发明名称
内容发布系统、记录设备和方法、重放设备
根据设备和方法及程序
摘要
本发明涉及内容发布系统、记录设备和方法、重放设备和方法及程序。内容供给设备供给涉及主
内容的子内容。DVD-ROM 存储对于该 DVD-ROM 唯一的绑定密钥并且作为数码制品的主内容。主
播放器从该 DVD-ROM 中读取绑定密钥，获取涉及存储于 DVD-ROM 上的主内容的子内容，通过根
据所读取的绑定密钥对所获取的子内容加密来产生加密子内容，并向 SD 存储卡写入所产生的加密内
容。子播放器从该 DVD-ROM 中读取绑定密钥，从 SD 存储卡中读取加密子内容，通过根据绑定密
钥对所读取的加密子内容解密来产生子内容，并重放所产生的子内容。
1、一种重放涉及主内容的子内容的内容重放设备，其中，
便携存储介质预存储为数模制品、标题 ID 和绑定密钥的主内容，
该标题 ID 用于唯一识别该主内容，该绑定密钥用作用于对该子内容
进行加密以产生加密子内容的加密密钥，
该内容重放设备包括：
第一读取单元，该第一读取单元可操作以从该存储介质中读取该
标题 ID 和该绑定密钥；
接收单元，该接收单元可操作以接收对应于该标题 ID 的加密子
内容；
信息存储单元，该信息存储单元可操作以存储相互对应的所接收
的加密子内容和该标题 ID；
第二读取单元，该第二读取单元可操作以从该信息存储单元读取
对应于所读取的标题 ID 的该加密子内容；
解密单元，该解密单元可操作以使用所读取的绑定密钥作为解密
密钥对所读取的加密子内容解密，以产生重放子内容；以及
重放单元，该重放单元可操作以重放所产生的重放子内容。

2、如权利要求 1 所述的内容重放设备，其中，
该接收单元还接收黑名单，该黑名单包括关于已经记录在非法记
录介质上的信息的特征的特征信息，该非法记录介质上记录有通过非
法复制主内容而产生的非法内容，并且
该信息存储单元还存储所接收的黑名单，
该重放单元提取示出存储于该存储介质上的信息的特征的特征信
息，判断所提取的特征信息是否与该黑名单中的特征信息相匹配，
且当判断为肯定时，禁止该重放子内容和记录在该存储介质上的信息
的重放。

3、如权利要求 1 所述的内容重放设备，其中，
该存储介质为 ROM 介质。

4、一种用于内容重放设备的内容重放方法，该内容重放设备包括信息存储单元并重放涉及主内容的子内容，其中，

便携存储介质预存储为数码制品、标题 ID 和绑定密钥的主内容，该标题 ID 用于唯一识别该主内容，该绑定密钥用作于对该子内容进行加密以产生加密子内容的加密密钥，

该内容重放方法包括：
第一读取步骤，从该存储介质中读取该标题 ID 和该绑定密钥；
接收步骤，接收对应于该标题 ID 的加密子内容；
信息存储步骤，将相互对应的所接收的加密子内容和该标题 ID 存储在该信息存储单元中；

第二读取步骤，从该信息存储单元读取对应于所读取的标题 ID 的该加密子内容；

解密步骤，使用所读取的绑定密钥作为解密密钥对所读取的加密子内容解密，以产生重放子内容；以及

重放步骤，重放所产生的重放子内容。
说明

内容发布系统、记录设备和方法、重放设备和方法及程序

本发明为分案申请，其原申请日是 2005 年 7 月 11 日进入中国国家阶段，国际申请日为 2004 年 1 月 9 日的国际专利申请 PCT/JP2004/000095，该原申请的中国国家申请号是 200480002065.4，发明名称为“内容发布系统、记录设备和方法、重放设备和方法及程序”。

技术领域

本发明涉及用于发布数字内容的技术。

背景技术

记录例如电影和音乐的数字作品的如 DVD 的记录介质正在普及。诸如 DVD 的记录介质其上记录有大量数字化的信息，且因此可以非永久使用而不退化。

通过使用这种记录介质出售和/或出租记录有电影和音乐的记录介质的商业发展，已建立了庞大的市场。对于这种商业贸易，防止非法使用记录在记录介质上的数字作品是至关重要的。

日本专利 No. 3073590 公开了一种电子数据保护系统，其旨在防止非法使用存储在记录介质上的计算机软件、电子出版物等。

根据来自自由使用许可方控制的设备的使用许可，该电子数据保护系统保护在用户设备中使用的记录介质上存储的电子数据。记录设备存储唯一指定加密电子数据和记录介质的介质唯一号码。使用许可设备包括：解密密钥，用于将存储在记录介质上的加密电子数据解密；许可信息产生单元，根据存储在记录介质上的介质唯一号码，对电子数据解密密钥加密并产生许可信息；和写入单元，将由许可信息产生单元产生的许可信息写入到记录介质。用户设备包括：读取单元，从
记录介质中读取许可信息、加密电子数据和介质唯一号码；解密密钥
产生单元，根据介质唯一号码，对许可信息解密并产生电子数据解密
密钥；和电子数据解密单元，根据由解密密钥产生单元产生的电子数
据解密密钥，来对加密电子数据解密。

根据该结构，可以获得能够使用户设备仅使用存储在合法存储介
质上的加密电子数据的电子数据保护系统，且该电子数据保护系统的
使用已由使用许可设备许可。

而且，在国际公开号 WO 00/63860（国际公开日：2000 年 10 月
26 日，国际申请号：PCT/US00/10414）中公布的摘要公开了下述技
术。

提供一种用于电子追踪内容发布的系统、方法和制品。首先，将
电子存储介质追踪标识符加入到电子存储介质中并存储在数据库中。
接着，使程序包追踪标识符位于存储了电子存储介质的程序包上。然
后当利用追踪程序包上的标识符来在各实体（entity）之间发送电子
存储介质时追踪电子存储介质。而且，可以利用电子存储介质上的追
踪标识符来识别电子存储介质，以提供对包含在电子存储介质上的信
息的许可使用。

由于上述各种技术能够防止非法使用写入到记录介质上的内容，
所以出租和/或出售这种记录介质的商业贸易发展起来。

然而，最近，以不同于记录介质的方式来发布涉及记录在记录介
质上的内容的子内容。一个子内容的实例为对记录在记录介质上的电
影的结局的预览。通过因特网或等同物来将该预览分配给用户。

然而，虽然上述用于防止非法使用内容的技术可以防止非法使用
写入到记录介质中的内容，但是存在这种技术不能防止非法使用涉及
写入记录介质中的内容的子内容，子内容经由另一发布路径发布该记
录介质。

发明内容

本发明的目的是提供能够防止非法使用与记录于便携式 ROM 介
质上的主内容相关的子内容的内容发布系统、内容记录设备、内容重放设备、内容记录方法、内容重放方法、计算机程序和记录介质。

为了获得上述目的，本发明为一内容发布系统，该内容发布系统发布与主内容相关的子内容，且由内容供给设备、内容记录设备和内容重放设备组成。

内容供给设备输出与主内容相关的子内容。ROM 介质存储关于 ROM 介质是唯一的唯一信息和数制制品。内容记录介质从该便携式 ROM 介质中读取该唯一信息，获得与存储在 ROM 介质上的主内容相关的子内容，根据读取的唯一信息对所获得的子内容加密，以产生加密子内容，并将所产生的加密子内容写入到便携式半导体存储器。

内容重放设备从 ROM 介质中读取唯一信息，根据所读取的唯一信息对加密的子内容解密，以产生重放子内容，并重放所产生子内容

由于该结构，仅在该 ROM 介质和该半导体存储器介质都安装在内容重放设备中时，内容重放设备才重放子内容。这意味着，如果将由另一方购买的 ROM 介质与半导体存储器一起安装在内容重放设备中，则不能重放半导体存储器上的子内容。因此，对子内容的保护提高了。

附图说明

图 1 是示出内容发布系统 1 的结构的框图；
图 2 是示出 DVD 制造设备 100 的结构的框图；
图 3 是示出记录在 DVD 500 上的信息的一个实例；
图 4 是示出内容供给设备 200 的结构的框图；
图 5 是示出主播放器 300 的结构的框图；
图 6 是示出存储卡 600 的结构的框图；
图 7 是示出子播放器 400 的结构的框图；
图 8 是示出 DVD 制造设备 100 的操作的流程图；
图 9 是示出主播放器 300 用于获取子内容的操作的流程图，并在图 10 中继续；
图 10 是示出主播放器 300 用于获取子内容的操作的流程图，并
在图11中继续；

图11是图10的延续，示出了主播放器300用于获取子内容的操作的流程图；

图12示出用于在内容供给设备200与主播放器300之间相互认证的操作的流程图；

图13示出主播放器300用于重播子内容的操作的流程图；

图14示出子播放器400用于重播子内容的操作的流程图，并在图15中继续；

图15是图14的继续，示出了子播放器400用于重播子内容的操作的流程图；

图16是示出用于在子播放器400与存储卡600之间相互认证的操作的流程图；

图17示出作为一个变形实例的内容发布系统1b的结构和操作。

具体实施方式

1. 第一实施例

下面描述作为本发明一个实施例的内容发布系统1a。

1.1 内容发布系统1a的结构

如图1中所示，内容发布系统1a由DVD制造设备100、内容供给设备200、主播放器300和子播放器400构成。

由DVD制造者拥有的DVD制造设备100将主内容写入DVD。这里，DVD是指仅可以向其写入一次信息的ROM型记录介质。而且，主内容的一个实例为由数字视频数据和数字音频数据构成的电影信息。由销售方将写入了主内容的DVD500卖出。用户购买并因此拥有该DVD500。

