能够安全且对于使用者使用方便地实现系统内的设备的共享。

另外，根据本实施形态，即使是在其他客户机装置上连接的设备，也可能如同在服务器上直接连接的设备那样使用。亦即，即使是在其他客户机装置上连接有设备的场合，为使用该设备，也不需要在各客户机装置上有特别的结构。因此，不管是将设备虚拟连接在服务器上，还是将其直接连接在服务器上，都能够采用同样的结构，故此可以减低系统整体的制造成本。

另外，根据本实施形态，能够作成这样的设定，即通过认证管理服务器 101 管理许可、不许可的，而不许可的设备不能作为虚拟设备使用的设定。因此，能够对在网络 103 上连接的设备进行适当的管理，在服务器客户机系统中，能够提高在处于远地的服务器之间共享设备的场合的安全性。

再有，因为通过在使设备进入可共享的状态的步骤中进行认证，给使用者是否可使用设备赋予规则，提供在使用者在手头操作的 PC、瘦客户机等终端和位于远处的服务器之间共享设备的安全而且简便的手段，所以能够在提高使用系统时的安全性的同时，提高使用者的便利性。

在本实施形态中，如上所述，是具有主要在服务器侧存储程序或数据，而客户机侧主要对服务器给出操作指示的结构的服务器客户机系统。因此，能够提供保留有减少在操作侧的客户机装置内遗留的机密信息的特征、而且提高客户机使用时的安全性及方便性的信息处理系统。

此外，在上述实施形态中，把服务器或相当于客户机的信息设备都作为 PC 进行了说明，但是一方或者双方也可以是服务器、Personal Digital Assistants

(PDA)、工作站、高功能复印机、现金自动提款机（ATM）、便携电话、数字静物照相机、音乐重放(录音)装置、销售时商品管理系统、街头终端、Intelligent Transport Systems (ITS) 用发送机、售券机、结算终端、自动售货机、房间进出管理装置、游戏机、公用电话、征求订货用便携终端等。在这些场合也能得到同样的效果。

<<第二实施形态>>

下面说明使用本发明的第二实施形态。本实施形态基本上和上述第一实施形态相同。但是在第一实施形态中，设备通过 PC 或者集线器连接在网络 103 上，但是在本实施形态中，设备直接连接在网络 103 上。因此，本实施形态的设备在内部具有设备管理管理程序等。

图 13 是本实施形态的设备管理系统的详细的框图。在本图中，和图 1 所示的第一实施形态的同名的设备基本上具有同样的结构。在本实施形态中，还在网络 103 上连接设备 X1101。

设备 X1101，是 CD—ROM 等存储设备，或者键盘、显示器等人—机接口设备等外围设备。如本图所示，本实施形态的设备 X1101 在内部包括第一实施形态的集线器 116 的功能。亦即，设备 X1101，通过未图示的网络接口连接网络 103，具有硬盘驱动器或者闪存等存储设备 1166 以及未图示的存储器及 CPU，具有执行运算的集线器 1116。设备 X1101 在集线器 116 中实现设备管理管理程序 1126。另外，在存储设备 1166 中保存日志 1176。

因此，本实施形态的设备 X1101，和第一实施形态的各设备同样，使用者能够使用刀片服务器 106 内的 PC 等虚拟设备。进而，和第一实施形态的集线器 116 同样，通过设备管理管理程序 1126，能够在本设备管理系统内接受适当的管理。

亦即，本实施形态所示的设备管理系统，在第一实施形态所示的设备管理系统的特征之外，还具有能够把像设备 X1101 那样具有集线器 116 的功能的设备直接连接到网络 103 上的便利性。

通过该便利性，本实施形态所示的设备管理系统，在第一实施形态所示的设备管理系统的特征之外，使用者不限定连接设备的集线器或 PC，通过在网络 103 上插入设备 X1101，亦即通过把设备 X1101 直接连接到网络 103 具

有的接口上，就可以从网络上的 PC 使用设备 X。另外，不需要连接设备的集线器或 PC，因此，不仅维持高的安全性，同时还进一步提高使用者的便利性。从而降低构成系统的成本。

<<第三实施形态>>

下面说明使用本发明的第三实施形态。本实施形态基本上和上述第二实施形态相同。

图 14 是本实施形态的设备管理系统的详细的框图。如本图所示，本实施形态的设备管理系统，和第二实施形态的设备管理系统同样，具有设备 Y1201，该设备 Y1201 为 CD—ROM 等存储设备，或者键盘、显示器等人—机接口设备等外围设备，通过未图示的网络接口连接网络 103，具有硬盘驱动器或者闪存等存储设备 1166 以及未图示的存储器及 CPU，并具有执行运算的集线器 1116。

本实施形态的设备 Y1201，在集线器 1116 内部，还具有人体通信用认证装置 1206，在设备 Y1201 内的集线器 1116 的外部还具有人体通信用收发机 1203。

使用者，佩带未图示的人体通信用收发机，接触设备 Y1201 的人体通信用收发机 1203。认证信息，按照认证管理服务器 101、人体通信用认证装置 1206、人体通信用收发机 1203、使用者佩带的未图示的人体通信用收发机的顺序在这些设备间被收发，进行使用者的认证。

在本实施形态中，仅在认证成功的场合，设备 Y1201 才能够作为网络 103 上的 PC 使用。

如上所述，本实施形态所示的设备管理系统，一方面具有第二实施形态所示的设备管理系统的特征，同时进一步具有像设备 Y1201 那样能够在网络 103 上直接连接具有人体通信用认证装置以及人体通信用收发机的设备的便利性。

由于该便利性，本实施形态所示的设备管理系统，一方面具有第二实施形态所示的设备管理系统的特征，同时只接触使用者认证的设备便能够把设备作为在网络 103 上连接的 PC 的设备使用，所以，进一步提高安全性以及使用者的便利性。

