



(12) 发明专利

(10) 授权公告号 CN 109660505 B

(45) 授权公告日 2022.01.14

(21) 申请号 201811175067.3

(51) Int.CI.

(22) 申请日 2018.10.10

H04L 9/40 (2022.01)

(65) 同一申请的已公布的文献号

H04W 12/065 (2021.01)

申请公布号 CN 109660505 A

G10L 15/22 (2006.01)

G06F 21/32 (2013.01)

(43) 申请公布日 2019.04.19

(56) 对比文件

(30) 优先权数据

CN 105959287 A, 2016.09.21

2017-197216 2017.10.10 JP

CN 101719248 A, 2010.06.02

(73) 专利权人 佳能株式会社

US 2014223518 A1, 2014.08.07

地址 日本东京

CN 102419847 A, 2012.04.18

(72) 发明人 舟根奈央

CN 101789064 A, 2010.07.28

(74) 专利代理机构 中国贸促会专利商标事务所
有限公司 11038

审查员 肖丽金

代理人 刘前红

权利要求书3页 说明书20页 附图14页

(54) 发明名称

系统、语音操作设备、控制方法以及存储介

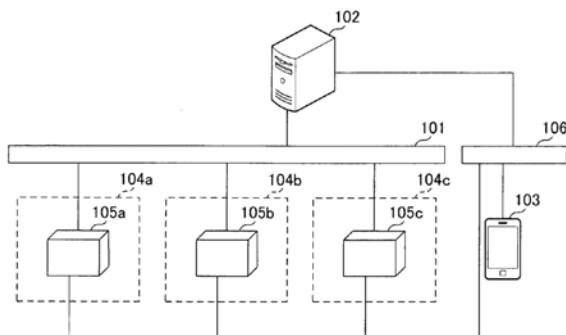
质

(57) 摘要

本发明涉及系统、语音操作设备、控制方法以及存储介质。一种系统，包括具有认证器、防篡改的TPM的移动终端以及语音助理。语音助理根据用户的语音输入向服务器发起与输入对应的处理请求，从服务器接收生物特征认证请求，经由无线通信根据生物特征认证请求向用户的移动终端发起对于生物特征认证处理的请求，并将来自移动终端的认证结果发送到服务器。移动终端根据来自语音助理的对于生物特征认证处理的请求而使用存储于认证器和TPM中的生物特征信息来执行生物特征认证处理，并将认证结果发送到语音助理。

B

CN 109660505



1. 一种包括信息处理终端和语音操作设备的系统，信息处理终端具有用于生物特征认证的认证模块和防篡改的存储单元，该存储单元存储有在使用所述认证模块执行认证处理时所必需的用户的生物特征信息，语音操作设备接收语音输入并且执行与该语音输入对应的处理，

其中，语音操作设备被配置为：

向外部系统发起与用户的语音输入对应的处理请求；

从外部系统接收认证请求，其中从外部系统接收的认证请求包含用于指定信息处理终端的认证模块的标识信息；

基于接收到的认证请求中包含的标识信息，经由无线通信向用户的信息处理终端发送对于认证处理的请求；以及

作为对于所述认证请求的响应，将从信息处理终端接收的认证结果发送到外部系统，并且

其中，信息处理终端被配置为：

根据来自语音操作设备的对于认证处理的请求，使用认证模块和存储于存储单元中的生物特征信息执行生物特征认证处理；以及

将生物特征认证处理的认证结果发送到语音操作设备。

2. 如权利要求1所述的系统，其中，生物特征认证处理的认证结果包括通过使用与生物特征信息相关联地存储于存储单元中的秘密密钥创建的签名以及由注册了与所述秘密密钥配对的公共密钥的外部系统发布的验证数据。

3. 如权利要求1所述的系统，其中，信息处理终端显示用于使用生物特征信息传感器读取生物特征信息的屏幕，以在外部系统中注册包括与生物特征信息相关联地生成的公共密钥的用户注册信息。

4. 如权利要求3所述的系统，

其中，信息处理终端向外部系统发起对于注册信息的注册请求，并且

其中，外部系统根据来自信息处理终端的注册请求相互关联地管理信息处理终端的认证模块和由信息处理终端的用户使用的语音操作设备。

5. 如权利要求4所述的系统，

其中，从与所述外部系统不同的外部系统接收到的另一认证请求不包括用于指定已向语音操作设备执行了语音输入的用户的信息处理终端的认证模块的标识信息，并且

其中，当针对信息处理终端请求认证处理时，语音操作设备从注册了注册信息的所述外部系统获取与语音操作设备相关联的信息处理终端的认证模块的标识信息。

6. 如权利要求3所述的系统，

其中，信息处理终端向外部系统发起对于注册信息的注册取消的取消请求，并且

其中，外部系统根据来自信息处理终端的取消请求删除对应用户的注册信息。

7. 如权利要求1所述的系统，其中，当根据来自语音操作设备的对于认证处理的请求执行生物特征认证处理时，信息处理终端显示用于使用生物特征信息传感器读取生物特征信息的屏幕。

8. 如权利要求1所述的系统，其中，语音操作设备被配置为根据认证结果的成功验证而在语音操作设备中执行从外部系统提供的专用于通过认证的用户的服务。

9.一种包括信息处理终端和语音操作设备的系统中的控制方法,信息处理终端具有用于生物特征认证的认证模块和防篡改的存储单元,该存储单元存储有在使用所述认证模块执行认证处理时所必需的用户的生物特征信息,语音操作设备接收语音输入并且执行与该语音输入对应的处理,该方法包括:

由语音操作设备向外部系统发起与用户的语音输入对应的处理请求;

由语音操作设备从外部系统接收认证请求,其中从外部系统接收的认证请求包含用于指定信息处理终端的认证模块的标识信息;

由语音操作设备基于接收到的认证请求中包含的标识信息经由无线通信向用户的信息处理终端发送对于认证处理的请求;

由信息处理终端根据来自语音操作设备的对于认证处理的请求使用认证模块和存储于存储单元中的生物特征信息来执行生物特征认证处理;

由信息处理终端将生物特征认证处理的认证结果发送到语音操作设备;以及

作为对于所述认证请求的响应,由语音操作设备将从信息处理终端接收的认证结果发送到外部系统。

10.一种语音操作设备,该语音操作设备接收语音输入并且执行与该语音输入对应的处理,该语音操作设备被配置为:

根据用户的语音输入向外部系统发起与该语音输入对应的处理请求;

从外部系统接收认证请求,其中从外部系统接收的认证请求包含用于指定用户的信息处理终端的认证模块的标识信息;

基于接收到的认证请求中包含的标识信息经由无线通信向用户的信息处理终端发送认证处理请求,该信息处理终端具有用于生物特征认证的认证模块和防篡改的存储单元,该存储单元存储有在使用认证模块执行认证处理时所必需的用户的生物特征信息;以及

作为对于接收到的认证请求的响应,向外部系统发送通过根据认证处理请求使用认证模块和存储于存储单元中的生物特征信息执行生物特征认证处理而从信息处理终端获得的认证结果。

11.一种用于语音操作设备的控制方法,该语音操作设备接收语音输入并且执行与该语音输入对应的处理,该方法包括:

根据用户的语音输入向外部系统发起与该语音输入对应的处理请求;

从外部系统接收认证请求,其中从外部系统接收的认证请求包含用于指定用户的信息处理终端的认证模块的标识信息;

基于接收到的认证请求中包含的标识信息经由无线通信向用户的信息处理终端发送认证处理请求,该信息处理终端具有用于生物特征认证的认证模块和防篡改的存储单元,该存储单元存储有在使用认证模块执行认证处理时所必需的用户的生物特征信息;以及

作为对于接收到的认证请求的响应,向外部系统发送通过根据认证处理请求使用认证模块和存储于存储单元中的生物特征信息执行生物特征认证处理而从信息处理终端获得的认证结果。

12.一种非瞬态存储介质,在该非瞬态存储介质上存储有使计算机执行用于语音操作设备的方法的计算机程序,该语音操作设备接收语音输入并且执行与该语音输入对应的处理,该方法包括:

根据用户的语音输入向外部系统发起与该语音输入对应的处理请求；

从外部系统接收认证请求，其中从外部系统接收的认证请求包含用于指定用户的信息处理终端的认证模块的标识信息；

基于接收到的认证请求中包含的标识信息经由无线通信向用户的信息处理终端发送认证处理请求，该信息处理终端具有用于生物特征认证的认证模块和防篡改的存储单元，该存储单元存储有在使用认证模块执行认证处理时所必需的用户的生物特征信息；以及

作为对于接收到的认证请求的响应，向外部系统发送通过根据认证处理请求使用认证模块和存储于存储单元中的生物特征信息执行生物特征认证处理而从信息处理终端获得的认证结果。

系统、语音操作设备、控制方法以及存储介质

技术领域

[0001] 本发明涉及提供安全认证方法并改善用户便利性的系统。

背景技术

[0002] 近年来,作为用于包括生物特征认证(biometric authentication)在内的认证的新系统,线上快速身份验证(Fast Identity Online,FIDO)已经受到关注。不同于在相关技术的ID/密码认证中使用的密码,当用于生物特征认证的生物特征信息(诸如指纹和静脉)被泄露到外部一次时,不可能重写生物特征信息,因此信息泄漏是灾难性的。

[0003] 另一方面,FIDO使得要预先在用户手上的设备和提供web服务的服务器之间执行注册处理。在注册处理中,与用户的生物特征信息相关联的秘密密钥被保存在设备中,并且诸如与生物特征信息相关联的认证标识信息和与秘密密钥配对的公开密钥之类的信息被注册在服务器中。此外,对用户手上的设备执行认证,而不是经由互联网对服务器执行认证,并且用秘密密钥签名的认证结果在网络上运行。即,由于生物特征信息不在网络上流传,因此可以说信息泄漏的风险低。

[0004] 同时,近年来已经广泛使用具有扬声器功能的语音辅助设备(语音操作设备)。这种语音辅助设备将在下面被称为语音助理。语音助理是具有使用语音识别功能翻译用户的话语并执行来自用户的各种指令的功能的信息装置。由于这种语音助理可以通过语音来命令,因此有利之处在于可以节省常规的个人计算机和智能电话所必需的按键操作和触摸输入的工作量。

[0005] 作为语音助理的使用方法的示例,语音助理被安装在房屋的起居室等当中,并且用户可以通过用他或她的声音给出指令来播放期望的音乐或者可以在互联网上运行的电话营销服务中定购产品。此外,这种语音助理不仅在家庭中而且在包括诸如酒店之类的住宿设施的公共设施中也被积极地引入。

[0006] 一般而言,诸如酒店之类的住宿设施提供综合服务,诸如为其客人搜索事件和买票等,以及客房服务。预计语音助理将成为在提供服务时客人轻松接收服务的手段,而无需繁琐的工作。

[0007] JP 2003-132435A公开了一种酒店客人服务器系统,该系统使得能够在酒店中使用房间钥匙和个人标识号码来执行服务的提供和支付。JP 2003-132435A公开了酒店的房间钥匙具有RFID无线电标签,该RFID无线电标签预先存储隶属于它的房间号码、个人标识号码、客人号码、要支付的金额等的信息,并且在退房时立即进行支付。

[0008] 在使用ID和密码的常规认证方法中,用户必需输入他或她的ID和密码以便接收各种服务,并且努力输入并记住信息,这不能说是方便的。此外,仍然存在包括ID和密码在内的信息泄露的风险。

[0009] 但是,当用户经由可以被许多未指定的人使用的公共场所(诸如酒店)中的语音助理使用服务时,必需在语音助理中保存与生物特征信息相关联的各种信息,以使用诸如上述FIDO之类的认证方法。与生物特征信息相关联的这各种信息在下面将被称为生物特征认

证信息。将生物特征认证信息保存在用户家中使用的语音助理中不是问题，但是，预期在部署于许多未指定的人使用的地方的设备中注册生物特征认证信息会由于生物特征认证信息泄漏的可能性而造成用户的抵制。

发明内容

[0010] 本发明提供了可以提高用户便利性并提供安全认证方法的系统。
[0011] 根据本发明实施例的系统是一种包括信息处理终端和语音操作设备的系统，信息处理终端具有用于生物特征认证的认证模块和防篡改的存储单元，该存储单元存储有在使用认证模块执行认证处理时所必需的用户的生物特征信息，语音操作设备接收语音输入并执行与输入对应的处理。语音操作设备具有：第一请求单元，根据输入向外部系统发起与用户的语音输入对应的处理请求；接收单元，从外部系统接收认证请求；第二请求单元，经由无线通信根据认证请求向用户的信息处理终端发起对于认证处理的请求；以及发送单元，将来自信息处理终端的认证结果发送到外部系统。信息处理终端具有：执行单元，根据来自语音操作设备的对于认证处理的请求而使用认证模块和存储于存储单元中的生物特征信息执行生物特征认证处理；以及发送单元，向语音操作设备发送生物特征认证处理的认证结果。
[0012] (参考附图) 阅读示例性实施例的以下描述，本发明的其它特征将变得清楚。

附图说明

[0013] 图1是例示了根据本发明的实施例的系统的整体配置的图。
[0014] 图2是例示了服务器的硬件配置示例的图。
[0015] 图3是例示了移动终端的硬件配置示例的图。
[0016] 图4是例示了语音助理的硬件配置示例的图。
[0017] 图5A至图5C是例示了每个设备的功能配置的示例的图。
[0018] 图6是例示了开始使用服务的处理的序列图。
[0019] 图7是例示了为使用服务而执行的处理的序列图。
[0020] 图8是例示了结束使用服务的处理的序列图。
[0021] 图9是例示了登记入住屏幕的示例的图。
[0022] 图10是例示了生物特征信息注册屏幕的示例的图。
[0023] 图11是例示了生物特征信息输入请求屏幕的示例的图。
[0024] 图12是例示了退房屏幕的示例的图。
[0025] 图13是例示了为使用音乐分发服务而执行的处理的序列图。
[0026] 图14是例示了为使用音乐分发服务而执行的处理的修改例的序列图。
[0027] 图15是例示了为使用音乐分发服务而执行的处理的修改例的序列图。

具体实施方式

[0028] 将参考附图等描述用于实现本发明的示例性实施例。
[0029] 要注意的是，本发明涉及一种机制，在该机制中，经由网络从外部系统提供的服务对用户手上的设备(信息处理终端)执行生物特征认证以便认证用户，并且作为结果，该服

