



(12) 发明专利

(10) 授权公告号 CN 113763603 B

(45) 授权公告日 2023. 12. 15

| | |
|---|------------------------------|
| (21) 申请号 202110601568.9 | CN 206021341 U, 2017.03.15 |
| (22) 申请日 2021.05.31 | CN 109919557 A, 2019.06.21 |
| (65) 同一申请的已公布的文献号 申请公布号 CN 113763603 A | CN 2905977 Y, 2007.05.30 |
| (43) 申请公布日 2021.12.07 | JP 2018113586 A, 2018.07.19 |
| (30) 优先权数据 2020-095690 2020.06.01 JP | JP 2012210019 A, 2012.10.25 |
| (73) 专利权人 丰田自动车株式会社 地址 日本爱知县 | KR 20190014192 A, 2019.02.12 |
| (72) 发明人 狩野宏和 林雅敏 龟井玲汰 原菜美香 | CA 3051848 A1, 2020.02.14 |
| (74) 专利代理机构 中国贸促会专利商标事务所 有限公司 11038 专利代理师 孙蕾 | US 2019293437 A1, 2019.09.26 |
| (51) Int. Cl. G07C 9/00 (2020.01) H04W 4/40 (2018.01) H04W 12/06 (2021.01) | JP 2019191858 A, 2019.10.31 |
| (56) 对比文件 CN 101855861 A, 2010.10.06 | CN 109204227 A, 2019.01.15 |
| CN 111094082 A, 2020.05.01 | CN 110288729 A, 2019.09.27 |
| CN 110910156 A, 2020.03.24 | CN 110065470 A, 2019.07.30 |
| CN 110400102 A, 2019.11.01 | JP 2019053484 A, 2019.04.04 |
| CN 110517375 A, 2019.11.29 | KR 20180110286 A, 2018.10.10 |
| CN 110336892 A, 2019.10.15 | JP 2001112071 A, 2001.04.20 |
| | CN 206617017 U, 2017.11.07 |
| | JP 2018133062 A, 2018.08.23 |
| | JP 2015191602 A, 2015.11.02 |
| | US 2020138304 A1, 2020.05.07 |
| | JP 2005307736 A, 2005.11.04 |
| | US 2016112389 A1, 2016.04.21 |
| | US 2020136826 A1, 2020.04.30 |
| | CN 107786393 A, 2018.03.09 |
| | CN 110143175 A, 2019.08.20 |
| | CN 104635501 A, 2015.05.20 |

(续)

审查员 左丹

权利要求书2页 说明书10页 附图7页

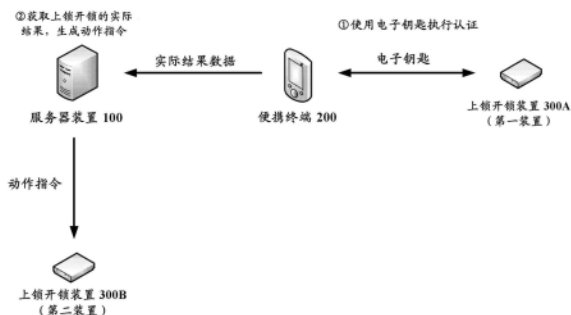
(54) 发明名称

信息处理装置、方法、计算机可读存储介质及便携终端

(57) 摘要

本公开涉及信息处理装置、方法、计算机可读存储介质及便携终端。在构成为具有多个设备的网络中取得设备之间的协作。获取第一数据，该第一数据表示基于从便携装置获取的电子钥匙进行认证的第一装置所进行的认证的实际结果，基于所述第一数据，生成包含对第二装置的动作指令的第二数据，并向所述第二装置发送。

动作指令的第二数据，并向所述第二装置发送。



CN 113763603 B

[接上页]

(56) 对比文件

CN 109920114 A, 2019.06.21
CN 111090238 A, 2020.05.01
CN 105196950 A, 2015.12.30
JP 2008072160 A, 2008.03.27

WO 2019017010 A1, 2019.01.24
JP 2019087801 A, 2019.06.06
CN 103547466 A, 2014.01.29
CN 110611883 A, 2019.12.24
CN 106790602 A, 2017.05.31
CN 108924016 A, 2018.11.30

1. 一种信息处理装置,该信息处理装置具有控制部,该控制部执行:
获取第一数据,该第一数据表示基于从便携装置获取到的电子钥匙进行认证的第一装置所进行的认证的实际结果;以及
参照将所述便携装置、所述第一装置和第二装置关联起来的协作数据以及所述第一数据,在判定为存在应协作地动作的装置的情况下,确定所述第二装置和应由所述第二装置进行的动作,生成包含对所述第二装置的动作指令的第二数据,并向所述第二装置发送,
其中,所述第一装置是根据所述认证的结果控制车辆的点火或主电源的装置,
在所述认证成立时,以所述车辆的发动机起动、发动机停止、主电源接通或者主电源关机为触发,所述便携装置将所述第一数据向所述信息处理装置发送,
所述第一装置和所述第二装置中的一者是设于车辆的装置,另一者是设于住宅的装置。
2. 根据权利要求1所述的信息处理装置,其中,
还具有存储部,将所述便携装置、所述第一装置以及所述第二装置对应起来存储。
3. 根据权利要求2所述的信息处理装置,其中,
所述第一数据是将识别所述便携装置的第一标识符、识别所述第一装置的第二标识符以及作为所述认证的结果所进行的动作相互关联起来的数据。
4. 根据权利要求1~3中任一项所述的信息处理装置,其中,
所述控制部基于进行了所述认证的场所,决定是否生成所述第二数据。
5. 根据权利要求1~3中任一项所述的信息处理装置,其中,
所述控制部从接收了所述动作指令的所述第二装置接收响应,向所述便携装置通知所述响应的内容。
6. 根据权利要求1所述的信息处理装置,其中,
所述第二装置是与住宅的防盗相关联的装置,
所述动作指令是切换在家模式、不在家模式的指令。
7. 一种信息处理方法,由信息处理装置执行,包括如下步骤:
获取第一数据,该第一数据表示基于从便携装置获取到的电子钥匙进行认证的第一装置所进行的认证的实际结果;
参照将所述便携装置、所述第一装置和第二装置关联起来的协作数据以及所述第一数据,判定是否存在应协作地动作的装置;以及
在判定为存在应协作地动作的装置的情况下,确定所述第二装置和应由所述第二装置进行的动作,生成包含对所述第二装置的动作指令的第二数据,并向所述第二装置发送,
其中,所述第一装置是根据所述认证的结果控制车辆的点火或主电源的装置,
在所述认证成立时,以所述车辆的发动机起动、发动机停止、主电源接通或者主电源关机为触发,所述便携装置将所述第一数据向所述信息处理装置发送,
所述第一装置和所述第二装置中的一者是设于车辆的装置,另一者是设于住宅的装置。
8. 根据权利要求7所述的信息处理方法,其中,还包括如下步骤:
获取所述便携装置、所述第一装置以及所述第二装置的对应关系的步骤。
9. 根据权利要求8所述的信息处理方法,其中,

