(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 1971740 B
(45)授权公告日 2010.06.16

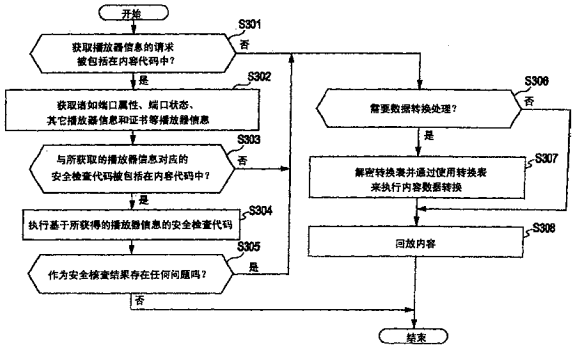
(21)申请号 200610149572.1
(22)申请日 2006.11.20
(30)优先权数据
2005-336226 2005.11.21 JP
(73)专利权人 索尼株式会社
地址 日本东京
(72)发明人 高岛芳和
(74)专利代理机构 北京东方亿思知识产权代理有限责任公司 11258
代理人 宋鹤
(51)Int.Cl.
G11B 20/10(2006.01)
G06F 12/14(2006.01)
G06F 21/00(2006.01)
(56)对比文件
JP 2003288752 A,2003.10.10, 全文.
JP 2005157966 A,2005.06.16, 全文.
审查员 马莹莹
权利要求书 2 页 说明书 19 页 附图 16 页

(54)发明名称

信息处理设备和方法、信息记录介质及其制造设备和方法

(57)摘要

一种信息处理设备，包括：数据处理器，用于在使用内容时获取记录在信息记录介质上的内容代码中所包括的安全检查代码，并根据所获得的安全检查代码对信息处理设备进行安全检查。该数据处理器获取基于与信息处理设备或内容使用应用程序对应的标识信息和配置信息中的至少一个的信息，并且在被分类成多个数据文件的安全检查代码当中，该数据处理器选择对应于所获得的信息的安全检查代码以根据所选择的安全检查代码来执行安全检查。



CN 1971740 B

1. 一种对记录在信息记录介质上的内容执行回放处理的信息处理设备，包括：

数据处理器，用于在使用所述内容时获取记录在所述信息记录介质上的内容代码中所包括的安全检查代码，并根据所获得的安全检查代码对所述信息处理设备进行安全检查，其中所述安全检查代码包括用于验证要执行内容回放的所述信息处理设备的正当性的程序，

所述数据处理器获取存储在所述信息处理设备的存储单元中的播放器证书以验证所述播放器证书的正当性，并且在验证了所述播放器证书的正当性的条件下，所述数据处理器从记录在所述播放器证书上的信息中获取对应于所述信息处理设备或内容使用应用程序的标识信息，并且在被分类成多个数据文件的安全检查代码当中，所述数据处理器选择对应于所获得的标识信息的安全检查代码以根据所选择的安全检查代码来进行安全检查。

2. 一种对记录在信息记录介质上的内容执行回放处理的信息处理设备，包括：

数据处理器，用于在使用所述内容时获取记录在所述信息记录介质上的内容代码中所包括的安全检查代码，并根据所获得的安全检查代码对所述信息处理设备进行安全检查，其中所述安全检查代码包括用于验证要执行内容回放的所述信息处理设备的正当性的程序，

所述数据处理器获取关于所述信息处理设备的端口属性信息、端口状态信息、存储区大小信息和数据处理模式信息中的至少一个作为配置信息，并且在被分类成多个数据文件的安全检查代码当中，所述数据处理器选择对应于所获得的配置信息的安全检查代码以根据所选择的安全检查代码来进行安全检查。

3. 如权利要求 2 所述的信息处理设备，其特征在于，当获得所述配置信息时，所述数据处理器获取由操作系统管理的装置信息并进行对应于所获得的信息的安全检查。

4. 如权利要求 2 所述的信息处理设备，其特征在于，当所述配置信息被更新时，所述数据处理器获取更新后的配置信息并进行对应于所述更新后的配置信息的安全检查。

5. 一种在信息处理设备中使用的、用记录在信息记录介质上的数据来执行数据处理的信息处理方法，包括以下步骤：

通过在使用记录在所述信息记录介质上的内容时获取记录在所述信息记录介质上的内容代码中所包括的安全检查代码，和通过根据所获得的安全检查代码对所述信息处理设备进行安全检查来执行数据处理，其中所述安全检查代码包括用于验证要执行内容回放的所述信息处理设备的正当性的程序，

在所述数据处理的执行过程中，获取存储在所述信息处理设备的存储单元中的播放器证书以验证所述播放器证书的正当性，并且在验证了所述播放器证书的正当性的条件下，从记录在所述播放器证书上的信息中获取对应于所述信息处理设备或内容使用应用程序的标识信息，并且在被分类成多个数据文件的安全检查代码当中，选择对应于所获得的标识信息的安全检查代码以根据所选择的安全检查代码来进行安全检查。

6. 一种在信息处理设备中使用的、用记录在信息记录介质上的数据来执行数据处理的信息处理方法，包括以下步骤：

通过在使用记录在所述信息记录介质上的内容时获取记录在所述信息记录介质上的内容代码中所包括的安全检查代码，和通过根据所获得的安全检查代码对所述信息处理设备进行安全检查来执行数据处理，其中所述安全检查代码包括用于验证要执行内容回放的

所述信息处理设备的正当性的程序，

在所述数据处理的执行过程中，获取关于所述信息处理设备的端口属性信息、端口状态信息、存储区大小信息和数据处理模式信息中的至少一个作为配置信息，并且在被分类成多个数据文件的安全检查代码当中，选择对应于所获得的配置信息的安全检查代码以根据所选择的安全检查代码来进行安全检查。

7. 如权利要求 6 所述的信息处理方法，其特征在于，在所述数据处理的执行过程中，在获取所述配置信息时获取由操作系统管理的装置信息，并进行对应于所获得的信息的安全检查。

8. 如权利要求 6 所述的信息处理方法，其特征在于，在所述数据处理的执行过程中，当所述配置信息被更新时，获取更新后的配置信息，并进行对应于所述更新后的配置信息的安全检查。

信息处理设备和方法、信息记录介质及其制造设备和方法

[0001] 相关申请的参照

[0002] 本发明包含涉及2005年11月21日向日本专利局提交的日本专利申请第2005-336226号的主题，其整个内容通过引用包括在此。

技术领域

[0003] 发明涉及信息处理设备和方法、信息记录介质制造设备和方法以及信息记录介质。更具体地，本发明涉及允许通过使用作为内容使用控制程序和内容一起记录在信息记录介质上的内容代码来执行安全检查处理的信息处理设备和方法、信息记录介质制造设备和方法以及信息记录介质。

背景技术

[0004] 诸如音乐等音频数据、影片等图像数据、游戏程序和各种应用程序等各种软件数据（下文称为“内容”）能作为数字数据被存储在例如使用蓝色激光的蓝光盘（商标）、数字多功能盘(DVD)、迷你盘(MD)、光盘(CD)等记录介质上。特别地，使用蓝色激光的蓝光盘（商标）是高密度记录盘并且能将大量视频内容记录成高质量的图像数据。

[0005] 数字内容被存储在诸如上述那些信息记录介质等各种信息记录介质上并被提供给用户。用户通过将其在用户的个人计算机(PC)或诸如盘播放器等播放器上回放来使用数字内容。

[0006] 通常，诸如音乐数据和图像数据等许多内容数据的颁发权由这些内容数据的创作者或销售者拥有。因此，基本上在分发内容时会强加某些使用限制，即只对授权用户允许内容的使用，从而防止未授权的复制。

[0007] 根据数字记录设备和记录介质，图像和声音能被重复地记录和回放而没有质量损失。因此，非法复制的内容通过因特网的分发、诸如光盘可记录(CD-R)盘等其上记录了复制的内容的称为所谓“盗版盘”的记录介质的流通、以及存储在例如PC等的硬盘中的复制的内容的使用是普遍的。

[0008] DVD或诸如最近开发的使用蓝色激光的记录介质等大容量记录介质能在一个介质上记录例如多达几部影片的大量数据作为数字信息。因为能将视频信息记录成如上所述的数字信息，所以通过防止未授权的复制来进行版权保护变得很重要。如今，为了防止数字数据的未授权的复制，用于防止未授权复制的各种技术被实际应用于数字记录设备或记录介质。

[0009] 一种增强版权保护的方法是加密内容。然而，根据此方法，如果发生用于加密内容的密钥的泄漏，则难以防止内容的未授权复制和此类复制内容的分发。解决这种问题的一种方法是在日本未审专利申请特开2002-311998号公报中公开的配置。在此配置中，在部分内容数据备用伪数据替换的状态下记录内容从而能防止内容的未授权的回放。

[0010] 当回放包括伪数据的内容时，需要用正确的内容数据替换伪数据。此数据转换处理应在防止正确内容数据泄漏的同时执行，并且最好还采取某些措施来防止诸如伪数据的

位置和转换方法等处理信息的泄漏。

[0011] 如上所述，当回放内容时，需要执行内容解密处理和数据转换处理，且在某些情况下，将进行诸如正当性确认处理等用于确定要使用内容的信息处理设备或回放（播放器）程序是否是授权设备或具有许可证的程序的安全检查。这种数据处理是通过执行作为内容使用控制程序和内容一起记录在信息记录介质上的内容代码来执行的。在例如WO2005/008385中公开了使用内容代码的内容使用处理的例子。

[0012] 内容代码被设置成独立于内容的文件，并被记录在信息记录介质上。因此，可以只将内容代码移动或复制到另一信息记录介质上。如果发生可能导致内容的未授权分发和使用的内容代码泄漏，则有可能许多内容项被非法回放和使用，从而造成巨大损害。

[0013] 可假定由不同制造商制造的各种类型的设备或应用程序被用于回放内容。如果只根据一个共用的顺序来执行使用内容代码的安全检查，则难以根据设备或应用程序的类型执行足够的检查。另外，可能无论内容的类型为何均使用一个用于为每一回放设备执行安全检查的文件。因此，重复使用该文件是合乎需要的。

发明内容

[0014] 因此，需要提供一种能实现作为内容使用控制程序和内容一起记录在信息记录介质上的内容代码所用的严格管理结构、同时允许重复使用内容代码中所包括的安全检查代码、并且在通过使用安全检查代码验证播放器时能执行根据播放器的类型的最优安全检查的信息处理设备和方法、信息记录介质制造设备和方法以及信息记录介质。

[0015] 根据本发明的一个实施例，提供了一种对记录在信息记录介质上的内容执行回放处理的信息处理设备。该信息处理设备包括数据处理器，用于在使用所述内容时获取记录在所述信息记录介质上的内容代码中所包括的安全检查代码，并根据所获得的安全检查代码对所述信息处理设备进行安全检查，其中所述安全检查代码包括用于验证要执行内容回放的所述信息处理设备的正当性的程序。所述数据处理器获取存储在所述信息处理设备的存储单元中的播放器证书以验证所述播放器证书的正当性，并且在验证了所述播放器证书的正当性的条件下，所述数据处理器从记录在所述播放器证书上的信息中获取对应于所述信息处理设备或内容使用应用程序的标识信息，并且在被分类成多个数据文件的安全检查代码当中，所述数据处理器选择对应于所获得的标识信息的安全检查代码以根据所选择的安全检查代码来进行安全检查。

[0016] 根据本发明另一实施例，提供了一种对记录在信息记录介质上的内容执行回放处理的信息处理设备。该信息处理设备包括数据处理器，用于在使用所述内容时获取记录在所述信息记录介质上的内容代码中所包括的安全检查代码，并根据所获得的安全检查代码对所述信息处理设备进行安全检查，其中所述安全检查代码包括用于验证要执行内容回放的所述信息处理设备的正当性的程序。所述数据处理器可以获取关于信息处理设备的端口属性信息、端口状态信息、存储区大小信息和数据处理模式信息中的至少一个作为配置信息，并且在被分类成多个数据文件的安全检查代码当中，所述数据处理器选择对应于所获得的配置信息的安全检查代码以根据所选择的安全检查代码来进行安全检查。

[0017] 当获得配置信息时，数据处理器可以获取由操作系统 (OS) 管理的装置信息，并进行对应于所获得的信息的安全检查。

[0018] 当配置信息被更新时，数据处理器可以获取更新后的配置信息，并进行对应于更新后的配置信息的安全检查。

[0019] 根据本发明的另一实施例，提供了一种信息记录介质制造设备，包括：内容文件获取装置，用于获取存储了要记录在信息记录介质上的内容数据的内容文件；内容代码文件获取装置，用于获取存储了包括在内容被使用时要执行的安全检查处理程序的内容代码的内容代码文件；以及记录装置，用于在信息记录介质上记录由该内容文件获取装置获得的内容文件和由该内容代码文件获取装置获得的内容代码文件。内容代码文件获取装置获取对应于信息处理设备或内容使用应用程序的类型的多个内容代码文件。

[0020] 内容代码文件获取装置可以获取存储了不依赖于信息处理设备或内容使用应用程序的类型的共用内容代码的内容代码文件、和存储了依赖于信息处理设备或内容使用应用程序的类型的内容代码的内容代码文件。

[0021] 内容代码文件获取装置可以获取存储了用于确定信息处理设备或内容使用应用程序的类型的代码的代码文件。

[0022] 根据本发明的另一实施例，提供了一种信息记录介质，该信息记录介质包含存储了内容数据的内容文件、和存储了包括要在内容被使用时执行的安全检查处理程序在内的内容代码的内容代码文件。内容代码文件包括与信息处理设备和内容使用应用程序对应的多个内容代码文件。

[0023] 内容代码文件可包括存储了不依赖于信息处理设备或内容使用应用程序的类型的共用内容代码的内容代码文件、和存储了依赖于信息处理设备或内容使用应用程序的类型的内容代码的内容代码文件。

[0024] 内容代码文件可以包括存储用于确定信息处理设备或内容使用应用程序的类型的代码的代码文件。

[0025] 根据本发明的另一实施例，提供了一种在信息处理设备中使用的、用记录在信息记录介质上的数据来执行数据处理的信息处理方法，包括以下步骤：通过在使用记录在所述信息记录介质上的内容时获取记录在所述信息记录介质上的内容代码中所包括的安全检查代码，和通过根据所获得的安全检查代码对所述信息处理设备进行安全检查来执行数据处理，其中所述安全检查代码包括用于验证要执行内容回放的所述信息处理设备的正当性的程序。在所述数据处理的执行过程中，获取存储在所述信息处理设备的存储单元中的播放器证书以验证所述播放器证书的正当性，并且在验证了所述播放器证书的正当性的条件下，从记录在所述播放器证书上的信息中获取对应于所述信息处理设备或内容使用应用程序的标识信息，并且在被分类成多个数据文件的安全检查代码当中，选择对应于所获得的标识信息的安全检查代码以根据所选择的安全检查代码来进行安全检查。

[0026] 根据本发明的另一实施例，提供了一种在信息处理设备中使用的、用记录在信息记录介质上的数据来执行数据处理的信息处理方法，包括以下步骤：通过在使用记录在所述信息记录介质上的内容时获取记录在所述信息记录介质上的内容代码中所包括的安全检查代码，和通过根据所获得的安全检查代码对所述信息处理设备进行安全检查来执行数据处理，其中所述安全检查代码包括用于验证要执行内容回放的所述信息处理设备的正当性的程序。在数据处理的执行过程中，可以获取关于信息处理设备的端口属性信息、端口状态信息、存储区大小信息和数据处理模式信息中的至少一个作为配置信息，并且在被分类

成多个数据文件的安全检查代码当中，选择对应于所获得的配置信息的安全检查代码以根据所选择的安全检查代码来进行安全检查。

[0027] 在数据处理的执行过程中，可以在获取配置信息时获取由 OS 管理的装置信息，并进行对应于所获得的信息的安全检查。

[0028] 在数据处理的执行过程中，当配置信息被更新时，可以获取更新后的配置信息，并进行对应于更新后的配置的信息的安全检查。

[0029] 根据本发明的另一实施例，提供了一种在信息记录介质制造设备中使用的信息记录介质制造方法。该信息记录介质制造方法包括以下步骤：获取存储了要记录在信息记录介质上的内容数据的内容文件，获取存储了包括要在内容被使用时执行的安全检查处理程序的内容代码的内容代码文件，并且将所获得的内容文件和所获得的内容代码文件记录在信息记录介质上。在获取内容代码文件的执行过程中，获取对应于信息处理设备或内容使用应用程序的类型的多个内容代码文件。