务可以认证用户。这可以通过预先在服务中注册与用户手上的设备中包含的生物特征认证相关联的信息(例如,认证标识信息、公共密钥等)来实现。

[0030] 虽然FIDO被例示为这种机制的示例,但是应当提前注意的是,本发明不限于FIDO。要注意的是,虽然在本实施例中将用户携带的移动终端103描述为用户手上的执行生物特征认证的设备的示例,但是本发明不限于此。作为另一个示例,将在第二实施例中描述语音助理105和服务器102执行生物特征认证的情况。

[0031] [第一实施例]

[0032] 图1是例示了根据本发明的实施例的系统的整体配置的示例的图。

[0033] 图1中所示的系统包括服务器102、移动终端103和语音助理(语音操作设备)105a至105c。

[0034] 要注意的是,为了便于描述,将关于语音助理105描述语音助理105a至105c共有的事项。虽然图1例示了有三个语音助理105连接到网络101并且安装了多个语音助理105,但是本发明不限于此,并且可以提供一个或多个语音助理。此外,服务器102是提供服务的外部系统并且可以由多个设备构成,并且设备中的一些或全部可以使用虚拟机和存储装置等的资源来构造。

[0035] 服务器102和语音助理105经由网络101相互连接。网络101是例如包括互联网的LAN、WAN、电话线路、专用数字线路、ATM、帧中继线路、有线电视线路、数据广播无线电线路等之一。此外,网络101是通过组合上述线路而实现的所谓的通信网络。网络101可以是有可能在其上发送和接收数据的任何网络。

[0036] 服务器102和语音助理105经由移动终端103和网络106相互连接。除了上面提到的诸如LAN之类的网络线路之外,网络106还包括例如近距离无线通信,诸如近场通信(NFC)或蓝牙(注册商标)。

[0037] 在本实施例中假设语音助理被安装在诸如酒店之类的住宿设施中。语音助理105a至105c各自被安装在作为酒店房间的房间104a至104c中。即,语音助手105a被安装在房间104a中。要注意的是,为了便于描述,将关于房间104描述房间104a至104c共有的事项。

[0038] 图2是例示了服务器102的硬件配置示例的图。

[0039] CPU 201执行存储于ROM 203中的程序以及从外部存储器210加载在RAM 202上的诸如操作系统(OS)和应用之类的程序。即,通过执行存储于可读存储介质中的程序,CPU 201充当执行下面将描述的每个流程图的处理的每个处理单元。

[0040] RAM 202是CPU 201的主存储器,并且充当工作区等。键盘控制器204控制来自键盘208或定点设备(未示出)的操作输入。定点设备是例如鼠标、触摸垫、触摸面板或轨迹球等。显示器控制器205控制显示器209的显示。

[0041] 盘控制器206控制对于存储各种数据的外部存储器210(诸如硬盘(HD)或软盘(FD))的数据访问。网络I/F 207连接到网络并执行控制与连接到网络的另一个装置的通信的处理。接近通信I/F 211是支持诸如NFC或蓝牙(注册商标)之类的接近通信方法的网络I/F,并且与移动终端103等通信以交换数据。

[0042] 图3是例示了移动终端103的硬件配置示例的图。

[0043] CPU 222执行存储于ROM 224和存储设备225中的程序,并经由内部总线221全面地控制下面将描述的每个组成元件。程序还包括实现下面将描述的每个流程图的程序。RAM

223充当CPU 222的存储器或工作区。

[0044] 存储设备225是诸如固态驱动器 (SSD) 或SD存储卡之类的存储设备，并且充当外部存储设备。篡改模块 (TPM) 226是出于处理或存储机密信息的目的而具有防止从外部读取所存储的数据的防篡改性质的存储单元。网络I/F 227单向或双向地与外部网络装置交换数据。

[0045] 生物特征信息传感器228是读取用户的生物特征信息的传感器，并且将生物特征信息(例如，用户的指纹、虹膜、静脉、声纹、面部图像等)转换成可读信号。要注意的是，生物特征信息不限于此。触摸面板229具有显示和输入两种功能，显示应用屏幕、键盘等，并且当用户用他或她的手或专用笔在屏幕上施加压力时把被触摸的屏幕位置的信息作为信号信息输出到外部。

[0046] 当应用使用输出信号信息时，用户可以通过触摸面板229操作应用。接近通信I/F 230是支持诸如NFC或蓝牙(注册商标)之类的接近通信方法的网络I/F，并且与服务器102等通信以交换数据。

[0047] 图4是例示了语音助理105的硬件配置示例的图。

[0048] CPU 241执行存储于ROM 243中的程序以及从外部存储器248加载在RAM 242上的诸如操作系统 (OS) 和应用之类的程序。即，通过执行存储于可读存储介质中的程序，CPU 241充当执行下面将描述的每个流程图的处理的每个处理单元。

[0049] RAM 242是CPU 241的主存储器，并且充当工作区等。盘控制器244控制对于存储各种数据的外部存储器248(诸如硬盘 (HD) 或软盘 (FD))的数据访问。网络I/F 245连接到网络并执行控制与连接到网络的另一个装置的通信的处理。扬声器控制器246控制扬声器249。麦克风控制器247控制麦克风250。

[0050] 要注意的是，语音助理105不限于具有图4中所示的硬件配置。语音助理是接收语音输入并执行与输入对应的处理的语音操作设备，并且还可以执行例如下面将描述的第二实施例中的生物特征认证处理。在这种情况下，语音助理105也可以是用于读取生物特征信息的硬件(例如，相机等)。

[0051] 图5A是例示了服务器102的功能配置的示例的图。

[0052] 在服务器102中，酒店服务310作为要提供给用户的服务的示例而操作。当服务器102的CPU 201将存储于其ROM 203中的程序读到RAM 202中并执行该程序时，实现酒店服务310。

[0053] 酒店服务310具有注册处理单元311、数据存储单元312、认证器信息处理单元313、认证器信息存储单元314、生物特征认证控制单元315、服务处理单元316和通信单元317。注册处理单元311是在数据存储单元312中存储诸如用户信息和用户的住宿历史之类的数据的软件模块。

[0054] 认证器信息处理单元313是使用由通信单元317接收的凭证来在认证器信息存储单元314中存储关于下面将描述的认证器330的信息的软件模块。此外，认证器信息处理单元313验证由通信单元317接收的断言信息(断言(assertion))，断言信息(断言)将在下面描述。

[0055] 通信单元317是经由网络I/F 207与诸如语音助理105或移动终端103之类的外部装置通信的软件模块。认证器信息存储单元314是使用表G在外部存储器210或外部存储系

统(未示出)中存储下面将描述的关于认证器330的信息(认证器信息)的软件模块。

[0056] 生物特征认证控制单元315是向认证器330发起生物特征认证请求并接收生物特征认证的结果的软件模块。在本实施例中,生物特征认证控制单元315经由语音助理105向移动终端103的认证器330发起生物特征认证请求。要注意的是,虽然在本实施例中生物特征认证控制单元315被包括在酒店服务310中,但是本发明不限于此。

[0057] 生物特征认证控制单元315可以例如独立于酒店服务310地被配置,并且酒店服务310可以调出独立的生物特征认证控制单元315。通过如上所述将生物特征认证控制单元315配置为独立于酒店服务310,生物特征认证控制单元315可以被配置为不仅由酒店服务310而且还由另一个服务调出。

[0058] 服务处理单元316是根据由通信单元317接收的服务请求来搜索服务信息或进行服务预约的软件模块。服务处理单元316使用表D在数据存储单元312中存储下面将描述的关于服务提供的信息(服务提供信息)。

[0059] 图5B是例示了移动终端103的功能配置的示例的图。

[0060] 在移动终端103中,应用320和认证器330被操作。当移动终端103的CPU 222将存储于其ROM 224中的程序读到RAM 223中并执行该程序时,实现应用320和认证器330。

[0061] 应用320与服务器102合作向用户提供使用根据本实施例的生物特征信息的认证功能和服务器102的服务。应用320是本机应用或在移动设备中安装的web浏览器。应用320具有显示单元321、通信单元322和认证器注册控制单元323。

[0062] 显示单元321是提供在移动终端103中安装的应用的UI或经由触摸面板229接收用户的操作的软件模块。通信单元322是经由网络I/F 227或接近通信I/F 230与诸如服务器102之类的外部装置通信的软件模块。认证器注册控制单元323是向认证器330发起下面将描述的对于创建凭证的请求的软件模块。

[0063] 要注意的是,虽然在本实施例中认证器注册控制单元323被包括在应用320中,但是本发明不限于此。例如,认证器注册控制单元323可以独立于应用320被配置,并且应用320可以调出独立的认证器注册控制单元323。此外,认证器注册控制单元313可以默认被安装在OS中。

[0064] 通过如上所述将认证器注册控制单元323配置为独立于应用320,另一个应用以及应用320可以调出认证器注册控制单元323。

[0065] 认证器330是使用从生物特征信息传感器228读取的生物特征信息进行生物特征认证的认证模块。认证器330具有认证器注册处理单元331、生物特征认证处理单元332、认证信息存储单元333、以及生物特征信息请求单元334。

[0066] 认证器注册处理单元331从应用320的认证器注册控制单元323等接收用于创建凭证的请求。此外,认证器注册处理单元331是创建配对密钥(秘密密钥和公共密钥)和凭证的软件模块。生物特征认证处理单元332是从酒店服务310的生物特征认证控制单元315等接收生物特征认证请求并使用由生物特征信息传感器228读取的生物特征信息执行生物特征认证的软件模块。

[0067] 认证信息存储单元333是存储用于TPM 226的认证信息等的软件模型。认证信息是例如下面将描述的表A中所示的信息。生物特征信息请求单元334是经由触摸面板229向用户提供用于接收生物特征信息的输入的UI的软件模块。

[0068] 图5C是例示了语音助理105的功能配置的示例的图。

[0069] 在语音助理105中,语音服务340被操作。当语音助理105的CPU 241将存储于其ROM 243中的程序读到RAM 242中并执行该程序时,实现语音服务340。语音服务340与服务器102合作向用户提供服务器102的服务。

[0070] 语音服务340具有语音接收单元341、语音分析单元342、语音发出单元343、生物特征认证控制单元344和通信单元345。语音接收单元341是接收由用户经由语音助理105的麦克风250发出的语音的软件模块。语音分析单元342是分析由语音接收单元341接收的语音的软件模块。

[0071] 语音发出单元343是经由语音助理105的扬声器249通过语音向用户提供指导的软件模块。生物特征认证控制单元344是向认证器330发起生物特征认证请求并接收生物特征认证的结果的软件模块。通信单元345是经由网络I/F 245与诸如服务器102或移动终端103之类的外部装置通信的软件模块。

[0072] 接下来,将描述由移动终端103和服务器102存储的各种数据。

[0073] 表A是由移动终端103的认证器330的认证信息存储单元333存储在TPM 226中的数据的示例。

[0074] [表1]

[0075] 表A

认证信息ID	服务ID	秘密密钥	生物特征信息ID
407c-8841-79d	hotel-service.com	1faea2da-a269-4fa7-812a-509470d9a0cb	d493a744
4c04-428b-a7a2	service-a.com	d7ae30c8-3775-4706-8597-aaf681bc30f5	dcc97daa
92b2-498d-bea6	service-b.com	36ae5eed-732b-4b05-aa7b-4dddb4be3267	51caacaa
...

[0077] 在表A中所示的认证信息管理表中,一个记录表示认证信息的一个条目。当移动终端103在服务器102的酒店服务310中注册认证器330时表A的记录被创建并然后被添加到表A。在认证信息ID列中,存储了用于唯一地标识每条认证信息的ID。在服务ID列中,存储了用于唯一地标识使用利用生物特征信息执行的认证功能的服务的ID。

[0078] 在本实施例中,服务的域名,具体而言,顶级域和第二级域的信息,被用作服务ID。例如,当酒店服务310的URL是http://www.hotel-service.com时,假设酒店服务310的服务ID是hotel-service.com。在秘密密钥列中,存储了所创建的配对密钥中的秘密密钥。与秘密密钥对应(配对)的公共密钥在服务ID列中所示的服务中注册。

[0079] 在生物特征信息ID列中,存储了与生物特征信息的特征量对应的ID。稍后将描述存储与认证信息管理表的每列对应的信息的过程以及在服务中存储公共密钥的过程。要注意的是,如表A中所示的认证信息管理表是示例,表A不限于此,并且可以存储其它信息。例如,可以在其中存储在服务中用于唯一地标识用户的ID,这在常规认证中用于在服务中验证用户ID和密码的对应关系。

[0080] 表B至表G是由服务器102的酒店服务310的数据存储单元312和认证器信息存储单元314存储在外部存储器210等中的数据的示例。

[0081] [表2]

[0082] 表B

[0083]	用户ID	密码	姓名	地址	年龄	职业
	user001	***	aaa aaa	abc	20	学生
	user002	***	bbb bbb	def	30	雇员

[0084] 表B中所示的用户信息管理表是由酒店服务310的数据存储单元312管理的数据。在用户信息管理表中,一个记录表示一条用户信息。在用户ID列中,存储了用于唯一地标识酒店服务310的用户的ID。在密码列中,存储了用于认证用户的密码。当用户在酒店服务310中执行用户注册时,密码被指定。此外,用户信息管理表可以存储在用户登记入住酒店时所需的关于用户的属性信息(诸如用户的姓名、地址、年龄、职业等)。

[0085] [表3]

[0086] 表C

[0087]	用户ID	登记入住日期	退房日期	房间号	语音助理ID
	user001	2017/7/12	2017/7/13	Room104a	105a
	user001	2017/2/10	2017/7/11	Room104b	105b
	user002	2017/7/12	2017/7/13	Room104c	105c

[0088] 表C中所示的住宿历史管理表是由酒店服务310的数据存储单元312管理的数据。在住宿历史管理表中,一个记录表示用户的一次住宿的信息。在用户ID列中,存储了在用户信息管理表(表B)中管理的用户信息的用户ID列的值。此外,住宿历史管理表存储登记入住日期、退房日期、用户所住房间的房间号以及用于指定安装在用户所住房间中的语音助理的ID作为一次住宿的信息。

[0089] [表4]

[0090] 表D

[0091]	用户ID	服务ID	服务细节	金额	日期	支付信息
	user001	s0001	客房服务A	1000日元	2017/2/10	是
	user001	s0001	客房服务A	1000日元	2017/7/12	否
	user002	s0002	客房服务B	2000日元	2017/7/13	否

[0092] 表D中所示的服务信息管理表是由酒店服务310的数据存储单元312管理的数据。在服务信息管理表中,一个记录表示向一个用户提供一项服务的状态。在用户ID列中,存储了与上述表B和C的用户ID列中相同的值。此外,服务信息管理表存储以下项作为用于指定提供给用户的服务的信息。即,存储了诸如服务ID和指示所提供服务的细节的服务细节之类的信息、提供服务的日期以及在需要支付的服务的情况下金额、支付信息等。

[0093] [表5]

[0094] 表E

[0095]	语音助理ID	移动终端(认证器)
	105a	a12345
	105b	a23456

105c	a34567
...	...

