



[12] 发明专利说明书

专利号 ZL 02103443.5

[45] 授权公告日 2005 年 10 月 5 日

[11] 授权公告号 CN 1221907C

[22] 申请日 2002.2.4 [21] 申请号 02103443.5

[30] 优先权

[32] 2001.2.2 [33] JP [31] 027278/2001

[71] 专利权人 松下电器产业株式会社

地址 日本大阪府

[72] 发明人 东吾纪男 村上弘规 松尾隆史

中原彻 难波孝彰 后藤吉正

中西正典 宫崎雅也 小塙雅之

审查员 李延峰

[74] 专利代理机构 永新专利商标代理有限公司

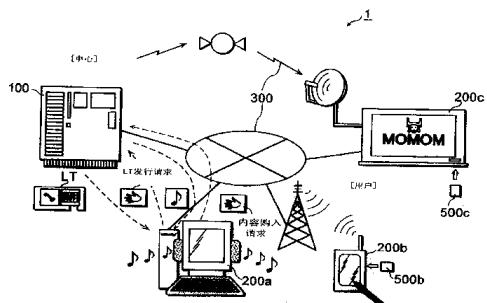
代理人 黄剑锋

权利要求书 4 页 说明书 26 页 附图 19 页

[54] 发明名称 内容使用管理系统和内容使用管理方法

[57] 摘要

本发明公开的内容使用管理系统和内容使用管理方法，其中，该内容使用管理系统 1 由使用作为数字作品的内容的用户终端 200a 和通过传送网络 300 来管理内容的终端装置 200a 中使用的服务器 100 构成，服务器 100 包括存储涉及使用用户终端 200a 的用户所有的内容使用权限的权利信息的用户权利信息 DB120，和根据来自所述用户的请求，生成作为表示该用户所有使用权限一部分的权利信息的 LT，向用户终端 200a 发送的内容信息生成部 170，用户终端 200a 包括从服务器 100 接收可发送的 LT 的通信部 210，和根据接收到的 LT 表示的使用权限，控制内容使用的许可信息处理部 260。



1. 一种内容使用管理系统，其由使用作为数字作品的内容的终端装置和通过传送路径来管理所述内容在所述终端装置中的使用的服务器装置构成，其特征在于：

所述服务器装置包括：

存储涉及使用所述终端装置的用户所具有的内容使用权限的权利信息的权利信息存储装置；和

许可证发送装置，根据来自所述用户的请求从存储于权利信息存储装置的权利信息提取部分使用权限，而生成作为表示该用户所具有的部分使用权限的权利信息的许可证，并向所述终端装置发送，

所述终端装置包括：

接收从所述服务器装置发送来的许可证的接收装置；和

根据接收到的许可证表示的使用权限，控制所述内容使用的权利信息存储装置，

权利信息存储装置的权利信息在许可证发送时被更新，使许可证表示的部分权利信息被除外。

2. 根据权利要求 1 所述的内容使用管理系统，其特征在于：

所述许可证发送装置，从该用户处取得指定所述用户所具有的部分使用权限的请求，生成对应于该指定的许可证，发送到所述终端装置。

3. 根据权利要求 1 所述的内容使用管理系统，其特征在于：

所述许可证发送装置，生成表示构成所述用户所具有的使用权限的最小单位使用权限许可证，发送到所述终端装置。

4. 根据权利要求 1 所述的内容使用管理系统，其特征在于：

所述许可证是由涉及内容使用的一个以上的是否可行信息构成的。

5. 根据权利要求 4 所述的内容使用管理系统，其特征在于：

所述是否可行信息是表示是否可行进行内容的再现、移动和复制中的任一个的是可行。

6. 根据权利要求 4 所述的内容使用管理系统，其特征在于：

所述是否可行信息表示可以或不可以对内容作一次以上包含无限次数的使用。

7. 根据权利要求 1 所述的内容使用管理系统，其特征在于：

所述许可证发送装置在加密所述许可证后，发送到所述终端装置，

所述终端装置还包括解密由所述接收装置接收的许可证的解密装置，

所述内容使用控制装置，根据解密后的许可证所表示的使用权限，控制所述内容的使用。

8. 根据权利要求 7 所述的内容使用管理系统，其特征在于：

所述解密装置和内容使用控制装置，为耐篡改的安全模块。

9. 根据权利要求 1 所述的内容使用管理系统，其特征在于：

所述许可证中包含用于检测是否篡改过该许可证内容的检测信息。

10. 根据权利要求 1 所述的内容使用管理系统，其特征在于：

所述内容使用控制装置，在使用内容后，判断是否允许再使用所述许可证的内容，在不允许的情况下，无效该许可证。

11. 根据权利要求 10 所述的内容使用管理系统，其特征在于：

所述终端装置还包括可装卸的外部记录媒体，

所述内容使用控制装置，在内容被使用前的许可证、以及内容使用后再允许内容使用的许可证，允许内容移动的情况下，将该许可证存储在所述外部记录媒体中。

12. 根据权利要求 11 所述的内容使用管理系统，其特征在于：

所述终端装置还包括判定装置，判定与该终端装置连接的所述外部记录媒体是否包括根据所述许可证表示的使用权限来控制所述内容的使用的装置，

所述内容使用控制装置，在判定为所述外部记录媒体包括所述控制装置的情况下，将许可证存储在外部记录媒体中。

13. 根据权利要求 12 所述的内容使用管理系统，其特征在于：

所述内容使用控制装置，在判定为所述外部记录媒体不包括所述控制装

置的情况下，将所述许可证变换为不同格式的内容控制信息。

14. 根据权利要求 6 所述的内容使用管理系统，其特征在于：

所述是否可行信息包含以判断进行一次内容使用为基准的判定条件，
所述内容使用控制装置根据所述判定条件将内容使用判定为一次。

15. 根据权利要求 14 所述的内容使用管理系统，其特征在于：

根据内容的使用状态来设定所述判定条件。

16. 根据权利要求 15 所述的内容使用管理系统，其特征在于：

所述判定条件为再现内容的时间，

所述内容使用控制装置，根据内容的所述再现时间将内容的使用判定为
一次。

17. 根据权利要求 16 所述的内容使用管理系统，其特征在于：

所述内容使用控制装置，在从所述再现开始的由所述判定条件表示的时
间内，设定为所述一次使用。

18. 一种内容使用管理方法，其是由使用作为数字作品的内容的终端装
置和通过传送路径来管理所述内容的所述终端装置中使用的服务器装置构成
的系统的内容使用管理方法，其特征在于：

所述服务器装置进行：

存储涉及使用所述终端装置的用户所具有的内容的使用权限的权利信息
的权利信息存储步骤；和

许可证发送步骤，根据来自所述用户的请求从存储于权利信息存储装置
的权利信息提取部分使用权限，而生成作为表示该用户所具有的部分使用权
限的权利信息的许可证，并向所述终端装置发送，

所述终端装置进行：

接收从所述服务器装置发送来的许可证的接收步骤；和

根据接收到的许可证表示的使用权限，控制所述内容使用的內容使用控
制步骤；

所述权利信息存储装置的权利信息在许可证发送时被更新，以便许可证
表示的部分权利信息除外。

19. 根据权利要求 18 所述的内容使用管理方法，其特征在于：

在所述许可证发送步骤中，从该用户处取得指定所述用户所具有的部分
使用权限的请求，生成对应于该指定的许可证，发送到所述终端装置。

内容使用管理系统和内容使用管理方法

技术领域

本发明涉及一种管理由通信或播放等配送的音乐或图像等的数字内容使用的系统和方法，具体而言，是涉及一种能确实并简单地实施限制内容再现次数的内容权利管理和使用控制的系统和方法。

背景技术

近年来，开发了通过因特网或数字播放等配送音乐或图像、游戏等数字作品的系统，其一部分进入了实用化阶段。对应于这些内容的配送，从版权保护等观点来看，同时研究了限制配送内容的再现次数或移动、复制等内容权利管理和使用控制方式（DRM：数字权利管理）。

在现有的数字内容配送系统中，如特开 2000-48076 号公报或特开 2000-293439 号公报中所述，对各用户的内容使用条件进行模型化，与内容一起配送至接收侧，通过整个用户终端侧来进行管理。

例如，在某一用户购入三次视听电影“Matrix”的权利的情况下，用户终端在从配送服务器通过通信接收电影“Matrix”的同时，还接收了表示“可三次视听 Matrix”的使用条件，根据使用条件来管理内容的再现。

配送服务器在向用户终端配送上述使用条件之后，就不再与用户的使用条件相关。

在再现用户终端存储的内容后视听“Matrix”的情况下，每视听一次，就进行减少一次用户终端管理的使用条件的处理，当可视听次数为 0 时，进行不允许视听的处理。

图 1 表示现有的数字内容配送系统的结构。

配送服务器 1000 包括存储会员注册的用户的 ID 信息等的用户管理数据库 1001；存储加密内容的内容键和内容使用条件的内容信息数据库 1003；存

储内容的内容数据库 1006；进行用户认证的用户认证部 1002；生成包含内容使用条件和内容键信息的内容信息生成部 1004；通过用户 ID 等用户固有信息来加密内容信息的内容信息加密部 1005；从内容数据库 1006 取得指定内容的内容取得部 1007；通过内容键加密内容的内容加密部 1008；以及与用户终端 2000 进行通信的通信部 1009。

另一方面，用户终端 2000 包括与配送服务器 1000 之间进行通信的通信部 2001；存储 ID 信息的 ID 信息存储部 2002；存储加密内容的存储部 2003 (HDD)；根据接收的内容信息来对内容键和使用条件进行解密的内容信息解密部 2006；管理内容的使用条件和内容键的使用条件管理部 2007；进行内容再现时的使用条件处理的使用条件处理部 2008；在满足使用条件时，通过从使用条件处理部 2008 取得的内容键来对内容进行解密的内容解密部 2005；以及向外部媒体 5000 输出内容的外部媒体访问部 2004。

图 2 表示在该数字内容配送系统中，用户终端 2000 从配送服务器 1000 购入内容时的处理流程。

当有用户的内容购入请求时，用户终端 2000 的通信部 2001 取得存储在 ID 信息存储部 2002 中的用户终端 2000 的 ID 信息，将该 ID 信息和内容购入请求一直发送到配送服务器 1000 (S1001)。

通过配送服务器 1000 的通信部 1009 接收该信息的用户认证部 1002 在将接收到的 ID 信息与存储在用户管理数据库 1001 中的 ID 信息相对照进行用户认证后，将内容购入请求传送到内容信息生成部 1004 (S1002)。

内容信息生成部 1004 对内容购入进行收费处理，从内容信息数据库 1003 取得购入内容的使用条件和内容键的信息，将内容键与购入内容的信息一起传送到内容取得部 1007。在生成包含使用条件和内容键信息的内容信息后传送到内容信息加密部 1005，内容信息加密部 1005 对内容信息进行加密 (S1003)。

内容取得部 1007 从内容数据库 1006 取得该内容后，内容加密部 1008 使用内容键对该内容进行加密 (S1004)。

配送服务器 1000 的通信部 1009 将加密后的内容和加密后的内容信息发

送到用户终端 2000。

用户终端 2000 的通信部 2001 接收加密后的内容和包含内容键及使用条件信息的加密后的内容信息 (S1005)，将内容传送并存储在存储部 2003 中 (S1006)。

向内容信息解密部 2006 发送内容信息。内容信息解密部 2006 对加密的内容信息进行解密，取出使用条件和内容键后存储在使用条件管理部 2007 中 (S1007)。

图 3 表示在该数字内容配送系统中，用户终端 2000 再现内容时的处理流程。

当有用户的内容再现请求时，使用条件处理部 2008 取得使用条件管理部管理的相应内容的使用条件和内容键 (S2001)，检查使用条件的再现次数 (允许的再现次数) (S2002)。

当再现次数比 0 大时 (S2003)，减少使用条件的再现次数 (S2004)，将使用条件和内容键存储在使用条件管理部 2007 中 (S2005)。

内容解密部 2005，从存储部 2003 取得相应内容 (S2006)，采用从使用条件处理部传送来的内容键，解密内容，再现内容 (S2007)。

在步骤 S2003 中，当再现次数不比 0 大时，结束再现处理。

再现内容的图像/声音从内容解密部 2005 输出到 TV 等的监视器。并且将内容移动到外部媒体 5000，进行复制的情况下，通过外部媒体访问部 2004 将内容的图像/声音输出到外部媒体 5000。

为了防止秘密信息的泄密，通常将处理秘密信息的 ID 信息存储部 2002、内容信息解密部 2006 和使用条件管理部 2007，设置在 IC 卡等安全模块中，将该安全模块安装在用户终端 2000 上。

在该情况下，当从使用条件管理部 2007 向使用条件处理部 2008 发送使用条件和内容键的信息时，对这些信息加密后从安全模块输出，使用条件处理部 2008 对这些信息进行解密后使用。另外，当将使用条件处理部 2008 更新后的使用条件存储于使用条件管理部 2007 中时，也再次进行加密后发送到安全模块。

在现有的数字内容配送系统中，通过这种方式，在用户终端侧对各用户的内容的使用条件进行管理。

但是，在用户终端管理各用户的使用条件的情况下，存在以下问题：

(1) 在用户终端必须进行复杂的使用条件管理，用户终端的功能有可能变的庞大而臃肿。

(2) 因配送服务器完全不涉及配送内容使用、权利管理处理，故即使在用户终端进行内容复制时，也不能跟踪内容，并了解何时复制到何媒体中。

(3) 在用户终端的存储装置(HDD)紊乱(拥挤)时，难以恢复用户的使用条件等(因为在用户终端以外没有保持该信息)。

(4) 在实施当购入新内容时自动对已购入的内容使用条件的再现次数加上1的服务并追加新的使用条件的情况下，有必要变更配送服务器和用户终端两者的硬件、软件。因此，实际上难以进行扩大这种使用条件的服务和使用条件的追加等的处理。

另外，在配送服务器侧管理全部各用户的使用条件，并且用户终端不控制使用条件，虽然也考虑了通过每次视听、通信途径而从配送服务器取得内容本身(或在加密内容的情况下，可仅为内容键)的模型，但该情况下存在以下问题。

(5) 在向用户终端传送内容后，因为没有对该内容进行使用控制，所以有可能在用户终端无限制地使用取得的内容(特别是再现)。

发明的内容

为了解决上述现有的问题，本发明的目的在于提供一种内容使用管理系统、内容使用管理方法等，其不增加用户终端的负担，而确实并简单地控制在用户终端的内容的使用。

为了实现上述目的，本发明采取以下技术方案：

本发明的内容使用管理系统由使用作为数字作品的内容的终端装置和通过传送路径来管理所述内容在所述终端装置中的使用的服务器装置构成，其特征在于：所述服务器装置包括存储涉及使用所述终端装置的用户所具有的内容使用权限的权利信息的权利信息存储装置；和许可证发送装置，根据来