由于内容供给者拥有的内容供给设备200经由因特网10将涉及主内容的子内容分配给用户以收取费用。子内容为涉及主内容的内容。子内容的实例包括作为主内容的电影的预览的视频和音频信息、用文字表示的电影中演员所讲述的剧本的字幕、以及有关电影中的演员的信息。
由用户拥有的主播放器 300 设置在用户居住的屋内。显示器 351和扬声器 352 连接于主播放器 300。用户将所购买的 DVD 500 放置在主播放器 300 中。根据用户操作，主播放器 300 重放记录在 DVD 500 中的主内容，并向显示器 351 和扬声器 352 输出视频和音频。而且，主播放器 300 连接于因特网 10，并根据用户操作，从内容供给设备 200 获取涉及记录在 DVD 500 上的主内容的子内容，并将所获取的子内容写入存储卡 600 上。

由用户拥有的子播放器 400 设置在用户汽车上。子播放器 400 包括显示器（未示出）和扬声器 451。用户将所购买的 DVD 500 放置于子播放器 400 中。根据用户操作，子播放器 400 重放记录在 DVD 500 上的主内容，并向内部显示器和扬声器 451 输出视频和音频。而且，用户将所购买的 DVD 500 和存储卡 600 都放置在子播放器 400 中。子播放器 400 根据用户操作来从存储卡 600 中读取子内容，并仅在 DVD 500 和存储卡 600 都放置于子播放器 400 中时，重放所读取的子内容。

1.2 DVD 制造设备 100 的结构

如图 2 中所示，DVD 制造设备 100 由控制单元 101、显示单元 102、输入单元 103、信息存储单元 104、加密单元 105、绑定（bind）密钥产生单元 106 和输出单元 107 构成。

DVD 制造设备 100 具体地是由微处理器、ROM、RAM、硬盘单元、显示单元、键盘等构成的计算机。RAM 和硬盘单元存储计算机程序。DVD 制造设备 100 根据计算机程序来通过微处理器操作实现其功能。

值得注意的是，图 2 中的每一模块通过连接线连接于其它模块，但是在图 2 中省略了部分连接线。这里，每一连接线表示能够传送信号和信息的一个路径。而且，在连接于示出加密单元 105 的模块的多个连接线中，其上具有密钥标记的那些连接线示出的路径表示通过该路径将信息作为密钥传送到加密单元 105。这还适用于其它附图。

（1）信息存储单元 104

具体地，信息存储单元 104 由硬盘单元构成。如图 2 中所示，信
息存储单元 104 具有主内容表 121。主内容表 121 包括多条主内容信息，每条主内容信息由主内容标题 ID、主内容和主内容密钥构成。

在这里，作为一个实例，主内容为由数字视频数据和数字音频数据构成的电影信息。

主内容标题 ID 为唯一识别主内容的识别号。主内容标题 ID 的一个实例为“MID001”，如图 2 中所示。这里，“MID001”中的第一字符“M”为示出该内容为主内容的识别代码。跟随“M”后的字符串“IID”为示出该标题 ID 为标题标识符的识别代码。而且，跟随“IID”后的字符串“001”用于识别主内容的号码。

主内容密钥为在对主内容加密时用作密钥的信息。通过某些方式将主内容密钥供给到合法购买 DVD 的用户，该 DVD 上记录了利用主内容密钥加密的加密主内容。值得注意的是，由于向用户供给主内容密钥不是本发明的主题，因此省略其说明。

（2）控制单元 101、显示单元 102 和输入单元 103

输入单元 103 从操作者接收将主内容写入 DVD 的操作和主内容的标题 ID。输入单元 103 向控制单元 101 输出通过所接收的操作示出的指令信息和主内容标题 ID。

控制单元 101 接收该指令信息和主内容标题 ID，并根据所接收的指令信息和主内容标题 ID 来控制加密单元 105、约束单元 106 和输出单元 107。

显示单元 102 根据控制单元 101 的控制来显示各种信息。

（3）加密单元 105

作为一个实例，加密单元 105 具有由 DES（数据加密标准）指定的加密算法 E1。

加密单元 105，根据控制单元 101 的控制，从主内容表 121 中读取主内容和对应于主内容标题 ID 的主内容密钥，其中输入单元 103 接收针对该主内容标题 ID 的输入。加密单元 105 利用所读取的主内容密钥作为密钥通过将加密算法 E1 应用于所读取的主内容来产生加密主内容，并向输出单元 107 输出所产生的加密主内容。

（4）绑定密钥产生单元 106
绑定密钥产生单元 106 根据控制单元 101 的控制为每个 DVD 产生一个随机序号，并将所产生的每一随机序号作为绑定密钥输出到输出单元 107。

值得注意的是，能够产生绑定密钥，使多个 DVD 具有相同的绑定密钥，而非对每一 DVD 产生单独的绑定密钥。

（5）输出单元 107

输出单元 107 从控制单元 101 接收主内容标题 ID。然后，输出单元 107 根据控制单元 101 的控制从加密单元 105 接收加密主内容，并从绑定密钥产生单元 106 接收绑定密钥。

接着，输出单元 107 根据控制单元 101 的控制，将相对应的所接收的主内容标题 ID、绑定密钥和加密主内容写入 DVD。

这样，如图 3 中所示，制造其上记录了主内容标题 ID、绑定密钥和加密主内容的 DVD 500。

1.3 内容供给设备 200 的结构

内容供给设备 200，如图 4 中所示，由控制单元 201、显示单元 202、输入单元 203、信息存储单元 204、记账（billing）单元 205、加密单元 206、发送/接收单元 207 和认证单元 208 组成。

内容供给设备 200 为类似于 DVD 制造设备 100 的计算机。内容供给设备 200 通过微处理器根据计算机程的操作来序实现其功能。

（1）信息存储单元 204

具体地，信息存储单元 204 由硬盘单元构成。信息存储单元 204，如图 4 中所示，具有子内容表 221、黑名单 222 和器件失效列表 223。

【子内容表 221】

子内容表 221，如图 4 中所示，包括多条子内容信息，每条子内容信息由子内容标题 ID、子内容和子内容密钥构成。

这里，子内容为涉及主内容的信息，如前所描述，具体为电影预览、字幕信息、关于电影中的演员的信息等。子内容标题 ID 为唯一识别子内容的识别号。子标题 ID 的一个实例为 “SID00101”，如图 4 中所示。这里，“SID00101” 的第一个字符 “S” 为示出内容为子内容
的识别代码。跟随“S”后的字符串“ID”为示出标题ID为标题标识符的识别代码。而且，跟随“ID”后的字符串“001”为用于识别涉及该子内容的主内容的号码。而且，跟随“001”后的字符串“01”为用于识别子内容的号码。这样，用于指定相关主内容的标题ID的信息包含在子内容标题ID中。因此，如果子内容标题ID已知，则相关主内容标题ID也已知。反过来说，如果主内容标题ID已知，则相关子内容标题ID已知。

根据上述命名标题ID的规则，可以将多个子内容与一个主内容相关联。

值得注意的是，用于命名标题ID的规则并不限于上面描述的那些。可以将多个子内容与多个主内容相关联。

子内容密钥为在对子内容加密时用作密钥的信息。

〈黑名单 222〉

黑名单222包括识别非法记录介质的信息，在该非法记录介质上，记录了非法复制主内容的非法内容，换句话说，为盗版盘。具体地，黑名单由多条特征信息构成，如图4中所示。

该特征信息由记录在盗版盘上的非法数据视频数据和非法音频数据部分构成。该特征信息为非法数据的特征且通过分析非法数据而被提取。该特征信息为不包含在合法数字视频数据或数字音频数据中的信息。

当从记录在记录介质上的数字数据中提取了特征信息时，就认为该记录介质为盗版盘。

〈器件失效列表 223〉

设置器件失效列表223，使得当信息写入记录介质的写入设备和重放来自记录介质的信息的重放设备的的密钥或加密或解密系统被非法暴露给第三方之后，可以防止该写入设备和重放设备被非法使用。

器件失效列表223，如图4中所示，包括多个器件ID。每一器件ID为用于识别其密钥或加密或解密系统被非法暴露给第三方的器件的识别号。
（2）控制单元 201

控制单元 201 经由因特网 10 和发送/接收单元 207 接收来自主播播放器 300 的用户 ID、子内容获取请求和主内容标题 ID。

当从主播播放器 300 接收用户 ID、子内容获取请求和主内容标题 ID 时，控制单元 201 控制认证单元 208 以便于该认证单元 208 执行与主播播放器 300 之间的相互器件认证。

接着，仅当认证单元 208 进行的器件认证被通过后，控制单元 201 根据所接收的主内容标题 ID 来产生子内容检索标题 ID。具体地，当主内容标题 ID 为“MID001”时，控制单元 201 从“MID001”提取扇区“001”，并经过合并识别代码“S”、识别代码“ID”和提取的“001”部分来产生子内容检索标题 ID。接着，控制单元 201 使用前向匹配检索方法以从子内容表 221 中提取与检索标题 ID 相匹配的包括子内容标题 ID 的子内容信息。而且，控制单元 201 从通过提取获得的子内容信息中提取子内容标题 ID。接着，控制单元 201 向记账单元 205 输出用户 ID、子内容获取请求和子内容标题 ID，并控制以使记账单元 205 执行记账处理。

