

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.



[12] 发明专利说明书

专利号 ZL 200580042810.2

G06F 21/20 (2006.01)
H04N 7/16 (2006.01)
G06F 21/24 (2006.01)
H04N 7/167 (2006.01)
H04L 9/08 (2006.01)

[45] 授权公告日 2009年8月12日

[11] 授权公告号 CN 100527148C

[22] 申请日 2005.12.12

[21] 申请号 200580042810.2

[30] 优先权

[32] 2004.12.13 [33] JP [31] 360436/2004

[32] 2004.12.13 [33] JP [31] 360437/2004

[86] 国际申请 PCT/JP2005/022779 2005.12.12

[87] 国际公布 WO2006/064765 日 2006.6.22

[85] 进入国家阶段日期 2007.6.13

[73] 专利权人 松下电器产业株式会社

地址 日本大阪府

共同专利权人 国立大学法人东京大学

[72] 发明人 中野稔久 野仲真佐男 布田裕一

大森基司 五味刚 古原和邦

今井秀树

[56] 参考文献

CN1082215C 2002.4.3

JP2001-118333A 2001.4.27

US6226747B1 2001.5.1

JP9-167477A 1997.6.24

审查员 夏贝贝

[74] 专利代理机构 永新专利商标代理有限公司

代理人 徐殿军

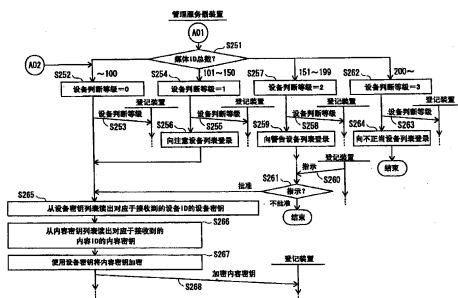
权利要求书4页 说明书56页 附图34页

[54] 发明名称

不正当设备检测装置及不正当设备检测系统

[57] 摘要

提供一种能够发现并确定不正当地制造或改造的设备的设备的不正当设备检测系统。DVD播放器(400a)将自身的设备ID向存储卡(200a)写入。在使用者购入内容时,登记装置(300)从存储卡(200a)读出媒体ID与设备ID,将媒体ID与设备ID向管理服务器装置(100)发送。管理服务器装置(100)根据预先存储的媒体ID及设备ID的组、和接收到的媒体ID及设备ID的组,计算与接收到的设备ID相对应的媒体ID的总数,将计算出的总数与阈值比较。如果为阈值以上,则将接收到的设备ID识别的DVD播放器推测为不正当设备。



1、一种不正当设备检测装置，检测通过仿造制造的不正当的设备，其特征在于，具备：

媒体数存储机构，存储有由保持与对象设备识别符相同的设备识别符的设备所使用的可改写的可移动媒体的媒体数，其中该对象设备识别符是由作为不正当检测的对象的检测对象设备所保持的；

比较机构，将预先设定的不正当阈值与计算出的上述媒体数进行比较；以及

识别符存储机构，在上述媒体数超过上述不正当阈值的情况下，存储上述对象设备识别符。

2、如权利要求1所述的不正当设备检测装置，其特征在于，上述不正当设备检测装置还包括：

取得部，从由上述检测对象设备使用的可改写的对象可移动媒体取得识别该对象可移动媒体的对象媒体识别符、和该检测对象设备所保持的对象设备识别符；

存储部，与由过去成为不正当检测的对象的管理对象设备所保持的管理设备识别符相对应地，存储分别识别由该管理对象设备使用的1个以上的可改写的可移动媒体的1个以上的管理媒体识别符；以及

计算机构，使用所存储的上述管理设备识别符及上述管理媒体识别符、以及所取得的上述对象设备识别符及上述对象媒体识别符，计算与所取得的对象设备识别符相同的设备识别符所对应的管理媒体识别符的数目和对象媒体识别符的数目之和，作为上述媒体数，并将计算出的上述媒体数写入到上述媒体数存储机构中。

3、如权利要求2所述的不正当设备检测装置，其特征在于，

上述比较机构还将比上述不正当阈值小的警告阈值、与计算出的上述媒体数进行比较；

在计算出的上述媒体数为上述不正当阈值以下，且超过上述警告阈值的情况下，上述识别符存储机构还存储所取得的上述对象设备识别符。

4、如权利要求2所述的不正当设备检测装置，其特征在于，

上述设备是将加密的内容解密并再现的再现设备；

上述不正当设备检测装置还包括：

禁止机构，在计算出的上述媒体数超过不正当阈值的情况下，禁止对上述对象可移动媒体输出为了将加密的内容解密而使用的解密密钥；以及

输出机构，在计算出的上述媒体数没有超过不正当阈值的情况下，对上述对象可移动媒体输出上述解密密钥。

5、如权利要求 1 所述的不正当设备检测装置，检测通过仿造制造的不正当的设备，其特征在于，包括：

系列数存储机构，存储有通过保持与对象设备识别符相同的设备识别符的设备来收看收听的内容的视听履历系列的系列数，其中该对象设备识别符是由作为不正当检测的对象的检测对象设备所保持的；

比较机构，将预先设定的不正当阈值与计算出的上述系列数进行比较；以及

存储机构，在上述系列数超过上述不正当阈值的情况下，存储上述对象设备识别符。

6、如权利要求 1 所述的不正当设备检测装置，检测通过仿造制造的不正当的设备，其特征在于，包括：

存储机构，与由过去成为不正当检测的对象的对象设备保持的管理设备识别符相对应地，存储分别识别在该对象设备中收看收听的 1 个以上的内容的 1 个以上的管理内容识别符；

取得机构，从在作为不正当检测的对象的检测对象设备中使用的可改写的对象可移动媒体中，取得分别识别在该检测对象设备中收看收听的 1 个以上的内容的 1 个以上的对象内容识别符、和该检测对象设备保持的对象设备识别符；

提取机构，从上述存储机构提取与所取得的上述对象设备识别符相同的管理设备识别符所对应的 1 个以上的管理内容识别符；

比较机构，将所提取的上述管理内容识别符与所取得的上述对象内容识别符进行比较；以及

登录机构，在所提取的上述管理内容识别符的任何一个都与所取得

的上述对象内容识别符的任一个不一致的情况下，将所取得的上述对象设备识别符登录到不正当设备列表中。

7、如权利要求 6 所述的不正当设备检测装置，其特征在于，

上述存储机构还与上述管理内容识别符相对应地，存储有表示由该管理内容识别符识别的内容被收看收听的顺序的管理视听顺序；

上述取得机构还与上述对象内容识别符相对应地，取得表示由该对象内容识别符识别的内容被收看收听的顺序的对象视听顺序；

上述提取机构还提取对应于管理内容识别符的管理视听顺序；

上述比较机构还将所提取的管理视听顺序与所取得的对象视听顺序进行比较；

在所提取的上述管理内容识别符与所取得的上述对象内容识别符一致的情况下，在对应于 1 个管理内容识别符的管理视听顺序和对应于与上述管理内容识别符相同的对象内容识别符的对象视听顺序不一致时，上述登录机构还将所取得的上述对象设备识别符登录到不正当设备列表中。

8、如权利要求 6 所述的不正当设备检测装置，其特征在于，

上述设备是将加密的内容解密并再现的再现设备；

上述不正当设备检测装置还包括：

禁止机构，在所提取的上述管理内容识别符的任一个都与所取得的上述对象内容识别符的任一个不一致的情况下，禁止对上述对象可移动媒体输出为了将加密的内容解密而使用的解密密钥；以及

输出机构，在所提取的上述管理内容识别符的任一个与所取得的上述对象内容识别符的任一个一致的情况下，对上述对象可移动媒体输出上述解密密钥。

9、一种不正当设备检测系统，由检测通过仿造制造的不正当的设备的正当设备检测装置、和作为不正当检测的对象的检测对象设备构成，其特征在于，

上述不正当设备检测装置具备：

媒体数存储机构，存储有由保持与对象设备识别符相同的设备识别符的设备所使用的可改写的可移动媒体的媒体数，其中该对象设备

识别符是由作为不正当检测的对象的检测对象设备所保持的；

比较机构，将预先设定的不正当阈值与计算出的上述媒体数进行比较；以及

识别符存储机构，在上述媒体数超过上述不正当阈值的情况下，存储上述对象设备识别符；

上述检测对象设备包括写入机构，该写入机构对上述可移动媒体写入自身保持的对象设备识别符。

10、一种不正当设备检测方法，在不正当设备检测装置中使用，该不正当设备检测装置检测通过仿造制造的不正当的设备、并具备媒体数存储机构，该媒体数存储机构存储有由保持与对象设备识别符相同的设备识别符的设备所使用的可改写的可移动媒体的媒体数，其中该对象设备识别符是由作为不正当检测的对象的检测对象设备所保持的，其特征在于，该方法包括：

比较步骤，将预先设定的不正当阈值与计算出的上述媒体数进行比较；以及

识别符存储步骤，在上述媒体数超过上述不正当阈值的情况下，存储上述对象设备识别符。

不正当设备检测装置及不正当设备检测系统

技术领域

本发明涉及发现或确定通过仿造制造或改造的不正当设备的不正当设备检测技术。

背景技术

近年来，以多媒体关联技术的发展、大容量记录媒体的出现等为背景，出现了将由动态图像、声音等构成的数字内容（以下称作内容）保存在光盘等的大容量记录媒体中发布、或者经由网络或广播来分发的系统。

一般，为了保护内容的著作权，即为了防止内容的不正当再现或不正当拷贝等的不正当利用而使用加密技术。具体而言，使用加密密钥加密的内容被记录在光盘等的记录媒体中发布。相对于此，只有保有对应于该加密密钥的解密密钥的终端，才能将从记录媒体读出的加密内容利用该解密密钥解密，进行内容的再现。

另外，作为将内容加密的方法，有使用加密密钥将内容本身加密、利用对应于加密密钥的解密密钥将加密内容解密的方法，以及将内容利用内容密钥加密、再将内容密钥利用加密密钥加密、利用对应于该加密密钥的解密密钥将加密内容密钥解密、利用生成的内容密钥将加密内容解密的方法等。

此时，终端所保有的解密密钥需要被严格地管理以使其不泄漏到外部，但在不正当者进行的终端内部的解析中，有使某个解密密钥暴露到外部的危险性。如果某个解密密钥一旦暴露给不正当者，则认为不正当者会制造不正当地利用内容的记录装置、再现装置、或者会制作不正当利用内容的软件而通过因特网将它们散布。在这样的情况下，考虑希望实现用著作权者一旦暴露的密钥无法处理接着提供的内容。该技术称作密钥无效化技术，在专利文献1及专利文献2中公开。

但是，在专利文献1及专利文献2中，对于确定泄漏到外部的密钥（应无效化的密钥）的方法没有公开。因此，将大量流通到市场中的认为是不正当的记录装置、再现装置或认为是不正当的软件回收，通过解析它们的内部，从而确定不正当设备或不正当软件。该方法需要许多的人手和资金。

此外，根据专利文献3，目的是提供一种移动通信系统，在便携电话等的移动通信系统中，能够检测不正当地拷贝的克隆终端的存在而通知给维护者，在移动终端中不具有用来进行克隆终端存在检测的特别的功能，而能够检测克隆终端的存在，公开了一种移动通信系统，其特征在于，具备为了进行向移动终端的来电处理而用来将该移动终端的存在位置向系统侧通知的位置登录的处理的机构、将具有与该移动终端相同的电话号码的至少1个以上的其他终端在该其他移动终端所属于的基站的控制下发出的位置登录信息与在系统侧最后位置登录的位置登录信息进行比较的机构、和根据该比较结果检测具有相同的电话号码的多个移动终端的存在的机构。

专利文献1：日本 特开 2000-31922 号公报

专利文献2：日本 特开 2002-281013 号公报

专利文献3：日本 特开 2000-184447 号公报

但是，在记录或再现内容的记录装置或再现装置中，如上述的移动通信系统那样，不是以一边移动一边进行的通信为前提，由专利文献3公开的技术的应用并不现实。

发明内容

本发明的目的是提供一种能够发现、确定通过仿造而不正当地制造或改造的设备的正当设备检测装置、正当设备检测系统、正当设备检测方法及用来进行正当设备检测的计算机程序。

为了达到上述目的，本发明是一种正当设备检测装置，检测通过仿造制造的不正当的设备，其特征在于，具备：媒体数存储机构，存储有由保持与对象设备识别符相同的设备识别符的设备所使用的可改写的可移动媒体的媒体数，其中该对象设备识别符是由作为不正

当检测的对象的检测对象设备所保持的；比较机构，将预先设定的不正当阈值与计算出的上述媒体数进行比较；以及识别符存储机构，在上述媒体数超过上述不正当阈值的情况下，存储上述对象设备识别符。

