(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 119768789 A
(43)申请公布日 2025.04.04

(21)申请号 202380061353.X

(22)申请日 2023.06.27

(30)优先权数据
2022-138693 2022.08.31 JP

(85)PCT国际申请进入国家阶段日
2025.02.21

(86)PCT国际申请的申请数据
PCT/JP2023/023713 2023.06.27

(87)PCT国际申请的公布数据
WO2024/048045 JA 2024.03.07

(71)申请人 松下知识产权经营株式会社
地址 日本

(72)发明人 中谷德夫 福田秀树 山口隆
西川浩

(74)专利代理机构 永新专利商标代理有限公司 72002
专利代理师 高迪

(51)Int.Cl.
G06F 21/10(2006.01)
G06F 21/44(2006.01)
G06F 21/60(2006.01)
G06F 21/64(2006.01)

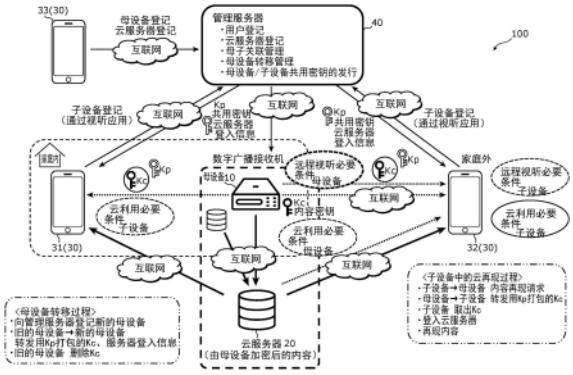
权利要求书4页 说明书24页 附图24页

(54)发明名称

终端装置、录像管理系统、管理服务器装置、控制方法及程序

(57)摘要

作为终端装置的子设备(30)具备电路以及与该电路连接的存储器,电路使用存储器,在与作为录像装置的母设备(10)之间进行设备认证,从母设备(10)取得被加密的内容密钥(Kc),使用由母设备(10)与子设备(30)共享的共用密钥(Kp)对内容密钥(Kc)进行解密,不经由母设备(10)而访问云服务器(20),读出由母设备(10)向云服务器(20)录像而且被加密的内容,使用内容密钥(Kc)对读出的内容进行解密并再现。



CN 119768789 A

1.一种终端装置,被用于录像再现系统,

所述录像再现系统包括:

云服务器装置;

录像装置,接收被分发的内容并加密,将被加密的所述内容经由互联网向所述云服务器装置录像;以及

所述终端装置,再现所述内容,

所述终端装置具备电路以及与所述电路连接的存储器,

所述电路使用所述存储器,

在与所述录像装置之间进行设备认证,

从所述录像装置取得被加密的内容密钥,

使用由所述录像装置与所述终端装置共享的共用密钥对所述内容密钥进行解密,

不经由所述录像装置而访问所述云服务器装置,读出所述云服务器装置中被录像而且被加密的所述内容,

使用所述内容密钥对读出的所述内容进行解密并再现。

2.如权利要求1所述的终端装置,

所述电路经由管理服务器装置在与所述录像装置之间进行设备认证,从而取得从所述管理服务器装置向所述终端装置及所述录像装置发送的所述共用密钥。

3.一种录像管理系统,被用于录像再现系统,

所述录像再现系统包括:

云服务器装置;

所述录像管理系统,接收被分发的内容并加密,将被加密的所述内容经由互联网向所述云服务器装置录像;以及

终端装置,再现所述内容,

所述录像管理系统具备电路以及至少1个存储器,

所述至少1个存储器将有效性判定信息和内容密钥与所述云服务器装置建立关联地保持,

所述电路,

从所述至少1个存储器读出所述内容密钥并用于所述内容的加密,

从所述至少1个存储器读出所述有效性判定信息,并使用所述有效性判定信息判定所述云服务器装置中录像的所述内容的有效性。

4.如权利要求3所述的录像管理系统,

所述录像管理系统具备:

录像装置,进行所述内容向所述云服务器装置的录像;以及

管理服务器装置,经由互联网连接至所述录像装置,

所述电路及所述至少1个存储器各自被配置于所述录像装置或者所述管理服务器装置。

5.如权利要求3或者4所述的录像管理系统,

所述有效性判定信息是表示针对所述内容的管理信息的校验和、哈希值以及所述内容的复制次数之中的至少1个的信息。

6.如权利要求5所述的录像管理系统,

在所述录像管理系统和所述云服务器装置各自中保持并更新所述管理信息的情况下,

所述电路对根据所述录像管理系统的所述管理信息得到的所述有效性判定信息与根据所述云服务器装置的所述管理信息得到的有效性判定信息进行比较,从而判定所述云服务器装置中录像的所述内容的有效性。

7.一种管理服务器装置,被用于录像再现系统,

所述录像再现系统包括:

云服务器装置;

第1录像装置,接收被分发的内容并加密,将被加密的所述内容经由互联网向所述云服务器装置录像;

终端装置,再现所述内容;以及

所述管理服务器装置,与所述第1录像装置经由互联网连接,

所述管理服务器装置具备电路以及与所述电路连接的存储器,

所述存储器将用于识别所述第1录像装置的第1识别信息与所述云服务器装置建立关联地保持,

所述电路,

在所述第1录像装置被替换为第2录像装置的情况下,

将与所述云服务器装置建立关联地保持在所述存储器中的所述第1识别信息,置换为用于识别所述第2录像装置的第2识别信息,

将用于保护所述内容且在所述第1录像装置中保持的保护信息,转移至所述第2录像装置。

8.如权利要求7所述的管理服务器装置,

在所述第1录像装置被从所述录像再现系统中移除的情况下,所述电路执行:

(a)由所述第1录像装置向所述云服务器装置录像的所述内容的删除;

(b)所述第1录像装置或者所述存储器中保持的用于访问所述云服务器装置的云账户信息的删除;以及

(c)与所述云账户信息建立关联地保持在所述存储器中的所述第1识别信息的删除;

之中的至少1个。

9.如权利要求8所述的管理服务器装置,

所述保护信息是表示用于对所述内容进行解密的内容密钥、针对所述内容的管理信息的校验和、哈希值以及所述内容的复制次数之中的至少一个的信息。

10.一种控制方法,是被用于录像再现系统的终端装置所进行的控制方法,

所述录像再现系统包括:

云服务器装置;

录像装置,接收被分发的内容并加密,将被加密的所述内容经由互联网向所述云服务器装置录像;以及

所述终端装置,再现所述内容,

在所述控制方法中,

在与所述录像装置之间进行设备认证,

从所述录像装置取得被加密的内容密钥，

使用由所述录像装置与所述终端装置共享的共用密钥对所述内容密钥进行解密，

不经由所述录像装置而访问所述云服务器装置，读出所述云服务器装置中被录像而且被加密的所述内容，

使用所述内容密钥对读出的所述内容进行解密并再现。

11.一种控制方法，是被用于录像再现系统的录像管理系统所进行的控制方法，

所述录像再现系统包括：

云服务器装置；

所述录像管理系统，接收被分发的内容并加密，将被加密的所述内容经由互联网向所述云服务器装置录像；以及

终端装置，再现所述内容，

在所述控制方法中，

将有效性判定信息和内容密钥与所述云服务器装置建立关联地保持，

从存储器读出所述内容密钥并用于所述内容的加密，

从所述存储器读出所述有效性判定信息，使用所述有效性判定信息判定所述云服务器装置中录像的所述内容的有效性。

12.一种控制方法，是被用于录像再现系统的管理服务器装置所进行的控制方法，

所述录像再现系统包括：

云服务器装置；

第1录像装置，接收被分发的内容并加密，将被加密的所述内容经由互联网向所述云服务器装置录像；

终端装置，再现所述内容；以及

所述管理服务器装置，与所述第1录像装置经由互联网连接，

在所述控制方法中，

将用于识别所述第1录像装置的第1识别信息与所述云服务器装置建立关联地保持，

在所述第1录像装置被替换为第2录像装置的情况下，

将与所述云服务器装置建立关联地保持在存储器中的所述第1识别信息，置换为用于识别所述第2录像装置的第2识别信息，

将用于保护所述内容且在所述第1录像装置中保持的保护信息，转移至所述第2录像装置。

13.一种用于被用于录像再现系统的终端装置的程序，

所述录像再现系统包括：

云服务器装置；

录像装置，接收被分发的内容并加密，将被加密的所述内容经由互联网向所述云服务器装置录像；以及

所述终端装置，再现所述内容，

所述程序使所述终端装置的计算机执行：

在与所述录像装置之间进行设备认证，

从所述录像装置取得被加密的内容密钥，

使用由所述录像装置与所述终端装置共享的共用密钥对所述内容密钥进行解密，

不经由所述录像装置而访问所述云服务器装置，读出所述云服务器装置中被录像而且被加密的所述内容，

使用所述内容密钥对读出的所述内容进行解密并再现。

14.一种用于被用于录像再现系统的录像管理系统的程序，

所述录像再现系统包括：

云服务器装置；

所述录像管理系统，接收被分发的内容并加密，将被加密的所述内容经由互联网向所述云服务器装置录像；以及

终端装置，再现所述内容，

所述程序使所述录像管理系统的计算机执行：

将有效性判定信息和内容密钥与所述云服务器装置建立关联地保持，

从存储器读出所述内容密钥并用于所述内容的加密，

从所述存储器读出所述有效性判定信息，使用所述有效性判定信息判定所述云服务器装置中录像的所述内容的有效性。

15.一种用于被用于录像再现系统的管理服务器装置的程序，

所述录像再现系统包括：

云服务器装置；

第1录像装置，接收被分发的内容并加密，将被加密的所述内容经由互联网向所述云服务器装置录像；

终端装置，再现所述内容；以及

所述管理服务器装置，与所述第1录像装置经由互联网连接，

所述程序使所述管理服务器装置的计算机执行：

将用于识别所述第1录像装置的第1识别信息与所述云服务器装置建立关联地保持，

在所述第1录像装置被替换为第2录像装置的情况下，

将与所述云服务器装置建立关联地保持在存储器中的所述第1识别信息，置换为用于识别所述第2录像装置的第2识别信息，

将用于保护所述内容且在所述第1录像装置中保持的保护信息，转移至所述第2录像装置。

终端装置、录像管理系统、管理服务器装置、控制方法及程序

技术领域

[0001] 本公开涉及在对被分发的例如节目等的内容进行录像并再现的系统等中使用的技术。

背景技术

[0002] 以往,提出了包括安全地进行内容的收发的内容发送装置及内容接收装置的内容传送系统(例如参照专利文献1)。在该内容传送系统中,内容发送装置进行与内容接收装置的相互认证及共享密钥的交付等,使用根据该共享密钥生成的加密密钥对内容进行加密并向内容接收装置发送。此时,内容发送装置根据内容接收装置是否具有规定的安全性强度,对交付的共享密钥进行切换。

[0003] 另外,提出了在恰当的利用范围内将家庭内的服务器中积蓄的内容经由外部网络向终端发送的内容传送系统(例如参照专利文献2)。在该内容传送系统中,服务器针对通过远程访问请求内容的终端,许可比可再现时间短的内容的传送,与通过远程访问而传送的内容的再现时间相应地减少可再现时间。

[0004] 在先技术文献

[0005] 专利文献

[0006] 专利文献1:日本特许第6390618号公报

[0007] 专利文献2:日本特许第6187139号公报

发明内容

[0008] 发明所要解决的课题

[0009] 但是,在通用的云服务器中对内容进行录像的情况下,在上述专利文献1及2的内容传送系统中,存在难以恰当地抑制与该内容相关的非法行为的课题。

[0010] 于是,本公开提供能够恰当地抑制与内容相关的非法行为的终端装置等。

[0011] 用于解决课题的手段

[0012] 本公开的一个方式所涉及的终端装置被用于录像再现系统,所述录像再现系统具备:云服务器装置;录像装置,接收被分发的内容并加密,将被加密的所述内容经由互联网向所述云服务器装置录像;以及所述终端装置,再现所述内容,所述终端装置具备电路以及与所述电路连接的存储器,所述电路使用所述存储器,在与所述录像装置之间进行设备认证,从所述录像装置取得被加密的内容密钥,使用由所述录像装置与所述终端装置共享的共用密钥对所述内容密钥进行解密,不经由所述录像装置而访问所述云服务器装置,读出所述云服务器装置中被录像而且被加密的所述内容,使用所述内容密钥对读出的所述内容进行解密并再现。

[0013] 此外,这些概括或者具体的方式也可以由装置、方法、集成电路、计算机程序或者计算机可读取的CD-ROM等记录介质实现,也可以通过装置、方法、集成电路、计算机程序及记录介质的任意组合来实现。另外,记录介质也可以是非易失性的记录介质。

[0014] 发明效果

[0015] 本公开的终端装置能够恰当地抑制与内容相关的非法行为。

[0016] 此外,本公开的一个方式中的进一步的优点及效果通过说明书及附图而明确。相关的优点以及/或者效果由若干实施方式以及说明书和附图所记载的构成提供,但不一定需要全部构成。

附图说明

[0017] 图1是表示实施方式中的录像再现系统的构成例的图。

[0018] 图2是简略地表示实施方式中的录像再现系统的构成的图。

[0019] 图3是表示实施方式中的录像再现系统的母设备及管理服务器所具有的信息的一例的图。

[0020] 图4是表示实施方式中的管理服务器的构成及管理服务器所具有的信息的一例的图。

[0021] 图5是表示实施方式中的母设备的构成以及母设备所具有的信息的一例的图。

[0022] 图6是表示实施方式中的母设备所具有的信息的其他例的图。

[0023] 图7是用于说明实施方式中的母设备权的转移的图。

[0024] 图8是表示实施方式中的包括内容和管理信息的数据结构例的图。

[0025] 图9是表示实施方式中的在进行管理服务器的账户制作及母设备的登记时的录像再现系统中的处理动作的一例的时序图。

[0026] 图10是表示实施方式中的在进行云服务器的云账户制作时的录像再现系统中的处理动作的一例的时序图。

[0027] 图11是表示实施方式中的在母设备与云服务建立关联时的录像再现系统中的处理动作的一例的时序图。

[0028] 图12是表示实施方式中的在母设备与云服务建立关联时的录像再现系统中的处理动作的其他例的时序图。

[0029] 图13是表示实施方式中的在进行子设备的登记以及向母设备建立关联时的录像再现系统中的处理动作的一例的时序图。

[0030] 图14是表示实施方式中的在母设备将内容向云服务录像时的录像再现系统中的处理动作的一例的时序图。

[0031] 图15是表示实施方式中的在母设备对云服务中的内容进行再现时的录像再现系统中的处理动作的一例的时序图。

[0032] 图16是表示实施方式中的在子设备对云服务中的内容进行再现时的录像再现系统中的处理动作之中的第1处理动作的一例的时序图。

[0033] 图17是表示实施方式中的在子设备对云服务中的内容进行再现时的录像再现系统中的处理动作之中的第2处理动作的一例的时序图。

[0034] 图18是表示实施方式中的在母设备对云服务中的内容进行复制时的录像再现系统中的处理动作的一例的时序图。

[0035] 图19是表示实施方式中的在子设备删除该子设备的登记时的录像再现系统中的处理动作的一例的时序图。

[0036] 图20是表示实施方式中的在子设备删除其他子设备的登记时的录像再现系统中的处理动作的一例的时序图。

[0037] 图21是表示实施方式中的在子设备对云服务进行变更时的录像再现系统中的处理动作所包括的第1处理动作的一例的时序图。

[0038] 图22是表示实施方式中的在子设备对云服务进行变更时的录像再现系统中的处理动作之中的第2处理动作的一例的时序图。

[0039] 图23是表示实施方式中的在进行母设备权的转移时的录像再现系统中的处理动作之中的第1处理动作的一例的时序图。

[0040] 图24是表示实施方式中的在进行母设备权的转移时的录像再现系统中的处理动作之中的第2处理动作的一例的时序图。

[0041] 图25是表示实施方式中的在进行母设备的转让时的录像再现系统中的处理动作的一例的时序图。

具体实施方式

[0042] 本公开的一个方式所涉及的终端装置被用于录像再现系统,所述录像再现系统具备:云服务器装置;录像装置,接收被分发的内容并加密,将被加密的所述内容经由互联网向所述云服务器装置录像;以及所述终端装置,再现所述内容,所述终端装置具备电路以及与所述电路连接的存储器,所述电路使用所述存储器,在与所述录像装置之间进行设备认证,从所述录像装置取得被加密的内容密钥,使用由所述录像装置与所述终端装置共享的共用密钥对所述内容密钥进行解密,不经由所述录像装置而访问所述云服务器装置,读出所述云服务器装置中被录像而且被加密的所述内容,使用所述内容密钥对读出的所述内容进行解密并再现。此外,终端装置、录像装置及云服务器装置也分别被称为子设备、母设备及云服务器。

[0043] 由此,在进行由录像装置将内容向云服务器装置录像的云录像的情况下,在终端装置从云服务器装置直接再现内容时,也能够充分保护该内容,并且保证个人使用的范围,向用户提供自由的再现功能。例如,能够抑制由任意的终端对云服务器装置的内容进行再现的情况。由此,能够恰当地抑制与内容相关的非法行为,能够实现恰当的子设备访问控制。

[0044] 另外也可以是,所述电路经由管理服务器装置在与所述录像装置之间进行设备认证,从而取得从所述管理服务器装置向所述终端装置及所述录像装置发送的所述共用密钥。

[0045] 由此,共用密钥通过设备认证而在终端装置与录像装置之间共享,因此能够提高安全性的强度。

[0046] 另外也可以是,本公开的一个方式所涉及的录像管理系统被用于录像再现系统,所述录像再现系统包括:云服务器装置;所述录像管理系统,接收被分发的内容并加密,将被加密的所述内容经由互联网向所述云服务器装置录像;以及终端装置,再现所述内容,所述录像管理系统具备电路以及至少1个存储器,所述至少1个存储器将有效性判定信息和内容密钥与所述云服务器装置建立关联地保持,所述电路从所述至少1个存储器读出所述内容密钥并用于所述内容的加密,从所述至少1个存储器读出所述有效性判定信息,使用所述

有效性判定信息判定所述云服务器装置中录像的所述内容的有效性。例如也可以是,录像管理系统具备:录像装置,进行所述内容向所述云服务器装置的录像;以及管理服务器装置,经由互联网连接至所述录像装置,所述电路及所述至少1个存储器各自被设置于所述录像装置或者所述管理服务器装置。另外也可以是,所述有效性判定信息是表示针对所述内容的管理信息的校验和、哈希(Hash)值以及所述内容的复制次数之中的至少1个的信息。此外,终端装置、录像装置、云服务器装置及管理服务器装置分别也被称为子设备、母设备、云服务器及管理服务器。

[0047] 由此,如有效性判定信息或者内容密钥那样的与内容保护相关的信息,不是在云服务器装置中,而是在作为从不特定的用户无法访问的区域的录像管理系统的至少1个存储器中,在与云服务器装置建立了关联的状态下被管理。因此,在录像管理系统即母设备或者管理服务器中,对与云服务器装置相关联的有效性判定信息(管理信息的校验和、哈希值、每个节目的复制次数等)及内容密钥进行管理,因此能够实现即使非法制作了内容的COPY(拷贝、复制)、其也被视为无效而无法再现的框架。也就是说,能够实现云服务上的恰当的非法COPY对策。因此,能够恰当地抑制与内容相关的非法行为。

[0048] 另外也可以是,在所述录像管理系统和所述云服务器装置各自中保持并更新所述管理信息的情况下,所述电路对根据所述录像管理系统的所述管理信息得到的所述有效性判定信息与根据所述云服务器装置的所述管理信息得到的有效性判定信息进行比较,从而判定所述云服务器装置中录像的所述内容的有效性。

[0049] 由此,录像管理系统的有效性判定信息与云服务器装置的有效性判定信息被比较,例如,如果它们相互不同,则判定为内容无效。结果,能够恰当地判定内容的有效性。

[0050] 另外,本公开的一个方式所涉及的管理服务器装置被用于录像再现系统,所述录像再现系统包括:云服务器装置;第1录像装置,接收被分发的内容并加密,将被加密的所述内容经由互联网向所述云服务器装置录像;终端装置,再现所述内容;以及所述管理服务器装置,与所述第1录像装置经由互联网连接,所述管理服务器装置具备电路以及与所述电路连接的存储器,所述存储器将用于识别所述第1录像装置的第1识别信息与所述云服务器装置建立关联地保持,所述电路在所述第1录像装置被替换为第2录像装置的情况下,将与所述云服务器装置建立关联地保持在所述存储器中的所述第1识别信息,置换为用于识别所述第2录像装置的第2识别信息,将用于保护所述内容而且在所述第1录像装置中保持的保护信息,转移至所述第2录像装置。此外,终端装置、录像装置及云服务器装置也分别被称为子设备、母设备及云服务器。另外,保护信息例如表示内容密钥、管理信息的校验和或哈希值、复制次数等。

[0051] 由此,在第1录像装置被替换为第2录像装置的情况下,与云服务器装置建立了关联的第1录像装置的第1识别信息,被置换为第2录像装置的第2识别信息。即,向云服务器装置的内容的访问权(也被称为母设备权)转移至第2录像装置。进而,第1录像装置中保持的保护信息转移至第2录像装置。结果,能够充分保护内容,并且省事而且容易地进行母设备的转移、即母设备权从第1录像装置向第2录像装置的转移。因此,能够恰当地抑制与内容相关的非法行为。另外,这样的转移可以认为在个人的利用范围内而且不超出个人使用的范畴。也就是说,能够实现恰当的母设备的转移。

[0052] 另外也可以是,所述电路在所述第1录像装置被从所述录像再现系统中移除的情

况下,执行(a)由所述第1录像装置向所述云服务器装置录像的所述内容的删除;(b)所述第1录像装置或者所述存储器中保持的用于访问所述云服务器装置的云账户信息的删除;以及(c)与所述云账户信息建立关联地保持在所述存储器中的所述第1识别信息的删除之中的至少1个。

[0053] 由此,进行云服务器装置中录像的内容的删除、云账户信息的删除(或者复位)等。如果第1录像装置或管理服务器装置中记录的云账户信息被删除(或者复位),则无法从该第1录像装置访问云服务器装置。因此,能够充分抑制转让后的第1录像装置非法访问云服务器装置的情况,能够容易地实现第1录像装置即母设备的恰当的转让。

[0054] 另外,所述保护信息是表示用于对所述内容进行解密的内容密钥、针对所述内容的管理信息的校验和、哈希值、以及所述内容的复制次数之中的至少一个的信息。

[0055] 由此,用于有效地保护内容的保护信息从第1录像装置转移至第2录像装置,因此能够提高安全性的强度并实现恰当的母设备的转移。

[0056] 以下,关于实施方式,参照附图具体进行说明。

[0057] 此外,以下说明的实施方式均示出概括性或者具体性的例子。以下的实施方式所示的数值、形状、材料、构成要素、构成要素的配置位置及连接方式、步骤、步骤的顺序等是一例,并非意在限定本公开。此外,关于以下的实施方式中的构成要素之中表示最上位概念的独立权利要求中没有记载的构成要素,作为任意的构成要素而被说明。

[0058] 另外,各图是示意图,不一定严密地图示。另外,在各图中,针对相同的构成部件赋予相同的标记。

[0059] (实施方式)

[0060] 图1是表示本实施方式中的录像再现系统的构成例的图。

[0061] 本实施方式中的录像再现系统100具备母设备10、云服务器20、子设备31、子设备32、子设备33及管理服务器40。此外,在图1中,在录像再现系统100中具备子设备31~33,但也可以仅具备1个子设备。另外,也可以在录像再现系统100中具备多个母设备10。

[0062] 母设备10作为接收通过数字广播而分发的例如节目等的内容的接收机或者录像装置构成。母设备10使用内容密钥Kc对其接收的内容进行加密,并经由互联网向云服务器20录像。

[0063] 云服务器20针对经由互联网向云服务器20访问的设备提供云服务。云服务是存放由母设备10录像的被加密的内容、并向上述的设备发送该内容的服务。此外,云服务器20也可以被称为云录像服务器或者云服务器装置。

[0064] 子设备31~33各自是经由互联网访问云服务器20、并接收该云服务器20中存放的内容并再现的终端装置。此外,各个子设备31~33有时总称为子设备30。