接着，控制单元 201 向加密单元 206 输出所提取的子内容标题 ID，并控制以使加密单元 206 对子内容加密。

此外，控制单元 201 向发送/接收单元 207 输出所提取的子内容标题 ID，并控制以使发送/接收单元 207 发送子内容标题 ID、加密子内容、子内容密钥、黑名单和器件失效列表。

（3）记账单元 205

记账单元 205 从控制单元 201 接收用户 ID、子内容获取请求和子内容标题 ID。一旦接收用户 ID、子内容获取请求和子内容标题 ID，记账单元 205 将由所接收的子内容标题 ID 所表示的子内容记在所接收的用户 ID 示出的用户的账上。

（4）认证单元 208

认证单元 208 与主播播放器 300 的认证单元 304 执行相互的器件认证。

当认证单元 208 在器件认证中失败时，内容供给设备 200 结束子
内容供给过程。当认证单元 208 在器件认证成功时，内容供给设备 200 继续子内容供给过程。

稍候详细描述认证单元 208 的认证操作的细节。

（5）加密单元 206

根据控制单元 201 的控制，加密单元 206 从信息存储单元 204 读取包括子内容标题 ID 的子内容信息，并且从所读取的子内容信息中提取子内容和子内容密钥。

接着，根据控制单元 201 的控制，加密单元 206 利用该子内容密钥作为密钥通过对子内容运用加密算法 E1 来产生加密子内容，并向发送/接收单元 207 输出所产生的加密子内容和子内容密钥。

（6）发送/接收单元 207

根据控制单元 201 的控制，发送/接收单元 207 从信息存储单元 204 中读取黑名单 222 和器件失效列表 223。

接着，根据控制单元 201 的控制，发送/接收单元 207 将子内容标题 ID、加密子内容、子内容密钥、黑名单和器件失效列表经由因特网 10 发送到主播放器 300。

（7）显示单元 202 和输入单元 203

根据控制单元 201 的控制，显示单元 202 显示各种信息。

输入单元 203 接收来自用户的输入，并将所接收的输入信息输出到控制单元 201。

1.4 主播放器 300 的结构

如图 5 中所示，主播放器 300 由控制单元 301、显示单元 302、输入单元 303、认证单元 304、发送/接收单元 305、加密单元 306、驱动单元 307、解密单元 308、信息存储单元 309、输入/输出单元 310、解密单元 311、重放单元 312、解密单元 313、认证单元 314、散列（hash）单元 315 和提取单元 316。将显示器 351 和扬声器 352 连接于重放单元 312。

主播放器 300 为类似于 DVD 制造设备 100 的计算机系统。主播放器 300 通过微处理器根据计算机程序的操作来实现其功能。
（1）信息存储单元 309

具体地，信息存储单元 309 由硬盘单元构成，而且，如图 5 中所示，包括用于存储子内容标题 ID、加密子内容密钥、加密内容和黑名单的区域。

子内容标题 ID 为用于唯一识别子内容的识别信息。

加密子内容密钥为已经被加密的子内容密钥。

加密子内容为已经被加密的子内容。

这里，标题 ID、加密子内容密钥和加密子内容相互对应。

如先前所述，黑名单包括识别其上记录非法内容的非法记录介质的信息，该非法内容为非法复制的主内容，换句话说为盗版盘。具体地，黑名单由多个特征信息块构成。

（2）输入单元 303

当要获取子内容时，输入单元 303 接收来自用户的子内容获取请求，并向控制单元 301 输出所接收的获取请求。

当要重放子内容时，输入单元 303 经由遥控装置 353 接收来自用户的要被重放的子内容的标题 ID 的输入，并向控制单元 301 输出已接收其输入的标题 ID。

（3）控制单元 301

当要获取子内容时，控制单元 301 从输入单元 303 接收获取请求，控制驱动单元 307 以便于从 DVD 500 中读取子内容标题 ID，并从驱动单元 307 接收主内容标题 ID。接着，控制单元 301 经由发送/接收单元 305 和因特网 10 向内容供给设备 200 发送内部存储的用户 ID、子内容获取请求和主内容标题 ID。这里，用户 ID 为用于唯一识别用户的识别信息。

另外，控制单元 301 从认证单元 314 中接收示出认证成功或失败的认证结果信息，并根据所接收的认证结果信息来控制各种构成元件。

另外，当要重放子内容时，控制单元 301 向驱动单元 307 输出所接收的子内容标题 ID。

（4）发送/接收单元 305
发送/接收单元 305 从内容供给设备 200 经由因特网 10 接收子内容标题 ID、加密子内容、子内容密钥、黑名单和器件失效列表，并根据控制单元 301 的控制，向加密单元 306 输出所接收的子内容密钥，向输入/输出单元 310 输出所接收的加密子内容，向输入/输出单元 310 输出所接收的黑名单和器件失效列表，并向散列单元 315 输出所接收的黑名单。

此外，发送/接收单元 305 将所接收的内容标题 ID 和所接收的加密子内容写入到信息存储单元 309。

（5）认证单元 304
认证单元 304 与内容供给设备 200 的认证单元 208 一起执行相互器件认证。

当认证单元 304 在器件认证中失败时，主播放器 300 结束子内容获取过程。当认证单元 304 在器件认证成功时，主播放器 300 继续子内容获取处理。

稍后描述认证单元 304 的认证操作细节。

（6）驱动单元 307
根据控制单元 301 的控制，驱动单元 307 从 DVD 500 中读取主内容标题 ID，并向控制单元 301 输出所读取的主内容标题 ID。

驱动单元 307 从 DVD 500 中读取对应于主内容标题 ID 的绑定密钥，并向加密单元 306 输出所读取的绑定密钥。

当子内容被重放时，驱动单元 307 从控制单元 301 中接收主内容标题 ID，并从 DVD 500 中读取对应于所接收的主内容标题 ID 的绑定密钥，并向解密单元 311 输出所读取的绑定密钥。

（7）散列单元 315
散列单元 315 从发送/接收单元 305 中接收黑名单，通过向黑名单应用散列函数 Hash 来计算散列值 H，并将所计算的散列值 H 输出到加密单元 306。

散列单元 315 从信息存储单元 309 中读取对应于子内容标题 ID 的黑名单。

当提取单元 316 判断所产生的特征信息不包含在所读取的黑名单
上时，散列单元 315 从信息存储单元 309 中读取黑名单，通过向所读
t的黑名单应用散列函数 Hash 来产生散列值 H=Hash（黑名单），并
将所产生的散列值 H 输出到解密单元 311。

（8）加密单元 306
加题单元 306 从驱动单元 307 接受绑定密钥，从散列单元 315 中
接收散列值 H 并从发送/接收单元 305 中接收子内容密钥。接着，
加密单元 306 通过将所接收的散列值 H 与所接收的绑定密钥以该顺序
连接来产生密钥，并通过使用所产生的密钥对所接收的子内容密钥应
用加密算法 E2 来产生加密子内容密钥。这里，加密算法 E2 为 DES
加密算法。

接着，加密单元 306 向输入/输出单元 310 输出所产生的加密子
内容密钥。另外，加密单元 306 将所产生的加密子内容密钥写入信息
存储单元 309。

（9）认证单元 314
当要将信息写入存储卡 600 时，认证单元 314 与存储卡 600 的认
证单元 602 一起执行相互器件认证。

当认证单元 314 在与存储卡 600 的认证单元 602 的器件认证中失
败时，主播放器 300 结束用于访问存储卡 600 的处理。

仅当认证单元 314 在与存储卡 600 的认证单元 602 的器件认证成
功时，主播放器继续对访问存储卡 600 的进一步处理。

认证单元 314 向控制单元 301 输出示出认证成功或失败的认证结
果信息。

（10）输入/输出单元 310
仅当认证单元 314 的器件认证成功时，输入/输出单元 310 接收
来自控制单元 301 的子内容标题 ID、接收来自发送/接收单元 305 的
加密子内容、黑名单和器件失效列表、接收来自加密单元 306 的加密
子内容，并向存储卡 600 输出所接收的子内容标题 ID、加密子内容
密钥、加密子内容、黑名单和器件失效列表。

（11）解密单元 311
解密单元 311 从信息存储单元 309 中读取对应于子内容标题 ID
的子内容密钥。

而且，解密单元 311 从驱动单元 307 接收绑定密钥，从散列单元 315 接收散列值 H，并通过将所接收的散列值 H 和所接收的绑定密钥该该顺序连接来产生密钥。接着，解密单元 311 通过利用所产生的密钥对所读取的加密子内容密钥应用解密算法 D2 来产生子内容密钥，并将所产生的子内容密钥输出到解密单元 313。

这里，解密算法 D2 对应于加密算法 E2，是用于对由加密算法 E2 加密的密码解密的算法。

（12）解密单元 313

解密单元 313 从信息存储单元 309 中读取对应于子内容标题 ID 的加密子内容。

接着，解密单元 313 从解密单元 311 接收子内容密钥，并通过利用所接收的子内容密钥对所读取的加密子内容应用解密算法 D1 来产生子内容，并向重放单元 312 输出所产生的子内容。

这里解密算法 D1 对应于加密算法 E1，是用于对由加密算法 E1 加密的密码解密的算法。

（13）提取单元 316

提取单元 316 经由驱动单元 307 从 DVD 500 中读取主内容，并从所读取的主内容中提取特征以产生特征信息。然后，提取单元 316 从信息存储单元 309 中读取黑名单，并判断所产生的特征信息是否包含在所读取的黑名单上。当判断包含特征信息时，认为 DVD 500 为盗版盘，且提取单元 316 向控制单元 301 输出指令以停止随后的处理。当判断不包含特征信息时，提取单元 316 向控制单元 301 输出指令以继续处理。

