

[19] 中华人民共和国国家知识产权局



[12] 发明专利说明书

专利号 ZL 03101697.9

[51] Int. Cl.

H04L 9/32 (2006.01)

H04M 11/08 (2006.01)

H04M 9/00 (2006.01)

G06F 12/14 (2006.01)

[45] 授权公告日 2009 年 8 月 12 日

[11] 授权公告号 CN 100527667C

[22] 申请日 2003.1.15 [21] 申请号 03101697.9

[30] 优先权

[32] 2002.1.15 [33] JP [31] 2002-006564

[73] 专利权人 三洋电机株式会社

地址 日本国大阪府

共同专利权人 株式会社日立制作所

[72] 发明人 堀吉宏 平井达哉

[56] 参考文献

US6078338A 2000.6.20

CN1322422A 2001.11.14

JP2001-36523A 2001.2.9

CN1154551A 1997.7.16

审查员 王 侠

[74] 专利代理机构 中科专利商标代理有限责任公司

代理人 汪惠民

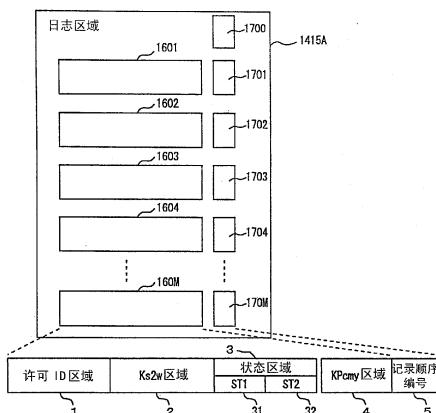
权利要求书 5 页 说明书 45 页 附图 19 页

[54] 发明名称

可以正确恢复加密数据的输入输出的存储装置

[57] 摘要

一种存储装置，可以正确恢复加密数据的输入输出。存储卡的日志区域(1415A)包括多个日志条目(1601 ~ 160M)和多个管理信息存储部(1700 ~ 170M)。多个日志条目(1601 ~ 160M)的每一个由许可 ID 区域(1)、Ks2w 区域(2)、状态区域(3)及 KPcmy 区域(4)构成。状态区域(3)由 ST1 区域(31)和 ST2 区域(32)构成，用于保存通信状态。许可 ID 区域(1)保存许可 ID。Ks2w 区域(2)保存会话密钥(Ks2w)。KPcmy 区域(4)保存存储卡的类公开加密密钥(KPcmy)。管理信息存储部(1700)保存与保存最新的通信历史信息的日志条目对应的最后记录顺序编号。



1. 一种存储装置，是按照一定顺序进行机密数据的输入输出并且保存所述机密数据的存储装置（40），其特征在于，包括：

与外部进行数据的输入输出的接口（1424）；

保存所述机密数据的数据存储部（1415B）；

保存有关所述机密数据的输入输出的历史信息的多个日志存储部（1601～160M）；以及

控制所述机密数据的输入输出的控制部（1420），

在所述多个日志存储部（1601～160M）中所保存的多个历史信息中的每一个包含识别机密数据的识别信息（1），

所述控制部（1420），在所述机密数据的输入输出处理开始后，相应地通过所述接口（1424）接收识别成为输入输出对象的机密数据的所述识别信息（1），当在所述多个日志存储部（1601～160M）中存在保存有包含所述接收到的所述识别信息（1）的历史信息的日志存储部时，选择该日志存储部，并在所选择的日志存储部中按照所述机密数据的输入输出的顺序的进程保存历史信息。

2. 根据权利要求1所述的存储装置，其特征在于，分别保存在所述多个日志存储部（1601～160M）中的各个历史信息，还包括：记录机密数据的输入输出的进行状态的状态信息（3），

所述控制部（1420），当在所述多个日志存储部（1601～160M）中不存在保存有包含所述接收到的所述识别信息（1）的历史信息的日志存储部时，从所述多个日志存储部（1601～160M）中，在保存有根据所述状态信息（3）已完成其它机密数据的输入的历史信息的日志存储部中选择1个，在所选择的日志存储部中按照所述机密数据的输入输出的顺序的进程保存历史信息。

3. 根据权利要求2所述的存储装置，其特征在于，所述控制部（1420），当不存在保存有根据所述状态信息（3）已完成其它机密数据的输入的历史信息的日志存储部时，从所述多个日志存储部（1601～160M）中，在保存有根据所述状态信息（3）而处于其它机密数据的输出等待状态的历

史信息的日志存储部中选择 1 个，在所选择的日志存储部中按照所述机密数据的输入输出的顺序的进程保存历史信息。

4. 根据权利要求 1 所述的存储装置，其特征在于，还包括：用于管理利用所述多个日志存储部（1601～160M）的每一个的顺序的日志管理存储部（1700～170M），

所述控制部（1420），当在所述多个日志存储部（1601～160M）中不存在保存有包含所述接收到的所述识别信息（1）的历史信息的日志存储部时，根据所述日志管理存储部（1700～170M）从所述多个日志存储部（1601～160M）中选择被判断是保存了最旧的历史信息的日志存储部，在所选择的日志存储部中按照所述机密数据的输入输出的顺序的进程保存历史信息。

5. 根据权利要求 1 所述的存储装置，其特征在于，还包括：用于管理利用所述多个日志存储部（1601～160M）的每一个的顺序的日志管理存储部（1700～170M），

所述多个历史信息中的每一个还包括：确定机密数据的输入输出的输入输出特定信息（2）；和记录机密数据的输入输出的进行状态的状态信息（3），

所述控制部（1420），当在所述多个日志存储部（1601～160M）中不存在保存有包含所述接收到的所述识别信息（1）的历史信息的日志存储部时，按照给定顺序从所述多个日志存储部（1601～160M）中选择保存有利用概率最低的历史信息的日志存储部，在所选择的日志存储部中按照所述机密数据的输入输出的顺序的进程保存历史信息。

6. 根据权利要求 5 所述的存储装置，其特征在于，所述给定顺序是，保存有具有表示没有出现机密数据消失的状态的状态信息（3）的日志存储部，根据所述日志管理存储部（1700～170M）保存了被判断为最旧的历史信息的日志存储部的顺序。

7. 根据权利要求 5 所述的存储装置，其特征在于，在接收从外部提供的所述机密数据的输入流程中，

所述控制部（1420），在通过所述接口（1424）从外部获取了成为输入对象的机密数据的识别信息（1）后，在所选择的日志存储部中保存所

获取的识别信息（1）和确定该输入流程的输入输出特定信息（2），并将保存在所选择的日志存储部中的状态信息（3）变更为输入等待，当通过所述接口（1424）从外部获取所述机密数据后，将保存在所选择的日志存储部中的状态信息（3）变更为输入完毕。

8. 根据权利要求 5 所述的存储装置，其特征在于，还包括：为了构筑安全进行所述机密数据的输入输出的加密通信路径，产生通过所述接口（1424）向外部输出的临时密钥的临时密钥生成部（1418），

所述控制部（1420），将在所述临时密钥生成部（1418）中产生的临时密钥作为所述输入输出的特定信息（2）保存在所选择的日志存储部中。

9. 根据权利要求 5 所述的存储装置，其特征在于，所述机密数据包括：识别该机密数据的识别信息（1），

所述控制部（1420），当保存在所选择的日志存储部中的历史信息中的第 1 识别信息（1）、与所输入的机密数据中的第 2 识别信息（1）一致时，将所述所输入的机密数据保存在所述数据存储部（1415B）中，当所述第 1 识别信息（1）与所述第 2 识别信息（1）不一致时，通过所述接口（1424）向外部输出出错消息。

10. 根据权利要求 1 所述的存储装置，其特征在于，所述控制部（1420），根据由所述接口（1424）输入的、来自外部的识别信息（1）和历史信息的输出要求，在所述多个日志存储部（1601～160M）中对保存有包含与所述来自外部的识别信息（1）一致的识别信息（1）的历史信息的日志存储部进行检索，当存在保存有包含与所述来自外部的识别信息（1）一致的识别信息（1）的历史信息的日志存储部时，将保存在该日志存储部中的历史信息的全部或者一部分，通过所述接口（1424）向外部输出。

11. 根据权利要求 10 所述的存储装置，其特征在于，还包括：根据通过所述接口（1424）从外部获取的密钥，对所述历史信息的全部或者一部分的署名值进行运算生成署名值的署名值运算部（1420），

所述控制部（1420），将所述历史信息的全部或者一部分和针对所述历史信息的署名值通过所述接口（1424）向外部输出。

12. 根据权利要求 1 所述的存储装置，其特征在于，还包括：用于管

理利用所述多个日志存储部（1601～160M）的每一个的顺序的日志管理存储部（1700～170M），

所述多个历史信息的每一个还包括：确定机密数据的输入输出的输入输出特定信息（2）；和记录机密数据的输入输出的进行状态的状态信息（3），

所述控制部（1420），当在所述多个日志存储部（1601～160M）中不存在保存有包含所接收到的所述识别信息（1）的历史信息的日志存储部时，按照给定顺序从所述多个日志存储部（1601～160M）中选择保存有利用概率最低的历史信息的日志存储部，在所选择的日志存储部中按照所述机密数据的输入输出的顺序的进程保存历史信息，

在向外部提供所述机密数据的输出流程中，

所述控制部（1420），当通过所述接口（1424）获取识别要输出的机密数据的识别信息（1）和确定所述机密数据的输出的输入输出特定信息（2）后，在所选择的日志存储部中保存所获取的识别信息（1）和输入输出特定信息（2），并将保存在所选择的日志存储部中的状态信息（3）变更为输出等待，当通过所述接口（1424）向外部输出所述机密数据后，将保存在所选择的日志存储部中的状态信息（3）变更为输入完毕。

13. 根据权利要求 12 所述的存储装置，其特征在于，在所述输出流程中，

所述控制部（1420），为构筑安全进行所述机密数据的输入输出的加密通信路径，通过所述接口（1424）从外部获取临时密钥，将所获取的临时密钥作为所述输入输出特定信息（2）保存在所选择的日志存储部中。

14. 根据权利要求 12 所述的存储装置，其特征在于，所述机密数据包括：识别该机密数据的识别信息（1），

在所述输出流程中，

所述控制部（1420），当保存在所选择的日志存储部中的历史信息中的第 1 识别信息（1）、与保存在所述数据存储部（1415B）中的机密数据中的第 2 识别信息（1）一致时，通过所述接口（1424）向外部输出保存在所述数据存储部（1415B）中的所述机密数据，当所述第 1 识别信息（1）与所述第 2 识别信息（1）不一致时，通过所述接口（1424）向外部发出

出错消息。

15. 根据权利要求 1 所述的存储装置，其特征在于，所述控制部（1420），经由所述接口（1424）从外部输入历史信息的获取后，在所述多个日志存储部（1601～160M）中检索保存有包含与来自所述外部的历史信息中的第 1 识别信息（1）一致的第 2 识别信息（1）的历史信息的日志存储部，当存在保存有包含所述第 2 识别信息（1）的历史信息的日志存储部时，根据保存在保存有包含所述第 2 识别信息（1）的历史信息的日志存储部中的历史信息和来自所述外部的历史信息，判断是否将与所述第 2 识别信息（1）对应的机密数据通过所述接口（1424）向外部输出。

可以正确恢复加密数据的输入输出的存储装置

技术领域

本发明涉及一种保存许可协议的存储装置，该许可协议用于对通过能对复制信息进行版权保护的数据投递系统所获取的加密数据进行解码或者播放，特别涉及在可多路存取的存储装置中可以对复制信息进行版权保护的存储装置。

背景技术

近年，随着因特网等数字信息通信网络等的进步，利用携带电话等个人终端，各用户可以容易存取网络信息。

在这样的数字信息通信网络中，通过数字信号传送信息。因此，例如在上述那样的信息通信网络中传送的音乐数据、映像数据即使由各个用户进行复制，基本上可以在不损失音质和图像质量的情况下进行数据的复制。

因此，在这样的数字信息通信网络上传递包含音乐数据和映像数据等具有作者的权利的内容时，如果不采取适当的版权保护措施，作者的权利很有可能会明显受到侵犯。

另一方面，如果以版权保护作为最优先考虑的因素，而使得不能通过急剧膨胀的数字信息通信网络进行内容数据的配送时，这对于通过复制品数据时可以征收一定版权费的作者而言，也是不利的。

但是，通过数字信息通信网络向公众配送音乐数据和映像数据等内容数据，这本身会受到作者的公众配送权的限制，因而需要构筑版权保护的足够措施。

这时，对于通过数字信息通信网络向公众配送的音乐数据和映像数据等内容数据，需要防止随意地对利用一次接收到的内容数据进行复制的情况。

因此，提出了一种由持有对内容数据进行加密后的加密内容数据的配送服务器，通过终端装置将加密内容数据配送到安装在携带电话等终端装置上的存储卡上的数据配送系统的方案。在该数据配送系统中，在要求配送加密内容数据时，向配送服务器传送预先在认证机构通过认证的存储卡的公开密钥及其证书，配送服务器在确认接收到认证后的证书后，向存储卡传送加密内容数据和用于对加密内容数据进行解密的许可协议。许可协议包含为将加密内容数据解密的解密密钥（以下称为「内容密码」）、用于识别许可协议的许可 ID、以及限制许可协议的利用的控制信息。配送服务器向存储卡传送许可协议时，配送服务器和存储卡分别生成会话密钥，通过在配送服务器和存储卡之间进行密钥的交换，构筑加密通信通道。

最终，配送服务器通过所构筑的加密通信通道，向存储卡发送许可协议。这时，存储卡在内部存储器中保存所接收到的加密内容数据和许可协议。

播放加密内容数据时，在具有专用电路的终端装置中装入保存了加密内容数据和许可协议的存储卡。专用电路是从存储卡中读出加密内容数据和内容密码、对加密内容数据进行解密进行播放、向外部输出的专用电路。在读出许可密码时，在存储卡和专用电路之间构筑加密通信通道，许可密码通过加密通信通道从存储卡传送给专用电路。

另外，存储卡具备与其它存储卡之间进行许可转移或者复制的功能。这时，和从配送服务器传送许可协议相同，根据发送端的存储卡和接收端的存储卡双方所具有的功能构筑加密通信通道，将许可协议从发送端的存储卡传送给接收端的存储卡。对许可协议究竟是移动还是复制，根据包含在许可协议中的控制信息来确定。

并且，存储卡还具备，当在收发过程中由于意外中断造成许可协议消失时可以恢复其处理，并且为防止重复发送许可协议而记录有关许可协议的输入输出的最近的历史信息，并根据需要输出的功能。作为发送端的配送服务器或者存储卡，从作为接收端的存储卡获取历史信息，根据该历史信息判断是否恢复许可协议的收发通信。历史信息包含许可 ID 和表示收发的状态信息。

这样，终端装置的用户可以利用通信网络，从配送服务器接收加密内容数据和许可协议，并保存到存储卡中，然后可以将保存在存储卡上的加密内容数据进行播放，或者转移到其它存储卡上，而且可以保护版权。

但是，在现有技术的存储卡中，只保存最近的历史信息，在中断之后，进行许可协议收发时，先前的中断的历史信息消失。这时，通过保存多个历史信息，可以方便用户。

另外，随着存储器件的存取速度的高速化，可以预见会出现同时并行进行多个许可协议的输入输出的要求。这时，至少需要能保存并行处理中的有关许可协议的输入输出的历史信息。

这样，为了能保存多个历史信息，而在许可协议保存之后，假定将该许可协议转移到其它存储卡中，对于同一许可 ID 保存具有不同状态的 2 个历史信息，所保存的历史信息出现矛盾。因此，存在重复发送许可协议的危险性，而造成不能确保安全的问题。

发明内容

因此，本发明的目的在于，提供一种既可以确保许可协议的唯一性、还可以使对中断后的许可协议的输入输出进行恢复而所需要的历史信息不会产生矛盾的存储装置。

依据本发明的存储装置，是按照一定顺序进行机密数据的输入输出并且保存机密数据的存储装置，包括与外部进行数据的输入输出的接口、保存机密数据的数据存储部、保存有关机密数据的输入输出的历史信息的多个日志存储部、控制机密数据的输入输出的控制部。在多个日志存储部中保存的多个历史信息的每一个包含识别机密数据的识别信息。控制部机密数据的输入输出处理开始后通过接口接收识别成为输入输出对象的机密数据的识别信息，当在多个日志存储部中保存包含接收到的识别信息的历史信息的日志存储部存在时，选择该日志存储部，在所选择的日志存储部中按照机密数据的输入输出的顺序的进程保存历史信息。

优选，在多个日志存储部中分别保存的历史信息的每一个进一步包括记录机密数据的输入输出的进行状态的状态信息，控制部，当在多个

日志存储部中保存包含所接收到的识别信息的历史信息的日志存储部不存在时，根据状态信息，从保存了其它机密数据的输入已经结束后的历史信息的日志存储部中选择 1 个，在所选择的日志存储部中按照机密数据的输入输出的顺序的进程保存历史信息。

优选，控制部，当根据状态信息保存了其它机密数据的输入已经结束后的历史信息的日志存储部不存在时，从在多个日志存储多个日志存储部中根据状态信息在保存了其它机密数据处于输出等待状态的历史信息的日志存储部中选择 1 个，在所选择的日志存储部中按照机密数据的输入输出的顺序的进程保存历史信息。

优选，进一步包括为管理利用多个日志存储部的每一个的顺序的日志管理存储部，控制部，当在多个日志存储部中保存包含接收到的识别信息的历史信息的日志存储部不存在时，根据日志管理存储部从多个日志存储部中选择保存了被认为是最旧的历史信息的日志存储部，在所选择的日志存储部中按照机密数据的输入输出的顺序的进程保存历史信息。

优选，进一步包括为管理利用多个日志存储部的每一个的顺序的日志管理存储部，多个历史信息的每一个进一步包括为特定机密数据的输入输出的输入输出特定信息、记录机密数据的输入输出的进行状态的状态信息，控制部，当在多个日志存储部中保存包含接收到的识别信息的历史信息的日志存储部不存在时，按照给定顺序从多个日志存储部中选择保存了利用概率最低的历史信息的日志存储部，在所选择的日志存储部中按照机密数据的输入输出的顺序的进程保存历史信息。

优选，给定顺序是保存具有表示没有出现机密数据消失的状态的状态信息的日志存储部，根据日志管理存储部保存了判断为最旧的历史信息的日志存储部的顺序。

优选，在接收从外部提供的机密数据的输入流程中，控制部，在通过接口从外部获取了成为输入对象的机密数据的识别信息后，在所选择的日志存储部中保存所获取的识别信息和特定该输入流程的输入输出特定信息，将保存在所选择的日志存储部中的状态信息变更为输入等待，当通过接口从外部获取机密数据后，将保存在所选择的日志存储部中的

状态信息变更为输入完毕。

优选，进一步包括为了构筑安全进行机密数据的输入输出的加密通信路径，产生通过接口向外部输出临时密钥的临时密钥生成部，在输入流程中，控制部，在临时密钥生成部中产生的临时密钥作为输入输出的特定信息保存在所选择的日志存储部中。

优选，机密数据包括识别该机密数据的识别信息，在输入流程中，控制部，当包含保存在所选择的日志存储部中的历史信息中的第1识别信息、与包含在所输入的机密数据中的第2识别信息一致时将所输入的机密数据保存在数据存储部中，当第1识别信息与第2识别信息不一致时通过接口向外部发出出错消息。

优选，控制部，根据通过接口输入的来自外部的识别信息和历史信息的输出要求，在多个日志存储部中检索保存了包含与来自外部的识别信息一致的识别信息的历史信息的日志存储部，当保存了包含与来自外部的识别信息一致的识别信息的历史信息的日志存储部存在时，将保存在该日志存储部中的历史信息的全部或者一部分通过接口向外部输出。

优选，进一步包括根据通过接口从外部获取的密钥对数据的署名值进行运算的署名值运算部，署名值运算部对历史信息的全部或者一部分运算署名值，产生署名值，控制部，将历史信息的全部或者一部分和针对历史信息的署名值通过接口向外部输出。

优选，进一步包括为管理利用多个日志存储部的每一个的顺序的日志管理存储部，多个历史信息的每一个进一步包括为特定机密数据的输入输出的输入输出特定信息、记录机密数据的输入输出的进行状态的状态信息，控制部，当在多个日志存储部中保存包含所接收到的识别信息的历史信息的日志存储部不存在时，按照给定顺序从多个日志存储部中选择保存了利用概率最低的历史信息的日志存储部，在所选择的日志存储部中按照机密数据的输入输出的顺序的进程保存历史信息。另外，在向外部提供机密数据的输出流程中，控制部，在通过接口获取识别要输出的机密数据的识别信息和特定机密数据的输出的输入输出特定信息后，在所选择的日志存储部中保存所获取的识别信息和输入输出特定信息，将保存在所选择的日志存储部中的状态信息变更为输出等待，当通

过接口向外部输出机密数据后，将保存在所选择的日志存储部中的状态信息变更为输入完毕。

优选，在输出流程中，控制部，为构筑安全进行机密数据的输入输出的加密通信路径，通过接口从外部获取临时密钥，将所获取的临时密钥作为输入输出特定信息保存在所选择的日志存储部中。

优选，机密数据包括识别该机密数据的识别信息，在输出流程中，控制部，当包含保存在所选择的日志存储部中的历史信息中的第1识别信息、与包含在保存在数据存储部中的机密数据中的第2识别信息一致时接口向外部输出保存在数据存储部中的历史信息，当第1识别信息与第2识别信息不一致时通过接口向外部发出出错消息。

优选，控制部，根据通过接口从外部输入历史信息的获取，在多个日志存储部中检索保存了包含了与在来自外部的历史信息中包含的第1识别信息一致的第2识别信息的历史信息的日志存储部，当保存了包含第2识别信息的历史信息的日志存储部存在时，根据保存在该日志存储部中的历史信息和来自外部的历史信息，判断是否将与第2识别信息对应的机密数据通过接口向外部输出。

附图说明

图1表示说明数字配送系统的概念的概略图。

图2表示在图1所示数字配送系统中在获取有加密内容数据的许可协议的存储卡之间转移许可协议的概念图。

图3表示在图1所示数字配送系统中进行通信的数据、信息等的特性图。

图4表示在图1所示数字配送系统中进行通信的数据、信息等的特性图。

图5表示在图1所示下载服务器的构成的概略方框图。

图6表示在图1所示终端装置的构成的概略方框图。

图7表示在图1所示存储卡的构成的概略方框图。

图8表示在图1所示日志区域的构成的概略方框图。

图9表示在图1所示数字配送系统中说明配送动作的第1流程图。

图 10 表示在图 1 所示数字配送系统中说明配送动作的第 2 流程图。

图 11 表示在图 9 所示第 S128 步的详细动作的流程图。

图 12 表示在存储卡中播放列表和许可协议区域的构成方框图。

图 13 表示在图 1 所示数字配送系统中说明再配送动作的第 1 流程图。

图 14 表示在图 1 所示数字配送系统中说明再配送动作的第 2 流程图。

图 15 表示在存储卡之间进行复制/转移动作的第 1 流程图。

图 16 表示在存储卡之间进行复制/转移动作的第 2 流程图。

图 17 表示在存储卡之间进行复制/转移的再动作的第 1 流程图。

图 18 表示在存储卡之间进行复制/转移的再动作的第 2 流程图。

图 19 表示在存储卡之间进行复制/转移的再动作的第 3 流程图。

图 20 表示在终端装置中加密内容数据的播放动作的流程图。

具体实施方案

以下参照附图详细说明本发明的实施方案。此外，图中相同或者相当的部分采用相同的符号，并省略其重复说明。

图 1 表示依据本发明的存储装置获取加密内容数据以及为对加密内容数据解密的许可协议的数据配送系统的整体构成的概念性概略图。

以下虽然是以通过移动电话网络，将音乐数据配送给装载在用户的终端装置、在此为携带电话上的存储卡 40 的数据配送系统的构成为例进行说明，但在以下的说明可以看到，本发明并不限于这种情况，也可以适用于配送其它出版物的内容数据，例如映像数据、动画数据等的情况下。另外，作为通信网络可以适用于一般数字通信网络中。作为存储装置，也并不限于存储卡，也可以适用于内藏有硬盘驱动器等控制器的存储装置中。