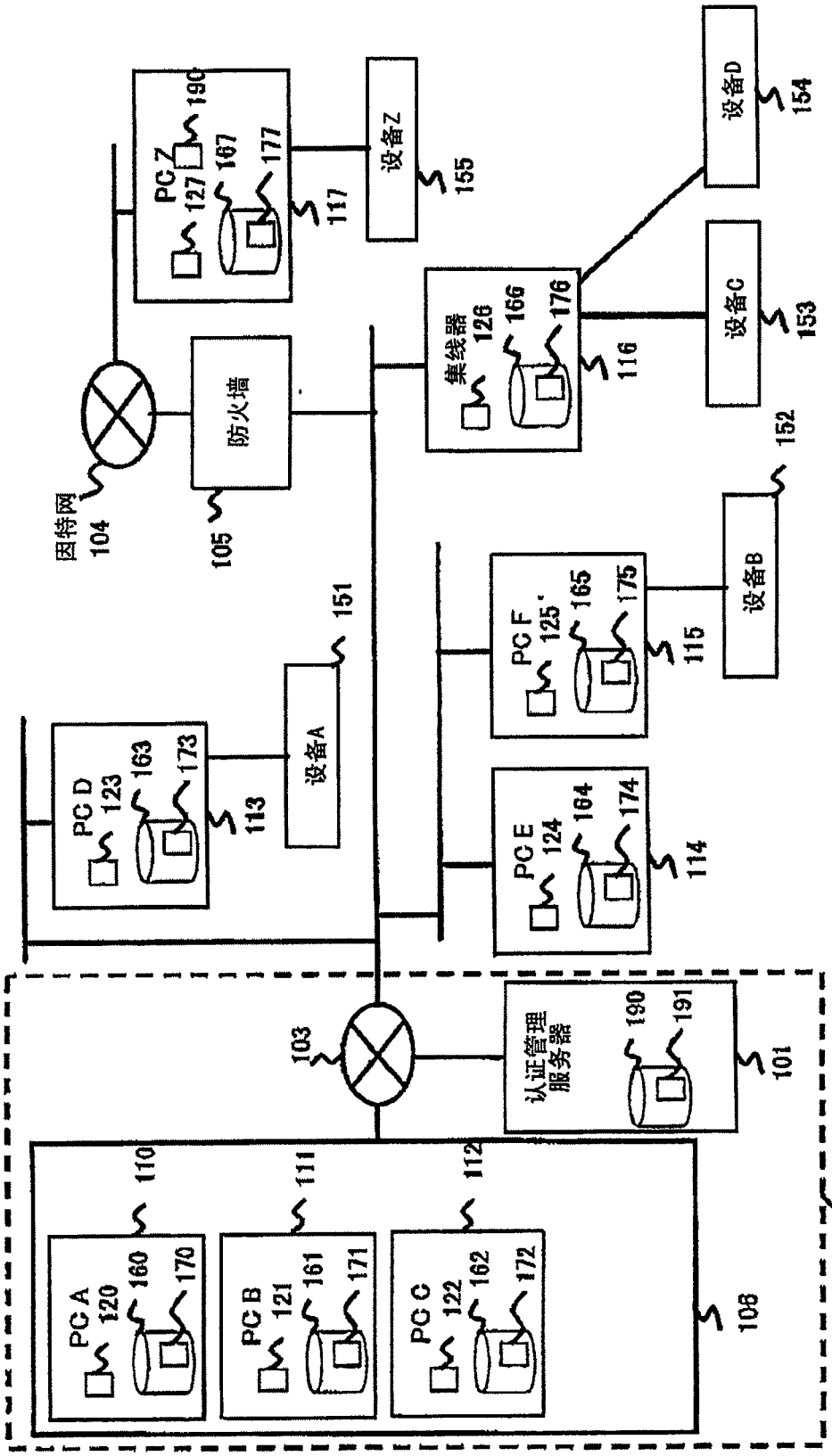

因特网
104
防火墙
105
PC Z
127
167
177
190
117
设备Z
155
集线器
126
166
176
116
设备C
153
设备D
154
152
设备B
PC F
125'
165
175
115
151
设备A
PC D
123
163
173
113
PC E
124
164
174
114
103
认证管理
服务器
190
191
101
110
111
112
PC A
120
160
170
PC B
121
161
171
PC C
122
162
172
108
信息中心102

图 1

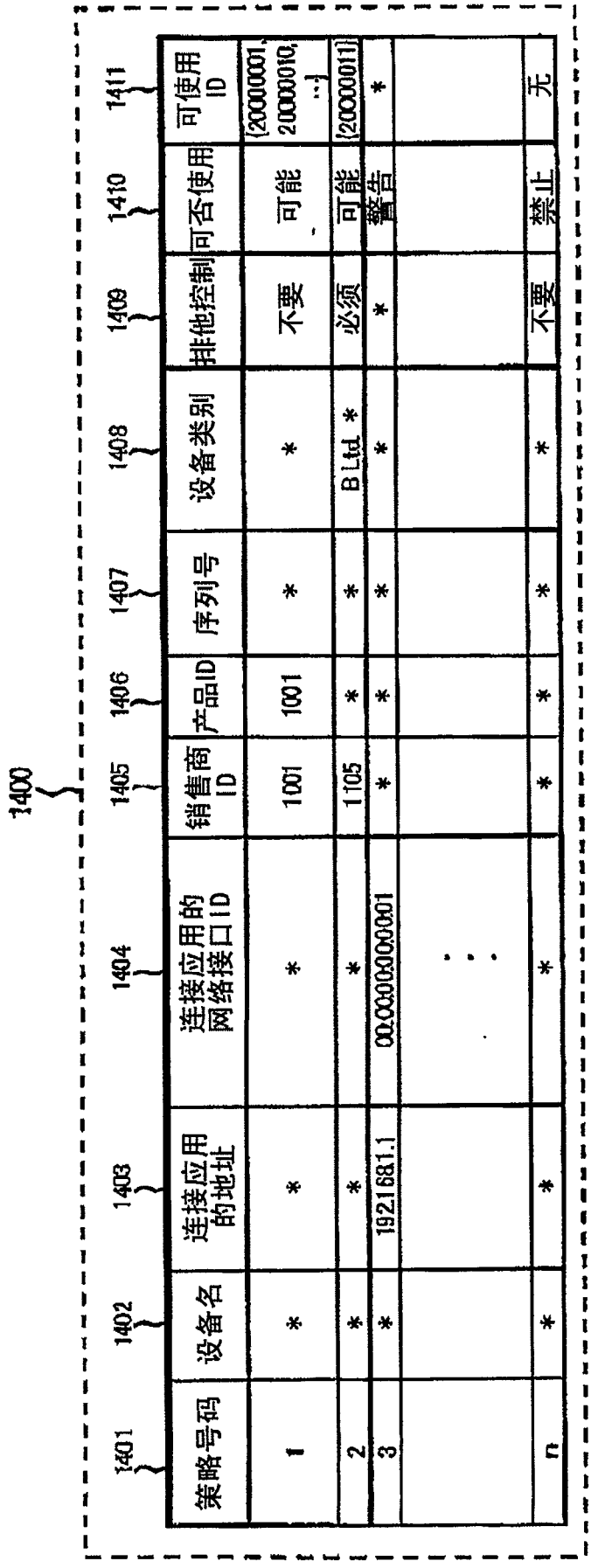
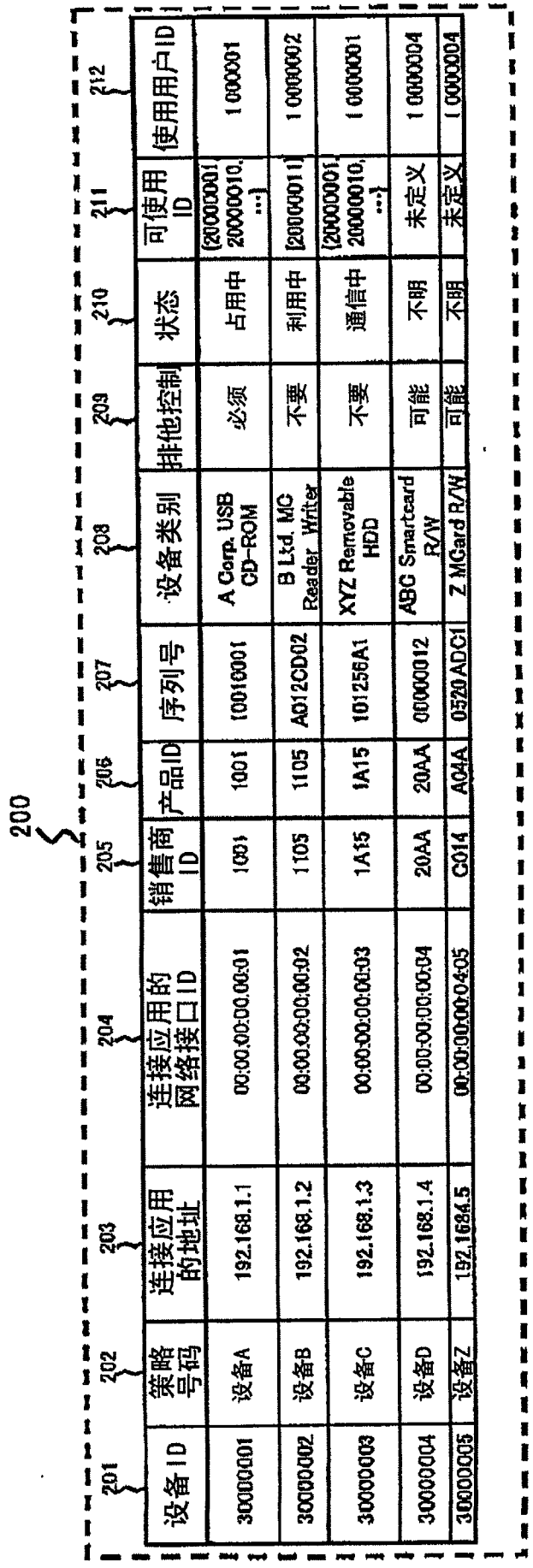

1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
策略号码
设备名
连接应用的地址
连接应用的网络接口ID
销售商ID
产品ID
序列号
设备类别
排他控制
可否使用
可使用ID
1
*
*
*
1001
1001
*
*
不要
可能
{20000001, 20000010, ...}
2
*
*
*
1105
*
*
BLtd *
必须
可能
{20000011}
3
*
192168.1.1
00:00:00:00:00:01
*
*
*
*
警告
*
n
*
*
*
*
*
*
不要
禁止
无

