(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 102982254 B
(45)授权公告日 2017.06.09

(21)申请号 201210171325.7

(22)申请日 2012.05.29

(65)同一申请的已公布的文献号
申请公布号 CN 102982254 A

(43)申请公布日 2013.03.20

(30)优先权数据
2011-121344 2011.05.31 JP

(73)专利权人 索尼公司
地址 日本东京都

(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 北京市柳沈律师事务所 11105
代理人 郭定辉

(51)Int.Cl.
G06F 21/10(2013.01)
H04L 29/06(2006.01)

(56)对比文件

CN 101243686 A,2008.08.13,说明书第2页第5行至第8页第8行,第9页第4行至第10页第24行,第12页第17-27行,第18页第26行至第19页第6行、图1-6.

CN 101243686 A,2008.08.13,说明书第2页第5行至第8页第8行,第9页第4行至第10页第24行,第12页第17-27行,第18页第26行至第19页第6行、图1-6.

US 2006/0115232 A1,2006.06.01,说明书第[0041]-[0045]段、图4-7.

US 2006/0075228 A1,2006.04.06,说明书第[0090]-[0091]段、图3A-3B,9.

US 2009/0019279 A1,2009.01.15,说明书第[0104],[0208]段.

US 2010/0008509 A1,2010.01.14,全文.

JP 2003-78520 A,2003.03.14,全文.

JP 2005-31895 A,2005.02.03,全文.

审查员 张峰

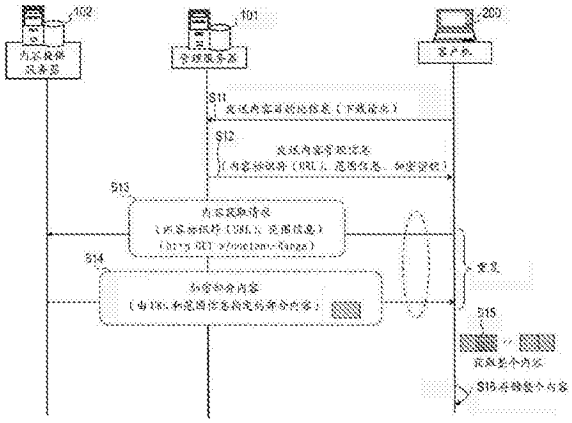
权利要求书3页 说明书18页 附图20页

(54)发明名称

信息处理系统、信息处理装置、信息处理方法和程序

(57)摘要

提供了信息处理系统、信息处理装置、信息处理方法和程序。该信息处理系统包括:客户机,执行内容的获取和再现;管理服务器,向客户机提供应用于获取内容的内容选择信息;以及内容提供服务器,从客户机接收内容选择信息并且提供根据内容选择信息选择的内容,其中内容选择信息包括:内容标识符,作为由不同加密密钥分别加密的加密内容的标识符;以及范围信息,指示作为各个加密内容的配置数据的范围数据的数据区域,以及内容提供服务器向客户机提供通过组合由内容标识符和范围信息指定的作为加密内容的部分数据的范围数据而形成的加密内容。



CN 102982254 B

1.一种信息处理系统,包括:

客户机,执行内容的获取和再现,

管理服务器,向所述客户机提供应用于获取内容的内容选择信息;以及

内容提供服务器,从所述客户机接收所述内容选择信息并且提供根据所述内容选择信息选择的内容,

其中,所述内容选择信息包括:内容标识符,作为利用不同加密密钥分别加密相同内容而获得的加密内容的标识符;以及范围信息,指示作为各个加密内容的配置数据的范围数据的数据区域,以及

所述内容提供服务器向所述客户机提供通过组合作为由所述内容标识符和所述范围信息指定的加密内容的部分数据的范围数据而形成的加密内容。

2.根据权利要求1所述的信息处理系统,

其中,所述内容提供服务器保存由不同加密密钥分别加密的加密内容#1至#n、选择与从所述客户机收到的内容标识符对应的加密内容、且还从所选的加密内容中提取由所述范围信息指定的范围数据以提供给所述客户机。

3.根据权利要求1所述的信息处理系统,

其中,所述内容提供服务器保存每个由根据每个加密内容而不同的一个加密密钥加密的加密内容#1至#n、选择与从所述客户机收到的内容标识符对应的加密内容、且还从所选的加密内容中提取由所述范围信息指定的范围数据以提供给所述客户机。

4.根据权利要求1所述的信息处理系统,

其中,所述内容提供服务器保存由多个不同加密密钥分别加密的加密内容#1至#n、选择与从客户机收到的内容标识符对应的加密内容、且还从所选的加密内容中提取由所述范围信息指定的范围数据以提供给所述客户机。

5.根据权利要求1所述的信息处理系统,

其中,每次相对于所述客户机提供所述内容选择信息的处理中,所述管理服务器产生具有不同内容标识符和范围信息的不同内容选择信息,并且将所述信息提供给所述客户机。

6.根据权利要求1所述的信息处理系统,

其中,所述管理服务器执行产生管理信息并将所述管理信息存储在存储单元中的处理,所述管理信息中提供给所述客户机的内容选择信息与所述内容选择信息已经提供到的客户机的客户机信息相关联。

7.根据权利要求1所述的信息处理系统,

其中,在从所述内容提供服务器收到的内容的再现处理时,所述客户机通过参考范围信息而切换每个范围数据中的加密密钥来执行解密处理。

8.一种信息处理装置,包括

存储单元,存储利用不同加密密钥分别加密相同内容而获得的加密内容#1至#n;

通信单元,从客户机接收作为加密内容的标识符的内容标识符和指示作为各个加密内容的配置数据的范围数据的数据区域的范围信息;以及

数据处理单元,选择通过组合内容标识符和范围信息指定为要提供给所述客户机的数据的、作为加密内容的部分数据的范围数据而形成的加密内容。

9.一种信息处理装置,包括

通信单元,与执行内容的获取和再现的客户机进行通信;以及

数据处理单元,产生并且提供响应于来自所述客户机的内容请求的内容获取的内容选择信息,

其中,在每次相对于所述客户机提供内容选择信息的处理中,所述数据处理单元产生具有不同内容标识符和范围信息的不同内容选择信息,并且将所述信息提供给所述客户机,并且

其中,所述内容标识符作为利用不同加密密钥分别加密相同内容而获得的加密内容的标识符,并且所述范围信息指示作为各个加密内容的配置数据的范围数据的数据区域。

10.根据权利要求9所述的信息处理装置,

其中,所述信息处理装置执行产生管理信息的处理,其中提供给所述客户机的内容选择信息与所述内容选择信息已经提供到的客户机的客户机信息相关联;以及执行将所述信息存储在存储单元中的处理。

11.一种信息处理装置,包括:

通信单元,与内容提供服务器进行通信;以及

数据处理单元,将包括作为利用不同加密密钥分别加密相同内容而获得的加密内容的标识符的内容标识符和指示作为各个加密内容的配置数据的范围数据的数据区域的范围信息的内容选择信息发送到内容提供服务器,从所述内容提供服务器接收通过组合由所述内容标识符和所述范围信息指定的作为加密内容的部分数据的范围数据而形成的加密内容并且将所述内容存储在存储单元中。

12.根据权利要求11所述的信息处理装置,

其中,在从所述内容提供服务器收到的内容的再现处理时,所述数据处理单元通过参考所述范围信息而切换每个范围数据中的加密密钥来执行解密处理。

13.一种在具有存储利用多个不同加密密钥分别加密相同内容而获得的加密内容#1至#n的存储单元的信息处理装置中执行的信息处理方法,所述方法包括:

通过通信单元从客户机接收作为加密内容的标识符的内容标识符和用于指示作为各个加密内容的配置数据的范围数据的数据区域的范围信息;以及

选择通过组合由所述内容标识符和所述范围信息指定的作为加密内容的部分数据的范围数据而形成的加密内容,作为由数据处理单元提供给所述客户机的数据。

14.一种在信息处理装置中执行的信息处理方法,包括:

由数据处理单元产生并且提供响应于来自执行内容的获取和再现的客户机的内容请求而用于内容获取的内容选择信息,

其中,所述数据处理是每次相对于所述客户机提供内容选择信息的处理时,产生具有不同内容标识符和范围信息的不同内容选择信息,并且将所述信息提供给客户机的处理,其中

所述内容标识符作为利用不同加密密钥分别加密相同内容而获得的加密内容的标识符,并且所述范围信息指示作为各个加密内容的配置数据的范围数据的数据区域。

15.一种在信息处理装置中执行的信息处理方法,包括:

将包括作为利用不同加密密钥分别加密相同内容而获得的加密内容的标识符的内容

标识符和指示作为各个加密内容的配置数据的范围数据的数据区域的范围信息的内容选择信息发送到内容提供服务器;以及

从所述内容提供服务器接收通过组合由所述内容标识符和所述范围信息指定的作为加密内容的部分数据的范围数据而形成的加密内容并且将所述内容存储在存储单元中。

信息处理系统、信息处理装置、信息处理方法和程序

技术领域

[0001] 本发明涉及信息处理系统、信息处理装置、信息处理方法和程序，本发明具体地涉及能够防止内容的非授权使用的信息处理系统、信息处理装置、信息处理方法和程序。

背景技术

[0002] 最近几年，广泛采用通过诸如因特网之类的网络的数据通信，并且通过网络广泛地分布大量图像数据、音乐数据等。

[0003] 在诸如音乐数据和图像数据的许多内容中，复制权、分布权等由创建者或者销售者拥有。因此，例如，当服务提供商通过网络从服务器向用户提供服务时，通常进行控制，从而仅允许具有合法使用权的用户使用内容。

[0004] 具体地说，例如，进行控制，以使得作为加密内容发送内容，该加密内容只能利用提供到对内容执行了合法购买处理的用户的加密密钥解密。然而，即使当执行上述控制时，在例如获取了加密内容或者加密密钥的用户解密的内容被非法分布或者公开的情况下，仍发生不确定数量的用户的内容的非授权使用。特别是，最近几年，出现了很多非法公开或者分布数据的情况，并且如何防止这种非授权使用成为一大问题。

[0005] 将参考附图解释非法分布加密密钥和内容的具体示例。

[0006] 图1是示出非法公开加密密钥的示例的示意图。内容提供服务器10对利用加密密钥12执行了合法内容购买过程的客户机A 21和客户机B 22提供应用加密密钥12加密的加密内容11。

[0007] 客户机A 21和客户机B 22可以通过应用加密密钥12对加密密钥11执行解密来进行内容再现。

[0008] 然而，假定客户机B 22例如通过网络在任何人都可以访问的网站上公开加密密钥12。

[0009] 当进行公开密钥的上述处理时，所公开的加密密钥31可能由不确定数量的用户获取。

[0010] 因此，所公开的加密密钥31可以由未执行合法内容购买处理的非授权用户23通过例如网络获取，此外，可以从另一客户机等获得加密内容的副本32，因此，非授权用户23可以通过应用所公开的加密密钥31解密加密内容的副本32，并且再现该内容。

[0011] 如果发生这种情况，则内容的非授权使用将泛滥。

[0012] 在图1所示的示例中，对所有用户提供相同的加密密钥，因此，当一个非法用户泄漏密钥时，利用非法密钥可以解密对其他客户机提供的所有内容。此外，难以确定非法公开密钥的客户机。

[0013] 作为解决该问题的方法，出现了利用不同加密密钥加密对各个客户机提供的加密内容的配置。

[0014] 即，如图2所示，内容提供服务器10利用加密密钥A 14对客户机A 24提供应用加密密钥A 14加密的加密内容。

[0015] 内容提供服务器10利用加密密钥B 15对客户机B 25提供应用加密密钥B 15加密的加密内容。

[0016] 内容提供服务器10利用加密密钥C 16对客户机C 26提供应用加密密钥C 16加密的加密内容。

[0017] 由于应用了上述设置，所以如果因为某种原因加密密钥泄漏，则利用泄漏的密钥解密的内容限于利用泄漏的密钥加密的一个加密内容，并且可以指定泄漏源，即，公开该加密密钥的非法客户机。

[0018] 然而，为了改变每个客户机的加密密钥，内容提供服务器10需要根据每个客户机产生不同的加密密钥，这产生的问题是增加了服务器端的处理负荷。

[0019] 参考图1和图2解释的示例是非法公开和泄漏对内容进行加密/解密处理应用的加密密钥的示例，然而，不仅加密密钥而且解密内容都可能成为非法公开或者泄漏的目标。

[0020] 图3示出解密内容的非法公开的示例。

[0021] 内容提供服务器10将应用加密密钥12加密的解密内容11提供给客户机28。作为合法内容购买处理执行提供处理。

[0022] 然而，当客户机28通过应用加密密钥12解密该加密内容11并且非法公开该解密内容11时，包括图3所示的非授权用户29的不确定数量的用户可以使用非法公开内容33。

[0023] 当解密内容如上所述公开时，解密内容的非授权使用将泛滥，并且即使加密密钥对每个客户机不同，仍难以指定非法公开加密内容的客户机。

发明内容

[0024] 鉴于上述情况，希望提供能够防止内容的非授权使用的信息处理系统、信息处理装置、信息处理方法和程序。

[0025] 还希望提供在不对服务器过度增加处理负荷的情况下能够防止内容的非授权使用的信息处理系统、信息处理装置、信息处理方法和程序。

[0026] 本公开的实施例涉及信息处理系统，包括：客户机，用于执行内容的获取和再现；管理服务器，用于对客户机提供应用于获取内容的内容选择信息；以及内容提供服务器，用于从客户机接收内容选择信息并且提供根据内容选择信息选择的内容，其中内容选择信息包括：内容标识符，作为由不同加密密钥分别加密的加密内容的标识符；以及范围信息，用于指示作为各个加密内容的配置数据的范围数据的数据区域，以及内容提供服务器对客户机提供通过组合作为由内容标识符和范围信息指定的加密内容的部分数据的范围数据而形成的加密内容。

[0027] 在根据本公开实施例的信息处理系统中，内容提供服务器可以保存由不同加密密钥分别加密的加密内容#1至#n、可以选择对应于从客户机收到的内容标识符的加密内容、以及可以进一步从所选加密内容中提取由范围信息指定的要提供到客户机的范围数据。

[0028] 在根据本公开实施例的信息处理系统中，内容提供服务器可以保存每个由根据每个加密内容而不同的一个加密密钥加密的加密内容#1至#n、可以选择对应于从客户机收到的内容标识符的加密内容、以及可以进一步从所选的加密内容中提取由范围信息指定的要提供到客户机的范围数据。

[0029] 在根据本公开实施例的信息处理系统中，内容提供服务器可以保存由多个不同加

密密钥分别加密的加密内容#1至#n、可以选择对应于从客户机收到的内容标识符的加密内容、以及可以进一步从所选加密内容中提取由范围信息指定的要提供到所述客户机的范围数据。

[0030] 在根据本公开实施例的信息处理系统中，在每次对客户机提供内容选择信息的处理中，管理服务器都可以产生具有不同内容标识符和范围信息的不同内容选择信息，并且将该信息提供给客户机。

[0031] 在根据本公开实施例的信息处理系统中，管理服务器执行：产生管理信息的处理，其中提供给客户机的内容选择信息与内容选择信息已经提供到的客户机的客户机信息相关联；以及将该信息存储在存储单元中。

[0032] 在根据本公开实施例的信息处理系统中，在对从内容提供服务器收到的内容执行再现处理时，客户机通过参考范围信息切换每个范围数据中的加密密钥来执行解密处理。

[0033] 本发明的另一实施例涉及信息处理装置，包括：存储单元，用于存储由多个不同加密密钥分别加密的加密内容#1至#n；通信单元，用于从客户机接收作为加密内容的标识符的内容标识符和指示作为各个加密内容的配置数据的范围数据的数据区域的范围信息；以及数据处理单元，用于选择内容标识符和范围信息指定的、通过组合作为加密内容的部分数据的范围数据形成的加密内容作为要提供给客户机的数据。

[0034] 本公开的又一实施例涉及信息处理装置，包括：通信单元，用于与执行内容的获取和再现的客户机进行通信；以及数据处理单元，用于产生并且提供根据来自客户机的内容请求用于获取内容的内容选择信息，其中在每次对客户机提供内容选择信息的处理中，数据处理单元都产生具有不同内容标识符和范围信息的不同内容选择信息，并且将该信息提供给客户机。

[0035] 在根据本公开实施例的信息处理装置中，信息处理装置可以执行：产生管理信息的处理，其中提供给客户机的内容选择信息与内容选择信息已经提供到的客户机的客户机信息相关联；以及将该信息存储在存储单元中。

[0036] 本公开的又一实施例涉及信息处理装置，包括：通信单元，用于与内容提供服务器进行通信；以及数据处理单元，用于将包括作为由不同加密密钥分别加密的加密内容的标识符的内容标识符和指示作为各个加密内容的配置数据的范围数据的数据区域的范围信息的内容选择信息发送到内容提供服务器；从内容提供服务器接收通过组合作为内容标识符和范围信息指定的加密内容的部分数据的范围数据而形成的加密内容；以及将内容存储在存储单元中。

