(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 103177739 A
(43)申请公布日 2013.06.26

(21)申请号 201210448305.X

(22)申请日 2012.11.09

(30)优先权数据
2011-251735 2011.11.17 JP

(71)申请人 索尼公司
地址 日本东京都

(72)发明人 小林义行 久野浩 林隆道

(74)专利代理机构 北京集佳知识产权代理有限公司 11227
代理人 李春晖 李德山

(51)Int.Cl.
*G11B 20/00*(2006.01)

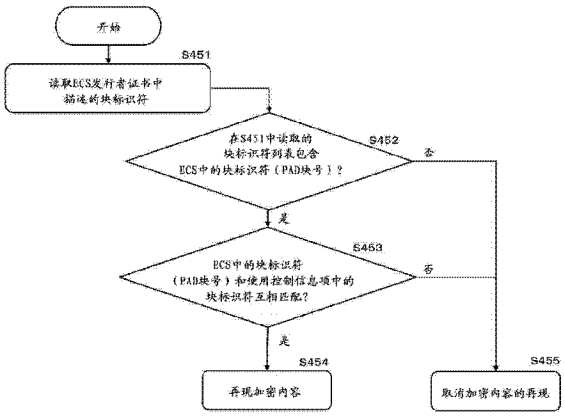
权利要求书3页 说明书47页 附图34页

(54)发明名称

信息处理装置、系统和方法以及信息存储装置和程序

(57)摘要

本申请提供了一种信息处理装置、信息存储装置、信息处理系统、信息处理方法和程序。该信息存储装置包括被配置成存储加密内容以及要应用于对加密内容进行解密的加密密钥的存储单元，包括：保护区域，在保护区域中存储转换加密密钥并且设置了对保护区域的访问限制，转换加密密钥是通过加密密钥的转换获取的数据项，以及通用区域，通用区域存储加密内容以及与加密内容对应地设置的加密内容签名文件，加密内容签名文件包含下述块标识符作为记录数据项，该块标识符指示在保护区域中的哪些区域中准许存储转换加密密钥，从而准许再现装置执行应用该块标识符的内容再现可能性判断，再现装置被配置成从存储单元中读取加密内容并执行再现处理。




CN 103177739 A

1. 一种信息存储装置，包括：

存储单元，被配置成存储加密内容以及要被应用于对所述加密内容进行解密的加密密钥，所述存储单元包括：

保护区域，在所述保护区域中存储转换加密密钥并且设置了对所述保护区域的访问限制，所述转换加密密钥是通过所述加密密钥的转换而获取的数据项，以及

通用区域，所述通用区域存储所述加密内容以及与所述加密内容对应地设置的加密内容签名文件，所述加密内容签名文件包含下述块标识符作为记录数据项，所述块标识符指示在所述保护区域中的哪些区域中准许存储所述转换加密密钥，从而准许再现装置执行应用所述块标识符的内容再现可能性判断，所述再现装置被配置成从所述存储单元中读取所述加密内容并且执行再现处理。

2. 根据权利要求 1 所述的信息存储装置，其中，

所述加密内容签名文件包含 ECS 发行者证书，所述 ECS 发行者证书存储来自作为所述加密内容签名文件的发行者的 ECS 发行者的公开密钥，所述 ECS 发行者证书包含下述块标识符范围作为记录数据项，所述块标识符范围为所述保护区域中的每个区域中准许存储所述转换加密密钥的范围，以及

所述信息存储装置准许所述再现装置判断所述加密内容签名文件中记录的所述块标识符是否落在所述 ECS 发行者证书中记录的所述块标识符范围中，并且基于所述判断的结果来确定是否能够再现所述加密内容，所述再现装置被配置成从所述存储单元中读取所述加密内容并且执行所述再现处理。

3. 根据权利要求 1 所述的信息存储装置，其中，

所述通用区域还存储与所述加密内容对应的使用控制信息项，所述使用控制信息项是包含指示在哪些块中存储所述加密密钥的不同块标识符的信息项，以及

所述信息存储装置准许所述再现装置判断所述加密内容签名文件中记录的所述块标识符是否与所述使用控制信息项中记录的所述不同块标识符匹配，并且基于所述判断的结果来确定是否能够再现所述加密内容，所述再现装置被配置成从所述存储单元中读取所述加密内容并且执行所述再现处理。

4. 一种信息处理装置，包括：

数据处理单元，被配置成执行介质中记录的加密内容的解密处理和再现处理，所述数据处理单元被配置成：

从所述介质中读取与所述加密内容对应地设置的加密内容签名文件，

从所述加密内容签名文件中获取指示在哪些区域中准许存储要被应用于对所述加密内容进行解密的加密密钥的块标识符，以及

执行应用所述块标识符的内容再现可能性判断处理。

5. 根据权利要求 4 所述的信息处理装置，其中，

所述加密内容签名文件包含 ECS 发行者证书，所述 ECS 发行者证书存储来自作为所述加密内容签名文件的发行者的 ECS 发行者的公开密钥，所述 ECS 发行者证书包含下述块标识符范围作为记录数据项，所述块标识符范围为每个区域中准许存储所述加密密钥的范围，以及

所述数据处理单元判断所述加密内容签名文件中记录的所述块标识符是否落在所述

ECS 发行者证书中记录的所述块标识符范围中，并且基于所述判断的结果来确定是否能够再现所述加密内容。

6. 根据权利要求 4 所述的信息处理装置，其中，

所述介质还存储与所述加密内容对应的使用控制信息项，所述使用控制信息项是包含指示在哪些块中存储所述加密密钥的不同块标识符的信息项，以及

所述数据处理单元判断所述加密内容签名文件中记录的所述块标识符是否与所述使用控制信息项中记录的所述不同块标识符匹配，并且基于所述判断的结果来确定是否能够再现所述加密内容。

7. 一种信息处理装置，包括：

数据处理单元，被配置成输出要被记录到介质的加密内容以及要被应用于对所述加密内容进行解密的加密密钥，所述数据处理单元被配置成：

获取与所述加密内容对应地设置的加密内容签名文件，

从所述加密内容签名文件中获取指示在哪些区域中准许存储所述加密密钥的块标识符，以及

执行应用所述块标识符的内容输出可能性判断处理。

8. 根据权利要求 7 所述的信息处理装置，其中，

所述加密内容签名文件包含 ECS 发行者证书，所述 ECS 发行者证书存储来自作为所述加密内容签名文件的发行者的 ECS 发行者的公开密钥，所述 ECS 发行者证书包含下述块标识符范围作为记录数据项，所述块标识符范围为每个区域中准许存储所述加密密钥的范围，以及

所述数据处理单元判断所述加密内容签名文件中记录的所述块标识符是否落在所述 ECS 发行者证书中记录的所述块标识符范围中，并且基于所述判断的结果来确定是否能够输出所述加密内容。

9. 根据权利要求 7 所述的信息处理装置，其中，

所述数据处理单元被配置成：

获取与所述加密内容对应地设置的使用控制信息项，

从所获取的使用控制信息项中获取指示在哪些块中存储了所述加密密钥的不同块标识符，

判断所述加密内容签名文件中记录的所述块标识符是否与所述使用控制信息项中记录的所述不同块标识符匹配，以及

基于所述判断的结果来确定是否能够输出所述加密内容。

10. 一种要由信息处理装置执行的信息处理方法，所述信息处理装置包括被配置成执行介质中记录的加密内容的解密处理和再现处理的数据处理单元，所述数据处理单元被配置成：

从所述介质中读取与所述加密内容对应地设置的加密内容签名文件，

从所述加密内容签名文件中获取指示在哪些区域中准许存储要被应用于对所述加密内容进行解密的加密密钥的块标识符，以及

执行应用所述块标识符的内容再现可能性判断处理。

11. 一种要由信息处理装置执行的信息处理方法，所述信息处理装置包括被配置成输

出要被记录到介质的加密内容以及要被应用于对所述加密内容进行解密的加密密钥的数据处理单元，所述数据处理单元被配置成：

获取与所述加密内容对应地设置的加密内容签名文件，

从所述加密内容签名文件中获取指示在哪些区域中准许存储所述加密密钥的块标识符，以及

执行应用所述块标识符的内容输出可能性判断处理。

12. 一种使信息处理装置执行信息处理的程序，所述信息处理装置包括被配置成执行介质中记录的加密内容的解密处理和再现处理的数据处理单元，所述程序使所述数据处理单元执行：

从所述介质中读取与所述加密内容对应地设置的加密内容签名文件的处理，

从所述加密内容签名文件中获取指示在哪些区域中准许存储要被应用于对所述加密内容进行解密的加密密钥的块标识符的处理，以及

应用所述块标识符的内容再现可能性判断处理。

13. 一种使信息处理装置执行信息处理的程序，所述信息处理装置包括被配置成输出要被记录到媒体的加密内容以及要被应用于对所述加密内容进行解密的加密密钥的数据处理单元，所述程序使所述数据处理单元执行：

获取与所述加密内容对应地设置的加密内容签名文件的处理，

从所述加密内容签名文件中获取指示在哪些区域中准许存储所述加密密钥的块标识符的处理，以及

应用所述块标识符的内容输出可能性判断处理。

# 信息处理装置、系统和方法以及信息存储装置和程序

## 技术领域

[0001] 本公开涉及一种信息处理装置、信息存储装置、信息处理系统、信息处理方法及程序。更具体地，本公开涉及一种用于防止对内容的欺诈性使用的信息处理装置、信息存储装置、信息处理系统、信息处理方法及程序。

## 背景技术

[0002] 内容比如电影和音乐作品通过各种媒体比如 DVD（数字多功能盘）、蓝光盘（商标）和闪存、网络比如因特网、或广播波提供给用户。用户可以通过使用记录 / 再现装置比如 PC、移动终端、BD 播放器或者各种信息处理装置比如电视机来再现这些内容。

[0003] 但是，提供给用户的内容中的很多内容比如音乐数据产品和图像数据产品的版权、发行权等由创建者或销售者拥有。因此，在很多情况下，当向用户提供内容时，这些内容的提供者设置了对内容的预定使用限制。

[0004] 通过使用数字记录装置和数字记录媒体，例如图像和声音可以被重复地记录和再现而不会受损。因此，存在有非法复制内容的使用的扩散的问题，具体地，存在非法复制内容通过因特网的分发问题以及被称为盗版盘的分发问题。

[0005] 为了防止这样的非法数据复制，各种用于防止向数字记录装置和数字记录媒体的非法复制的技术已经投入实际使用。

[0006] 作为这些技术的一个示例，存在一种只向具有许可证即内容使用权的再现装置提供加密数据项的解密密钥的内容加密处理。将许可证给予被设计为遵循预定操作规则比如禁止非法复制规则的再现装置。因此，没有被给予该许可证的其他再现装置没有加密数据项的解密密钥，从而不能对该加密数据项进行解密。

[0007] 但是，即使执行了这样的内容加密，内容还是仍被欺诈性地使用。

[0008] 这里，对内容的欺诈性使用的示例进行描述。

[0009] 在该示例中，假设下述配置，其中内容服务器将加密内容分发给用户装置比如记录 / 再现装置、PC 和移动终端。

[0010] 当将加密内容分发给用户装置时，内容服务器例如经由网络向用户装置分发下述数据项。

[0011] (a) 加密内容

[0012] (b) 用于加密和对加密内容进行解密的加密密钥。

[0013] 当将同一内容比如同一电影分发给大量的用户装置时，内容服务器执行例如下述两个处理中的任意一个处理。

[0014] (A) 通过应用单独的不同加密密钥来生成不同的加密内容，并且将该不同的加密内容分别提供给用户装置。

[0015] (B) 生成以相同的加密密钥加密的相同的加密内容，并且将该相同的加密内容提供给多个用户装置中的每个用户装置。

[0016] 考虑到防止对内容的欺诈性使用的安全性，上述处理 (A) 是有利的。

[0017] 但是，为了执行上述处理 (A)，必须要执行分别为大量的用户设置单独的加密密钥以及生成单独的加密内容的处理。结果，引起下述问题：与接收内容的用户数量成比例地，由于例如加密密钥的生成和管理以及生成加密内容的处理而使得服务器的处理负荷变高。

[0018] 因此，在许多情况下，实施上述处理 (B)，换言之，通过以相同加密密钥进行加密来生成相同内容的相同加密内容并且将相同加密内容提供给多个用户中的每个用户的处理。

[0019] 例如，对于具有某个标题的内容设置一个加密密钥(换言之，标题密钥)，并且通过应用这个加密密钥来生成相同的加密内容。然后，将下述数据集分发给大量用户中的每个用户。

[0020] (a) 加密内容

[0021] (b) 标题密钥

[0022] 该处理减小了内容服务器的处理负荷。

[0023] 注意，在下述描述中，将以内容的标题为单位设置的加密密钥定义为“标题密钥”。

[0024] 注意，标题密钥应用于对与标题对应的内容进行加密和对加密内容进行解密的处理。

[0025] 但是，当相同的数据集即下述数据项的相同组合：

[0026] (a) 加密内容，以及

[0027] (b) 标题密钥，以该方式分发给大量用户时，一些“未授权用户”可以执行下述处理。

[0028] 具体地，可以实施下述欺诈行为。

[0029] (1)“未授权用户”读取从服务器接收的标题密钥，并且将该标题密钥透露给不确定数量的用户。

[0030] 或者，(2)“未授权用户”使用与某个加密内容 A 相对应的标题密钥 A 以便加密完全不同的内容 B，并且将下述数据组合分发给不确定数量的用户。

[0031] (X) 标题密钥 A

[0032] (Y) 用标题密钥 A 加密的加密内容 B

[0033] 例如，在执行上述处理 (1) 的情况下，已经获取非法透露的标题密钥的大量用户欺诈性地使用以与非法透露的标题密钥相同的标题密钥所加密的内容。

[0034] 另外，在执行上述处理 (2) 的情况下，当大量用户从上述“未授权用户”获取非法数据集时，即获取：

[0035] (X) 标题密钥 A，以及

[0036] (Y) 由“未授权用户”生成的用标题密钥 A 加密的加密内容 B 时，加密内容 B 被非法使用。

[0037] 结果，更少的用户合法购买原始的合法数据集，即：

[0038] 加密内容 B，以及

[0039] 与加密内容 B 对应的标题密钥 B，从而版权拥有者和发行权拥有者的收益受到显著损失。

[0040] 进一步地，对欺诈性处理的具体示例进行描述。

[0041] 在该具体示例中，假设内容服务器保存下述(1)至(3)项的加密内容(C)以及标题密钥(Kt)的数据集。

[0042] (1)(Kt11,C11)

[0043] (2)(Kt12,C12)

[0044] (3)(Kt13,C13)

[0045] 注意:Cnn 表示内容文件,并且

[0046] Ktnn 表示用于对内容的加密的标题密钥。

[0047] (Kt11,C11)表示标题密钥(Kt11)和用标题密钥(Kt11)加密的内容(C11)的数据集。

[0048] 例如,假设某个“未授权用户 Ux”购买了所有上述三个数据集:

[0049] (1)(Kt11,C11),

[0050] (2)(Kt12,C12),以及

[0051] (3)(Kt13,C13),并且

[0052] 假设这次购买处理本身是基于用户装置比如“未授权用户 Ux”的 PC 与内容服务器之间的预定合法购买过程而执行的。

[0053] 该“未授权用户 Ux”将上述数据集(1)至(3)记录到介质比如作为用户装置的 PC 的硬盘。

[0054] 该“未授权用户 Ux”从该介质比如作为用户装置的 PC 的硬盘读取上述数据集(1)至(3),并且使用对应的标题密钥来解密所有的加密内容。以此方式,获取了下述数据项。

[0055] 标题密钥:Kt11、Kt12 和 Kt13

[0056] 解密的内容:C11、C12 和 C13

[0057] 注意,当在授权的再现装置中使用正常内容再现程序时,不能将标题密钥读取出来。但是,可以例如通过在装置本身比如该 PC 上安装恶意程序来读取标题密钥。因此,要完全防止读取标题密钥仍是困难的。

[0058] 进一步地,该“未授权用户 Ux”生成通过解密的内容:C11 至 C13 的串接而获取的数据项

[0059] C11||C12||C13

[0060] 并且用标题密钥:Kt11 对此串接的数据项进行加密。

[0061] 换言之,该“未授权用户 Ux”生成下述数据集

[0062] (Kt11,C11||C12||C13),

[0063] 并且将该数据集通过网络进行非法分发。具体地,将该数据集以低价售卖,或免费地提供给大量用户。

[0064] 这样的处理使得大量的普通用户能够从上述“未授权用户 Ux”获取上述非法生成的数据集,即:

[0065] (Kt11,C11||C12||C13)。

[0066] 该数据集包括下述数据项:

[0067] (a)用标题密钥 Kt11 加密的加密内容,以及

[0068] (b)标题密钥 Kt11,并且具有和由授权内容提供者向用户提供的数据集内容的数据结构相同的数据结构。

[0069] 因此,只要具有许可的正常内容再现程序,任何授权的再现装置均可以通过使用标题密钥 Kt11 没有任何困难地来解密和再现该加密内容 [C11||C12||C13]。

[0070] 结果，内容被越来越多地没有合法购买而欺诈性地使用。在此示例中，更少的用户合法地购买内容比如 C11 至 C13。最终，合法权利拥有者的收益受到损失。

[0071] 这里，更具体地描述该欺诈处理。例如，假设关于系列内容比如片段 1 至片段 12 的十二个标题的戏剧，如下以片段为单元设置内容的购买单元。

[0072] 片段 1=（Kt01，C01）

[0073] 片段 2=（Kt02，C02）

[0074] 片段 3=（Kt03，C03）

[0075] ...

[0076] 片段 12=（Kt12，C12）

[0077] 在此情况下，某个“未授权用户”可以执行下述处理 ：购买整个系列，即从片段 1 到片段 12 的所有十二个标题 ；串接与片段 1 到片段 12 相对应的内容 ：C01 到 C12 ；并且通过用与片段 1 对应的标题密钥再加密来生成数据集，即

[0078] （Kt01，C01||C02||C03…||C12）从而使得在网络上透露此数据集或者非法售卖此数据集。

[0079] 在此情况下，使得大量用户装置能够通过获取“未授权用户”生成的欺诈数据集

[0080] （Kt01，C01||C02||C03…||C12）

[0081] 来再现和使用该内容。

[0082] 例如，假设以片段为单位上述十二个片段中的每个片段的全价是￥2000，购买所有十二个片段的花费如下。

[0083] 12× ￥2000= ￥24000

[0084] 当该“未授权用户”以例如￥6000 价格售卖该欺诈数据集

[0085] （Kt01，C01||C02||C03…||C12）时，使得大量用户能够购买该低价内容。结果，妨碍了内容的合法销售，导致原版权拥有者和发行权拥有者的收益的损失和权利的侵害。

[0086] 除了上述示例，可以使用与某个内容 C11 对应地设置的标题密钥 Kt11 来加密各种其他不相关的其他内容 Cxx，如下数据集。

[0087] （Kt11，Cxx）

[0088] 内容 Cxx 可以包含各种内容，从而产生所有内容都能够用单一标题密钥无限制地解密和再现的问题。

[0089] 换言之，即使在使用了禁止再现明文内容的再现装置情况下，通过使用上述欺诈数据集，仍然可以执行解密和再现，就如同解密和再现合法购买的内容那样。

[0090] 另外，还使得该“未授权用户”能够提供对标题密钥的替代和再加密的服务，从而使得该“未授权用户”能够表现地像授权服务器那样。

[0091] 如上所述，仅用这样的内容加密处理作为对策难以防止欺诈性使用。

[0092] 作为一种非加密处理的用于消除对内容的欺诈性使用的方法，有一种使再现装置验证内容是否被篡改的方法。通过采用此方法，例如在分发内容的处理过程中，在确认内容中有一些改动（篡改）的情况下，可以取消被篡改的内容的使用。

[0093] 具体地，可以采用下述控制系统 ：只有当使得执行内容再现的用户装置执行内容是否被篡改的验证处理并且确认内容中没有篡改的情况下，才准许内容的再现 ；以及在确认内容中有一些篡改的情况下取消内容的再现。

[0094] 例如，专利文献 1（日本专利申请公开号 2002-358011）公开了一种控制系统：根据要再现的内容的文件来计算哈希值；执行该哈希值与预备的验证哈希值即基于正常内容数据项预先计算的验证哈希值的比较；并且在新计算的哈希值与验证哈希值匹配并且判断出在内容中确认没有篡改的情况下，转到内容的再现处理。

[0095] 但是，在执行基于内容计算哈希值的处理的情况下，当作为哈希值的计算的源数据项的内容数据项的量大时，计算要求过高的处理负荷和过长的处理时间段。近年来，运动图像的质量变得越来越高，因此，在很多情况下，一个内容具有从几个千兆字节到几十个千兆字节的数据量。当使执行内容的再现的用户装置执行基于这样的大量数据来计算内容的哈希值的处理时，引起对用户装置要求过高的数据处理能力的问题，并且引起由于内容的验证要求更长时间段而导致不能高效执行内容再现处理的问题。

[0096] 另外，专利文献 2（日本专利号 4576936）公开了一种系统，其中，将设置为在信息记录介质中存储的内容的分段数据项的相应哈希单元的哈希值记录在内容哈希列表中，并且和内容一起存储在信息记录介质中。

[0097] 根据专利文献 2 公开的系统，执行内容再现的信息处理装置基于随机选择的哈希单元中的至少一个来执行哈希值验证处理。使用此系统，可以不管内容的数据量，具体地，基于具有小数据量的哈希单元来执行计算和验证哈希值的处理。结果，在执行内容再现的用户装置中可以高效地执行内容验证。

[0098] 但是，在专利文献 2 中公开的系统是以信息记录介质中存储的内容的处理为前提而设计的。换言之，存在下述问题：尽管专利文献 2 中公开的系统能够应用于不仅内容而且哈希值也被同时记录的情况，例如在制造信息记录介质时，但是该系统难以应用于例如从服务器下载的内容。

[0099] 另外，以上专利文献 1 和专利文献 2 中的每一个都将重点放在内容是否被篡改的验证上，因而具有难以限制分发非法复制内容的问题。

[0100] 如上所述，采用现有技术中对内容加密和验证内容是否被篡改的处理，并没有充分地防止非法复制内容的分发或者内容加密密钥的泄露。

## 发明内容

[0101] 考虑到上述问题，需要提供一种有效防止对内容的欺诈性使用的信息处理装置、信息存储装置、信息处理系统、信息处理方法及程序。

[0102] 根据本公开的第一实施方式，提供了一种信息存储装置，包括：

[0103] 存储单元，被配置成存储加密内容以及要被应用于对所述加密内容进行解密的加密密钥，所述存储单元包括：

[0104] 保护区域，在所述保护区域中存储转换加密密钥并且设置了对所述保护区域的访问限制，所述转换加密密钥是通过所述加密密钥的转换而获取的数据项，以及

[0105] 通用区域，所述通用区域存储所述加密内容以及与所述加密内容对应地设置的加密内容签名文件，所述加密内容签名文件包含下述块标识符作为记录数据项，所述块标识符指示在所述保护区域中的哪些区域中准许存储所述转换加密密钥，从而准许再现装置执行应用所述块标识符的内容再现可能性判断，所述再现装置被配置成从所述存储单元中读取所述加密内容并且执行再现处理。

[0106] 此外，在根据本公开的第一实施方式的信息存储装置中，

[0107] 所述加密内容签名文件包含 ECS 发行者证书，所述 ECS 发行者证书存储来自作为所述加密内容签名文件的发行者的 ECS 发行者的公开密钥，所述 ECS 发行者证书包含下述块标识符范围作为记录数据项，所述块标识符范围为所述保护区域中的每个区域中准许存储所述转换加密密钥的范围，以及

[0108] 所述信息存储装置准许所述再现装置判断所述加密内容签名文件中记录的所述块标识符是否落在所述 ECS 发行者证书中记录的所述块标识符范围中，并且基于所述判断的结果来确定是否能够再现所述加密内容，所述再现装置被配置成从所述存储单元中读取所述加密内容并且执行所述再现处理。

[0109] 再者，在根据本公开的第一实施方式的信息存储装置中，

[0110] 所述通用区域还存储与所述加密内容对应的使用控制信息项，所述使用控制信息项是包含指示在哪些块中存储所述加密密钥的不同块标识符的信息项，以及

[0111] 所述信息存储装置准许所述再现装置判断所述加密内容签名文件中记录的所述块标识符是否与所述使用控制信息项中记录的所述不同块标识符匹配，并且基于所述判断的结果来确定是否能够再现所述加密内容，所述再现装置被配置成从所述存储单元中读取所述加密内容并且执行所述再现处理。

[0112] 此外，根据本公开的第二实施方式，提供了一种信息处理装置中，包括

[0113] 数据处理单元，被配置成执行介质中记录的加密内容的解密处理和再现处理，所述数据处理单元被配置成：

[0114] 从所述介质中读取与所述加密内容对应地设置的加密内容签名文件，

[0115] 从所述加密内容签名文件中获取指示在哪些区域中准许存储要被应用于对所述加密内容进行解密的加密密钥的块标识符，以及

[0116] 执行应用所述块标识符的内容再现可能性判断处理。

[0117] 再者，在根据本公开的第二实施方式的信息处理装置中，

[0118] 所述加密内容签名文件包含 ECS 发行者证书，所述 ECS 发行者证书存储来自作为所述加密内容签名文件的发行者的 ECS 发行者的公开密钥，所述 ECS 发行者证书包含下述块标识符范围作为记录数据项，所述块标识符范围为每个区域中准许存储所述加密密钥的范围，以及

[0119] 所述数据处理单元判断所述加密内容签名文件中记录的所述块标识符是否落在所述 ECS 发行者证书中记录的所述块标识符范围中，并且基于所述判断的结果来确定是否能够再现所述加密内容。

[0120] 另外，在根据本公开的第二实施方式的信息处理装置中，

[0121] 所述介质还存储与所述加密内容对应的使用控制信息项，所述使用控制信息项是包含指示在哪些块中存储所述加密密钥的不同块标识符的信息项，以及

[0122] 所述数据处理单元判断所述加密内容签名文件中记录的所述块标识符是否与所述使用控制信息项中记录的所述不同块标识符匹配，并且基于所述判断的结果来确定是否能够再现所述加密内容。

[0123] 此外，根据本公开的第三实施方式，提供了一种信息处理装置中，包括

[0124] 数据处理单元，被配置成输出要被记录到介质的加密内容以及要被应用于对所述

加密内容进行解密的加密密钥，所述数据处理单元被配置成：

[0125] 获取与所述加密内容对应地设置的加密内容签名文件，

[0126] 从所述加密内容签名文件中获取指示在哪些区域中准许存储所述加密密钥的块标识符，以及

[0127] 执行应用所述块标识符的内容输出可能性判断处理。

[0128] 再者，在根据本公开的第三实施方式的信息处理装置中，

[0129] 所述加密内容签名文件包含 ECS 发行者证书，所述 ECS 发行者证书存储来自作为所述加密内容签名文件的发行者的 ECS 发行者的公开密钥，所述 ECS 发行者证书包含下述块标识符范围作为记录数据项，所述块标识符范围为每个区域中准许存储所述加密密钥的范围，以及

[0130] 所述数据处理单元判断所述加密内容签名文件中记录的所述块标识符是否落在所述 ECS 发行者证书中记录的所述块标识符范围中，并且基于所述判断的结果来确定是否能够输出所述加密内容。

[0131] 另外，在根据本公开的第三实施方式的信息处理装置中，所述数据处理单元被配置成：

[0132] 获取与所述加密内容对应地设置的使用控制信息项，

[0133] 从所获取的使用控制信息项中获取指示在哪些块中存储了所述加密密钥的不同块标识符，

[0134] 判断所述加密内容签名文件中记录的所述块标识符是否与所述使用控制信息项中记录的所述不同块标识符匹配，以及

[0135] 基于所述判断的结果来确定是否能够输出所述加密内容。

[0136] 此外，根据本公开的第四实施方式，提供了一种要由信息处理装置执行的信息处理方法，所述信息处理装置包括被配置成执行介质中记录的加密内容的解密处理和再现处理的数据处理单元，所述数据处理单元被配置成：

[0137] 从所述介质中读取与所述加密内容对应地设置的加密内容签名文件，

[0138] 从所述加密内容签名文件中获取指示在哪些区域中准许存储要被应用于对所述加密内容进行解密的加密密钥的块标识符，以及

[0139] 执行应用所述块标识符的内容再现可能性判断处理。

[0140] 此外，根据本公开的第五实施方式，提供了一种要由信息处理装置执行的信息处理方法，所述信息处理装置包括被配置成输出要被记录到介质的加密内容以及要被应用于对所述加密内容进行解密的加密密钥的数据处理单元，所述数据处理单元被配置成：

[0141] 获取与所述加密内容对应地设置的加密内容签名文件，

[0142] 从所述加密内容签名文件中获取指示在哪些区域中准许存储所述加密密钥的块标识符，以及

[0143] 执行应用所述块标识符的内容输出可能性判断处理。

[0144] 此外，根据本公开的第六实施方式，提供了一种使信息处理装置执行信息处理的程序，所述信息处理装置包括被配置成执行介质中记录的加密内容的解密处理和再现处理的数据处理单元，所述程序使所述数据处理单元执行：

[0145] 从所述介质中读取与所述加密内容对应地设置的加密内容签名文件的处理，

[0146] 从所述加密内容签名文件中获取指示在哪些区域中准许存储要被应用于对所述加密内容进行解密的加密密钥的块标识符的处理，以及

[0147] 应用所述块标识符的内容再现可能性判断处理。

[0148] 此外，根据本公开的第七实施方式，提供了一种使信息处理装置执行信息处理的程序，所述信息处理装置包括被配置成输出要被记录到媒体的加密内容以及要被应用于对所述加密内容进行解密的加密密钥的数据处理单元，

[0149] 所述程序使所述数据处理单元执行：

[0150] 获取与所述加密内容对应地设置的加密内容签名文件的处理，

[0151] 从所述加密内容签名文件中获取指示在哪些区域中准许存储所述加密密钥的块标识符的处理，以及

[0152] 应用所述块标识符的内容输出可能性判断处理。

[0153] 注意，根据本公开的实施方式的程序包括能够由记录媒体或通信媒体提供给例如能够执行不同程序和代码的信息处理装置、计算机及系统的程序。通过提供这种计算机可读形式的程序，可以在信息处理装置、计算机及系统中执行与该程序对应的处理。

[0154] 在该说明书中使用的术语“系统”意指多个装置的逻辑集合配置，因而这些如上文所述配置的装置不一定设置在同一壳体中。

[0155] 根据本公开的一个实施方式中的配置，提供了一种用于有效防止对内容的欺诈性使用的装置和方法。

[0156] 具体地，从与加密内容对应地设置的加密内容签名文件中获取指示在哪些区域中准许存储要被应用于解密该加密内容的加密密钥的块标识符。之后，执行应用该块指示符的内容再现可能性判断处理。该加密内容签名文件包含由作为加密内容签名文件的发行者的ECS发行者发行的证书。执行关于加密内容签名文件中记录的块标识符是否落在ECS发行者证书中记录的块标识符范围中的判断，以及执行关于加密内容签名文件中记录的块标识符是否与使用控制信息项中记录的不同块标识符匹配的判断。基于这些判断的结果，确定是否能够再现该内容。

[0157] 通过使用从加密内容签名文件获取的块标识符信息项，能够基于关于密钥信息项是否被记录在某个准许访问的块中的判断来进行内容使用控制。

[0158] 根据以下对如附图中所示的本公开的最佳模式的实施方式的详细描述，本公开的这些和其他目的、特征和优点将会变得更加明显。

## 附图说明

[0159] 图1是内容提供处理和内容使用处理的概况的说明图；

[0160] 图2是存储卡中记录的内容的使用模式的说明图；

[0161] 图3是存储卡中的存储区域的具体配置示例的说明图；

[0162] 图4是主机证书的说明图；

[0163] 图5是服务器证书的说明图；

[0164] 图6是存储在存储卡中的数据的具体配置示例和访问控制处理的示例的说明图；

[0165] 图7是本公开的实施方式的被配置成防止对内容的欺诈性使用的信息处理系统的整体配置的说明图；

[0166] 图 8 是在装置中应用于防止对内容的欺诈性使用的数据项的交换的说明图；

[0167] 图 9 是加密内容签名文件（ECS 文件）的配置示例的说明图；

[0168] 图 10 是另一个加密内容签名文件（ECS 文件）的配置示例的说明图；

[0169] 图 11 是包含在加密内容签名文件中的 ECS 发行者证书的配置示例的说明图；

[0170] 图 12 是 ECS 发行者证书失效列表的配置示例的说明图；

[0171] 图 13 是加密内容签名文件（ECS 文件）的生成处理和数据结构的概况的说明图；

[0172] 图 14 是加密内容签名文件（ECS 文件）的生成、内容提供和使用处理序列的说明性序列图；

[0173] 图 15 是加密内容签名文件（ECS 文件）的生成、内容提供和使用处理序列的另一个说明性序列图；

[0174] 图 16 是示出了参照加密内容签名文件（ECS 文件）中记录的日期数据进行的内容提供可能性判断处理的序列的说明性流程图；

[0175] 图 17 是示出了参照加密内容签名文件（ECS 文件）中记录的日期数据进行的另一个内容提供可能性判断处理的序列的说明性流程图；

[0176] 图 18 是示出了参照加密内容签名文件（ECS 文件）中记录的日期数据进行的内容再现可能性判断处理的序列的说明性流程图；

[0177] 图 19 是由服务器进行的针对存储卡的数据记录处理的示例的说明图；

[0178] 图 20 是由主机进行的针对存储卡中的记录数据的读取处理的示例的说明图；

[0179] 图 21 是存储卡中记录的数据的配置示例的说明图；

[0180] 图 22 是存储卡中记录的数据的另一个配置示例的说明图；

[0181] 图 23 是存储卡中的通用区域中记录的使用控制信息的数据项的配置示例的说明图；

[0182] 图 24 是通过替代处理的对内容的欺诈性使用的示例的说明图；

[0183] 图 25 是示出了通过替代处理的对内容的欺诈性记录处理的示例的说明性流程图；

[0184] 图 26 是示出了通过替代处理记录的欺诈性内容不能被再现的说明性流程图；

[0185] 图 27 是通过替代处理的对内容的欺诈性使用的另一个示例的说明图；

[0186] 图 28 是示出了通过替代处理的对内容的欺诈性记录处理的另一个示例的说明性流程图；

[0187] 图 29 是示出了通过替代处理记录的欺诈性内容不能被再现的另一个说明性流程图；

[0188] 图 30 是加密内容签名文件（ECS 文件）中记录的块标识符和使用控制信息文件中记录的不同块标识符的说明图；

[0189] 图 31 是示出了参照加密内容签名文件（ECS 文件）中记录的块标识符和使用控制信息文件中记录的不同块标识符的内容提供可能性判断序列的说明性流程图；

[0190] 图 32 是示出了从 ECS 发行者证书读取块标识符的处理序列的说明性流程图；

[0191] 图 33 是示出了参照加密内容签名文件（ECS 文件）中记录的块标识符和使用控制信息文件中记录的不同块标识符的内容再现可能性判断序列的说明性流程图；

[0192] 图 34 是信息处理装置的硬件配置示例的说明图；以及

[0193] 图 35 是作为信息存储装置的存储卡的硬件配置示例的说明图。

## 具体实施方式

[0194] 在下文中，将参照附图详细描述根据本公开的实施方式的信息处理装置、信息存储装置、信息处理系统、信息处理方法和程序。注意，在以下部分中按下述顺序进行描述。