[0030] 在获取内容代码文件的执行过程中，可以获取存储了不依赖于信息处理设备或内容使用应用程序的类型的共用内容代码的内容代码文件、和存储了依赖于信息处理设备或内容使用应用程序的类型的内容代码的内容代码文件。

[0031] 在获取内容代码文件的执行过程中，可以获取存储了用于确定信息处理设备或内容使用应用程序的类型的代码的代码文件。

[0032] 根据本发明的一个实施例，在使用内容时获取记录在信息记录介质上的内容代码中所包括的安全检查代码，并根据所获得的安全检查代码来对信息处理设备进行安全检查。获取基于与信息处理设备或内容使用应用程序对应的标识信息和配置信息中的至少一个的信息，并且选择对应于所获得的信息的安全检查代码，并根据所选择的安全检查代码来进行安全检查。因此，能进行根据各种类型和版本的设备或各种回放应用程序的最优安全检查，由此有效地防止内容的未授权的使用。另外，可以实现安全代码的重复使用，从而实现信息记录介质的高效制造。

[0033] 从以下参照附图对示例性实施例的描述中，本发明的其它特征和优点将变得显而易见。

附图说明

[0034] 图 1 示出信息记录介质中的存储数据以及驱动器和信息处理设备的配置和处理；

[0035] 图 2 示出设置在信息记录介质中的存储内容中的内容管理单元；

[0036] 图 3 示出设置在信息记录介质中的存储内容中的内容管理单元与分配给这些内容管理单元的单元密钥之间的关联；

[0037] 图 4 示出记录在信息记录介质上的内容和内容回放所需的数据转换处理；

[0038] 图 5 示出内容回放处理的一个例子；

[0039] 图 6 示出当内容被回放时所执行的数据转换处理；

[0040] 图 7 示出要记录在信息记录介质上的数据的目录结构；

[0041] 图 8 示出要记录在信息记录介质上的内容和管理数据的目录结构；

[0042] 图 9 示出要记录在信息记录介质上的内容代码的目录结构；

[0043] 图 10 示出要记录在信息记录介质上的内容代码的生成 / 记录过程的细节；

[0044] 图 11 示出播放器证书的数据结构的一个例子；

[0045] 图 12 示出除了播放器证书外其它的播放器信息；

[0046] 图 13 示出用于获取播放器信息的处理的一个例子；

[0047] 图 14 是示出由信息处理设备执行的内容回放序列的流程图；

[0048] 图 15 示出信息处理设备的硬件配置的一个例子；以及

[0049] 图 16 是示出信息记录介质制造设备的配置的框图。

具体实施方式

[0050] 下面参照附图描述根据本发明的一个实施例的信息处理设备和方法、信息记录介质制造设备和方法以及信息记录介质的细节。其描述按下列次序给出。

[0051] 1. 信息记录介质中的存储数据及由驱动器和主机执行的处理的概述

[0052] 2. 内容管理单元 (CPS 单元)

[0053] 3. 包括经修改的数据的内容数据的结构及数据转换处理的概述

[0054] 4. 内容回放处理

[0055] 5. 使用安全检查代码的处理

[0056] 6. 信息处理设备的配置

[0057] 7. 信息记录介质制造设备和信息记录介质

[0058] 1. 信息记录介质中的存储数据及由驱动器和主机执行的处理的概述

[0059] 首先描述信息记录介质中的存储数据及由驱动器和主机执行的处理的概述。图 1 示出存储了内容的信息记录介质 100、驱动器 120 和主机 140 的配置。主机 140 是由例如 PC 等信息处理设备执行的数据回放（或记录）应用程序，并根据预定的数据处理序列通过使用例如 PC 等信息处理设备的硬件来执行处理。

[0060] 信息记录介质 100 是盘制造厂在具有授权的内容版权或颁发权的所谓“内容权所有人”的许可下制造的存储了授权内容的信息记录介质（例如，只读存储器 (ROM) 盘）或诸如蓝光盘（商标）或 DVD 等数据可重写信息记录介质（例如 RE 盘）。在以下实施例中，使用盘介质作为信息记录介质。然而，在本发明中，能使用各种形式的信息记录介质。

[0061] 如图 1 所示，信息记录介质 100 存储：经加密处理和替换（盖写）处理——即由另一数据盖写部分数据——的已加密内容 101；基于已知为广播加密系统的一种模式的树结构密钥分发系统生成的用作密码密钥块的媒体密钥块 (MKB)102；包括用于内容解密处理的已加密标题密钥（已加密内容保护系统 (CPS) 单元密钥）的标题密钥文件 103；包括作为内容复制 / 回放控制信息的复制控制信息 (CCI) 的使用规则信息 104；以及包括在使用已加密内容 101 时执行的数据转换处理程序的内容代码 105。

[0062] 内容代码 105 包括存储与在内容的预定区域中要被替换的数据对应的转换数据的转换表（修正表）106，还包括诸如用于验证执行内容回放的播放器（回放设备）的正当性的程序等安全检查代码 107。

[0063] 当回放内容时，信息处理设备根据包括在内容代码 105 中的安全检查代码 107 来验证例如播放器的正当性，然后根据包含在内容代码 105 中的数据转换处理程序来提取包括在内容代码 105 中的转换表（修正表）106 中所存储的转换数据以替换构成内容的部分数据。

[0064] 转换表 106 和安全检查代码 107 包括转换表和各种类型的代码，以使得能根据播放器的类型的播放器端口信息来执行处理，即安全检查和转换处理。例如，转换表 106 和安全检查代码 107 包括与公司 A 制造的播放器对应的转换表和安全检查代码和与公司 B 制造的播放器对应的转换表和安全检查代码。为了使用内容，播放器选择与该播放器相对应的安全检查代码和转换表并执行处理。

[0065] 内容代码 105 不仅包括数据转换处理程序，还包括用于执行诸如启动处理和安全检查处理等各种其它类型的处理的信息和程序。内容代码 105 的细节在以下给出。图 1 中所示的信息记录介质 100 中的存储数据只是例子，可以根据盘的类型存储不同的存储数据。以下讨论各种信息项的概述。

[0066] 已加密内容

[0067] 在信息记录介质 100 中，存储诸如活动图像内容的视听 (AV) 流等各种内容数据项，例如，由特定标准定义的高清晰度 (HD) 影片内容、游戏程序、图像文件、声音数据和文本数据。那些内容项是根据特定 AV 数据格式存储的特定的 AV 格式标准数据。更具体地，例如，根据蓝光 ROM 标准格式，内容被存储为蓝光盘（商标）ROM 标准数据。

[0068] 用作服务数据的游戏程序、图像文件、声音数据或文本数据可被存储。那些内容项可以被存储为具有与特定 AV 数据格式不符的数据格式的数据。

[0069] 作为内容的类型，包括诸如音乐数据、如活动图像和静止图像等图像数据、游戏程序和 WEB 内容等各种内容。这些内容包括各种模式的信息，例如能只通过来自信息记录介质 100 的数据来使用的内容信息、以及通过来自信息记录介质 100 的数据和从通过网络连接至记录介质 100 的服务器提供的数据的组合来使用的内容信息。为了单独控制每一内容段的使用，通过将不同的密钥（又被称为“标题密钥”的 CPS 单元密钥或单元密钥）分配给诸段，并用与其它段的密钥不同的密钥加密每一个段来将内容存储在信息记录介质 100 中。分配了一个单元密钥的单元被称为“内容管理单元 (CPS 单元)”。在内容中，部分数据通过被不同于正确数据的数据替换而被设置为破损数据，因此，即使内容被解密，它也不能被正确地回放。为了正确地回放内容，需要用注册在转换表中的正确数据替换破损数据。下面详细描述这种替换处理。

[0070] MKB

[0071] MKB 102 是根据已知为广播加密方法的一种模式的树结构密钥分发系统生成的密码密钥块。MKB 102 是密钥信息块，它使得能仅仅通过用存储在具有有效许可证的信息处理设备中的装置密钥 (Kd) 进行处理（解密）来获取解密内容所需的密钥 - 媒体密钥 (Km)。MKB 102 是基于根据所谓的分层树结构的信息分发系统。MKB 102 使得只在用户装置（信息处理设备）具有有效许可证时才能获取媒体密钥 (Km)，并使已被无效的用户装置不能获取媒体密钥 (Km)。

[0072] 通过改变用于加密存储在 MKB 102 中的密钥信息的装置密钥，作为许可证实体的管理中心允许 MKB 102 使特定用户装置中所存储的装置密钥不能解密内容，亦即使用户装置不能获取解密内容所需的媒体密钥。因此，可以只向具有有效许可证的装置提供已加密的内容，而在合适的时间使未授权装置无效。以下讨论内容解密处理。

[0073] 标题密钥文件

[0074] 如上所述，在每个内容或一组多个内容项中，内容段被用各自的加密密钥（标题

密钥或 CPS 单元密钥）加密，然后被存储在信息记录介质 100 中。即，需要将 AC 流、音乐数据、如活动图像和静止图像等图像数据、游戏程序和 WEB 内容划分成使用内容所用的多个单元，并为所划分的单元生成不同的标题密钥，并用所生成的不同的标题密钥解密这些内容单元。用于生成标题密钥的信息是标题密钥数据，且能通过以用例如媒体密钥生成的密钥将已加密的标题密钥解密来获得标题密钥。相应单元的标题密钥是用标题密钥数据根据预定密码密钥生成序列来生成的，从而内容单元可被解密。

[0075] 使用规则信息

[0076] 使用规则信息包括例如复制 / 回放控制信息 (CCI)，即用于控制信息记录介质 100 中所存储的已加密内容 101 的使用的复制限制信息或回放限制信息。可以以各种方式设置该复制 / 回放控制信息 (CCI)，例如为用作内容管理单元的每一 CPS 单元设置，或为多个 CPS 单元设置。

[0077] 内容代码

[0078] 如上所述，内容代码 105 包括其中注册了对应要在内容的预定区域中被替换的数据的转换数据的转换表（修正表）106 以及诸如用于验证执行内容回放的播放器（回放设备）的正当性的程序等安全检查代码 107。

[0079] 如上所述，转换表 106 和安全检查代码 107 包括各种代码以使得能根据各种播放器的类型和播放器端口信息来执行处理。为了使用内容，播放器选择对应于该播放器的安全检查代码和转换表并分别执行安全检查处理和数据转换处理。

[0080] 用作播放器的回放应用程序 150 以回放内容的主机 140 设置一个执行数据转换处理的虚拟机 (VM)，并通过使用该 VM 根据从信息记录介质 100 读取的内容代码来执行安全检查处理和数据转换处理，以通过使用注册在转换表 106 中的条目来转换构成该内容的数据的一部分。

[0081] 存储在信息记录介质 100 中的已加密内容 101 已进行了某种加密处理，且构成内容 101 的数据的一部分是不同于正确数据的破损数据。当回放已加密内容 101 时，需要用注册在转换表 106 中的转换数据替换（盖写）多个破损数据。

[0082] 许多破损数据被分散地设置在已加密内容 101 中，且为了回放内容 101，需要用注册在转换表 106 中的转换数据替换（盖写）该多个破损数据。因为破损数据的存在，所以即使发生密码密钥的泄漏并执行了内容的未授权的解密，也不能正确地回放该内容。结果，能防止内容的未授权的使用。

[0083] 转换表 106 不仅包括正常转换数据还包括使得对构成用于标识内容播放器或内容回放应用程序的标识信息的位的分析能够进行的特定转换数据。更具体地，该特定转换数据包括其上记录了作为播放器（执行主机应用程序的装置）的标识数据的播放器 ID 或根据播放器 ID 生成的标识信息的识别标记。包括识别标记的特定转换数据是通过以不影响内容的回放的程度稍微修改构成正确内容数据的位来生成的。

[0084] 内容代码 105 不仅包括通过使用转换表 106 执行的数据转换处理程序，还包括用于执行诸如启动处理和安全处理等其它类型的处理的信息和程序。下面描述内容代码 105 的细节。

[0085] 下面参照图 1 讨论主机 140 和驱动器 120 的配置及由其执行的处理的概述。存储在信息记录介质 100 中的内容通过经由驱动器 120 将关于该内容的数据传递至主机 140 来

回放。

[0086] 在主机 140 中，设置了回放（播放器）应用程序 150 和安全 VM 160。回放应用程序 150 是内容回放处理器，并执行诸如驱动器 120 的认证、内容解密和解码等处理。

[0087] 安全 VM 160 通过使用包括转换表 106 和安全检查代码 107 的内容代码 105 来执行处理。安全 VM 160 从安全检查代码 105 中选择与相关联的播放器对应的安全检查代码 107，并且还通过使用转换表 106 来执行用于替换构成该内容的数据的一部分的替换处理。安全 VM 160 被设置成主机 140 中的虚拟机。作为直接分析中间语言并执行它的虚拟计算机的虚拟机 (VM) 从信息记录介质 100 读取独立于平台的中间语言的指令代码信息，并分析该指令代码信息以执行它。

[0088] 安全 VM 160 用作获取包含用于使用记录在信息记录介质 100 上的加密内容 101 的程序或信息的内容代码 105 并执行内容代码 105 以执行数据处理的数据处理器。

[0089] 通过从回放应用程序 150 到安全 VM 160 的中断 (INTRP) 和从安全 VM160 到回放应用程序 150 的响应（呼叫）的序列来执行诸如发送和接收信息和处理请求等在回放应用程序 150 与安全 VM 160 之间的通信。

[0090] 由主机 140 执行的主要处理如下。在使用内容之前，进行驱动器 120 与主机 140 之间的相互认证处理。在作为相互认证处理的结果验证了驱动器 120 和主机 140 的正当性之后，将已加密内容 101 从驱动器 120 传送至主机 140，且主机 140 将已加密内容 101 解密，并且还通过使用转换表 106 执行数据转换处理来回放该内容。

[0091] 驱动器 120 的数据处理器 121 进行主机 140 的认证以使用内容，并从信息记录介质 100 读取数据并将其传送至主机 140。

[0092] 作为由例如 PC 等信息处理设备执行的数据回放（或记录）应用程序的主机 140 的回放（播放器）应用程序 150 通过使用信息处理设备的硬件根据预定的数据处理序列来执行处理。

[0093] 主机 140 包括 ：数据处理器 151，用于执行与驱动器 120 的相互认证和数据传送控制 ；解密处理器 153，用于将已加密内容 101 解密 ；数据转换处理器 154，用于根据注册在转换表 106 中的数据来执行数据转换处理 ；以及解码处理器 155，用于执行解码（例如，MPEG 解码）。

[0094] 解密处理器 153 通过使用存储在存储器 156 中的各种信息和从信息记录介质 100 读取的数据来生成用于将已加密内容 101 解密的密钥，以将已加密内容 101 解密。数据转换处理器 154 通过使用注册在转换表 106 中的转换数据根据从信息记录介质 100 获得的数据转换处理程序来执行用于替换（盖写）构成该内容的数据的一部分的替换（盖写）处理。解码处理器 155 执行解码（例如 MPEG 解码）处理。

[0095] 在存储器 156 中，存储用于相互认证和解密的装置密钥 (Kd) 和密钥信息。装置密钥 (Kd) 是用于上述 MKB 处理的密钥。MKB 102 是使得能仅仅通过使用具有有效许可证的信息处理装置中所存储的装置密钥 (Kd) 进行处理（解密）来获得解密内容所需的密钥 - 媒体密钥 (Km) 的密钥信息块。为了将已加密内容 101 解密，回放应用程序 150（信息处理设备）通过使用存储在存储器 156 中的装置密钥 (Kd) 来执行 MKB 处理。以下给出内容解密处理的细节。

[0096] 2. 内容管理单元 (CPS 单元）

[0097] 如上所述，为了根据不同内容单元控制内容的使用，通过将不同密钥分配给诸内容单元来加密和存储信息记录介质中所存储的内容。即，内容被分段成多个内容管理单元(CPS 单元)，且 CPS 单元被单独加密，并对单独的 CPS 单元执行使用控制。

[0098] 为了使用内容，需要首先获取分配给每一单元的 CPS 单元密钥（又称为“标题密钥”），然后通过使用该CPS单元密钥和其它所需的密钥及密钥生成信息，执行基于预定解密处理序列的数据处理，以回放内容。下面参照图 2 讨论内容管理单元 (CPS 单元）的设置的一个例子。

[0099] 如图 2 所示，内容具有包括 (A) 索引层 210、(B) 影片对象层 220、(C) 播放列表层 230 和 (D) 剪辑层 240 的分层结构。当指定诸如标题等由回放应用程序访问的索引时，与该标题相关联的回放程序被指定，并根据关于所指定的回放程序的程序信息来选择定义例如内容回放次序的播放列表。