自所述用户的请求从存储于权利信息存储装置的权利信息提取部分使用权，而生成作为表示该用户所具有的部分使用权限的权利信息的许可证，并向所述终端装置发送，所述终端装置包括接收可从所述服务器装置发送的许可证的接收装置、和根据接收到的许可证表示的使用权限，控制所述内容使用的内容使用控制装置，权利信息存储装置的权利信息在许可证发送时被更新，以使许可证表示的部分权利信息被除外。

在本说明书中，内容的“使用”包含内容的“再现”、“移动”、“复制”或电子书籍的内容“印刷”等使用内容的所有操作，并且，还包含作为这些操作的事先行为下载“许可信息”的操作（事先下载许可证）。

在此如此构成的内容使用管理系统中，服务器装置的许可证发送装置根据来自所述用户的请求，生成作为表示该用户所具有的部分使用权限的权利信息的许可证，发送到所述终端装置。终端装置的内容使用控制装置根据接收到的许可证表示的使用权限来控制所述内容的使用。

因此，在终端装置中，不必要管理用户所具有的全部使用权限，通过仅管理许可证表示的用户的部分使用权限，就可以控制内容的使用，从而可以大幅度降低终端装置的管理负担。服务器装置可以在发送许可证的同时把握各终端装置中的内容使用状况，即使在终端装置中进行内容复制等情况下，可以在服务器装置中通过复制许可查询来检测出何时复制到何种媒体上，从而能够跟踪内容。另外，因为服务器装置中保持有用户所具有的使用权限，所以即使在终端装置的存储装置（HDD）紊乱时，也可容易的恢复用户的使用条件，容易进行实施所谓自动对内容的使用条件的再现次数加1的服务的这种扩大使用条件的服务或使用条件追加等处理。并且，因为终端装置的内容使用控制装置可根据接收到的许可证表示的使用权限来控制所述内容的使用，所以可确实防止终端装置中内容的无限制使用。

其中，特征在于，所述许可证发送装置从该用户处取得指定所述用户所具有的部分使用权限的请求，生成对应于该指定的许可证，发送到所述终端装置，并生成表示构成所述用户所具有使用权限的最小单位的使用权限的许可证，发送到所述终端装置。根据该结构，可详细把握各终端装置处的内容

使用状况，并可将各终端装置的使用权限管理负荷降至最低。

另外，可构成为在所述许可证中包含用于检测是否篡改过该许可证内容的检测信息。由此，可确实防止许可证的篡改。

本发明在实现了作为构成所述内容使用管理系统的服务器装置和终端装置的同时，还实现了将构成这些服务器装置和终端装置的特征装置作为步骤的内容使用管理方法，以及实现了作为个人计算机等中执行这些步骤的程序。不用说，通过DVD等记录媒体或因特网等传送媒体，可使该程序广泛地流通。

附图的简要说明

图1是表示现有的数字内容配送系统的结构的框图。

图2是表示现有的数字内容配送系统的内容购入时的处理的流程图。

图3是表示现有的数字内容配送系统的内容再现时的处理的流程图。

图4是表示本实施例的内容使用管理系统1的整体结构的图。

图5是表示图4所示服务器100和用户终端200a-200c的结构的功能框图。

图6是表示图5所示用户管理表格111的结构实例的图。

图7是表示图5所示用户权利信息管理表格121的结构实例的图。

图8是表示图5所示许可信息的结构实例的图。

图9是表示内容信息生成部170生成的LT数据格式结构的图。

图10是表示该系统中，在用户购入内容的情况下，用户终端200a和服务器100中各自进行的处理的流程图。

图11是表示内容购入画面(1)的图。

图12是表示内容购入画面(2)的图。

图13是表示该系统中，在用户使用内容的情况下，用户终端200a和服务器100中各自进行的处理的流程图。

图14是表示使用内容选择画面的图。

图15是表示内容使用请求画面的图。

图16是表示配送给用户终端的提取使用条件和服务器管理的使用条件的变动的关系的图。

图 17 是表示一次使用条件与使用时间的关系的图。

图 18 是表示该系统中，在向外部媒体移动内容或 LT 的情况下，用户终端 200a 所进行的处理的流程图。

图 19 是表示移动内容选择画面的图。

发明的具体实施方式

下面使用附图来详细说明本发明的实施例。

图 4 是表示本实施例的内容使用管理系统 1 的整体结构的图。

该内容使用管理系统 1 为如下的系统：以中心侧为主体动态地管理赋予购入音乐、电影、书籍等数字化内容的用户的每项内容的使用权利（许可），根据用户请求来配送用于使用内容的许可证（下面记为“LT”），通过在 LT 中包含的使用条件的范围内使用内容，以保护内容的著作权，该系统由配置在中心处的服务器 100、使用内容的用户所使用的用户终端 200a-200c 和与这些服务器及用户终端等连接的通信网络 300 构成。

服务器 100 为工作站等计算机，具有作为用户管理服务器、内容配送服务器、收费服务器、许可管理服务器的功能。具体而言，服务器 100 管理加入本系统 1 的用户和其它用户所有的终端，并从用户终端 200a-200c 等接收内容的购入，具有接收来自用户终端 200a-200c 等的许可证发送请求（以下记为“LT 发送请求”）的网页，根据来自用户终端 200a-200c 的内容购入请求进行收费，向各用户终端 200a-200c 配送加密的内容，并根据 LT 发送请求，配送用于用户终端 200a-200c 中使用的加密后内容的 LT。该 LT 包括用于解密加密后的内容的内容键，和从内容中赋予用户的使用权利（许可）中提取其中一部分的提取使用条件。

用户终端 200a-200c 为个人计算机、便携式信息终端、数字电视等计算机装置，用作对于服务器 100 的客户。具体而言，用户终端 200a-200c 对应于用户的操作，使用因特网浏览器软件等工具来访问服务器 100 的网页，在发送内容购入请求后接收内容的配送，同时根据内容使用来发送 LT 发送请求，接收 LT，在 LT 提取使用条件范围内再现内容。

可在用户终端 200a 上安装用户终端 200b 用的外部媒体 500b（例如 SD

卡) 和用户终端 200c 用的外部媒体 500c (例如 IC 卡), 如此构成, 以将用户终端 200a 保持的内容或 LT 一边转录到外部媒体 500b、500c 上, 一边移动, 通过用户终端 200b、200c 来再现内容。

通信网络 300 为因特网、CATV 等有线或数字播放等无线通信媒体。

图 5 是表示图 4 所示服务器 100 和用户终端 200a-200c 的结构的功能框图。因为用户终端 200a-200c 的功能结构相同, 所以图示用户终端 200a 作为代表。另外, 本图中还同时表示了通信网络 300。

服务器 100 粗分是, 包括由存储于硬盘等中的数据文件实现的数据部(用户管理 DB110、用户权利信息 DB120、内容信息 DB130、内容 DB140); 及由 CPU、RAM、ROM 等硬件和 CPU 执行的程序等实现的处理部 (用户认证部 150、用户权利处理部 160、许可信息生成部 165、内容信息生成部 170、内容信息加密部 175、内容取得部 180、内容加密部 185、通信部 190)。

用户管理 DB110 存储在该内容使用管理系统 1 中进行了会员注册的用户的用户信息等。具体而言, 用户管理 DB110 为了管理用户的权利, 使用分配给每个用户终端的唯一的客户 ID (终端 ID), 对应于包含用户 ID 的用户信息来进行管理。是存储多个用于注册・管理、进行了会员注册的用户所具有的用户终端客户 ID、赋予该用户的固有 ID 信息 (用户 ID) 和该用户的用户信息等的用户管理表格 111 的存储部。

用户权利信息 DB120 存储用户对于内容的权利信息 (许可)。具体而言, 用户权利信息 DB120 为存储多个在每个使用状态 (例如再现、移动、复制、印刷、使用期限等) 下管理用户购入的内容或用户对该内容具有的使用权 (许可) 的残留信息所用的用户权利信息管理表格 121 的存储部。

内容信息 DB130 存储内容的关联信息 (内容键等)。具体而言, 内容信息 DB130 保持用于加密内容的多个内容键 131 和记录该内容键 131 与内容 ID 的对应关系的内容键表格 132 等。

内容 DB140 存储内容。具体而言, 内容 DB140 存储并保持多个内容 141 和记录该内容与内容 ID 的对应关系的内容表格 142。

用户认证部 150 进行用户认证。具体而言, 用户认证部 150 根据从用户

终端 200a-200c 接收到的内容购入请求或包含于 LT 发送请求中的 ID 信息(许可 ID)，使用用户管理表格 111，特定用户 ID 或由用户管理的权利。用户认证部 150 一边在用户住所等变更的情况下更新用户管理表格 111 的用户信息，一边在购入用户终端装置的情况下向用户管理表格 111 追加许可 ID。

用户权利处理部 160 一边根据购入请求注册用户对内容的权利信息，一边根据使用请求更新权利信息。具体而言，用户权利处理部 160 通过根据内容购入请求来执行收费处理，将该用户的权利注册在用户权利信息 DB120 的用户权利信息管理表格 121 中。

因为收费处理本身不是本发明的本质，所以图中未记载执行收费处理的部分。在注册用户权利时，赋予内容提供者设定的初始值，作为由用户管理的用户权利信息的 UR-U_s (关于服务器的用户使用规则: Usage Rule for User on server)。用户权利处理部 160 在有 LT 发送请求时，确认是否可从此时的权利信息 UR-U_s 中向用户提取请求部分的使用权 UR-U_c (关于客户的用户使用规则: Usage Rule for User on client)。在向许可信息生成部 165 传送确认并请求的使用权 UR-U_c 的同时，将用户管理的权利信息 UR-U_s 更新为仅减少提取部分 UR-U_c 后的内容。在存在用户权利处理部 160 一边增加来自内容提供者的权利信息的变更通知、例如在对内容购入者的服务中的使用次数，一边延长使用期限的通知的情况下，一律更新各内容购入者的许可信息。

许可信息生成部 165 生成被请求内容的使用权、许可信息。

内容信息生成部 170 一边从内容信息 DB130 取得内容键，一边生成包含从许可信息生成部 165 传送来的许可信息或取得的内容键的信息的内容信息 (LT)。具体而言，内容信息生成部 170 访问内容信息 DB130，使用内容键表格 132，取得对应于内容 ID 的内容键 131，并生成包含该内容键和从许可信息生成部 165 传送来的许可信息、提取使用条件 (UR-U_c) 的 LT。

内容信息加密部 175 对内容信息进行加密。

具体而言，内容信息加密部 175 在附加 LT 内容键和脚注 (footer) 的情况下，必要时根据该脚注进行加密。该加密例如通过发出 LT 发送请求的用户终端 200a-200c 的终端 ID 来进行加密。由此，当通过客户 ID 进行加密时，可

将 LT 赋值给具有该宽客户 ID 的用户终端。

也可使用公开键密码方式，通过用户公开键来进行加密。另外，也可使用服务器和终端公共的密钥来进行加密。

在服务器 100、用户终端 200a-200c 之间，例如通过 SSL（加密套接字协议层）等的相互认证形式来形成 SAC（Secure Authenticated Channel：安全认证信道），在服务器和终端之间确保安全信道的情况下，任意（不是必须）加密许可信息。但在本实施例中，说明在服务器终端之间形成 SAC 的同时，内容信息加密部 175 执行 LT 加密处理。

内容取得部 180 从内容 DB140 处取得指定的内容。具体而言，内容取得部 180 参照内容 DB140 的内容表格 142，取得对应于内容 ID 的内容 141，传送给内容加密部 185。

内容加密部 185 加密内容。具体而言，内容加密部 185 加密从内容加密部 185 传送来的内容。该加密通过内容键来进行加密。

通信部 190 与用户终端 200 进行通信。具体而言，通信部 190 为通过通信网络 300 与用户终端 200a-200c 进行通信的由记录在网页上的命令表（script）或程序等实现的通信接口，分析从用户终端 200a-200c 发送来的命令或信息，根据该结果，边依赖于用户认证部 150 的处理，边向用户终端 200a-200c 配送从内容加密部传送来的内容，向用户终端 200a-200c 配送从内容信息加密部 175 传送来的 LT，在与终端之间形成 SAC。

另一方面，用户终端 200 包括通信部 210、操作部 220、ID 信息存储部 230、内容存储部 240、LT 存储部 245、内容信息解密部 250、许可信息处理部 260、内容解密部 270 和外部媒体访问部 280。

通信部 210 与服务器 100 之间进行通信。具体而言，通信部 210 为根据浏览软件等通过通信网络 300 与服务器 100 进行通信的通信接口，根据来自操作部 220 的请求，发送内容购入请求或 LT 发送请求的信息，并将服务器 100 发送的内容存储于内容存储部 240 中，将 LT 存储于 LT 存储部 245 是，在与服务器 100 的通信部 190 之间形成 SAC。

操作部 220 为接收用户操作并显示服务器 100 提供的网页的用户接口。

ID 信息存储部 230 存储其终端的 ID 信息（客户 ID）。具体而言，ID 信息存储部 230 存储并保持事先赋予每个终端的固有的客户 ID。另外，ID 信息存储部 230 也保持用于加密 LT 的公开键加密方式的公开键或密钥键，或公共键加密方式的加密键。

内容存储部 240 例如由 HDD 等构成，存储加密后的内容。

LT 存储部 245 存储从通信部 210 发送来的 LT。

内容信息解密部 250 根据接收到的内容信息（LT）解密内容键和许可信息。具体而言，内容信息解密部 250 通过客户 ID、公开键加密方式的密钥键或公共加密方式的密钥键来解密包含于存储于 LT 存储部 245 中的 LT 内容键等。

许可信息处理部 260 根据许可信息来识别是否可行使用内容键。具体而言，该处理部 260 判断是否可行再现，如果可以再现，则向内容解密部 270 传送内容键，提取内容解密部 270 的内容再现处理，进行监视，以便遵守使用条件。

内容解密部 270 对通过从许可信息处理部 260 处取得的内容键加密的内容进行解密。具体而言，内容解密部 270 使用从许可信息处理部 260 处获得的内容键解密加密的内容，在许可信息处理部 260 的管理下再现内容。