[0195] 1. 内容提供处理和内容使用处理的概述

[0196] 2. 存储卡的配置示例和使用示例

[0197] 3. 包含针对保护区域的访问准许信息项的证书

[0198] 4. 参照装置的证书来访问存储卡的处理的示例

[0199] 5. 使用加密内容签名（ECS）发行者的内容提供系统

[0200] 6.ECS 文件的配置示例

[0201] 7.ECS 发行者密钥失效列表的结构

[0202] 8. 加密内容签名文件（ECS 文件）的生成处理

[0203] 9. 应用 ECS 文件和 ECS 发行者证书的日期信息项的处理

[0204] 10. 相关加密密钥和 ECS 发行者的签名的配置

[0205] 11. 应用加密内容签名（ECS）文件中记录的块标识符的处理

[0206] 12. 每个装置的硬件配置示例

[0207] 13. 本公开的配置的总结

[0208] [1. 内容提供处理和内容使用处理的概述 ]

[0209] 在下文中，将参照附图详细描述根据本公开的实施方式的信息处理装置、信息处理方法和程序。

[0210] 首先，将参照图 1 和后续附图描述内容提供处理和内容使用处理的概述。

[0211] 图 1 从其左手侧示出了下述项的示例。

[0212] （a）内容提供装置

[0213] （b）内容记录 / 再现装置（主机）

[0214] （c）内容记录介质

[0215] （c）内容记录介质是在其中用户记录内容并且用户使用其来再现内容的介质。在这里，示出了存储卡 31，其是信息存储装置比如闪存。

[0216] 注意，在下文的实施方式中作为典型示例描述的示例中，尽管由内容提供装置提供的内容是加密内容，但是根据本公开的实施方式的配置不局限于提供的内容是加密内容的情况，而是也能够适用于提供的内容是未加密的明文内容的情况。

[0217] 用户使用存储卡 31 来记录各种内容比如音乐作品和电影。这些内容包括要在使用方面受控制的内容，比如受版权保护的内容。

[0218] 要在使用方面受控制的内容包括禁止被无限制复制的内容或者以复制数据的形式分发的内容，以及限制于可使用时间段的内容。注意，当将这样的使用受控内容记录在存储卡 31 中时，同时记录对应于该内容的使用控制信息项（使用规则）。

[0219] 作为使用控制信息项（使用规则），记录有与内容的使用有关的信息项，比如内容的准许的可使用时间段和内容的准许的复制次数。

[0220] 内容提供装置与内容对应地并且与内容一起提供这种使用控制信息项。

[0221] (a)内容提供装置是内容比如音乐作品和电影的提供源。作为内容提供装置的示例,图 1 示出了广播电台 11 和内容服务器 12。

[0222] 广播电台 11 比如电视台在陆地波或通过卫星的卫星波上向用户装置[(b)内容记录/再现装置(主机)]提供各种广播内容。

[0223] 内容服务器 12 是通过网络比如因特网提供内容比如音乐作品和电影的服务器。

[0224] 例如,用户将存储卡 31 作为(c)内容记录介质插入(b)内容记录/再现装置(主机)中。以此方式,经由(b)内容记录/再现装置(主机)自身的接收单元或连接到内容记录/再现装置(主机)的接收装置来接收由广播电台 11 和内容服务器 12 提供的内容,并且将其记录在存储卡 31 中。

[0225] (b)内容记录/再现装置(主机)将存储卡 31 认作(c)内容记录介质,以将从作为(a)内容提供装置的广播电台 11 和内容服务器 12 接收的内容记录在存储卡 31 中。

[0226] (b)内容记录/再现装置(主机)包括专用记录/再现装置 21(CE 装置:消费品电子装置)21,比如 DVD 播放器,其设置有盘比如硬盘、DVD 和 BD。另外,(b)内容记录/再现装置(主机)包括 PC22 和移动终端 23 比如智能电话、移动电话、移动播放器和平板终端。所有这些都是能够将存储卡 31 认作(c)内容记录介质的装置。

[0227] 通过使用专用记录/再现装置 21、PC 22 和移动终端 23 等,用户从广播电台 11 和内容服务器 12 接收内容比如音乐作品和电影,并且将这些内容记录在存储卡 31 中。

[0228] 参照图 2 描述如何使用记录在存储卡 31 中的内容。

[0229] 作为信息存储装置的存储卡 31 是相对于内容再现装置比如 PC 可拆卸的记录介质,因此可以与从其记录了内容的装置自由地分离,并且还可以插入到其他的用户装置中。

[0230] 具体地,如图 2 所示,执行下述处理。

[0231] (1)记录处理

[0232] (2)再现处理

[0233] 注意,一些设备只执行记录和再现的其中之一。

[0234] 另外,不一定由同一装置执行记录处理和再现处理,从而,用户可以自由地选择和使用记录装置或再现装置。

[0235] 注意,在很多情况下,记录在存储卡 31 中的使用受控内容被记录为加密内容。内容再现装置比如专用记录/再现装置 21、PC 22 和移动终端 23 基于预定序列执行解密处理,然后再现该内容。

[0236] 另外,在与内容对应地设置的使用控制信息项(使用规则)中记录的使用准许模式下执行再现处理等。

[0237] (b)内容记录/再现装置(主机)存储了程序(主机应用),该程序被配置成基于使用控制信息项(使用规则)来执行内容使用处理和内容解密处理。基于该程序(主机应用)来再现内容。

[0238] [2. 存储卡的配置示例和使用示例]

[0239] 接下来,描述用作用于内容记录的记录介质的存储卡比如闪存的配置示例和使用示例。

[0240] 图 3 示出了存储卡 31 中的存储区域的具体配置示例。

[0241] 如图 3 所示,存储卡 31 的存储区域由下述两个区域组成。

[0242] (a)保护区域 51

[0243] (b)通用区域 52

[0244] (b)通用区域 52 是用户使用的记录 / 再现装置可以自由访问的区域,并且记录内容、与内容对应的使用控制信息项(使用规则)、以及其他通用内容管理数据项等。

[0245] 在通用区域 52 中,可以例如由服务器或者用户的记录 / 再现装置自由地读取和写入数据。

[0246] 同时,(a)保护区域 51 是不准许自由访问的区域。

[0247] 将保护区域 51 划分成块(#0、#1、#2、…)作为多个分段区域,并且在各块单元中设置访问权限。

[0248] 例如,当例如利用由用户使用的记录 / 再现装置或由通过网络连接的服务器使用的记录 / 再现装置读取或者写入数据时,存储卡 31 的数据处理单元基于预存储在存储卡 31 中的程序来确定是否能够在与装置对应的块单元内执行读取或者写入。

[0249] 存储卡 31 不仅包括被配置成执行预存储的程序的数据处理单元,还包括被配置成执行认证处理的认证处理单元。首先,存储卡 31 执行对于要针对存储卡 31 读取或者写入数据的装置的认证处理。

[0250] 在认证处理阶段,从对方装置即访问请求装置接收包括公开密钥证书等的装置证书。

[0251] 例如,当访问请求装置是服务器时,接收由服务器持有的服务器证书。之后,基于证书中包含的信息来判断是否准许访问保护区域 51 的块(分段区域)的单元。

[0252] 同时,当访问请求装置是主机装置比如作为用户装置的被配置成记录和再现内容的记录 / 再现装置(主机)时,接收由记录 / 再现装置(主机)持有的主机证书。之后,基于该证书中包含的信息判断是否准许访问保护区域 51 的块(分段区域)。

[0253] 在图 3 所示的保护区域 51 中的块(图 3 所示的区域 #0、#1、#2、…)的单元中执行该访问权限的判断处理。存储卡 31 使服务器或者主机只执行块的单元中准许的处理(处理比如数据的读 / 写)。

[0254] 将对于介质的读 / 写限制信息项(PAD 读 /PAD 写)设置在要访问该介质的装置比如内容服务器或者记录 / 再现装置(主机)的单元中。将这些信息项记录在与装置对应的服务器证书和主机证书中。

[0255] 注意,术语“证书(certification)”在下文中被简写为“证书(cert)”。

[0256] 如上所述,存储卡 31 基于预存储在存储卡 31 中的管理程序来验证服务器证书和主机证书中的记录数据项,之后执行仅对访问准许区域准许访问的处理。

[0257] [3. 包含针对保护区域的访问准许信息项的证书 ]

[0258] 接下来,参照图 4 和图 5 描述当服务器或主机装置(即记录 / 再现装置)作为用户装置访问存储卡 31 中的上述保护区域 51 时,要求呈现给存储卡的证书的配置示例。

[0259] 如上所述,存储卡 31 执行对于要针对存储卡 31 读取或写入数据的装置的认证处理。在认证处理的阶段,从对方装置即访问请求装置接收包含公开密钥证书等的装置证书比如服务器证书或主机证书。然后,基于包含在证书中的信息来判断是否准许访问保护区域 51 的分段区域。

[0260] 作为该认证处理中使用的装置证书的示例,将参照图 4 描述要存储在用户装置

(主机装置)比如图 1 所示的专用记录 / 再现装置 21、PC 22 和移动终端 23 中的主机证书的配置示例。

[0261] 例如由作为发行公开密钥证书的主体的证书授权机构将主机证书提供给对应的用户装置(主机装置)。例如,主机证书是由证书授权机构给证书授权机构准许执行内容使用处理的用户装置(主机装置)发行的证书,换言之,存储了公开密钥等的证书。用证书授权机构秘密密钥来设置主机证书的签名。以此方式,主机证书被配置成防篡改的数据项。

[0262] 注意,可以在制造装置时基于装置的类型等的确认结果将装置证书预存储在装置的存储器中。为了在用户购买后获取该证书,可以采用下述配置 :其中,基于装置与证书授权机构或其他管理站之间的预定序列来执行对装置的类型、可使用的内容的类型等进行确认的处理,然后将证书发行给装置并且存储在装置的存储器中。

[0263] 注意,访问存储卡 31 的保护区域的服务器持有与主机证书的公开密钥相同的结构的服务器公开密钥、以及在其中记录了用于准许访问存储卡的信息项的服务器证书。

[0264] 图 4 示出了由证书授权机构提供给主机装置(用户装置)的主机证书的具体示例。

[0265] 如图 4 所示,主机证书包括下述数据项。

[0266] (1)类型信息项

[0267] (2)主机 ID (用户装置 ID)

[0268] (3)主机公开密钥

[0269] (4)保护区域访问权限信息项(对于介质中的保护区域的读 / 写限制信息项(PAD 读 /PAD 写))

[0270] (5)其他信息项

[0271] (6)签名

[0272] 在下文中,描述项(1)到项(6)的数据项。

[0273] (1)类型信息项

[0274] 类型信息项是指示证书类型和用户装置类型的信息项。例如,在类型信息项中,记录了指示证书是主机证书的数据项以及指示装置的类型、具体地指示了装置是 PC、音乐播放器等的数据项。

[0275] (2)主机 ID

[0276] 主机 ID 是在其中记录了作为装置标识信息项的装置 ID 的区域。

[0277] (3)主机公开密钥

[0278] 主机公开密钥是用于主机装置的公开密钥,并且与为主机装置(用户装置)提供的秘密密钥一起被配置成基于公开密钥加密方法的密钥对。

[0279] (4)保护区域访问权限信息项(对于介质中的保护区域的读 / 写限制信息项(PAD 读 /PAD 写))

[0280] 在保护区域访问权限信息项中,记录有被配置为记录例如图 3 所示的存储卡 31 的内容的介质中的存储区域中设置的保护区域(PDA)51 中的块(分段区域)的单元的信息项,块(分段区域)中准许数据项的读取和写入。

[0281] 访问权限被记录为保护区域中的块(分段区域)的单元的访问权限。

[0282] (5)其他信息项和(6)签名

[0283] 在主机证书中,记录了与上述数据项(1)至(4)不同的各种其他信息项,例如关于

信息项(1)至(5)的签名数据项。

[0284] 该签名用来自证书授权机构的秘密密钥执行。当提取主机证书中记录的信息项比如主机公开密钥来使用时,首先,执行应用发行自证书授权机构的公开密钥的签名验证处理,以确认该主机证书没有被篡改。如果确认没有篡改,则使用存储在证书中的数据项比如主机公开密钥。

[0285] 图4示出了记录用于准许从用户装置(主机装置)访问存储卡的保护区域的信息项的主机证书。例如,针对要求访问保护区域的服务器,比如被配置为向存储卡提供内容的内容提供服务器,设置了与图4所示的主机证书类似的证书,该证书[服务器证书(例如,存储服务器公开密钥的公开密钥证书)]记录准许访问存储卡的保护区域的信息项。

[0286] 参照图5描述要提供给服务器的服务器证书的配置示例。注意,在下文的描述中,术语“服务器”包括图1所示的所有内容提供装置,具体地,包括被配置为向用户装置提供内容的装置,比如广播电台11和内容服务器12。

[0287] 由作为发行公开密钥证书的主体的证书授权机构将服务器证书提供给装置例如被配置成提供内容的内容服务器。例如,服务器证书是由证书授权机构发行给由证书授权机构准许执行内容提供处理并且存储服务器公开密钥等的服务器。用证书授权机构秘密密钥来设置服务器证书的签名。以此方式,服务器证书被配置成防篡改的数据项。

[0288] 图5示出了由证书授权机构提供给内容服务器的服务器证书的具体示例。

[0289] 如图5所示,服务器证书包含类似于参照图4所描述的主机证书的下述数据项。

[0290] (1)类型信息项

[0291] (2)服务器ID

[0292] (3)服务器公开密钥

[0293] (4)对于介质的读/写限制信息项(PAD读/PAD写)

[0294] (5)其他信息项

[0295] (6)签名

[0296] 这些信息项类似于参照图4所描述的信息项,因此这里不详细描述。

[0297] 注意,在“(4)对于介质的读/写限制信息项(PAD读/PAD写)”中,针对每个服务器记录有存储卡31中的保护区域51中的块(分段区域)的单元的访问权限(数据读/写准许信息项)。

[0298] 注意,当将记录在服务器证书中的信息项比如服务器公开密钥提取出来使用时,首先,执行应用来自证书授权机构的公开密钥的签名验证处理以确认该服务器证书没有被篡改。如果确认没有篡改,则使用存储在证书中的数据项比如服务器公开密钥。

[0299] [4.参照装置的证书来访问存储卡的处理的示例]

[0300] 如参照图4和图5所述,当服务器或主机装置(用户装置比如记录/再现装置)访问存储卡31中的保护区域51中的块时,需要向存储卡展示如图4和图5所示的证书。

[0301] 存储卡确认如图4和图5所示的证书以判断是否准许访问图3所示的存储卡31中的保护区域51中的块的单元。

[0302] 主机装置拥有例如参照图4所述的主机证书,并且要执行内容提供等的服务器拥有参照图5所述的服务器证书。

[0303] 当这些装置访问存储卡的保护区域时,这些装置有必要给存储卡提供它们的证

书，并且有必要基于存储卡侧的验证来判断是否准许访问。

[0304] 参照图 6 描述在针对存储卡的访问请求装置是服务器的情况下以及是主机装置例如记录 / 再现装置的情况下的设置访问限制的示例。

[0305] 图 6 从左示出了服务器 A 61、服务器 B 62，和作为对于存储卡的访问请求装置的主机装置 63，和存储卡 70。

[0306] 服务器 A 61 和服务器 B 62 提供了例如加密内容（Con1、Con2、Con3、…）作为要记录到存储卡 70 的内容。

[0307] 这些服务器还提供标题密钥（Kt1、Kt2、…）作为对加密内容进行解密的密钥以及与内容对应的使用控制信息项（使用规则 :UR1、UR2、…）。

[0308] 主机装置 63 是执行再现存储在存储卡 70 中的内容的处理的装置。

[0309] 主机装置 63 读取存储在存储卡 70 的通用区域中的加密内容（Con1、Con2、Con3、…）和使用控制信息项（使用规则 :UR1、UR2、…）。另外，主机装置 63 从保护区域 80 中的块（分段区域）81 和 82 中读取要被应用于内容解密处理的标题密钥（Kt1、Kt2、…），之后，参照标题密钥执行解密处理。以此方式，主机装置 63 基于使用控制信息项（使用规则）来使用内容。

[0310] 存储卡 70 包括保护区域 80 和通用区域 90。在通用区域 90 中记录加密内容、使用控制信息项（使用规则）等。

[0311] 在保护区域 80 中记录标题密钥，作为用于内容再现需要的密钥。

[0312] 如上参照图 3 所述，将保护区域 80 划分成多个块（分段区域）。

[0313] 图 6 所示的示例仅示出了下述两个块。

[0314] 块 #0（保护区域 #0）81

[0315] 块 #1（保护区域 #1）82

[0316] 在保护区域 80 中，设置有大量的其他块。

[0317] 可以采用各种块的设置模式。

[0318] 在图 6 示出的示例中，

[0319] 块 #0（保护区域 #0）81 被设置为专用于服务器 A 61 的块，换言之，存储用于解密要从服务器 A 61 提供的内容的标题密钥的区域，以及

[0320] 块 #1（保护区域 #1）82 被设置为专用于服务器 B 62 的块，换言之，存储用于解密要从服务器 B 62 提供的内容的标题密钥的区域。

[0321] 在此设置下，要提供内容的服务器 A 61 在块 #0（保护区域 #0）81 中记录了解密要从其提供的内容需要的标题密钥。

[0322] 在这种情况下，要记录在服务器 A 61 的服务器证书中的写入准许区域信息项（PAD 写）被配置成其中设置了针对块 #0（保护区域 #0）81 的写入准许的证书。

[0323] 注意，在图 6 所示的示例中的设置下，针对准许写入的块也同样准许读取。

[0324] 另外，服务器 B 62 在块 #1（保护区域 #1）82 中记录了解密要从其提供的内容需要的标题密钥。

[0325] 在这种情况下，要记录在服务器 B 62 的服务器证书中的写入准许区域信息项（PAD 写）被配置成其中设置了针对块 #1（保护区域 #1）82 的写入准许的证书。

[0326] 另外，被配置成通过读取块 #0 和块 #1 中记录的标题密钥来执行内容再现的作为

再现装置的主机装置 63 拥有的主机证书被配置成其中设置了针对块 #0 和块 #1 的读取准许的证书。

[0327] 在此示例中，在主机证书中没有设置针对块 #0 和块 #1 两者的写入准许。

[0328] 注意，在删除内容的时候，为了还可以删除与要被删除的内容对应的标题密钥，可以设置删除块 #0 和块 #1 两者的处理的准许。

[0329] 另外，在其他处理中，当主机装置 63 必须向保护区域写入数据时，可以在主机证书中设置写入准许。

[0330] 存储卡 70 中的数据处理单元从访问请求装置比如提供内容的服务器或者使用内容的主机接收针对保护区域 80 的访问请求。然后，数据处理单元参照这些装置的装置证书来确认准许访问块单元的信息项。以此方式，数据处理单元判断是否准许访问块。

[0331] 存储卡 70 响应于来自访问请求装置的数据写入或读取的输入来区分写入请求或读取请求的数据项类型，并且选择块（#0、#1、#2、…）作为数据写入目的单元或者作为数据读取源。

[0332] 如参照图 4 和图 5 所述，在访问请求装置的证书（服务器证书、主机证书等）中记录了访问控制信息项。存储卡首先验证从访问请求装置接收的这些证书的签名以便确认这些证书的有效性。之后，存储卡读取包含在这些证书中的访问控制信息项，即下述信息项。

[0333] 读取准许区域信息项（PAD 读）

[0334] 写入准许区域信息项（PAD 写）

[0335] 基于这些信息项，只准许和执行被准许的要由访问请求装置执行的处理。

[0336] [5. 使用加密内容签名（ECS）发行者的内容提供系统 ]

[0337] 如以上参照图 1 所述，由内容提供装置来提供要被提供给用户装置的内容。但是，在一些情况中，内容提供装置本身提供非法复制的内容。在下文中，描述防止用不同于用户装置的配置的配置进行欺诈行为比如由服务器进行的欺诈性处理的配置。

[0338] 参照图 7，描述根据本公开的实施方式的被配置成防止对内容的欺诈性使用的信息处理系统的总体配置。

[0339] 图 7 示出了该信息处理系统的总体配置的示例。图 7 示出了下述四个类型的装置形成的层级结构。

[0340] （A）许可证发行者（LA）101

[0341] （B）加密内容签名（ECS）发行者 102-1 到 102-n

[0342] （C）内容提供装置（内容服务器）103-1 到 103-m

[0343] （D）用户装置（内容再现装置）104-1 到 104-f

[0344] 图 7 所示的（C）内容提供装置（内容服务器）103-1 到 103-m 对应于图 1 所示的广播电台 11、内容服务器 12 等。

[0345] 另外，图 7 所示的（D）用户装置（内容再现装置）104-1 到 104-f 对应于图 1 所示的用户装置比如专用记录 / 再现装置 21、PC 22 和移动终端 23。

[0346] （C）内容提供装置（内容服务器）103-1 到 103-m 包括各种信息处理装置比如发送内容的装置，更具体地，内容服务器和广播电台，以及例如在媒体中记录内容的装置，并且还包括提供介质比如存储内容的盘的介质提供公司。这些装置大量存在。

[0347] （D）用户装置（内容再现装置）104-1 到 104-f 是下述装置，该装置被配置成通过经

由因特网、广播波或者介质比如光盘从(C)内容提供装置(内容服务器)103-1 到 103-m 接收或读取内容比如电影、音乐作品和其他内容来执行再现处理。具体地,(D)用户装置(内容再现装置)104-1 到 104-f 包括各种能够再现内容的信息处理装置,比如 PC、移动终端、DVD 播放器、BD 播放器和电视。

[0348] (B)加密内容签名(ECS)发行者 102-1 到 102-n 生成与从(C)内容提供装置(内容服务器)103-1 到 103-m 提供的内容对应的加密内容签名文件(ECS 文件)。

[0349] (C)内容提供装置(内容服务器)103-1 到 103-m 针对(B)加密内容签名(ECS)发行者 102-1 到 102-n 发起下述请求,该请求用于生成与要新提供给用户装置 104 的内容比如电影内容对应的这种加密内容签名文件(ECS 文件)。

[0350] 响应于这些请求,(B)加密内容签名(ECS)发行者 102-1 到 102-n 生成并向(C)内容提供装置(内容服务器)103-1 到 103-m 提供加密内容签名文件(ECS 文件)。

[0351] 注意,在下文中详细描述加密内容签名文件(ECS 文件)的具体配置和生成处理。

[0352] (C)内容提供装置(内容服务器)103-1 到 103-m 从(B)加密内容签名(ECS)发行者 102-1 到 102-n 接收加密内容签名文件(ECS 文件),并且将加密内容签名文件(ECS 文件)与加密内容一起提供给(D)用户装置(内容再现装置)104-1 到 104-f。

[0353] 在再现内容之前,(D)用户装置(内容再现装置)104-1 到 104-f 的每一个对加密内容签名文件(ECS 文件)执行签名验证处理。仅在通过签名验证处理确认没有篡改的情况下,允许对内容进行解密和再现。

[0354] 注意,如果通过对加密内容签名文件(ECS 文件)的签名验证确认没有篡改,则(D)用户装置(内容再现装置)104-1 到 104-f 的每一个存储基于执行内容的解密和再现的序列的再现处理程序。基于该再现处理程序,执行内容再现可能性判断处理比如对加密内容签名文件(ECS 文件)的签名验证以及执行内容再现。

[0355] 例如,在通过对加密内容签名文件(ECS 文件)的签名验证确认有一些篡改的情况下,禁止内容的再现。

[0356] (A)许可证发行者(LA)101 向(B)加密内容签名(ECS)发行者 102-1 到 102-n 提供许可证作为发行 ECS 文件的许可证。

[0357] 在通过基于预设置的许可证发行序列确认这些加密内容签名(ECS)发行者是否有效以确认这些加密内容签名(ECS)发行者的有效性之后,(A)许可证发行者(LA)101 向(B)加密内容签名(ECS)发行者 102-1 到 102-n 发行许可证。

[0358] 注意,具体地,许可证是分别用来自许可证发行者(LA)101 的秘密密钥签发的公开密钥证书。公开密钥证书存储了针对(B)加密内容签名(ECS)发行者 102-1 到 102-n 的公开密钥。注意,(A)许可证发行者(LA)101 还向(B)加密内容签名(ECS)发行者 102-1 到 102-n 提供与保存在公开密钥证书中的公开密钥对应的秘密密钥。

[0359] 接下来,参照图 8 描述要在下述三个装置中执行的处理。

[0360] (A)许可证发行者(LA)101

[0361] (B)加密内容签名(ECS)发行者 102

[0362] (C)内容提供装置(内容服务器)103

[0363] 图 8 示出了下述三个装置和要在这些装置中执行的主处理。

[0364] (A)许可证发行者(LA)101

[0365] (B)加密内容签名(ECS)发行者 102

[0366] (C)内容提供装置(内容服务器)103

[0367] 要由许可证发行者(LA)101 执行的处理被表示为处理(A1)和处理(A2)。

[0368] 具体地,如下是要由许可证发行者(LA)101 执行的处理(A1)和处理(A2)的内容。

[0369] 处理(A1):向加密内容签名(ECS)发行者 102 提供具有有效期的 ECS 发行者证书。

[0370] 处理(A2):向内容提供装置 103 提供 ECS 发行者密钥失效列表。

[0371] 要由加密内容签名 (ECS) 发行者 102 执行的处理被表示为处理(B1)和处理(B2)。

[0372] 具体地,如下是要由加密内容签名 (ECS) 发行者 102 执行的处理(B1)和处理(B2)的内容。

[0373] 处理(B1):生成加密内容签名文件(ECS 文件)。

[0374] 处理(B2):向内容提供装置 103 提供加密内容签名文件(ECS 文件)。

[0375] 要由内容提供装置 103 执行的处理被表示为处理(C1)和处理(C2)。

[0376] 具体地,如下是要由内容提供装置 103 执行的处理(C1)和处理(C2)的内容。

[0377] 处理(C1):向加密内容签名(ECS)发行者 102 提供 ECS 文件生成数据项。例如,提供内容哈希列表集、标题密钥的哈希值和块标识符。

[0378] 处理(C2):使用 ECS 文件执行内容提供可能性判断处理。

[0379] [6.ECS 文件的配置示例 ]

[0380] 接下来,描述由加密内容签名(ECS)发行者 102 生成的 ECS 文件的配置示例。

[0381] 图 9 示出了 ECS 文件的配置示例以及 ECS 发行者证书的也被设置成作为 ECS 文件的一个组成数据项的数据项。

[0382] ECS 文件是由加密内容签名(ECS)发行者 102 生成的文件,并且存储从内容提供装置接收的内容哈希列表集、标题密钥的哈希值、块标识符等作为组成数据项。

[0383] 如图 9 的(A)所示,ECS 文件是包含下述数据项的文件。

[0384] (1)内容哈希列表集(哈希列表集)

[0385] (2)ECS 发行时间

[0386] (3)块标识符(PAD 块号)

[0387] (4)ECS 发行者的签名

[0388] (5)ECS 发行者证书

[0389] (6)内容块表格(存储的内容块表格)

[0390] (1)内容哈希列表集(哈希列表集)是由内容提供装置(内容服务器)103 生成的数据项,并且由加密内容签名(ECS)发行者 102 接收。具体地,(1)内容哈希列表集(哈希列表集)是包含哈希值以及哈希值的属性信息项(偏置、长度等的指示例如作为哈希值的源的内容块的位置的信息项)的数据项,该哈希值基于要提供给用户装置的内容、具体地要由用户装置再现的内容比如电影的组成数据项生成。

[0391] (2)ECS 发行日期是在加密内容签名(ECS)发行者 102 中生成 ECS 文件的日期的信息项。

[0392] 该日期的信息项对应于例如(4)ECS 发行者的签名的生成日期。

[0393] (3)块标识符(PAD 块号)是由内容提供装置(内容服务器)103 通知给加密内容签名(ECS)发行者 102 的数据项,更具体地,是指示作为与从内容提供装置 103 提供给用户装

置 104 的内容对应的加密密钥的标题密钥存储在介质的保护区域中的哪些块中的标识符。换言之，(3) 块标识符(PAD 块号) 是指示内容提供装置 103 可以使用介质的保护区域中的哪些块的标识符。

[0394] 如上参照例如图 3 和图 6 所述，提前设置内容提供装置可以使用的介质的保护区域中的哪些块，并且记录这样的访问准许块的信息项。

[0395] (4) ECS 发行者的签名是 ECS 发行者的电子签名。

[0396] 要签发的数据项包括组成数据项，比如内容哈希列表集、ECS 发行日期、块标识符和标题密钥(哈希值)。

[0397] (5) ECS 发行者证书是与 ECS 发行者 102 对应的公开密钥证书，并且如图 9 的(B) 所示，ECS 发行者证书存储了 ECS 发行者 102 的公开密钥等。在下文详细描述该配置。

[0398] (6) 内容块表格(存储的内容块表格) 被设置成如下字段，当在上述内容哈希列表集(哈希列表集) 中记录了与多个内容对应的哈希列表时，在该字段中记录哈希列表与多个内容之间的对应信息项。

[0399] 接下来，描述图 9 的(B) 所示的 ECS 发行者证书的数据结构。

[0400] ECS 发行者证书由许可证发行者(LA)101 生成并且提供给 ECS 发行者 102。ECS 发行者 102 通过向许可证发行者(LA) 101 提供 ECS 发行者证书的生成所需的数据项，来请求 ECS 发行者证书的生成。

[0401] 许可证发行者(LA) 101 响应于该请求生成 ECS 发行者证书。

[0402] 如图 9 的(B) 所示，ECS 发行者证书是包含下述数据项的文件。

[0403] (1) ECS 证书 ID

[0404] (2) 块标识符起始号(起始 PAD 块号)

[0405] (3) 块标识符范围(PAD 块号计数器)

[0406] (4) 发行者证书有效期(有效期)

[0407] (5) ECS 发行者公开密钥

[0408] (6) LA 的签名

[0409] (1) ECS 证书 ID 是 ECS 证书的标识符。

[0410] (2)块标识符起始号(起始PAD块号)是介质中的保护区域中准许访问块的起始号，内容提供装置 103 准许 ECS 发行者 102 访问该块。

[0411] (3) 块标识符范围(PAD 块号计数器) 是指示从介质的保护区域中内容提供装置 103 准许 ECS 发行者 102 访问的访问准许块的起始号开始的范围的信息项。

[0412] (4) 发行者证书有效期(有效期) 是此发行者证书的有效期的信息项。

[0413] (5) ECS 发行者公开密钥是 ECS 发行者的公开密钥。

[0414] (6) LA 的签名是由图 7 和图 8 所示的许可证发行者(LA) 发行的电子签名。具体地，(6) LA 的签名是基于 ECS 发行者证书的上述组成数据项(1) 到(5) 生成的电子签名。

[0415] 图 10 示出了 ECS 文件的语法。

[0416] 图 11 示出了 ECS 发行者证书的语法。

[0417] 注意，下述两个记录在 ECS 发行者证书中的数据项 ：

[0418] (2) 块标识符起始号(起始 PAD 块号)

[0419] (3) 块标识符范围(PAD 块号计数器) 是指示如上所述介质的保护区域中的准许访

问块的信息项，其中，内容提供装置 103 准许 ECS 发行者 102 对准许访问块进行访问。

[0420] 具体地，当设置了关系：块标识符起始号≤ N ≤块标识符起始号 + 块标识符范围时，满足此关系的所有整数 N 被设置成块标识符。

[0421] 另外，当块标识符起始号被设置成 0XFFFFFFFF 时，介质的保护区域中的所有块都是准许访问块。

[0422] 注意，尽管在参照图 9 到图 11 所示的示例中 ECS 文件包含 ECS 发行者证书，但是 ECS 文件不一定包含 ECS 发行者证书，并且 ECS 文件和 ECS 发行者证书可以被配置成单独的文件。

[0423] [7. ECS 发行者密钥失效列表的结构 ]

[0424] 接下来，参照图 12 描述 ECS 发行者密钥失效列表的结构。

[0425] 如上参照图 8 所述，ECS 发行者密钥失效列表是由许可证发行者（LA）101 发行的列表。该列表例如在内容提供装置 103 中使用。

[0426] 许可证发行者（LA）101 使被判断是欺诈性的存储 ECS 发行者的公开密钥的 ECS 发行者证书（参照图 9 的（B））作废，然后生成 ECS 发行者密钥失效列表作为登记作废的 ECS 发行者（具体地，作废的 ECS 发行者证书）的标识符（ID）的列表。

[0427] 如图 12 所示，ECS 发行者密钥失效列表存储下述数据项。

[0428] （1）版本

[0429] （2）条目的数量

[0430] （3）失效的（作废的）ECS 发行者证书的 ID

[0431] （4）失效的（失效的）ECS 发行者证书的失效日期

[0432] （5）许可证发行者（LA）101 的电子签名

[0433] （5）许可证发行者（LA）101 的电子签名是针对数据项（1）到（4）的每个数据项的电子签名。

[0434] 注意，当新发现欺诈性的 ECS 发行者时，通过添加该欺诈性的 ECS 发行者的 ID 来更新 ECS 发行者密钥失效列表为新的版本，并且继而将其发行以提供给内容提供装置 103。

[0435] [8. 加密内容签名文件（ECS 文件）的生成处理 ]

[0436] 接下来，参照图 13 描述加密内容签名文件（ECS 文件）的生成处理。

[0437] 加密内容签名文件（ECS 文件）是由加密内容签名（ECS）发行者 102 基于来自内容提供装置（内容服务器）103 的生成请求而生成的。

[0438] 内容提供装置（内容服务器）103 针对加密内容签名（ECS）发行者 102 发出生成与要新提供给用户装置 104 的内容比如电影内容对应的这种加密内容签名文件（ECS 文件）的请求。

[0439] 响应于该请求，加密内容签名（ECS）发行者 102 生成并且向内容提供装置（内容服务器）103 提供加密内容签名文件（ECS 文件）。

[0440] 图 13 是在该加密内容签名（ECS）的生成处理过程中要由内容提供装置（内容服务器）103 和加密内容签名（ECS）发行者 102 执行的处理的说明图。

[0441] 如图 13 所示，在发出生成新的加密内容签名文件（ECS 文件）的请求时，内容提供装置（内容服务器）103 生成内容哈希列表集（哈希列表集）183，该内容哈希列表集（哈希列表集）183 包含基于内容 181 的组成数据项（内容块）生成的哈希值。

[0442] 注意，将内容哈希列表集(哈希列表集)183生成为存储了基于要提供给用户装置104的加密内容的组成数据项(内容块)而生成的哈希值的内容哈希列表集。

[0443] 内容提供装置(内容服务器)103向加密内容签名(ECS)发行者102提供这样生成的内容哈希列表集(哈希列表集)183。

[0444] 另外，还向加密内容签名(ECS)发行者102提供作为要被应用于内容181的加密的加密密钥的标题密钥182或者该标题密钥的哈希值。

[0445] 内容哈希列表集(哈希列表集)183是包含了基于要提供给用户装置的内容——具体地，要由用户装置再现的内容比如电影——的组成数据项生成的哈希值、以及该哈希值的属性信息项的数据项。

[0446] 注意，属性信息项包括例如已计算了其哈希值的内容块的位置信息的属性信息项。

[0447] 在图13所示的步骤S11中，加密内容签名(ECS)发行者102生成与从内容提供装置(内容服务器)103接收的数据项以及ECS文件的组成数据项对应的签名，具体地，与下述数据项对应的签名。

[0448] 内容哈希列表集

[0449] ECS发行日期

[0450] 块标识符

[0451] 标题密钥(哈希)

[0452] 在生成这些签名的数据项时，应用加密内容签名(ECS)发行者102拥有的秘密密钥。例如，基于ECDSA算法生成签名。

[0453] 如图13所示，这样生成的签名被设置成加密内容签名文件(ECS文件)的组成数据项。

[0454] 如以上参照图9的(A)所述，由加密内容签名(ECS)发行者102生成的加密内容签名文件(ECS文件)200包含下述数据项作为组成数据项。

[0455] (1)内容哈希列表集(哈希列表集)

