[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 21/00 (2006.01)
G11B 20/00 (2006.01)
G11B 27/10 (2006.01)

[12] 发明专利申请公开说明书

[21] 申请号 200610072695.X

[43] 公开日 2006 年 10 月 18 日

[11] 公开号 CN 1848128A

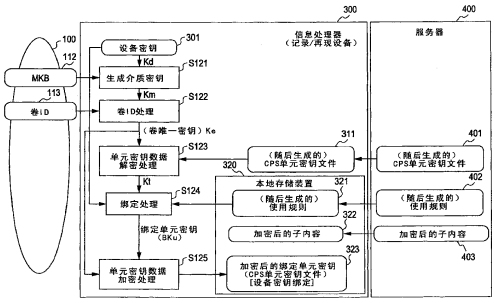
[22] 申请日 2006.4.11
[21] 申请号 200610072695.X
[30] 优先权
[32] 2005.4.11 [33] JP [31] 2005-113035
[71] 申请人 索尼株式会社
地址 日本东京都
[72] 发明人 上田健二朗 大石丈於 村松克美 高岛芳和
[74] 专利代理机构 北京东方亿思知识产权代理有限责任公司
代理人 孙明岩
权利要求书 5 页 说明书 49 页 附图 21 页

[54] 发明名称

信息处理器、信息处理方法和计算机程序

[57] 摘要

本发明提供了一种信息处理器，该信息处理器包括：数据处理部分，其执行将随后生成的数据存储到存储单元上的处理，随后生成的数据是随后利用从信息记录介质读取的信息生成或获取的。 数据处理部分被配置为：执行将加密后的随后生成的数据存储到存储单元上的处理，加密后的随后生成的数据作为用单元密钥加密的加密后的数据，单元密钥作为与随后生成的数据所属的内容管理单元相对应的加密密钥；以及执行获取加密后的绑定单元密钥并将加密后的绑定单元密钥存储到存储单元上的处理，加密后的绑定单元密钥是绑定单元密钥的加密后的数据，绑定单元密钥包括单元密钥以及从信息处理器获取的密钥信息和从信息记录介质获取的标识信息之一作为其构成数据。



1. 一种信息处理器，包括：

数据处理部分，其执行将随后生成的数据存储到存储装置上的处理，所述随后生成的数据是随后利用从信息记录介质读取的信息生成或获取的，

其中所述数据处理部分被配置为：执行将加密后的随后生成的数据存储到所述存储装置上的处理，所述加密后的随后生成的数据作为用单元密钥加密的加密后数据，所述单元密钥作为与所述随后生成的数据所属的内容管理单元相对应的加密密钥；以及执行获取加密后的绑定单元密钥并将所述加密后的绑定单元密钥存储到所述存储装置上的处理，所述加密后的绑定单元密钥是绑定单元密钥的加密后数据，所述绑定单元密钥包括所述单元密钥以及从所述信息处理器获取的密钥信息和从所述信息记录介质获取的标识信息之一作为其构成数据。

2. 根据权利要求 1 所述的信息处理器，其中所述数据处理部分被配置为执行获取加密后的绑定单元密钥并将所述加密后的绑定单元密钥存储到所述存储装置上的处理，所述加密后的绑定单元密钥在所述绑定单元密钥中包括与所述随后生成的数据所属的内容管理单元相对应的使用规则。

3. 根据权利要求 2 所述的信息处理器，其中：

所述信息记录介质是光盘；并且

所述与所述随后生成的数据所属的内容管理单元相对应的使用规则包括指示以下之一的绑定类型信息：

所述加密后的绑定单元密钥是否是在与所述信息处理器相关联的同时被加密的；

所述加密后的绑定单元密钥是否是在与所述信息记录介质相关联的同时被加密成与记录在所述光盘上的内容相对应的 ID 和为制造所述光盘时使用的每个压模设置的 ID 信息之一的；以及

所述加密后的绑定单元密钥是否是在与赋予所述光盘的序列号相关联的同时被加密的。

4. 根据权利要求 1 所述的信息处理器，其中所述数据处理部分被配置为生成对所述信息处理器唯一的并且被存储在所述信息处理器中的设备密钥，以及作为包括所述单元密钥作为其构成数据的绑定单元密钥的加密后数据的加密后的绑定单元密钥。

5. 根据权利要求 1 所述的信息处理器，其中所述数据处理部分被配置为生成对所述信息记录介质唯一的并且被存储在所述信息记录介质上的标识信息，以及作为包括所述单元密钥作为其构成数据的绑定单元密钥的加密后数据的加密后的绑定单元密钥。

6. 根据权利要求 1 所述的信息处理器，其中所述数据处理部分被配置为生成存储在所述信息记录介质上并且对预定数目的信息记录介质的集合唯一的标识信息，以及作为包括所述单元密钥作为其构成数据的绑定单元密钥的加密后数据的加密后的绑定单元密钥。

7. 根据权利要求 1 所述的信息处理器，其中所述数据处理部分被配置为通过基于所述单元密钥以及从所述信息处理器获取的密钥信息和从所述信息记录介质获取的标识信息之一的计算处理来生成绑定单元密钥。

8. 根据权利要求 1 所述的信息处理器，其中所述信息处理器被配置为将从随后生成数据提供服务器获取的随后生成的数据存储到所述存储装置上，并且通过对与从所述随后生成数据提供服务器和不同于所述随后生成数据提供服务器的服务器之一获取的随后生成的数据相对应的加密后的单元密钥进行解密来获取所述加密后的绑定单元密钥。

9. 一种信息处理器，包括：

数据处理部分，其执行加密后的内容的解密处理，

其中：

所述数据处理部分被配置为执行以下处理：从存储装置获取加密后的绑定单元密钥，所述加密后的绑定单元密钥是包括用于对所述加密后的内容进行加密的单元密钥的加密后数据；对所获取的加密后的绑定单元密钥进行解密；以及通过解除绑定处理来计算所述单元密钥；并且

针对所述加密后的绑定单元密钥的所述解除绑定处理被执行为这样的数据处理：从所述信息处理器获取的密钥信息和从信息记录介质获取的标

识信息之一被应用到该数据处理。

10. 根据权利要求 9 所述的信息处理器，其中：

所述绑定单元密钥包括与所述随后生成的数据所属的内容管理单元相对应的使用规则作为其构成数据；并且

所述数据处理部分被配置为执行以下数据处理作为所述解除绑定处理：从所述信息处理器获取的密钥信息和从信息记录介质获取的标识信息之一以及所述使用规则被应用到该数据处理。

11. 根据权利要求 10 所述的信息处理器，其中：

所述信息记录介质是光盘；

所述使用规则包括指示以下之一的绑定类型信息：

所述加密后的绑定单元密钥是否是在与所述信息处理器相关联的同时被加密的；

所述加密后的绑定单元密钥是否是在与和记录在所述光盘上的内容相对应的 ID 和为制造所述光盘时使用的每个压模设置的 ID 信息之一相关联的同时被加密的；以及

所述加密后的绑定单元密钥是否是在与赋予所述光盘的序列号相关联的同时被加密的。

12. 根据权利要求 11 所述的信息处理器，其中所述数据处理部分被配置为从所述使用规则获取所述绑定类型信息，并且根据所获取的绑定类型信息来确定要应用到所述解除绑定处理的执行的数据。

13. 一种信息处理方法，包括：

数据处理步骤，该步骤执行将随后生成的数据存储到存储装置上的处理，所述随后生成的数据是随后利用从信息记录介质读取的信息生成或获取的，

其中所述数据处理步骤包括：

将加密后的随后生成的数据存储到所述存储装置上的步骤，所述加密后的随后生成的数据作为用单元密钥加密的加密后数据，所述单元密钥作为与所述随后生成的数据所属的内容管理单元相对应的加密密钥；

加密后绑定单元密钥获取步骤，该步骤获取加密后的绑定单元密钥，

所述加密后的绑定单元密钥是绑定单元密钥的加密后数据，所述绑定单元密钥包括所述单元密钥以及从信息处理器获取的密钥信息和从所述信息记录介质获取的标识信息之一作为其构成数据；以及

执行将所述加密后的绑定单元密钥存储到所述存储装置上的处理的步骤。

14. 一种信息处理方法，包括：

数据处理步骤，该步骤执行加密后的内容的解密处理，其中：

所述数据处理步骤包括：

从存储装置获取加密后的绑定单元密钥的步骤，所述加密后的绑定单元密钥是包括用于对所述加密后的内容进行加密的单元密钥的加密后数据；

解密步骤，该步骤执行所获取的加密后的绑定单元密钥的解密处理；以及

解除绑定处理步骤，该步骤通过解除绑定处理计算所述单元密钥；并且

所述解除绑定处理步骤被执行为这样的数据处理：从信息处理器获取的密钥信息和从信息记录介质获取的标识信息之一被应用到该数据处理。

15. 一种用于在计算机上执行信息处理的计算机程序，包括：

数据处理步骤，该步骤执行将随后生成的数据存储到存储装置上的处理，所述随后生成的数据是随后利用从信息记录介质读取的信息生成或获取的，

其中所述数据处理步骤包括：

将加密后的随后生成的数据存储到所述存储装置上的步骤，所述加密后的随后生成的数据作为用单元密钥加密的加密后数据，所述单元密钥作为与所述随后生成的数据所属的内容管理单元相对应的加密密钥；

加密后绑定单元密钥获取步骤，该步骤获取加密后的绑定单元密钥，所述加密后的绑定单元密钥是绑定单元密钥的加密后数据，所述绑定单元密钥包括所述单元密钥以及从信息处理器获取的密钥信息和从所述信息记录介质获取的标识信息之一作为其构成数据；以及

执行将所述加密后的绑定单元密钥存储到所述存储装置上的处理的步骤。

16. 一种用于在计算机上执行信息处理的计算机程序，包括：

数据处理步骤，该步骤执行加密后的内容的解密处理，其中：

所述数据处理步骤包括：

从存储装置获取加密后的绑定单元密钥的步骤，所述加密后的绑定单元密钥是包括用于对所述加密后的内容进行加密的单元密钥的加密后数据；

解密步骤，该步骤执行所获取的加密后的绑定单元密钥的解密处理；以及

解除绑定处理步骤，该步骤通过解除绑定处理计算所述单元密钥；并且

所述解除绑定处理步骤被执行为这样的数据处理：从信息处理器获取的密钥信息和从信息记录介质获取的标识信息之一被应用到该数据处理。

信息处理器、信息处理方法和计算机程序

技术领域

本发明涉及信息处理器、信息处理方法和计算机程序。更具体而言，本发明涉及针对存储在信息记录介质上的内容在每单元基础上实现使用控制以及针对随后生成的数据（诸如由用户随后下载或生成的数据）实现严格的使用控制的信息处理器、信息处理方法和计算机程序。

背景技术

各种软件数据，包括音频数据（例如音乐）、图像数据（例如电影）、游戏程序、各种应用程序等等（在下文中这些都被称为“内容”），可以作为数字数据被存储到记录介质上，例如利用蓝色激光的 Blu-ray Disc（商标）、DVD（数字多功能盘）、MD（微型盘）或 CD（高密度盘）。具体而言，利用蓝色激光的 Blu-ray Disc（商标）是能够进行高密度记录的盘，其可以以高图像质量数据的形式存储大量视频内容。

数字内容被存储在将要提供给用户的各种这样的信息记录介质（记录介质）上。用户利用用户所拥有的诸如 PC（个人计算机）或盘播放器之类的再现设备来再现或使用内容。

对于诸如音乐数据、图像数据之类的许多种类的内容，内容的发行权等一般为内容的创建者或销售者所有。因此，这些种类的内容的发行一般受到某些使用限制，即，通过只许可经授权的用户使用内容，防止了未经授权的复制等等。

数字记录器或记录介质实现了重复记录和再现，而不会导致例如图像或声音质量的劣化。这导致了以下问题的蔓延：未经授权的复制内容在因特网上的传递、通过将内容复制到 CD-R 等之上而产生的所谓的盗版盘的流通以及对存储在 PC 等的硬盘上的复制内容的使用。

DVD 或诸如利用蓝色激光的记录介质这样的海量存储记录介质的开发

在近年来已经取得了进步，其允许等同于例如十部到数十部电影的大量数据以数字信息的形式被记录在单个介质上。由于可以以这种方式将视频信息等记录为数字信息，因此防止未经授权的复制以保护著作权所有者的权利变得越发重要。目前，为了防止数字数据的这种未经授权的复制，已经针对数字记录器和记录介质实现了各种用于防止非法复制的技术。

例如，对 DVD 播放器采用了内容加扰系统（Content Scramble System）。根据内容加扰系统，视频数据、音频数据等以加密后的形式被存储在 DVD-ROM（只读存储器）上。用于对加密后的数据进行解密的密钥被提供给有许可证的 DVD 播放器。许可证被提供给被设计为遵守预定操作要求的 DVD 播放器，所述要求例如是不执行未经授权的复制。因此，在有许可证的 DVD 播放器上，可以通过利用给定的密钥对记录在 DVD-ROM 上的加密后的数据进行解密来从 DVD-ROM 再现图像或声音。

另一方面，没有获得许可证的 DVD 播放器不能对记录在 DVD-ROM 上的加密后的数据进行解密，因为它没有对加密后的数据进行解密所必需的密钥。这样一来，利用内容加扰系统，就不能利用不满足颁发许可证时所要求的条件的 DVD 播放器执行记录数字数据的 DVD-ROM 上的数据的再现，从而防止了未经授权的复制。

发明内容

用于存储在信息记录介质上的内容的管理系统的构造方式如上。此外，例如，在日本专利申请公布 No. 2003-140662 中公开了一种使得用户能够很容易地下载诸如声音效果、运动和静止图片之类的内容作为视频作品的素材的系统。此外，在日本专利申请公布 No. 2002-311967 中，公开了一种使得与整个音乐数据的一部分相对应的数据能够被另一数据替换的技术。但是，很难说为随后生成的数据实现了安全的数据管理或使用管理，所述随后生成的数据例如是由执行程序的用户生成的作为存储在信息记录介质上的内容的数据，或者是从外部服务器获取的数据或内容。

具体而言，在可以执行各种应用程序的环境中，例如 PC 环境中，在许多情况下，通用文件系统要管理的目录被设置，这意味着随后生成的数

据，即用户随后生成或获取的数据，可以被各种应用所访问。因此，即使要被内容管理系统管理的随后生成的数据也需要被设置在这种通用文件系统管理的目录中。因此，除非进行特殊设置，否则就会从各种应用程序进行访问，这不利地允许了对数据进行未经授权的使用或改变。

此外，存在各种随后生成的数据，包括与存储在特定信息记录介质上的内容相对应地使用的随后生成的数据、可以与作为提供内容的内容提供实体的特定工作室所提供的内容相对应地共同使用的随后生成的数据以及可以与不同工作室提供的内容相对应地共同使用的随后生成的数据。需要根据这些各个种类的随后生成的数据执行使用控制。但是，利用传统系统，难以根据随后生成的数据的种类执行这种使用控制。

因此，需要提供一种信息处理器、一种信息处理方法和一种计算机程序，其针对随后生成的数据，例如从外部获取的数据或由用户生成的与存储在信息记录介质上的内容相对应的数据，实现与对存储在信息记录介质上的内容执行的使用控制相同的使用控制，并且还使得能够根据各种随后生成的数据来执行使用控制。

根据本发明的第一方面，提供了一种信息处理器，其包括：数据处理部分，其执行将随后生成的数据存储到存储装置上的处理，随后生成的数据是随后利用从信息记录介质读取的信息生成或获取的，其中数据处理部分被配置为：执行将加密后的随后生成的数据存储到存储装置上的处理，加密后的随后生成的数据作为用单元密钥加密的加密后数据，单元密钥作为与随后生成的数据所属的内容管理单元相对应的加密密钥；以及执行获取加密后的绑定单元密钥并将加密后的绑定单元密钥存储到存储装置上的处理，加密后的绑定单元密钥是绑定单元密钥的加密后数据，绑定单元密钥包括单元密钥以及从信息处理器获取的密钥信息和从信息记录介质获取的标识信息之一作为其构成数据。

此外，在根据本发明实施例的信息处理器中，数据处理部分被配置为执行获取加密后的绑定单元密钥并将加密后的绑定单元密钥存储到存储装置上的处理，加密后的绑定单元密钥在绑定单元密钥中包括与随后生成的数据所属的内容管理单元相对应的使用规则。

此外，在根据本发明实施例的信息处理器中，数据处理部分被配置为生成对信息处理器唯一的并且被存储在信息处理器中的设备密钥，以及作为包括单元密钥作为其构成数据的绑定单元密钥的加密后数据的加密后的绑定单元密钥。

此外，在根据本发明实施例的信息处理器中，数据处理部分被配置为生成对信息记录介质唯一的并且被存储在信息记录介质上的标识信息，以及作为包括单元密钥作为其构成数据的绑定单元密钥的加密后数据的加密后的绑定单元密钥。

此外，在根据本发明实施例的信息处理器中，数据处理部分被配置为生成存储在信息记录介质上并且对预定数目的信息记录介质的集合唯一的标识信息，以及作为包括单元密钥作为其构成数据的绑定单元密钥的加密后数据的加密后的绑定单元密钥。

此外，在根据本发明实施例的信息处理器中，数据处理部分被配置为通过基于单元密钥以及从信息处理器获取的密钥信息和从信息记录介质获取的标识信息之一的计算处理来生成绑定单元密钥。

此外，在根据本发明实施例的信息处理器中，计算处理是异或运算。

此外，在根据本发明实施例的信息处理器中，信息处理器被配置为将从随后生成数据提供服务器获取的随后生成的数据存储到存储装置上，并且通过对与从随后生成数据提供服务器和不同于随后生成数据提供服务器的服务器之一获取的随后生成的数据相对应的加密后的单元密钥进行解密来获取加密后的绑定单元密钥。

此外，根据本发明的第二方面，提供了一种信息处理器，其包括：数据处理部分，其执行加密后的内容的解密处理，其中：数据处理部分被配置为执行以下处理：从存储装置获取加密后的绑定单元密钥，加密后的绑定单元密钥是包括用于对加密后的内容进行加密的单元密钥的加密后的数据；对所获取的加密后的绑定单元密钥进行解密；以及通过解除绑定处理计算单元密钥；并且针对加密后的绑定单元密钥的解除绑定处理被执行为这样的数据处理：从信息处理器获取的密钥信息和从信息记录介质获取的标识信息之一被应用到该数据处理。

此外，在根据本发明实施例的信息处理器中，绑定单元密钥包括与随后生成的数据所属的内容管理单元相对应的使用规则作为其构成数据；并且数据处理部分被配置为执行以下数据处理作为解除绑定处理：从信息处理器获取的密钥信息和从信息记录介质获取的标识信息之一以及使用规则被应用到该数据处理。

此外，在根据本发明实施例的信息处理器中，数据处理部分被配置为从与随后生成的数据相对应的使用规则或从另一数据文件获取随后生成的数据的绑定类型，并且根据所获取的信息来确定要应用到解除绑定处理的执行的数据。

此外，根据本发明的第三方面，提供了一种信息处理方法，其包括：数据处理步骤，该步骤执行将随后生成的数据存储到存储装置上的处理，随后生成的数据是随后利用从信息记录介质读取的信息生成或获取的，其中数据处理步骤包括：将加密后的随后生成的数据存储到存储装置上的步骤，加密后的随后生成的数据作为用单元密钥加密的加密后数据，单元密钥作为与随后生成的数据所属的内容管理单元相对应的加密密钥；加密后绑定单元密钥获取步骤，该步骤获取加密后的绑定单元密钥，加密后的绑定单元密钥是绑定单元密钥的加密后数据，绑定单元密钥包括单元密钥以及从信息处理器获取的密钥信息和从信息记录介质获取的标识信息之一作为其构成数据；以及执行将加密后的绑定单元密钥存储到存储装置上的处理的步骤。

此外，根据本发明的第四方面，提供了一种信息处理方法，其包括：数据处理步骤，该步骤执行加密后的内容的解密处理，其中数据处理步骤包括：从存储装置获取加密后的绑定单元密钥的步骤，加密后的绑定单元密钥是包括用于对加密后的内容进行加密的单元密钥的加密后数据；解密步骤，该步骤执行所获取的加密后的绑定单元密钥的解密处理；以及解除绑定处理步骤，该步骤通过解除绑定处理计算单元密钥；并且其中解除绑定处理步骤被执行为这样的数据处理：从信息处理器获取的密钥信息和从信息记录介质获取的标识信息之一被应用到该数据处理。

此外，根据本发明的第五方面，提供了一种用于在计算机上执行信息

处理的计算机程序，其包括：数据处理步骤，该步骤执行将随后生成的数据存储到存储装置上的处理，随后生成的数据是随后利用从信息记录介质读取的信息生成或获取的，其中数据处理步骤包括：将加密后的随后生成的数据存储到存储装置上的步骤，加密后的随后生成的数据作为用单元密钥加密的加密后数据，单元密钥作为与随后生成的数据所属的内容管理单元相对应的加密密钥；加密后绑定单元密钥获取步骤，该步骤获取加密后的绑定单元密钥，加密后的绑定单元密钥是绑定单元密钥的加密后数据，绑定单元密钥包括单元密钥以及从信息处理器获取的密钥信息和从信息记录介质获取的标识信息之一作为其构成数据；以及执行将加密后的绑定单元密钥存储到存储装置上的处理的步骤。

此外，根据本发明的第六方面，提供了一种用于在计算机上执行信息处理的计算机程序，其包括：数据处理步骤，该步骤执行加密后的内容的解密处理，其中数据处理步骤包括：从存储装置获取加密后的绑定单元密钥的步骤，加密后的绑定单元密钥是包括用于对加密后的内容进行加密的单元密钥的加密后数据；解密步骤，该步骤执行所获取的加密后的绑定单元密钥的解密处理；以及解除绑定处理步骤，该步骤通过解除绑定处理计算单元密钥；并且其中解除绑定处理步骤被执行为这样的数据处理：从信息处理器获取的密钥信息和从信息记录介质获取的标识信息之一被应用到该数据处理。

注意，根据本发明实施例的计算机程序例如是可以被提供给能够利用以计算机可读格式提供的记录介质（包括诸如 DVD、CD、MO 之类的记录介质）或者利用通信介质（例如网络）来执行各种程序代码的计算机系统的计算机程序。通过以计算机可读的格式提供这种程序，在计算机上实现了根据程序的处理。

本发明的以上和其他目的、特征和优点将从以下基于本发明实施例的详细描述和附图中变得清楚，本发明的实施例将在稍后描述。注意，本说明书中使用的术语“系统”是指多个设备的逻辑集合结构，并且每个结构的设备不必存在于同一外壳内。

根据本发明的实施例，当将随后生成的数据（例如用户随后利用存储

在信息记录介质上的信息而生成的信息或下载的信息）记录到诸如硬盘或可移除介质之类的本地存储装置上时，作为随后生成的数据的加密密钥的单元密钥作为绑定到从信息处理器获取的密钥信息或从信息记录介质获取的标识信息的数据而被生成，并且以加密后的形式被记录。从而，要使用记录在本地存储装置上的随后生成的数据，则需要解除绑定处理。解除绑定处理要求以下条件。即，例如在设备绑定型随后生成数据的情况下，要求要使用随后生成的数据的信息处理器是与执行记录的信息处理器相同的信息处理器；例如在盘绑定型随后生成数据的情况下，要求与记录随后生成的数据时使用的相同的盘被加载到信息处理器中；例如在封装绑定型随后生成数据的情况下，要求信息处理器被加载以与记录随后生成的数据时使用的盘具有相同封装 ID 的盘。因此，可以以各种方式实现随后生成的数据的使用限制。

附图说明

图 1 是示出存储在信息记录介质上的数据以及信息处理器的配置和处理的图；

图 2 是示出针对存储在信息记录介质上的内容而设置的内容管理单元的设置示例的图；

图 3 是示出针对存储在信息记录介质上的内容而设置的内容管理单元和单元密钥之间的对应关系的图；

图 4 是示出存储在信息记录介质上的加密后的内容（CPS 单元）和 CPS 单元密钥的加密配置的图。

图 5A 至 5Bc 是示出随后生成的数据的绑定类型和作为绑定类型记录的数据示例的图。

图 6 是示出用于获取设备绑定型随后生成数据的处理序列的图；

图 7 是示出信息处理器在将设备绑定型随后生成数据记录到本地存储装置上时所执行的处理序列的图；

图 8 是示出 AES 加密算法的图；

图 9 是示出用于再现存储在信息记录介质上的内容的处理序列的图；

图 10 是示出用于再现设备绑定型随后生成数据的处理序列的图；

图 11 是示出用于获取盘绑定型随后生成数据的处理序列的图；

图 12 是示出信息处理器在将盘绑定型随后生成数据记录到本地存储装置上时所执行的处理序列的图；

图 13 是示出用于再现盘绑定型随后生成数据的处理序列的图；

图 14 是示出用于获取封装绑定型随后生成数据的处理序列的图；

图 15 是示出信息处理器在将封装绑定型随后生成数据记录到本地存储装置上时所执行的处理序列的图；

图 16 是示出用于再现封装绑定型随后生成数据的处理序列的图；

图 17 是示出用于获取可向其应用存储在信息记录介质上的 CPS 单元密钥的随后生成的数据的处理序列的图；

图 18 是示出用于再现可向其应用存储在信息记录介质上的 CPS 单元密钥的随后生成的数据的处理序列的图；

图 19 是示出用于获取和记录随后生成的数据的处理序列的流程图；

图 20 是示出用于再现随后生成的数据的处理序列的流程图；以及

图 21 是示出信息记录介质被加载到其中以便执行再现或记录处理的信息处理器的配置示例的图。

具体实施方式

以下，将参考附图详细描述根据本发明实施例的信息处理器、信息处理方法和计算机程序。注意，将针对以下项目进行描述。

1. 存储在信息记录介质上的数据和信息处理器的概况

2. 关于内容管理单元（CPS 单元）

3. 用于获取、记录和使用随后生成的数据的处理的细节

（3.1）用于获取、记录和使用设备绑定随后生成数据的处理的细节

（3.2）用于获取、记录和使用盘绑定随后生成数据的处理的细节

（3.3）用于获取、记录和使用封装绑定随后生成数据的处理的细节

（3.4）当与随后生成的数据相对应的 CPS 单元密钥已经被存储在信息记录介质上时用于获取、记录和使用随后生成的数据的处理的细节

（3.5）用于获取、记录和使用随后生成的数据的处理序列

4. 信息处理器的配置示例

[1. 存储在信息记录介质上的数据和信息处理器的概况]

