[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 15/00 (2006.01)

[12] 发明专利申请公开说明书

[21] 申请号 200480022341.3

[43] 公开日 2006 年 9 月 13 日

[11] 公开号 CN 1833234A

[22] 申请日 2004.8.4
[21] 申请号 200480022341.3
[30] 优先权
[32] 2003. 8. 8 [33] JP [31] 290053/2003
[86] 国际申请 PCT/JP2004/011160 2004.8.4
[87] 国际公布 WO2005/015417 日 2005.2.17
[85] 进入国家阶段日期 2006.2.5
[71] 申请人 索尼株式会社
地址 日本东京
[72] 发明人 大森睦弘 角田智弘 岛田繁广

[74] 专利代理机构 上海专利商标事务所有限公司
代理人 钱慰民

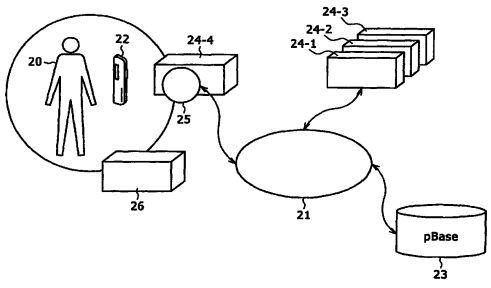
权利要求书 5 页 说明书 50 页 附图 58 页
按照条约第 19 条的修改 1 页

[54] 发明名称

信息处理设备和方法、程序以及记录媒体

[57] 摘要

有可能提供一种不使用户担心且令人愉快的对用户友好的服务。 当把 PMD 作为个人信息存储在用户(20)处的 PK(22)首次与服务系统(24)相互通信并使用该服务系统(24)时，它存储着该服务系统(24)的服务 ID 以及防电子欺骗方法。 当 PK(22)第二次和以后再与服务系统(24)通信时，在向服务系统(24)提供 PMD 之前先在彼此之间执行防电子欺骗处理。 根据用户(20)的预设访问准许信息，由服务系统(24)来执行对 PMD 的读出或修改。 本发明可以应用于 PDA。



1.一种用于存储与用户有关的用户信息并与多个其它的信息处理设备进行通信的信息处理设备，所述信息处理设备包括：

呈现装置，用于呈现要被所述其它信息处理设备读取或改变的用户信息；

指定装置，用于指定准许读取或改变由所述呈现装置呈现的用户信息；

识别装置，用于识别所述其它信息处理设备；以及

存储装置，用于存储由与所述其它信息处理设备相关联的所述识别装置识别出的所述其它信息处理设备所读取或改变的用户信息。

2.如权利要求 1 所述的信息处理设备，其特征在于，所述信息处理设备还包括用于进行准静电场通信、电磁波通信、光通信或电通信的通信装置。

3.如权利要求 1 所述的信息处理设备，其特征在于，

所述信息处理设备外部的设备被用作输入或输出接口。

4. 如权利要求 1 所述的信息处理设备，其特征在于，

当与所述其它信息处理设备进行初次通信时，用于识别所述信息处理设备的信息被发送到所述其它信息处理设备。

5. 如权利要求 1 所述的信息处理设备，其特征在于，

当与所述其它信息处理设备进行初次通信时，产生由所述信息处理设备用来加密信息的第一代码以及与所述第一代码相应产生的第二代码，并且所述第一代码被发送到所述其它信息处理设备，并且

由所述其它信息处理设备用来加密信息的第三代码是通过所述通信装置获得的。

6. 如权利要求 1 所述的信息处理设备，其特征在于，

所述用户信息是基于所述其它信息处理设备所提供的内容使用历史来更新的。

7. 如权利要求 1 所述的信息处理设备，其特征在于，

与用来管理所述用户信息的信息管理设备进行的通信是通过网络来进行的，并且更新所述用户信息使得存储在所述信息处理设备中的用户信息的内容与存储在所述信息管理设备中的用户信息的内容完全一致。

8. 如权利要求 7 所述的信息处理设备，其特征在于，

所述信息管理设备识别被准许读取或改变所述用户信息的所述其它信息处理设备，并通过所述网络将所述用户信息提供给被准许读取或改变所述用户信息的其它信息处理设备。

9. 如权利要求 1 所述的信息处理设备，其特征在于，

所述用户是基于发生在所述用户的身体上的准静电场或静电场的变化模式来被验证的。

10. 如权利要求 1 所述的信息处理设备，其特征在于，

所述用户信息具有用于表示所述用户偏好的偏好信息，以及

所述偏好信息被发送到由所述用户指定的信息设备，并且与所述偏好信息协同操作所述信息设备。

11. 如权利要求 1 所述的信息处理设备，其特征在于，

新的用户信息是基于与多个其它信息处理设备相关联的多条用户信息而创建的。

12.一种信息处理设备的信息处理方法，所述信息处理设备存储着与用户有关的用户信息并与多个其它信息处理设备进行通信，所述信息处理方法包括：

呈现步骤，用于呈现要被所述其它信息处理设备读取或改变的用户信息；

指定步骤，用于指定准许读取或改变由所述呈现步骤的过程呈现的用户信息；

识别步骤，用于识别所述其它信息处理设备；以及

存储步骤，用于存储由与所述其它信息处理设备相关联的所述识别步骤的过程识别出的所述其它信息处理设备来读取或改变的用户信息。

13.一种信息处理设备的程序，所述信息处理设备存储着与用户有关的用户信息并与多个其它的信息处理设备进行通信，所述程序使计算机执行：

呈现控制步骤，用于控制呈现要被所述其它信息处理设备读取或改变的用户信息；

指定控制步骤，用于控制指定准许读取或改变由所述呈现控制步骤的过程所呈现的用户信息；

识别控制步骤，用于控制识别所述其它信息处理设备；以及

存储控制步骤，用于执行控制以便存储由所述其它信息处理设备读取或改变

的用户信息，所述其它信息处理设备是由与所述其它信息处理设备相关联的所述识别控制步骤的过程来识别的。

14.一种在其上记录有信息处理设备的程序的记录媒体，所述信息处理设备存储着与用户有关的用户信息并与多个其它信息处理设备进行通信，所述程序使计算机执行：

呈现控制步骤，用于控制呈现要被所述其它信息处理设备读取或改变的用户信息；

指定控制步骤，用于控制指定准许读取或改变由所述呈现控制步骤的过程所呈现的用户信息；

识别控制步骤，用于控制识别所述其它信息处理设备；以及

存储控制步骤，用于执行控制以便存储由所述其它信息处理设备读取或改变的用户信息，所述其它信息处理设备是由与所述其它信息处理设备相关联的所述识别控制步骤的过程来识别的。

15.一种用于通过网络与多个其它的信息处理设备进行通信并存储与用户有关的用户信息的信息处理设备，所述信息处理设备包括：

通信装置，用于通过所述网络与所述用户持有的便携式终端进行通信；

获取装置，用于获取存储在所述便携式终端中并涉及所述用户的用户信息；

更新装置，用于基于所述获取装置所获取的用户信息来更新存储在所述用户处理设备中的所述用户信息；以及

产生装置，用于产生更新存储在所述便携式终端中的所述用户信息所需的数据。

16.如权利要求15所述的信息处理设备，其特征在于，

当所述便携式终端没有连接到所述网络时，所述通信装置与所述其它信息处理设备而非所述便携式终端进行通信。

17.如权利要求16所述的信息处理设备，其特征在于，

作为所述用户信息而被存储的还有：

用于识别所述便携式终端的信息；

所述便携式终端验证所述其它信息处理设备所用的密码；

所述便携式终端加密信息时所用的第一代码以及与所述第一代码相应产生的

第二代码；

用于识别所述其它信息处理设备的信息；

所述其它信息处理设备验证所述便携式终端所用的密码；以及

所述其它信息处理设备用来加密信息时所用的第三代码。

18.如权利要求 15 所述的信息处理设备，其特征在于，所述信息处理设备还包括用于基于所述其它信息处理设备所提供的内容使用历史来更新所述用户信息的更新装置。

19.如权利要求 15 所述的信息处理设备，其特征在于，

将所述便携式终端与所述网络相连的访问点被识别出，所述用户的当前值是基于被识别出的所述访问点的位置来确定的，并且关于所述用户的当前位置的信息是作为所述用户信息来存储的。

20.如权利要求 19 所述的信息处理设备，其特征在于，

用于识别与所述访问点相对应的设备和与所述设备进行通信所必需的访问密匙的 ID 可进一步作为所述用户信息被存储。

21.如权利要求 20 所述的信息处理设备，其特征在于，

所述通信装置以预定的时间间隔与所述便携式终端进行通信，以便更新关于所述用户当前位置的信息、用于识别与所述访问点相对应的设备的 ID、以及所述访问密匙。

22.如权利要求 21 所述的信息处理设备，其特征在于，

当通过所述网络从所述其它信息处理设备中接收到用于表示请求与所述用户进行会话的请求信号时，所述用户信息被发送到所述其它信息处理设备。

23.如权利要求 15 所述的信息处理设备，其特征在于，

超出所述便携式终端的存储容量的所述用户信息被进一步存储。

24.一种信息处理设备的信息处理方法，所述信息处理设备通过网络与多个其它的信息处理设备进行通信并存储着与用户有关的用户信息，所述信息处理方法包括：

通信步骤，用于通过所述网络与所述用户持有的便携式终端进行通信；

获取步骤，用于获取存储在所述便携式终端中并涉及所述用户的用户信息；

更新步骤，用于基于所述获取步骤的过程所获取的用户信息来更新存储在所

述信息处理设备中的所述用户信息；以及

产生步骤，用于产生更新存储在所述便携式终端中的所述用户信息所需的数据。

25.一种信息处理设备的程序，所述信息处理设备通过网络与多个其它的信息处理设备进行通信并存储与用户有关的用户信息，所述程序使计算机执行：

通信控制步骤，用于执行控制以便通过所述网络与所述用户所持有的便携式终端进行通信；

获取控制步骤，用于控制获取存储在所述便携式终端中并涉及所述用户的用户信息；

更新控制步骤，用于执行控制以便基于所述获取控制步骤的过程所获取的用户信息来更新存储在所述信息处理设备中的所述用户信息；以及

产生控制步骤，用于控制产生更新存储在所述便携式终端中的所述用户信息所需的数据。

26.一种在其上记录有信息处理设备的程序的记录媒体，所述信息处理设备通过网络与多个其它的信息处理设备进行通信并存储与用户有关的用户信息，所述程序使计算机执行：

通信控制步骤，用于执行控制以便通过所述网络与所述用户所持有的便携式终端进行通信；

获取控制步骤，用于控制获取存储在所述便携式终端中并涉及所述用户的用户信息；

更新控制步骤，用于执行控制以便基于所述获取控制步骤的过程所获取的用户信息来更新存储在所述信息处理设备中的所述用户信息；以及

产生控制步骤，用于控制产生更新存储在所述便携式终端中的所述用户信息所需的数据。

信息处理设备和方法、程序以及记录媒体

技术领域

本发明涉及用于信息处理的设备和方法、程序以及记录媒体，它们可为用户提供更多方便，还为用户提供舒适和安全的服务。

背景技术

最近通过展示个人信息来接收各种服务已成为可能。个人信息包括各种信息，比如名字、地址、爱好信息、某项服务的验证信息、点数信息、从另一个人处接收到的信息等。

一项技术已经提出，当用户带着存有这种个人信息的卡进入商场时，安装在购物车上的读卡机读取卡片上的信息，基于卡片上的信息便显示出了广告、楼面导购信息、最爱商品的打折信息等（例如，可参考非专利文档 1）。

另外，通过使用个人信息执行个人验证，可尝试使购物、付款等过程更为方便（例如，可参看专利文档 1 到 3）。

根据专利文档 1，在用户终端上输入项目代码（或读取项目的条形码）。通过使用呼机等的远程通信来连接到公共网络，并且项目代码可转移到家里的 PC 或 PCS NCC（个人通信服务网络控制中心）。PCS NCC 将来自于项目代码的项目价格等信息发送到用户端。项目信息只显示在用户终端上。当发出购物请求时，使用电子钱币等进行实际的付款。

专利文档 2 旨在提供一个用于控制来自远方的金融信息的平台。该金融信息是由银行提供的。此外，在银行与非银行之间提供并不涉及银行业务的服务。

专利文档 3 旨在用便携电话来实现电子钱包功能、无线 PIN（个人身份号码）发射器。移动电话公司等中的服务提供商保留账户和授权信息。当从便携电话中输入预定的功能代码时，该功能代码可转移给服务提供商，并进行所请求的交易。服务提供商的中央处理单元决定验证是否是必需的。当验证是必需的时，个人验证号码可转移给中央处理单元，中央处理单元执行验证处理，并

且进行该交易。

〔专利文档 1〕

US5,991,601（个人交互通信购物及实行系统）

〔专利文档 2〕

US5,787,403（银行中心服务平台、网络及系统）

〔专利文档 3〕

US5,991,749（用于收税、进行金融交易以及授权其它活动的无线电话）

〔非专利文档 1〕

US2002-174025-A1 用于提供有针对性的广告以及个性化的客户服务的方法及系统（IBM）

发明内容

不过，非专利文档 1 的技术并不允许与在另一个商场中接收到的服务交互信息。另外，非专利文档 1 的技术并不提供用来对使用该卡片的用户进行验证的结构。

专利文档 1 的技术要求创建数据库以便于从 PCS NCC 的数据库管理中的项目代码中检索出项目信息，所以无法立刻进行处理。

专利文档 2 的技术定义了服务流程，但并未考虑在用户端执行何种验证处理。

专利文档 3 的技术要求固定的功能代码。因此，需要创建依赖于验证系统和物件信息的便携电话等，因此无法执行灵活的系统管理。结果，可能给用户带来不便。

本发明正是在看到这种情况下才产生的，本发明的目的在于给用户提供方便并进一步为用户提供舒适安全的服务。

根据本发明，提供了第一信息处理设备，它存储与用户相关的用户信息并与多个其它的信息处理设备相互通信。该第一信息处理设备可以包括：呈现装置，用于呈现要由其它信息处理设备读取或改变的用户信息；指定装置，用于指定准许读取或改变由呈现装置所呈现的用户信息；识别装置，用于识别其它信息处理设备；以及存储装置，用于存储由与其它信息处理设备相关联的识别

装置所识别出的其它信息处理设备所要读取或改变的用户信息。

第一信息处理设备可进一步包括通信装置，用于执行准静电场通信、电磁波通信、光通信或电通信。

在信息处理设备外部的设备可用作输入或输出接口。

当与其它信息处理设备进行首次通信时，用于识别信息处理设备的信息可被发送到其它信息处理设备。

当与其它信息处理设备进行首次通信时，可以产生由信息处理设备用来加密信息的第一代码以及与第一代码相应地产生的第二代码，并且第一代码可以被发送到其它信息处理设备，并且通过通信装置可以获得由其它信息处理设备用来加密信息的第三代码。

基于其它信息处理设备所提供的内容的使用历史，可以更新用户信息。

通过网络，可以与用来管理用户信息的信息管理设备进行通信，并可以更新用户信息，所以存储在信息处理设备中的用户信息内容与存储在信息管理设备中的用户信息内容完全一样。

信息管理设备可以识别被准许读取或改变用户信息的其它信息处理设备，并可以将用户信息提供给被准许通过网络来读取或改变用户信息的其它信息处理设备。

基于发生在用户身体上的准静电场或静电场的变化图案，可以对该用户进行验证。

用户信息可以具有表示用户偏好的偏好信息，该偏好信息可以被发送到由该用户指定的信息设备，并且该信息设备可以在与该偏好信息一致的情况下运行。

基于与多个其它信息处理设备相关联的多条用户信息，可以创建新的用户信息。

根据本发明，提供了信息处理设备的第一信息处理方法，该信息处理设备存储着与用户相关的用户信息并与多个其它的信息处理设备通信。第一信息处理方法可以包括：呈现步骤，用于呈现要被其它信息处理设备读取或改变的用户信息；指定步骤，用于指定准许读取或改变由呈现步骤的过程所呈现的用户信息；识别步骤，用于识别其它信息处理设备；以及存储步骤，用于存储与其

它信息处理设备相关联的识别步骤的过程所识别出的其它信息处理设备所读取或改变的用户信息。

根据本发明，提供了信息处理设备的第一程序，该信息处理设备存储着与用户相关的用户信息并与多个其它的信息处理设备相互通信。该第一程序可使计算机执行：呈现控制步骤，用于控制着要被其它信息处理设备读取或改变的用户信息的呈现过程；指定控制步骤，用于控制着允许读取或改变由呈现控制步骤的过程所呈现的用户信息的指定过程；识别控制步骤，用于控制着其它信息处理设备的识别过程；以及存储控制步骤，用于执行控制以便存储由其它信息处理设备读取或改变的用户信息，该其它信息处理设备是由与其它信息处理设备相关联的识别控制步骤的过程识别出的。

根据本发明，提供了在其上记录着信息处理设备的程序的第一记录媒体，该信息处理设备存储着与用户相关的用户信息并与多个其它的信息处理设备相互通信。该程序可以使计算机执行：呈现控制步骤，用于控制着要被其它信息处理设备读取或改变的用户信息的呈现过程；指定控制步骤，用于控制着允许读取或改变由呈现控制步骤的过程所呈现的用户信息的指定过程；识别控制步骤，用于控制着其它信息处理设备的识别过程；以及存储控制步骤，用于执行控制以便存储由其它信息处理设备读取或改变的用户信息，该其它信息处理设备是由与其它信息处理设备相关联的识别控制步骤的过程识别出的。

在第一信息处理设备、第一信息处理方法以及第一程序中，呈现要被另一个信息处理设备读取或改变的用户信息，指定准许读取或改变所呈现的用户信息，与其它信息处理设备相关联地存储由所识别的其它信息处理设备读取或改变的用户信息。

根据本发明，提供了第二信息处理设备，它用于通过网络与多个其它的信息处理设备相互通信并存储与用户相关的用户信息。第二信息处理设备可以包括：通信装置，用于通过网络与经用户处理过的便携终端进行相互通信；获取装置，用于获取存储在便携终端中并与用户相关的用户信息；更新装置，用于基于由获取装置获取的用户信息来更新存储在信息处理设备中的用户信息；以及产生装置，用于产生更新存储在便携终端中的用户信息所需的数据。

当便携终端并未连接到网络上时，通信装置可以与替代该便携终端的其它

信息处理设备相互通信。

进一步存储的用户信息可以是：用于识别便携终端的信息；便携终端验证其它信息处理设备所需的密码；便携终端用来加密信息的第一代码以及与该第一代码相应而生的第二代码；用于识别其它信息处理设备的信息；其它信息处理设备验证便携终端所需的密码；以及其它信息处理设备用来加密信息的第三代码。

信息处理设备可进一步包括更新装置，用于基于其它信息处理设备所提供的内容的使用历史来更新用户信息。

可以识别将便携终端与网络相连的访问点，基于识别出的访问点的位置可以确定用户目前的值，并且关于用户当前位置的信息可以作为用户信息来存储。

用于识别某一设备的 ID 可以作为用户信息来存储，该设备对应于与该设备进行通信所必需的访问点和访问密匙。

通信装置可以每隔预定的时间与便携终端进行通信以更新关于用户当前位置的信息，用于识别服务的 ID 对应于访问点和访问密匙。

当通过网络接收到来自于其它信息处理设备的、表示请求与用户进行对话的请求信号时，用户信息可以被发送到其它信息处理设备。

可以进一步存储超出便携终端存储容量的用户信息。

根据本发明，提供了信息处理设备的第二信息处理方法，该信息处理设备通过网络与多个其它的信息处理设备进行通信并存储与用户相关的用户信息。第二信息处理方法可以包括：通信步骤，用于通过网络与经用户处理过的便携终端进行通信；获取步骤，用于获取存储在便携终端中并涉及该用户的用户信息；更新步骤，用于基于获取步骤的过程中所获取的用户信息来更新存储在信息处理设备中的用户信息；以及产生步骤，用于产生更新存储在便携终端中的用户信息所需的数据。

根据本发明，提供了信息处理设备的第二程序，该信息处理设备通过网络与多个其它的信息处理设备进行通信并存储与用户有关的用户信息。第二程序可以使计算机执行：通信控制步骤，用于执行控制以便通过网络与经用户处理过的便携终端进行通信；获取控制步骤，用于控制对存储在便携终端中并与用

户有关的用户信息的获取过程；更新控制步骤，用于执行控制以便基于获取控制步骤的过程中所获取的用户信息来更新存储在信息处理设备中的用户信息；以及产生控制步骤，用于控制更新存储在便携终端中的用户信息所需的数据的产生过程。

根据本发明，提供了在其上记录有信息处理设备的程序的第二记录媒体，该信息处理设备通过网络与多个其它的信息处理设备进行通信并存储与用户有关的用户信息。该程序可以使计算机执行：通信控制步骤，用于执行控制以便通过网络与经用户处理过的便携终端进行通信；获取控制步骤，用于控制对存储在便携终端中并与用户有关的用户信息的获取过程；更新控制步骤，用于执行控制以便基于获取控制步骤的过程中所获取的用户信息来更新存储在信息处理设备中的用户信息；以及产生控制步骤，用于控制更新存储在便携终端中的用户信息所需的数据的产生过程。

在第二信息处理设备、第二信息处理方法以及第二程序中，通过网络与经用户处理过的便携终端进行通信，获取存储在便携终端中并涉及该用户的用户信息，基于所获取的用户信息来更新存储在信息处理设备中的用户信息，并且产生更新存储在便携终端中的用户信息所需的数据。

根据本发明，有可能为用户提供极为便利的服务。特别是，有可能为用户提供舒适且安全的服务。

附图说明

图 1 示出了根据本发明的服务提供系统的结构示例的方框图；

图 2 是示出了图 1 中的 PK 的结构示例的方框图；

图 3 是示出了图 1 中的 pBase 的结构示例的方框图；

图 4 是示出了图 1 中的 PK 的软件配置示例的方框图；

图 5 是示出了服务 ID 首次注册过程的流程的箭头图；

图 6 是示出了在 PK 与服务系统之间防电子欺骗的流程的箭头图；

图 7 是示出了在 PK 与服务系统之间防电子欺骗的流程的箭头图；

图 8 是解释密匙管理过程的辅助流程图；

图 9 是解释服务 ID 注册过程的辅助流程图；

图 10 是解释服务 ID 匹配过程的辅助流程图；

图 11A 示出了 PK 验证用户的一个示例；

图 11B 示出了 PK 验证用户的一个示例；

图 12 是解释第一用户验证过程的辅助流程图；

图 13 是解释第二用户验证过程的辅助流程图；

图 14 是解释 PMD 管理过程的辅助流程图；

图 15 示出了使用 PK 的外部设备以构成输入/输出接口的一个示例；

图 16 示出了到外围设备的访问密匙被 PK 隐藏的一种状态；

图 17A 示出了在 PK、pBase 和服务系统之间的通信模式；

图 17B 示出了在 PK、pBase 和服务系统之间的通信模式；

图 17C 示出了在 PK、pBase 和服务系统之间的通信模式；

图 18 是示出了在 pBase 和服务系统之间防电子欺骗的处理流程的箭头图；

图 19 是示出了在 pBase 和服务系统之间防电子欺骗的处理流程的箭头图；

图 20A 示出了 PMD 组成的一个示例；

图 20B 示出了 PMD 组成的一个示例；

图 20C 示出了 PMD 组成的一个示例；

图 21 是解释 PMD 更新过程的辅助流程图；

图 22 示出了基于多条 PMD 而产生的新的 PMD；

图 23 示出了基于多条 PMD 而产生的新的 PMD；

图 24 示出了内容服务分组组成的一个示例；

图 25 示出了由 PK 使各种设备个性化的一个示例；

图 26 是解释音乐再现处理的辅助流程图；

图 27 是解释 web 信息提供过程的辅助流程图；

图 28 示出了由 PK 使各种设备个性化的一个示例；

图 29 示出了通过具有防火墙功能的路由器而进行通信的一个示例；

图 30 是示出了 PMD 同步处理流程的箭头图；

图 31 是解释 PMD 同步处理的辅助流程图；

图 32 示出了在 PK 中保留各种卡片信息并使用该信息的一个示例；

图 33 示出了在控制台终端中安装控制代码的一个示例；

图 34 是示出了获取控制代码的流程的箭头图；

图 35 示出了由 PK 打开一扇门的一个示例；

图 36 示出了在终端上显示 PK 中的面孔特征信息的一个示例；

图 37 示出了对话连接服务的一个示例；

图 38 是示出了实现对话连接的流程的箭头图；

图 39 示出了使用 PK 来确定用户位置的一个示例；

图 40 是示出了确定用户位置的流程的箭头图；

图 41 是提供地图信息服务的一个示例；

图 42 示出了使用照相机来确定用户位置的一个示例；

图 43 是解释第一访问点检测过程的辅助流程图；

图 44 示出了检测访问点的方法；

图 45 是解释第二访问点检测过程的辅助流程图；

图 46 示出了检测访问点的方法；

图 47 示出了 PK 的多个通信路线；

图 48 示出了 PMD 组成的一个示例；

图 49 是解释 PK 的程序执行过程的辅助流程图；

图 50 是示出了用作为服务系统的 pBase 来执行的流程的箭头图；

图 51 是解释通信备用过程的辅助流程图；

图 52 示出了在备用期间通信的一个示例；

图 53 示出了执行 RF 通信的一个示例；

图 54A 示出了由 PK 通知用户一则消息的一个示例；

图 54B 示出了由 PK 通知用户一则消息的一个示例；

图 55 示出了通信列表的一个示例；

图 56 示出了会议室中的一些设备；

图 57 示出了在会议室中就坐的诸多位置；

图 58 示出了减小 IP 电话的功耗的一个示例；

图 59 示出了在一个设备中实现 PK 的软件和服务系统的软件的一个示例；以及

图 60 示出了使用协作过滤服务器和 PMD 来执行个性化处理的一个示例。

具体实施方式

参照附图将在下文中对本发明的较佳实施例进行描述。图 1 是示出了应用本发明的服务提供系统 1 的结构示例的方框图。在本示例中，用户 20 带着用较小的便携式计算机等构成的 PK（个人密匙）22，该 PK 存储着关于该用户的个人相关信息。在这种情况下的个人相关信息并不仅指用于识别该用户的那些信息，比如姓名、地址等，而还指一组涉及该用户的各种信息，这类信息包括偏好信息、验证信息、点数信息、从另一个人处接收到的信息等。

PK 22 与访问点 25 相互通信，访问点 25 则通过访问点 25 周围地区 41 中的像 RF（无线电频率）通信这样的无线通信、准静电场通信、光通信等连接到互联网 21 上。PK 22 也通过无线通信等与附近的信息设备进行通信。PK 22 具有基于加密密匙对信息进行加密的加密功能。按要求，加密密匙的密匙数据存储在 SB（安全按钮）中。SB 26 是具有通信功能的计算机。SB 26 与 PK 22 进行通信以便将密匙数据发送到 PK 22 或接收来自于 PK 22 的密匙数据。

互联网 21 与 pBase（个人信息基本库）23 相连，pBase 23 通过互联网 21 从 PK 22 中获取作为关于用户 20 的个人相关信息的 PMD（个人元数据），并将所获取的 PMD 作为数据库来存储。pBase 23 是由计算机构成的，并且与连接到互联网 21 的另一个信息处理装置进行通信。另外，pBase 23 也存储除 PK 22（用户 20）之外的诸多 PK（诸多用户）的多条 PMD。

互联网 21 也与由计算机等构成的服务系统 24-1 到 24-3 相连，各服务系统执行预定的进程。服务系统 24-1 到 24-3 通过互联网获取来自于 PK 22 或 pBase 23 的 PMD，并基于所获取的 PMD 来执行预定的程序，由此为该用户提供诸多服务，比如提供信息、为购物账单付款等。

例如，服务系统 24-1 是一个向个人计算机提供网页、音乐信息等的内容服务器。服务系统 24-2 是用信用卡执行付款等的信用卡处理服务器。服务系统 24-3 是控制与用户 20 进行的通信的通信服务器。访问点 25 被包括在与 PK 22 进行通信的服务系统 24-4 中。另外，当不需要对这些服务系统作单独区分时，这些服务系统将被共同地称为服务系统 24。

尽管本示例中示出了服务系统 24-1 到 24-4，但是在实践中可以有大量的

服务系统。服务系统 24 并不限于个人计算机、服务器等，还可以由控制台终端各种客户电子设备（CE 设备）等构成。此外，服务系统 24 并不限于连接到互联网 21，而是可以安装到任何地方，只要服务系统 24 具有通信功能即可。另外，PK 22 和服务系统 24 可以直接通信而不用互联网 21 的介入。

图 2 是示出了 PK 22 的结构示例的方框图。CPU（中央处理单元）101 根据存储在 ROM（只读存储器）102 中的程序或根据从存储单元 108 加载到 RAM（随机存取存储器）103 中的程序来执行各种进程。RAM 103 也存储 CPU 101 执行各种进程所必需的数据等。

CPU 101、ROM 102 以及 RAM 103 通过总线 104 互连起来。总线 104 也与输入/输出接口 105 相连。

输入/输出接口 105 连接到由开关、按钮等构成的输入单元 106 以及由点阵显示器、扬声器、振动马达等和要通过图像、音频、盲人用的点字、振动等呈现给用户的输出信息一起构成的输出单元 107。输入/输出接口 105 还连接到由硬盘构成的存储单元 108、EEPROM（电擦除可编程只读存储器）等以及由无线电发送及接收设备等构成的通信单元 109。另外，根据各种通信方法可以提供多个通信单元，比如 RF 通信（电磁波通信）、准静电场通信、光通信等。

例如，RF（无线电频率）通信是一种以 IEEE 802.11b 为代表的无线 LAN 通信。这种通信在预定的访问点（集线器）周围约几十米的半径内是可行的。准静电场通信是这样一种通信系统，它形成一个闭合静电信息空间，该空间的物理特性（瞬时的特性）不能沿长距离传播，并且准静电场通信只形成于人体附近闭合区域中。使用人体作为弱静电的天线，这种通信只在人体附近半径约几厘米或几米的有限空间内可行。带着 PK 22 的用户因此可以在例如行走的同时使 PK 22 通信。

当然，通信单元 109 也可以进行以 Ethernet（注册商标）等为代表的电线电通信或使用红外线等的光通信。

输入/输出接口 105 按要求与驱动器 110 相连。作为在其上记录有根据本发明的程序的记录媒体，例如，将可移动媒体 111 载入驱动器 110。按照需求，从可移动媒体 111 中读取的计算机程序被安装在存储单元 108 中。

图 3 是示出了 pBase 23 的结构示例的方框图。pBase 23 的结构与图 2 所示

的 PK 22 的结构相似。图 3 中的 CPU 121 到可移动的媒体 131 对应于图 2 中的 CPU 101 到可移动的媒体 111。各部件的功能与图 2 中的那些部件相似，因此略去有关描述。不过，通信单元 129 是由无线电发送及接收设备以及像 LAN 卡、调制解调器等电线通信设备构成的。

服务系统 24 也具有与图 3 相似的结构，相同的数字应用于该服务系统 24。

图 4 是示出了存储在 PK 22 的存储单元 108 中的软件 60 的配置示例的方框图。软件 60 包括 PMDB 67，PMDB 67 将作为存储在 PK 22 中的个人信息的 MPD 存储成数据库，并且通信模块 61 控制通信单元 109 以便进行通信。

软件 60 包括：受用户控制的准许输入模块 62，该模块 62 用于接收准许访问 PMD 的说明；以及被准许的项目确认模块，该模块用于呈现该 PMD 以允许用户来决定是否允许服务系统 24 访问所请求的 PMD。软件 60 进一步包括：防电子欺骗模块 63，该模块用于防止服务系统 24 的电子欺骗；以及用于按要求来改变 PMD 的 PMD 改变模块 65。基于来自于受用户控制的准许输入模块 62 到 PMD 改变模块 65 的指令（请求），DB 访问模块 66 访问 PMDB 67 以便读取或改变 PMD。

PMDB 67 是包括多条 PMD 的数据库。各条 PMD 信息以目录的形式彼此相关，其服务 ID 作为唯一的 ID 对应于用作一个密匙的各服务系统 24。在服务 ID 1 的目录（PMD）中，访问准许信息、元数据 A-1、元数据 A-2、元数据 A-3 等彼此相互关联。

访问准许信息表示是否准许从服务系统 24 访问到与该目录相关联的信息，并且该访问准许信息是由用户设置的。元数据 A-1、元数据 A-2、元数据 A-3 等是在与服务 ID 1 相对应的服务系统 24 中使用的个人相关信息。当对应于服务 ID 1 的服务系统是用于提供像电影、电视节目等内容的内容服务器时，例如，所观看的节目的元数据存储在元数据 A-1、元数据 A-2、元数据 A-3 等中。另外，用于识别 PK 22（用户 20）的用户 ID、像防电子欺骗处理中所要求的密码和加密密匙等验证信息、基于所观看的节目的用户偏好信息、以及用于控制电视接收机等的控制信息都作为 PMD 加以存储。

相似的是，在服务 ID 2 的目录（PMD）中，访问准许信息、元数据 B-1、元数据 B-2、元数据 B-3 等彼此相关联。当 PK 使用新的服务系统 24 时，便注

册了新的服务 ID，并且创建了与该服务 ID 相对应的目录。各目录是作为 PMD 设置的以便构成 PMDB 67。另外，随后会参照图 20 详细描述 PMD 组成的一个示例的细节。

图 5 是当与服务系统 24 相对应的服务 ID 首先注册（首次注册）到 PK 22 中时的流程的箭头图。在步骤 S1 处，服务系统 24 向 PK 22 发送注册请求、服务 ID 以及表示要被该服务系统读取或改变的元数据的信息。在步骤 S21 中，这是由 PK 的通信模块 61 来接收的。

在步骤 S22 中，通信模块 61 将接收到的内容转移到被准许的项目确认模块 63。在步骤 S42 中，被准许的项目确认模块 63 向用户呈现要被读取或改变的元数据。同时，例如，元数据内容作为文本、图形等显示在点阵显示器等上，或通过扬声器用语音来读取。或者，元数据内容可以用机械装置以盲人用的点字来产生并呈现，或作为像通过振动而产生的鼠标信号这样的信号来呈现。

在步骤 S43 中，被准许的项目确认模块 63 将确认请求输出到受用户控制的准许输入模块 62。这在步骤 S61 中被接收。在步骤 S62 中，受用户控制的准许输入模块 62 决定该用户是否拒绝访问要被读取或改变的元数据，该元数据在步骤 S42 中被呈现。当受用户控制的准许输入模块 62 决定该用户拒绝访问该元数据时，受用户控制的准许输入模块 62 输出一个拒绝信号。这在步骤 S23 中由通信模块 61 来接收。在步骤 S24 中，通信模块 61 将拒绝信号发送到服务系统 24。这在步骤 S2 中被接收。

另一方面，当受用户控制的准许输入模块 62 在步骤 S62 中决定该用户并不拒绝访问要被读取或改变的、在步骤 S42 中被呈现过的元数据时，受用户控制的准许输入模块 62 在步骤 S63 中会基于用户说明为每条要被读取或改变的元数据设置诸如“准许读取和改变”或“只准读取”这样的信息。这些信息作为访问准许信息（图 4）被存储在 PMDB 67 中。在步骤 S64 中，受用户控制的准许输入模块 62 通知被准许的项目确认模块 63 访问控制信息已设置。这在步骤 S44 中被接收。在步骤 S45 中，被准许的项目确认模块 63 向防电子欺骗模块 64 发出请求以产生确认代码。这在步骤 S81 中由防电子欺骗模块 64 来接收。

在步骤 S82 中，防电子欺骗模块 64 产生确认代码。该确认代码表示当 PK 22 与服务系统 24 下次彼此通信时所执行的防电子欺骗方法。即，该确认代码

表示一种用于相互确认的方法，要确认的是未经授权的用户或截取通信的第三方并没有通过虚报该未经授权的用户或该第三方的地址、ID 等来电子欺骗 PK 22 或服务系统 24。

作为防电子欺骗方法，可使用如下各种验证：使用密码的验证，使用由公共密匙来加密的信息的验证，使用由普通密匙来加密的信息的验证。不过，在与服务系统 24 进行通信的过程中，最佳防电子欺骗方法是根据所要求的安全度、用于防电子欺骗的检查范围及频率、加密密匙管理方法的安全性和容易度、加密和解密过程中的计算量等来选择的。与防电子欺骗方法相对应的确认代码便产生了。另外，随后将参照附图 6 和 7 对防电子欺骗过程进行描述。

在步骤 S82 中，防电子欺骗模块 64 将确认代码输出到通信模块 61。这在步骤 S25 中由通信模块 61 来接收。在步骤 S26 中，通信模块 61 将在步骤 S25 中获取的确认代码发送到服务系统 24。这在步骤 S3 中被接收。

另外，此时，用于识别 PK 22（PK 22 的用户）的用户 ID 也由服务系统 24 接收到。服务系统 24 存储用户 ID 以及与该用户 ID 相对应的确认代码。用户 ID 可以是任何形式，只要该用户 ID 允许服务系统 24 识别该 PK 22（PK 22 的用户）即可。例如，用户 ID 可以是由数字组合过程的，或可以由预定的字符串过程。此外，可以创建不同的用户 ID 以对应于多个服务系统 24。

在步骤 S46，被准许的项目确认模块 63 向 DB 访问模块 66 输出服务 ID 注册请求。这在步骤 S101 中由 DB 访问模块 66 来接收。在步骤 S102 中，DB 访问模块 66 执行随后参照图 9 将加以描述的服务 ID 注册过程。由此便注册了服务 ID，并且产生了与该服务 ID 相对应的 PMD。

因此，在 PK 22 中注册了与服务系统 24 相对应的服务 ID。当服务 ID 注册后，服务系统 24 将所要读取或改变 PMD 元数据呈现给用户。因此，用户可以在带有更大的安全感的情况下接收服务。当 PK 22 与下次要注册其服务 ID 的服务系统 24 进行通信时，可以基于确认代码执行防电子欺骗处理。相似的是，当服务系统 24 与下次要注册其用户 ID 的 PK 22 进行通信时，可以基于确认代码来执行防电子欺骗处理。

下面将参照图 6 和 7 来描述当 PK 22 与其服务 ID 已经注册过的服务系统 24 进行通信时的防电子欺骗处理。

图 6 是解释在 PK 22 与服务系统 24 之间使用密码验证作为防电子欺骗方法时的防电子欺骗处理流程的辅助箭头图。在本示例中，PK 22 确认服务系统 24 没有被电子欺骗，并且之后服务系统 24 确认 PK 22 没有被电子欺骗。在 PK 22 和服务系统 24 确认服务系统 24 和 PK 22 并没有被电子欺骗之后，便执行读取或改变 PMD 的处理。

例如，密码可以是预定的字符串或代码。当在 PK 22 中注册服务 ID 时，用于验证服务系统 24 的密码（服务密码）以及用于验证 PK 的密码（PK 密码）都作为与该服务 ID 相对应的密码而产生了，并存储在 PMDB 67 中。当注册了服务 ID 时，服务密码和 PK 密码也被发送到服务系统 24。服务密码和 PK 密码存储在服务系统 24 的存储单元 128 的数据库中并与 PK 22 的用户 ID 相关联。

在步骤 S201 中，服务系统 24 将连接请求、服务 ID 以及密码发送到 PK 22。这在步骤 S221 中由 PK 22 的通信模块来接收。另外，在步骤 S201 中也发送如上所述的服务密码。在步骤 S222 中，通信模块 61 将在步骤 S221 中接收到的内容发送到防电子欺骗模块 64。这在步骤 S281 中被接收。

在步骤 S282 中，防电子欺骗模块 64 执行随后参照图 9 将加以描述的服务 ID 匹配处理，并由此识别该服务 ID。在步骤 S283 中，防电子欺骗模块 64 将对与服务 ID 相对应的用户 ID 和密码的请求传送到 DB 访问模块 66。这在步骤 S301 中由 DB 访问模块 66 来接收。另外，在步骤 S282 中的服务匹配处理可以由 DB 访问模块 66 来执行。