[0065] 管理服务器40对子设备31~33、以及由母设备10与各个子设备31~33共享的共用密钥Kp进行管理。共用密钥Kp也被称为共通密钥或者共享密钥。

[0066] 此外,母设备10例如被设置在家庭内,该母设备10及子设备31~33通过家庭内网络连接。

[0067] 在这样的录像再现系统100中,具体进行以下的处理。

[0068] 例如,管理服务器40从子设备33经由互联网受理用户的新登记、云服务器20的登记。进而,管理服务器40将子设备31~33与母设备10建立关联地管理。进而,管理服务器40

对母设备权的转移进行管理。母设备权的转移,是从原录像装置向转移目的地的录像装置转移母设备权的处理,该母设备权是向云服务器20进行访问的母设备10的功能或者作用。仅由具有该母设备权的录像装置作为向云服务器20进行访问的母设备10发挥功能。此外,以下,有时将具有母设备权的录像装置和不具有母设备权的录像装置都表现为母设备10。

[0069] 进而,管理服务器40向母设备10和子设备31～33各自发行共用密钥Kp。例如,管理服务器40向母设备10及子设备32,发送由母设备10和子设备32共享的共用密钥Kp、以及为了向云服务器20访问而需要的云服务器登入信息。云服务器登入信息例如是后述的云账户名及云密码等信息。

[0070] 母设备10在将内容向云服务器20(即云服务)录像时,使用内容密钥Kc对该内容进行加密,并将被加密的内容向云服务录像。在图1中,记作母设备10直接经由网络将内容向云服务器20录像,但也可以基于按每个云服务使规格差(即差量)被智能手机吸收的方式,将智能手机用作网络路由器(即桥)的方式,经由智能手机将内容向云服务记录。由此,在每次追加所支持的云服务时,无需变更母设备10的嵌入软件,仅通过智能手机侧的软件更新就能够应对。母设备10仅仅总是访问智能手机,因此母设备10也可以不知晓与云服务相关的信息。

[0071] 另外,母设备10使用共用密钥Kp对该内容密钥Kc进行加密,并将被加密的内容密钥Kc经由互联网向子设备32发送。

[0072] 子设备32作为与母设备10建立关联的设备被登记在管理服务器40中。另外,子设备32向母设备10进行内容的再现请求。通过该再现请求,子设备32从母设备10取得通过共用密钥Kp被加密的内容密钥Kc。子设备32使用共用密钥Kp对该内容密钥Kc进行解密。然后,子设备32向管理服务器40中登记的云服务器20访问并登入,取得该云服务器20中存放的内容。进而,子设备32使用内容密钥Kc对该内容进行解密并再现。即,子设备32对流进行解码。

[0073] 另外,在录像再现系统100中使用的母设备10被替换为其他录像装置的情况、即进行母设备权的转移的情况下,例如,子设备33向管理服务器40登记新的母设备。母设备10向该新的母设备转发内容密钥Kc和云服务器登入信息。然后,母设备10删除内容密钥Kc等。

[0074] 此外,子设备31例如处于家庭内,且满足云利用必要条件。该云利用必要条件是指为了对云服务上记录的内容进行再现而规定的必要条件,决定对子设备、母设备(包括管理服务器)要求的内容。也就是说,子设备31能够经由互联网访问云服务器20,取得该云服务器20中存放的内容并再现。另外,子设备32例如处于家庭外,且满足远程视听必要条件。该远程视听必要条件例如是作为ARIB规格的地面数字电视广播运营规定ARIB TR-B14第5分册附录C数字广播接收机中的远程视听必要条件。进而,子设备32满足上述的云利用必要条件。也就是说,子设备32访问母设备10,如果在该母设备10中存放有内容,则子设备32能够取得该内容并再现,进而能够经由互联网访问云服务器20,并对该云服务器20中存放的内容进行再现。

[0075] 此外,在该图1中,说明了包括管理服务器40的系统的例子。但是,如后述的图5所示,也可以考虑使母设备10具有管理服务器40的功能的情形、以及使智能手机等子设备30侧具有管理服务器40的功能的一部分或全部的情形。在使智能手机等的子设备30侧具有管理服务器40的功能的情况下,母设备10从子设备30取得云服务的信息并访问云服务器20,这与上述的例子相同。但是,在子设备30访问云服务器20的情况下,信息在子设备30内封

闭,因此不发生向外部取得信息的情况。因此,适于从子设备30对云服务器20上的内容进行再现。但是,相反地,在子设备30有多台的情况下,由于无法共享信息,因此存在各个子设备30必须保持与云服务相关的信息的课题。另一方面,不设置管理服务器40对于系统负荷而言是很大的优点,因此也可以作为本公开的一个方式考虑。

[0076] 图2是简略地表示本实施方式中的录像再现系统100的构成的图。

[0077] 如图2所示,母设备10例如是在家庭内配置的录像装置,接收作为通过广播而分发的数字数据的节目等的内容。母设备10既可以使其接收的内容在电视图像接收机上作为影像及语音输出,也可以将其存放至记录介质。另外,本实施方式中的母设备10经由互联网与云服务器20、子设备30及管理服务器40连接。此外,云服务器20也可以被称为通用云服务。另外,子设备30既可以是图1所示的子设备31～33之中的任1个子设备,也可以由多个子设备构成的集合。

[0078] 此外,在本实施方式中,内容通过广播而分发,但也可以经由互联网分发。

[0079] 图3是表示录像再现系统100的母设备10及管理服务器40所具有的信息的一例的图。

[0080] 母设备10将内容的复制次数、内容的管理信息的校验和、以及内容密钥Kc分别作为信息保持。例如,这些信息被存放于母设备10所具备的存储器。

[0081] 复制次数是云服务器20中录像的内容的能够复制的次数。

[0082] 管理信息的校验和,是针对作为用于对云服务器20中录像的内容进行管理的信息的管理信息的校验和。例如在遵循BDAV(Blu-ray(注册商标)Disc Audio/Visual、蓝光盘音频/视频)规格对1个以上的内容进行录像的情况下,管理信息的校验和被用于判断云服务器20中的BDAV的有效性。也就是说,该校验和被用于判断遵循BDAV规格录像的1组内容(即盘整体)的有效性。此外,校验和也被称为管理信息校验和。另外,管理信息的具体例如图8所示。另外,每个内容的复制次数也被用于判断该内容的有效性。

[0083] 内容密钥Kc是被用于云服务器20中录像的内容的加密及解密的密钥。

[0084] 管理服务器40将管理列表作为信息保持。例如,管理列表被存放于管理服务器40所具备的存储器。该管理列表是对母设备10、子设备30及云服务器20进行管理的列表,例如包括图4所示的账户列表L1、子设备列表L3、云服务列表L4、母设备列表L5等。

[0085] 图4是表示管理服务器40的构成及管理服务器40所具有的信息的一例的图。

[0086] 管理服务器40具备账户管理部41、共用密钥管理部42、子设备管理部43、云服务账户管理部44和母设备管理部45。

[0087] 账户管理部41对表示1个以上的用户各自的账户信息L2的账户列表L1进行管理。账户列表L1例如具有1个用户的账户信息L2。账户信息L2包括用户的账户名与密码的组、以及母设备子设备关联列表。母设备子设备关联列表表示1个以上的母设备/子设备集合信息,该母设备/子设备集合信息表示由母设备ID、子设备ID、共用密钥ID以及有效期限构成的组。也就是说,在母设备子设备关联列表所表示的各组中,母设备ID、子设备ID、共用密钥ID及有效期限被建立关联。

[0088] 母设备ID是母设备10的识别信息,子设备ID是子设备30的识别信息。共用密钥ID是与该共用密钥建立了关联的信息,而且是由母设备ID的母设备10与子设备ID的子设备30共享的共用密钥的识别信息。有效期限是与该有效期限建立了关联的子设备ID所对应的子

设备30的认证有效期限。

[0089] 在该母设备子设备关联列表所表示的各组中,表示被进行了设备认证的母设备10及子设备30各自的识别信息。因此可以说,账户管理部41通过账户列表L1所表示的账户信息L2,对母设备10与子设备30的设备认证关系进行管理。

[0090] 此外,各组所表示的母设备ID既可以相互不同,也可以相同。另外,各组所包括的子设备ID的数量不限于1个,也可以是多个。

[0091] 共用密钥管理部42对1个以上的共用密钥Kp进行管理。具体而言,共用密钥管理部42按账户列表L1所包括的每个账户信息L2,对该账户信息L2所表示的1个以上的共用密钥ID各自所对应的共用密钥Kp进行管理。

[0092] 此外,在图4的例中,有效期限在账户信息L2的母设备子设备关联列表中与子设备ID及共用密钥ID建立关联地表示,但也可以不表示在母设备子设备关联列表中。在该情况下,共用密钥管理部42也可以按每个共用密钥ID,对具有由该共用密钥ID表示的共用密钥Kp的子设备30的有效期限进行管理。也就是说,有效期限作为共用密钥Kp的有效期限被管理。

[0093] 母设备管理部45对表示与1个以上的母设备10相关的信息的母设备列表L5进行管理。母设备列表L5关于家庭内网络中登记的1个以上的母设备10中的各个母设备,表示该母设备10的母设备ID、IP(互联网协议(Internet Protocol))地址、以及母设备密码。

[0094] 子设备管理部43对表示与1个以上的子设备30相关的信息的子设备列表L3进行管理。子设备列表L3关于家庭内网络中登记的1个以上的子设备30中的各个子设备,表示该子设备30的子设备ID、以及IP(互联网协议(Internet Protocol))地址。

[0095] 云服务账户管理部44对表示母设备10与云服务的关系的云服务列表L4进行管理。云服务列表L4按每个云服务,将与该云服务相关的信息和与母设备10相关的信息建立关联地表示。与云服务相关的信息,包括作为云服务的识别信息的云服务ID、表示该云服务所在之处的URL(统一资源定位符(Uniform Resource Locator))、以及为了利用云服务而需要的云账户名及云密码。与母设备10相关的信息包括母设备ID和母设备密码。

[0096] 在上述的母设备权的转移中,云服务账户管理部44对云服务列表L4的母设备ID进行更新。另外,在进行云服务的删除或者迁移时,云服务账户管理部44对该云服务列表L4进行更新。

[0097] 在图4的例中,管理服务器40保持了包括账户列表L1及子设备列表L3等的管理列表,但也可以由母设备10保持管理列表。

[0098] 图5是表示母设备10的构成及母设备10所具有的信息的一例的图。

[0099] 在母设备10具有管理列表的情况下,该母设备10替代管理服务器40而具备账户管理部41、共用密钥管理部42、子设备管理部43及云服务账户管理部44。在该情况下,在管理列表中,不包括与母设备10相关的信息。另外,如图5所示的例子那样,在母设备10具有管理列表的情况下,可以说该母设备10具备管理服务器40的功能。因此,在这样的情况下,录像再现系统100也可以不具备管理服务器40。

[0100] 此外,在图5所示的例中,母设备10是对应于多用户的装置,账户管理部41对表示多个用户各自的账户信息L2的账户列表L1进行管理。另一方面,母设备10也可以是对应于单用户的装置。在该情况下,管理服务器40不具有账户管理部41及账户列表L1,而直接对1

个账户信息L2进行管理。

[0101] 另外,在图5所示的例中,母设备10对共用密钥Kp进行管理,因此该共用密钥Kp在子设备30的设备认证时被提供给该子设备30并能够利用直到有效期限为止。

[0102] 图6是表示母设备10所具有的信息的其他例的图。

[0103] 母设备10如图6所示,具有作为与该母设备10所登记的云服务相关的信息的云服务信息L11或者L12。这样的云服务信息L11或者L12被存放于母设备10所具备的存储器。云服务信息L11表示母设备10所登记的云服务的云服务ID、URL、云账户名及云密码。

[0104] 另一方面,云服务信息L12表示母设备10所登记的云服务的云服务ID,而未表示URL、云账户名及云密码。此外,在本实施方式中的图9～图25所示的例中,母设备10不具有云服务信息L11,而具有云服务信息L12,使用该云服务信息L12进行处理。在该情况下,母设备10及子设备30在访问云服务时,每次都需要从管理服务器40取得云服务的URL、云账户名及云密码。

[0105] 另外,母设备10保持表示复制次数、管理信息的校验和以及内容密钥Kc的内容关联信息L13。具体而言,内容关联信息L13表示云服务ID、与由该云服务ID表示的云服务相关联的管理信息校验和、以及该云服务的节目管理列表。

[0106] 节目管理列表按作为云服务中录像的内容的每个节目,表示作为该节目的识别信息的节目ID、该节目的复制次数、以及该节目的内容密钥Kc。此外,节目ID例如也可以使用后述的图8所示的rpls文件的由5位数的数值构成的文件名。

[0107] 另外,在图6中,母设备10持有内容关联信息L13,但也考虑其全部或一部分由管理服务器40持有。通过在管理服务器40侧持有,无论母设备10的电源状态(接通/关断)如何,都能够从管理服务器40取得内容关联信息L13,即使母设备10的电源已关断,也能够从云服务20直接进行再现。

[0108] 图7是用于说明母设备权的转移的图。

[0109] 在母设备权的转移中,管理服务器40将云服务列表L4所表示的母设备ID和母设备密码改写。此时,在作为原母设备10的录像装置与新设为母设备10的转移目的地的录像装置之间,进行原母设备10所管理的复制次数、内容密钥Kc及管理信息校验和等的交接。进行管理服务器40中的改写以及录像装置间的交接这2个处理,母设备权的转移完成。

[0110] 此外,在母设备10具备管理服务器40的功能的情况、即录像再现系统100中不具备管理服务器40的情况下,如图5所示,在母设备10中存在云服务列表L4。因此,在录像装置间,不仅交接复制次数、内容密钥Kc、以及管理信息的校验和等,还交接云服务列表L4。但是,在这样的例中,在用户在转移动作中断开电源等的情况下,有可能非法复制母设备权,因此存在安全性上的漏洞。因此,在录像再现系统100中与母设备10分别地具备管理服务器40的方式,与母设备10具备管理服务器40的功能的方式相比,能够进一步提高安全性。

[0111] 另外,在母设备权转移时,也可以在录像装置间还交接共用密钥Kp及子设备30的设备认证状态。但是,关于设备认证,由于在子设备30侧也保持了母设备10的信息,因此仅通过母设备10及管理服务器40的处理,转移并未完结。因此,也可以不进行共用密钥Kp及子设备30的设备认证状态的交接,而由新的母设备10从子设备30的设备认证开始重新进行处理。在该情况下,与进行交接的情况相比,能够提高安全性的强度。

[0112] 图8是表示包括内容和管理信息的数据结构例的图。

[0113] 例如,云服务器20如图8所示,遵循BDAV规格的数据结构,存放1个以上的内容。在该数据结构中,在root目录中存在BDAV目录。BDAV目录是BDAV规格的源目录。在该BDAV目录中,存在文件“Info.bdav”、PLAYLIST目录、CLIPINF目录和STREAM目录。

[0114] 文件“Info.bdav”是BDAV目录以下的整体的管理信息,具有节目列表(即节目一览表)。例如,该文件“Info.bdav”的校验和或者哈希值被用于判定BDAV目录整体(即上述的盘整体)的有效性。也就是说,上述的管理信息校验和的一例是文件“Info.bdav”的校验和。

[0115] 在PLAYLIST目录中,存在“00001.rpls”等rpls文件。rpls文件表示节目名等的详细信息,进而表示CLIPINF目录所包括的clpi文件的再现顺序(脚本)。

[0116] 在CLIPINF目录中,存在“00100.clpi”等clpi文件。clpi文件是内容的管理信息,具有Audio/Video(音频/视频)的属性信息和再现用映射表。此外,在通过BDAV规格内对内容密钥Kc进行管理的情况下,内容密钥Kc由该clpi文件管理。另外,内容也被称为流、流数据或者流文件。

[0117] 通常,在内容刚录像后,与该内容相关的PLAYLIST目录的文件与CLIPINF目录的文件成为1:1的关系。在进行了节目结合的情况下,1个节目(即PLAYLIST目录的文件)有时也会参照CLIPINF目录的多个文件。反之,在进行了节目分割的情况下,PLAYLIST目录的多个文件有时也会参照(或者共享)CLIPINF目录的1个文件。此外,在节目结合及节目分割中,CLIPINF目录的文件及STREAM目录的文件不被变更,而仅对PLAYLIST目录的文件进行修正。此外,关于节目结合及节目分割,进行遵循BDAV规格的处理。

[0118] 在STREAM目录中,存在“00100.m2ts”等m2ts文件。该m2ts文件是相当于内容的流数据。在内容的再现中,最少需要该m2ts文件。另外,图8所示的数据结构之中的至少是包括m2ts文件的STREAM目录需要被配置于云服务上。另外,CLIPINF目录的文件与STREAM目录的文件处于1:1的关系。此外,在此以MPEG2 Transport(MPEG2传输)流为例进行了说明,因此设为M2TS,但在记录了4K广播的情况下记录MMT/TLV流,因此作为MMTS文件记录。文件的名字按存放流的每个容器而不同,但表示在其中记录流。

[0119] 在此,内容的有效性的判定由用户无法操作的母设备10进行。云服务器20中的内容的有效性通过第1判定方法及第2判定方法之中的至少1个来判定。

[0120] 在第1判定方法中,灵活利用管理信息的校验和或者哈希值等。例如,在云服务器20中遵循BDAV规格的管理信息的构造而记录内容的情况下,存在对盘整体进行管理的上述的“info.bdav”文件。如果总是对该文件的校验和进行更新,并持续对其在云服务器20及母设备10中进行同步,则能够判定盘整体的有效性。也就是说,母设备10和云服务器20各自反复同步执行“info.bdav”文件的校验和的更新。母设备10在由该母设备10更新的校验和与由云服务器20更新的校验和不同的情况下,判定为在由云服务器20的“info.bdav”文件管理的全部内容中包括无效的内容。在该情况下,复制次数也可以被保持于云服务器20。

[0121] 在第2判定方法中,母设备10对各个节目的复制次数进行管理。母设备10在每次进行内容的复制时,使该内容的复制次数减1。最终,如果该复制次数成为0,则母设备10从母设备10所具有的节目管理列表中,删除作为该内容的节目的条目自身。由此,假如非法制作正规的节目的COPY节目,反复进行正规的节目的复制,且云服务器20中的正规的节目被置换为COPY节目,也能够抑制规定数量以上的复制。

[0122] 仅通过第2判定方法,在实际上执行了针对内容的处理的定时,对复制次数进行确

认,根据该复制次数将内容判定为无效。因此,在用户好不容易选择了节目之后,才向用户提示该节目无效。另一方面,在第1判定方法中,能够在访问盘(即BDAV目录)的瞬间判定该盘是有效还是无效,因此能够迅速地向用户显示警告面板。

[0123] 另外,在本实施方式中,云服务器20基于遵循BDAV规格的形式保持内容,以使子设备30也能够直接访问云服务器20并对内容进行再现。也就是说,云服务器20不仅保持内容,而且保持该内容的管理信息。因此,子设备30如果使用能够对BDAV规格进行解释的应用软件(也被称为视听应用),从母设备10获得内容密钥Kc,则能够在该子设备30中执行包括云服务器20中存放的BDAV规格的管理信息的解释在内的再现处理。但是,在本实施方式中,在基本上,管理信息的解释由母设备10进行。其中,在子设备30如上所述安装对管理信息进行解释的视听应用的情况下,也可以在子设备30中封闭地进行包括该解释在内的再现处理。

[0124] 另一方面,为了尽可能减少被置于云服务器20中的信息,也可以在云服务器20中仅放置作为流数据的内容,而由母设备10保持其他管理信息。另外,也可以不是由母设备10而是由管理服务器40持有管理信息。在该情况下,如果使管理服务器40也持有内容密钥Kc,则能够与母设备10的设备状态完全隔离地从子设备30实现再现。

[0125] 在该情况下,子设备30向母设备10问询来实现内容列表(即节目一览表)的显示、被再现的节目的选择、再现位置的决定等。子设备30从母设备10获得流数据的URL(即提供流数据的云服务的URL),最后,仅仅是获得作为被再现的流数据的内容这一处理通过向云服务器20访问来进行。此外,在远程视听的情况下,母设备10对流数据进行解密,对其通过DTCP(数字传输内容保护(Digital Transmission Content Protection))进行保护(即加密)并向子设备30分发。

[0126] 另外,在管理信息被置于云服务器20中的情形1、以及管理信息被置于母设备10中的情形2之间,内容的有效性的判定方法也可以不同。在情形1的情况下,使用复制次数及校验和等进行有效性的判定。另一方面,在情形2的情况下,由于流数据以外的BDAV的管理信息全部处于母设备10,因此也可以无需这样的使用校验和判定有效性的处理。

[0127] 此外,在本实施方式中,作为数据结构的一例而使用了BDAV规格的数据结构。但是,在本实施方式中,只要是具有内容列表、各个内容的管理信息以及流文件的数据结构,则不限于BDAV规格的数据结构,可以使用任意的数据结构。

[0128] 图9是表示进行管理服务器40的账户制作及母设备10的登记时的录像再现系统100中的处理动作的一例的时序图。

[0129] 首先,例如作为个人计算机(也被称为PC)或者智能电话(也被称为智能手机)的子设备30访问管理服务器40(步骤S1)。然后,子设备30向管理服务器40指定账户名及密码,从而请求制作账户并登入(步骤S2)。

[0130] 管理服务器40向账户列表L1新追加账户信息L2,并在该账户信息L2中记录上述的被指定的账户名及密码(步骤S3)。

[0131] 另一方面,1个以上的母设备10各自例如响应于用户的输入操作,进行家庭内网络的设定,进而进行母设备密码的设定(步骤S15)。也就是说,1个以上的母设备10各自与家庭内网络连接,保持设备名、IP地址及母设备密码。此外,设备名由用户设定,但也可以替代于此,是唯一决定的母设备ID。

[0132] 子设备30探索与家庭内网络连接的1个以上的母设备10中的各个母设备,作为被

登记的母设备10的候选(步骤S4)。也就是说,子设备30从与家庭内网络连接的1个以上的母设备10中的各个母设备,取得该母设备10的设备名及IP地址(步骤S5)。然后,子设备30显示与家庭内网络连接的1个以上的母设备10的列表作为母设备候选列表(步骤S6)。在母设备候选列表中,例如表示上述的1个以上的母设备10各自的设备名及IP地址。子设备30响应于用户的登记操作,从母设备候选列表中决定被登记的母设备10(步骤S7)。然后,子设备30向该决定的母设备10输入母设备密码并尝试登入(步骤S8)。

[0133] 子设备30判定是否通过步骤S8的处理成功登入(步骤S9)。在此,子设备30如果判定为登入失败(步骤S9:否),则结束用于母设备10的登记的处理。另一方面,子设备30如果判定为登入成功(步骤S9:是),则从在步骤S8中登入的母设备10登出(步骤S10)。进而,子设备30向管理服务器40请求向管理服务器40所具有的母设备列表L5的登记、即在步骤S7中决定的母设备10的母设备ID、IP地址及母设备密码的登记(步骤S11)。管理服务器40响应于来自该子设备30的请求,向母设备列表L5登记母设备ID、IP地址及母设备密码(步骤S12)。

[0134] 接下来,子设备30向管理服务器40,指定在步骤S7中决定的母设备10的母设备ID及母设备密码,并请求向账户信息L2登记母设备(步骤S13)。管理服务器40响应于来自该子设备30的请求,将在步骤S7中决定的母设备10作为能够向云服务器20访问的母设备10向账户信息L2登记。即,管理服务器40将由子设备30指定的母设备ID向账户信息L2登记(步骤S14)。

[0135] 图10是表示进行云服务器20的云账户制作时的录像再现系统100中的处理动作的一例的时序图。

[0136] 首先,例如作为PC或者智能手机的子设备30向管理服务器40请求云服务登记处理(步骤S21)。管理服务器40响应于来自该子设备30的请求,向该子设备30请求云服务登记处理所需的信息的输入(步骤S22)。

[0137] 子设备30例如响应于用户的输入操作,受理云账户名、云密码、电子邮件地址及结算信息等的输入,作为云服务登记处理所需的信息的输入(步骤S23)。然后,子设备30将该信息向管理服务器40发送(步骤S24)。

[0138] 管理服务器40如果从子设备30接收到上述的信息,则将该信息向云服务器20发送,并且向云服务器20请求制作云账户(步骤S25)。云服务器20对该信息(即输入信息)进行检查,根据该信息的内容,制作云账户(步骤S26)。然后,云服务器20向管理服务器40通知云账户制作完成以及访问URL(步骤S27)。

[0139] 管理服务器40向云服务列表L4新追加与由云服务器20制作的云账户对应的云服务ID。进而,管理服务器40将从云服务器20通知的访问URL(即URL)与该云服务ID建立关联并向云服务列表L4登记。进而,管理服务器40将通过从子设备30发送的信息表示的云账户名以及云密码,与该云服务ID建立关联并向云服务列表L4登记(步骤S28)。