[0456] (2)ECS发行日期

[0457] (3)块标识符(PAD块号)

[0458] (4)ECS发行者的签名

[0459] (5)ECS发行者证书

[0460] (6)内容块表格(存储的内容块表格)

[0461] [9.应用ECS文件和ECS发行者证书的日期信息项的处理]

[0462] 接下来，描述应用ECS文件和ECS发行者证书的日期信息项的处理。

[0463] 如参照图9所述，在下述文件中记录各种日期信息项。

[0464] (1)由ECS发行者102生成的并且提供给内容提供装置的ECS文件

[0465] (2)由许可证发行者(LA)101生成的并且提供给ECS发行者102的ECS发行者证书

[0466] 例如，在ECS文件中记录了ECS发行日期。

[0467] 另外，在ECS发行者证书中记录了发行者证书有效期(有效期)。

[0468] 内容提供装置103通过应用在这些ECS文件和ECS发行者证书中记录的日期信息

项以及以上参照图 12 描述的 ECS 发行者密钥失效列表，来执行针对用户装置 104 判断内容提供处理的可能性的处理。

[0469] 同时，从内容提供装置 103 接收内容的用户装置 104，通过应用在 ECS 文件和 ECS 发行者证书中记录的日期信息项以及以上参照图 12 描述的 ECS 发行者密钥失效列表，来执行判断用户装置 104 中的内容再现处理的可能性的处理。

[0470] 在下文中，描述这些处理。

[0471] 首先，参照图 14 和图 15 的序列图描述加密内容签名文件（ECS 文件）的生成、内容提供和使用处理序列。

[0472] 图 14 从其左手边起示出了下述装置。

[0473] 许可证发行者 101

[0474] 加密内容签名（ECS）发行者 102

[0475] 内容提供装置 103

[0476] 将步骤 S111 和 S121 到 S128 的处理示出为时序处理。

[0477] 描述这些步骤的处理。

[0478] 步骤 S111

[0479] 在步骤 S111 中，许可证发行者 101 向加密内容签名（ECS）发行者 102 发行许可证（ECS 发行者证书）。

[0480] 如上参照例如图 8 所述，许可证发行者 101 针对加密内容签名（ECS）发行者 102 提供许可证作为发行 ECS 文件的许可证，即 ECS 发行者证书。

[0481] 许可证发行者（LA）101 在通过基于预设的许可证发行序列来确认加密内容签名（ECS）发行者 102 是否有效，从而确认该加密内容签名（ECS）发行者 102 的有效性之后，向该加密内容签名（ECS）发行者 102 发行 ECS 发行者证书。

[0482] ECS 发行者证书是具有参照图 9 的（B）所描述的数据结构的公开密钥证书。ECS 发行者证书存储该加密内容签名（ECS）发行者 102 的公开密钥。注意，许可证发行者（LA）101 还向加密内容签名（ECS）发行者 102 提供与存储在该加密内容签名（ECS）发行者证书中的公开密钥对应的秘密密钥。

[0483] 步骤 S121 到 S124 对应于参照图 13 所描述的加密内容签名文件（ECS 文件）的生成处理的序列。

[0484] 针对要由内容提供装置 103 提供给用户装置的每个内容顺序地执行该处理，以便获取与每个要新提供的内容对应的加密内容签名文件（ECS 文件）。

[0485] 在加密内容签名（ECS）发行者 102 和内容提供装置 103 之间执行该处理。

[0486] 首先，在步骤 S121 中，内容提供装置 103 生成加密内容签名文件（ECS 文件）的生成所需的数据项。

[0487] 具体地，如参照图 13 所述，执行内容哈希列表集（哈希列表集）183 的生成处理等。

[0488] 如上所述，内容哈希列表集（哈希列表集）是包含哈希值以及哈希值的属性信息项的数据项，该哈希值基于要提供给用户装置的内容、具体地要由用户装置再现的内容比如电影的组成数据项生成。

[0489] 注意，属性信息项包括例如计算了其哈希值的内容块的位置信息。

[0490] 注意，内容提供装置 103 生成要被应用于内容的加密处理和解密处理的标题密钥

和该标题密钥的哈希值，作为要被提供给加密内容签名（ECS）发行者 102 的数据项。

[0491] 接下来，在步骤 S122 中，内容提供装置 103 通过向加密内容签名（ECS）发行者 102 发送生成的数据项，来请求加密内容签名文件（ECS 文件）的生成和发送。

[0492] 接下来，在步骤 S123 中，加密内容签名（ECS）发行者 102 执行针对从内容提供装置 103 接收的数据项的签名生成处理。

[0493] 换言之，加密内容签名（ECS）发行者 102 执行参照图 13 所描述的步骤 S11 的签名生成处理。

[0494] 另外，加密内容签名（ECS）发行者 102 生成具有如上参照图 9 的（A）所描述的数据结构的加密内容签名文件（ECS 文件），并且在步骤 S124 中，向内容提供装置 103 发送这样生成的加密内容签名文件（ECS 文件）。

[0495] 如上参照图 9 的（A）所述，加密内容签名文件（ECS 文件）包含下述数据项。

[0496] （1）内容哈希列表集（哈希列表集）

[0497] （2）ECS 发行日期

[0498] （3）块标识符（PAD 块号）

[0499] （4）ECS 发行者的签名

[0500] （5）ECS 发行者证书

[0501] （6）内容块表格（存储的内容块表格）

[0502] 在接收到加密内容签名文件（ECS 文件）之后，在步骤 S125 中，内容提供装置 103 执行内容提供可能性判断处理，该内容提供可能性判断处理判断是否准许提供应用了该加密内容签名文件（ECS 文件）的内容。

[0503] 在步骤 S126 中，在已经判断出准许提供该内容的情况下，在步骤 S127 中执行针对用户装置的内容提供处理。

[0504] 同时，在步骤 S126 中，在已经判断出不准许提供该内容的情况下，流程进行到步骤 S128 以取消内容提供处理。

[0505] 注意，参照图 16 和随后的图更加详细地描述步骤 S125 至步骤 S128 的处理。

[0506] 接下来，参照图 15 描述从内容提供装置 103 到用户装置 104 的内容提供以及在用户装置 104 中的内容再现序列。

[0507] 图 15 从其左手边起示出了下述内容。

[0508] 内容提供装置 103

[0509] 用户装置 104

[0510] 首先，在步骤 S131 中，内容提供装置 103 向用户装置 104 发送下述数据项。

[0511] （1）加密内容

[0512] （2）加密内容签名文件（ECS 文件）

[0513] （3）标题密钥

[0514] 注意，作为步骤 S131 的处理的预处理，已经从用户装置 104 向内容提供装置 103 发出了例如向用户装置 104 发送内容的请求。内容提供装置 103 根据来自用户装置 104 的请求提供内容。

[0515] 注意，

[0516] 在步骤 S131 中要从内容提供装置 103 发送的（1）加密内容是用与该内容对应地

设置的上述“(3)标题密钥”加密的内容。

[0517] 另外，

[0518] (2)加密内容签名文件(ECS 文件)是与上述(1)加密内容对应地生成的文件，并且存储了以上参照图 9 所描述的加密内容签名文件(ECS 文件)的组成数据项。

[0519] 用户装置 104 接收这些数据项并且将其存储在介质比如硬盘中。

[0520] 之后，在执行再现内容的处理时，执行图 15 所示的步骤 S132 和后续步骤的处理。

[0521] 在步骤 S132 中，用户装置 104 读取与要再现的内容对应的加密内容签名文件(ECS 文件)，并且应用该加密内容签名文件(ECS 文件)，以便执行判断是否准许内容的再现的内容再现可能性判断处理。

[0522] 在步骤 S133 中，在已经判断出准许内容的再现的情况下，在步骤 S134 中执行内容再现处理。

[0523] 同时，在步骤 S133 中，在已经判断出不准许内容的再现的情况下，流程进行到步骤 S135 以取消内容再现处理。

[0524] 注意，以下参照图 18 更详细地描述步骤 S132 到步骤 S135 的处理。

[0525] 接下来，参照图 16 和 17 中所示的流程图来描述参照图 14 所描述的内容提供装置中的步骤 S125|S128 的子程序，换言之，描述应用加密内容签名文件(ECS 文件)的内容提供可能性判断处理的详细序列。

[0526] 作为图 16 所示的流程图中的步骤 S151 的预处理，内容提供装置应用 ECS 发行者的签名来执行签名验证，该 ECS 发行者的签名设置在从加密内容签名(ECS)发行者接收的加密内容签名文件(ECS 文件)中。

[0527] 在通过该签名验证确认没有篡改的情况下，换言之，在已经确认了加密内容签名文件(ECS 文件)的有效性的情况下，执行存储在加密内容签名文件(ECS 文件)中的 ECS 发行者证书的另一个签名验证。如果在两个签名验证处理中都确认没有篡改则执行步骤 S151 和后续步骤的处理。

[0528] 在两个签名验证处理的至少一个中已经确认有篡改的情况下，不确认加密内容签名文件(ECS 文件)的有效性或者 ECS 发行者证书的有效性。因此，不执行步骤 S151 和后续步骤的处理。在此情况下，也不执行内容提供处理。

[0529] 在通过加密内容签名文件(ECS 文件)和 ECS 发行者证书的两个签名认证处理确认没有篡改的情况下，换言之，在已经确认了加密内容签名文件(ECS 文件)的有效性和 ECS 发行者证书的有效性的情况下，内容提供装置执行步骤 S151 的处理。

[0530] 内容提供装置读取作为记录在加密内容签名文件(ECS 文件)中的数据项的 ECS 发行日期，然后读取作为记录在 ECS 发行者证书中的数据项的 ECS 发行者证书有效期(有效期)。

[0531] 另外，内容提供装置通过对比这些日期信息项来判断 ECS 发行者证书有效期(有效期)是否先于 ECS 发行日期。

[0532] 在已经判断出 ECS 发行者证书有效期(有效期)先于 ECS 发行日期(是)的情况下，流程进行到步骤 S156 以取消加密内容的分发。

[0533] 同时，在已经判断出 ECS 发行者证书有效期(有效期)不是先于 ECS 发行日期(否)的情况下，流程进行到步骤 S152，以在 S153 和后续步骤中开始应用在加密内容签名文件

(ECS 文件)和 ECS 发行者证书中记录的日期信息项(时间戳)的内容提供可能性判断处理。

[0534] 在步骤 S153 中,将 ECS 发行者证书有效期(有效期)与内容提供装置的时钟或者从可靠时间信息提供服务器获取的实际时间作比较。

[0535] 在已经判断出 ECS 发行者证书有效期(有效期)先于实际时间一天或者更多的情况下,流程进行到步骤 S156 以取消内容提供处理。

[0536] 同时,在已经判断出 ECS 发行者证书有效期(有效期)没有先于实际时间一天或者更多的情况下,流程进行到步骤 S154。

[0537] 在步骤 S154 中,将 ECS 发行日期与内容提供装置的时钟或者从可靠时间信息提供服务器获取的实际时间作比较。

[0538] 在已经判断出 ECS 发行日期先于实际时间一天或者更多的情况下,流程进行到步骤 S156 以取消内容提供处理。

[0539] 同时,在已经判断出 ECS 发行日期没有先于实际时间一天或者更多的情况下,流程进行到步骤 S155。

[0540] 接下来,参照图 17 所示的流程图描述要在步骤 S155 和后续步骤中执行的应用失效列表的内容提供可能性判断处理。

[0541] 注意,内容提供装置已经提前获取了参照图 12 所描述的 ECS 发行者密钥失效列表。可以从例如许可证发行者(LA)101 获取 ECS 发行者密钥失效列表。

[0542] 在步骤 S161 中,内容提供装置从 ECS 发行者证书中获取 ECS 证书 ID,并且判断该 ID 是否已经登记在 ECS 发行者密钥失效列表中。

[0543] 在该 ID 没有登记在 ECS 发行者密钥失效列表中(否)的情况下,确认该 ECS 发行者证书是有效的而没有作废(失效)。在此情况下,流程进行到步骤 S164 以执行内容提供处理。

[0544] 同时,在步骤 S161 中,在判断出该 ECS 证书 ID 登记在 ECS 发行者密钥失效列表中(是)的情况下,流程进行到步骤 S162。

[0545] 在步骤 S162 中,互相比较下述两个日期数据项。

[0546] 登记在 ECS 发行者密钥失效列表中的 ECS 发行者证书被作废(失效)的日期,即失效日期

[0547] 作为加密内容签名文件(ECS 文件)中记录的数据项的 ECS 发行日期

[0548] 在已经判断出作为加密内容签名文件(ECS 文件)中记录的数据项的 ECS 发行日期先于失效日期(是)的情况下,流程进行到步骤 S164 以执行内容提供处理。

[0549] 这是因为内容提供处理可以被判断成基于未失效的有效 ECS 发行者证书的处理。

[0550] 同时,在步骤 S162 中,在已经判断出作为加密内容签名文件(ECS 文件)中记录的数据项的 ECS 发行日期没有先于失效日期(否)的情况下,流程进行到步骤 S163 以取消内容提供处理。

[0551] 这是因为取消内容提供处理可以被判断为基于失效的作废 ECS 发行者证书的处理。

[0552] 接下来,参照图 18 所示的流程图来详细描述以上参照图 14 的步骤 S132 到步骤 S135 所描述的应用用户装置 104 中的加密内容签名文件(ECS 文件)的内容再现可能性判断处理。

[0553] 注意，在图 18 所示的步骤 S171 之前，用户装置执行应用 ECS 发行者的签名的签名验证，该 ECS 发行者的签名设置在从内容提供装置接收的加密内容签名文件（ECS 文件）中。

[0554] 在通过该签名验证确认没有篡改的情况下，换言之，在确认了加密内容签名文件（ECS 文件）的有效性的情况下，执行存储在加密内容签名文件（ECS 文件）中的 ECS 发行者证书的另一个签名验证。如果两个签名验证处理中都确认没有篡改，则执行步骤 S171 和后续步骤的处理。

[0555] 在两个签名验证处理的至少一个中已经确认有篡改的情况下，不确认加密内容签名文件（ECS 文件）的有效性或者 ECS 发行者证书的有效性。因此，不执行步骤 S171 和后续步骤的处理。在此情况下，也不执行内容再现处理。

[0556] 在通过加密内容签名文件（ECS 文件）和 ECS 发行者证书的两个签名认证处理确认没有篡改的情况下，换言之，在已经确认了加密内容签名文件（ECS 文件）的有效性和 ECS 发行者证书的有效性的情况下，用户装置执行步骤 S171。

[0557] 在步骤 S171 中，用户装置读取在加密内容签名文件（ECS 文件）中记录的数据项 ECS 发行日期，然后读取在 ECS 发行者证书中记录的数据项 ECS 发行者证书有效期（有效期）。

[0558] 另外，通过对比这些日期信息项，用户装置判断 ECS 发行者证书有效期（有效期）是否先于 ECS 发行日期。

[0559] 在已经判断出 ECS 发行者证书有效期（有效期）先于 ECS 发行日期（是）的情况下，流程进行到步骤 S175 以取消对内容的解密处理和再现处理。

[0560] 这是因为确认了 ECS 发行者证书已经过期。

[0561] 同时，在步骤 S171 中，在已经判断出 ECS 发行者证书有效期（有效期）没有先于 ECS 发行日期（否）的情况下，流程进行到步骤 S172 以执行步骤 S173 和后续步骤中的应用失效列表的内容提供可能性判断处理。

[0562] 注意，用户装置预先已经获取了参照图 12 所描述的 ECS 发行者密钥失效列表。该 ECS 发行者密钥失效列表可以从例如许可证发行者（LA）101 获取。

[0563] 在步骤 S173 中，用户装置从 ECS 发行者证书获取 ECS 证书 ID，并且判断该 ID 是否登记在 ECS 发行者密钥失效列表中。

[0564] 在该 ID 没有登记在 ECS 发行者密钥失效列表（否）中的情况下，确认该 ECS 发行者证书是有效的而没有作废（失效）。在此情况下，流程进行到步骤 S176 以执行内容再现处理。

[0565] 注意，在开始内容再现处理之前，不仅执行了获取和生成要被应用于解密该加密内容的标题密钥的处理，还执行了应用加密内容签名文件中包含的内容哈希列表集的哈希值验证处理。在通过哈希值验证确认内容中没有篡改的情况下，准许内容的再现。

[0566] 同时，在步骤 S173 中，在判断出该 ECS 发行者证书 ID 登记在 ECS 发行者密钥失效列表（是）中的情况下，流程进行到步骤 S174。

[0567] 在步骤 S174 中，互相比较下述两个日期数据项。

[0568] 登记在 ECS 发行者密钥失效列表中的 ECS 发行者证书作废（失效）的日期，即失效日期

[0569] 在加密内容签名文件（ECS 文件）中记录的数据项 ECS 发行日期

[0570] 在已经判断出在加密内容签名文件(ECS 文件)中记录的数据项 ECS 发行日期先于失效日期(是)的情况下,流程进行到步骤 S176 以执行内容再现处理。

[0571] 这是因为内容再现处理可以被判断为基于未失效的有效 ECS 发行者证书的处理。

[0572] 同时,在步骤 S173 中,在已经判断出在加密内容签名文件(ECS 文件)中记录的数据项 ECS 发行日期没有先于失效日期(否)的情况下,流程进行到步骤 S175 以取消内容再现处理。

[0573] 这是因为取消内容再现处理可以被判断为基于失效的作废 ECS 发行者证书的处理。

[0574] [10. 相关加密密钥和 ECS 发行者的签名的配置 ]

[0575] 接下来,描述将加密密钥和 ECS 发行者的签名彼此相关的配置。

[0576] 如以上参照图 3 和图 6 所述,在用户装置 104 中,内容等在被使用同时被记录在例如由闪存等形成的存储卡等中。

[0577] 如以上参照图 3 所述,存储卡 31 中的存储区域由下述两个区域形成。

[0578] (a) 保护区域 51

[0579] (b) 通用区域 52

[0580] (b) 通用区域 52 是从用户使用的记录 / 再现装置能够自由访问的区域,并且记录内容、与内容对应的使用控制信息项(使用规则)、以及其他通用内容管理数据项等。

[0581] 在通用区域 52 中,可以例如由服务器或者用户的记录 / 再现装置来自由地写入数据和读取数据。

[0582] 同时,(a) 保护区域 51 是不准许自由访问的区域。

[0583] 保护区域 51 被划分成作为多个分段区域的块(#0、#1、#2、…),并且在块单元中设置了访问权限。

[0584] 例如,当利用由用户使用的记录 / 再现装置或者经由网络连接的服务器使用的记录 / 再现装置写入或者读取数据时,存储卡 31 的数据处理单元基于预存储在存储卡 31 中的程序来确定是否可以在与装置对应的块单元中执行读取或者写入。

[0585] 存储卡 31 不仅包括被配置成执行预存储的程序的数据处理单元,还包括被配置成执行认证处理的认证处理单元。首先,存储卡 31 执行针对要对存储卡 31 的写入数据或者读取数据的装置的认证处理。

[0586] 在认证处理阶段,从对方装置即访问请求装置接收包含公开密钥证书等的装置证书。

[0587] 例如,当访问请求装置是服务器时,接收参照图 5 所描述的服务器拥有的服务器证书。然后,基于该证书中包含的信息来判断是否准许访问保护区域 51 的块(分段区域)的单元。

[0588] 同时,当访问请求装置是主机装置比如作为用户装置的被配置成记录和再现内容的记录 / 再现装置(主机)时,接收由参照图 4 所描述的记录 / 再现装置(主机)所拥有的主机证书。然后,基于该证书中包含的信息来判断是否准许访问保护区域 51 的块(分段区域)。

[0589] 在图 3 所示的保护区域 51 中的块(图 3 所示的区域 #0、#1、#2、…)的单元中执行这样的访问权限判断处理。存储卡 31 使该服务器或者该主机仅执行在块的单元中准许的处理(处理比如数据读取 / 写入)。

[0590] 参照图 19 描述在用户装置 104 接受介质来记录从内容提供装置 103 接收的内容的情况下的数据配置示例。

[0591] 图 19 示出了下述处理的示例，在该处理中，作为内容提供装置的服务器 A 201 向插入到作为用户装置的主机 202 中的存储卡 210 提供和记录加密内容。

[0592] 存储卡 210 包括：

[0593] 保护区域 211，以及

[0594] 通用区域 212。

[0595] 在提供加密内容的处理时，作为内容提供装置的服务器 A 201 向保护区域中的预定块提供要被应用于要提供的内容的加密和解密的标题密钥。

[0596] 服务器 A 201 拥有以上参照图 5 所述的服务器证书。

[0597] 首先，服务器 A201 执行针对存储卡 210 的相互认证处理，并且同时将服务器证书输出到存储卡 210。

[0598] 存储卡 210 确认从服务器 A 201 接收的服务器证书中记录的保护区域访问权限信息项。

[0599] 只有在通过此确认处理而判断出服务器 A 201 具有对块 #0 的访问权限（执行写入的权限）的情况下，才准许服务器 A 201 向设置在存储卡 210 中的保护区域 211 中的块 #0 写入数据。

[0600] 如图 19 所示，服务器 A 201 将要被应用于对要提供的内容进行解密的标题密钥存储在块 #0（保护区域 211 中的 221）中。

[0601] 注意，该标题密钥不是存储成其在保护区域中的形式，而是作为关于标题密钥 Kt 的下述信息项（a）和（b）的串接数据项的哈希值的异或运算的结果。

[0602] （a）使用控制信息项（UR：使用规则）

[0603] （b）ECS 发行者的签名，其是参照图 9 的（A）所描述的 ECS 文件的组成数据项。

[0604] 例如，在保护区域中将与内容（a1）对应的标题密钥：Kt(a1) 存储成下述的标题密钥转换数据项。

[0605] Kt(a1)(+)(UR(a1)||ECSSig(a1))hash

[0606] 注意，

[0607] UR(a1) 表示与内容 a1 对应的使用控制信息项，以及

[0608] ECSSig(a1) 表示 ECS 发行者的签名，其是 ECS 文件的组成数据项并且与内容 a1 对应。

[0609] 另外，作为运算符的符号的含义定义如下。

[0610] (+)：异或运算

[0611] ||：数据项的串接，例如 a||b 表示数据项 a 和数据项 b 的串接数据项。

[0612] hash：哈希值，例如 (a||b)hash 表示数据项 a 和数据项 b 的串接数据项的哈希值。

[0613] 在图 19 所示的示例中，服务器 A 201 在存储卡 210 的通用区域 212 中记录下述内容、使用控制信息项和 ECS 文件。

[0614] 内容：Con(a1)、Con(a2)、和 Con(a3)

[0615] 与内容对应的使用控制信息项（使用规则）：UR(a1)、UR(a2)、和 UR(a3)

[0616] 与内容对应的 ECS 文件：Ecs(a1)、Ecs(a2)、和 Ecs(a3)

[0617] 记录这些内容、使用控制信息项和 ECS 文件的集合。

[0618] 另外，服务器 A 201 在块 #0（存储卡 210 的保护区域 211 中的 221）中记录下述数据项，换言之，记录下述数据项之间的异或（XOR）运算的结果。

[0619] 分别与各内容对应的标题密钥

[0620] 分别与各内容对应的使用控制信息项（使用规则）和 ECS 发行者的签名（ECSSig）的串接数据项的哈希值。

[0621] Kt(a1)(+)(UR(a1)||ECSSig(a1))hash

[0622] Kt(a2)(+)(UR(a2)||ECSSig(a2))hash

[0623] Kt(a3)(+)(UR(a3)||ECSSig(a3))hash

[0624] 注意，如同图 19 所示的服务器由 A 201 执行的处理的示例，例如，另一服务器 B 在保护区域的预定块中存储类似的标题密钥转换数据项，该预定块被准许作为与要从服务器 B 提供的内容（bx）对应的标题密钥的存储区域，例如块 #1 ：

[0625] Kt(bx)(+)(UR(bx)||ECSSig(bx))hash

[0626] 图 20 示出了使用内容的用户装置（主机）202 和存储内容等的存储卡 210。

[0627] 用户装置（主机）202 拥有如上参照图 4 所描述的主机证书。

[0628] 首先，用户装置（主机）202 执行与存储卡 210 的相互认证处理，并且，同时将主机证书输出到存储卡 210。

[0629] 存储卡 210 确认从用户装置（主机）202 接收的主机证书中记录的保护区域访问权限信息项。

[0630] 只有在通过该确认处理已经判断出用户装置（主机）202 具有对块 #0 的访问权限（执行读取的权限）的情况下，才准许用户装置（主机）202 从设置在存储卡 210 中的保护区域 211 中的块 #0 读取数据。

[0631] 在通过相互认证确认了访问权限之后，用户装置（主机）202 执行下述处理以使用内容。

[0632] 首先，用户装置（主机）202 从存储卡中的通用区域 212 获取使用目标内容 ：Con(xy)、对应的使用控制信息项 :UR（xy）、和对应的 ECS 文件 :ECS（xy）。

[0633] 接下来，用户装置（主机）202 参照使用控制信息项 :UR（xy）以确认使用目标内容 ：Con（xy）的标题密钥存储在保护区域中的哪些块中。

[0634] 在使用控制信息项 :UR（xy）中记录了存储使用目标内容 :Con（xy）的标题密钥的块的标识符。

[0635] 在确定保护区域 211 中的哪些块存储了标题密钥后，用户装置（主机）202 执行读取记录在该块中的数据项的处理。

[0636] 例如，从选择的块中读取下述数据项。

[0637] Kt(xy)(+)(UR(xy)||ECSSig(xy))hash

[0638] 接下来，用户装置（主机）202 执行串接下述内容的处理和计算其哈希值的处理。

[0639] 使用控制信息项 :UR（xy）以及

[0640] ECS 发行者的签名（ECSSig（xy）），该 ECS 发行者的签名（ECSSig（xy））存储在 ECS 文件 :ECS（xy）中，该 ECS 文件 :ECS（xy）已从通用区域 212 中读取。

[0641] 换言之，用户装置（主机）202 计算 (UR(xy)||ECSSig(xy))hash 以获得计算结果

P(xy)。

[0642] 之后，通过下述计算获取标题密钥 Kt（xy)。

[0643] [从块中读取的数据项(标题密钥转换数据项)](+)P(xy)

[0644] =(Kt(xy)(+)(UR(xy)||ECSSig(xy))hash)(+)P(xy)

[0645] =(Kt(xy)(+)(UR(xy)||ECSSig(xy))hash)(+)(UR(xy)||ECSSig(xy))hash)

[0646] =Kt(xy)

[0647] 通过这样的计算处理获取标题密钥 Kt(xy)，通过用这样获得的标题密钥来解密该加密内容来使用加密内容。

[0648] 参照图 21 描述在存储卡中记录的数据项的示例。

[0649] 图 21 示出了要由两个不同服务器、即服务器 A 和服务器 B 写入存储卡的数据项的示例。

[0650] 服务器 A 具有对存储卡中的保护区域中的块 #0 的访问权限。

[0651] 同时，服务器 B 具有对存储卡中的保护区域中的块 #1 的访问权限。

[0652] 每个服务器将内容和其他数据项记录到插入在作为用户装置的主机装置的存储卡。

[0653] 要从服务器 A 提供的内容表示为 Con(a1)、Con(a2) 和 Con(a3)。

[0654] 要从服务器 B 提供的内容表示为 Con(b1) 和 Con(b2)。

[0655] 如图 21 所示，服务器 A 将下述数据项记录到存储卡的通用区域。

[0656] 内容 :Con(a1)、Con(a2) 和 Con(a3)

[0657] 分别与内容对应的使用控制信息项(使用规则):UR(a1)、UR(a2)、和 UR(a3)

[0658] 分别与内容对应的 ECS 文件 :Ecs(a1)、Ecs(a2)、和 Ecs(a3)

[0659] 另外，服务器 A 将下述数据项记录到存储卡的保护区域中的块 #0。

[0660] 通过要应用于对上述内容进行解密的标题密钥 :Kt(a1)、Kt(a2) 和 Kt(a3) 的转换而获取的数据项，即，

[0661] Kt(a1)(+)(UR(a1)||ECSSig(a1))hash

[0662] Kt(a2)(+)(UR(a2)||ECSSig(a2))hash

[0663] Kt(a3)(+)(UR(a3)||ECSSig(a3))hash

[0664] 同时，服务器 B 将下述数据项记录到存储卡的通用区域中。

[0665] 内容 :Con(b1) 和 Con(b2)

[0666] 分别与内容对应的使用控制信息项(使用规则):UR(b1) 和 UR(b2)

[0667] 分别与内容对应的 ECS 文件 :Ecs(b1) 和 Ecs(b2)

[0668] 另外，服务器 B 将下述数据项记录到存储卡的保护区域中的块 #1。

[0669] 通过要应用于对上述内容进行解密的标题密钥 :Kt(b1) 和 Kt(b2) 的转换而获取的数据项，即，

[0670] Kt(b1)(+)(UR(b1)||ECSSig(b1))hash

[0671] Kt(b2)(+)(UR(b2)||ECSSig(b2))hash

[0672] 当每个服务器将数据项记录到存储卡的保护区域时，存储卡基于服务器证书中的记录来执行访问权限的确认，即执行针对块执行写入的权限的确认。只有在确认了访问权限的情况下，才执行数据写入。

[0673] 图 22 示出了数据记录的示例，在该示例中，服务器 A 和服务器 B 分别具有对存储卡的保护区域中的块 #0 的访问权限，并且服务器 C 和服务器 D 分别具有对存储卡的保护区域中的块 #1 的访问权限。

[0674] 服务器 A 将下述数据项记录到存储卡中的通用区域。

[0675] 内容 :Con(a1)、Con(a2) 和 Con(a3)

[0676] 分别与内容对应的使用控制信息项(使用规则):UR(a1)、UR(a2)、和 UR(a3)

[0677] 分别与内容对应的 ECS 文件 :Ecs(a1)、Ecs(a2)、和 Ecs(a3)

[0678] 另外，服务器 A 将下述数据项记录到存储卡的保护区域中的块 #0。

[0679] 通过要应用于对上述内容进行解密的标题密钥 :Kt(a1)、Kt(a2) 和 Kt(a3) 的转换而获取的数据项，即，

[0680] Kt(a1)(+)(UR(a1)||ECSSig(a1))hash

[0681] Kt(a2)(+)(UR(a2)||ECSSig(a2))hash

[0682] Kt(a3)(+)(UR(a3)||ECSSig(a3))hash

[0683] 服务器 B 将下述数据项记录到存储卡的通用区域中。

[0684] 内容 :Con(b1) 和 Con(b2)

[0685] 分别与内容对应的使用控制信息项(使用规则):UR(b1) 和 UR(b2)

[0686] 分别与内容对应的 ECS 文件 :Ecs(b1) 和 Ecs(b2)

[0687] 另外，服务器 B 将下述数据项记录到存储卡的保护区域中的块 #0。

[0688] 通过要应用于对上述内容进行解密的标题密钥 :Kt(b1) 和 Kt(b2) 的转换而获取的数据项，即，

[0689] Kt(b1)(+)(UR(b1)||ECSSig(b1))hash

[0690] Kt(b2)(+)(UR(b2)||ECSSig(b2))hash

[0691] 服务器 C 将下述数据项记录到存储卡的通用区域中。

[0692] 内容 :Con(c1)

[0693] 与该内容对应的使用控制信息项 ( 使用规则 ) :UR(c1)

[0694] 与该内容对应的 ECS 文件 :ECS(c1)

[0695] 另外，服务器 C 将下述数据项记录到存储卡的保护区域中的块 #1。

[0696] 通过要应用于对上述内容进行解密的标题密钥 :Kt(c1) 的转换而获取的数据项，即，

[0697] Kt(c1)(+)(UR(c1)||ECSSig(c1))hash

[0698] 服务器 D 将下述数据项记录到存储卡的通用区域中。

[0699] 内容 :Con(d1) 和 Con(d2)

[0700] 分别与内容对应的使用控制信息项(使用规则):UR(d1) 和 UR(d2)

[0701] 分别与内容对应的 ECS 文件 :Ecs(d1) 和 Ecs(d2)

[0702] 另外，服务器 D 将下述数据项记录到存储卡的保护区域中的块 #1。

[0703] 通过要应用于对上述内容的解密的标题密钥 :Kt(d1) 和 Kt(d2) 的转换而获取的数据项，即，

[0704] Kt(d1)(+)(UR(d1)||ECSSig(d1))hash

[0705] Kt(d2)(+)(UR(d2)||ECSSig(d2))hash

[0706] 注意，当执行内容再现的用户装置（主机）从通用区域中选择要再现的内容时，该用户装置（主机）必须确定要再现的内容的标题密钥存储在保护区域中的哪些块中。

[0707] 从与每个内容对应的使用控制信息项（UR）中获取用于确定该块的信息项。

[0708] 参照图 23 描述使用控制信息项的使用示例。图 23 （a)示出了与存储卡中的通用区域中记录的内容 a1 对应的使用控制信息项（使用规则）a1 的具体示例。

[0709] 使用控制信息项（使用规则）中记录了下述数据项

[0710] （1）块标识符（#0）

[0711] （2）标题密钥标识符（a1）

[0712] （3）ECS 文件标识符（a1）

[0713] （1）块标识符是指示下述块的信息项，该块存储了与使用控制信息项（使用规则）UR(a1) 对应的内容 :Con(a1) 的标题密钥 Kt(a1)。

[0714] 在该示例中，块标识符是 #0，因而准许执行内容的再现的用户装置（主机装置）选择块 #0。

[0715] （2）标题密钥标识符是指示如下内容的信息项 :存储在块 #0 中的大量标题密钥中的哪一个是与使用控制信息项（使用规则）UR(a1) 对应的内容 :Con(a1) 的标题密钥。

[0716] 在该示例中，标题密钥标识符是 a1，因而准许用户装置（主机装置）选择标题密钥 Kt(a1)。

[0717] （3）ECS 文件标识符（a1）是用于识别哪个 ECS 文件与内容（a1）对应的信息项。

[0718] 用户装置（主机）参照使用控制信息项 :UR(a1)，以确认与使用目标内容 :Con(a1) 对应的标题密钥存储在保护区域中的哪些块中。然后，用户装置（主机）从确定的块中读取下述数据项。

[0719] Kt(a1)(+)(UR(a1)||ECSSig(a1))hash

[0720] 接下来，用户装置（主机）执行串接下述内容的处理和计算其哈希值的处理。

[0721] 使用控制信息项 :UR(a1) 和

[0722] ECS 发行者的签名（ECSSig(a1)），该 ECS 发行者的签名（ECSSig(a1)）存储在从通用区域读取的 ECS 文件 :ECS （a1）中。

[0723] 换言之，用户装置（主机）计算下式。

[0724] P(a1)=(UR(a1)||ECSSig(a1))hash

[0725] 之后，用户装置（主机）执行下述计算以获得标题密钥 Kt(a1)。

[0726] [ 从块读取的数据项（标题密钥转换数据项）](+)P(a1)

[0727] =(Kt(a1)(+)(UR(a1)||ECSSig(a1))hash)(+)P(a1)

[0728] =(Kt(a1)(+)(UR(a1)||ECSSig(a1))hash)(+)(UR(a1)||ECSSig(a1))hash)

[0729] =Kt(a1)

[0730] 通过这样的计算处理，获取了标题密钥 Kt(a1)，并且通过用这样获得的标题密钥解密该加密内容来使用该加密内容。

[0731] 如上所述，将要记录到存储卡中的保护区域的标题密钥存储成下述内容之间的异或（XOR）运算的结果 :使用控制信息项（UR）和 ECS 发行者的签名（ECSSig）的串接数据项 ; 标题密钥。

