



(12)发明专利申请

(10)申请公布号 CN 107925576 A

(43)申请公布日 2018.04.17

(21)申请号 201680049899.3

(74)专利代理机构 北京林达刘知识产权代理事

(22)申请日 2016.08.04

务所(普通合伙) 11277

(30)优先权数据

代理人 刘新宇

2015-170760 2015.08.31 JP

(51)Int.Cl.

H04L 9/14(2006.01)

(85)PCT国际申请进入国家阶段日

G06F 21/44(2006.01)

2018.02.26

H04L 9/08(2006.01)

(86)PCT国际申请的申请数据

H04L 9/32(2006.01)

PCT/JP2016/003595 2016.08.04

(87)PCT国际申请的公布数据

W02017/038009 JA 2017.03.09

(71)申请人 松下知识产权经营株式会社

地址 日本大阪府

(72)发明人 高添智树 增田洋一 松岛秀树

海上勇二

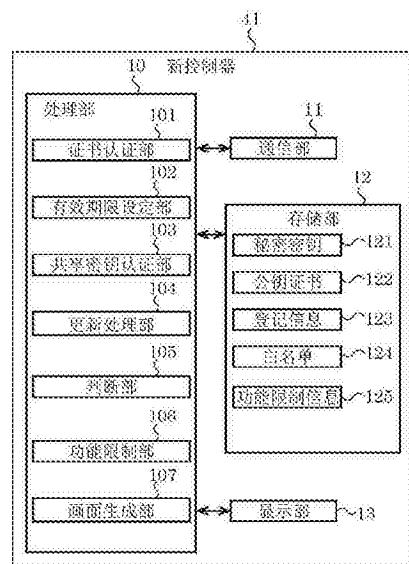
权利要求书2页 说明书12页 附图13页

(54)发明名称

控制器、通信方法、以及通信系统

(57)摘要

新控制器(对应于设备认证)(41)是，与利用电子证书而相互认证成功的设备进行加密通信的控制器，具备：判断部(105)，判断通信对象的设备是否是与相互认证对应的认证对应设备；功能限制部(106)，在由判断部(105)判断为不是认证对应设备的情况下，对该通信对象的设备具有的功能之中的、能够由新控制器(对应于设备认证)(41)操作的功能进行限制；以及通信部(11)，在由功能限制部(106)的功能限制之下与通信对象的设备以明文进行通信。



1. 一种控制器，与利用电子证书而相互认证成功的设备进行加密通信，所述控制器，具备：

判断部，判断通信对象的设备是否是与所述相互认证对应的认证对应设备；

功能限制部，在由所述判断部判断为不是所述认证对应设备的情况下，对所述通信对象的设备具有的功能之中的、能够由该控制器操作的功能进行限制；以及

通信部，在由所述功能限制部的功能限制之下与所述通信对象的设备以明文进行通信。

2. 如权利要求1所述的控制器，

所述判断部，在判断为所述通信对象的设备不是所述认证对应设备的情况下，进一步，判断所述通信对象的设备是符合允许列表的允许设备还是不符合所述允许列表的非允许设备，

在由所述判断部判断为是所述允许设备的情况下，与判断为是所述非允许设备的情况相比，所述功能限制部的功能限制少。

3. 如权利要求2所述的控制器，

在由所述判断部判断为是所述非允许设备的情况下，所述功能限制部，仅允许工作状态以及设定信息的获得命令。

4. 如权利要求2所述的控制器，

在由所述判断部判断为是所述允许设备的情况下，所述功能限制部，除了允许工作状态以及设定信息的获得命令以外，还允许操作系统以及设定系统的命令，但是，不允许收费及隐私有关的信息的获得以及运转工作状态的设定及变更。

5. 如权利要求1至4的任一项所述的控制器，

进一步，在由所述判断部判断为不是所述认证对应设备的情况下，为了向用户询问是否允许与所述通信对象的设备连接，而使与该控制器能够通信的显示部显示确认画面。

6. 如权利要求1至5的任一项所述的控制器，

进一步，为了变更由所述功能限制部的功能限制，而使与该控制器能够通信的显示部显示确认画面。

7. 如权利要求1至6的任一项所述的控制器，

所述判断部，在所述相互认证的开始时接收依据ECHONET的数据包的情况下，判断为不是所述认证对应设备。

8. 一种通信方法，该通信方法是控制器与利用电子证书而相互认证成功的设备进行加密通信时的通信方法，包括：

判断步骤，所述控制器判断通信对象的设备是否是与所述相互认证对应的认证对应设备；

功能限制步骤，在所述判断步骤中所述控制器判断为不是所述认证对应设备的情况下，对所述通信对象的设备具有的功能之中的、能够由该控制器操作的功能进行限制；以及

通信步骤，所述控制器在所述功能限制步骤中的功能限制之下与所述通信对象的设备以明文进行通信。

9. 如权利要求8所述的通信方法，

所述通信方法还包括显示步骤，

在所述显示步骤中，在所述判断步骤中判断为不是所述认证对应设备的情况下，为了向用户询问是否允许与所述通信对象的设备连接，而使与该控制器能够通信的显示部显示确认画面。

10. 如权利要求8或9所述的通信方法，

所述通信方法还包括显示步骤，

在所述显示步骤中，为了变更所述功能限制步骤中的功能限制，而使与该控制器能够通信的显示部显示确认画面。

11. 一种通信系统，该通信系统是控制器与利用电子证书而相互认证成功的设备进行加密通信的通信系统，

所述控制器，具备：

判断部，判断通信对象的设备是否是与所述相互认证对应的认证对应设备；

功能限制部，在由所述判断部判断为不是所述认证对应设备的情况下，对所述通信对象的设备具有的功能之中的、能够由该控制器操作的功能进行限制；以及

通信部，在由所述功能限制部的功能限制之下与所述通信对象的设备以明文进行通信。

## 控制器、通信方法、以及通信系统

### 技术领域

[0001] 本发明涉及,与利用电子证书而相互认证成功的设备进行加密通信的控制器、通信方法、以及通信系统。

### 背景技术

[0002] 近几年,会有如下情况,即,将家庭区域网与控制器连接,经由控制器进行设备与外部的服务器之间的通信(例如参照专利文献1)。于是,需要安全设定控制器与各个设备的连接,从而对家庭内的通信进行控制,防止基于非法设备的冒充的连接、或基于通信内容的旁听的信息泄漏等。

[0003] 例如,在利用证书局发行的公钥证书(电子证书),设备彼此进行相互认证的认证系统中,在各个设备第一次登记时,利用公钥证书生成共享密钥,利用该共享密钥简化以后的认证的技术被周知(例如参照专利文献2)。

[0004] (现有技术文献)

[0005] (专利文献)

[0006] 专利文献1:日本特开2014-217073号公报

[0007] 专利文献2:日本特开2004-247799号公报

[0008] 而且,在实际运用时,存在与所述的利用电子证书的相互认证(以下,称为“设备认证”。)对应的设备和不对应的设备混在一起的环境。即使在这样的环境下,也需要安全地操作不与设备认证对应的设备。

### 发明内容

[0009] 鉴于所述问题点,本发明的目的在于,提供即使在与设备认证对应的设备以及不对应的设备混在一起的环境下,也能够安全地操作不与设备认证对应的设备的控制器、通信方法、以及通信系统。

[0010] 为了实现所述目的,本发明的第一实施方案涉及的控制器的宗旨是,与利用电子证书而相互认证成功的设备进行加密通信的控制器,具备:判断部,判断通信对象的设备是否是与所述相互认证对应的认证对应设备;功能限制部,在由所述判断部判断为不是所述认证对应设备的情况下,对所述通信对象的设备具有的功能之中的、能够由该控制器操作的功能进行限制;以及通信部,在由所述功能限制部的功能限制之下与所述通信对象的设备以明文进行通信。

[0011] 本发明的第二实施方案涉及的通信方法的宗旨是,该通信方法是控制器与利用电子证书而相互认证成功的设备进行加密通信时的通信方法,包括:判断步骤,所述控制器判断通信对象的设备是否是与所述相互认证对应的认证对应设备;功能限制步骤,在所述判断步骤中所述控制器判断为不是所述认证对应设备的情况下,对所述通信对象的设备具有的功能之中的、能够由该控制器操作的功能进行限制;以及通信步骤,所述控制器在所述功能限制步骤中的功能限制之下与所述通信对象的设备以明文进行通信。

[0012] 本发明的第三实施方案涉及的通信方法的宗旨是，该通信系统是控制器与利用电子证书而相互认证成功的设备进行加密通信的通信系统，所述控制器，具备：判断部，判断通信对象的设备是否是与所述相互认证对应的认证对应设备；功能限制部，在由所述判断部判断为不是所述认证对应设备的情况下，对所述通信对象的设备具有的功能之中的、能够由该控制器操作的功能进行限制；以及通信部，在由所述功能限制部的功能限制之下与所述通信对象的设备以明文进行通信。

[0013] 根据本发明，能够提供即使在与设备认证对应的设备以及不对应的设备混在一起的环境下，也能够安全地操作不与设备认证对应的设备的控制器、通信方法、以及通信系统。

## 附图说明

- [0014] 图1是说明本发明的实施例涉及的认证系统的基本结构的框图。
- [0015] 图2是说明本发明的实施例涉及的认证系统具备的控制器的基本结构的框图。
- [0016] 图3是说明本发明的实施例涉及的用于认证系统的公钥证书的基本数据结构的框图。
- [0017] 图4是说明本发明的实施例涉及的用于认证系统的登记信息的基本数据结构的框图。
- [0018] 图5是说明本发明的实施例涉及的认证系统具备的设备的基本结构的框图。
- [0019] 图6是说明本发明的实施例涉及的用于认证系统的登记信息的基本数据结构的框图。
- [0020] 图7是说明本发明的实施例涉及的说明认证系统的工作的序列图。
- [0021] 图8是说明本发明的实施例涉及的认证系统的利用公钥证书的相互认证的处理的序列图。
- [0022] 图9是说明本发明的实施例涉及的认证系统的利用共享密钥的相互认证的处理的序列图。
- [0023] 图10是说明本发明的实施例涉及的认证系统的公钥证书的更新的处理的序列图。
- [0024] 图11是用于说明本发明的实施例涉及的通信系统中需要对应遗留设备的情况的概念图。
- [0025] 图12是说明本发明的实施例涉及的通信系统具备的新控制器(对应于设备认证)的基本结构的框图。
- [0026] 图13是示出本发明的实施例涉及的通信系统具备的新控制器(对应于设备认证)与其他的设备的连接例的框图。
- [0027] 图14是示出本发明的实施例涉及的通信系统具备的新控制器(对应于设备认证)的工作的流程图。
- [0028] 图15是示出本发明的实施例涉及的通信系统具备的新控制器(对应于设备认证)的显示部显示的画面例的图。
- [0029] 图16是示出本发明的实施例涉及的通信系统具备的新控制器(对应于设备认证)的显示部显示的其他的画面例的图。
- [0030] 图17是示出本发明的实施例涉及的通信系统具备的新控制器(对应于设备认证)