发明效果

根据该结构，能够通过由不正当的设备使用的可移动媒体的数量推测通过仿造制造的不正当的设备。

这里，也可以是，上述不正当设备检测装置还包括：取得部，从由上述检测对象设备使用的可改写的对象可移动媒体取得识别该对象可移动媒体的对象媒体识别符、和该检测对象设备所保持的对象设备识别符；存储部，与由过去成为不正当检测的对象的管理对象设备所保持的管理设备识别符相对应地，存储分别识别由该管理对象设备使用的1个以上的可改写的可移动媒体的1个以上的管理媒体识别符；以及计算机构，使用所存储的上述管理设备识别符及上述管理媒体识别符、以及所取得的上述对象设备识别符及上述对象媒体识别符，计算与所取得的对象设备识别符相同的设备识别符所对应的管理媒体识别符的数目和对象媒体识别符的数目之和，作为上述媒体数，并将计算出的上述媒体数写入到上述媒体数存储机构中。

根据该结构，能够可靠地计算上述媒体数。

这里，也可以是，上述比较机构还将比上述不正当阈值小的警告阈值、与计算出的上述媒体数进行比较；在计算出的上述媒体数为上述不正当阈值以下，且超过上述警告阈值的情况下，上述识别符存储机构存储所取得的上述对象设备识别符。

根据该结构，能够推测不正当的设备及应该警告的设备。

这里，也可以是，上述设备是将加密的内容解密并再现的再现设备；上述不正当设备检测装置还包括：禁止机构，在计算出的上述媒体数超过不正当阈值的情况下，禁止对上述对象可移动媒体输出为了将加密的内容解密而使用的解密密钥；以及输出机构，在计算出的上述媒体数没有超过不正当阈值的情况下，对上述对象可移动媒体输出上述解密密钥。

根据该结构，在推测为不正当的设备的情况下，能够禁止解密密钥的输出,而防止内容的不正当的利用。

这里，也可以是，是检测通过仿造制造的不正当的设备，具备：系列数存储机构，存储有通过保持与对象设备识别符相同的设备识别符的设备来收看收听的内容的视听履历系列的系列数，其中该对象设备识别符是由作为不正当检测的对象的检测对象设备所保持的；比较机构，将预先设定的不正当阈值与计算出的上述系列数进行比较；以及存储机构，在上述系列数超过上述不正当阈值的情况下，存储上述对象设备识别符。

根据该结构，能够通过由不正当的设备收看收听的内容的视听履历系列的系列数，推测通过仿造制造的不正当的设备。

这里，也可以是，是检测通过仿造制造的不正当的设备，具备：存储机构，与由过去成为不正当检测的对象的对象设备保持的管理设备识别符相对应地，存储分别识别在该对象设备中收看收听的1个以上的内容的1个以上的管理内容识别符；取得机构，从在作为不正当检测的对象的检测对象设备中使用的可改写的对象可移动媒体中，取得分别识别在该检测对象设备中收看收听的1个以上的内容的1个以上的对象内容识别符、和该检测对象设备保持的对象设备识别符；提取机构，从上述存储机构提取与和所取得的上述对象设备识别符相同的管理设备识别符相对应的1个以上的管理内容识别符；比较机构，将所提取的上述管理内容识别符与所取得的上述对象内容识别符进行比较；以及登录机构，在所提取的上述管理内容识别符的任一个都与所取得的上述对象内容识别符的任一个不一致的情况下，将所取得的上述对象设备识别符登录到不正当设备列表中。

根据该结构，能够通过由不正当的设备收看收听的内容，推测通过仿造制造的不正当的设备。

这里，也可以是，上述存储机构还与上述管理内容识别符相对应地，存储有表示由该管理内容识别符识别的内容被收看收听的顺序的管理视听顺序；上述取得机构还与上述对象内容识别符相对应地，取得表示由该对象内容识别符识别的内容被收看收听的顺序的对象视

听顺序；上述提取机构还提取对应于管理内容识别符的管理视听顺序；上述比较机构还将所提取的管理视听顺序与所取得的对象视听顺序进行比较；在所提取的上述管理内容识别符与所取得的上述对象内容识别符一致的情况下、在对应于 1 个管理内容识别符的管理视听顺序和对应于与上述管理内容识别符相同的对象内容识别符的对象视听顺序不一致时，上述登录机构将所取得的上述对象设备识别符登录到不正当设备列表中。

根据该结构，通过内容的视听顺序能够更严密地推测通过仿造制造的不正当的设备。

这里，也可以是，上述设备是将加密的内容解密并再现的再现设备；上述不正当设备检测装置还包括：禁止机构，在所提取的上述管理内容识别符的任何一个都与所取得的上述对象内容识别符的任何一个不一致的情况下，禁止对上述对象可移动媒体输出为了将加密的内容解密而使用的解密密钥；以及输出机构，在所提取的上述管理内容识别符的任何一个与所取得的上述对象内容识别符的任何一个一致的情况下，对上述对象可移动媒体输出上述解密密钥。

根据该结构，在推测为不正当的设备的条件下，能够禁止解密密钥的输出，而防止内容的不正当的利用。

通常，考虑不正当设备的台数是 1000 台或者是 10000 台的量级，相反，个人所拥有的可移动媒体的上限如果是 100 个就足够了。因而，例如在设阈值为 100 的情况下，即使是拥有多个可移动媒体的用户，如果以设备 ID 为基准计数媒体 ID，则其数量不会超过 100。此外，流通的具有相同的设备 ID 的不正当设备，由于各个使用者保持的可移动媒体的媒体 ID 不同，所以在存在 1000 台不正当设备的情况下，如果以设备 ID 为基准计数媒体 ID 则其数量超过 1000，所以在超过了作为阈值的 100 的时刻，能够判断该设备 ID 正在被不正当设备利用。

附图说明

图 1 是表示不正当设备检测系统 1 的结构的系统结构图。

图 2 是表示管理服务器装置 100 的结构的框图。

图 3 是表示管理表 120 的数据构造的数据构造图。

图 4 是表示设备密钥列表 130 的数据构造的数据构造图。

图 5 是表示内容密钥列表 140 的数据构造的数据构造图。

图 6 是表示注意设备列表 150 的数据构造的数据构造图。

图 7 是表示警告设备列表 160 的数据构造的数据构造图。

图 8 是表示不正当设备列表 170 的数据构造的数据构造图。

图 9 是表示控制部 102 的控制的模式的表。

图 10 是表示存储卡 200 的结构的框图。

图 11 是表示登记装置 300 的结构的框图。

图 12 是表示 DVD 播放器 400 的结构的框图。

图 13 是表示 DVD 播放器 400 从存储卡 200a 取得设备 ID 的运动的流程图。

图 14 是表示登记装置 300 从管理服务器装置 100 取得加密内容密钥的运动的流程图。后接图 15。

图 15 是表示登记装置 300 从管理服务器装置 100 取得加密内容密钥的运动的流程图。后接图 16。

图 16 是表示登记装置 300 从管理服务器装置 100 取得加密内容密钥的运动的流程图。后接图 17。

图 17 是表示登记装置 300 从管理服务器装置 100 取得加密内容密钥的运动的流程图。前接图 16。

图 18 是表示 DVD 播放器 400 的加密内容的解密和再现的运动的流程图。后接图 19。

图 19 是表示 DVD 播放器 400 的加密内容的解密和再现的运动的流程图。前接图 18。

图 20 是表示作为变形例的存储卡 200e 的结构的框图。

图 21 是表示作为变形例的管理服务器装置 100 所具有的服务器履历信息表 120e 的数据构造的数据构造图。

图 22 是表示作为变形例的 DVD 播放器再现内容时的运动的流程图。

图 23 是表示作为变形例的 DVD 购入时的各装置的动作的流程图。后接图 24。

图 24 是表示作为变形例的 DVD 购入时的各装置的动作的流程图。前接图 23。

图 25 表示用来进行集合 α 及集合 β 的比较的第 1 例。

图 26 表示用来进行集合 α 及集合 β 的比较的第 2 例。

图 27 表示用来进行集合 α 及集合 β 的比较的第 3 例。

图 28 是表示作为变形例的存储卡 200e 所具有的使用者履历信息列表 231f 的数据构造的数据构造图。

图 29 是表示作为变形例的管理服务器装置 100 所具有的服务器履历信息列表 120f 的数据构造的数据构造图。

图 30 是表示 DVD 购入时的管理服务器装置 100 的动作的流程图。

图 31 表示用来进行集合 α 及集合 β 的比较的第 1 例。

图 32 表示用来进行集合 α 及集合 β 的比较的第 2 例。

图 33 是表示作为变形例的 DVD 购入时的管理服务器装置 100 的动作的流程图。

图 34 是表示所提取的服务器履历信息群 621 的数据构造的数据构造图。

具体实施方式

1、不正当设备检测系统1

对作为有关本发明的 1 个实施方式的不正当设备检测系统 1 进行说明。

1. 1 不正当设备检测系统 1 的概要

不正当设备检测系统 1 如图 1 所示, 由管理服务器装置 100、登记装置 300 及 DVD 播放器 400a、……、400b、400c、……、400d 构成。管理服务器装置 100 与登记装置 300 经由因特网 10 连接。

DVD 播放器 400a、……、400b 是正规的制造业者制造的正规的播放器, 分别在内部中存储有唯一地识别自身的设备 ID。这里, DVD

播放器 400a、……、400b 的合计例如假设为 1 万台。

另一方面，DVD 播放器 400c、……、400d 是不正当的制造业者不正当地仿造 DVD 播放器 400b 而制造的播放器。DVD 播放器 400c、……、400d 分别在内部中存储有与唯一地识别 DVD 播放器 400b 的设备 ID 相同的设备 ID。这里，DVD 播放器 400c、……、400d 的合计例如假设为 1 万台。

DVD 播放器 400a 的使用者在新购入 DVD 之前，使用者将存储卡 200a 安装到 DVD 播放器 400a 中。在存储卡 200a 中记录有唯一地识别自身的媒体 ID。如果安装了存储卡 200a，则 DVD 播放器 400a 将自身存储在内部中的设备 ID 写入到存储卡 200a 中。

接着，使用者在购入 DVD 时，拿着存储有识别 DVD 播放器 400a 的设备 ID 的存储卡 200a 去往零售商店。使用者在零售商店中选择期望的 DVD 包 500。在 DVD 包 500 中包含有 DVD500a。接着，使用者将存储卡 200a 和 DVD 包 500 交给作为登记装置 300 的操作者的店员。店员将存储卡 200a 安装到登记装置 300 中，通过登记装置 300 的条码读取器扫描显示在 DVD 包 500 上的条码。

登记装置 300 从显示在 DVD 包 500 上的条码读出记录在包含于 DVD 包 500 中的 DVD500a 中的内容的内容 ID，并且从安装的存储卡 200a 读出设备 ID 及媒体 ID，将内容 ID、读出的设备 ID 及媒体 ID 的组，经由因特网 10 向管理服务器装置 100 发送。

管理服务器装置 100 中，与识别 DVD 播放器的设备 ID 相对应地存储有分别识别安装在该 DVD 播放器中的 1 个以上的存储卡的媒体 ID、和表示上述存储卡的总数的媒体 ID 总数。

管理服务器装置 100 如果从登记装置 300 经由因特网 10 接收到内容 ID、设备 ID 及媒体 ID 的组，则判断接收到的设备 ID 是否存储在内部中。在接收到的设备 ID 存储在内部中的情况下，再判断接收到的媒体 ID 是否存储在内部中。在接收到的媒体 ID 没有存储的情况下，将接收到的媒体 ID 与上述设备 ID 建立对应而存储，对媒体 ID 总数加上“1”的值。在判断为接收到的设备 ID 没有存储在内部中的情况下，存储设备 ID 及媒体 ID 的组，使媒体 ID 总数为“1”。

接着，管理服务器装置 100 判断对应于接收到的设备 ID 的媒体 ID 总数属于 (i) “100” 以下、(ii) “101” 以上 “150” 以下、(iii) “151” 以上 “199” 以下、(iv) “200” 以上的哪个范围中。

(i) 如果媒体 ID 总数为 “100” 以下，则管理服务器装置 100 将对应于接收到的内容 ID 的内容密钥加密，将加密内容密钥与表示使用者所使用的设备不是不正当设备的设备判断等级一起，经由因特网 10 向登记装置 300 发送。

(ii) 如果媒体 ID 总数为 “101” 以上 “150” 以下，则管理服务器装置 100 将设备 ID 向保持于内部中的注意设备列表登录，将对应于接收到的内容 ID 的内容密钥加密，将加密内容密钥与表示使用者所使用的设备是需要注意的设备的设备判断等级一起，经由因特网 10 向登记装置 300 发送。

