(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 103117073 A
(43)申请公布日 2013.05.22

(21)申请号 201210331383.1
(22)申请日 2012.09.07
(30)优先权数据
2011-202184 2011.09.15 JP
(71)申请人 索尼公司
地址 日本东京
(72)发明人 久野浩 林隆道 小林义行 村松克美
(74)专利代理机构 中国国际贸易促进委员会专利商标事务所 11038
代理人 王莉莉
(51)Int.Cl.
G11B 20/10(2006.01)
G06F 12/14(2006.01)
G06F 21/78(2013.01)

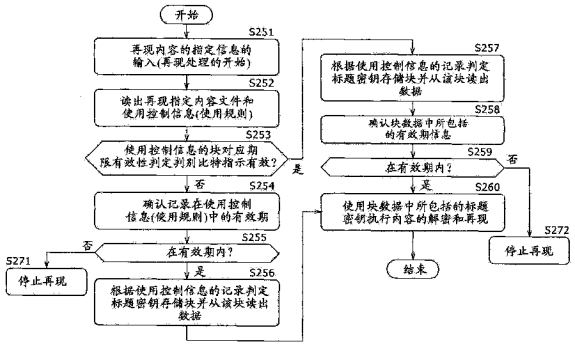
权利要求书4页 说明书35页 附图30页

(54)发明名称

信息处理设备、信息处理方法和程序

(57)摘要

本发明涉及信息处理设备、信息处理方法和程序。信息处理设备包括数据处理部分，构造为再现存储在介质中的内容；介质具有通用区域和保护区域，在通用区域中存储加密内容和与加密内容对应的使用控制信息，保护区域由多个块构成，对于多个块设置了访问限制，并且多个块包括存储用于解密加密内容的加密密钥的块；数据处理部分从通用区域获取与内容对应的使用控制信息；数据处理部分用于基于所获取的使用控制信息的记录数据来判定是从使用控制信息还是从存储加密密钥的块获取指示内容使用允许时间段的有效期信息，根据判定的结果从使用控制信息或块获取有效期信息，然后把所获取的有效期信息与当前日期信息进行比较以判定是否允许内容的再现。



CN 103117073 A

1. 一种信息处理设备，包括：

数据处理部分，构造为再现存储在介质中的内容；

所述介质具有

通用区域，在所述通用区域中存储加密内容和与加密内容对应的使用控制信息；和

保护区域，所述保护区域由多个块构成，对于所述多个块设置了访问限制，并且所述多个块包括存储用于解密所述加密内容的加密密钥的块；

所述数据处理部分从所述通用区域获取与内容对应的使用控制信息；

所述数据处理部分用于基于所获取的使用控制信息的记录数据来判定是从所述使用控制信息还是从存储加密密钥的块获取指示内容使用允许时间段的有效期信息，根据判定的结果从所述使用控制信息或块获取有效期信息，然后把所获取的有效期信息与当前日期信息进行比较以判定是否允许内容的再现。

2. 如权利要求 1 所述的信息处理设备，其中

所述使用控制信息的记录数据根据判别比特构造，基于该判别比特能够判定记录在存储所述加密密钥的块中的有效期信息的有效性；以及

所述数据处理部分响应于所述判别比特的值从块和所述使用控制信息中的一个获取所述有效期信息。

3. 如权利要求 1 所述的信息处理设备，其中记录在存储用于解密所述加密内容的加密密钥并设置了访问限制的块中的有效期信息被共同应用于与记录在该块中的多个加密密钥对应的多个内容。

4. 如权利要求 1 所述的信息处理设备，其中所述数据处理部分基于所述使用控制信息的记录数据指定存储用于解密所述加密内容的加密密钥的块，以及获取所指定的块的存储数据，然后获取所获取的数据中包含的有效期信息。

5. 如权利要求 1 所述的信息处理设备，其中所述数据处理部分执行这样的处理，即当从使用控制信息或块获取的有效期信息和当前日期信息之间进行比较处理时，应用从可靠的时间信息提供服务器获取的当前日期信息。

6. 如权利要求 1 所述的信息处理设备，其中

存储所述加密密钥的块是基于介质做出的访问权限判定而允许访问的块；以及

在块的数据读出处理时，所述数据处理部分把信息处理设备的证书发送给介质，并且在通过介质做出的访问权限判定而确认数据读出权限的条件下执行块的数据读出。

7. 如权利要求 1 所述的信息处理设备，其中

存储所述加密密钥的块是基于介质做出的访问权限判定而允许访问的块；以及

由具有对块的数据写入处理的权限的服务器写入和更新记录在块中的有效期信息。

8. 一种信息处理设备，包括：

数据处理部分，被构造为把内容记录到介质中；

所述介质具有：

通用区域，在所述通用区域中存储加密内容和与所述加密内容对应的使用控制信息，以及

保护区域，所述保护区域由多个块构成，对所述多个块设置了访问限制，所述多个块包括存储用于解密所述加密内容的加密密钥的块；

所述数据处理部分执行以下处理：

执行用于把加密内容和与所述加密内容对应的使用控制信息记录到所述通用区域的处理；

把用于解密记录在通用区域中的加密内容的加密密钥记录到所述保护区域的块中；

执行用于记录或更新有效期信息的处理，所述有效期信息作为块的记录数据指示可共同应用于与记录在保护区域的块中的多个加密密钥对应的内容的内容的使用允许时间段。

9. 如权利要求 8 所述的信息处理设备，其中所述数据处理部分执行用于把数据记录到介质的通用区域的使用控制信息中的处理，利用该数据能够判定是从使用控制信息还是从存储加密密钥的块获取指示内容使用允许时间段的有效期信息。

10. 如权利要求 8 所述的信息处理设备，其中

存储加密密钥的块是基于介质做出的访问权限判定而允许访问的块；以及

在对块的数据记录处理时，所述数据处理部分把信息处理设备的证书发送给介质，并且在通过介质的访问权限判定而确认所述信息处理设备具有数据记录处理的权限的条件下执行对块的数据记录处理。

11. 一种信息存储设备，包括：

数据存储部分；

所述数据存储部分包括：

通用区域，在所述通用区域中存储加密内容和与所述加密内容对应的使用控制信息，以及

保护区域，所述保护区域由多个块构成，对所述多个块设置了访问限制，所述多个块包括存储用于解密所述加密内容的加密密钥的块；

存储用于解密所述加密内容的加密密钥的块还具有有效期信息作为记录数据，所述有效期信息指示可共同应用于与记录在块中的多个加密密钥对应的内容的内容的使用允许时间段；

所述信息存储设备使得执行加密内容的再现处理的再现设备基于对记录在块中的有效期信息的参照处理来执行内容再现允许 / 禁止判定。

12. 如权利要求 11 所述的信息存储设备，其中

所述使用控制信息被构造为记录存储用于解密所述加密内容的加密密钥的块的识别信息；以及

所述信息存储设备使得执行所述加密内容的再现的再现设备基于对记录在使用控制信息中的块标识符的参照处理来执行块指定处理。

13. 如权利要求 11 所述的信息存储设备，还包括：

数据处理部分，所述数据处理部分被构造为获取对保护区域的块的访问请求设备的证书以及基于所获取的证书执行访问允许判定处理。

14. 一种信息处理系统，包括：

介质，被构造为在其中记录数据；

再现设备，被构造为再现存储在所述介质中的内容；以及

服务器，被构造为执行对所述介质的数据记录；

所述介质具有：

通用区域，在所述通用区域中存储加密内容和与所述加密内容对应的使用控制信息，以及

保护区域，所述保护区域被构造为多个块，对所述多个块设置了访问限制，所述多个块包括存储用于解密所述加密内容的加密密钥的块；

所述服务器用于执行以下处理：

执行用于把加密内容和与所述加密内容对应的使用控制信息记录到通用区域中的处理，

把用于解密记录在通用区域中的加密内容的加密密钥记录到保护区域的块中，以及

执行记录或更新有效期信息的处理，所述有效期信息作为块的数据指示可共同应用于与记录在保护区域的块中的多个加密密钥对应的内容的内容的使用允许时间段；

所述再现设备从通用区域获取与内容对应的使用控制信息；

所述再现设备用于基于所获取的使用控制信息的记录数据来判定是从使用控制信息还是从存储所述加密密钥的块获取指示内容使用允许时间段的有效期信息，根据判定的结果从使用控制信息或所述块获取有效期信息，然后基于所获取的有效期信息和当前日期信息之间的比较来判定允许或禁止内容再现。

15. 一种由信息处理设备执行的信息处理方法，所述信息处理设备执行内容再现处理并且包括数据处理部分，所述数据处理部分被构造为再现存储在介质中的内容，所述介质包括通用区域和保护区域，在所述通用区域中存储加密内容和与所述加密内容对应的使用控制信息，所述保护区域由多个块构成，对所述多个块设置了访问限制，所述多个块包括存储用于解密所述加密内容的加密密钥，所述信息处理方法由所述数据处理部分执行并且包括以下步骤：

从所述通用区域获取与内容对应的使用控制信息；以及

基于所获取的使用控制信息的记录数据来判定是从使用控制信息还是从存储所述加密密钥的块获取指示内容使用允许时间段的有效期信息，根据判定的结果从所述使用控制信息或块获取有效期信息，然后通过所获取的有效期信息和当前日期信息之间的比较来判定是否允许内容的再现。

16. 一种由信息处理设备执行的信息处理方法，所述信息处理设备执行对介质的内容记录处理，所述介质包括通用区域和保护区域，在所述通用区域中存储加密内容和与所述加密内容对应的使用控制信息，所述保护区域被构造成多个块，对所述多个块设置了访问限制，所述多个块包括存储用于解密所述加密内容的加密密钥的块，所述信息处理方法由所述信息处理设备执行并且包括以下步骤：

执行用于把加密内容和与所述加密内容对应的使用控制信息记录到通用区域的处理；

把用于解密记录在通用区域中的加密内容的加密密钥记录到保护区域的块中；以及

执行用于记录或更新有效期信息的处理，所述有效期信息作为块的记录数据指示可共同应用于与记录在保护区域的块中的多个加密密钥对应的内容的内容的使用允许时间段。

17. 一种用于使信息处理设备执行信息处理的程序，所述信息处理设备执行内容再现处理并且包括数据处理部分，所述数据处理部分被构造为再现存储在介质中的内容，所述介质包括通用区域和保护区域，在所述通用区域中存储加密内容和与所述加密内容对应的

使用控制信息，所述保护区域由多个块构成，对所述多个块设置了访问限制，所述多个块包括存储用于解密所述加密内容的加密密钥，所述程序使所述数据处理部分执行以下处理：

从所述通用区域获取与内容对应的使用控制信息的处理；以及

基于所获取的使用控制信息的记录数据来判定是从使用控制信息还是从存储所述加密密钥的块获取指示内容使用允许时间段的有效期信息，根据判定的结果从所述使用控制信息或块获取有效期信息，然后通过所获取的有效期信息和当前日期信息之间的比较来判定是否允许内容的再现的处理。

18. 一种用于使信息处理设备执行信息处理的程序，所述信息处理设备执行对介质的内容记录处理，所述介质包括通用区域和保护区域，在所述通用区域中存储加密内容和与所述加密内容对应的使用控制信息，所述保护区域被构造成多个块，对所述多个块设置了访问限制，所述多个块包括存储用于解密所述加密内容的加密密钥的块，所述程序使所述信息处理设备执行以下处理：

执行用于把加密内容和与所述加密内容对应的使用控制信息记录到通用区域的处理的处理；

把用于解密记录在通用区域中的加密内容的加密密钥记录到保护区域的块中的处理；以及

用于记录或更新有效期信息的处理，所述有效期信息作为块的记录数据指示可共同应用于与记录在保护区域的块中的多个加密密钥对应的内容的内容的使用允许时间段。

信息处理设备、信息处理方法和程序

技术领域

[0001] 本发明涉及一种信息处理设备、信息处理方法和程序，更具体地讲，涉及一种执行记录在记录介质（诸如例如，存储卡）中的内容的使用控制的信息处理设备、信息处理方法和程序。

背景技术

[0002] 近来，诸如DVD（数字通用盘）、蓝光盘（注册商标）和闪存的各种介质用作信息记录介质。特别地，近年来，包括具有大存储容量的闪存的存储卡被广泛地使用。用户能够把诸如音乐或电影的内容记录在这些各种信息记录介质中并把介质装入到再现设备或播放器中以执行内容的再现。

[0003] 然而，关于许多内容（诸如，音乐数据和图像数据），版权、发行权等由内容创造者或内容销售者拥有。因此，当内容被提供给用户时，通常应用诸如应用固定使用限制（也就是说，仅对具有合法使用权的用户授予使用内容的许可）的控制，从而无法执行非正常的使用，诸如未经允许的复制。

[0004] 例如，作为与内容的使用控制相关的标准，已知AACS（高级访问内容系统）。AACS标准定义用于例如记录在蓝光盘（注册商标）上的内容的使用控制结构。特别地，AACS标准规定加密内容用作例如记录在蓝光盘（注册商标）上的内容，并规定算法等以便可以使能够获取内容的加密密钥的用户仅仅限制于授权用户。该处理处理公开于例如日本专利提前公开No.2008-98765中。

[0005] 作为内容的使用控制结构，除了内容加密之外，存在使用与内容对应的使用控制信息（使用规则）的结构。

[0006] 例如，当内容被提供给用户时，另外提供与内容的允许使用形式相关的信息，诸如例如关于内容的使用时间段的信息或记录复制处理等的允许信息的使用控制信息（使用规则）。

[0007] 当在用户的再现设备上使用内容时，参照与内容对应的使用控制信息，从而在由使用控制信息（使用规则）规定的范围内执行内容的使用。

[0008] 然而，近年来，从服务器等的内容获取处理已变得普遍，在用户设备中使用的记录介质的记录容量已增加并且由用户设备保留的内容的数量已迅速增加。

[0009] 在保留这种大量内容的用户设备中，保留大量的成对的内容和与内容对应的使用控制信息。

[0010] 例如，在使用控制信息（使用规则）中，记录与使用控制信息关联的内容的使用允许时间段，即有效期信息。

[0011] 当用户想要延长内容的使用时间段时，需要重写与内容对应的使用控制信息（使用规则）的有效期的处理。这种重写处理不能由用户设备任意地执行，而是由内容管理服务器等执行。

[0012] 为了延长大量内容的有效期，需要逐条地重写许多条使用控制信息（使用规则）

的处理。这增加了用户设备和服务器之间的通信处理并增加了它们的处理负荷。

发明内容

[0013] 因此，希望提供一种可以高效地执行使用允许时间段的改变或使用管理对象的内容的更新处理以增强内容使用控制中的方便性的信息处理设备、信息处理方法和程序。

[0014] 根据本发明的实施例，提供了一种信息处理设备，包括数据处理部分，所述数据处理部分构造为再现存储在介质中的内容；所述介质具有通用区域和保护区域，在所述通用区域中存储加密内容和与加密内容对应的使用控制信息，所述保护区域由多个块构成，对于所述多个块设置了访问限制，并且所述多个块包括存储用于解密所述加密内容的加密密钥的块；所述数据处理部分从所述通用区域获取与内容对应的使用控制信息；所述数据处理部分用于基于所获取的使用控制信息的记录数据来判定是从所述使用控制信息还是从存储加密密钥的块获取指示内容使用允许时间段的有效期信息，根据判定的结果从所述使用控制信息或块获取有效期信息，然后把所获取的有效期信息与当前日期信息进行比较以判定是否允许内容的再现。

[0015] 所述信息处理设备可构造为，所述使用控制信息的记录数据根据判别比特构造，基于该判别比特能够判定记录在存储所述加密密钥的块中的有效期信息的有效性；以及所述数据处理部分响应于所述判别比特的值从块和所述使用控制信息中的一个获取所述有效期信息。

[0016] 记录在存储用于解密所述加密内容的加密密钥并设置了访问限制的块中的有效期信息被共同应用于与记录在该块中的多个加密密钥对应的多个内容。

[0017] 所述数据处理部分可以基于所述使用控制信息的记录数据指定存储用于解密所述加密内容的加密密钥的块，以及获取所指定的块的存储数据，然后获取所获取的数据中包含的有效期信息。

[0018] 所述数据处理部分可以执行这样的处理，即当从使用控制信息或块获取的有效期信息和当前日期信息之间进行比较处理时，应用从可靠的时间信息提供服务器获取的当前日期信息。

[0019] 所述信息处理设备可构造为，存储所述加密密钥的块是基于介质做出的访问权限判定而允许访问的块；以及在块的数据读出处理时，所述数据处理部分把信息处理设备的证书发送给介质，并且在通过介质做出的访问权限判定而确认数据读出权限的条件下执行块的数据读出。

[0020] 所述信息处理设备可构造为，存储所述加密密钥的块是基于介质做出的访问权限判定而允许访问的块；以及由具有对块的数据写入处理的权限的服务器写入和更新记录在块中的有效期信息。

[0021] 根据本发明的第二实施例，提供了一种信息处理设备，包括数据处理部分，所述数据处理部分被构造为把内容记录到介质中；所述介质具有通用区域以及保护区域，在所述通用区域中存储加密内容和与所述加密内容对应的使用控制信息，所述保护区域由多个块构成，对所述多个块设置了访问限制，所述多个块包括存储用于解密所述加密内容的加密密钥的块，所述数据处理部分执行以下处理：执行用于把加密内容和与所述加密内容对应的使用控制信息记录到所述通用区域的处理；把用于解密记录在通用区域中的加密内容的

加密密钥记录到所述保护区域的块中；执行用于记录或更新有效期信息的处理，所述有效期信息作为块的记录数据指示可共同应用于与记录在保护区域的块中的多个加密密钥对应的内容的内容的使用允许时间段。

[0022] 所述数据处理部分可以执行用于把数据记录到介质的通用区域的使用控制信息中的处理，利用该数据能够判定是从使用控制信息还是从存储加密密钥的块获取指示内容使用允许时间段的有效期信息。

[0023] 所述信息处理设备可构造为，存储加密密钥的块是基于介质做出的访问权限判定而允许访问的块；以及在对块的数据记录处理时，所述数据处理部分把信息处理设备的证书发送给介质，并且在通过介质的访问权限判定而确认所述信息处理设备具有数据记录处理的权限的条件下执行对块的数据记录处理。

[0024] 根据本发明的第三实施例，提供了一种信息存储设备，包括数据存储部分，所述数据存储部分包括通用区域和保护区域，，在所述通用区域中存储加密内容和与加密内容对应的使用控制信息，所述保护区域由多个块构成，对于所述多个块设置了访问限制，并且所述多个块包括存储用于解密所述加密内容的加密密钥的块；存储用于解密所述加密内容的加密密钥的块还具有有效期信息作为记录数据，所述有效期信息指示可共同应用于与记录在块中的多个加密密钥对应的内容的内容的使用允许时间段；所述信息存储设备使得执行加密内容的再现处理的再现设备基于对记录在块中的有效期信息的参照处理来执行内容再现允许 / 禁止判定。

[0025] 所述信息存储设备可构造为，所述使用控制信息被构造为记录存储用于解密所述加密内容的加密密钥的块的识别信息；以及所述信息存储设备使得执行所述加密内容的再现的再现设备基于对记录在使用控制信息中的块标识符的参照处理来执行块指定处理。

[0026] 所述信息存储设备还包括数据处理部分，所述数据处理部分被构造为获取对保护区域的块的访问请求设备的证书以及基于所获取的证书执行访问允许判定处理。

[0027] 根据本发明的第四实施例，提供了一种信息处理系统，包括：介质，被构造为在其中记录数据；再现设备，被构造为再现存储在所述介质中的内容；以及服务器，被构造为执行对所述介质的数据记录；所述介质具有通用区域以及保护区域，在所述通用区域中存储加密内容和与所述加密内容对应的使用控制信息，所述保护区域被构造为多个块，对所述多个块设置了访问限制，所述多个块包括存储用于解密所述加密内容的加密密钥的块；所述服务器用于执行以下处理，即执行用于把加密内容和与所述加密内容对应的使用控制信息记录到通用区域中的处理，把用于解密记录在通用区域中的加密内容的加密密钥记录到保护区域的块中，以及执行记录或更新有效期信息的处理，所述有效期信息作为块的数据指示可共同应用于与记录在保护区域的块中的多个加密密钥对应的内容的内容的使用允许时间段；所述再现设备从通用区域获取与内容对应的使用控制信息；所述再现设备用于基于所获取的使用控制信息的记录数据来判定是从使用控制信息还是从存储所述加密密钥的块获取指示内容使用允许时间段的有效期信息，根据判定的结果从使用控制信息或所述块获取有效期信息，然后基于所获取的有效期信息和当前日期信息之间的比较来判定允许或禁止内容再现。

[0028] 根据本发明的第五实施例，提供了一种由信息处理设备执行的信息处理方法，所述信息处理设备执行内容再现处理并且包括数据处理部分，所述数据处理部分被构造为再

现存储在介质中的内容，所述介质包括通用区域和保护区域，在所述通用区域中存储加密内容和与所述加密内容对应的使用控制信息，所述保护区域由多个块构成，对所述多个块设置了访问限制，所述多个块包括存储用于解密所述加密内容的加密密钥，所述信息处理方法由所述数据处理部分执行并且包括以下步骤：从所述通用区域获取与内容对应的使用控制信息；以及基于所获取的使用控制信息的记录数据来判定是从使用控制信息还是从存储所述加密密钥的块获取指示内容使用允许时间段的有效期信息，根据判定的结果从所述使用控制信息或块获取有效期信息，然后通过所获取的有效期信息和当前日期信息之间的比较来判定是否允许内容的再现。

[0029] 根据本发明的第六实施例，提供了一种由信息处理设备执行的信息处理方法，所述信息处理设备执行对介质的内容记录处理，所述介质包括通用区域和保护区域，在所述通用区域中存储加密内容和与所述加密内容对应的使用控制信息，所述保护区域被构造成多个块，对所述多个块设置了访问限制，所述多个块包括存储用于解密所述加密内容的加密密钥的块，所述信息处理方法由所述信息处理设备执行并且包括以下步骤：执行用于把加密内容和与所述加密内容对应的使用控制信息记录到通用区域的处理；把用于解密记录在通用区域中的加密内容的加密密钥记录到保护区域的块中；以及执行用于记录或更新有效期信息的处理，所述有效期信息作为块的记录数据指示可共同应用于与记录在保护区域的块中的多个加密密钥对应的内容的内容的使用允许时间段。

[0030] 根据本发明的第七实施例，提供了一种用于使信息处理设备执行信息处理的程序，所述信息处理设备执行内容再现处理并且包括数据处理部分，所述数据处理部分被构造为再现存储在介质中的内容，所述介质包括通用区域和保护区域，在所述通用区域中存储加密内容和与所述加密内容对应的使用控制信息，所述保护区域由多个块构成，对所述多个块设置了访问限制，所述多个块包括存储用于解密所述加密内容的加密密钥，所述程序使所述数据处理部分执行以下处理：从所述通用区域获取与内容对应的使用控制信息的处理；以及基于所获取的使用控制信息的记录数据来判定是从使用控制信息还是从存储所述加密密钥的块获取指示内容使用允许时间段的有效期信息，根据判定的结果从所述使用控制信息或块获取有效期信息，然后通过所获取的有效期信息和当前日期信息之间的比较来判定是否允许内容的再现的处理。

[0031] 根据本发明的第八实施例，提供了一种用于使信息处理设备执行信息处理的程序，所述信息处理设备执行对介质的内容记录处理，所述介质包括通用区域和保护区域，在所述通用区域中存储加密内容和与所述加密内容对应的使用控制信息，所述保护区域被构造成多个块，对所述多个块设置了访问限制，所述多个块包括存储用于解密所述加密内容的加密密钥的块，所述程序使所述信息处理设备执行以下处理：执行用于把加密内容和与所述加密内容对应的使用控制信息记录到通用区域的处理的处理；把用于解密记录在通用区域中的加密内容的加密密钥记录到保护区域的块中的处理；以及用于记录或更新有效期信息的处理，所述有效期信息作为块的记录数据指示可共同应用于与记录在保护区域的块中的多个加密密钥对应的内容的内容的使用允许时间段。

[0032] 应该注意的是，例如，通过以计算机可读形式提供给能够执行各种程序代码的信息处理设备或计算机系统的存储介质或通信介质，能够提供本发明的程序。通过以计算机可读形式提供这种程序，在信息处理设备或计算机系统上实现根据程序的处理。

[0033] 根据本发明的实施例的结构，提供了实现如下功能的设备和方法，其中与块对应的有效期信息被设置到存储于介质中的内容的加密密钥存储块，并且能够执行多个内容的集体有效期的设置和更新。

[0034] 具体地讲，再现存储在介质中的内容，该介质具有通用区域和保护区域，在通用区域中存储加密内容和使用控制信息，保护区域由多个块构成，对所述多个块设置了访问限制，所述多个块包括存储用于解密该加密内容的加密密钥的块。再现设备从通用区域获取与内容对应的使用控制信息。然后，再现设备基于使用控制信息的记录数据判定是从使用控制信息还是从存储加密密钥的块来获取指示内容使用允许时间段的有效期信息。然后，再现设备响应于判定的结果而从使用控制信息或块获取有效期信息，然后通过所获取的有效期信息与当前日期信息之间的比较来判定是允许还是禁止内容再现。判定

[0035] 通过该处理，实现了这样的设备和方法，它们能把块对应有效期信息设置到介质中存储的内容的加密密钥存储块中并且执行多个内容的集体有效期的设置和更新。

[0036] 通过下面结合附图进行的描述和所附权利要求，本发明的以上和其它特征和优点将会变得清楚，在附图中，相似的零件或元件由相似的标号表示。应该注意的是，在本说明书中，术语“系统”用于代表多个设备的逻辑集合结构，并且不限于组成设备容纳于同一壳体中的系统。

附图说明

[0037] 图 1 是表示内容提供处理和内容使用处理的概要的示意图；

[0038] 图 2 是表示记录在存储卡中的内容的使用形式的示意图；

[0039] 图 3 是表示存储卡的存储区域的具体结构的例子的示图；

[0040] 图 4 是表示主机证书的示图；

[0041] 图 5 是表示服务器证书的示图；

[0042] 图 6 是表示存储卡的存储区域的具体结构的例子和访问控制处理的例子的示意图；

[0043] 图 7 是表示存储卡的存储的数据的例子的示图；

[0044] 图 8 是表示服务器到存储卡的数据记录处理的例子的方框图；

[0045] 图 9 是类似的示图，但表示由主机记录来自存储卡的数据的读取处理的例子；

[0046] 图 10 是表示内容的有效期信息的更新处理序列的示图；

[0047] 图 11 是表示设置与块对应的有效期信息的内容的再现处理序列的流程图；

[0048] 图 12 是表示与块对应的有效期信息和使用控制信息的有效期信息的共存结构的示意图；

[0049] 图 13 是表示与块对应的有效期信息和使用控制信息的有效期信息的共存结构中由服务器执行的处理的例子的示意图；

[0050] 图 14 是表示与块对应的有效期信息和使用控制信息的有效期信息的共存结构中由主机执行的处理的例子的示意图；

[0051] 图 15 是表示与块对应的有效期信息和使用控制信息的有效期信息的共存结构中由主机执行的内容再现处理序列的流程图；

[0052] 图 16 和图 17 是表示与多个块对应的有效期信息被设置到一个块的结构的例子的

示意图；

[0053] 图 18 是表示在与多个块对应的有效期信息被设置到一个块的结构中由多个服务器使用一个块的例子的示意图；

[0054] 图 19 是表示在与多个块对应的有效期信息被设置到一个块的结构中由多个服务器使用一个块的情况下记录数据的例子的示图；

[0055] 图 20、图 21 和图 22 是表示记录关于内容等的首次再现日期和时间的状态信息并设置根据状态信息的内容使用期限的不同例子的示意图；

[0056] 图 23 是表示记录关于内容等的首次再现日期和时间的状态信息并设置根据状态信息的内容使用期限的例子中的服务器的处理的示意图；

[0057] 图 24 是表示记录关于内容等的首次再现日期和时间的状态信息并设置根据状态信息的内容使用期限的例子中的主机的处理的示意图；

[0058] 图 25 和图 26 是表示记录关于内容等的首次再现日期和时间的状态信息并设置根据状态信息的内容使用期限的例子中的主机的处理的流程图；

[0059] 图 27 和图 28 是表示不同介质之间的内容的移动处理的示意图；

[0060] 图 29 是显示具有再现设备的形式的主机的硬件结构的例子的方框图；和

[0061] 图 30 是显示存储卡的硬件结构的例子的方框图。

具体实施方式

[0062] 在下面，参照附图描述本发明的信息处理设备、信息处理方法和程序的细节。

[0063] 应该注意的是，根据下面各项进行描述。

[0064] 1. 内容提供处理和内容使用处理的概要

[0065] 2. 存储卡的结构的例子和使用的例子

[0066] 3. 具有对保护区域的访问允许信息的证书

[0067] 4. 对应用用于不同设备的证书的存储卡的访问处理的例子

[0068] 5. 以块为单位设置有效期信息的处理的例子

[0069] 6. 以块为单位的有效期信息和使用控制信息的有效期信息的共存使用处理的例子

[0070] 7. 把多个有效期的信息设置于一个块并响应于内容选择性地应用该信息的处理的例子

[0071] 8. 记录内容的首次使用信息的处理的例子

[0072] 9. 介质之间的内容的移动处理

[0073] 10. 设备的硬件结构的例子

[0074] 11. 本发明的结构的总结

[0075] 1. 内容提供处理和内容使用处理的概要

[0076] 在下面，参照附图描述本发明的信息处理设备、信息处理方法和程序的细节。

[0077] 首先，参照图 1 等描述内容提供处理和内容使用处理的概要。

[0078] 图 1 从左侧开始显示

[0079] (a) 内容提供源，

[0080] (b) 内容记录和再现设备（主机），和

[0081] (c) 内容记录介质。

[0082] (c) 内容记录介质是这样一种介质：用户在该介质上或介质中记录内容，并且该介质用于内容的再现处理。这里，内容记录介质指示存储卡 31，存储卡 31 是信息记录装置（诸如例如，闪存）。

[0083] 用户将会把各种内容（诸如，音乐和电影）记录在存储卡 31 上并使用它们。内容包括变为使用控制的对象的那些内容，诸如例如变为版权的管理的对象的那些内容。

[0084] 变为使用控制的对象的内容是例如禁止关于该内容的未受管理的复制、未受管理的复制数据散播等、关于该内容的使用的时间段受到限制以及其它类似内容。应该注意的是，当使用受控的内容被记录在存储卡 31 中时，与内容对应的使用控制信息（使用规则）被一起记录。