[0732] 即使是在要应用于 ECS 发行者的签名（ECSSig）的 ECS 发行者的签名密钥（秘密密

钥）泄露的情况下，这样的处理也可以防止对内容的欺诈性使用。

[0733] 例如，这样的处理使得内容提供服务器或者用户装置能够防止通过应用泄露的ECS发行者的签名密钥（秘密密钥）的欺诈性处理、具体地为替换加密内容的处理而欺诈性地使用内容。

[0734] 注意，替换意指，例如用与某个内容（C1）对应的不同标题密钥（Kt1）来加密其他内容（C2）、（C3）、（C4）、……并且将这样加密的内容提供给用户的处理。

[0735] 这样的处理使得拥有标题密钥（Kt1）的用户装置能够在没有合法购买这些内容的情况下解密和再现该其他内容（C2）、（C3）、（C4）、……。

[0736] 通过将存储卡中的保护区域中记录的标题密钥存储成下述数据之间的异或（XOR）运算的结果：使用控制信息项（UR）和ECS发行者的签名（ECSSig）的串接数据项；以及标题密钥，可以防止上述替换。

[0737] 参照图24和后续图来描述防止替换的这种优点。

[0738] 图24的（a）示出了与内容（C1）对应的有效数据存储结构，以及

[0739] 图24的（b）示出了通过使用内容（C1）对应的标题密钥（Kt1）而对内容（C2）加密所生成的替换的数据项的数据存储结构。

[0740] 在图24的（a）所示的有效数据存储结构中，存储卡中的通用区域存储了下述数据项。

[0741] （a1）用与内容（C1）对应的有效标题密钥（Kt1）加密的加密内容（C1（Kt1））

[0742] （a2）与内容（C1）对应的有效使用控制信息项（UR1）

[0743] （a3）与内容（C1）对应的ECS文件ECS1（C1，Kt1）

[0744] 注意，ECS文件存储了ECS发行者的签名（ECSSig），如以上参照图13所述，该ECS发行者的签名（ECSSig）包含了基于内容（C1）的哈希列表集和标题密钥（Kt1）的哈希值的数据项生成的电子签名。为了阐明此签名数据项的源数据项，将ECS文件ECS1表示为（C1，Kt1）。

[0745] 另外，图24的（a）所示的有效数据存储结构中，将通过标题密钥（Kt1）的转换而获取的数据项即下述数据项记录到存储卡的保护区域中的块N。

[0746] Kt1(+)(UR1||ECS1Sig)hash

[0747] 注意，

[0748] UR1表示与内容（C1）对应的使用控制信息项，以及

[0749] ECS1Sig表示ECS发行者的签名，该ECS发行者的签名是ECS文件的组成数据项并且与内容（C1）对应。

[0750] 另外，作为运算符的符号的含义定义如下。

[0751] （+）：异或运算

[0752] ||：数据项的串接，例如，a||b表示数据项a和数据项b的串接数据项。

[0753] hash：哈希值，例如，（a||b）hash表示数据项a和数据项b的串接数据项的哈希值。

[0754] 例如，恶意的内容提供服务器可以将内容（C1）的标题密钥（Kt1）用作另一内容（C2）的加密密钥，并且将该标题密钥（Kt1）提供给用户。

[0755] 分发这样的非法内容的结果是，在存储卡中存储了图24的（b）所示的“替换数据

项”。

[0756] 在图 24 的(b)所示的“替换数据”存储结构中,在存储卡的通用区域中存储下述数据项。

[0757] (b1)对于内容(C2)用欺诈性标题密钥(Kt1)加密的欺诈性加密内容(C2 (Kt1))

[0758] (b2)欺诈性地对应于内容(C2)的使用控制信息项(UR1)[ 使用控制信息项(UR1)应该对应于内容(C1)]

[0759] (b3)欺诈性地生成的对应于内容(C2)的欺诈性 ECS 文件 ECS2 (C2,Kt1)

[0760] 注意,欺诈性 ECS 文件 ECS2 存储了 ECS 发行者的签名(ECSSig),该 ECS 发行者的签名(ECSSig)包含基于内容(C2)的哈希列表集和与内容(C1)对应的标题密钥(Kt1)的哈希值的数据项参照从 ECS 发行者发行的泄露的签名密钥(秘密密钥)而生成的电子签名。为了阐明该签名数据项的源数据项,将 ECS 文件 ECS2 表示成(C2,Kt1)。

[0761] 另外,在图 24 的(b)所示的“替换数据”存储结构中,将通过标题密钥(Kt1)的转换而获取的数据项即下述数据项记录到存储卡的保护区域中的块 N。

[0762] Kt1(+)(UR1||ECS1Sig)hash

[0763] 参照图 25 所示的流程图来描述图 24 的(b)所示的这些“替换数据项”的记录处理的序列。

[0764] 注意,图 25 所示的处理是通过使用存储了与图 24 的(a)所示的内容(C1)对应的有效数据集的存储卡而执行的处理,更具体地,是通过具有执行数据读取处理的权限作为下述访问权限的内容提供服务器或者用户装置所执行的处理,该访问权限作为针对存储卡的保护区域中的块 N 的访问权限。

[0765] 首先,在步骤 S201 中,准备了新内容 C2。

[0766] 接下来,在步骤 S202 中,从存储卡中的通用区域中记录的内容(C1)的使用控制信息项(UR1)处获取“块标识符”和“标题密钥标识符”。基于这些获取的信息项,根据保护区域中的预定块即标题密钥存储块读取与下述标题密钥转换数据项对应的正常内容(C1)。

[0767] Kt1(+)(UR1||ECS1Sig)hash

[0768] 注意,ECS1Sig 表示 Sign (ECS 签名密钥,M),M 表示内容 C1 的内容哈希列表集与 Kt1 的哈希值的串接数据项。

[0769] 接下来,在步骤 S203 中,计算下述从通用区域读取的与正常内容 (C1)对应的使用控制信息项(UR1)以及 ECS 文件(ECS1 (C1,Kt1)的串接数据项的哈希值。然后,执行该计算结果和上述从保护区域读取的标题密钥转换数据项之间的异或(XOR)运算以获取与内容(C1)对应的正常标题密钥(Kt1)。

[0770] 换言之,基于下述公式获取标题密钥(Kt1)。

[0771] Kt1= (从保护区域读取的数据项) (+) (从通用区域读取的数据项)

[0772] =Kt1(+)(UR1||ECS1Sig)hash(+)(UR1||ECS1Sig)hash

[0773] 注意,(+)表示异或运算(XOR)。

[0774] 接下来,在步骤 S204 中,应用步骤 S203 中获取的标题密钥(Kt1)来加密新内容 C2。

[0775] 以此方式,生成加密内容 C2 (Kt1)。

[0776] 接下来,在步骤 S205 中,在存储卡中的通用区域中记录加密内容 C2 (Kt1)。

[0777] 接下来，在步骤206中，生成加密内容签名ECS2Sig，该加密内容签名ECS2Sig对应于基于内容C2生成的内容哈希列表集和Kt1的哈希值。换言之，生成下述签名数据项。

[0778] ECS2Sig=Sign（ECS签名密钥，M）

[0779] 注意，M表示内容C2的内容哈希列表集与Kt1的哈希值的串接数据项。

[0780] 另外，将由加密内容签名发行者发行的泄露的签名密钥(秘密密钥)应用于该签名的生成。

[0781] 最后，在步骤S207中，生成包含步骤S206中欺诈性地生成的ECS签名(ECS2Sig(C2，Kt1))的ECS文件，并将其记录到存储卡的通用区域。

[0782] 通过图25所示的一系列处理，完成了记录图24的(b)所示的记录“替换数据项”的处理。

[0783] 通过这样的替换处理，生成了通过与不同内容(C1)对应的标题密钥(Kt1)的应用加密的内容C2（Kt1)。

[0784] 注意，在这个示例中，将与内容C1对应的使用控制信息项(UR1)原样用作与非法记录的内容C2（Kt1)对应的使用控制信息项。

[0785] 接下来，参照图26所示的流程图描述用户装置如何通过使用图24的(b)所示的“替换数据项”来执行再现内容C2的处理。

[0786] 首先，在步骤S221中，用户装置从存储卡中的通用区域读取要被再现的加密内容C2（Kt1)和与加密内容C2（Kt1)对应地生成的ECS文件(ECS2（C2，Kt1))。

[0787] 接下来，在步骤S222中，从存储卡中的通用区域中与内容C2对应地记录的使用控制信息项(UR1)中读取指示存储标题密钥的块的标识符。

[0788] 如上所述，在此例中，与内容C1对应的使用控制信息项(UR1)被原样用作与非法记录的内容C2（Kt1)对应的使用控制信息项。

[0789] 如以上参照图23所述，使用控制信息项(UR)记录了指示存储该标题密钥的块的标识符、标题密钥标识符等。

[0790] 在步骤S222中，从与内容C1对应的使用控制信息项(UR1)中读取块标识符和标题密钥标识符。

[0791] 这些块标识符和标题密钥标识符是分别与存储与内容C1对应的正常标题密钥Kt1的块对应的标识符以及与在相同块中存储的标题密钥对应的标识符。

[0792] 因此，这样读取的数据项对应于与内容C1对应的标题密钥转换数据项，即，

[0793] Kt1(+)(UR1||ECS1Sig)hash。

[0794] 接下来，在步骤S223中，计算从通用区域读取的使用控制信息项(UR1)与对应于内容C2欺诈性地生成的ECS文件(ECS2(C2，Kt1))的串接数据项的哈希值。然后，执行该计算结果与上述已经从保护区域读取的标题密钥转换数据项之间的异或(XOR)运算，以便获取与内容C2对应的解密标题密钥Kt2。

[0795] 在此情况下，当这样获取的标题密钥Kt2等于Kt1时，标题密钥获取成功。

[0796] 换言之，进行基于下述公式执行标题密钥计算处理的尝试。

[0797] Kt2=（从保护区域读取的数据项）(+)（从通用区域读取的数据项）

[0798] =Kt1 (+) (UR1||ECS1Sig)hash (+) (UR1||ECS2Sig)hash

[0799] 进行基于该标题密钥计算公式获取标题密钥(Kt2)的尝试。

[0800] 注意，(+)表示异或运算(XOR)。

[0801] 但是，在上述标题密钥计算公式中下述关系成立。

[0802] ECS2Sig ≠ ECS1Sig

[0803] 因此，基于上述计算公式获取的值：Kt2 不等于 Kt1，换言之，下述关系成立。

[0804] Kt2 ≠ Kt1

[0805] 结果，如步骤S224所述，用户装置不能获取应用于内容C2的加密的标题密钥Kt1，所以内容 C2 的解密和再现失败。

[0806] 另外，在步骤S225中，基于预设置的再现序列，用户装置执行验证ECS发行者的签名(ECSSig)的处理，该ECS发行者的签名(ECSSig)包含在从通用区域读取的ECS文件中。

[0807] 基于下述算式执行签名验证处理。

[0808] Verify (ECS发行者公开密钥，ECS2Sig，M)

[0809] 注意，Verify (k，S，M)表示使用验证密钥k来验证与数据项M对应的电子签名S的处理。

[0810] M表示内容C2的内容哈希列表集与Kt2的哈希值的串接数据项。

[0811] 在步骤S223中计算出的值被用作为Kt2。

[0812] ECS文件中存储的ECS2Sig是图25所示的流程的步骤S206中生成的欺诈性签名，即下述数据项。

[0813] ECS2Sig=Sign (ECS签名密钥，M)

[0814] 注意，

[0815] M表示内容C2的内容哈希列表集与Kt1的哈希值的串接数据项。

[0816] 如上所述，要应用于签名验证的数据项M是包含Kt2的哈希值的数据项。同时，ECS文件中存储的签名数据项ECS2Sig是对应于包含Kt1的哈希值的M生成的。

[0817] 因此，如图26中的步骤S226所述，通过步骤S225中的签名验证确认了一些篡改。

[0818] 以此方式，即使当通过使用图24的(b)所示的“替换数据项”来试图解密和再现内容C2时，用户装置具有下述结果。

[0819] 内容C2的解密失败

[0820] 通过ECS文件的签名验证确认了一些篡改

[0821] 结果，不能使用内容C2。

[0822] 参照图24到图26描述的处理示例是试图通过应用与内容C1对应的标题密钥Kt1来加密和解密新内容C2的处理示例。

[0823] 接下来，参照图27和后续图来描述在与内容C1对应的正常使用控制信息项(UR1)被欺诈性地篡改以生成新的使用控制信息项(UR2)的情况下的示例。

[0824] 使用控制信息项记录了内容的可用时间段、复制限制信息项等信息项。因此，通过重写该使用信息控制信息项可以执行例如延长使用有效期的欺诈行为。

[0825] 类似于上述图24，图27包括以下内容。

[0826] 图27的(a)示出了与内容(C1)对应的有效数据存储结构，以及

[0827] 图27的(b)示出了通过使用与内容(C1)对应的标题密钥(Kt1)对内容(C2)加密生成的替换数据项的数据存储结构。

[0828] 在图27的(a)所示的有效数据存储结构中，存储卡中的通用区域存储下述数据

项。

[0829] (a1)使用与内容(C1)对应的有效标题密钥(Kt1)加密的加密内容(C1 (Kt1))

[0830] (a2)与内容(C1)对应的有效使用控制信息项(UR1)

[0831] (a3)与内容(C1)对应的有效 ECS 文件 ECS1 (C1,Kt1)

[0832] 注意,ECS 文件存储了 ECS 发行者的签名(ECSSig),如上参照图 13 所述,该 ECS 发行者的签名(ECSSig)包含基于内容(C1)的哈希列表集和标题密钥(Kt1)的哈希值的数据项生成的电子签名。为了阐明此签名数据项的源数据项,将ECS 文件ECS1 表示成(C1,Kt1)。

[0833] 另外,在图 27 的(a)所示的有效数据存储结构中,将通过标题密钥(Kt1)的转换获取的数据项、即下述数据项记录在存储卡中的保护区域中的块 N。

[0834] Kt1 (+) (UR1||ECS1Sig)hash

[0835] 注意,

[0836] UR1 表示与内容(C1)对应的使用控制信息项,以及

[0837] ECS1Sig 表示 ECS 发行者的签名,该ECS 发行者的签名是 ECS 文件的组成数据项并且与内容(C1)对应。

[0838] 另外,作为运算符的符号的含义定义如下。

[0839] (+):异或运算

[0840] ||:数据项的串接,例如,a||b 表示数据项 a 和数据项 b 的串接数据项

[0841] Hash:哈希值,例如,(a||b)hash 表示数据项 a 和数据项 b 的串接数据项的哈希值。

[0842] 例如,恶意的内容提供服务器或者用户装置可以重写与此内容(C1)对应的使用控制信息项(UR1)。

[0843] 这样的欺诈性处理的结果是将图 27 的(b)所示的“替换数据项”存储在存储卡中。

[0844] 在图 27 的(b)所示的“替换数据”存储结构中,存储卡的通用区域存储下述数据项。

[0845] (b1)用针对内容(C1)欺诈性地生成的标题密钥(Kt2)加密的欺诈性加密内容(C1(Kt2))

[0846] (b2)对应于内容(C1)欺诈性地生成的使用控制信息项(UR2)

[0847] (b3)对应于内容(C1)欺诈性地生成的欺诈性 ECS 文件 ECS2 (C1,Kt2)

[0848] 注意,该欺诈性 ECS 文件 ECS2 存储了 ECS 发行者的签名(ECSSig),该 ECS 发行者的签名(ECSSig)包含基于下述数据项生成的电子签名:内容(C1)的哈希列表集,以及参照从 ECS 发行者发行的泄露的签名密钥(秘密密钥)而欺诈性地生成的标题密钥(Kt2)的哈希值。为了阐明此签名数据项的源数据项,将 ECS 文件 ECS2 表示为(C1,Kt2)。

[0849] 另外,在图 27 的(b)所示的“替换数据项”存储结构中,通过标题密钥(Kt1)的转换获取的数据项,即下述数据项记录到存储卡的保护区域中的块 N。

[0850] Kt1 (+) (UR1||ECS1Sig)hash

[0851] 参照图 28 中所示的流程图描述图 27 的(b)中所示的这些“替换数据项”的记录处理的序列。

[0852] 注意,图 28 所示的处理是通过使用存储卡存储与图 27 的(a)中所示的内容(C1)对应的有效数据集执行的处理,更具体地,该处理是由例如具有执行数据记录处理的权限

作为针对存储卡的保护区域中的块 N 的访问权限的内容提供服务器或者用户装置执行的处理。

[0853] 首先，在步骤 S241 中，从通用区域读取与内容 C1 对应的使用控制信息项 UR1，然后执行篡改比如重写可用时间段信息项，以获取欺诈性的使用控制信息项（UR2）。

[0854] 接下来，在步骤 S242 中，从存储卡的通用区域中记录的内容（C1）的使用控制信息项（UR1）获取“块标识符”和“标题密钥标识符”。基于这些获取的信息项，从保护区域中的预定块即标题密钥存储块处读取与下述标题密钥转换数据项对应的正常内容（C1）。

[0855] Kt1 （+）（UR1||ECS1Sig）hash

[0856] 注意，ECS1Sig 表示 Sign （ECS 签名密钥，M），且 M 表示内容 C1 的内容哈希列表集与 Kt1 的哈希值的串接数据项。

[0857] 接下来，在步骤 S243 中，计算下述从通用区域读取的与正常内容 (C1)对应的使用控制信息项（UR1）以及 ECS 文件（ECS1 （C1，Kt1））的串接数据项的哈希值。然后，执行该计算结果与上述从保护区域读取的标题密钥转换数据项之间的异或运算（XOR）以获取与内容（C1）对应的正常标题密钥（Kt1）。

[0858] 换言之，基于下述公式获取标题密钥（Kt1）。

[0859] Kt1=（从通用区域读取的数据项）（+）（从保护区域读取的数据项）

[0860] =(UR1||ECS1Sig)hash(+)Kt1(+)(UR1||ECS1Sig)hash

[0861] 注意，（+）表示异或运算（XOR）。

[0862] 另外，基于下述公式计算要应用于内容 C2 的解密和加密的标题密钥 Kt2。

[0863] Kt2=Kt1(+)(UR1||ECS1Sig)hash(+)(UR2||ECS1Sig)hash

[0864] 接下来，在步骤 S244 中，应用步骤 S243 中生成的标题密钥 Kt1 来解密内容 C1(Kt1)。另外，将步骤 S243 中生成的新的标题密钥 Kt2 应用于加密该内容 C1 以生成加密内容 C1 （Kt2）。

[0865] 接下来，在步骤 S245 中，将加密内容 C2 （Kt2）记录到存储卡中的通用区域。

[0866] 接下来，在步骤 S246 中，生成加密内容签名 ECS2Sig，该加密内容签名 ECS2Sig 与基于内容 C1 生成的内容哈希列表集和 Kt2 的哈希值对应。换言之，生成下述签名数据项。

[0867] ECS2Sig=Sign （ECS 签名密钥，M）

[0868] 注意，M 表示内容 C1 的内容哈希列表集与 Kt2 的哈希值的串接数据项。

[0869] 另外，将由加密内容签名发行者发行的泄露的签名密钥（秘密密钥）应用于此签名的生成。

[0870] 接下来，在步骤 S247 中，生成包含步骤 S246 中欺诈性地生成的 ECS 签名（ECS2Sig（C1，Kt2））的 ECS 文件，并且将其记录到存储卡的通用区域。

[0871] 最后，在步骤 S248 中，将步骤 S241 中生成的使用控制信息项（UR2）记录到通用区域。

[0872] 通过图 28 所述的一系列处理，完成了记录图 27 的（b）所示的“替换数据项”的处理。

[0873] 通过这样的替换处理，该欺诈性地生成的使用控制信息项（UR2）与内容 C1 对应。

[0874] 注意，当用新的标题密钥 Kt2 加密内容 C1 的时候记录内容 C1。

[0875] 接下来，参照图 29 所示的流程图描述用户装置通过使用图 27 的（b）所示的“替换

数据项”如何执行内容 C1 的再现处理。

[0876] 首先，在步骤 S261 中，用户装置从存储卡中的通用区域读取要再现的加密内容 C1（Kt2）和与加密内容 C1（Kt2）对应地生成的 ECS 文件（ECS2（C1，Kt2））。

[0877] 接下来，在步骤 S262 中，从新的使用控制信息项（UR2）读取指示存储标题密钥的块的块标识符和标题密钥标识符，该新的使用控制信息项（UR2）是对应于内容 C1 在存储卡的通用区域中欺诈性地生成的。

[0878] 将这些块标识符和标题密钥标识符设置成保持与在有效的未篡改使用控制信息项（UR1）中的块标识符和标题密钥标识符相同。

[0879] 换言之，这些块标识符和标题密钥标识符是分别与存储与内容 C1 对应的正常标题密钥 Kt1 的块对应的标识符和与在相同块中存储的标题密钥对应的标识符。

[0880] 因此，这样读取的数据项与对应于内容 C1 的标题密钥转换数据项相对应，即

[0881] Kt1(+)(UR1||ECS1Sig)hash

[0882] 在步骤 S263 中，计算下述数据项的串接数据项的哈希值：欺诈性地生成并且从通用区域读取的使用控制信息项（UR2）；以及非法生成的 ECS 文件（ECS1（C1，Kt2）。然后，执行该计算结果与上述从保护区域读取的标题密钥转换数据项之间的异或运算（XOR）以获取与内容 C1 对应的解密标题密钥 Kt3。

[0883] 在此情况下，当这样获得的标题密钥 Kt3 等于 Kt2 时，标题密钥获取成功。

[0884] 接下来，在步骤 S263 中，做出基于下述公式的执行标题密钥计算处理的尝试。

[0885] Kt3=（从保护区域读取的数据项）（+）（从通用区域读取的数据项）

[0886] =Kt1(+)(UR1||ECS1Sig)hash(+)(UR2||ECS2Sig)hash

[0887] 标题密钥（Kt3）基于此标题密钥计算公式生成。

[0888] 注意，（+）表示异或运算（XOR）。

[0889] 但是，不能在上述标题密钥计算公式中获取 Kt2。因此，基于上述计算公式获取的值：Kt3 不等于 Kt1 或者 Kt2，换言之，下述关系成立。

[0890] $Kt3 \neq Kt2$

[0891] $Kt3 \neq Kt1$

[0892] 结果，如步骤 S264 所述，用户装置不能获取应用于内容 C1 的再加密的标题密钥 Kt2，并且内容 C1 的解密和再现失败。

[0893] 另外，在步骤 S265 中，基于预设的再现序列，用户装置执行 ECS 发行者的签名（ECSSig）的验证处理，该 ECS 发行者的签名（ECSSig）包含在从通用区域读取的 ECS 文件中。

[0894] 基于下述算式执行签名验证处理。

[0895] Verify（ECS 发行者公开密钥，ECS2Sig，M）

[0896] 注意，Verify（k，S，M）表示使用验证密钥 k 来验证与数据项 M 对应的电子签名 S 的处理。

[0897] M 表示内容 C1 的内容哈希列表集与 Kt3 的哈希值的串接数据项。

[0898] 在步骤 S263 中计算出的值被用作为 Kt3。

[0899] ECS 文件中存储的 ECS2Sig 是图 28 所示的流程的步骤 S246 中生成的欺诈性签名，即下述数据项。

[0900] ECS2Sig=Sign（ECS 签名密钥，M）

[0901] 注意，

[0902] M 表示内容 C1 的内容哈希列表集与 Kt2 的哈希值的串接数据项。

[0903] 如上所述，要应用于签名验证的数据项 M 是包含 Kt3 的哈希值的数据项。同时，ECS 文件中存储的签名数据项 ECS2Sig 是与包含 Kt2 的哈希值的 M 对应地生成的。

[0904] 因此，如图 29 中的步骤 S266 所述，通过步骤 S265 中的签名验证确认了一些篡改。

[0905] 以此方式，即使当通过使用图 27 的（b）所示的“替换数据项”来试图解密和再现内容 C1 时，用户装置具有下述结果。

[0906] 内容 C1 的解密失败

[0907] 通过 ECS 文件的签名验证确认了一些篡改

[0908] 结果，不能使用内容 C1。

[0909] 如上所述，当要记录到存储卡中的保护区域中的标题密钥被存储为使用控制信息项（UR）与 ECS 发行者的签名（ECSSig）的串接数据项的哈希值和标题密钥之间的异或运算（XOR）的结果时，即使是在要应用于 ECS 发行者的签名（ECSSig）的 ECS 发行者发行的签名密钥（秘密密钥）已经泄露的情况下，也可以防止对内容的欺诈性使用。

[0910] 例如，这样的处理使得内容提供服务器或者用户装置能够防止通过应用从 ECS 发行者发行的泄露的签名密钥（秘密密钥）的欺诈性处理、具体地为替换加密内容的加密密钥或者篡改使用控制信息项的处理而欺诈性地使用内容。

[0911] [11. 应用加密内容签名（ECS）文件中记录的块标识符的处理 ]

[0912] 接下来，描述应用加密内容签名（ECS）文件中记录的块标识符（PAD 块号）的处理。

[0913] 如以上参照图 9 的（A）所述，块标识符（PAD 块号）记录在加密内容签名（ECS）文件中。

[0914] 如参照图 13 所述，块标识符（PAD 块号）是要从内容提供装置（内容服务器）103 通知给加密内容签名（ECS）发行者 102 的数据项，更具体地，块标识符是指示了在介质的保护区域中的哪些块中存储了作为与从内容提供装置 103 提供给用户装置 104 的内容对应的加密密钥的标题密钥。换言之，块标识符（PAD 块号）是指示了内容提供装置 103 可以使用的介质的保护区域中的哪些块的标识符。

[0915] 例如，如以上参照图 3 和图 6 所述，内容提供装置 103 可以使用的介质的保护区域中的哪些块是预先设置的，并且记录这样的访问准许块的信息项。

[0916] 另外，如参照图 9 的（B）所述，将与块标识符（PAD 块号）对应的信息项也记录在 ECS 发行者证书中。

[0917] 如以上参照图 9 的（B）所述，记录了下述数据项。

[0918] （a）块标识符起始号（起始 PAD 块号）

[0919] （b）块标识符范围（PAD 块号计数器）

[0920] （a）块标识符起始号（起始 PAD 块号）是介质的保护区域中的访问准许块的起始号，其中，内容提供装置 103 准许 ECS 发行者 102 对访问准许块进行访问。

[0921] （b）块标识符范围（PAD 块号计数器）是指示从介质的保护区域中内容提供装置 103 准许 ECS 发行者 102 访问的访问准许块的起始号开始的范围的信息项。

[0922] 另外，如以上参照图 23 所述，不同块标识符也记录在与内容对应的使用控制信息

项(UR)中。该记录在使用控制信息项(UR)中的不同块标识符是指示哪些块中存储了与内容对应的标题密钥的标识符。

[0923] 图 30 示出了下述内容间的联系。

[0924] 加密内容签名(ECS)文件

[0925] 使用控制信息项(UR)

[0926] 记录在加密内容签名(ECS)文件中和使用控制信息项(UR)中的块标识符

[0927] 保护区域中的标题密钥存储块(图示中的块 k)

[0928] 如图 30 所示,存储卡的通用区域存储了与内容对应的下述数据项。

[0929] 加密内容签名(ECS)文件

[0930] 使用控制信息项(UR)

[0931] 另外,保护区域中的块 k 存储了通过与内容对应的标题密钥的转换而获取的数据项,即,

[0932] Kt(+)UR||(ECSSig)hash。

[0933] 要向用户装置提供内容的内容提供装置对以下两者进行比较 :作为内容提供装置本身的主机证书(参照图 4)中记录的保护区域访问权限信息项的块标识符 ;作为 ECS 发行者证书中的块标识符的写入准许区域信息项。

[0934] 基于该比较的结果,判断是否可以提供内容。

[0935] 另外,用于执行内容的再现的用户装置将使用控制信息项中的块标识符和 ECS 文件中的块标识符相互比较。

[0936] 基于该比较的结果,判断是否可以再现内容。

[0937] 首先,参照图 31 所示的流程图描述内容提供装置如何通过使用块标识符判断是否可以提供内容的序列。

[0938] 作为图 31 所示的流程图中的步骤 S401 的预处理,内容提供装置执行应用 ECS 发行者的签名的签名验证,该 ECS 发行者的签名设置在从加密内容签名(ECS)发行者接收的加密内容签名文件(ECS 文件)中。

[0939] 在通过该签名验证确认没有篡改的情况下,换言之,在确认了加密内容签名文件(ECS 文件)的有效性的情况下,执行存储在加密内容签名文件(ECS 文件)中的 ECS 发行者证书的另一个签名验证。如果两个签名验证都确认没有篡改,则执行步骤 S401 和后续步骤的处理。

[0940] 在两个签名验证处理的至少一个处理中确认了一些篡改的情况下,不确认加密内容签名文件(ECS 文件)的有效性或者 ECS 发行者证书的有效性。因此,不执行步骤 S401 和后续步骤的处理。在这种情况下,也不执行内容提供处理。

[0941] 注意,关于作为存储在加密内容签名文件(ECS 文件)中的内容哈希列表集的源数据的内容哈希,可以设置加密内容的哈希或者未加密内容的哈希。

[0942] 在通过加密内容签名文件(ECS 文件)和 ECS 发行者证书的两个签名验证处理确认没有篡改的情况下,换言之,在确认了加密内容签名文件(ECS 文件)的有效性和 ECS 发行者证书的有效性的情况下,内容提供装置执行步骤 S401 的处理。

[0943] 首先,在步骤 S401 中,内容提供装置读取 ECS 文件中的 ECS 发行者证书以读取 ECS 发行者证书中记录的块标识符的信息项。

[0944] 参照图 32 所示的流程图描述步骤 S401 的细节。

[0945] 在步骤 S421 中，从 ECS 发行者证书中读取块标识符起始号(起始 PAD 块号)。

[0946] 块标识符起始号(起始 PAD 块号)是介质的保护区域中的访问准许块的起始号，其中，ECS 发行者 102 准许内容提供装置 103 对访问准许块进行访问。

[0947] 接下来，在步骤S422中，判断ECS发行者证书中的块标识符起始号(起始PAD块号)是否是 0xFFFFFFFF。

[0948] 注意，当块标识符起始号(起始 PAD 块号)是 0xFFFFFFFF 时，准许访问所有的块。

[0949] 在步骤 S422 中，在判断出块标识符起始号(起始 PAD 块号)是 0xFFFFFFFF 的情况下，流程进行到步骤 S423 以将介质的保护区域中的所有块当作访问准许块。

[0950] 同时，在步骤 S422 中，在判断出块标识符起始号(起始 PAD 块号)不是 0xFFFFFFFF 时，流程进行到步骤 S424。

[0951] 在步骤 S424 中，从 ECS 发行者证书中读取块标识符范围(PAD 块号计数器)。

[0952] 块标识符范围(PAD 块号计数器)是指示从介质的保护区域中内容提供装置 103 准许 ECS 发行者 102 访问的访问准许块的起始号开始的范围的信息项。

[0953] 后续步骤 S425 到 S428 的处理均是将指示块标识符的变量 I 顺序地从 0 到 1、2、3、.... 增加的迭代程序。

[0954] 首先，在步骤 S425 中，设置下述等式。

[0955] 变量 :I=1

[0956] 接下来，在步骤 S426 中，将块标识符起始号(起始 PAD 块号)+I 添加入块标识符列表(PAD 块号列表)。

[0957] 接下来，在步骤 S427 中，下述等式成立。

[0958] I=I+1

[0959] 接下来，在步骤 S428 中，判断 I 是否等于块标识符范围(PAD 块号计数器)。

[0960] 当 I 等于块标识符范围(PAD 块号计数器)时，流程完成。同时，当 I 不等于块标识符范围(PAD 块号计数器)时，流程返回到步骤 S426 以重复此处理。

[0961] 基于这个流程，执行图 31 所示的流程中的步骤 S401 的处理。

[0962] 在步骤 S401 中，将 ECS 发行者证书中的块标识符起始号(起始 PAD 块号)和块标识符范围(PAD 块号计数器)应用于计算由 ECS 发行者证书定义的访问准许范围。然后，将访问准许范围设置成访问准许块标识符列表。

[0963] 接下来，在步骤 S402 中，判断步骤 S401 中生成的访问准许块标识符列表是否包含作为加密内容签名(ECS)文件中记录的数据项的块标识符(PAD 块号)。

[0964] 当访问准许块标识符列表不包含块标识符(PAD 块号)时，流程进行到步骤 S405，不执行将内容提供给用户装置的处理。

[0965] 同时，当访问准许块标识符列表包含了块标识符(PAD 块号)时，流程进行到步骤 S403。

[0966] 在步骤 S403 中，判断作为加密内容签名(ECS)文件中记录的数据项的块标识符(PAD 块号)是否与使用控制信息项(UR)中记录的不同块标识符匹配。

[0967] 当块标识符(PAD 块号)与该不同块标识符不匹配时，流程进行到步骤 S405，不执行将内容提供给用户装置的处理。

[0968] 同时，当块标识符（PAD 块号）与该不同块标识符时匹配，流程进行到步骤 S404，执行将内容提供给用户装置的处理。

[0969] 以此方式，内容提供装置判断是否都满足下述条件（a）和条件（b）两者。

[0970] （a）加密内容签名（ECS）文件中记录的块标识符（PAD 块号）落在 ECS 发行者证书中记录的访问准许块范围中。

[0971] （b）加密内容签名（ECS）文件中记录的块标识符（PAD 块号）与使用控制信息项（UR）中记录的不同块标识符匹配。

[0972] 只有当满足条件（a）和条件（b）两者时，才将内容提供给用户装置。

[0973] 接下来，参照图 33 所示的流程图描述用于执行内容再现处理的用户装置如何执行应用块标识符的处理。

[0974] 注意，在图 33 所示的步骤 S451 之前，用户装置执行应用 ECS 发行者的签名的签名验证，ECS 发行者的签名设置在从内容提供装置接收的加密内容签名文件（ECS 文件）中。

[0975] 在通过该签名验证确认没有篡改的情况下，即在确认了加密内容签名文件（ECS 文件）的有效性的情况下，执行该加密内容签名文件（ECS 文件）中存储的 ECS 发行者证书的另一个签名验证。如果两个签名验证处理都确认没有篡改，则执行步骤 S451 和后续步骤的处理。

[0976] 在两个签名验证处理的至少一个验证中确认了一些篡改的情况下，则不确认加密内容签名文件（ECS 文件）的有效性或者 ECS 发行者证书的有效性。因此，不执行步骤 S451 和后续步骤的处理。在此情况下，也不执行内容再现处理。

[0977] 在通过加密内容签名文件（ECS 文件）和 ECS 发行者证书的两个签名验证处理两者都确认没有篡改的情况下，换言之，在确认了加密内容签名文件（ECS 文件）和 ECS 发行者证书的有效性的情况下，用户装置执行步骤 S451 的处理。

[0978] 在步骤 S451 中，执行与以上描述为内容提供装置的处理即与图 31 所示的流程中的步骤 S401 的处理相同的处理。换言之，如参照图 32 所示的流程所详细描述的，应用 ECS 发行者证书中的块标识符起始号（起始 PAD 块号）和块标识符范围（PAD 块号计数器）来计算 ECS 发行者证书所定义的访问准许范围。然后，将访问准许范围设置成访问准许块标识符列表。

[0979] 接下来，在步骤 S452 中，判断步骤 S451 中生成的访问准许块标识符列表是否包含被描述成在加密内容签名（ECS）文件中记录的数据项的块标识符（PAD 块号）。