[0100] 播放列表包括一个或多个播放项作为关于要回放的区的信息。根据作为由播放项定义的回放区的剪辑信息，有选择地读取作为真实内容数据的 AV 流或命令，以回放 AV 流或执行命令。存在多个播放列表或多个播放项，且播放列表 ID 或播放项 ID 作为标识信息与播放列表或播放项相关联。

[0101] 图 2 示出构成信息记录介质中所存储的内容的一部分的两个 CPS 单元。CPS 单元 1271 和 CPS 单元 2272 包括作为索引的标题、作为回放程序文件的影片对象、播放列表和作为真实内容数据的 AV 流文件。

[0102] 内容管理单元 (CPS 单元）1271 包括标题 1211 和标题 2212、回放程序 221、222 和 223、播放列表 231 和 232 以及剪辑 241 和 242。至少分别包含在两个剪辑 241 和 242 中的用作真实内容数据的 AV 流数据文件 261 和 262 是要加密的数据，并且基本上用作为与内容管理单元 (CPS 单元）1271 相关联的密码密钥的标题密钥 (Kt1)（又称为“CPS 单元密钥”）来进行加密。

[0103] 内容管理单元 (CPS 单元）2272 包括 :作为索引的应用程序 1213、回放程序 224、播放列表 233 和剪辑 243。包含在剪辑 243 中的用作真实内容数据的 AV 流数据文件 263 用与内容管理单元 (CPS 单元）2272 相关联的密码密钥 - 标题密钥 (Kt2) 进行加密。

[0104] 为了回放与内容管理单元 (CPS 单元）1271 相关联的应用程序文件或内容，用户需要获取为该内容管理单元 (CPS 单元）1271 设置的密码密钥 - 标题密钥 (Kt1) 来执行解密处理。为了回放与内容管理单元 (CPS 单元）2272 相关联的应用程序文件或内容，用户需要获取为该内容管理单元 (CPS 单元）2272 设置的密码密钥 - 标题密钥 (Kt2) 来执行解密处理。

[0105] 图 3 中示出 CPS 单元的设置和 CPS 单元与标题密钥之间的关联的一个例子。更具体地，图 3 示出用于设置使用存储在信息记录介质中的已加密内容所用的管理单元 -CPS 单元的元素与用于 CPS 单元的标题密钥 (CPS 单元密钥）之间的关联。可以预先存储要用于以后由用户生成或获取的数据的 CPS 单元和标题密钥。例如，数据部分 281 是用于以后由用户生成或获取的数据的条目。

[0106] 可以将各种元素用于设置 CPS 单元，例如，内容标题、应用程序、数据组等。在 CPS 单元管理表中，设置了用作与 CPS 单元相关联的标识符的 CPS 单元 ID。

[0107] 在图 3 中，例如，标题 1 属于 CPS 单元 1，并且为了解密属于 CPS 单元 1 的已加密内

容，需要生成标题密钥 (Kt) 并通过使用所生成的标题密钥 (Kt1) 来解密内容。

[0108] 如上所述，为了单独地控制内容单元，用不同的密钥来加密构成信息记录介质 100 中所存储的内容的内容管理单元 (CPS 单元)。为了单独地控制每一 CPS 单元的使用，为每一 CPS 单元设置使用规则 (UR)。如上所述，使用规则包括内容的复制 / 回放控制信息 (CCI)，例如关于每一 CPS 单元中所包括的关于已加密内容的复制限制信息和回放限制信息。

[0109] 为了生成标题密钥，需要用存储在信息记录介质中的各信息项来进行数据处理。

[0110] 3. 包括经修改的数据的内容数据的结构及数据转换处理的概述

[0111] 下面描述包括经修改的数据的内容数据的结构和数据转换处理的概述。如上所述，在信息记录介质 100 中所存储的已加密内容 101 中，构成已加密内容 101 的数据的一部分被不同于正确数据的数据替换并被设置为破损数据。通过这种安排，即使包括破损数据的已加密内容 101 被解密，也难以正确地回放内容。为了正确地回放内容，需要用记录在转换表 106 中的转换数据替换（盖写）破损数据。

[0112] 下面参照图 4 讨论信息记录介质 100 中所存储的内容的结构及回放处理的概述。在信息记录介质 100 中存储了例如影片等 AV 内容。该内容被加密，并且能在用只能由具有授权许可证的回放设备获得的密码密钥解密之后被回放。以下讨论具体的内容回放处理。在存储在信息记录介质 100 中的内容里，部分数据被用经修改的数据替换。

[0113] 图 4 示出存储在信息记录介质 100 中的内容 291 的结构。内容 291 包括未经修改的正确内容 292 和经修改的破损数据 293。破损数据 293 是通过破坏原始的正确内容来生成的。因此，不能通过使用包括破损数据 293 的内容 291 来正确地执行内容回放。

[0114] 为了正确地执行内容回放，需要通过用正确内容数据替换内容 291 中所包含的破损数据 293 来生成回放内容 296。为了生成回放内容 296，从注册在内容代码 105 中所包含的转换表（修正表）106（见图 1）中的转换条目 295 获得用作用于替换相应破损数据区域中的破损数据 293 的正确内容数据的转换数据，并用所获得的转换数据来替换破损数据 293。然后，回放内容 296 被回放。

[0115] 在生成回放内容 296 时，除了用是正确内容数据的转换数据 297 替换破损数据 293 以外，还用用于分析构成用于标识内容播放器或内容回放应用程序的标识信息（例如，播放器 ID）的位的标识符设置转换数据 298 替换内容 291 的一部分。通过这一替换，如果非法复制的内容被分发，则能通过分析所分发的内容中的标识符设置转换数据 298 来指出未授权的内容的分发源。

[0116] 转换条目 295 被存储在转换表 106 中，然后它们还可以被分散地记录在构成该内容的数据中的特定分组中。即，实现了图 1 中所示的转换表 106 和已加密内容 101 中的转换条目 295 的多重记录。要回放内容的信息处理设备通过使用转换表 106 中所存储的转换数据或分散记录在内容中的转换条目 295 来执行替换处理。

[0117] 4. 内容回放处理

[0118] 下面参照图 5 描述由主机 345 执行的内容回放处理。在图 5 中，示出一个其中存储了已加密内容的信息记录介质 330、设置该信息记录介质 330 并从其读取数据的驱动器 340、以及连接至驱动器 340 以与之相互通信来执行回放（播放器）应用程序的主机 345，该回放应用程序通过驱动器 340 获得存储在信息记录介质 330 中的内容并回放内容。

[0119] 在图 5 中所示的主机 345 中，执行内容解密、解码和数据转换处理的回放应用程序

块 350 以及具有安全 VM 361 的安全 VM 块 360 是分离的。安全 VM361 计算用于根据包含在信息记录介质 330 上所记录的内容代码 334 中的安全检查代码 335 来进行安全检查以及用于根据转换表（修正表）336 执行转换处理的参数。

[0120] 信息记录介质 330 包括 MKB 331、标题密钥文件 332、已加密内容 333 和作为记录的数据的内容代码 334。在已加密内容 333 中，如参照图 4 所讨论的，部分数据被用破损数据替换，且需要用从转换表 336 获得的数据替换这些破损数据。

[0121] 内容代码 334 包括安全检查代码 335 和转换表 336。安全检查代码 335 包括用于验证要执行内容回放的播放器（回放设备）的正当性的程序。转换表 336 存储与要在内容的预定区域中被替换的数据对应的转换数据。主机 345 存储用于 MKB 处理的装置密钥 351。

[0122] 由主机 345 执行的用于通过驱动器 345 获得信息记录介质 330 中所存储的内容并回放该内容的回放处理序列如下。在从信息记录介质 330 读取内容之前，在步骤 S101 中，主机 345 和驱动器 340 进行相互认证以检查它们是否是授权的应用程序和设备。相互认证能以各种方式进行。在成功进行相互认证后，驱动器 340 和主机 345 共享共用会话密钥 (Ks)，该共用会话密钥是共用私钥。

[0123] 然后，在步骤 S102 中，主机 345 的回放应用程序 350 通过驱动器 340 获取信息记录介质 330 上所记录的 MKB 331，并通过使用存储在存储器中的装置密钥 351 对 MKB 331 执行处理以获得媒体密钥 (Km)。

[0124] MKB 331 是根据已知为广播加密方法的一种模式的树结构密钥分发系统生成的密码密钥块。MKB 331 是使得只能通过使用具有有效许可证的信息处理设备中所存储的装置密钥 (Kd) 进行处理（解密）来获得解密内容所需的密钥 - 媒体密钥 (Km) 的密钥信息块。

[0125] 然后，在步骤 S103 中，回放应用程序 350 通过使用在步骤 S102 中执行的 MKB 处理中获得的媒体密钥 (Km) 来解密从信息记录介质 330 读取的标题密钥文件 332 以获取标题密钥 (Kt)。存储在信息记录介质 330 中的标题密钥文件 332 是包括用媒体密钥 (Km) 加密的数据的文件，并且通过用媒体密钥 (Km) 解密该标题密钥文件 332，能获得用于解密该内容的标题密钥 (Kt)。能通过使用例如高级加密标准 (AES) 加密算法来执行步骤 S103 中的解密处理。

[0126] 然后，回放应用程序 350 通过驱动器 340 读取信息记录介质 330 中所存储的已加密内容 333 并将所读取的已加密内容 333 存储在轨道 (track) 缓冲器 352 中。然后，在步骤 S104 中，回放应用程序 350 通过使用标题密钥 (Kt) 解密轨道缓冲器 352 中所存储的已加密内容 333，以获取已解密的内容。

[0127] 已解密的内容被存储在明文传输流（明文 TS）缓冲器 353 中。明文 TS 缓冲器 353 中所存储的已解密的内容包含上述破损数据，因此，需要预定的数据转换（通过盖写进行的数据替换）。

[0128] 在步骤 S105 中，安全 VM 361 从内容代码 334 生成进行数据转换所需的参数。然后，在步骤 S106 中，在实时事件处理器 356 的控制下执行表复原 / 数据转换处理。通过实时事件处理器 356 的控制，回放应用程序 350 响应于内容段的切换向安全 VM 361 输出参数计算请求作为中断 (INTRP)。在接着从安全 VM 361 接收到参数时，回放应用程序 350 解密或计算转换表块以获得明文转换表块，并提取所获得的转换表块中所包含的转换条目。

[0129] 在转换条目中，记录了 (a) 转换数据、(b) 标识符设置转换数据、和关于转换数据

在内容中的记录位置的记录位置指定信息。在步骤 S106 中，回放应用程序 350 与内容回放处理或输出处理同时地执行用于实时地将转换数据和标识符设置转换数据写入指定位置的数据转换处理。

[0130] 安全 VM 361 根据内容代码 334 为各个内容段生成不同的参数并输出所生成的参数。如果参数 SP1、SP2、SP3、.... 是与对应于内容段的转换条目的异或 (XOR) 计算参数，则在步骤 S106 中执行下列互斥计算操作作为表复原处理：

[0131] [转换条目 1](XOR)[SP1]

[0132] [转换条目 2](XOR)[SP2]

[0133] [转换条目 3](XOR)[SP3]，依此类推。

[0134] 然后，获取包含在转换表块数据中的转换条目。在以上的计算操作中，[A](XOR)[B] 指 A 和 B 之间的异或 (XOR) 运算。

[0135] 以此方式，记录在信息记录介质 330 上的内容 333 中所包括的转换条目与参数 SP1、SP2、SP3 等进行异或 (XOR) 运算。那些参数 SP1、SP2、SP3 等由安全 VM 361 获取并输出。

[0136] 在步骤 S106 中的表复原 / 数据转换处理中，从用参数 SP1、SP2、SP3 等计算或加密所复原的转换条目获取转换数据，并用所获得的是正确内容数据的转换数据替换该内容中所包括的破损数据。此外，部分数据还被标识符设置转换数据替换。然后，存储在明文 TS 缓冲器 353 中的数据被变成经转换数据。下面参照图 6 讨论此数据转换处理的概述。

[0137] 存储在信息记录介质 330 中的已加密内容 333 被临时存储在主机 350 的轨道缓冲器 352 中。存储在轨道缓冲器 352 中的已加密内容 333 对应于由图 6 中的 (1) 指示的轨道缓冲器存储数据 401。轨道缓冲器存储数据 401 被主机 350 解密成图 6 中的 (2) 所指示的已解密数据 402，并被存储在明文 TS 缓冲器 353 中。

[0138] 已解密数据 402 包含不是正确内容数据的破损数据 403。主机 350 的数据转换处理器因而用是正确内容数据的转换数据 404 替换破损数据 403。通过重写（盖写）明文 TS 缓冲器 353 中所存储的数据 402 的一部分来执行此替换处理。

[0139] 除了用是正确内容数据的转换数据 404 替换破损数据 403 的替换处理以外，如图 6 所示，主机 350 用标识符设置转换数据 405 替换一部分已解密数据 402。

[0140] 如上所述，标识符是可分析构成用于标识内容回放设备或内容回放应用程序的标识信息的位的数据。更具体地，标识符是关于是作为执行主机应用程序的播放器的信息处理设备的标识信息（播放器 ID）或根据播放器 ID 生成的标识标记。标识符设置转换数据 405 是通过以不影响内容的回放的程度稍微修改构成正确内容数据的位来生成的。

[0141] 多个标识符设置转换数据 405 被设置在内容中，且通过集中分析标识符设置转换数据 405，能标识例如播放器 ID。标识符设置转换数据 405 是能通过 MPEG 位流分析来标识构成标识标记的位的数据。

[0142] 在存储在信息记录介质 330 中的转换表 336 中，注册了图 6 中所示的许多转换数据 404 和标识符设置转换数据 405，并且还注册了关于转换数据 404 和标识符设置转换数据 405 的记录位置的信息。通过根据存储在转换表 336 中的信息来执行数据转换处理，存储在明文 TS 缓冲器 353 中的数据被用由图 6 中的 (3) 指示的经转换数据 406 替换。

[0143] 然后，经转换 TS 通过网络向外部源输出，并由外部回放设备回放。或者，在步骤

S107 中，TS 由多路分解器转换成流元 (ES)，且在步骤 S108 中，ES 被解码。已解码的 ES 由显示器扬声器回放。

[0144] 5. 使用安全检查代码的处理

[0145] 在开始上述内容回放处理前，安全 VM 361 用包含在内容代码 334 中的安全检查代码 335 进行安全检查。如果需要，安全 VM 361 在内容被回放时继续安全检查。

[0146] 安全 VM 361 在事件处理器 354 的控制下根据包含在内容代码 334 中的安全检查代码 335 来验证播放器（回放设备）的正当性。如上所述，转换表 336 和安全检查代码 335 包含各种类型的代码以允许根据播放器的类型和播放器端口信息来执行处理。

[0147] 安全 VM 361 获取诸如存储在播放器的存储单元中的播放器证书等关于播放器的信息（播放器信息 355）和关于播放器的端口的信息，并从安全检查代码 335 中选择对应于该播放器的安全检查代码以进行安全检查。即，安全 VM361 获取与信息处理设备或内容使用应用程序对应的标识信息和属性信息中的至少一个作为播放器信息，并选择与该播放器信息对应的安全检查代码以根据所选择的代码来执行安全检查。

[0148] 如上所述，当使用存储在信息记录介质中的内容时，安全 VM 361 执行安全检查。在作为安全检查的结果验证了播放器的正当性之后并且在根据例如播放器信息 355 确保未授权的内容输出被拒绝之后，该内容被回放。如果播放器的配置被改变，例如，如果新的装置被连接至播放器的端口，则可以根据播放器的改变后的配置来进行安全检查。

[0149] 根据回放设备的配置或回放应用程序的类型可能需要不同类型的安全检查。因此，安全检查代码 335 被作为与各种播放器和应用程序对应的一组代码记录在内容代码 334 中。

[0150] 下面参照图 7-9 来讨论记录在信息记录介质中的内容代码的结构。图 7 示出存储在信息记录介质中的全部数据的目录结构。信息记录介质中的存储数据主要被划分为两种数据：一种是包括诸如内容管理数据、CPS 单元密钥、内容使用控制信息 (CCI) 等的内容相关数据和内容的 BDMV 目录，另一种是包括诸如安全检查代码和转换表等内容代码的 BDSVM 目录。

[0151] 下面分别参照图 8 和 9 讨论 BDMV 目录和 BDSVM 目录的细节。当将具有参照图 2 讨论的分层结构的内容存储在信息记录介质中时，根据例如图 8 中所示的目录结构将诸如内容代码等各种数据和程序作为单独的文件记录在信息记录介质中。存储在信息记录介质中的文件是例如如下：