[0085] 在使用控制信息（使用规则）中，记录与内容使用相关的信息，诸如例如允许内容使用时间段和允许复制次数。

[0086] 内容提供源与内容一起提供和该内容对应的使用控制信息。

[0087] (a) 内容提供源是内容（诸如，音乐或电影）的提供源。在图 1 中，广播站 11 和内容服务器 12 显示为内容提供源的例子。

[0088] 广播站 11 是例如电视广播站，并在地面波或者经卫星的卫星波上把各种广播内容提供给用户设备，诸如“(b) 内容记录和再现设备（主机）”。

[0089] 内容服务器 12 是通过网络（诸如，互联网）提供内容（诸如，音乐或电影）的服务器。

[0090] 用户能够把例如作为 (c) 内容记录介质的存储卡 31 装入到 (b) 内容记录和再现设备（主机）中，并把从广播站 11 或内容服务器 12 提供的内容记录在存储卡 31 中。能够由 (b) 内容记录和再现设备（主机）自己的接收部分或由连接到 (b) 内容记录和再现设备（主机）的接收设备接收内容。

[0091] 把作为 (c) 内容记录介质的存储卡 31 装入到 (b) 内容记录和再现设备（主机）中，并且 (b) 内容记录和再现设备（主机）把从广播站 11 或内容服务器 12（广播站 11 或内容服务器 12 中的每一个是 (a) 内容提供源）接收的内容记录在存储卡 31 中。

[0092] 作为 (b) 内容记录和再现设备（主机），存在记录和再现设备 (CE 设备：消费电子设备）21，诸如例如 DVD 播放器，该记录和再现设备 21 包括诸如硬盘、DVD（数字通用盘）或 BD 的盘。另外，存在 PC（个人计算机）22 和便携式终端 23，诸如智能电话、便携式电话机、便携式播放器或平板式终端。所有这些是能够装入作为 (c) 内容记录介质的存储卡 31 的设备。

[0093] 用户将会使用记录和再现设备 21、PC 22、便携式终端 23 等从广播站 11 或内容服务器 12 接收内容（诸如，音乐或电影），并把接收的内容记录在存储卡 31 中。

[0094] 参照图 2 描述记录在存储卡 31 中的内容的使用方式。

[0095] 作为信息记录装置的存储卡 31 是能够以可移动的方式装入到内容再现设备（诸如例如，PC) 中的记录介质。能够自由地从已执行内容记录的设备取出存储卡 31，然后把存储卡 31 装入到另一用户设备中。

[0096] 具体地讲，如图 2 中所见，存储卡 31 执行诸如这些处理：

[0097] (1) 记录处理；和

[0098] (2) 再现处理。

[0099] 应该注意的是，可应用仅执行记录和再现之一的设备。

[0100] 另外，不必要求单个设备既执行记录处理又执行再现处理，而是用户可自由地选择性地使用记录设备和再现设备。

[0101] 应该注意的是，在多数情况下，记录在存储卡 31 中的使用受控的内容被记录为加密内容，并且内容再现设备（诸如，记录和再现设备 21、PC 22 或便携式终端 23 等）首先根据预定序列执行解密处理，然后执行内容的再现。

[0102] 另外，内容再现设备按照对应于内容设置的使用控制信息（使用规则）中所记录的允许使用方式执行再现处理等。

[0103] 在 (b) 内容记录和再现设备（主机）中，存储用于根据使用控制信息（使用规则）执行内容使用和内容解密处理的程序或主机应用。根据该程序或主机应用执行内容再现。

[0104] 2. 存储卡的结构的例子和使用的例子

[0105] 现在，描述用作内容的记录介质的存储卡（诸如，闪存）的结构的例子和使用的例子。

[0106] 存储卡 31 的存储区域的特定结构的例子表示在图 3 中。

[0107] 参照图 3，存储卡 31 的存储区域由包括 (a) 保护区域 51，和 (b) 通用区域 52 的两个区域构成。

[0108] 通用区域 52 是能够由用户使用的记录和再现设备自由地访问的区域，并且内容、与内容对应的使用控制信息（使用规则）、其它一般内容管理数据等被记录在通用区域 52 中。

[0109] 通用区域 52 是这样的区域：能够由服务器、用户的记录和再现设备等自由地把数据写在该区域中或者从该区域读出数据。

[0110] 同时，保护区域 51 是不允许对其自由访问的区域。

[0111] 保护区域 51 被分成块 #0、#1、#2、…作为多个分割区域，并且以块为单位设置访问权限。

[0112] 例如，如果试图通过由用户使用的记录和再现设备或者通过网络连接到记录和再现设备的服务器等执行数据的写入或读取，则存储卡 31 的数据处理部分根据预先存储在存储卡 31 中的程序响应于该设备以块为单位确定是允许还是禁止这种读取 (Read) 或写入 (Write)。

[0113] 存储卡 31 包括：数据处理部分，用于执行预先存储的程序；和认证处理部分，用于执行认证处理。存储卡 31 首先对试图执行把数据写在存储卡 31 中或从存储卡 31 读取数据的设备执行认证处理。

[0114] 在这种认证处理的阶段，存储卡 31 从相对设备（即，访问请求设备）接收设备证书，诸如公钥证书。

[0115] 例如，如果访问请求设备是服务器，则存储卡 31 接收由该服务器拥有的服务器证书，并且使用证书中描述的信息以保护区域 51 的块或分割区域为单位判定是否允许访问。

[0116] 另一方面，如果访问请求设备是主机设备（诸如，例如作为执行内容记录或再现的用户设备的记录和再现设备（主机）），则存储卡 31 接收由该记录和再现设备或主机设备拥有的主机证书。然后，存储卡 31 使用接收的证书中描述的信息判定是否允许访问保护区

域 51 的各个块或分割区域。

[0117] 以图 3 中表示的保护区域 51 中的块为单位（也就是说，对于各区域 #0、#1、#2、…）执行访问权限判定处理。存储卡 31 允许服务器或主机仅执行以块为单位允许的处理（诸如数据的读取 / 写的处理）。

[0118] 例如以试图访问介质的设备为单位（诸如例如，以内容服务器或记录和再现设备或主机设备为单位）设置介质的读取 / 写限制信息 (PADRead/PAD Write)。这种信息被记录在与各个设备对应的服务器证书或主机证书中。

[0119] 应该注意的是，“证书”可在附图中缩写为“cert”。

[0120] 以这种方式，根据预先存储在存储卡 31 中的规定程序，存储卡 31 执行这样的处理 :验证服务器证书或主机证书的记录的数据，并仅允许访问允许访问的区域。

[0121] 3. 具有对保护区域的访问允许信息的证书

[0122] 现在，参照图 4 和 5 描述当服务器或主机设备（该主机设备是记录和再现设备并且是用户设备）将要访问存储卡 31 的保护区域 51 时需要提供给存储卡 31 的证书的结构的例子。

[0123] 如上所述，存储卡 31 对试图执行把数据写在存储卡 31 中或从存储卡 31 读取数据的设备执行认证处理。在这种认证处理的阶段，存储卡 31 从相对设备（即，访问请求设备）接收设备证书，诸如公钥证书（诸如例如，服务器证书或主机证书）。然后，存储卡 31 使用所接收的证书中描述的信息判定是否允许访问保护区域 51 的各个分割区域。

[0124] 参照图 4 描述作为认证处理中使用的设备证书的例子的存储在用户设备或主机设备（诸如，图 1 中显示的记录和再现设备 21、PC 22 或便携式终端 23) 中的主机证书的结构的例子。

[0125] 由认证机构把主机证书提供给每个用户设备或主机设备，认证机构是公钥证书的颁发的主要单位。例如，主机证书是由认证机构颁发给其内容使用处理被允许的用户设备或主机设备的用户设备的证书，并且主机证书中包含了公钥等。在主机证书中，通过认证机构秘密密钥设置签名，并且签名构造为防止伪造的数据。

[0126] 应该注意的是，例如在设备的制造时基于设备的类型等的设备确认，设备证书能够预先存储在设备中的存储器中。如果用户在购买设备之后获取设备证书，则可以执行根据设备和认证机构或某一其它管理机构之间的预定序列的设备类型、可用内容的类型等的确认处理。然后，设备证书可以被颁发给每个设备并存储在设备中的存储器中。

[0127] 应该注意的是，用于执行对存储卡 31 的保护区域的访问的服务器保留服务器证书，在服务器证书中记录服务器公钥和对存储卡的访问允许信息，并且服务器证书具有与主机证书的结构类似的结构。

[0128] 图 4 表示由认证机构提供给每个主机设备或用户设备的主机证书的特定例子。

[0129] 如图 4 中所见，主机证书包括下面的数据 :

[0130] (1) 类型信息，

[0131] (2) 主机 ID 或用户设备 ID，

[0132] (3) 主机公钥，

[0133] (4) 保护区域访问权限信息（介质的保护区域的读取 / 写限制信息 (PAD Read/PAD Write))，

[0134] (5) 其它信息，和

[0135] (6) 签名。

[0136] 在下面，描述上述数据 (1) 至 (6)。

[0137] (1) 类型信息

[0138] 类型信息是代表证书的类型或用户设备的类型的信息。在类型信息中，记录这样的信息，诸如例如指示有关的证书是主机证书的数据和设备的类型（比如设备是 PC 或音乐再现播放器的信息）。

[0139] (2) 主机 ID

[0140] 主机 ID 是记录作为设备识别信息的设备 ID 的区域。

[0141] (3) 主机公钥

[0142] 主机公钥是主机设备的公钥。主机公钥与提供给主机设备或用户设备的秘密密钥一起构造根据公钥方法的密钥对。

[0143] (4) 保护区域访问权限信息（介质的保护区域的读取 / 写限制信息 (PAD Read/PAD Write)）

[0144] 在保护区域访问权限信息中，记录以记录内容的介质（诸如例如，图 3 中显示的存储卡 31）的存储区域中设置的保护区域 51 中的允许数据读取 (Read) 或写 (Write) 的块或分割区域为单位的信息。

[0145] 访问权限被记录为以保护区域中的块或分割区域为单位的访问权限。

[0146] (5) 其它信息和 (6) 签名

[0147] 在主机证书中，除了上述信息 (1) 至 (4) 之外，还记录各种信息，特别地，记录关于 (1) 至 (5) 的信息的签名数据。

[0148] 签名由认证机构的秘密密钥执行。当取出并使用记录在主机证书中的信息（例如，主机公钥）时，执行应用认证机构的公钥的签名验证处理以确认主机证书未经受任何伪造。以成功地进行这种确认为条件，执行证书存储数据（诸如，主机公钥）的使用。

[0149] 图 4 表示主机证书，在该主机证书中，记录对于存储卡的保护区域的用户设备或主机设备的访问允许信息。然而，对于需要访问保护区域的服务器（诸如例如，向存储卡提供内容的内容提供服务器），提供记录对于存储卡的保护区域的访问允许信息的证书，即服务器证书（诸如例如，存储服务器公钥的公钥证书），类似于图 4 中表示的主机证书。

[0150] 参照图 5 描述提供给服务器的服务器证书的结构的例子。应该注意的是，在下面的描述中，服务器包括图 1 中显示的所有内容提供源，或者换句话说，包括把内容提供给用户设备的任何设备，诸如广播站 11 和内容服务器 12。

[0151] 例如从认证机构把服务器证书提供给执行内容提供的设备（诸如，内容服务器），认证机构是颁发公钥证书的主要单位。例如，服务器证书是由认证机构颁发给允许其内容提供处理的服务器的服务器的证书，并且在该证书中，存储服务器公钥等。对于服务器证书，通过认证机构秘密密钥设置签名，并且签名构造为防止伪造的数据。

[0152] 图 5 表示从认证机构提供给每个内容服务器的服务器证书的特定例子。

[0153] 参照图 5，类似于上文参照图 4 描述的主机证书，服务器证书包括下面的数据：

[0154] (1) 类型信息，

[0155] (2) 服务器 ID，

[0156] (3) 服务器公钥，

[0157] (4) 介质的读取 / 写限制信息 (PAD Read/PAD Write)，

[0158] (5) 其它信息，和

[0159] (6) 签名。

[0160] 上述各种信息是与上文参照图 4 描述的信息类似的信息，因此，本文省略对它们的重复的详细描述以避免冗余。

[0161] 应该注意的是，在“(4) 介质的读取 / 写限制信息 (PAD Read/PAD Write)”中，以服务器为单位记录以存储卡 31 的保护区域 51 的块或分割区域为单位的访问权限，即数据读取 (Read)/ 写 (Write) 允许信息。

[0162] 应该注意的是，在将要取出并使用记录在服务器证书中的信息（例如，服务器公钥）的情况下，执行应用认证机构的公钥的签名验证处理以确认服务器证书未经受伪造。然后，以成功地进行这种确认为条件，执行证书存储数据（诸如，服务器公钥等）的使用。

[0163] 4. 应用用于不同设备的证书的存储卡的访问处理的例子

[0164] 如参照图 4 和 5 所述，为了使服务器或主机设备（该主机设备是用户设备，诸如记录和再现设备）访问存储卡 31 的保护区域 51 中的块，如上文参照图 4 或 5 所述的这种证书被提供给存储卡。

[0165] 存储卡 31 确认图 4 或 5 中表示的证书以判定是否允许以图 3 中表示的存储卡 31 的保护区域 51 的块为单位的访问。

[0166] 主机设备保留例如上文参照图 4 描述的主机证书，而执行内容的提供等的服务器保留上文参照图 5 描述的服务器证书。

[0167] 为了使这些设备中的每一个访问存储卡的保护区域，它把由此拥有的证书提供给存储卡，从而存储卡基于验证判定访问的允许 / 拒绝。

[0168] 参照图 6 描述当对于存储卡的访问请求设备是服务器时以及当访问请求设备是主机设备（诸如，记录和再现设备）时的访问限制的设置的例子。

[0169] 在图 6 中，从左侧开始依次显示作为对存储卡的访问请求设备的服务器 A 61、服务器 B 62、主机设备 63 以及存储卡 70。

[0170] 服务器 A 61 和服务器 B 62 提供例如加密内容 Con1、Con2、Con3、…，这些加密内容是存储卡 70 的记录内容。

[0171] 服务器 A 61 和服务器 B 62 提供标题密钥 Kt1、Kt2、Kt3、…（这些标题密钥是用于加密内容的解密的密钥）和与内容对应的使用控制信息（使用规则）UR1、UR2、…。

[0172] 主机设备 63 执行存储在存储卡 70 中的内容的再现处理。

[0173] 主机设备 63 读取记录在存储卡 70 的通用区域 90 中的加密内容 Con1、Con2、Con3、…和使用控制信息（使用规则）UR1、UR2、…。另外，主机设备 63 从保护区域 80 的块或分割区域 81 和 82 读取将要应用于内容解密处理的标题密钥 Kt1、Kt2、…，并通过标题密钥执行解密处理以根据使用控制信息（使用规则）执行内容使用。

[0174] 存储卡 70 具有保护区域 80 和通用区域 90，并且加密内容、使用控制信息（使用规则）等被记录在通用区域 90 中。

[0175] 在内容再现时需要的标题密钥被记录在保护区域 80 中。

[0176] 如上文参照图 3 所述，保护区域 80 被分割成多个块或分割区域。

[0177] 在图 6 中表示的例子中，仅显示两个块，包括块 #0（保护区域 #0）81 和另一块 #1（保护区域 #1）82。

[0178] 除了上述两个块之外，保护区域 80 还包括大量的块。

[0179] 作为块的设置模式，存在各种设置模式。

[0180] 在图 6 中表示的例子中，块 #0（保护区域 #0）81 是专用于服务器 A61 的块（也就是说，用于存储用于服务器 A 61 的提供内容的解密的标题密钥的区域），并且块 #1（保护区域 #1）82 是专用于服务器 B 62 的块（也就是说，用于存储用于服务器 B 62 的提供内容的解密的标题密钥的区域）。

[0181] 在如上所述的这种设置中，例如，内容提供服务器 A 61 把提供内容的解密所需的标题密钥记录在块 #0（保护区域 #0）81 中。

[0182] 在这种情况下，记录在服务器 A 61 的服务器证书中的写允许区域信息 (PAD Write) 构造为设置对块 #0（保护区域 #0）81 的写允许的证书。

[0183] 应该注意的是，图 6 中表示的例子代表这样的设置 :对于允许其写 (Write) 的块，也允许读取 (Read)。

[0184] 另外，服务器 B 62 把提供内容的解密所需的标题密钥记录在块 #1（保护区域 #1）82 中。

[0185] 在这种情况下，记录在服务器 B 62 的服务器证书中的写允许区域信息 (PAD Write) 构造为设置对块 #1（保护区域 #1）82 的写 (Write) 允许的证书。

[0186] 同时，由读取记录在块 #0 和 #1 中的标题密钥以执行内容再现的、作为再现设备的主机设备 63 保留的主机证书构造为设置块 #0 和 #1 的读取 (Read) 允许的证书。

[0187] 在本例子中，在主机证书中未设置块 #0 和 #1 的写 (Write) 允许。

[0188] 然而，为了使用在内容删除时能够删除与要删除的内容对应的标题密钥的设置，可使用允许删除处理的这种设置。

[0189] 另外，当在其它处理中主机设备 63 需要执行对保护区域的数据写入时，可设置对主机证书的写 (Write) 允许。

[0190] 当存储卡 70 的数据处理部分从访问请求设备（诸如，提供内容的服务器或者使用内容的主机）接收对保护区域 80 的访问请求时，它参照该设备的设备证书以确认以块为单位的访问允许信息从而判定是否允许对块的访问。

[0191] 存储卡 70 响应于从访问请求设备输入到它的数据写或读取请求判定写或读取请求数据的类型，并选择块 #0、#1、#2、…作为数据写或读取目标。

[0192] 访问控制信息被记录在每个访问请求设备的证书（诸如，服务器证书或主机证书）中，如上文参照图 4 和图 5 所述。因此，存储卡首先对从访问请求设备接收的证书执行签名验证。在确认证书的有效性之后，存储卡读取证书中描述的访问控制信息，即下面的信息 :

[0193] 读允许区域信息 (PAD Read)，和

[0194] 写允许区域信息 (PAD Write)。

[0195] 存储卡基于读取的信息仅允许对于访问请求设备允许的处理并执行该处理。

[0196] 由图 6 中表示的服务器 A 61 和服务器 B 62 写入到存储卡 70 中的数据的例子表示在图 7 中。

[0197] 每个服务器把内容和其它数据记录在装入到作为用户设备的主机设备中的存储卡 70 中。

[0198] 假设服务器 A 的提供内容是内容 Con(a1)、Con(a2) 和 Con(a3)。

[0199] 还假设服务器 B 的提供内容是内容 Con(b1) 和 Con(b2)。

[0200] 如图 7 中所见，服务器 A 把下面的数据：

[0201] 内容 Con(a1)、Con(a2) 和 Con(a3)

[0202] 与内容对应的使用控制信息（使用规则）UR(a1)、UR(a2) 和 UR(a3) 记录在存储卡的通用区域中。

[0203] 另外，服务器 A 把下面的数据：

[0204] 应用于内容的解密的标题密钥 Kt(a1)、Kt(a2)、Kt(a3) 或标题密钥的转换数据记录在存储卡的保护区域的块 #0 中。

[0205] 记录在存储卡的保护区域中的标题密钥的转换数据特别地是每个标题密钥和对应的使用控制信息（使用规则）的哈希 (hash) 值之间的异或 (XOR) 算术运算的结果。

[0206] 特别地，Kt(a1)-UR(a1)hash、Kt(a2)-UR(a2)hash 和 Kt(a3)-UR(a3)hash 是转换数据。

[0207] 服务器 B 把下面的数据：

[0208] 内容 Con(b1) 和 Con(b2)

[0209] 与内容对应的使用控制信息（使用规则）UR(b1) 和 UR(b2) 记录在存储卡的通用区域中。

[0210] 另外，服务器 B 把下面的数据：

[0211] 每个标题密钥和对应的使用控制信息（使用规则）的哈希值之间的异或 (XOR) 算术运算的结果 Kt(b1)-UR(b1)hash 和 Kt(b2)-UR(b2)hash 记录在存储卡的保护区域的块 #1 中。

[0212] 当每个服务器把数据记录在存储卡的保护区域中的块中时，存储卡基于上文描述的服务器证书的记录执行访问权限确认以执行对块的写权限的确认。然后，仅当确认访问权限时，执行数据写入。

[0213] 应该注意的是，当作为用户设备的主机设备使用内容时，按照下面的序列执行处理。

[0214] 首先，主机设备从存储卡的通用区域获取使用对象内容 Con(xy) 和对应的使用控制信息 UR(xy)。

[0215] 另外，主机设备从保护区域获取对应的标题密钥哈希值 Kt(xy)-UR(xy)hash。

[0216] 然后，主机设备计算使用控制信息 UR(xy) 的哈希值 UR(xy)hash。

[0217] 然后，主机设备执行计算的哈希值 UR(xy)hash 和从保护区域读出的标题密钥哈希值 Kt(xy)-UR(xy)hash 之间的异或 (XOR) 以获取标题密钥 Kt(xy)。

[0218] 最后，主机设备使用标题密钥 Kt(xy) 执行加密内容 Con(xy) 的解密处理以执行内容的再现和使用。

[0219] 按照如上所述的这种序列执行内容使用，诸如内容的再现。

[0220] 应该注意的是，在这个处理中，当主机设备从保护区域的块获取标题密钥哈希值 Kt(xy)-UR(xy)hash 时，也执行由存储卡基于主机证书进行的对块的访问权限（在这种情

况下，读取权限）的确认。仅当确认访问权限时，执行标题密钥哈希值 Kt(xy)-UR(xy)hash 的读取。

[0221] 5. 以块为单位设置有效期信息的处理的例子

[0222] 现在，描述不把作为提供给用户的内容的使用允许时间段的内容的有效期信息设置于与内容对应的使用控制信息（使用规则）而是把该有效期信息设置于存储标题密钥的块的处理的例子。

[0223] 通常，当向提供给用户的内容设置使用允许时间段时，使用允许时间段被记录在对应于每个内容颁发的使用控制信息（使用规则）中。

[0224] 将要执行内容再现的用户设备或主机设备执行如下所述的这种处理。具体地说，它在执行内容再现处理之前确认使用控制信息（使用规则）的记录。然后，如果使用允许时间段被记录在使用控制信息（使用规则）中，则判定当前日期是否对应于使用允许时间段。仅当当前日期和时间对应于使用允许时间段时，执行内容的使用。

[0225] 应该注意的是，用户设备或主机设备保留内容再现程序，内容再现程序是主机应用，包括参照使用控制信息（使用规则）判定内容的使用的允许 / 拒绝的处理。根据再现程序执行内容再现。

[0226] 然而，使用允许时间段被记录在对应于每个内容颁发的使用控制信息（使用规则）中的设置引起下面的问题。

[0227] 如上文所述，如果大量的内容被记录在作为用户的内容记录介质的存储卡中并且每个内容的使用允许时间段被设置于与每个内容对应的使用控制信息，则当执行使用时间段的延长或更新时，必须执行许多条使用控制信息的记录信息的重写。

[0228] 这种重写处理由服务器执行，并且这种处理需要服务器、主机和存储卡之间的通信。这对各设备施加了很大的处理负荷。

[0229] 作为用于减小如上所述的这种处理负荷的结构，参照图 8 等描述以存储标题密钥的保护区域的块为单位设置有效期信息的处理的例子。

[0230] 图 8 表示由服务器 A 61 执行的把内容提供给存储卡 70 以及把内容记录在存储卡 70 中的处理的例子。在这种内容提供处理时，设置作为提供内容的使用允许时间段的有效期信息，并且该有效期信息被记录在存储提供内容的标题密钥的保护区域的块中。

[0231] 具体地说，有效期信息与应用于来自服务器 A 61 的提供内容的解密的标题密钥一起被记录在存储该标题密钥的保护区域 80 的块 #0（保护区域 #0）81 中。

[0232] 在图 8 中表示的例子中，服务器 A 61 把以下给出的内容和使用控制信息记录在存储卡 70 的通用区域 90 中：

[0233] 内容 Con(a1)、Con(a2) 和 Con(a3)

[0234] 与内容对应的使用控制信息（使用规则）UR(a1)、UR(a2) 和 UR(a3)。

[0235] 记录内容使用控制信息的设置。

[0236] 另外，服务器 A 61 把下面的数据记录在存储卡 70 的保护区域 80 的块 #0（保护区域 #0）81 中：

[0237] 标题密钥和对应的使用控制信息的哈希值之间的异或 (XOR) 算术运算的结果 Kt(a1)-UR(a1)hash、Kt(a2)-UR(a2)hash 和 Kt(a3)-UR(a3)hash，

[0238] 作为服务器 A 的提供内容 Con(a1)、Con(a2) 和 Con(a3) 的使用允许时间段的有效

期信息，例如

[0239] 2011/01/12 至 2011/10/31。

[0240] 按照与标题密钥关联的关系来记录为所述多个内容设置的有效期信息。

[0241] 简而言之，服务器 A 设置与其提供内容对应的集体的有效期，并按照与同服务器 A 的提供内容对应的标题密钥关联的关系把有效期信息记录在存储标题密钥的块中。

[0242] 通过按照这种方式执行以存储多个标题密钥的块为单位的有效期信息的设置处理，例如，实现如下所述的优点。

[0243] 例如，当更新服务器 A 的提供内容的有效期时，服务器 A 仅需要重写记录在块中的有效期信息。具体地说，不需要执行逐个地重写与提供内容对应的使用控制信息（使用规则）的处理，能够减少服务器、主机和存储卡之间的通信处理，以及减少它们的处理负荷。

[0244] 应该注意的是，尽管图 8 表示例如服务器 A 61 的处理的例子，但服务器 B 62 能够把与服务器 B 的提供内容对应的集体的有效期记录在保护区域的块 #1 中，保护区域的块 #1 是与服务器 B 的提供内容对应的标题密钥的存储区域。

[0245] 应该注意的是，特别地，在采用例如服务器 A 的提供内容的使用允许时间段在预定时间间隔（例如，以一个月为单位）之后被连续更新的内容使用模式的情况下，以块为单位的有效期信息的设置结构很方便。

[0246] 例如，用户能够进行设置，从而通过每月支付会员费能够以一个月为单位自由地使用服务器 A 的提供内容。

[0247] 应该注意的是，如刚刚所述的这种内容使用服务称为例如订购服务。

[0248] 如果提供订购服务的服务器在每个更新月中重写记录在块中的有效期信息，则该服务器能够集体更新与记录在块中的标题密钥对应的内容的使用允许时间段。

[0249] 应该注意的是，尽管图 8 表示服务器 A 的提供内容的一个集体的有效期被记录在一个块中的设置例子，但也可采用替代的结构，其中设置服务器 A 的多个写允许块以使得对于不同的块设置不同的有效期。

[0250] 例如，可使用另一结构，其中服务器 A 的提供内容被分成多个分段并且使用的块以分段为单位改变，从而在不同的块之间设置不同的有效期。

[0251] 参照图 9 描述当以这种方式执行以存储卡的保护区域的块为单位的有效期设置时的内容的使用处理。

[0252] 图 9 显示作为使用内容的用户设备的主机设备 63 和存储内容等的存储卡 70。

[0253] 参照图 9，主机设备 63 在使用内容时执行下面的处理。

[0254] 另外，主机设备 63 从存储卡的通用区域获取使用对象内容 Con(xy) 和对应使用控制信息 UR(xy)。

[0255] 然后，主机设备 63 参照使用控制信息 UR(xy) 以确认在多个块的哪个块中存储使用对象内容 Con(xy) 的标题密钥。

[0256] 在使用控制信息 UR(xy) 中，记录存储使用对象内容 Con(xy) 的标题密钥的块的标识符。

[0257] 在指定块之后，执行块中的记录的数据的读出处理。

[0258] 首先，读出作为块内数据的有效期信息。把有效期和当前日期彼此比较，并且如果当前日期在有效期内，则获取记录在块中的标题密钥哈希值 Kt(xy)-UR(xy)hash。

[0259] 如果当前日期不在有效期内，则在这个时间点停止处理。换句话说，不执行内容的解密和使用处理。

[0260] 仅当当前日期在有效期内时，主机设备 63 获取记录在块中的标题密钥哈希值 Kt(xy)-UR(xy)hash。

[0261] 然后，主机设备 63 计算使用控制信息 UR(xy) 的哈希值 UR(xy)hash。然后，主机设备 63 执行计算的哈希值 UR(xy)hash 和从保护区域读取的标题密钥哈希值 Kt(xy)-UR(xy)hash 之间的异或 (XOR) 以获取标题密钥 Kt(xy)。

[0262] 最后，主机设备 63 使用标题密钥 Kt(xy) 执行加密内容 Con(xy) 的解密处理以执行内容的再现和使用。

[0263] 应该注意的是，优选地设置在记录为块内数据的有效期信息和当前日期信息之间的比较处理中使用的当前日期信息，以使用由可靠的时间信息提供服务器提供的时间信息。

[0264] 另外，当主机设备 63 从存储卡 70 的保护区域 80 的块获取标题密钥哈希值 Kt(xy)-UR(xy)hash 时，存储卡 70 基于主机证书执行对块的访问权限（在这种情况下，读取权限）的确认。仅当确认访问权限时，执行标题密钥哈希值 Kt(xy)-UR(xy)hash 的读取。

[0265] 现在，参照图 10 描述以存储标题密钥的块为单位设置有效期的更新处理序列。

[0266] 图 10 表示在提供并管理内容的内容服务器和存储以存储标题密钥的块为单位设置有效期的内容的存储卡之间执行的有效期的更新处理序列。

[0267] 应该注意的是，存储卡被装入到执行例如内容记录或再现的用户设备中，并且通过用户设备执行服务器和存储卡之间的通信。

[0268] 首先在步骤 S101，执行内容服务器和存储卡之间的认证处理。

[0269] 例如，执行包括内容服务器和存储卡的公钥证书的交换处理等的认证处理。

[0270] 应该注意的是，关于这个处理，服务器把上文参照图 5 描述的服务器证书提供给存储卡。

[0271] 如果认证处理的结果为失败，则停止处理。换句话说，不执行有效期的更新处理。

[0272] 如果认证处理的结果为成功并且判定两个设备都是可靠的，则存储卡在步骤 S102 基于服务器证书确认以保护区域中的块为单位的访问权限。仅当确认关于从服务器接收到更新请求的块的访问权限（也就是说，写权限）时，该处理前进至下面的处理。

[0273] 如果确认块访问权限，则服务器在步骤 S103 读出记录服务器提供内容的标题密钥和以块为单位的有效期信息的块的记录数据。

[0274] 在步骤 S104，更新读出的块数据中的有效期信息。

[0275] 例如，执行从更新前有效期信息 2011/09/01 至 2011/09/30 到更新后有效期信息 2011/10/01 至 2011/10/31 的有效期信息的重写处理。