（14）重放单元 312

重放单元 312 接收子内容，并由该接收的子内容产生视频信号，并将所产生的视频信号输出到显示器 351，且还由所接收的子内容产生音频信号，并将所产生的音频信号输出到扬声器 352。

1.5 存储卡 600 的结构
如图6中所示，存储卡600由输入/输出单元601、认证单元602和信息存储单元603构成。

存储卡600为类似于DVD制造设备100的计算机系统。存储卡600通过微处理器根据计算机程序的操作来实现其功能。

存储卡600安装在主播放器300或子播放器400中。

存储卡600从其所安装的主播放器300和子播放器400的中接收信息，并将所接收的信息写入信息存储单元603。

而且，随着来自主播放器300或子播放器400的指令，存储卡600从信息存储单元603中读取信息，并将所读取的信息输出到主播放器300或子播放器400。

（1）信息存储单元603

如图6中所示，信息存储单元603具有用于存储子内容标题621、加密子内容密钥622、加密子内容623、黑名单624和器件失效列表625的区域。

这些与先前所述相同，因此略去描述。

（2）输入/输出单元601

输入/输出单元601在信息存储单元603与主播放器300之间或信息存储单元603与子播放器400之间执行信息的输入/输出和输出。

（3）认证单元602

当将存储卡600安装在主播放器300中时，认证单元602与主播放器300的认证单元314一起执行相互器件验证。认证单元602仅当认证成功时继续随后的处理。当认证失败时，认证单元602结束处理。

当存储卡600安装在子播放器400中时，认证单元602与子播放器400的认证单元414一起执行相互器件认证。认证单元602仅当认证成功时继续随后的处理。当认证失败时，认证单元602结束处理。

1.6子播放器400的结构

如图7中所示，子播放器400由控制单元401、显示单元402、输入单元403、驱动单元407、解密单元408、输入/输出单元410、解密单元411、重放单元412、解密单元413、认证单元414、散列单
元 415、提取单元 416、监视单元 417 和 ID 存储单元 418 构成。

子播放器 400 为类似于 DVD 制造设备 100 的计算机系统。子播放器 400 通过微处理器根据计算机程序的操作来实现其功能。

（1）输入单元 403

输入单元 403 接收来自用户的对要被重放的子内容的指定，并经有输入/输出单元 410 从存储卡 600 中获取指定子内容的标题 ID。接着，输入单元 403 向控制单元 401 输出所获取的子内容标题 ID。

（2）控制单元 401

控制单元 401 接收子内容标题 ID，并根据所接收的子内容标题 ID 来产生主内容标题 ID。这里，用于产生主内容标题 ID 的方法是基于先前描述的命名标题 ID 的规则。接着，控制单元 401 向驱动单元 407 输出所产生主内容标题 ID。

（3）驱动单元 407

驱动单元 407 从控制单元 401 接收主内容标题 ID，并从 DVD 500 中读取对应于所接收的主内容标题 ID 的绑定密钥，并向解密单元 411 输出所读取的绑定密钥。

（4）认证单元 414

认证单元 414 与存储卡 600 的认证单元 602 一起执行相互的器件认证。当器件认证成功时，该认证单元继续随后的处理。当器件认证失败时，所述各种设备停止随后的处理。

（5）输入/输出单元 410

当相互的器件认证成功时，输入/输出单元 410 向存储器卡 600 输出请求以读取黑名单、加密子内容密钥和加密子内容。

接着，输入/输出单元 410 从存储卡 600 中接收黑名单、加密子内容密钥和加密子内容。

（6）提取单元 416

提取单元 416 经由驱动单元 407 从 DVD 500 中读取主内容，并通过从所读取的主内容中提取特征来产生特征信息。接着，提取单元 416 从输入/输出单元 410 中接收黑名单，并判断所产生的特征信息是否包含在黑名单中。
当判断该特征信息包含在黑名单中时，认为 DVD 500 为盗版盘，且提取单元 416 向控制单元 401 输出指令以停止随后处理。此时，控制单元 401 控制各种构成元件以便于停止随后的处理。这样，子播放器 400 停止子内容的重放。

当判断特征信息不包含在黑名单中时，处理继续。

(7) 散列单元 415

当提取单元 416 判断所产生的特征信息不包含在黑名单上时，散列单元 415 从输入/输出单元 410 中接收黑名单，通过对该黑名单应用散列函数 Hash 来产生散列值 H=Hash（黑名单），并将所产生的散列值 H 输出到解密单元 411。

(8) 解密单元 411

解密单元 411 从驱动单元 407 接收绑定密钥，从散列单元 415 接收散列值 H，通过将所接收的散列值 H 与所接收的绑定密钥按这一顺序连接来产生密钥，通过使用所产生的密钥对所读取的加密子内容密钥应用解密算法 D2，来产生子内容密钥，并将所产生的子内容密钥输出到解密单元 413。

(9) 解密单元 413

解密单元 413 从输入/输出模块 410 接收加密的子内容。此外，解密单元 413 从解密单元 411 接收子内容密钥，通过利用所接收的子内容密钥对所接收的加密内容应用解密算法 D1 来产生子内容，并将所产生的子内容输出到重放单元 412。

(10) 重放单元 412

重放单元 412 从解密单元 413 接收子内容，由所接收的子内容来产生视频信号并将所产生的视频信号输出到显示器 417，且还由所接收的子内容产生音频信号，并将所产生的音频信号输出到扬声器 451。

1.6 DVD 制造设备 100 的操作

下面利用图 8 中的流程图，来描述 DVD 制造设备 100 的操作。

输入单元 103 从操作者接收用于向 DVD 写入的操作或者用于结束
向 DVD 写入的操作，并将示出所接收的操作的指令信息输出到控制单元 101（步骤 S101）。

当控制单元 101 接收到示出结束向 DVD 写入的指令信息（步骤 S102）时，控制单元 101 结束 DVD 制造设备 100 的处理。

当控制单元 101 接收到示出向 DVD 写入的指令信息（步骤 S102）时，输入单元 103 额外地接收来自用户的主内容标题 ID，并将所接收的主内容标题 ID 输出到控制单元 101，且控制单元 101 接收该标题 ID（步骤 S103）。

接着，根据控制单元 101 的控制，加密单元 105 从主内容表 121 中读取与其输入已被接收的标题 ID 对应的主内容和主内容密钥（步骤 S104）。加密单元 105 通过利用所读取的内容密钥作为密钥向所读取的主内容应用加密算法 E1 来产生加密主内容，并将所产生的加密主内容输出到输出单元 107（步骤 S105）。

然后，根据控制单元 101 的控制，绑定密钥产生单元 106 产生对于该 DVD 唯一的随机号，并将所产生的随机号作为绑定密钥输出到输出单元 107（步骤 S106）。

接着，输出单元 107 从控制单元 101 接收标题 ID，从加密单元 105 接收加密主内容，从绑定密钥产生单元 106 接收绑定密钥，然后将所接收的主内容标题 ID、绑定密钥和加密主内容写入到 DVD（步骤 S107）。接着，DVD 制造设备 100 返回步骤 S101 并重复该处理。

1.7 主播放器 300 用于获取子内容的操作

下面利用于 9 至 11 中的流程图来描述主播放器 300 用于获取子内容的操作。

主播放器 300 的输入单元 303 接收来自用户的获取子内容的获取请求，并将所接收的获取请求输出到控制单元 301。控制单元 301 从输入单元 303 接收获取请求（步骤 S121）。另外，控制单元 301 控制驱动单元 307 使得驱动单元 307 读取该标题 ID，且控制单元 301 从驱动单元 307 接收标题 ID（步骤 S122）。

接着，控制单元 301 将内部存储的用户 ID、子内容获取请求和主
内容标题 ID 经由发送/接收单元 305 和因特网 10 发送到内容供给设备 200 （步骤 S123）。

接着，内容供给设备 200 的控制单元 201 经由因特网 10 和发送/接收单元 207 从主播放器 300 中接收用户 ID、子内容获取请求和主内容标题 ID （步骤 S123）。

接着，主播放器 300 的认证单元 304 和内容供给设备 200 的认证单元 208 执行相互器件认证 （步骤 S124、S125）。

当认证单元 304 和认证单元 208 的任意一个没有通过器件认证时，或当二者均没有通过器件认证 （步骤 S126、S127）时，该设备结束处理。

仅当认证单元 304 和认证单元 208 都在器件认证中成功 （步骤 S126、S127）时，该处理才进行到下一步骤。

接着，根据控制单元 201 的控制，内容供给设备 200 的加密单元 206 从信息存储单元 204 中读取包括子内容标题 ID 的子内容信息，并从所读取的子内容信息中提取子内容和子内容密钥。根据控制单元 201 的控制，发送/接收单元 207 从信息存储单元 204 中读取黑名单 222 和器件失效列表 223 （步骤 S130）。

接着，根据控制单元 201 的控制，加密单元 206 通过利用该子内容密钥作为密钥对该内容采用加密算法 E1 来产生加密的子内容，并将所产生的子内容和子内容密钥输出到发送/接收单元 207 （步骤 S131）。

然后，根据控制单元 201 的控制，发送/接收单元 207 经由因特网 10 向主播放器 300 发送加密子内容、子内容密钥、黑名单和器件失效列表 （步骤 S132）。