[0152] (A) 对应于图 2 中所示的索引层的 index.bdmv 文件；

[0153] (B) 对应于图 2 中所示的影片对象层 220 的 MovieObject.bdmv 文件；

[0154] (C) 对应于图 2 中所示的播放列表层 230 的 PLAYLIST 目录下的文件；

[0155] (D) 对应于图 2 中所示的剪辑层 240 的 CLIPNET 目录下的文件和 STREAM 目录下的文件，图 8 中所示的 CLIPNET 目录和 STREAM 目录下的文件根据相同的文件编号与图 2 中所示的剪辑和流相关联；以及

[0156] (E) 诸如存储声音数据和字体数据的 AUXDATA 文件、存储元数据的 META 文件和存储 BD-J 对象的 BDJO 文件等其它文件。

[0157] 在信息记录介质中所存储的内容中，如上所述，部分数据被不同于正确内容数据的破损数据所替换。为了正确地回放内容，需要用注册在转换表中的数据（已转换数据）

替换破损数据。在此替换处理中，通过用存储在信息记录介质中的内容代码将破损数据转换成注册在转换表（修正表）中的数据。

[0158] 包括转换表和安全检查代码的内容代码还作为单独的文件被存储在信息记录介质中。图 9 中示出包括内容代码的目录结构。图 9 中所示的目录结构是包括为具有图 8 中所示的目录结构的 AV 内容创建的内容代码的结构。

[0159] 如上所述，内容代码包括安全检查代码和转换表。如图 9 中所示，信息记录介质中的内容代码被存储在 BDSVM 目录中所设置的多个单独文件 nnnnn.svm 中。备份数据也被设置在 BACKUP 目录中作为复制数据。

[0160] 存储内容代码的文件被分类成下列类别：

[0161] (a) 所有内容项和所有播放器（回放设备或回放应用程序）共用的内容代码；

[0162] (b) 内容固有的内容代码；

[0163] (c) 播放器（回放设备或回放应用程序）固有的内容代码；和

[0164] (d) 内容和播放器（回放设备或回放应用程序）固有的内容代码。

[0165] 通过将内容代码分类成类别 (a)-(d)，该内容代码能被设置为独立的数据文件，因此能重复使用这些内容代码。即，可以将某些内容代码文件重复共用于不同的内容项和不同的播放器（回放设备或回放应用程序）。下面参照图 10 讨论内容代码的重复使用。

[0166] 在图 10 中，内容代码文件 601-604 是由内容代码生产或提供实体保持的文件。内容代码文件 601-604 分别是内容 / 播放器共用内容代码文件 00000.svm601、播放器固有内容代码文件 00001.svm 和 00002.svm 602、内容固有内容代码文件 00003.svm 603 和内容 / 播放器固有内容代码文件 00004.svm 604。

[0167] 在将内容代码生产或提供实体的数字签名被附加于内容代码文件 601-604 之后，它们被保持在内容代码生产实体或提供实体中。

[0168] 当生产存储新内容的信息记录介质时，每一实体能重复使用已用于另一内容的内容代码文件 601-604。如果，例如，内容固有内容代码文件和播放器固有内容代码文件被设置为同一文件，且在此情况中，如果内容被改变，则内容固有内容代码文件必须被改变。这意味着即使不必改变播放器固有内容代码，内容固有内容代码文件和播放器固有内容代码文件共用的内容代码文件也要被改变。因此，因为数字签名被附加于内容代码文件，所以它也应被改变，这妨碍了播放器固有内容代码文件的重复使用。相反，如果如图 10 所示，根据类别单独地创建内容代码文件，则在制造另一张盘时能重复使用例如播放器固有内容代码文件。

[0169] 为了防止内容代码的篡改，每一内容代码文件被提供给管理中心 (KIC)，并且被提供一数字签名并被存储在信息记录介质 610 中。管理中心将数字签名和唯一的 ID 附加于要被记录在信息记录介质 610 中的内容代码。如图 10 所示，记录在信息记录介质 610 上的内容代码 620 包括安全检查代码 621 和转换表（修正表）622。在特定的目录结构中，如图 10 中所示的目录结构 630 所指示地设置由单独的实体生成的内容代码。

[0170] 以此方式，能将内容代码重复用于各个内容项，并且能重复使用的内容代码和应改变的内容代码被适当地组合并被记录在信息记录介质中。

[0171] 如图 9 所示，内容代码文件能根据下列类别来设置：

[0172] 内容代码文件 00001.svm：用于确定播放器信息的代码；

[0173] 内容代码文件 00001.svm 和 00002.svm：根据播放器信息选择的代码（例如，00001.svm 是播放器 A 的代码而 00002.svm 是播放器 B 的代码）；以及

[0174] 内容代码文件 00003.svm：不依赖于播放器的代码（例如，00003.svm 中指示的默认代码被用于在内容发行之后出售的播放器）。

[0175] 如以上所讨论的，分类成各种类别的不同内容代码被存储在信息记录介质中，并且用内容代码进行安全检查的播放器（回放设备）选择与该播放器相关联的安全检查代码。

[0176] 图 5 中所示的安全 VM 361 选择对应于与安全 VM 361 相关联的播放器的安全检查代码以执行安全检查。在此情况中，安全 VM 361 获取播放器信息 355 以通过使用安全检查代码来执行安全检查。

[0177] 播放器信息 355 包括存储在播放器的存储器中的播放器证书和关于播放器的端口的信息。播放器信息 355 包括诸如能由安全 VM 361 从存储器中直接获取的信息、能通过回放应用程序获得的信息和能通过操作系统 (OS) 获得的信息等各种类型的信息。

[0178] 例如，能通过回放应用程序来获取诸如播放器证书等信息。然而，诸如为播放器设置的端口的数目等关于播放器的信息或关于连接至端口的装置的信息不一定直接通过回放应用程序来获取，而能仅通过诸如 OS 等另一程序来获取。安全 VM 361 直接或通过回放应用程序或另一程序来获取信息以执行安全检查。

[0179] 由安全 VM 361 执行的一种安全检查是检查回放设备是否具有授权的播放器证书。播放器证书证明内容的使用权，并由管理该内容的管理实体发放。

[0180] 图 11 中示出播放器证书的配置的一个例子。如图 11 中所示，播放器证书包括指示播放器证书大小、证书版本、播放器制造商 ID、序列号、签名时间和日期、装置（播放器）属性信息、播放器公钥和数字签名的数据。还可以包括除了上述数据以外的其它数据，诸如关于播放器型号名称和播放器型号版本等。

[0181] 安全 VM 361 根据从信息记录介质 330 读取的安全检查代码 335 来验证播放器证书，并且在验证了播放器证书的正当性之后，安全 VM 361 能从此证书中获取进一步的安全检查所需的信息。更具体地，安全 VM 361 首先通过使用例如作为已将签名附加于播放器证书的实体的管理中心的公钥来检查附加于播放器证书的签名的正当性。管理中心的公钥可以被预先存储在回放设备的存储器中或可以直接从信息记录介质 330 中或通过网络获取。

[0182] 如果播放器证书的正当性没有被验证，则不停止用于执行伴随着数据转换的内容回放的处理。如果播放器证书的正当性被验证，则对播放器进行安全检查。能从播放器证书中获取诸如制造商等基本播放器信息。

[0183] 即，安全 VM 361 检查播放器证书的正当性，并在播放器证书的正当性被验证的条件下，安全 VM 361 从记录在播放器证书上的信息中获取诸如该设备或应用程序的制造商、类型、版本和序列号等与信息处理设备或内容使用应用程序对应的标识信息或属性信息。基于所获取的信息，安全 VM 361 选择与所获取的信息对应的安全检查代码，以根据所选择的代码进行安全检查。诸如安全检查所需的信息等播放器信息由回放应用程序 350 或安全 VM 361 获取。

[0184] 下面参照图 12 描述除了播放器证书以外的播放器信息（播放器配置信息）。如图 12 中所示，用于进行安全检查的播放器信息包括下列信息：

[0185] ＊端口属性：单向、双向、模拟、数字、视频、音频、可记录 / 不要记录；

[0186] ＊端口状态：通过端口输出的数据的格式（复合视频、成分视频、数字音频和数字视频）和协议信息（VGA/HDCP/DTCP）；以及

[0187] ＊播放器信息：RAM 大小、系统时钟、和虚拟机器（VM）的数据转换（媒体转换）处理方法。

[0188] 当检查内容的未授权使用的可能性时，安全 VM 361 可能需要检查是否已执行使用特定端口的未授权的内容输出或复制。在此情况中，安全 VM 361 参考作为播放器信息 355 获取的端口属性和端口状态，并选择与该播放器信息 355 对应的合适的安全检查代码以检查内容的未授权使用。通过使用播放器信息 355 选择和应用合适的安全检查代码实现了使用内容代码的高效且有效的安全检查。即，执行内容代需要一定的执行时间。因此，通过执行从存储在盘中的多个安全检查代码选择的必要安全检查代码，能快速地执行安全检查而不会降低安全等级。能如下地确保安全检查代码的执行速度。首先指定播放器，并根据所指定的播放器的性能来选择安全检查代码以允许具有较高性能的播放器比具有较低性能的播放器执行更多安全检查代码。以此安排，用户无需在安全检查代码被执行时等待。更具体地，首先确定用于执行安全检查代码的时间，然后，生成和选择安全检查代码以使得能在给定时间内完成安全检查代码的执行。

[0189] 回放应用程序 350 或安全 VM 361 经由各种路由来获取播放器信息 355。必要的播放器信息 355 被获取，且安全 VM 361 通过使用该播放器信息 355 来执行安全检查代码 355，以进行安全检查。

[0190] 下面参照图 13 讨论用于获取播放器信息的处理。图 13 示出构成例如 PC 或只回放装置（消费者电子（CE）设备）等执行内容回放的回放设备的层。在图 13 中，示出诸如执行内容回放的回放应用程序 701 等作为最高层的过程执行应用程序，OS 711 在回放应用程序 701 之下，而包括各种硬件和装置驱动器的硬件 / 装置驱动器 721 在 OS 711 之下。

[0191] 作为虚拟机由回放应用程序 701 生成的安全 VM 702 用安全检查代码进行安全检查。安全 VM 702 通过获取各种播放器信息来进行安全检查。例如，图 11 中所示的播放器证书被存储在回放设备的存储器中，并被包含在能由回放应用程序 701 直接获取的播放器信息 703 中。诸如装置 / 应用程序相关信息等其它信息，例如 CE 装置的端口数目，也被包含在播放器信息 703 中。

[0192] 相反，关于与回放设备的端口连接的各种装置的信息不包含在能由回放应用程序 701 直接获取的播放器信息 703 中。这种信息包括关于硬件 / 装置驱动器 721 的装置信息，并被包含在能由 OS 711 获取的播放器信息 713 中。

[0193] 回放应用程序 701 从 OS 711 获取播放器信息 713，并将其提供给执行安全检查的安全 VM 702。

[0194] 能由回放应用程序 701 从 OS 711 获取的播放器信息 713 包括可以由例如系统的扩展或外部装置的连接改变的信息。这种信息能在回放应用程序 701 被执行的同时从 OS 711 的装置管理器 712 获取，并包括关于例如平台和端口的信息。

[0195] 现在假设当回放应用程序 701 被启动时，它检查设备的状况，然后根据设备的配置执行内容回放。在此情况中，回放应用程序 701 获取关于设备的状况的信息并向安全 VM 702 提供该信息。如果回放应用程序 701 具有在回放应用程序 701 被启动后获取关于例如

与该设备连接的新装置的最新信息的功能，则它在需要时向安全 VM 702 提供更新后的信息。

[0196] 存在一些诸如由图 13 中的 C2 指示的不能由回放应用程序 701 从 OS 711 获取的装置信息。例如，一般的回放应用程序难以获取存储在装置驱动器中的寄存器值，除非它在装置驱动器和 OS 711 的帮助下执行特定的处理。

[0197] 基本上，回放应用程序 701 不获取这种信息，并通过只使用诸如播放器证书和设备信息等可用的播放器信息来进行安全检查。

[0198] 下面参照图 14 中的流程图来给出包括用内容代码中所包括的安全检查代码进行安全检查处理和用转换表进行转换处理的内容回放序列的说明。

[0199] 在步骤 S301 中，安全 VM 从信息记录介质获取内容代码并确定获取播放器信息的请求是否被包括在内容代码中。例如，安全 VM 读取图 9 中所示的目录结构中存储用于确定播放器信息的代码的内容代码文件 00000.svm。

[0200] 如果在步骤 S301 中确定获取播放器信息的请求没有被包括在内容代码中，则过程进到步骤 S306。如果获取播放器信息的请求被包括在内容代码中，则过程进到步骤 S302 以获取安全检查所需的播放器信息。播放器信息包括例如图 11 中所示的播放器证书、及端口属性、端口状态、以及诸如图 12 中所示的其它播放器信息。如参照图 13 所讨论的，诸如 PC 等具有扩展功能的设备从 OS 的装置管理功能获取播放器信息以获取端口属性。CE 装置获取固定的值作为播放器信息，因为 CE 装置的端口属性是固定的。以此方式，取决于设备的类型，所需的播放器信息是不同的，并且还以不同的方式获取播放器信息。

[0201] 在步骤 S303 中，确定与所获取的播放器信息对应的安全检查代码是否被包括在内容代码中。如果在步骤 S303 中确定安全检查代码被包括，则过程进到步骤 S304 以执行与此安全检查代码对应的安全检查。通过使用根据播放器信息选择的例如图 9 中所示的内容代码文件 00001.svm 或 00002.svm 来进行安全检查。

[0202] 如果然后在步骤 S305 中确定是否存在任何问题作为安全检查的结果。如果发现问题，则终止用于执行内容回放的处理。如果作为安全检查的结果不存在问题，则过程进到步骤 S306 以确定是否需要用包含在内容代码中的转换表进行数据转换处理。如果不需要数据转换处理，则过程进到步骤 S308 以执行内容回放。

[0203] 如果在步骤 S306 中确定需要进行数据转换处理，则过程进到步骤 S307 以获取转换表并将其解密以通过使用记录在转换表中的信息来执行内容转换处理。此转换处理对应于参照图 6 所讨论的处理。然后，在步骤 S307 中，内容被回放。应注意，步骤 S307 中的数据转换处理和步骤 S308 中的内容回放处理同时执行。

[0204] 6. 信息处理设备的配置

[0205] 现在参照图 15 给出用上述回放（播放器）应用程序和安全 VM 执行数据处理的信息处理设备（主机）800 的硬件配置的说明。信息处理设备 800 包括：中央处理单元 (CPU)809、用作其中存储程序和参数的存储区的 ROM 808、存储器 810、用于输入和输出数字信号的数字输入 / 输出接口 (I/F)802、用于输入和输出模拟信号并包括模数 (A/D) 和数模 (D/A) 转换器 805 的模拟输入 / 输出接口 804、用于编码和解码 MPEG 数据的 MPEG 编解码器 803、用于执行传输流 (TS) / 程序流 (PS) 处理的 TS/PS 处理器 806、用于执行相互认证和诸如已加密内容的解密等各种类型的加密处理的加密单元 807、诸如硬盘等记录介质 812、

以及用于驱动记录介质 812 并输入和输出数据记录 / 回放信号的驱动器 811。上述单元与总线 801 连接。CPU 809 执行根据包括伴随由 OS 或内容回放 / 记录应用程序执行的处理的各种类型的处理在内的各种程序的数据处理、相互认证处理和内容回放，例如基于安全检查代码的安全检查处理和使用转换表的数据转换处理。

[0206] 信息处理设备 800 通过诸如先进技术附加分组接口 (ATAPI)-BUS 总线等连接总线连接至驱动器 811。转换表和内容通过数字输入 / 输出接口 802 输入或输出。加密处理器 807 通过使用例如 AES 算法来执行加密处理和解密处理。

[0207] 用于执行内容回放 / 记录处理的程序被存储在例如 ROM 808 中，且存储器 810 用作工作区或在程序被执行时用于存储参数和数据。

[0208] 在 ROM 808 或记录介质 812 中，存储了上述播放器证书、用于验证播放器证书的签名的管理中心的公钥、用于执行驱动器 811 的认证的主机私钥和主机公钥、以及被无效的公钥证书的无效列表。

[0209] 为了回放内容或向外部源输出内容，通过使用从信息记录介质 812 获取的数据转换处理程序，根据上述处理序列，执行已加密内容的解密、转换表的复原和根据存储在转换表中的数据的转换数据的盖写。