图 2



设备ID	策略号码	连接应用的地址	连接应用的网络接口ID	销售商ID	产品ID	序列号	设备类别	排他控制	状态	可使用ID	使用用户ID
30000001	设备A	192.168.1.1	00:00:00:00:00:01	1001	1001	10010001	A Corp. USB CD-ROM	必须	占用中	{20000001, 20000010, ...}	10000001
30000002	设备B	192.168.1.2	00:00:00:00:00:02	1105	1105	A012CD02	B Ltd. MC Reader Writer	不要	利用中	{20000011}	10000002
30000003	设备C	192.168.1.3	00:00:00:00:00:03	1A15	1A15	101256A1	XYZ Removable HDD	不要	通信中	{20000001, 20000010, ...}	10000001
30000004	设备D	192.168.1.4	00:00:00:00:00:04	20AA	20AA	00000012	ABC Smartcard R/W	可能	不明	未定义	10000004
30000005	设备Z	192.1684.5	00:00:00:00:04:05	C014	A04A	0520ADC1	Z MCard R/W	可能	不明	未定义	10000004

图 3

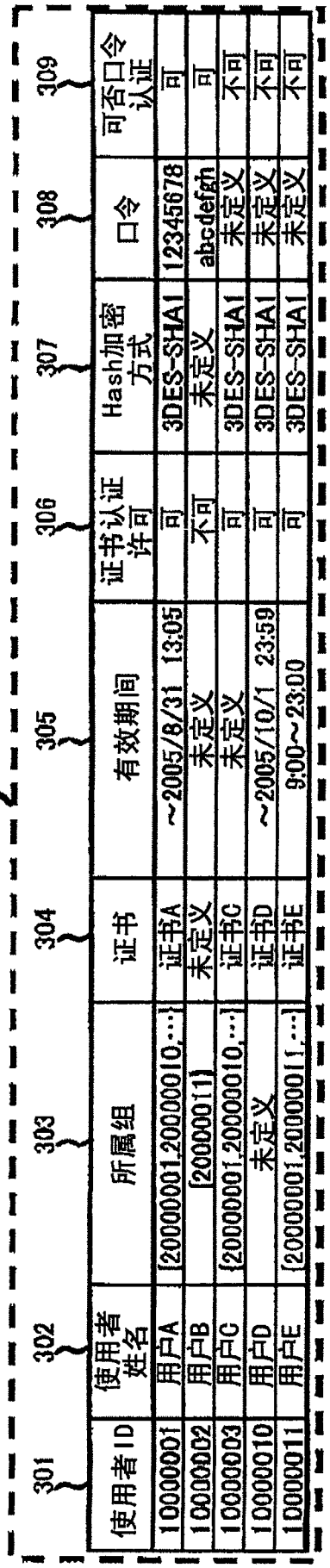

300
301
302
303
304
305
306
307
308
309
使用者ID
使用者姓名
所属组
证书
有效期间
证书认证许可
Hash加密方式
口令
可否口令认证
10000001 用户A {20000001,20000010,...} 证书A ~2005/8/31 13:05 可 3DES-SHA1 12345678 可
10000002 用户B {20000011} 未定义 未定义 不可 未定义 abcdefgh 可
10000003 用户C {20000001,20000010,...} 证书C 未定义 可 3DES-SHA1 未定义 不可
10000010 用户D 未定义 证书D ~2005/10/1 23:59 可 3DES-SHA1 未定义 不可
10000011 用户E {20000001,20000011,...} 证书E 9:00~23:00 可 3DES-SHA1 未定义 不可

图 4

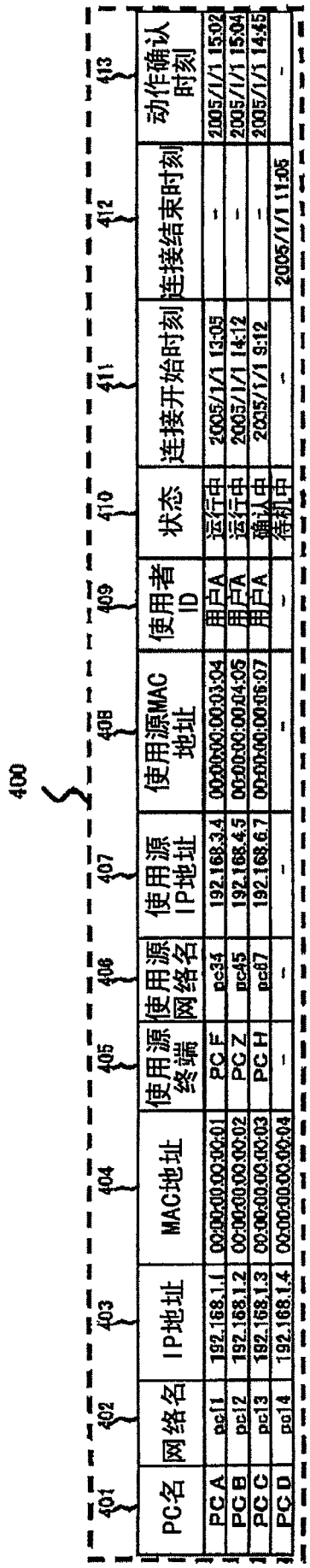

400
401
402
403
404
405
406
407
408
409
410
411
412
413
PC名
网络名
IP地址
MAC地址
使用源终端
使用源网络名
使用源IP地址
使用源MAC地址
使用者ID
状态
连接开始时刻
连接结束时刻
动作确认时刻
PC A
pc11
192.168.1.1
00:00:00:00:00:01
PC F
pc34
192.168.3.4
00:00:00:00:03:04
用户A
运行中
2005/1/1 13:05
-
2005/1/1 15:02
PC B
pc12
192.168.1.2
00:00:00:00:00:02
PC Z
pc45
192.168.4.5
00:00:00:00:04:05
用户A
运行中
2005/1/1 14:12
-
2005/1/1 15:04
PC C
pc13
192.168.1.3
00:00:00:00:00:03
PC H
pc67
192.168.6.7
00:00:00:00:06:07
用户A
确认中
2005/1/1 9:12
-
2005/1/1 14:45
PC D
pc14
192.168.1.4
00:00:00:00:00:04
-
-
-
-
待机中
2005/1/1 11:05
-
-

