

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.

H04L 9/00 (2006.01)

H04Q 7/22 (2006.01)



[12] 发明专利申请公开说明书

[21] 申请号 200610000599.4

[43] 公开日 2006 年 7 月 19 日

[11] 公开号 CN 1805332A

[22] 申请日 2006.1.11

[21] 申请号 200610000599.4

[30] 优先权

[32] 2005.1.11 [33] JP [31] 2005-004408

[71] 申请人 株式会社 NTT 都科摩

地址 日本东京

[72] 发明人 大前浩司 松本洋一

[74] 专利代理机构 北京三友知识产权代理有限公司

代理人 李 辉

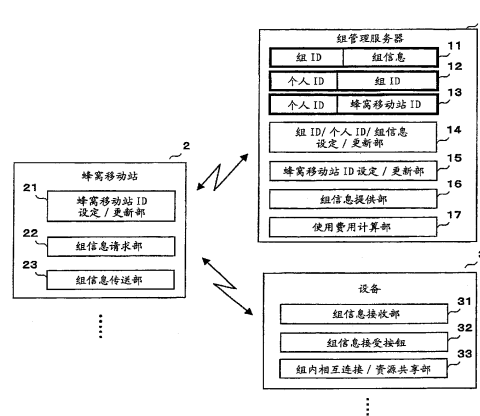
权利要求书 3 页 说明书 13 页 附图 14 页

[54] 发明名称

安全组管理系统

[57] 摘要

一种安全组管理系统，能够在属于规定组的设备之间进行安全的相互连接或资源共享。该安全组管理系统具备蜂窝移动站、属于一组的两个或更多个设备、以及组管理服务器。组管理服务器包括：存储单元，被构成为预先存储由该组的成员登记的关于蜂窝移动站的信息和关于该组的组信息；以及组信息提供单元，被构成为仅仅响应于来自登记的蜂窝移动站的接入而提供组信息。蜂窝移动站具有组信息传送单元，所述组信息传送单元被构成为向所述两个或更多个设备提供组信息以使得所述两个或更多个设备可以识别出它们属于该组并且可以在它们之间进行安全的相互连接和/或资源共享。



1、一种安全组管理系统，包括蜂窝移动站、属于一组的一个或多个设备、以及组管理服务器，

5 其特征在于，组管理服务器包括：

存储单元，被构成为预先存储关于蜂窝移动站的信息和关于该组的组信息；以及

组信息提供单元，被构成为仅仅响应于来自登记的蜂窝移动站的接入而提供组信息；并且

10 其特征在于，蜂窝移动站具有组信息传送单元，所述组信息传送单元被构成为将组信息提供给所述一个或多个设备以使得所述一个或多个设备可以识别出它们属于该组并且可以在它们之间进行安全的相互连接和/或资源共享。

2、根据权利要求1所述的安全组管理系统，其特征在于，组信息是
15 包含分配给该组的第一公钥并且利用与该第一公钥成对的第一私钥进行了签名的电子证书。

3、根据权利要求2所述的安全组管理系统，其特征在于，当所述一个或多个设备中的一个接收到电子证书时，该设备随后信赖该电子证书的发行者作为证书授权。

20 4、根据权利要求2所述的安全组管理系统，其特征在于，组信息是由对各个设备分配的第二私钥和第二公钥组成的设备密钥对。

5、根据权利要求1所述的安全组管理系统，其特征在于，组信息是分配给该组的对等密钥。

25 6、根据权利要求1所述的安全组管理系统，其特征在于，组信息是列出属于该组的设备的列表。

7、根据权利要求1所述的安全组管理系统，其特征在于，在安全套接层客户认证成功之后开始蜂窝移动站与组管理服务器之间的通信。

8、根据权利要求1所述的安全组管理系统，其特征在于，蜂窝移动站和所述一个或多个设备具有近距离无线接口，并且通过近距离无线

通信将组信息从蜂窝移动站提供给所述两个或更多个设备。

9、根据权利要求1所述的安全组管理系统，其特征在于，所述两个或更多个设备中的至少一个具有一硬件按钮，用于将对组信息的接收限制于按下该硬件按钮之后的规定时间段内。

5 10、根据权利要求1所述的安全组管理系统，其特征在于，存储单元包括：

 第一存储单元，被构成为将组标识符与组信息相关联地存储；

 第二存储单元，被构成为将表示属于该组并使用蜂窝移动站的个人的个人标识符与组标识符相关联地存储；以及

10 第三存储单元，被构成为将表示蜂窝移动站的蜂窝移动站标识符与个人标识符相关联地存储。

 11、根据权利要求10所述的安全组管理系统，其特征在于，响应于来自蜂窝移动站的请求在第三存储单元中对蜂窝移动站标识符进行登记和更新。

15 12、根据权利要求1所述的安全组管理系统，其特征在于，组管理服务器生成并输出包含表示蜂窝移动站的用户个人标识符以及该组管理服务器的网络地址的二维码，并且蜂窝移动站具有用于读取发布给所述用户的二维码以接入组管理服务器的码读取器。

20 13、根据权利要求1所述的安全组管理系统，其特征在于，存储单元进一步与表示蜂窝移动站的蜂窝移动站标识符相关联地存储表示各个设备的设备标识符、以及相关关联的设备的属性。

 14、根据权利要求13所述的安全组管理系统，其特征在于，通过蜂窝移动站从所述设备获取设备标识符，并且从蜂窝移动站将该设备标识符提供给组管理服务器。

25 15、根据权利要求13所述的安全组管理系统，其特征在于，通过蜂窝移动站的用户生成设备标识符，将所述设备标识符赋予所述设备，并在组管理服务器的存储单元中对其进行登记和更新。

 16、根据权利要求13所述的安全组管理系统，其特征在于，存储单元与各个设备的业务优先级相关联地存储该设备的主要用途作为属性。

17、根据权利要求 16 所述的安全组管理系统，其特征在于，存储单元响应于来自蜂窝移动站的请求暂时改变业务优先级，并且组信息提供单元通过蜂窝移动站将该改变通知给设备。

18、根据权利要求 16 所述的安全组管理系统，其特征在于，所述两个或更多个设备中的至少一个具有两个或更多个无线接口，并且所述两个或更多个无线接口分类为普通业务类和优先业务类以防止频率彼此重叠。

19、根据权利要求 16 所述的安全组管理系统，其特征在于，在从蜂窝移动站接收到对内容发布的请求时，组管理服务器从存储单元选择最适当的设备来接收内容并将内容发布给所选择的设备。

20、根据权利要求 1 所述的安全组管理系统，其特征在于，组管理服务器进一步包括：

使用费用计算单元，被构成为根据存储区域使用大小、服务使用时间、接入次数、接入时间、取得信息量中的至少一项来计算使用费用。

21、一种应用于网状网络的安全组管理方法，所述网状网络包括蜂窝移动站、属于一组的一个或更多个设备、以及组管理服务器，所述方法包括如下步骤：

预先将蜂窝移动站登记在组管理服务器中；

在组管理服务器中针对所述组生成并存储组信息；

仅仅响应于来自登记的蜂窝移动站的接入而将组信息从组管理服务器提供给蜂窝移动站，以及

将组信息从蜂窝移动站提供给所述一个或更多个设备以使得所述一个或更多个设备可以识别出它们属于该组并且可以在它们之间进行安全的相互连接和/或资源共享。

安全组管理系统

5 技术领域

本发明涉及一种能够在属于规定组的多个设备之间进行安全的相互连接或资源共享的安全组管理系统。

背景技术

10 以往，为了只许可来自属于规定组的成员所使用的个人计算机等设备（机器）的接入，而防止来自除此之外的没有权限的第三者的不正当接入，使用接入控制表（ACL），通过拒绝未登记在该接入控制表中的使用者或设备的连接等，防止了来自没有权限的第三者的不正当接入。

在无线局域网连接的情况下，使用被称作 MAC（Media Access
15 Control，介质接入控制）地址过滤的接入控制表进行接入控制，多个接入点（AP）共享该接入控制表，并且拒绝来自 MAC 地址未登记在接入控制表中的设备的接入。

如上所述，以往只是单纯地根据接入控制表的登记信息来防止来自第三者的不正当接入，因此存在如下问题。

20 即，上述现有技术是通过规定路径接入的情况下，由该路径内的接入点等进行基于接入控制表的检查，然而不能应对在多个设备之间进行直接相互连接或者资源共享的情况。例如，考虑如下情况，即，在属于规定组的成员之间把个人计算机等设备相互连接以进行信息交换，或者利用信息家电等设备组成网状网络以进行设备间的相互连接或资源共享，
25 在该情况下，被连接侧的设备很难预先确定对方的设备，因此，难以防止怀有恶意的第三者的冒充。因此，存在本应该只对组内成员公开的信息泄露到组外的危险。

此外，即使在接入路径内设置基于接入控制表的检查机构的情况下，每次添加新用户或设备时管理人员也必须更新接入控制表的内容，操作

烦杂，而且难以进行迅速的响应。特别地，在形成网状网络的情况下该问题尤为突出，网状网络的优点之一是可以使多人的设备加入到网状网络中而扩大覆盖区域，但是为了发挥该优点，多个网格加入者必须能够自由地把各自的设备连接到网状网络，而这用现有的技术是很难实现的。