[0140] 然后,管理服务器40向子设备30通知云账户制作完成以及云服务ID(步骤S29)。

[0141] 图11是表示母设备10与云服务建立关联时的录像再现系统100中的处理动作的一例的时序图。此外,在图11的例中,通过该处理动作,向母设备10记录云服务ID。也就是说,母设备10保持图6所示的云服务信息L12。

[0142] 首先,子设备30响应于用户的输入操作,决定向云服务访问的母设备10(步骤S31)。然后,子设备30向管理服务器40输入与该云服务对应的云服务ID和被决定的母设备

10的母设备ID所成的组,从而设定向该云服务访问的母设备(步骤S32)。

[0143] 管理服务器40从母设备列表L5中探索该输入的母设备ID,取得在母设备列表L5中与该母设备ID建立了关联的母设备密码。进而,管理服务器40将该母设备ID及母设备密码与在步骤S32中输入的云服务ID建立关联并向云服务列表L4登记(步骤S33)。由此,母设备10与云服务建立关联。

[0144] 另一方面,母设备10受理用户的输入操作(步骤S34),并启动云录像设定(步骤S35)。然后,母设备10向管理服务器40输入母设备ID,并向管理服务器40问询能够利用的云服务(步骤S36)。

[0145] 管理服务器40响应于来自母设备10的问询,从云服务列表L4中,探索具有该母设备ID的条目(步骤S37)。也就是说,管理服务器40从云服务列表L4中,检索与该母设备ID建立了关联的云服务ID。然后,管理服务器40向母设备10发送该检索出的云服务ID(步骤S38)。母设备10如果从管理服务器40接收到云服务ID,则作为录像目的地追加云服务(步骤S39)。也就是说,母设备10将该接收的云服务ID向云服务信息L12记录。此外,在该图11所示的例中,母设备10在登入云服务时,每次都向管理服务器40问询与该云服务相关的详细信息(例如URL、云账户名及云密码等)。

[0146] 另外,子设备30在步骤S32的处理之后,从管理服务器40登出(步骤S40)。

[0147] 图12是表示母设备10与云服务建立关联时的录像再现系统100中的处理动作的其他例的时序图。此外,在图12的例中,通过该处理动作,在母设备10中不仅记录云服务ID而且也记录云账户名及云密码。也就是说,母设备10保持图6所示的云服务信息L11。

[0148] 首先,在录像再现系统100中,执行与图11所示的步骤S31～S36的处理同样的处理(步骤S41～S46)。

[0149] 接下来,管理服务器40响应于来自母设备10的问询,从云服务列表L4中,探索具有从母设备10输入的母设备ID的条目(步骤S47)。此时,管理服务器40从云服务列表L4中,检索与该母设备ID建立了关联的云服务ID、URL(即云URL)、云账户名及云密码。然后,管理服务器40将该检索出的云服务ID、URL、云账户名及云密码向母设备10发送(步骤S48)。母设备10如果从管理服务器40接收到云服务ID等,则作为录像目的地追加云服务(步骤S49)。也就是说,母设备10将该接收的云服务ID、URL、云账户名及云密码向云服务信息L11记录。此外,在该图12所示的例中,母设备10在登入云服务时,也可以不向管理服务器40问询与该云服务相关的详细信息。

[0150] 然后,子设备30在步骤S42的处理之后,从管理服务器40登出(步骤S50)。

[0151] 图13是表示进行子设备30的登记以及向母设备10建立关联时的录像再现系统100中的处理动作的一例的时序图。

[0152] 首先,例如作为智能手机的子设备30向管理服务器40输入账户名及密码并登入(步骤S51)。然后,子设备30将该子设备30的子设备ID及IP地址向管理服务器40发送,以使已登入的该子设备30被登记(步骤S52)。

[0153] 管理服务器40如果从子设备30接收到子设备ID及IP地址,则在子设备列表L3中将该子设备ID及IP地址相互建立关联并登记(步骤S53)。然后,管理服务器40向子设备30通知该子设备30的登记完成(步骤S54)。

[0154] 子设备30如果接受到来自管理服务器40的通知,则从管理服务器40取得母设备列

表L5(步骤S55)。此外,从该母设备列表L5中省去母设备密码。然后,子设备30响应于用户的输入操作,从该母设备列表L5中决定母设备10(步骤S56)。也就是说,子设备30从母设备列表L5所表示的1个以上的母设备10中,选择从该子设备30访问的母设备10。进而,子设备30向管理服务器40输入该子设备30的子设备ID、以及从母设备列表L5中决定的母设备10的母设备ID及母设备密码,并向管理服务器40请求向该母设备10的访问设定(步骤S57)。

[0155] 管理服务器40响应于来自子设备30的请求,判定被输入的母设备ID及母设备密码是否正确(步骤S58)。也就是说,管理服务器40进行使用该母设备ID及母设备密码的向母设备10的访问检查,从而判定该母设备ID及母设备密码是否正确。在该母设备ID及母设备密码正确的情况下,管理服务器40在账户信息L2中制作母设备/子设备集合信息,从而将子设备30与母设备10建立关联并登记(步骤S60)。母设备/子设备集合信息是将被判定为正确的母设备ID、向管理服务器40进行了请求的子设备30的子设备ID、共用密钥ID、共用密钥Kp的有效期限建立关联并表示的信息。也就是说,管理服务器40设定有效期限,生成共用密钥Kp,并向该共用密钥Kp分配共用密钥ID。通过这样的步骤S57～S60,在母设备10与子设备30之间进行设备认证。然后,管理服务器40向子设备30通知共用密钥Kp(步骤S61),并向与该子设备30建立了关联的母设备10也通知共用密钥Kp(步骤S62)。

[0156] 此外,在图13的例中,在步骤S61及S62的定时向子设备30及母设备10通知共用密钥Kp,但也可以在其他定时通知。例如,也可以在云服务的内容被再现的定时,母设备10及子设备30各自向管理服务器40指定母设备ID、子设备ID及云服务ID,并向管理服务器40请求共用密钥Kp的通知。

[0157] 另外,在本实施方式中,在步骤S58中进行向母设备10的访问检查,但也可以不进行该访问检查。但是,在母设备10的密码有可能变更的情况下,进行这样的访问检查为佳。

[0158] 图14是表示母设备10将内容向云服务录像时的录像再现系统100中的处理动作的一例的时序图。

[0159] 首先,母设备10响应于用户的输入操作,受理以云服务作为录像目的地的录像的开始(步骤S65)。接下来,母设备10使用该母设备10的母设备ID及母设备密码向管理服务器40登入,并向管理服务器40请求云服务器20(即云服务)的URL、云账户名及云密码(步骤S66)。管理服务器40响应于来自母设备10的请求,向母设备10通知云服务器20的URL、云账户名及云密码(步骤S67)。

[0160] 母设备10如果接受了来自管理服务器40的通知,则从管理服务器40登出(步骤S68),并使用该URL、云账户名及云密码登入云服务(步骤S69)。进而,母设备10向云服务器20请求制作管理信息(步骤S70)。此外,该管理信息也可以是图8所示的数据结构之中的除了流文件(即m2ts文件)以外的各种信息。

[0161] 接下来,母设备10反复执行步骤S71～S75的处理直到录像停止为止。例如,步骤S71～S75的处理按被广播的内容的每个块执行。具体而言,母设备10对被广播的内容进行解析,取得该内容的属性信息、用于特殊再现的映射信息等(步骤S71)。此外,用于特殊再现的映射信息例如在MPEG2Video(MPEG2视频)中是每个GOP(图片组(Group of Picture)s)的管理表,对流文件内的地址、时间码、IPIC大小进行管理。同样在H.264、H.265中也在每次检测出Stream(流)内的Ipic时,制作用于特殊再现的映射信息。这样的用于特殊再现的映射信息在跳转再现、特殊再现等中使用,在通常再现时也被用于导出开始地址。接下来,母设

备10使用内容密钥Kc,对作为内容的流数据进行加密(步骤S72)。母设备10向云服务器20请求该被加密的流数据的写入(步骤S73)。进而,母设备10进行管理信息的更新(步骤S74),并向云服务器20请求管理信息的更新(步骤S75)。

[0162] 然后,母设备10例如响应于用户的输入操作,如果受理了录像停止的指示(步骤S76),则向云服务器20请求管理信息的CLOSE(关闭)(步骤S77)。进而,母设备10向云服务器20请求流数据的CLOSE(步骤S78)。然后,母设备10记录内容密钥Kc及复制次数(步骤S79),并从云服务器20登出(步骤S80)。

[0163] 图15是表示母设备10对云服务中的内容进行再现时的录像再现系统100中的处理动作的一例的时序图。

[0164] 首先,母设备10将该母设备10的母设备ID及母设备密码向管理服务器40输入并登入(步骤S81)。接下来,母设备10将云服务ID向管理服务器40输入,从管理服务器40取得与该云服务ID建立了关联的云账户名、云密码及URL(步骤S82)。进而,母设备10向通过该URL表示的云服务输入云账户名及云密码并登入(步骤S83)。然后,母设备10从该云服务(即云服务器20),从管理信息中读出作为被录像的内容的一览表的节目一览表从而取得该节目一览表(步骤S84)。

[0165] 母设备10显示该取得的节目一览表,例如响应于用户的输入操作,从该节目一览表中选择要再现的节目,并开始用于对作为该节目的内容进行再现的处理(步骤S85)。也就是说,母设备10从云服务器20取得该节目的管理信息(步骤S86),并从该管理信息取得流文件名(步骤S87)。接下来,母设备10使用流路径在云服务内进行探索,访问该流文件名的流文件并进行OPEN(打开)(步骤S88)。

[0166] 然后,母设备10反复进行步骤S89及S90的处理直到再现停止为止。也就是说,母设备10对该流文件(即流数据)之中的加密块的整数倍的大小的数据进行READ(读取)(步骤S89)。接下来,母设备10使用内容密钥Kc对流文件的数据进行解密,并对该数据以GOP单位进行解码(步骤S90)。此外,加密的单位(即加密块)与解码的单位(即GOP)相互不同。加密的单位是固定长度,而解码的单位是可变长度。由此,解码结果向TV等的监视器画面输出,从而实现再现。

[0167] 接下来,母设备10向云服务器20请求流文件的CLOSE(步骤S91),并从云服务器20登出(步骤S92)。进而,母设备10从管理服务器40登出(步骤S93)。步骤S93既可以在该定时执行,也可以在刚进行步骤S82后实施。

[0168] 图16是表示子设备30对云服务中的内容进行再现时的录像再现系统100中的处理动作之中的第1处理动作的一例的时序图。

[0169] 首先,例如作为智能手机的子设备30将账户名及密码向管理服务器40输入并登入(步骤S95)。然后,子设备30将母设备ID向管理服务器40输入,并从管理服务器40取得与该母设备ID建立了关联的IP地址(步骤S96)。接下来,子设备30向与该母设备ID及IP地址对应的母设备10,输入母设备密码并登入(步骤S97)。进而,子设备30选择被设为再现目的地的云服务,并向上述的母设备10指定该云服务(步骤S98)。此时,在母设备10将多个云服务设为录像目的地的情况下,与内置HDD或光盘等并列地对云服务进行列表显示,成为供用户从其中选择要再现的云服务的操作的图像。

[0170] 母设备10将该母设备10的母设备ID及母设备密码向管理服务器40输入并登入(步

骤S99)。然后,母设备10将自身保持的云服务ID向管理服务器40输入,从管理服务器40取得与该云服务ID建立了关联的云账户名、云密码及URL,并登出(步骤S100)。母设备10向与该取得的URL对应的云服务器20,输入取得的云账户名及云密码并登入(步骤S101)。然后,母设备10通过从该云服务器20读出管理信息来取得节目一览表(步骤S102),并将上述的云服务ID和节目一览表向子设备30提供(步骤S103)。

[0171] 子设备30从该提供的节目一览表中,决定要再现的节目(步骤S104),向母设备10指定被决定的节目,而且向母设备10请求该节目的内容密钥Kc和流文件的URL(步骤S105)。

[0172] 接受了该请求的母设备10从云服务器20取得该节目的管理信息(步骤S106)。进而,母设备10从该管理信息中取得流文件名,生成流路径(步骤S107)。然后,母设备10使用该流路径从云服务器20中探索上述的流文件名的流文件,并取得该流文件的URL(步骤S108)。或者,母设备10也可以根据用于访问云服务器20的URL,生成用于访问流文件的URL。对此,考虑到按每个云服务而作法不同,因此只要能够取得通过与该服务器相应的方法能够访问流文件的信息即可。

[0173] 图17是表示子设备30对云服务中的内容进行再现时的录像再现系统100中的处理动作之中的第2处理动作的一例的时序图。此外,第2处理动作是后续于第1处理动作而进行的动作。

[0174] 母设备10在图16的步骤S108的处理之后,使用共用密钥Kp对流文件的内容密钥Kc进行加密(步骤S110)。进而,母设备10将该被加密的内容密钥Kc和流文件的URL向子设备30提供(步骤S111)。

[0175] 子设备30如果取得了该被加密的内容密钥Kc,则使用共用密钥Kp对该内容密钥Kc进行解密(步骤S112)。然后,子设备30将在步骤S103中被提供的云服务ID向管理服务器40输入,并向管理服务器40请求与该云服务ID建立了关联的云账户名、云密码及URL(步骤S113)。管理服务器40响应于来自子设备30的请求,向子设备30提供云账户名、云密码及URL(步骤S114)。

[0176] 子设备30向与该被提供的URL对应的云服务器20,输入被提供的云账户名及云密码并登入(步骤S115)。进而,子设备30向该云服务器20指定流文件的URL并对该流文件进行OPEN(步骤S116)。进而,子设备30反复执行步骤S117及S118的处理直到再现停止为止。也就是说,子设备30对该流文件(即流数据)之中的加密块的整数倍的大小的数据进行READ(步骤S117)。接下来,子设备30使用内容密钥Kc对流文件的数据进行解密,并对该数据以GOP单位进行解码(步骤S118)。将该解码的结果显示在子设备30所具备的输出设备上来实现再现。

[0177] 进而,子设备30对云服务器20的流文件进行CLOSE(步骤S119)。接下来,子设备30从云服务器20登出(步骤S120),并从母设备10登出(步骤S121)。结果,母设备10从云服务器20登出(步骤S122)。然后,子设备30也从管理服务器40登出(步骤S123)。

[0178] 此外,在图17的例中,在步骤S115中进行登入,但也可以省去该登入。在云服务器20的设定中设定为从谁都能够访问的情况下,不特别需要登入,也有在利用URL访问的情况下能够立即以READ ONLY(只读)方式访问文件的情形,在设想为这种情形的情况下,能够省去登入。

[0179] 图18是表示母设备10对云服务中的内容进行复制时的录像再现系统100中的处理

动作的一例的时序图。

[0180] 首先,母设备10例如响应于用户的输入操作,选择云服务器20中的盘作为复制对象(步骤S125)。接下来,母设备10将该母设备10的母设备ID及母设备密码向管理服务器40输入并登入(步骤S126)。进而,母设备10将云服务ID向管理服务器40输入,从管理服务器40取得与该云服务ID建立了关联的云账户名、云密码及URL(步骤S127),并从该管理服务器40登出(步骤S128)。

[0181] 接下来,母设备10向与该URL对应的云服务器20,输入云账户名及云密码并登入(步骤S129),并从该云服务器20中,通过从管理信息读出来取得节目一览表(步骤S130)。此外,该节目一览表也可以被称为云录像节目列表或者节目列表。母设备10例如响应于用户的输入操作,从该节目一览表中决定作为要复制的节目的内容,并受理向光盘复制的开始执行(步骤S131)。

[0182] 其后,母设备10从云服务器20读出要复制的节目的管理信息(步骤S132),并向母设备10中配置的光盘写入该节目的管理信息(步骤S133)。然后,母设备10从云服务器20中读出要复制的节目的流数据(步骤S134)。母设备10使用内容密钥对该读出的流数据进行解密,进而,进行光盘用的加密,并将被加密的流数据向光盘记录(步骤S135)。母设备10针对该节目的复制次数(也被称为DUB次数),例如通过使其减少来进行更新(步骤S136)。在此,母设备10在更新的结果是DUB次数成为0的情况下,删除该节目的内容密钥,并删除云服务(即云服务器20)上的节目(步骤S137)。然后,母设备10从云服务器20登出(步骤S138)。

[0183] 图19是表示子设备30对该子设备30的登记进行删除时的录像再现系统100中的处理动作的一例的时序图。

[0184] 首先,例如作为智能手机的子设备30将账户名及密码向管理服务器40输入并登入(步骤S141)。接下来,子设备30将该子设备30的子设备ID向管理服务器40输入并请求删除子设备(步骤S142)。

[0185] 管理服务器40响应于来自子设备30的请求,从子设备列表L3中探索要删除的子设备30的子设备ID,并删除具有该子设备ID的条目(步骤S143)。也就是说,管理服务器40从子设备列表L3删除该子设备ID以及与该子设备ID建立了关联的IP地址。接下来,管理服务器40从账户信息L2检索具有该子设备ID的母设备/子设备集合信息,并删除作为该母设备/子设备集合信息的条目(步骤S144)。然后,子设备30从管理服务器40登出(步骤S145)。

[0186] 图20是表示子设备30对其他子设备30的登记进行删除时的录像再现系统100中的处理动作的一例的时序图。例如,子设备30是PC,其他子设备30是智能手机。

[0187] 首先,PC将账户名及密码向管理服务器40输入并登入(步骤S146)。然后,PC向管理服务器40请求子设备列表L3(步骤S147)。

[0188] 管理服务器40响应于来自PC的请求,将子设备列表L3向PC发送(步骤S148)。PC如果接收到该子设备列表L3,则例如响应于用户的输入操作,从该子设备列表L3中决定要删除的子设备30(即智能手机)(步骤S149)。然后,PC将该决定的智能手机的子设备ID向管理服务器40输入并请求删除子设备(步骤S150)。

[0189] 管理服务器40响应于来自PC的请求,从子设备列表L3中探索要删除的智能手机的子设备ID,并删除具有该子设备ID的条目(步骤S151)。也就是说,管理服务器40从子设备列表L3删除该子设备ID以及与该子设备ID建立了关联的IP地址。接下来,管理服务器40从账

户信息L2检索具有该子设备ID的母设备/子设备集合信息,并删除作为该母设备/子设备集合信息的条目(步骤S152)。然后,PC从管理服务器40登出(步骤S153)。

[0190] 图21是表示子设备30对云服务进行变更时的录像再现系统100中的处理动作所包括的第1处理动作的一例的时序图。

[0191] 首先,例如作为PC的子设备30将账户名及密码向管理服务器40输入并登入(步骤S161),向管理服务器40请求云服务登记处理(步骤S162)。管理服务器40响应于来自该子设备30的请求,向该子设备30请求云服务登记处理所需的信息的输入(步骤S163)。

[0192] 子设备30例如响应于用户的输入操作,受理云账户名、云密码、电子邮件地址及结算信息等的输入,作为云服务登记处理所需的信息的输入(步骤S164)。然后,子设备30将该信息向管理服务器40发送(步骤S165)。

[0193] 管理服务器40如果从子设备30接收到上述的信息,则将该信息向云服务器20发送,并且向云服务器20请求制作云账户(步骤S166)。云服务器20对该信息(即输入信息)进行检查,并根据该信息的内容,制作云账户(步骤S167)。然后,云服务器20向管理服务器40通知云账户制作完成以及访问URL(步骤S168)。管理服务器40如果受理了来自云服务器20的通知,则向子设备30通知云账户制作完成(步骤S169)。

[0194] 子设备30如果接受了云账户制作完成的通知,则从管理服务器40取得云服务列表L4(步骤S170),并从该的云服务列表L4中确定子设备30当前能够利用的云服务(步骤S171)。此外,也可以从向子设备30提供的云服务列表L4中省去云密码及母设备密码(在由母设备10的管理列表进行管理的情况下)。接下来,子设备30从管理服务器40取得与该确定的云服务的母设备ID建立了关联的IP地址(即母设备IP地址)(步骤S172)。

[0195] 图22是表示子设备30对云服务进行变更时的录像再现系统100中的处理动作之中的第2处理动作的一例的时序图。此外,第2处理动作是后续于第1处理动作而进行的动作。

[0196] 子设备30使用在图21的步骤S172中取得的母设备IP地址、以及与该母设备IP地址对应的母设备10的母设备密码,尝试向该母设备10登入(步骤S175)。然后,子设备30判定是否通过步骤S175的处理成功登入(步骤S179)。在此,子设备30如果判定为登入失败(步骤S179:否),则结束子设备30的用于对云服务进行变更的处理。另一方面,子设备30如果判定为登入成功(步骤S179:是),则向管理服务器40请求从原云服务的条目中删除该母设备10的母设备ID及母设备密码(步骤S180)。此外,原云服务是在图21的步骤S171中确定的云服务。也就是说,请求删除云服务列表L4之中的与原云服务的云服务ID建立了关联的母设备ID及母设备密码。

[0197] 管理服务器40响应于来自子设备30的请求,从原云服务的条目中,删除母设备ID及母设备密码(步骤S181)。

[0198] 接下来,子设备30向管理服务器40请求向新的云服务的条目设定母设备ID及母设备密码(步骤S182)。管理服务器40响应于来自子设备30的请求,向新的云服务的条目设定母设备ID及母设备密码(步骤S183)。此外,新的云服务是与在图21的步骤S167中制作的云账户对应的云服务。也就是说,将母设备ID及母设备密码与云服务列表L4中的表示新的云服务的云服务ID建立关联。

[0199] 然后,子设备30向母设备10请求删除与原云服务建立了关联的管理信息校验和、复制次数及内容密钥Kc(步骤S184)。进而,子设备30向母设备10通知新的云服务的云服务

ID(步骤S185),并从母设备10登出(步骤S186)。

[0200] 在步骤S184、S185中,从子设备30向母设备10请求处理,但也可以由管理服务器40向母设备10请求。另外,在图22的例中,未记载关于云服务器20上的内容的删除的处理。这是因为,该内容成为无法再现的数据。但是,由于该内容作为多余的数据残留,因此子设备30或管理服务器40也可以在执行步骤S184的定时向云服务器20请求记录节目的删除或格式化。

[0201] 图23是表示进行母设备权的转移时的录像再现系统100中的处理动作之中的第1处理动作的一例的时序图。

[0202] 首先,例如作为智能手机的子设备30将账户名及密码向管理服务器40并登入(步骤S191),并向管理服务器40请求云服务列表L4(步骤S192)。管理服务器40响应于来自子设备30的请求,将云服务列表L4向子设备30发送(步骤S193)。此外,也可以从向子设备30提供的云服务列表L4中省去云密码及母设备密码。

[0203] 子设备30如果接收到云服务列表L4,则例如响应于用户的输入操作,从该云服务列表L4中决定设为母设备权的转移对象的云服务(以下也被称为处理对象云服务)(步骤S194)。在母设备权的转移中,变更与该处理对象云服务建立了关联的母设备10。接下来,子设备30向管理服务器40请求从家庭内网络对母设备进行再探索(步骤S195)。管理服务器40响应于来自子设备30的请求,将母设备列表L5向子设备30发送(步骤S196)。此外,从母设备列表L5中省去母设备密码。

[0204] 子设备30如果接收到母设备列表L5,则从该母设备列表L5中,选择与处理对象云服务建立了关联的母设备10(以下也被称为转移源的母设备10)、以及与处理对象云服务新建立关联的母设备(以下也被称为转移目的地的母设备10),并向管理服务器40指定。也就是说,子设备30向管理服务器40输入处理对象云服务的云服务ID、转移源的母设备10的母设备ID及母设备密码、以及转移目的地的母设备10的母设备ID及母设备密码,并请求母设备10的变更(步骤S197)。

[0205] 管理服务器40响应于来自子设备30的请求,判定转移源的母设备10的母设备ID及母设备密码,与处理对象云服务的条目中的母设备ID及母设备密码是否分别一致(步骤S198)。此外,处理对象云服务的条目中的母设备ID及母设备密码,是在云服务列表L4中与处理对象云服务的云服务ID建立了关联的母设备ID及母设备密码。在此,管理服务器40如果判定为不一致(步骤S199:否),则结束用于母设备权的转移的处理,如果判定为一致(步骤S199:是),则向第1母设备登入(步骤S200)。第1母设备是上述的转移源的母设备10。

[0206] 另外,作为上述的转移目的地的母设备10的第2母设备例如响应于用户的输入操作,进行家庭内网络的设定,进而,进行母设备密码的设定(步骤S201)。也就是说,第2母设备与家庭内网络连接,保持母设备ID、IP地址及母设备密码。