的存储部存储的功能限制信息的一个例子的图。

## 具体实施方式

[0031] 以下,对于本实施例涉及的控制器等,参照附图进行说明。而且,以下说明的实施例,都示出本发明的优选的一个具体例子。因此,以下的实施例示出的数值、形状、材料、构成要素、构成要素的配置及连接形态、以及工序(步骤)及工序的顺序等是一个例子而不是限定本发明的宗旨。因此,对于以下的实施例的构成要素中的、示出本发明的最上位概念的实施方案中没有记载的构成要素,作为任意的构成要素而被说明。而且,各个图是模式图,并不一定是严密示出的图。

[0032] 在以下的附图的记载中,相同或类似的部分附上相同或类似的符号,也有省略重复说明的部分。

[0033] (实施例)

[0034] 《基本结构》

[0035] 对于本实施例涉及的通信系统,以下述认证系统为前提进行说明。

[0036] (认证系统)

[0037] 本实施例涉及的认证系统,如图1示出,具备:控制器1;多个设备2;以及经由作为通信线路的互联网3,与控制器1可通信地连接的服务器4。服务器4是,针对控制器1以及多个设备2发行公钥证书,管理发行的公钥证书的证书局。

[0038] 控制器1(第一设备)是,例如,管理多个设备2的使用电力量、发电剩余电力量等的家庭能源管理系统(HEMS)中的控制器。控制器1是,与多个设备2可通信地连接的通信设备。控制器1,与多个设备2进行相互认证来登记多个设备2,从而与多个设备2构成HEMS5。

[0039] 控制器1,如图2示出,具备,处理部10、按照处理部10的控制与其他进行的通信部11、以及存储程序以及各种数据等的信息的存储部12。通信部11进行的通信,也可以是无线通信,也可以是有线通信。存储部12,存储控制器1本身的秘密密钥121及公钥证书122、以及作为与已经登记的设备2有关的信息的登记信息123。

[0040] 公钥证书122,如图3示出,包括,公钥证书122的版本、发行者、有效期间的开始时、有效期间的结束时(有效期限)、证书ID(标识符)、控制器1的公钥、以及服务器4的签名。公钥证书122的公钥,与秘密密钥121对应。公钥证书122的签名,利用服务器4的秘密密钥而被制作。公钥证书122,由服务器4发行,在控制器1的制造时由存储部12存储。

[0041] 登记信息123,如图4示出,包括,识别已经登记的设备2的设备ID、识别各个设备2的公钥证书222(参照图6)的证书ID、共享密钥(事先共享密钥)、群组密钥、会话密钥、以及会话剩余时间。共享密钥,在控制器1与各个设备2之间分别被共享。群组密钥,用于控制器1向各个设备2一并发送的信息的加密以及解密。属于同一小组的设备2,与控制器1共享同一群组密钥。会话密钥,用于控制器1与各个设备2之间的单播通信的加密以及解密。会话剩余时间,是在控制器1与各个设备2之间设定的、会话有效的剩余时间。

[0042] 处理部10包括,证书认证部101、有效期限设定部102、共享密钥认证部103、以及更新处理部104,以作为逻辑结构。处理部10,由中央运算装置(CPU)等的处理装置构成。

[0043] 证书认证部101,利用公钥证书122以及作为认证的对象设备的设备2的公钥证书222,与设备2进行相互认证,从而生成与设备2共享的共享密钥。有效期限设定部102,将公

钥证书122以及公钥证书222的任一个的有效期限,设定到证书认证部101生成的共享密钥中。

[0044] 共享密钥认证部103,在没有超过共享密钥中设定的有效期限的情况下,不利用公钥证书122以及公钥证书222,而利用证书认证部101生成的共享密钥,与设备2进行相互认证。更新处理部104,在超过共享密钥中设定的有效期限的情况下,将公钥证书122更新为新的公钥证书122。

[0045] 设备2(第二设备),例如,由空调、冰箱、照明装置等的负载设备、太阳电池、蓄电池等的电源设备、以及智能仪表等分别构成。设备2是,由控制器1登记来加入到HEMS5,与控制器1进行加密通信的通信设备。设备2也可以是,具有控制功能、管理功能等的与控制器1同等的设备。而且,在具有管理功能的设备在同一网络上存在多个的情况下,仅先连接的设备体现管理功能,以后连接的设备不体现管理功能。

[0046] 各个设备2,如图5示出,具备,处理部20、按照处理部20的控制与控制器1进行通信的通信部21、以及存储程序以及各种数据的存储部22。通信部21进行的通信,也可以是无线通信,也可以是有线通信。存储部22,存储设备2本身的秘密密钥221及公钥证书222、以及作为与设备2本身被登记的控制器1有关的信息的登记信息223。

[0047] 公钥证书222,与公钥证书122同样,包括,公钥证书222的版本、发行者、有效期间的开始时、有效期间的结束时(有效期限)、证书ID(标识符)、设备2的公钥、以及服务器4的签名。公钥证书222的公钥,与秘密密钥221对应。公钥证书222的签名,利用服务器4的秘密密钥而被制作。公钥证书222,由服务器4发行,在设备2的制造时由存储部22存储。

[0048] 登记信息223,如图6示出,包括,识别设备2本身被登记的控制器1的控制器ID、识别控制器1的公钥证书122的证书ID、共享密钥、群组密钥、会话密钥、以及会话剩余时间。共享密钥,在控制器1与各个设备2之间被共享。群组密钥,用于控制器1向各个设备2一并发送的信息的加密以及解密。会话密钥,用于与控制器1之间的单播通信的加密以及解密。会话剩余时间,是在与控制器1之间设定的、会话有效的剩余时间。

[0049] 处理部20具有,证书认证部201、有效期限设定部202、共享密钥认证部203、以及更新处理部204,以作为逻辑结构。处理部20,由CPU等的处理装置构成。

[0050] 证书认证部201,利用公钥证书222以及作为认证的对象设备的控制器1的公钥证书122,与控制器1进行相互认证,从而生成与控制器1共享的共享密钥。有效期限设定部202,将公钥证书222以及公钥证书122的任一个的有效期限,设定到证书认证部201生成的共享密钥中。

[0051] 共享密钥认证部203,在没有超过共享密钥中设定的有效期限的情况下,不利用公钥证书222以及公钥证书122,而利用证书认证部201生成的共享密钥,与设备2进行相互认证。更新处理部204,在超过共享密钥中设定的有效期限的情况下,将公钥证书222更新为新的公钥证书222。

[0052] (认证方法)

[0053] 参照图7的序列图,说明本实施例涉及的认证系统的认证方法。

[0054] 首先,在步骤S1中,设备2的证书认证部201,经由通信部21,将请求利用公钥证书的认证的认证请求、自己的设备ID以及公钥证书222发送到控制器1。控制器1的通信部11,接收步骤S1中从设备2发送的认证请求、设备ID以及公钥证书222。

[0055] 在步骤S2中,控制器1的证书认证部101,按照经由通信部11获得的认证请求,与证书认证部201一起,进行利用公钥证书122以及公钥证书222的相互认证。步骤S2中的相互认证是,基于公钥基础(PKI)的相互认证。

[0056] 证书认证部101以及证书认证部201,确认彼此的公钥证书的合法性,相互认证成功,从而通过密钥交换方式生成共享密钥。有效期限设定部102以及有效期限设定部202,由证书认证部101以及证书认证部201,在由控制器1以及设备2共享的共享密钥中,设定公钥证书122以及公钥证书222的任一个的有效期限。而且,证书认证部101以及证书认证部201,在利用公钥证书的相互认证失败的情况下,结束处理。

[0057] 在步骤S3中,共享密钥认证部103以及共享密钥认证部203,在没有超过控制器1以及设备2所共享的共享密钥中设定的有效期限的情况下,不利用公钥证书122以及公钥证书222,而利用共享密钥,进行相互认证。共享密钥认证部103以及共享密钥认证部203,确认彼此的共享密钥的合法性,相互认证成功,据此,在需要时,设定群组密钥、会话密钥以及会话有效期间等。而且,共享密钥认证部103以及共享密钥认证部203,在利用共享密钥的相互认证失败的情况下,结束处理。

[0058] 在步骤S4中,共享密钥认证部203,将共享密钥、设定的群组密钥、会话密钥以及会话有效期间等,与控制器1的控制器ID以及公钥证书122的证书ID建立关联,作为登记信息223登记。

[0059] 在步骤S5中,共享密钥认证部103,将控制器1的控制器ID及公钥证书122的证书ID、以及设备2的设备ID及公钥证书222的证书ID,经由通信部11发送到服务器4。此时通信部11,与服务器4进行SSL(Secure Socket Layer)通信。

[0060] 在步骤S6中,共享密钥认证部103,将共享密钥、设定的群组密钥、会话密钥以及会话有效期间等,与设备2的设备以及公钥证书222的证书ID建立关联,作为登记信息223登记。

[0061] 在步骤S7中,服务器4,接收步骤S5中发送的控制器1的控制器ID及公钥证书122的证书ID、以及设备2的设备ID及公钥证书222的证书ID,作为认证的通信设备登记。而且,也可以省略步骤S5和步骤S7的工作。

[0062] (利用公钥证书的相互认证)

[0063] 参照图8的序列图,说明图7的序列图的步骤S2中的利用公钥证书的相互认证的处理的一个例子。

[0064] 在步骤S1中,证书认证部101,根据证书吊销列表(CRL)等,验证从设备2发送的公钥证书222的有效性。另外,证书认证部101,验证公钥证书222的有效期限。证书认证部101,在确认公钥证书222有效的情况下,进行步骤S22的处理,在判断为失效的情况下,结束处理。

