[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 21/22 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200710103441.4

[43] 公开日 2007 年 10 月 3 日

[11] 公开号 CN 101046839A

[22] 申请日 2002.8.6

[21] 申请号 200710103441.4

分案原申请号 02811577.5

[30] 优先权

[32] 2001. 8. 8 [33] JP [31] 2001 - 241095

[71] 申请人 松下电器产业株式会社

地址 日本国大阪府门真市

[72] 发明人 中原彻 东吾纪男

[74] 专利代理机构 上海专利商标事务所有限公司

代理人 张 鑫

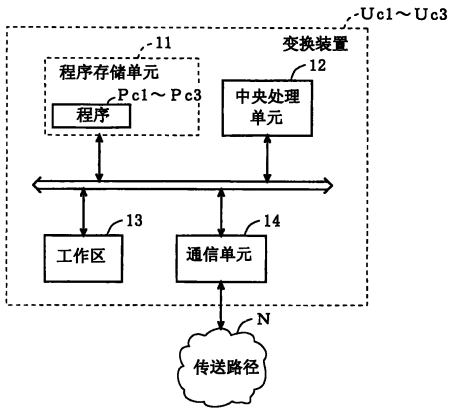
权利要求书 1 页 说明书 32 页 附图 24 页

[54] 发明名称

许可信息变换装置

[57] 摘要

至少 2 台终端装置分别根据在自己加入的内容传送系统中生成的许可信息，来利用内容数据。 变换装置(Uc1)具有存储面向 1 台终端装置的许可信息的工作区(13)，以及将存入工作区(13)的许可信息变换为面向另一台终端装置的许可信息的中央处理单元(12)。 通过这样，能够提供进行变换、使得可将自己的许可信息转让给他人的变换装置(Uc1)。



1.一种电子设备，用于将第1许可信息变换为第2许可信息，所述第1许可信息包含许可利用内容用的一个或多个利用许可信息，其特征在于，

所述利用许可信息给予或不给予对变换为第2许可信息的许可，

所述电子设备包括：

存储可变换性信息的存储部，所述可变换性信息为第 1 许可信息中包含的至少一个利用许可信息指出是否给予对变换为第 2 许可信息的许可；以及

根据从存储部获得的所述可变换性信息将所述第 1 许可信息中所包含的、除了不给予对变换为第 2 许可信息的许可的利用许可信息之外的信息变换成第2许可信息的变换部。

2.如权利要求1所述的电子设备，其特征在于，所述第1许可信息还包含许可在第1系统中利用所述内容用的第1利用许可信息，

所述第2许可信息还包含许可在不同于所述第1系统的第2系统中利用所述内容用的第2利用许可信息，

所述电子设备还包括用于获取指明所述第2系统的系统信息的获取部，并且

所述变换部用来将第1许可信息变换成在由所获取的系统信息指明的第2系统中所使用的第2许可信息。

3.一种方法，用于利用电子设备将第1许可信息变换为第2许可信息，所述第1许可信息包含许可利用内容用的一个或多个利用许可信息，其特征在于，

所述利用许可信息给予或不给予对变换为第2许可信息的许可，

所述方法包括：

存储可变换性信息的存储步骤，所述可变换性信息为第 1 许可信息中包含的至少一个利用许可信息指出是否给予对变换为第2许可信息的许可；以及

获得所述可变换性信息、并根据所获得的所述可变换性信息将所述第1许可信息中所包含的、除了不给予对变换为第 2 许可信息的许可的利用许可信息之外的信息变换成第2许可信息的变换步骤。

许可信息变换装置

本申请是申请人于2002年8月6日提交的、申请号为“02811577.5”（国际申请号 PCT/JP 02/08009）的、发明名称为“许可信息变换装置”的发明专利申请的分案申请。

技术领域

本发明涉及变换装置，更特别涉及将对终端装置中的内容数据的利用进行控制的许可信息加以变换的变换装置。

背景技术

近年来，利用以互联网为代表的网络的宽带化及通常的连接环境，内容传送正成为身旁普通的事情。为了更进一步普及这样的内容传送，重要的是要保护与内容数据有关联的权利(例如著作权或销售权)，因此一直以来正在进行各种各样权利管理技术的研究及开发。这里，在本申请说明书中，将与内容数据有关联的权利称为数字权限。另外，作为权利管理技术，代表性的有DRM(Digital Rights Management,数字权限管理)。下面说明内装有 DRM 的内容传送系统。

在以往的内容传送系统中，服务器与终端装置利用网络连接，能够进行数据通信。服务器至少存储1组内容数据、内容解密密钥及许可信息。内容数据例如是表示音乐的数字数据，以预定的方式进行加密。内容解密密钥是将加密的内容数据进行解密用的密钥。许可信息是在DRM中表示上述的内容数据的利用条件。作为利用条件，代表性的是内容数据的利用次数。

在以上构成的内容传送系统中，如下所述那样传送内容数据。首先，终端装置请求服务器传送内容数据。一般，终端装置通过网络向服务器发送内容标识符及终端固有信息，通过这样进行请求发送内容数据。内容标识符是唯一确定上述内容数据的信息。终端固有信息由终端装置预先保持，是唯一能够确定上述的内容数据的请求源即终端装置的信息。

服务器对于来自终端装置的请求进行应答，将上述的内容解密密钥使用这次接收的终端固有信息进行加密。然后，服务器将上述加密的内容数据、用终

端固有信息加密的内容解密密钥及许可信息发送给终端装置。终端装置接收由服务器传送的内容数据、内容解密密钥及许可信息，存入内部具有的存储装置。

在以上存储之后，终端装置的用户处于能够利用这一次解密的内容数据的状态。在实际上利用内容数据时，用户将该意思向终端装置发出指示。终端装置对该指示进行应答，如下那样进行工作。终端装置判断这次的利用与根据存储装置内的许可信息表示的利用条件是否一致。终端装置只有在与利用条件一致时执行以下的处理。然后，因为存贮装置内的内容解密密钥被加密，终端装置使用自己保持的终端固有信息，将该内容解密密钥进行解密。再有，由于存储装置内的内容数据还如上所述进行了加密，因此终端装置使用已解密的内容解密密钥，将该内容数据进行解密，然后将解密的内容数据进行重放。

下面说明以上的内容传送系统具有的问题。终端装置的用户(下面称为第 1 用户)有时想要将自己的许可信息即内容数据的利用权转让给其他的用户(下面称为第 2 用户)。但是，第 2 用户不一定加入上述的内容传送系统，有可能加入别的内容传送系统。再有，在两个内容传送系统之间，许可信息的结构还有可能有差异。结果，第 2 用户侧的终端装置即使能够从第 1 用户侧的终端装置接受许可信息，也不能解释接受的许可信息。因此，在以往的内容传送系统中，不能将自己的许可信息转让给他人。

另外，有的情况是用户加入互相不同的第 1 及第 2 内容传送系统，具有仅能够解释从第 1 内容传送系统得到的许可信息的第 1 终端装置及仅能够解释从第 2 内容传送系统得到的许可信息的第 2 终端装置。在这样的状况下，如上所述，由于第 1 及第 2 内容传送系统中各自使用的许可信息的结构有可能有差异，因此第 2 终端装置即使假设能够接受第 1 内容传送系统的许可信息，也不能对它进行解释。因此，在上述的状况下，产生自己的终端装置不能利用用户所有的许可信息的情况。

所以，本发明的目的在于提供将许可信息变换为使得其他人能够利用或用其它终端装置能够利用的变换装置。

发明内容

本发明为了达到上述目的，具有以下所述的特征。本发明的第 1 方面是将面向第 1 终端装置的许可信息变换为面向第 2 终端装置用的变换装置，第 1 及所述第 2 终端装置能够接收由互不相同的第 1 和第 2 密钥进行加密的内容数据，根据互不相同的第 1 和第 2 许可信息利用接收的内容数据，第 1 许可信息包含

对由所述第 1 密钥进行加密的内容数据进行译码用的第 1 解密密钥。变换装置具有：存储面向所述第 1 终端装置的第 1 许可信息的工作区，以及判断是否存于所述工作区的第 1 许可信息的构成要素中至少第 1 解密密钥的变换处理得到许可，在判断为变换处理得到许可的情况下，将所述第 1 许可信息的第 1 解密密钥置换为对所述第 2 密钥进行加密的内容数据进行解密用的第 2 解密密钥，以此将存于所述工作区的第 1 许可信息变换为面向所述第 2 终端装置的第 2 许可信息的处理单元。

第 2 方面是从属于第 1 方面的，第 1 许可信息还包含许可在第 1 终端装置一侧利用内容数据用的第 1 利用许可信息。处理单元还将第 1 许可信息所包含的第 1 利用许可信息变换为许可在第 2 终端装置一侧利用内容数据用的第 2 利用许可信息。

第 3 方面是从属于第 2 方面的，处理单元根据预定的变换比例，将第 1 许可信息所包含的第 1 利用许可信息变换为许可在第 2 终端装置侧利用内容数据用的第 2 利用许可信息。

根据以上的第 1～第 3 方面，变换装置将面向第 1 终端装置的第 1 许可信息变换为面向第 2 终端装置的第 2 许可信息。通过这样，第 1 用户能够将以自己的第 1 许可信息为基础而生成的而且在第 2 终端装置能够利用的第 2 许可信息转让给第 2 用户。

第 4 方面是从属于第 1 方面的，第 1 及第 2 终端装置与第 1 及第 2 服务器连接。第 1 及第 2 服务器至少生成第 1 及第 2 许可信息，发送给第 1 及第 2 终端装置。再有，第 1 及第 2 服务器保持着表示第 1 及第 2 许可信息的格式的第 1 及第 2 格式数据。这里，变换装置还具有与第 1 及第 2 服务器进行通信、接收第 1 及第 2 格式数据的通信单元。另外，处理单元根据通信单元接收的第 1 及第 2 格式数据，将存入工作区的第 1 许可信息变换为面向第 2 终端装置的第 2 许可信息。

第 5 方面是从属于第 1 方面的，变换装置还具有存储表示第 1 及第 2 许可信息的格式的第 1 及第 2 格式数据的格式存储单元。另外，处理单元根据存入格式存储单元的第 1 及第 2 格式数据，将存入工作区的第 1 许可信息变换为面向第 2 终端装置的第 2 许可信息。

第 6 方面是从属于第 1 方面的，变换装置还具有与第 1 终端装置进行通信、接收该第 1 终端装置保持的第 1 许可信息的通信单元。另外，在工作区中存储

利用通信单元接收的第 1 许可信息。

第 7 方面是从属于第 1 方面的，变换装置与生成面向第 1 终端装置的第 1 许可信息的第 1 服务器连接，并能够进行通信。变换装置还具有与第 1 服务器进行通信，接收面向该第 1 终端装置生成的第 1 许可信息的通信单元。工作区存储利用通信单元接收的第 1 许可信息。

第 8 方面是从属于第 1 方面的，变换装置被组装于所述第 1 终端装置。

第 9 方面是从属于第 1 方面的，处理单元判断第 1 及第 2 终端装置是否是正当用户，在第 1 及第 2 终端装置双方都是正当用户时，将存入工作区的第 1 许可信息变换为面向第 2 终端装置的第 2 许可信息。

第 10 方面是从属于第 9 方面的，处理单元在第 1 及第 2 终端装置的一方或双方不是正当用户时，将存入工作区的第 1 许可信息送回第 1 终端装置。

根据第 9 及第 10 方面，能够排除来自不正当用户的许可信息变换处理的请求。

第 11 方面是从属于第 1 方面的，许可信息包含表示构成要素变换处理是否许可的变换可否信息。处理单元使用第 1 许可信息所包含的变换可否信息，判断存入工作区的第 1 许可信息的每个构成要素是否许可进行变换处理。

第 12 方面是从属于第 1 方面的，处理单元从外部取得表示对存入工作区的第 1 许可信息的每个构成要素是否许可进行变换处理的变换可否信息，并使用取得的变换可否信息，判断存入所述工作区的第 1 许可信息的每个构成要素是否许可进行变换处理。

根据第 11 和第 12 方面，由于能够对第 1 许可信息的每个构成要素控制进行变换处理，因此能够提供考虑到内容数据传送者一侧的意图的变换装置。

第 13 方面是从属于第 1 方面的，第 1 终端装置与第 1 服务器连接，处理单元将存入工作区的第 1 许可信息内不许可进行变换处理的构成要素送回第 1 服务器。

第 14 方面是从属于第 1 方面的，处理单元将存入工作区的第 1 许可信息内不许可进行变换处理的构成要素保持在内部。

根据第 13 及第 14 方面，对于不许可进行变换处理的第 1 许可信息的构成要素，因为或者返回第 1 服务器，或者保持在内部，因此比较典型的是在将变换后的第 2 许可信息再变换为第 1 许可信息时能够使用。

第 15 方面是一种变换方法，是第 1 及第 2 终端装置能够接收由互不相同

的第 1 和第 2 密钥进行加密的内容数据，根据互不相同的第 1 和第 2 许可信息，能够使用于利用内容数据的环境的变换方法，第 1 许可信息包含对由第 1 密钥进行加密的内容数据进行解密用的第 1 解密密钥。变换方法包含将面向第 1 终端装置的第 1 许可信息存入工作区的存储步骤、以及判断是否存于工作区的第 1 许可信息的构成要素中至少第 1 解密密钥的变换处理得到许可，在判断为变换处理得到许可的情况下，将第 1 许可信息的第 1 解密密钥置换为对第 2 密钥进行加密的内容数据进行解密用的第 2 解密密钥，以此将存于工作区的第 1 许可信息变换为面向所述第 2 终端装置的第 2 许可信息的变换步骤。

第 16 方面是从属于第 15 方面的，变换方法是作为用计算机装置执行的计算机程序来实现的。

第 17 方面是以属于第 16 方面的，变换方法是作为用计算机装置执行的计算机程序记录在记录介质中的。

附图说明

图 1 所示为本发明第 1～第 3 实施形态有关的变换装置 Uc1～Uc3 及它们的周边环境图。

图 2 所示为图 1 的服务器 21 及终端装置 22 的详细构成方框图。

图 3(a)为说明图 1 的经营者α准备的已加密内容数据 ect1 的说明图，图 3(b)所示为图 2 的内容数据库 211 的详细构成图。

图 4(a)及(b)所示为图 2 的解密密钥数据库 212 及用户信息数据 213 的详细构成图。

图 5 所示为图 2 的利用权数据库 214 的详细构成图。

图 6 所示为图 2 的服务器 31 及终端装置 32 的详细构成方框图。

图 7(a)及(b)所示为图 6 的内容数据库 311 及解密密钥数据库 312 的详细构成图。

图 8(a)及(b)所示为图 6 的用户信息数据库 313 及利用权数据库 314 的详细构成图。

图 9 所示为图 1 的变换装置 Uc1～Uc3 的构成方框图。

图 10 所示为图 1 的内容传送系统 Scd1 中内容传送时的服务器 21 及终端装置 22 的处理流程图。

图 11(a)所示为在图 10 的步骤 S11 生成的取得请求 Drr，图 11(b)所示为在图 10 的步骤 S16 读出的数据集 Dst1。

图 12 所示为图 1 的内容传送系统 Scd2 中许可信息提供时的服务器 21 及终端装置 22 的处理流程图的前半部分。

图 13 所示为图 1 的内容传送系统 Scd2 中许可信息提供时的服务器 21 及终端装置 22 的处理流程图的后半部分。

图 14(a)所示为在图 12 的步骤 S22 生成的发布请求 Dir，图 14(b)所示为在图 13 的步骤 S214 生成的许可信息 Dlc1。

图 15(a)所示为存入图 2 的格式存储单元 218 的格式数据 Dfm1，图 15(b)所示为图 1 的内容传送系统 Scd2 中使用的许可信息 Dlc2。

图 16 所示为存入图 6 的格式存储单元 318 的格式数据 Dfm2。

图 17 所示为图 9 所示的变换装置 Uc1 及图 2 的终端装置 22 在许可变换处理时的处理流程图的前半部分。

图 18 所示为图 9 所示的变换装置 Uc1 及图 2 的终端装置 22 在许可变换处理时的处理流程图的后半部分。

图 19(a)所示为在图 17 的步骤 S31 生成的变换请求 Dcr，图 19(b)及(c)所示为在图 17 的步骤 S35 生成的变换可否请求 Dc91 及 Dc92，图 19(d)及(e)所示为在图 17 的步骤 S39 生成的第 1 变换可否信息 Iack1 及 Iack2，图 19(f)及(g)所示为在图 17 的步骤 S35 生成的格式发送请求 Dfr1 及 Dfr2。

图 20 所示为本发明第 2 实施形态有关的变换装置 Uc2 在许可变换处理中接受了变换请求 Dcr 之后进行的处理的前半部分流程图。

图 21 所示为本发明第 2 实施形态有关的变换装置 Uc2 在许可变换处理中接受了变换请求 Dcr 之后进行的处理的后半部分流程图。

图 22 所示为在图 20 的步骤 S42 生成的格式/解密密钥发送请求 Dfd。

图 23(a)～(c)所示为第 3 实施形态中成为变换对象的许可信息 Dlc1。

图 24 所示为本发明第 3 实施形态有关的变换装置 Uc3 在许可变换处理中接受了变换请求 Dcr 之后进行的处理的前半部分流程图。

具体实施形态

第 1 实施形态

图 1 所示为本发明第 1 实施形态有关的变换装置 Uc1 及其周边环境的方框图。在图 1 中，变换装置 Uc1 通过有线或无线的传送路径 N，与内容传送系统 Scd1 及 Scd2 连接，并能够进行数据通信。另外，在内容传送系统 Scd1 中，至

少 1 个服务器 21 及至少 1 个终端装置 22 通过上述传送路径 N 连接，并能够进行数据通信。这里，服务器 21 设置在与作为内容传送一个例子的音乐传送有关的经营者α-侧，终端装置 22 根据与经营者α的合同，设置在接受音乐传送的签约者β-侧。另外，在内容传送系统 Scd2 中，至少 1 个服务器 31 及至少 1 个终端装置 32 通过上述传送路径 N 连接，并能够进行数据通信。这里，服务器 31 设置在与作为内容传送一个例子的音乐传送有关的经营者 r 一侧，终端设置 32 根据与经营者 r 的合同，设置在接受音乐传送的签约者δ一侧。这里，从本实施形态中容易理解说明的观点出发，假定经营者 r 是与经营者α不同的经营者，另外签约者δ是与签约者β是不同的签约者也可以签约者β与签约者δ是同一个人。即，既是签约者β而且又是签约者δ的同一用户加入互相不同的内容传送系统 Scd1 及 Scd2 的两个系统，具有终端装置 22 及终端装置 32 的两个终端装置，而对于这种情况本实施形态有关的变换装置 Uc1 也是有效的。

下面依次对内容传送系统 Scd1、Scd2 及变换装置 Uc1 分别说明其详细构成。

图 2 所示为图 1 所示的服务器 21 及终端装置 22 的详细构成方框图。在图 2 中，服务器 21 具有内容数据库(下面称为内容 DB)211、解密密钥数据库(下面称为解密密钥 DB)212、用户信息数据库(以下称为用户信息 DB)213 利用权数据库(下面称为利用权 DB)214、中央处理单元 215、工作区 216、通信单元 217 及格式存储单元 218。另外，终端装置 22 具有标识符存储单元 211、通信单元 222、中央处理单元 223、工作区 224 及存储装置 225。

下面说明在内容传送系统 Scd1 中，在签约者β从经营者α接受内容传送之前必须进行的有关准备工作。首先，由经营者α构筑图 2 的内容 DB211、解密密钥 DB212 及用户信息 DB213。

更具体来说，经营者α如图 3(a)所示，备有应该向签约者β提供的内容数据 Dct1。内容数据 Dct1 是用终端装置 22 能够利用的，在本实施形态中表示音乐。另外，经营者α对各内容数据 Dct1 分配内容标识符 Ict1。内容标识符 Ict1 是唯一确定内容数据 Dct1 的内容的代码。如上述内容数据 Dct1 表示音乐时，作为内容标识符 Ict1 能够适用的有 ISRC(International Standard Recording Code，国际标准记录代码)。关于 ISRC，已于 2001 年 7 月 23 日公布在 http://www.ifpi.org/index.html 上。

然后，经营者α对各内容数据 Dct1 分配加密密钥 Ke1。利用专用的加密密

钥 Ke1，将以上的内容数据 Dct1 进行加密，通过这样生成已加密内容数据 Dect1。内容 DB211 如图 3(b)所示，成为以上的内容标识符 Ict1 及已加密内容数据 Dect1 的组合的集合。在内容 DB211 中，内容标识符 Ict1 特别还唯一确定同一组的已加密内容数据 Dect1。另外，为了下面的说明方便起见，对于图 3(a)所示的 1 个已加密内容数据 Dect1，假定附加作为内容标识符 Ict1 的“a”。再有，该已加密内容数据 Dect1 假定是利用作为加密钥 Ke1 的“b”进行加密的。

然后，从服务器 21 向终端装置 22 传送上述已加密内容数据 Dect1。因此，必须向终端装置 22 提供能够将已加密内容数据 Dect1 进行解密的解密密钥 Kd1。所以，经营者α备有与内容 DB211 内的各加密密钥 Ke1(参照图 4(a))对应的解密密钥 Kd1。这里，解密密钥 Kd1 可以由与加密密钥相同的位串构成(公用密钥加密方式)，也可以由与该加密密钥 Ke1 不同的位串构成(公开密钥加密方式)。解密密钥 DB212 如图 4(a)所示，成为前述内容标识符 Ict1 及解密密钥 Kd1 的组合的集合。在解密密钥 DB212 中，解密密钥 Kd1 用于对能够用同一组的内容标识符 Ict1 确定的已加密内容数据 Dect1 进行解密。