主播放器 300 的发送/接收单元 305 经由因特网 10 从内容供给设备 200 接收加密子内容、子内容密钥、黑名单和器件失效列表，并根据控制单元 301 的控制，向加密单元 306 输出所接收的子内容密钥，向输入/输出单元 310 输出所加密的子内容，向输入/输出单元 310 输出黑名单和器件失效列表，并向散列单元 315 输出黑名单 （步骤 S132）。
驱动单元 307 从 DVD 500 接收对应于主内容标题 ID 的绑定密钥，并向加密单元 306 输出所读取的绑定密钥（步骤 S133）。接着，散列单元 315 从发送/接收单元 305 中接收黑名单，通过对所接收的黑名单应用散列函数 Hash 来计算散列值 H，并向加密单元 306 输出所计算的散列值 H（步骤 S134）。

接着，加密封单元 306 从驱动单元 307 接收绑定密钥，从散列单元 315 中接收散列值 H，并从发送/接收单元 305 中接收子内容密钥。加密单元 306 通过将所接收的散列值 H 和所接收的绑定密钥按照上述顺序合并来产生密钥，并通过利用所产生的密钥对所接收的子内容应用加密算法 E2 来产生密钥子内容密钥（步骤 135）。

然后，控制单元 301 向信息存储单元 309 写入子内容标题 ID，加密单元 306 向信息存储单元 309 写入加密子内容，并且发送/接收单元 305 向信息存储单元 309 写入加密子内容（步骤 S136）。

接着，当没有信息写入存储卡 600（步骤 S137）时，主播放器 300 结束子内容获取处理。

另一方面，当有信息写入存储卡 600（步骤 S137）时，主播放器 300 的认证单元 314 和存储卡 600 的认证单元 602 执行相互的器件认证（步骤 S138、S139）。

当认证单元 314 或认证单元 602 没有通过器件认证时，或当二者均没有通过器件认证（步骤 S140、S141）时，设备结束处理。

仅当认证单元 314 和认证单元 602 在器件认证中都成功（步骤 S140、S141）时，该处理继续进行到下一步骤。

输入/输出单元 310 从控制单元 301 接收子内容标题 ID，从发送/接收单元 305 接收加密子内容、黑名单和器件失效列表，从加密单元 306 接收加密子内容密钥，并向存储卡 600 输出所接收的子内容标题 ID、加密子内容密钥、加密子内容、黑名单和器件失效列表（步骤 S142）。

存储卡 600 的输入/输出单元 601 从主播放器 300 接收子内容标题 ID、加密子内容密钥、加密子内容、黑名单和器件失效列表（步骤 S142），并将相互一致的所接收的子内容标题 ID、加密子内容密钥、
加密子内容，黑名单和器件失效列表写入信息存储单元 603（步骤 S143）。

1.8 内容供给设备 200 和主播放器 300 进行相互认证的操作

下面利用图 12 中的流程图来描述内容供给设备 200 和主播放器 300 进行相互认证的操作。注意，这里所述的相互认证的操作为在图 9 中的流程图中的步骤 S124 至 S127 的操作的细节。

值得注意的是，内容供给设备 200 的认证单元 208 经由发送/接收单元 207、因特网 10 和主播放器 300 的发送/接收单元 305 执行用于与认证单元 304 的相互认证的信息的发送和接收。同样，主播放器 300 的认证单元 304 经由发送/接收单元 305、因特网 10 和内容供给设备 200 的发送/接收单元 207 执行用于与内容供给设备 200 的认证单元 208 的相互认证的信息的发送和接收。值得注意的事，在下文中，将信息简化地描述为在认证单元 304 与认证单元 208 之间发送/接收，并省略其间路径的叙述。

认证单元 208 产生随机号 R1（步骤 S161），并将所产生的随机号 R1 发送到认证单元 304（步骤 S162）。认证单元 208 通过对随机号 R1，应用加密算法 E4 来产生密码 A1（步骤 S163）。

另一方面，认证单元 304 从认证单元 208 接收随机号 R1（步骤 S162），并且通过与所接收的随机号 R1，应用加密算法产生密码 B1（步骤 S164），并将所产生的密码 B1 发送到认证单元 208（步骤 S165）。

接着，认证单元 208 从认证单元 304 中接收密码 B1（步骤 S165），并判断所产出的密码 A1 与所接收的密码 B1 是否相匹配。当两者不匹配（步骤 S166）时，认证单元 208 认为认证失败，并向控制单元 201 和发送/接收单元 207 输出指令以停止随后与主播放器 300 之间的信息发送和接收。

同时，认证单元 304 产生随机号 R2（步骤 S167），向认证单元 208 发送所产生的随机号 R2（步骤 S168），并通过与所产生的随机号 R2，应用加密算法 E5 来产生密码 A2（步骤 S170）。
接着，当认证单元 208 判断所产生的密码 A1 与所接收的密码 B1 匹配（步骤 S166）时，认证单元 208 认为认证成功，另外从认证单元 304 接收随机号 R2（步骤 S168），通过接收的随机号码 R2 应用加密算法 E5 来产生密码 B2（步骤 S169），并将所产生的密码 B2 发送到认证单元 304（步骤 S171）。

接着，认证单元 304 从认证单元 208 中接收密码 B2（步骤 S171），判断所产生的密码 A2 与所接收的密码 B2 是否匹配，当两者不匹配（步骤 S172）时，认为认证失败，并向控制单元 301 和发送/接收单元 305 输出指令以停止随后与内容供给设备 200 之间的信息发送和接收。

当两者匹配（步骤 S172）时，认证单元 304 认为认证成功。

1.9 主播放器 300 用于重放子内容的操作

下面利用图 13 中的流程图来描述主播放器 300 用于重放子内容的操作。

主播放器 300 的输入单元 303 接收来自用户的要被重放的子内容指示，获取该子内容的标题 ID（已接收关于该子内容的指示），并将所获取的子内容标题 ID 输出到控制单元 301（步骤 S201）。

接着，控制单元 301 由所接收的子内容标题 ID 来产生主内容标题 ID，并将所产生的主内容标题 ID 输出到驱动单元 307。驱动单元 307 从控制单元 301 接收该标题 ID，从 DVD 500 中读取与所接收的标题 ID 对应的绑定密钥，并向解密单元 311 输出所读取的绑定密钥（步骤 S202）。

接着，解密单元 311 从信息存储单元 309 中读取对应于该子内容标题 ID 的加密子内容密钥，解密单元 313 从信息存储单元 309 读取对应于该子内容标题 ID 的加密子内容，而散列单元 315 从信息存储单元 309 中读取对应于该子内容标题 ID 的黑名单（步骤 S203）。

接着，提取单元 316 经由驱动单元 307 从 DVD 500 中读取加密的主内容，通过对加密主内容解密来产生主内容，并从所产生的主内容中提取特征以产生特征信息（步骤 S204）。提取单元 316 从信息存储单元 309 中读取黑名单，并判断所产生的特征信息是否包含在黑名单
上。当所产生的特征信息包含在黑名单上（步骤 S205）时，提取单元 316 认为 DVD 500 为盗版盘，并向控制单元 301 输出指令以停止随后的处理。控制单元 301 控制各种构成元件以停止随后的处理。这样，主播放器 300 停止对该子内容的重放。

当提取单元 316 判断所产生的特征信息不包含在所读取的黑名单上（步骤 S205）时，散列单元 315 则从信息存储单元 309 中读取黑名单，通过对所读取的黑名单应用散列函数 Hash 来产生散列值 H=Hash（黑名单），并将所产生的散列值 H 输出到解密单元 311（步骤 S206）。解密单元 311 从驱动单元 307 中接收绑定密钥，从散列单元 315 中接收散列值 H，并通过将所接收的散列值 H 与所接收的绑定密钥按上述顺序连接来产生密钥。然后解密单元 311 通过利用所产生的密钥对所读取的加密子内容应用解密算法 D2 来产生子内容密钥，并将所产生的子内容密钥输出到解密单元 313（步骤 S207）。

解密单元 313 从解密单元 311 中接收子内容密钥，通过利用所接收的子内容密钥对所读取的加密子内容应用解密算法 D1 来产生子内容，并向重放单元 312 输出所产生的子内容（步骤 S208）。

重放单元 312 接收该子内容，由所接收的子内容产生视频信号，并将所产生的视频信号输出到显示器 351，且还由所接收的子内容产生音频信号，并将所产生的音频信号输出到扬声器 352（步骤 S209）。

1.10 子播放器 400 用于重放子内容的操作

下面利用图 14 至 15 中示出的流程图来描述子播放器 400 用于重放子内容的操作。

子播放器 400 的输入单元 403 从用户接收关于要被播放的子内容的指示，并从存储卡 600 中获取该子内容的标题 ID（已接收了关于该子内容的指示），并向控制单元 401 输出所获取的子内容标题 ID（步骤 S301）。

接着，控制单元 401 由所接收的子内容标题 ID 产生主内容标题 ID，并向驱动单元 407 输出所产生的主内容标题 ID。驱动单元 407 从控制单元 401 中接收该标题 ID，从 DVD 500 中读取对应于所接收
的标题 ID 绑定密钥，并向解密单元 411 输出所读取的绑定密钥（步骤 S302）。

接着，子播放器 400 和存储卡 600 执行相互器件认证（步骤 S303 至 S304）。当相互器件认证失败（步骤 S305、S306）时，该设备停止随后的处理。