[0276] 最后，在步骤 S105，执行把包括更新后的有效期信息的块记录数据写入或改写到存储卡的同一块中的处理。

[0277] 现在，参照图 11 中显示的流程图描述执行内容使用的用户设备或主机设备的内容再现处理序列。

[0278] 根据图 11 中表示的流程的处理由用户设备的数据处理部分（诸如，CPU）根据存储在用户设备中的内容再现程序或主机应用执行。

[0279] 首先，在步骤 S151，用户设备的数据处理部分检测到来自用户的再现内容指定信息的输入。例如，数据处理部分检测到内容指定信息的输入，该输入是用户关于作为显示在再现设备的显示部分上的菜单的内容列表的输入。

[0280] 然后，在步骤 S152，数据处理部分从装入在用户设备中的存储卡的通用区域读取再现指定内容和使用控制信息。特别地，获取使用对象内容 Con(xy) 和对应使用控制信息 UR(xy)。

[0281] 然后，在步骤 S153，数据处理部分参照所读取的使用控制信息 UR(xy) 确认使用对象内容 Con(xy) 的标题密钥存储在哪个块中。

[0282] 如果指定了块，则数据处理部分在步骤 S154 执行该块中的记录数据的读取处理以确认记录为块内数据的有效期信息。

[0283] 数据处理部分把这个有效期和当前日期彼此比较以判定当前日期是否在有效期内。

[0284] 如果在步骤 S155 判定当前日期不在有效期内，则处理前进至步骤 S157，在步骤 S157，停止处理。换句话说，不执行内容的解密和使用处理。

[0285] 另一方面，如果在步骤 S155 判定当前日期在有效期内，则处理前进至步骤 S156。

[0286] 在步骤 S156，数据处理部分获取记录在块中的标题密钥，并使用标题密钥执行内容的解密处理以执行内容的再现和使用。

[0287] 应该注意的是，存储在块中的标题密钥存储为标题密钥与使用控制信息 (UR：使用规则）的哈希值的异或算术运算的结果。因此，通过 UR 哈希的计算、与 UR 哈希的异或算术运算处理等，数据处理部分执行标题密钥的获取。

[0288] 以这种方式，当当前日期不在记录在块中的有效期内时，在这个时间点停止处理。应该注意的是，优选地进行这样的设置，即作为在记录为块内数据的有效期信息和当前日期信息之间的比较处理中使用的当前日期信息，使用由可靠的时间信息提供服务器提供的时间信息。

[0289] 以这种方式，在本实施例中，应用这样的结构，其中以存储与不同内容对应的多个标题密钥的块为单位设置内容的有效期信息。因此，可以减小多个内容的有效期的设置或更新处理中所涉及的通信处理或数据处理的负荷。

[0290] 6. 以块为单位的有效期信息和使用控制信息的有效期信息的共存使用处理的例子

[0291] 描述以块为单位的有效期信息和使用控制信息的有效期信息的共存使用处理的例子。

[0292] 在上述实施例中，描述了服务器设置与用于提供给用户的所有多个内容的一个块对应的一个有效期的例子。

[0293] 然而，有时希望设置与一个内容对应的独立有效期。

[0294] 类似于到目前为止的设备中一样，与一个内容对应的这种单个有效期可以被例如记录在关于内容的使用控制信息（使用规则）中。

[0295] 然而，如果应用这种设置，则涉及两种有效期，这两种有效期包括以块为单位的有效期信息和使用控制信息（使用规则）的有效期信息，并且不知道应该参照这两种有效期中的哪一个。

[0296] 在下面，描述解决如刚刚所述的这种问题的结构（也就是说，以块为单位的有效期信息和使用控制信息的有效期信息共存从而对于每个内容选择性地应用这两种有效期信息之一的结构）的例子。

[0297] 参照图 12 描述本处理的例子的概要。

[0298] 例如，从服务器提供的内容被记录在存储卡的通用区域中。

[0299] 与内容对应的使用控制信息（使用规则）也被从服务器提供给存储卡并被记录在存储卡的通用区域中。这个处理类似于以前的处理，并且类似的处理也由上文描述的记录以块为单位的有效期信息的结构执行。

[0300] 在上文描述的记录以块为单位的有效期信息的结构中，进行这样的设置，即内容的有效期信息未被记录在与内容对应的使用控制信息（使用规则）中。

[0301] 在本处理例子中，与内容对应的使用控制信息（使用规则）采用图 12 中表示的两种设置 (a) 和 (b) 之一。

[0302] 具体地，图 12 的 (a) 指示这样的设置，其中内容的有效期信息被记录在使用控制信息（使用规则）中并且指示无效的比特“0”被记录在块对应期限有效性判定判别比特（订购使能比特）中。

[0303] 图 12 的 (b) 指示这样的设置，其中内容的有效期信息未被记录在使用控制信息（使用规则）中而且指示有效的比特“1”被记录在块对应期限有效性判定判别比特（订购使能比特）中。

[0304] 当提供内容的服务器设置单独为内容设置的有效期作为提供内容的有效期时，产生根据上述设置 (a) 的使用控制信息（使用规则）。然后，使用控制信息（使用规则）与内容一起被提供给用户设备以便被记录在存储卡的通用区域中。

[0305] 另一方面，当服务器设置并非单独为内容设置而是针对块设置用于块中的多个内容的有效期作为提供内容的有效期时，产生根据上述设置 (b) 的使用控制信息（使用规则）。然后，使用控制信息（使用规则）与内容一起被提供给用户设备以便被记录在存储卡的通用区域中。

[0306] 服务器响应于内容选择并提供这两种设置之一的使用控制信息（使用规则）。

[0307] 执行内容的再现和使用的用户设备或主机设备在使用内容时参照与使用内容对应的使用控制信息（使用规则）以确认块对应期限有效性判定判别比特（订购使能比特）的设置。

[0308] 如果块对应期限有效性判定判别比特（订购使能比特）的设置是代表无效的比特“0”，则参照使用控制信息（使用规则）中的有效期信息。

[0309] 另一方面，如果块对应期限有效性判定判别比特（订购使能比特）的设置是代表有效的比特“1”，则参照记录在存储与内容对应的标题密钥的保护区域的块中的有效期信息。

[0310] 通过如刚刚所述的这种处理，可以允许记录在使用控制信息中的单独用于内容的有效期和对于多个内容共同设置的与块对应的有效期的共存，从而能够响应于内容没有错误地选择性地多个应用有效期之一。

[0311] 现在，参照图 13 描述由服务器 A 61 执行的把新内容记录到存储卡 70 的记录处理序列。

[0312] 图 13 表示内容提供处理的两个例子，包括：

[0313] 使用与块对应的有效期的内容 a1 的提供处理，和

[0314] 单个内容的有效期被记录在使用控制信息中的内容 a2 的提供处理。

[0315] 首先，描述使用与块对应的有效期的内容 a1 的提供处理。

[0316] 当服务器 A 61 将要把设置了对于其它提供内容而言共同的与块对应的有效期的内容记录在存储卡 70 中时，与内容对应的使用控制信息（使用规则）的块对应期限有效性判定判别比特（订购使能比特）被设置为指示有效的比特“1”。

[0317] 具有这种设置的使用控制信息（使用规则）与内容一起被记录在存储卡的通用区域中。

[0318] 与这个内容对应的标题密钥被记录在允许服务器 A 61 进行写入的保护区域中的块中。

[0319] 在图 13 中表示的例子中，块 #081 是允许服务器 A 61 进行写入的块，并且标题密钥被写入到这个块中。应该注意的是，特别地，记录标题密钥的转换数据，标题密钥的转换数据是标题密钥与使用控制信息（使用规则）的哈希值的异或算术运算的结果。

[0320] 在这个块 #081 中，与服务器 A 的其它提供内容对应的有效期被一起记录。对于内容 a1，使用记录在该块中的有效期。

[0321] 用户设备或主机设备在内容的再现时确认记录在与内容 a1 对应的使用控制信息（使用规则）中的块对应期限有效性判定判别比特（订购使能比特）的设置。然后，用户设备或主机设备基于确认的设置参照记录在块中的有效期以执行有效期确认。

[0322] 现在，描述单个内容的有效期被记录在使用控制信息中的内容 a2 的提供处理。

[0323] 当服务器 A 61 将要把设置了单独用于内容的有效期的内容记录在存储卡 70 中时，作为提供内容的使用允许时间段的有效期信息被记录在使用控制信息（使用规则）中。

[0324] 另外，产生这样的使用控制信息（使用规则），其中使用控制信息（使用规则）的块对应期限有效性判定判别比特（订购使能比特）的设置被设置为指示无效的比特“0”。然后，产生的使用控制信息（使用规则）与内容一起被记录在存储卡的通用区域中。

[0325] 与这个内容对应的标题密钥被记录在允许服务器 A 61 进行写入的保护区域中的块中。

[0326] 在图 13 中表示的例子中，块 #081 是允许服务器 A 61 进行写入的块，并且标题密钥被写入到这个块中。应该注意的是，特别地，记录标题密钥的转换数据，标题密钥的转换数据是标题密钥与使用控制信息（使用规则）的哈希值的异或算术运算的结果。

[0327] 应该注意的是，在这个块 #081 中，与服务器 A 的其它提供内容对应的块的有效期被一起记录。然而，对于内容 a2，不使用与块对应的有效期，而是使用记录在与内容 a2 对应的使用控制信息（使用规则）中的有效期。

[0328] 具体地，用户设备或主机设备在内容的再现时确认记录在与内容 a2 对应的使用控制信息（使用规则）中的块对应期限有效性判定判别比特（订购使能比特）的设置。然后，用户设备或主机设备基于确认的设置参照记录在使用控制信息（使用规则）中的有效期以执行有效期确认。

[0329] 现在，参照图 14 描述内容的使用处理的例子。

[0330] 图 14 显示作为用户设备并使用内容的主机设备 63 和存储内容等的存储卡 70。

[0331] 主机设备 63 在使用内容时执行下面的处理。

[0332] 首先，主机设备 63 从存储卡的通用区域获取使用对象内容 Con(xy) 和对应的使用控制信息 UR(xy)。

[0333] 然后，主机设备 63 确认使用控制信息 UR(xy) 的块对应期限有效性判定判别比特（订购使能比特）的设置。

[0334] 如果该比特设置是代表无效的比特“0”，则主机设备 63 参照使用控制信息（使用规则）中的有效期信息。

[0335] 然而，如果该比特设置是代表有效的比特“1”，则主机设备 63 参照记录在存储与内容对应的标题密钥的保护区域的块中的块对应有效期信息。

[0336] 通过如上所述的这种处理，可以允许记录在使用控制信息中的单独用于内容的有效期和对于多个内容共同设置的块对应有效期的共存，并且响应于内容没有错误地选择性地应用多个有效期之一。

[0337] 参照图 15 中显示的流程图描述执行内容的使用的用户设备或主机设备的内容再现处理序列。

[0338] 根据图 15 中表示的流程的处理由用户设备的数据处理部分（诸如，CPU）根据存储在用户设备中的内容再现程序或主机应用执行。

[0339] 首先，在步骤 S251，数据处理部分检测到来自用户的再现内容指定信息的输入。例如，数据处理部分检测到内容指定信息的输入，该输入是例如用户对于作为显示在再现设备的显示部分上的菜单的内容列表的输入。

[0340] 然后，在步骤 S252，数据处理部分从装入在用户设备中的存储卡的通用区域读取再现指定内容和使用控制信息。特别地，数据处理部分获取使用对象内容 Con(xy) 和对应的使用控制信息 UR(xy)。

[0341] 然后，在步骤 S253，数据处理部分参照读取的使用控制信息 UR(xy) 确认使用控制信息 UR(xy) 的块对应期限有效性判定判别比特（订购使能比特）的设置。

[0342] 如果该比特设置是代表无效的比特“0”，则处理前进至步骤 S254。然而，如果该比特设置是代表有效的比特“1”，则处理前进至步骤 S257。

[0343] 如果该比特设置是代表无效的比特“0”并且处理前进至步骤 S254，则在步骤 S254，数据处理部分参照使用控制信息（使用规则）中的有效期信息。

[0344] 然后，在步骤 S255，数据处理部分判定当前日期是否在有效期内。如果数据处理部分判定当前日期不在有效期内，则处理前进至步骤 S271，在步骤 S271，停止处理。换句话说，不执行内容的解密和使用处理。

[0345] 另一方面，如果在步骤 S255 判定当前日期在有效期内，则处理前进至步骤 S256。

[0346] 在步骤 S256，数据处理部分辨别存储记录在使用控制信息（使用规则）中的标题密钥的块并从该块读取数据。

[0347] 最后，在步骤 S260，数据处理部分获取存储在从该块读取的数据中的标题密钥，并使用标题密钥执行内容的解密处理以执行内容的再现和使用。

[0348] 另一方面，如果在步骤 S253 判定使用控制信息 UR(xy) 的块对应期限有效性判定判别比特（订购使能比特）的设置是代表有效的比特“1”，则处理前进至步骤 S257。在步骤 S257，数据处理部分辨别存储记录在使用控制信息（使用规则）中的标题密钥的块并从

该块读取数据。

[0349] 然后，在步骤 S258，数据处理部分执行该块中的记录数据的读出处理并确认记录为块内数据的有效期信息。

[0350] 然后，数据处理部分把块对应有效期和当前日期彼此比较以判定当前日期是否在有效期内。

[0351] 如果在步骤 S259 判定当前日期不在有效期内，则处理前进至步骤 S272，在步骤 S272，停止处理。换句话说，不执行内容的解密和使用处理。

[0352] 另一方面，如果在步骤 S259 判定当前日期在有效期内，则处理前进至步骤 S260。

[0353] 在步骤 S260，数据处理部获取记录在该块中的标题密钥，并使用标题密钥执行内容的解密处理以执行内容的再现和使用。

[0354] 应该注意的是，在块中存储的标题密钥被存储为与使用控制信息（使用规则）的哈希值的异或 (XOR) 算术运算的结果，并且执行通过上文描述的 UR 哈希的计算、与 UR 哈希的 XOR 算术运算处理等实现标题密钥的获取。

[0355] 以这种方式，当当前日期不在记录在块中的有效期内时，在这个时间点停止处理。应该注意的是，如上文所述，优选地设置在记录为块内数据的有效期信息和当前日期信息之间的比较处理中使用的当前日期信息，以使用由可靠的时间信息提供服务器提供的时间信息。

[0356] 以这种方式，在本实施例中，允许两种有效期信息的共存，所述两种有效期信息包括记录在使用控制信息中的有效期信息和记录在块中的有效期信息。另外，关于应该使用两种有效期信息中的哪一种的辨别信息被记录在内容对应使用控制信息（使用规则）中。

[0357] 通过这些设置，服务器能够为单个内容设置有效期并且还能够使与多个内容对应的块对应有效期与将要使用的内容关联。

[0358] 另外，作为内容使用设备的用户设备能够响应于内容没有错误地选择性地应用这两种类型的有效期之一。

[0359] 7. 把多个有效期的信息设置于块并响应于内容选择性地应用该信息的处理的例子

[0360] 现在，描述把多个有效期的信息设置于块并响应于内容选择性地应用该信息的处理的例子。

[0361] 在上述实施例中，仅一个与块对应的有效期被设置于存储卡的保护区域中的一个块。

[0362] 在下面，描述另一结构例子，其中多个有效期的信息被记录在存储卡的保护区域的一个块中，从而响应于内容参照并使用从所述多个有效期选择的一个有效期。

[0363] 参照图 16 描述本实施例。

[0364] 图 16 表示记录内容的存储卡 70 的通用区域 90 中的记录数据和存储卡 70 的保护区域 80 的一个块 #081 的记录数据的例子。

[0365] 在通用区域 90 中，记录下面的数据：

[0366] 内容 a1 ；和

[0367] 与内容 a1 对应的使用控制信息（使用规则）a1。

[0368] 应该注意的是，在通用区域 90 中，另外记录大量的数据集，包括内容和内容的使

用控制信息。

[0369] 同时，在由提供内容 a1 的服务器 A 专用的保护区域 80 的一个块 #081 中，与服务器 A 的提供内容对应的标题密钥被记录在标题密钥存储区域中。

[0370] 特别地，记录如图 16 中所示的这种数据

[0371] Kt(a1)-UR(a1)hash

[0372] Kt(a2)-UR(a2)hash

[0373] .

[0374] .

[0375] Kt(an)-UR(an)hash。

[0376] 应该注意的是，如上文所述，每个标题密钥存储为与使用控制信息（使用规则）的哈希值的 XOR 算术运算的结果。

[0377] 在由服务器 A 专用的保护区域 80 的一个块 #081 中，除了上述标题密钥之外，还设置记录多个有效期数据的有效期信息存储区域。

[0378] 特别地，在有效期信息存储区域中记录诸如下面的数据

[0379] After#Af1,After#Af2,After#Af3,…

[0380] Before#Bf1,Before#Bf2,Before#Bf3,…

[0381] 数据 After#Af1,After#Af2,After#Af3，…特别地是诸如下面的数据

[0382] After#Af1= 在 2011/09/01 之后

[0383] After#Af2= 在 2011/10/01 之后

[0384] After#Af3= 在 2011/11/01 之后。

[0385] 数据 After#Afn(n=1,2,3，…）代表在设置的日期及之后允许内容的使用。

[0386] 以这种方式，多个不同的有效期开始日期的信息被记录为数据 After#Af1,After#Af2,After#Af3,…。

[0387] 同时，数据 Before#Bf1,Before#Bf2,Before#Bf3,…具体地是诸如下面的数据

[0388] Before#Bf1= 在 2011/09/30 之前。

[0389] Before#Bf2= 在 2011/10/31 之前

[0390] Before#Bf3= 在 2011/11/30 之前

[0391] 数据 Before#Bfn 代表在设置的日期及之前允许内容的使用。

[0392] 以这种方式，多个不同的有效期结束日期的信息被记录为数据 Before#Bf1,Before#Bf2,Before#Bf3,…。

[0393] 图 16 的 (a) 表示与记录在通用区域 90 中的内容 a1 对应的使用控制信息（使用规则）a1 的特定例子。

[0394] 在使用控制信息（使用规则）中，记录诸如块标识符、标题密钥标识符、块对应期限有效性判定判别比特和有效期信息标识符的数据。

[0395] 块标识符是代表与使用控制信息（使用规则）UR(a1) 对应的内容 Con(a1) 的标题密钥 Kt(a1) 的存储块。

[0396] 在本例子中，块标识符是 #0，并且执行内容再现的用户设备或主机设备能够选择块 #0。

[0397] 标题密钥标识符是代表存储在块 #0 中的大量标题密钥中的哪一个标题密钥用于

与使用控制信息（使用规则）UR(a1) 对应的内容 Con(a1) 的信息。

[0398] 在本例子中，标题密钥标识符是 a1，因此，能够选择标题密钥 Kt(a1)。

[0399] 块对应期限有效性判定判别比特是在上文结合前一实施例描述的信息。

[0400] 如果块对应期限有效性判定判别比特（订购使能比特）的设置是指示无效的比特“0”，则参照使用控制信息（使用规则）中的有效期信息。

[0401] 另一方面，如果块对应期限有效性判定判别比特（订购使能比特）的设置是指示有效的比特“1”，则参照记录在存储与内容对应的标题密钥的保护区域的块中的有效期信息。

[0402] 在块对应期限有效性判定判别比特（订购使能比特）的设置是指示有效的比特“1”（或者，换句话说，记录在块中的有效期信息有效）的情况下，记录有效期信息标识符。

[0403] 这个有效期信息标识符代表将要使用记录在块的有效期信息存储区域中的大量有效期中的哪一个有效期。

[0404] 在图 16 中表示的例子中，有效期信息标识符指示该有效期信息标识符的设置 =Af3,Bf3。实际上，记录数据诸如 After#Af3= 在 2011/11/01 之后和 Before#Bf3= 在 2011/11/30 之前。

[0405] 因此，使用控制信息（使用规则）UR(a1) 的对应内容 Con(a1) 的有效使用时间段是 2011/11/01 至 2011/11/30。

[0406] 以这种方式，执行内容再现的用户设备或主机设备能够基于记录在使用控制信息（使用规则）中的有效期信息标识符从设置于块的大量有效期之中选择性地使用与内容对应的有效期。

[0407] 根据本例子，当与大量内容对应的标题密钥被记录在一个块中时，可以记录内容或标题密钥的单独的有效期。

[0408] 应该注意的是，也在这种设置中，通过执行重写记录在块中的有效期信息的处理能够执行有效期的更新处理，而不需要单独的使用控制信息的重写。

[0409] 应该注意的是，根据上述结构，也能够使用这种设置 :替代于把一个块设置给一个内容提供构成部分（诸如例如，仅一个服务器），一个块由多个不同的内容提供服务器共同地使用。

[0410] 特别地，一个块的标题密钥存储区域被分割以设置用于服务器 A 的标题密钥存储区域和用于服务器 B 的另一标题密钥存储区域，如图 17 中所见。

[0411] 每个内容提供服务器由此把与提供的内容对应的标题密钥存储在对应的标题密钥存储区域中。

[0412] 同时，有效期信息存储区域由服务器 A 和 B 共同地使用。

[0413] 当每个服务器提供内容时，它把上文参照图 16 的 (a) 描述的各种信息（也就是说，块标识符、标题密钥标识符、块对应期限有效性判定判别比特和有效期信息标识符）记录在存储卡的通用区域中的使用控制信息（使用规则）中。

[0414] 通过使用如上所述的这种设置，可以允许一个块由多个服务器共同地使用以便以服务器为单位以及以内容为单位自由地设置有效期。

[0415] 设置例子中的服务器的访问权限设置的例子显示在图 18 中，其中存储卡的一个块以这种方式用作多个服务器的标题密钥写区域。

[0416] 图 18 显示四个服务器，包括服务器 A 61、另一服务器 B 62、又一服务器 C 64 和再一服务器 D 65。

[0417] 服务器 A 61 和服务器 B 62 具有对存储卡的保护区域 80 的块 #081 的访问权限（读 / 写）。

[0418] 服务器 C 64 和服务器 D 65 具有对存储卡的保护区域 80 的不同的块 #182 的访问权限（读 / 写）。

[0419] 在如刚刚所述的这种情况下，记录由每个服务器拥有的服务器证书，从而如图 18 中所见，由服务器 A 61 和服务器 B 62 拥有的服务器证书中记录了对块 #081 的访问权限（读 / 写）允许信息，并且由服务器 C 64 和服务器 D 65 拥有的服务器证书中记录了对块 #182 的访问权限（读 / 写）允许信息。

[0420] 在如上所述的这种设置中记录在存储卡中的数据的例子表示在图 19 中。

[0421] 如图 19 中所见，由服务器 A 至 D 提供的内容和使用控制信息（使用规则）被记录在存储卡的通用区域中。

[0422] 同时，在存储卡的保护区域中，块 #0 中存储与服务器 A 和服务器 B 的提供内容对应的标题密钥，并且块 #1 中存储与服务器 C 和服务器 D 的提供内容对应的标题密钥。

[0423] 应该注意的是，每个标题密钥存储为例如该标题密钥与使用控制信息（使用规则）的哈希值的 XOR 算术运算的结果。

[0424] 如上文所述，利用本发明的结构，可以为与记录在保护区域的一个块中的多个标题密钥对应的多个内容单独地设置有效期。还可以实现这种设置，其中一个块用作能够由多个服务器使用的共享块。

[0425] 8. 记录内容的首次使用信息的处理的例子

[0426] 虽然可以设置绝对期限信息，像是如上所述的这种有效期“2011/10/01 至 2011/10/31”，但也可以应用这种形式，即从作为开始点的用户的首次使用的时间点开始的预定时间段（诸如，从用户对内容的首次使用的日期开始的一个月）被设置为使用允许时间段。

[0427] 在设置如上所述的这种使用允许时间段的情况下，使用允许时间段根据用户的首次使用的时间而不同，因此，不能执行从服务器提供内容的日期开始的时间段设置。另外，服务器不能固定地设置使用期限。

[0428] 在下面，描述可以如上所述设置这种取决于用户处理的内容使用期限的处理的例子。

[0429] 参照图 20 描述用于实现刚刚描述的处理的存储卡的保护区域中的记录数据的设置的例子。

[0430] 图 20 表示在存储卡 70 的保护区域 80 中设置的两个块中（也就是说，块 #0 和块 #1 中）的记录数据的例子。

[0431] 块 #0 是用于记录与上文结合前一实施例参照图 16 描述的块 #0 中的数据类似的数据的区域。

[0432] 特别地，块 #0 是记录标题密钥和有效期信息的区域，如图 20 的 (b1) 中所示。这个块称为标题密钥存储块。

[0433] 在本实施例中，除了标题密钥存储块之外，还使用保护区域 80 中的不同的块。

[0434] 该不同的块是图 20 中表示的块 #1 和图 20 的 (b2) 中表示的状态存储块。

[0435] 在这个状态存储块中，记录与记录在存储卡的通用区域中的内容 Con(a1)，Con(a2)，…对应的首次再现日期和时间信息。

[0436] 例如，在图 20 的 (b2) 中，Con(a1) 的状态表示内容 Con(a1) 的首次再现日期和时间信息的记录区域，并且 Con(a2) 的状态表示内容 Con(a2) 的首次再现日期和时间信息的记录区域。

[0437] 应该注意的是，内容的首次再现日期和时间信息由执行内容再现的用户设备或主机设备记录。

[0438] 用户设备或主机设备保留记录对块 #1 的写允许信息的主机证书。

[0439] 当用户设备或主机设备首次再现内容（例如，内容 Con(a1)）时，设备把首次再现日期和时间信息记录在图 20 的 (b2) 中表示的“Con(a1) 的状态”区域中。

[0440] 参照图 21 和图 22 描述本实施例中的使用控制信息（使用规则）的结构的例子。

[0441] 图 21 表示记录内容的存储卡 70 的通用区域 90 中的记录数据和作为保护区域 80 的标题密钥存储块的块 #081 中的记录数据的例子。

[0442] 图 22 表示作为保护区域 80 的状态存储块的块 #182 中的记录数据的例子。

[0443] 在图 21 中表示的通用区域 90 中，记录下面的数据：

[0444] 内容 a1；和

[0445] 与内容 a1 对应的使用控制信息（使用规则）a1。

[0446] 应该注意的是，在通用区域 90 中，记录大量的内容及其使用控制信息的数据集。

[0447] 另一方面，在由提供内容 a1 的服务器 A 专用的作为保护区域 80 的标题密钥存储块的块 #081 的标题密钥存储区域中，记录与服务器 A 的提供内容对应的标题密钥，如图 21 的 (b1) 中所见。

[0448] 特别地，记录如图 16 中所示的这种数据

[0449] Kt(a1)-UR(a1)hash

[0450] Kt(a2)-UR(a2)hash

[0451] .

[0452] .