所述第一数据是将识别所述便携装置的第一标识符、识别所述第一装置的第二标识符以及作为所述认证的结果所进行的动作相互关联起来的数据。

10. 根据权利要求7~9中任一项所述的信息处理方法,其中,基于进行了所述认证的场所,决定是否生成所述第二数据。

11. 根据权利要求7~9中任一项所述的信息处理方法,其中,从接收了所述动作指令的所述第二装置接收响应,向所述便携装置通知所述响应的内容。

12. 一种计算机可读存储介质,

该计算机可读存储介质非临时地存储用于使计算机执行权利要求7~11中任一项所述的信息处理方法的程序。

13. 一种便携终端,该便携终端具有:存储部,存储电子钥匙;和控制部,该控制部执行:利用所述电子钥匙对具有认证功能的第一装置请求认证;

生成表示所述第一装置进行了所述认证的意思的第一数据,并向第一信息处理装置发送;

从所述第一信息处理装置接收如下结果:响应于将所述便携终端、所述第一装置和所述第二装置关联起来的协作数据以及所述第一数据,在判定为存在应协作地动作的装置的情况下,确定所述第二装置和应由所述第二装置进行的动作,并发行了对所述第二装置的动作指令的结果;以及

向用户提示所述结果,

其中,所述第一装置是根据所述认证的结果控制车辆的点火或主电源的装置,

在所述认证成立时,以所述车辆的发动机起动、发动机停止、主电源接通或者主电源关机为触发,所述便携终端将所述第一数据向所述第一信息处理装置发送,

所述第一装置和所述第二装置中的一者是设于车辆的装置,另一者是设于住宅的装置。

信息处理装置、方法、计算机可读存储介质及便携终端

技术领域

[0001] 本公开涉及信息处理装置、信息处理方法、计算机可读存储介质以及便携终端。

背景技术

[0002] 近年来,与网络连接的IoT设备正在增加。例如,在汽车领域中,具备通信模块的联网汽车增加,在住宅中,能够经由网络控制室内的设备的服务器装置也呈现普及的征兆。

[0003] 与此相关联地,在专利文献1中公开了在利用不同的协议的多个设备之间能够相互访问的系统。

[0004] 现有技术文献

[0005] 专利文献

[0006] 专利文献1:日本特表2019-505060号公报

发明内容

[0007] 发明要解决的问题

[0008] 在构成为具有多个IoT设备的网络中,期望进一步提高便利性。

[0009] 本公开是考虑上述课题而完成的,其目的在于在构成为具有多个设备的网络取得设备之间的协作。

[0010] 用于解决问题的方案

[0011] 本公开的第一方式的信息处理装置的特征在于,

[0012] 该信息处理装置具有控制部,该控制部执行:获取第一数据,该第一数据表示基于从便携装置获取到的电子钥匙进行认证的第一装置所进行的认证的实际结果;以及基于所述第一数据,生成包含对第二装置的动作指令的第二数据,并向所述第二装置发送。

[0013] 另外,本公开的第二方式的信息处理方法的特征在于,

[0014] 该信息处理方法包括如下步骤:获取第一数据,该第一数据表示基于从便携装置获取到的电子钥匙进行认证的第一装置所进行的认证的实际结果;以及基于所述第一数据,生成包含对第二装置的动作指令的第二数据,并向所述第二装置发送。

[0015] 另外,本公开的第三方式的便携终端的特征在于,

[0016] 该便携终端具有:存储部,存储电子钥匙;和控制部,该控制部执行:利用所述电子钥匙对具有认证功能的第一装置请求认证;生成表示所述第一装置进行了所述认证的意思的第一数据,并向第一信息处理装置发送;从所述第一信息处理装置接收响应于所述第一数据而发行了对第二装置的动作指令的结果;以及向用户提示所述结果。

[0017] 另外,作为其他方式,可列举出用于使计算机执行上述信息处理方法的程序或者非临时地存储有该程序的计算机可读存储介质。

[0018] 发明效果

[0019] 根据本发明,能够在构成为具有多个设备的网络中取得设备之间的协作。

附图说明

- [0020] 图1是第一实施方式的认证系统的概要图。
- [0021] 图2是概略性地表示系统所包含的构成要素的一例的框图。
- [0022] 图3是表示服务器装置所生成的钥匙数据的例子的图。
- [0023] 图4是表示服务器装置所存储的实际结果数据的例子的图。
- [0024] 图5是表示服务器装置所存储的协作数据的例子的图。
- [0025] 图6是在各构成要素之间收发的数据的流程图。
- [0026] 图7是表示第二实施方式的实际结果数据/协作数据的例子的图。
- [0027] 图8是第三实施方式的安全装置的概要框图。
- [0028] 附图标记说明
- [0029] 100…服务器装置;101、201、401…通信部;102、202、302、402…控制部;103、203、303、403…存储部;200…便携终端;205…输入输出部;204、304、404…近距离通信部;300…上锁开锁装置;400…安全装置;405…传感器组。

具体实施方式

[0030] 本公开的一技术方案的信息处理装置是用于基于使用电子钥匙进行了认证的实际情况来使多个装置协作动作的装置。

[0031] 具体而言,特征在于,具有执行如下动作的控制部:获取第一数据,该第一数据表示基于从便携装置获取的电子钥匙进行认证的第一装置所进行的认证的实际情况,基于所述第一数据,生成包含对第二装置的动作指令的第二数据,并向所述第二装置发送。

[0032] 便携装置是使用电子钥匙从第一装置接受认证的装置。便携装置既可以是智能手机等小型计算机(便携终端),也可以是IC卡等。另外,第一装置例如既可以搭载于车辆,也可以配备于设备或者建筑物。另外,也可以是基于认证结果控制上锁开锁的装置。

[0033] 第一数据是表示对便携装置的认证的实际情况的数据。第一数据例如响应于第一装置认证了便携终端的情况而生成。第一数据既可以从便携装置发送,也可以从第一装置发送。

[0034] 控制部基于获取到的第一数据,生成用于使第二装置进行预定的动作的第二数据,并向第二装置发送。需要说明的是,第二数据也可以仅在认证成功的情况下生成。

[0035] 根据该结构,能够以便携装置从第一装置接受了认证为触发,使关联的装置(第二装置)进行预定的动作。即,能够与用户的行动相配合地,使多个设备进行协作动作。

[0036] 另外,也可以特征在于,信息处理装置还具有将所述便携装置、所述第一装置以及所述第二装置相对应地进行存储的存储部。

[0037] 另外,也可以特征在于,所述第一数据包括识别所述便携装置的第一标识符和识别所述第一装置的第二标识符,所述控制部基于所述第一标识符和所述第二标识符,决定被发送所述第二数据的所述第二装置。