[0037] 在根据本公开实施例的信息处理装置中，在对从内容提供服务器收到的内容执行再现处理时，数据处理单元通过参考范围信息切换每个范围数据中的加密密钥来执行解密处理。

[0038] 本公开的又一实施例涉及在具有用于存储由多个不同加密密钥分别加密的加密内容#1至#n的存储单元的信息处理装置中执行的信息处理方法，该方法包括：通过通信单元从客户机接收作为加密内容的标识符的内容标识符和用于指示作为各个加密内容的配置数据的范围数据的数据区域的范围信息；以及选择通过组合作为由内容标识符和范围信息指定的加密内容的部分数据的范围数据而形成的加密内容，作为由数据处理单元提供给客户机的数据。

[0039] 本公开的又一实施例涉及在信息处理装置中执行的信息处理方法，包括：由数据处理单元产生并且提供响应于来自执行获取和再现内容的客户机的内容请求而应用于获取内容的内容选择信息，并且将该信息提供给客户机，其中，数据处理是在每次对客户机提供内容选择信息的处理中，都产生具有不同内容标识符和范围信息的不同内容选择信息。

[0040] 本公开的又一实施例涉及在信息处理装置中执行的信息处理方法，包括：将包括作为由不同加密密钥分别加密的加密内容的标识符的内容标识符和指示作为各个加密内容的配置数据的范围数据的数据区域的范围信息的内容选择信息发送到内容提供服务器；以及从内容提供服务器接收通过组合作为内容标识符和范围信息指定的加密内容的部分数据的范围数据而形成的加密内容并且将该内容存储在存储单元中。

[0041] 本公开的又一实施例涉及用于使具有用于存储由多个不同加密密钥分别加密的加密内容#1至#n的存储单元的信息处理装置执行信息处理的程序，包括：使信息处理装置通过通信单元从客户机接收作为加密内容的标识符的内容标识符和用于指示作为各个加密内容的配置数据的范围数据的数据区域的范围信息；以及使数据处理单元选择通过组合作为由内容标识符和范围信息指定的加密内容的部分数据的范围数据而形成的加密内容，作为提供给客户机的数据。

[0042] 本公开的又一实施例涉及用于使信息处理装置执行信息处理的程序，包括：使数据处理单元产生并且提供响应于来自执行内容的获取和再现的客户机的内容请求应用于获取内容的内容选择信息，并且将该信息提供给客户机，其中数据处理是在每次对客户机提供内容选择信息的处理中，都产生具有不同内容标识符和范围信息的不同内容选择信息。

[0043] 本公开的又一实施例涉及用于使信息处理装置执行信息处理的程序，包括：使信息处理装置将包括作为由不同加密密钥分别加密的加密内容的标识符的内容标识符和指示作为各个加密内容的配置数据的范围数据的数据区域的范围信息的内容选择信息发送到内容提供服务器；以及使信息处理装置从内容提供服务器接收通过组合作为内容标识符和范围信息指定的加密内容的部分数据的范围数据而形成的加密内容并且将该内容存储在存储单元中。

[0044] 根据本公开实施例的程序是，通过以计算机可读格式提供程序的记录介质或者通信介质，可以提供给例如能够执行各种程序代码的信息处理装置或者计算机系统的程序。以计算机可读格式提供该程序，因此，根据图像处理装置或者计算机系统上的程序实现处理。

[0045] 通过根据后面描述的本公开实施例和附图进行详细解释，本公开的其他特征和优点显而易见。在说明书中将系统定义为多个装置的逻辑集合，并且并不局限于各个配置的装置位于同一外壳内的系统。

[0046] 根据本公开实施例，可以实现能够防止内容的非授权使用的配置。

[0047] 具体地说，对客户机执行提供内容的处理的内容提供服务器对客户机提供通过组合作为内容标识符和范围信息指定的加密内容的部分数据的范围数据而形成的加密内容。包括内容标识符和范围信息的内容选择信息设置为根据每个客户机不同的数据，并且内容选择信息与客户机之间的对应数据登记在数据库中作为管理信息。当发现非法分布内容时，通过分析范围数据，可以指定源客户机，这可以防止内容的非授权使用。

附图说明

[0048] 图1是用于解释因为加密密钥的非法公开的内容的非授权使用的示例的示意图；

[0049] 图2是用于解释因为加密密钥的非法公开的内容的非授权使用的示例的示意图；

[0050] 图3是用于解释因为解密内容的非法公开的内容的非授权使用的示例的示意图；

[0051] 图4是用于解释本公开的概况的示意图；

[0052] 图5是用于解释根据本公开实施例的全部处理序列的时序图；

[0053] 图6是用于解释内容提供服务器的存储数据的示例的示意图；

[0054] 图7A和图7B是用于解释内容提供服务器对客户机提供的数据示例的示意图；

[0055] 图8是用于解释作为内容选择信息的内容标识符和范围信息的图表；

[0056] 图9A和图9B是用于解释内容提供服务器对客户机提供的数据示例的示意图；

[0057] 图10是用于解释作为内容选择信息的内容标识符和范围信息的图表；

[0058] 图11是用于解释由管理服务器产生和保存的管理信息的数据配置示例的图表；

[0059] 图12是用于解释管理服务器的处理序列的流程图；

[0060] 图13是用于解释客户机的数据获取序列的流程图；

[0061] 图14是用于解释客户机的内容再现序列的流程图；

[0062] 图15是用于解释管理服务器的检验非法分布的序列的流程图；

[0063] 图16A和图16B是用于解释内容提供服务器对客户机提供的数据示例的示意图；

[0064] 图17A和图17B是用于解释内容提供服务器对客户机提供的数据示例的示意图；

[0065] 图18是用于解释管理服务器产生并保存的管理信息的数据配置示例的图表；

[0066] 图19是用于解释服务器的硬件配置的示意图；以及

[0067] 图20是用于解释客户机的硬件配置的示意图。

具体实施方式

[0068] 下面将参考附图详细解释根据本公开实施例的信息处理系统、信息处理装置、信息处理方法和程序。根据下面的项进行解释。

[0069] 1.本公开实施例的概况

[0070] 2.内容提供服务器的存储数据和内容提供处理的示例

[0071] 3.管理服务器的管理信息

[0072] 4.从管理服务器到客户机的数据提供处理序列

[0073] 5.客户机中的数据接收和存储处理序列

[0074] 6.客户机中的内容再现序列

[0075] 7.服务器中根据非法分布内容的源确定处理序列

[0076] 8.内容加密的其他配置示例

[0077] 9.各个装置的硬件配置

[0078] 10.本公开的主要配置

[0079] [1.本公开实施例的概况]

[0080] 下面将参考附图详细解释根据本公开实施例的信息处理系统、信息处理装置、信息处理方法和程序。

[0081] 首先，参考图4解释本公开实施例的概况。本公开意在防止内容的非授权使用，当非法分发向各个客户机提供的内容时，其能够确定例如通过网络分发的非法内容的发送源。

[0082] 本公开还有意实现上述配置，而不增加执行内容传送的服务器的处理负荷。

[0083] 在图4中，示出了使用诸如电影或者音乐之类的内容的许多客户机200。客户机200包括各种用户使用的PC、电视机、便携式终端等。

[0084] 这些客户机被配置以通过网络与管理服务器101和内容提供服务器102相连并与其执行通信。

[0085] 对客户机提供内容的处理有各种方法。在下面的实施例中，例如，根据下面描述的处理作为示例对客户机提供内容。

[0086] 管理服务器101是从客户机200接收内容请求的窗口。

[0087] 管理服务器101从客户机接收内容请求，并且将用于获取请求内容的管理信息，例如作为内容标识符的内容URL等发送到客户机200。

[0088] 客户机200利用从管理服务器101收到的内容URL等从内容提供服务器102获取(下载)内容。

[0089] 即，在图4所示的配置中，内容提供服务器102保存内容数据。管理服务器101不保存内容数据，从客户机200接收内容请求，以及对客户机提供客户机200获取内容所需的客户机信息等。

[0090] 内容提供服务器102是形成例如所谓CDN(内容传递网络(Content Delivery Network))的高速缓存服务器(或者边缘服务器(edge server))。内容提供服务器102通过分布到例如各个区域而设置。

[0091] 具体地说，通过分布到诸如欧洲、北美洲、日本和亚洲的各个地址来布置内容提供服务器102，并且内容提供服务器102被配置以从更靠近每个区域内的客户机的内容提供服务器或者从具有较小拥堵的内容提供服务器获取内容。

[0092] 尽管图4中示出了两个内容提供服务器102a和102b，但是除了这两个服务器外，还存在大量内容提供服务器102c、102d、.....。

[0093] 将参考图5所示的时序图解释对客户机的内容提供序列。

[0094] 图5从左侧开始示出用于执行内容提供处理的内容提供服务器102、用于提供内容获取、再现处理等所需的内容管理信息的管理服务器101、以及用于获取用于执行诸如再现的内容使用处理的内容的客户机200。

[0095] 首先，在步骤S11，客户机200将具有希望获取的内容的指定信息的内容请求(下载请求)发送到管理服务器101。

[0096] 管理服务器101通过诸如因特网之类的通信网将诸如内容清单的可以获取的内容的信息提供给客户机200。使用客户机200的用户将该清单显示在客户机200的显示器上。当用户选择特定内容时，选择信息发送到管理服务器101。

[0097] 接着，在步骤S12，当管理服务器101从客户机200收到内容指定信息时，管理服务器101产生包括用于获取指定内容的内容标识符(例如，内容URL)、范围信息以及应用于内容解密的加密密钥的内容管理信息，并且将该信息提供(发送)给客户机200。

[0098] 请注意，范围信息是用于标识包括在该内容中的部分内容的范围的信息，即，包括

部分内容标识信息的信息。

[0099] 通过组合对应于多个范围的多个部分内容来完成整个内容。

[0100] 接着，在步骤S13，客户机200将来自管理服务器101的内容标识符(例如，内容URL)和范围信息发送到内容提供服务器102。具体地说，客户机200根据例如其中执行http1.1限定的[Content-Range(内容范围)]的指定的范围来执行获取部分内容的处理。

[0101] 在步骤S14，根据从客户机200收到的内容请求，内容提供服务器102执行将基于指定范围的部分内容发送到客户机200的处理。

[0102] 从步骤S13到S14的处理重复执行对应于包括在从管理服务器101提供给客户机200的范围信息中的单独范围指定信息的数量的次数。

[0103] 根据该重复处理，客户机200从内容提供服务器102获取对应于多个范围的多个部分内容，以获取整个内容数据。

[0104] 在步骤S16，客户机200将包括对应于多个范围的多个获取的部分内容的内容存储在诸如硬盘的记录介质中。客户机200还与内容一起记录已经从管理服务器101获取的作为对应于存储内容的管理信息的范围信息和加密密钥。

[0105] [2.内容提供服务器的存储数据和内容提供处理的示例]

[0106] 接着，将参考图6和后续附图，描述内容提供服务器的存储数据和内容提供处理的示例。

[0107] 内容提供服务器是用于对客户机提供内容的服务器。

[0108] 正如参考图4和图5所解释的，从客户机输入内容标识符(例如，URL)和范围信息，并且内容提供服务器从对应于要提供给客户机的内容标识符的内容中获取对应于指定范围的部分内容。

[0109] 图6是示出存储在诸如一个内容提供服务器102内的数据库之类的存储单元内的数据的示例的示意图。

[0110] 如图6所示，内容提供服务器102存储多个加密内容(a1)至(an)。

[0111] 全部n条内容都是通过利用不同加密密钥(k1至kn)加密诸如电影之类的要再现的相同内容而获得的加密内容。

[0112] 例如，通过利用存储单元中的n条不同加密密钥(k1至kn)分别加密一个特定电影内容而获得n条加密内容。

[0113] 图6所示的数据仅指示加密内容组(a1)至(an)为对应于一个内容的服务器存储数据，然而，内容提供服务器102存储由多个加密密钥分别加密的多个加密内容，以对应于各个内容。

[0114] 图6所示的数据(a1)至(an)包括下面利用不同加密密钥(k1至kn)相对于一个内容加密的加密内容(#1至#n)。

[0115] (a1)由加密密钥k1加密的第一加密内容#1

[0116] (a2)由加密密钥k2加密的第二加密内容#2

[0117] (a3)由加密密钥k3加密的第三加密内容#3

[0118] (an)由加密密钥kn加密的第n加密内容#n

[0119] 全部n条加密内容#1至#n是通过应用不同加密密钥(k1至kn)对同一个内容加密而获得的内容。

[0120] 图4所示的内容提供服务器102a、102b、.....分别存储图6所示的加密内容(a1)#1至(an)#n。

[0121] 接着，将参考图7A、图7B和图8解释从内容提供服务器提供给客户机的内容的模式。

[0122] 如上参考图5的时序图所解释的，内容标识符(例如，URL)和范围信息从客户机200输入，并且内容提供服务器102从对应于要提供给客户机200的内容标识符的内容中获取对应于指定范围的部分内容。

[0123] 图7A和图7B是用于解释要提供给特定客户机A的内容的示例的示意图。图7A示出内容提供服务器要提供给客户机A的数据，而图7B示出客户机A收到的数据。

[0124] 在图7A的“内容提供服务器提供给客户机A的数据”中显示的多个加密内容(a1)#1至(an)#n中，箭头范围指示根据从客户机A发送到内容提供服务器的范围信息选择的数据。即，加密内容(a1)#1至(an)#n中的箭头范围规定的范围内的部分数据被选择并且提供给客户机A。

[0125] 在图7A所示的示例中，从各个加密内容#1至#n中提取作为规定部分数据的范围数据，并且将它提供给客户机A，如下所述。

[0126] (a1)作为内容的部分数据的范围Ra0至Ra1中的由加密密钥k1加密的第一加密内容#1的范围Ra0至Ra1，

[0127] (a3)范围Ra1至Ra2中的由加密密钥k3加密的第三加密内容#3的范围Ra1至Ra2，

[0128] (an)范围Ra2至Ra3中的由加密密钥kn加密的第n加密内容#n的范围Ra2至Ra31，

[0129] (a1)范围Ra(m-1)至Ram中的由加密密钥k1加密的第一加密内容#1的范围Ra(m-1)至Ram，

[0130] 根据客户机200从管理服务器101收到的并且发送到内容提供服务器102的内容标识符(URL)和范围信息，执行选择部分内容的处理。

[0131] 图8示出客户机A从管理服务器101收到的并且发送到内容提供服务器102的信息的示例。

[0132] 图8所示的内容标识符(URL)和范围信息是对应于图7A的箭头所选的部分内容的数据。

[0133] 如图8所示，客户机A将下面的内容标识符和范围信息发送到内容提供服务器。

[0134] 第一加密内容#1的URL：范围Ra0至Ra1

[0135] 第三加密内容#3的URL：范围Ra1至Ra2

[0136] 第n加密内容#n的URL：范围Ra2至Ra3

[0137] 例如，特定电影内容的整个数据划分为m个范围[(Ra0至Ra1)至(Ra(m-1)至Ram)]，并且内容提供服务器根据从客户机输入的内容标识符(URL)和范围信息选择各个范围数据，并且将该信息提供给客户机。

[0138] 内容提供服务器从客户机A接收图8所示的内容标识符(URL)和范围信息，并且根据要提供给客户机的接收数据执行图7A所示的数据选择。

[0139] 一次执行图5所示时序图中的S13和S14的处理对应于通过发送一个内容标识符(URL)和范围信息选择性地发送一个部分内容的处理。

[0140] 例如，在如图7A所示，在整个内容划分为m个范围的情况下，对每个范围执行步骤

S13和S14的处理，并且通过重复m次处理，客户机可以获得形成一个内容的m个范围(部分内容)的整个数据。

[0141] 因此，客户机A将收到图7B所示的数据。加密内容包括下面的范围数据(部分内容)：

[0142] 第一加密内容#1在范围Ra0至Ra1内

[0143] 第三加密内容#3在范围Ra1至Ra2内

[0144] 第n加密内容#n在范围Ra2至Ra3内

[0145] .....以及

[0146] 第一加密内容#1在范围Ra(m-1)至Ram内。

[0147] 诸如电影的整个加密内容由m条范围数据形成。

[0148] 然而，加密密钥(k1至kn)根据这些内容的每个范围而不同，并且需要通过根据再现内容时的范围切换加密密钥来解码该内容。

[0149] 下面将解释内容再现序列。

[0150] 参考图7A、图7B和图8解释了对客户机A的内容提供处理的示例。范围信息设置为根据每次传递内容，即，根据客户机而不同。

[0151] 内容标识符(URL)和范围信息是图5所述时序图中在步骤S12从管理服务器提供给客户机的信息。

[0152] 该信息提供给各个客户机，在管理服务器中根据每个客户机而不同地设置，并且登记在管理服务器中作为管理信息。

[0153] 图9A、图9B和图10是用于解释对与前面参考图7A、图7B和图8解释的客户机A不同的客户机B执行的内容提供处理和内容选择信息(内容标识符(URL)和范围信息)的示意图。