(iii) 如果媒体 ID 总数为 “151” 以上 “199” 以下，则管理服务器装置 100 将设备 ID 向保持于内部中的警告设备列表登录，将对应于接收到的内容 ID 的内容密钥加密，将加密内容密钥与表示使用者所使用的设备是需要警告的设备的设备判断等级一起，经由因特网 10 向登记装置 300 发送。

(iv) 如果媒体 ID 总数为 “200” 以上，则管理服务器装置 100 将设备 ID 向保持于内部中的不正当设备列表登录，将表示使用者所使用的设备是不正当设备的设备判断等级，经由因特网 10 向登记装置 300 发送。但是，在此情况下不发送内容密钥。

登记装置 300 经由因特网 10 从管理服务器装置 100 接收设备判断等级。并且有时也接收加密内容密钥。

(i) 在接收到的设备判断等级表示使用者所使用的 DVD 播放器不是不正当设备的情况下，登记装置 300 将接收到的加密内容密钥向存储卡 200a 写入。在此情况下，使用者向零售商店支付 DVD 包 500 的价格。

(ii) 在接收到的设备判断等级表示使用者所使用的设备是需要注意的设备的情况下，登记装置 300 进行注意显示，将接收到的加密内容密钥向存储卡 200a 写入。在此情况下，使用者向零售商店支付

DVD 包 500 的价格。

(iii) 在接收到的设备判断等级表示使用者所使用的设备是需要警告的设备的情况下，登记装置 300 进行警告显示，对操作者要求批准加密内容密钥的提供或不批准的指示的输入，在指示是批准时，将接收到的加密内容密钥向存储卡 200a 写入。此时，使用者对零售商店支付 DVD 包 500 的价格。在指示是不批准时，不将接收到的加密内容密钥提供给使用者。此时，零售商店拒绝对使用者的 DVD 包 500 的销售。

(iv) 在接收到的设备判断等级表示使用者所使用的设备是不正当设备的情况下，登记装置 300 进行不正当显示并结束。不将加密内容密钥提供给使用者。在此情况下，零售商店拒绝对使用者的 DVD 包 500 的销售。

在上述的 (i)、(ii)、(iii) 的情况下，在使用者购入了 DVD 包 500 时，使用者将存储卡 200a 及 DVD 包 500 拿回，将存储卡 200a 安装到 DVD 播放器 400a 中，将包含在 DVD 包 500 中的 DVD500a 安装到 DVD 播放器 400a 中。

DVD 播放器 400a 从存储卡 200a 读出加密内容密钥，将读出的加密内容密钥解密而生成解密内容密钥，利用所生成的解密内容密钥，将记录在 DVD500a 中的加密内容解密而生成解密内容，将生成的解密内容变换为影像信号及声音信号，将影像信号及声音信号向监视器 411a 输出。

这里，DVD 播放器 400a、……、400b 的合计是 1 万台，但由于各自的设备 ID 不同，所以在各自的使用者例如具有各 10 张存储卡、经过上述那样的操作的情况下，管理服务器装置 100 所具有、对应于设备 ID 而存储的媒体 ID 总数充其量为 10 个。此时，管理服务器装置 100 判断这些 DVD 播放器 400a、……、400b 的每个为正规的设备。

另一方面，DVD 播放器 400c、……、400d 的合计是 1 万台，但由于各自的设备 ID 相同，所以如果各自的使用者例如具有各 1 张存储卡，则在经过上述那样的操作的情况下，管理服务器装置 100 所具有、对应于设备 ID 而存储的媒体 ID 总数为 1 万。此时，管理服务器

装置 100 将这些 DVD 播放器 400c、……、400d 的每个判断为不正当的设备。这样，管理服务器装置 100 能够判断 DVD 播放器的正当性。

1. 2 管理服务器装置 100 的结构

管理服务器装置 100 如图 2 所示，由通信部 101、控制部 102、管理表存储部 103、内容密钥存储部 104、选择部 105、设备密钥存储部 106、加密部 107、设备列表存储部 108、输入部 110、显示部 111 及认证部 112 构成。

管理服务器装置 100 具体而言是由微处理器、ROM、RAM、硬盘单元、显示器单元、键盘、鼠标等构成的计算机系统。在上述 RAM 或上述硬盘单元中存储有计算机程序。通过上述微处理器按照上述计算机程序动作，管理服务器装置 100 实现其一部分的功能。

(1) 管理表存储部 103、内容密钥存储部 104、设备密钥存储部 106 及设备列表存储部 108

管理表存储部 103、内容密钥存储部 104、设备密钥存储部 106 及设备列表存储部 108 具体而言由 1 台硬盘单元构成。

(管理表存储部 103)

管理表存储部 103 如图 2 所示，具有管理表 120。

管理表 120 作为一例，如图 3 所示，具备用来存储 1 个以上的媒体 ID 信息的区域。媒体 ID 信息通常对应于 1 台正规的设备（在本实施方式中是 1 台 DVD 播放器）。但是，在存在不正当地存储设备 ID 的不正当设备的情况下，媒体 ID 信息对应于存储有相同的设备 ID 的所有设备。媒体 ID 信息包括设备 ID、1 个以上的媒体 ID 和媒体 ID 总数。

设备 ID 是唯一地识别与包含该设备 ID 的媒体 ID 信息相对应的设备的识别信息。但是，如上所述，在存在不正当地存储有设备 ID 的不正当设备的情况下，并不限于能够唯一地识别设备。

媒体 ID 是唯一地识别安装在对应于包含有该媒体 ID 的媒体 ID 信息的设备中使用的存储卡的识别信息。

媒体 ID 总数表示在包含有该媒体 ID 总数的媒体 ID 信息中所包括的媒体 ID 的个数。

如图 3 所示, 管理表 120 由媒体 ID 信息 128、129、……构成。

媒体 ID 信息 128 由于包括设备 ID121“ID-A”、媒体 ID122“MID-1”、123“MID-5”及媒体 ID 总数 124“2”, 所以表示将由“MID-1”及“MID-5”识别的两个存储卡安装在由“ID-A”识别的设备(DVD 播放器)中使用。

此外, 媒体 ID 信息 129 由于包括设备 ID125“ID-B”、媒体 ID126“MID-2”、及媒体 ID 总数 127“1”, 所以表示将由“MID-2”识别的 1 个存储卡安装在由“ID-B”识别的设备(DVD 播放器)中使用。

(设备密钥存储部 106)

设备密钥存储部 106 如图 2 所示, 具有设备密钥列表 130。

设备密钥列表 130 作为一例, 如图 4 所示, 包括 1 个以上的设备密钥信息而构成。设备密钥信息对应于 1 台的设备(在本实施方式中是 1 台 DVD 播放器), 包括设备 ID 与设备密钥。另外, 在存在不正当的设备的情况下, 设备密钥信息与设备之间的对应关系与上述的情况相同。

设备 ID 是唯一地识别与包含该设备 ID 的设备密钥信息相对应的设备的识别信息。

设备密钥是分配给对应于包含该设备密钥的设备密钥信息的设备的密钥信息。设备密钥作为一例是 128 位长。

如图 4 所示, 设备密钥列表 130 包含设备密钥信息 133、134、……而构成。设备密钥信息 133 由于包括设备 ID131“ID-A”及设备密钥 132“DK-A”, 所以表示分配给由“ID-A”识别的设备(DVD 播放器)的设备密钥是“DK-A”。

(内容密钥存储部 104)

内容密钥存储部 104 如图 2 所示, 具有内容密钥列表 140。

内容密钥列表 140 作为一例, 如图 5 所示, 包含 1 个以上的内容密钥信息 143、144、145、……而构成。内容密钥信息对应于 1 个内容, 包括内容 ID 与内容密钥。例如, 内容密钥信息 143 包括内容 ID141“C001”和内容密钥 142“CK-1”。

内容 ID 是唯一地识别与包含有该内容 ID 的内容密钥信息相对应的内容的识别信息。

内容密钥是分配给对应于包含该内容密钥的内容密钥信息的内容的密钥信息。

(设备列表存储部 108)

设备列表存储部 108 如图 2 所示, 具有注意设备列表 150、警告设备列表 160 及不正当设备列表 170。

注意设备列表 150 作为一例, 如图 6 所示, 具备用来存储 1 个以上的注意设备 ID 的区域。注意设备 ID 如上所述, 是唯一地识别被判断为需要注意的设备的识别信息。

注意设备列表 150 如图 6 所示, 由于包括注意设备 ID151 “ID-X005”、注意设备 ID152 “ID-Y007”、注意设备 ID153 “ID-Z009”、……, 所以由 “ID-X005”、“ID-Y007”、“ID-Z009” 识别的设备 (DVD 播放器) 是需要注意的。

警告设备列表 160 作为一例, 如图 7 所示, 具备用来存储 1 个以上的警告设备 ID 的区域。警告设备 ID 如上所述, 是唯一地识别被判断为需要警告的设备的识别信息。

警告设备列表 160 如图 7 所示, 由于包括警告设备 ID161 “ID-X003”、警告设备 ID162 “ID-Y004”、警告设备 ID163 “ID-Z004”、……, 所以由 “ID-X003”、“ID-Y004”、“ID-Z004” 识别的设备 (DVD 播放器) 是需要警告的。

不正当设备列表 170 作为一例, 如图 8 所示, 具备用来存储 1 个以上的不正当设备 ID 的区域。不正当设备 ID 如上所述, 是唯一地识别被判断为不正当的设备的识别信息。

不正当设备列表 170 如图 8 所示, 由于包括不正当设备 ID171 “ID-X001”、不正当设备 ID172 “ID-Y002”、不正当设备 ID173 “ID-Z005”、……, 所以由 “ID-X001”、“ID-Y002”、“ID-Z005” 识别的设备 (DVD 播放器) 是不正当的设备。

(2) 控制部 102

(与登记装置 300 的相互的设备认证)

控制部 102 从登记装置 300 经由因特网 10 及通信部 101 获取连接请求。如果获取了上述连接请求，则对认证部 122 指示以与登记装置 300 之间进行相互的设备认证。

接着，控制部 102 从认证部 112 获取表示相互的设备认证的结果的认证结果信息。在所获取的认证结果信息表示相互的设备认证失败的情况下不进行以后的处理。在所获取的认证结果信息表示相互的设备认证成功的情况进行以下所示的处理。

（内容密钥的发送）

控制部 102 从登记装置 300 经由因特网 10 及通信部 101 获取内容密钥的请求、内容 ID、设备 ID 及媒体 ID。

如果获取了内容密钥的请求、内容 ID、设备 ID 及媒体 ID，则控制部 102 从管理表 120 检索与所获取的设备 ID 相同的设备 ID，在管理表 120 内不存在相同的设备 ID 的情况下，将媒体 ID 总数设为“1”，将所获取的设备 ID、媒体 ID 和媒体 ID 总数作为媒体 ID 信息，向管理表 120 写入。

在管理表 120 内存在相同的设备 ID 的情况下，控制部 102 从管理表 120 中提取包含有相同的设备 ID 的媒体 ID 信息，判断在所提取的媒体 ID 信息中是否包含有与所获取的媒体 ID 相同的媒体 ID，在不包含的情况下，对包含在所提取的媒体 ID 信息中的媒体 ID 总数加上“1”的值，在所提取的媒体 ID 信息中追加写入所获取的媒体 ID。接着，将追加写入了媒体 ID 的上述媒体 ID 信息向在管理表 120 中作为提取对象的上述媒体 ID 信息进行覆盖。

在所提取的媒体 ID 信息中包含有与所获取的媒体 ID 相同的媒体 ID 的情况下，控制部 102 不更新该提取出的媒体 ID 信息。

接着，控制部 102 判断媒体 ID 总数属于 (i) “100” 以下、(ii) “101” 以上 “150” 以下、(iii) “151” 以上 “199” 以下、(iv) “200” 以上的哪个范围中。

以下，对上述 4 种情况分别进行说明。另外，在图 9 所示的表 180 的各栏中，对在栏 181、栏 182、栏 183 及栏 184 中表示的上述 4 种情况的每一个，记载了控制部 102 中的处理的概要。

(i) 在媒体 ID 总数为“100”以下的情况下，或者，在上述中，从管理表 120 检索与所获取的设备 ID 相同的设备 ID，在管理表 120 内不存在相同的设备 ID 的情况下，控制部 102 将设备判断等级设定为表示使用者所使用的设备不是不正当设备的“0”。接着，将设定为“0”的设备判断等级经由通信部 101 及因特网 10 向登记装置 300 发送。此外，控制部 102 将接收到的内容 ID 向选择部 105 输出，输出进行内容密钥的选择的指示。进而，将接收到的设备 ID 向加密部 107 输出，输出将内容密钥加密的指示（栏 189）。