[0038] 通过将三者相关联地存储,能够针对便携装置和第一装置的每个组合,使恰当的装置进行处理。

[0039] 另外,也可以特征在于,所述第一装置是控制上锁开锁的装置。

[0040] 另外,也可以特征在于,所述第一数据还包括上锁/开锁的类别,所述控制部基于

所述类别,生成对所述第二装置的所述动作指令。

[0041] 在第一装置是控制上锁开锁的装置的情况下,例如能够将外出、回家这样的用户的行动作为触发,使第二装置进行预定的动作。由此,例如在用户对正门进行了上锁的情况下,能够使与该用户相关联的车辆自动地开锁。

[0042] 另外,也可以特征在于,所述控制部基于进行所述认证的场所,决定是否生成所述第二数据。

[0043] 根据该结构,例如能够仅在便携装置靠近第二装置的情况下进行处理。由此,例如能够与车辆被上锁的情况联动地将自家的正门开锁,但在该车辆离开自家的情况下不进行开锁。

[0044] 另外,也可以特征在于,所述控制部从接收到所述动作指令的所述第二装置接收响应,向所述便携装置通知所述响应的内容。

[0045] 通过向用户转送从第二装置接收到的响应,用户能够知道装置可靠地进行了动作。

[0046] 另外,也可以特征在于,所述第一装置和所述第二装置中的一者是设于车辆的装置,另一者是设于住宅的装置。

[0047] 根据该结构,能够使车辆与智能家居协作。例如,能够在用户离开正门的情况下使车辆的空调自动地启动,在用户到达自家的情况下,使自家的空调自动地启动。

[0048] 另外,能够在用户上车了的情况下,将自家自动地上锁、或者在用户下车了的情况下,将自家自动地开锁。

[0049] 另外,也可以特征在于,所述第二装置是与住宅的防盗相关联的装置,所述动作指令是切换在家模式/不在家模式的指令。

[0050] 根据该结构,例如能够在用户上车了的情况(即,离开自家的情况)下,使住宅的安全装置工作。

[0051] 以下,基于附图,说明本公开的实施方式。以下的实施方式的结构是例示,本公开并不限定于实施方式的结构。

[0052] (第一实施方式)

[0053] 参照图1说明第一实施方式的认证系统的概要。本实施方式的系统构成为包括服务器装置100、用户所持有的便携终端200、设于用户利用的设备(例如,住宅、设施、建筑物或者车辆等)的多个上锁开锁装置(300A、300B···)。

[0054] 多个上锁开锁装置300被分类成用户进行交互的装置和与该交互联动地动作的装置。在本实施方式中,将前者称为第一装置(上锁开锁装置300A),将后者称为第二装置(上锁开锁装置300B)。

[0055] 在本实施方式的系统中,便携终端200在与上锁开锁装置300A之间执行使用了电子钥匙的认证。在认证完成时,便携终端200将表示认证的结果或者实际结果的数据(第一数据。在实施方式中称为实际结果数据)向服务器装置100发送。接收到实际结果数据的服务器装置100对预先指定的第二装置发送包含预定的动作指令的数据(第二数据)。

[0056] 由此,用户能够仅通过进行一次动作来使关联的多个装置动作。例如,能够在将自家的正门上锁的情况下使此后要乘坐的车辆自动地开锁。

[0057] 详细地说明系统的构成要素。

[0058] 图2是概略性地示出图1所示的服务器装置100、便携终端200以及上锁开锁装置300的结构的一例的框图。

[0059] 服务器装置100是进行根据来自便携终端200的请求发行电子钥匙的处理和基于接收到的实际结果数据指示设备之间的协作动作的处理的装置。

[0060] 服务器装置100能够由通用的计算机构成。即,服务器装置100能够构成为具有CPU、GPU等处理器、RAM、ROM等主存储装置、EPROM、硬盘驱动器、可移动介质等辅助存储装置的计算机。需要说明的是,可移动介质例如也可以是USB存储器或者CD、DVD那样的盘记录介质。在辅助存储装置中储存有操作系统(OS)、各种程序、各种表等,通过执行储存于此的程序,能够实现后述那样的与预定的目的相一致的各功能。但是,一部分或者全部的功能也可以通过ASIC、FPGA这样的硬件电路来实现。

[0061] 服务器装置100构成为具有通信部101、控制部102以及存储部103。

[0062] 通信部101是用于将服务器装置100与网络连接的通信部件。在本实施方式中,通信部101能够利用4G、LTE等移动通信服务,经由网络而与其他装置(例如便携终端200)进行通信。

[0063] 控制部102是负责服务器装置100的控制的部件。控制部102例如由CPU构成。

[0064] 控制部102具有电子钥匙发行部1021和协作动作部1022作为功能模块。各功能模块也可以通过利用CPU执行存储于ROM等存储部件的程序来实现。

[0065] 电子钥匙发行部1021根据来自便携终端200的请求发行电子钥匙。电子钥匙是用于供便携终端200从上锁开锁装置300接受认证的数字数据。

[0066] 电子钥匙发行部1021在从便携终端200接收到电子钥匙的发行请求的情况下,发行与该便携终端200相对应的电子钥匙。电子钥匙既可以获取预先存储的电子钥匙,也可以动态地生成。例如,也能够生成仅在预定的时间段有效的电子钥匙、指定了使用次数的电子钥匙(例如,一次性钥匙等)、仅能够在预定的便携终端200中使用的电子钥匙等。

[0067] 需要说明的是,在便携终端200访问多个上锁开锁装置300的情况下,电子钥匙发行部1021能够针对每个作为对象的上锁开锁装置300向便携终端200发行多个电子钥匙。

[0068] 图3是示出在发行电子钥匙时向便携终端200发送的数据的图。如图所示,电子钥匙发行部1021将上锁开锁装置的标识符(上锁开锁装置ID)、其名称、对应的电子钥匙数据(二进制数据)对应起来,作为钥匙数据发送给便携终端200。

[0069] 协作动作部1022进行使多个上锁开锁装置300协作地动作的处理。第一,协作动作部1022接受从便携终端200发送的实际结果数据。另外,第二,协作动作部1022从后述的存储部103获取与装置的协作有关的数据(协作数据),基于该协作数据和接收到的实际结果数据,生成用于使第二装置动作的指令(动作指令)。

[0070] 说明实际结果数据和协作数据。

[0071] 图4是实际结果数据的例子。实际结果数据是表示第一装置(上锁开锁装置300A)对便携终端200进行了认证的实际结果的数据。实际结果数据是将日期和时间、便携终端200的标识符、作为第一装置的上锁开锁装置300A的标识符、作为认证结果所进行的动作(是上锁还是开锁)相互关联起来的数据。需要说明的是,实际结果数据也可以包括认证的结果(成功或者失败,在失败的情况下为出错代码等)。

[0072] 图5是协作数据的例子。

[0073] 协作数据是将便携终端(便携装置)、第一装置(第一装置)、第二装置(第二装置)关联起来的数据。具体而言,定义了如下意思:在便携终端200与第一装置之间认证成功的情况下,基于其结果,向第二装置发送预定的动作指令。

