[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04N 7/173 (2006.01)
G06F 15/00 (2006.01)
G06F 12/14 (2006.01)
H04N 5/44 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200580029634.9

[43] 公开日 2007 年 8 月 1 日

[11] 公开号 CN 101010957A

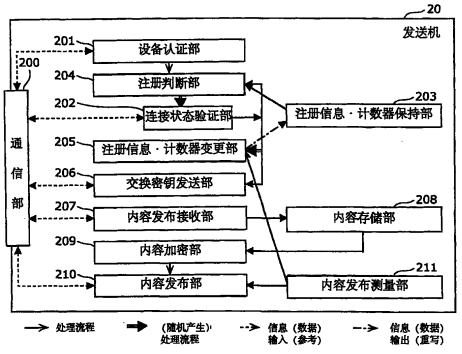
[22] 申请日 2005.9.6
[21] 申请号 200580029634.9
[30] 优先权
[32] 2004. 9. 7 [33] JP [31] 259214/2004
[86] 国际申请 PCT/JP2005/016333 2005.9.6
[87] 国际公布 WO2006/028092 日 2006.3.16
[85] 进入国家阶段日期 2007.3.2
[71] 申请人 松下电器产业株式会社
地址 日本大阪府
[72] 发明人 高辻绫子 饭塚裕之 臼木直司
[74] 专利代理机构 北京德琦知识产权代理有限公司
代理人 陆 弋 宋志强
权利要求书 3 页 说明书 16 页 附图 6 页

[54] 发明名称

内容发布管理装置

[57] 摘要

本发明提供一种内容发布管理装置，用于管理对能够允许共享发送机中存储的内容的接收机的内容发布。 内容发布管理装置是用于管理在发送机向多个接收机发布内容的情况下的内容发布的装置，具有用于将接收有效期间设定到注册信息・计数器保持部(203)的注册信息・计数器变更部(205)，接收有效期间是指被允许共享所述发送机发布的内容的所述接收机能够接收所述内容的时间的上限；注册信息・计数器变更部(205)基于来自所述发送机的内容的发布状况，管理被允许内容共享的全部所述接收机能够接收所述内容的时间。



1. 一种内容发布管理装置，用于管理发送机向多个接收机发布内容的情况下的内容发布，其包括:

设定单元，用于将接收有效期间设定到保持单元，所述接收有效期间是被允许共享所述发送机发布的内容的所述接收机能够接收所述内容的时间的上限;

管理单元，用于基于来自所述发送机的内容的发布状况，对被允许内容共享的全部所述接收机，管理能够接收所述内容的时间。

2、如权利要求 1 所述的内容发布管理装置，其中，

各所述接收机分配有固有的标识;

所述内容发布管理装置进一步具有注册单元，其用于将被允许共享所述发送机发布的内容的所述接收机的标识保存到所述保持单元;

所述设定单元在所述注册单元已将所述接收机的标识保存到所述保持单元的情况下，将所述接收有效期间设定到所述保持单元; 所述管理单元在所述接收有效期间被设定到所述保持单元后，所述发送机发布的内容的发布时间达到所述接收有效期间的情况下，注销所述保持单元中注册的标识。

3、如权利要求 1 所述的内容发布管理装置，其中，

所述发布时间是所述发送机发布内容的实际时间; 所述管理单元从所述接收机能够接收所述内容的时间中减去所述发送机发布内容的实际时间。

4、如权利要求 1 所述的内容发布管理装置，其中，

所述发布时间是由所述发送机发布的内容的播放时间; 所述管理单元从所述接收机能够接收所述内容的时间中减去由所述发送机发布的内容的播放时间。

5、如权利要求 1 所述的内容发布管理装置，其中，

所述发送机加密并发布内容;

被允许共享所述内容的所述接收机是与所述发送机的连接状态满足预

定关系的接收机;

所述设定单元将与所述发送机的连接状态满足预定关系的接收机的标识设定到所述保持单元;

所述发送机在所述标识被设定到所述保持单元之后,向对应于所述标识的所述接收机发送用于解密已加密的所述内容所需的信息。

6、一种内容发布管理装置,用于管理发送机向一个或多个接收机发布内容的情况下的内容的发布,其中各所述接收机分配有固有的标识,所述装置包括:

注册单元,用于将被允许共享所述发送机具有的内容的所述接收机的标识保存到保持单元;

设定单元,用于在所述注册单元已将所述接收机的标识保存到所述保持单元的情况下,将接收有效期间设定到所述保持单元,所述接收有效期间是所述接收机能够接收所述内容的时间的上限;

管理单元,用于在所述接收有效期间被设定到所述保持单元后,在所述发送机发布的内容发布时间达到所述接收有效期间的情况下,注销所述保持单元中注册的标识。

7、如权利要求6所述的内容发布管理装置,其中,

所述发布时间是所述发送机发布内容的实际时间;

所述管理单元从所述接收机能够接收所述内容的时间中减去所述发送机发布内容的实际时间。

8、如权利要求6所述的内容发布管理装置,其中,

所述发布时间是由所述发送机发布的内容的播放时间;

所述管理单元从所述接收机能够接收所述内容的时间中减去由所述发送机发布的内容的播放时间。

9、如权利要求6所述的内容发布管理装置,其中,

所述发送机加密并发布内容;

被允许共享所述内容的所述接收机是与所述发送机的连接状态满足预

定关系的接收机;

所述设定单元将与所述发送机的连接状态满足预定关系的接收机的标识设定到所述保持单元;

所述发送机在所述标识被设定到所述保持单元后,将用于解密被加密的所述内容所需的信息发送到与所述标识对应的所述接收机。

10、一种内容发布管理方法,用于管理发送机向多个接收机发布内容的情况下的内容的发布,包括以下步骤:

设定步骤,用于将接收有效期间设定到保持单元,所述接收有效期间是被允许共享所述发送机发布的内容的所述接收机能够接收所述内容的时间的上限;

管理步骤,用于基于来自所述发送机的内容的发布状况,对被允许内容共享的全部所述接收机,管理能够接收所述内容的时间。

11、一种内容发布管理方法,用于管理发送机向一个或多个接收机发布内容的情况下的内容的发布,其中,各所述接收机分配有固有的标识,所述方法包括:

注册步骤,将被允许共享所述发送机具有的内容的所述接收机的标识保存到保持单元;

设定步骤,所述注册步骤中所述接收机的标识已保存到所述保持单元的情况下,将接收有效期间设定到所述保持单元,所述接收有效期间是所述接收机能够接收所述内容的时间的上限;

管理步骤,在所述接收有效期间被设定到所述保持单元之后,在所述发送机发布的内容的发布时间达到所述接收有效期间的情况下,注销所述保持单元中注册的标识。

内容发布管理装置

技术领域

本发明涉及对发送机的内容的发布进行管理的内容发布管理装置。

背景技术

近年，家庭内的设备通过网络连接起来，用于各种内容共享的家庭网络正在逐步实现。作为一种家庭网络的实现方式可以考虑在家庭内设置一台路由器，此路由器将电视机和录像机等设备（以下称为“接收机”）与存储内容的 DVD 刻录机等发送机以星型方式连接。在此，将路由器设为家庭内唯一与家庭外网络连接的设备。发送机具有将存储的内容根据来自接收机的请求而向此接收机发布的功能。这样，各接收机能够共享发送机中存储的各种内容。

另一方面，从著作权保护的角度，不赞成内容的无限制的共享。所以，仅仅在家庭内的接收机允许共享的内容应当限定为不能向家庭外的接收机发布。因此，发送机收到来自接收机的内容发布请求时，需要判断此接收机是否是被允许共享此内容的家庭内的接收机。

