[19]中华人民共和国国家知识产权局

[51]Int. Cl[7]
G06F 12/00
G06F 12/14 G06F 13/00

[12]发明专利申请公开说明书

[21]申请号 00802346.8

[43]公开日 2001年12月19日

[11]公开号 CN 1327557A

[22]申请日 2000.10.25 [21]申请号 00802346.8
[30]优先权
[32]1999.10.25 [33]JP [31]303138/1999
[86]国际申请 PCT/JP00/07475 2000.10.25
[87]国际公布 WO01/31452 日 2001.5.3
[85]进入国家阶段日期 2001.6.21
[71]申请人 索尼公司
地址 日本东京都
[72]发明人 石黑隆二 河上达 田边充 江面裕一
佐藤一郎 海老原宗毅

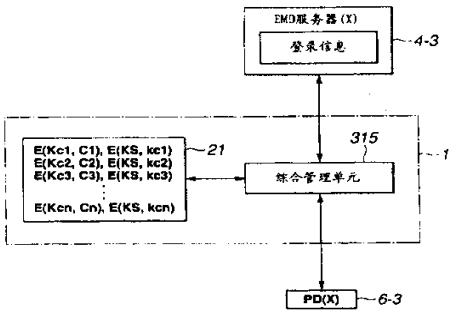
[74]专利代理机构 柳沈知识产权律师事务所
代理人 马 莹

权利要求书9页 说明书38页 附图页数26页

[54]发明名称 内容供给系统

[57]摘要

即使通过网络发送的内容数据已经被损坏，内容数据可以被恢复而对版 权的保护保持不变。PC 在硬盘上存储所发送的音乐内容的备份，并将存储在 硬盘中的音乐内容的使用登录信息提供给 EMD 服务器。如果例如在硬盘中的 音乐内容已经被损坏时，PC 从 EMD 服务器读取使用登录信息并根据使用登录 信息再现在硬盘中存储的备份数据。



ISSN1008-4274

01.06.21

权　利　要　求　书

1、一种内容供给系统，包括:

内容服务器，用于在网络上发送内容数据；以及

数据处理器，具有用于再现和/或控制内容数据的再现控制程序，所述数据处理器将由内容服务器发送的内容数据存储在记录介质上以用于再现和/或控制，并且将所发送的内容数据的备份数据存储在记录介质上，所述数据处理器还将内容数据的使用登录（log）信息发送到所述内容服务器;

如果从所述记录介质中不再提供所述内容数据，所述数据处理器从所述内容服务器获得使用登录信息，所述数据处理器根据使用登录信息对存储于所述记录介质中的内容数据的备份数据执行再现和/或控制。

2、一种内容供给系统，包括:

内容服务器，用于在网络上发送内容数据；以及

数据处理器，具有用于再现和/或控制内容数据的再现控制程序，所述数据处理器将由内容服务器发送的内容数据存储在记录介质上以用于再现和/或控制，所述数据处理器还将所述内容数据的使用登录信息发送到所述内容服务器;

如果从所述记录介质中不再提供内容数据，所述数据处理器具有从所述内容服务器中重新发送的所述不再提供的内容数据，所述数据处理器还从所述内容服务器获得使用登录信息并根据所述使用登录信息对重新发送的内容数据执行再现和/或控制。

3、一种用于在具有再现和或控制内容数据的再现处理程序的数据处理器与用于通过网络将内容数据发送到所述数据处理器的内容服务器之间发送内容的方法，该方法包括步骤:

所述内容服务器将内容数据发送到所述数据处理器;

所述数据处理器将所述从内容服务器发送的内容数据存储在记录介质中以用于再现和/或控制，并且还将所发送的内容数据的备份数据存储在记录介质中;

数据处理器将所述内容数据的使用登录信息发送到所述内容服务器;

如果所述数据处理器不能从所述记录介质中获得所述内容数据，则所述内容服务器将使用所述登录信息发送到所述数据处理器；以及

所述数据处理器响应所述登录信息再现和/或控制存储在所述记录介质中的内容数据的备份数据。

4、一种用于通过网络在具有再现和/或控制内容数据的再现控制程序的数据处理器与将内容数据发送到数据处理器的内容服务器之间发送内容的方法，该方法包括步骤：

所述内容服务器将内容数据发送到所述数据处理器；

所述数据处理器将从所述内容服务器发送的内容数据存储在记录介质中以用于再现和/或控制；

所述数据处理器将所述内容数据的使用登录信息发送到所述内容服务器；

如果所述数据处理器不能从所述记录介质中获得所述内容数据，则所述内容服务器重新发送已变得不能提供给所述数据处理器的内容数据到所述数据处理器，并发送所述使用登录信息发送到所述数据处理器；

所述数据处理器根据使用所述登录信息再现和/或控制该重新发送的内容数据。

5、一种适于在数据处理器中安装的、在其中存储有用于获得通过网络从再现和/或控制内容数据的内容服务器发送的内容数据的再现控制程序的记录介质，所述再现控制程序包括：

将从所述内容服务器发送的内容数据存储在记录介质中以用于再现和/或控制，并存储所发送的内容数据的备份数据，以及将所述内容数据的使用登录信息发送所述内容服务器；以及

如果不再从所述记录介质提供内容数据，从所述内容服务器获得所述使用登录信息，并与使用登录信息一致来再现和/或控制存储在所述记录介质中的内容数据的备份数据。

6、一种适于在数据处理器中安装的并且在其中存储有用于获得通过网络从再现和/或控制内容数据的内容服务器发送的内容数据的再现控制程序的记录介质，所述再现控制程序包括：

将从所述内容服务器发送的内容数据存储在记录介质中以用于再现和/或控制；并将所述内容数据的使用登录信息发送到所述内容服务器；以及

如果不再从所述记录介质提供内容数据，则使内容数据从内容服务器重新发送，从所述内容服务器获得使用登录信息并与使用登录信息一致来再现

和/或控制重新发送的内容数据。

说　明　书

内容供给系统

技术领域

本发明涉及通过网络提供诸如音乐数据的内容数据的内容供给系统、内容发送系统以及一种记录介质。

背景技术

近来，使用诸如因特网或有线电视提供音乐内容的在线发送已经进入了实际应用。

如果，在用于音乐内容的发送系统中，内容发送者通过网络例如在网站发送音乐信息。利用该音乐发送系统的用户使用他或她自己的个人计算机来访问由内容发送者提供的网站以便下载所需的音乐内容。

同时，在这个音乐发送系统中，所下载的音乐内容是通过例如网络可进行支付的。

但是，如果一旦用户拥有的个人计算机中的数据被破坏，则曾经购买的音乐内容就丢失了。所以为了恢复该音乐内容，则就需要再购买该内容。

发明概述

因此，本发明的一个目的在于提供一种内容供给系统，在该系统中，即使通过网络发送的内容被破坏了，在该版权保护得到保证的同时，该内容数据能够得到恢复。

本发明的另一个目的在于提供一种内容发送系统，在该系统中，即使通过网络发送的内容被破坏了，在该版权保护得到保证的同时，该内容数据能够得到恢复。

本发明的再一个目的在于提供一种记录介质，在其上存储有重放控制程序，该重放程序能够在即使通过网络发送的内容被破坏了的情况下，在该版权保护得到保证的同时，恢复内容数据。

在一方面中，本发明提供一种内容供给系统，包括：内容服务器，用于在网络上发送内容数据；以及数据处理器，具有用于再现和/或控制内容数据的再现控制程序；其中数据处理器将由内容服务器发送的内容数据存储在记录介质以用于再现和/或控制，并且将所发送的内容数据的备份数据存储在记

录介质上，该数据处理器还将内容数据的使用登录（log）信息发送到内容服务器。如果从记录介质中不再提供内容数据，在根据使用登录信息对存储于记录介质中的内容数据的备份数据执行再现和/或控制的同时，该数据处理器从内容服务器获得使用登录信息。

在该内容供给系统中，数据处理器基于从内容服务器重新获得的使用登录信息再现和/或控制备份恢复数据。

在另一方面中，本发明提供一种内容供给系统，包括内容服务器，用于在网络上发送内容数据；以及数据处理器，具有用于再现和/或控制内容数据的再现控制程序；其中数据处理器将由内容服务器发送的内容数据存储在记录介质以用于再现和/或控制，并且内容数据的使用登录信息被发送到内容服务器。如果从记录介质中不再提供内容数据，则该数据处理器具有从内容服务器重新发送的内容数据。在对根据使用登录信息重新发送的内容数据执行再现和/或控制的同时，该数据处理器还从内容服务器获得使用登录信息。

在该内容供给系统中，数据处理器再现和/或控制基于从内容服务器重新获得的使用登录信息的重新发送的内容数据。

在再一方面中，本发明提供一种用于在具有再现和或控制内容数据的再现处理程序的数据处理器与用于通过网络将内容数据发送到数据处理器的内容服务器之间发送内容的方法，其中该方法包括步骤：内容服务器将内容数据发送到数据处理器；数据处理器将从内容服务器发送的内容数据存储在记录介质中以用于再现和或控制，并且还将所发送的内容数据的备份数据存储在记录介质中；数据处理器将内容数据的使用登录信息发送到内容服务器；如果数据处理器不能从记录介质中获得内容数据，则内容服务器将使用登录信息发送到数据处理器；以及数据处理器响应使用登录信息再现和/或控制存储在记录介质中的内容数据的备份数据。

在该内容发送方法中，数据处理器基于从内容服务器重新获得的使用登录信息再现和/或控制备份恢复数据。

在再一方面中，本发明提供一种用于在具有再现和/或控制内容数据的再现控制程序的数据处理器与用于通过网络将内容数据发送到数据处理器的内容服务器之间发送内容的方法，其中该方法包括步骤：内容服务器将内容数据发送到数据处理器；数据处理器将从内容服务器发送的内容数据存储在用于再现和/或控制的记录介质中；数据处理器将内容数据的使用登录信息发送

到内容服务器；如果数据处理器不能从记录介质中获得内容数据，则内容服务器重新发送已变得不能提供给数据处理器的内容数据，并将使用登录信息发送到数据处理器；以及数据处理器根据使用登录信息再现和/或控制该重新发送的内容数据。

在该内容发送方法中，数据处理器再现和/或控制基于从内容服务器重新获得的使用登录信息的重新发送的内容数据。

在再一方面中，本发明提供一种适于在数据处理器中安装的、在其中存储有用于获得通过网络从内容服务器发送的内容数据以用于再现和/或控制内容数据的再现控制程序的记录介质，其中再现控制程序包括：将从内容服务器发送的内容数据存储在记录介质中以用于再现和/或控制，并存储所发送的内容数据的备份数据；以及将内容数据的使用登录信息发送内容服务器，并且如果不再从记录介质提供内容数据，从内容服务器获得使用登录信息；以及与使用登录信息一致来再现和/或控制存储在记录介质中的内容数据的备份数据。

在该记录介质中，再现控制程序根据从内容服务器重新获得的使用登录信息来再现和/或控制数据处理器的恢复备份数据。使再现控制程序安装于记录介质上。

在再一方面中，本发明提供适于在数据处理器中安装的并且在其中存储有用于获得通过网络从内容服务器发送的内容数据以用于再现和/或控制内容数据的再现控制程序的记录介质，其中再现控制程序包括：将从内容服务器发送的内容数据存储在记录介质中以用于再现和/或控制；将内容数据的使用登录信息发送到内容服务器；如果不再从记录介质提供内容数据，则使内容数据从内容服务器重新发送；以及从内容服务器获得使用登录信息并与使用登录信息一致来再现和/或控制重新发送的内容数据。

在该记录介质中，根据从内容服务器重新获得的使用登录信息，再现控制程序再现和/或控制数据处理器这样发送的内容数据，使再现控制程序安装于记录介质上。

附图的简要说明

图 1 表示体现本发明的音乐内容发送系统的系统结构；

图 2 说明在内容数据管理系统中使用的个人计算机的配置；

图 3 说明包含在内容数据管理系统中的便携式设备的配置；

图 4 说明个人计算机的功能;

图 5 表示显示/操作指令窗口的示例;

图 6 表示记录程序使显示单元显示的窗口的示例;

图 7 说明在音乐内容发送系统中发送方的具有不同格式的内容的统一操作;

图 8 表示统一传输协议层和应用层之间的关系;

图 9A、9B 表示一般使用的使用条件信息的格式;

图 10 表示在综合管理单元中使用的构成统一使用条件信息的文件;

图 11 表示统一使用条件信息的自动机(automaton)文件的格式;

图 12 表示指示在自动机文件的自动机说明部分中说明的音乐内容的操作转换的自动机的示例;

图 13 表示元组串(tuple string)中的自动机。

图 14 表示自动机说明部分的结构。

图 15 表示根据 XML 的参数确定的 DTD 中定义的事件和命令。

图 16 表示自动机说明部分的第一说明示例;

图 17 表示第一说明示例的状态转换图;

图 18 表示自动机说明部分的第二说明示例;

图 19 表示第二说明示例的状态转换图;

图 20 表示自动机说明部分的第三说明示例;

图 21 表示第三说明示例的状态转换图;

图 22 表示自动机说明部分的第四说明示例;

图 23 表示统一使用条件信息的参数文件的结构;

图 24 表示在参数文件改变的情况下的结构;

图 25 表示参数文件的参数说明部分的结构;

图 26 表示由综合管理单元监督内容的方法;

图 27 表示在从 CD-ROM 安装了综合管理单元的情况下的处理顺序;

图 28 表示从网络正在下载安装综合管理单元的情况下的处理顺序;

图 29 表示从发送(rippling)密钥到 EMD 密钥的更新顺序;

图 30 表示 EMD 密钥更新顺序的第一示例;

图 31 表示 EMD 密钥更新顺序的第二示例。

实施本发明的的最佳模式

下文将参考附图对体现本发明、代表本发明的最佳模式的音乐内容发送系统进行描述。该音乐内容发送系统是这样一种系统，该系统通过网络从服务器将音乐内容下载到便携式设备中，并监督所下载的音乐内容和从 CD 读出的音乐内容。

(1) 音乐内容发送系统的总体结构

图 1 表示体现本发明的音乐内容发送系统 1 的结构。

体现本发明的音乐内容发送系统 1 包括：个人计算机 1、例如为局域网的网络 2、注册服务器 3、多个发送音乐内容(下文称为内容)的 EMD(电子音乐发送)服务器 4(4-1、4-2 和 4-3)、WWW 服务器 5(5-1 和 5-2)。个人计算机 1 已经通过 USB 电缆 7(7-1、7-2 和 7-3)在其中存储了一种例如为存储卡的存储介质，并连接到作为用于再现该内容的便携式音乐再现设备的便携式设备(6-1、6-2 和 6-3)。

个人计算机通过网络 2 连接到 EMD 注册服务器 3、EMD 服务器 4(4-1、4-2 和 4-3)和 WWW 服务器 5(5-1 和 5-2)。

个人计算机接收按照预设的压缩系统压缩的内容，并按照预设的加密系统加密压缩的内容以用于存储。作为压缩系统，可以使用 ATRAC(自适应变换声编码)3(商标)或 MP3(MPEG 音频层 3)。作为加密系统，可以使用例如描述(数据加密标准)。

在接收发送的内容时，个人计算机 1 也接收发送的指示内容的使用条件的使用条件信息以记录发送的数据。当记录例如从 CD 中读出的内容时，个人计算机 1 依据内容再现条件生成使用条件信息以记录生成的使用条件信息。

此外，在响应记录和存储更新使用条件信息的同时，个人计算机 1 通过 USB 电缆 7(7-1、7-2 和 7-3)将所记录和加密的内容连同诸如使用条件信息、音乐编号的标题以及表演者的姓名之类的相关信息记录和存储在便携式设备(6-1、6-2 和 6-3)中。该处理被称为校验输出。在该校验输出操作中，在使用条件信息中对由个人计算机 1 记录的内容可以进行的校验输出的次数按 1 递减。如果可以校验输出操作的次数为 0，则不能输出相应的内容。

而且，个人计算机 1 通过 USB 电缆 7(7-1、7-2 和 7-3)将存储在便携式设备(6-1、6-2 和 6-3)中的内容删除，并与该删除相关联，对使用条件信息进行更新。该删除操作被称为校验输入，在该校验输入操作中，由个人计算机 1 记录的可以校验输出操作的次数按 1 递增。注意也可以使该内容变为不

能使用，而不是被删除。

注意到个人计算机 1 不能将其它计算机已经校验输出到便携式设备 6 的内容校验输入。即，个人计算机 1 仅能够校验输入只由个人计算机 1 校验输出的内容。

当个人计算机 1 开始从 EMD 服务器 4 (4-1、4-2 和 4-3) 获取内容时，EMD 服务器 3 响应来自个人计算机 1 的请求，在将连接到 EMD 服务器 4 (4-1、4-2 和 4-3) 的程序发送到个人计算机的同时，通过网络 2 将个人计算机 1 和 EMD 服务器 4 (4-1、4-2 和 4-3) 之间相互鉴定所必须的鉴定密钥发送到个人计算机 1。

EMD 服务器 4 (4-1、4-2 和 4-3) 每一个都响应个人计算机的请求通过网络 2 将内容连同使用条件信息和诸如音乐编号的标题或表演者的姓名之类的与该内容有关的数据提供到个人计算机 1。

由各自的 EMD 服务器 4（4-1、4-2 和 4-3）发送的内容已经根据预设的加密系统被压缩，每个服务器的加密系统可以彼此不同。另一方面，由 EMD 服务器 4（4-1、4-2 和 4-3）提供的内容被以根据预设置的加密系统加密的形式发送，每个服务器的加密系统可以彼此不同。

WWW 服务器 5（5-1、5-2）每一个都响应个人计算机 1 的请求将对应于已经读取了诸如 CD 碟名或 CD 销售公司之类的内容的 CD 的数据提供给个人计算机 1，并将对应于从该 CD 读取的诸如音乐编号的名称或作曲者的姓名之类内容的数据提供给个人计算机。

便携式设备 6（6-1、6-2 和 6-3）再现从个人计算机 1 提供的内容，即诸如校验输出的内容，以将再现的内容输出给例如耳机（未示出）。

每一便携式设备 6（6-1、6-2 和 6-3）具有存储内容的记录介质。作为记录介质，可以使用装载在装置的内部衬底上的不可移动的 IC 存储器或可移动存储卡。便携式设备 6（6-1、6-2 和 6-3）通过用于发送内容的诸如 USB 之类的物理接口 7（7-1、7-2 和 7-3）连接到个人计算机 1。也附加有使用条件信息的内容以加密和压缩的形式被传输。

便携式设备 6（6-1、6-2 和 6-3）通常使用在这种状态下，即单个设备 6 与个人计算机 1 是不相连的。如果在这种状态中用户发出重放命令，则加密的内容被从记录介质中读取并再现。而且，便携式设备 6（6-1、6-2 和 6-3）根据附加在各自内容上的使用条件信息对控制进行管理以限制重放、或者在

需要时删除该内容或更新该使用条件。

下面，如果不必要区分每一个便携式设备 6（6-1、6-2 和 6-3），则将他们简单地称为便携式设备 6。

图 2 是个人计算机 1 的配置的示例说明。

正如所示的，个人计算机 1 包括 CPU（中央处理单元）11。CPU 11 实际上执行各种应用（将在以后描述）和 OS（操作系统）。在个人计算机 1 中还提供 ROM（只读存储器）12，ROM 12 通常存储基本上固定的程序数据和在 CPU 11 中使用的计算参数。并且，在个人计算机 1 中也包括 RAM（随机存储器）13，用以存储用于由 CPU 11 执行该应用和 OS 的程序以及在应用和 OS 执行中适当可变的参数。CPU 11、ROM 12 和 RAM 13 通过由 CPU 总线等组成的主总线（host bus）14 彼此相互连接。

主总线 14 通过桥 15 连接到诸如 PCI（外围部件互连/接口）的外部总线 16。

键盘 18 由用户操作输入各种命令给 CPU 11。用户使用鼠标 19 指向和选择显示器单元 20 的屏幕上的点。显示器单元 20 是液晶显示器或者 CRT（阴极射线管）用以显示文本和/或图像形式的各种信息。而且 HDD（硬盘驱动器）21 驱动硬盘以便在硬盘中写入或从硬盘中读出将由 CPU 11 执行的程序和信息。

驱动器 22 读取记录在连接到磁盘 41、光盘 42（包括 CD）、磁光盘 43 和半导体存储器 44 中的任何一个中的数据或程序，并通过接口 17、外部总线 16、桥 15 和主总线 14 将读取的数据或程序提供到所连接的 RAM 13。

USB 口 23（23-1、23-2、23-3）通过 USB 电缆 7（7-1、7-2、7-3）连接便携设备 6（6-1、6-2、6-3），并将由 HDD21、CPU 11 或 RAM 13 提供的数据通过接口 17、外部总线 16、桥 15 或主总线 14 输出到便携式设备 6（6-1、6-2、6-3）。

具有 IEC（国际电工技术委员会）60958 终端 24 的音频输入/输出接口 24 与数字音频输入/输出或模拟音频输入/输出相接。扬声器 45 根据来自音频输入/输出接口 24 的音频信号提供对应于每一内容的预定的声音。

包括键盘 18、鼠标 19、显示器 20、HDD21、驱动器 22、USB 口 23 和音频输入/输出接口 24 的附件连接到接口 17，反过来接口 17 通过外部总线 16、桥 15 和主总线 14 依次连接到 CPU 11。

连接到网络 2 的通信块 25 在通过网络 2 将存储在接收包中的数据(例如，鉴定密钥或内容）输出到 CPU 11、RAM 13 或 HDD 21 的同时，通过网络 2 将来自 CPU 11 或 HDD 21 的作为在包中以预定的方式存储的数据（例如，注册请求或发送内容请求）发送。

作为半导体 IC 集成形成的、并连接到个人计算机 1 的适配器 26 的 CPU 32 通过外部总线 16、桥 15 和主总线 14 连接到 CPU 11，并且和 CPU 11 一起执行各种处理。RAM 33 存储 CPU 32 执行各种处理所需的数据和程序。非易失存储器 34 存储在个人计算机 1 关机以后仍将保持的数据。ROM 36 存储个人计算机 1 传输的加密程序的解密程序。RTC（实时时钟）35 保持时间以提供时间信息。半导体 IC 被设计具有安全的环境并具有容许来自外部的错误访问。该功能可以以软件程序来建立。