[0210] 7. 信息记录介质制造设备和信息记录介质

[0211] 下面讨论信息记录介质和信息记录介质制造设备，更具体地，在上述内容回放处理中所使用的信息记录介质和用于该信息记录介质的制造设备和方法。

[0212] 信息记录介质制造设备是用于制造例如参照图 1 所述的存储所记录的数据的信息记录介质 100 的设备。如图 16 所示，信息记录介质制造设备包括 :用于生成存储要记录在信息记录介质 910 上的内容数据的内容文件的内容文件生成器 901、用于生成存储包括使用内容要执行的安全检查处理程序的内容代码的内容代码文件的内容代码文件生成器 902、以及将由内容文件生成器 901 生成的内容文件和由内容代码文件生成器 902 生成的内容代码文件记录在信息记录介质 910 上的记录器 903。

[0213] 如参照图 9 所讨论的，内容代码文件生成器 902 根据信息处理设备和内容使用应用程序的各种类型生成多个内容代码文件。

[0214] 内容代码文件生成器 902 还生成存储不依赖于信息处理设备或内容使用应用程序的类型的共用内容代码的内容代码文件、存储依赖于信息处理设备或内容使用应用程序的类型的内容代码的内容代码文件、以及存储用于确定信息处理设备或内容使用应用程序的类型的代码的内容代码文件。记录器 903 将那些各种内容代码文件记录在信息记录介质 910 上。

[0215] 当产生多个存储被分类成不同类别的内容代码的内容代码文件时，内容代码文件生成器 902 生成多个均设有数字签名的文件或多个只有其中之一设有数字签名的文件。附加于由内容代码文件生成器 902 生成的文件的数字签名可以只是管理中心 (KIC) 的数字签名，或可以是管理中心的数字签名和内容代码生产或提供实体的数字签名。

[0216] 在由信息记录介质制造设备生成的信息记录介质 910 上，记录了以上讨论的各种数据。更具体地，至少记录了用于存储内容数据的内容文件和用于存储包括使用内容所要执行的安全检查处理程序的内容代码的内容代码文件。内容代码文件包括与信息处理设备或内容使用应用程序相关联的多个内容代码文件。

[0217] 如以上参照图 9 所讨论的，记录在信息记录介质 910 上的内容代码文件可以被分类成用于存储不依赖于信息处理设备或内容使用应用程序的类型的共用内容代码的代码文件、用于存储依赖于信息处理设备或内容使用应用程序的类型的内容代码的代码文件、和存储用于确定信息处理设备或内容使用应用程序的类型的代码的代码文件。

[0218] 要被记录在信息记录介质上的内容代码文件包括存储被分类成不同类别的内容代码的多个内容代码文件。在多个所记录的文件中，可以只有一个文件设有数字签名，或可所有文件均设有数字签名。内容代码生产或提供实体的数字签名可以被附加于内容代码文件。

[0219] 本说明书中所描述的一系列处理操作可以由硬件、软件或其组合来执行。如果使用软件，则可以将其中存储处理序列的程序安装到置于专用硬件中的计算机存储器中，或安装到能执行各种类型的处理的通用计算机中，然后执行该程序。

[0220] 程序可以被预先存储在用作记录介质的硬盘或 ROM 中。或者，程序可以被临时或永久地存储（记录）在诸如软盘、光盘只读存储器 (CD-ROM)、磁光盘 (MO)、数字多功能盘 (DVD)、磁盘或半导体存储器等可移动记录介质中。这种可移动记录介质可以作为所谓的“软件包”被提供。

[0221] 如上所述，可以将程序从上述可移动记录介质安装到计算机中。或者，可以无线地或经由诸如局域网 (LAN) 或因特网等网络以有线方式将程序从下载站点传送至计算机。在此情况中，计算机接收该程序并将其安装到诸如硬盘等内建记录介质中。

[0222] 可以按本说明书中所讨论的时间顺序来执行本说明书中所描述的各种处理操作。或者，可以根据执行处理的设备的性能或根据需要并行地或单独地执行这些处理操作。在本说明书中，系统是多个装置的逻辑组，且这些装置不一定要在同一外壳中。

[0223] 本领域的技术人员应理解，根据设计要求和其它因素可以有各种修改、组合、子组合和变更，但它们仍落在所附权利要求或其等效方案的范围内。

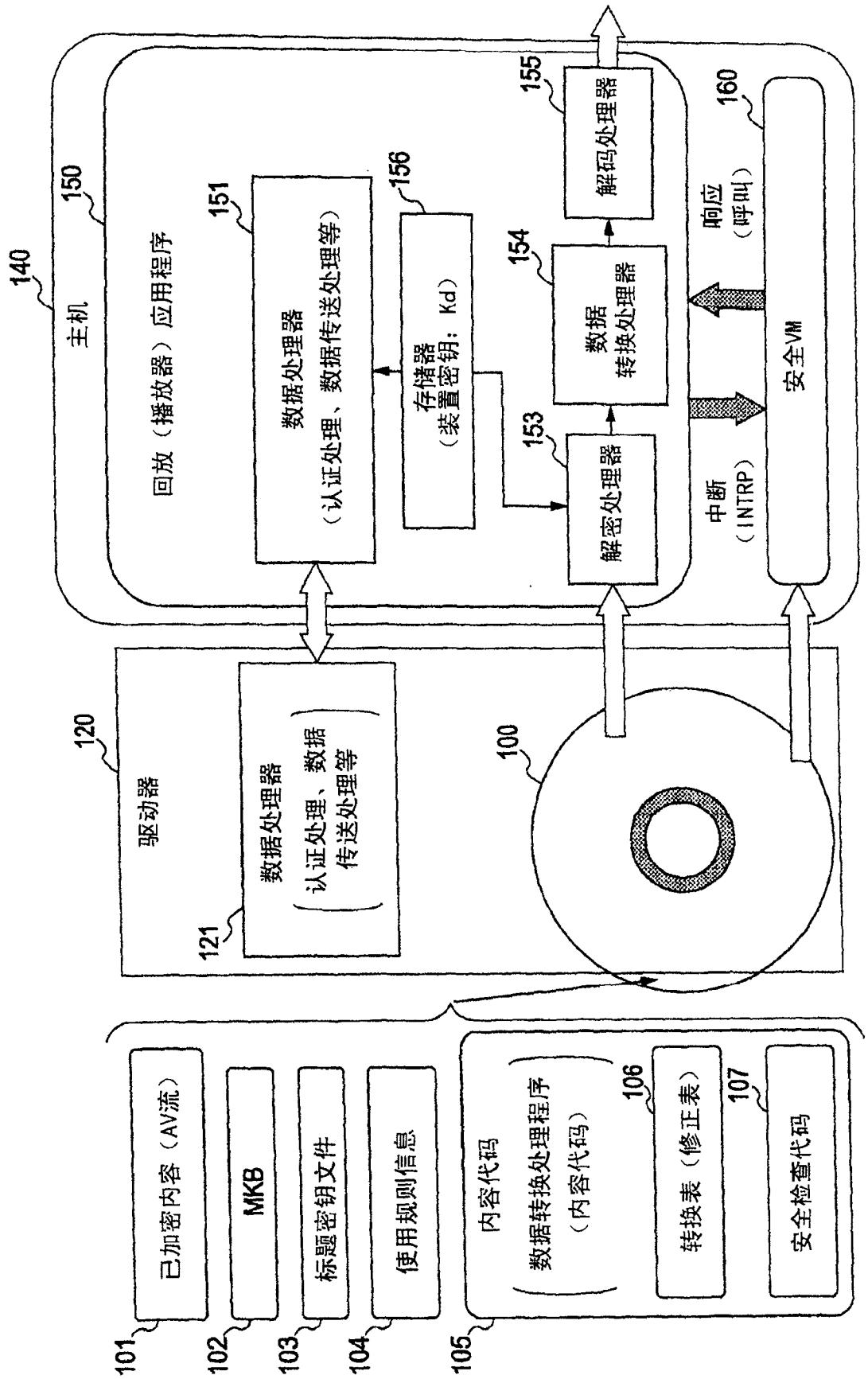

140
主机
150
回放（播放器）应用程序
151
数据处理器
（认证处理、数据传送处理等）
156
存储器
（装置密钥：Kd）
153
解密处理器
154
数据
转换处理器
155
解码处理器
160
响应
（呼叫）
中断
（INTRP）
安全VM
120
驱动器
121
数据处理器
（认证处理、数据
传送处理等）
100
101
已加密内容（AV流）
102
MKB
103
标题密钥文件
104
使用规则信息
105
内容代码
数据转换处理程序
（内容代码）
106
转换表（修正表）
107
安全检查代码

图 1

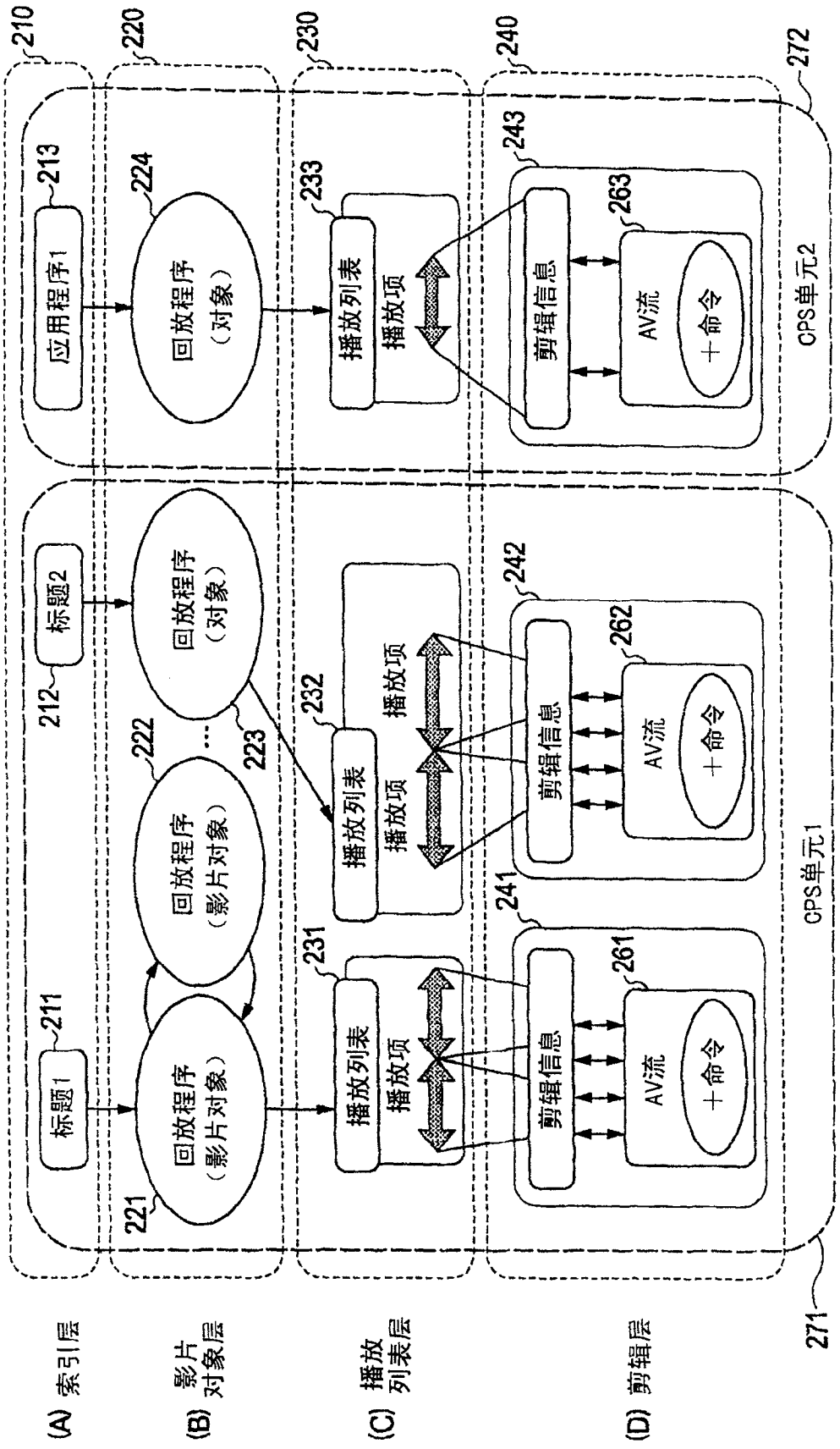

210
220
230
240
272
应用程序1
213
224
回放程序
（对象）
233
播放列表
播放项
243
剪辑信息
263
AV流
+命令
CPS单元2
标题2
212
回放程序
（对象）
222
回放程序
（影片对象）
223
232
播放列表
播放项
播放项
242
剪辑信息
262
AV流
+命令
标题1
211
回放程序
（影片对象）
221
231
播放列表
播放项
241
剪辑信息
261
AV流
+命令
CPS单元1
271
(A) 索引层
(B) 影片对象层
(C) 播放列表层
(D) 剪辑层

图 2

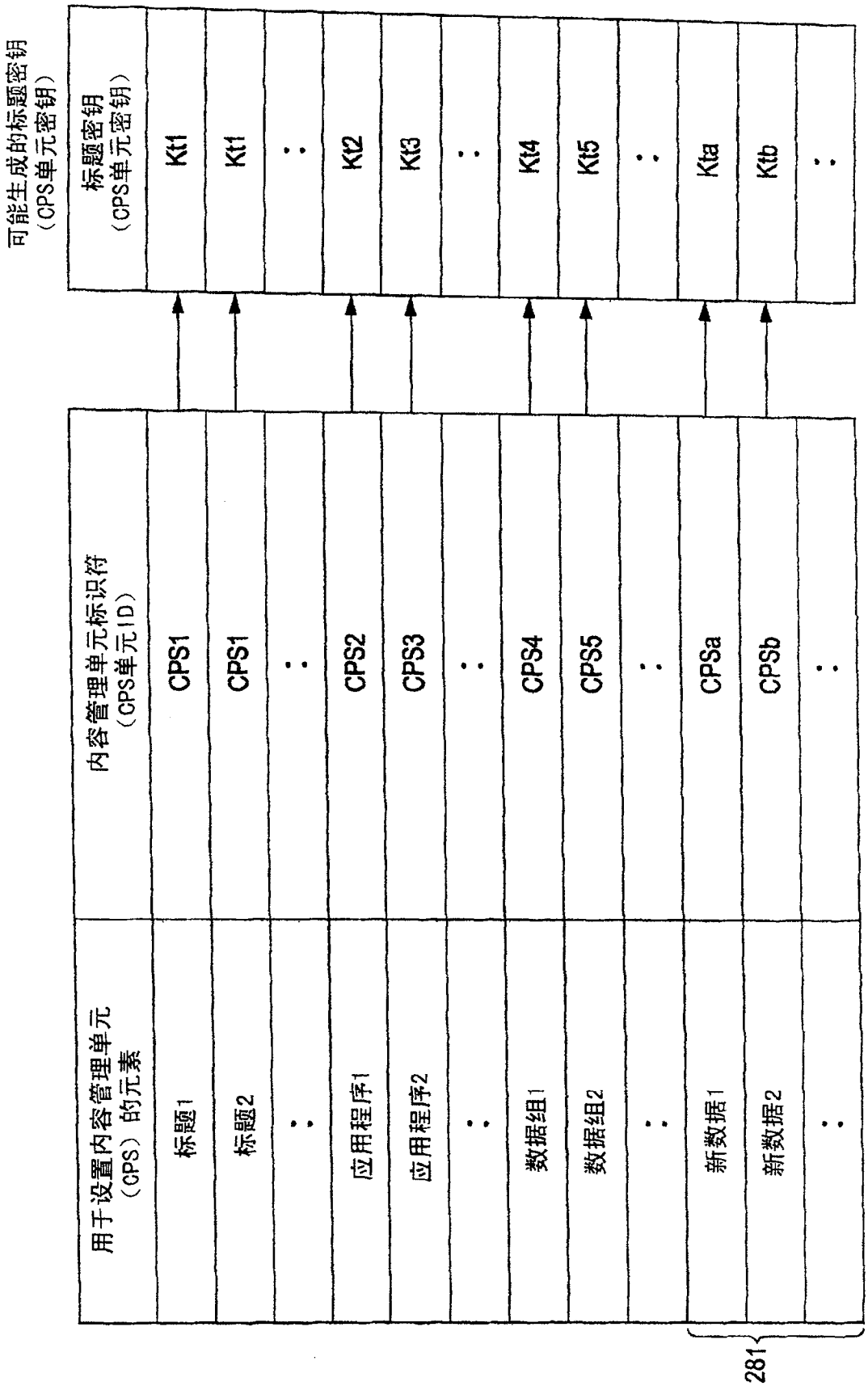

可能生成的标题密钥
（CPS单元密钥）
标题密钥
（CPS单元密钥）
Kt1
Kt1
Kt2
Kt3
Kt4
Kt5
Kta
Ktb
内容管理单元标识符
（CPS单元ID）
CPS1
CPS1
CPS2
CPS3
CPS4
CPS5
CPSa
CPSb
用于设置内容管理单元
（CPS）的元素
标题1
标题2
应用程序1
应用程序2
数据组1
数据组2
新数据1
新数据2
281