例如，DTLA(Digital Transmission Licensing Administrator)许可的 DTCP 格式（Digital Transmission Content Protection Specification）中，作为此判断方法正在研究：检测发送机和接收机间的通信所用时间是否没有达到预定时间的方法（参考非专利文献 1）。

非专利文献 1： Work Plan for Localizing Transmission, 2003 年 9 月 9 日

但是，还没有考虑到以下具体方法：判断出是家庭内的接收机，管理向能够共享发送机中存储的内容的接收机的内容发布。例如，即使是已判定为家庭内接收机的接收机，从著作权保护的角度而言，也需要防止发送机向此接收机无限制地发布内容。

发明内容

本发明的目的在于提供一种内容发布管理装置，用于管理向能够共享发送机中存储的内容的接收机进行的内容发布。

为达成前述目的，本发明内容发布管理装置，用于管理发送机向多个接收机发布内容的情况下的内容的发布；其具备将接收有效期间设定到保持单元的设定单元，其中，接收有效期间是指被允许共享所述发送机发布的内容的所述接收机能够接收所述内容的时间的上限；以及管理单元，用于基于来自所述发送机的内容的发布状况，对被允许内容共享的全部所述接收机，管理能够接收所述内容的时间。

例如，各所述接收机分配有固有的标识，本发明内容发布管理装置进一步具有注册单元，用于将被允许共享所述发送机发布的内容的所述接收机的标识保存到所述保持单元；所述设定单元在所述注册单元已将所述接收机的标识保存到所述保持单元的情况下，将所述接收有效期间设定到所述保持单元；所述管理单元在所述接收有效期间被设定到所述保持单元之后，所述发送机发布内容的发布时间已达到所述接收有效期间的情况下，注销所述保持单元中注册的标识。

例如，所述发布时间是所述发送机发布内容的实际时间；所述管理单元从所述接收机能够接收所述内容的时间中减去所述发送机发布内容的实际时间。

例如，所述发布时间是由所述发送机发布的内容的播放时间；所述管理单元从所述接收机能够接收所述内容的时间中减去由所述发送机发布的内容的播放时间。

例如，所述发送机加密并发布内容，被允许共享所述内容的所述接收机是与所述发送机的连接状态满足预定关系的接收机，所述设定单元将与所述发送机的连接状态满足预定关系的接收机的标识设定到所述保持单元；所述发送机在所述标识被设定到所述保持单元之后，向所述标识对应的所述接收

机发送用于解密已加密的所述内容所需的信息。

另外，本发明内容发布管理装置是管理发送机向一个或多个接收机发布内容的情况下的内容的发布的装置，各所述接收机分配有固有的标识；所述装置具有注册单元，用于将被允许共享所述发送机具有的内容的所述接收机的标识保存到保持单元；设定单元，用于在所述注册单元将所述接收机的标识保存到所述保持单元的情况下，将接收有效期间设定到所述保持单元，其中接收有效期间是指所述接收机能够接收所述内容的时间的上限；以及管理单元，用于在所述接收有效期间已被设定到所述保持单元之后，在所述发送机发布内容的发布时间已达到所述接收有效期间的情况下，注销所述保持单元中注册的标识。

例如，所述发布时间是所述发送机发布内容的实际时间；所述管理单元从所述接收机能够接收所述内容的时间中减去所述发送机发布内容的实际时间。

例如，所述发布时间是由所述发送机发布的内容的播放时间；所述管理单元从所述接收机能够接收所述内容的时间中减去由所述发送机发布的内容的播放时间。

例如，所述发送机加密并发布内容；被允许共享所述内容的所述接收机是与所述发送机的连接状态满足预定关系的接收机；所述设定单元将与所述发送机的连接状态满足预定关系的接收机的标识设定到所述保持单元；所述发送机在所述标识被设定到所述保持单元之后，向所述标识对应的所述接收机发送用于解密已加密的所述内容所需的信息。

本发明也能通过以本发明内容发布管理装置的特征性结构单元作为步骤的内容发布管理方法实现；还能通过使这些步骤在计算机中运行的程序而实现。此程序也能通过 CD－ROM 等存储介质、通信网络等传输介质而流通。

本发明能够提供一种内容发布管理装置，用于管理对能够共享发布机中存储的内容的接收机的内容发布。

本发明内容发布管理装置中，发送机可以并不分别获知对各个接收机的

发布状况而统一管理内容发布状况，所以管理很容易，同时，能够可靠地防止无限制的内容共享。且，对于注册状态的接收机，通过免去费时的有关连接状态的判断处理，既实现了内容的安全保护，又减轻了对接收机的允许判断处理的负担。另外，还有这样的效果：例如，由于只以发送机已发布内容的时间为对象，测量接收机能够接收内容的时间，所以，接收机被允许内容共享之后，即使在用户中途不得已而中断欣赏的情况下（不速之客等情况）的空白时间也没耗费，减少再次得到发送机许可的处理频率。

这样，通过一个计数器管理多个接收机各自能够接收内容的时间，发送机能够以很少的资源管理内容的发布，并且能方便安装。

还有这样的效果：针对每个接收机，利用计数器管理接收机能够接收内容的时间，在各接收机注册的时刻分别将计数器的值初始化为预定值，从而，不会因为受到在此接收机注册之前的其他接收机的发布状况的影响等等而将此接收机的初始值动态地设短，以减少得到发送机许可的处理频率。

附图说明

图 1 是表示本实施方式中家庭网络 1 的结构的图。

图 2 是表示实施方式中发送机 20 的结构的图。

图 3 是表示第一实施方式中直到发送机 20 向进行认证请求的接收机发送交换密钥的处理步骤的图。

图 4 是表示第一实施方式中从发送机 20 开始内容的发布到结束的处理步骤的图。

图 5 是表示第一实施方式的发送机 20 保持的、指定各接收机能够接收内容的期间的计数器的值的变化的示例的图。

图 6 是表示第二实施方式的发送机 20 保持的、指定各接收机能够接收内容的期间的计数器的值的变化的示例的图。

附图标记说明

1 家庭网络

10 路由器

20 发送机

30 接收机

31 接收机

32 接收机

200 通信部

201 设备认证部

202 连接状态验证部

203 注册信息·计数器保持部

204 注册判断部

205 注册信息·计数器变更部

206 交换密钥发送部

207 内容发布接收部

208 内容存储部

209 内容加密部

210 内容发布部

211 内容发布测量部

具体实施方式

下面参考附图说明本发明的具体实施方式。

（第一实施方式）

首先，用附图 1 说明第一实施方式的家庭网络 1 的结构。

图 1 是表示第一实施方式的家庭网络 1 的结构的图。

家庭网络 1 是为了实现家庭内的内容共享的网络，由路由器 10、发送机 20 以及接收机 30、31、32 构成。路由器 10 在家庭网络 1 中唯一与家庭网络 1 的外部网络（因特网）连接。发送机 20 和接收机 30、31、32 连接路由

器 10。家庭网络 1 是以路由器 10 为中心的星型网络。

发送机 20 中存储有各种内容，通过路由器 10 接收来自其他设备的认证请求，判断其他设备是家庭网络 1 内的设备，并判断其是否是能够共享发送机 20 存储的内容的设备。在判断出其他设备是能够共享内容的设备的情况下，发送机 20 向其他设备发布其他设备所请求的内容。