[0065] 在步骤S22中,证书认证部101,利用服务器4的公钥,验证公钥证书222的签名。证书认证部101,在确认公钥证书222的签名为合法的情况下,进行步骤S23的处理,在判断为失效的情况下,结束处理。

[0066] 在步骤S23中,证书认证部101,经由通信部11,将控制器1的控制器ID以及公钥证书122,发送到发送了认证请求的设备2。设备2的证书认证部201,经由通信部21获得,从控制器1发送的控制器ID以及公钥证书122。

[0067] 在步骤S24中,证书认证部201,根据CRL、有效期限等,验证公钥证书122的有效性。证书认证部201,在确认公钥证书222有效的情况下,进行步骤S25的处理,在判断为失效的情况下,结束处理。

[0068] 在步骤S25中,证书认证部201,利用服务器4的公钥,验证公钥证书122的签名。证书认证部201,在确认公钥证书122的签名为合法的情况下,进行步骤S26的处理,在判断为失效的情况下,结束处理。

[0069] 在步骤S26中,证书认证部201,将通知对公钥证书122的验证成功的成功通知,发送到控制器1。而且,对于步骤S21至步骤S26中的数字签名方式以及验证方法,也可以基于椭圆曲线数字签名算法(ECDSA)。

[0070] 在步骤S27以及S28中,证书认证部101以及证书认证部201,通过密钥交换方式,生成共享密钥。该密钥交换方式也可以是,椭圆曲线迪菲-赫尔曼密钥共享(ECDH)方式。并且,对于共享密钥,也可以利用高度加密标准(AES)的密钥长度128位,根据所述共享的值计算散列值,设为计算出的散列值的高128位。

[0071] 有效期限设定部102以及有效期限设定部202,在证书认证部101以及证书认证部201所生成的共享密钥中,设定公钥证书122以及公钥证书222的任一个的有效期限。有效期限设定部102以及有效期限设定部202,例如,将公钥证书122以及公钥证书222的有效期限之中的、短的有效期限,作为共享密钥的有效期限设定。存储部12以及存储部22,将共享密钥以及共享密钥中设定的有效期限彼此建立关联来存储。

[0072] (利用共享密钥的相互认证)

[0073] 参照图9的序列图,说明图7的序列图的步骤S3中的利用共享密钥的相互认证的处理的一个例子。利用共享密钥的相互认证是,通过挑战应答认证方式进行的。

[0074] 在步骤S301以及步骤S302中,共享密钥认证部103以及共享密钥认证部203,确认共享密钥中设定的有效期限。在规定的定时进行有效期限的确认。例如,也可以在控制器1和设备2的通信的会话更新时进行有效期限的确认。

[0075] 在超过共享密钥的有效期限的情况下,证书认证部101,停止当前的处理,等待来自设备2的新的认证请求。或者,证书认证部101也可以,利用当前的公钥证书122,向设备2发送新的认证请求。共享密钥认证部103,在没有超过有效期限的情况下,进行步骤S303的处理。在步骤S303中,共享密钥认证部103,生成任意的随机数A,经由通信部11发送到设备2。

[0076] 在步骤S304中,共享密钥认证部203,将从控制器1发送的、经由通信部21获得的随机数A,利用共享密钥加密,计算加密随机数a。并且,共享密钥认证部203,生成任意的随机数B。在步骤S305中,共享密钥认证部203,将计算出的加密随机数a以及生成的随机数B,经由通信部21发送到控制器1。

[0077] 在步骤S306中,共享密钥认证部103,经由通信部11获得从设备2发送的加密随机数a以及随机数B,将加密随机数a,利用共享密钥解密。共享密钥认证部103,在解密结果与随机数A一致的情况下,设为对随机数A的验证成功,进行步骤S307的处理,在解密结果与随机数A不一致的情况下,结束处理。

[0078] 在步骤S307中,共享密钥认证部103,将从设备2发送的随机数B,利用共享密钥加密,计算加密随机数b。

[0079] 在步骤S308中,共享密钥认证部103,在需要时,生成群组密钥。群组密钥也可以是,例如AES的密钥长度128位。或者,共享密钥认证部103,参照登记信息123,获得已经生成的群组密钥。在步骤S309中,共享密钥认证部103,生成会话密钥。会话密钥也可以是,例如AES的密钥长度128位。

[0080] 在步骤S310中,共享密钥认证部103,设定规定的会话有效期间(例如24小时,72小时等)。在步骤S311中,共享密钥认证部103,将步骤S308以及步骤S309中获得的群组密钥以及会话密钥,利用共享密钥加密。而且,步骤S308至步骤S311的处理是,在为了通信而需要群组密钥以及会话密钥的生成时进行的处理,能够省略。

[0081] 在步骤S312中,共享密钥认证部103,将加密随机数b、加密的群组密钥以及会话密钥、会话有效期间,经由通信部11发送到设备2。设备2的通信部21,接收从控制器1发送的加密随机数b、加密的群组密钥以及会话密钥、会话有效期间。

[0082] 在步骤S313中,共享密钥认证部203,将从通信部21获得的加密随机数b,利用共享密钥解密。共享密钥认证部203,在解密结果与随机数B一致的情况下,设为对随机数B的验证成功,进行步骤S314的处理,在解密结果与随机数B不一致的情况下,结束处理。

[0083] 在步骤S314中,共享密钥认证部203,将加密的群组密钥以及会话密钥,利用共享密钥解密。并且,在步骤S315中,将通知对随机数B的验证成功的成功通知,发送到控制器1。

[0084] (超过有效期限时的处理)

[0085] 参照图10的序列图,说明图9的序列图的步骤S301以及步骤S302中,共享密钥的有效期限的确认结果为,超过有效期限时的其他的处理的一个例子。

[0086] 在步骤S11中,更新处理部104,生成新的秘密密钥121以及与新的秘密密钥121对应的新的公钥。在步骤S12中,更新处理部104,将生成的新的公钥,经由通信部11发送到服务器4。

[0087] 在步骤S13中,服务器4,接收步骤S12中发送的公钥,公钥中添加服务器4的签名等,发行新的公钥证书122。在步骤S14中,服务器4,将新的公钥证书122发送到控制器1。

[0088] 在步骤S15中,更新处理部104,接收步骤S14中发送的新的公钥证书122,将存储部12中已经存储的公钥证书122置换为新的公钥证书122并存储。如此,控制器1能够,利用有效的新的公钥证书122与设备2进行相互认证,生成设定了新的有效期限的共享密钥。

[0089] 根据本实施例涉及的认证系统,将公钥证书122或公钥证书222的有效期限设定到共享密钥中,从而能够考虑公钥证书的有效期限,进行基于共享密钥的相互认证,能够提高通信的安全性以及可靠性。

[0090] 并且,根据本实施例涉及的认证系统,将公钥证书122以及公钥证书222的有效期限之中的、短的期限设定到共享密钥中,从而能够更提高通信的安全性以及可靠性。

[0091] 并且,根据本实施例涉及的认证系统,每当更新会话时进行有效期限的确认,从而能够提高检测不是有效的共享密钥的效率,能够更提高通信的安全性以及可靠性。

[0092] 《向遗留设备的对应》

[0093] 而且,在实际运用时,存在与所述的利用电子证书的相互认证(以下,称为“设备认证”。)对应的设备和不对应的设备混在一起的环境。即使在这样的环境下,也需要安全地操作不与设备认证对应的设备。

[0094] 以下,说明本实施例涉及的通信系统。在以下的说明中,将与设备认证对应的设备

称为“认证对应设备”，将不与设备认证对应的设备称为“遗留设备”。设备认证是，《基本结构》中说明那样的。

[0095] (通信系统)

[0096] 图11是用于说明本实施例涉及的通信系统中需要对应遗留设备的情况的概念图。在此设想为，如图11的左边示出，仅由控制器(遗留)31、设备(遗留)32、以及媒体转换器(遗留)33等的遗留设备构成通信系统的情况。

[0097] 在这样的通信系统中，情况1示出，新导入新设备(对应于设备认证)42的情况。禁止由控制器(遗留)31操作新设备(对应于设备认证)42，因此，存在不能操作新导入的新设备(对应于设备认证)42的问题。作为该问题的对策，可以考虑对控制器(遗留)31进行固件升级或交换。

[0098] 接着，情况2示出，新导入新控制器(对应于设备认证)41的情况。新控制器(对应于设备认证)41，与设备认证对应，但是，设备(遗留)32等的遗留设备，不与设备认证对应。因此，新控制器(对应于设备认证)41和设备(遗留)32的相互认证会失败。也就是说，存在不能由新导入的新控制器(对应于设备认证)41操作遗留设备的问题。作为该问题的对策，可以考虑有条件地容许由新控制器(对应于设备认证)41操作遗留设备(后述)。

[0099] 最后，情况3示出，新导入新设备(对应于设备认证)42和新控制器(对应于设备认证)41的情况。即使该情况3，只要设备(遗留)32等的遗留设备混在一起，就存在与情况2同样的问题。

[0100] (新控制器)

[0101] 图12是说明本实施例涉及的通信系统具备的新控制器(对应于设备认证)41的基本结构的框图。新控制器(对应于设备认证)41是，与利用电子证书而相互认证成功的设备进行加密通信的控制器，如图12示出，具备处理部10、通信部11、存储部12、以及显示部13。处理部10包括，判断部105、功能限制部106、以及画面生成部107。存储部12包括，白名单124、以及功能限制信息125。

[0102] 判断部105，判断通信对象的设备是否是认证对应设备。功能限制部106，在判断部105判断为不是认证对应设备的情况下，对该通信对象的设备具有的功能之中的、能够由新控制器(对应于设备认证)41操作的功能进行限制。通信部11，在由功能限制部106的功能限制之下，以明文与通信对象的设备进行通信。据此，能够将新控制器(对应于设备认证)41与遗留设备连接，有条件地容许由新控制器(对应于设备认证)41操作遗留设备。

[0103] 画面生成部107，生成各种画面。显示部13是，由画面生成部107显示生成的各种画面的显示装置。白名单124是，列举与符合AIF等的特定的标准的设备有关的信息(制造厂，型号等)的允许列表。功能限制信息125是，按照阶段性的安全级别规定不同强度的功能限制的信息，由功能限制部106参照。其他的各个处理部是，所述《基本结构》中说明那样的。