在步骤 S302 中，DB 访问模块 66 从 PMDB 67 中读取与服务 ID 相对应的服务密码、PK 密码以及用户 ID，并接着将服务密码、PK 密码以及用户 ID 输出到防电子欺骗模块 64。防电子欺骗模块 64 将在步骤 S284 中获取的服务密码与在步骤 S281 中获取的密码进行比较。当防电子欺骗模块 64 确定在步骤 S284 中获取的服务密码与在步骤 S281 中获取的密码并不匹配时，防电子欺骗模块 64 确定服务系统 24 可能被电子欺骗了，并且将表示拒绝通信的拒绝信号传送到通信模块 61。这在步骤 S223 中由通信模块 61 来接收。在步骤 S224 中，通信模块 61 将拒绝信号发送到服务系统 24。这在步骤 S202 中由服务系统来接收。

由此，当开始通信时没有从服务系统 24 中发送出与服务 ID 相对应的密码，在这种情况下，PK 22 便拒绝该通信。

另一方面，当防电子欺骗模块 64 在步骤 S285 中确定在步骤 S284 中获取的服务密码与在步骤 S281 中获取的密码匹配时，防电子欺骗模块 64 在步骤 S286 中向通信模块 61 输出用于表示已确认服务系统 24 没有被电子欺骗的代码（OK）、用户 ID、以及在步骤 S284 中获取的 PK 密码。这在步骤 S225 中由通信模块 61 来接收。在步骤 S226 中，通信模块 61 将在步骤 S225 中获取的信息发送到服务系统 24。这在步骤 S203 中由服务系统 24 来接收。

在步骤 S204 中，服务系统 24 从服务系统 24 自身的数据库中读取在步骤 S203 中接收到的、与用户 ID 相对应的 PK 密码，将所读取的 PK 密码与在步骤 S203 中接收到的密码进行比较，并确定这些密码是否相互匹配。当服务系统 24 在步骤 S204 中确定这些密码并不相互匹配时，服务系统 24 确定 PK 22 可能被电子欺骗，并向 PK 22 发送表示拒绝通信的拒绝信号。这在步骤 S287 中由防电子欺骗模块 64 通过 PK 22 中的通信模块 61 来接收。

由此，当开始通信时没有从 PK 22 中发出与用户 ID 相对应的密码，在这种情况下，服务系统 24 拒绝通信。

另一方面，当服务系统 24 在步骤 S204 中确定这些密码相互匹配时，服务系统 24 确定 PK 22 没有被电子欺骗。在步骤 S205 中，服务系统 24 向 PK 22 发送请求以读取 PMD。这在步骤 S227 中由 PK 22 的通信模块 61 来接收。在步骤 S228 中，通信模块 61 向 DB 访问模块 66 输出在步骤 S227 中接收到的内容。这在步骤 S303 中由 DB 访问模块 66 来接收。

在步骤 S304 中，DB 访问模块 66 检查由服务系统 24 请求读取的 PMD（PMD 元数据）是否与和服务系统 24 相对应的服务 ID 相一致，以及是否允许被读取。当 PMD 允许被读取时，DB 访问模块 66 从 PMDB 67 中读取该 PMD。在步骤 S305 中，DB 访问模块 66 将所读取的 PMD 输出给通信模块 61。这在步骤 S229 中由通信模块 61 来接收。

在步骤 S230 中，通信模块 61 将在步骤 S229 中获取的信息发送到服务系统 24。这在步骤 S206 中由服务系统 24 来接收。

在步骤 S207 中，服务系统 24 基于在步骤 S206 中接收到的 PMD 执行各种处理（与处理相对应的服务）。当作为步骤 S207 中处理的结果需要改变 PMD 时，服务系统 24 在步骤 S208 中改变 PMD 的内容，并将该内容发送到 PK 22。

这在步骤 S231 中由 PK 22 的通信模块 61 来接收。

在步骤 S232 中，通信模块 61 将在步骤 S231 中接收到的信息输出给 DB 访问模块 66。这在步骤 S306 中由 DB 访问模块 66 来接收。在步骤 S307 中，DB 访问模块 66 检查在步骤 S306 中获取的 PMD 是否与和服务系统 24 相对应的服务 ID 相一致，以及是否允许被改变。当 PMD 允许被改变时，在 PMDB 67 中相应的 PMD 就被改变了（被更新了，以对应于被改变的内容）。

由此，既然在读取或改变 PMD 之前可以检查是否被电子欺骗，所以可以提供安全的服务。此外，既然 PK 22 对服务系统 24 做电子欺骗与否的检查并且服务系统 24 也对 PK 22 做电子欺骗与否的检查，那么便可以提供安全的服务了。

下面将参照图 7 对当 PK 22 与其服务 ID 已经注册过的服务系统 24 进行通信时所用的另一个防电子欺骗处理的示例进行描述。图 7 是一个箭头图，它辅助说明了在 PK 22 与服务系统 24 之间使用用公共密匙来加密的信息的验证作为防电子欺骗方法时防电子欺骗处理的流程。

在本示例中，PK 22 确认服务系统 24 没有被电子欺骗，并且之后服务系统 24 确认 PK 22 没有被电子欺骗。在 PK 22 和服务系统 24 确认服务系统 24 和 PK 22 都没有被电子欺骗之后，执行读取或改变 PMD 的处理。

在本示例中，PK 22 和服务系统 24 具有用像 RSA 等公共密匙系统的加密算法来加密或解密信息的功能。当服务 ID 已注册过时，PK 22 将服务系统 24 的公共密匙存储在与服务系统 24 的服务 ID 相关联的 PMDB 67 中，并且服务系统 24 将 PK 22 的公共密匙存储在与 PK 22 的用户 ID 相关联的存储单元 128 中的数据库中。PK 22 和服务系统 24 的私人密匙存储在各自的存储单元 108 和 128 中。

在步骤 S401 中，服务系统 24 将连接请求和服务 ID 发送到 PK 22。这在步骤 S421 中由 PK 22 的通信模块来接收。在步骤 S422 中，通信模块 61 将在步骤 S421 中接收到的信息发送到防电子欺骗模块 64。这在步骤 S481 中被接收。

在步骤 S482 中，防电子欺骗模块 64 执行随后将参照图 10 给予描述的服务 ID 匹配处理，并由此识别该服务 ID。在步骤 S483 中，防电子欺骗模块 64 向 DB 访问模块 66 传送一个请求，请求与该服务 ID 相对应的用户 ID、该 PK

的私人密匙、以及服务系统 24 的公共密匙。这在步骤 S501 中由 DB 访问模块 66 来接收。另外，在步骤 S482 中的服务匹配处理可以由 DB 访问模块 66 来执行。

在步骤 S502 中，DB 访问模块 66 从 PMDB 67 中读取与该服务 ID 相对应的服务系统 24 的公共密匙以及该 PK 的公共密匙，然后，将服务系统 24 的公共密匙和该 PK 的公共密匙输出给防电子欺骗模块 64。这在步骤 S484 中由防电子欺骗模块 64 来接收。

在步骤 S485 中，为验证服务系统 24，防电子欺骗模块 64 产生用预定的代码构成的询问代码，用与服务 ID 相对应的公共密匙（服务系统 24 的公共密匙）来加密询问代码，并且将加密过的询问代码和用户 ID 输出到通信模块 61。这在步骤 S424 中由通信模块 61 来接收。在步骤 S424 中，通信模块 61 将在步骤 S423 中获取的信息发送到服务系统 24。这在步骤 S402 中由服务系统 24 来接收。

在步骤 S403 中，服务系统 24 用服务系统 24 的私人密匙来解密在步骤 S402 中接收到的已加密过的询问代码，将解密过的询问代码设置成响应代码，用与用户 ID 相对应的公共密匙（PK 22 的公共密匙）来加密该响应代码，并将加密过的响应代码发送到 PK 22。这在步骤 S425 中由 PK 22 的通信模块 61 来接收。

在步骤 S426 中，通信模块 61 将在步骤 S425 中接收到的加密过的响应代码输出给防电子欺骗模块 64。这在步骤 S486 中由防电子欺骗模块 64 来接收。

在步骤 S487 中，防电子欺骗模块 64 用 PK 22 的私人密匙来解密在步骤 S486 中接收到的经加密过的响应代码，并将解密过的响应代码与在步骤 S485 中产生的询问代码进行比较以确定该询问代码与响应代码是否相互匹配。当防电子欺骗模块 64 确定询问代码与响应代码并不匹配时，防电子欺骗模块 64 确定服务系统 24 可能被电子欺骗了，并向通信模块 61 传送一个表示拒绝通信的拒绝信号。这在步骤 S426 中由通信模块 61 来接收。在步骤 S427 中，通信模块 61 将拒绝信号发送到服务系统 24。这在步骤 S404 中由服务系统 24 来接收。

由此，当开始通信时从 PK 22 中发出了询问代码。当从服务系统 24 中没有返回与询问代码相匹配的响应代码时，PK 22 便拒绝通信。

另一方面，当防电子欺骗模块 64 在步骤 S487 中确定询问代码与响应代码

相互匹配时，防电子欺骗模块 64 在步骤 S488 中通过通信模块 61 向服务系统 24 输出一个用于表示已确认服务系统 24 没有被电子欺骗的代码（OK）。这在步骤 S405 中由服务系统 24 来接收。

在步骤 S406 中，为验证 PK 22，服务系统 24 产生由预定的代码构成的询问代码，用与用户 ID 相对应的公共密匙（PK 22 的公共密匙）来加密该询问代码，并将加密过的询问代码输出给 PK 22。这在步骤 S429 中由 PK 22 的通信模块 61 来接收。在步骤 S430 中，通信模块 61 将在步骤 S429 中的获取的信息发送到防电子欺骗模块 64。这在步骤 S489 中由防电子欺骗模块 64 来接收。

在步骤 S490 中，防电子欺骗模块 64 用 PK 22 的私人密匙来解密在步骤 S489 中接收到的经加密过的询问代码，将解密过的询问代码设置成响应代码，用与服务 ID 相对应的公共密匙（服务系统 24 的公共密匙）来加密该响应代码，并将加密过的响应代码输出到通信模块 61。这在步骤 S431 中由通信模块 61 来接收。在步骤 S432 中，通信模块 61 将在步骤 S431 中接收到的信息发送到服务系统 24。这在步骤 S407 中由服务系统 24 来接收。

在步骤 S408 中，服务系统 24 用服务系统 24 的私人密匙来解密在步骤 S407 中接收到的经加密过的响应代码，并确定解密过的响应代码是否与在步骤 S406 中产生的询问代码相匹配。当服务系统 24 确定该询问代码并不匹配该响应代码时，服务系统 24 确定 PK 22 可能被电子欺骗，并向 PK 22 传送一个表示拒绝通信的拒绝信号。这在步骤 S433 中由 PK 22 的通信模块 61 来接收。在步骤 S434 中，通信模块 61 将在步骤 S433 中接收到的信息发送到防电子欺骗模块 64。这在步骤 S491 中由防电子欺骗模块 64 来接收。

由此，当开始通信时从服务系统 24 中发出询问代码。当从 PK 22 中没有返回与询问代码相匹配的响应时，服务系统 24 便拒绝通信。

另一方面，当服务系统 24 在步骤 S408 中确定询问代码与响应代码彼此匹配时，服务系统 24 确定已确认 PK 22 没有被电子欺骗。在步骤 S409 中，服务系统 24 将读取 PMD 的请求发送到 PK 22。这在步骤 S435 中由 PK 22 的通信模块 61 来接收。在步骤 S436 中，通信模块 61 将在步骤 S435 中接收到的信息输出给 DB 访问模块 66。这在步骤 S503 中由 DB 访问模块 66 来接收。

在步骤 S504 中，DB 访问模块 66 检查由服务系统 24 请求读取的 PMD（PMD

元数据）是否与和服务系统 24 相对应的服务 ID 相一致，以及是否允许被读取。当 PMD 被允许读取时，DB 访问模块 66 从 PMDB 67 中读取 PMD。在步骤 S505 中，DB 访问模块 66 将所读取的 PMD 输出给通信模块 61。这在步骤 S437 中由通信模块 61 来接收。

在步骤 S438 中，通信模块 61 将在步骤 S437 中获取的信息发送到服务系统 24。这在步骤 S410 中由服务系统 24 来接收。

在步骤 S411 中，服务系统 24 基于在步骤 S410 中接收到的 PMD 来执行各种处理（与处理相对应的服务）。当作为步骤 S411 中处理的结果需要改变 PMD 时，服务系统 24 在步骤 S412 中改变 PMD 的内容，并将该内容发送到 PK 22。这在步骤 S439 中由 PK 22 的通信模块 61 来接收。

在步骤 S440 中，通信模块 61 将在步骤 S439 中接收到的信息输出给 DB 访问模块 66。这在步骤 S506 中由 DB 访问模块 66 来接收。在步骤 S507 中，DB 访问模块 66 检查在步骤 S506 中获取的 PMD 是否与和服务系统 24 相对应的服务 ID 相一致，以及是否允许被改变。当 PMD 被允许改变时，PMDB 67 中相应的 PMD 便被改变（被更新为已改变的内容）。

因此，既然在读取或改变 PMD 之前，PK 22 和服务系统 24 可以相互检查电子欺骗与否，那么便可提供安全的服务。另外，用于验证 PK 22 或服务系统 24 的询问代码和响应代码是用 PK 22 或服务系统 24 的公共密匙或私人密匙来加密或解密的。因此，即便第三方截取该通信，询问代码和响应代码的内容也还是隐藏的，所以可以更为可靠地防止电子欺骗。

注意到，尽管参照图 7 所作出的描述是用公共密匙系统的加密算法来对询问代码和响应代码进行加密的，但是 PK 22 和服务系统 24 可以具有用普通密匙系统的加密算法而非公共密匙系统的加密算法来对信息进行加密及解密的功能，所以 PK 22 和服务系统 24 保留对于 PK 22 和服务系统 24 而言共同的加密密匙，并用要被传送的密匙来对询问代码和响应代码进行加密。在这种情况下，当服务 ID 已注册过时，PK 22 产生与服务 ID 相对应的加密密匙，并将该加密密匙存储在与该服务 ID 相关联的 PMDB 67 中。同时，PK 22 将相同的加密密匙发送到服务系统 24，并且该加密密匙被存储在与 PK 22 的用户 ID 相一致的服务系统 24 的数据库中。

当加密密匙泄漏时，PK 22 和服务系统 24 需要改变加密密匙。当用在确定的服务系统的公共密匙系统的加密算法中的私人密匙泄漏时，例如，在大量的使用该服务系统的 PK 中需要改变与该服务 ID 相对应的公共密匙。不过，当 PK 22 和服务系统 24 保留该 PK 22 和该服务系统 24 共同的加密密匙时，仅通过改变使用该密匙的 PK 22 和服务系统 24 的加密密匙便可以处理该加密密匙泄漏的情况。

注意到，尽管参照图 7 所描述的示例是对询问代码和响应代码进行加密，但是也可以对所有的通信内容进行加密。

此外，尽管参照图 7 所描述的示例是私人密匙（或普通密匙）是存储在 PK 22（PMDB 67）中的，但是私人密匙（或普通密匙）可以存储在不同于 PK 22 的设备中，例如图 1 中的 SB 26。在这种情况下，在与服务系统 24 进行通信之前，PK 22 和 SB 26 彼此通信使得私人密匙从 SB 26 被发送到 PK 22（同时，SB 作为一个服务系统与 PK 进行通信）。当某段时间过去时 PK 会擦除私人密匙，并与 SB 26 进行通信以便每次要求私人密匙时就能获取私人密匙。

参照图 8 将对这种情况下 PK 22 的密匙管理过程进行描述。该过程的执行先于当 PK 22 与服务系统 24 进行通信时所执行的如图 7 所示的防欺骗过程。

在步骤 S681 中，PK 22 的 CPU 101 从 SB 26 中获取密匙，并将该密匙存储在存储单元 108 中。在步骤 S682 中，CPU 101 确定预定的时间（例如，一小时）是否已过去。CPU 101 处于待用直到 CPU 101 确定预定的时间已过去。当 CPU 101 在步骤 S682 中确定预定的时间已过去时，在步骤 S683 中便擦除存储在存储单元 108 中的密匙。

因此进行密匙管理。这防止了私人密匙的泄漏，甚至是当 PK 22 被偷的时候。

下面将参照图 9 对图 5 所示的步骤 S102 中的服务 ID 注册过程的细节进行描述。在许多情况下，服务系统 24 是连接到互联网 21 上的服务器。该过程的执行是发生在当在图 5 的步骤 S102 中构成服务系统 24 的服务器的 URI（统一资源标识符）作为用于识别该服务系统 24 的信息而被获取的时候。

在步骤 S801 中，DB 访问模块 66 获取 URI。在步骤 S802 中，DB 访问模块 66 确定是否存在掩码。掩码是用于表示 URI 中预定部分的信息，并由用户

预先设置。

在互联网 21 上，URI 是作为独一无二的地址来管理的。例如，全世界各种服务器都以“http://aaa.bbb.ccc”来命名。“http://aaa.bbb.”（或“http://aaa.”）这部分通常表示与服务器所提供的服务相对应的公司等的名字。“ccc”这部分随服务的内容而变化。当用户允许针对由特定公司提供的各种服务来读取或改变 PMD 时，可以通过只引用“http://aaa.bbb.”这部分来识别服务系统 24。在这种情况下，第二部分（“ccc”这部分）被设置成掩码。

当 DB 访问模块 66 在步骤 S802 中确定存在掩码时，该过程继续到步骤 S804，其中 DB 访问模块 66 将通过除去掩码部分而获得的 URI（http://aaa.bbb.）注册成服务 ID。当 DB 访问模块 66 在步骤 S802 中确定没有掩码时，该过程继续到步骤 S803，其中 DB 访问模块 66 将 URI 本身（“http://aaa.bbb.ccc”）注册成服务 ID。

在步骤 S803 或 804 的过程之后，该过程继续到步骤 S805，其中通过使服务 ID 与用在对应于该服务 ID 的服务系统 24 中的个人相关信息相互关联，DB 访问模块 66 产生了与该服务 ID 相对应的 PMD。

由此，注册该服务 ID。

下面将参照图 10 对图 6 中的步骤 S282 或图 7 中的步骤 S482 中的服务 ID 匹配过程的细节进行描述。另外，在本示例中，服务 ID 匹配过程是由 DB 访问模块 66 来执行的。

在步骤 S841 中，DB 访问模块 66 获取 URI。在步骤 S842 中，DB 访问模块 66 将 URI 剪切成与服务 ID 的长度一样长。此时，当获取作为 URI 的“http://aaa.bbb.ccc”时，例如，http://aaa.bbb.这部分被切去。在步骤 S843 中，DB 访问模块 66 将在步骤 S842 中切去的 URI 与注册过的服务 ID 相比较。

在步骤 S844 中，DB 访问模块 66 确定该 URI 是否与步骤 S843 中作为比较结果的服务 ID 相匹配。当 DB 访问模块 66 确定该 URI 并不与服务 ID 匹配时，该过程继续到步骤 S846，其中 DB 访问模块 66 确定是否检查所有的已注册的 ID。当 DB 访问模块 66 确定所有的已注册的 ID 并没有被检查时，该过程继续到步骤 S847，其中 DB 访问模块 66 将在步骤 S842 中切去的 URI 与下一个服务 ID 相比较，然后返回到步骤 S844。

当 DB 访问模块 66 在步骤 S844 中确认该 URI 与步骤 S843 中作为比较结果的服务 ID 匹配时，该过程继续到步骤 S845，其中匹配的服务 ID 被视为用于识别服务系统 24 的服务 ID。

当 DB 访问模块 66 在步骤 S846 中确认所有的已注册 ID 都被检查过时，该过程继续到步骤 S848，其中 DB 访问模块 66 通知拒绝该服务。

由此，识别出该服务 ID。

如上所述，个人相关信息是作为 PMD 存储在 PK 22 中的。所期望的是，存储在 PK 22 内的 PMD 应该被加密并由此被隐藏，这样即便 PK 22 被偷也可防止 PK 22 被滥用。

例如，按要求，可以用 PK 22 的公共密匙来对 PMD 进行加密，并用私人密匙来解密。私人密匙存储在 SB 中。因此，当 PK 22 和 SB 之间的通信被中止时，私人密匙将不存在于该 PK 中，并因此无法读取或改变 PMD。

或者，PK 22 可以验证用户 20，这样仅当用户 20 被验证过时才可以使用该 PMD。

当在某段时间内用户没有通过一次性密码（或固定密码）的验证或生物测定验证时，例如，便可以禁止用于读取或改变 PMD 的控制，或可以自动擦除该 PMD。当该 PMD 被擦除并且用户通过了一次性密码或生物测定验证时，便使用存储在 pBase 23 中的 PMD 来重新存储 PK 22 的 PMD。

图 11 表示由 PK 22 来验证用户 20 的示例。图 11A 表示 PK 22 检测总由用户 20 携带的芯片 201 并验证该用户的一个示例。例如，芯片 201 是一个足够小的发射机，它时刻发出特定频率的无线电波，并且用户 20 总携带着它。假定存在这样的情况，PK 22 具有用于检测由芯片 201 发出的无线电波的传感器，并且该传感器连接到 PK 22 的输入单元 106。通过检测其频率预先注册过的、由芯片 201 发射的无线电波，PK 22 便可以验证用户 20。

参照图 12 将对 PK 22 验证用户 20 的第一验证过程进行描述。当 PK 22 处于状态 ON 时，便一直连续执行该过程。

在步骤 S901 中，PK 22 的 CPU 101 将由传感器检测到的信号与注册过的芯片 201 的信号进行比较。在步骤 S902 中，CPU 101 确定这些信号是否彼此匹配，并以此作为步骤 S901 中比较的结果。当 CPU 101 确定这些信号彼此并

不匹配时，该过程返回到步骤 S901。

当 CPU 101 在步骤 S902 中确定这些信号彼此匹配时，该过程继续到步骤 S903，其中用户验证信息被存储。此时，表示用户 20 已通过验证的信息作为用户验证信息与当前时间（日期和时间）一起被存储在存储单元 108 中。

在步骤 S904 中，CPU 101 确定预定时间（例如，一小时）是否已过去。CPU 101 待用，直到 CPU 101 确认预定的时间已过去。当 CPU 101 在步骤 S904 中确定预定的时间已过去时，该过程继续到 S905，其中 CPU 101 删除该用户验证信息。然后，该过程返回到步骤 S901 以便重复从步骤 S901 往下的过程。

或者，可以执行使用生物测定特征（指纹、声音印记、虹膜、步行模式等）的验证，即生物测定验证。图 11B 示出了通过检测作为用户 20 的生物测定特征的步行模式 202 来验证用户 20 的一个示例。假定存在这种情况，为 PK 22 提供了一个用于检测准静电场变化的传感器，并且该传感器连接到 PK 22 的输入单元 106。通过检测预先注册过的用户 20 的步行模式，PK 22 便可验证该用户 20。另外，步行模式是当人在步行时发生在人体上的准静电场的变化模式，并且这种模式可以被用来识别不同的人(例如,可参看特许公开号为 2003-58857 的日本专利“METHOD AND DEVICE FOR DETECTING WALK”）。

参照图 13 将对在这种情况下 PK 22 验证用户 20 的第二用户验证过程进行描述。当 PK 22 处于状态 ON 时，一直连续执行该过程。

在步骤 S921 中，PK 22 的 CPU 101 将由传感器检测到的准静电场的变化模式（步行模式）与注册用户的步行模式进行比较。在步骤 S902 中，CPU 101 确定这些步行模式是否彼此匹配，并将其作为步骤 S921 中比较的结果。当 CPU 101 确定这些步行模式并不彼此匹配时，该过程返回到步骤 S921。

当 CPU 101 在步骤 S922 中确定这些步行模式彼此匹配时，该过程继续到步骤 S923，其中用户验证信息被存储。此时，用于表示用户 20 已通过验证的的信息作为验证信息与当前时间（日期与时间）一起被存储。

在步骤 S924 中，CPU 101 确定预定的时间（例如，一个小时）是否已过去。CPU 101 待用直到 CPU 101 确定预定的时间已过去。当 CPU 101 在步骤 S924 中确定预定的时间已过去时，该过程继续到步骤 S925，其中 CPU 101 删除用户验证信息。然后，该过程返回到步骤 S921 以重复从步骤 S921 往下的过

程。

因此，PK 22 以预定时间的间隔验证用户 20。尽管在本示例中已描述的是用芯片 201 或步行模式 202 来验证用户 20，但用户验证方法并不限于此。例如，使 PK 22 与附近的个人计算机进行通信，并且可以基于从个人计算机输入的密码来验证该用户。

如上所述，当用户无法通过验证时，PK 22 可以自动擦除 PMD。参照图 14 将对这种情况下的 PMD 管理过程进行描述。每当在 PK 22 中要求 PMD 时，将执行该过程。另外，在执行之前，PK 22 的 CPU 101 检查在图 12 的步骤 S903 中或图 13 的步骤 S923 中存储的用户验证信息还存在于存储单元 108 中（即检查该用户已通过验证）。

在步骤 S941 中，CPU 101 与 pBase 23 进行通信以便从 pBase 23 中获取 PMD，并将 PMD 存储在存储单元 108 中。在步骤 S942 中，CPU 101 确定预定的时间（例如，三个小时）是否已过去，因为在步骤 S941 中已获取了 PMD。CPU 101 待用直到 CPU 101 确定预定的时间已过去。

当 CPU 101 在步骤 S942 中确定预定的时间已过去时，该过程继续到步骤 S943，其中 CPU 101 确定用户是否通过验证。此时，CPU 101 确定在图 12 的步骤 S903 或图 13 的步骤 S923 中存储的用户验证信息还存在于存储单元 108 中。当用户验证信息还在时，CPU 101 确定该用户已通过验证。当用户验证信息不在时，CPU 101 确定该用户未通过验证。当 CPU 101 在步骤 S943 中确定用户已通过验证时，该过程返回到步骤 S942 以重复从步骤 S942 往下的过程。

当 CPU 101 在步骤 S943 中确认该用户没有通过验证时，CPU 101 继续到步骤 S944 以擦除在步骤 S941 中从存储单元 108 中获取的 PMD。

因此，当 PK 22 无法验证该用户时，PMD 被自动擦除。

如上所述，PK 22 是用户可以很容易携带的小计算机。当各种接口（例如，显示器、触摸屏等）直接排列在 PK 22 上时，用户可能因为这种 PK 22 的大小和重量的增大就无法很容易地携带该 PK 22 了。

因此，所期望的是，直接排列在 PK 22 上的诸多接口应该尽可能的小，并且在 PK 22 外部的设备等应该作为输入或输入复杂信息的接口来使用。

图 15 示出了 PK 22 使用外部控制台 221 和外部控制台 222 作为输入或输

出的接口的一个示例。在这种情况下，PK 22 与外部控制台 221 和 222 进行像 RF 通信等无线通信。外部控制台 221 包括项目列表屏幕 242 以及按钮开关 241。例如，PMD 列表显示在项目列表屏幕 242 上。通过操作按钮开关 241，用户指定准许访问被显示在项目列表屏幕 242 上的 PMD。

外部控制台 222 具有带一个触摸屏的显示器 261。可以改变在带一个触摸屏的显示器 261 上显示的控制台，以便提供与服务 ID 相对应的不同的接口。

例如，外部控制台 221 和 222 可以被视为一个向 PK 22 提供接口服务的服务系统。在这种情况下，PK 22 与存储着用于作为服务系统的外部控制台 221 和 222 的控制代码的服务器进行通信，并由此获取用于外部控制台 221 和 222 的控制代码。之后，PK 22 与作为服务系统的外部控制台 221 和 222 进行通信，以便在外部控制台 221 和 222 中实现该控制代码。

如图 16 所示，通过经 PK 22 控制像服务系统 24 中的外部控制台 221 这样的外围设备，便可以在从服务系统 24 中隐藏像外围设备（外部控制台 221）地址这样的访问密匙 280 的同时接收服务。

下面将参看图 17 来描述 PK 22、pBase 23 以及服务系统 24 使用 PMD 的情况。如上所述，PK 22 通过像 RF 通信这样的无线通信、准静电场通信、光通信等与连接到互联网 21 上的访问点 25 进行通信，并因此连接到互联网 21 上。此时，如图 17A 所示，PK 22 和 pBase 23 通过互联网 21 而彼此相连，PK 22 和 pBase 23 的 PMD 内容彼此相互比较，并且进行 PMD 的同步化。例如，当更新 PK 22 的 PMD 内容时，pBase 23 的 PMD 也以相同的方式来更新，由此进行 PMD 的同步化。另外，PMD 的同步化细节将在下文中给予描述。

另外，例如，当所有的 PMD 无法存储在 PK 22 中时，PMD 可以存储在 pBase 23 中，使得如图 17B 所示，服务系统 24 将服务提供给查阅 pBase 23 中的 PMD 的 PK 22 的用户。

或者，如图 17C 所示，当 PK 22 无法连接到互联网 21 时，既然 pBase 23 存储 PK 22 的 PMD，那么用户可以通过使 pBase 23 与服务系统 24 而非 PK 22（通过用 pBase 23 替代 PK 22）进行通信来接收服务。在这种情况下，在服务系统 24 与 pBase 23 而非 PK 22 之间执行防欺骗过程以及 PMD 发送及接收。

参照图 18 和图 19，将对图 17C 中在 pBase 23 和服务系统 24 之间的流程

进行描述。假定在图 18 的示例中，与 PK 22（PK 22 的用户）相对应 PMD 存储在 pBase 23 的存储单元 128 的数据库中，并且像图 6 的情况那样在 pBase 23 与服务系统 24 之间使用密码验证作为防欺骗方法。

在相同的图中，pBase 23 确认服务系统 24 没有被欺骗，并且之后服务系统 24 确认 pBase 23 没有被欺骗。在 pBase 23 和服务系统 24 确认该服务系统 24 和该 pBase 23 都没有被欺骗时，便执行用于读取或改变 PMD 的过程。假定在本示例中 PK 密码、服务系统密码、PK 22 的用户 ID、以及服务系统 24 的服务 ID 也作为 PK 22 的 PMD 存储在 pBase 23 的存储单元 128 的数据库中。

在步骤 S1101 中，服务系统 24 将连接请求、服务 ID 以及密码发送到 pBase 23。这在步骤 S1121 中被接收。在步骤 S1122 中，pBase 23 执行在上文中参照图 10 描述过的服务 ID 匹配过程，并由此识别出该服务 ID。pBase 23 从存储单元 128 的数据库中读取与该服务 ID 相对应的服务密码、PK 密码、以及用户 ID。在步骤 S1123 中，pBase 23 将在步骤 S1121 中获取的服务密码与从存储单元 128 的数据库中读取的服务密码进行比较。当 pBase 23 确定这些服务密码并不彼此匹配时，pBase 23 确定该服务系统 24 可能被欺骗。pBase 23 将表示拒绝通信的拒绝信号传送到服务系统 24。这在步骤 S1102 中被收到。

由此，当开始通信时从服务系统 24 中没有发出与服务 ID 相对应的密码，在这种情况下，pBase 23 拒绝通信。

另一方面，当 pBase 23 在步骤 S1123 中确定这些服务密码彼此匹配时，pBase 23 在步骤 S1124 中向服务系统 24 发送用于表示已确认服务系统 24 未被欺骗的代码（OK）、用户 ID、以及与该用户 ID 相对应的 PK 密码。这在步骤 S1103 中被接收。

在步骤 S1104 中，服务系统 24 从服务系统 24 自身的数据库中读取在步骤 S1103 中接收到的、与用户 ID 相对应的 PK 密码，将所读取的 PK 密码与在步骤 S1103 中接收到的 PK 密码进行比较，并且确定这些 PK 密码是否彼此匹配。当服务系统 24 在步骤 S1104 中确认这些 PK 密码彼此并不匹配时，服务系统 24 确定 pBase 23 可能没有被欺骗。服务系统 24 将用于表示拒绝通信的拒绝信号发送到 pBase 23。这在步骤 S1125 中被接收。

由此，当开始通信时没有从 pBase 23 中发送出与用户 ID 相对应的密码，

在这种情况下，服务系统 24 拒绝通信。

另一方面，当服务系统 24 在步骤 S1104 中确认这些 PK 密码彼此匹配时，服务系统 24 确定 pBase 23 没有被欺骗。在步骤 S1105 中，服务系统 24 向 pBase 23 发送读取 PMD 的请求。这在步骤 S1126 中被接收。在步骤 S1127 中，pBase 23 检查由服务系统 24 请求读取的 PMD 是否与对应于服务系统 24 的服务 ID 相一致，以及是否被允许读取。当该 PMD 被允许读取时，pBase 23 从存储单元 128 的数据库中读取该 PMD。在步骤 S1128 中，pBase 23 将所读取的 PMD 发送到服务系统 24。这在步骤 S1106 中被接收。

在步骤 S1107 中，服务系统 24 基于在步骤 S1106 中接收到的 PMD 执行各种过程（与过程相对应的服务）。当作为步骤 S1107 中的过程的结果需要改变 PMD 时，服务系统 24 在步骤 S1108 中改变 PMD 的内容，并将该内容发送到 pBase 23。这在步骤 S1129 中被接收。在步骤 S1130 中，pBase 23 检查在步骤 S1129 中接收到的 PMD 是否与对应于服务系统 24 的服务 ID 相一致，以及是否被允许改变。当 PMD 被允许改变时，在存储单元 128 的数据库中相应的 PMD 便被改变（被更新成已改变过的内容）。

由此，既然如图 6 所示的情况那样在读取或改变 PMD 之前可以在服务系统 24 与 pBase 23 而非 PK 22 之间检查是否欺骗，那么便可以提供安全的服务。

下面将参照图 19 对图 17C 所示的、在 pBase 23 和服务系统 24 之间另一个过程示例进行描述。假定在这种情况下与 PK 22（PK 22 的用户）相对应的 PMD 存储在 pBase 23 的存储单元 128 中，并且如图 7 所示的那样在 pBase 23 和服务系统 24 之间使用用公共密匙来加密的信息的验证作为防电子欺骗方法。

在相同的图中，pBase 23 确认服务系统 24 没有被欺骗，并且之后服务系统 24 确认 pBase 23 没有被欺骗。在 pBase 23 和服务系统 24 确认该服务系统 24 和该 pBase 23 都没有被欺骗时，便执行用于读取或改变 PMD 的过程。假定在本示例中 pBase 23 和服务系统 24 具有用像 RSA 等公共密匙系统的加密算法来加密或解密信息的功能。另外，假定 PK 22 的私人密匙、服务系统 24 的公共密匙、PK 22 的用户 ID、以及服务系统 24 的服务 ID 都作为 PK 22 的 PMD 存储在 pBase 23 的存储单元 128 的数据库中。

在步骤 S1861 中，服务系统 24 将连接请求和服务 ID 发送到 pBase 23。这

在步骤 S1881 中被接收。在步骤 S1882 中，pBase 23 以上文参照图 10 所描述的方式来执行服务 ID 匹配过程，并由此识别该服务 ID。pBase 23 获取与该服务 ID 相对应的用户 ID、服务系统 24 的公共密匙、以及 PK 22 的私人密匙。

在步骤 S1883 中，为验证服务系统 24，pBase 23 产生由预定的代码构成的询问代码，用对应于该服务 ID 的公共密匙（服务系统 24 的公共密匙）来加密该询问代码，并将已加密的询问代码或用户 ID 发送到服务系统 24。这在步骤 S1862 中被接收。

在步骤 S1863 中，服务系统 24 用该服务系统 24 的私人密匙来解密在步骤 S1862 中接收到的经加密过的询问代码，将解密过的询问代码设置成响应代码，用对应于该用户 ID 的公共密匙来加密响应代码，并将加密过的响应代码发送到 pBase 23。这在步骤 S1884 中被接收。

在步骤 S1885 中，pBase 23 用 PK 22 的私人密码来解密在步骤 S1884 中接收到的经加密过的响应代码，并将解密过的响应代码与在步骤 S1883 中产生的询问代码进行比较，以确认询问代码与响应代码彼此是否匹配。当 pBase 23 确认询问代码与响应代码并不匹配时，pBase 23 确定服务系统 24 没有被欺骗。pBase 23 将用于表示拒绝通信的拒绝信号传送给服务系统 24。这在步骤 S1864 中被接收。

因此，当开始通信时从 pBase 23 中发送出询问代码。当从服务系统 24 中没有返回与询问代码相匹配的响应代码时，pBase 23 便拒绝该通信。

另一方面，当 pBase 23 在步骤 S1885 中确定询问代码与响应代码彼此匹配时，pBase 23 在步骤 S1886 中向服务系统 24 发送用于表示已确认服务系统 24 没有被欺骗的代码（OK）。这在步骤 S1865 中被接收。

在步骤 S1866 中，为验证 pBase 23（PK 22），服务系统 24 产生由预定的代码构成的询问代码，用对应于该用户 ID 的公共密匙（PK 22 的公共密匙）来加密询问代码，并将加密过的询问代码发送到 pBase 23。这在步骤 S1887 中被接收。

在步骤 S1888 中，pBase 23 用 PK 22 的私人密匙来解密在步骤 S1887 中接收到的询问代码，将解密过的询问代码设置成响应代码，用对应于服务 ID 的公共密匙来加密响应代码，并将加密过的响应代码发送到服务系统 24。这在步

骤 S1867 中由服务系统 24 来接收。

在步骤 S1868 中，服务系统 24 用该服务系统 24 的私人密匙来解密在步骤 S1867 中接收到的经加密过的响应代码，并确定解密过的响应代码是否与在步骤 S1866 中产生的询问代码相匹配。当服务系统 24 确定询问代码并不与响应代码相匹配时，服务系统 24 确定 pBase 23 可能被欺骗了。服务系统 24 向 pBase 23 发送用于表示拒绝通信的拒绝信号。这在步骤 S1889 中被接收。

因此，当开始通信时从服务系统 24 中发送出询问代码。当从 pBase 23 中没有返回与询问代码相匹配的响应代码时，服务系统 24 便拒绝通信。

另一方面，当服务系统 24 在步骤 S1868 中确定询问代码与响应代码彼此匹配时，服务系统 24 确定已确认 pBase 23 并没有被欺骗。在步骤 S1869 中，服务系统 24 向 pBase 23 发送读取 PMD 的请求。这在步骤 S1890 中被接收。在步骤 S1891 中，pBase 23 检查由服务系统 24 请求读取的 PMD 是否与对应于该服务系统 24 的服务 ID 相一致，以及是否允许被读取。当 PMD 允许被读取时，pBase 23 从存储单元 128 的数据库中读取该 PMD。在步骤 S1892 中，pBase 23 将所读取的 PMD 发送到服务系统 24。这在步骤 S1870 中由服务系统 24 来接收。

在步骤 S1871 中，服务系统 24 基于在步骤 S1870 中接收到的 PMD 来执行各种过程（与过程相对应的服务）。当作为步骤 S1871 中过程的结果需要改变 PMD 时，服务系统 24 在步骤 S1872 中改变该 PMD 的内容，并将这些内容发送到 pBase 23。这在步骤 S1893 中被接收。在步骤 S1894 中，pBase 23 检查在步骤 S1893 中接收到的 PMD 是否与对应于服务系统 24 的服务 ID 相一致，以及是否允许被改变。当 PMD 允许被改变时，在存储单元 128 的数据库中相应的 PMD 便被改变（被更新成已改变过的内容）。

因此，既然在读取或改变 PMD 之前像图 7 的情况那样在服务系统 24 与 pBase 23 而非 PK 22 之间检查欺骗与否，那么便可以提供安全的服务。另外，在参照图 19 所作的示例描述中，询问代码和响应代码是用公共密匙系统的加密算法来加密的，但询问代码和响应代码也可以用普通密匙系统的加密算法来加密。