图 5

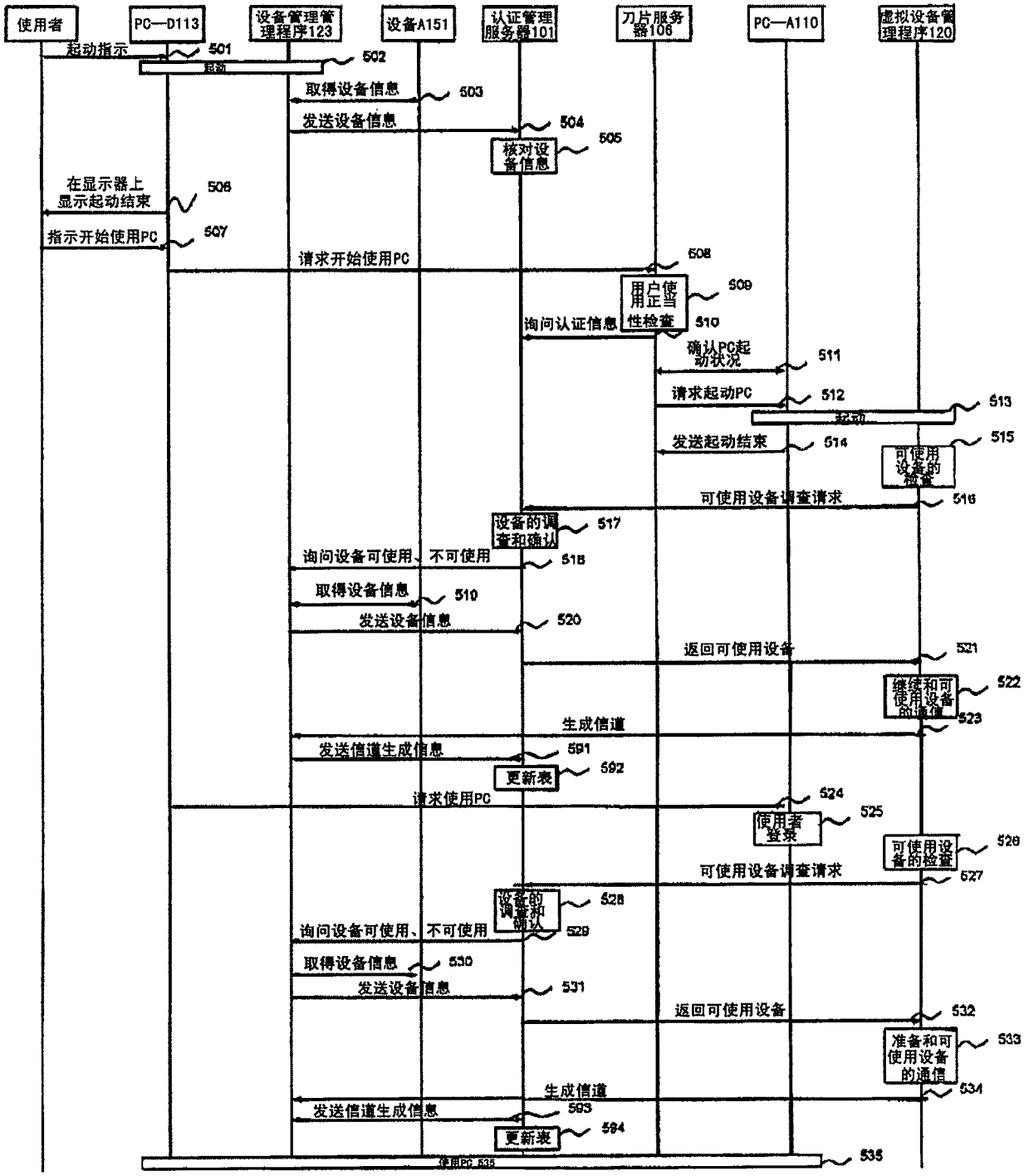

使用者
PC—D113
设备管理管理程序123
设备A151
认证管理服务器101
刀片服务器106
PC—A110
虚拟设备管理程序120
起动指示
501
起动
502
取得设备信息
503
发送设备信息
504
核对设备信息
505
在显示器上显示起动结束
506
指示开始使用PC
507
请求开始使用PC
508
用户使用正当性检查
509
询问认证信息
510
确认PC起动状况
511
请求起动PC
512
起动
513
发送起动结束
514
可使用设备的检查
515
可使用设备调查请求
516
设备的调查和确认
517
询问设备可使用、不可使用
518
取得设备信息
519
发送设备信息
520
返回可使用设备
521
继续和可使用设备的通信
522
523
生成信道
发送信道生成信息
591
更新表
592
请求使用PC
524
使用者登录
525
可使用设备的检查
526
可使用设备调查请求
527
设备的调查和确认
528
询问设备可使用、不可使用
529
取得设备信息
530
发送设备信息
531
返回可使用设备
532
准备和可使用设备的通信
533
生成信道
534
发送信道生成信息
593
更新表
594
使用PC 535
535

图 6

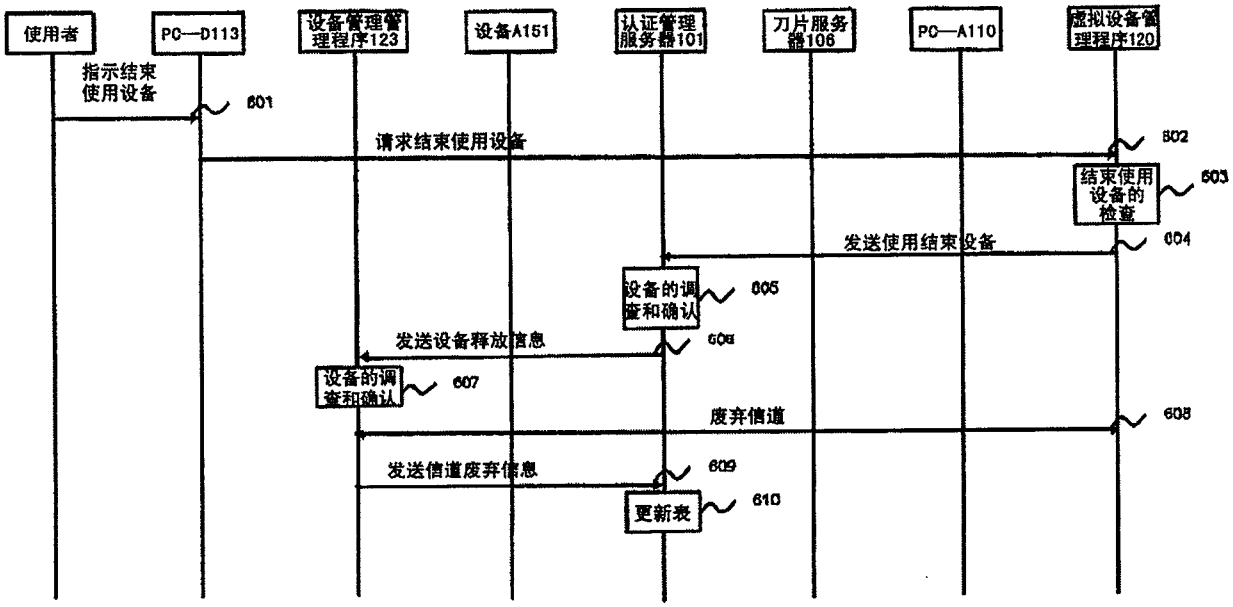

使用者
PC—D113
设备管理管理程序123
设备A151
认证管理服务器101
刀片服务器106
PC—A110
虚拟设备管理程序120
指示结束使用设备
601
请求结束使用设备
602
结束使用设备的检查
603
发送使用结束设备
604
设备的调查和确认
605
发送设备释放信息
606
设备的调查和确认
607
废弃信道
608
发送信道废弃信息
609
更新表
610