[0096] 表E中所示的关联信息管理表是由酒店服务310的数据存储单元312管理的数据。在关联信息管理表中,在用户所住房间中安装的语音助理105与作为由用户使用并在酒店服务310中注册的移动终端103的认证器330相关联。

[0097] 作为示例,将描述在一个房间中安装一个语音助理105的情况。语音助理105a被安装在房间104a中。当住在房间104a中的用户在下面将描述的认证器注册处理中注册认证器330时,语音助理105a的ID和所注册的认证器的ID被关联并被存储。

[0098] 要注意的是,还存在一个房间中两个或更多个用户使用语音助理105的情况。在这种情况下,针对作为用户拥有的移动终端103的每个认证器330执行认证器的注册。然后,在关联信息管理表中,两个或更多个认证器330与一个语音助理105相关联并注册在一个语音助理105中。

[0099] [表6]

[0100] 表F

证明质询	用户ID	到期日期
65C9B063-9C33	user001	2017-07-13T12:00:34Z
7317EFBA-4E63	user101	2017-07-13T12:03:12Z
...

[0102] 表F中所示的证明质询(attestation challenge)管理表是由酒店服务310的数据存储单元312管理的数据。在证明质询管理表中,一个记录表示证明质询的一条信息。证明质询是用作执行质询响应认证(challenge response authentication)的验证数据的参数并且是针对每个用户发布的。

[0103] 下面将描述证明质询发布处理。在证明质询列中,存储了证明质询的值。在用户ID列中,存储了为其发布证明质询的用户的用户ID。在到期日期列中,存储了证明质询的到期日期。

[0104] [表7]

[0105] 表G

认证信息ID	公共密钥	用户ID
407c-8841-79d	AC43C5FB-BFA2-48D1-A71B-FB04ACDA347A	user001
4c04-428b-a7a2	8143CA9F-35C9-4333-*948F-BFCE66A74310	user002
...

[0107] 表G中所示的认证器信息管理表是由酒店服务310的认证器信息存储单元314管理的数据。在认证器信息管理表中,一个记录表示一条认证器信息。当认证器330在服务器102中注册时,记录被添加到认证器信息管理表。

[0108] 在认证信息ID列中,存储了认证信息管理表(表A)中由所注册的认证器330管理的认证信息的认证信息ID列的值。在公共密钥列中,存储了与由认证器330创建并在认证信息管理表(表A)中管理的秘密密钥对应(配对)的公共密钥。

[0109] 即,关于认证信息管理表(表A)和认证器信息管理表(表G)中与认证信息ID的相同值相关联的秘密密钥和公共密钥,用存储在表A中的秘密密钥加密的数据可以用存储在表G

中的公共密钥解密。在用户ID列中，存储了由酒店服务310用来唯一地标识用户的ID。

[0110] 接下来，将参考图6描述当酒店的新客人（用户）登记入住酒店时开始使用酒店服务310的处理。

[0111] 在开始使用酒店服务310的处理中，执行在服务器102中注册由用户携带的移动终端103的认证器330的处理。

[0112] 虽然下面将描述注册移动终端103的认证器330的情况，但是相同的描述适用于认证器被包括在语音助理105中的情况。要注意的是，在服务器102中注册认证器330的信息被简称为认证器的注册。

[0113] 要注意的是，为了使用酒店服务310，假设用户预先在移动终端103中安装与酒店服务310相关联的应用320。可替代地，可以指定由酒店服务310提供的web服务的URL，然后可以在移动终端103的web浏览器中显示用于使用酒店服务310的服务屏幕。

[0114] 将描述用户使用移动终端103的应用320来执行开始使用酒店服务310的处理的情况。首先，应用320通过用户操作显示登记入住屏幕。具体而言，通过操作应用320的菜单显示（未示出）来显示登记入住屏幕。

[0115] 图9是由应用320的显示单元321显示的登记入住屏幕的示例。

[0116] 用户输入登记入住酒店所必需的用户的属性信息（诸如他或她的姓名、地址、年龄、职业等）以及要在酒店服务310中使用的密码。

[0117] 现在描述将返回到图6。在步骤S401中，在接收到用户信息的输入时，应用320经由通信单元322向酒店服务310发送用户的使用注册请求。要注意的是，该请求包括由用户输入的属性信息和密码。在步骤S401中，酒店服务310的通信单元317接收从应用320发送的请求。

[0118] 在步骤S402中，酒店服务310的注册处理单元311发布用户ID，并将包括用户ID的用户信息存储在数据存储单元312的用户信息管理表（表B）中。用户信息包括在步骤S401中接收到的属性信息和密码。在步骤S403中，酒店服务310的认证器信息处理单元313经由通信单元317向应用320发送凭证创建请求。

[0119] 下面将描述凭证创建请求中包括的参数。

[0120] 凭证创建请求中包括的参数由账户信息、加密参数、证明质询和认证扩展区域构成。账户信息存储在步骤S402中为酒店服务310注册的用户ID和与该用户ID相关联的属性信息。

[0121] 加密参数存储关于所注册的认证信息的属性信息（诸如由酒店服务310支持的加密算法等）。证明质询存储将被用于执行质询响应认证的验证数据。当在步骤S402中创建凭证创建请求中包括的参数时，验证数据（即，证明质询）被创建。

[0122] 然后，所创建的证明质询与用户ID、到期日期等相关联地存储在证明质询管理表（表F）中。认证扩展区域存储可由酒店服务310指定的扩展参数。例如，认证扩展区域存储用于控制认证器330的操作的参数等。

[0123] 现在描述将返回到图6。应用320的通信单元322接收在步骤S403中发送的凭证创建请求。在接收到凭证创建请求时，应用320的显示单元321显示用于向用户发起输入生物特征认证中使用的生物特征信息的请求的生物特征信息注册屏幕。

[0124] 图10是生物特征信息注册屏幕的示例。

[0125] 生物特征信息注册屏幕促使用户输入生物特征信息以在酒店服务310中注册认证器330。按钮721用于读取诸如指纹之类的生物特征信息并包括生物特征信息传感器228。要注意的是，静脉、虹膜、声纹、面部图像等的信息可以被用作生物特征信息，并且不限于此。

[0126] 在这里，移动终端103被配置为使得任何一条生物特征信息或多条任意生物特征信息的组合被输入作为要在生物特征认证中使用的生物特征信息。此外，虽然在本实施例中生物特征信息的输入是在登记入住时如上所述那样请求的，但是本发明不限于此。例如，可以稍后在实际需要生物特征认证时请求生物特征信息的输入，而无需在登记入住时请求输入生物特征信息。

[0127] 当生物特征信息传感器228在生物特征信息注册屏幕上读取生物特征信息时，应用320的认证器注册控制单元323将生物特征信息传送到认证器330并请求创建凭证。除了读取的生物特征信息之外，此时的请求还包括在步骤S403中从酒店服务310接收的凭证创建请求中包括的参数以及服务ID。

[0128] 服务ID是用于唯一地标识在认证信息管理表(表A)中描述的注册了认证器330的服务的ID。在这种情况下，包括酒店服务310的服务ID。此外，可以包括应用ID等，应用ID是用于唯一地指定用于在酒店服务310中注册认证器330的应用320的ID。

[0129] 现在将返回到图6。在步骤S404中，认证器330的生物特征认证处理单元332创建用于唯一地标识从应用320接收到的生物特征信息的特征量的生物特征信息ID以及生物特征信息本身。生物特征信息的特征量是通过将个人独有的信息(诸如指纹的图案、虹膜的图案、静脉的形状或声纹)转换成不损害唯一性的值而获得的值。在生物特征认证中，使用个人特有的特征量来指定个人。

[0130] 在步骤S405中，认证器注册处理单元331创建一对秘密密钥和公共密钥以及用于唯一地标识认证信息的认证信息ID。然后，认证器注册处理单元331经由认证信息存储单元333将以下信息存储在TPM 226中所存储的认证信息管理表(表A)中。即，存储在步骤S404中创建的生物特征信息ID、在步骤S405中创建的秘密密钥和认证信息ID以及注册了认证器的服务ID。

[0131] 在本实施例中，存储由认证器330从应用320接收的凭证创建请求中包括的酒店服务310的服务ID。在步骤S406中，认证器注册处理单元331创建凭证。

[0132] 下面将描述凭证。

[0133] 凭证由认证信息ID、算法、公共密钥和证明构成。认证信息ID是在步骤S405中创建并存储在认证信息管理表(表A)中的认证信息ID。此外，公共密钥是在步骤S405中创建的密钥对中的公共密钥。

[0134] 该算法存储用于在步骤S405中创建密钥对的算法。此外，证明是通过使用在步骤S405中生成的秘密密钥加密在步骤S403中接收的凭证创建请求中所包括的参数的证明质询而获得的数据。认证器注册处理单元331将在步骤S406中创建的凭证和用于指定应用320的认证器330的认证器ID传送到应用320。

[0135] 在步骤S407中，应用320的通信单元322将从认证器330接收到的凭证和认证器ID发送到酒店服务310。在步骤S408中，酒店服务310的认证器信息处理单元313使用接收到的凭证来执行认证器330的注册处理。

[0136] 下面将描述由认证器信息处理单元313执行的凭证注册处理。

[0137] 首先,认证器信息处理单元313使用在同一凭证中包括的公共密钥来解密该凭证中包括的证明,以验证注册请求是否非法。

[0138] 此外,认证器信息处理单元313指定证明质询管理表(表F)的具有与通过用公共密钥加密证明所获得的值相同的值的证明质询列的记录。然后,认证器信息处理单元313将所指定的记录的用户ID设置为与凭证相关联的用户ID。

[0139] 然后,认证器信息处理单元313将凭证中包括的认证信息ID和公共密钥和与该凭证相关联的用户ID存储(注册)在认证器信息管理表(表G)中。

[0140] 现在描述将返回到图6。在步骤S409中,注册处理单元311将在用户所住的房间中安装的语音助理105与在步骤S407中接收到的认证器ID的关联存储在关联信息管理表(表E)中。最后,酒店服务310的通信单元317向移动终端103的应用320报告认证器注册处理已正常完成。

[0141] 接下来,将使用图7描述由用户经由语音助理105执行使用酒店服务310的处理。

[0142] 用户通过话语(语音)向语音助理105发起使用酒店服务310的请求。例如,当用户想要客房服务时,可以通过说“告诉我客房服务的列表”来发起请求。

[0143] 要注意的是,客房服务是由酒店服务310提供的服务的示例,并且不限于此。通过使用酒店服务310,票或出租车的预订等也是可能的。此外,通过使用酒店服务310,用户还可以联系酒店关于用户所住的房间不需要清洁等事实。

[0144] 在步骤S501中,语音助理105的语音服务340的语音接收单元341通过用户的语音接收提供服务的请求。在步骤S502中,语音分析单元342分析所接收到的语音并确定请求的细节。在步骤S503中,通信单元345将在步骤S502中分析的处理请求发送到酒店服务310。

[0145] 酒店服务310的通信单元317接收来自语音助理105的请求。在步骤S504中,酒店服务310的服务处理单元316执行与接收到的请求对应的处理。具体而言,首先,服务处理单元316确定用户认证对于执行接收到的请求是否是必需的。当在酒店服务310中注册关于服务的信息时,预先设置是否必需用户认证。

[0146] 例如,伴随有支付的请求可被设置为需要用户认证。当确定用户认证对于执行请求是不必要的时,服务处理单元316执行与该请求对应的处理,而不需要用户认证。在这里,将描述请求是“告诉我客房服务的列表”的情况。即,可以将可用的客房服务的列表发送到用作发出请求的源的语音助理105。

[0147] 由于请求不是伴随有支付的请求,因此服务处理单元316确定用户认证不是必需的。然后,服务处理单元316搜索客房服务,作为与请求“告诉我客房服务的列表”对应的处理。要注意的是,下面将在步骤S510中描述当用户认证为必需时执行的处理。

[0148] 在步骤S505中,服务处理单元316经由通信单元317以客房服务列表向语音助理105回复。要注意的是,在这个时候,服务处理单元316可以从服务信息管理表(表D)搜索与作为发出请求的源的语音助理105相关联的用户的过去客房服务的订单历史,并且以列表连同推荐的客房服务的建议信息进行回复。

[0149] 语音服务340的通信单元345从酒店服务310接收客房服务列表。在步骤S506中,语音服务340的语音发出单元343向用户提供关于所接收到的客房服务列表的语音指导。用户通过话语(语音)向语音助理105定购客房服务的具体菜单。即,向酒店服务310发起请求。

[0150] 由于语音助理105接收请求并将用户的请求发送到酒店服务310的步骤S507至

S509的处理与步骤S501至S503的处理相同,因此省略其描述。在步骤S510中,酒店服务310的服务处理单元316根据接收到的请求执行处理。具体而言,服务处理单元316确定用户认证对于执行接收到的请求是否是必需的,如步骤S504中那样。

[0151] 在这里,由于请求的是客房服务的具体菜单的定购,并且它是伴随有支付的请求,因此服务处理单元316确定用户认证是必需的。因此,在步骤S511中,酒店服务310的认证器信息处理单元313经由通信单元31向语音助理105发起用户认证请求,即,生物特征认证请求。在这个时候,认证器信息处理单元313创建生物特征认证参数并且在请求中包括所生成的生物特征认证参数。

[0152] 下面将描述生物特征认证参数。

[0153] 生物特征认证参数是当酒店服务310执行应用320的认证时使用的数据。生物特征认证参数由断言质询和断言扩展区域构成。断言质询存储用于执行质询响应认证的验证数据。