外部媒体访问部 280 向外部媒体 500b 或外部媒体 500c 输出内容和 LT 中的任一方或双方。

将上述 ID 信息存储部 230、LT 存储部 245、内容信息解密部 250、许可信息处理部 260 设置在对硬件耐篡改的安全模块、例如内置芯片的 IC 卡内。此时，加密的许可信息的解密及许可信息处理也可通过安全模块来进行。确立 SAC 的状态下从服务器取得 LT 时，因许可信息加密是任意的，故仅在加密许可信息时才做解密处理。故不可能从外部访问著作权保护上的重要秘密信息、客户 ID、包含于 LT 的内容键、使用条件等，针对在物理上要盗取这些秘密信息等的猛烈攻击，也成为很强的设计。其中，安全模块也可是耐篡改的软件。另外，许可信息处理部 260 也可设置在用户终端的安全部分中。

在此如此构成的内容使用管理系统 1 中，对于各用户内容的权利信息基本

上全部由配送服务器侧进行管理。用户购入（或预购）的内容以加密状态存储于用户终端 200a 的内容存储部 240 中。在一边再现存储于用户终端 200 中的内容、一边进行移动或复制的情况下，从用户终端 200 向服务器 100 发出请求、LT 发送请求信息。服务器 100 确认对于用户请求的内容的使用条件（或购买条件）UR-Us，当存在用户的使用权时，向用户配送包含“许可信息”和内容键的内容信息、LT。许可信息由是否可行再现、移动、复制内容等的信息构成，用户终端执行由许可信息许可的内容的使用。

在用户通过购入等取得各个内容的情况下，服务器 100 的用户权利信息 DB120 中，管理涉及用户取得的内容的使用条件。将该形式称为每次购入型模型。该系统也可适用其它订购型（预购型）模型。该订购型是在播放上称为所谓的包月收费（tear billing）形态，是所谓的当进行信道购买时，可看见该信道的整个节目的收费形态。此时，在用户权利信息 DB120 中保持购买信息作为用户权利信息。

图 6 是表示图 5 所示用户管理表格 111 的结构实例的图。

该用户管理表格 111 由赋予加入该内容使用管理系统 1 的用户的用户 ID、与该用户 ID 相关联的用户信息（“姓名”、“住址”、“电话号码 1”、“电话号码 2”、…“电子邮件 1”、“电子邮件 2”…）或事先赋予该用户在该内容使用管理系统 1 中使用的用户终端的客户 ID（“客户 ID1”、“客户 ID2”、“客户 ID3”…）等构成。根据如此构成的用户管理表格 111，当知道客户 ID 时，可特定拥有该客户 ID 的终端设备的用户的用户 ID。

图 7 是表示图 5 所示用户权利信息管理表格 121 的结构实例的图。

该用户权利信息管理表格 121 由客户 ID 或用户 ID、用户购入的内容的内容 ID、对每个内容 ID 设定的由服务器管理的用户使用权（UR-Us）的 ID、对用户拥有的使用权（许可）的每个使用状态设定的残留（差额）信息等构成。对每个使用状态设定的残留信息分别表示可再现几次各用户购入的内容，可移动几次该内容，可复制几次该内容，可使用几次该内容，或可打印几次该内容等。另外，附属设定于残留信息中的最长使用时间表示，于再现处理等可连续使用内容的最大时间，一次判定阈值表示内容的使用被判断为一次

时的时间，积累使用时间表示可使用内容的积累时间。

使用权的内容在内容提供者或服务器管理者根据内容属性对每个内容事先设定初始值，在购入内容时赋予初始值作为许可的残留信息。其中，即使内容相同，也可是因用户取得的使用条件而存在价格不同的买卖形态下，因购入价格而不同的初始值。该许可残留信息对根据用户的 LT 发送请求提取的使用条件、许可信息中的每一个都从初始值开始依次减少，根据内容提供者的服务提供请求来增加。

在该用户权利信息管理表格 121 中，通过用户 ID 来管理使用权，但也可使用客户 ID 来管理用户的使用权。

图 8 是表示图 5 所示许可信息的结构实例的图。

该许可信息由提取的使用权、例如使用条件最小限度的使用条件要素信息生成，由涉及内容使用的一个或多个是否可行信息形成，各是否可行信息由仅表示是否可行的参数构成。其中，图 8 中所示 α 为关于活动、再现的是否可行信息，图 8 中所示 β 为关于活动、移动的是否可行信息，图 8 中所示 γ 为关于活动、复制的是否可行信息。这些是否可行信息的种类和数量，根据内容的属性而变化。

其中，虽然说明了最小限度的使用权的情况，但在用户请求的情况下，也可生成请求提取的使用权、即，不仅是否可行，而且包含可以情况的多次使用条件的许可信息。另外，图 8 中，虽然表示了一个许可信息由多个涉及内容使用的条件构成的实例，但也可构成许可信息来作为各自独立的信息，并将其多个组合后来得到作为对于一个内容的许可信息。

图 9 是表示内容信息生成部 170 生成的内容信息、LT 的数据格式结构的图。

内容信息生成部 170 生成的 LT600 由 LT 标题 610、许可信息、即作为内容操作内容的活动、表示对于活动的条件等的一个或多个 LT 活动标记块 620#1-620#n、LT 内容键标记块 630、和 LT 脚注 640 构成。

LT 标题 610 由表示该数据是由该内容使用管理系统 1 获得的许可证的 LT 识别符 611、表示由该内容使用管理系统 1 设定规格的版本的版本序号 612、

表示 LT 整体的数字尺寸的 LT 尺寸 613、表示该 LT 相关联的内容的内容 ID 的内容 ID614、表示变为该 LT 的发送源的 UR-UsID 的 UR-UsID615、表示 LT 变为有效的日期时间的 LT 有效期限开始时刻 616、表示 LT 变为无效的日期时间的 LT 有效期限结束时刻 617、表示是否许可从某个用户终端向可搬运的外部媒体或其它用户终端移动内容或 LT 等的 LT 移动许可标志 618、和表示适用于 LT 内容键标记块 630 和 LT 脚注 640 的加密方式 (DES、AES 等) 的 LT 加密方法 619 构成。

LT 活动标记块 620#1-620#n 由表示特定对于内容的活动内容 ID 的活动 ID621、表示可连续操作内容的最大时间的最长使用时间 622、表示内容操作被判断为一次的时间的一次判定阈值 623、表示可由该 LT 操作的内容的最大次数的次数计数 624、表示可操作内容的积累操作时间的积累使用时间 625 构成。将最长时间设定为通常比 2 小时长的值 (例如 4 小时)，以便即使为了电视播放广告而暂时中断 (暂停) 再现时，也可观看到电影的结局。另外，积累使用时间用于比最长使用时间还进行严密控制的情况下，通常设定成比 2 小时长比最长使用时间短的值 (例如 3 小时)。

其中，在一次判定阈值 623 为“0”时，用户终端 200a 在开始时刻将内容操作 (使用) 判定为一次，在指定某个时间的情况下，到达该时间时判定为一次。另外，在每进行内容操作时都减少次数计数 624 中设定的值。在一次判定阈值有效的情况下 (非“0”的情况下)，在到达一次判定阈值的值的时刻减去内容的连续操作时间。在连续操作期间，仅对次数计数进行一次减法。另外，根据内容的操作时间来减去最长使用时间 622 和积累使用时间 625 中设定的时间。但是，虽然在暂停中也减去最长使用时间 622 中设定的时间，但积累使用时间 625 中设定的时间在暂停时不停止减法。如果次数计数 624 的值为 1 以上，则表示可以，若为 0，则表示不可以，另外，若为 1，则表示最小限度的使用条件。也可将次数计数 624 用作是否可行信息。

LT 内容键标记块 630 存储解除与该 LT 相关联的内容的加密的解密键、内容键。

LT 脚注 640 为随意附加的功能块，在附加的情况下，为了防止从 LT 标

题 610 至 LT 脚注 640 的正前方、即 LT 内容键标记块 630 的部分被篡改，存储 SHA-1 算法的散列值。

虽然在 LT600 中将内容 ID 存储于 LT 标题 610 中，但将内容 ID 设定为内容信息和与内容相关联的识别符，由此，根据内容使用时取得的内容 ID，因为内容信息为可特定的重要信息，也可存储于标记块中。

对于以上构成的本发明实施例的内容使用管理系统 1，下面用图 10 所示流程图来说明内容购入时的动作。

图 10 是表示该系统中，在用户购入内容的情况下，用户终端 200a 和服务器 100 中各自进行的处理的流程图。

在购入内容的情况下，用户终端 200a 的用户操作操作部 220，访问服务器 100 的网页，显示图 11 所示的内容购入画面（1）。

该内容购入画面（1）可由该系统网络购入的内容种类、“音乐”、“游戏”、“电子书籍”、“电影”、…、“收费电视节目”的显示、选择这些种类的复选栏、“继续”按钮、“返回”按钮等构成。

在想购入的内容种类为音乐时，用户操作操作部 220，点击对应于“音乐”的复选栏，按下“继续”按钮。由此显示图 12 所示的内容购入画面（2）。

该内容购入画面（2）由种类、属于音乐的曲子的“内容 ID”、“标题名称”、“权利信息”、“出售价格”的内容、选择这些曲子的复选栏、“购入”按钮、“返回”按钮等构成。在“权利信息”中显示由内容提供者设定的使用条件、即残留信息的初始值、再现次数、移动次数、复制次数、使用期限等。在想购入的曲子是“冲浪乔治”的情况下，用户操作操作部 220，点击对应于“冲浪乔治”的复选栏，按下“购入”按钮，输入内容购入请求。

当存在用户的内容购入请求时，用户终端 200a 的通信部 210 在与服务器 100 的通信部 190 之间形成 SAC 之后，取得存储于 ID 信息存储部 230 中的用户终端 200 的 ID 信息（客户 ID），将包含该 ID 信息的内容购入请求信息发送给服务器 100（S1）。该内容购入请求信息例如由表示内容购入的内容 ID、希望购入的内容的内容 ID、和请求内容购入的用户终端的客户 ID 等构成。

用户认证部 150 通过服务器 100 的通信部 190 接收该信息时，将接收到

的 ID 信息与存储于用户管理 DB110 中的 ID 信息进行对照进行用户认证后，将内容购入请求传送到用户权利处理部 160 (S2)。具体而言，用户认证部 150 参照用户管理表格 111，根据客户 ID 特定用户 ID 后，将用户 ID、内容 ID 等作为内容购入请求传送给用户权利处理部 160。

用户权利处理部 160 在进行内容购入的收费处理后，将用户对于购入内容的权利信息注册在用户权利信息 DB120 中 (S3)。具体而言，用户权利处理部 160 访问用户权利信息 DB120，根据用户 ID (pana01) 来特定购入内容的用户（例如东口△）用的用户权利信息管理表格 121（参照图 7）。用户权利处理部 160 分别在用户权利信息管理表格 121 的内容 ID 栏中存储曲 1，在每个内容 ID 的许可信息栏中分别存储曲 1 的权利信息 UR-U_s 的 ID、“权利信息 A”及其内容。在该权利信息 A 的内容中设定内容提供者设定的初始值的残留信息（再现次数、移动次数、复制次数等）。之后，用户权利处理部 160 将内容 ID 传送给内容信息生成部 170。

内容信息生成部 170 从内容信息 DB130 中取得该内容的关联信息（内容键等）后传送到内容取得部 180 (S4)。具体而言，内容信息生成部 170 访问内容信息 DB130，参照内容键表格 132，取得对应于内容 ID 的内容键 131，将取得的内容键和内容 ID 传送给内容取得部 180。

内容取得部 180 从内容 DB140 处取得该内容，内容加密部 185 使用内容键对该内容进行加密 (S5)。具体而言，内容取得部 180 访问内容 DB140，参照内容表格 142，取得对应于内容 ID 的内容，将取得的内容、从内容信息生成部 170 处接收的内容键和客户 ID 传送给内容加密部 185。内容加密部 185 使用内容键对接收的内容进行加密，将加密后的内容传送给通信部 190。服务器 100 的通信部 190 将加密后的内容发送给用户终端 200 (S5)。

用户终端 200 的通信部 210 在接收加密后的内容时 (S6)，向内容存储部发送内容并进行存储 (S7)。

通过这些用户终端 200a 和服务器 100 的各自执行的处理，结束内容购入时的对话 (session)。

在内容购入时的对话中，在用户终端 200a-服务器 100 之间形成 SAC，因

为可用公共的对话键进行加密通信，所以可防止内容购入请求信息或加密内容在网络上被解密。

图 13 是表示该系统中，在用户使用内容的情况下，用户终端 200a 和服务器 100 中各自进行的处理的流程图。

在使用内容的情况下，用户终端 200a 的用户操作操作部 220，显示图 14 所示的使用内容选择画面。该使用内容选择画面由用户终端 200a 的用户购入的内容标题、内容 ID 或预购的内容的许可证的事先申请等、这些内容的复选栏、“继续”按钮、“返回”按钮等构成。

在使用内容的情况下，输入用户操作操作部 220 再现的内容的使用信息。具体而言，用户显示图 14 所示的使用内容选择画面，向希望再现的内容（例如冲浪乔治）的复选栏中输入复选标记，点击“继续”按钮。之后，显示图 15 所示内容使用请求画面。内容使用请求画面由该内容可使用的活动、再现、移动、复制，选择该活动的复选栏、输入活动次数的文字栏、“确定”按钮、“返回”按钮等构成。

作为输入使用信息的一个环节，用户操作操作部 220，在选择的内容（冲浪乔治）中，向必要的请求内容（本例中为再现、移动）复选栏中加入复选标记，向加入复选标记的请求内容的文字栏中输入请求数量（在本例中，再现为“2”次，移动为“1”次），点击“确定”按钮。

当向复选栏中加入复选标记时，事先向该文字栏中输入“1”，作为最小使用条件。在用户希望使用“2”次以上的情况下，向文字栏中输入希望的次数。

当存在用户的内容再现请求时，用户终端 200 的通信部 210 在与服务器 100 的通信部 190 形成 SAC 之后，取得存储于 ID 信息存储部 230 中的用户终端 200 的 ID 信息（客户 ID），并向服务器 100 发送包含该 ID 信息的 LT 发送请求信息（S11）。该 LT 发送请求信息例如由表示 LT 发送请求的信息 ID、使用对象的内容的内容 ID（例如曲 1）、内容再现请求、即表示内容使用请求内容的请求信息（再现 2 次、移动 1 次）、请求 LT 发送的用户终端的客户 ID（例如 nat01）等构成。

通过服务器 100 的通信部 190 接收该信息的用户认证部 150 在对照接收到的 ID 信息和存储在用户管理 DB110 中的 ID 信息进行用户认证后，将用户信息和内容再现请求发送到用户权利处理部 160 (S12)。具体而言，用户认证部 150 参照用户管理表格 111，根据客户 ID 特定用户 ID 后，向用户权利处理部 160 传送用户 ID、客户 ID、内容 ID、请求信息等，作为内容再现请求。