[0207] 图24是表示进行母设备权的转移时的录像再现系统100中的处理动作之中的第2处理动作的一例的时序图。此外,第2处理动作是后续于第1处理动作而进行的动作。

[0208] 管理服务器40使用作为转移目的地的母设备10的第2母设备的母设备ID及母设备密码,尝试向该第2母设备登入(步骤S211)。管理服务器40判定是否通过步骤S211的处理成功登入(步骤S213)。在此,管理服务器40如果判定为登入失败(步骤S213:否),则结束用于母设备权的转移的处理。另一方面,管理服务器40如果判定为登入成功(步骤S213:是),则

向第1母设备请求管理信息校验和、内容密钥集合及复制次数等的信息，并从第1母设备取得该信息(步骤S214)。此外，内容密钥集合由1个以上的内容密钥Kc构成。进而，管理服务器40向第2母设备请求写入作为该取得的信息的管理信息校验和、内容密钥集合、复制次数等的信息，并将该信息向第2母设备写入(步骤S215)。

[0209] 接下来，管理服务器40对云服务列表L4的云服务的条目中的母设备ID进行更新(步骤S216)。也就是说，管理服务器40将云服务列表L4中与处理对象云服务的云服务ID建立了关联的母设备ID，从第1母设备的母设备ID变更为第2母设备的母设备ID。进而，管理服务器40向第1母设备请求删除第1母设备所具有的管理信息校验和、内容密钥集合及复制次数等的信息(步骤S217)。然后，管理服务器40从第1母设备登出(步骤S218)，从第2母设备登出(步骤S219)，并向子设备30通知转移作业完成(步骤S220)。子设备30如果接受了转移作业完成的通知，则从管理服务器40登出(步骤S221)。

[0210] 图25是表示进行母设备10的转让时的录像再现系统100中的处理动作的一例的时序图。

[0211] 首先，例如作为智能手机的子设备30将账户名及密码向管理服务器40输入并登入(步骤S231)。接下来，子设备30向管理服务器40输入被转让的母设备10的母设备ID及母设备密码，并向管理服务器40请求删除母设备10(步骤S232)。

[0212] 管理服务器40响应于来自子设备30的请求，从母设备列表L5中检测该母设备ID，并确定与该母设备ID建立了关联的母设备密码(步骤S233)。然后，管理服务器40判定该确定的母设备密码是否与在步骤S232中输入的母设备密码一致(步骤S234)。在此，管理服务器40如果判定为母设备密码不一致(步骤S234:否)，则结束用于母设备10的转让的处理。另一方面，管理服务器40如果判定为母设备密码一致(步骤S234:是)，则从母设备列表L5中删除在步骤S232中输入的母设备ID的条目。进而，管理服务器40从云服务列表L4中清除该母设备ID，并从账户信息L2的母设备子设备关联列表中删除该母设备ID的条目(即母设备/子设备集合信息)(步骤S235)。

[0213] 另外，被转让的母设备10例如响应于用户的输入操作，将该母设备10所保持的个人信息复位(步骤S236)。

[0214] (实施方式的汇总)

[0215] 如上，本实施方式中的子设备30是被用于录像再现系统100的终端装置。也就是说，录像再现系统100包括:作为云服务器20的云服务器装置、作为母设备10的录像装置、以及作为子设备30的终端装置。录像装置接收被分发的内容并加密，将被加密的内容经由互联网向云服务器装置录像。终端装置再现该内容。这样的终端装置具备电路以及与该电路连接的存储器。电路使用该存储器，在与录像装置之间进行设备认证，从录像装置取得被加密的内容密钥，使用由录像装置与终端装置共享的共用密钥对该内容密钥进行解密，不经由录像装置而访问云服务器装置，读出该云服务器装置中被录像而且被加密的内容，使用内容密钥对读出的内容进行解密并再现。

[0216] 例如，在以往的远程视听中，母设备及子设备各自支持DTCP等的内容保护技术。在此基础上，在母设备与子设备之间进行设备认证，保证个人使用的范围内的视听。这基于通过母设备保持内容且不经由母设备就无法再现该内容的系统构成而得到的制约而成立。但是，在内容向云服务器装置的录像(即云录像)中，内容的录像目的地有时是通用的云服务

器装置。也考虑到这样的通用的云服务器装置不支持DTCP等的情况,而且,作为向云服务器装置中的内容的访问,只要知晓该内容或者云服务器装置的URL,则任意的PC都能够进行访问。另外,该PC无需经由母设备访问内容。在这样的状况下,在上述的专利文献1及2的技术中,难以充分保持内容并且保证个人使用的范围并向用户提供自由的再现功能。

[0217] 但是,本实施方式中的作为子设备30的终端装置在与作为母设备的录像装置之间进行设备认证,从该录像装置取得被加密的内容密钥Kc,并使用该内容密钥Kc,对从云服务器装置读出的内容进行解密并再现。因此,终端装置在从云服务器装置直接再现内容的情况下,能够充分保护该内容,并且保证个人使用的范围,向用户提供自由的再现功能。也就是说,能够实现恰当的子设备访问控制。

[0218] 另外,在本实施方式中的终端装置(即子设备30)中,电路经由管理服务器40在与母设备10之间进行设备认证,由此取得从管理服务器40向子设备30及母设备10发送的共用密钥Kp。由此,共用密钥Kp通过设备认证而在子设备30与母设备10之间共享,因此能够提高安全性的强度。

[0219] 另外,本实施方式中的录像管理系统是被用于录像再现系统100的系统。也就是说,录像再现系统100包括:作为云服务器20的云服务器装置、录像管理系统、以及作为子设备30的终端装置。录像管理系统接收被分发的内容并加密,将被加密的内容经由互联网向云服务器装置录像。终端装置再现该内容。具体地,录像管理系统具备电路以及至少1个存储器,该至少1个存储器将有效性判定信息和内容密钥与云服务器装置建立关联地保持。电路从至少1个存储器读出内容密钥并用于上述的内容的加密,从至少1个存储器读出有效性判定信息,并使用该有效性判定信息判定云服务器装置中录像的内容的有效性。此外,录像管理系统也可以具备作为母设备10的录像装置、以及作为管理服务器40的管理服务器装置。也就是说,录像管理系统具备将内容向云服务器装置进行录像的录像装置、以及与该录像装置经由互联网连接的管理服务器装置。在该情况下,上述的电路及至少1个存储器各自被配置于录像装置或者管理服务器装置。另外,有效性判定信息是表示针对内容的管理信息的校验和、哈希值、以及内容的复制次数之中的至少1个的信息。

[0220] 在此,如上述的专利文献1及2中也记载的那样,与模拟数据相比,数字数据的复制、窜改等非常容易。另外,在作为数字数据的内容的录像目的地利用云服务器装置的情况下,从PC等任意的设备都能够访问该云服务器装置,因此该内容的复制等非法使用更加容易。在以往的录像机对内容的录像中,内容和与内容的保护相关的信息(内容密钥、复制次数等)一起被记录至HDD(硬盘驱动器(Hard Disk Drive))内。在这样的方式中,利用独立文件系统,或者在从用户无法访问的区域中保持有设备绑定信息。例如,在SQV(SeeQVault(注册商标))、BD盘(Blu-ray(注册商标)Disc)等中,在需要安全访问的区域中存放有信息,防止非法的COPY。但是,在将内容向云服务器装置录像的情况下,从任意的PC等都能够访问该内容,也能够进行文件操作,因此如果内容是文件,则有可能简单地制作该内容的COPY。另外,在云服务器装置是通用的云服务器装置的情况下,使该云服务器装置支持安全访问等是不现实的。

[0221] 于是,在本实施方式中的录像管理系统中,与内容保护相关的信息不是在云服务器装置中,而是在作为从不特定的用户无法访问的区域的上述的至少1个存储器中,在与云服务器装置建立了关联的状态下被管理。与内容保护相关的信息,是有效性判定信息或者

内容密钥。由此,在录像管理系统、即母设备10或者管理服务器40中,与云服务器装置相关联的有效性判定信息(管理信息的校验和、哈希值、每个节目的复制次数等)及内容密钥被管理,因此能够实现即使非法制作了内容的COPY、其也被视为无效而无法再现的框架。也就是说,能够实现云服务上的恰当的非法COPY对策。

[0222] 此外,有效性判定信息也可以是用于判断内容的有效性的标记。

[0223] 另外,在本实施方式中的录像管理系统中,在录像管理系统和云服务器装置各自中对管理信息进行保持并更新的情况下,录像管理系统的电路对根据录像管理系统的管理信息得到的有效性判定信息,与根据云服务器装置的管理信息得到的有效性判定信息进行比较,从而判定云服务器装置中录像的内容的有效性。由此,录像管理系统的有效性判定信息与云服务器装置的有效性判定信息被比较,例如,如果它们相互不同,则判定为该内容无效。结果,能够恰当地判定内容的有效性。

[0224] 另外,本实施方式中的管理服务器40是被用于录像再现系统100的管理服务器装置。也就是说,录像再现系统100具备:作为云服务器20的云服务器装置、作为母设备10的第1录像装置、作为子设备30的终端装置、以及作为管理服务器40的管理服务器装置。第1录像装置接收被分发的内容并加密,将被加密的内容经由互联网向云服务器装置录像。终端装置再现该内容。管理服务器装置与第1录像装置经由互联网连接。这样的管理服务器装置具备电路以及与该电路连接的存储器。该存储器将用于识别第1录像装置的第1识别信息与云服务器装置建立关联地保持。电路在第1录像装置被替换为第2录像装置的情况下,将与云服务器装置建立关联地保持在存储器中的第1识别信息,置换为用于识别第2录像装置的第2识别信息,并将用于保护内容且在第1录像装置中保持的保护信息转移至第2录像装置。该保护信息例如表示内容密钥、管理信息的校验和或哈希值、复制次数等。

[0225] 以往也存在录像机间的录像节目的转移及复制功能。但是,在这样的录像节目的转移中,录像节目处于录像机的内置HDD内或者被进行了设备绑定的USB(通用串行总线(Universal Serial Bus))-HDD内,因此需要录像节目自身的移动。如果将这样的以往的方法也适用于将内容向云服务器20录像的云录像,则会发生如下麻烦:一旦从云服务器20将录像节目的数据读出并对其进行解密,而且为了对其通过DTCP进行收发而进行加密,并在转移目的地对其再次进行解密之后,通过本地密码进行加密并向内置HDD等记录。也就是说,转移对象是录像节目自身,该录像节目被记录在录像机内,因此需要使录像节目自身移动。因此非常费事。

[0226] 但是,在云录像中,如果着眼于数据(即录像节目)处于云服务器20这一点,则不一定需要移动录像节目,只要向云服务器20的录像节目的访问权以及表示数据的有效性的信息(即保护信息)能够移动即可。

[0227] 因此,本实施方式中的管理服务器装置如上所述,在第1录像装置被替换为第2录像装置的情况下,将与云服务器装置建立了关联的第1录像装置的第1识别信息,置换为第2录像装置的第2识别信息。即,向云服务器装置的内容的访问权被转移至第2录像装置。进而,管理服务器装置将第1录像装置中保持的保护信息转移至第2录像装置。

[0228] 由此,能够充分保护内容,并且省事而且容易地进行母设备10的转移、即母设备权从第1录像装置向第2录像装置的转移。另外,这样的转移可以认为在个人的利用范围内而且不超出个人使用的范畴。也就是说,能够实现恰当的母设备10的转移。

[0229] 另外,本实施方式中的管理服务器装置的电路在第1录像装置被从录像再现系统100移除的情况下,执行(a)由第1录像装置向云服务器装置录像的内容的删除、(b)第1录像装置或者存储器中保持的用于向云服务器装置访问的云账户信息的删除、以及(c)与云账户信息建立关联地保持在存储器中的第1识别信息的删除之中的至少1个。例如,在(b)中,图6所示的云服务信息L11或者L12作为云账户信息被删除。或者,在(b)中,图4或图5所示的云服务列表L4的云服务ID、URL、云账户名及云密码作为云账户信息被删除。在(c)中,图4所示的云服务列表L4的母设备ID作为第1识别信息被删除。

[0230] 在此,在以往的录像机中,在该录像机被转让给他人的情况下,也推荐进行个人信息复位及HDD的格式化。在支持云录像的录像机的情况下,仅这些并不充分,除此之外,还需要禁止向云服务上的录像节目访问、或者删除云服务上的录像节目。如果用户忘记进行这些处理,则被转让的录像机所进行的处理有可能超出个人使用的范围。

[0231] 于是,在本实施方式中,如上所述,进行云服务器装置中录像的内容的删除、云账户信息的删除(或者复位)等。如果第1录像装置或管理服务器装置中记录的云账户信息被删除(或者复位),则无法从该第1录像装置访问云服务器装置。另外,在由管理服务器装置对云服务列表L4进行管理的情况下,通过从智能手机、PC等向管理服务器装置登入并删除云服务列表L4的条目,也能够防止从第1录像装置进行访问。因此,能够充分抑制转让后的第1录像装置非法访问云服务器装置的情况,能够容易地实现第1录像装置即母设备的恰当的转让。

[0232] 此外,本公开中的信息的管理意味着保持该信息,也可以还意味着该信息的变更及删除等。

[0233] 另外,本实施方式中的保护信息是表示用于对内容进行解密的内容密钥Kc、针对内容的管理信息的校验和、哈希值、以及内容的复制次数之中的至少一个的信息。由此,用于有效地保护内容的保护信息从第1录像装置转移至第2录像装置,因此能够提高安全性的强度并实现恰当的母设备10的转移。

[0234] (其他方式等)

[0235] 以上基于实施方式说明了本公开的1个或者多个方式所涉及的系统、装置等,但本公开不限定于该实施方式。只要不脱离本公开的主旨,对上述实施方式施以本领域技术人员所想到的各种变形而得到的方式也包含在本公开中。

[0236] 此外,如下的情况也包含在本公开中。

[0237] (1)上述的至少1个装置具体而言,是由微处理器、ROM(只读存储器(Read Only Memory))、RAM(随机存取存储器(Random Access Memory))、硬盘单元、显示器单元、键盘、鼠标等构成的计算机系统。在该RAM或者硬盘单元中,存储有计算机程序。通过微处理器依照计算机程序进行动作,上述的至少1个装置达成其功能。在此,计算机程序通过为了达成规定的功能而将多个表示针对计算机的指令的命令码组合来构成。

[0238] (2)构成上述的至少1个装置的构成要素的一部分或者全部也可以由1个系统LSI(Large Scale Integration:大规模集成电路)构成。系统LSI是将多个构成部集成在1个芯片上来制造的超多功能LSI,具体而言,是包含微处理器、ROM、RAM等而构成的计算机系统。在所述RAM中存储有计算机程序。通过微处理器依照计算机程序进行动作,系统LSI达成其功能。

[0239] (3)构成上述的至少1个装置的构成要素的一部分或者全部也可以由能够相对于该装置拆装的IC卡或者单体的模组构成。IC卡或者模组是由微处理器、ROM、RAM等构成的计算机系统。IC卡或者模组也可以包括上述的超多功能LSI。通过微处理器依照计算机程序进行动作,IC卡或者模组达成其功能。该IC卡或者该模组也可以具有耐篡改性。

[0240] (4)本公开也可以作为上述所示的方法。另外,也可以作为由计算机实现这些方法的计算机程序,还可以作为由计算机程序构成的数字信号。

[0241] 另外,本公开也可以记录于能够由计算机读取计算机程序或者数字信号的记录介质,例如软盘、硬盘、CD(紧凑盘(Compact Disc))-ROM、DVD、DVD-ROM、DVD-RAM、BD(Blu-ray(注册商标)Disc)、半导体存储器等。另外,也可以作为在这些记录介质中记录的数字信号。

[0242] 另外,本公开也可以将计算机程序或者数字信号经由电气通信线路、无线或有线通信线路、以互联网为代表的网络、数据广播等传送。

[0243] 另外,也可以通过将程序或者数字信号记录至记录介质并转送,或者通过将程序或者数字信号经由网络等转送,从而由独立的其他计算机系统实施。

[0244] 工业实用性

[0245] 本公开例如能够适用于对节目等的内容进行录像并再现的录像再现系统等。

[0246] 附图标记说明:

[0247]	10	母设备(录像装置)
[0248]	20	云服务器(云服务器装置)
[0249]	30、31、32、33	子设备(终端装置)
[0250]	40	管理服务器
[0251]	41	账户管理部
[0252]	42	共用密钥管理部
[0253]	43	子设备管理部
[0254]	44	云服务账户管理部
[0255]	45	母设备管理部
[0256]	100	录像再现系统
[0257]	Kp	共用密钥
[0258]	Kc	内容密钥
[0259]	L1	账户列表
[0260]	L2	账户信息
[0261]	L3	子设备列表
[0262]	L4	云服务列表
[0263]	L5	母设备列表
[0264]	L11、L12	云服务信息
[0265]	L13	内容关联信息

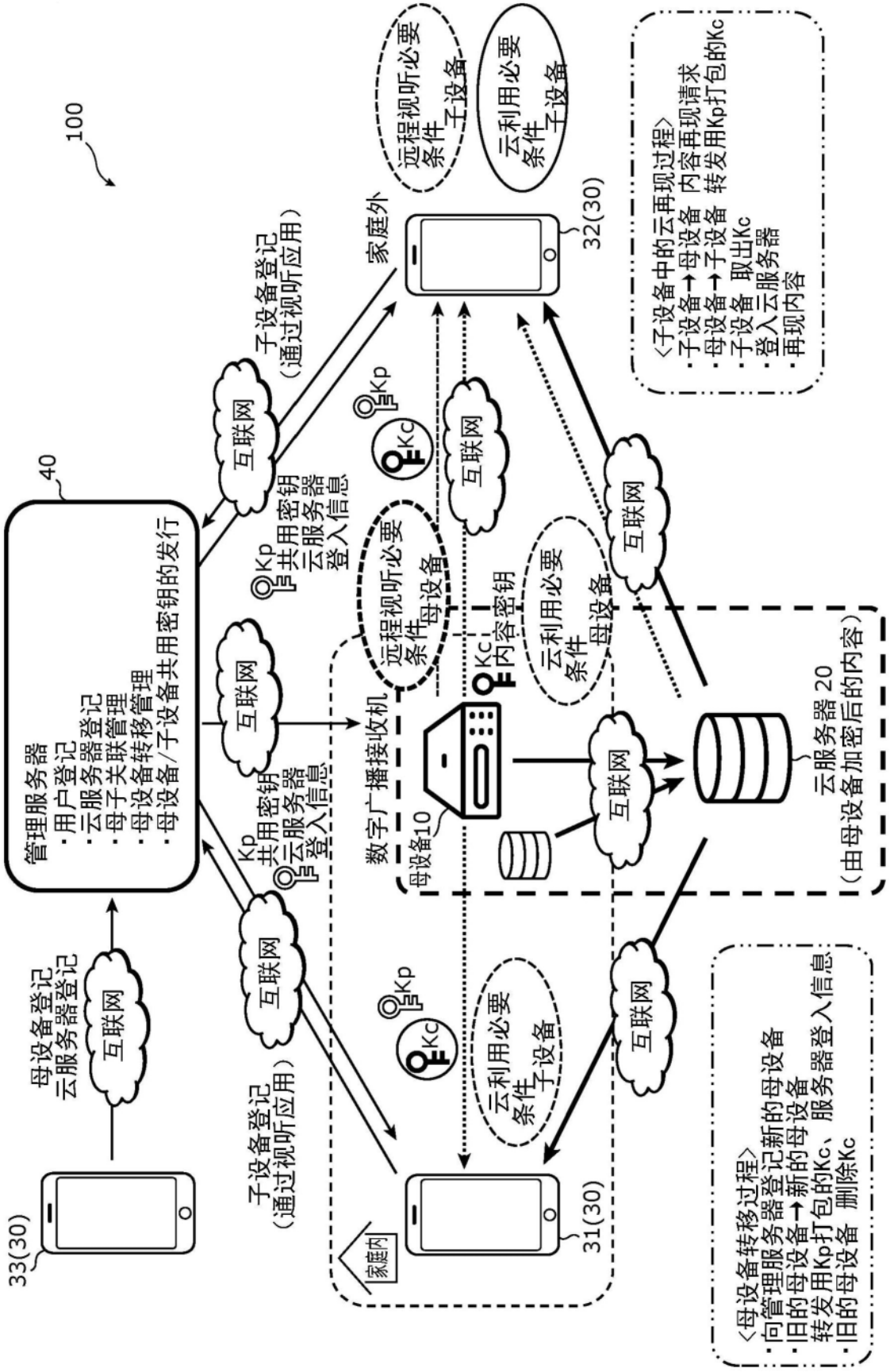

100
管理服务器
·用户登记
·云服务器登记
·母子关联管理
·母设备转移管理
·母设备/子设备共用密钥的发行
40
母设备登记
云服务器登记
互联网
33(30)
互联网
子设备登记
（通过视听应用）
互联网
Kp
共用密钥
云服务器
登入信息
数字广播接收机
母设备10
Kc
内容密钥
远程视听必要条件
母设备
云利用必要条件
母设备
互联网
互联网
互联网
互联网
云服务器 20
（由母设备加密后的内容）
Kp
Kc
云利用必要条件
子设备
31(30)
家庭内
子设备登记
（通过视听应用）
互联网
Kp
Kc
家庭外
远程视听必要条件
子设备
云利用必要条件
子设备
32(30)
〈子设备中的云再现过程〉
·子设备→母设备 内容再现请求
·母设备→子设备 转发用Kp打包的Kc
·子设备 取出Kc
·登入云服务器
·再现内容
〈母设备转移过程〉
·向管理服务器登记新的母设备
·旧的母设备→新的母设备
转发用Kp打包的Kc、服务器登入信息
·旧的母设备 删除Kc

