(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 102957686 A
(43)申请公布日 2013.03.06

(21)申请号 201210274516.6

(22)申请日 2012.08.03

(30)优先权数据
2011-175607 2011.08.11 JP

(71)申请人 索尼公司
地址 日本东京

(72)发明人 上田健二朗 久野浩 林隆道

(74)专利代理机构 中国国际贸易促进委员会专利商标事务所 11038
代理人 陈芳

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 9/32(2006.01)

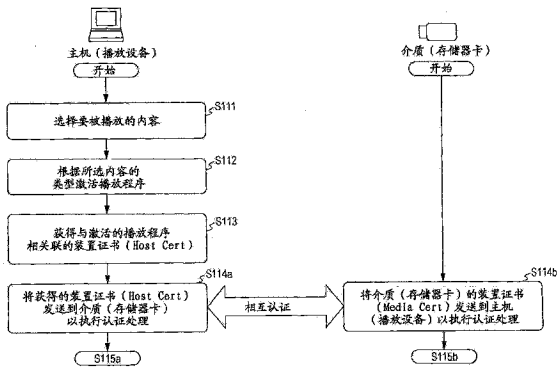
权利要求书 3 页 说明书 29 页 附图 23 页

(54)发明名称

信息处理装置和信息处理方法,以及程序

(57)摘要

本公开涉及信息处理装置和信息处理方法,以及程序。一种信息处理系统包括:介质,存储有要被播放的内容;以及播放设备,用于播放存储在所述介质中的内容,其中,所述播放设备被配置用来:判别被选作要被播放的对象的内容的内容类型,从存储单元选择性地获得与判别的内容类型相关联的装置证书,以及将选择性地获得的装置证书发送到所述介质;所述装置证书是关于内容类型的装置证书,其中记录有能够利用该装置证书的内容类型信息;并且,所述介质确定已经从所述播放设备对其执行了读取请求的加密密钥是否是用于解密与记录在所述装置证书中的可用内容类型匹配的加密内容的加密密钥,并仅在匹配的情况下允许读出该加密密钥。



CN 102957686 A

1. 一种信息处理系统，包括：

介质，存储有充当要被播放的对象的内容；以及

播放设备，被配置用来播放存储在所述介质中的内容，

其中，所述播放设备被配置用来

判别被选作要被播放的对象的内容的内容类型，

从存储单元选择性地获得与判别的内容类型相关联的装置证书，以及

将选择性地获得的装置证书发送到所述介质；

所述装置证书是关于内容类型的装置证书，其中记录有能够利用该装置证书的内容类型信息；并且

所述介质确定已经从所述播放设备对其执行了读取请求的加密密钥是否是用于解密与记录在所述装置证书中的可用内容类型匹配的加密内容的加密密钥，并仅在匹配的情况下允许读出该加密密钥。

2. 根据权利要求 1 所述的信息处理系统，其中，所述播放设备执行不依赖于内容类型的内容播放程序，并根据该内容播放程序判别被选作要被播放的对象的内容的类型。

3. 根据权利要求 1 所述的信息处理系统，其中，所述装置证书具有这样的结构：其中，高附加值内容和除高附加值内容以外的普通内容中的至少一个作为能够利用该装置证书的内容类型被记录；

并且，所述介质确定已经请求了从所述播放设备对其进行读取的加密密钥是否是用于解密与作为记录在所述装置证书中的可用内容类型的高附加值内容或普通内容相匹配的加密内容的加密密钥，并仅仅在匹配的情况下许可读出该加密密钥。

4. 根据权利要求 1 所述的信息处理系统，其中，所述播放设备发送获得的装置证书以执行认证处理；

并且，在将所述认证处理的成立作为条件的情况下，所述介质执行来自所述播放设备的加密密钥读出请求的许可确定处理。

5. 根据权利要求 1 所述的信息处理系统，其中，根据与被选作要被播放的对象的内容相关联的属性信息，所述播放设备判别选择的内容的类型，并从存储单元选择性地获得与判别的内容类型相关联的装置证书。

6. 根据权利要求 1 所述的信息处理系统，其中，所述介质将加密密钥存储在基于播放设备的访问特权的确认来许可对其进行访问的保护区域中，基于要从所述播放设备接收的装置证书中记录的保护区域访问特权信息来确认存储所述加密密钥的保护区域的访问特权，并在所述播放设备的访问特权被确认的情况下，许可由所述播放设备读出加密密钥。

7. 根据权利要求 1 所述的信息处理系统，其中，所述装置证书具有这样的结构：其中，记录有能够利用该装置证书的播放设备类型信息；

所述介质根据编码算法执行作为所述介质的标识信息的介质 ID 的编码处理以发送到所述播放设备，所述编码算法是根据所述装置证书中记录的播放设备类型信息来选择的；并且

所述播放设备执行伴随着应用了介质 ID 的数据处理的内容的解码或播放，该介质 ID 是通过根据与该设备本身的装置类型相对应的解码算法对从所述介质接收的编码介质 ID 进行解码而获得的。

8. 一种信息处理装置，包括：

数据处理单元，被配置用来执行存储在介质中的内容的读出和重放处理；

其中，所述数据处理单元被配置用来

判别被选作要被播放的对象的内容的内容类型，

选择性地获得与判别的内容类型相关联的装置证书，以将选择性地获得的装置证书发送到所述介质，并且还

将加密内容以及要被应用于该加密内容的解密的加密密钥的读出请求输出到所述介质，并且

在以通过所述介质进行确认为条件的情况下，从所述介质获得加密密钥，以通过对加密内容应用获得的加密密钥来执行该加密内容的解密，其中，已经对其执行了读出请求的加密密钥是与记录在所述装置证书中的能够使用的内容类型相匹配的内容的加密密钥。

9. 根据权利要求 8 所述的信息处理装置，其中，所述数据处理单元执行不依赖于内容类型的内容播放程序，并根据该内容播放程序判别被选作要被播放的对象的内容的类型。

10. 根据权利要求 8 所述的信息处理装置，其中，所述装置证书具有这样的结构：其中，高附加值内容和除高附加值内容以外的普通内容中的至少一个作为能够利用该装置证书的内容类型被记录。

11. 根据权利要求 8 所述的信息处理装置，其中，所述数据处理单元将获得的装置证书发送到所述介质以执行认证处理。

12. 根据权利要求 8 所述的信息处理装置，其中，所述数据处理单元根据与被选作要被播放的对象的内容相关联的属性信息来判别选择的内容的类型。

13. 根据权利要求 8 所述的信息处理装置，其中，所述装置证书具有这样的结构：其中，记录有能够利用该装置证书的播放设备类型信息；

所述介质根据编码算法执行作为所述介质的标识信息的介质 ID 的编码处理，以发送到所述信息处理装置，所述编码算法是根据所述装置证书中记录的播放设备类型信息来选择的；并且

伴随着应用了介质 ID 的数据处理，所述信息处理装置的数据处理单元执行内容的解码或播放，该介质 ID 是通过根据与该设备本身的装置类型相对应的解码算法对从所述介质接收的编码介质 ID 进行解码而获得的。

14. 一种要在信息处理系统中执行的信息处理方法，该信息处理系统具有：

介质，存储有充当要被播放的对象的内容；以及

播放设备，被配置用来播放存储在所述介质中的内容，其中，所述播放设备被配置用来

判别被选作要被播放的对象的内容的内容类型，

从存储单元选择性地获得与判别的内容类型相关联的装置证书，以将选择性地获得的装置证书发送到所述介质；

所述装置证书是记录有能够利用该装置证书的内容类型信息的装置证书；并且

所述介质确定已经从所述播放设备对其执行了读取请求的加密密钥是否是用于解密与记录在所述装置证书中的可用内容类型匹配的加密内容的加密密钥，并仅在匹配的情况下允许读出该加密密钥。

15. 一种要在信息处理装置中执行的信息处理方法，其中，数据处理单元被配置用来

判别被选作要被播放的对象的内容的内容类型，

从存储单元选择性地获得与判别的内容类型相关联的装置证书，以将选择性地获得的装置证书发送到所述介质，并且还

将加密内容以及要被应用于该加密内容的解密的加密密钥的读出请求输出到所述介质，并且

在以通过所述介质进行确认为条件的情况下，从所述介质获得加密密钥，以通过对加密内容应用获得的加密密钥来执行该加密内容的解密，其中，已经对其执行了读出请求的加密密钥是与记录在所述装置证书中的能够使用的内容类型相匹配的内容的加密密钥。

16. 一种程序，使得信息处理装置执行信息处理，并且使得数据处理单元

判别被选作要被播放的对象的内容的内容类型，

从存储单元选择性地获得与判别的内容类型相关联的装置证书，以将选择性地获得的装置证书发送到所述介质，并且还

将加密内容以及要被应用于该加密内容的解密的加密密钥的读出请求输出到所述介质，并且

在以通过所述介质进行确认为条件的情况下，从所述介质获得加密密钥，以通过对加密内容应用获得的加密密钥来执行该加密内容的解密，其中，已经对其执行了读出请求的加密密钥是与记录在所述装置证书中的能够使用的内容类型相匹配的内容的加密密钥。

信息处理装置和信息处理方法，以及程序

技术领域

[0001] 本公开涉及信息处理装置和信息处理方法，以及程序，具体地涉及有效地防止对记录在诸如存储器卡等之类的记录介质中的内容的未授权使用的信息处理装置和信息处理方法，以及程序。

背景技术

[0002] 近来，诸如 DVD（数字多功能盘）、蓝光盘（Blu-ray Disc，注册商标）、闪存等的各种介质已经被用作信息记录介质。特别地，近来，诸如具有大容量闪存的 USB 存储器的存储器卡的使用已经变得普及。通过将诸如音乐、电影等内容记录在这样的各种信息记录介质中并将其安装在播放设备（播放器）上，用户可以执行内容的播放。

[0003] 但是，对于诸如音乐数据、图像数据等的很多内容，版权和发行权等由其作者或销售者拥有。因此，在将内容提供给用户的情况中，通常提供一定的使用限制，即，执行控制以便仅许可具有合法的使用权的用户使用该内容，并防止在未经允许的情况下诸如复制等的无节制的使用。

[0004] 例如，AACS（高级访问内容系统）已经作为与内容的使用控制有关的标准被使用。例如，AACS 的标准定义了关于蓝光盘（Blu-ray Disc，注册商标）的记录内容的使用控制配置。具体地说，例如，AACS 的标准规定了这样的算法，该算法用于将要记录在蓝光盘（Blu-ray Disc，注册商标）中的内容作为加密内容，并使得可以获得其加密密钥的用户能够被限制为常规用户，等等。

[0005] 但是，就当前的 AACS 规定而言，尽管存在与关于诸如蓝光盘（Blu-ray Disc，注册商标）等的盘记录内容的使用控制配置有关的规定，但是，例如，没有与要记录在诸如存储器卡等的闪存中的内容有关的足够的规定。因此，关于在这样的存储器卡中的记录内容，对版权的保护可能是不够的，从而，已经要求建立与使用诸如存储器卡等的介质的内容使用有关的使用控制配置。

[0006] 例如，就 AACS 规定而言，存在关于诸如蓝光盘（Blu-ray Disc，注册商标）等的盘记录内容的使用控制配置的如下规定。

[0007] （a）关于从已经记录有内容的介质（例如，ROM 盘）复制到诸如蓝光盘（Blu-ray Disc，注册商标）的盘的内容的使用规定

[0008] （b）关于从服务器下载并记录到诸如蓝光盘（Blu-ray Disc，注册商标）的盘中的内容的使用规定

[0009] 例如，这些内容的使用控制被规定。

[0010] 就 AACS 而言，例如，在上述（a）中在介质之间执行内容的复制的情况中，规定了以从管理服务器获得复制许可信息作为条件的管理复制（MC：管理复制）。

[0011] 此外，作为在上述（b）中从服务器下载内容的处理，就 AACS 而言，规定了各种类型的下载模式，例如使用诸如 PC 等用户装置的 EST（电子销售（Electric Sell Through））、使用安装在便利店等中的共享终端的 MoD（按需制造），并且在通过这些模式的每一种下载

处理将内容记录在盘中并使用该内容的情况中，需要根据预先确定的规则来执行处理。例如，请注意，这些处理在日本未审专利申请公开 No. 2008-98765 中进行了描述。

[0012] 但是，如上所述，就 AACS 规定而言，存在一个问题，其中，这些规定假定执行诸如蓝光盘（Blu-ray Disc，注册商标）等的盘记录内容的使用控制，并且没有与关于在诸如包括 USB 存储器等的闪存类型的存储器卡中记录的内容的足够的使用控制有关的规范。

发明内容

[0013] 已经发现，希望提供在诸如闪存等的信息记录介质中记录内容并使用其来防止对内容的未授权使用的情况中建立使用控制配置的信息处理装置和信息处理方法，以及程序。

[0014] 根据本公开的实施例，一种信息处理系统包括：介质，存储有充当要被播放的对象的内容；以及播放设备，被配置用来播放存储在该介质中的内容，其中，该播放设备被配置用来：判别被选作要被播放的对象的内容的内容类型，从存储单元选择性地获得与判别的内容类型相关联的装置证书，并将选择性地获得的装置证书发送到该介质；该装置证书是关于内容类型的装置证书，其中记录有可以利用该装置证书的内容类型信息；并且，该介质确定已经从播放设备对其执行了读取请求的加密密钥是否是用于解密与记录在装置证书中的可用内容类型匹配的加密内容的加密密钥，并仅在匹配的情况下允许读出该加密密钥。

[0015] 此外，在根据本公开的信息处理系统的实施例中，该播放设备执行不依赖于内容类型的内容播放程序，并根据该内容播放程序判别被选作要被播放的对象的内容的类型。

[0016] 此外，在根据本公开的信息处理系统的实施例中，该装置证书具有这样的结构：其中，高附加值内容和除高附加值内容以外的普通内容中的至少一个作为可以利用该装置证书的内容类型被记录；其中，该介质确定已经请求了从该播放设备对其进行读取的加密密钥是否是用于解密与作为记录在装置证书中的可用内容类型的高附加值内容或普通内容相匹配的加密内容的加密密钥，并仅在匹配的情况下许可读出该加密密钥。

[0017] 此外，在根据本公开的信息处理系统的实施例中，该播放设备发送获得的装置证书以执行认证处理；其中，在将认证处理的成立作为条件的情况下，该介质执行来自该播放设备的加密密钥读出请求的许可确定处理。

[0018] 此外，在根据本公开的信息处理系统的实施例中，根据与被选作要被播放的对象的内容相关联的属性信息，该播放设备判别选择的内容的类型，并从存储单元选择性地获得与判别的内容类型相关联的装置证书。

[0019] 此外，在根据本公开的信息处理系统的实施例中，该介质将加密密钥存储在基于该播放设备的访问特权的确认来许可对其进行访问的保护区域中，基于要从播放设备接收的装置证书中记录的保护区域访问特权信息来确认存储加密密钥的保护区域的访问特权，并在该播放设备的访问特权被确认的情况下，许可由该播放设备读出加密密钥。

[0020] 此外，在根据本公开的信息处理系统的实施例中，该装置证书具有记录有可以利用该装置证书的播放设备类型信息的结构；其中，该介质根据编码算法执行作为该介质的标识信息的介质 ID 的编码处理，以发送到该播放设备，该编码算法是根据装置证书中记录的播放设备类型信息来选择的；并且，该播放设备执行伴随着应用了介质 ID 的数据处理的

内容的解码或播放，该介质 ID 是通过根据与该设备本身的装置类型相对应的解码算法对从该介质接收的编码介质 ID 进行解码而获得的。

[0021] 根据本公开的实施例，一种信息处理装置包括数据处理单元，该数据处理单元被配置用来执行存储在介质中的内容的读出和重放处理；其中，所述数据处理单元被配置用来：判别被选作要被播放的对象的内容的内容类型，选择性地获得与判别的内容类型相关联的装置证书，以将选择性地获得的装置证书发送到所述介质，并且还将加密内容以及要被应用于该加密内容的解密的加密密钥的读出请求输出到所述介质，并且在以通过所述介质进行确认为条件的情况下，从所述介质获得加密密钥，以通过对加密内容应用获得的加密密钥来执行该加密内容的解密，其中，已经对其执行了读出请求的加密密钥是与记录在所述装置证书中的能够使用的内容类型相匹配的内容的加密密钥。

[0022] 此外，在根据本公开的信息处理装置的实施例中，该数据处理单元执行不依赖于内容类型的内容播放程序，并根据该内容播放程序判别被选作要被播放的对象的内容的类型。

[0023] 此外，在根据本公开的信息处理装置的实施例中，该装置证书具有这样的结构：其中，高附加值内容和除高附加值内容以外的普通内容中的至少一个作为可以利用该装置证书的内容类型被记录。

[0024] 此外，在根据本公开的信息处理装置的实施例中，该数据处理单元将获得的装置证书发送到该介质以执行认证处理。

[0025] 此外，在根据本公开的信息处理装置的实施例中，该数据处理单元根据与被选作要被播放的对象的内容相关联的属性信息来判别选择的内容的类型。

[0026] 此外，在根据本公开的信息处理装置的实施例中，该装置证书具有记录有可以利用该装置证书的播放设备类型信息的结构；其中，该介质根据编码算法执行作为标识信息的介质 ID 的编码处理，以发送到该信息处理装置，该编码算法是根据装置证书中记录的播放设备类型信息来选择的；并且，该信息处理装置的数据处理单元执行伴随着应用了介质 ID 的数据处理的内容的解码或播放，该介质 ID 是通过根据与该设备本身的装置类型相对应的解码算法对从该介质接收的编码介质 ID 进行解码而获得的。

[0027] 本公开的实施例是要在信息处理系统中执行的信息处理方法，该信息处理系统具有存储有充当要被播放的对象的内容的介质以及播放设备，该播放设备被配置用来播放存储在该介质中的内容，其中，该播放设备被配置用来：判别被选作要被播放的对象的内容的内容类型，以及选择性地从存储单元获得与该判别的内容类型相关联的装置证书以将选择性地获得的装置证书发送到该介质；该装置证书是记录有可以利用该装置证书的内容类型信息的装置证书；并且，该介质确定已经从播放设备对其执行了读取请求的加密密钥是否是用于解密与记录在装置证书中的可用内容类型匹配的加密内容的加密密钥，并仅在匹配的情况下允许读出该加密密钥。

[0028] 本公开的实施例是要在信息处理装置中执行的信息处理方法，其中，数据处理单元被配置用来：判别被选作要被播放的对象的内容的内容类型，选择性地从存储单元获得与该判别的内容类型相关联的装置证书以将选择性地获得的装置证书发送到该介质，还将加密内容以及要被应用于该加密内容的解密的加密密钥的读出请求输出到该介质，并且在以通过该介质进行确认为条件的情况下从该介质获得加密密钥，以通过对加密内容应用获

得的加密密钥来执行该加密内容的解密，其中，已经对其执行了读出请求的加密密钥是与记录在装置证书中的可以使用的内容类型相匹配的内容的加密密钥。

[0029] 本公开的实施例是一种程序，该程序使得信息处理装置执行信息处理，并使得数据处理单元：判别被选作要被播放的对象的内容的内容类型，选择性地从存储单元获得与该判别的内容类型相关联的装置证书以将选择性地获得的装置证书发送到该介质，还将加密内容以及要被应用于该加密内容的解密的加密密钥的读出请求输出到该介质，并且在以通过该介质进行确认为条件的情况下从该介质获得加密密钥，以通过对加密内容应用获得的加密密钥来执行该加密内容的解密，其中，已经对其执行了读出请求的加密密钥是与记录在装置证书中的可以使用的内容类型相匹配的内容的加密密钥。

[0030] 请注意，根据本公开的程序是例如可以使用存储介质或通信介质提供的程序，以便以与可以执行各种程序代码的信息处理装置或计算机系统有关的计算机可读取格式来提供。这样的程序以计算机可读取格式来提供，并且，因此，实现与在该信息处理装置或计算机系统之上的该程序相对应的处理。

[0031] 根据稍后描述的本公开的实施例和附图，本公开的进一步的目的、特征和优点将变得显而易见。请注意，在本说明书中使用的系统是多个装置的逻辑组配置，并且不限于每一个部件装置都在同一壳体之内。

[0032] 根据本公开的实施例，实现与存储在介质中的内容的内容类型相对应的内容使用控制。

[0033] 具体地说，播放设备根据内容的类型保持对应于可用内容类型的装置证书，该内容的类型为，例如，诸如高附加值内容和除了高附加值内容以外的普通内容的内容类型，该高附加值内容为诸如向公众发布不久的电影。该播放设备判别由用户选择的要被播放的内容的类型，并根据该判别的内容类型获得对应于其内容类型的装置证书，以发送到该介质。该介质确认记录在该装置证书中的对应的内容类型信息，并且只有在由该播放设备请求的作为加密密钥的标题密钥对应于与记录在装置证书中的对应内容类型匹配的内容的情况下，才许可标题密钥的读出。

[0034] 根据这些处理，可以执行与内容类型相应的标题密钥读出控制，并且，因此实现了与内容类型相应的内容使用控制。

附图说明

[0035] 图 1 是用于描述内容提供处理和使用处理的概要的示图；

[0036] 图 2 是用于描述记录在存储器卡中的内容的使用模式的示图；

[0037] 图 3 是用于描述该存储器卡的存储区域的特定配置例子的示图；

[0038] 图 4 是用于描述主机证书(Host Certificate)的示图；

[0039] 图 5 是用于描述该存储器卡的存储区域的特定配置例子和访问控制处理的例子的示图；

[0040] 图 6 是用于描述存储器卡的存储数据的例子的示图；

[0041] 图 7 是用于描述其中记录有装置类型和对应的内容类型的类型信息的主机证书(Host Certificate)的数据配置例子的示图；

[0042] 图 8 是用于描述要被记录在主机证书(Host Certificate)中的装置类型和对应

的内容类型的类型信息的特定例子的示图；

[0043] 图 9 是示出用于描述要通过根据内容类型选择性地激活播放程序并使用与激活的播放程序相关联的主机证书(Host Certificate)来执行的内容使用序列的流程图的示图；

[0044] 图 10 是示出用于描述要通过根据内容类型选择性地激活播放程序并使用与激活的播放程序相关联的主机证书(Host Certificate)来执行的内容使用序列的流程图的示图；

[0045] 图 11 是示出用于描述要通过根据内容类型选择性地激活播放程序并使用与激活的播放程序相关联的主机证书(Host Certificate)来执行的内容使用序列的流程图的示图；