首先，将描述存储在信息记录介质上的数据和信息处理器的概况。图1示出其上存储了内容的信息记录介质100和信息处理器（再现设备）150的配置。在该示例中，信息被存储在ROM盘上，该ROM盘充当其上已经存储了内容的盘。各种类型的信息信息处理器，例如PC或只读设备，被用作信息处理器150。信息处理器150具有驱动器120，用于执行从信息记录介质100读取数据的处理。

作为信息记录介质100的ROM盘例如是诸如Blu-ray Disc（商标）或DVD之类的信息记录介质，其上存储了经授权的内容，并且其是在拥有内容的合法著作权或发行权的所谓的内容所有者的许可之下在盘制造工厂中制造的。注意，虽然在以下对实施例的描述中盘形介质被用作信息记录介质的示例，但是，本发明也可应用于使用各种类型的信息记录介质的配置。

如图1所示，信息记录介质100存储：已经历加密处理的加密后的内容111；作为加密密钥块的MKB（介质密钥块）112，所述加密密钥块是在被认为是一种类型的广播加密系统的树结构密钥分发系统基础上生成的；卷ID 113，其在每制造单元基础上被设置为每预定数目的信息记录介质的标识信息；封装ID 114，其被设置为每个单元的标识信息，例如内容标题、内容所有者或者工作室；包括CCI（复制控制信息）的使用规则115，其作为内容复制/再现控制信息；CPS单元密钥文件116，其存储CPS单元密钥，该CPS单元密钥作为针对每个作为内容使用管理单元的内容管理单元（CPS单元）设置的加密密钥；序列号117，其被设置为每个信息记录介质100的单独号码；以及下载信息118，例如获取随后生成的数据的服务器的地址。以下将会描述这些不同种类的信息的概要。

（1）加密后的内容111

各种内容被存储在信息记录介质100上。例如，这些内容包括具有特定标准所指定的格式的运动图片内容（例如作为高清晰度运动图片数据的

HD（高清晰度）电影内容）的 AV（视听）流，或者游戏程序、图像文件、声音数据或者文本数据。这些内容是特定 AV 格式标准数据，并且根据特定 AV 数据格式被存储。更具体而言，例如，根据 Blu-ray Disc（商标）ROM 标准格式，这些内容被存储为 Blu-ray Disc（商标）ROM 标准数据。

此外，例如，在某些情况下可以存储作为服务数据的游戏程序、图像文件、声音数据、文本数据等等。这些内容在某些情况下可以被存储为其数据格式不遵循特定 AV 数据格式的数据。

对于内容的种类，存在各种内容，例如音乐数据、运动图片的图像数据、静止图片等、游戏程序和 WEB 内容。这些内容可以包括各种类型的信息，例如只能与来自信息记录介质 100 的数据一起使用的内容信息以及可以与从经由网络连接的服务器提供的数据以及来自信息记录介质 100 的数据一起使用的内容信息。为了对分段的内容实现不同的使用控制，存储在信息记录介质上的内容是以加密的形式被存储的，并且不同的密钥（CPS 单元密钥或单元密钥（或者它们常被称作的标题密钥））被分配给每个分段内容。被分配一个单元密钥的单元被称为内容管理单元（CPS 单元）。

（2）MKB

MKB（介质密钥块）112 是在被认为是一种类型的广播加密系统的树结构密钥分发系统的基础上生成的加密密钥。MKB 112 是只允许通过基于存储在具有有效许可证的用户的信息处理器中的设备密钥[Kd]的处理（解密）获取介质密钥[Km]的密钥信息块，所述介质密钥是内容解密所必需的密钥。MKB 112 代表遵循所谓的分级树结构的信息分发系统的应用；仅当用户设备（信息处理器）拥有有效许可证时，才允许介质密钥[Km]的获取，并且介质密钥[Km]不能被已被撤销的用户设备所获取。

作为许可证实体的管理中心可生成这样配置的 MKB：这种配置使得通过用于存储在 MKB 中的密钥信息的加密的设备密钥的变化，MKB 不能被存储在特定用户设备中的设备密钥所解密，即，内容解密所必需的介质密钥不能被获取。因此，可以通过在任意定时撤销未经授权的设备来提供

仅能够针对具有有效许可证的设备被解密的加密后内容。稍后将描述内容解密处理。

（3）卷 ID（封装 ID）

卷 ID 例如是在每压模（stamper）的基础上设置的，并且是被设置为用于所制造的每预定数目的信息记录介质的标识信息的 ID。卷 ID 被用作用于生成用来对内容解密的密钥的信息。此外，即使卷 ID 具有相同的标题，在创建两个或更多个（压模或母盘）的情况下，对于每个压模或母盘可以设置不同的卷 ID。稍后将描述这些处理。

（4）封装 ID

封装 ID 例如是针对记录具有相同标题的内容的信息介质共同设置的 ID，或者是针对存储由同一个作为内容创建公司的工作室所提供的内容的信息介质共同设置的 ID。封装 ID 被设置为诸如内容标题、内容所有者或工作室之类的每个单元的信息记录介质的标识信息。即，与卷 ID 不同，当标题相同时，封装 ID 变成同一个 ID。

（5）使用规则

使用规则例如包括复制控制信息（CCI），该复制控制信息包括复制限制信息或再现限制信息，用于与存储在信息记录介质 100 上的加密后的内容 111 相对应的使用控制。复制控制信息（CCI）允许各种设置，包括它被设置成每一个被设置为内容管理单元的 CPS 单元的信息的情况，或者它被设置成与多个 CPS 单元相对应的情况。稍后将描述该信息的细节。注意，存储在信息记录介质 100 上的使用规则是作为加密后的数据被存储的。稍后将描述特定加密结构。

（6）CPS 单元密钥文件

如上所述，存储在信息记录介质 100 上的加密后的内容 111 是以每一个被设置为内容管理单元的 CPS 单元的加密密钥来加密的。诸如 AV（视听）流、音乐数据、图像数据（例如运动图片或静止图片）、游戏程序、WEB 内容之类的构成内容并且被 MPEG-2、MPEG4-AVC、VC1 等编码的图像数据被分段成作为内容使用的管理单元的 CPS 单元。要求要执行再现处理的信息处理器确定要再现的内容所属的 CPS 单元，并且利用 CPS 单

元密钥作为与这样确定出的 CPS 单元相对应的加密密钥来执行解密处理。存储获取该 CPS 单元密钥所必需的数据的文件是 CPS 单元密钥文件。稍后将描述 CPS 单元密钥文件的细节。注意，对于内容的再现，不仅需要使用 CPS 单元密钥，而且还需要使用各种其他密钥信息、密钥生成信息等等。这种情况下的特定处理也将在稍后描述。

（7）序列号

序列号是被设置为每个信息记录介质 100 的个体号码的号码。

（8）下载信息

当存在随后可以获取的与存储在信息记录介质 100 上的数据相对应的数据时，下载信息例如包括加密后的内容 111、获取随后生成的数据所必需的信息。更具体而言，下载信息包括用于获取随后生成的数据的服务器的地址，以及用于确定要下载服务器中的哪些内容的信息，例如用于标识内容所有者的信息（工作室 ID）或者用于标识由内容所有者提供的盘（或内容）的信息（封装 ID）。注意，当加密后的内容 111 例如是外语电影时，随后生成的数据是指电影的各种数据，例如字幕数据、解说词数据或额外奖励数据。

图 1 所示的服务器 130 是提供随后生成的数据的服务器。服务器 130 根据预定的序列执行与信息处理器 150 的通信处理，并且向信息处理器 150 发送作为随后生成的数据 131 的加密后的子内容、关于随后生成的数据 131 的使用规则 132，以及作为被应用到随后生成的数据 131 的加密密钥信息的 CPS 单元密钥文件。信息处理器 150 将这些数据存储和保存在例如本地存储装置 155 上，该本地存储装置 155 例如是硬盘。注意，稍后将描述随后生成数据获取处理序列的细节。

图 1 示出执行存储在信息记录介质 100 上的内容的再现处理的信息处理器 150 的示意性配置。信息处理器 150 具有驱动器 120，用于执行读取存储在信息记录介质 100 上的数据的处理。被驱动器 120 所读取的数据被输入到用于执行加密后内容的解密处理和解码（例如 MPEG 解码）处理的再现处理执行 LSI 151。

再现处理执行 LSI 151 具有用于执行加密后内容的解密处理的解密处

理单元 152 以及用于执行解码（例如 MPEG 解码）处理的解码处理单元 153。解密处理单元 152 通过利用存储在存储器 154 中的各种信息以及从信息记录介质 100 读取的数据生成用于对内容解密的密钥，然后执行加密后的内容 111 的解密处理。

此外，再现处理执行 LSI 151 还执行存储在本地存储装置 155 上的随后生成的数据的解密处理。例如，再现处理执行 LSI 151 从信息记录介质 100 读取电影内容，并且对电影内容解密，同时，对来自本地存储装置 155 的作为加密后的随后生成的数据的字幕数据执行解密，并且执行同时再现这些数据的处理。

设备密钥:Kd 被存储在信息处理器 150 的存储器 154 中。设备密钥:Kd 是应用到上述 MKB 处理的密钥。MKB 112 是只允许通过基于存储在具有有效许可证的用户的信息处理设备中的设备密钥[Kd]的处理（解密）来获取介质密钥[Km]的密钥信息块，所述介质密钥[Km]是内容解密所必需的。对于加密后的内容的解密，信息处理器 150 通过利用存储在存储器 154 中的设备密钥:Kd 来执行 MKB 112 的处理。注意，内容解密处理的细节将在稍后描述。

[2. 关于内容管理单元（CPS 单元）]

如上所述，为了对每个单元实现不同的使用控制，在每个单元被分配不同的密钥的同时，将要存储在信息记录介质上的内容经历加密处理。即，内容被分段成用于个体加密处理的内容管理单元（CPS 单元），以允许个体使用控制。

为了使用内容，首先，必须获取分配给各个单元的 CPS 单元密钥，此外，通过利用其他必要的密钥、密钥生成信息等等，执行基于规定的解密序列的数据处理以执行再现。将参考图 2 描述如何设置内容管理单元（CPS 单元）。

如图 2 所示，内容具有分层结构，其中包括（A）索引 210、（B）电影对象 220、（c）播放列表以及（D）剪辑 240。例如，一旦指定要被再现应用访问的索引（例如标题），就指定与标题相关联的要再现的程序，并且根据指定的再现程序的程序信息选择限定内容再现顺序等的播放列

表。

播放列表包括作为要再现的数据信息的播放项目。利用作为由包括在播放列表中的播放项目限定的再现部分的剪辑信息，作为实际内容数据的 AV 流或命令被选择性地读取，以执行 AV 流的再现或命令的执行。注意，存在大量播放列表和播放项目，其中每一个与一个作为标识信息的播放列表 ID 或播放项目 ID 相关联。

图 2 示出两个 CPS 单元。这些 CPS 单元构成存储在信息记录介质上的内容的一部分。CPS 单元 1、271 和 CPS 单元 2、272 中的每一个的被设置为这样一个单元：该单元包括作为索引的标题、作为再现程序文件的电影对象、播放列表以及包括作为实际内容数据的 AV 流文件的剪辑。

内容管理单元（CPS）单元 1、271 包括标题 1、211 和标题 2、212、再现程序 221 和 222、播放列表 231 和 232 以及剪辑 241 和剪辑 242。至少包括在两个相应的剪辑 241、242 中的作为实际内容数据的 AV 流数据文件 261、262 是要被加密的数据，按照一般规则，这些数据分别被设置为以 CPS 单元密钥（Ku1）加密的数据，所述 CPS 单元密钥是与内容管理单元（CPS 单元）1、271 相关联设置的加密密钥。

内容管理单元（CPS 单元）2、272 包括作为索引的应用 1、213、要再现的程序 224、播放列表 233 和剪辑 243。包括在剪辑 243 中的作为实际内容数据的 AV 流数据文件 263 被用 CPS 单元密钥（Ku2）加密，所述 CPS 单元密钥是与内容管理单元（CPS 单元）2、272 相关联设置的加密密钥。

例如，为了使用户执行与内容管理单元 1、271 相对应的应用文件或内容的再现处理，必需获取作为与内容管理单元（CPS 单元）1、271 相关联设置的加密密钥的单元密钥:Ku1，然后执行解密处理。为了使用户执行与内容管理单元 2、272 相对应的应用文件或内容的再现处理，必需获取作为与内容管理单元（CPS 单元）2、272 相关联设置的加密密钥的单元密钥:Ku2，然后执行解密处理。

CPS 单元的设置配置和相应的单元密钥的示例在图 3 中示出。图 3 示出了作为存储在信息记录介质上的解密后的内容的使用管理单元的 CPS 单

元设置单元与应用到各自的 CPS 单元的 CPS 单元密钥之间的对应关系。注意，还可以预先为随后生成的数据存储和设置 CPS 单元。例如，数据部分 281 充当用于随后生成的数据的条目。

CPS 单元是在各种单元中设置的，所述各种单元例如是内容标题、应用、数据群组等等。在 CPS 单元管理表中，CPS 单元 ID 被设置为与各自的 CPS 单元相对应的标识符。

在图 3 中，标题 1 例如是 CPS 单元 1。对于属于 CPS 单元 1 的加密后的内容的解密，必须生成单元密钥 Ku1，并且基于生成的单元密钥 Ku1 执行解密处理。

如上所述，为了对每个单元实现不同的使用控制，在每个单元被分配不同的密钥的同时，要存储在信息记录介质上的内容经历加密处理。每个内容管理单元（CPS 单元）的使用规则（UR）被设置成为每个内容管理单元（CPS 单元）执行个体使用控制。如上所述，使用规则是例如包括关于内容的复制控制信息（CCI）的信息，所述复制控制信息例如是每个内容管理单元（CPS 单元）中包括的加密后的内容的复制限制信息和再现限制信息。

参考图 4，将描述包括存储在信息记录介质 100 上的内容的 CPS 单元的加密模式，以及被设置为用于解密各自 CPS 单元的 CPS 单元密钥的存储文件的 CPS 单元密钥文件的特定数据结构。如图 4 所示，每个 CPS 单元（CPS_Unit#n）是作为用相应单元密钥（Ku_n）加密的数据[Enc(Ku_n, CPS_Unit#n)]而被存储的。注意，Enc(A, B)指示用密钥（A）加密的数据（B）的加密后数据。

每个 CPS 单元密钥[Ku_n]作为加密后的数据被存储在每个 CPS 单元密钥文件中，所述 CPS 单元密钥文件被设置为用于对存储在信息记录介质 100 上的每个 CPS 单元解密的 CPS 单元密钥的存储文件。即，如图 4 所示，CPS 单元（CPS_Unit#n）的 CPS 单元密钥[Ku_n]被存储在信息记录介质 100 上，作为其中卷唯一密钥[Ke（嵌入密钥）]被应用到具有相应的使用规则（UR#n）的计算结果[f(Ku_n, UR#n)]的加密后数据，即作为[Enc(ke, f(Ku_n, UR#n))]。

注意，f(A, B)是指数据 A 和数据之间的计算。f(Ku_n, UR#n)例如代表诸如 CPS 单元（CPS_Unit#n）的单元密钥[Ku_n]和使用规则（UR#n）之间的异或运算的计算处理，并且被存储在信息记录介质 100 上，作为利用关于计算结果的卷唯一密钥[Ke]加密的数据。注意，卷唯一密钥[Ke（嵌入密钥）]是相应于信息记录介质 100 的卷 ID 设置的密钥。

如上所述，预先存储在信息记录介质 100 上的内容被分段成 CPS 单元，被存储为用与每个单元相对应的单元密钥加密的加密后数据，并且经历基于与每个 CPS 单元相对应的使用规则的使用控制。

基于 CPS 单元的使用管理也可以在除了预先存储在信息记录介质 100 上的内容之外的其他内容上执行，例如随后生成的数据，例如由用户随后生成的或在外部获取的数据。在下文中，将描述随后生成的数据的获取处理和使用控制处理。

[3. 随后生成的数据的获取和管理配置]

如图 1 所示，从服务器 130 获取的 SD 中，例如随后生成的数据（加密后的子内容）131（例如与电影内容相对应的字幕数据），也被设置为属于 CPS 单元的数据。注意，存在用于随后生成的数据的 CPS 单元被设置为新的 CPS 单元情况，以及先前为信息记录介质 100 设置的 CPS 单元被用作 CPS 单元的情况。

当随后生成的数据 131 属于先前为信息记录介质 100 设置的 CPS 单元时，存储在信息记录介质 100 上的与预设的 CPS 单元相对应的使用规则（UR）可以被用作随后生成的数据的使用规则（UR）。另一方面，当用于随后生成的数据的 CPS 单元被设置为新的 CPS 单元时，服务器 130 向用户的信息处理器 150 提供与随后生成的数据 131 相对应的使用规则（UR）132，以及存储与新的 CPS 单元相对应的单元密钥的 CPS 单元密钥文件 133。

注意，正如稍后将描述的，存在为随后生成的数据设置不同于预先存储在信息记录介质 100 上的内容的绑定类型的情况。在为其设置绑定类型的随后生成的数据的情况下，描述绑定类型的使用规则（UR）被提供给用户的信息处理器，作为随后生成的数据的使用规则（UR）。即使在随后生

成的数据 131 属于预先存储在信息记录介质 100 上的 CPS 单元的情况下，当要设置绑定类型时，描述与随后生成的数据的相对应的绑定类型的使用规则（UR）也会被提供给用户的信息处理器 150。

信息处理器 150 将随后生成的数据存储到图 5 所示的信息处理器 150 中的本地存储装置 155 上以供使用，所述本地存储装置 155 例如是硬盘。注意，所使用的本地存储装置 155 不限于是硬盘，而可以是闪存型卡存储器或者可移动介质，例如可写数据的 DVD。

对于存储在本地存储装置上的随后生成的数据的使用，与对应于存储在信息记录介质 100 上的 CPS 单元的内容类似，随后生成的数据的使用是根据由与随后生成的数据所属的 CPS 单元相对应的使用规则指定的使用限制来执行的。此外，需要获取相应于与随后生成的数据相对应的 CPS 单元而设置的 CPS 单元密钥，并且执行作为随后生成的数据的加密后的数据的解密。

和对应于预先存储在信息记录介质 100 上的 CPS 单元的内容一样，存储在本地存储装置 155 上的随后生成的数据也是在预定的使用控制管理下被使用的。因此，例如，防止了随后生成的数据被没有使用内容的权利的第三方复制到外部存储介质上以供未经授权的使用。

与预先存储在信息记录介质 100 上的内容不同，随后生成的数据经历对随后生成的数据来说唯一的使用限制模式。即，根据对随后生成的数据来说唯一的使用限制模式，随后生成的数据被分段成以下四种种类（绑定类型）。

（1）设备绑定型随后生成数据：仅许可已获取（下载）了随后生成的数据的设备（信息处理器）使用随后生成的数据。

（2）盘绑定型随后生成数据：仅在信息处理器中设置具有与获取（下载）随后生成数据时使用的信息记录介质（盘）的序列号相同的序列号的盘的情况下，才允许使用随后生成的数据。

（3）封装绑定型随后生成数据：仅在信息处理器中设置具有与获取（下载）随后生成数据时使用的信息记录介质（盘）的封装 ID 相同的封装 ID 的信息记录介质（盘）的情况下，才允许使用随后生成的数据。

（4）未绑定型随后生成数据：未对其规定特定使用限制的随后生成的数据。

（5）其他随后生成的数据：除了以上项目（1）至（4）中所描述的那些之外的随后生成的数据。其他随后生成的数据例如包括由作为独立提供内容的实体的工作室开发的方法为其设置使用限制的随后生成的数据。其中例如包括已经经历利用诸如 JAVA 应用之类的程序进行的加密的随后生成的数据。

当图 1 所示的信息处理器 150 从服务器 130 获取随后生成的数据 131 时，提供了如图 1 所示的使用规则（Usage Rule）132。其中记录了要获取的随后生成的数据的使用限制信息的使用规则（Usage Rule）132 包括关于以上项目（1）至（5）中描述的指示随后生成的数据的使用限制模式的绑定类型的描述。

将参考图 5 描述与随后生成的数据相对应的使用规则（Usage Rule）中包括的绑定类型的特定描述示例。

图 5A 示出与随后生成的数据相对应的绑定类型和代码（8 位）之间的对应关系的示例。在图示示例中，这些代码或绑定类型是在每 CPS 单元的基础上指定的，并且被记录在与随后生成的数据相对应的使用规则（Usage Rule）中。图 5Ba 示出其中随后生成的数据的绑定类型被 XML 描述所记录的使用规则（UR）的示例。图 5Bb 示出这样的使用规则（UR）：其中随后生成的数据的绑定类型是在每 CPS 单元的基础上指定的，并且随后生成的数据的绑定类型的代码数据被 8 位的二进制描述所记录。

注意，绑定类型不一定要被记录在使用规则（Usage Rule）中，而是可以被记录在不同于使用规则（Usage Rule）的数据文件中。例如，与各自的随后生成的数据相对应的绑定类型可以被记录在存储随后生成的数据的搜索数据的随后生成数据搜索信息文件中。图 5Bc 示出了这种情况，其中记录了这样的数据，在该数据中记录在本地存储装置上的随后生成的数据的名称和绑定类型彼此相关联。

当信息处理器获取新的随后生成的数据并且将其记录到本地存储装置

上时，与随后生成的数据相对应的文件名称和绑定信息被获取，并且存储随后生成的数据的搜索数据的随后生成数据搜索信息文件被更新。如图5Bc 所示，在每个随后生成的数据的绑定类型被记录在随后生成数据搜索信息文件中的情况下，当利用随后生成的数据时，信息处理器可以读取存储在本地存储装置上的随后生成数据搜索信息文件，以获取所需要的随后生成的数据的绑定类型，从而可以以高效的方式检查每个随后生成的数据的绑定类型。

接下来，参考图 6 及之后的附图，将按下述顺序分别针对：

（1）设备绑定型随后生成数据；

（2）盘绑定型随后生成数据；以及

（3）封装绑定型随后生成数据，

以所列的顺序分别描述以下三个处理序列的细节：

（a）获取随后生成的数据的处理；

（b）用于将随后生成的数据记录到本地存储装置上的处理；以及

（c）对记录在本地存储装置上的随后生成的数据进行解密和使用的处理。

[（3.1）用于获取、记录和使用设备绑定型随后生成数据的处理的细节]

首先，将详细描述用于获取、记录和使用设备绑定型随后生成数据的处理。

如上所述，设备绑定型随后生成数据是这样一种类型随后生成数据，这种类型的随后生成数据只许可已获取（下载）了随后生成的数据的设备（信息处理器）使用随后生成的数据。

（3.1.a）设备绑定型随后生成数据的获取处理

现将参考图 6 描述设备绑定型随后生成数据的获取处理。在图 6 中，获取随后生成的数据的信息处理器在左侧示出，提供随后生成的数据的服务器在右侧示出。

信息处理器利用以上所述的被加载到信息处理器的驱动器中的存储被分段成 CPS 单元的内容的信息记录介质来执行随后生成的数据的获取处

理。其卷 ID = #m 的信息记录介质存储：

加密后的内容：Enc(Ku1, CPS_Unit#1)到 Enc(Ku_n, CPS_Unit#n)；以及

CPS 单元密钥文件：Enc(Ke, f(Ku_1, UR#1)到(Ke, f(Ku_n, UR#n))。

此外，参考图 1 描述的各种信息被记录到信息记录介质上。图 6 示出作为这种信息的一部分的卷 ID、下载信息、MKB 等各自的数据。

此外，设备密钥[Kd]被存储在信息处理器的存储器中。设备密钥[Kd]是应用到 MKB 的处理的密钥。MKB 是只允许通过基于存储在拥有有效许可证的用户的信息处理器中的设备密钥[Kd]的处理（解密）来获取介质密钥[Km]的密钥信息块，所述介质密钥[Km]是对内容解密所必需的。为了对加密后的内容进行解密，信息处理器利用存储在存储器中的设备密钥[Kd]执行 MKB 处理。注意，内容解密处理的细节将在稍后描述。