图1

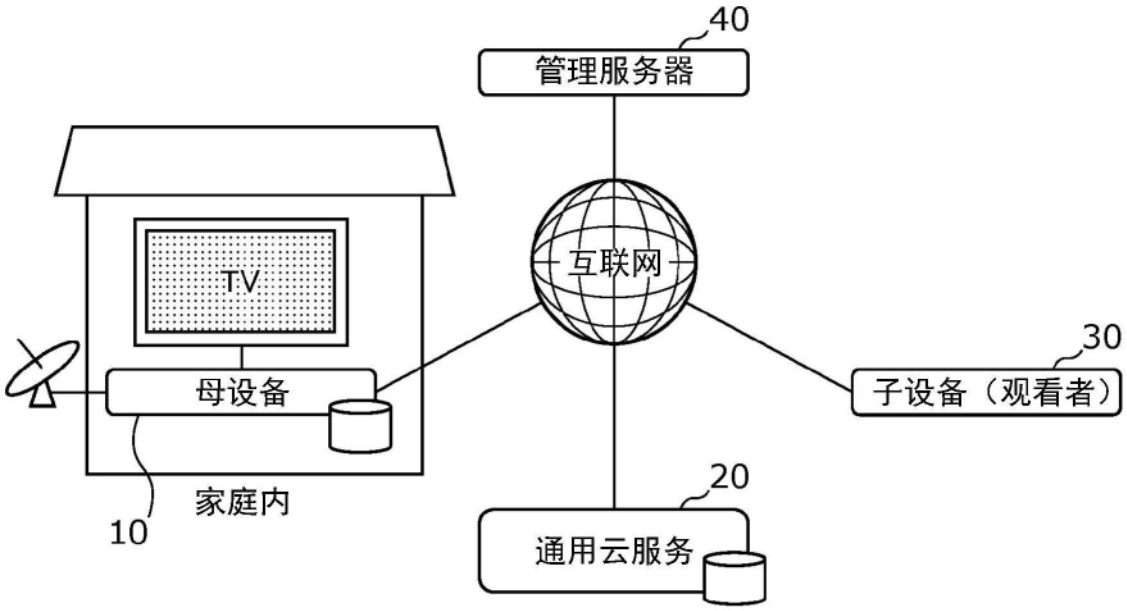

40
管理服务器
互联网
TV
母设备
30
子设备（观看者）
家庭内
10
20
通用云服务

图2

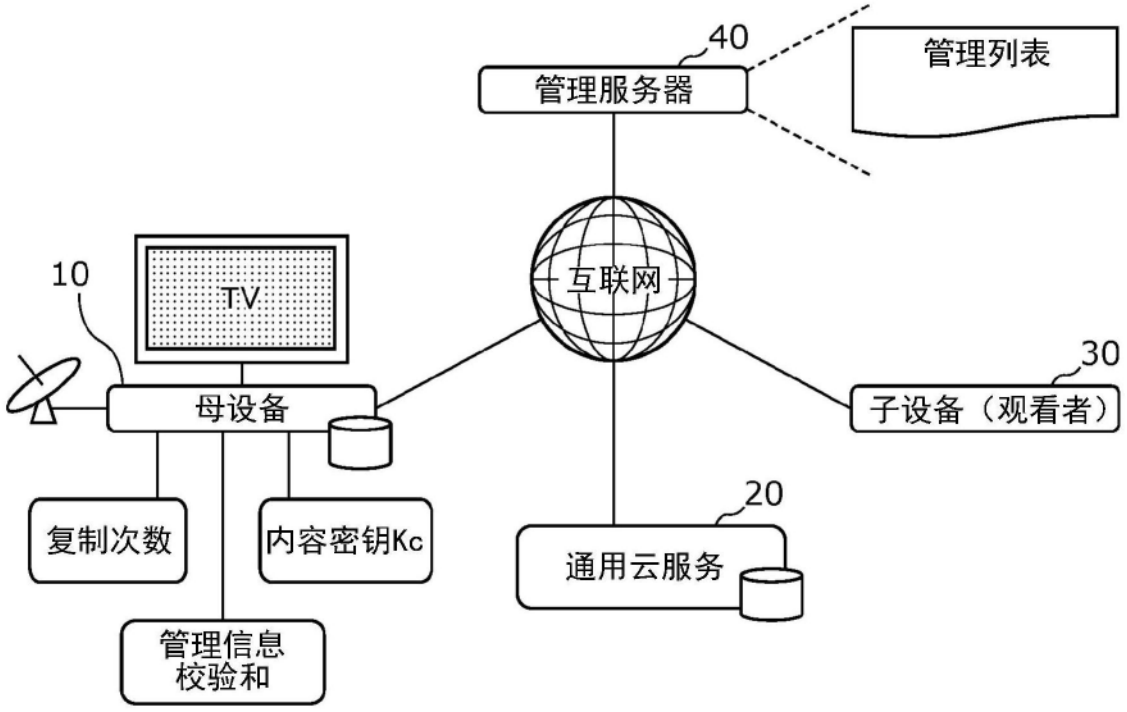

40
管理服务器
管理列表
互联网
10
TV
母设备
30
子设备（观看者）
复制次数
内容密钥Kc
20
通用云服务
管理信息
校验和

图3

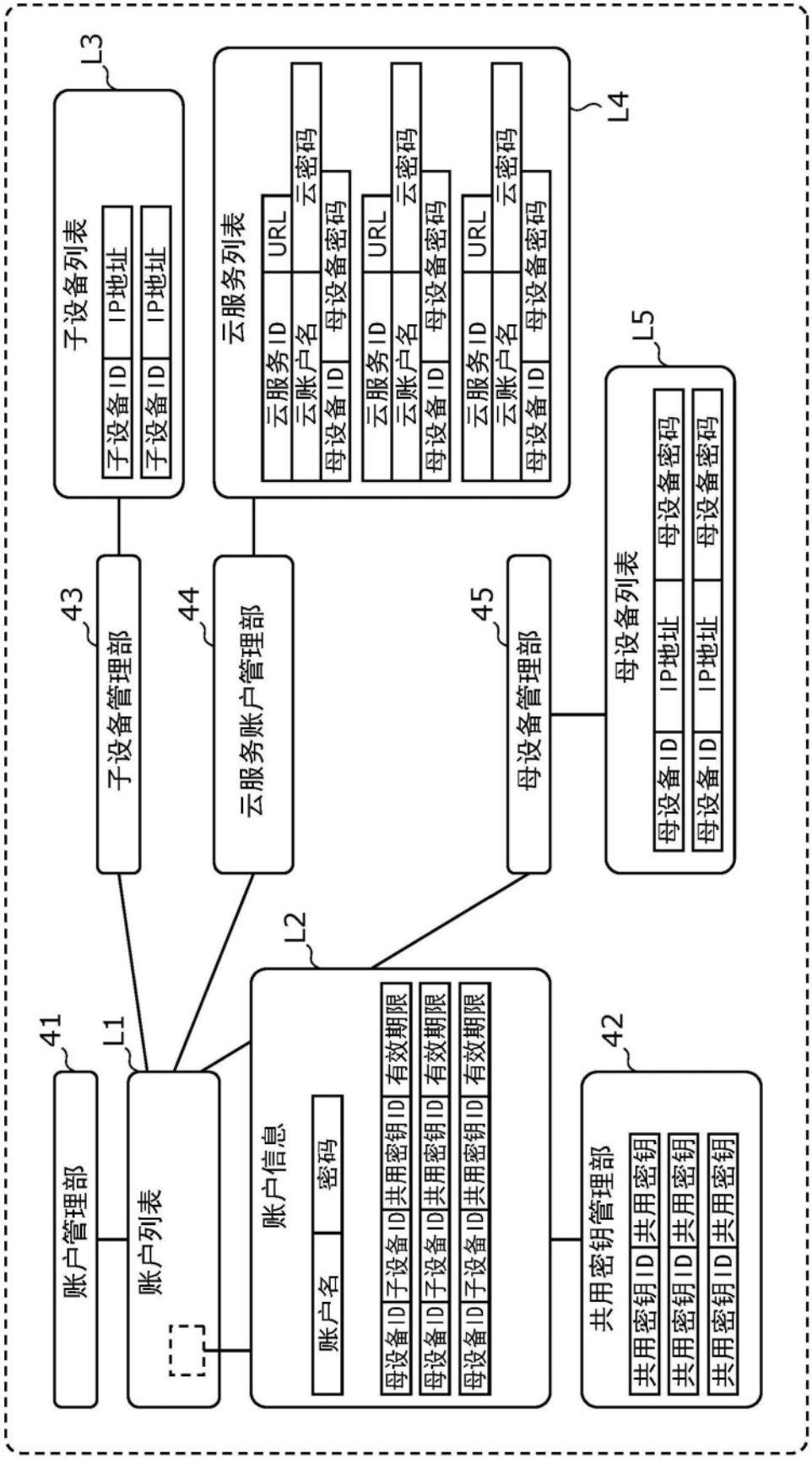

L3
子设备列表
子设备ID
IP地址
子设备ID
IP地址
L4
云服务列表
云服务ID
URL
云账户名
云密码
母设备ID
母设备密码
云服务ID
URL
云账户名
云密码
母设备ID
母设备密码
云服务ID
URL
云账户名
云密码
母设备ID
母设备密码
L5
母设备列表
母设备ID
IP地址
母设备密码
母设备ID
IP地址
母设备密码
43
子设备管理部
44
云服务账户管理部
45
母设备管理部
41
账户管理部
L1
账户列表
L2
账户信息
账户名
密码
母设备ID
子设备ID
共用密钥ID
有效期限
母设备ID
子设备ID
共用密钥ID
有效期限
母设备ID
子设备ID
共用密钥ID
有效期限
42
共用密钥管理部
共用密钥ID
共用密钥
共用密钥ID
共用密钥
共用密钥ID
共用密钥

图4

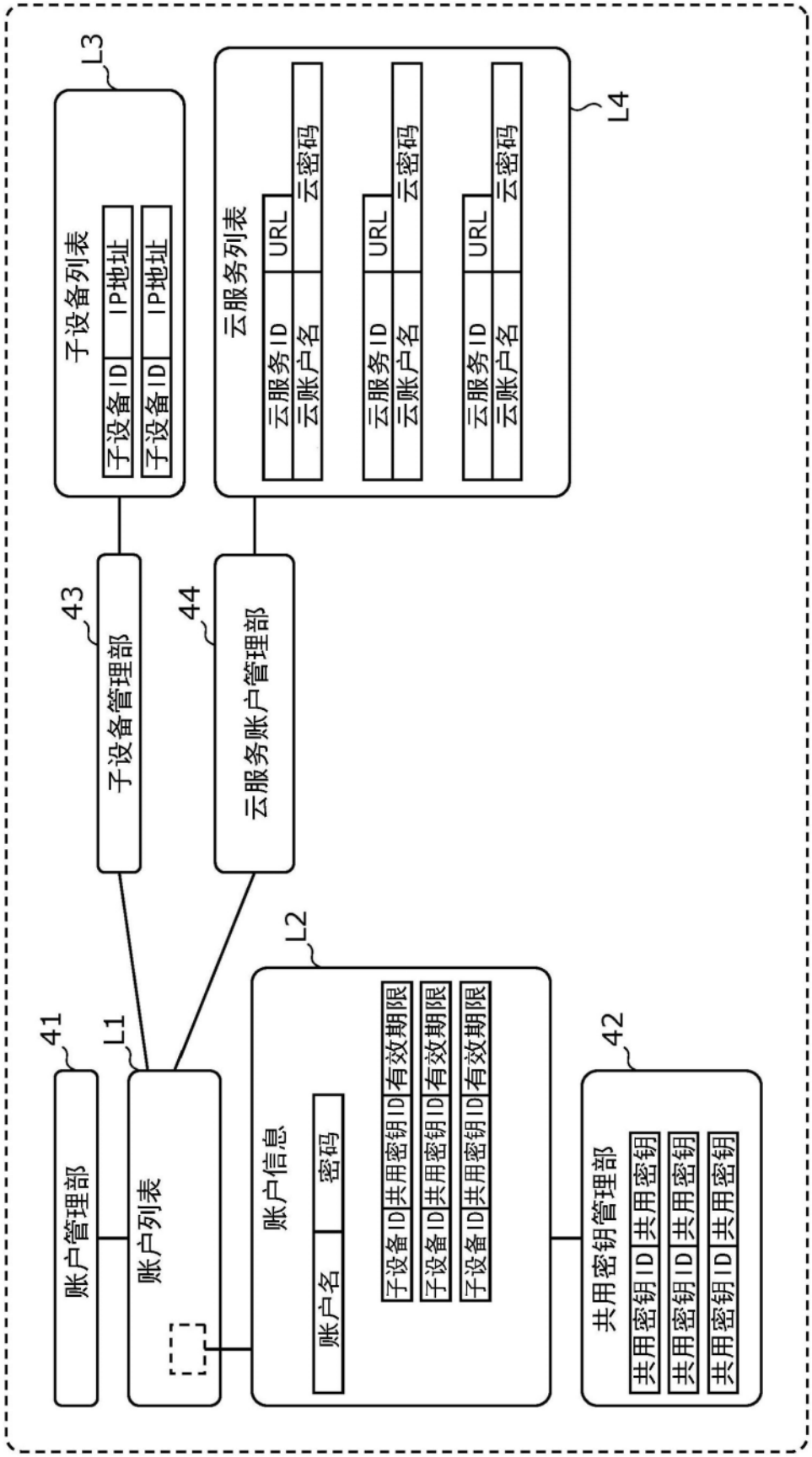

L3
子设备列表
子设备ID
IP地址
子设备ID
IP地址
L4
云服务列表
云服务ID
URL
云账户名
云密码
云服务ID
URL
云账户名
云密码
云服务ID
URL
云账户名
云密码
43
子设备管理部
44
云服务账户管理部
41
账户管理部
L1
账户列表
L2
账户信息
账户名
密码
子设备ID
共用密钥ID
有效期限
子设备ID
共用密钥ID
有效期限
子设备ID
共用密钥ID
有效期限
42
共用密钥管理部
共用密钥ID
共用密钥
共用密钥ID
共用密钥
共用密钥ID
共用密钥

图5

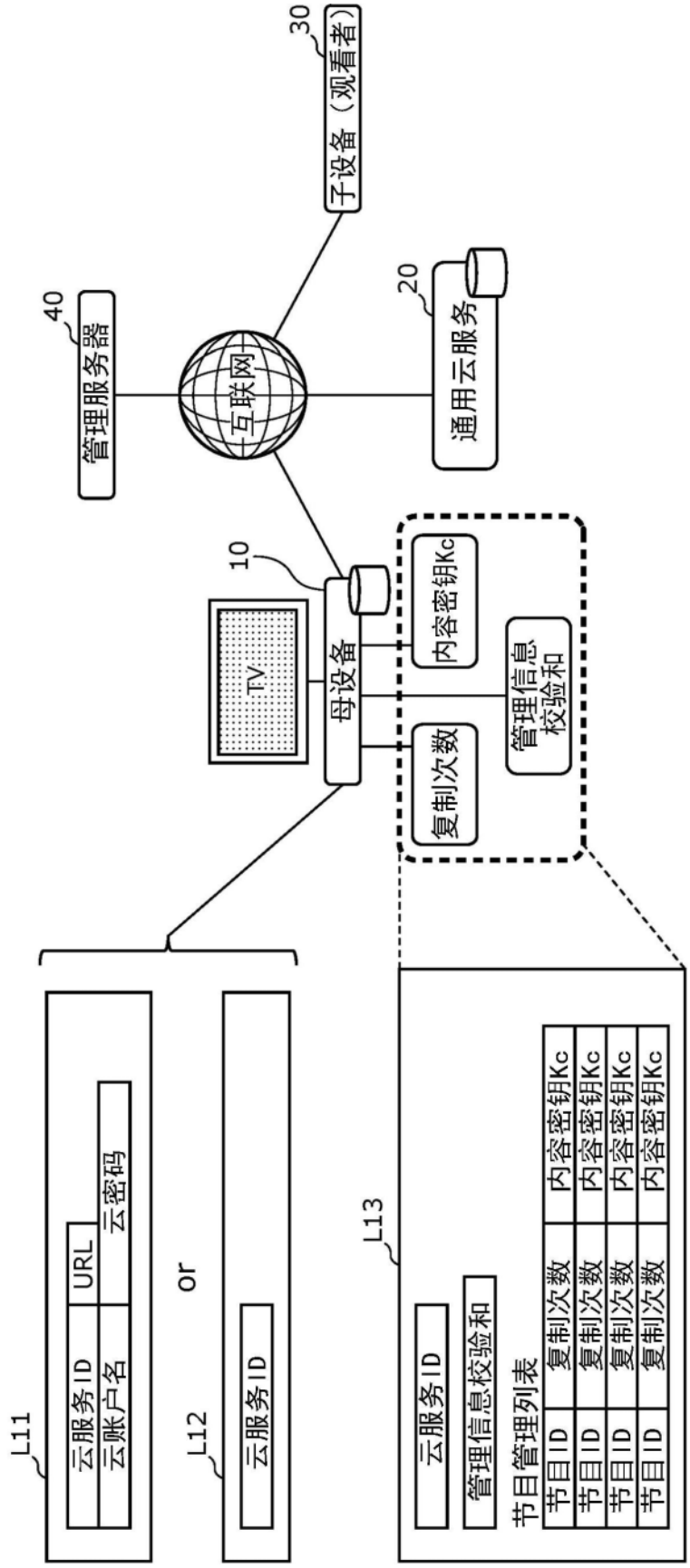

30
子设备（观看者）
40
管理服务器
互联网
20
通用云服务
10
TV
母设备
内容密钥Kc
管理信息校验和
复制次数
L11
云服务ID
云账户名
URL
云密码
or
L12
云服务ID
L13
云服务ID
管理信息校验和
节目管理列表
节目ID 复制次数 内容密钥Kc
节目ID 复制次数 内容密钥Kc
节目ID 复制次数 内容密钥Kc
节目ID 复制次数 内容密钥Kc

图6

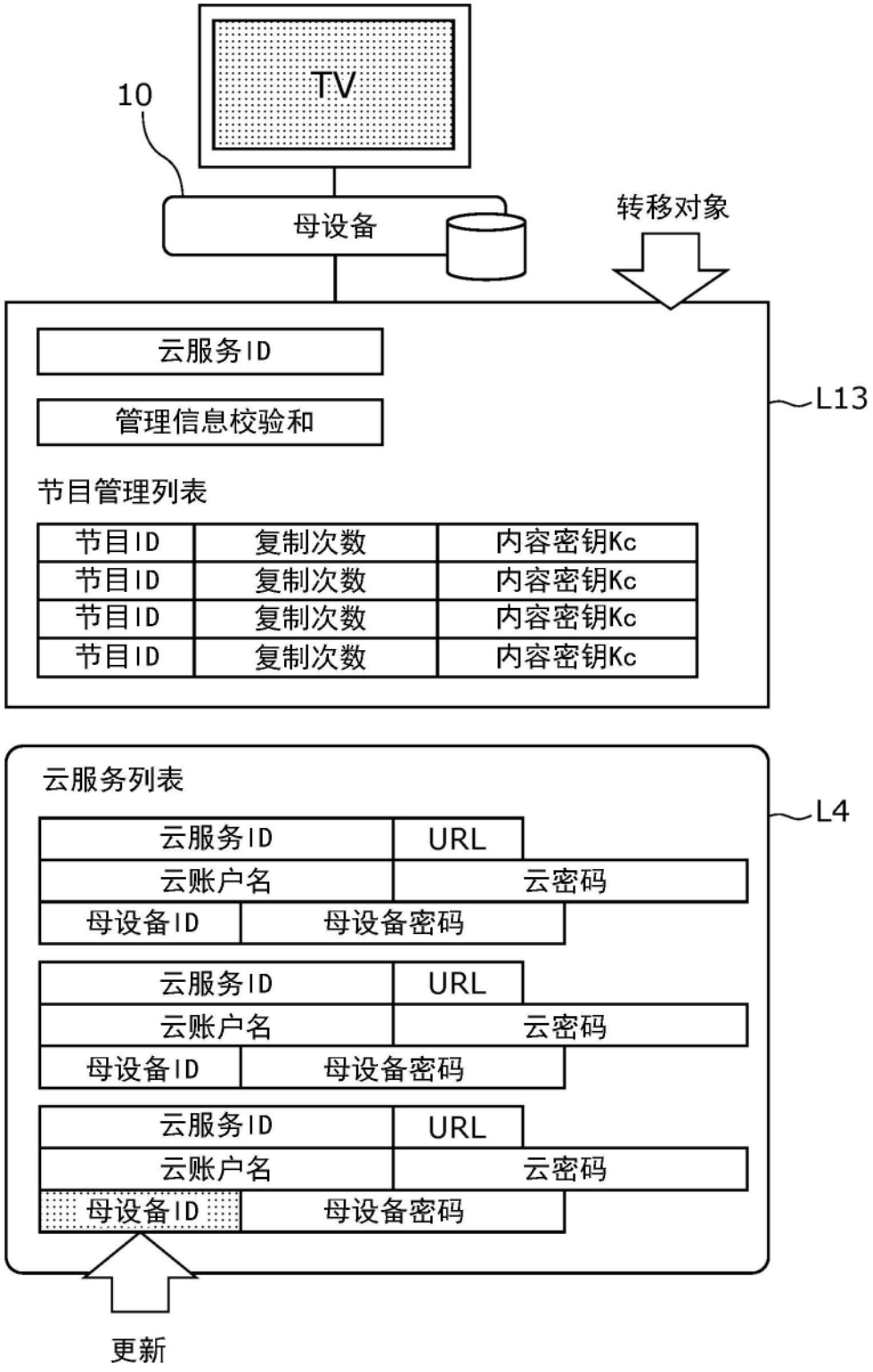

TV
10
母设备
转移对象
云服务ID
管理信息校验和
L13
节目管理列表
节目ID 复制次数 内容密钥Kc
节目ID 复制次数 内容密钥Kc
节目ID 复制次数 内容密钥Kc
节目ID 复制次数 内容密钥Kc
云服务列表
L4
云服务ID URL
云账户名 云密码
母设备ID 母设备密码
云服务ID URL
云账户名 云密码
母设备ID 母设备密码
云服务ID URL
云账户名 云密码
母设备ID 母设备密码
更新

图7

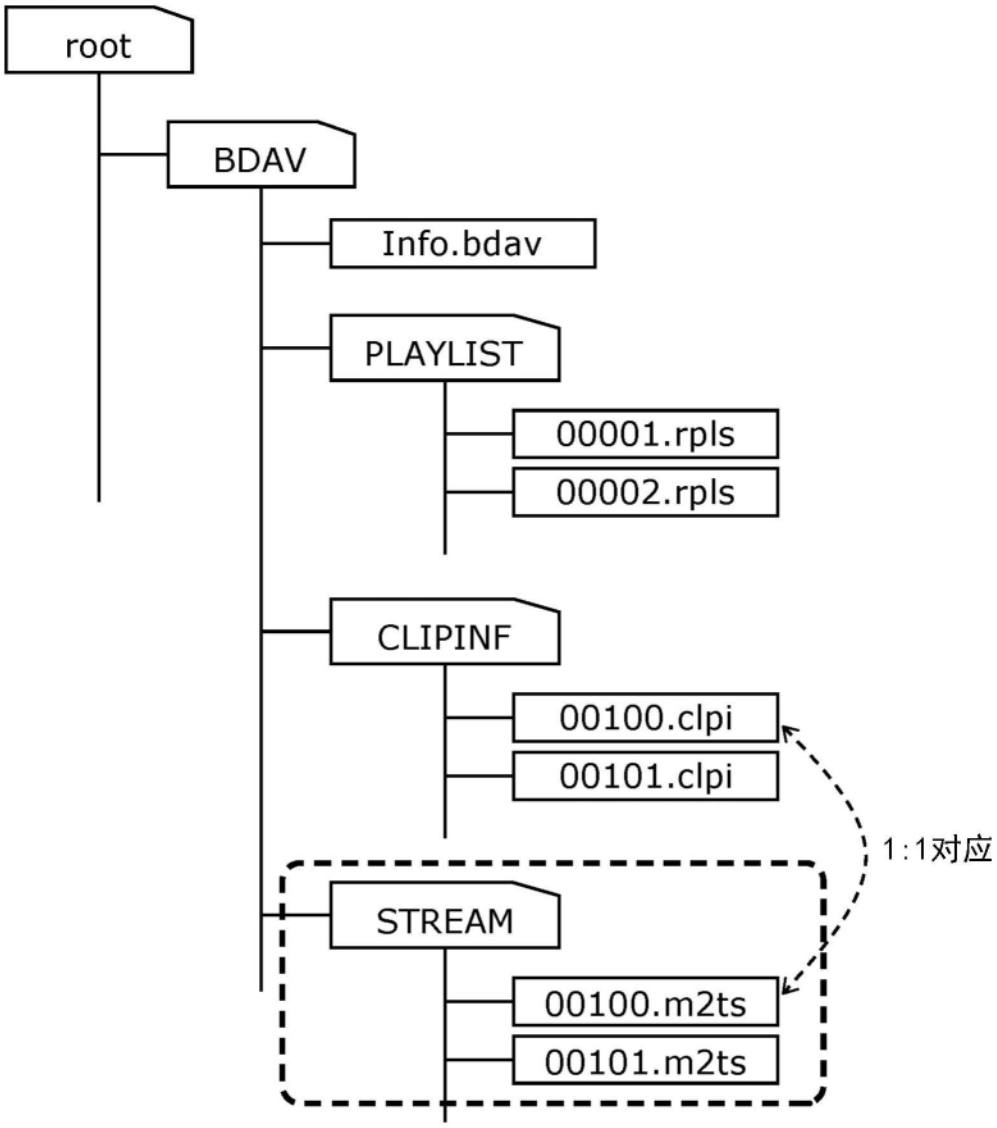

root
BDAV
Info.bdav
PLAYLIST
00001.rpls
00002.rpls
CLIPINF
00100.clpi
00101.clpi
1:1对应
STREAM
00100.m2ts
00101.m2ts