发送机 20 是具备发布存储的各种内容的功能的 AV 服务器等。

接收机 30、31、32 是具有获取各种内容的功能的电视机、录像机、DVD 播放机等。

第一实施方式中，发送机 20 对于允许内容共享的接收机，能够在预定的接收有效期间接收内容。在此，预定的接收有效期间是预先确定的基准时间。发送机 20 具有用于指定，被允许内容共享的接收机中，接收机能够接收内容的期间的计数器。发送机 20 对于来自接收机的认证请求，判断此接收机是合法设备（以下称为“认证”），并且，确认发送机 20 与此接收机间的连接状态是否满足预定条件（以下称为“连接状态验证”）；在判断出此接收机能够允许共享内容的情况下，将此接收机作为允许内容共享的接收机而注册到内部，并在计数器设定此接收机用的预定的接收有效期间。即，对此接收机用的计数器进行初始化。利用此接收机用的计数器，在表示已经过预定的接收有效期间的时间点，从发送机 20 注销此接收机的注册。

虽然发送机 20 发出的内容是加密发布的，但是，对于来自接收机的认证请求，如果此接收机尚未注册，则发送机 20 进行认证和连接状态验证，在注册之后，才向此接收机发送对加密内容进行解密所需的信息。另一方面，如果此接收机已经注册，则发送机 20 只对此接收机进行认证，就向其发送对加密内容进行解密所需的信息。

在发送机 20 发布内容的期间，各接收机用的计数器都递减。换言之，如果向已注册接收机中任一个发布内容，则全部接收机用计数器同样地递减。

在此，例如，使用实时传输协议（RTP），为了实时播放而以一定的数

据速率广播（或者多播）发布内容。因为发布的内容已加密，即使接收机被允许共享内容，如果没有获得解密所需信息，也无法对加密的内容进行解密。

以下详细说明实现前述功能的发送机 20。

首先，用图 2 说明发送机 20 的结构。

图 2 是表示发送机 20 的结构的图。

发送机 20 包括通信部 200、设备认证部 201、连接状态验证部 202、注册信息· 计数器保持部 203、注册判断部 204、注册信息· 计数器变更部 205、交换密钥发送部 206、内容发布接收部 207、内容存储部 208、内容加密部 209、内容发布部 210，以及内容发布测量部 211。

通信部 200 与发送机 20 的外部设备进行通信。发送机 20 内部的各组成部分通过通信部 200 与发送机 20 的外部设备进行通信。

设备认证部 201 接收来自接收机的认证请求，并且通过认证确认此接收机是否是合法设备。在此，作为此设备认证的方法是，例如，发送机 20 和接收机各自保留公钥密码的钥匙对（公钥、密钥）和证书，发送机 20 和接收机利用公钥和密钥以挑战/应答方式进行认证。

连接状态验证部 202 验证进行认证请求的接收机（请求接收机）的连接状态是否满足预定条件。在此，使用的验证方法是：例如，测定从发送机 20 向请求接收机发送回显（echo）请求数据开始，直到接收来自请求接收机的对应于此回显请求数据的回显应答数据所需的往返时间，如果测到的往返时间在预先规定的基准时间以内，则判定请求接收机是家庭网络 1 内的设备。以下，将采用此方法的验证称为回路响应时间（RTT）验证。前述连接状态验证和 RTT 验证在实施方式中具有相同含义。

注册信息· 计数器保持部 203 保持识别码和表示预定的接收有效期间的计数器，该识别码是设备认证部 201 的认证结果及连接状态验证部 202 的验证结果都为肯定的接收机的识别码。在此，例如，使用由设备认证部 201 得到的证书中记载的设备固有信息（例如，设备 ID）作为识别码。

注册判断部 204 检查注册信息· 计数器保持部 203，判断设备认证部 201

的认证结果为肯定的接收机是否是已注册的设备。

注册信息·计数器变更部 205 变更注册信息·计数器保持部 203 的信息。变更包括：（A）新的注册／计数器的初始化；（B）向计数器反映实施的内容发布时间；（C）注册（／计数器）的删除。（A）中，在注册信息·计数器保持部 203 保存应注册的接收机的识别码，并将此接收机的计数器初始化。在此，初始化是指将计数器的值设定为预先设定的基准值（接收有效期间：接收机能够接收内容的期间的上限）。在此，基准值是时间，接收有效期间为 40 个时间的情况下，例如，将计数器初始值设为“40”，将变更单位设为 1 个时间。（B）中，内容发布测量部 211 测量到的内容发布的时间每增加 1 个时间，将注册信息·计数器保持部 203 中保持的全部注册接收机的计数器的值减“1”。在此，若有值变为“0”的计数器，就从注册信息·计数器保持部 203 中删除此计数器所对应的接收机的注册（换言之，删除此计数器所对应的接收机的识别码和计数器）（C）。

交换密钥发送部 206 对已注册状态的接收机发送对加密的内容进行解密所需的信息。在此，例如，所需的信息是指交换密钥，在生成内容解密中使用的内容·密钥时，这是必需的。此交换密钥，通过设备认证部 201，使用发送机 20 和前述已注册状态的接收机之间共享的认证密钥发送。发送机 20 按照预定规则的时序变更交换密钥，但是变更时序的规则不是本发明的重点，故省略其说明。实施方式中，交换密钥发送部 206 发送最新的交换密钥，即，如果当前内容正在发布中，就发送用于解密此内容的交换密钥。

内容发布接收部 207 接收来自各接收机的内容发布请求，并应答。

内容存储部 208 存储成为发布对象的各种内容。

内容加密部 209 对发布内容进行加密。内容加密部 209，例如，根据交换密钥和内容的复制控制信息等生成内容·密钥，由此加密发布内容。

内容发布部 210 发布加密后的内容。

内容发布测量部 211 测量内容被发布的时间。

接下来，用图 3 和图 4 说明发送机 20 的工作。

首先，用图 2 和图 3 说明发送机 20 向进行认证请求的接收机发送交换密钥为止的处理顺序。

图 3 是表示发送机 20 向进行认证请求的接收机发送交换密钥为止的处理顺序的图。

步骤 S21：设备认证部 201 中执行，对进行认证请求的接收机进行设备认证，确认是否是合法设备。设备认证的方法如前述。如果确认是合法设备，则进入步骤 S22，判断此设备是否是已注册的接收机。如果不是，则结束处理。

步骤 S22：注册判断部 204 中执行，判断由设备认证部 201 认证为合法设备的接收机是否是已注册的设备。注册判断中利用步骤 S21 中获得的设备固有的识别码。如果识别码是注册的，则进入步骤 S25，发送交换密钥。如果不是，则进入步骤 S23，进行 RTT 验证。

步骤 S23：连接状态验证部 202 中执行，进行 RTT 验证，以判断由设备认证部 201 认证为合法设备的接收机的连接状态是否满足预定条件。RTT 验证如前述。如果确认满足预定条件，则进入步骤 S24，将此接收机作为能够共享内容的接收机而注册到注册信息·计数器保持部 203。如果不是，则结束处理。

步骤 S24：注册信息·计数器变更部 205 中执行，将由连接状态验证部 202 判断为连接状态满足预定条件的接收机的、在步骤 S21 中获得的识别码注册到注册信息·计数器保持部 203，并且将对应的计数器初始化。之后进入步骤 S25，发送交换密钥。

步骤 S25：交换密钥发送部 206 中执行，将对发布的加密内容进行解密所需的交换密钥，用步骤 S21 中共享的认证密钥进行加密，并且发送给进行认证请求的接收机。

以下，用图 2 和图 4 说明从发送机 20 开始内容发布到结束为止的处理顺序。

图 4 是表示从发送机 20 开始发布内容到结束的处理顺序的图。

以下的步骤 S31、步骤 S32 及步骤 S33 在内容发布测量部 211 中执行；步骤 S34、步骤 S35 及步骤 S36 在注册信息· 计数器变更部 205 中执行。