如图 1 所示，下载服务器 10，接收从装载了存储卡 40 的终端装置（携带电话等）20 的用户发出的配送请求。管理音乐数据的下载服务器 10 进行认证处理，判断装载在请求数据配送来访问的终端装置 20 上的存储卡 40 是否持有正当的认证数据，即是否是正规的存储卡。然后，下载服务器 10 对正当的存储卡按照为保护版权设置的给定加密方式对音乐数据（以下称为内容数据）进行加密，并将这样的加密内容数据和作为能播放加

密内容数据所必要的信息包含了对加密内容数据解密的许可密码向终端装置 20 配送。

在图 1 中，例如在终端装置 20 中，装载了可装卸的存储卡 40。存储卡 40 通过总线 BS 获取由终端装置 20 收到的加密内容数据以及许可协议，并保存。

进一步，例如用户通过连接在终端装置 20 上头戴耳机（图中未画出）播放这样的内容数据，可以收听。

此外，存储卡 40 从下载服务器 10 接收加密内容数据以及许可协议时，终端装置 20 所起的作用只不过将加密内容数据以及许可协议通过总线 BS 传送给存储卡 40，在此下载服务器 10 以及终端装置 20 一起作为内容提供装置 30。

装载在终端装置 20 上的存储卡 40，也可以将从下载服务器 10 接收到的加密内容数据以及许可协议传送给其它存储卡。

图 2 表示从存储卡 40 向存储卡 41 传送加密内容数据以及许可协议时的概念图。实际上，存储卡 40 装载在终端装置 20 上，通过总线 BS 与终端装置 20 之间存取数据，而存储卡 41 装载在终端装置 21 上，通过总线 BS 与终端装置 21 之间存取数据。然后，从存储卡 40 向存储卡 41 传送加密内容数据以及许可协议时，存储卡 40 通过总线 BS 将加密内容数据以及许可协议传送给终端装置 20，而终端装置 20 通过无线通信将加密内容数据以及许可协议传送给终端装置 21。然后，终端装置 21 将从终端装置 20 接收到的加密内容数据以及许可协议通过总线 BS 传送给存储卡 41。

但是，在存储卡 40 和存储卡 41 之间进行加密内容数据以及许可协议的传送时，由于终端装置 20、21 所起的作用只不过是将加密内容数据以及许可协议分别传送给存储卡 40、41，为此在图 2 中，终端装置 20、21 作为一个终端装置表示。

因此，从存储卡 40 向存储卡 41 传送加密内容数据以及许可协议时，存储卡 40 通过总线 BS 将加密内容数据以及许可协议传送给终端装置 20、21，而终端装置 20、21 将从存储卡 40 接收到的加密内容数据以及许可协议通过总线 BS 传送给存储卡 41。

另外，在同一终端装置中可以装载 2 个存储卡 40、41 时，同样可以采用图 2 进行说明。

在图 1 所示的构成中，为了在终端装置中可以播放加密后配送的内容数据，在系统上，第一需要在通信中配送许可协议的方式，第二需要对内容数据加密的方式，第三需要实现为防止许可协议被无限制复制的保护的构成。

在本发明的实施方案中，特别是在配送、复制/移动、以及播放的各处理中，充实了对许可协议的输出目标的认证和校对功能，对于非认证的存储装置（存储卡）以及终端装置（包括内容播放电路的携带电话等），通过防止内容数据的输出，防止许可密码的流出，进一步强化版权的保护，在此对该构成进行说明。

此外，在以下的说明中，将从下载服务器 10 向终端装置传送加密内容数据以及许可协议的处理称为「配送」

图 3 表示图 1 所示数据配送系统中，用于通信中的数据、信息的特性等。

首先对由下载服务器 10 配送的数据进行说明。Dc 表示音乐数据等的内容数据。内容数据 Dc 被实施了可以采用内容密钥 Kc 进行解密的加密处理。实施了可以采用内容密钥 Kc 进行解密的加密处理的内容数据 E(Kc、Dc)采用该形式从下载服务器 10 配送给终端装置 20 的用户。

在以下的说明中，标记“E(X,Y)”表示通过密钥 X 对数据 Y 进行加密。

并且，由下载服务器 10 配送加密内容数据的同时，还配送作为有关内容数据的明文信息的附加信息 Di。此外，附加信息 Di，包含识别内容数据 Dc 的数据 ID(DID)。

另外，作为许可协议，包括内容密钥 Kc、许可 ID(LID)、数据 ID(DID)、控制信息 AC。

数据 ID，是为识别内容数据 Dc 以及内容密钥 Kc 的编码，许可 ID 管理由下载服务器 10 配送的许可协议，为识别每个许可协议的编码。控制信息 AC 是将存储装置（存储卡）上的许可协议或者内容密钥向外部输出时的控制信息，包括可播放次数（为播放而输出许可密钥的数量）、

有关许可协议的移动、复制的限制信息。

以后，将许可 ID、数据 ID、内容密钥 K_c 、控制信息 AC 一起统称为许可 LIC。

另外，在以后，为了简化，控制信息 AC 只包括限制播放次数的控制信息的播放次数（0：不能播放，1~254：可播放次数，255：无限制播放）、限制许可协议的移动以及复制的移动、复制标志位（0：禁止移动复制，1：只可移动，2：可以移动复制）两项。

图 4 表示在图 1 所示数据配送系统中所使用的用于认证的数据、信息等的特性。

在终端装置 20、21 内的内容播放电路以及存储卡 40、41 中设置了固有公开加密密钥 K_{Pcxy} 。在此，公开加密密钥 K_{Pcxy} 按照机器的种类分配， x 是为识别内容播放电路和存储装置的识别子，当机器是内容播放电路等的播放装置时 $x=p$ ，当机器是存储卡等存储装置时 $x=m$ 。 y 是为识别机器种类的识别子。公开加密密钥 K_{Pcxy} 由密码解密密钥 K_{cxy} 可以被解密。这些公开加密密钥 K_{Pcxy} 和密码解密密钥 K_{cxy} ，根据内容播放电路以及存储卡的种类而具有不同的值。这些公开加密密钥以及密码解密密钥统称为类密钥，将这些公开加密密钥称为类公开加密密钥，密码解密密钥称为类密码解密密钥，类密钥共同的单位称为类。类根据制造厂商、产品的种类、制造时的批量号而不同。

另外，作为存储卡以及内容播放电路的类证书，设置 C_{xy} 。这些类证书根据内容播放电路以及存储卡的种类而具有不同的信息。

内容播放电路以及存储卡的类证书 C_{xy} 在出厂时以 $K_{Pcxy}/1cxy//E(Ka,H(K_{Pcxy}/1cxy))$ 的形式保存在内容播放电路以及存储卡中。在此， $1cxy$ 是针对每个类的机器以及类公开加密密钥 K_{Pcxy} 的信息数据。另外， $H(X)$ 表示 X 的散列值， $X//Y$ 表示 X 和 Y 之间的连接。 $E(Ka, H(K_{Pcxy}/1cxy))$ 是 $K_{Pcxy}/1cxy$ 的署名数据。

K_{Pa} 对于整个数据配送系统是共同的公开认证密钥，用于对在认证局由主密钥 Ka 对类公开加密密钥 K_{Pcxy} 和类信息 $1cxy$ 进行加密后的署名数据进行解密。主密钥 Ka 是在认证局中制作类证书的署名数据所使用的密码加密密钥。

另外，作为管理存储卡 40、41 内的数据处理的密钥，包括根据每个存储卡 40、41 的存储装置设定的公开加密密钥 KPomz、对由公开加密密钥 KPomz 加密后的数据可以解密的固有的密码解密密钥 Komz。这些根据每个存储卡设置的公开加密密钥和密码解密密钥统称为个别密钥，公开加密密钥 KPomz 称为个别公开加密密钥，密码解密密钥 Komz 称为个别密码解密密钥。z 是为识别存储装置的识别子。

每次进行许可协议的配送、移动、复制以及读出时，需要用到在下载服务器 10、终端装置 20、21 以及存储卡 40、41 中产生的共同密钥 Ks1w、Ks2w。

在此，共同密钥 Ks1w、Ks2w 是针对每个在下载服务器与内容播放电路或者存储卡之间进行通信的单位或者存取的单位的「会话」产生的固有共同密钥，以后这些共同密钥 Ks1w、Ks2w 也称为「会话密钥」。

这些会话密钥 Ks1w、Ks2w，针对每个处理具有固有的值，由下载服务器、内容播放电路、存储装置（存储卡）进行管理。具体讲，会话密钥 Ks1w 在数据发送侧按每个处理产生，而会话密钥 Ks2w 在数据接收侧按每个处理产生。在各处理中，接收这些会话密钥，接收在其它机器上产生的会话密钥，由该会话密钥进行加密后进行许可密钥等的传送，这样可以在处理中提高防范力度。

图 5 表示图 1 所示的下载服务器 10 的构成的概略方框图。

下载服务器 10 包括为保存按照给定方式加密内容数据后的数据和数据 ID 等配送信息的信息数据库 304、根据终端装置的各用户保存开始存取内容数据后的缴费信息的缴费数据库 302、保存在信息数据库 304 中的内容数据的菜单的菜单数据库 307、在每次许可协议的配送时产生、并且保存有关特定许可协议的许可 ID 等的配送的日志记录的配送记录数据库 308、通过总线 BS1 接收来自信息数据库 304、缴费数据库 302、菜单数据库 307、配送记录数据库 308 的数据、进行给定处理的数据处理部 310、通过通信网络在配送载体和数据处理部 310 之间进行数据收发的通信装置 350。

数据处理部 310 包括根据总线 BS1 上的数据控制数据处理部 310 的动作的配送控制部 315、由配送控制部 315 控制、在配送处理时产生会话

密钥 Ks1w 的会话密钥产生部 316、为保存对从存储卡传送来的用于认证的类证书 $C_{xy} = K_{Pcxy} // 1c_{xy} // E(ka, H(K_{Pcxy} // 1c_{xy}))$ 进行解密的公开解密密钥 KPa 的认证密钥保存部 313、通过通信装置 350 接收从存储卡传送来的用于认证的类证书 Cxy、由来自认证密钥保存部 313 的认证密钥 KPa 进行解密处理的解密处理部 312、采用由解密处理部 312 获得的类公开加密密钥 K_{Pcxy} 对由会话密钥产生部 316 产生的会话密钥 Ks1w 进行加密、向总线 BS1 输出的加密处理部 318、通过总线 BS1 接收由会话密钥 Ks1w 加密后发送的数据、并由会话密钥 Ks1w 进行解密处理的解密处理部 320。

数据处理部 310 进一步包括对由配送控制部 315 给出的内容密钥 Kc 以及控制信息 AC 采用由解密处理部 320 获取的存储卡的个别公开加密密钥 K_{Pomz} 加密的加密处理部 326、对加密处理部 326 的输出采用解密处理部 320 给出的会话密钥 Ks2w 进一步加密后向总线 BS1 输出的加密处理部 328。

下载服务器 10 的配送处理的动作，在后面将用流程图详细说明。

图 6 表示图 1 所示的包括内容播放电路的终端装置 20 的构成的概略方框图。

终端装置 20 包括接收无线发送的信号的天线 1102、接收来自天线 1102 的信号并转换成基带信号、或者将来自终端装置 20 的数据调制后发送给天线 1102 的收发部 1104、在终端装置 20 的各部之间进行数据收发的总线 BS2、通过总线 BS2 控制终端装置 20 的动作的控制器 1106、将来自外部的指令传送给终端装置 20 的操作面板 1108、将控制器 1106 等输出的信息表示成用户可视的信息的显示面板 1110。

终端装置 20 进一步包括保存来自下载服务器 10 的内容数据（音乐数据）并且进行解密处理的可装卸的存储卡 40、控制存储卡 40 与总线 BS2 之间的数据收发的存储卡接口 1200、内容播放电路 1550。

内容播放电路 1550 包括保存类证书 $C_{p3} = K_{Pcp3} // 1cp3 // E(ka, H(K_{Pcp3} // 1cp3))$ 的证书保存部 1500。在此假设终端装置 20 的类 y 为 y=3。

终端装置 20 进一步包括保存类的固有解密密钥的 Kcp3 的 Kcp 保存部 1502、从总线 BS2 接收到的数据采用解密密钥 Kcp3 进行解密、获得由存储卡 40 产生的会话密钥 Ks1w 的解密处理部 1504。

终端装置 20 进一步包括在对保存在存储卡 40 中的内容数据进行播放的播放处理中通过随机数产生与存储卡 40 之间在总线 BS2 上收发的数据进行加密的会话密钥 Ks2w 的会话密钥产生部 1508、在加密内容数据的播放处理中接收来自存储卡 40 的内容密钥 Kc 以及播放控制信息时、对由会话密钥产生部 1508 产生的会话密钥 Ks2w 采用由解密处理部 1504 获得的存储卡 40 的会话密钥 Ks1w 进行加密后输出到总线 BS2 上的加密处理部 1506。

终端装置 20 进一步包括由会话密钥 Ks2w 解密总线 BS2 上的数据后输出内容密钥 Kc 的解密处理部 1510、通过总线 BS2 接收加密内容数据 E(Kc, Dc)、由来自解密处理部 1510 的内容密钥 Kc 对加密内容数据 E(Kc, Dc) 进行解密后将内容数据 Dc 输出给音乐播放部 1518 的解密处理部 1516。

终端装置 20 进一步包括接收来自解密处理部 1516 的输出、播放内容数据 Dc 的音乐播放部 1518、将音乐播放部 1518 的输出从数字信号变换成模拟信号的 DA 转换部 1519、将 DA 转换部 1519 的输出向头戴耳机等外部输出装置（图中未画出）输出的端子 1530。

终端装置 20 的各构成部分的各处理动作，将在后面采用流程图进行详细说明。

图 7 表示图 1 所示的存储卡 40 的构成的概略方框图。

如已经说明的那样，作为存储卡 40 的类公开加密密钥以及类密码解密密钥分别设置 KPcmy 以及 Kcm，存储卡的类证书设置 $C_{xy} = KP_{cxy} // 1cxy // E(ka, H(KP_{cxy} // 1cxy))$ ，在存储卡 40 中，类识别子由 $y=1$ 表示。另外，识别存储卡的个别识别子 z 由 $z=2$ 表示。

因此，存储卡 40 包括类证书 $Cp_3 = KP_{cp3} // 1cp3 // E(ka, H(KP_{cp3} // 1cp3))$ 的证书保存部 1400、保存针对每个存储卡设置的固有解密密钥的个别密码解密密钥 Kom2 的 Kom 保存部 1402、保存类密码解密密钥 Kcm1 的 Kcm 保存部 1421、保存可以用个别密码解密密钥 Kom2 解密的公开加密密钥 KPom2 的 KPom 保存部 1416。

这样，通过存储卡那样的存储装置的解密密钥，如以下说明的那样，可以按存储卡单位管理配送的内容数据和加密许可协议密钥。

存储卡 40 进一步包括通过端子 1436 与存储卡接口 1200 之间收发数据的接口 1424、与接口 1424 之间传送数据的总线 BS3、对从接口 1424 输出到总线 BS3 上的数据采用来自 Kcm 保存部 1421 的类密码解密密钥 Kcm1 的解密处理部 1422、接收来自 KPa 保存部 1414 的认证密钥 KPa、利用认证密钥 KPa 对其它机器的类证书的署名数据 $E(ka, H(KPcxy//1cxy))$ 进行解密处理后将解密结果输出给控制器 1420 的解密处理部 1408、通过切换开关 1442 选择的从其它机器传来的会话密钥将由切换开关 1446 选择的数据加密并输出到总线 BS3 上的加密处理部 1406。

存储卡 40 进一步包括在配送、复制/移动以及播放的各处理中产生会话密钥 Ks1w、Ks2w 的会话密钥产生部 1418，会话密钥产生部 1418 输出的会话密钥 Ks1w 由其它机器的类公开加密密钥 KPcpz 或者 KPcmz 加密后输出到总线 BS3 上的加密处理部 1410、通过总线 BS3 接收加密后的数据由会话密钥产生部 1418 或者的会话密钥 Ks1w、Ks2w 进行解密的解密处理部 1412、在移动/复制处理中成为许可协议发送端时从存储器 1415 读出的内容密钥 Kc 利用其它存储卡的个别公开加密密钥 KPomz ($z \neq 2$) 进行加密的加密处理部 1417。

存储卡 40 进一步包括将总线 BS3 上的由个别公开加密密钥 KPom2 加密的数据利用存储卡 40 的个别密码解密密钥 Kom2 进行解密的解密处理部 1404、对在下载服务器 10 和其它存储卡之间的通信过程中保存历史记录的日志、加密内容数据 $E(Kc, Dc)$ 、播放加密内容数据 $E(Kc, Dc)$ 的许可协议 (Kc, Ac 、许可 ID、数据 ID)、附加信息 Di、加密内容数据的播放列表、许可协议进行管理的许可协议管理文件通过总线 BS3 被接收到后进行保存的存储器 1415。

存储器 1415 由日志区域 1415A、许可协议区域 1415B、数据区域 1415C 构成。日志区域 1415A 是为记录日志的区域。日志区域 1415A 将在后面详细说明。

许可协议区域 1415B 是为记录许可协议的区域。许可协议区域 1415B 为记录许可协议 (内容密钥 Kc、控制信息 AC、许可 ID、数据 ID) 和有效标志位而以称为条目的许可协议专用的记录单位保存许可协议和有效标志位。对许可协议存器时，保存了许可协议、或者要记录许可协议的

条目由保存位置进行指定。

在本发明的实施方案中，从发送端的存储装置（存储卡）向接收目标的存储装置进行许可协议的移动/复制时，使用表示保存在发送端的存储装置中的有效、无效的有效标志位。该有效标志位为有效时，表示可以从存储卡向外部输出许可协议，有效标志位为无效时，表示禁止从存储卡向外部输出许可协议。

数据区域 1415C 是为记录加密内容数据 E(Kc, Dc)、加密内容数据 E(Kc, Dc) 的附加信息 Di、针对每个加密内容数据记录为管理许可协议所必要的信息的许可协议管理文件、记录为存取保存在存储卡上的加密内容数据 E(Kc, Dc) 和许可协议的基本信息的播放列表、以及管理许可协议区域 1415B 的条目的条目信息的区域。然后，数据区域 1415C 可以从外部直接存取。许可协议管理文件以及播放列表将在后面详细说明。

存储卡 40 进一步包括通过总线 BS3 与外部之间进行数据接收、与总线 BS3 之间传递控制信息 AC、控制存储卡 40 的动作的控制器 1420。

此外，除了数据区域 1415C 之外所有的构成均在耐热固模块区域中构成。

图 8 表示包含在存储卡 40 中的存储器 1415 的日志区域 1415A 的详细图。在图 8 中，日志区域 1415A 包括保存历史信息的 M 个日志条目 1601～160M（M 为自然数）、M+1 个的管理信息存储部 1700～170M。日志条目 1601～160M 是为保存一条存储卡 40 与下载服务器 10 或者其它存储卡之间收发许可协议时的通信历史信息的存储部。管理信息存储部 1701～170M 分别与日志条目 1601～160M 一一对应，是保存表示日志条目的顺序的记录顺序编号的存储部。管理信息存储部 1700 是对保存最近更新的历史信息的条目进行编号的记录顺序编号（以下称为「最终记录顺序编号」）的存储部。记录顺序编号是 N 比特的自然数，它是在所利用的日志条目上依次一条一条增加编号的管理编号。记录顺序编号在 2 的 N 次幂的剩余数系统中运算。

例如，日志条目 1602 的历史信息更新时，赋予记录顺序编号「101」，在与日志条目 1602 对应的管理信息存储部 1702 和保存最终记录顺序编号的管理信息存储部 1700 中保存「101」。然后，当日志条目 1604 的历

史信息更新时，访问管理信息存储部 1700 获得最终记录顺序编号「101」之后，在记录顺序编号「101」上加 1 后的记录顺序编号「102」赋予给日志条目 1604 的历史信息，在与日志条目 1604 对应的管理信息存储部 1704 和保存最终记录顺序编号的管理信息存储部 1700 中保存「102」。最终，通过管理信息存储部 1700 中保存的最终记录循序编号、与各日志条目的历史信息的更新时赋予的、保存在与各个日志条目分别对应的管理信息存储部 1700~170M 中的记录顺序编号进行比较可以确定保存最早历史信息的日志条目。

日志条目 1601~160M 的每一个，由许可 ID 区域 1、Ks2w 区域 2、状态区域 3、KPcmy 区域 4 构成。许可 ID 区域 1 保存在移动/复制处理中成为传送对象的许可协议的许可 ID。Ks2w 区域 2 保存在传送许可协议的通信中在接收目标的存储卡中产生的会话密钥 Ks2w。状态区域 3 由 ST1 区域 31 和 ST1 区域 32 构成，在 ST1 区域 31 中保存「接收等待」、「接受完毕」、「发送等待」以及「发送完毕」中的任一项，在 ST1 区域 32 中，保存「无数据」、「有数据」以及「移动完毕」中的任一项。也就是说，ST1 区域 31 表示收发许可协议的通信的最终通信状态，ST1 区域 32 表示实际上是否发送或者接收到许可协议。

KPcmy 区域 4 保存在存储卡之间的许可协议的复制/移动处理中发送端的类公开加密密钥 KPcmy。

日志条目 1601~160M 为有限个历史信息，历史信息的个数 M 与在管理信息存储部 1700~170M 的每一个中保存的记录顺序编号的位数之间存在 $2N-1 \gg M$ 的关系，由此确定 M 以及 N。

以下说明在图 1 所示的数据配送系统中各处理的动作。

[配送]

首先说明在图 1 所示的数据配送系统中，从下载服务器 10 向终端装置 20 的存储卡 40 配送为将加密内容数据解密的许可协议的动作。

图 9 和图 10 表示在图 1 所示的数据配送系统中在许可协议下载时向装载在终端装置 20 上的存储卡 40 配送许可协议的处理的第 1 以及第 2 流程图。

在图 9 中进行处理以前，是以终端装置 20 的用户通过电话网络与下载服务器 10 连接、获取希望下载的内容的数据 ID、向下载服务器 10 发出了配送请求的事件为前提，并且对存储卡 40 获取条目管理信息确认了许可协议区域 1415B 内的空余区域的事件为前提。