图8

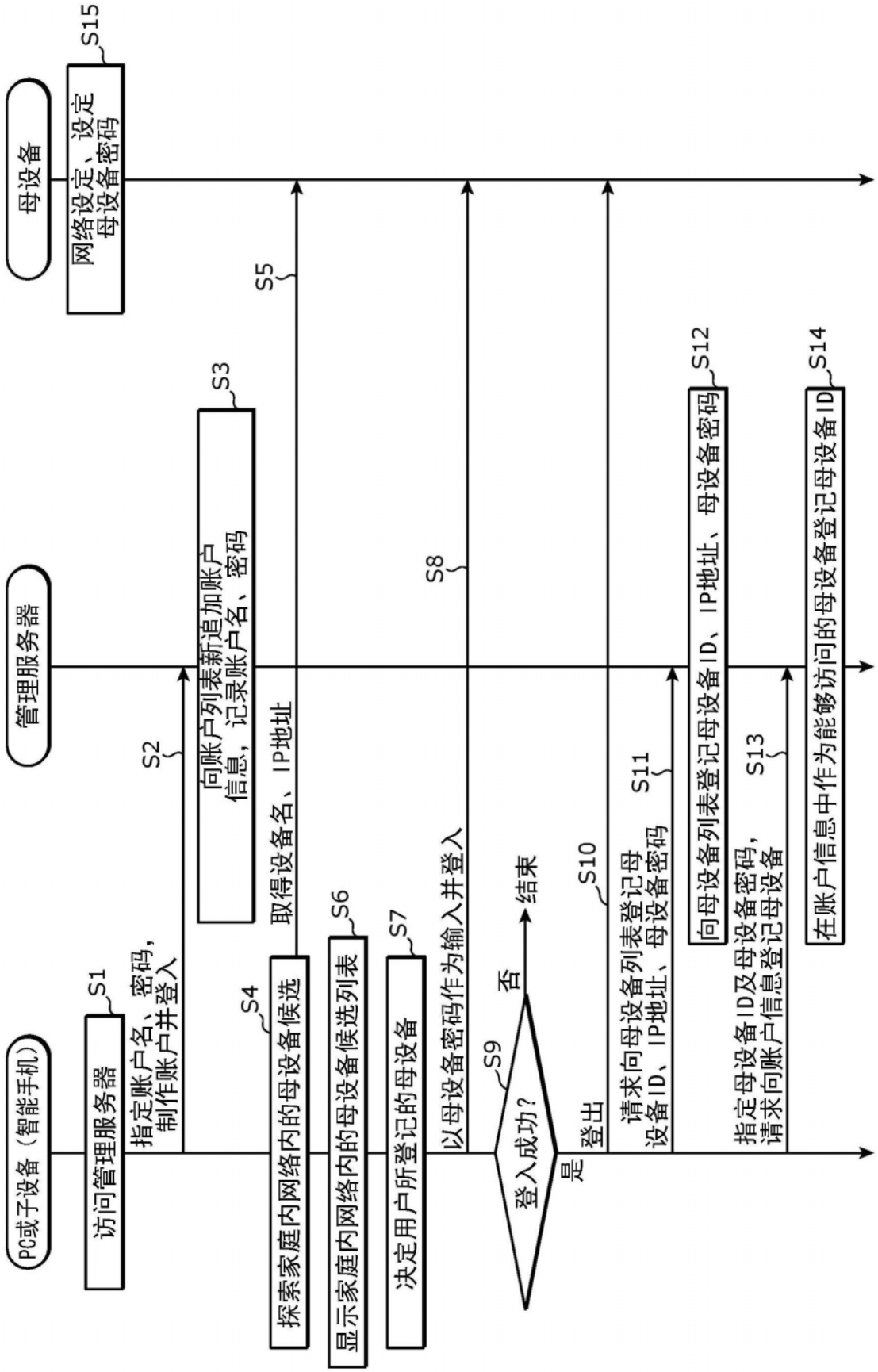

PC或子设备（智能手机）
管理服务器
母设备
访问管理服务器
S1
指定账户名、密码，制作账户并登入
S2
向账户列表新追加账户信息，记录账户名、密码
S3
网络设定、设定母设备密码
S15
S5
探索家庭内网络内的母设备候选
S4
取得设备名、IP地址
显示家庭内网络内的母设备候选列表
S6
决定用户所登记的母设备
S7
S8
以母设备密码作为输入并登入
登入成功？
S9
否
结束
是
登出
S10
请求向母设备列表登记母设备ID、IP地址、母设备密码
S11
向母设备列表登记母设备ID、IP地址、母设备密码
S12
指定母设备ID及母设备密码，请求向账户信息登记母设备
S13
在账户信息中作为能够访问的母设备登记母设备ID
S14

图9

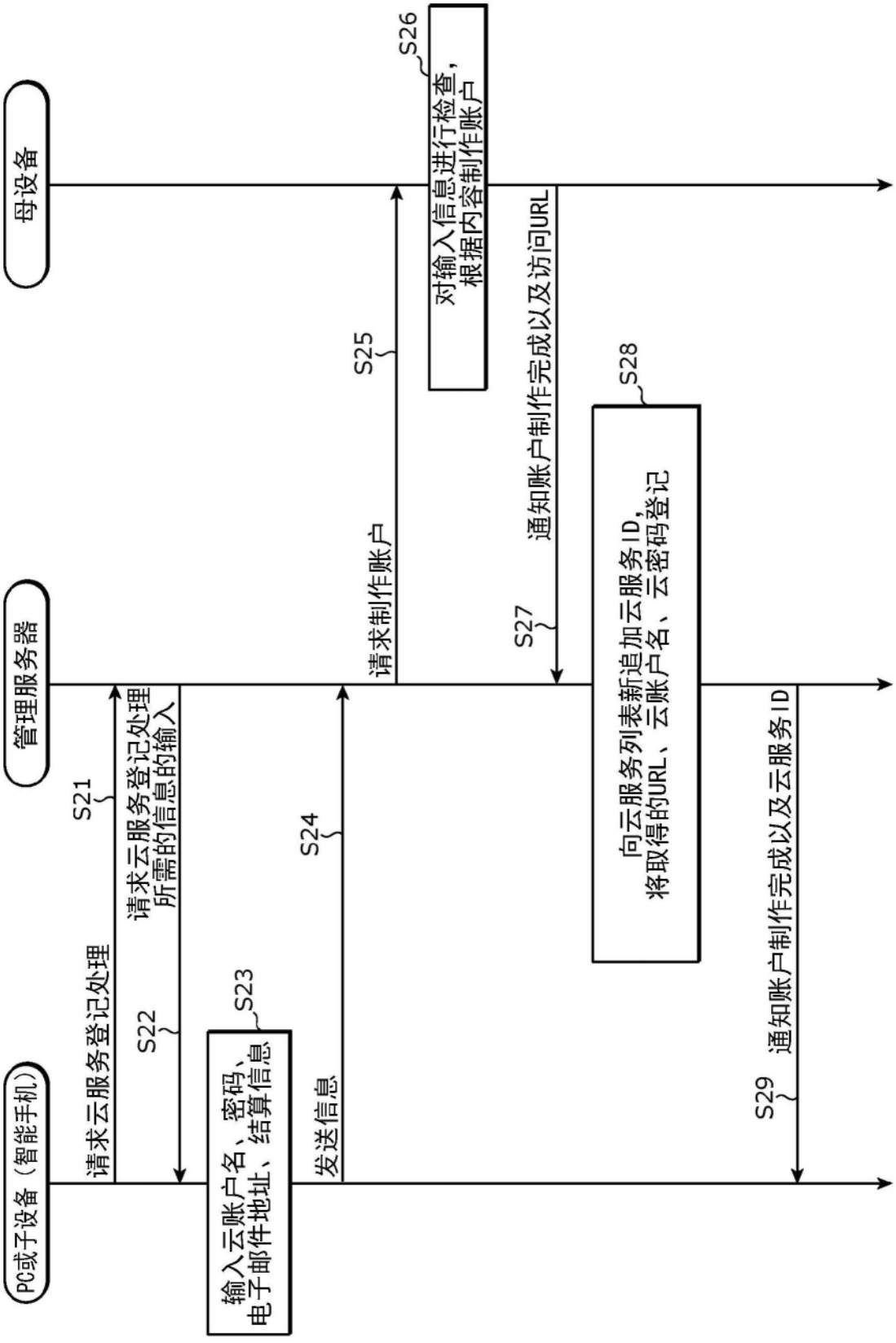

PC或子设备（智能手机）
管理服务器
母设备
请求云服务登记处理
S21
请求云服务登记处理所需的信息的输入
S22
输入云账户名、密码、电子邮件地址、结算信息
S23
发送信息
S24
请求制作账户
S25
对输入信息进行检查，根据内容制作账户
S26
通知账户制作完成以及访问URL
S27
向云服务列表新追加云服务ID，将取得的URL、云账户名、云密码登记
S28
通知账户制作完成以及云服务ID
S29

图10

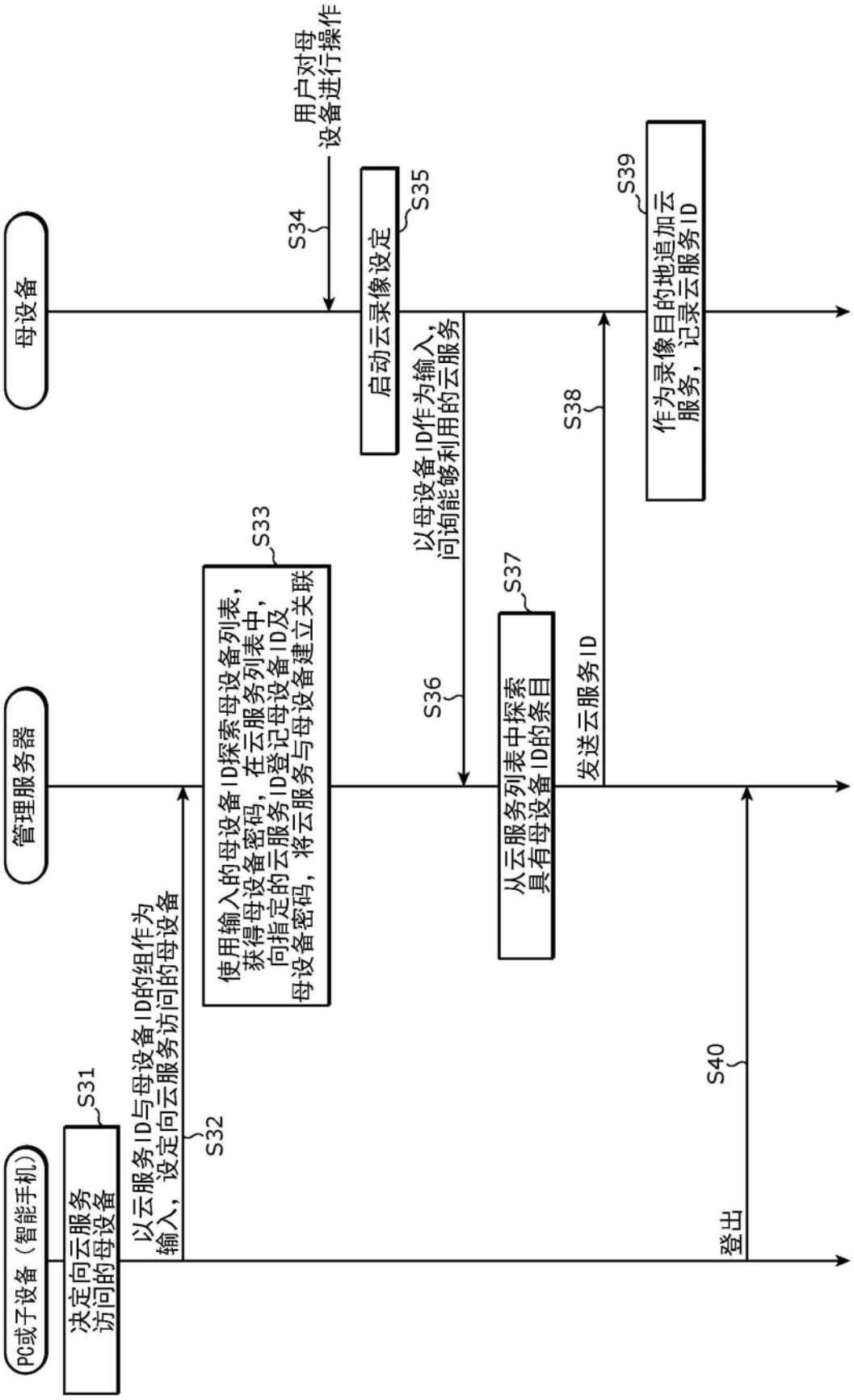

PC或子设备（智能手机）
管理服务器
母设备
决定向云服务访问的母设备
S31
以云服务ID与母设备ID的组作为输入，设定向云服务访问的母设备
S32
使用输入的母设备ID探索母设备列表，获得母设备密码，在云服务列表中，向指定的云服务ID登记母设备ID及母设备密码，将云服务与母设备建立关联
S33
用户对母设备进行操作
S34
启动云录像设定
S35
以母设备ID作为输入，问询能够利用的云服务
S36
从云服务列表中探索具有母设备ID的条目
S37
发送云服务ID
S38
作为录像目的地追加云服务，记录云服务ID
S39
登出
S40

图11

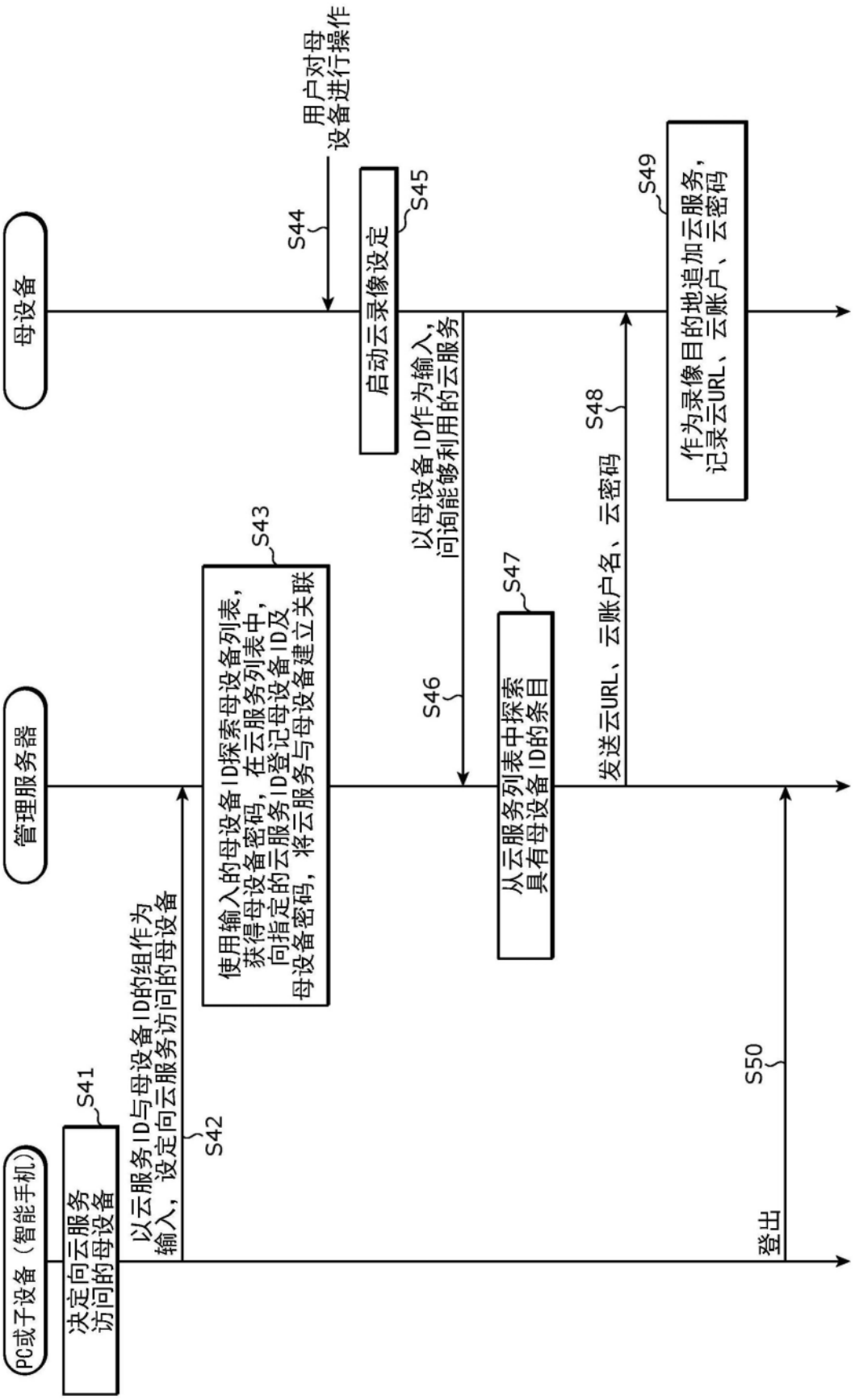

PC或子设备（智能手机）
管理服务器
母设备
决定向云服务访问的母设备
S41
以云服务ID与母设备ID的组作为输入，设定向云服务访问的母设备
S42
使用输入的母设备ID探索母设备列表，获得母设备密码，在云服务列表中，向指定的云服务ID登记母设备ID及母设备密码，将云服务与母设备建立关联
S43
用户对母设备进行操作
S44
启动云录像设定
S45
以母设备ID作为输入，问询能够利用的云服务
S46
从云服务列表中探索具有母设备ID的条目
S47
发送云URL、云账户名、云密码
S48
作为录像目的地追加云服务，记录云URL、云账户、云密码
S49
登出
S50

图12

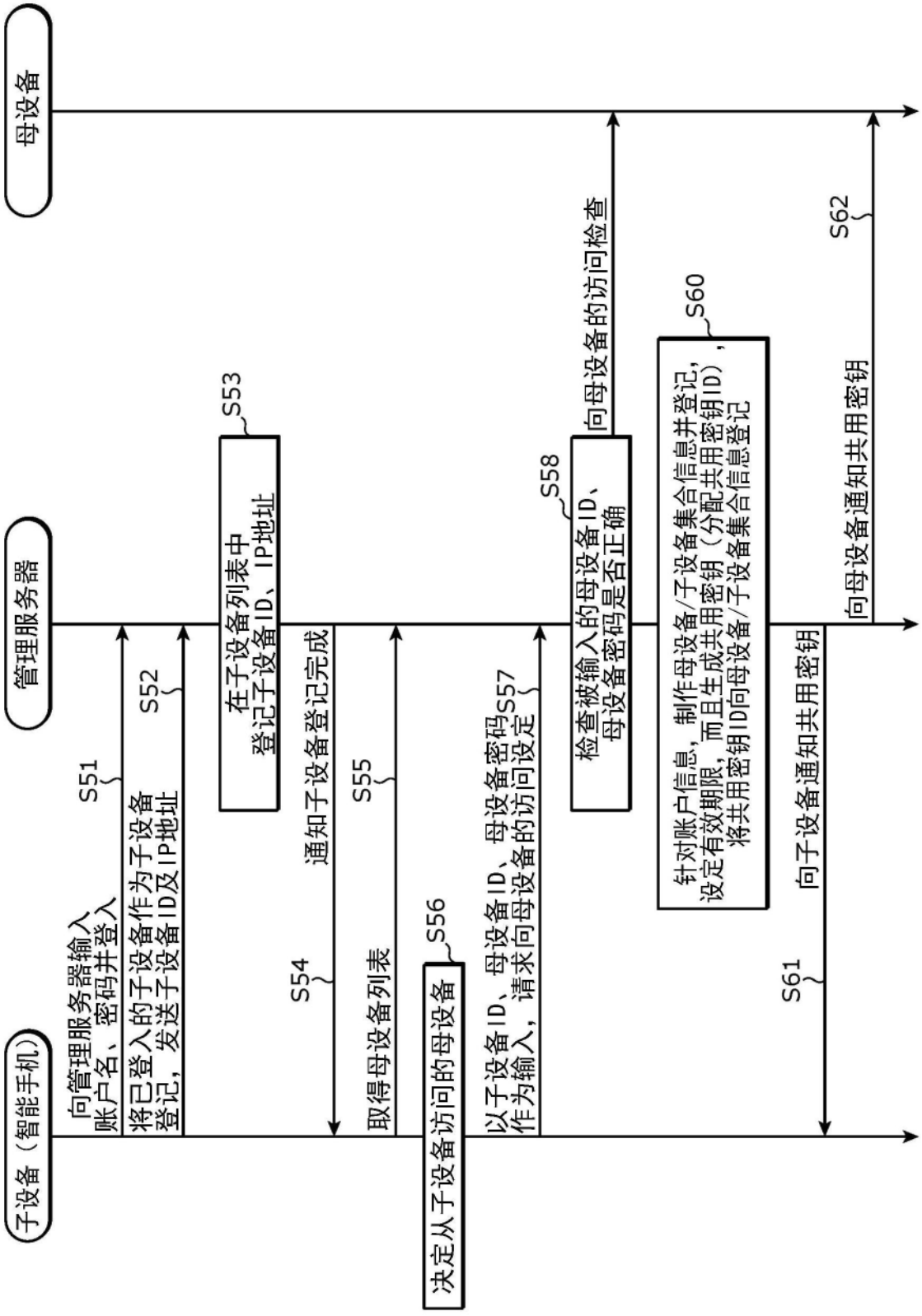

子设备（智能手机）
管理服务器
母设备
向管理服务器输入账户名、密码并登入
S51
将已登入的子设备作为子设备登记，发送子设备ID及IP地址
S52
在子设备列表中登记子设备ID、IP地址
S53
通知子设备登记完成
S54
取得母设备列表
S55
决定从子设备访问的母设备
S56
以子设备ID、母设备ID、母设备密码作为输入，请求向母设备的访问设定
S57
检查被输入的母设备ID、母设备密码是否正确
S58
向母设备的访问检查
针对账户信息，制作母设备/子设备集合信息并登记，设定有效期限，而且生成共用密钥（分配共用密钥ID），将共用密钥ID向母设备/子设备集合信息登记
S60
向子设备通知共用密钥
S61
向母设备通知共用密钥
S62

图13

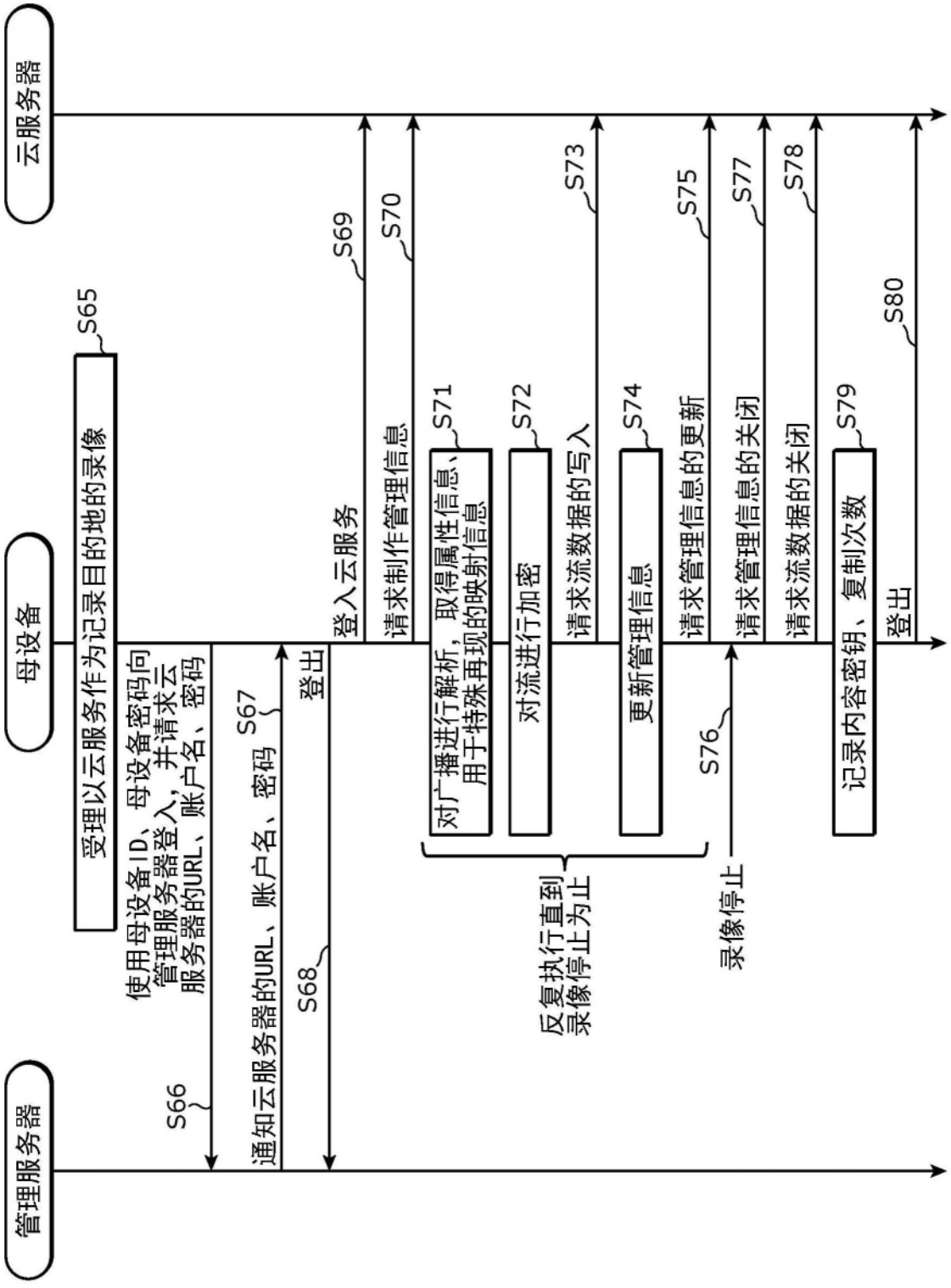

管理服务器
母设备
云服务器
受理以云服务作为记录目的地的录像
S65
使用母设备ID、母设备密码向管理服务器登入，并请求云服务器的URL、账户名、密码
S66
通知云服务器的URL、账户名、密码
S67
登出
S68
登入云服务
S69
请求制作管理信息
S70
对广播进行解析，取得属性信息、用于特殊再现的映射信息
S71
对流进行加密
S72
请求流数据的写入
S73
更新管理信息
S74
请求管理信息的更新
S75
录像停止
S76
请求管理信息的关闭
S77
请求流数据的关闭
S78
记录内容密钥、复制次数
S79
登出
S80
反复执行直到录像停止为止