通信块 25 和适配器 26 通过外部总线 16、桥 15 和主总线 14 连接到 CPU 11。

现在参考图 3，便携式设备 6 以方框图的形式示例性地说明。

电源电路 52 将干电池 51 提供的电压转换成预定电压的内部电源。将电源提供给从 CPU 53 至显示器单元 67 的元件，电源电路 52 将如此驱动整个便携式设备 6。

当通过 USB 连接器 56 和 USB 电缆 7 连接到个人计算机 1 时，USB 控制器 57 通过内部总线 58 将包括从个人计算机 1 发送的内容的数据提供给 CPU 53。

将从个人计算机 1 发送的数据由每包 64 字节的数据组成，并且以 12 兆比特/秒的传输率从个人计算机 1 发送。

将发送到便携式设备 6 的数据由标题和内容组成。标题存储内容 ID、文件名称、标题大小、内容密钥、文件大小、编解码器(codec) ID、文件信息等，并且还存储重放限制所需要的使用条件信息等。该内容由诸如 ATRAC3 的编码方法编码并被加密。

标题大小指示着标题的数据长度（例如，33 字节），并且文件大小指示着内容的数据长度（例如 33，636，138 字节）。

内容密钥是用于对加密的内容解密的密钥，并根据通过在个人计算机 1 和便携式设备 6 之间的相互鉴定产生的对话密钥(临时)以加密的格式从个人计算机 1 发送到便携式设备 6。

当便携式设备 6 通过 USB 电缆 7 连接到个人计算机 1 的 USB 接口 23 时，将进行在个人计算机 1 和便携式设备 6 之间的相互鉴定。该相互鉴定是例如

质询-响应（challenge-response）类型。注意：当进行质询-响应类型的鉴定时，在便携式设备 6 中也提供 DSP（数字信号处理器）59 以解密加密的内容。

上述的质询-响应类型相互鉴定是这样，即响应由个人计算机产生的某个值（质询），例如通过使用便携式设备 6 和个人计算机 1 所共同专有的密钥，由便携式设备 6 产生一个值(响应)。在质询-响应类型相互鉴定中，由个人计算机 1 产生的值每一次鉴定都变化。所以，即使当例如使用专用密钥产生的并从便携式设备 6 输出的值被读取，即，发生了所谓的伪装攻击，则个人计算机 1 能够检测欺骗，因为下一次相互鉴定是使用不同的值进行的。

内容 ID 是用于鉴定内容的一个内容 ID。

编解码器 ID 是对应于内容的编码方法的 ID。例如，编解码器 ID 的“1”对应于 ATRAC3，而编解码器 ID 的“0”对应于 MP3（MPEG（运动图像专家组）音频层-3）。

文件名称是从对应于内容的内容文件(将在后文描述)的转换中得到的数据并以 ASCII 码（美国国家信息互换标准代码）记录在个人计算机 1 中。文件信息是将音乐标题（内容名称）、演奏该音乐的艺术家的名字、音乐的歌曲作者的名字或音乐片段的作曲者的名字的转换成 ASCII 码中得到的数据。

当便携式设备 6 从个人计算机 1 中接收内容和内容写入命令时，执行从 RAM 54 或 ROM 55 读取的主程序的 CPU 53 将接收写命令，控制快闪存储器控制器 60 并将从个人计算机 1 接收的内容写入到快闪存储器 61。

快闪存储器 61 具有大约存储 64M 字节内容的存储能力。并且，快闪存储器已经事先将重放代码存储于其中用以扩展以预定方式已经压缩的内容。

注意：快闪存储器 61 可以作为可连接到便携式设备 6 并从便携式设备 6 中移去的存储卡。

当通过操作键控制器 62 将具有对应于播放/停止按钮（未示出）的下拉操作的重放命令提供给 CPU 53 时，CPU 53 将使快闪存储器 60 从快闪存储器 61 中读取重放代码和内容并将他们发送到便携式设备 6 的 DSP 59。

在根据从快闪存储器 61 发送的重放代码用 CRC（循环冗余码校验）方法检测出内容中的错误时，DSP 59 将重放该内容和重放的数据（在图 3 中以 D1 指示）传送到数字/模拟转换电路 63。

DSP 59 是和在便携式设备 6 内部提供的发送电路（未示出）集成形成的

用以根据外部晶振 59A 的主时钟 MCLK 重放内容，并将主时钟 MCLK、基于主时钟 MCLK 并由内部振荡电路产生的、具有预定频率的比特时钟 BCLK 和由以帧单元中的 L 通道时钟 LCLK 和 R 通道 RCLK 组成的操作时钟 LRCLK 提供给数字/模拟转换电路 63。

为了重放内容，DSP 59 根据重放代码将上述的操作时钟提供给数字/模拟转换电路 63。当没有内容重放时，DSP 59 根据重放代码将停止提供操作时钟以关闭数字/模拟转换电路 63，由此降低了整个便携式设备 6 的功耗。

相似地，CPU 53 和 USB 控制器 57 具有分别连接于其上的外部晶振 53A 和 57A，并根据分别从晶振 53A 和 57A 提供的主时钟 MCLK 执行预定操作。

由于上述的结构，便携式设备 6 不需要时钟产生模块来为 CPU 53、DSP 59 和 USB 控制器的每一个提供时钟，并且因此能够设计为具有更简单和紧凑的电路结构。

数字/模拟转换电路 63 将重放的内容转换成模拟音频信号并将其提供给放大电路 64。放大电路 64 放大该音频信号并通过耳机插座 65 将其提供给耳机。

因此，当按下播放/停止按钮时，便携式设备 6 在 CPU 53 的控制下重放存储在快闪存储器 61 中的内容。当在重放内容的过程中按下播放/停止按钮时，便携式设备 6 将停止重放内容。

当在停止内容重放操作之后按下播放/停止按钮时，便携式设备 6 在 CPU 53 的控制下，将在重放操作已经停止的位置处恢复内容重放。当在按下播放/停止按钮停止内容重放操作之后几秒内没有另外的操作执行时，便携式设备 6 将自动关闭电源，从而降低功耗。

在此应该注意，当在电源关闭之后按下播放/停止按钮时，便携式设备 6 将恢复播放第一首音乐或第 1 号音乐，而不重放先前重放操作停止位置处的内容。

而且，便携式设备 6 的 CPU 53 使 LCD 控制器 68 在显示器 67 上显示重放模式（例如，重复播放、介绍播放等）、均衡调整（即，对音频信号的频带的增益调整）、音乐的标号、播放时间、诸如播放、停止、快进和快退之类的操作模式以及诸如音量和干电池 51 的电压电平之类的信息。

而且，便携式设备 6 将写在快闪存储器 80 中的内容的数目、内容所写入的快闪存储器 61 的块的位置以及存储在存储器中的各种信息的所谓的 FAT

（文件分区表）分别存储在 EEPROM 68 中。

应该注意：在该实施例中，内容被当作是 64K 字节的一个块，并且每首音乐的内容的块的位置是存储在 FAT 中的。

在 FAT 被存储在快闪存储器 61 中的情况下，当在 CPU 53 的控制下，第一首音乐的内容被写入到快闪存储器 61 中时，对应于第一首音乐的内容的块的位置将作为 FAT 被写入到快闪存储器中，并且当第二首音乐的内容被写入到快闪存储器 61 中时，对应于第二首音乐的内容的块的位置将作为 FAT 被写入到快闪存储器 61 中（在和已经写入的第一首音乐相同的区域中）。

以这种方式，当每次内容被写入到快闪存储器 61 中时，FAT 被重新写入，并且为了保护该数据，相同的数据将被再次写入以备保留。

当 FAT 被写入到快闪存储器 61 中时，在快闪存储器中的相同位置对应于第一次内容的写入将被写入两次。由于这种原因，当已经进行了几次的内容写入时，将达到快闪存储器 61 重写的指定的次数，使得快闪存储器 61 将不能再被重写。

为了避免上述问题，便携式设备 6 使 EEPROM 68 存储 FAT，使得 FAT 在快闪存储器 61 中在每一内容的写入上的重写次数将降低。

通过将重写许多次的 FAT 存储在 EEPROM 68 中，便携式设备 6 能够适于内容可以十倍于 FAT 被存储到快闪存储器 61 中的频率被写入到快闪存储器 61。而且，因为 CPU 53 使 EEPROM 68 也存储 FAT，则在 EEPROM 68 中的相同区域以降低的频率被重写以防止 EEPROM 过早地变成不可重写。

当便携式设备 6 通过 USB 电缆 7（此后将称作“USB 连接”）连接到个人计算机 1 时，根据从 USB 控制器 57 向 CPU 53 提供的中断信号来识别 USB 连接已经进行。

当便携式设备 6 识别出 USB 连接时，通过 USB 电缆 7 从个人计算机 1 将具有特定电流值的外部电源提供给便携式设备 6，并且便携式设备 6 使电源电路 52 停止从干电池 51 供电。

当建立了 USB 连接时，CPU 53 将停止 DSP 59 的重放内容。因此，CPU 53 将防止从个人计算机 1 供给的外部电源超过特定的电流值使得能够一直提供特定电流值的外部电源。

因此，当建立了 USB 连接时，CPU 53 在干电池 51 提供的电源和个人计算机 1 提供的电源之间选择。即，可以使用个人计算机 1 的廉价的外部电源，

因此较少地消耗从干电池 51 提供的昂贵的电源。因此，干电池 51 可以使用较长的使用寿命。

注意：当通过 USB 电缆 7 从个人计算机 1 提供外部电源时，CPU 53 停止 DSP 59 重放内容以降低 DSP 59 的辐射，使得包括个人计算机 1 的整个系统的辐射可以进一步降低。

通过执行安装在个人计算机 1 中的程序而实现的个人计算机 1 的功能将在下面说明。

现在参考图 4，示出个人计算机 1 的示意图，该图说明通过执行预定的程序而实现的个人计算机 1 的功能。

如图所示，个人计算机 1 使用由包括 EMD 选择程序 131、校验输入/校验输出管理程序 132、复制管理程序 133、移动管理程序 134、加密方法转换程序 135、压缩方法转换程序 136、加密程序 137、压缩/扩展程序 138、使用规则转换程序 139、使用规则管理程序 140、鉴定程序 141、解密程序 142、PD 驱动程序 143、购买程序 144 和 145 的多个程序组成的内容管理程序 111。

在上述程序中，内容管理程序 111 由混洗（shuffle）或加密指令组成，例如，从外部取消所指令的操作使得翻译该指令很困难（例如，即使用户可以直接读出内容管理程序 111，他或她不能识别该指令）。

当内容管理程序 111 被安装在个人计算机 1 中但它是在 EMD 注册时通过网络 2 从 EMD 注册服务器 3 中被接收的时候，EMD 选择程序 131 不包括在内容管理程序 111 中。EMD 选择程序 131 选择和 EMD 服务器 4（4-1 至 4-3）的连接以使购买应用 115、购买程序 144 或 145 能够与 EMD 服务器 4(4-1 至 4-3)（例如，购买内容的下载）通信。

根据在内容数据库 114 中记录的校验输入或校验输出和使用规则文件 162-1 至 162-N 的设置，校验输入/校验输出管理程序 132 将存储在内容文件 161-1 至 161-N 中的内容校验输出到便携式设备 6 中的任意一个，或对在便携式设备 6 中存储的内容进行校验输入。

为响应已经进行的校验输入或校验输出，校验输入/校验输出管理程序 132 更新在内容数据库 114 中记录的存储在使用规则文件 162-1 至 162-N 中的使用规则。

根据记录在内容数据库 114 中的使用规则文件 162-1 至 162-N，复制管理程序 133 将在内容文件 161-1 至 161-N 中存储的内容复制到任一便携式设

备 6，或从便携式设备 6 复制内容到内容数据库 114。

还根据记录在内容数据库 114 中的使用规则文件 162-1 至 162-N，移动管理程序 134 将存储在内容文件 161-1 至 161-N 中的内容移动到任一便携式设备 6，或从便携式设备 6 移动内容到内容数据库 114。

加密方法转换程序 135 转换到和记录在内容数据库 114 中的内容文件 162-1 至 162-N 中存储的内容所使用的加密方法、购买应用 115 通过网络 2 从 EMD 服务器 4-1 接收的内容所使用的加密方法、购买程序 144 通过网络 2 从 EMD 服务器 4-2 接收的内容所使用的加密方法，相同的加密方法。

压缩方法转换程序 136 转换到和在内容数据库 114 中记录的内容文件 161-1 至 161-N 中存储的内容所使用的压缩方法、购买应用 115 通过网络 2 从 EMD 服务器 4-1 接收的内容所使用的压缩方法、购买程序 144 通过网络 2 从 EMD 服务器 4-2 接收的内容所使用的压缩方法，相同的压缩方法。

加密程序 137 被用于以与记录在内容数据库 114 中的内容文件 161-1 至 161-N 中存储的内容所使用的相同的加密方法加密从 CD 中读取的和从例如记录程序 113 提供的内容（未加密）。

压缩/扩展程序 138 以与记录在内容数据库 114 中的内容文件 161-1 至 161-N 中存储的内容所使用的相同的编码方法编码从 CD 中读取的和从例如记录程序 113 提供的内容（未压缩）。并且，压缩/扩展程序 138 将扩展（解密）所编码的内容。

使用规则转换程序 139 转换到和记录在内容数据库 114 中的使用规则文件 162-1 至 162-N 中存储的使用规则、购买应用 115 通过网络 2 从 EMD 服务器 4-1 接收的内容的使用规则、购买程序 144 通过网络 2 从 EMD 服务器 4-2 接收的内容的使用规则，相同的格式。

在执行内容复制、移动、校验输入或校验输出之前，使用规则管理程序 140 根据满足记录在内容数据库 114 中的使用规则文件 162-1 至 162-N 中存储的使用规则的混编（hash）值（将在以后描述）检测使用规则的伪造或改变。由于记录在内容数据库 114 中的使用规则文件 162-1 至 162-N 中存储的使用规则是随着内容复制、移动、校验输入或校验输出而更新的，所以使用规则管理程序 140 更新满足使用规则的混编值。

鉴定程序 141 执行在内容管理程序 111 和购买应用 115 之间相互鉴定，以及在内容管理程序 111 和购买程序 144 之间的相互鉴定。并且，鉴定程序

141 将存储在 EMD 服务器 4-3 和购买程序 145 之间的相互鉴定中使用的鉴定密钥。

应该注意到当在个人计算机 1 中安装了内容管理程序 111 时，鉴定程序 141 在相互鉴定中使用的鉴定密钥尚未存储在鉴定程序 141 中，但当显示/操作-指令程序 112 已经成功地注册了鉴定密钥时，该密钥被从 EMD 注册服务器 3 中提供并存储在鉴定程序 141 中。

当个人计算机 1 重放记录在内容数据库 114 中的内容文件 161-1 至 161-N 中存储的内容时，解密程序 142 解密内容。

当将预定的内容校验输出到便携式设备 6 或从便携式设备 6 校验输入预定的内容时，PD 驱动程序 143 为便携式设备 6 提供内容或使便携式设备 6 执行预定操作的命令。

通过网络 2 从 EMD 注册服务器 3 或当记录在预定的 CD 中时所提供的购买程序 144 与内容管理程序 111 一起被安装在个人计算机 1 中。当安装在个人计算机 1 中时，购买程序 144 将通过内容管理程序 111 具有的预定形式的接口发送或接收内容管理程序 111 和数据。

购买程序 144 由混洗的或加密的指令组成，例如，隐藏从外部所指示的操作使得翻译该指令很困难（例如，即使用户可以直接读出购买程序 144，他也不能识别该指令）。

购买程序 144 通过网络 2 请求 EMD 服务器 4-2 发送预定的内容并因此接收来自 EMD 服务器 4-2 的内容。在接收来自 EMD 服务器 4-2 的内容时，购买程序 144 将计算该内容。

购买程序 145 将和内容管理程序 11 一起被安装。它通过网络 2 请求 EMD 服务器 4-3 发送预定的内容并因此接收来自 EMD 服务器 4-3 的内容。在接收来自 EMD 服务器 4-3 的内容时，购买程序 144 将计算该内容。

根据过滤数据文件 181、显示数据文件 182、图像文件 183-1 至 183-K 或历史数据文件 184，显示/操作-指令程序 112 在显示器单元 20 中显示预定窗口的图像并响应用户进行的键盘 18 或鼠标 19 的操作将校验输入或校验输出指令给出到内容管理程序 111。

过滤数据文件 181 存储用于加权记录在内容数据库 114 中的内容文件 161-1 至 161-N 中存储的内容的数据，并被记录在 HDD 21 中。

显示数据文件 182 存储对应于记录在内容数据库 114 中的内容文件

161-1 至 161-N 中存储的内容的数据，并被记录在 HDD 21 中。

图像文件 183-1 至 183-K 存储对应于记录在内容数据库 114 中的内容文件 161-1 至 161-N 的图像或对应于包（将在以后描述）的图像，并被记录在 HDD 21 中。

此后只要图像文件 183-1 至 183-K 不被单独提及，将被简单地称为“图像文件 183”。

历史数据文件 184 存储包括对记录在内容数据库 114 中的内容文件 161-1 至 161-N 中存储的内容已经校验输出的次数、已经校验输入的内容次数和进行校验输出和校验输入的日期的历史数据。历史数据文件 184 记录在 HDD 21 中。

为了注册，在通过网络 2 接收来自 EMD 注册服务器 3 的鉴定密钥和 EMD 选择程序 131 并将他们提供到内容管理程序 111 的同时，显示/操作-指令程序 112 通过网络将预存储的内容管理程序 111 的 ID 发送到 EMD 注册服务器 3。

记录程序 113 被用于响应用户的键盘 18 或鼠标 19 的操作显示预定窗口的图像，并且读取诸如来自 CD 的内容的记录时间的数据，该 CD 在本实施例中是驱动器 22 中设置的光盘 42。

根据在 CD 中记录的内容的记录时间，记录程序 113 通过网络 2 请求 WWW 服务器 5-1 或 5-2 发送对应于 CD 的诸如碟名或艺术家名字之类的数据或者对应于在 CD 中记录的内容的诸如音乐标题之类的数据，并通过网络 2 接收这些来自 WWW 服务器 5-1 或 5-2 的对应于 CD 或在 CD 中记录的内容的数据。

而且，记录程序 113 将对应于 CD 的接收的数据或对应于 CD 中记录的内容的数据提供给显示/操作-指令程序 112。

进一步，当被提供了记录指令时，记录程序 113 将来自在本实施例中为设置在驱动器 22 中的光盘 42 的 CD 的内容读取并输出到内容管理程序 111。

内容数据库 114 将来自内容管理程序 111 的、已经按照预定方式压缩并按照预定方式加密的内容存储为内容文件 161-1 至 161-N 的任一个（将内容记录到 HDD 21 中）。内容数据库 114 将存储在内容文件 161-1 至 161-N 中的内容的使用规则存储成对应于在其中存储了该内容的内容文件 161-1 至 161-N 的使用规则文件 162-1 至 162-N 的任何一个（将使用规则记录到 HDD 21 中）。

内容数据库 114 可以记录作为记录的内容文件 161-1 至 161-N 或使用规

则文件 162-1 至 162-N。

例如存储在内容文件 161-1 中的内容使用规则被存储在使用规则文件 162-1 中。例如存储在内容文件 161-N 中的内容使用规则被存储在使用规则文件 162-N 中。

此后只要内容文件 161-1 至 161-N 不被单独提及，将被简单地称为“内容文件 161”。并且此后只要使用规则文件 162-1 至 162-N 不被单独提及，将被简单地称为“使用规则文件 162”。

通过网络 2 或以在预定的 CD-ROM 中记录的方式，从 EMD 注册服务器 3 提供购买应用 115。在从 EMD 服务器 4-1 中接收该内容并将它提供给内容管理程序 111 的同时，购买应用 115 通过网络 2 请求 EMD 服务器 4-1 发送预定内容。并且在从 EMD 服务器 4-1 中接收程序时，购买应用 115 将计算该内容。

下面，下面将描述在存储在显示数据文件 82 的数据和存储在内容数据库 114 中的内容文件 161-1 至 161-N 之间的关系。

首先，存储在任何内容文件 161-1 至 161-N 中的内容属于预定的包。更具体地说，该包是原始包、我所选择的包和过滤包中的任何一个。

在上述包中，原始包具有属于此的一个以上的内容。该包对应于在 EMD 服务器 4 中的内容分类（即所谓的碟名）或对应于一个 CD。内容属于任何原始包并且不能属于多个原始包。而且，内容所属的原始包不能被修改。用户可以编辑对应于原始包的部分信息（例如，附加信息或附加信息的改动）。

由用户自由选择的多于一个的内容属于我所选择的包。用户可以分别对我所选择的包任意编辑指定的内容。同时内容可以属于多于一个的我所选择的包。并且，内容也可以不属于任何我所选择的包。

根据存储在过滤数据文件 181 中的过滤数据所选择的内容属于过滤包。通过网络 2 从 EMD 服务器 4 或 WWW 服务器 5 或作为在预定 CD 中记录提供过滤数据。用户可以编辑在过滤数据文件 181 中存储的过滤数据。

过滤数据是对预定内容的选择或对应于该内容加权计算的参考。例如，对应于每周 J-POP（日本流行音乐）的前十名的过滤数据可以由个人计算机 1 使用来识别每周 J-POP 的 No. 1 至 10 的内容。

过滤数据文件 181 包括以在过去的一个月中已经校验输出的周期的长度的降序排列的用于内容选择的过滤数据、以在过去的半年中已经校验输出的次数的降序排列的用于内容选择的过滤数据、或用于选择在其中字符“AI”

（爱）包含在音乐标题（内容名字）中的内容的滤波数据。

因此，通过将过滤数据与内容显示数据 221（包括用户已经设置的数据）、历史数据 184 等相比较来选择在过滤包中的内容。

驱动程序 117 在内容管理程序 111 等的控制下驱动音频输入/输出接口 24 以输入作为从外部提供的数字数据的内容并将它提供给内容管理程序 111，并作为数字数据通过内容管理程序 111 输出从内容数据库 114 提供的内容，或者通过内容管理程序 111 输出对应于从内容数据库 114 提供的内容的模拟信号。