[0046] 图 12 是示出用于描述其中播放程序根据内容类型选择性地使用主机证书(Host Certificate)的序列的流程图的示图；

[0047] 图 13 是示出用于描述其中播放程序根据内容类型选择性地使用主机证书(Host Certificate)的序列的流程图的示图；

[0048] 图 14 是示出用于描述其中播放程序根据内容类型选择性地使用主机证书(Host Certificate)的序列的流程图的示图；

[0049] 图 15 是用于描述存储器卡的存储数据的例子的示图；

[0050] 图 16 是用于描述使用介质 ID (MID) 的内容解码和播放序列的示图；

[0051] 图 17 是用于描述根据主机(播放设备)的类型改变介质 ID (MID)的转换模式的处理的示图；

[0052] 图 18 是用于描述在根据主机(播放设备)的类型改变介质 ID (MID)的转换模式的情况中的内容解码和重放处理的示图；

[0053] 图 19 是用于描述在通过根据主机(播放设备)的类型改变介质 ID (MID)的转换模式来执行内容解码和重放处理的情况中的处理序列的流程图的示图；

[0054] 图 20 是用于描述在根据主机(播放设备)的类型改变介质 ID (MID)的转换模式来执行内容解码和重放处理的情况中的处理序列的流程图的示图；

[0055] 图 21 是用于描述在根据主机(播放设备)的类型改变介质 ID (MID)的转换模式来执行内容解码和重放处理的情况中的处理序列的流程图的示图；

[0056] 图 22 是用于描述主机(播放设备) 的硬件配置例子的示图；以及

[0057] 图 23 是用于描述存储器卡的硬件配置例子的示图。

具体实施方式

[0058] 在下文中，将参考附图就根据本公开的信息处理装置、信息处理方法以及程序的细节进行描述。请注意，将根据下列项目进行描述。

[0059] 1. 内容提供处理和使用处理的概要

[0060] 2. 存储器卡的配置例子和使用例子

[0061] 3. 具有关于保护区域的访问许可信息的证书

[0062] 4. 关于已经应用每一个装置证书的存储器卡的访问处理例子

[0063] 5. 主机(播放设备) 与介质(存储器卡) 之间的处理例子

[0064] 5-1.（第一实施例）根据内容类型使用装置证书的主机与介质之间的处理例子

[0065] 5-2.（第二实施例）用于选择由播放程序应用的装置证书的处理例子

[0066] 5-3.（第三实施例）用于根据播放装置的类型改变介质（存储器卡）的标识符（介质ID）的转换模式的处理例子

[0067] 6. 每个装置的硬件配置例子

[0068] 7. 本公开的配置的概要

[0069] 1. 内容提供处理和使用处理的概要

[0070] 在下文中，将参考附图就根据本公开的信息处理装置、信息处理方法以及程序的细节进行描述。

[0071] 首先，将参考图 1 及其后面的附图描述内容提供处理和使用处理的概要。

[0072] 图 1 从左开始示出下面的例子。

[0073] （a）内容提供源

[0074] （b）内容记录 / 播放设备（主机）

[0075] （c）内容记录介质

[0076] （c）内容记录介质是用于已经由用户记录的内容的重放处理的介质。这里，例如，这指示作为诸如闪存等的信息记录设备的存储器卡 31。

[0077] 用户在存储器卡 31 中记录诸如音乐、电影等的各种内容，并使用这些内容。例如，充当使用控制的对象的内容（诸如充当要管理的版权的对象的内容）被包含在这些内容中。

[0078] 这里提及的充当使用控制的对象的内容是禁止未授权的复制、复制数据的发布等的内容。请注意，在将使用控制内容记录在存储器卡 31 中的情况中，对应于其内容的使用控制信息（使用规则），具体地说，其中规定了诸如可允许的复制次数等的复制限制信息的使用控制信息（使用规则）也被一起记录在存储器卡 31 中。

[0079] （a）内容提供源是诸如音乐、电影等的内容的提供源。例如，图 1 示出广播电台 11 和作为内容提供源的内容服务器 12。例如，广播电台 11 是电视台，并通过地面波或经由卫星的卫星波向用户装置 [（b）内容记录 / 播放设备（主机）] 提供各种广播内容。内容服务器 12 是用于经由诸如互联网等的网络提供诸如音乐、电影等的内容的服务器。

[0080] 例如，可以进行这样的布置，其中，用户将作为（c）内容记录介质的存储器卡 31 安装到（b）内容记录 / 播放设备（主机）上，经由（b）内容记录 / 播放设备（主机）本身的接收单元或连接到（b）内容记录 / 播放设备（主机）的接收装置接收从广播电台 11 或内容服务器 12 提供的内容，并将该内容记录到存储器卡 31 中。

[0081] （b）内容记录 / 播放设备（主机）安装作为（c）内容记录介质的存储器卡 31，并将从作为（a）内容提供源的广播电台 11 或内容服务器 12 接收的内容记录到存储器卡 31 中。

[0082] （b）内容记录 / 播放设备（主机）的例子包括包含硬盘或诸如 DVD、BD 等盘的仅用于记录 / 播放的装置（CE 装置 :消费电子装置）21，例如，DVD 播放器等，并且，（b）内容记录 / 播放设备（主机）的例子还包括 PC 22，诸如智能电话、蜂窝电话、便携式播放器、平板终端（tablet terminal）等的便携式终端 23。这些都是可以安装作为（c）内容记录介质的存储器卡 31 的装置。

[0083] 用户使用仅用于记录 / 播放的装置 21、PC 22、便携式终端 23 等从广播电台 11 或内容服务器 12 接收诸如音乐、电影等的内容，并记录在存储器卡 31 中。

[0084] 将参考图 2 描述记录在存储器卡 31 中的内容的使用模式。

[0085] 存储器卡 31 是对于诸如 PC 等的内容播放器可附接 / 可拆卸的记录介质，并且可以自由地从已经执行了内容记录的装置拆卸，并安装到另一个用户装置上。

[0086] 具体地说，如图 2 所示，下列处理的执行装置不必相同，并且用户可以自由地、选择性地使用记录装置和播放装置。

[0087] (1) 记录处理

[0088] (2) 重放处理

[0089] 请注意，在很多情况中，记录在存储器卡 31 中的使用控制内容被记录为加密内容，并且诸如仅用于记录 / 播放的装置 21、PC 22、便携式终端 23 等的内容播放设备在根据预定序列执行解密处理后执行内容重放。

[0090] 2. 存储器卡的配置例子和使用例子

[0091] 下面，将就被用作内容记录介质的诸如闪存等的存储器卡的配置例子和使用例子进行描述。在图 3 中示出了存储器卡 31 的存储区域的特定配置例子。

[0092] 如图 3 所示，存储器卡 31 的存储区域由如下两个区域构成。

[0093] (a) 保护区域 (Protected Area) 51 和

[0094] (b) 通用区域 (General Purpose Area) 52

[0095] 例如，(b) 通用区域 (General Purpose Area) 52 是记录有内容、一般内容管理数据等的可以由用户使用的记录 / 播放设备自由地访问的区域，例如，可以由服务器或用户的记录 / 播放设备自由地执行数据的写入或读取的区域。

[0096] 另一方面，(a) 保护区域 (Protected Area) 51 是不允许自由访问的区域。

[0097] 例如，在试图使用用户使用的记录 / 播放设备或经由网络连接的服务器等执行数据的写入或读取的情况中，存储器卡 31 的数据处理单元确定能否按照事先存储在存储器卡 31 中的程序根据每个设备来执行读取 (Read) 或写入 (Write)。

[0098] 存储器卡 31 包含用于执行事先存储的程序的数据处理部分和用于执行认证处理的认证处理部分，并首先用试图对存储器卡 31 执行数据的写入或读取的装置执行认证处理。

[0099] 就该认证处理的阶段而言，存储器卡 31 从伙伴终端 (即，访问请求设备) 接收诸如公共密钥证书等的装置证书。例如，在访问请求设备是服务器的情况中，存储器卡 31 接收该服务器拥有的服务器证书 (Server Certificate)，并使用其证书中描述的信息来确定对保护区域 (Protected Area)51 的各分区区域的访问是否是允许的。此外，在访问请求设备是例如充当执行内容的记录 / 播放的用户机器的记录 / 播放设备 (主机) 的情况中，存储器卡 31 接收由记录 / 播放设备 (主机) 拥有的主机证书 (Host Certificate)，并使用在其证书中描述的信息来确定对保护区域 (Protected Area) 51 的各分区区域的访问是否是允许的。

[0100] 该访问特权确定处理在图 3 中示出的保护区域 (Protected Area) 51 内以分区区域 (在图中示出的区域 #0、#1、#2 等) 为单位 (increment) 执行，并且存储器卡 31 仅允许在允许的分区区域中被许可的处理 (诸如数据的读取 / 写入等处理)，并使服务器或主机执行其处理。

[0101] 对该介质的读取 / 写入限制信息 (PAD 读取 /PAD 写入) 以装置 (例如，内容服务器

或记录 / 播放设备(主机))为单位设置以执行访问。这样的信息被记录在对应于每个装置的服务器证书(Server Certificate)或主机证书(Host Certificate)中。

[0102] 请注意,在下文中,“Certificate (证书)”将以简化的形式被称为“Cert”。

[0103] 以这种方式,存储器卡 31 根据事先存储在存储器卡 31 中的规定程序来验证服务器证书(Server Cert)或主机证书(Host Cert)的记录数据,并执行处理以允许仅针对访问许可区域的访问。

[0104] 3. 具有关于保护区域的访问许可信息的证书

[0105] 接下来,将参考图 4 针对证书的配置例子进行描述,在对上述的存储器卡 31 的保护区域(Protected Area)51 执行访问的情况中涉及该证书的关于存储器卡的呈现。

[0106] 如上所述,存储器卡 31 用试图对存储器卡 31 进行数据的写入或读取的装置执行认证处理。在该认证处理的一个阶段中,存储器卡 31 从伙伴装置(即,访问请求设备)接收诸如公共密钥证书等(例如,服务器证书(Server Cert)或主机证书(Host Cert))的装置证书,并使用在其证书中描述的信息来确定是否允许访问保护区域(Protected Area)51 的每一个分区区域。

[0107] 将参考图 4 针对作为用于该认证处理的装置证书的例子的主机证书(Host Cert)的配置例子进行描述,该主机证书(Host Cert)存储在诸如图 1 中示出的记录 / 播放设备 21、PC 22、便携式终端 23 等的用户机器(主机机器)中。

[0108] 例如,主机证书(Host Cert)由作为公共密钥证书发放者的证书颁发机构提供给每一个用户机器(主机机器)。例如,主机证书(Host Cert)是发放给其内容使用处理已经由证书颁发机构准许的用户机器(主机机器)的用户机器的证书,并且是其中存储有公共密钥等的证书。主机证书(Host Cert)被配置为这样的数据,在该数据中,已经通过证书颁发机构秘密密钥设置了签名以防止篡改。请注意,在制造装置时,装置证书可以基于诸如装置的类型等的装置确认事先存储在装置内的存储器中。在用户购买后获得装置证书的情况中,可以进行这样的布置,其中,执行与装置、证书颁发机构或另一个管理机构之间的预定序列相应的装置类型、可用内容的类型等的确认处理,以向每一个装置发放装置证书并存储在该装置内的存储器中。

[0109] 请注意,对存储器卡 31 的保护区域执行访问的服务器保持服务器证书(Server Cert),该服务器证书(Server Cert)中记录有具有与主机证书相同的配置的服务器公共密钥和存储器卡的访问许可信息。

[0110] 图 4 示出证书颁发机构提供给每一个主机机器(用户机器)的主机证书(Host Cert)的特定例子。

[0111] 主机证书(Host Cert)包含如图 4 所示的下列数据。

[0112] (1)类型信息

[0113] (2)主机 ID (用户机器 ID)

[0114] (3)主机公共密钥(Host Public Key)

[0115] (4)保护区域访问特权信息(关于介质的保护区域的读取 / 写入限制信息(PAD 读取 /PAD 写入))

[0116] (5)其它信息

[0117] (6)签名

[0118] 在下文中，将描述上述(1)到(6)的每一种数据。

[0119] (1)类型信息

[0120] 类型信息是指示证书的类型或用户机器的类型的信息，其中记录有指示本证书是主机证书的数据和指示机器的类型(例如，诸如 PC 或音乐播放器的机器的类型)的信息等。

[0121] (2)主机 ID

[0122] 主机 ID 是记录充当装置标识信息的装置 ID 的区域。

[0123] (3)主机公共密钥(Host Public Key)

[0124] 主机公共密钥是主机机器的公共密钥。该公共密钥与秘密密钥一起构成与公共密钥密码系统相应的密钥对，以提供给主机机器(用户机器)。

[0125] (4)保护区域访问特权信息(关于介质的保护区域的读取 / 写入限制信息(PAD 读取 /PAD 写入))

[0126] 例如，就保护区域访问特权信息而言，存在关于其中记录有内容的介质例如图 3 中示出的存储器卡 31 的存储区域中要设置的保护区域(PDA :Protected Area)51 内准许数据的读取(Read)和写入(Write)的分区区域的记录信息。

[0127] (5)其它信息、(6)签名

[0128] 就主机证书而言，记录了除上述(1)到(4)以外的各种类型的信息，并且记录了关于(1)到(5)中的信息的签名数据。签名是通过证书颁发机构的秘密密钥来执行的。在提取和使用记录在主机证书中的信息(例如，主机公共密钥)的情况中，已经应用了证书颁发机构的公共密钥的签名验证处理被首先执行，以确认没有对主机证书进行篡改，并且诸如主机公共密钥的证书存储数据在以其确认作为条件执行的情况下被使用。

[0129] 请注意，尽管图 4 是其中记录有关于存储器卡的保护区域的用户机器(主机机器)的访问许可信息的主机证书，但是其中记录有关于存储器卡的保护区域的访问许可信息的证书 [服务器证书(例如，其中存储有服务器公共密钥的公共密钥证书)] 以与图 4 中示出的主机证书相同的方式被提供给必须对保护区域进行访问的服务器。

[0130] 4. 关于已经应用每一个装置证书的存储器卡的访问处理例子

[0131] 如参考图 4 所述，在对存储器卡 31 的保护区域(Protected Area)51 执行访问的情况中，如图 4 所示的证书必须呈现给存储器卡。

[0132] 存储器卡确认在图 4 中示出的证书，并确定是否可以对图 3 中示出的存储器卡 31 的保护区域(Protected Area)51 执行访问。

[0133] 例如，主机机器保持参考图 4 描述的主机证书(Host Cert)，并且执行内容提供的服务器保持对应于该服务器的证书(服务器证书 :Server Certificate)。

[0134] 在这些装置中的每一个都对存储器卡的保护区域(Protected Area)执行访问的情况中，每一个装置必须向存储器卡提供其拥有的证书，以接收基于存储器卡侧上的验证的关于是否可以执行访问的确定。

[0135] 将参考图 5 针对在关于存储器卡的访问请求设备是诸如记录 / 播放设备等的主机机器的情况中的访问限制设置例子进行描述。

[0136] 从左边开始，图 5 示出作为关于存储器卡的访问请求装置的主机(记录 / 播放设备)70，以及存储器卡 31。

[0137] 主机(记录 / 播放设备)70 是诸如图 1 所示的仅用于记录 / 播放的装置 21、PC 22、

便携式终端 23 的用户机器等，并且是执行对存储器卡 31 的内容记录处理或播放记录在存储器卡 31 中的内容的装置。

[0138] 在将从广播电台或服务器接收的内容或存储在该装置本身的存储单元中的内容输出到用于记录的存储器卡 31 时，主机（记录 / 播放设备）70 执行用于将要应用到内容的加密或解密处理的标题密钥或者标题密钥的加密或转换数据写入到存储器卡 31 的保护区域（Protected Area）51 中的处理。

[0139] 此外，在播放记录在存储器卡 31 中的加密内容的情况中，主机（记录 / 播放设备）70 执行用于获得写入在存储器卡 31 的保护区域（Protected Area）51 中的标题密钥或标题密钥的加密或转换数据的处理。主机（记录 / 播放设备）70 必须以这种方式在内容记录 / 重放处理中对存储器卡 31 的保护区域（Protected Area）51 执行访问。

[0140] 存储器卡 31 包含保护区域（Protected Area）51 和通用区域（General Purpose Area）52，并且加密内容等被记录在通用区域（General Purpose Area）52 中。

[0141] 作为用于内容重放的密钥的标题密钥被记录在保护区域（Protected Area）51 中。

[0142] 如前文参考图 3 所描述的，保护区域（Protected Area）51 被分成多个区域。

[0143] 就在图 5 中示出的例子而言，示出了具有下列两个分区区域的例子 ：分区区域 #0（Protected Area#0）61 和分区区域 #1 （Protected Area#1）62。

[0144] 针对这些分区区域的设置模式，可以执行各种设置。图 5 示出主机（记录 / 播放设备）70 保持的主机证书（Host Cert）的保护区域访问特权信息。

[0145] 使用在图 5 中示出的主机证书的访问控制信息执行下列设置。

[0146] 对于分区区域 #0 （Protected Area#0），数据的写入（Write）和读取（Read）的两种处理都是许可的。

[0147] 对于分区区域 #1 （Protected Area#1），仅许可读取（Read）处理。

[0148] 就图 5 中示出的主机证书（Host Cert）而言，未设置对于分区区域 #1 （Protected Area#1）的写入（Write）许可。例如，其中记录有这样的保护区域访问特权信息的证书被提供给用户机器。

[0149] 试图访问存储器卡 31 的保护区域（Protected Area）51 的装置向存储器卡输出其中记录有该保护区域访问特权信息的证书。存储器卡基于存储器卡内的数据处理分区内的证书验证处理来确定是否可以执行访问。主机（记录 / 播放设备）70 根据确定信息访问存储器卡 31 的保护区域（Protected Area）51。

[0150] 以这种方式，存储器卡的保护区域（Protected Area）被配置为访问控制区域，其中，数据的写入（Write）和读取（Read）的许可或不许可已经以访问请求设备为单位且还以分区区域（#0、#1、#2 等）为单位被设置。

[0151] 如参考图 4 所描述的，保护区域访问特权信息被记录在每一个访问请求设备的证书（服务器证书、主机证书等）中，并且存储器卡首先对从访问请求设备接收的证书执行签名验证，在确认有效性后，读取在证书中描述的访问控制信息，即，下列信息 ：读取许可区域信息（PAD 读取），以及写入许可区域信息（PAD 写入）。

[0152] 基于这样的信息，存储器卡仅许可并执行对于访问请求设备所准许的处理。

[0153] 请注意，对于主机，例如，也有各种类型的机器，诸如记录器、播放器等的 CE 装置、PC 等。

[0154] 装置证书是由这些装置各自保持的证书，并且，根据这些装置的类型可以具有不同的设置。

[0155] 此外，基于记录在装置证书中的下列信息，即：读取许可区域信息（PAD 读取）和写入许可区域信息（PAD 写入），此外，不仅基于这些信息，而且还基于参考图 4 描述的证书中包含的类型信息（Type），存储器卡的数据处理分区可以以保护区域的分区区域为单位执行访问许可确定。

[0156] 5. 主机（播放设备）与介质（存储器卡）之间的处理例子

[0157] 接下来，将针对执行存储在介质（存储器卡）中的内容的重放处理的主机（播放设备）与介质（存储器卡）之间的处理例子进行描述。

[0158] 5-1. （第一实施例）使用与内容类型相应的装置证书的主机与介质之间的处理例子

[0159] 首先，作为主机（播放设备）与介质（存储器卡）之间的处理例子的第一实施例，将描述利用与内容类型相应的装置证书的处理例子。

[0160] 存在从广播电台或内容服务器向用户机器提供的各种类型的内容。

[0161] 例如，存在诸如电影内容、音乐内容、运动图像内容和静止图像内容的各种内容。

[0162] 此外，例如，在电影内容当中也存在向公众发布不久的电影内容和向公众发布后过了一定量的时间的电影内容。

[0163] 在诸如向公众发布不久的新电影的新内容的未授权复制流通的事件中，会发生一个问题，其中，该新内容的内容价值迅速地降低，并且其版权持有人和发行权持有人的利益显著地下降。另一方面，对于老内容（诸如向公众发布后已经过去若干年且 DVD 等的销售峰值已经过去的老电影）来说，版权持有人和发行权持有人的利益水平已经降低，因此即使产生了未授权复制，其影响相对来说也较小。

[0164] 以这种方式，根据内容的类型价值有所不同，并且存在应当更严格地防止非法使用的高附加值内容、以及除此以外的内容。就下面的描述而言，更严格地防止非法使用的内容将称为高附加值内容（增强内容），除了高附加值内容以外的其它内容将称为普通内容（基本内容）。

[0165] 响应于其中存在这样的各种类型的内容的当前情况，关于用于增强高附加值内容（增强内容）的保护的对策的例子，将描述利用与内容类型相应的装置证书的处理例子。例如，该装置证书应当是之前参考图 4 描述的主机证书（Host Cert）。如参考图 4 和图 5 所述的，对于装置证书而言，记录有以存储器卡的保护区域（Protected Area）的分区区域（#0、#1、#2 等）为单位的访问特权，并且具体地说，诸如仅用于读取（Read）的许可、仅用于写入（Write）的许可、用于读取 / 写入（Read/Write）的许可等的各种类型的访问特权信息。

[0166] 根据内容类型发放多个这样的装置证书，并且一个内容证书应当被作为只能用于特定类型的内容的内容证书。

[0167] 图 6 示出记录在存储器卡 100 中的加密内容和要应用于加密内容的解密的标题密钥的存储例子。

[0168] 如上所述，存储器卡 100 被分成以下两个区域：保护区域（Protected Area）101 和通用区域（General Purpose Area）102。

[0169] 加密内容被记录在通用区域（General Purpose Area）102 中。

[0170] 如图所示，内容被分成以下两种类型：(a)普通内容(基本内容)；(b)高附加值内容(增强内容)。

[0171] 内容作为设置被记录，由此可以区分内容类型，例如，可以区分是(a)普通内容(基本内容)还是(b)高附加值内容(增强内容)。例如，内容与元数据一同被记录，在该元数据中记录有这些内容的内容类型。这些内容是解密内容，并且在内容重放时，必须执行使用对应于每一个内容(标题)的标题密钥的解密处理。

[0172] 标题密钥被记录在保护区域(Protected Area)101中。请注意，标题密钥可以被记录为加密的或转换的数据。这是抵制泄漏的对策之一。如图6所示，记录在保护区域(Protected Area)101的标题密钥还以与加密内容的类型相同的方式被简单地分成下列两种类型：(a)用于普通内容的标题密钥(用于基本内容的标题密钥)；(b)用于高附加值内容的标题密钥(用于增强内容的标题密钥)。

[0173] 标题密钥作为设置被记录，由此可以区分由标题密钥解密的内容类型，例如，可以区分是(a)普通内容(基本内容)还是(b)高附加值内容(增强内容)。例如，标题密钥与元数据一同被记录，在该元数据中记录有这些标题密钥的内容类型。请注意，这两种类型的标题密钥可以被设置为针对每一种类型存储在不同的分区区域中，并且可以被设置为基于记录的分区来区分对应的内容类型。在这种情况中，可以在具有不同分区单位的访问特权下执行访问控制。

[0174] 在执行内容重放的情况中，执行内容重放处理的播放设备(主机)(例如，诸如仅用于记录/播放的装置、PC、便携式终端等的播放设备)必须从存储器卡的保护区域读出对应于要被播放的内容的标题密钥。

[0175] 为了执行该标题密钥读出处理，播放设备(主机)将该装置证书(Cert)呈现给存储器卡。

[0176] 这里，如上所述，装置证书被设置为与内容类型相应的装置证书。

[0177] 在图7中示出与内容类型相应的主机证书(Host Cert)的配置例子。

[0178] 图7示出下列两种类型的主机证书(Host Cert)的例子：(A)可以被用于播放高附加值内容和普通内容两者的主机证书(HostCert)；(B)可以被用于仅播放普通内容的主机证书(Host Cert)。

[0179] 在图7中示出的主机证书(Host Cert)是以与之前参考图4描述的方式相同的方式记录下列数据的证书。

[0180] (1)类型信息

[0181] (2)主机ID(用户装置ID)

[0182] (3)主机公共密钥(Host Public Key)

[0183] (4)保护区域访问特权信息(关于介质的保护区域的读取/写入限制信息(PAD读取/PAD写入))

[0184] (5)其它信息

[0185] (6)签名(Signature)

[0186] 但是，在图7中示出的主机证书的不同之处在于，在(1)类型信息中记录下列信息。

[0187] (1a)装置类型信息

[0188] (1b)对应的内容类型信息

[0189] “(1a)装置类型信息”是指示保持该主机证书(Host Cert)的主机是什么类型的装置的信息。具体地说,例如,该信息是指示主机是下列哪种类型的装置的信息。

[0190] * 仅用于记录 / 播放的装置

[0191] *PC,或者

[0192] * 便携式终端(平板型终端等)

[0193] “(1b)对应的内容类型信息”是指示允许使用该主机证书(Host Cert)从存储器卡获得的标题密钥的内容类型的信息。具体地说,该信息是指示本主机证书是否可以用于获得对应于下列内容中的任何一种或两种内容的标题密钥的信息。

[0194] * 高附加值内容(增强内容),和

[0195] * 普通内容(基本内容)

[0196] 如上所述,就装置证书而言,其中记录有指示装置本身的装置类型的装置类型和指示对应于可以通过应用该装置证书获得的标题密钥的内容的类型的对应内容类型信息。