图 3

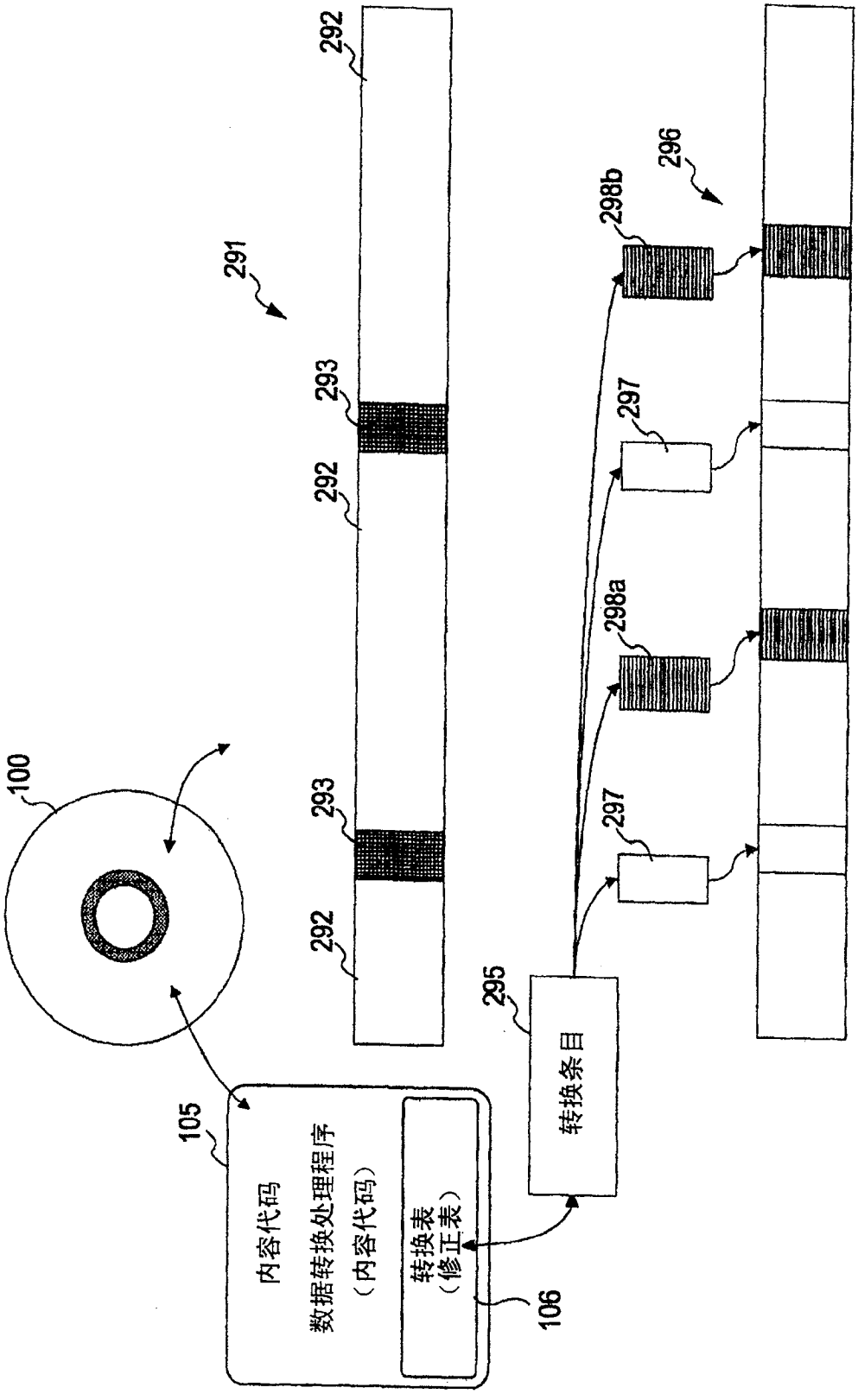

100
105
内容代码
数据转换处理程序
（内容代码）
转换表
（修正表）
106
291
292
293
292
293
292
295
转换条目
296
298b
297
298a
297

图 4

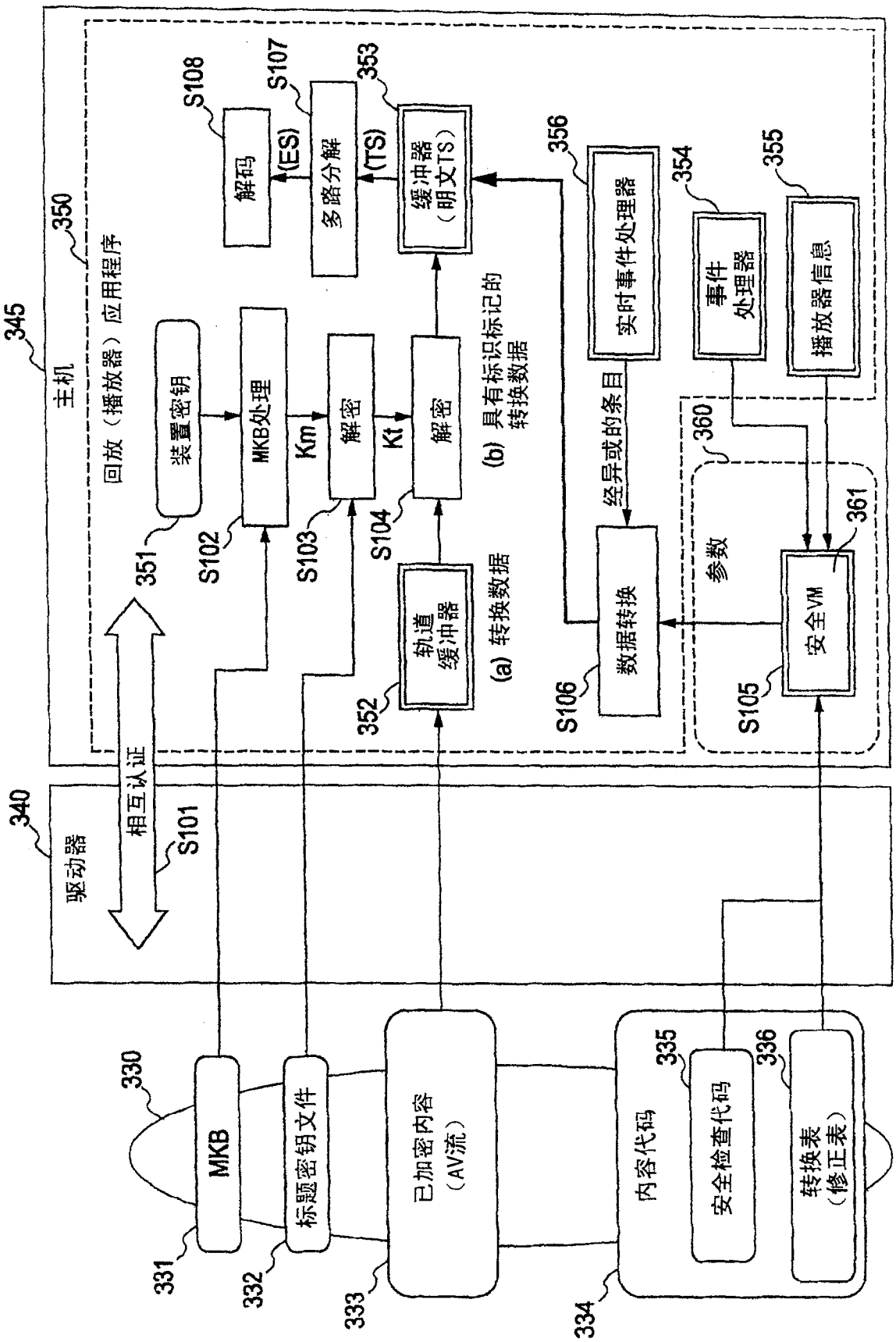

345
主机
350
回放（播放器）应用程序
340
驱动器
相互认证
S101
351
装置密钥
S102
MKB处理
Km
S103
解密
Kt
S104
解密
352
轨道缓冲器
(a) 转换数据
(b) 具有标识标记的转换数据
S108
解码
S107
(ES)
多路分解
(TS)
353
缓冲器（明文TS）
356
实时事件处理器
经异或的条目
S106
数据转换
360
参数
S105
安全VM
361
354
事件处理器
355
播放器信息
330
MKB
331
标题密钥文件
332
已加密内容（AV流）
333
内容代码
335
安全检查代码
336
转换表（修正表）
334

图 5

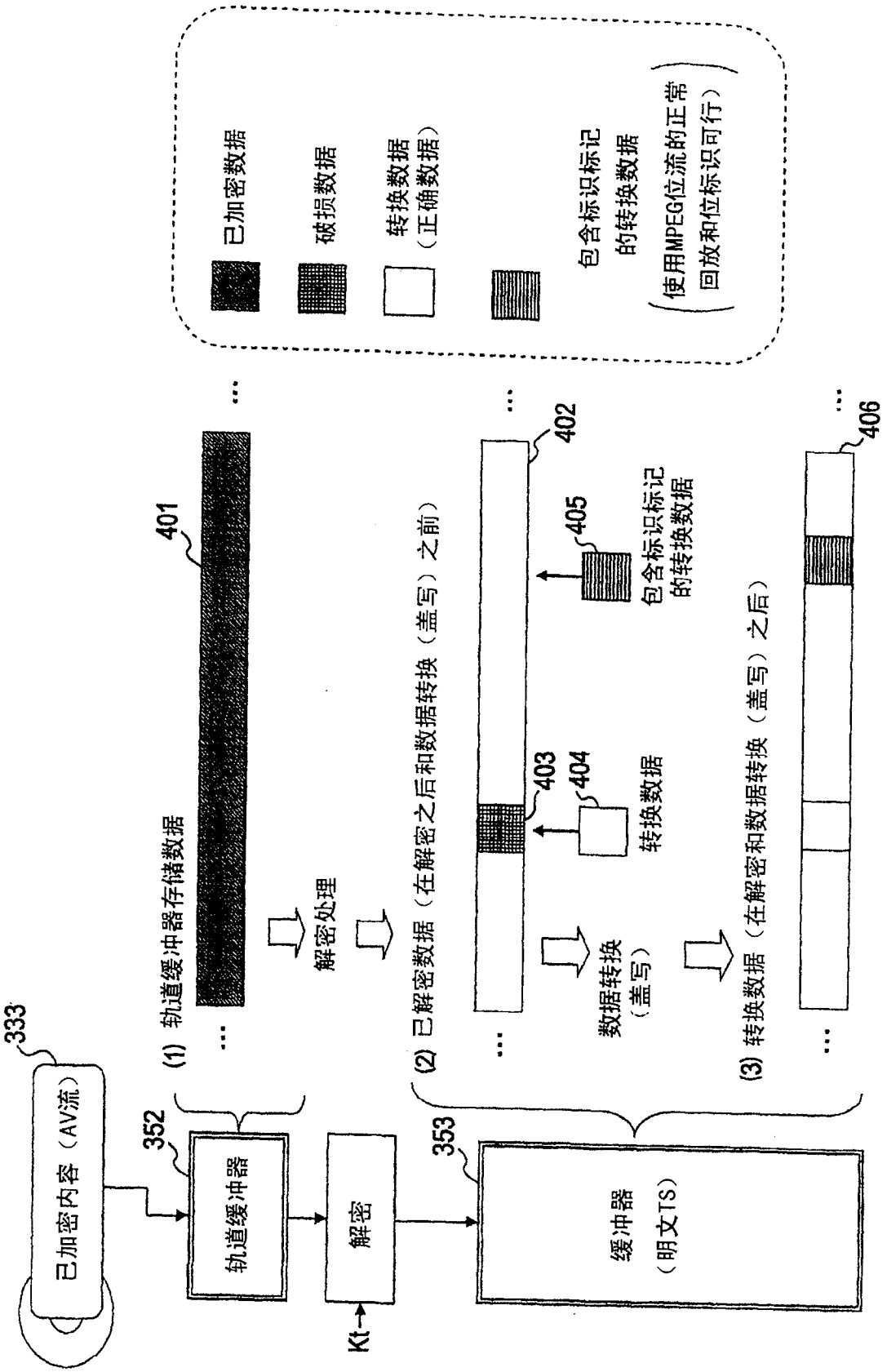

已加密数据
破损数据
转换数据
（正确数据）
包含标识标记
的转换数据
（使用MPEG位流的正常
回放和位标识可行）
333
已加密内容（AV流）
352
轨道缓冲器
解密
Kt
353
缓冲器
（明文TS）
(1) 轨道缓冲器存储数据
401
解密处理
(2) 已解密数据（在解密之后和数据转换（盖写）之前）
402
403
404
405
转换数据
包含标识标记
的转换数据
数据转换
（盖写）
(3) 转换数据（在解密和数据转换（盖写）之后）
406