[0154] 在断言扩展区域中,存储了可以由酒店服务310指定以被酒店服务310用于控制认证器330等的操作的扩展参数。断言扩展区域存储例如用于控制认证器330等的操作的参数。

[0155] 现在描述将返回到图7。在步骤S511中,当酒店服务310的认证器信息处理单元313经由通信单元317向语音助理105发起生物特征认证请求时,该请求还包括以下信息。即,认证器信息处理单元313在请求中包括关联信息管理表(表E)中的用于指定与作为请求源的语音助理105相关联的认证器330的认证器ID。

[0156] 此外,认证器信息处理单元313在请求中包括诸如订单量等之类的信息。要注意的是,在这个时候,认证器信息处理单元313可以在请求中包括要向用户推荐的建议信息。例如,认证器信息处理单元313经由服务处理单元316从住宿历史管理表(表C)中指定与用作请求源的语音助理105对应的房间(房间104)的用户信息。

[0157] 然后,认证器信息处理单元313基于用户信息从服务信息管理表(表D)获取用户的过去的服务历史,并且在请求中包括要向用户推荐的建议信息。此外,认证器信息处理单元313可以在请求中包括与用户无关的服务的促销信息等。

[0158] 在步骤S512中,语音服务340的生物特征认证控制单元344根据请求中包括的认证器ID来指定用作在步骤S511中接收到的生物特征认证请求的报告目的地的认证器330。在步骤S513中,生物特征认证控制单元344向移动终端103发起生物特征认证请求。要注意的是,生物特征认证请求包括自生生物特征认证参数(auth-biometric authentication parameter)。

[0159] 将描述从语音助理105发送到移动终端103的生物特征认证请求中包括的自生生物特征认证参数。

[0160] 自生生物特征认证参数包括由酒店服务310的认证器信息处理单元313创建并且在上述步骤S511中从酒店服务310发送到语音助理105的生物特征认证参数。此外,自生生物特征认证参数包括服务ID和web起源(web origin)。

[0161] 服务ID存储酒店服务310的顶级域和第二级域的信息。例如,当酒店服务310的URL是http://www.hotel-service.com时,服务ID是hotel-service.com。web起源是协议、主机名和端口的组合,并且在本实施例中酒店服务310的起源被存储。

[0162] 现在描述将返回到图7。当移动终端103在步骤S514中接收到生物特征认证请求时,执行生物特征认证处理。下面将描述由移动终端103执行的生物特征认证处理。

[0163] 当移动终端103接收到生物特征认证请求时,应用320的显示单元321显示生物特征信息输入请求屏幕。

[0164] 图11是由应用320的显示单元321显示的生物特征信息输入请求屏幕的示例。

[0165] 生物特征信息输入请求屏幕促使用户输入生物特征信息,以便在移动终端103中执行生物特征认证。要注意的是,虽然在本实施例中应用320的显示单元321显示生物特征信息输入请求屏幕,但是验证器330可以具有显示单元(未示出)并显示该屏幕。

[0166] 按钮811是用于读取生物特征信息的按钮,并且包括生物特征信息传感器228。要注意的是,还在生物特征信息输入请求屏幕上显示在步骤S511中从酒店服务310发送到语音助理105的生物特征认证请求中包括的各种信息。该信息包括例如用户订购的菜单的价格等信息、要向用户推荐的建议信息、其它服务的促销信息,等等。

[0167] 当在生物特征信息输入请求屏幕上生物特征信息传感器228读取生物特征信息时,应用320的认证器注册控制单元323将生物特征信息传送到认证器330并发起认证请求。要注意的是,认证器注册控制单元323在认证请求中包括在步骤S513中从语音助理105接收的认证生物特征认证参数。

[0168] 认证器330的生物特征认证处理单元332获取所接收到的生物特征信息的特征量。生物特征认证处理单元332基于所获取的特征量从由认证信息存储单元333管理的认证信息管理表(表A)中指定记录。具体而言,由于由特征量指示的生物特征信息ID被指定,因此在认证信息管理表(表A)中包括的与生物特征信息对应的认证信息ID和秘密密钥被指定。

[0169] 即,当认证器330在执行生物特征认证之后成功认证时,秘密密钥被取出。要注意的是,与特征量那样,可以验证在自生生物特征认证参数中包括的服务ID是否匹配表A的服务ID匹配。然后,生物特征认证处理单元332创建通过用指定的秘密密钥加密在自生生物特征认证参数中包括的断言质询而获得的签名。此外,生物特征认证处理单元332创建包括所指定的认证信息ID和所创建的签名的断言信息。

[0170] 在步骤S515中,生物特征认证处理单元332以所创建的断言信息向语音助理105回复。在步骤S516中,语音服务340的通信单元345以在步骤S515中接收的断言信息向酒店服务310回复。

[0171] 要注意的是,当步骤S514的生物特征认证处理的结果是认证失败或者用户未执行生物特征信息的输入长达某个时间段时,应用320的显示单元321在生物特征信息输入请求屏幕上呈现指示认证失败并且处理结束的显示。然后,在步骤S515和S516中均回复指示生物特征认证处理的结果是认证失败的信息。在接收到指示认证失败的信息时,酒店服务310结束图7的处理。

[0172] 在步骤S517中,酒店服务310的认证器信息处理单元313验证在步骤S516中接收的断言信息。具体而言,认证器信息处理单元313验证断言信息是否与在S511中创建的生物特征认证参数中包括的断言质询匹配。要注意的是,认证器信息管理表(表G)被用于指定公共密钥。

[0173] 使用利用在断言信息中包括的认证ID指定的公共密钥来解密在断言信息中包括的签名。认证器信息管理表(表G)被用于指定公共密钥。然后,验证解密的值是否与步骤

S511中创建的生物特征认证参数中包括的断言质询匹配。

[0174] 当解密的值与步骤S511中创建的生物特征认证参数中包括的断言质询不匹配时，酒店服务310的服务处理单元316以指示用户认证失败的信息向语音助理105回复。然后，服务处理单元316结束该处理。在接收到指示用户认证已失败的信息时，语音服务340的语音发出单元343通过语音向用户报告尚未执行在步骤S507中接收到的请求。

[0175] 另一方面，当解密的值与步骤S511中创建的生物特征认证参数中包括的断言质询匹配时，处理前进到步骤S518。在步骤S518中，酒店服务310的服务处理单元316根据在步骤S507中接收到的请求确认提供服务，即，客房服务的菜单的定稿。

[0176] 服务处理单元316将关于经确认的服务的信息存储在服务信息管理表中(表D)。要注意的是，由于支付是在退房时马上全部进行的，因此指示尚未进行支付的数据被存储在服务信息管理表的支付信息中。然后，服务处理单元316向负责该服务的人发起提供服务的请求。

[0177] 在步骤S519中，服务处理单元316将在步骤S509中从语音助理105接收到的对于提供服务的请求的受理结果发送到语音助理105。在步骤S520中，语音服务340的语音发出单元343通过语音向用户报告在步骤S519中接收到的受理结果。

[0178] 接下来，将使用图8描述当酒店的客人(用户)退房时结束使用酒店服务310的处理。

[0179] 在结束酒店服务310的使用的处理中，执行注册取消处理，其中从酒店服务310取消由用户携带的移动终端103的认证器330的注册。

[0180] 首先，用户通过用户操作使移动终端103的应用320显示在退房屏幕上。具体而言，通过操作应用320的菜单显示(未示出)来显示退房屏幕。

[0181] 图12是由应用320的显示单元321显示的退房屏幕的示例。

[0182] 在酒店入住期间由于用户使用服务而产生的服务费显示在退房屏幕上。在通过用户操作接收到显示退房屏幕的指令时，应用320经由通信单元322查询该用户在酒店住宿期间接收到的酒店服务310的服务的细节。

[0183] 酒店服务310从在数据存储单元312中存储的服务信息管理表(表D)中获取用户接收到的服务的细节，并将细节发送到应用320。例如，基于接收到的服务细节，应用320计算服务信息管理表中用户接收到的服务量的总和，并在退房屏幕上显示该总和作为服务费。用户在退房屏幕上检查他或她接收到的服务的细节和服务费，并前进到酒店前台的支付处理。

[0184] 要注意的是，退房屏幕具有选择是否要保留生物特征认证信息的单元。生物特征认证信息是与生物特征信息相关联的各种信息。在图12所示的示例中，可以在复选框中选择是否要保留生物特征认证信息。当用户选择保留他的生物特征认证信息时，在他或她下次住宿时要执行开始使用图6中所示的酒店服务310的处理中，可以跳过在服务器102中注册认证器330的处理(S403至S408)。

[0185] 当选择保留其生物特征认证信息的用户下次住宿同一酒店时，用户可以在登记入住期间在图9的登记入住屏幕上输入在先前登记入住中发布的用户ID以及之前设置的密码。可以使用在先前登记入住中在图4的步骤S402中发布的用户ID。

[0186] 因而，酒店服务310的注册处理单元311参考用户信息管理表(表B)执行用户ID与

现有用户信息的核对，并确定该用户ID与具有对应用户ID和密码h的记录的用户是同一个人。然后，酒店服务310的注册处理单元311确定在认证器信息管理表(表G)中是否存在具有该用户ID的记录。

[0187] 当存在具有该用户ID的记录时，注册处理单元311省略图4的步骤S403至S408的处理。当按下退房屏幕上的“OK”按钮时，执行结束使用酒店服务310的处理(退房处理)的指令被给予应用320，并且开始图8中所示的处理的执行。

[0188] 现在描述将返回到图8。在步骤S601中，在从用户接收到执行退房处理的指令时，应用320将退房请求发送到酒店服务310。该请求包括由用户在退房屏幕上选择是否要保留他或她的生物特征认证信息的选择结果。

[0189] 在以下步骤S602和S603中，关于存储在服务器102中的移动终端103的用户的注册信息被更新。首先，在步骤S602中，酒店服务310的注册处理单元311取消在用户所住的房间中安装的语音助理105与移动终端103的认证器330的关联。即，存储于关联信息管理表(表E)中的其中语音助理105与用于指定认证器330的认证器ID相关联的记录被删除。

[0190] 在步骤S603中，在退房屏幕上选择不保留生物特征认证信息，注册处理单元311删除以下记录。即，删除证明质询管理表(表F)和认证器信息管理表(表G)中的用户的对应记录。要注意的是，用户信息管理表(表B)、住宿历史管理表(表C)和服务信息管理表(表D)中用户的对应记录被设置为保留而不被删除，以用于改善下次用户住宿时可能提供的服务。

[0191] 在步骤S604中，注册处理单元311以指示退房处理已完成的信息向移动终端103的应用320回复。要注意的是，指示退房处理已完成的信息包括用户在退房屏幕上选择是否要保留生物特征认证信息的选择结果。

[0192] 在步骤S605中，当选择不保留生物特征认证信息时，应用320请求从认证器330删除在认证信息管理表(表A)中关于酒店服务310的记录。在从应用320接收到记录删除请求时，认证器330的认证器注册处理单元331删除该记录。即，经由认证信息存储单元333在存储于TPM 226中的认证信息管理表(表A)中删除关于酒店服务310的记录。

[0193] 根据本实施例，可以如上所述提供安全认证方法，而无需在部署在由许多未指定的人使用的地方的设备中注册生物特征认证信息。

[0194] [第二实施例]

[0195] 在第一实施例中，已经描述了当酒店的客人利用语音助理使用酒店提供的服务(诸如客房服务)时执行的各种处理。另一方面，在本实施例中，将描述客户利用语音助理使用由酒店外部(即，与服务器102不同的外部系统)提供的服务的情况。

[0196] 要注意的是，在本实施例中，相同的附图标记被赋予与第一实施例相同的设备的配置和各种处理的过程，并且将省略其描述。在本实施例中，将描述使用音乐分发服务107作为除酒店之外提供的服务的示例的情况。语音助理105经由网络101连接到音乐分发服务107。此外，移动终端103经由网络106连接到音乐分发服务107。

[0197] 要注意的是，假设用户预先与音乐分发服务107签订合同以利用他或她的房屋的语音助理接收服务，并从该服务获取ID和密码，以将他或她自己注册为该服务的用户。即，该服务专用于经过认证的用户。此外，假设音乐分发服务107支持认证方法，类似于第一实施例中描述的酒店服务310。

[0198] 即，假设音乐分发服务107具有如下机制，在该机制中，对用户手上的设备执行生

物特征认证以认证用户，并且服务基于结果认证用户。此外，假设用户预先使用移动终端103在音乐分发服务107中注册与生物特征认证相关联的信息（例如，认证标识信息、公共密钥等）。

[0199] 图13是用于描述在酒店的客人（用户）住宿的房间中经由语音助理105使用音乐分发服务107而执行的处理的图。

[0200] 用户通过话语（语音）向语音助理105发起使用音乐分发服务107的请求。例如，当期望音乐分发时，通过说出“在音乐分发服务中播放音乐”来发起请求。

[0201] 在步骤S1001中，语音助理105的语音服务340的语音接收单元341通过语音从用户接收对于提供服务的请求。在步骤S1002中，语音分析单元342分析所接收到的语音并确定请求的细节。在步骤S1003中，通信单元345将在步骤S1002中分析的处理请求发送到音乐分发服务107。

[0202] 在从语音助理105接收到请求时，音乐分发服务107在步骤S1004中根据接收到的请求来执行处理。在这里，当在音乐分发服务中提供服务时，假设用户认证是必需的。因此，在步骤S1005中，音乐分发服务107向语音助理105发起用户认证请求。

[0203] 要注意的是，假设这里提到的用户认证使用第一实施例中由酒店服务310使用的认证机制（图7）。具体而言，对用户手上的设备执行生物特征认证，并且基于结果认证用户。即，在步骤S1005中，音乐分发服务107向语音助理105发起生物特征认证请求。

[0204] 在这个时候，音乐分发服务107在请求中包括所生成的生物特征认证参数，如在图7的步骤S511的处理中那样。此外，音乐分发服务107可以在请求中包括其它信息。例如，可以包括诸如促销信息或价格指导信息之类的任何信息。

[0205] 要注意的是，在图7的步骤S511中，当酒店服务310发送对于用户认证的请求时，用于指定与语音助理105相关联的认证器330的认证器ID与生物特征认证参数一起被发送。但是，由于音乐分发服务107不保留诸如关联信息管理表（表E）之类的信息，因此不发送与其对应的信息。