在用户权利信息 DB120 中注册用户权利处理部 160。确认对于请求内容的用户权利信息 (S13)。具体而言，用户权利处理部 160 访问用户权利信息 DB120，根据用户 ID (pana01) 来特定使用内容的用户（例如东口△）用的用户权利信息管理表格 121（参照图 7）。用户权利处理部 160 参照用户权利信息管理表格 121 的内容 ID 栏、曲 1，确认在曲 1 的残留信息 (UR-U_s) 中是否包含再现、移动，是否剩余对再现、移动请求的次数等。

通过判定请求的内容包含于何种订购（单）中，以及用户是否具有该订购，来确认订购型（预购型）情况下的用户权利信息。

当注册的权利信息中包含对于请求内容的再现权利信息时 (S14)，用户权利处理部 160 根据该权利信息向许可信息生成部 165 传送是否可行再现，更新再现的权利信息的内容（可再现次数的减少）后存储于用户权利信息 DB120 (S15) 中。许可信息生成部 165 根据从用户权利处理部 160 传送来的信息生成许可信息，并传送到内容信息生成部 170 (S15)。具体而言，如图 16 所示，用户权利处理部 160 将用户 ID “pana01”的内容 ID 的残留信息、再现次数“10 次”、移动次数“2 次”、复制次数“3 次”更新为再现次数“8 次”、移动次数“1 次”、复制次数“3 次”，即将使用条件 (UR-U_s) 中再现从 10 次减少为 8 次，将移动从 3 次减少到 2 次，许可信息生成部 165 将再现次数“2 次”、移动次数“1 次”的许可信息传送给内容信息生成部 170，作为 LT 发送给用户终端 200a。

通过服务器侧的判断，可将满足用户终端请求的使用权利的使用权利作为 LT 进行发送。例如，即使在用户终端请求两次再现权利的情况下，通过将一次的再现权利作为 LT 来发送，通过业务判断等，可确保所谓的每次发送最

小限度使用权利的策略。

内容信息生成部 170 从内容信息 DB130 中读出该内容的内容键信息，生成包含该内容键和许可信息的内容信息 (LT) (S16)。具体而言，内容信息生成部 170 生成由 LT 标题 610、活动再现中的次数计数值 “2” 的 LT 活动标记块 620#1、在活动、移动中的次数计数值 “1”的 LT 活动标记块 620#2、LT 内容键标记块 630 和 LT 脚注 640 构成的 LT600。内容信息加密部 175 加密该内容信息 (S16)。具体而言，内容信息加密部 175 加密 LT 内容键标记块 630 和 LT 脚注 640。

服务器 100 的通信部 190 将加密后的内容键和许可信息作为 LT 发送给用户终端 200。

在步骤 S14 中，当用户的权利信息中不包含涉及请求内容的再现权利信息时，从服务器 100 向用户终端 200 发送不可再现应答信息。该不可再现应答信息例如由表示作为对 LT 发送请求信息的应答的信息 ID 和表示不存在、不可再现对应于请求的 UR-Us 的状态 ID 构成。

另一方面，在用户终端 200 中，接收内容信息的通信部 210 将 LT 存储于 LT 存储部 245 中后，向内容信息解密部 250 发送 LT 和存储于 ID 信息存储部 230 中的客户 ID (S18)。内容信息解密部 250 使用客户 ID 对加密后的内容信息 (LT) 进行解密，将许可信息和内容键传送给许可信息处理部 260 (S18)。

许可信息处理部 260 检验许可信息的是否可行再现信息 (S19)，当可以再现时 (S20)，向内容解密部 270 传送内容键。具体而言，许可信息处理部 260 检验活动、再现的次数计数是否为 1 以上，当为 1 以上时，向内容解密部 270 传送内容键。内容解密部 270 从内容存储部 240 处取得内容 (S21)，使用内容键解密内容，在许可信息处理部 260 的提取使用条件的管理下，再现曲 1 “冲浪乔治” (S22)。

在活动、再现的 LT 活动标记块 620#1 中除次数计数值外，还包含一次判定阈值、最长使用时间、积累使用时间。

因此，在用户终端的内容再现中，采取在从再现开始经过一定时间时，判断进行一次再现的方式，通过从配送服务器配送该一定时间的信息，可改

变一定时间。

作为在再现开始时刻进行一次再现，可采取如下方式：若在从再现开始后的一段时间内，则可当做相同的再现，允许再现，配送表示该范围的信息，可作为一次再现的期限。

即，如图 17 所示，若将某一时间设定为一次判定阈值，在该时间未界满时再现（例如卷到头等事先再现等）的情况下，不将该再现计数为一次。在到达一次判定阈值开始，可计数为一次再现。另外，若将某个时间设定为最长使用时间，则在到达最长使用时间之前，通过仅消耗一次再现权利，可断续地再现该内容，所以可实现所谓在再现中可暂时停止（暂停）的弹性使用形式。若将某个时间设定为积累使用时间，则在到达该积累使用时间之前，可积累再现内容。因此，可对用户提供多种内容使用。

也可根据内容种类（例如电影和音乐）来改变涉及可再现期间的判断方式的策略。

当从服务器 100 接收不可再现应答信息时（S17），并且在步骤 S20 中不可再现许可信息时，不再现内容，结束处理。其中，通过由表示对应于请求的使用权 UR-U_s 不存在的状态码 ERROR-URUS 形成的应答信息来进行不可再现的通知。另外，也可由包含再现次数计数值为“0”的 LT 活动标记块 620 的 LT 来通知不可再现。

在许可信息规定仅可使用一次内容的情况下，许可信息处理部 260 在使用内容之后，消除该许可信息，或设定表示为无效的标志等，来进行无效许可信息（LT）的处理。

在许可信息包含多个活动条件（例如再现和移动）、并与其一起作为对于一个内容的许可信息时，仅无效该使用条件（例如再现）。

即使是订购型，可能存在对各内容识别无限制使用的情况（例如包月收费），也存在规定使用上限的情况（例如，PPV（付费选取看节目）时，每月的上限为 5000 日圆等）。在有使用条件上限的情况下，当确认用户的权利信息时，在判定所述合同后，判定用户是否具有该内容的使用条件（每次合同型的判定）。用户权利信息 DB120 也可分离合同信息的数据库和使用条件数据库进

行管理。

这里，在内容使用管理系统 1 中，当内容的移动或复制通过许可信息为“可以”时，通过外部媒体访问部 280，可在向外部媒体 500b、500c 移动内容的同时，移动权利信息（使用条件）和内容键。此时，权利信息通过变换为外部媒体 500b、500c 支持的数据形式来进行移动或复制。另外，也可通过外部媒体 500b、500c 支持的加密方式来加密变换（再次加密）内容，同样，也可将内容键变换为对应于外部媒体 500b、500c 支持的加密方式的加密键。由此，通过使用外部媒体，可通过本内容使用管理系统和其它内容管理方法实现内容的著作权保护，可使用内容。另外，在外部媒体支持本发明的内容使用管理系统 1 的情况下，不必进行权利信息的数据变换或内容的加密变换。

图 18 是表示该系统中，在向外部媒体移动内容或 LT 的情况下，用户终端 200a 所进行的处理的流程图。

在移动内容或 LT 的情况下，用户终端 200a 的用户操作操作部 220，显示图 19 所示的移动内容选择画面。该移动内容选择画面由用户终端 200a 的用户购入的内容标题、内容 ID 或事先接收的许可证等、这些内容、LT 的复选栏、“确定”按钮等构成。用户显示图 19 所示的使用内容选择画面，向希望移动的内容（例如冲浪乔治）复选栏输入复远标记，点击“确定”按钮。

当存在用户的内容移动请求时，用户终端 200a 的许可信息处理部 260 向内容信息解密部 250 传送存储于 ID 信息存储部 230 中的客户 ID、存储于 LT 存储部 245 中的 LT。内容信息解密部 250 使用客户 ID 对加密的内容信息（LT）进行加密，向许可信息处理部 260 传送许可信息和内容键。

许可信息处理部 260 检验许可信息的是否可行移动信息，判断是否可行使用，即判断移动的 LT 活动标记块 620#2 的次数计数值是否为 1 以上（“使用前”或“并在使用后可使用”的情况下）(S31)。若可使用 (S31 为是)，则通过内容解密部 270、外部媒体访问部 280 来判断外部媒体 500b 或外部媒体 500c 是否可行处理 LT (S32)。

若不能处理 (S32 为否)，则许可信息处理部 260 判断是否可行将使用条件格式变换已转换成内容控制信息的信息 (S33)。即，许可信息处理部 260

判断外部媒体 500b 或外部媒体 500c 是否可通过内容控制信息由耐篡改的安全模块管理内容。若可管理，则许可信息处理部 260 将移动的 LT 活动标记块 620#2 变换为内容控制信息 (S34)，将变换后的内容控制信息和内容键传递给内容解密部 270。内容解密部 270 从内容存储部 240 处取得内容，使用内容键解密内容，将解密后的内容和从许可信息处理部 260 传送来的内容控制信息传递给外部媒体访问部 280。外部媒体访问部 280 将从内容解密部 270 传递来的解密内容和内容控制信息移动到外部媒体 500b 或外部媒体 500c (S35)。

若步骤 S32 中为可处理，则许可信息处理部 260 将 LT 传递给内容解密部 270。内容解密部 270 从内容存储部 240 处取得内容，使用内容键解密内容，将解密后的内容和从许可信息处理部 260 传递来的 LT 传递给外部媒体访问部 280。外部媒体访问部 280 将从内容解密部 270 传递来的解密内容和 LT 移动到外部媒体 500b 或外部媒体 500c (S35)。此时，内容解密部 270 不对内容进行解密，而是传递给外部媒体访问部 280，外部媒体访问部 280 也可原样加密内容后移动到外部媒体 500b 或外部媒体 500c (S35)。

通过该外部媒体 500b 或外部媒体 500c，即使是便携式信息终端或数字电视等其它终端，也可使用内容。

在步骤 S31 为不可使用的情况下，即移动的 LT 活动标记块 620#2 的次数计数值为“0”时，或在步骤 S33 中，外部媒体 500b 或外部媒体 500c 不能通过内容控制信息由耐篡改的安全模块管理内容的情况下，许可信息处理部 260 结束移动处理。从而不损害著作权。

虽然在该流程图中说明了移动，但通过将步骤 S35 变更为复制的处理，也可适用于复制处理。另外，也可向外部媒体 500b 或外部媒体 500c 仅移动或复制事先写入的 LT。

如上所述，在本系统中，可在配送服务器侧作为主体管理各用户对内容的使用。因此，服务器可把握各用户终端上的内容使用状况。即使在有奖活动中实施扩大用户取得权利的服务，也可仅通过上升存储于配送服务器中的用户权利信息来实现。

另一方面，用户终端根据许可信息，仅通过执行涉及再现或移动、复制等的控制就可实现，避免了复杂使用条件管理的负担。另外，通过在配送服务器侧一维化这种使用条件的管理，可防止终端的使用条件的篡改等不正当使用。

从以上说明可知，根据本实施例的内容使用管理系统，服务器 100 包括存储涉及使用用户终端 200a 的用户所具有的内容的使用权限的权利信息的用户权利信息 DB120；和根据来自所述服务器的请求，生成作为表示该用户所具有的部分使用权限的权利信息的 LT，并发送给用户终端 200a 的内容信息生成部 170，用户终端 200a 包括接收从服务器 100 发送的 LT 的通信部 210；和根据接收到的 LT 表示的使用权限，控制内容使用的许可信息处理部 260。

因此，在终端装置中不必管理用户所具有的全部使用权限，通过仅管理许可证表示的用户的部分使用权限，就可控制内容的使用，大大减轻终端装置的管理负担。另外，服务器装置可在许可证发送的同时，把握各终端装置处的内容的使用状况，即使在终端装置处进行内容复制等的情况下，也可通过在服务器装置中进行复制许可的对照来检测何时在何种媒体中进行复制，可追踪内容。因为通过服务器装置保持用户所具有的使用权限，所以即使在终端装置的存储装置（HDD）紊乱的时候，也可容易恢复用户的使用条件等，另外，可容易地进行扩大所谓自动对内容的使用条件的再现次数加 1 的这种实施服务的使用条件的服务或使用条件的追加等处理。另外，因为终端装置的内容使用控制装置根据接收的许可证表示的使用权限，控制所述内容的使用，所以可确实防止终端装置处内容的无限制使用。

在上述实施例中，在内容 DB140 中存储未加密的内容，虽然在内容购入时加密内容后配送（图 10、S5），但也可事先在服务器 100 中用内容键加密内容后存储于内容 DB140 中。此时，在接收来自用户的购入请求的情况下，可原样配送加密后的内容，可减轻服务器的负荷及用户的等待时间。

在上述实施例中，虽然说明了通信中传送内容和 LT 的情况，但也可通过播放来传送内容或 LT。此时，将用户的许可信息在使用内容前配送给用户终端，或通过播放同时配送内容和 LT，则可直接使用接收到的内容，可提高内

容使用时的应答。另外，可取消内容使用时的通信处理，减轻配送服务器的负荷。

在上述实施例中，在服务器—终端之间形成 SAC 的同时，虽然由内容信息加密部 175 执行了 LT 的加密处理，但也可省略内容信息加密部 175 的 LT 加密处理。

在从服务器取得许可信息时，在未加密许可信息的情况下，当将 LT 存储于 LT 存储部 245 中时，为了防止内容键的暴露、不正当篡改、其它用户的不正当使用，也可由终端 ID（客户 ID）等用户固有信息进行加密后存储。因此，在由耐篡改的硬件实现 LT 存储部 245 的情况下，没必要加密。

在 CD-ROM、DVD-ROM 等记录媒体中配置记录了各种加密内容的信息，作为杂志的附录，也可适用于用户购入注册信息时的形态。或者，使用播放系统的配送路径，配送业务者方开始配送各种内容，对于用户终端 220a 内容存储部 240 中进行存储而言，也可适用于用户仅购入注册信息的形态。在这些情况下，用户通过进行购入手续，可在服务器 100 的用户权利信息 DB120 中生成对应于用户注册的内容的权利。由此用户可在内容使用时请求发送 LT。根据这种形态，因为可极力抑制内容配送中的成本，所以可抑制内容自身的价格。

将加密内容记录在 CD-ROM、DVD-ROM 等记录媒体中也可适用于与通常的数据包一样买卖的形式。购买这种记录媒体的用户履行注册手续，在用户 100 内的用户权利信息 DB120 中生成对应于购入内容的权利。之后在使用内容时可请求发送 LT。

在上述实施例中，在用户请求再现后，请求发送 LT，确认 LT 存储部 245 中是否具有 LT，当有 LT 时，用该 LT 来判断是否可行再现，若可再现，则再现，在没有 LT 的情况下，开始请求发送 LT。