[0104] 而且，新控制器(对应于设备认证)41和显示部13也可以没有形成为一体。也就是说，显示部13是，能够与新控制器(对应于设备认证)41进行通信的显示装置即可，例如，也可以是智能手机等的其他的终端设备。

[0105] (AIF)

[0106] 空调、照明、蓄电池、供给热水机、电动汽车充放电器、燃料电池、太阳光发电以及智能仪表，被视为HEMS中相互连接更重要的设备。AIF(Application Interface)是，对于这

样的重要的设备,为了提高相互连接性,而规定ECHONET-Lite的应用程序级的使用方法的说明书。

[0107] 也可以说,与AIF对应的设备,与依据通用的ECHONET-Lite标准的遗留设备相比,认证的功能高。因此,针对与AIF对应的设备的功能限制,与针对遗留设备的功能限制相比放宽。

[0108] 具体而言,判断部105,在判断为通信对象的设备不是认证对应设备的情况下,进一步,判断通信对象的设备是符合允许列表(白名单124)的允许设备还是不符合允许列表的非允许设备(遗留设备)。据此,在判断部105判断为是允许设备的情况下,与判断为是非允许设备的情况相比,能够减少功能限制。

[0109] (连接例)

[0110] 以下,说明新控制器(对应于设备认证)41的结构以及其工作。在此设想为,如图13示出,新设备(对应于设备认证)42、设备(对应于AIF)52、设备(遗留)32等的各种设备混在一起的环境。并且,设备认证是,将按钮按下作为触发来执行的。

[0111] 首先,用户按下新控制器(对应于设备认证)41和新设备(对应于设备认证)42的按钮。据此,新控制器(对应于设备认证)41,与新设备(对应于设备认证)42执行设备认证,从而判断是否是认证对应设备(图14,步骤S31→S32→S33)。而且,若从新设备(对应于设备认证)42接收设备ID以及公钥证书222等,则判断为是认证对应设备(图14,步骤S33:是)。在此判断为是认证对应设备的情况下,将安全级别判断为“3”(图14,步骤S34),按照通常与新设备(对应于设备认证)42连接。在此情况下,能够通过加密通信安全地连接。

[0112] 接着,用户按下新控制器(对应于设备认证)41和设备(对应于AIF)52的按钮。据此,新控制器(对应于设备认证)41,与设备(对应于AIF)52执行设备认证,从而判断是否是认证对应设备(图14,步骤S31→S32→S33)。而且,若从设备(对应于AIF)52接收明文,则判断为不是认证对应设备(图14,步骤S33:否)。也就是说,在相互认证的开始时接收明文(依据ECHONET的数据包)的情况下,判断为不是认证对应设备。在此判断为不是认证对应设备的情况下,进一步,判断是否是符合白名单124的允许设备(对应于AIF)(图14,步骤S35)。是否是对应于AIF的判断是,根据从设备(对应于AIF)52接收的依据ECHONET的数据包进行的。此时,若不能判断是否对应于AIF,则也可以从设备(对应于AIF)52还获得信息。设备(对应于AIF)52,符合白名单124,因此,判断为是允许设备(对应于AIF)(图14,步骤S35:是)。在此判断为是允许设备(对应于AIF)的情况下,将安全级别判断为“2”(图14,步骤S36),在用户确认之下与设备(对应于AIF)52连接。而且,在此情况下,也可以在功能限制的状态下与设备(对应于AIF)52连接。

[0113] 接着,用户按下新控制器(对应于设备认证)41和设备(遗留)32的按钮。据此,新控制器(对应于设备认证)41,与设备(遗留)32执行设备认证,判断是否是认证对应设备(图14,步骤S31→S32→S33)。而且,若从设备(遗留)32接收明文,则判断为不是认证对应设备(图14,步骤S33:否),进一步,判断是否是符合白名单124的允许设备(对应于AIF)(图14,步骤S35)。设备(遗留)32,不符合白名单124,因此,判断为不是允许设备(对应于AIF)(图14,步骤S35:否)。在此判断为不是允许设备(对应于AIF)的情况下,将安全级别判断为“1”(图14,步骤S37),在用户确认之下与设备(遗留)32连接。

[0114] 如上所述,在本实施例涉及的通信系统中,判断阶段性的安全级别,按照该阶段性

的安全级别施加不同强度的功能限制。据此,即使在与设备认证对应的设备以及不对应的设备混在一起的环境下,也能够安全地操作不与设备认证对应的设备。

[0115] 而且,在向设备(遗留)32以及设备(对应于AIF)52的连接期间(运用方面)中存在问题的情况下,也可以由新控制器(对应于设备认证)41切断连接。也就是说,即使在存在功能限制以及用户确认的情况下,在预先决定的期间不容许限制的情况下切断连接。据此,能够更安全地操作不与设备认证对应的设备。

[0116] (画面例)

[0117] 图15是示出新控制器(对应于设备认证)41的显示部13显示的画面例的图。如已经说明,在与设备(遗留)32以及设备(对应于AIF)52连接的情况下,向用户询问与这些设备的连接允许。例如,在设备(对应于AIF)52是空调B的情况下也可以,如图15示出,将“空调B不与新的连接方式对应。是否要连接伟003F伟”等的消息显示在显示部13,以使用户选择“是”或“否”。在该确认画面13A中选择“是”的情况下,与设备(对应于AIF)52进行通信。

[0118] 也就是说,设备(遗留)32以及设备(对应于AIF)52,不与设备认证对应,因此,从新控制器(对应于设备认证)41接收错误,或者,在一定时间后超时。即使在这样的情况下,也能够在新控制器(对应于设备认证)41的显示部13弹出确认画面13A,在由用户的确认之下,将设备(遗留)32以及设备(对应于AIF)52与新控制器(对应于设备认证)41连接。

[0119] 而且,在此,向用户询问连接允许,但是,确认画面,不仅限于此。例如,也可以将催促设备(遗留)32以及设备(对应于AIF)52的固件升级或交换的消息显示在显示部13。据此,在设备(遗留)32以及设备(对应于AIF)52被交换为新设备(对应于设备认证)42的情况下,能够通过加密通信更安全地连接。

[0120] 图16是示出新控制器(对应于设备认证)41的显示部13显示的其他的画面例的图。如该图示出,也可以将用于确认功能限制部106的功能限制的一览的确认画面13B显示在显示部13。这样的功能限制的一览是,能够根据功能限制信息125生成的。在此,示出按每个设备与“安全级别”“功能限制”“设备删除”对应的情况的例子。在该确认画面13B中,也可以由用户的责任变更“功能限制”(包括解除)。在用户变更“功能限制”的情况下,在该变更后的功能限制之下进行通信。

[0121] (功能限制信息)

[0122] 图17是示出新控制器(对应于设备认证)41的存储部12存储的功能限制信息的一个例子的图。该功能限制信息125是,按照阶段性的安全级别规定不同强度的功能限制的表。按空调、蓄电池、太阳光发电、以及即热式热水器等的每个设备,规定功能限制信息125。据此,新控制器(对应于设备认证)41,能够实现与各个设备的特性对应的功能限制。

[0123] 如图17示出,在安全级别1时为“有功能限制”,在安全级别2时为“有一部分功能限制”,在安全级别3时为“没有功能限制”。具体而言,在安全级别1的情况下,新控制器(对应于设备认证)41,仅允许基本的信息(工作状态以及设定信息)的获得命令。并且,在安全级别2的情况下,新控制器(对应于设备认证)41,除了安全级别1的情况以外,还允许一部分的操作系统以及设定系统的命令。但是,禁止与收费及隐私有关的信息的获得、以及运转工作状态的设定及变更。这是因为,在不是安全级别3的情况下(不与设备认证对应的情况下),会有命令的篡改的可能性的缘故。以下,按空调、蓄电池、太阳光发电、以及即热式热水器等的每个设备进行更详细说明。

[0124] 新控制器(对应于设备认证)41,对于空调,在安全级别1的情况下,仅允许获得信息,禁止操作系统的全部。并且,在安全级别2的情况下,允许设定非不安全的温度上下限度范围内的温度。

[0125] 新控制器(对应于设备认证)41,对于蓄电池,在安全级别1的情况下,仅允许获得基本的信息,禁止操作系统以及获得与电力买卖等的收费有关的电力量信息。并且,在安全级别2的情况下,禁止不安全的工作以及会有给电力系统带来影响的可能性的工作。

[0126] 新控制器(对应于设备认证)41,对于太阳光发电,在安全级别1的情况下,仅允许获得基本的信息。并且,在安全级别2的情况下,禁止获得与收费有关的累计发电量测量值。

[0127] 新控制器(对应于设备认证)41,对于即热式热水器,在安全级别1的情况和安全级别2的情况下,都仅允许获得基本的信息,禁止设定会有用户不意图的热水器运转的可能性的浴室自动模式。

[0128] 如上说明,本实施例涉及的通信系统具备的新控制器(对应于设备认证)41是,与利用电子证书而相互认证成功的设备进行加密通信的控制器,具备,判断部105、功能限制部106以及通信部11。判断部105,判断通信对象的设备是否是与相互认证对应的认证对应设备。功能限制部106,在由判断部105判断为不是认证对应设备的情况下,对该通信对象的设备具有的功能之中的、能够由新控制器(对应于设备认证)41操作的功能进行限制。通信部11,在由功能限制部106的功能限制之下与通信对象的设备以明文进行通信。据此,即使在与设备认证对应的设备以及不对应的设备混在一起的环境下,也能够安全地操作不与设备认证对应的设备。

[0129] 并且,判断部105也可以,在判断为通信对象的设备不是认证对应设备的情况下,进一步,判断通信对象的设备是符合白名单124的允许设备还是不符合白名单124的遗留设备。功能限制部106也可以,在由判断部105判断为是允许设备的情况下,与判断为是遗留设备的情况相比功能限制少。据此,例如,能够使针对与AIF对应的设备的功能限制,与针对遗留设备的功能限制相比放宽。

[0130] 并且,功能限制部106也可以,在由判断部105判断为是遗留设备的情况下,仅允许工作状态以及设定信息的获得命令。据此,能够尽量抑制遗留设备受到威胁的可能性。

[0131] 并且,功能限制部106也可以,在由判断部105判断为是允许设备的情况下,除了允许工作状态以及设定信息的获得命令以外,还允许操作系统以及设定系统的命令(但是,除了与收费及隐私有关的信息的获得、以及运转工作状态的设定及变更以外)。据此,能够一边减少允许设备受到威胁的可能性,一边利用与允许设备的特性对应的命令。