[0197] 将参考图 8 描述下列信息的组合的例子。

[0198] (1a)装置类型信息

[0199] (1b)对应的内容类型信息

[0200] 如图 8 所示,(1a)装置类型信息被分成下列两种类型 :仅用于记录 / 播放的装置(代码 :0x0001);PC/ 便携式终端(平板型终端等)(代码 :0x0002)。

[0201] 请注意,这种类型分类是一个例子,并且,可以进一步地被细分。

[0202] 此外,(1b)对应的内容类型信息被分成下列三种类型 :仅对应于普通内容(代码 :0x0001);仅对应于高附加值内容(代码 :0x0002);对应于高附加值内容和普通内容两者(代码 :0x0003)。

[0203] 请注意,这种类型分类是一个例子,并且可以进一步地被细分。例如,可以设置与各种内容(诸如运动图像内容、电影内容、静止图像内容等)的类型相应的分类。

[0204] 接下来,将参考图 9 到图 11 中示出的流程图描述使用对应于内容类型的装置证书的内容重放处理的序列。

[0205] 在图 9 到图 11 中示出的流程图顺序地示出了在左侧的用于执行内容重放的主机(播放设备)和在右侧的存储有加密内容和标题密钥的介质(存储器卡),并顺序地示出由这两个装置执行的处理。将描述各步骤的处理的细节。

[0206] 在步骤 S111 中,其上安装有介质(存储器卡)的主机(播放设备)输入要被播放的内容的选择信息。

[0207] 例如,主机(播放设备)在主机的显示器上显示存储在存储器卡中的内容的列表,并且用户从显示的内容列表选择要播放的内容,从而,主机的数据处理部分识别用户指定的选择的内容。

[0208] 在步骤 S112 中,主机根据选择的内容的类型来激活播放程序。

[0209] 就本处理例子而言,内容的类型是下面(a)和(b)之一 :(a)普通内容,和(b)高附加值内容。

[0210] 请注意,对于每一个内容,指示内容类型的信息被记录在与内容相关联的属性信息(元数据)中,并且基于该属性信息来判别内容类型。或者,可以进行这样的布置,其中,内

容文件作为根据内容类型具有不同扩展名的设置被记录，并且参考该扩展名来判别内容。

[0211] 或者，可以根据扩展名自动地选择要激活的程序。

[0212] 主机保持用于执行普通内容的重放处理的普通内容播放程序和用于执行高附加值内容的重放处理的高附加值内容播放程序，并激活对应于被选作要被播放的内容的类型的播放程序。请注意，虽然主机可以仅具有普通内容播放程序，但是这样的主机将不能执行高附加值内容的重放处理。此外，高附加值内容播放程序可以被设置为仅播放高附加值内容，或者可以被设置为能够播放高附加值内容和普通内容两者的程序。

[0213] 接下来，在步骤 S113 中，主机从装置本身的存储器获得与根据内容的类型激活的播放程序相关联的装置证书(Host Cert)。该装置证书(Host Cert)是之前参考图 7 描述的主机证书(Host Cert)，并且是其中记录下列信息作为类型信息的证书：(1a)装置类型信息；(1b)对应的内容类型信息。

[0214] 请注意，例如，在图 7 中的(B)中示出的，普通内容播放程序可以获得单独地只对应于普通内容的主机证书，在图 7 中的(A)中示出的，高附加值内容播放程序可以获得单独地对应于高附加值内容和普通内容的主机证书。例如，就用于获得记录在每一个播放程序中的主机证书的信息(例如，存储器地址)而言，仅记录了对应于图 7 中的(A)和(B)中的任意一个的主机证书的信息(地址)，每一个播放程序都可以获得可以由该程序本身使用的唯一的主机证书。

[0215] 接下来，在步骤 S114a 和 S114b 中，在主机(播放设备)与介质(存储器卡)之间的相互认证处理被执行。通过该相互认证处理，主机(播放设备)将从主机的存储器获得的主机证书(Host Cert)发送到介质(存储器卡)。

[0216] 另一方面，介质(存储器卡)将存储在介质(存储器卡)内的存储器中的介质的装置证书(Media Cert)发送到主机(播放设备)。例如，该认证处理作为已经应用这两种公共密钥证书的公共密钥密码系统的相互认证处理被执行。

[0217] 接下来，将描述在图 10 中示出的步骤 S115a 和 S115b 及其后面的步骤中的处理。

[0218] 在步骤 S115a 和 S115b 中，对主机(播放设备)与介质(存储器卡)之间的相互认证是否已经建立进行确定。

[0219] 在没有建立相互认证的情况中，确定两装置之间的可靠性未被确认，流程前进到步骤 S130，并停止内容重放处理。

[0220] 在已经建立了相互认证的情况中，流程前进到步骤 S116a 和 S116b。

[0221] 在步骤 S116a 中，主机(播放设备)将对应于要被播放的内容的标题密钥读取请求发送到介质(存储器卡)。

[0222] 在步骤 S116b 中，介质(存储器卡)接收该标题密钥读取请求。

[0223] 接下来，在步骤 S117 中，参考在之前认证信息时从主机(播放设备)接收到的主机证书(Host Cert)的类型信息，介质(存储器卡)确定从主机(播放设备)接收到的主机证书(Host Cert)是否是其中记录有对应的内容类型信息的主机证书(Host Cert)，该对应的内容类型信息对应于与主机请求的标题密钥相对应的内容的类型。

[0224] 例如，假定这样的布置，其中在图中 7 示出的两种类型的主机证书(Host Cert)可用。在被安排为要被播放的内容是普通内容，并且主机请求的标题密钥是对应于普通内容的标题密钥的情况中，即使当从主机接收到的主机证书是如下在图 7 中示出的两个证书

((A)可以被用于播放高附加值内容和普通内容两者的主机证书(Host Cert),以及(B)可以被用于仅播放普通内容的主机证书(Host Cert))之一时,在步骤 S117 中的确定也为“是”。

[0225] 此外,在被安排为要被播放的内容是高附加值内容,并且主机请求的标题密钥是对应于高附加值内容的标题密钥的情况中,只有当从主机接收到的主机证书是如下在图 7 中示出的(A)可以被用于播放高附加值内容和普通内容两者的主机证书(Host Cert)时,在步骤 S117 中的确定才为“是”。

[0226] 当从主机接收到的主机证书是如下在图 7 中示出的(B)可以被用于仅播放普通内容的主机证书(Host Cert)时,在步骤 S117 中的确定为“否”。

[0227] 在步骤 S117 中的确定为“否”的情况中,流程前进到步骤 S130,停止内容的播放。也就是说,没有执行针对主机提供标题密钥。

[0228] 在确定从主机(播放设备)接收到的主机证书(Host Cert)是其中记录有对应的内容类型信息的主机证书(Host Cert)(该对应的内容类型信息对应于与主机请求的标题密钥相对应的内容的类型)的情况中,在步骤 S117 中的确定为“是”,并且流程前进到步骤 S118。

[0229] 接下来,在步骤 S118 中,参考在之前的认证处理时从主机(播放设备)接收到的主机证书(Host Cert)的保护区域访问特权信息,介质(存储器卡)确认主机请求的标题密钥的存储区域(即,保护区域的分区区域)是否已经被设置为数据读取许可区域。

[0230] 如之前参考图 4 和图 5 所述,以存储器卡的保护区域的分区区域为单位的访问特权(读取 / 写入)的许可信息被记录在主机证书(Host Cert)的保护区域访问特权信息区域中。参考该保护区域访问特权信息,介质(存储器卡)确定主机请求的标题密钥的存储区域(即,保护区域的分区区域)是否已经被设置为数据读取许可区域。

[0231] 在图 11 示出的步骤 S119 中,在其中存储主机请求的标题密钥的保护区域的分区区域没有作为数据读取许可区域被记录在主机证书(Host Cert)中的情况中,在步骤 S119 中的确定为“否”。

[0232] 在这种情况中,流程前进到步骤 S130,并停止内容播放。也就是说,没有执行针对主机提供标题密钥。

[0233] 另一方面,在其中存储主机请求的标题密钥的保护区域的分区区域已经作为数据读取许可区域被记录在主机证书(Host Cert)中的情况中,在步骤 S119 中的确定为“是”,并且流程前进到步骤 S120。

[0234] 在步骤 S120a 中,介质(存储器卡)从保护区域获得从主机(播放设备)请求的标题密钥,并进一步从通用区域获得加密内容,并发送到主机。

[0235] 在步骤 S120b 中,主机(播放设备)从介质(存储器卡)接收标题密钥和加密内容。

[0236] 接下来,在步骤 S121 中,主机(播放设备)通过应用获得的标题密钥来执行对加密内容的解密处理以开始内容重放。

[0237] 5-2. (第二实施例)用于选择播放程序应用的装置证书的处理例子

[0238] 就参考图 9 到图 11 中示出的流程图描述的根据第一实施例的内容重放序列而言,进行了这样的布置,其中,要被激活的播放程序是根据被选作要被播放的内容的内容的类型来选择的,并且使用对应于选择的被激活的播放程序设置的主机证书(Host Cert)(即,被设置为可以由选择的被激活的播放程序访问的一个主机证书(Host Cert))来执行处理。

[0239] 具体地说，已经假定了这样的布置，其中，播放程序被设置为与内容的类型相应的专用程序，诸如对应于普通内容的播放程序或者对应于高附加值内容的播放程序，并且每一次一个地给每个播放程序分配可用的主机证书(Host Cert)。

[0240] 接下来，将参考在图 12 到图 14 中示出的流程图描述不同于上述第一实施例的用于执行处理的第二实施例。就当前第二实施例而言，当在主机(播放设备)处要被执行的播放程序是一个播放程序的情况中，即，在要被播放的内容是普通内容或高附加值内容的情况中，通过同一程序执行重放处理。就本实施例而言，播放程序本身判别被选作要被播放的内容的内容的类型，根据该判别，选择并使用要被使用的主机证书(Host Cert)。

[0241] 具体地说，作为播放程序的处理，判别内容类型，并且根据判别的内容类型，选择并使用下列两种类型的主机证书(Host Cert)之一：(A)可以被用于播放高附加值内容和普通内容两者的主机证书(Host Cert)；(B)可以被用于仅播放普通内容的主机证书(Host Cert)。

[0242] 将描述在图 12 到图 14 中示出的流程图的步骤中的处理。

[0243] 在图 12 到图 14 中示出的流程图以与在图 9 到图 11 中的流程图相同的方式顺序地示出了在左侧的用于执行内容重放的主机(播放设备)和在右侧的其中存储有加密内容和标题密钥的介质(存储器卡)，并顺序地示出由这两个装置执行的处理。

[0244] 在步骤 S211 中，其上安装有介质(存储器卡)的主机(播放设备)输入要被播放的内容的选择信息。例如，主机在主机的显示器上显示存储在存储器卡中的内容的列表，并且用户从显示的内容列表选择要播放的内容，从而，主机的数据处理部分识别用户指定的选择的内容。例如，存储在主机的存储器中的内容播放程序通过选择要被播放的内容作为触发器来被激活。

[0245] 请注意，就在之前的图 9 到图 11 中示出的流程的处理而言，虽然激活的程序根据内容的类型(高附加值 / 普通)不同，但是对于本处理例子，激活的程序没有根据选择的内容的类型(高附加值 / 普通)改变。

[0246] 在步骤 S212 中，播放程序判别由用户选择的内容的类型。就本处理例子而言，内容的类型也是下面(a)和(b)之一。

[0247] (a)普通内容

[0248] (b)高附加值内容

[0249] 请注意，对于每一个内容，指示内容类型的信息被记录在与内容相关联的属性信息(元数据)中，并且基于该属性信息来判别内容类型。或者，可以进行这样的布置，其中，作为根据内容类型具有不同扩展名的设置记录内容文件，并且参考该扩展名来判别内容。

[0250] 接下来，在步骤 S213 中，主机根据确定的内容类型从装置本身的存储器选择并获得要使用的装置证书(Host Cert)。

[0251] 该装置证书(Host Cert)是之前参考图 7 描述的主机证书(Host Cert)，并且是其中记录下列信息作为类型信息的证书：(1a)装置类型信息；(1b)对应的内容类型信息。

[0252] 就本例子而言，播放程序本身执行对主机证书(Host Cert)的选择，该主机证书(Host Cert)对应于被安排为要被播放的内容的类型。在被选作要被播放的内容的内容是高附加值内容的情况中，例如，选择并获得主机证书(Host Cert)，其中，高附加值内容作为可用内容被设置在参考图 7 描述的主机证书(Host Cert)的(1b)对应的内容类型信息中。

具体地说，例如，选择并获得在图 7 中的(A)中示出的主机证书。

[0253] 另一方面，在被选作要被播放的内容的内容是普通内容的情况中，选择并获得主机证书(Host Cert)，其中，普通内容作为可用内容被设置在参考图 7 描述的主机证书(Host Cert)的(1b)对应的内容类型信息中。具体地说，例如，选择并获得在图 7 中的(B)中示出的主机证书。请注意，在这种情况中，在图 7 中的(A)中示出的证书也可以用于播放普通内容，因此可以选择在图 7 中的(A)中示出的证书。

[0254] 但是，例如，在主机(播放设备)仅保持在图 7 中的(B)中示出的对应于普通内容的主机证书(Host Cert)的情况中，如果高附加值内容已经被选作要被播放的内容，无法获得可用的主机证书(Host Cert)，因此将不执行内容重放。

[0255] 以这种方式，在步骤 S213 中，主机(播放设备)根据内容类型选择性地获得下列两种类型的主机证书(Host Cert)中的任何主机证书：(A)可以被用于播放高附加值内容和普通内容两者的主机证书(Host Cert)；(B)可以被用于仅播放普通内容的主机证书(Host Cert)。

[0256] 接下来，在步骤 S214a 和 S214b 中，主机(播放设备)执行主机(播放设备)与介质(存储器卡)之间的相互认证处理。通过该相互认证处理，主机(播放设备)将根据内容类型从主机的存储器选择的主机证书(Host Cert)发送到介质(存储器卡)。

[0257] 另一方面，介质(存储器卡)将存储在介质(存储器卡)内的存储器中的介质(存储器卡)的主机证书发送到主机(播放设备)。例如，该认证处理作为已经应用这两种公共密钥证书的公共密钥密码系统的相互认证处理被执行。

[0258] 接下来，将描述在图 13 中示出的步骤 S215a 和 S215b 及其后面的步骤中的处理。

[0259] 在图 13 到图 14 中示出的步骤 S215a 到 S221 中的处理与之前参考图 9 到图 11 描述的流程的步骤 S115a 到 S121 中的处理基本上相同。

[0260] 在步骤 S215a 和 S215b 中，对主机(播放设备)与介质(存储器卡)之间的相互认证是否已经建立进行确定。在没有建立相互认证的情况中，确定两装置的可靠性未被确认，流程前进到步骤 S230，并停止内容重放处理。

[0261] 在已经建立了相互认证的情况中，流程前进到步骤 S216a 和 S216b。

[0262] 在步骤 S216a 中，主机(播放设备)将对应于要被播放的内容的标题密钥读取请求发送到介质(存储器卡)。

[0263] 在步骤 S216b 中，介质(存储器卡)接收该标题密钥读取请求。

[0264] 接下来，在步骤 S217 中，介质(存储器卡)参考在之前的认证处理时从主机(播放设备)接收到的主机证书(Host Cert)的类型信息，以确定从主机(播放设备)接收到的主机证书(Host Cert)是否是其中记录有对应的内容类型信息的主机证书(Host Cert)，该对应的内容类型信息对应于与主机请求的标题密钥相对应的内容的类型。

[0265] 例如，假定这样的布置，其中在图 7 中示出的两种类型的主机证书(Host Cert)可用。

[0266] 在被安排为要被播放的内容是普通内容，并且主机请求的标题密钥是对应于普通内容的标题密钥的情况中，从主机接收到的主机证书是如下两种类型的主机证书(Host Cert)中的任何主机证书，在步骤 S217 中的确定为“是”。

[0267] (A)可以被用于播放高附加值内容和普通内容两者的主机证书(Host Cert)

[0268] (B)可以被用于仅播放普通内容的主机证书(Host Cert)

[0269] 此外,在被安排为要被播放的内容是高附加值内容,并且主机请求的标题密钥是对应于高附加值内容的标题密钥的情况中,只有当从主机接收到的主机证书是在图 7 中示出的如下主机证书(Host Cert)类型((A)可以被用于播放高附加值内容和普通内容两者的主机证书(Host Cert))时,在步骤 S217 中的确定为“是”。

[0270] 当从主机接收到的主机证书是在图 7 中示出的如下主机证书(Host Cert)类型((B)可以被用于仅播放普通内容的主机证书(Host Cert))时,在步骤 S217 中的确定为“否”。

[0271] 在步骤 S217 中的确定为“否”的情况中,流程前进到步骤 S230,并停止内容的播放。也就是说,没有执行针对主机提供标题密钥。

[0272] 当确定从主机(播放设备)接收到的主机证书(Host Cert)是其中记录有对应的内容类型信息的主机证书(Host Cert)(该对应的内容类型信息对应于与主机请求的标题密钥相对应的内容的类型)时,在步骤 S217 中的确定为“是”,并且流程前进到步骤 S218。

[0273] 接下来,在步骤 S218 中,介质(存储器卡)参考在之前的认证处理时从主机(播放设备)接收到的主机证书(Host Cert)的保护区域访问特权信息,以确定主机请求的标题密钥的存储区域(即,保护区域的分区区域)是否被设置为数据读取许可区域。

[0274] 如之前参考图 4 和图 5 所述,以存储器卡的保护区域的分区区域为单位的访问特权(读取 / 写入)的许可信息被记录在主机证书(Host Cert)的保护区域访问特权信息区域中。介质(存储器卡)参考该保护区域访问特权信息以确定主机请求的标题密钥的存储区域(即,保护区域的分区区域)是否被设置为数据读取许可区域。

[0275] 在图 14 示出的步骤 S219 中,在其中存储主机请求的标题密钥的保护区域的分区区域没有作为数据读取许可区域被记录在主机证书(Host Cert)中的情况中,在步骤 S219 中的确定为“否”。

[0276] 在这种情况中,流程前进到步骤 S230,并停止内容重放。也就是说,没有执行针对主机提供标题密钥。

[0277] 另一方面,在其中存储主机请求的标题密钥的保护区域的分区区域已经作为数据读取许可区域被记录在主机证书(Host Cert)中的情况中,在步骤 S219 中的确定为“是”,并且流程前进到步骤 S220a 和 S220b。

[0278] 在步骤 S220a 中,介质(存储器卡)从保护区域获得从主机(播放设备)请求的标题密钥,并进一步从通用区域获得加密内容,并发送到主机。

[0279] 在步骤 S220b 中,主机(播放设备)从介质(存储器卡)接收标题密钥和加密内容。

[0280] 接下来,在步骤 S221 中,主机(播放设备)通过应用获得的标题密钥来执行对加密内容的解密处理以开始内容重放。

[0281] 5-3. (第三实施例)用于根据播放装置的类型改变介质(存储器卡)的标识符(介质 ID)的转换模式的处理例子

[0282] 接下来,用于根据播放装置的类型改变介质(存储器卡)的标识符(介质 ID)的转换模式的处理例子将作为主机(播放设备)与介质(存储器卡)之间的处理例子的第三实施例进行描述。

[0283] 其中存储加密内容以及被应用于加密内容的解密的标题密钥的介质(存储器卡)

保持介质 ID（MID），该介质 ID（MID）是介质本身的标识信息。如图 15 所示，介质（存储器卡）300 包括保护区域（Protected Area）311 和通用区域（General Purpose Area）312，在保护区域（Protected Area）311 中基于在每一个装置证书中记录的访问特权信息来许可访问，将标题密钥存储在保护区域（Protected Area）311 中，并将加密内容存储在通用区域（General Purpose Area）312 中。

[0284] 除了加密内容以外，内容使用控制信息（使用规则），以及此外如图中所示出的介质 ID（MID）315 和充当其验证值的介质 ID-MAC（消息认证代码）316 被记录在通用区域（General Purpose Area）312 中。

[0285] 介质 ID（MID）315 是介质（存储器卡）的标识符，并且被设置为与每一个介质都不同的值（介质本征值）。

[0286] 介质 ID-MAC 316 是介质 ID（MID）315 的篡改验证值，并且例如，被配置为设置管理者的签名的数据。

[0287] 在播放记录在介质（存储器卡）300 中的内容的情况中，介质 ID（MID）315 和介质 ID-MAC 316 由播放设备（主机）读出，并执行利用 MAC 的验证处理。根据该验证处理，在确认介质 ID（MID）315 的有效性作为条件的情况下，该处理可以前进到利用标题密钥的对加密内容的解密。

[0288] 事先在播放设备（主机）中存储的内容播放程序根据这样的预定重放处理序列执行介质 ID（MAC）的验证和通过应用标题密钥的对加密内容的解密。

[0289] 将参考图 16 对用于介质 ID（MAC）的验证和应用标题密钥的加密内容解密处理的序列的例子进行描述。图 16 示出其中存储有加密内容等的介质（存储器卡）320 和用于执行存储在介质（存储器卡）320 中的加密内容的解密和播放的主机（播放设备）350。

[0290] 如图中所示，下列数据被存储在介质（存储器卡）320 中：介质 ID-MAC 321、介质 ID（MID）322、转换标题密钥（XORed 标题密钥）323、使用控制信息（使用规则）324 和加密内容（Encrypted Content）325。

[0291] 请注意，虽然在介质（存储器卡）320 中还另外存储有各种类型的数据，但是仅示出了要被应用于介质 ID（MAC）的验证和应用标题密钥的加密内容解密处理的序列的数据。

[0292] 使用控制信息（使用规则）324 是对应于加密内容（Encrypted Content）325 的使用控制信息，例如，具体来说，是记录有诸如用于复制内容的许可信息的使用许可信息的数据。在使用加密内容（Encrypted Content）325 时，主机（播放设备）根据使用控制信息（使用规则）324 的规定使用内容。

[0293] 转换标题密钥（XORed 标题密钥）323 是标题密钥的转换数据，并存储在存储器卡的保护区域（Protected Area）中。具体地说，标题密钥数据与使用控制信息（使用规则）324 的散列值（hash value）之间的异或（XOR）结果作为转换标题密钥被存储。

[0294] 将描述主机（播放设备）350 的处理序列。在图 16 中示出的步骤 S301 到 S305 的序列中，将对主机（播放设备）350 执行的处理进行描述。

[0295] 首先，在步骤 S301 中，主机（播放设备）350 从介质（存储器卡）320 读出使用控制信息（使用规则）324，并计算其散列值，例如，根据 AES 加密算法执行散列值计算。

[0296] 接下来，在步骤 S302 中，主机（播放设备）350 根据诸如访问特权的确认等的预定过程计算从介质（存储器卡）320 的保护区域（Protected Area）读出的使用控制信息（使用

规则)324 的散列值与转换标题密钥(XORed 标题密钥)323 之间的异或(XOR)。根据该处理，生成标题密钥。

[0297] 接下来，在步骤 S303 中，主机(播放设备)350 通过应用在步骤 S302 中生成的标题密钥来对从介质(存储器卡) 320 读出的介质 ID (MID) 322 执行 MAC 计算。

[0298] 接下来，在步骤 S304 中，主机(播放设备) 350 执行从介质(存储器卡) 320 读出的介质 ID-MAC 321 与在步骤 S303 中计算的 MAC 值之间的匹配处理。

[0299] 就该匹配处理而言，当从介质(存储器卡) 320 读出的介质 ID-MAC 321 与在步骤 S303 中计算的 MAC 值匹配时，MAC 匹配成立(settle)，确定对介质(存储器卡)320 的有效性已经进行确认，并且流程前进到应用标题密钥的加密内容解密处理。

[0300] 另一方面，就该匹配处理而言，当从介质(存储器卡) 320 读出的介质 ID-MAC 321 与在步骤 S303 中计算的 MAC 值不匹配时，MAC 匹配不成立，确定对介质(存储器卡) 320 的有效性尚未进行确认，并且不执行应用标题密钥的加密内容解密处理。