[0206] 因此，在本实施例中，语音助理105执行指定用作生物特征认证请求的报告目的地的认证器330的处理。在步骤S1006中，语音服务340的生物特征认证控制单元344查询关于用作酒店服务310的生物特征认证请求的报告目的地的移动终端103的认证器330。

[0207] 在步骤S1007中，酒店服务310的服务处理单元316指定关联信息管理表（表E）中的与用作请求源的语音助理105相关联的移动终端103的认证器330。然后，在步骤S1008中，服务处理单元316以指示由语音助理105指定的认证器330的认证器ID回复。

[0208] 在步骤S1009中，语音服务340的生物特征认证控制单元344使用在步骤S1008中接收到的请求结果中包括的认证器ID来指定用作生物特征认证请求的报告目的地的认证器330。然后，生物特征认证控制单元344向移动终端103发起生物特征认证请求。要注意的是，生物特征认证请求包括在第一实施例中描述的自生生物特征认证参数。

[0209] 由于在步骤S1010至S1013中执行的生物特征认证处理与在第一实施例的步骤S514至S517中执行的处理相同，因此将省略其描述。当作为步骤S1013中执行的对断言信息的验证的结果而用户认证成功时，音乐分发服务107在步骤S1014中开始向语音助理105提供服务。即，音乐分发服务107将音乐数据分发到语音助理105。

[0210] 另一方面，当作为步骤S1013中执行的对断言信息的验证的结果，用户认证失败

时,音乐分发服务107以指示用户认证失败的信息向语音助理105回复,并且结束处理。在接收到指示用户认证失败的信息时,语音服务340的语音发出单元343通过语音向用户报告在步骤S1001中接收到的请求尚未被执行的事实。在步骤S1015中,语音服务340的语音发出单元343根据来自音乐分发服务107的服务的提供来播放音乐。

[0211] <第二实施例的修改例1>

[0212] 将使用图14描述在酒店的客人(用户)所住的房间中利用语音助理105使用音乐分发服务的处理(图13)的修改例。在图13所示的处理中,经由语音助理105向音乐分发服务107发起对于提供服务的请求(S1003)。

[0213] 另一方面,在图14所示的修改例中,移动终端103直接向音乐分发服务107发起请求,而不通过语音助理105。对于提供服务的请求是例如指定音乐的标题并从音乐分发服务107获取音乐数据等的请求。

[0214] 要注意的是,移动终端103安装由音乐分发服务107提供的应用,并与音乐分发服务107合作,并使用该应用发起对于提供服务的请求。可替代地,在移动终端103的web浏览器上,可以指定由音乐分发服务107提供的web服务的URL,并且可以通过用于使用音乐分发服务的服务屏幕来发起对于提供服务的请求。由音乐分发服务107提供并与音乐分发服务107合作的应用在下面将被称为合作应用。

[0215] 在步骤S1021中,移动终端103的合作应用根据来自用户的指令向音乐分发服务发起提供服务的请求。在步骤S1022中,音乐分发服务107从移动终端103接收处理请求,并根据所接收到的请求执行处理。在这里,假设用户认证对于从音乐分发服务接收服务提供是必需的。因此,在步骤S1023中,音乐分发服务107向语音助理105发起对于用户认证的请求。

[0216] 要注意的是,对于这里提到的用户认证,假设要使用在第一和第二实施例中由酒店服务310和音乐分发服务107使用的认证机制(图7和图13)。具体而言,对用户手上的设备执行生物特征认证,并且基于结果认证用户。即,在步骤S1023中,音乐分发服务107向移动终端103发起生物特征认证请求。

[0217] 在步骤S1024中,移动终端103执行生物特征认证处理。要注意的是,由于生物特征认证处理与第一和第二实施例中描述的相同,因此省略其描述。在步骤S1025中,移动终端103以断言信息向音乐分发服务107回复。在步骤S1026中,音乐分发服务107验证在步骤S1025中接收到的断言信息。

[0218] 当作为断言信息的验证的结果而用户认证成功时,音乐分发服务107在步骤S1027中开始向移动终端103提供服务。即,音乐分发服务107将在步骤S1021中请求的音乐数据分发到移动终端103。

[0219] 另一方面,当作为断言信息的验证的结果,用户认证失败时,音乐分发服务107以指示用户认证失败的信息向移动终端103回复,并且结束处理。在接收到用户认证失败的信息时,移动终端103在步骤S1028中将音乐数据传送到在移动终端103的用户所住的房间中安装的语音助理105。然后,用户通过话语(语音)向语音助理105发起请求。例如,用户指定在步骤S1028中传送的音乐的标题并发起播放音乐的请求。

[0220] 在步骤S1029中,语音助理105的语音服务340的语音接收单元341接收来自用户的语音请求。在步骤S1030中,语音分析单元342分析所接收到的语音并确定请求的细节。在步骤S1031中,语音发出单元343根据所分析的请求的细节播放音乐。

[0221] <第二实施例的修改例2>

[0222] 将使用图15描述在酒店的客人(用户)所住的房间中通过语音助理105使用音乐分发服务的处理(图13)的另一个修改例。在第一实施例中,当音乐分发服务107对用户进行认证时,生物特征认证是对用作用户手上的设备的移动终端103执行的,并且基于结果认证用户。另一方面,在图15所示的修改例中,生物特征认证是对语音操作设备执行的,该语音操作设备是用作用户手上的设备的语音助理105。

[0223] 要注意的是,假设音乐分发服务107和酒店服务310相互合作,并且客人可以在酒店房间中使用音乐分发服务107的服务。例如,假设音乐数据从音乐分发服务107被分发到语音助理105,并且语音助理105可以播放分发的音乐。

[0224] 音乐分发服务107检查来自酒店的合作的语音助理105的提供服务的请求的细节以及已经发起提供服务的请求的用户是否是合法的客人,然后将音乐数据分发到语音助理105。在这个时候,使用在第一或第二实施例中实现的认证机制来执行用户认证。具体而言,对用户手上的设备执行生物特征认证,并且基于结果认证用户。

[0225] 但是,与第一和第二实施例的不同之处在于语音助理105被用作用户手上的设备,而不是使用移动终端103。要注意的是,用于指定在酒店内使用的语音助理105的信息预先被注册(存储)在音乐分发服务107中。

[0226] 当登记入住酒店时,用户在语音助理105中注册他或她的生物特征体认证信息。生物特征认证信息的注册通过与第一实施例中在酒店登记入住时移动终端103的认证器330相对于服务器102的注册处理(S403到S408)相同的处理来执行。

[0227] 在本修改例中,语音助理105具有认证器330并且语音助理105的认证器330执行上面描述的从步骤S403至S408的处理中,类似于移动终端103。因而,用户的生物特征信息被存储在语音助理105中。要注意的是,如在其它实施例中那样,生物特征信息可以是任何类型的信息。例如,在这里假设生物特征信息是声纹信息。客人(用户)通过对语音助理105讲话来将他或她的声纹信息注册在语音助理105中。

[0228] 当用户想要从音乐分发服务107接收服务提供时,用户通过言语(语音)向语音助理105发起对于提供服务的请求。例如,用户指定音乐的标题并发起播放音乐的请求。

[0229] 在步骤S1041中,语音助理105的语音服务340的语音接收单元341接收来自用户的语音请求。在步骤S1042中,语音分析单元342分析所接收到的语音并确定请求的细节。在步骤S1043中,通信单元345将在步骤S1042中分析的处理请求发送到音乐分发服务107。

[0230] 在从语音助理105接收到请求时,音乐分发服务107在步骤S1044中根据所接收到的请求执行处理。详细而言,首先,音乐分发服务107确定用户认证对于执行接收到的请求是否是必需的。假设是否必需用户认证是预先在音乐分发服务107中设置的。例如,如果请求是获取音乐列表,那么确定用户认证不是必需的,并且如果请求是播放音乐,那么确定用户认证是必需的。

[0231] 在这里,由于所请求的是播放音乐,因此音乐分发服务107确定用户认证是必需的。因此,在步骤S1045中,音乐分发服务107向语音助理105发起对于用户认证的请求,即,生物特征认证请求。在这个时候,音乐分发服务107创建生物特征认证参数并在请求中包括所生成的生物特征认证参数,如第一实施例中那样。生物特征认证参数包括断言质询,该断言质询是将被用于执行如上所述的质询响应认证的验证数据。

[0232] 在接收到生物特征认证请求时,语音助理105在步骤S1046中执行生物特征认证处理。在由语音助理105执行的生物特征认证处理中,语音服务340的语音发出单元343通过语音指示用户接受生物特征认证并请求输入生物特征信息。例如,语音发出单元343通过语音指示用户说“将执行声纹认证,因此请说些什么”,并促使用户输入他或她的生物特征信息。

[0233] 在步骤S1046中从用户接收到语音时,语音助理105使用所接收到的语音的声纹信息执行生物特征认证处理。要注意的是,语音助理105具有与第一实施例中描述的移动终端103的认证器330相同的功能。然后,在步骤S1046中,在语音助理105中执行与由图7中所示的由移动终端103执行的生物特征认证处理(S514)相同的处理。

[0234] 当作为步骤S1046的生物特征认证处理的结果而认证成功时,语音助理105在步骤S1047中以所创建的断言信息向音乐分发服务107回复。断言信息包括作为生物特征认证处理的结果通过使用与生物特征信息相关联地存储的秘密密钥而创建的签名以及在步骤S1045中接收到的生物特征认证参数中包括的断言质询。

[0235] 要注意的是,当作为步骤S1046的生物特征认证处理的结果而认证失败时或者当用户未执行生物特征信息输入长达某个时间段时,语音服务340的语音发出单元343向用户报告它无法执行用户认证并且处理结束。然后,在步骤S1047中,回复指示生物特征认证处理的结果是认证失败的信息。在接收到指示认证已经失败的信息时,音乐分发服务107结束图15的处理。

[0236] 在步骤S1048中,音乐分发服务107验证在步骤S1047中接收到的断言信息。由于断言的验证是与第一实施例中图7的S517中由酒店服务310执行的处理相同的处理,因此省略其描述。

[0237] 当作为步骤S1048中执行的对断言信息的验证的结果而用户认证成功时,音乐分发服务107在步骤S1049中开始向语音助理105提供服务。即,音乐分发服务107将音乐数据分发到语音助理105。

[0238] 另一方面,当作为步骤S1048中执行的对断言信息的验证的结果而用户认证失败时,音乐分发服务107以指示用户认证已经失败的信息向语音助理105回复并且结束处理。在接收到指示用户认证已经失败的信息时,语音服务340的语音发出单元343通过语音向用户报告尚未执行在步骤S1041中接收到的请求。

[0239] 在步骤S1050中,语音服务340的语音发出单元343根据来自音乐分发服务107的服务提供来播放音乐。要注意的是,虽然在本修改例中已经描述了在语音助理105中注册生物特征信息的示例,但是本发明不限于此。例如,服务器102可以具有认证器330,并且用户的生物特征信息可以存储在服务器102中。

[0240] 在这种情况下,当语音助理105在步骤S1046中从用户接收到语音时,所接收的语音的声纹信息被发送到酒店服务310。然后,酒店服务310将接收到的声纹信息传送到其自己的认证器,并且由认证器执行生物特征认证处理。生物特征认证处理的结果从酒店服务310回复到语音助理105。

[0241] 此外,在本修改例中已经描述了音乐分发服务107执行用户的生物特征认证作为用户认证的方法的情况,但是本发明不限于此。例如,该方法可以是使用关键字的方法。在这种情况下,用户在登记入住时针对语音助理105设置任意关键字。执行关键字的注册,使得例如用户通过语音向语音助理105说出关键字。

[0242] 语音助理105在步骤S1045中从音乐分发服务接收对于用户认证的请求，并且向用户发起对于在登记入住时注册的关键字的请求。在接收到用户通过语音输入关键字时，语音助理105分析语音，并且当输入的关键字与登记入住时设置的关键字匹配时，语音助理确定用户认证处理成功。

[0243] (其它实施例)

[0244] 本发明的一个或多个实施例还可以通过读出并执行记录在存储介质(其也可以被更完整地称为“非瞬态计算机可读存储介质”)上的计算机可执行指令(例如，一个或多个程序)以执行上述一个或多个实施例中的一个或多个的功能和/或包括用于执行上述一个或多个实施例中的一个或多个的功能一个或多个电路(例如，专用集成电路(ASIC))的系统或装置的计算机来实现，以及通过例如由系统或装置的计算机从存储介质读出并执行计算机可执行指令以执行上述一个或多个实施例中的一个或多个的功能和/或控制一个或多个电路执行上述一个或多个实施例中的一个或多个的功能而执行的方法来实现。计算机可以包括一个或多个处理器(例如，中央处理单元(CPU)、微处理单元(MPU))，并且可以包括单独的计算机或单独的处理器的网络，以读出并执行计算机可执行指令。计算机可执行指令可以例如从网络或存储介质提供给计算机。存储介质可以包括例如硬盘、随机存取存储器(RAM)、只读存储器(ROM)、分布式计算系统的存储装置、光盘(诸如紧凑盘(CD)、数字多功能盘(DVD)或蓝光盘(BD)TM)、闪存设备、存储卡等中的一个或多个。

[0245] 虽然已经参考示例性实施例描述了本发明，但是应当理解的是，本发明不限于所公开的示例性实施例。所附权利要求的范围将被赋予最宽泛的解释，以便涵盖所有此类修改以及等同的结构和功能。