图 20A 到 20C 示出了 PMD 组成的详细示例。如上所述，相同的图中所示的 PMD 是一组与服务 ID（例如，服务 ID 1）相互关联的元数据。在 PMD 中

所描述的是作为识别信息的诸多属性以及这些特性的内容，这些属性用于识别元数据。属性“姓名”表示被提供给与服务 ID 1 相对应的服务系统 24 的用户 ID，并且“foo”被描述成属性的内容。

图 20A 中的属性“防电子欺骗方法”表示与对应于服务 ID 1 的服务系统 24 一起执行的防电子欺骗过程的方法，并且“公共密匙系统”被描述成属性的内容。属性“防电子欺骗方法”对应于在图 5 的步骤 S82 中产生的确认代码。属性“服务公共密匙”表示与服务 ID 1 相对应的服务系统 24 的公共密匙，并且密匙数据被描述成属性的内容。属性“PK 私人密匙”表示 PK 22 的私人密匙，并且密匙数据被描述成属性的内容。

如图 20B 所示，当“普通密匙系统”被描述成属性“防电子欺骗方法”的内容时，属性“普通密匙”便产生于 PMD 中以替代属性“服务公共密匙”和属性“PK 私人密匙”，并且密匙数据被描述成属性的内容。如图 20C 所示，当“密码系统”被描述成属性“防电子欺骗方法”的内容时，属性“服务密码”和属性“PK 密码”便产生于 PMD 中以替代属性“服务公共密匙”和属性“PK 私人密匙”，并且服务密码和 PK 密码被分别描述成属性的内容。

属性“行动”表示由与服务 ID 1 相对应的服务来执行的处理程序，并且程序被描述成属性的内容。属性“程序偏好信息”表示在与服务 ID 1 相对应的服务中使用的用户偏好信息，并且“体育 10、杂耍表演 7、音乐 5、及其它 3”被描述成属性的内容。

访问控制描述与属性内容相对应的访问控制信息。控制信息是为每个属性设置的。控制信息是由预定数目的比特构成的代码，并且按下述来设置。

第一比特所作出的设置用于表示，是否准许读取对应于服务 ID 1 的服务中的属性内容。第二比特所作出的设置用于表示，是否准许改变对应于服务 ID 1 的服务中的属性内容。第三比特所作出的设置用于表示，是否准许读取对应于除服务 ID 1 之外的服务 ID 的服务中的属性内容。第四比特所作出的设置用于表示，是否准许改变对应于除服务 ID 1 之外的服务 ID 的服务中的属性内容。

另外，可以提供用于设置表示是否准许执行程序的比特、用于设置允许自由访问（不限于访问）的比特等。另外，在访问控制下的控制信息可以作为访问准许信息来共同存储（图 4）。

下面将参照图 21 来描述 PMD 更新过程。当服务系统 24 提供内容观看服务时，该过程是由服务系统 24 来执行的，像是图 6 的步骤 S207 或图 7 的步骤 S411 中的一种服务相应处理过程。

在步骤 S1901 中，CPU 121 获取观看到的节目（内容）的元数据。在步骤 S1902 中，CPU 121 分析该元数据的类型。在步骤 S1903 中，CPU 121 确定在步骤 S1902 中分析的类型是否是体育。当 CPU 121 确定该类型是体育时，CPU 121 继续到步骤 S1904 以便在 PMD 的属性“节目偏好信息”的内容中增大体育的点数。例如，图 20 中的“体育 10、杂耍表演 7、音乐 5、及其它 3”变为“体育 11、杂耍表演 7、音乐 5、及其它 3”。

当 CPU 121 在步骤 S1903 中确定在步骤 S1902 中分析的类型不是体育时，CPU 121 在步骤 S1905 中确定该类型是否是杂耍表演。当 CPU 121 确定该类型是杂耍表演时，CPU 121 继续到步骤 S1906 以便在 PMD 的属性“节目偏好信息”的内容中增大杂耍表演的点数。例如，图 20 中的“体育 10、杂耍表演 7、音乐 5、及其它 3”变为“体育 10、杂耍表演 8、音乐 5、及其它 3”。

当 CPU 121 在步骤 S1905 中确定在步骤 S1902 中所分析的类型不是杂耍表演时，CPU 121 在步骤 S1907 中确认该类型是否是音乐。当 CPU 121 确定该类型是音乐时，CPU 121 继续到步骤 S1908 中以便在 PMD 的属性“节目偏好信息”的内容中增大音乐的点数。例如，图 20 中的“体育 10、杂耍表演 7、音乐 5、及其它 3”变为“体育 10、杂耍表演 7、音乐 6、及其它 3”。

当 CPU 121 在步骤 S1907 中确认在步骤 S1902 中所分析的类型不是音乐时，CPU 121 继续到步骤 S1909 以便在 PMD 的属性“节目偏好信息”的内容中增大其它的点数。例如，例如，图 20 中的“体育 10、杂耍表演 7、音乐 5、及其它 3”变为“体育 10、杂耍表演 7、音乐 6、及其它 4”。

PMD 便是由此在服务系统 24 中获得更新的。更新过的 PMD 被发送到 PK 22，然后 PK 22 的 PMD 便获得更新。

尽管在上面描述的示例中服务系统 24 执行 PMD 更新过程并且 PK 22 的 PMD 作为该更新的响应也被更新，但是 PK 22 可以执行 PMD 更新过程。或者，pBase 23 可以执行 PMD 更新过程，并且 PK 22 的 PMD 与 pBase 23 的 PMD 是同步化的。

通过将用在不同服务中的 PMD 的内容组合起来，有可能产生新的 PMD。假定与服务 ID 1 相对应的服务以及与服务 ID 2 相对应的服务都提供涉及音乐的内容，并且如图 22 所示在对应于服务 ID 1 的 PMD 301 和对应于服务 ID 2 的 PMD 302 中有属性“R&B”、属性“爵士”以及属性“POP”。

在这种情况下，PMD 301 和 PMD 302 彼此组合起来以产生新的 PMD 303。此时 PMD 301 的属性“R&B”的内容（15）与 PMD 302 的属性“R&B”的内容（17）添加在一起，这样在新的 PMD 303 中属性“R&B”的内容便设置成“32（＝17＋15）”。相似的是，在新的 PMD 303 中属性“爵士”的内容便设置成“10（＝5＋5）”，并且在新的 PMD 303 中属性“POP”的内容便设置成“15（＝15＋0）”。

由此产生的新的 PMD 303 是作为与多个音乐提供服务的服务 ID 相对应的 PMD 而产生的，并被当作 PK 22 的用户的音乐偏好信息来使用。

通过将多个 PK 22 的 PMD 内容组合起来，服务系统 24 也有可能产生新的 PMD。图 23 示出了这种情况下的一个示例。存在使用一个服务系统 24（或 pBase 23）的多个 PK，比如 PK 22-1 和 PK 22-2。在 PK 22-1 的 PMD 321 和 PK 22-2 的 PMD 322 中，有属性“R&B”、属性“爵士”以及属性“POP”。在这种情况下，服务系统 24（或 pBase 23）通过将 PMD 321 和 PMD 322 彼此组合起来来产生新的新的 PMD 323。

此时，PMD 321 的属性“R&B”的内容（15）与 PMD 322 的属性“R&B”的内容（17）相加在一起，所以在新的 PMD 323 中属性“R&B”的内容被设置成“32（＝17＋15）”。相似的是，在新的 PMD 323 中属性“爵士”的内容被设置成“10（＝5＋5）”，而在新的 PMD 323 中属性“POP”的内容被设置成“15（＝15＋0）”。

由此产生的新的 PMD 303 是作为多个用户共同的 PMD 而产生的，并被提供给其偏好信息并未存储过的那个 PK 22 的用户。

有可能从另一种设备而非 PK 22 中来使用服务系统 24。在这种情况下，如图 24 所示，用户 20 使 PK 22 与该用户 20 所指定的终端 362 进行通信以便将内容服务分组 361 发送到终端 26。然后，终端 362 与服务系统 24 进行通信。内容访问分组 361 是这样一种分组，其中收集有与服务系统 24 进行通信所必

需的信息。例如，内容访问分组 361 包括像内容 URI 等用于识别内容的唯一的 ID、由简单图像构成的图标、涉及内容的字符串等、在终端 362 和服务系统 24 之间执行防电子欺骗过程所使用的 PK 验证信息（例如，PK 22 的私人密匙、用户 ID 等）、以及服务验证信息（例如，服务系统 24 的公共密匙，服务 ID 等）。

由此，用户可以使用终端 362，好像终端 362 就是 PK 22 一样（作为虚拟 PK）。

下面将参照图 25 到 27 来描述在信息设备中使用 PMD 来反映一个人的偏好信息的示例（在下文中这种反映被称为个性化）。在图 25 中，PK 22 的用户 20 使用用来基于预定的音乐数据来再现音乐的音乐再现设备 381，以及连接到互联网 21 以便于 Web 浏览等的个人计算机 382。

通过使用 PK 22 的 PMD，用户 20 可以使音乐再现设备再现用户最喜欢的音乐。在这种情况下，PK 22 通过无线通信等与音乐再现设备 381 进行通信而无需互联网 21 的介入，其中音乐再现设备 381 是用作一个服务系统。此时，在 PK 22 和音乐再现设备 381 之间执行图 6 或图 7 所表示的过程。此时，例如，在图 7 的步骤 S409 中，读取音乐偏好信息的 PMD 的一则请求被从音乐再现设备 381 发送到 PK 22。在步骤 S504 中，音乐偏好信息的 PMD 被从 PK 22 发送到音乐再现设备 381。然后，当在步骤 S410 中音乐再现设备 381 从 PK 22 中获取 PMD 时，作为步骤 S411 中的服务对应过程，执行对用户最喜欢的音乐进行再现的过程。参照图 26 将描述在这种情况下音乐再现设备 381 的音乐再现过程。

在步骤 S1921 中，音乐再现设备 381 从 PK 22 中获取 PMD。在步骤 S1922 中，音乐再现设备 381 分析在步骤 S1921 中获取的 PMD 中的偏好信息。在步骤 S1923 中，音乐再现设备 381 再现与该偏好信息相对应的音乐。

通过将包括偏好信息的 PMD 发送到音乐再现设备 381，便可以再现最喜欢的音乐。既然 PMD 被存储在 PK 22 中并且因此可以被携带到各种地方，那么现场的音乐再现设备可以被个性化地设置成再现某人最喜欢的音乐的音乐再现设备。

通过使用 pBase 23 的 PMD，图 25 中的用户 20 也可以使个人计算机 382

显示该用户最喜欢的 Web 页。在这种情况下，PK 22 通过互联网 21 与服务系统 24-10 进行通信。此时，在 PK 22 和服务系统 24-10 之间执行图 6 或图 7 所示的过程。然后，服务系统 24-10 基于 PK 22 的用户 ID 来识别存储着用户 20 的 PMD 的 pBase 23，并从 pBase 23 中获取用户 20 的 PMD。此时，在服务系统 24-10 与 pBase 23 之间执行如图 18 或 19 所示的过程。例如，在图 19 的步骤 S1869 中，读取 Web 偏好信息的 PMD 的一则请求被从服务系统 24-10 发送到 pBase 23。在步骤 S1891 中，Web 偏好信息的 PMD 被从 pBase 23 发送到服务系统 24-10。

当服务系统 24-10 在步骤 S1870 中从 pBase 23 中获取 PMD 时，服务系统 24-10 执行将适合用户口味的 Web 服务提供给个人计算机 382 的过程，就像步骤 S1871 中的服务相应处理过程那样。参照图 27 将描述在这种情况下服务系统 24-10 的 Web 信息提供过程。

在步骤 S1941 中，服务系统 24-10 获取 PK 22 的用户 ID。在步骤 S1942 中，服务系统 24-10 从 pBase 23 中获取与在步骤 S1941 中获取的用户 ID 相对应的 PMD。在步骤 S1943 中，服务系统 24-10 分析在步骤 S1942 中获取的 PMD 的偏好信息。在步骤 S1944 中，服务系统 24-10 提供与该偏好信息相对应的 Web 服务。

或者，由服务系统 24-10 在用户的个人计算机 382 中创建的作为文本文件的点心文件可以作为 PK 22 或 pBase 23 中的 PMD 来存储，并且每当执行 Web 浏览时该点心文件便可以被发送到个人计算机 382 上。

由此便提供了 Web 服务。因其体积较大而无法存储的 PMD 可存储在 pBase 23 中，并且像个人计算机等信息设备可以基于 pBase 23 的 PMD 来个性化处理。结果，可以执行能更为准确反映用户偏好的个性化处理。

参照图 28 将描述使用 PMD 对信息设备进行个性化处理的另一个示例。在相同的图中，三个用户 20-1 到 20-3 住在房屋 400 中。用户 20-1 到 20-3 分别拥有 PK 22-1 到 22-3。房屋 400 有三个房间：客厅 400-1；厨房 400-2；以及儿童的房间 400-3。获取像各种图像或音乐这样的数据（内容）并存储或再现这些内容的内容寄存器 421-1 到 421-3 被安装在各个房间。

内容寄存器 421-1 到 421-3 通过 LAN 402 连接到路由器 403 中。内容寄存

器 421-1 到 421-3 通过路由器 403 与连接到互联网 21 上的各种服务器进行通信以获取各种内容。

内容寄存器 421-1 到 421-3 具有用于检测步行模式的传感器。当用户通过传感器时，该传感器检测步行模式以识别用户。路由器 403 具有防火墙功能，用于防止来自互联网 21 的未经授权的访问，它还具有用于存储预定数据量的存储单元。LAN 402 与支架 401 相连，诸多 PK 安装在支架上以便充电。支架 401 将被安装的 PK 的信息发送到路由器 403。

当用户 20-1 到 20-3 外出时，用户 20-1 到 20-3 携带着 PK 22-1 到 22-3，当返回房屋 400 时就把他们的 PK 安装到支架 401 上。当 PK 22-1 到 22-3 安装在支架 401 上时，支架 401 将 PK 22-1 到 22-3 的 PMD 发送到路由器 403。路由器 403 通过互联网 21 与 Pbse 23 进行通信以便从 Pbse 23 中获取用户 20-1 到 20-3 的 PMD，并将用户 20-1 到 20-3 的 PMD 存储在存储单元中。另外，假定关于用户 20-1 到 20-3 的偏好与步行模式的偏好信息与步行模式信息存储在用户 20-1 到 20-3 的 PMD 中。

内容寄存器 421-1 到 421-3 从路由器 403 中获取关于用户 20-1 到 20-3 的步行模式的步行模式信息，并再现适合附近的用户口味的内容。例如，当用户 20-2 在厨房时，用来检测用户 20-2 的步行模式 202-2 的内容寄存器 421-2 从路由器 403 中获取用户 20-2 的 PMD，分析该偏好信息，并在存储于内容寄存器 421-2 内的诸多内容中再现与偏好信息相对应的音乐等。

当用户 20-1 到 20-3 位于客厅 400-1 时，内容寄存器 421-1 检测用户 20-1 和 20-3 的步行模式 202-1 和 202-3，从路由器 403 中获取用户 20-1 的 PMD 以及用户 20-3 的 PMD，分析用户 20-1 的 PMD 和用户 20-3 的 PMD 的偏好信息，并在存储于内容寄存器 421-1 内的诸多内容中再现适合用户 20-1 口味的音乐以及适合用户 20-3 口味的视频。

尽管在本示例中，已描述过内容寄存器 421-1 到 421-3 是个性化的，但各种 CE 设备等是可以用相似的方法来个性化处理的，并且用户可以通过使用 PK 使想要的设备个性化。

既然如上所述路由器 403 具有防火墙功能，那么在连接到 LAN 402 上的设备与连接到互联网 21 上的设备之间的通信便是受限的（例如，可用在内容寄

存器与 pBase 之间的通信中的协议（端口号）是受限的）。因此，如图 29 所示，在连接到 LAN 402 的设备与互联网 21 之间进行通信。首先，如从内容寄存器 421-1 到 pBase 23 的箭头 441 所示，使用 https（SSL）协议开始会话。在建立会话之后，如虚线 442 所示，内容寄存器 421-1 和 pBase 23 使用 https 协议进行通信。

另外，如上文参照图 17A 所描述的那样，在 PK 22-1 到 22-3 与 pBase 23 之间执行 PMD 同步化。在图 28 的示例中，PMD 同步化是通过支架 402 和内容寄存器 421-1 到 421-3 来执行的。参照图 30 将描述在 PK 22-1、支架 401、pBase 23 以及内容寄存器 421-1 之间执行 PMD 同步化时的流程。

在步骤 S2001 中，当 PK 22-1 被安装在支架 401 上时，PK 22-1 将 PK 22-1 自身的 PMD 内容发送到支架 401。这在步骤 S2021 中被接收。在步骤 S2022 中，支架 401 将在步骤 S2021 中接收到的信息发送到 pBase 23。这在步骤 S2041 中被接收。在步骤 S2042 中，pBase 23 执行随后将参照图 31 加以描述的 PMD 同步过程。由此，存储在 pBase 23 中的 PMD 获得更新，并且产生了用于更新 PK 22-1 的 PMD 的同步化数据。

在步骤 S2043 中，pBase 23 将同步化数据发送到支架 401。这在步骤 S2023 中被接收。在步骤 S2024 中，支架 401 将在步骤 S2023 中接收到的信息发送到 PK 22-1。这在步骤 S2002 中被接收。然后，在步骤 S2003 中，PK 22-1 基于在步骤 S2002 中接收到的同步化数据来更新 PK 22-1 的 PMD，由此，PK 22-1 的 PMD 便与 pBase 23 的 PMD 同步化了。

当内容寄存器 421-1 再现内容时，内容寄存器 421-1 在步骤 S2061 中向 pBase 23 发送历史信息，比如内容观看的历史等。这在步骤 S2044 中被接收。pBase 23 基于该历史信息更新 PMD 的偏好信息。在步骤 S2045 中，pBase 23 将更新 PMD 的结果作为同步数据发送到支架 401。这在步骤 S2025 中被接收。在步骤 S2026 中，支架 401 将在步骤 S2025 中接收到的信息发送到 PK 22-1。这在步骤 S2003 中被接收。在步骤 S2005 中，更新 PK 22-1 的 PMD。

由此执行 PMD 同步化。

下面将参照图 31 描述图 30 的步骤 S2042 中 PMD 同步化过程的诸多细节。

在步骤 S2081 中，CPU 121 将在图 30 的步骤 S2041 中接收到的 PMD 的内

容与存储在 pBase 23 中的内容进行比较。此时，每次从存储在 pBase 23 内要被比较的 PMD 中提取一条与接收到的 PMD 相对应的 PMD，并且当比较上一次更新的 PMD 时更新表示日期和时间的日期和时间信息。

在步骤 S2082 中，CPU 121 确定在步骤 S2041 中接收到的 PMD 的更新日期和时间是否比存储在 pBase 23 中的 PMD 的更新日期和时间要新。当 CPU 121 确定所接收到的 PMD 的更新日期和时间比存储在 pBase 23 中的 PMD 的更新日期和时间要新时，CPU 121 继续到步骤 S2083 以便将存储在 pBase 23 中的 PMD 的内容更新为接收到的 PMD 的内容。

另一方面，当 CPU 121 在步骤 S2082 中确定在步骤 S2041 中接收到的 PMD 的更新日期和时间并不比存储在 pBase 23 中的 PMD 的日期和时间新时，CPU 121 继续到步骤 S2084 以便将存储在 pBase 23 中的 PMD 的内容设置成同步数据。在 PMD 同步化过程结束之后，在步骤 S2043（图 30）中这种同步化数据被发送到 PK 22-1。PK 22-1 便基于该同步化数据更新 PMD。

在步骤 S2083 或 S2084 的过程之后，CPU 121 在步骤 S2085 中确定是否对所有的 PMD 进行检查。当 CPU 121 确定并非所有的 PMD 被检查过时，CPU 121 继续到步骤 S2086 已检查下一个 PMD。之后，该过程返回到步骤 S2081 以便重复从步骤 S2081 往下的过程。

当 CPU 121 在步骤 S2085 中确定所有的 PMD 都被检查过了时，该过程便结束了。

由此在 pBase 23 中执行了 PMD 同步化。

下面将参照图 32 描述将各种卡片信息存储在 PK 中并使用该信息的示例。假定在本示例中具有卡片信息的 PMD 461 存储在 PK 22 中。当用户 20 进行购物时，例如，PK 22 通过无线通信等与收银机 481 进行通信，所以由收银机 481 来获取 PMD 461 的信息。PMD 461 包括用于描述卡片 1 到 N 的卡片号码的卡片信息，比如由用户 20 所保留的信用卡等。此时，在 PK 22 和收银机 481 之间执行图 6 或图 7 所示的过程，其中收银机 481 用作服务系统。然后，收银机 481 与通过互联网 21 与用于执行购物账单付款等的卡片处理服务器 483 进行通信，并由此付清账单。

例如，像预付卡的剩余金额、卡片使用历史等信息都存储在通过互联网 21

连接到卡片处理服务器 483 的其它服务器的数据库 482-1 到 482-N。在付清账单之后，卡片处理服务器 483 更新数据库 482-1 到 482-N 的内容。

因此，当使用 PK 22 作为虚拟卡容器时，可以将各种卡片一起放在卡片容器中，并且必要时可以提取并使用这些卡片。另外，可以为 PK 22 提供读卡器功能，这样读取卡片信息并将内容发送到 PK 22 附近的收银机 481 中。

下面将参照图 33 来描述在使用 PK 的用户附近控制多个设备的一个示例。在相同的图中，同时携带着 PK 22 和具有带触摸屏的显示器 521 的控制台终端 521 的用户 20 进入在其中安装有投影仪 503 的会议室。访问点 25 安装在该会议室中。访问点 25 连接到互联网 21。互联网 21 连接到保留控制信息的环境服务器 501，该控制信息用于控制像在访问点 25 附近存在的投影仪 503 等设备。用户 20 通过使用 PK 22 来获取用于控制投影仪 503 的控制代码，并通过操作控制台终端 521 来控制投影仪 503。

参照图 34 将描述此时从环境服务器中获取投影仪 503 的控制代码的流程。在步骤 S2121 中，PK 22 通过无线通信等与控制台终端 502 进行通信以便将一则对设备信息的请求发送到控制台终端 502。这在步骤 S2101 中被接收。在步骤 S2102 中，控制台终端 502 将控制台终端 502 自身的设备信息发送到 PK 22。这在步骤 S2122 中被接收。

当用户进入会议室时，PK 22 通过无线通信等与访问点 25 进行通信，并且通过访问点 25 与环境服务器 501 进行通信。此时，在 PK 22 与环境服务器 501 之间执行图 6 或图 7 所示的处理过程，其中环境服务器 501 用作服务系统。然后在步骤 S2123 中，PK 22 将获取控制代码的一则请求发送到环境服务器 501，其中控制台终端 502 的设备信息用作一条 PMD。这在步骤 S2141 中被接收。在步骤 S2142 中，环境服务器 501 将要被安装到控制台终端 502 中的投影仪 503 的控制代码添加到 PMD，并将该 PMD 发送到 PK 22。这在步骤 S2124 中被接收。

之后，在 PK 22 与控制台终端 502 之间执行图 6 或图 7 所示的过程，其中控制台终端 502 用作服务系统。然后，在步骤 S2125 中，PK 22 将在步骤 S2124 中接收到的 PMD 发送到控制台终端 502。这在步骤 S2103 中被接收。投影仪 503 的代码被安装在控制台终端 502 中。用户 20 通过操作带触摸屏的显示器

521 来控制投影仪 503。

因此，通过使用 PK，可控制在用户附近的设备。通过选择并发送与附近的设备相对应的合适的控制代码或数据等，各种设备都可以适当地受到控制。

作为控制使用 PK 的用户附近的设备的另一个示例，有可能像图 35 所示的那样打开和关上房门。在本实施例中，有房门 543 和房门打开控制器 542，该控制器用于通过使访问点 25 附近的房门 543 开锁而打开房门 543。房门打开控制器 542 通过互联网 21 连接到用于存储房门打开控制器 542 的控制代码的服务器 541。

当用户 20 进入可能与访问点 25 进行通信的区域 41 时，便执行图 6 或图 7 所示的过程，其中服务器 541 用作服务系统。由用户 20 携带的 PK 22 通过访问点 25 与连接到互联网 21 上的服务器 541 进行通信。服务器 541 控制房门打开控制器 542 以便使房门打开控制器 542 打开房门 543。

在这种情况下，例如，像用于识别用户 20（PK 22）附近房门 543 的 ID 等信息作为 PMD 被发送到服务器 541。服务器 541 基于接收到的 PMD 来识别房门 543，并将用于使房门打开控制器 542 打开房门 543 的控制代码发送到房门打开控制器 542。

因此，当用户 20 靠近房门 543 附近的访问点 25 时，房门 543 可以自动打开。另外，既然在 PK 22 和服务器 541 之间执行图 6 或图 7 所示的防电子欺骗过程，那么便可防止未经授权的入侵者打开房门 543。

另外，当在房门 543 附近有一个守卫的房间并且该守卫一直在看守以便防止未经授权的入侵者进入房门 543 时，通过将包括 ID 号码和面孔照片数据的 PMD 发送到守卫的房间里的个人计算机 562 并像图 36 所示的那样在个人计算机 562 上显示与该 PMD 相对应的面孔照片时，安全性可以进一步提高。因此，与 PK 22（用户 20）的 PMD 相对应的面孔照片便显示在个人计算机 562 上。因此，即便当未经授权的入侵者使用偷来的 PK 22 试图从房门 543 中入侵时，该入侵者无法从房门 543 中入侵，因为守卫可以辨别该入侵者不是其面孔已被显示的那个人（该入侵者不是用户 20）。

参照图 37 将描述使用 PK 和外围设备进行会话的一个示例。假定在本示例中，用户 20-2 期望与具有 PK 22-1 的用户 20-1 会话。假定 PK 22-1 以预定的时

间间隔与 pBase 23 进行通信，并且 PMD 同步化过程是像参照图 31 所描述的那样进行。

访问点 25、电话 581、以及用于视频会议的照相机 582 和显示器 583 存在于用户 20-1 附近。存储着用于电话 581 到显示器 583 的控制代码的环境服务器 584 连接到互联网 21。此外，互联网 21 连接到 pBase 23 和提供会话连接服务的会话连接服务器 601。会话连接服务器 601 接收从用户（例如，用户 20-2）到其它端处特定的人（例如，用户 20-1）的会话连接请求，通过使用在其它端处的那个人的外围设备来提供对话。

参照图 38 将描述在这种情况下作出会话连接的流程。PK 22-1 执行如图 6 或 7 所示的过程，其中像照相机 582 到显示器 583 这样的外围设备用作服务系统以便与外围设备进行通信。在步骤 S2221 中，PK 22-1 向外围设备发送对设备信息的请求。这在步骤 S2201 中被接收。在步骤 S2202 中，像照相机 582 到显示器 583 这样的外围设备将像外围设备自身的 ID、地址等设备信息作为 PMD 发送到 PK 22-1。这在步骤 S2222 中被接收。在步骤 S2223 中，所接收到的 PMD 作为用于表示用户 20-1 可用设备的 PMD 被发送到 pBase 23。这在步骤 S2241 中被接收（在 PK 22-1 与 pBase 23 之间执行 PMD 同步化）。

当从用户 20-2 中接收到与用户 20-1 进行会话连接的一则请求时，会话连接服务器 601 在步骤 S2261 中将会话请求发送到保留 PMD 的 pBase 23，该 PMD 与用户 20-1 相对应。这在步骤 S2242 中被接收。此时，执行图 6 或图 7 所示的过程，并在会话连接服务器 601 与 pBase 23 之间进行通信，其中会话连接服务器 601 用作服务系统并且 pBase 23 替代（用作）PK 22-1。然后，在步骤 S2243 中，pBase 23 将表示用户 20-1 可用设备的 PMD 发送到会话连接服务器 601。

在步骤 S2263 中，会话连接服务器 601 通过环境服务器 584 来控制外围设备，所以在用户 20-1 和用户 20-2 之间执行使用电话 581 的会话或使用照相机 582 及显示器 583 的视频会议。因此，通过使用 PK，执行使用外围设备的会话。因此，即便当用户 20-1 来到另一个地方，仍然可以基于用于表示用户 20-1 的可用设备的 PMD 来进行会话。另外，既然以预定时间间隔在 PK 22-1 与 pBase 23 之间执行 PMD 同步化，那么用户可以使用外围设备在任何时间及任何地点进行会话。

下面参照图 39 将描述确定使用 PK 的用户的当前位置的一个示例。在本示例中，用户 20 携带着 PK 22，并且 PK 22 与附近的接入点 25-1 进行通信。访问点 25-1 到 25-n 连接到空间服务器 641。空间服务器 641 存储着 PK 22 与之进行通信的访问点的 ID 等信息。空间服务器 641 连接到互联网 21。互联网 21 连接到 pBase 23 和用于确定用户当前位置的定位服务器 642。

参照图 40 将描述用于确定用户当前位置的流程，该用户使用了连接到互联网的设备 643。

PK 22 执行图 6 或图 7 所示的过程以便与空间服务器 641 进行通信，其中空间服务器 641 用作服务系统。然后，在步骤 S2321 中，PK 22 请求空间服务器 641 去获取 PK 22 正与之进行通信的访问点的 ID。这在步骤 S2301 中被接收。在步骤 S2302 中，空间服务器 641 将访问点 25-1 的 ID 作为 PMD 发送到 PK 22。这在步骤 S2322 中被接收。在步骤 S2323 中，接收到的 PMD 作为表示用户 20 附近的访问点的 PMD 被发送到 pBase 23。这在步骤 S2341 中被接收（在 PK 22-1 与 pBase 23 之间执行 PMD 同步化）。

在步骤 S2381 中，设备 643 向定位服务器 642 发送获取用户 20 当前位置的一则请求。这在步骤 S2361 中被接收。在步骤 S2362 中，定位服务器 642 向保留用户 20 的 PMD 的 pBase 23 发送获取用户 20 当前位置的一则请求。这在步骤 S2342 中被接收。此时，执行图 18 或 19 所示的过程，并在定位服务器 642 与 pBase 23 之间进行通信，其中定位服务器 642 用作服务系统而 pBase 23 则代替（用作）PK 22。然后，在步骤 S2343 中，pBase 23 向定位服务器 642 发送用于表示用户 20 附近的访问点的 PMD。这在步骤 S2363 中被接收。

基于在步骤 S2363 中接收到的 PMD，定位服务器 642 获取关于用户 20 附近访问点的信息（在这种情况下是访问点 25-1），并确定访问点的位置。然后，定位服务器 642 将访问点 25-1 的附近设置成用户 20 的当前位置。定位服务器 642 在步骤 S2382 中向设备 643 发送当前位置的信息。这在步骤 S2382 中被接收。

因此，通过使用 PK，确定了用户 20 的当前位置。因此，即便当用户 20 来到另一个地方（例如，访问点 25-2 的附近），也依然能够基于表示用户 20 附近访问点的 PMD 来准确地确定当前位置。

表示用户 20 附近访问点的 PMD 可以存储在 PK 22 中。例如，如图 41 所示，当用户 20 正在旅途中时，用户 20 携带着 PK 22，并且 PK 22 产生包括用户当前位置（关于附近的接入点的信息）以及目的地的地址的 PMD 660。在移动的同时，用户 20 使 PK 22 与提供地图信息的终端 661 进行通信以便将 PMD 660 发送到该终端 661。由此，在终端 661 上显示出一张地图，该地图示出了从当前位置到目的地的路线。

PMD 660 可以被发送到方向指示器 662 以显示继续的方向。通过使用 PMD 660，可以为用户提供很方便的路线引导。

或者，有可能基于确定好的用户当前位置将消息发送给用户。例如，连接到互联网 21 的邮件服务器可以从空间服务器 641 中接收关于用户当前位置的信息，通过图 37 所示的方法来获取关于用户可用设备的信息，并发送电子邮件。由此，当用户位于总公司时，电子邮件被发送到总公司的个人计算机。当用户在商务旅行中来到了分支办公室时，电子邮件便被发送到分支办公室的个人计算机。结果，无论用户在哪个地方用户一定可以接收针对该用户的消息。

尽管在上面描述的示例中是从关于用户附近的访问点的信息中确定该用户的当前位置的，但是还可以更为准确地确定该当前位置。例如，如图 42 所示，当携带 PK 22-1 的用户 20-1 和携带 PK 22-2 的用户 20-2 位于访问点 25 附近时，PK 22-1 或 PK 22-2 与空间服务器 641 进行通信以便将包括用户 20-1 或用户 20-2 的面部特征信息的 PMD 发送到空间服务器 641。另外，假定 PK 22-1 或 PK 22-2 可以与区域 41 中的访问点 25 进行通信。

照相机 681 安装在访问点 25 附近。照相机 681 拍摄区域 42 中的物体，并输出图像数据。空间服务器 641 连接到照相机 681。空间服务器 641 将从照相机 681 中输出的图像数据与用户 20-1 或用户 20-2 的面孔特征信息进行比较。当与面孔特征信息相匹配的图像被检测到时，空间服务器 641 确定用户 20-1 或用户 20-2 在访问点 25 的附近。空间服务器 641 将访问点 25 的 ID 发送到 PK 22-1 或 PK 22-2。

由此，用户 20-1 或用户 20-2 的当前位置可以被更为准确地确定为照相机 681 附近（在区域 42 中）而非访问点附近（在区域 41 中）。

或者，从照相机 681 中输出的图像数据可以作为 PMD 被存储在 pBase 23

中，并且按要求作为关于用户当前位置周围的信息被提供给服务系统。由此，有可能在隐藏确切的用户当前位置的同时还提供用户周围的图像。

当多个访问点彼此相对接近地安放时，PK 22 需要选择（检测）与哪个访问点进行通信。

参照图 43 就描述由 PK 22 检测访问点的一个示例，即第一访问点检测过程。在步骤 S2501 中，PK 22 使通信输出功率最小化。如上所述，通过像 RF(无线电频率)这样的无线通信、准静电场通信、光通信等，PK 22 与访问点进行通信。在步骤 S2501 中，PK 22 将 PK 22 的无线电波输出设置成最小。

在步骤 S2502 中，PK 22 确定是否检测到访问点。当 PK 22 确定没有检测到任何访问点时，PK 22 继续到步骤 S2506 以便确定通信输出功率是否是最大。当 PK 22 确定通信输出功率并非最大时，PK 22 继续到步骤 S2507 以便将通信输出功率增大一级。该过程返回到步骤 S2502 以便重复从步骤 S2502 往下的过程。

参照图 44 将进行更为详细地描述。当通信功率是最小功率时，PK 22 可以在区域 701 中输出无线电波。当访问点 25-1 到 25-n 检测到来自于 PK 22 的无线电波时，访问点 25-1 到 25-n 发送由 PK 22 接收的响应，由此 PK 22 检测到这些访问点。既然，在区域 701 中没有访问点，那么 PK 22 便无法检测到访问点。因此，PK 22 将通信输出功率增大一级以便在区域 702 中输出无线电波。访问点 25-1 位于区域 702 中。PK 22 检测访问点 25-1。

回到图 43，当 PK 22 在步骤 S2502 中确定访问点被检测到时，PK 22 继续到步骤 S2503 以便与检测到的 25-1 进行通信。

另一方面，当 PK 22 在步骤 S2506 中确定通信输出功率是最大时，PK 22 确定在 PK 22 附近没有访问点。在步骤 S2508 中执行出错过程。然后，访问点检测过程结束。

因此，PK 22 逐渐地增大 PK 22 的通信输出，并与 PK 22 首先找到的访问点进行通信。由此，在图 44 中 PK 22 并不与访问点 25-2 进行通信，并由此减小通信的功耗。

尽管参照图 43 已描述了在改变通信输出的同时 PK 22 还检测访问点这样一个示例，但是有这样的情况存在，即在 PK 22 的相同的通信输出情况下检测

到多个访问点。在这种情况下，可以基于访问点所发出的通信输出（例如，场强）来检测访问点。参照图 45 将描述由 PK 22 检测访问点的另一个示例，即第二访问点检测过程。

在步骤 S2521 中，PK 22 获取检测到的访问点的场强。在步骤 S2522 中，PK 22 检索其场强最高的访问点。在步骤 S2523 中，PK 22 与接收到的访问点进行通信。

参照图 46 将进行更为详细地描述。在区域 711-1 中，由 PK 22 从访问点 25-1 中接收到场强为 1 的无线电波。在区域 712-1 中，由 PK 22 从访问点 25-1 中接收到场强为 2 的无线电波。相似的是，在区域 711-2 中，由 PK 22 从访问点 25-2 中接收到场强为 1 的无线电波。。在区域 712-2 中，由 PK 22 从访问点 25-2 中接收到场强为 2 的无线电波。

现在，PK 22 正在从访问点 25-1 中接收场强为 1 的无线电波，并且同时正在从访问点 25-2 中接收场强为 2 的无线电波。在这种情况下，从多个访问点（访问点 25-1 和 25-2）中接收场强最高的访问点。在这种情况下，访问点 25-1 被检索到，并且 PK 22 与访问点 25-1 进行通信。

访问点就是这样被检测的。由此，即便当访问点被安装在有用户的房间以及有用户的相邻房间中，PK 22 也一定能够使用有用户的房间中的那个访问点来进行通信。

另外，PK 并不限于单通信通路，并且可以有多个通信通路。此外，可以用各个不同的方法来执行多个通信通路中的通信。图 47 示出了 PK 22 的多个通信通路。

在相同的图中，PK 22 在区域 41 中输出无线电波以便与访问点 25 进行 RF 通信。然后，PK 22 通过访问点 25 连接到互联网 21 以便与服务系统 24-2 进行通信。同时，PK 22 与附近的具有光通信接口 762 的个人计算机 761 进行光通信。在这种情况下，沿箭头 781 从 PK 22 和个人计算机 761 中发出像红外线这样的具有方向性的光线。

另外，当用户 20 在用于准静电场通信的接口 762 上时，如箭头 782 所示，PK 22 与接口 762 进行准静电场通信。接口 762 连接到服务系统 24-1。PK 22 通过接口 762 与服务系统 24-1 进行通信。

当如图 39 所示的那样来确定用户的当前位置并且用户（PK 22）的当前位置是基于准静电场通信接口 762 的位置信息而非用于 RF 通信的访问点 25 的位置信息来确定的时候，用户的当前位置可以更为准确地来确定。此外，当用户的当前位置是基于具有高方向性的光通信的接口 762 的位置信息来确定的时候，用户的当前位置可以更为准确地被确定。例如，当在会议室桌面上提供多个光通信接口 762 并且就坐的各用户用其各自的 PK 与这些光通信接口 762 进行通信时，有可能准确地把握住哪位用户坐在哪个位子上了。

或者，在图 5 所示的服务系统 24 首次注册以及之后通信的情况下，可以为通信设置不同的通信通路。例如，当执行服务系统 24 的首次注册时，既然在 PK 22 和服务系统 24 之间没有确定防电子欺骗方法，那么 PK 22 就通过像光通信等很难截取的通信直接与服务系统 24 进行通信从而执行首次注册。在之后的通信过程中，PK 22 可以用 RF 通信通过互联网 21 与服务系统 24 进行通信。由此可提供更为安全的服务。

如上所述，PK 是小计算机，并且 PK 本身可以运行程序以便执行预定的过程（例如，显示检索到的电子邮件的过程）。参照图 48 和 49 将描述 PK 运行程序以便执行预定过程的一个示例。

在图 48 中，假定 PK 具有 PMD 801。PMD 801 中的属性“程序”表示要由 PK 22 来运行的程序，并且程序代码条目是作为该属性的内容来存储的。属性“名字”表示 PK 的用户 ID，“foo”被描述成属性的内容。属性“进栈”表示要被处理的数据（例如，接收到的电子邮件），并且“接收到的紧急消息…”被描述成属性的内容。