[0453] Kt(an)-UR(an)hash。

[0454] 应该注意的是，如上文所述，每个标题密钥存储为与使用控制信息（使用规则）的哈希值的 XOR 算术运算的结果。

[0455] 在由服务器 A 专用的保护区域 80 的一个块 #081 中，除了标题密钥之外，还设置记录多个有效期数据的有效期信息存储区域。特别地，有效期数据 After#Af1, After#Af2, After#Af3, …和 Before#Bf1, Before#Bf2, Before#Bf3, …存储在有效期信息存储区域中。

[0456] 提及的数据包括与上文参照图 16 描述的数据类似的数据。

[0457] 例如，有效期数据 After#Af1, After#Af2 和 After#Af3 特别地是诸如下面的数据

[0458] After#Af1= 在 2011/09/01 之后

[0459] After#Af2= 在 2011/10/01 之后

[0460] After#Af3= 在 2011/11/01 之后。

[0461] 每个数据 After#Afn 指示在设置的日期以及之后允许内容的使用。

[0462] 同时，有效期数据 Before#Bf1, Before#Bf2 和 Before#Bf3 特别地是诸如例如下面的数据

[0463] Before#Bf1= 在 2011/09/30 之前

[0464] Before#Bf2= 在 2011/10/31 之前

[0465] Before#Bf3= 在 2011/11/30 之前。

[0466] 每个数据 Before#Bfn 指示在设置的日期以及之前（包含该日期）允许内容的使用。

[0467] 除了如上所述的这种实际日期信息之外，本实施例还具有能够执行诸如下面的有效期设置的结构

[0468] After#Afp= 在 (Con(xy) 的状态）之后或者

[0469] Before#Bfq= 在 (Con(xy) 的状态 + 一个月）之前。

[0470] 数据“After#Afp= 在 (Con(xy) 的状态）之后”代表在记录在图 20 的 (b2) 中表示的状态存储块中的内容的首次再现日期和时间以及之后的一定时间段是内容的使用允许时间段。

[0471] 数据“Before#Bfq= 在 (Con(xy) 的状态 + 一个月）之前”代表在记录在图 20 的 (b2) 中表示的状态存储块中的内容的首次再现日期和时间之后经过一个月为止的时间段是内容的使用允许时间段。

[0472] 通过使用这种设置，可以设置与记录在图 20 的 (b2) 中表示的状态存储块中的内容的首次再现日期和时间对应的内容有效期信息。

[0473] 图 21 的 (a) 表示记录在通用区域 90 中的与内容 a1 对应的使用控制信息（使用规则）a1 的特定例子。

[0474] 在使用控制信息（使用规则）中，记录诸如块标识符、标题密钥标识符、块对应期限有效性判定判别比特、有效期信息标识符、状态存储块标识符和状态信息标识符的数据。

[0475] 块标识符至有效期信息标识符是与上文参照图 16 描述的信息类似的信息，并且本文省略对它们的重复的描述以避免冗余。

[0476] 这些数据是与图 21 的 (b1) 中表示的标题密钥存储块对应的信息。

[0477] 以下参照图 22 描述状态存储块标识符和状态信息标识符的数据。

[0478] 这些数据是与状态存储块 #182 对应的信息。

[0479] 状态存储块标识符是指示存储使用控制信息（使用规则）UR(a1) 的对应内容 Con(a1) 的状态信息的状态存储块的信息。

[0480] 在本例子中，状态存储块标识符 =#1，并且执行内容再现的用户设备或主机设备能够辨别状态信息的存储块是块 #1。

[0481] 状态信息标识符是指示存储在状态存储块（也就是说，块 #1）中的许多条状态信息中的哪一条状态信息代表使用控制信息（使用规则）UR(a1) 的对应内容 Con(a1) 的状态。

[0482] 在本例子中，状态信息标识符 =a1，并且能够选择状态信息 (a1)。

[0483] 在作为设置于图 22 的 (b2) 中表示的存储卡 70 的保护区域 80 的状态存储块的块 #182 中，记录内容的首次再现日期和时间。

[0484] 内容的首次再现日期和时间由使用该内容的用户设备或主机设备记录。

[0485] 应该注意的是，在由服务器提供内容时，在作为在存储卡 70 的保护区域 80 中设置的状态存储块的块 #182 中，未记录内容使用开始日期数据，而是仅设置用于记录首次再现日期和时间的状态数据记录区域。

[0486] 每个服务器在内容提供时把上文参照图 22 的 (a) 描述的各种信息（也就是说，块标识符、标题密钥标识符、块对应期限有效性判定判别比特、有效期信息标识符、状态存储块标识符和状态信息标识符）记录在存储卡的通用区域中的使用控制信息（使用规则）中。

[0487] 另外，每个服务器如上文所述把作为状态信息的“内容首次再现日期和时间”的记录区域设置在存储卡的保护区域的状态存储块中。

[0488] 当执行内容再现的用户设备或主机设备执行内容的首次再现时，它把实际首次再现日期和时间数据记录在存储卡的保护区域的状态存储块中。

[0489] 参照图 23 描述由执行内容提供处理的服务器执行的处理。

[0490] 图 23 表示由提供内容的服务器 A 61 执行的存储卡 70 的保护区域 80 的数据记录处理。

[0491] 应该注意的是，除了图 23 中表示的向保护区域 80 的数据记录处理之外，服务器 A 61 还向存储卡 70 的通用区域执行上文参照图 21 和 22 描述的内容和使用控制信息（使用规则）的记录处理。

[0492] 如图 23 中所见，服务器 A 61 把与提供内容对应的标题密钥记录在作为存储卡 70 的保护区域 80 的标题密钥存储块的块 #081 中。

[0493] 另外，在标题密钥的这种记录处理之前，服务器 A 61 把提供内容的状态记录区域设置于存储卡 70 的保护区域 80 的块 #182，并设置每个内容的使用开始日期的记录区域。

[0494] 服务器 A 61 保留记录对块 #081 和块 #182 的写允许信息的服务器证书，并把服务器证书提供给存储卡 70。服务器 A 61 响应于存储卡 70 的访问权限判定处理的结果执行对于各块的标题密钥的写处理和状态信息的记录区域设置。

[0495] 现在，参照图 24 描述执行内容使用的主机设备 63 的处理。

[0496] 当主机设备 63 使用内容时，它根据与使用内容对应的使用控制信息（使用规则）的记录的信息辨别标题密钥的存储块和状态的存储块。

[0497] 根据上文参照图 21 和 22 描述的使用控制信息（使用规则）的记录的信息执行这些处理。

[0498] 主机设备 63 从作为标题密钥存储块的块 #081 获取与使用内容对应的标题密钥。

[0499] 另外，在内容的首次再现时，主机设备 63 把首次再现日期和时间信息记录在状态存储块的状态信息记录区域中。

[0500] 应该注意的是，在记录日期和时间信息时，优选地，主机设备 63 从可靠的时间信息提供服务器等获取并记录准确的日期和时间信息。

[0501] 并非在内容的首次再现处理中，而是在以后的再现处理中，主机设备 63 参照记录在状态存储块的状态信息记录区域中的首次再现日期和时间信息并且还参照记录在状态存储块的状态信息记录区域中的有效期信息，以判定当前日期是否在内容的有效期内。

[0502] 例如，假设关于某一内容 Con(xy) 的记录在状态信息记录区域中的首次再现日期

和时间信息是 2011/09/01。

[0503] 另外，假设在与内容 Con(xy) 对应的使用控制信息 (UR：使用规则）中记录包括块标识符 #0 和有效期信息标识符 #Afp 和 #Bfq 的有效期信息标识符。

[0504] 用户设备或主机设备选择性地从保护区域的块 #0 获取有效期信息标识符 #Afp 和 #Bfq 的有效期信息。假设以下面的方式设置有效期信息：

[0505] After#Afp= 在 (Con(xy) 的状态）之后，

[0506] Before#Bfq= 在 (Con(xy) 的状态 + 一个月）之前。

[0507] 在这种设置的情况下，内容的使用允许时间段是 2011/09/01 至 2011/09/31。

[0508] 用户设备判定当前日期是否被包括在内容使用允许时间段中。如果当前日期被包括在内容使用允许时间段中，则执行内容的解密和再现。然而，如果当前日期未被包括在内容使用允许时间段中，则停止内容使用。

[0509] 应该注意的是，优选地从可靠的时间信息提供服务器等获取当前日期和时间信息。

[0510] 尽管在前面的描述中描述记录为有效期信息或状态信息的首次再现日期和时间信息被设置成单位是天，但它可以不同地被设置为诸如小时、分和秒的单位的时间单位。

[0511] 现在，参照图 25 和图 26 中表示的流程图描述执行内容使用的用户设备或主机设备的内容再现处理序列。

[0512] 根据图 25 和图 26 中表示的流程的处理由用户设备的数据处理部分（诸如，CPU）根据存储在用户设备中的内容再现程序或主机应用执行。

[0513] 首先，在步骤 S301，用户设备的数据处理部分检测到来自用户的再现内容指定信息的输入。例如，数据处理部分检测到内容指定信息的输入，该输入是例如用户在作为显示在再现设备的显示部分上的菜单的内容列表上的输入。

[0514] 然后，在步骤 S302，数据处理部分从装入在用户设备中的存储卡的通用区域读取再现指定内容和使用控制信息。

[0515] 特别地，数据处理部分获取使用对象内容 Con(xy) 和对应使用控制信息 UR(xy)。

[0516] 然后，在步骤 S303，数据处理部分参照读取的使用控制信息 UR(xy) 确认使用控制信息 UR(xy) 的块对应期限有效性判定判别比特（订购使能比特）的设置。

[0517] 如果该比特设置是代表无效的比特“0”，则处理前进至步骤 S304。然而，如果该比特设置是代表有效的比特“1”，则处理前进至步骤 S307。

[0518] 当该比特设置是代表无效的比特“0”并且处理前进至步骤 S304 时，在步骤 S304，数据处理部分参照使用控制信息（使用规则）中的有效期信息。

[0519] 在步骤 S305，数据处理部分判定当前日期是否在有效期内。如果数据处理部分判定当前日期不在有效期内，则处理前进至步骤 S351，在步骤 S351，停止处理。换句话说，不执行内容的解密和使用处理。

[0520] 另一方面，如果在步骤 S305 判定当前日期在有效期内，则处理前进至步骤 S306。

[0521] 在步骤 S306，数据处理部分判定记录在使用控制信息（使用规则）中的标题密钥存储块并从该块读取数据。

[0522] 最后，在步骤 S311，数据处理部分获取存储在从该块读取的数据中的标题密钥，并使用标题密钥执行内容的解密处理，然后执行内容的再现和使用。

[0523] 应该注意的是，在块中存储的标题密钥存储为与使用控制信息（使用规则）的哈希值的异或（XOR）算术运算的结果。数据处理部分通过上文描述的 UR 哈希的计算、与 UR 哈希的 XOR 算术运算处理等执行标题密钥的获取。

[0524] 另一方面，如果在步骤 S303 判定使用控制信息 UR(xy) 的块对应期限有效性判定判别比特（订购使能比特）的设置是指示有效的比特“1”，则处理前进至步骤 S307。在步骤 S307，数据处理部分辨别记录在使用控制信息（使用规则）中的标题密钥存储块并从该块读取数据。

[0525] 然后，在步骤 S308，数据处理部分执行该块中的记录数据的读出处理并确认记录为块内数据的有效期信息。

[0526] 另外，在步骤 S309，数据处理部分判定记录为块内数据的有效期信息是否是状态信息参照类型。

[0527] 状态信息参照类型是如下所述的这种设置的有效期信息的上述类型：

[0528] After #Afp= 在 (Con(xy) 的状态）之后，

[0529] Before#Bfq= 在 (Con(xy) 的状态 + 一个月）之前。

[0530] 在如刚刚所述的这种设置的情况下，如果有效期信息是状态信息参照类型，则处理前进至步骤 S321。

[0531] 如果有效期信息不是如上所述的这种状态信息参照类型，则处理前进至步骤 S310。

[0532] 在步骤 S310，数据处理部分把从块获取的有效期信息和当前日期彼此比较以判定当前日期是否在有效期内。

[0533] 如果在步骤 S310 判定当前日期不在有效期内，则处理前进至步骤 S352，在步骤 S352，停止处理。换句话说，不执行解密和使用处理。

[0534] 另一方面，如果在步骤 S310 判定当前日期在有效期内，则处理前进至步骤 S311。

[0535] 在步骤 S311，数据处理部获取记录在该块中的标题密钥，并使用标题密钥执行内容的解密处理，然后执行内容的再现和使用。

[0536] 另一方面，如果在步骤 S309 判定记录为块内数据的有效期信息是状态信息参照类型，则处理前进至步骤 S321。

[0537] 在这种情况下，数据处理部分在图 26 中表示的步骤 S321 根据使用控制信息文件的记录获取从状态存储块指定的状态信息。

[0538] 然后在步骤 S322，数据处理部分判定首次再现日期和时间信息是否被记录在获取的状态信息中。

[0539] 如果首次再现日期和时间信息被记录在状态信息中，则处理前进至步骤 S323。

[0540] 另一方面，如果首次再现日期和时间信息未被记录在状态信息中，则处理前进至步骤 S324。

[0541] 当首次再现日期和时间信息未被记录在状态信息中并且处理前进至步骤 S324 时，数据处理部分把首次再现日期和时间信息记录为状态信息。应该注意的是，在这种首次再现信息记录处理中，优选地，数据处理部分从可靠的时间信息提供服务器等获取准确的时间信息，并执行时间信息的记录处理。

[0542] 在首次再现日期和时间信息的记录处理之后，处理前进至步骤 S325，在步骤

S325，数据处理部分获取记录在标题密钥存储块中的标题密钥，并使用标题密钥执行内容的解密处理，然后执行内容的再现和使用。

[0543] 另一方面，如果在步骤 S322 辨别首次再现日期和时间信息被记录在获取的状态信息中，则处理前进至步骤 S323。

[0544] 在步骤 S323，数据处理部分基于记录在状态信息中的首次再现日期和时间信息和在步骤 S308 获取的状态信息参照类型的有效期信息判定当前日期是否在有效期内。

[0545] 如果在步骤 S323 判定当前日期不在有效期内，则处理前进至步骤 S353，在步骤 S353，停止处理。换句话说，不执行内容的解密和使用处理。

[0546] 另一方面，如果在步骤 S323 判定当前日期在有效期内，则处理前进至步骤 S325。

[0547] 在步骤 S325，数据处理部获取记录在该块中的标题密钥，并使用标题密钥执行内容的解密处理并执行内容的再现和使用。

[0548] 以这种方式，在本实施例中，记录在块中的有效期信息构造为状态信息参照类型的信息，该信息能够由用户设备记录以由此实现这样的构造 ：在根据用户的内容再现处理设置内容的使用允许时间段的结构中，允许在使用允许时间段的有效期的设置范围内的内容使用。

[0549] 9. 介质之间的内容的移动处理

[0550] 现在，描述在如上所述记录状态信息的结构中当内容在不同介质之间移动时的处理。

[0551] 更具体地讲，描述当记录在作为某一存储卡的第一介质中的内容移动到作为另一存储卡的第二介质时的处理。

[0552] 在为移动对象的内容设置状态参照类型的有效期信息的情况下，状态信息也一起移动。

[0553] 例如，当执行设置了状态参照类型的有效期信息的内容 Con(xy) 在不同介质之间的移动处理时，执行以下各项的移动处理 ：

[0554] 内容 Con(xy)，

[0555] 与内容 Con(xy) 对应的使用控制信息 UR(xy)，

[0556] 与内容 Con(xy) 对应的标题密钥 Kt(xy)，

[0557] 标题密钥 Kt(xy) 的存储块的有效期信息，和

[0558] 记录在使用控制信息 UR(xy) 中的状态存储块的对应状态信息。

[0559] 在进行这种数据移动时，执行从作为移动源介质的第一存储卡的保护区域的块的数据读取和在作为移动目的地介质的第二存储卡的保护区域的块中的数据记录处理。

[0560] 因此，执行由具有对各个块的访问权限的服务器执行的处理。

[0561] 参照图 27 和图 28 描述在内容的移动处理中的服务器的处理。

[0562] 特别地，图 27 表示移动源介质的处理，并且图 28 表示移动目的地介质的处理。

[0563] 应该注意的是，图 27 和图 28 仅表示当执行服务器 A 61 的提供内容的移动处理时的用于存储卡的保护区域的记录数据的处理。

[0564] 通用区域的数据移动能够由用户设备执行。

[0565] 首先，参照图 27 描述移动源介质的处理。

[0566] 服务器 A 61 从作为移动源介质 301 的标题密钥存储块的块 #0 读出并获取与移动

对象内容对应的标题密钥，并从块 #0 删除标题密钥数据。

[0567] 另外，服务器 A 61 从作为移动源介质 301 的状态存储块的块 #1 读出并获取与移动对象内容对应的状态信息，然后从块 #1 删除状态信息。

[0568] 通过这种处理，从移动源介质 301 删除与移动对象内容对应的标题密钥和状态信息。

[0569] 现在，参照图 28 描述移动目的地介质的处理。

[0570] 服务器 A 61 把从移动源介质获取的与移动对象内容对应的标题密钥记录在作为移动目的地介质 302 的标题密钥存储块的块 #0 中。

[0571] 另外，服务器 A 61 把从移动源介质获取的与移动对象内容对应的状态信息记录在作为移动目的地介质 302 的状态存储块的块 #1 中。

[0572] 通过该处理，与移动对象内容对应的标题密钥和状态信息被记录在移动目的地介质 302 中。

[0573] 应该注意的是，在执行以上参照图 27 描述的服务器 A 61 和移动源介质 301 之间的处理时，执行服务器 A 61 和移动源介质 301 之间的相互认证处理。另外，移动源介质 301 基于从服务器 A 61 接收的服务器证书执行块的访问权限确认。

[0574] 以认证的成功和访问权限的确认为条件，执行上文参照图 27 描述的处理。

[0575] 类似地，在执行以上参照图 28 描述的服务器 A 61 和移动目的地介质 302 之间的处理时，执行服务器 A 61 和移动目的地介质 302 之间的相互认证处理。另外，移动目的地介质 302 基于从服务器 A 61 接收的服务器证书执行块的访问权限确认。

[0576] 以认证的成功和访问权限的确认为条件，执行上文参照图 28 描述的处理。

[0577] 10. 设备的硬件结构的例子

[0578] 最后，参照图 29 和图 30 描述执行上述处理的设备的硬件结构的例子。

[0579] 首先，参照图 29 描述主机设备的硬件结构的例子，该主机设备执行把数据记录在装入在主机设备中的存储卡中的处理或者对来自该存储卡的数据执行再现处理。

[0580] CPU（中央处理单元）701 用作数据处理部分，该数据处理部分根据存储在 ROM（只读存储器）702 或存储部分 708 中的程序执行各种处理。例如，CPU 701 执行从广播站或服务器的内容接收处理、把接收数据记录到作为图 29 中的可移动介质 711 的存储卡中的记录处理、从存储卡（即，从可移动介质 711）的数据再现处理和其它处理。由 CPU 701 执行的程序、数据等合适地存储在 RAM（随机存取存储器）703 中。CPU 701、ROM 702 和 RAM 703 经总线 704 彼此连接。

[0581] CPU 701 通过总线 704 连接到输入 / 输出接口 705，并且输入部分 706 和输出部分 707 连接到输入 / 输出接口 705，输入部分 706 由各种开关、键盘、鼠标、麦克风等形成，输出部分 707 由显示单元、扬声器等形成。CPU 701 根据从输入部分 706 输入的指令执行各种处理，并把处理的结果输出到例如输出部分 707。

[0582] 连接到输入 / 输出接口 705 的存储部分 708 例如由硬盘驱动器构成，并存储由 CPU 701 执行的程序和各种数据。通信部分 709 通过网络（诸如，互联网或局域网）与外部设备通信。

[0583] 连接到输入 / 输出接口 705 的驱动器 710 驱动可移动介质 711（诸如，磁盘、光盘、磁光盘或存储卡），并获取记录在可移动介质 711 上的各种数据（诸如，内容或密钥信息）。

例如，使用获取的内容或密钥信息，根据由 CPU 701 执行的再现程序执行内容的解密和再现处理。

[0584] 图 30 显示存储卡的硬件结构的例子。

[0585] 参照图 30，CPU（中央处理单元）801 用作数据处理部分，该数据处理部分根据存储在 ROM（只读存储器）802 或存储部分 807 中的程序执行各种处理。例如，CPU 801 执行与在实施例的前面描述中在上文描述的服务器或主机设备的通信处理、诸如写入存储部分 807 中以及从存储部分 807 读取的处理、以存储部分 807 的保护区域 811 的分割区域为单位的访问允许 / 拒绝判定处理和其它处理。由 CPU 801 执行的程序、数据等合适地存储在 RAM（随机存取存储器）803 中。CPU801、ROM 802 和 RAM 803 通过总线 804 彼此连接。

[0586] CPU 801 通过总线 804 连接到输入 / 输出接口 805，并且通信部分 806 和存储部分 807 连接到输入 / 输出接口 805。

[0587] 连接到输入 / 输出接口 805 的通信部分 806 执行例如与服务器或主机设备的通信。存储部分 807 是用于数据的存储区域，并具有如上文所述访问受限的保护区域 811 和能够自由地记录和读出数据的通用区域 812。

[0588] 应该注意的是，服务器能够由具有与例如图 29 中显示的主机设备的硬件结构相似的硬件结构的设备实现。

[0589] 11. 本发明的结构的总结

[0590] 尽管已具体地描述了本发明的特定实施例，但能够由本领域技术人员基于本发明的技术范围以各种方式对本发明做出修改或改变。换句话说，作为说明而给出本发明，而不应该以限制性的方式解释本发明。为了判定本发明的主题，应该参照权利要求。

[0591] 应该注意的是，本文公开的技术能够具有如下所述的这种构造。

[0592] (1) 一种信息处理设备，包括：

[0593] 数据处理部分，构造为再现存储在介质中的内容；

[0594] 所述介质具有

[0595] 通用区域，在所述通用区域中存储加密内容和与加密内容对应的使用控制信息；和

[0596] 保护区域，所述保护区域由多个块构成，对于所述多个块设置了访问限制，并且所述多个块包括存储用于解密所述加密内容的加密密钥的块；

[0597] 所述数据处理部分从所述通用区域获取与内容对应的使用控制信息；

[0598] 所述数据处理部分用于基于所获取的使用控制信息的记录数据来判定是从所述使用控制信息还是从存储加密密钥的块获取指示内容使用允许时间段的有效期信息，根据判定的结果从所述使用控制信息或块获取有效期信息，然后把所获取的有效期信息与当前日期信息进行比较以判定是否允许内容的再现。

[0599] (2) 如以上 (1) 所述的信息处理设备，其中所述使用控制信息的记录数据根据判别比特构造，基于该判别比特能够判定记录在存储所述加密密钥的块中的有效期信息的有效性；以及所述数据处理部分响应于所述判别比特的值从块和所述使用控制信息中的一个获取所述有效期信息。

[0600] (3) 如以上 (1) 或 (2) 所述的信息处理设备，其中记录在存储用于解密所述加密内容的加密密钥并设置了访问限制的块中的有效期信息被共同应用于与记录在该块中的多

个加密密钥对应的多个内容。

[0601] (4) 如以上 (1) 至 (3) 中任何一项所述的信息处理设备，其中所述数据处理部分基于所述使用控制信息的记录数据指定存储用于解密所述加密内容的加密密钥的块，以及获取所指定的块的存储数据，然后获取所获取的数据中包含的有效期信息。

[0602] (5) 如以上 (1) 至 (4) 中任何一项所述的信息处理设备，其中所述数据处理部分执行这样的处理，即当从使用控制信息或块获取的有效期信息和当前日期信息之间进行比较处理时，应用从可靠的时间信息提供服务器获取的当前日期信息。

[0603] (6) 如以上 (1) 至 (5) 中任何一项所述的信息处理设备，其中存储所述加密密钥的块是基于介质做出的访问权限判定而允许访问的块；以及在块的数据读出处理时，所述数据处理部分把信息处理设备的证书发送给介质，并且在通过介质做出的访问权限判定而确认数据读出权限的条件下执行块的数据读出。

[0604] (7) 如以上 (1) 至 (6) 中任何一项所述的信息处理设备，其中存储所述加密密钥的块是基于介质做出的访问权限判定而允许访问的块；以及由具有对块的数据写入处理的权限的服务器写入和更新记录在块中的有效期信息

[0605] (8) 一种信息处理设备，包括：

[0606] 数据处理部分，被构造为把内容记录到介质中；

[0607] 所述介质具有：

[0608] 通用区域，在所述通用区域中存储加密内容和与所述加密内容对应的使用控制信息，以及

[0609] 保护区域，所述保护区域由多个块构成，对所述多个块设置了访问限制，所述多个块包括存储用于解密所述加密内容的加密密钥的块；

[0610] 所述数据处理部分执行以下处理：

[0611] 执行用于把加密内容和与所述加密内容对应的使用控制信息记录到所述通用区域的处理；

[0612] 把用于解密记录在通用区域中的加密内容的加密密钥记录到所述保护区域的块中；

[0613] 执行用于记录或更新有效期信息的处理，所述有效期信息作为块的记录数据指示可共同应用于与记录在保护区域的块中的多个加密密钥对应的内容的内容的使用允许时间段。

[0614] (9) 如以上 (8) 所述的信息处理设备，其中所述数据处理部分执行用于把数据记录到介质的通用区域的使用控制信息中的处理，利用该数据能够判定是从使用控制信息还是从存储加密密钥的块获取指示内容使用允许时间段的有效期信息。

[0615] (10) 如以上 (8) 或 (9) 所述的信息处理设备，其中存储加密密钥的块是基于介质做出的访问权限判定而允许访问的块；以及在对块的数据记录处理时，所述数据处理部分把信息处理设备的证书发送给介质，并且在通过介质的访问权限判定而确认所述信息处理设备具有数据记录处理的权限的条件下执行对块的数据记录处理。

[0616] (11) 一种信息存储设备，包括：

[0617] 数据存储部分；

[0618] 所述数据存储部分包括：

[0619] 通用区域，在所述通用区域中存储加密内容和与所述加密内容对应的使用控制信息，以及

[0620] 保护区域，所述保护区域由多个块构成，对所述多个块设置了访问限制，所述多个块包括存储用于解密所述加密内容的加密密钥的块；

[0621] 存储用于解密所述加密内容的加密密钥的块还具有有效期信息作为记录数据，所述有效期信息指示可共同应用于与记录在块中的多个加密密钥对应的内容的内容的使用允许时间段；

[0622] 所述信息存储设备使得执行加密内容的再现处理的再现设备基于对记录在块中的有效期信息的参照处理来执行内容再现允许 / 禁止判定。

[0623] (12) 如以上 (11) 所述的信息处理设备，其中所述使用控制信息被构造为记录存储用于解密所述加密内容的加密密钥的块的识别信息；以及所述信息存储设备使得执行所述加密内容的再现的再现设备基于对记录在使用控制信息中的块标识符的参照处理来执行块指定处理。(13) 如以上 (11) 或 (12) 所述的信息处理设备，还包括数据处理部分，所述数据处理部分被构造为获取对保护区域的块的访问请求设备的证书以及基于所获取的证书执行访问允许判定处理。

[0624] (14) 一种信息处理系统，包括：

[0625] 介质，被构造为在其中记录数据；

[0626] 再现设备，被构造为再现存储在所述介质中的内容；以及

[0627] 服务器，被构造为执行对所述介质的数据记录；

[0628] 所述介质具有：

[0629] 通用区域，在所述通用区域中存储加密内容和与所述加密内容对应的使用控制信息，以及

[0630] 保护区域，所述保护区域被构造为多个块，对所述多个块设置了访问限制，所述多个块包括存储用于解密所述加密内容的加密密钥的块；

[0631] 所述服务器用于执行以下处理：

[0632] 执行用于把加密内容和与所述加密内容对应的使用控制信息记录到通用区域中的处理，

[0633] 把用于解密记录在通用区域中的加密内容的加密密钥记录到保护区域的块中，以及

[0634] 执行记录或更新有效期信息的处理，所述有效期信息作为块的数据指示可共同应用于与记录在保护区域的块中的多个加密密钥对应的内容的内容的使用允许时间段；

[0635] 所述再现设备从通用区域获取与内容对应的使用控制信息；

[0636] 所述再现设备用于基于所获取的使用控制信息的记录数据来判定是从使用控制信息还是从存储所述加密密钥的块获取指示内容使用允许时间段的有效期信息，根据判定的结果从使用控制信息或所述块获取有效期信息，然后基于所获取的有效期信息和当前日期信息之间的比较来判定允许或禁止内容再现。

[0637] 在上述设备和系统中执行的处理的方法和用于执行该处理的程序也被包括在本发明的结构中。

[0638] 另外，在说明书中在上文描述的一系列处理能够由硬件、软件或者它们的复合结

构执行。在由软件执行所述一系列处理的情况下，记录处理序列的程序被安装在专用硬件中所包括的计算机中的存储器中以便由计算机执行。或者程序可以被安装在能够执行各种功能的通用计算机中以便由计算机执行。例如，可以预先把程序记录在记录介质中。程序可以被从记录介质安装到计算机。或者，可以通过网络（诸如，LAN（局域网）或互联网）接收程序并把程序安装在内置记录介质（诸如，硬盘）中。

[0639] 应该注意的是，在本发明中描述的各种处理可以根据描述的次序按照时间顺序执行，或者可以基于组成设备的处理能力或在必要时并行地或者单独地执行。另外，在本说明书中，术语“系统”用于代表多个设备的逻辑集合结构，并且不限于组成设备容纳于同一壳体中的系统。

[0640] 如上所述，根据本发明的实施例的结构，实现了这样的设备和方法，其中把与块对应的有效期信息设置到存储介质中存储的内容的加密密钥的块，并且能够执行多个内容的集体的有效期的设置和更新。

[0641] 具体地讲，再现存储在介质中的内容，该介质具有通用区域和保护区域，在通用区域中存储加密内容和使用控制信息，保护区域由多个块构成，对所述多个块设置了访问限制，所述多个块包括存储用于解密该加密内容的加密密钥的块。再现设备从通用区域获取与内容对应的使用控制信息。然后，再现设备基于使用控制信息的记录数据判定是从使用控制信息还是从存储加密密钥的块获取指示内容使用允许时间段的有效期信息。然后，再现设备响应于判定的结果而从使用控制信息或块获取有效期信息，然后通过所获取的有效期信息与当前日期信息之间的比较来判定是允许还是禁止内容再现。

[0642] 通过该处理，实现了这样的设备和方法，它们能够把块对应有效期信息设置到存储介质中存储的内容的加密密钥的块，并且执行多个内容的集体的有效期的设置和更新。

[0643] 本发明包含与 2011 年 9 月 15 日提交给日本专利局的日本优先权专利申请 JP 2011-202184 中公开的主题相关的主题，该专利申请的全部内容通过引用包含于此。