[0246] 本申请要求于2017年10月10日提交的日本专利申请No.2017-197216的权益，该申请通过引用整体上并入本文。

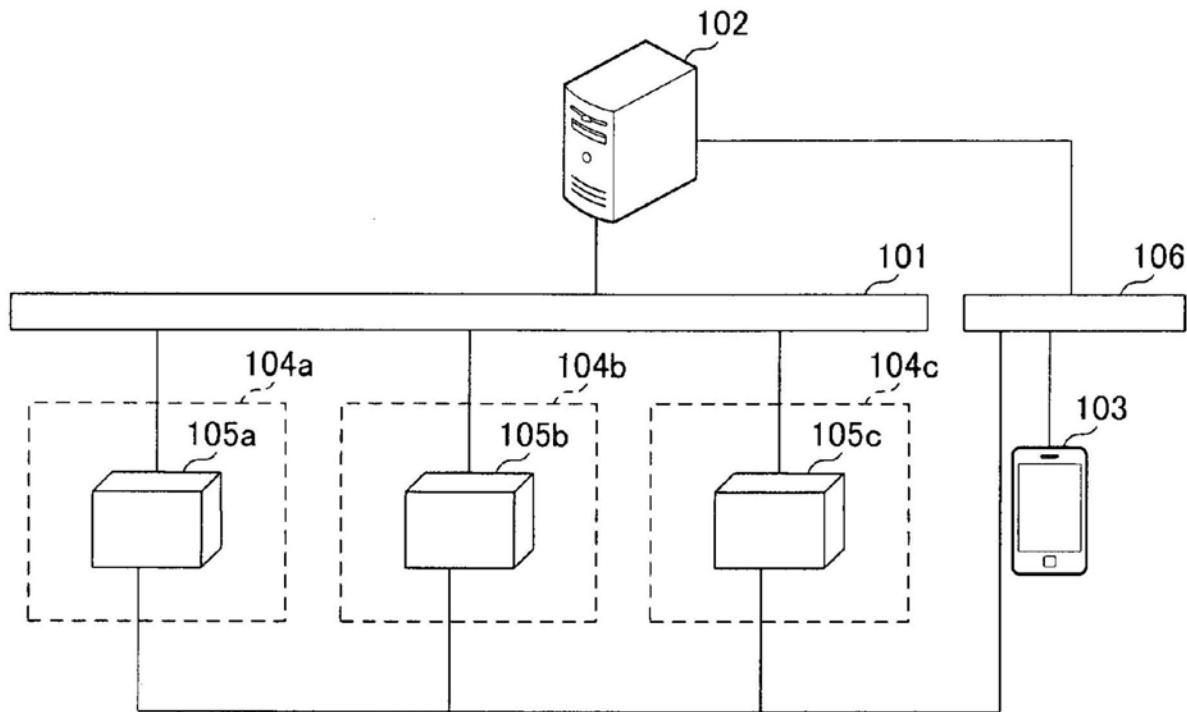


图1

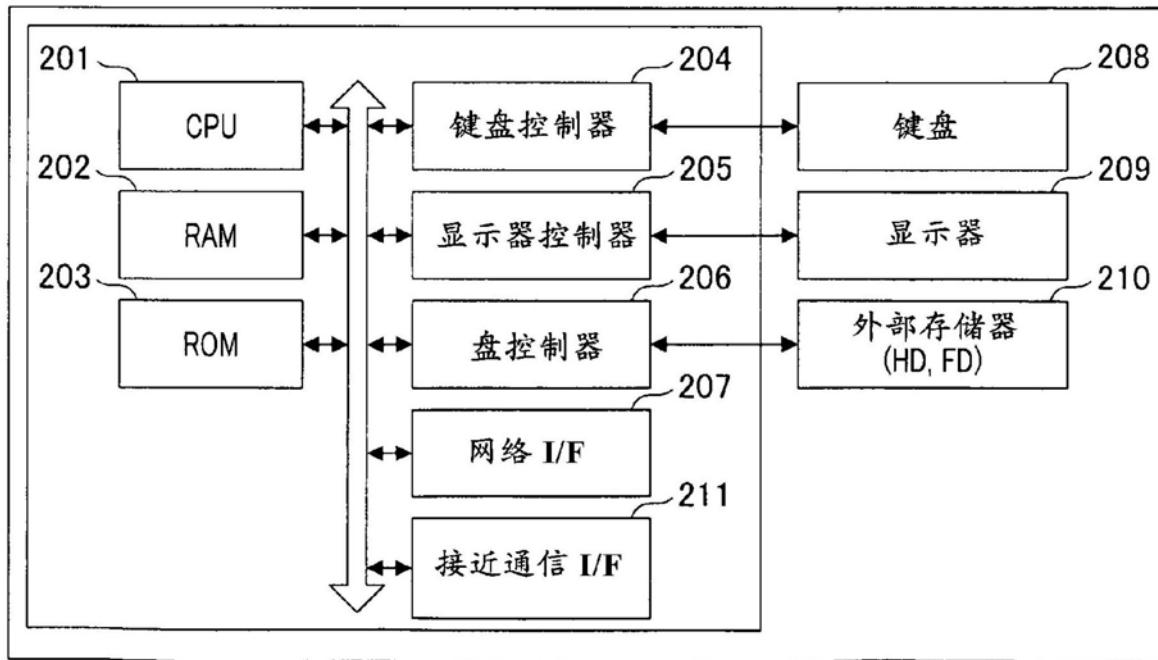


图2

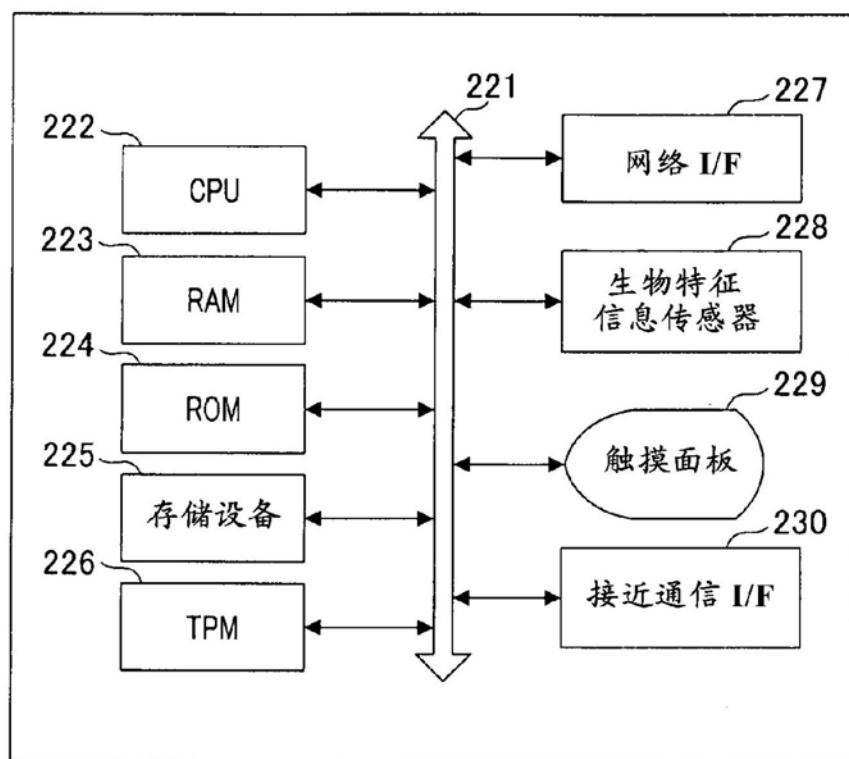


图3

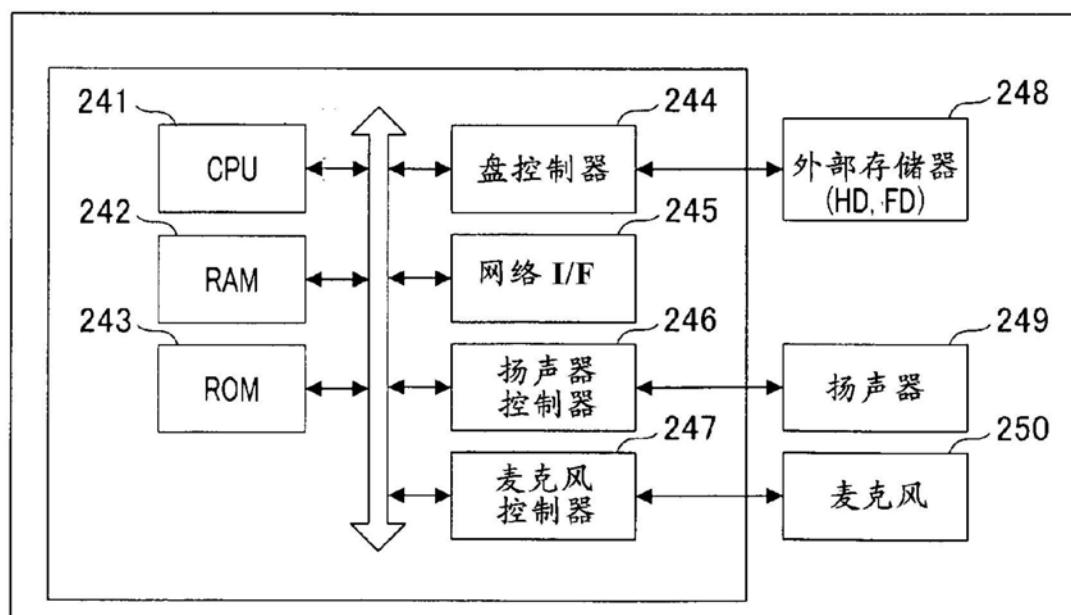


图4

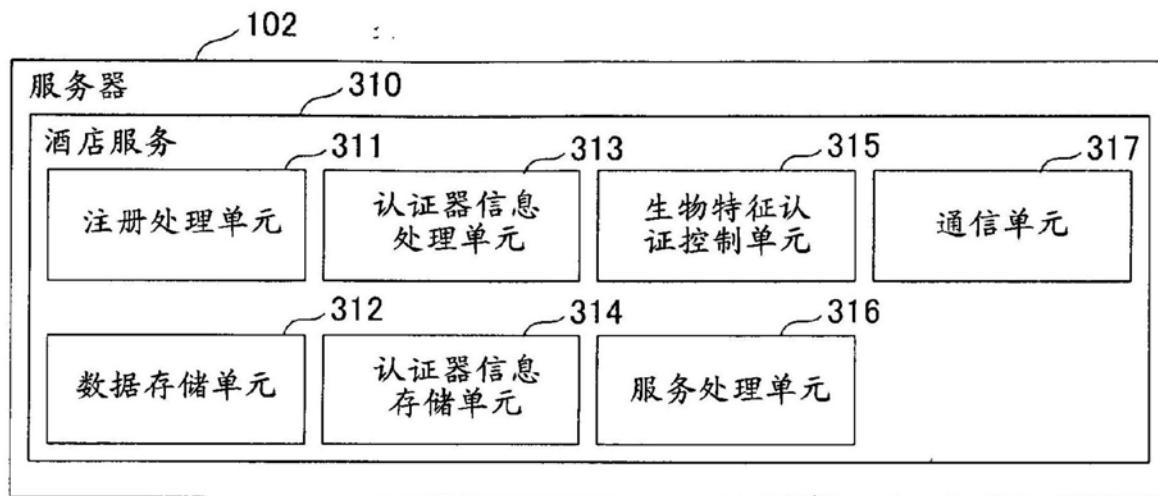