发明内容

本发明是鉴于上述现有技术的问题而提出的，其目的在于提供一种能够在属于规定组的设备之间进行安全的相互连接或资源共享的安全组管理系统。

为了解决上述问题，本发明的第一方面提供了一种安全组管理系统，包括蜂窝移动站、属于一组的一个或多个设备、以及组管理服务器。在该系统中，组管理服务器包括：存储单元，被构成为预先存储该组的成员登记的关于蜂窝移动站的信息以及关于该组的组信息；以及组信息提供单元，被构成为仅仅响应于来自登记的蜂窝移动站的接入而提供组信息。蜂窝移动站具有组信息传送单元，所述组信息传送单元被构成为向所述一个或多个设备提供组信息以使得所述一个或多个设备可以识别出它们属于该组并且可以在它们之间进行安全的相互连接和/或资源共享。从而，仅通过由属于规定组的成员使用的、预先登记的蜂窝移动站向设备提供组信息，因此通过成员与蜂窝移动站的一体性，可以防止怀有恶意的第三者的冒充，并且可以在属于规定组的设备之间进行安全的相互连接或资源共享。此外，由于通过蜂窝移动站向设备提供组信息，因此即使没有专用接收器的小型设备也能够共享组信息。

根据本发明的第二方面，上述组信息可以是利用预先分配给该组的私钥进行了签名并且包括与上述私钥成对的公开密钥的电子证书。从而，能够进行基于该电子证书的设备间安全相互连接或资源共享。

根据本发明的第三方面，上述组信息可以包括上述设备用的私钥和公钥对。从而，能够进行基于设备用私钥和公钥对的设备间安全相互连接或资源共享。

根据本发明的第四方面,上述组信息可以是预先分配给该组的对等密钥(symmetric key)。从而,能够进行基于对等密钥的设备间安全相互连接或资源共享。

根据本发明的第五方面,上述组信息是属于该组的设备的一览表。

5 从而,能够仅在属于规定组的设备之间进行安全的相互连接或资源共享。

根据本发明的第六方面,上述蜂窝移动站和上述组管理服务器之间的通信可以经过SSL(安全套接层)客户认证来进行。从而,即使把组管理服务器配置在互联网上,也能够确保与蜂窝网同等的安全等级,能够安全地发布组信息。

10 根据本发明的第七方面,上述蜂窝移动站和上述设备之间的通信可以通过近距离无线接口来进行。从而,能够迅速地提供组信息,并且限定了组信息被提供的范围,能够降低泄露、窃听等的危险。

根据本发明的第八方面,仅在按下了上述设备侧的硬件按钮之后的一定时间段内,能够从上述蜂窝移动站向上述设备提供组信息。从而,
15 能够防止因蜂窝移动站的误操作而造成无意地提供组信息。

根据本发明的第九方面,上述组管理服务器可以具备:第1存储单元,其将用于标识组的组ID和上述组信息对应地保存;第2存储单元,其将用于标识属于组的个人的个人ID和上述组ID对应地保存;第3存储单元,其将上述个人ID和用于识别上述蜂窝移动站的蜂窝移动站ID对应地保存。
20 从而,属于组的个人能够自由地设定/更新蜂窝移动站ID。

根据本发明的第十方面,可以根据来自上述蜂窝移动站的请求对上述蜂窝移动站ID进行设定或更新。从而在组管理服务器侧,只要以个人为单位来对组进行管理即可,而不需要细到对每个人拥有的蜂窝移动站进行管理,因此能够简化组管理服务器侧的管理作业而不会降低安全性。

25 根据本发明的第十一方面,通过由上述蜂窝移动站读取包含个人ID、密码和上述组管理服务器的地址的QR代码,能够进行从上述蜂窝移动站到上述组管理服务器的连接。从而,能够防止误输入,并且能够简化设定蜂窝移动站ID时的操作。

根据本发明的第十二方面,上述存储单元保存用于标识上述设备的

设备 ID、该设备的属性、蜂窝移动站 ID。从而，能够容易地管理限定属于规定组的设备的设备一览。

根据本发明的第十三方面，通过蜂窝移动站从上述设备获取设备 ID，并且通过从蜂窝移动站把设备 ID 提供给组管理服务器，从而在存储单元
5 中对设备 ID 进行设定或更新。由此能够迅速且可靠地进行对设备 ID 的设定。

根据本发明的第十四方面，可以根据使用上述蜂窝移动站的个人的命令生成上述设备 ID 并将其赋予给上述设备，并且在组管理服务器的存储单元对设备 ID 进行设定或更新。从而能够使用用户独自的设备 ID 体
10 系。

根据本发明的第十五方面，存储单元可以把属性设成设备的主要用途，并且能够对应地保存与上述主要用途对应的业务优先级。从而，能够自动设定与设备的用途相对应的合理的优先级，能够确保稳定的 QoS（服务质量）。

15 根据本发明的第十六方面，可以根据来自上述蜂窝移动站的请求暂时改变上述业务优先级，并且把该变更通知给其它设备。从而，当用户对组管理服务器自动设定的优先级不满意时，能够确保与用户要求对应的通信环境。

根据本发明的第十七方面，可以把上述设备所安装的两个以上的无线局域网接口的使用频率设定为普通业务用和优先业务专用以防止重
20 叠。从而，可以防止干扰，稳定地确保优先业务的 QoS。

根据本发明的第十八方面，可以在每次向设备发布内容时，根据上述主要用途在指定的组内选择最合适的设备进行发布。从而，无需个别地指定发布目的地的设备，而只需要指定组并请求内容就能够接受提供
25 的服务，提高了便利性。

根据本发明的第十九方面，可以具备根据存储区域的利用大小、利用时间、接入次数、接入时间、取得信息大小中的任一项来计算使用费用的单元。从而，能够防止不必要的接入，并且能够减轻组管理服务器的负担。

本发明的安全组管理系统中，由于仅通过属于规定组的成员所使用

的预先登记的蜂窝移动站来向设备提供组信息，因此能够防止怀有恶意的第三者的冒充，并在属于规定组的设备之间进行安全的相互连接或资源共享。

5 附图说明

图 1 为本发明的第一实施方式的安全组管理系统的结构图。

图 2 为表示组 ID 和个人 ID 的设定示例的图。

图 3 为表示服务器接入用 QR 码的分发示例的图。

图 4 为表示蜂窝移动站 ID 的设定示例的图。

10 图 5 为表示组信息的取得示例的图。

图 6 为表示根据组信息在个人计算机之间进行聊天的示例的图。

图 7 为表示使用设备构建家庭内网状网络的示例的图。

图 8 为本发明的第二实施方式所涉及的安全组管理系统的结构图。

图 9 为表示蜂窝移动站 ID 的登记示例的图。

15 图 10 为表示使用设备构建家庭内网状网络的示例的图。

图 11 为表示组管理服务器中的设备的优先级设定和提供给设备的设备一览的示例的图（之一）。

图 12 为表示组管理服务器中的设备的优先级设定和提供给设备的设备一览的示例的图（之二）。

20 图 13 为表示组管理服务器中的设备的优先级设定和提供给设备的设备一览的示例的图（之三）。

图 14 为表示内容发布的示例的图。

标号说明

1：组管理服务器；11：第 1 存储部；12：第 2 存储部；13：第 3 存储部；14：组 ID/个人 ID/组信息设定/更新部；15：蜂窝移动站 ID 设定/更新部；16：组信息提供部；17：使用费用计算部；18：存储部；19：设备 ID/属性设定/更新部；2：蜂窝移动站；21：蜂窝移动站 ID 设定/更新部；22：组信息请求部；23：组信息传送部；24：设备 ID/属性设定/更新部；3：设备；31：组信息接收部；32：组信息接受按钮；33：组

25

内相互连接/资源共享部；34：设备 ID/属性应答/接收部。

具体实施方式

下面，参照附图，对本发明的优选实施方式进行说明。

- 5 图 1 为本发明的第一实施方式的安全组管理系统的结构图。在图 1 中，安全组管理系统具有管理组信息的组管理服务器 1、属于组的成员所使用的蜂窝移动站 2、在组内进行相互连接或资源共享的设备 3。

组管理服务器 1 具有：第 1 存储部 11，其把用于标识组的组 ID 和用于对属于规定组进行识别的组信息对应地保存；第 2 存储部 12，其把用于标识属于组的个人的个人 ID 和组 ID 对应地保存；第 3 存储部 13，其
10 把个人 ID 和用于标识蜂窝移动站的蜂窝移动站 ID 对应地保存。并且，还具备：组 ID/个人 ID/组信息设定/更新部 14，其根据管理人员等的指示，设定/更新第 1 存储部 11、第 2 存储部 12、第 3 存储部 13 的组 ID、个人 ID、组信息；蜂窝移动站 ID 设定/更新部 15，其响应于来自蜂窝移
15 动站 2 的请求，在第 3 存储部 13 中设定/更新蜂窝移动站 ID；组信息提供部 16，其仅仅响应于来自登记在第 3 存储部 13 中的规定蜂窝移动站 2 的请求而提供组信息；使用费用计算部 17，其根据存储区域的利用大小、利用时间、接入次数、接入时间、取得信息大小中的任一项来计算使用费用。

- 20 蜂窝移动站 2 具有：蜂窝移动站 ID 设定/更新部 21，其向组管理服务器 1 请求设定/更新自己的蜂窝移动站 ID；组信息请求部 22，其向组管理服务器 1 请求提供组信息；组信息传送部 23，其把从组管理服务器 1 提供的接受组信息传送（提供）给设备 3。