步骤 S31：判断从内容的发布开始，或者从 1 个时间测量被重置开始，内容的发布是否已经过 1 个时间。如果没有经过 1 个时间，则进入步骤 S32，确认内容是否结束。如果经过了 1 个时间，则进入步骤 S33，重置 1 个时间测量。

步骤 S32：判断内容是否结束。如果内容继续，则返回步骤 S31；判断是否已经过 1 个时间。如果内容结束，则结束处理。

步骤 S33：重置 1 个时间的测量。之后，进入步骤 S34，将全部注册接收机的计数器递减。

步骤 S34：从全部注册接收机的计数器（表示能够进行内容发布的剩余的时间）中减去（递减）“1”（表示已进行内容发布 1 个时间的值）。之后进入步骤 S35，确认是否有计数器的值变为“0”的注册接收机。

步骤 S35：确认是否有值变为“0”的注册接收机的计数器。如果有值变为“0”的计数器，则进入步骤 S36，从注册信息· 计数器保持部 203 中注销此接收机的注册。如果没有值变为“0”的计数器，则直接返回步骤 S31，判断是否又经过了 1 个时间。

步骤 S36：从注册信息· 计数器保持部 203 中删除计数器的值变为“0”的接收机的识别码，使注册无效。直接返回步骤 S31，判断是否又经过了 1 个时间。

图 5 是表示第一实施方式的发送机 20 保持的计数器的值的变化的示例的图，其中，计数器用于指定各接收机能够接收内容的期间。

发送机 20 接收来自接收机 30 的内容发布请求 CR01、CR02，分别发布内容 1、内容 2；接收来自接收机 32 的内容发布请求 CR21，发布内容 3。然后，发送机 20 接收来自接收机 30 的内容发布请求 CR03，发布内容 4。而且，接收机 31 在发送机 20 接收到来自接收机 30 的内容发布请求 CR01 并发布内容 1 的时候，请求同时共享内容 1（CR11）。

内容 1 的长度是 15 个时间；内容 2 的长度是 20 个时间；内容 3 的长度是 13 个时间；内容 4 的长度是 10 个时间。

在此，说明与接收机 30 对应的计数器的值的变化。

发送机 20 接收来自接收机 30 的认证请求 AR01，进行认证（A1）和 RTT 验证（B1），判断出接收机 30 是合法设备并其连接状态满足预定条件，对此接收机进行向注册信息· 计数器保持部 203 的注册。在此，接收机 30 的计数器被初始化为“40”（TC01）；交换密钥 Kx1（X01）被发送到接收机 30。

发送机 20 接收来自接收机 30 的内容 1 的发布请求（CR01），利用基于交换密钥 Kx1 生成的内容· 密钥而加密内容 1，并发布。执行内容发布的同时，接收机 30 对应的计数器递减下去。发送机 20 接着接收到来自接收机 30 的内容 2 的发布请求（CR02）。发送机 20 利用基于交换密钥 Kx1 生成的内容· 密钥加密内容 2，并发布。

在此，假设，接收机 30 在接收到 15 个时间的内容 2 时，中断发布请求（BR01）。例如，接收机 30 的用户正在欣赏内容 2 的时候，有不速之客到来，从而中止欣赏的情况。在此情况下，内容 2 的发布被中断，对应于接收机 30 的计数器的值只递减内容 2 的发布已进行的 15 个时间，停止在“10”（TC02）。

中断内容 2 的发布之后，发送机 20 接收到来自接收机 32 的认证请求 AR21，进行认证（A1）和 RTT 验证（B1），判断出接收机 32 是合法设备且其连接状态满足预定条件，进行注册，向接收机 32 发送交换密钥 Kx2（X21）。

另一方面，接收机 30 在中断内容 2 的接收后，例如，暂时处于关机状态，一段时间后再次成为开机状态。此时，发送机 20 接收来自接收机 30 的认证请求 AR02，进行认证（A2），接收机 30 的计数器的值是“10”，因为能够确认此接收机是没有超过接收有效期间的注册中的接收机，所以不进行 RTT 验证，而向接收机 30 发送最新的交换密钥 Kx2（X02）。然后，发

送机 20 接收来自接收机 32 的内容 3 的发布请求（CR21），利用基于交换密钥 Kx2 生成的内容· 密钥加密内容 3，并发布。

在此，内容发布请求只有请求源 IP 地址这样的动态信息。因此，发送机 20 很难判断该内容发布请求是来自哪个接收机的请求。虽然可以利用在内容发布请求中添加认证· 注册时用到的识别码等的方法来识别· 管理内容发布请求源接收机，但是处理变得很复杂。另外，假设即使识别出内容发布请求源接收机，但广播中的内容发布中，也不能保证只有内容发布请求源接收机接收内容。例如，内容发布请求 CR21 是来自接收机 32 的发布请求，即使是在接收机 30 没有向发送机 20 发出内容 3 的发布请求的情况下，接收机 30 也能利用已经得到的交换密钥 Kx2，接收并解密内容 3。

因此，在执行内容 3 的发布的同时，发送机 20 不仅递减接收机 32 的计数器，而且不管接收机 30 是否正在接收内容，递减接收机 30 的计数器。在接收机 30 的计数器的值变为“0”的时刻（TC03），从注册信息· 计数器保持部 203 中注销允许接收机 30 内容共享的注册。

然后，如果发送机 20 接收到来自接收机 30 的认证请求 AR03，由于接收机 30 的注册已不存在，所以进行认证（A3）和 RTT 验证（B3），判断出接收机 30 是合法设备并其连接状态满足预定条件，并进行注册。在此，接收机 30 的计数器被初始化为“40”（TC04），最新交换密钥 Kx3（X03）被发送到接收机 30。

在此，假设，在发布上述内容 3 时，发送机 20 以某种方法识别出内容发布请求 CR21 是来自接收机 32 的发布请求；不递减接收机 30 的计数器；在认证请求 AR03 的时刻，接收机 30 的注册还在继续（图 5 中对应于接收机 30 的计数器的值的虚线部 D）。在此情况下，如果接收机 30 还接收并解密了内容 3 的发布，尽管向接收机 30 进行的是超过接收有效时间 40 个时间的 43 个时间的内容发布，发送机 20 接收到来自接收机 30 的认证请求 AR03 后，只进行认证（A3），而不进行 RTT 验证（B3），就向接收机 30 发送最新交换密钥 Kx3。

如果假设接收机30在进行内容4的发布请求（CR03）之前就被带出家庭外，则在进行认证请求 AR03 的时刻，即使在 RTT 验证中判断出不满足预定条件等情况下，接收机30也可能在进一步超过被允许的接收有效期间，非法接收并解密内容。

其次，说明对应于接收机31的计数器的值的变化。

发送机20接收来自接收机30的内容发布请求（CR01），在内容1的发布中，接收来自接收机31的认证请求 AR11，进行认证（A1）和 RTT 验证（B1），判断出接收机31是合法设备并其连接状态满足预定条件，并进行注册。在此，接收机31的计数器被初始化为“40”（TC11）；交换密钥 Kx1（X11）发送到接收机31。然后，无论是否有来自接收机31的内容发布请求 CR11，在执行内容1的发布的同时，对应于接收机31的计数器递减，在内容 1 的发布结束的时候，对应于接收机 31 的计数器的值变为“34”（TC12）。

接下来，如果发送机20接收到来自接收机30的发布请求 CR02，则在执行内容2的发布的同时，将接收机31的计数器递减下去，不管接收机31是否正在接收内容。由于内容2的发布被接收机30中断，对应于接收机31的计数器的值只是递减内容 2 的发布已进行的 15 个时间，停止在“19”（TC13）。然后，发送机20接收来自接收机32的内容发布请求 CR21，发布内容3；接收来自接收机30的内容发布请求 CR03，发布内容4；在执行这些内容的发布的同时，递减对应于接收机31的计数器。对应于接收机31的计数器的值在13个时间的内容3的发布结束的时候，变成“6”（TC14）；在内容4的发布过程中成为“0”（TC15）。