另外，为了下面的说明方便起见，在图 4(a)中，对于与作为内容标识符 Ict1 的“a”相同的组，假定登录“c”作为解密密钥 Kd1。由上述可知，作为解密密钥 Kd1 的“c”与作为加密密钥 Ke1 的“b”相对应。

另外，上述的签约者β交换从经营者α接受音乐传送用的加入合同。根据加入合同，经营者α对签约者β分配终端标识符 Itn1。终端标识符 Itn1 在内容传送系统 Scd1 唯一确定签约者β的终端装置 22。用户信息 DB213 如图 4(b)所示，成为如上所示的终端标识符 Itn1 的集合。

这里再一次参照图 2。以上的终端标识符 Itn1 还进一步设定在签约者β一侧的终端装置 22 中的标识符存储单元 221。

另外，终端标识符 Itn1 也可以在终端装置 22 出厂时预先设定在标识符存储单元 221 中。在这种情况下，签约者β在上述加入合同的情况下，将终端装置 22 中设定的终端标识符 Itn1 通知经营者α。经营者α将通知的终端标识符 Itn1 登录在上述的用户信息 DB213 中。

另外，为了下面的说明方便起见，如图 4(b)所示，在用户信息 DB213 中对于终端装置 22 假定登录“x1”作为 1 个终端标识任 Itn1。在该假定的情况下，如图 2 所示，在标识符存储单元 221 中设定作为终端标识符 Itn1 的“x1”。

另外，在图 5 中所示为利用权 DB214，关于它的情况将在后面说明。

图 6 所示为图 1 所示的服务器 31 及终端装置 32 的详细构成方框图。在图 6 中，服务器 31 具有内容数据库(下面称为内容 DB)311、解密密钥数据库(下面称为解密密钥 DB)312、用户信息数据库(下面称为用户信息 DB)313、利用权数据库(下面称为利用权 DB)314、中央处理单元 315、工作区 316、通信单元 317 及格式存储单元 318。另外，终端装置 32 具有标识符存储单元 321、通信单元 322、中央处理单元 323、工作区 324 及存储装置 325。

在以上构成的内容传送系统 Scd2 中也与内容传送系统 Scd1 相同，首先，由经营者 r 构筑内容 DB311、解密密 DB312 及用户信息 DB313。

更具体来说，与参照图 3(a)所说明的相同，经营者 r 备有应该向签约者δ提供的内容数据 Dct2(未图示)。这里，内容数据 Dct2 在本实施形态中是用终端装置 32 能够利用的，表示音乐。另外，对各内容数据 Dct2 分配如前述的 ISRC 那样的唯一确定其内容的内容标识符 Ict2(参照图 7(a))。这里需要注意的是，虽然经营者α及 r 是独自备有内容数据 Dct1 及 Dct2，但有时它们表示互相相同的内容。若举其一个例子，如有时内容数据 Dct1 及 Dct2 双方表示由同一歌手唱的同一首歌曲。即，在本实施形态中，对于内容数据 Dct2 其表示的内容，具有与内容数据 Dct1 的同一性。对于具有这样同一性的内容数据 Dct1 及 Dct2，分配具有互相相同代码的内容标识符 Ict1 及 Ict2。

再进一步，对各内容数据 Dct2 分配加密密钥 Ke2(参照图 7(a))。利用专用的加密密钥 Ke2，将以上的内容数据 Dct2 进行加密，通过这样生成已加密内容数据 Dect2(参照图 7(a))。这里，在本实施形态中，假定内容传送系统 Scd1 及 Scd2 中的加密密钥 Ke2 与前述的加密密钥 Ke1 相同。

内容 DB311 如图 7(a)所示，成为内容标识符 Ict2 及已加密内容数据 Dect2 的组合的集合。这里需要注意的是，在以上的内容 DB311 中，至少 1 个已加密的内容数据 Dect2 与内容 DB211 的已加密内容数据 Dect1 具有前述的同一性。因而，对于具有这样同一性的已加密内容数据 Dect2，附加与对应的已加密内容数据 Dect1 所附加的内容标识符 Ict1 具有同一代码的内容标识符 Ict2。

另外，为了说明方便起见，假定图 7(a)所示的 1 个已加密内容数据 Dect2，用与加密密钥 Ke1 相同的作为加密密钥 Ke2 的“b”进行加密，并与图 3(b)的上端所示的已加密内容数据 Dect1 具有同一性。在该假定的情况下，对上述已加密内容数据 Dect2 附加表示与已加密内容数据 Dect1 的内容标识符 Ict1 相

同代码的“a”作为内容标识符 Ict2，而已加密内容数据 Dect1 与已加密内容数据 Dect2 本身具有同一性。

根据与经营者α的情况相同的理由，经营者 r 备有与内容 DB311 内的各加密密钥 Ke2 对应的解密密钥 Kd2。这里，解密密钥 Kd2 可以由与加密密钥 Ke2 相同的位串构成(公用密钥加密方式)，也可以由与该加密密钥 Ke2 不同的位串构成(公开密钥加密方式)。另外，在本实施形态中为了方便起见，假定解密密钥 Kd2 与前述的解密密钥 Kd1 相同。解密密钥 DB312 如图 7(b)所示，成为前述的内容标识符 Ict2 及解密密钥 Kd2 的组合的集合。

另外，为了说明方便起见，在图 7(b)中，对于与作为内容标识符 Ict2 的“a”相同的组，假定登录“c”作为解密密钥 Kd2。由上述可知，作为解密密钥 Kd2“c”用于对利用加密密钥 Ke2 的“b”的已加密内容数据 Dect2 进行解密。

另外，上述的签约者δ也交换从经营者 r 接受音乐传送用的加入合同。因而，经营者 r 与签约者δ，或者对签约者δ分配终端标识符 Itn2，或者从该签约者δ接受终端标识符 Itn2。终端标识符 Itn2 在内容传送系统 Scd2 中唯一确定签约者δ的终端装置 32。用户信息 DB313 如图 8(a)所示，成为如上所示的终端标识符 Itn2 的集合。另外，以上的终端标识符 Itn2 还进一步如图 6 所示，设定在终端装置 32 的标识符存储单元 321 中。

另外，为了说明方便起见，如图 8(a)所示，在用户信息 DB313 中假定登录“x2”作为 1 个终端标识符 Itn2。在该假定的情况下，如图 6 所示，在标识符存储单元 321 中设定作为终端标识符 Itn2 的“x2”。

另外，在图 8(b)中所示为利用权 DB314，关于它的情况将在后面说明。

图 9 所示为图 1 所示的变换装置 Uc1 的构成方框图。在图 9 中，变换装置 Uc1 具有程序存储单元 11、中央处理单元 12、工作区 13 及通信单元 14。程序存储单元 11 比较典型的是用 ROM 或硬盘驱动器构成，存储程序 Pc1。中央处理单元 12 根据程序 Pc1 工作，进行是本实施形态的特征的许可信息变换处理(参照图 17 及图 18)。工作区 13 在中央处理单元 12 进行各种处理时使用。通信单元 14 与前述的传送路径 N 连接，与内容传送系统 Scd1 及 Scd2 进行通信。

下面说明具有以上构成的变换装置 Uc1、内容传送系统 Scd1 及 Scd2 的工作情况。

下面，首先参照图 10，说明在内容传送系统 Scd1 中终端装置 22 从服务器 21 接受内容传送时的各部分的处理。首先，签约者β操作终端装置 22 访问服务

器 21，确定从存入内容 DB211 的内容数据 Dct1 中这次想要取得的内容数据的内容标识符 Ict1。在以后的说明中，将这次确定的内容数据 Dct1 称为取得对象内容数据 Dct1。然后，签约者β指定利用取得对象内容数据 Dct1 时的利用条件 Cct1。

下面对于利用条件 Cct1 更详细地进行说明。在内容数据 Dct1 表示音乐时，作为利用条件 Cct1 代表性的有有效期间、重放次数、最大连续重放时间、总重放时间或重放品质。另外，利用条件 Cct1 也可以是有效期间、再生次数、最大连续再生时间、总再生时间及再生品质中的 2 个以上(含 2 个)的组合。作为利用条件 Cct1 的有效期间，例如设定为从 2001 年 6 月 1 日至 2001 年 8 月 31 日，只要在设定的期间内，终端装置 22 能够再生内容数据 Dct1。再生次数例如设定为 5 次，只要在设定的次数内，终端装置 22 能够再生内容数据 Dct1。最大连续再生时间例如设定为 10 秒，是在终端装置 22 的 1 次再生中允许内容数据 Dct1 再生的最大时间。这样的最大连续再生时间对于音乐的推销是特别有效的。总再生时间例如设定为 10 小时，若是在设定的时间范围内，则终端装置 22 能够自由再生内容数据 Dct1。再生品质例如设定为 CD(Compact Disc，小型光盘)的品质，终端装置 22 能够以设定的重放品质重放内容数据 Dct1。另外，由于利用条件 Cct1 的种类不是本实施形态的本质性的事项，因此在该实施形态中，为方便起见，利用条件 Cct1 作为是内容数据 Dct1 的重放次数，接着进行以下的说明。

如上所述，签约者β操作终端装置 22，指定内容标识符 Ict1 及利用条件 Cct1。根据这样的指定，在终端装置 22 的工作区 224 上，存入内容标识符 Ict1 及利用条件 Cct1。对这些存储进行应答，中央处理单元 223 生成图 11(a)所示的取得请求 Drr(图 10 的步骤 S11)。取得请求 Drr 是向服务器 11 请求传送取得对象内容数据 Dct1 用的信息。若更具体地说明步骤 S11，则首先中央处理单元 223 将标识符存储单元 221 内的终端标识符 Itn1 传送至工作区 224。然后，中央处理单元 223 对工作区 224 上的终端标识符 Itn1、内容标识符 Ict1 及利用条件 Cct1 附加预定的取得请求标识符 Irr，生成取得请求 Drr(参照图 11(a))。这里，取得请求标识符 Irr 是为了服务器 21 确定取得请求 Drr 而使用的。

中央处理单元 223 将生成的取得请求 Drr，从工作区 224 传送至通信单元 222，通信单元 222 将接受的取得请求 Drr，通过传送路径 N 发送给服务器 21(步

骤 S12)。

在服务器 21(参照图 2)中，通信单元 217 接收来自传送路径 N 的取得请求 Drr，传送给工作区 216 并进行存储。对该存储进行应答，中央处理单元 215 确认与取得请求 Drr 中设定的终端标识符 Itn1 一致的终端标识符是否登录在上述的用户信息 DB213(参照图 4(b))中(步骤 S13)。在一致的终端标识符 Itn1 没有登录的情况下，中央处理单元 215 判断这次的取得请求 Drr 是签约者β以外的取得请求，将其删除(步骤 S14)，并结束处理。另外，在不是那样的情况下，中央处理单元 215 判断为接受了签约者β的取得请求 Drr，则进行利用权登录处理(步骤 S15)。

在步骤 S15，首先中央处理单元 215 确认该取得请求标识符 Irr，识别这次已接受了取得请求 Drr。然后，中央处理单元 215 从这次的取得请求 Drr 取出终端标识符 Itn1、内容标识符 Ict1 及利用条件 Cct1,将它们的组合登录在利用权 DB214 中。这里，利用取得请求 Drr，终端装置 22 不仅请求取得内容数据 Dct1，还请求取得对象内容数据 Dct1 的利用权。即，终端标识符 Itn1、内容标识符 Ict1 及利用条件 Cct1 的组合，表示终端装置 22 按照利用条件 Cct1 来利用取得对象内容数据 Dct1 的所谓权利。根据以上的观点，中央处理单元 215 将从取得请求 Drr 取出的组合作为利用权信息 Drgt1 来处理。即，利用权 DB214 如图 5 所示，成为由终端标识符 Itn1、内容标识符 Ict1 及利用条件 Cct1 构成的利用权信息 Drgt1 的组合的集合。

这里，说明登录在以上的利用权 DB214 中的利用的权信息 Drgt1 的具体例子。如已经说明的那样，在本实施形态中，假定利用条件 Cct1 是重放次数。再有，今次的取得请求 Drr 中，假定作为终端标识符 Itn1 设定为“x1”，作为内容标识符 Ict1 设定为“a”，作为利用条件 Cct1 设定为“重放 m 次”(m 为自然数)。在以上的假定情况下，如图 5 所示，在 1 个利用权信息 Drgt1 中，作为终端标识符 Itn1 设定为“x1”，作为内容标识符 Ict1 设定为“a”，作为利用条件 Cct1 设定为“重放 m 次”。

另外，虽然与本实施形态的技术性特征无关，但在步骤 S15 中，中央处理单元 215 每登录一次利用权信息 Drgt1，也可以对签约者β进行收费。

然后，中央处理单元 215 访问内容 DB211(参照图 3(b))，将根据这次的取得请求 Drr 所指定的内容标识符 Ict1、及分配了该内容标识符 Ict1 的已加密内容数据 Dect1 作为图 11(b)所示的数据集 Dst1，读出在工作区 216 上(步骤

S16)。

中央处理单元 215 将读出的数据集 Dst1，从工作区 216 传送给通信单元 217,通信单元 217 将接受的数据集 Dst1,通过传送路径 N 发送给终端装置 22(步骤 S17)。

在终端装置 22 中，通信单元 222 接收来自传送路径 N 的数据集 Dst1(步骤 S18)，传送给工作区 224 并进行存储。对该存储进行应答，中央处理单元 223 根据其中所含的内容标识符 Ict1，识别这次接收到发送的已加密内容数据 Dct1。然后，中央处理单元 223 将内容标识符 Ict1 及已加密内容数据 Dect1 存入存储装置 225(步骤 S19)。

根据数据权限保护的观点，终端装置 22 由于接收已加密内容数据 Dect1，因此为了利用它，就必须用服务器 21 提供的解密密钥 Kd1，将已加密内容数据 Dect1 进行解密。这里，在本内容传送系统 Scd1 中，为了将解密密钥 Kd1 提供给终端装置 22，要采用在后面详细说明的许可信息 Dlc1。

下面参照图 12 及图 13，说明终端装置 22 从服务器 21 接受所提供的许可信息 Dlc 时的各部分的处理。

首先，签约者β操作终端装置 22，从存入存储装置 225 的已加密数据 Dect1 中，指定这次想利用的已加密内容数据作为解密对象内容数据 Dect1。根据这样的指定结果，将解密对象内容数据 Dect1 及其内容标识符 Ict1 从存储装置 225 传送给工作区 224 并进行存储(图 12 的步骤 S21)。对这些存储进行应答，中央处理单元 223 生成图 14(a)所示的发布请求 Dir(步骤 S22)。发布请求 Dir 是为了请求服务器 21 提供许可信息 Dlc1、即为了接受解密对象内容数据 Dect1 的利用许可用的信息。若更具体地说明步骤 S22，则首先中央处理单元 223 将标识存储单元 221 内的终端标识符 Itn1 传送给工作区 224。然后，中央处理单元 223 对工作区 224 上的终端标识符 Itn1 及内容标识符 Ict1 附加预定的发布请求标识符 Iir，生成发布请求 Dir(参照图 14(a))。这里，发布请求标识符 Iir 是为了服务器 21 确定发布请求 Dir 而使用的。

中央处理单元 223 将生成的发布请求 Dir 从工作区 224 传送给通信单元 222,通信单元 222 将接受的发布请求 Dir,通过传送路径 N 发送给服务器 21(步骤 S23)。

在服务器 21(参照图 2)中，通信单元 217 接收来自传送路径 N 的发布请求 Dir，传送给工作区 216 并进行存储。对该存储进行应答，中央处理单元 215

对发布请求 Dir 进行与图 10 的步骤 S13 同样的处理(步骤 S24)，若没有成为对象的终端标识符 Itn1，则与前述的步骤 S14 相同，删除这次的发布请求 Dir(步骤 S25)。反之，若有成为对象的终端标识符 Itn1，则中央处理单元 215 首先确认该发布请求标识符 Iir，识别这次已接受了发布请求 Dir。

若这样进行识别，则中央处理单元 215 判别在利用权 DB214(参照图 5)中是否登录了包含与这次发布请求 Dir 内相同的终端标识符 Itn1 及内容标识符 Ict1 的利用权信息 Drgt1(步骤 S26)。

若以上那样的利用权信息 Drgt1 是未登录的，中央处理单元 215 生成表示拒绝利用解密对象内容数据 Dect1 的信息即利用拒绝，通过通信单元 217 及传送路径 N，发送给终端装置 22(步骤 S27)。在终端装置 22 中，中央处理单元 223 通过通信单元 222，接受利用拒绝(步骤 S28)。但是，从这以后，中央处理单元 223 就不进行对于解密对象内容数据 Dect1 的解密所必需的处理。如上所述，在本内容传送系统 Scd1 中，在利用权 DB214 中未登录利用权信息 Drgt1 的情况下，服务器 21 拒绝在终端装置 22 一侧进行解密。通过这样，能够保护前述的数据权限。

反之，在步骤 S26 中，若利用权信息 Drgt1 已登录，则中央处理单元 215 参照其所含的利用条件 Cct1，判断对终端装置 22 是否能够给予利用许可(步骤 S29)。若是不能赋予利用许可，则中央处理单元 215 执行上述的步骤 S27。结果，在终端装置 22 一侧不进行与解密对象内容数据 Dect1 的解密有关联的处理。如上所述，在本内容传送系统 Scd1 中，在利用权 DB114 中未登录有效的利用权信息 Drgt1 的情况下，也由于服务器 21 拒绝在终端装置 22 中进行解密，因此与上述相同，能够保护数字权限。

反之，在步骤 S29 中，若能够赋予利用许可，则中央处理单元 215 生成利用许可信息 Dlw1，存入工作区 216(步骤 S210)。利用许可信息 Dlw1 是对利用这次的发布请求 Dir 确定的终端装置 22 许可利用内容数据 Dct1 用的信息。但是，若无条件地对终端装置 22 赋予利用许可，则从保护前述的数字权限的观点来说是不利的，因此利用许可信息 Dlw1 最好表示在什么样的条件下对终端装置 22 给予利用许可。这里如前所述，利用权信息 Drgt1 的利用要件 Cct1 表示终端装置 22 在什么样的条件下利用内容数据 Dct1。根据以上的观点，在本实施形态中，利用许可信息 Dlw1 还最好表示在不超出利用条件 Cct1 的范围内终端装置 22 是许可利用的。

另外，在本实施形态中，通过生成利用许可信息 Dlw1，终端装置 22 能够使用利用权信息 Drgt1 的一部分或全部。因此，在步骤 S210 的下一个步骤，中央处理单元 215 更新使用过的利用权信息 Drgt1(步骤 S211)。

下面说明从以上的步骤 S26 到 S211 的处理的具体例子。现在假定在利用权 DB214 中如图 5 所示，登录了由作为终端标识符 Itn1 的“x1”、作为内容标识符 Ict1 的“a”及作为利用条件 Cct1 的“重放 m 次”构成的利用权信息 Drgt1。另外，假定这次的发布请求 Dir 包含作为终端标识符 Itn1 的“x1”及作为内容标识符 Ict1 的“a”。

在以上的假定情况下，在步骤 S26 中，判断为包含作为终端标识符 Itn1 的“x1”及作为内容标识符 Ict1 的“a”的利用权信息 Drgt1 已经登录。再有，在步骤 S29 中，由于在该利用权信息 Drgt1 中设定为“重放 m 次”，因此判断为对终端装置 22 能够给予利用许可。若如上所述判断的结果，则在步骤 S210 中生成利用许可信息 Dlw1。这时生成的利用许可信息 Dlw1 例如表示“重放 n 次”。这里，n 为不超过上述的 m 的自然数，最好是根据终端装置 22 的处理能力进行设定。例如，若是终端装置 22 装有较低性能的硬件时，n 最好设定为像“1”那样，设定为终端装置 22 能够利用解密对象内容数据 Dect1 的最低限度的值。另外，为方便起见，在本实施形态中，设 n=1，并继续进行说明。

根据以上所述，终端装置 22(终端标识符 Itn1 为“x1”)将使用 n 次内容数据 Dct1(内容标识符 Ict1 为“a”)的利用权。因此，在步骤 S211 中，利用条件 Cct1 从“重放 m 次”更新为“重放(m-n)次”。

在步骤 S211 的下一个步骤，中央处理单元 215 从解密密钥 DB212(参照图 4 (a))将与这次的发布请求 Dir 所包含的相同的内容标识符 Ict1 相同组的解密密钥 Kd1 读出给工作区 216(图 13 的步骤 S212)。接着，中央处理单元 215 从这次的发布请求 Dir 将终端标识符 Itn1 及内容标识符 Ict1 取出给工作区 216(步骤 S213)。利用以上的步骤 S213，在工作区 216 上汇总了终端标识符 Itn1、内容标识符 Ict1、利用许可信息 Dlw1 及解密密钥 Kd1。中央处理单元 215 然后将工作区 216 上的终端标识符 Itn1、内容标识符 Ict1、利用许可信息 Dlw1 及解密密钥 Kd1 依次排列，生成图 14(b)所示的许可信息 Dlc1(步骤 S214)。以上的许可信息 Dlc1 是对解密对象内容数据 Dect1 在终端装置 22 中的利用进行控制用的信息。另外，关于图 14(b)中的 p1～p4，将在后面叙述。

这里，若根据前述的假定，在这次的许可信息 Dlc1 中，终端标识符 Itn1

为“x1”，内容标识符 Ict1 为“a”，利用许可信息 Dlw1 为“1”，再有解密密钥 Kd1 为“c”。

中央处理单元 215 将以上那样生成的许可信息 Dlc1 从工作区 216 传送给通信单元 217，通信单元 217 将接受的许可信息 Dlc1,通过传送径 N 发送给终端装置 22(步骤 S215)。另外，由于许可信息 Dlc1 对于与签约者β无关的人员是不能利用的，因此服务器 21 及终端装置 22 最好在以 SSL(Secure Socket Layer，安全套接层)为代表的安全通信之下交换许可信息 Dlc1。