(ii) 在媒体 ID 总数为“101”以上“150”以下的情况下，控制部 102 将设备判断等级设定为表示使用者所使用的设备是需要注意的设备的“1”。接着，将设定为“1”的设备判断等级经由通信部 101 及因特网 10 向登记装置 300 发送。接着，将所获取的设备 ID 向注意设备列表 150 追加写入（栏 194）。进而，控制部 102 将接收到的内容 ID 向选择部 105 输出，输出进行内容密钥的选择的指示，将接收到的设备 ID 向加密部 107 输出，输出将内容密钥加密的指示（栏 190）。

(iii) 在媒体 ID 总数为“151”以上“199”以下的情况下，控制部 102 将设备判断等级设定为表示使用者所使用的设备是需要警告的设备的“2”。接着，将设定为“2”的设备判断等级经由通信部 101 及因特网 10 向登记装置 300 发送。接着，将所获取的设备 ID 向警告设备列表 160 追加写入（栏 195）。此外，控制部 102 从登记装置 300 经由因特网 10 及通信部 101，获取表示批准内容密钥的向使用者的提供的指示或表示不批准的指示，在所获取的指示表示不批准的情况下，结束处理。在所获取的指示表示批准的情况下，控制部 102 将接收到的内容 ID 向选择部 105 输出，输出进行内容密钥的选择的指示，将接收到的设备 ID 向加密部 107 输出，输出将内容密钥加密的指示（栏 191）。

(iv) 在媒体 ID 总数为“200”以上的情况下，控制部 102 将设备判断等级设定为表示使用者所使用的设备是不正当的设备的“3”。接着，将所获取的设备 ID 向不正当设备列表 170 追加写入（栏 196）。

接着，将设定为“3”的设备判断等级经由通信部 101 及因特网 10 向登记装置 300 发送。接着，控制部 102 结束处理（栏 191）。

（3）选择部 105

选择部 105 从控制部 102 获取进行内容 ID 及内容密钥的选择的指示。如果获取了内容 ID 及上述指示，则从内容密钥列表 140 中读出包含与所获取的内容 ID 相同的内容 ID 的内容密钥信息，从所读出的内容密钥信息中提取内容密钥，接着将所提取的内容密钥向加密部 107 输出。

（4）加密部 107

加密部 107 从控制部 102 获取将接收到的设备 ID 及内容密钥加密的指示，从选择部 105 获取内容密钥。接着，从设备密钥列表 130 中读出包含与所获取的设备 ID 相同的设备 ID 的设备密钥信息，从所读出的设备密钥信息中提取设备密钥。

接着，加密部 107 利用所提取的设备密钥，对所获取的内容密钥实施加密算法 E1，生成加密内容密钥。

加密内容密钥 = E1（设备密钥，内容密钥）

这里， $A = E(B, C)$ 表示利用密钥 B 对明文 C 实施加密算法 E 而生成的密文 A。

此外，这里，加密算法 E1 作为一例是基于 AES（Advanced Encryption Standard：高级加密标准）的算法。

接着，加密部 107 经由通信部 101 及因特网 10，将生成的上述加密内容密钥向登记装置 300 发送。

另外，在图 2 中，表示管理服务器装置 100 的各结构部的各块通过连接线与其他块连接。但是，也有省略了一部分的连接线的情况。这里，各连接线表示传递信号及信息的路径。此外，连接到表示加密部 107 的块的多个连接线中的、在连接线上描绘有密钥标志的，表示将作为密钥的信息向加密部 107 传递的路径。此外，对于其他附图也同样。

（5）输入部 110 及显示部 111

输入部 110 从管理服务器装置 100 的操作者受理各种信息的输

入，或者受理各种指示的输入，将受理了输入的信息或指示向控制部 102 输出。

显示部 111 通过控制部 102 的指示显示各种信息。

(6) 认证部 112

认证部 112 根据控制部 102 的指示，经由通信部 101 及因特网 10，在与登记装置 300 之间进行询问应答（challenge-response）型的相互的设备认证。在相互的设备认证中，认证部 112 确认登记装置 300 的正当性，并且接受登记装置 300 的正当性的认证。

另外，关于上述的相互的设备认证，由于是公知的，所以省略详细的说明。

如果相互的设备认证成功或失败，则认证部 112 将表示相互的设备认证成功或失败的认证结果向控制部 102 输出。

(7) 通信部 101

通信部 101 在登记装置 300 与控制部 102 之间中继各种信息的收发。并且在登记装置 300 与认证部 112 之间中继各种信息的收发。

1.3 存储卡 200 的结构

存储卡 200 如图 10 所示，由输入输出部 201、认证部 202 及存储部 203 构成。

存储卡 200 具体而言是由微处理器、ROM、RAM 等构成的计算机系统。在上述 RAM 中存储有计算机程序。通过上述微处理器按照上述计算机程序动作，存储卡 200 实现其一部分的功能。

以下，对构成存储卡 200 的各要素进行说明。

(1) 存储部 203

存储部 203 如图 10 所示，具备媒体 ID 区域 204 及一般区域 205。

媒体 ID 区域 204 如图 10 所示，存储有媒体 ID211。媒体 ID211 是唯一地识别存储卡 200 的识别信息。

一般区域 205 如图 10 所示，具有加密内容密钥列表 221。

加密内容密钥列表 221 如图 10 所示，具备用来存储 1 个以上的加密内容密钥信息的区域。

各加密内容密钥信息包括由 1 个设备 ID、内容 ID 和加密内容密

钥构成的 1 个以上的组，加密内容密钥信息对应于 1 台设备（在该实施方式中是 DVD 播放器），内容 ID 与加密内容密钥的组对应于 1 个内容。但是，在存在不正当地存储设备 ID 的不正当的设备的情况下，加密内容密钥信息对应于存储有相同的设备 ID 的所有的设备。

设备 ID 是唯一地识别设备（在该实施方式中是 DVD 播放器）的识别信息。但是，如上所述，在存在不正当地存储有设备 ID 的不正当设备的情况下，并不限于能够唯一地识别设备。

内容 ID 是唯一地识别与包含有该内容 ID 的组相对应的内容的识别信息。

加密内容密钥是通过将内容密钥用分配给对应的设备的设备密钥加密而生成的，其中该内容密钥是在将对应于包含该加密内容密钥的组的内容加密时所使用的内容密钥。

图 10 所示的加密内容密钥信息 236 包含有设备 ID231“ID-A”、由内容 ID232“C001”和加密内容密钥 234“E1(DK-A, CK-1)”构成的组 237、和由内容 ID233“C002”和加密内容密钥 238“E1(DK-A, CK-2)”构成的组 238。

这里，包含在组 237 中的加密内容密钥 234“E1(DK-A, CK-1)”，是使用分配给由设备 ID231“ID-A”识别的 DVD 播放器的设备密钥“DK-A”作为密钥、将分配给由内容 ID232“C001”识别的内容的内容密钥“CK-1”加密而生成的。

此外，包含在组 238 中的加密内容密钥 235“E1(DK-A, CK-2)”，是使用分配给由设备 ID231“ID-A”识别的 DVD 播放器的设备密钥“DK-A”作为密钥、将分配给由内容 ID233“C002”识别的内容的内容密钥“CK-2”加密而生成的。

(2) 输入输出部 201

输入输出部 201 从存储部 203 的媒体 ID 区域 204 或一般区域 205 中读出信息，将读出的信息向安装有存储卡 200 的外部的装置输出。此外，从上述外部的装置获取信息，将所获取的信息向存储部 203 的一般区域 205 写入。这里，所谓的外部装置，是登记装置 300 及 DVD 播放器 400a、……、400b、400c、……、400d。

(3) 认证部 202

认证部 202 在存储卡 200 安装在外部的装置中时, 经由输入输出部 201 在与外部装置之间相互进行设备认证。这里, 设备认证是询问应答型的认证。另外, 关于询问应答型的设备认证, 由于是公知的, 所以这里省略详细的说明。

这里, 所谓的外部装置, 是登记装置 300 及 DVD 播放器 400a、……、400b、400c、……、400d。

认证部 202 在与外部装置之间相互的设备认证成功的情况下, 控制输入输出部 201, 以在存储部 203 与外部的装置之间进行信息的收发。在设备认证失败的情况下, 控制输入输出部 201 在此后在存储部 203 与外部的装置之间不进行信息的收发。

1. 4 登记装置 300 的结构

登记装置 300 如图 11 所示, 由认证部 301、输入部 302、显示部 303、显示部 304、输入输出部 305、控制部 306、通信部 307、印字部 308、保管库 309、条码处理部 310、信息存储部 312 及认证部 313 构成。此外, 在登记装置 300 上连接着条码读取器 311。

登记装置 300 是进行从使用者支付的以 DVD 为代表的商品的销售费用的结算、保管等的现金登记装置, 并且也是从管理服务器装置 100 取得分配给保存于 DVD 中的内容的内容密钥、并经由存储卡向使用者提供的装置。

登记装置 300 具体而言是由微处理器、ROM、RAM、硬盘单元、显示器单元、键盘等构成的计算机系统。在上述硬盘单元中存储有计算机程序。通过上述微处理器按照上述计算机程序动作, 登记装置 300 实现其一部分的功能。

(1) 信息存储部 312

信息存储部 312 如图 11 所示, 具备价格列表 321。

价格列表 321 如图 11 所示, 包含多个价格信息。各价格信息与 DVD 对应, 包括内容 ID 及销售价格。

内容 ID 是唯一地识别保存在对应于包含该内容 ID 的销售信息的 DVD 中的内容的识别信息。这里, 假设在该 DVD 中仅保存有 1 个内

容。

销售价格表示对应于包含该销售价格的销售信息的 DVD 的销售价格。

(2) 认证部 313

认证部 313 在登记装置 300 中安装有存储卡时, 经由输入输出部 305 在与安装的存储卡之间相互地进行设备认证。这里, 设备认证是询问应答型的认证。关于询问应答型的认证, 由于是公知的, 所以这里省略详细的说明。

认证部 313 在认证部 313 与安装的存储卡之间相互的设备认证成功的情况下, 将表示设备认证成功的认证结果通知给控制部 306。此外, 在设备认证失败的情况下, 将表示设备认证失败的认证结果通知给控制部 306。

在设备认证失败的情况下, 在此以后, 登记装置 300 在与该存储卡之间不进行信息的收发。

(3) 认证部 301

认证部 301 经由通信部 307 在与管理服务器装置 100 之间相互进行设备认证。这里, 设备认证是询问应答型的认证。关于询问应答型的认证, 由于是公知的, 所以这里省略详细的说明。

认证部 301 在认证部 301 与管理服务器装置 100 之间相互的设备认证成功的情况下, 将表示设备认证成功的认证结果通知给控制部 306。此外, 在设备认证失败的情况下, 将表示设备认证失败的认证结果通知给控制部 306。

在设备认证失败的情况下, 在此以后, 登记装置 300 在与管理服务器装置 100 之间不进行信息的收发。

(4) 输入输出部 305

输入输出部 305 基于控制部 306 的控制而在控制部 306 与安装的存储卡之间, 或者基于认证部 313 的控制而在认证部 313 与安装的存储卡之间双向地进行信息的收发。

(5) 条码读取器 311 及条码处理部 310

条码读取器 311 以光学方式读取印刷在 DVD 包 500 的表面上

条码而生成对应的读取信息，将生成的读取信息向条码处理部 310 输出。

条码处理部 310 从条码读取器 311 获取读取信息，从所获取的读取信息生成内容 ID，将生成的内容 ID 向控制部 306 输出。

(6) 控制部 306

(与管理服务器装置 100 的连接)

控制部 306 经由通信部 307 及因特网 10 向管理服务器装置 100 发送连接请求。接着，控制部 306 对认证部 301 指示以使其在与管理服务器装置 100 之间进行相互的设备认证。

如果从认证部 301 获取了表示设备认证失败的认证结果，则控制部 306 结束处理。

(内容 ID 的取得)

如果从认证部 301 获取了表示设备认证成功的认证结果，则控制部 306 从条码处理部 310 获取内容 ID，从价格列表 321 中读出包含有与所获取的内容 ID 相同的内容 ID 的价格信息，从所读出的价格信息提取销售价格，将所获取的内容 ID 与所提取的销售价格向显示部 303 及 304 输出，对显示部 303 及 304 指示以将它们进行显示。

(与存储卡的连接)

控制部 306 从输入输出部 305 获取表示安装有存储卡 200a 的安装信息。如果获取了上述安装信息，则控制部 306 对认证部 313 指示以使其在与所安装的存储卡 200a 之间进行相互的设备认证。如果从认证部 313 获取了表示设备认证失败的认证结果，则控制部 306 结束处理。