[0154] 图9A示出内容提供服务器提供给客户机B的数据，而图9B示出客户机以与前面解释的图7A和图7B相同的方式收到的数据。

[0155] 在图9A的“(a)内容提供服务器提供给客户机B的数据”中示出的多个加密内容(a1)#1至(an)#n中，箭头范围指示根据从客户机B发送到内容提供服务器的范围信息而选择的数据。即，加密内容(a1)#1至(an)#n中的箭头范围规定的范围内的部分数据被选择并且提供给客户机B。

[0156] 在图9A所示的示例中，从各个加密内容#1至#n中提取作为规定部分数据的范围数据，并且将它提供给客户机B，如下所述。

[0157] (a1)由加密密钥k1加密的第一加密内容#1的范围Rb0至Rb1是作为内容的部分数据的范围Rb0至Rb1，

[0158] (a2)由加密密钥k2加密的第二加密内容#2的范围Ra1至Ra2是范围Rb1至Rb2，

[0159] (a3)由加密密钥k3加密的第三加密内容#3的范围Rb2至Rb3是范围Rb2至Rb3，

[0160] (a1)由加密密钥kn加密的第n加密内容#n的范围Rb(m-1)至Rbm是范围Rb(m-1)至Rbm。

[0161] 因此，客户机将收到图9B所示的数据。加密内容包括下面的范围数据(部分内容)：

[0162] 第一加密内容#1在范围Ra0至Ra1内

[0163] 第二加密内容#2在范围Ra1至Ra2内

[0164] 第三加密内容#3在范围Ra2至Ra3内

[0165] .....以及

[0166] 第n加密内容#n在范围Rb(m-1)至Rbm内。

[0167] 诸如电影的整个加密内容由m条范围数据形成。

[0168] 通过将图9A、图9B与图7A、图7B进行比较可以看出，图9A、图9B所示的范围数据的选择状态与图7A和图7B所示的选择状态不同。这是因为每个客户机从管理服务器101收到的并且发送到内容提供服务器102的内容选择信息(内容标识符(URL)和范围信息)根据每个客户机而不同。

[0169] 图10示出相对于参考图9A和图9B解释的客户机B应用于内容选择处理的内容选择信息(内容标识符(URL)和范围信息)。

[0170] 如图10所示，客户机B将下面的内容标识符(URL)和范围信息发送到内容提供服务器。

[0171] 第一加密内容#1的URL：范围Rb0至Rb1

[0172] 第二加密内容#2的URL：范围Rb1至Rb2

[0173] 第三加密内容#3的URL：范围Ra2至Ra3

[0174] 从管理服务器接收具有上述设置的内容选择信息，并且将其发送到内容提供服务器。

[0175] 内容管理服务器通过根据从客户机B收到的内容选择信息(内容标识符(URL)和范围信息)选择参考图9A和图9B解释的范围数据来执行内容提取处理，并且将包括提取的范围数据的内容提供给客户机B。

[0176] 如上所述，管理服务器根据来自各个客户机的内容请求设置不同的内容选择信息(内容标识符(URL)和范围信息)，以发送到客户机。

[0177] 内容提供服务器对各个客户机提供包括根据从各个客户机收到的内容选择信息(内容标识符(URL)和范围信息)而具有不同组合的范围数据的内容。

[0178] [3.管理服务器的管理信息]

[0179] 如上所述，管理服务器根据来自各个客户机的内容请求设置要发送到客户机的不同内容选择信息(内容标识符(URL)和范围信息)。

[0180] 管理服务器将要发送到各个客户机的信息保存在存储单元(数据库)中，作为内容管理信息。

[0181] 将参考图11解释管理服务器作为传递内容的管理信息而记录的数据。

[0182] 图11是管理服务器的存储单元内保存的管理信息的数据配置示例。

[0183] 如图11所示，管理信息包括例如下面的信息：

[0184] 传递内容信息，

[0185] 传递目的地信息

[0186] 传递用户信息

[0187] 传递日期信息

[0188] 范围信息，以及

[0189] 传递加密密钥信息。

[0190] 传递内容信息包括诸如内容名称和内容ID之类的信息。

[0191] 传递目的地信息是内容传递目的地的地址的，例如，对应于客户机或者用户的地

址的信息。

[0192] 传递用户信息是诸如用户名、地址和联系地址之类的用户信息。

[0193] 传递日期信息是内容的传递日期的信息。

[0194] 范围信息是其中记录提供给各个客户机的加密内容(#1至#n)和范围的数据。

[0195] 在图11所示的示例中，相对于项(1)的客户机登记下面数据的发送：

[0196] 加密内容(#1)：范围Ra1至Ra2，和Rax至Ray，

[0197] 加密内容(#2)：范围Ra2至Ra3

[0198] 相对于项(2)的客户机登记下面数据的发送：

[0199] 加密内容(#1)：范围Rb1至Rb2，

[0200] 加密内容(#3)：范围Rb2至Rb3，和Rbx至Rby，

[0201] 例如，当发现非法分布的内容时，管理服务器分析包括在非法分布内容中的范围数据，并且利用管理信息检验该数据，从而提取具有相应范围数据模式的项。可以指定提取的项中登记的客户机为非法分布内容的来源。

[0202] 传递加密密钥信息记录应用于各个所提供的内容的加密处理的加密密钥的信息。具体地说，提供给各个客户机的范围数据的组合不同，如参考图7A、图7B和图9A、图9B所解释的，并且解密范围数据所需的加密密钥也根据范围数据的每个组合而不同。因此，提供给各个客户机的加密密钥的组合也不同。因此，例如，当密钥非法分布时，可以利用管理信息的登记信息来检验非法分布密钥的组合，以确定密钥的来源。

[0203] 图11所示的管理信息的示例是一个示例，并且不需要始终记录所有信息。还优选地保存所示信息之外的信息作为管理信息。

[0204] [4.从管理服务器到客户机的数据提供处理序列]

[0205] 接着，将参考图12所示的流程图解释从管理服务器到客户机的数据提供处理序列。

[0206] 根据图12所示的流程执行的处理由管理服务器的数据处理单元执行。根据先前存储在例如存储单元内的程序执行该处理。

[0207] 首先，在步骤S101，从客户机接收下载内容指定信息。

[0208] 内容指定信息是包括例如用户在客户机端根据包括由管理服务器提供的各种电影和音乐的内容列表选择的内容标识符的数据。

[0209] 接着，在步骤S102，管理服务器产生对应于客户机(用户)的范围信息。该范围信息对应于参考图7A、图7B和图9A、图9B解释的作为图11所示管理信息中登记的范围信息的范围信息。

[0210] 即，数据包括提供给与所设置的多个相应加密内容(#1至#n)相关的客户机的部分内容(范围数据)的组合信息，从而对应于该内容。

[0211] 具体地说，例如，产生包括下面的各个加密内容的范围数据的组合的范围信息。

[0212] 加密内容(#1)：范围Ra1至Ra2，Rax至Ray

[0213] 加密内容(#2)：范围Ra2至Ra3，

[0214] 当所有范围数据组合时，可以再现诸如一部电影的整个内容的数据。

[0215] 在步骤S103中，在步骤S103选择对应于要提供给客户机的范围数据的加密密钥。

[0216] 例如，选择与其中设置了在步骤S102选择的范围数据的加密内容(#1至#n)对应的

加密密钥(k1至kn)。

[0217] 接着,在步骤S104,与其中设置在步骤S102选择的范围数据的加密内容(#1至#n)对应的内容标识符(例如,URL),范围信息,即,用于识别范围的数据以及在步骤S103选择的加密密钥发送到客户机。

[0218] 最后,在步骤S105,产生包括内容提供客户机信息、范围信息和加密密钥信息的对应数据的管理信息,以存储在存储单元中。具体地说,产生前面参考图11解释的管理信息,以存储在存储单元中。

[0219] [5.客户机中的数据接收和存储处理序列]

[0220] 接着,将参考图13的流程图解释客户机端执行的处理,即,在客户机从管理服务器和内容提供服务器的数据接收和存储处理序列。

[0221] 在诸如PC的客户机的数据处理单元中执行根据图13所示的流程执行的处理。根据事先存储在存储单元中的程序来执行该处理。

[0222] 首先,在步骤S201,下载内容指定信息发送到管理服务器。

[0223] 内容指定信息是包括例如用户在客户机端根据包括管理服务器提供的各种电影和音乐的内容列表而选择的内容标识符的数据。

[0224] 接着,在步骤S202,从管理服务器接收下面的数据:

[0225] 内容标识信息(URL),

[0226] 范围信息,

[0227] 加密密钥。

[0228] 上面是在步骤S102和S103的处理(作为前面参考图12的流程解释的管理服务器的处理)中管理服务器相对于每个客户机产生的数据,其是根据每个客户机而不同的数据。

[0229] 接着,在步骤S203,客户机将从管理服务器收到的内容选择信息(内容标识符(URL)和范围信息)发送到内容提供服务器,并且接收对应数据。

[0230] 该处理对应于图5所示的时序图的步骤S13至S14的处理。

[0231] 具体地说,参考例如图8和图10解释的内容选择信息(内容标识符(URL)和范围信息)被顺序发送到内容提供服务器并且接收对应数据。

[0232] 接着,在步骤S204,客户机确定对从管理服务器收到的范围信息的所有数据执行的处理是否已经完成。即,客户机确定是否已经从内容提供服务器收到形成内容的所有范围数据。

[0233] 当该处理未完成时,重复执行步骤S203的处理。

[0234] 当确定所有处理已经完成时,该处理进入步骤S205。

[0235] 最后,在步骤S205,客户机集成从内容提供服务器收到的范围数据(部分内容),并且将该数据作为一个内容文件存储在存储单元中。

[0236] 从管理服务器收到的加密密钥和范围信息也存储,从而作为管理数据与内容文件相关联。

[0237] [6.客户机中的内容再现序列]

[0238] 接着,将参考图14所示的流程图解释将内容存储在存储单元中的客户机根据图13所示的流程图执行的内容再现序列。

[0239] 在诸如PC的客户机的数据处理单元中执行根据图14所示的流程执行的处理。例

如，根据先前存储在存储单元中的程序执行该处理。

[0240] 首先，在步骤S301，执行内容再现处理的客户机读取存储在存储单元中的内容文件和范围信息。

[0241] 接着，在步骤S302，客户机根据读取的范围数据从存储单元读取各个范围数据的加密密钥，并且解密该范围数据，从而再现该内容。

[0242] 如图所示，例如，在前面解释的图7B和图9B中，客户机从内容提供服务器收到的内容由包括在诸如电影的内容中的部分内容(范围数据)的组合形成。

[0243] 范围数据的每个范围分别具有根据其中设置了范围数据的加密内容(#1至#n)而不同的加密密钥(k1至kn)。

[0244] 因此，执行内容再现处理的客户机根据每个范围数据执行应用于数据解密的加密密钥的切换。从管理服务器收到的范围信息应用于该处理。

[0245] 在步骤S303，由对应于各个范围数据的加密密钥解密的数据被解码和再现。

[0246] 如上所述，执行内容再现的客户机参考范围信息选择对应于各个范围数据的的加密密钥，从而执行解密和再现处理。

[0247] [7.服务器中根据非法分布内容的源确定处理序列]

[0248] 接着，将参考图15所示的流程图解释发现非法分布内容时执行的源确定处理序列。

[0249] 在例如管理服务器的数据处理单元中执行根据图15的流程执行的处理。

[0250] 首先，在步骤S501，获取非法分布内容。

[0251] 非法分布内容是例如从网络上的任何人都可以访问的网站自由下载的内容、记录在非法分布的盘中的复制内容等。

[0252] 接着，在步骤S502，通过分析非法分布内容，分析形成内容的范围数据的步骤。

[0253] 接着，在步骤S503，利用记录在管理信息中的范围信息检验从非法分布内容获取的范围数据步骤信息，以确定作为非法分布内容的分布源的内容传递目的地客户机。

[0254] 该管理信息指示前面解释的图11所示的管理信息。

[0255] 在图15所示的流程中，解释了根据非法分布内容分析范围数据布置的处理的示例。通过利用图11所示的管理信息中的登记信息检验非法分布的一组密钥，可以执行发现非法分布密钥源的处理。

[0256] [8.内容加密的其他配置示例]

[0257] 在前面解释的示例中，如例如图7A、图7B和图9A、图9B所示，解释了通过在诸如电影的特定内容的整个内容中设置应用多个不同密钥(k1至kn)的加密内容(#1至#n)，而执行处理的示例。

[0258] 即，在上面描述的示例中，加密内容是通过利用一个加密密钥对整个内容加密而获得的内容。

[0259] 加密配置可能更复杂，并且还优选地将一个加密内容#x设置为应用多个加密密钥的数据的组合。

[0260] 将参考图16A、图16B和后续附图解释处理示例。

[0261] 图16A示出内容提供服务器保存并且提供给客户机A的数据，而图16B示出客户机A以图7A、图7B和图9A、图9B所示的上述实施例中解释的方式相同的方式收到的数据。

[0262] 图16A所示的“内容提供服务器保存并且提供给客户机A的数据”中示出的多个加密内容(a1)#1至(an)#n具有其中在各个部分数据中由多个加密密钥加密一个加密内容(#x)的配置，该配置与前面参考图7A、图7B和图9A、图9B解释的加密内容(a1)#1至(an)#n的配置不同。

[0263] 例如：

[0264] (a1)加密内容#1是由各个部分内容中由加密密钥k11至k1n执行加密的加密数据的组合形成的。

[0265] (a2)加密内容#2是由各个部分内容中由加密密钥k21至k2n执行加密的加密数据的组合形成的。

[0266] 因此，在本实施例中，每个加密内容(#x)都是应用多个加密密钥的加密数据的组合。

[0267] 此外，在该处理示例中，客户机从管理服务器接收与上述实施例类似的数据，即：

[0268] 内容标识符(URL)，

[0269] 范围信息，以及

[0270] 加密密钥。

[0271] 在该示例中，增加了从管理服务器提供给客户机的加密密钥的数量。

[0272] 关于从客户机发送到内容提供服务器的内容选择信息(内容标识符(URL)和范围信息)执行与前面解释的处理相同的处理，并且以与上述实施例相同的处理执行此后由内容提供服务器执行的内容选择。

[0273] 例如，图16A中的箭头范围指示根据从客户机A发送到内容发送服务器的范围信息选择的数据。即，加密内容(a1)#1至(an)#n中箭头范围规定的范围内的部分数据被选择并且提供给客户机A。

[0274] 在图16A所示的示例中，从各个加密内容#1至#n中提取作为规定部分数据的范围数据，并且将其提供给客户机A，如下所述。

[0275] (a1)作为内容的部分数据的范围Ra0至Ra1中，由加密密钥k11加密的第一加密内容#1的加密数据，

[0276] (a2)范围Ra1至Ra2中，由加密密钥k21加密的第二加密内容#2的加密数据和由加密密钥k22加密的加密数据。

[0277] 因此，客户机A收到的数据是图16B所示的数据。

[0278] 图17A和图17B示出与图16A和图16B不同的相对于客户机B的处理示例。

[0279] 即，图17A示出内容提供服务器保存并且提供给服务器B的数据，而图17B示出客户机B收到的数据。

[0280] 加密内容(a1)#1至(an)#n与图16A所示的加密内容相同，具有在各个部分数据中由多个加密密钥加密一个加密数据(#x)的配置。

[0281] 例如，图17A所示的箭头范围指示根据从客户机B发送到内容发送服务器的范围信息选择的数据。即，加密内容(a1)#1至(an)#n中的箭头范围规定的范围内的部分数据被选择并且发送到客户机B。

[0282] 在图17A所示的示例中，部分数据规定的范围数据是从各个加密内容#1至#n中提取的，并且提供给客户机B，如下所述。

[0283] (a1)作为内容的部分数据的范围Ra0至Ra1中，由加密密钥K11加密的第一加密内容#1的加密数据和由加密密钥k12加密的加密数据，

[0284] (a2)范围Ra1至Ra2中，由加密密钥k22加密的第二加密内容#2的加密数据和由加密密钥k23加密的加密数据

[0285] 因此，客户机B收到的数据是图17B所示的数据。

[0286] 在该实施例中，即使在一个范围数据中，客户机解密内容也需要多个密钥。因此，包括密钥切换位置信息的范围信息从管理服务器提供给客户机，然后，客户机参考该范围信息进行密钥切换，并且当执行再现处理时解密并再现该内容。