设备 3 具有：组信息接收部 31，其从蜂窝移动站 2 接收组信息；组
25 信息接受按钮 32，其由为了防止因蜂窝移动站 2 的误操作而引起组信息的接收故限定在被按下后的一定时间段内方可接收组信息的硬件按钮构成；组内相互连接/资源共享部 33，其通过根据由蜂窝移动站 2 提供的组信息来判断是否属于同一组内，进行设备间的安全的相互连接或资源共享。

下面,根据图 2 至图 6,说明属于大学的规定研究课程(组)的学生(成员)之间通过把自己的个人计算机(设备)相互连接以通过聊天而进行信息交换的情况。

图 2 为表示组 ID 和个人 ID 的设定示例的图,大学教务处的 A 老师
5 在组管理服务器 1 的第 3 存储部 13 中制作学号一览表,并且根据学生提交的选修科目报告在第 2 存储部 12 中制作每一研究课程名称(科目)的选修者的学号表。

其次,如图 3 所示,在组管理服务器 1 中,针对第 3 存储部 13 的每一个学号自动生成密码,打印包含学号、密码和组管理服务器 1 的地址
10 的 QR 码, A 老师把 QR 码分发给学生 B、C、...。

如图 4 所示,接收了 QR 码的学生 B 使用自己的蜂窝移动站 2B 配备的 QR 码读取器来将 QR 码读入蜂窝移动站 2B,并根据包含在 QR 码中的地址,通过基于 SSL 客户认证的加密通信而连接到组管理服务器 1 (步骤 S11)。这时,在组管理服务器 1 中取得蜂窝移动站 2B 的公钥(步骤 S12)。

其次,从蜂窝移动站 2B 向组管理服务器 1 发送包含在 QR 码中的学号
15 和密码(步骤 S13)。在组管理服务器 1 中,根据第 3 存储部 13 的登记信息确认学号和密码的一致(步骤 S14、S15),在得到确认的情况下,把蜂窝移动站 2B 的公钥 K_b 与学号对应地存储在第 3 存储部 13 中(步骤 S16)。同样,学生 C 也向组管理服务器 1 登记自己的蜂窝移动站的公钥 K_c 。

然后,在选修相同研究课程“线性代数 II”的学生 B 和 C 通过文本
20 聊天来交换与研究论文有关的信息的情况下,如图 5 所示,学生 B 利用自己的蜂窝移动站 2B,通过基于 SSL 客户认证的加密通信而连接到组管理服务器 1 (步骤 S21),请求生成个人计算机用的密钥(步骤 S22)。

组管理服务器 1 利用在进行基于 SSL 客户认证的加密通信时所取得
25 的蜂窝移动站 2B 的公钥 K_b ,从第 3 存储部 13 确定学号“1234567”,根据该学号通过第 2 存储部 12 确认对研究课程名称“线性代数 II”的选修(步骤 S23)。并且,根据研究课程名称,通过第 1 存储部 11 取得分配给每一个研究课程名称的私钥/公钥对,根据该私钥/公钥对生成个人计算机用的私钥/公钥,并且生成利用预先分配给该研究课程的私钥进行了签

名并包括与该私钥成对的公钥的电子证书（Certification）并将其发送给蜂窝移动站 2B（步骤 S24）。

在蜂窝移动站 2B 中，将从组管理服务器 1 取得的个人计算机用私钥/公钥和电子证书按近距离无线方式发送给个人计算机 3B 并进行设定（步骤 S25）。以后，个人计算机 3B 将信赖该电子证书。同样，学生 C 也从组管理服务器 1 取得个人计算机用的私钥/公钥和电子证书并设定在自己的个人计算机上，并且信赖电子证书。

然后，如图 6 所示，学生 B 和学生 C 试着通过网络将个人计算机 3B 和 3C 相互连接，并且进行公钥方式的相互认证（步骤 S31）。由于两者都已经信赖从组管理服务器 1 取得的电子证书，因此认证成功（步骤 S32），可以交换聊天用的对话密钥以进行私密性高的安全的加密通信（步骤 S33）。

其次，图 7 为表示利用设备构建家庭内网状网络的示例的图。

首先，作为“田中家”家长的“田中一郎”D 通过书件的邮寄等方式向组管理服务器 1 的运营商请求“田中家”的组登记。登记内容包括：

- “田中一郎”D 所拥有的蜂窝移动站 2D 的公钥；
- “田中花子”E 所拥有的蜂窝移动站 2E 的公钥；
- “田中顺”F 所拥有的蜂窝移动站 2F 的公钥。

这些都通过组管理服务器 1 的运营商登记在第 1 存储部 11 等中。

组管理服务器 1 的运营商针对组“田中家”，生成作为在同一组使用的对等密钥的 WEP（Wired Equivalent Privacy，有线对等保密）密钥和 SSID（Service Set Identifier，服务集标识符），并将其登记在第 1 存储部 11 等中。之后，组管理服务器 1 只对来自“田中一郎”D 所拥有的蜂窝移动站 2D、“田中花子”E 所拥有的蜂窝移动站 2E、“田中顺”F 所拥有的蜂窝移动站 2F 的接入发布作为组信息的 WEP 密钥和 SSID。

当“田中一郎”D 购买电视机 3#1 和网络接入点功能的内置型 AV 服务器 3#2 作为设备并将其设置在起居室等中的情况下，“田中一郎”D 利用自己的蜂窝移动站 2D，通过基于 SSL 客户认证的加密通信与组管理服务器 1 连接（步骤 S41）。由于“田中一郎”D 的蜂窝移动站 2D 的公钥

作为“田中家”的成员登记在组管理服务器 1 中，因此从组管理服务器 1 把组“田中家”的 WEP 密钥“tanaka1234567”和 SSID“tanaka_family”发布给蜂窝移动站 2D。

“田中一郎”D 以近距离无线方式把发布的 WEP 密钥和 SSID 安装在电视机 3#1 和 AV 服务器 3#2，从而，电视机 3#1 和 AV 服务器 3#2 共享 WEP 密钥和 SSID，由此能够进行加密的安全通信。

日后，当“田中顺”F 购买游戏机 3#3 并把该游戏机连接到家庭内网状网络的情况下，其利用自己的蜂窝移动站 2F 通过基于 SSL 客户认证的加密通信与组管理服务器 1 连接（步骤 S42）。由于“田中顺”F 的蜂窝移动站 2F 的公钥作为“田中家”的成员登记在组管理服务器 1 中，因此从组管理服务器 1 把组“田中家”的 WEP 密钥“tanaka1234567”和 SSID“tanaka_family”发布给蜂窝移动站 2F。

“田中顺”F 以近距离无线方式把发布的 WEP 密钥和 SSID 安装在游戏机 3#3，从而，游戏机 3#3 与电视机 3#1 和 AV 服务器 3#2 共享 WEP 密钥和 SSID，由此能够进行加密的安全通信，能够把电视机 3#1 用作监视器来玩游戏。

日后，当“田中花子”E 购买了内置有通信功能的冰箱的情况下，同样，可以把冰箱连接到家庭内网状网络上。

然后，图 8 为本发明的第二实施方式所涉及的安全组管理系统的结构图，该系统能够确保设备间通信的 QoS。

在图 8 中，在组管理服务器 1 中新设置有：存储部 18，其保存用于标识设备的设备 ID、该设备的属性（主要用途、优先级等）和蜂窝移动站 ID；设备 ID/属性设定/更新部 19，其对上述存储部 18 中的设备 ID 和属性进行设定/更新。其它结构与图 1 所示的结构相同。

在蜂窝移动站 2 新设置有设备 ID/属性设定/更新部 24，该设备 ID/属性设定/更新部 24 从设备 3 取得设备 ID 和属性并对组管理服务器 1 进行设定/更新，或者自己生成设备 ID 并对组管理服务器 1 和设备 3 进行设定/更新。此外，设备 ID/属性设定/更新部 24 也具有如下功能：对设备 3 暂时改变在属性中所包含的优先级并通知给其它设备 3。其它结构与

图 1 所示的结构相同。

在设备 3 中，新设置有设备 ID/属性应答/接收部 34，在蜂窝移动站 2 进行了请求的情况下该设备 ID/属性应答/接收部 34 把自己的设备 ID 和属性作为应答，并且还接收由蜂窝移动站 2 生成并通知的设备 ID。并且，设备 ID/属性应答/接收部 34 还具有接收由蜂窝移动站 2 暂时改变的属性的功能。其它结构与图 1 所示的结构相同。此外，当通过组内相互连接/资源共享部 33 在多个设备 3 之间进行相互连接或资源共享时，在设备 3 安装有两个以上的无线局域网接口的情况下，优选把它们分成普通业务用和优先业务专用，并且将使用频率设定为不重叠。

下面，根据图 9 至图 13，对利用设备来构建家庭内网状网络的情况的示例进行说明。

在图 9 中，在组管理服务器 1 的存储部 18 中，登记有称作“田中家”的组，存储有“田中一郎”D 所拥有的蜂窝移动站 2D、“田中花子”E 所拥有的蜂窝移动站 2E、“田中顺”F 所拥有的蜂窝移动站 2F 作为能够获取/改变组信息的蜂窝移动站。