另外，在上述实施例中，请求再现内容的用户在没有该内容的再现权利时（图 13 的步骤 S14 为否），通知不可再现，配送用户通知不可再现，获得用户的了解，或作为得到默许了解，也可进行该再现权利的追加购入的处理。此时，向默许了解中追加购入处理的方式仅在使用上变为所谓的收费服务，

简化了购入手续。

这里，虽然说明了许可信息具有涉及一次再现、移动或复制的可/不可的参数的情况，但许可信息中可包含表示仅许可再现一次内容或许可无限制之一的参数，并可包含表示不许可内容移动或许可无限制之一的参数。此时，当许可信息表示无限制许可时，用户终端 200a 的许可信息处理部 260 保持内容键，进行经常向内容解密部 270 提供内容键的操作。

通过由许可信息与多个是否可行信息相组合，可设定各种内容使用条件。例如，仅配送再现是否可行信息和移动是否可行信息，通过对对其进行组合，实现所谓的登记/结帐（Check-in/Check-out）的处理。当登记/结帐在复制内容时，不仅进行复制，也可通过可再现、不可移动（当然不可复制），形成母内容与子内容的关系，防止子内容的自由移动。在该许可信息的情况下，配送服务器保持登记/结帐的信息，作为许可信息，不必特地要求所谓的登记/结帐是否可行信息，由服务器侧或接收侧管理登记/结帐时的母（服务器）和子（存储媒体）的关系，并且，作为配送的信息，可通过仅组合再现和移动来表现。因此，削减了配送给用户终端的参数，从而可减轻用户终端的负担，可简单地控制从子到孙的复制禁止等、代复制。

在上述实施例中，由 LT 脚注 640 来检验正当性，但各 LT 活动标记块 620#1-620#n 中也可包含用于检验正当性的篡改检测用信息。

在上述实施例中，虽然将配送的使用前的许可信息（LT）存储在用户终端 200a 的 LT 存储部 245 中，但也可将 LT 暂时存储于外部媒体 500b 或外部媒体 500c 中。

在用户终端 200a 将内容移动到外部媒体 500b、500c 的情况下，虽然用户终端 200a 判断是否可移动，但服务器 100 在移动前事先判定外部媒体 500 是否可处理许可信息，仅在可处理时，才向用户终端发送许可内容移动的许可信息。此时，配送服务器与用户终端进行通信，取得移动前的外部媒体的信息，确定是否可行移动内容。

对于外部媒体 500a、500c 可如何处理许可信息或可处理的内容控制信息如何，可在用户终端 200a 的外部媒体访问部 280 认证外部媒体 500a、500c