图 5 示出了显示/操作-指令程序 112 使显示器单元 20 显示的显示/操作-指令窗口的例子。

在显示/操作-指令窗口中显示的有用于启动记录程序 113 的按钮 201、用于启动 EMD 选择程序 131 的按钮 202、用于显示设置校验输入或校验输出的区域的按钮 203、用于显示我所选择的包将被编辑的区域的按钮 204 等。

当选择按钮 205 时，对应于原始包的数据被显示在窗口的区域 211 中。当选择按钮 206 时，对应于我所选择的包的数据被显示在窗口的区域 211 中。当选择按钮 207 时，对应于过滤包的数据被显示在窗口的区域 211 中。

在区域 211 中显示的数据是关于包的数据。例如它是包名或艺术家的名字。

如图 5 所示，在区域 211 中显示的有包名“FIRST”和艺术家名字“A TARO”、包名 “SECOND” 和艺术家名字 “A TARO” 等。

显示/操作-指令窗口还具有区域 212，在区域 212 中显示对应于属于在区域 211 中选择的包的内容的数据。在该区域中显示的数据是音乐标题、播放时间或该内容可以被校验输出的次数。

在图 5 中，对应于包名 “SECOND” 的包被选择。所以，在区域 212 中显示的是对应于属于对应于包名 “SECOND” 是包的内容的音乐标题（内容名字）“MINAMI-NO-SAKABA”、该内容可以被校验输出的（例如，1/8 音符是用于校验输出一次以及 2/8 音符是用于校验输出两次）次数，以及音乐标题（内容名字）“KITA-NO-HAKABA” 和该内容可以被校验输出的次数（例如，1/8 音符对应于校验输出一次）。

因此，显示在区域 212 中的作为内容可以被校验输出的次数指示着相应的内容可以校验输出一次。

显示在区域 212 中的其它作为内容可以被校验输出的次数指示相应的内容不能被校验输出（校验输出数目是 0；但是，个人计算机可以重放那个内容）。显示在区域 212 中的作为内容可以被校验输出的次数的 C ce1f 指示着相应的内容的校验输出是没有限制的（该内容可以被以任意次数校验输出）。

注意：可以被校验输出的内容的次数可以用如图 5 中所示的相应个数的预定符号（例如，它可以是圆圈、星号、月牙等）和数字来指示。

在显示/操作-指令窗口中还显示有区域 208，在区域 208 中显示有对应于选择的包或内容（对应于图 4 中的图像文件 183-1 至 183-K 的任何一个）的图像等。在该区域中，当重放一个选择的内容（将对应于该内容的声音输出到扬声器 45）时，点击按钮 209。

在选择按钮 205 并且对应于原始包的数据正在被显示在区域 211 中的同时，当选择了在区域 212 中显示的预定内容（内容名字）的音乐标题并且进行删除操作时，显示/操作-指令程序 112 将使内容管理程序 111 对应于所选择的音乐标题，删除存储在内容数据库 114 中的预定的内容。

在记录程序 113 的控制下正在选择（使有效）显示在窗口中的按钮 255（将在以后说明）的同时，当从 CD 读出的内容被记录在内容数据库 114 中时，显示/操作-指令程序 112 将使显示/操作-指令窗口显示区域 213，在区域 213 中显示有在预指定的便携式设备 6 中存储的内容的音乐标题（内容名字）。

在记录程序 113 的控制下正在选择（使有效）显示在窗口中的按钮 255（将在以后说明）的同时，当从 CD 读出的内容被记录在内容数据库 114 中时，显示/操作-指令程序 112 将使内容管理程序 111 将在内容数据库 114 中记录的和从 CD 读取的内容校验输出到预指定的便携式设备 6。

在区域 213 的对应于内容的音乐标题（内容名字）的最左边的位置上显示有一个符号，指示着该内容是否能校验输入到个人计算机 1 中。例如，在区域 213 的最左边的符号“○”指示着对应于内容的音乐标题的内容可以校验输入到个人计算机 1 中（即，它已经从个人计算机 1 中被校验输出）。在区域 213 的最左边的符号“×”指示着对应于内容的音乐标题不可以校验输入到个人计算机 1 中（即，它还没有从个人计算机 1 中被校验输出，例如它已经从其他的个人计算机中被校验输出）。

当显示/操作-指令程序 112 已经在显示/操作-指令窗口中显示了区域 213 时，显示/操作-指令程序 112 将在显示/操作-指令窗口中显示区域 214，

在区域 214 中显示便携包（存储在便携式设备 6 中的内容属于该便携包）的名字、关闭区域 213 的按钮 210 和执行校验输入或校验输出操作的按钮 215。

而且，当显示/操作-指令程序 112 已经在显示/操作-指令窗口中显示了区域 213 时，显示/操作-指令程序 112 将在显示/操作-指令窗口中显示对对应于在区域 212 中选择的音乐标题的内容设置校验输出操作的按钮 216、对对应于在区域 213 中选择的音乐标题的内容设置校验输入操作的按钮 217、对对应于在区域 213 中显示的内容名字的所有内容设置校验输入操作的按钮 218、和取消校验输入或校验输出设置的按钮 219。

尽管具有通过按钮 216 至 219 设定的校验输入或校验输出设置，但是，个人计算机 1 将不执行校验输入或校验输出操作。

当在通过使用按钮 216 至 219 设置了校验输入或校验输出之后点击了按钮 215 时，显示/操作-指令程序 112 将使内容管理程序 111 执行校验输入或校验输出。也就是说，当点击按钮 215 时，显示/操作-指令程序 112 将根据校验输入或校验输出设置使内容管理程序 111 发送内容或删除对应于校验输入设置的预定内容的命令（例如，删除存储在便携式设备 6 中的预定内容的命令）到便携式设备 6，并对应于所发送的内容或命令更新存储在使用规则文件 162 中的使用规则。

当执行校验输入或校验输出操作时，显示/操作-指令程序 112 将响应所发送的内容或命令以更新在历史数据文件 184 中存储的历史数据。历史数据包括用于识别已经校验输入或校验输出的内容的信息或内容被校验输入或校验输出的日期，以及从该便携式设备校验输出内容的便携式设备 6 的名字。

因为校验输入或校验输出操作可以在短时间内设置，所以用户可以很快地知道校验输入或校验输出执行之后的状态，所以耗时的校验输入或校验输出操作的次数可以降低以便使校验输入或校验输出步骤中花费的总时间（包括校验输入或校验输出操作的设置和执行）最少。

图 6 示出了记录程序 113 使显示单元 20 显示的窗口的例子。

例如根据从 WWW 服务器 5-2 中接收的 CD 信息，记录程序 113 将在区域 251 中显示诸如“ACYNCHRONIZED”的 CD 标题。并且，根据从 WWW 服务器 5-2 中接收的 CD 信息，记录程序 113 将在区域 252 中显示诸如“KUWAI”的艺术家名字。

根据从 WWW 服务器 5-2 中接收的 CD 信息，记录程序 113 将在显示音乐标

题的区域253中显示诸如“HEAT”、“PLANET”、“BLACK”、“SOUL”等之类的音乐标题。相似地，记录程序113将在显示艺术家名字的区域253中显示诸如“KUWAI”的艺术家名字。

在接收预定的CD信息之后，记录程序113将其存储在HDD 21中的预定的目录中。

在通过点击按钮254接收用于获得CD信息的指令时，记录程序113将首先在HDD 21中的预定目录中搜索。当发现CD信息存储在该目录中时，记录程序113将显示对话框（未示出）以提示用户选择他或她是否将使用存储在目录中的CD信息。

当通过记录程序113显示的窗口中显示的指令开始记录内容的按钮25被点击时，记录程序113将从设置在驱动器22中的CD中读取内容，并将其和CD信息一起提供给内容管理程序111。内容管理程序111的压缩/扩展程序138以预定的方式压缩从记录程序113提供的内容，并且加密程序137加密压缩后的内容。而且，使用规则转换程序139产生压缩和加密后的内容的使用规则。

内容管理程序111将压缩和加密后的内容和使用规则一起提供给内容数据库114。

内容数据库114将为从内容管理程序111接收的内容产生内容文件116和使用规则文件162，并将内容存储在内容文件161，将使用规则存储在使用规则文件183中。

当内容和内容使用规则被存储在内容数据库114中时，内容管理程序111将从记录程序113接收的CD信息和使用规则提供给显示/操作-指令程序112。

显示/操作-指令程序112根据通过记录和CD信息存储在内容数据库114中的内容的使用规则将存储的数据显示在显示数据文件182。

由记录程序113显示的窗口已经显示按钮255用以当从CD读取的内容被记录在内容数据库114中时，自动地设置便携式设备是否校验输出从CD读取的内容。

例如，当点击按钮255时，记录程序113将显示示出便携式设备6的下拉菜单。当用户从下拉菜单中选择便携式设备6时，个人计算机1自动地将从CD记录的内容校验输出到所选择的便携式设备6。当用户从下拉菜单中选择“不校验输出”时，个人计算机1将对从CD记录的内容不校验输出。

因此，当从 CD 读取的内容被记录到内容数据库 114 中，仅有通过记录程序 113 显示的窗口中的按钮 255 被设置成有效时，个人计算机 1 可以使预指定的便携式设备 6-1 至 6-3 的任一个对从 CD 读取的内容进行校验输出。

（2）不同格式间的处理

同时，存在有多个供给音乐内容的内容发送方，各个内容发送方的内容加密系统和使用条件信息的格式互不相同。所以，用户一般必须购买内容管理应用或便携式设备用于各个不同的发送方所提供的所需内容的再现或校验输入/校验输出。并且因此用户不能通过一个单独的管理应用或一个单独的便携式设备处理存储在个人计算机上的音乐内容。

所以，本系统设想在个人计算机 1 上以一种统一的方式处理不同发送方的不同格式的内容。

参考图 7，在该音乐内容发送系统中的不同发送方的不同格式的内容的统一处理将参考图 7 进行说明。

假设连接到网络 2 上的多个 EMD 服务器是发送由音乐提供公司 A 提供的音乐内容的 EMD 服务器 A4-1、发送由音乐提供公司 B 提供的音乐内容的 EMD 服务器 B4-2 以及发送由音乐提供公司 X 提供的音乐内容的 EMD 服务器 X4-3。这些 EMD 服务器 4（4-1、4-2 和 4-3）将每一公司特有节目的音乐内容通过网络 2 提供给用户拥有的个人计算机 1。而且，通过服务器 4 采用各服务器独特的音乐内容的加密系统、使用条件（使用规则）信息的格式、音乐内容压缩系统和移动补偿的收费系统，各自的 EMD 服务器 4（4-1、4-2 和 4-3）以不同的形式发送音乐内容。

在个人计算机 1 中，安装有用于再现或管理音乐内容的应用软件：用于购买、监督和再现来自 EMD 服务器 A4-1 的音乐内容的再现应用 A311；用于购买、监督和再现来自 EMD 服务器 B4-2 的音乐内容的再现应用 B312；用于将音乐内容发送到便携式设备 A6-1 的设备驱动程序 A313；以及用于将音乐内容发送到便携式设备 B6-2 的设备驱动程序 B314。同时，图 7 所示的再现应用 311、312 分别对应于图 4 所示的购买应用 115 和驱动程序 117。

在个人计算机 1 中，安装有用于管理 HDD 21 中存储的全部音乐内容的综合控制的综合管理单元 X 315。该综合管理单元 X 315 是由 EMD 的接收接口 316、EMD317 的发送接口和 PD 318 的驱动程序组成。

这里假设便携式设备 A6-1 是复制音乐提供公司 A 的音乐的专用设备、便

携式设备 B6-2 是复制音乐提供公司 B 的音乐的专用设备、便携式设备 X6-3 是复制音乐提供公司 X 的音乐的专用设备。还假设存储在存储卡中的音乐内容根据每一音乐提供公司独特的加密系统、使用也各不相同的使用条件信息或压缩系统的格式被加密，使得音乐内容不能例如通过直接连接被发送到其他设备驱动器。

再现应用 A311 执行连接 EMD 服务器、上传例如登录文件和下载音乐内容、内容密钥和使用条件信息的处理。该再现应用 A311 适用于执行仅该应用能够处理的 EMD 服务器的连接处理。这里，再现应用 A311 适用于执行与 EMD 服务器 4-1 有关的处理，但它不能执行对任何其他的 EMD 服务器的连接处理。再现应用 A311 还适用于执行对与 EMD 服务器 A4-1 连接的鉴定的处理、对与便携式设备 A6-1 的连接的鉴定的处理、以及对在 HDD 21 中存储的音乐内容和使用条件信息的加密/解密的处理。再现应用 A311 使用内容密钥加密从 EMD 服务器 4-1 下载的音乐内容和相应的使用条件信息并使用对话密钥加密该内容密钥以将加密的密钥存储在 HDD 21 中。同时，各自的再现应用采用各自的独特的加密系统，使得存储在个人计算机 1 中的相同的 HDD 21 中的音乐内容不能解密其他的再现应用而只能解密专用的再现应用。

再现应用 A311 还管理附加在每一音乐内容上的使用条件信息。例如，如果在使用条件信息中说明了再现的次数的限制值，则这样的限制就施加在可能的内容再现的次数上，再现应用 A311 对于每次再现或复制对再现或复制的次数的限制值减 1。

再现应用 A311 还将它在 HDD 21 上管理的音乐内容和使用条件信息发送到综合管理单元 X 315 的 EMD 的接收接口 316。

再现应用 B312 执行连接 EMD 服务器、上传例如登录文件和下载音乐内容、内容密钥和使用条件信息的处理。该再现应用 B312 适用于执行仅该应用能够处理的 EMD 服务器的连接处理。具体地说，再现应用 B312 适用于执行与 EMD 服务器 4-2 有关的处理，但它不能执行对与任何其他的 EMD 服务器连接的处理。再现应用 B312 执行对与 EMD 服务器 4-2 的连接的鉴定的处理、对便携式设备 B6-2 的连接的鉴定的处理、以及对存储在 HDD 21 中的音乐内容和使用条件信息的加密/解密的处理。例如，再现应用 B312 使用内容密钥加密从 EMD 服务器 4-2 下载的音乐内容和相应的使用条件信息，并使用对话密钥加密内容密钥并将加密后的内容密钥存储在 HDD 21 中。

再现应用 B312 还管理附加在各自音乐内容上的使用条件信息。例如，如果在使用条件信息中说明了再现的次数的限制值，则这样的限制就施加在可能的内容再现的次数上，再现应用 B312 对于每次再现或复制对再现或复制的次数的限制值减 1。

再现应用 B312 还将它在 HDD 21 上管理的音乐内容和使用条件信息发送到综合管理单元 X 315 的 EMD 的接收接口 316。

设备驱动程序 A313 是将音乐内容发送到便携式设备 A6-1 的应用软件。设备驱动程序 A313 将音乐内容发送到便携式设备 A6-1。

设备驱动程序 B314 是将音乐内容发送到便携式设备 B6-2 的应用软件。设备驱动程序 B314 将音乐内容发送到便携式设备 B6-2。

综合管理单元（X）315 是提供有来自 EMD 服务器（X）4-3 的音乐内容的音乐提供公司 X 的专用应用软件。该综合管理单元（X）315 还是用于在它和设备驱动程序（A）313、设备驱动程序（B）314、再现应用（A）311 和再现应用（B）312 之间发送音乐内容和使用条件信息以便综合管理个人计算机 1 中的音乐内容的监督软件。综合管理单元（X）315 还能够将其监督的音乐内容发送到专用便携式设备 6-3 中，该专用便携式设备 6-3 是便携式音乐再现设备。

综合管理单元（X）315 执行对应于图 4 中所示的内容管理程序 111 的处理。

描述（projection）显示单元 318 是用于连接便携式设备 6-3 的接口模块，并在其和便携接口 6-3 之间执行鉴定处理和加密处理。而且，在将音乐内容等发送到其他的便携式设备 6-1、6-2 时，描述显示单元 318 将音乐内容和使用条件信息通过设备驱动程序(A) 313 至设备驱动程序（B）314 发送。

在通过网络 2 接收自 EMD 服务器（X）4-3 发送的音乐内容和使用条件信息并将该音乐内容和使用条件信息与 PD 驱动程序 318 进行交换的同时，EMD316 的接收接口接收来自再现应用（A）311 和再现应用（B）312 的音乐内容和使用条件信息。

在接收来自再现应用（A）311 和再现应用（B）312 的音乐内容和使用条件信息时，EMD316 的接收接口执行相互鉴定、加密系统的转换、附加在正在发送的音乐内容上的使用条件信息等的格式的转换以及正在发送的音乐内容的压缩系统的转换。由再现应用（A）311 和再现应用（B）312 使用的加密系

统、使用条件信息或压缩系统被转换成综合管理单元（X）315 使用的系统。以下将综合管理单元（X）315 使用的系统称为统一传输协议。EMD 316 的接收接口通过PD驱动程序 318 将如此转换为统一传输协议的音乐内容和使用条件信息发送到设备驱动程序（A）313 或设备驱动程序（B）314。EMD 316 的接收接口还通过PD驱动程序 318 将如此转换为统一传输协议的音乐内容和使用条件信息发送到便携式设备 6-3。

EMD 服务器（A）4-1 和 EMD 服务器（B）4-2 提供的音乐内容一旦由再现应用（A）311 和再现应用（B）312 下载，并且加密系统、压缩系统和音乐内容的使用条件信息被转换成统一传输协议并被发送到综合管理单元（X）315。综合管理单元（X）315 全面地监督从 EMD 服务器（A）4-1 和 EMD 服务器（B）4-2 和 EMD 服务器（X）4-3 下载的内容提供公司的音乐内容。

EMD316 的接收接口也具有音乐内容的复制、移动和执行校验输入和校验输出的功能。

EMD316 的接收接口根据来自用户的复制或移动命令执行复制或移动存储在再现应用(A)311 至再现应用(B)312 中的音乐内容的处理。此时，EMD316 的接收接口将音乐内容的加密系统、压缩系统和使用条件的陈述格式转换成统一传输协议。

EMD316 的接收接口还根据来自用户的 CD 发送（ripping）命令或校验输入命令执行将存储在诸如 CD 的外部介质中或便携式设备 6-1 至 6-3 中的音乐内容复制或校验输入到综合管理单元（X）315 的处理。如果此时音乐内容的加密系统或压缩系统或使用条件的描述格式没有被转换成统一传输协议，则 EMD316 的接收接口使其转换为统一传输协议。

EMD316 的接收接口还根据来自用户的校验输出命令对通过在便携式设备 6-3 中的综合管理单元（X）315 管理的音乐内容执行记录的处理。如果此时音乐内容的加密系统或压缩系统或使用条件的描述格式没有被转换成统一传输协议，则 EMD316 的接收接口使其转换为统一传输协议。而且此刻使用条件的校验输出的可用数目被减 1。

如图 8 所示，综合管理单元（X）315 具有在较低的应用层的统一传输协议，该较低的应用层用于将数据传输到其他购买应用。综合管理单元(X)315 使用在统一传输协议以下的层作为 http(超文本传输协议)与 EMD 服务器(X) 4-3 进行数据发送/接收。

在上述的音乐内容发送系统中，自 EMD 服务器（A）4-1 和 EMD 服务器（B）4-2 发送的音乐内容由综合管理单元（X）315 获得用以再现或管理。并且，该 EMD 服务器（X）4-3、EMD 服务器（A）4-1 和 EMD 服务器（B）4-2 发送的音乐内容被传输到便携式设备（X）6-3。

在如上所述的音乐内容发送系统中，综合管理单元（X）315 主要与各自的再现应用和设备驱动程序相关联进行操作以转换将要发送的音乐内容的加密系统、附加在将要发送的音乐内容上的使用条件信息的格式或将要发送的音乐内容的压缩系统，以在统一传输协议的帮助下实现音乐内容的传输。因此，由再现应用（A）311 从 EMD 服务器（A）4-1 下载的音乐内容和由再现应用（B）312 从 EMD 服务器（B）4-2 下载的音乐内容可以被发送到综合管理单元（X）315 使得例如仅由音乐提供公司 A 提供的艺术家的音乐内容可以被发送到便携式设备（X）6-3。即，因为本音乐内容发送系统将音乐内容的加密系统、使用条件信息的格式和音乐内容的压缩系统转换成统一传输协议，所以存储在个人计算机 1 中的硬盘上的不定的系统的音乐内容可以由综合管理单元（X）315 或便携式设备（X）6-3 再现。特别地，因为音乐内容发送系统在发送时转换加密系统和使用条件信息，所以在确保音乐内容的版权保护的同时提高了处理音乐内容的自由度。

即，在音乐内容发送系统中，至少加密系统和使用条件信息在适用于再现或控制音乐内容的再现应用之间被转换以发送音乐内容和使用条件信息。通过这样做，即使存在多个再现应用，音乐内容发送系统仍能够移动存储在例如个人计算机 1 的硬盘 21 中的音乐内容，并因此能够进行该音乐内容的统一管理。而且，因为使用条件信息和音乐内容一起被发送，这就不存在使用条件覆盖唯一的音乐内容的危险从而保证音乐内容的保护更可靠。

（3）使用条件信息

(说明通常使用的使用条件信息)

现在将说明在再现应用（A）311 中使用的使用条件信息的典型的格式。

在再现应用（A）311 中，使用例如在图 9a 中的表格形式表示的使用条件信息。

在列方向中，表格的左和右边的列分别说明了使用条件的原则和该原则的特定值。例如，可能的重播日期（从）、重播截止日期（至）或每次重播的花费（支付/播放）被作为原则加以说明。如图 9B 所示，作为附加于每一音乐

内容上的信息，使用条件信息被从 EMD 服务器（A）4-1 发送。再现应用（A）311 根据所说明的原则和相应的值来控制音乐内容。例如，假设可能的重播日期（从）是 1999 年 10 月 25 日，重播截止日期（至）是 1999 年 11 月 24 日，以及每次重播的花费（支付/播放）是：是/10 日元。在这种情况下，可以从 1999 年 10 月 25 日再现音乐内容，即使用户发出重播的命令，仍禁止在该日期之前的再现。该音乐内容可以在 1999 年 11 月 24 日之前被再现，在该日期之后该音乐内容将被删除。也对音乐内容进行设置使得每次重播估价为 10 日元。用户再现的次数作为将上传到 EMD 服务器（A）4-1 的单独的登录信息被存储以对收听或观看的用户对应于该音乐内容被收听或观看的次数的总数进行估价。