在图 9 中，终端装置 20 的用户通过操作面板 1108 发出接收许可协议的接收处理的指示。

发出接收许可协议的接收处理的指示后，控制器 1106 通过总线 BS2 以及存储卡接口 1200 向存储卡 40 输出类证书的输出请求（第 S100 步）。存储卡 40 的控制器 1420 通过端子 1426、接口 1424 以及总线 BS3 接收类证书的输出请求（第 S1020 步）。然后，控制器 1420 通过总线 BS3 从证书保存部 1400 读出类证书 Cm1，通过总线 BS2、接口 1424 以及端子 1426 输出类证书（第 S104 步）。

终端装置 20 的控制器 1106，向下载服务器 10 发送来自存储卡 30 的类证书 Cm1，下载服务器 10 接收来自终端装置 20 的类证书 Cm1（第 S106 步）。然后，解密处理部 312 利用认证密钥 KPa 对存储卡 40 输出的类证书 $Cm1 = KPcm1//1cm1// E(ka, H(KPcm1//1cm1))$ 的署名数据 $E(ka, (KPcm1 //1cm1))$ 进行解密，将解密后的数据的散列值 $H(KPcm1//1cm1)$ 向配送控制部 315 输出。配送控制部 315 对类证书 Cm1 的 $KPcm1//1cm1$ 计算散列值，通过确认所计算的散列值是否与解密处理部 312 接收到的散列值 $H(KPcm1//1cm1)$ 一致，进行类证书 Cm1 的正当性的验证（第 S108 步）。当 2 个散列值一致时，判定类证书 Cm1 是正当的。

配送控制部 315，在判定验证结果为正当时，转移到下一步处理（第 S110 步）。如果不是正当的类证书 Cm1，配送控制部 315 不受理类公开加密密钥 KPcm1，结束配送处理（第 S166 步）。

当认证结果确认是来自装载了具有正当类证书的存储卡的终端装置的访问时，在下载服务器 10 中，配送控制器 315 受理包含在存储卡 40 的类证书 Cm1 中的类公开加密密钥 KPcm1（第 S110 步），产生为识别有配送请求的许可协议的许可 ID（第 S112 步）。

然后，会话密钥产生部 316，生成用于配送的会话密钥 Ks1a（第 S114 步）。会话密钥 Ks1a 在加密处理部 318 由存储卡 40 的类公开加密密钥

KPcm1 加密（第 S116 步）。

配送控制部 315 将许可 ID 以及加密后的会话密钥 Ks1a，作为许可 ID//E(KPcm1, Ks1a)，通过总线 BS1 以及通信装置 350 向终端装置 20 发送。

终端装置 20 的控制器 1106 接收到许可 ID//E(KPcm1, Ks1a)后，将许可 ID//E(KPcm1, Ks1a)输入给存储卡 40（第 S118 步）。控制器 1420 通过端子 1426 以及接口 1424 受理存储卡 40 的许可 ID//E(KPcm1, Ks1a)（第 S120 步）。然后，控制器 1420 通过总线 BS3 将加密数据 E(KPcm1, Ks1a)输出给解密处理部 1422，解密处理部 1422 利用保存在 Kcm 保存部 1421 中的存储卡 40 固有的类密码解密密钥 Kcm1 对加密数据 E(KPcm1, Ks1a)进行解密，受理会话密钥 Ks1a（第 S122 步）。

这样，终端装置 20 的控制器 1106 通过存储卡接口 1200 向存储卡 40 发送会话密钥的输出请求（第 S124 步）。存储卡 40 的控制器 1420 通过端子 1426 以及接口 1424 受理会话密钥的输出请求，控制使会话密钥产生部 1418 产生会话密钥。然后，会话密钥产生部 1418 产生会话密钥 Ks2a（第 S126 步），控制器 1420 按照给定的顺序从日志区域 1415A 的多个日志条目 1601~160M 中选用保存为记录从下载服务器 10 接收许可协议的通信的历史信息的日志条目 160i ($1 \leq i \leq M$)（第 S128 步）。

在此，利用图 11 说明选用保存为记录从下载服务器 10 接收许可协议的通信的历史信息的日志条目的方法。动作开始后，控制器 1420 检索在日志条目 1601~160M 中是否存在包含与要从下载服务器 10 接收的许可 ID(LID)相同的许可 ID 的历史信息（第 S1281 步）。然后，当检索到保存包含与要从下载服务器 10 接收的许可 ID(LID)相同的许可 ID 的历史信息的日志条目时，转移到第 S1285 步。另一方面，在第 S1281 步中，如果没有检索到包含保存与要从下载服务器 10 接收的许可 ID(LID)相同的许可 ID 的历史信息的日志条目时，检索在状态区域 3 的 ST1 区域 31 中保存记录了「接收完毕」的历史信息的日志条目（第 S1282 步），当检索到在状态区域 3 的 ST1 区域 31 中保存记录了「接收完毕」的历史信息的日志条目时转移到第 S1285 步。另一方面，在第 S1282 步中，如果没有检索到在状态区域 3 的 ST1 区域 31 中保存记录了「接收完毕」的历史信

息的日志条目时，检索在状态区域 3 的 ST1 区域 31 中保存记录了「发送等待」的历史信息的日志条目（第 S1283 步），如果检索到在状态区域 3 的 ST1 区域 31 中保存记录了「发送等待」的历史信息的日志条目时转移到第 S1285 步。另一方面，如果没有检索到在状态区域 3 的 ST1 区域 31 中保存记录了「发送等待」的历史信息的日志条目时，选定记录了使管理信息存储部 1700 所保存的最终记录顺序编号和保存在各个 M 个的管理信息存储部 1700~170M 的每一个中的记录顺序编号之差成为最大的记录顺序编号的管理信息存储部，检测出与所选定的管理信息存储部对应的日志条目，也就是说，检测出记录了最旧历史信息的日志条目（第 S1284 步）。

然后，控制器 1420 选用在第 S1281~S1284 步中的任一步检测到的日志条目 160i ($1 \leq i \leq M$)（第 S1285 步），将保存在管理信息存储部 1700 中的最终记录顺序编号加 1（第 S1286 步）。然后，控制器 1420 以保存在与选用的日志条目 160i 对应的管理信息存储部 170i 中的记录顺序号变更成保存在管理信息存储部 1700 中的最终记录顺序编号（第 S1287 步），结束选择日志条目的动作。

如上所述，在图 11 所示的选择方法中，按照在保存在日志条目 1601~160M 中的历史信息中包含成为通信对象的许可协议的许可 ID 的日志条目、所保存的历史信息 ST1 区域 31 为「接受完毕」的日志条目、所保存的历史信息 ST1 区域 31 为「发送等待」的日志条目、更新保存了最旧的历史信息的日志条目、的顺序从日志条目 1601~160M 中选择 1 个日志条目 160i。

第 1 条件的在历史信息中包含成为通信对象的许可协议的许可 ID 的日志条目是为了对 1 个许可协议不记录重复的历史信息而设定的选择基准。第 2 条件的所保存的历史信息 ST1 区域 31 为「接受完毕」的日志条目，以及第 3 条件的所保存的历史信息 ST1 区域 31 为「发送等待」的日志条目是为了选择即使不进行许可协议的再发送处理可以在良好状态下更新而不存在问题的条目而设定的基准。也就是说，「接受完毕」表示在接收端的存储卡中许可协议已经保存在存储器 1415 的许可协议区域 1415B 中，「发送等待」表示在发送端的存储卡中处于没有输出许可协议

的状态（许可协议保存在存储器 1415 的许可协议区域 1415B 中的状态）。

第 4 条件的更新保存了最旧的历史信息的日志条目是为了选择被认为再次发送的概率最低的条目而设定的基准。

再次返回到图 9 中，在第 S128 步之后，控制器 1420 将接收到的许可 ID 以及所生成的会话密钥 Ks2a 分别保存在在第 S128 步中所选用的日志条目 160i 的许可 ID 区域 1 以及 Ks1w 区域 2 中，将状态区域 3 的 ST1 区域 31 变更成「接收等待」（第 S130 步）。

加密处理部 1406，利用通过切换开关 1442 的触点 Pa 由解密处理部 1433 给出的会话密钥 Ks1a，将通过对切换开关 1446 的触点切换后输出的会话密钥 Ks2a、以及个别公开加密密钥 KPom2 一起作为一个数据列进行加密，之后将加密数据 $E(Ks1a, Ks2a/KPom2)$ 输出到总线 BS3 上（第 S132 步）。将在输出到总线 BS3 上的加密数据 $E(Ks1a, Ks2a/KPom2)$ 上增加了许可 ID(LID)后的数据 LID// $E(Ks1a, Ks2a/KPom2)$ 通过总线 BS3、接口 1424 以及端子 1426 输出给终端装置 20（第 S134 步），终端装置 20 将数据 LID// $E(Ks1a, Ks2a/KPom2)$ 发送给下载服务器 10。

下载服务器 10 接收数据 LID// $E(Ks1a, Ks2a/KPom2)$ （第 S136 步），解密处理部 320 利用会话密钥 Ks1a 对加密数据 $E(Ks1a, Ks2a/KPom2)$ 进行加密，受理在存储卡 40 生成的会话密钥 Ks2a、以及存储卡 40 的个别公开加密密钥 KPom2（第 S138 步）。

配送控制部 315 产生控制信息 AC（第 S140 步），从信息数据库 304 中获取数据 ID 以及内容密钥 Kc（第 S142 步）。

配送控制部 315 将许可 ID、数据 ID、内容密钥 Kc 以及控制信息 AC，即许可 LIC 输出给加密处理部 326。加密处理部 326，利用由解密处理部 320 获得的存储卡 40 的个别公开加密密钥 KPom2 对许可 LIC 进行加密，产生加密数据 $E(KPom2, LIC)$ （第 S144 步）。然后，加密处理部 328 对来自加密处理部 326 的加密数据 $E(KPom2, LIC)$ 利用由解密处理部 320 解密的会话密钥 Ks2a 进行加密，产生加密数据 $E(Ks2a, E(KPom2, LIC))$ （第 S146 步）。

在图 10 中，配送控制部 315 通过总线 BS1 以及通信装置 350 将加密数据 $E(Ks2a, E(KPom2, LIC))$ 传送给终端装置 20。

终端装置 20 的控制器 1106，在接收到传送来的加密数据 E(Ks2a, E(KPom2, LIC))后，通过总线 BS2 以及存储卡接口 1200 输出给存储卡 40 (第 S148 步)。然后，存储卡 40 受理加密数据 E(Ks2a, E(KPom2, LIC)) (第 S150 步)，解密处理部 1412，通过端子 1426 以及接口 1424，将输出到总线 BS3 上的加密数据 E(Ks2a, E(KPom2, LIC))利用会话密钥 Ks2a 进行解密，获得加密数据 E(KPom2, LIC)(第 S152 步)。然后，将加密数据 E(KPom2, LIC)输入到解密处理部 1404，解密处理部 1404 利用保存在 Kom 保存部 1402 中的个别公开密码解密密钥 Kom2 对加密数据 E(KPom2, LIC)进行解密后获得许可 LIC (第 S154 步)。

这样，从终端装置 20 输出许可协议的存储位置 (第 S156 步)，存储卡 40 的控制器 1420，通过端子 1426、接口 1424 以及总线 BS3 获得许可协议的存储位置 (第 S158 步)。然后，控制器 1402 判定包含在所获取的许可 LIC 中的许可 ID 与在第 S130 步中保存在日志条目 160i 中的许可 ID 是否一致 (第 S160 步)，如果不一致，控制器 1420 通过总线 BS3、接口 1424 以及端子 1426 向终端装置 20 输出出错消息 (第 S162 步)。然后，终端装置 20 通过存储卡接口 1200 接收出错消息并传送给下载服务器 10，下载服务器 10 获取出错消息 (第 S164 步)。然后，拒绝写入，结束配送处理 (第 S166 步)。

另一方面，在第 S1630 步中，如果 2 个许可 ID 一致，控制器 1420 将许可 LIC 保存在由许可协议区域 1415B 的许可协议存储位置所指定的条目中 (第 S168 步)，将记录接收许可协议的通信的日志条目 160i 的 ST1 区域 31 变更为「接受完毕」(第 S170 步)，正常结束配送处理 (第 S172 步)。

此外，虽然没有在上面说明，在将许可协议保存在许可协议区域 1415B 中时，将与保存了许可协议的条目对应的有效标志位变更为有效。

另外，许可协议的配送处理结束后，终端装置 20 的控制器 1106 向下载服务器 10 发送加密内容数据的配送请求，下载服务器 10 接收加密内容数据的配送请求。然后，下载服务器 10 的配送控制部 315 从信息数据库 304 中获取加密内容数据 E(Kc, Dc)以及附加信息 Di，通过总线 BS1 以及通信装置 350 将这些数据发送给终端装置 20。

终端装置 20 接收数据 $E(K_c, D_c)/Di$ ，获取加密内容数据 $E(K_c, D_c)$ 以及附加信息 Di 。这样，控制器 1106 将加密内容数据 $E(K_c, D_c)$ 以及附加信息 Di 作为 1 个内容文件通过总线 BS2 以及存储卡接口 1200 输入给存储卡 40。另外，控制器 1106 产生包含保存在存储卡 40 中的许可协议的条目编号、明文许可 ID、数据 ID 并且针对加密内容数据 $E(K_c, D_c)$ 以及附加信息 Di 的许可协议管理文件，所生成的许可协议管理文件通过总线 BS2 以及存储卡接口 1200 输入给存储卡 40。进一步，控制器 1106 在记录在存储卡 40 的存储器 1415 中的播放列表中，作为接收到的内容的信息，追加记录所记录的内容文件名称、许可协议管理文件名称、以及从附加信息 Di 中抽出的有关加密内容数据的信息（曲名、作者名）等，然后结束整个处理。

这样，在确认装载在终端装置 20 上的、保存许可协议的存储卡 40 是保存了正当的认证数据的机器、同时公开加密密钥 KPcm1 为有效的基础上，可以进行内容数据的配送，而且可以禁止向不正当存储卡配送内容数据。

进一步，通过存储在配送服务器以及存储卡上分别生成的加密密钥，利用相互接收到的加密密钥进行加密，将该加密数据传送给对方，在各自发送加密数据中可以进行事实上的相互认证，提高数据配送系统的安全性。

图 12 表示在存储卡 40 的存储器 1415 中的许可协议区域 1415B 和数据区域 1415C。在数据区域 1415C 中保存播放列表文件 160、条目管理信息 165、内容文件 1611～161n、许可管理文件 1621～162n。内容文件 1611～161n 将接收到的加密内容数据 $E(K_c, D_c)$ 以及附加信息 Di 一起作为 1 个文件保存。另外，许可管理文件 1621～162n 分别与内容文件 1611～161n 对应保存。

存储卡 40，在从下载服务器 10 接收到加密内容数据以及许可协议时，通过「复制/转移处理」从其它存储卡接收到加密内容数据以及许可协议时，将加密内容数据以及许可协议保存在存储器 1415 中。

传送给存储卡 40 的加密内容数据的许可协议，记录在由存储器 1415 的许可协议区域 1415B 的条目编号所指定的区域中，如果读出保存在存

储器 1415 的数据区域 1415C 中的播放列表文件 160 的许可协议管理文件, 可以获得条目编号, 根据所获取的条目编号可以从许可协议区域 1415B 读出对应的许可协议。

另外, 许可协议管理文件 1622 用虚线表示, 是表示实际上并没有保存。这表示虽然有内容文件 1612 但由于没有许可协议而不能播放, 例如这相当于终端装置 20 从其它终端装置只接收了加密内容数据的情况。

另外, 内容文件 1613 用虚线表示, 例如这相当于终端装置 20 从下载服务器 10 接收了加密内容数据以及许可协议, 而只将所接收到的加密内容数据传送给了其它终端装置的情况, 表示虽然有许可协议 1415 但不存在加密内容数据。

[再发送]

配送加密内容数据的许可协议的上述配送处理以错误结束时（这是通过在图 10 的第 S148～S162、S168、S170 之间通信被切断, 配送处理中断的情况), 希望向存储卡 40 再次发送成为对象的许可协议。在此, 以在图 10 的第 S148～S162、S168、S170 之间的动作成为许可协议再发送的对象, 是因为在输出由下载服务器 10 将许可协议 LIC 加密后的加密数据 $E(Ks2a, E(KPom2, LIC))$ (参见图 10 的第 S148 步) 之后, 实际上是否正确向存储卡 40 传送了该加密数据 $E(Ks2a, E(KPom2, LIC))$, 直到在第 S164 步向存储卡 40 发出出错消息之前不会知道。

图 13 以及图 14 表示在配送许可协议的配送处理被意外中断结束、许可协议消失时, 成为该配送对象的许可协议向存储卡 40 再发送时的动作的第 1 以及第 2 流程图。

在图 13 中, 许可协议的再发送动作开始后, 下载服务器 10 的配送控制部 315 控制会话密钥产生部 316 产生为选定许可协议的再发送中的通信的会话密钥 $Ks1b$, 会话密钥产生部 316 产生会话密钥 $Ks1b$ (第 S200 步)。然后, 解密处理部 318, 利用存储卡 40 的公开加密密钥 $KPcm1$ 对会话密钥 $Ks1b$ 进行加密, 产生加密数据 $E(KPcm1, Ks1b)$ (第 S202 步)。这样, 配送控制部 315 将在加密数据 $E(KPcm1, Ks1b)$ 上增加识别成为对象的许可协议的许可 ID (LID) 后的数据 LID// $E(KPcm1, Ks1b)$ 通过总线

BS1 以及通信装置 350 向终端装置 20 发送。终端装置 20 接收数据 LID//E(KPcm1, Ks1b)，通过总线 BS2 以及存储卡接口 1200 向存储卡 40 传送（第 S204 步）。然后，存储卡 40 的控制器 1420 通过端子 1426、接口 1424 以及总线 BS3 获取数据 LID// E(KPcm1, Ks1b)（第 S206 步）。

控制器 1420 向解密处理部 1422 输出加密数据 E(KPcm1, Ks1b)，解密处理部 1422 利用 Kcm 存储部 1421 的密码解密密钥 Kcm1 对加密数据 E(KPcm1, Ks1b) 进行解密，获得会话密钥 Ks1b（第 S208 步）。

这样，终端装置 20 通过总线 BS2 以及存储卡接口 1200 向存储卡 40 传送日志的输出请求（第 S210 步）。存储卡 40 的控制器 1420 通过端子 1426、接口 1424 以及总线 BS3 获取日志的输出请求（第 S212 步）。然后，控制器 1420 检索保存了包含与在第 S206 步获取的许可 ID 相同的许可 ID 的历史信息的日志条目（第 S214 步），如果检测不到该日志条目，则产生出错消息，通过总线 BS3、接口 1424 以及端子 1426 向终端装置 20 输出（第 S216 步）。

终端装置 20 获取来自存储卡 40 的出错消息（第 S218 步），通过再次拒绝写入结束这一系列动作（第 S252 步）。

另一方面，在第 S214 步，如果检测到日志条目，则成为在图 9 以及图 10 中中断的检测日志条目 160i。控制器 1420 利用在第 S206 步受理的许可 ID 检索许可协议区域 1415B 的条目，检索保存了包含与该许可 ID 相同的许可 ID 的许可协议的日志条目（第 S220 步）。

在第 S220 步中，如果检测到了保存了许可协议的条目，控制器 1420 利用与条目对应的有效标志位（参见图 12）判定所检测到的许可协议的有效性（第 S222 步），如果所检测到的许可协议有效，将在第 S214 步中检测到的日志条目 160i 的 ST2 区域 32 变更成「有数据」（第 S224 步）。另一方面，如果在第 S220 步中判定许可协议无效，控制器 1420 将日志条目 160i 的 ST2 区域 32 变更成「转移完毕」（第 S226 步）。这表示当包含在许可协议中的有效标志位为无效时，虽然在许可协议区域 1415B 中存在许可协议，由于该许可协议已经转移给其它存储卡等，禁止许可协议的复制，不能从存储卡 40 的许可协议区域 1415B 进一步输出许可协议。也就是说，许可协议无效表示该许可协议通过转移处理已经转移到其它

存储卡等中。

在第 S220 步中，如果没有检测到许可协议，由于这表示在存储卡 40 中不存在成为配送对象的许可协议，控制器 1420 将日志条目 160i 的 ST2 区域 32 变更成「无数据」（第 S228 步）。

在第 S224、S226、S228 步中的任一步之后，控制器 1420 获取在日志条目 160i 中保存的历史信息（第 S230 步），取出包含在该历史信息的 Ks2w 区域 2 中的会话密钥 Ks2c，输出到切换开关 1446 的触点 Pf。加密处理部 1406 通过切换开关 1446 的触点 Pf 接收会话密钥 Ks2c，通过切换开关 1442 的触点 Pa 接收会话密钥 Ks1b。然后，加密处理部 1406 利用会话密钥 Ks1b 对会话密钥 Ks2c 进行加密，将加密数据 E(Ks1b, Ks2c) 输出到总线 BS3（第 S232 步）。

这样，控制器 1420 产生在总线 BS3 上的加密数据 E(Ks1b, Ks2c) 上增加保存在第 S230 步中获取的历史信息中的许可 ID、以及状态信息（ST1、ST2）之后的数据 LID// E(Ks1b, Ks2c)//ST1//ST2，计算所生成的数据 LID// E(Ks1b, Ks2c)//ST1//ST2 的散列值 H(LID// E(Ks1b, Ks2c)//ST1//ST2)（第 S234 步）。然后，控制器 1420 通过总线 BS3 向切换开关 1446 的触点 Pf 输出散列值 H(LID// E(Ks1b, Ks2c)//ST1//ST2)，解密处理部 1406 通过切换开关 1446 的触点 Pf 接收散列值 H(LID// E(Ks1b, Ks2c)//ST1//ST2)，利用会话密钥 Ks1b 对该散列值 H(LID// E(Ks1b, Ks2c)//ST1//ST2) 进行加密，向总线 BS3 输出署名数据 E(Ks1b, H(LID// E(Ks1b, Ks2c)//ST1//ST2))（第 S236 步）。

然后，控制器 1420 生成在署名数据 E(Ks1b, H(LID// E(Ks1b, Ks2c)//ST1//ST2)) 上增加日志数据 LID//E(Ks1b, Ks2c)//ST1//ST2 后的带署名的日志数据 LID//E(Ks1b, Ks2c)//ST1//ST2//E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2))，通过总线 BS3、接口 1424 以及端子 1426 向终端装置 20 输出（第 S238 步）。

终端装置 20 向下载服务器 10 传送从存储卡 40 接收到的带署名的日志数据 LID//E(Ks1b, Ks2c)//ST1//ST2//E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2))，下载服务器 10 受理带署名的日志数据 LID//E(Ks1b, Ks2c)//ST1//ST2 //E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2))（第 S240 步）。