当“田中一郎”D 购买电视机 3#1 和具有无线局域网网格功能内置的网关（GW）功能的家庭服务器 3#2 作为设备并将其配置在“田中家”中的情况下，如图 10 所示，通过下面步骤构建家庭内网状网络。

- 把电视机 3#1 和家庭服务器 3#2 登记到组管理服务器 1（步骤 S51 至 S55）

- 利用蜂窝移动站 2D 从组管理服务器 1 取得设备一览（步骤 S56）
- 把设备一览安装到电视机 3#1 和家庭服务器 3#2（步骤 S57、S58）

- 开始电视机 3#1 和家庭服务器 3#2 之间的通信（步骤 S59）

日后，当“田中顺”F 购买了与无线局域网网格对应的游戏机 3#3 的情况下，如同上述，可以按下面的步骤连接游戏机 3#3 和电视机 3#1。

- 把游戏机 3#3 登记到组管理服务器 1
- 利用蜂窝移动站 2F 从组管理服务器 1 取得设备一览
- 把设备一览安装到游戏机 3#3

- 开始通信

此外，“田中一郎”D 以与上述相同的步骤在自己的房间里拥有与无线局域网网格对应的个人计算机 3#4，并且通过该个人计算机 3#4 检查积存在家庭服务器 3#2 中的邮件。

5 现在，如图 11 所示，在设备一览中存在电视机 3#1、家庭服务器 3#2、游戏机 3#3、个人计算机 3#4，对于对延迟值要求严格的游戏机 3#3 和接收动态图像的电视机 3#1，在组管理服务器 1 中设定高优先级“1”。通过蜂窝移动站把带有优先级的设备一览分发给各个设备，从而各设备共享接入类别。

10 这里，考虑“田中顺”F 的游戏通信和“田中一郎”D 的邮件接收同时发生的情况。在这里产生的业务主要有以下两种。

- 发送源为游戏机 3#3、目的地为电视机 3#1 的第 1 业务
- 发送源为家庭服务器 3#2、目的地为个人计算机 3#4 的第 2 业务

15 这里，由于第 1 业务的发送源和目的地均为接入类别“1”，因此与该业务有关的分组被确定为接入类别“1”，并且，由于第 2 业务的发送源和目的地均为接入类别“2”，因此与该业务有关的分组被确定为接入类别“2”，分别进行发送。假定在发送源接入类别与目的地接入类别不一致的情况，采用优先级高（数值小）的接入类别。

20 由此，由于第 1 业务优先于第 2 业务，因此对延迟值要求严格的游戏通信不会发生障碍。

其次，如图 12 所示，考虑“田中顺”F 观赏家庭服务器 3#2 的电影、同时“田中一郎”D 用个人计算机 3#4 上网冲浪的情况。

这里，主要有两种业务。

- 25
- 发送源为家庭服务器 3#2、目的地为电视机 3#1 的第 3 业务
 - 发送源为家庭服务器 3#2、目的地为个人计算机 3#4 的第 4 业务

第 3 业务的发送源接入类别为“2”，目的地接入类别为“1”，在该情况下，确定赋予第 3 业务的接入类别为“1”。由于第 4 业务的发送源

和目的地均为接入类别“2”，因此与该业务有关的分组被确定为接入类别“2”。

但是，由于电影需要大量的业务收发，因此以两个业务之间的接入类别数值的差为“1”的程度无法确保电影的足够的画面质量。每次在个人计算机 3#4 上显示新的 Web 页时，电影就不稳定，使“田中顺”F 感到烦恼。

在该情况下，如图 13 所示，“田中顺”F 利用自己的蜂窝移动站 2F 通过近距离无线通信对电视机 3#1 指示暂时把接入类别从“1”改变为“0”。电视机 3#1 通过无线局域网的信标信号（beacon signal）把接入类别已改变的新设备一览表通知给各设备。

其结果，第 3 业务的发送源接入类别为“2”，而目的地接入类别成为“0”，在该情况下，确定赋予第 3 业务的接入类别为“0”。此外，第 4 业务的接入类别依然是“2”。

结果，如图 13 所示，即使在发生了“田中一郎”的 Web 业务的情况下，接入类别的数值差成为“2”，成为使电影业务足够优先的数值差。从而，电影不稳定的情况减少，“田中顺”F 能够在令人满意的画面质量下欣赏电影。

接着，根据图 14，对内容发布的示例进行说明。

图 14 中，“高桥”君 G 用与无线局域网网格对应的网关（GW）3#11、电视机 3#12、HD 刻录器 3#13、带 HDD 的立体音响 3#14、冰箱 3#15 来构建家庭网络，假设在组管理服务器 1 的存储部 18 中有如图所示的设备一览表。

这里，“高桥”君 G 想听歌手 #2 的曲名 #2，就利用自己的蜂窝移动站 2G 请求组管理服务器 1 发布该曲的内容。这样，组管理服务器 1 判定该内容为音乐，从组内检索最适合作为再现音乐的设备的立体音响 3#14，并向其进行发布。

并且，在另一天，在“高桥”君 G 请求发布料理烹调法的情况下，组管理服务器 1 从组内检索最适合作为使用料理烹调法的设备的冰箱 3#15，并向其进行发布。

以上，通过本发明的最佳实施方式说明了本发明。这里给出了特定的具体示例来说明本发明，但在不脱离在权利要求范围内所定义的本发明的广泛的宗旨和范围的情况下，可以对这些具体示例进行各种修改和变化，这是显然的。即，不能解释为利用详细的具体例和附图来对本发明进行限定。