[0132] 进一步,也可以是,在由判断部105判断为不是认证对应设备的情况下,为了向用户询问是否允许与通信对象的设备连接,而使与新控制器(对应于设备认证)41能够通信的显示部13显示确认画面13A。据此,能够在用户确认之下允许与通信对象的设备连接,因此,能够避免进行不需要的功能限制的不良情况。

[0133] 进一步,也可以是,为了变更由功能限制部106的功能限制,而使与新控制器(对应于设备认证)41能够通信的显示部13显示确认画面13B。据此,能够在用户确认之下变更(包括解除)功能限制,因此,能够避免进行不需要的功能限制的不良情况。

[0134] 并且,判断部105也可以,在相互认证的开始时接收依据ECHONET的数据包的情况下,判断为不是认证对应设备。据此,能够确实且容易判断是否是认证对应设备。

[0135] 而且,在所述说明中,根据通信对象的设备是认证对应设备还是允许设备还是遗留设备,判断三个阶段的安全级别,但是,安全级别是两个阶段以上即可。除了最高的安全级别的情况以外,若施加某种功能限制,则能够获得同样的效果。

[0136] 并且,作为允许设备示出了与AIF对应的设备的例子,但是,若是与某种标准对应的设备,则能够作为允许设备采用。在采用多个种类的允许设备的情况下,也可以按每个允许设备设定不同的安全级别。在此情况下,当然也可以与按每个允许设备不同的安全级别对应施加不同强度的功能限制。

[0137] 并且,在与设备(遗留)32以及设备(对应于AIF)52连接的情况下显示确认画面13A(参照图15),但是,也可以在与设备(遗留)32连接时和与设备(对应于AIF)52连接时显示不同确认画面。据此,也能够安全级别越低,用户就越难以发出连接允许。

[0138] 并且,判断部105,在相互认证的开始时接收依据ECHONET的数据包的情况下,判断为不是认证对应设备,但是,对于判断认证对应设备的定时以及判断的方法,没有特别的限定。例如,在设备(遗留)32以及设备(对应于AIF)52依据ECHONET以外的标准的情况下,判断是否接收依据ECHONET以外的标准的数据包即可。

[0139] 并且,除了能够作为新控制器(对应于设备认证)41实现以外,还能够作为将新控制器(对应于设备认证)41具备的具有特征的处理部设为各个步骤的通信方法实现,也能够作为使计算机执行这些各个步骤的程序实现。当然,也可以经由CD-ROM等的记录介质以及互联网等的传输介质分发这样的程序。

[0140] (其他的实施例)

[0141] 如上所述,记载了实施例,但是,对于构成该公开的一部分的论述以及附图,应该不理解为限定本实施例。根据该公开,本领域的技术人员会能够明确各种代替实施方式、实施例以及运用技术。

[0142] 例如,在已经说明的实施例中,也可以使图7至图10的序列图,即使控制器1与设备2相反,也能够进行同样的处理。

[0143] 当然包括所述以外的、在此没有记载的各种各样的实施例等。因此,本实施例的技术范围仅由根据所述说明妥当的要求范围涉及的发明特定事项决定。

[0144] 符号说明

[0145] 11、21 通信部

[0146] 13 显示部

[0147] 13A、13B 确认画面

[0148] 41 新控制器(对应于设备认证),控制器

[0149] 105 判断部

[0150] 106 功能限制部

[0151] 124 白名单(允许列表)

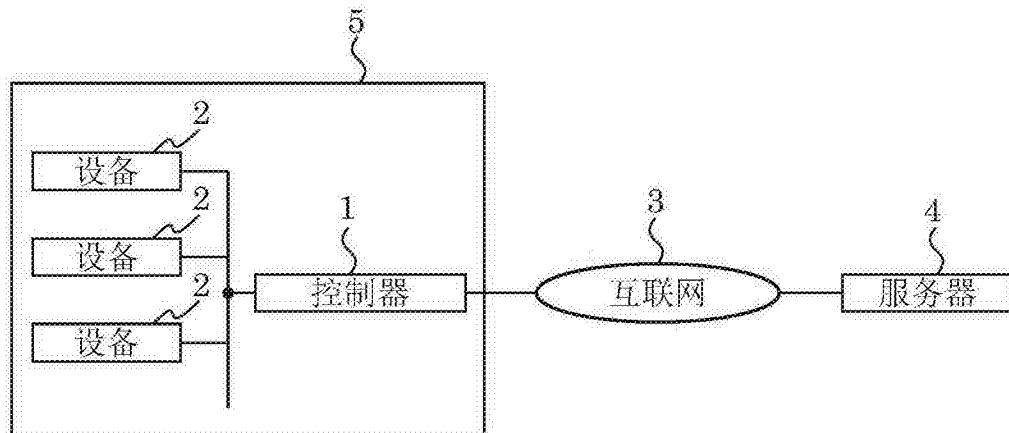


图1

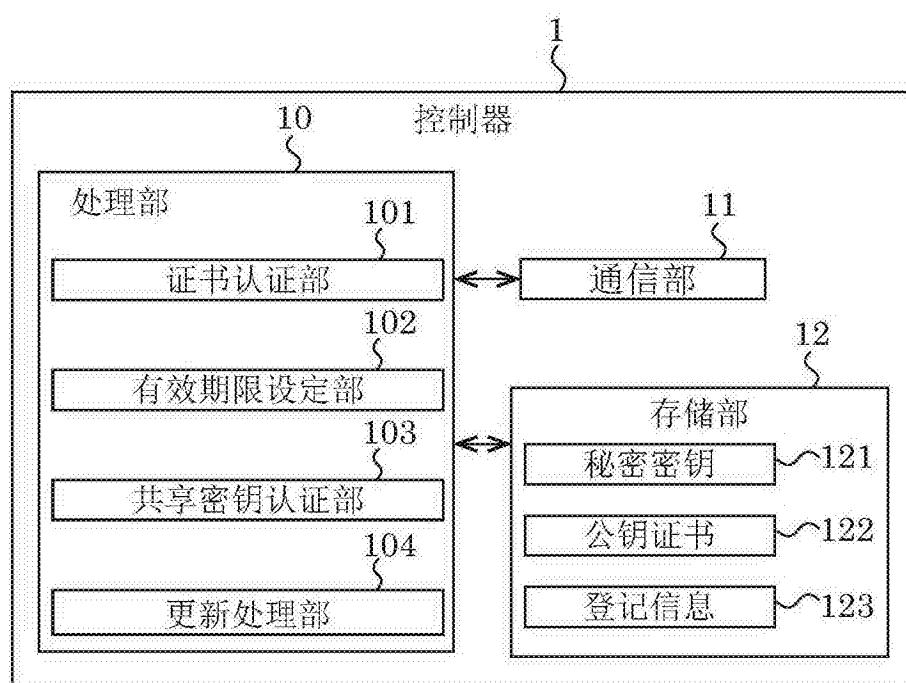


图2

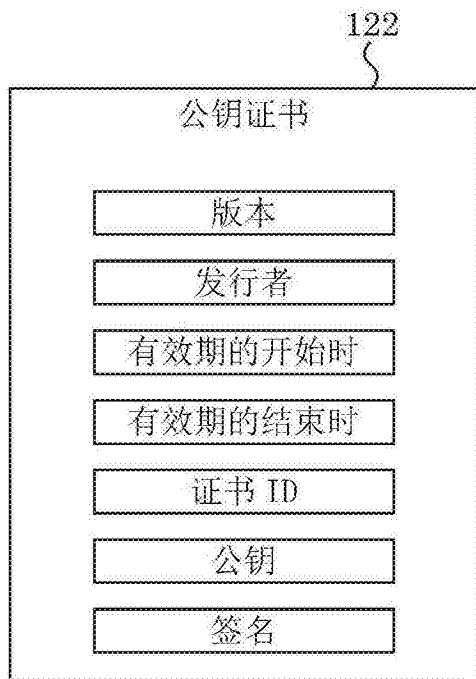


图3

123

设备 ID	证书 ID	共享密钥	群组密钥	会话密钥	会话剩余时间
D1	P1	01234...	11223...	11122...	13:40:50
D2	P2	98765...		22233...	13:41:24
D3	P3	19283...		33344...	16:02:13
...	...	...		...	...

图4

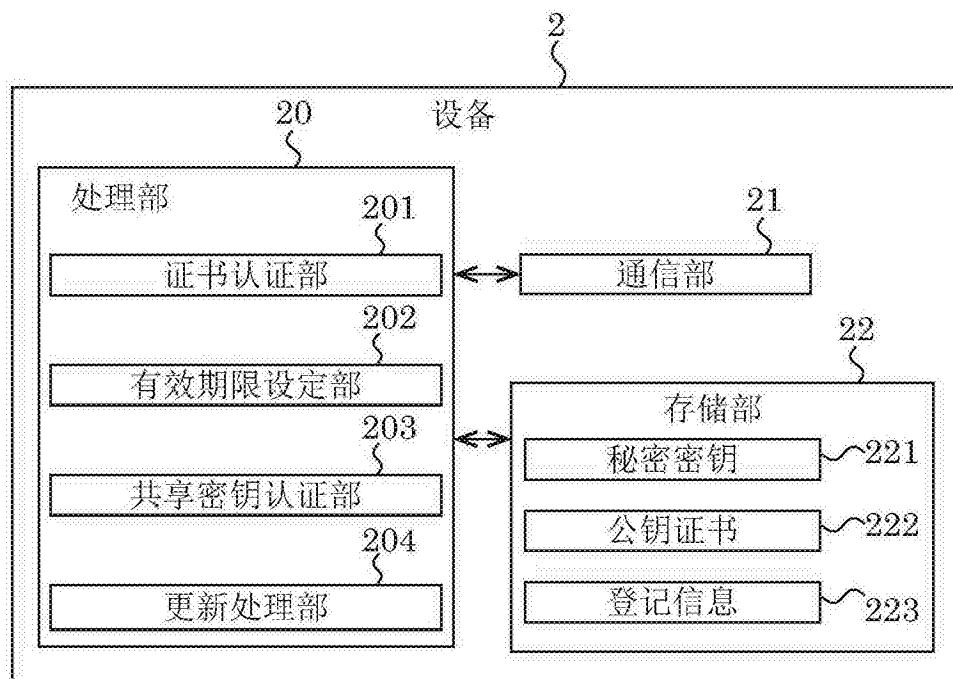


图5

控制器 ID	证书 ID	共享密钥	群组密钥	会话密钥	会话剩余时间
C1	Q1	01234...	11223...	11122...	13:40:50...
...	...	...	...	...	...