后，由用户终端 200a 进行判断。

另外，在上述实施例中，虽然服务器 100 除权利管理外，还管理内容配送、收费等，但也可分别形成内容配送和收费等功能。

图 1

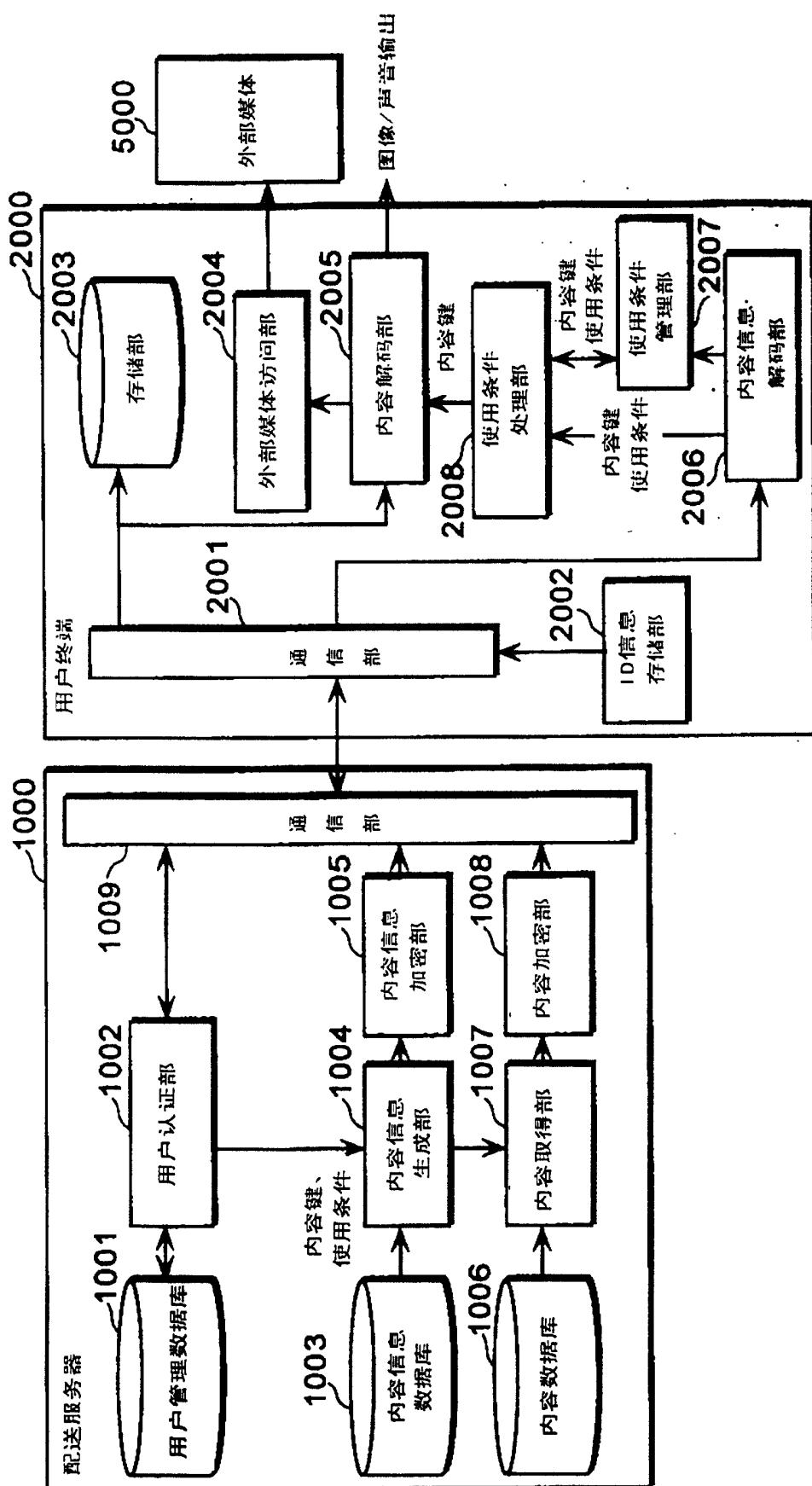


图2

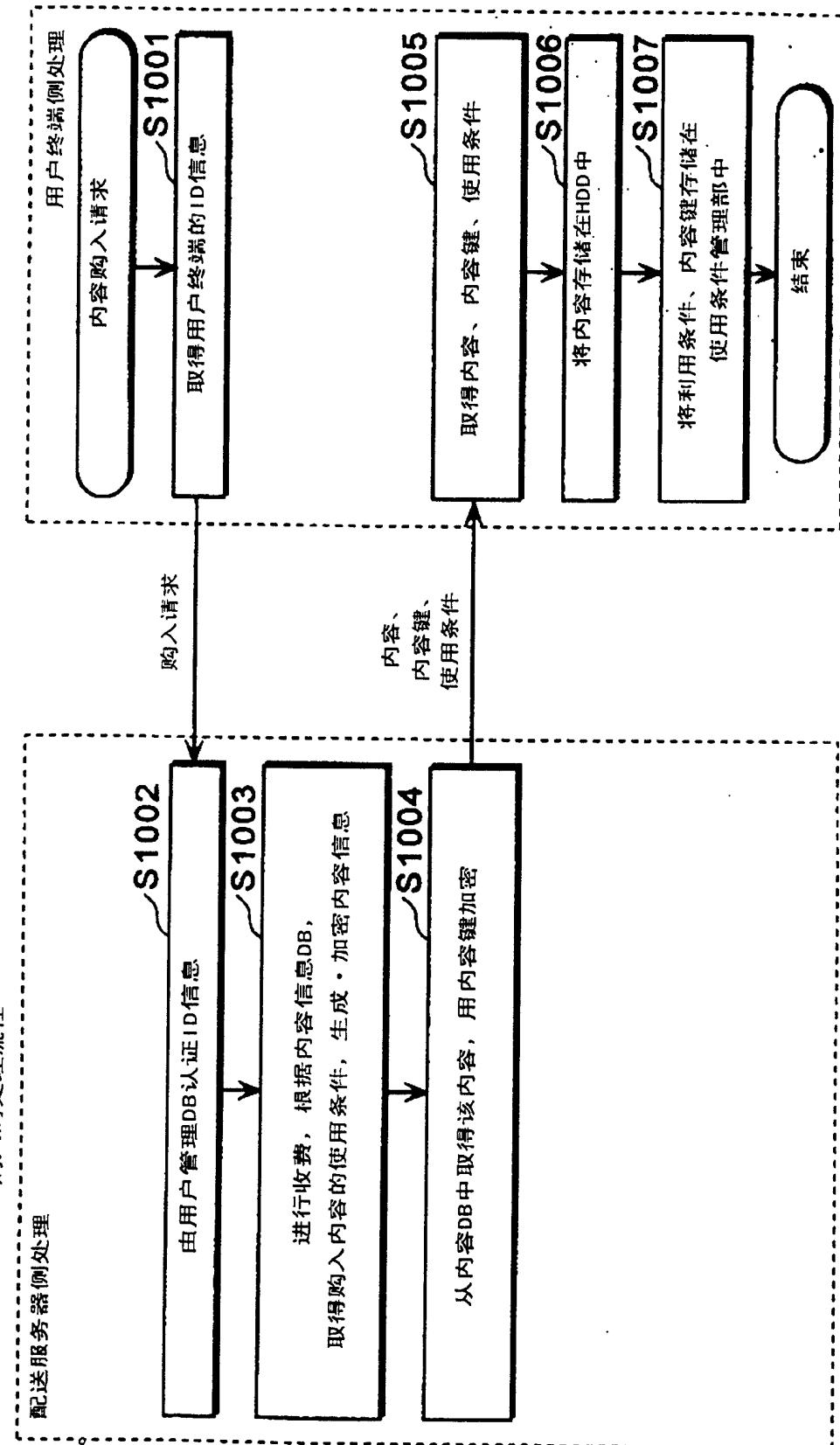


图3

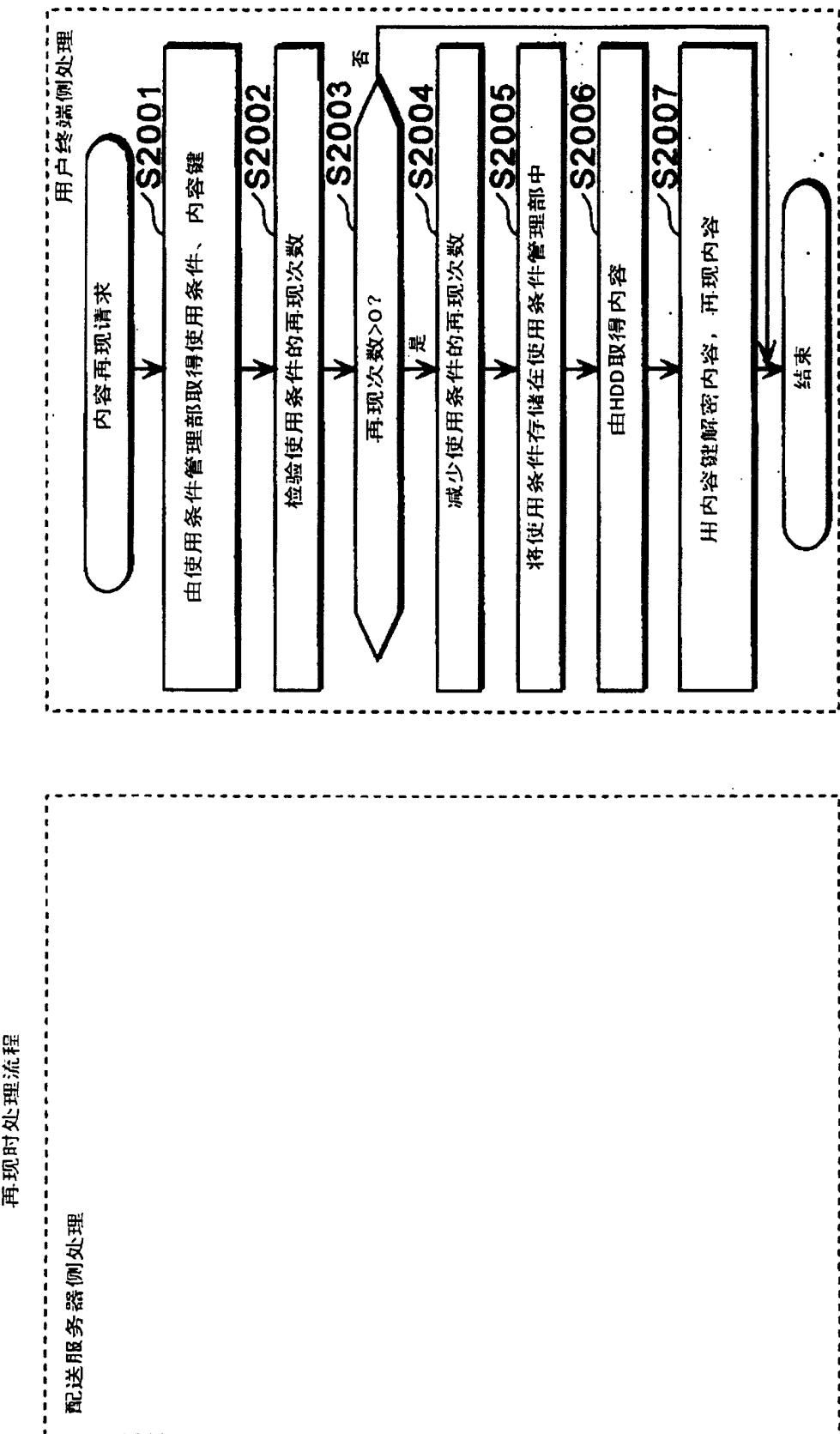


图4

1

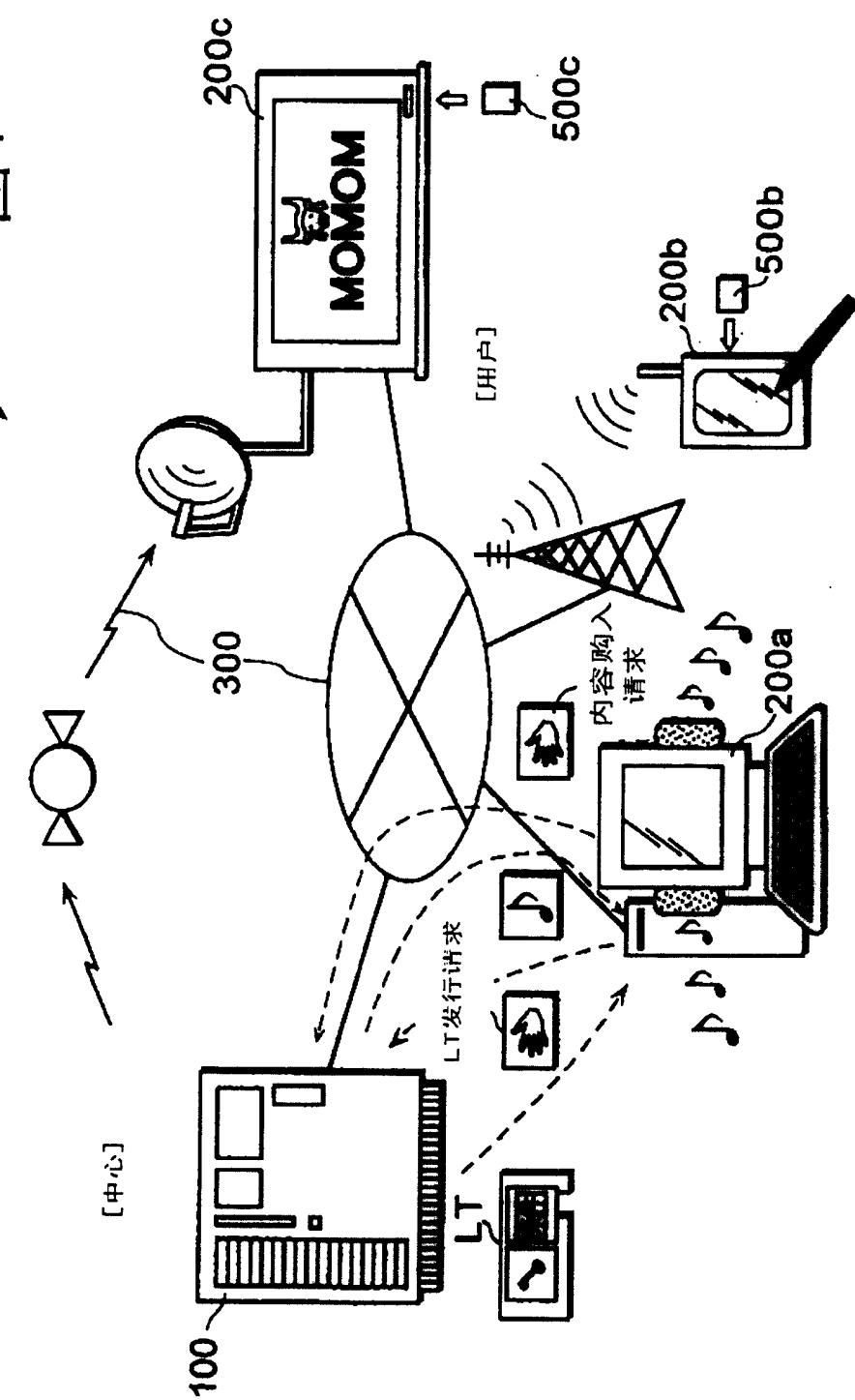


图5

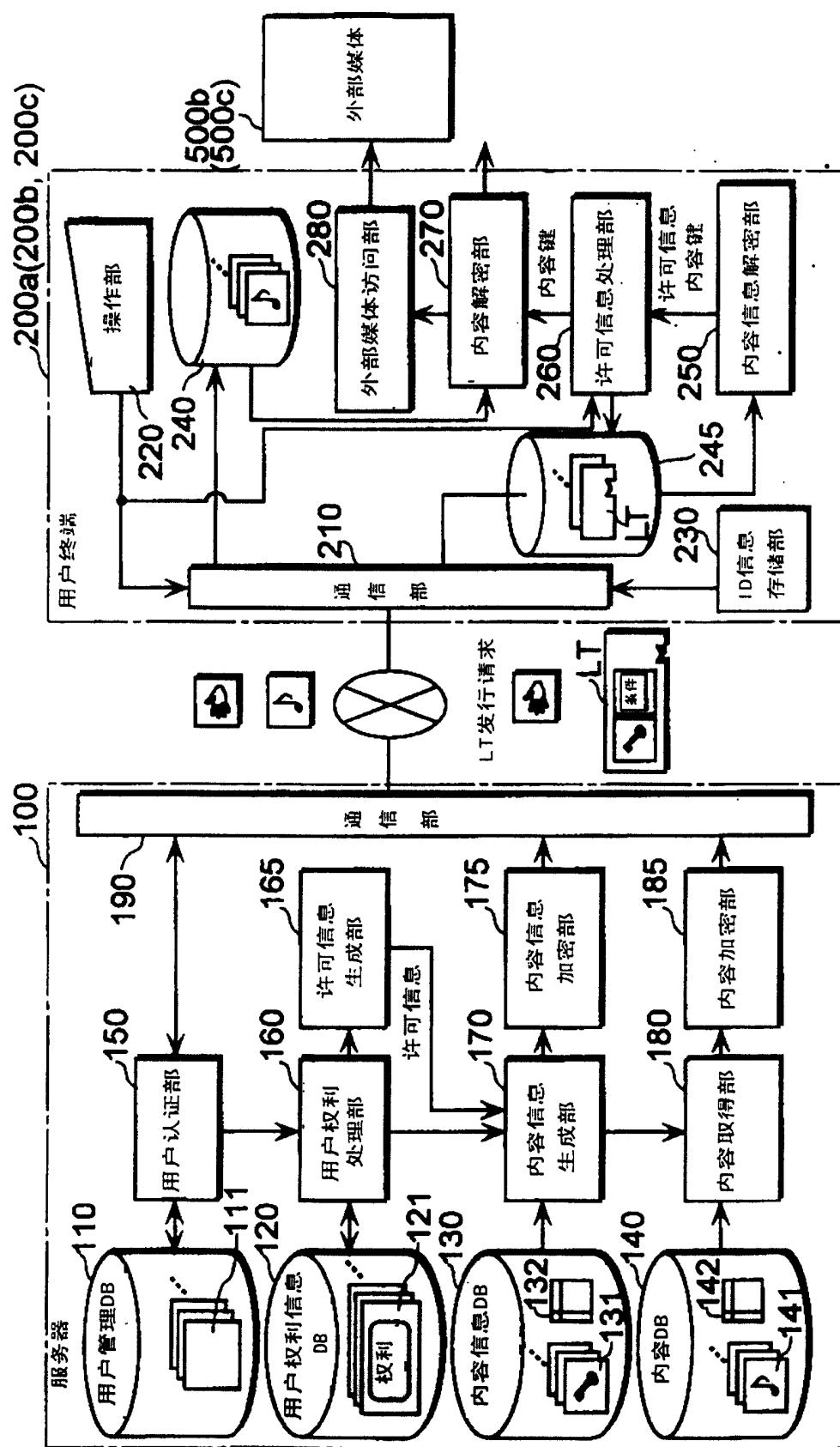


图6

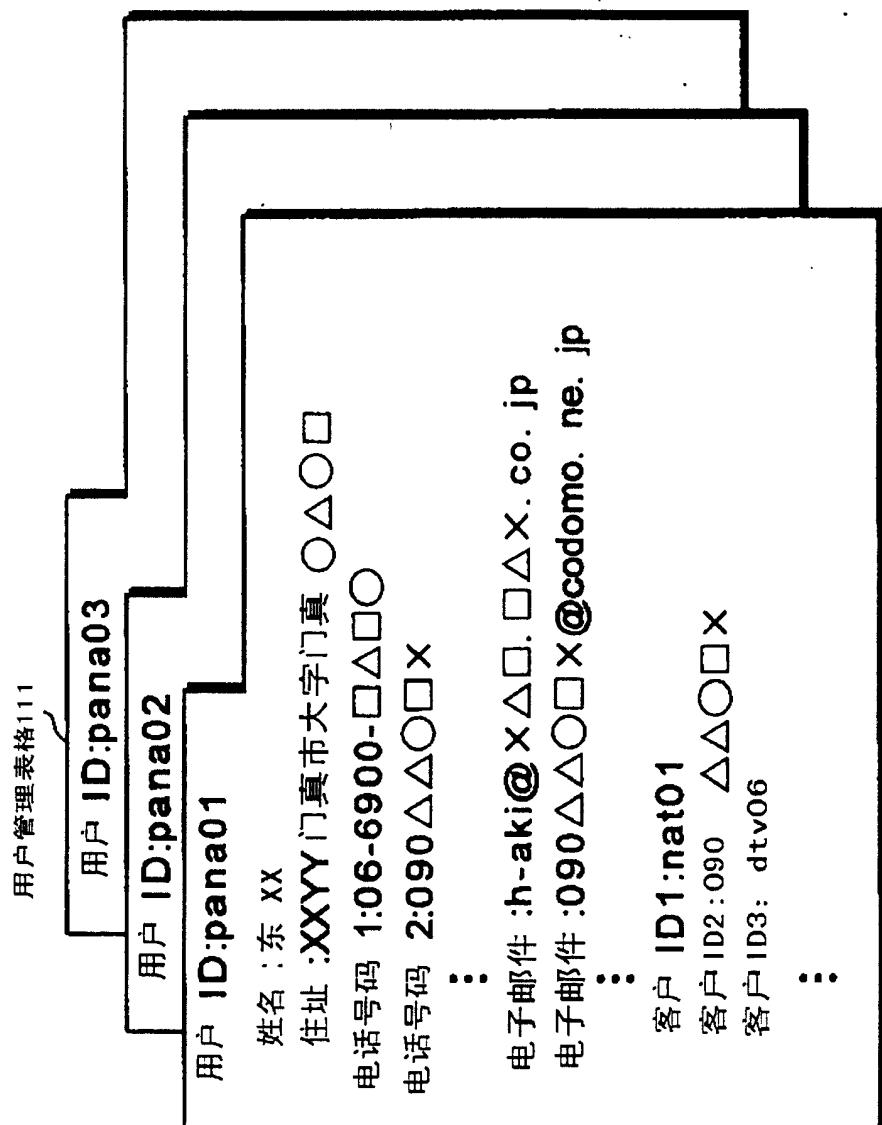


图 7

用户权利信息管理表格121

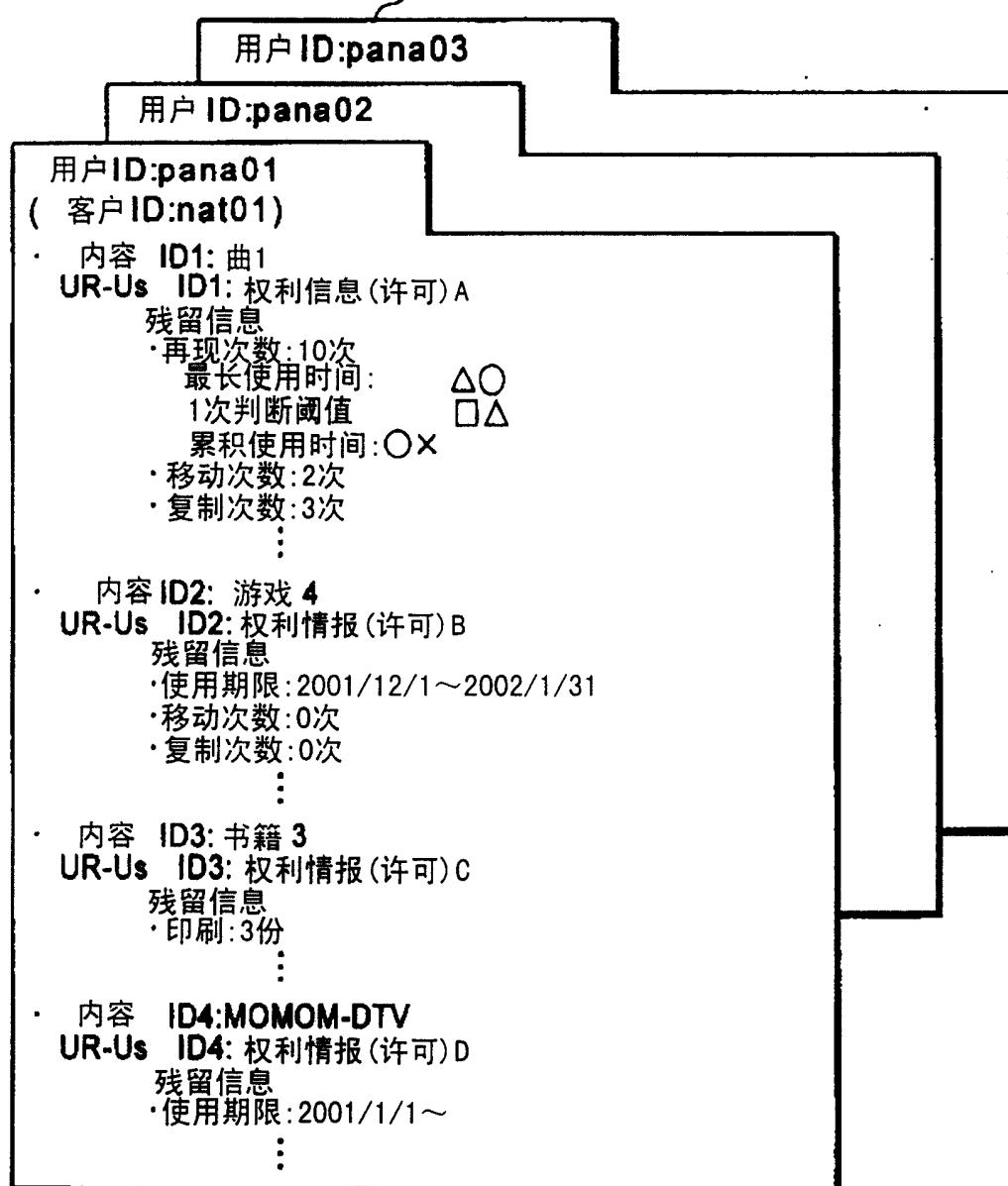


图8

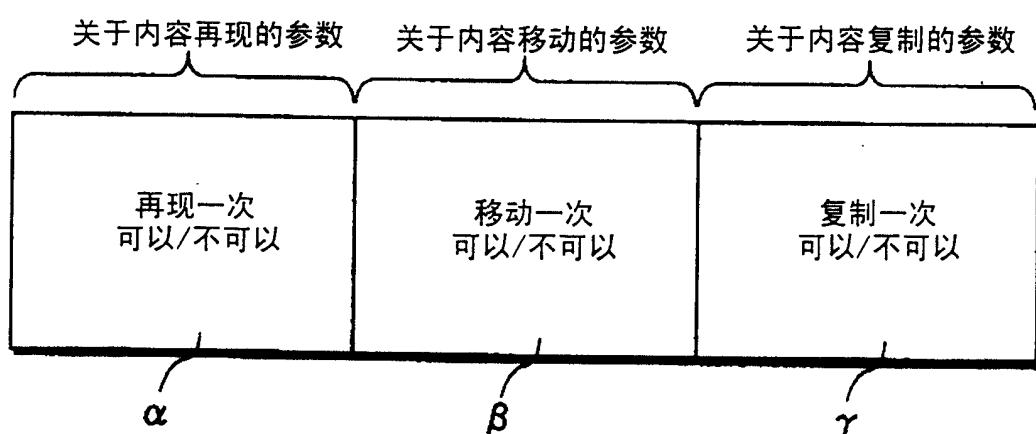


图9

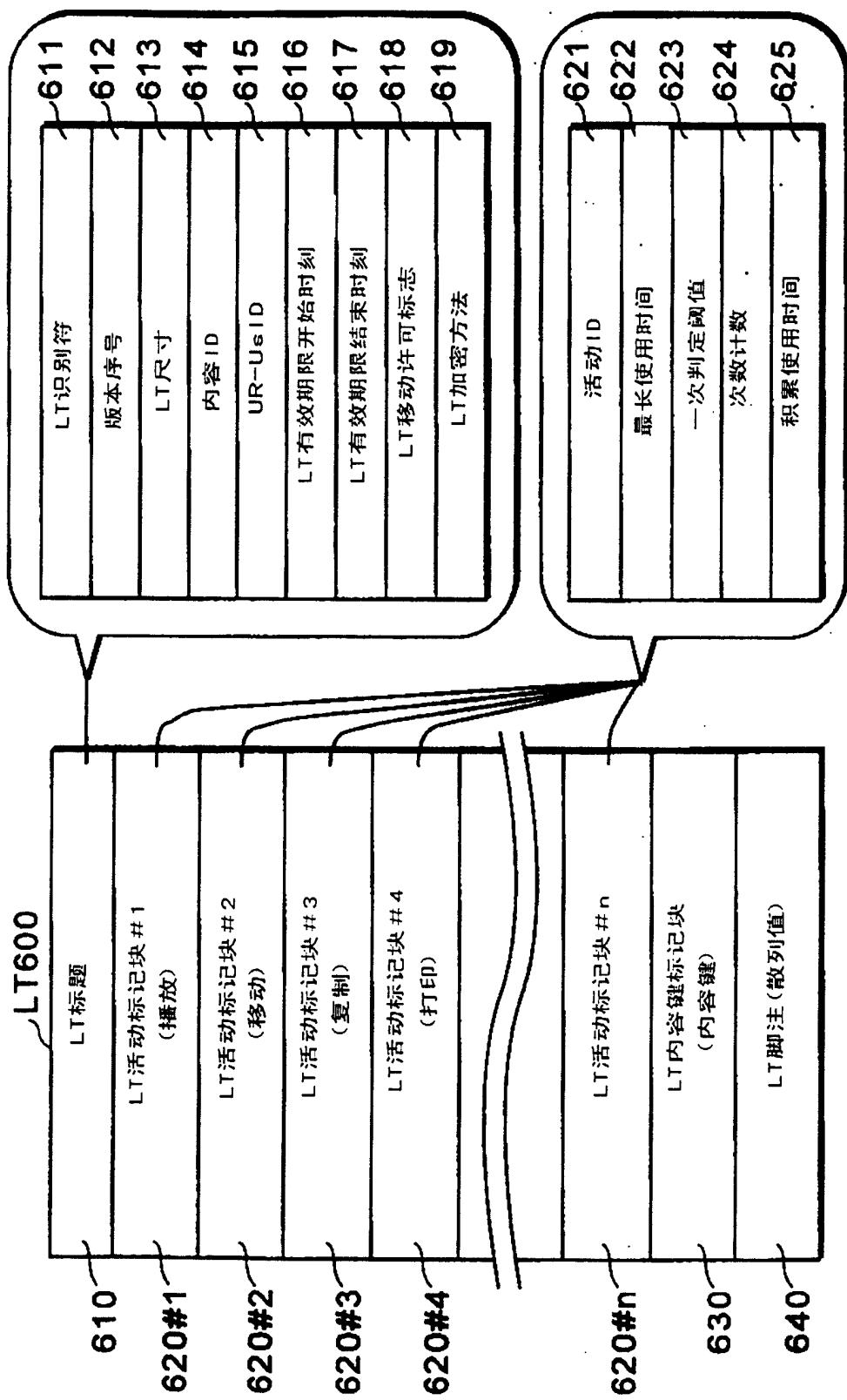


图 10

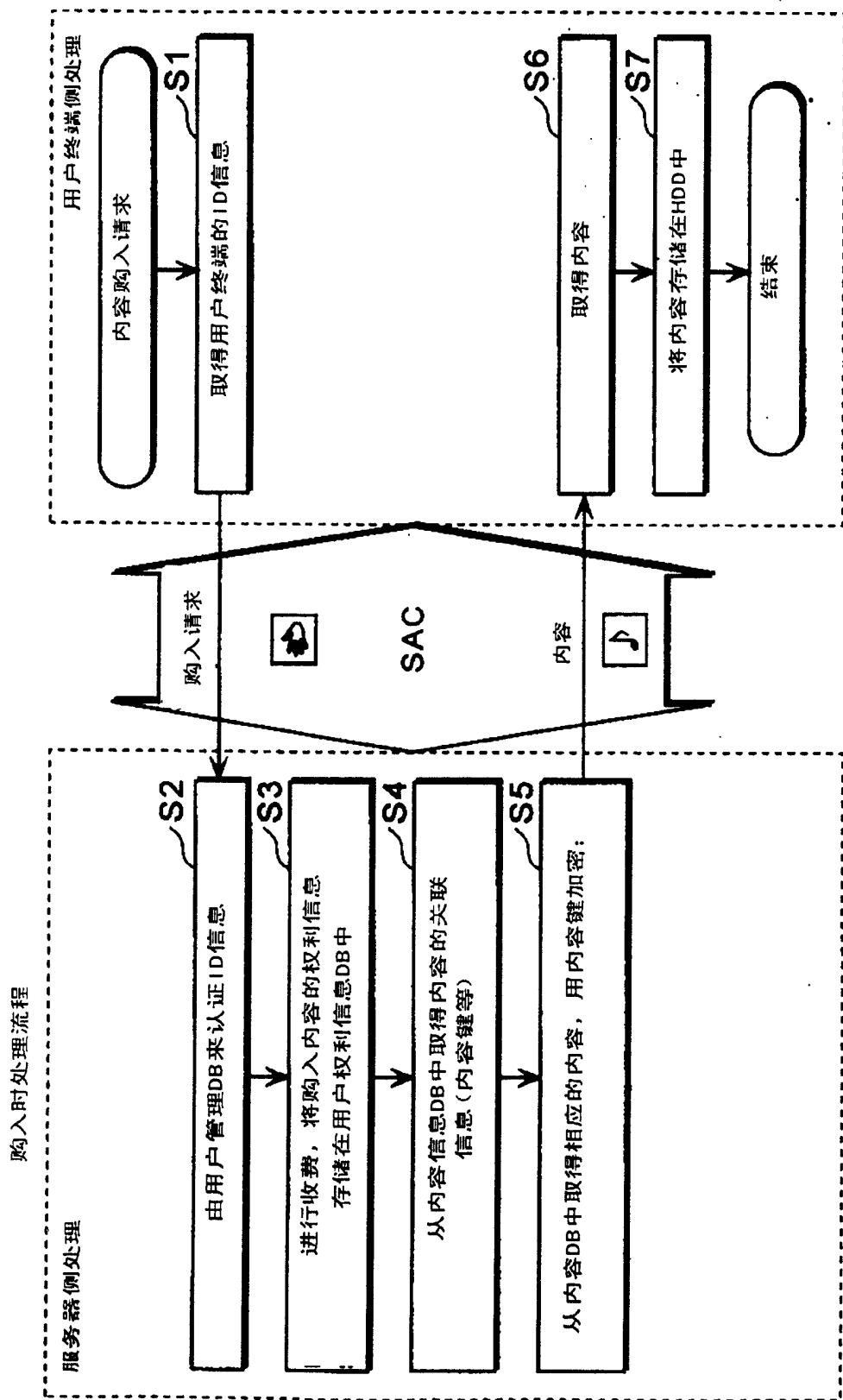