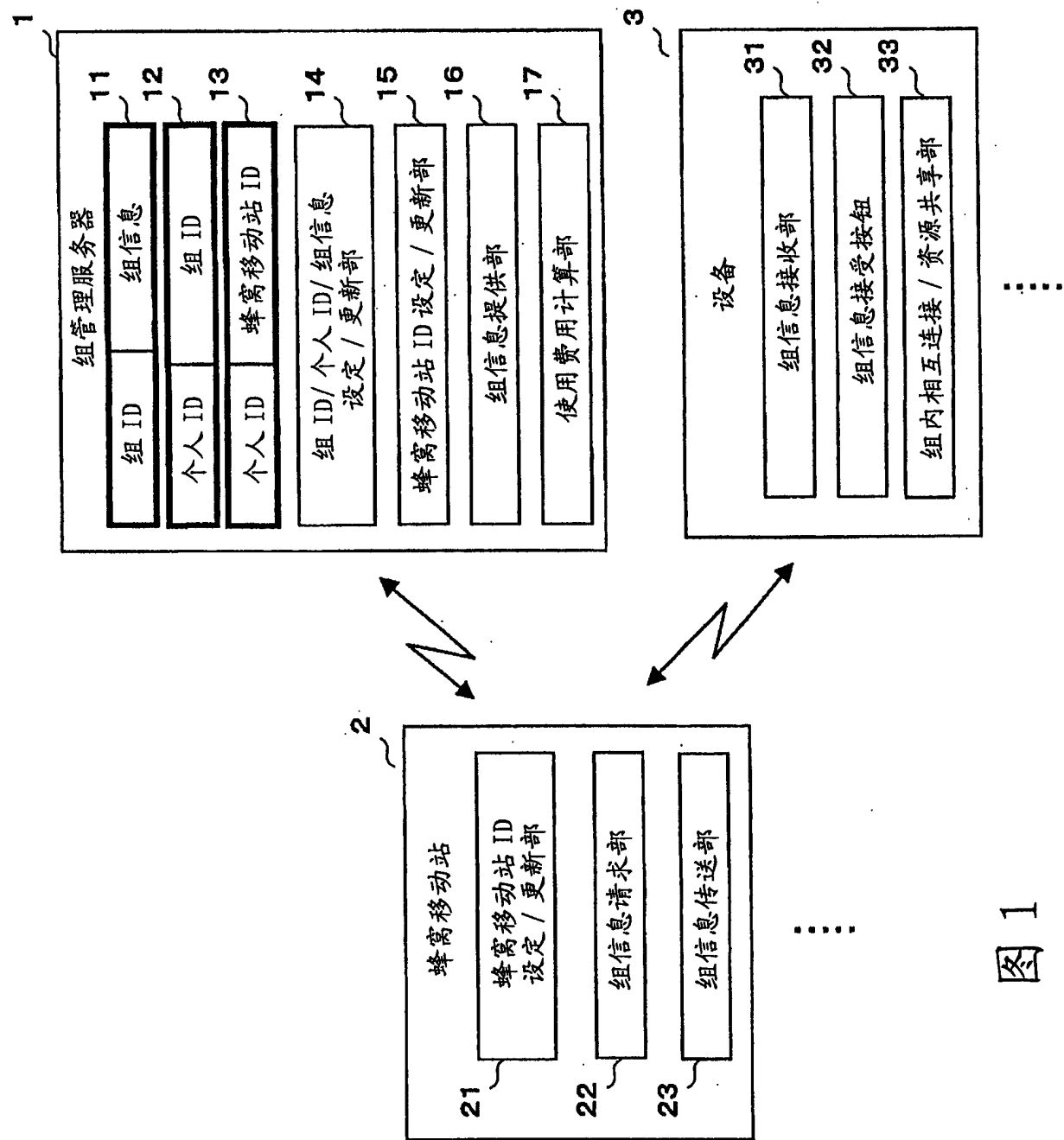


图 1

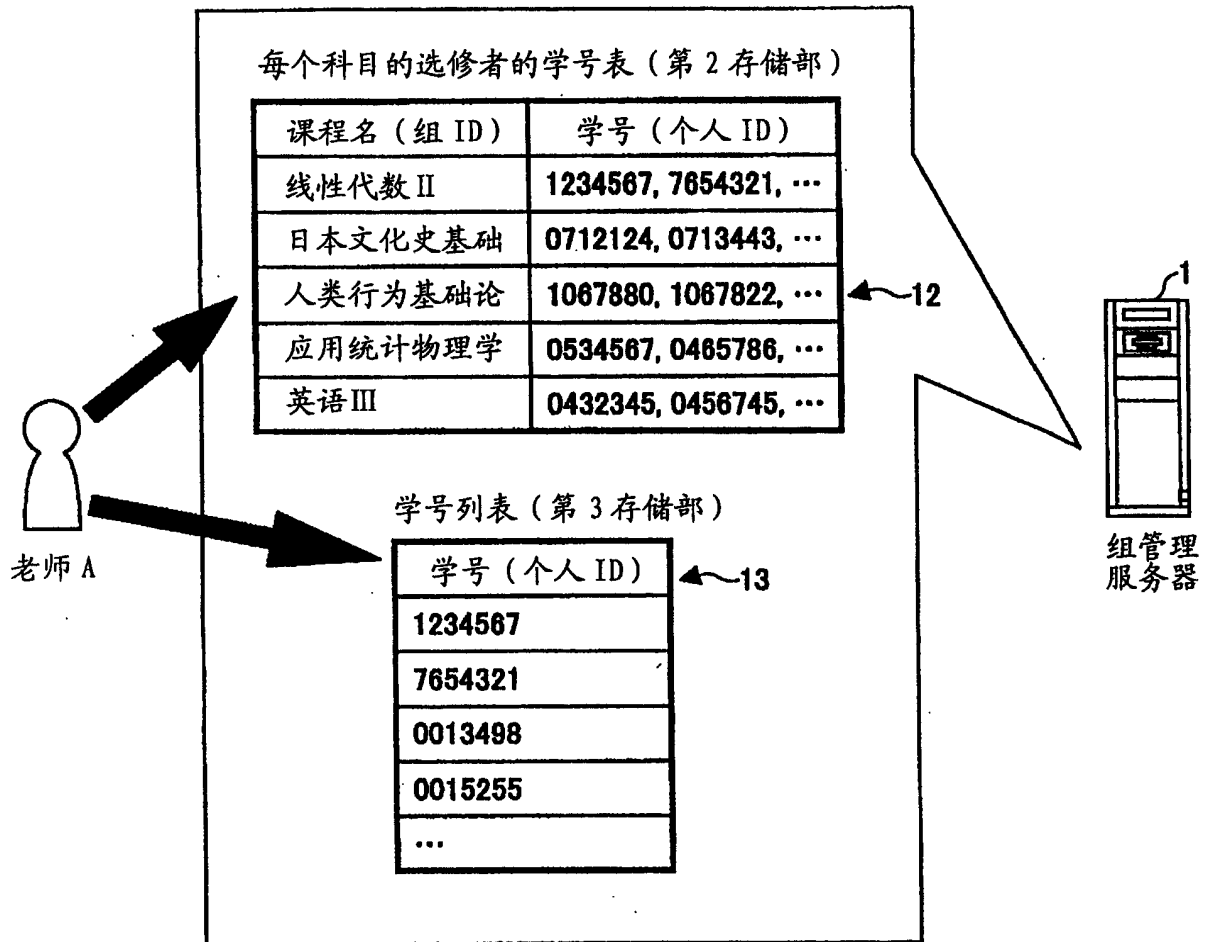


图 2

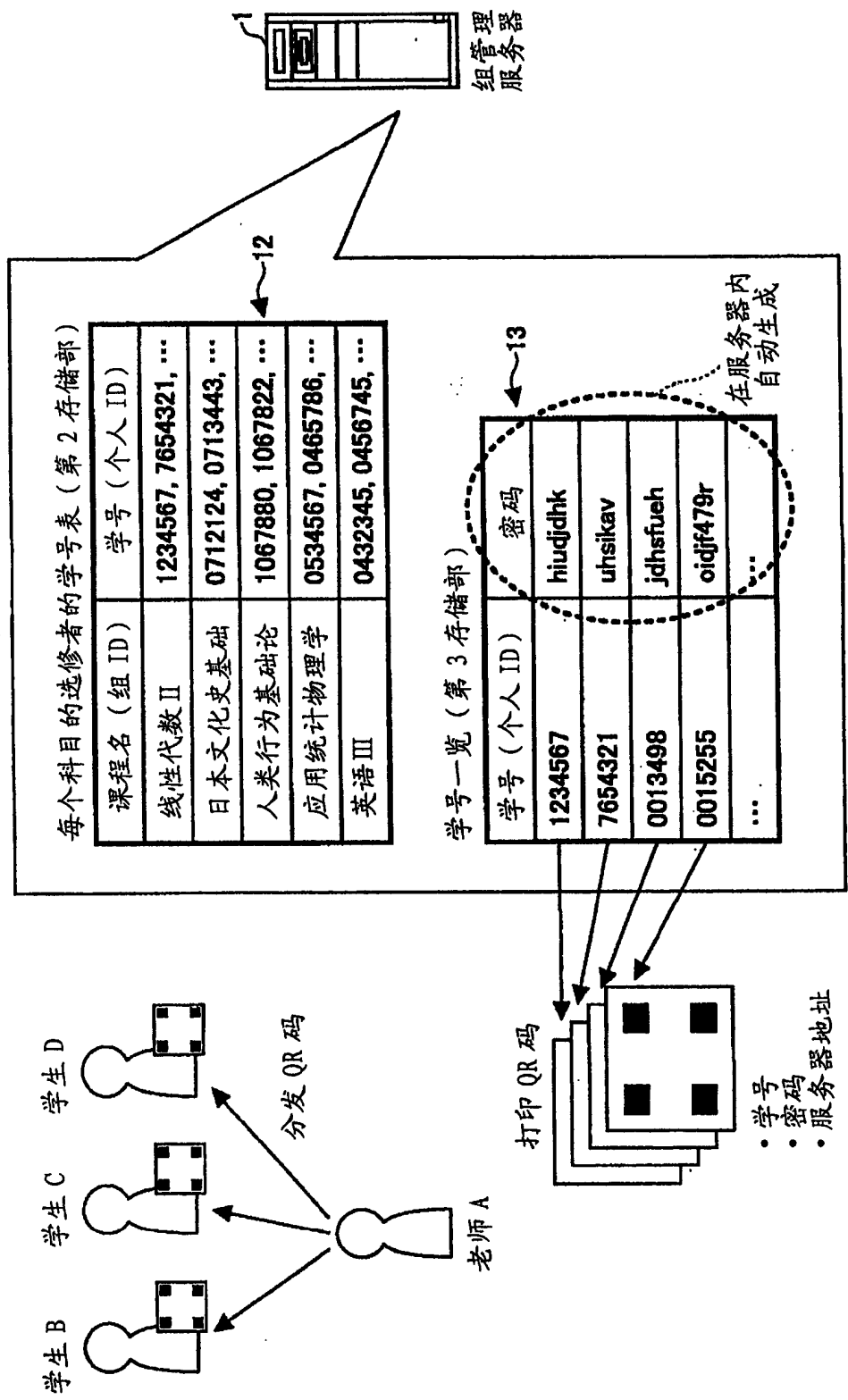


图 3