[0287] 图18是用于解释在处理示例中管理服务器要作为传递内容的管理信息记录的数据的图表。

[0288] 图18示出保存在管理服务器的存储单元内的管理信息的数据配置示例。

[0289] 如图18所示，管理信息包括例如下面信息：

[0290] 传递内容信息，

[0291] 传递目的地信息，

[0292] 传递用户信息，

[0293] 传递日期信息，

[0294] 范围信息，以及

[0295] 传递加密密钥信息。

[0296] 该设置与在上述实施例中解释的图11所示的管理信息相同。

[0297] 传递内容信息包括诸如内容名称和内容ID的信息。

[0298] 传递目的地信息是内容传递目的地的地址，例如，对应于客户机或者用户的地址的信息。

[0299] 传递用户信息是诸如用户名、地址和联系地址的用户信息。

[0300] 传递日期信息是内容的传递日期的信息。

[0301] 范围信息是其中记录提供给各个客户机的加密内容(#1至#n)和范围的数据。

[0302] 在图18所示的示例中，相对于项(1)的客户机登记下面数据的发送：

[0303] 加密内容(#1)：范围Ra1至Ra2，和Rax至Ray，

[0304] 加密内容(#2)：范围Ra2至Ra3

[0305] 相对于项(2)的客户机登记下面数据的发送：

[0306] 加密内容(#1)：范围Rb1至Rb2，

[0307] 加密内容(#3)：范围Rb2至Rb3，和Rbx至Rby，

[0308] 在该示例中，传递解密密钥信息与参考图11解释的上述管理信息不同，并且登记了更多的密钥信息。

[0309] 例如，当发现非法分布内容时，管理服务器分析包括在非法分布内容中的范围数据，并且利用管理信息检验该数据，从而提取具有相应范围数据模式的项。可以将提取的项中登记的客户机指定为非法分布内容的来源。

[0310] 还可以利用管理信息中登记的传递加密密钥信息检验非法分布密钥的组合，从而指定非法分布密钥的来源。

[0311] [9.各个装置的硬件配置]

[0312] 最后，将参考图19和图20解释执行上述处理的各个装置的硬件配置的示例。

[0313] 首先，将参考图19解释用于执行管理信息处理和内容提供处理的服务器的硬件配置的示例。

[0314] CPU(中央处理单元)601用作用于根据ROM(只读存储器)602或者存储单元608内存储的程序执行各种处理的数据处理单元。

[0315] 例如，CPU 601执行在上述各实施例中解释的加密内容的生成处理、内容提供处理、管理信息的创建/记录处理等。在RAM(随机存取存储器)603中，适当地存储CPU 601执行的程序和数据。CPU 601、ROM 602和RAM 603通过总线604互连。

[0316] 通过总线604，CPU 601连接到输入/输出接口605，并且包括各种开关、键盘、鼠标、麦克风等的输入单元606和包括显示器、扬声器等的输出单元607连接到输入/输出接口605。CPU 601响应于从输入单元606输入的指令执行各种处理，并且将处理结果输出到例如输出单元607。

[0317] 连接到输入/输出接口605的存储单元608包括例如硬盘等，用于存储CPU 601执行的程序和各种数据。例如，记录加密内容、管理信息等。

[0318] 通信单元609通过诸如因特网和局域网之类的网络与外部装置进行通信。

[0319] 接着，将参考图20解释用于对内容执行接收和再现处理的客户机装置的硬件配置的示例。

[0320] CPU(中央处理单元)701用作用于根据RAM(只读存储器)702或者存储单元708内存储的程序执行各种处理的数据处理单元。

[0321] 例如，CPU 701执行与服务器的通信处理、从服务器发送到存储单元708(硬盘等)的接收数据的记录处理、存储单元708(硬盘等)中的数据的再现处理。

[0322] 在RAM(随机存取存储器)703中，适当地存储CPU 701执行的程序和数据。CPU 701、ROM 702和RAM 703通过总线704互连。

[0323] CPU 701通过总线704连接到输入/输出接口705，并且包括各种开关、键盘、鼠标、麦克风等的输入单元706和包括显示器、扬声器等的输出单元707连接到输入/输出接口705。CPU 701响应于从输入单元706输入的指令执行各种处理，并且将处理结果输出到例如输出单元707。

[0324] 连接到输入/输出接口705的存储单元708包括例如硬盘等，用于存储CPU 701执行的程序和各种数据。通信单元709通过诸如因特网和局域网的之类网络与外部装置进行通信。

[0325] 连接到输入/输出接口705的驱动器710驱动诸如磁盘、光盘、磁光盘或者半导体存储器之类的可拆卸介质711，用于获取所记录的诸如内容和程序的各种数据。

[0326] [10.本公开的主要配置]

[0327] 如上所述，参考具体示例详细描述了本公开的配置。然而，本领域技术人员明白，可以对实施例进行修改或者替换，而不脱离本公开的要旨。即，作为举例说明披露了本公开，并且不应当以受限方式理解它。要确定本公开的要旨，应当考虑所附权利要求书。

[0328] 根据本公开的技术可以由下面的配置予以实现。

[0329] (1)一种信息处理系统，包括：

[0330] 客户机，执行内容的获取和再现，

[0331] 管理服务器，向客户机提供应用于获取内容的内容选择信息，以及

[0332] 内容提供服务器，从客户机接收内容选择信息并提供根据内容选择信息选择的内容，

[0333] 其中，内容选择信息包括：内容标识符，作为由不同加密密钥分别加密的加密内容的标识符；以及范围信息，指示作为各个加密内容的配置数据的范围数据的数据区域，以及

[0334] 内容提供服务器向客户机提供通过组合作为由内容标识符和范围信息指定的加密内容的部分数据的范围数据而形成的加密内容。

[0335] (2)根据上述(1)所述的信息处理系统，

[0336] 其中，内容提供服务器保存由不同加密密钥分别加密的加密内容#1至#n、选择与从客户机收到的内容标识符对应的加密内容、以及进一步从所选的加密内容中提取由范围信息指定的范围数据以提供给客户机。

[0337] (3)根据上述(1)或者(2)所述的信息处理系统，

[0338] 其中，内容提供服务器保存每个由根据每个加密内容而不同的一个加密密钥加密的加密内容#1至#n、选择与从客户机收到的内容标识符对应的加密内容、以及进一步从所选的加密内容中提取由范围信息指定的范围数据以提供给客户机。

[0339] (4)根据上述(1)或者(2)所述的信息处理系统，

[0340] 其中，内容提供服务器保存由多个不同加密密钥分别加密的加密内容#1至#n、选择与从客户机收到的内容标识符对应的加密内容、以及进一步从所选的加密内容中提取由范围信息指定的范围数据以提供给客户机。

[0341] (5)根据上述(1)至(4)中的任何一项所述的信息处理系统，

[0342] 其中，在每次相对于客户机提供内容选择信息的处理中，管理服务器产生具有不同内容标识符和范围信息的不同内容选择信息，并且将该信息提供给客户机。

[0343] (6)根据上述(1)至(5)中的任何一项所述的信息处理系统，

[0344] 其中，管理服务器执行产生管理信息的处理，其中提供给客户机的内容选择信息与内容选择信息已经提供到的客户机的客户机信息相关联；以及将该信息存储在存储单元中的处理。

[0345] (7)根据上述(1)至(6)中的任何一项所述的信息处理系统，

[0346] 其中，在从内容提供服务器收到的内容的再现处理时，客户机通过参考范围信息切换每个范围数据中的加密密钥来执行解密处理。

[0347] 此外，包括在上述系统中的各个装置、各个装置中执行的处理方法以及执行处理的程序包括在本公开的配置中。

[0348] 说明书中解释的一系列处理可以由硬件/软件、硬件和软件的复合配置执行。当利用软件执行处理时，可以将记录了处理序列的要执行的程序安装在并入专用硬件的计算机的存储器中，也可以将要执行的程序安装在可以执行各种处理的通用计算机中。例如，可以事先将程序记录在记录介质中。除了将程序从记录介质安装到计算机中，可以通过诸如LAN(局域网)或者因特网的网络下载程序，并且将它安装在诸如内部硬盘的记录介质中。

[0349] 此外，说明书中描述的各种处理不仅可以以根据描述的时间顺序执行，而且可以根据执行处理的装置的处理能力或者根据需要并行执行或者单独执行。说明书中将系统定义为多个装置的逻辑集合，并且并不局限于各种配置的装置位于同一外壳内的系统。

[0350] 如上所述，根据本公开实施例，可以实现能够防止内容的非授权使用的配置。

[0351] 具体地说，对客户机执行提供内容处理的内容提供服务器向客户机提供通过组合作为由内容标识符和范围信息指定的加密内容的部分数据的范围数据而形成的加密内容。包括内容标识符和范围信息的内容选择信息根据每个客户机设置为不同的数据，并且内容选择信息与客户机之间的对应数据登记在数据库中，作为管理信息。当发现非法分布的内容时，可以指定源客户机，这样可以防止内容的非授权使用。

[0352] 本公开含有与于2011年5月31日向日本专利局提交的第JP2011-121344号日本优先权专利申请公开的主题有关的主题，在此通过引用包括该专利申请的全部内容。

[0353] 本技术领域内的技术人员应当明白，根据设计要求和其他因素，可以设想各种修改、组合、部分组合和变型，然而，它们均落入所附权利要求书或者其等同的范围内。

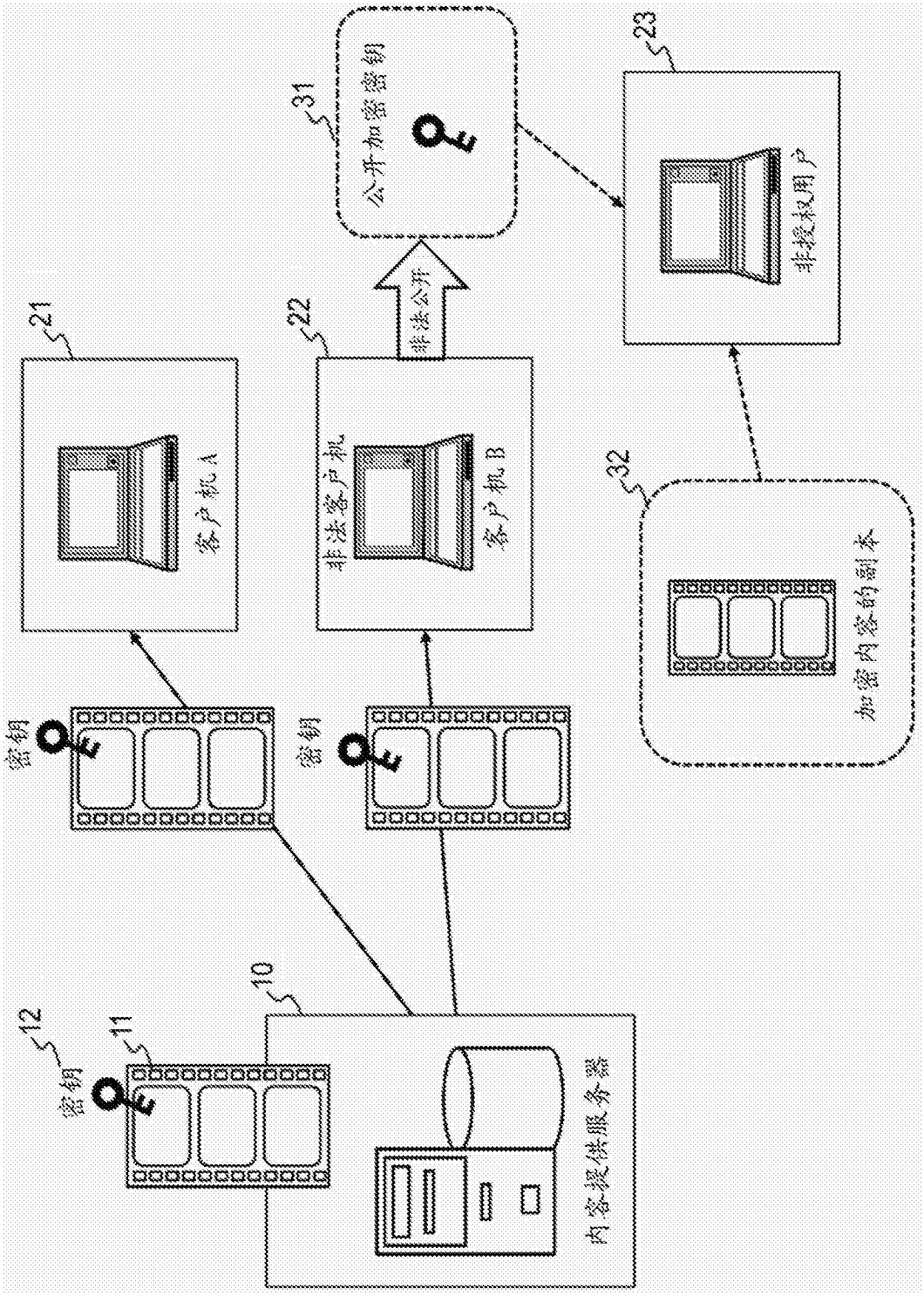

公开加密密钥
31
23
非授权用户
21
22
非法公开
客户机 A
非法客户机
客户机 B
32
加密内容的副本
密钥
密钥
10
12
密钥
11
内容提供服务器