此外，如图 6 所示，提供随后生成的数据的服务器与卷 ID 和下载信息相关联地存储：

作为随后生成的数据的加密后的子内容[Enc(Ku_n+1, CPS_Unit#n+1)]；

通过对用于对作为随后生成的数据的加密后的子内容进行解密的单元密钥进行加密而创建的 CPS 单元密钥文件[Enc(Ke, f(Ku_n+1, UR#n+1))]；以及

与作为随后生成的数据的加密后的子内容相对应的使用规则（UR：Usage Rule#n+1）。

现将描述步骤 S101 到 S107 各自的处理。在步骤 S101 中，信息处理器向服务器发送从信息记录介质获取的卷 ID（Volume ID#m）和下载信息（Download_info）。

在步骤 S102 中，接收到卷 ID（Volume ID#m）和下载信息（Download_info）的服务器执行数据库搜索，并且获取与卷 ID（Volumn ID#m）和下载信息（Download_info）相关联存储的数据，即服务器获取以下各数据：

通过对用于对作为随后生成的数据的加密后的子内容进行解密的单元

密钥进行加密而创建的 CPS 单元密钥文件[Enc(Ke, f(Ku_n+1, UR#n+1))]；

与作为随后生成的数据的加密后的子内容相对应的使用规则（UR：Usage Rule#n+1）；以及

作为随后生成的数据的加密后的子内容[Enc(Ku_n+1, CPS_Unit#n+1)]，

并且在步骤 S103 和 S104 中将所获取的这些数据发送到信息处理器。注意，步骤 S103 中的发送服务器帮助从所发送的卷 ID 和下载信息加密后的子内容，并且步骤 S104 中的发送服务器帮助保持相应内容；这些服务器当然可以是同一个服务器，或者可以是能够向彼此传输信息的多个服务器。

一旦接收到从服务器发送来的数据，在步骤 S105 中，信息处理器就利用卷唯一密钥[Ke]对 CPS 单元密钥文件的数据进行解密，所述 CPS 单元密钥文件也就是通过对用于对加密后的子内容进行解密的单元密钥进行加密而创建的 CPS 单元密钥文件[Enc(Ke, f(Ku_n+1, UR#n+1))]。在步骤 S106 中，信息处理器利用存储在存储器中的设备密钥[Kd]执行绑定处理，以及解密处理，从而生成加密后的绑定单元密钥[Enc(Ke, f(Ku_n+1, UR#n+1, Kd))]。注意，这些数据处理的细节将在稍后参考图 7 来描述。

在步骤 S107 中，从服务器获取的数据，包括：

作为随后生成的数据的加密后的子内容[Enc(Ku_n+1, CPS_Unit#n+1)]；以及

与作为随后生成的数据的加密后的子内容相对应的使用规则（UR：Usage Ruge#n+1）；以及

由信息处理器在从服务器获取的 CPS 单元密钥文件[Enc(Ke, f(Ku_n+1, UR#n+1))]基础上生成的数据，即：

加密后的绑定单元密钥[Enc(Ke, f(Ku_n+1, UR#n+1, Kd))]，

被存储到本地存储装置上。

（3.1.b）用于将设备绑定型随后生成数据记录到本地存储装置上的处理

接下来，将参考图 7 描述用于将设备绑定型随后生成数据记录到本地

存储装置上的处理，尤其是用于生成加密后的绑定单元密钥[Enc(Ke, f(Ku_n+1, UR#n+1, Kd))}的处理序列。

图 7 示出用于从服务器获取随后生成的数据等并且将所获取的数据和关于所获取的数据的处理数据存储到本地存储装置 320 上的信息处理器 300、提供随后生成的数据等的服务器 400，以及被加载到信息处理器 300 中的信息记录介质 100。

虽然信息记录介质 100 存储了以上参考图 1 所描述的各种数据，但在图示示例中，只有作为加密密钥块的 MKB 112 和卷 ID 113 被示为要被应用到用于将设备绑定型随后生成数据记录到本地存储装置上的处理的数据。

正如以上参考图 6 所描述的，服务器向信息处理器 300 提供以下数据：

作为随后生成的数据的加密后的子内容 [Enc(Ku_n+1, CPS_Unit#n+1)]403；

通过对用于对作为随后生成的数据的加密后的子内容 403 进行解密的单元密钥进行加密而创建的 CPS 单元密钥文件[Enc(Ke, f(Ku_n+1, UR#n+1))]401；以及

与作为随后生成的数据的加密后的子内容 403 相对应的使用规则（UR：Usage Rule#n+1)402。

现将描述信息处理器 300 的处理。首先，信息处理器 300 读取存储在存储器中的设备密钥[Kd]301。设备密钥 301 是存储在接收到关于内容使用的许可证的信息处理器中的密钥。

接下来，在步骤 S121 中，信息处理器 300 通过利用设备密钥 301 执行 MKB 112 的解密处理，来获取介质密钥 Km，所述 MKB 112 是存储被存储在信息记录介质 100 上的介质密钥 Km 的加密密钥块。

接下来，在步骤 S122 中，通过基于由步骤 S121 中的 MKB 处理所获取的介质密钥 Km 和从信息记录介质 100 读取的卷 ID 113 的加密处理来生成卷唯一密钥 Ke（嵌入密钥）。这个密钥生成处理被执行为根据例如 AES 加密算法的处理。

现将参考图 8 详细描述 AES 加密算法。作为根据 AES 加密算法的处理，例如实现了基于 AES 的散列函数[AES_H]。如图 8 所示，基于 AES 的散列函数是由密钥生成处理执行部分（AES_G）和异或部分的组合构成的，所述密钥生成处理执行部分涉及被应用了 AES 加密处理的数据解密处理。此外，如图 8 所示，AES_G 部分由 AES 解密部分[AES_H]和异或部分的组合构成。

图 7 中步骤 S122 中的生成卷唯一密钥 Ke 的处理例如被执行为被应用基于 AES 的散列函数[AES_H]的处理，其中以在步骤 S121 中的 MKB 处理中获取的介质密钥 Km 和从信息记录介质 100 读取的卷 ID 113 作为输入。

接下来，在步骤 S123 中，利用卷唯一密钥 Ke，执行从服务器获取的 CPS 单元密钥文件[Enc(Ke, f(Ku_n+1, UR#n+1))]311（=401）的解密处理。通过这个解密处理，

从：CPS 单元密钥文件[Enc(Ke, f(Ku_n+1, UR#n+1))]

获取了数据[Kt] = f(Ku_n+1, UR#n+1)。

接下来，在步骤 S124 中，通过执行计算处理来生成绑定单元密钥（BKu）数据，其中存储在信息处理器 300 的存储器中的设备密钥[Kd]和与从服务器获取的随后生成的数据相对应的使用规则（UR：Usage Rule#n+1）321（=402）被应用到该计算处理。绑定单元密钥（BKu）是以下数据：

BKu = f(Ku_n+1, UR#n+1, Kd)

绑定单元密钥：BKu = f(Ku_n+1, UR#n+1, Kd)是与 CPS 单元#n+1 对应的单元密钥[Ku_n+1]、使用规则[UR#n+1]和设备密钥[Kd]之间的异或运算之类的计算结果数据。

此外，在步骤 S125 中，利用步骤 S122 中计算的卷唯一密钥 Ke 执行绑定单元密钥：BKu = f(Ku_n+1, UR#n+1, Kd)的加密处理，并且生成加密后的绑定单元密钥[Enc(Ke, f(Ku_n+1, UR#n+1, Kd))]并将其存储到本地存储装置 320 上。

注意本地存储装置 320 存储：

由上述处理生成的加密后的绑定单元密钥[Enc(Ke, f(Ku_n+1, UR#n+1,

Kd))]323；以及

从服务器获取的以下数据：

作为随后生成的数据的加密后的子内容 [Enc(Ku_n+1, CPS_Unit#n+1)]322（=403）；以及

与作为随后生成的数据的加密后的子内容 322 相对应的使用规则（UR：Usage Rule#n+1）321（=402）。

（3.1.c）用于对记录在本地存储装置上的设备绑定型随后生成数据进行解密和使用的处理

接下来，将描述用于使用记录在本地存储装置上的设备绑定型随后生成数据的处理。用于使用记录在本地存储装置上的设备绑定型随后生成数据的处理被执行为与用于使用记录在信息记录介质上的内容的数据处理类似的处理。首先，将参考图 9 描述用于使用记录在信息记录介质上的内容的数据处理。

首先，信息处理器 300 读取存储在存储器中的设备密钥[Kd]301。设备密钥 301 是存储在接收到关于内容使用的许可证的信息处理器中的密钥。

接下来，在步骤 S131 中，信息处理器 300 通过利用设备密钥 301 执行 MKB 112 的解密处理，来获取介质密钥 Km，所述 MKB 112 是作为存储被存储在信息记录介质 100 上的介质密钥 Km 的加密密钥块的。

接下来，在步骤 S132 中，通过基于由步骤 S131 中的 MKB 处理所获取的介质密钥 Km 和从信息记录介质 100 读取的卷 ID 113 的加密处理来生成卷唯一密钥 Ke（嵌入密钥）。这个密钥生成处理被执行为根据例如以上参考图 8 描述的 AES 加密算法的处理。

接下来，在步骤 S133 中，执行 CPS 单元密钥文件 116 的解密处理，CPS 单元密钥文件 116 也就是从信息记录介质 100 读取的[Enc(Ke, f(Ku_n+1, UR#n+1))]。注意，此时使用的 CPS 单元被假定为 CPS 单元[CPS_Unit#n]。

通过步骤 S133 中的 CPS 单元密钥文件 116 的解密处理，获取了

数据[Kt] = f(Ku_n+1, UR#n+1)

并且在步骤 S134 中，针对：

数据[Kt] = f(Ku_n+1, UR#n+1)，

执行被应用了从信息记录介质 100 读取的使用规则（UR：Usage Rule#n）115 的计算处理，从而获得单元密钥[Ku_n]。

当例如数据[Kt] = f(Ku_n+1, UR#n+1)是单元密钥[Ku_n]和使用规则（UR#n）之间的异或（XOR）结果数据时，可以通过再对上述计算结果执行从信息记录介质 100 读取的使用规则（UR#n）的异或（XOR）运算，来获取单元密钥[Ku_n]。

接下来，在步骤 S135 中，针对从信息记录介质 100 读取的加密后的内容，执行利用单元密钥[Ku_n]的解密处理（例如 AES_D）。在步骤 S136 中，执行必要的解码操作，例如 MPEG 解码、压缩/解压缩或解扰，以获取内容 350。

通过该处理，可以对存储在信息记录介质 100 上的作为 CPS 单元被管理的加密后的内容进行解密以便使用，即以便再现。

接下来，参考图 10，将描述用于使用存储在本地存储装置 320 上的作为随后生成的数据的加密后的子内容 322 的处理。假设本地存储装置 320 存储以下数据作为通过以上参考图 6 和图 7 描述的处理而存储的数据：

作为随后生成的数据的加密后的子内容 [Enc(Ku_n+1, CPS_Unit#n+1)]322；

与作为随后生成的数据的加密后的子内容 322 相对应的使用规则（UR：Usage Rule#n+1）321（=402）；以及

加密后的绑定单元密钥[Enc(Ke, f(Ku_n+1, UR#n+1, Kd))]322。

首先，信息处理器 300 读取存储在存储器中的设备密钥[Kd]301。设备密钥 301 是存储在已接收到关于内容使用的许可证的信息处理器中的密钥。

接下来，在步骤 S151 中，信息处理器 300 通过利用设备密钥 301 执行 MKB 112 的解密处理，来获取介质密钥 Km，所述 MKB 112 是作为存储被存储在信息记录介质 100 上的介质密钥 Km 的加密密钥块的。

接下来，在步骤 S152 中，通过基于由步骤 S151 中的 MKB 处理所获取的介质密钥 Km 和从信息记录介质 100 读取的卷 ID 113 的加密处理来生

成卷唯一密钥 Ke。这个密钥生成处理被执行为根据例如以上参考图 8 描述的 AES 加密算法的处理。

接下来，在步骤 S153 中，利用卷唯一密钥 Ke，执行从本地存储装置 320 读取的加密后的绑定单元密钥[Enc(Ke, f(Ku_n+1, UR#n+1, Kd))]的解密处理。

通过步骤 S153 中的加密后的绑定单元密钥[Enc(Ke, f(Ku_n+1, UR#n+1,KD))]的解密处理，获取了

绑定单元密钥[BKu] = f(Ku_n+1, UR#n+1, Kd)

并且在步骤 S154 中，针对：

绑定单元密钥[BKu] = f(Ku_n+1, UR#n+1, Kd)，

执行计算处理，其中从本地存储装置 320 读取的使用规则（UR：Usage Rule#n+1）321 和存储在信息处理器 300 的存储器中的设备密钥[Kd]被应用到该计算处理，从而获得单元密钥[Ku_n+1]

当例如绑定单元密钥[BKu] = f(Ku_n+1, UR#n+1, Kd)是单元密钥[Ku_n+1]、使用规则[UR#n+1]和设备密钥[Kd]之间的异或（XOR）数据时，可以通过再次针对绑定单元密钥[BKu]在从本地存储装置 320 读取的使用规则（UR：Usage Rule#n+1）和存储在信息处理器 300 的存储器中的设备密钥[Kd]之间执行异或（XOR）运算来获取单元密钥[Ku_n+1]。

接下来，在步骤 S155 中，针对从本地存储装置 320 读取的加密后的子内容[Enc(Ku_n+1, CPS_Unit#n+1)]322，执行利用单元密钥[Ku_n+1]的解密处理（例如 AES_D）。在步骤 S156 中，执行必要的解码处理，例如 MPEG 解码、压缩/解压缩或解扰，以获取内容 350。

通过该处理，可以对存储在本地存储装置 320 中的作为随后生成的数据的加密后的子内容[Enc(Ku_n+1, CPS_Unit#n+1)]322 进行解密以便使用，即以便再现。

这样，对于设备绑定型随后生成数据，正如以上参考图 7 所描述的，当将从服务器获取的随后生成的数据存储到本地存储装置上时，通过从服务器接收到的、被加密并以加密后的绑定单元密钥的形式被存储到本地存储装置上的 CPS 单元密钥文件的处理，CPS 单元密钥和设备密钥[Kd]被绑

定在一起；正如以上参考图 10 所描述的，要使用随后生成的数据，必须利用设备密钥[Kd]执行处理，以从存储在本地存储装置上的加密后的绑定单元密钥获取单元密钥。

解除绑定和单元密钥获取的必要条件是再现随后生成的数据时使用的设备密钥[Kd]是与记录随后生成的数据时使用的相同的密钥[Kd]。因此，如上所述，设备绑定型随后生成数据是仅许可已获取（下载）了随后生成的数据的设备（信息处理器）使用的随后生成的数据。

[（3.2）用于获取、记录和使用盘绑定型随后生成数据的处理的细节]

接下来，将详细描述用于获取、记录和使用盘绑定型随后生成数据的处理。如上所述，盘绑定型随后生成数据是这样一种类型的随后生成数据，这种类型的随后生成数据的使用只在信息处理器被加载以与获取（下载）随后生成的数据时使用的信息记录介质（盘）具有相同序列号的盘时才被许可。

（3.2.a）盘绑定型随后生成数据的获取处理

现将参考图 11 描述盘绑定型随后生成数据的获取处理。在图 11 中，获取随后生成的数据的信息处理器在左侧示出，提供随后生成的数据的服务器在右侧示出。

信息处理器利用以上所述的被加载到信息处理器的驱动器中的存储被分段成 CPS 单元的内容的信息记录介质来执行随后生成的数据的获取处理。其卷 ID = #m 的信息记录介质存储：

加密后的内容：Enc(Ku_1, CPS_Unit#1)到 Enc(Ku_n, CPS_Unit#n)；以及

CPS 单元密钥文件：Enc(Ke, f(Ku_1, UR#1)到(Ke, f(Ku_n, UR#n))。

此外，参考图 1 描述的各种信息被记录到信息记录介质上。图 6 示出作为这种信息的一部分的卷 ID、下载信息、MKB 等各自的数据。

正如以上参考图 6 所描述的，提供随后生成的数据的服务器与卷 ID 和下载信息相关联地存储：

作为随后生成的数据的加密后的子内容 [Enc(Ku_n+1, CPS_Unit#n+1)]；

通过对用于对作为随后生成的数据的加密后的子内容进行解密的单元密钥进行加密而创建的 CPS 单元密钥文件[Enc(Ke, f(Ku_n+1, UR#n+1))]；以及

与作为随后生成的数据的加密后的子内容相对应的使用规则（UR：Usage Rule#n+1）。

现将描述步骤 S201 到 S207 各自的处理。在步骤 S201 中，信息处理器向服务器发送从信息记录介质获取的卷 ID（Volume ID#m）和下载信息（Download_info）。

在步骤 S202 中，接收到卷 ID（Volume ID#m）和下载信息（Download_info）的服务器执行数据库搜索，并且获取与卷 ID（Volumn ID#m）和下载信息（Download_info）相关联地存储的数据，即服务器获取以下各数据：

通过对用于对作为随后生成的数据的加密后的子内容进行解密的单元密钥进行加密而创建的 CPS 单元密钥文件[Enc(Ke, f(Ku_n+1, UR#n+1))]；

与作为随后生成的数据的加密后的子内容相对应的使用规则（UR：Usage Rule#n+1）；以及

作为随后生成的数据的加密后的子内容[Enc(Ku_n+1, CPS_Unit#n+1)]，

并且在步骤 S203 和 S204 中将所获取的这些数据发送到信息处理器。

一旦接收到从服务器发送来的数据，在步骤 S205 中，信息处理器就利用卷唯一密钥[Ke]对 CPS 单元密钥文件的数据进行解密，所述 CPS 单元密钥文件也就是通过对用于对加密后的子内容进行解密的单元密钥进行加密而创建的 CPS 单元密钥文件[Enc(Ke, f(Ku_n+1, UR#n+1))]。在步骤 S206 中，信息处理器利用从信息记录介质读取的序列号[SN]执行绑定处理，以及解密处理，从而生成加密后的绑定单元密钥[Enc(Ke, f(Ku_n+1, UR#n+1, SN))]。注意，这些数据处理的细节将在稍后参考图 12 来描述。

在步骤 S207 中，从服务器获取的数据，包括：

作为随后生成的数据的加密后的子内容[Enc(Ku_n+1, CPS_Unit#n+1)]；以及

与作为随后生成的数据的加密后的子内容相对应的使用规则（UR：Usage Ruge#n+1）；以及

由信息处理器在从服务器获取的 CPS 单元密钥文件[Enc(Ke, f(Ku_n+1, UR#n+1))]基础上生成的数据，即：

加密后的绑定单元密钥[Enc(Ke, f(Ku_n+1, UR#n+1, SN))]，

被存储到本地存储装置上。

（3.2.b）用于将盘绑定型随后生成数据记录到本地存储装置上的处理

接下来，将参考图 12 描述用于将盘绑定型随后生成数据记录到本地存储装置上的处理，尤其是用于生成加密后的绑定单元密钥[Enc(Ke, f(Ku_n+1, UR#n+1, SN))]的处理序列。

图 12 示出用于从服务器获取随后生成的数据等并且将所获取的数据和关于所获取的数据的处理数据存储到本地存储装置 320 上的信息处理器 300、提供随后生成的数据等的服务器 400，以及被加载到信息处理器 300 中的信息记录介质 100。

虽然信息记录介质 100 存储了以上参考图 1 所描述的各种数据，但在图示示例中，只有作为加密密钥块的 MKB 112、卷 ID 113 和序列号 117 被示为要被应用到用于将盘绑定型随后生成数据记录到本地存储装置上的处理的数据。

正如以上参考图 11 所描述的，服务器向信息处理器 300 提供以下数据：

作为随后生成的数据的加密后的子内容[Enc(Ku_n+1, CPS_Unit#n+1)]403；

通过对用于对作为随后生成的数据的加密后的子内容 403 进行解密的单元密钥进行加密而创建的 CPS 单元密钥文件[Enc(Ke, f(Ku_n+1, UR#n+1))]401；以及

与作为随后生成的数据的加密后的子内容 403 相对应的使用规则（UR：Usage Rule#n+1）402。

现将描述信息处理器 300 的处理。首先，信息处理器 300 读取存储在存储器中的设备密钥[Kd]301。设备密钥 301 是存储在接收到关于内容使用

的许可证的信息处理器中的密钥。

接下来，在步骤 S211 中，信息处理器 300 通过利用设备密钥 301 执行 MKB 112 的解密处理，来获取介质密钥 Km，所述 MKB 112 是存储被存储在信息记录介质 100 上的介质密钥 Km 的加密密钥块。

接下来，在步骤 S212 中，通过基于由步骤 S211 中的 MKB 处理所获取的介质密钥 Km 和从信息记录介质 100 读取的卷 ID 113 的加密处理来生成卷唯一密钥 Ke（嵌入密钥）。这个密钥生成处理被执行为根据例如以上参考图 8 所描述的 AES 加密算法的处理。

接下来，在步骤 S213 中，利用卷唯一密钥 Ke，执行从服务器获取的 CPS 单元密钥文件[Enc(Ke, f(Ku_n+1, UR#n+1))]311（=401）的解密处理。通过这个解密处理，

从：

CPS 单元密钥文件[Enc(Ke, f(Ku_n+1, UR#n+1))]

获取了数据[Kt] = f(Ku_n+1, UR#n+1)。

接下来，在步骤 S214 中，通过执行计算处理来生成绑定单元密钥（BKu）数据，其中从信息记录介质 100 读取的序列号[SN]和与从服务器获取的随后生成的数据相对应的使用规则（UR：Usage Rule#n+1）321（=402）被应用到该计算处理。绑定单元密钥（BKu）是以下数据：

BKu = f(Ku_n+1, UR#n+1, SN)

绑定单元密钥：BKu = f(Ku_n+1, UR#n+1, SN)是与 CPS 单元#n+1 对应的单元密钥[Ku_n+1]、使用规则[UR#n+1]和序列号[SN]之间的异或运算之类的计算结果数据。

此外，在步骤 S215 中，利用步骤 S212 中计算的卷唯一密钥 Ke 执行绑定单元密钥：BKu = f(Ku_n+1, UR#n+1, SN)的加密处理，并且生成加密后的绑定单元密钥[Enc(Ke, f(Ku_n+1, UR#n+1, SN))]并将其存储到本地存储装置 320 上。

注意本地存储装置 320 存储：

由上述处理生成的加密后的绑定单元密钥[Enc(Ke, f(Ku_n+1, UR#n+1, SN))]324；以及

从服务器 400 获取的以下数据：

作为随后生成的数据的加密后的子内容 [Enc(Ku_n+1, CPS_Unit#n+1)]322（=403）；以及

与作为随后生成的数据的加密后的子内容 322 相对应的使用规则（UR：Usage Rule#n+1）321（=402）。

（3.2.c）用于对记录在本地存储装置上的盘绑定型随后生成数据进行解密和使用的处理

接下来，将参考图 13 描述用于使用记录在本地存储装置上的盘绑定型随后生成数据的处理。假设本地存储装置 320 存储以下数据作为通过以上参考图 11 和 12 描述的处理而存储的数据：

作为随后生成的数据的加密后的子内容 [Enc(Ku_n+1, CPS_Unit#n+1)]322；

与作为随后生成的数据的加密后的子内容 322 相对应的使用规则（UR：Usage Rule#n+1）321（=402）；以及

加密后的绑定单元密钥[Enc(Ke, f(Ku_n+1, UR#n+1, SN))]324。

首先，信息处理器 300 读取存储在存储器上的设备密钥[Kd]301。设备密钥 301 是存储在接收到关于内容使用的许可证的信息处理器中的密钥。

接下来，在步骤 S251 中，信息处理器 300 通过利用设备密钥 301 执行 MKB 112 的解密处理，来获取介质密钥 Km，所述 MKB 112 是作为存储被存储在信息记录介质 100 上的介质密钥 Km 的加密密钥块的。

接下来，在步骤 S252 中，通过基于由步骤 S251 中的 MKB 处理所获取的介质密钥 Km 和从信息记录介质 100 读取的卷 ID 113 的加密处理来生成卷唯一密钥 Ke。这个密钥生成处理被执行为根据例如以上参考图 8 描述的 AES 加密算法的处理。

接下来，在步骤 253 中，利用卷唯一密钥 Ke，执行从本地存储装置 320 读取的加密后的绑定单元密钥[Enc(Ke, f(Ku_n+1, UR#n+1, SN))]324 的解密处理。

通过步骤 S253 中的加密后的绑定单元密钥[Enc(Ke, f(Ku_n+1, UR#n+1, SN))]324 的解密处理，获取了

绑定单元密钥[BKu] = f(Ku_n+1, UR#n+1, SN)

并且在步骤 S254 中，针对：

绑定单元密钥[BKu] = f(Ku_n+1, UR#n+1, SN)，

执行计算处理，其中从本地存储装置 320 读取的使用规则（UR：Usage Rule#n+1）321 和从信息记录介质读取的序列号[SN]被应用到该计算处理，从而获得单元密钥[Ku_n+1]。

当例如绑定单元密钥[BKu] = f(Ku_n+1, UR#n+1, SN)是单元密钥[Ku_n+1]、使用规则[UR#n+1]和序列号[SN]之间的异或（XOR）数据时，可以通过再次针对绑定单元密钥[BKu]在从本地存储装置 320 读取的使用规则（UR：Usage Rule#n+1）和从信息记录介质 100 读取的序列号[SN]之间执行异或（XOR）运算来获取单元密钥[Ku_n+1]。