（对综合管理单元（X）315 使用的使用条件信息的说明）

现在说明综合管理单元（X）315 使用的使用条件信息。现在说明的使用条件信息是附加在从 EMD 服务器（X）4-3 下载的音乐内容上的，并在综合管理单元（X）315 管理音乐内容的控制时使用。而且，当在再现应用（A）311 和综合管理单元（X）315 之间以及再现应用（B）312 和综合管理单元（X）315 之间相互发送音乐内容时使用条件信息以统一的格式被使用。以下该使用条件信息被称为统一使用条件信息。

如图 4 所示，统一使用条件信息由索引文件 331、自动机文件 332、参数文件 333 和滞后文件 334 组成。这些文件是以 XML（可扩展标记语言）语言说明的。

在索引文件 331 中例如每一文件的参考信息被说明。

如图 11 所示，自动机文件 332 附加有：由自动机说明使用条件的自动机说明部分 341；内容密钥的鉴定代码（MAC；消息鉴定代码）342；内容提供者的签名（Sig）343；以及用于确认签名的认证（Cer）344。内容密钥用 KC 表示，而准备内容的内容提供者的专用密钥和公共密钥分别用 K^{-1}_E 和 K^{1}_E 表示。

自动机说明部分 341 使用在元组序列中的扩展状态机器描述音乐内容的操作状态。

利用当前音乐内容的操作状态的集 Q 和利用代表音乐内容的事件的输入符号的集 Σ，自动说明部分 341 表示下面跟随状态变换的音乐内容的操作状态的集 Q'：

$$Q' = \{d \mid d = \delta(q, \alpha) \mid qQ, \quad \alpha Q, \quad \delta: Q \times \Sigma \rightarrow Q\}$$

如上式所示，操作状态的集Q被表示为d。d由具有变量q、α的函数δ定义。q指示着音乐内容的操作状态的集Q的一个操作状态。α指示着事件集Σ的一个事件。函数δ是Q和Σ的幂集对Q的映射。

根据上述的Q、Σ和Q'，每一个元组由

{< q，α，d>|q，d∈Q，α∈Σ}

表示。注意：< q，α，d>指示着q、α、d的排列组合的一个例子。

在Σ中，诸如重播（play）、复制（copy）、总量（pay Y）、可能的播放开始日期和时间（from YMD）、播放结束日期和时间（to YMD）、可使用的天数的数目（in Ddays）、或无效事件（ε）的事件说明如下：

Σ=（Play，copy，pay Y，from YMD，to YMD，in Ddays，ε）

这样，在自动机描述器341中将进行下面的描述。

此后将说明在自动机描述器341中的具体的描述。

在图13中示出代表在图12中所示的音乐内容的操作变换的使用自动机的元组-行的说明性的描述。

该自动机执行如现在所描述的状态变换。

首先，产生从初始状态q0至状态q1及至状态q5的变换。从状态q1至状态q5，并行移动出现。

如果诸如10日元（pay 10）的预设置总量的支付事件出现在状态q1，则出现至状态q2的变换。如果播放事件（play）出现在状态q2，则产生至状态q1的变换。即，当前的自动机指示如果支付了10日元，仅可以再现一次音乐内容。如果诸如1000日元（pay 1000）的预设置总量的支付事件出现在状态q1，则再次产生至状态q3的变换。具体地说，该总量指示如果支付了100日元，可以再现音乐内容而与再现次数无关。如果出现对应于一次再现的n倍的再现总量的总量中的事件，诸如10日元（pay 10×n）出现，则产生至状态q4的变换。如果在至状态q4的变换之后，出现播放事件（play），则再次产生至该状态q4的变换。如果n个播放事件出现在该状态q4中，则产生至状态q1的变换。即，在这个自动机中，表明了如果支付了10×n日元，则音乐内容可以被再现n次。

如果诸如100日元的预设置总量的支付事件出现在状态q5，则产生至状态q6的变换。如果在状态q6中出现复制事件，则产生至状态q5的变换。如果在状态q6中出现复制事件，则产生至状态q8的变换。如果在状态q8中出

现播放事件，则再次产生至状态 q8 的变换。如果在状态 q8 中出现复制事件，则产生至状态 q9 的变换。该状态 q9 是最终状态，在状态 q9 中不出现至其他状态的变换并且没有事件出现。即，该总量表明如果支付了 100 日元，音乐内容可以被复制到其他设备一次。而且，该总量还表明了尽管复制的音乐内容可以被再现任何所需的次数，如果一旦如果音乐内容被复制到另一个设备，则不能被再现。

如果诸如 2000 日元（pay 2000）的预设置总量的支付事件出现在状态 q5，则产生至状态 q7 的变换。如果在状态 q7 中出现复制事件，则再次产生至状态 q7 的变换。如果在状态 q7 中出现复制事件，则产生至状态 q8 的变换。如果在状态 q8 中出现播放事件，则再次产生至状态 q8 的变换。如果在状态 q8 中出现复制事件，则产生至状态 q9 的变换。该状态 q9 是最终状态，在状态 q9 中不出现至其他状态的变换并且没有事件出现。即，该总量表说明了如果支付了 2000 日元，音乐内容可以不限次数被复制到其他设备。而且，该总量还表明尽管复制的音乐内容可以被再现任何所需的次数，一旦如果音乐内容被复制到另一个装置，则不能被再现。

图 13 示出了执行上述状态变换的自动机的元组行说明。

为了更新音乐内容的移动，自动机说明部分 341 可以说明操作状态的并行合成。例如，操作 a_0 和 a_1 的并行合成可以由下列的元组序列表示:

$<q_0, \alpha, a_0, q_0>$

$<q_0, \alpha, a_1, q_0>$

在自动机说明部分 341 中还可以说明伴随状态变换的行为（action）。例如，该行为由下列的元组表示:

$<q_0, \alpha, q_1,$ action$>$

该行为被表示为使用预定义的变量的函数。该变量由 ID、范围和初始值组成。例如，使用表示碟（a）的购买价格的变量 n，说明就是 a.n: =1000。下面示出了说明根据该变量的行为的自动机说明部分 341 的例子。

$< q_0,$ pay 100, $q_1,$ a.n:=a.n−100$>$ ...(1)

$< q_0,$ pay (a.n), $q_1,$ a.n:=0$>$ ...(2)

$< q_1,$ play, $q_2 >$ ...(3)

该例子指示着单个音乐内容（式（1））的购买价格影响着碟购买（式（2））的价格。

如图 14 所示，上述的自动说明部分 341 是由实体 ID 345、内容 ID346、版本信息 347、变量信息 348 和元组序列 349 组成。

下面将描述已经定义了描述格式的自动机说明部分 341 的具体的例子。

同时，下面使用的作为自动机描述的事件和命令由根据 XML 标准规定的 DTD（文档类型定义）定义。例如，再现（play），复制（copy）、播放支付（pay-for-play）、复制支付（pay-for-copy）、整碟播放支付（pay-for-album-play）、整碟复制的支付（pay-for-album-copy）、能够使用开始日期（from）、使用结束日期（to）、无效操作（null）由 DTD 设置作为事件。

图 16 示出了用 XML 语言定义的指示着音乐内容可以从 1999 年 9 月 1 日开始被再现的的自动机说明部分 341 的示例性的描述。

图 16 中所示的描述是图 17 所示的自动机。该自动机由作为初始状态的状态 q1 和状态 q2 构成。当日期变成状态 q1 中的能够使用开始日期（from）1999 年 9 月 1 日时，状态移动到状态 q2。当在状态 q2 中产生再现事件（play）时，音乐内容被再现，并且状态再次移动到状态 q2。用这种方式，自动机控制以使从 1999 年 9 月 1 日开始能够再现音乐内容。

图 18 示出了由 XML 语言定义的指示着音乐内容可以直到 1999 年 10 月 31 日被再现的自动机说明部分 341 的示例性的描述。

图 18 中的描述是图 19 所示的自动机。该自动机由作为初始状态的状态 q1 和作为结束状态的状态 end 构成。当在状态 q2 中产生再现事件（play）时，音乐内容被再现，并且状态再次移动到状态 q2。当日期变成状态 q2 中的使用结束日期（to）1999 年 10 月 31 日时，状态移动到状态 end。在状态 end 中，状态不移动到任何状态或不产生任何事件。以这种方式，自动机控制再现音乐内容直到 1999 年 10 月 31 日为止。

图 20 示出了由 XML 语言定义的自动机说明部分 341 的示例性的描述，指示音乐内容的能够再现的时间为从 1999 年 9 月 1 日至 1999 年 10 月 31 日，能够再现的次数是 16。

图 20 中的描述是图 21 所示的自动机。该自动机由作为初始状态的状态 q1、状态 q2 和作为结束状态的状态 end 构成。当日期变成状态 q1 中的能够使用开始日期（from）1999 年 9 月 1 日时，状态移动到状态 q2。当在状态 q2 中产生再现事件（play）时，音乐内容被再现，并且状态再次移动到状态 q2。当日期变成状态 q2 中的使用结束日期（to）1999 年 10 月 31 日或者再现事

件产生了 16 次时，状态移动到状态 end。在状态 end 中，状态不移动到任何状态或不产生任何事件。以这种方式，自动机控制确定再现音乐内容的时间是从 1999 年 9 月 1 日至 1999 年 10 月 31 日，并确定再现的次数是 16 次。

图 22 示出了由 XML 语言定义的指示着音乐内容的再现的次数限制为 16 的自动机说明部分 341 的示例性的描述。

参数文件 333 附加有参数说明部分 351、内容密钥的鉴定代码 352、内容提供者的签名 353、以及用于确认签名的鉴定文书 354，如图 23 所示。内容密钥用 KC 表示，同时准备内容的内容提供者的专用密钥和公共密钥分别用 K^{-1}_E 和 K^{1}_E 表示。

参数文件 333 可以由例如诸如内容零售商的第二提供者或者中间内容发送者的内容提供者而不是准备自动机文件 332 的内容提供者来重新编写。这样重新编写的参数文件 333 被附加一个与提供者或中间发送者相一致的独特的实体 ID355。同时，K'_C 是第二提供者的内容密钥，$K'_C=H(K_C$，实体 ID)。第二提供者的内容密钥 K'_C 从第一提供者的内容密钥 K_C 中得来的。第一和第二提供者通过鉴定文书彼此区分。

如果已经掌有了内容密钥，则由 MAC 确认参数文件 333。如果由于安全的原因没有提供内容密钥，则由签名和证明文件(instrument)确认参数文件 333。

使用第一和第二内容提供者 S 和 A，以及使用终端 B，由 MAC 确认的协议如下。S→A 指示着从 S 至 A 的发送，S→B 指示着从 S 至 B 的发送，以及 A→B 指示着从 A 至 B 的发送。ID_A 指示着设备 A 的 ID。

S→A: $K'_C = H\ (K_C,\ ID_A)$

S→B: $X=E_{KC}\ (K_C)$ 1

A→B: ID_A, Parameters, M=MAC K'_C (Parameters)

B: M≡ $MAC'_{K\ C}$ (Parameters)?

参数说明部分 351 说明了用于改变在自动文件 332 的自动机说明部分 341 中说明的值的函数的系数。例如，在图 13 中所示的例子中，存在着这样的情况，其中音乐内容的价格变成函数，如下所示:

$< q_0,\ pay(f_1(10)),\ q_1) >$

$< q_1,\ pay(f_2(10) \times n),\ q_2) >$

在该情况中，上述的函数 f_1 和 f_2 例如被定义如下:

$f_1(n)=0.9n$

$f_2(n)=90+0.1n$

通过如上定义函数，第一提供者能够设置默认价格值以及第二提供者能够重写参数文件 333 以改变该价格。

上述的参数说明部分 351 由实体 ID356、内容 ID357 和系数信息 358 组成，如图 25 所示。

滞后文件 334 是用于说明在自动机说明部分 341 中根据描述内容操作的音乐内容的操作的轨迹（trajectory）的文件。在自动机说明部分 341 的元组中的状态和变量被记录。例如，在图 13 中的例子中再现被执行两次。

图 13，

$<q_0, q_1, q_0, q_1>$

结果，得到下面操作的轨迹。

<pay10, play, pay10, play>

如果这在例如综合管理单元（X）315 中被相加并上传，则用户能够计算可支付的总量。

在使用了表示自动机的使用条件的统一使用条件信息的音乐内容发送系统 1 中，可以增加内容使用条件的描述的自由度，在该自动机中原则自身和其具体值被编程。

（4）被破坏的音乐内容的再存储和再下载

现在将说明综合管理单元（X）315 进行的音乐内容的备份。

首先，通过参考图 26 来说明综合管理单元（X）315 的主要管理方法。

综合管理单元（X）315 在个人计算机 1 中的硬盘 21 中存储音乐内容 C1、C2、C3...Cn。综合管理单元（X）315 还分别存储与音乐内容 C1、C2、C3...Cn 相关的内容密钥 Kc1、Kc2、Kc3、...、Kcn。内容密钥 Kc 是和音乐内容 C 一对一对应的。内容 ID 附加到音乐内容 C1、C2、C3...Cn 以用于识别。这些内容 ID 记为 CID1、CID2、CID3、...CIDn。

音乐内容 C1、C2、C3...Cn 由内容密钥 Kc1、Kc2、Kc3...Kcn 加密，并且，在此状态下，被记录在个人计算机 1 的硬盘 21 中。E（K，C）表示内容 C 已经使用密钥 K 加密。通常，内容 ID 被记录在音乐内容 C 的头部并和音乐内容一起被加密，或者 MAC 附加在音乐内容 C 上，使得内容 ID 与音乐内容的主体部分不可分离。

内容密钥 Kc1、Kc2、Kc3...Kcn 被存储密钥 KS 加密并以状态 E(SK,Kc1)、E(SK, Kc2)、E(SK, Kc3)...E(SK, Kcn)被记录在个人计算机 1 的硬盘 21。这个存储密钥 KS 展示了所谓的抗短波长并被保存在一般用户不能参考的记录区中。

如果在执行上述的密钥管理的综合管理单元(X)315 中，例如音乐内容 C1 将被再现，则使用存储密钥 KS 解密内容密钥 Kc1，并随后使用内容密钥 Kc1 解密音乐内容 C1。以这种方式，综合管理单元(X)315 能够再现音乐内容 C1。

如果在执行上述的密钥管理的综合管理单元(X)315 中，例如音乐内容 C1 将被从硬盘 21 移到便携式设备(X)6-3，则使用便携式设备(X)6-3 执行相互鉴定。完成鉴定后，内容密钥 Kc1 被对话密钥解密并且加密的内容密钥 Kc1 和加密的音乐内容 C1 一起被发送到便携式设备(X)6-3。加密的内容密钥 Kc1 和加密的音乐内容 C1 二者都被发送到便携式设备(X)6-3。内容密钥 Kc1 和音乐内容 C1 二者都被从硬盘 21 中删除。通过这样做，综合管理单元(X)315 能够将音乐内容移到便携式设备(X)6-3 中。

下面将说明由于例如硬盘 21 损坏时，音乐内容或内容密钥停止从硬盘 21 中再现时，所必须的音乐内容的再生的方法。

通常，综合管理单元(X)315 在硬盘 21 中存储加密的音乐内容 C 和内容密钥 Kc 的备份数据。

而且，通常，综合管理单元(X)315 使用登录信息监督从 EMD 服务器(X)4-3 下载的音乐内容的购买记录以及在硬盘 21 中存储的音乐内容的全部的内容 ID 的清单。在当音乐内容被从 EMD 服务器(X)4-3 中下载或被移动到便携式设备(X)6-3 中时，在控制音乐内容的同时该登录信息被更新。综合管理单元(X)315 周期地或在访问之后上载登录信息到 EMD 服务器(X)4-3。

如果存储在综合管理单元(X)315 的硬盘 21 中的音乐内容 C 或内容密钥 Kc 被破坏，将执行下面的处理。

如果音乐内容 C 或内容密钥 Kc 被破坏，综合管理单元(X)315 首先访问 EMD 服务器(X)4-3 以执行用户鉴定。

EMD 服务器(X)4-3 接着从授权的用户的用户 ID 中参考综合管理单元(X)315 的使用登录信息，以产生完整性校验值(ICV)。根据作为在使用登录信息中说明的音乐内容 C 的内容 ID 的 CID 和综合管理单元(X)315 的存储密

钥 KS，并根据

ICV=H（SK，CID1||CID2||...||CIDn）

产生该 ICV。

其中 H（K，Data）是单方向的散列函数并且其值随密钥 K 改变。

EMD 服务器（X）4-3 接着发送所产生的完整性校验值 ICV 到综合管理单元（X）315。

如果音乐内容 C 或内容密钥 Kc 被备份，则综合管理单元（X）315 重新恢复备份数据以在硬盘 21 中保存音乐内容 C 或内容密钥 Kc。如果音乐内容 C 或内容密钥 Kc 被备份，则破坏的音乐内容 C 或内容密钥 Kc 将被从 EMD 服务器（X）4-3 中重新发送。此时，如果内容已经被购买，则 EMD 服务器（X）4-3 参考用户的购买滞后，并不再估价。

综合管理单元（X）315 执行上面的处理以便重新建立损坏的音乐内容 C 或内容密钥 Kc。

如果重新生成的音乐内容 C 或内容密钥 Kc 将被再现或控制时，综合管理单元（X）315 使用完整性校验值 ICV 检查音乐内容的 CID。通过使用完整性校验值 ICV 检查重新建立的音乐内容 C 或内容密钥 Kc，在音乐内容 Ci 被移动到便携式设备（X）6-3 中并从硬盘 21 中被删除的情况下，将 E（Kci，Ci）存储为加密的音乐内容 Ci 并再存储音乐内容的恶意用户，是不能够通过控制方式再现或移动数据的。

如果不是音乐内容 C 或内容密钥 Kc 而是存储密钥 KS 已经被破坏，则综合管理单元（X）315 被重新安装。即使在这种情况下，如果在 EMD 服务器（X）4-3 中进行了用户注册并且登录信息被上载，重新存储和重新下载仍是可行的。

如上所述，在音乐内容发送系统 1 中，即使音乐内容由于硬盘压碎已经被破坏，受版权的保护，该音乐内容仍能被重新建立。例如，如果音乐内容已经正确地购买了，则它就可以免费地重新建立。

（5）分配综合管理单元（X）的主密钥和鉴定密钥的方法

在综合管理单元（X）315 和便携式设备（X）6-3 之间，通过使用 ID 和适用于便携式设备（X）6-3 的鉴定密钥（MG-ID/IK）以及适用于综合管理单元（X）315 的主密钥（OMG-MK）进行相互鉴定。

如果在综合管理单元（X）315 和便携式设备（X）6-3 之间已经进行了相

互鉴定，对于综合管理单元（X）315 来说，从综合管理单元（X）315 将音乐内容发送到便携式设备（X）6-3 或者将音乐内容从便携式设备（X）6-3 返回到综合管理单元（X）315 就变得成为可能。同时，综合管理单元（X）315 拥有透视图 3 中的硬盘 21 中的加密的音乐内容，同时便携式设备（X）6-3 拥有在诸如存储卡的内部记录介质中的加密音乐内容。如果从综合管理单元(X) 315 将音乐内容发送到便携式设备（X）6-3，则在个人计算机 1 上的硬盘 21 中的音乐内容被发送到便携式设备 10 上装载的存储卡上。另一方面，如果将音乐内容从便携式设备（X）6-3 发送到综合管理单元（X）315，则在便携式设备（X）6-3 上装载的存储卡上的音乐内容被发送到在个人计算机 1 上的硬盘 21。

便携式设备（X）6-3 一开始拥有 ID 信息（MG-ID）、用于多个生成（generation）的鉴定密钥（MG-IK）以及用于多个生成的主密钥（OMG-MK）。外部不提供便携式设备（X）6-3 这些密钥或信息。便携式设备（X）6-3 更新鉴定密钥（MG-IK）和主密钥（OMG-MK）的生成。便携式设备（X）6-3 不是通过旧生成的鉴定密钥或主密钥而是新生成的鉴定密钥或主密钥来实现相互鉴定。下面假设便携式设备（X）6-3 正在拥有从第 0 次到第 100 次的 100 次生成的鉴定密钥（MG-ID）和主密钥（OMG-MK）。用于第 i 次生成的鉴定密钥表示为（MG-IK[i]）并且用于第 i 次生成的主密钥表示为（OMG-MK[i]）。

拥有主密钥（OMG-MK）的综合管理单元（X）315 能够将音乐内容从例如音频 CD 中发送到个人计算机 1 并保存在其中。另一方面，拥有主密钥(OMG-MK) 的综合管理单元（X）315 能够从 EMD 服务器（X）4-3 中将音乐内容下载以存储在个人计算机 1 中。

注意：在综合管理单元（X）315 中，能够从 CD 中发送音乐内容而不能从 EMD 服务器（X）4-3 中下载音乐内容的主密钥（OMG-MK），不同于既能够从 CD 中发送音乐内容又能从 EMD 服务器（X）4-3 中下载音乐内容的主密钥（OMG-MK）。下面，能够从 CD 中发送音乐内容而不能从 EMD 服务器（X）4-3 中下载音乐内容的密钥被称为专用于发送的密钥，并且既能够从 CD 中发送音乐内容又能从 EMD 服务器（X）4-3 中下载音乐内容的密钥被称为 EMD 密钥。

在本实施例中，用于第 0 次生成的主密钥（OMG-MK[0]）是专用于发送的密钥，而主密钥（OMG-MK[1 to 99]）是 EMD 密钥。

现在说明使用专用于发送的密钥进行处理的步骤。

如图 27 中所示，如果综合管理单元（X）315 欲从 CD-ROM 中安装，则例如便携式设备（X）6-3 和软盘 52 与已经在其中安装了综合管理单元（X）315 的安装软件的 CD-ROM51 作为一套被销售。在软盘 52 中存储有便携式设备(X) 6-3 的 ID 信息（MG-ID）、用于第 0 次生成的鉴定密钥（MG-IK[0]）和用于第 0 次生成的主密钥（OMG-MK[0]）。

为了使将使用的已售出的便携式设备（X）6-3 等能够使用，首先 CD-ROM 361 被载入到个人计算机 1 上（步骤 S11）。接着从 CD-ROM 361 安装综合管理单元（X）315 到个人计算机 1（步骤 S12）。接着，综合管理单元（X）315 被安装到个人计算机 1 的硬盘中（步骤 S13）。接着存储在软盘 362 中的便携式设备（X）6-3 的 ID 信息(MG-ID)以及用于第 0 次生成的鉴定密钥（MG-IK[0]）和用于第 0 次生成的主密钥（OMG-MK[0]）被保存在个人计算机 1 中（步骤 S14）。