这样，配送控制部 315 将署名数据 $E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2))$ 输出给解密处理部 320，解密处理部 320 利用会话密钥 $Ks1b$ 对署名数据 $E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2))$ 进行解密，将解密后的散列值 $H(LID//E(Ks1b, Ks2c)//ST1//ST2)$ 输出给配送控制部 315。然后，配送控制部 315 在从存储卡 40 接收到的带署名的日志数据 $LID//E(Ks1b, Ks2c)//ST1//ST2//E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2))$ 中对日志数据 $LID//E(Ks1b, Ks2c)//ST1//ST2$ 计算散列值，确认所计算的散列值是否与从解密处理部 320 接收到的在存储卡 40 中运算的散列值 $H(LID//E(Ks1b, Ks2c))$ 一致。然后，配送控制部 315 通过确认 2 个散列值一致来验证带署名的日志数据 $LID//E(Ks1b, Ks2c)//ST1//ST2//E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2))$ (第 S242 步)。如果 2 个散列值不一致，带署名的日志数据 $LID//E(Ks1b, Ks2c)//ST1//ST2//E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2))$ 不被承认，通过再次写入拒绝结束这一系列动作 (第 S252 步)。在第 S242 步中，如果 2 个散列值一致时，带署名的日志数据 $LID//E(Ks1b, Ks2c)//ST1//ST2//E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2))$ ，配送控制部 315 利用许可 ID 检索配送记录数据库 (日志 DB) 308，检索是否存在向存储卡 40 的成为配送对象的许可协议 (第 S244 步)。然后，如果许可协议不存在，转移到第 S252 步通过再次写入拒绝结束这一系列动作。

在第 S244 步中当许可协议存在时，根据从存储卡 40 受理的历史信息的 ST1 区域 31 以及 ST2 区域 32 的数据判断存储卡 40 实际上是否受理了许可协议 (第 S246 步)，如果存储卡 40 实际上已经接收到许可协议，即接收后保存在存储器 1415 中时，转移到第 S252 步，通过再次写入拒绝结束这一系列动作。

在第 S246 步中，如果判定存储卡 40 实际上没有接收到许可协议时，转移到图 14 的第 S248 步。

在图 14 中，解密处理部 320 受理在利用会话密钥 $Ks1b$ 对加密数据 $E(Ks1b, Ks2c)$ 进行解密后在存储卡 40 中生成的会话密钥 $Ks2c$ (第 S248 步)。然后，配送控制部 315，判断在将许可协议向存储卡 40 的配送处理中从存储卡 40 受理的会话密钥 $Ks2a$ (参见图 9 的第 S138 步) 与在第 S248

步中受理的会话密钥 Ks2c 是否一致(第 S250 步)。然后,当会话密钥 Ks2a 与会话密钥 Ks2c 不一致时转移到第 S252 步,通过再次写入拒绝结束这一系列动作。

在将许可协议向存储卡 40 的配送处理中在存储卡 40 的日志区域 1415A 的历史信息中保存会话密钥 Ks2a(参见图 9 的第 S130 步),保存了会话密钥 Ks2a 的历史信息在第 S230 步(参见图 13)从日志区域 1415A 中获取,向下载服务器 10 发送,而在第 S130 步以后的各步骤中,在将许可协议向存储卡 40 的配送处理中为了明确是包含在从存储卡 40 向下载服务器 10 发送的历史信息中的会话密钥,而用“会话密钥 Ks2c”表示。因此,如果因图 9 的配送处理出现错误而结束后进行再发送处理时,会话密钥 Ks2a 与会话密钥 Ks2c 一致。

在此,当在第 S250 步中判定会话密钥 Ks2a 与会话密钥 Ks2c 一致时,配送控制部 315 通过总线 BS1 以及通信装置 350 将会话密钥请求发送给终端装置 20。

终端装置 20 接收到会话密钥请求之后通过总线 BS1 以及存储卡接口 1200 向存储卡 40 发送(第 S254 步),存储卡 40 的控制器 1420 通过端子 1426、接口 1424 以及总线 BS3 接收会话密钥请求。这样,控制器 1420 控制会话密钥产生部 1418,会话密钥产生部 1418 生成会话密钥 Ks2b(第 S256 步)。然后,控制器 1420 按照图 11 所示的流程图从日志区域 1415A 的日志条目 1601~160M 中选用保存用于记录下载服务器 10 向存储卡 40 再发送许可协议的通信的历史信息的日志条目(第 S258 步)。此外,这时一定采用日志条目 160i。

控制器 1420 将在第 S206 步中受理的许可协议 ID 和由会话密钥产生部 1418 生成的会话密钥 Ks2b 保存在所选用的日志条目 160i 中,将日志条目 160i 的 ST1 区域 31 变更为「接收等待」(第 S260 步)。然后,加密处理部 1406 通过切换开关 1446 的触点 Pe 从 KPom 保存部 1416 接收个别公开加密密钥 KPom2,通过切换开关 1446 的触点 Pd 接收会话密钥 Ks2b,利用会话密钥 Ks1b 对会话密钥 Ks2b 和个别公开加密密钥 KPom2 进行加密,产生加密数据 E(Ks1b, Ks2b//KPom2) 输出到总线 BS3(第 S262 步)。然后,控制器 1420 在加密数据 E(Ks1b, Ks2b//KPom2) 上增加了许

可 ID 后的数据 LID// E(Ks1b, Ks2b//KPom2)通过总线 BS3、接口 1424 以及端子 1426 向终端装置 20 输出 (第 S264 步), 终端装置 20 将数据 LID// E(Ks1b, Ks2b//KPom2)向下载服务器 10 发送, 下载服务器 10 接收数据 LID// E(Ks1b, Ks2b//KPom2) (第 S266 步)。

在下载服务器 10 中, 解密处理部 320 利用会话密钥 Ks1b 对加密数据 E(Ks1b, Ks2b//KPom2)进行解密, 获得会话密钥 Ks2b 和个别公开加密密钥 KPom2 (第 S268 步)。这样, 配送控制部 315 生成控制信息 (第 S270 步), 从信息数据库 304 获取数据 ID 以及内容密钥 Kc (第 S272 步)。

配送控制部 315 将许可 ID、数据 ID、内容密钥 Kc 以及控制信息 AC, 即许可 LIC 输出给加密处理部 326。加密处理部 326 利用由解密处理部 320 获得的存储卡 40 的个别公开加密密钥 KPom2 对许可 LIC 进行加密, 生成加密数据 E(KPom2, LIC) (第 S274 步)。然后, 加密处理部 328 利用由解密处理部 320 获得的会话密钥 Ks2b, 对来自加密处理部 326 的加密数据 E(KPom2, LIC)进行加密, 产生加密数据 E(Ks2b, E(KPom2, LIC))。

配送控制部 315, 通过总线 BS1 以及通信装置 350 将加密数据 E(Ks2b, E(KPom2, LIC))向终端装置 20 发送 (第 S278 步)。

终端装置 20 接收传送来的加密数据 E(Ks2b, E(KPom2, LIC)), 通过总线 BS2 以及存储卡接口 1200 向存储卡 40 输入 (第 S278 步)。然后, 存储卡 40 接收加密数据 E(Ks2b, E(KPom2, LIC)) (第 S280 步), 解密处理部 1412, 利用会话密钥 Ks2b 对通过端子 1426 以及接口 1424 向总线 BS3 输出的加密数据 E(Ks2b, E(KPom2, LIC))进行解密, 获得加密数据 E(KPom2, LIC) (第 S282 步)。然后, 将加密数据 E(KPom2, LIC)输入给解密处理部 1404, 解密处理部 1404 利用保存在 Kom 保存部 1402 中的个别密码解密密钥 Kom2 对加密数据 E(KPom2, LIC)进行解密, 获得许可 LIC (第 S284 步)。

这样, 从终端装置 20 输出许可协议的保存位置 (第 S286 步), 存储卡 40 的控制器 1420 通过端子 1426、接口 1424 以及总线 BS3 接收许可协议的保存位置 (第 S288 步)。然后, 控制器 1420 判定包含在所接收的许可 LIC 中的许可 ID 与在第 S260 步中保存在日志条目 160i 中的许可 ID 是否一致 (第 S290 步), 如果不一致, 控制器 1420 通过总线 BS3、接口

1424 以及端子 1426 向终端装置 20 输出出错消息（第 S292 步）。然后，终端装置 20 通过存储卡接口 1200 接收出错消息并向下载服务器 10 发送，下载服务器 10 接收出错消息（第 S294 步）。然后，由于错误结束配送处理（第 S296 步）。

另一方面，在第 S290 步中如果 2 个许可 ID 一致时，控制器 1420 将许可 LIC 保存在由许可协议区域 1415B 的许可协议保存位置所指定的条目中（第 S298 步），将记录再发送许可协议的通信的日志条目 160i 的 ST1 区域 31 变更成「接收完毕」（第 S300 步），正常结束许可协议的再发送的处理（第 S302 步）。

当向存储卡 40 再发送加密内容数据的许可协议的处理由于出现错误结束时（这是由于在图 14 的第 S278～S292、S298、S300 之间通信被切断，再发送处理被中断时的情况），再次按照图 13 以及图 14 所示的流程图向存储卡 40 再发送许可协议。

另外，在图 14 的第 S278～S292、S298、S300 之间的动作成为许可协议的再发送的对象的理由和上述理由相同。

[移动/复制]

如上所述，在图 1 所示的数据配送系统中，装载在终端装置 20 上的存储卡 40 可以接收来自下载服务器 10 的加密内容数据以及许可协议并保存。然后，终端装置 20 的用户可以将记录在自己的存储卡 40 中的加密内容数据向装载在终端装置 21 中的存储卡 41 自由复制。但是，终端装置 21 的用户即使将加密内容数据复制到自己的存储卡 41 中，如果不获取为解密所复制的加密内容数据的许可协议，也不能播放加密内容数据。

在此，说明从存储卡 40 向存储卡 41 进行的许可协议的复制/转移。这时，采用图 2 所示的系统在 2 个存储卡 40、41 之间进行许可协议的转移/复制。另外，存储卡 41 和存储卡 40 具有相同的构成，存储卡 41 的类识别子 y 和存储卡 40 相同，为 $y=1$ ，区别每个存储卡的识别子 z 为 $z=5$ 。

图 15 以及图 16 表示在图 2 中将记录在存储卡 40 中的许可协议向存储卡 41 移动/复制的流程图。此外，在图 15 中的处理之前，终端装置 20、21 的控制器 1106，与用户为进行许可协议的转移/复制而进行内容指定以

及为请求许可协议的转移/复制的输入装置（图中未画出）连接，接收由用户进行的为转移/复制许可协议而进行的内容指定、许可协议的转移/复制请求。然后，其前提条件是控制器 1106 访问发送端的存储卡 40 内的播放列表，获取了进行许可协议的转移/复制的许可协议管理文件，并且获取了保存在发送端的存储卡 40 以及接收目标的存储卡 41 内的各自的条目管理信息。进一步的前提条件是利用保存在发送端的存储卡 40 中的条目管理信息，确认在接收目标的存储卡 41 的许可协议区域 1415B 内有空余条目。

在图 15 中，当用户发出转移/复制请求的指示后，控制器 1106 通过总线 BS 向存储卡 41 发送类证书的输出要求（第 S400 步）。然后，存储卡 41 的控制器 1420 通过端子 1426、接口 1424 以及总线 BS3 接收证书数据的输出要求（第 S402 步）。

存储卡 41 的控制器 1420 接收到类证书的输出要求后，通过总线 BS3 从证书保存部 1400 读出类证书 Cm1，通过总线 BS3、接口 1424 以及端子 1426 向终端装置 21 的控制器 1106 输出所读出的类证书（第 S404 步）。然后，控制器 1106 通过总线 BS 接收类证书 Cm1（第 S405 步），通过总线 BS 向存储卡 40 发送存储卡 41 的类证书 Cm1（第 S406 步）。

这样，存储卡 40 的控制器 1420 通过端子 1426、接口 1424 以及总线 BS3 接收类证书 Cm1（第 S408 步），将接收到的类证书 Cm1 的署名数据 $E(KPa, H(KPcm1//1cm1))$ 输出给解密处理部 1408。然后，解密处理部 1408，利用来自 KPa 保存部 1414 的认证密钥 KPa 对署名数据 $E(KPa, H(KPcm1// 1cm1))$ 实施解密处理，并将该解密结果的散列值 $H(KPcm1//1cm1)$ 向控制器 1420 输出。控制器 1420 对类证书 Cm1 的数据 $KPcm1//1cm1$ 计算散列值，确认所计算的散列值是否与解密处理部 1408 接收到的散列值 $H(KPcm1//1cm1)$ 一致。即验证类证书 Cm1（第 S410 步）。

当 2 个散列值一致时，即判定是正当的类证书时，控制器 1420 承认从类证书 Cm1 获取的类公开加密密钥 KPcm1 并接收（第 S412 步）。当 2 个散列值不一致时，即判定是不正当的类证书时，将不承认，控制器 1420 通过总线 BS3、接口 1424 以及端子 1426 向终端装置 20 的控制器 1106 输出出错消息（第 S488 步），终端装置 20 的控制器 1106 接收出错消息

(第 S490 步), 通过写入拒绝结束这一系列动作 (第 S492 步)。

根据认证结果如果确认是向具有正当类证书的存储卡进行许可协议的转移/复制时, 在发送端的存储卡 40 中, 控制器 1420 控制会话密钥产生部 1418, 会话密钥产生部 1418 产生用于转移的会话密钥 Ks1d (第 S414 步)。会话密钥 Ks1d 在加密处理部 1410 中利用由解密处理部 1408 获取的存储卡 41 所对应的类公开加密密钥 KPcm1 被加密 (第 S416 步)。然后, 存储卡 40 的控制器 1420 通过总线 BS3 获取加密数据 E(KPcm1, Ks1d), 并通过总线 BS3、接口 1424 以及端子 1426 向终端装置 20 的控制器 1106 输出 (第 S418 步)。

控制器 1106 从发送端接收加密数据 E(KPcm1, Ks1d) (第 S420 步), 从发送端的存储卡 40 的许可管理信息获取许可 ID。然后, 控制器 1106 将所获得的许可 ID、和在第 S420 步接收到的加密数据 E(KPcm1, Ks1d) 作为一个数据通过总线 BS 向接收端的存储卡 41 输入数据 LID// E(KPcm1, Ks1d) (第 S422 步)。这样, 存储卡 41 的控制器 1420 通过端子 1426、接口 1424 以及总线 BS3 接收数据 LID//E(KPcm1, Ks1d) (第 S424 步)。然后, 控制器 1420 通过总线 BS3 向解密处理部 1422 输出加密数据 E(KPcm1, Ks1d), 解密处理部 1422 利用保存在 Kcm 保存部 1421 中的存储卡 41 固有的类密码解密密钥 Kcm1 进行解密处理, 获得会话密钥 Ks1d, 并受理会话密钥 Ks1d (第 S426 步)。

这样, 控制器 1106 通过总线 BS 向存储卡 40 发送会话密钥的输出要求(第 S428 步), 存储卡 41 的控制器 1420 通过端子 1426 以及接口 1424 接收会话密钥的输出要求, 控制会话密钥产生部 1418 产生会话密钥。然后, 会话密钥产生部 1418 产生会话密钥 Ks2d (第 S430 步), 控制器 1420 按照图 11 所示的给定流程从日志区域 1415A 的日志条目 1601~160M 中选用为记录从存储卡 40 接收许可协议的通信的历史信息的日志条目 (第 S432 步)。在此, 选用日志条目 160j ($1 \leq j \leq M$)。

然后, 控制器 1420 分别将接收到的许可 ID 以及所生成的会话密钥 Ks2d 分别保存在日志条目 160j 的许可 ID 区域 1 以及 Ks2w 区域 2 中, 将状态区域 3 的 ST1 区域 31 变更为「接收等待」(第 S434 步)。

加密处理部 1406, 利用通过切换开关 1442 的触点 Pa 由解密处理部

1422 输出的会话密钥 Ks1d，将通过依次对切换开关 1446 的触点进行切换所获得的会话密钥 Ks2d、以及个别公开加密密钥 KPom5 作为 1 个数据进行加密，将加密数据 E(Ks1d, Ks2d//KPom5)输出给总线 BS3（第 S436 步）。控制器 1420 通过总线 BS3、接口 1424 以及端子 1426 向终端装置 21 的控制器 1106 输出在输出到总线 BS3 上的加密数据 E(Ks1d, Ks2d//KPom5) 中增加许可 ID(LID)后的数据 LID//E(Ks1d, Ks2d//KPom5)（第 S438 步），控制器 1106 接收数据 LID//E(Ks1d, Ks2d//KPom5)（第 S440 步），通过总线 BS3 将接收到的数据 LID//E(Ks1d, Ks2d//KPom5)发送给存储卡 40（第 S442 步）。

存储卡 40 的控制器 1420 通过端子 1426、接口 1424 以及总线 BS3 接收数据 LID//E(Ks1d, Ks2d//KPom5)（第 S444 步），解密处理部 1413 利用会话密钥 Ks1d 解密出加密数据 E(Ks1d, Ks2d//KPom5)，接收在存储卡 41 生成的会话密钥 Ks2d、以及存储卡 41 的个别公开加密密钥 KPom5（第 S446 步）。然后，控制器 1420 按照图 11 所示的给定流程，从日志区域 1415A 的多个日志条目 1601~160M 中选用为记录向存储卡 41 进行许可协议的转移/复制的通信的历史信息的日志条目（第 S448 步）。在此，选用日志条目 160k ($1 \leq k \leq M$)。然后，控制器 1420 将许可 ID、会话密钥 Ks2d、类公开加密密钥 KPcm1 分别保存在所选用的日志条目 160k 的许可 ID 区域 1、Ks2w 区域 2 以及 KPcm1 区域 4 中，将日志条目 160k 的 ST1 区域 31 变更为「发送等待」（第 S450 步）。

这样，终端装置 20 的控制器 1106 输出许可协议的保存位置（第 S452 步），存储卡 40 的控制器 1420 通过端子 1426、接口 1424 以及总线 BS3 接收许可协议的保存位置（第 S454 步）。然后，控制器 1420 从由所接收的许可协议的保存位置所指定的许可协议区域 1415B 的条目中获取许可 LIC（第 S456 步），判断包含在所获取的许可 LIC 中的许可 ID 是否与在第 S450 步中在日志条目 160k 的许可 ID 区域 1 中记录的许可 ID 一致（第 S458 步），如果不一致，控制器 1420 通过总线 BS3、接口 1424 以及端子 1426 向控制器 1106 输出出错消息（第 S488 步），控制器 1106 接收出错消息（第 S490 步），通过写入拒绝结束这一系列的动作（第 S492 步）。

在第 S458 步中如果判定 2 个许可 ID 一致，则转移到图 16 的第 S460

步。

在图 16 中，存储卡 40 的控制器 1420 根据包含在第 S456 步获取的许可 LIC 中的控制信息 AC 确认是否没有禁止向存储卡 41 复制/转移许可协议（第 S460 步）。然后，如果禁止复制/转移，经过第 S488、S490 步后，通过写入拒绝结束这一系列的动作（第 S492 步）。如果允许复制/转移，加密处理部 1417 利用存储卡 41 的个别公开加密密钥 KPom5 对许可 LIC 进行加密（第 S462 步），加密处理部 1406 通过切换开关 1446 的触点 Pc 接收加密数据 E(KPom5, LIC)，利用通过切换开关 1442 的触点 Pb 接收到的会话密钥 Ks2d 对加密数据 E(KPom5, LIC)进一步加密（第 S464 步）。

这样，存储卡 40 的控制器 1420 根据控制信息 AC 判断是允许进行许可协议的复制，还是允许许可协议的转移（第 S466 步），如果判定是允许许可协议的转移时，使与保存了成为转移对象的许可协议的条目相对应的有效标志位设置成无效（第 S468 步），将日志条目 160k 的 ST1 区域 31 变更为「发送完毕」（第 S470 步）。

在第 S466 步中，如果判定是允许进行许可协议的复制，并且在第 S460 步之后，存储卡 40 的控制器 1420 通过总线 BS3、接口 1424 以及端子 1426 向控制器 1106 输出加密数据 E(Ks2d, E(KPom5, LIC))（第 S472 步）。

控制器 1106 接收发送来的加密数据 E(Ks2d, E(KPom5, LIC))，通过总线 BS3 向存储卡 41 输入。然后，存储卡 41 接收加密数据 E(Ks2d, E(KPom5, LIC))（第 S474 步），解密处理部 1412 通过端子 1426 以及接口 1424，接收利用会话密钥 Ks2d 对于输出到总线 BS3 的加密数据 E(Ks2d, E(KPom5, LIC)) 进行解密后的加密数据 E(KPom5, LIC)（第 S476 步）。然后，向解密处理部 1404 输入加密数据 E(KPom5, LIC)，解密处理部 1404 利用保存在 Kom 保存部 1402 中的存储卡 41 的个别密码解密密钥 Kom5 对加密数据 E(KPom5, LIC) 进行解密，获得许可 LIC（第 S478 步）。

这样，控制器 1106 输出许可协议的保存位置（第 S480 步），存储卡 41 的控制器 1420 通过端子 1426、接口 1424 以及总线 BS3 接收许可协议的保存位置（第 S482 步）。然后，存储卡 41 的控制器 1420 判断包含在所获取的许可 LIC 中的许可 ID 是否与在第 S434 步中在日志条目 160j 的

许可 ID 区域 1 中记录的许可 ID 一致（第 S484 步），如果不一致，控制器 1420 通过总线 BS3、接口 1424 以及端子 1426 向终端装置 21 的控制器 1106 输出出错消息（第 S486 步）。然后，终端装置 21 的控制器 1106 接收出错消息，并向终端装置 20 发送，终端装置 20 接收出错消息（第 S490 步）。然后，通过写入拒绝结束这一系列的动作（第 S492 步）。

另一方面，在第 S484 步中如果判定 2 个许可 ID 一致，控制器 1420 将许可 LIC 记录在由许可协议区域 1415B 的许可协议保存位置所指定的许可协议区域 1415B 的条目中（第 S494 步），将日志条目 160j 的 ST1 区域 31 变更为「接收完毕」（第 S496 步），正常结束复制/转移处理（第 S498 步）。

此外，从存储卡 40 向存储卡 41 进行加密内容数据的转移/复制、也可以在许可协议的转移/复制结束后，从存储卡 40 的数据区域 1415C 中读出加密内容数据向存储卡 41 发送。

另外，对于接收侧的存储卡 41，对于转移/复制后的许可协议的许可协议管理文件已经记录时，通过在许可协议管理文件的保存位置上写入，更新对象的许可协议管理文件。另外，成为对象的许可协议管理文件如果没有在存储卡 40 中记录时，产生新的许可协议管理文件，将所生成的许可协议管理文件记录在接收侧的存储卡 41 中。

这样，在确认装载在终端装置 21 上的存储卡 41 是正当的机器、同时类公开加密密钥 KPcm1 有效的基础上，只可以对向正当存储卡的转移要求进行许可协议的转移，可以禁止向非正当存储卡的转移。

另外，通过在存储卡上生成的加密密钥，利用相互接收到的加密密钥进行加密，将该加密数据传送给对方，在各自发送加密数据中可以进行事实上的相互认证，在许可协议的转移/复制的动作中提高安全性。

[转移/复制中的再发送]

当上述加密内容数据的许可协议的复制/转移的处理由于出现意外中断结束时（这是由于在从图 15 的第 S452 步到图 16 的第 S486、S494、S496 之间通信被切断，复制/转移处理被中断时的情况），希望可以向存储卡 41 再次发送成为对象的许可协议。