接下来，在步骤 S255 中，针对从本地存储装置 320 读取的加密后的子内容[Enc(Ku_n+1, CPS_Unit#n+1)]322，执行利用单元密钥[Ku_n+1]的解密处理（例如 AES_D）。在步骤 S256 中，执行必要的解码处理，例如 MPEG 解码、压缩/解压缩或解扰，以获取内容 350。

通过该处理，可以对存储在本地存储装置 320 中的作为随后生成的数据的加密后的子内容[Enc(Ku_n+1, CPS_Unit#n+1)]322 进行解密以便使用，即以便再现。

这样一来，对于盘绑定型随后生成数据，正如以上参考图 12 所描述的，当将从服务器获取的随后生成的数据存储到本地存储装置上时，通过从服务器接收到的、被加密并以加密后的绑定单元密钥的形式被存储到本地存储装置上的 CPS 单元密钥文件的处理，CPS 单元密钥和序列号[SN]被绑定在一起；正如以上参考图 13 所描述的，要使用随后生成的数据，必须利用序列号[SN]执行处理，以从存储在本地存储装置上的加密后的绑定单元密钥获取单元密钥。

解除绑定和单元密钥获取的必要条件是再现随后生成的数据时使用的序列号[SN]是与记录随后生成的数据时使用的相同的序列号[SN]。因此，如上所述，盘绑定型随后生成数据是这样的随后生成数据，这种随后生成的数据的使用只在信息处理器被加载以与获取（下载）随后生成的数据时

使用的信息记录介质（盘）具有相同序列号的盘时才被许可。

[（3.3）用于获取、记录和使用封装绑定型随后生成数据的处理的细节]

接下来，将详细描述用于获取、记录和使用封装绑定型随后生成数据的处理。如上所述，封装绑定型随后生成数据是这样一种类型的随后生成数据，这种类型的随后生成数据的使用只在信息处理器被加载以与获取（下载）随后生成的数据时使用的信息记录介质（盘）具有相同封装 ID 的信息记录介质（盘）时才被许可。

（3.3.a）封装绑定型随后生成数据的获取处理

现将参考图 14 描述封装绑定型随后生成数据的获取处理。在图 14 中，获取随后生成的数据的信息处理器在左侧示出，提供随后生成的数据的服务器在右侧示出。

信息处理器利用以上所述的被加载到信息处理器的驱动器中的存储被分段成 CPS 单元的内容的信息记录介质来执行随后生成的数据的获取处理。其卷 ID = #m 的信息记录介质存储：

加密后的内容：Enc(Ku1, CPS_Unit#1)到 Enc(Ku_n, CPS_Unit#n)；以及

CPS 单元密钥文件：Enc(Ke, f(Ku_1, UR#1)到(Ke, f(Ku_n, UR#n))。

此外，参考图 1 描述的各种信息被记录到信息记录介质上。图 6 示出作为这种信息的一部分的卷 ID、下载信息、MKB 等各自的数据。

正如以上参考图 6 所描述的，提供随后生成的数据的服务器联系卷 ID 和下载信息存储：

作为随后生成的数据的加密后的子内容 [Enc(Ku_n+1, CPS_Unit#n+1)]；

通过对用于对作为随后生成的数据的加密后的子内容进行解密的单元密钥进行加密而创建的 CPS 单元密钥文件[Enc(Ke, f(Ku_n+1, UR#n+1))]；以及

与作为随后生成的数据的加密后的子内容相对应的使用规则（UR：Usage Rule#n+1）。

现将描述步骤 S301 到 S307 各自的处理。在步骤 S301 中，信息处理器向服务器发送从信息记录介质获取的卷 ID（Volume ID#m）和下载信息（Download_info）。

在步骤 S302 中，接收到卷 ID（Volume ID#m）和下载信息（Download_info）的服务器执行数据库搜索，并且获取联系卷 ID（Volumn ID#m）和下载信息（Download_info）存储的数据，即服务器获取以下各数据：

通过对用于对作为随后生成的数据的加密后的子内容进行解密的单元密钥进行加密而创建的 CPS 单元密钥文件[Enc(Ke, f(Ku_n+1, UR#n+1))]；

与作为随后生成的数据的加密后的子内容相对应的使用规则（UR：Usage Rule#n+1）；以及

作为随后生成的数据的加密后的子内容 [Enc(Ku_n+1, CPS_Unit#n+1)]，

并且在步骤 S303 和 S304 中将所获取的这些数据发送到信息处理器。

一旦接收到从服务器发送来的数据，在步骤 S305 中，信息处理器就利用卷唯一密钥[Ke]对 CPS 单元密钥文件的数据进行解密，所述 CPS 单元密钥文件也就是通过对用于对加密后的子内容进行解密的单元密钥进行加密而创建的 CPS 单元密钥文件[Enc(Ke, f(Ku_n+1, UR#n+1))]。在步骤 S306 中，信息处理器利用从信息记录介质读取的封装 ID[PID]执行绑定处理，以及解密处理，从而生成加密后的绑定单元密钥[Enc(Ke, f(Ku_n+1, UR#n+1, PID))]。注意，这些数据处理的细节将在稍后参考图 15 来描述。

在步骤 S307 中，从服务器获取的数据，包括：

作为随后生成的数据的加密后的子内容 [Enc(Ku_n+1, CPS_Unit#n+1)]；以及

与作为随后生成的数据的加密后的子内容相对应的使用规则（UR：Usage Ruge#n+1）；以及

由信息处理器在从服务器获取的 CPS 单元密钥文件[Enc(Ke, f(Ku_n+1, UR#n+1))]基础上生成的数据，即：

加密后的绑定单元密钥[Enc(Ke, f(Ku_n+1, UR#n+1, PID))]，

被存储到本地存储装置上。

（3.3.b）用于将封装绑定型随后生成数据记录到本地存储装置上的处理

接下来，将参考图 15 描述用于将封装绑定型随后生成数据记录到本地存储装置上的处理，尤其是用于生成加密后的绑定单元密钥[Enc(Ke, f(Ku_n+1, UR#n+1, PID))]的处理序列。

图 15 示出用于从服务器获取随后生成的数据等并且将所获取的数据和关于所获取的数据的处理数据存储到本地存储装置 320 上的信息处理器 300、提供随后生成的数据等的服务器 400，以及被加载到信息处理器 300 中的信息记录介质 100。

虽然信息记录介质 100 存储了以上参考图 1 所描述的各种数据，但在图示示例中，只有作为加密密钥块的 MKB 112、卷 ID 113 和封装 ID114 被示为要被应用到用于将封装绑定型随后生成数据记录到本地存储装置上的处理的数据。

正如以上参考图 14 所描述的，服务器向信息处理器 300 提供以下数据：

作为随后生成的数据的加密后的子内容[Enc(Ku_n+1, CPS_Unit#n+1)]403；

通过对用于对作为随后生成的数据的加密后的子内容 403 进行解密的单元密钥进行加密而创建的 CPS 单元密钥文件[Enc(Ke, f(Ku_n+1, UR#n+1))]401；以及

与作为随后生成的数据的加密后的子内容 403 相对应的使用规则（UR：Usage Rule#n+1）402。

现将描述信息处理器 300 的处理。首先，信息处理器 300 读取存储在存储器中的设备密钥[Kd]301。设备密钥 301 是存储在接收到关于内容使用的许可证的信息处理器中的密钥。

接下来，在步骤 S311 中，信息处理器 300 通过利用设备密钥 301 执行 MKB 112 的解密处理，来获取介质密钥 Km，所述 MKB 112 是存储被存储在信息记录介质 100 上的介质密钥 Km 的加密密钥块。

接下来，在步骤 S312 中，通过基于由步骤 S311 中的 MKB 处理所获取的介质密钥 Km 和从信息记录介质 100 读取的卷 ID 113 的加密处理来生成卷唯一密钥 Ke（嵌入密钥）。这个密钥生成处理被执行为根据例如以上参考图 8 所描述的 AES 加密算法的处理。

接下来，在步骤 S313 中，利用卷唯一密钥 Ke，执行从服务器获取的 CPS 单元密钥文件[Enc(Ke, f(Ku_n+1, UR#n+1))]311（=401）的解密处理。通过这个解密处理，

从：

CPS 单元密钥文件[Enc(Ke, f(Ku_n+1, UR#n+1))]

获取了数据[Kt] = f(Ku_n+1, UR#n+1)。

接下来，在步骤 S314 中，通过执行计算处理来生成绑定单元密钥（BKu）数据，其中从信息记录介质 100 读取的封装 ID[PID]和与从服务器获取的随后生成的数据相对应的使用规则（UR：Usage Rule#n+1）321（=402）被应用到该计算处理。绑定单元密钥（BKu）是以下数据：

BKu = f(Ku_n+1, UR#n+1, PID)

绑定单元密钥：BKu = f(Ku_n+1, UR#n+1, PID)是与 CPS 单元#n+1 对应的单元密钥[Ku_n+1]、使用规则[UR#n+1]和封装 ID[PID]之间的异或运算之类的计算结果数据。

此外，在步骤 S315 中，利用步骤 S312 中计算的卷唯一密钥 Ke 执行绑定单元密钥：BKu = f(Ku_n+1, UR#n+1, PID)的加密处理，并且生成加密后的绑定单元密钥[Enc(Ke, f(Ku_n+1, UR#n+1, PID))]并将其存储到本地存储装置 320 上。

注意本地存储装置 320 存储：

由上述处理生成的加密后的绑定单元密钥[Enc(Ke, f(Ku_n+1, UR#n+1, PID))]325；以及

从服务器 400 获取的以下数据：

作为随后生成的数据的加密后的子内容[Enc(Ku_n+1, CPS_Unit#n+1)]322（=403）；以及

与作为随后生成的数据的加密后的子内容 322 相对应的使用规则

（UR：Usage Rule#n+1）321（=402）。

（3.3.c）用于对记录在本地存储装置上的封装绑定型随后生成数据进行解密和使用的处理

接下来，将参考图 16 描述用于使用记录在本地存储装置上的封装绑定型随后生成数据的处理。假设本地存储装置 320 存储以下数据作为通过以上参考图 14 和 15 描述的处理而存储的数据：

作为随后生成的数据的加密后的子内容 [Enc(Ku_n+1, CPS_Unit#n+1)]322；

与作为随后生成的数据的加密后的子内容 322 相对应的使用规则（UR：Usage Rule#n+1）321（=402）；以及

加密后的绑定单元密钥[Enc(Ke, f(Ku_n+1, UR#n+1, PID))]325。

首先，信息处理器 300 读取存储在存储器上的设备密钥[Kd]301。设备密钥 301 是存储在接收到关于内容使用的许可证的信息处理器中的密钥。

接下来，在步骤 S351 中，信息处理器 300 通过利用设备密钥 301 执行 MKB 112 的解密处理，来获取介质密钥 Km，所述 MKB 112 是作为存储被存储在信息记录介质 100 上的介质密钥 Km 的加密密钥块的。

接下来，在步骤 S352 中，通过基于由步骤 S351 中的 MKB 处理所获取的介质密钥 Km 和从信息记录介质 100 读取的卷 ID 113 的加密处理来生成卷唯一密钥 Ke（嵌入密钥）。这个密钥生成处理被执行为根据例如以上参考图 8 描述的 AES 加密算法的处理。

接下来，在步骤 353 中，利用卷唯一密钥 Ke，执行从本地存储装置 320 读取的加密后的绑定单元密钥[Enc(Ke, f(Ku_n+1, UR#n+1, PID))]325 的解密处理。

通过步骤 S353 中的加密后的绑定单元密钥[Enc(Ke, f(Ku_n+1, UR#n+1, PID))]325 的解密处理，获取了

绑定单元密钥[BKu] = f(Ku_n+1, UR#n+1, PID)

并且在步骤 S354 中，针对：

绑定单元密钥[BKu] = f(Ku_n+1, UR#n+1, PID)，

执行计算处理，其中从本地存储装置 320 读取的使用规则（UR：

Usage Rule#n+1）321 和从信息记录介质读取的封装 ID[PID]被应用到该计算处理，从而获得单元密钥[Ku_n+1]。当例如绑定单元密钥[BKu] = f(Ku_n+1, UR#n+1, PID)是单元密钥[Ku_n+1]、使用规则[UR#n+1]和封装 ID[PID]之间的异或（XOR）数据时，可以通过再次针对绑定单元密钥[BKu]在从本地存储装置 320 读取的使用规则（UR：Usage Rule#n+1）和从信息记录介质 100 读取的封装 ID[PID]之间执行异或（XOR）运算来获取单元密钥[Ku_n+1]。

接下来，在步骤 S355 中，针对从本地存储装置 320 读取的加密后的子内容[Enc(Ku_n+1, CPS_Unit#n+1)]322，执行利用单元密钥[Ku_n+1]的解密处理（例如 AES_D）。在步骤 S356 中，执行必要的解码处理，例如 MPEG 解码、压缩/解压缩或解扰，以获取内容 350。

通过该处理，可以对存储在本地存储装置 320 中的作为随后生成的数据的加密后的子内容[Enc(Ku_n+1, CPS_Unit#n+1)]322 进行解密以便使用，即以便再现。

这样一来，对于封装绑定型随后生成数据，正如以上参考图 15 所描述的，当将从服务器获取的随后生成的数据存储到本地存储装置上时，通过从服务器接收到的、被加密并以加密后的绑定单元密钥的形式被存储到本地存储装置上的 CPS 单元密钥文件的处理，CPS 单元密钥和封装 ID[PID]被绑定在一起；正如以上参考图 16 所描述的，要使用随后生成的数据，必须利用封装 ID[PID]执行处理，以从存储在本地存储装置上的加密后的绑定单元密钥获取单元密钥。

解除绑定和单元密钥获取的必要条件是再现随后生成的数据时使用的封装 ID[PID]是与记录随后生成的数据时使用的相同的封装 ID[PID]。因此，如上所述，封装绑定型随后生成数据是这样的随后生成数据，这种随后生成的数据的使用只在信息处理器被加载以与获取（下载）随后生成的数据时使用的信息记录介质（盘）具有相同的封装 ID 的信息记录介质（盘）时才被许可。虽然在本示例中，随后生成的数据被绑定到封装 ID，但是随后生成的数据也可以被绑定到卷 ID。

[（3.4）当与随后生成的数据相对应的 CPS 单元密钥被预先存储在信

息记录介质上时用于获取、记录和使用随后生成的数据的处理的细节]

接下来，将详细描述当与随后生成的数据相对应的 CPS 单元密钥被预先存储在信息记录介质上时用于获取、记录和使用随后生成的数据的处理。存在这样的情况：在获取随后生成的数据时，与随后生成的数据相对应的 CPS 单元密钥或使用规则（UR）被预先存储在信息记录介质上。在这种情况下，不需要从服务器获取 CPS 单元密钥文件或使用规则（UR）。现将描述在这种情况下用于获取、记录和使用随后生成的数据的处理的细节。

（3.4.a）用于随后生成的数据的获取处理

现将参考图 17 描述当与随后生成的数据相对应的 CPS 单元密钥被预先存储在信息记录介质上时用于随后生成的数据的获取处理。在图 17 中，获取随后生成的数据的信息处理器在左侧示出，提供随后生成的数据的服务器在右侧示出。

信息处理器利用以上所述的被加载到信息处理器的驱动器中的存储被分段成 CPS 单元的内容的信息记录介质来执行随后生成的数据的获取处理。其卷 ID = #m 的信息记录介质存储：

加密后的内容：Enc(Ku1, CPS_Unit#1)到 Enc(Ku_n, CPS_Unit#n)；以及

CPS 单元密钥文件：Enc(Ke, f(Ku_1, UR#1)到(Ke, f(Ku_n, UR#n))。

此外，参考图 1 描述的各种信息被记录到信息记录介质上。图 6 示出作为这种信息的一部分的卷 ID、下载信息、MKB 等各自的数据。

提供随后生成的数据的服务器联系卷 ID 和下载信息存储：

作为随后生成的数据的加密后的子内容[Enc(Ku_n+1, CPS_Unit#n′)]。加密后的子内容[Enc(Ku_n+1, CPS_Unit#n′)]是用存储在信息记录介质 100 上的 CPS 单元密钥[Ku_n]加密的数据。

现将描述步骤 S401 到 S404 各自的处理。在步骤 S401 中，信息处理器向服务器发送从信息记录介质获取的卷 ID（Volume ID#m）和下载信息（Download_info）。

在步骤 S402 中，接收到卷 ID（Volume ID#m）和下载信息

（Download_info）的服务器执行数据库搜索，并且获取联系卷 ID（Volumn ID#m）和下载信息（Download_info）存储的数据，即：

作为随后生成的数据的加密后的子内容[Enc(Ku_n+1, CPS_Unit#n′)]，

并且在步骤 S403 中将所获取的数据发送到信息处理器。

一旦接收到从服务器发送来的数据，在步骤 S404 中，信息处理器就存储从服务器获取的数据，即：

作为随后生成的数据的加密后的子内容[Enc(Ku_n+1, CPS_Unit#n′)]，

并将该数据存储到本地存储装置上。

（3.4.b）用于对随后生成的数据进行解密和使用的处理

接下来，将参考图 18 描述当与随后生成的数据的 CPS 单元密钥被预先存储在信息记录介质上时用于使用随后生成的数据的处理。假设本地存储装置 320 存储以下数据作为通过以上参考图 17 描述的处理而存储的数据：

作为随后生成的数据的加密后的子内容[Enc(Ku_n+1, CPS_Unit#n′)]322。

首先，信息处理器 300 读取存储在存储器中的设备密钥[Kd]301。设备密钥 301 是存储在接收到关于内容使用的许可证的信息处理器中的密钥。

接下来，在步骤 S451 中，信息处理器 300 通过利用设备密钥 301 执行 MKB 112 的解密处理，来获取介质密钥 Km，所述 MKB 112 是作为存储被存储在信息记录介质 100 上的介质密钥 Km 的加密密钥块的。

接下来，在步骤 S452 中，通过基于由步骤 S451 中的 MKB 处理所获取的介质密钥 Km 和从信息记录介质 100 读取的卷 ID 113 的加密处理来生成卷唯一密钥 Ke。这个密钥生成处理被执行为根据例如以上参考图 8 描述的 AES 加密算法的处理。

接下来，在步骤 S453 中，利用卷唯一密钥 Ke，执行从信息记录介质 100 读取的 CPS 单元密钥文件[Enc(Ke, f(Ku_n+1, UR#n))]116 的解密处理，从而获取：

数据[t] = f(Ku_n+1, UR#n)

接下来，在步骤 S454 中，针对：

数据[t] = f(Ku_n+1, UR#n)，

执行被应用了从信息记录介质 100 读取的使用规则（UR：Usage Rule#n）115 的计算处理，从而获得单元密钥[Ku_n]。

接下来，在步骤 S455 中，针对从本地存储装置 320 读取的加密后的子内容[Enc(Ku_n+1, CPS_Unit#n′)]322，执行利用单元密钥[Ku_n]的解密处理（例如 AES_D）。在步骤 S456 中，执行必要的解码操作，例如 MPEG 解码、压缩/解压缩或解扰，以获取内容 350。

通过该处理，可以对作为存储在本地存储装置 320 中的作为随后生成的数据的加密后的子内容[Enc(Ku_n+1, CPS_Unit#n′)]322 进行解密以便使用，即以便再现。

这样一来，当在与随后生成的数据相对应的 CPS 单元密钥被预先存储在信息记录介质上的情况下使用存储在本地存储装置上的随后生成的数据时，可以通过与以上参考图 9 描述的用于对存储在信息记录介质 100 上的与 CPS 单元相对应的加密后的子内容进行解密和再现的处理序列相同的处理序列来执行随后生成的数据的解密和再现。

[（3.5）用于获取、记录和使用随后生成的数据的处理序列]

在上文中，已描述了用于每种绑定类型的处理序列。但是，实际上，信息处理器顺序获取各种绑定类型的随后生成的数据以作为随后生成的数据，并将它们记录到诸如硬盘这样的本地存储装置上，或者使用它们。在这种情况下，信息处理器将识别绑定类型并根据识别出的绑定类型来执行处理。

参考图 19 和 20 的流程图，现将描述用于识别绑定类型、根据识别结果来获取和记录随后生成的数据以及使用存储在本地存储装置上的随后生成的数据的处理序列，该处理序列是在信息处理器中执行的。

首先，参考图 19 的流程图，现将描述用于获取和记录随后生成的数据的处理序列。注意，该处理是由其驱动器中已加载有信息记录介质的信息处理器来执行的，所述信息记录介质存储了在被分段成 CPS 单元的同时被管理的内容，即以上参考图 1 所描述的其上记录了诸如加密后的内容 111 和 MKB 112 之类的各种数据的记录介质。

首先，信息处理器与提供随后生成的数据的服务器执行相互认证处理。例如，采用根据公钥加密系统的认证、利用口令的认证之类的来作为认证模式。当认证不成功时，后续处理中断。当认证成功时，处理前进到步骤 S502，在该步骤中信息处理器从加载的信息记录介质读取卷 ID 和下载信息，并且在步骤 S503 中将这些信息发送（上载）到步骤器。服务器搜索与这些卷 ID 和下载信息相对应的随后生成的数据集合。当没有相应的随后生成的数据时，服务器向信息处理器发送指示没有相应数据的消息。当信息处理器接收到该消息时（步骤 S504：否），信息处理器中断处理。

当在服务器内有相应的随后生成的数据时，在步骤 S505 中，信息处理器接收（下载）相应的随后生成的数据。注意，所接收到的数据基本上包括作为随后生成的数据的加密后的子内容、CPS 单元密钥文件和 UR（UR）。但是，当信息处理器要接收存储在信息记录介质上的 CPS 单元密钥对其适用的随后生成的数据时，可能存在只有加密后的子内容被发送的情况。

一旦接收到来自服务器的数据，在步骤 S506 中，信息处理器计算卷唯一密钥[Ke]。正如以上参考图 9 等所述，卷唯一密钥是通过基于介质密钥[Km]和从信息记录介质获取的卷 ID 的密钥生成处理来生成的，所述介质密钥[Km]是通过利用存储在信息处理器的存储器中的设备密钥从 MKB 获取的。

接下来，在步骤 S507 中，利用卷唯一密钥[Ke]对作为从服务器接收到的 CPS 单元密钥文件的构成数据的加密后的单元密钥进行解密，所述 CPS 单元密钥文件也就是例如：

CPS 单元密钥文件[Enc(Ke, f(Ku_n+1, UR#n+1))]。

此外，在步骤 508 中，通过参考从服务器获取的使用规则（UR），检查随后生成的数据的绑定类型。如果随后生成的数据的绑定类型是盘绑定型（步骤 S509：是），则执行步骤 S514 的处理。如果随后生成的数据的绑定类型是设备绑定型（步骤 S510：是），则执行步骤 S513 的处理。如果随后生成的数据的绑定类型是封装绑定型（步骤 S511：是），则执行步

骤 S512 的处理。

步骤 S512 是用于生成与封装绑定型随后生成数据相对应的加密后的绑定单元密钥的处理步骤。正如以上参考图 14 和 15 所描述的，该处理生成包含封装 ID[PID]的加密后的绑定单元密钥，例如：

加密后的绑定单元密钥[Enc(Ke, f(Ku_n+1, UR#n+1, PID))]。

步骤 S513 是用于生成与设备绑定型随后生成数据相对应的加密后的绑定单元密钥的处理步骤。正如以上参考图 6 和 7 所描述的，该处理生成包含设备密钥[Kd]的加密后的绑定单元密钥，例如：

加密后的绑定单元密钥[Enc(Ke, f(Ku_n+1, UR#n+1, Kd))]。

步骤 S514 是用于生成与盘绑定型随后生成数据相对应的加密后的绑定单元密钥的处理步骤。正如以上参考图 11 和 12 所描述的，该处理生成包含盘序列号[SN]的加密后的绑定单元密钥，例如：

加密后的绑定单元密钥[Enc(Ke, f(Ku_n+1, UR#n+1, SN))]。

当绑定类型不与以上任何一个相对应时，不执行绑定单元密钥的生成。例如，这对应于以上参考图 17 所描述的处理情况：与随后生成的数据相对应的 CPS 单元密钥被预先存储在信息记录介质上。

当不必生成绑定单元密钥时，或者在已经执行了步骤 S512 至 S514 的处理中的任何一个之后，处理前进到步骤 S515，在该步骤中，所生成的加密后的绑定单元密钥、来自服务器的作为随后生成的数据的加密后的子内容以及使用规则被记录到本地存储装置上，并且处理结束。

接下来，将参考图 20 描述用于使用记录在本地存储装置上的随后生成的数据的处理。注意，该处理也是由其驱动器中已加载有信息记录介质的信息处理器来执行的，所述信息记录介质存储了在被分段成 CPS 单元的同时被管理的内容，即以上参考图 1 所描述的其上记录了诸如加密后的内容 111 和 MKB 112 之类的各种数据的记录介质。

首先，在步骤 S601 中，信息处理器计算卷唯一密钥[Ke]。正如以上参考图 10 等所述，卷唯一密钥是通过基于介质密钥[Km]和从信息记录介质获取的卷 ID 的密钥生成处理来生成的，所述介质密钥[Km]是通过利用存储在信息处理器的存储器中的设备密钥从 MKB 获取的。

接下来，在步骤 S602 中，利用生成的卷唯一密钥[Ke]执行记录在本地存储装置上的加密后的绑定单元密钥的解密。加密后的绑定单元密钥是盘绑定型、设备绑定型和封装绑定型中的一种类型的，即，是以下加密后的绑定单元密钥之一：