图14

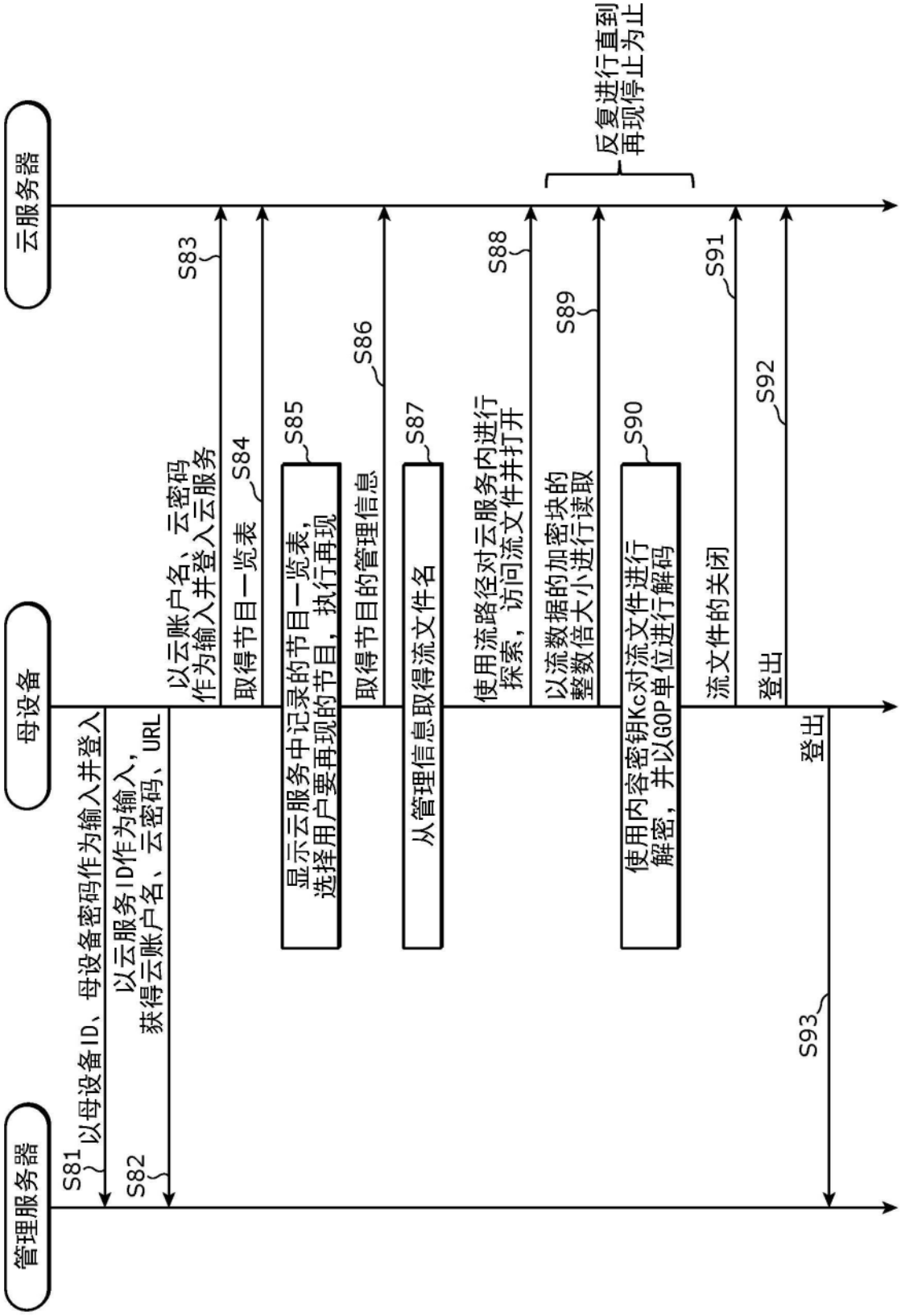

管理服务器
母设备
云服务器
反复进行直到
再现停止为止
S81
以母设备ID、母设备密码作为输入并登入
S82
以云服务ID作为输入，
获得云账户名、云密码、URL
S83
以云账户名、云密码
作为输入并登入云服务
S84
取得节目一览表
S85
显示云服务中记录的节目一览表，
选择用户要再现的节目，执行再现
S86
取得节目的管理信息
S87
从管理信息取得流文件名
S88
使用流路径对云服务内进行
探索，访问流文件并打开
S89
以流数据的加密块的
整数倍大小进行读取
S90
使用内容密钥Kc对流文件进行
解密，并以GOP单位进行解码
S91
流文件的关闭
S92
登出
S93
登出

图15

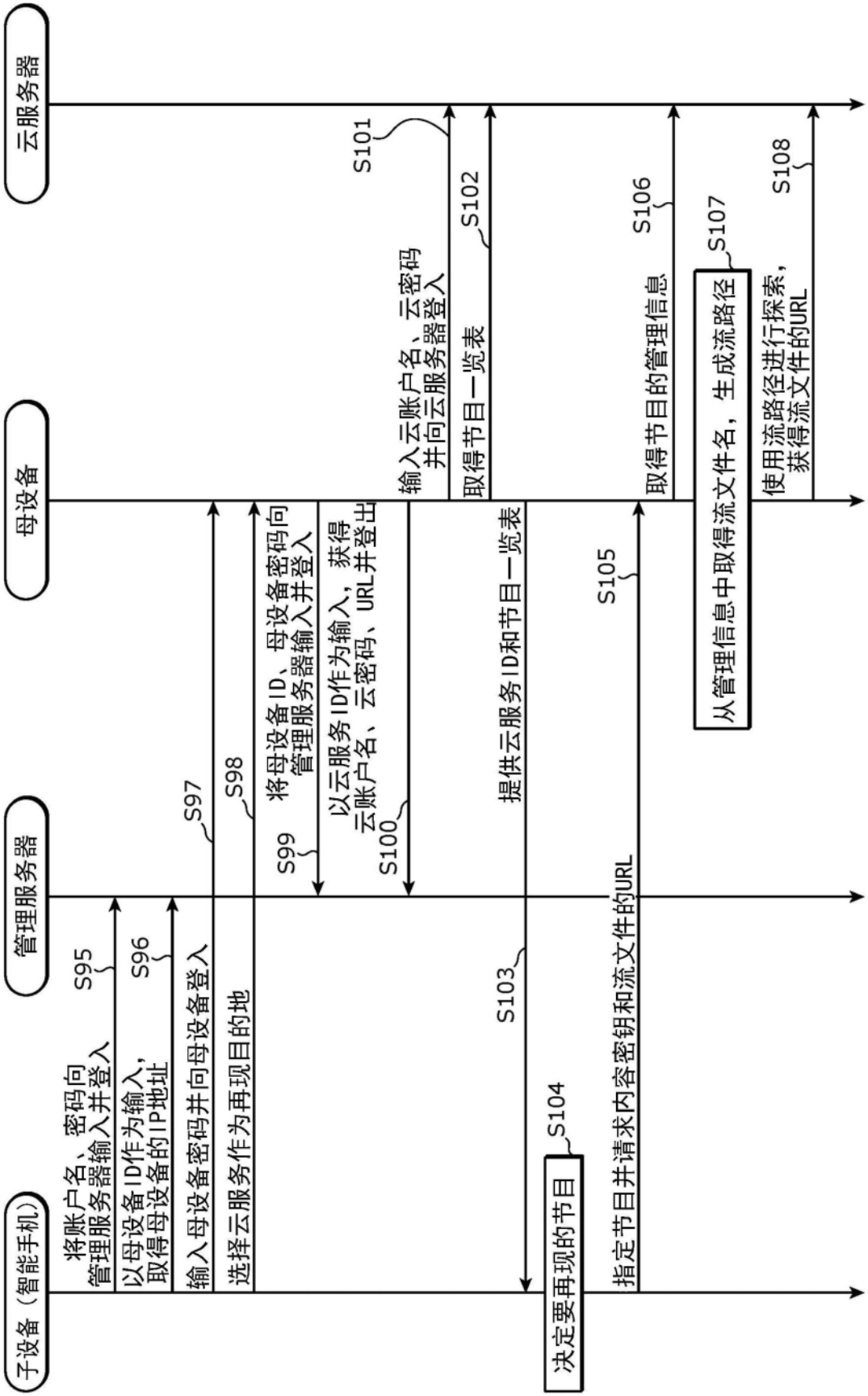

子设备（智能手机）
管理服务器
母设备
云服务器
将账户名、密码向管理服务器输入并登入
S95
以母设备ID作为输入，取得母设备的IP地址
S96
输入母设备密码并向母设备登入
S97
选择云服务作为再现目的地
S98
将母设备ID、母设备密码向管理服务器输入并登入
S99
以云服务ID作为输入，获得云账户名、云密码、URL并登出
S100
输入云账户名、云密码并向云服务器登入
S101
取得节目一览表
S102
提供云服务ID和节目一览表
S103
决定要再现的节目
S104
指定节目并请求内容密钥和流文件的URL
S105
取得节目的管理信息
S106
从管理信息中取得流文件名，生成流路径
S107
使用流路径进行探索，获得流文件的URL
S108

图16

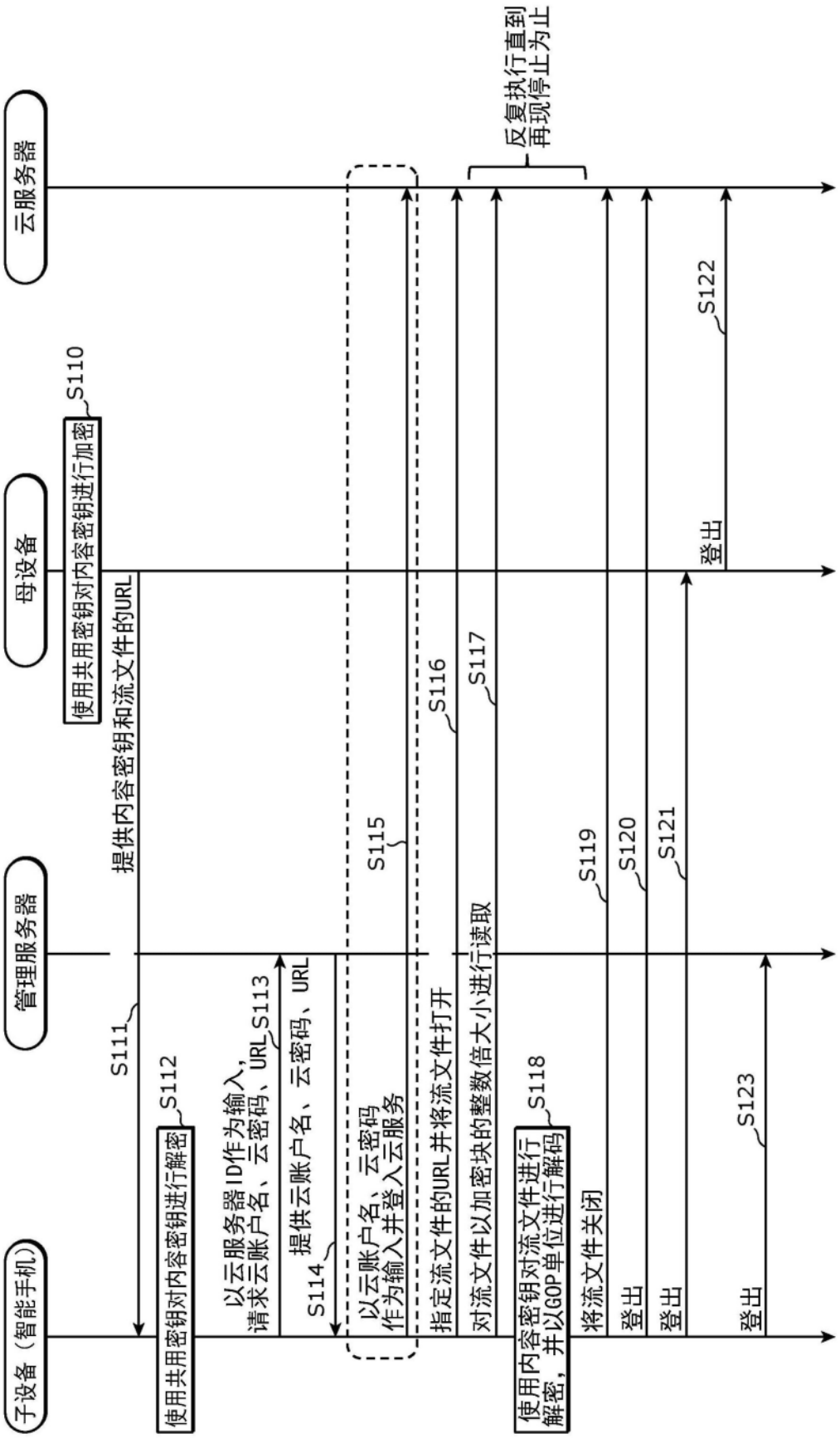

子设备（智能手机）
管理服务器
母设备
云服务器
使用共用密钥对内容密钥进行加密
S110
提供内容密钥和流文件的URL
S111
使用共用密钥对内容密钥进行解密
S112
以云服务器ID作为输入，
请求云账户名、云密码、URL
S113
提供云账户名、云密码、URL
S114
以云账户名、云密码
作为输入并登入云服务
S115
指定流文件的URL并将流文件打开
S116
对流文件以加密块的整数倍大小进行读取
S117
使用内容密钥对流文件进行
解密，并以GOP单位进行解码
S118
将流文件关闭
S119
登出
S120
登出
S121
登出
S122
登出
S123
反复执行直到
再现停止为止

图17

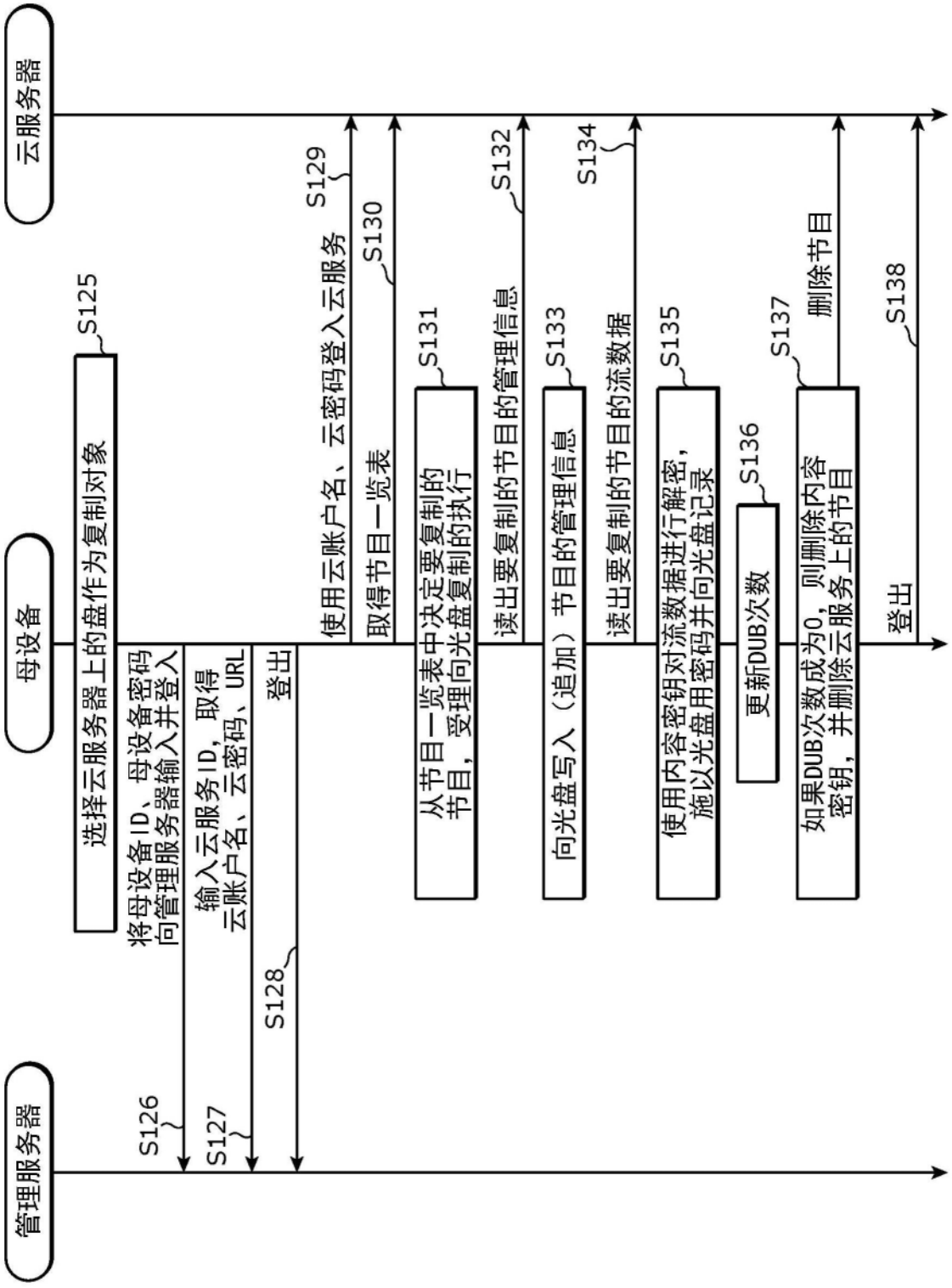

管理服务器
母设备
云服务器
选择云服务器上的盘作为复制对象
S125
将母设备ID、母设备密码向管理服务器输入并登入
S126
输入云服务ID，取得云账户名、云密码、URL
S127
登出
S128
使用云账户名、云密码登入云服务
S129
取得节目一览表
S130
从节目一览表中决定要复制的节目，受理向光盘复制的执行
S131
读出要复制的节目的管理信息
S132
向光盘写入（追加）节目的管理信息
S133
读出要复制的节目的流数据
S134
使用内容密钥对流数据进行解密，施以光盘用密码并向光盘记录
S135
更新DUB次数
S136
如果DUB次数成为0，则删除内容密钥，并删除云服务上的节目
S137
删除节目
登出
S138

图18

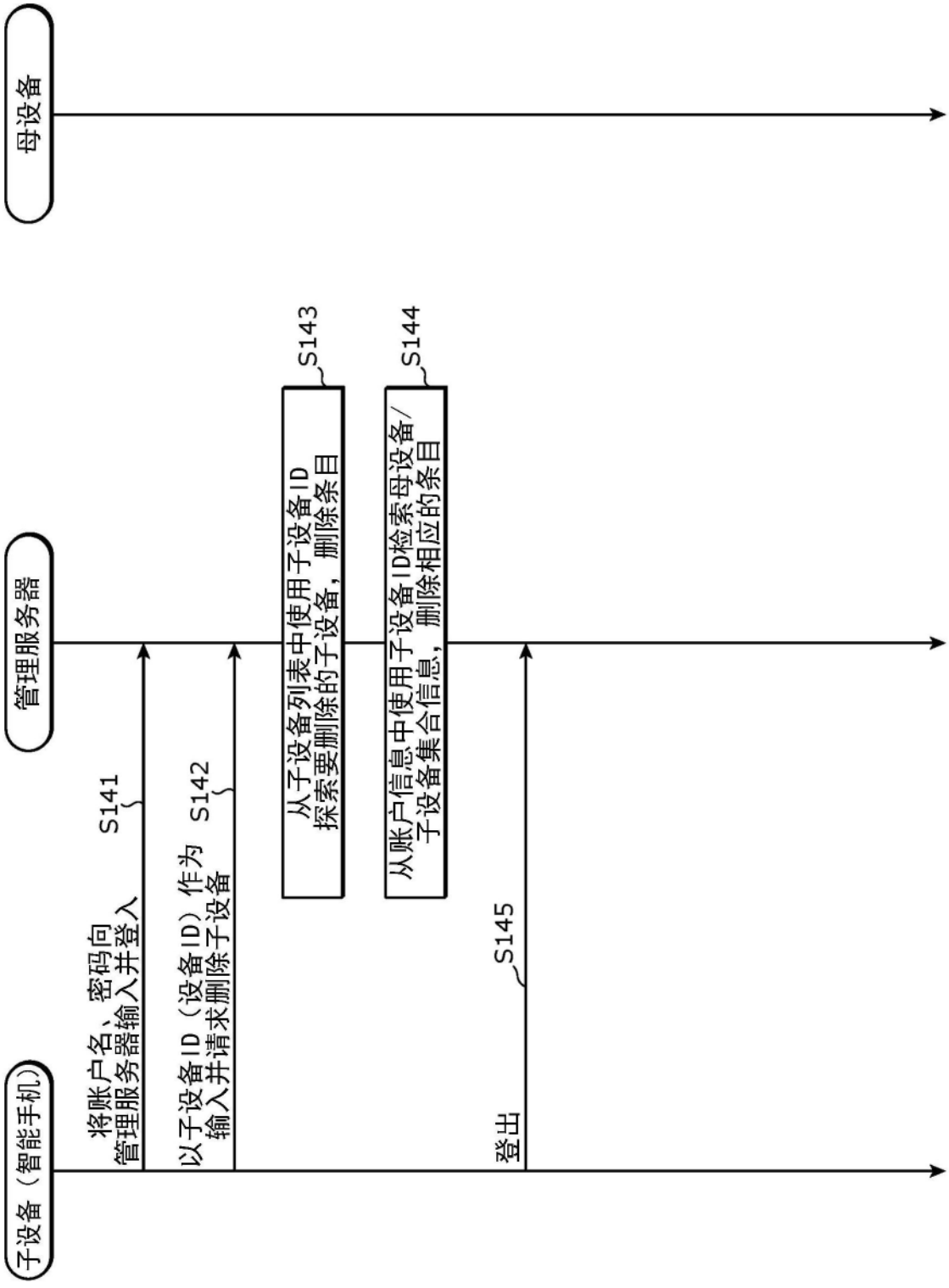

子设备（智能手机）
管理服务器
母设备
将账户名、密码向管理服务器输入并登入
S141
以子设备ID（设备ID）作为输入并请求删除子设备
S142
从子设备列表中使用子设备ID探索要删除的子设备，删除条目
S143
从账户信息中使用子设备ID检索母设备/子设备集合信息，删除相应的条目
S144
登出
S145