这使由例如音乐 CD363 供给的音乐内容能够被存储在个人计算机 1 的硬盘中（步骤 S15）。同时，由于用于第 0 次生成的主密钥（OMG-MK[0]）是专用于发送的密钥，所以音乐内容不能从 EMD 服务器（X）4-3 中被下载。

便携式设备（X）6-3 拥有用于 100 次生成的鉴定密钥和主密钥以处理生成更新。在初始设置中，生成是第 0 次生成。所以，在拥有用于第 0 次生成的鉴定密钥和主密钥的综合管理单元（X）315 和便携式设备（X）6-3 之间的相互鉴定就变得可行。因此，可以将音乐 CD363 等供给的音乐内容存储在便携式设备（X）6-3 的存储卡中（步骤 S16）。

在另一方面，如果综合管理单元（X）315 通过网络被提供，则与综合管理单元（X）315 一起被提供的还有在因特网上的 EMD 注册服务器上的地址、用户 ID 和口令等。

如果所销售的便携式设备（X）6-3 等能够使用，则通过使用用户 ID 和口令访问在因特网上的 EMD 注册服务器 3（步骤 S21）。EMD 注册服务器 3 接着鉴定用户 ID 和口令（步骤 S22）。如果在鉴定中没有问题，则 EMD 注册服务器 3 将综合管理单元（X）315 的安装软件、便携式设备（X）6-3 的 ID 信息（MG-ID）、第 0 次生成的鉴定密钥（MG-IK[0]）和第 0 次生成的主密钥（OMG-MK[0]）发送给个人计算机 1（步骤 S23）。接着在将便携式设备（X）6-3 的 ID 信息（MG-ID）、第 0 次生成的鉴定密钥（MG-IK[0]）和第 0 次生成的主密钥（OMG-MK[0]）保存在硬盘 21 中的同时，个人计算机 1 引导综合管

理单元（X）315 的安装软件以安装综合管理单元（X）315（步骤 S24）。这就在硬盘中存储了综合管理单元（X）315（步骤 S25）。

这使由例如音乐 CD363 供给的综合管理单元（X）315 能够被存储在个人计算机 1 的硬盘中（步骤 S26）。同时，由于第 0 次生成的主密钥（OMG-MK[0]）是专用于发送的密钥，所以音乐内容不能从 EMD 服务器（X）4-3 中被下载。

便携式设备（X）6-3 拥有用于 100 次生成的鉴定密钥和主密钥以处理生成更新。在初始状态中，生成被设置成第 0 次生成。所以，可以进行在拥有第 0 次生成的鉴定密钥和主密钥的综合管理单元（X）315 和便携式设备（X）6-3 之间的相互鉴定。因此，能够将音乐 CD363 等供给的音乐内容存储在便携式设备（X）6-3D 的存储卡中。

除在图 27 和 28 中所示的方法外，这样的方法也可以被用在其中综合管理单元（X）315 和专用于发送的第 0 次生成的主密钥（OMG-MK[0]）存储在 CD-ROM 361 中，并且其中关于便携式设备（X）6-3 的鉴定 ID 和用于第 0 次生成的鉴定密钥（MG-ID/IK）被通过网络提供。

下面将说明用于更新专用于发送的密钥为能够处理从 EMD 服务器(X)4-3 下载的音乐内容的 EMD 密钥的操作的顺序。

通过诸如 CD-ROM 的可移动介质或通过诸如因特网的网络，使用在图 27 和 28 中所示的操作顺序提供综合管理单元（X）315，并且综合管理单元（X）315 被安装在个人计算机 1 中的硬盘 21 中。此时，便携式设备（X）6-3 的密钥处于默认生成，综合管理单元（X）315 正拥有专用于发送的第 0 次生成的主密钥（OMG-MK[0]）和第 0 次生成的鉴定密钥（MG-ID/IK）

首先，个人计算机 1 使用用户 ID 和口令访问网络上的 EMD 注册服务器 3（步骤 S31），如图 29 所示。接着 EMD 注册服务器 3 鉴定用户 ID 和口令（步骤 S32）。如果在鉴定中没有问题，EMD 注册服务器 3 注册个人计算机 1 的 ID 信息（OMG-ID）用以生成综合管理单元（X）315 的打开密钥（OMG-PK）、秘密密钥（OMG-SK）和打开密钥的鉴定文书（Cer[PK]）以连接到 EMD 服务器（X）4-3（步骤 S33）。EMD 注册服务器 3 接着将产生的打开密钥（OMG-PK）、秘密密钥（OMG-SK）和打开密钥的鉴定文书（Cer[PK]）发送到个人计算机 1（步骤 S34）。

EMD 注册服务器 3 接着将便携式设备（X）6-3 的 ID 信息（MG-ID）、第 i 次生成的鉴定密钥（MG-IK[i]）和第 i 次生成的主密钥（OMG-IK[i]）发送到

个人计算机 1（步骤 S35）。EMD 注册服务器 3 接着根据所接收的 ID 信息（MG-ID）、第 i 次生成的鉴定密钥（MG-IK[i]）和第 i 次生成的主密钥（OMG-IK[i]）将接收到的密钥等更新到第 i 次生成（步骤 S36）。接着综合管理单元（X）315 执行便携式设备（X）6-3 的鉴定（步骤 S37）。在鉴定便携式设备（X）6-3 中，将所拥有的密钥的生成更新到第 i 次生成（步骤 S38）。

这使综合管理单元（X）315 能够存储由例如音乐 CD363 供给的将被存储的音乐内容至个人计算机 1 的硬盘 21 中以及存储从 EMD 服务器（X）4-3 下载的音乐内容至个人计算机 1 的硬盘 21 中（步骤 S39）。

下面说明例如 EMD 密钥的生成更新的操作顺序。

当便携式设备（X）6-3 的生成也是第 i 次生成时，综合管理单元（X）315 正拥有第 i 次生成的主密钥（OMG-MK[i]）、au 的 ID 和第 0 次生成的鉴定密钥（MG-IK[0]）。

首先，如图 30 所示，如果个人计算机 1 访问 EMD 注册服务器 3 以进行某些处理，则 EMD 注册服务器 3 鉴定综合管理单元（X）315 的 ID 以便将第（i+k）次生成的鉴定密钥（MG-IK[i+k]）和第（i+k）次生成的主密钥（OMG-IK[i+k]）发送给个人计算机 1（步骤 S41）。个人计算机 1 的综合管理单元（X）315 更新所接收的鉴定密钥和主密钥为第（i+k）次生成（步骤 S42）。综合管理单元（X）315 接着鉴定便携式设备（X）6-3（步骤 S43）。当鉴定后，便携式设备（X）6-3 更新所拥有的密钥的生成从第 i 次生成为第 i+k 次生成（步骤 S44）。

另一方面，如图 31 所示，如果便携式设备（X）6-3 使用的鉴定密钥等的生成是第（i+k）次生成，并且由综合管理单元（X）315 所拥有的鉴定密钥等的生成是第 i 次生成，则即使试图进行这样的鉴定，在便携式设备（X）6-3 和综合管理单元（X）315 之间的鉴定失败，（步骤 S51）。如果鉴定失败，则综合管理单元（X）315 向 EMD 注册服务器 3 请求一个密钥（步骤 S52）。如果有密钥请求，则 EMD 注册服务器 3 鉴定综合管理单元（X）315 的 ID 以便发送第（i+k）次生成的鉴定密钥（MG-IK[i+k]）和第（i+k）次生成的主密钥（OMG-MK[i+k]）（步骤 S53）。综合管理单元（X）315 接着更新所接收的鉴定密钥和主密钥到第（i+k）次生成（步骤 S54）。综合管理单元（X）315 接着鉴定便携式设备（X）6-3（步骤 S55）。

这使综合管理单元（X）315 能够存储由音乐 CD363 等供给的音乐内容至个人计算机 1 的硬盘 21 中以及存储从 EMD 服务器（X）4-3 下载的音乐内容

至个人计算机 1 的硬盘 21 中（步骤 S38）。

在上述音乐内容发送系统 1 中，综合管理单元（X）315 和便携式设备（X）6-3 使用的主密钥和鉴定密钥被分类为专用于发送的密钥和连接到服务器的密钥，并且连接到服务器的密钥被从网络上下载。结果就是：在音乐内容发送系统 1 中，改进了从服务器发送的音乐内容的安全性，这使得，即使专用于发送的密钥被破坏，从服务器下载的音乐内容不能被破坏。

在音乐内容发送系统 1 中，综合管理单元（X）315 和便携式设备（X）6-3 使用的主密钥和鉴定密钥被用于生成更新。而且，通过网络为综合管理单元（X）315 提供用于生成更新的主密钥和鉴定密钥，因此提高了音乐内容的安全性。

产业上的可应用性

根据本发明，数据处理装置基于从内容服务器重新获得的使用登录信息再现和/或控制重新存储和重新发送的备份内容数据。

因此，根据本发明，即使通过网络发送的内容数据一旦被损坏，在版权得到保证时，内容数据可以被恢复。

说　明　书　附　图

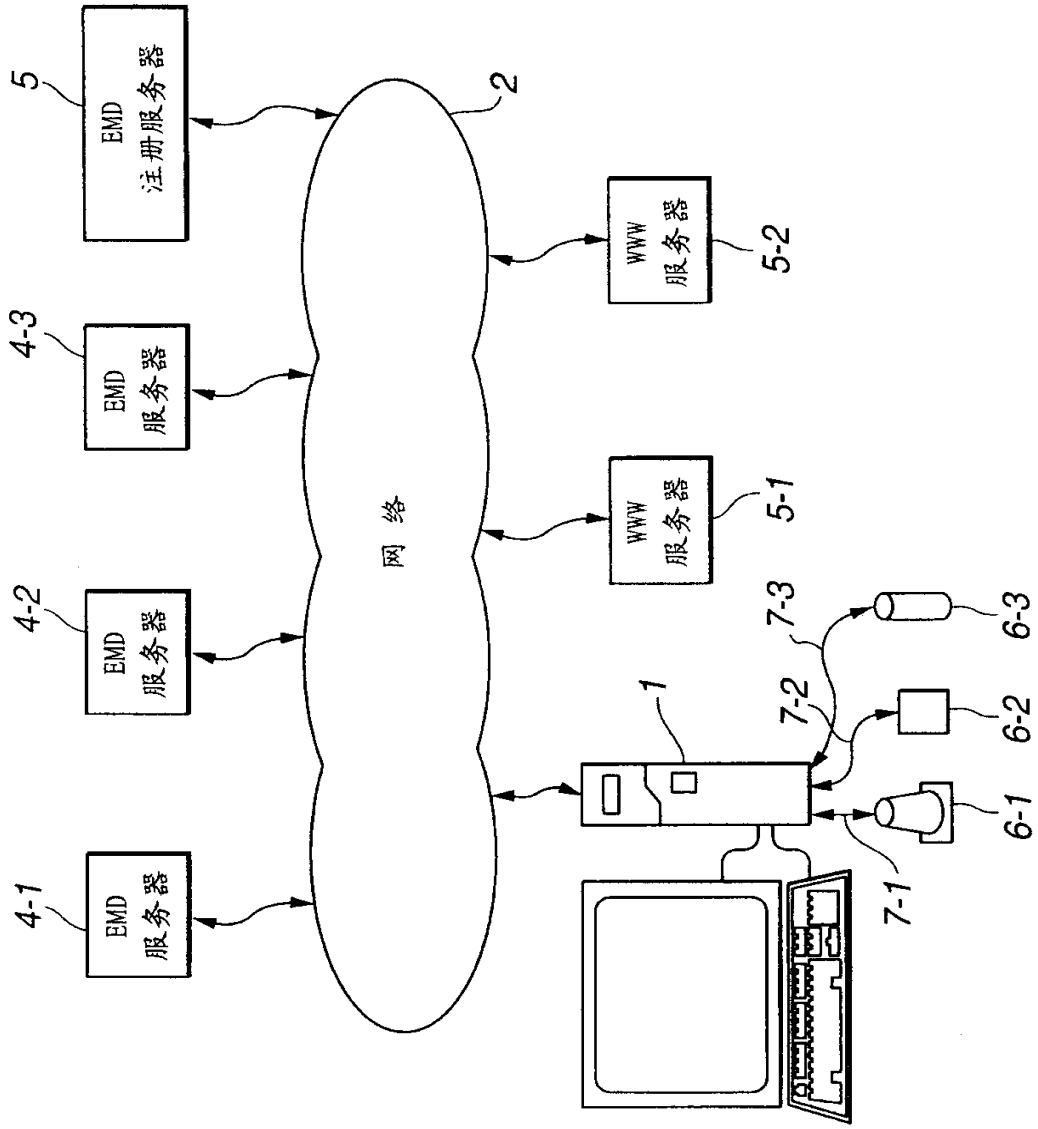

5
EMD
注册服务器
2
网络
WWW
服务器
5-2
4-3
EMD
服务器
WWW
服务器
5-1
4-2
EMD
服务器
7-3
6-3
1
7-2
6-2
4-1
EMD
服务器
6-1
7-1

图 1

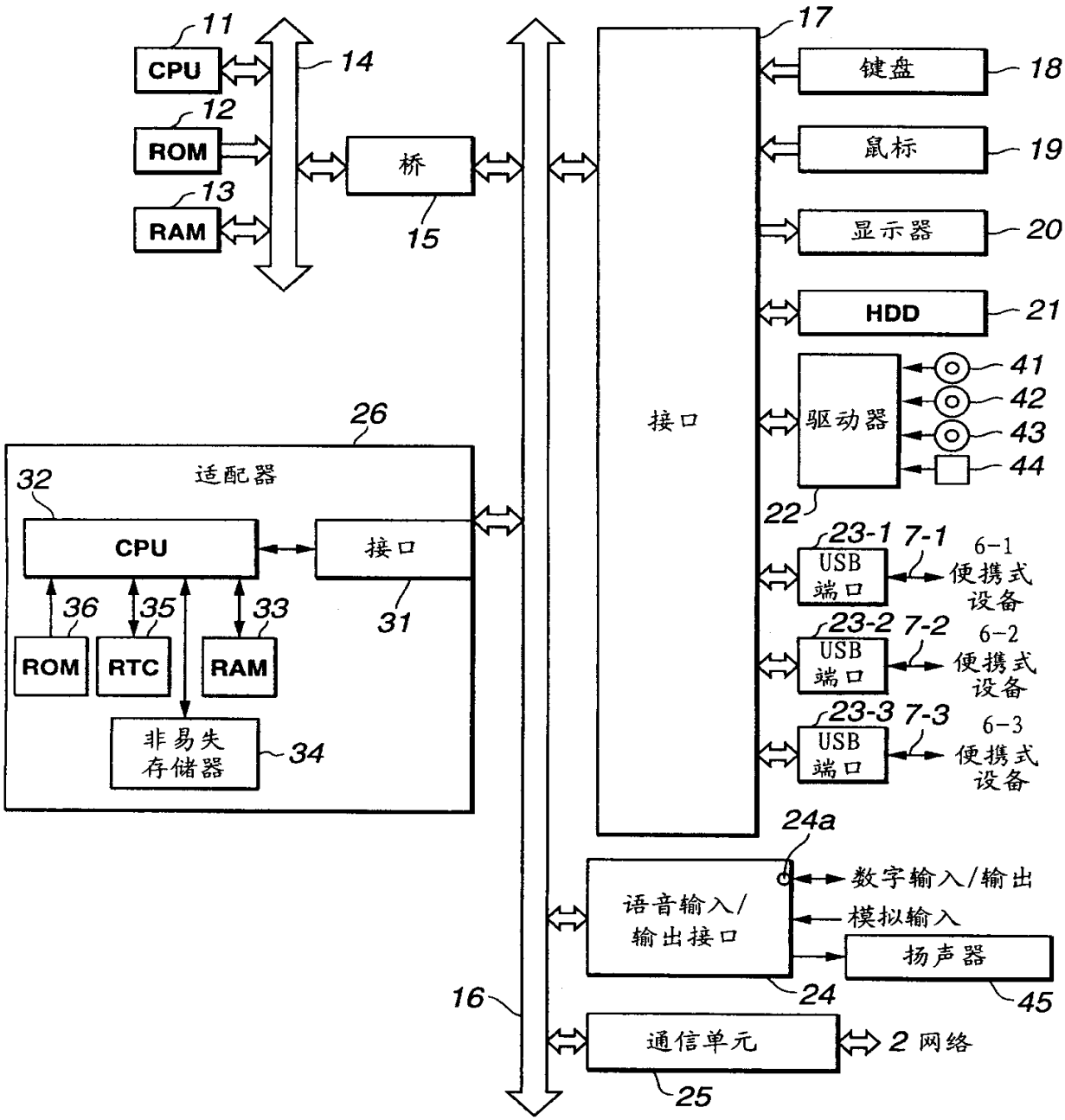

11
CPU
12
ROM
13
RAM
14
桥
15
16
17
接口
键盘
18
鼠标
19
显示器
20
HDD
21
驱动器
41
42
43
44
22
23-1 7-1
USB 端口
6-1
便携式设备
23-2 7-2
USB 端口
6-2
便携式设备
23-3 7-3
USB 端口
6-3
便携式设备
24a
数字输入/输出
模拟输入
语音输入/输出接口
24
扬声器
45
通信单元
2 网络
25
26
适配器
32
CPU
接口
31
36
35
33
ROM
RTC
RAM
非易失存储器
34

图 2

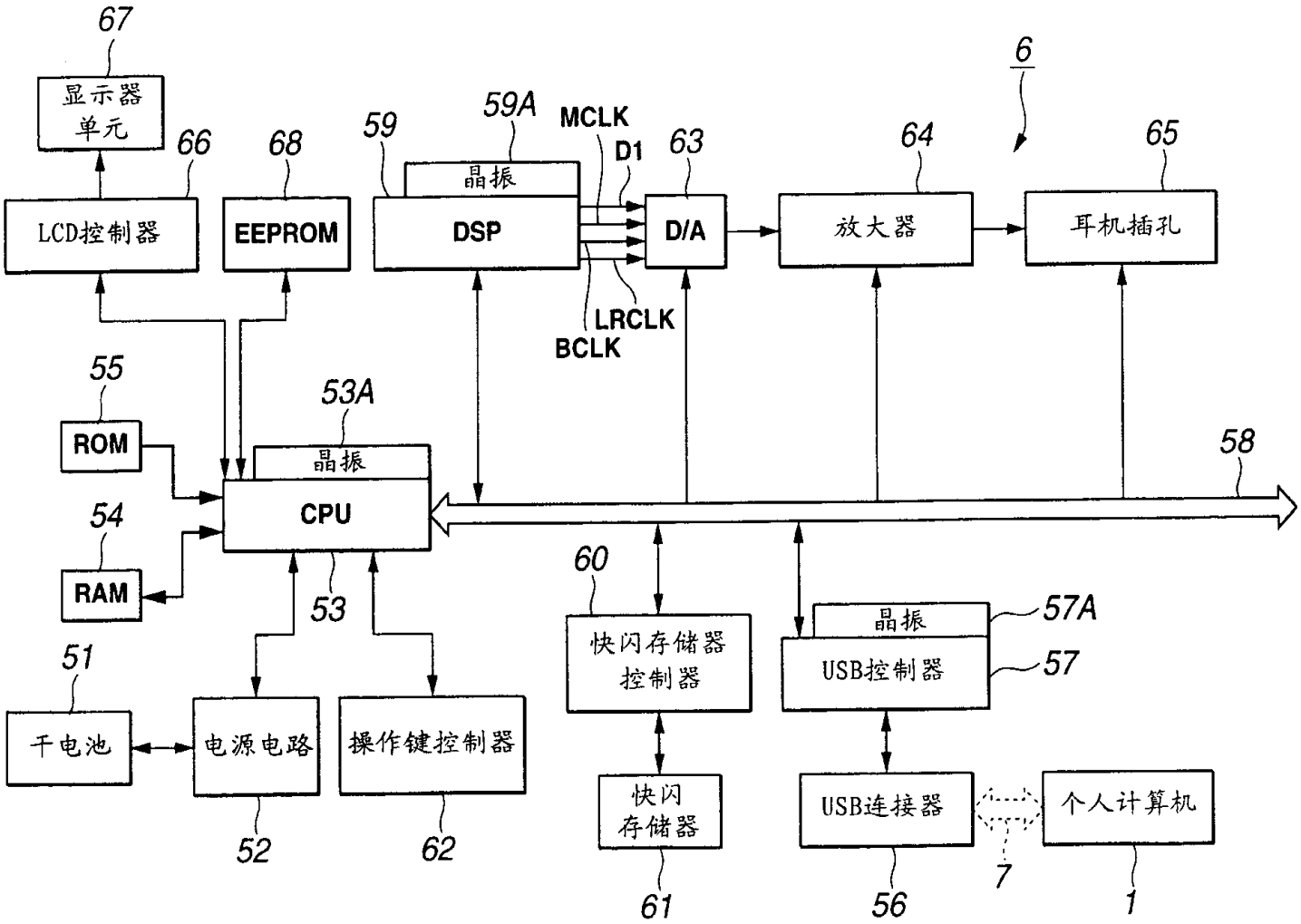

67
显示器
单元
66
LCD控制器
68
EEPROM
59
59A
晶振
DSP
MCLK
D1
63
D/A
64
放大器
6
65
耳机插孔
LRCLK
BCLK
55
ROM
53A
晶振
CPU
58
54
RAM
53
60
快闪存储器
控制器
晶振
57A
USB控制器
57
51
干电池
电源电路
操作键控制器
52
62
快闪
存储器
61
USB连接器
56
7
个人计算机
1