加密后的绑定单元密钥[Enc(Ke, f(Ku_n+1, UR#n+1, SN))]；

加密后的绑定单元密钥[Enc(Ke, f(Ku_n+1, UR#n+1, Kd))]；以及

加密后的绑定单元密钥[Enc(Ke, f(Ku_n+1, UR#n+1, PID))]。

接下来，在步骤 S603 中，通过参考从服务器获取的使用规则（UR），检查要使用的随后生成的数据的绑定类型。注意，正如以上参考图 5Bc 所描述的，在本地存储装置中的每个随后生成的数据的绑定类型被记录在本地存储装置中被设置为记录文件的随后生成数据搜索信息集合中的配置中，可以通过参考随后生成数据搜索信息来检查要使用的随后生成的数据的绑定类型。

如果随后生成的数据的绑定类型是盘绑定型（步骤 S604：是），则执行步骤 S608 的处理。如果随后生成的数据的绑定类型是设备绑定型（步骤 S605：是），则执行步骤 S609 的处理。如果随后生成的数据的绑定类型是封装绑定型（步骤 S606：是），则执行步骤 S610 的处理。

步骤 S608 是通过对与盘绑定型随后生成数据相对应的加密后的绑定单元密钥的解密来生成单元密钥的处理步骤。在该处理中，正如以上参考图 13 所描述的，在利用卷唯一密钥[Ke]对例如：

加密后的绑定单元密钥[Enc(Ke, f(Ku_n+1, UR#n+1, SN))]

进行解密之后，通过经由基于从服务器获取的使用规则[UR#n+1]和从信息记录介质读取的序列号[SN]的计算的解除绑定处理来计算单元密钥[Ku_n+1]，然后对从服务器获取的并且被记录在本地存储装置上的作为随后生成的数据的加密后的子内容 Enc(Ku_n+1, CPS_Unit#n+1)进行解密。

步骤 S609 是通过对与设备绑定型随后生成数据相对应的加密后的绑定单元密钥的解密来生成单元密钥的处理步骤。在该处理中，正如以上参考图 9 所描述的，在利用卷唯一密钥[Ke]对例如：

加密后的绑定单元密钥[Enc(Ke, f(Ku_n+1, UR#n+1, Kd))]

进行解密之后，通过经由基于从服务器获取的使用规则[UR#n+1]和从信息处理器的存储器获取的设备密钥[Kd]的计算的解除绑定处理来计算单元密钥[Ku_n+1]，然后对从服务器获取的并且被记录在本地存储装置上的作为随后生成的数据的加密后的子内容 Enc(Ku_n+1, CPS_Unit#n+1)进行解密。

步骤 S610 是通过对与封装绑定型随后生成数据相对应的加密后的绑定单元密钥的解密来生成单元密钥的处理步骤。在该处理中，正如以上参考图 13 所描述的，在利用卷唯一密钥[Ke]对例如：

加密后的绑定单元密钥[Enc(Ke, f(Ku_n+1, UR#n+1, PID))]

进行解密之后，通过经由基于从服务器获取的使用规则[UR#n+1]和从信息记录介质读取的封装 ID[PID]的计算的解除绑定处理来计算单元密钥[Ku_n+1]，然后对从服务器获取的并且被记录在本地存储装置上的作为随后生成的数据的加密后的子内容 Enc(Ku_n+1, CPS_Unit#n+1)进行解密。

在上述处理步骤中的任何一个之后，在步骤 S611 中，内容被再现。注意，当随后生成的数据不与以上绑定类型中的任何一种相对应时，可以通过利用存储在信息记录介质上的 CPS 单元密钥执行解密处理，从而来执行再现。

虽然在上述实施例中，随后生成的数据是从服务器获取的，但是在随后生成的数据是经由除服务器外的其他存储介质（例如 DVD）获取的情况下，也可执行相同的处理。此外，由信息处理器生成的随后生成的数据也可以被记录到本地存储装置上，以便通过相同处理使用。

[4. 信息处理器的配置示例]

接下来，参考图 21，将描述对内容执行上述记录和再现的信息处理器的配置示例。

图 21 所示的信息处理器 900 具有：驱动器 909，用于驱动信息记录介质 910 执行记录和再现信号的数据的输入/输出：CPU 907，作为用于根据各种程序执行数据处理的控制装置；ROM 906，作为程序、参数等的存储区域；存储器 908；输入/输出 I/F 902，用于输入/输出数字信号；输入/输出 I/F 903，用于输入/输出模拟信号，输入/输出 I/F 903 具有 A/D、D/A 转

换器 904；MPEG 编解码器 921，用于执行 MPEG 数据的编码/解码处理；TS/PS 处理装置 922，用于执行 TS（传输流）/PS（程序流）处理；密码处理装置 905，用于执行各种加密处理；以及存储装置 930，作为本地存储装置，例如硬盘。各个块连接到总线 901。

当信息处理器 900 要执行来自信息记录介质 910 的包括 MPEG-TS 数据的 AV 流数据的再现时，被从信息记录介质 910 读取到驱动器 909 中的数据按照密码处理装置 905 的要求被解密，并且被 TS/PS 处理装置 922 划分成相应的数据，例如视频、音频和字幕。

此外，被 MPEG 编解码器 921 解密的数字数据被输入/输出 I/F 902 中的 D/A 转换器 904 转换成模拟信号，并被输出。此外，当执行数字输出时，被密码处理装置 905 解密的 MPEG-TS 数据作为数字数据经由输入/输出 I/F 902 输出。在这种情况下，输出是对数字接口进行的，所述数字接口例如是 IEEE 1394、以太网电缆、无线 LAN 等等。注意，当支持网络连接功能时，输入/输出 I/F 902 配备有用于功能连接的功能。

此外，在数据在经历信息处理器 900 中的转换而被转换成允许它被输出目的地设备重复的格式之后被输出的情况下，速率转换处理和编解码转换处理被 MPEG 编解码器 921 临时应用在被 TS/PS 处理装置 922 分割的相应的视频、音频、字幕等数据上，然后同样由 TS/PS 处理装置 922 多路复用为 MPEG-TG 或 MPEG-PS 的数据被从数字输入/输出 I/F 902 输出。或者，在 CPU 907 的控制下，执行到除 MPEG 或多路复用文件之外的其他编解码器的转换，以便从数字输入/输出 I/F 902 输出。

诸如作为 CPS 单元管理数据的使用规则这样的管理数据在被从信息记录介质 910 读取之后，被保存在存储器 908 中。在执行再现时必需的每个 CPS 单元的密钥信息可以从保存在存储器中的数据获取。

随后生成数据的数据，例如信息处理器 900 生成或获取的数据，被记录在存储装置 930（例如硬盘）上。通过合并应用构建虚拟文件系统，并且与从记录介质读取的内容一起执行再现处理。

接下来，将描述用于记录随后生成数据的数据的操作，例如由信息处理器 900 生成或获取的数据。对于要记录的数据，可以设想两种情况，即

数字信号被输入的情况和模拟信号被输入的情况。在数字信号的情况下，数字信号从输入/输出 I/F 902 输入，并且根据需要被密码处理装置 905 执行了适当的加密处理的数据被存储到信息记录介质 910 或存储装置 930 上。

由信息处理器 900 等生成或获取的随后生成的数据被记录在存储装置 930（例如硬盘）上。加密后的绑定单元密钥、使用规则等被进一步记录在存储装置 930 上。

当输入数字信号要其数据格式被转换之后要被存储时，输入数字信号被 MPEG 编解码器 921、CPU 907 和 TS/PS 处理装置 922 转换成用于存储的数据格式。然后，所得到的数据经历密码处理装置 905 进行的适当的加密处理，并被存储到信息记录介质 910 上。在模拟信号的情况下，输入到输入/输出 I/F 903 的模拟信号被 A/D 转换器 904 转换成数字信号，并且被 MPEG 编解码器 921 转换成记录时使用的编解码器。

然后，所得到的数据被 TS/PS 处理装置转换成作为记录数据格式的 AV 多路复用数据，并且根据需要被密码处理装置 905 执行了适当加密处理的数据被存储到信息记录介质 910 上。

当要经由信息处理器外部的网络获取信息处理器 900 所需的信息时，所获取的数据被临时存储到信息处理器 900 中的存储器 908 中。要存储的数据的示例包括内容再现所必需的密钥信息、要与内容再现同时再现的字幕、诸如音频或静止图片之类的数据以及内容管理信息。

随后生成或获取的数据被临时存储到存储器 908 中，并通过用户选择或根据预定控制序列被存储到存储装置 930（例如硬盘）上。

注意，用于执行再现或记录处理的程序被存储在 ROM 906 中。在程序被执行的同时，存储器 908 被用作参数和数据的存储和工作区域。虽然图 21 示出了启用数据记录和再现的设备配置，但是也可以配置只具有再现功能的设备或只具有记录功能的设备。本发明也可以应用到这些种类的设备。

以上已经通过本发明的特定实施例的方式详细描述了本发明。但是，很明显，本领域的技术人员可以对本发明进行各种改变或替换，而不会脱

离本发明的范围。即，本发明只是以示例方式公开的，从而不应当被限制性地解释。本发明的范围应当由所附权利要求书确定。

例如，虽然在实施例中设备绑定型（图 6 和 7）、盘绑定型（图 12 和 13）以及封装绑定型（图 14 和 15）被分开描述，但是设备绑定型和盘绑定型也可以与彼此组合以形成设备/盘绑定型，或者，可以采用设备/封装绑定型。即，具体而言，当绑定类型是设备/盘绑定型时，只能通过使用用于获取随后生成的数据的盘和用于获取随后生成的数据的设备的组合来执行再现。因此，即使存储在设备上的随后生成的数据被复制到另一再现设备上，数据再现也不能被执行，这是因为存储在设备上并用于绑定的信息（在本实施例中是设备密钥）是不同的，从而使得能够进行更严格的再现管理。注意，在这种情况下，利用预留的区域，上述设备/盘绑定和设备/封装绑定可以被添加到图 5A 所示的绑定类型。注意，在图 7 所示的步骤 S124 中和图 21 所示的步骤 S214 中的绑定处理中，设备/盘绑定可以通过利用设备密钥和序列号执行异或运算来实现，而设备/封装绑定可以通过利用设备密钥和封装 ID 号执行异或运算来实现。

注意，本说明书中描述的一系列处理可以由硬件或软件执行，或者由两者的合成结构执行。软件处理可以通过将其中记录了处理序列的程序安装到结合在专用硬件中的计算机的存储器中并且执行该程序来执行，或者通过将程序安装到能够执行各种处理的通用计算机上并且致使该计算机执行该程序来执行。

例如，程序可以被预先存储在作为记录介质的硬盘或 ROM（只读存储器）上。或者，程序可以被临时或永久地存储（记录）在可移除记录介质上，例如软盘、CD-ROM（高密盘只读存储器）、MO（磁光）盘、DVD（数字多功能盘）、磁盘或半导体存储器。这种可移除记录介质可以以所谓的软件包的形式来提供。

注意，除了如上所述的从可移除记录介质安装到计算机上之外，程序还可以从下载站点以无线方式传送到计算机，或者可以经由网络（例如 LAN（局域网）或以太网）以有线方式传送到计算机；这样传送的程序可以被计算机接收，以便被安装到内置的记录介质（例如硬盘）中。

注意，本说明书中描述的各种处理不仅可以被按所描述的时间顺序执行，还可以根据需要被并行地或独立地执行，这取决于执行处理的设备的吞吐量。此外，本说明书中使用的术语“系统”是指多个设备的逻辑集合结构，并且每个结构的设备不一定存在于同一外壳内。

如上所述，根据本发明的实施例，当将随后生成的数据，例如用户随后利用存储在信息记录介质上的信息来生成或下载的信息，记录到诸如硬盘或可移除介质之类的本地存储装置上时，作为随后生成的数据的加密密钥的单元密钥作为绑定到从信息处理器获取的密钥信息或从信息记录介质获取的标识信息的数据被生成，并且以加密后的形式被记录。从而，要使用记录在本地存储装置上的随后生成的数据，则需要解除绑定处理。解除绑定处理要求以下条件。即，例如在设备绑定型随后生成数据的情况下，要求要使用随后生成的数据的信息处理器是与执行记录的信息处理器相同的信息处理器；例如在盘绑定型随后生成数据的情况下，要求与记录随后生成的数据时使用的相同的盘被加载到信息处理器中；例如在封装绑定型随后生成数据的情况下，要求信息处理器被加载以与记录随后生成的数据时使用的盘具有相同封装 ID 的盘。因此，可以以各种方式实现随后生成的数据的使用限制。

本发明包含与 2005 年 4 月 11 日在日本专利局递交的日本专利申请 JP 2005-113035 相关的主题，这里通过引用将其全部内容结合进来。

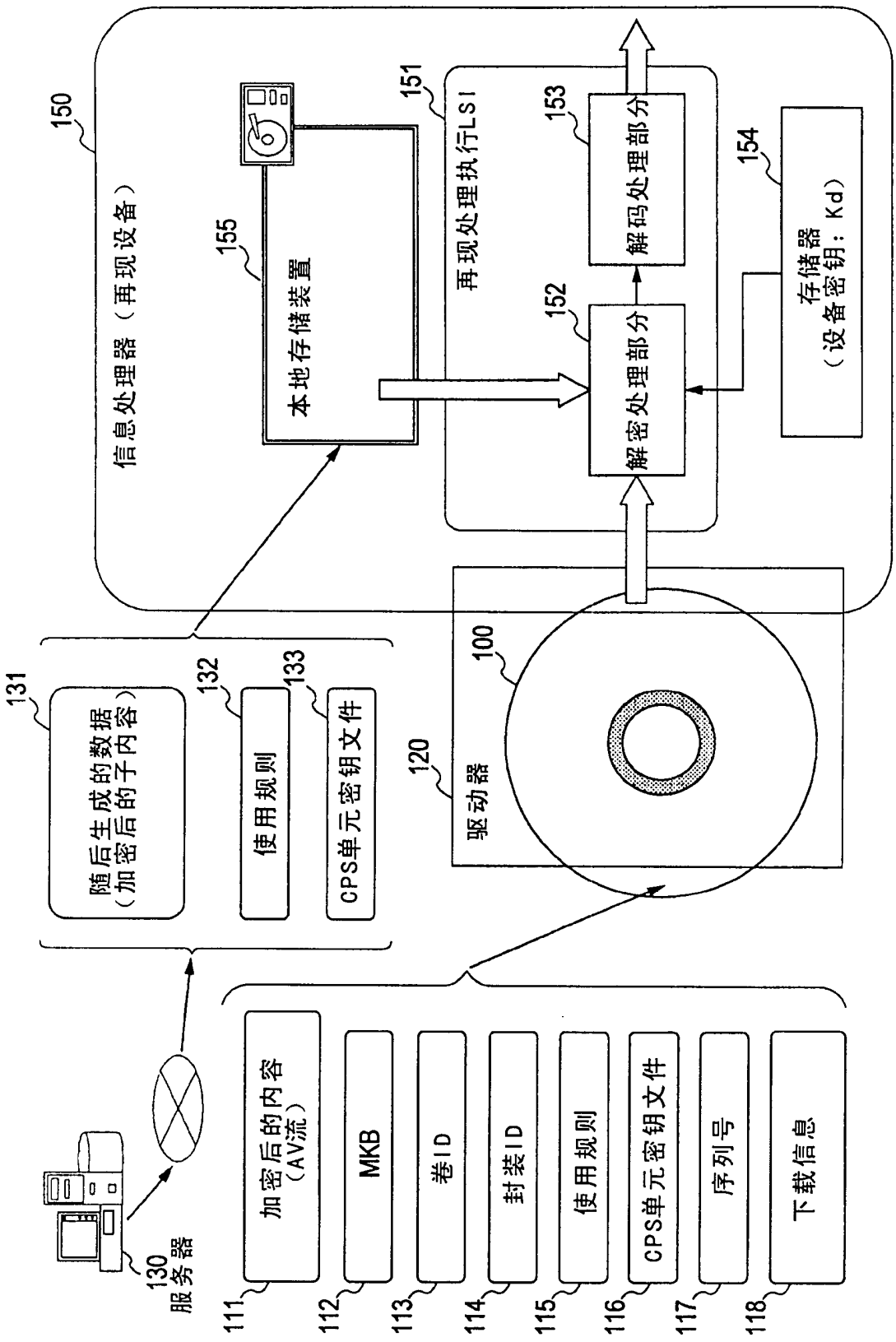

150
信息处理器（再现设备）
155
本地存储装置
151
再现处理执行LSI
153
解码处理部分
154
存储器
（设备密钥：Kd）
152
解密处理部分
131
随后生成的数据
（加密后的子内容）
132
使用规则
133
CPS单元密钥文件
120
驱动器
100
130
服务器
111
加密后的内容
（AV流）
112
MKB
113
卷ID
114
封装ID
115
使用规则
116
CPS单元密钥文件
117
序列号
118
下载信息

图1

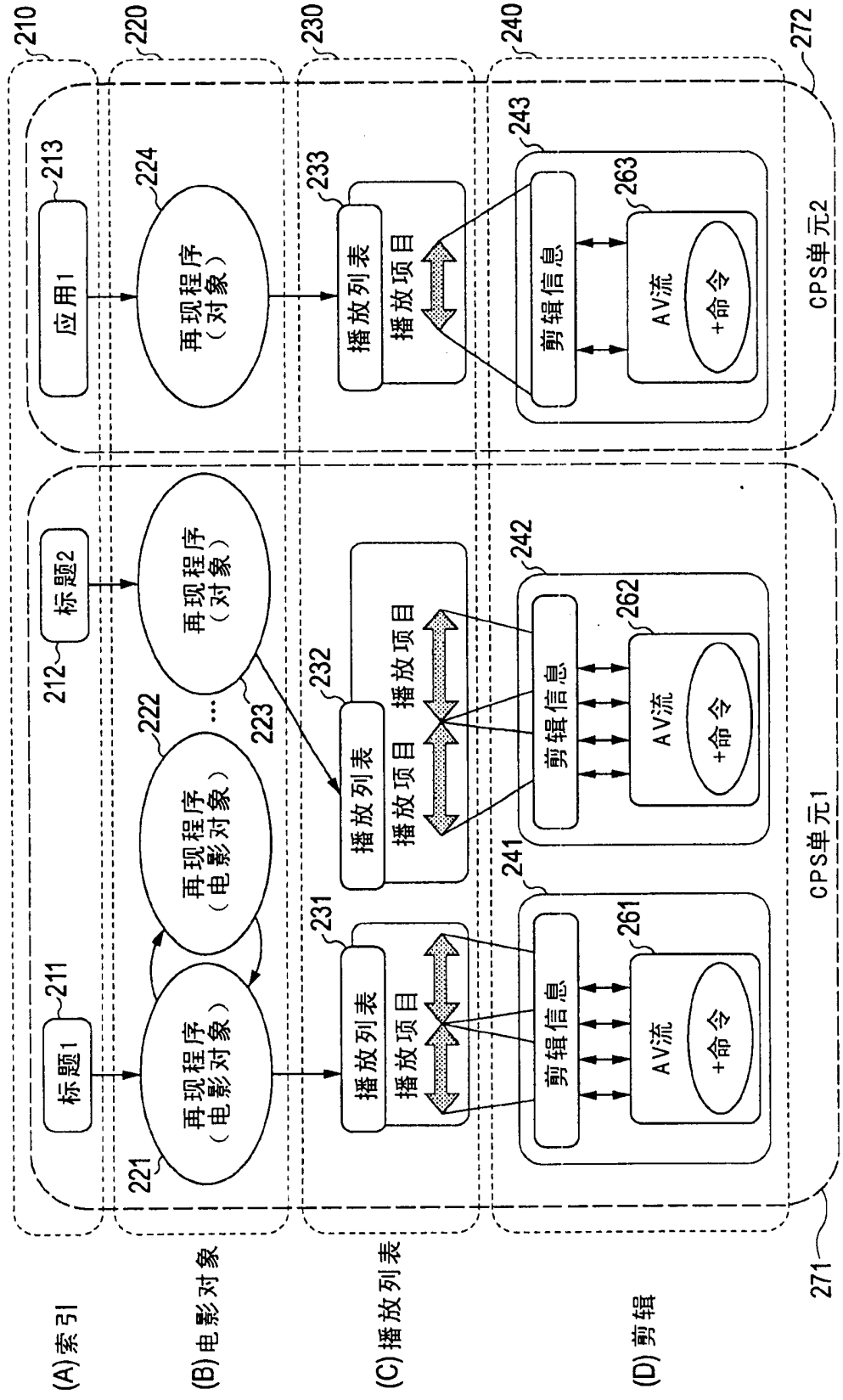

(A)索引
(B)电影对象
(C)播放列表
(D)剪辑
标题1
标题2
应用1
再现程序（电影对象）
再现程序（电影对象）
再现程序（对象）
再现程序（对象）
播放列表
播放项目
播放项目
播放列表
播放项目
剪辑信息
剪辑信息
剪辑信息
AV流
+命令
AV流
+命令
AV流
+命令
CPS单元1
CPS单元2
210
211
212
213
220
221
222
223
224
230
231
232
233
240
241
242
243
261
262
263
271
272

图2

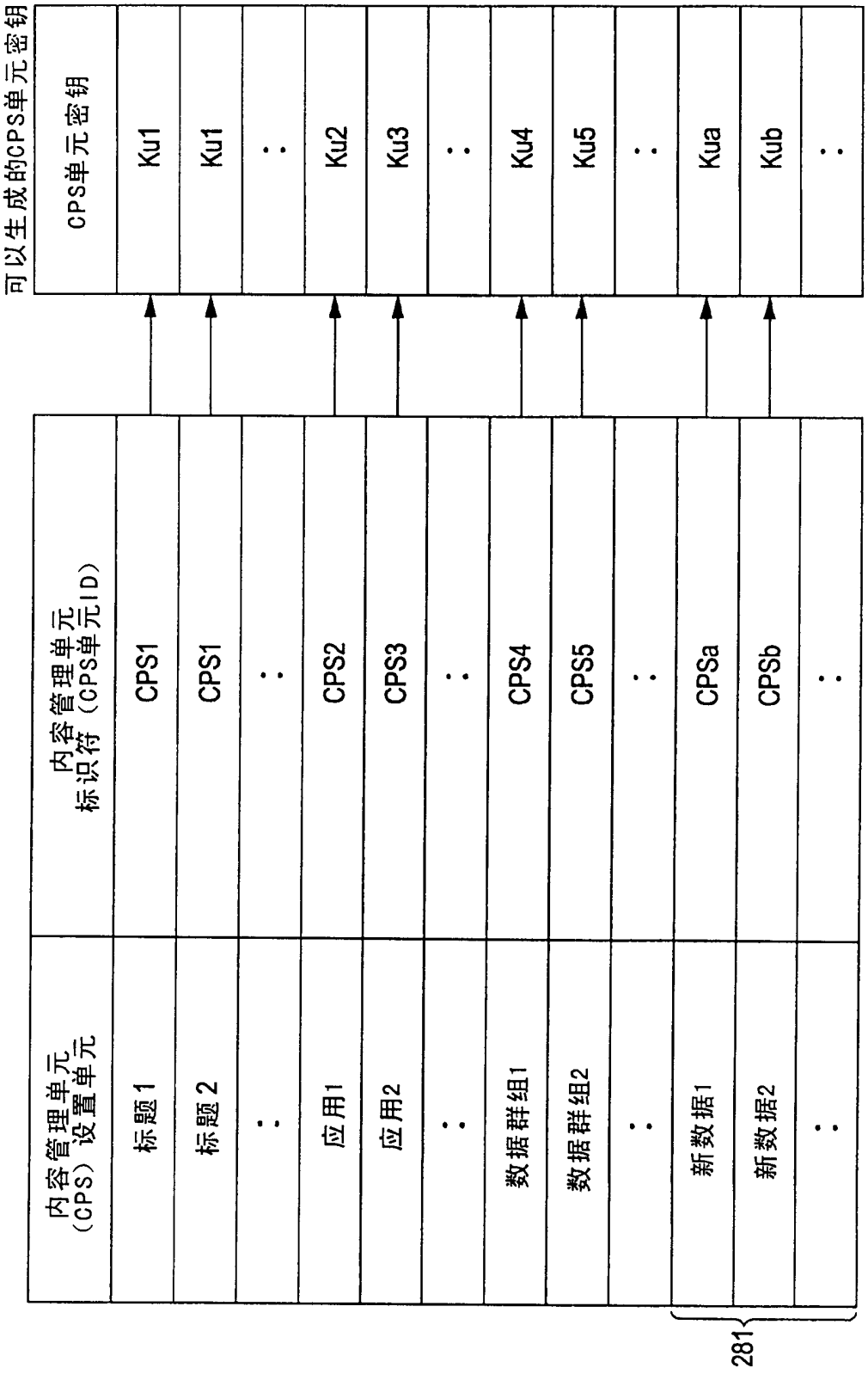

可以生成的CPS单元密钥
CPS单元密钥
Ku1
Ku1
:
Ku2
Ku3
:
Ku4
Ku5
:
Kua
Kub
:
内容管理单元
标识符（CPS单元ID）
CPS1
CPS1
:
CPS2
CPS3
:
CPS4
CPS5
:
CPSa
CPSb
:
内容管理单元
（CPS）设置单元
标题1
标题2
:
应用1
应用2
:
数据群组1
数据群组2
:
新数据1
新数据2
:
281