图 6

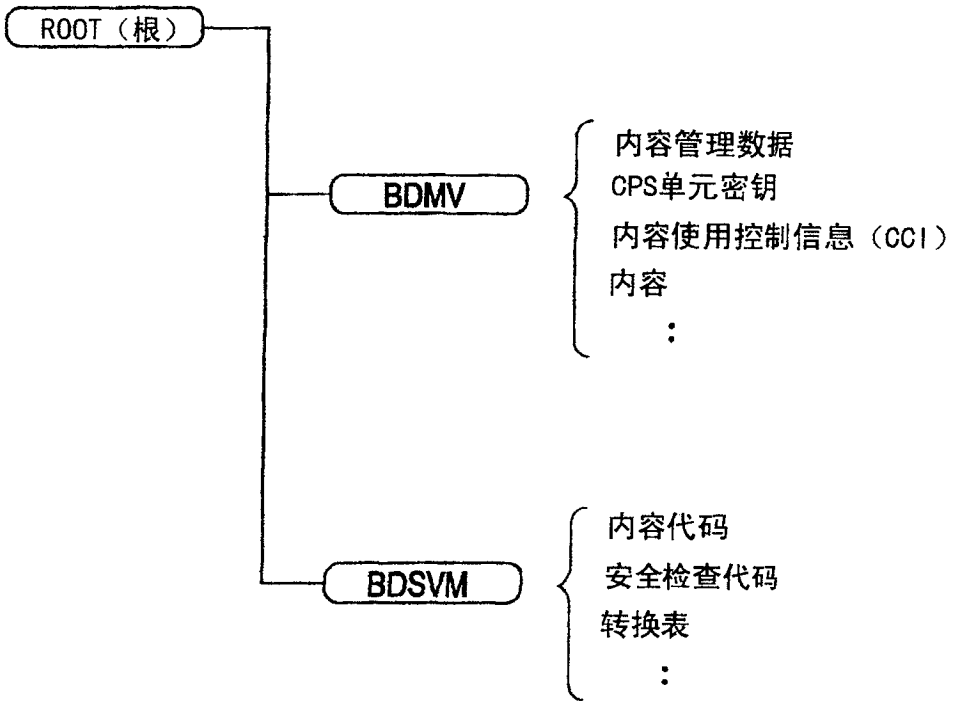

ROOT（根）
BDMV
内容管理数据
CPS单元密钥
内容使用控制信息（CCI）
内容
：
BDSVM
内容代码
安全检查代码
转换表
：

图 7

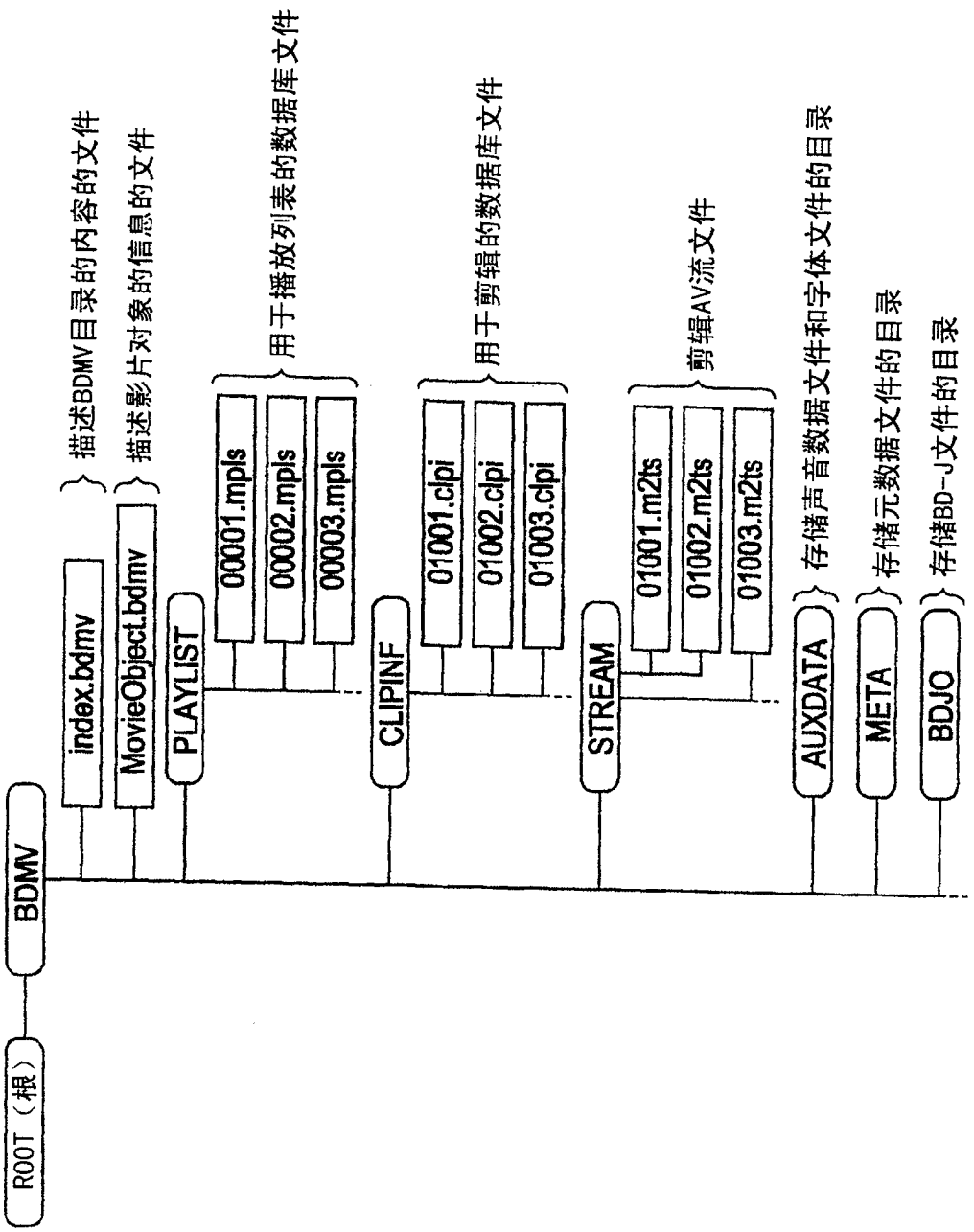

ROOT（根）
BDMV
index.bdmv
描述BDMV目录的内容的文件
MovieObject.bdmv
描述影片对象的信息的文件
PLAYLIST
00001.mpls
00002.mpls
00003.mpls
用于播放列表的数据库文件
CLIPINF
01001.clpi
01002.clpi
01003.clpi
用于剪辑的数据库文件
STREAM
01001.m2ts
01002.m2ts
01003.m2ts
剪辑AV流文件
AUXDATA
存储声音数据文件和字体文件的目录
META
存储元数据文件的目录
BDJO
存储BD-J文件的目录

图 8

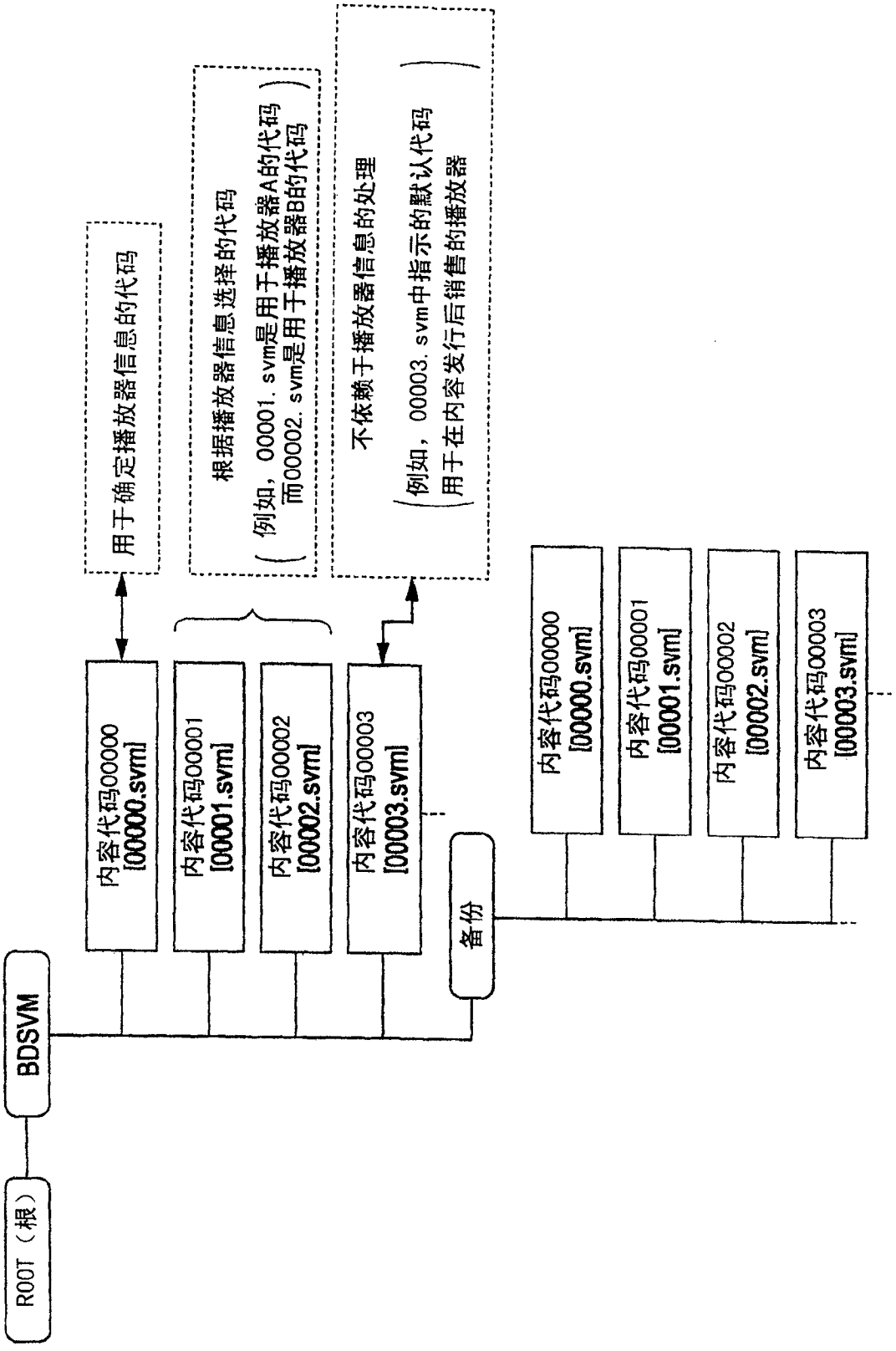

ROOT（根）
BDSVM
内容代码00000 [00000.svm]
内容代码00001 [00001.svm]
内容代码00002 [00002.svm]
内容代码00003 [00003.svm]
备份
内容代码00000 [00000.svm]
内容代码00001 [00001.svm]
内容代码00002 [00002.svm]
内容代码00003 [00003.svm]
用于确定播放器信息的代码
根据播放器信息选择的代码
（例如，00001. svm是用于播放器A的代码
而00002. svm是用于播放器B的代码）
不依赖于播放器信息的处理
（例如，00003. svm中指示的默认代码
用于在内容发行后销售的播放器）

图 9

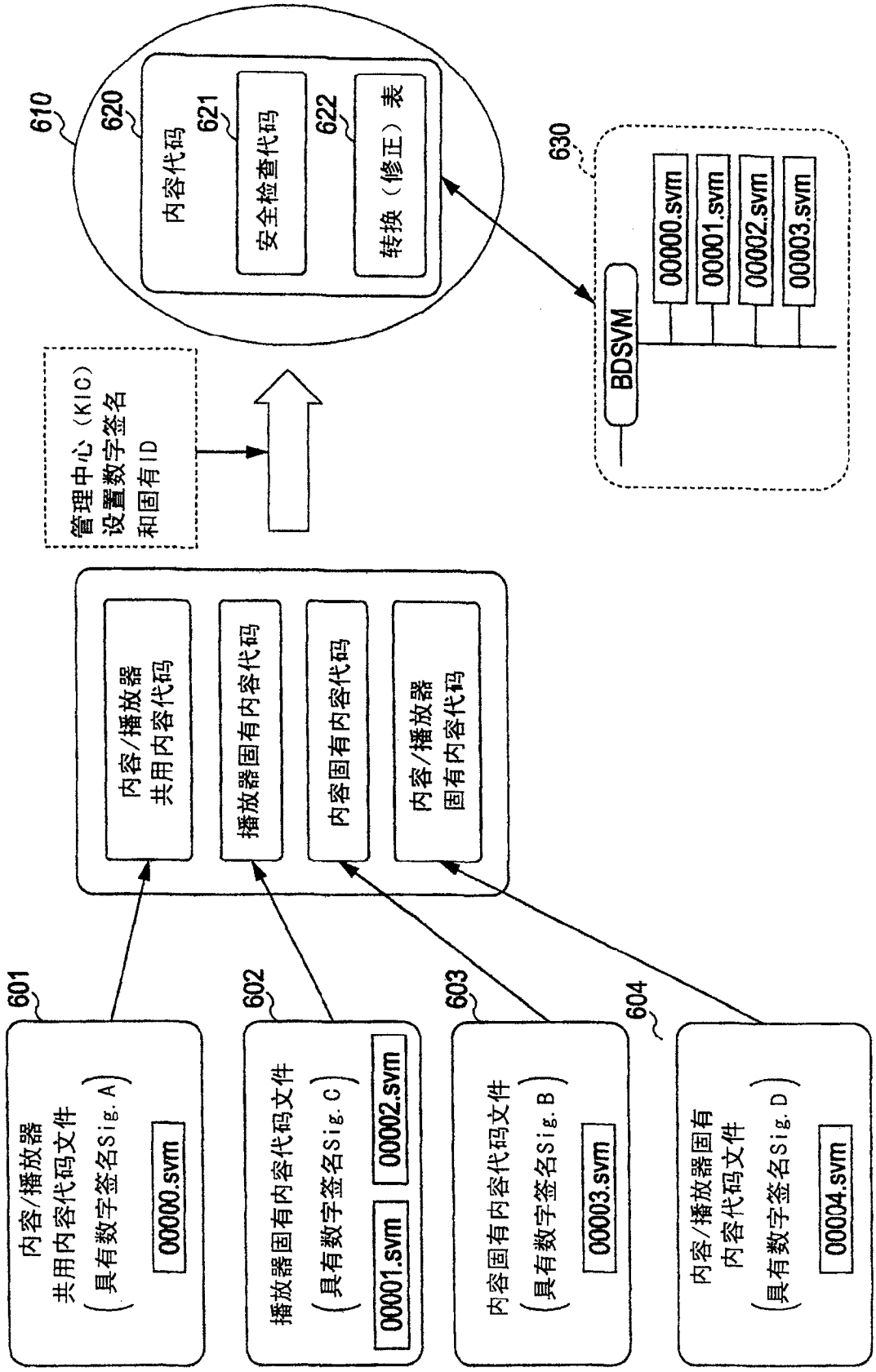

610
620
内容代码
621
安全检查代码
622
转换（修正）表
630
BDSVM
00000.svm
00001.svm
00002.svm
00003.svm
管理中心（KIC）
设置数字签名
和固有ID
内容/播放器
共用内容代码
播放器固有内容代码
内容固有内容代码
内容/播放器
固有内容代码
601
内容/播放器
共用内容代码文件
（具有数字签名Sig.A）
00000.svm
602
播放器固有内容代码文件
（具有数字签名Sig.C）
00001.svm
00002.svm
603
内容固有内容代码文件
（具有数字签名Sig.B）
00003.svm
604
内容/播放器固有
内容代码文件
（具有数字签名Sig.D）
00004.svm

图 10

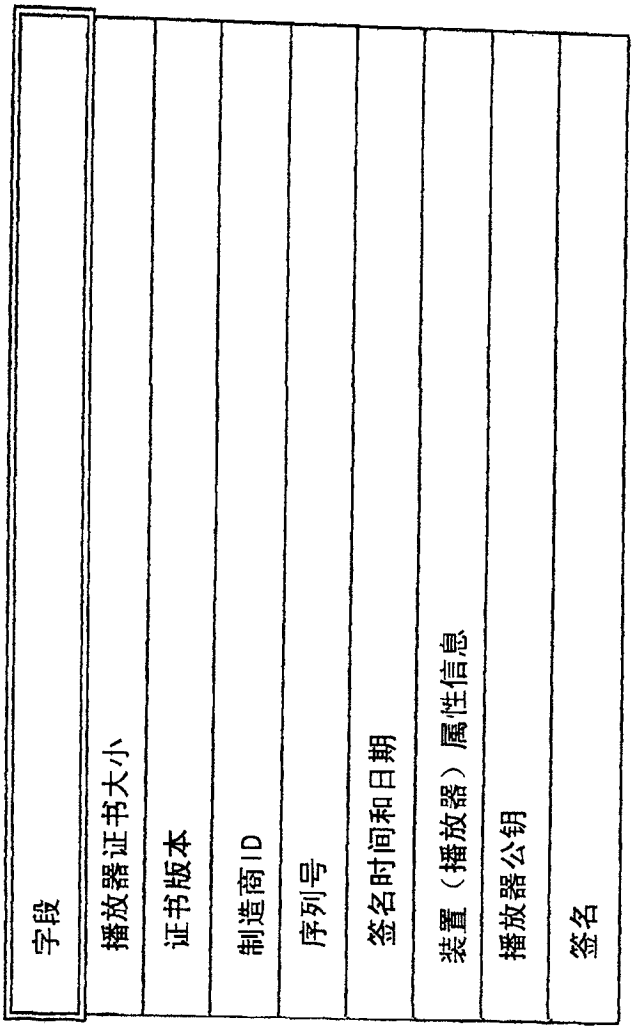


图 11

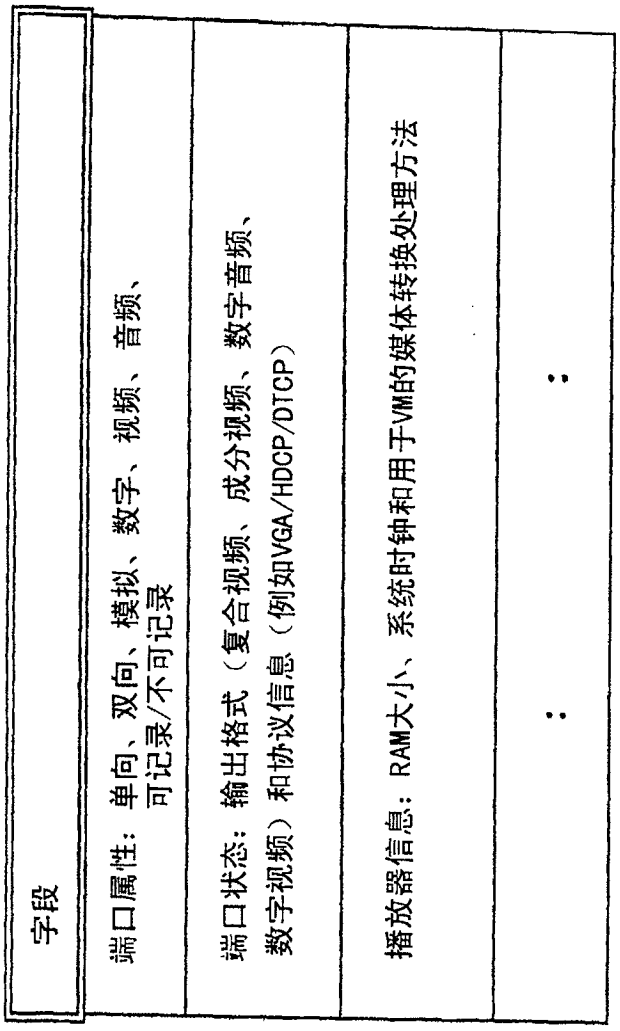

字段
端口属性：单向、双向、模拟、数字、视频、音频、
可记录/不可记录
端口状态：输出格式（复合视频、成分视频、数字音频、
数字视频）和协议信息（例如VGA/HDCP/DTCP）
播放器信息：RAM大小、系统时钟和用于VM的媒体转换处理方法
：
：