图 3

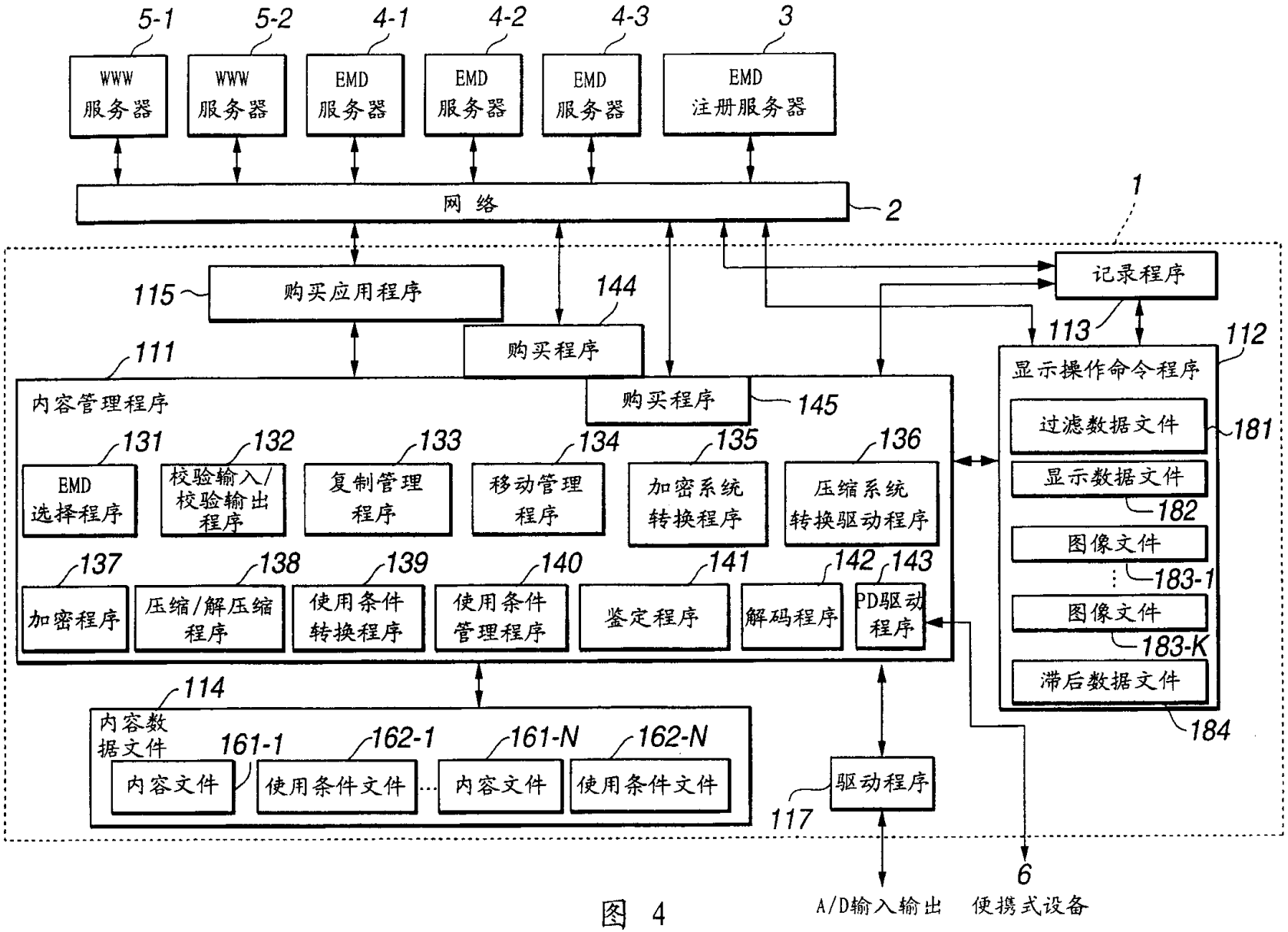

5-1
5-2
4-1
4-2
4-3
3
WWW 服务器
WWW 服务器
EMD 服务器
EMD 服务器
EMD 服务器
EMD 注册服务器
网 络
2
1
115
购买应用程序
144
购买程序
记录程序
113
112
111
显示操作命令程序
内容管理程序
购买程序
145
过滤数据文件
181
显示数据文件
182
131
132
133
134
135
136
EMD 选择程序
校验输入/校验输出程序
复制管理程序
移动管理程序
加密系统转换程序
压缩系统转换驱动程序
图像文件
183-1
137
138
139
140
141
142
143
加密程序
压缩/解压缩程序
使用条件转换程序
使用条件管理程序
鉴定程序
解码程序
PD驱动程序
图像文件
183-K
滞后数据文件
184
114
内容数据文件
161-1
162-1
161-N
162-N
内容文件
使用条件文件
内容文件
使用条件文件
驱动程序
117
6
A/D输入输出
便携式设备

图 4

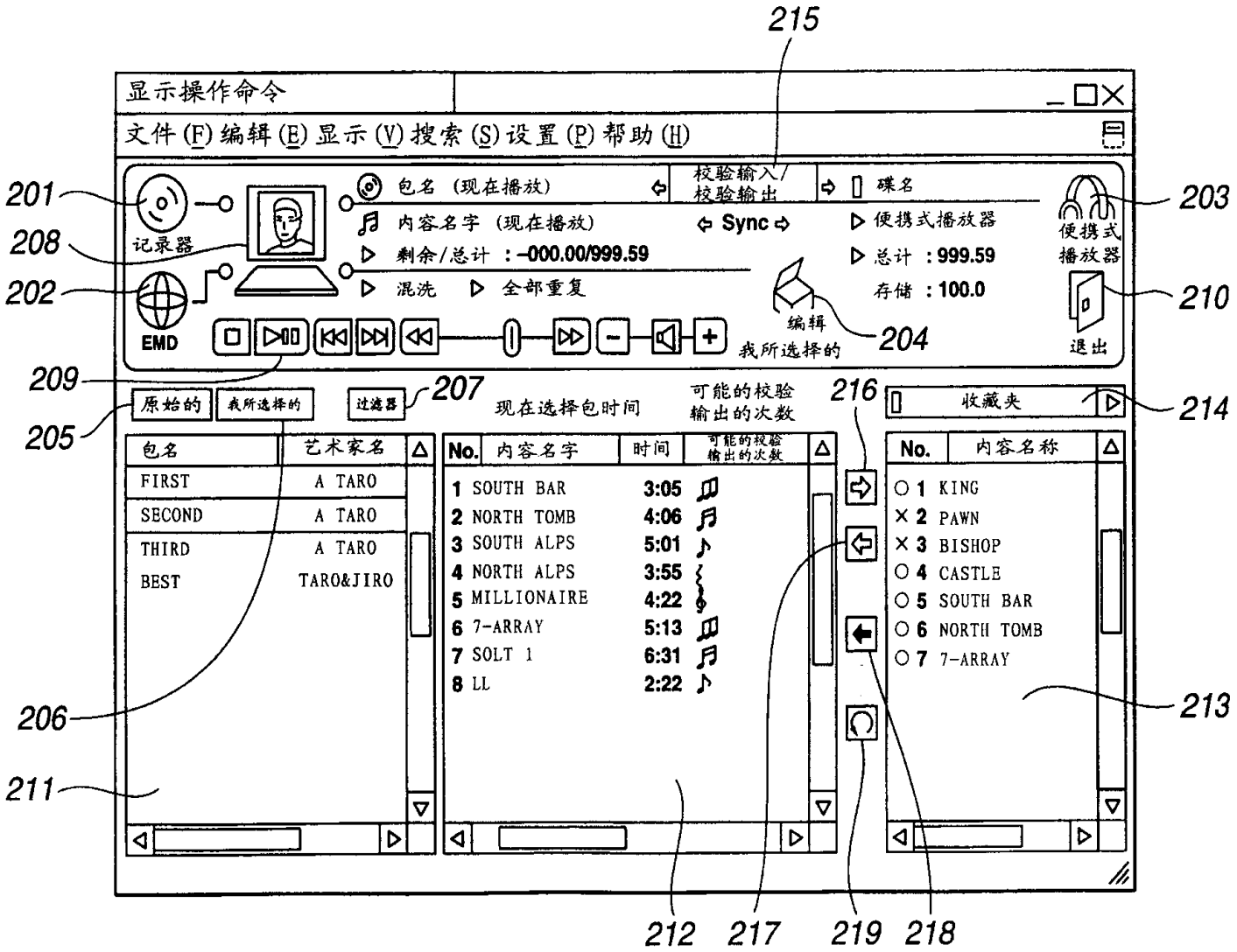

显示操作命令
文件(F) 编辑(E) 显示(V) 搜索(S) 设置(P) 帮助(H)
包名 (现在播放)
内容名字 (现在播放)
剩余/总计 : -000.00/999.59
混洗
全部重复
校验输入/
校验输出
Sync
碟名
便携式播放器
总计 : 999.59
存储 : 100.0
记录器
EMD
编辑
我所选择的
退出
原始的
我所选择的
过滤器
现在选择包时间
可能的校验
输出的次数
收藏夹
包名
艺术家名
FIRST A TARO
SECOND A TARO
THIRD A TARO
BEST TARO&JIRO
No.
内容名字
时间
1 SOUTH BAR 3:05
2 NORTH TOMB 4:06
3 SOUTH ALPS 5:01
4 NORTH ALPS 3:55
5 MILLIONAIRE 4:22
6 7-ARRAY 5:13
7 SOLT 1 6:31
8 LL 2:22
No.
内容名称
1 KING
2 PAWN
3 BISHOP
4 CASTLE
5 SOUTH BAR
6 NORTH TOMB
7 7-ARRAY
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219

图 5

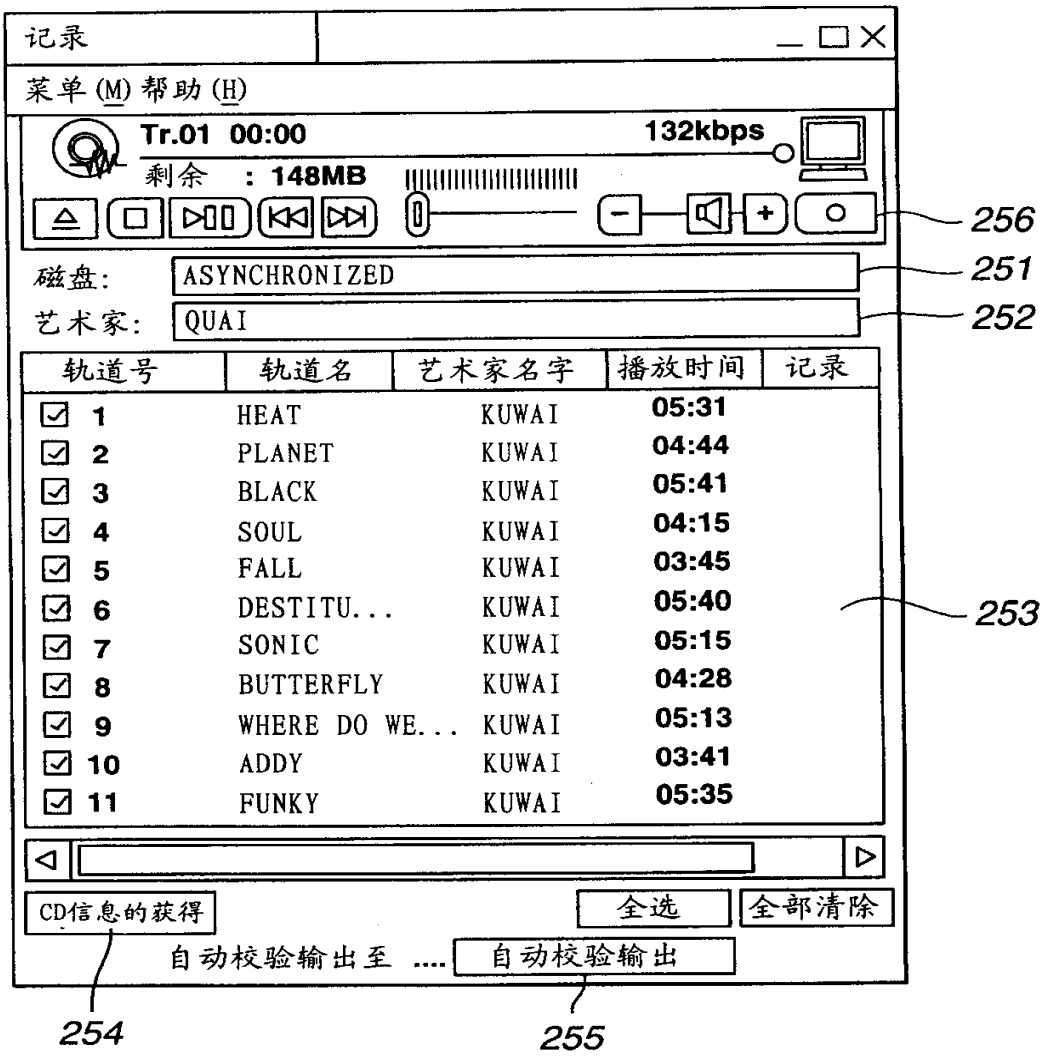

记录
菜单(M) 帮助(H)
Tr.01 00:00
132kbps
剩余 : 148MB
磁盘:
ASYNCHRONIZED
艺术家:
QUAI
轨道号
轨道名
艺术家名字
播放时间
记录
1 HEAT KUWAI 05:31
2 PLANET KUWAI 04:44
3 BLACK KUWAI 05:41
4 SOUL KUWAI 04:15
5 FALL KUWAI 03:45
6 DESTITU... KUWAI 05:40
7 SONIC KUWAI 05:15
8 BUTTERFLY KUWAI 04:28
9 WHERE DO WE... KUWAI 05:13
10 ADDY KUWAI 03:41
11 FUNKY KUWAI 05:35
CD信息的获得
全选
全部清除
自动校验输出至 ....
自动校验输出
256
251
252
253
254
255

图 6

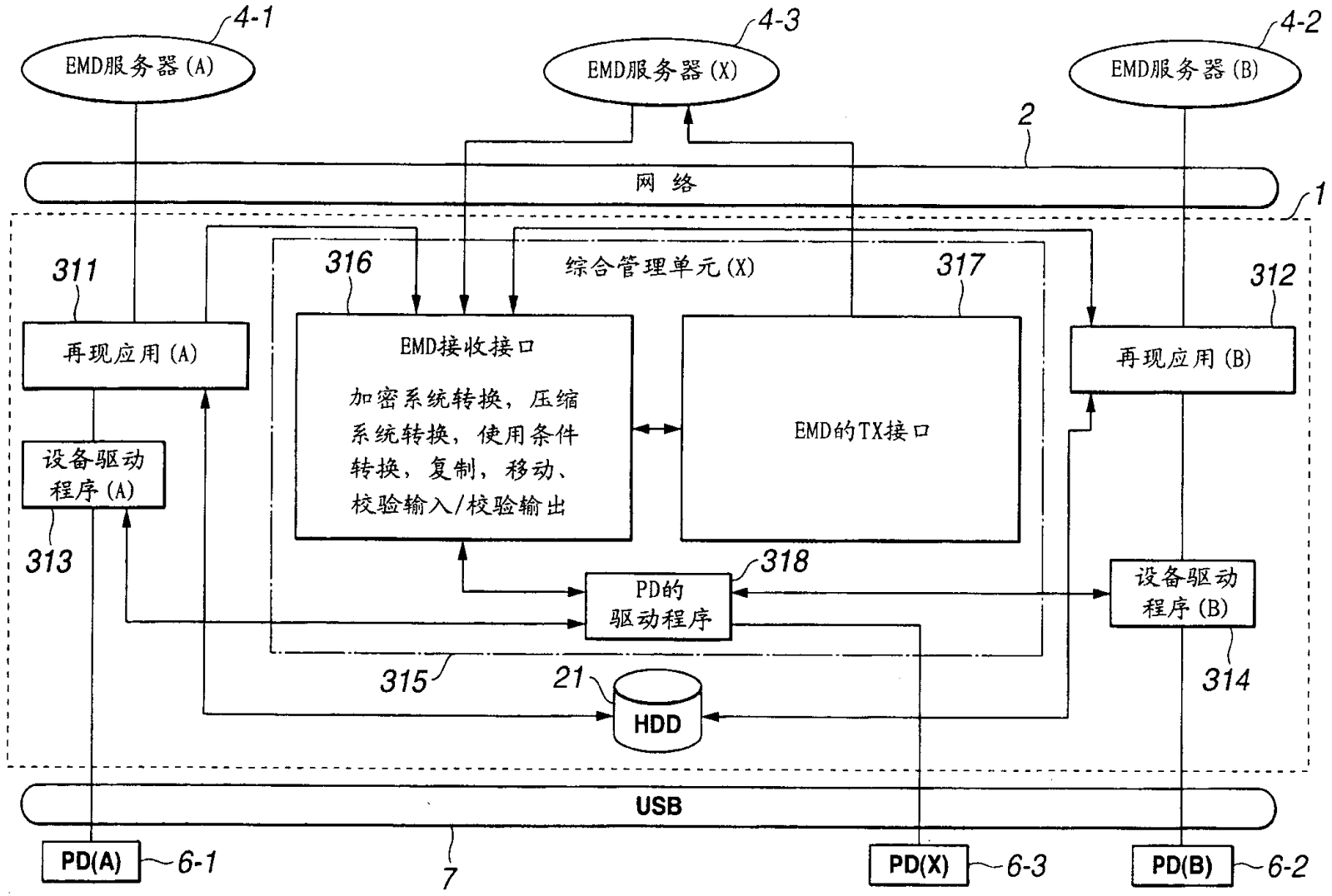

4-1
EMD服务器(A)
4-3
EMD服务器(X)
4-2
EMD服务器(B)
2
网 络
1
311
316
综合管理单元(X)
317
312
再现应用(A)
EMD接收接口
加密系统转换，压缩
系统转换，使用条件
转换，复制，移动、
校验输入/校验输出
EMD的TX接口
再现应用(B)
设备驱动
程序(A)
313
318
PD的
驱动程序
设备驱动
程序(B)
315
21
HDD
314
USB
PD(A)
6-1
7
PD(X)
6-3
PD(B)
6-2

图 7

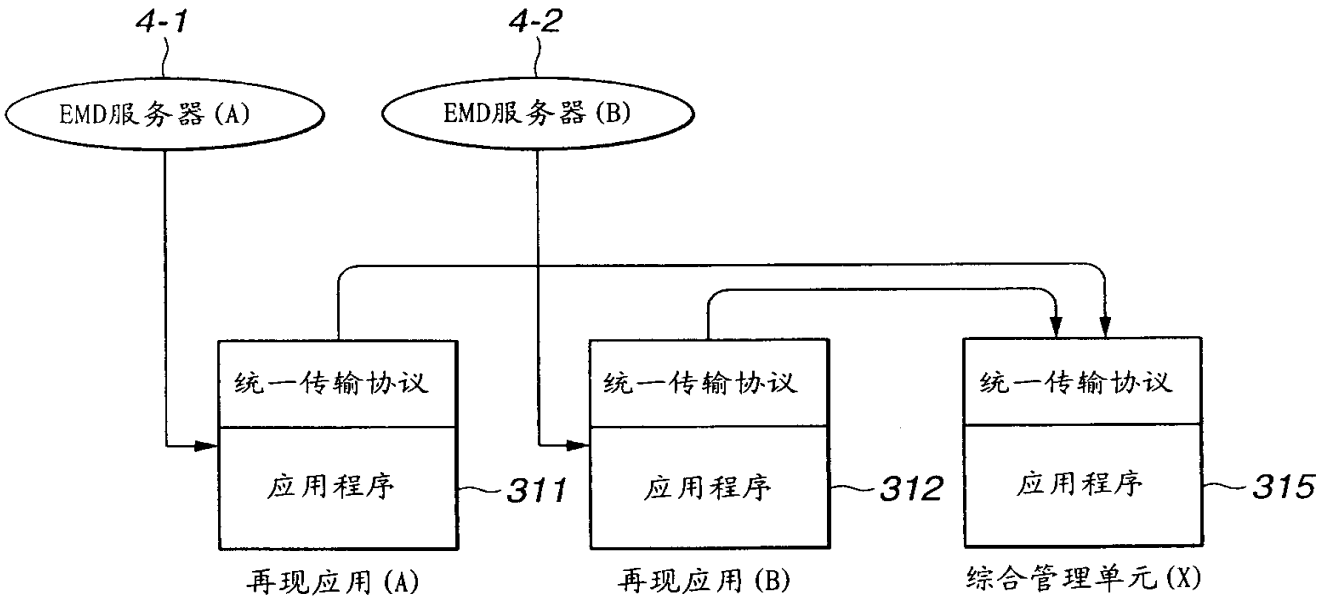

4-1
4-2
EMD服务器(A)
EMD服务器(B)
统一传输协议
应用程序
311
统一传输协议
应用程序
312
统一传输协议
应用程序
315
再现应用(A)
再现应用(B)
综合管理单元(X)