图6

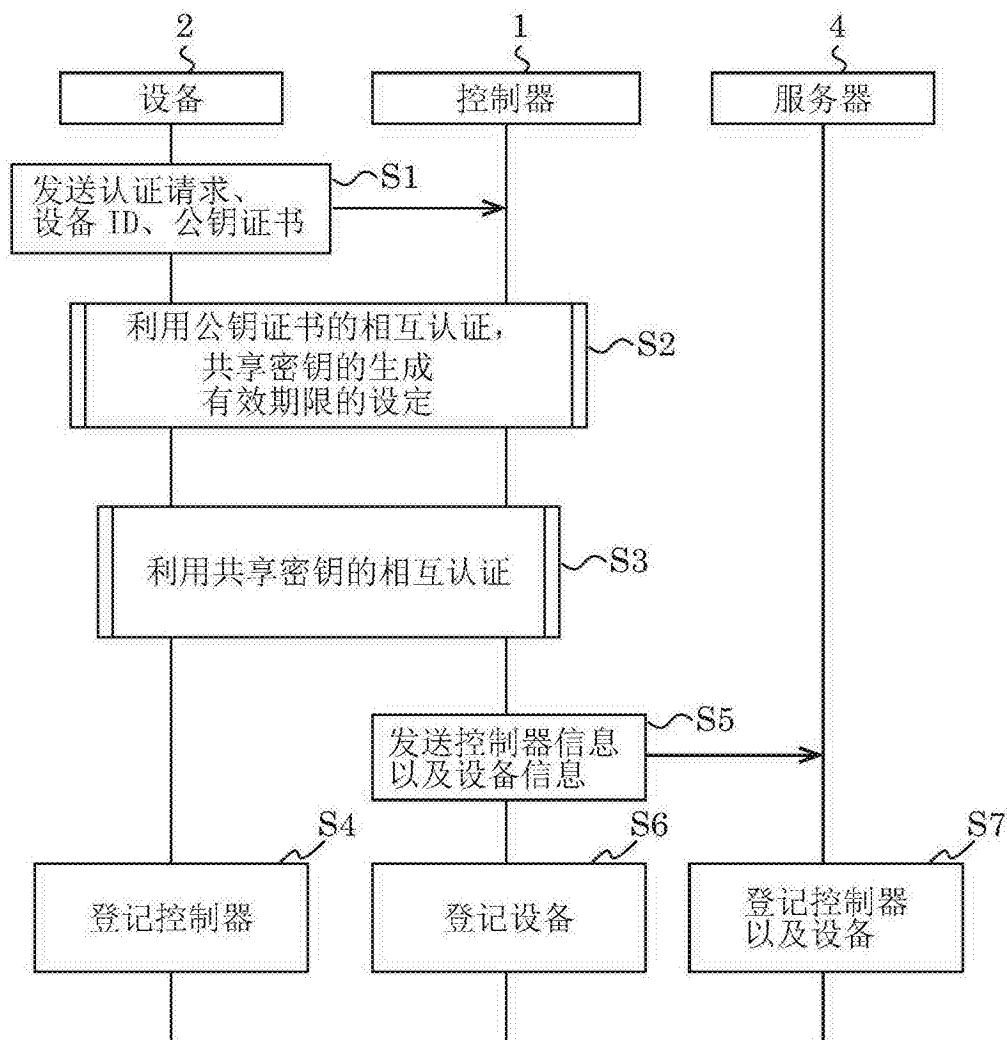


图7

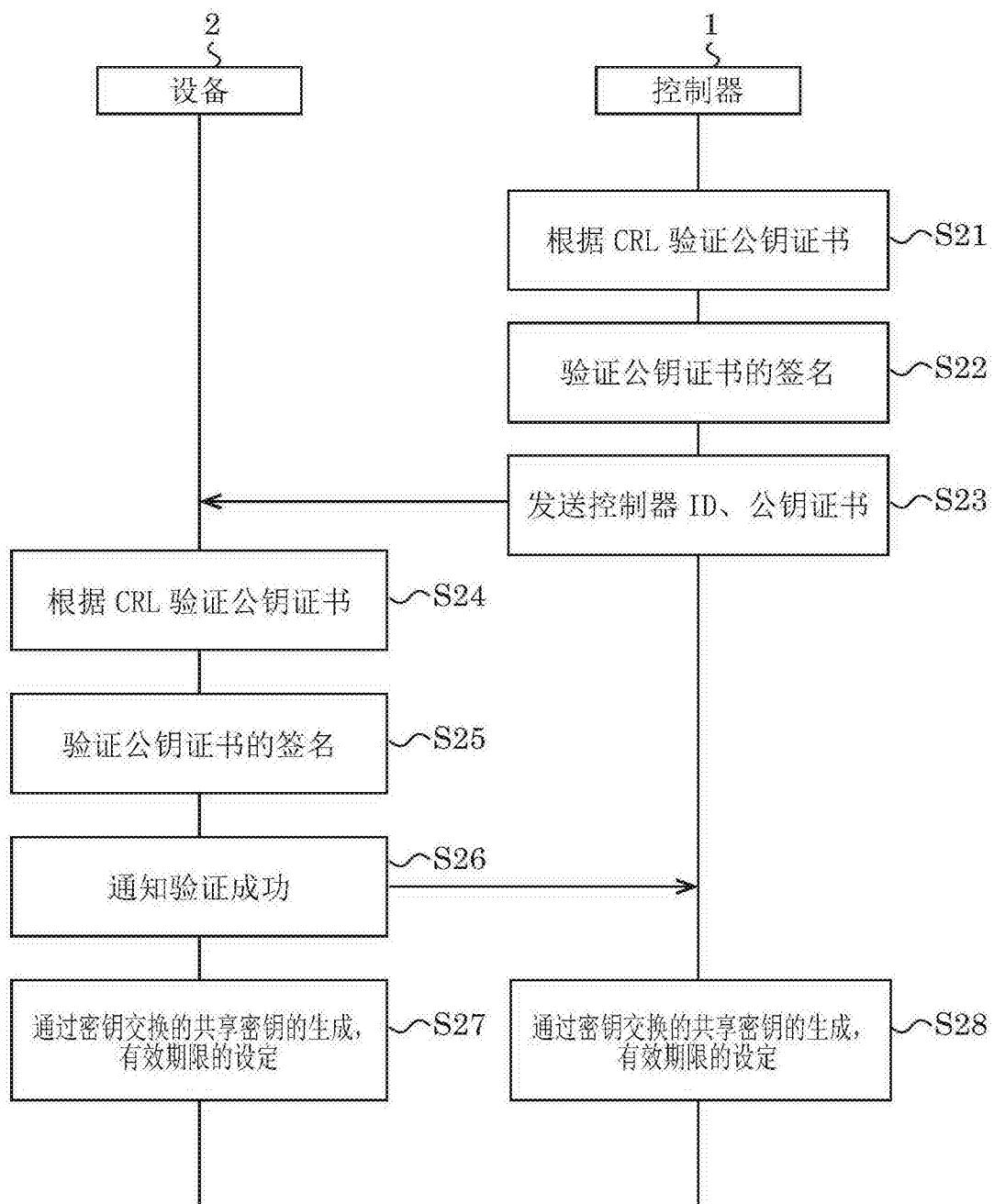


图8

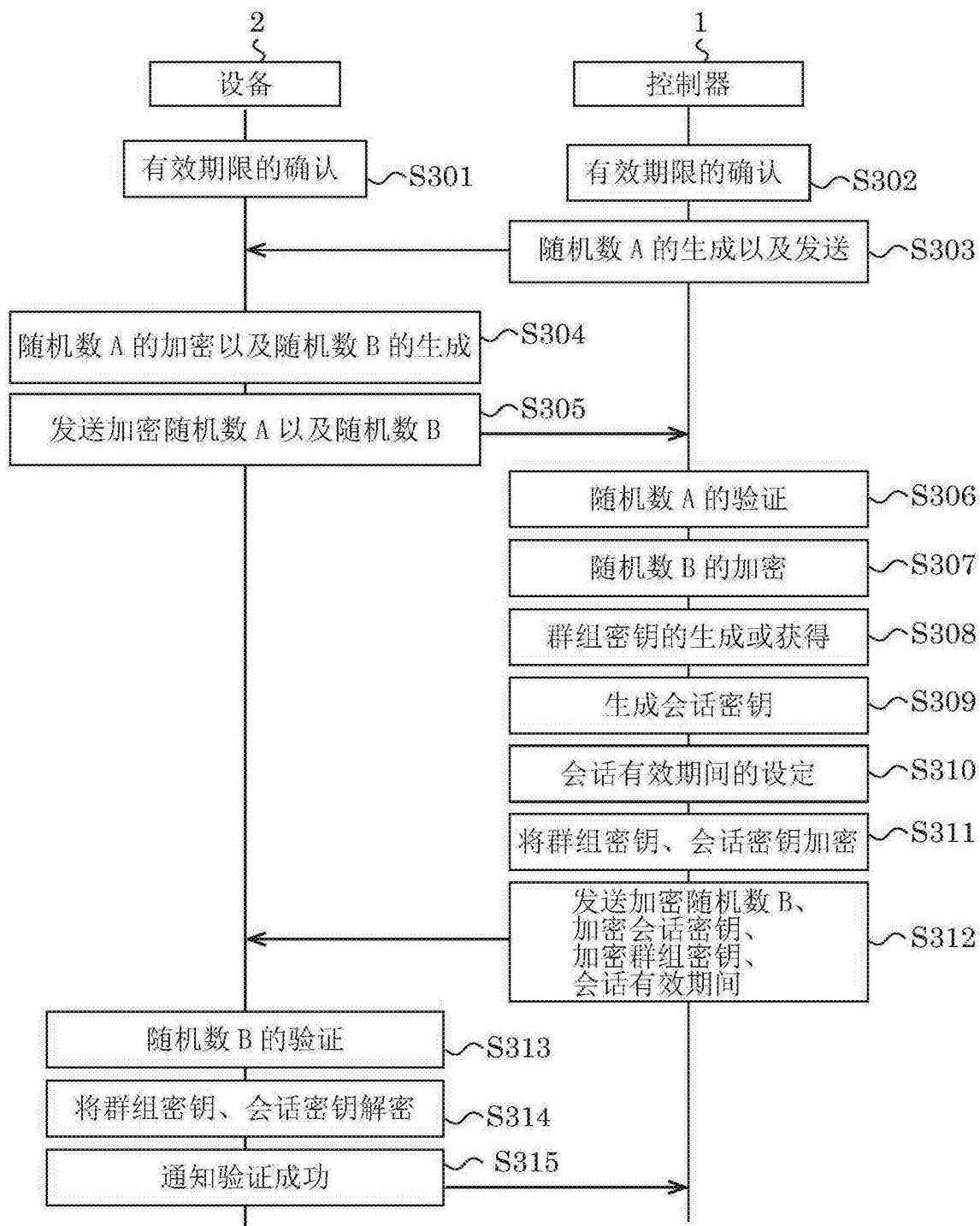


图9

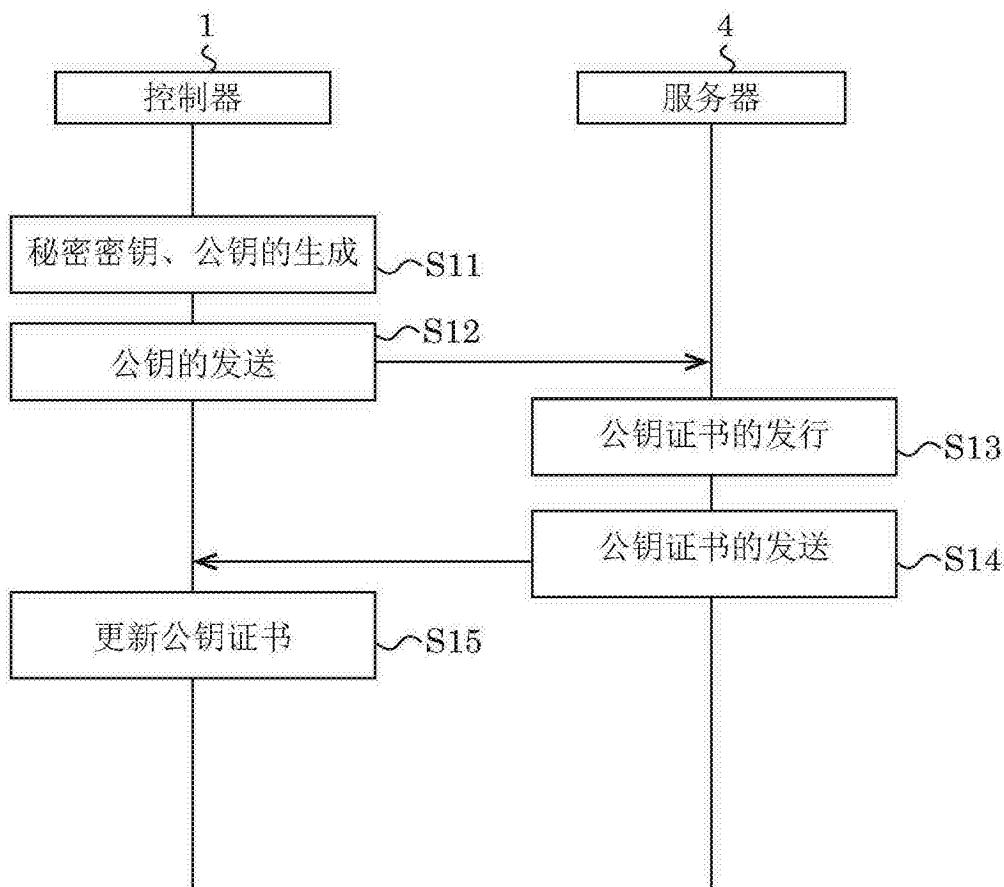


图10

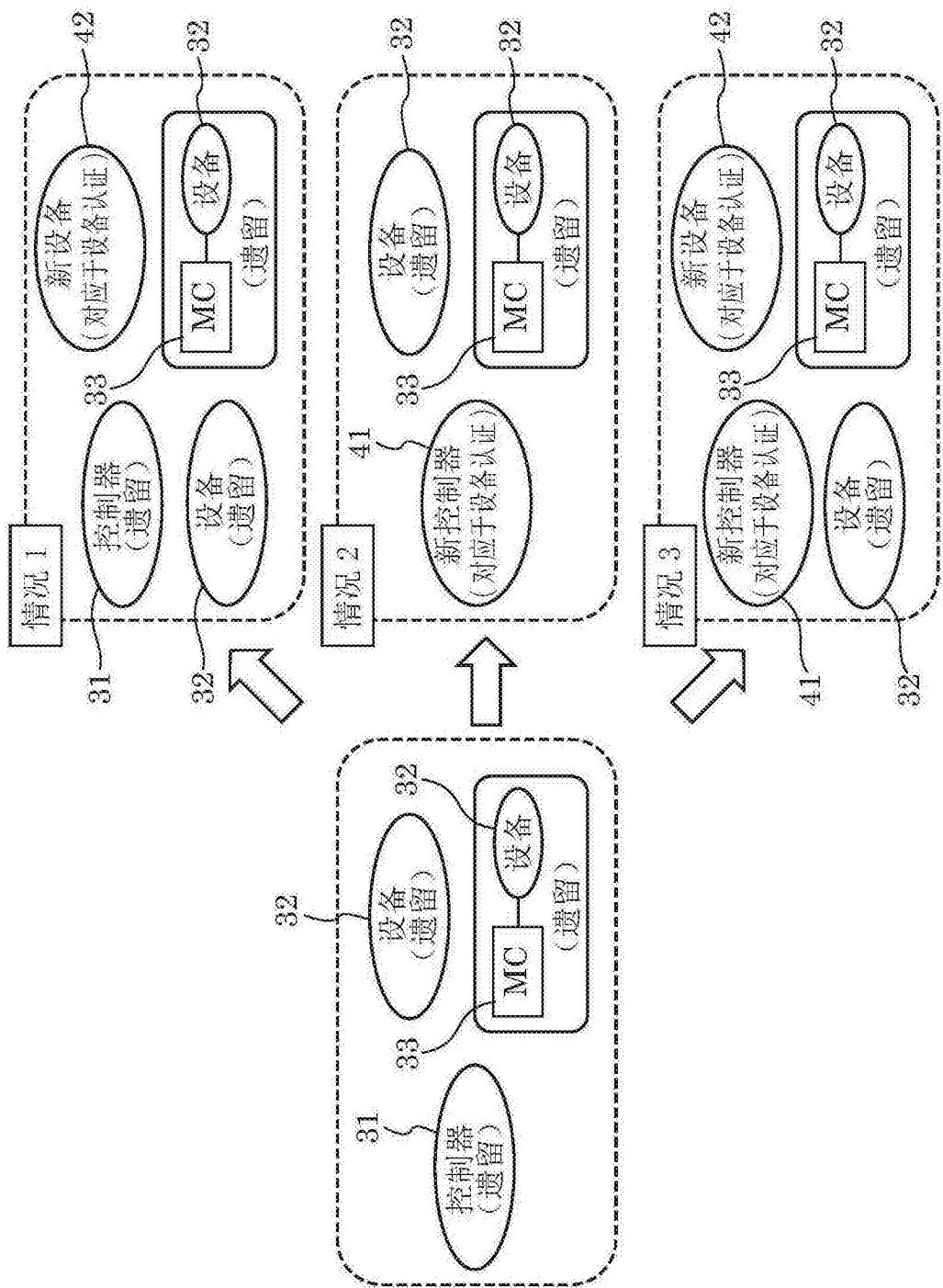


图 11

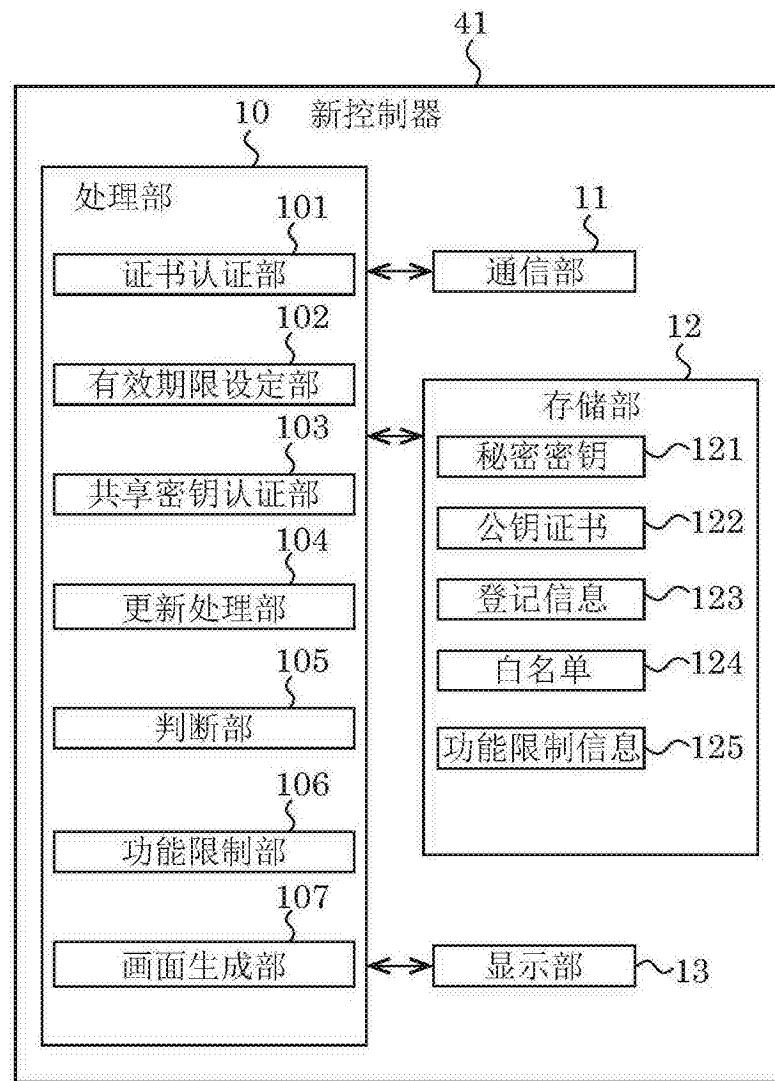


图12

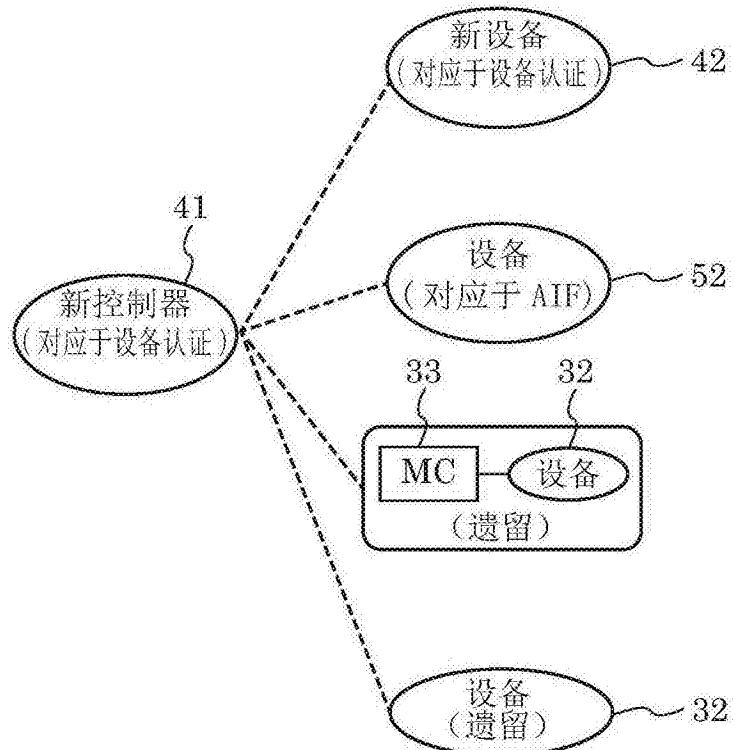


图13

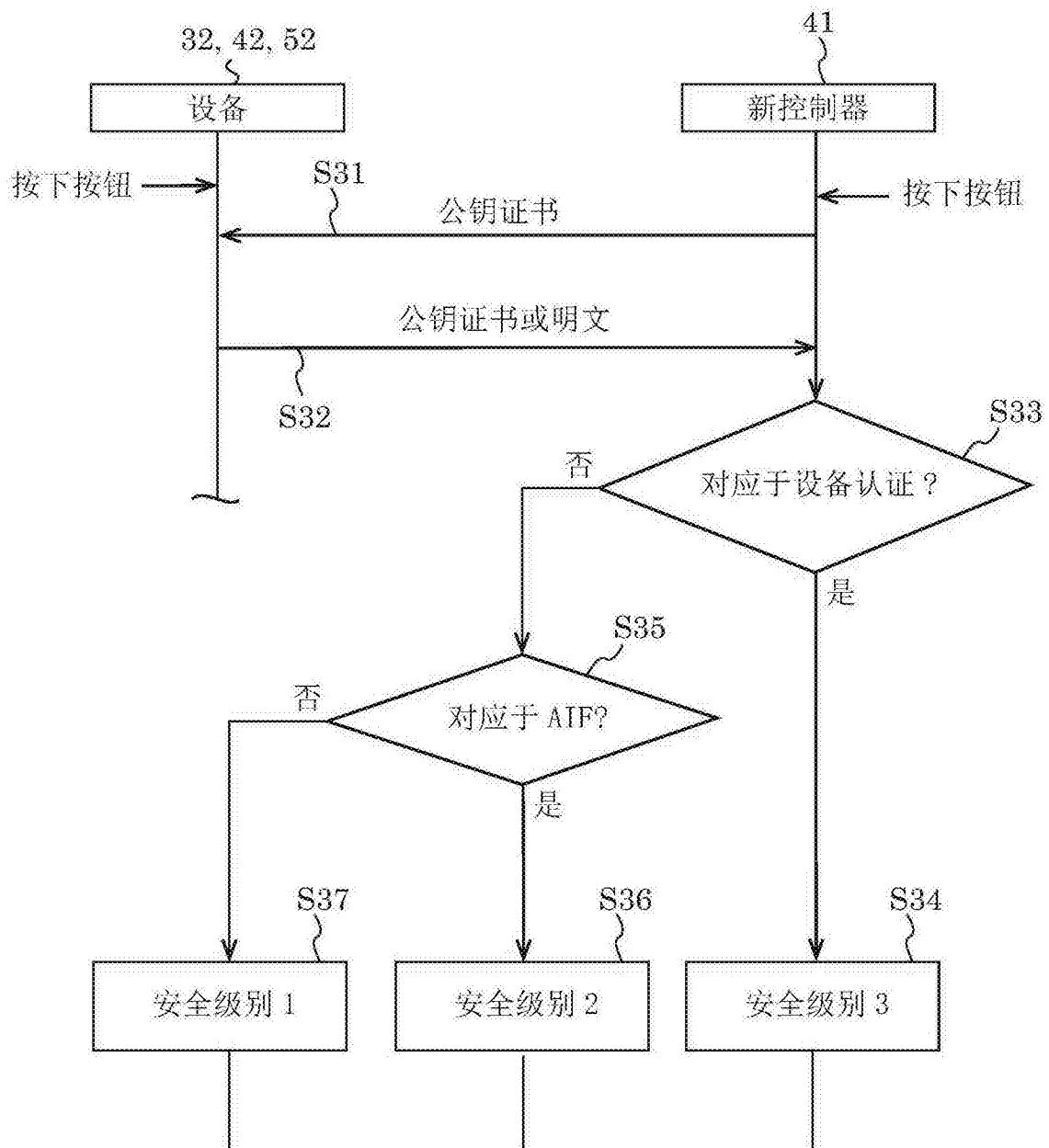


图14

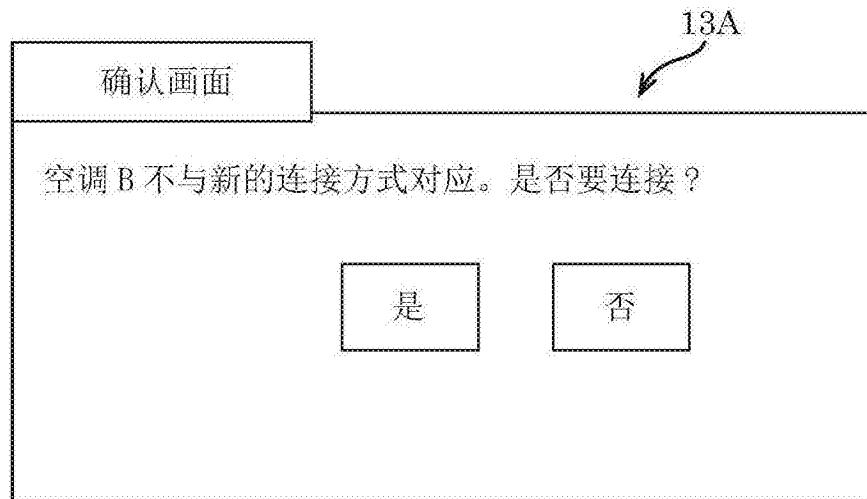


图15

13B

设定确认一览

	安全级别	功能限制	设备删除
空调 A	3	没有	—
空调 B	2	一部分	—
照明	1	仅 On/Off	—

This diagram shows a 'Setting Confirmation List' dialog box labeled '13B'. At the top left is a button labeled '设定确认一览' (Setting Confirmation