[0980] 当该访问准许块标识符列表不包含该块标识符（PAD 块号）时，流程进行到步骤 S455，不执行再现内容的处理。

[0981] 同时，当该访问准许块标识符列表包含该块标识符（PAD 块号）时，流程进行到步骤 S453。

[0982] 在步骤 S453 中，判断被描述成在加密内容签名（ECS）文件中记录的数据项的块标识符（PAD 块号）是否与使用控制信息项（UR）中记录的不同块标识符匹配。

[0983] 当该块标识符（PAD 块号）与该不同块标识符不匹配时，流程进行到步骤 S455，不执行再现内容的处理。

[0984] 同时，当该块标识符（PAD 块号）与该不同块标识符匹配时，流程进行到步骤 S454，执行再现内容的处理。

[0985] 注意，开始内容再现处理之前，不仅执行了获取和生成要被应用于对加密内容进行解密的标题密钥的处理，而且还执行了应用加密内容签名文件中包含的内容哈希列表集的哈希值验证处理。在通过哈希值验证确认内容中没有篡改的情况下，准许内容的再现。

[0986] 以此方式，再现内容的用户装置判断是否都满足下述条件(a)和条件(b)两者。

[0987] (a)加密内容签名(ECS)文件中记录的块标识符(PAD 块号)落在 ECS 发行者证书中记录的访问准许块范围中。

[0988] (b)加密内容签名(ECS)文件中记录的块标识符(PAD 块号)与使用控制信息项(UR)中记录的不同块标识符匹配。

[0989] 只有当满足条件(a)和条件(b)两者时，用户装置才再现内容。

[0990] [12. 每个装置的硬件配置示例 ]

[0991] 最后，参照图 34 描述上文描述的执行处理的每个装置的硬件配置示例。

[0992] 图 34 示出了信息处理装置的硬件配置示例，该信息处理装置可应用于图 7 和图 8 所示的用户装置 104、内容提供装置 103、加密内容签名发行者 102、许可证发行者 101 的任何一个。

[0993] CPU(中央处理单元)701 用作基于存储在 ROM(只读存储器)702 或者存储单元 708 中的程序来执行各种处理的数据处理单元。例如，CPU701 执行基于上文所描述的流程图的处理。RAM(随机存取存储器)703 适当地存储要由 CPU 701 执行的程序、数据项等。这些 CPU 701、ROM702 和 RAM 703 用总线 704 互相连接。

[0994] CPU 701 通过总线 704 连接至输入 / 输出接口 705。输入 / 输出接口 705 连接有输入单元 706 和输出单元 707，输入单元 706 包括各种开关、键盘、鼠标和麦克风，输出单元 707 包括显示器和扬声器。CPU 701 响应于从输入单元 706 输入的命令执行各种处理，并且例如向输出单元 707 输出处理结果。

[0995] 连接至输入 / 输出接口 705 的存储单元 708 包括例如硬盘，并且存储要由 CPU 701 执行的程序和各种数据项。通信单元 709 通过网络比如因特网和局域网来与外部装置通信。

[0996] 连接至输入 / 输出接口 705 的驱动器 710 驱动可拆除介质 711 例如磁盘、光盘、磁光盘和半导体存储器比如存储卡，并且获取在其中存储的各种数据项比如内容和密钥信息项。例如，通过使用内容和密钥数据项，基于要由 CPU 执行的再现程序对内容执行解密处理、再现处理等。

[0997] 图 35 示出了作为信息存储装置的存储卡的硬件配置示例。

[0998] CPU(中央处理单元)801 用作基于存储在 ROM(只读存储器)802 或者存储单元 807 中的程序来执行各种处理的数据处理单元。例如，CPU801 执行在上文实施方式中描述的与服务器和主机装置的通信处理，例如执行对于存储单元 807 的读取数据和写入数据的处理、以及存储单元 807 的保护区域 811 中的分段区域的单元中的访问可能性判断处理。RAM(随机存取存储器)803 适当地存储要由 CPU 801 执行的程序、数据项等。这些 CPU 801、ROM 802 和 RAM 803 用总线 804 互相连接。

[0999] CPU 801 通过总线 804 连接至输入 / 输出接口 805。输入 / 输出接口 805 连接有通信单元 806 和存储单元 807。

[1000] 连接至输入 / 输出接口 805 的通信单元 806 执行例如到服务器和主机的通信。存

储单元 807 是数据的存储区域，并且如上所述，存储单元 807 包括设置了访问限制的保护区域 811 和可以从其自由读取数据的通用区域 812。

[1001] 在上文实施方式中描述的典型示例中，要由内容提供装置提供的内容是加密内容。但是，根据本公开的实施方式的配置不局限于要提供的内容是加密内容的情况，并且可以应用于要提供的内容是未加密的明文内容的情况。注意，在内容是明文内容的情况下，在上文的实施方式所描述的标题密钥包括现有技术的数据串比如值都是零的密钥数据项的前提下，可以执行与上文描述的加密内容提供处理相同的处理。

[1002] [13. 本公开的配置的总结 ]

[1003] 在上文中，已经参照具体的实施方式详细地描述了本公开的实施方式。但是，实际上，本领域的技术人员可以在不脱离本公开的要旨的情况下对实施方式做出修改和替换。换言之，已描述的本公开仅是说明，所以不应该被限制性地解释。应该基于所附权利要求的范围判断本公开的要旨。

[1004] 注意，在本说明书中公开的技术可以包括下述配置。

[1005] (1) 一种信息存储装置，包括存储单元，被配置成存储加密内容以及要被应用于对所述加密内容进行解密的加密密钥，所述存储单元包括 ：

[1006] 保护区域，在所述保护区域中存储转换加密密钥并且设置了对所述保护区域的访问限制，所述转换加密密钥是通过所述加密密钥的转换而获取的数据项，以及

[1007] 通用区域，所述通用区域存储所述加密内容以及与所述加密内容对应地设置的加密内容签名文件，所述加密内容签名文件包含下述块标识符作为记录数据项，所述块标识符指示在所述保护区域中的哪些区域中准许存储所述转换加密密钥，从而准许再现装置执行应用所述块标识符的内容再现可能性判断，所述再现装置被配置成从所述存储单元中读取所述加密内容并且执行再现处理。

[1008] (2) 根据第 (1) 项所述的信息存储装置，其中，

[1009] 所述加密内容签名文件包含 ECS 发行者证书，所述 ECS 发行者证书存储来自作为所述加密内容签名文件的发行者的 ECS 发行者的公开密钥，所述 ECS 发行者证书包含下述块标识符范围作为记录数据项，所述块标识符范围为所述保护区域中的每个区域中准许存储所述转换加密密钥的范围，以及

[1010] 所述信息存储装置准许所述再现装置判断所述加密内容签名文件中记录的所述块标识符是否落在所述 ECS 发行者证书中记录的所述块标识符范围中，并且基于所述判断的结果来确定是否能够再现所述加密内容，所述再现装置被配置成从所述存储单元中读取所述加密内容并且执行所述再现处理。

[1011] (3) 根据第 (1) 项或第 (2) 项所述的信息存储装置，其中，

[1012] 所述通用区域还存储与所述加密内容对应的使用控制信息项，所述使用控制信息项是包含指示在哪些块中存储所述加密密钥的不同块标识符的信息项，以及

[1013] 所述信息存储装置准许所述再现装置判断所述加密内容签名文件中记录的所述块标识符是否与所述使用控制信息项中记录的所述不同块标识符匹配，并且基于所述判断的结果来确定是否能够再现所述加密内容，所述再现装置被配置成从所述存储单元中读取所述加密内容并且执行所述再现处理。

[1014] (4) 一种信息处理装置，包括 ：

[1015] 数据处理单元，被配置成执行介质中记录的加密内容的解密处理和再现处理，所述数据处理单元被配置成：

[1016] 从所述介质中读取与所述加密内容对应地设置的加密内容签名文件，

[1017] 从所述加密内容签名文件中获取指示在哪些区域中准许存储要被应用于对所述加密内容进行解密的加密密钥的块标识符，以及

[1018] 执行应用所述块标识符的内容再现可能性判断处理。

[1019] (5)根据第(4)项所述的信息处理装置，其中，

[1020] 所述加密内容签名文件包含 ECS 发行者证书，所述 ECS 发行者证书存储来自作为所述加密内容签名文件的发行者的 ECS 发行者的公开密钥，所述 ECS 发行者证书包含下述块标识符范围作为记录数据项，所述块标识符范围为每个区域中准许存储所述加密密钥的范围，以及

[1021] 所述数据处理单元判断所述加密内容签名文件中记录的所述块标识符是否落在所述 ECS 发行者证书中记录的所述块标识符范围中，并且基于所述判断的结果来确定是否能够再现所述加密内容。

[1022] (6)根据第(4)项或第(5)项所述的信息处理装置，其中，

[1023] 所述介质还存储与所述加密内容对应的使用控制信息项，所述使用控制信息项是包含指示在哪些块中存储所述加密密钥的不同块标识符的信息项，以及

[1024] 所述数据处理单元判断所述加密内容签名文件中记录的所述块标识符是否与所述使用控制信息项中记录的所述不同块标识符匹配，并且基于所述判断的结果来确定是否能够再现所述加密内容。

[1025] (7)一种信息处理装置，包括：

[1026] 数据处理单元，被配置成输出要被记录到介质的加密内容以及要被应用于对所述加密内容进行解密的加密密钥，所述数据处理单元被配置成：

[1027] 获取与所述加密内容对应地设置的加密内容签名文件，

[1028] 从所述加密内容签名文件中获取指示在哪些区域中准许存储所述加密密钥的块标识符，以及

[1029] 执行应用所述块标识符的内容输出可能性判断处理。

[1030] (8)根据第(7)项所述的信息处理装置，其中，

[1031] 所述加密内容签名文件包含 ECS 发行者证书，所述 ECS 发行者证书存储来自作为所述加密内容签名文件的发行者的 ECS 发行者的公开密钥，所述 ECS 发行者证书包含下述块标识符范围作为记录数据项，所述块标识符范围为每个区域中准许存储所述加密密钥的范围，以及

[1032] 所述数据处理单元判断所述加密内容签名文件中记录的所述块标识符是否落在所述 ECS 发行者证书中记录的所述块标识符范围中，并且基于所述判断的结果来确定是否能够输出所述加密内容。

[1033] (9)根据第(7)项或第(8)项所述的信息处理装置，其中，

[1034] 所述数据处理单元被配置成：

[1035] 获取与所述加密内容对应地设置的使用控制信息项，

[1036] 从所获取的使用控制信息项中获取指示在哪些块中存储了所述加密密钥的不同

块标识符，

[1037] 判断所述加密内容签名文件中记录的所述块标识符是否与所述使用控制信息项中记录的所述不同块标识符匹配，以及

[1038] 基于所述判断的结果来确定是否能够输出所述加密内容。

[1039] 另外，根据本公开的实施方式的配置包括执行上述装置和系统中的处理的方法和执行这些处理的程序。

[1040] 另外，本说明书中描述的一系列处理可以由硬件、软件或者硬件和软件的组合配置来执行。当由软件执行处理时，可以用下述程序来执行处理，所述程序存储了处理序列并且安装在被结合在专用硬件中的计算机的存储器中或者安装在能够执行各种处理的通用计算机中。例如，程序可以预先记录在记录介质中，并且可以从该记录介质安装到计算机中。可替选地，程序可以经由网络比如因特网或者 LAN（局域网）接收然后安装到记录介质例如内置硬盘。

[1041] 注意，本说明书中描述的各种处理不仅可以以根据本说明书的时序来执行，也可以依照执行处理的装置的处理能力或者当有必要时并行或者单独执行。另外，在本说明书中使用的术语“系统”意指多个装置的逻辑集合配置，因而如上所述配置的这些装置不一定设置在同一壳体中。

[1042] 如上文所述，根据本公开的一个实施方式中的配置，提供了一种用于有效地防止对内容的欺诈性使用的装置和方法。

[1043] 具体地，从与加密内容对应地设置的加密内容签名文件中获取指示在哪些区域中准许存储要被应用于对加密内容进行解密的加密密钥的块标识符。然后，执行应用该块标识符的内容再现可能性判断处理。加密内容签名文件包含来自作为加密内容签名文件的发行者的 ECS 发行者的证书。执行关于加密内容签名文件中记录的块标识符是否落在 ECS 发行者证书中记录的块标识符范围中的判断，以及执行关于加密内容签名文件中记录的块标识符是否与使用控制信息项中记录的不同块标识符匹配的判断。基于这些判断的结果来确定是否能够再现内容。

[1044] 通过使用从加密内容签名文件中获取的块标识符信息项，能够基于关于密钥信息项是否被记录在某个访问准许块中的判断来进行内容使用控制。

[1045] 本公开包含与 2011 年 11 月 17 日提交于日本专利局的日本在先专利申请 JP 2011-251735 中公开的主题相关的主题，其全部内容通过引用合并于此。

[1046] 本领域的技术人员应该理解，取决于设计要求和其他因素可以进行各种修改、组合、子组合和改变，这样这些修改、组合、子组合和改变在所附权利要求或其等同内容的范围内。

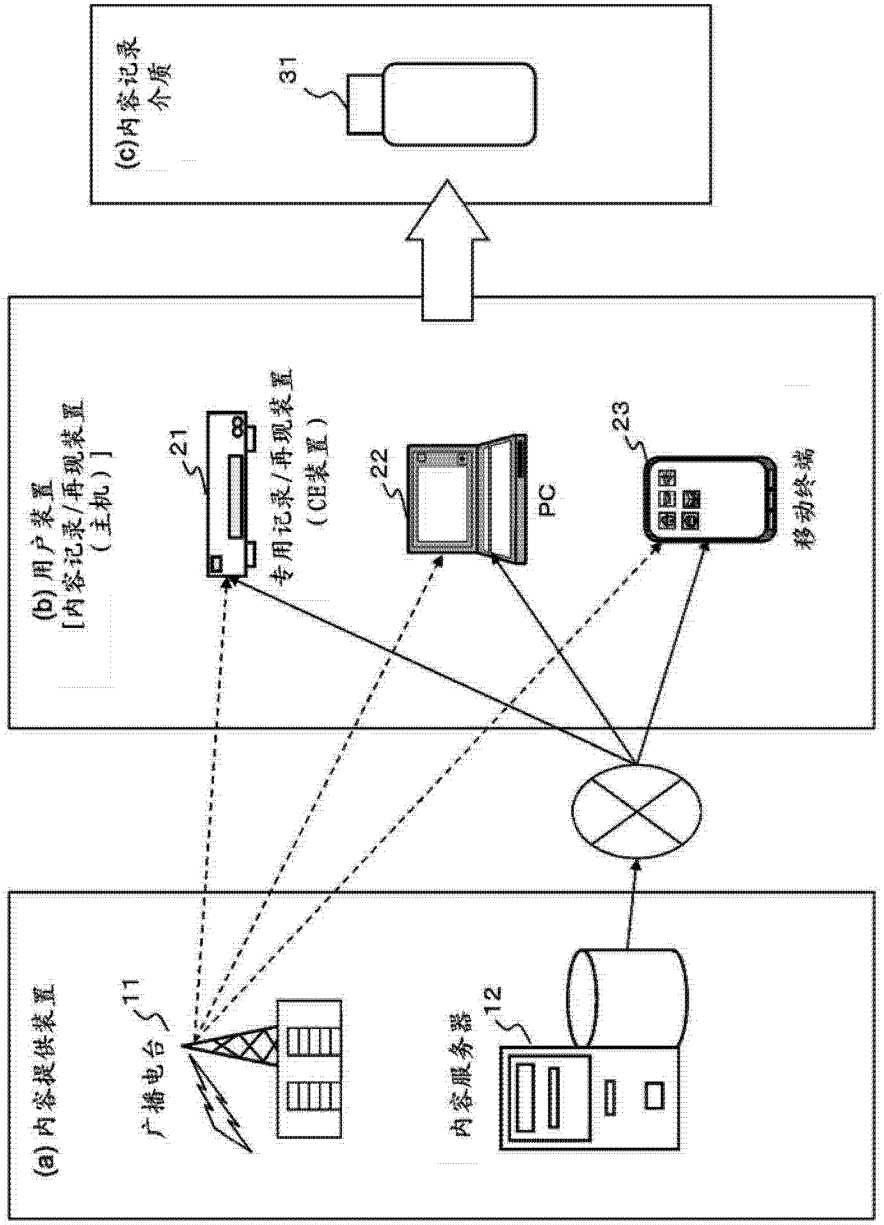

(c)内容记录介质
31
(b)用户装置
[内容记录/再现装置（主机）]
21
专用记录/再现装置（CE装置）
22
PC
23
移动终端
(a)内容提供装置
11
广播电台
12
内容服务器

图 1

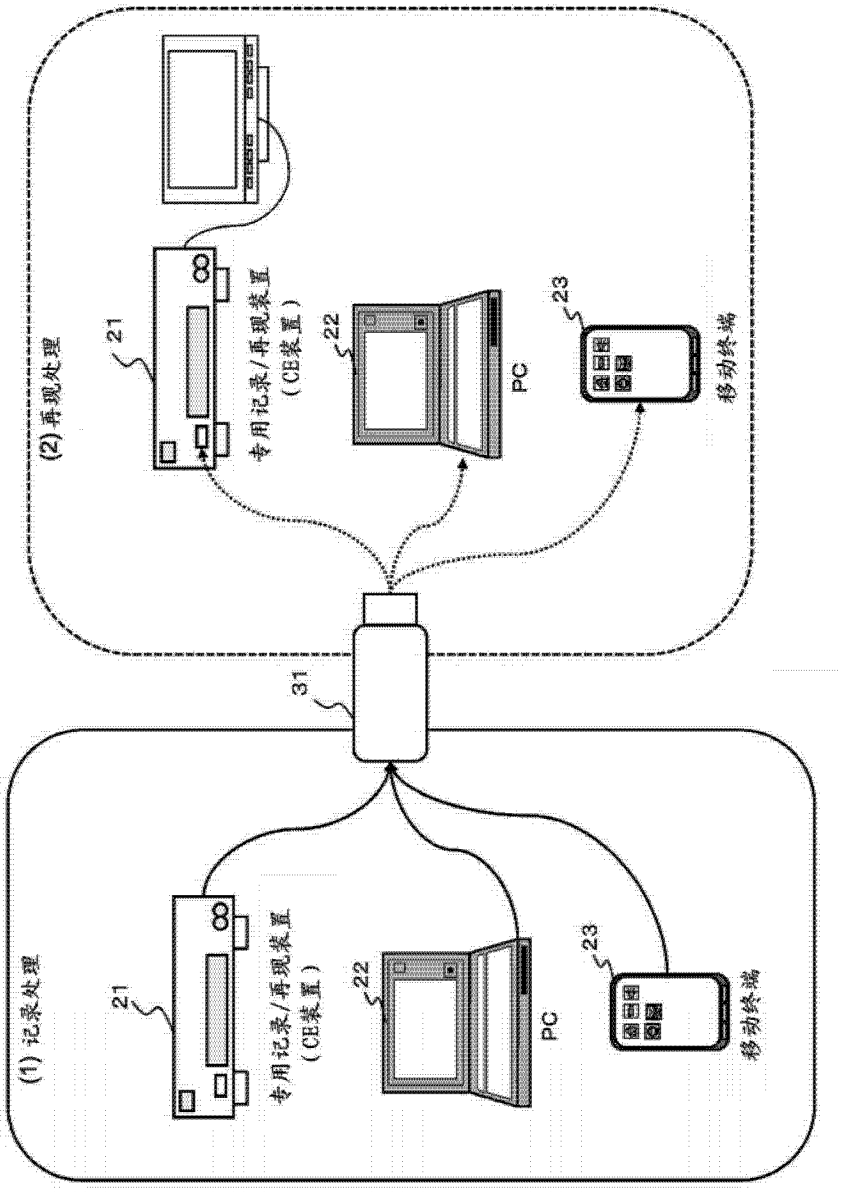

(2) 再现处理
21
专用记录/再现装置
(CE装置)
22
PC
23
移动终端
31
(1) 记录处理
21
专用记录/再现装置
(CE装置)
22
PC
23
移动终端

图 2

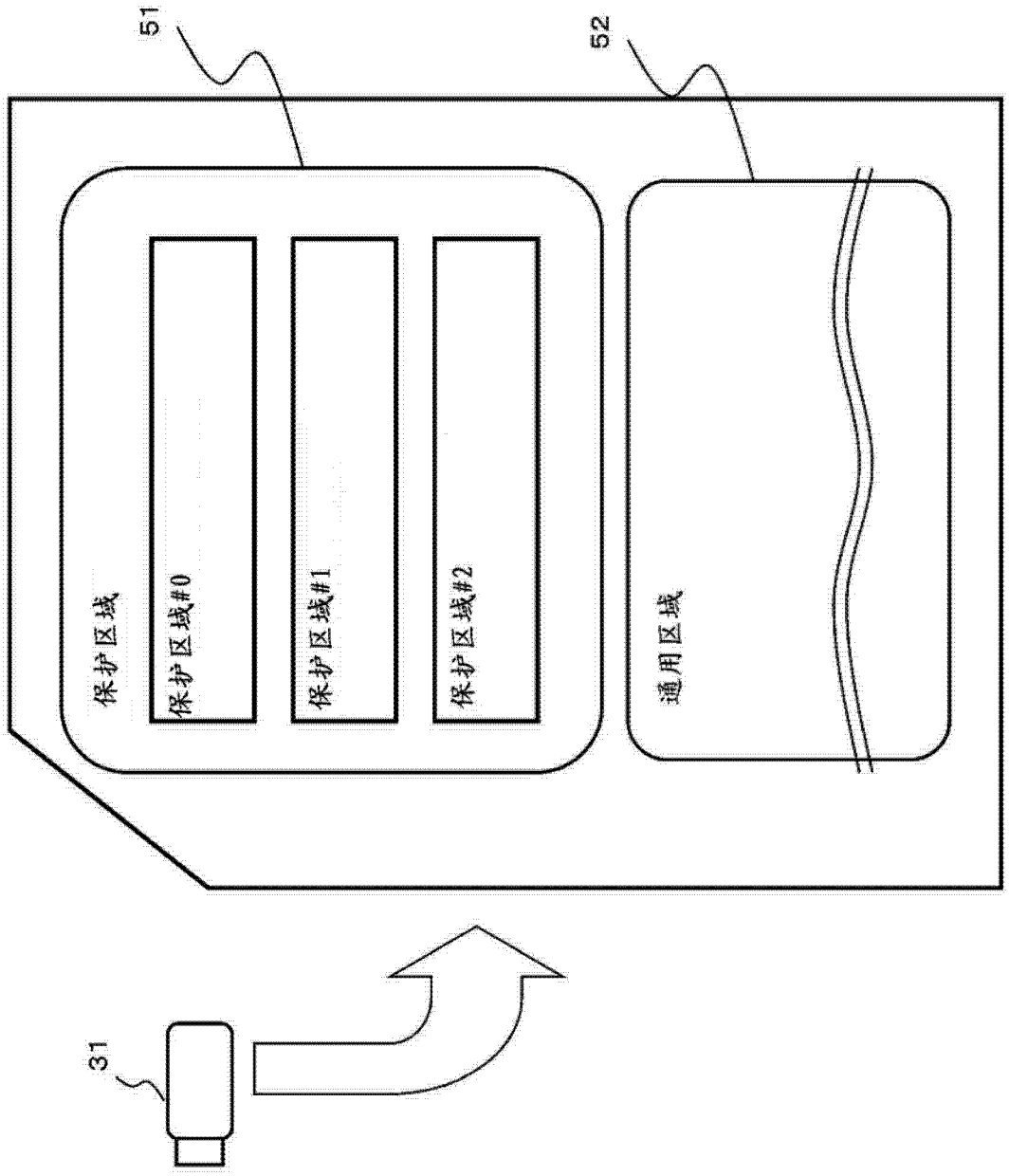



图 3

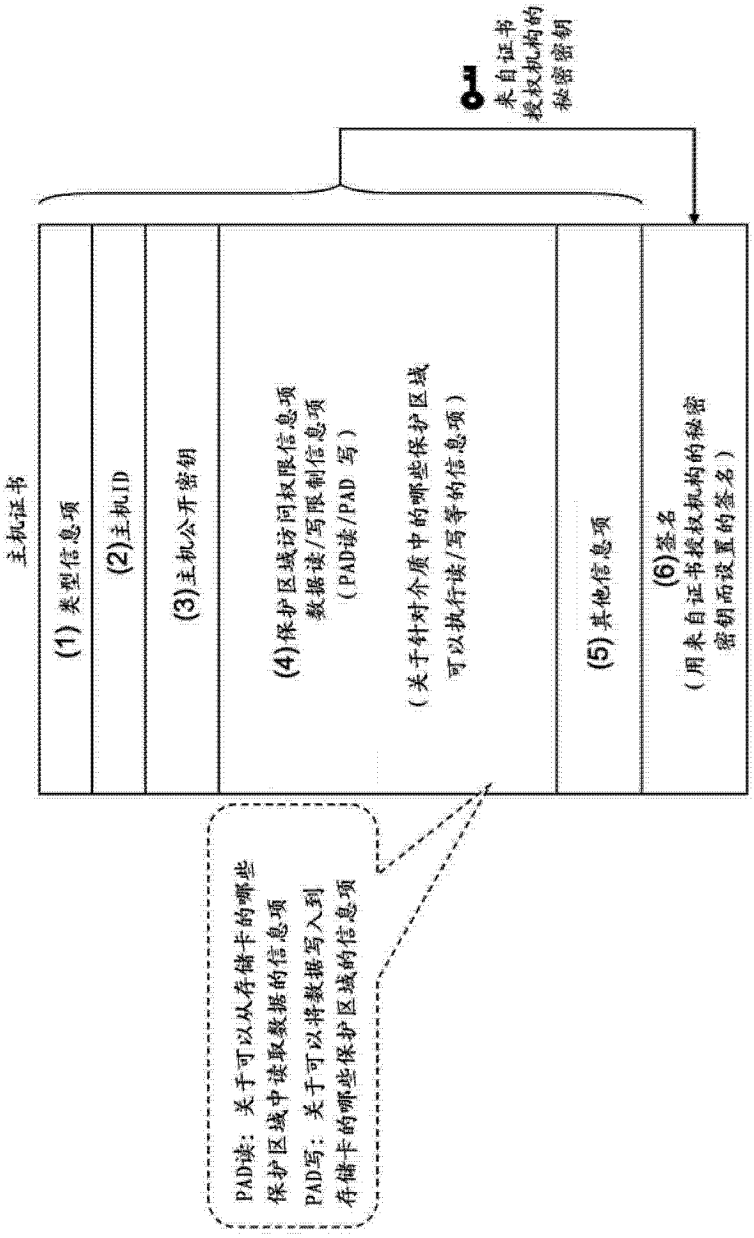

来自证书授权机构的秘密密钥
主机证书
(1) 类型信息项
(2)主机ID
(3)主机公开密钥
(4)保护区域访问权限信息项
数据读/写限制信息项
(PAD读/PAD 写)
(关于针对介质中的哪些保护区域可以执行读/写等的信息项)
(5) 其他信息项
(6)签名
(用来自证书授权机构的秘密密钥而设置的签名)
PAD读：关于可以从存储卡的哪些保护区域中读取数据的信息项
PAD写：关于可以将数据写入到存储卡的哪些保护区域的信息项

图 4

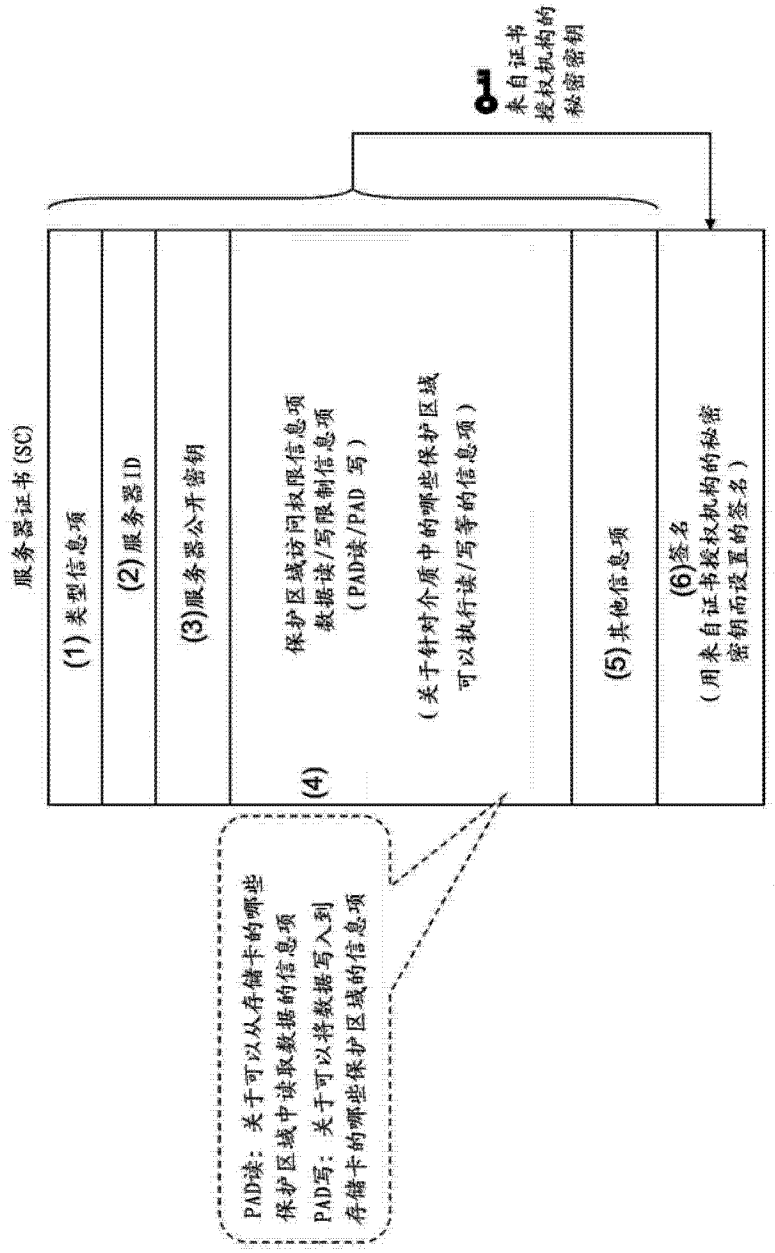

来自证书
授权机构的
秘密密钥
服务器证书(SC)
(1)类型信息项
(2)服务器ID
(3)服务器公开密钥
(4)
保护区域访问权限信息项
数据读/写限制信息项
(PAD读/PAD 写)
(关于针对介质中的哪些保护区域
可以执行读/写等的信息项)
(5)其他信息项
(6)签名
(用来自证书授权机构的秘密
密钥而设置的签名)
PAD读：关于可以从存储卡的哪些
保护区域中读取数据的信息项
PAD写：关于可以将数据写入到
存储卡的哪些保护区域的信息项

图 5

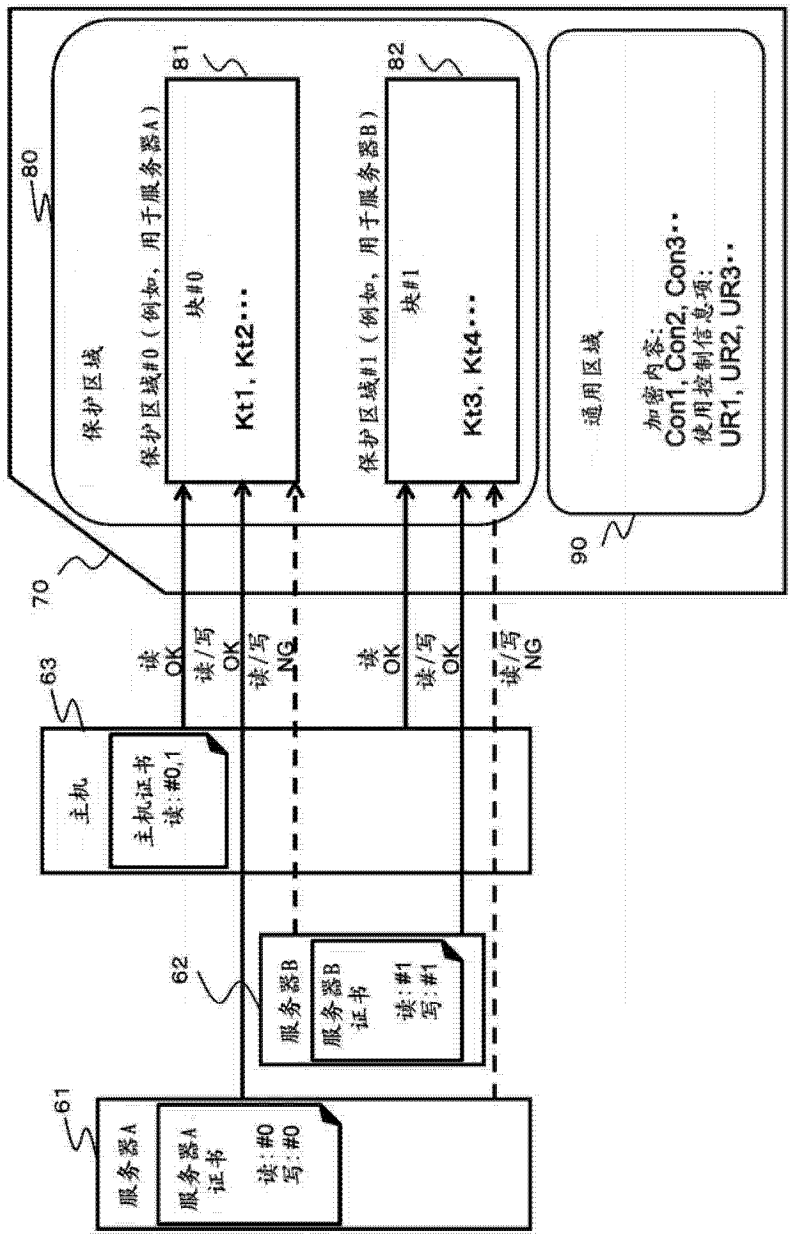

80
保护区域
保护区域#0（例如，用于服务器A）
81
块#0
Kt1, Kt2···
保护区域#1（例如，用于服务器B）
82
块#1
Kt3, Kt4···
通用区域
加密内容:
Con1, Con2, Con3··
使用控制信息项:
UR1, UR2, UR3··
90
70
读
OK
读/写
OK
读/写
NG
读
OK
读/写
OK
读/写
NG
63
主机
主机证书
读:#0,1
62
服务器B
服务器B
证书
读:#1
写:#1
61
服务器A
服务器A
证书
读:#0
写:#0