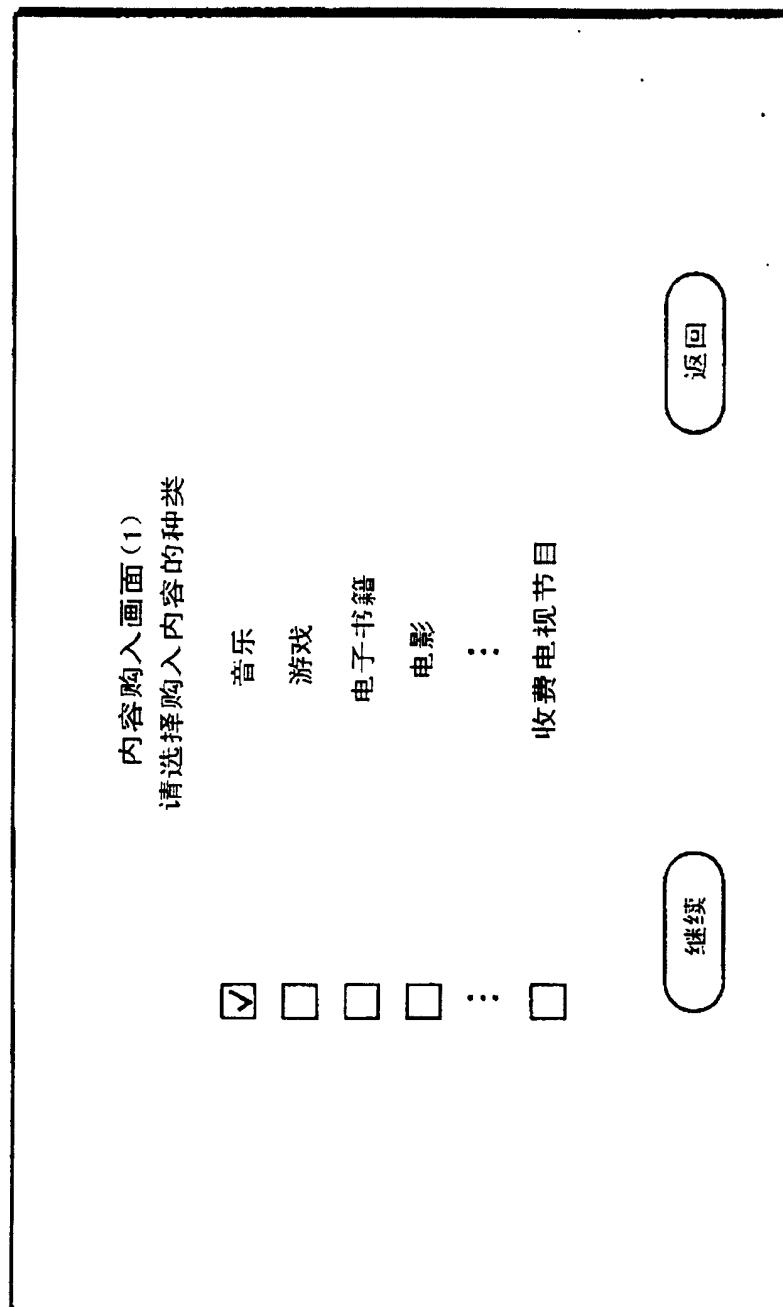
图 11

图12

| 内容购入画面(2) | | | |
|--|---------|------------------------------|-----------------------------------|
| 内容ID | 主题 | 权利信息 | 出售价格 |
| <input checked="" type="checkbox"/> 曲1 | 冲浪乔治 | 使用条件 再现次数 移动次数 复制次数 | 500 日元 10 次 2 次 3 次 |
| <input type="checkbox"/> 曲2 | 凤蝶 | 使用条件 使用期限 移动次数 复制次数 | 100 日元 12/1~12/31 禁止 禁止 |
| <input type="checkbox"/> 曲3 | 啊！秋天的盛会 | 使用条件 再生次数 移动次数 复制次数 | 1500 日元 无限制 无限制 无限制 |
| | | | <input type="button" value="购入"/> |
| | | | <input type="button" value="返回"/> |