如果从认证部 313 获取了表示设备认证成功的认证结果，则控制部 306 经由输入输出部 305 将表示存储在存储卡 200a 中的媒体 ID 及设备 ID 的读出的读出指示向存储卡 200a 输出。接着，经由输入输出部 305 获取读出结果。读出结果获取为媒体 ID、1 个以上的设备 ID 或表示并未存储设备 ID 的设备 ID 不存在信息“无”。

在获取了设备 ID 不存在信息“无”的情况下，控制部 306 将表示在存储卡 200a 中并未存储设备 ID 的消息向显示部 303 及 304 输出，

对显示部 303 及 304 指示以使其显示该消息，结束处理。

在获取了多个设备 ID 的情况下，控制部 306 将所获取的多个设备 ID 向显示部 303 及 304 输出，对显示部 303 及 304 指示以使其显示该多个设备 ID，接着从输入部 302 获取由使用者从上述多个设备 ID 之中选择的 1 个设备 ID 的指定。

在获取了 1 个设备 ID 的情况下，控制部 306 原样利用该设备 ID。

（从管理服务器装置 100 的内容密钥的取得）

接着，控制部 306 经由通信部 307 向管理服务器装置 100 发送表示内容密钥的请求的请求信息，此外，将所获取的内容 ID、上述 1 个设备 ID 及所获取的媒体 ID 经由通信部 307 向管理服务器装置 100 发送。

接着，控制部 306 从管理服务器装置 100 经由通信部 307 获取设备判断等级。有时还获取加密内容密钥。这里，获取加密内容密钥的是上述获取的设备判断等级是“0”、“1”、及“2”中的任一种的情况。在上述获取的设备 ID 是“3”的情况下，不获取加密内容密钥。

接着，控制部 306 判断所获取的设备判断等级是“0”、“1”、“2”及“3”的哪一个。

在判断所获取的设备判断等级是“0”的情况下，控制部 306 将表示允许向使用者提供所获取的加密内容密钥的消息向显示部 303 及 304 输出，对显示部 303 及 304 指示以使其显示该消息。此外，将设备 ID 及内容 ID 经由输入输出部 305 向存储卡 200a 输出，再将加密内容密钥经由输入输出部 305 向存储卡 200a 输出。

在判断所获取的设备判断等级是“1”的情况下，控制部 306 将对登记装置 300 的操作者表示注意的消息向显示部 303 及 304 输出，对显示部 303 及 304 指示以使其显示该消息。此外，与判断为“0”的情况相同，将设备 ID、内容 ID 及加密内容密钥经由输入输出部 305 向存储卡 200a 输出。

在判断所获取的设备判断等级是“2”的情况下，控制部 306 将对登记装置 300 的操作者表示警告的消息向显示部 303 及 304 输出，对显示部 303 及 304 指示以使其显示该消息。进而，从登记装置 300

的操作者经由输入部 302 获取表示批准还是不批准向使用者提供该加密内容密钥的指示。在获取了不批准的指示的情况下，控制部 306 结束处理。即，对于存储卡 200a，不输出设备 ID、内容密钥及加密内容密钥。在获取了批准的指示的情况下，与判断为“0”的情况相同，将设备 ID、内容 ID 及加密内容密钥经由输入输出部 305 向存储卡 200a 输出。

在判断所获取的设备判断等级是“3”的情况下，控制部 306 将对登记装置 300 的操作者表示不正当的消息向显示部 303 及 304 输出，对显示部 303 及 304 指示以使其显示该消息。接着，控制部 306 结束处理。即，不将加密内容密钥对存储卡 200a 输出。

(7) 输入部 302、显示部 303、显示部 304、印字部 308 及保管库 309

输入部 302 从登记装置 300 的操作者受理信息或指示的输入，将受理了输入的信息或指示向控制部 306 输出。此外，显示部 303 及显示部 304 从控制部 306 获取要显示的信息，并显示所获取的信息。

印字部 308 通过控制部 306 的控制而打印各种信息。

保管库 309 保管纸币及硬币。

(8) 通信部 307

通信部 307 经由因特网 10 与管理服务器装置 100 连接，在控制部 306 与管理服务器装置 100 之间进行信息的收发，此外，在认证部 301 与管理服务器装置 100 之间进行信息的收发。

1. 5 DVD 播放器 400a、……、b、c、……、d 的结构

DVD 播放器 400a、……、b、c、……、d 分别具有同样的结构。这里，作为它们的代表，对 DVD 播放器 400 的结构进行说明。

DVD 播放器 400 如图 12 所示，由设备 ID 存储部 401、输入输出部 402、设备密钥存储部 403、解密部 404、读出部 405、解密部 406、再现部 407、显示部 408、输入部 409、控制部 410 及认证部 411 构成。此外，在 DVD 播放器 400 上连接有附带扬声器的监视器。

DVD 播放器 400 具体而言是包括微处理器、ROM、RAM 等而构成的计算机系统。在上述 ROM 中存储有计算机程序。通过上述微处

理器按照上述计算机程序动作，DVD 播放器 400 实现其功能的一部分。

(1) 设备 ID 存储部 401 及设备密钥存储部 403

设备 ID 存储部 401 设计为不能从外部访问，如图 12 所示，预先存储有设备 ID421。设备 ID421 是唯一地识别 DVD 播放器 400 的识别信息。但是，在 DVD 播放器 400 是不正当的设备的情况下，设备 ID421 并不限于唯一地识别 DVD 播放器 400。

设备密钥存储部 403 设计为不能从外部访问，如图 12 所示，预先存储有设备密钥 422。

设备密钥 422 是分配给 DVD 播放器 400 的密钥信息。

(2) 读出部 405

读出部 405 基于控制部 410 的控制而从安装在 DVD 播放器 400 中的 DVD 读出信息，将读出的信息向控制部 410 或解密部 406 输出。

(3) 输入输出部 402

输入输出部 402 如果安装有存储卡，则检测到安装有存储卡的情况，将表示被检测到的检测信息向控制部 410 输出。

此外，输入输出部 402 基于控制部 410 的控制而在控制部 410 与安装在 DVD 播放器 400 中的存储卡之间、或者基于认证部 411 的控制而在认证部 411 与安装的存储卡之间双向地进行信息的收发。

(4) 认证部 411

认证部 411 在存储卡安装在 DVD 播放器 400 中时，经由输入输出部 402 在与安装的存储卡之间相互地进行设备认证。这里，设备认证是询问应答型的认证。关于询问应答型的认证，由于是公知的，所以这里省略详细的说明。

认证部 411 在认证部 411 与存储卡之间相互的设备认证成功的情况下，将表示设备认证成功的认证结果向控制部 410 通知。此外，在设备认证失败的情况下，将表示设备认证失败的认证结果向控制部 410 通知。

在设备认证失败的情况下，在此以后，DVD 播放器 400 在与存储卡之间不进行信息的收发。

(5) 解密部 404

解密部 404 根据控制部 410 的指示，从设备密钥存储部 403 读出设备密钥 422，从输入输出部 402 获取加密内容密钥，使用所读出的设备密钥作为密钥，对加密内容密钥实施解密算法 D1，生成再现内容密钥，将生成的再现内容密钥向解密部 406 输出。这里，作为解密算法 D1 使用 AES。

(6) 解密部 406

解密部 406 从解密部 404 获取再现内容密钥，经由读出部 405 从 DVD 读出加密内容，使用所获取的再现内容密钥，对读出的加密内容实施解密算法 D2，生成再现内容。这里，作为解密算法 D2 使用 AES。接着，解密部 406 将生成的再现内容向再现部 407 输出。

(7) 再现部 407、监视器及扬声器

再现部 407 从解密部 406 获取再现内容，将所获取的再现内容分离为压缩影像信息和压缩声音信息，将压缩影像信息解码而生成影像信息，将影像信息变换为模拟的影像信号，将压缩声音信息解码而生成声音信息，将声音信息变换为模拟的声音信号，将生成的影像信号向监视器输出，将生成的声音信号向附属于监视器的扬声器输出。

监视器获取影像信号，显示影像，附属于监视器的扬声器获取声音信号而输出声音。

(7) 控制部 410

(存储卡的检测)

控制部 410 从输入输出部 402 获取表示检测出安装了存储卡的检测信息。

如果获取上述检测信息，则控制部 410 对认证部 411 指示以在与安装的存储卡之间进行相互的设备认证。接着，从认证部 411 获取认证结果。在所获取的认证结果表示认证失败的情况下，控制部 410 进行指示以将表示该情况的消息向显示部 408 输出并显示，然后结束处理。

在所获取的认证结果表示认证成功的情况下，控制部 410 从设备 ID 存储部 401 读出设备 ID421，接着，对输入输出部 402 输出表示读

出存储在所安装的存储卡中的设备 ID 的读出指示，进行指示以读出设备 ID。

接着，控制部 410 经由输入输出部 402 从安装的存储卡获取读出结果。所获取的读出结果是 1 个以上的设备 ID、或者表示设备 ID 没有存储在存储卡中的不存在信息。

在所获取的读出结果是不存在信息的情况下，或者在获取了 1 个以上的设备 ID 的情况下，在其中不存在所读出的设备 ID421 时，将所读出的设备 ID421 经由输入输出部 402 向安装的存储卡输出，对输入输出部 402 指示以使其将设备 ID421 写入到存储卡的内部中。

（内容的再现）

控制部 410 经由输入部 409 从 DVD 播放器 400 的使用者受理再现保存在 DVD 中的加密内容的指示。如果受理了上述指示，则经由读出部 405 从 DVD 读出内容 ID，对输入输出部 402 输出内容 ID 及自身的设备 ID，进行指示以从存储卡读出对应于内容 ID 及自身的设备 ID 两者的内容密钥。

接着，控制部 410 经由输入输出部 402 获取读出结果。这里，读出结果是 1 个加密内容密钥或表示没有符合的加密内容密钥的不存在信息“无”。

在作为读出结果而获取了不存在信息“无”的情况下，控制部 410 将表示该情况的消息向显示部 408 输出，对显示部 408 指示以使其显示该消息。

在读出结果是加密内容密钥的情况下，控制部 410 对解密部 404 指示以使其将加密内容密钥解密，然后，对解密部 406 指示以使其将加密内容解密，然后，对再现部 407 指示以使其将再现内容再现而输出给监视器。

（8）显示部 408 及输入部 409

显示部 408 根据控制部 410 的指示而显示被指定的消息。

此外，输入部 409 从 DVD 播放器 400 的使用者受理指示，将所受理的指示向控制部 410 输出。

1.6 不正当设备检测系统 1 的动作

对不正当设备检测系统 1 的动作进行说明。

(1) DVD 播放器 400 进行的从存储卡 200a 取得设备 ID 的动作利用图 13 所示的流程图, 对 DVD 播放器 400 进行的从存储卡 200a 取得设备 ID 的取得动作进行说明。

DVD 播放器 400 的控制部 410 如果从输入输出部 402 获取了表示检测出存储卡的安装检测信息(步骤 S101 中的是), 则对认证部 411 指示以使其在与安装的存储卡之间进行相互的设备认证(步骤 S102), 在从认证部 411 获取的认证结果表示认证失败的情况下(步骤 S103 中的否), 控制部 410 将表示该情况的消息向显示部 408 输出并指示其进行显示(步骤 S105), 然后结束处理。

在所获取的认证结果表示认证成功的情况下(步骤 S103 中的是), 控制部 410 从设备 ID 存储部 401 读出设备 ID421(步骤 S106), 接着, 对输入输出部 402 输出表示读出存储在所安装的存储卡中的设备 ID 的读出指示, 进行指示以读出设备 ID(步骤 S107)。

存储卡 200 的输入输出部 201 从一般区域 205 的加密内容密钥列表 221 尝试设备 ID 的读出(步骤 S108), 将读出结果向 DVD 播放器 400 输出, 控制部 410 经由输入输出部 402 从安装的存储卡获取读出结果(步骤 S109)。

在所获取的读出结果是不存在信息的情况下, 或者在获取了 1 个以上的设备 ID 的情况下, 在其中不存在读出的设备 ID421 时(步骤 S110 中的是), 将所读出的设备 ID421 经由输入输出部 402 向安装的存储卡输出(步骤 S111), 存储卡 200 的输入输出部 201 将所获取的设备 ID 向加密内容密钥列表 221 写入(步骤 S112)。

(2) 登记装置 300 的加密内容密钥的取得动作

利用图 14~图 17 所示的流程图, 对登记装置 300 的从管理服务器装置 100 取得加密内容密钥的动作进行说明。

登记装置 300 的控制部 306 经由通信部 307 及因特网 10 向管理服务器装置 100 发送连接请求(步骤 S200)。接着, 控制部 306 对认证部 301 指示以使其在与管理服务器装置 100 之间进行相互的设备认证(步骤 S201), 如果从认证部 301 获取了表示设备认证失败的