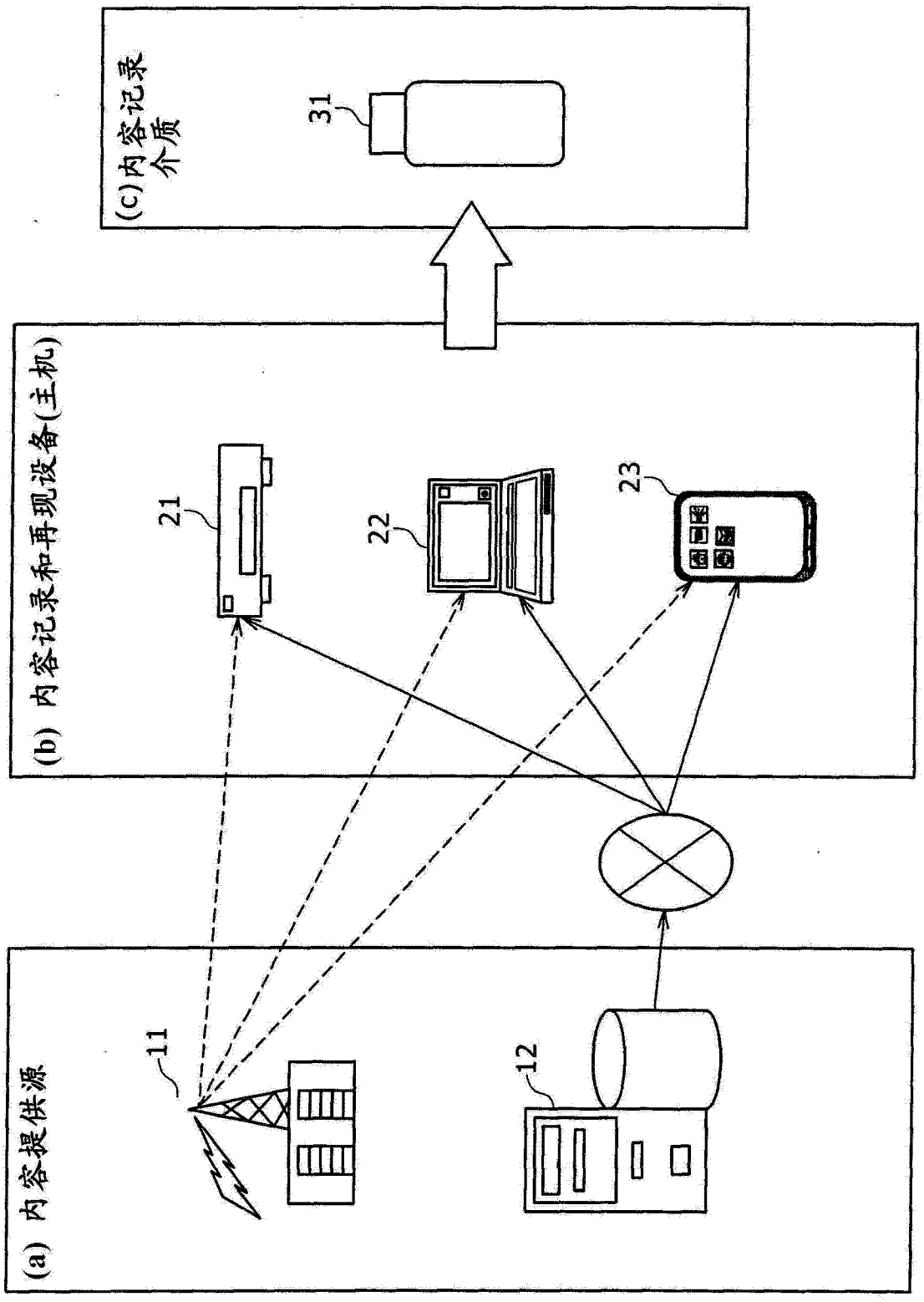


图 1

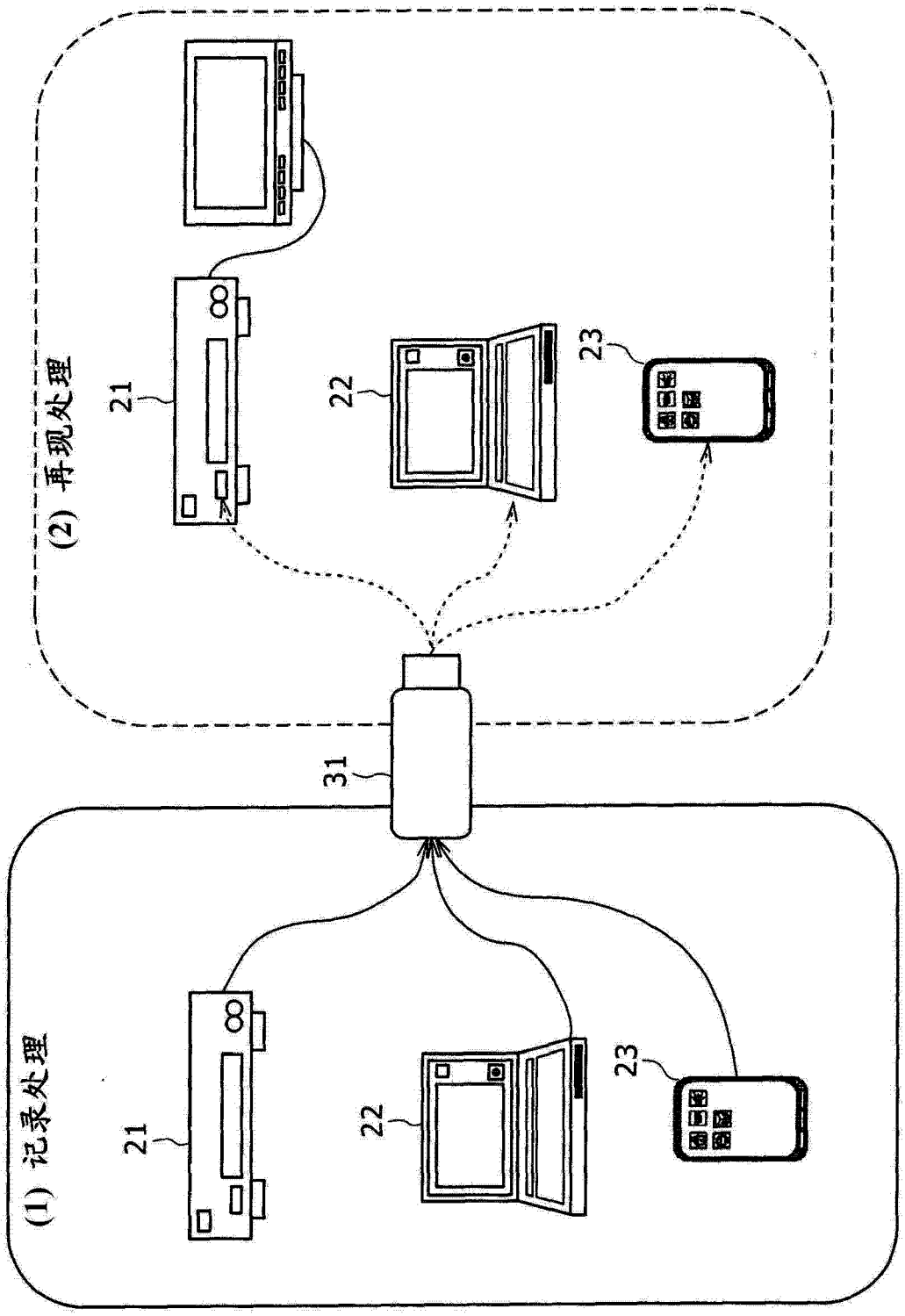


图 2

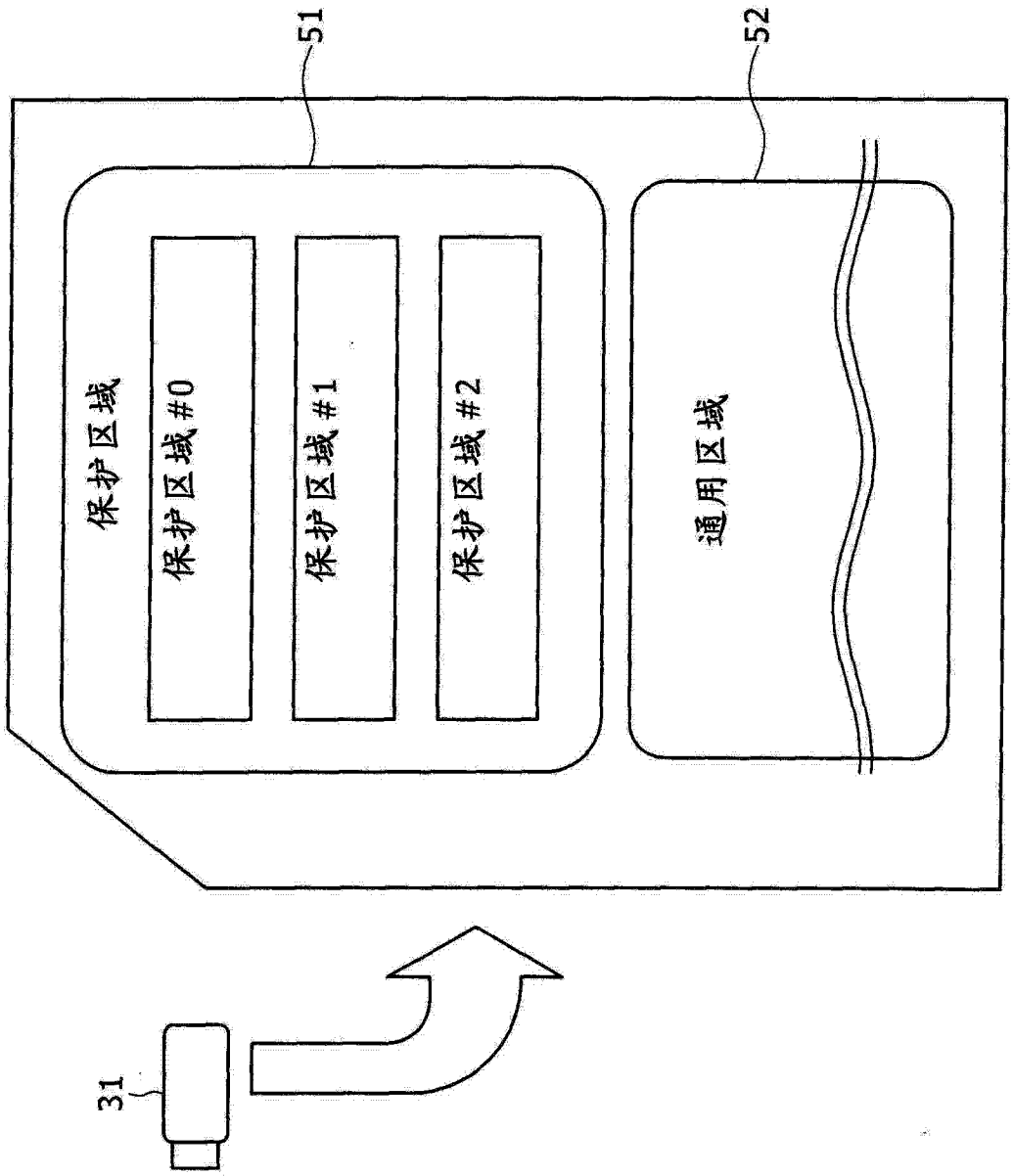


图 3

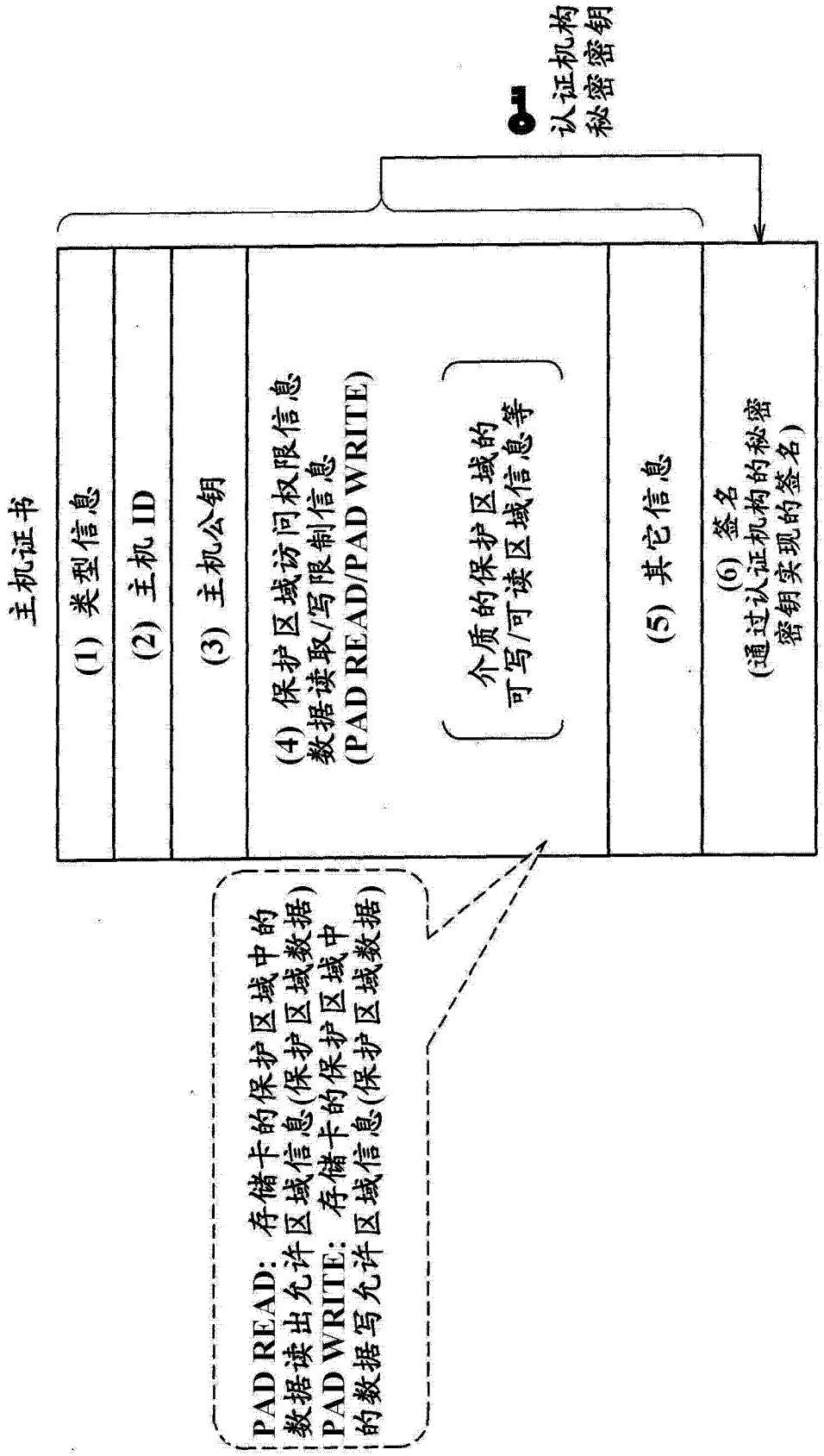

主机证书
(1) 类型信息
(2) 主机 ID
(3) 主机公钥
(4) 保护区域访问权限信息
数据读取/写限制信息
(PAD READ/PAD WRITE)
介质的保护区域的
可写/可读区域信息等
(5) 其它信息
(6) 签名
(通过认证机构的秘密
密钥实现的签名)
认证机构
秘密密钥
PAD READ: 存储卡的保护区域中的
数据读出允许区域信息(保护区域数据)
PAD WRITE: 存储卡的保护区域中
的数据写允许区域信息(保护区域数据)

图 4

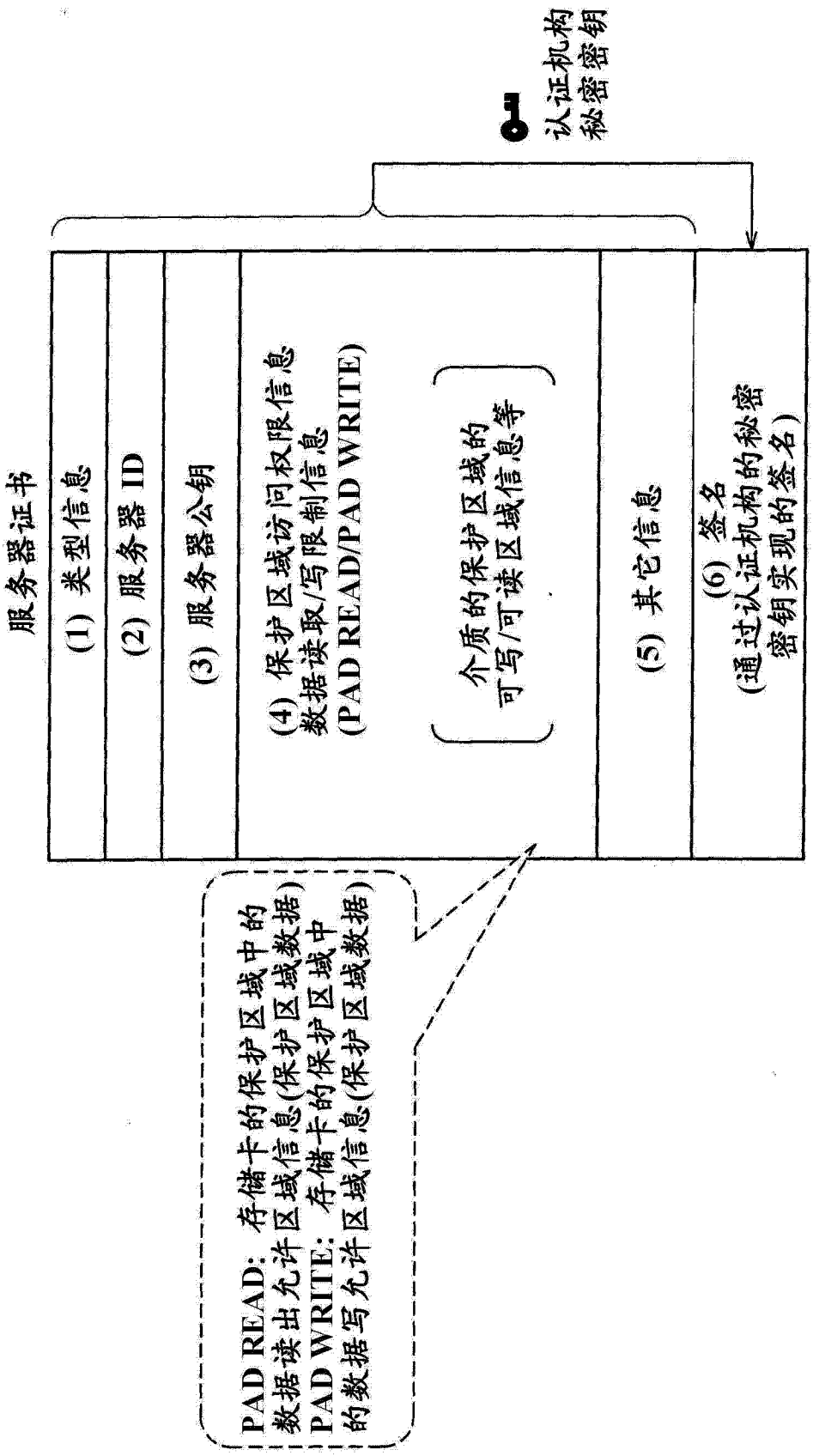

认证机构
秘密密钥
服务器证书
(1) 类型信息
(2) 服务器 ID
(3) 服务器公钥
(4) 保护区域访问权限信息
数据读取/写限制信息
(PAD READ/PAD WRITE)
介质的保护区域的
可写/可读区域信息等
(5) 其它信息
(6) 签名
(通过认证机构的秘密
密钥实现的签名)
PAD READ: 存储卡的保护区域中的
数据读出允许区域信息(保护区域数据)
PAD WRITE: 存储卡的保护区域中
的数据写允许区域信息(保护区域数据)

图 5

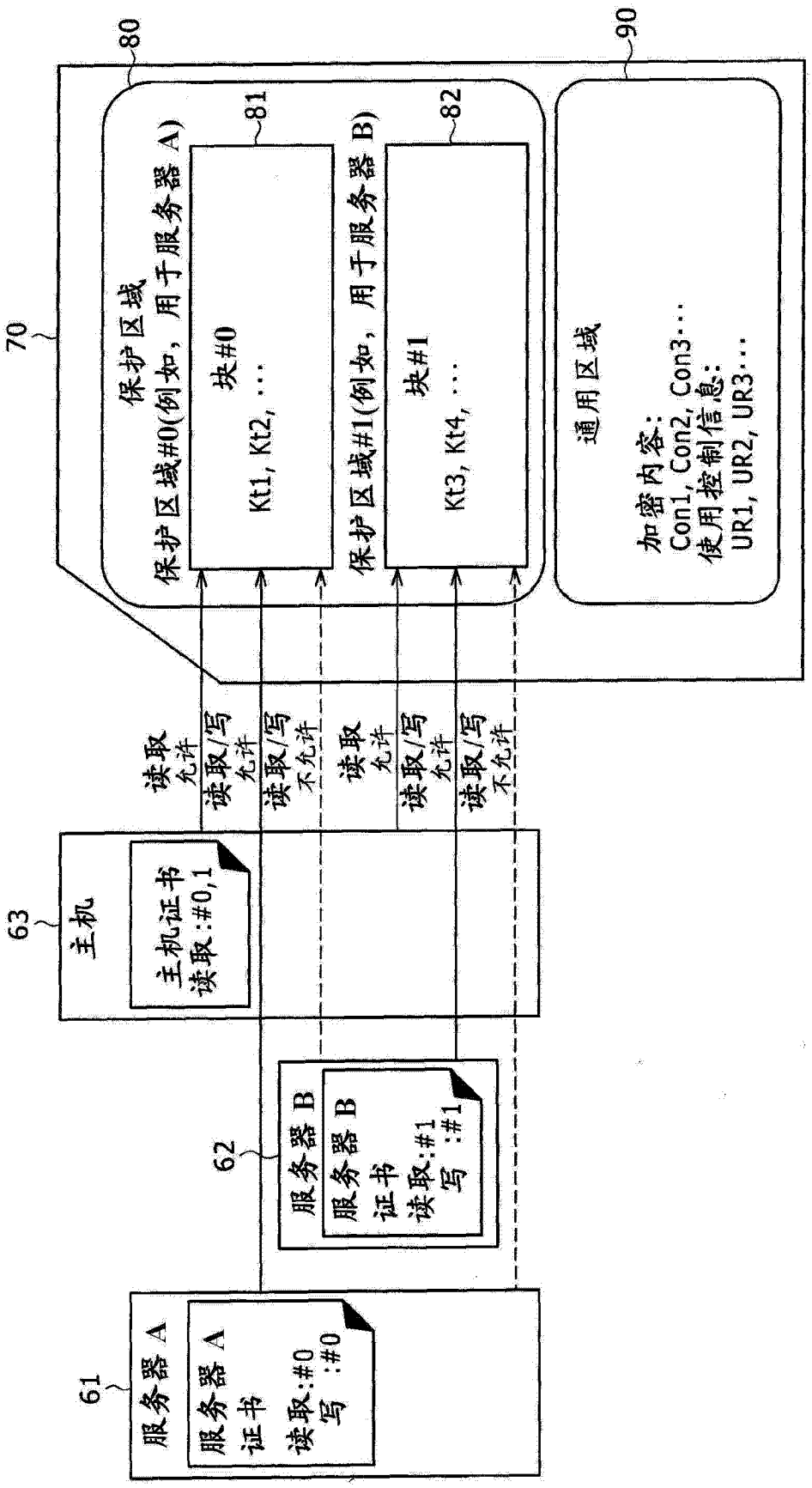
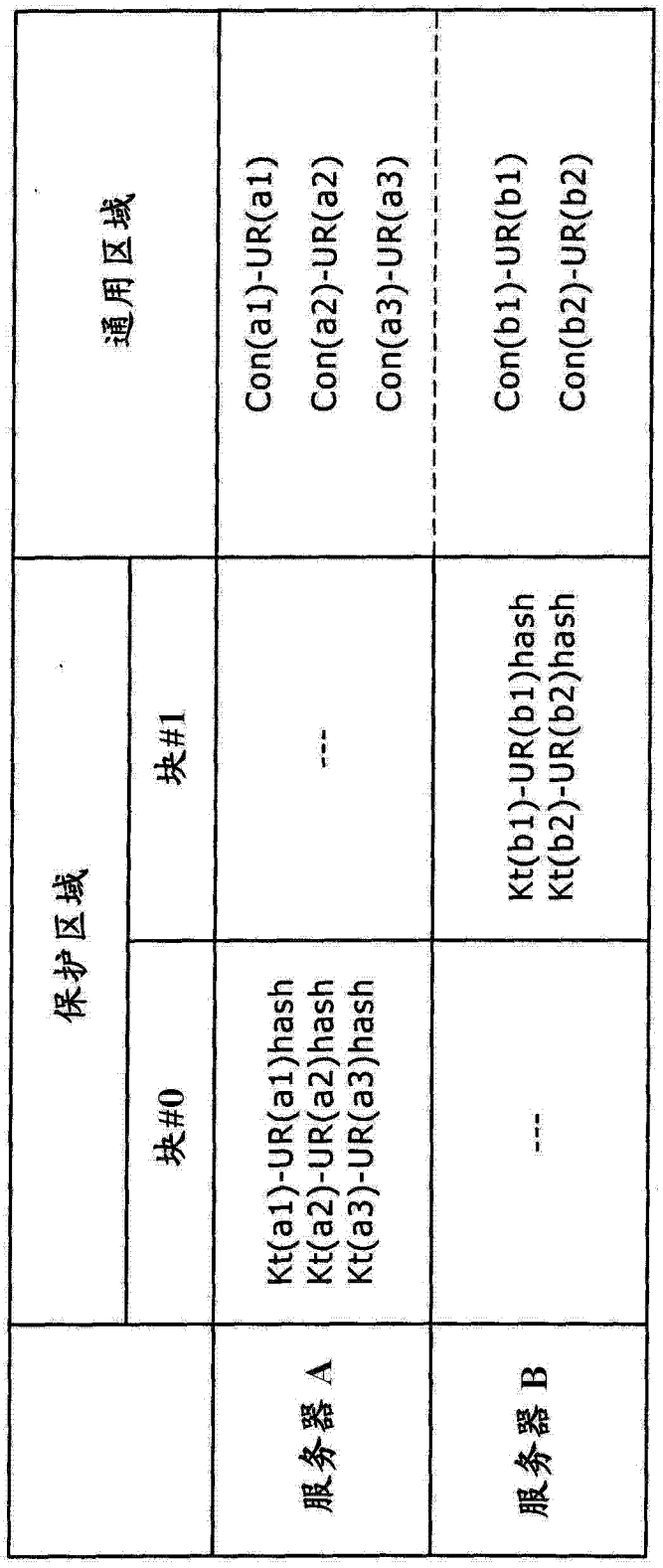

70
80
保护区域
保护区域#0(例如，用于服务器 A)
块#0
Kt1, Kt2, ···
81
保护区域#1(例如，用于服务器 B)
块#1
Kt3, Kt4, ···
82
90
通用区域
加密内容:
Con1, Con2, Con3···
使用控制信息:
UR1, UR2, UR3···
读取
允许
读取/写
允许
读取/写
不允许
读取
允许
读取/写
允许
读取/写
不允许
63
主机
主机证书
读取:#0,1
62
服务器 B
服务器 B
证书
读取:#1
写 :#1
61
服务器 A
服务器 A
证书
读取:#0
写 :#0

图 6


保护区域
通用区域
块#0
块#1
服务器 A
Kt(a1)-UR(a1)hash
Kt(a2)-UR(a2)hash
Kt(a3)-UR(a3)hash

Con(a1)-UR(a1)
Con(a2)-UR(a2)
Con(a3)-UR(a3)
服务器 B

Kt(b1)-UR(b1)hash
Kt(b2)-UR(b2)hash
Con(b1)-UR(b1)
Con(b2)-UR(b2)

图 7

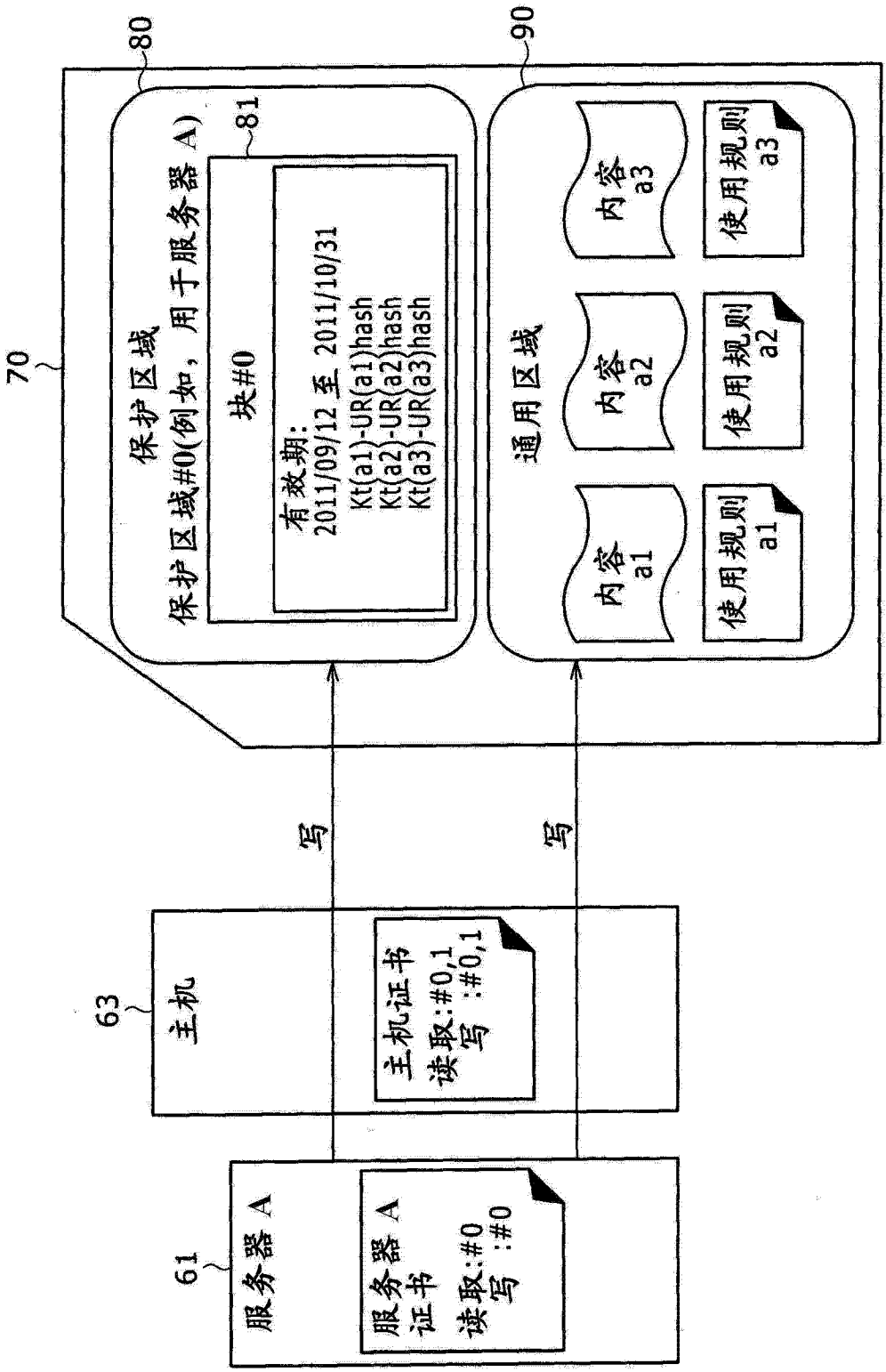

70
80
保护区域
保护区域#0(例如，用于服务器 A)
81
块#0
有效期:
2011/09/12 至 2011/10/31
Kt(a1)-UR(a1)hash
Kt(a2)-UR(a2)hash
Kt(a3)-UR(a3)hash
90
通用区域
内容 a1
使用规则 a1
内容 a2
使用规则 a2
内容 a3
使用规则 a3
写
写
63
主机
主机证书
读取:#0,1
写 :#0,1
61
服务器 A
服务器 A 证书
读取:#0
写 :#0