[0074] 在本例中,定义了如下意思:具有T001这样的标识符的便携终端与具有D001这样的标识符的第一装置(控制自家正门的上锁开锁的装置)进行认证,在进行了“上锁”的情况下,使具有D002这样的标识符的第二装置(控制车辆的上锁开锁的装置)进行“开锁”(附图标记501)。

[0075] 由此,在用户将正门的电子锁上锁的情况下,能够接下来进行使车辆的门开锁的应对。

[0076] 同样地,定义了如下意思:在标识符为D002的第一装置进行了“上锁”的情况下,使标识符为D001的第二装置进行“开锁”。

[0077] 由此,在用户将车辆上锁的情况下,能够接下来进行将正门的门开锁的应对。

[0078] 存储部103是存储信息的部件,由RAM、磁盘、闪速存储器等存储介质构成。在存储部103中存储有由控制部102执行的各种程序、数据等。另外,在存储部103中存储有用于生成电子钥匙的各种数据(认证关联数据)、前述的实际结果数据以及协作数据。

[0079] 接下来,说明便携终端200。

[0080] 便携终端200是例如智能手机、移动电话、平板电脑终端、个人信息终端、可穿戴计算机(智能手表等)这样的小型计算机。便携终端200构成为具有:通信部201、控制部202、存储部203、近距离通信部204以及输入输出部205。

[0081] 通信部201与通信部101同样,是用于经由网络而与服务器装置100进行通信的通信接口。

[0082] 控制部202是负责便携终端200的控制的部件。控制部202例如由微型计算机构成。控制部202也可以通过由CPU执行存储于后述的存储部203的程序来实现这些功能。

[0083] 控制部202具有认证请求部2021和实际结果数据生成部2022作为功能模块。各功能模块也可以通过由CPU执行存储于存储部件(ROM等)的程序而实现。

[0084] 认证请求部2021执行从服务器装置100获取电子钥匙的处理和与上锁开锁装置300进行通信并委托上锁开锁的处理。

[0085] 第一,认证请求部2021进行获取电子钥匙的处理。在本实施方式中,服务器装置100根据便携终端200的请求,生成包含电子钥匙的钥匙数据,经由通信部101向便携终端200发送。

[0086] 第二,认证请求部2021经由后述的输入输出部205向用户提供操作画面,基于用户所进行的操作,生成用于进行上锁或者开锁的请求。例如,认证请求部2021向触摸板显示器输出用于进行开锁的图标、用于进行上锁的图标等,基于由用户进行的操作,生成请求上锁或者开锁的数据(上锁开锁请求)。

[0087] 需要说明的是,用户所进行的操作不限于借助触摸板显示器进行的操作。例如,也可以基于硬件开关等。

[0088] 需要说明的是,在便携终端200不具有电子钥匙的情况下,无法从操作画面进行上锁操作和开锁操作。

[0089] 便携终端200所获取的电子钥匙既可以是固定钥匙,也可以是一次性钥匙。在任一

情况下,与电子钥匙相对应的认证信息被事先存储于上锁开锁装置300。

[0090] 在基于上锁开锁装置300的认证成功并执行了上锁开锁的情况下,实际结果数据生成部2022执行生成表示进行了上锁开锁的实际结果的数据(实际结果数据)并向服务器装置100发送的处理。

[0091] 存储部203是存储信息的部件,由RAM、磁盘、闪速存储器等存储介质构成。在存储部203中存储有从服务器装置100发送的钥匙数据、实际结果数据生成部2022所生成的实际结果数据以及由控制部202执行的各种程序、数据等。

[0092] 近距离通信部204是用于与上锁开锁装置300之间进行近距离无线通信的接口。近距离通信部204使用预定的无线通信标准进行近距离(几cm左右)的通信。

[0093] 在本实施方式中,近距离通信部204进行基于NFC标准(Near Field Communication:近场通信)的数据通信。需要说明的是,在本实施方式中例示NFC,但也能够利用其他无线通信标准。例如,也能够利用Bluetooth(注册商标)、UWB(Ultra Wideband:超宽带)、Wi-Fi(注册商标)等。

[0094] 输入输出部205是接受用户所进行的输入操作并对用户提示信息的部件。具体而言,由触摸板及其控制部件、液晶显示器及其控制部件构成。触摸板和液晶显示器在本实施方式中由一个触摸板显示器构成。

[0095] 接下来,说明上锁开锁装置300。

[0096] 上锁开锁装置300是用于对预定的设备、设施、或者建筑物的门进行上锁和开锁的装置,是构成智能钥匙系统的一部分的装置。

[0097] 上锁开锁装置300具有与便携终端200进行近距离无线通信来认证该便携终端200的功能以及基于认证了便携终端200的结果进行电子锁的上锁开锁的功能。上锁开锁装置300构成为具有控制部302、存储部303以及近距离通信部304。

[0098] 近距离通信部304是通过与近距离通信部204相同的通信标准,在与便携终端200之间进行通信的部件。

[0099] 控制部302是进行经由近距离通信部304而与便携终端200进行近距离无线通信来认证便携终端200的控制和基于认证结果进行电子锁的上锁开锁的控制的模块。控制部302例如由微型计算机构成。

[0100] 控制部302具有认证部3021和钥匙控制部3022作为功能模块。各功能模块也可以通过由CPU执行存储于存储部件(ROM等)的程序来实现。

[0101] 认证部3021基于从便携终端200发送的电子钥匙进行便携终端200的认证。具体而言,将存储于存储部303的认证信息与从便携终端200发送的电子钥匙进行对照,在它们匹配的情况下,判断为认证成功。在双方不匹配的情况下,判断为认证失败。在认证部3021对便携终端200的认证成功的情况下,用于进行上锁开锁的指令被向后述的钥匙控制部3022发送。

[0102] 需要说明的是,认证部3021所进行的认证的方式既可以是单纯地对认证信息彼此进行比较而验证同一性的方式,也可以是使用了非对称加密的方式。

[0103] 钥匙控制部3022基于从认证部3021发送来的指令控制电子锁。

[0104] 存储部303是存储信息的部件,由RAM、磁盘、闪速存储器等存储介质构成。在存储部303中存储有用于与从便携终端200发送的电子钥匙进行核对的认证信息、由控制部302

执行的各种程序、数据等。

[0105] 接下来,说明前述的各构成要素所进行的处理。图6是在各构成要素之间收发的数据的流程图。

[0106] 首先,便携终端200对服务器装置100发送请求电子钥匙的发行的数据(钥匙请求)(步骤S11A)。在该步骤中,同时发送以下的信息。

[0107] (1) 钥匙请求

[0108] (2) 识别便携终端200的信息

[0109] (3) 用于证明便携终端200的正当性的数据

[0110] 用于证明便携终端200的正当性的数据既可以是密码,也可以是生物体信息等。另外,也可以将这些信息哈希化。

[0111] 电子钥匙发行部1021在对便携终端200进行了认证的基础上,生成或者获取该便携终端200所固有的电子钥匙,并向便携终端200发送(步骤S11B)。

[0112] 在便携终端200的用户进行经由输入输出部205访问上锁开锁装置300A的操作时,便携终端200(认证请求部2021)对上锁开锁装置300A发送电子钥匙(步骤S12)。此时,也可以同时发送请求具体的处理(例如,上锁或者开锁)的数据(上锁开锁请求)。