图 13

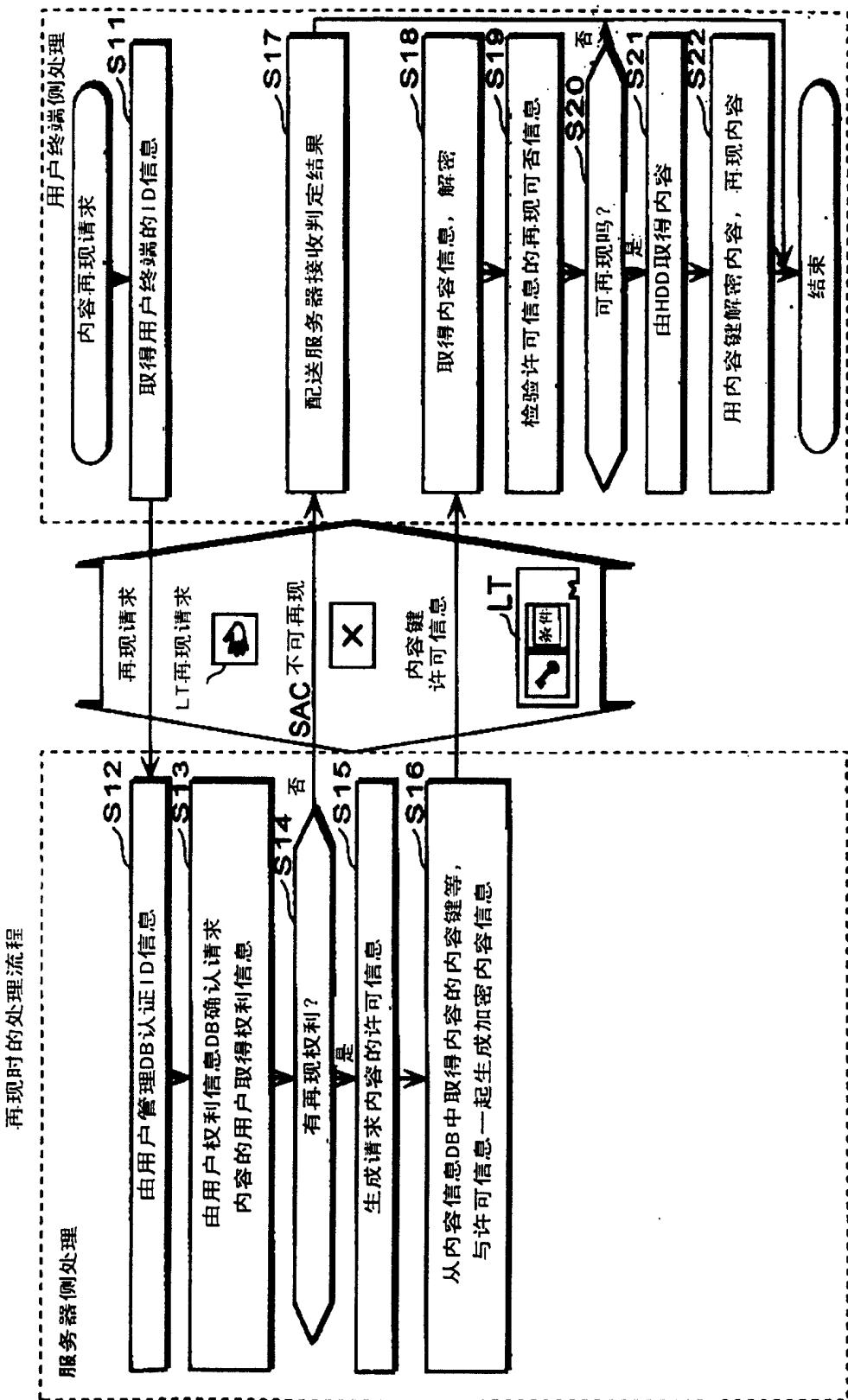


图 14

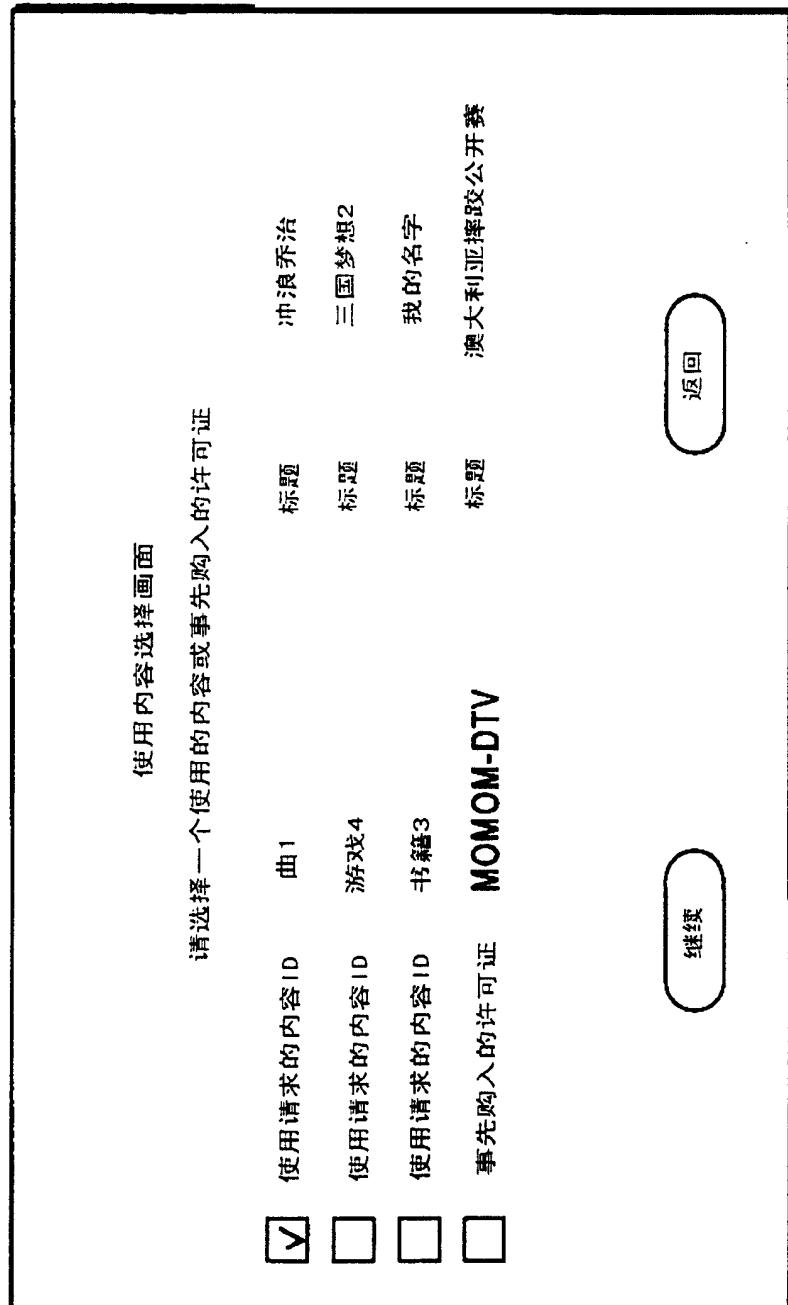


图15

请求使用的内容

标题

曲1
冲浪乔治

请求内容

再现
 移动
 复制

次数

2 次
1 次
 次

返回

确定

图 16

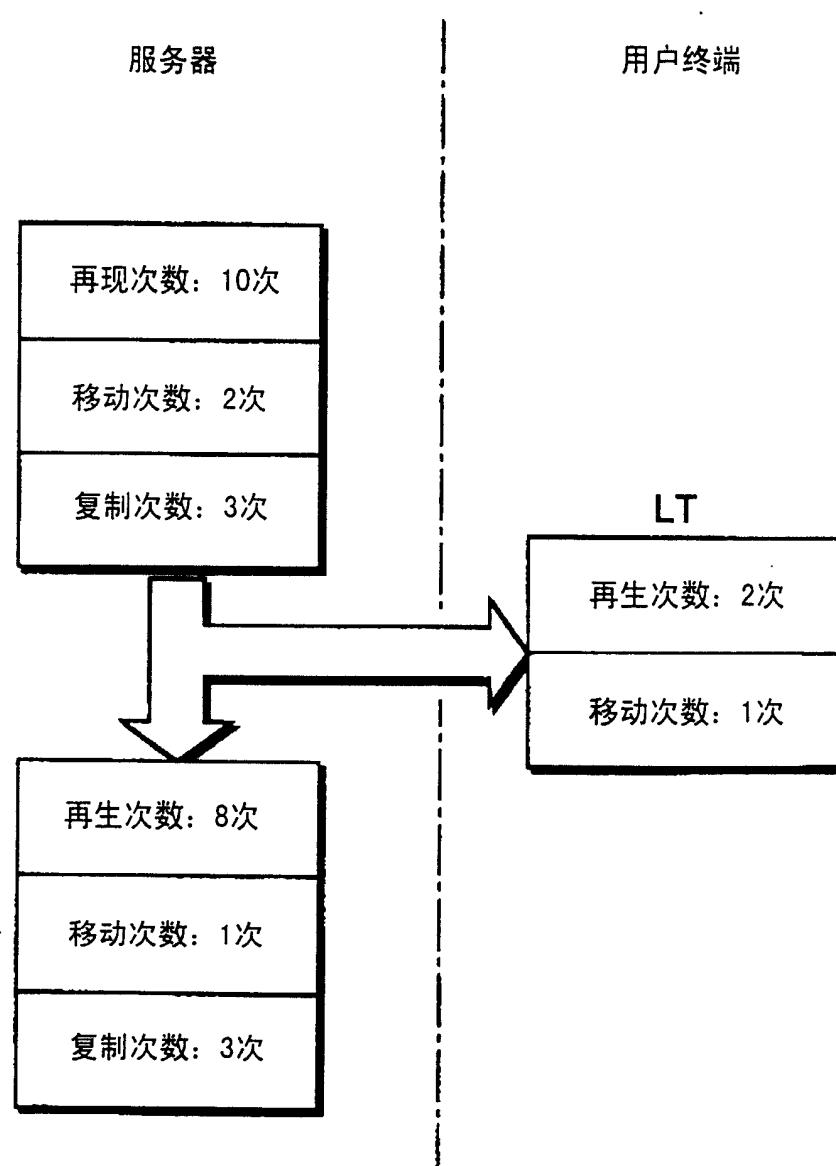


图17

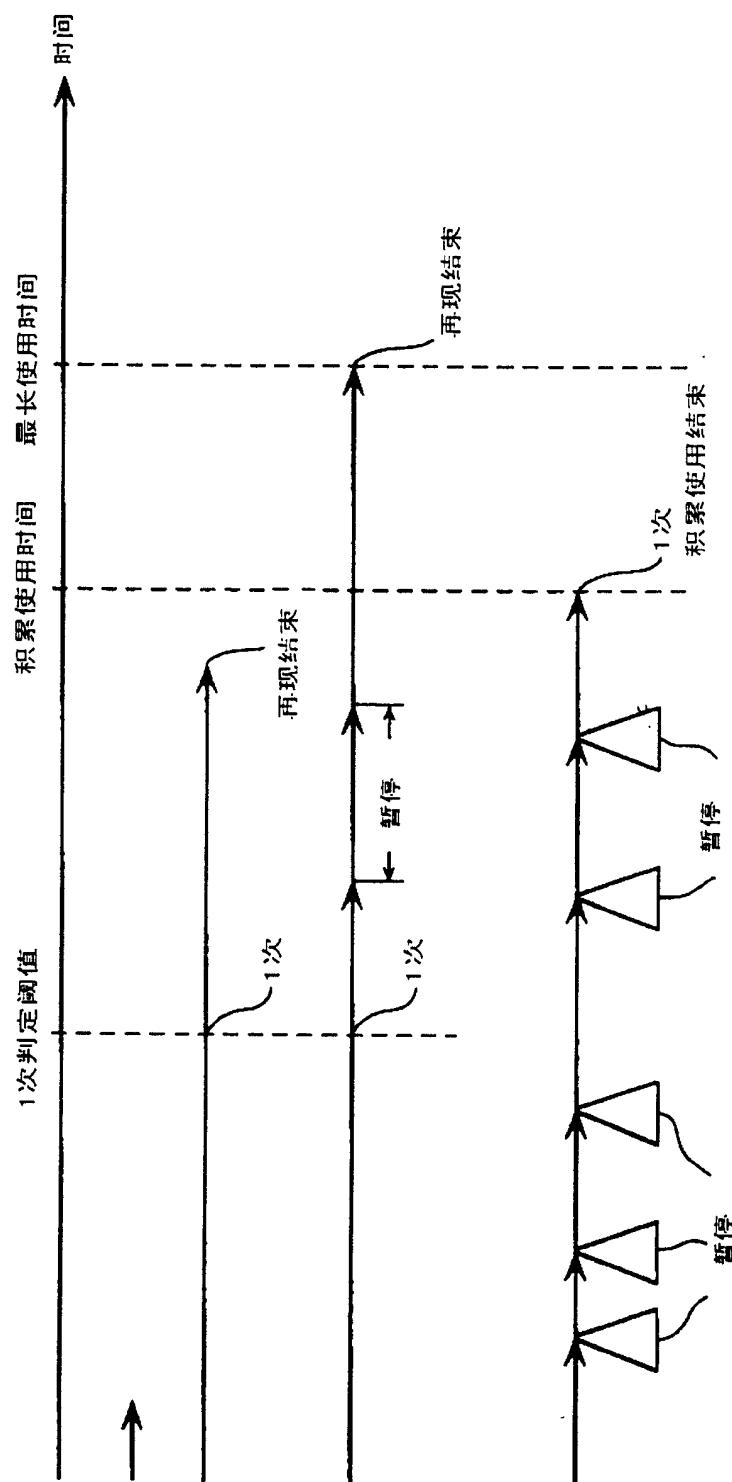


图 18

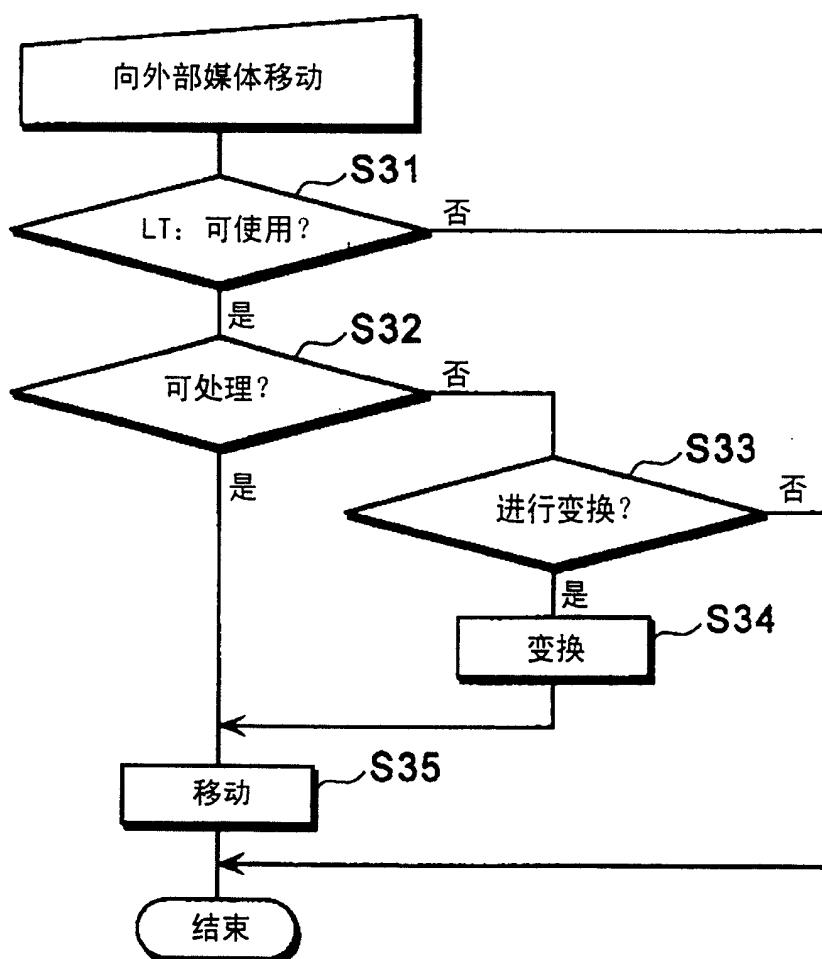


图 19