图1

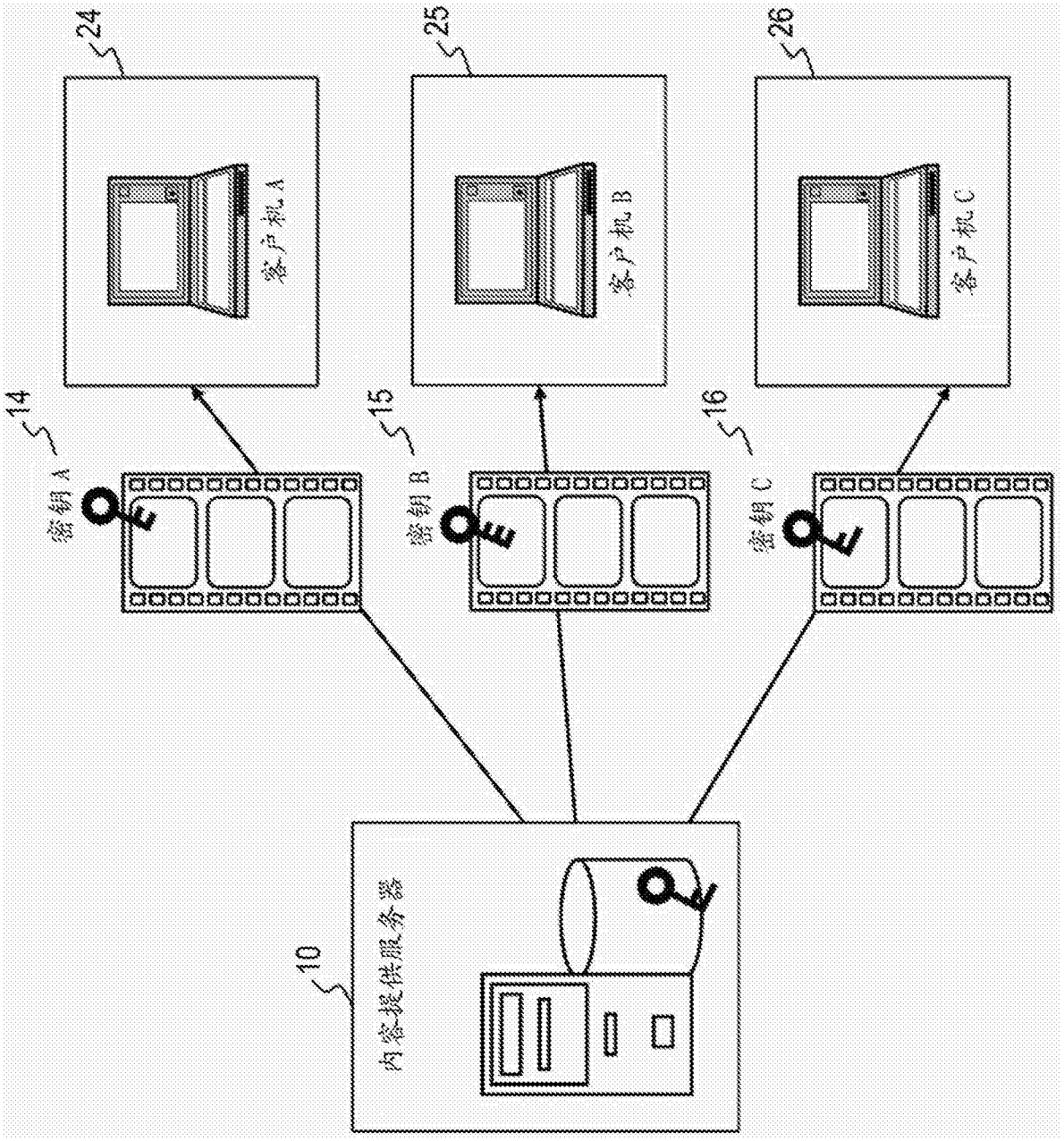


图2

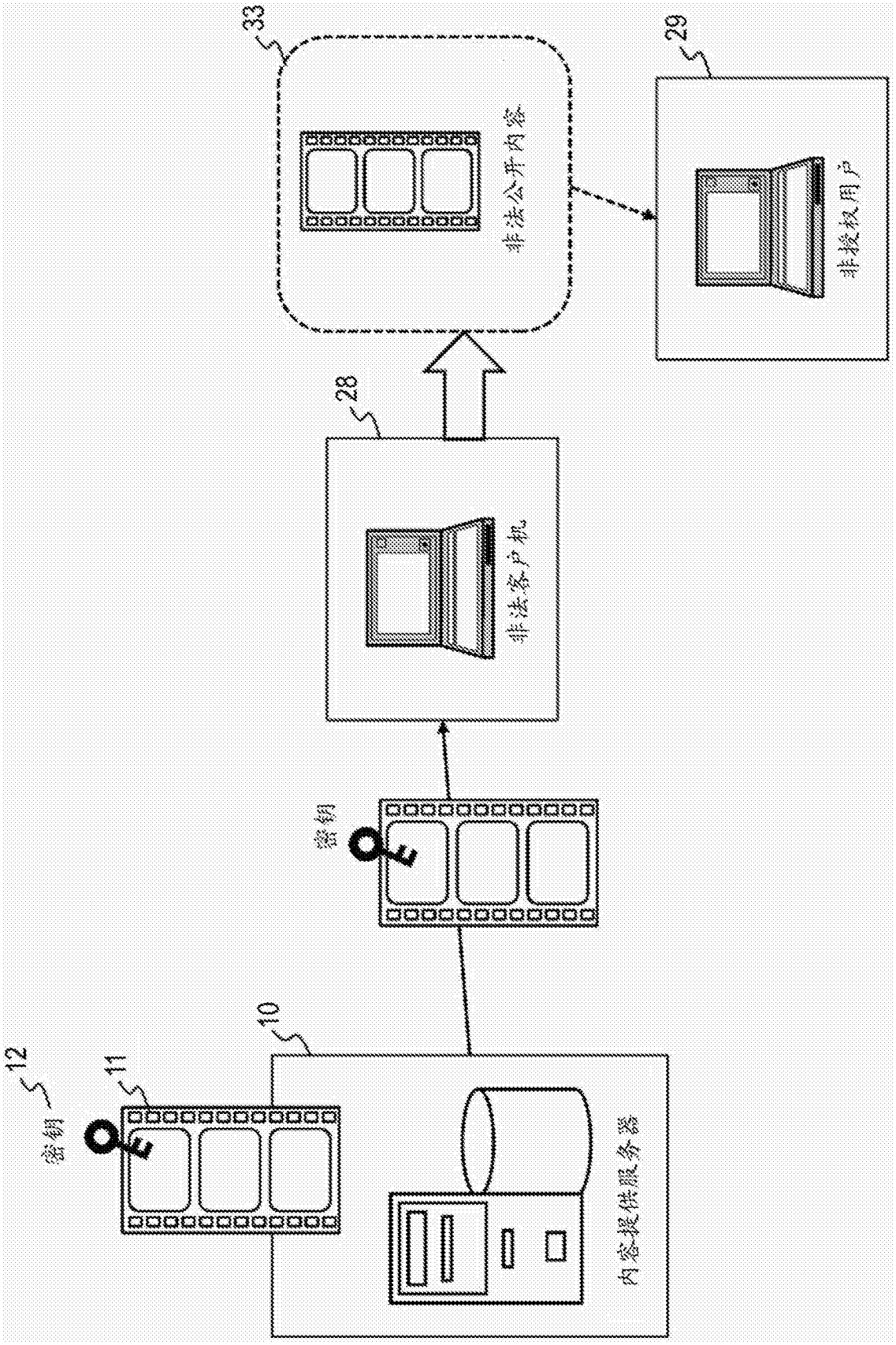


图3

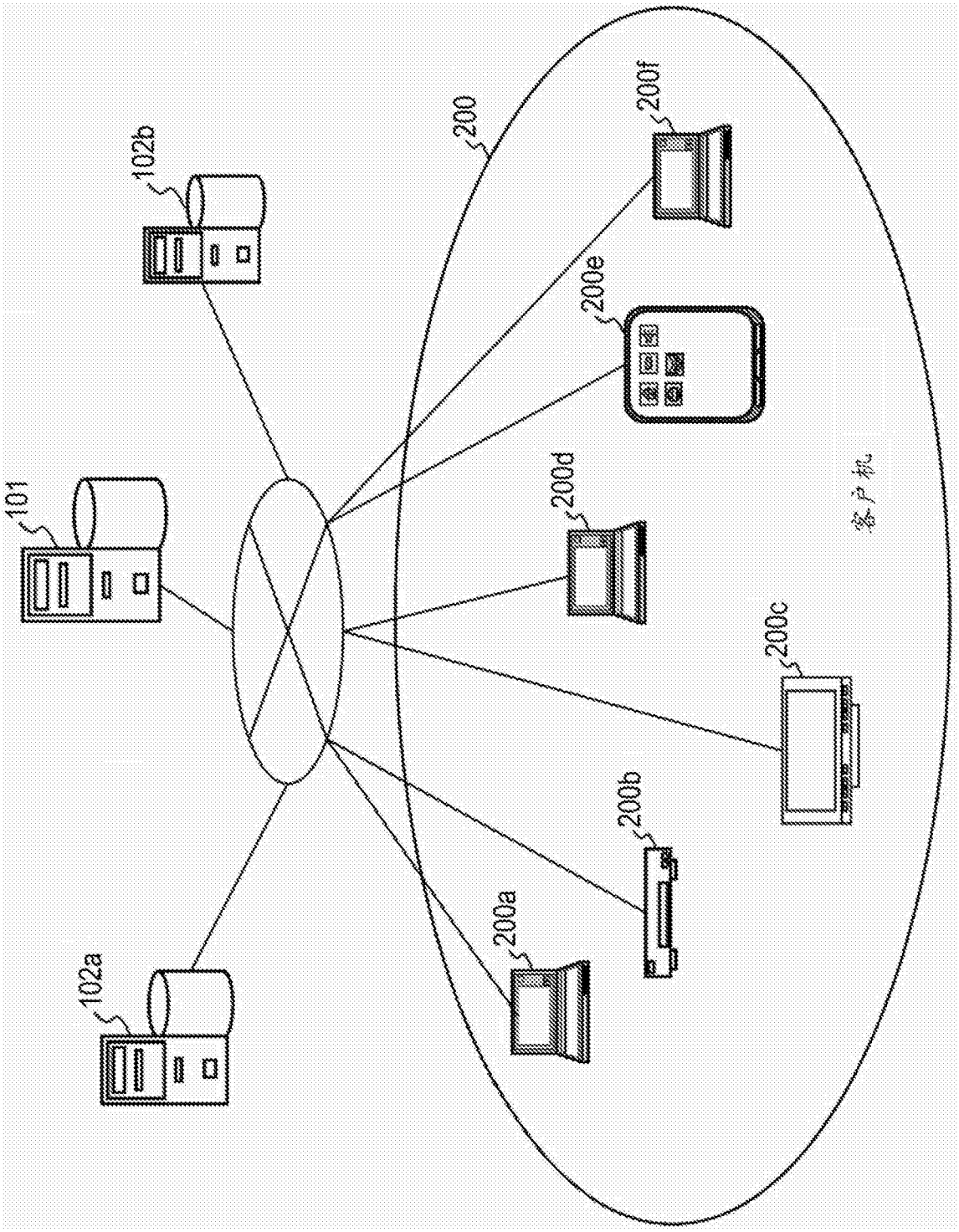


图4

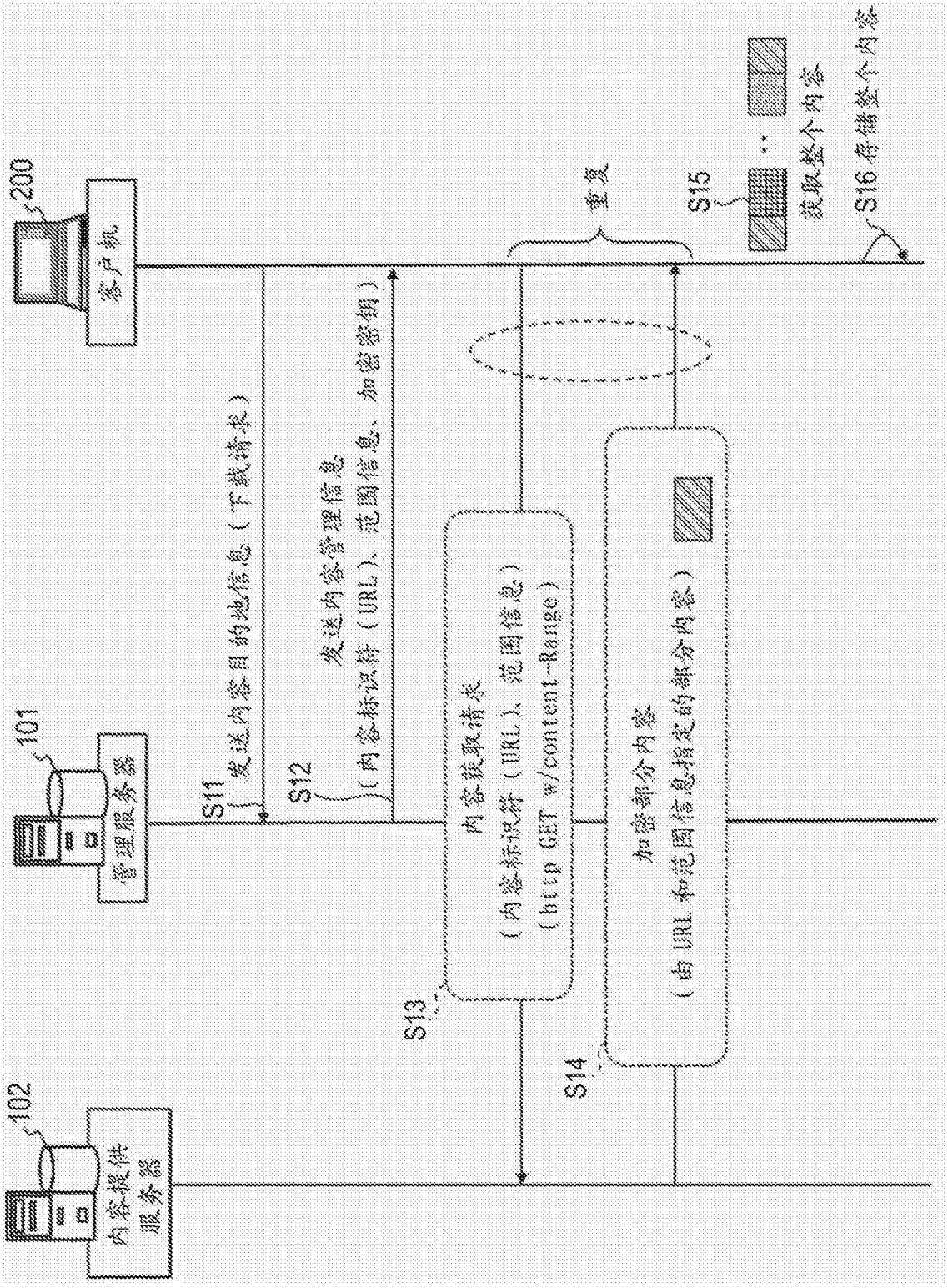

200
客户机
101
管理服务器
102
内容提供服务器
S11
发送内容目的地信息（下载请求）
S12
发送内容管理信息
（内容标识符（URL）、范围信息、加密密钥）
S13
内容获取请求
（内容标识符（URL）、范围信息）
（http GET w/content-Range）
S14
加密部分内容
（由URL和范围信息指定的部分内容）
重复
S15
获取整个内容
S16 存储整个内容

图5

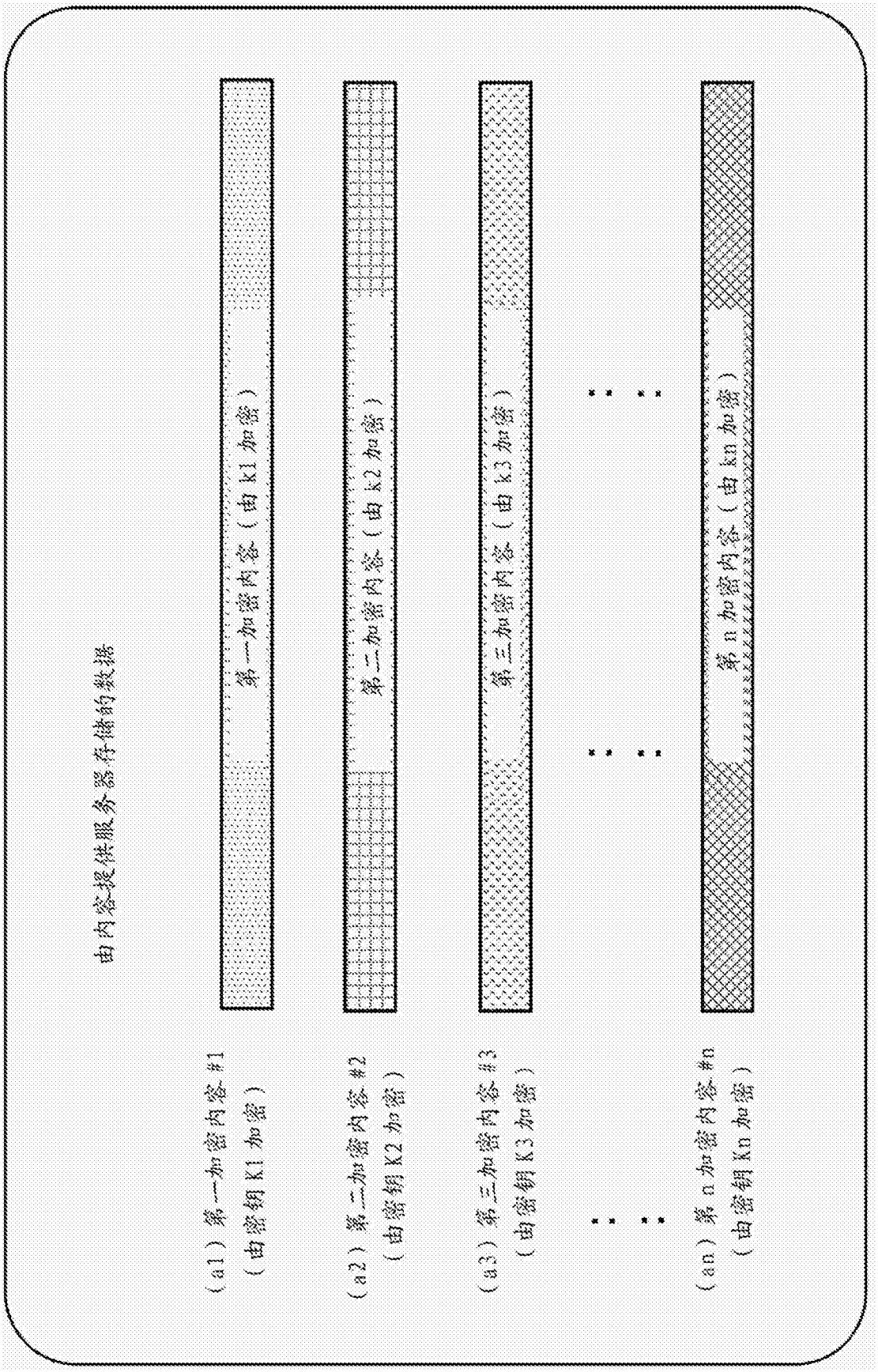

由内容提供服务器存储的数据
第一加密内容（由 K1 加密）
第二加密内容（由 K2 加密）
第三加密内容（由 K3 加密）
第 n 加密内容（由 Kn 加密）
（a1）第一加密内容 #1
（由密钥 K1 加密）
（a2）第二加密内容 #2
（由密钥 K2 加密）
（a3）第三加密内容 #3
（由密钥 K3 加密）
（an）第 n 加密内容 #n
（由密钥 Kn 加密）