接下来说明对应于接收机32的计数器的值的变化。

发送机 20 接收来自接收机 32 的认证请求 AR21，进行认证（A1）和 RTT 验证（B1），判断出接收机32是合法设备并其连接状态满足预定条件，并进行注册。在此，接收机32的计数器被初始化为“40”（TC21），发送机20向接收机32发送交换密钥 Kx2。

发送机 20 接收来自接收机 32 的内容 3 的发布请求（CR21），利用基于交换密钥 Kx2 生成的内容· 密钥加密内容 3，并发布。发布内容 3 的同时，对应于接收机 32 的计数器递减，在 13 个时间的内容 3 的发布结束的时候，对应于接收机 32 的计数器的值变成“27”（TC22）。然后，发送机 20 接收来自接收机 30 的内容发布请求 CR03，并发布内容 4，将对应于接收机 32 的计数器递减下去。

因而，发送机 20 可以并不分别获知对各个接收机的发布状况而统一管理内容发布状况，所以内容发布的管理很容易，同时，能够可靠地防止无限制的内容共享。另外，对于注册状态的接收机，通过免去费时的有关连接状态的判断处理，既实现了内容的安全保护，又减轻了允许接收机共享内容的判断处理的负担。

指定接收机能够接收内容的期间的计数器，由于在发送机 20 注册各接收机的时刻被分别初始化为预定值，例如，不会因为受到接收机被注册前的发布状况的影响而把初始值动态地设短，所以，接收机得到发送机 20 的许可的处理频率就降低。另外，由于计数器只递减发送机 20 发布内容的时间，所以，接收机被允许内容共享之后，即使在用户中途不得已而中断欣赏的情况下（不速之客等情况）的空白时间也没耗费，再次请求发送机 20 的许可的处理频率也降低。

虽然在第一实施方式中，说明了发送机 20 实时地以流发布内容的情况，但是本发明并不限于此，例如，在各接收机使用 HTTP 协议下载而共享发送机 20 中存储的内容的非实时发布的情况也适用。在非实时发布中，可以假定 2 个时间的内容能够用 1 个时间发布。明显地，在这样的情况下，指定接收有效期间的计数器递减的可以不是内容的发布时间（1 个时间）而是播放时的内容的长度（2 个时间）。

虽然第一实施方式中，是以假定内容发布管理装置安装在发送机 20 中的情况进行了说明。但是，内容发布管理装置与发送机 20 也可以单独设置。注册信息· 计数器变更部 205 只是本发明的内容发布管理装置的设定单元、

管理单元、及注册单元的一个示例。

（第二实施方式）

第二实施方式中，说明与第一实施方式不同的部分。

第二实施方式中，发送机 20 对于被允许内容共享的接收机测量接收机能够接收内容的期间时，仅用一个计数器管理全注册接收机的内容发布状况。发送机 20 对来自接收机的认证请求，进行认证和 RTT 验证，并且在判定可以允许内容共享的情况下，将此接收机作为许可接收机而注册。发送机 20，在一个接收机注册的时刻，将全部接收机能够接收内容的期间的上限（接收有效期间）设定到共通计数器。即，发送机 20 将对应于全部注册接收机的共通计数器初始化。在测量到已经过预定的接收有效期间的时刻，从发送机 20 注销全部注册接收机的注册。计数器在发送机 20 发布内容的期间递减。也就是说，如果内容发布到已注册的接收机中的任何一个，计数器就递减。

图 6 是表示第二实施方式中的发送机 20 保持的计数器的值的变化的示例的图，其中，此计数器规定各接收机能够接收内容的期间。

接收机 30、31、32 的动作与前述第一实施方式中的图 5 的情况相同。

发送机 20 接收来自接收机 30 的认证请求 AR01，进行认证（A1）和 RTT 验证（B1），判断出接收机 30 是合法设备并其连接状态满足预定条件，并进行注册（R1）。在此，计数器被初始化为“40”（TC01）；交换密钥 Kx1 发送到接收机 30（X01）。发送机 20 接收来自接收机 30 的内容 1 的发布请求（CR01），并且使用基于交换密钥 Kx1 生成的内容· 密钥加密内容 1，并发布。执行内容的发布的同时，计数器递减。

其间，发送机 20 从接收机 31 接收认证请求 AR11，进行认证（A1）和 RTT 验证（B1），判断出接收机 31 是合法设备并其连接状态满足预定条件，并进行注册（R2）。接收机 30 接着进行内容 2 的发布请求（CR02）。发送机 20 使用基于交换密钥 Kx1 生成的内容· 密钥加密内容 2，并发布。在此，如果接收机 30 在接收了 15 个时间的内容 2 时中断发布请求，则内容 2 的发布被中断，计数器的值只递减内容 2 的发布已进行的 15 个时间，停止在“10”

（TC02）。

接收机 30 中断内容 2 的接收后，发送机 20 从接收机 32 接收认证请求 AR21，进行认证（A1）和 RTT 验证（B1），判断出接收机 32 是合法设备并其连接状态满足预定条件，进行注册（R3），并向接收机 32 发送交换密钥 Kx2。

一方面，在此，虽然发送机 20 从接收机 30 接收认证请求 AR02，并进行认证（A2），但是由于计数器的值是“10”，并且，接收机 30 的注册仍然存在，因此，不进行 RTT 验证，就向接收机 30 发送最新交换密钥 Kx2（X02）。然后，发送机 20 从接收机 32 接收内容 3 的发布请求（CR21），使用基于交换密钥 Kx2 生成的内容·密钥加密内容 3，并发布。发送机 20 在执行内容 3 的发布的同时，递减计数器。在计数器的值变成“0”的时刻（TC03），注销允许全部注册接收机（接收机 30、31、32）的内容共享的注册。

然后，如果发送机 20 从接收机 30 接收到认证请求 AR03，则由于接收机 30 没有被注册到注册信息·计数器保持部 203，所以进行认证（A3）和 RTT 验证（B3），判断出接收机 30 是合法设备并其连接状态满足预定条件，并进行注册。在此，计数器被初始化为“40”（TC04），最新交换密钥 Kx3 发送到接收机 30（X03）。

因此，明显的，本发明能够可靠地防止无限制的内容共享，发送机 20 以很少的资源就能管理内容的发布，安装也很简单。

在实施方式中，用 RTT 验证来验证发送机和进行认证请求的接收机之间的连接状态是否满足预定条件。也可以用存活时间（Time To Live）来验证连接状态是否满足预定条件。