图 6

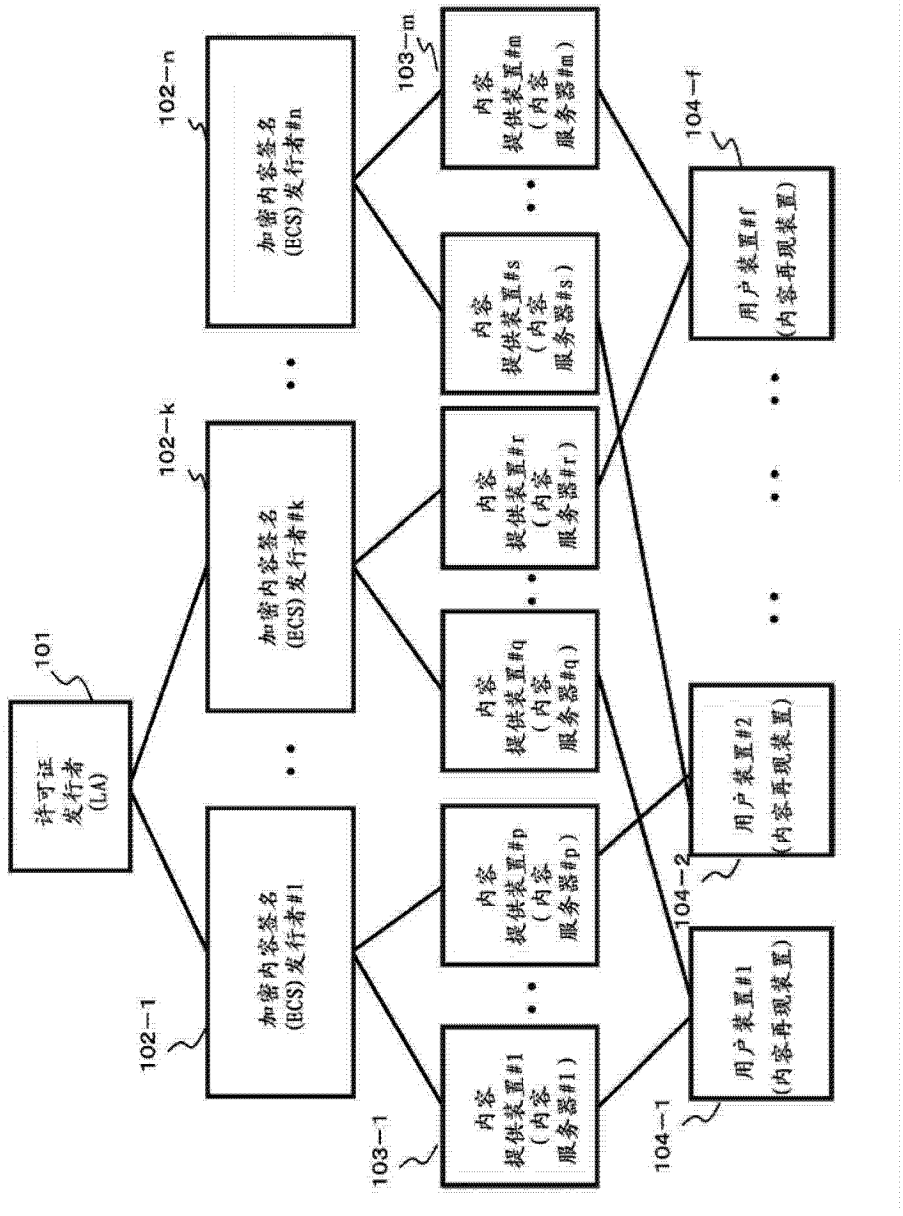

101
许可证
发行者
(LA)
102-1
加密内容签名
(ECS)发行者#1
102-k
加密内容签名
(ECS)发行者#k
102-n
加密内容签名
(ECS)发行者#n
103-1
内容
提供装置#1
(内容
服务器#1)
内容
提供装置#p
(内容
服务器#p)
内容
提供装置#q
(内容
服务器#q)
内容
提供装置#r
(内容
服务器#r)
内容
提供装置#s
(内容
服务器#s)
103-m
内容
提供装置#m
(内容
服务器#m)
104-1
用户装置#1
(内容再现装置)
104-2
用户装置#2
(内容再现装置)
104-f
用户装置#f
(内容再现装置)

图 7

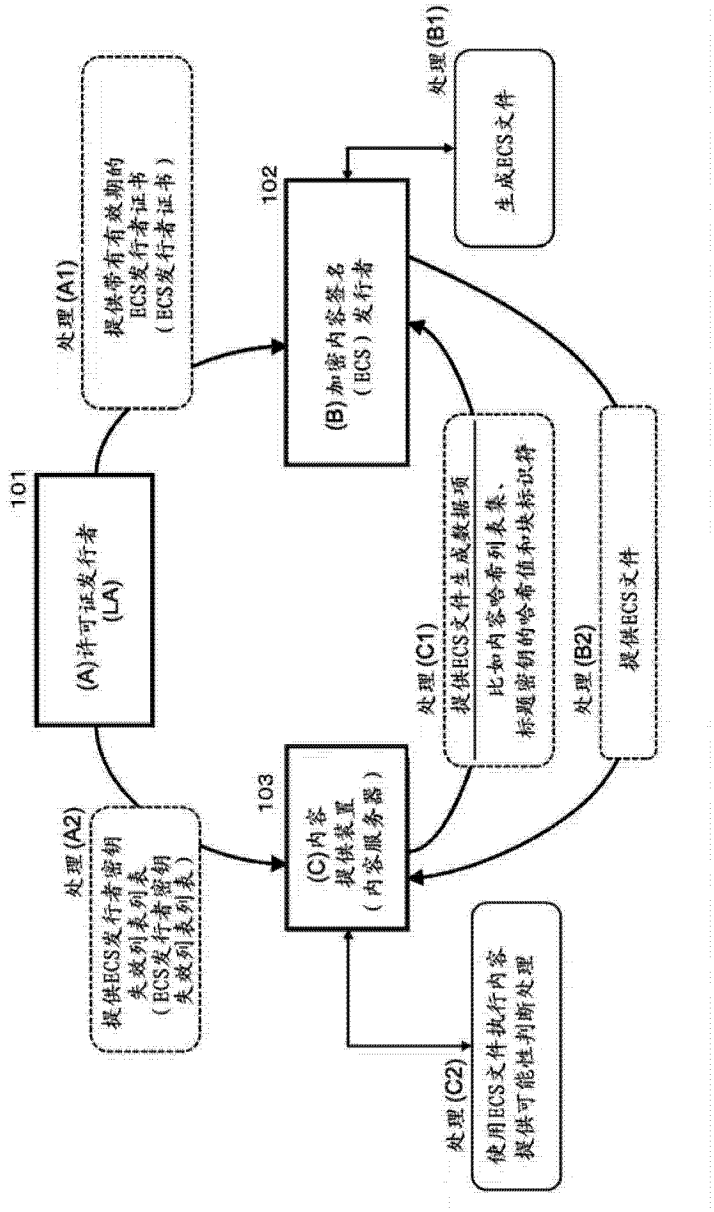

101
(A)许可证发行者
(LA)
处理(A1)
提供带有有效期的
ECS发行者证书
(ECS发行者证书)
102
(B)加密内容签名
(ECS)发行者
处理(B1)
生成ECS文件
处理(A2)
提供ECS发行者密钥
失效列表列表
(ECS发行者密钥
失效列表列表)
103
(C)内容
提供装置
(内容服务器)
处理(C1)
提供ECS文件生成数据项
比如内容哈希列表集、
标题密钥的哈希值和块标识符
处理(B2)
提供ECS文件
处理(C2)
使用ECS文件执行内容
提供可能性判断处理

图 8

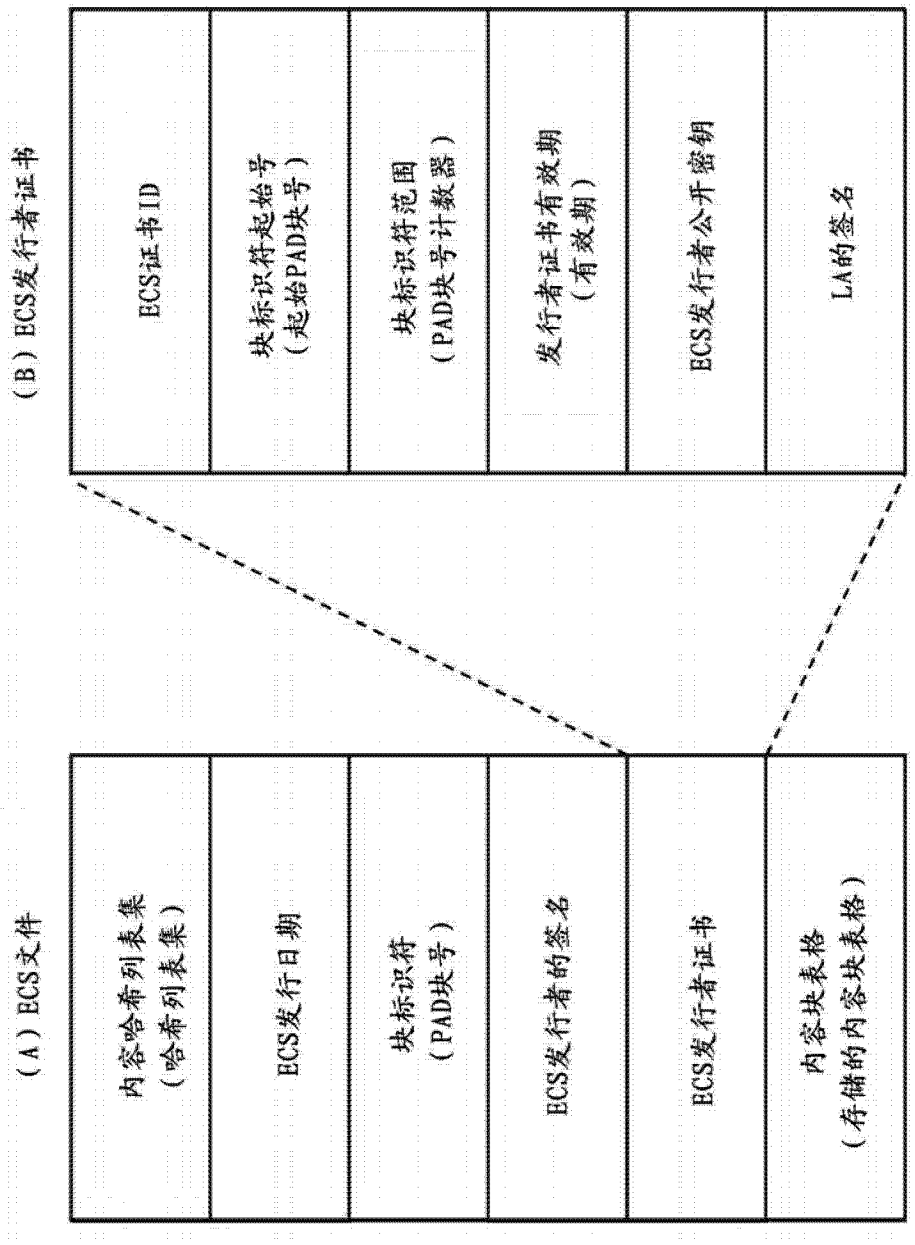

（A）ECS文件
内容哈希列表集
（哈希列表集）
ECS发行日期
块标识符
（PAD块号）
ECS发行者的签名
ECS发行者证书
内容块表格
（存储的内容块表格）
（B）ECS发行者证书
ECS证书ID
块标识符起始号
（起始PAD块号）
块标识符范围
（PAD块号计数器）
发行者证书有效期
（有效期）
ECS发行者公开密钥
LA的签名

图 9

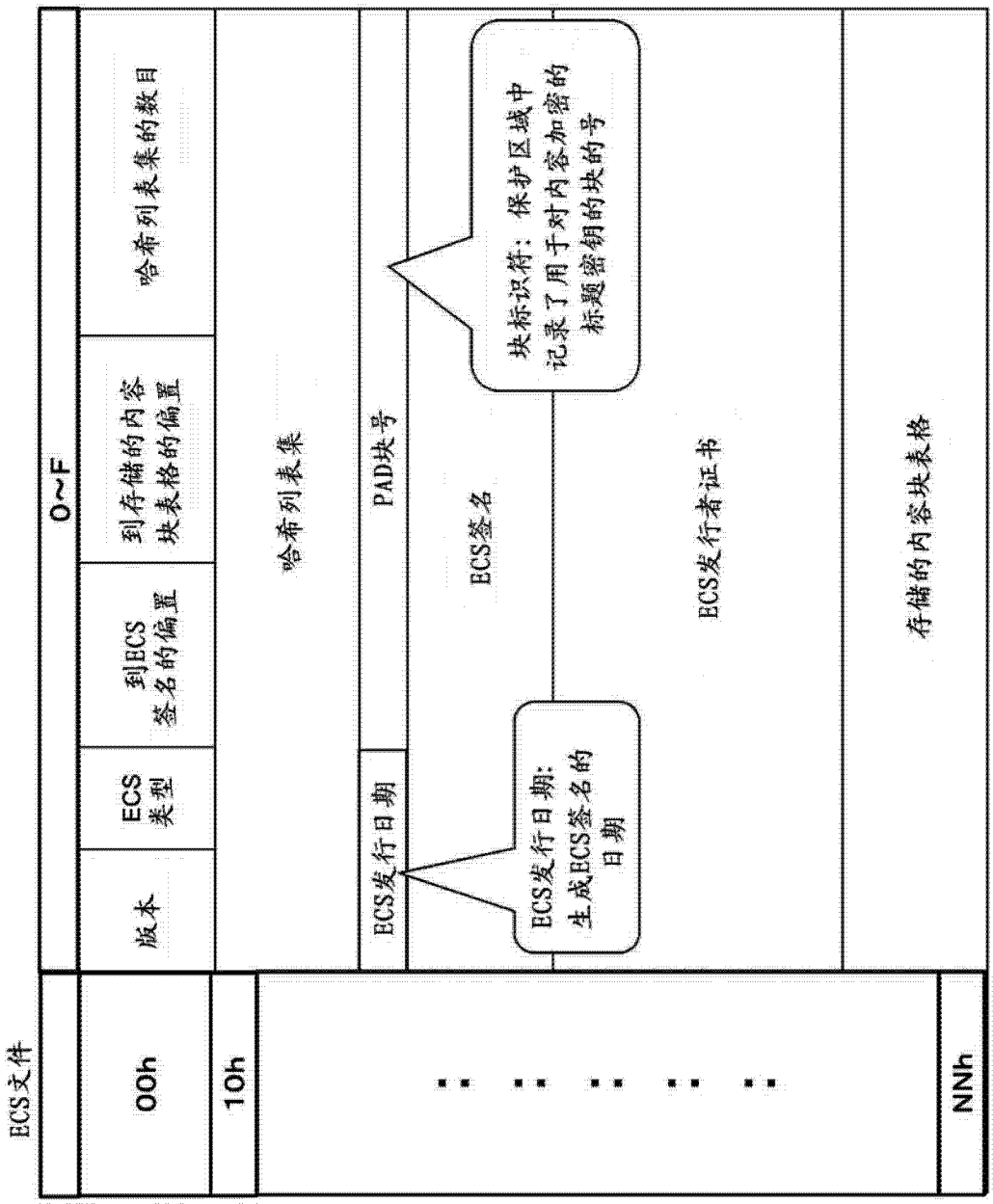

ECS文件
00h
10h
NNh
0~F
版本
ECS类型
到ECS签名的偏置
到存储的内容块表格的偏置
哈希列表集的数目
哈希列表集
ECS发行日期
PAD块号
ECS签名
ECS发行者证书
存储的内容块表格
ECS发行日期：生成ECS签名的日期
块标识符：保护区域中记录了用于对内容加密的标题密钥的块的号

图 10

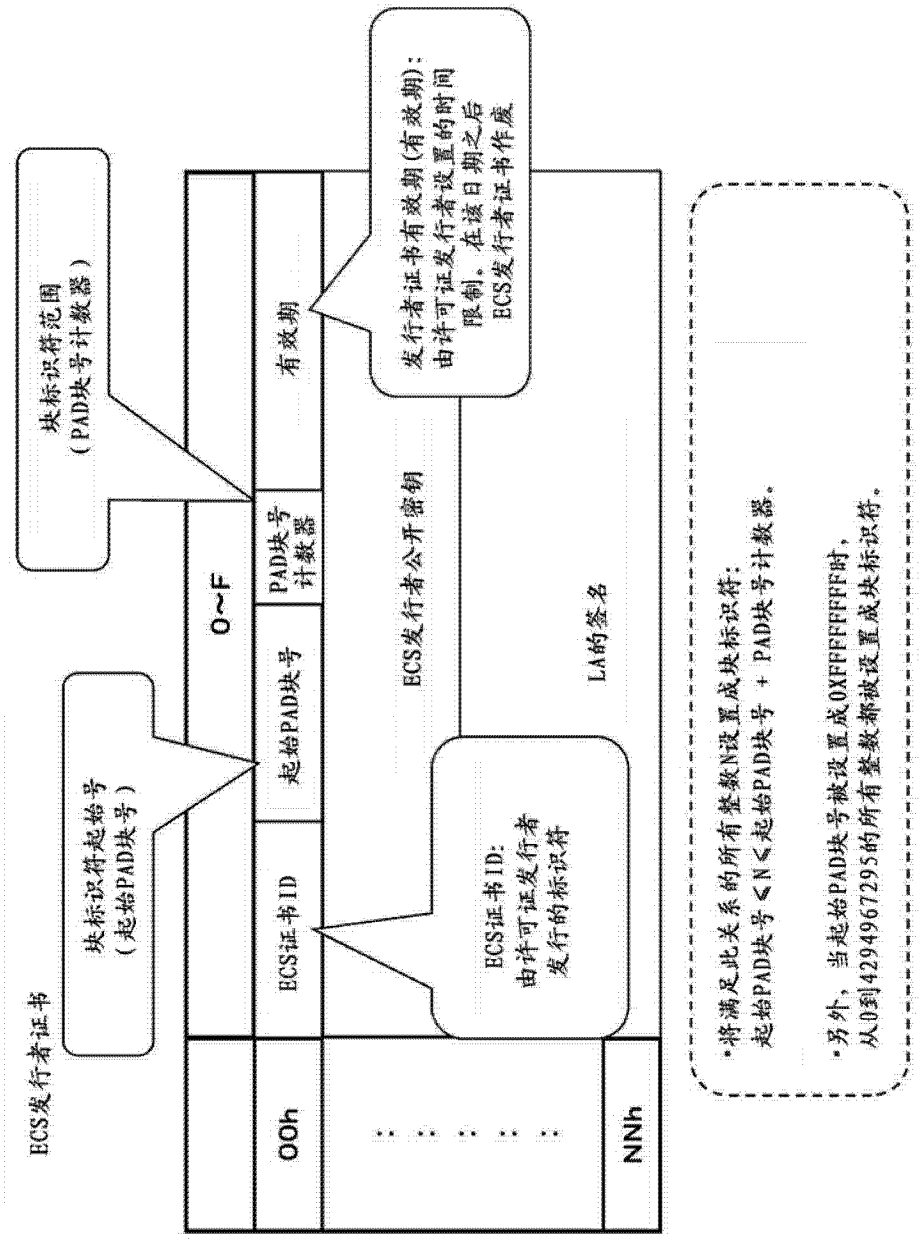

ECS发行者证书
块标识符起始号
（起始PAD块号）
块标识符范围
（PAD块号计数器）
发行者证书有效期(有效期)：
由许可证发行者设置的时间
限制，在该日期之后
ECS发行者证书作废
0~F
ECS证书ID
起始PAD块号
PAD块号
计数器
有效期
ECS发行者公开密钥
ECS证书ID:
由许可证发行者
发行的标识符
LA的签名
00h
NNh
•将满足此关系的所有整数N设置成块标识符:
起始PAD块号 ≤ N ≤起始PAD块号 + PAD块号计数器。
•另外，当起始PAD块号被设置成0XFFFFFFFF时，
从0到4294967295的所有整数都被设置成块标识符。

图 11

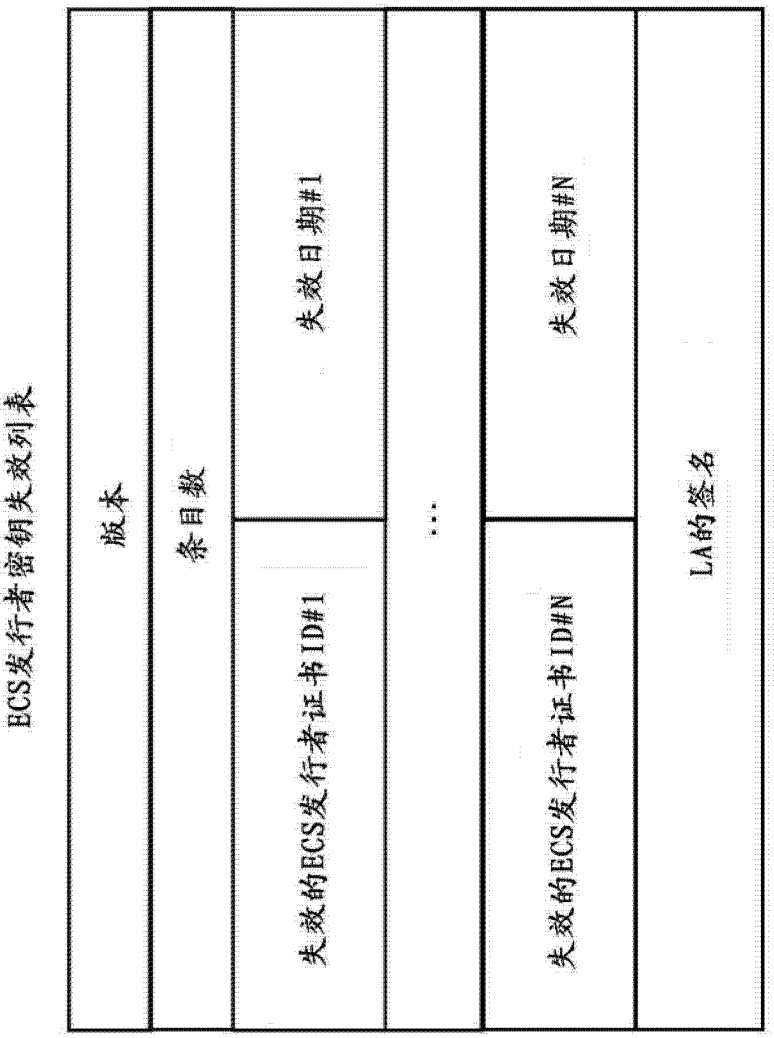

ECS发行者密钥失效列表
版本
条目数
失效的ECS发行者证书ID#1
失效日期#1
...
失效的ECS发行者证书ID#N
失效日期#N
LA的签名

图 12

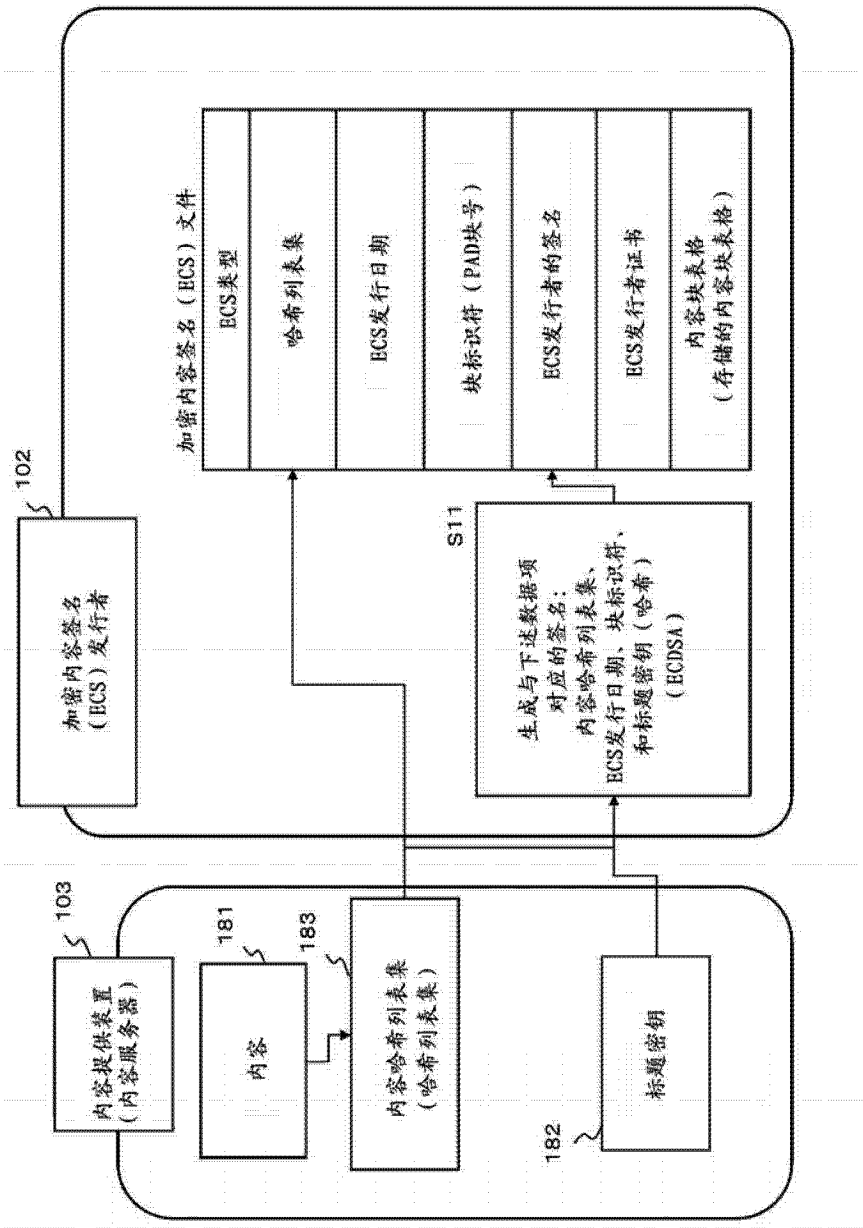

102
加密内容签名（ECS）发行者
加密内容签名（ECS）文件
ECS类型
哈希列表集
ECS发行日期
块标识符（PAD块号）
ECS发行者的签名
ECS发行者证书
内容块表格
（存储的内容块表格）
S11
生成与下述数据项
对应的签名：
内容哈希列表集，
ECS发行日期，块标识符，
和标题密钥（哈希）
（ECDSA）
103
内容提供装置
（内容服务器）
181
内容
183
内容哈希列表集
（哈希列表集）
182
标题密钥

图 13

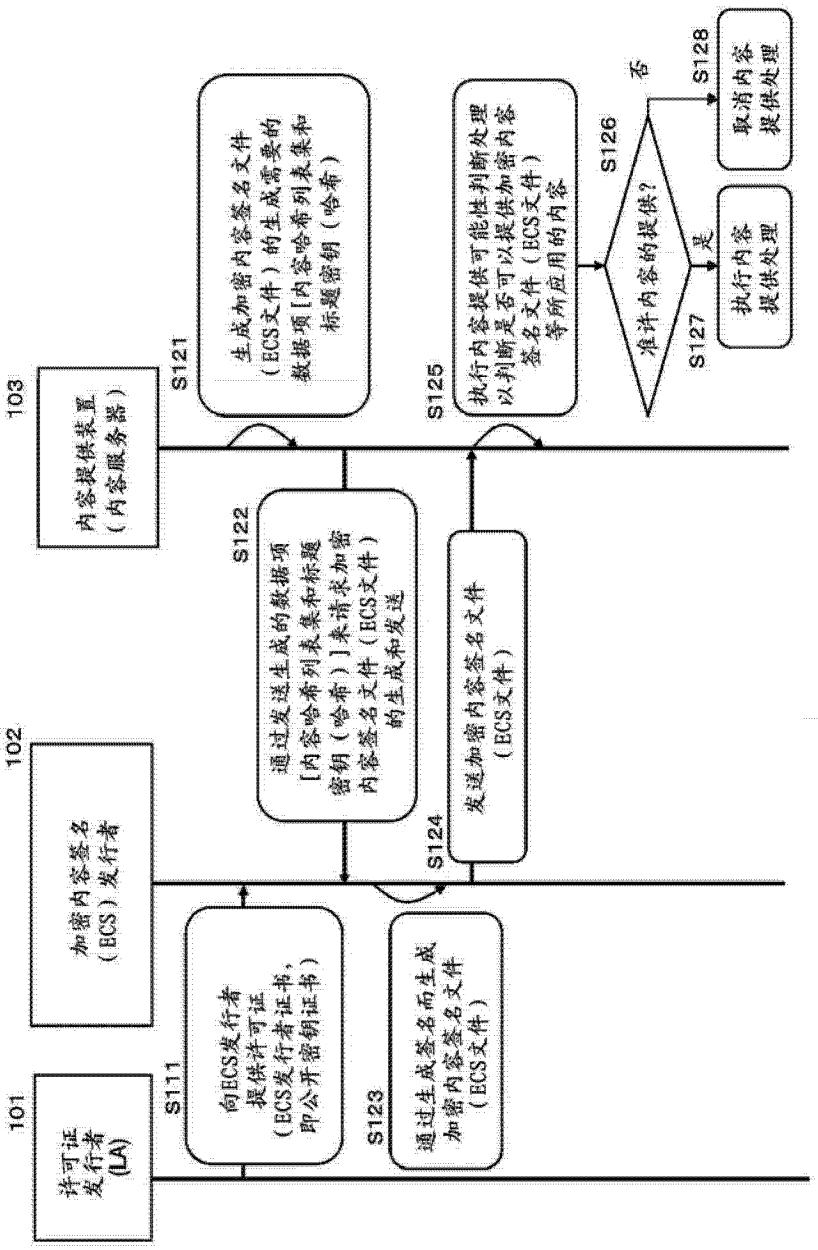

101
许可证发行者(LA)
102
加密内容签名者(ECS)发行者
103
内容提供装置(内容服务器)
S111
向ECS发行者提供许可证(ECS发行者证书,即公开密钥证书)
S121
生成加密内容签名文件(ECS文件)的生成需要的数据项[内容哈希列表集和标题密钥(哈希)
S122
通过发送生成的数据项[内容哈希列表集和标题密钥(哈希)]来请求加密内容签名文件(ECS文件)的生成和发送
S123
通过生成签名而生成加密内容签名文件(ECS文件)
S124
发送加密内容签名文件(ECS文件)
S125
执行内容提供可能性判断处理以判断是否可以提供加密内容签名文件(ECS文件)等所应用的内容
S126
准许内容的提供?
否
是
S127
执行内容提供处理
S128
取消内容提供处理

图 14

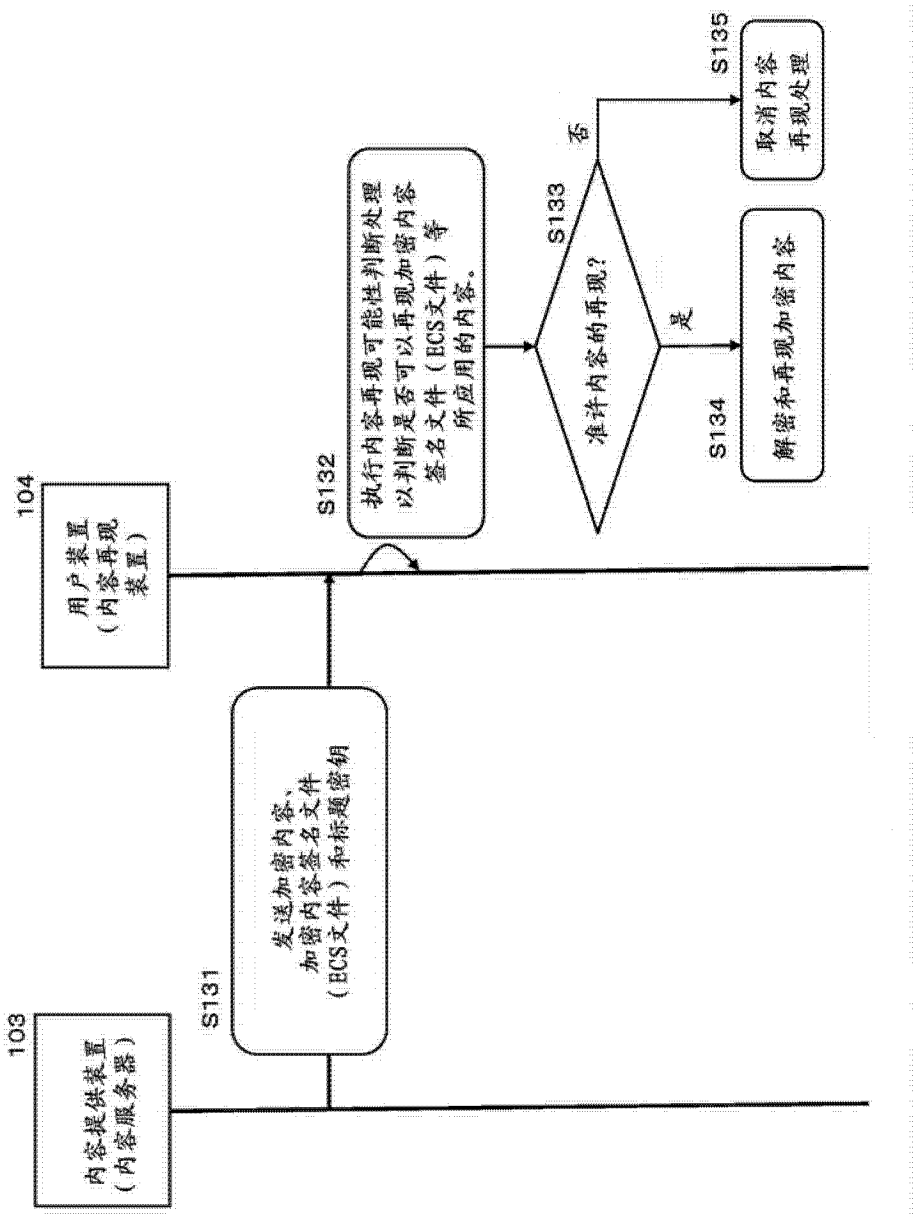

103
内容提供装置
（内容服务器）
S131
发送加密内容、
加密内容签名文件
（ECS文件）和标题密钥
104
用户装置
（内容再现
装置）
S132
执行内容再现可能性判断处理
以判断是否可以再现加密内容
签名文件（ECS文件）等
所应用的内容。
S133
准许内容的再现?
是
否
S134
解密和再现加密内容
S135
取消内容
再现处理

图 15

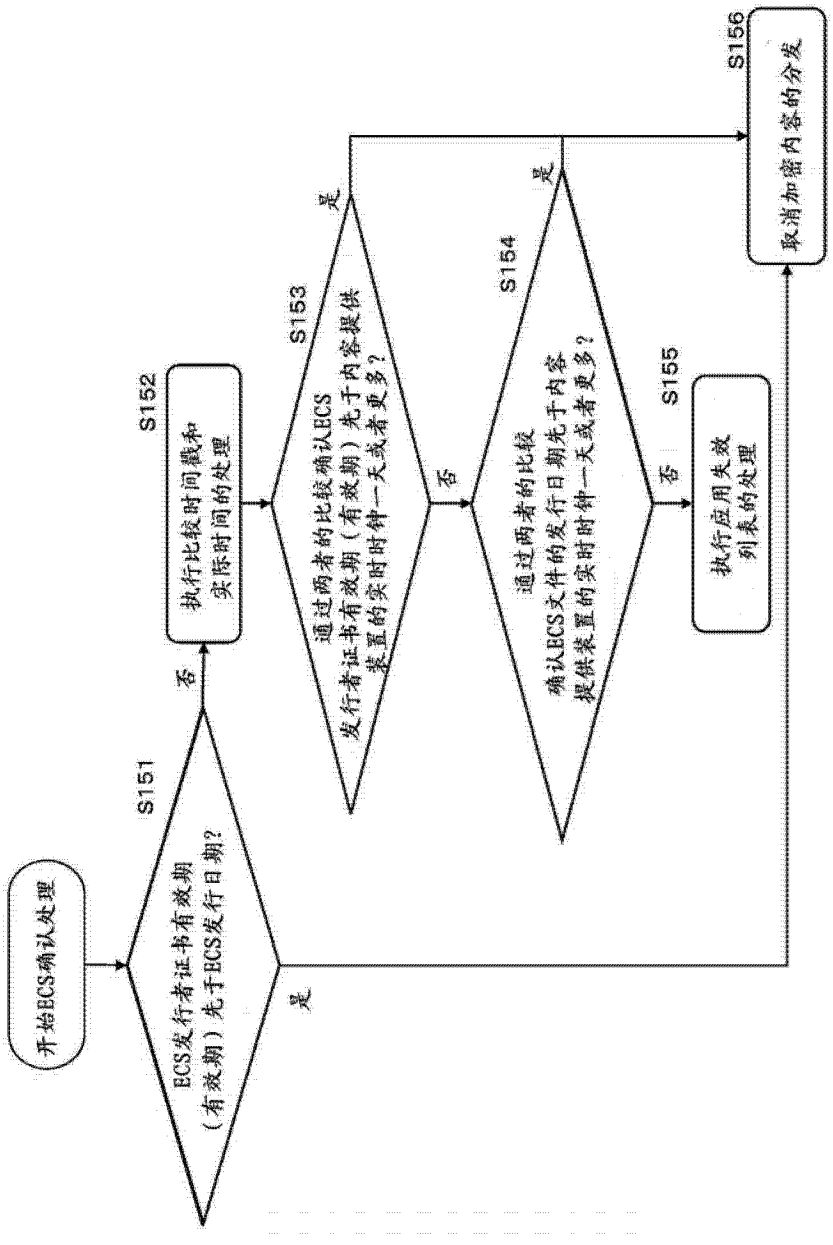

开始ECS确认处理
S151
ECS发行者证书有效期（有效期）先于ECS发行日期?
否
是
S152
执行比较时间截和实际时间的处理
S153
通过两者的比较确认ECS发行者证书有效期（有效期）先于内容提供装置的实时时钟一天或者更多?
否
是
S154
通过两者的比较确认ECS文件的发行日期先于内容提供装置的实时时钟一天或者更多?
否
是
S155
执行应用失效列表的处理
S156
取消加密内容的分发