图6

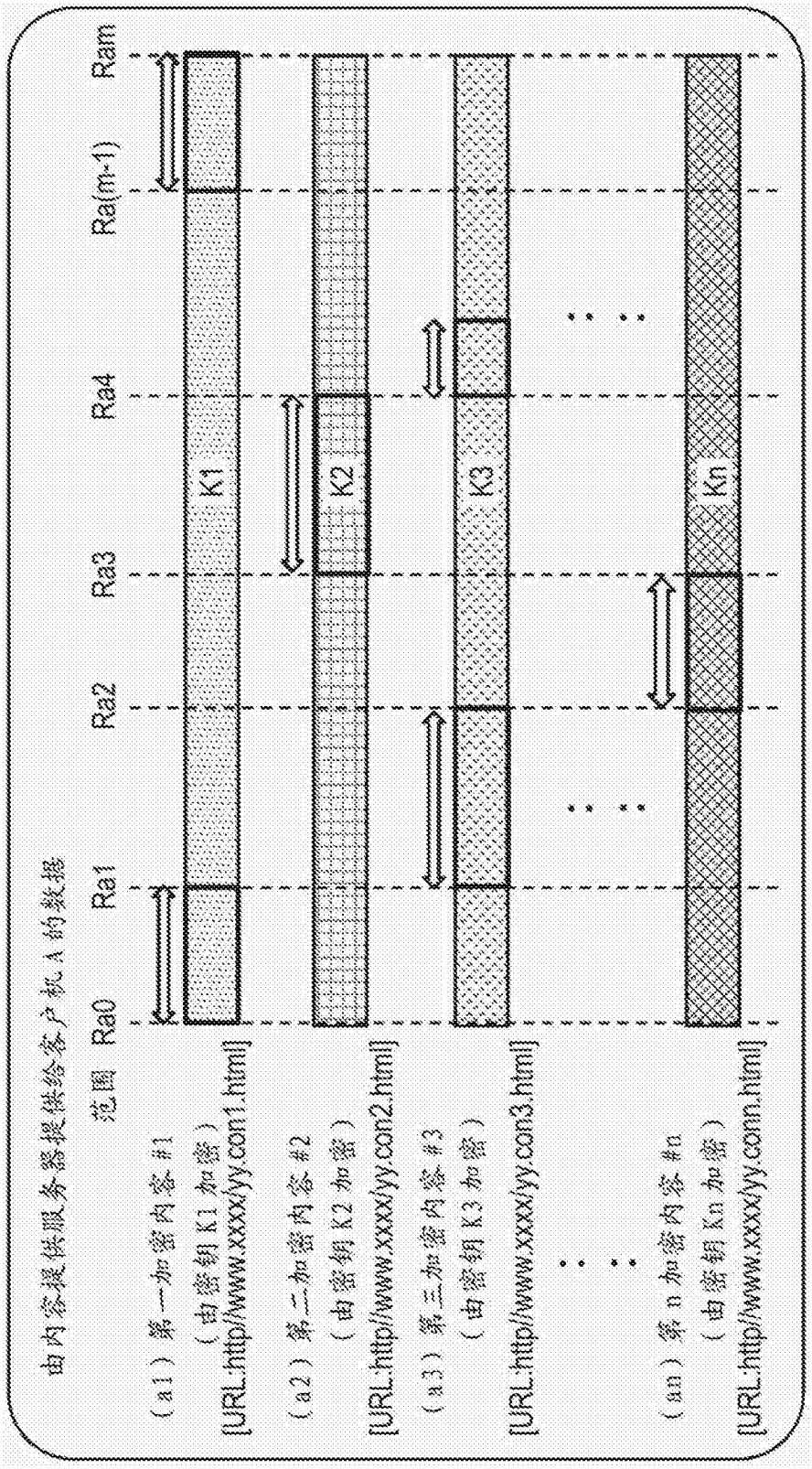

由内容提供服务器提供给客户机 A 的数据
范围 Ra0 Ra1 Ra2 Ra3 Ra4 Ra(m-1) Ram
（a1）第一加密内容 #1
（由密钥 K1 加密）
[URL:http://www.xxxx/yy.con1.html]
K1
（a2）第二加密内容 #2
（由密钥 K2 加密）
[URL:http://www.xxxx/yy.con2.html]
K2
（a3）第三加密内容 #3
（由密钥 K3 加密）
[URL:http://www.xxxx/yy.con3.html]
K3
（an）第 n 加密内容 #n
（由密钥 Kn 加密）
[URL:http://www.xxxx/yy.conn.html]
Kn
客户机 A 收到的数据
范围 Ra0 Ra1 Ra2 Ra3 Ra4 Ra(m-1) Ram
K1 K3 Kn K2 K3 K1

图7A 图7B

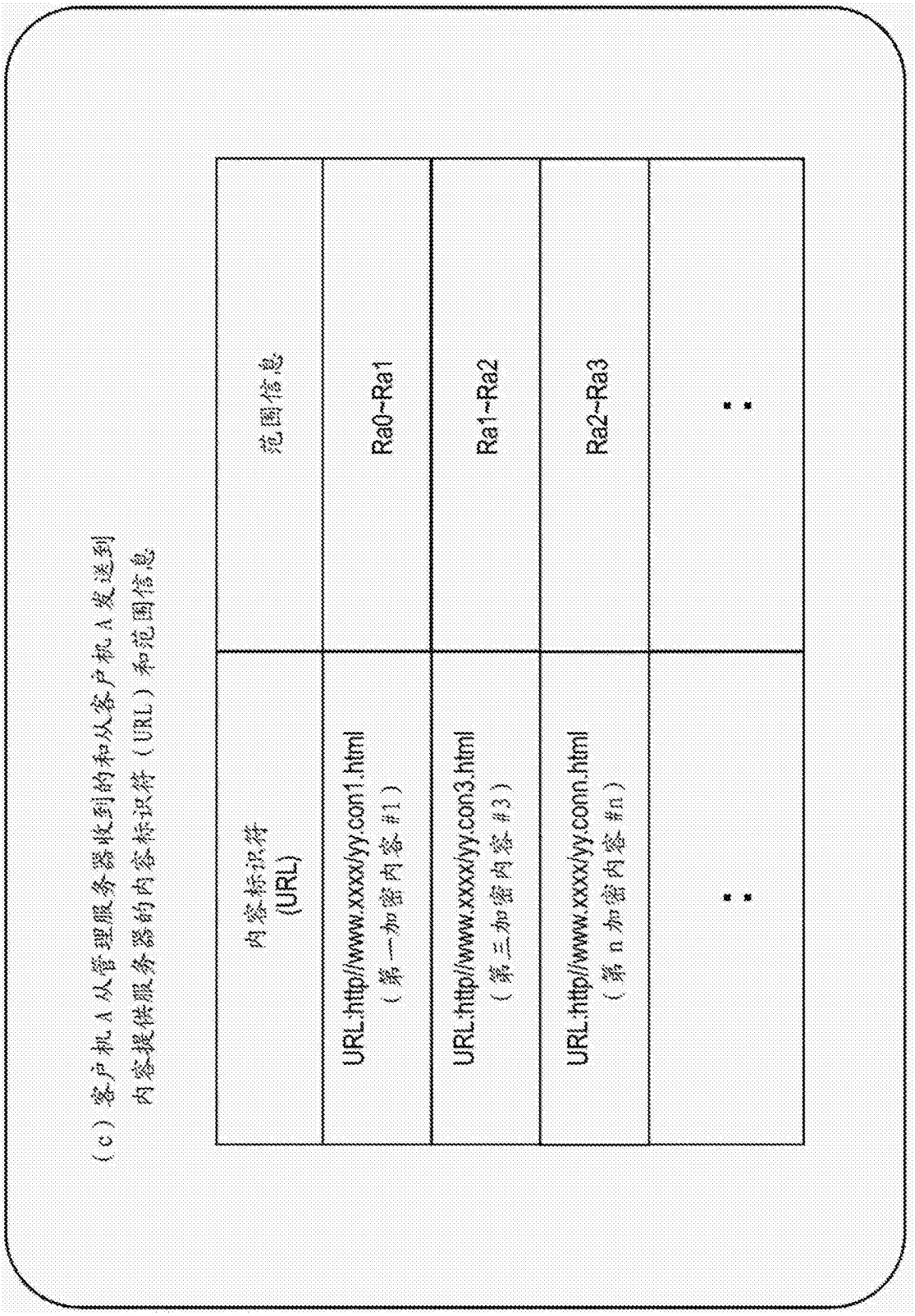

（c）客户机 A 从管理服务器收到的和从客户机 A 发送到
内容提供服务器的内容标识符（URL）和范围信息
内容标识符 (URL)
范围信息
URL:http://www.xxxx/yy.con1.html （第一加密内容 #1）
Ra0~Ra1
URL:http://www.xxxx/yy.con3.html （第三加密内容 #3）
Ra1~Ra2
URL:http://www.xxxx/yy.conn.html （第 n 加密内容 #n）
Ra2~Ra3

图8

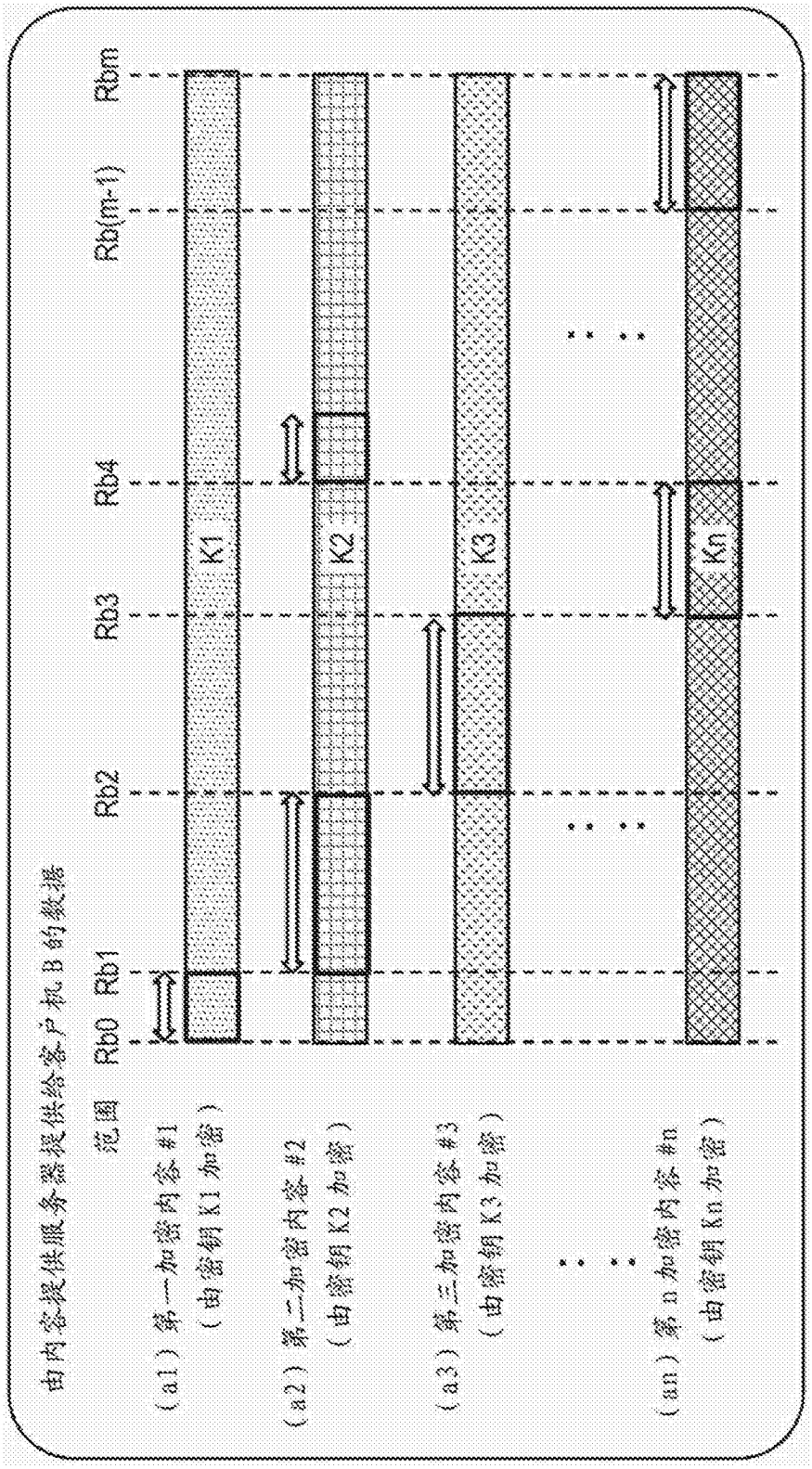

由内容提供服务器提供给客户机 B 的数据
范围 Rb0 Rb1 Rb2 Rb3 Rb4 Rb(m-1) Rbm
(a1) 第一加密内容 #1
(由密钥 K1 加密)
K1
(a2) 第二加密内容 #2
(由密钥 K2 加密)
K2
(a3) 第三加密内容 #3
(由密钥 K3 加密)
K3
(an) 第 n 加密内容 #n
(由密钥 Kn 加密)
Kn
客户机 B 收到的数据
范围 Rb0 Rb1 Rb2 Rb3 Rb4 Rb(m-1) Rbm
K1 K2 K3 Kn K2 Kn

图9A 图9B

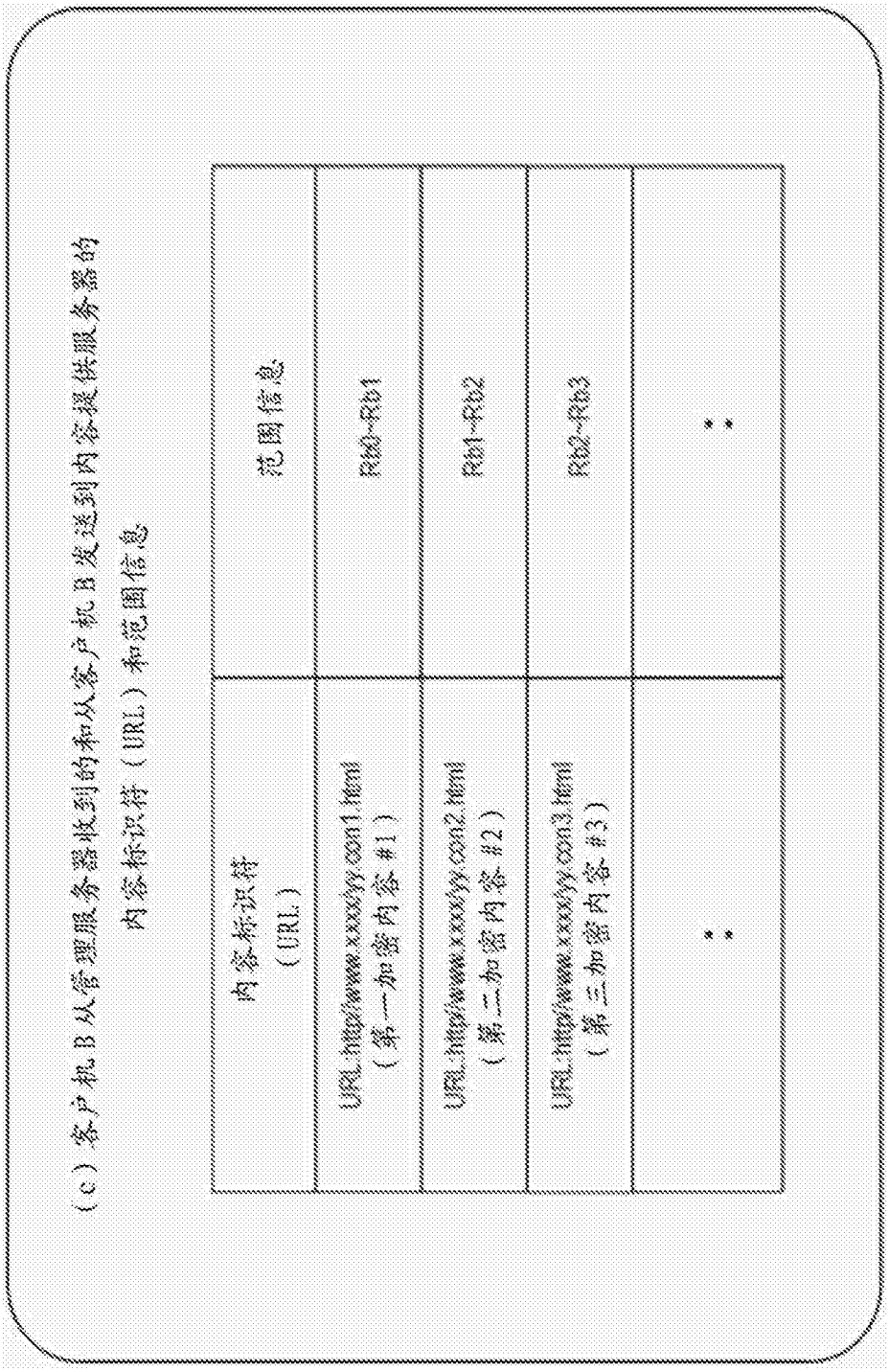

(c) 客户机 B 从管理服务器收到的和从客户机 B 发送到内容提供服务器的
内容标识符（URL）和范围信息
内容标识符
（URL）
范围信息
URL:http://www.xxxyy.com1.html
（第一加密内容 #1）
Rb0-Rb1
URL:http://www.xxxyy.com2.html
（第二加密内容 #2）
Rb1-Rb2
URL:http://www.xxxyy.com3.html
（第三加密内容 #3）
Rb2-Rb3
* *
* *
* *