此外，在从图 15 的第 S452 步到图 16 的第 S486、S494、S496 之间的动作成为再发送的对象的理由和上述理由相同。

图 17~图 19 表示许可协议的复制/转移处理被中断结束时，向存储卡 41 再次发送成为发送对象的许可协议时的动作的第 1、第 2 以及第 3 流程图。

在图 17 中，在许可协议的复制/转移处理中再发送的动作开始后，终端装置 20 的控制器 1106 向存储卡 40 发送数据 LID//恢复请求（第 S500 步）。然后，存储卡 40 的控制器 1420 通过端子 1426、接口 1424 以及总线 BS3 接收数据 LID//恢复请求，检索是否包含和所接收的许可 ID(LID)相同的许可 ID 的日志条目（第 S500 步）。图 15、16 的处理因错误而结束时，保存在日志条目 160k 中的历史信息与此相当。如果没有包含相同许可 ID 的历史信息时，存储卡 40 的控制器 1420 通过总线 BS3、接口 1424 以及端子 1426 向控制器 1106 输出出错消息（第 S630 步），控制器 1106 接收出错消息（第 S634 步），通过写入拒绝结束这一系列的动作（第 S636 步）。

在第 S502 步中，如果检测到包含相同许可 ID 的历史信息，存储卡 40 的控制器 1420 读出该历史信息，根据包含在所读出的历史信息中的 ST1 区域 31 判断是否向存储卡 41 发送许可协议（第 S504 步），当许可协议已经向存储卡 41 发送时，转移到第 S630 步，如上所述，通过写入拒绝结束这一系列的动作（第 S636 步）。

在第 S504 步中，如果判定许可协议没有向存储卡 41 发送时，控制器 1420 控制会话密钥产生部 1418 产生为选定向存储卡 41 再发送许可协议的通信的会话密钥 Ks1e，会话密钥产生部 141 产生会话密钥 Ks1e（第 S506 步）。然后，加密处理部 1410 利用包含在所读出的历史信息中的存储卡 41 的类公开加密密钥 KPcm1 对会话密钥 Ks1e 进行加密，生成加密数据 E(KPcm1, Ks1e)（第 S508 步）。这样，存储卡 40 的控制器 1420，将在加密数据 E(KPcm1, Ks1e)增加了为识别成为发送对象的许可协议的许可 ID(LID)后的数据 LID// E(KPcm1, Ks1e)，通过总线 BS3、接口 1424 以及端子 1426 向控制器 1106 发送（第 S510 步）。控制器 1106 接收数据 LID// E(KPcm1, Ks1e)（第 S512 步），将数据 LID// E(KPcm1, Ks1e)通过

总线 BS 向存储卡 41 发送（第 S514 步）。然后，存储卡 41 的控制器 1420 通过端子 1426、接口 1424 以及总线 BS3 接收数据 LID// E(KPcm1, Ks1e)（第 S516 步）。

存储卡 41 的控制器 1420 将加密数据 E(KPcm1, Ks1e)输出给解密处理部 1422，解密处理部 1422 利用 Kcm 保存部 1421 中的类密码解密密钥 Kcm1 对加密数据 E(KPcm1, Ks1e)进行解密，获得会话密钥 Ks1e（第 S518 步）。

这样，终端装置 20 的控制器 1106，向终端装置 21 输出日志输出请求，终端装置 21 的控制器 1106 通过总线 BS 向存储卡 41 输出日志输出请求（第 S520 步）。存储卡 40 的控制器 1420 通过端子 1426、接口 1424 以及总线 BS3 接收日志输出请求（第 S522 步）。然后，控制器 1420 检索在许可 ID 区域 1 中记录了与在第 S516 步中接收的许可 ID 相同的许可 ID 的日志条目（第 S524 步），如果没有检索到该日志条目，产生出错消息通过总线 BS3、接口 1424 以及端子 1426 向终端装置 21 的控制器 1106 输出（第 S632 步）。然后，如上所述，通过写入拒绝结束这一系列的动作（第 S634、S636 步）。

另一方面，在第 S524 步中，如果检索到保存了相同的许可 ID 的日志条目，处理继续进行。然后，图 15 以及图 16 所示的转移、复制处理中断时检测日志条目 160j。这样，控制器 1420，采用在第 S516 步中接收的许可 ID 检索许可协议区域 1415B 的日志条目，检索包含和该许可协议 ID 相同的许可 ID 的许可协议（第 S526 步）。

在第 S526 步中，如果检测到许可协议，存储卡 41 的控制器 1420 利用与记录了所检测许可协议的日志条目对应的有效标志位（参见图 12）判定许可协议的有效性（第 S528 步），如果检测到的许可协议有效，在第 S524 步中将日志条目 160j 的 ST2 区域 32 变更为「有数据」（第 S530 步）。另一方面，在第 S528 步中如果判定许可协议无效，控制器 1420 将日志条目 160j 的 ST2 区域 32 变更为「转移完毕」（第 S532 步）。该「转移完毕」的意义和上述相同。

在第 S526 步中，如果没有检测到许可协议，表明在存储卡 41 中成为发送对象的许可协议不存在，存储卡 41 的控制器 1420 将日志条目 160j

的 ST2 区域 32 变更为「无数据」(第 S534 步)。

在第 S530、S532、S534 步中的任一步之后，存储卡 41 的控制器 1420 获取日志条目 160j 内的历史信息(日志) LID//Ks2f//ST1//ST2(第 S536 步)，取出会话密钥 Ks2f，输出到切换开关 1446 的触点 Pf 上。加密处理部 1406 通过切换开关 1446 的触点 Pf 接收会话密钥 Ks2f，通过切换开关 1442 的触点 Pa 接收会话密钥 Ks1e。然后，加密处理部 1406 利用会话密钥 Ks1e 对会话密钥 Ks2f 加密，将加密数据 E(Ks1e, Ks2f) 输出到总线 BS3 上(第 S538 步)。

然后，存储卡 41 的控制器 1420，生成在总线 BS3 上的加密数据 E(Ks1e, Ks2f) 中增加了保存在第 S536 步获取的历史信息中的许可 ID、以及状态信息(ST1、ST2)之后的日志数据 LID// E(Ks1e, Ks2f)//ST1//ST2，计算所生成的日志数据 LID// E(Ks1e, Ks2f)//ST1//ST2 的散列值 H(LID// E(Ks1e, Ks2f)//ST1//ST2)(第 S540 步)。然后，控制器 1420 将散列值 H(LID// E(Ks1e, Ks2f)//ST1//ST2) 通过总线 BS3 输出到切换开关 1446 的触点 Pf 上，加密处理部 1406 通过切换开关 1446 的触点 Pf 接收散列值 H(LID//E(Ks1e, Ks2f)//ST1//ST2)，利用会话密钥 Ks1e 对所接收的散列值 H(LID//E(Ks1e, Ks2f)//ST1//ST2) 进行加密后，将署名数据 E(Ks1e, H(LID // E(Ks1e, Ks2f)//ST1//ST2)) 输出到总线 BS3 上(第 S542 步)。

然后，存储卡 41 的控制器 1420 生成在署名数据 E(Ks1e, H(LID // E(Ks1e, Ks2f)//ST1//ST2)) 中增加了日志数据 LID//E(Ks1e, Ks2f)//ST1// ST2 后的带署名的日志数据 LID// E(Ks1e, Ks2f)//ST1//ST2//E(Ks1e, H(LID //E(Ks1e, Ks2f)//ST1//ST2))，并通过总线 BS3、接口 1424 以及端子 1426 向终端装置 21 的控制器 1106 输出(第 S544 步)。

控制器 1106 接收存储卡 41 所接收的带署名的日志数据 LID// E(Ks1e, Ks2f)//ST1//ST2//E(Ks1e, H(LID //E(Ks1e, Ks2f)//ST1//ST2))(第 S546 步)，将所接收的带署名的日志数据 LID// E(Ks1e, Ks2f)//ST1//ST2//E(Ks1e, H(LID //E(Ks1e, Ks2f)//ST1//ST2)) 向存储卡 40 输出(第 S548 步)。

在图 18 中，存储卡 40 的控制器 1420 通过端子 1426、接口 1424 以及总线 BS3 接收带署名的日志数据 LID// E(Ks1e, Ks2f)//ST1//ST2//E(Ks1e, H(LID //E(Ks1e, Ks2f)//ST1//ST2))(第 S550 步)。

这样，控制器 1420 将署名数据 $E(Ks1e, H(LID//E(Ks1e, Ks2f)//ST1//ST2))$ 输出给解密处理部 1412，解密处理部 1412 利用会话密钥 $Ks1e$ 对署名数据 $E(Ks1e, H(LID // E(Ks1e, Ks2f)//ST1//ST2))$ 进行解密，将解密后的散列值 $H(LID// E(Ks1e, Ks2f)//ST1//ST2)$ 向控制器 1420 输出。另外，存储卡 41 的控制器 1420 对日志数据 $LID// E(Ks1e, Ks2f)//ST1//ST2$ 计算散列值，确认所计算的散列值是否与在存储卡 41 中计算的散列值 $H(LID// E(Ks1e, Ks2f)//ST1//ST2)$ 一致。然后，存储卡 40 的控制器 1420 通过确认 2 个散列值一致，验证从存储卡 41 接收到的带署名的日志数据 $LID// E(Ks1e, Ks2f)//ST1//ST2//E(Ks1e, H(LID //E(Ks1e, Ks2f)//ST1//ST2))$ (第 S552 步)。

如果 2 个散列值不一致，不承认带署名的日志数据 $LID// E(Ks1e, Ks2f)//ST1//ST2//E(Ks1e, H(LID //E(Ks1e, Ks2f)//ST1//ST2))$ ，如上所述，通过写入拒绝结束这一系列的动作 (第 S636 步)。另一方面，在第 S552 步中如果 2 个散列值一致，带署名的日志数据 $LID//E(Ks1e, Ks2f)//ST1//ST2//E(Ks1e, H(LID //E(Ks1e, Ks2f)//ST1//ST2))$ 被承认，控制器 1420 利用许可 ID 检索许可协议区域 1415B 的日志条目，检索是否存在成为向存储卡 41 发送的对象的许可协议 (第 S554 步)。然后，如果许可协议不存在，转移到第 S630 步，通过写入拒绝结束这一系列的动作 (第 S636 步)。

在第 S554 步中如果许可协议存在，控制器 1420 利用与该许可协议的条目对应的有效标志位判断许可协议的有效性 (第 S556 步)，如果许可协议有效转移到第 S562 步。另一方面，在第 S556 步中如果判断许可协议无效，控制器 1420 根据从存储卡 41 接收的历史信息的 ST1 区域 31 以及 ST1 区域 32 的数据判断存储卡 41 实际上是否接收到许可协议 (第 S558 步)，如果存储卡 41 实际上接收到许可协议，转移到第 S630 步，通过写入拒绝结束这一系列的动作 (第 S636 步)。

在第 S558 步中，如果判断存储卡 41 实际上没有接收到许可协议，存储卡 40 的控制器 1420 使检索到的许可协议有效 (第 S560 步)，通过总线 BS3、接口 1424 以及端子 1426 向终端装置 20 的控制器 1106 输出恢复消息。然后，控制器 1106 向终端装置 21 输出恢复消息，终端装置 21 的控制器 1106 接收恢复消息 (第 S564 步)。

这样，控制器 1106 通过总线 BS 向存储卡 41 发送会话密钥请求（第 S566 步），存储卡 41 的控制器 1420 通过端子 1426、接口 1424 以及总线 BS3 接收会话密钥请求。然后，控制器 1420 控制会话密钥产生部 1418，会话密钥产生部 1418 生成会话密钥 Ks2e(第 S568 步)。然后，控制器 1420 按照图 11 所示的流程图从日志区域 1415A 的日志条目 1601~160M 中选用保存用于记录存储卡 40 向存储卡 41 再发送许可协议的通信的历史信息（第 S570 步）。在此一定采用日志条目 160j。

控制器 1420 将在第 S516 步中接收到的许可 ID 以及由会话密钥产生部 1418 所生成的会话密钥 Ks2e 保存所选用的日志条目 160j 中，将日志条目 160j 的 ST1 区域 31 变更为「接收等待」（第 S572 步）然后，加密处理部 1406，通过切换开关 1446 的触点 Pe 接收来自 KPom 保存部 1416 的个别公开加密密钥 KPom5，通过切换开关 1446 的触点 Pd 接收会话密钥 Ks2e，利用会话密钥 Ks1e 对会话密钥 Ks2e 和个别公开加密密钥 KPom5 进行加密，生成加密数据 E(Ks1e, Ks2e//KPom5)，输出给总线 BS3(第 S574 步)。然后，控制器 1420 通过总线 BS3、接口 1424 以及端子 1426 向控制器 1106 输出在输出到总线 BS3 上的加密数据 E(Ks1e, Ks2e//KPom5) 中增加了许可 ID 后的数据 LID// E(Ks1e, Ks2e//KPom5)（第 S576 步），控制器 1106 接收数据 LID// E(Ks1e, Ks2e//KPom5)（第 S578 步）。然后，控制器 1106 向存储卡 40 输出数据 LID// E(Ks1e, Ks2e//KPom5)（第 S580 步），存储卡 40 的控制器 1420 通过端子 1426、接口 1424 以及总线 BS3 接收数据 LID// E(Ks1e, Ks2e//KPom5)（第 S582 步）。

在存储卡 40 中，解密处理部 1412 利用会话密钥 Ks1e 对加密数据 E(Ks1e, Ks2e//KPom5)进行解密，接收会话密钥 Ks2e 和个别公开加密密钥 KPom5（第 S584 步）。

在图 19 中，在第 S584 步之后，控制器 1420 按照图 11 所示的给定流程，从多个日志条目 1601~160M 中选用为记录向存储卡 41 再发送许可协议的通信的日志条目（第 S586 步）。在此，一定选用日志条目 160k。然后，控制器 1420 将在第 S582 步接收的许可 ID、由会话密钥产生部 1418 产生的会话密钥 Ks2e 以及类公开加密密钥 KPcm1 分别保存在所选用的日志条目 160k 的许可 ID 区域 1、Ks2w 区域 2 以及 KPcm1 区域 4 中，

将日志条目 160k 的 ST1 区域 31 变更为「发送等待」(第 S588 步)。

这样，控制器 1106 向存储卡 40 输出许可协议的保存位置(第 S590 步)，存储卡 40 的控制器 1420 通过端子 1426、接口 1424 以及总线 BS3 接收许可协议的保存位置(第 S592 步)。然后，控制器 1420 从由所接收的许可协议的保存位置所指定的条目中获取许可 LIC(第 S594 步)，判断包含在所获取的许可 LIC 中的许可 ID 是否与在第 S588 步中保存在日志条目 160j 中的许可 ID 一致(第 S596 步)，如果不一致，控制器 1420 通过总线 BS3、接口 1424 以及端子 1426 向控制器 1106 输出出错消息(第 S630 步)，控制器 1106 接收出错消息(第 S634 步)，通过写入拒绝结束这一系列的动作(第 S636 步)。

在第 S596 步中如果判定 2 个许可 ID 一致，控制器 1420 根据包含在第 S596 步获取的许可 LIC 中的控制信息 AC 确认是否没有禁止向存储卡 41 复制/转移许可协议(第 S598 步)。然后，如果禁止复制/转移，经过第 S630、S634 步后，通过写入拒绝结束这一系列的动作(第 S636 步)。如果允许复制/转移，加密处理部 1417 利用存储卡 41 的个别公开加密密钥 KPom5 对许可 LIC 进行加密(第 S600 步)，加密处理部 1406 通过切换开关 1446 的触点 Pc 接收加密数据 E(KPom5, LIC)，利用通过切换开关 1442 的触点 Pb 接收到的会话密钥 Ks2e 对加密数据 E(KPom5, LIC)进一步加密(第 S602 步)。

这样，控制器 1420 根据控制信息 AC 判断是允许进行许可协议的复制，还是允许许可协议的转移(第 S604 步)，如果判定是允许许可协议的转移时，使与保存了成为转移对象的许可协议的条目相对应的有效标志位设置成无效(第 S606 步)，将日志条目 160k 的 ST1 区域 31 变更为「发送完毕」(第 S608 步)。

在第 S604 步中，如果判定是允许进行许可协议的复制，并且在第 S608 步之后，控制器 1420 通过总线 BS3、接口 1424 以及端子 1426 向控制器 1106 输出加密数据 E(Ks2e, E(KPom5, LIC)) (第 S610 步)。

控制器 1106 接收发送来的加密数据 E(Ks2e, E(KPom5, LIC))，通过总线 BS3 向存储卡 41 输入。然后，存储卡 40 接收加密数据 E(Ks2e, E(KPom5, LIC)) (第 S612 步)，解密处理部 1412 通过端子 1426 以及接口

1424，接收利用会话密钥 Ks2e 对于输出到总线 BS3 的加密数据 E(Ks2e, E(KPom5, LIC)) 进行解密后的加密数据 E(KPom5, LIC) (第 S614 步)。然后，向解密处理部 1404 输入加密数据 E(KPom5, LIC)，解密处理部 1404 利用保存在 Kom 保存部 1402 中的个别密码解密密钥 Kom5 对加密数据 E(KPom5, LIC) 进行解密，获得许可 LIC (第 S616 步)。

这样，控制器 1106 向存储卡 41 输出许可协议的保存位置 (第 S618 步)，存储卡 41 的控制器 1420 通过端子 1426、接口 1424 以及总线 BS3 接收许可协议的保存位置 (第 S620 步)。然后，存储卡 41 的控制器 1420 判断包含在所获取的许可 LIC 中的许可 ID 是否与在第 S572 步中在日志条目 160j 的许可 ID 区域 1 中记录的许可 ID 一致 (第 S622 步)，如果不一致，控制器 1420 通过总线 BS3、接口 1424 以及端子 1426 向终端装置 21 的控制器 1106 输出出错消息 (第 S632 步)，控制器 1106 接收出错消息 (第 S634 步)。然后，通过写入拒绝结束这一系列的动作 (第 S636 步)。

另一方面，在第 S622 步中如果判定 2 个许可 ID 一致，存储卡 41 的控制器 1420 将许可 LIC 记录在由许可协议区域 1415B 的许可协议保存位置所指定的位置中 (第 S624 步)，将日志条目 160j 的 ST1 区域 31 变更为「接收完毕」(第 S626 步)，正常结束复制/转移处理 (第 S628 步)。

此外，从存储卡 40 向存储卡 41 进行加密内容数据的转移/复制、也可以在许可协议的转移/复制结束后，从存储卡 40 的数据区域 1415C 中读出加密内容数据向存储卡 41 发送。

当加密内容数据的许可协议向存储卡 41 再发送的会话因出现错误而结束时 (这是由于在从图 19 的第 S610~S626 步之间通信被切断，再发送处理被中断时的情况)，按照图 17~图 19 所示的流程图向存储卡 41 再发送许可协议。

此外，在从图 19 的第 S610~S626 步之间的动作成为再发送的对象的理由和上述理由相同。

[播放]

如上所述，装载在终端装置 20 上的存储卡 40 可以直接从下载服务器 10 接收加密内容数据以及许可协议。另外，存储卡 41 可以从存储卡 40，

利用「转移」的概念，接收加密内容数据以及许可协议。

在此，对利用上述各种方法存储卡接收到的加密内容数据的播放进行说明。

图 20 表示存储卡 40 接收的加密内容数据 $E(Kc, Dc)$ 在终端装置 20 的内容播放电路 1550 中进行播放时的动作的流程图。在终端装置 20 上装载存储卡 41，可以进行播放，这时按照图 20 进行播放。此外，在图 20 中的处理之前，其前提条件是以终端装置 20 的用户按照存储卡 40 的数据区域 1415C 中记录的播放列表，确定了要播放的内容（乐曲），选定了内容文件，获取了许可协议管理文件。

在图 20 中，播放动作开始后，终端装置 20 的用户通过操作面板 1108 将播放请求输入给终端装置 20。这样，控制器 1106 通过总线 BS2 对内容播放电路 1550 发出类证书的输出要求，内容播放电路 1550 输出类证书 Cp3，控制器 1106 通过总线 2 以及存储卡接口 1200，向存储卡 40 输入类证书 Cp3（第 S700 步）。

然后，存储卡 40 接收类证书 $Cp3 = KPcp3//1cp3//E(Ka, H(KPcp3//1cp3))$ ，解密处理部 1408 从类证书 Cp3 中利用保存在 KPa 保存部 1414 中的认证密钥 KPa 对署名数据 $E(Ka, H(KPcp3//1cp3))$ 进行解密，解密后的散列值 $H(KPcp3//1cp3)$ 向控制器 1420 输出。控制器 1420 对类证书 Cp3 中的数据 $KPcp3//1cp3$ 计算散列值，确认所计算的散列值是否与在内容播放电路 1550 中计算的散列值 $H(KPcp3//1cp3)$ 是否一致。然后，通过确认 2 个散列值一致，验证内容播放电路 1550 接收的类证书 Cp3（第 S704 步）。当 2 个散列值不一致时，类证书 Cp3 不被认证，控制器 1420 通过总线 BS3、接口 1424 以及端子 1426 向终端装置 20 的控制器 1106 输出出错消息（第 S752 步），控制器 1106 接收出错消息（第 S754 步）。然后，通过拒绝播放结束这一系列的动作（第 S756 步）。

当 2 个散列值一致时，类证书 Cp3 被承认，控制器 1420 接收公开加密密钥 KPcp3（第 S706 步），控制会话密钥产生部 1418 产生会话密钥。这样，会话密钥产生部 1418 产生播放处理用的会话密钥 Ks1g（第 S708 步）。然后，加密处理部 1410 利用由解密处理部 1408 解密后的类公开加密密钥 KPcp3 对会话密钥产生部 1418 生成的会话密钥 Ks1g 进行加密，

将加密数据 $E(KPcp3, Ks1g)$ 向总线 BS3 输出（第 S710 步）。这样，控制器 1420 通过接口 1424 以及端子 1426 向存储卡接口 1200 输出加密数据 $E(KPcp3, Ks1g)$ （第 S712 步）。终端装置 20 的控制器 1106 通过存储卡接口 1200 接收加密数据 $E(KPcp3, Ks1g)$ （第 S714 步）。然后，控制器 1106 通过总线 BS2 将加密数据 $E(KPcp3, Ks1g)$ 向内容播放电路 1550 的解密处理部 1504 输出，解密处理部 1504 通过 Kcp 保存部 1502 输出的、与公开加密密钥 KPcp3 成对的类密码解密密钥 Kcp3 对加密数据 $E(KPcp3, Ks1g)$ 进行解密，向加密处理部 1506 输出会话密钥 $Ks2g$ （第 S716 步）。这样，会话密钥产生部 1508 产生播放处理用的会话密钥 $Ks2g$ ，将所产生的会话密钥 $Ks2g$ 向加密处理部 1506 输出（第 S718 步）。加密处理部 1506 利用解密处理部 1504 输出的会话密钥 $Ks1g$ 对会话密钥产生部 1508 输出的会话密钥 $Ks2g$ 进行加密，生成加密数据 $E(Ks1g, Ks2g)$ （第 S720 步），控制器 1106 通过总线 BS3 以及存储卡接口 1200 向存储卡 40 输出加密数据 $E(Ks1g, Ks2g)$ （第 S722 步）。

然后，存储卡 40 的解密处理部 1412 通过端子 1426、接口 1424 以及总线 BS3 输入加密数据 $E(Ks1g, Ks2g)$ （第 S724 步）。解密处理部 1412 利用在会话密钥产生部 1518 产生的会话密钥 $Ks1g$ 对加密数据 $E(Ks1g, Ks2g)$ 进行解密，接收在终端装置 20 产生的会话密钥 $Ks2g$ （第 S726 步）。