本发明的内容发布管理装置适用于作为在网络中向内容共享的接收机发布预定期间内容的同时，管理此内容的发布的发送机等。

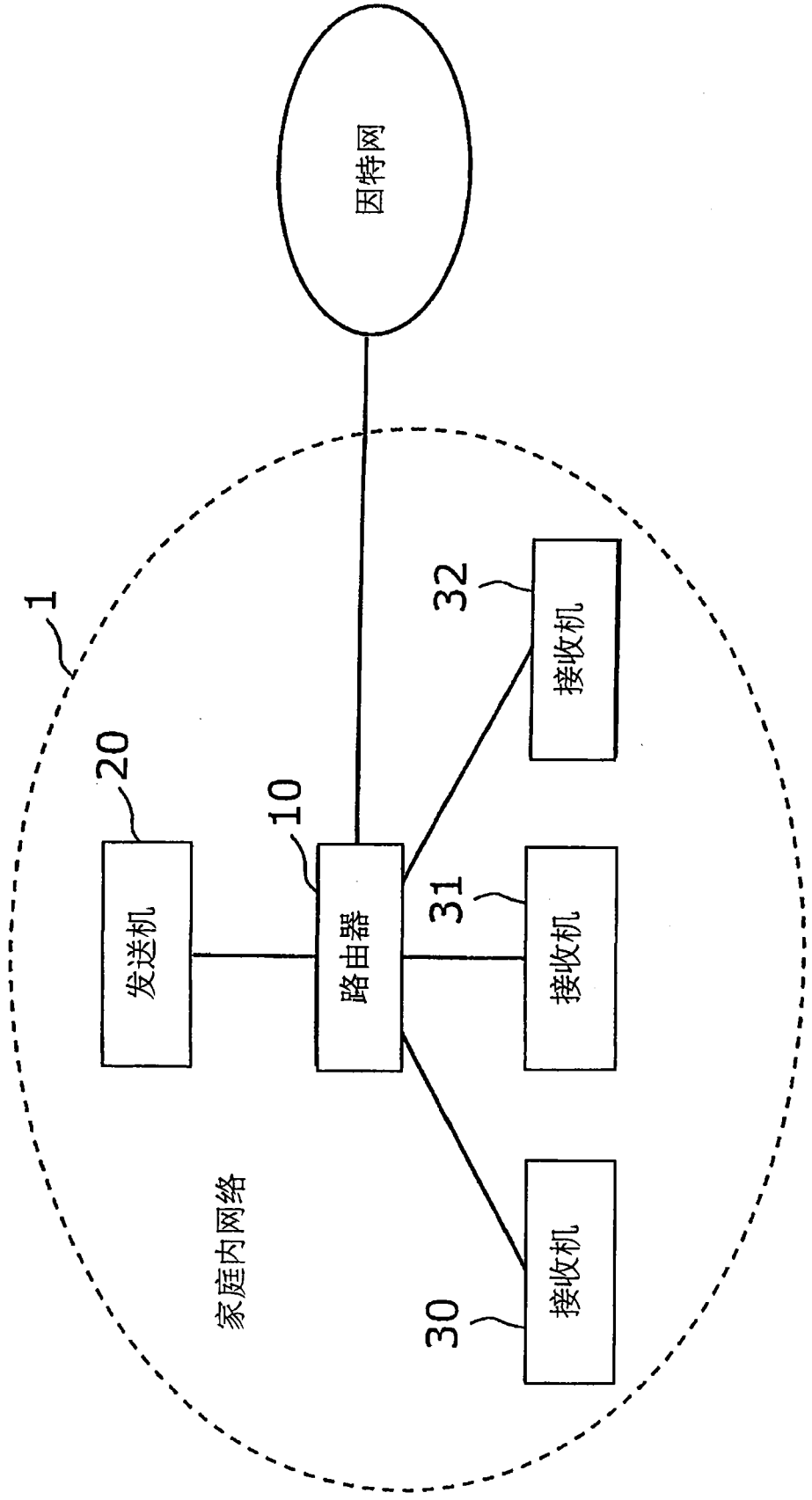


图 1

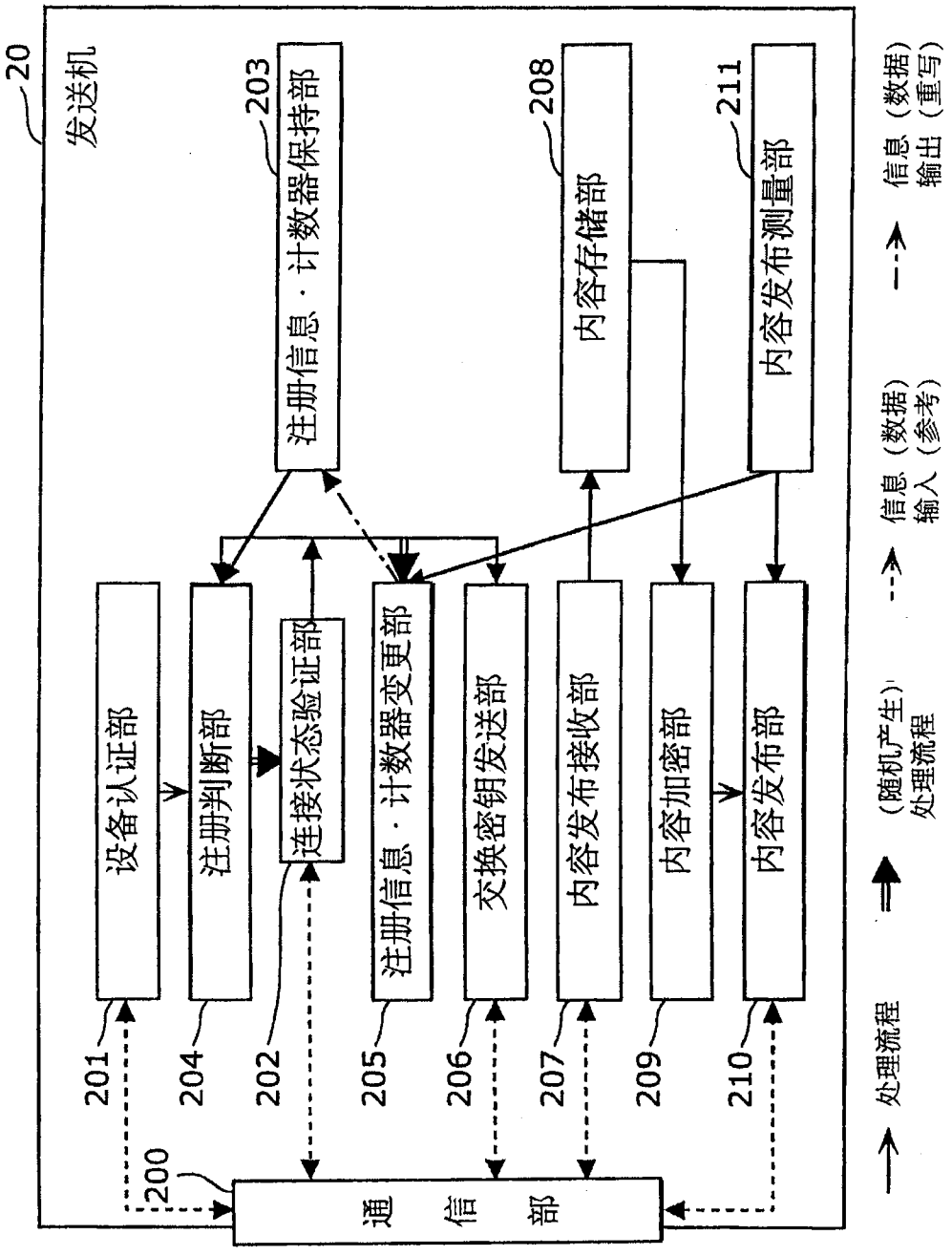

20
发送机
设备认证部
注册判断部
连接状态验证部
注册信息·计数器保持部
注册信息·计数器变更部
交换密钥发送部
内容发布接收部
内容加密部
内容发布部
内容存储部
内容发布测量部
通 信 部
200
201
202
203
204
205
206
207
208
209
210
211
处理流程
(随机产生)
处理流程
信息(数据)
输入(参考)
信息(数据)
输出(重写)