图3

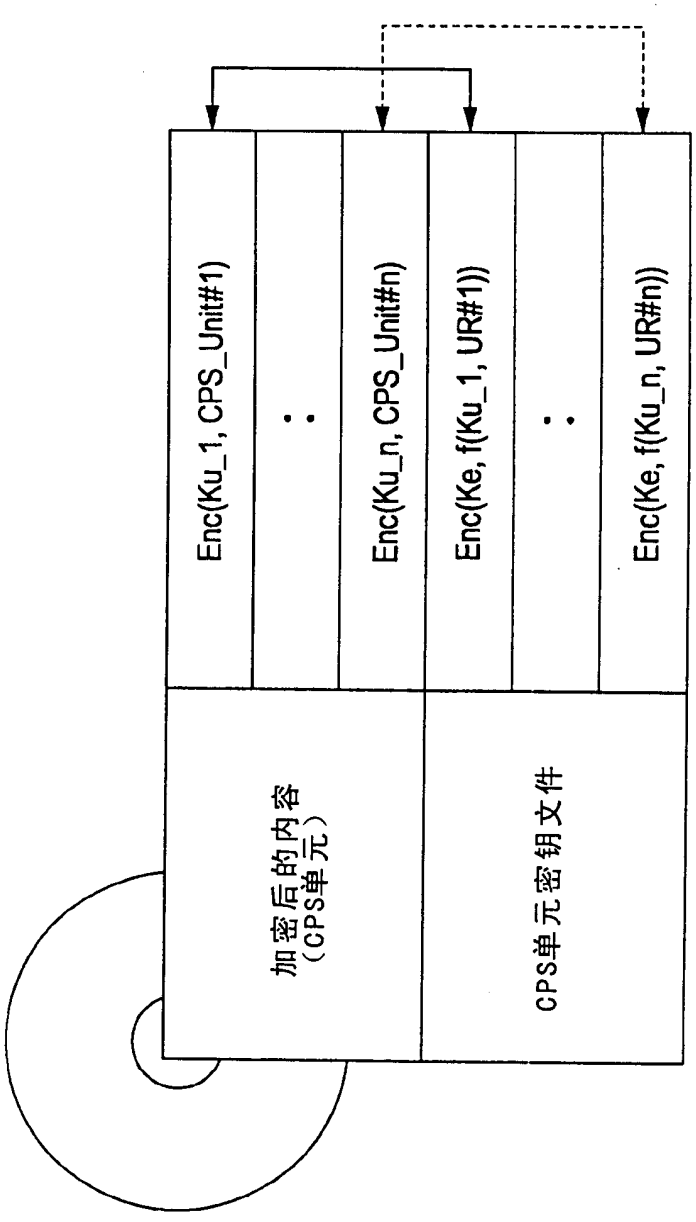

Enc(Ku_1, CPS_Unit#1)
Enc(Ku_n, CPS_Unit#n)
Enc(Ke, f(Ku_1, UR#1))
Enc(Ke, f(Ku_n, UR#n))
加密后的内容
（CPS单元）
CPS单元密钥文件

图4

（绑定类型代码值示例：8位）	
代码	绑定类型
01h	设备绑定
02h	盘序号绑定
03h	封装绑定
04h	未绑定
05-FFh	预留以供私用

图5A

在每CPS单元基础上进行指定
以写入到使用规则的情况（XML表达式）

```
<cci_info type="BindingInfo">
  <cci_value type="Binding" data="01"/>
</cci_info>
```

图5Ba

在每CPS单元基础上进行指定以写入
到使用规则的情况（二进制表达式）

```
CCI_Info Binding(){
  Binding type          8bits
  reserved              8bits
}
```

图5Bb

在逐文件基础上进行指定以写入到除使用规则或访问许可/限制信息之外的文件的情况

[文件名称]	[绑定类型]	
BDMV/AUXDATA/sound.bdmv	"02"	(声音效果文件)
BDMV/STREAM/00001.m2ts	"01"	(AV流)
BDMV/AUXDATA/01000.otf	"03"	(字体文件)
BDMV/AUXDATA/studio1.dat	"0F"	(对工作室唯一的数据)

图5Bc

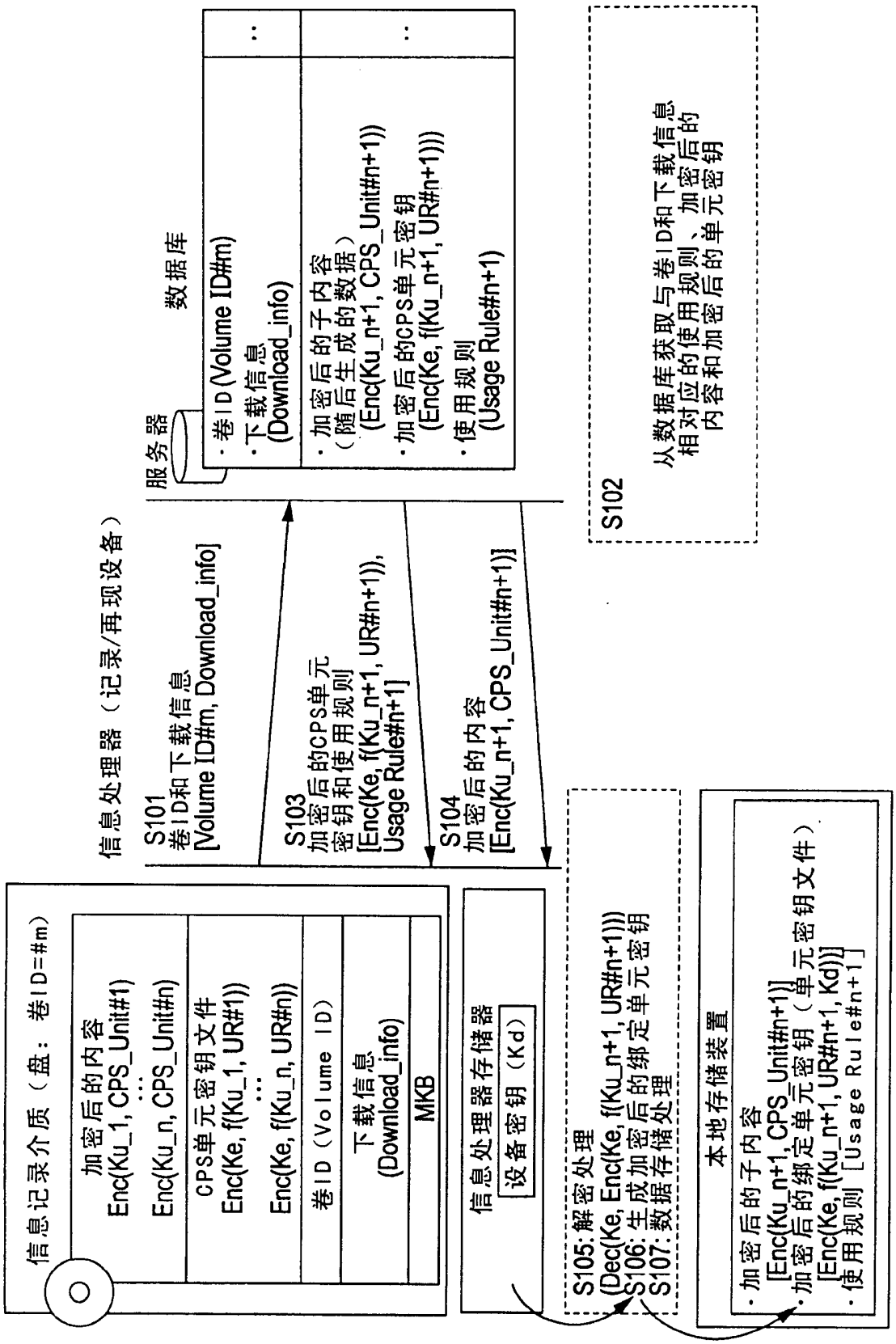

信息记录介质（盘：卷ID=#m）
加密后的内容
Enc(Ku_1, CPS_Unit#1)
…
Enc(Ku_n, CPS_Unit#n)
CPS单元密钥文件
Enc(Ke, f(Ku_1, UR#1))
…
Enc(Ke, f(Ku_n, UR#n))
卷ID（Volume ID）
下载信息
(Download_info)
MKB
信息处理器存储器
设备密钥（Kd）
信息处理器（记录/再现设备）
服务器
数据库
S101
卷ID和下载信息
[Volume ID#m, Download_info]
· 卷ID (Volume ID#m)
· 下载信息
(Download_info)
S103
加密后的CPS单元
密钥和使用规则
[Enc(Ke, f(Ku_n+1, UR#n+1)),
Usage Rule#n+1]
· 加密后的子内容
（随后生成的数据）
(Enc(Ku_n+1, CPS_Unit#n+1))
· 加密后的CPS单元密钥
(Enc(Ke, f(Ku_n+1, UR#n+1)))
· 使用规则
(Usage Rule#n+1)
S104
加密后的内容
[Enc(Ku_n+1, CPS_Unit#n+1)]
S102
从数据库获取与卷ID和下载信息
相对应的使用规则、加密后的
内容和加密后的单元密钥
S105: 解密处理
(Dec(Ke, Enc(Ke, f(Ku_n+1, UR#n+1)))
S106: 生成加密后的绑定单元密钥
S107: 数据存储处理
本地存储装置
· 加密后的子内容
[Enc(Ku_n+1, CPS_Unit#n+1)]
· 加密后的绑定单元密钥（单元密钥文件）
[Enc(Ke, f(Ku_n+1, UR#n+1, Kd))]
· 使用规则 [Usage Rule#n+1]

图6

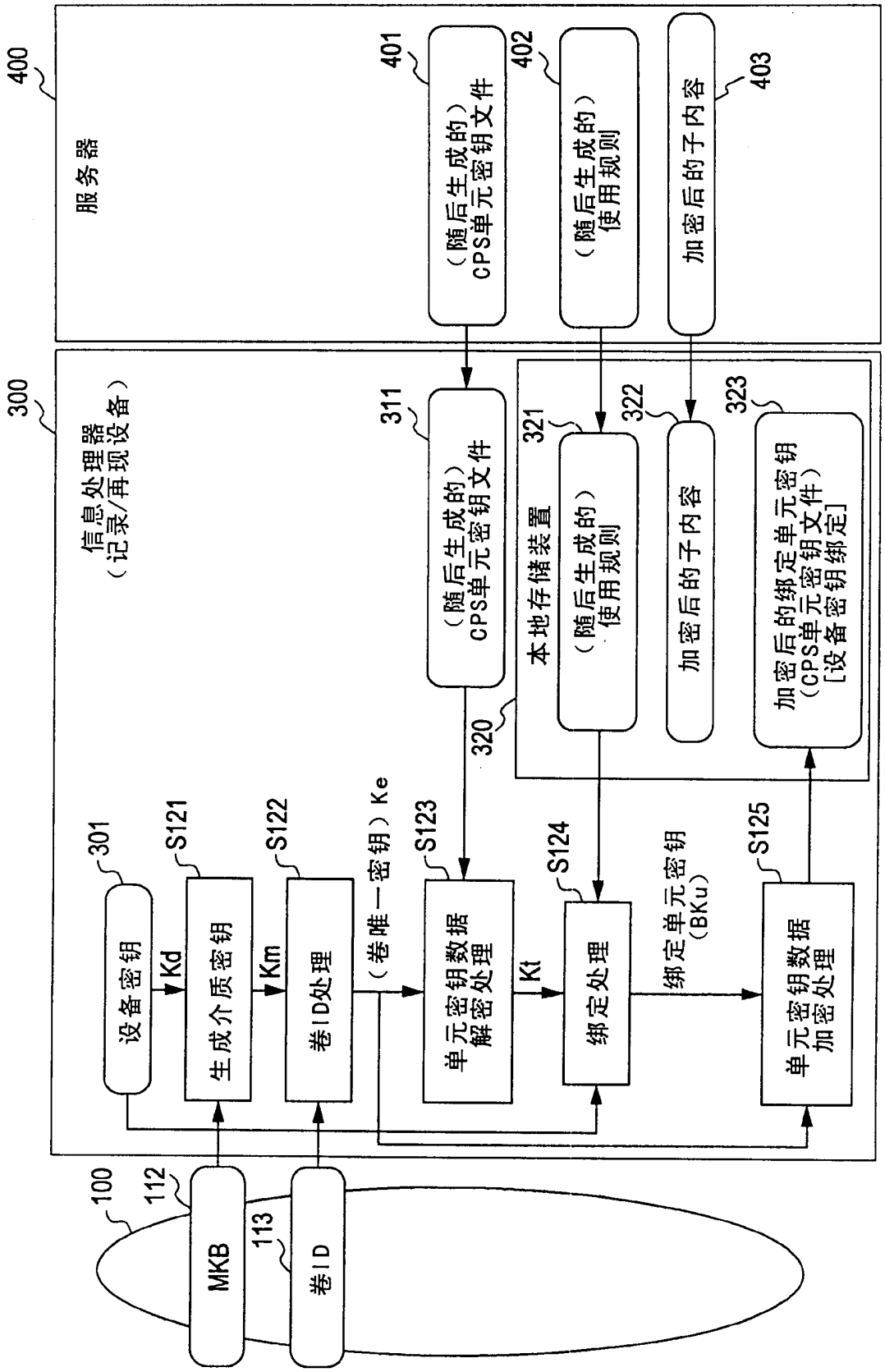

100
112
MKB
113
卷ID
301
设备密钥
S121
Kd
生成介质密钥
S122
Km
卷ID处理
（卷唯一密钥）Ke
S123
单元密钥数据
解密处理
Kt
S124
绑定处理
绑定单元密钥
（BKu）
S125
单元密钥数据
加密处理
300
信息处理器
（记录/再现设备）
311
（随后生成的）
CPS单元密钥文件
320
本地存储装置
321
（随后生成的）
使用规则
322
加密后的子内容
323
加密后的绑定单元密钥
（CPS单元密钥文件）
[设备密钥绑定]
400
服务器
401
（随后生成的）
CPS单元密钥文件
402
（随后生成的）
使用规则
403
加密后的子内容

图7

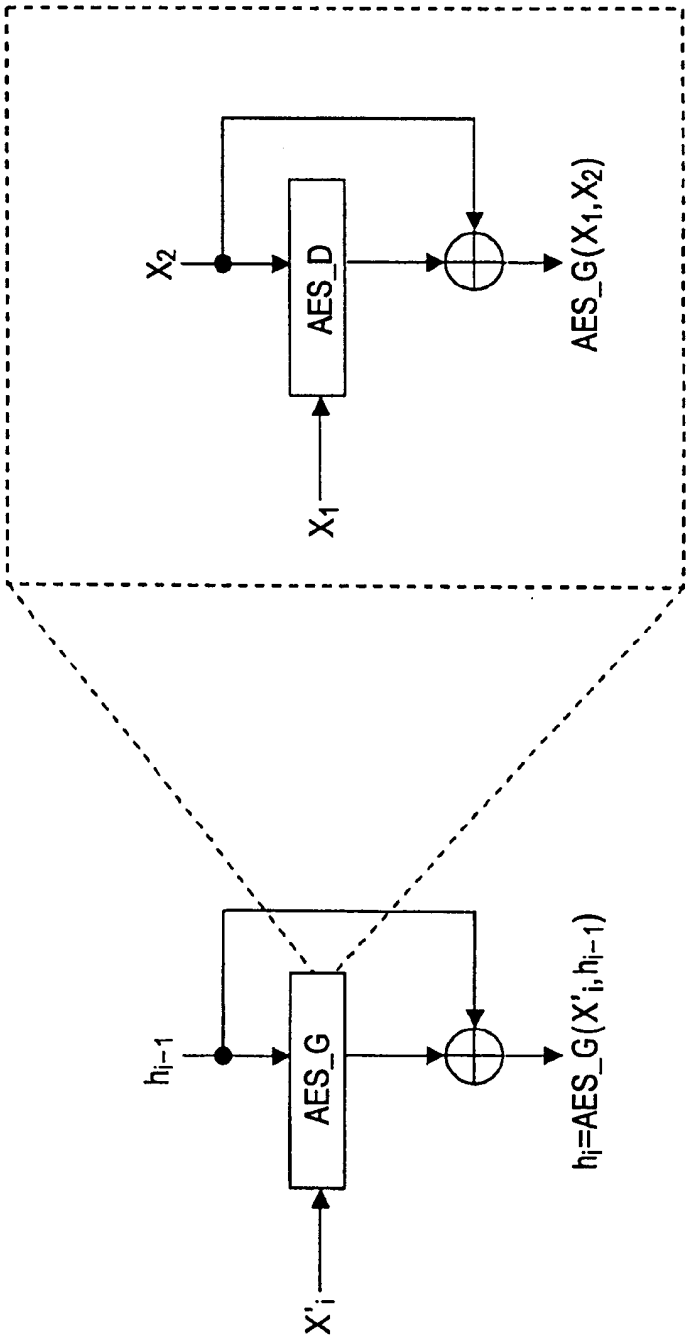


图8

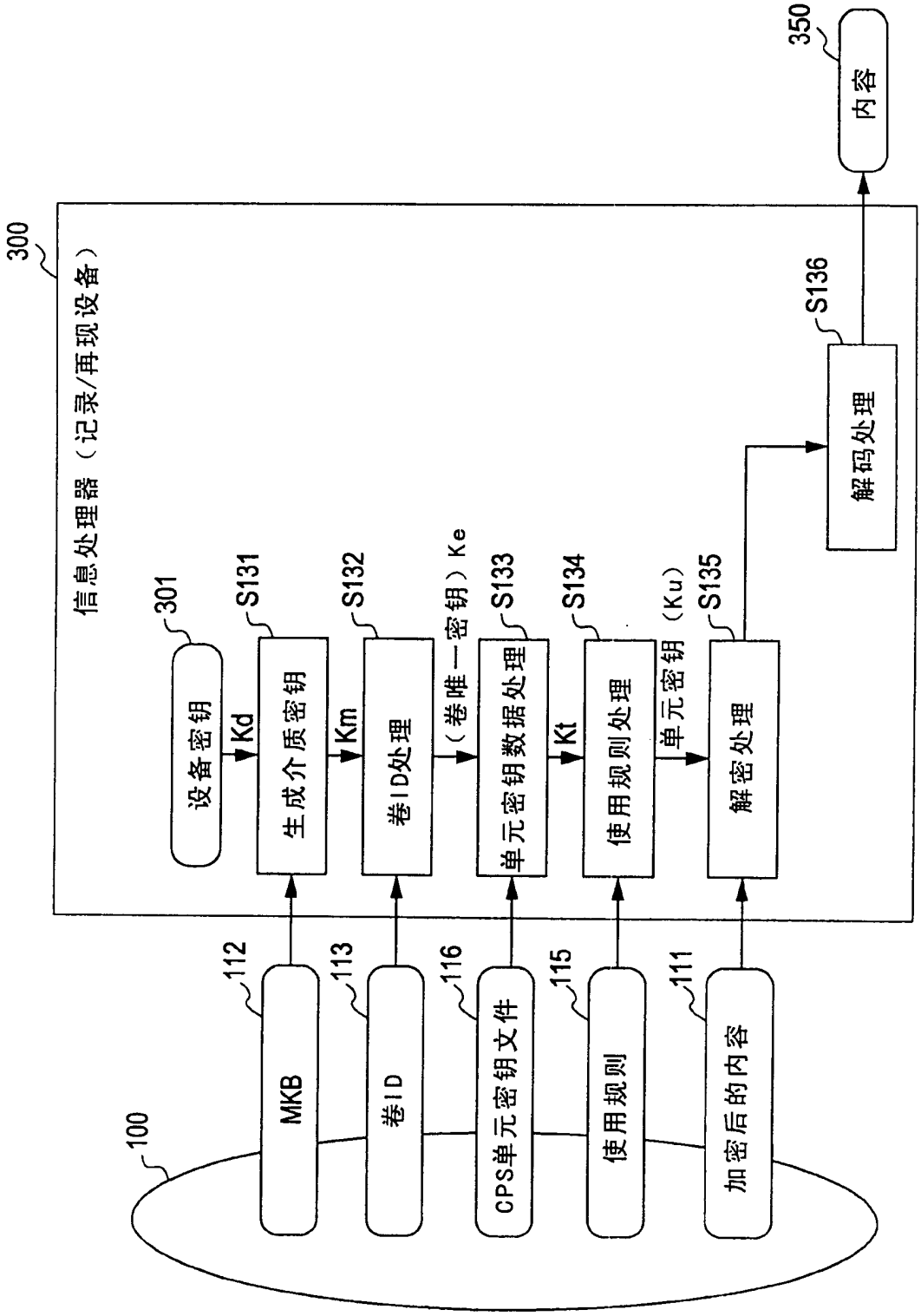

100
MKB
112
卷ID
113
CPS单元密钥文件
116
使用规则
115
加密后的内容
111
300
信息处理器（记录/再现设备）
301
设备密钥
S131
生成介质密钥
Kd
S132
Km
卷ID处理
（卷唯一密钥）Ke
S133
单元密钥数据处理
Kt
S134
使用规则处理
单元密钥（Ku）
S135
解密处理
S136
解码处理
350
内容

图9

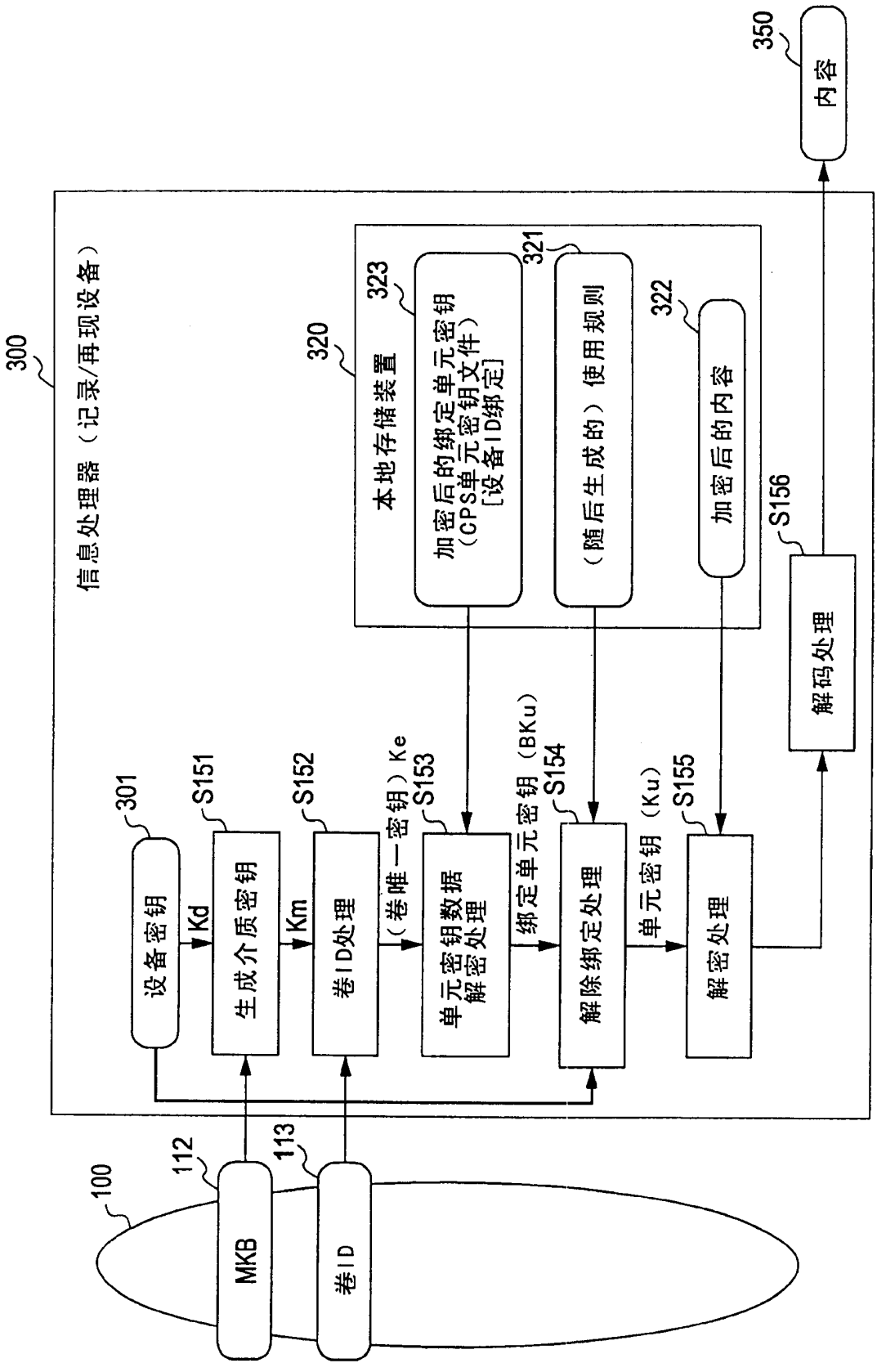

300
信息处理器（记录/再现设备）
320
本地存储装置
323
加密后的绑定单元密钥
（CPS单元密钥文件）
[设备ID绑定]
321
（随后生成的）使用规则
322
加密后的内容
350
内容
S156
解码处理
301
设备密钥
S151
Kd
生成介质密钥
Km
S152
卷ID处理
（卷唯一密钥）Ke
S153
单元密钥数据
解密处理
绑定单元密钥（BKu）
S154
解除绑定处理
单元密钥（Ku）
S155
解密处理
100
112
MKB
113
卷ID