当相互器件认证成功（步骤 S305、S306）时，输入/输出单元 410 向存储卡 600 输出请求以读取黑名单、加密子内容密钥和加密子内容（步骤 S307）。

存储卡 600 的输入/输出单元 601 接收该读取请求（步骤 S307），从信息存储单元 603 中读取黑名单、加密子内容密钥和加密子内容，并将所读取的黑名单、加密子内容密钥和加密子内容输出到子播放器 400。输入/输出单元 410 接收黑名单、加密子内容密钥和加密子内容（步骤 S309）。

提取单元 416 经由驱动单元 407 从 DVD 500 中读取加密主内容，通过对加密主内容加密产生主内容，并从所产生的主内容中提取特征以产生特征信息（步骤 S310）。提取单元 416 从输入/输出单元 410 中接收黑名单，并判断所产生的特征信息是否包含在黑名单上。当所产生的特征信息包含在黑名单上（步骤 S311）时，提取单元 416 认为该 DVD 为盗版盘，并向控制单元 401 输出指令以停止随后的处理。控制单元 401 控制各种构成元件以停止随后的处理。这样，子播放器 400 停止对子内容的播放。

当提取单元 416 判断所产生的特征信息不包含在所读取的黑名单上（步骤 S311）时，散列单元 415 则从输入/输出单元 410 中接收黑名单，通过对所接收的黑名单应用散列函数 Hash 来产生散列值 H=Hash（黑名单），并将所产生的散列值 H 输出到解密单元 411 （步骤 S312）。解密单元 411 从驱动单元 407 接收绑定密钥，从散列单元 415 中接收散列值 H，并将所接收的散列值 H 与所接收的绑定密钥按上述顺序连接来产生密钥。然后解密单元 411 通过利用所产生的密钥对所读取的加密子内容应用解密算法 D2 来产生子内容密钥，并将所生产的子内容密钥输出到解密单元 413（步骤 S313）。
解密单元 413 从解密单元 411 接收子内容密钥，通过利用所接收的子内容密钥对所读取的加密子内容应用解密算法 D1 来产生子内容，并将所产生的子内容输出到重放单元 412（步骤 S314）。

重放单元 412 接收子内容，由所接收的子内容产生视频信号并将所产生的视频信号输出到显示器 417，并且由所接收的子内容产生音频信号并将所产生的音频信号输出到扬声器 451（步骤 S315）。

1.12 子播放器 400 和存储卡 600 用于相互认证的操作

下面利用图 16 中的流程图来描述子播放器 400 和存储卡 600 用于相互认证的操作。值得注意的是，这里描述的用于相互认证的操作为在图 14 中流程图的步骤 S303 至 S306 的操作细节。

子播放器 400 的认证单元 414 经由输入/输出单元 410 和存储卡 600 的输入/输出单元 601 执行用于与认证单元 602 的相互认证的信息的发送和接收。同样，存储卡 600 的认证单元 602 经由输入/输出单元 600 和子播放器 400 的输入/输出单元 410 执行用于与认证单元 414 的相互认证的信息的发送和接收。值得注意的是下文中，信息被简化描述为在认证单元 414 与认证单元 602 之间发送/接收，而省略其间路径的描述。

认证单元 414 和认证单元 602 利用与图 12 中的流程图中示出的相互认证相同的方法执行器件认证（步骤 S331）。

当相互器件认证成功时，认证单元 602 从认证单元 414 中请求器件 ID（步骤 S332）。

认证单元 414 接收该请求（步骤 S332），从 ID 存储单元 418 读取器件 ID（步骤 S333），并向认证单元 602 输出所读取的器件 ID（步骤 S334）。

认证单元 602 接收该器件 ID（步骤 S334），判断所接收的器件 ID 是否包含在存储于信息存储单元 603 中的器件失效列表 625 中，并且当器件失效列表 625 不包含该器件 ID（步骤 S335）时，认为认证成功。

当器件失效列表 625 包含器件 ID（步骤 S335）时，认证单元 602
认为子播放器 400 为失效设备，并控制输入/输出单元 601 停止随后的操作。

2. 变型

值得注意的是，虽然已经根据上述实施例描述了本发明，但是本发明不限于该实施例。下述情形包含于本发明中。


和上面实施例所描述的一样，仅当被写入“Galaxy Wars: The Birth of the Galaxy Allies”的 DVD 和被写入子内容的存储卡都装在主播放器中时，主播放器才根据用户指令重放写入存储卡中的加密子内容。这使得用户能够重放和欣赏短片“Galaxy Wars: The Secret Story of the Birth of the Galaxy Allies”。这同样适用于子播放器。

这里，用户租借其上分别记录电影“Galaxy Wars: The Takeover”和“Galaxy Wars: The Demise of Allies”作为主内容的 DVD。这些电影为“Galaxy Wars: The Birth of the Allies”的续集。

当用户将记录有加密子内容的存储卡和所借的记录有“Galaxy Wars: The Demise of Allies”的 DVD 都装在主播放器中时，主播放器根据用户指令来重放写入在存储卡中的加密子内容。同样在这种情况下，用户能够重放和欣赏短片“Galaxy Wars: The Secret Story of the Birth of the Galaxy Allies”。这同样适用于子播放器。

这样，如上面实施例中所述那样，当用户通过合法购买等而合法拥有记录有主内容 A 的 DVD 时，主播放器可以从内容供给设备中获取涉及主内容 A 的子内容 B，并将其写入到存储卡中。
接着，假设用户通过除购买之外的合法方法，如租借，来获取分别记录有与主内容 A 相关的主内容 C 和 D 的 DVD。这里，子内容可记帐，且当将存储卡和其上记录主内容 C 的 DVD 都装在主播放器中时，主播放器能够重放记录在存储卡上的子内容。当将存储卡和记录有主内容 D 的 DVD 都装在主播放器中时，情况是相同的。而且，这还适用于子播放器。

下面描述了用于实现上述变型的具体结构。

内容发布系统 1b 具有与内容发布系统 1 相似的结构，但是，如图 17 中所示，取代内容供给设备 200、主播放器 300 和子播放器 400，内容发布系统 1b 包括内容供给设备 200b、主播放器 300b 和子播放器 400b。

用户合法购买 DVD 500A。另外，用户租借 DVD 500C 和 DVD 500D。

在 DVD 500A 上记录主内容 A、保密密钥 SA、公共密钥 PA、公共密钥 PC 和公共密钥 PD。这里，保密密钥 SA 为对应于主内容 A 的保密密钥，而公共密钥 PA 为对应于主内容 A 的公共密钥。而且，公共密钥 PC 和公共密钥 PD 为分别对应于稍后所描述的主内容 C 和主内容 D 的公共密钥。

主内容 C 和保密密钥 SC 记录在 DVD 500C 上。主内容 C 为涉及主内容 A 的内容。保密密钥 SC 为对应于主内容 C 的保密密钥。

主内容 D 和保密密钥 SD 记录在 DVD 500D 上。主内容 D 为涉及主内容 A 的内容。保密密钥 SD 为对应于主内容 D 的保密密钥。

保密密钥和公共密钥遵守公共密钥加密方法。

公共密钥 PA 用于对纯文本加密。保密密钥 SA 对应于公共密钥 PA，并用于对利用公共密钥 PA 而产生的密码解密。

而且，公共密钥 PC 用于对纯文本加密。保密密钥 SC 对应于公共密钥 PC，并用于对利用公共密钥 PC 而产生的密码解密。

此外，公共密钥 PD 用于对纯文本加密。保密密钥 SD 对应于公共密钥 PD，并用于对利用公共密钥 PD 而产生的密码解密。

用户将 DVD 500A 和存储卡 600 装在主播放器 300b 中，并命令主播放器 300b 从内容供给设备 200b 中获取涉及主内容 A 的子内容。此
时，信息仍未记录在存储卡 600b 上。

主播放器 300b 向内容供给设备 200b 输出指令以获取子内容。内容供给设备 200b 通过利用子内容密钥对该子内容加密来产生加密子内容（步骤 S401）。接着，内容供给设备 200b 向主播放器 300b 提供子内容密钥（步骤 S402），并向主播放器 300b 提供加密子内容（步骤 S403）。

主播放器 300b 从内容供给设备 200b 获取子内容密钥（步骤 S402），并从内容供给设备 200b 获取加密子内容（步骤 S403）。接着，主播放器 300b 从 DVD 500A 中读取公共密钥 PA、公共密钥 PC 和公共密钥 PD（步骤 S404），并通过分别利用所读取的公共密钥 PA、公共密钥 PC 和公共密钥 PD 对所接收的子内容密钥加密来产生加密子内容密钥 EA、加密子内容密钥 EC 和加密子内容密钥 ED（步骤 S405）。主播放器 300b 将所产生的加密子内容密钥 EA、加密的子内容密钥 EC 和加密的子内容密钥 ED 写入到存储卡 600b（步骤 S406），然后将所接收的加密子内容写入到存储卡 600b（步骤 S407）。

这样，将加密子内容密钥 EA、加密子内容密钥 EC、加密子内容密钥 ED 和加密子内容记录在存储卡 600b 中，如图 17 中所示。

接着，用户将记录有加密子内容密钥 EA、加密子内容密钥 EC、加密子内容密钥 ED 和加密子内容的存储卡 600b 和 DVD 500D 一起装在子播放器 400b 中，并命令该子播放器重放记录在存储卡 600b 上的加密子内容。