图 2

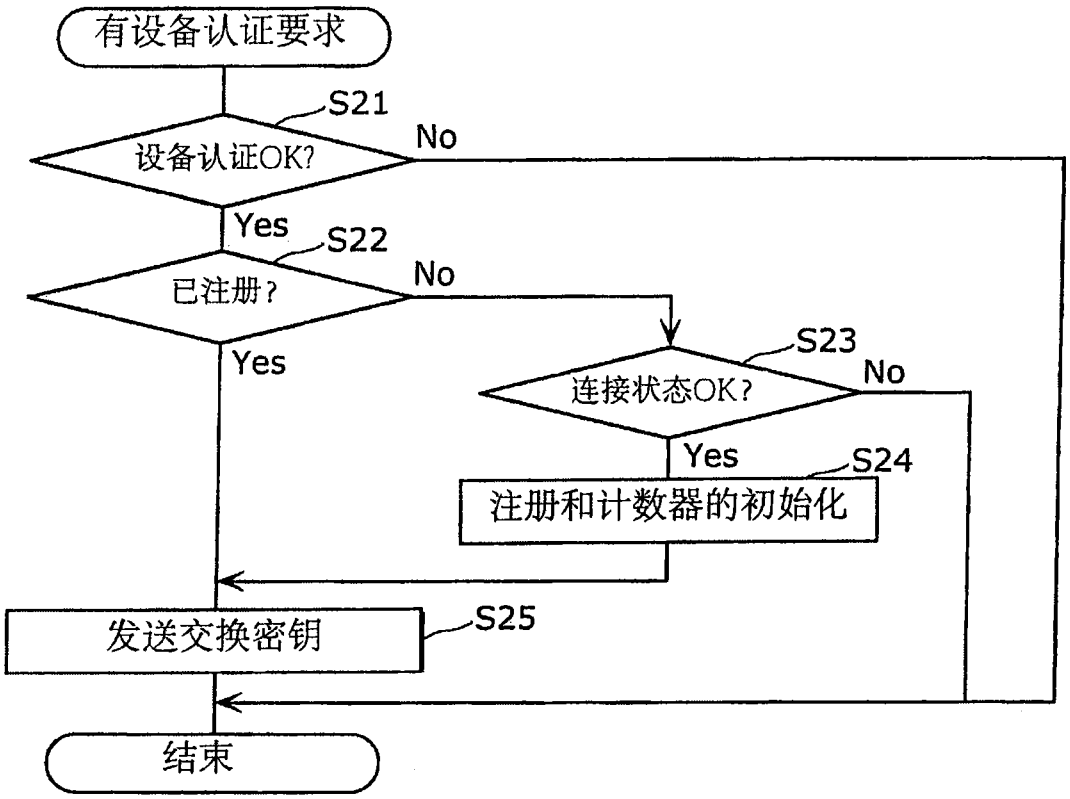

有设备认证要求
S21
设备认证OK?
No
Yes
S22
已注册?
No
Yes
S23
连接状态OK?
No
Yes
S24
注册和计数器的初始化
发送交换密钥
S25
结束

图 3

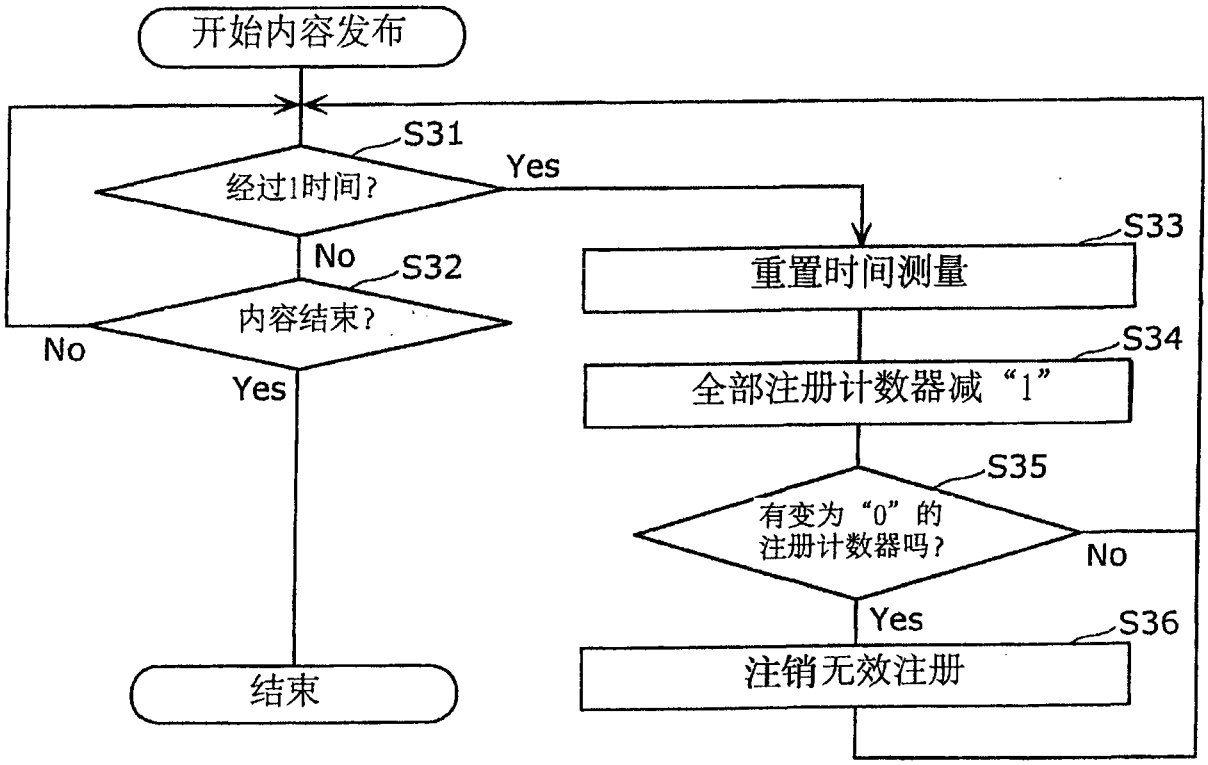

开始内容发布
S31
经过1时间?
Yes
No
S32
内容结束?
No
Yes
结束
S33
重置时间测量
S34
全部注册计数器减“1”
S35
有变为“0”的
注册计数器吗?
No
Yes
S36
注销无效注册