图5A

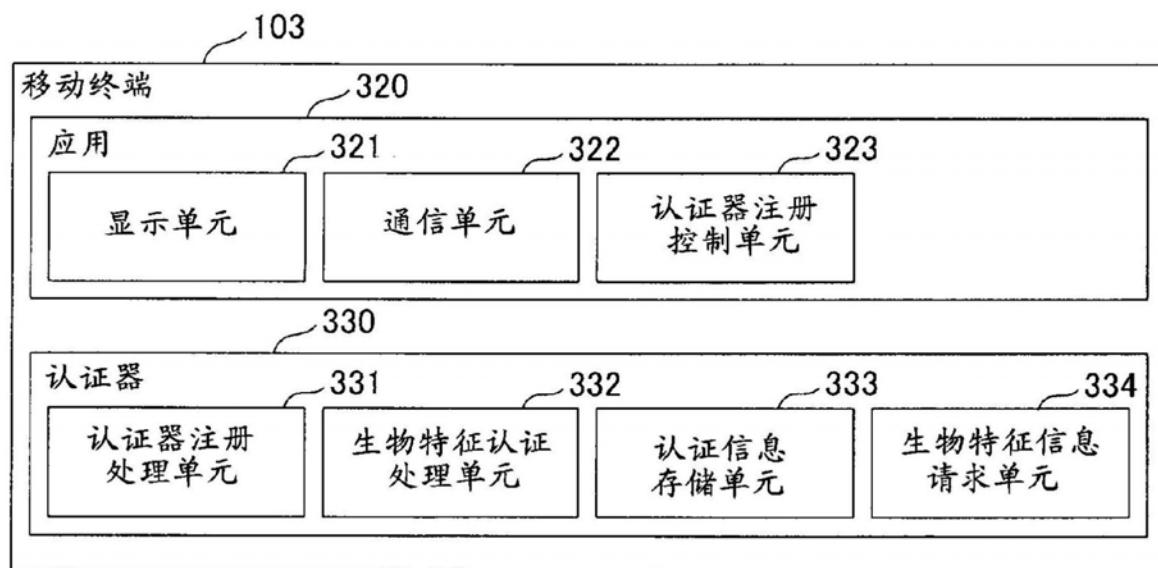


图5B

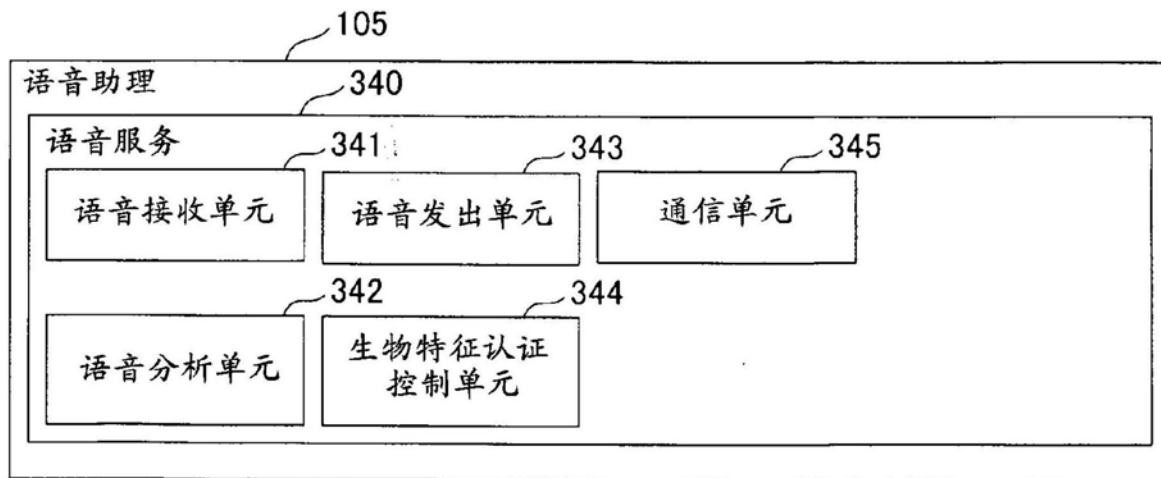


图5C

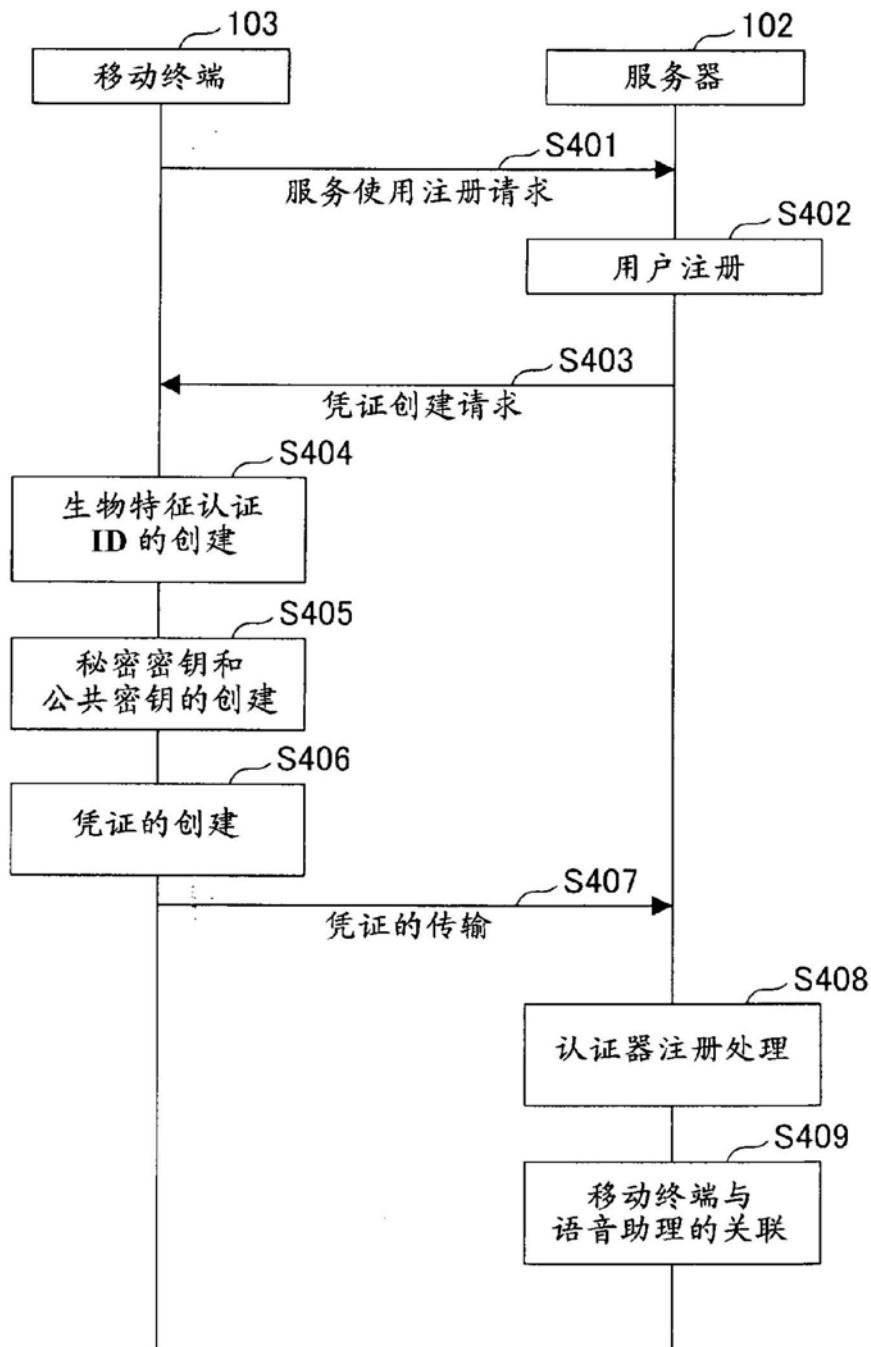


图6

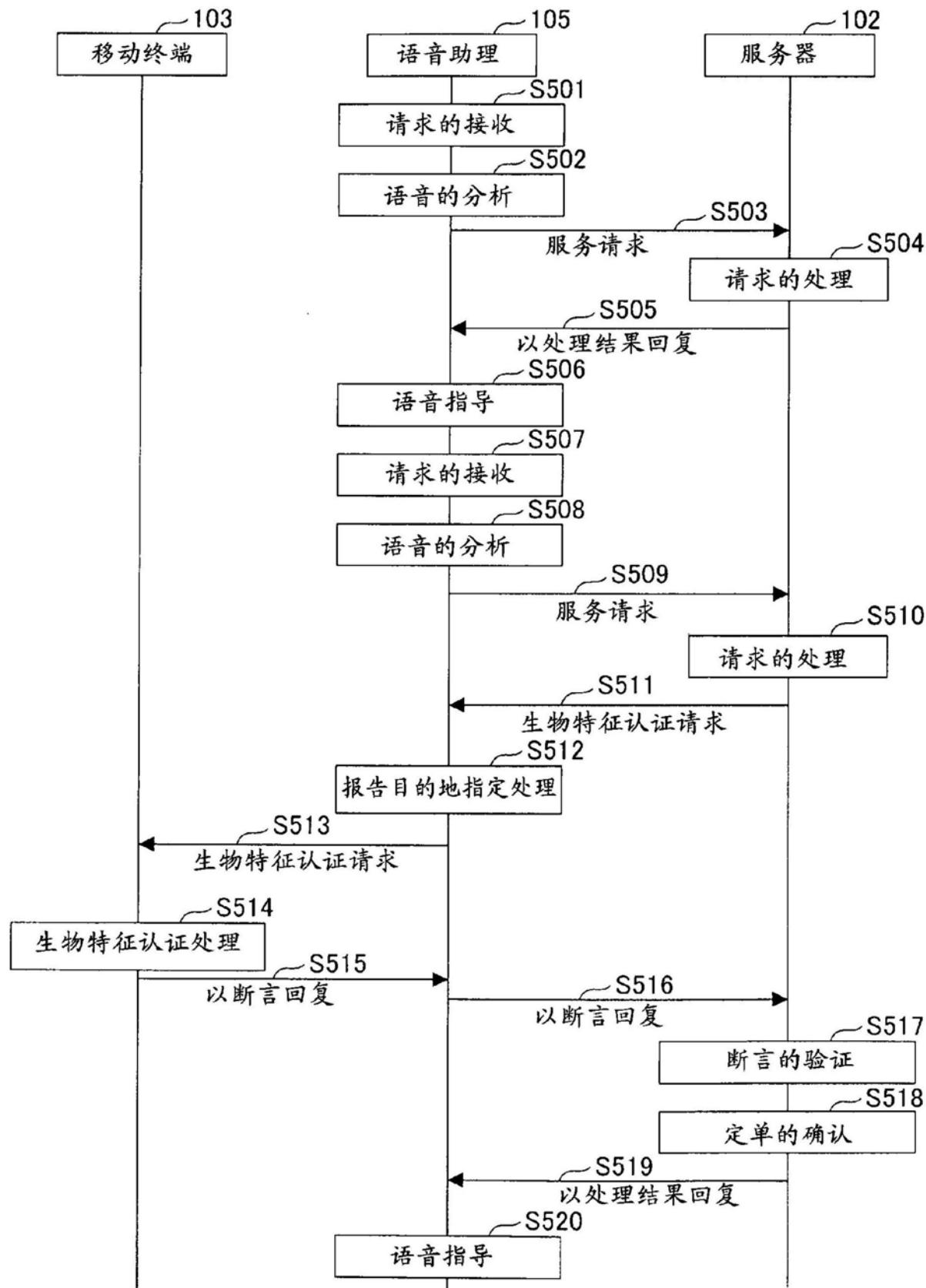


图7

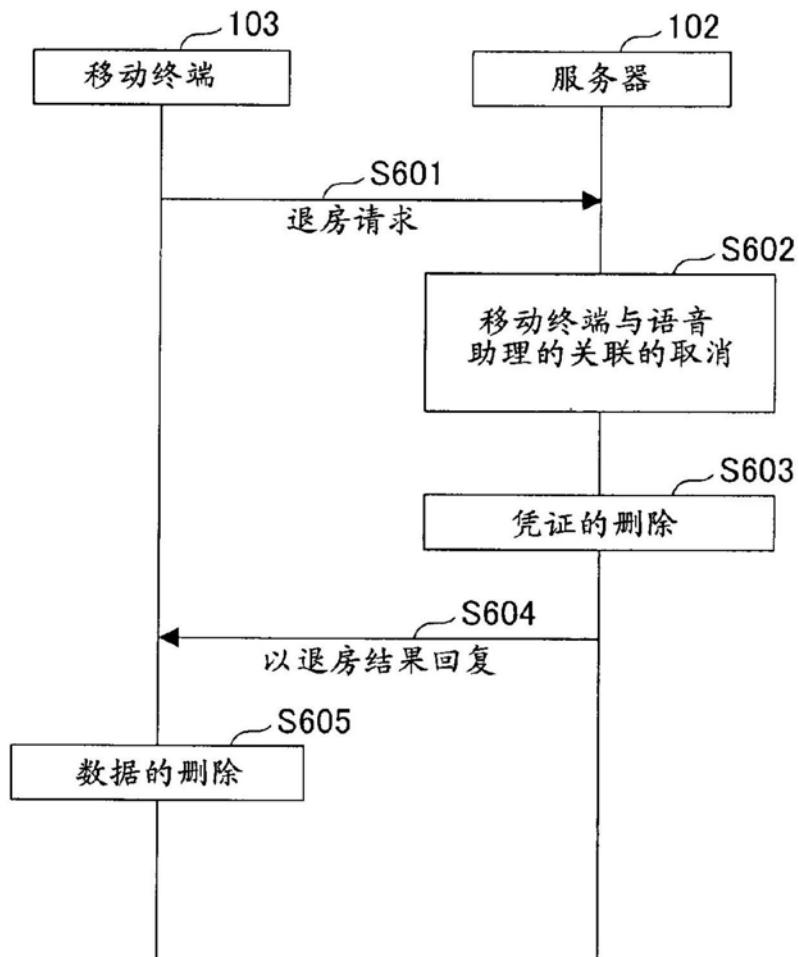


图8