子播放器 400b 从 DVD 500 中读取保密密钥 SD（步骤 S411），从存储卡 600b 中读取加密子内容密钥 ED（步骤 S412），并通过利用所读取的保密密钥 SD 对加密子内容密钥 ED 解密来产生子内容密钥（步骤 S413）。接着，子播放器 400b 从存储卡 600b 中读取加密子内容（步骤 S414），并通过利用所产生的子内容密钥对所读取的加密子内容解密来产生子内容（步骤 S415）。接着，子播放器 400b 重放该子内容。

这样，当安装了存储卡 600b 和 DVD 500D 时，子播放器 400b 能够对记录在存储器卡 600b 上的加密子内容解密并将其重放。主播放器 300b 以相同方式重放。
而且，当将存储卡 600b 和 DVD 500A 都安装在子播放器 400b 中时，上述情况同样适用。而且，当将存储卡 600b 和 DVD 500C 都安装在子播放器 400b 中时，上述情况同样适用。而且，上述情况同样适用于子播放器 300b。

（2）可以将唯一识别 DVD 500 的盘 ID 记录在 DVD 500 上。在这种情况下，当主播放器 300 从内容供给设备 200 中请求子内容时，主播放器 300 从 DVD 500 中读取该盘 ID，并将所读取的该盘 ID 发送到内容供给设备 200。当向主播放器 300 供给子内容时，内容供给设备 200 可以存储相应的所接收的盘 ID 和子内容。

内容供给设备 200 可以具有如此结构，当其下一次接收从内容供给设备 200 获取子内容的请求时，它不允许供给所接收的标题 ID 和盘 ID 的结合的子内容。这防止了子内容被重复提供。

而且，在出现标题 ID 和磁盘 ID 的相同结合的情况下，子内容的供给者还能够向用户单独收取有关该子内容的付款。

（3）子播放器 400 可以具有诸如硬盘的内部存储单元，读取存储在存储卡 600 上的加密子内容，并将所读取的加密子内容存储在该存储单元中。

（4）主播放器 300 可以从 DVD 500 中读取绑定密钥，并内部存储所读取的绑定密钥。这里，主播放器 300 利用内部存储的绑定密钥对子内容密钥加密。而且，当重放子内容时，主播放器 300 可以利用内部存储的绑定密钥对加密内容解密。这还适用于子播放器 400。

（5）在上述实施例中，主播放器 300 接收子内容和黑名单，并将所接收的子内容和黑名单写入信息存储单元 309，或将所接收的子内容和黑名单写入存储卡 600。

这里，当主播放器 300 下一次接收另一子内容和另一黑名单时，主播放器 300 可以将所接收的子内容写入信息存储单元 309，并将所接收的黑名单写入信息存储单元 309 以覆盖已经存储于信息存储单元 309 的黑名单。或者，主播放器可以将所接收的子内容写入存储卡 600，并将所接收的黑名单写入信息存储单元 309 以覆盖已经存储于信息存储单元 309 中的黑名单。
这样，主播放器 300 和存储卡 600 仅存储最近发送的黑名单。

（6）下面是当主播放器 300 从内容供给设备 200 获取子内容时的可能结构。

当内容供给设备 200 和主播放器 300 根据各自的认证单元 208 和认证单元 304 来执行相互的器件认证，它们共享对话密钥 Kses。特别地，在图 12 中示出的内容供给设备 200 与主播放器 300 之间的相互认证处理中，内容供给设备 200 与主播放器 300 中的认证单元 208 和认证单元 304 分别利用下述表达式计算对话密钥 Kses，

对话密钥 Kses = E6 (R1 (+) R2)

这里，R1 和 R2 为由图 12 中示出的内容供给设备 200 和主播放器 300 在相互认证处理中获取的随机号。

此外，（+）为表示异或运算符。

而且，Y = E6 (X) 表示通过向纯文本 X 应用加密算法 E6 获得的密码 Y。这里，加密算法 E6 例如为 DES 加密。

接着，主播放器 300 通过利用对话密钥 Kses 对从 DVD 500 读取的绑定密钥加密来产生加密绑定密钥，并将加密绑定密钥发送到内容供给设备 200。

内容供给设备 200 接收加密绑定密钥，并通过利用对话密钥 Kses 对加密绑定密钥解密来产生绑定密钥。

接着，内容供给设备 200（a）通过利用该绑定密钥对子内容加密来产生加密子内容密钥，且然后通过利用该对话密钥 Kses 对加密子内容密钥进一步加密来产生双加密子内容密钥，（b）通过利用该子内容密钥对子内容加密来产生加密子内容，且然后通过利用对话密钥 Kses 对加密子内容进一步加密来产生双加密子内容，以及（c）通过利用对话密钥 Kses 对黑名单加密来产生加密黑名单。然后内容供给设备 200 将双加密子内容密钥、双加密子内容和加密黑名单发送到主播放器 300。

接着，主播放器 300 接收双加密子内容密钥、双加密子内容和加
密黑名单。然后主播放器 300（a）通过利用对话密钥 Kses 对双加密子内容密钥解密来产生加密子内容密钥，（b）通过利用对话密钥 Kses 对双加密子内容解密来产生加密子内容，以及（c）通过利用对话密钥 Kses 对加密黑名单解密来产生黑名单。

接着，主播放器 300 将子内容标题 ID、加密子内容密钥、加密子内容和黑名单写入信息存储单元 309。而且，主播放器 300 将子内容标题 ID、加密子内容密钥、加密子内容和黑名单写入存储卡 600 中。

主播放器 300 将加密子内容按照下述方法写入存储卡 600。

当在主播放器 300 与存储卡 600 之间执行相互器件认证时，由认证单元 314 和认证单元 602 按照先前描述的方式共享对话密钥 Kses。

主播放器 300（a）通过利用对话密钥 Kses 对子内容加密来产生双加密的子内容密钥，（b）通过利用对话密钥 Kses 对加密的子内容加密来产生双加密的子内容，以及（c）通过利用对话密钥 Kses 对加密黑名单加密来产生加密黑名单。然后主播放器 300 将子内容标题 ID、双加密子内容密钥、双加密子内容和加密黑名单发送到存储卡 600。

存储卡 600 接收子内容标题 ID、双加密子内容密钥、双加密子内容和加密黑名单。存储卡 600（a）通过利用对话密钥 Kses 对双加密子内容密钥解密来产生加密子内容密钥，（b）通过利用对话密钥 Kses 对双加密子内容解密来产生加密子内容，以及（c）通过利用对话密钥 Kses 对加密黑名单解密来产生黑名单。接着，存储卡 600 将子内容标题 ID、加密子内容密钥、加密子内容和黑名单写入信息存储单元 603。

而且，主播放器 300 按照下述方式从存储卡 600 读取加密子内容。

当在主播放器 300 与存储卡 600 之间执行相互器件认证时，由认证单元 314 和认证单元 602 按照先前描述的方式共享对话密钥 Kses。

存储卡 600（a）通过利用对话密钥 Kses 对加密子内容加密来产生双加密的内容密钥，（b）通过利用对话密钥 Kses 对加密的子内容加密来产生双加密子内容，以及（c）通过利用对话密钥 Kses 对加密黑名单加密来产生加密黑名单。接着，存储卡 600 将子内容标题 ID、双加密子内容密钥、双加密子内容和加密黑名单发送到主播放器 300。
主播放器 300 接收子内容标题 ID、双加密子内容密钥、双加密子内容和加密黑名单。主播放器 300 (a) 通过利用对话密钥 Kses 对双加密子内容密钥解密来产生加密子内容密钥，(b)通过利用对话密钥 Kses 对双加密子内容解密来产生加密子内容，以及 (c) 通过利用对话密钥 Kses 对加密黑名单解密来产生黑名单。

(7) 虽然在该实施例中利用子内容密钥对子内容加密，但是对于子内容密钥的存在并非强制性的。

换句话说，内容供给设备 200 可以利用绑定密钥对子内容加密来产生加密子内容，并将所产生的加密子内容发送到主播放器 300。

主播放器 300 接收加密子内容，并将加密子内容存储在信息存储单元 300 和存储卡 600 中。当重放加密子内容时, 主播放器 300 通过利用绑定密钥对加密内容解密来产生子内容，并重放所产生的子内容。

(8) 虽然将记录有主内容的记录介质描述为仅能向其一次性写入信息的 ROM 型 DVD，但是也可以使用另一种类型的记录介质。例如，和 CD-ROM 一样，ROM 型 BD (Blu-ray 盘) 是可用的。此外，记录有主内容的记录介质并不限于为 ROM 型记录介质。可以使用可读/可写记录介质。

(9) 本发明可以是上文所示出的方法。而且，该方法可以为由计算机实现的计算机程序，且可以是计算机程序的数字信号。

而且，本发明可以为存储计算机程序或数字信号的计算机可读记录介质设备，诸如软盘、硬盘、CD-ROM、MO、DVD、DVD-ROM、DVD RAM、BD (Blu-Ray 盘)、或半导体存储器。而且，本发明可以为记录在前述记录介质设备的任意一种上的计算机程序或数字信号。