图 16

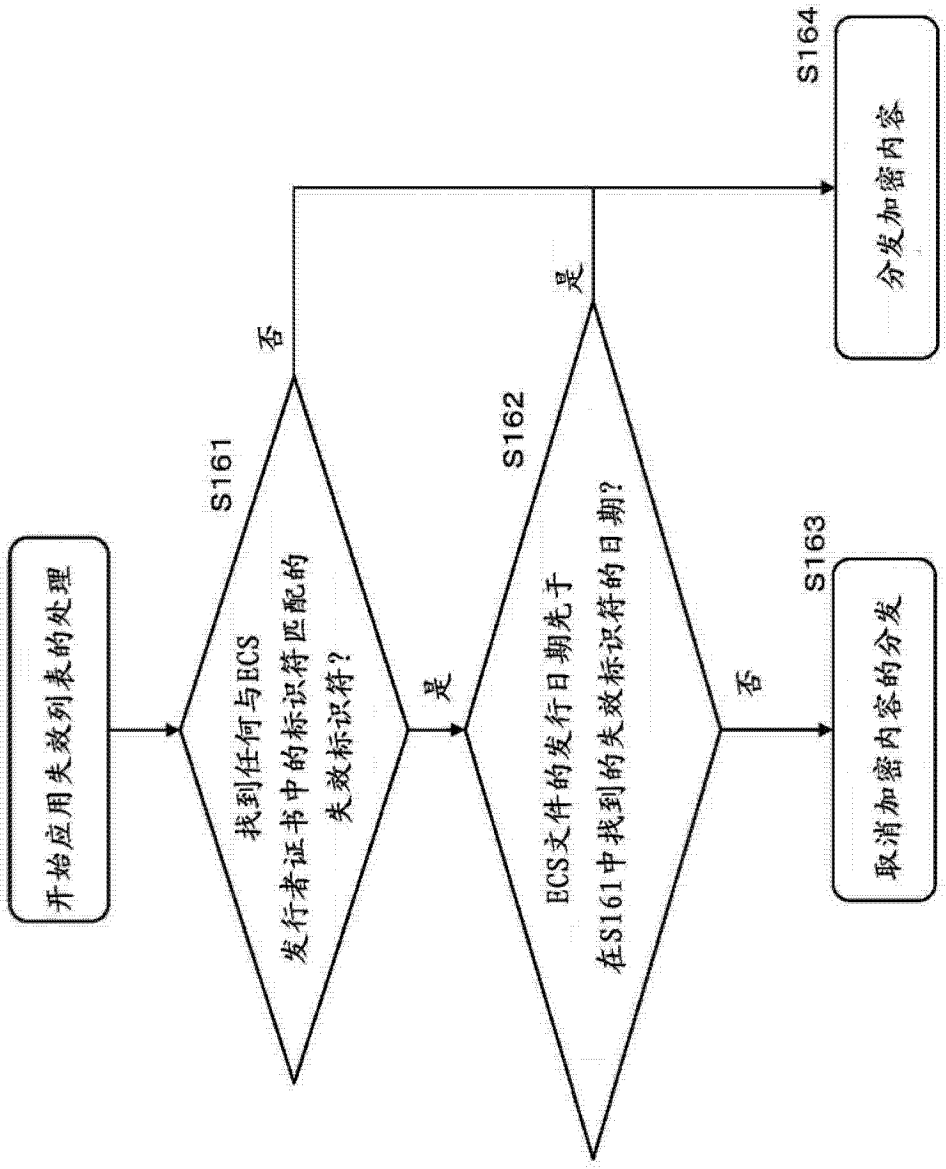

开始应用失效列表的处理
S161
找到任何与ECS
发行者证书中的标识符匹配的
失效标识符?
否
是
S162
ECS文件的发行日期先于
在S161中找到的失效标识符的日期?
是
否
S163
取消加密内容的分发
S164
分发加密内容

图 17

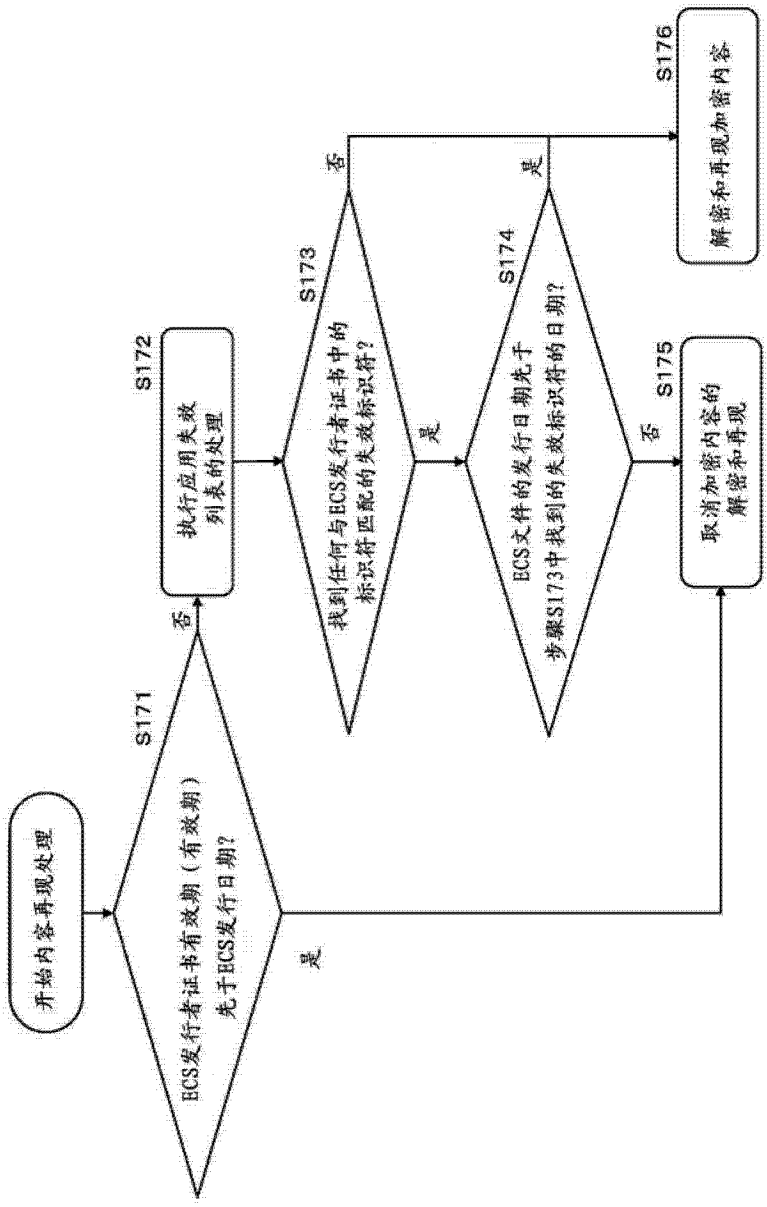

开始内容再现处理
S171
ECS发行者证书有效期（有效期）先于ECS发行日期?
否
是
S172
执行应用失效列表的处理
S173
找到任何与ECS发行者证书中的标识符匹配的失效标识符?
否
是
S174
ECS文件的发行日期先于步骤S173中找到的失效标识符的日期?
是
否
S175
取消加密内容的解密和再现
S176
解密和再现加密内容

图 18

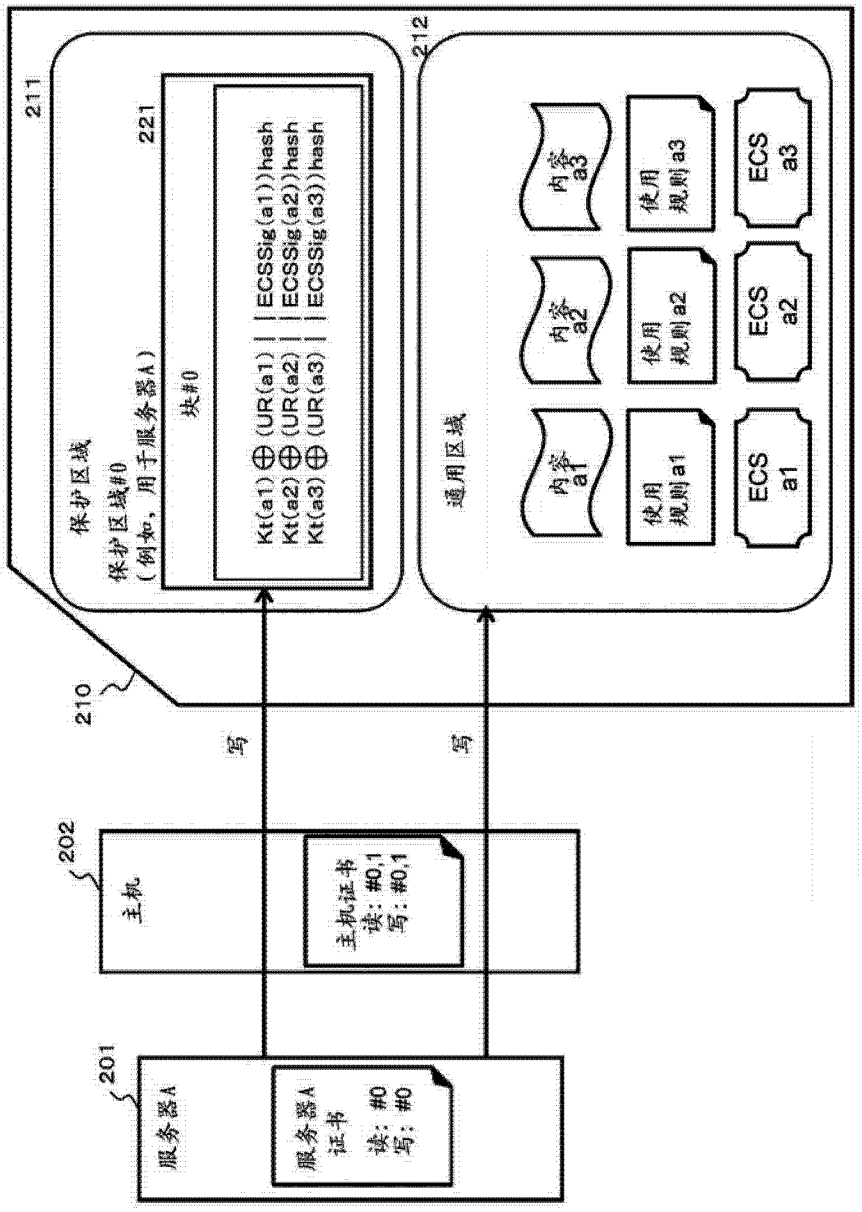

服务器A
服务器A
证书
读：#0
写：#0
201
主机
主机证书
读：#0,1
写：#0,1
202
写
写
210
211
保护区域
保护区域#0
（例如，用于服务器A）
221
块#0
Kt(a1)⊕(UR(a1)||ECSSig(a1))hash
Kt(a2)⊕(UR(a2)||ECSSig(a2))hash
Kt(a3)⊕(UR(a3)||ECSSig(a3))hash
212
通用区域
内容a1
使用规则a1
ECS a1
内容a2
使用规则a2
ECS a2
内容a3
使用规则a3
ECS a3

图 19

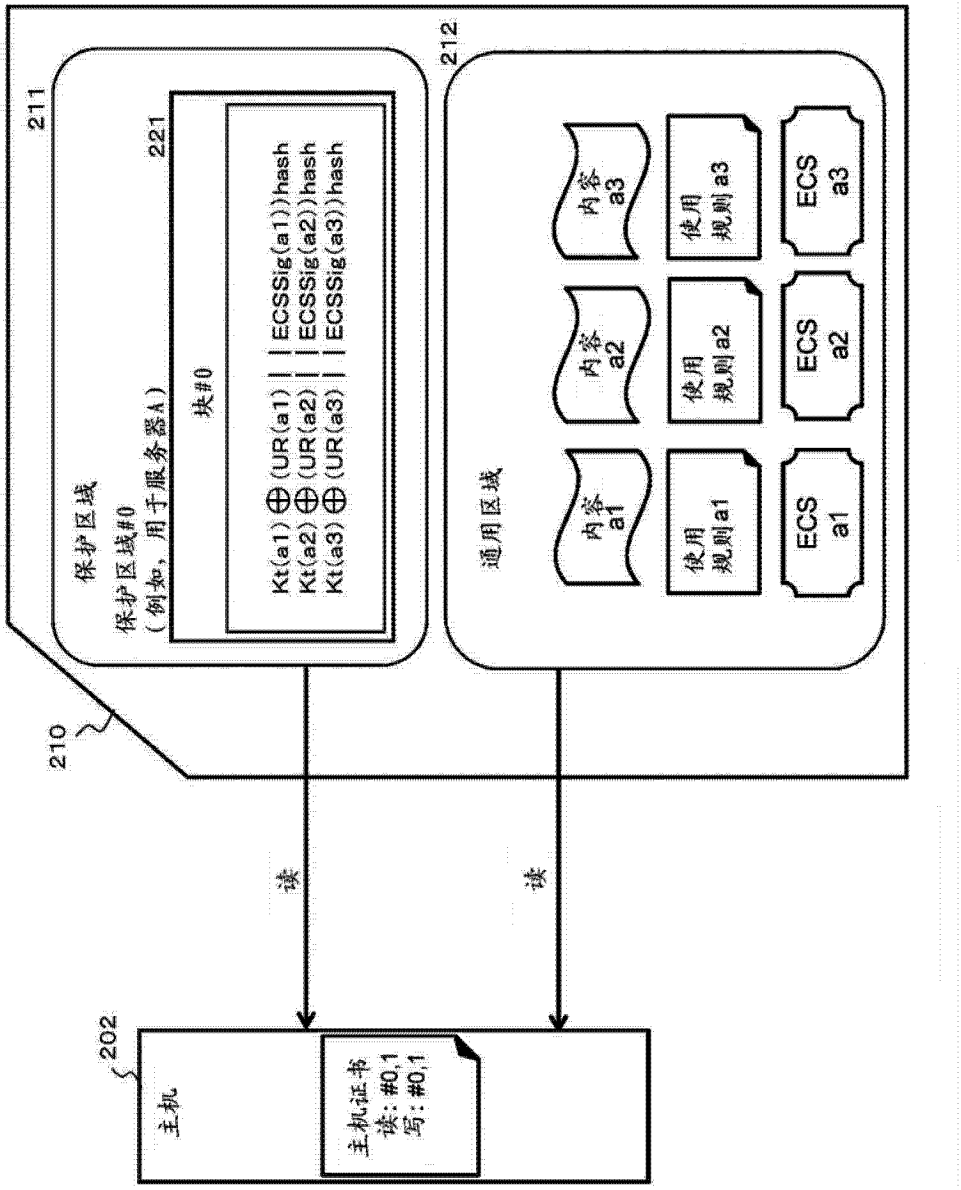

211
保护区域
保护区域#0
（例如，用于服务器A）
221
块#0
Kt(a1) ⊕ (UR(a1) | | ECSSig(a1))hash
Kt(a2) ⊕ (UR(a2) | | ECSSig(a2))hash
Kt(a3) ⊕ (UR(a3) | | ECSSig(a3))hash
212
通用区域
内容 a1
使用规则a1
ECS a1
内容 a2
使用规则a2
ECS a2
内容 a3
使用规则a3
ECS a3
210
读
读
202
主机
主机证书
读：#0,1
写：#0,1

图 20

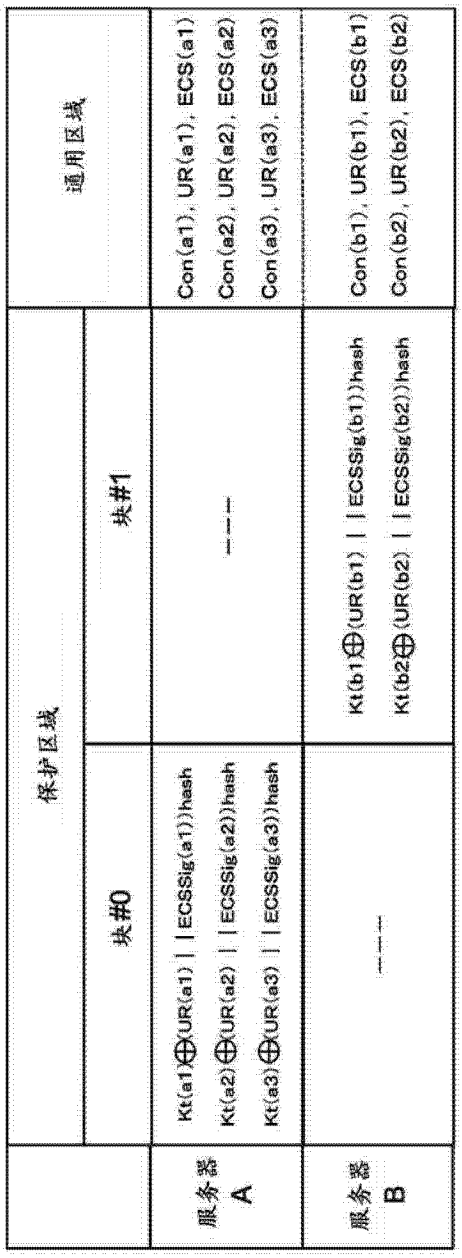

保护区域
通用区域
块#0
块#1
服务器A
Kt(a1)⊕(UR(a1)||ECSSig(a1))hash
Kt(a2)⊕(UR(a2)||ECSSig(a2))hash
Kt(a3)⊕(UR(a3)||ECSSig(a3))hash
---
Con(a1), UR(a1), ECS(a1)
Con(a2), UR(a2), ECS(a2)
Con(a3), UR(a3), ECS(a3)
服务器B
---
Kt(b1)⊕(UR(b1)||ECSSig(b1))hash
Kt(b2)⊕(UR(b2)||ECSSig(b2))hash
Con(b1), UR(b1), ECS(b1)
Con(b2), UR(b2), ECS(b2)

图 21

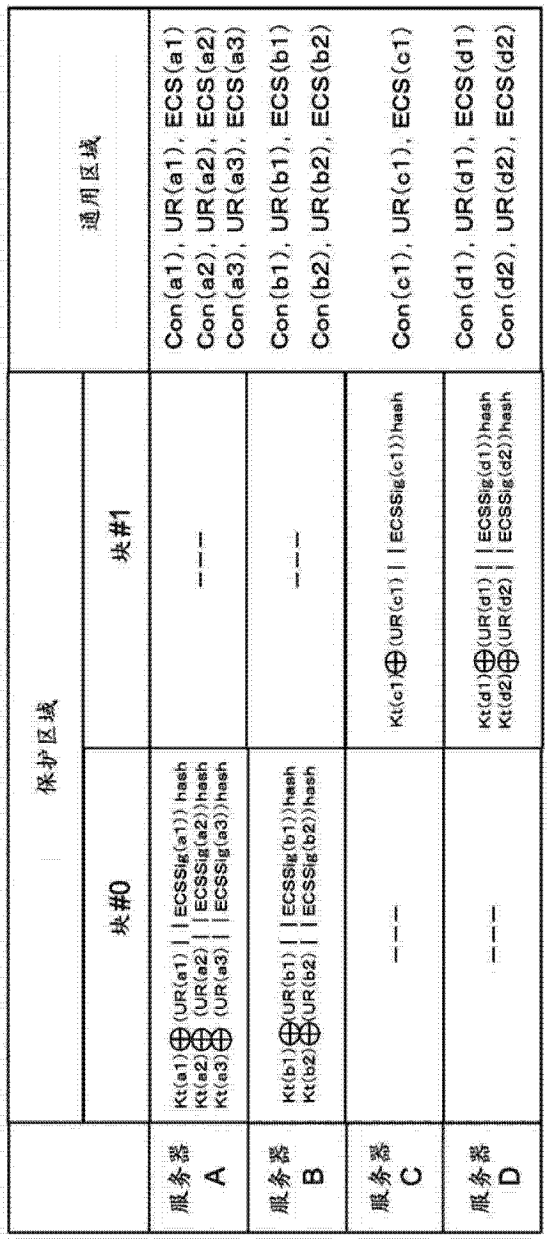

保护区域
通用区域
块#0
块#1
服务器A
Kt(a1)⊕(UR(a1)||ECSSig(a1))hash
Kt(a2)⊕(UR(a2)||ECSSig(a2))hash
Kt(a3)⊕(UR(a3)||ECSSig(a3))hash
---
Con(a1), UR(a1), ECS(a1)
Con(a2), UR(a2), ECS(a2)
Con(a3), UR(a3), ECS(a3)
服务器B
Kt(b1)⊕(UR(b1)||ECSSig(b1))hash
Kt(b2)⊕(UR(b2)||ECSSig(b2))hash
---
Con(b1), UR(b1), ECS(b1)
Con(b2), UR(b2), ECS(b2)
服务器C
---
Kt(c1)⊕(UR(c1)||ECSSig(c1))hash
Con(c1), UR(c1), ECS(c1)
服务器D
---
Kt(d1)⊕(UR(d1)||ECSSig(d1))hash
Kt(d2)⊕(UR(d2)||ECSSig(d2))hash
Con(d1), UR(d1), ECS(d1)
Con(d2), UR(d2), ECS(d2)

图 22

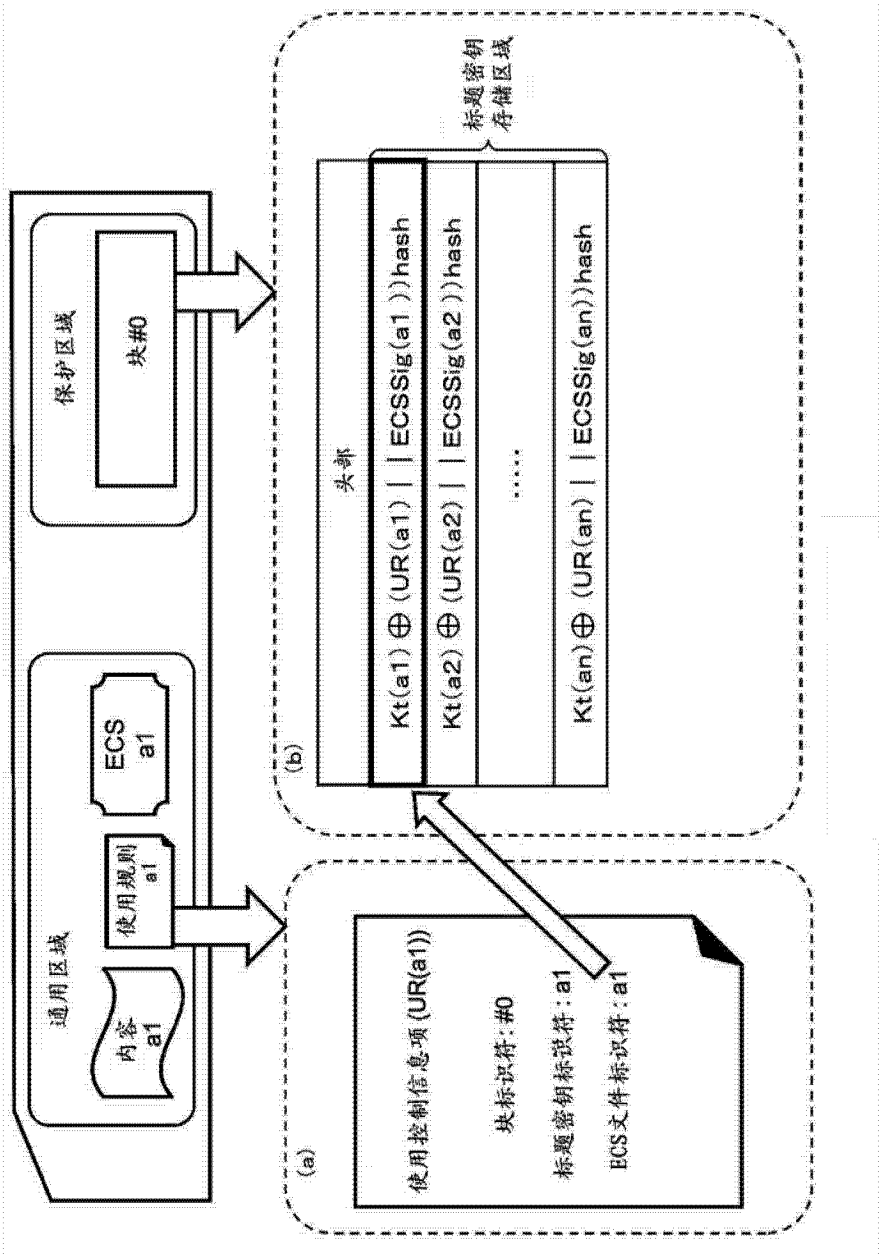

保护区域
块#0
通用区域
ECS
a1
使用规则
a1
内容
a1
(a)
使用控制信息项(UR(a1))
块标识符:#0
标题密钥标识符:a1
ECS文件标识符:a1
(b)
头部
标题密钥
存储区域
Kt(a1)⊕(UR(a1)||ECSSig(a1))hash
Kt(a2)⊕(UR(a2)||ECSSig(a2))hash
.....
Kt(an)⊕(UR(an)||ECSSig(an))hash

图 23

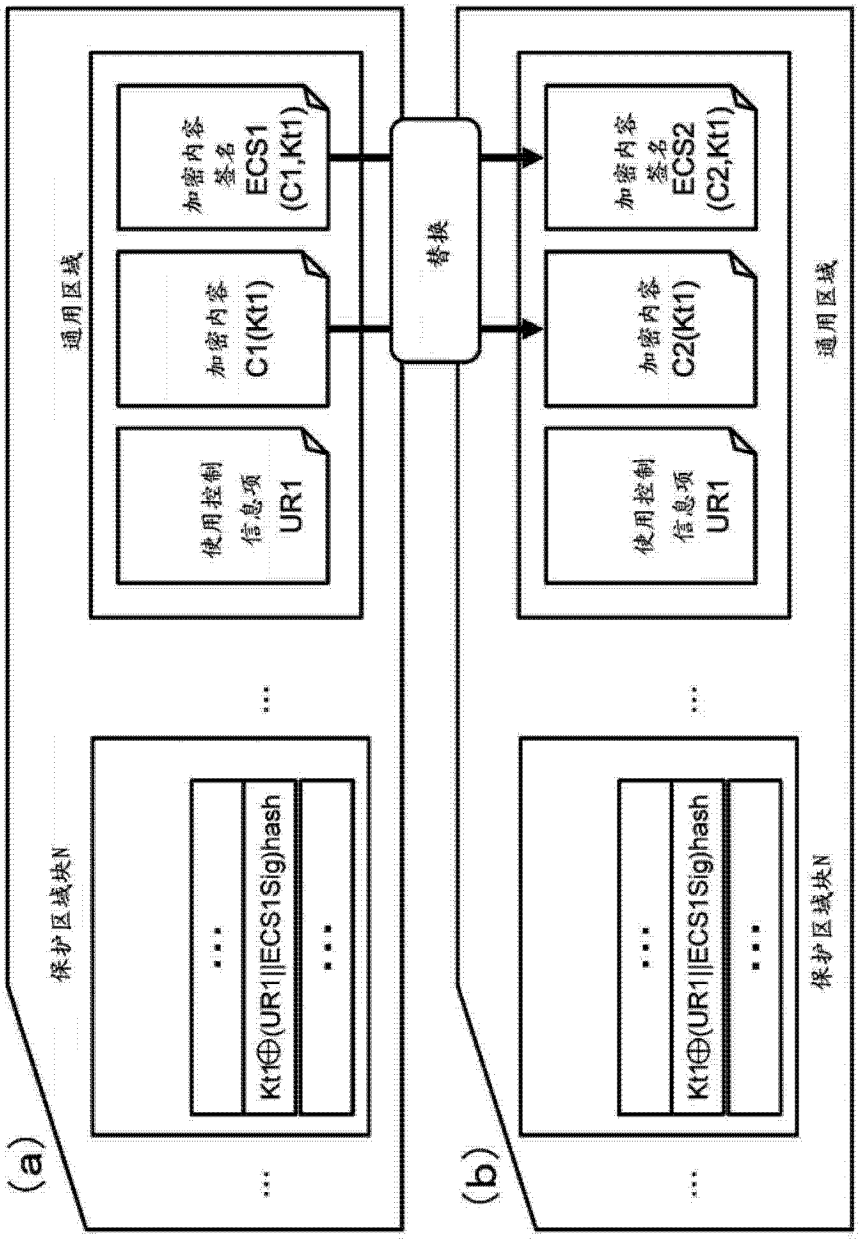

(a)
通用区域
加密内容签名 ECS1 (C1,Kt1)
加密内容 C1(Kt1)
使用控制信息项 UR1
保护区域块N
Kt1⊕(UR1||ECS1Sig)hash
替换
(b)
通用区域
加密内容签名 ECS2 (C2,Kt1)
加密内容 C2(Kt1)
使用控制信息项 UR1
保护区域块N
Kt1⊕(UR1||ECS1Sig)hash

图 24

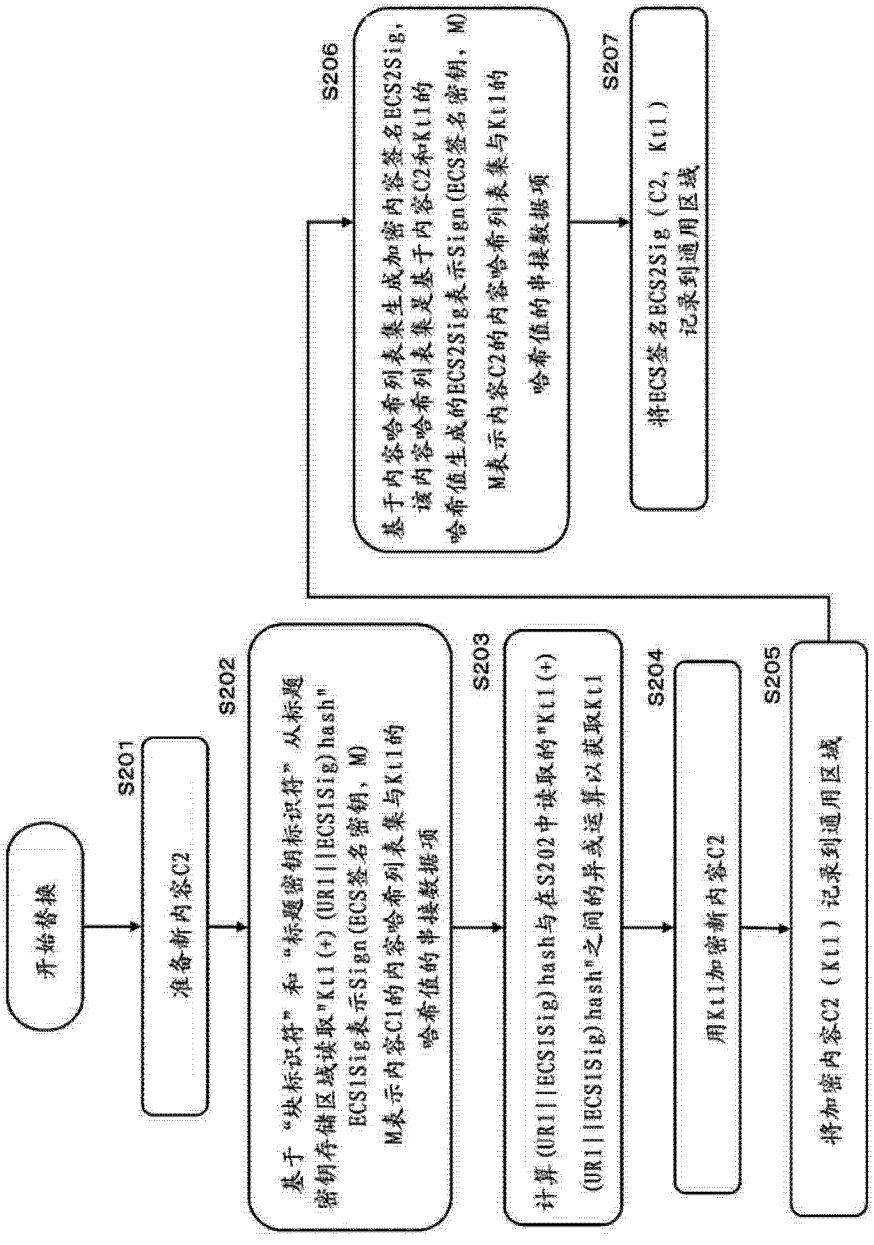

开始替换
S201
准备新内容C2
S202
基于“块标识符”和“标题密钥标识符”从标题密钥存储区域读取"Kt1(+)(UR1||ECS1Sig)hash"
ECS1Sig表示Sign(ECS签名密钥，M)
M表示内容C1的内容哈希列表集与Kt1的哈希值的串接数据项
S203
计算(UR1||ECS1Sig)hash与在S202中读取的"Kt1(+)(UR1||ECS1Sig)hash"之间的异或运算以获取Kt1
S204
用Kt1加密新内容C2
S205
将加密内容C2（Kt1）记录到通用区域
S206
基于内容哈希列表集生成加密内容签名ECS2Sig，该内容哈希列表集是基于内容C2和Kt1的哈希值生成的ECS2Sig表示Sign(ECS签名密钥，M)
M表示内容C2的内容哈希列表集与Kt1的哈希值的串接数据项
S207
将ECS签名ECS2Sig（C2，Kt1）记录到通用区域