图 7

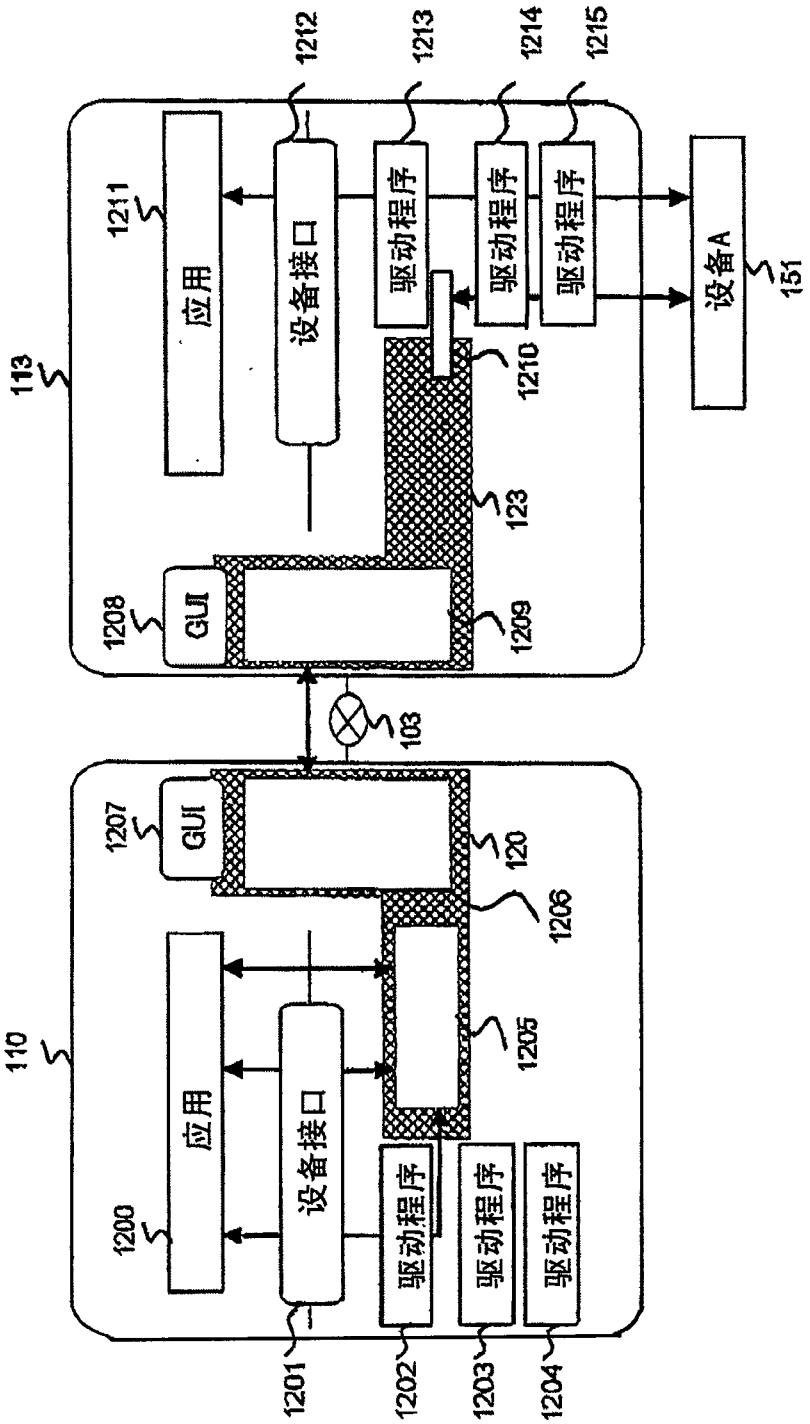

110
113
应用
设备接口
驱动程序
驱动程序
驱动程序
GUI
GUI
应用
设备接口
驱动程序
驱动程序
驱动程序
设备A
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
120
123
151
103

图 8

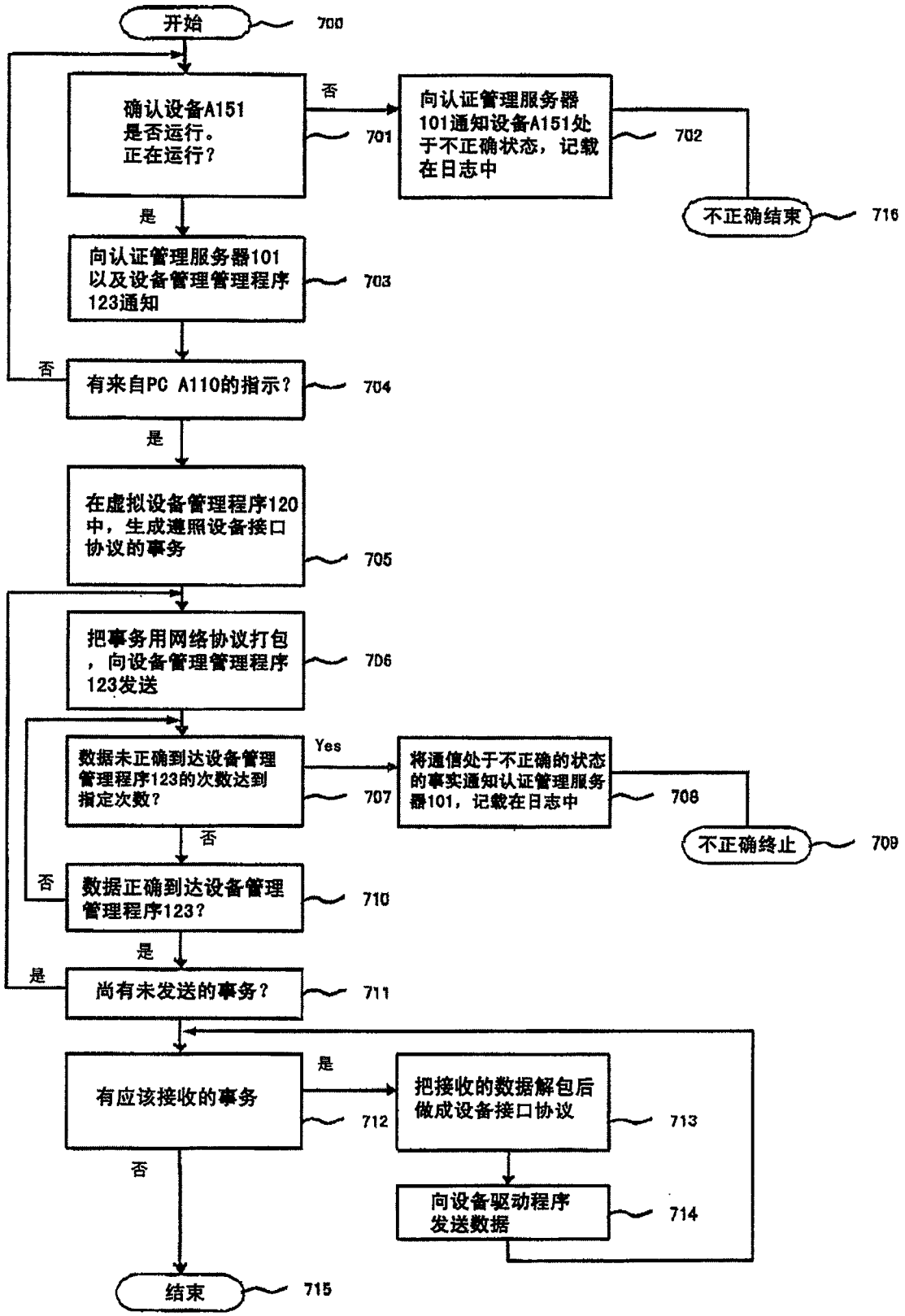

开始
700
确认设备A151是否运行。正在运行？
701
否
向认证管理服务器101通知设备A151处于不正确状态，记载在日志中
702
不正确结束
716
是
向认证管理服务器101以及设备管理管理程序123通知
703
否
有来自PC A110的指示？
704
是
在虚拟设备管理程序120中，生成遵照设备接口协议的事务
705
把事务用网络协议打包，向设备管理管理程序123发送
706
数据未正确到达设备管理管理程序123的次数达到指定次数？
707
Yes
将通信处于不正确的状态的事实通知认证管理服务器101，记载在日志中
708
不正确终止
709
否
数据正确到达设备管理管理程序123？
710
否
是
尚有未发送的事务？
711
是
有应该接收的事务
712
是
把接收的数据解包后做成设备接口协议
713
向设备驱动程序发送数据
714
否
结束
715