[0113] 在步骤S13中,上锁开锁装置300A(认证部3021)将从便携终端200发送的电子钥匙和事先存储的认证信息进行核对,进行认证处理。另外,在认证成功的情况下,执行所请求的处理(上锁开锁处理)。例如,钥匙控制部3022控制电子锁实施上锁或者开锁。

[0114] 上锁开锁装置300A所具有的钥匙控制部3022在上锁或者开锁完成之后,对便携终端200发送处理完成的意思的通知(完成通知)(步骤S14)。由此,在便携终端200的触摸屏上输出上锁或者开锁完成的意思的通知。需要说明的是,在终端认证信息是一次性钥匙的情况下,也可以在该时刻使该一次性钥匙无效化。

[0115] 在步骤S15中,便携终端200生成本终端的标识符、上锁开锁装置300A的标识符以及表示对该上锁开锁装置300A所进行的动作(上锁或者开锁)的数据(实际结果数据),并向服务器装置100发送。实际结果数据是表示利用上锁开锁装置300A对便携终端200进行了认证的实际结果的数据。服务器装置将接收到的实际结果数据储存于存储部103。

[0116] 接下来,在步骤S16中,服务器装置100(协作动作部1022)参照实际结果数据和协作数据,判定是否存在应协作地动作的装置。具体而言,判定预先定义的便携终端200、上锁开锁装置300A(第一装置)、处理类别的组合中是否存在与实际结果数据匹配的组合,在存在的情况下,指定第二装置和应由第二装置进行的动作。例如,在第二装置是搭载于车辆的上锁开锁装置300B而应进行的动作为“开锁”的情况下,协作动作部1022对上锁开锁装置300B发送指示开锁的动作指令(步骤S17)。

[0117] 当在实际结果数据与协作数据之间没有一致的组合的情况下,处理结束。

[0118] 接收到动作指令的第二装置(上锁开锁装置300B)基于该动作指令进行处理(步骤S18)。具体而言,钥匙控制部3022控制电子锁实施上锁或者开锁。

[0119] 若处理完成,则第二装置(上锁开锁装置300B)将处理完成的意思的通知向服务器装置100发送(步骤S19)。该通知向便携终端200转送,经由输入输出部205向用户提供。

[0120] 如以上说明的那样,在第一实施方式的认证系统中,在用户使用便携终端进行了上锁开锁的情况下,使不同的上锁开锁装置联动地动作。由此,例如在将自家的正门上锁了

的情况下,能够自动地将车辆开锁,或者,在将车辆上锁了的情况下,能够自动地将自家的正门开锁。

[0121] (第二实施方式)

[0122] 在第一实施方式中,服务器装置100基于实际结果数据和协作数据生成动作指令。然而,在上锁开锁装置300是搭载于车辆的装置的情况下,有时会产生不期望的联动。例如,可能发生在用户在外出目的地将车辆上锁的情况下自家的正门开锁的不良情况。

[0123] 第二实施方式是为了应对这种情况而组合使用位置信息来判断是否需要协作动作的实施方式。

[0124] 在第二实施方式中,便携终端200构成为能够获取位置信息。位置信息例如能够经由GPS模块获取。另外,在第二实施方式中,便携终端200(实际结果数据生成部2022)在步骤S15中获取位置信息,使获取到的位置信息包含在实际结果数据中并向服务器装置100发送。

[0125] 图7的(A)是第二实施方式的实际结果数据的例子。实际结果数据所包含的位置信息(附图标记701)表示进行了上锁开锁的场所,即,便携终端200对第一装置发送了电子钥匙的场所。

[0126] 另外,在第二实施方式中,将“进行了上锁开锁的场所”满足预定的条件的情况设为协作动作的条件。图7的(B)是第二实施方式的协作数据的例子。在第二实施方式中,将位置条件(附图标记702)附加到协作数据中。

[0127] 在本例中,将协作动作的条件设为“在以自家为中心的预定的范围内进行了上锁开锁的情况”。即,仅在发送了表示在该范围内进行了上锁开锁的实际结果数据的情况下,生成对第二装置的动作指令。

[0128] 例如,在步骤S16中,协作动作部1022对协作数据所表示的位置条件和实际结果数据所表示的位置信息进行比较,在条件一致的情况下,生成动作指令。

[0129] 根据第二实施方式,能够防止发生不期望的上锁开锁。

[0130] (第三实施方式)

[0131] 在第一和第二实施方式中,利用上锁开锁装置作为第二装置。相对于此,第三实施方式是利用进行住宅的无人警备的家用安全装置作为第二装置的实施方式。

[0132] 图8是在第三实施方式中利用的家用安全装置(安全装置400)的系统结构图。安全装置400构成为具有通信部401、控制部402、存储部403、近距离通信部404以及传感器组405。

[0133] 关于通信部401、存储部403、近距离通信部404,由于与通信部201、存储部303、近距离通信部304是同样的,因此省略说明。

[0134] 控制部402是进行使用后述的传感器组405所包含的传感器进行住宅内的无人警备的处理和借助近距离通信部404进行便携终端200的认证并基于认证结果进行模式的切换的处理的模块。控制部402例如由微型计算机构成。

[0135] 控制部402具有认证部4021和监视部4022作为功能模块。各功能模块也可以通过CPU执行存储于存储部件(ROM等)的程序来实现。

[0136] 认证部4021与认证部3021同样地,基于通过近距离无线通信获取到的电子钥匙,对便携终端200进行认证。

[0137] 认证部4021基于认证结果,将装置的模式(以下,安全模式)切换为警戒模式和在家模式中的任一者。在安全模式处于警戒模式的情况下,后述的监视部4022的安全功能运转,进行基于传感器的住宅内的无人警备。在安全模式处于在家模式的情况下,解除安全功能。

[0138] 在安全模式处于警戒模式的情况下,监视部4022使用传感器组405所包含的多个传感器进行住宅内的警备。具体而言,监视住宅内有无无人,根据需要进行警报的生成、向相关机构的通报。

[0139] 传感器组405包括设于住宅内的多个传感器。多个传感器只要能够检测到位于住宅内的人,其种类就没有限制。例如,能够利用红外线传感器、门开闭传感器、图像传感器等。感测的结果被发送给监视部4022。

[0140] 在本实施方式中,利用安全装置400作为第二装置。图5的附图标记502所示的行是在本实施方式中利用的协作数据的例子。

[0141] 如图示的例子那样,在第一装置是搭载于车辆的上锁开锁装置而处理类别是“开锁”的情况下,对作为第二装置的安全装置400发送指示向警戒模式切换的动作指令。另外,在处理类别是“上锁”的情况下,对作为第二装置的安全装置400发送指示向在家模式切换的动作指令。