终端装置 20 的控制器 1106 获取在从存储卡 40 事先获取的播放请求乐曲的许可协议管理文件中保存的许可协议的保存位置，通过存储卡接口 1200 向存储卡 40 输出所获取的保存位置（第 S728 步）。

存储卡 40 的控制器 1420 接收保存位置（第 S730 步），获取在由所接收的保存位置指定的条目中保存的许可协议以及与条目对应的有效标志位。然后，控制器 1420 利用有效标志位确认许可协议的有效性（第 S732 步）。在第 S732 步中，当许可协议为「无效」时，由于在指定的条目中许可协议不存在，经过第 S752、S754 步后，通过拒绝播放接收播放动作（第 S756 步）。在第 S732 步中，当许可协议为「有效」时，由于在指定的条目中存在许可协议，获取许可协议（第 S734 步）。

然后，控制器 1420 确认控制信息 AC（第 S736 步）。

在第 S736 步中，通过确认控制信息 AC，具体讲，通过确认播放次

数；如果是已经不能播放的状态时，结束播放动作，当有限制控制信息 AC 的播放次数时，在变更控制信息 AC 的播放次数（第 S738 步）后进入到下一步（第 S740 步）。

另一方面，当控制信息 AC 的播放次数不限制播放时，跳过第 S738 步，不对控制信息 AC 的播放次数进行变更而进入到下一步处理（第 S740 步）。

在第 S736 步中，当在播放动作中判断是不能播放时，将记录在存储器 1415 的许可协议区域 1415B 中的播放请求乐曲的内容密钥 Kc 输出到总线 BS3 上（第 S740 步）。

所获得的内容密钥 Kc，通过切换开关 1446 的触点 Pf 传送给加密处理部 1406。加密处理部 1406，利用通过切换开关 1442 的触点 Pb 由解密处理部 1412 接收到的会话密钥 Ks2g，对通过切换开关 1446 接收到的内容密钥 Kc 加密（第 S742 步），将加密数据 E(Ks2g, Kc) 向总线 BS3 输出（第 S744 步）。

输出到总线 BS3 上的加密数据 E(Ks2g, Kc) 通过接口 1424、端子 1426、以及存储卡接口 1200 传送给终端装置 20 的控制器 1106。

在终端装置 20 中，控制器 1106 接收通过存储卡接口 1200 传递到总线 BS2 上的加密数据 E(Ks2g, Kc)（第 S746 步），将所接收的加密数据 E(Ks2g, Kc) 向解密处理部 1510 输出，解密处理部 1510 利用会话密钥 Ks2g 对加密数据 E(Ks2g, Kc) 进行解密，获取内容密钥 Kc（第 S748 步）。然后，解密处理部 1510，将内容密钥 Kc 向解密处理部 1516 输出。

控制器 1106 通过存储卡接口 1200 向存储卡 40 请求加密数据 E(Kc, Dc)，通过总线 BS3、接口 1424 以及端子 1426 向存储卡接口 1200 输出加密数据 E(Kc, Dc)。

终端装置 20 的控制器 1106 通过存储卡接口 1200 获取加密数据 E(Kc, Dc)，通过总线 BS2 将加密数据 E(Kc, Dc) 向内容播放电路 1550 输出。

然后，内容播放电路 1550 的解密处理部 1516 利用解密处理部 1510 输出的内容密钥 Kc 对加密数据 E(Kc, Dc) 解密后，获取内容数据 Dc。

然后，将解密后的内容数据 Dc 向音乐播放部 1518 输出，音乐播放部 1518 播放内容数据，DA 播放器 1519 将数字信号转换成模拟信号后向

端子 1530 输出。然后音乐数据从端子 1530 通过外部输出装置向头戴耳机输出，进行播放。这样正常结束播放动作（第 S750 步）。

在上面的说明中，虽然是以为对加密内容数据解密的许可协议为例，对许可协议的复原处理进行了说明，但在本发明中，作为复原对象，并不限定于对加密内容数据解密的许可协议，个人信息、以及信用卡信息等不能同时有 2 个以上存在的要求保密的数据均可以成为复原的对象。对于这样的数据可以采用上述的各个处理。

这时，用要求保密的数据替换许可协议内的内容密钥 K_c ，可以容易实现。

上述实施方案只是对所有的点进行了例示，并不应该认为是对本发明的限制。本发明的范围并不是上述实施方案中说明的范围，而是由权利要求的范围确定，只要在与权利要求的范围等同的内容以及范围内，可以进行各种变形。

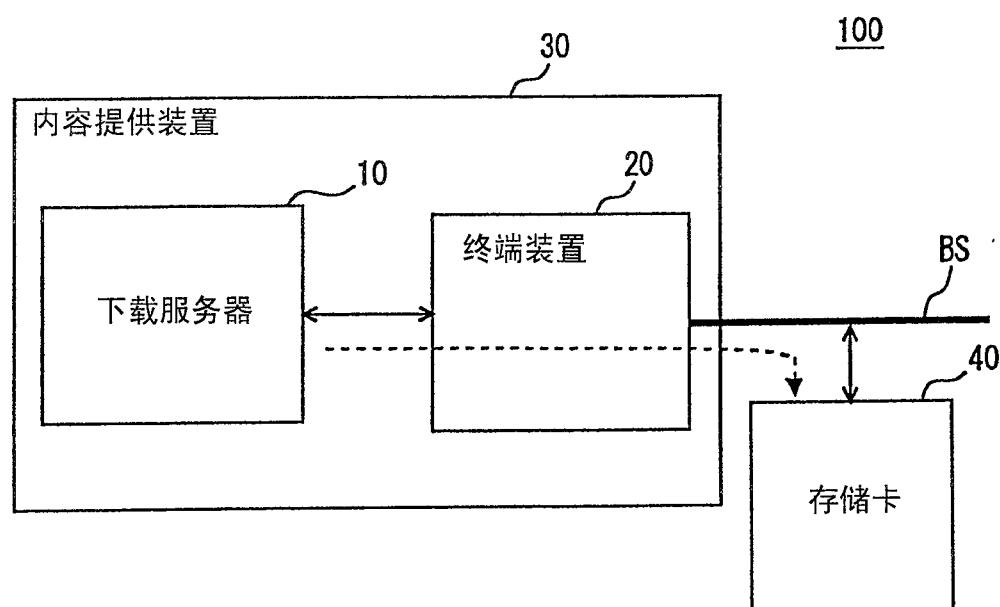


图 1

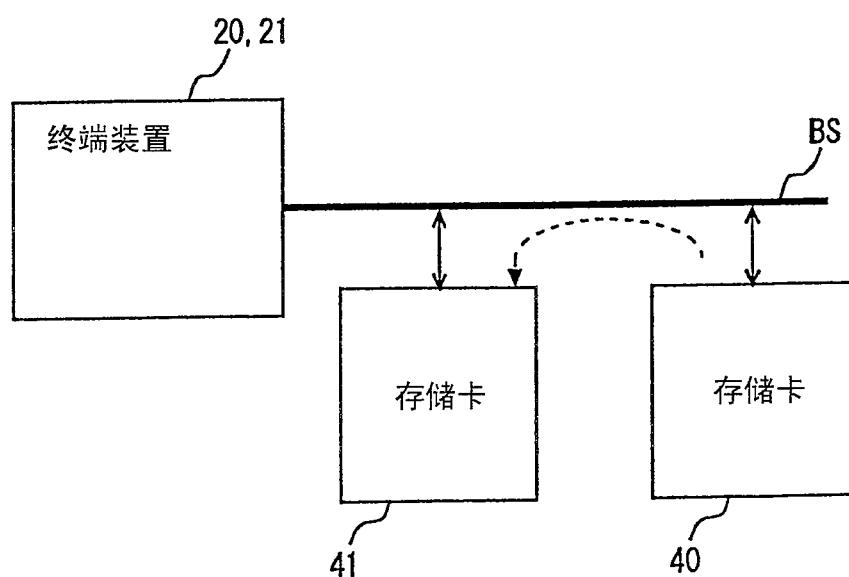


图 2

名称	记号	属性	特性
数据	Dc	数据固有	例：音乐数据、朗读数据、教材数据、图象数据、用内容密钥加密后的加密数据 E(Kc, Dc) 进行记录管理
数据信息	Di	数据固有	Dc 中付随的明文数据。包含 DID
数据 ID	DID	数据固有	用于确定数据以及内容密钥的管理编码
内容密钥	Kc	数据固有	对加密数据加密 / 解密的共同密钥
控制信息	AC	许可协议固有	关于播放和许可协议的处理的限制事项
许可 ID	LID	许可协议固有	用于确定许可协议的管理编码
许可协议	LIC	许可协议固有	Kc//AC//DID//LID的总称

图 3

名称	记号	特性
主密钥	Ka	用于制作类证书的加密密钥，由认证局管理
认证密钥	KPa	在认证局验证证书的公开解密密钥，由许可协议提供者管理
类公开加密密钥	KPcxy	分配给机器的种类（以种类为单位）的加密密钥。 x是识别机器的识别子，在播放装置中为 p，在存储中为 m，y 是识别类的识别子
类密码解密密钥	Kcxy	对用类公开加密密钥 KPcxy 加密的数据进行解密的非对称解密密钥。
类信息	Icxy	有关每个类的机器以及类公开加密密钥的信息数据
类证书	Cxy	KPcxy // Icxy // E(Ka, H(KPcxy // Icxy)) 由认证密钥可以确认其正当性
个别公开加密密钥	KPomz	针对每个存储装置具有固有的值的个别公开加密密钥， z是识别存储装置的识别子
个别密码解密密钥	Komz	对用个别公开加密密钥 KPomz 加密的数据进行解密 的非对称解密密钥。
会话密钥	Ks1w	每次接收许可协议时在许可协议发送源处产生的临时密钥， w是识别会话密钥产生的识别子
会话密钥	Ks2w	每次接收许可协议时在许可协议发送目标处产生的临时密钥， w是识别会话密钥产生的识别子

图 4

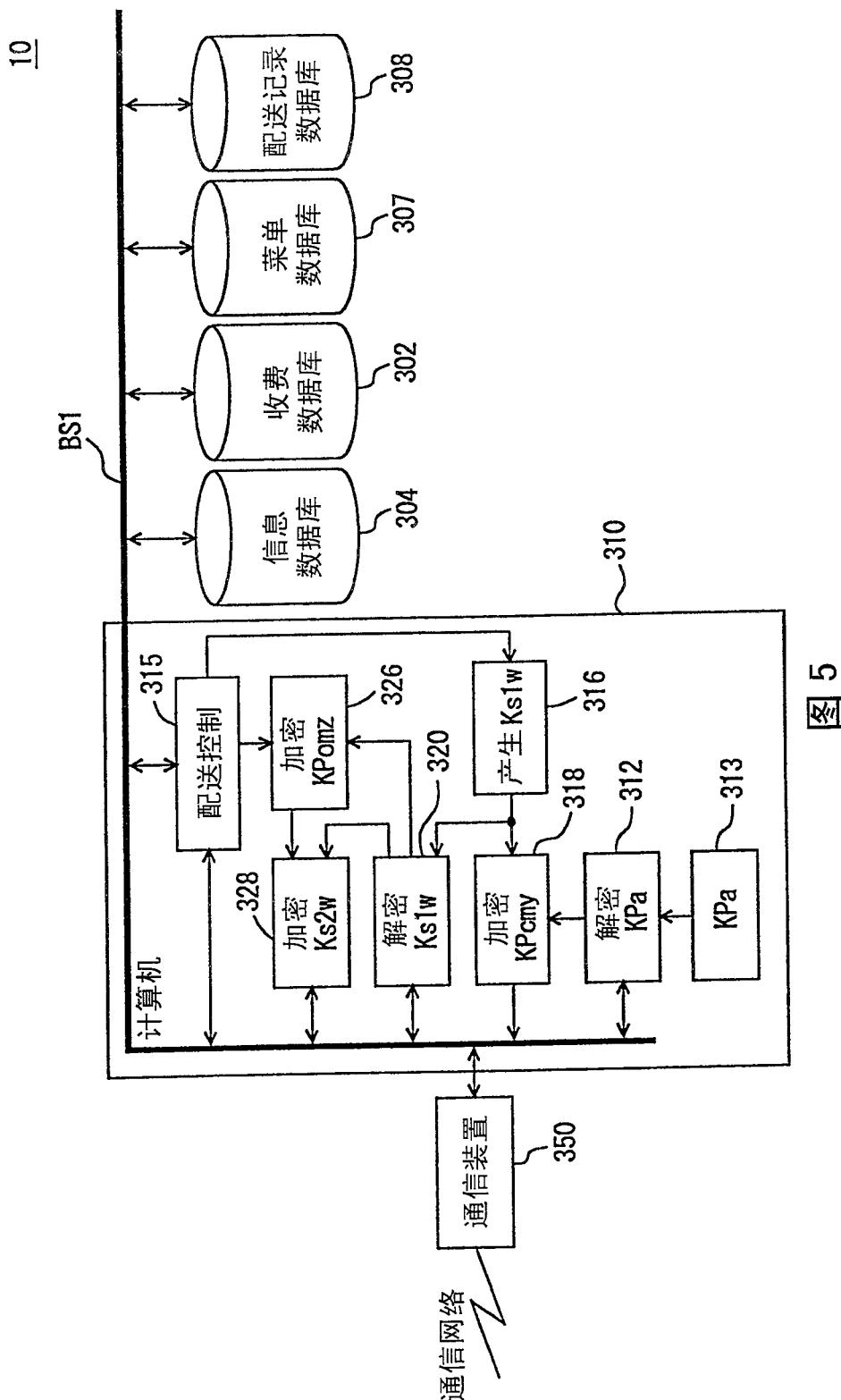


图 5

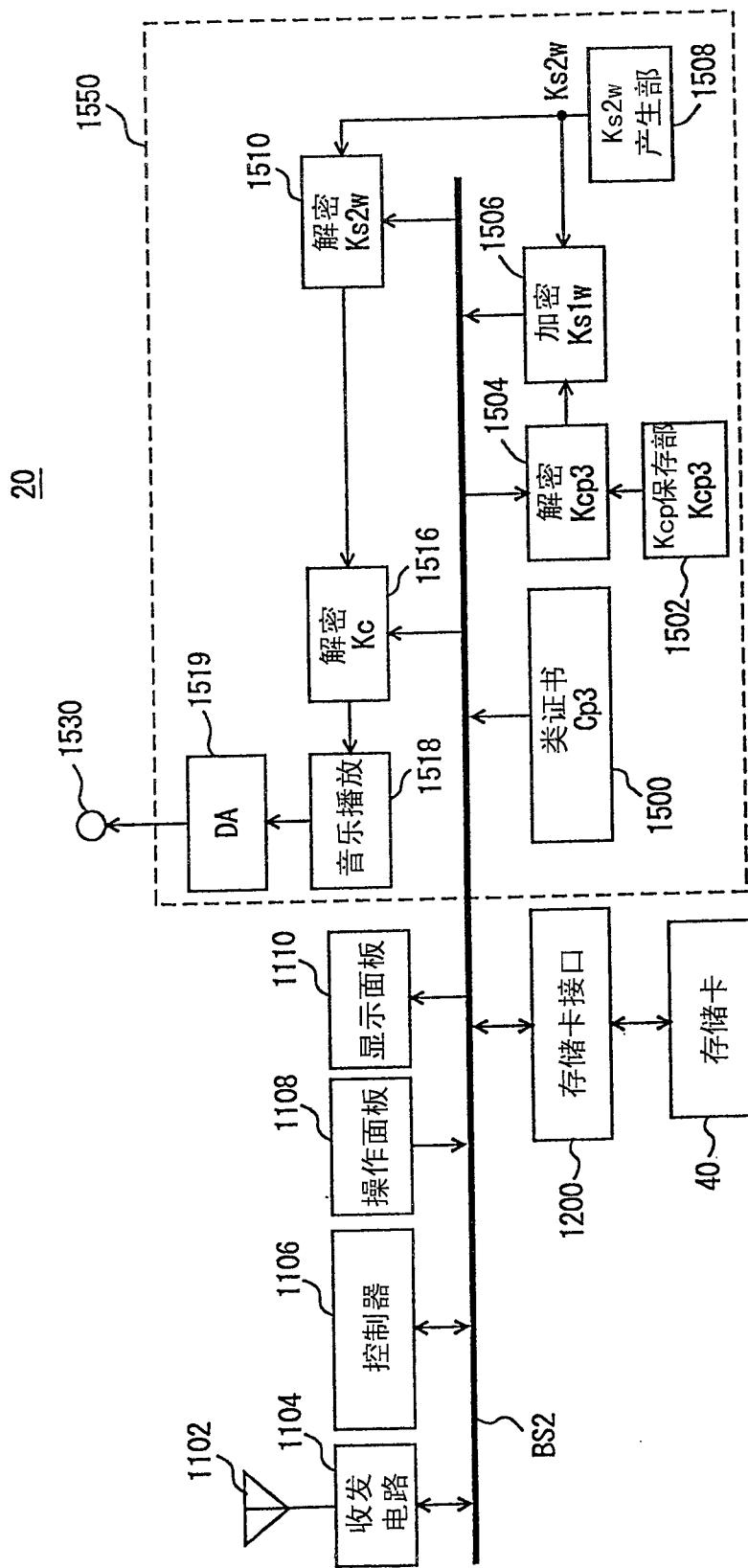


图 6

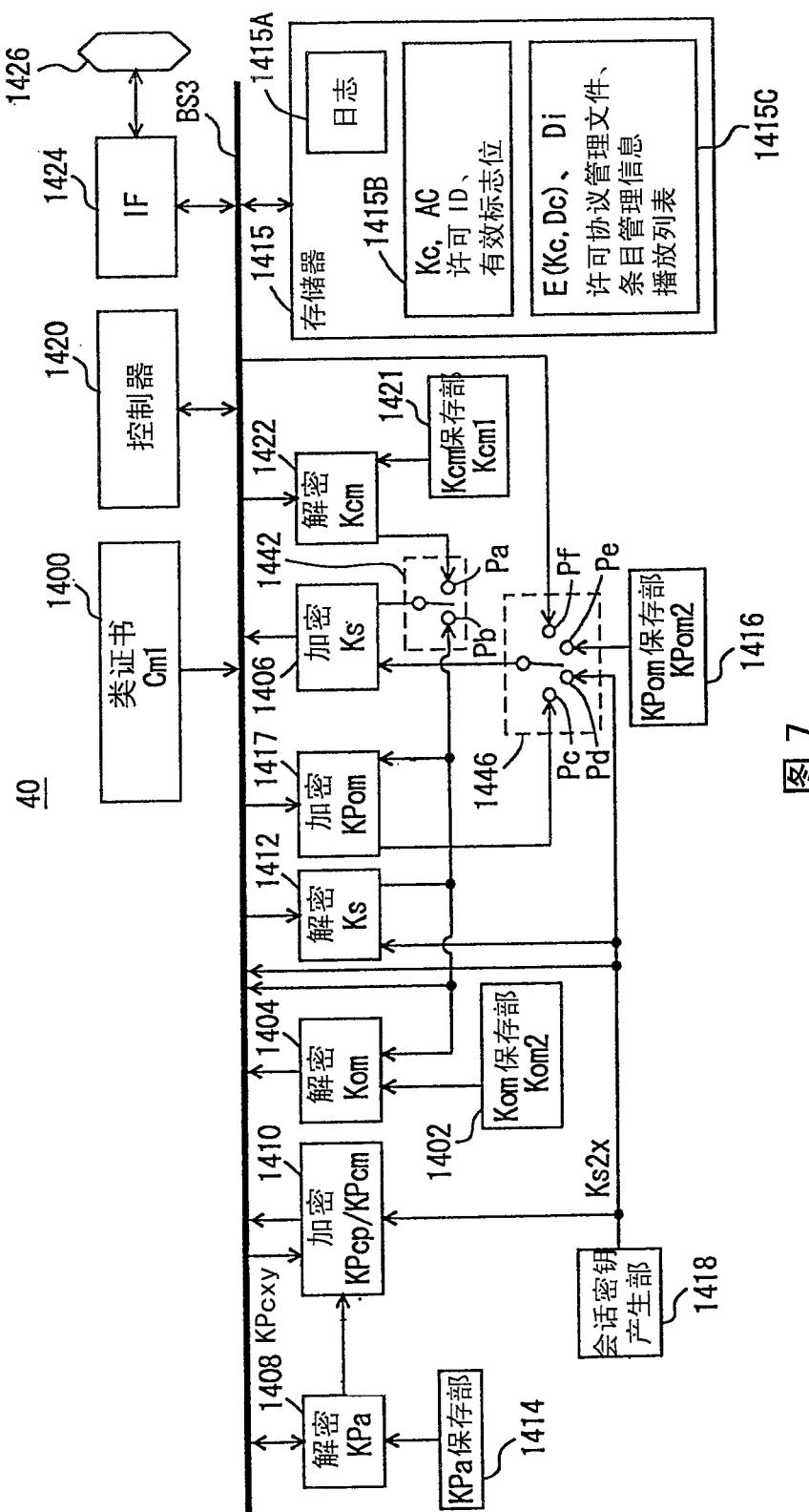
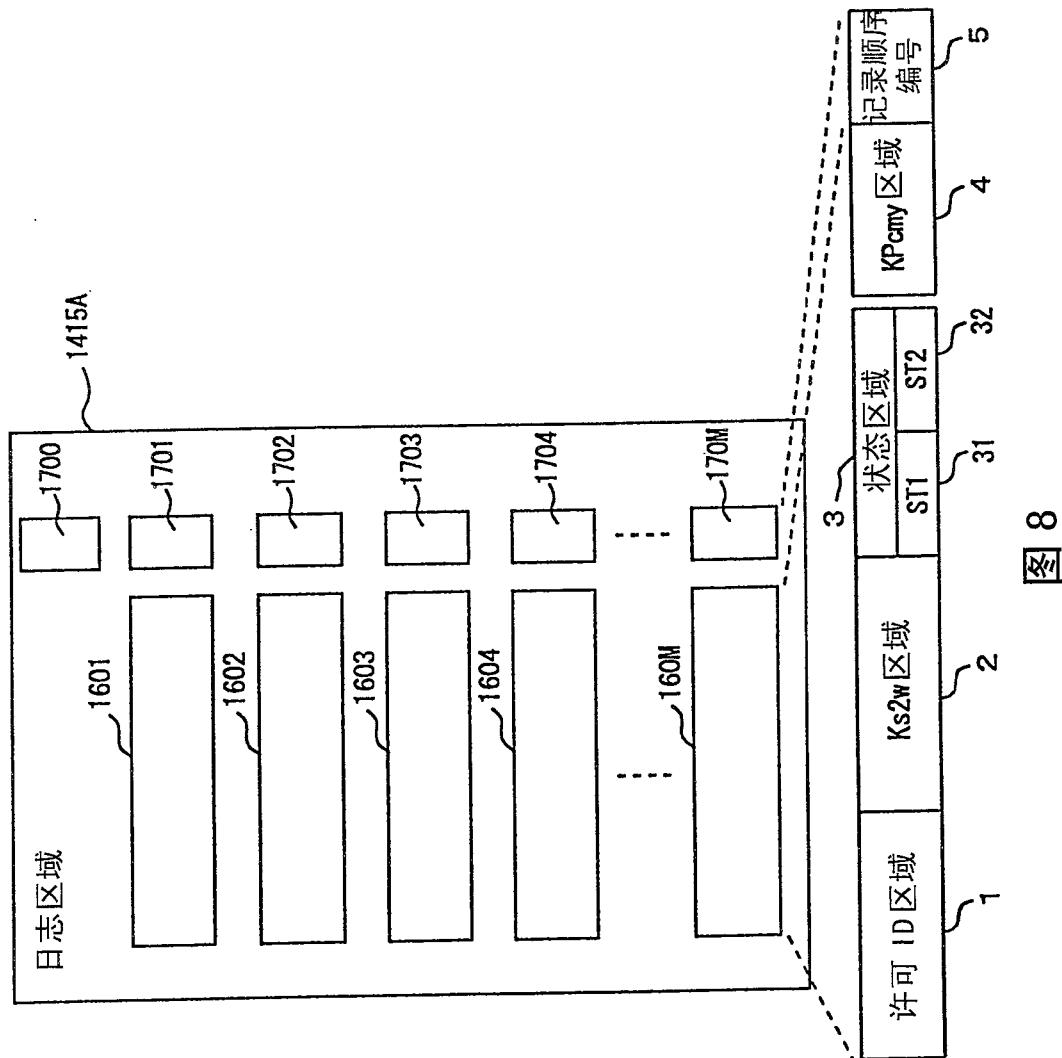