图10

	传送内容信息	传送目的地信息	传送用户	传送日期信息	范围信息	传送加密密钥信息
(1)	ABC 故事	xyz@patnet.co.jp	SUZUKI ICHIRO	2010.07.22	#1:Ra1~Ra2,Rax~Ray #2:Ra2~Ra3 #3: • • • • • • •	K1,K2,K3 • • •
(2)	ABC 故事	jkl@ynos.ne.jp	TANAKA KAORU	2010.09.15	#1:Rb1~Rb2 #2:- #3:Rb2~Rb3,Rbx~Rby • • • •	K1,K3 • • •
• •	• •	• •	• •	• •	• •	• •

图11

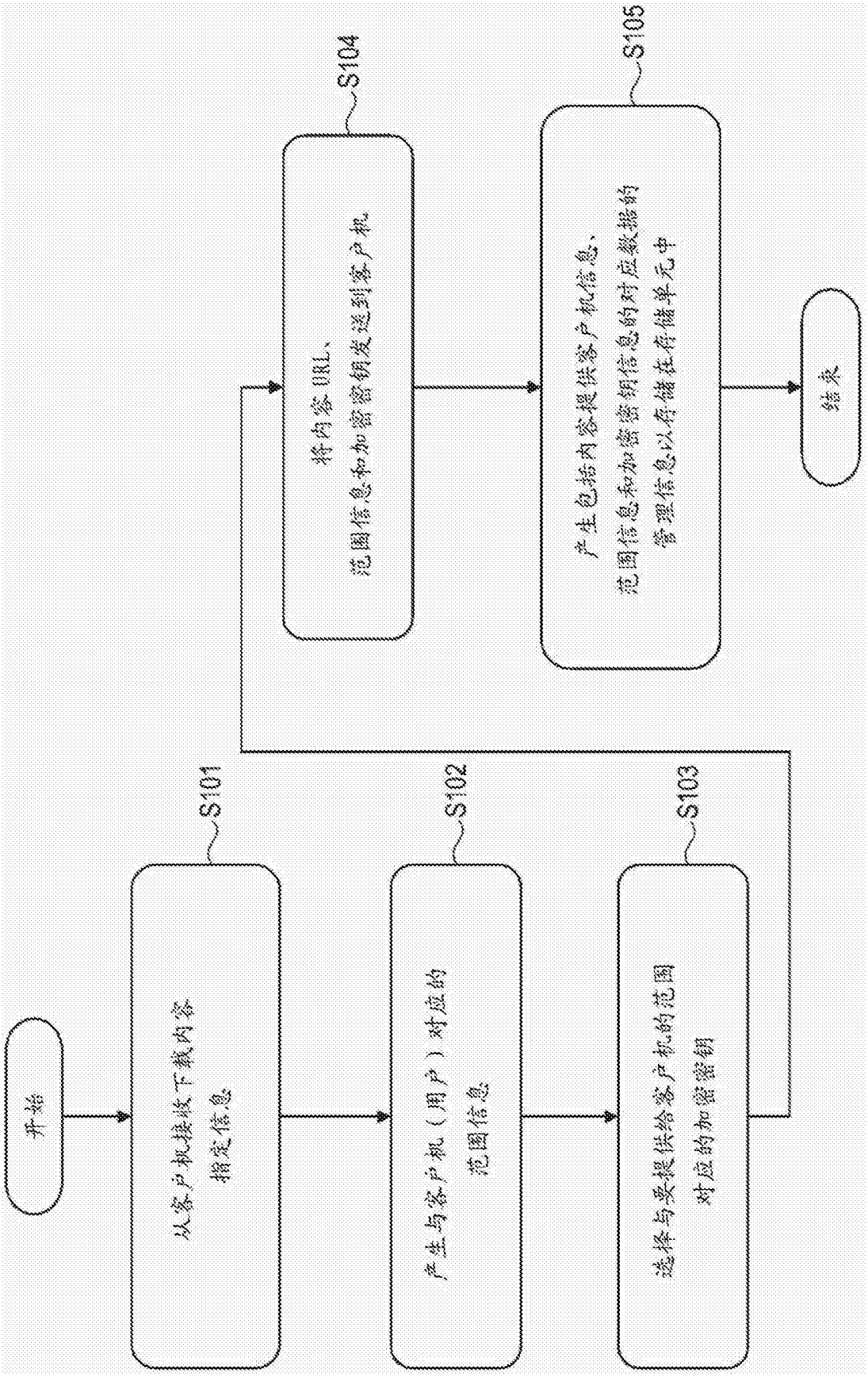

开始
从客户机接收下载内容
指定信息
S101
产生与客户机（用户）对应的
范围信息
S102
选择与要提供给客户机的范围
对应的加密密钥
S103
将内容 URL、
范围信息和加密密钥发送到客户机
S104
产生包括内容提供客户机信息、
范围信息和加密密钥信息的对应数据的
管理信息以存储在存储单元中
S105
结束

图12

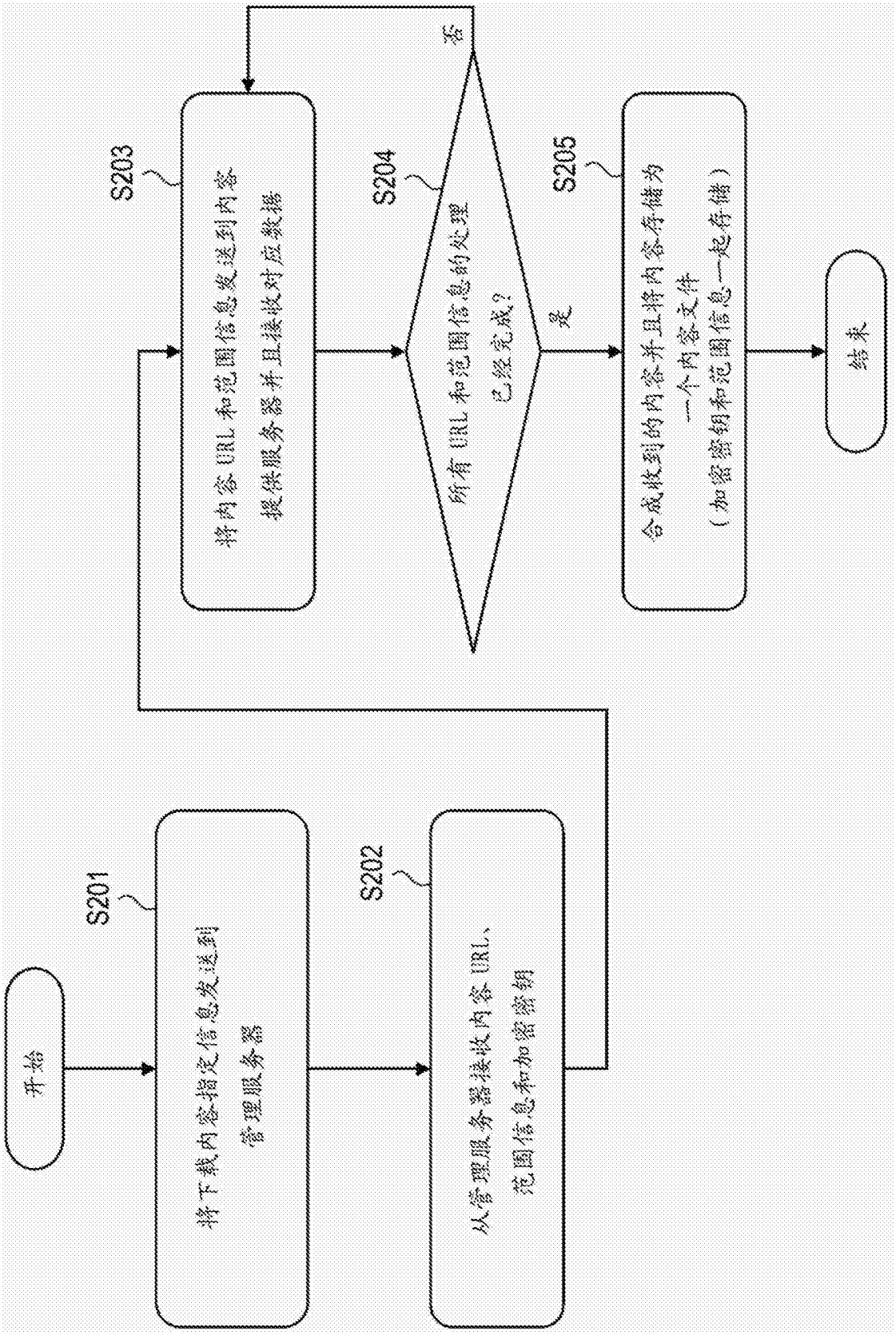

开始
S201
将下载内容指定信息发送到
管理服务器
S202
从管理服务器接收内容 URL、
范围信息和加密密钥
S203
将内容 URL 和范围信息发送到内容
提供服务器并且接收对应数据
S204
所有 URL 和范围信息的处理
已经完成?
否
是
S205
合成收到的内容并且将内容存储为
一个内容文件
(加密密钥和范围信息一起存储)
结束

图13

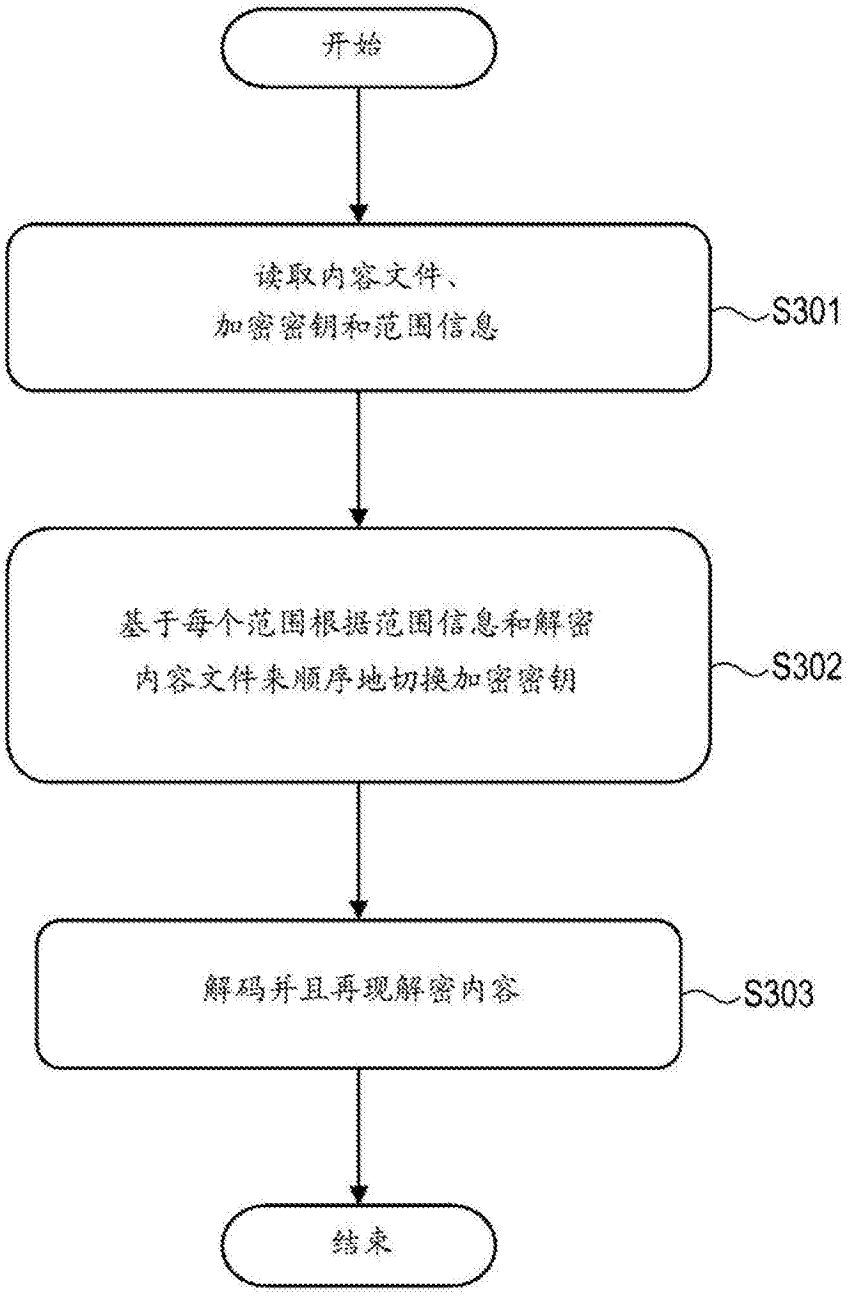

开始
读取内容文件、
加密密钥和范围信息
S301
基于每个范围根据范围信息和解密
内容文件来顺序地切换加密密钥
S302
解码并且再现解密内容
S303
结束

图14

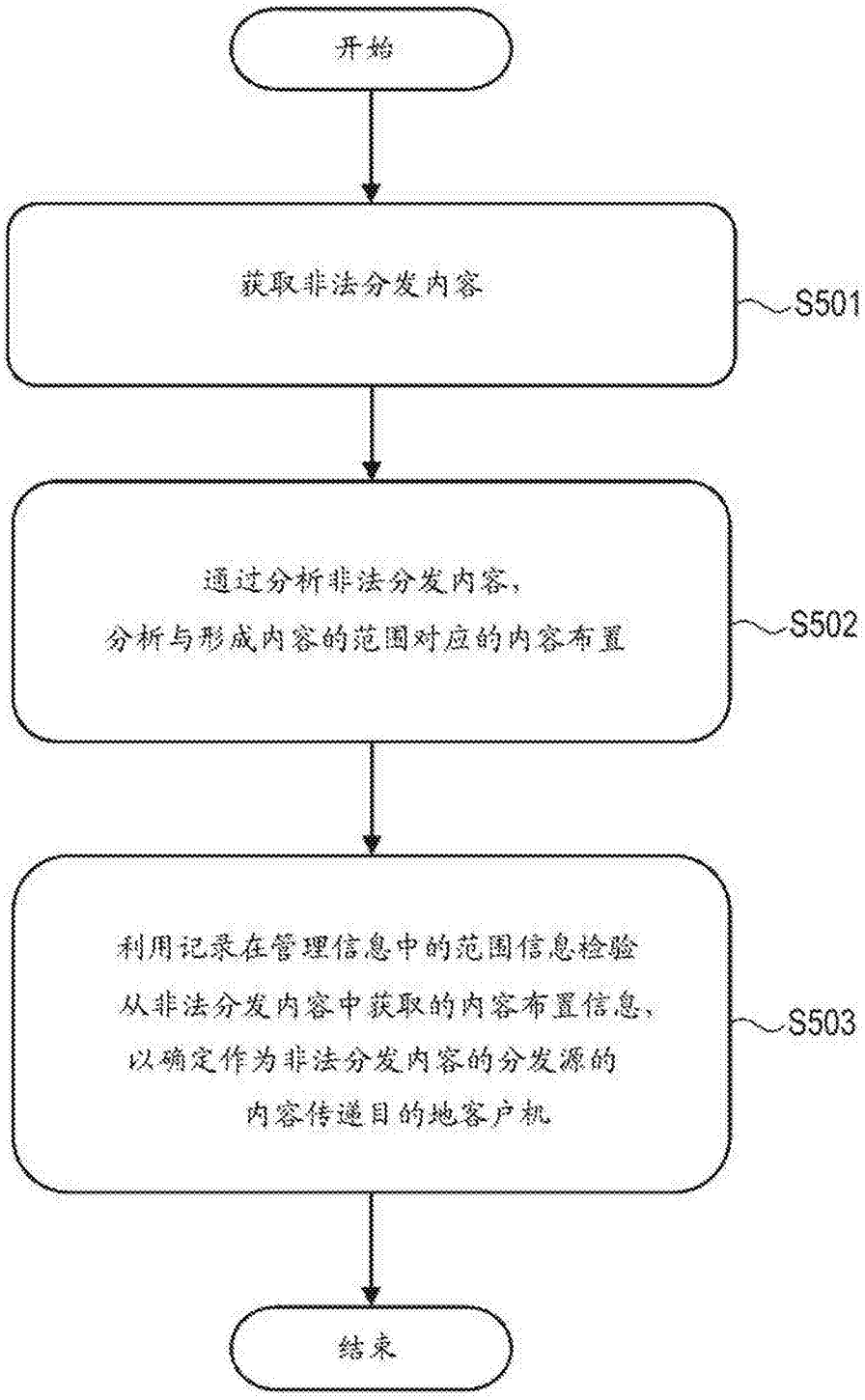

开始
获取非法分发内容
S501
通过分析非法分发内容、
分析与形成内容的范围对应的内容布置
S502
利用记录在管理信息中的范围信息检验
从非法分发内容中获取的内容布置信息、
以确定作为非法分发内容的分发源的
内容传递目的地客户机
S503
结束