参照图 49 将描述 PK 22 的程序运行过程。该过程可以以预定的间隔（例如，间隔一个小时）来执行，或者可以基于用户要求来执行。通过以预定次数按下构成 PK 22 的输入单元 106 的开关，来发布用户命令。在步骤 S2541 中，CPU 101 确定 PMD 801 中的属性“进栈”是否具有数据。当 CPU 101 确定属性“进栈”具有数据时，CPU 101 继续到步骤 S2542 以便在显示器上显示属性“进栈”的内容。在这种情况下，“接收到的紧急消息…”被显示。在步骤 S2543 中，CPU 101 擦除属性“进栈”的内容。

当 CPU 101 在步骤 S2541 中确定属性“进栈”没有数据时，该过程结束。

由此，PK 自身运行程序以便执行显示所接收的电子邮件的过程。当执行图 6 或图 7 所示的过程并且在作为一个服务系统的 PK 与另一个 PK 之间发送电子邮件时，可以进一步提高电子邮件的安全性，因为用户用防电子欺骗过程可以正确地被验证。

另外，可以使 pBase 23 作为一个服务系统与 PK 22 进行通信，这样 PK 22 基于来自 pBase 23 的请求来运行程序。参照图 50 将描述在这种情况下的流程。相同的图对应于图 7，并且图 7 中的服务系统 24 是由 pBase 23 来替代的。

图 50 中的步骤 S2801 到步骤 S2808 的过程与图 7 中的步骤 S401 到步骤 S408 的过程很相似，因此省略有关描述。图 50 中的步骤 S2821 到步骤 S2836 的过程与图 7 中的步骤 S421 到步骤 S436 的过程很相似，因此省略有关描述。图 50 中的步骤 S2881 到步骤 S2891 的过程与图 7 中的步骤 S481 到步骤 S491 的过程很相似，图 50 中的步骤 S2901 和步骤 S2902 的过程与图 7 中的步骤 S501 和步骤 S502 的过程很相似，因此省略有关描述。

在步骤 S2809 中，pBase 23 向 PK 22 发送运行程序的请求。这在步骤 S2835 中由 PK 22 的通信模块 61 来接收。在步骤 S2836 中，通信模块 61 通过 DB 访问模块 66 将在步骤 S2835 中接收的内容输出给一程序。这在步骤 S2921 中被接收，并因此运行该程序。

由此，基于来自 pBase 23 的请求来执行 PK 22 的程序。

另外，尽管参照图 50 已描述过使 pBase 23 作为一个服务系统与 PK 22 进行通信，但 PK 22-1 可以将 PK 22-2（另一个 PK）视为一个服务系统，并与 PK 22-2 进行通信。

既然 PK 22 是由用户来携带的，那么便由电池等来提供电源。因此期望使通信所用的功率最小化。参照图 51 将描述 PK 22 的通信备用过程。

在步骤 S3101 中，CPU 101 以备用模式进行通信。此时，PK 22 只执行图 47 所示的多个通信通路中功耗最少的准静电场通信。在步骤 S3102 中，CPU 101 确定通信是否被接收。当 CPU 101 确定通信被接收时，CPU 101 在步骤 S3103 中开始 802.11b RF 通信。在步骤 S3104 中，CPU 101 确定预定的时间是否已过去。CPU 101 待用直到预定的时间过去。

当 CPU 101 在步骤 S3104 中确定预定的时间已过去时，CPU 101 继续到步

骤 S3105 以结束 802.11b RF 通信。之后，该过程返回到步骤 S3101 以便重复从步骤 S3101 往下的过程。

参照图 52 和图 53 将进行更为详细地描述。在图 52 中，当用户 20 在准静电场通信的接口 821-1 到 821-3 上时，PK 22 与接口 762 进行准静电场通信。服务系统 822 连接到接口 821-1 到 821-3。服务系统 822 一直在将由服务 ID 和服务信息构成的分组 823 发送到接口 821-1 到 821-3。既然用户 20 现在在接口 821-1 到 821-3 上，那么 PK 22 接收分组 823，并由此确定通信被接收（图 51 中的步骤 S3102）。

然后，PK 22 开始 RF 通信（图 51 中的步骤 S3103）。如图 53 所示，PK 22 与区域 41 中的访问点 25 进行通信，并通过访问点 25 与服务系统 822 进行通信。

由此，有可能在正常时候（备用模式）执行与 RF 通信相比功耗更少的准静电场通信，并仅在有必要与服务系统 822 进行通信时才通过使用比准静电场通信速度更高的 RF 通信来进行高速通信。由此，功耗可以被减小，并且可以进行有效的通信。

参照图 54 到 58 将描述由 PK 或 pBase 来实现多个服务的组合示例。在图 54A 中，当携带 PK 22 的用户进入在其中安装有访问点的房间时，从 pBase 23 中发出用户 20 所对应的消息的内容。由此，消息“从 A 中接收到的通信”便显示在 PK 22 的显示器上。或者，如图 54B 所示，安装在房间 881 的房门中的显示设备 882 可以被打开以便通知用户 20 有一个给用户 20 的消息。

如图 55 所示，当用户 20 被通知到有一个给用户 20 的消息时，用户 20 使 PK 22 与个人计算机 901 进行通信从而使个人计算机 901 从 pBase 23 中获取包括通信列表的 PMD 并显示该通信列表。该通信列表描述的是人物列表，来自于这些人的、给用户 20 的通信都已被接收，该通信列表示出了来自于四个人 A 到 D 的通信已被接收。

人物 A 到 D 也具有 PK。各个人物的当前位置是由图 39 所示的方法来确定的。例如，通信列表示出了人物 A 正在运动，人物 B 位于该人物 B 的座位上，人物 C 位于会议室 C，人物 D 留下了一则消息。

当用户 20 期望联系会议室中的人物 C 时，用户 20 进入附近的会议室 A 以

便与会议室 C 进行视频会议。如图 56 所示，在会议室 A 中安装有用于显示电子文档等的监视器 921、用于显示人物 C 的面孔的监控器 922、用于显示整个会议室 C 的监控器 923、以及具有带触摸屏的显示器的控制台终端 924。

此时，用户 20 用图 33 所示的方法在控制台终端 924 上安装用于监控器 921 到 923 的控制代码，并通过操作控制台终端 924 来控制监控器 921 到 923。

如图 57 所示，当六个人，即人物 C 和人物 F 到 I 都在会议室 C 中时，假定每个人都拥有自己的 PK，并且每个人都使自己的 PK 与安装在会议室 C 的桌面上的光通信设备进行通信。光通信具有高方向性，并由此使 PK 所在的地方能够被准确地确定。由此，人物 C 以及人物 F 到 I 的名字、姿态、座位等都被显示在会议室 A 的控制台终端 924 上。

由此，PK 和 pBase 可以提供对用户而言极为方便的通信装置。

图 58 辅助解释了通过将 PK 22 与 pBase 23 组合起来从而减小 IP 电话 961 的备用功率的一个示例。访问点 25 以及 IP 电话 961 存在于携带着 PK 22 的用户 20 附近。IP 电话 961 连接到互联网 21 上以便于与预定的人物进行电话会谈。另外，IP 电话 961 通常是关闭的以便减小功耗。

在这种情况下，PK 22 通过访问点 25 与 pBase 23 进行通信，以便用图 37 所示的方法将用于表示用户 20 可用的设备的 PMD 发送到 pBase 23（图 58 中的箭头 1001）。期望与用户 20 会话的设备 981 向互联网 21 上的会话连接服务器发出会话连接请求，并且该会话连接请求被发送到 pBase 23（图 58 中的箭头 1002）。pBase 23 与 PK 22 进行通信以便将会话连接请求通知到 PK 22（图 58 中的箭头 1003）。结果，如上文参照图 49 所描述的那样，该连接请求被显示在 PK 22 的显示器上。

当用户 20 注意到会话连接请求并打开 IP 电话 961 时，用于表明 IP 电话 961 已变为可用的信息被发送到 pBase 23（图 58 中的箭头 1004）。此外，pBase 23 通知设备 981 IP 电话 961 已变为可用（图 58 中的箭头 1005）。由此，便开始了使用设备 981 和 IP 电话 961 的会话。

由此，用户 20 可用在减小功耗的同时使用 IP 电话 961。

尽管在上述中假设 PK 22 是可以由用户携带的小计算机，但是图 4 中的软件可以在通用个人计算机这实现，这样通用个人计算机被用作 PK。

图 59 示出了在由用户携带的便携式设备 1101 和 1102 中实现 PK 22 的软件 60 的一个示例。在相同的图中，便携式设备 1101 和 1102 是像 Walkman（商标）这样的小的音乐再现设备，它可再现用户想要的音乐数据。PK 22 的软件 60 是在便携式设备 1101 和 1102 中实现的，并且服务系统 24-20 的软件也在该便携式设备 1101 和 1102 中实现，其中服务系统 24-20 用作获取或发送与用户偏好信息相匹配的音乐数据的服务系统。

即，便携式设备 1101 和 1102 是 PK 22 和作为一个信息处理设备的服务系统 24-20 的实现。可以向用户提供服务而并不需要通过通信来发送或接收数据。结果，无论用户走到哪里，该用户都可以基于存储在便携式设备 1101 和 1102 中的 PMD 偏好信息来收听适合该用户口味的音乐。

另外，可以为便携式设备 1101 和 1102 提供通信功能。这使便携式设备 1101 的用户 22-11 以及便携式设备 1102 的用户 22-12 在路上遇到时能够交换适合该他们口味的音乐的音乐数据。

另外，参照图 25 已描述过基于用户的 PMD 中的偏好信息来执行个性化的示例，但是，当用户偏好信息已经在连接到网络的另一个服务器中被分析过时，便可以用分析的结果来执行更为详细的个性化。在图 60 中，连接到互联网 21 的服务系统 24-21 基于 PK 22 的用户偏好信息来推荐电视节目。另一方面，互联网 21 与用协同过滤来分析用户偏好的协同过滤服务器 1201 相连。

协同过滤服务器 1201 从 pBase 23 中获得用户的 PMD，并分析被包括在 PMD 中的观赏（操作）历史。协同过滤服务器 1201 将该用户的观赏历史与其它用户的观赏历史进行比较，并获取与正在被讨论的用户的观赏历史相似的另一个用户的观赏历史。协同过滤服务器 1201 获取并推荐其观赏历史与正在被讨论的用户的观赏历史相似的另一个用户所观赏、但正在被讨论的用户还没有观赏过的节目的名字。

服务系统 24-21 基于 PK 22 的 PMD 来选择由协同过滤服务器 1201 推荐的节目，并且将该节目推荐给该用户。由此，可以向用户推荐与其偏好匹配地更近的节目。

当然，协同过滤服务器 1201 推荐的节目可以直接推荐给用户。既然偏好信息已经由 PK 22 或 pBase 23 将其存储在用户的 PMD 中，那么与直接从设备

（例如，电视接收机等）的观赏历史等中收集偏好信息并在不使用 PK 22 和 pBase 23 的情况下推荐节目的情况相比，在协同过滤服务器 1201 上处理负载可以被减小。

用于实现在本说明书中描述的一系列过程的步骤不仅包括在描述的顺序中以时间序列来实现的那些过程，还包括并行地或单独地并且并非必然以时间序列来实现的那些过程。

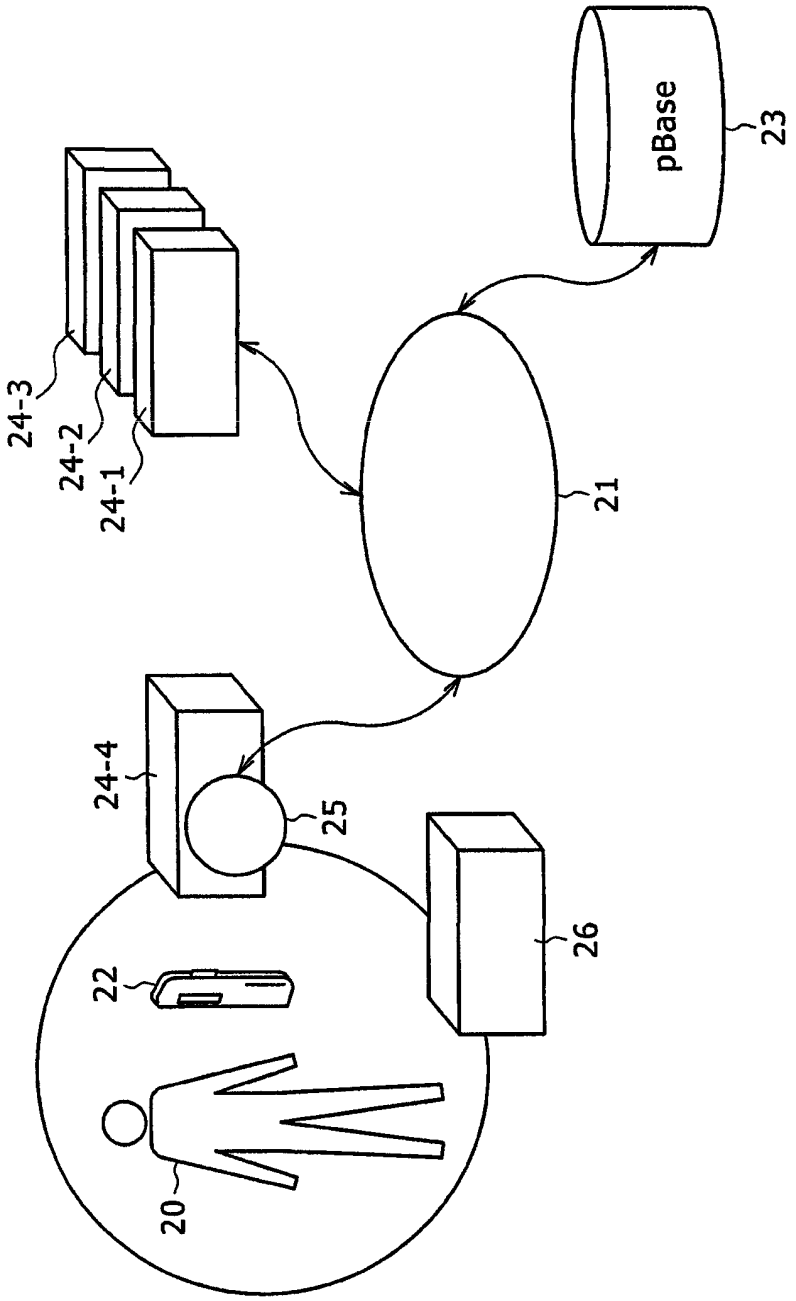


图 1

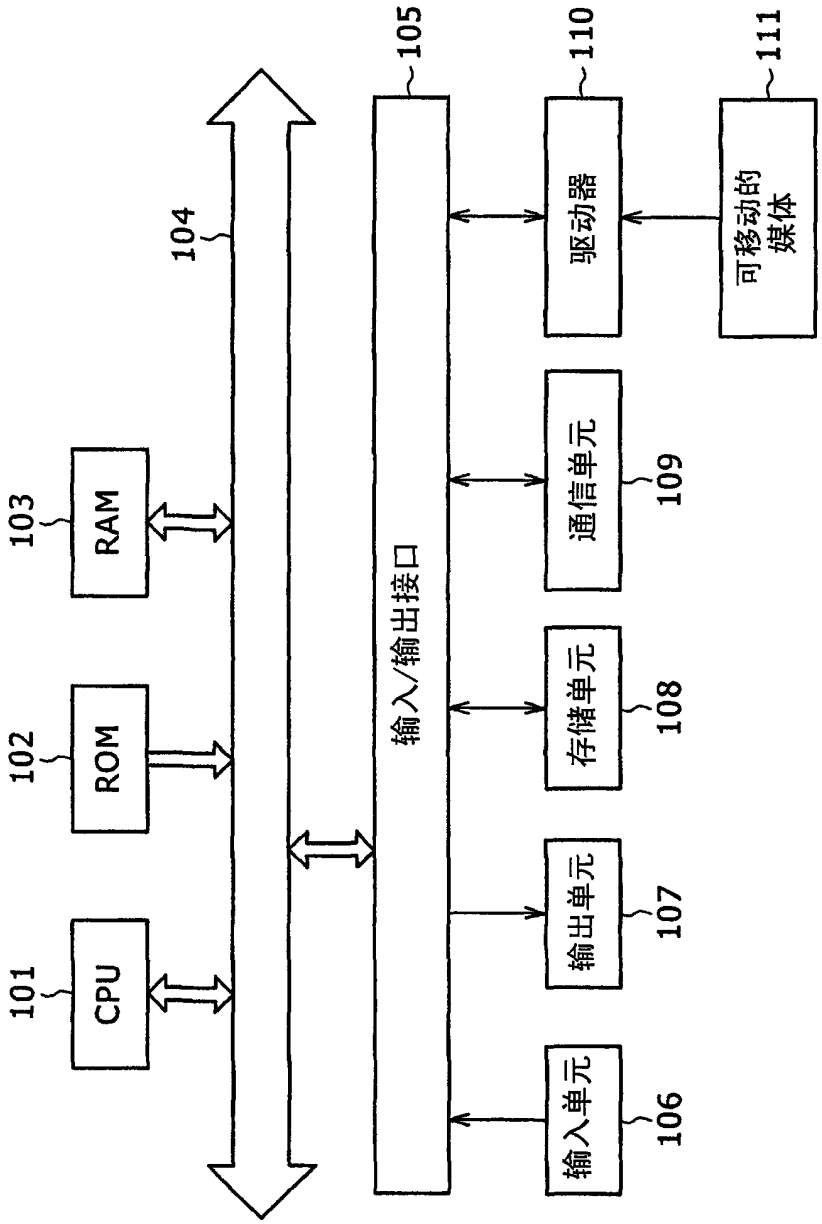

101
CPU
102
ROM
103
RAM
104
105
输入/输出接口
106
输入单元
107
输出单元
108
存储单元
109
通信单元
110
驱动器
111
可移动的媒体

图 2

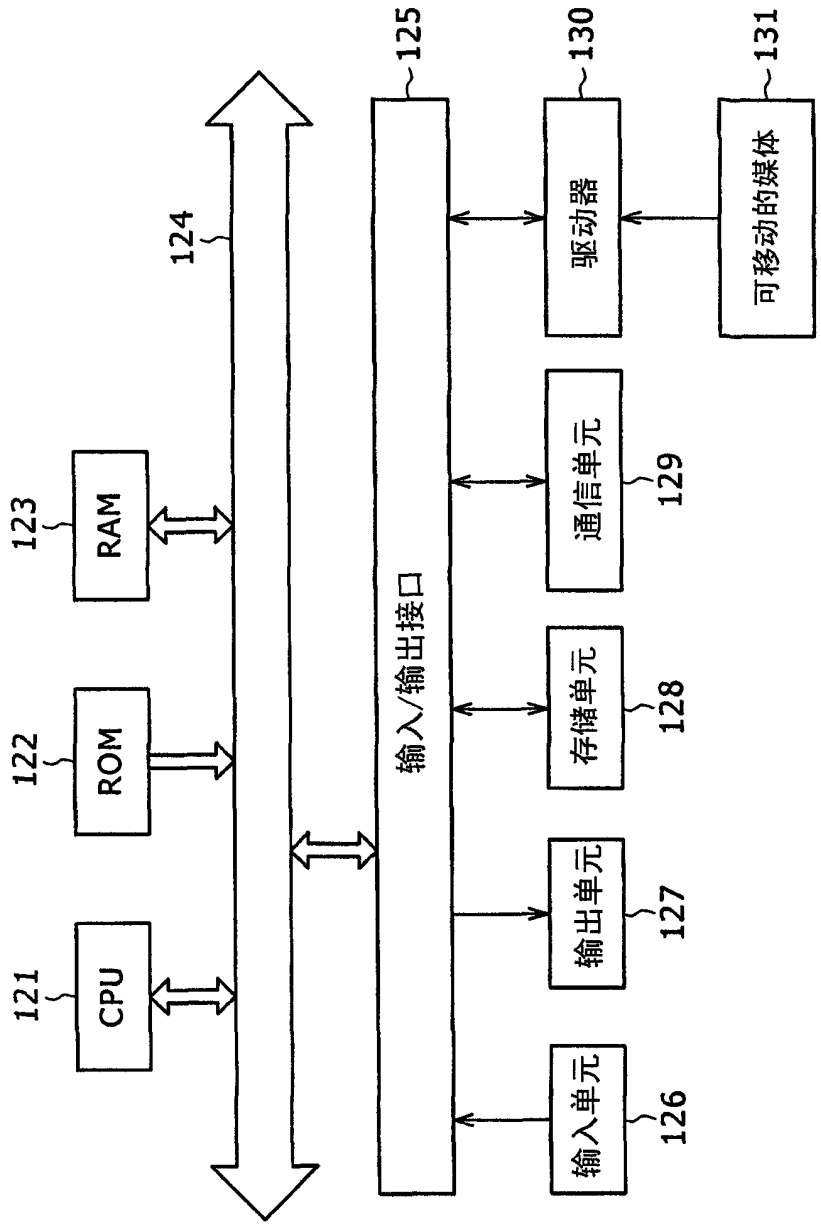

121
CPU
122
ROM
123
RAM
124
125
输入/输出接口
126
输入单元
127
输出单元
128
存储单元
129
通信单元
130
驱动器
131
可移动的媒体

图 3

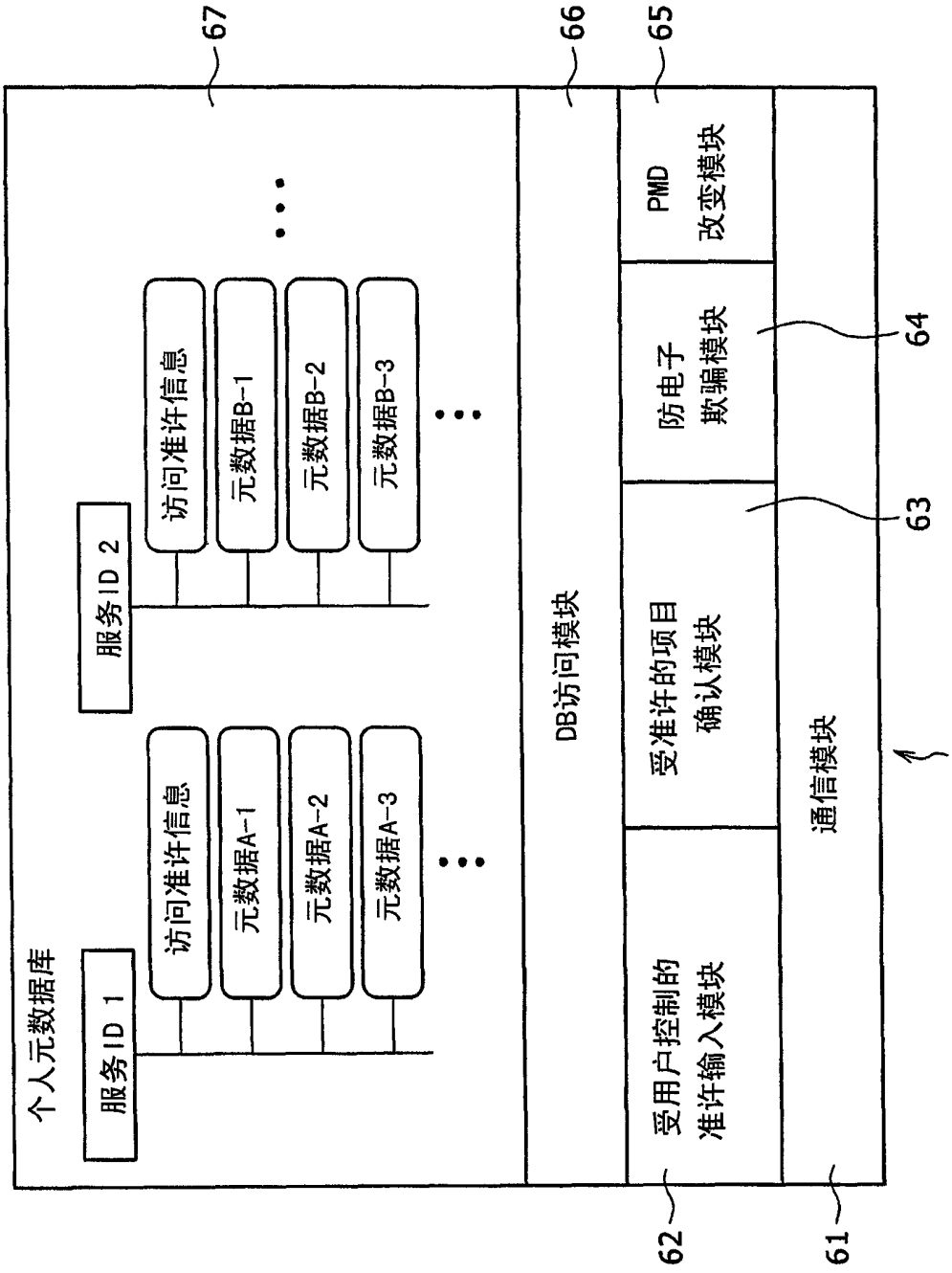

个人元数据库
服务ID 1
访问准许信息
元数据A-1
元数据A-2
元数据A-3
服务ID 2
访问准许信息
元数据B-1
元数据B-2
元数据B-3
67
DB访问模块
66
PMD
改变模块
防电子
欺骗模块
65
64
受准许的项目
确认模块
63
受用户控制的
准许输入模块
通信模块
62
61
60

图 4

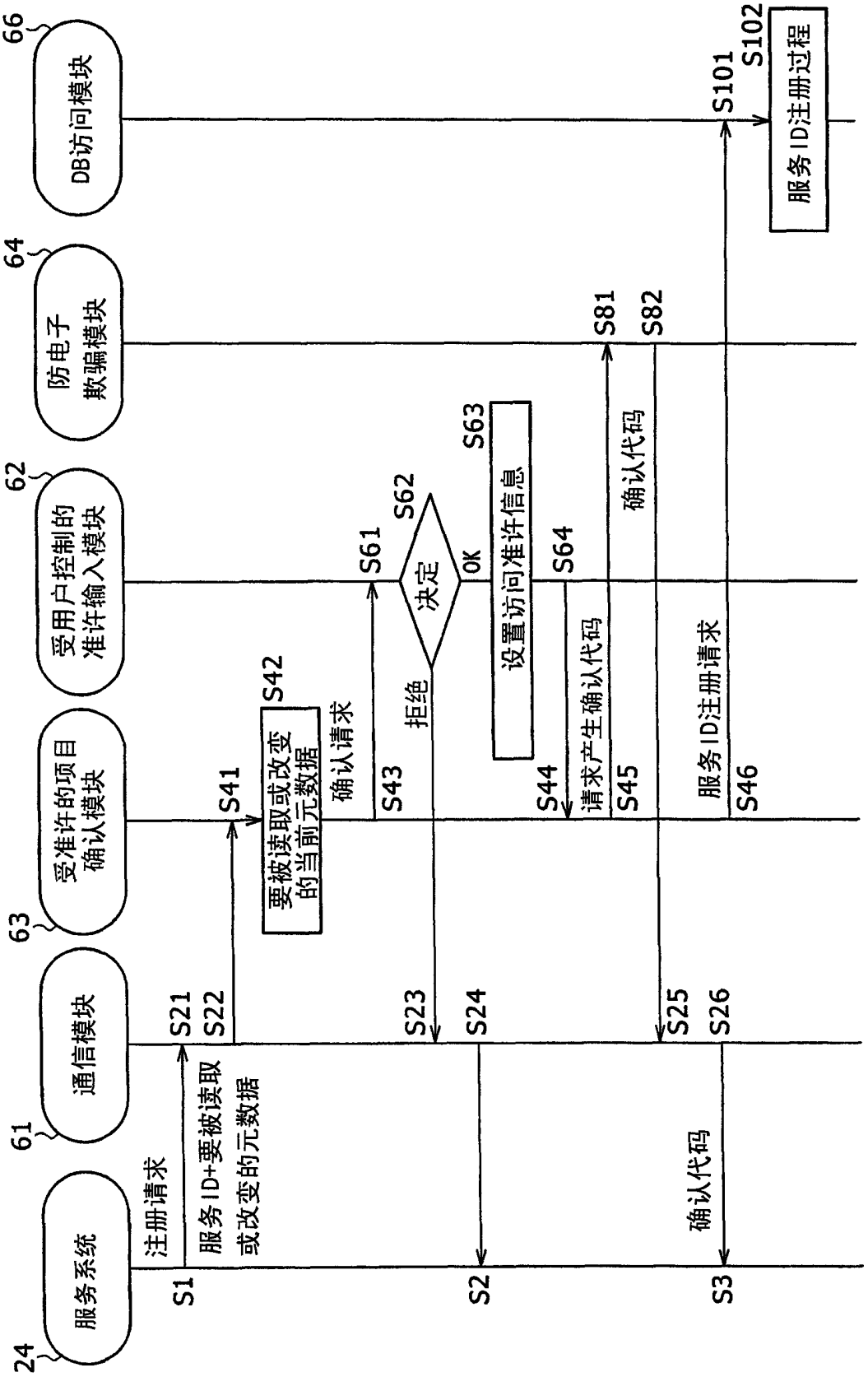

24
服务系统
61
通信模块
63
受准许的项目
确认模块
62
受用户控制的
准许输入模块
64
防电子
欺骗模块
66
DB访问模块
注册请求
服务ID+要被读取
或改变的元数据
S1
S21
S22
S41
要被读取或改变
的当前元数据
S42
确认请求
S43
S61
S62
决定
拒绝
OK
S63
设置访问准许信息
S64
S44
请求产生确认代码
S45
S81
S82
确认代码
S101
S102
服务ID注册过程
S23
S24
S25
S26
服务ID注册请求
S46
确认代码
S2
S3

图 5

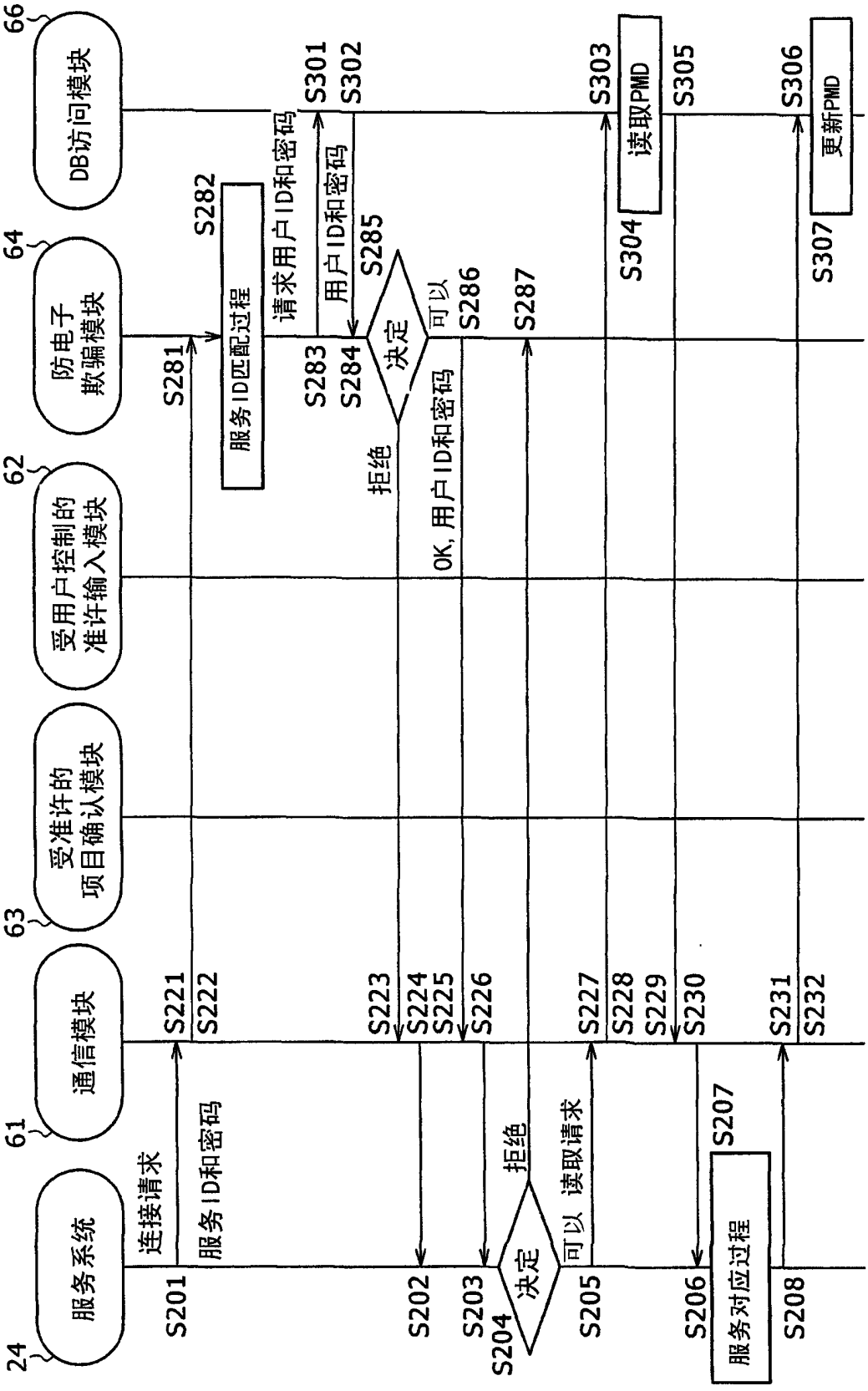

24
服务系统
61
通信模块
63
受准许的项目确认模块
62
受用户控制的准许输入模块
64
防电子欺骗模块
66
DB访问模块
连接请求
服务ID和密码
S201
S221
S222
S281
服务ID匹配过程
S282
请求用户ID和密码
S301
S302
用户ID和密码
S283
S284
S285
决定
拒绝
可以
OK, 用户ID和密码
S286
S287
S303
读取PMD
S304
S305
S306
更新PMD
S307
S223
S224
S225
S226
S227
S228
S229
S230
S231
S232
S202
S203
S204
决定
拒绝
S205
可以 读取请求
S206
S207
服务对应过程
S208

图 6

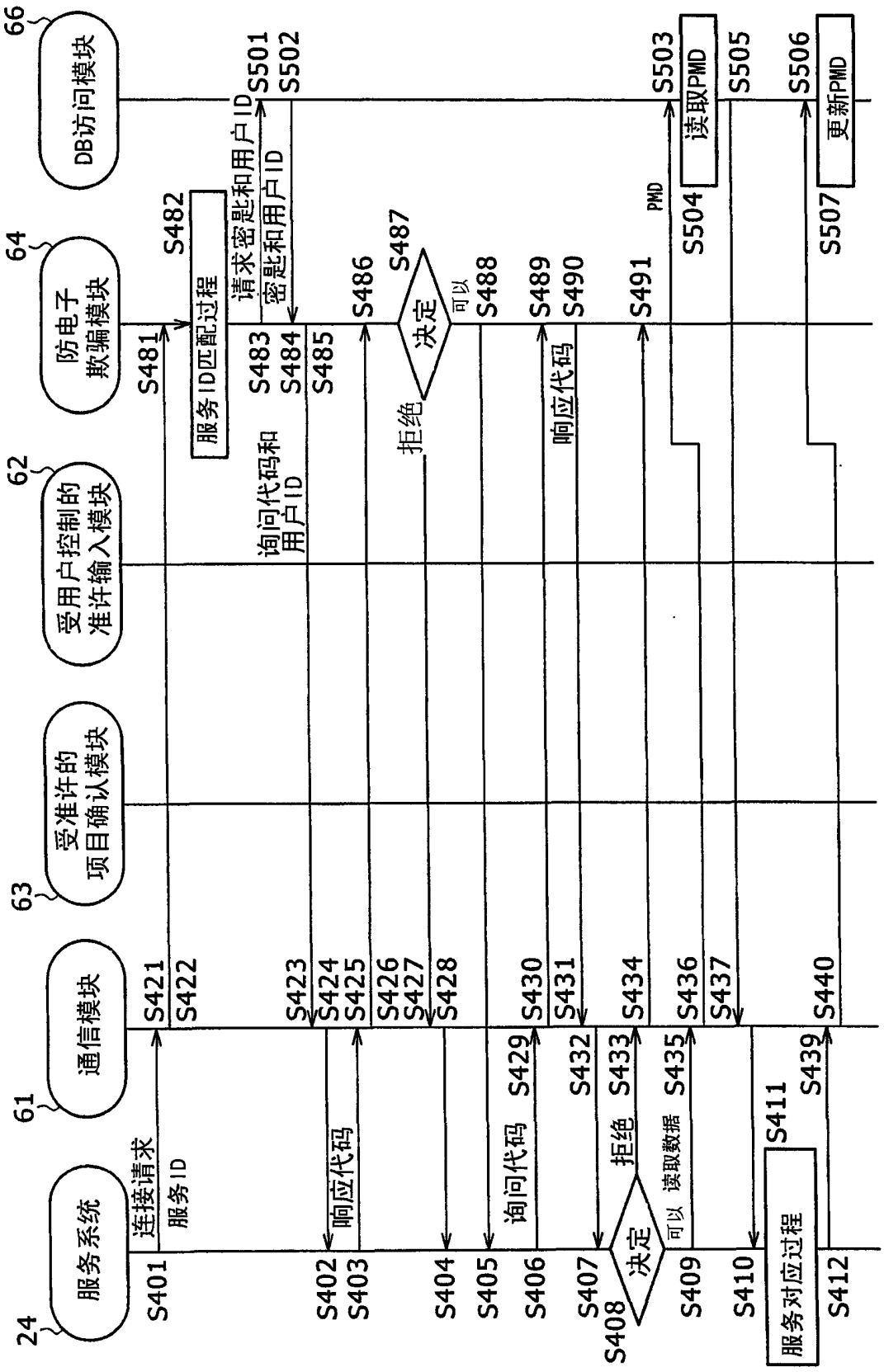

24
服务系统
61
通信模块
63
受准许的项目确认模块
62
受用户控制的准许输入模块
64
防电子欺骗模块
66
DB访问模块
S401
连接请求
服务ID
S402
响应代码
S403
S404
S405
询问代码
S406
S407
S408
决定
拒绝
S409
可以
读取数据
S410
S411
服务对应过程
S412
S421
S422
S423
S424
S425
S426
S427
S428
S429
S430
S431
S432
S433
S434
S435
S436
S437
S439
S440
S481
S482
服务ID匹配过程
S483
询问代码和用户ID
S484
S485
S486
S487
决定
拒绝
可以
S488
S489
响应代码
S490
S491
PMD
S501
请求密匙和用户ID
密匙和用户ID
S502
S503
S504
读取PMD
S505
S506
S507
更新PMD