图10

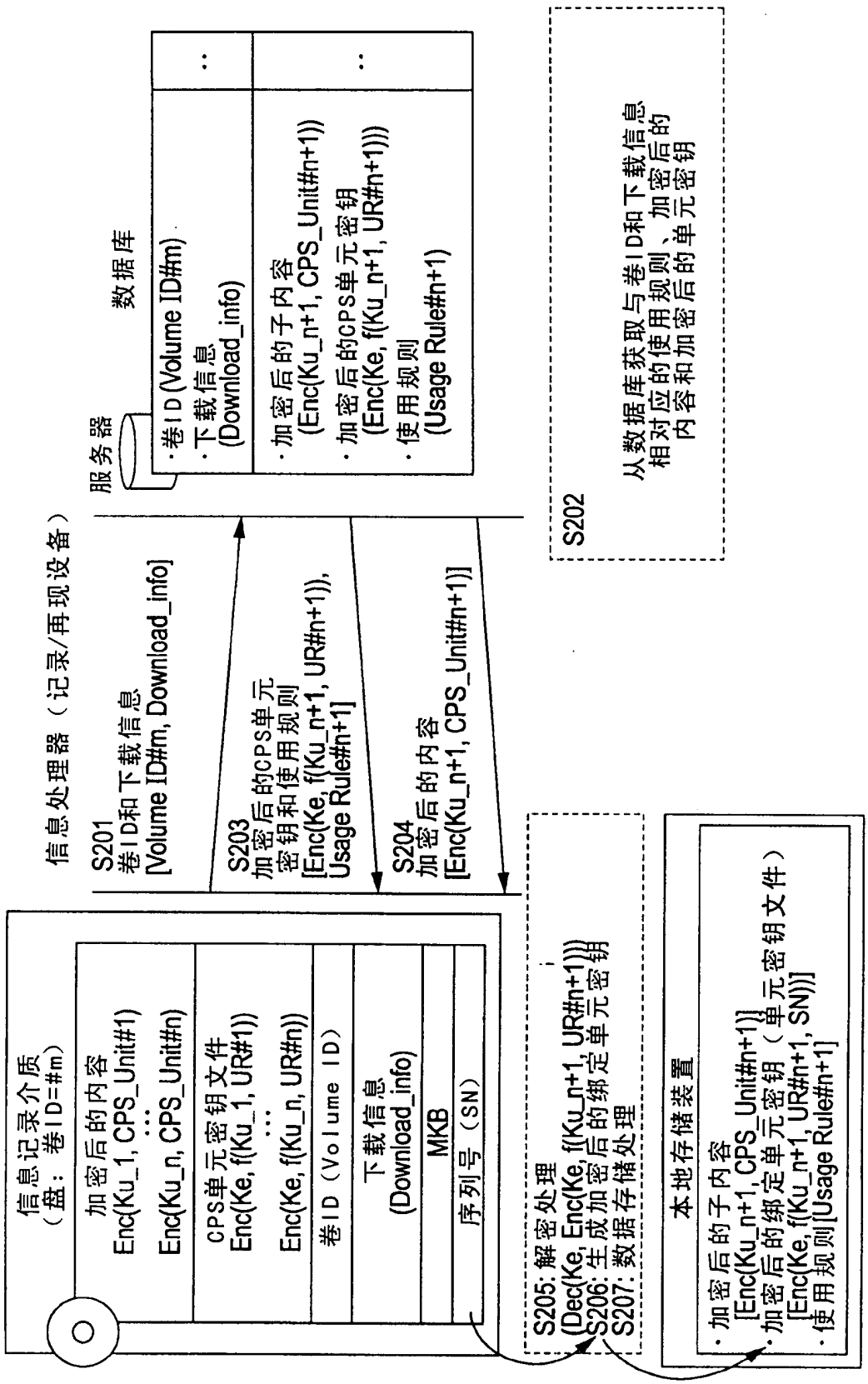

信息记录介质
（盘：卷ID=#m）
加密后的内容
Enc(Ku_1, CPS_Unit#1)
…
Enc(Ku_n, CPS_Unit#n)
CPS单元密钥文件
Enc(Ke, f(Ku_1, UR#1))
…
Enc(Ke, f(Ku_n, UR#n))
卷ID（Volume ID）
下载信息
(Download_info)
MKB
序列号（SN）
信息处理器（记录/再现设备）
S201
卷ID和下载信息
[Volume ID#m, Download_info]
服务器
数据库
·卷ID (Volume ID#m)
·下载信息
(Download_info)
S203
加密后的CPS单元
密钥和使用规则
[Enc(Ke, f(Ku_n+1, UR#n+1)),
Usage Rule#n+1]
·加密后的子内容
(Enc(Ku_n+1, CPS_Unit#n+1))
·加密后的CPS单元密钥
(Enc(Ke, f(Ku_n+1, UR#n+1)))
·使用规则
(Usage Rule#n+1)
S204
加密后的内容
[Enc(Ku_n+1, CPS_Unit#n+1)]
S202
从数据库获取与卷ID和下载信息
相对应的使用规则、加密后的
内容和加密后的单元密钥
S205: 解密处理
(Dec(Ke, Enc(Ke, f(Ku_n+1, UR#n+1))))
S206: 生成加密后的绑定单元密钥
S207: 数据存储处理
本地存储装置
·加密后的子内容
[Enc(Ku_n+1, CPS_Unit#n+1)]
·加密后的绑定单元密钥（单元密钥文件）
[Enc(Ke, f(Ku_n+1, UR#n+1, SN))]
·使用规则[Usage Rule#n+1]

图11

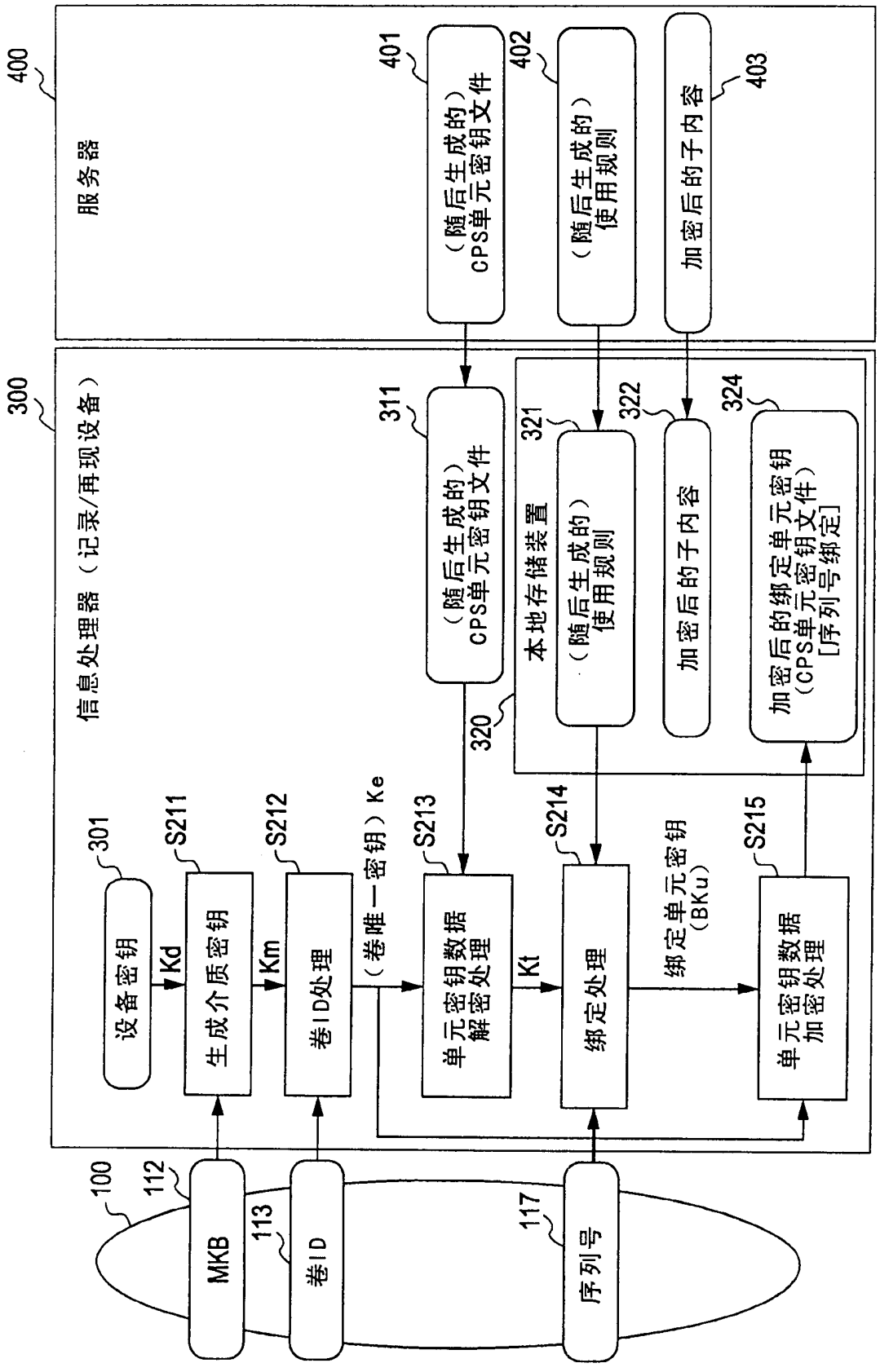

400
服务器
401
（随后生成的）
CPS单元密钥文件
402
（随后生成的）
使用规则
403
加密后的子内容
300
信息处理器（记录/再现设备）
311
（随后生成的）
CPS单元密钥文件
320
本地存储装置
321
（随后生成的）
使用规则
322
加密后的子内容
324
加密后的绑定单元密钥
（CPS单元密钥文件）
[序列号绑定]
301
设备密钥
S211
Kd
生成介质密钥
S212
Km
卷ID处理
（卷唯一密钥）Ke
S213
单元密钥数据
解密处理
Kt
S214
绑定处理
绑定单元密钥
（BKu）
S215
单元密钥数据
加密处理
100
112
MKB
113
卷ID
117
序列号

图12

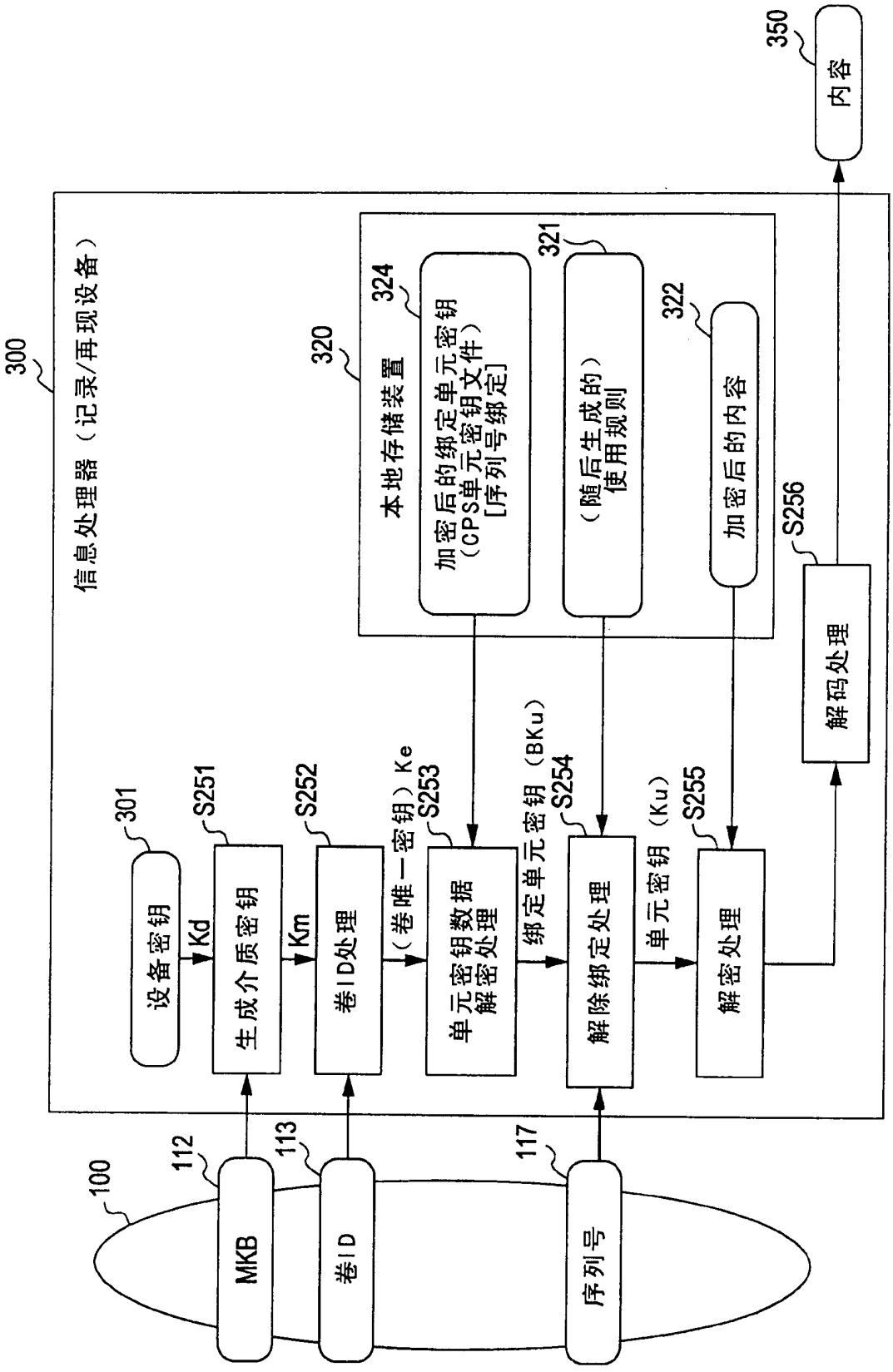

100
112
113
117
MKB
卷ID
序列号
300
信息处理器（记录/再现设备）
301
设备密钥
S251
Kd
生成介质密钥
Km
S252
卷ID处理
（卷唯一密钥）Ke
S253
单元密钥数据解密处理
绑定单元密钥（BKu）
S254
解除绑定处理
单元密钥（Ku）
S255
解密处理
320
本地存储装置
324
加密后的绑定单元密钥（CPS单元密钥文件）[序列号绑定]
321
（随后生成的）使用规则
322
加密后的内容
S256
解码处理
350
内容

图13

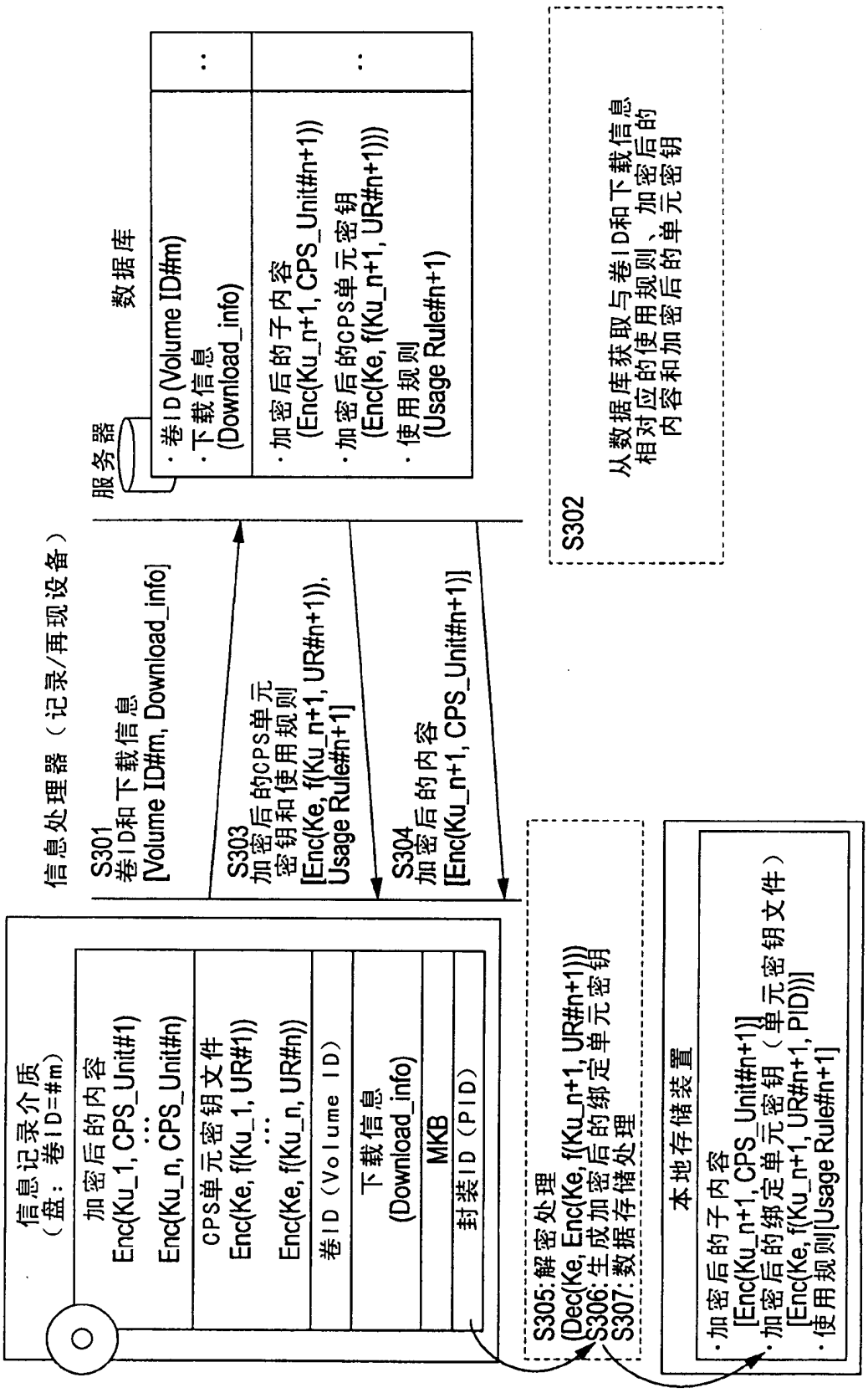

信息记录介质
（盘：卷ID=#m）
加密后的内容
Enc(Ku_1, CPS_Unit#1)
…
Enc(Ku_n, CPS_Unit#n)
CPS单元密钥文件
Enc(Ke, f(Ku_1, UR#1))
…
Enc(Ke, f(Ku_n, UR#n))
卷ID（Volume ID）
下载信息
(Download_info)
MKB
封装ID（PID）
信息处理器（记录/再现设备）
S301
卷ID和下载信息
[Volume ID#m, Download_info]
S303
加密后的CPS单元
密钥和使用规则
[Enc(Ke, f(Ku_n+1, UR#n+1)),
Usage Rule#n+1]
S304
加密后的内容
[Enc(Ku_n+1, CPS_Unit#n+1)]
服务器
数据库
· 卷ID (Volume ID#m)
· 下载信息
(Download_info)
· 加密后的子内容
(Enc(Ku_n+1, CPS_Unit#n+1))
· 加密后的CPS单元密钥
(Enc(Ke, f(Ku_n+1, UR#n+1)))
· 使用规则
(Usage Rule#n+1)
S302
从数据库获取与卷ID和下载信息
相对应的使用规则、加密后的
内容和加密后的单元密钥
S305: 解密处理
(Dec(Ke, Enc(Ke, f(Ku_n+1, UR#n+1)))
S306: 生成加密后的绑定单元密钥
S307: 数据存储处理
本地存储装置
· 加密后的子内容
[Enc(Ku_n+1, CPS_Unit#n+1)]
· 加密后的绑定单元密钥（单元密钥文件）
[Enc(Ke, f(Ku_n+1, UR#n+1, PID))]
· 使用规则[Usage Rule#n+1]

图14

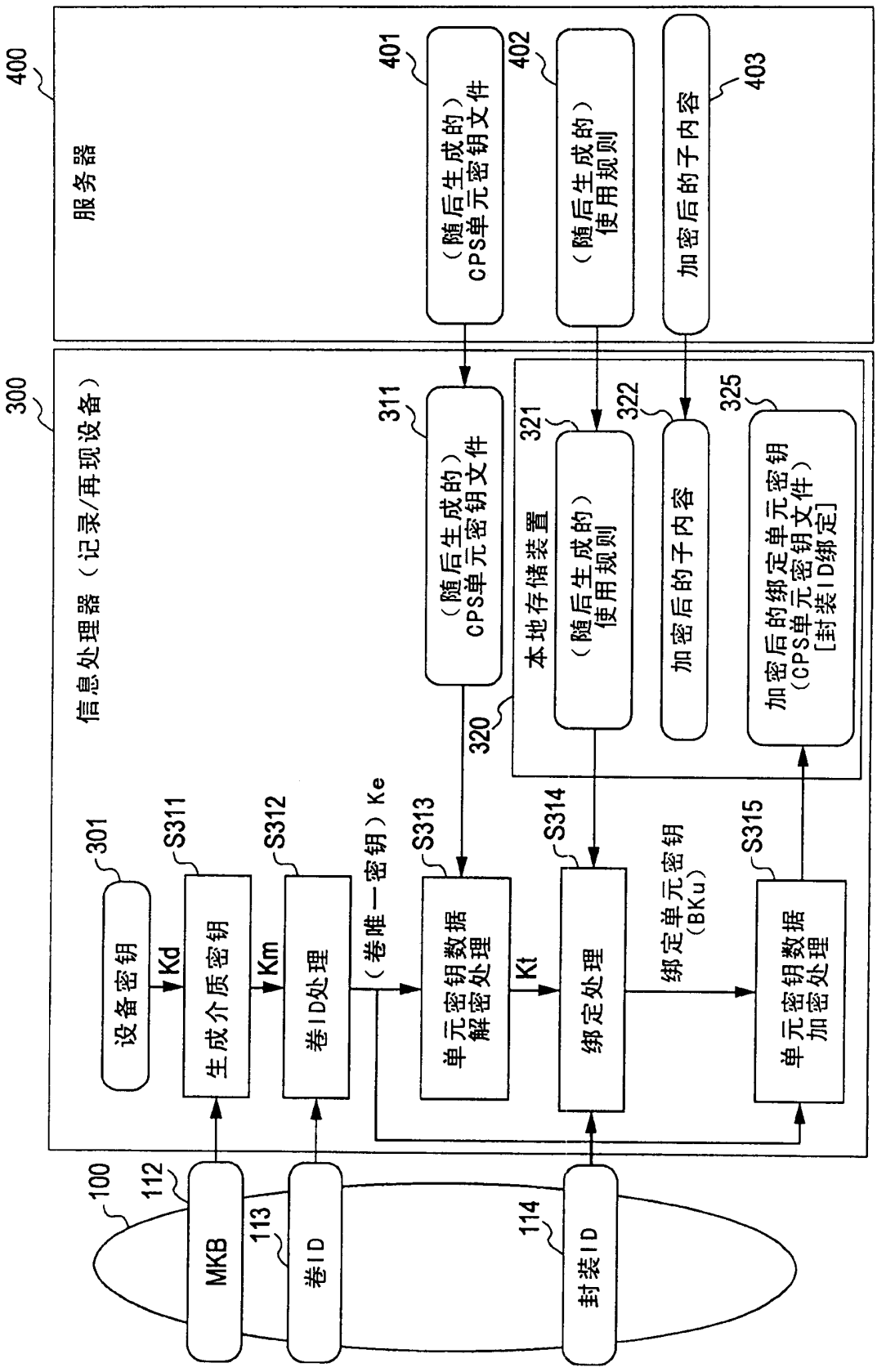

400
服务器
401
（随后生成的）
CPS单元密钥文件
402
（随后生成的）
使用规则
403
加密后的子内容
300
信息处理器（记录/再现设备）
311
（随后生成的）
CPS单元密钥文件
320
本地存储装置
321
（随后生成的）
使用规则
322
加密后的子内容
325
加密后的绑定单元密钥
（CPS单元密钥文件）
[封装ID绑定]
301
设备密钥
S311
Kd
生成介质密钥
S312
Km
卷ID处理
（卷唯一密钥）Ke
S313
单元密钥数据
解密处理
Kt
S314
绑定处理
绑定单元密钥
（BKu）
S315
单元密钥数据
加密处理
100
112
MKB
113
卷ID
114
封装ID