[0142] 本实施方式的数据流除了第二装置是安全装置400这一点之外,与图6所示的都相同。

[0143] 接收了动作指令的安全装置400(监视部4022)基于该动作指令,进行向所指定的模式的切换。

[0144] 在切换完成时,安全装置400向服务器装置100发送处理完成的意思的通知。该通知向便携终端200转送,经由输入输出部205向用户提供。由此,用户能够知道在家模式切换为警戒模式的情况或者警戒模式切换为在家模式的情况。

[0145] 需要说明的是,在本实施方式中,将第一装置设为车载的上锁开锁装置,将第二装置设为安全装置。即,将车辆的上锁开锁作为触发来切换安全装置的模式,但也可以将第一装置设为安全装置,将第二装置设为车载的上锁开锁装置。即,也可以将安全装置的模式切换作为触发,来进行车辆的上锁开锁。

[0146] 例如,在由用户将装置从在家模式切换为警戒模式的情况下,也可以向第二装置(例如,车载的上锁开锁装置300B)发送用于进行车辆的开锁的动作指令。另外,在由用户将装置切换为在家模式的情况下,也可以向第二装置(上锁开锁装置300B)发送用于进行车辆的上锁的动作指令。

[0147] 另外,在本实施方式中,将第一装置设为车载的上锁开锁装置,但也可以利用设于住宅的上锁开锁装置作为第一装置。根据该方式,能够与正门的上锁开锁联动地自动地切换安全装置的模式。

[0148] (变形例)

[0149] 上述实施方式至多是一例,本发明能够在不脱离其要旨的范围内适当变更来实施。

[0150] 例如,在本公开中说明的处理、方法只要不产生技术上的矛盾,就能够自由地组合来实施。

[0151] 另外,在实施方式的说明中,将第一装置设为是上锁开锁装置,但只要具有认证便携终端200的功能,第一装置就不限于控制上锁开锁的装置。例如,也可以是管理进出的装置、其他装置等。

[0152] 另外,第一装置也可以是车辆或者车载装置。第一装置例如能够设为基于认证了用户的结果来控制车辆的点火、主电源的装置。在该情况下,例如能够以车辆的发动机启动或者电源接通为触发,生成对第二装置的动作指令。同样地,能够以车辆的发动机停止或者系统关机为触发,生成对第二装置的动作指令。

[0153] 而且,也可以追加用于生成对第二装置的动作指令的进一步的条件。例如,也可以在进行了用户的认证的车辆离开预定的地点的情况下,生成动作指令。由此,例如在车辆从自家出发了的情况下,能够将自家的安全装置切换为警戒模式。

[0154] 另外,在实施方式的说明中,服务器装置100从便携终端200接收到实际结果数据,但只要能够获取表示使用电子钥匙进行了认证的意思的数据,该数据的发送源就也可以不是便携终端。例如,也可以是第二装置生成并发送实际结果数据。

[0155] 另外,在实施方式的说明中,将第二装置设为单个的装置,但也可以指定多个装置作为第二装置。例如,也可以指定设于住宅的正门的上锁开锁装置和家用安全装置这两者作为第二装置。在该情况下,能够与第一装置联动地,例如进行“正门的上锁开锁”和“安全模式的切换”这两者。

[0156] 另外,作为1个装置所进行的处理而说明的处理也可以由多个装置分担执行。或者,作为不同的装置所进行的处理而说明的处理也可以由1个装置执行。在计算机系统中,能够灵活地变更由怎样的硬件结构(服务器结构)实现各功能。

[0157] 本公开也能够通过向计算机提供安装有在上述实施方式中说明的功能的计算机程序并且该计算机所具有的1个以上的处理器读取并执行程序来实现。这样的计算机程序既可以利用能够与计算机的系统总线连接的非临时性计算机可读存储介质向计算机提供,也可以经由网络向计算机提供。非临时性计算机可读存储介质例如包括磁盘(软(注册商标)盘、硬盘驱动器(HDD)等)、光盘(CD-ROM、DVD盘·蓝光盘等)等任意类型的盘、只读存储器(ROM)、随机存取存储器(RAM)、EPROM、EEPROM、磁卡、闪速存储器、光卡、适于储存电子命令的任意类型的介质。