图 7

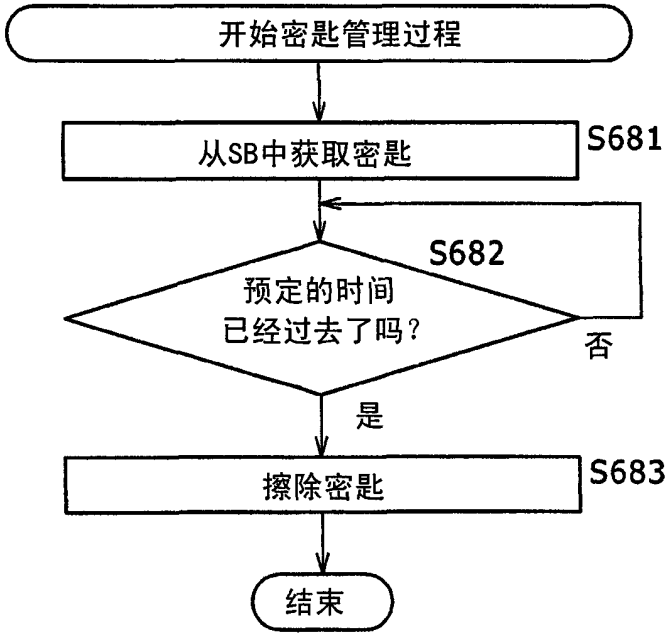

开始密匙管理过程
从SB中获取密匙
S681
S682
预定的时间
已经过去了吗？
否
是
擦除密匙
S683
结束

图 8

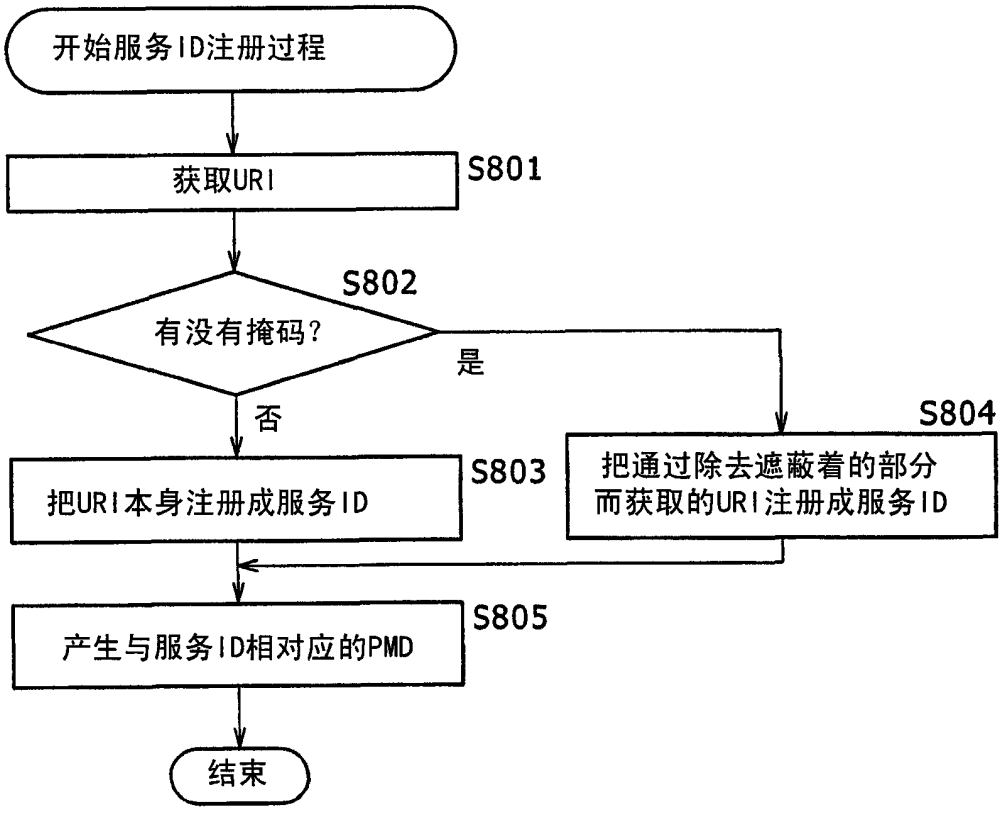

开始服务ID注册过程
获取URI
S801
S802
有没有掩码？
是
否
S804
把通过除去遮蔽着的部分
而获取的URI注册成服务ID
把URI本身注册成服务ID
S803
产生与服务ID相对应的PMD
S805
结束

图 9

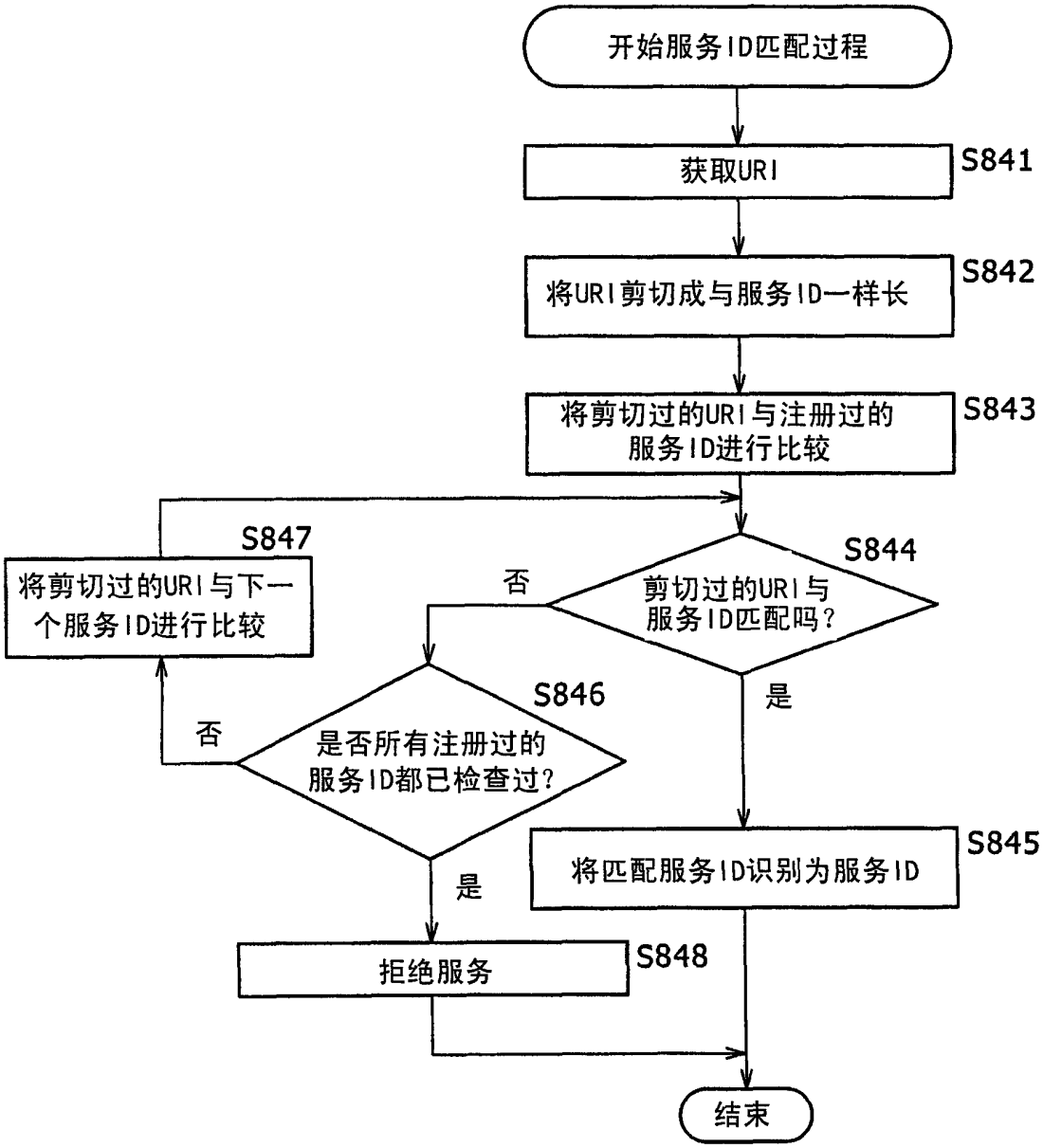

开始服务ID匹配过程
获取URI
S841
将URI剪切成与服务ID一样长
S842
将剪切过的URI与注册过的服务ID进行比较
S843
S844
剪切过的URI与服务ID匹配吗？
否
是
S846
是否所有注册过的服务ID都已检查过？
否
是
S847
将剪切过的URI与下一个服务ID进行比较
将匹配服务ID识别为服务ID
S845
拒绝服务
S848
结束

图 10

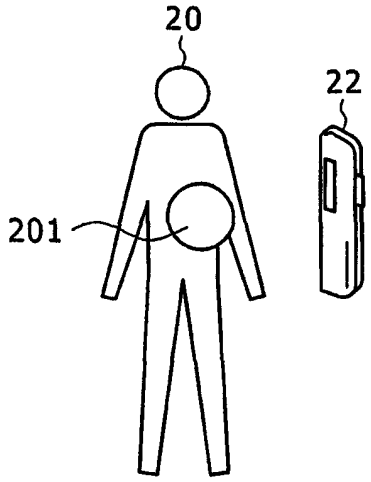


图 11A

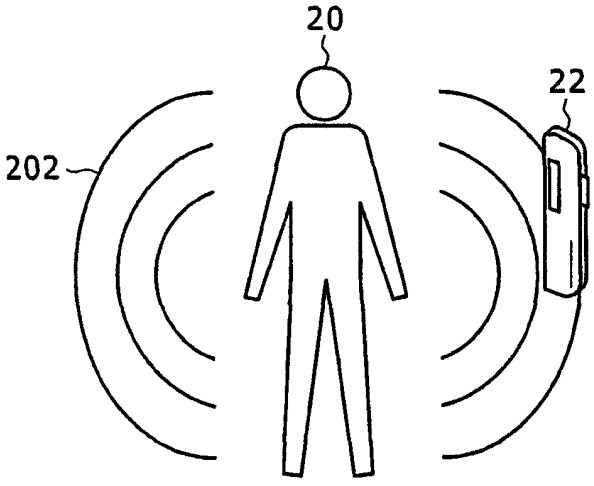


图 11B

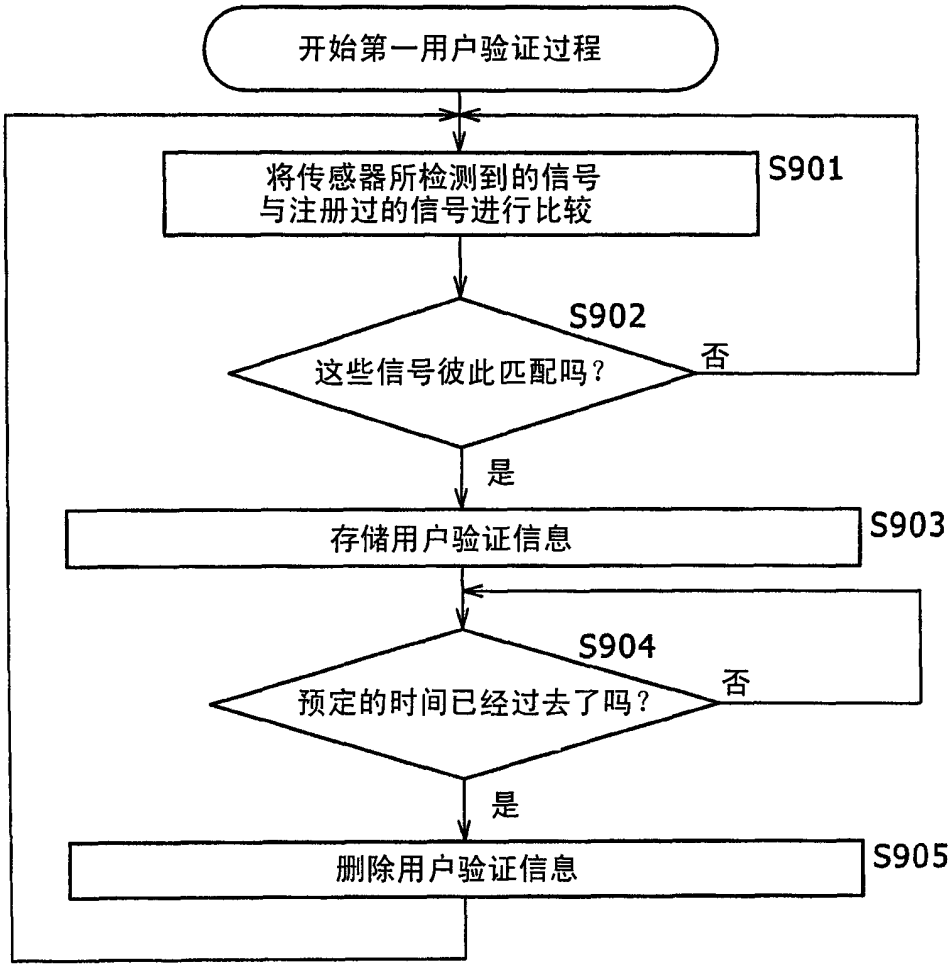

开始第一用户验证过程
将传感器所检测到的信号
与注册过的信号进行比较
S901
S902
这些信号彼此匹配吗？
否
是
存储用户验证信息
S903
S904
预定的时间已经过去了吗？
否
是
删除用户验证信息
S905

图 12

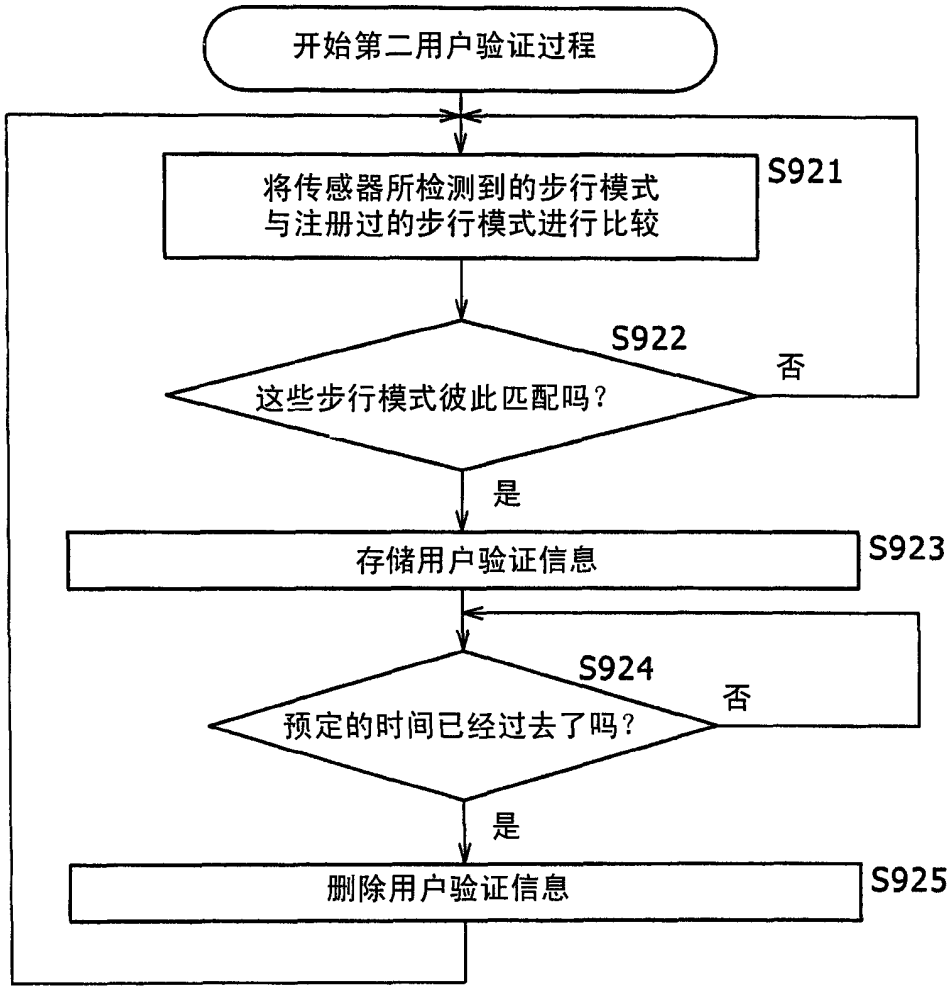

开始第二用户验证过程
将传感器所检测到的步行模式
与注册过的步行模式进行比较
S921
S922
这些步行模式彼此匹配吗？
否
是
存储用户验证信息
S923
S924
预定的时间已经过去了吗？
否
是
删除用户验证信息
S925

图 13

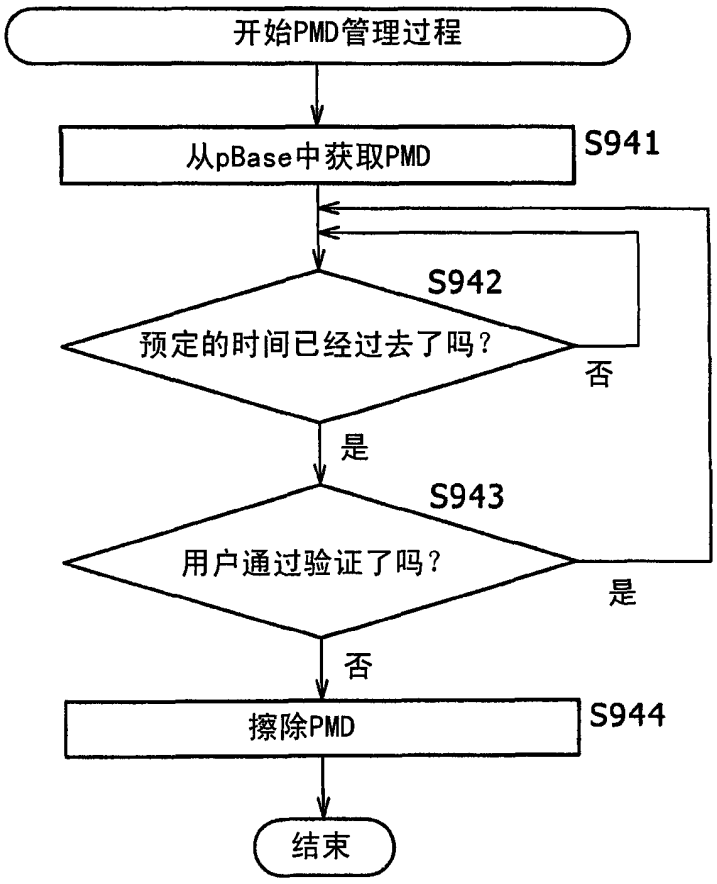

开始PMD管理过程
从pBase中获取PMD
S941
S942
预定的时间已经过去了吗？
否
是
S943
用户通过验证了吗？
是
否
擦除PMD
S944
结束

图 14

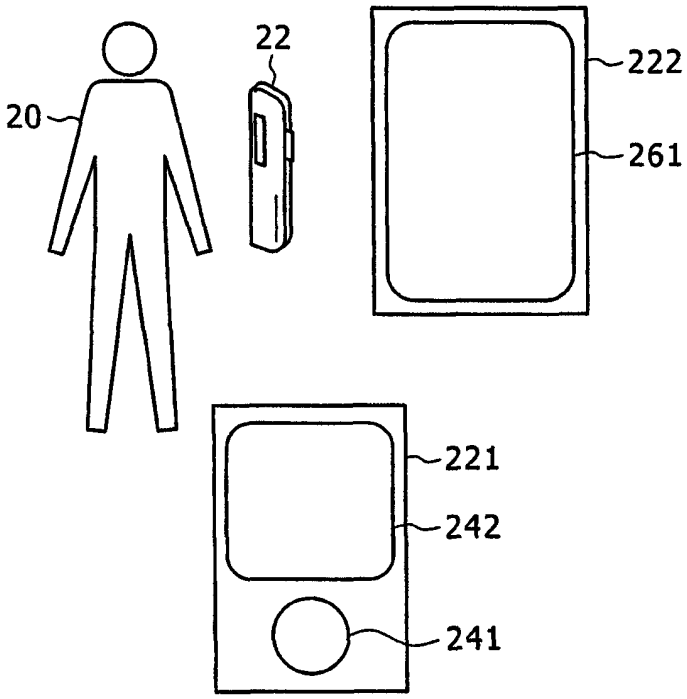


图 15

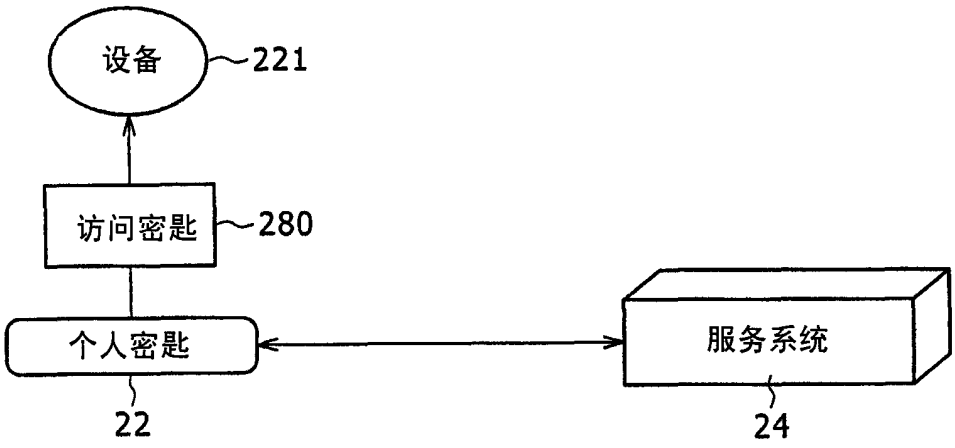


图 16

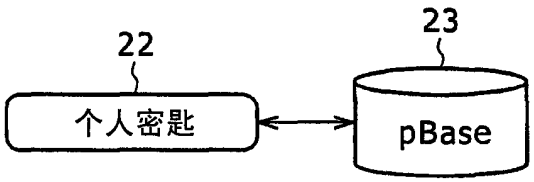


图 17A

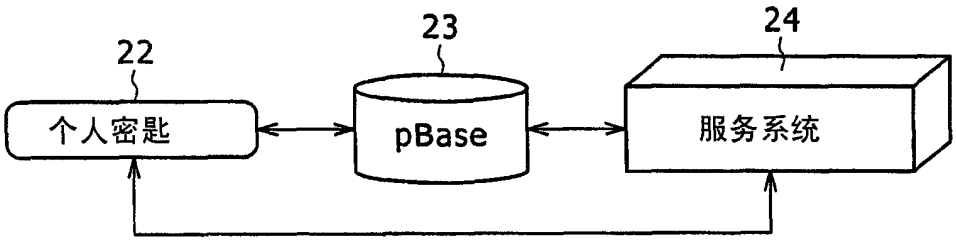


图 17B

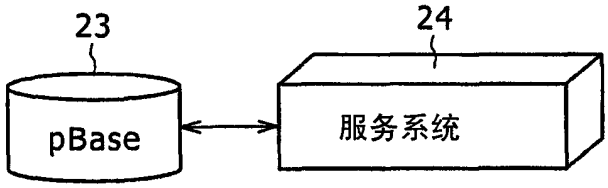


图 17C

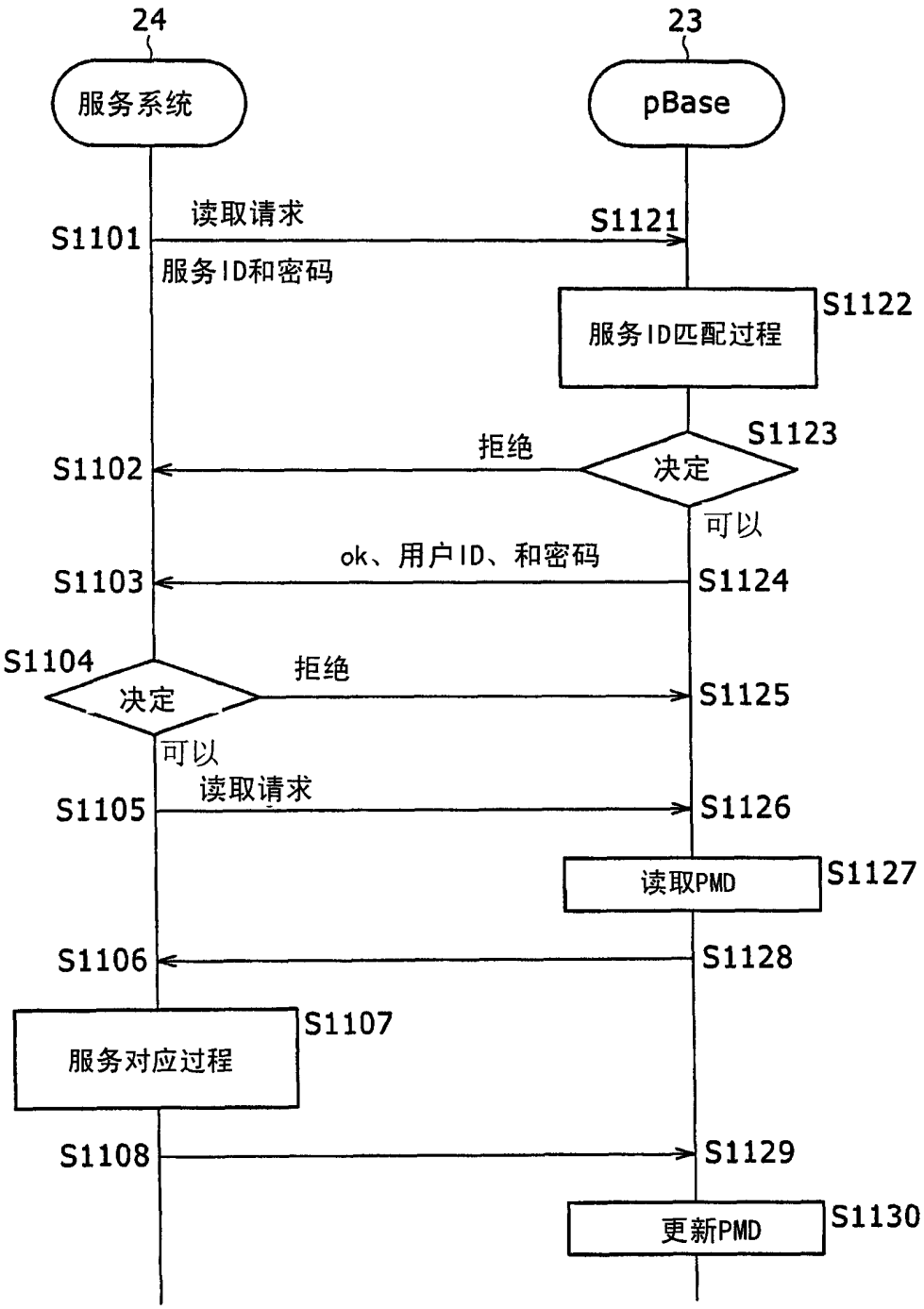

24
23
服务系统
pBase
S1101
读取请求
S1121
服务ID和密码
服务ID匹配过程
S1122
S1123
拒绝
S1102
决定
可以
ok、用户ID、和密码
S1103
S1124
S1104
拒绝
决定
S1125
可以
读取请求
S1105
S1126
读取PMD
S1127
S1106
S1128
服务对应过程
S1107
S1108
S1129
更新PMD
S1130

图 18

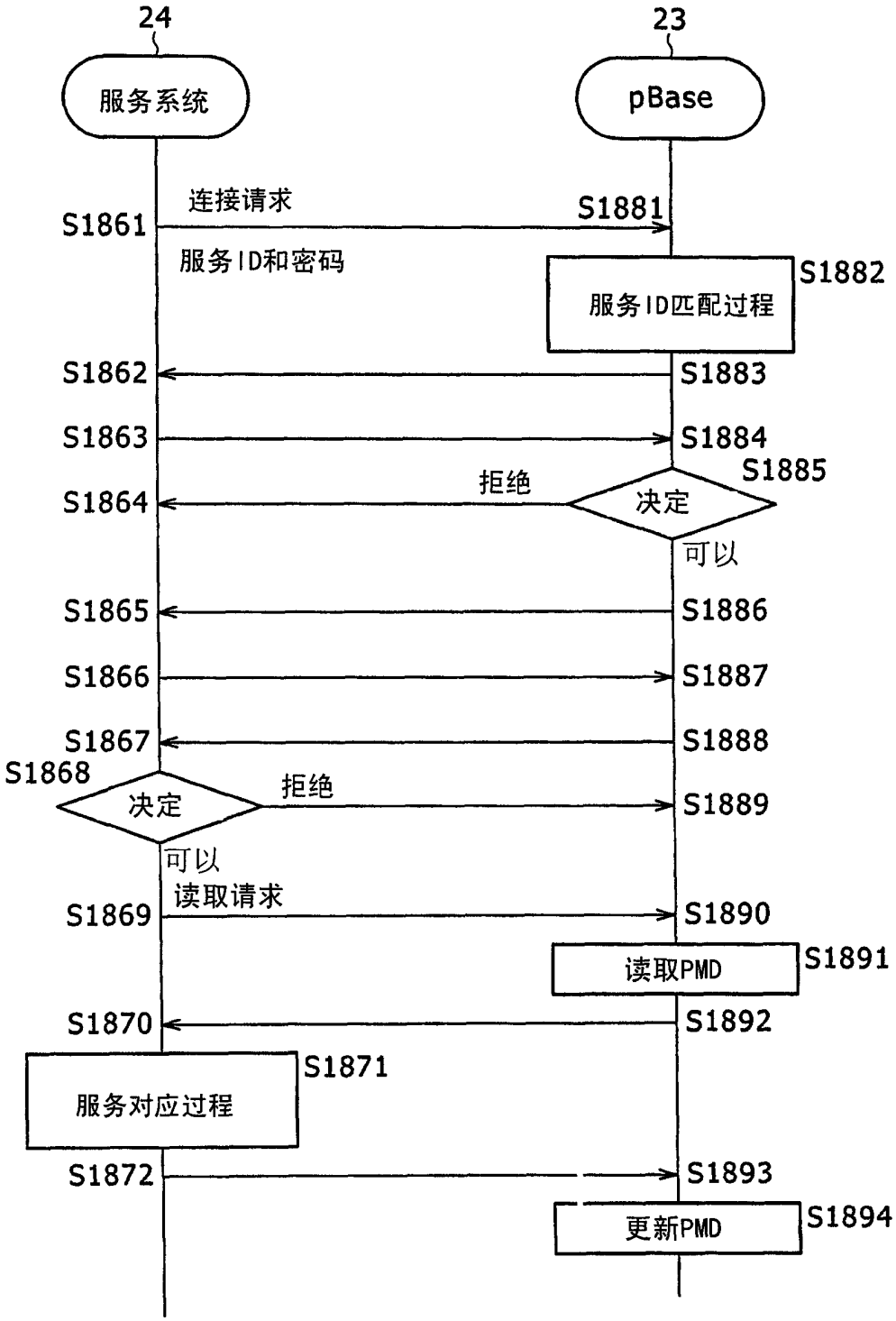
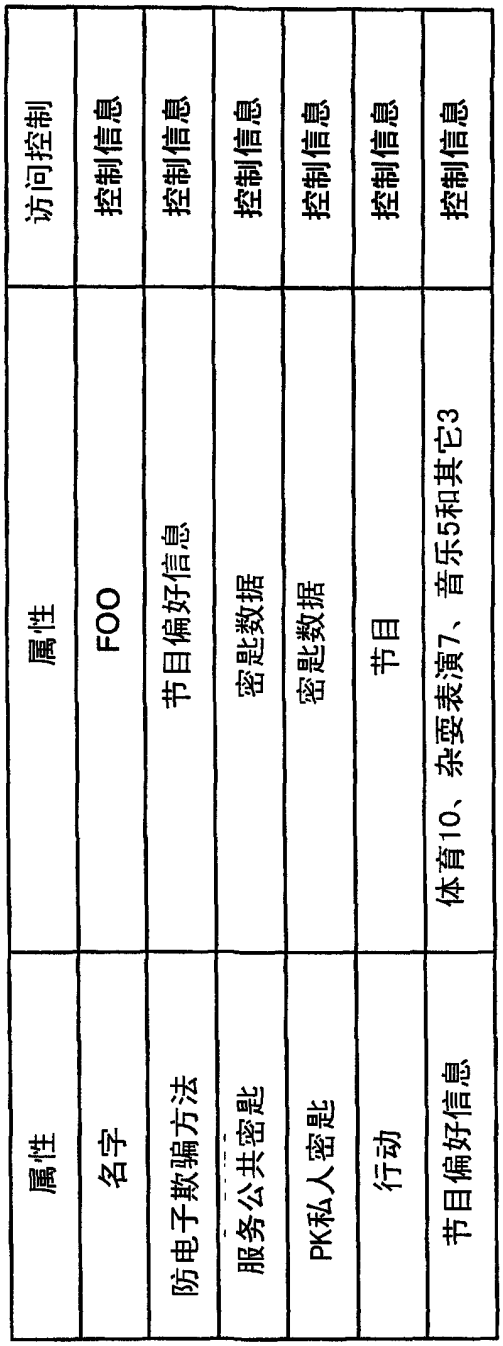

24
23
服务系统
pBase
连接请求
S1861
S1881
服务ID和密码
服务ID匹配过程
S1882
S1862
S1883
S1863
S1884
拒绝
S1885
S1864
决定
可以
S1865
S1886
S1866
S1887
S1867
S1888
S1868
决定
拒绝
S1889
可以
读取请求
S1869
S1890
读取PMD
S1891
S1870
S1892
服务对应过程
S1871
S1872
S1893
更新PMD
S1894

图 19



属性	属性	访问控制
名字	FOO	控制信息
防电子欺骗方法	节目偏好信息	控制信息
服务公共密匙	密匙数据	控制信息
PK私人密匙	密匙数据	控制信息
行动	节目	控制信息
节目偏好信息	体育10、杂耍表演7、音乐5和其它3	控制信息
⋮	⋮	⋮

图 20A

属性	内容	访问控制
名字	FOO	控制信息
防电子欺骗方法	普通密匙系统	控制信息
普通密匙	密匙数据	控制信息
行动	节目	控制信息
节目偏好信息	体育10、杂耍表演7、音乐5和其它3	控制信息

：

图 20B

属性	内容	访问控制
名字	FOO	控制信息
防电子欺骗方法	密码系统	控制信息
服务密码	密匙数据	控制信息
PK密码	密匙数据	控制信息
行动	节目	控制信息
节目偏好信息	体育10、杂耍表演7、音乐5和其它3	
⋮		

图 20C

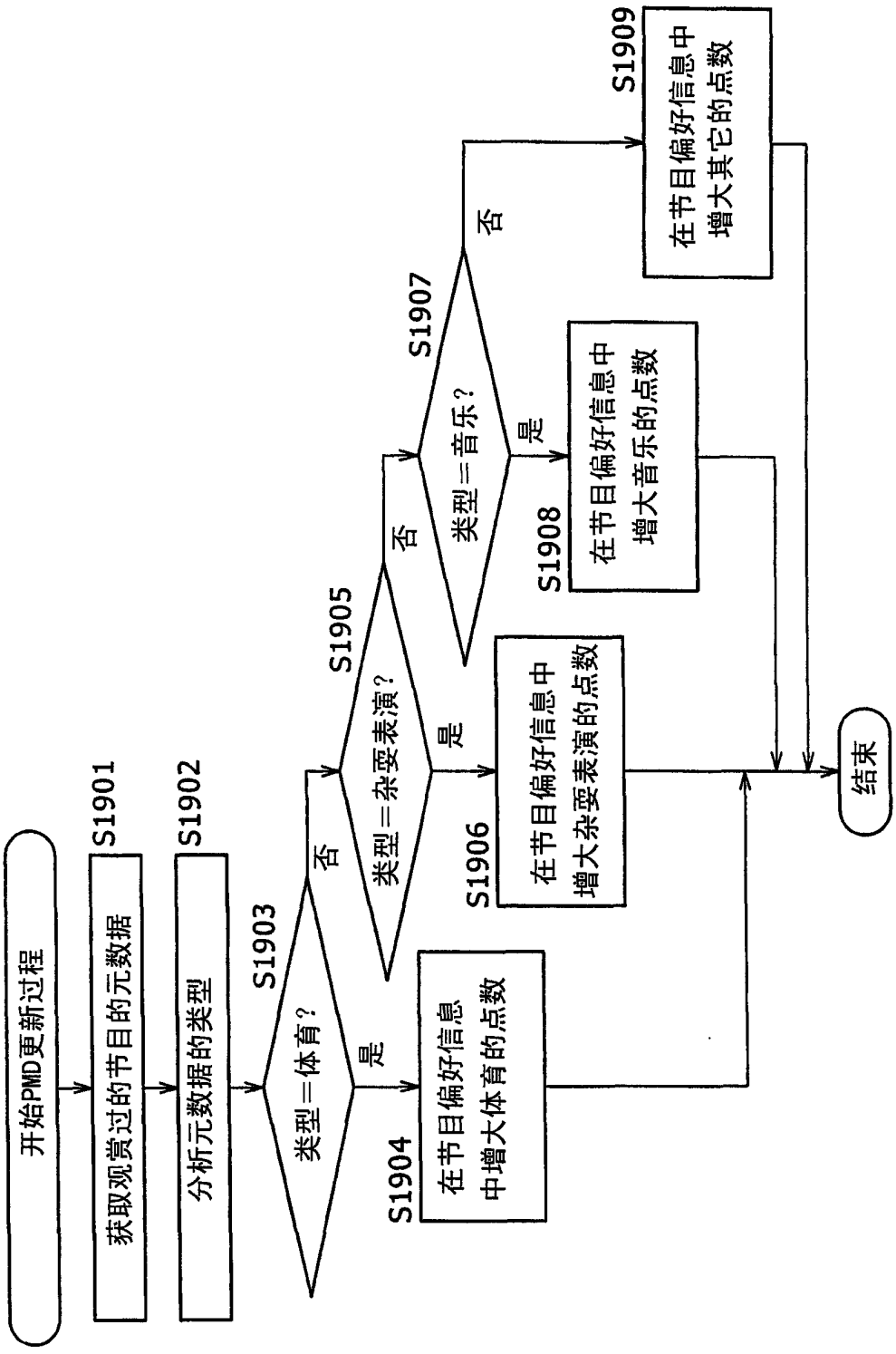

开始PMD更新过程
S1901
获取观赏过的节目的元数据
S1902
分析元数据的类型
S1903
类型＝体育？
是
S1904
在节目偏好信息中增大体育的点数
否
S1905
类型＝杂耍表演？
是
S1906
在节目偏好信息中增大杂耍表演的点数
否
S1907
类型＝音乐？
是
S1908
在节目偏好信息中增大音乐的点数
否
S1909
在节目偏好信息中增大其它的点数
结束

图 21

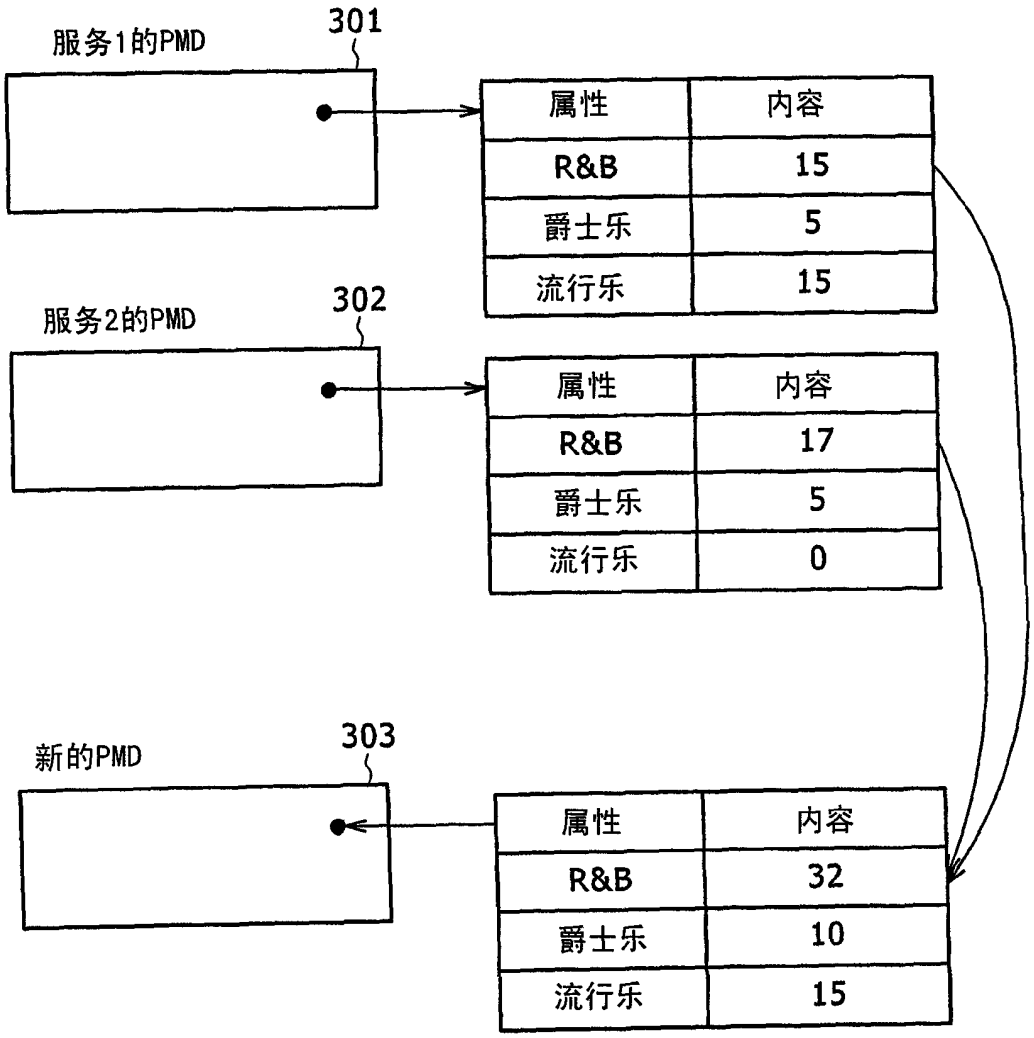

服务1的PMD
301
属性
内容
R&B
15
爵士乐
5
流行乐
15
服务2的PMD
302
属性
内容
R&B
17
爵士乐
5
流行乐
0
新的PMD
303
属性
内容
R&B
32
爵士乐
10
流行乐
15