图15

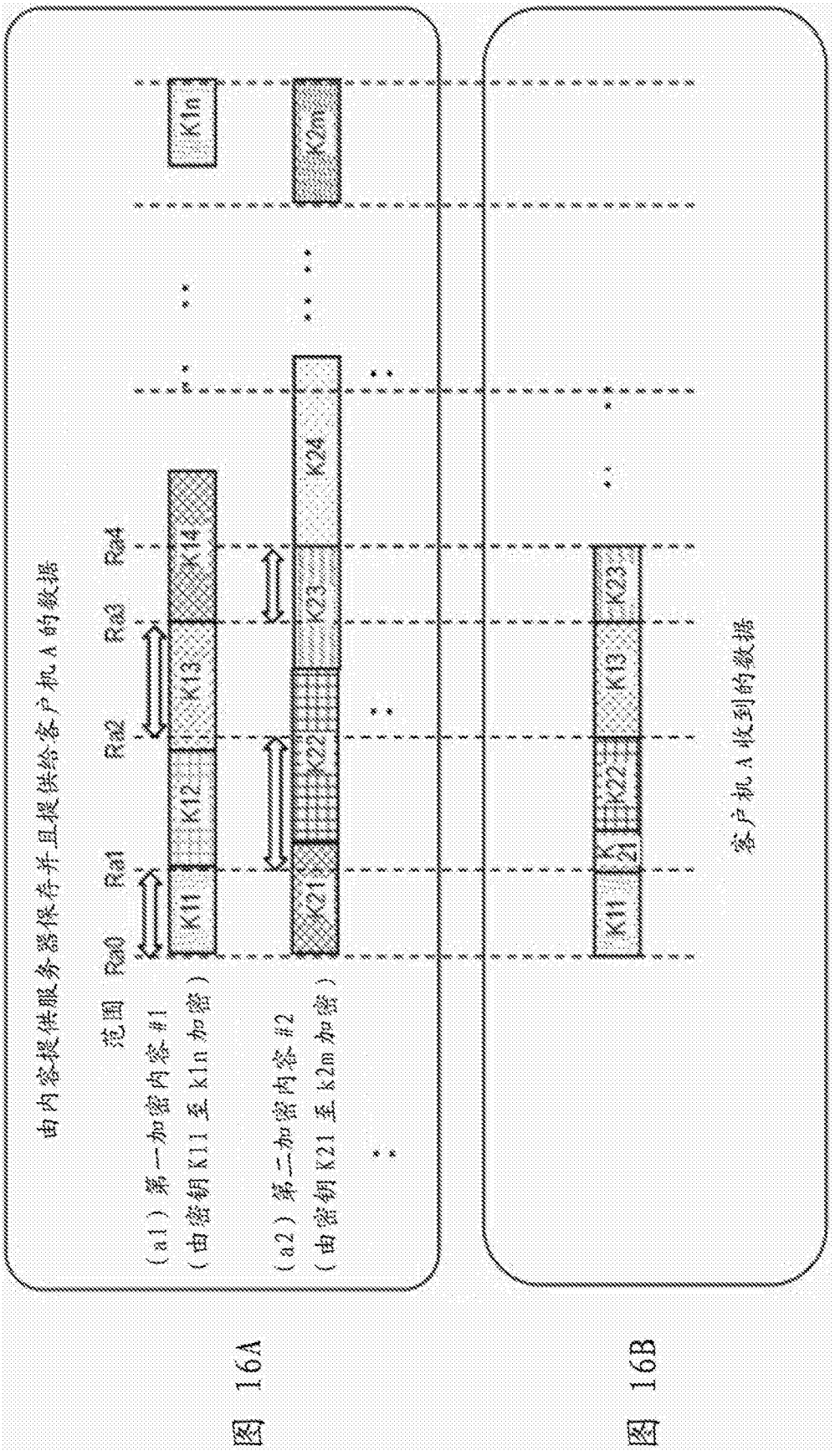

由内容提供服务器保存并且提供给客户机A的数据
范围 Rx#0 Rx#1 Rx#2 Rx#3 Rx#4
(a1) 第一加密内容#1
(由密钥K11至k1n加密)
K11 K12 K13 K14 K1n
(a2) 第二加密内容#2
(由密钥K21至k2m加密)
K21 K22 K23 K24 K2m
K11 K12 K13 K23
客户机A收到的数据

图 16A

图 16B

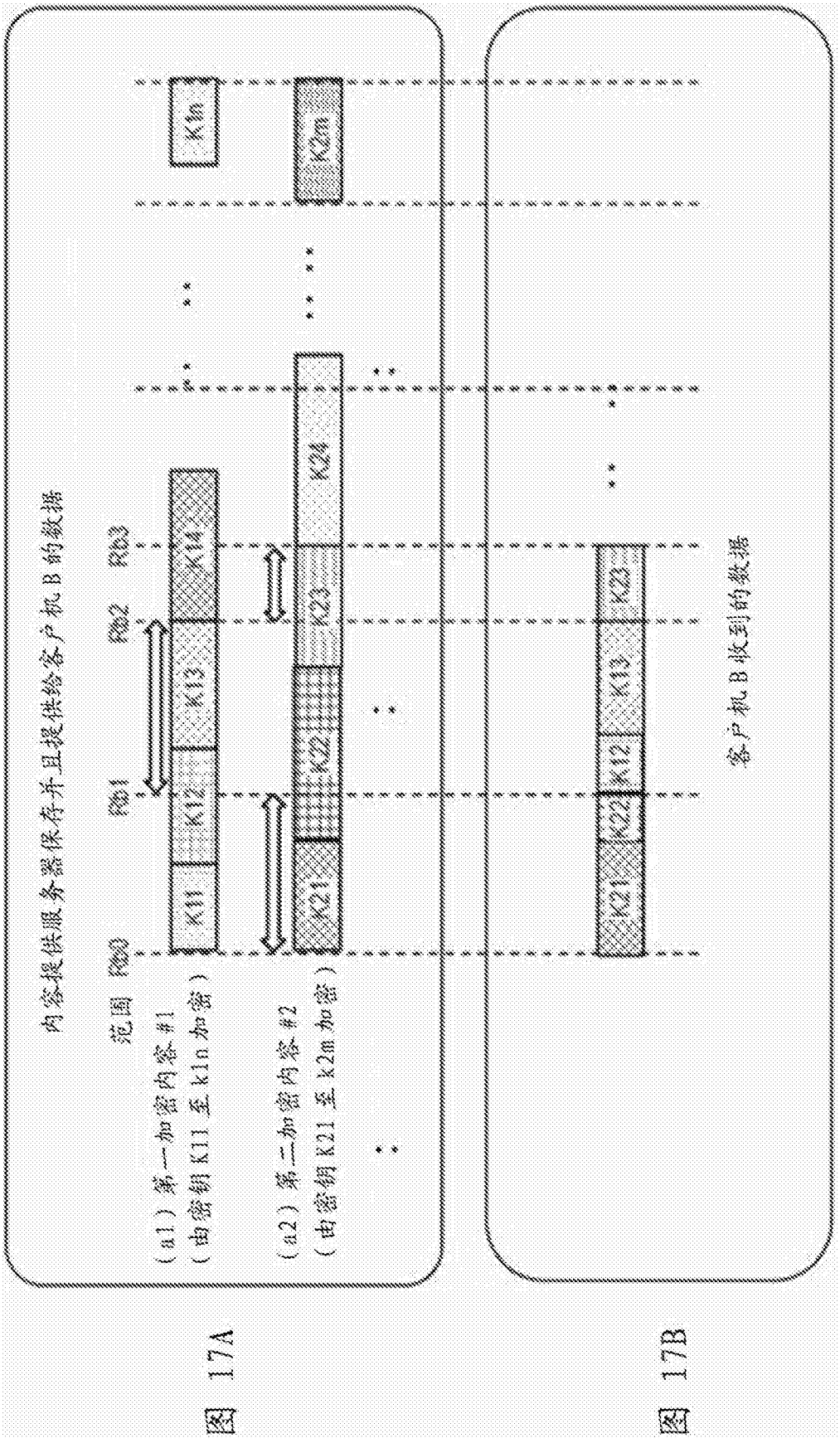

内容提供服务器保存并且提供给客户机 B 的数据
范围 #3
#1
#2
#3
(a1) 第一加密内容 #1
(由密钥 K11 至 k1n 加密)
(a2) 第二加密内容 #2
(由密钥 K21 至 k2m 加密)
K11
K12
K13
K14
K1m
K21
K22
K23
K24
K2m
客户机 B 收到的数据

图 17A 图 17B

传递内容信息	传递目的地信息	传递用户	传递日期信息	范围信息	传递加密密钥信息
ABC故事	xyz@patnet.co.jp	SUZUKI ICHIRO	2010.07.22	#1:Ra1~Ra2,Rax~Ray #2:Ra2~Ra3 #3:・・・ ・・・・	K11,K12,K23・・・
ABC故事	jkl@ynos.ne.jp	TANAKA KAORU	2010.09.15	#1:Rb1~Rb2 #2:- #3:Rb2~Rb3,Rbx~Rby ・・・・	K11,K32・・・
・・	・・	・・	・・	・・	・・

图18

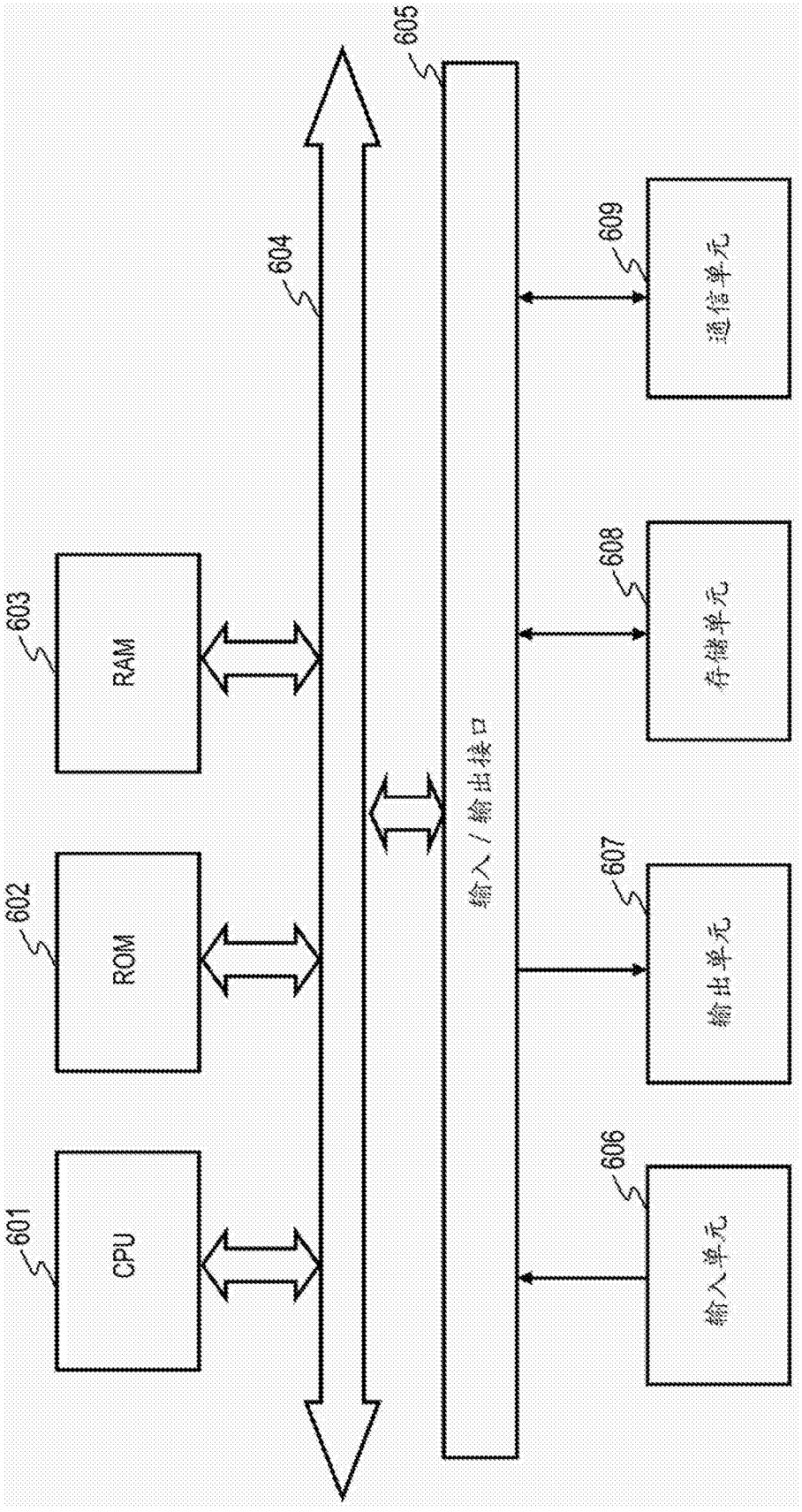

605
604
609
通信单元
603
RAM
608
存储单元
输入/输出接口
602
ROM
607
输出单元
601
CPU
606
输入单元

图19

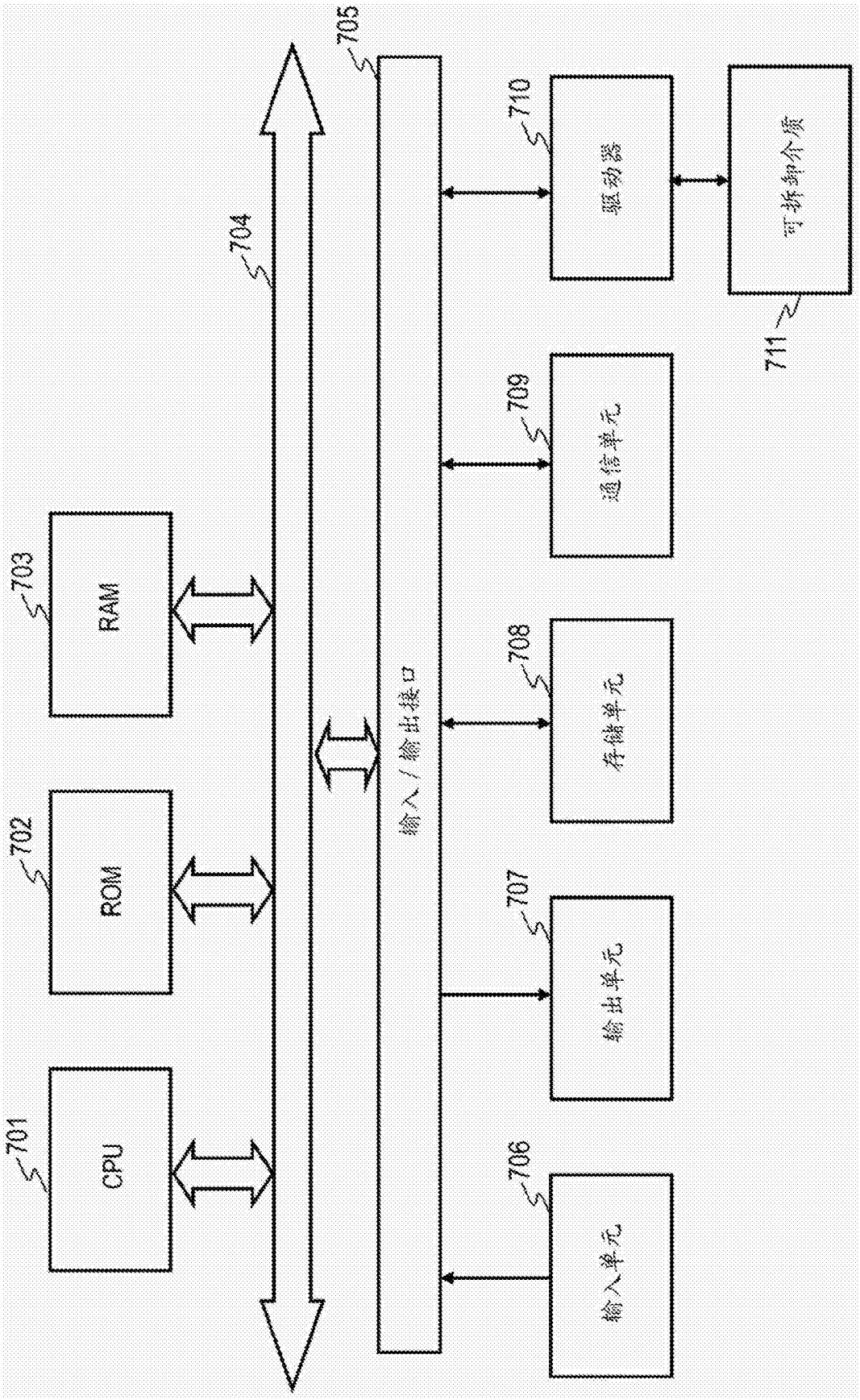

701
CPU
702
ROM
703
RAM
704
705
输入/输出接口
706
输入单元
707
输出单元
708
存储单元
709
通信单元
710
驱动器
711
可拆卸介质

图20