图 9

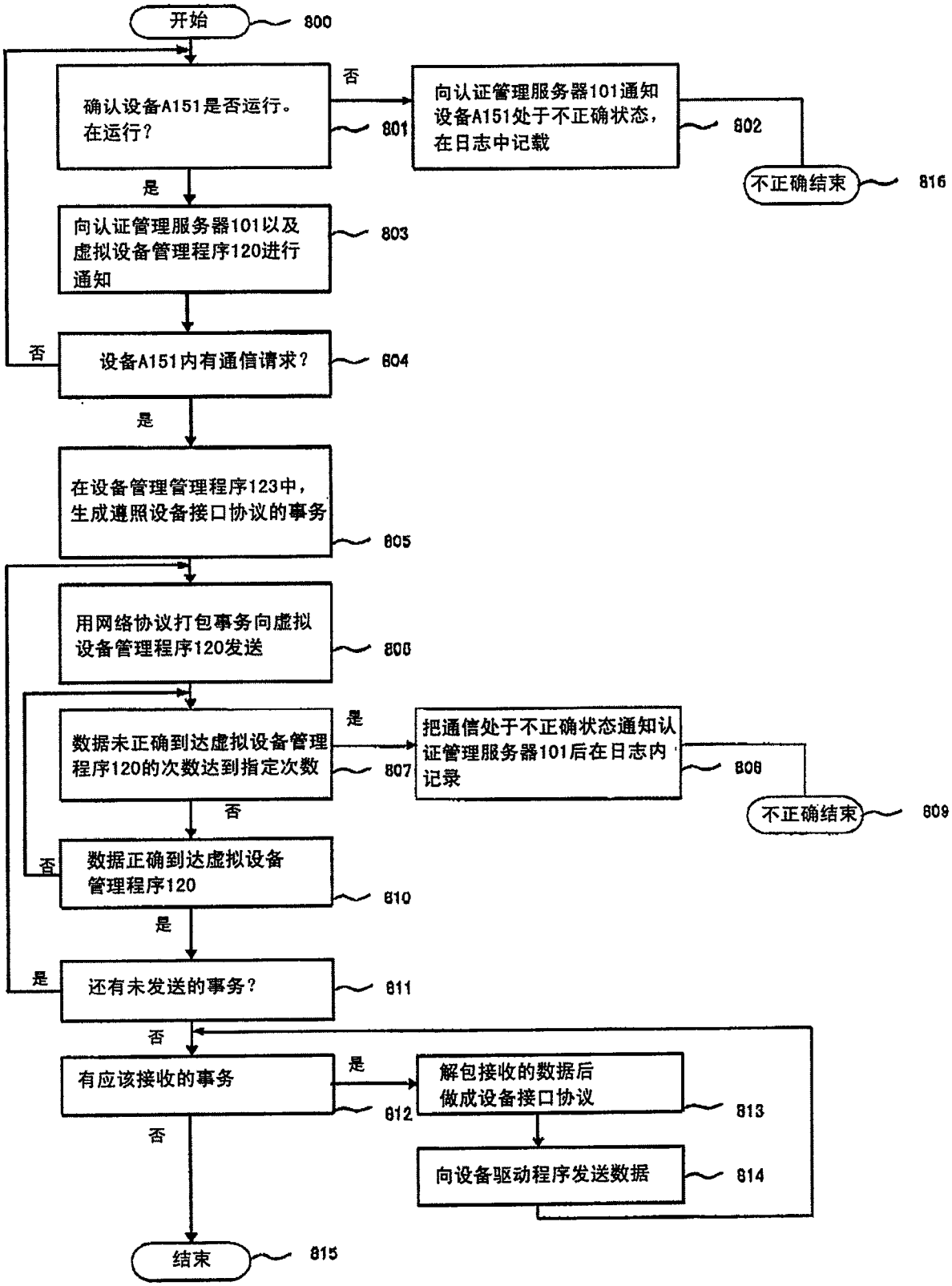

开始
800
确认设备A151是否运行。在运行?
801
否
向认证管理服务器101通知设备A151处于不正确状态,在日志中记载
802
不正确结束
816
是
向认证管理服务器101以及虚拟设备管理程序120进行通知
803
否
设备A151内有通信请求?
804
是
在设备管理管理程序123中,生成遵照设备接口协议的事务
805
用网络协议打包事务向虚拟设备管理程序120发送
806
数据未正确到达虚拟设备管理程序120的次数达到指定次数
807
是
把通信处于不正确状态通知认证管理服务器101后在日志内记录
808
不正确结束
809
否
否
数据正确到达虚拟设备管理程序120
810
是
是
还有未发送的事务?
811
否
有应该接收的事务
812
是
解包接收的数据后做成设备接口协议
813
向设备驱动程序发送数据
814
否
结束
815

图 10

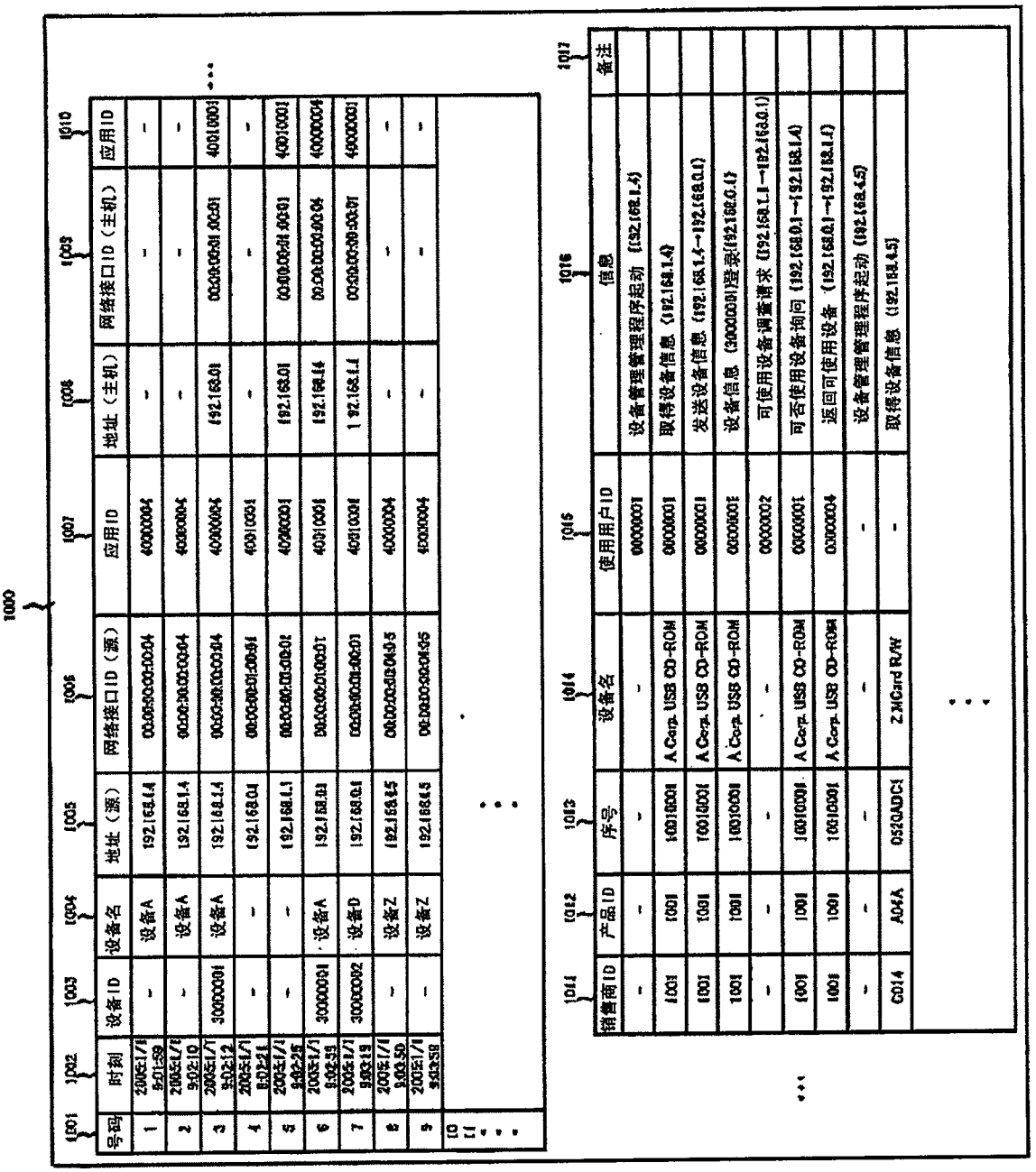

1000
1001 1002 1003 1004 1005 1006 1007 1008 1009 1010
号码 时刻 设备ID 设备名 地址（源） 网络接口ID（源） 应用ID 地址（主机） 网络接口ID（主机） 应用ID
1 2005/1/1 9:01:59 - 设备A 192.168.1.4 00:05:5D:00:00:04 40000004 - - -
2 2005/1/1 9:02:10 - 设备A 192.168.1.4 00:02:3D:00:00:04 40000004 - - -
3 2005/1/1 9:02:12 30000001 设备A 192.168.1.4 00:05:5D:00:00:04 40000004 192.168.0.1 00:00:00:01:00:01 40010001
4 2005/1/1 9:02:21 - - 192.168.0.1 00:00:00:01:00:01 40010001 - - -
5 2005/1/1 9:02:25 - - 192.168.1.1 00:00:3D:00:00:01 40000001 192.168.0.1 00:00:00:01:00:01 40010001
6 2005/1/1 9:02:33 30000001 设备A 192.168.0.1 00:00:00:01:00:01 40010001 192.168.1.4 00:00:00:00:00:04 40000004
7 2005/1/1 9:03:19 30000002 设备D 192.168.0.1 00:00:00:01:00:01 40010001 192.168.1.4 00:00:00:00:00:01 40000001
8 2005/1/1 9:03:30 - 设备Z 192.168.1.5 00:00:00:00:04:05 40000004 - - -
9 2005/1/1 9:03:58 - 设备Z 192.168.1.5 00:00:00:00:04:05 40000004 - - -
10
11
1011 1012 1013 1014 1015 1016 1017
销售商ID 产品ID 序号 设备名 使用用户ID 信息 备注
- - - - 00000001 设备管理管理程序起动（192.168.1.4） -
1001 1001 10010001 A Corp. USB CD-ROM 00000001 取得设备信息（192.168.1.4） -
1001 1001 10010001 A Corp. USB CD-ROM 00000001 发送设备信息（192.168.1.4→192.168.0.1） -
1001 1001 10010001 A Corp. USB CD-ROM 00000001 设备信息（30000001登录192.168.0.1） -
- - - - 00000002 可使用设备调查请求（192.168.1.1→192.168.0.1） -
1001 1001 10010001 A Corp. USB CD-ROM 00000001 可否使用设备询问（192.168.0.1→192.168.1.4） -
1001 1001 10010001 A Corp. USB CD-ROM 00000004 返回可使用设备（192.168.0.1→192.168.1.4） -
- - - - - 设备管理管理程序起动（192.168.4.5） -
CD14 A04A 0520ADC1 ZMCard R/W - 取得设备信息（192.168.4.5） -