图 25

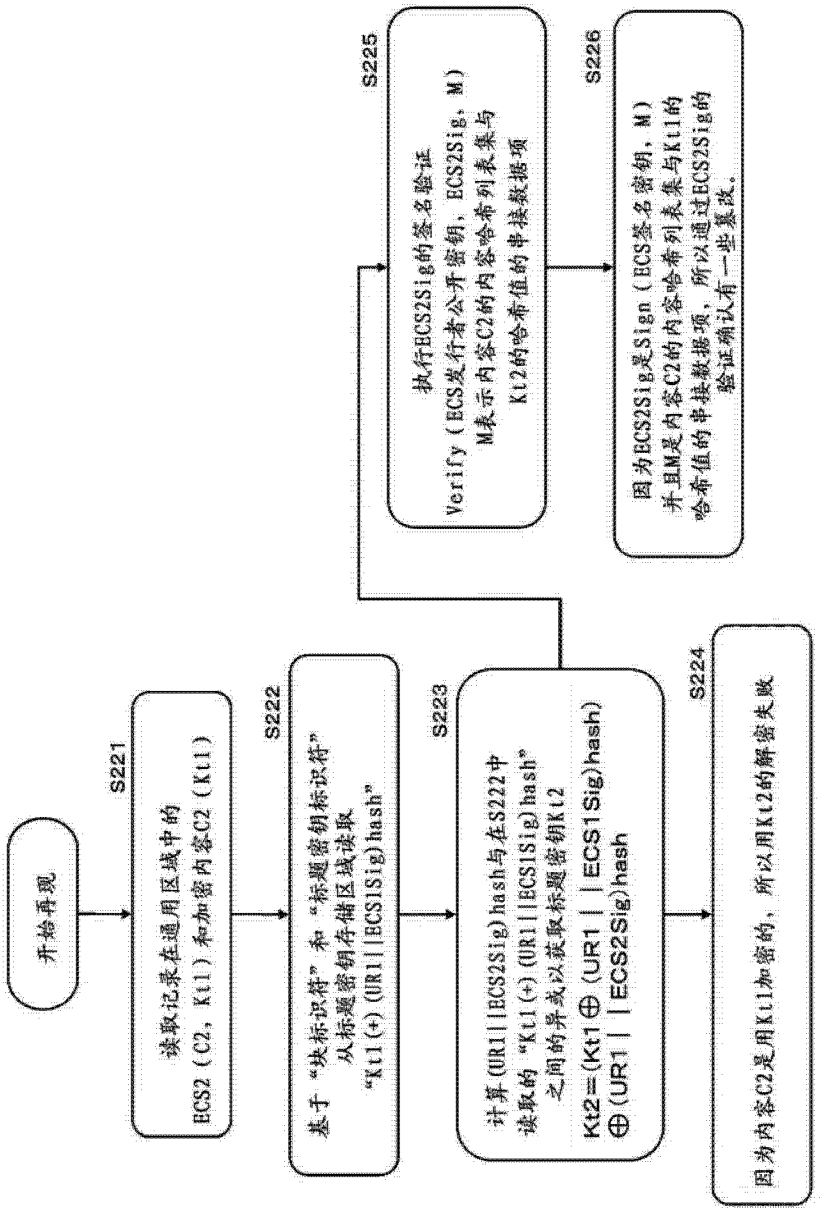

开始再现
S221
读取记录在通用区域中的
ECS2（C2，Kt1）和加密内容C2（Kt1）
S222
基于“块标识符”和“标题密钥标识符”
从标题密钥存储区域读取
“Kt1(+)(UR1||ECS1Sig)hash”
S223
计算(UR1||ECS2Sig)hash与在S222中
读取的“Kt1(+)(UR1||ECS1Sig)hash”
之间的异或以获取标题密钥Kt2
Kt2=(Kt1⊕(UR1||ECS1Sig)hash)
⊕(UR1||ECS2Sig)hash
S224
因为内容C2是用Kt1加密的，所以用Kt2的解密失败
S225
执行ECS2Sig的签名验证
Verify（ECS发行者公开密钥，ECS2Sig，M）
M表示内容C2的内容哈希列表集与
Kt2的哈希值的串接数据项
S226
因为ECS2Sig是Sign（ECS签名密钥，M）
并且M是内容C2的内容哈希列表集与Kt1的
哈希值的串接数据项，所以通过ECS2Sig的
验证确认有一些篡改。

图 26

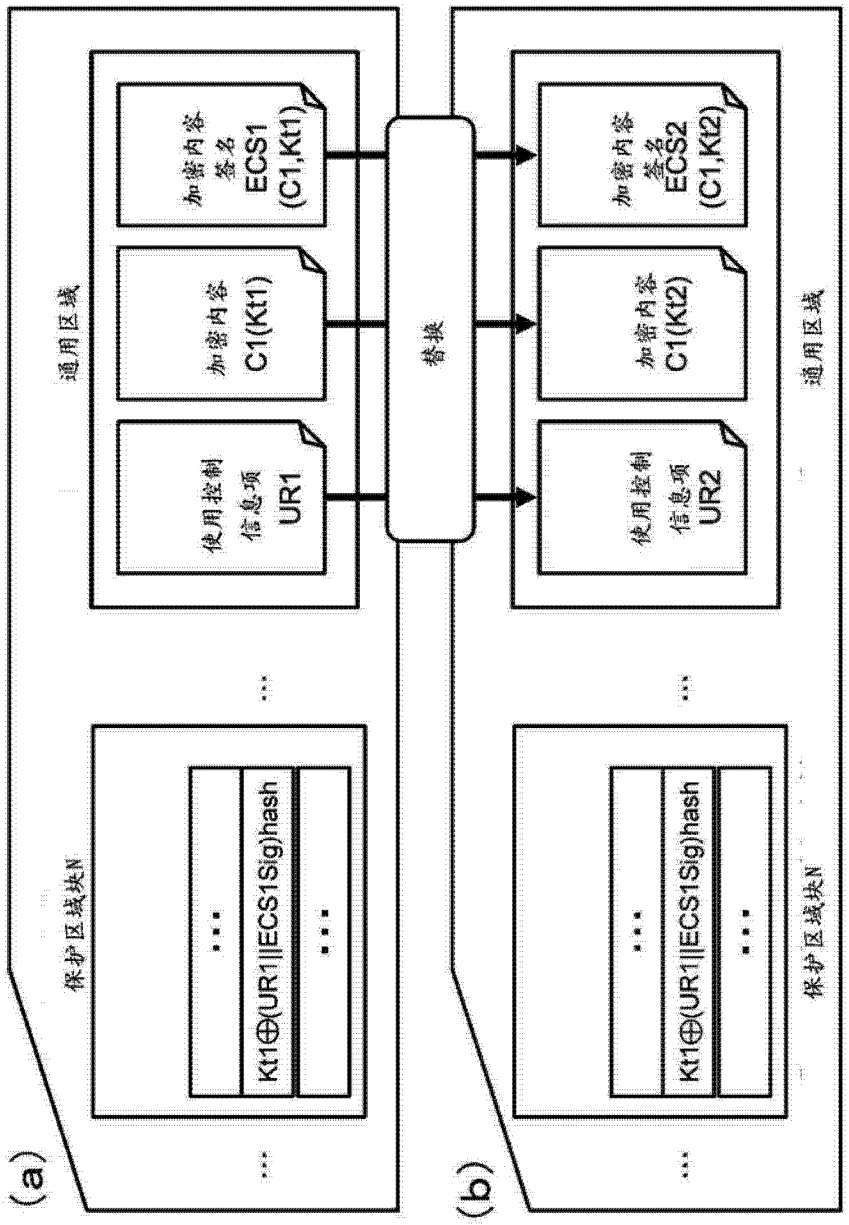

(a)
通用区域
加密内容
签名
ECS1
(C1,Kt1)
加密内容
C1(Kt1)
使用控制
信息项
UR1
保护区域块N
Kt1⊕(UR1||ECS1Sig)hash
替换
(b)
通用区域
加密内容
签名
ECS2
(C1,Kt2)
加密内容
C1(Kt2)
使用控制
信息项
UR2
保护区域块N
Kt1⊕(UR1||ECS1Sig)hash

图 27

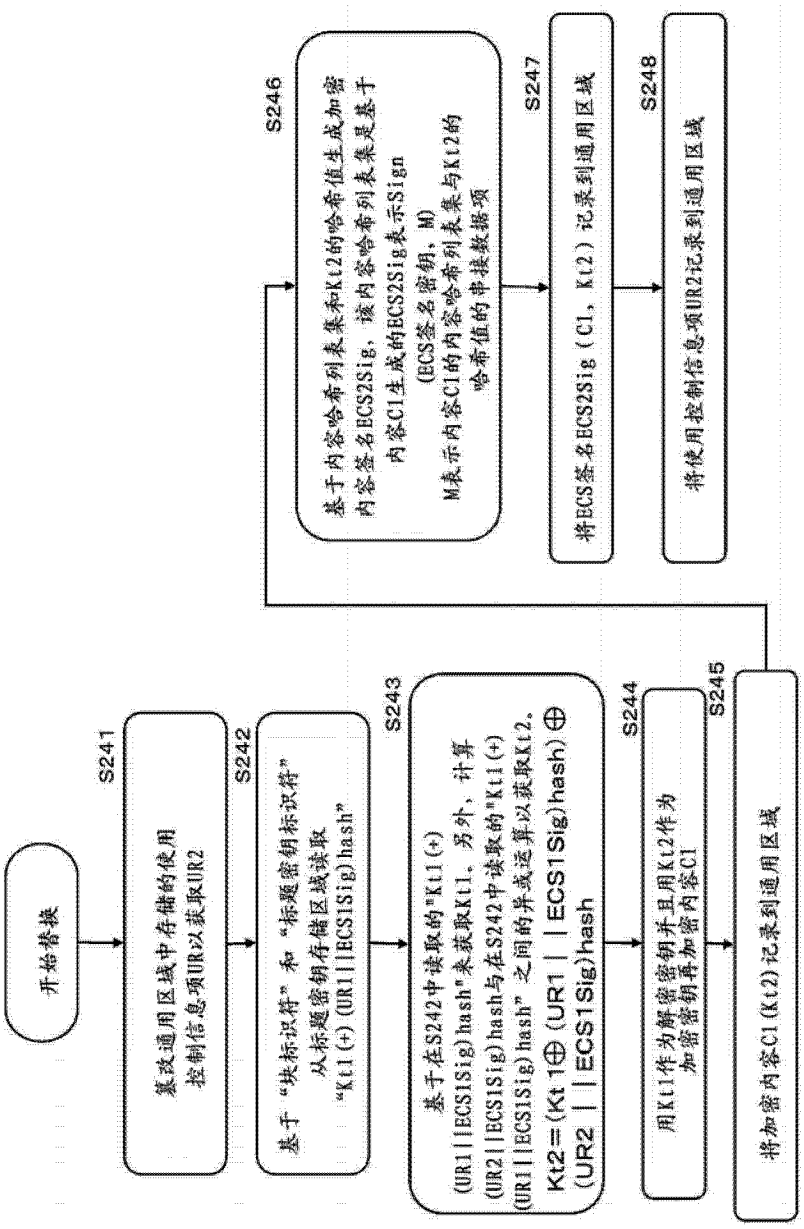

开始替换
S241
基改通用区域中存储的使用
控制信息项UR以获取UR2
S242
基于“块标识符”和“标题密钥标识符”
从标题密钥存储区域读取
“Kt1(+)(UR1||ECS1Sig)hash”
S243
基于在S242中读取的"Kt1(+)
(UR1||ECS1Sig)hash"来获取Kt1。另外，计算
(UR2||ECS1Sig)hash与在S242中读取的"Kt1(+)
(UR1||ECS1Sig)hash”之间的异或运算以获取Kt2。
Kt2=(Kt 1⊕(UR1||ECS1Sig)hash)⊕
(UR2||ECS1Sig)hash
S244
用Kt1作为解密密钥并且用Kt2作为
加密密钥再加密内容C1
S245
将加密内容C1(Kt2)记录到通用区域
S246
基于内容哈希列表集和Kt2的哈希值生成加密
内容签名ECS2Sig，该内容哈希列表集是基于
内容C1生成的ECS2Sig表示Sign
(ECS签名密钥，M)
M表示内容C1的内容哈希列表集与Kt2的
哈希值的串接数据项
S247
将ECS签名ECS2Sig(C1，Kt2)记录到通用区域
S248
将使用控制信息项UR2记录到通用区域

图 28

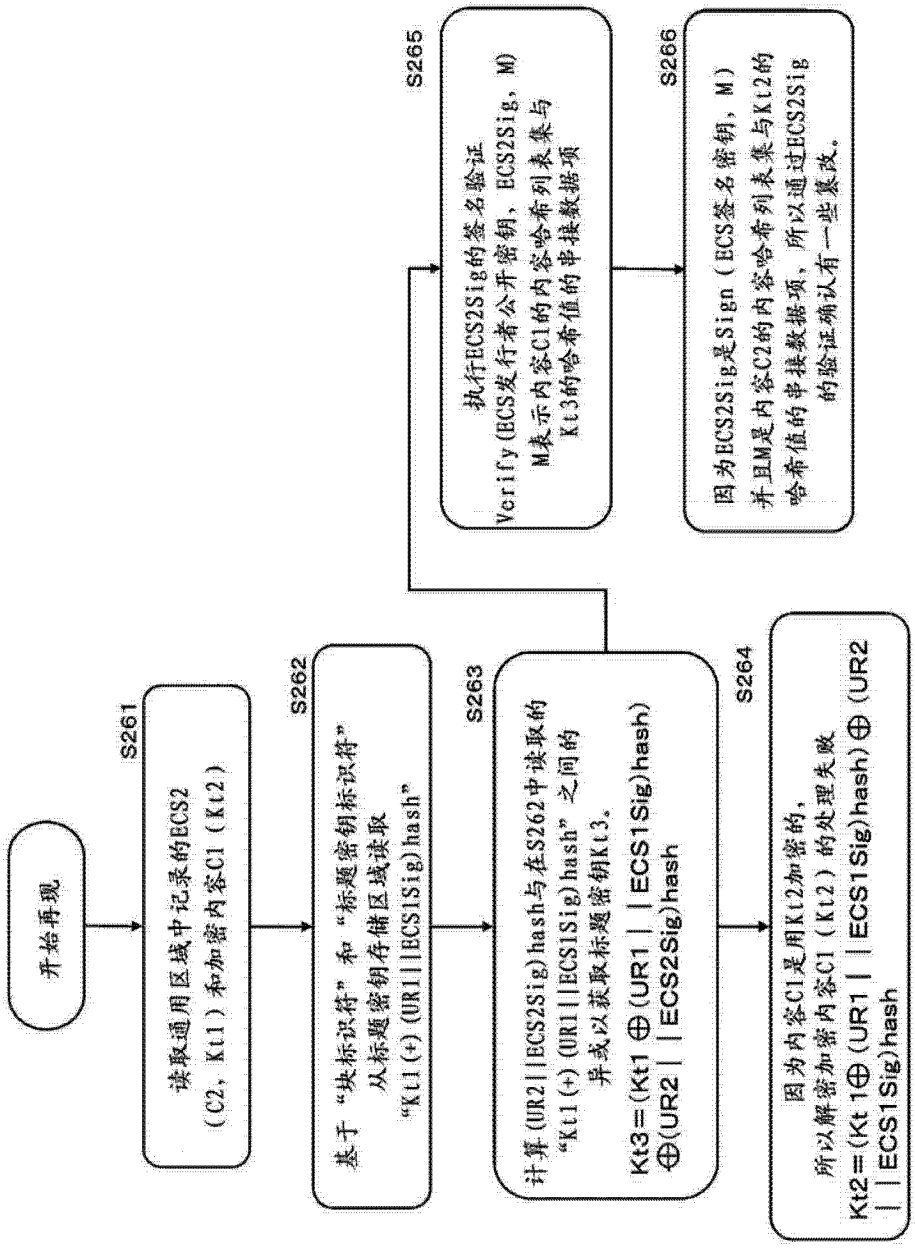

开始再现
S261
读取通用区域中记录的ECS2
（C2，Kt1）和加密内容C1（Kt2）
S262
基于“块标识符”和“标题密钥标识符”
从标题密钥存储区域读取
“Kt1(+)(UR1||ECS1Sig)hash”
S263
计算(UR2||ECS2Sig)hash与在S262中读取的
“Kt1(+)(UR1||ECS1Sig)hash”之间的
异或以获取标题密钥Kt3。
Kt3=(Kt1⊕(UR1||ECS1Sig)hash)
⊕(UR2||ECS2Sig)hash
S264
因为内容C1是用Kt2加密的，
所以解密加密内容C1（Kt2）的处理失败
Kt2=(Kt 1⊕(UR1||ECS1Sig)hash)⊕(UR2
||ECS1Sig)hash
S265
执行ECS2Sig的签名验证
Verify(ECS发行者公开密钥，ECS2Sig，M)
M表示内容C1的内容哈希列表集与
Kt3的哈希值的串接数据项
S266
因为ECS2Sig是Sign（ECS签名密钥，M）
并且M是内容C2的内容哈希列表集与Kt2的
哈希值的串接数据项，所以通过ECS2Sig
的验证确认有一些篡改。

图 29

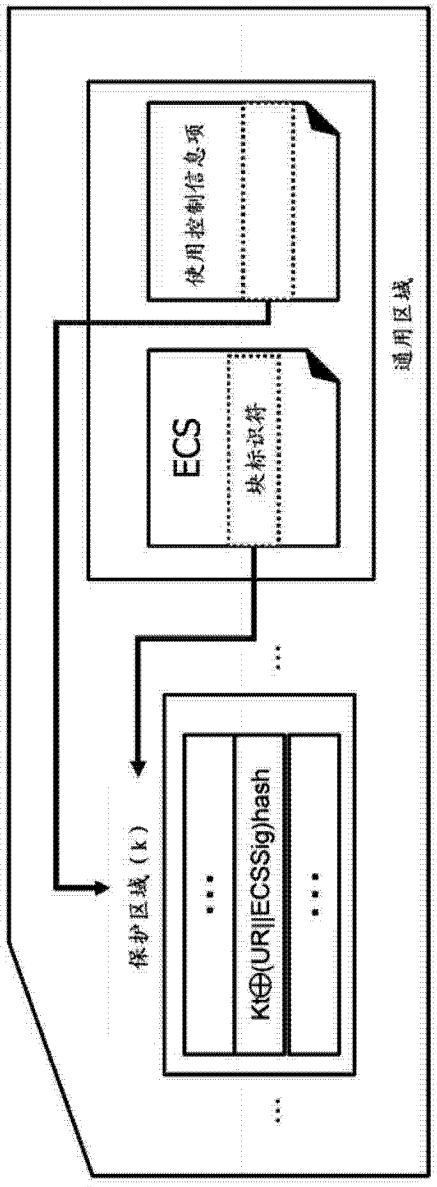



图 30

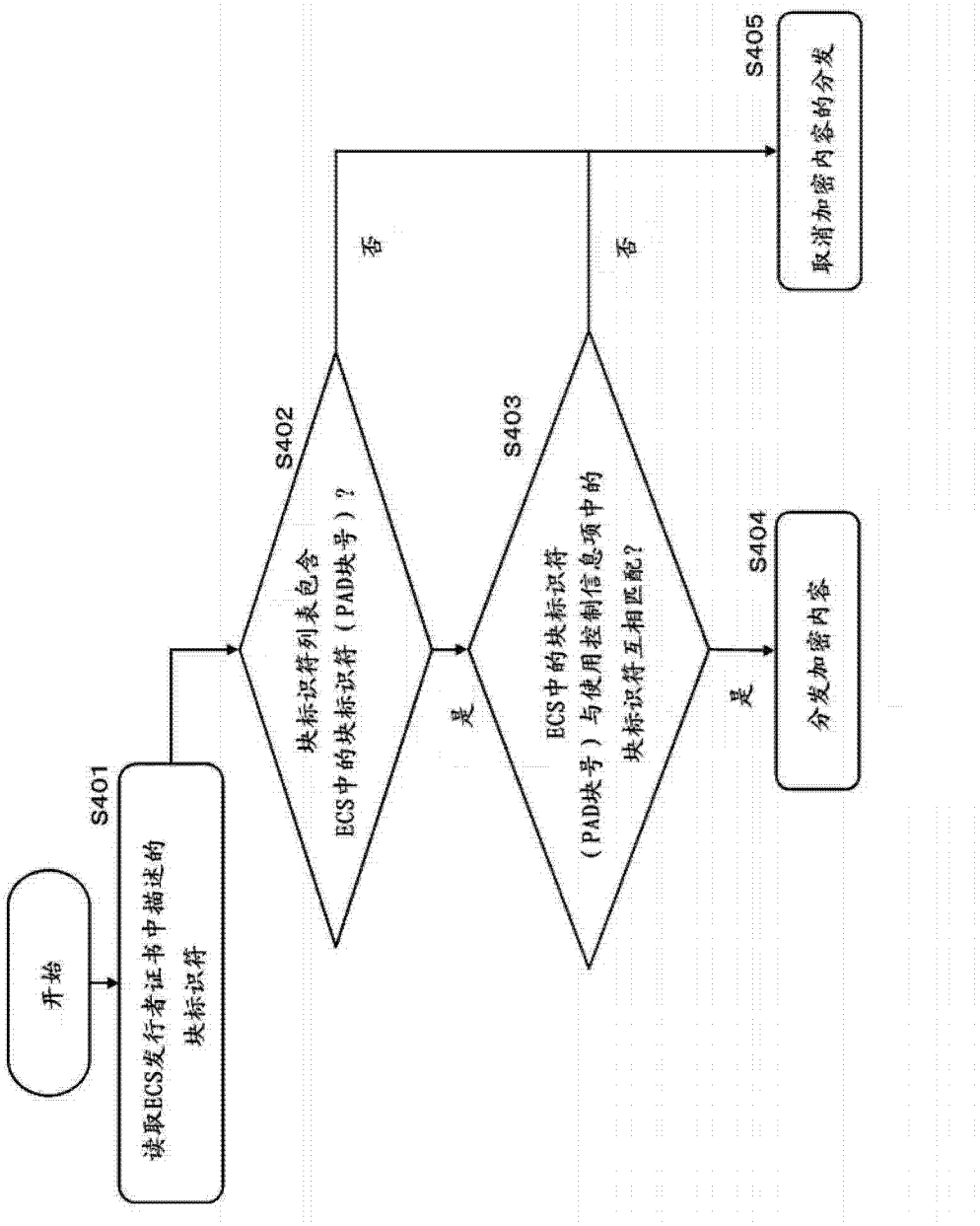

开始
S401
读取ECS发行者证书中描述的块标识符
S402
块标识符列表包含ECS中的块标识符（PAD块号）？
否
S405
取消加密内容的分发
是
S403
ECS中的块标识符（PAD块号）与使用控制信息项中的块标识符互相匹配？
否
是
S404
分发加密内容

图 31

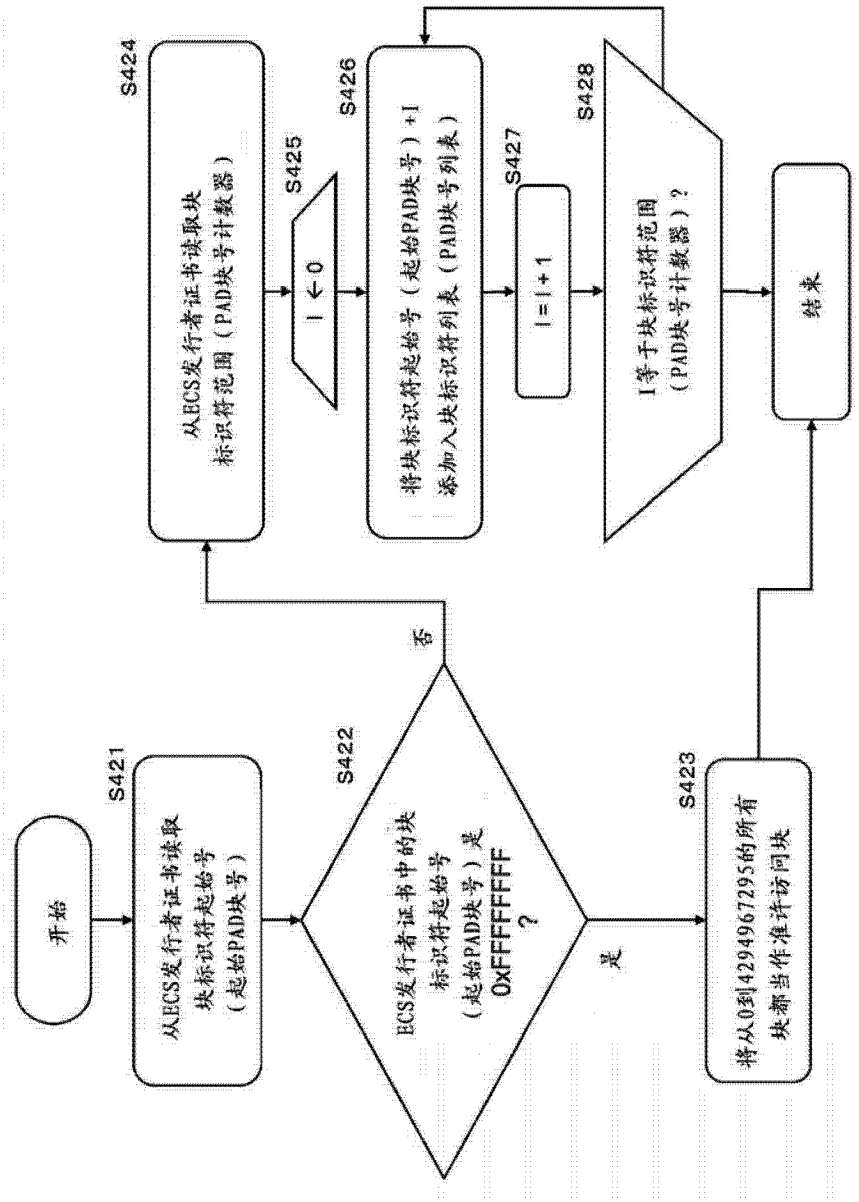

开始
S421
从ECS发行者证书读取块标识符起始号（起始PAD块号）
S422
ECS发行者证书中的块标识符起始号（起始PAD块号）是0xFFFFFFFF？
否
是
S423
将从0到4294967295的所有块都当作准许访问块
S424
从ECS发行者证书读取块标识符范围（PAD块号计数器）
S425
I ← 0
S426
将块标识符起始号（起始PAD块号）+I添加入块标识符列表（PAD块号列表）
S427
I = I + 1
S428
I等于块标识符范围（PAD块号计数器）？
结束

图 32

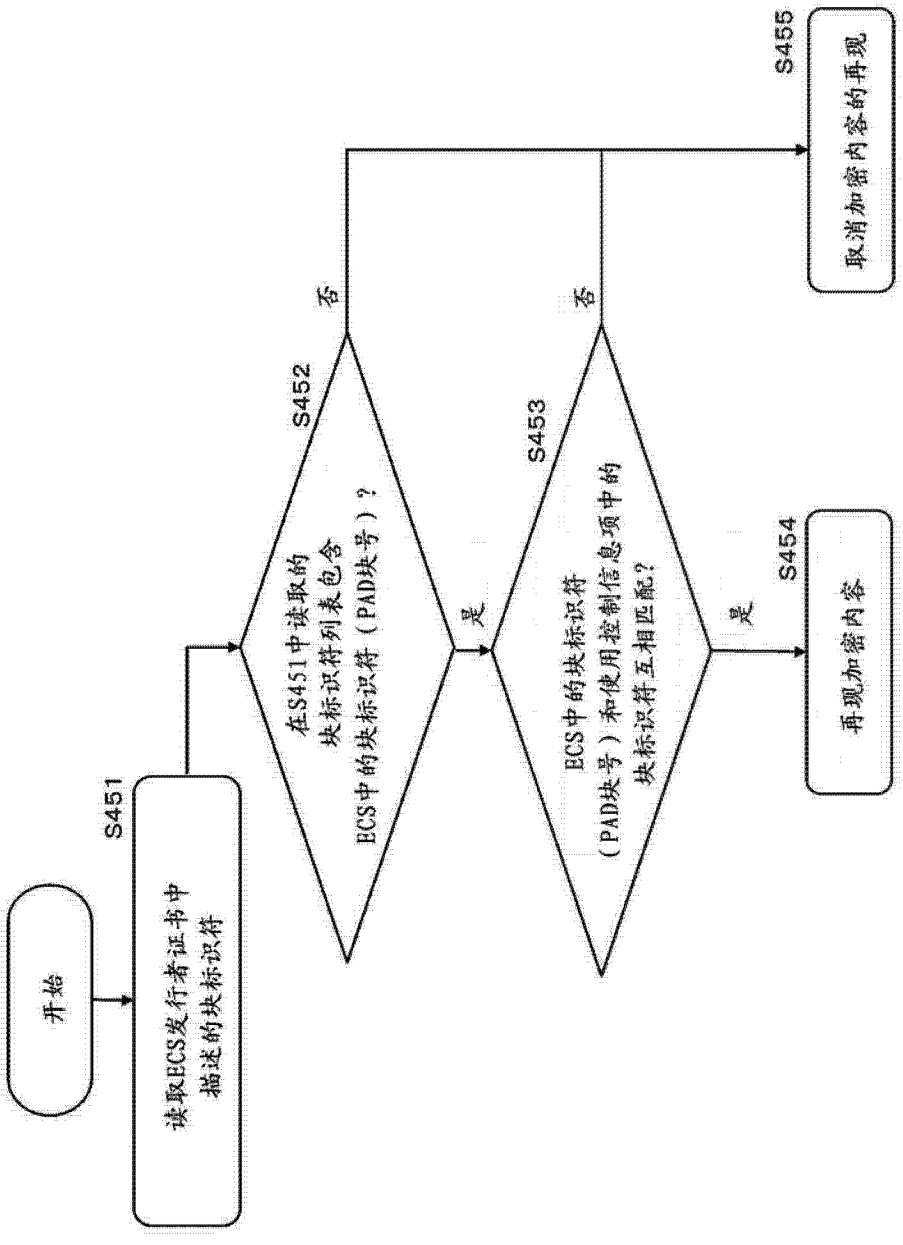

开始
S451
读取ECS发行者证书中
描述的块标识符
S452
在S451中读取的
块标识符列表包含
ECS中的块标识符（PAD块号）？
否
是
S453
ECS中的块标识符
（PAD块号）和使用控制信息项中的
块标识符互相匹配？
否
是
S454
再现加密内容
S455
取消加密内容的再现

图 33

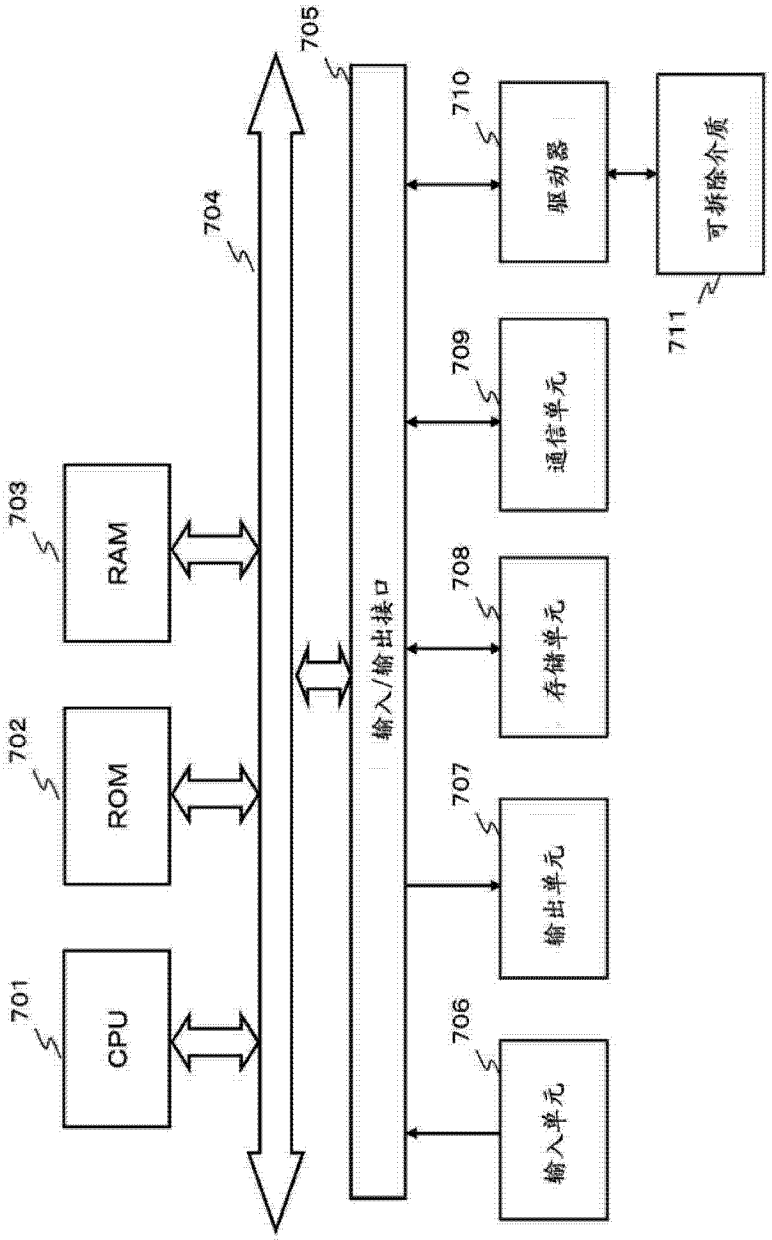

705
704
710
驱动器
可拆除介质
711
709
通信单元
703
RAM
708
存储单元
输入/输出接口
702
ROM
707
输出单元
701
CPU
706
输入单元

图 34

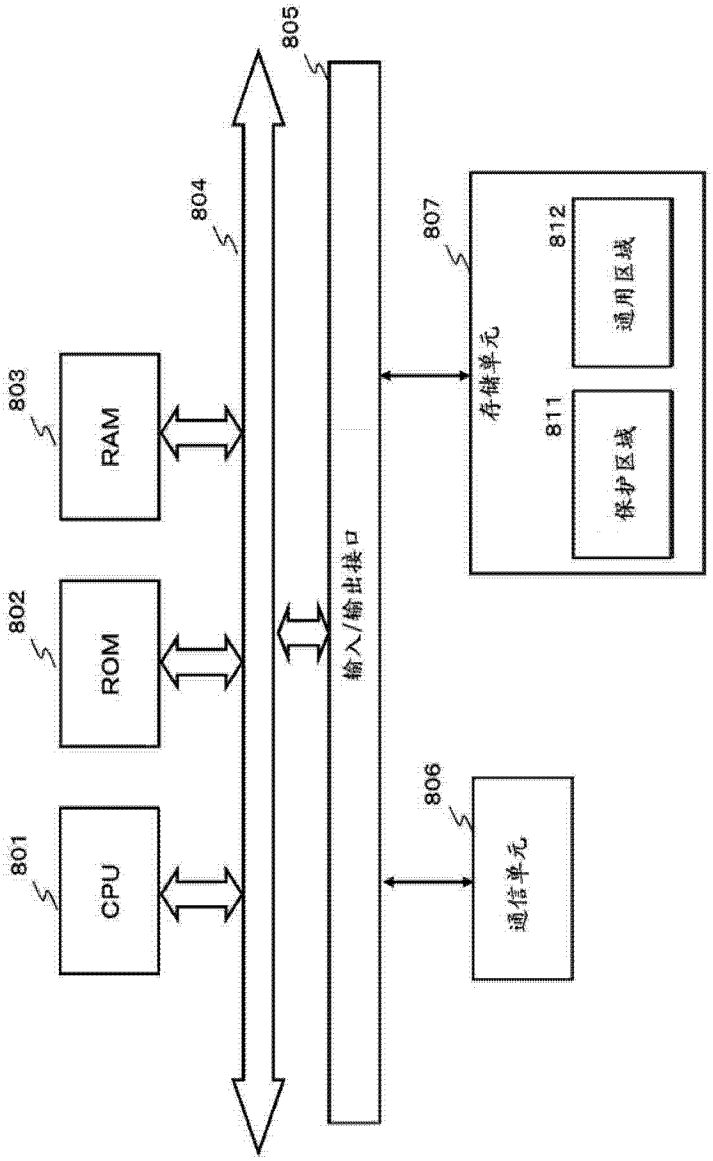

805
804
807
812
通用区域
存储单元
803
RAM
811
保护区域
802
ROM
输入/输出接口
806
801
CPU
通信单元

图 35