在终端装置 22 中，通信单元 222 接收来自传送路径 N 的许可信息 Dlc1，根据接收的许可信息 Dlc1，判断它是否是送往本地的信息(步骤 S216)。若接收的许可信息 Dlc1 不是送往本地的，则中央处理单元 223 不进行以后的处理。与此相反，在判断为接收了送往本地的许可信息 Dlc1 的情况下，中央处理单元 223 将它传送给工作区 224 并进行存储。对该存储进行应答，中央处理单元 223 参照这次的许可信息 Dlc1 内的利用许可信息 Dlw1，判断对解密对象内容数据 Dect1 是否赋予利用许可(步骤 S217)。

若没有赋予利用许可，则中央处理单元 223 不进行以后的处理。如上所述，在本内容传送系统 Scd1 中，只要不从服务器 21 赋予利用许可，终端装置 22 就不对解密对象内容数据 Dect1 进行解密。通过这样，能够保护前述的数字权限。

反之，在步骤 S217 中，若赋予利用许可，则中央处理单元 223 从接受的许可信息 Dlc1 取出解密密钥 Kd1(步骤 S218)。

下面说明以上的步骤 S217 及 S218 的具体例子。在上述的假定情况下，利用这次的许可信息 Dlc1 的利用许可信息 Dlw1，内容数据 Dct1 的重放仅许可 1 次。在这样的情况下，中央处理单元 223 由于利用许可信息 Dlw1 中设定的重放次数为“1”，因此在步骤 S217 中，判断为对解密对象内容数据 Dect1 赋予利用许可，在步骤 S218 中，从接受的许可信息 Dlc1 取出作为解密密钥 Kd1 的“c”。

然后，如前所述，在工作区 224 已经存入解密对象内容数据 Dect1(参照图 12 的步骤 S21)。中央处理单元 223 用步骤 S218 得到的解密密钥 Kd1，将该解密对象内容数据 Dect1 进行解密(步骤 S219)。通过这样，中央处理单元 223 能够得到内容数据 Dct1，从未图示的扬声器输出音乐。通过这样，签约者β能够听到喜欢的音乐。另外，中央处理单元 223 在本实施形态那样的利用许可信息

Dlw1 是表示重放次数的情况下，以上的内容数据 Dct1 每次结束重放，最好将这次的许可信息 Dlc1 中的利用许可信息 Dlw1 仅减少“1”。

另外，在图 6 所示的内容传送系统 Scd2 中也与内容传送系统 Scd1 相同，终端装置 32 接受服务器 31 传送的内容传送及提供的许可信息。由于在内容传送时，两者的处理情况若参照图 10 将可明白，在许可信息提供时，两者的处理情况若参照图 12 及图 13 将可明白，因此省略其说明。另外，许可信息提供时，服务器 31 参照图 8(b)所示的利用权 DB314，与许可信息 Dlc1 相同，生成在终端装置 32 中对内容数据 Dct2 的利用进行控制用的许可信息 Dlc2。

另外，在以上的说明中，内容数据 Dct1 不仅限于表示音乐，若是终端装置 22 能够利用的，则也可以是任何数据。作为例子，内容数据 Dct1 也可以表示电视节目、电影、广播电台节目、音乐、书籍或印刷品。另外，在以上的说明中，说明的是内容数据 Dct1 是表示音乐时的利用条件 Cct1。但是，不仅限于上述情况，利用条件 Dct1 最好根据内容数据 Dct1 表示的内容进行适当设定。在以上的说明中，由于了方便起见，内容数据 Dct1 表示音乐，因此说明的是终端装置 22 将在步骤 S218 中解密的内容数据 Dct1 表示的音乐从扬声器输出的情况。但是，不限于此，终端装置 22 也可以根据内容数据 Dct1 的种类，换成能够以图像输出电视节目、电影、书籍、印刷品及游戏内容的终端装置，或者换成能够以声音输出广播电台节目的终端装置。再有，终端装置 22 也可以具有将解密的内容数据 Dct1 能够传送给外部设备(电视接收机、收音机、音乐重放机、电子书籍阅读机、游戏机、PC、信息便携终端、移动电话及外部存储装置等)的接口。以上的情况也同样适用于内容传送系统 Scd2。

但是，在上述的说明中，是终端装置 22 使用由服务器 21 提供的许可信息 Dlc1，对内容数据 Dct1 的利用进行控制的情况。除此之外，还有的情况是，签约者β不使用内容数据 Dct1 而是想要转让自己的许可信息 Dlc1，给加入经营者 r 的内容传送的签约者δ。但是，以往的许可信息 Dlc1 的转让，由于内容传送系统 Scd1 及 Scd2 在各种各样方面由策略互相不同的经营者α及 r 进行管理，因此很困难。另外，在签约者β与签约者δ为同一个人时，也有的情况下用户想要在与内容传送系统 Scd2 对应的终端装置 32 中使用在内容传送系统 Scd1 中能够利用的许可信息 Dlc1。但是，以往这样的许可信息 Dlc1 的变更也因经营者α与 r 的互相不同的策略而很困难。

这里，在本实施形态中，假定经营者α与 r 的策略不同表现在许可信息 Dlc1

与 Dlc2 的格式上。这里，许可信息 Dlc1 已参照图 14(b)进行了说明，更具体来说是这样设定的，即终端标识符 Itn1 是从许可信息 Dlc1 的第 1 位算起，到 P1 位为止；内容标识符 Ict1 是从(P1+1)位起，到 P2 位为止；利用许可信息 Dlw1 是从(P2+1)位起，到 P3 位为止；再有解密密钥 Kd1 是从(P3+1)位起，到 P4 位为止。这里，P1～P4 是满足 P1<P2<P3<P4 的自然数。

表示以上许可信息 Dlc1 的格式的格式数据 Dfm1 存入服务器 21 的格式存储单元 218。如前所述，许可信息 Dlc1 由所谓终端标识符 Itn1、内容标识符 Ict1、利用许可信息 Dlw1 及解密密钥 Kd1 等构成要素构成。在这种情况下，格式数据 Dfm1 如图 15(a)所示，由相当于许可信息 Dlc1 的构成要素数的 4 组的要素信息 Imt11 及位的位置信息 Ibp11～要素信息 Imt14 及位的位置信息 Ibp14 构成。要素信息 Imt11 是确定终端标识符 Itn1。要素信息 Imt12 是确定内容标识符 Ict1。要素信息 Imt13 是确定利用许可信息 Dlw1。再有，要素信息 Imt14 是确定解密密钥 Kd1。另外，位的位置 Ibp11 由终端标识符 Itn1 的开始位的位置即 1 和其结束位的位置即 P1 构成。位的位置信息 Ibp12 由内容标识符 Ict1 的开始位的位置即(P1+1)和其结束位的位置即 P2 构成。位的位置信息 Ibp13 由利用许可信息 Dlw1 的开始位的位置即(P2+1)和其结束位的位置即 P3 构成。另外，位的位置信息 Ibp14 由解密密钥 Kd1 的开始位的位置即(P3+1)和其结束位的位置即 P4 构成。

另外，许可信息 Dlc2 是如上所述由服务器 32 生成的信息，如图 15(b)所示，包含终端标识符 Itn2、内容标识符 Ict2、利用许可信息 Dlw2 及解密密钥 Kd2。这里，利用许可信息 Dlw2 是对终端装置 32 中的内容数据 Dct2 的利用进行控制用的信息。是这样设定的，即终端标识符 Itn2 是从许可信息 Dlc2 的第 1 位算起，到 q1 位为止；内容标识符 Ict2 是从(q1+1)位起，到 q2 位为止；利用许可信息 Dlw2 是从(q2+1)位起，到 q3 位为止；再有解密密钥 Kd2 是从(q3+1)位起，到 q4 位为止。这里，q1～q4 是满足 q1<q2<q3<q4 的自然数。

这里需要注意的是，如前所述，许可信息 Dlc1 是对利用内容标识符 Ict1 确定的内容数据 Dct1 的利用进行控制的信息。因而，在许可信息 Dlc2 中，内容标识符 Ict2 必须是与根据许可信息 Dlc1 能够利用的内容数据 Dct1 具有同一性的内容数据 Dct2 的内容标识符。另外，在本实施形态中，对于相互具有同一性的内容数据 Dct1 及 Dct2，分配相同代码的内容标识符 Ict1 及 Ict2。根据上述情况，上述的 P1 及 q1 是作为相同的值，这样继续以下的说明。另外，

如前所述，在本实施形态中，假定解密密钥 Kd1 与 Kd2 是互相相同的。根据以上的情况，(p3-p2)与(q3-q2)作为相同的值，这样继续以下的说明。即，在本实施形态中，表现终端标识符 Itn1 及终端标识符 Itn2 用的位数和表现利用许可信息 Dlw1 及 Dlw2 用的位数是不相同的。

表示以上许可信息 Dlc2 的格式的格式数据 Dfm2 存入服务器 31 的格式存储单元 318。格式数据 Dfm2 如图 16 所示，与许可信息 Dlc2 的构成要素相关联，由 4 组要素信息 Imt21 及位的位置信息 Ibp21～要素信息 Imt24 及位的位置信息 Ibp24 构成。要素信息 Imt21 是确定终端标识符 Itn2。要素信息 Imt22 是确定内容标识符 Ict2。要素信息 Imt23 是确定利用许可信息 Dlw2。再有，要素信息 Imt24 是确定解密密钥 Kd2。另外，位的位置信息 Ibp21 由终端标识符 Itn2 的开始位的位置即 1 和其结束位的位置即 q1 构成。位的位置信息 Ibp22 由内容标识符 Ict2 的开始位的位置即(q1+1)和其结束位的位置即 q2 构成。位的位置信息 Ibp23 由利用许可信息 Dlw2 的开始位的位置即(q2+1)和其结束位的位置即 q3 构成。另外，位的位置信息 Ibp24 由解密密钥 Kd2 的开始位的位置即(q3+1)和其结束位的位置即 q4 构成。

如上所述，签约者δ一侧的终端装置 32 虽能够解释许可信息 Dlc2，但存在的问题是，即使照原样接受许可信息 Dlc1，也不能够解释。因此，变换装置 Uc1 要进行许可变换处理，将许可信息 Dlc1 的格式变换为在终端装置 32 中能够利用的格式。

下面参照图 17 及图 18，说明许可变换时的变换装置 Uc1 及终端装置 22 的处理情况。首先，签约者β操作终端装置 22，指定成为这次变换对它的许可信息 Dlc1。然后，签约者β操作终端装置 22，指定最终利用成为变换对象的许可信息 Dlc1 的终端标识符 Itn2。再进一步，签约者β操作终端装置 22，指定能够使用变换源的许可信息 Dlc1 的内容传送系统 Scd1 及格式变换宿的内容传送系统 Scd2。通过这样的指定，在工作区 224 上存入许可信息 Dlc1、终端标识符 Itn2、变换源确定信息 Ici 及变换宿确定信息 Idi(参照图 19(a))。这里，所谓变换源确定信息 Ici 是确定内容传送系统 Scd1 的服务器 21 的信息，所谓变换宿确定信息 Idi 是确定内容传送系统 Scd2 的服务器 31 的信息。

对以上的存储进行应答，中央处理单元 223 在工作区 224 上生成图 19(a)所示的变换请求 Dcr(图 17 的步骤 S31)。变换请求 Dcr 是对变换装置 Uc1 请求将上述许可信息 Dlc1 进行变换用的信息，如图 19(a)所示，包含终端标识符

Itn2、上述的变换源确定信息 Ici 及变换宿确定信息 Idi。

中央处理单元 223 将生成的变换请求 Dcr 及许可信息 Dlc1，从工作区 224 传送给通信单元 222。通信单元 222 将接受的变换请求 Dcr 及许可信息 Dlc1，通过传送路径 N 发送给变换装置 Uc1(步骤 S32)。另外，由于许可信息 Dlc1 对于与签约者β的无关人员不能利用，因此最好在以 SSL(Secure Socket Layer)为代表的安全通信下，变换装置与 Uc1 与终端装置 22 至少交换许可信息 Dlc1。

在变换装置 Uc1(参照图 9)中，通信单元 14 接收来自传送路径 N 的变换请求 Dcr 及许可信息 Dlc1，传送给工作区 13 并进行存储(步骤 S33)。对该存储进行应答 ，中央处理单元 12 根据程序存储单元 11 内的程序 Pc1 进行工作，首先从这次的变换请求 Dcr 取出终端标识符 Itn2、变换源确定信息 Ici 及变换宿确定信息 Idi(步骤 S34)。然后，中央处理单元 12 在工作区 13 上生成图 19(b)及(c)所示的变换可否请求 Dcq1 及 Dcq2(步骤 S35)。这里，变换可否请求 Dcq1 是对服务器 21 请求发送表示送来成为变换对象的许可信息 Dlc1 的终端装置 22 是否是内容传送系统 Scd1 的正当签约者β的第 1 变换可否信息 Iack1 用的信息，如图 19(b)所示，至少包含终端装置 22 的终端标识符 Itn1 及变换源确定信息 Ici。这里需要注意的一点是，变换装置 Uc1 由于与终端装置 22 的安全通信而确定了联系，因此即使变换请求 Dcr 中未设定终端标识符 Itn1，也能够取得终端标识符 Itn1。另外，变换可否请求 Dcq2 是对服务器 32 请求发送表示使用变换后的许可信息 Dlc2 的终端装置 32 是否是内容传送系统 Scd2 的正当签约者δ的第 1 变换可否信息 Iack2 用的信息，如图 19(c)所示，至少包含终端装置 32 的终端标识符 Itn2 及变换宿确定信息 Idi。

中央处理单元 12 将生成的变换可否请求 Dcq1 及 Dcq2，从工作区 13 传送给通信单元 14，通信单元 14 将接受的变换可否请求 Dcq1 及 Dcr2，通过传送路径 N 发送给服务器 21 及 31。(步骤 S36)

在服务器 21 及 31(参照图 2 及图 6)中，通信单元 217 及 317 接收来自传送路径 N 的变换可否请求 Dcq1 及 Dcq2，传送给工作区 216 及 316 并进行存储(步骤 S37)。在对存储的变换可否请求 Dcq1 及 Dcq2 进行解释之后，中央处理单元 215 及 315 检查分别在其中设定的终端标识符 Itn1 及 Itn2 是否登录在内容传送系统 Scd1 及 Scd2 的用户表(未图示)中(步骤 S38)。

然后，中央处理单元 215 及 315 的双方根据步骤 S38 的检查结果，在工作区 216 及 316 上生成图 19(d)及(e)所示的第 1 变换可否信息 Iack1 及 Iack2(步

骤 S39)。第 1 变换可否信息 Iack1 包含表示由服务器 21 在步骤 S38 的检查结果、即终端装置 22 是否是内容传送系统 Scd1 的正当用户的信息。另外，第 1 变换可否信息 Iack2 包含表示终端装置 32 是否是内容传送系统 Scd2 的正当用户的信息。

中央处理单元 215 及 315 将生成的第 1 变换可否信息 Iack1 及 Iack2，从工作区 216 及 316 传送给通信单元 217 及 317，通信单元 217 及 317 将接受的第 1 变换可否信息 Iack1 及 Iack2，通过传送路径 N 发送给变换装置 Uc1(步骤 S310)。

在变换装置 Uc1(参照图 9)中，通信单元 14 接收来自传送路径 N 的第 1 变换可否信息 Iack1 及 Iack2，存入工作区 13(步骤 S311)。然后，中央处理单元 12 对存储的第 1 变换可否信息 Iack1 及 Iack2 进行解释，判断终端装置 22 及 32 是否是内容传送系统 Scd1 及 Scd2 的正当用户(步骤 S312)。

中央处理单元 12 在判断为终端装置 22 及 23 即使某一方不是正当用户时，将这次的许可信息 Dlc1 送回终端装置 22(步骤 S313)。然后，图 17 及图 18 的处理结束。与此相反，在步骤 S312 中，判断为终端装置 22 及 23 的双方都是正当用户时，中央处理单元 12 在工作区 13 上，生成图 19(f)及(e)所示的格式发送请求 Dfr1 及 Dfr2(图 18 的步骤 S314)。这里，格式发送请求 Dfr1 及 Dfr2 是对用变换源确定信息 Ici 及变换宿确定信息 Idi 确定的服务器 21 及 31 请求发送格式数据 Dfm1 及 Dfm2 用的信息。

中央处理单元 12 将生成的格式发送请求 Dfm1 及 Dfm2，从工作区 13 传送给通信单元 14，通信单元 14 将接受的格式发送请求 Dfr1 及 Dfr2，通过传送路径 N 发送给服务器 21 及 31(步骤 S315)。

在服务器 21 及 31(参照图 2 及图 6)中，通信单元 217 及 317 接收来自传送路径 N 的格式发送请求 Dfr1 及 Dfr2，传送给工作区 216 及 316 并进行存储(步骤 S316)。在对存储的格式发送请求 Dfr1 及 Dfr2 进行解释之后，中央处理单元 215 及 315 将存入格式存储单元 218 及 318 的格式数据 Dfm1 及 Dfm2 取出给工作区 216 及 316(步骤 S317)。

中央处理单元 215 及 315 将取出的格式数据 Dfm1 及 Dfm2，从工作区 216 及 316 传送给通信单元 217 及 317，通信单元 217 及 317 将接受的格式数据 Dfm1 及 Dfm2，通过传送路径 N 发送给变换装置 Uc1(步骤 S318)。

在变换装置 Uc1(参照图 9)中，通信单元 14 接收来自传送路径 N 的格式数

据 Dfm1 及 Dfm2，传送给工作区 13 并进行存储(步骤 S319)。然后，中央处理单元 12 参照格式数据 Dfm1 及 Dfm2,将许可信息 Dlc1 变换为许可信息 Dlc2(步骤 S320)。

若更具体地说明步骤 S320，则在上述的假定情况下，通过比较格式数据 Dfm1 及 Dfm2，中央处理单元 12 识别利用许可信息 Dlw1 与利用许可信息 Dlw2 所使用的位数之不同。因此，中央处理单元 12 从许可信息 Dlc1 取出利用许可信息 Dlw1，并对其进行解释。然后，中央处理单元 12 将取出的利用许可信息 Dlw1 变换为相当于这样的解释结果的(q2-q1)位的利用许可信息 Dlw2(步骤 S321)。

进而，中央处理单元 12 从这次的变换请求 Dcr 取出终端标识符 Itn2(步骤 S322)。这里需要注意的是，如前所述，在内容标识符 Ict1 与 Ict2 中，假定双方的代码及位数相同，另外解密密钥 Kd1 与 Kd2 互相相同。因此，中央处理单元 12 照原样使用许可信息 Dlc1 的内容标识符 Ict1 及解密密钥 Kd1 作为许可信息 Dlw2 的内容标识符 Ict2 及解密密钥 Kd2。

利用以上的处理，在工作区 13 上汇总了许可信息 Dlc2 的构成要素即终端标识符 Itn2，内容标识符 Ict2，利用许可信息 Dlw2 及解密密钥 Kd2。然后，中央处理单元 12 根据格式数据 Dfm2 所示的位位置,将这些构成要素进行排列，组合成图 15(b)所示的许可信息 Dlc2(步骤 S323)。在上述的假定情况下，中央处理单元 12 按照终端标识符 Itn2、内容标识符 Ict2、利用许可信息 Dlw2 及解密密钥 Kd2 的顺序将它们进行排列。

利用以上的到步骤 S323 为止的处理，在工作区 13 上完成了从许可信息 Dlc1 变换得到的许可信息 Dlc2。然后，中央处理单元 12 将工作区 13 上的许可信息 Dlc2 传送给通信单元 14，通信单元 14 将接受的许可信息 Dlc2，通过传送路径 N 发送给终端装置 22(步骤 S324)。另外，由于许可信息 Dlc2 对于与签约者β无关的人员是不能利用的，因此变换装置 Uc1 及终端装置 22 最好在以 SSL(Secure Soctket Layer)为代表的安全通信之下交换许可信息 Dlc2。在终端装置 22(参照图 2)中,通信单元 222 接收来自传送路径 N 的许可信息 Dlc2(步骤 S325)。

如上所述，本实施形态有关的变换装置 Uc1 将面向签约者β的终端装置 22 的许可信息 Dlc1 变换为面向签约者δ的终端装置 32 的许可信息 Dlc2，返回该终端装置 22。通过这样，签约者β能够接受从自己的许可信息 Dlc1 加以变换、

而且在终端装置 32 一侧可正确使用的许可信息 Dlc2。签约者β将以上的许可信息 Dlc2 通过在线或离线方式交给签约者δ。这里，终端装置 32 根据签约者δ的操作，将包含接受的许可信息 Dlc2 内的内容标识符 Ict2 的内容取得请求发送给服务器 31。终端装置 32 使用许可信息 Dlc2，将上述结果得到的已加密内容数据 Dect2 进行解密后加以利用。通过在传送路径 N 上设置以上的变换装置 Uc1，能够解决以往的内容传送系统具有的问题，可将自己的许可信息 Dlc1 简单地转让给他人。

另外，以上的许可信息的变换处理本身不是用终端装置 22 执行的，而是用传送路径 N 上的变换装置 Uc1 执行的。通过这样，能够减轻终端装置 22 一侧为了进行变换处理的处理负担。

另外，在以上的第 1 实施形态中，是通过步骤 S35～312，变换装置 Uc1 使用通过与服务器 21 及 31 的通信而取得的第 1 变换可否信息 Iack1 及 Iack2，判断终端装置 22 及 32 是否是正当用户。但是，不限于此，变换装置 Uc1 也可以使用从服务器 21 及 31 以外取得的第 1 变换可否信息 Iack1 及 Iack2，进行步骤 S312 的判断，或者也可以使用预先保持在本地的辅助存储装置中的第 1 变换可否信息 Iack1 及 Iack2，进行步骤 S312 的判断。