认证结果（步骤 S203 中的否），则控制部 102 结束处理。如果从认证部 301 获取了表示设备认证成功的认证结果（步骤 S203 中的是），则控制部 306 从条码处理部 310 获取内容 ID（步骤 S204），从价格列表 321 读出包含有与所获取的内容 ID 相同的内容 ID 的价格信息，从所读出的结果信息中提取销售价格，将所获取的内容 ID 与所提取的销售价格向显示部 303 及 304 输出，对显示部 303 及 304 指示以将它们显示（步骤 S205）。

接着，控制部 306 对认证部 313 指示以使其在与安装的存储卡 200a 之间进行相互的设备认证（步骤 S206）。如果从认证部 313 获取了表示设备认证失败的认证结果（步骤 S207 中的否），则控制部 306 将表示设备认证失败的消息向显示部 303 及 304 输出，对显示部 303 及 304 指示以将它们显示（步骤 S209），然后结束处理。

如果从认证部 313 获取了表示设备认证成功的认证结果（步骤 S207 中的是），则控制部 306 经由输入输出部 305 将表示读出存储于存储卡 200a 中的媒体 ID 及设备 ID 的读出指示向存储卡 200a 输出（步骤 S210）。

接着，存储卡 200 的输入输出部 201 如果从认证部 202 获取了表示设备认证失败的认证结果（步骤 S208 中的否），则输入输出部 201 结束处理。

如果从认证部 202 获取了表示设备认证成功的认证结果（步骤 S208 中的是），则输入输出部 201 从一般区域 205 的加密内容密钥列表 221 中尝试设备 ID 的读出（步骤 S211），接着，将读出结果向 DVD 播放器 400 输出（步骤 S212）。

控制部 306 经由输入输出部 305 获取读出结果（步骤 S212）。

在获取了设备 ID 不存在信息“无”的情况下（步骤 S213），控制部 306 将表示在存储卡 200a 中并未存储设备 ID 的消息向显示部 303 及 304 输出，对显示部 303 及 304 指示以使其显示该消息（步骤 S214），接着结束处理。

在获取了多个设备 ID 的情况下（步骤 S213），控制部 306 将所获取的多个设备 ID 向显示部 303 及 304 输出，对显示部 303 及 304

指示以使其显示该多个设备 ID（步骤 S215），接着，从输入部 302 获取由使用者从上述多个设备 ID 之中选择的 1 个设备 ID 的指定（步骤 S216）。

接着，控制部 306 经由通信部 307，向管理服务器装置 100 发送表示内容密钥的请求的请求信息（步骤 S231），此外，将所获取的内容 ID、上述 1 个设备 ID 及所获取的媒体 ID 经由通信部 307 向管理服务器装置 100 发送（步骤 S232）。

管理服务器装置 100 的控制部 102 经由因特网 10 及通信部 101 从登记装置 300 获取内容密钥的请求、内容 ID、设备 ID 及媒体 ID（步骤 S231～步骤 S232），从管理表 120 中检索与所获取的设备 ID 相同的设备 ID（步骤 S233），在管理表 120 内不存在相同的设备 ID 的情况下（步骤 S234 中的否），设媒体 ID 总数为“1”（步骤 S235），将所获取的设备 ID 与媒体 ID 总数作为媒体 ID 信息，向管理表 120 写入（步骤 S236），接着将控制向步骤 S252 转移。

在管理表 120 内存在相同的设备 ID 的情况下（步骤 S234 中的是），控制部 102 从管理表 120 中提取包含相同的设备 ID 的媒体 ID 信息，判断在所提取的媒体 ID 信息中是否包含有与所获取的媒体 ID 相同的媒体 ID（步骤 S237），在不包含的情况下（步骤 S238 中的否），对包含在所提取的媒体 ID 信息中的媒体 ID 总数加上“1”的值（步骤 S239），将所获取的媒体 ID 追加写入到所提取的媒体 ID 信息中（步骤 S240）。

接着，控制部 102 判断包含在所提取的媒体 ID 信息中的媒体 ID 总数属于 (i) “100” 以下、(ii) “101” 以上 “150” 以下、(iii) “151” 以上 “199” 以下、(iv) “200” 以上的哪个范围中（步骤 S251）。

(i) 在媒体 ID 总数为“100” 以下的情况下（步骤 S251），或者在上述中，从管理表 120 检索与所获取的设备 ID 相同的设备 ID，并且在管理表 120 内不存在相同的设备 ID 的情况下（步骤 S234 中的否，步骤 S235、S236），控制部 102 将设备判断等级设定为表示使用者所使用的设备不是不正当设备的“0”（步骤 S252）。接着，将

设定为“0”的设备判断等级经由通信部 101 及因特网 10 向登记装置 300 发送（步骤 S253）。接着，加密部 107 从设备密钥列表 130 中读出包含有与所获取的设备 ID 相同的设备 ID 的设备密钥信息，从所读出的设备密钥信息中提取设备密钥（步骤 S265），选择部 105 从内容密钥列表 140 中读出包含有与所获取的内容 ID 相同的内容 ID 的内容密钥信息，从所读出的内容密钥信息中提取内容密钥，接着将所提取的内容密钥向加密部 107 输出（步骤 S266），接着，加密部 107 利用所提取的设备密钥，对所获取的内容密钥实施加密算法 E1 而生成加密内容密钥（步骤 S267），经由通信部 101 及因特网 10 将生成的上述加密内容密钥向登记装置 300 发送（步骤 S268）。

(ii) 在媒体 ID 总数为“101”以上“150”以下的情况下（步骤 S251），控制部 102 将设备判断等级设定为表示使用者所使用的设备是需要注意的设备的“1”（步骤 S254），将设定为“1”的设备判断等级经由通信部 101 及因特网 10 向登记装置 300 发送（步骤 S255），将所获取的设备 ID 向注意设备列表 150 追加写入（步骤 S256）。接着，将控制向步骤 S265 转移。

(iii) 在媒体 ID 总数为“151”以上“199”以下的情况下（步骤 S251），控制部 102 将设备判断等级设定为表示使用者所使用的设备是需要警告的设备的“2”（步骤 S257），将设定为“2”的设备判断等级经由通信部 101 及因特网 10 向登记装置 300 发送（步骤 S258），将所获取的设备 ID 向警告设备列表 160 追加写入（步骤 S259）。接着，控制部 102 从登记装置 300 经由因特网 10 及通信部 101 获取表示批准向使用者提供内容密钥的指示或表示不批准的指示（步骤 S260），在所获取的指示表示不批准的情况下（步骤 S261），结束处理。在所获取的指示表示批准的情况下（步骤 S261），将控制向步骤 S265 转移。

(iv) 在媒体 ID 总数为“200”以上的情况下（步骤 S251），控制部 102 将设备判断等级设定为表示使用者所使用的设备是不正当的设备的“3”（步骤 S262），将设定为“3”的设备判断等级经由通信部 101 及因特网 10 向登记装置 300 发送（步骤 S263），将所获

取的设备 ID 向不正当设备列表 170 追加写入（步骤 S264）。接着，结束处理。

接着，控制部 306 经由通信部 307 从管理服务器装置 100 获取设备判断等级（步骤 S253、S255、S258、S263）。并且有时也获取加密内容密钥（步骤 S268）。

接着，控制部 306 判断所获取的设备判断等级是“0”、“1”、“2”及“3”的哪一个（步骤 S281）。

在判断为所获取的设备判断等级是“0”的情况下（步骤 S281），控制部 306 将表示允许向使用者提供所获取的加密内容密钥的消息向显示部 303 及 304 输出，对显示部 303 及 304 指示以使其显示该消息（步骤 S282）。此外，将设备 ID 及内容 ID 经由输入输出部 305 向存储卡 200a 输出（步骤 S291），再将加密内容密钥经由输入输出部 305 向存储卡 200a 输出（步骤 S293）。

在判断为所获取的设备判断等级是“1”的情况下（步骤 S281），控制部 306 将对登记装置 300 的操作者表示注意的消息向显示部 303 及 304 输出，对显示部 303 及 304 指示以使其显示该消息（步骤 S283）。接着，将控制向步骤 S291 转移。

在判断为所获取的设备判断等级是“2”的情况下（步骤 S281），控制部 306 将对登记装置 300 的操作者表示警告的消息向显示部 303 及 304 输出，对显示部 303 及 304 指示以使其显示该消息（步骤 S284）。进而，经由输入部 301 从登记装置 300 的操作者获取表示批准或不批准向使用者提供该加密内容密钥的指示（步骤 S285），将所获取的指示向管理服务器装置 100 输出（步骤 S260）。在获取了不批准的指示的情况下（步骤 S287），控制部 306 结束处理。在获取了批准的指示的情况下（步骤 S287），接着，将控制向步骤 S291 转移。

在判断为所获取的设备判断等级是“3”的情况下（步骤 S281），控制部 306 将对登记装置 300 的操作者表示不正当的消息向显示部 303 及 304 输出，对显示部 303 及 304 指示以使其显示该消息（步骤 S288）。接着，控制部 306 结束处理。

存储卡 200 的输入输出部 201 获取设备 ID 及内容 ID（步骤 S291），

对应于设备 ID 而将内容 ID 写入到加密内容密钥列表 221 内（步骤 S292），获取加密内容密钥（步骤 S293），与内容 ID 相对应地将加密内容密钥写入到加密内容密钥列表 221 内（步骤 S294）。

（3）DVD 播放器 400 的加密内容的解密与再现

利用图 18～图 19 所示的流程图，对 DVD 播放器 400 的加密内容的解密与再现进行说明。

DVD 播放器 400 通过图 13 的流程图所示的步骤，从存储卡 200 取得设备 ID（步骤 S301）。接着，控制部 410 经由输入部 409 从 DVD 播放器 400 的使用者受理再现保存在 DVD 中的加密内容的指示（步骤 S302）。如果受理了上述指示，则经由读出部 405 从 DVD 读出内容 ID（步骤 S305），对输入输出部 402 输出内容 ID 及自身的设备 ID（步骤 S306）。存储卡 200 的输入输出部 201 尝试对应于内容 ID 及自身的设备 ID 两者的内容密钥的读出（步骤 S307），将读出结果向 DVD 播放器 400 输出（步骤 S308）。

接着，控制部 410 经由输入输出部 402 从存储卡获取读出结果（步骤 S308），在作为读出结果而获取了不存在信息“无”的情况下（步骤 S309），控制部 410 将表示该情况的消息向显示部 408 输出，对显示部 408 指示以使其显示该消息（步骤 S310），结束处理。

在读出结果是加密内容密钥的情况下（步骤 S309），解密部 404 根据控制部 410 的指示而从设备密钥存储部 403 读出设备密钥 422（步骤 S311），利用所读出的设备密钥作为密钥，对加密内容密钥实施解密算法 D1，生成再现内容密钥（步骤 S312）。

解密部 406 经由读出部 405 从 DVD 中读出加密内容（步骤 S313），利用再现内容密钥对所读出的加密内容实施解密算法 D2，生成再现内容（步骤 S314）。

再现部 407 将所获取的再现内容分离为压缩影像信息和压缩声音信息，将压缩影像信息解码而生成影像信息，将影像信息变换为模拟的影像信号，将压缩声音信息解码而生成声音信息，将声音信息变换为模拟的声音信号，监视器监视影像，附属于监视器的扬声器输出声音（步骤 S315）。

1.7 不正当设备检测系统 1 的总结

在不正当设备检测系统 1 中，不正当的 DVD 播放器不正当地存储有与唯一地识别正当的 DVD 播放器的设备 ID 相同的设备 ID，假设这样的仅存储 1 个相同的设备 ID 的不正当的 DVD 播放器在市场中流通了多个的情况。

存储有相同的设备 ID 的不正当的 DVD 播放器的使用者在将内容再现时，如上所述，不正当的 DVD 播放器将该 DVD 播放器所存储的设备 ID 写入到存储卡中。

存储在存储卡中的设备 ID 和唯一地识别该存储卡的媒体 ID 在使用者的新的 DVD 的购入时经由登记装置 300 被收集到管理服务器装置 100 中。

管理服务器装置 100 利用收集到的设备 ID 与媒体 ID 的多个组，统计对应于 1 个设备 ID 的媒体 ID 的数量而计算媒体 ID 总数，如果计算出的媒体 ID 总数是规定阈值以上，则判断具有该设备 ID 的 DVD 播放器是不正当的设备。