List). The main area contains a table with four columns: '安全级别' (Safety Level), '功能限制' (Function Limitation), and '设备删除' (Device Deletion). There are three rows of data corresponding to '空调 A', '空调 B', and '照明' (Lighting).

图16

125

安全 级别 设备	3 (对应于设备认证) 没有功能限制	2 (对应于 AIF) 有一部分功能限制	1 (遗留设备) 有功能限制
	(1) 允许获得工作状态 · 设定信息等 (2) 允许设定温度 (3) 允许电源 ON/OFF	(1) 允许获得工作状态 · 设定信息等 (2) 允许设定温度 <b>(3) 禁止电源 ON/OFF</b>	(1) 允许获得工作状态 · 设定信息等 (2) <b>禁止设定温度</b> (3) <b>禁止电源 ON/OFF</b>
空调	(1) 允许获得工作状态 · 设定信息等 (2) 允许设定温度 (3) 允许电源 ON/OFF	(1) 允许获得工作状态 · 设定信息等 (2) 允许获得电力质量信息 <b>(3) 禁止设定运转模式</b> <b>(急速充电 / 充电 / 放电 / 等待 / 试验 / 自动 / 其他)</b>	(1) 允许获得工作状态 · 设定信息等 (2) <b>禁止设定运转模式</b> (3) <b>禁止充电 / 充电 / 放电 / 等待 / 试验 / 自动 / 其他</b>