图 22

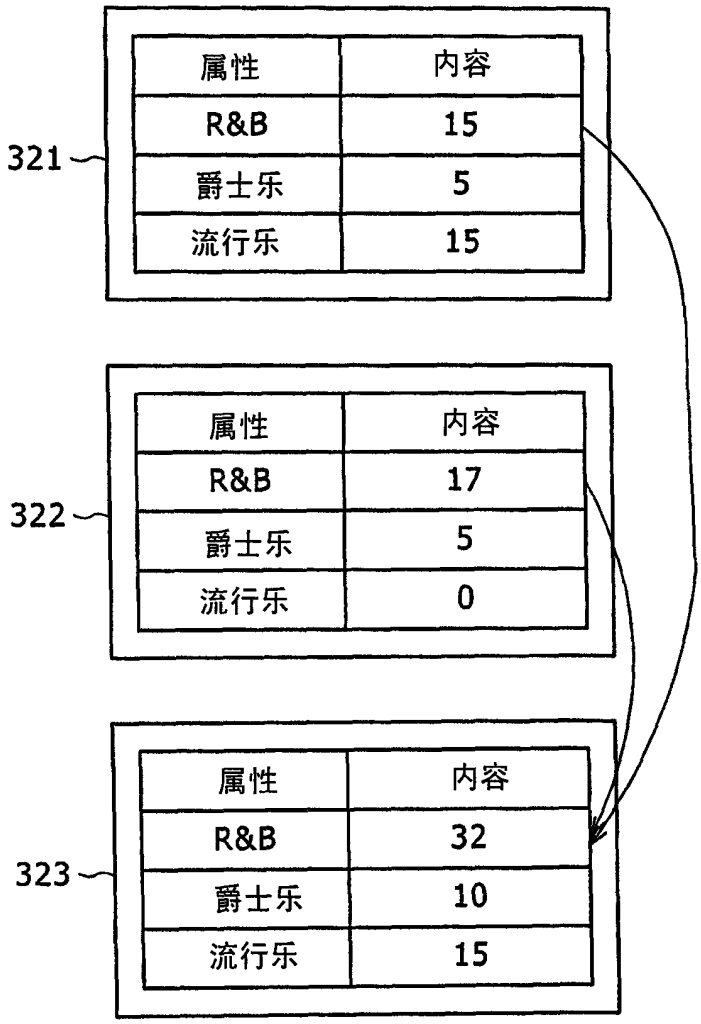

属性
内容
R&B
15
爵士乐
5
流行乐
15
321
属性
内容
R&B
17
爵士乐
5
流行乐
0
322
属性
内容
R&B
32
爵士乐
10
流行乐
15
323

图 23

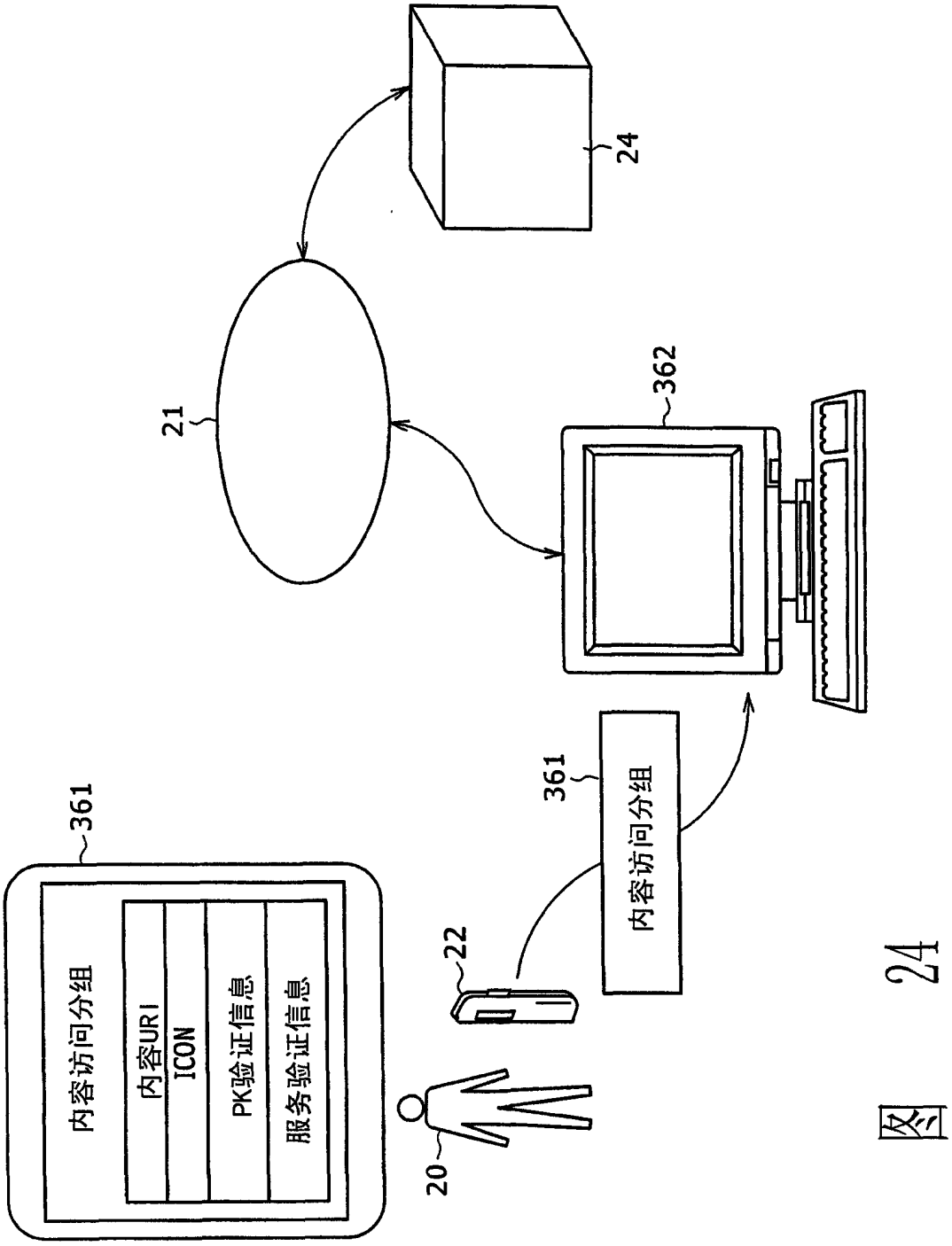

24
21
362
361
内容访问分组
22
20
361
内容访问分组
内容URI
ICON
PK验证信息
服务验证信息

图 24

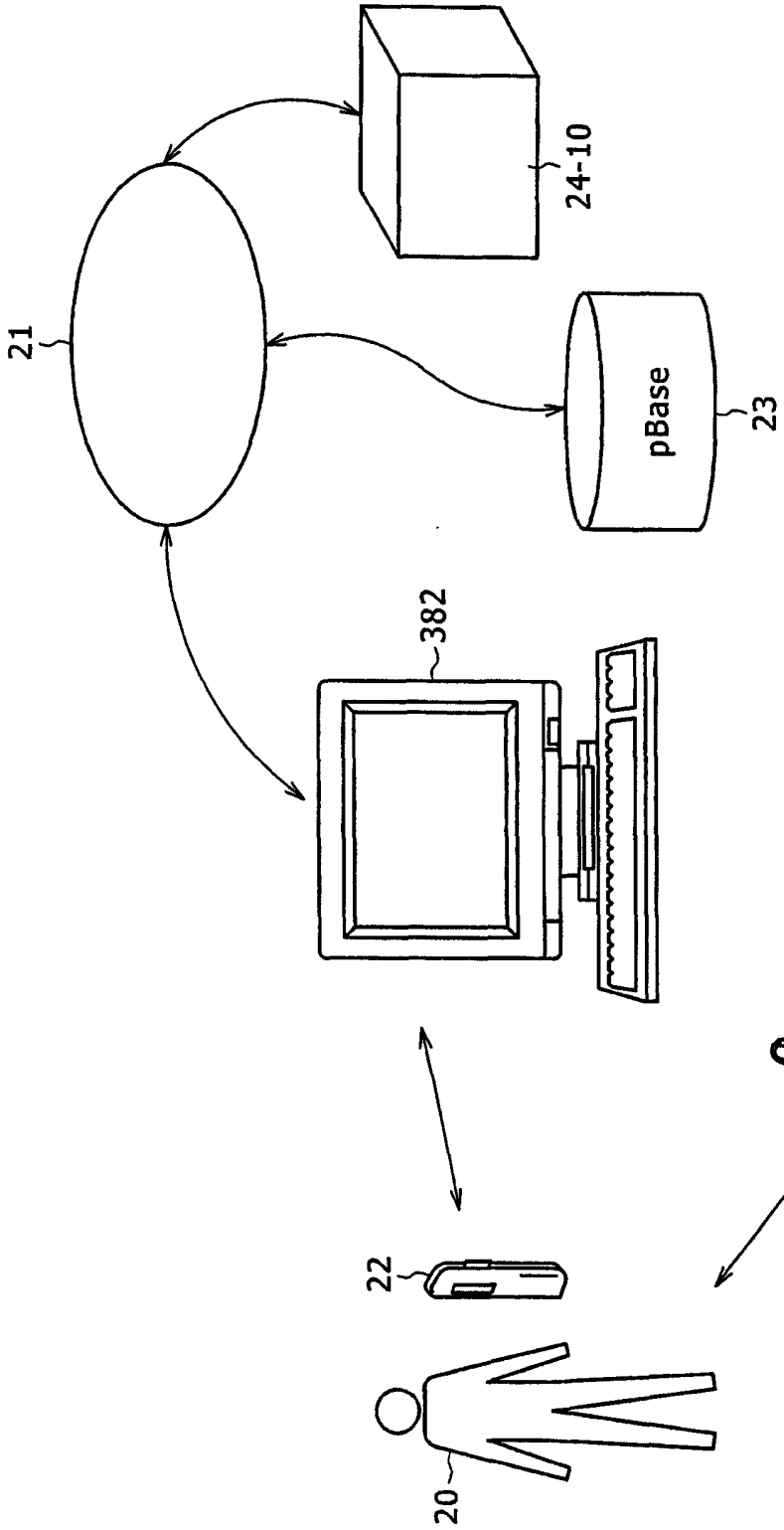


图 25

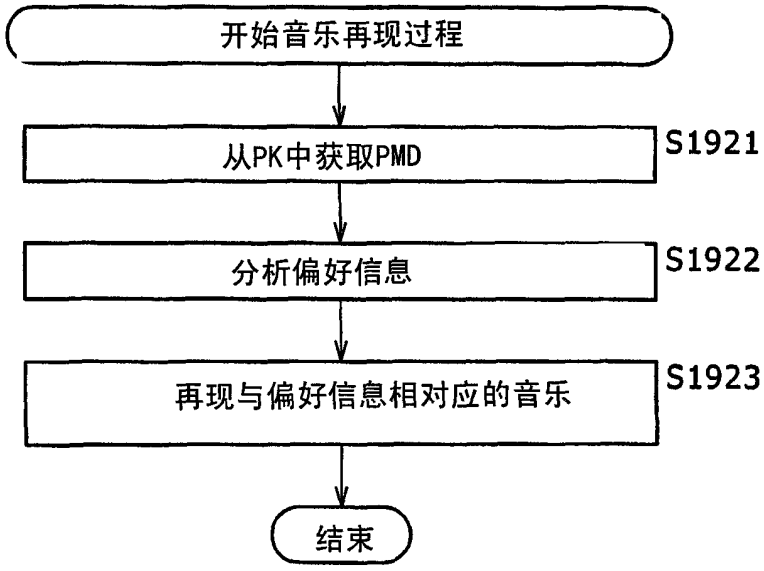

开始音乐再现过程
从PK中获取PMD
S1921
分析偏好信息
S1922
再现与偏好信息相对应的音乐
S1923
结束

图 26

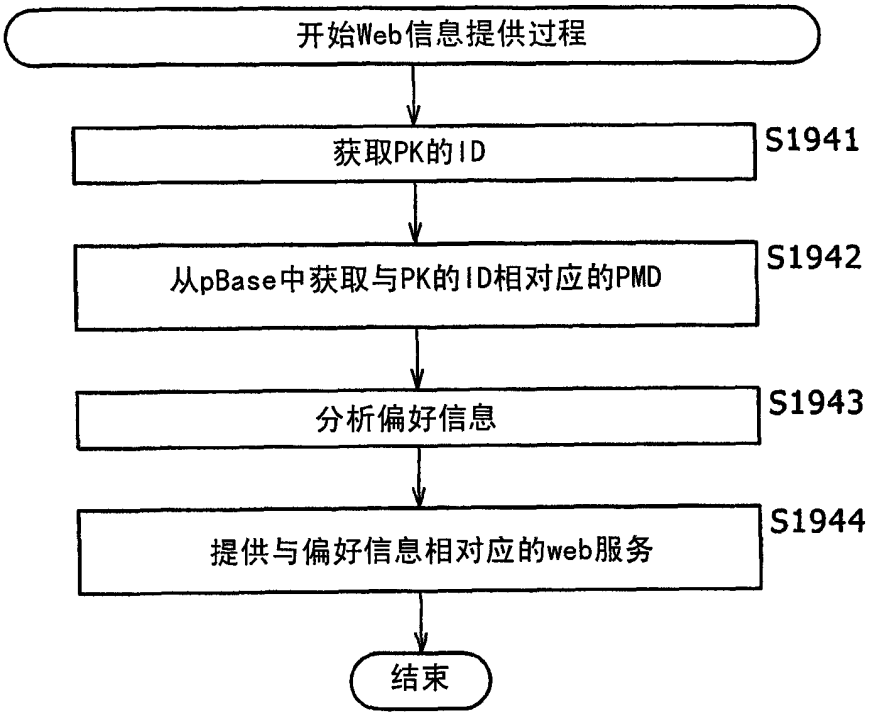

开始Web信息提供过程
获取PK的ID
S1941
从pBase中获取与PK的ID相对应的PMD
S1942
分析偏好信息
S1943
提供与偏好信息相对应的web服务
S1944
结束

图 27

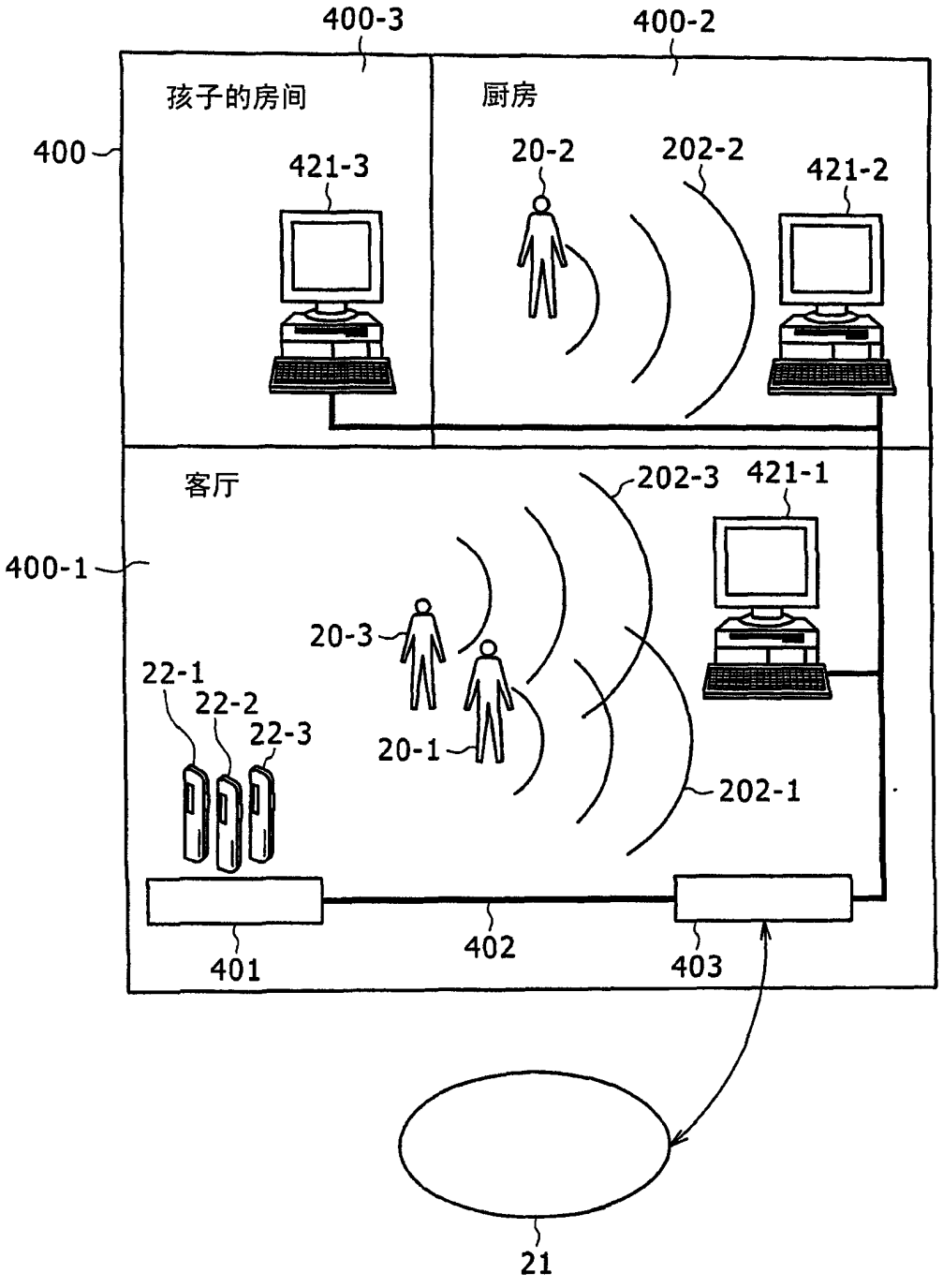

400-3
400-2
孩子的房间
厨房
400
421-3
20-2
202-2
421-2
客厅
202-3
421-1
400-1
20-3
22-1
22-2
22-3
20-1
202-1
401
402
403
21

图 28

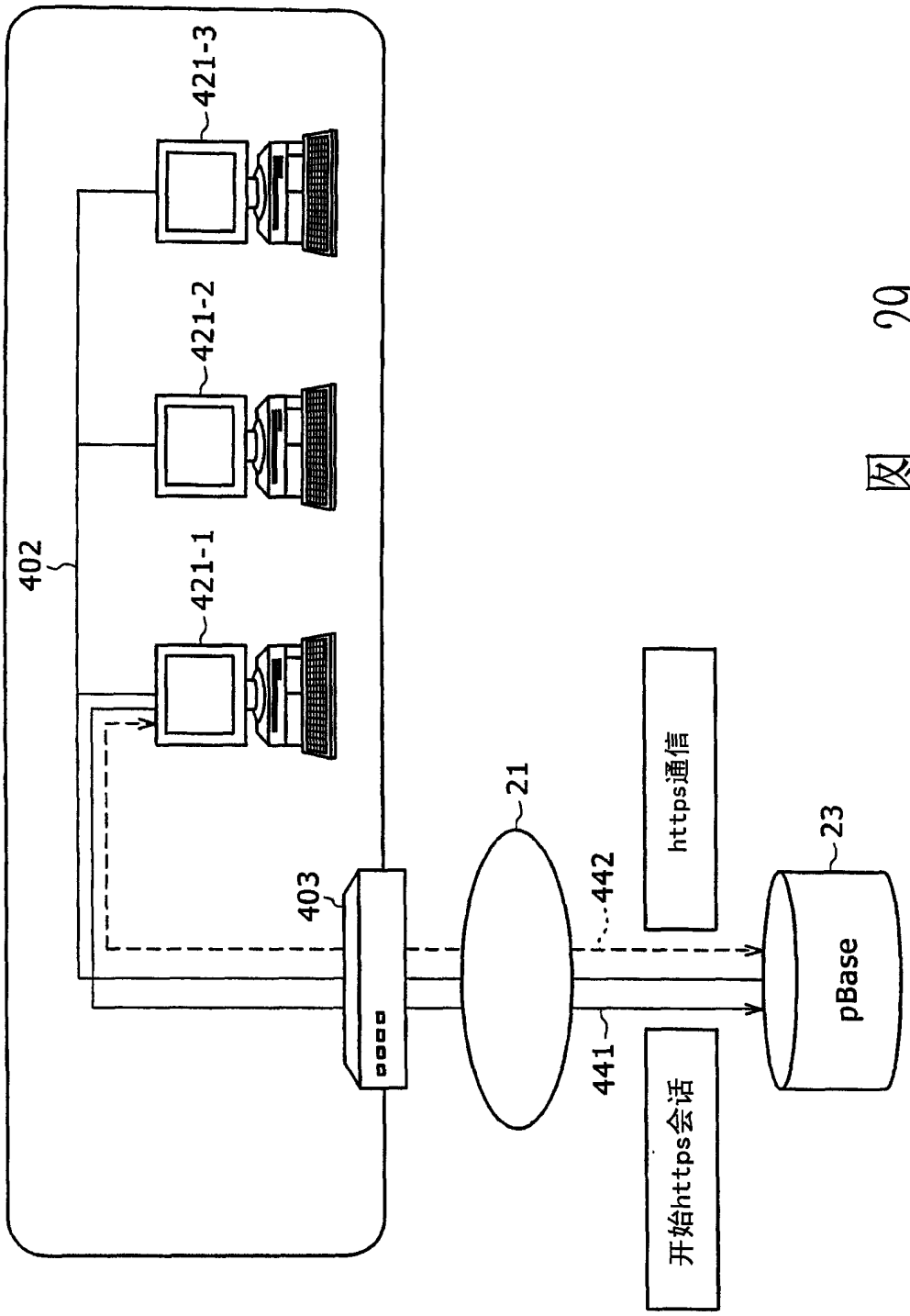


图 29

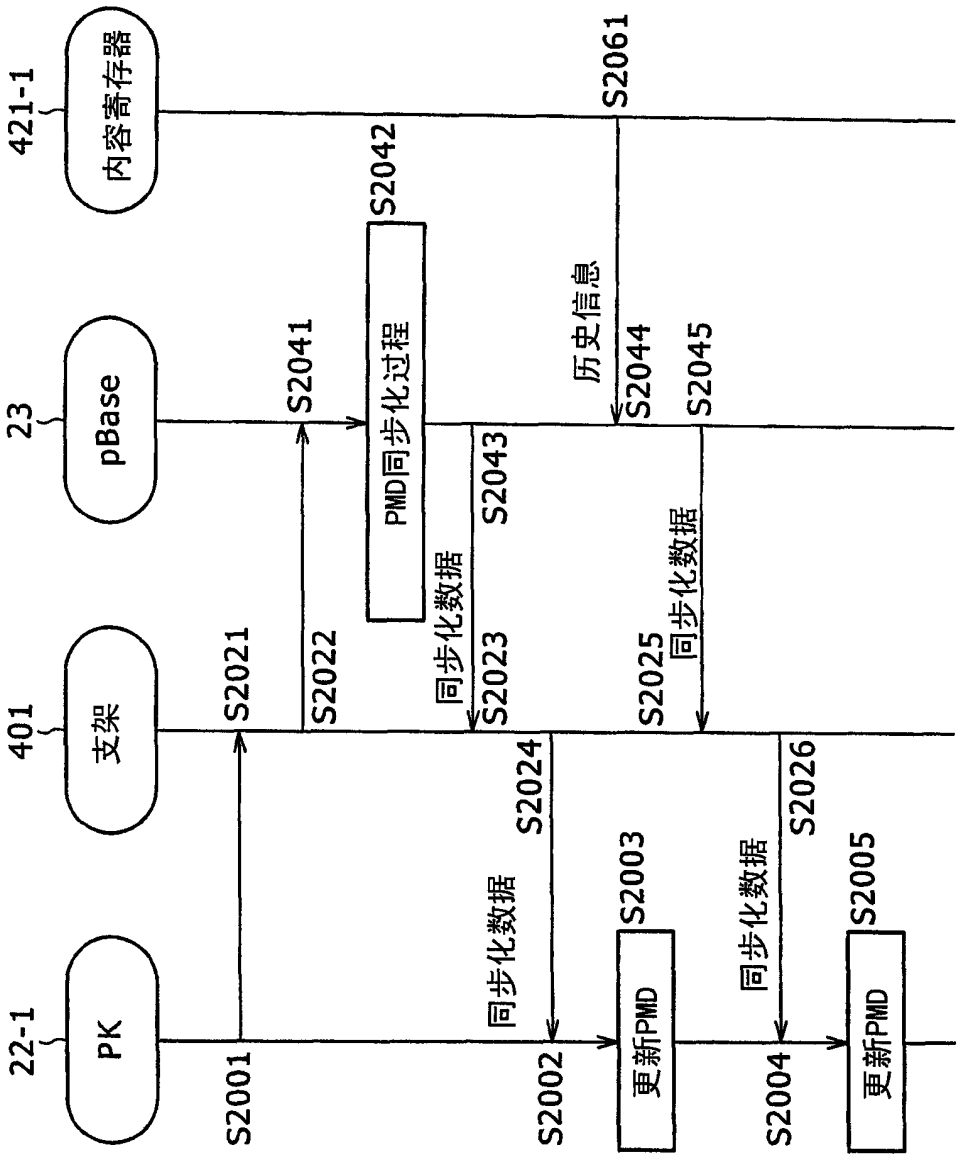

22-1
PK
401
支架
23
pBase
421-1
内容寄存器
S2001
S2021
S2022
S2041
S2042
PMD同步化过程
S2043
同步化数据
S2023
S2024
同步化数据
S2002
S2003
更新PMD
S2025
同步化数据
S2026
同步化数据
S2004
S2005
更新PMD
历史信息
S2044
S2045
S2061

图 30

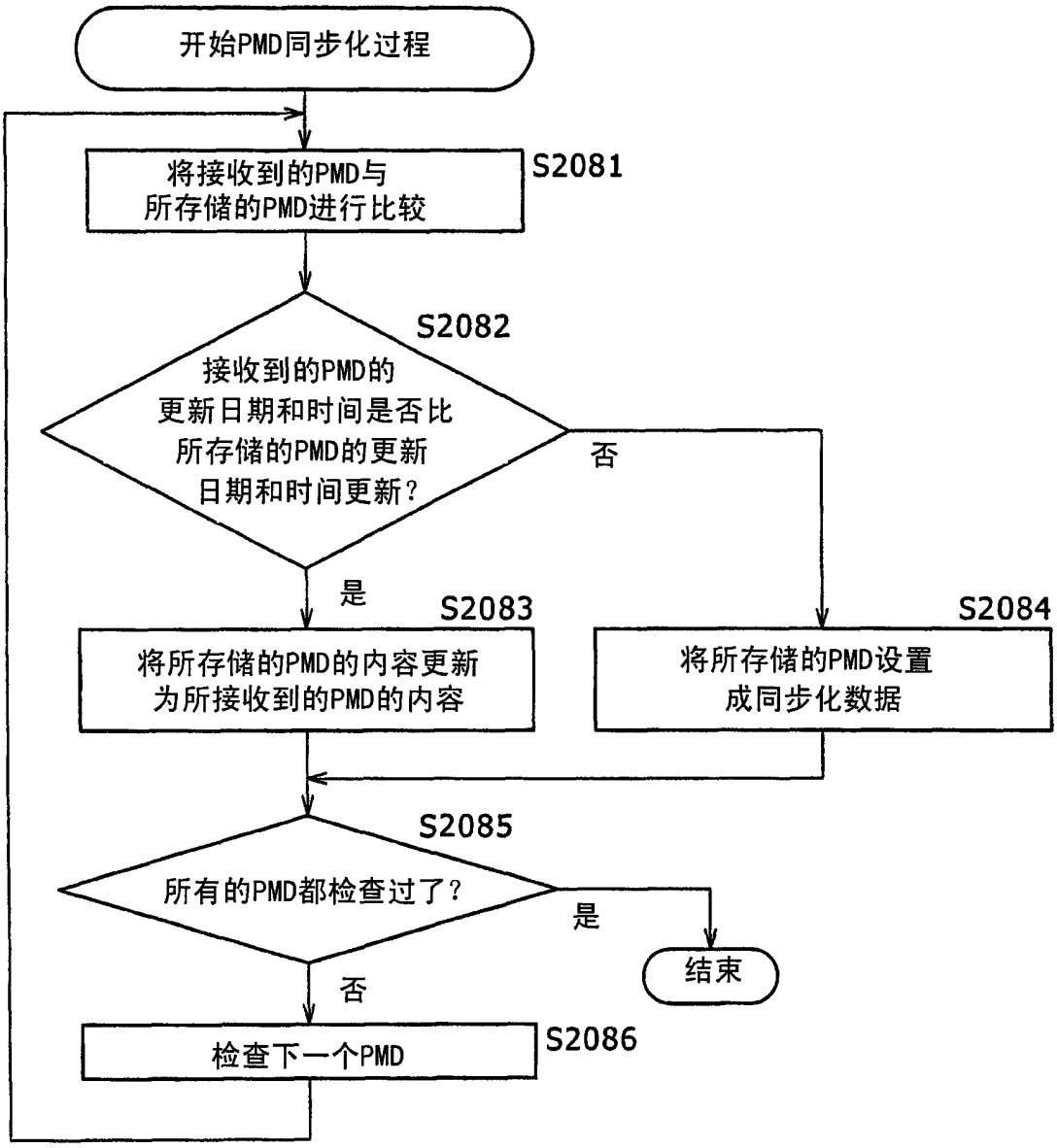

开始PMD同步化过程
将接收到的PMD与
所存储的PMD进行比较
S2081
S2082
接收到的PMD的
更新日期和时间是否比
所存储的PMD的更新
日期和时间更新?
否
是
S2083
将所存储的PMD的内容更新
为所接收到的PMD的内容
S2084
将所存储的PMD设置
成同步化数据
S2085
所有的PMD都检查过了?
是
结束
否
检查下一个PMD
S2086

图 31

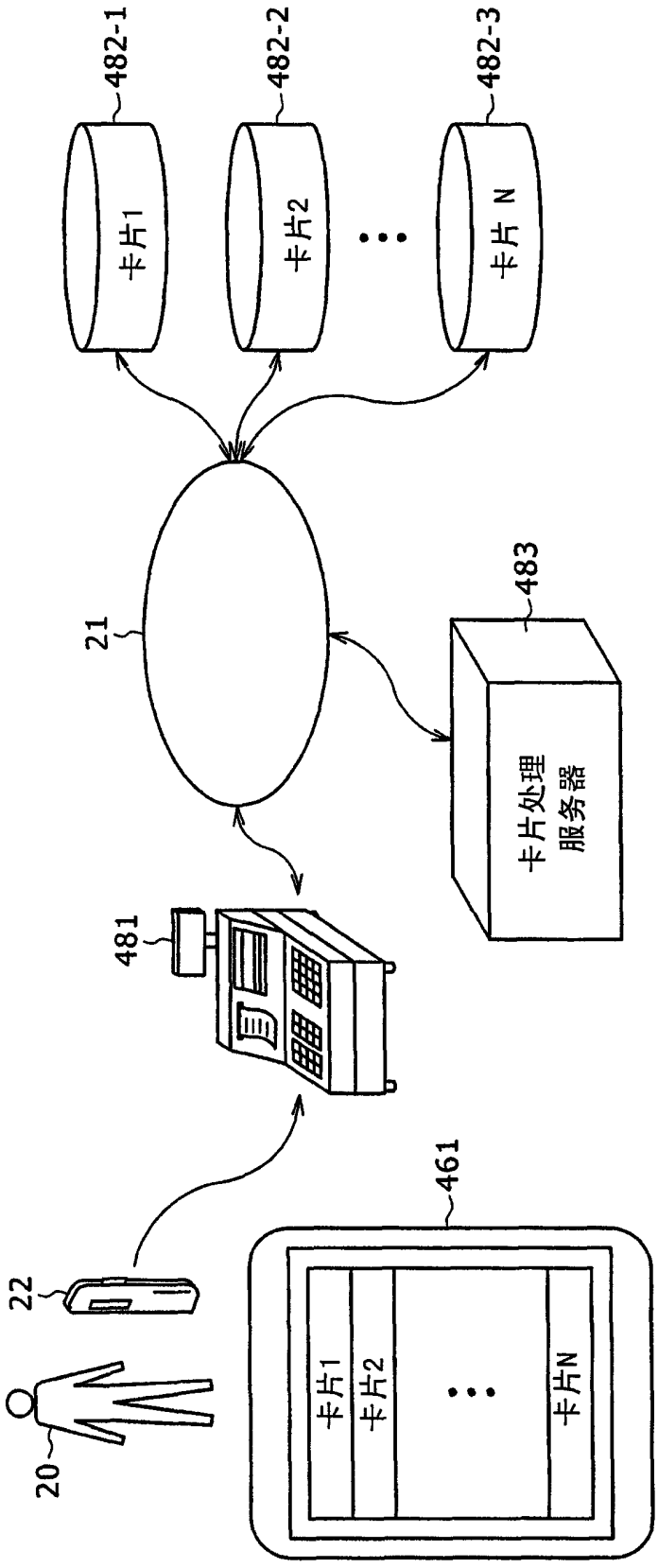

482-1
482-2
482-3
卡片1
卡片2
卡片 N
21
483
卡片处理
服务器
481
461
22
20
卡片1
卡片2
卡片N

图 32

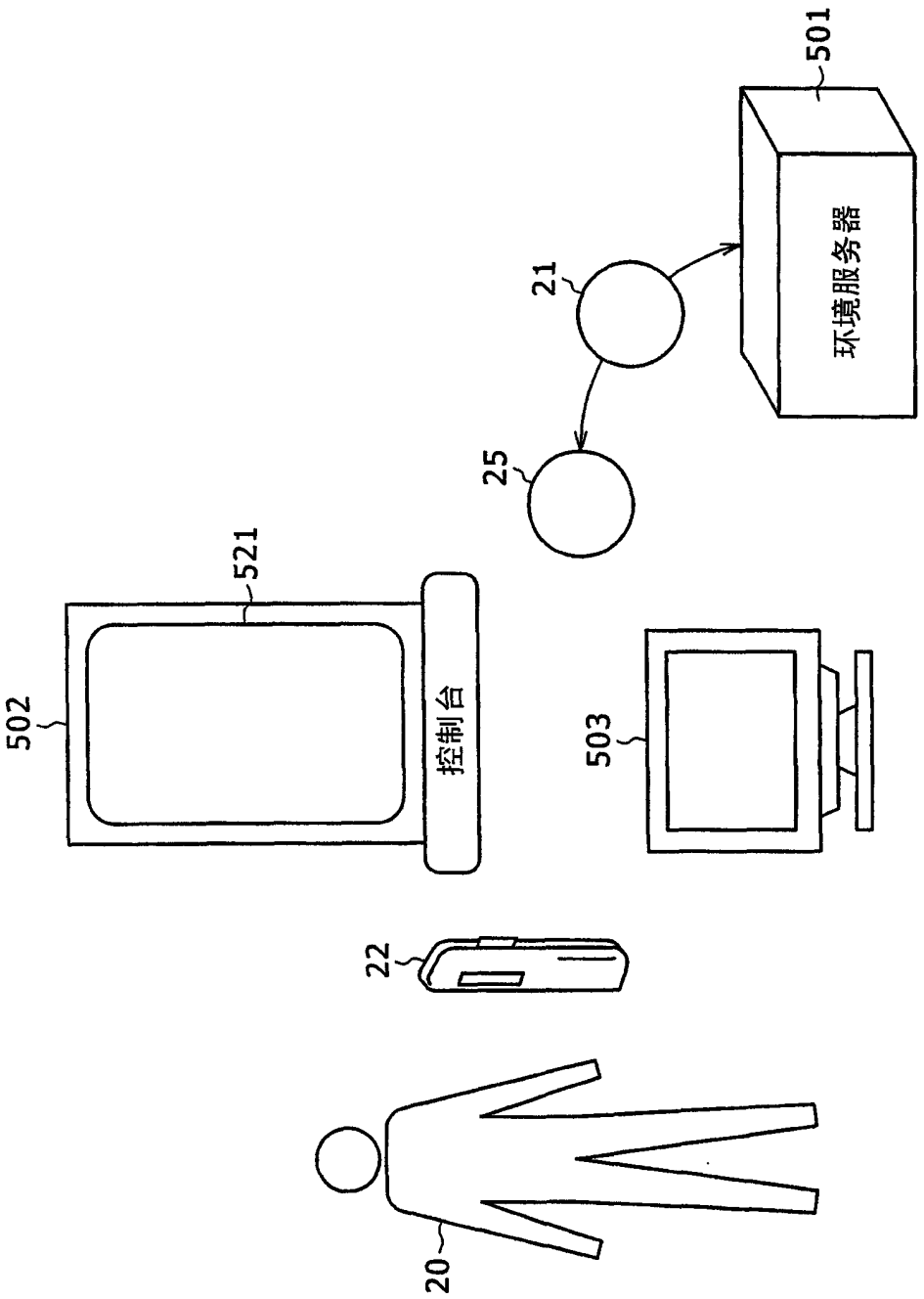


图 33

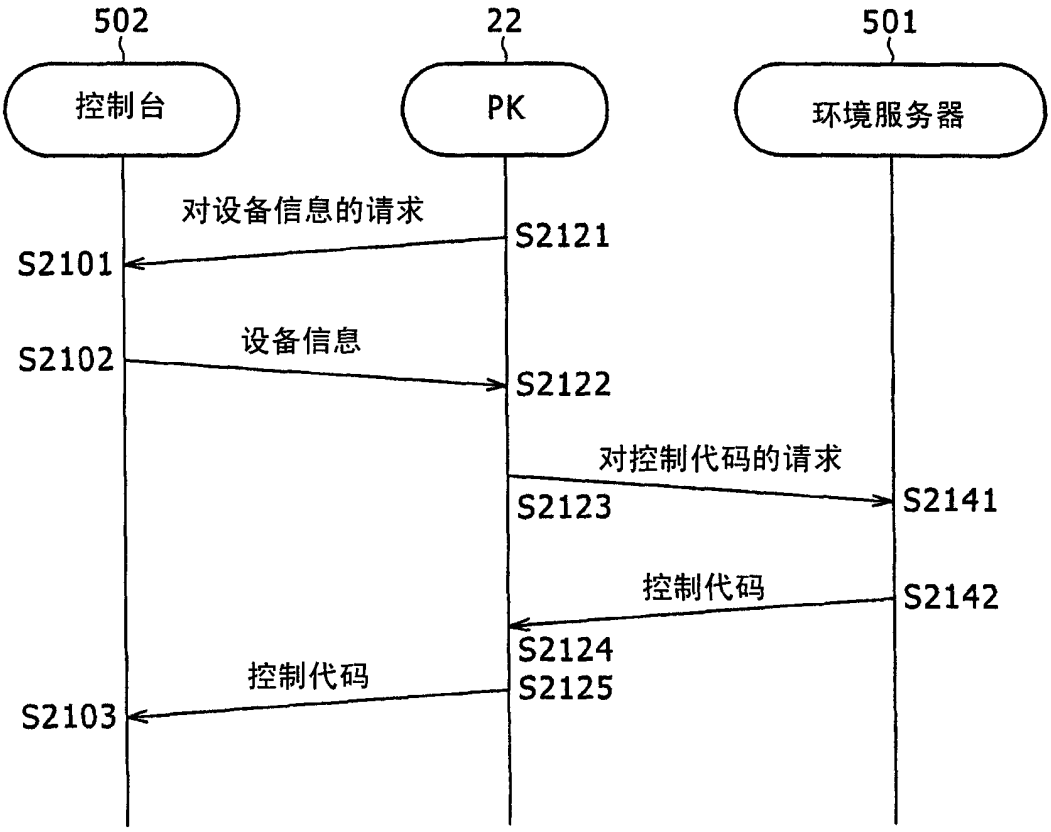

502
22
501
控制台
PK
环境服务器
对设备信息的请求
S2121
S2101
设备信息
S2102
S2122
对控制代码的请求
S2123
S2141
控制代码
S2142
S2124
控制代码
S2125
S2103