图 8

图 9A

原则	值
从	**99/10/25**
至	**99/11/24**
支付/播放	是/10日元

图 9B

内容
使用条件信息

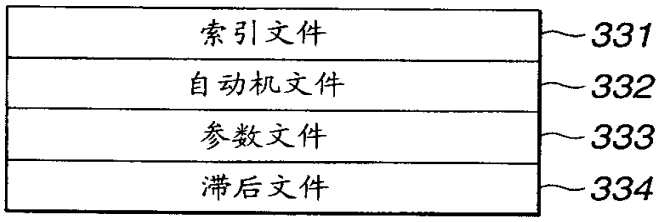


图 10

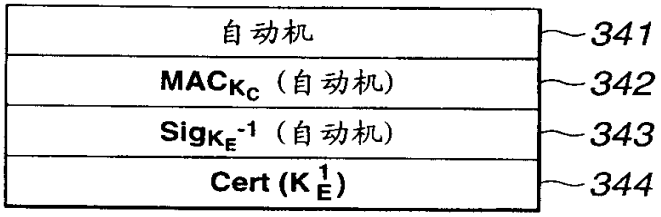


图 11

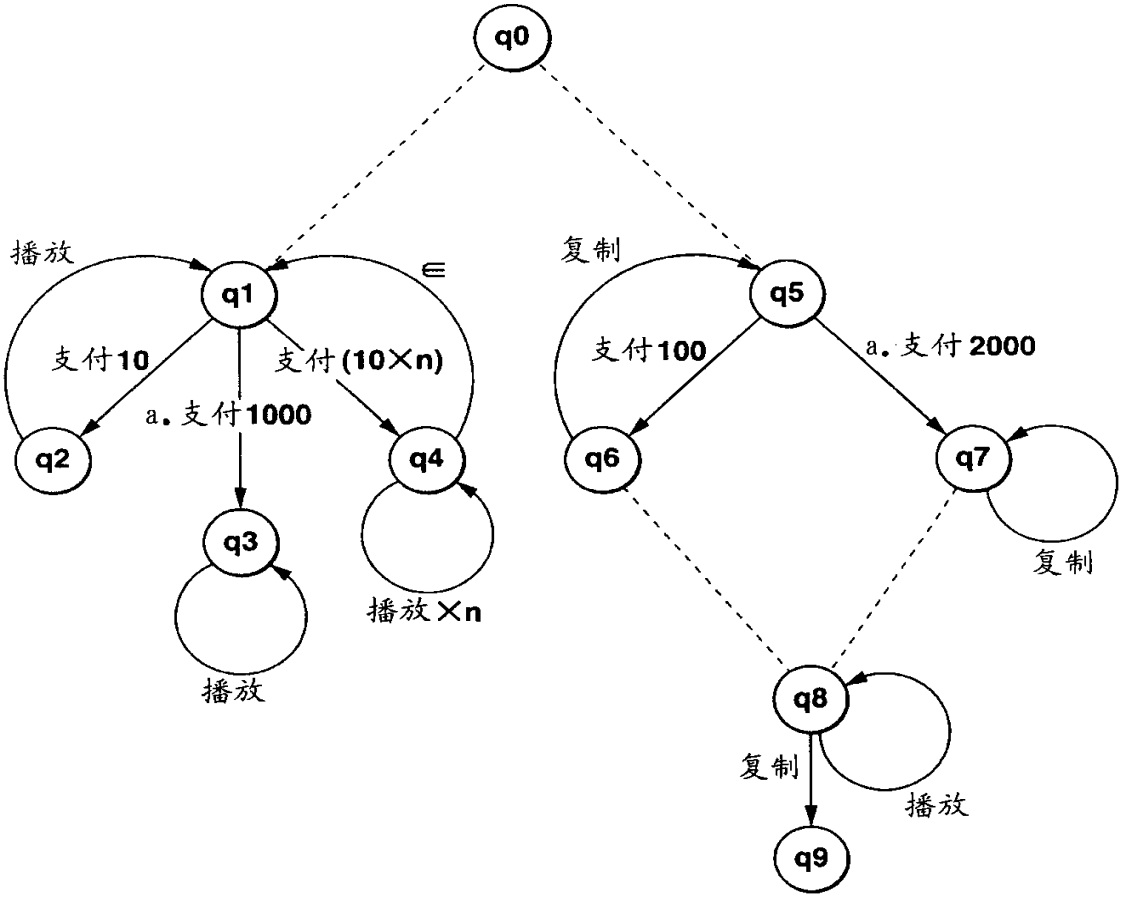

q0
播放
q1
∈
支付10
支付(10×n)
a. 支付1000
q2
q4
q3
播放×n
播放
复制
q5
支付100
a. 支付2000
q6
q7
复制
q8
复制
播放
q9

图 12

$\langle q_1, pay10, q_2 \rangle$
$\langle q_1, a.pay1000, q_3 \rangle$
$\langle q_1, pay(10 \times n), q_4 \rangle$
$\langle q_2, play, q_1 \rangle$
$\langle q_3, play, q_3 \rangle$
$\langle q_4, play \times n, q_4 \rangle$
$\langle q_4, \varepsilon, q_1 \rangle$
$\langle q_5, pay100, q_6 \rangle$
$\langle q_5, a.pay2000, q_7 \rangle$
$\langle q_6, copy, q_5 \rangle$
$\langle q_7, copy, q_7 \rangle$
$\langle q_8, play, q_8 \rangle$
$\langle q_8, copy, q_9 \rangle$

图 13

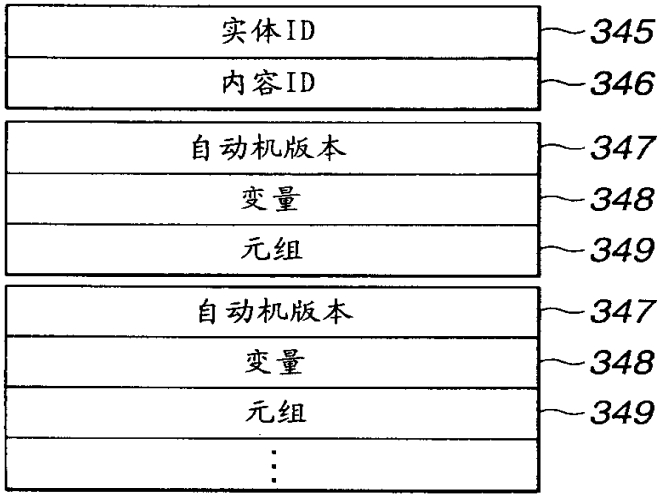


图 14

```
<!ENTITY% event" (
        play                    1
        copy                    1
        pay-for-play            1
        pay-for-copy            1
        pay-for-album-play      1
        pay-for-album-copy      1
        from                    1
        to                      1
        null                    1
)">
<!ENTITY% command" (
        drop                    1
        dup                     1
        swap                    1
        add                     1
        subtract                1
        multiply                1
        divide                  1
        remainder               1
        upper                   1
        lower                   1
        equal                   1
        less                    1
        greater                 1
        less-equal              1
        greater-equal           1
        and                     1
        or                      1
        not                     1
        bit-and                 1
        bit-or                  1
        bit-xor                 1
        bit-not                 1
)">
```

图 15

从1999/9/1内容可播放

```
<automaton>

   <!—This usage rule system has one Right Unit.
   Initial state is q1- ->
    <Initial-right-unit state="q1"/>

   <node state = "q1">
     <!—If after 1999/9/1, transfer to q2- ->
     <rule event="from" next-state="q2">
       <arguments>
         <integer value="time:19990901"/>
       </arguments>
     </rule>
   </node>

   <node state = "q2">
     <!- - playable - ->
     <rule event="play" next-state="q2"/>
   </node>

</automaton>
```

图 16

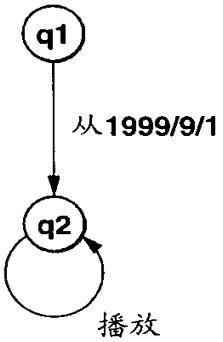


图 17

内容可播放至 1999/10/31

```
<automaton>

   <!- - This Usage Rule System has one Right Unit.
   Initial state is q2 - ->
    <Initial-right-unit state="q2"/>

   <node state = "q2">
      <!—If after 1999/10/31, transfer to end - ->
      <rule event="to" next-state="end">
        <arguments>
          <integer value="time:19991031"/>
        </arguments>
      </rule>

      <!- - playable - ->
      <rule event="play" next-state="q2">
      </rule>
   </node>

   <!—Unusable state - ->
   <node state = "end"/>

</automaton>
```

图 18

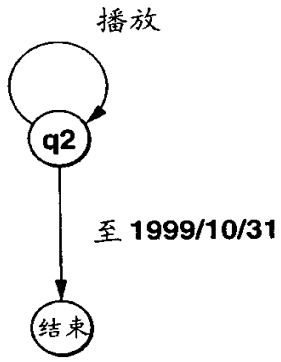


图 19

从1999/9/1至1999/10/31内容可播放16次

```
<automaton>

  <!--Define counter variables for playable numbers. Initial value is 16 -->
  <define-variable name="count" initial-value="16" />

  <!-- This Usage Rule System has one Right Unit. Initial state is q1 -->
  <initial-right-unit state="q1" />

  <node state="q1">
    <!--From 1999/9/1 transfer to q2 -->
    <rule event="from" next-state="q2">
      <arguments>
        <integer value="time:19990901" />
      </arguments>
    </rule>
  </node>

  <node state="q2">
    <!--From 1999/10/31, transfer to end -->
    <rule event="to" next-state="end">
      <arguments>
        <integer value="time:19991031" />
      </arguments>
    </rule>

    <rule event="play" next-state="q2">
      <!--Playable only for "count" numbers -->
      <arguments>
        <variable name="count" />
        <command name="load" />
      </arguments>
      <!--If this rule is selected, the "count" number decrements by one-->
      <action>
        <variable name="count" />
        <command name="load" />
        <integer value="1" />
        <command name="subtract" />
        <variable name="count" />
        <command name="store" />
      </action>
    </rule>
  </node>

  <!--Unusable state-->
  <node state="end" />

</automaton>
```

图 20

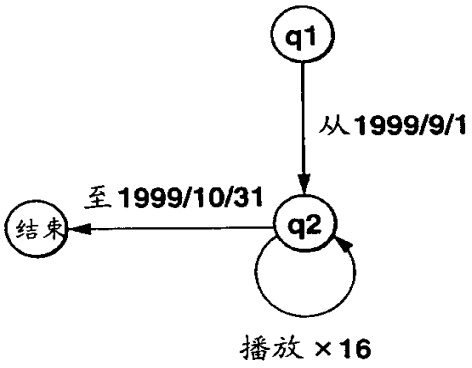


图 21

内容可播放小于和/或等于16次

```
〈automaton〉

  〈!--Define valuable counter for playable numbers. Initial value is 16 --〉
  〈define-variable name="count" initial-value="16" /〉

  〈!-- Usage Rule System has one Right Unit. Initial state is q2 --〉
  〈initial-right-unit state="q1" /〉

  〈node state="q2"〉
    〈rule event="play" next-state="q2"〉
      〈!--"Count" number of times playable --〉
      〈arguments〉
        〈variable name="count" /〉
        〈command name="load" /〉
      〈/arguments〉
      〈!--If this rule is selected. "count" number decrements by one--〉
      〈action〉
        〈variable name="count" /〉
        〈command name="load" /〉
        〈integer value="1" /〉
        〈command name="subtract" /〉
        〈variable name="count" /〉
        〈command name="store" /〉
      〈/action〉
    〈/rule〉
  〈/node〉

〈/automaton〉
```

图 22

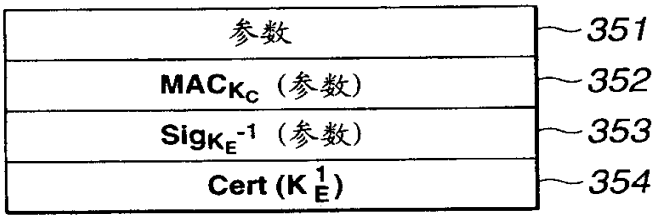

参数
MAC$_{K_C}$（参数）
Sig$_{K_E}^{-1}$（参数）
Cert (K_E^1)
351
352
353
354

图 23

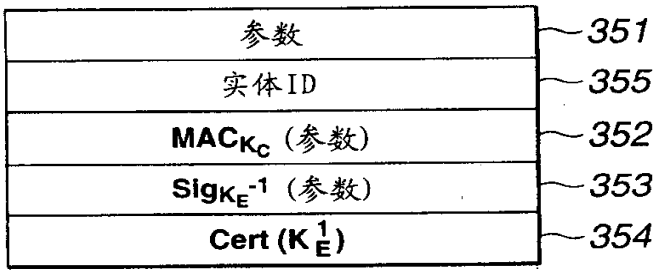

参数
实体ID
MAC$_{K_C}$（参数）
Sig$_{K_E}^{-1}$（参数）
Cert (K_E^1)
351
355
352
353
354

图 24

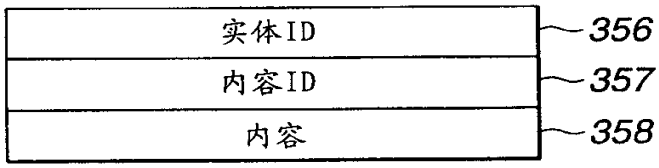

实体ID
内容ID
内容
356
357
358

图 25

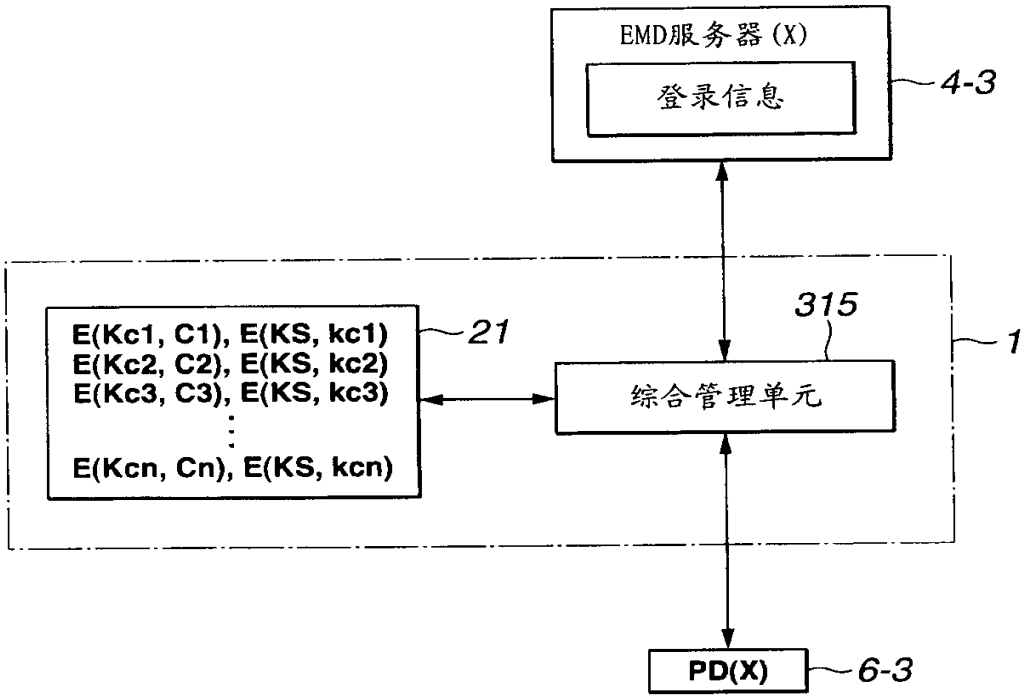

EMD服务器(X)
登录信息
4-3
315
1
E(Kc1, C1), E(KS, kc1)
E(Kc2, C2), E(KS, kc2)
E(Kc3, C3), E(KS, kc3)
E(Kcn, Cn), E(KS, kcn)
21
综合管理单元
PD(X)
6-3

图 26

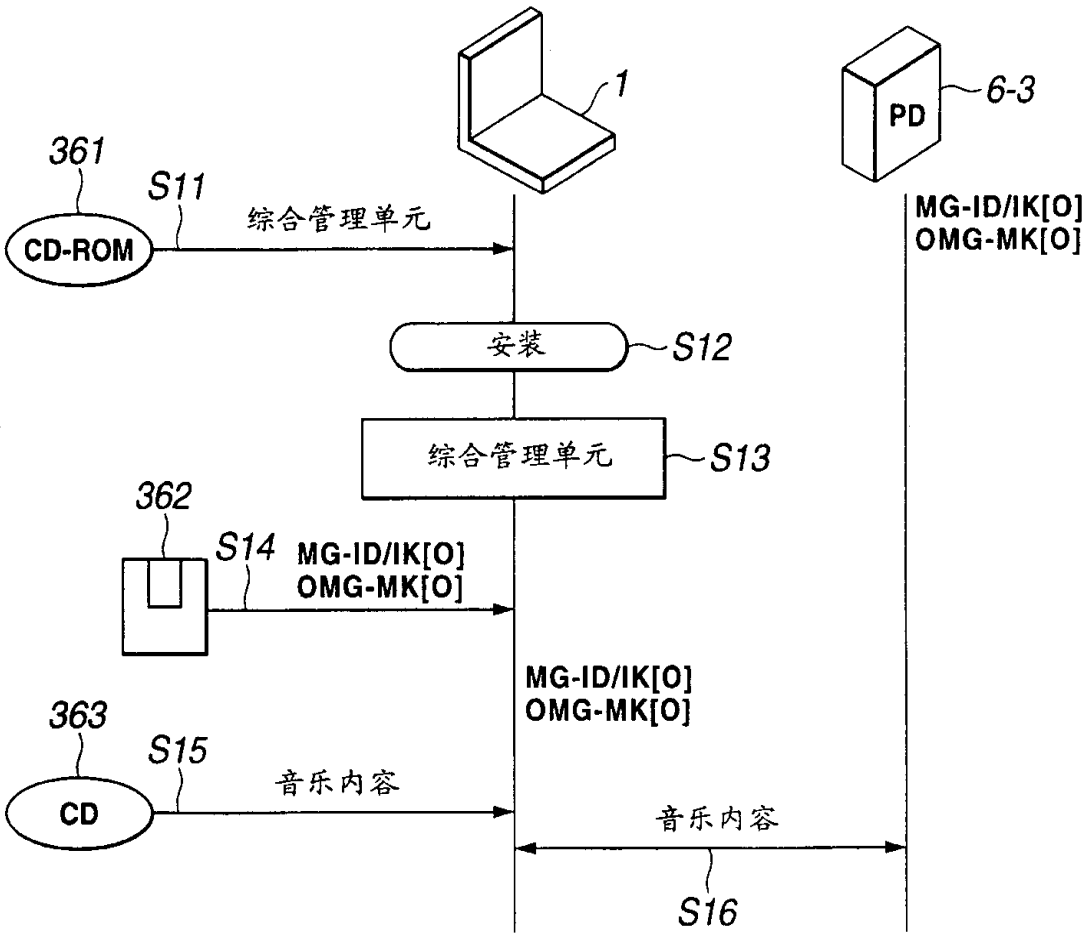

1
PD
6-3
361
S11
综合管理单元
CD-ROM
MG-ID/IK[O]
OMG-MK[O]
安装
S12
综合管理单元
S13
362
S14
MG-ID/IK[O]
OMG-MK[O]
MG-ID/IK[O]
OMG-MK[O]
363
S15
音乐内容
CD
音乐内容
S16

图 27

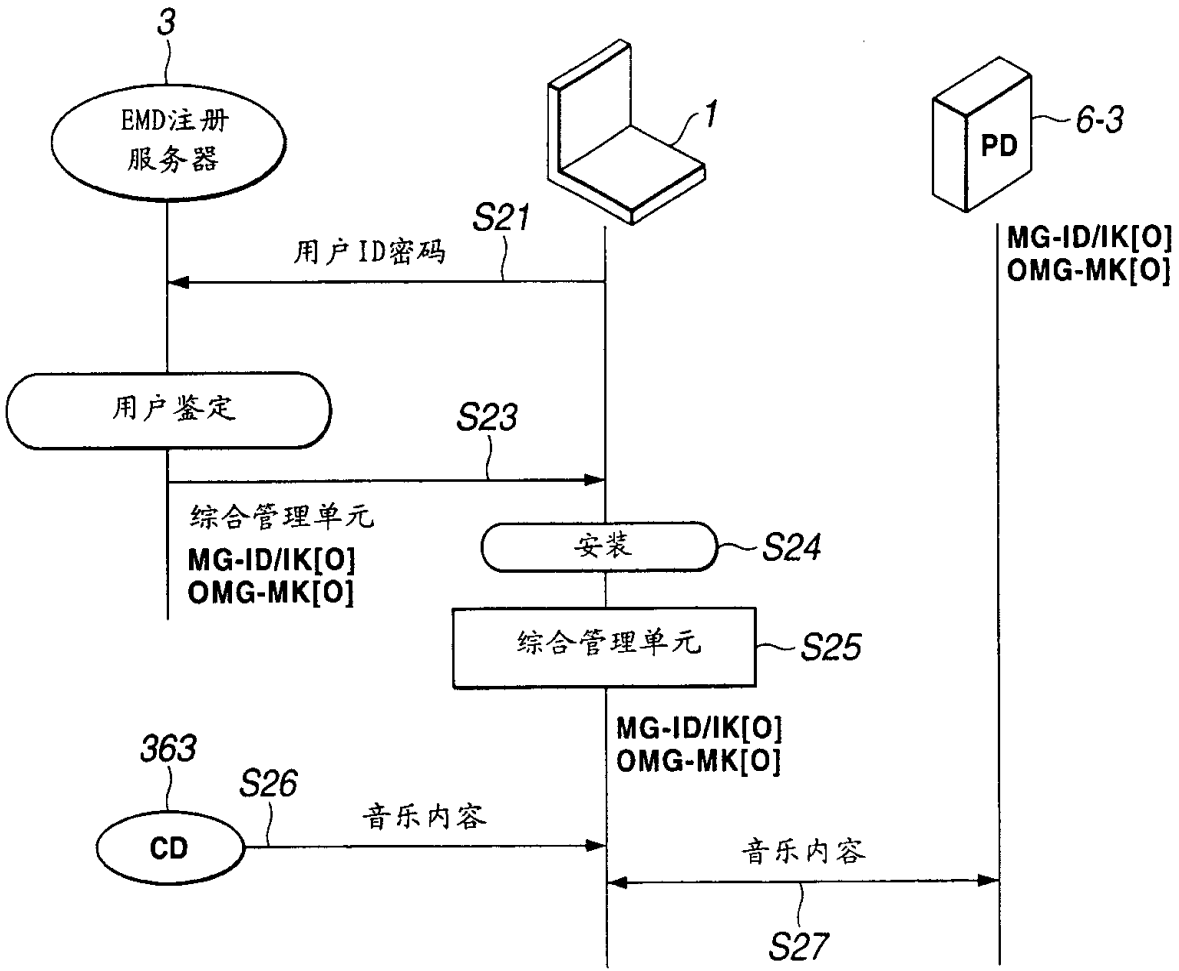

3
EMD注册
服务器
1
PD
6-3
MG-ID/IK[O]
OMG-MK[O]
S21
用户ID密码
用户鉴定
S23
综合管理单元
MG-ID/IK[O]
OMG-MK[O]
安装
S24
综合管理单元
S25
MG-ID/IK[O]
OMG-MK[O]
363
S26
CD
音乐内容
音乐内容
S27