[0301] 请注意，为了基于该确定处理来描述处理的执行 / 未执行，在图 16 中示出开关 351。该开关 351 是为了描述处理算法而示出的，并且不必作为实际硬件上的配置被包括在内。

[0302] 就步骤 S304 中的 MAC 验证处理而言，当从介质(存储器卡)320 读出的介质 ID-MAC 321 与在步骤 S303 中计算的 MAC 值匹配，并且介质的有效性被确认时，流程前进到步骤 S305。

[0303] 在步骤 S305 中，主机(播放设备)350 对从介质(存储器卡)320 读出的加密内容 325 执行应用了从转换标题密钥 323 生成的标题密钥的解密处理以生成内容(Content)371，并执行诸如内容重放等的内容使用处理。请注意，该内容使用被要求根据从介质(存储器卡) 320 读出的使用控制信息的规则(使用规则) 372 作为使用模式来执行。

[0304] 以这种方式，在存储在介质(存储器卡)中的内容的解密 / 重放处理时，必须执行使用作为介质的标识符的介质 ID (MID) 的介质的有效性确认。

[0305] 另一方面，存在用于执行内容重放的各种类型的内容装置。例如，如之前参考图 1 和图 2 所描述的，存在下列各种装置 :

[0306] * 诸如 DVD 播放器、BD 播放器等的仅用于记录 / 播放的装置(CE 装置) 21

[0307] *PC 22

[0308] * 诸如智能电话或平板终端等的便携式终端 23。

[0309] 将在下面描述的实施例是这样的布置例子，其中，介质(存储器卡) 的标识符(介质 ID) 的转换模式根据这些各种播放装置的类型而改变。也就是说，在将介质 ID (MID) 输出到用于执行内容重放的主机(播放设备)时，介质(存储器卡)执行根据主机(播放设备)的类型而不同的数据转换处理(编码) 以提供给主机(播放设备)。主机(播放设备) 根据装置的类型对从介质(存储器卡) 接收的转换介质 ID (MID) 执行恢复处理(解码) 以获得介质 ID (MID)。

[0310] 将参考图 17 描述特定的例子。

[0311] 图 17 是其中用于执行内容重放的装置(主机)被分成下列两种类型的例子 :(1)主机 = 仅用于记录 / 播放的装置 ;(2) 主机 =PC 和便携式终端。

[0312] 图 17 示出其中装置(主机) 被分成这两种类型并且根据每一种类型执行不同的处

理的例子。

[0313] 对于介质(存储器卡),介质 ID (MID) 401 被存储在存储器中。

[0314] 介质(存储器卡)确认其上安装有介质(存储器卡)的用于播放介质内的内容的主机(播放设备)的类型是下列类型中的哪一个 :

[0315] (1) 主机 = 仅用于记录 / 播放的装置

[0316] (2) 主机 =PC 和便携式终端。

[0317] 对主机(播放设备)的类型是上述哪种类型进行确认。

[0318] 请注意,例如,当要在主机(播放设备)与介质(存储器卡)之间执行相互认证处理之时,主机类型(播放设备类型)的该确认处理可以通过确认介质(存储器卡)从主机(播放设备)接收到的主机证书(Host Cert)的类型信息(参见图 7 和图 8)来执行。

[0319] 在介质(存储器卡)已经确认主机(播放设备)是仅用于记录 / 播放的装置的情况中,在图 17 的左侧示出的(1) 主机 = 仅用于记录 / 播放的装置的处理被执行。

[0320] 另一方面,在介质(存储器卡)已经确认主机(播放设备)是 PC 或便携式终端的情况中,在图 17 的右侧示出的(2) 主机 =PC 和便携式终端的处理被执行。

[0321] 就(1)主机 = 仅用于记录 / 播放的装置的处理而言,在步骤 S321 中,介质(存储器卡)执行对应于仅用于记录 / 播放的装置的介质(MID)的编码处理(编码)。充当该编码结果的仅用于记录 / 播放的装置的编码 MID 411 被提供给作为主机(播放设备)的仅用于记录 / 播放的装置。

[0322] 在步骤 S322 中,作为主机(播放设备)的仅用于记录 / 播放的装置应用该装置本身中包含的对应于仅用于记录 / 播放的装置的解码算法来对从介质(存储器卡)接收到的仅用于记录 / 播放的装置的编码 MID 411 进行解码,并获得介质 ID (MID) 431。

[0323] 另一方面,在(2) 主机 =PC 和便携式终端的情况中,在步骤 S331 中,介质(存储器卡)执行对应于 PC 和便携式终端的介质(MID)的编码处理(编码)。充当该编码结果的 PC/ 便携式终端编码 MID 412 被提供给作为主机(播放设备)的 PC 或便携式终端。

[0324] 在步骤 S332 中,作为主机(播放设备)的 PC 或便携式终端应用装置本身所包含的对应于 PC 和便携式终端的解码算法来对从介质(存储器卡)接收到的 PC/ 便携式终端编码 MID 412 进行解码,并获得介质 ID (MID) 431。

[0325] 介质(存储器卡)被配置为执行用于执行介质(MID)的编码处理(编码)的不同的多个编码算法,并选择性地根据主机(播放设备)的类型来应用编码算法,例如,在主机 = 仅用于记录 / 播放的装置的情况中,应用第一编码算法,并且,在主机 =PC 或便携式终端的情况中,应用第二编码算法。

[0326] 将参考图 18 对在根据这样的主机(播放设备)的类型执行介质 ID (MID)编码处理的情况中的内容解码 / 播放序列进行描述。

[0327] 图 18 是用于以与之前用图 16 描述的方式相同的方式描述介质 ID (MAC) 的验证和应用标题密钥的加密内容解密处理的序列的示图。

[0328] 图 18 以与图 16 相同的方式示出其中存储有加密内容等的介质(存储器卡)320 和用于执行存储在介质(存储器卡) 320 中的加密内容的解密 / 播放的主机(播放设备) 350。

[0329] 如图中所示,下列数据被存储在介质(存储器卡)320 中 :介质 ID-MAC 321、介质 ID (MID) 322、转换标题密钥(XORed 标题密钥) 323、使用控制信息(使用规则) 324 和加密内容

(Encrypted Content)325。

[0330] 请注意，虽然在介质(存储器卡)320 中还存储有各种类型的数据，但是仅示出了要被应用于介质 ID (MAC)的验证和应用标题密钥的加密内容解密处理的序列的数据。

[0331] 以之前参考图 16 描述的方式相同的方式，转换标题密钥(XORed 标题密钥)323 是标题密钥的转换数据，并存储在存储器卡的保护区域(Protected Area)中。具体地说，标题密钥数据与使用控制信息(使用规则)324 的散列值之间的异或(XOR)结果作为转换标题密钥被存储。

[0332] 首先，在步骤 S331 中，介质(存储器卡)320 根据用于执行内容重放的主机(播放设备)的类型来执行介质 ID (MID)322 的编码处理。

[0333] 请注意，作为该处理的前提，介质(存储器卡)320 和主机(播放设备)350 已经执行了相互认证处理，并且在执行该相互认证的处理时，介质(存储器卡)320 已经从主机(播放设备)350 接收了主机证书(Host Cert)。就主机证书(Host Cert)而言，如之前参考图 7 和图 8 所描述的，类型信息被记录，并且在其类型信息中记录指示装置的类型的装置类型信息。

[0334] 介质(存储器卡)320 参考从主机(播放设备)350 接收到的主机证书(Host Cert)中记录的类型信息(装置类型信息)来确认主机(播放设备)的类型。根据该装置类型的确认，确定介质 ID (MID)的编码(Encode)模式(编码算法)，并根据确定的编码(Encode)模式(编码算法)执行介质 ID (MID)的编码处理。

[0335] 介质(存储器卡)320 将在步骤 S331 中生成的对应于装置类型的编码介质 ID(MID)提供给主机(播放设备)350。

[0336] 在步骤 S351 中，主机(播放设备)350 执行从介质(存储器卡)320 接收的编码介质 ID (MID)的解码处理(Decode)。主机(播放设备)350 包括与其装置类型相应的解码程序或解码器，应用与其装置类型相应的解码程序或解码器来执行编码介质 ID (MID)的解码处理(Decode)。

[0337] 在主机(播放设备)350 是仅用于记录 / 播放的装置的情况中，仅用于记录 / 播放的装置保持与仅用于记录 / 播放的装置相关联的解码程序或解码器，并执行已经应用了该解码程序或解码器的处理。此外，在主机(播放设备)350 是诸如平板终端等的 PC 或者便携式终端的情况中，PC 或便携式终端保持与 PC 或便携式终端相关联的解码程序或解码器，并执行已经应用了该解码程序或解码器的处理。

[0338] 主机(播放设备)350 通过在步骤 S351 中的解码处理获得介质 ID (MID)。

[0339] 请注意，例如，尽管主机(播放设备)350 是 PC，但是，例如，在通过模仿仅用于记录 / 播放的装置来非法地转移用于记录 / 播放的装置的主机证书(Host Cert)以执行处理的事件中，PC 不能获得介质 ID (MID)，并且其后不能执行内容重放。这是由于，在这种情况中，介质(存储器卡)提供的介质 ID (MID)可以由仅用于记录 / 播放的装置单独保持的解码程序或解码器单独地解码并获得。

[0340] 在主机(播放设备)350 获得介质 ID (MID)后的处理，即，在步骤 S352 到 S356 中的处理与之前参考图 16 描述的步骤 S301 到 S305 中的处理相同。

[0341] 在步骤 S352 中，主机(播放设备)350 从介质(存储器卡)320 读出使用控制信息(使用规则)324，并计算其散列值，例如，根据 AES 加密算法执行散列值计算。

[0342] 接下来，在步骤 S353 中，主机（播放设备）350 根据诸如访问特权的确认等的预定过程计算读出的使用控制信息（使用规则）324 的散列值与转换标题密钥（XORed 标题密钥）323 之间的异或（XOR）。根据该处理，生成标题密钥。

[0343] 接下来，在步骤 S354 中，主机（播放设备）350 通过应用在步骤 S353 中生成的标题密钥来对从介质（存储器卡）320 读出的介质 ID（MID）322 执行 MAC 计算。

[0344] 接下来，在步骤 S355 中，主机（播放设备）350 执行从介质（存储器卡）320 读出的介质 ID-MAC 321 与在步骤 S354 中计算的 MAC 值之间的匹配处理。

[0345] 就该匹配处理而言，当从介质（存储器卡）320 读出的介质 ID-MAC 321 与在步骤 S354 中计算的 MAC 值匹配时，MAC 匹配成立，确定对介质（存储器卡）320 的有效性已经进行确认，并且流程前进到在步骤 S356 中的应用标题密钥的加密内容解密处理。

[0346] 另一方面，就在步骤 S355 中的匹配处理而言，当从介质（存储器卡）320 读出的介质 ID-MAC 321 与在步骤 S354 中计算的 MAC 值不匹配时，MAC 匹配不成立，确定对介质（存储器卡）320 的有效性尚未进行确认，并且不执行在步骤 S356 中的应用标题密钥的加密内容解密处理。

[0347] 请注意，该内容使用被要求根据从介质（存储器卡）320 读出的使用控制信息的规则（使用规则）324 作为使用模式来执行。

[0348] 以这种方式，就本实施例而言，介质（存储器卡）判别主机（播放设备）的类型，并根据判别的主机类型，介质 ID 的转换模式被改变并被提供给主机。主机利用装置本身中包含的对应于装置类型的解密算法来获得介质 ID（MID）。根据这样的布置，介质（存储器卡）可以根据主机（播放设备）的类型执行处理控制。

[0349] 接下来，将参考图 19 到图 21 中示出的流程图描述根据本实施例的内容重放处理序列。也就是说，这些流程图是用于描述与主机（播放设备）类型相应的伴随着介质 ID（MID）的转换处理的内容重放处理序列的流程图。

[0350] 在图 19 到图 21 中示出的流程图顺序地示出了在左侧的用于执行内容重放的主机（播放设备）和在右侧的其中存储有加密内容和标题密钥的介质（存储器卡），并顺序地示出由这两个装置执行的处理。将描述各步骤的处理的细节。

[0351] 在步骤 S511 中，其上安装有介质（存储器卡）的主机（播放设备）输入要被播放的内容的选择信息。例如，主机（播放设备）在主机的显示器上显示存储在存储器卡中的内容的列表，并且用户从显示的内容列表选择要播放的内容，从而，主机的数据处理部分识别用户指定的选择的内容。

[0352] 在步骤 S512 中，主机根据选择的内容的类型来激活播放程序。

[0353] 就本处理例子而言，内容的类型是下面（a）和（b）之一。

[0354] （a）普通内容，和

[0355] （b）高附加值内容

[0356] 具体地说，主机保持用于执行普通内容的重放处理的普通内容播放程序和用于执行高附加值内容的重放处理的高附加值内容播放程序，并激活对应于被选作要被播放的对象的内容的类型的播放程序。

[0357] 请注意，虽然主机可以仅具有普通内容播放程序，但是这样的主机不能执行高附加值内容的重放处理。此外，高附加值内容播放程序可以被设置为仅播放高附加值内容，或

者可以被设置为能够播放高附加值内容和普通内容两者的程序。

[0358] 接下来，在步骤 S513 中，主机从装置本身的存储器获得与根据内容的类型激活的播放程序相关联的装置证书（Host Cert）。该装置证书（Host Cert）是之前参考图 7 描述的主机证书（Host Cert），并且是其中记录有下列信息作为类型信息的证书：

[0359] （1a）装置类型信息

[0360] （1b）对应的内容类型信息。

[0361] 请注意，例如，在图 7 中的（B）中示出的，普通内容播放程序可以获得单独地对应于普通内容的主机证书，在图 7 中的（A）中示出的，高附加值内容播放程序可以获得单独地对应于高附加值内容和普通内容的主机证书。例如，就用于获得记录在每一个播放程序中的主机证书的信息（例如，存储器地址）而言，仅记录了对应于图 7 中的（A）和（B）中的任意一个的主机证书的信息（地址），每一个播放程序都可以获得可以由该程序本身使用的唯一的主机证书。

[0362] 接下来，在步骤 S514a 和 S514b 中，执行在主机（播放设备）与介质（存储器卡）之间的相互认证处理。就该相互认证处理而言，主机（播放设备）将从主机的存储器获得的主机证书（Host Cert）发送到介质（存储器卡）。

[0363] 另一方面，介质（存储器卡）将存储在介质（存储器卡）内的存储器中的介质的装置证书（Media Cert）发送到主机（播放设备）。例如，该认证处理作为已经应用了这两种公共密钥证书的公共密钥密码系统的相互认证处理被执行。

[0364] 接下来，将描述在图 20 中示出的步骤 S515a 和 S515b 及其后面的步骤中的处理。

[0365] 在步骤 S515a 和 S515b 中，对主机（播放设备）与介质（存储器卡）之间的相互认证是否已经建立进行确定。

[0366] 在没有建立相互认证的情况中，确定两装置之间的可靠性未被确认，流程前进到步骤 S530，并停止内容重放处理。

[0367] 在相互认证已经建立的情况中，在步骤 S516 中，介质（存储器卡）基于包含在装置证书（Host Cert）的类型信息中的装置类型信息来判别主机（播放设备）的类型。例如，介质（存储器卡）判别装置类型，从而主机为仅用于记录 / 播放的装置、PC 或者诸如平板终端等的便携式终端。

[0368] 接下来，在步骤 S517 中，介质（存储器卡）根据编码（Encode）算法执行介质 ID（MID）的编码处理，该编码（Encode）算法已经根据基于装置证书（Host Cert）判别的主机（播放设备）的类型（例如，仅用于记录 / 播放的装置、PC 或者平板终端）预先与装置类型相关联地被设置。

[0369] 介质（存储器卡）被配置为选择性地执行多个编码算法，并通过根据主机（播放设备）的类型从这多个编码算法中选择一个来执行对介质 ID（MID）的编码（Encode）。

[0370] 接下来，在步骤 S518a 中，介质（存储器卡）将编码的介质 ID（MID）发送到主机（播放设备）。

[0371] 在步骤 S518b，主机（播放设备）从介质（存储器卡）接收编码的介质 ID（MID）。

[0372] 接下来，在图 21 中示出的步骤 S519 中，主机（播放设备）应用装置本身可以执行的仅用于该装置的解码算法来执行编码的介质 ID（MID）的解码（decode）。

[0373] 当在步骤 S520 中确定解码失败的情况中，流程前进到步骤 S530，并停止内容重放

处理。

[0374] 当在步骤 S520 中确定解码成功，并且成功获得介质 ID（MID)的情况中，流程前进到步骤 S521。

[0375] 在步骤 S521a 中，介质(存储器卡）执行用于提供用于内容重放的数据的处理。具体地说，该数据的例子包括存储在保护区域中的标题密钥，以及存储在通用区域中的加密内容。

[0376] 在步骤 S521b，主机(播放设备）从介质(存储器卡）接收标题密钥、加密内容等。

[0377] 最后，主机(播放设备）使用从介质(存储器卡）接收的标题密钥执行加密内容的解密处理，以执行内容重放。

[0378] 请注意，虽然在步骤 S518a 到 S522 中的处理在本流程中以简化的方式示出，但是这些处理对应于之前参考图 18 描述的处理，其中，执行诸如介质 ID 的 MAC 验证处理、基于使用控制信息通过计算转换的标题密钥来获得标题密钥等的处理。

[0379] 以这种方式，介质(存储器卡）通过根据执行内容重放的主机(播放设备）改变介质 ID（MID)的转换模式来执行内容重放。根据该处理，只有在主机(播放设备）的类型与主机(播放设备）呈现的主机证书的类型信息之间的匹配已经被确认的情况下，才可以执行内容重放。

[0380] 此外，介质(存储器卡）可以基于主机证书(Host Cert）确认主机(播放设备）的类型，并且还可以根据主机(播放设备)执行内容使用控制。例如，可以进行这样的设置，其中，可以执行与主机(播放设备）的类型相应的内容使用控制，从而使得特定内容的使用单独地在仅用于记录 / 播放的装置处被允许，而在 PC 和便携式终端处不允许。

[0381] 请注意，就图 19 到图 21 中的流程图而言，以与参考图 9 到图 11 描述的方式相同的方式，虽然进行了这样的布置，其中在步骤 S512 中激活与选择的内容的类型相应的播放程序并且选择与播放程序相关联的主机证书(Host Cert)，但是也可以进行这样的布置，其中，与参考图 12 到图 14 描述的流程一样，内容播放程序本身根据内容类型来选择主机证书。

[0382] 此外，上述多个实施例，即 :(第一实施例）根据内容类型选择性地激活播放程序并使用与激活的播放程序相关联的主机证书(HostCert）的处理，(第二实施例）播放程序根据内容类型选择性地使用主机证书(Host Cert）的处理，以及(第三实施例）根据主机(播放设备)的类型改变介质 ID（MID)的转换模式的处理，这些处理可以被布置为独立地执行，或者可以被布置为作为第一实施例与第三实施例之间的组合或者第二实施例与第三实施例之间的组合来执行。

[0383] 6. 每个装置的硬件配置例子

[0384] 最后，将参考图 22 和图 23 描述用于执行上述处理的装置的硬件配置例子。

[0385] 首先，将参考图 22 描述用于执行数据记录 / 重放处理的其上安装有存储器卡的主机装置的硬件配置例子。

[0386] CPU（中央处理单元）701 充当用于根据存储在 ROM（只读存储器）702 或存储单元 708 中的程序执行各种类型的处理的数据处理部分。例如，CPU 701 执行从广播电台或服务器接收内容的内容接收处理，将接收到的数据记录到存储器卡(在图中的可移动介质 711）的记录处理，从存储器卡(在图中的可移动介质 711)重放数据的数据重放处理等。CPU 701

执行的程序、数据等被适当地存储在 RAM(随机存取存储器)703 中。这些 CPU 701、ROM 702 和 RAM 703 由总线 704 相互连接。

[0387] CPU 701 经由总线 704 连接到输入 / 输出接口 705，并且由各种类型的开关、键盘、鼠标、传声器等构成的输入单元 706，以及由显示器、扬声器等构成的输出单元 707 被连接到输入 / 输出接口 705。CPU701 执行对应于从输入单元 706 输入的命令的各种类型的处理，并将处理结果输出到例如输出单元 707。

[0388] 连接到输入 / 输出接口 705 的存储单元 708 由例如硬盘等构成，并且存储 CPU 701 执行的程序和各种类型的数据。通信单元 709 经由诸如互联网或局域网等的网络与外部装置通信。

[0389] 连接到输入 / 输出接口 705 的驱动器 710 驱动例如磁盘、光盘、磁光盘或诸如存储器卡等的半导体存储器的可移动介质 711，以获得诸如记录内容、密钥信息等的各种类型的数据。例如，根据 CPU 执行的播放程序使用获得的内容和密钥数据来执行内容解密 / 重放处理等。

[0390] 图 23 示出了存储器卡的硬件配置例子。CPU（中央处理单元）801 充当用于根据存储在 ROM（只读存储器)802 或存储单元 807 中的程序执行各种类型的处理的数据处理部分。例如，CPU 801 执行已经通过上述实施例进行了描述的服务器或主机装置之间的通信处理、对存储单元 807 的数据的写入或读取等的处理、以存储单元 807 的保护区域 811 的分区区域为单位的可访问 / 不可访问的确定处理等。CPU801 执行的程序、数据等被适当地存储在 RAM（随机存取存储器)803 中。这些 CPU 801、ROM 802 和 RAM 803 由总线 804 相互连接。

[0391] CPU 801 经由总线 804 连接到输入 / 输出接口 805，并且通信单元 806 和存储单元 807 被连接到输入 / 输出接口 805。

[0392] 例如，连接到输入 / 输出接口 805 的通信单元 804 执行与服务器或主机的通信。如之前在上文中所描述的，存储单元 807 是数据存储区域，并且，包括具有访问特权的保护区域(Protected Area)811、其中可以自由地执行数据记录 / 读取的通用区域(General Purpose Area)812。

[0393] 请注意，例如，服务器可以使用具有与在图 22 中示出的主机装置相同的硬件配置的装置来实现。

[0394] 7. 本公开的配置的概要

[0395] 已经参考特定实施例对本公开的实施例进行了详细描述。但是，显而易见的是，本领域技术人员在不脱离本公开的本质的情况下可以想到各种修改或替换。也就是说，已经以示例的方式对本公开进行了描述，其不应以限制性的方式被解释。为了确定本公开的本质，应当参考权利要求书。

[0396] 请注意，在本说明书中公开的技术可以具有下列布置。

[0397] (1) 一种信息处理系统，包括 ：

[0398] 介质，存储有充当要被播放的对象的内容 ；以及

[0399] 播放设备，被配置用来播放存储在所述介质中的内容，

[0400] 其中，所述播放设备被配置用来

[0401] 判别被选作要被播放的对象的内容的内容类型，

[0402] 从存储单元选择性地获得与判别的内容类型相关联的装置证书，以及

[0403] 将选择性地获得的装置证书发送到所述介质；

[0404] 所述装置证书是关于内容类型的装置证书，其中记录有可以利用该装置证书的内容类型信息；并且

[0405] 所述介质确定已经从所述播放设备对其执行了读取请求的加密密钥是否是用于解密与记录在所述装置证书中的可用内容类型匹配的加密内容的加密密钥，并仅在匹配的情况下允许读出该加密密钥。

[0406] (2)根据(1)的信息处理系统，其中，所述播放设备执行不依赖于内容类型的内容播放程序，并根据该内容播放程序判别被选作要被播放的对象的内容的类型。

[0407] (3)根据(1)或(2)的信息处理系统，其中，所述装置证书具有这样的结构：其中，高附加值内容和除高附加值内容以外的普通内容中的至少一个作为可以利用该装置证书的内容类型被记录；

[0408] 并且，所述介质确定已经请求了从所述播放设备对其进行读取的加密密钥是否是用于解密与作为记录在所述装置证书中的可用内容类型的高附加值内容或普通内容相匹配的加密内容的加密密钥，并仅仅在匹配的情况下许可读出该加密密钥。