图 34

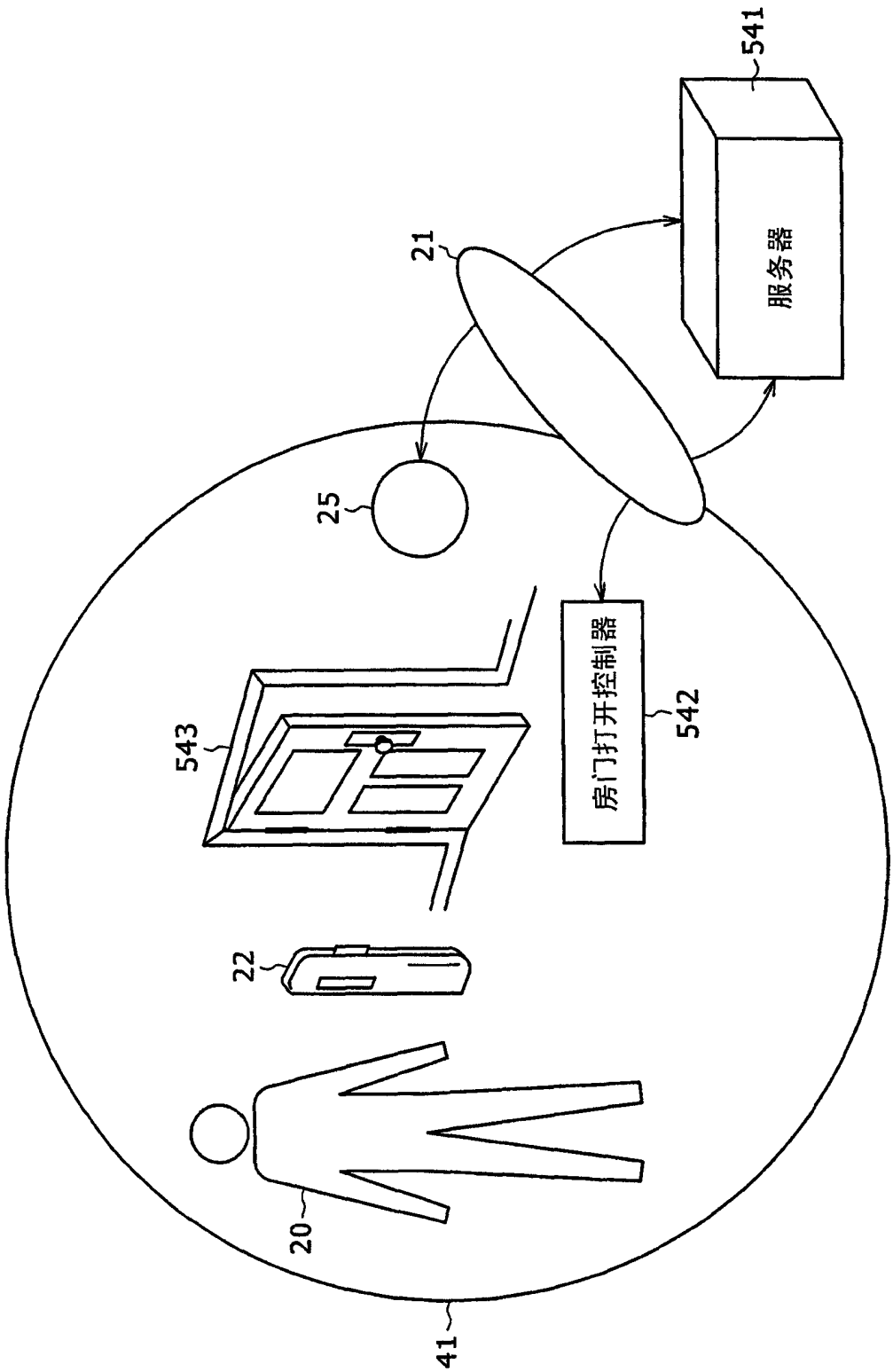


图 35

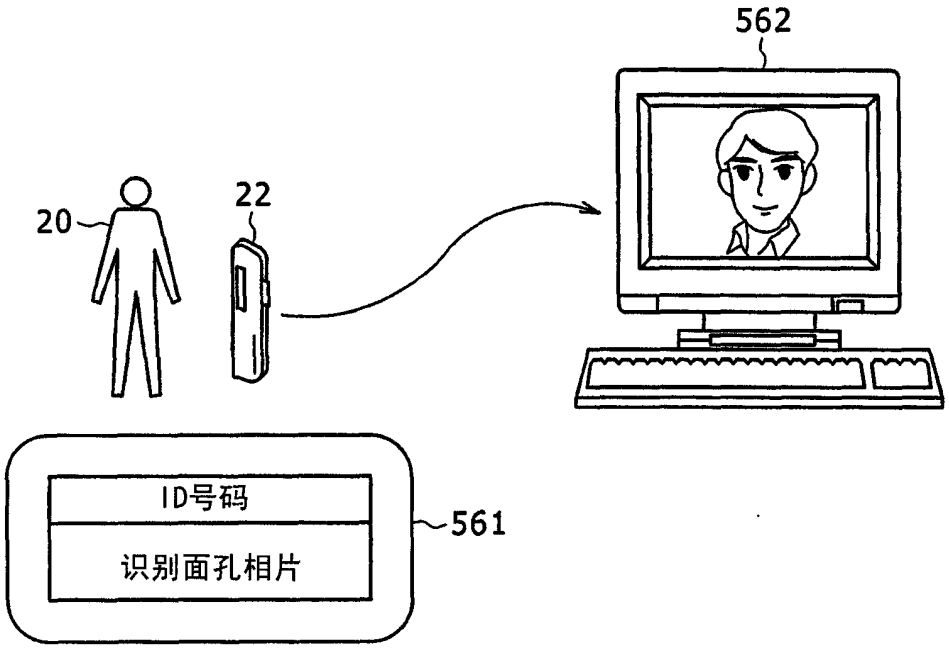


图 36

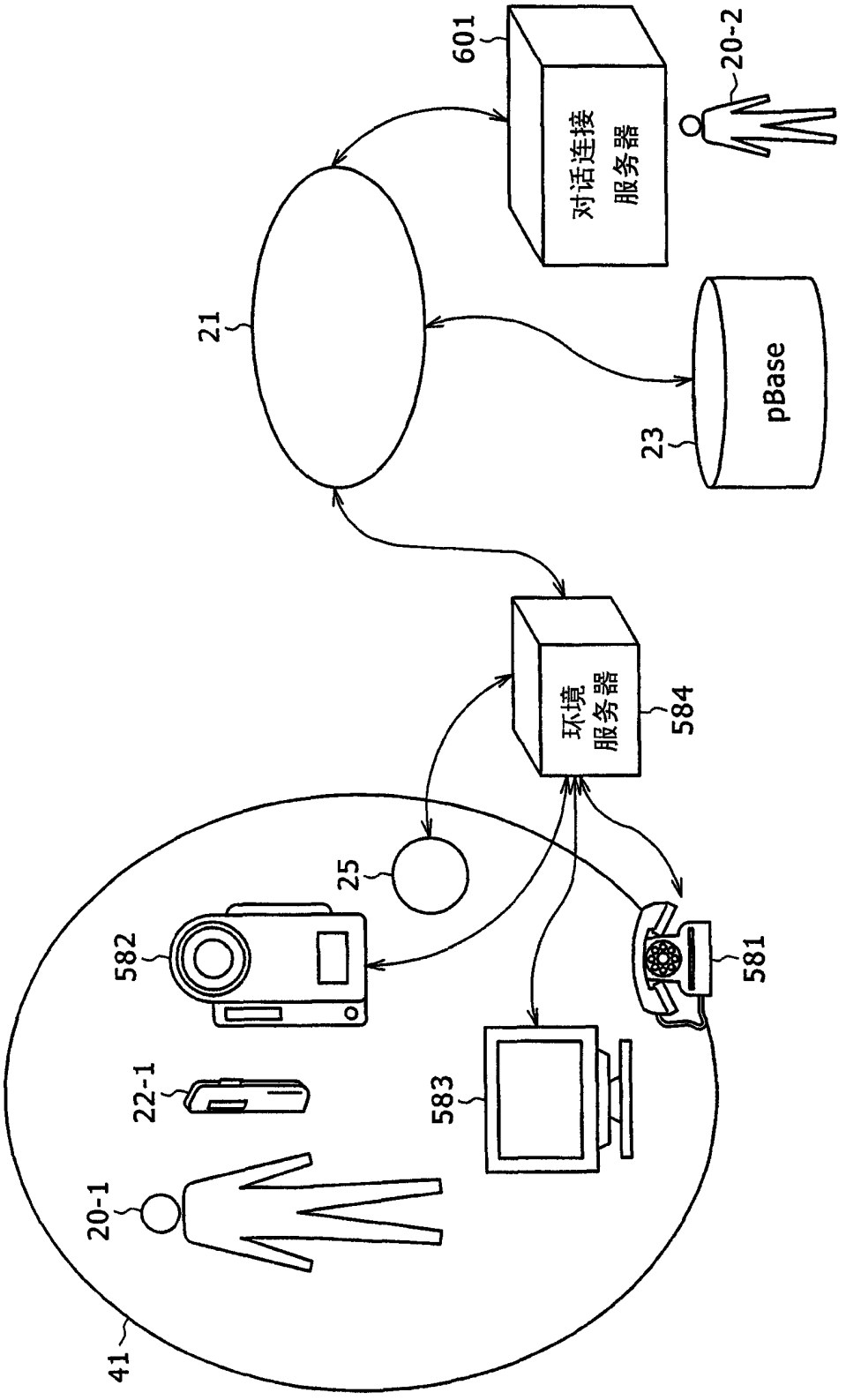


图 37

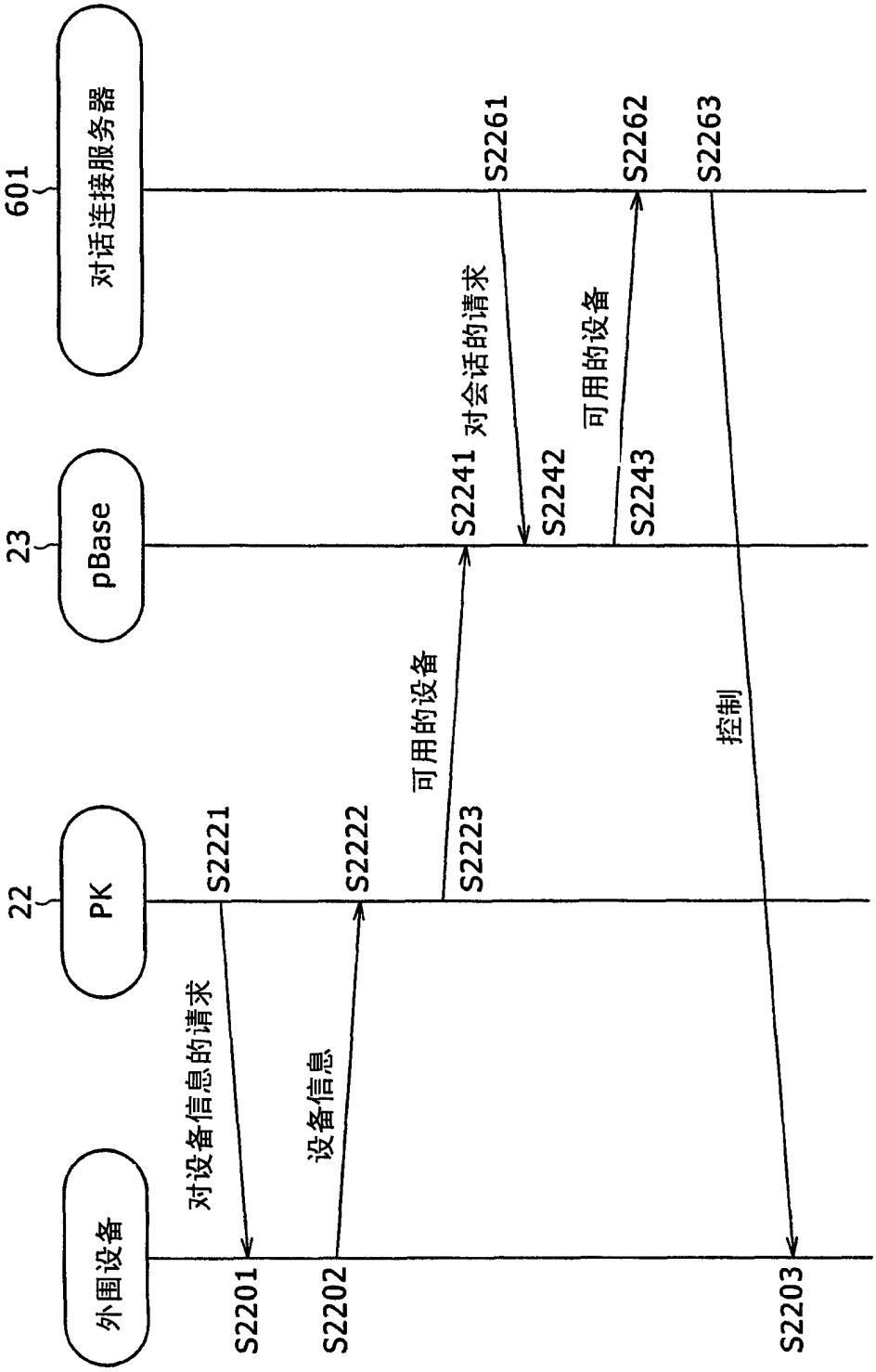

外围设备
22
PK
23
pBase
601
对话连接服务器
对设备信息的请求
设备信息
可用的设备
对会话的请求
可用的设备
控制
S2201
S2202
S2221
S2222
S2223
S2241
S2242
S2243
S2261
S2262
S2263
S2203

图 38

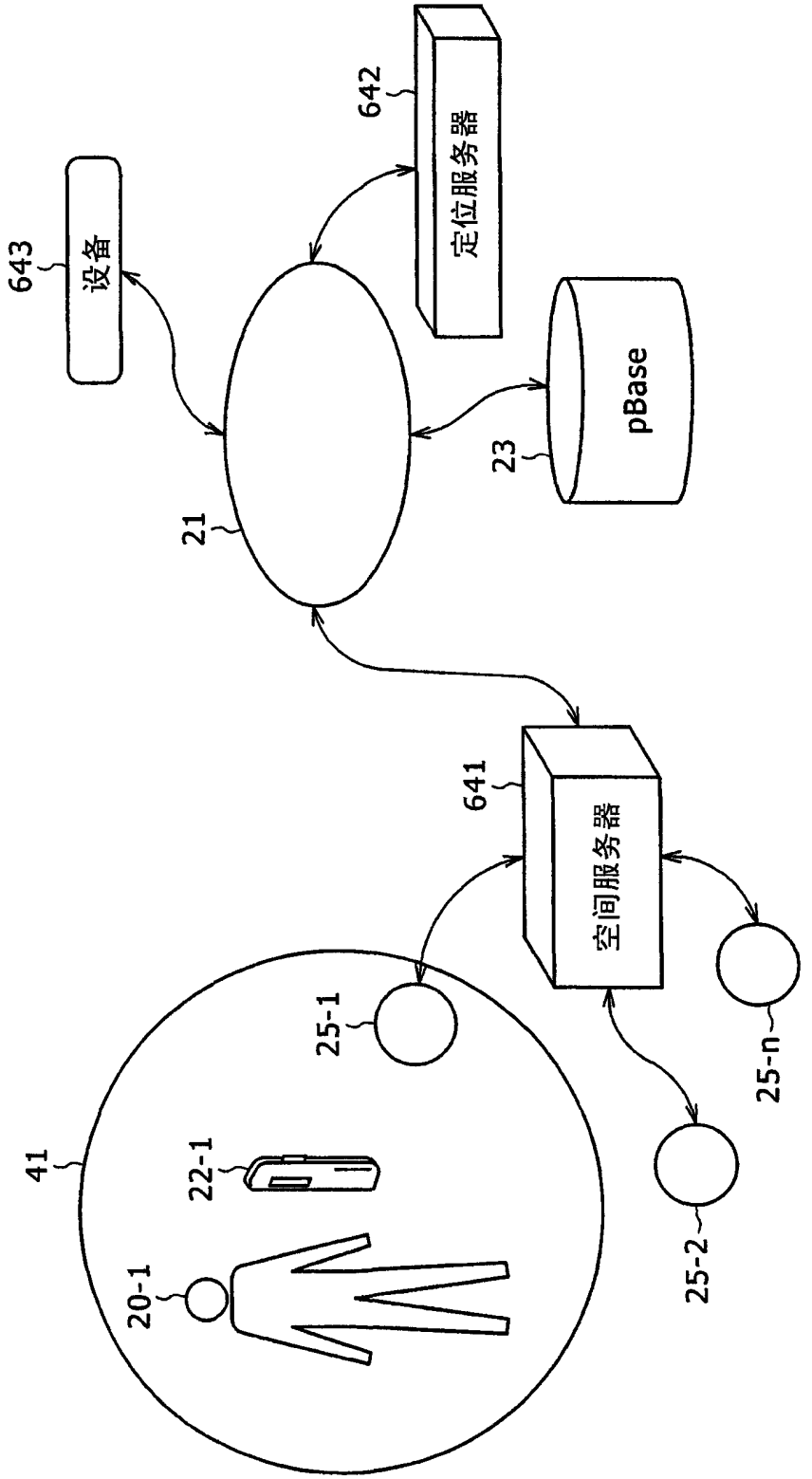


图 39

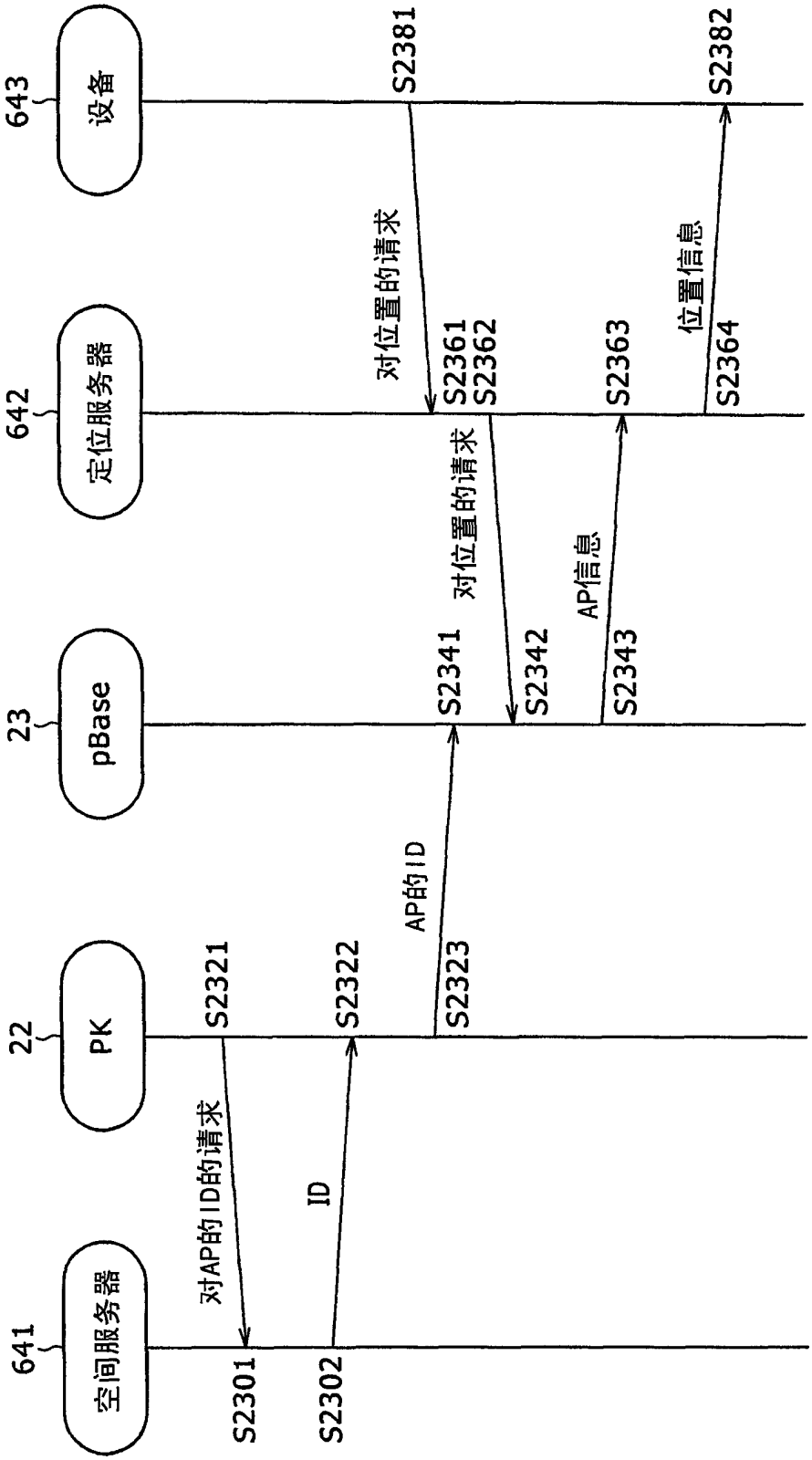

641
空间服务器
22
PK
23
pBase
642
定位服务器
643
设备
对AP的ID的请求
S2301
ID
S2302
S2321
S2322
AP的ID
S2323
S2341
对位置的请求
S2342
AP信息
S2343
对位置的请求
S2361
S2362
S2363
位置信息
S2364
S2381
S2382

图 40

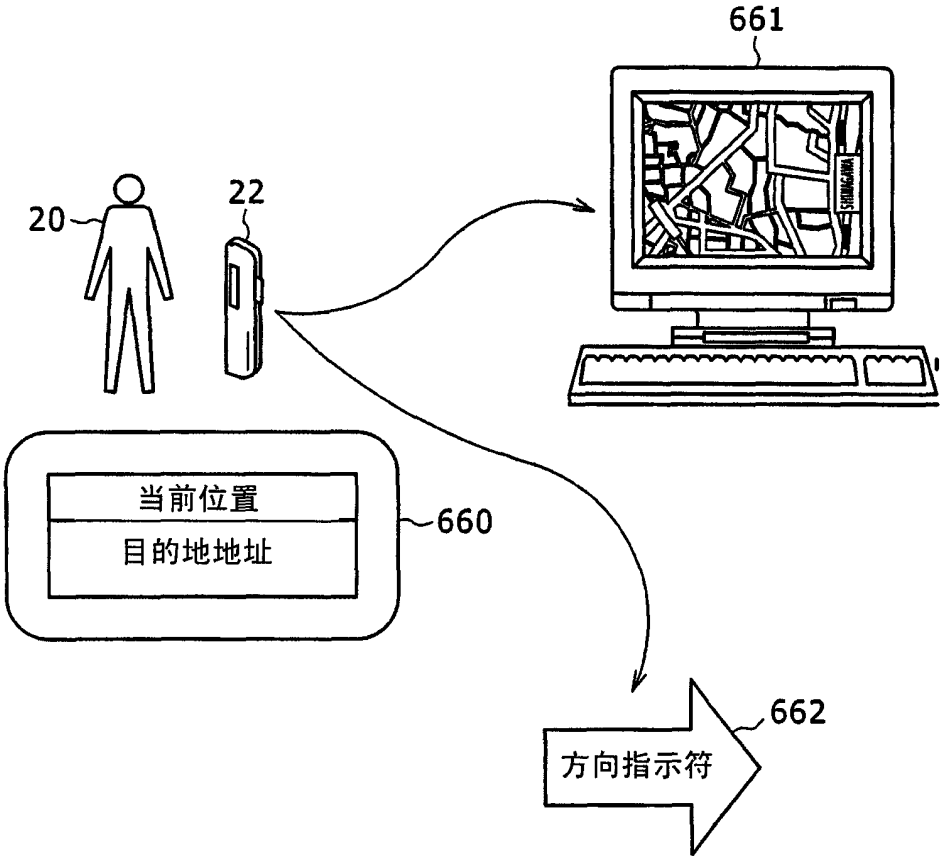


图 41

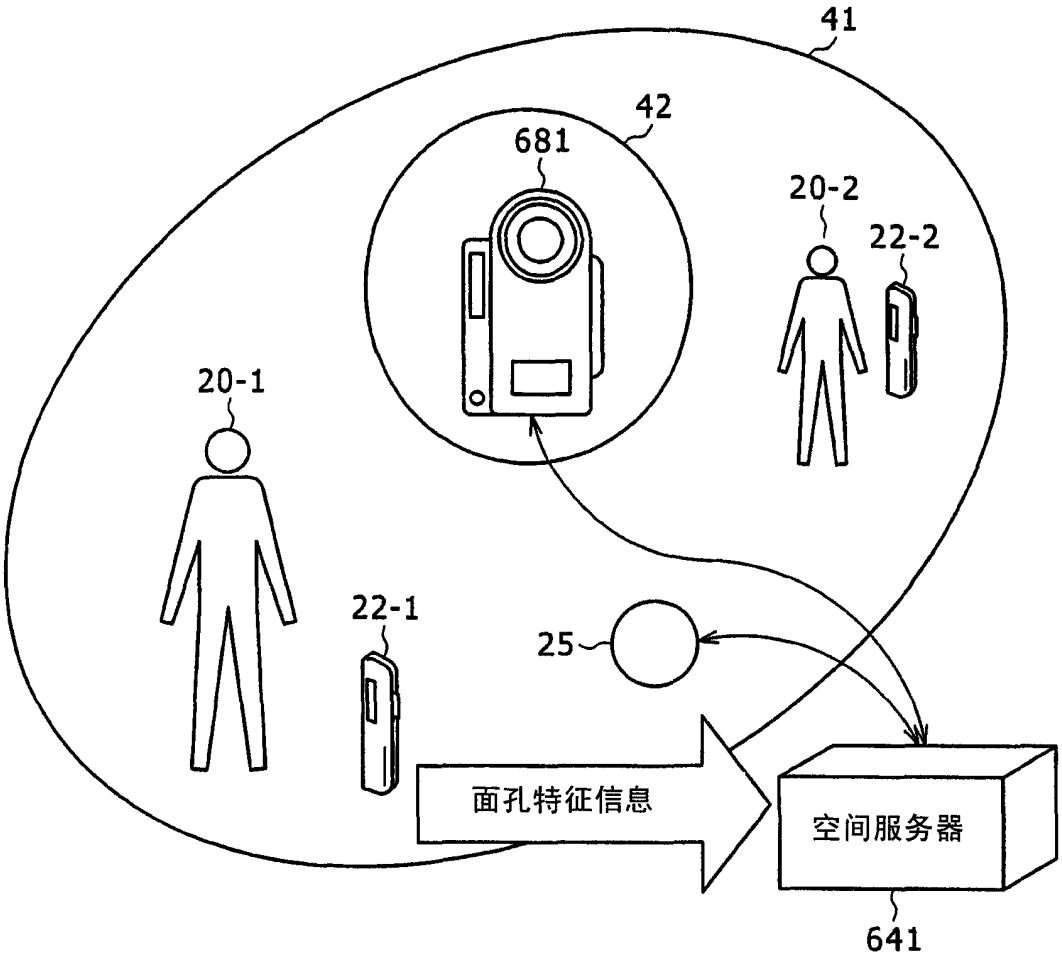


图 42

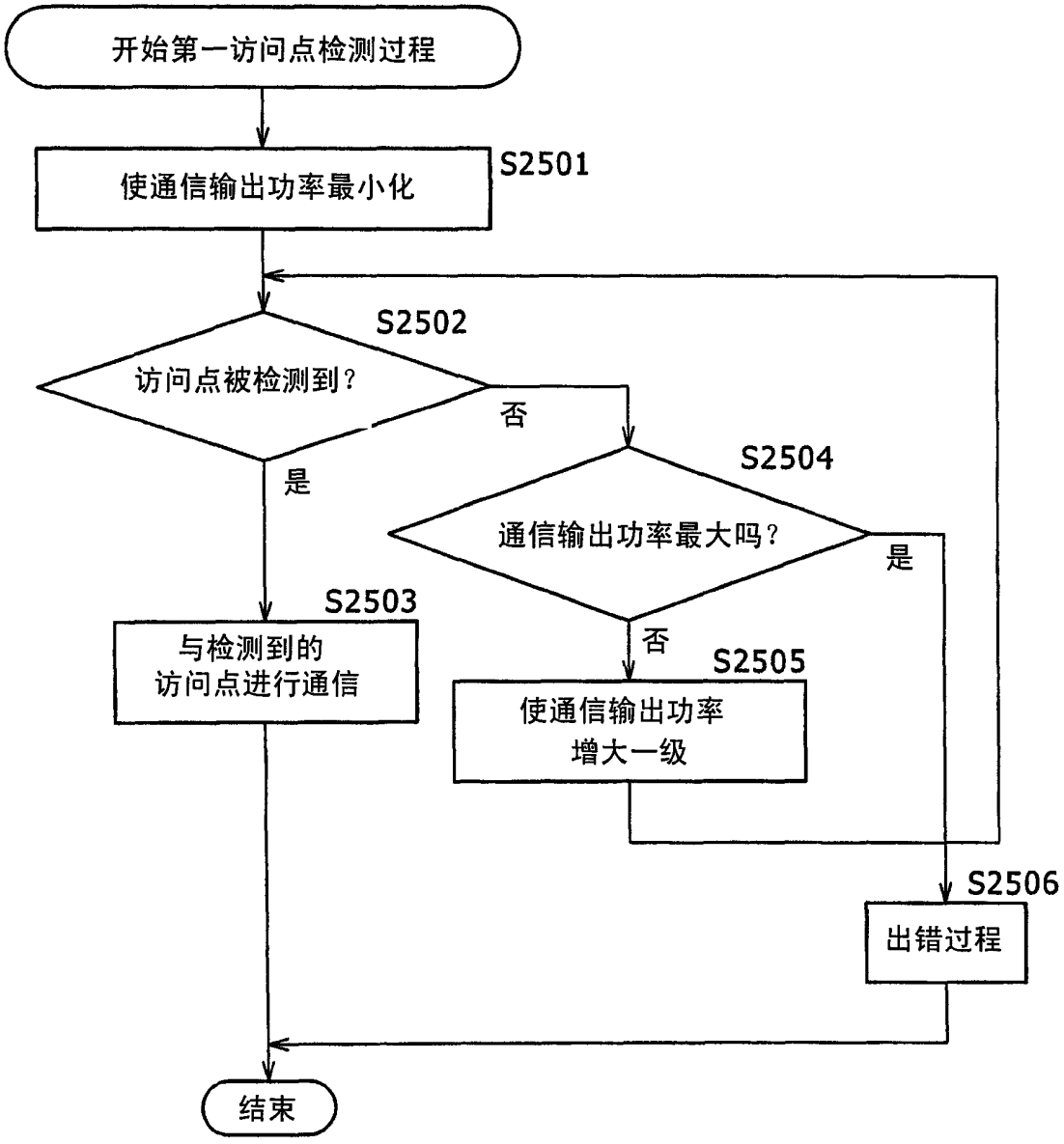

开始第一访问点检测过程
使通信输出功率最小化
S2501
S2502
访问点被检测到？
否
是
S2504
通信输出功率最大吗？
是
否
S2503
与检测到的
访问点进行通信
S2505
使通信输出功率
增大一级
S2506
出错过程
结束

图 43

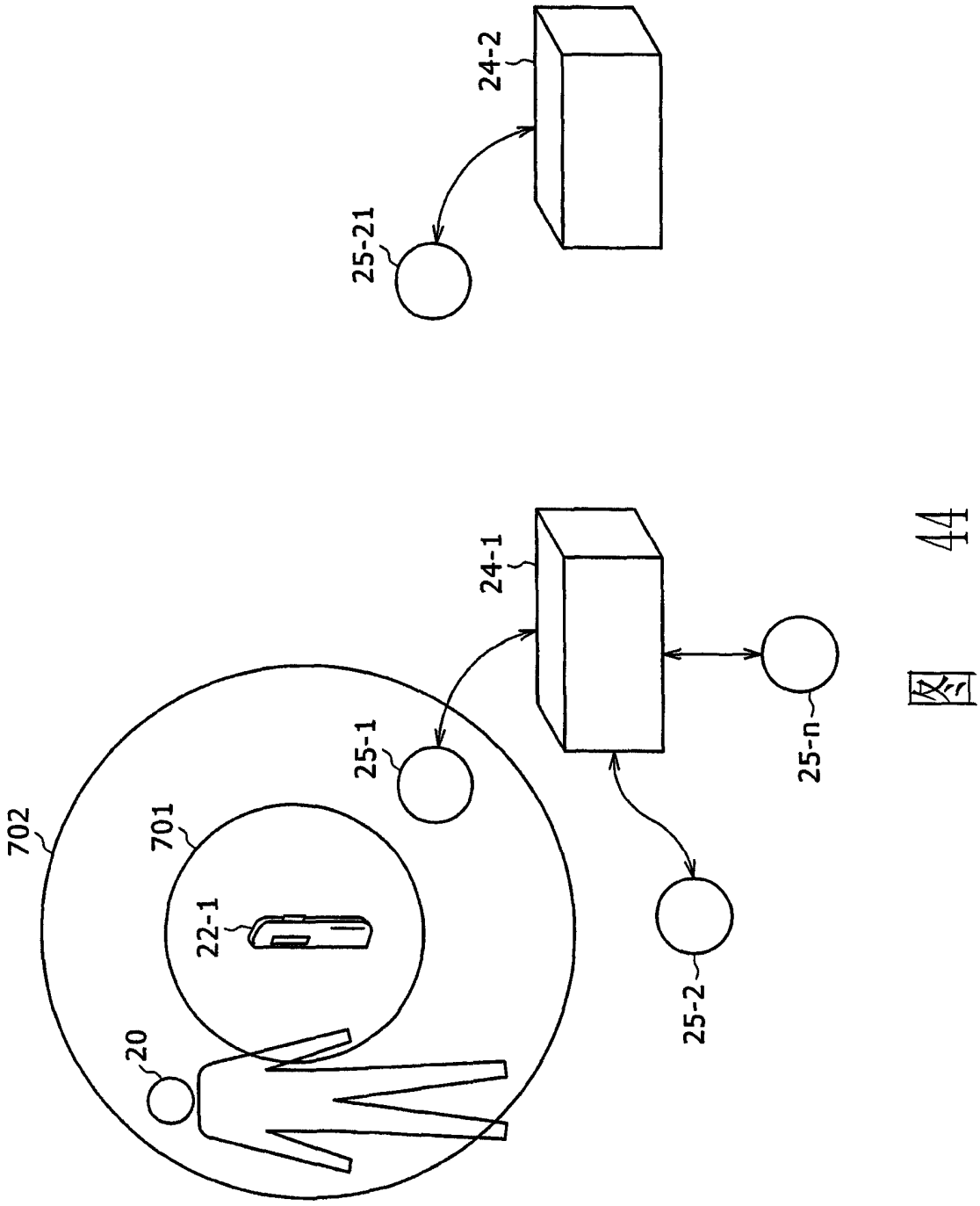


图 44

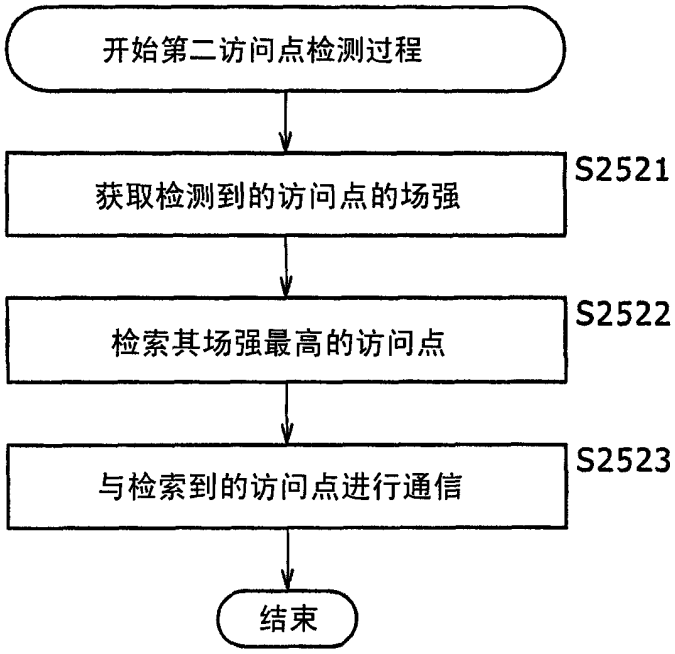

开始第二访问点检测过程
获取检测到的访问点的场强
S2521
检索其场强最高的访问点
S2522
与检索到的访问点进行通信
S2523
结束

图 45

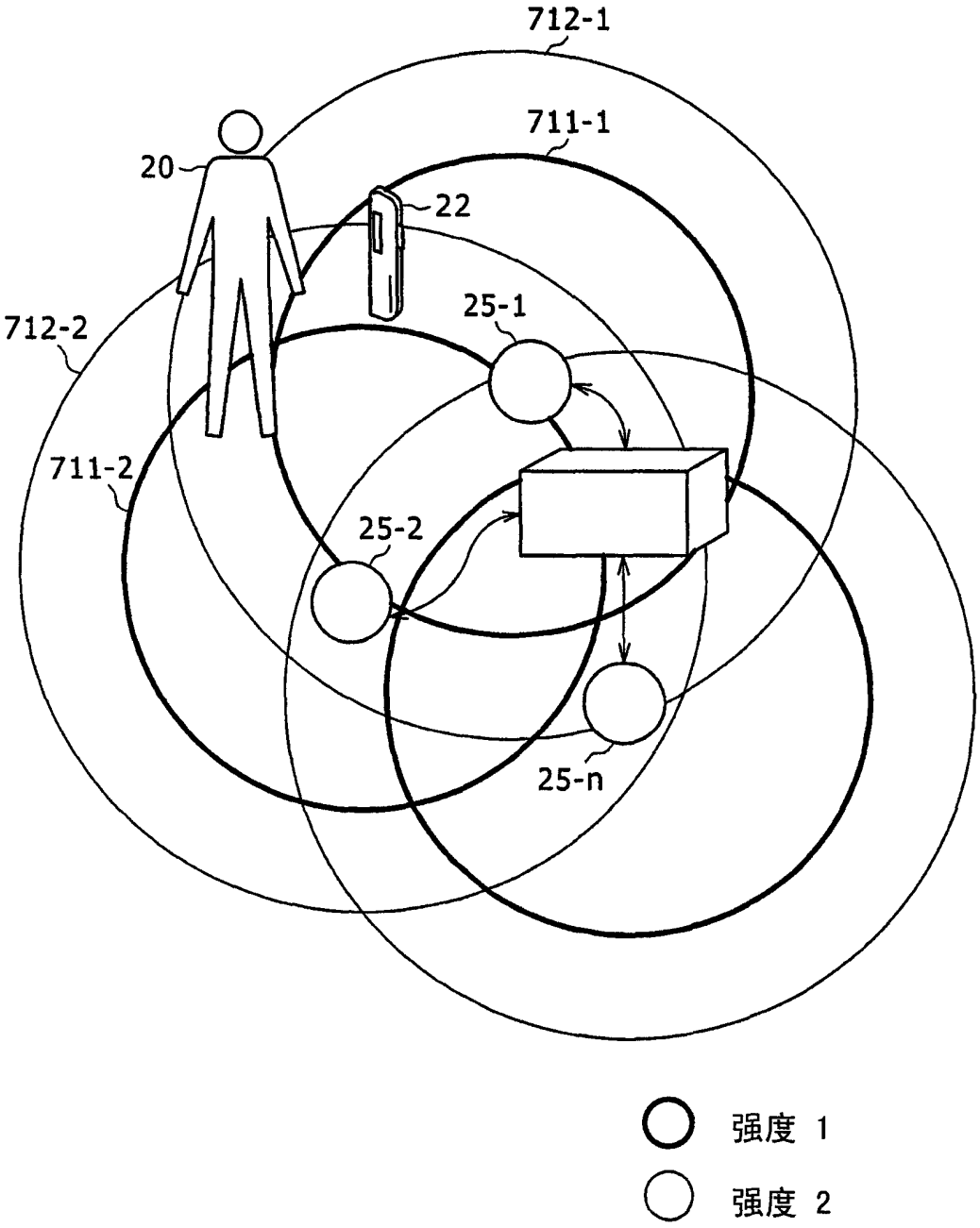


图 46

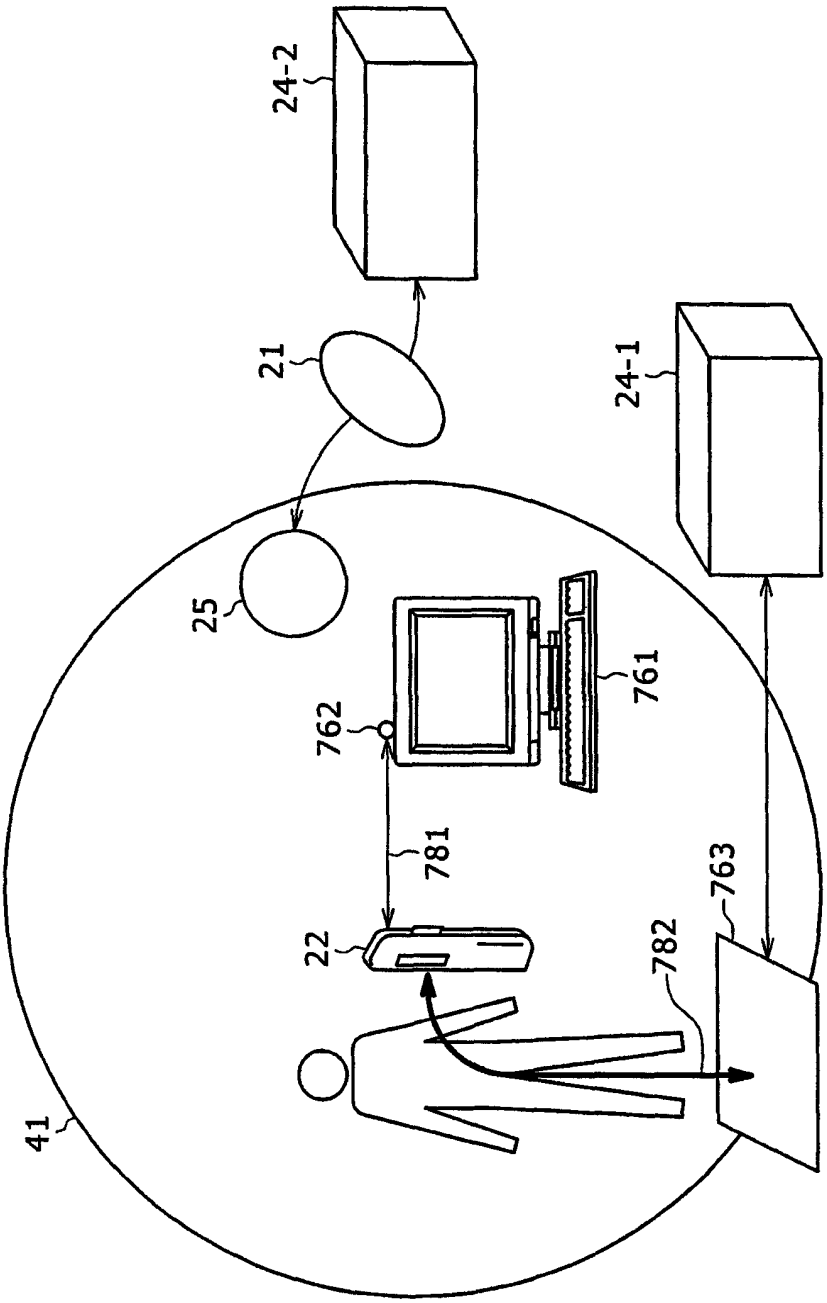


图 47

801

属性	内容
节目	节目代码条目
名字	FOO
PUSH	"接收到的紧急消息……"