这里，假设上述阈值例如为“100”。该阈值表示一个使用者可能拥有的存储卡数量的最大值。如果是一个使用者，则即使具有 100 张以内的存储卡也不认为是不自然的。

但是，假设不正当的 DVD 播放器被制造了多个、例如被制造了 1000 台而流通，假设得到了不正当的 DVD 播放器的使用者具有 100 张的存储卡，由于 1000 台的不正当的 DVD 播放器存储有相同的设备 ID，所以管理服务器装置 100 计算出 $100 \text{ 张} \times 1000 = 100000$ 作为对应于该设备 ID 的媒体 ID 的数量。因此，在计算出超过一个人可能拥有的合理的存储卡的数量媒体 ID 总数的情况下，将具有该设备 ID 的 DVD 播放器推测为不正当的。

2、变形例 (1)

这里，对作为不正当设备检测系统 1 的第 1 变形例的不正当设备检测系统 1e (未图示) 进行说明。

在不正当设备检测系统 1 中，使用媒体 ID 总数来确定不正当的 DVD 播放器，但在不正当设备检测系统 1e 中，如以下说明，管理服

务器装置 100 与设备 ID 相对应地存储有分别识别以由该设备 ID 识别的 DVD 播放器再现的 1 个以上的内容的内容 ID, 将识别用由特定的设备 ID 识别的 DVD 播放器再现的内容的内容 ID 的集合、与在管理服务器装置 100 中存储而与上述设备 ID 相对应的内容 ID 的集合比较, 在一个集合是另一个集合的子集的情况、以及一个集合与另一个集合完全一致的情况下, 将由该设备 ID 识别的 DVD 播放器推测为正当的设备, 否则, 将由该设备 ID 识别的 DVD 播放器推测为不正当的设备。

不正当设备检测系统 1e 具有与不正当设备检测系统 1 同样的结构。这里, 以与不正当设备检测系统 1 的不同点为中心进行说明。

(1) 存储卡 200e 的结构

在不正当设备检测系统 1e 中, 代替不正当设备检测系统 1 的存储卡 200 而使用图 20 所示的存储卡 200e。

存储卡 200e 如图 20 所示, 由输入输出部 201e 及存储部 203e 构成。另外, 存储卡 200e 与存储卡 200 同样, 也可以还具备与存储卡 200 所具有的认证部 202 同样的认证部 202e (未图示)。

存储部 203e 具备一般区域 205e, 一般区域 205e 具有使用者履历信息列表 231e。

使用者履历信息列表 231e 具备用来存储 1 个以上的使用者履历信息的区域。

各使用者履历信息包括 1 个设备 ID 及 1 个内容 ID, 使用者履历信息对应于在 1 台设备 (在该实施方式中是 DVD 播放器) 中再现的 1 个内容。

设备 ID 是唯一地识别将与包含该设备 ID 的使用者履历信息相对应的内容再现的设备 (在该实施方式中是 DVD 播放器) 的识别信息。但是, 如上所述, 在存在不正当地存储媒体 ID 的不正当设备的情况下, 并不限于能够唯一地识别设备。

内容 ID 是唯一地识别与包含该内容 ID 的使用者履历信息相对应的内容的识别信息。

输入输出部 201e 从存储部 203e 的一般区域 205e 中读出信息,

将读出的信息向安装存储卡 200e 的外部的装置输出。此外，从上述外部的装置获取信息，将所获取的信息向存储部 203e 的一般区域 205e 写入。这里，所谓的外部的装置，是登记装置及各 DVD 播放器。

(2) 管理服务器装置 100 的结构

管理服务器装置 100 具有与不正当设备检测系统 1 的管理服务器装置 100 同样的结构。

管理服务器装置 100 在管理表存储部 103 中具有图 21 所示的服务器履历信息列表 120e。

服务器履历信息列表 120e 包括多个服务器履历信息，各服务器履历信息对应于在 1 台设备（在该实施方式中是 DVD 播放器）中再现的 1 个内容。

各服务器履历信息包括设备 ID 及内容 ID。

设备 ID 是唯一地识别将与包含该设备 ID 的服务器履历信息相对应的内容再现的设备的识别信息。但是，如上所述，在存在不正当地存储有媒体 ID 的不正当的设备的情况下，并不限于能够唯一地识别设备。

内容 ID 是唯一地识别与包含该内容 ID 的服务器履历信息相对应的内容的识别信息。

控制部 102 经由登记装置 300 及因特网 10 从存储卡 200e 接收使用者履历信息列表，从接收到的使用者履历信息列表中提取设备 ID。这里，假设提取了 1 个设备 ID。

控制部 102 从服务器履历信息列表 120e 中提取全部的包含所提取的设备 ID 的服务器履历信息。将由所提取的全部的服务器履历信息构成的集合称作服务器履历信息群 β 。此外，将接收到的上述使用者履历信息列表称作集合 α 。

接着，控制部 102 将集合 α 与集合 β 比较，判断是集合 α 与集合 β 完全一致、集合 α 是集合 β 的子集、集合 β 是集合 α 的子集、还是其他的状态。

在集合 α 与集合 β 完全一致、集合 α 是集合 β 的子集、或者集合 β 是集合 α 的子集的情况下，控制部 102 将由提取的设备 ID 识别的

DVD 播放器作为正当的设备，使设备判断等级为“0”，在集合 β 是集合 α 的子集的情况下，将集合 β 与集合 α 的差追加写入到服务器履历信息列表 120e 中，将设备判断等级经由因特网 10 向登记装置 300 发送。

在是其他状态的情况下，控制部 102 将由提取的设备 ID 识别的 DVD 播放器作为不正当的设备，使设备判断等级为“3”，将所提取的设备 ID 向不正当设备列表追加写入，在集合 β 是集合 α 的子集的情况下，将集合 β 与集合 α 的差追加写入到服务器履历信息列表 120e 中，将设备判断等级经由因特网 10 向登记装置 300 发送。

(3) DVD 播放器的内容再现时的动作

利用图 22 所示的流程图对 DVD 播放器的内容再现时的动作进行说明。

DVD 播放器检测 DVD 的安装（步骤 S401），读出所存储的自身的设备 ID（步骤 S402），从所安装的 DVD 读出内容 ID（步骤 S403），将所读出的设备 ID 及内容 ID 的读出指示向存储卡 200e 输出（步骤 S404）。存储卡 200e 尝试设备 ID 与内容 ID 的组（视听履历信息）的读出（步骤 S405），将读出结果向 DVD 播放器输出（步骤 S406）。

DVD 播放器在读出结果表示不存在上述组的情况下，将上述设备 ID 及内容 ID 的写入指示向存储卡 200e 输出（步骤 S408）。存储卡 200e 将所获取的设备 ID 和内容 ID 写入到一般区域 205e 中（步骤 S411）。

另一方面，DVD 播放器从安装的 DVD 读出内容（步骤 S409），将所读出的内容再现（步骤 S410）。

(4) DVD 购入时的动作

利用图 23～图 24 所示的流程图，对 DVD 购入时的各装置的动作进行说明。

登记装置对安装的存储卡 200e 输出表示读出使用者履历信息列表的读出指示（步骤 S431），存储卡 200e 从一般区域 205e 读出使用者履历信息列表 231e（步骤 S432），将读出的使用者履历信息列表 231e 向登记装置 300 输出（步骤 S433）。

登记装置 300 将所获取的使用者履历信息列表经由因特网 10 向管理服务器装置 100 发送（步骤 S434）。

管理服务器装置 100 的控制部 102 从存储卡 200e 经由登记装置 300 及因特网 10 接收使用者履历信息列表（步骤 S433~S434），从接收到的使用者履历信息列表提取设备 ID（步骤 S435）。

接着，控制部 102 从服务器履历信息列表 120e 中提取所有包含所提取的设备 ID 的服务器履历信息（步骤 S436）。

接着，控制部 102 比较集合 α 与集合 β ，判断是集合 α 与集合 β 完全一致、集合 α 是集合 β 的子集、集合 β 是集合 α 的子集、还是其他的状态（步骤 S437）。

在集合 α 与集合 β 完全一致、集合 α 是集合 β 的子集、或者集合 β 是集合 α 的子集的情况下，控制部 102 使设备判断等级为“0”（步骤 S438），在集合 β 是集合 α 的子集的情况下，将集合 β 与集合 α 的差追加写入到服务器履历信息列表 120e 中（步骤 S441），将设备判断等级经由因特网 10 向登记装置 300 发送（步骤 S442）。

在是其他状态的情况下，控制部 102 使设备判断等级为“3”（步骤 S439），将所提取的设备 ID 向不正当设备列表追加写入（步骤 S440），在集合 β 是集合 α 的子集的情况下，将集合 β 与集合 α 的差追加写入到服务器履历信息列表 120e 中（步骤 S441），将设备判断等级经由因特网 10 向登记装置 300 发送（步骤 S442）。

（5）集合 α 与集合 β 的比较的例示

对于控制部 102 进行的集合 α 与集合 β 的比较，在表示例子的同时进行说明。这里，如上所述，集合 α 是从存储卡 200e 取得的，集合 β 是从管理服务器装置 100 所具有的服务器履历信息列表 120e 中提取的。

将集合 α 及集合 β 的第 1 例在图 25 中表示。该图所示的集合 α 601 作为内容 ID 而包括“C001”、“C002”、……、“C006”，集合 β 602 作为内容 ID 而包括“C001”、“C002”、……、“C005”。这样，集合 β 602 是集合 α 601 的子集，所以将所提取的设备 ID 判断为正当的。

另外，在图 25 所示的集合 $\alpha 601$ 及集合 $\beta 602$ 中，为了简化而省略作为集合的要素的一部分的设备 ID 的显示，仅显示内容 ID。在图 26、图 27 中也同样。

将集合 α 及集合 β 的第 2 例在图 26 中表示。该图所示的集合 $\alpha 603$ 作为内容 ID 而包括“C001”、“C002”，集合 $\beta 604$ 作为内容 ID 而包括“C001”、“C002”、……、“C005”。这样，集合 $\alpha 603$ 是集合 $\beta 604$ 的子集，所以在此情况下也将所提取的设备 ID 判断为正当的。

将集合 α 及集合 β 的第 3 例在图 27 中表示。该图所示的集合 $\alpha 605$ 作为内容 ID 而包括“X001”、“YC002”，集合 $\beta 606$ 作为内容 ID 而包括“M001”、“M002”。这样，集合 $\alpha 605$ 与集合 $\beta 606$ 相互不处于子集的关系，所以在此情况下将所提取的设备 ID 判断为不正当的。

(6) 补充说明 (1)

在使用者最初再现内容之前，在存储于存储卡 200e 中的使用者履历信息列表 231e 中不包含使用者履历信息。或者，在此情况下，在存储卡 200e 中也可以并未存储使用者履历信息列表 231e。

在此情况下，在登记装置 300 中安装有上述存储卡 200e 时，登记装置 300 由于在使用者履历信息列表 231e 中不包含使用者履历信息，或者由于不存在使用者履历信息列表 231e，所以不将使用者履历信息向管理服务器装置 100 发送。

(7) 补充说明 (2)

如上所述，在使用者最初再现内容之前，在存储于存储卡 200e 中的使用者履历信息列表 231e 中不包含使用者履历信息。

接着，如果使用者将由内容 ID “C001” 识别的内容再现，则在存储卡 200e 的使用者履历信息列表 231e 中写入由识别用于再现的设备的设备 ID、例如“ID-A”和内容 ID “C001”构成的使用者履历信息。

接着，将存储卡 200e 安装在登记装置 300 中，从登记装置 300 将使用者履历信息列表 231e 向管理服务器装置 100 发送，管理服务器装置 100 将由“ID-A”和内容 ID “C001”构成的使用者履历信

息写入到服务器履历信息列表 120e 中。

接着，如果使用者将由内容 ID “C002” 识别的内容再现，则在存储卡 200e 的使用者履历信息列表 231e 中写入由识别用于再现的设备的设备 ID、例如 “ID-A” 和内容 ID “C002” 构成的使用者履历信息。因而，在此情况下，使用者履历信息列表 231e 包括由 “ID-A” 和 “C001” 构成的使用者履历信息、以及由 “ID-A” 和 “C002” 构成的使用者履历信息。

接着，将存储卡 200e 安装在登记装置 300 中，从登记装置 300 将使用者履历信息列表 231e 向管理服务器装置 100 发送，管理服务器装置 100 将由 “ID-A” 和内容 ID “C002” 构成的使用者履历信息写入到服务器履历信息列表 120e 中。

以上，在使用者仅使用 1 张存储卡的情况下，由管理服务器装置 100 存储的集合 β 总是从存储卡 200e 发送来的集合 α 的子集。

接着，假设由于某种理由、使用者使用具有与存储卡 200e 相同结构的其他存储卡的情况。使用其他存储卡的理由可以考虑例如使用者将存储卡 200e 丢失的情况、存储卡 200e 损坏的情况、存储卡 200e 的存储容量全部用尽的情况等。