第 2 实施形态

然而，在前述第 1 实施形态中，相互具有同一性的内容数据 Dct1 及 Dct2 是利用相同的加密密钥 Ke1 及 Ke2 进行加密的。因此，终端装置 22 及 32 使用互相相同的解密密钥 Kd1 及 Kd2，将加密的内容数据 Dect1 及 Dect2 进行解密。但是，有的情况下，由于经营者α与 r 的策略不同，因此在内容传送系统 Scd1 与 Scd2 之间使用不同的加密方式，结果终端装置 22 及 32 使用互相不同的解密密钥 Kd1 及 Kd2。在这种情况下可以预计到，使用由第 1 实施形态有关的变换装置 Uc1 变换的许可信息 Dlc2,会产生终端装置 32 不能将已加密内容数据 Dect2 进行解密的问题。因此，在第 2 实施形态中为了解决这样的问题，提供即使在内容传送系统 Scd1 与 Scd2 之间采用不同的加密方式、也可将终端装置 22 的许可信息 Dlc1 变换为终端装置 32 能够正确使用的许可信息 Dlc2 的变换装置 Uc2。

这里,变换装置 Uc2 的方框图构成与图 9 所示的变换装置 Uc1 的构成相同。另外，变换装置 Uc2 的周边环境与图 1 所示的相同。因此，在变换装置 Uc2 中，对于与变换装置 Uc1 的构成相当的部分附加相同的参照符号。但是需要注意的

一点是，在变换装置 Uc2 的程序存储单元 11 中存储的不是程序 Pc1，而是程序 Pc2。

下面说明许可变换时的变换装置 Uc2 及终端装置 22 的处理情况。在终端装置 22 一侧进行图 17 的步骤 S31 及 S32，将变换请求 Dcr 及许可信息 Dlc1 通过传送路径 N 发送给变换装置 Uc2。

在变换装置 Uc2(参照图 9)中，若通过传送路径 N 有变换请求 Dcr 及许可信息 Dlc1 送到，则开始执行程序 Pc2。更具体来说，中央处理单元 12 根据程序 Pc2，执行图 20 及图 21 所示的处理顺序。图 20 及图 21 若与图 18 进行比较，则一部分具有相同的步骤。因此，在图 20 及图 21 中，对于与图 18 的流程图的步骤相当的步骤附加相同的步骤编号，并简化其说明。

首先，中央处理单元 12 在变换请求 Dcr 及许可信息 Dlc1 送到后，在图 17 的步骤 S312 中，判断为终端装置 22 及 23 是内容传送系统 Scd1 及 Scd2 的正当用户后，如图 20 所示，仅使用变换源确定信息 Ici，进行与步骤 S314～S315 同样的处理，生成格式发送请求 Dfr1，并发送给服务器 21。结果，在变换装置 Uc2 的工作区 13 中，仅存储由服务器 21 发送的格式数据 Dfm1(参照步骤 S316～S319)。

然后，中央处理单元 12 从这次的许可信息 Dlc1 取出内容标识符 Ict1(图 21 的步骤 S41)。然后，中央处理单元 12 如图 22 所示，在工作区 13 上生成包含内容标识符 Ict1 的格式/解密密钥发送请求 Dfd(步骤 S42)。这里，格式/解密密钥发送请求 Dfd 是对用变换宿确定信息 Idi 确定的服务器 31 请求发送格式数据 Dfm2 及解密密钥 Kd2 用的信息。

中央处理单元 12 将生成的格式/解密密钥发送请求 Dfd，从工作区 13 传送给通信单元 14，通信单元 14 将接受的格式/解密密钥发送请求 Dfd，通过传送路径 N 发送给服务器 31(步骤 S43)。

在服务器 31(参照图 6)中，通信单元 317 接收来自传送路径 N 的格式/解密密钥发送请求 Dfd，传送给工作区 316 并进行存储(步骤 S44)。在对存储的格式/解密密钥发送请求 Dfd 进行解释之后，中央处理单元 315 首先将存入格式存储单元 318 的格式数据 Dfm2 取出给工作区 316(步骤 S45)。

然后，中央处理单元 315 从解密密钥 DB312 中，检索具有与这次的格式/解密密钥发送请求 Dfd 所包含的内容标识符 Ict1 相同代码的内容标识符 Ict2，再将与检索的内容标识符 Ict2 同一组的解密密钥 Kd2 读出给工作区 324(步骤

S46)。然后，中央处理单元 315 将工作区 316 上的格式数据 Dfm2 及解密密钥 Kd2 作为数据集 Dst2 传送给通信单元 317。通信单元 317 将接受的数据集 Dst2，通过传送路径 N 发送给变换装置 Uc2(步骤 S47)。在变换装置 Uc2(参照图 9)中，通信单元 14 接收来自传送路径 N 的数据集 Dst2，传送给工作区 13 并进行存储(步骤 S48)。

然后，中央处理单元 12 参照格式数据 Dfm1 及 Dfm2，将许可信息 Dlc1 变换为许可信息 Dlc2(步骤 S49)。

若更具体地说明步骤 S49，则首先中央处理单元 12 通过进行前述的步骤 S321，将利用许可信息 Dlw1 变换为利用许可信息 Dlw2，再通过进行步骤 S322，取出终端标识符 Itn2。然后，中央处理单元 12 从步骤 S48 中得到的数据集 Dst2 取出解密密钥 Kd2(步骤 S410)。另外，如前所述，中央处理单元 12 照原样使用许可信息 Dlc1 的内容标识符 Ict1 作为许可信息 Dlw2 的内容标识符 Ict2。

利用以上的处理，在工作区 13 上汇总了许可信息 Dlc2 的构成要素即内容标识符 Ict2、利用许可信息 Dlw2 及解密密钥 Kd2。然后，中央处理单元 12 将图 15(b)所示的许可信息 Dlc2 进行组合(步骤 S411)。这里，利用步骤 S410 及 S411，许可信息 Dlc1 的解密密钥 Kd1 转换成解密密钥 Kd2。然后，中央处理单元 12 执行步骤 S324，通过通信单元 14 及传送路径 N，将组合的许可信息 Dlc2 发送给终端装置 22。在终端装置 22(参照图 2)中，通信单元 222 执行步骤 S325，接收来自传送路径 N 的许可信息 Dlc2。

如上所述，本实施形态有关的变换装置 Uc2 与变换装置 Uc1 相同，将面向终端装置 32 的许可信息 D　lc2 返回终端装置 22。特别是变换装置 Uc2 使用许可信息 Dlc1 的内容标识符 Ict1，与服务器 32 进行数据通信，得到与之对应的内容标识符 Ict2 所附加的解密密钥 Kd2。变换装置 Uc2 在许可信息 Dlc2 中设定得到的解密密钥 Kd2。通过这样，即使在内容传送系统 Scd1 与 Scd2 之间采用不同的加密方式，也能够提供将终端装置 22 的许可信息 Dlc1 变换为终端装置 32 能够正确使用的许可信息 Dlc2 的变换装置 Uc2。

另外，在以上的第 2 实施形态中，是利用步骤 S47 及 S48，变换装置 Uc2 通过与服务器 31 进行通信而取得解密密钥 Kd2 的。但是，不限于此，变换装置 Uc2 对于解密密钥 Kd2。也可以使用从服务器 31 以外取得的解密密钥 Kd2，生成许可信息 Dlc2，或者也可以使用预先保持在本地的辅助存储装置中解密密钥 Kd2，生成许可信息 Dlc2。

第 3 实施形态

然而，在以往的实施形态中，变换装 Uc1 及 Uc2 这两者都是对来自终端装置 22 的变换请求 Dcr 进行应答，无条件地进行许可信息的变换处理的。但是，也有的情况下，根据经营者α的策略，有的利用条件 Cct1 想要从许可信息的变换处理的对象中去除。因此，在第 3 实施形态中，提供能够对许可信息的变换处理加以限制的变换装置 Uc3。

这里，变换装置 Uc3 的方框图构成与图 9 所示的变换装置 Uc1 的构成相同。另外，变换装置 Uc3 的周边环境与图 1 所示的相同。因此，在变换装置 Uc3 中，对于与变换装置 Uc1 的构成相当的部分附加相同的参照符号。但是需要注意的一点是，在变换装置 Uc3 的程序存储单元 11 中存储的不是程序 Pc1，而是程序 Pc3。

下面说明许可变换时的变换装置 Uc3 及终端装置 22 的处理情况。在终端装置 22 一侧进行图 17 的步骤 S31 及 S32，将变换请求 Dcr 及许可信息 Dlc1 通过传送路径 N 发送给变换装置 Uc3。这里，在本实施形态中，许可信息 Dlc1 若与图 14(b)所示的进行比较，则不同点在于如图 23(a)所示，是附加了第 2 变换可否信息 Ica1。除此以外由于两个许可信息 Dlc1 之间没有不同点，因此在图 23(a)中，附加与图 14(b)所示的信息相同的参照符号，并分别省略说明，第 2 变换可否信息 Ica1 是根据经营者α的策略附加的、表示是否同意对相同许可信息 Dlc1 所包含的利用许可信息 Dlw1 进行变换处理的信息。

下面参照图 23(b)及(c)，举出两个第 2 变换可否信息 Ica1 的具体例子。首先，在图 23(b)中，许可信息 Dlc1 包含终端标识符 Itn1、内容标识符 Ict1、第 2 变换可否信息 Ica1、作为多个利用许可信息 Dlw1 的一个例子的利用许可信息 Dlw11 及 Dlw12、以及解密密钥 Kd1。利用许可信息 Dlw11 例如表示重放次数，利用许可信息 Dlw12 例如表示打印次数。第 2 变换可否信息 Ica1 表示是否允许对这样的全部利用许可信息 Dlw11 及 Dlw12 进行变换处理。另外，在图 23(c)中，许可信息 Dlc1 包含终端标识符 Itn1、内容标识符 Ict1、作为 1 个或多个第 2 变换可否信息 Ica1 与利用许可信息 Dlw1 的组合的一个例子的第 2 变换可否信息 Ica11 与利用许可信息 Dlw11 和第 2 变换可否信息 Ica12 与利用许可信息 Dlw12、以及解密密钥 Kd1。利用许可信息 Dlw11 及 Dlw12 如上所述，例如表示重放次数及打印次数。第 2 变换可否信息 Ica11 表示是否同意对同一组的利用许可信息 Dlw11 进行变换处理，第 2 变换可否信息 Ica12 表示是

否同意对同一组的利用许可信息 Dlw12 进行变换处理。

在变换装置 Uc3(参照图 9)中，若通过传送路径 N 有来自终端装置 22 的变换请求 Dcr 及许可信息 Dlc1 送到，则开始执行程序 Pc3。更具体来说，中央处理单元 12 根据程序 Pc3，执行图 24 所示的处理顺序。图 24 若与图 17 进行比较，则一部分具有相同的步骤。因此，在图 24 中，对于与图 17 的流程图的步骤相当的步骤附加相同的步骤编号，并简化其说明。

首先，中央处理单元 12 在变换请求 Dcr 及许可信息 Dlc1 送到后，检查第 2 变换可否信息 Ica1，判断是否允许对全部利用许可信息 Dlw1 进行变换处理(步骤 S51)。若不允许对全部利用许可信息 Dlw1 进行变换处理，则中央处理单元 12 将这次接收的许可信息 Dlc1 送回终端装置 22(步骤 S52)，并结束图 24 的处理。另外，变换装置 Uc3 也可以在步骤 S51 之前，进行步骤 S35 及 S36(参照图 17)，在从服务器 21 及 31 取得第 1 变换可否信息 Iack1 及 Iack2 之后，判断终端装置 22 及 32 是否是内容传送系统 Scd1 及 Scd2 的正当用户，然后进行步骤 S51。

与此相反，在步骤 S51 中，在判断为允许对一部分或全部利用许可信息 Dlw1 进行变换处理的情况下，中央处理单元 12 如在第 1 实施形态中说明的那样，将变换请求 Dcr 及许可信息 Dlc1 进行存储(步骤 S33)。然后，中央处理单元 12 根据第 2 变换可否信息 Ica1，判断的否允许对全部利用许可信息 Dlw1 进行变换(步骤 S53)。在允许对全部利用许可信息 Dlc1 进行变换时，中央处理单元 12 进行从步骤 S34 至 S316(参照图 18)的处理。

与此相反，在步骤 S53 中，在判断为允许对一部分利用许可信息 Dlw1 进行变换处理时，中央处理单元 12 根据第 2 变换可否信息 Ica1 进行分类，分成允许进行变换处理的利用许可信息 Dlw1 及不允许进行变换处理的利用许可信息 Dlw1。(步骤 S54)然后，中央处理单元 12 将不允许进行变换处理的利用许可信息 Dlw1 送回终端装置 22(步骤 S55)，然后将允许进行变换处理的利用许可信息 Dlw1 作为对象，进行从步骤 S34 至 S316(参照图 18)的处理。

利用以上的处理，本实施形态有关的变换装置 Uc3 通过使用第 2 变换可否信息 Ica1，能够对许可信息的变换处理加以限制。通过这样，能够实现可反映经营者α的策略的变换装置 Uc3。

另外，在第 3 实施形态中，说明的是第 2 变换可否信息 Ica1 是作为附加在许可信息 Dlc1 中的情况。但是，第 2 变换可否信息 Ica1 也可以不附加在许

可信息 Dlc1 中。在这种情况下，变换装置 Uc3 在例如变换请求 Dcr 及许可信息 Dlc1 送到后，比较典型的是向服务器 31 询问并取得与各利用许可信息 Dlw1 对应的第 2 变换可否信息 Ica1，然后进行步骤 S51 以后的处理。另外，变换装置 Uc3 也可以对内容传送系统 Scd1 中使用的每个利用许可信息 Dlw1，将第 2 变换可否信息 Ica1 预先保持在本地的辅助存储设置中，在变换请求 Dcr 及许可信息 Dlc1 送到后，使用本地的第 2 变换可否信息 Ica1，进行步骤 S51 以后的处理。

另外，在第 3 实施形态中，中央处理单元 12 是在步骤 S54 中进行分类，分为允许进行变换处理的利用许可信息 Dlw1 及不允许进行变换处理的利用许可信息 Dlw1。结果有的情况下，仅剩下单独 1 个利用许可信息 Dlw1 作为步骤 S34 以后的处理对象。还有的情况下，这样的利用许可信息 Dlw1 如果单独就没有意义。例如，在利用许可信息 Dlw1 是表示内容数据 Dect1 的复制许可时，即使终端装置 23 取得了变换后的许可信息 Dlc2，但因仅仅终端装置 22 能够复制内容数据 Dect1。因此仍不能重放或打印内容数据 Dect1。即，这样的许可信息 Dlc2 如果单独就没有意义。为了避免这样的无意义的许可信息进行变换处理，中央处理单元 12 最好检查步骤 S54 中剩下的利用许可信息 Dlw1 的内容，判断它们是否是有意义的，并将没有意义的不作为步骤 S34 以后的处理对象。

另外，在第 3 实施形态中，中央处理单元 12 在步骤 S52 及 S55 中，是将不允许进行变换处理的利用许可信息 Dlw1 送回终端装置 22，但不限于此，中央处理装置 12 也可以在内容传送系统 Scd2 中，在将许可信息 Dlc1 中设定的利用许可信息 Dlw1 不作为利用许可信息定义时，判断为不允许进行变换处理，然后在步骤 S55 中将利用允许进行变换处理，然后在步骤 S55 中将利用许可信息 Dlw1 送回终端装置 22。另外，在这样判断时，变换装置 Uc3 也可以在本地或远程的辅助存储装置中保持不能变换的利用权信息 Dlw1，或者也可以返回服务器 31。

另外，在以上的第 1～第 3 实施形态中，是签约者β为了将自己的许可信息 Dlc1 转让给签约者δ，而使用变换装置 Uc1～Uc3。但是，变换装置 Uc1～Uc3 也可以应用于其它状况，例如签约者β通过某种方法获得第 2 内容传送系统 Scd2 中能够使用的许可信息 Dlc2，并将获得的许可信息 Dlc2 变换为自己加入的内容传送系统 Scd1 中能够利用的许可信息 Dlc1，这样的状况也可以应用。另外，在将获得的许可信息 Dlc2 变换为自己没有加入的其它内容传送系统中能够利

用的许可信息时，也可以应用变换装置 Uc1～Uc3。

另外，在以上的第 1～第 3 实施形态中，在步骤 S314(参照图 18 及图 21)，变换装置 Uc1～Uc3 是将变换后的许可信息 Dlc2 返回终端装置 22。但是，不限于此，终端装置 22 将唯一确定成为许可信息 Dlc2 的转让目标之终端装置 32 的信息与变换请求 Dcr 一起发送给变换装置 Uc1～Uc3。然后，变换装置 Uc1～Uc3 也可以根据接受的信息，将变换后的许可信息 Dlc2 发送给终端装置 32。若归纳起来讲，变换后的许可信息 Dlc2 也可以通过随便什么方法交给终端装置 32。

另外，在第 1 实施形态中，是变换装置 Uc1 对许可信息进行变换处理的。但是，也可以将由前述步骤 S314 至 S323 的处理(参照图 18)构成的程序预先存入终端装置 22，来代替变换装置 Uc1。另外，在第 2 实施形态中，是变换装置 Uc2 对许可信息进行变换处理的。但是，也可以将由前述步骤 S314 至 S411 的处理(参照图 20 及图 21)构成的程序预先存入终端装置 22，来代替变换装置 Uc2。另外，在第 3 实施形态中，是变换装置 Uc3 对许可信息进行变换处理的。但是，也可以使终端装置 22 进行前述步骤 S51(参照图 24)以后的处理，来代替变换装置 Uc3。利用这些方法，终端装置 22 能够通过自己本身将面向自己的许可信息 Dlc1 变换为面向终端装置 32 的许可信息 Dlc2。这样，由于终端装置 22 不需要与变换装置 Uc1～Uc3 进行数据通信，因此能够减少通信成本等，而且能够迅速得到面向终端装置 32 的许可信息 Dlc2。

另外，在以上的第 1～第 3 实施形态中，变换装置 Uc1～Uc3 是将对终端装置 22 发布的许可信息 Dlc1 变换为在终端装置 23 能够利用的许可信息 Dlc2。但是，并不限于此，变换装置 Uc1～Uc3 也可以将例如分配给签约者β的利用权信息 Drgt1(参照图 5)进行变换，生成别的签约者δ用的利用权信息 Drgt2。即，对于许可信息 Dlc1，不限于在第 1～第 3 实施形态中说明的那样，也可以包含图 5 所示的利用权信息 Drgt1。另外，作为这时典型的处理，变换装置 Uc1～Uc3 将利用权信息 Drgt1 中设定的确定签约者β用的标识符(图 5 中未图示)，变换为确定签约者δ用的标识符。

另外，在以上的第 1～第 3 实施形态中，作为许可信息的变换处理是采用对利用许可信息 Dlw1 及 Dlw2 的位数进行调整为例进行说明的，但不限于此，例如有的情况下许可信息 Dlc1 与 Dlc2 是用互相不同的字符集生成的。在这种情况下，各变换装置 Uc1～Uc3 与服务器 21 及 31 的双方进行通信，确认在内

容传送系统 Scd1 及 Scd2 中使用什么样的字符集。根据这样的确认结果，各变换装置 Uc1～Uc3 也可以将许可信息 Dc11 的字符集变换为许可信息 Dlc2 的字符集。另外，变换装置 Uc1～Uc3 在预先保持描述内容传送系统 Scd1 及 Scd2 的双方中使用什么样字符集的表格时，也可以参照该表格，将许可信息 Dlc1 的字符集变换为许可信息 Dlc2 的字符集。

另外，许可信息 Dlc1 及 Dlc2 也可以用以 XML(eXtensible Markup Language，可扩展标记语言)或 XrML(eXtensible rights Markup Language，可扩展权限标记语言)为代表的描述语言来描述。在这种情况下，变换装置 Uc1～Uc3 也可以将 XML 或 XrML 的标签值进行变换，或者将描述语言本身进行变换，这样进行从许可信息 Dlc1 向 Dlc2 的变换处理。

另外还有的情况下，许可信息 Dlc1 与 Dlc2 的构成要素互相不同。其典型的例子是，在许可信息 Dlc1 中有利用许可信息 Dlw1，而在许可信息 Dlc2 中没有与其相当的利用许可信息 Dlw2。在这样的情况下，变换装置 Uc1～Uc3 也与服务器 21 及 31 的双方进行通信，确认在内容传送系统 Scd1 及 Scd2 的双方中使用什么样的构成要素来构成许可信息 Dlc1 及 Dlc2。根据这样的确认结果，变换装置 Uc1～Uc3 也可以将许可信息 Dlc1 的构成要素进行变换处理，使其与许可信息 Dlc2 的构成要素一致。另外，变换装置 Uc1～Uc3 在预先保持描述内容传送系统 Scd1 及 Scd2 的双方中使用什么样的构成要素来构成许可信息 Dlc1 及 Dlc2 的表格时，也可以参照该表格，将许可信息 Dlc1 的构成要素进行变换处理，使其与许可信息 Dlc2 的构成要素一致。

另外还有的情况下，许可信息 Dlc1 与 Dlc2 的构成要素本身虽然相同，但是该许可信息 Dlc1 及 Dlc2 中的构成要素的排列互相不同。在这样的情况下，各变换装置 Uc1～Uc3 也与服务器 21 及 31 的双方进行通信，确认在内容传送系统 Scd1 及 Scd2 的双方中以什么样的构成要素排列来构成许可信息 Dc1 及 Dlc2。根据这样的确认结果，各变换装置 Uc1～Uc3 也可以将许可信息 Dlc1 的构成要素排列进行变换处理，使其与许可信息 Dlc2 的构成要素排列一致。另外，各变换装置 Uc1～Uc3 在预先保持描述内容传送系统 Scd1 及 Scd2 的双方中以什么样的构成要素排列来构成许可信息 Dlc1 及 Dlc2 的表格时，也可以参照该表格，将许可信息 Dlc1 的构成要素排列进行变换处理，使其与许可信息 Dlc2 的构成要素排列一致。