[0409] (4)根据(1)到(3)中的任意一个的信息处理系统，其中，所述播放设备发送获得的装置证书以执行认证处理；

[0410] 并且，在将所述认证处理的成立作为条件的情况下，所述介质执行来自所述播放设备的加密密钥读出请求的许可确定处理。

[0411] (5)根据(1)到(4)中的任意一个的信息处理系统，其中，根据与被选作要被播放的对象的内容相关联的属性信息，所述播放设备判别选择的内容的类型，并从存储单元选择性地获得与判别的内容类型相关联的装置证书。

[0412] (6)根据(1)到(5)中的任意一个的信息处理系统，其中，所述介质将加密密钥存储在基于播放设备的访问特权的确认来许可对其进行访问的保护区域中，基于要从所述播放设备接收的装置证书中记录的保护区域访问特权信息来确认存储所述加密密钥的保护区域的访问特权，并在所述播放设备的访问特权被确认的情况下，许可由所述播放设备读出加密密钥。

[0413] (7)根据(1)到(6)中的任意一个的信息处理系统，其中，所述装置证书具有这样的结构：其中，记录有可以利用该装置证书的播放设备类型信息；

[0414] 所述介质根据编码算法执行作为所述介质的标识信息的介质 ID 的编码处理以发送到所述播放设备，所述编码算法是根据所述装置证书中记录的播放设备类型信息来选择的；并且

[0415] 所述播放设备执行伴随着应用了介质 ID 的数据处理的内容的解码或播放，该介质 ID 是通过根据与该设备本身的装置类型相对应的解码算法对从所述介质接收的编码介质 ID 进行解码而获得的。

[0416] (8)一种信息处理装置，包括：

[0417] 数据处理单元，被配置用来执行存储在介质中的内容的读出和重放处理；

[0418] 其中，所述数据处理单元被配置用来

[0419] 判别被选作要被播放的对象的内容的内容类型，

[0420] 选择性地获得与判别的内容类型相关联的装置证书，以将选择性地获得的装置证书发送到所述介质，并且还

[0421] 将加密内容以及要被应用于该加密内容的解密的加密密钥的读出请求输出到所述介质，并且

[0422] 在以通过所述介质进行确认为条件的情况下，从所述介质获得加密密钥，以通过对加密内容应用获得的加密密钥来执行该加密内容的解密，其中，已经对其执行了读出请求的加密密钥是与记录在所述装置证书中的能够使用的内容类型相匹配的内容的加密密钥。

[0423] (9)根据(8)的信息处理装置，其中，所述数据处理单元执行不依赖于内容类型的内容播放程序，并根据该内容播放程序判别被选作要被播放的对象的内容的类型。

[0424] (10)，根据(8)或(9)的信息处理装置，其中，所述装置证书具有这样的结构：其中，高附加值内容和除高附加值内容以外的普通内容中的至少一个作为可以利用该装置证书的内容类型被记录。

[0425] (11)根据(8)到(10)中的任意一个的信息处理装置，其中，所述数据处理单元将获得的装置证书发送到所述介质以执行认证处理。

[0426] (12)根据(8)到(11)中的任意一个的信息处理装置，其中，所述数据处理单元根据与被选作要被播放的对象的内容相关联的属性信息来判别选择的内容的类型。

[0427] (13)根据(8)到(12)中的任意一个的信息处理装置，其中，，所述装置证书具有这样的结构：其中，记录有可以利用该装置证书的播放设备类型信息；

[0428] 所述介质根据编码算法执行作为所述介质的标识信息的介质 ID 的编码处理，以发送到所述信息处理装置，所述编码算法是根据所述装置证书中记录的播放设备类型信息来选择的；并且

[0429] 所述信息处理装置的数据处理单元执行伴随着应用了介质 ID 的数据处理的内容的解码或播放，该介质 ID 是通过根据与该设备本身的装置类型相对应的解码算法对从所述介质接收的编码介质 ID 进行解码而获得的。

[0430] 此外，要在上述装置和系统中执行的处理方法，以及使得该装置和系统执行处理的程序也被包含在了本公开的布置中。

[0431] 此外，在本说明书中描述的一系列处理可以通过硬件或软件或两者的合成布置来执行。在根据软件执行处理的情况中，其中记录有处理序列的程序可以通过被安装在嵌入专用硬件中的计算机内的存储器中来执行，或者可以通过被安装在能够进行各种类型的处理的通用计算机中来执行。例如，该程序可以事先被记录在记录介质中。除了从记录介质安装到计算机中的程序外，程序还可以经由诸如 LAN（局域网）或互联网的网络被接收并安装在诸如内置式硬盘等的记录介质中。

[0432] 请注意，根据本说明书的各种类型的处理不仅包括根据所述序列按时间顺序执行的处理，而且包括不必按时间顺序执行而是根据处理能力或执行该处理的装置的需要并行或单独地执行的处理。此外，就本说明书而言，术语“系统”是多个装置的逻辑组配置，并不限于其中充当部件的装置不被包含在同一壳体中的配置。

[0433] 本公开包含与在 2011 年 8 月 11 提交在日本专利局中的日本在先专利申请 JP 2011-175607 中公开的主题相关的主题，该专利申请的全部内容以引用的方式并入本文中。

[0434] 本领域的技术人员应该理解，可以根据设计要求和其它因素进行各种修改、组合、子组合和替换，只要它们在所附权利要求或其等同物的范围即可。

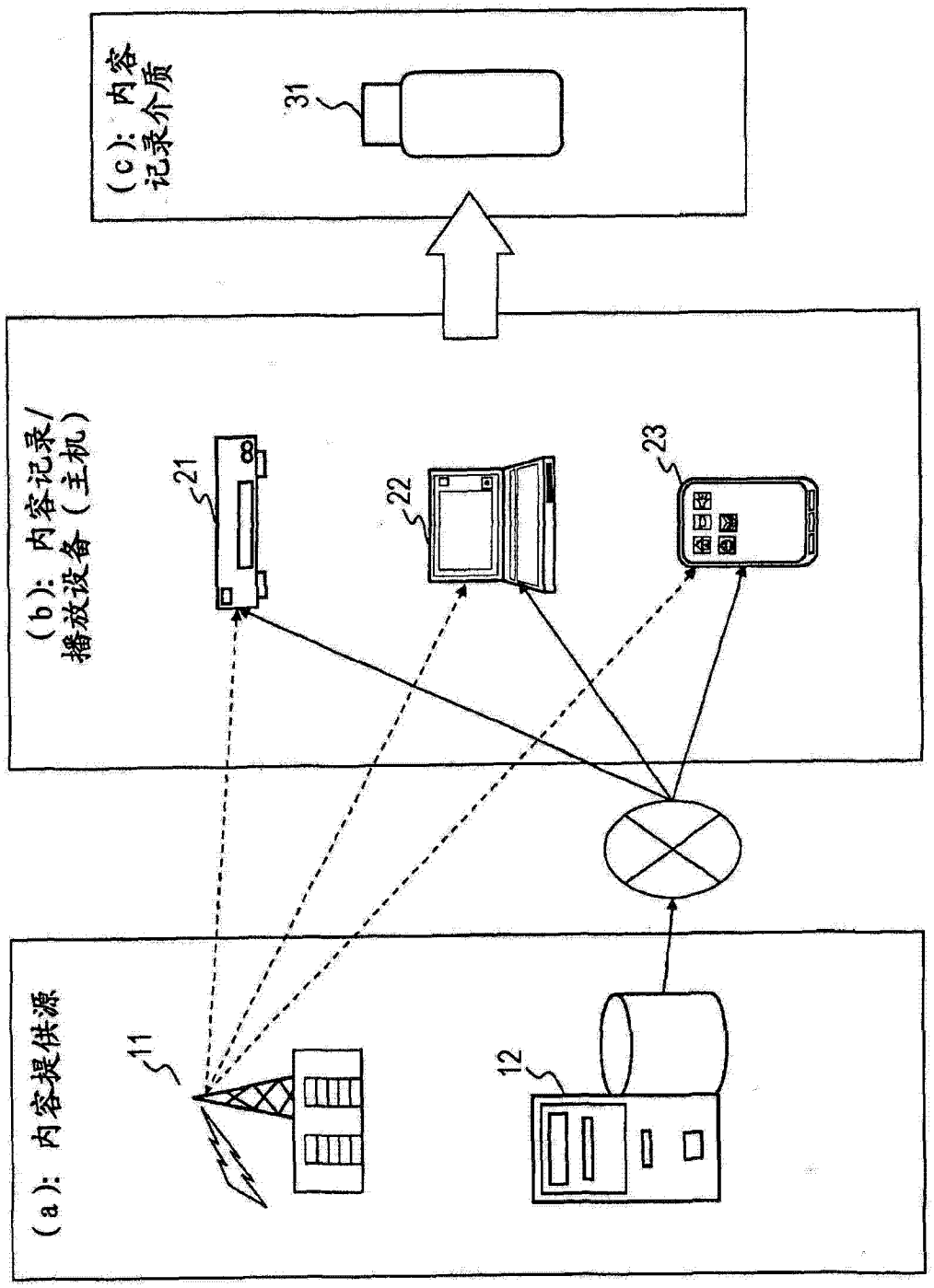


图 1

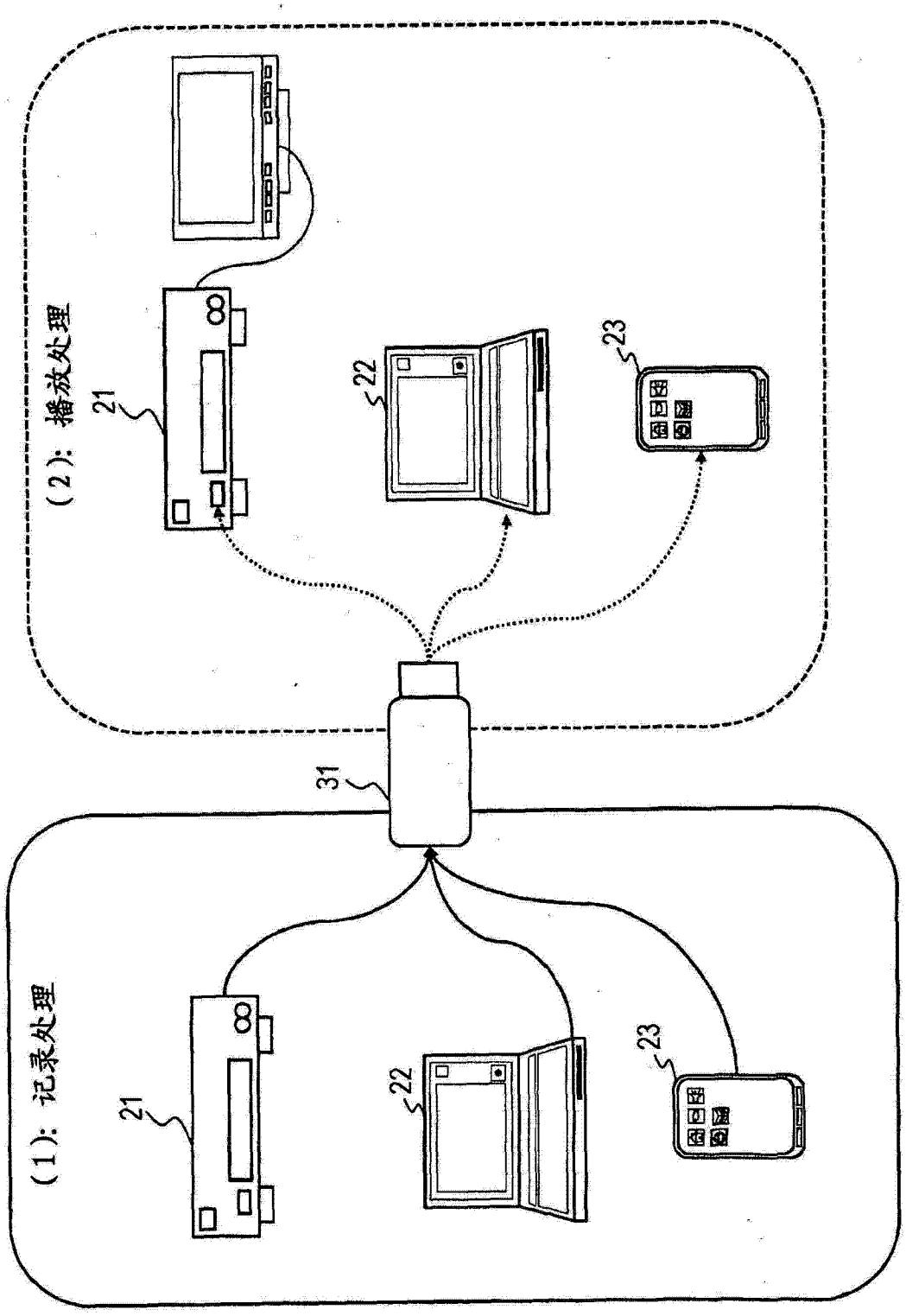


图 2

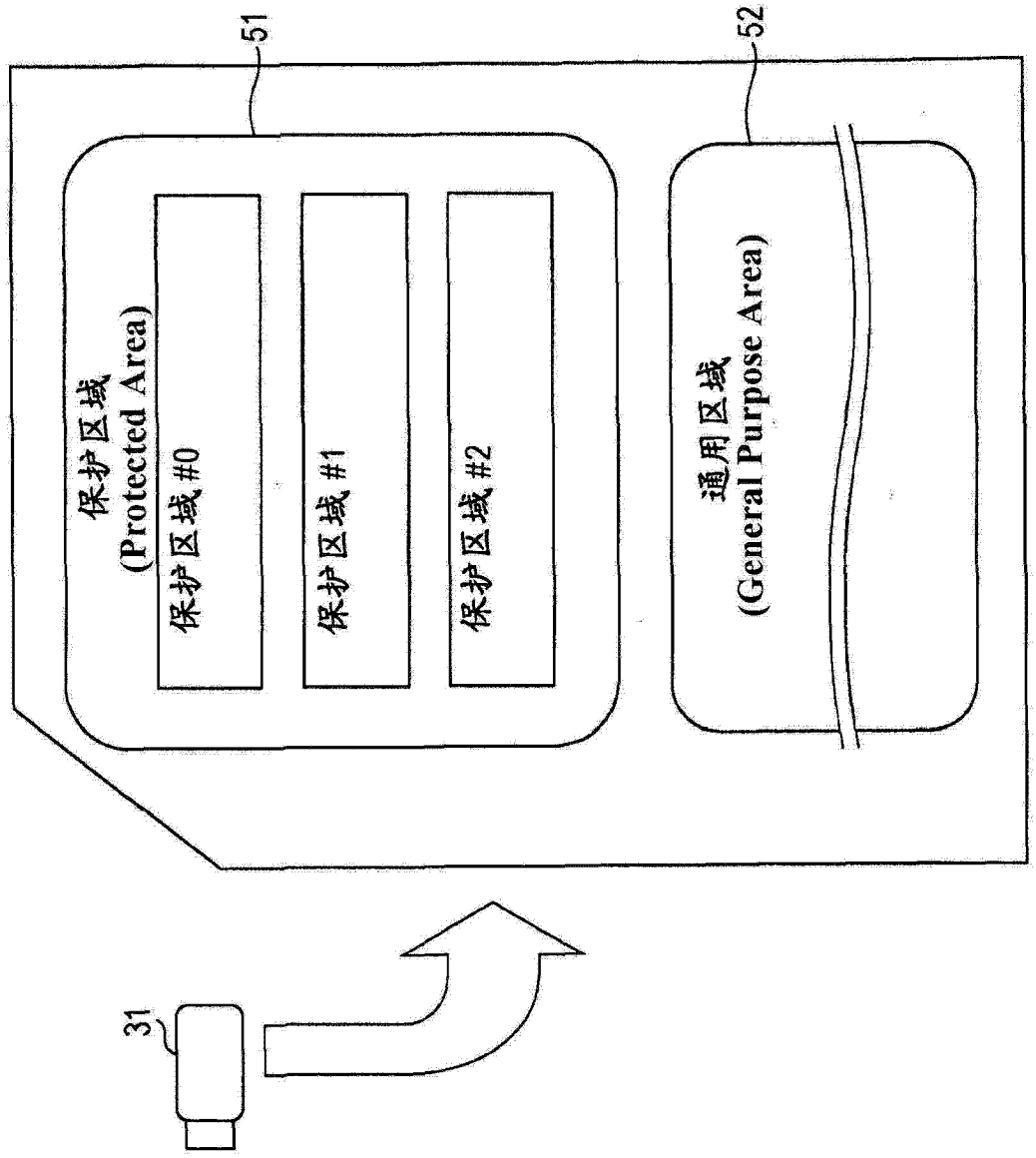

51
52
保护区域
(Protected Area)
保护区域 #0
保护区域 #1
保护区域 #2
通用区域
(General Purpose Area)
31

图 3

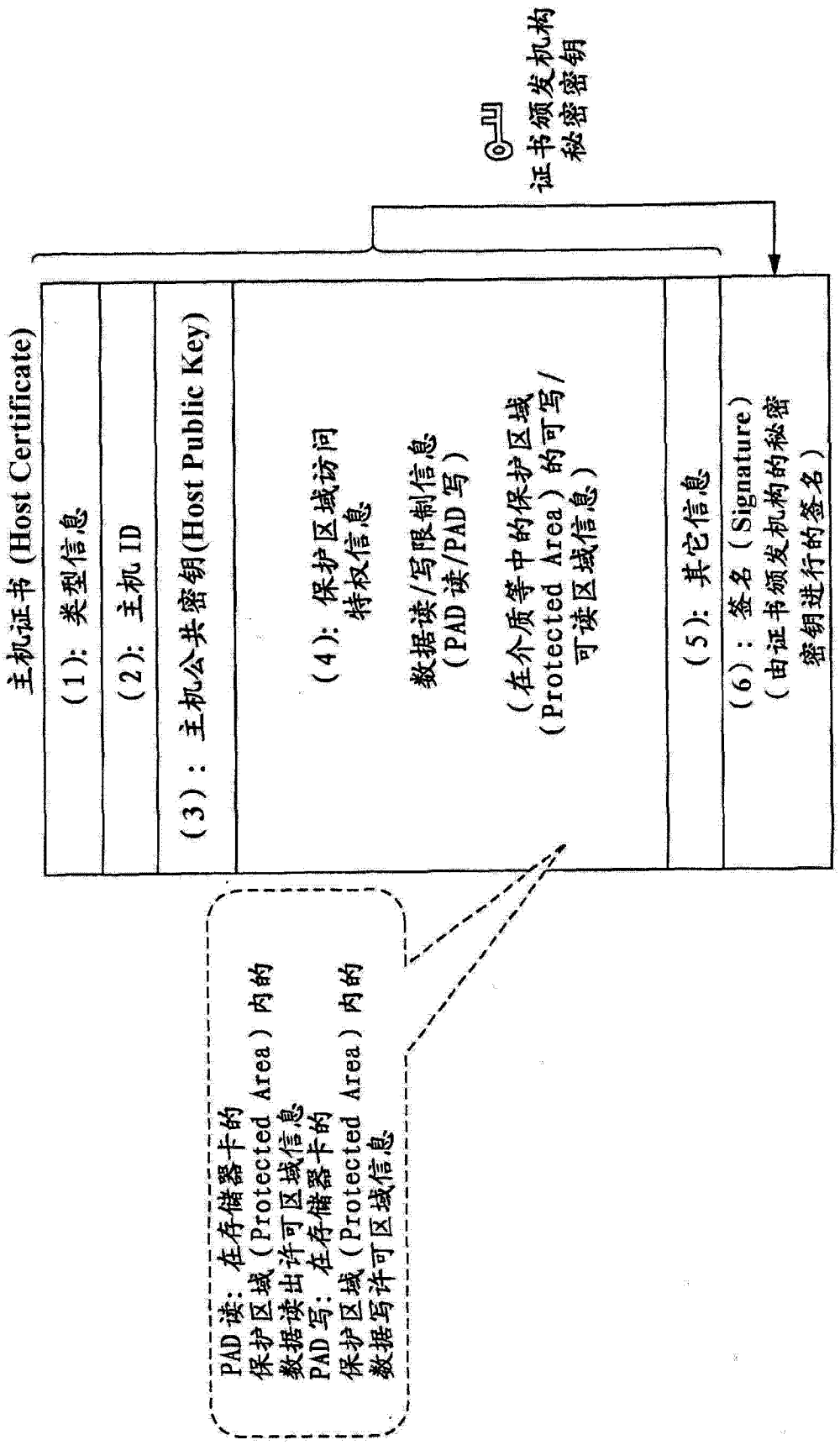

主机证书 (Host Certificate)
(1): 类型信息
(2): 主机 ID
(3): 主机公共密钥(Host Public Key)
(4): 保护区域访问
特权信息
数据读/写限制信息
(PAD 读/PAD 写)
(在介质等中的保护区域
(Protected Area)的可写/
可读区域信息)
(5): 其它信息
(6): 签名 (Signature)
(由证书颁发机构的秘密
密钥进行的签名)
证书颁发机构
秘密密钥
PAD 读: 在存储器卡的
保护区域 (Protected Area) 内的
数据读出许可区域信息
PAD 写: 在存储器卡的
保护区域 (Protected Area) 内的
数据写许可区域信息

图 4

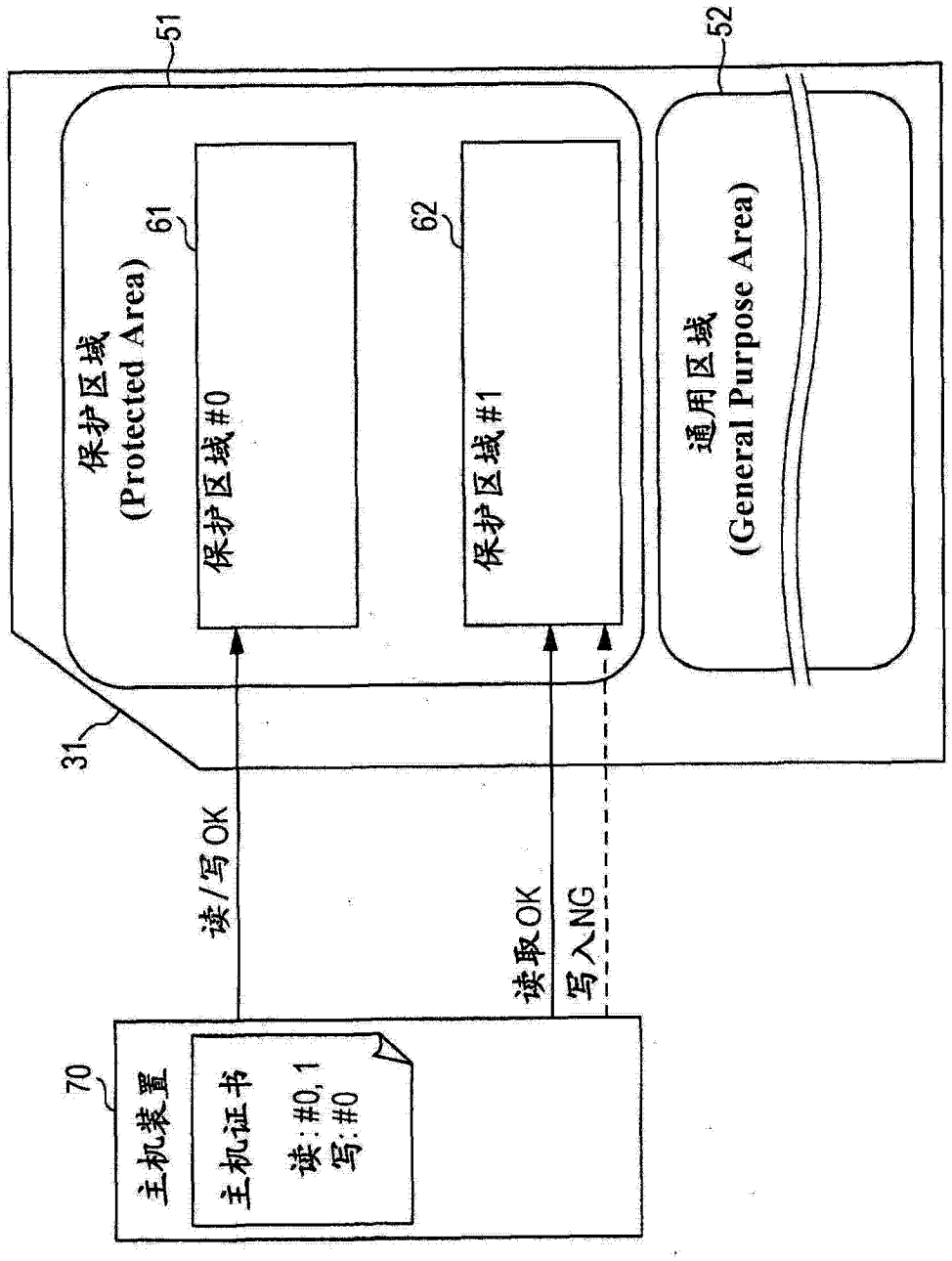

51
52
保护区域
(Protected Area)
61
保护区域#0
62
保护区域#1
通用区域
(General Purpose Area)
31
读/写 OK
读取 OK
写入NG
70
主机装置
主机证书
读:#0, 1
写:#0