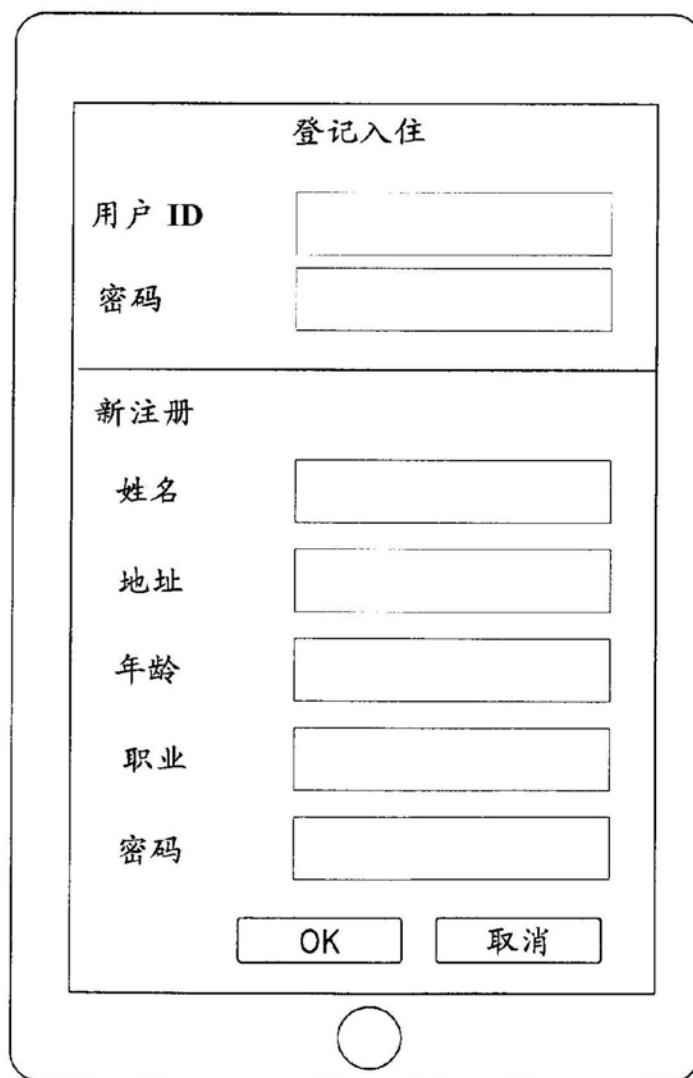


图9

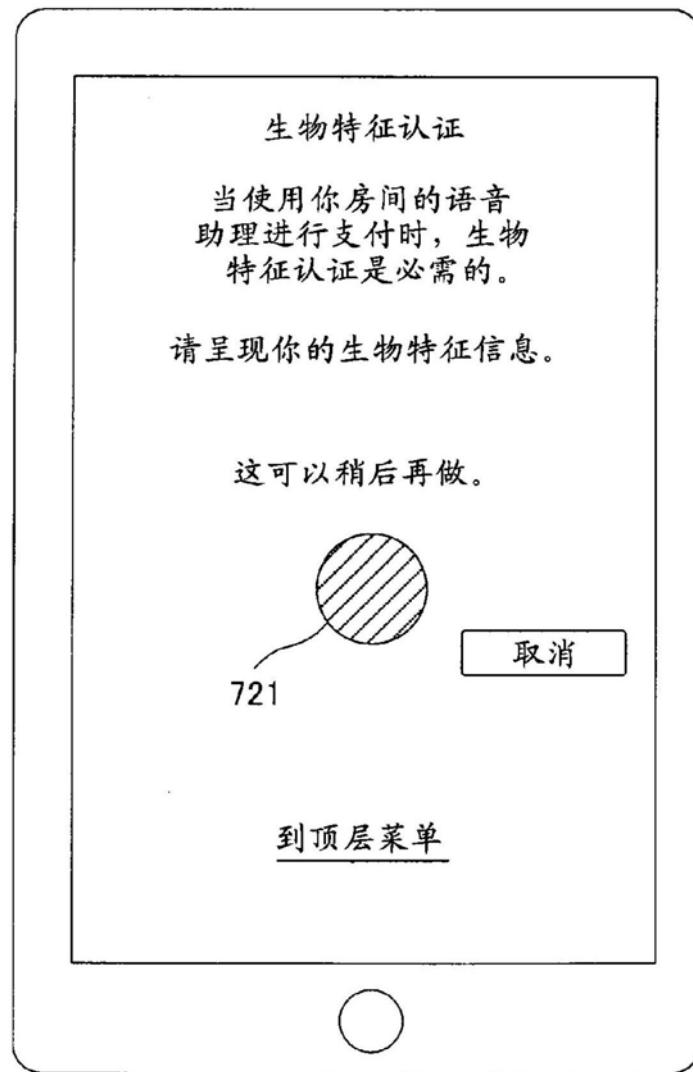


图10



图11

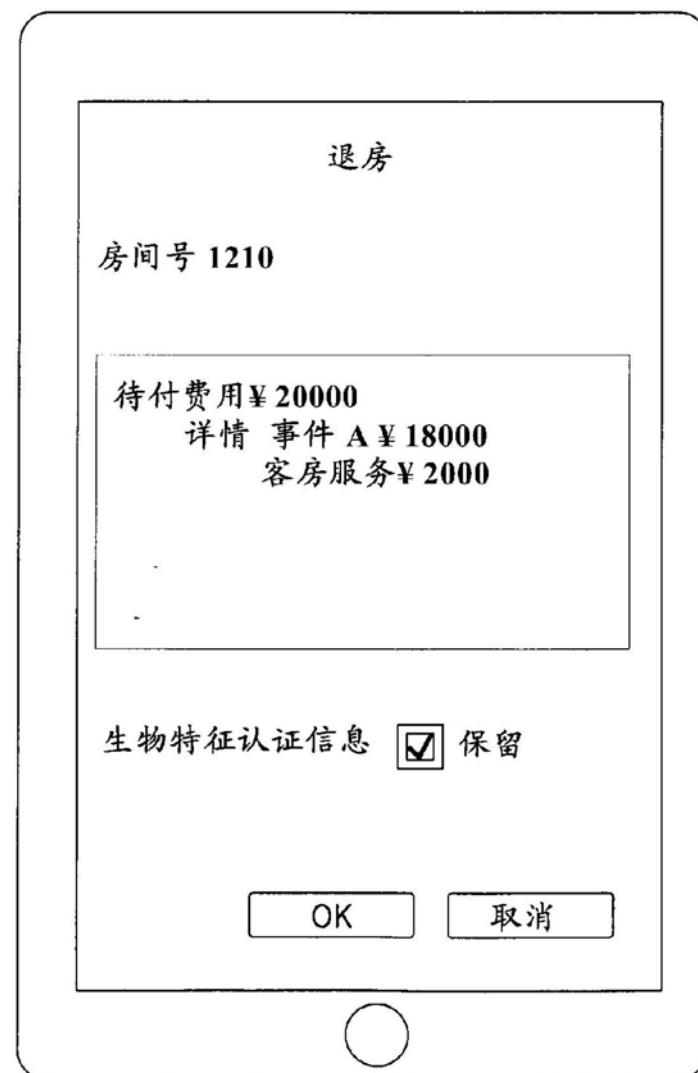


图12

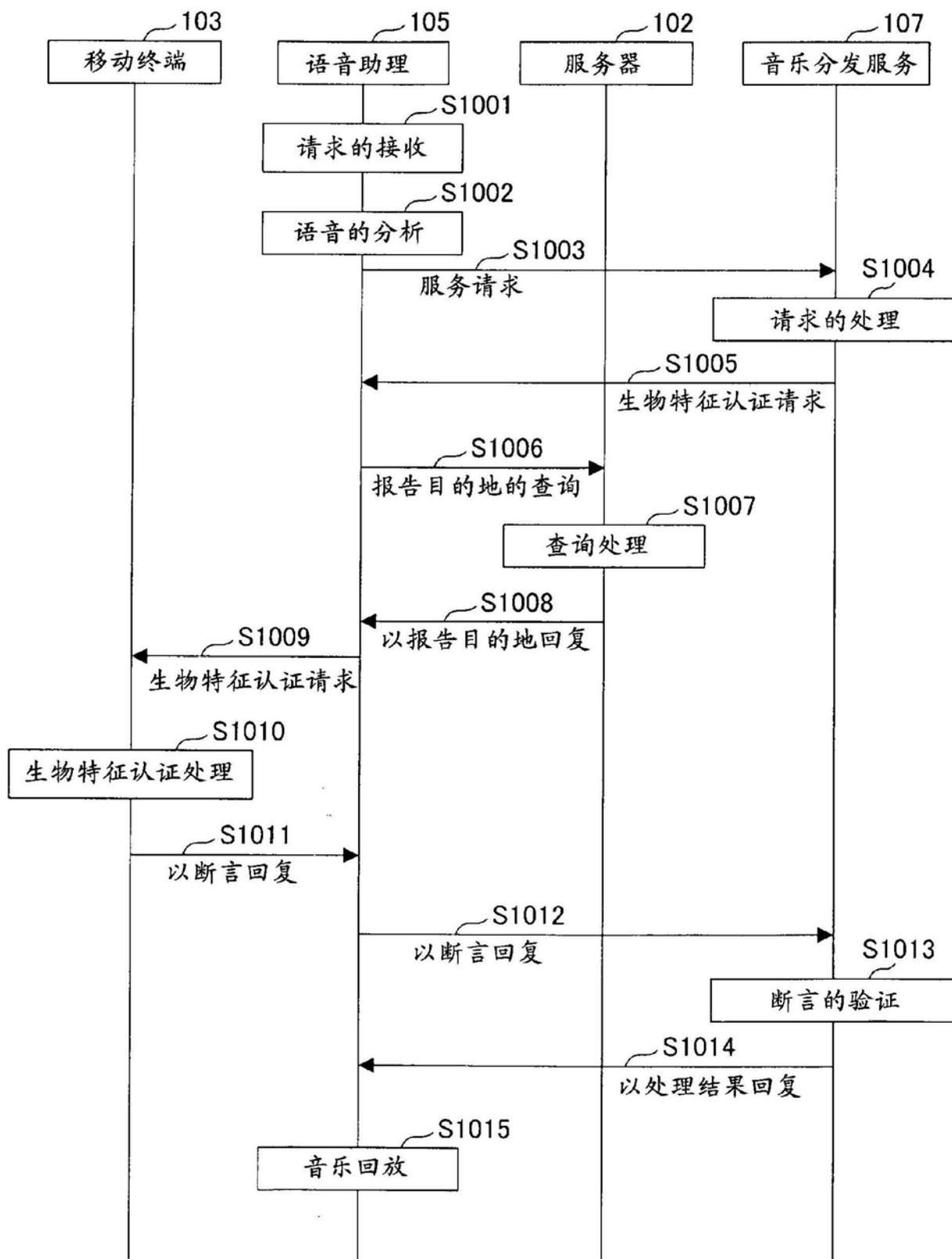


图13

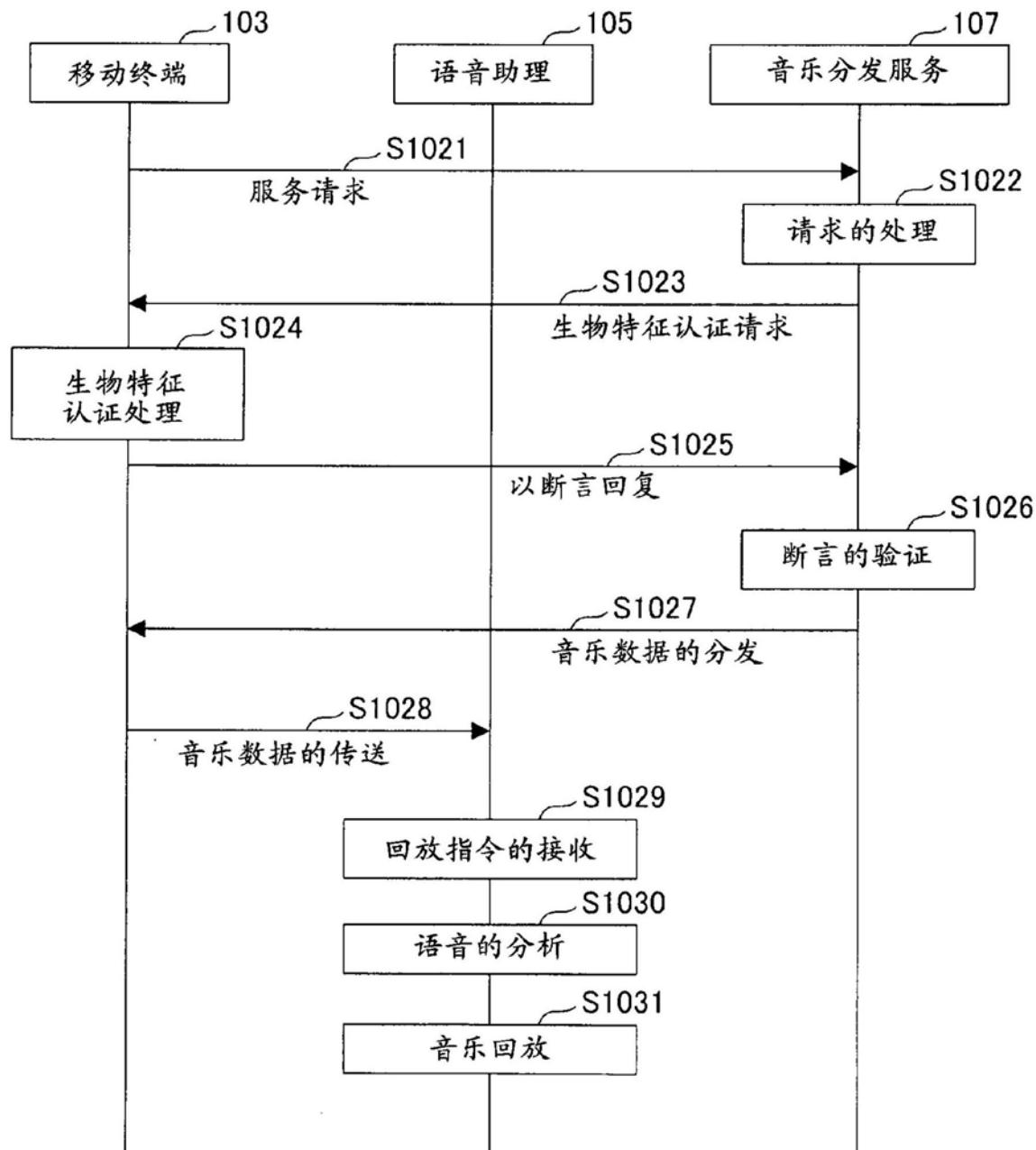


图14

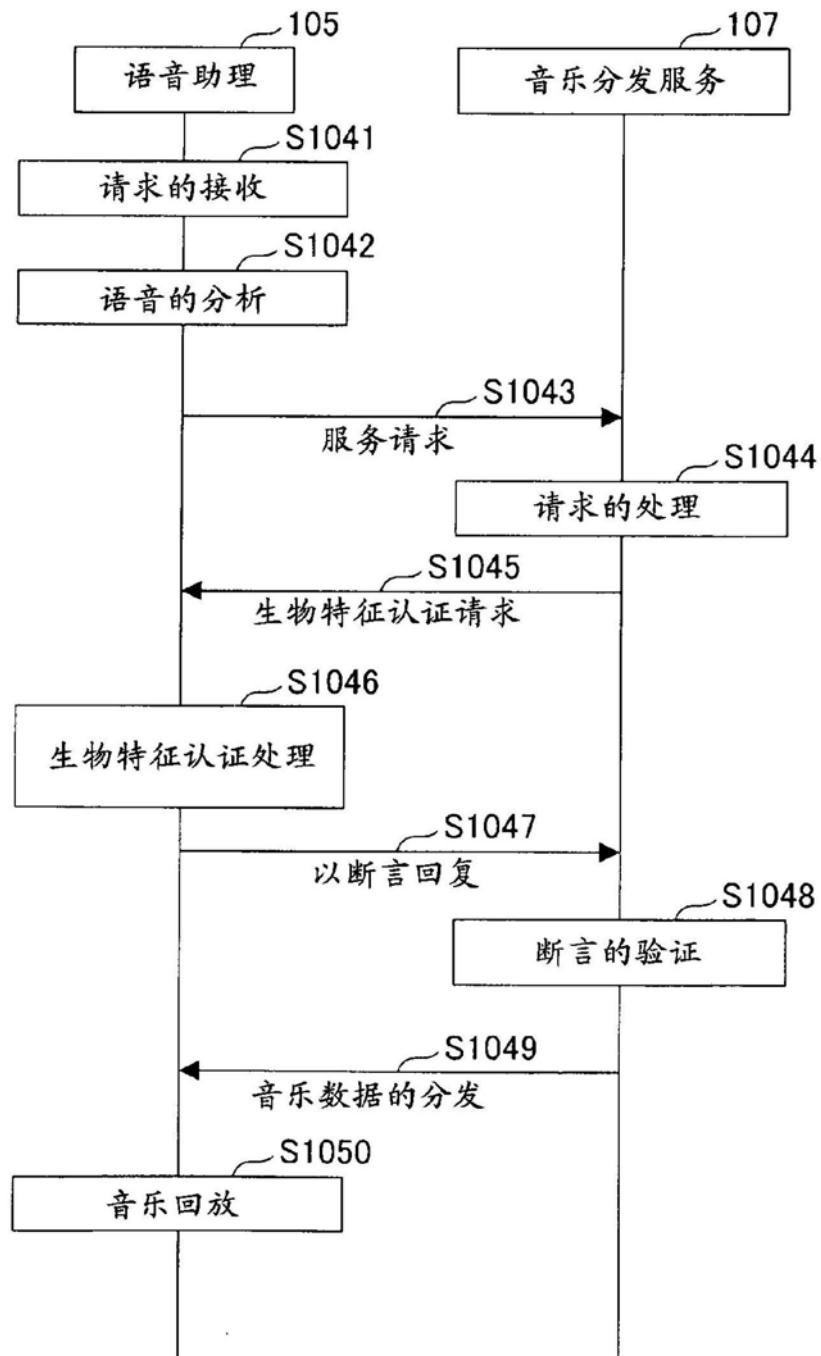


图15