图 7



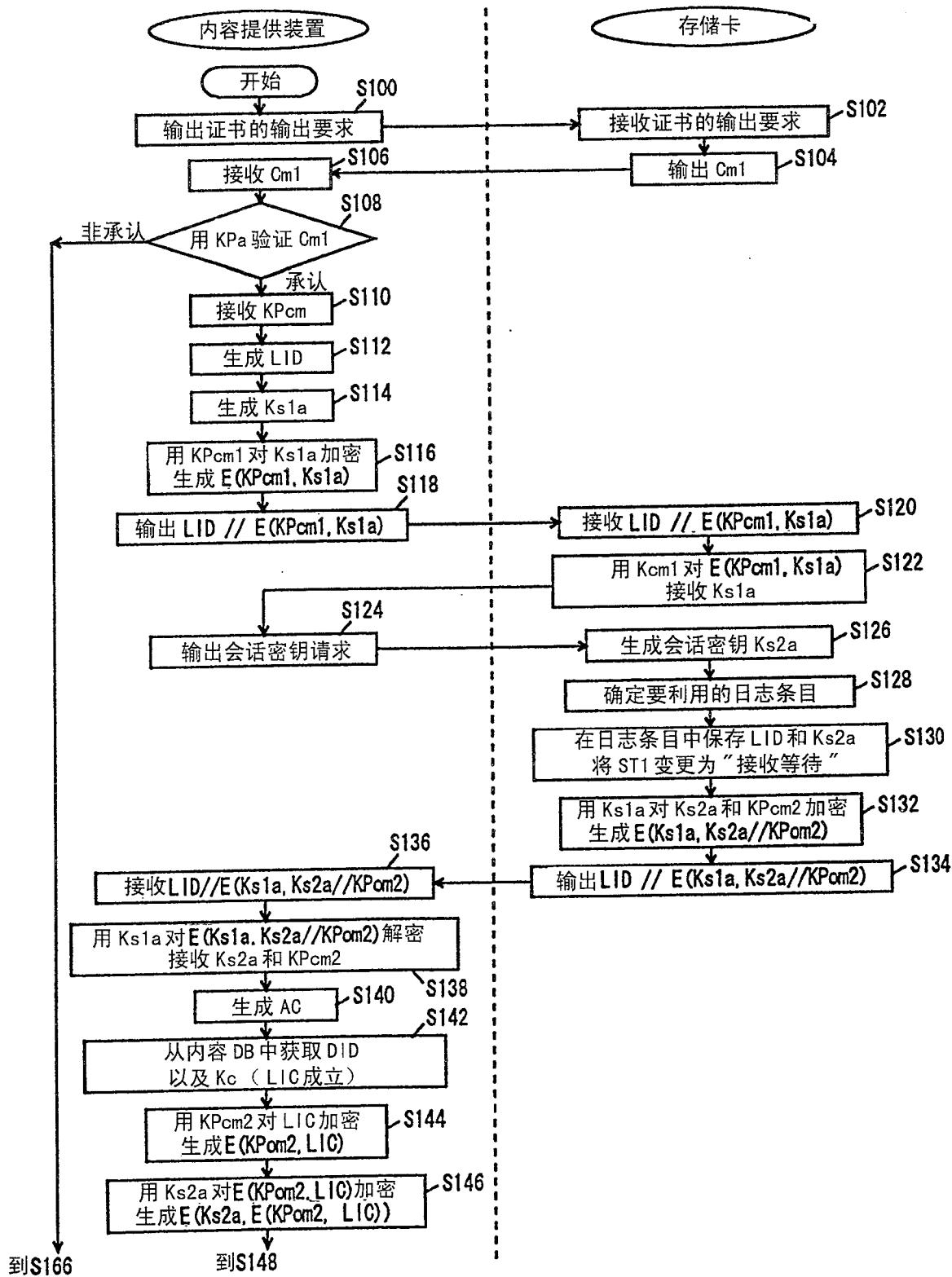


图 9

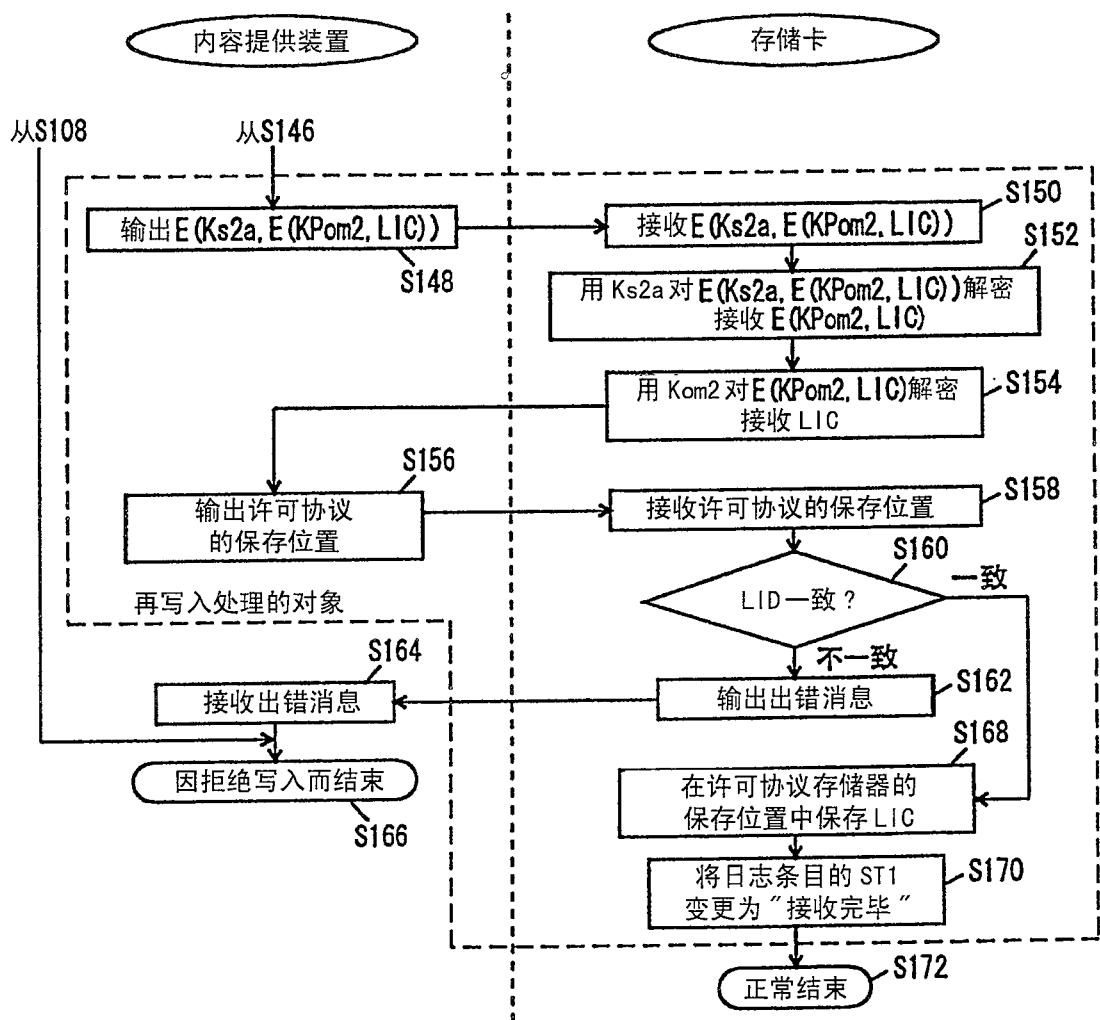


图 10

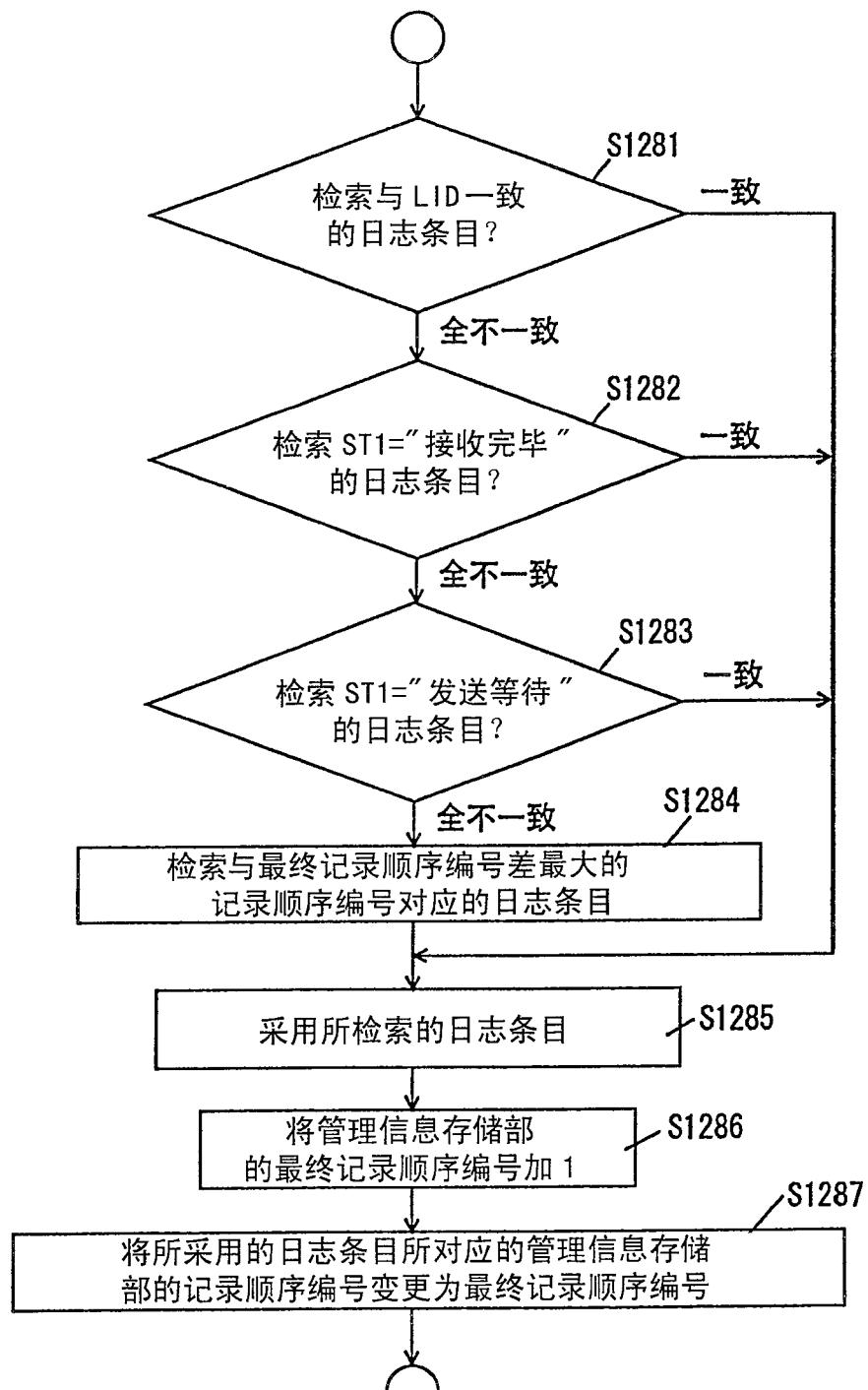


图 11

存储卡40

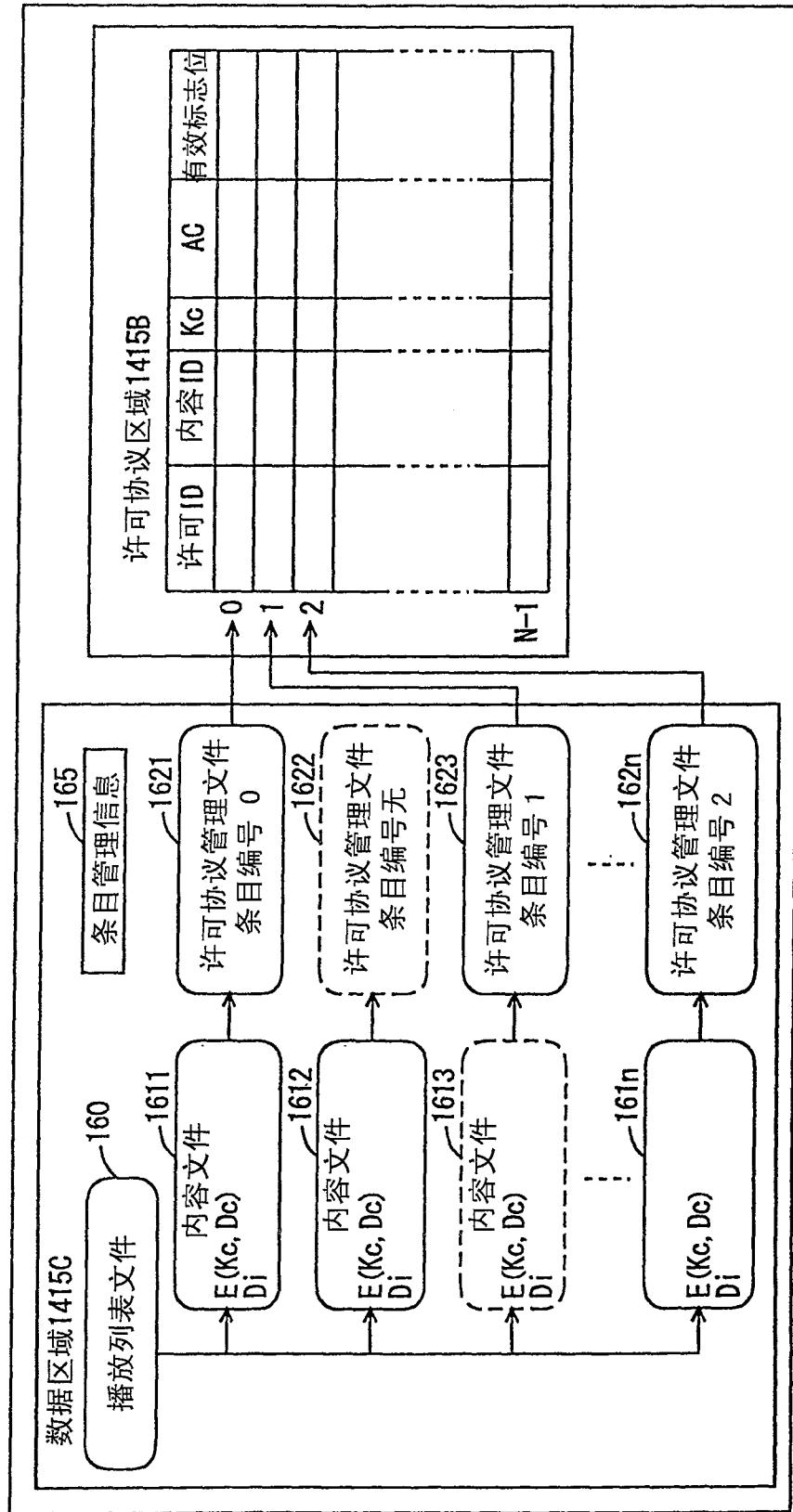
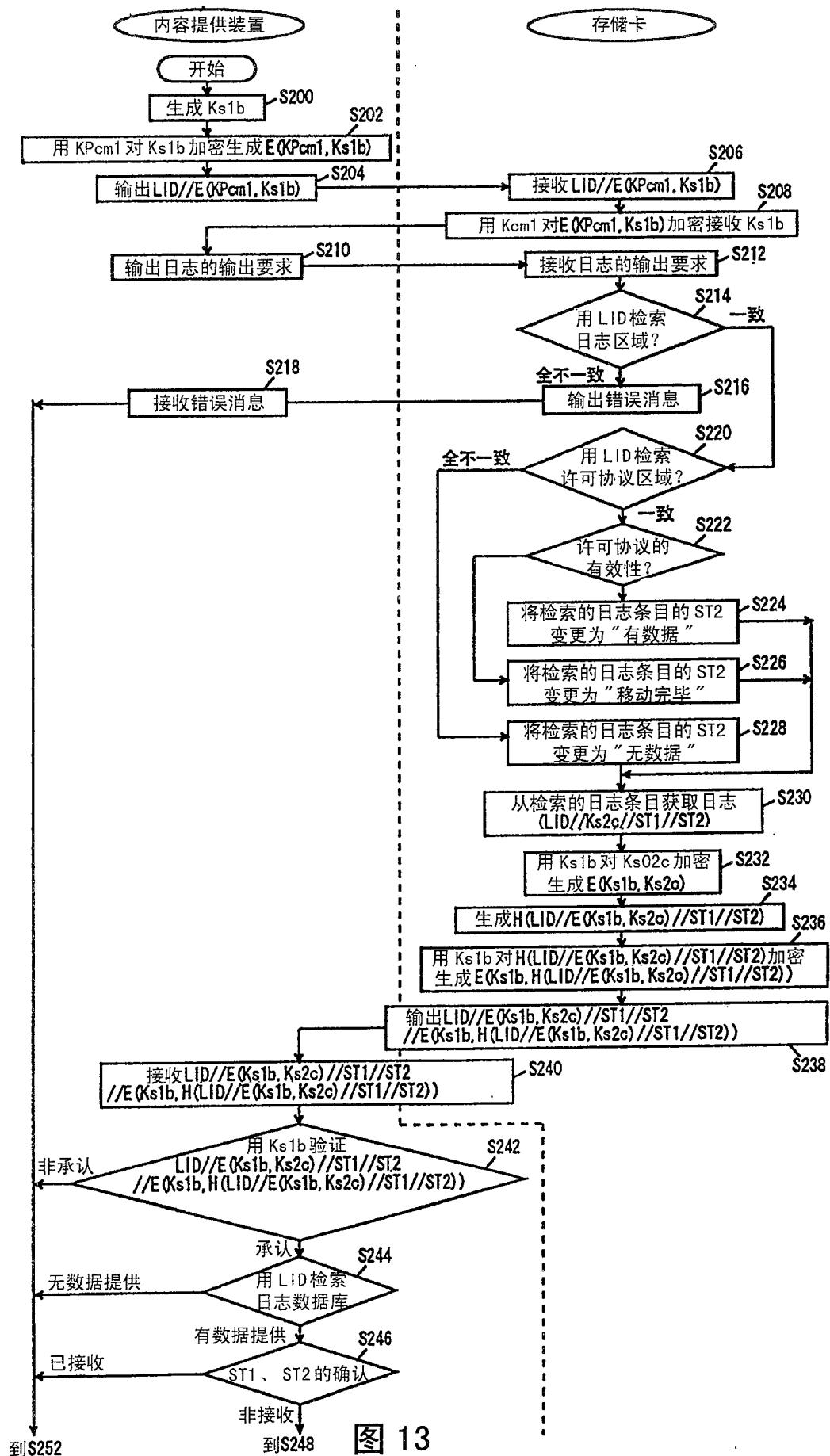