蓄电池	(1) 允许获得工作状态 · 设定信息等 (2) 允许获得电力质量信息 (3) 允许设定运转模式 (急速充电 / 充电 / 放电 / 等待 / 试验 / 自动 / 其他)	(1) 允许获得工作状态 · 设定信息等 (2) 允许获得电力质量信息 <b>(3) 禁止设定运转模式</b> <b>(急速充电 / 充电 / 放电 / 等待 / 试验 / 自动 / 其他)</b>	(1) 允许获得工作状态 · 设定信息等 (2) <b>禁止设定运转模式</b> (3) <b>禁止充电 / 充电 / 放电 / 等待 / 试验 / 自动 / 其他</b>
太阳光 发电	(1) 允许获得工作状态 · 设定信息等 (2) 允许获得测量值 (3) 允许获得累计发电量测量值	(1) 允许获得工作状态 · 设定信息等 (2) 允许获得测量值 <b>(3) 禁止获得累计发电量测量值</b>	(1) 允许获得工作状态 · 设定信息等 (2) <b>禁止获得测量值</b> (3) <b>禁止获得累计发电量测量值</b>
即热式 热水器	(1) 允许获得工作状态 · 设定信息等 (2) 允许设定浴室自动模式	(1) 允许获得工作状态 · 设定信息等 (2) <b>禁止设定浴室自动模式</b>	(1) 允许获得工作状态 · 设定信息等 (2) <b>禁止设定浴室自动模式</b>

图 17