图 5

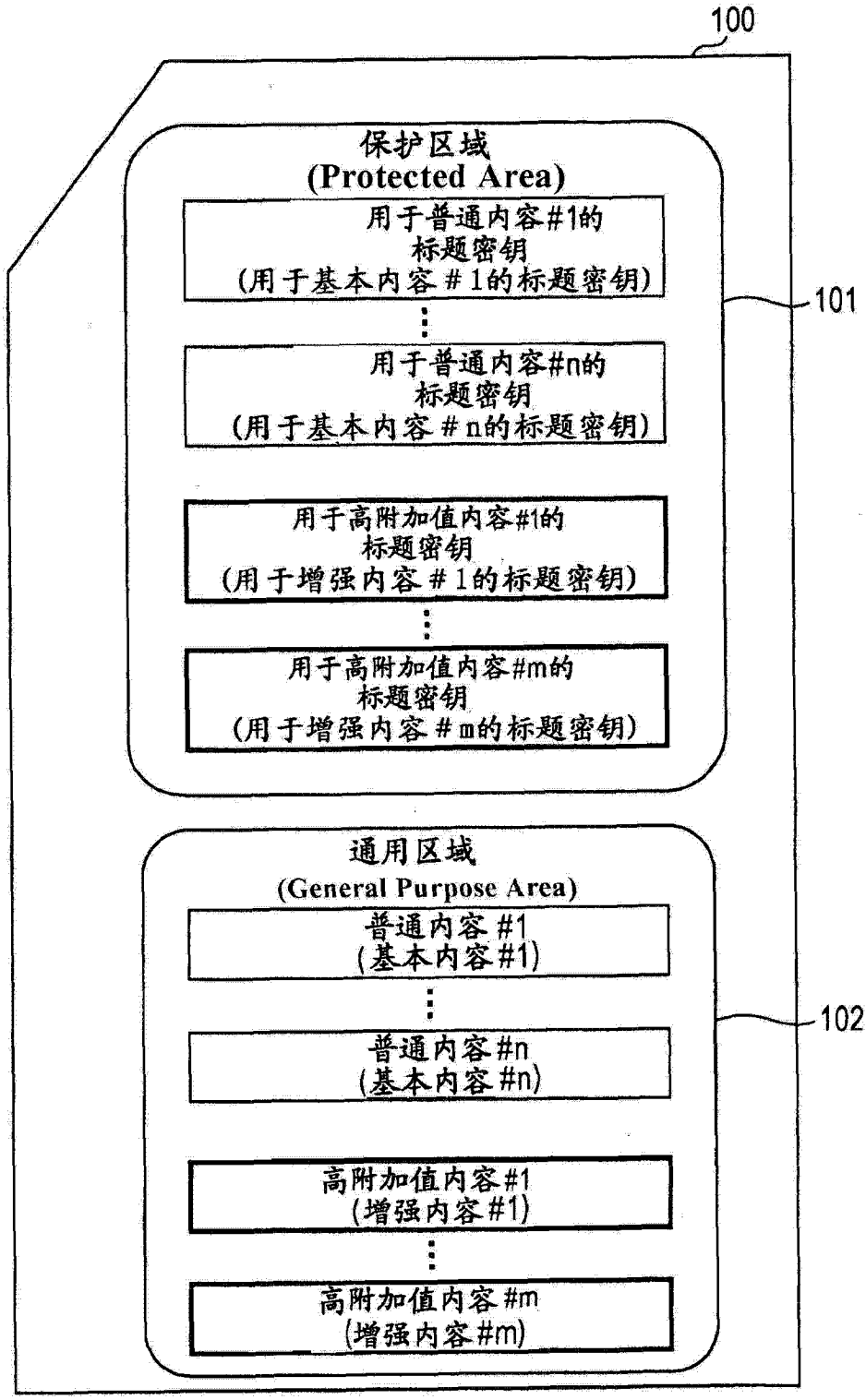

100
保护区域
(Protected Area)
用于普通内容#1的
标题密钥
(用于基本内容＃1的标题密钥)
用于普通内容#n的
标题密钥
(用于基本内容＃n的标题密钥)
用于高附加值内容#1的
标题密钥
(用于增强内容＃1的标题密钥)
用于高附加值内容#m的
标题密钥
(用于增强内容＃m的标题密钥)
101
通用区域
(General Purpose Area)
普通内容 #1
(基本内容#1)
普通内容#n
(基本内容#n)
高附加值内容#1
(增强内容#1)
高附加值内容#m
(增强内容#m)
102

图 6

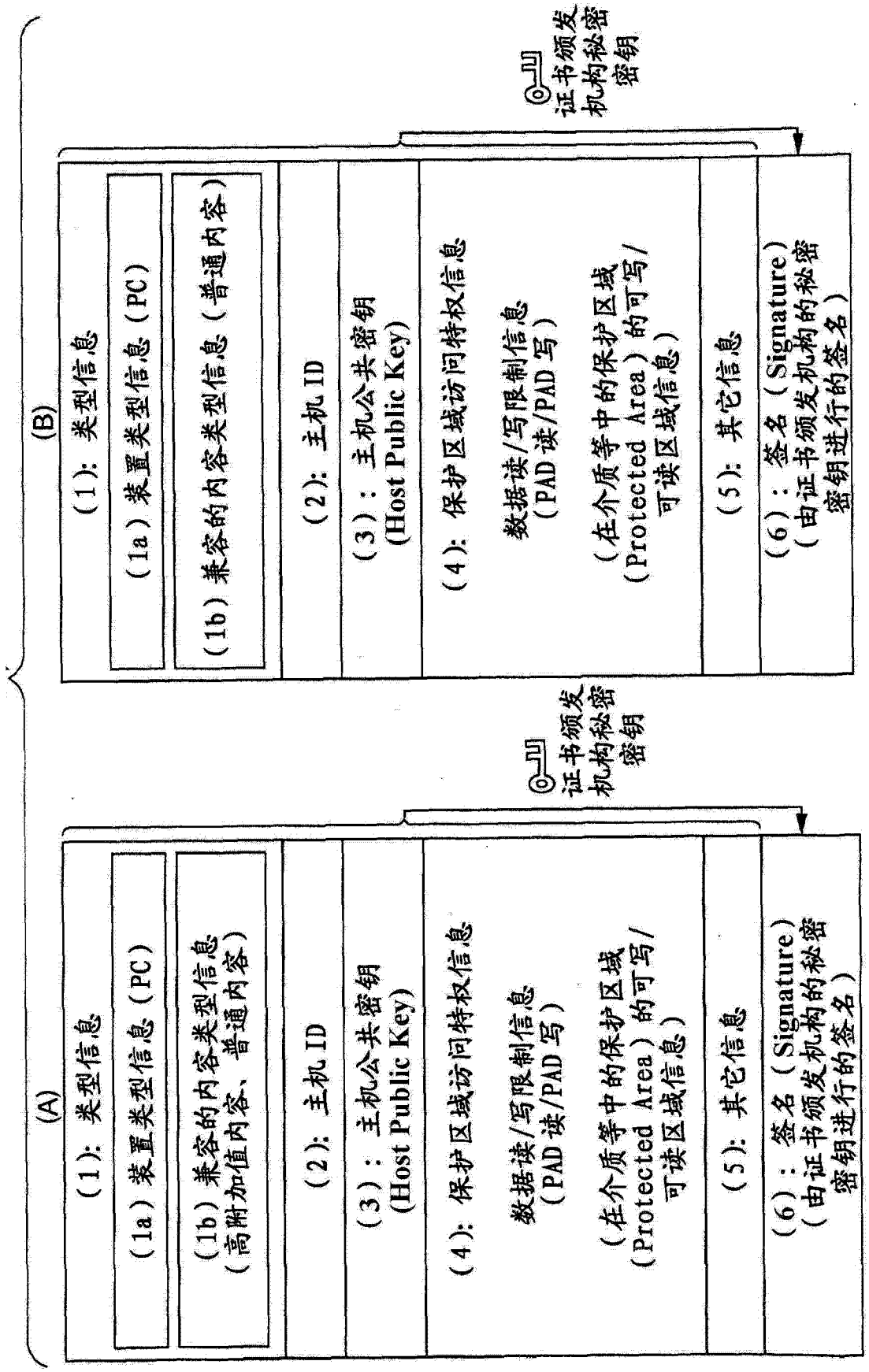

(A)
(1): 类型信息
(1a) 装置类型信息 (PC)
(1b) 兼容的内容类型信息 (高附加值内容、普通内容)
(2): 主机 ID
(3): 主机公共密钥 (Host Public Key)
(4): 保护区域访问特权信息
数据读/写限制信息 (PAD 读/PAD 写)
(在介质等中的保护区域 (Protected Area) 的可写/可读区域信息)
(5): 其它信息
(6): 签名 (Signature) (由证书颁发机构的秘密密钥进行的签名)
证书颁发机构秘密密钥
(B)
(1): 类型信息
(1a) 装置类型信息 (PC)
(1b) 兼容的内容类型信息 (普通内容)
(2): 主机 ID
(3): 主机公共密钥 (Host Public Key)
(4): 保护区域访问特权信息
数据读/写限制信息 (PAD 读/PAD 写)
(在介质等中的保护区域 (Protected Area) 的可写/可读区域信息)
(5): 其它信息
(6): 签名 (Signature) (由证书颁发机构的秘密密钥进行的签名)
证书颁发机构秘密密钥

图 7

（1a）装置类型信息（PC）	（1b）兼容的内容类型信息（高附加值内容、普通内容）
0x0001 （仅用于记录/播放的装置）	0x0001 仅对应于普通内容
	0x0002 仅对应于高附加值内容
	0x0003 对应于高附加值内容和普通内容两者
0x0002 PC/便携式终端	0x0001 仅对应于普通内容
	0x0002 仅对应于高附加值内容
	0x0003 对应于高附加值内容和普通内容两者

图 8

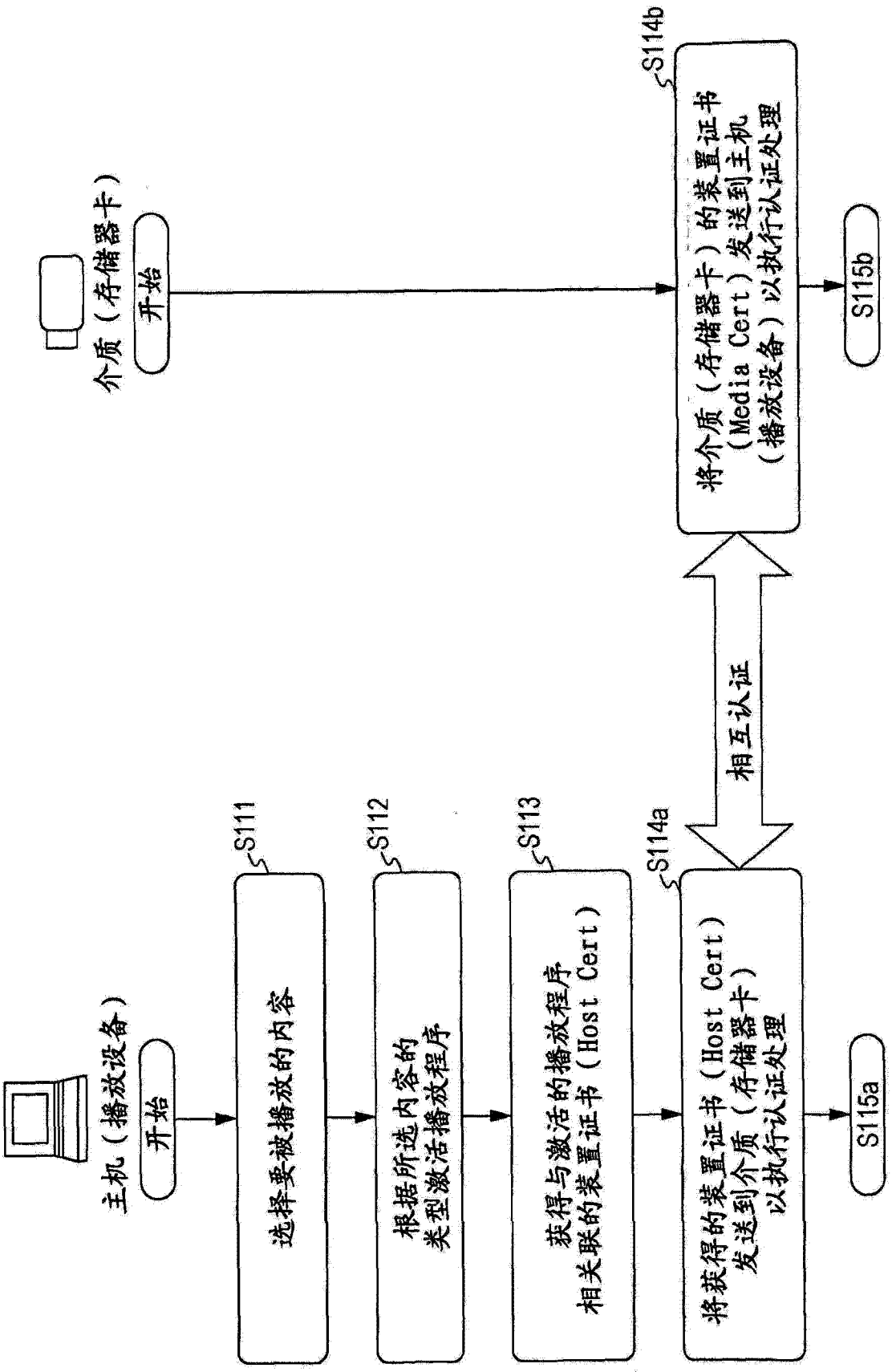

主机（播放设备）
开始
选择要被播放的内容
S111
根据所选内容的
类型激活播放程序
S112
获得与激活的播放程序
相关联的装置证书（Host Cert）
S113
将获得的装置证书（Host Cert）
发送到介质（存储器卡）
以执行认证处理
S114a
S115a
相互认证
介质（存储器卡）
开始
将介质（存储器卡）的装置证书
（Media Cert）发送到主机
（播放设备）以执行认证处理
S114b
S115b

图 9

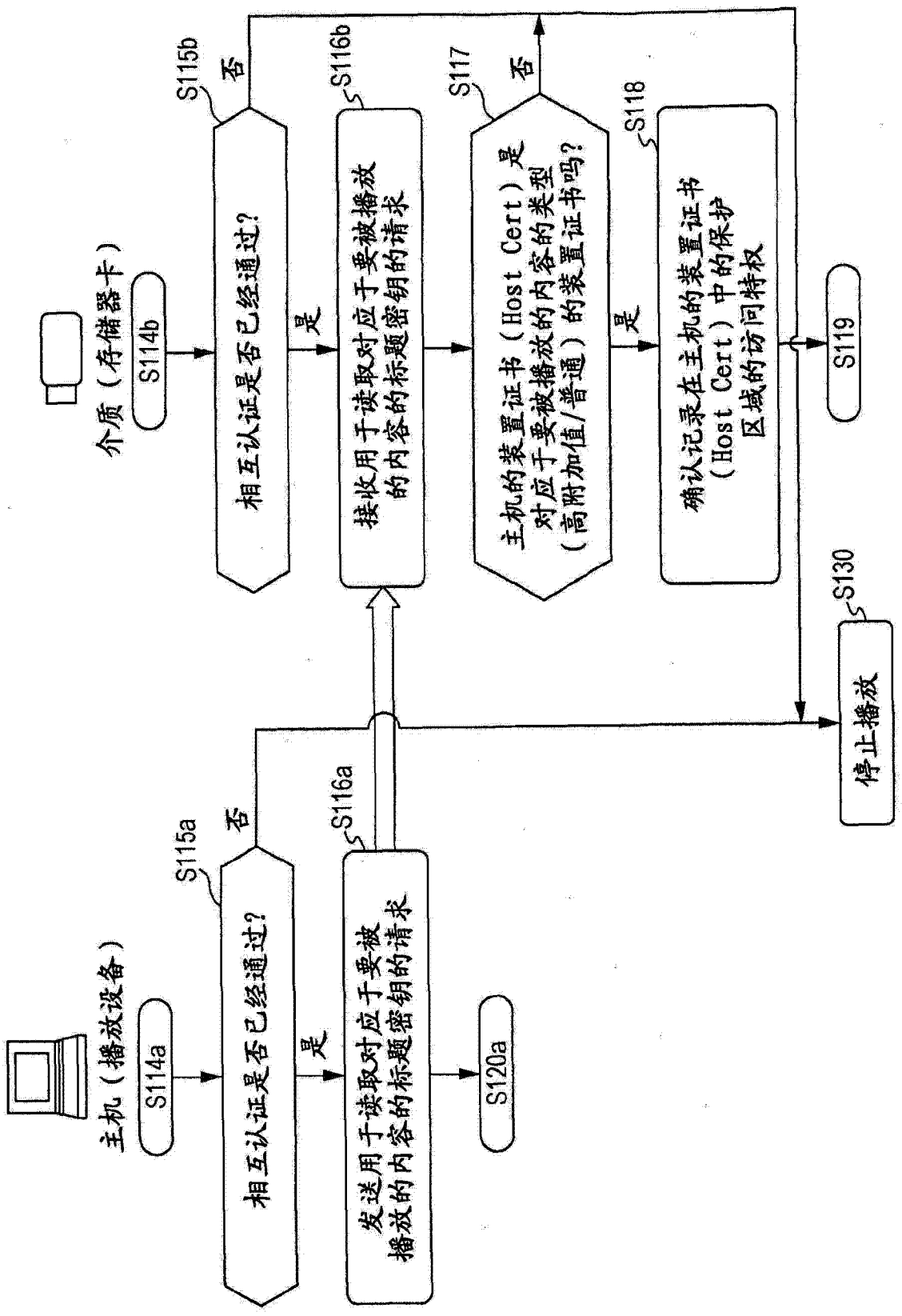

主机（播放设备）
介质（存储器卡）
S114a
S114b
相互认证是否已经通过?
S115a
否
是
S116a
发送用于读取对应于要被播放的内容的标题密钥的请求
S120a
S115b
否
是
S116b
接收用于读取对应于要被播放的内容的标题密钥的请求
S117
否
主机的装置证书（Host Cert）是对应于要被播放的内容的类型（高附加值/普通）的装置证书吗?
是
S118
确认记录在主机的装置证书（Host Cert）中的保护区域的访问特权
S119
S130
停止播放

图 10

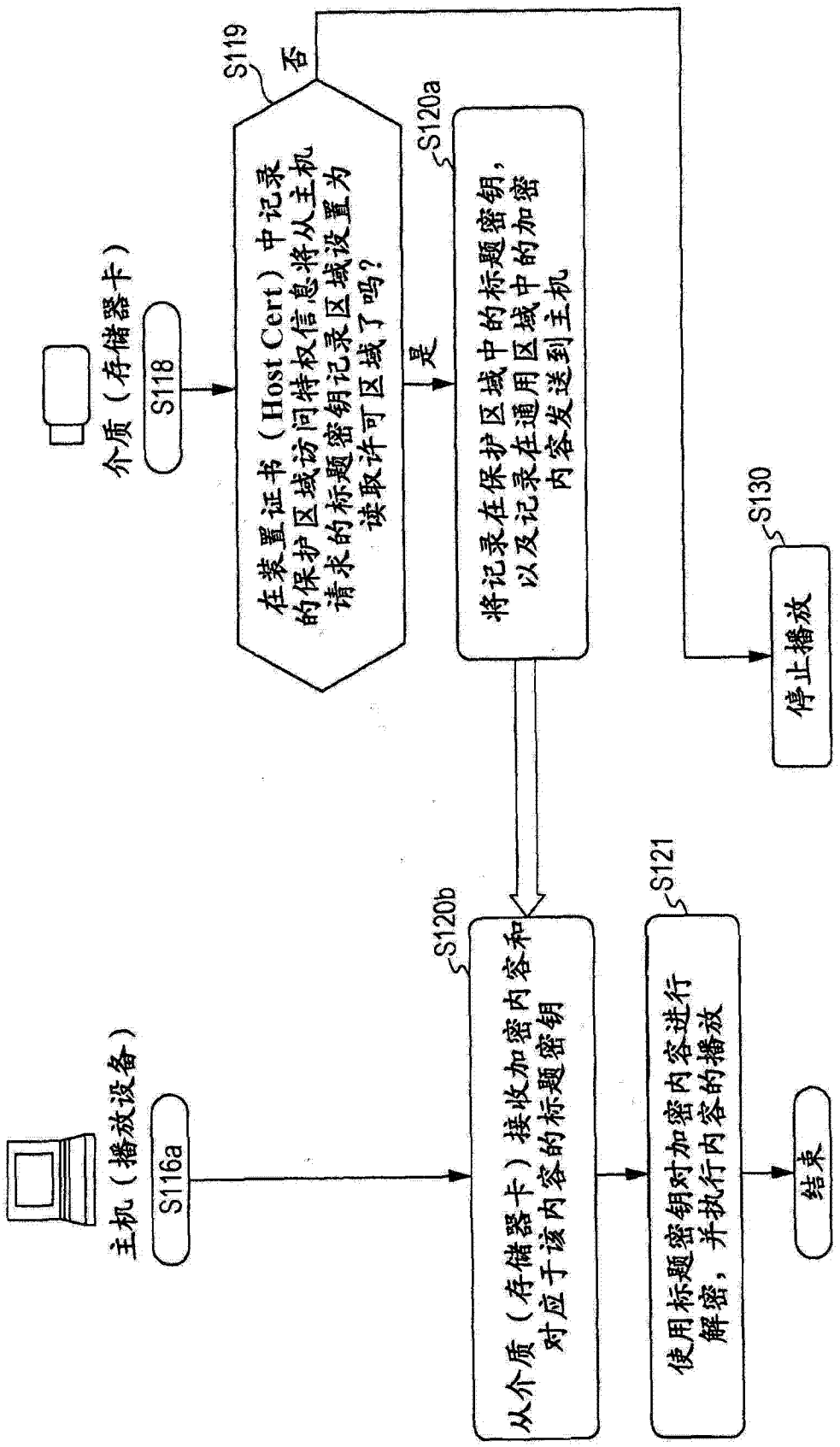

介质（存储器卡）
S118
在装置证书（Host Cert）中记录的保护区域访问特权信息将从主机请求的标题密钥记录区域设置为读取许可区域了吗？
S119
否
是
S120a
将记录在保护区域中的标题密钥，以及记录在通用区域中的加密内容发送到主机
S130
停止播放
主机（播放设备）
S116a
从介质（存储器卡）接收加密内容和对应于该内容的标题密钥
S120b
使用标题密钥对加密内容进行解密，并执行内容的播放
S121
结束