另外，在第 1～第 3 实施形态中，是作为对具有同一性的内容数据 Dct1 及

Dct2 分配具有互相相同代码的内容标识符 Ict1 及 Ict2 进行说明的。但是，并不限于此，也可以对具有同一性的内容数据 Dct1 及 Dct2 分配在内容传送系统 Scd1 及 Scd2 中具有唯一性代码的内容标识符 Ict1 及 Ict2。但是，在这样的情况下，各变换装置 Uc1～Uc3 必须将许可信息 Dlc1 所包含的内容标识符 Ict1 变换为内容标识符 Ict2。因此，变换装置 Uc1～Uc3 最好预先保持描述内容传送系统 Scd1 及 Scd2 中对互相具有同一性的内容数据 Dct1 及 Dct2 所分配的内容标识符 Ict1 与 Ict2 之对应关系的表格。变换装置 Uc1～Uc3 参照这样的表格，将许可信息 Dlc1 所包含的内容标识符 Ict1 变换为内容标识符 Ict2。

另外，在第 1～第 3 实施形态中，变换装置 Uc1～Uc3 是从终端装置 22 接受成为变换处理对象的许可信息 Dlc1。但是，并不限于此，变换装置 Uc1～Uc3 也可以与服务器 21 进行数据通信，取得面向终端装置 22 的许可信息 Dlc1。

另外，在第 1～第 3 实施形态中，服务器 21 是将内容数据 Dct1 及许可信息 Dlc1 在各自不同的时间发送给终端装置 22 的。但是，并不限于此，服务器 21 也可以将许可信息 Dlc1 作为电子水印，埋入内容数据 Dct1 中，将该内容数据 Dct1 同时发送给终端装置 22。对于这一点，服务器 31 也相同。

另外，在第 1～第 3 实施形态中，各变换装置 Uc1～Uc3 是从服务器 21 及 31 通过通信取得格式数据 Dfm1 及 Dfm2 的(步骤 S315～步骤 S319)。通过这样，各变换装置 Uc1～Uc3 平时在辅助存储装置中不需要预先保持格式数据 Dfm1 及 Dfm2。但是，并不限于通过通信取得，变换装置 Uc1～Uc3 也可以在本地的辅助存储装置中具有格式数据 Dfm1 及 Dfm2。通过这样，变换装置 Uc1～Uc3 也可以在本地的辅助存储装置中具有格式数据 Dfm1 及 Dfm2。通过这样，变换装置 Uc1～Uc3 由于不需要与服务器 21 及 31 进行通信，因此能够高速对许可信息进行变换处理。

另外，在第 1～第 3 实施形态中，各变换装置 Uc1～Uc3 是将许可信息 Dlc1 的格式变换为许可信息 Dlc2 的格式作为许可信息的变换处理的例子(步骤 S320)。更具体来说，是在利用许可信息 Dlw1 中，作为利用条件 Cct1 的重放次数设定为 1 次，变换装置 Uc1～Uc3 将这样的利用许可信息 Dlw1 变换为重放次数设定为 1 次的利用许可信息 Dlw2。但是，并不限于这样的格式变换。变换装置 Uc1～Uc3 也可以改变许可信息 Dlc1 所包含的利用条件 Cct1 本身，生成包含不同利用条件 Cct2 的许可信息 Dlc2。更具体来说，变换装置 Uc1 使用利用条件 Cct1 与 Cct2 的变换比例，将许可信息 Dlc1 的利用条件 Cct1 变换为利

用条件 Cct2。通过这样，例如将作为利用条件 Cct1 的重放次数 n_1 变换为作为利用条件 Cct2 的重放次数 n_2。作为其它的例子，在内容数据 Dct1 是表示静止图像时，将作为利用条件 Cct1 的重放次数 n1 变换为作为利用条件 Cct2 的打印次数 n_2。再有，将作为利用条件 Cct1 的有效期间变换为作为利用条件 Cct2 的无限期的利用期间。另外，变换装置 Uc1～Uc3 也可以与格式数据 Dfm1 等同样从外部取得变换比例，或者也可以保持在本地。

另外，在以上第 1～第 3 实施形态中，程序 Pc1～Pc3 是存储在变换装置 Uc1～Uc3 中。但是，并不限于此，程序 Pc1～Pc3 也可以记录在 CD-ROM 为代表的记录介质中的状态进行发布，或者也可以通过传送路径 N 进行传送。

另外，在以上的第 1～第 3 实施形态中，变换装置 Uc1～Uc3 也可以在服务器 21 及 31 和终端装置 22 及 32 中的所需要部分安装防窜改技术。另外，也可以至少对利用许可信息 Dlw1 附加以散列为代表的为了检测窜改所必需的信息。

工业应用性

本发明有关的变换装置能够用于内装有 DRM(Digital Rights Management)即权限管理技术的系统。

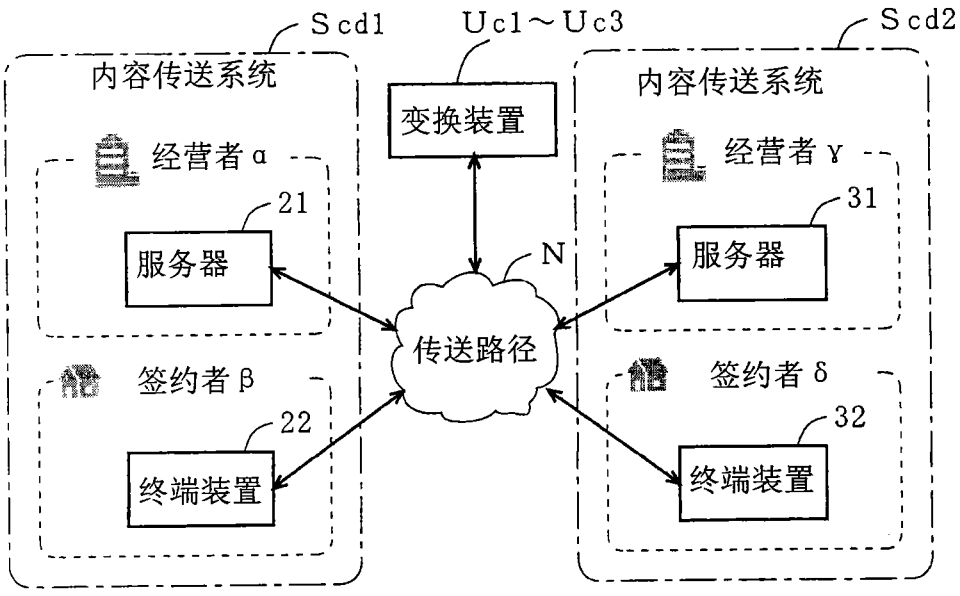

Scd1
Uc1～Uc3
Scd2
内容传送系统
变换装置
内容传送系统
经营者α
经营者γ
21
31
服务器
N
服务器
传送路径
签约者β
签约者δ
22
32
终端装置
终端装置

图 1

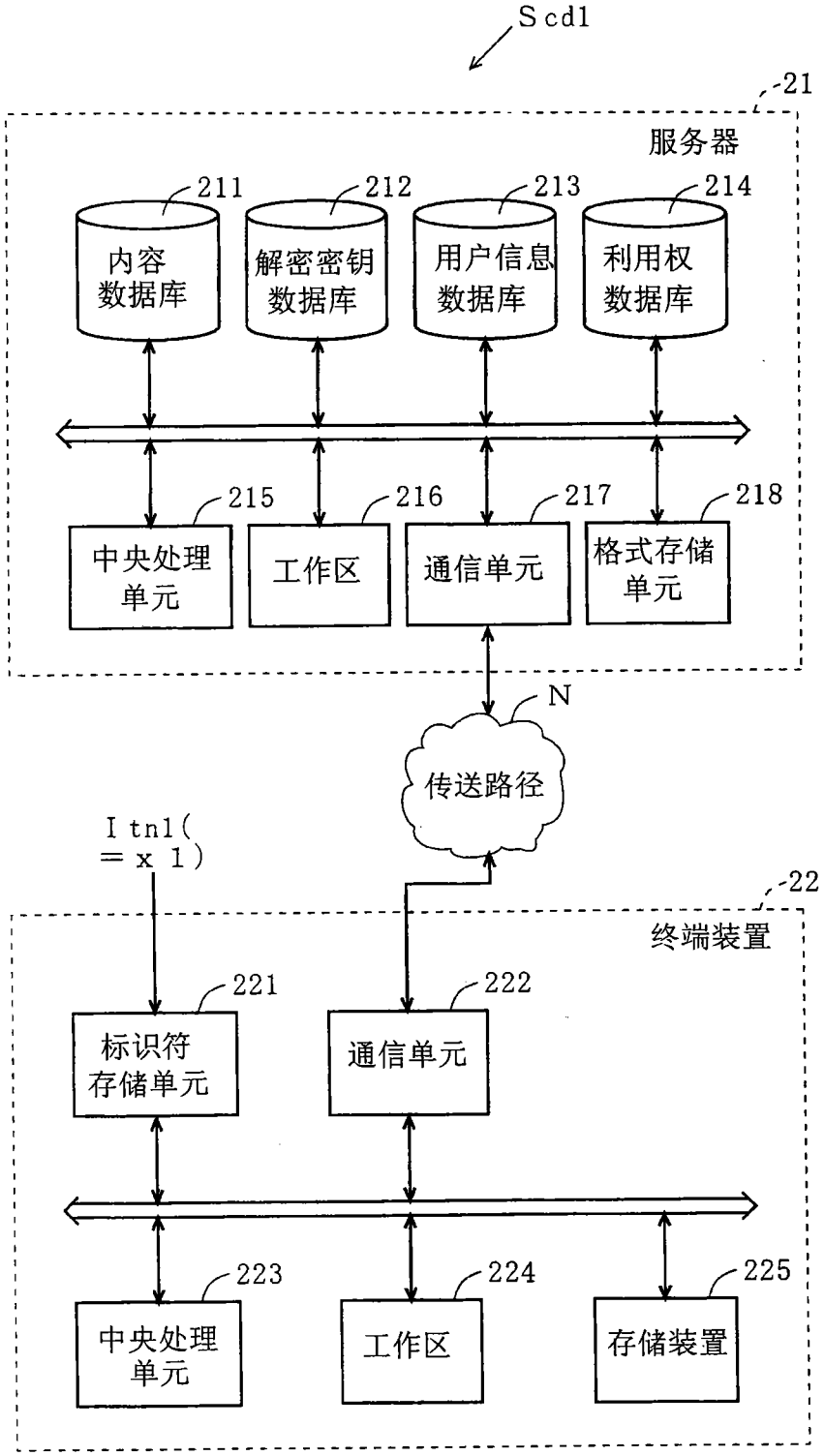
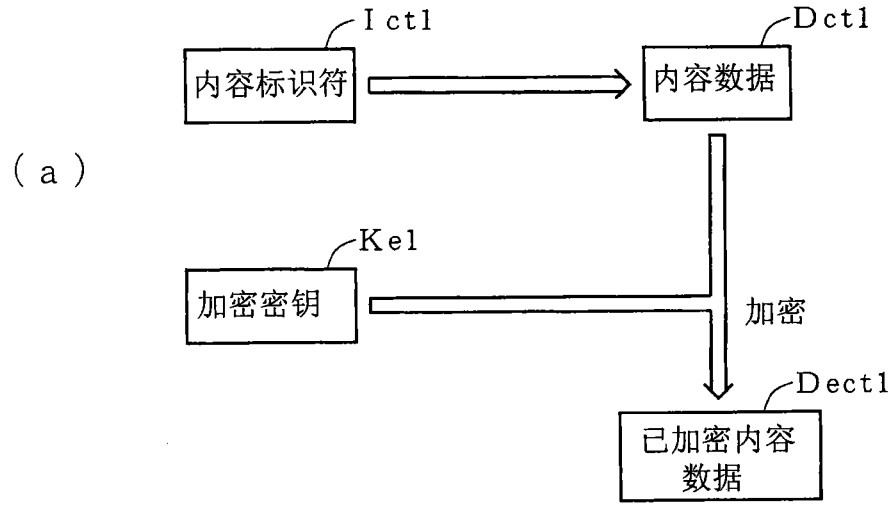

Scd1
21
服务器
211
212
213
214
内容数据库
解密密钥数据库
用户信息数据库
利用权数据库
215
216
217
218
中央处理单元
工作区
通信单元
格式存储单元
N
传送路径
Itn1(=x 1)
22
终端装置
221
222
标识符存储单元
通信单元
223
224
225
中央处理单元
工作区
存储装置

图 2


（a）
Ict1
内容标识符
Dct1
内容数据
Kel
加密密钥
加密
Dect1
已加密内容数据

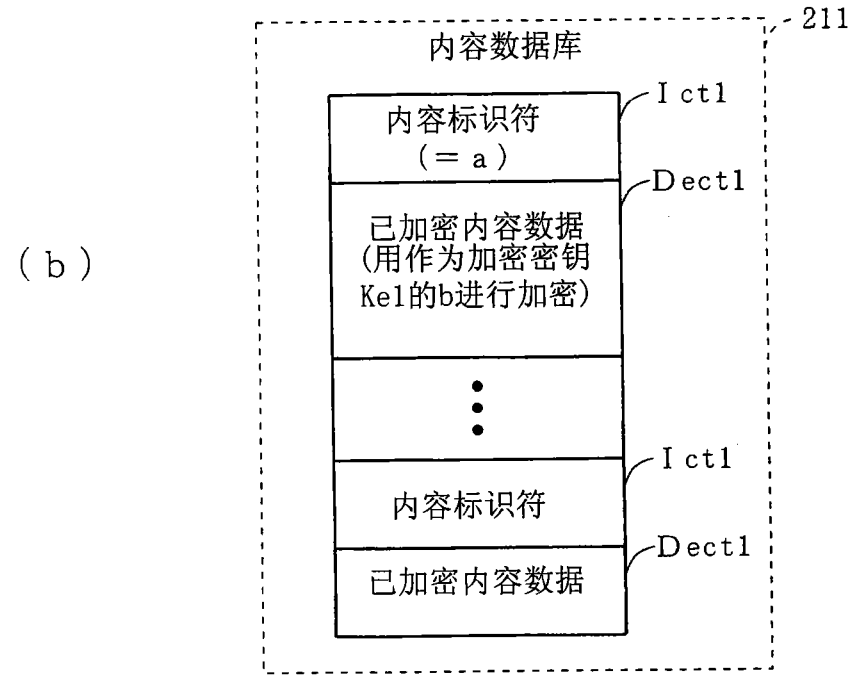
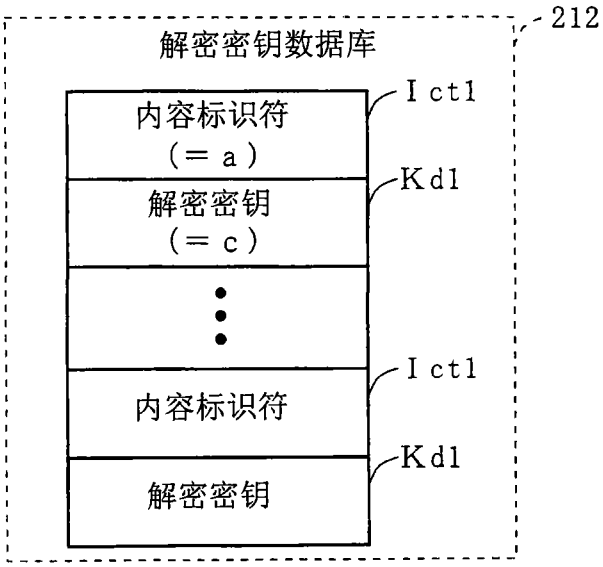

（b）
211
内容数据库
内容标识符
（＝a）
Ict1
Dect1
已加密内容数据
(用作为加密密钥
Kel的b进行加密)
Ict1
内容标识符
Dect1
已加密内容数据

图 3

（a）


212
解密密钥数据库
内容标识符
（＝a）
Ict1
解密密钥
（＝c）
Kd1
内容标识符
Ict1
解密密钥
Kd1

（b）

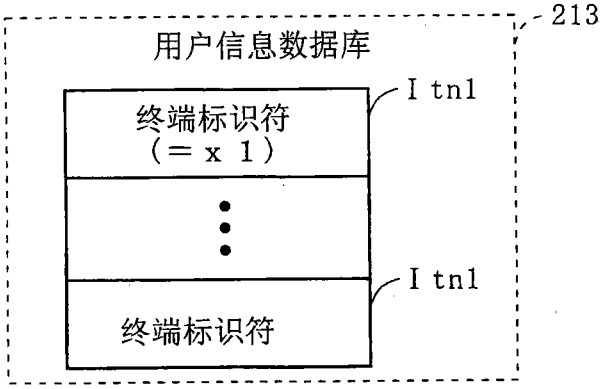

213
用户信息数据库
终端标识符
（＝x 1）
Itn1
终端标识符
Itn1

图 4

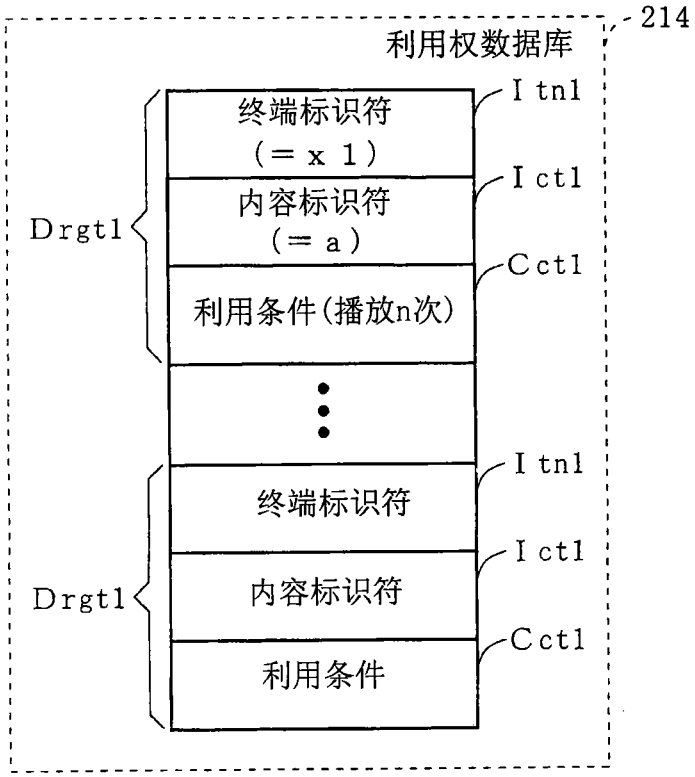

214
利用权数据库
终端标识符
（＝ｘ１）
内容标识符
（＝ａ）
利用条件(播放n次)
终端标识符
内容标识符
利用条件
Drgtl
Drgtl
Itnl
Ictl
Cctl
Itnl
Ictl
Cctl

图 5

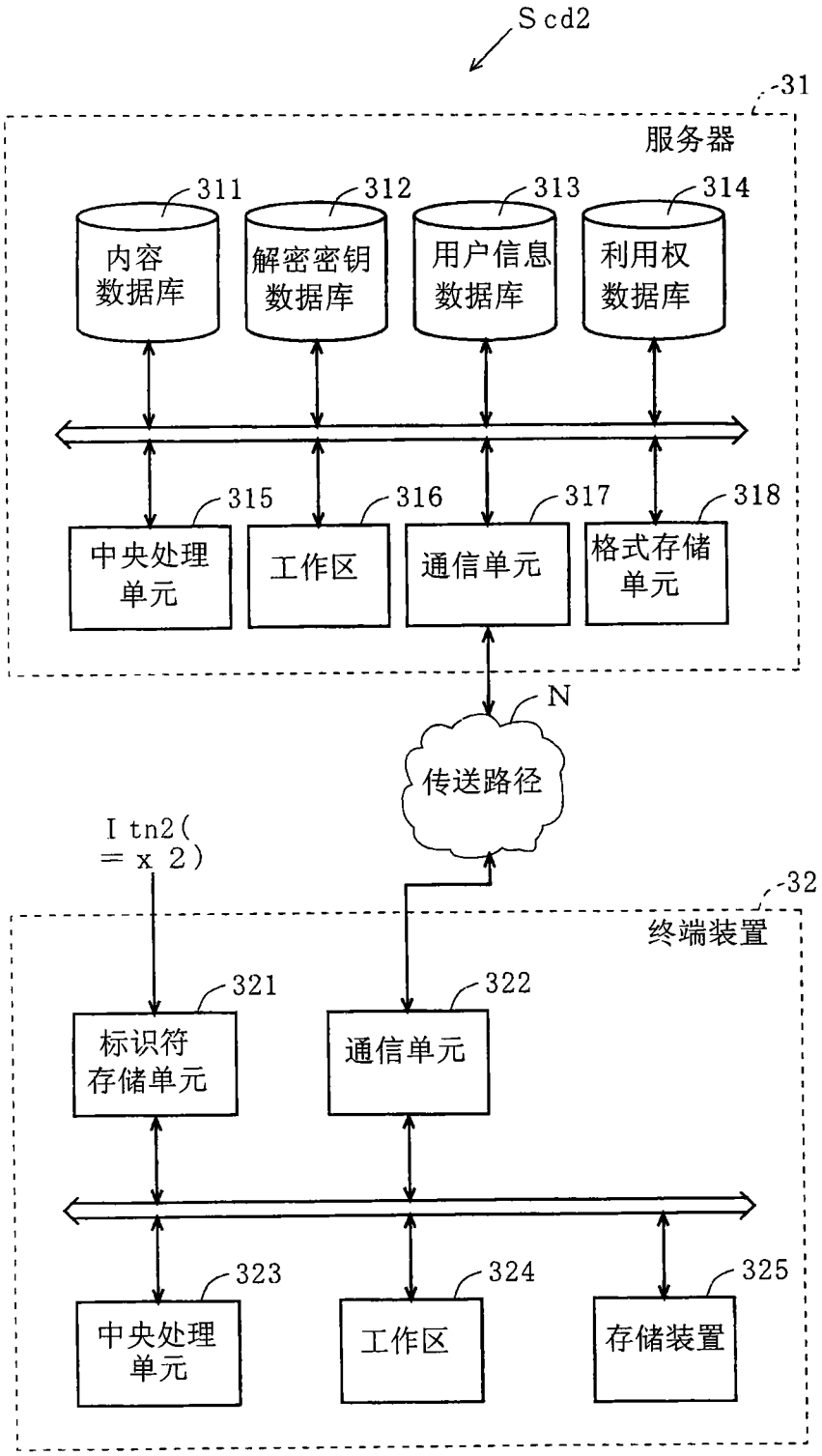
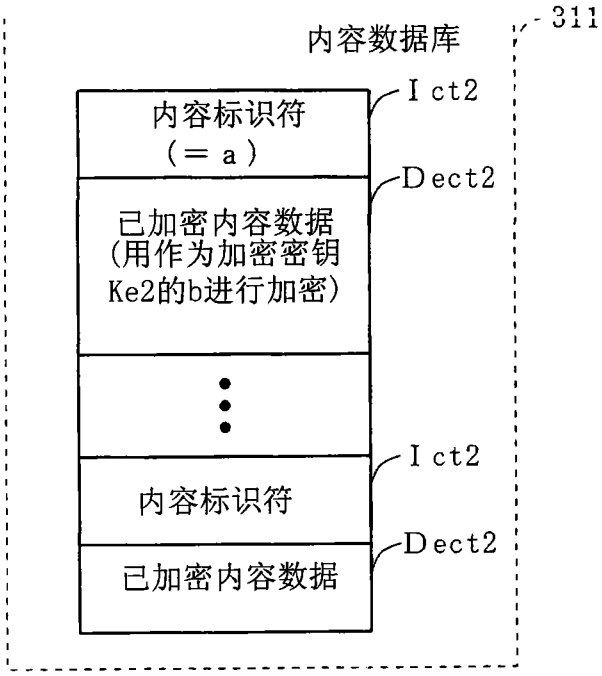