图 11

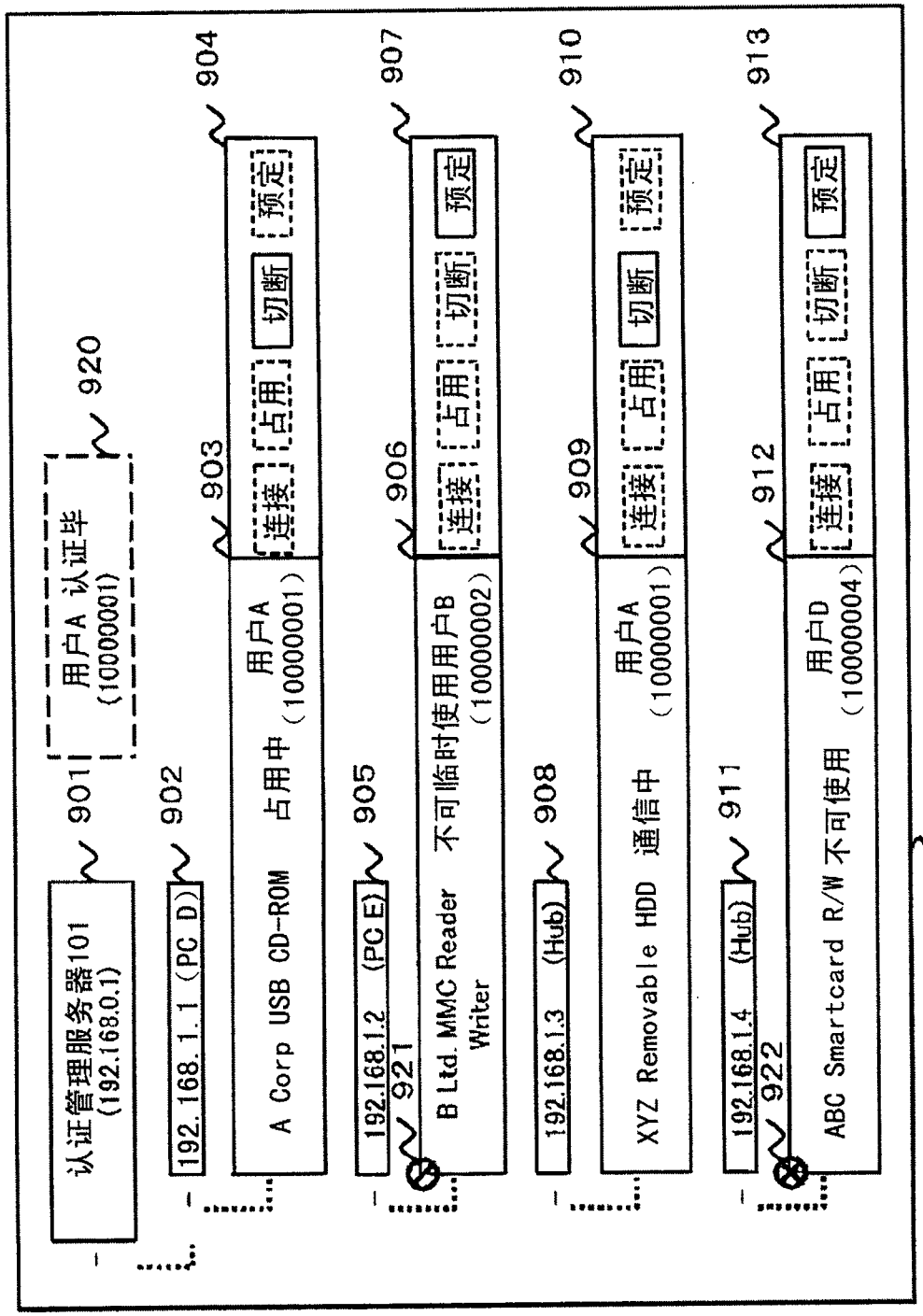

认证管理服务器101
(192.168.0.1)
901
用户A 认证毕
(10000001)
920
900
192.168.1.1 (PC D)
902
A Corp USB CD-ROM 占用中 用户A (10000001)
903
连接
占用
切断
预定
904
192.168.1.2 (PC E)
905
921
B Ltd. MMC Reader Writer 不可临时使用用户B (10000002)
906
907
192.168.1.3 (Hub)
908
XYZ Removable HDD 通信中 用户A (10000001)
909
910
192.168.1.4 (Hub)
911
922
ABC Smartcard R/W 不可使用 用户D (10000004)
912
913