图15

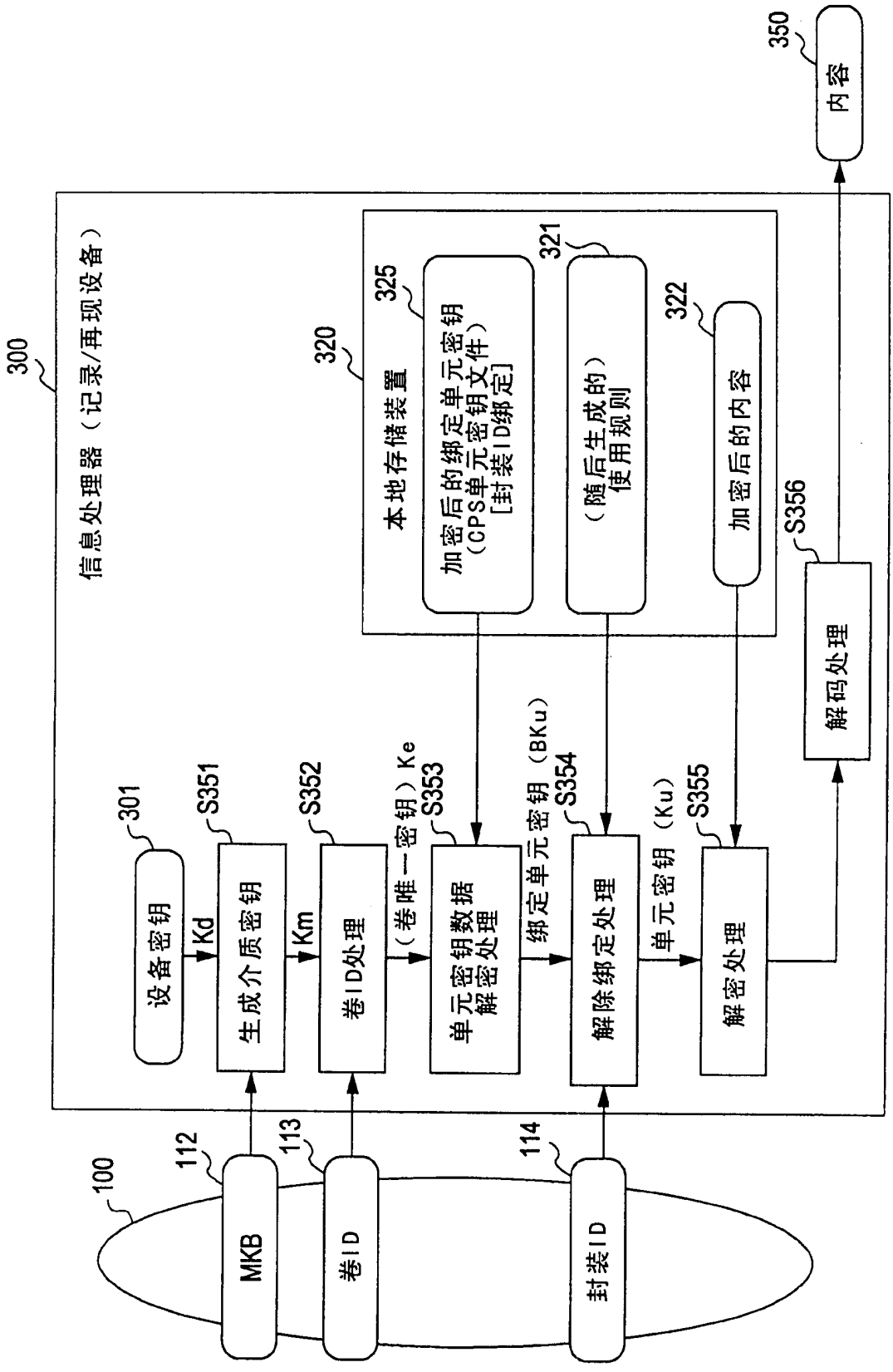

300
信息处理器（记录/再现设备）
320
本地存储装置
325
加密后的绑定单元密钥
（CPS单元密钥文件）
[封装ID绑定]
321
（随后生成的）
使用规则
322
加密后的内容
350
内容
S356
解码处理
301
设备密钥
S351
生成介质密钥
Kd
Km
S352
卷ID处理
（卷唯一密钥）Ke
S353
单元密钥数据
解密处理
绑定单元密钥（BKu）
S354
解除绑定处理
单元密钥（Ku）
S355
解密处理
100
112
MKB
113
卷ID
114
封装ID

图16

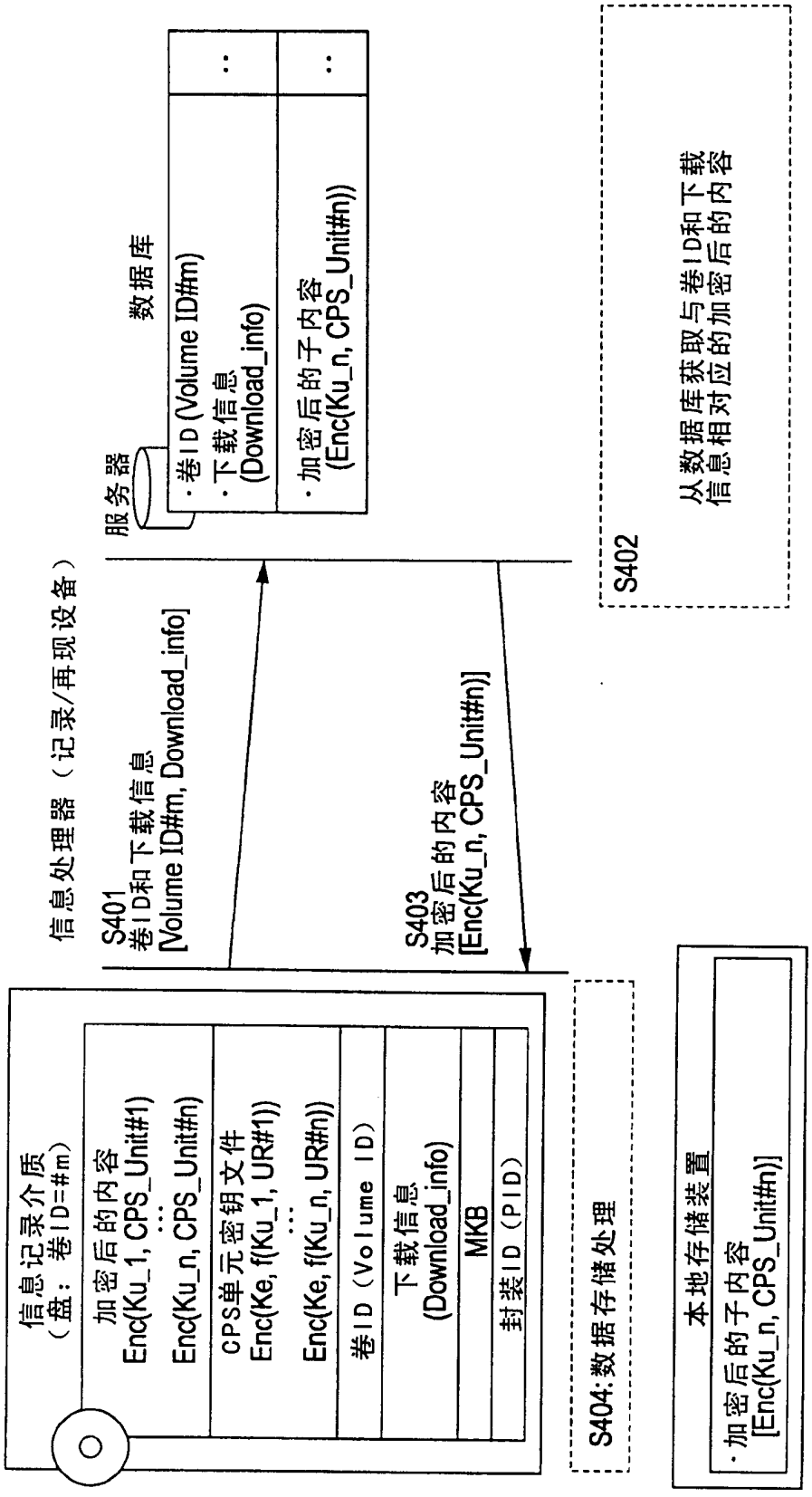

信息记录介质
（盘：卷ID=#m）
加密后的内容
Enc(Ku_1, CPS_Unit#1)
…
Enc(Ku_n, CPS_Unit#n)
CPS单元密钥文件
Enc(Ke, f(Ku_1, UR#1))
…
Enc(Ke, f(Ku_n, UR#n))
卷ID（Volume ID）
下载信息
(Download_info)
MKB
封装ID（PID）
信息处理器（记录/再现设备）
S401
卷ID和下载信息
[Volume ID#m, Download_info]
S403
加密后的内容
[Enc(Ku_n, CPS_Unit#n)]
服务器
数据库
·卷ID (Volume ID#m)
·下载信息
(Download_info)
·加密后的子内容
(Enc(Ku_n, CPS_Unit#n))
S402
从数据库获取与卷ID和下载
信息相对应的加密后的内容
S404: 数据存储处理
本地存储装置
·加密后的子内容
[Enc(Ku_n, CPS_Unit#n)]
S404: 生成加密后的绑定单元密钥
S405: 数据存储处理

图17

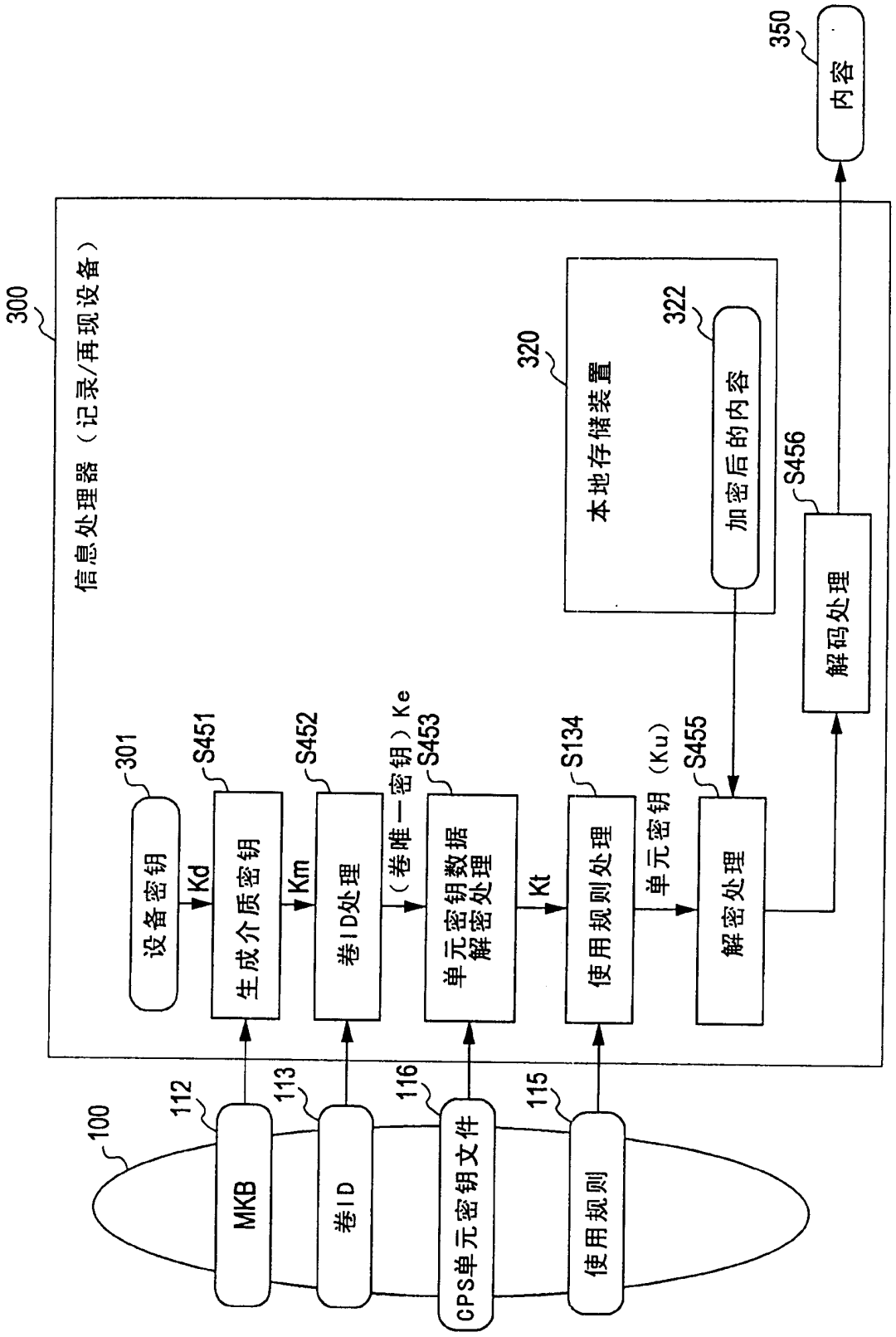

100
MKB
112
卷ID
113
CPS单元密钥文件
116
使用规则
115
300
信息处理器（记录/再现设备）
301
设备密钥
S451
生成介质密钥
Kd
S452
卷ID处理
Km
（卷唯一密钥）Ke
S453
单元密钥数据解密处理
Kt
S134
使用规则处理
单元密钥（Ku）
S455
解密处理
320
本地存储装置
322
加密后的内容
S456
解码处理
350
内容

图18

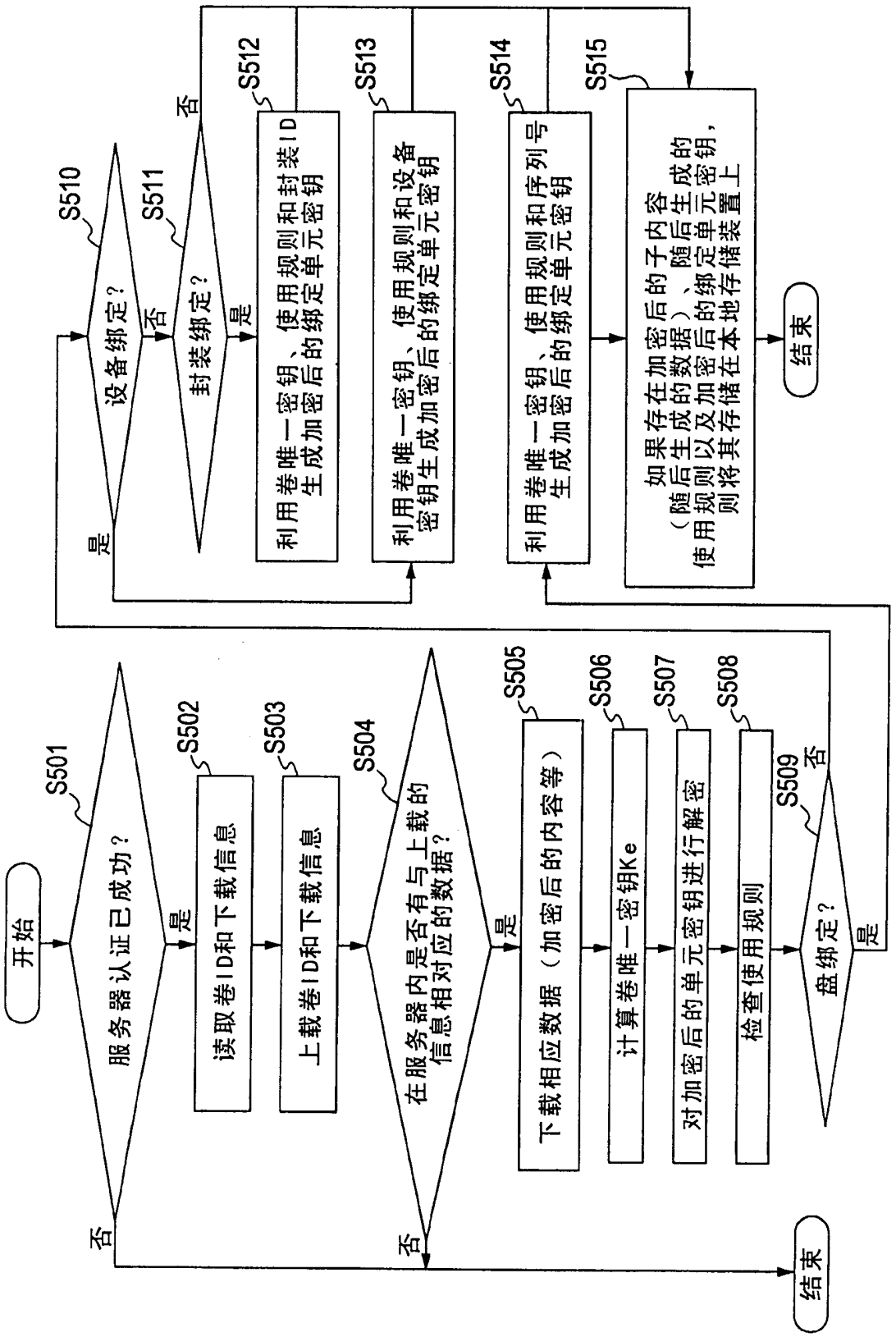

开始
服务器认证已成功？
否
是
读取卷ID和下载信息
上载卷ID和下载信息
在服务器内是否有与上载的信息相对应的数据？
否
是
下载相应数据（加密后的内容等）
计算卷唯一密钥Ke
对加密后的单元密钥进行解密
检查使用规则
盘绑定？
否
是
结束
S501
S502
S503
S504
S505
S506
S507
S508
S509
设备绑定？
否
是
封装绑定？
否
是
利用卷唯一密钥、使用规则和封装ID生成加密后的绑定单元密钥
利用卷唯一密钥、使用规则和设备密钥生成加密后的绑定单元密钥
利用卷唯一密钥、使用规则和序列号生成加密后的绑定单元密钥
如果存在加密后的子内容（随后生成的数据）、随后生成的使用规则以及加密后的绑定单元密钥，则将其存储在本地存储装置上
结束
S510
S511
S512
S513
S514
S515

图19

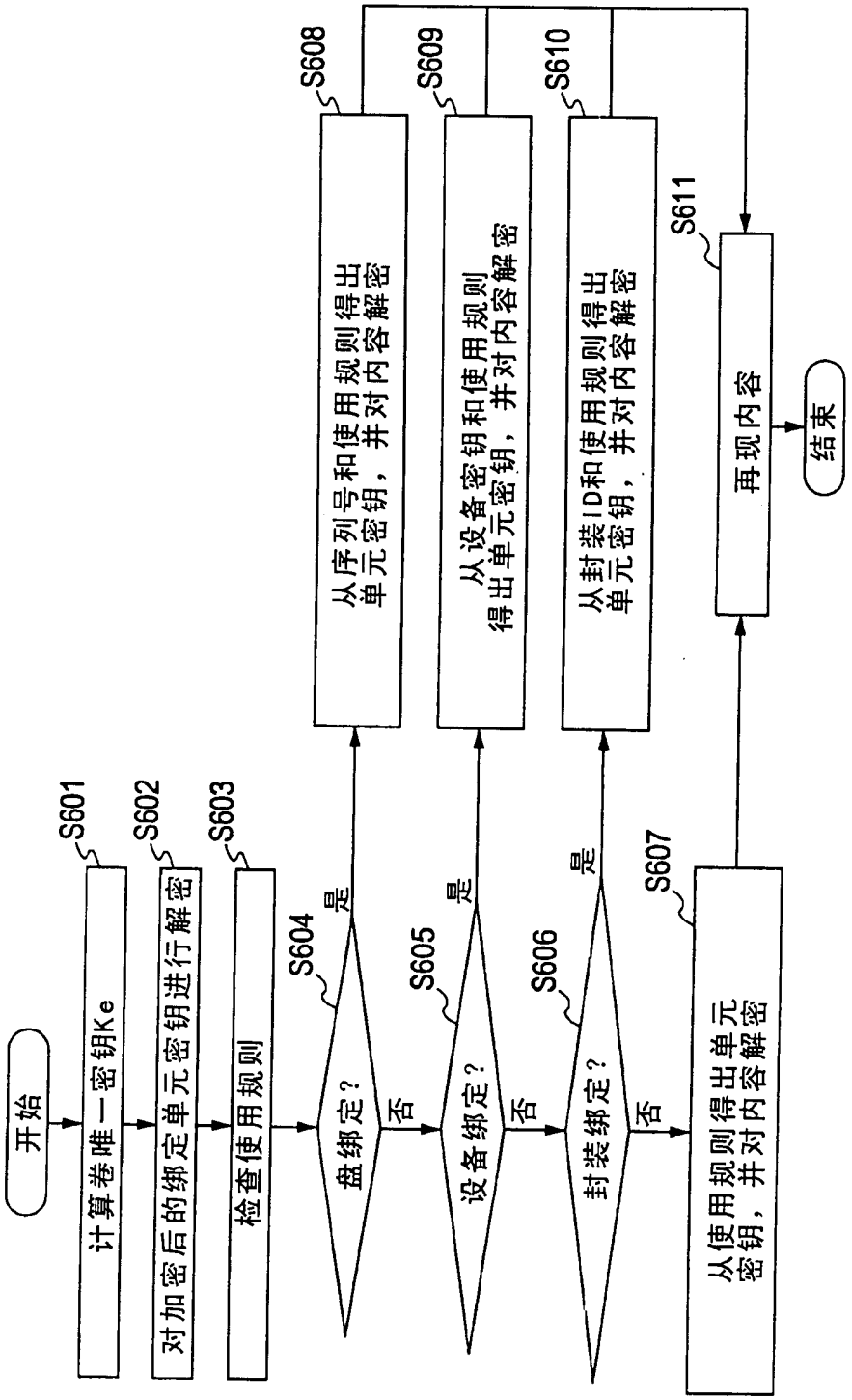

开始
S601
计算卷唯一密钥Ke
S602
对加密后的绑定单元密钥进行解密
S603
检查使用规则
S604
盘绑定？
是
否
S605
设备绑定？
是
否
S606
封装绑定？
是
否
S607
从使用规则得出单元密钥，并对内容解密
S608
从序列号和使用规则得出单元密钥，并对内容解密
S609
从设备密钥和使用规则得出单元密钥，并对内容解密
S610
从封装ID和使用规则得出单元密钥，并对内容解密
S611
再现内容
结束

图20

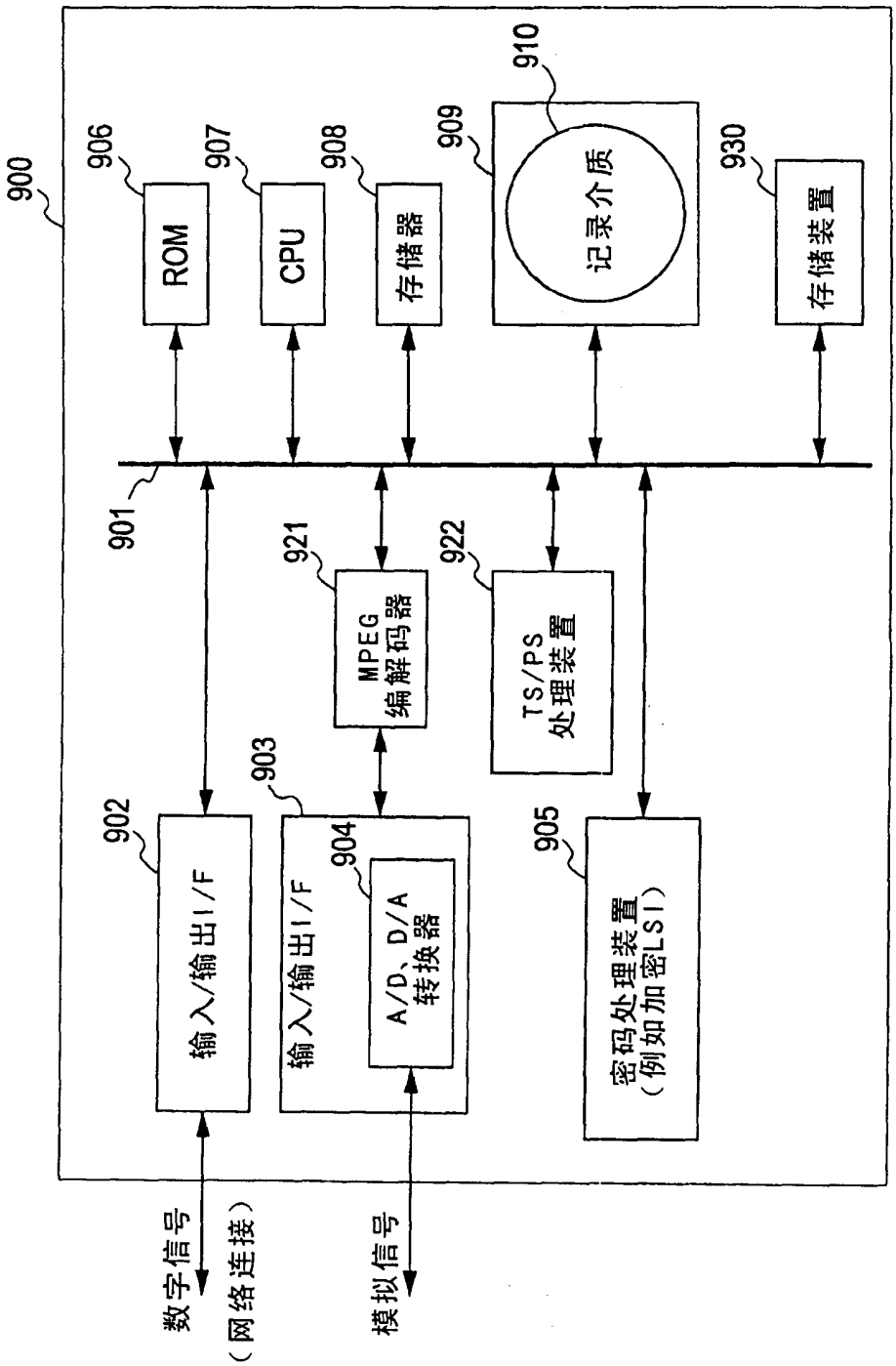

900
906
ROM
907
CPU
908
存储器
909
910
记录介质
930
存储装置
901
921
MPEG
编解码器
922
TS/PS
处理装置
902
输入/输出I/F
903
输入/输出I/F
904
A/D、D/A
转换器
905
密码处理装置
（例如加密LSI）
数字信号
（网络连接）
模拟信号

图21