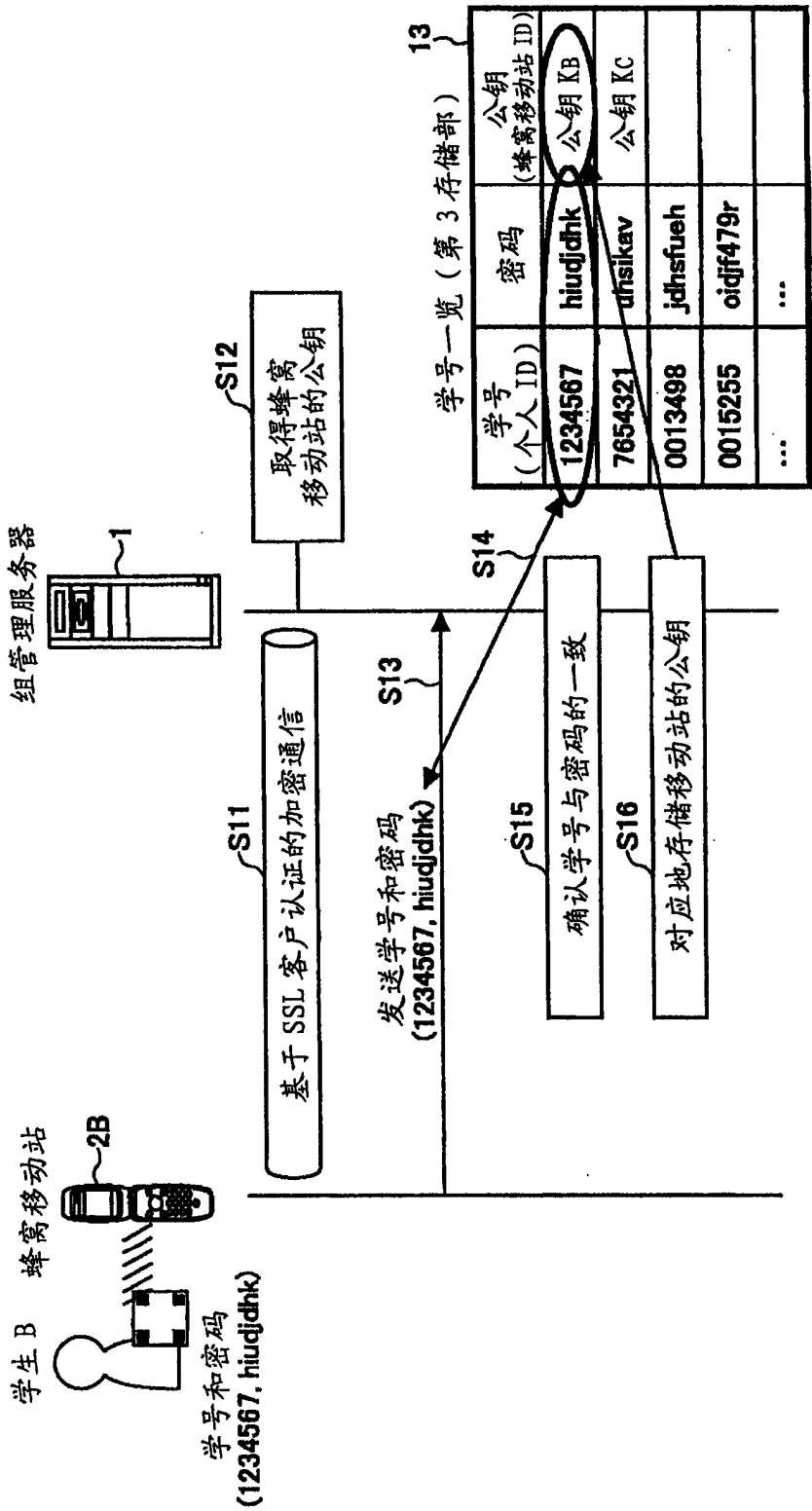


图 4

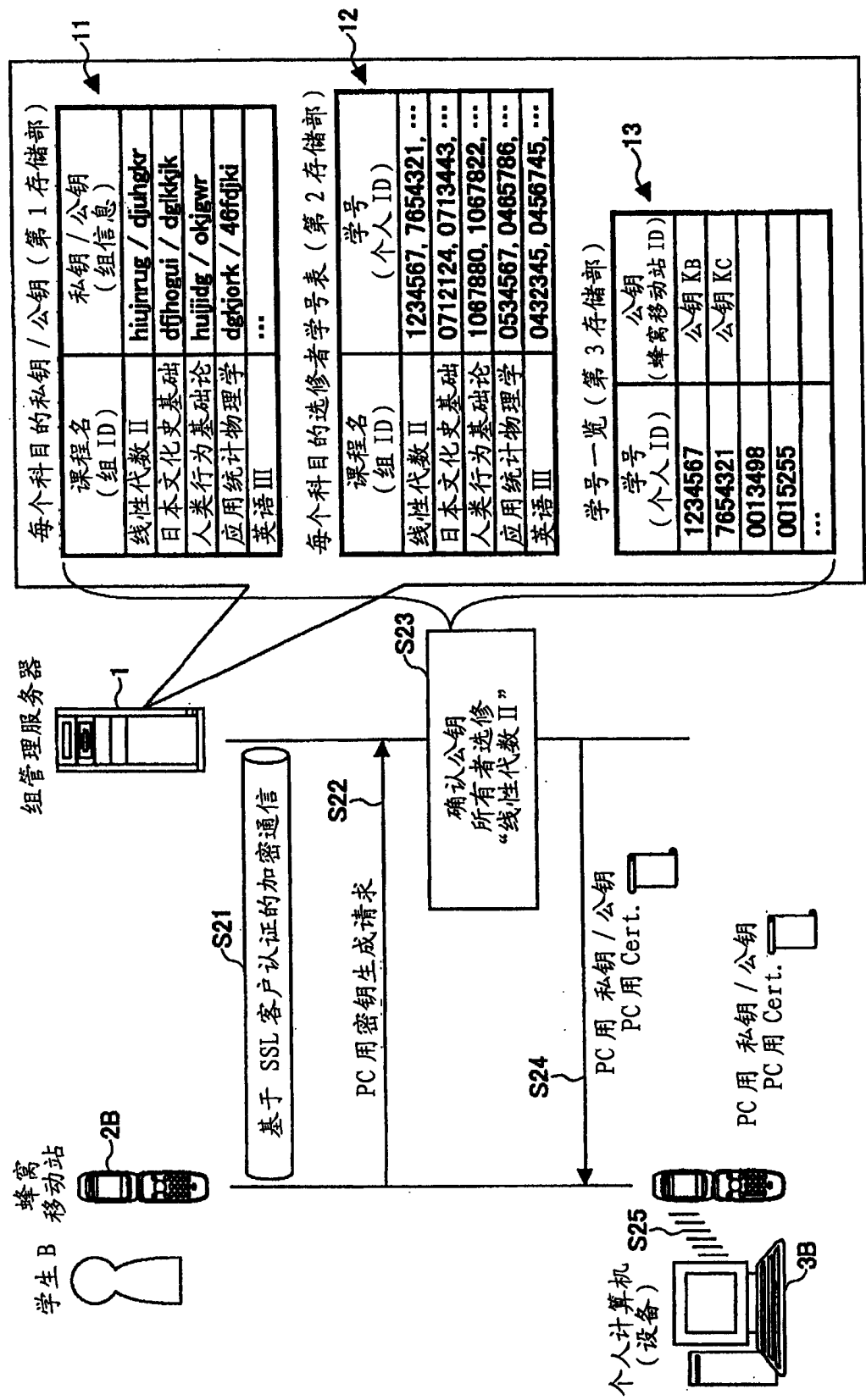


图 5

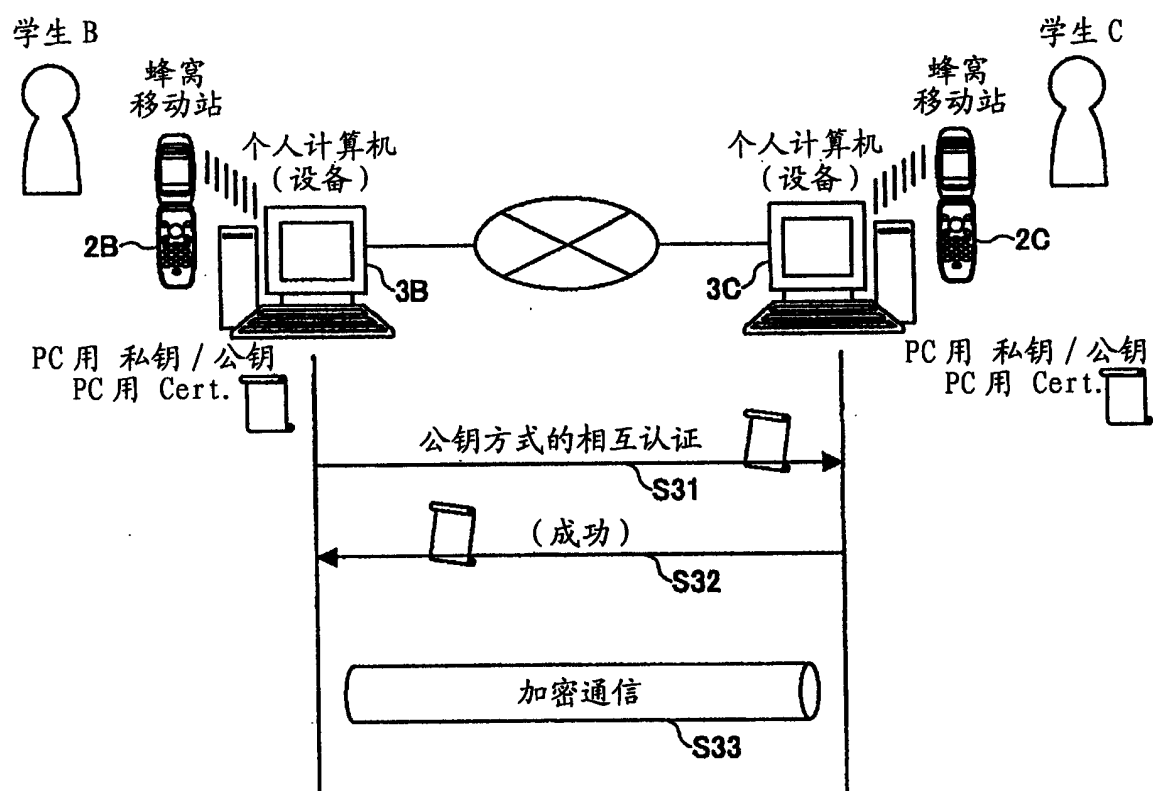
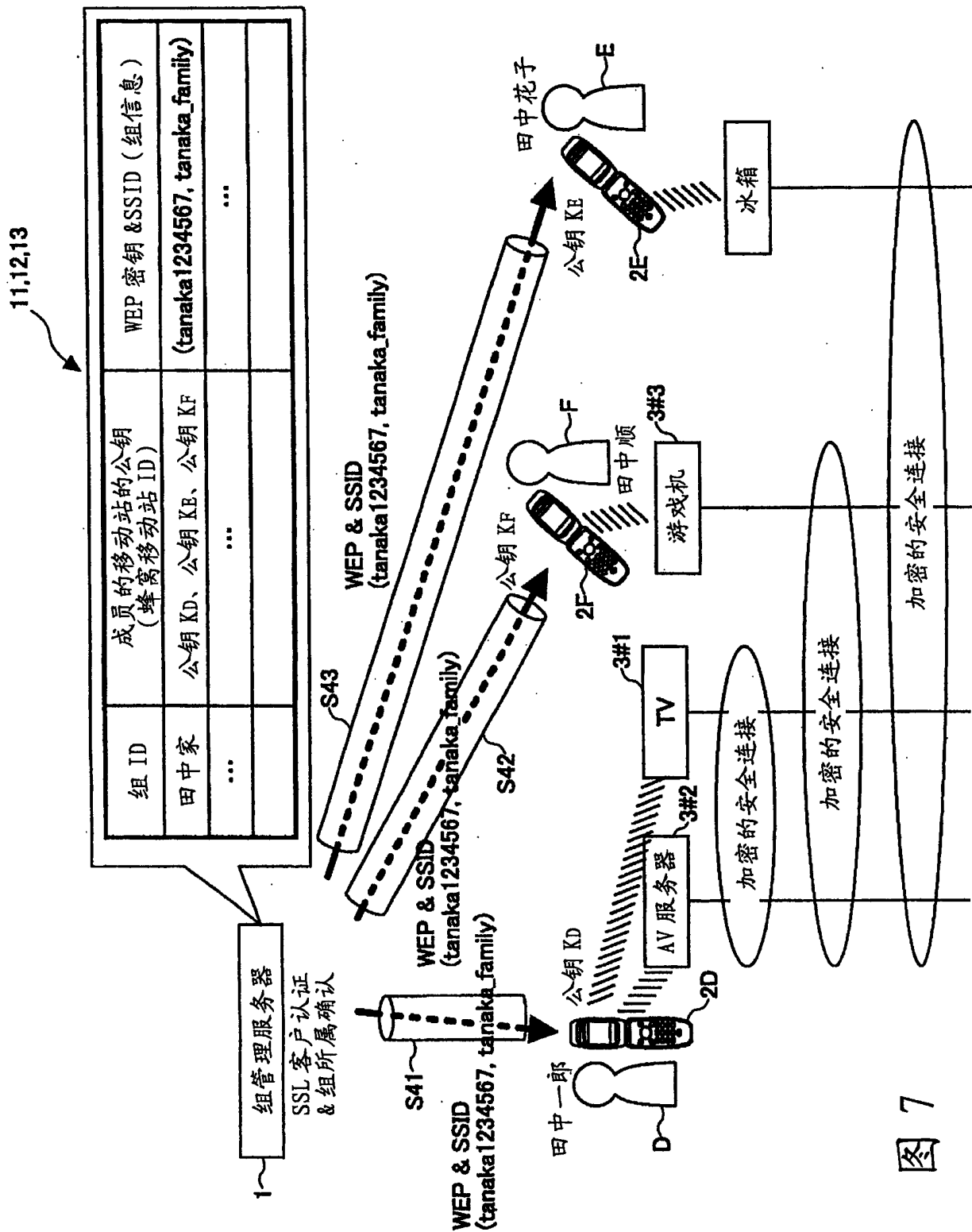