图 12



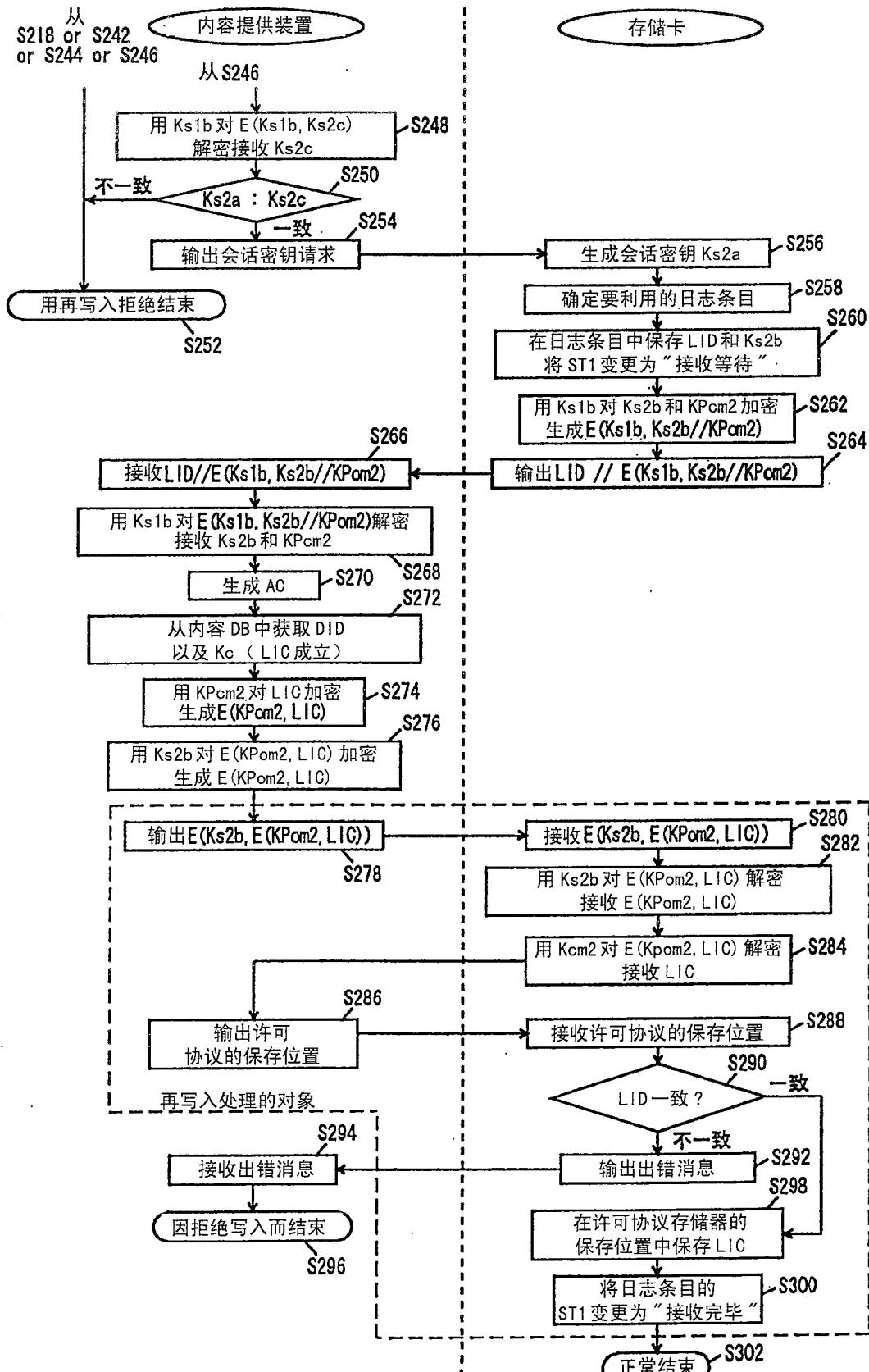


图 14

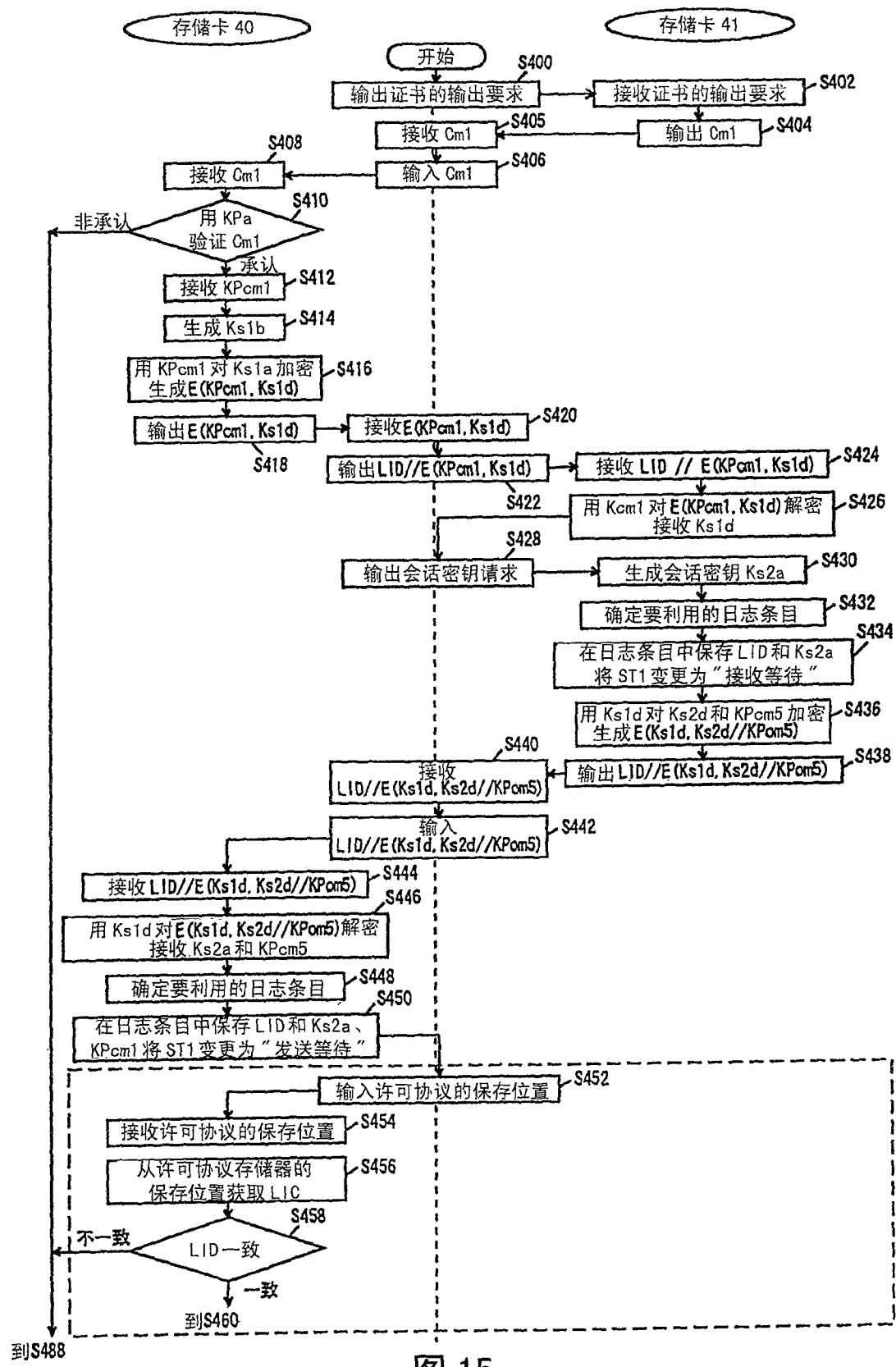


图 15

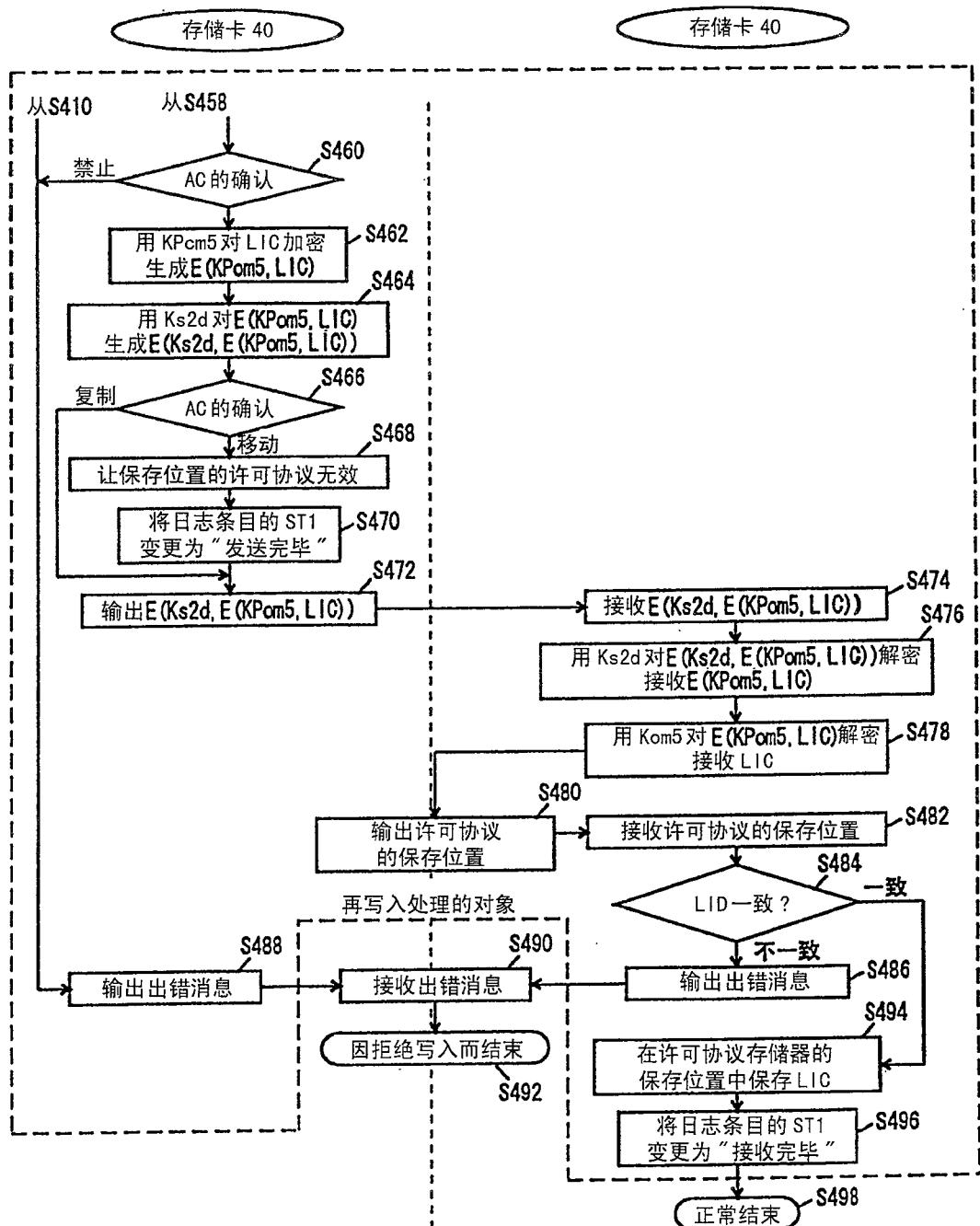


图 16

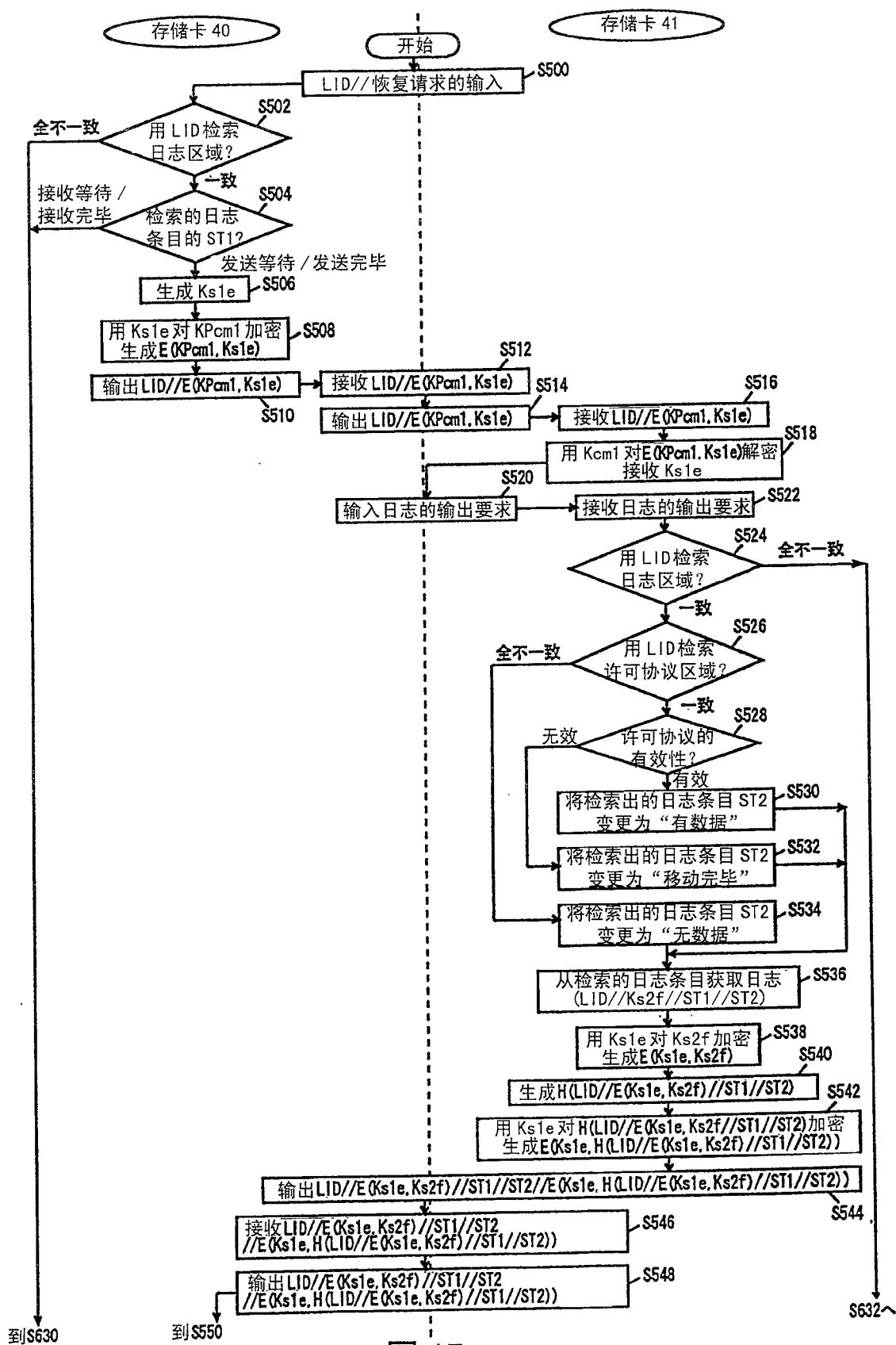


图 17

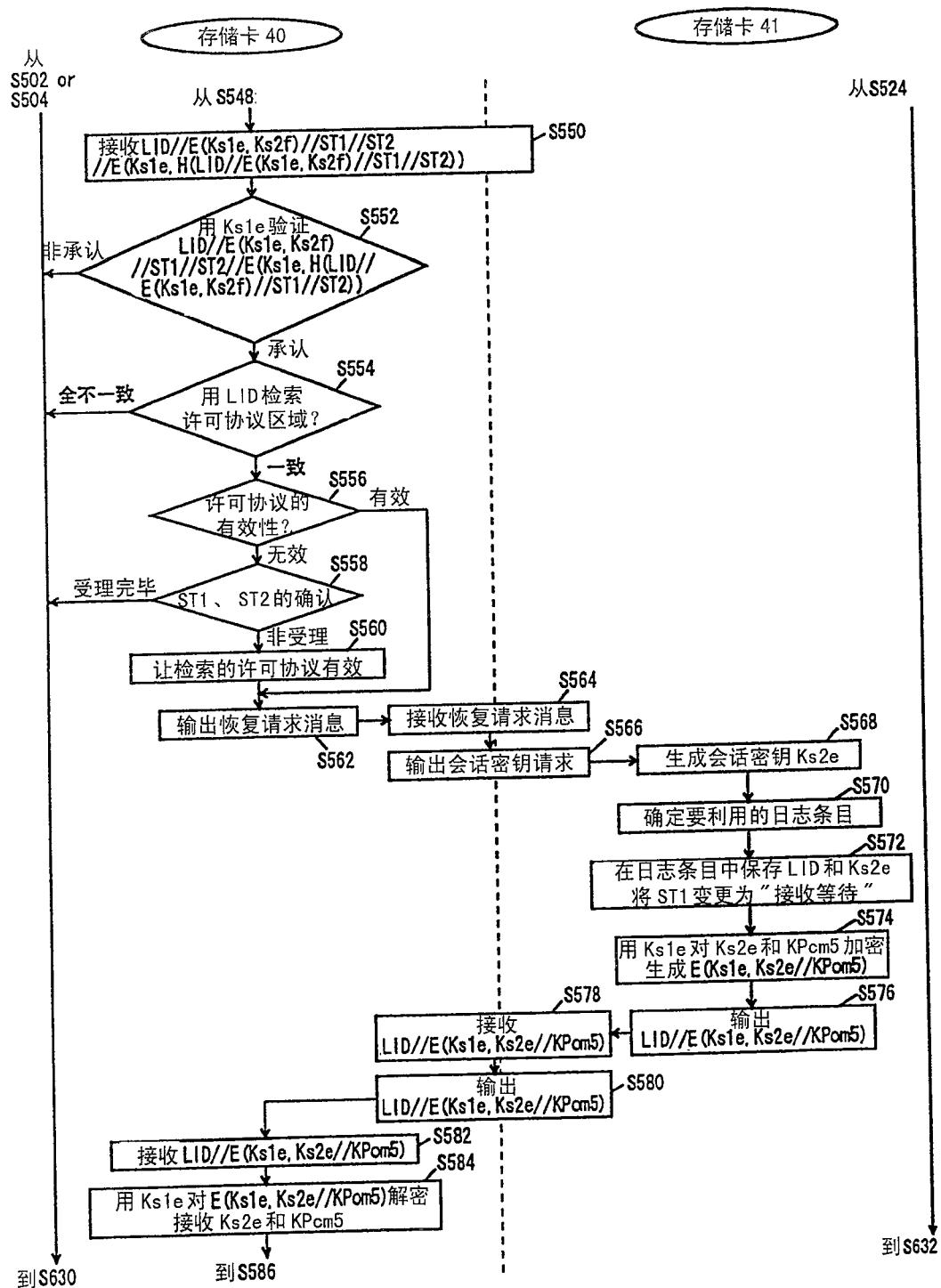


图 18

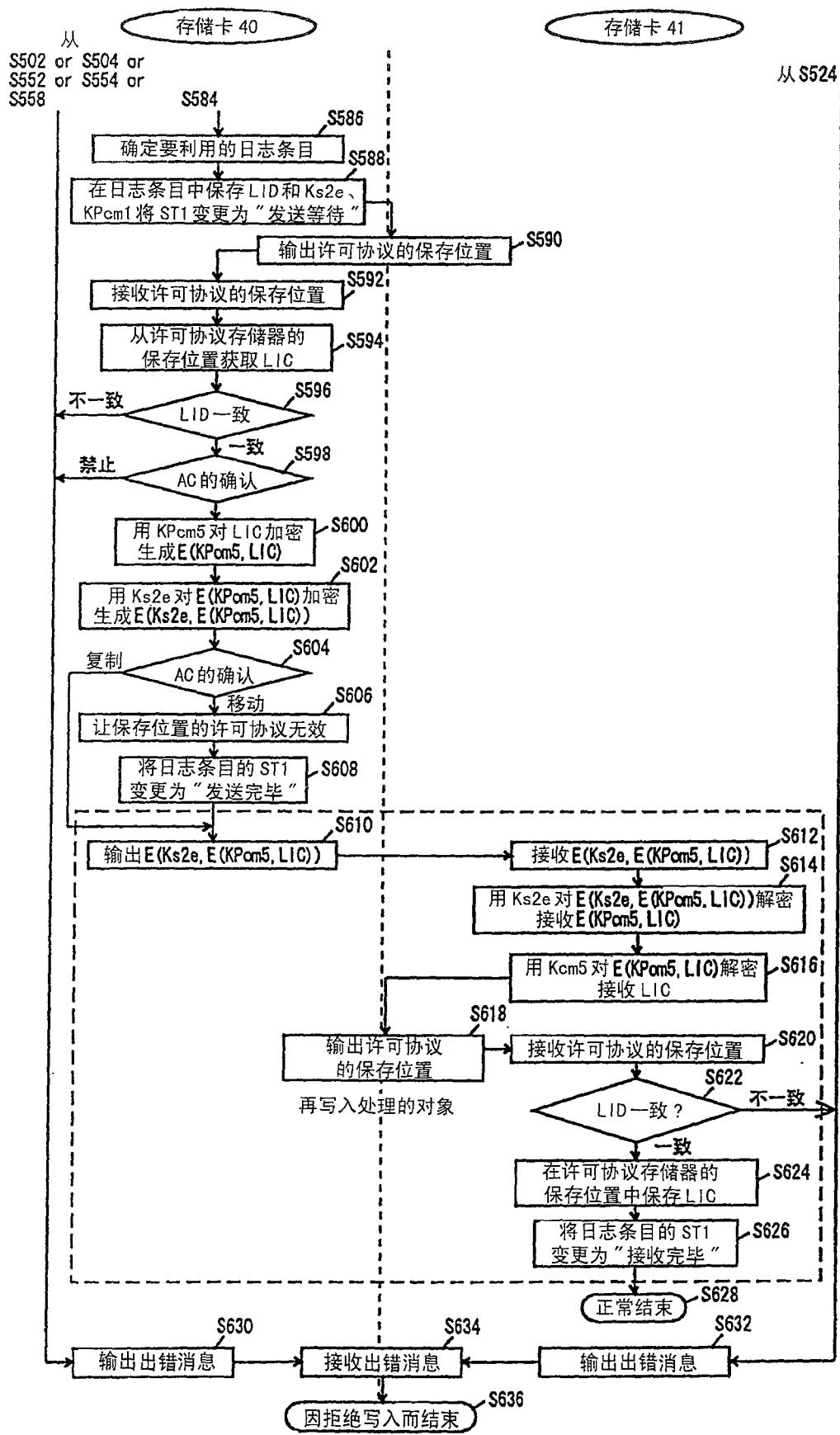


图 19

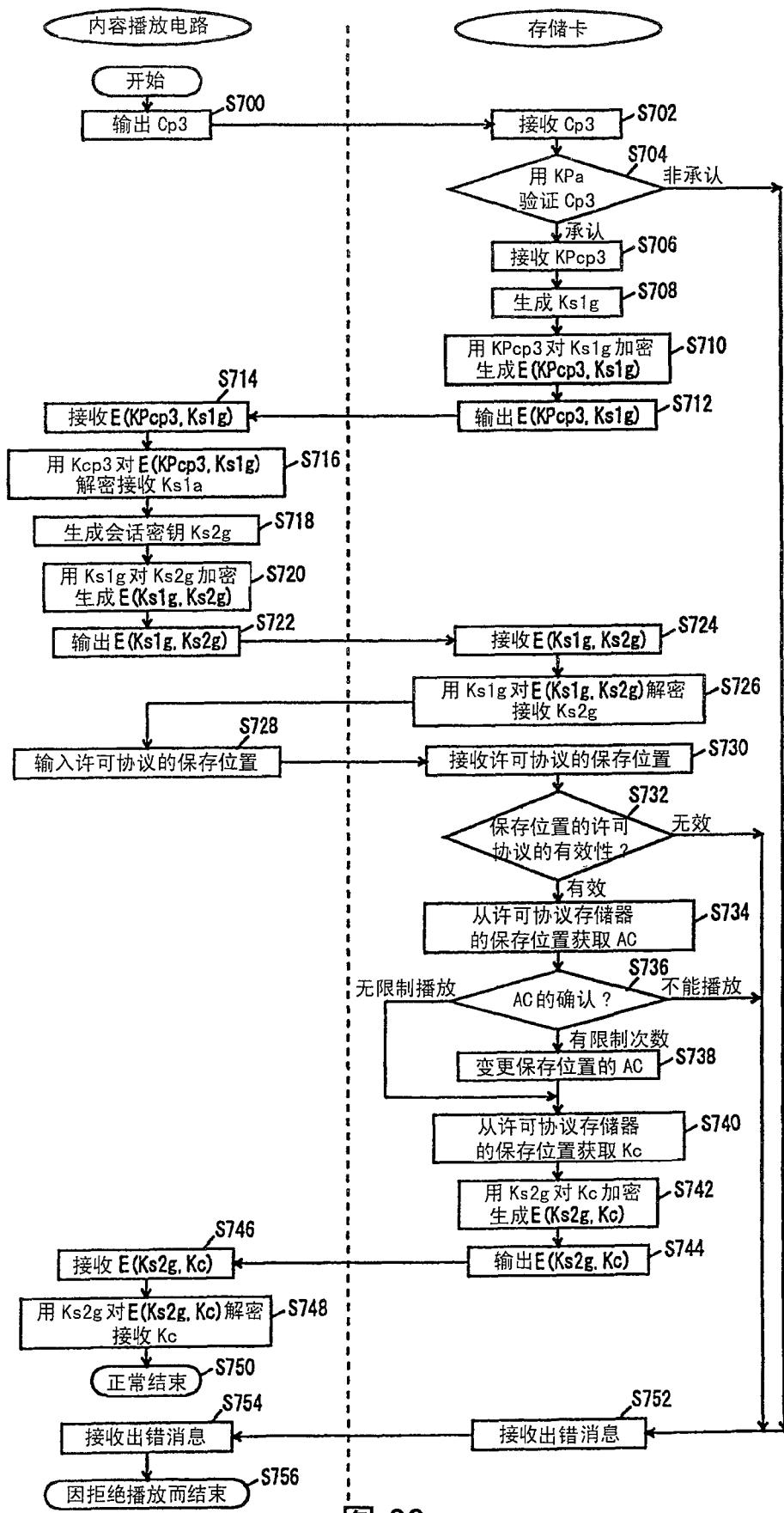


图 20