图 12

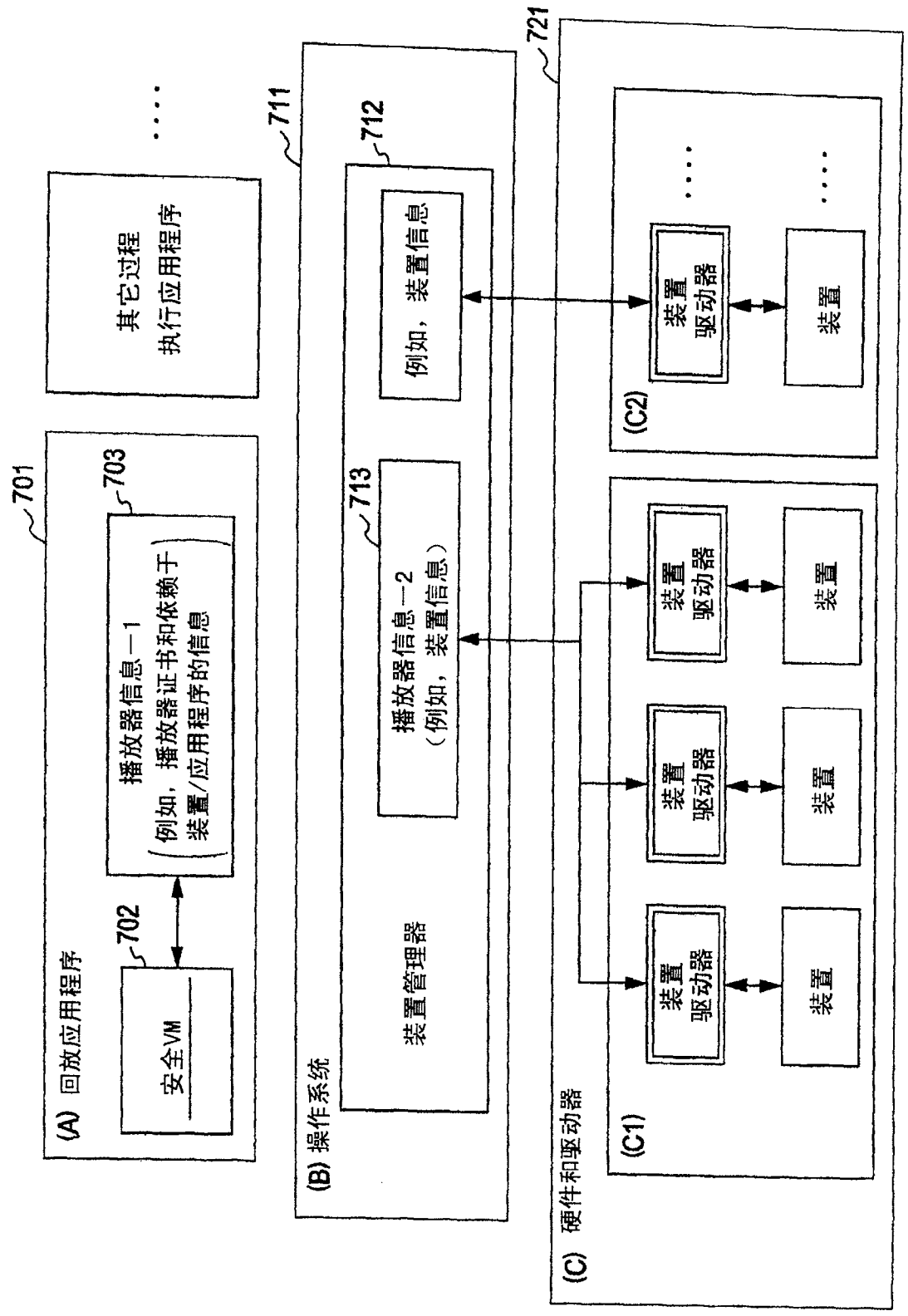

701
(A) 回放应用程序
703
播放器信息—1
(例如，播放器证书和依赖于装置/应用程序的信息)
702
安全VM
其它过程
执行应用程序
711
(B) 操作系统
712
例如，装置信息
713
播放器信息—2
(例如，装置信息)
装置管理器
721
(C) 硬件和驱动器
(C1)
(C2)
装置
驱动器

图 13

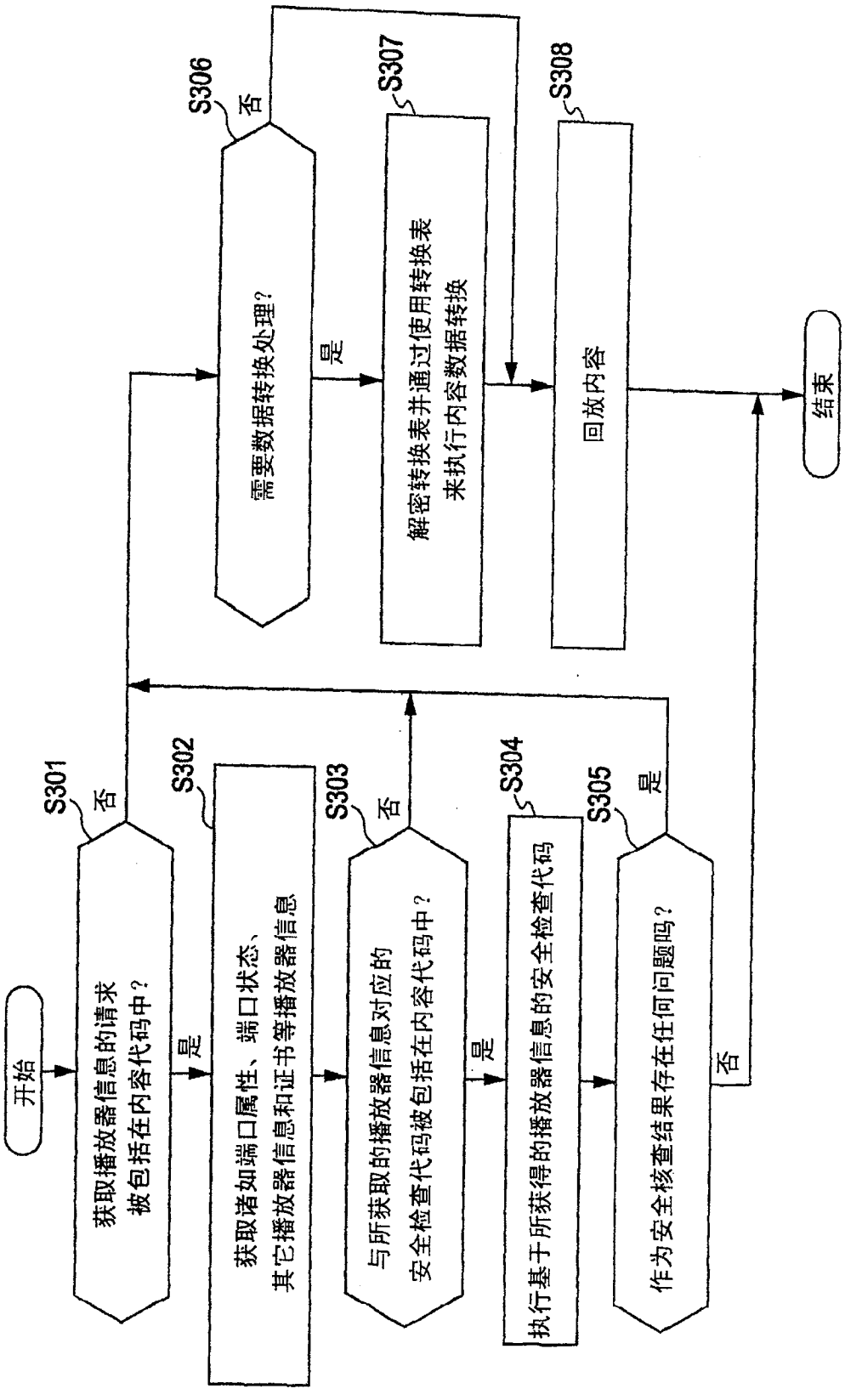

开始
获取播放器信息的请求
被包括在内容代码中？
S301
否
是
获取诸如端口属性、端口状态、
其它播放器信息和证书等播放器信息
S302
与所获取的播放器信息对应的
安全检查代码被包括在内容代码中？
S303
否
是
执行基于所获得的播放器信息的安全检查代码
S304
作为安全核查结果存在任何问题吗？
S305
是
否
需要数据转换处理？
S306
否
是
解密转换表并通过使用转换表
来执行内容数据转换
S307
回放内容
S308
结束

图 14

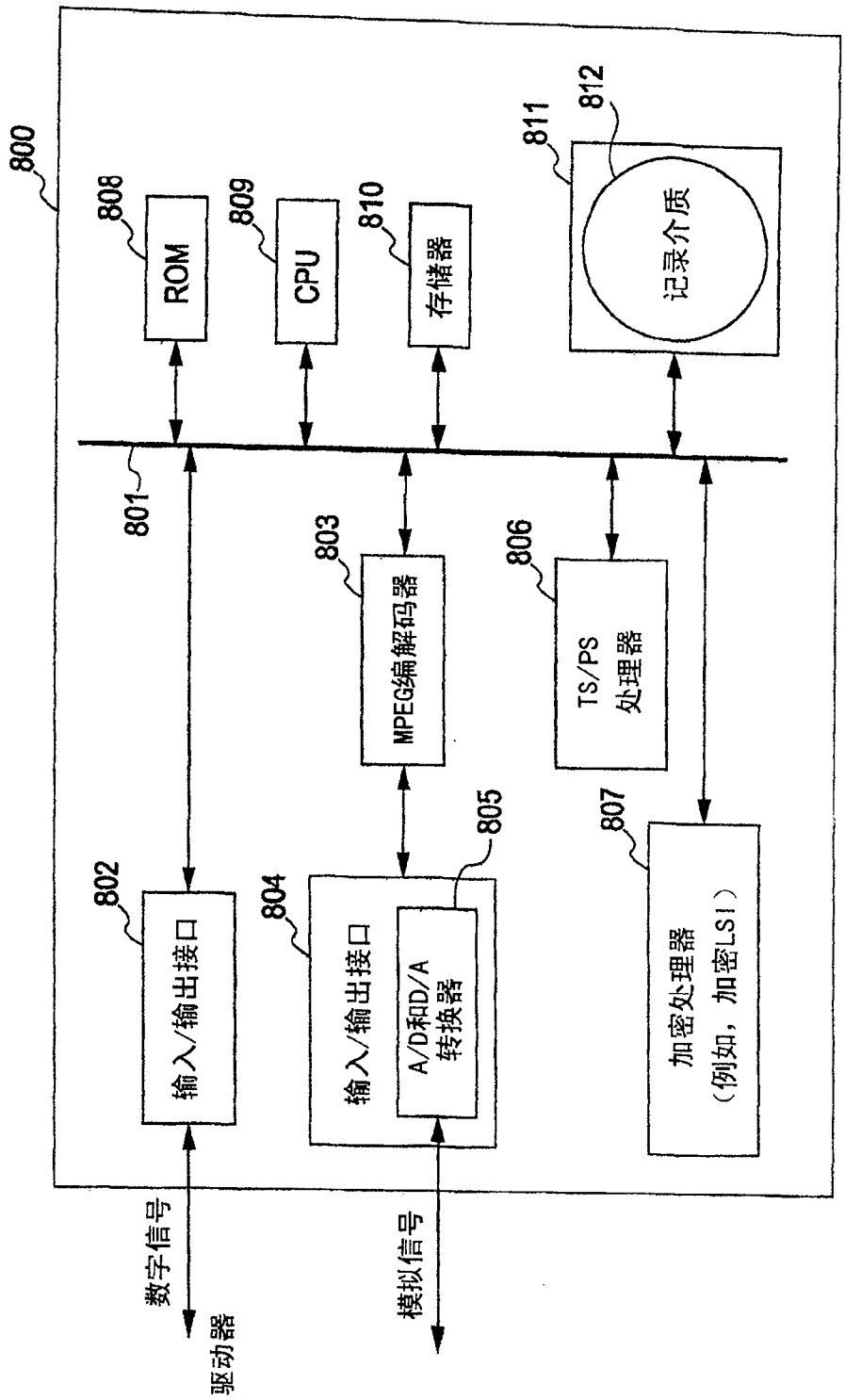

800
808
ROM
809
CPU
810
存储器
811
812
记录介质
801
803
MPEG编解码器
806
TS/PS
处理器
802
输入/输出接口
804
输入/输出接口
805
A/D和D/A
转换器
807
加密处理器
（例如，加密LSI）
数字信号
驱动器
模拟信号

图 15

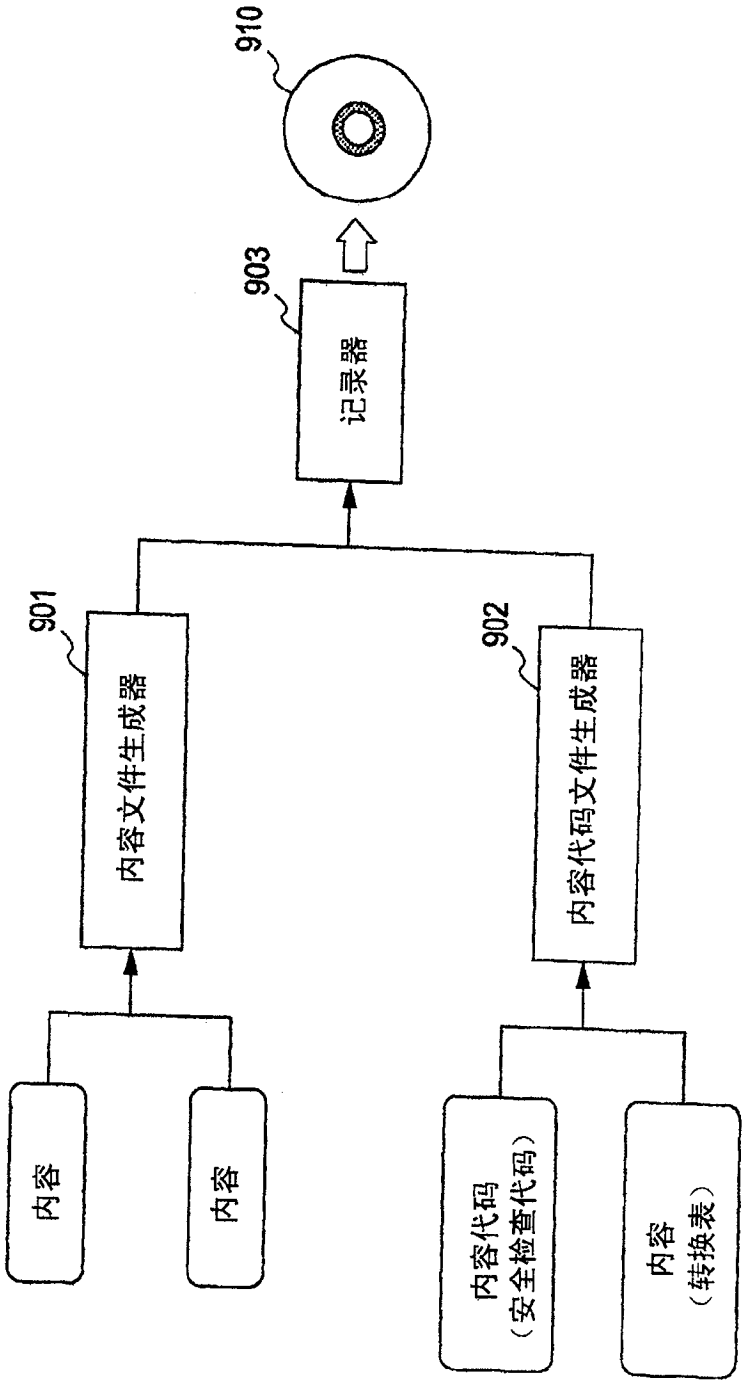

910
903
记录器
901
内容文件生成器
902
内容代码文件生成器
内容
内容
内容代码
（安全检查代码）
内容
（转换表）

图 16