图 48

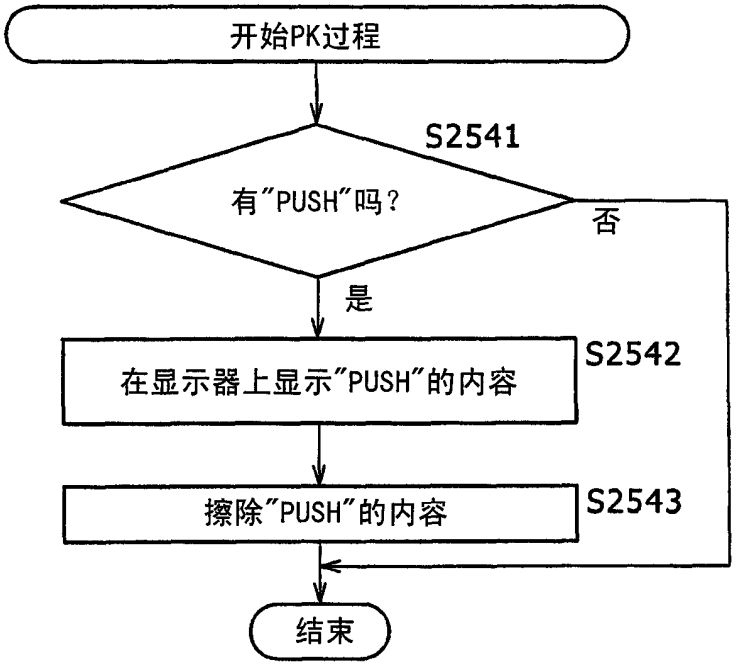


图 49

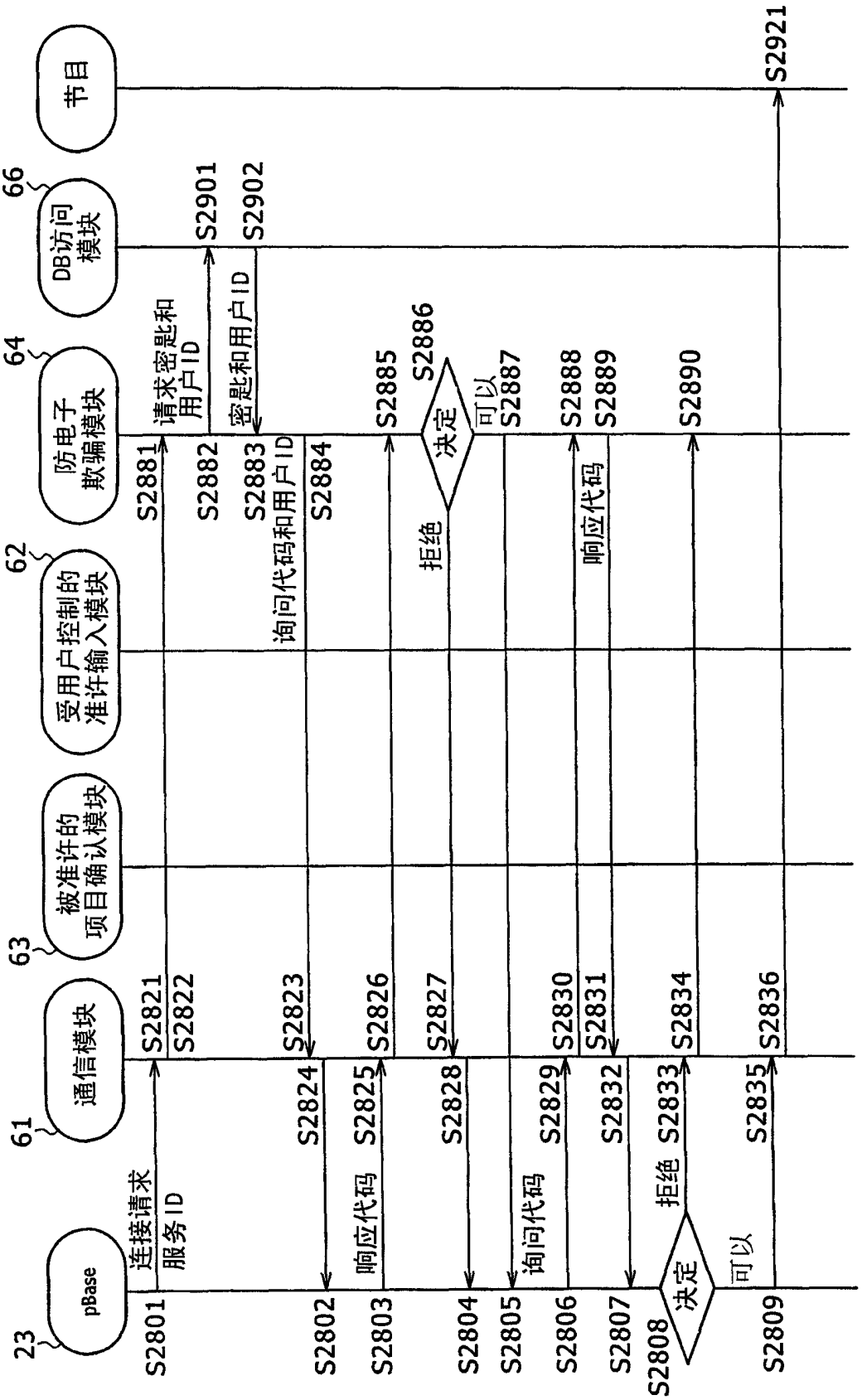

23
pBase
61
通信模块
63
被准许的项目确认模块
62
受用户控制的准许输入模块
64
防电子欺骗模块
66
DB访问模块
节目
S2801
连接请求
服务ID
S2802
S2803
响应代码
S2804
S2805
询问代码
S2806
S2807
S2808
决定
拒绝
可以
S2809
S2821
S2822
S2823
S2824
S2825
响应代码
S2826
S2827
S2828
S2829
S2830
S2831
S2832
S2833
拒绝
S2834
S2835
可以
S2836
S2881
请求密匙和用户ID
S2882
S2883
密匙和用户ID
询问代码和用户ID
S2884
S2885
S2886
决定
拒绝
可以
S2887
S2888
响应代码
S2889
S2890
S2901
S2902
S2921

图 50

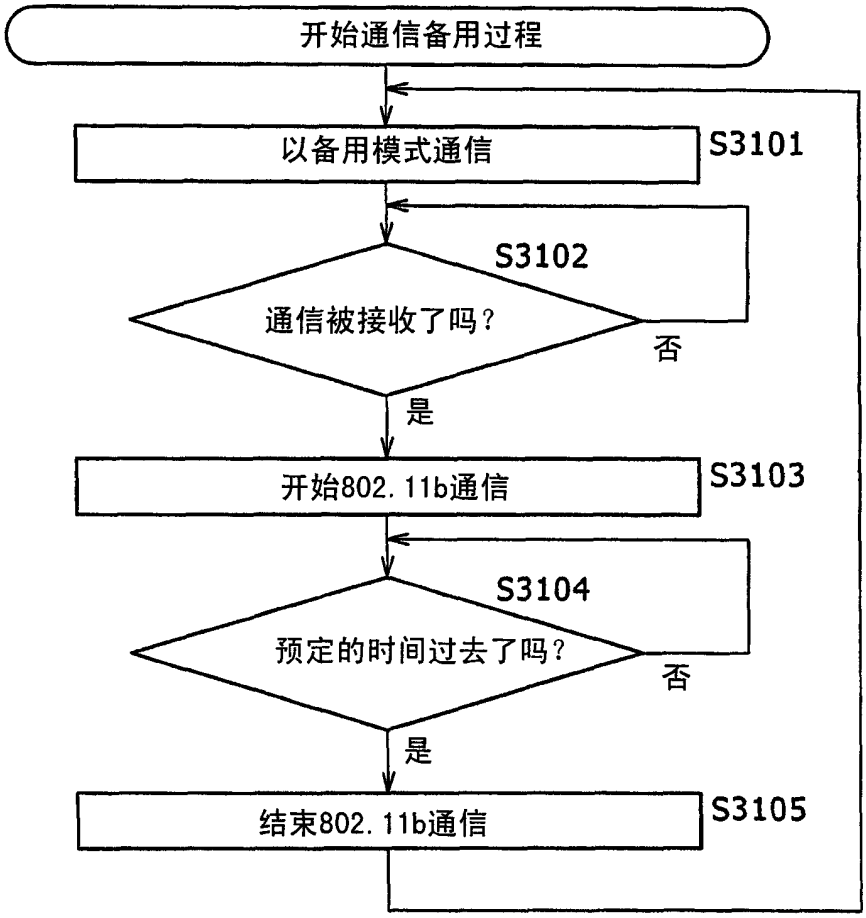

开始通信备用过程
以备用模式通信
S3101
S3102
通信被接收了吗？
否
是
开始802.11b通信
S3103
S3104
预定的时间过去了吗？
否
是
结束802.11b通信
S3105

图 51

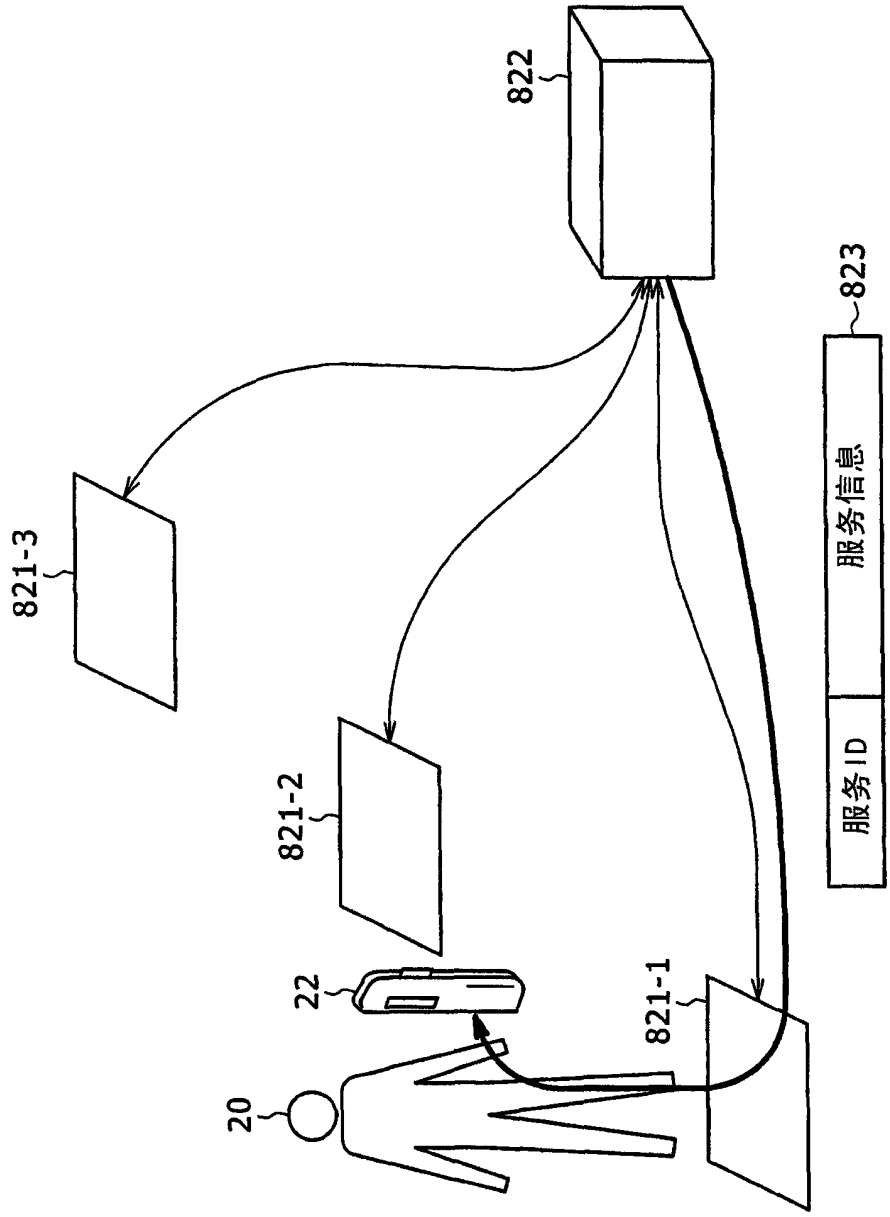


图 52

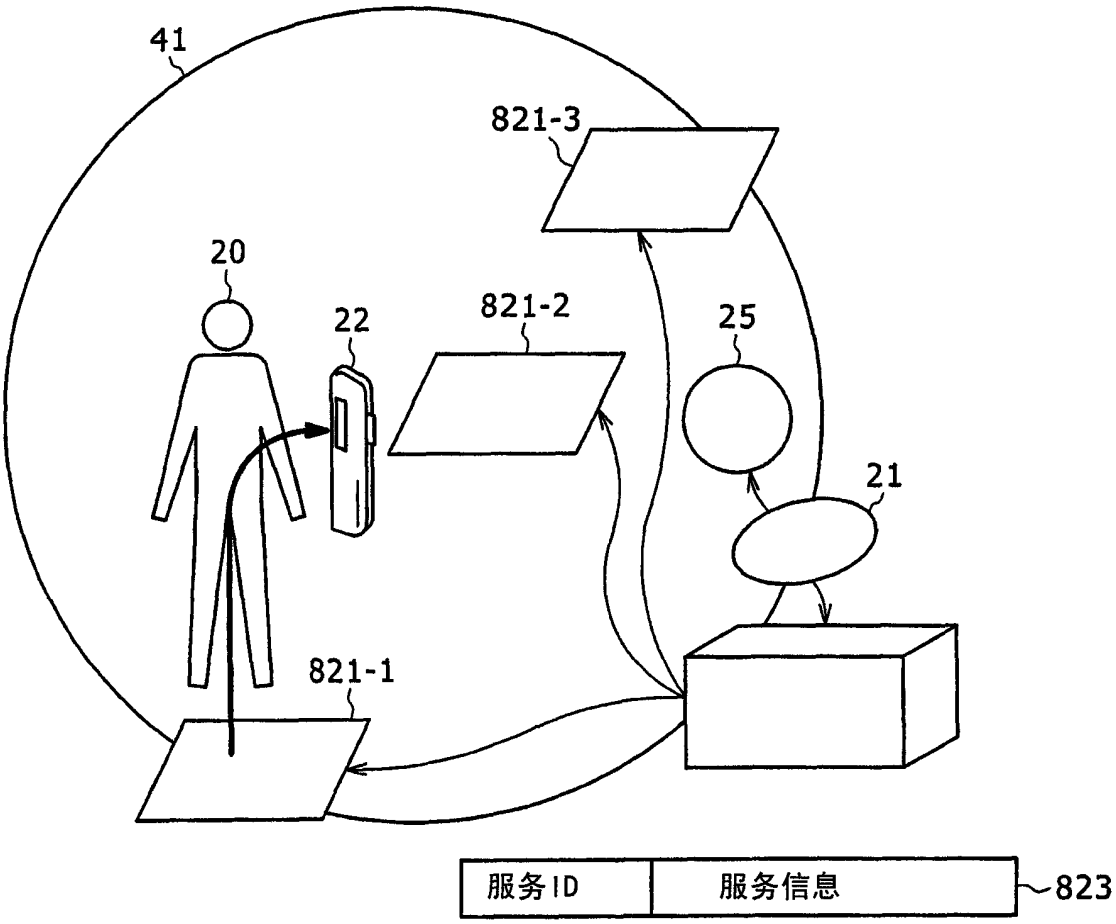


图 53

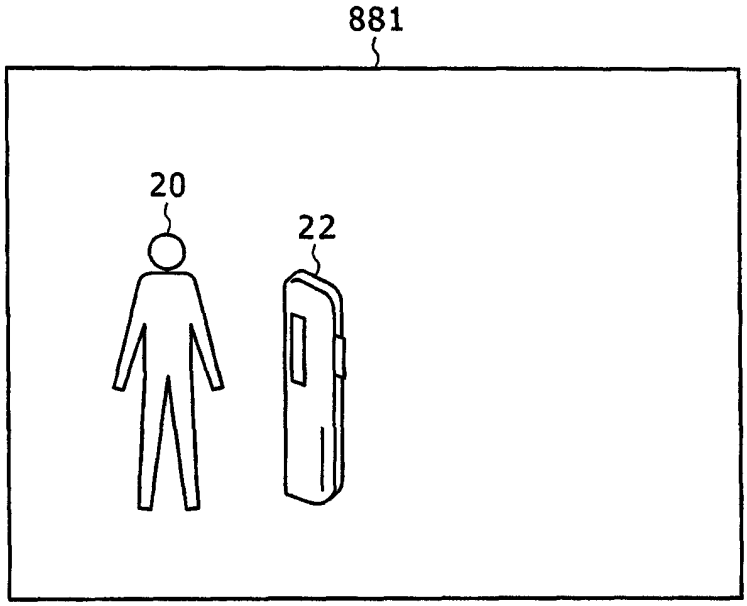


图 54A

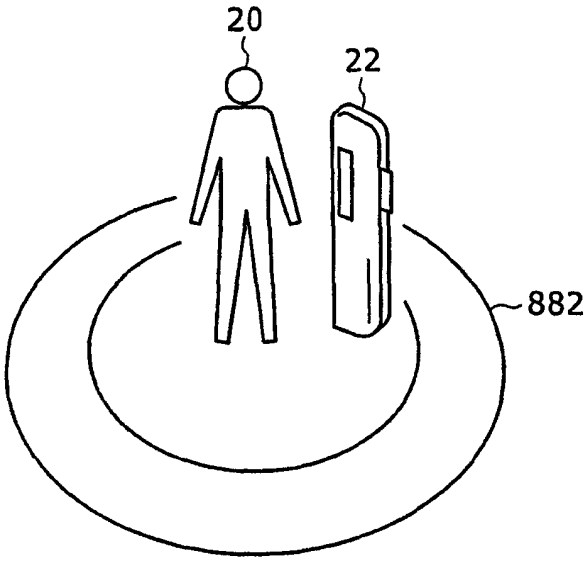


图 54B

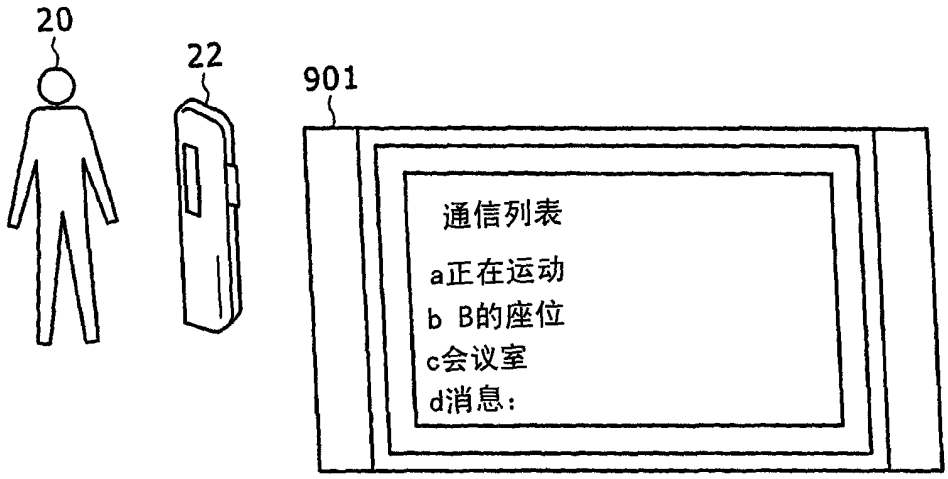


图 55

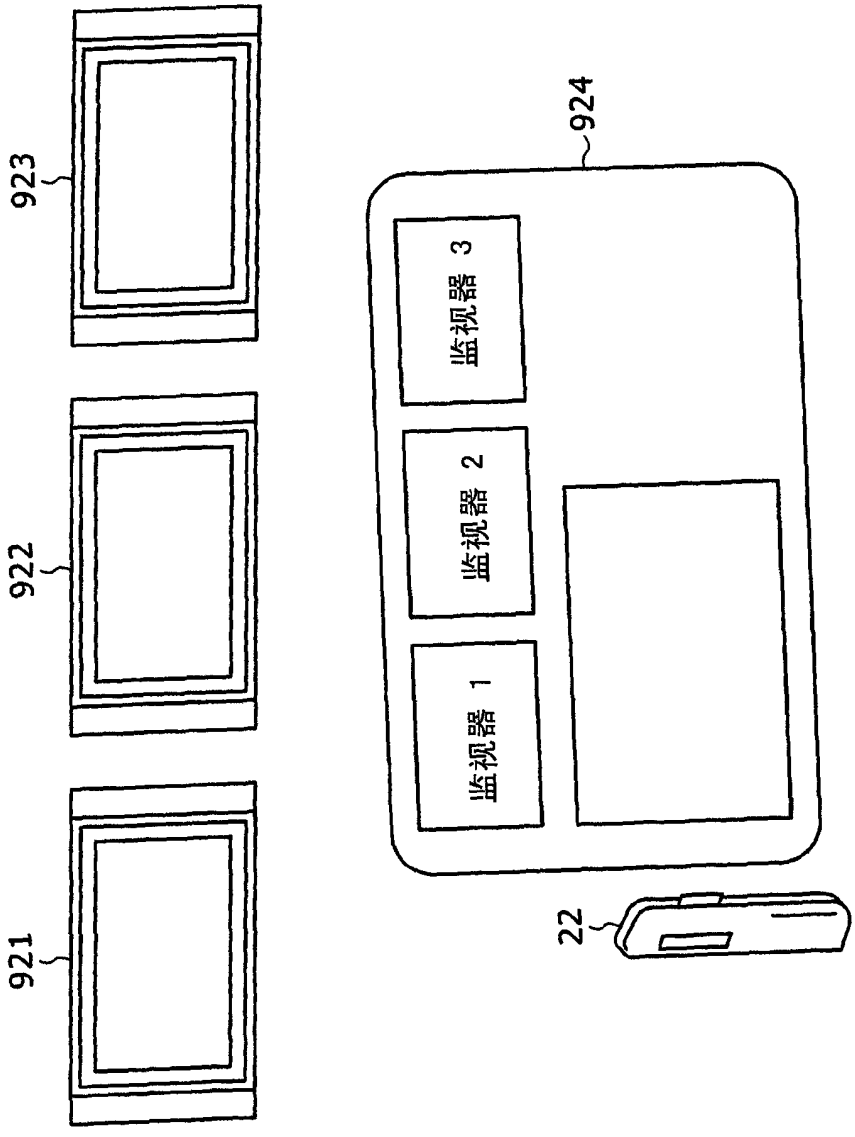


图 56

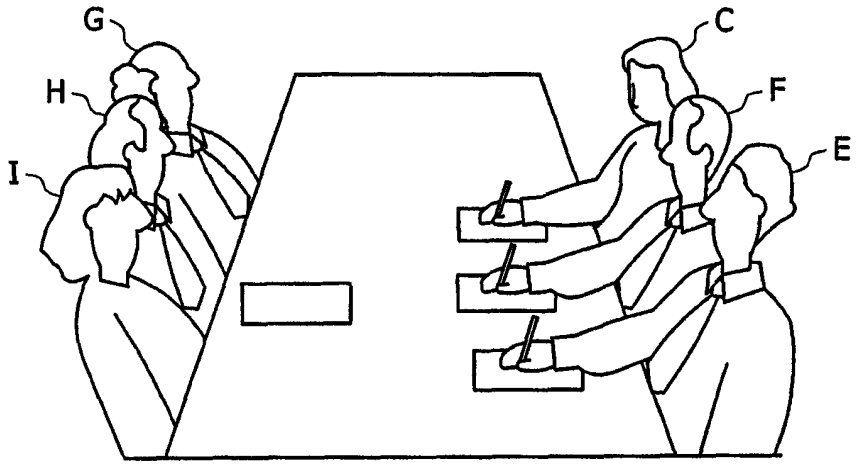


图 57

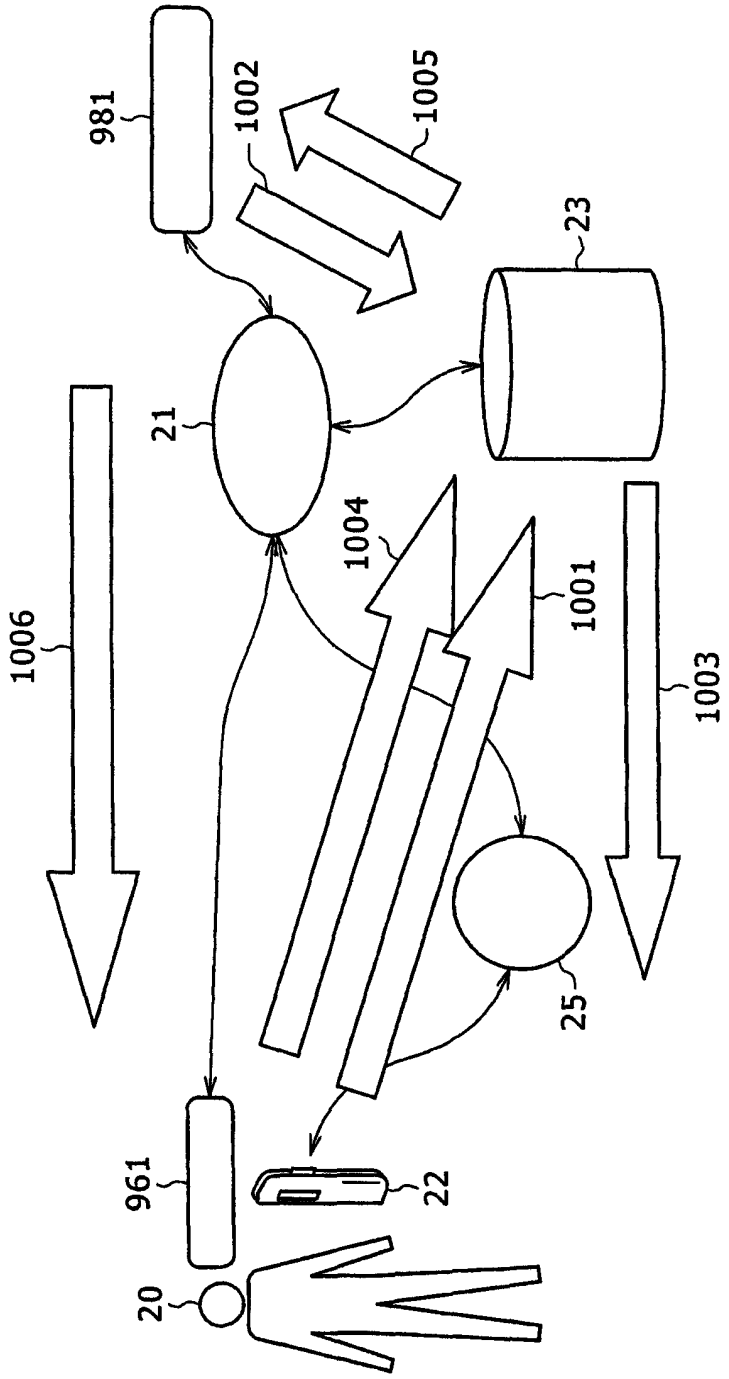


图 58

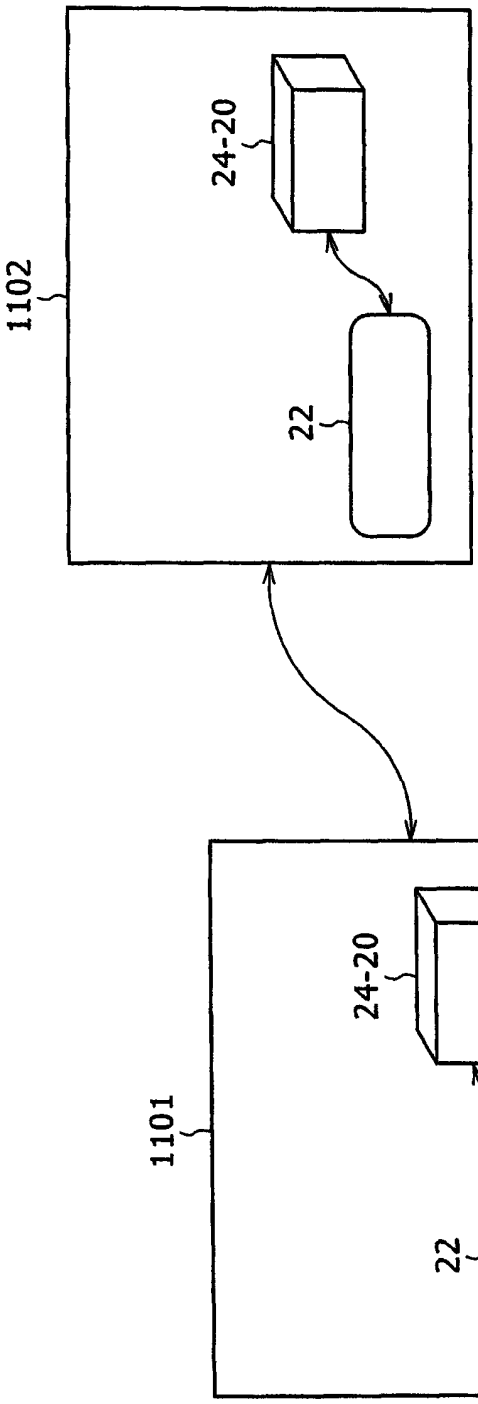


图 59

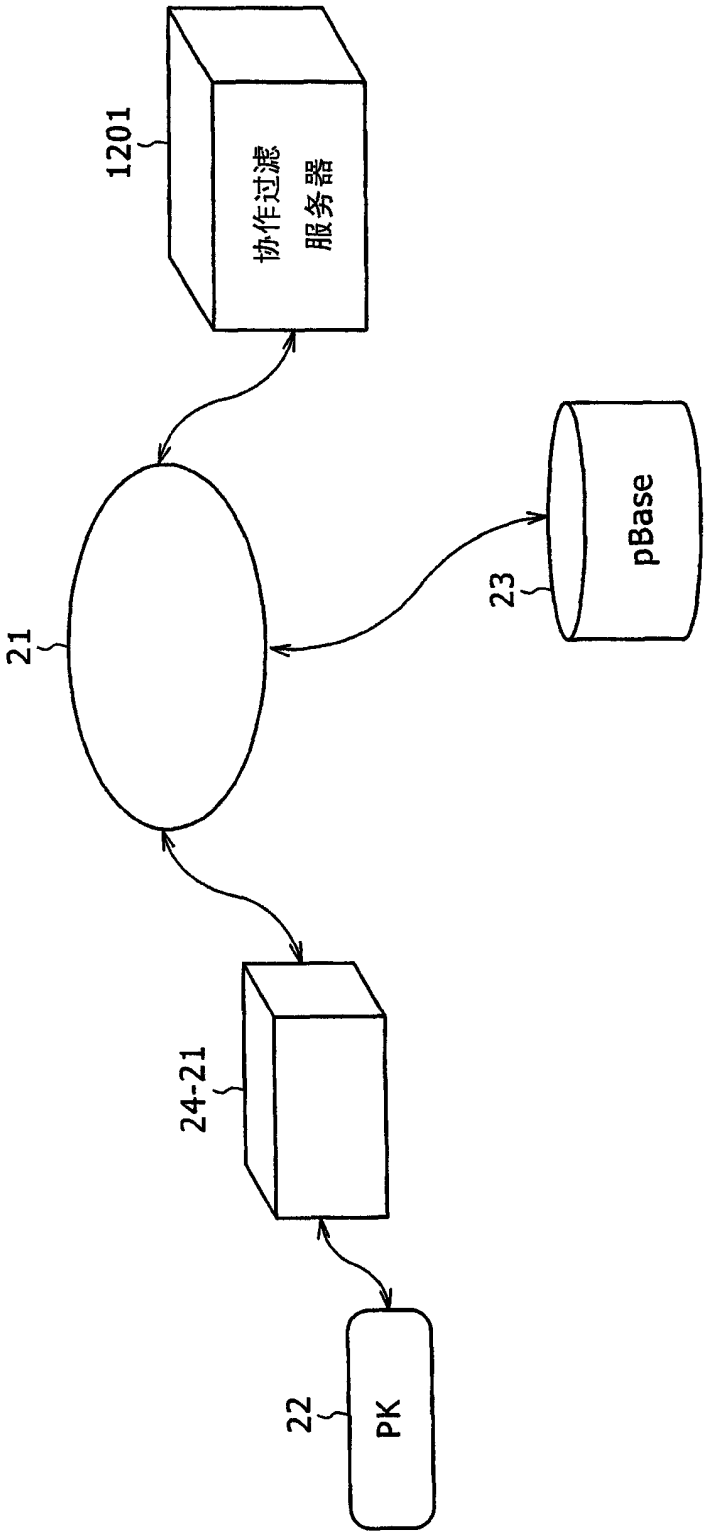


图 60

1.一种用于存储与用户有关的用户信息并与多个其它的信息处理设备进行通信的信息处理设备，所述信息处理设备包括：

呈现装置，用于呈现要被所述其它信息处理设备读取或改变的用户信息；

指定装置，用于指定准许读取或改变由所述呈现装置呈现的用户信息；

识别装置，用于识别所述其它信息处理设备；以及

存储装置，用于存储由与所述其它信息处理设备相关联的所述识别装置识别出的所述其它信息处理设备来读取或改变的用户信息。

2.如权利要求 1 所述的信息处理设备，其特征在于，所述信息处理设备还包括用于进行准静电场通信、电磁波通信、光通信或电通信的通信装置。

3.如权利要求 1 所述的信息处理设备，其特征在于，

所述信息处理设备外部的设备被用作输入或输出接口。

4. 如权利要求 1 所述的信息处理设备，其特征在于，

当与所述其它信息处理设备进行初次通信时，用于识别所述信息处理设备的信息被发送到所述其它信息处理设备。

5. ~~(有修改)~~ 如权利要求 2 所述的信息处理设备，其特征在于，

当与所述其它信息处理设备进行初次通信时，产生由所述信息处理设备用来加密信息的第一代码以及与所述第一代码相应产生的第二代码，并且所述第一代码被发送到所述其它信息处理设备，并且

由所述其它信息处理设备用来加密信息的第三代码是通过所述通信装置获得的。

6. 如权利要求 1 所述的信息处理设备，其特征在于，

所述用户信息是基于所述其它信息处理设备所提供的内容使用历史来更新的。