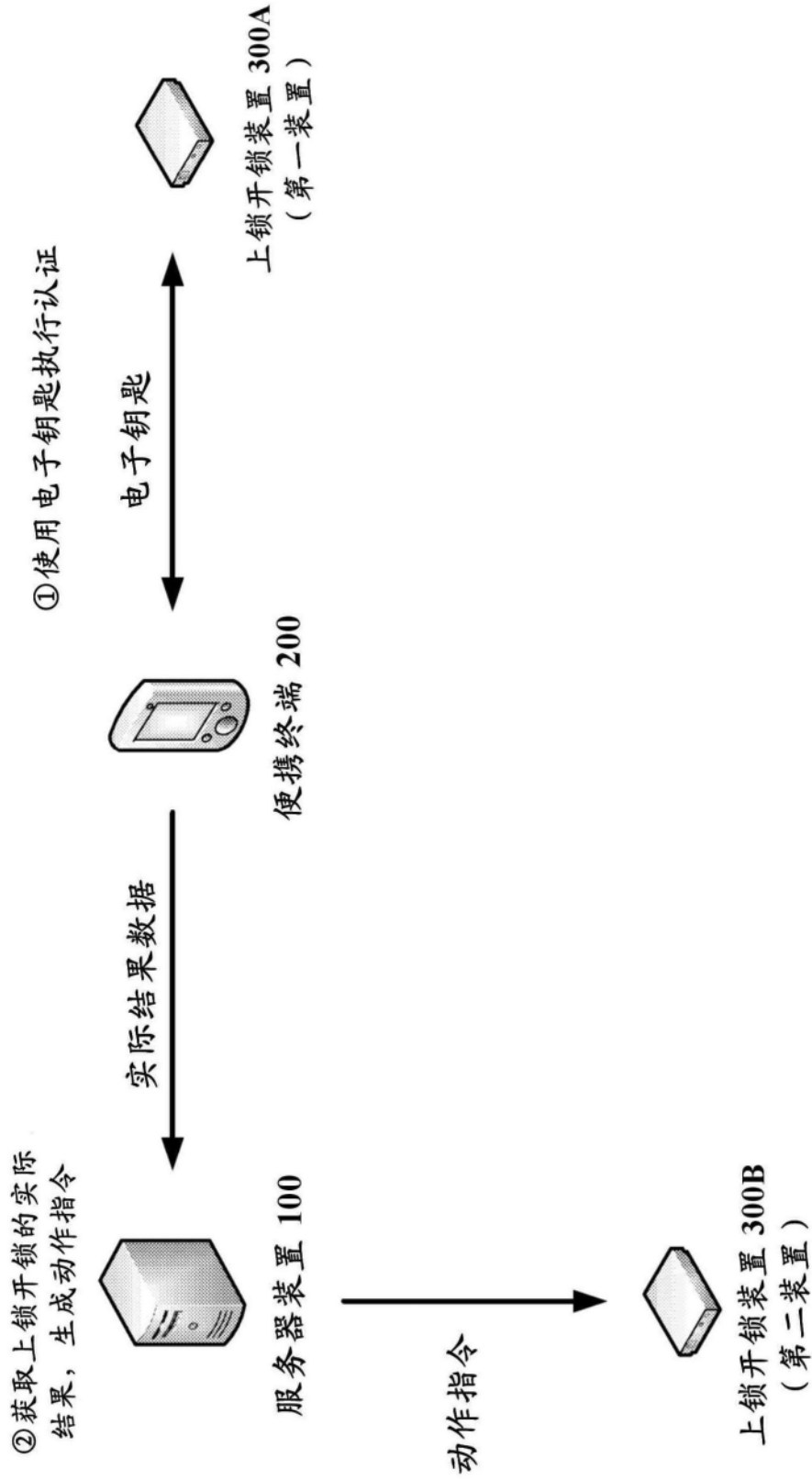


图1

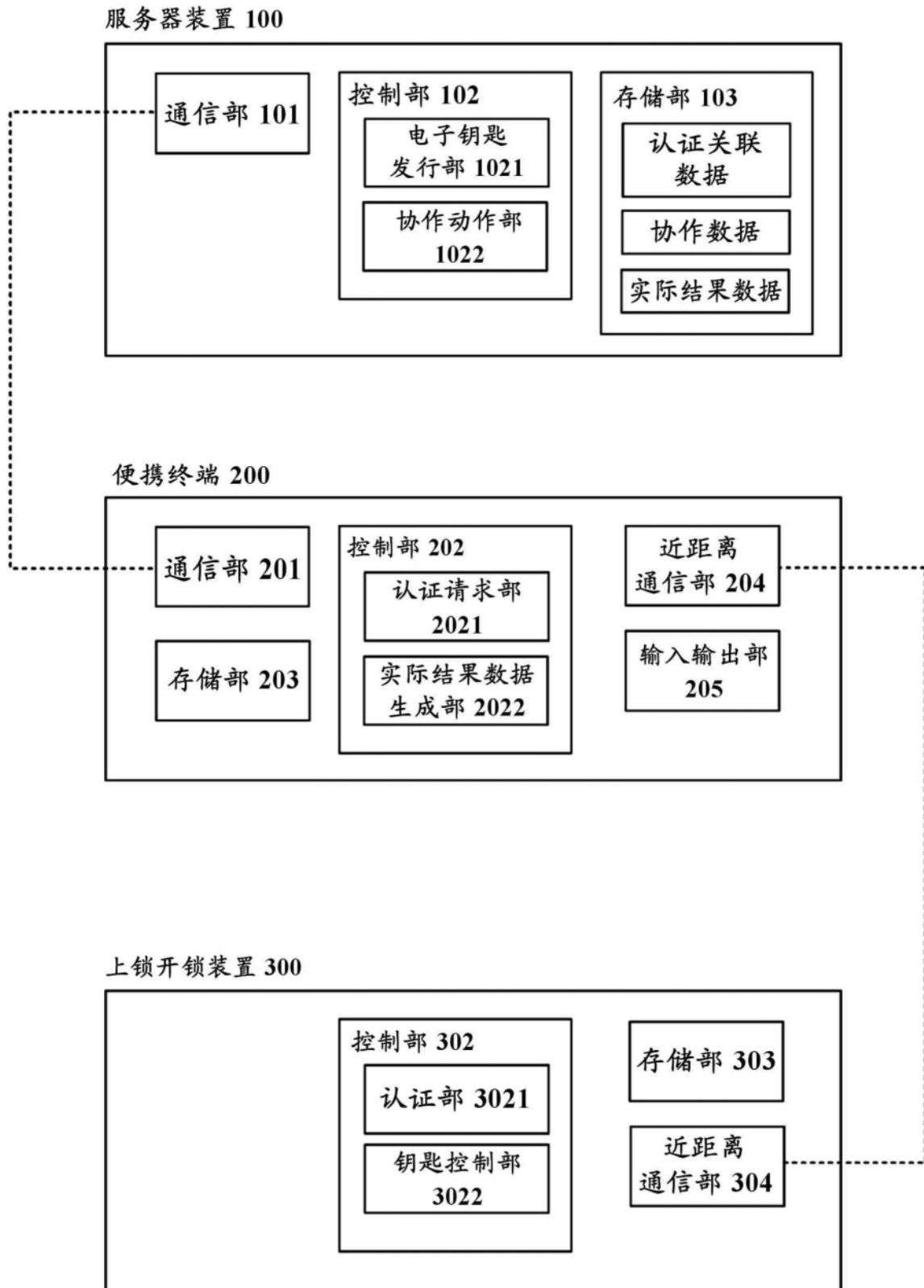


图2

钥匙数据

| 上锁开锁装置 ID | 名称 | 电子钥匙数据 |
|-----------|--------|--------|
| L001 | 自家正门 | (二进制) |
| L002 | 客车 | (二进制) |
| L003 | 工作单位正门 | (二进制) |
| L004 | 家用储物柜 | (二进制) |
| ... | ... | ... |
| | | |

图3

实际结果数据

| 日期和时间 | 便携终端 | 第一装置 | 动作 |
|-------|------|------|-----|
| ... | T001 | D001 | 上锁 |
| ... | T001 | D001 | 开锁 |
| ... | T001 | D001 | 上锁 |
| ... | T001 | D001 | 开锁 |
| ... | T001 | ... | ... |
| | | | |

图4

协作数据

| 便携终端 | 第一装置 | 动作 | 第二装置 | 动作指令 |
|------|------------|----|------------|---------|
| T001 | D001(自家正门) | 上锁 | D002(车辆) | 开锁 |
| T001 | D002(车辆) | 上锁 | D001(自家正门) | 开锁 |
| T002 | D003(车辆) | 开锁 | D004(安全装置) | 切换为警戒模式 |
| T002 | D003(车辆) | 上锁 | D004(安全装置) | 切换为在家模式 |