Scd2
31
服务器
311
内容
数据库
312
解密密钥
数据库
313
用户信息
数据库
314
利用权
数据库
315
中央处理
单元
316
工作区
317
通信单元
318
格式存储
单元
N
传送路径
Itn2(
=x 2)
32
终端装置
321
标识符
存储单元
322
通信单元
323
中央处理
单元
324
工作区
325
存储装置

图 6

（a）


311
内容数据库
内容标识符
（＝a）
Ict2
Dect2
已加密内容数据
(用作为加密密钥
Ke2的b进行加密)
Ict2
内容标识符
Dect2
已加密内容数据

（b）

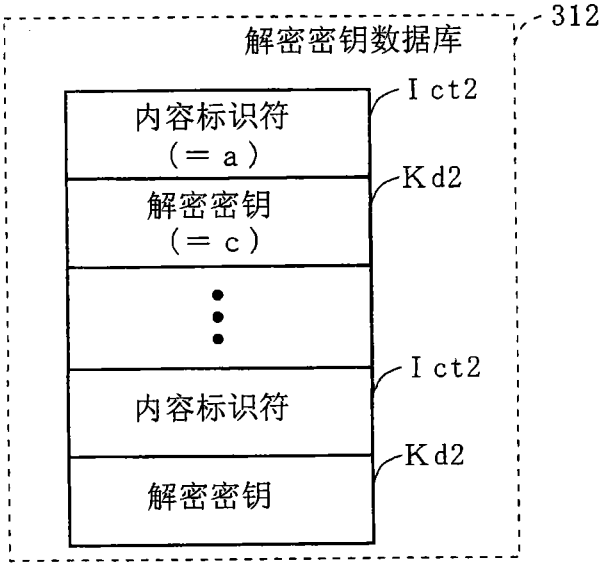
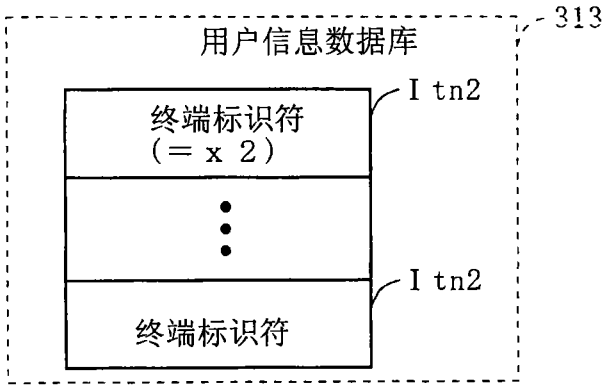

312
解密密钥数据库
内容标识符
（＝a）
Ict2
Kd2
解密密钥
（＝c）
Ict2
内容标识符
Kd2
解密密钥

图 7

（a）


313
用户信息数据库
终端标识符
（＝ｘ２）
Itn2
Itn2
终端标识符

（b）

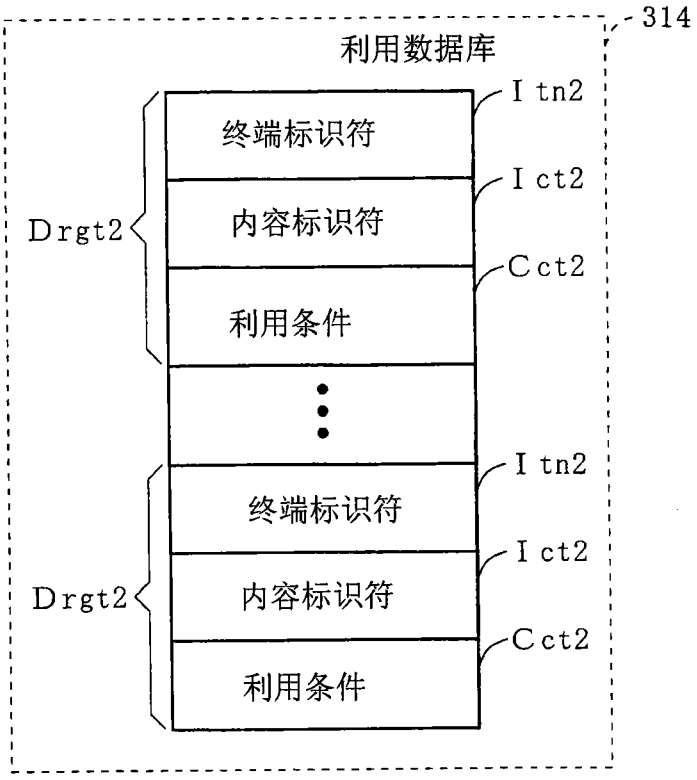

314
利用数据库
Itn2
终端标识符
Ict2
内容标识符
Drgt2
Cct2
利用条件
Itn2
终端标识符
Ict2
内容标识符
Drgt2
Cct2
利用条件

图 8

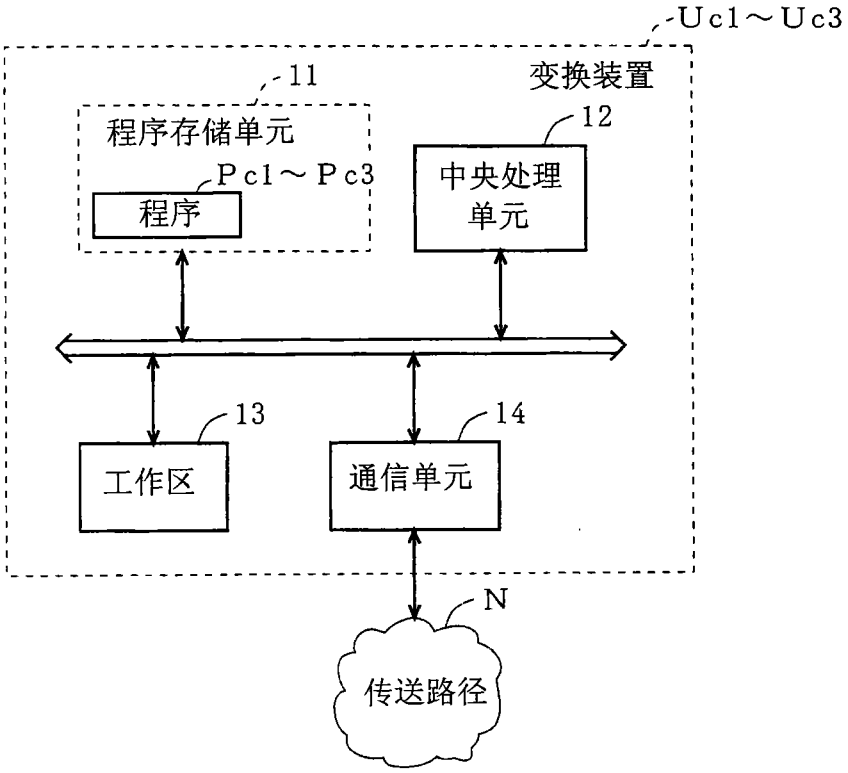

Uc1～Uc3
变换装置
11
程序存储单元
Pc1～Pc3
程序
12
中央处理
单元
13
工作区
14
通信单元
N
传送路径

图 9

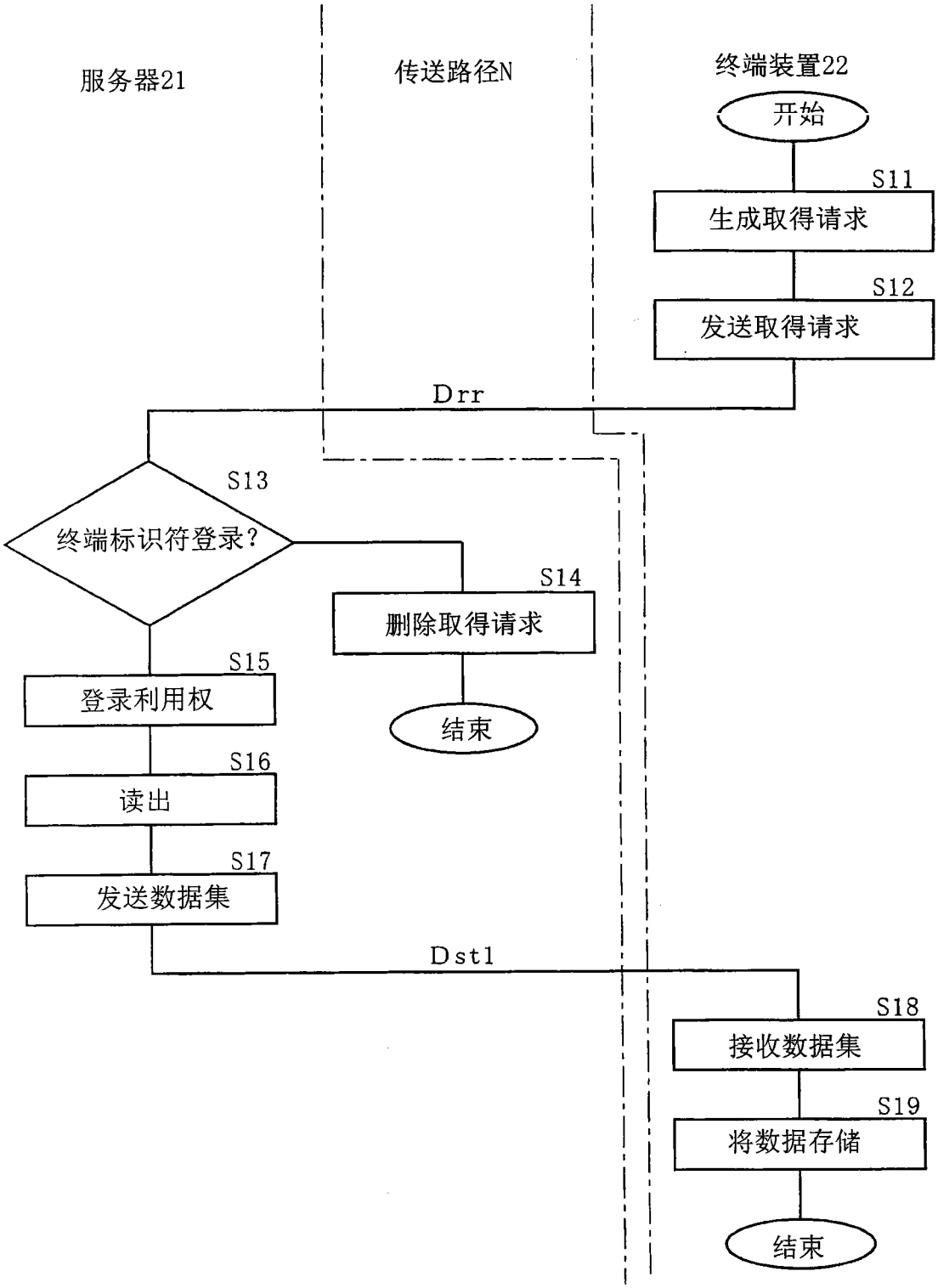

服务器21
传送路径N
终端装置22
开始
S11
生成取得请求
S12
发送取得请求
Drr
S13
终端标识符登录?
S14
删除取得请求
结束
S15
登录利用权
S16
读出
S17
发送数据集
Dst1
S18
接收数据集
S19
将数据存储
结束

图 10

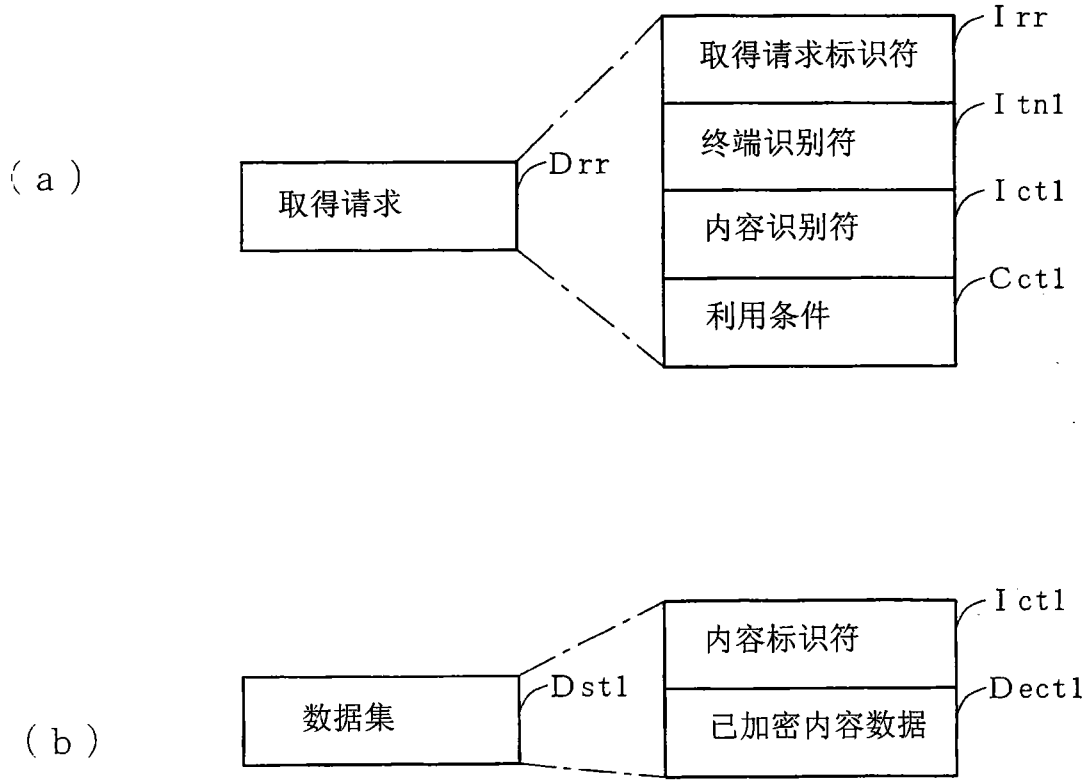

（a）
取得请求
Drr
取得请求标识符
终端识别符
内容识别符
利用条件
Irr
Itn1
Ict1
Cct1
（b）
数据集
Dst1
内容标识符
已加密内容数据
Ict1
Dect1

图 11

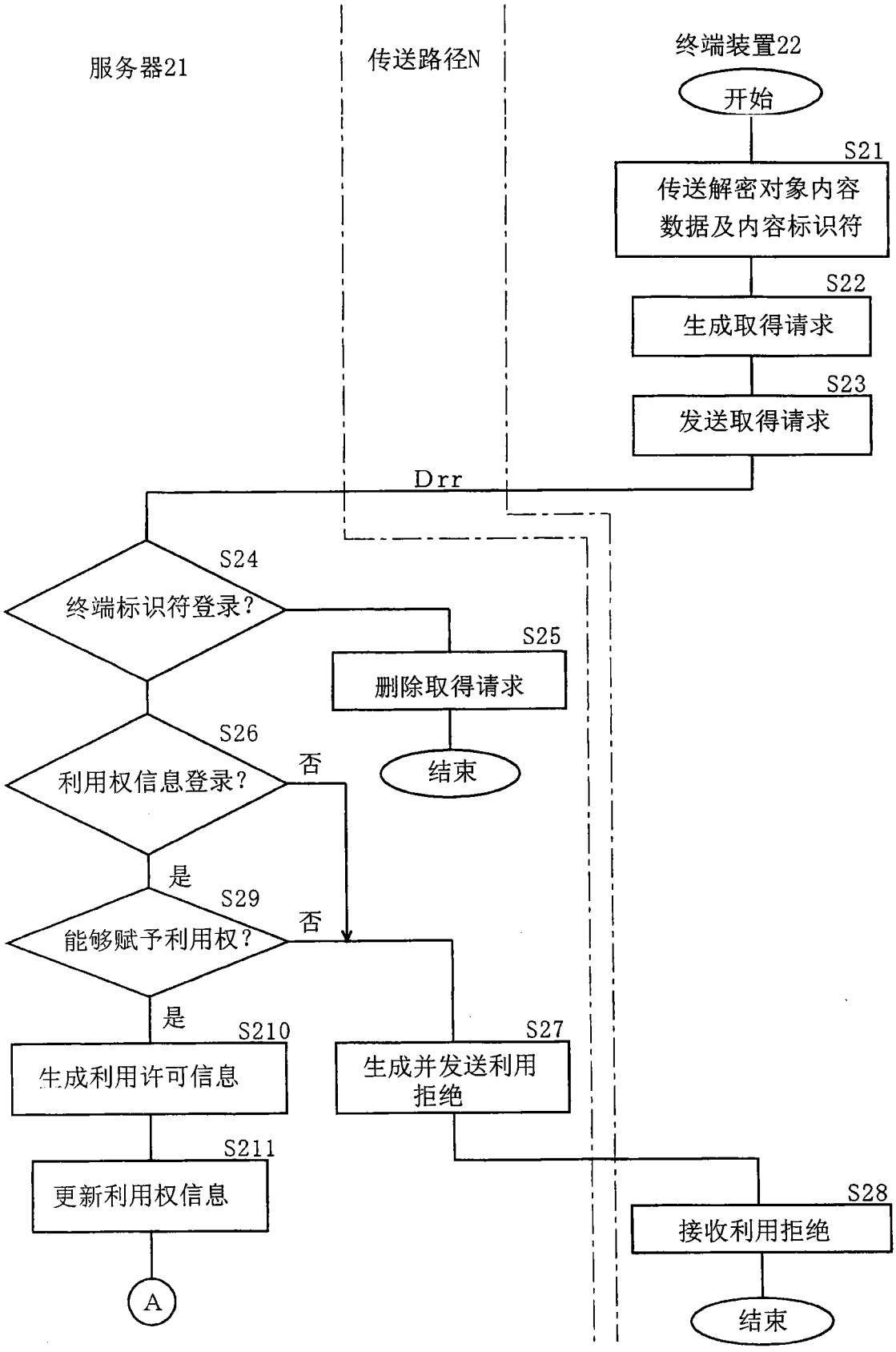

服务器21
传送路径N
终端装置22
开始
S21
传送解密对象内容数据及内容标识符
S22
生成取得请求
S23
发送取得请求
Drr
S24
终端标识符登录?
S25
删除取得请求
结束
S26
利用权信息登录?
否
是
S29
能够赋予利用权?
否
是
S210
生成利用许可信息
S27
生成并发送利用拒绝
S211
更新利用权信息
S28
接收利用拒绝
结束
A