图 8

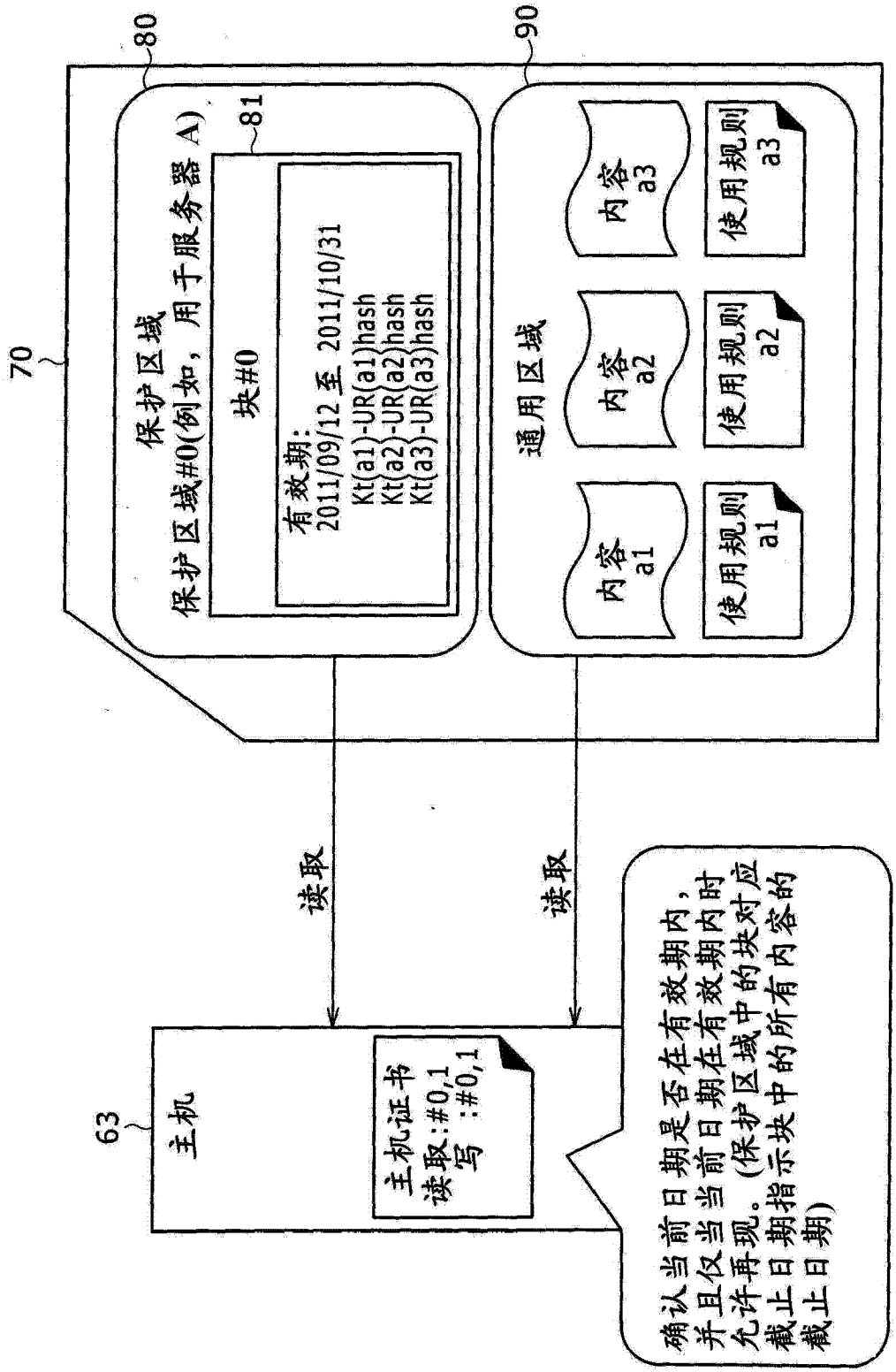

70
80
保护区域
保护区域#0(例如，用于服务器 A)
81
块#0
有效期:
2011/09/12 至 2011/10/31
Kt(a1)-UR(a1)hash
Kt(a2)-UR(a2)hash
Kt(a3)-UR(a3)hash
90
通用区域
内容 a1
使用规则 a1
内容 a2
使用规则 a2
内容 a3
使用规则 a3
读取
读取
63
主机
主机证书
读取:#0,1
写 :#0,1
确认当前日期是否在有效期内，并且仅当当前日期在有效期内时允许再现。(保护区域中的块对应截止日期指示块中的所有内容的截止日期)

图 9

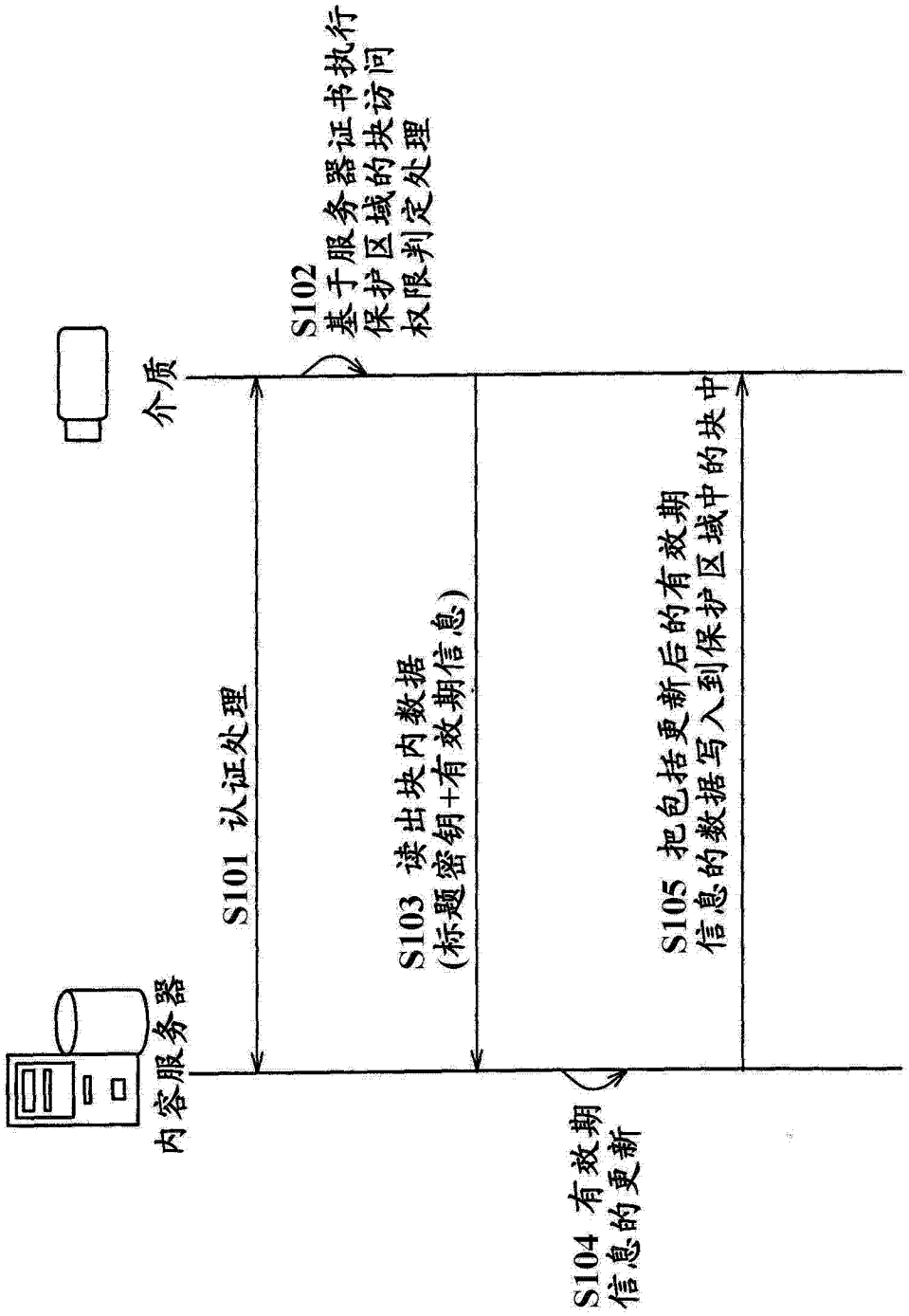

介质
内容服务器
S101 认证处理
S102
基于服务器证书执行
保护区域的块访问
权限判定处理
S103 读出块内数据
(标题密钥+有效期信息)
S104 有效期
信息的更新
S105 把包括更新后的有效期
信息的数据写入到保护区域中的块中

图 10

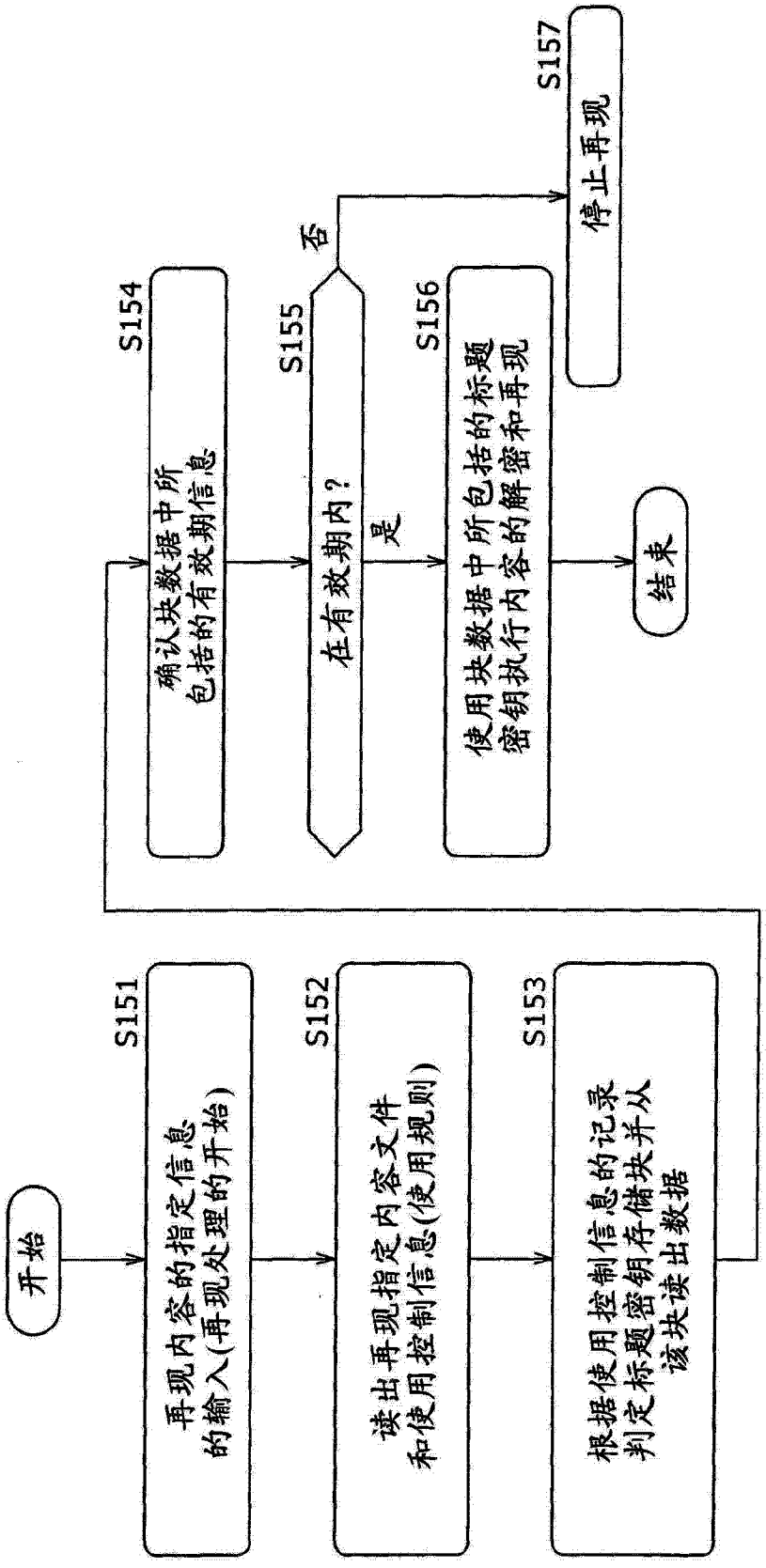
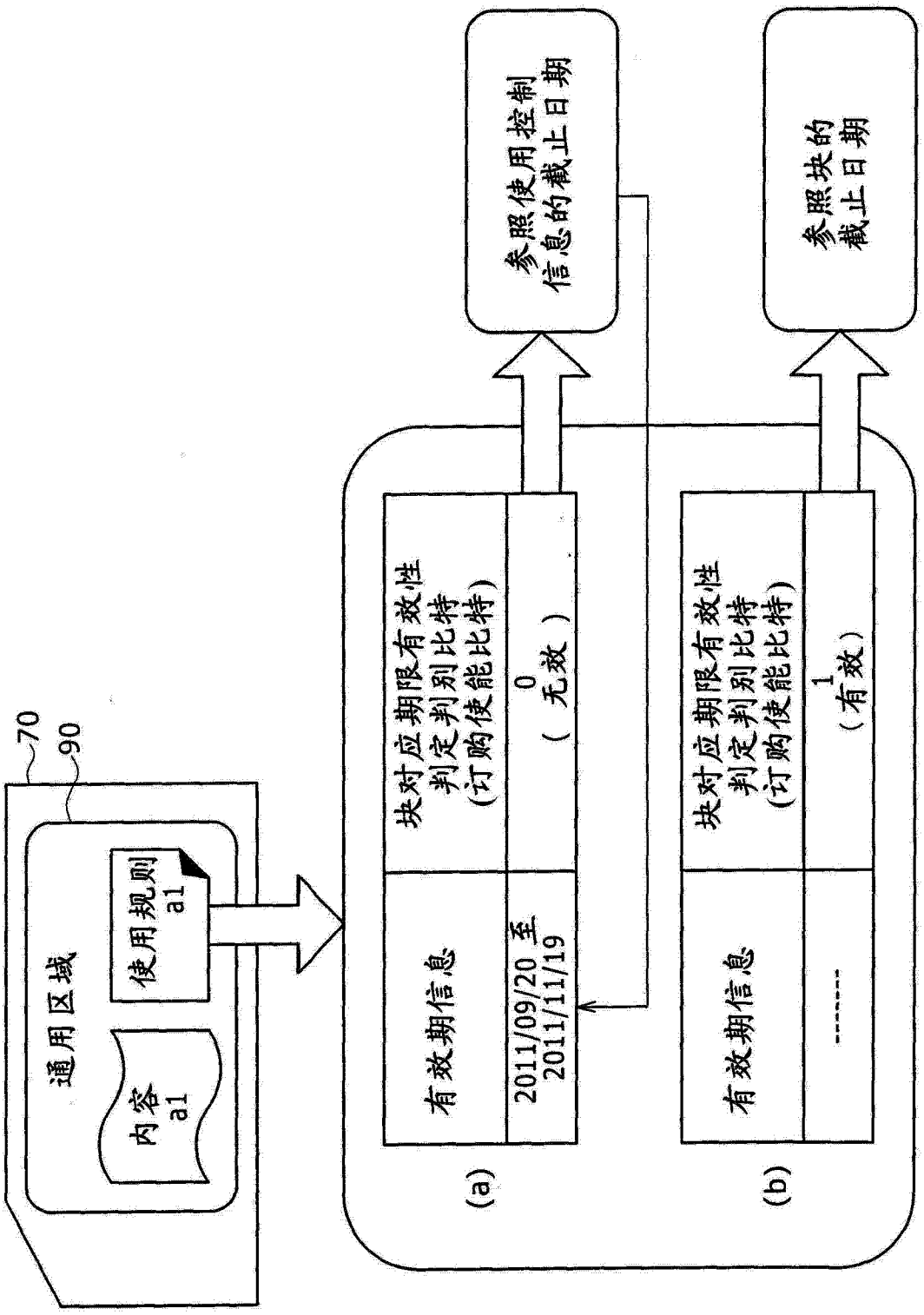

开始
S151
再现内容的指定信息
的输入(再现处理的开始)
S152
读出再现指定内容文件
和使用控制信息(使用规则)
S153
根据使用控制信息的记录
判定标题密钥存储块并从
该块读出数据
S154
确认块数据中所
包括的有效期信息
S155
在有效期内?
否
是
S156
使用块数据中所包括的标题
密钥执行内容的解密和再现
S157
停止再现
结束

图 11


70
90
通用区域
内容
a1
使用规则
a1
有效期信息
块对应期限有效性
判定判别比特
(订购使能比特)
2011/09/20 至
2011/11/19
0
(无效)
(a)
有效期信息
块对应期限有效性
判定判别比特
(订购使能比特)

1
(有效)
(b)
参照使用控制
信息的截止日期
参照块的
截止日期

图 12

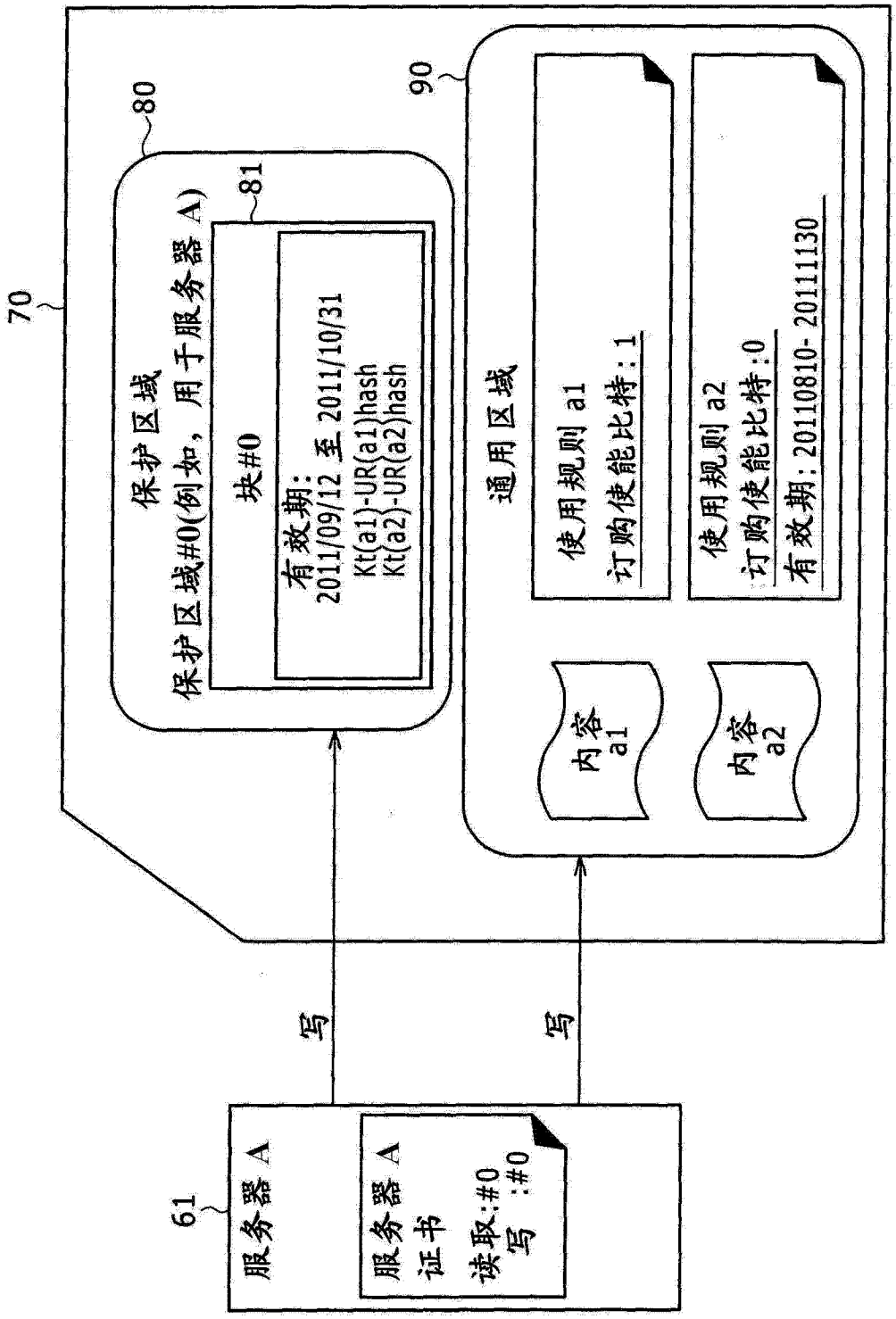

70
80
保护区域
保护区域#0(例如，用于服务器 A)
81
块#0
有效期：
2011/09/12 至 2011/10/31
Kt(a1)-UR(a1)hash
Kt(a2)-UR(a2)hash
90
通用区域
使用规则 a1
订购使能比特：1
使用规则 a2
订购使能比特：0
有效期：20110810- 20111130
内容
a1
内容
a2
写
写
61
服务器 A
服务器 A
证书
读取：#0
写 ：#0

图 13

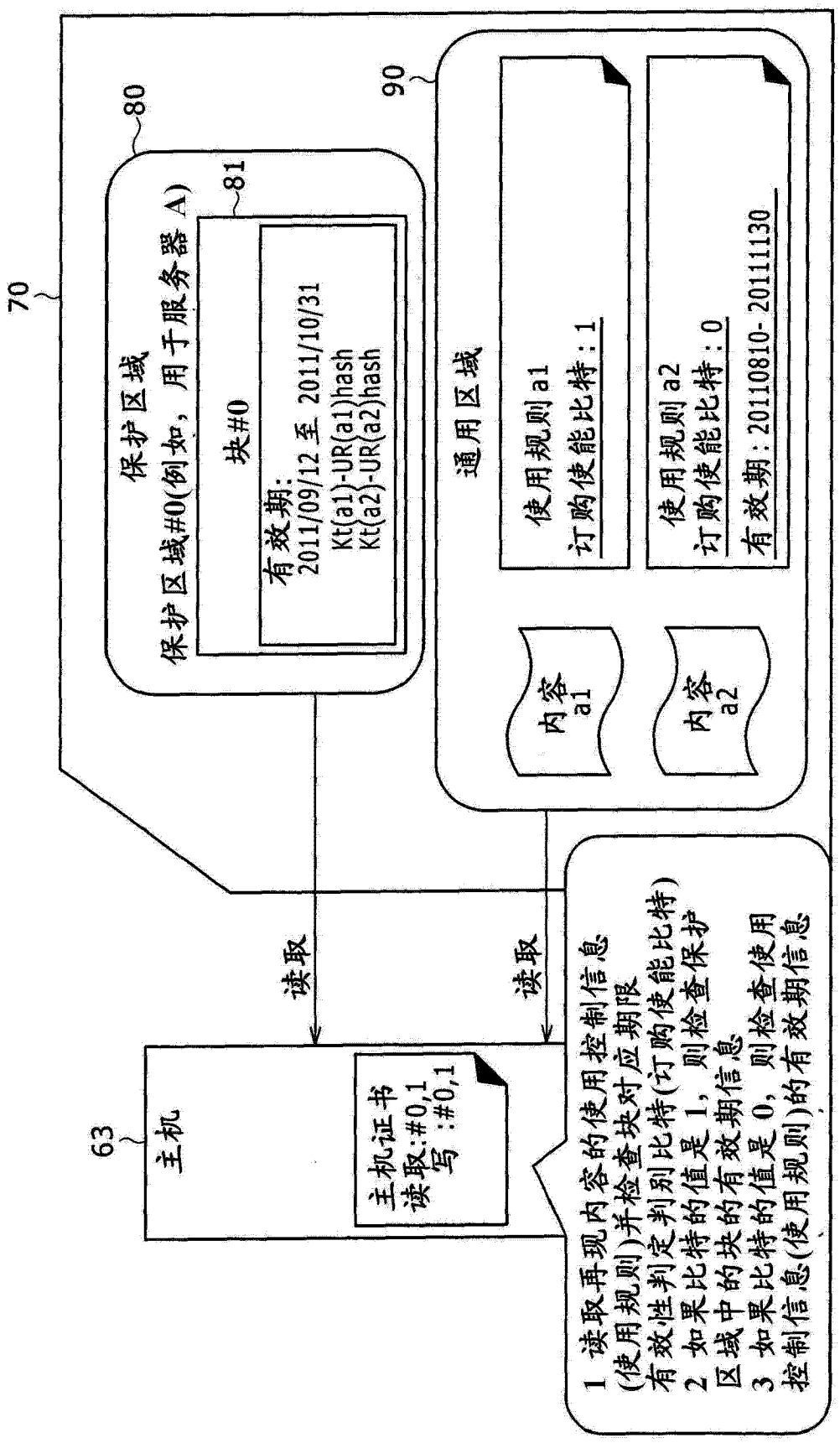

70
保护区域
保护区域#0(例如，用于服务器 A)
80
块#0
81
有效期:
2011/09/12 至 2011/10/31
Kt(a1)-UR(a1)hash
Kt(a2)-UR(a2)hash
通用区域
90
使用规则 a1
订购使能比特：1
使用规则 a2
订购使能比特：0
有效期：20110810- 20111130
内容
a1
内容
a2
读取
读取
63
主机
主机证书
读取:#0,1
写 :#0,1
1 读取再现内容的使用控制信息
(使用规则)并检查块对应期限
有效性判定判别比特(订购使能比特)
2 如果比特的值是 1，则检查保护
区域中的块的有效期信息
3 如果比特的值是 0，则检查使用
控制信息(使用规则)的有效期信息

图 14

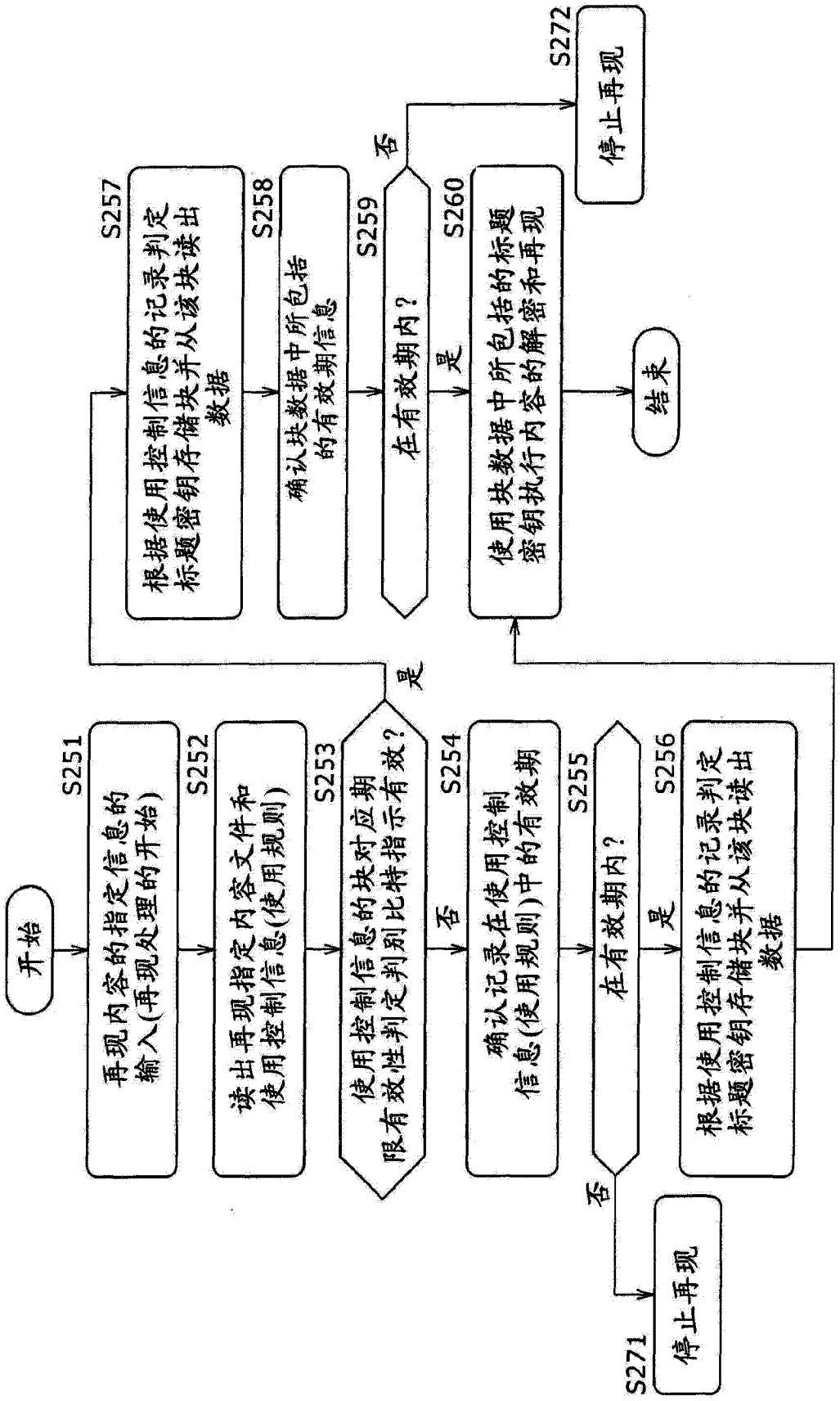

开始
S251
再现内容的指定信息的输入(再现处理的开始)
S252
读出再现指定内容文件和使用控制信息(使用规则)
S253
使用控制信息的块对应期限有效性判定判别比特指示有效?
否
是
S254
确认记录在使用控制信息(使用规则)中的有效期
S255
在有效期内?
否
是
S256
根据使用控制信息的记录判定标题密钥存储块并从该块读出数据
S257
根据使用控制信息的记录判定标题密钥存储块并从该块读出数据
S258
确认块数据中所包括的有效期信息
S259
在有效期内?
否
是
S260
使用块数据中所包括的标题密钥执行内容的解密和再现
结束
S271
停止再现
S272
停止再现

图 15

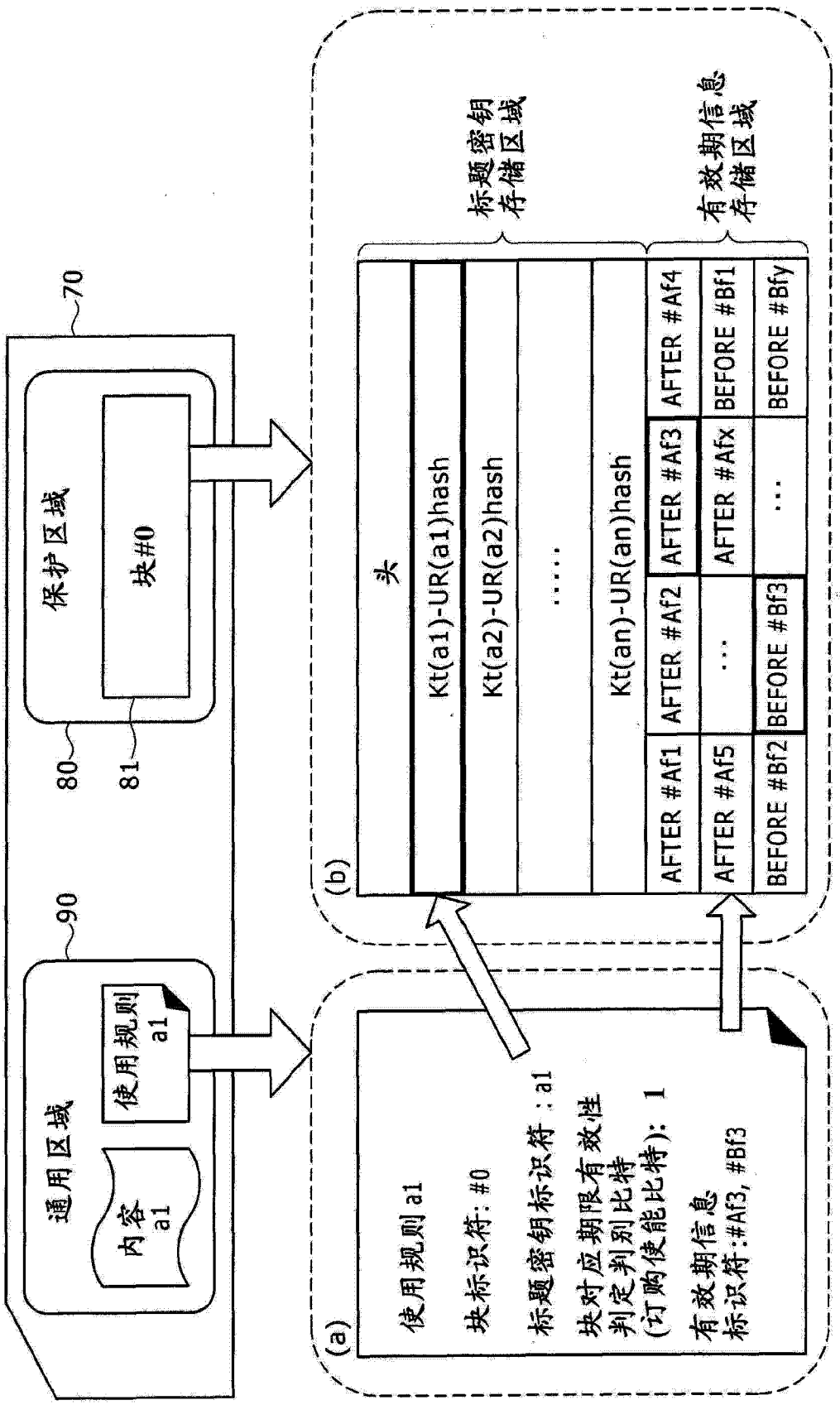

70
保护区域
块#0
80
81
通用区域
内容
a1
使用规则
a1
90
(a)
使用规则 a1
块标识符: #0
标题密钥标识符 : a1
块对应期限有效性
判定判别比特
(订购使能比特): 1
有效期信息
标识符:#Af3, #Bf3
(b)
头
Kt(a1)-UR(a1)hash
Kt(a2)-UR(a2)hash
.....
Kt(an)-UR(an)hash
标题密钥
存储区域
有效期信息
存储区域
AFTER #Af1
AFTER #Af2
AFTER #Af3
AFTER #Af4
AFTER #Af5
...
AFTER #Afx
BEFORE #Bf1
BEFORE #Bf2
BEFORE #Bf3
...
BEFORE #Bfy