图 11

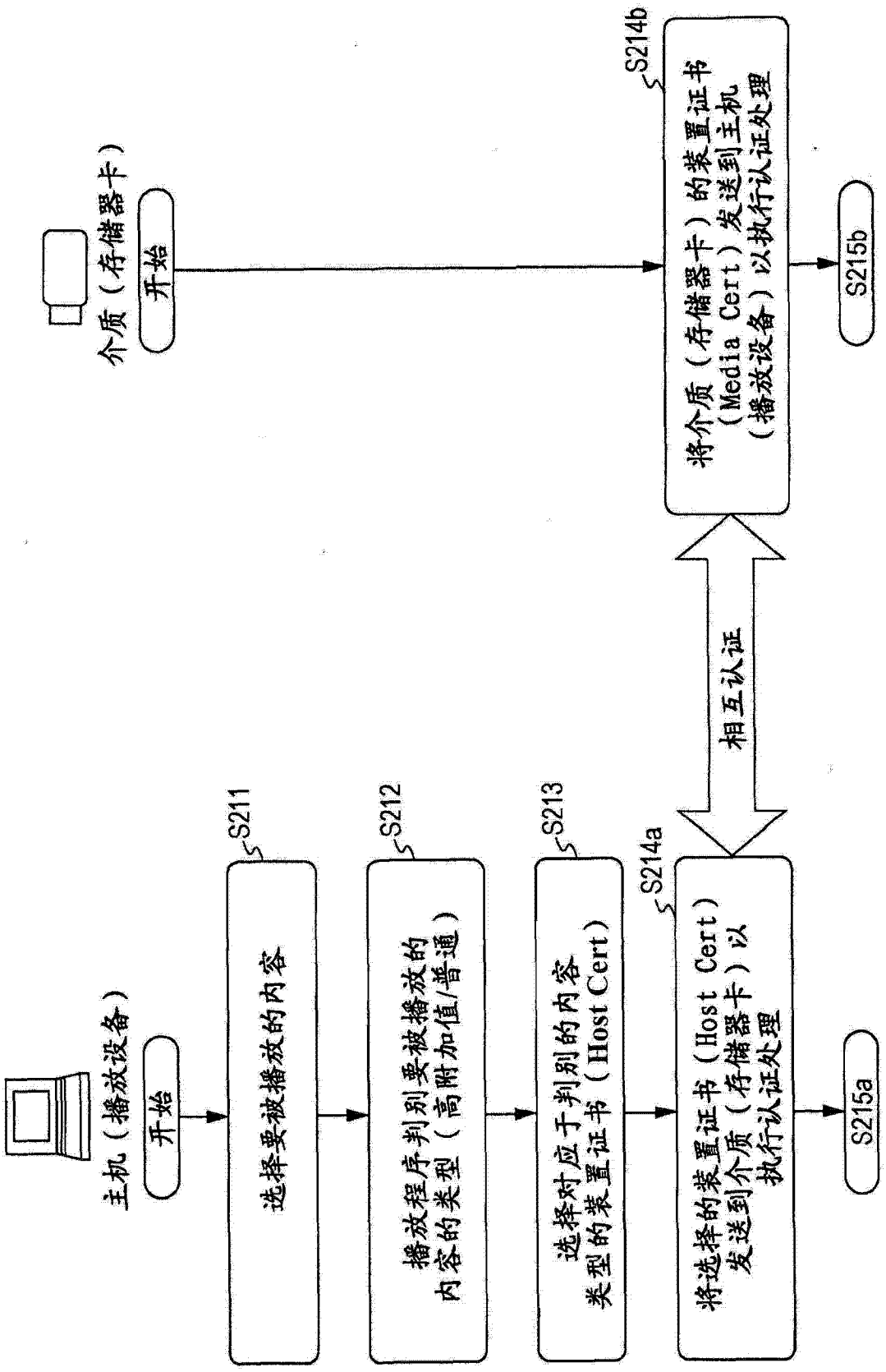

主机（播放设备）
开始
选择要被播放的内容
S211
播放程序判别要被播放的内容的类型（高附加值/普通）
S212
选择对应于判别的内容类型的装置证书（Host Cert）
S213
将选择的装置证书（Host Cert）发送到介质（存储器卡）以执行认证处理
S214a
S215a
介质（存储器卡）
开始
将介质（存储器卡）的装置证书（Media Cert）发送到主机（播放设备）以执行认证处理
S214b
S215b
相互认证

图 12

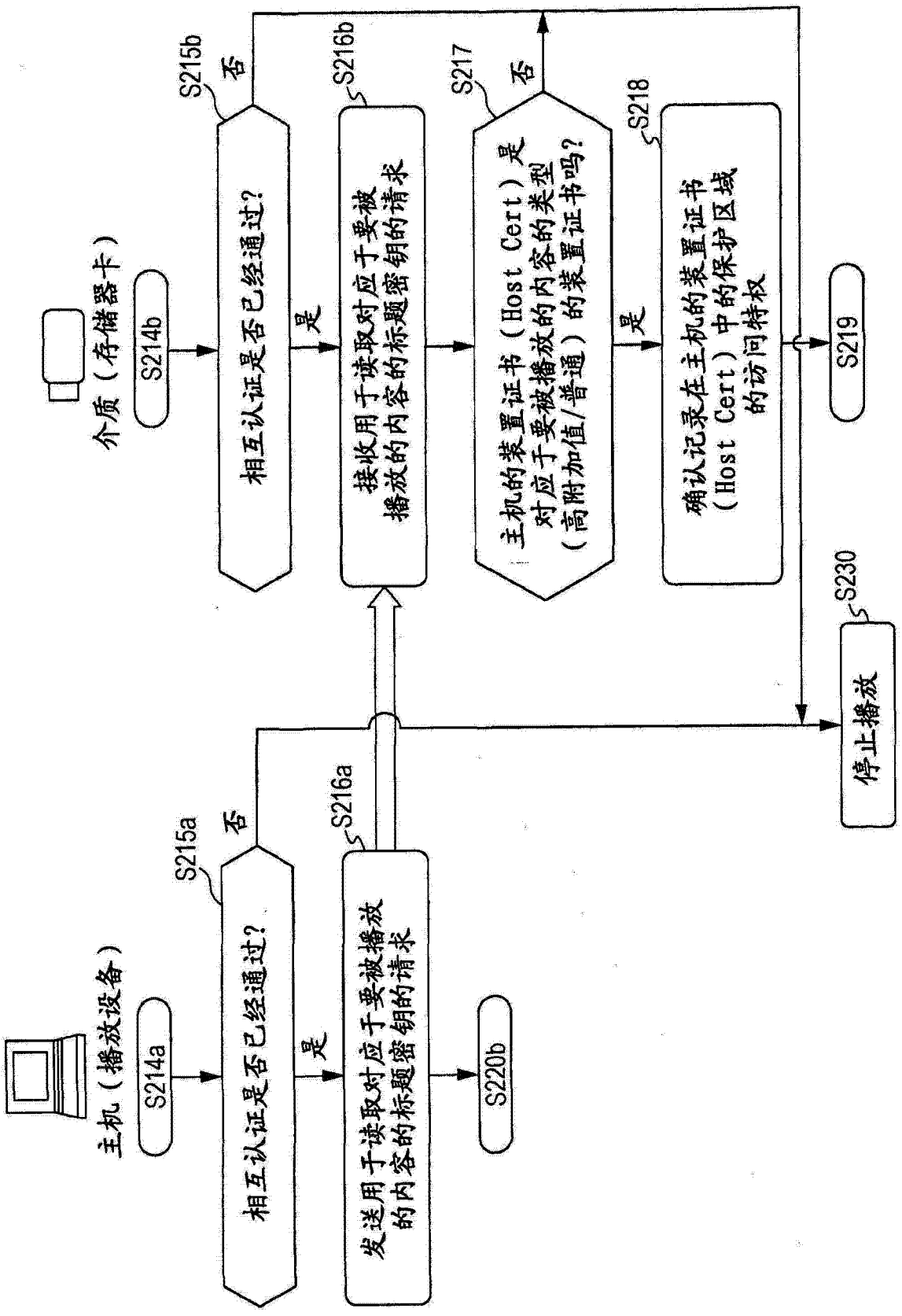

主机（播放设备）
介质（存储器卡）
S214a
S214b
相互认证是否已经通过?
是
否
S215a
S215b
发送用于读取对应于要被播放的内容的标题密钥的请求
S216a
接收用于读取对应于要被播放的内容的标题密钥的请求
S216b
S220b
主机的装置证书（Host Cert）是对应于要被播放的内容的类型（高附加值/普通）的装置证书吗?
S217
确认记录在主机的装置证书（Host Cert）中的保护区域的访问特权
S218
S219
停止播放
S230

图 13

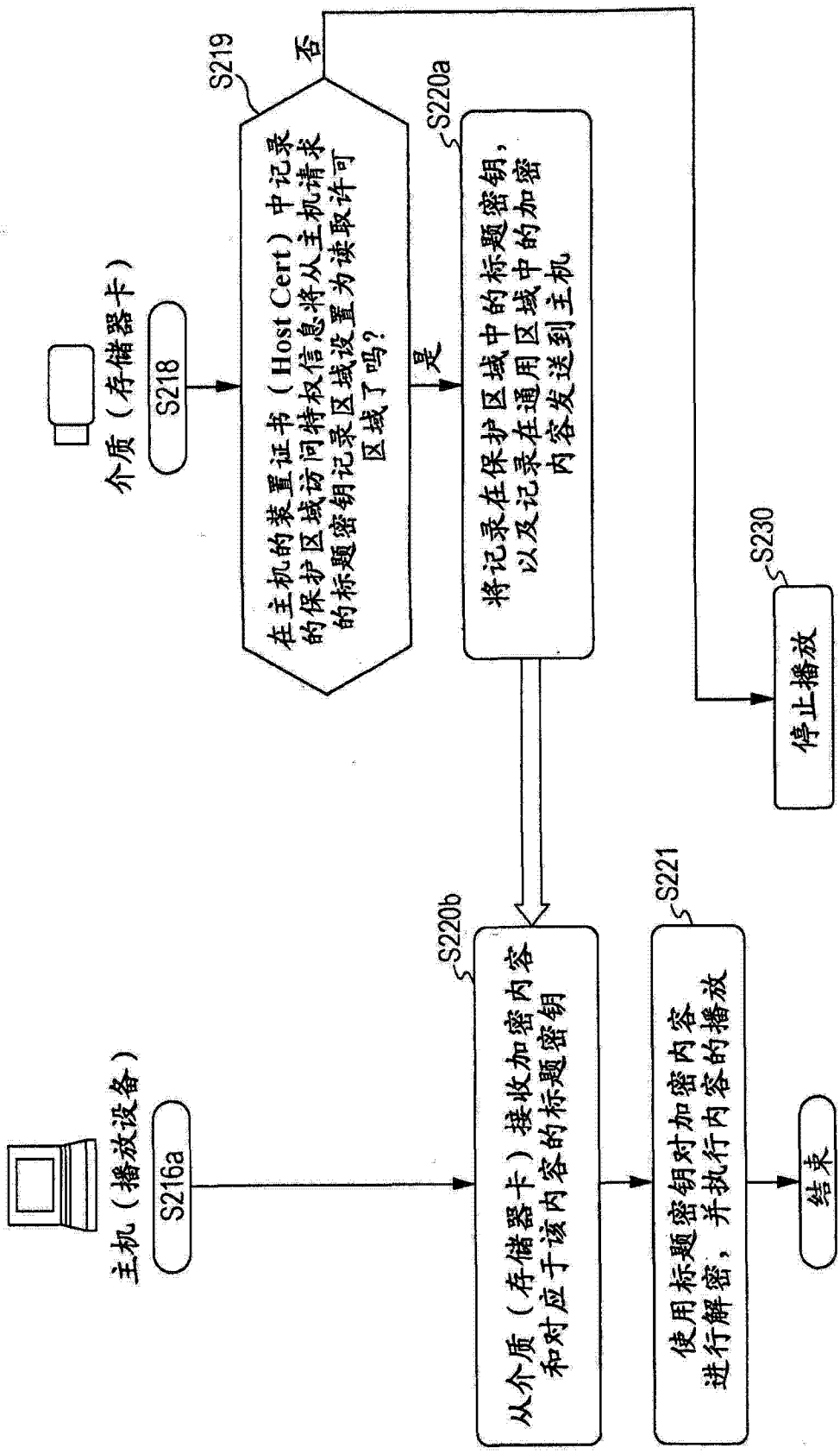

介质（存储器卡）
S218
在主机的装置证书（Host Cert）中记录的保护区域访问特权信息将从主机请求的标题密钥记录区域设置为读取许可区域了吗？
S219
否
是
S220a
将记录在保护区域中的标题密钥，以及记录在通用区域中的加密内容发送到主机
S230
停止播放
主机（播放设备）
S216a
从介质（存储器卡）接收加密内容和对应于该内容的标题密钥
S220b
使用标题密钥对加密内容进行解密，并执行内容的播放
S221
结束

图 14

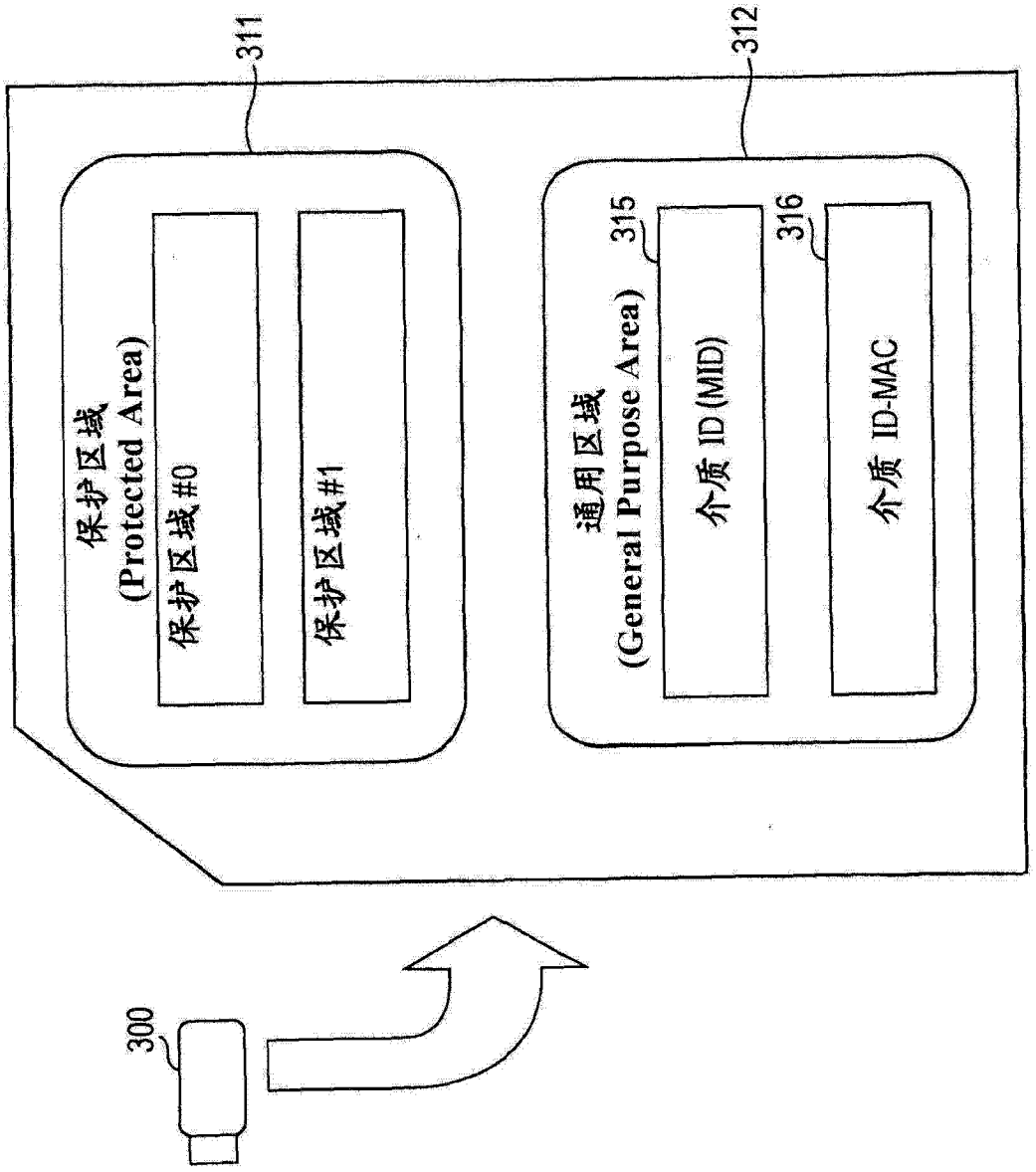

311
312
保护区域
(Protected Area)
保护区域#0
保护区域#1
通用区域
(General Purpose Area)
315
介质 ID (MID)
316
介质 ID-MAC
300

图 15

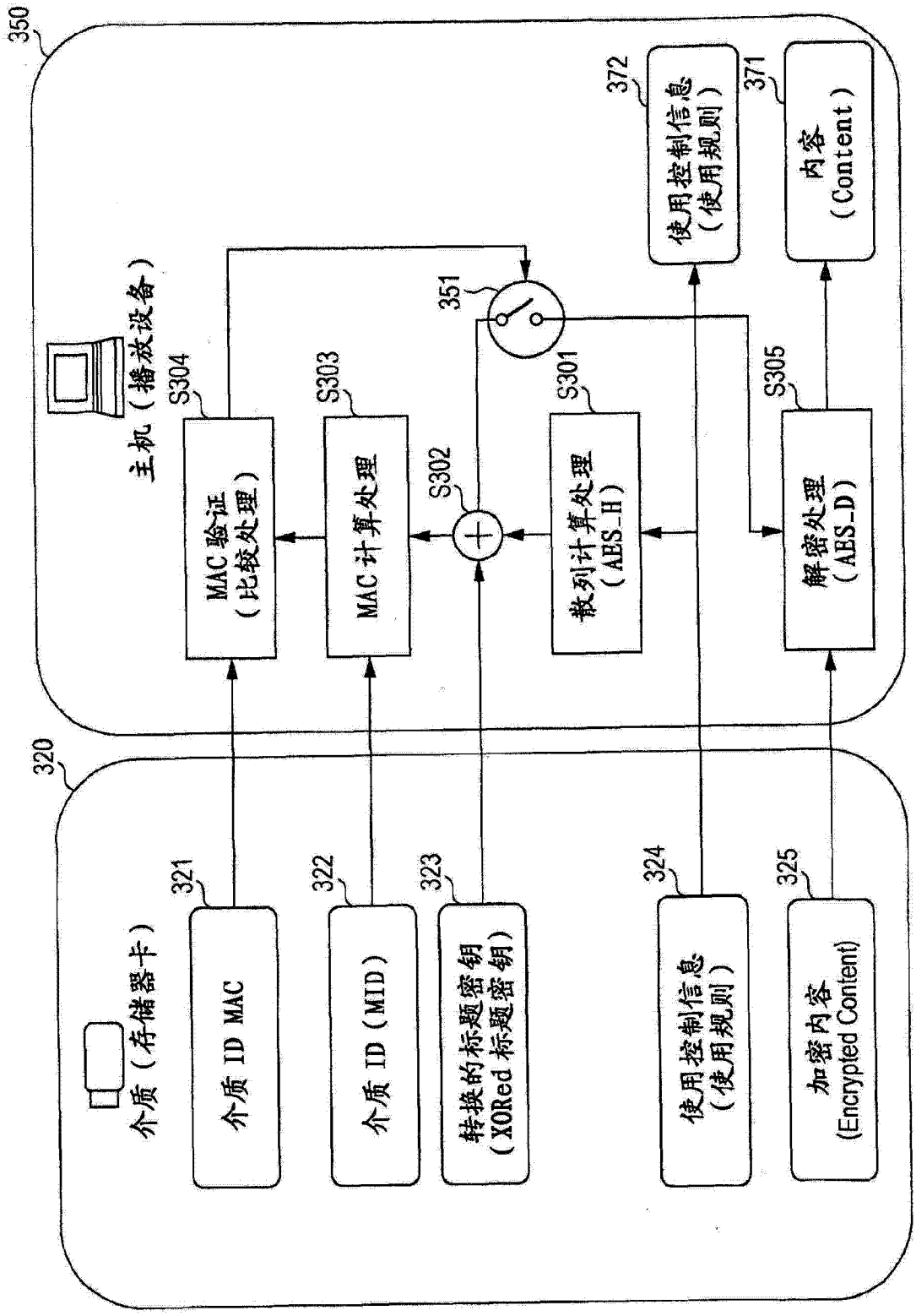

350
主机（播放设备）
MAC 验证（比较处理）
MAC 计算处理
散列计算处理（AES_H）
解密处理（AES_D）
S304
S303
S302
S301
S305
351
使用控制信息（使用规则）
内容（Content）
372
371
320
介质（存储器卡）
介质 ID MAC
介质 ID（MID）
转换的标题密钥（XORed 标题密钥）
使用控制信息（使用规则）
加密内容（Encrypted Content）
321
322
323
324
325

图 16

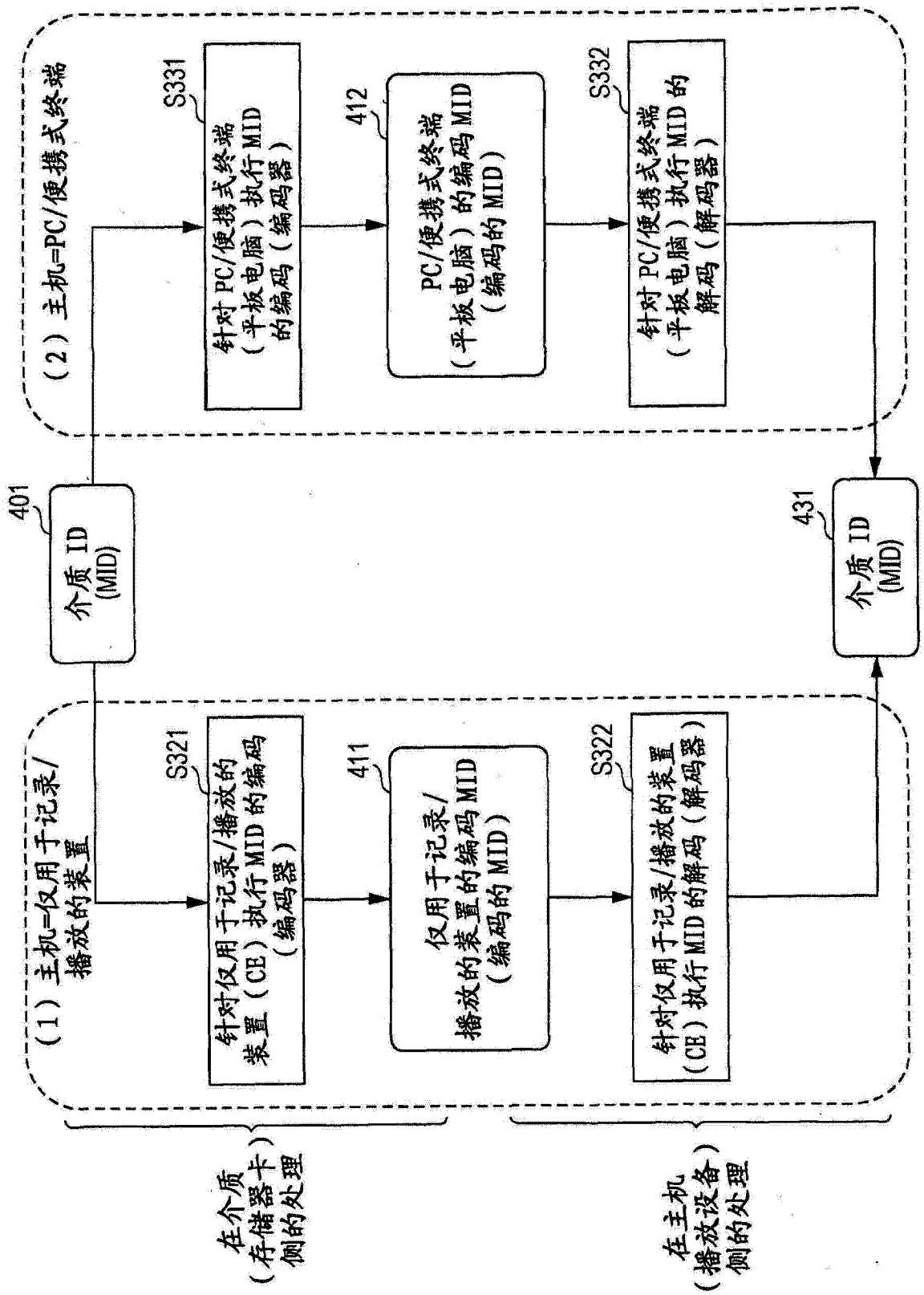

（2）主机=PC/便携式终端
S331
针对 PC/便携式终端（平板电脑）执行 MID 的编码（编码器）
412
PC/便携式终端（平板电脑）的编码 MID（编码的 MID）
S332
针对 PC/便携式终端（平板电脑）执行 MID 的解码（解码器）
401
介质 ID (MID)
431
介质 ID (MID)
（1）主机=仅用于记录/播放的装置
S321
针对仅用于记录/播放的装置（CE）执行 MID 的编码（编码器）
411
仅用于记录/播放的装置的编码 MID（编码的 MID）
S322
针对仅用于记录/播放的装置（CE）执行 MID 的解码（解码器）
在介质（存储器卡）侧的处理
在主机（播放设备）侧的处理