图 12

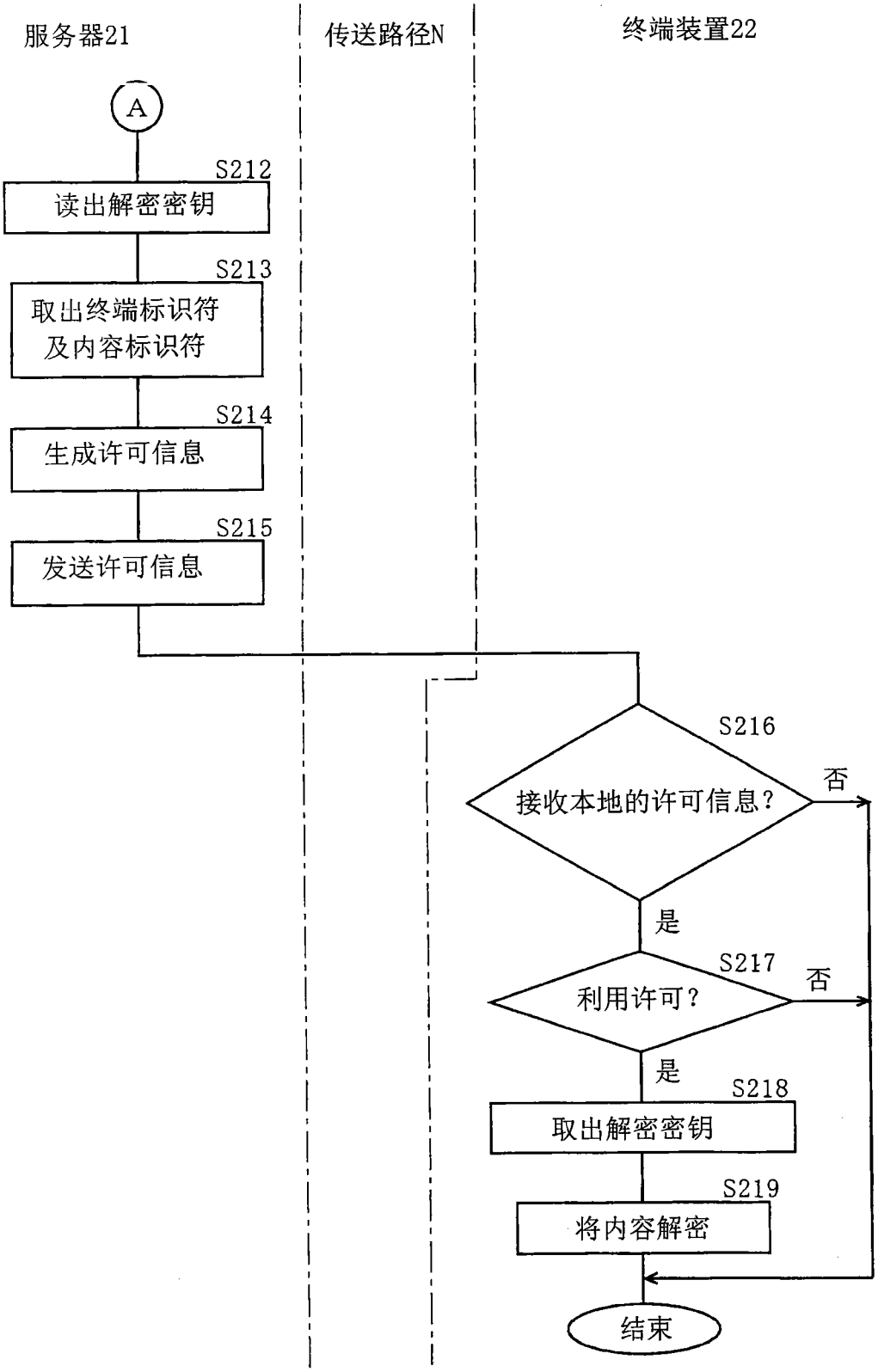

服务器21
传送路径N
终端装置22
A
S212
读出解密密钥
S213
取出终端标识符
及内容标识符
S214
生成许可信息
S215
发送许可信息
S216
接收本地的许可信息？
否
是
S217
利用许可？
否
是
S218
取出解密密钥
S219
将内容解密
结束

图 13

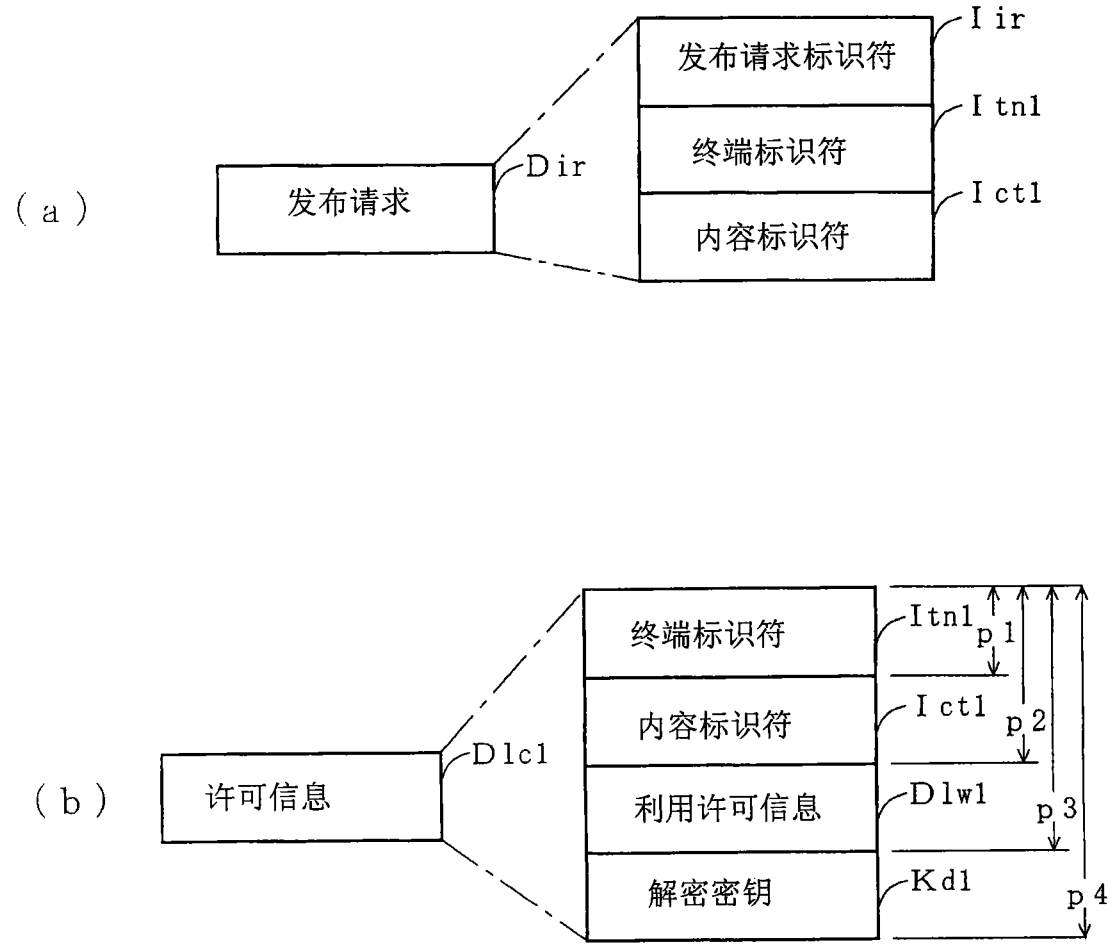

（a）
发布请求
Dir
发布请求标识符
终端标识符
内容标识符
Iir
Itnl
Ictl
（b）
许可信息
Dlcl
终端标识符
内容标识符
利用许可信息
解密密钥
Itnl
Ictl
Dlwl
Kdl
p1
p2
p3
p4

图 14

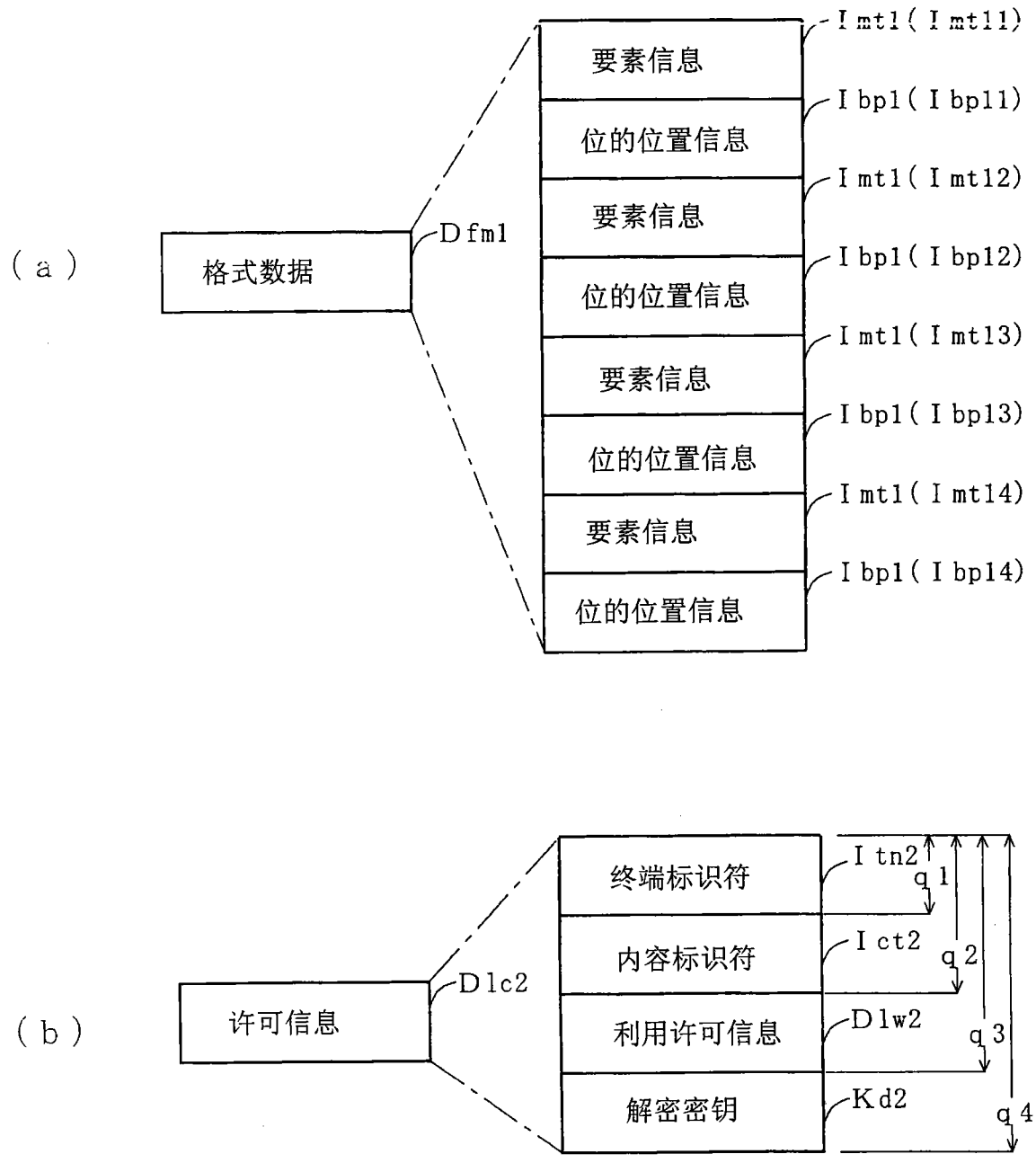

(a)
格式数据
Dfm1
要素信息
位的位置信息
要素信息
位的位置信息
要素信息
位的位置信息
要素信息
位的位置信息
Imt1(Imt11)
Ibp1(Ibp11)
Imt1(Imt12)
Ibp1(Ibp12)
Imt1(Imt13)
Ibp1(Ibp13)
Imt1(Imt14)
Ibp1(Ibp14)
(b)
许可信息
Dlc2
终端标识符
内容标识符
利用许可信息
解密密钥
Itn2
Ict2
Dlw2
Kd2
q1
q2
q3
q4

图 15

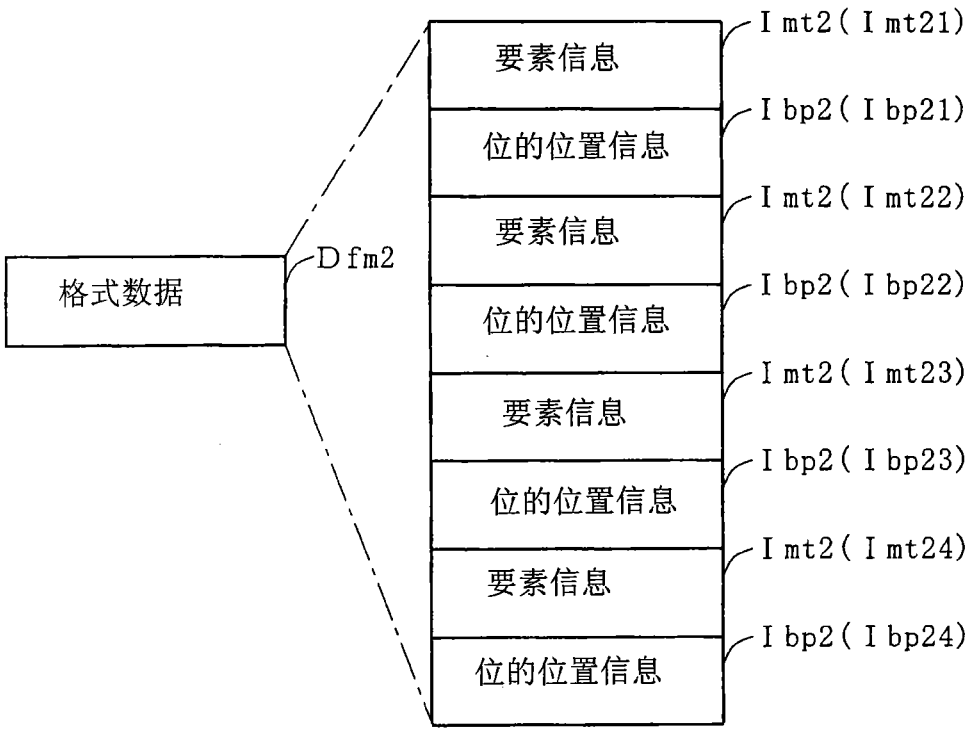

格式数据
Dfm2
要素信息
位的位置信息
要素信息
位的位置信息
要素信息
位的位置信息
要素信息
位的位置信息
Imt2(Imt21)
Ibp2(Ibp21)
Imt2(Imt22)
Ibp2(Ibp22)
Imt2(Imt23)
Ibp2(Ibp23)
Imt2(Imt24)
Ibp2(Ibp24)

图 16

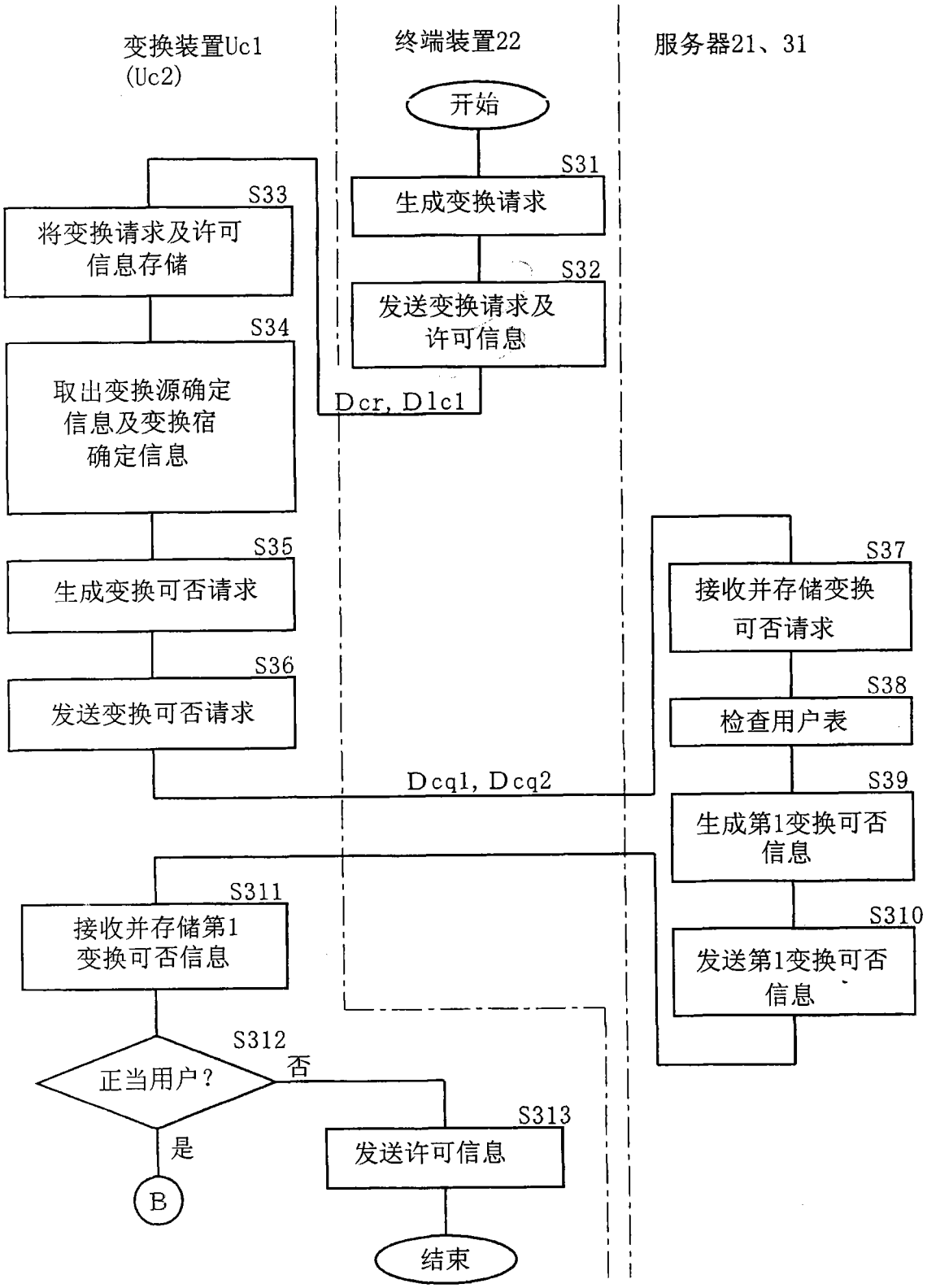

变换装置Uc1
(Uc2)
终端装置22
服务器21、31
开始
S31
生成变换请求
S32
发送变换请求及
许可信息
Dcr, Dlc1
S33
将变换请求及许可
信息存储
S34
取出变换源确定
信息及变换宿
确定信息
S35
生成变换可否请求
S36
发送变换可否请求
Dcq1, Dcq2
S37
接收并存储变换
可否请求
S38
检查用户表
S39
生成第1变换可否
信息
S310
发送第1变换可否
信息
S311
接收并存储第1
变换可否信息
S312
正当用户?
否
是
S313
发送许可信息
B
结束

图 17

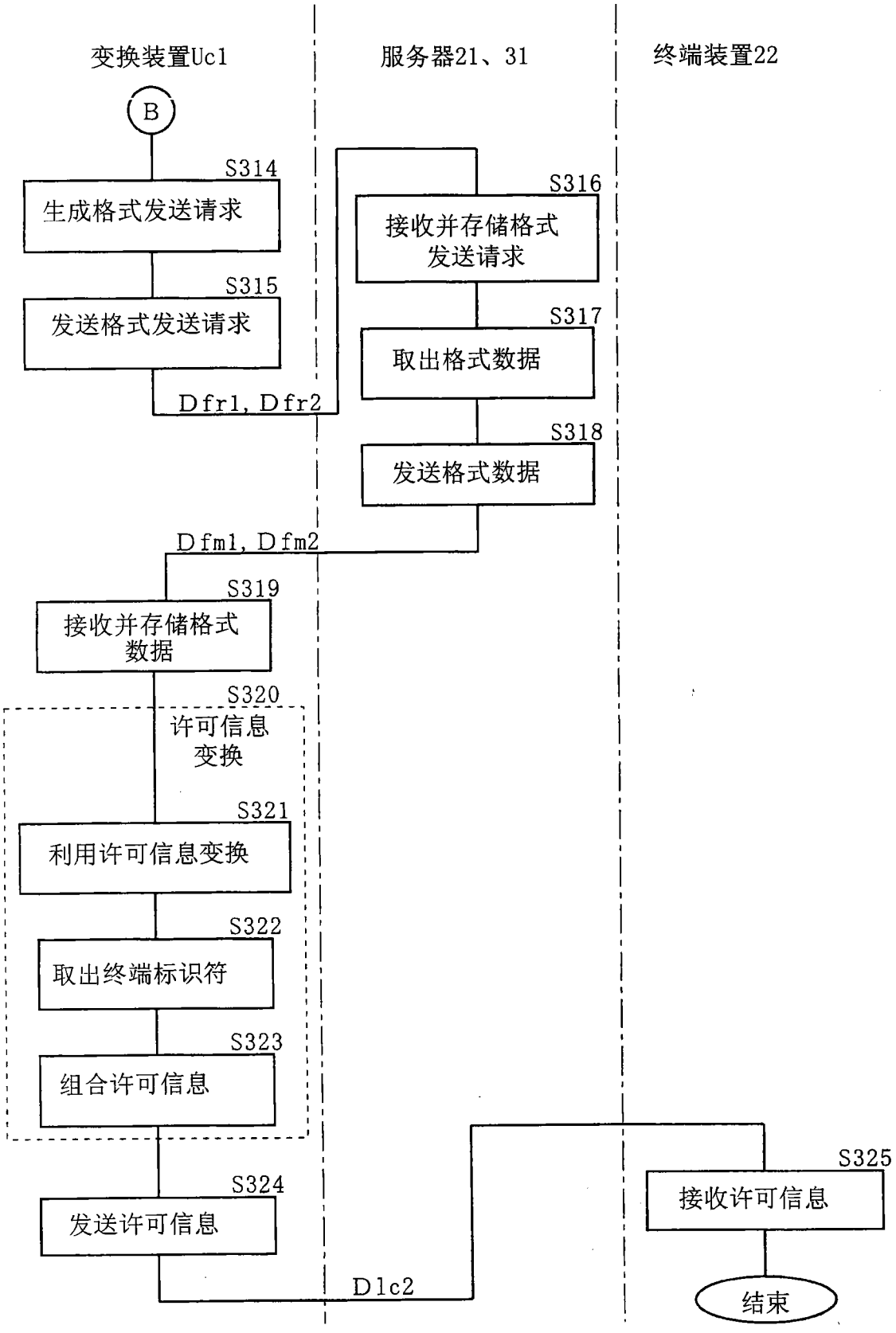

变换装置Uc1
服务器21、31
终端装置22
B
S314
生成格式发送请求
S315
发送格式发送请求
Dfr1, Dfr2
S316
接收并存储格式发送请求
S317
取出格式数据
S318
发送格式数据
Dfm1, Dfm2
S319
接收并存储格式数据
S320
许可信息变换
S321
利用许可信息变换
S322
取出终端标识符
S323
组合许可信息
S324
发送许可信息
Dlc2
S325
接收许可信息
结束