图 12

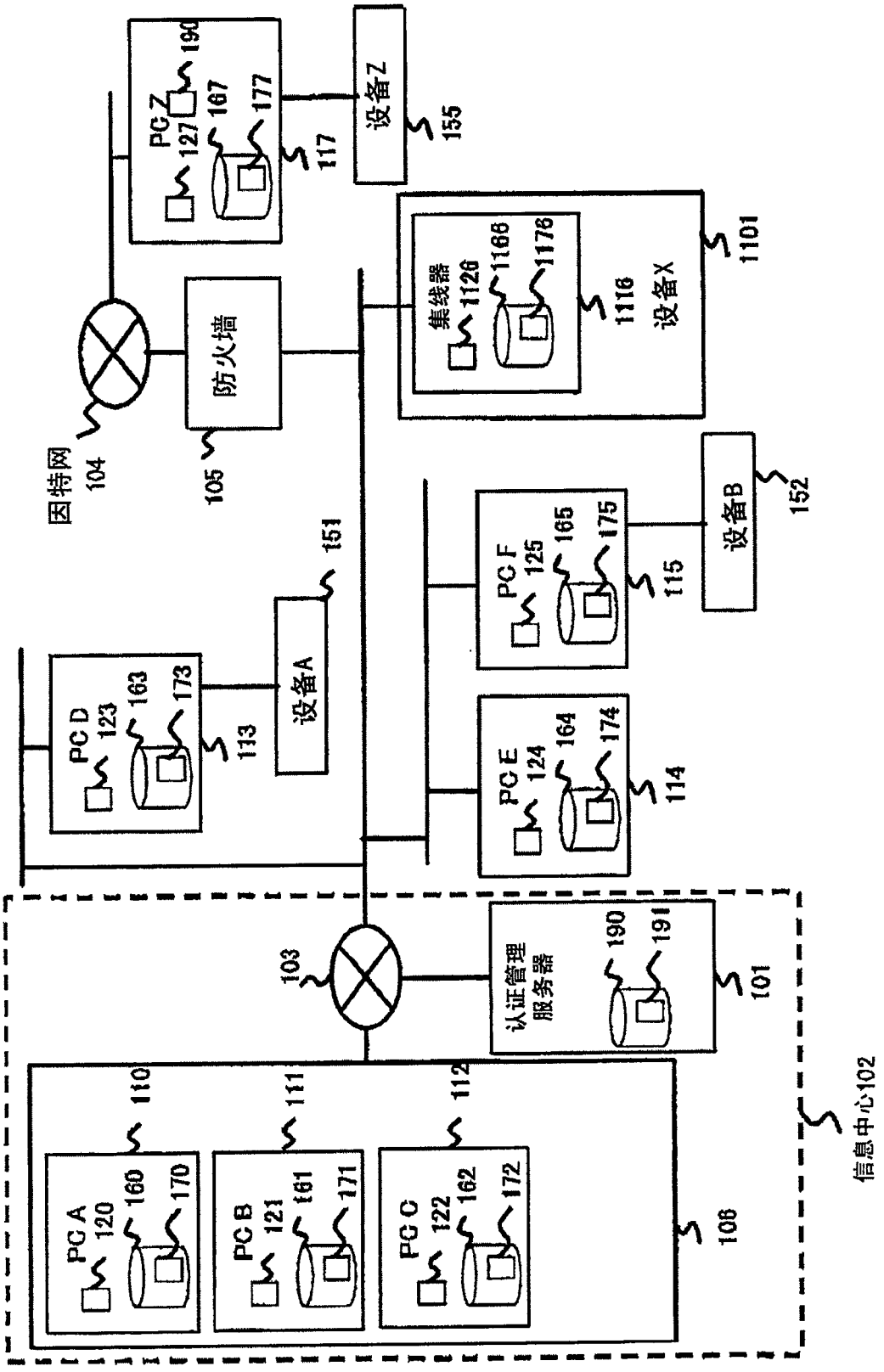

因特网
104
防火墙
105
PC Z
127
190
167
177
117
设备Z
155
集线器
1126
1166
1176
1116
设备X
1101
PC F
125
165
175
115
设备B
152
151
设备A
PC D
123
163
173
113
PC E
124
164
174
114
103
认证管理
服务器
190
191
101
110
111
112
PC A
120
160
170
PC B
121
161
171
PC C
122
162
172
106
信息中心102

图 13

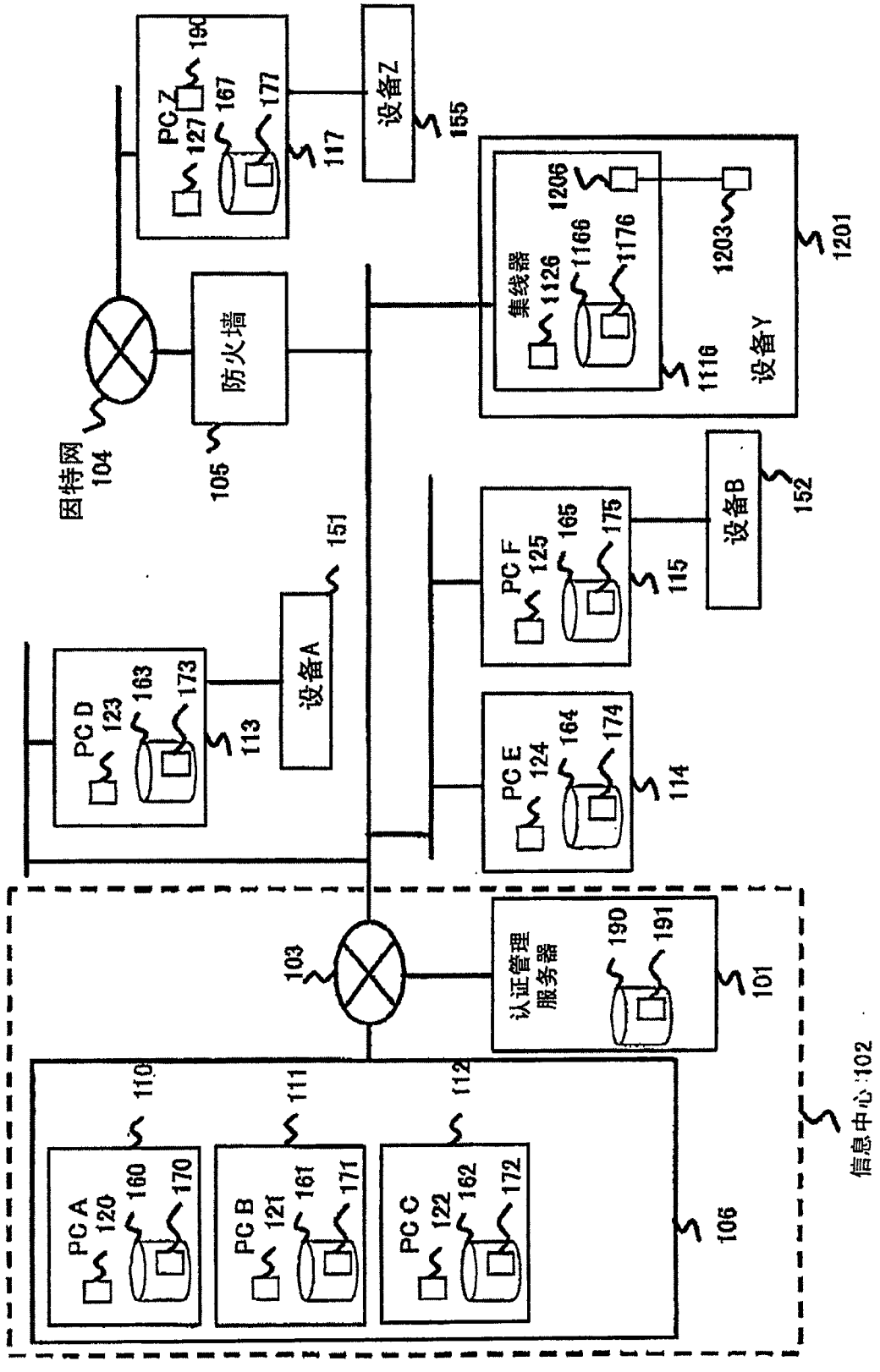

因特网
104
防火墙
105
PC Z
127
167
177
190
117
设备Z
155
集线器
1126
1166
1176
1206
1116
1203
设备Y
1201
PC F
125
165
175
115
设备B
152
PC D
123
163
173
113
设备A
151
PC E
124
164
174
114
103
认证管理
服务器
190
191
101
PC A
120
160
170
110
PC B
121
161
171
111
PC C
122
162
172
112
106
信息中心:102

图 14

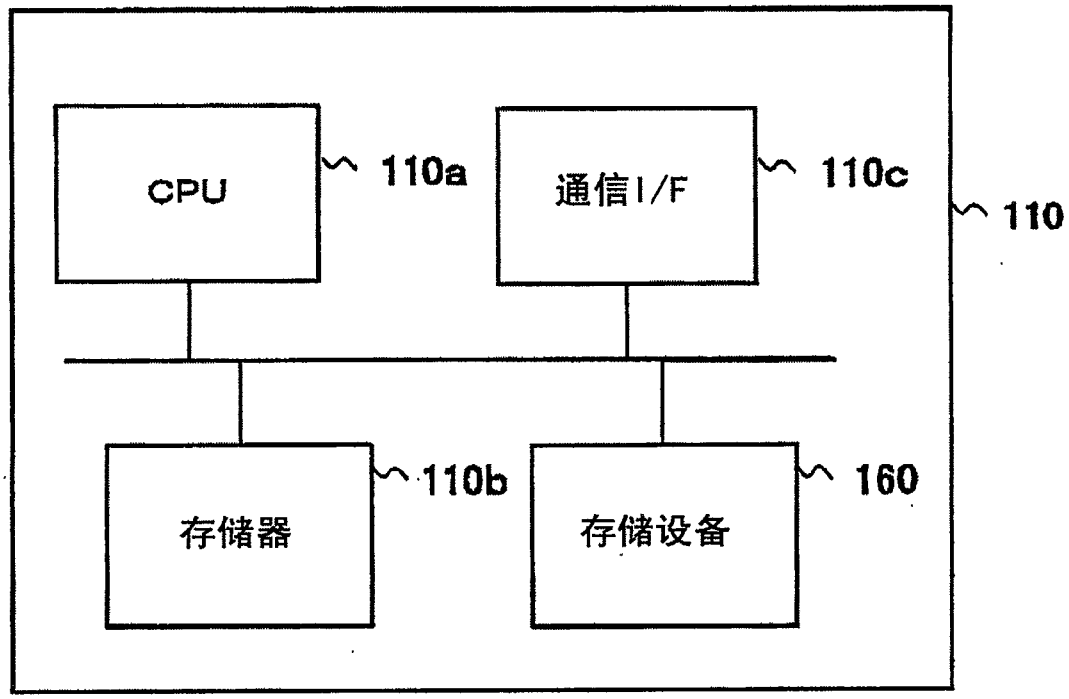


图 15