图 17

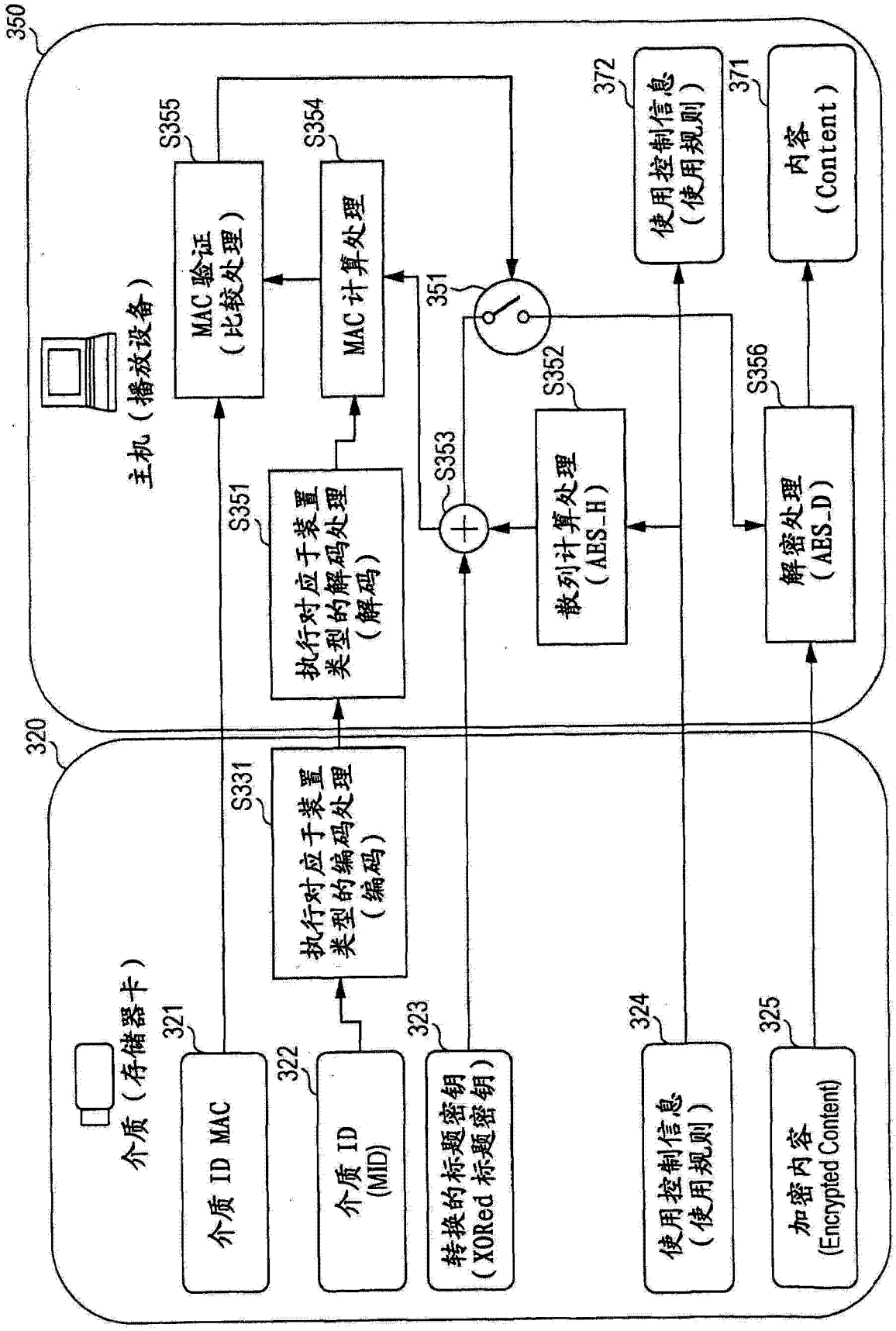

350
主机（播放设备）
S355
MAC 验证（比较处理）
S354
MAC 计算处理
372
使用控制信息（使用规则）
371
内容（Content）
351
S351
执行对应于装置类型的解码处理（解码）
S353
S352
散列计算处理（AES_H）
S356
解密处理（AES_D）
320
介质（存储器卡）
S331
执行对应于装置类型的编码处理（编码）
321
介质 ID MAC
322
介质 ID (MID)
323
转换的标题密钥（XORed 标题密钥）
324
使用控制信息（使用规则）
325
加密内容 (Encrypted Content)

图 18

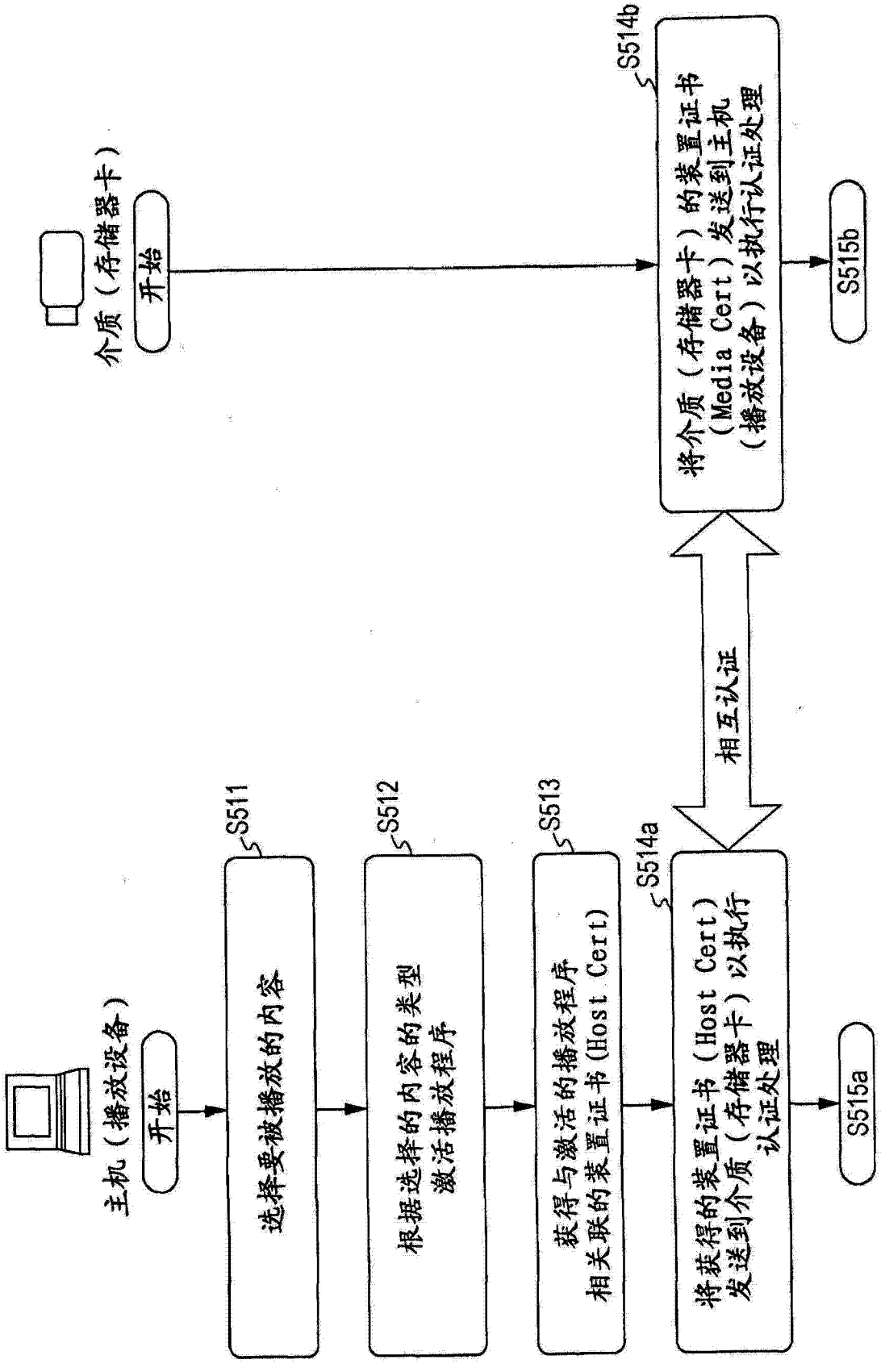

主机（播放设备）
开始
选择要被播放的内容
S511
根据选择的内容的类型
激活播放程序
S512
获得与激活的播放程序
相关联的装置证书（Host Cert）
S513
将获得的装置证书（Host Cert）
发送到介质（存储器卡）以执行
认证处理
S514a
S515a
介质（存储器卡）
开始
将介质（存储器卡）的装置证书
（Media Cert）发送到主机
（播放设备）以执行认证处理
S514b
S515b
相互认证

图 19

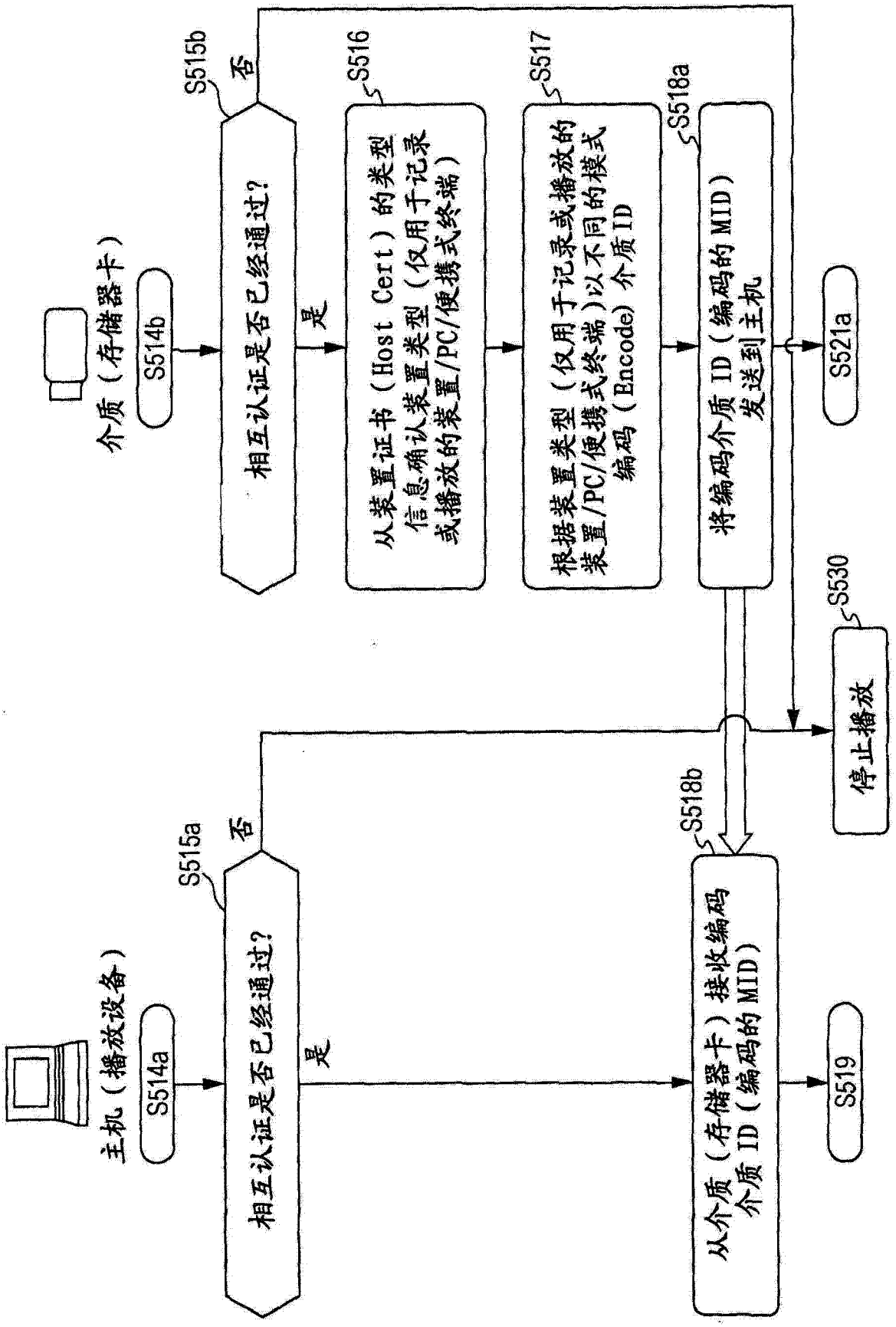

主机（播放设备）
介质（存储器卡）
S514a
S514b
相互认证是否已经通过?
S515a
S515b
否
是
从介质（存储器卡）接收编码介质 ID（编码的 MID）
S518b
S519
从装置证书（Host Cert）的类型信息确认装置类型（仅用于记录或播放的装置/PC/便携式终端）
S516
根据装置类型（仅用于记录或播放的装置/PC/便携式终端）以不同的模式编码（Encode）介质 ID
S517
将编码介质 ID（编码的 MID）发送到主机
S518a
S521a
停止播放
S530

图 20

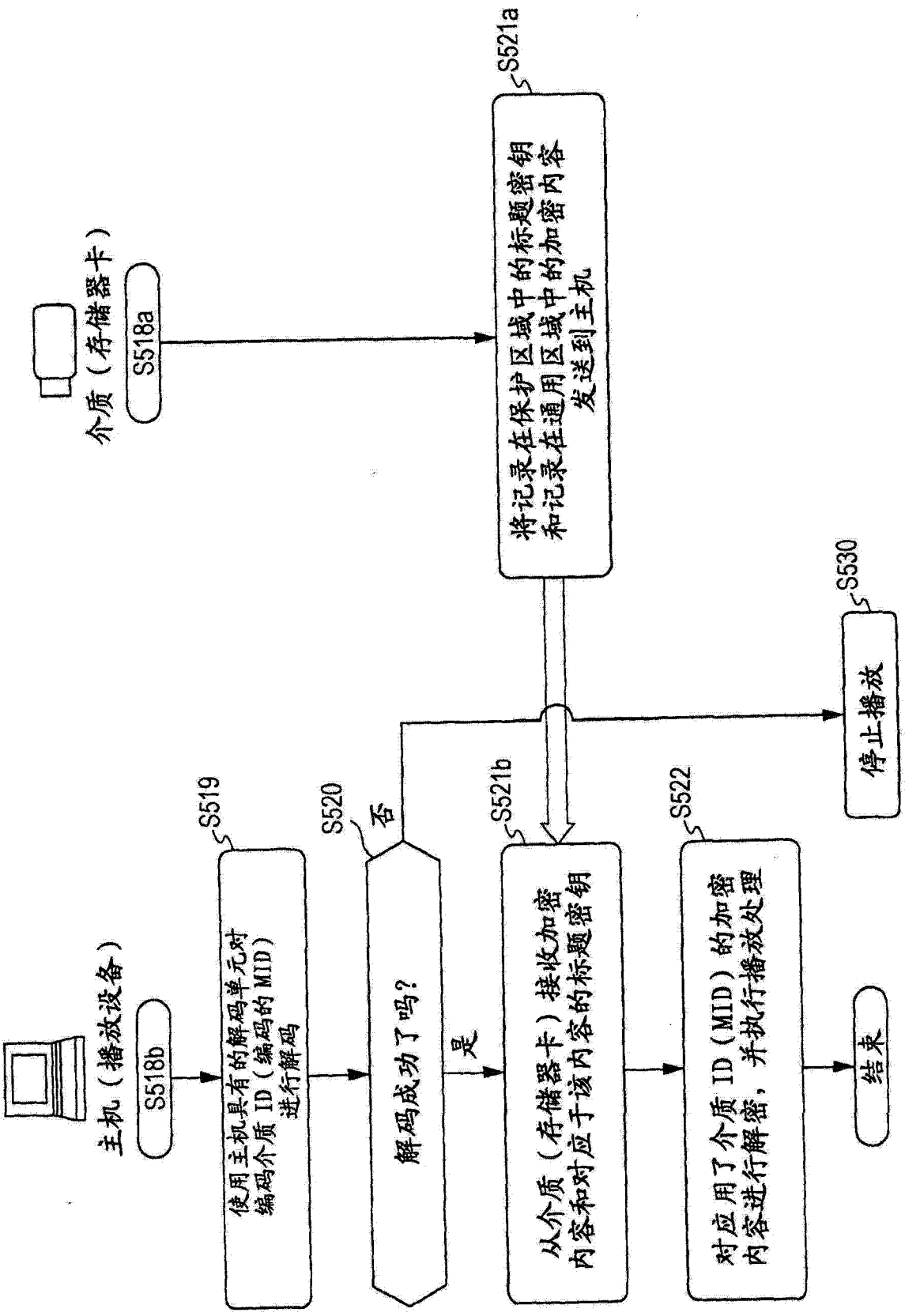

介质（存储器卡）
S518a
S521a
将记录在保护区域中的标题密钥和记录在通用区域中的加密内容发送到主机
主机（播放设备）
S518b
S519
使用主机具有的解码单元对编码介质ID（编码的MID）进行解码
S520
否
解码成功了吗？
是
S521b
从介质（存储器卡）接收加密内容和对应于该内容的标题密钥
S522
对应用了介质ID（MID）的加密内容进行解密，并执行播放处理
结束
S530
停止播放

图 21

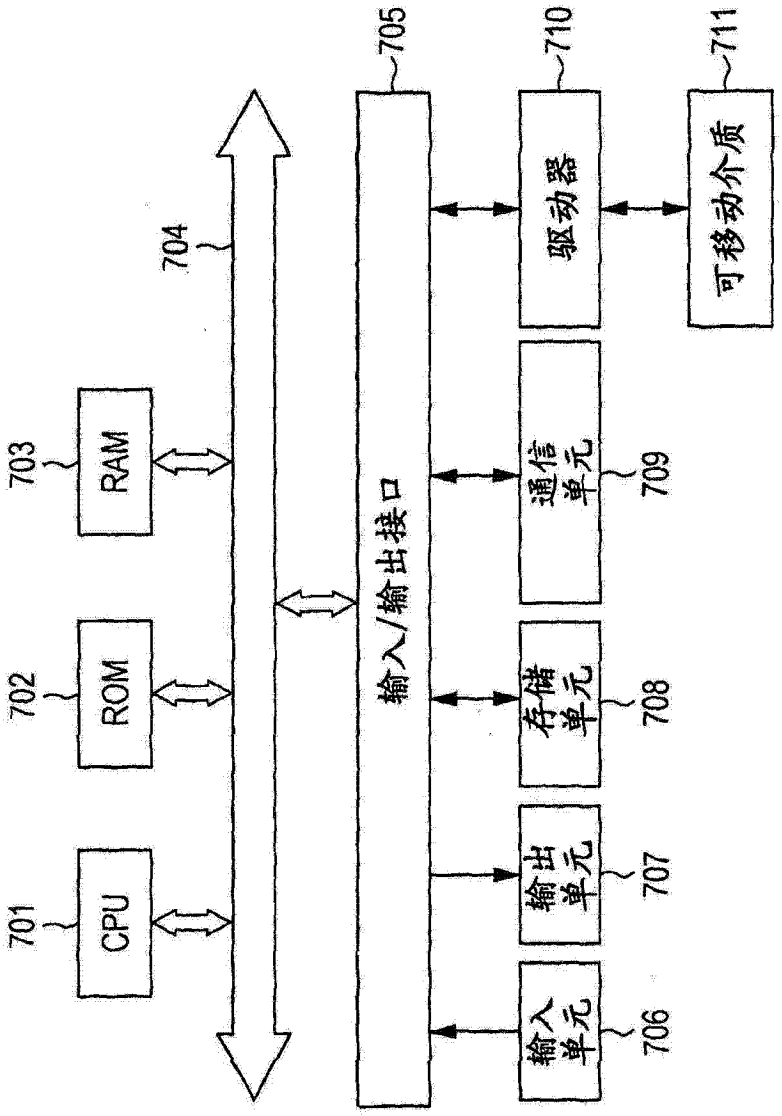

705
710
711
704
驱动器
可移动介质
703
RAM
通信单元
709
输入/输出接口
702
ROM
存储单元
708
701
CPU
输出单元
707
输入单元
706

图 22

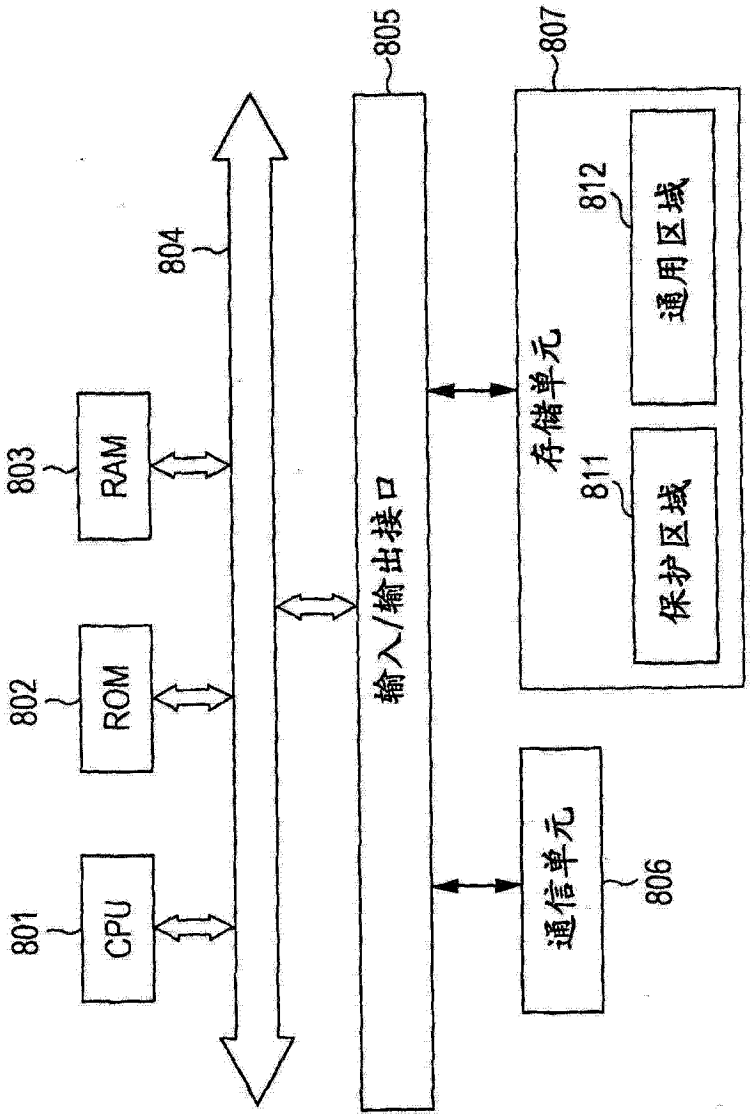

805
807
804
812
通用区域
存储单元
803
RAM
811
保护区域
输入/输出接口
802
ROM
801
CPU
通信单元
806

图 23