图19

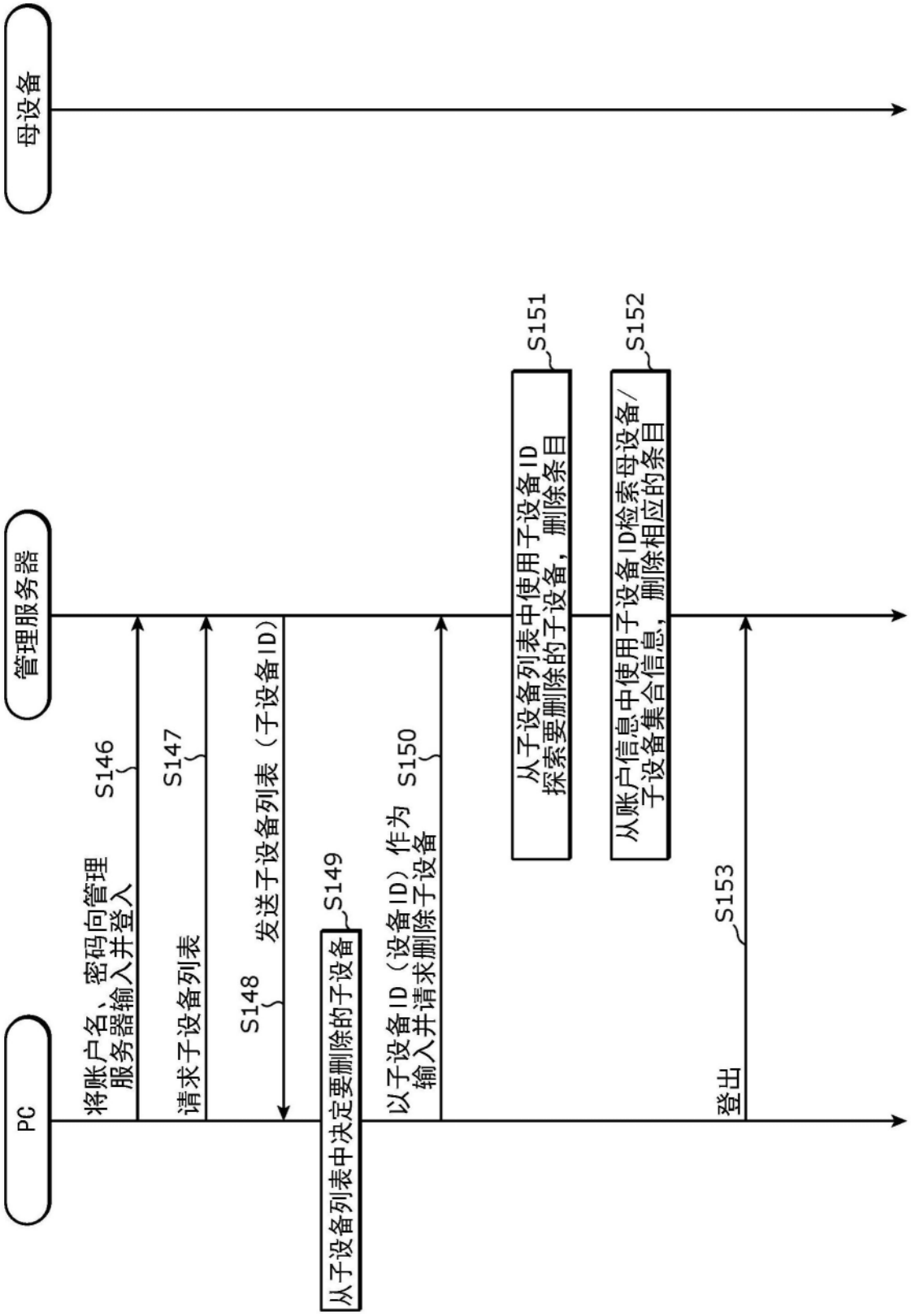

PC
管理服务器
母设备
将账户名、密码向管理服务器输入并登入
S146
请求子设备列表
S147
S148
发送子设备列表（子设备ID）
从子设备列表中决定要删除的子设备
S149
以子设备ID（设备ID）作为输入并请求删除子设备
S150
从子设备列表中使用子设备ID探索要删除的子设备，删除条目
S151
从账户信息中使用子设备ID检索母设备/子设备集合信息，删除相应的条目
S152
登出
S153

图20

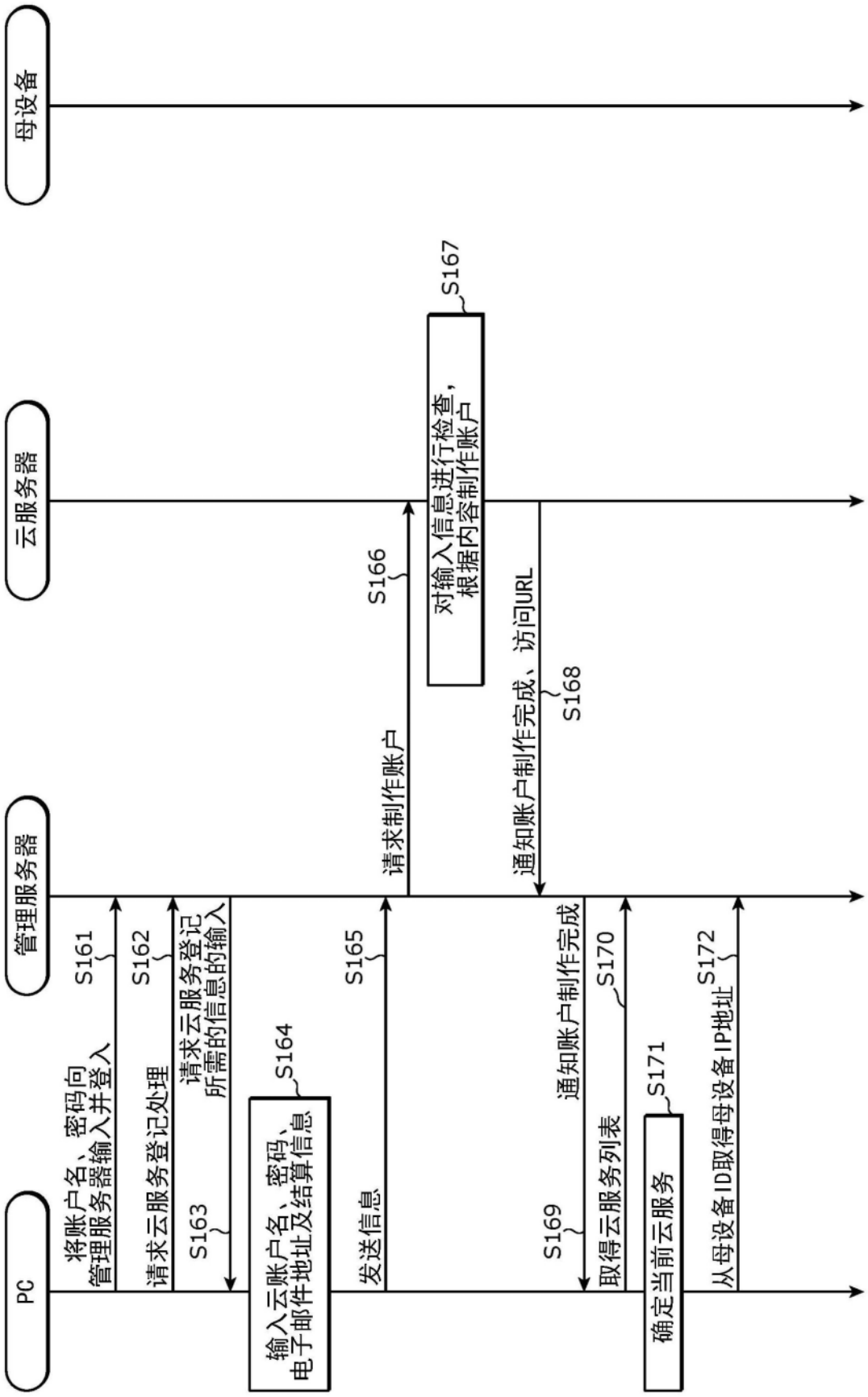

PC
管理服务器
云服务器
母设备
将账户名、密码向管理服务器输入并登入
S161
请求云服务登记处理
S162
请求云服务登记所需的信息的输入
S163
输入云账户名、密码、电子邮件地址及结算信息
S164
发送信息
S165
请求制作账户
S166
对输入信息进行检查，根据内容制作账户
S167
通知账户制作完成、访问URL
S168
取得云服务列表
S169
通知账户制作完成
S170
确定当前云服务
S171
从母设备ID取得母设备IP地址
S172

图21

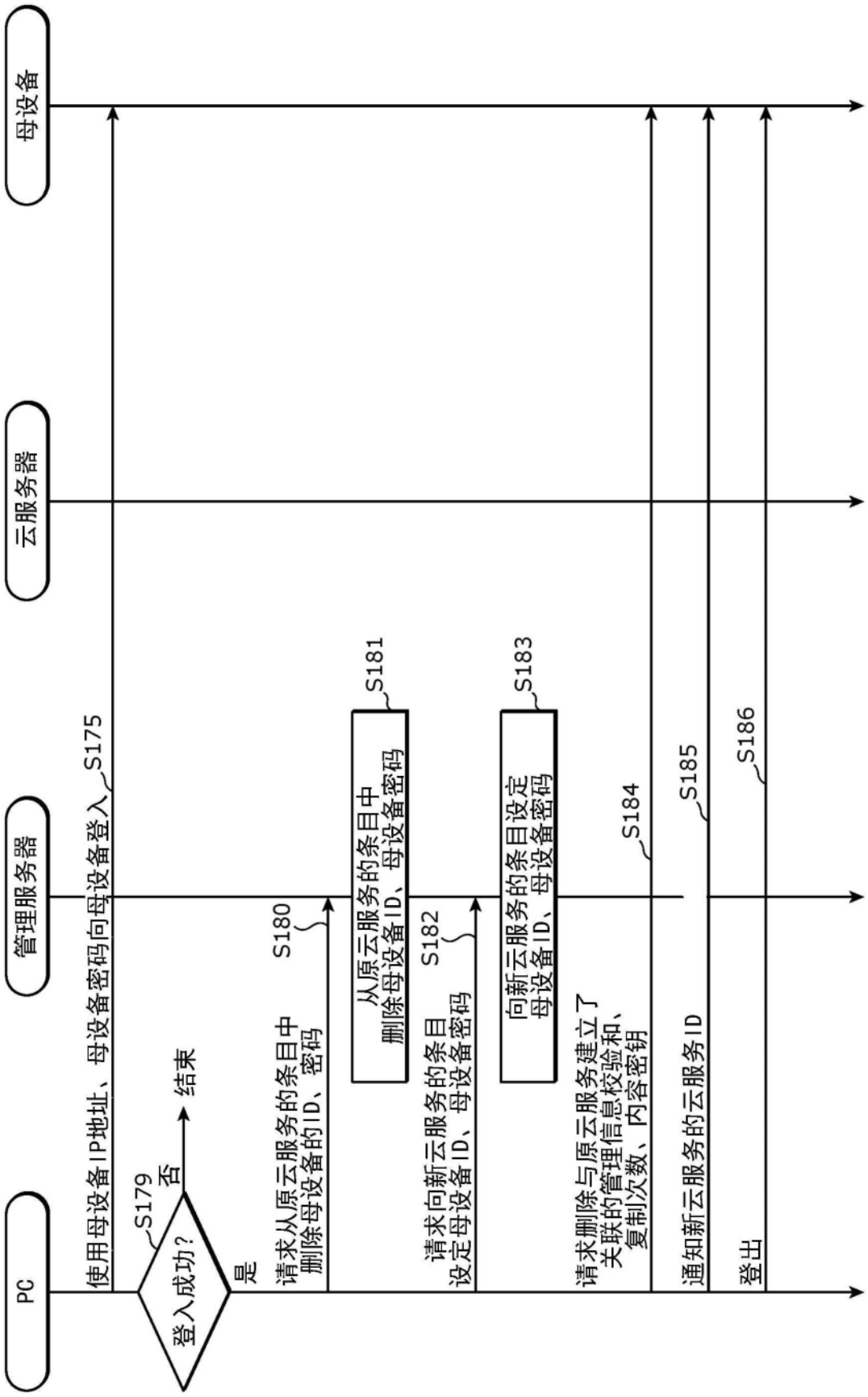

PC
管理服务器
云服务器
母设备
使用母设备IP地址、母设备密码向母设备登入
S175
S179
登入成功?
否
结束
是
请求从原云服务的条目中删除母设备的ID、密码
S180
从原云服务的条目中删除母设备ID、母设备密码
S181
请求向新云服务的条目设定母设备ID、母设备密码
S182
向新云服务的条目设定母设备ID、母设备密码
S183
请求删除与原云服务建立了关联的管理信息校验和、复制次数、内容密钥
S184
通知新云服务的云服务ID
S185
登出
S186

图22

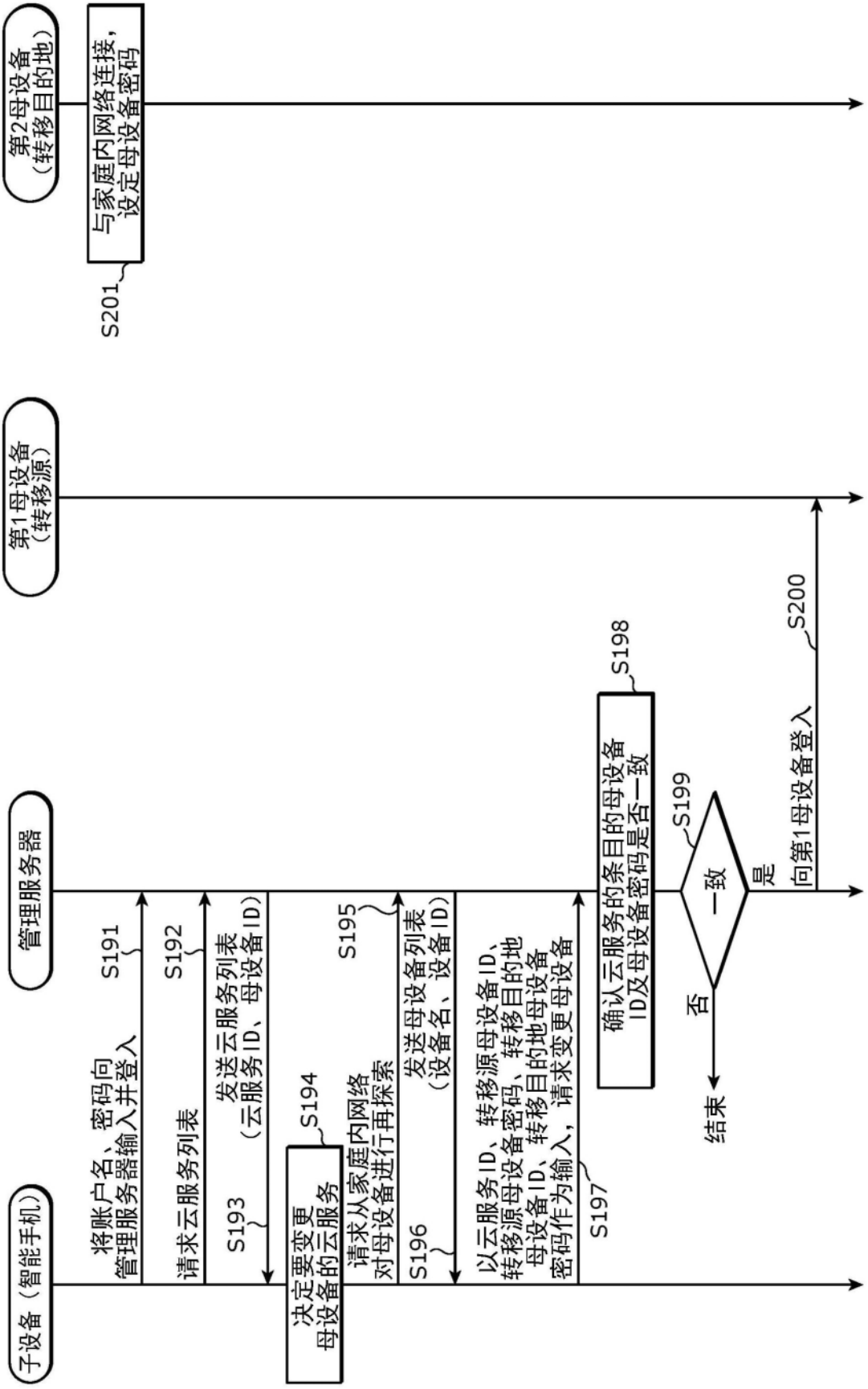

子设备（智能手机）
管理服务器
第1母设备（转移源）
第2母设备（转移目的地）
将账户名、密码向管理服务器输入并登入
S191
请求云服务列表
S192
发送云服务列表（云服务ID、母设备ID）
S193
决定要变更母设备的云服务
S194
请求从家庭内网络对母设备进行再探索
S195
发送母设备列表（设备名、设备ID）
S196
以云服务ID、转移源母设备ID、转移源母设备密码、转移目的地母设备ID、转移目的地母设备密码作为输入，请求变更母设备
S197
确认云服务的条目的母设备ID及母设备密码是否一致
S198
一致
S199
否
结束
是
向第1母设备登入
S200
S201
与家庭内网络连接，设定母设备密码

图23

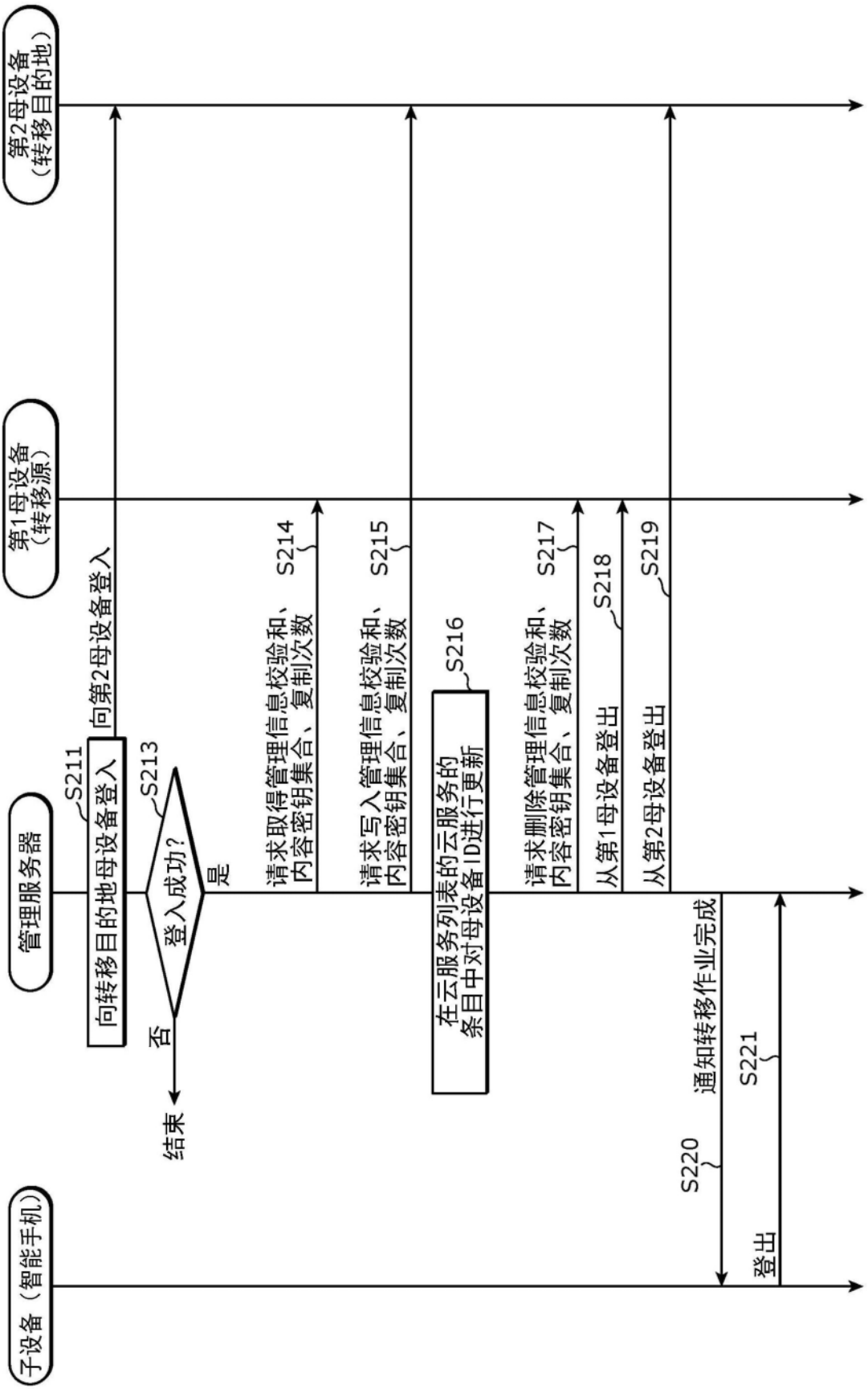

第2母设备
（转移目的地）
第1母设备
（转移源）
管理服务器
子设备（智能手机）
向转移目的地母设备登入
S211
向第2母设备登入
登入成功?
S213
否
是
结束
请求取得管理信息校验和、
内容密钥集合、复制次数
S214
请求写入管理信息校验和、
内容密钥集合、复制次数
S215
在云服务列表的云服务的
条目中对母设备ID进行更新
S216
请求删除管理信息校验和、
内容密钥集合、复制次数
S217
从第1母设备登出
S218
从第2母设备登出
S219
通知转移作业完成
S220
S221
登出

图24

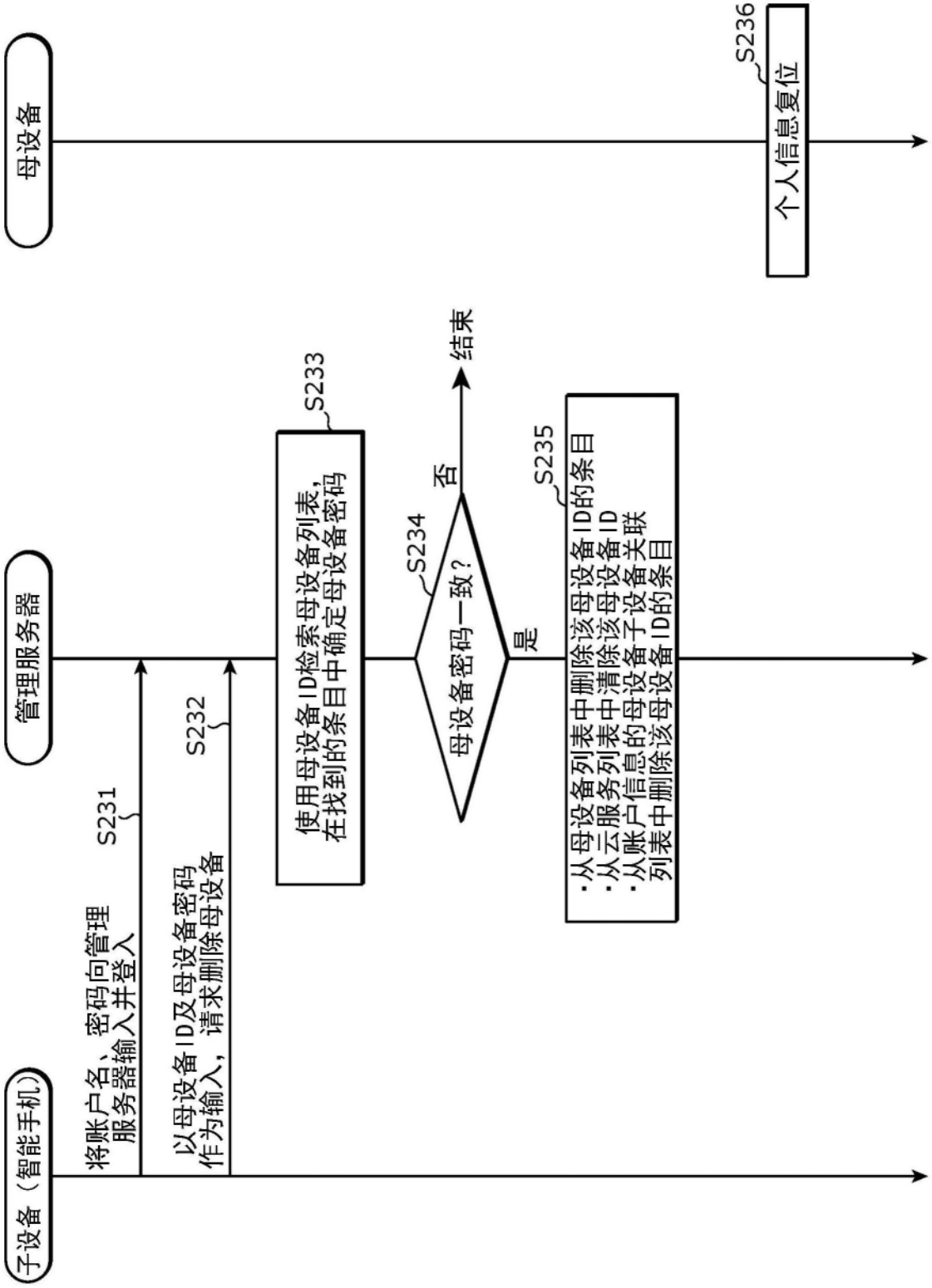

子设备（智能手机）
管理服务器
母设备
将账户名、密码向管理服务器输入并登入
S231
以母设备ID及母设备密码作为输入，请求删除母设备
S232
使用母设备ID检索母设备列表，在找到的条目中确定母设备密码
S233
母设备密码一致？
S234
否
结束
是
S235
·从母设备列表中删除该母设备ID的条目
·从云服务列表中清除该母设备ID
·从账户信息的母设备子设备关联列表中删除该母设备ID的条目
S236
个人信息复位

图25