图 18

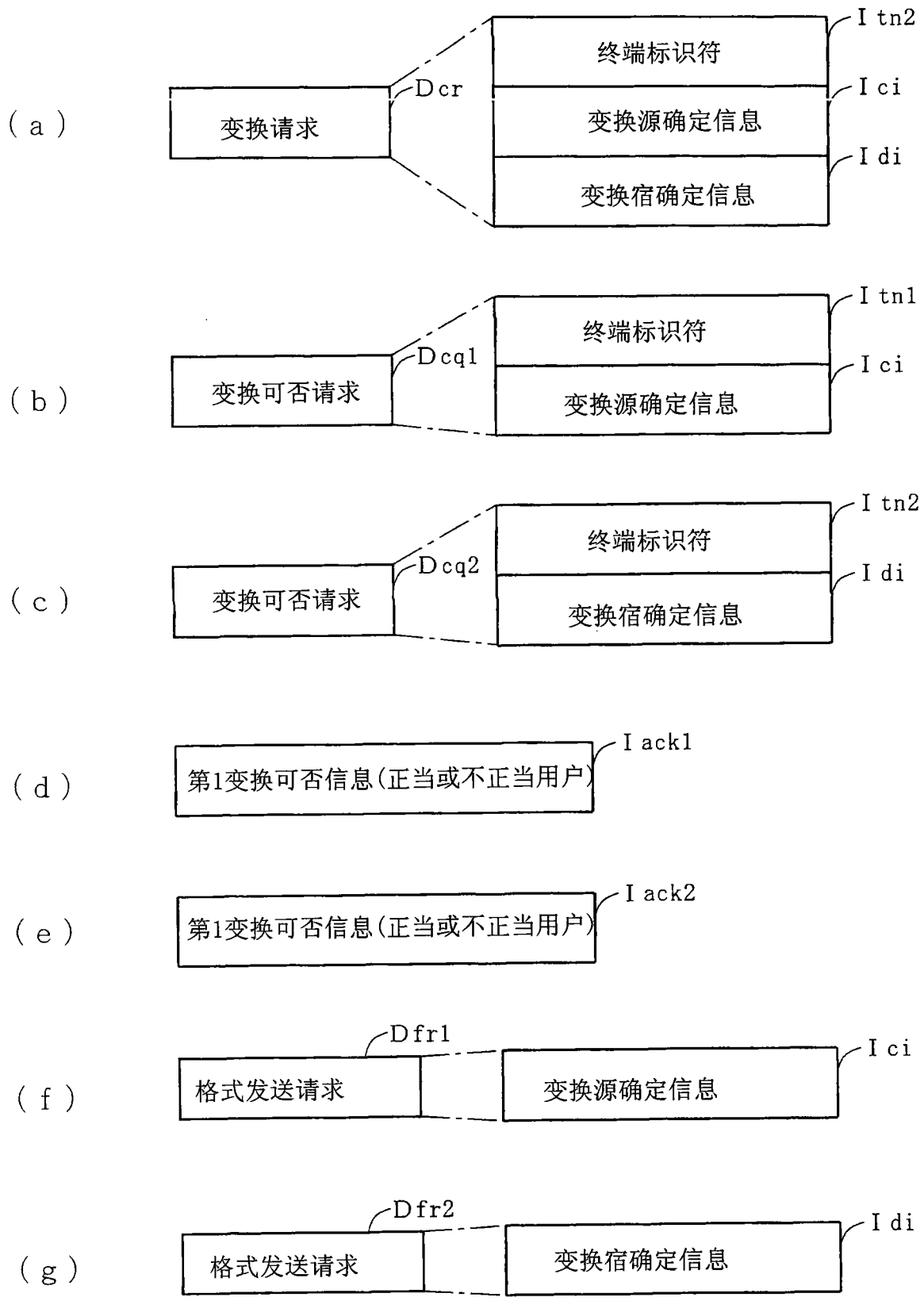

(a)
变换请求
Dcr
终端标识符
变换源确定信息
变换宿确定信息
Itn2
Ici
Idi
(b)
变换可否请求
Dcq1
终端标识符
变换源确定信息
Itn1
Ici
(c)
变换可否请求
Dcq2
终端标识符
变换宿确定信息
Itn2
Idi
(d)
第1变换可否信息(正当或不正当用户)
Iack1
(e)
第1变换可否信息(正当或不正当用户)
Iack2
(f)
格式发送请求
Dfr1
变换源确定信息
Ici
(g)
格式发送请求
Dfr2
变换宿确定信息
Idi

图 19

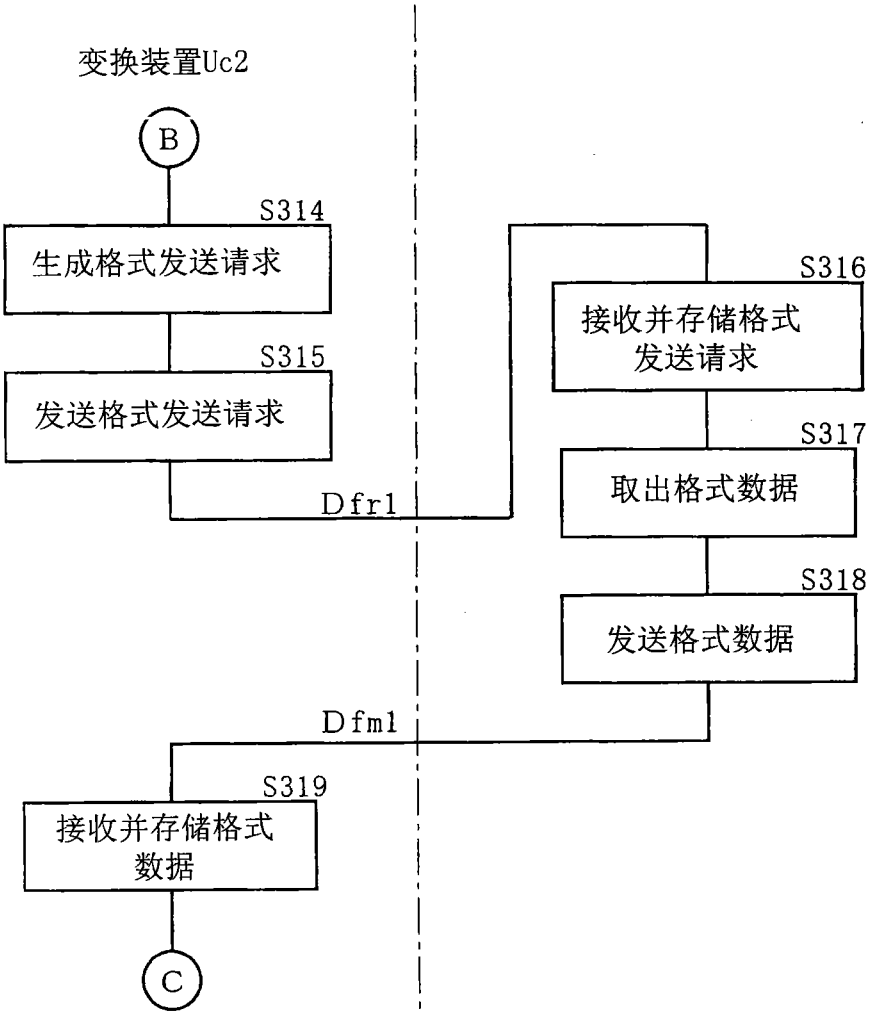

变换装置Uc2
B
S314
生成格式发送请求
S315
发送格式发送请求
Dfr1
S316
接收并存储格式发送请求
S317
取出格式数据
S318
发送格式数据
Dfm1
S319
接收并存储格式数据
C

图 20

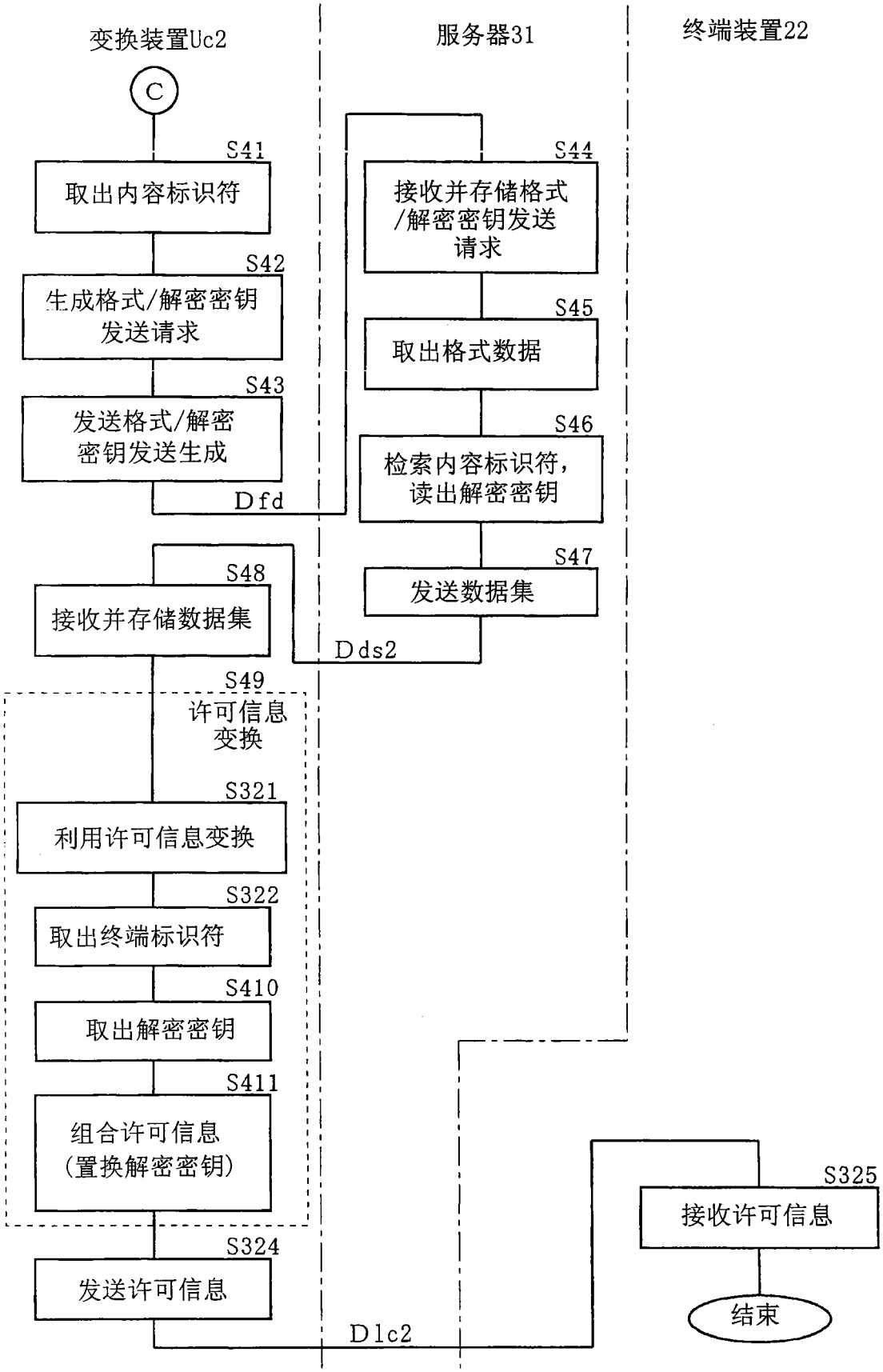

变换装置Uc2
服务器31
终端装置22
C
S41
取出内容标识符
S42
生成格式/解密密钥发送请求
S43
发送格式/解密密钥发送生成
Dfd
S44
接收并存储格式/解密密钥发送请求
S45
取出格式数据
S46
检索内容标识符，读出解密密钥
S47
发送数据集
Dds2
S48
接收并存储数据集
S49
许可信息变换
S321
利用许可信息变换
S322
取出终端标识符
S410
取出解密密钥
S411
组合许可信息（置换解密密钥）
S324
发送许可信息
Dlc2
S325
接收许可信息
结束

图 21

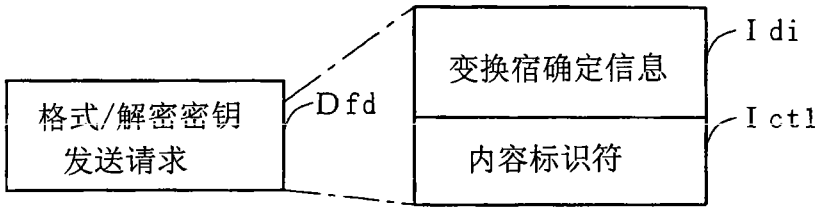


图 22

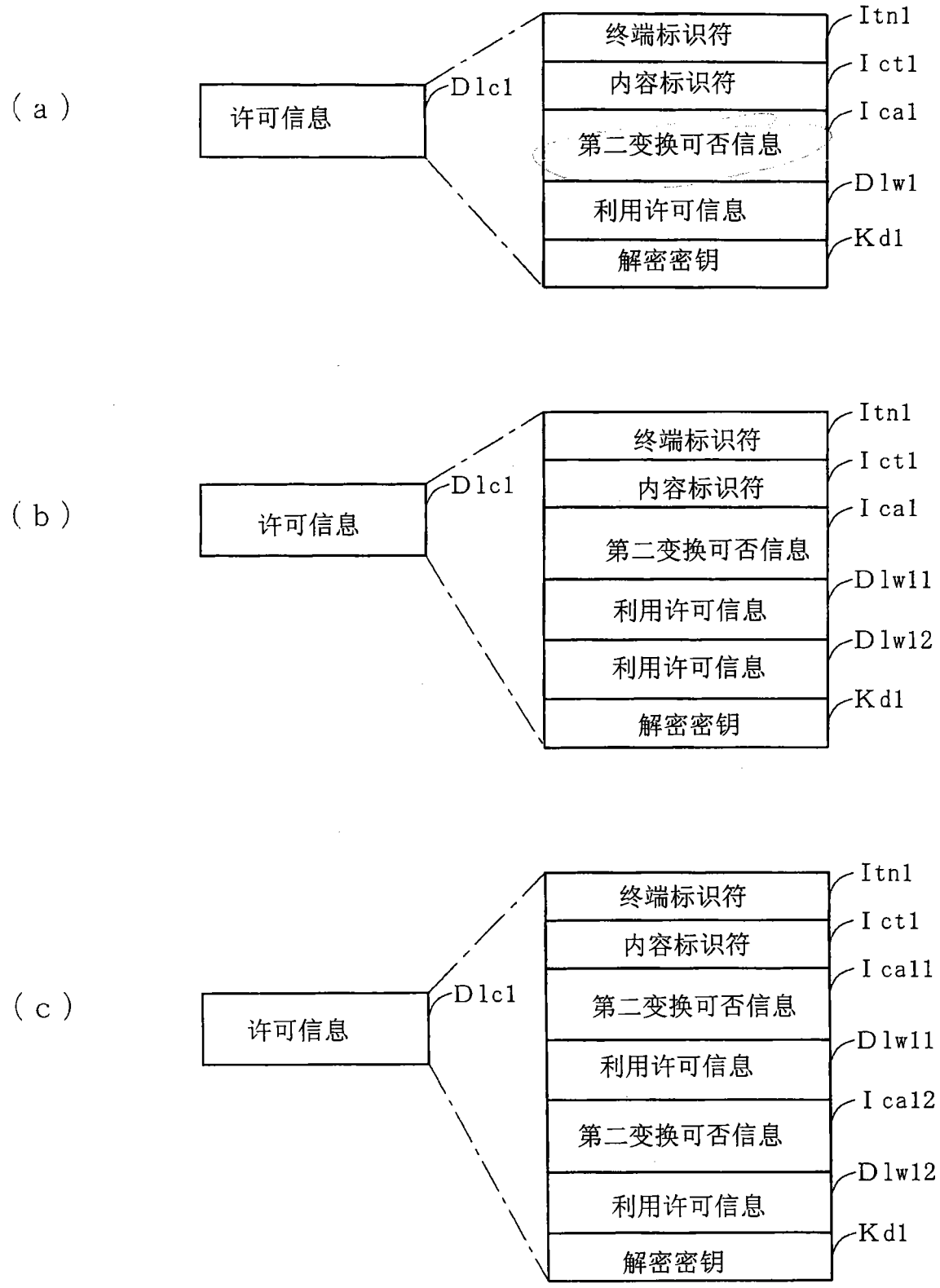

(a)
许可信息
Dlc1
终端标识符
内容标识符
第二变换可否信息
利用许可信息
解密密钥
Itn1
Ict1
Ica1
Dlw1
Kd1
(b)
许可信息
Dlc1
终端标识符
内容标识符
第二变换可否信息
利用许可信息
利用许可信息
解密密钥
Itn1
Ict1
Ica1
Dlw11
Dlw12
Kd1
(c)
许可信息
Dlc1
终端标识符
内容标识符
第二变换可否信息
利用许可信息
第二变换可否信息
利用许可信息
解密密钥
Itn1
Ict1
Ica11
Dlw11
Ica12
Dlw12
Kd1

图 23

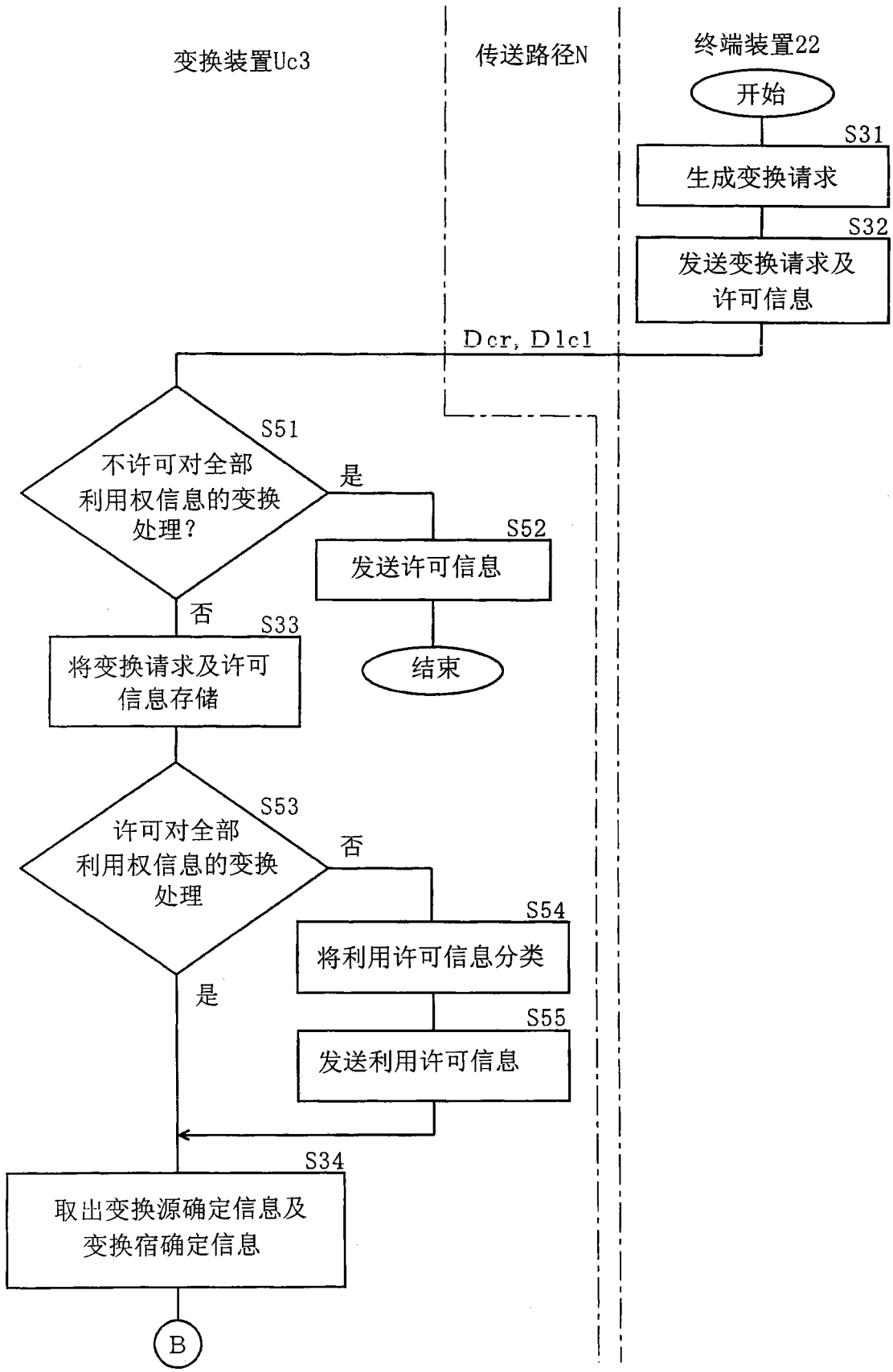

变换装置Uc3
传送路径N
终端装置22
开始
S31
生成变换请求
S32
发送变换请求及许可信息
Dcr, Dlc1
S51
不许可对全部利用权信息的变换处理？
是
S52
发送许可信息
结束
否
S33
将变换请求及许可信息存储
S53
许可对全部利用权信息的变换处理
否
S54
将利用许可信息分类
是
S55
发送利用许可信息
S34
取出变换源确定信息及变换宿确定信息
B

图 24