图 6



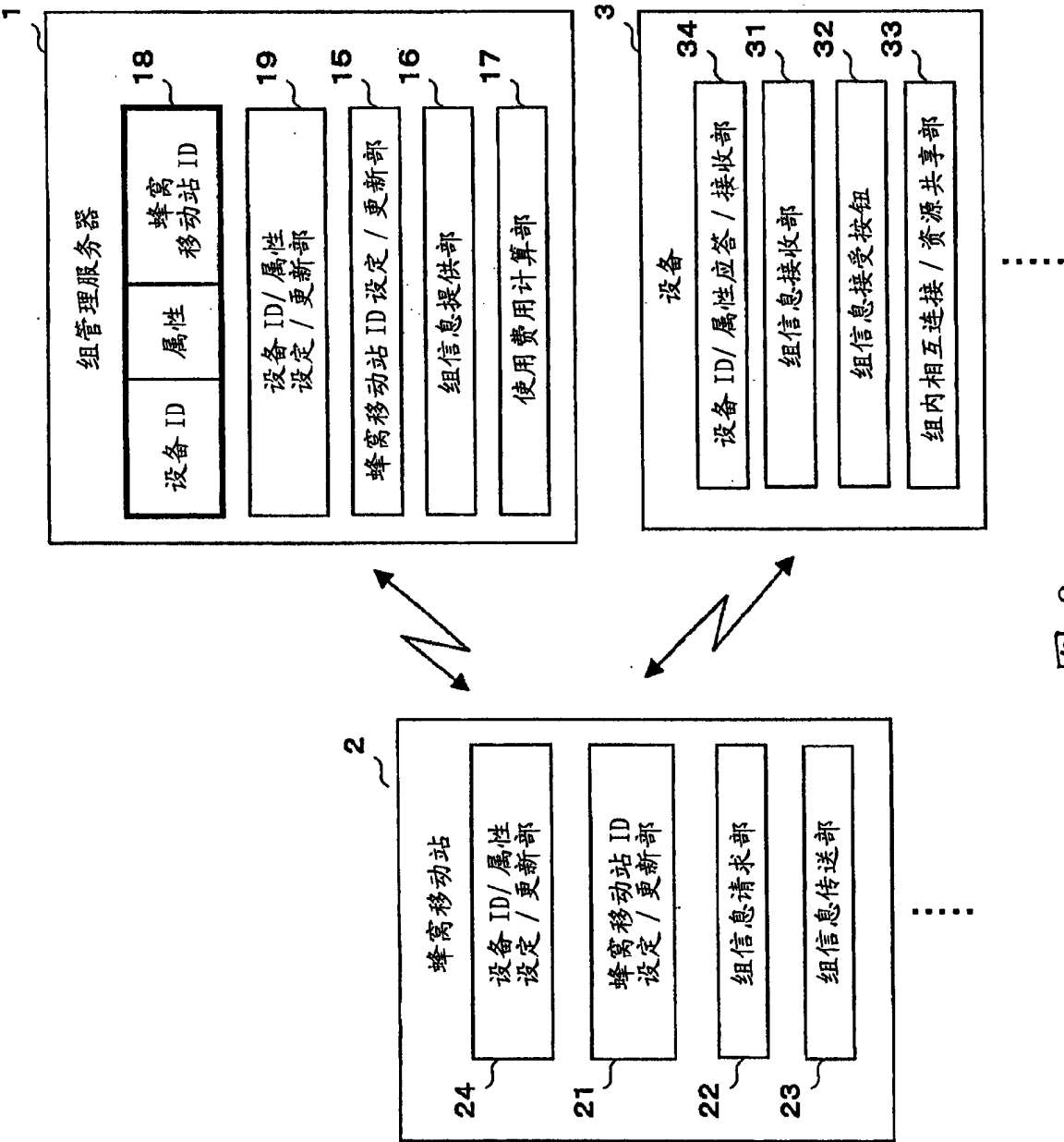
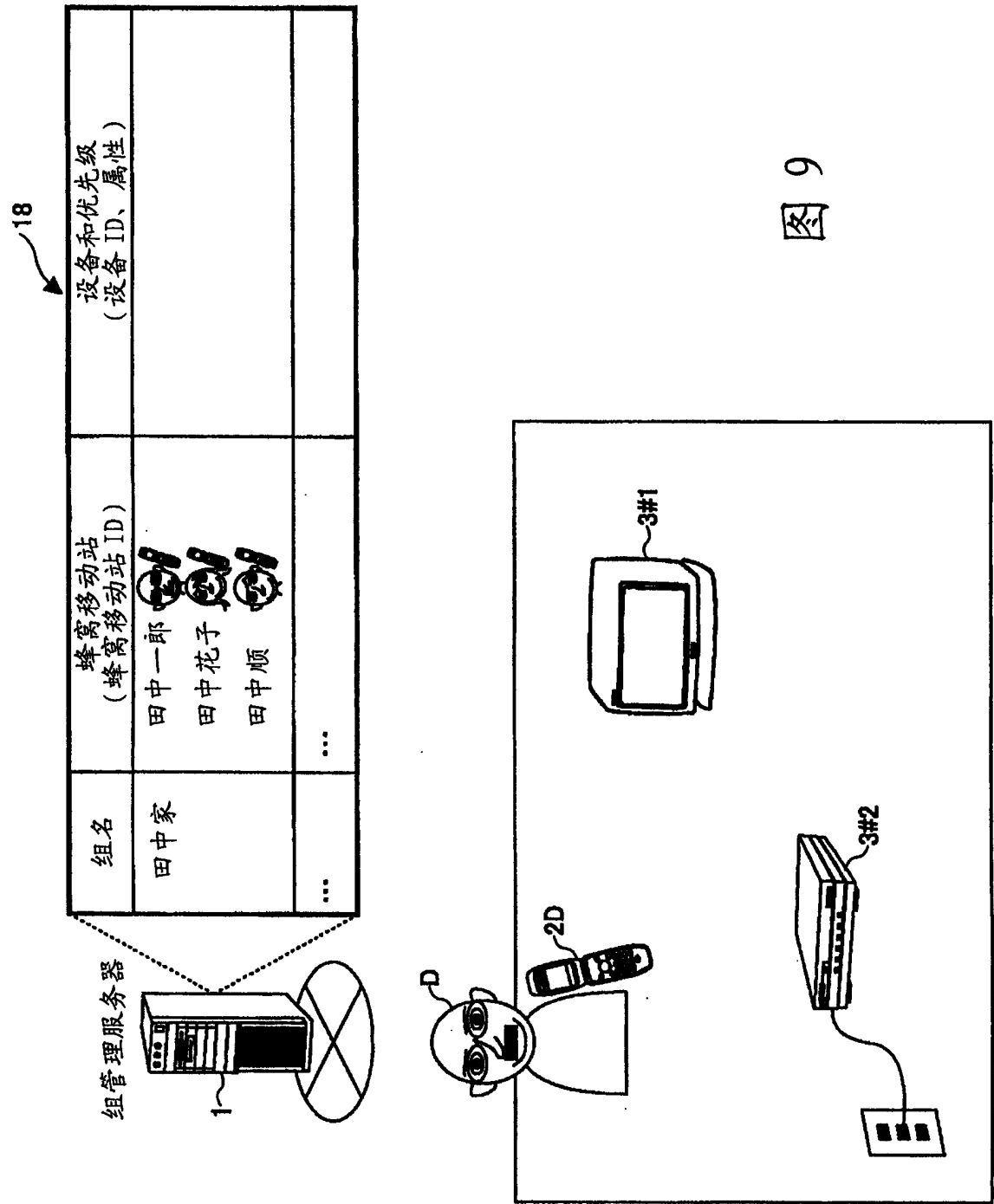