501 502

图5

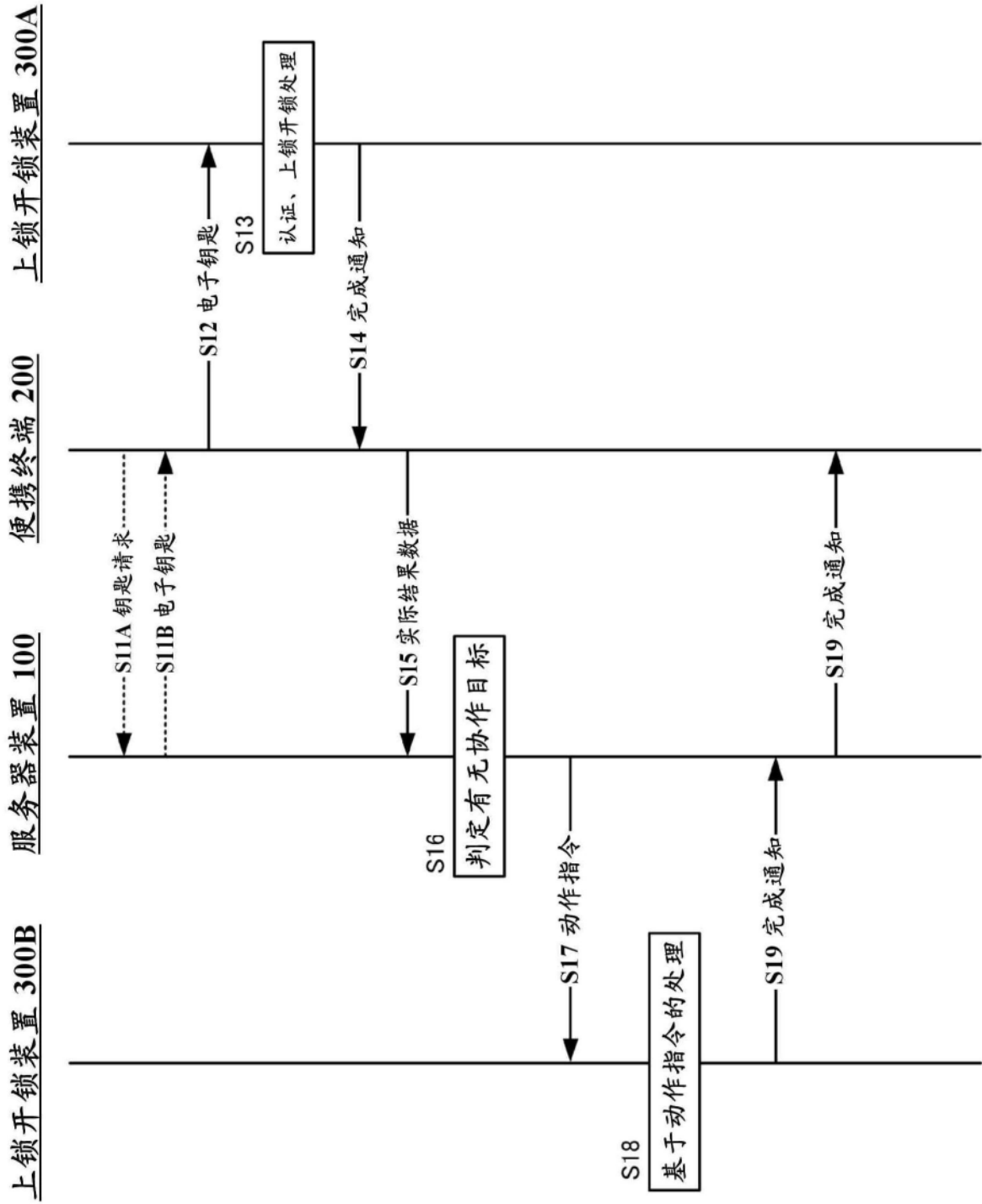


图6

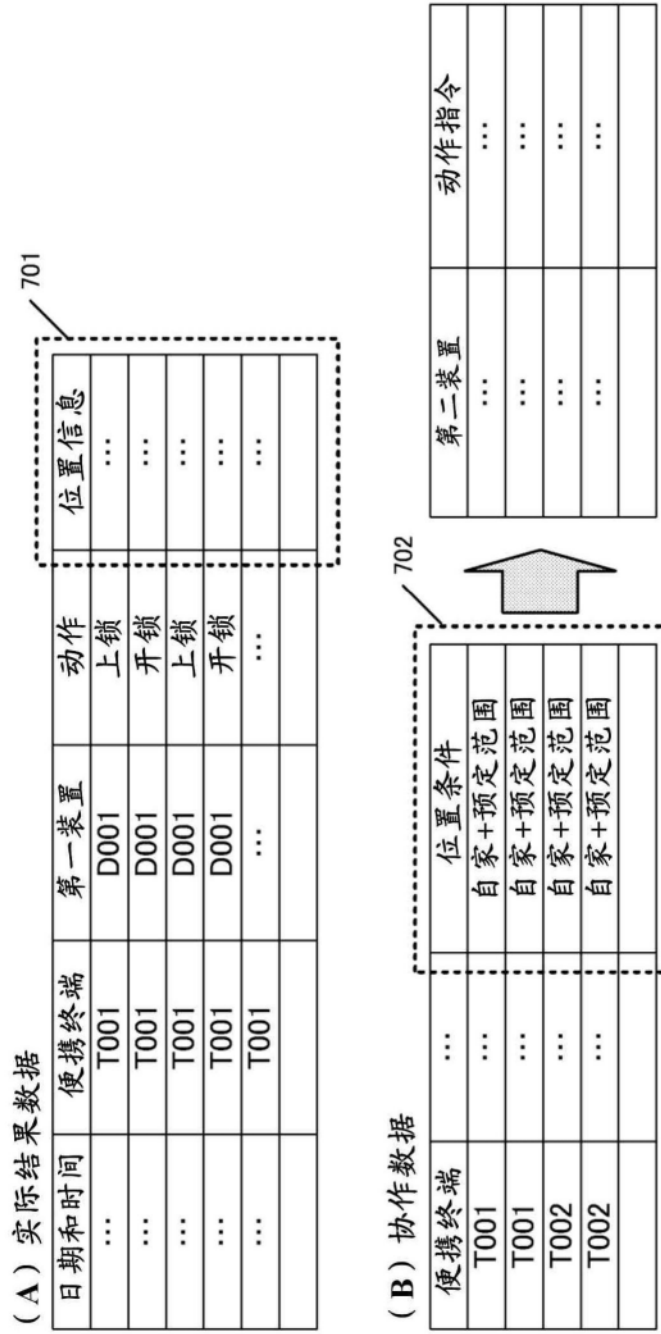


图7

安全装置 400

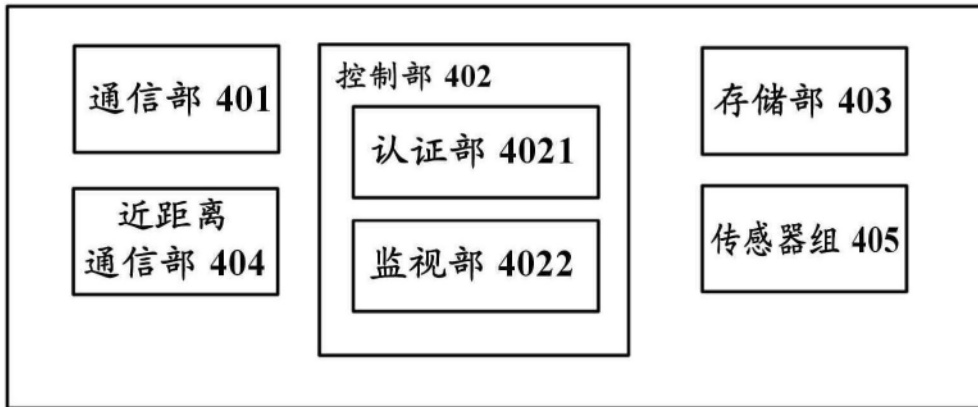


图8