而且，本发明可以为在电子通信线、无线或有线通信线、或以因特网为典型代表的网络上传输的计算机程序或数字信号。

此外，本发明可以是包括微处理器和存储器的计算机系统，该存储器存储该计算机程序，且微处理器根据计算机程序而操作。

此外，通过将程序或数字信号传输到记录介质设备，或者通过经
由网络等来传输程序或数字信号, 该程序或数字信号可以由另一个独立的计算机系统执行。

（10）本发明可以为上述实施例的任意组合和变形。

3. 发明效果

如上所述, 本发明为一种内容发布系统, 该内容发布系统分配涉及主内容的子内容, 并包括内容供给设备、内容记录设备和内容重放设备。

内容供给设备输出子内容。

内容记录设备（a）从便携式第一存储介质中读取特征信息，第一存储介质预存储特征信息和作为主内容的数码制品, 该特征信息为第一存储介质的特征, (b) 获取输出的子内容, (c) 根据所读取的特征信息对所获取的子内容加密, 以产生加密的子内容, 和 (d) 将所产生的加密子内容写入便携式第二存储介质。

内容重放设备（a）从第一存储介质中读取特征信息, (b) 从第二存储介质中读取加密子内容, (c) 根据所读取的特征信息来对所读取的加密子内容解密, 以产生重放子内容, 和 (d) 重放所产生的重放子内容。

而且, 本发明为记录涉及主内容的子内容的内容记录设备, 包括:

读取单元, 该读取单元可操作以从便携式第一存储介质中读取特征信息, 第一存储介质存储特征信息和作为主内容的数码制品, 该特征信息为第一存储介质的特征;

获取单元, 该获取单元可操作以获取子内容;

加密单元, 该加密单元可操作以根据特征信息对所获取的子内容加密, 以产生加密子内容; 和

写入单元, 该写入单元可操作以将所产生的加密子内容写入便携式第二存储介质。

而且, 本发明为重放涉及主内容的子内容的内容重放设备, 该内容重放设备包括:

第一读取单元, 该第一读取单元可操作以从便携式第一存储介质中读取特征信息, 第一存储介质预存储特征信息和为数码制品的主内
内容，该特征信息为第一存储介质的特征；

第二读取单元，第二读取单元可操作以从便携式第二存储介质中读取加密子内容，第二存储介质预存储加密子内容，该加密子内容是根据特征信息对子内容加密来产生的；

解密单元，该解密单元可操作以根据所读取的特征信息对所读取的加密子内容解密，以产生重放子内容；和

重放单元，该重放单元可操作以重放所产生的重放子内容。

根据所述的结构，内容记录设各通过根据存储于第一存储介质上的特征信息对子内容加密来产生加密子内容，并将加密内容写入便携式第二存储介质中。内容重放设备根据从第一存储介质中读取的特征信息来对加密子内容解密。因此，仅当第一存储介质和第二存储介质都安装在内容重放设备中时，内容重放设备能够对加密子内容解密。这样，仅允许存储主内容的第一存储介质的拥有者使用子内容。

这里，在该内容记录设备中，

获取单元还获取与该子内容绑定的黑名单。黑名单包括关于已经记录在非法记录介质上的信息特征的特征信息。该非法记录介质上记录有通过非法复制主内容而产生的非法内容。

写入单元将黑名单写入第二介质中，与该加密子内容绑定。

而且，在内容重放设备中，

第二读取单元还从第二记录介质中读取黑名单。第二记录介质还存储与加密子内容绑定的黑名单。黑名单包括关于已经记录在非法记录介质上的信息特征的特征信息。非法记录介质上记录有通过非法复制主内容而产生的非法内容。

重放单元提取示出存储于第一存储介质上的信息的特征的特征信息，判断所提取的特征信息是否与黑名单中的特征信息相匹配，且当判断为肯定时，禁止重放子内容和记录在第一存储介质上的信息的重放。

根据所述的结构，内容记录设备将黑名单写入第二存储介质，与加密子内容绑定，该黑名单包括示出记录于非法记录介质上的信息的特征的特征信息。内容重放设备从第一存储介质中提取该特征信息，
且当判断所提取的特征信息包含在黑名单中时，禁止重放子内容和存储于第一存储介质上的信息的重放。这样，可以控制记录在非法记录介质上的内容的重放。

这里，在内容记录设备中，

获取单元还获取与子内容绑定的器件失效信息。器件失效信息示出失效的器件。

写入单元将器件失效信息写入第二存储介质，与加密子内容绑定。

此外，在内容重放设备中，

第二存储介质包括信息存储单元和器件认证单元，且

信息存储单元存储加密子内容和与加密子内容绑定的器件失效信息，器件失效信息示出失效器件。

器件认证单元根据器件失效信息判断内容重放设备是否失效，且当判断为肯定时，禁止内容重放设备从信息存储单元中读取信息。

根据所述的结构，内容记录设备将器件失效信息写入第二存储介质，与加密子内容绑定，该器件失效信息示出失效的器件。第二存储介质判断内容重放设备是否失效，且当判断内容重放设备失效时，禁止内容重放设备重放存储在第二存储介质上的信息。这样，可以排除非法的内容重放设备。

此外，本发明为记录子内容的内容记录设备，该子内容涉及第一主内容和第二主内容，该内容记录设备包括：

读取单元，可操作以从便携式第一存储介质中读取第一特征信息，并从便携式第二存储介质中读取第二特征信息，第一存储介质存储表示第一存储介质特征的第一特征信息和表示第二存储介质特征的第二特征信息、以及为数据制品的第一主内容，而第二存储介质存储第二特征信息和为数据制品的第二主内容；

获取单元，该获取单元可操作以获取涉及第一主内容的子内容；

加密单元，该加密单元可操作以根据所读取的第一特征信息来对所获取的子内容加密，以产生第一加密内容，且根据所读取的第二特征信息来对所获取的子内容加密，以产生第二加密子内容；
写入单元，该写入单元可操作以将所产生的第一和第二加密子内容写入便携式第三存储介质。

此外，本发明为重放涉及第一主内容和第二主内容的子内容的内容重放设备，包括：

第一读取单元，该第一读取单元可操作以从便携式第二存储介质中读取第二特征信息，第二存储介质存储第二特征信息和作为数码制品的第二主内容，第二特征信息为第二存储介质的特征；

第二读取单元，该第二读取单元可操作以从第三存储介质中读取第二加密子内容，第三存储介质存储第一加密子内容和第二加密子内容，第一加密子内容是通过根据作为便携式第一存储介质的特征的第一特征信息对子内容加密来产生的，该便携式第一存储介质存储第一特征信息和第一主内容，第二加密子内容是通过根据第二特征信息对第二内容加密来产生的；

解密单元，该解密单元可操作以根据所读取的第二特征信息来对所读取的第二加密子内容解密，以产生重放子内容；和

重放单元，该重放单元可操作以重放所产生的重放子内容。

此外，本发明为发布涉及主内容的子内容的内容发布系统，包括：

内容供给设备，从内容记录设备接收特征信息，根据所接收的特征信息来对子内容加密，以产生加密子内容，并输出所产生的加密子内容，该特征信息为便携式第一存储介质的特征，便携式第一存储介质存储该特征信息和作为数码制品的主内容；

内容记录设备，从第一存储介质中读取特征信息，向内容供给设备发送所读取的特征信息，从内容供给设备获取加密子内容，并将所获取的加密子内容写入便携式第二存储介质；和

内容重放设备，(a)从第一存储介质中读取特征信息，(b)从第二读取介质中读取加密子内容，(c)根据所读取的特征信息对所读取的加密子内容解密，以产生重放子内容，和 (d) 重放所产生的重放内容。

此外，本发明为记录涉及主内容的子内容的内容记录设备，包括：

输出单元，该输出单元可操作以从便携式第一存储介质中读取特
征信息，并将所读取的特征信息输出到内容供给设备，该特征信息为第一存储介质的特征；

获取单元，该获取单元可操作以从内容供给设备中获取加密子内容，加密子内容由内容供给设备通过利用特征信息对子内容加密而产生；和

写入单元，该写入单元可操作以将所获取的加密子内容写入便携式第二存储介质。

工业应用

在制造和发布诸如电影和音乐等数码制品的内容的产业中，可以战略性使用本发明的内容发布系统，换句话说，可重复地且持续地使用。而且，在电子器件制造产业中，可以战略地、且可以重复并持续地制造和出售构成该内容发布系统的内供给设备、内容记录设备和内容重放设备。
图3
子内容获取

内容供给设备

主播放器

接收子内容获取请求

获取主内容标题ID

子内容获取请求、标题ID、用户ID

器件认证

成功

是

结束

记账处理

成功

否

结束

成功

否

结束

读取标题ID、子内容、子内容密钥、黑名单和器件失效列表

利用子内容密钥加密子内容

图9
图10
内容供给设备和主播放器的相互认证

内容供给设备

产生随机号R1

S163

A1 = E4(R1)

S166

A1 = B1

是

结束

（认证失败）

否

B1 = E4(R1)

S165

B1

S162

S164

S167

产生随机号R2

S168

R2

B2 = E5(R1)

S169

S171

B2

A2 = E5(R2)

S170

A2 = B2

（认证失败）

否

是

结束

（认证成功）

（认证成功）

图12
图13
子播放器的重放

子播放器

S301
接子内容的指定

S302
从DVD中读取对应于主内容标题ID的绑定密钥

S303
器件认证

S305
否

S306
成功

S304
器件认证

S307
读取请求

S308
读取

S309
黑名单、加密子内容密钥、加密子内容

S310
从存储于DVD上的主内容中提取特征

S311
特征

不在黑名单上

A13

图14
图15

图示流程如下：

1. **A13**
   - 发列值H=Hash（黑名单）
2. **S312**
   - 利用子列值H和绑定密钥对加密子内容密钥解密
3. **S313**
   - 利用子内容密钥对加密子内容解密
4. **S314**
5. **S315**
   - 重放子内容
在子播放器和存储卡之间的相互认证

图16