图 16

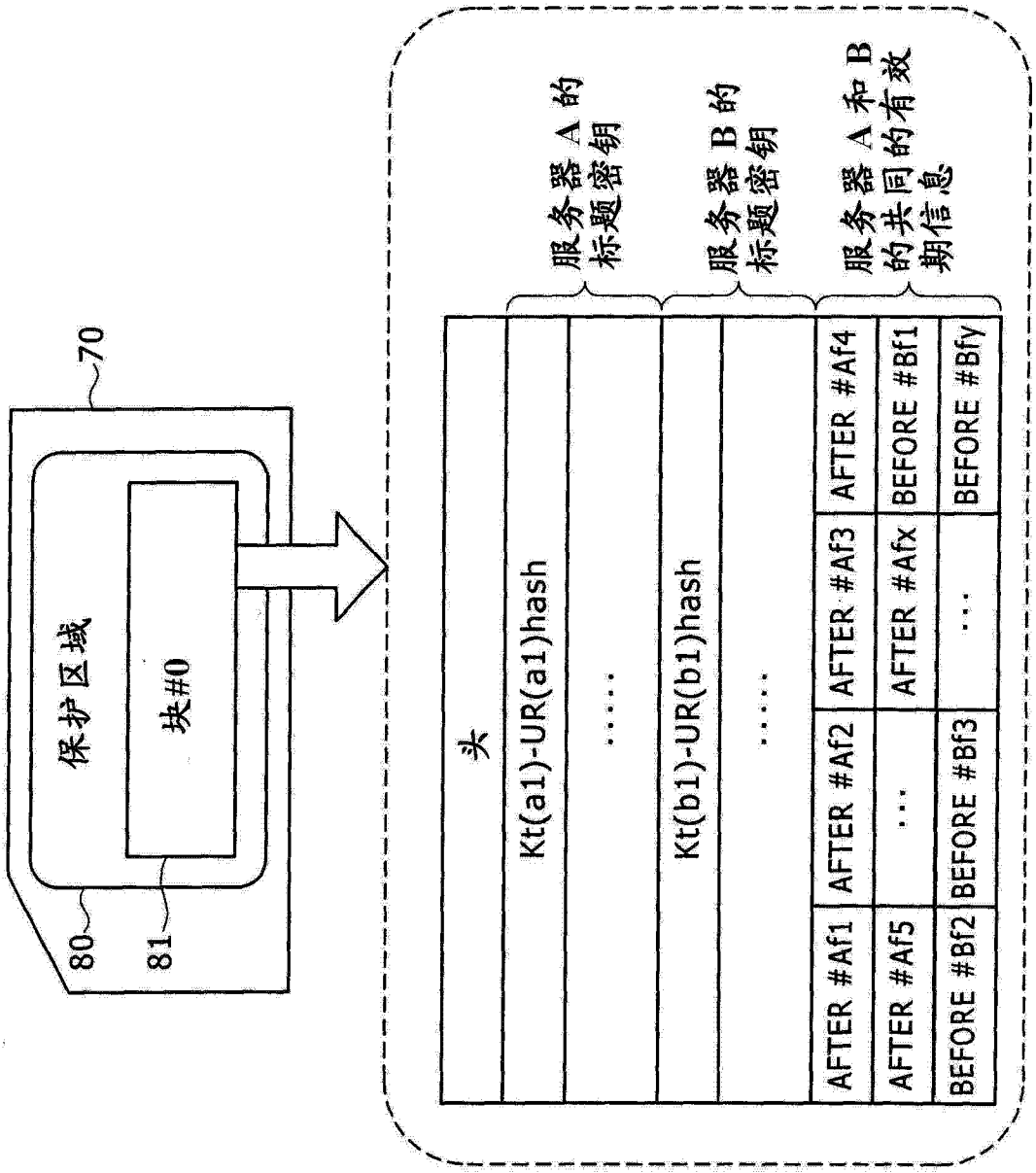

70
保护区域
块#0
80
81
头
Kt(a1)-UR(a1)hash
.....
Kt(b1)-UR(b1)hash
.....
AFTER #Af1
AFTER #Af5
BEFORE #Bf2
AFTER #Af2
...
BEFORE #Bf3
AFTER #Af3
AFTER #Afx
...
AFTER #Af4
BEFORE #Bf1
BEFORE #Bfy
服务器 A 的标题密钥
服务器 B 的标题密钥
服务器 A 和 B 的共同的有效期信息

图 17

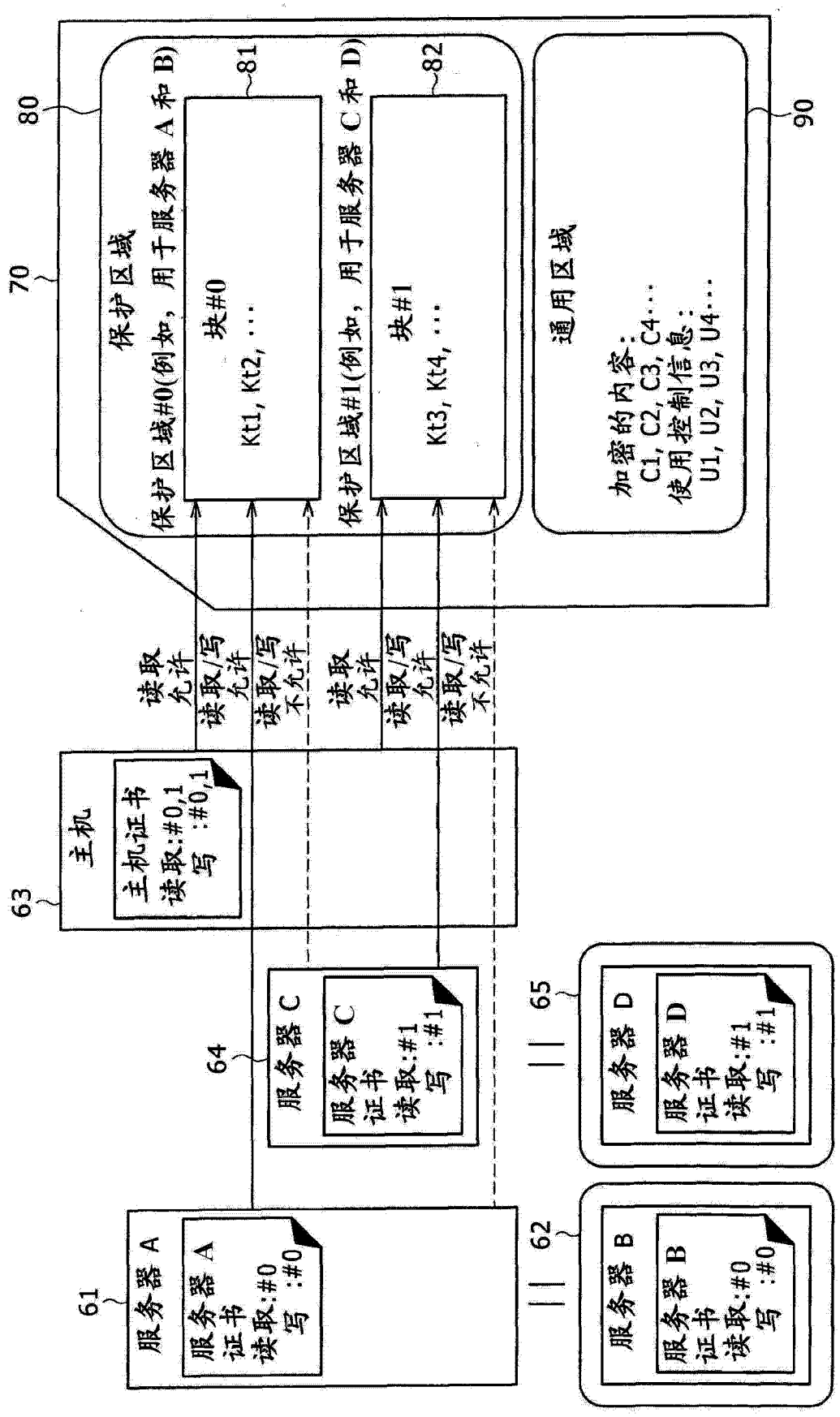
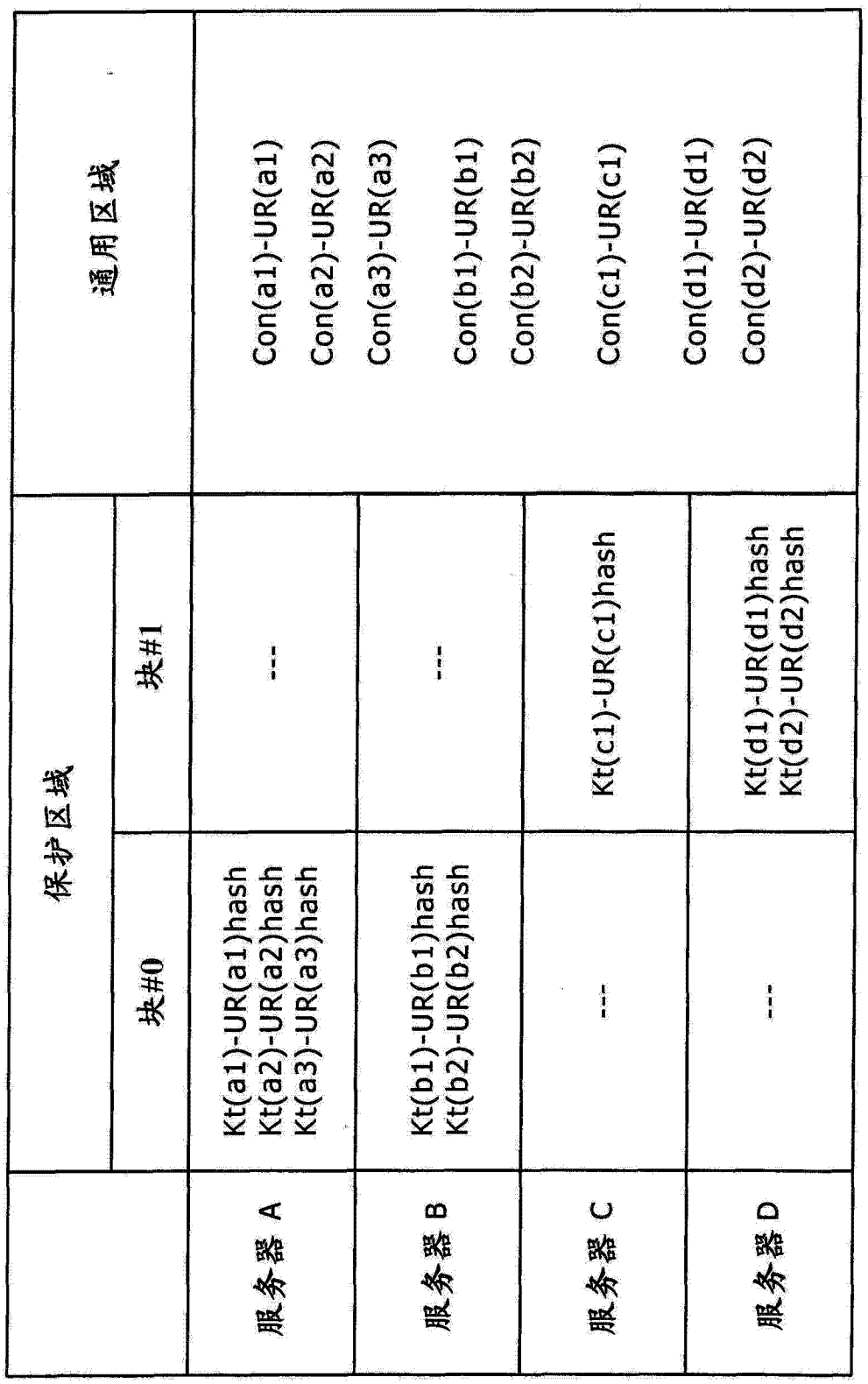

80
保护区域
保护区域#0(例如，用于服务器 A 和 B)
81
块#0
Kt1, Kt2, ···
保护区域#1(例如，用于服务器 C 和 D)
82
块#1
Kt3, Kt4, ···
90
通用区域
加密的内容：
C1, C2, C3, C4···
使用控制信息：
U1, U2, U3, U4···
70
读取
允许
读取/写
允许
读取/写
不允许
读取
允许
读取/写
允许
读取/写
不允许
63
主机
主机证书
读取:#0,1
写 :#0,1
64
服务器 C
服务器 C
证书
读取:#1
写 :#1
65
服务器 D
服务器 D
证书
读取:#1
写 :#1
62
服务器 B
服务器 B
证书
读取:#0
写 :#0
61
服务器 A
服务器 A
证书
读取:#0
写 :#0

图 18


保护区域
块#0
块#1
通用区域
服务器 A
Kt(a1)-UR(a1)hash
Kt(a2)-UR(a2)hash
Kt(a3)-UR(a3)hash

Con(a1)-UR(a1)
Con(a2)-UR(a2)
Con(a3)-UR(a3)
服务器 B
Kt(b1)-UR(b1)hash
Kt(b2)-UR(b2)hash

Con(b1)-UR(b1)
Con(b2)-UR(b2)
服务器 C

Kt(c1)-UR(c1)hash
Con(c1)-UR(c1)
服务器 D

Kt(d1)-UR(d1)hash
Kt(d2)-UR(d2)hash
Con(d1)-UR(d1)
Con(d2)-UR(d2)

图 19

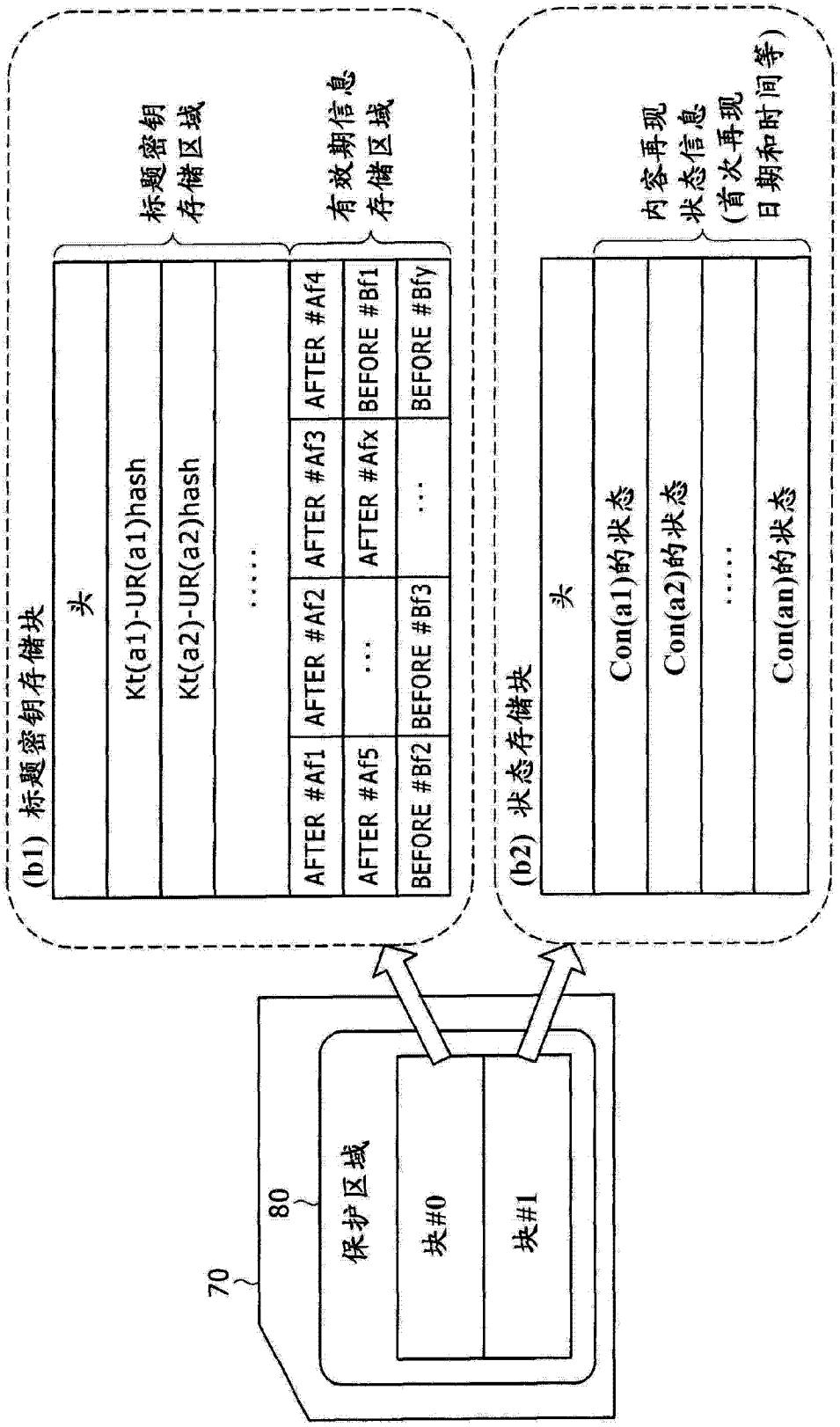

(b1) 标题密钥存储块
头
Kt(a1)-UR(a1)hash
Kt(a2)-UR(a2)hash
.....
AFTER #Af1
AFTER #Af2
AFTER #Af3
AFTER #Af4
AFTER #Af5
...
AFTER #Afx
BEFORE #Bf1
BEFORE #Bf2
BEFORE #Bf3
...
BEFORE #Bfy
标题密钥存储区域
有效期信息存储区域
(b2) 状态存储块
头
Con(a1)的状态
Con(a2)的状态
.....
Con(an)的状态
内容再现状态信息(首次再现日期和时间等)
70
80
保护区域
块#0
块#1

图 20

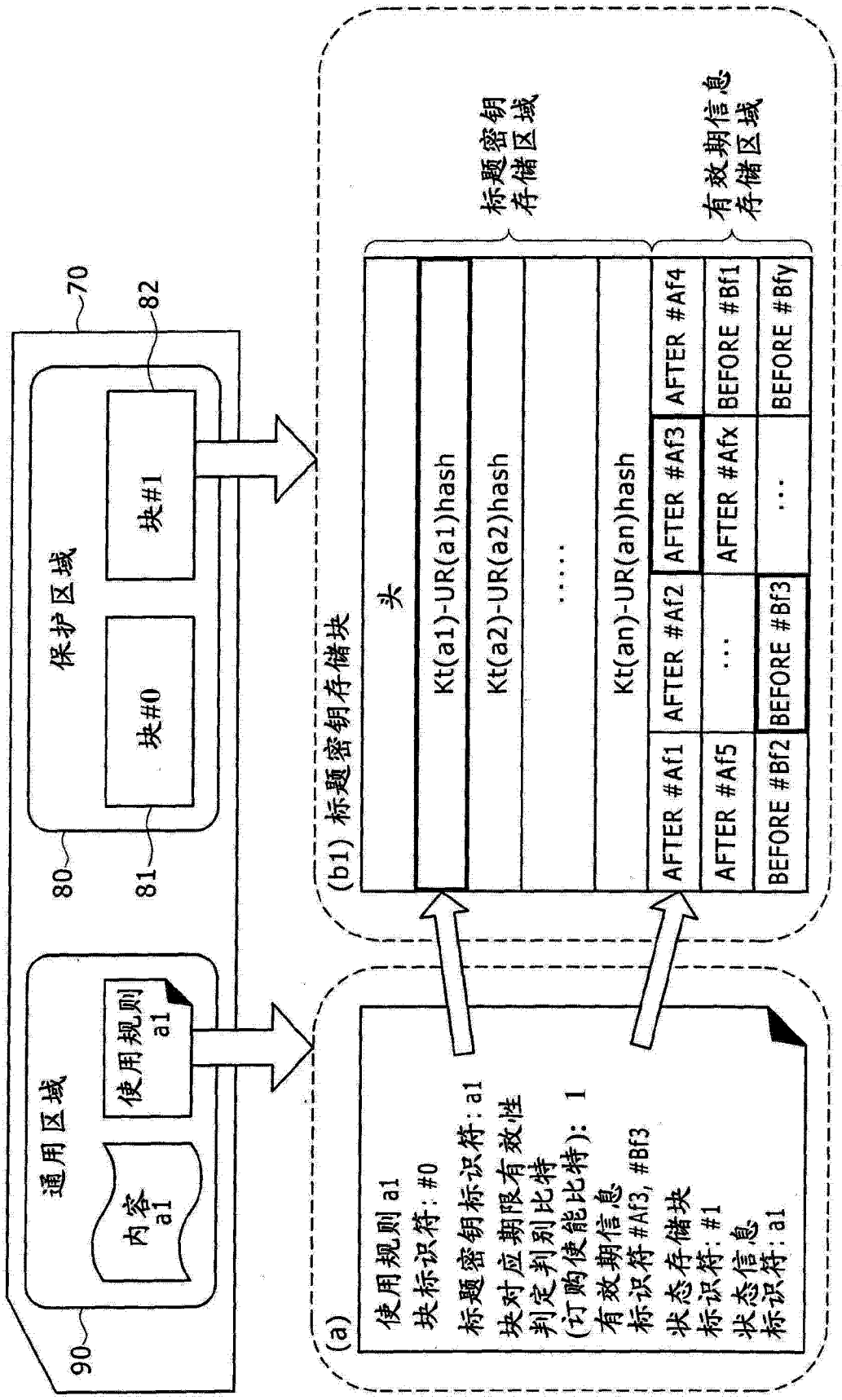

70
82
保护区域
块#1
块#0
80
81
通用区域
使用规则 a1
内容 a1
90
(a)
使用规则 a1
块标识符：#0
标题密钥标识符：a1
块对应期限有效性判定判别比特 (订购使能比特)： 1
有效期信息标识符 #Af3, #Bf3
状态存储块标识符：#1
状态信息标识符：a1
(b1) 标题密钥存储块
头
Kt(a1)-UR(a1)hash
Kt(a2)-UR(a2)hash
.....
Kt(an)-UR(an)hash
标题密钥存储区域
有效期信息存储区域
AFTER #Af1
AFTER #Af5
BEFORE #Bf2
AFTER #Af2
...
BEFORE #Bf3
AFTER #Af3
AFTER #Afx
...
AFTER #Af4
BEFORE #Bf1
BEFORE #Bfy

图 21

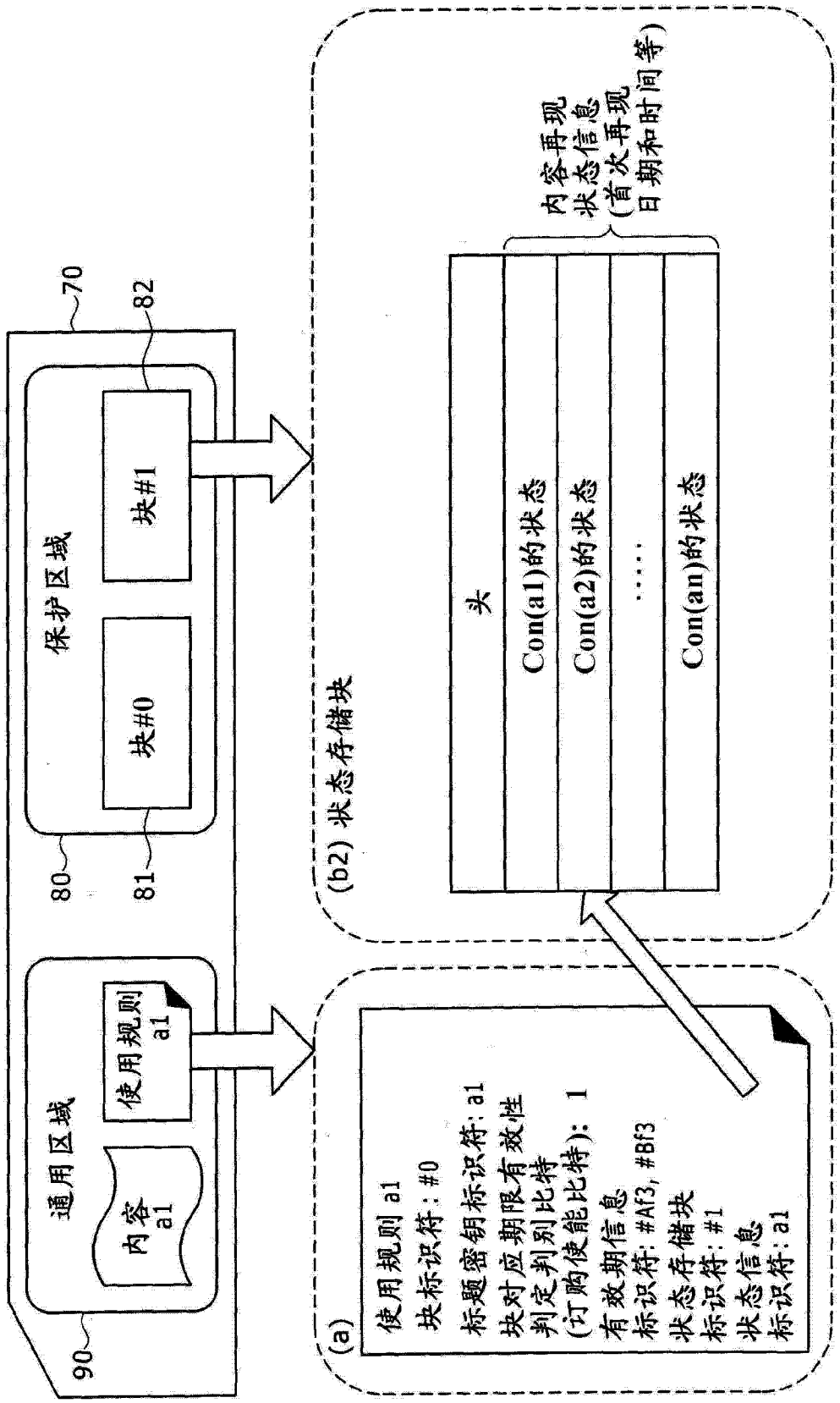

90
通用区域
内容
a1
使用规则
a1
70
保护区域
80
块#0
81
块#1
82
(a)
使用规则 a1
块标识符：#0
标题密钥标识符：a1
块对应期限有效性
判定判别比特
(订购使能比特)：1
有效期信息
标识符：#Af3，#Bf3
状态存储块
标识符：#1
状态信息
标识符：a1
(b2) 状态存储块
头
Con(a1)的状态
Con(a2)的状态
.....
Con(an)的状态
内容再现
状态信息
(首次再现
日期和时间等)

图 22

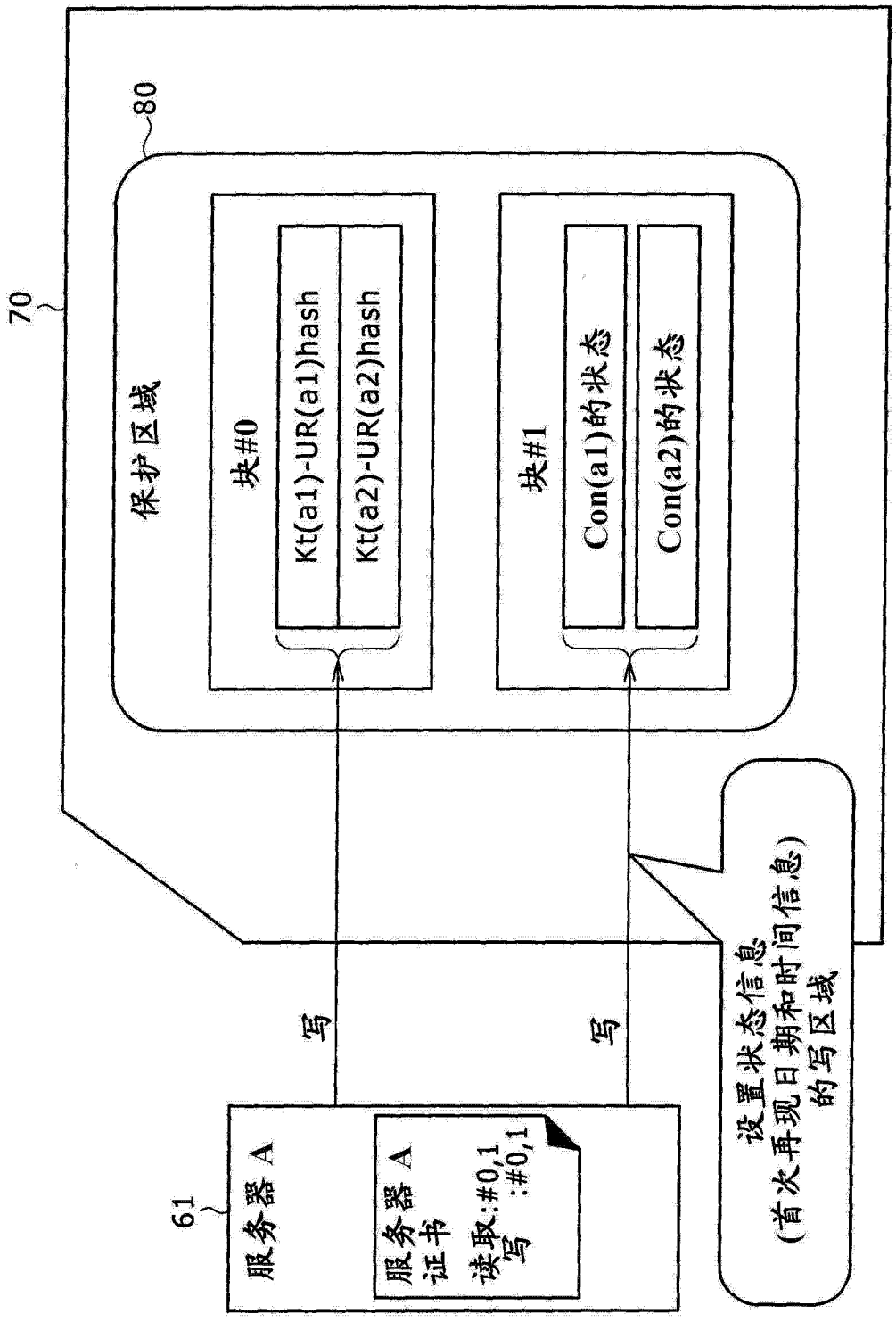

70
80
保护区域
块#0
Kt(a1)-UR(a1)hash
Kt(a2)-UR(a2)hash
块#1
Con(a1)的状态
Con(a2)的状态
写
写
61
服务器 A
服务器 A
证书
读取:#0,1
写 :#0,1
设置状态信息
(首次再现日期和时间信息)
的写区域