图 28

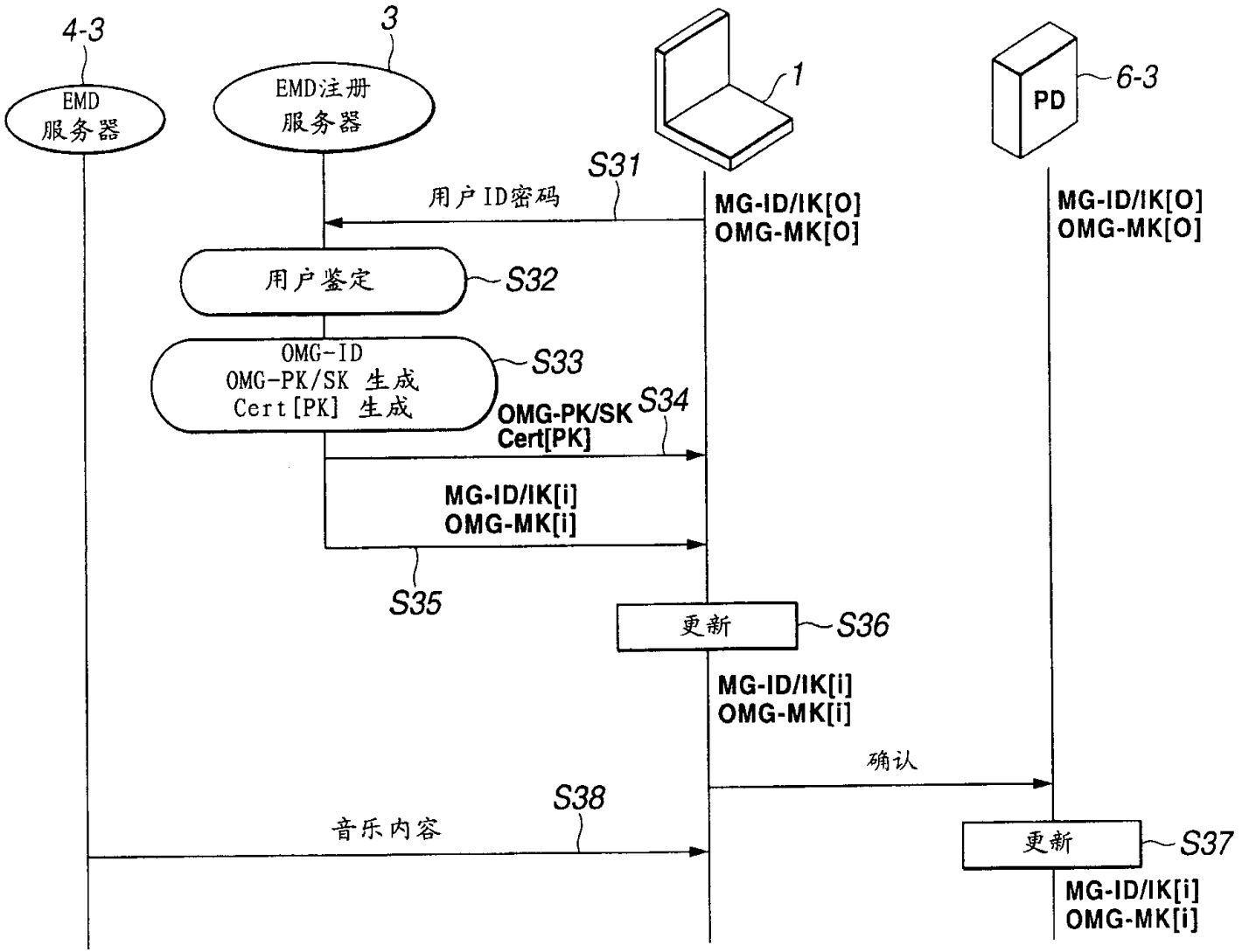

4-3
EMD
服务器
3
EMD注册
服务器
1
PD
6-3
S31
用户ID密码
MG-ID/IK[O]
OMG-MK[O]
MG-ID/IK[O]
OMG-MK[O]
用户鉴定
S32
OMG-ID
OMG-PK/SK 生成
Cert[PK] 生成
S33
OMG-PK/SK
Cert[PK]
S34
MG-ID/IK[i]
OMG-MK[i]
S35
更新
S36
MG-ID/IK[i]
OMG-MK[i]
确认
S38
音乐内容
更新
S37
MG-ID/IK[i]
OMG-MK[i]

图 29

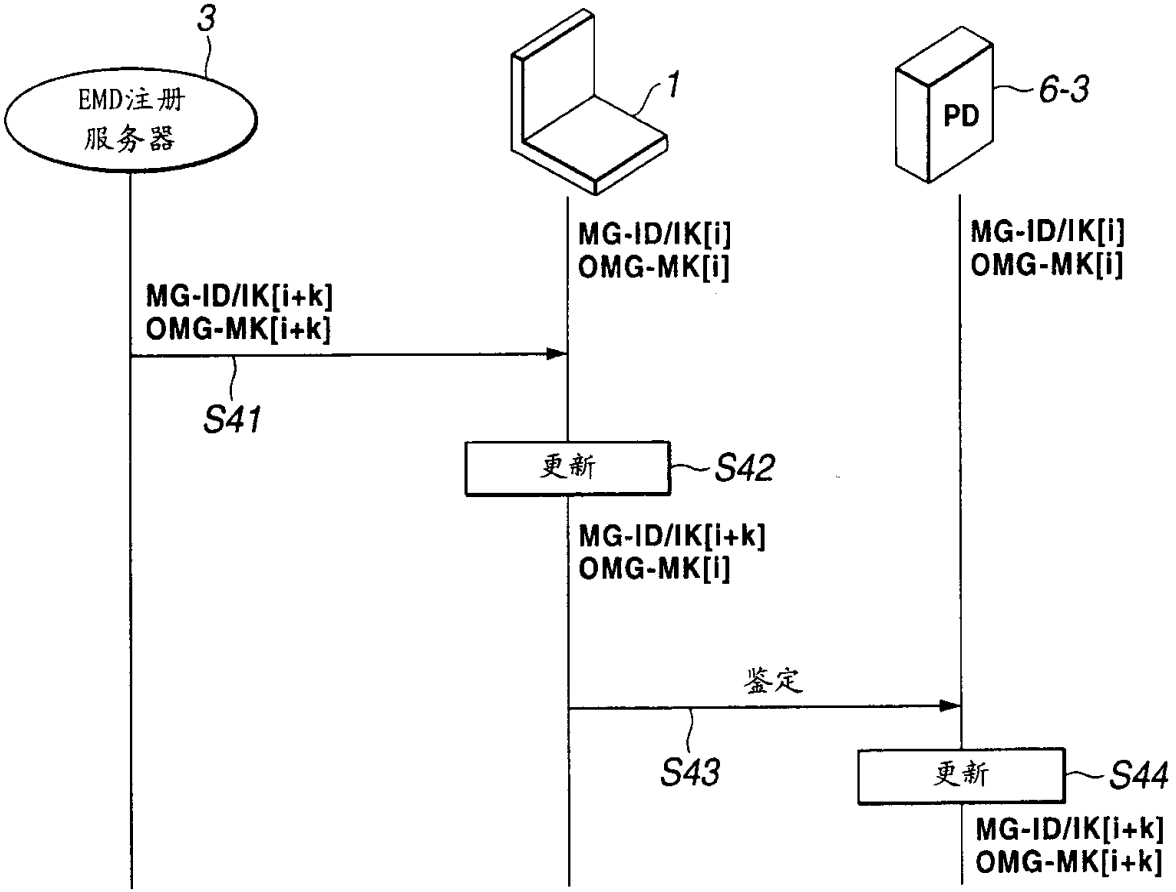

3
EMD注册
服务器
1
PD
6-3
MG-ID/IK[i]
OMG-MK[i]
MG-ID/IK[i]
OMG-MK[i]
MG-ID/IK[i+k]
OMG-MK[i+k]
S41
更新
S42
MG-ID/IK[i+k]
OMG-MK[i]
鉴定
S43
更新
S44
MG-ID/IK[i+k]
OMG-MK[i+k]

图 30

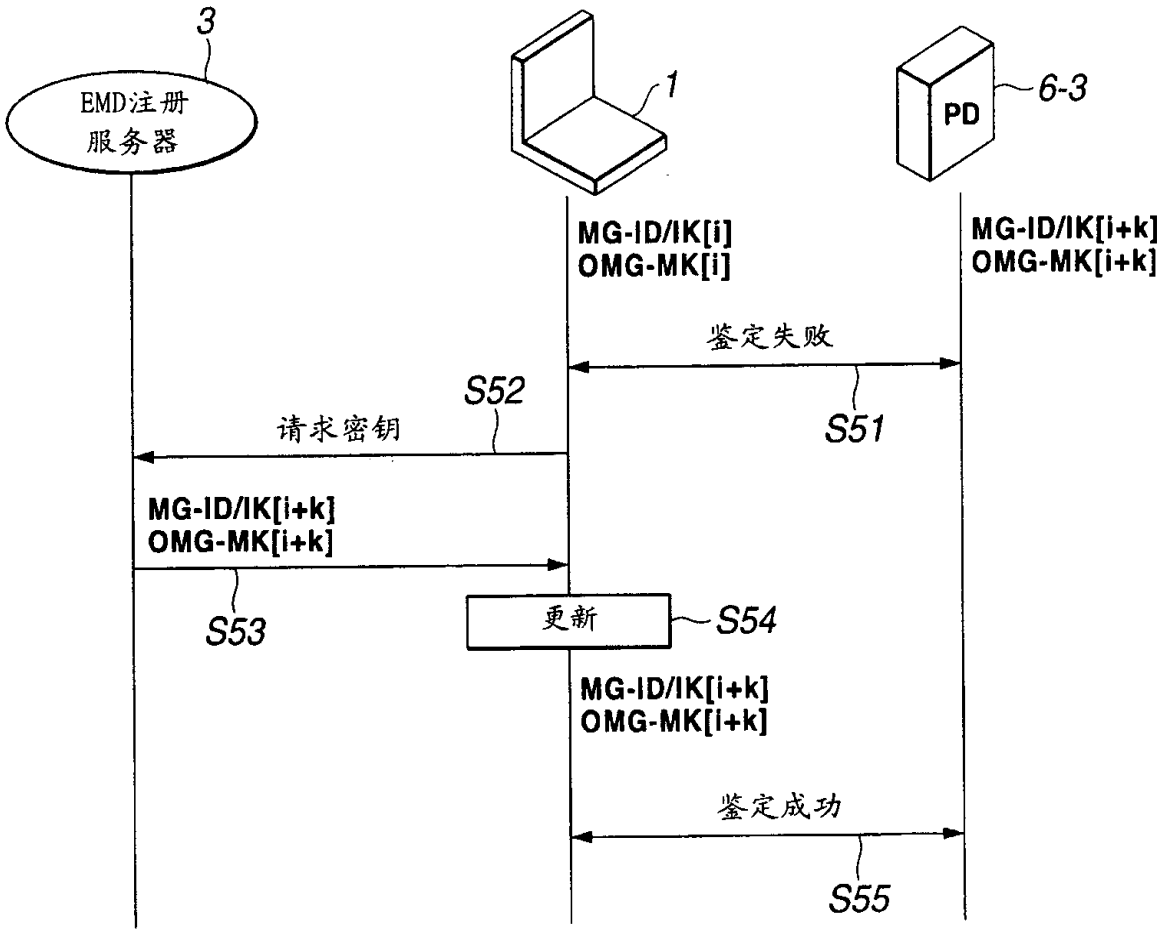

3
EMD注册
服务器
1
PD
6-3
MG-ID/IK[i]
OMG-MK[i]
MG-ID/IK[i+k]
OMG-MK[i+k]
鉴定失败
S51
S52
请求密钥
MG-ID/IK[i+k]
OMG-MK[i+k]
S53
更新
S54
MG-ID/IK[i+k]
OMG-MK[i+k]
鉴定成功
S55

图 31

权 利 要 求 书
按照条约第19条的修改

1、一种内容供给系统，包括:

内容服务器，用于在网络上发送内容数据；以及

数据处理器，具有用于再现和/或控制内容数据的再现控制程序，所述数据处理器将由内容服务器发送的内容数据存储在记录介质上以用于再现和/或控制，并且将所发送的内容数据的备份数据存储在记录介质上，所述数据处理器还将内容数据的使用登录（log）信息发送到所述内容服务器;

如果从所述记录介质中不再提供所述内容数据，所述数据处理器从所述内容服务器获得使用登录信息，所述数据处理器根据使用登录信息对存储于所述记录介质中的内容数据的备份数据执行再现和/或控制。

2、一种内容供给系统，包括:

内容服务器，用于在网络上发送内容数据；以及

数据处理器，具有用于再现和/或控制内容数据的再现控制程序，所述数据处理器将由内容服务器发送的内容数据存储在记录介质上以用于再现和/或控制，所述数据处理器还将所述内容数据的使用登录信息发送到所述内容服务器;

如果从所述记录介质中不再提供内容数据，所述数据处理器具有从所述内容服务器中重新发送的所述不再提供的内容数据，所述数据处理器还从所述内容服务器获得使用登录信息并根据所述使用登录信息对重新发送的内容数据执行再现和/或控制。

3、一种用于在具有再现和或控制内容数据的再现处理程序的数据处理器与用于通过网络将内容数据发送到所述数据处理器的内容服务器之间发送内容的方法，该方法包括步骤:

所述内容服务器将内容数据发送到所述数据处理器;

所述数据处理器将所述从内容服务器发送的内容数据存储在记录介质中以用于再现和/或控制，并且还将所发送的内容数据的备份数据存储在记录介质中;

数据处理器将所述内容数据的使用登录信息发送到所述内容服务器;

如果所述数据处理器不能从所述记录介质中获得所述内容数据，则所述内容服务器将使用所述登录信息发送到所述数据处理器；以及

所述数据处理器响应所述登录信息再现和/或控制存储在所述记录介质中的内容数据的备份数据。

4、一种用于通过网络在具有再现和/或控制内容数据的再现控制程序的数据处理器与将内容数据发送到数据处理器的内容服务器之间发送内容的方法，该方法包括步骤：

所述内容服务器将内容数据发送到所述数据处理器；

所述数据处理器将从所述内容服务器发送的内容数据存储在记录介质中以用于再现和/或控制；

所述数据处理器将所述内容数据的使用登录信息发送到所述内容服务器；

如果所述数据处理器不能从所述记录介质中获得所述内容数据，则所述内容服务器重新发送已变得不能提供给所述数据处理器的内容数据到所述数据处理器，并发送所述使用登录信息发送到所述数据处理器；

所述数据处理器根据使用所述登录信息再现和/或控制该重新发送的内容数据。

5、一种适于在数据处理器中安装的、在其中存储有用于获得通过网络从再现和/或控制内容数据的内容服务器发送的内容数据的再现控制程序的记录介质，所述再现控制程序包括：

将从所述内容服务器发送的内容数据存储在记录介质中以用于再现和/或控制，并存储所发送的内容数据的备份数据，以及将所述内容数据的使用登录信息发送所述内容服务器；以及

如果不再从所述记录介质提供内容数据，从所述内容服务器获得所述使用登录信息，并与使用登录信息一致来再现和/或控制存储在所述记录介质中的内容数据的备份数据。

6、一种适于在数据处理器中安装的并且在其中存储有用于获得通过网络从再现和/或控制内容数据的内容服务器发送的内容数据的再现控制程序的记录介质，所述再现控制程序包括：

将从所述内容服务器发送的内容数据存储在记录介质中以用于再现和/或控制；并将所述内容数据的使用登录信息发送到所述内容服务器；以及

如果不再从所述记录介质提供内容数据，则使内容数据从内容服务器重新发送，从所述内容服务器获得使用登录信息并与使用登录信息一致来再现

和/或控制重新发送的内容数据。

7、一种信息处理装置，包括:

重放控制程序，用于再现和/或控制通过网络从内容服务器发送的内容数据；以及

数据处理设备，用于存储从再现和/或控制该内容数据的所述内容服务器发送的内容数据，所述数据处理设备在所述的记录介质或其他的存储介质中存储所发送的内容数据的备份数据并将所述内容数据的使用登录信息发送给所述内容服务器;

当不能从所述记录介质中获得内容数据时，所述数据处理设备从所述内容服务器获得源自所述使用登录信息的数据以再现和/或控制在所述记录介质或所述其他的记录介质中存储的所述备份数据。

8、如权利要求 7 的信息处理装置，其中所述使用登录信息包括存储在所述记录介质中的内容 ID 和从所述内容服务器发送的内容的购买记录信息。

9、如权利要求 7 的信息处理装置，其中所述内容数据包括内容和内容密钥;

当存储在记录介质中的内容和/或内容密钥被破坏时，所述数据处理设备从所述内容服务器中获得源自所述使用登录信息的 ICV（完整性校验值），以便再现和/或控制存储在所述记录介质中或所述其他记录介质中的备份数据。

10、一种信息处理装置，包括:

重放控制程序，用于再现和/或控制通过网络从内容服务器发送的内容数据；以及

数据处理设备，用于将从所述内容服务器发送的内容数据存储在记录介质中以记录和/或再现内容数据，所述数据处理设备将所述内容数据的使用登录信息发送给所述内容服务器;

当不能从所述记录介质中获得内容数据时，则所述数据处理设备使不能提供的内容从所述内容服务器中重新发送到数据处理器，并从所述内容服务器获得源自所述使用登录信息的数据，所述数据处理设备根据源自所述使用登录信息的数据再现和/或控制重新发送的内容数据。

11、如权利要求 10 的信息处理装置，其中所述使用登录信息包括存储在记录介质中的内容 ID 和从内容服务器发送的内容的购买记录信息。

12 如权利要求 10 的信息处理装置，其中：内容数据包括内容和内容密

钥;

当存储在所述记录介质中的内容和/或内容密钥被破坏时,所述数据处理设备从所述内容服务器中获得源自所述使用登录信息的 ICV(完整性校验值),所述数据处理设备还使相应于破坏的内容数据从内容服务器重新发送并根据所述 ICV 再现和/或控制这样重新发送的内容数据。

13、一种用于再现和/或控制通过网络从内容服务器发送的内容数据的信息处理方法,包括:

存储从所述内容服务器发送的所述内容数据以用于再现和/或控制,在所述的记录介质或所述其他的存储介质中存储所发送的内容数据的备份数据并将所述内容数据的使用登录信息发送给所述内容服务器;

当不能从所述记录介质中获得内容数据时,从所述内容服务器获得源自所述使用登录信息的数据以再现和/或控制在所述记录介质或所述其他的记录介质中存储的备份数据。

14、如权利要求 13 的信息处理方法,其中所述使用登录信息包括存储在所述记录介质中的内容 ID 和从所述内容服务器发送的内容的购买记录信息。

15、如权利要求 13 的信息处理方法,其中所述内容数据包括内容和内容密钥,并且其中当存储在所述记录介质中的内容和/或内容密钥被破坏时,从所述内容服务器中获得源自所述使用登录信息的 ICV (完整性校验值),以再现和/或控制在所述记录介质或所述其他的记录介质中存储的所述备份数据。

16、一种用于再现和/或控制通过网络从内容服务器发送的内容数据的信息处理方法,其中

从所述内容服务器发送的内容数据被存储在记录介质中以用于再现和/或控制,并且所述内容数据的使用登录信息被发送到所述内容服务器,以及其中

当不能从所述记录介质中获得内容数据时,则从所述内容服务器中重新发送已变得不能获得的内容数据、从所述内容服务器获得的源自所述使用登录信息的数据,并且根据源自所述使用登录信息的数据再现和/或控制所重新发送的内容数据。

17、如权利要求 16 的信息处理方法,其中所述使用登录信息包括存储在所述记录介质中的内容 ID 和从所述内容服务器发送的内容的购买记录信息。

18、如权利要求 16 的信息处理方法,其中所述内容数据包括内容和内容

密钥，并且其中

当存储在所述记录介质中的内容和/或内容密钥被破坏时，从所述内容服务器中获得的源自所述使用登录信息的 ICV（完整性校验值），相应于被破坏的内容数据的内容数据被从所述内容服务器中重新发送并且根据 ICV 记录和/或再现这样重新发送的内容数据。

19、一种用于通过网络将内容数据发送到用于再现和/或控制的信息处理装置的内容发送方法，包括：

将所述内容数据发送到信息处理装置；

从所述信息处理装置接收发送自内容数据的使用登录信息并存储所接收的使用登录信息；

当不能从所述信息处理装置中的记录介质中获得内容数据时，从所述信息处理装置进行访问；以及

响应所述访问，将源自所述使用登录信息的数据发送到所述信息处理装置，以使所述信息处理装置响应源自所述使用信登录息的所述数据执行在所述信息处理装置中的所述记录介质或在所述其他的记录介质中存储的内容数据的备份数据的再现和/或控制。

20、如权利要求 19 的信息处理方法，其中：

所述使用登录信息包括存储在所述信息处理装置的所述记录介质中的内容 ID 和从所述信息处理装置发送的内容的购买记录信息；

当进行所述的访问时，根据所述购买记录信息确认不能获得的内容数据是否是用户已经购买的内容数据；以及其中

如果确认不能获得的内容数据是进行访问的用户已经购买的内容数据，对不能获得的内容数据是不被估价。

21、如权利要求 19 的信息处理方法，其中：

所述内容数据包括内容和/或内容密钥；

如果存储在所述信息处理装置的所述记录介质中的内容和/或内容密钥被破坏时，

从所述信息处理装置进行访问；以及其中

根据所述访问，将源自使用登录信息的 ICV（完整性校验值）发送到所述信息处理装置。

22、一种通过网络将内容数据发送到用于再现和/或处理的信息处理装置

的内容发送方法，包括:

将内容数据发送到所述信息处理装置;

从所述信息处理装置接收所发送的内容数据的使用登录信息并存储所接收的使用登录信息;

当不能从所述信息处理装置中的记录介质中获得内容数据时，从信息处理装置进行访问; 以及

根据所述访问，将不能被获得的内容数据重新发送到所述信息处理装置，并将源自所述使用登录信息的数据发送到所述信息处理装置使所述信息处理装置响应源自所述使用登录信息的数据执行所重新发送的内容数据的再现和/或控制。

23、如权利要求 22 的信息处理方法，其中

所述使用登录信息包括存储在所述信息处理装置的记录介质中的内容 ID 和从所述信息处理装置发送的内容的购买记录信息;

当进行所述的访问时，根据所述购买记录信息确认不能获得的内容数据是否是用户已经购买的内容数据; 以及其中

如果确认不能获得的内容数据是进行访问的用户已经购买的内容数据，对不能获得的内容数据是不被估价。

24、如权利要求 22 的信息处理方法，其中:

所述内容数据包括内容和/或内容密钥;

如果存储在所述信息处理装置的所述记录介质中的内容和/或内容密钥被破坏时，对所述信息处理装置进行访问; 以及其中

根据所述访问，将源自所述使用登录信息的 ICV（完整性校验值）和相应于所述被破坏的内容数据的内容数据发送到所述信息处理装置。