图8



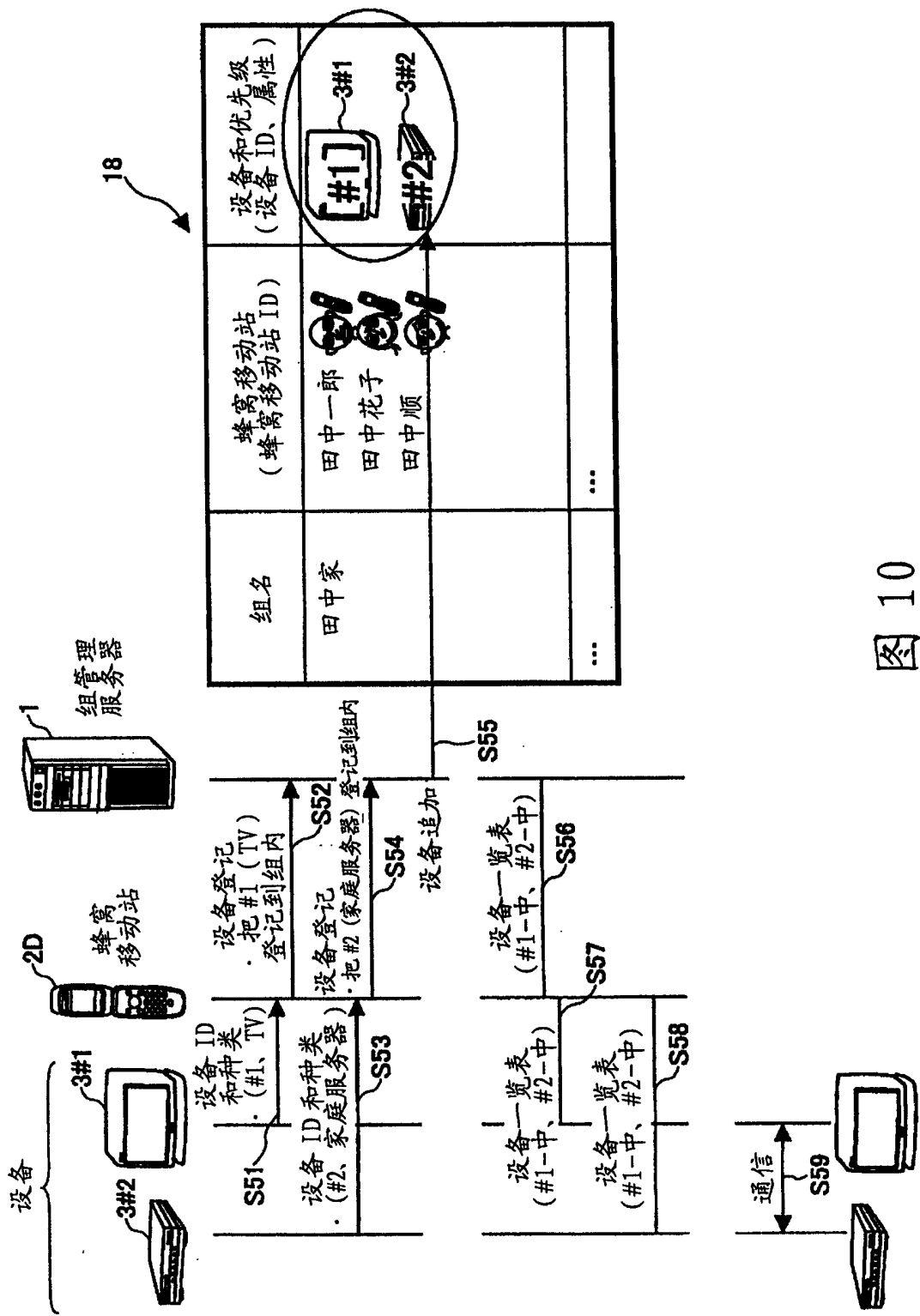


图 10

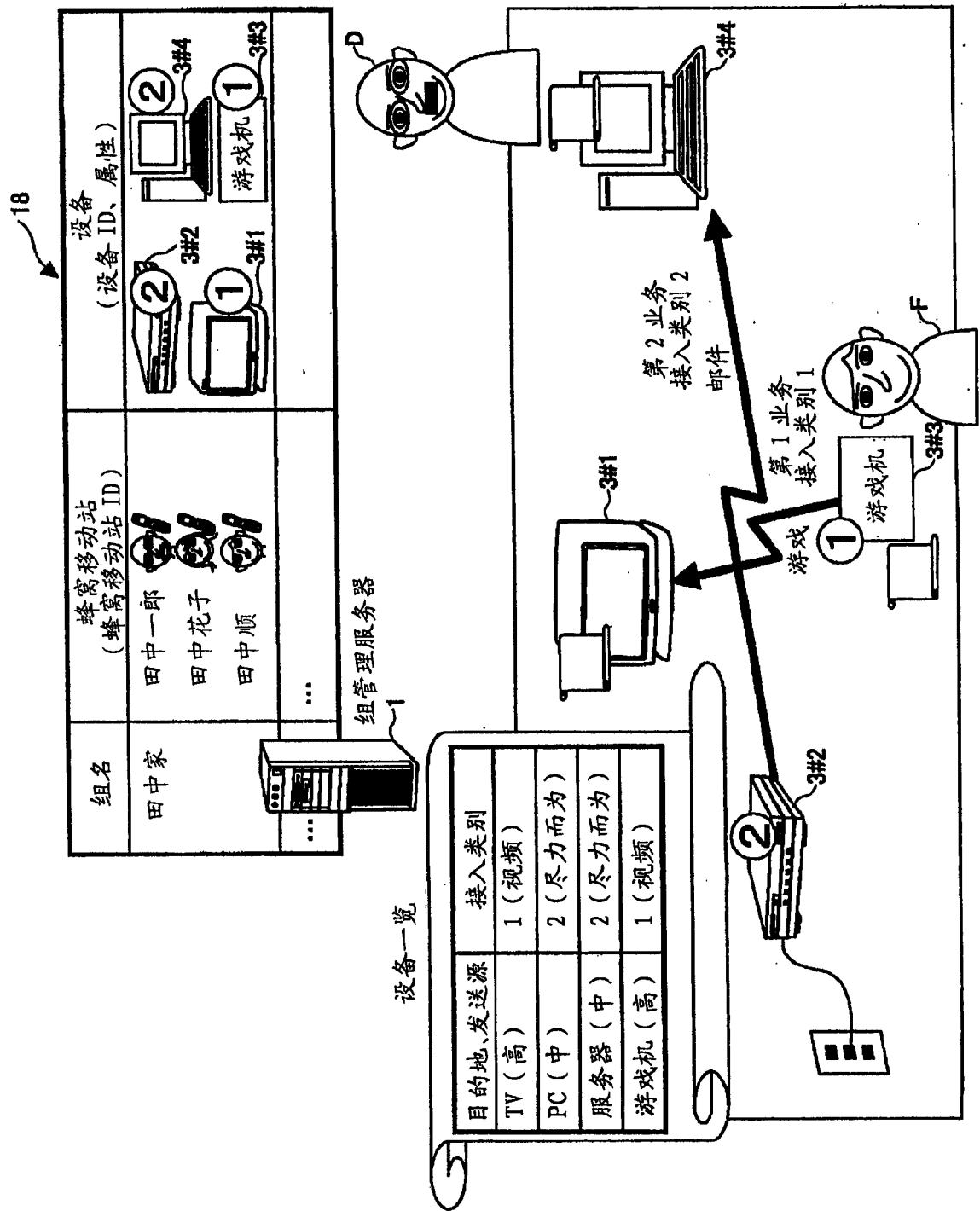


图 11