图 23

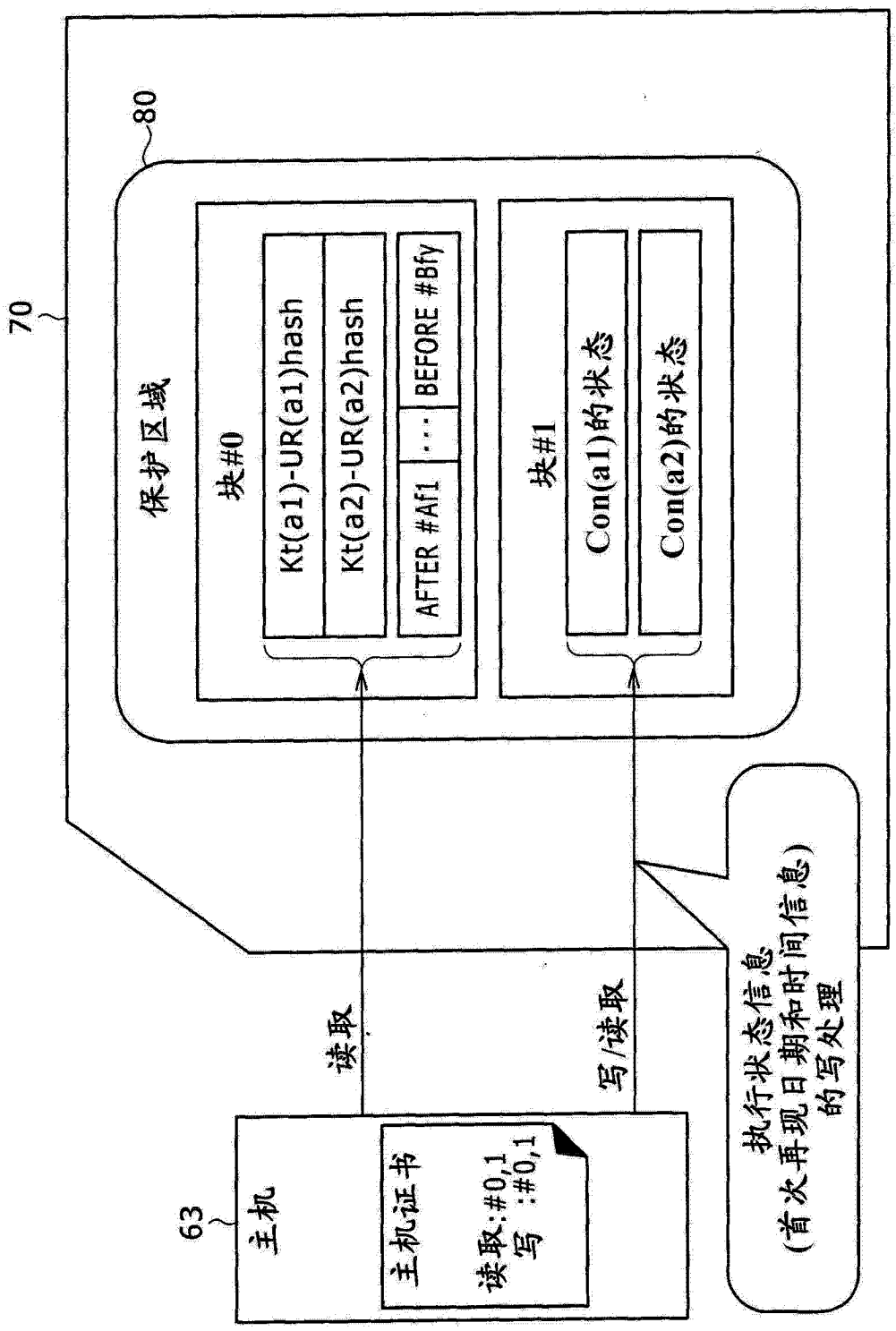

70
80
保护区域
块#0
Kt(a1)-UR(a1)hash
Kt(a2)-UR(a2)hash
AFTER #Af1
···
BEFORE #Bfy
块#1
Con(a1)的状态
Con(a2)的状态
读取
写/读取
63
主机
主机证书
读取:#0,1
写 :#0,1
执行状态信息
(首次再现日期和时间信息)
的写处理

图 24

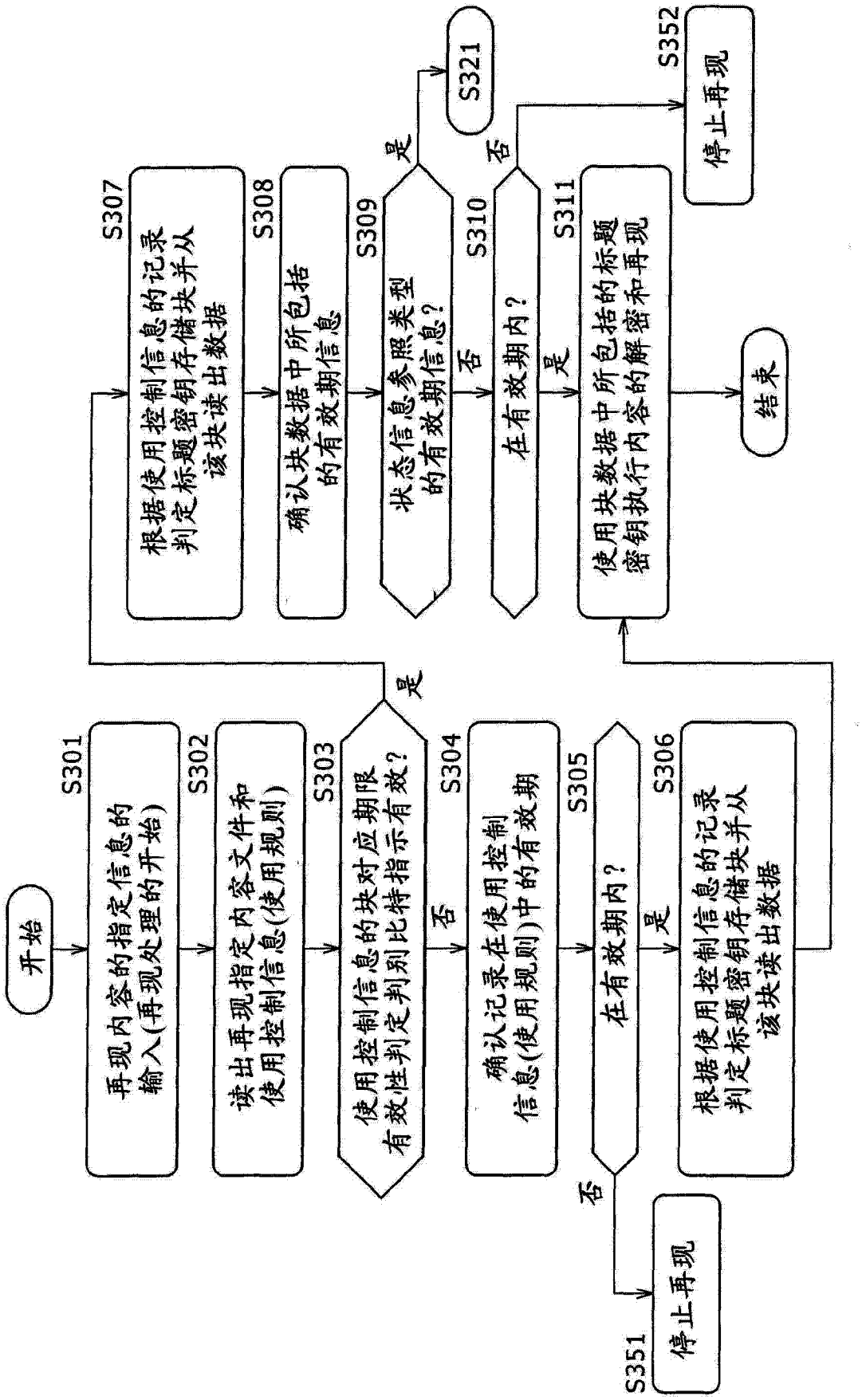

开始
S301
再现内容的指定信息的输入(再现处理的开始)
S302
读出再现指定内容文件和使用控制信息(使用规则)
S303
使用控制信息的块对应期限有效性判定判别比特指示有效?
否
是
S304
确认记录在使用控制信息(使用规则)中的有效期
S305
在有效期内?
否
是
S306
根据使用控制信息的记录判定标题密钥存储块并从该块读出数据
S307
根据使用控制信息的记录判定标题密钥存储块并从该块读出数据
S308
确认块数据中所包括的有效期信息
S309
状态信息参照类型的有效期信息?
是
否
S310
在有效期内?
否
是
S311
使用块数据中所包括的标题密钥执行内容的解密和再现
结束
S321
S351
停止再现
S352
停止再现

图 25

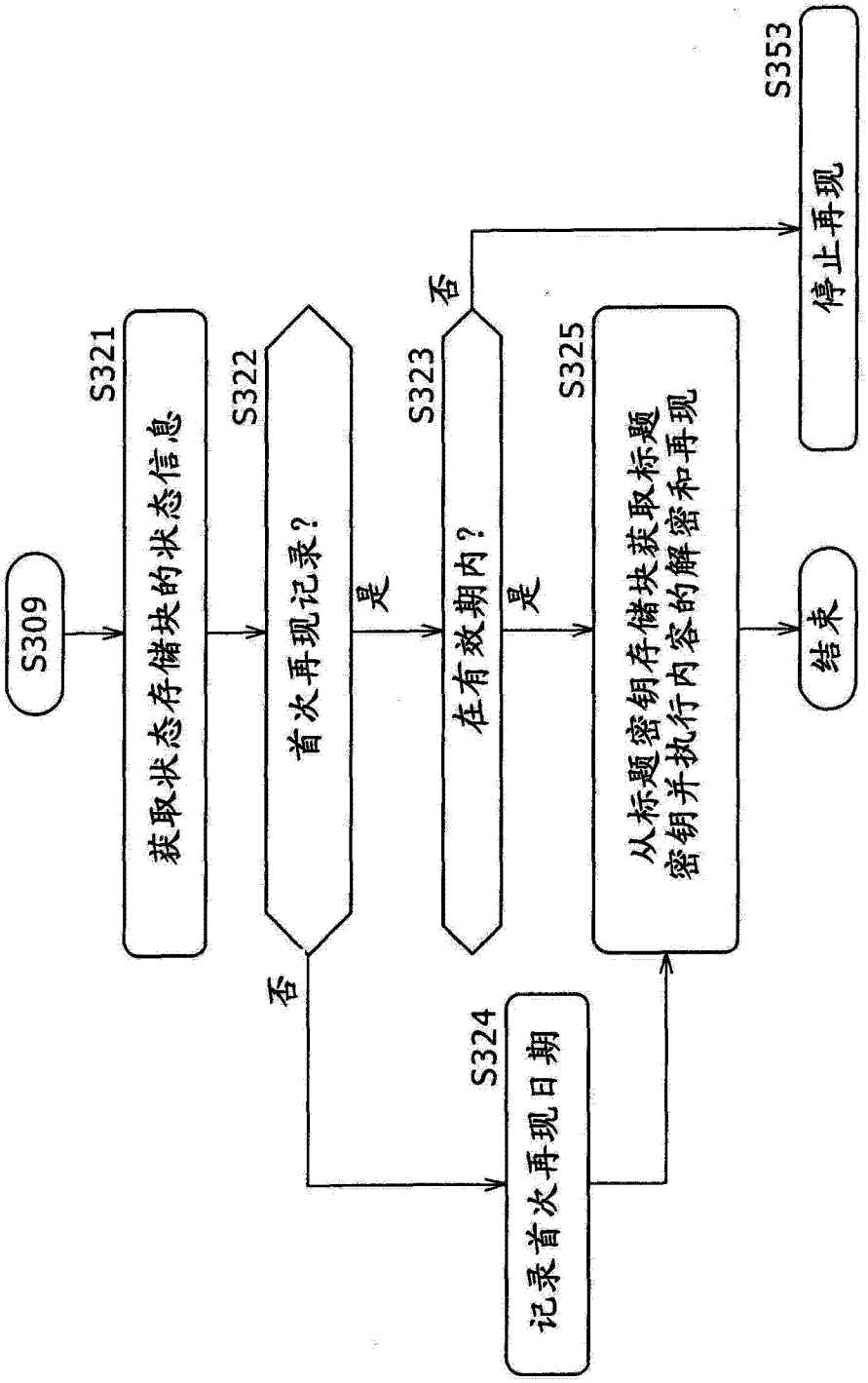

S309
S321
获取状态存储块的状态信息
S322
首次再现记录?
否
是
S323
在有效期内?
否
是
S325
从标题密钥存储块获取标题密钥并执行内容的解密和再现
S353
停止再现
结束
S324
记录首次再现日期

图 26

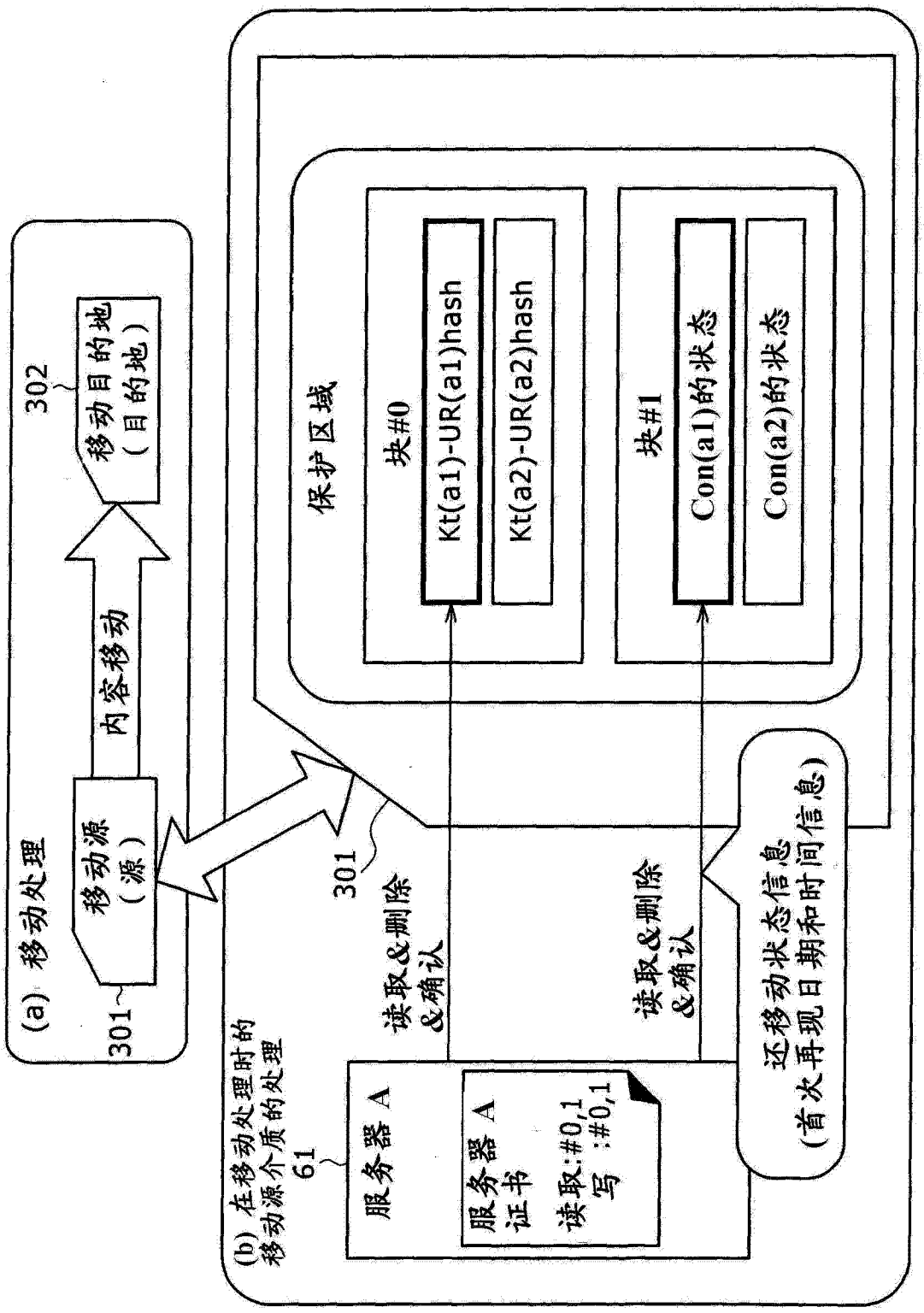

(a) 移动处理
302
移动目的地
（目的地）
内容移动
移动源
（源）
301
(b) 在移动处理时的
移动源介质的处理
61
服务器 A
服务器 A
证书
读取:#0,1
写 :#0,1
301
读取&删除
&确认
读取&删除
&确认
还移动状态信息
(首次再现日期和时间信息)
保护区域
块#0
Kt(a1)-UR(a1)hash
Kt(a2)-UR(a2)hash
块#1
Con(a1)的状态
Con(a2)的状态

图 27

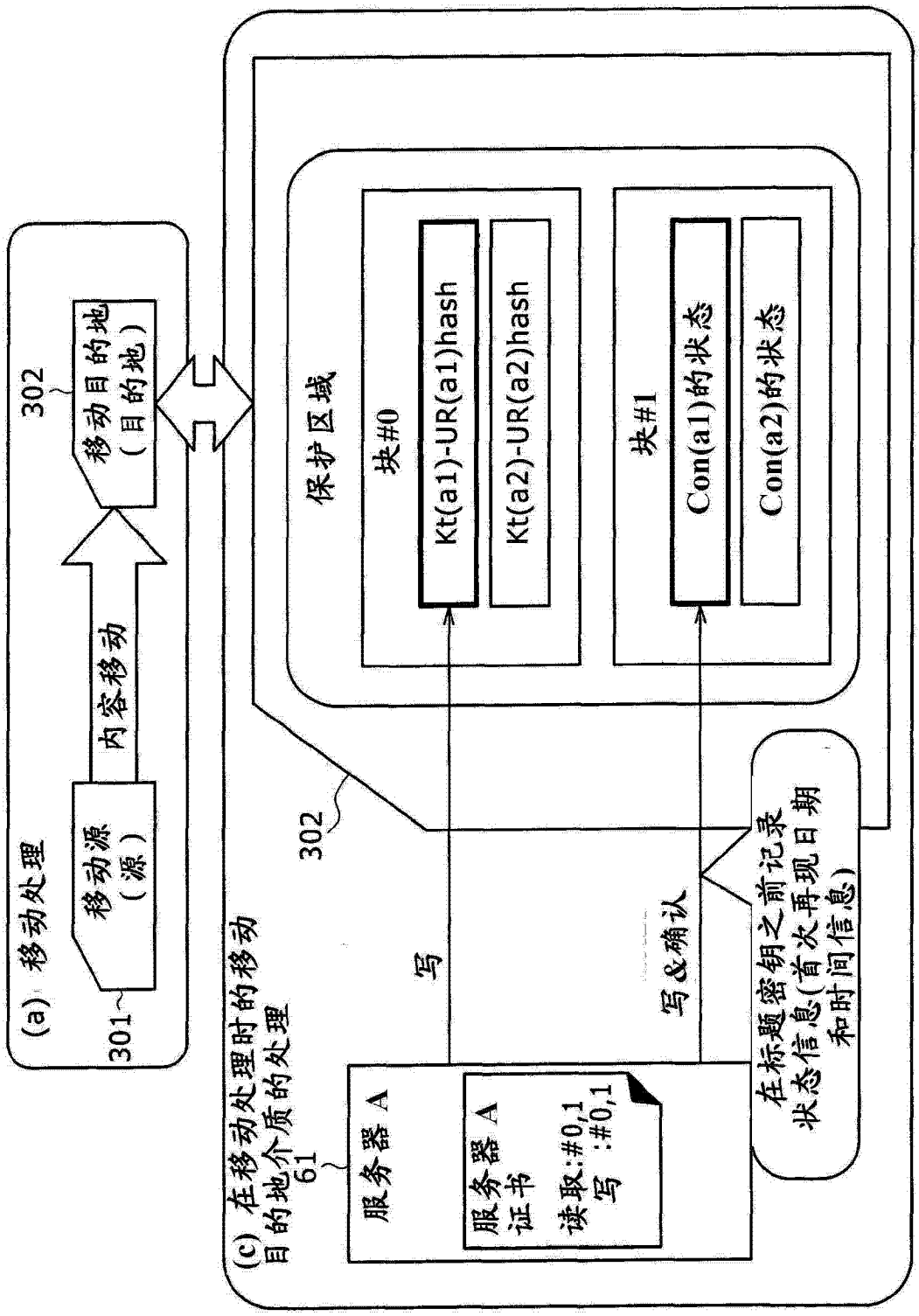

(a) 移动处理
302
移动目的地
（目的地）
内容移动
移动源
（源）
301
(c) 在移动处理时的移动
目的地介质的处理
61
服务器 A
服务器 A
证书
读取:#0,1
写 :#0,1
写
302
保护区域
块#0
Kt(a1)-UR(a1)hash
Kt(a2)-UR(a2)hash
块#1
Con(a1)的状态
Con(a2)的状态
写&确认
在标题密钥之前记录
状态信息(首次再现日期
和时间信息)

图 28

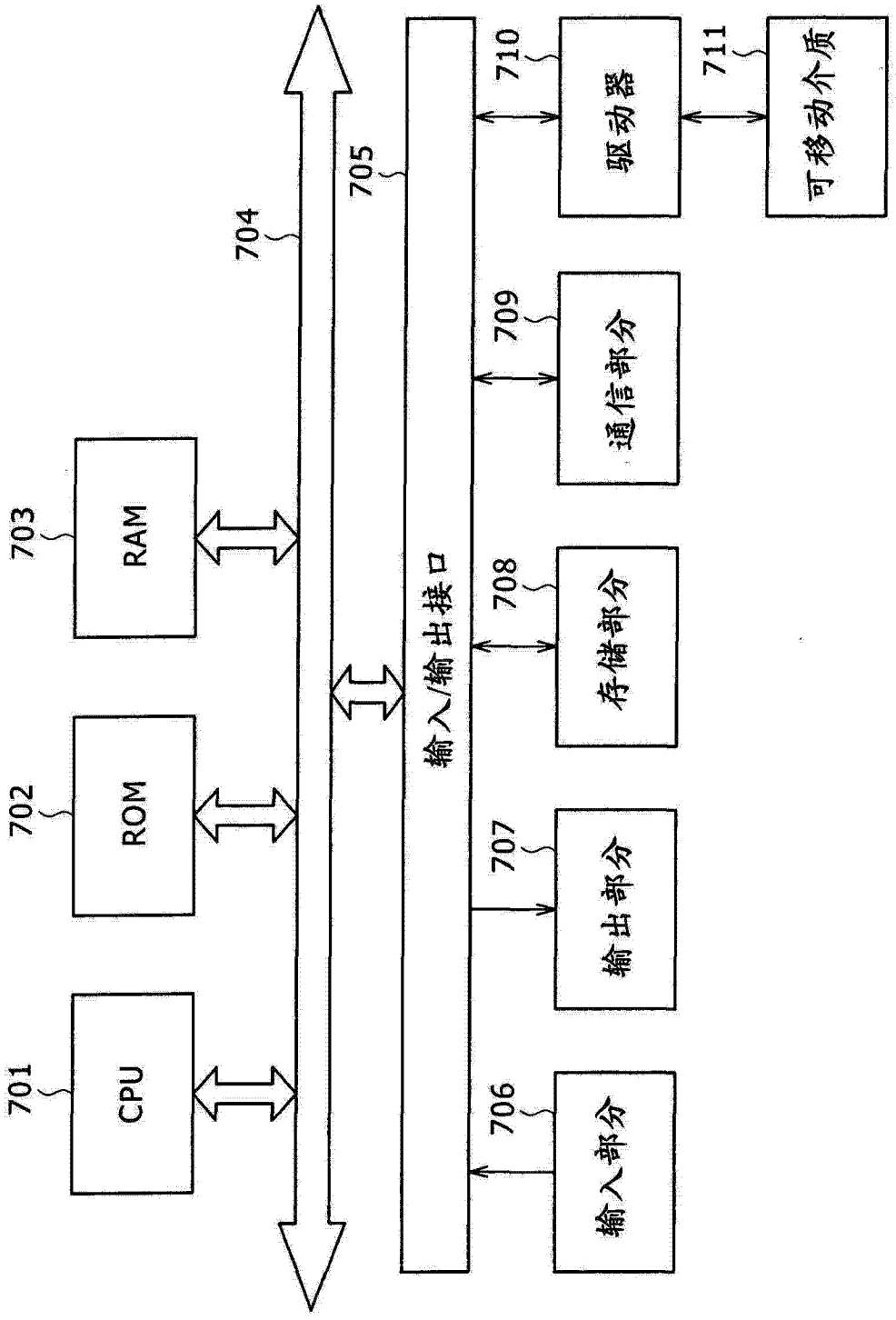

701
CPU
702
ROM
703
RAM
704
705
输入/输出接口
706
输入部分
707
输出部分
708
存储部分
709
通信部分
710
驱动器
711
可移动介质

图 29

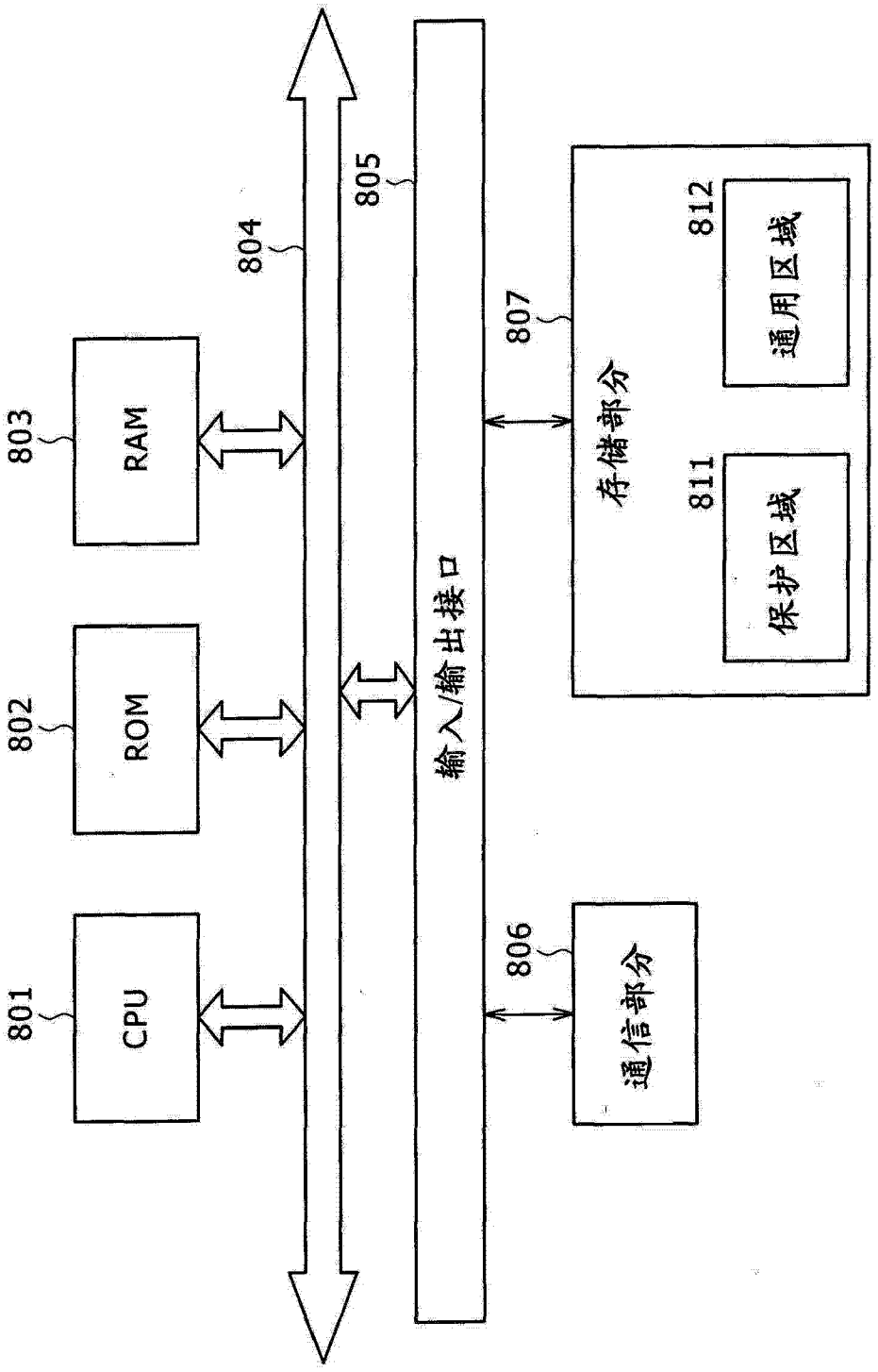

801
CPU
802
ROM
803
RAM
804
805
输入/输出接口
806
通信部分
807
存储部分
811
保护区域
812
通用区域

图 30