图 4

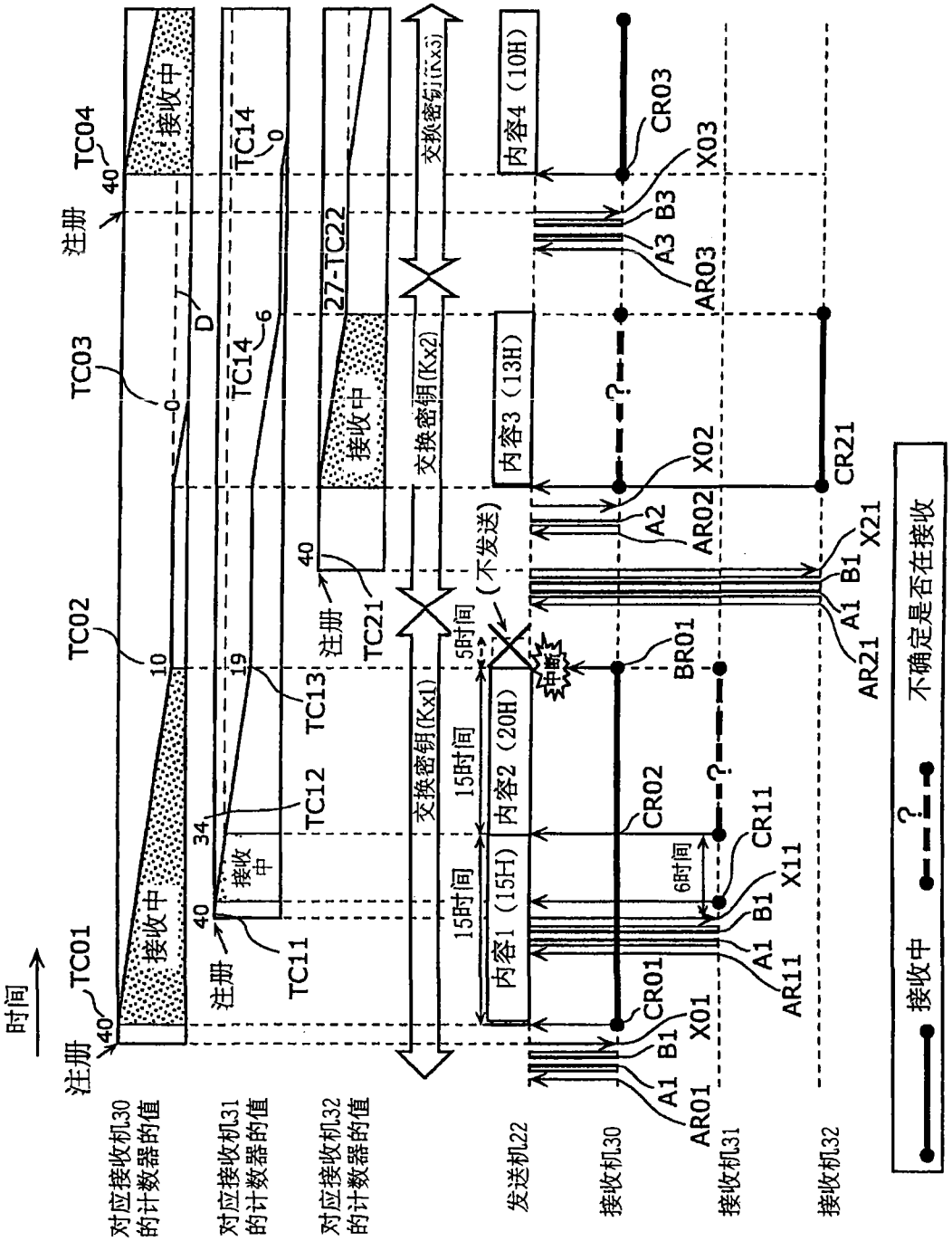

时间
注册
TC01
对应接收机30的计数器的值
接收中
TC02
TC03
TC04
注册
对应接收机31的计数器的值
TC11
TC12
TC13
TC14
对应接收机32的计数器的值
TC21
27-TC22
交换密钥(Kx1)
交换密钥(Kx2)
交换密钥(Kx3)
15时间
内容1（15H）
内容2（20H）
内容3（13H）
内容4（10H）
(不发送)
发送机22
接收机30
接收机31
接收机32
CR01
CR02
CR03
CR11
CR21
BR01
X01
X02
X03
X11
X21
A1
A2
A3
B1
B3
AR01
AR02
AR03
AR11
AR21
6时间
接收中
不确定是否在接收

图 5

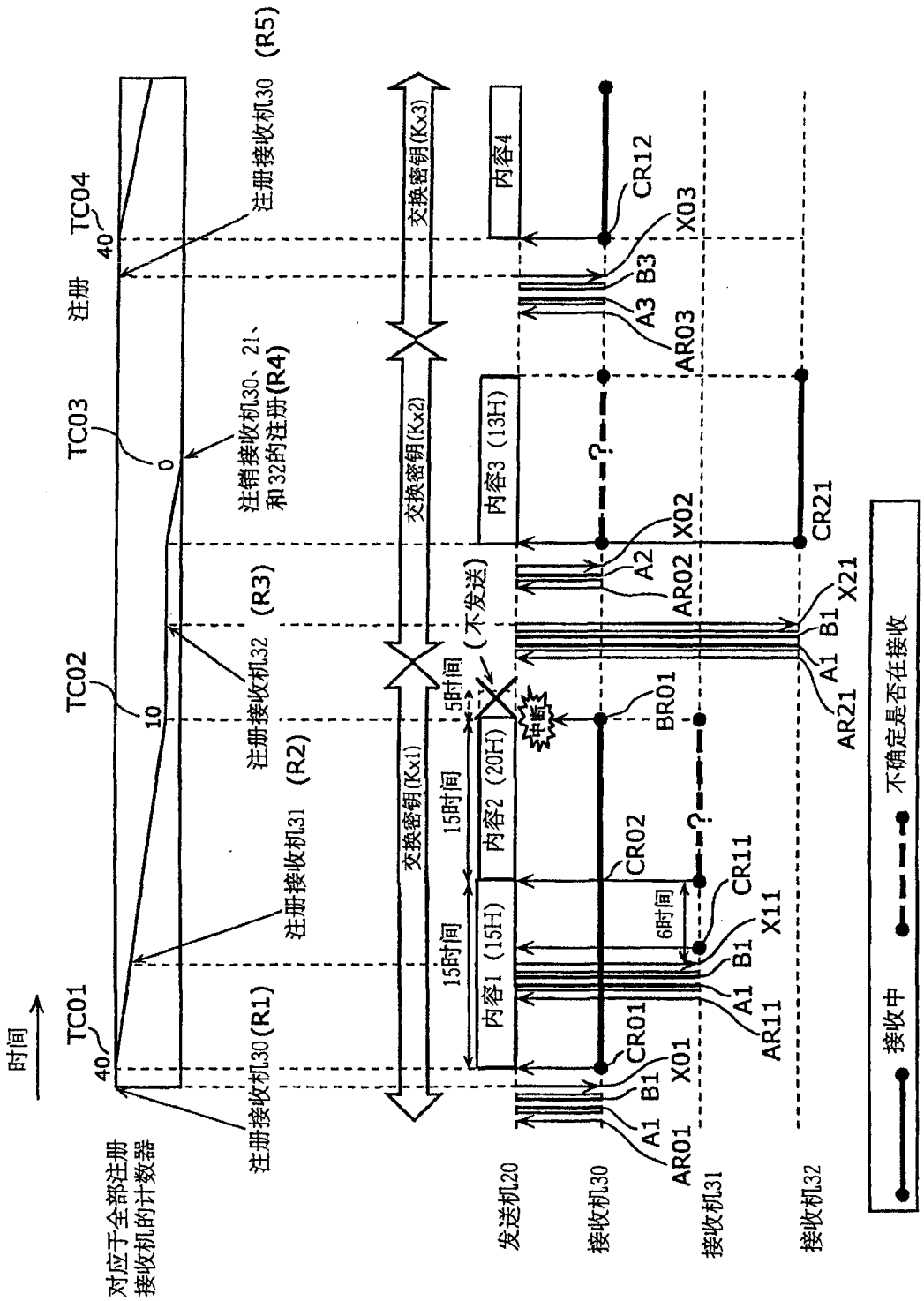

时间
TC01
TC02
TC03
TC04
注册
40
10
0
40
对应于全部注册接收机的计数器
注册接收机30(R1)
注册接收机31
注册接收机32 (R2)
注销接收机30、21、和32的注册(R4)
注册接收机30 (R5)
(R3)
交换密钥(Kx1)
交换密钥(Kx2)
交换密钥(Kx3)
15时间
15时间
5时间
(不发送)
中断
内容1 (15H)
内容2 (20H)
内容3 (13H)
内容4
6时间
发送机20
接收机30
接收机31
接收机32
CR01
CR02
CR11
CR12
CR21
X01
X02
X03
X11
X21
A1
B1
AR01
AR02
AR03
AR11
AR21
A2
A3
B3
BR01
接收中
不确定是否在接收

图 6