在此情况下，假设使用者使用上述其他的存储卡再现了由内容 ID “C001” 识别的内容。此时，在其他存储卡的使用者履历信息列表中写入由识别用于再现的设备的设备 ID、例如 “ID-A” 和内容 ID “C001” 构成的使用者履历信息。因而，在此情况下，该其他存储卡的使用者履历信息列表包括由 “ID-A” 和 “C001” 构成的使用者履历信息。

在此情况下，由于使用者仅使用第 2 张存储卡，所以由管理服务器装置 100 存储的集合 β 并不总是从存储卡 200e 发送来的集合 α 的子集，集合 α 为集合 β 的子集。

在这样的情况下，可以将由上述设备 ID 识别的设备看作正当的设备。

根据以上的理由，控制部 102 在集合 α 是集合 β 的子集的情况、和集合 β 是集合 α 的子集的情况这两种情况下，将由上述设备 ID 识

别的设备推测为正当的设备。

(8) 作为内容的再现装置的 DVD 播放器也可以如下所述构成。

DVD 播放器由以下部分构成：识别符存储部，存储有识别自身的设备识别符；履历存储部，如果安装了 BD，或者如果受理了使用者的存储在 BD 中的内容的再现指示，则每次、即每次在内容再现时，从 BD 取得识别该内容的内容识别符，并将所取得的内容识别符、和表示再现的日期时间的日期时间信息作为表示该内容的再现的再现履历信息，与内容的再现顺序一起进行存储；写入部，如果存储卡被安装到 DVD 播放器中，则对安装的存储卡，将上述设备识别符、上述再现履历信息及上述再现顺序写入到上述存储卡中。

3、变形例（2）

这里，对作为不正当设备检测系统 1e 的进一步的变形例的不正当设备检测系统 1f（未图示）进行说明。

在不正当设备检测系统 1f 中，如以下说明，管理服务器装置 100 与设备 ID 相对应地存储有分别识别用由该设备 ID 识别的 DVD 播放器再现的 1 个以上的内容的内容 ID、和表示将这些内容再现的顺序的再现顺序号，将识别用由特定的设备 ID 识别的 DVD 播放器再现的内容的内容 ID 及再现顺序号的集合、与在管理服务器装置 100 中存储的与上述设备 ID 相对应的内容 ID 及再现顺序号的集合进行比较，在一个集合与另一个集合完全一致的情况下，即在包含在一个集合中的所有的内容 ID 与包含在另一个集合中的所有的内容 ID 完全一致、并且关于一致的两个内容 ID 的各组、各自的再现顺序号一致的情况下，将由该设备 ID 识别的 DVD 播放器推测为正当的设备，否则，将由该设备 ID 识别的 DVD 播放器推测为不正当的设备。

不正当设备检测系统 1f 具有与不正当设备检测系统 1e 同样的结构。这里，以与不正当设备检测系统 1e 的不同点为中心进行说明。

（1）存储卡 200e 的结构

在不正当设备检测系统 1f 中，与不正当设备检测系统 1e 同样使用存储卡 200e。存储卡 200e 的存储部 203e 具备一般区域 205e，一般区域 205e 代替使用者履历信息列表 231e 而具有图 28 所示的使用

者履历信息列表 231f。这里，以与在不正当设备检测系统 1e 中使用的存储卡 200e 的不同点为中心进行说明。

使用者履历信息列表 231f 具备用来存储 1 个以上的使用者履历信息的区域。

各使用者履历信息包括 1 个设备 ID、1 个再现顺序号及 1 各内容 ID，使用者履历信息对应于在 1 台设备（在该实施方式中是 DVD 播放器）中再现的 1 个内容。

设备 ID 是唯一地识别将与包含该设备 ID 的使用者履历信息相对应的内容再现的设备（在该实施方式中是 DVD 播放器）的识别信息。但是，如上所述，在存在不正当地存储媒体 ID 的不正当设备的情况下，并不限于能够唯一地识别设备。

内容 ID 是唯一地识别与包含该内容 ID 的使用者履历信息相对应的内容的识别信息。

再现顺序号是表示与包含该再现顺序号的使用者履历信息相对应的内容，在上述设备中再现的序列的信息。

(2) 管理服务器装置 100 的结构

管理服务器装置 100 具有与不正当设备检测系统 1e 的管理服务器装置 100 同样的结构。这里，以与不正当设备检测系统 1e 的管理服务器装置 100 的不同点为中心进行说明。

管理服务器装置 100 在管理表存储部 103 中代替服务器履历信息列表 120e 而具有图 29 所示的服务器履历信息列表 120f。

服务器履历信息列表 120f 包括多个服务器履历信息，各服务器履历信息对应于在 1 台设备（在该实施方式中是 DVD 播放器）中再现的 1 个内容。

各服务器履历信息包括设备 ID、再现顺序号及内容 ID。

设备 ID 是唯一地识别将与包含该设备 ID 的服务器履历信息相对应的内容再现的设备的识别信息。但是，如上所述，在存在不正当地存储有媒体 ID 的不正当的设备的情况下，并不限于能够唯一地识别设备。

内容 ID 是唯一地识别与包含该内容 ID 的服务器履历信息相对应

的内容的识别信息。

再现顺序号是表示与包含该再现顺序号的服务器履历信息相对应的内容在上述设备中再现的顺序的信息。

控制部 102 经由登记装置 300 及因特网 10 从存储卡 200e 接收使用者履历信息列表，从接收到的使用者履历信息列表中提取设备 ID。这里，假设提取了 1 个设备 ID。

控制部 102 从服务器履历信息列表 120f 中提取全部的包含所提取的设备 ID 的服务器履历信息。将由所提取的全部的服务器履历信息构成的集合称作服务器履历信息群 β 。此外，将接收到的上述使用者履历信息列表称作集合 α 。

接着，控制部 102 将集合 α 与集合 β 比较，判断是集合 α 与集合 β 完全一致、还是其他的状态。

这里，所谓的完全一致，是指如下的状态。

包含在集合 α 中的所有的内容 ID，与包含在集合 β 中的所有的内容 ID 完全一致，并且，对于一致的两个内容 ID 的各组、对应于各个内容 ID 的两个再现顺序号一致。

在集合 α 与集合 β 完全一致的情况下，控制部 102 将由提取的设备 ID 识别的 DVD 播放器作为正当的设备，使设备判断等级为“0”，将设备判断等级经由因特网 10 向登记装置 300 发送。

在是其他状态的情况下，控制部 102 将由提取的设备 ID 识别的 DVD 播放器作为不正当的设备，使设备判断等级为“3”，将所提取的设备 ID 向不正当设备列表追加写入，将集合 α 追加写入到服务器履历信息列表 120f 中，将设备判断等级经由因特网 10 向登记装置 300 发送。

(3) DVD 购入时的动作

利用图 30 所示的流程图，对 DVD 购入时的管理服务器装置 100 的动作进行说明。

管理服务器装置 100 的控制部 102 从存储卡 200e 经由登记装置 300 及因特网 10 接收使用者履历信息列表，从接收到的使用者履历信息列表提取设备 ID，从服务器履历信息列表 120e 中提取所有包含

所提取的设备 ID 的服务器履历信息。

接着，控制部 102 比较集合 α 与集合 β ，在包含于集合 α 中的内容 ID 与包含在集合 β 中的内容 ID 一致的情况下（步骤 S437f），比较再现顺序号，在两个再现顺序号一致的情况下、即在集合 α 与集合 β 完全一致的情况下（步骤 S451），控制部 102 使设备判断等级为“0”（步骤 S438f）。

在是其他状态的情况下（步骤 S437f），控制部 102 使设备判断等级为“3”（步骤 S439f），将所提取的设备 ID 向不正当设备列表追加写入（步骤 S440f）。

（4）集合 α 与集合 β 的比较的例示

对于控制部 102 进行的集合 α 与集合 β 的比较，在表示例子的同时进行说明。这里，如上所述，集合 α 是从存储卡 200e 取得的，集合 β 是从管理服务器装置 100 所具有的服务器履历信息列表 120e 中提取的。

将集合 α 及集合 β 的第 1 例在图 31 中表示。该图所示的集合 α 611 作为再现顺序号及内容 ID 的组而包括{“1”，“C001”}、{“2”，“C002”}、{“3”，“C003”}、{“4”，“C004”}、{“5”，“C005”}，集合 β 612 作为再现顺序号及内容 ID 的组而包括{“1”，“C001”}、{“2”，“C002”}、{“3”，“C003”}、{“4”，“C004”}、{“5”，“C005”}。

在此情况下，由于集合 α 611 与集合 β 612 完全一致，所以将所提取的设备 ID 推测为正当的。

将集合 α 及集合 β 的第 2 例在图 32 中表示。该图所示的集合 α 613 作为再现顺序号及内容 ID 的组而包括{“2”，“C001”}、{“1”，“C002”}、{“3”，“C003”}、{“4”，“C004”}、{“5”，“C005”}，集合 β 614 作为再现顺序号及内容 ID 的组而包括{“1”，“C001”}、{“2”，“C002”}、{“3”，“C003”}、{“4”，“C004”}、{“5”，“C005”}。这样，如果比较集合 α 613 与集合 β 614，则虽然包含在各个集合中的内容 ID 一致，但内容 ID “C001” 及 “C002” 的再现顺序不同。因而，在此情况下，将所提取的设备 ID 推测为不正当的。

(5) 不正当设备检测系统 1f 的变形例

在上述中，在集合 α 与集合 β 完全一致的情况下推测为正当的设备，但并不限于此。除了集合 α 与集合 β 完全一致的情况以外，也可以为如下所示。

控制部 102 着眼于作为集合 α 的要素的一部分的内容 ID、和作为集合 β 的要素的一部分的内容 ID，比较作为集合 α 的要素的内容 ID 的集合 A、和作为集合 β 的要素的内容 ID 的集合 B，判断是集合 A 是集合 B 的子集、集合 B 是集合 A 的子集、还是其他的状态。

接着，控制部 102 在集合 A 是集合 B 的子集的情况下，以及集合 B 是集合 A 的子集的情况下，提取包含在集合 A 及集合 B 两者中的 1 个以上的内容 ID。

接着，对所提取的各内容 ID，从集合 α 中提取对应的再现顺序号，从集合 β 中提取对应的再现顺序号，判断所提取的两个再现顺序号是否一致。在所提取的两个再现顺序号不一致的情况下，将所提取的设备 ID 推测为识别不正当的设备的设备 ID。

在对于所提取的所有内容 ID，所提取的两个再现顺序号一致的情况下，将所提取的设备 ID 推测为识别正当的设备的设备 ID。

4、变形例 (3)

这里，对作为不正当设备检测系统 1f 的进一步的变形例的不正当设备检测系统 1g（未图示）进行说明。

如在对不正当设备检测系统 1f 的说明中所述，在使用者最初将内容再现之前，在存储于存储卡 200e 中的使用者履历信息列表 231f 中不包含使用者履历信息。

接着，如果使用者将由内容 ID “C001” 识别的内容再现，则将由识别用于再现的设备的设备 ID、例如 “ID-A” 和再现顺序号 “1” 以及内容 ID “C001” 构成的使用者履历信息，写入到存储卡 200e 的使用者履历信息列表 231f 中。

接着，将存储卡 200e 安装到登记装置 300 中，将使用者履历信息列表 231f 从登记装置 300 向管理服务器装置 100 发送，管理服务器装置 100 将由 “ID-A”、再现顺序号 “1” 和内容 ID “C001” 构

成的使用者履历信息写入到服务器履历信息列表 120f 中。

接着，如果使用者将由内容 ID “C002” 识别的内容再现，则将由识别用于再现的设备的设备 ID、例如 “ID-A”、再现顺序号 “2” 和内容 ID “C002” 构成的使用者履历信息写入到存储卡 200e 的使用者履历信息列表 231f 中。因而，在此情况下，使用者履历信息列表 231f 包括由 “ID-A”、“1” 和 “C001” 构成的使用者履历信息、和由 “ID-A”、“2” 和 “C002” 构成的使用者履历信息。

接着，将存储卡 200e 安装到登记装置 300 中，将使用者履历信息列表 231f 从登记装置 300 向管理服务器装置 100 发送，管理服务器装置 100 将由 “ID-A”、再现顺序号 “1” 和内容 ID “C002” 构成的使用者履历信息写入到服务器履历信息列表 120f 中。

如以上那样，在使用者仅使用 1 张存储卡的情况下，由管理服务器装置存储的集合 β 总是从存储卡 200e 发送的集合 α 的子集。

接着，假设使用者使用具有与存储卡 200e 相同的结构的其他存储卡，将由内容 ID “C003” 识别的内容再现。关于使用其他存储卡的理由如上所述。此时，在其他的存储卡的使用者信息列表中，写入识别用于再现的设备的设备 ID、例如 “ID-A”、再现顺序号 “1” 和内容 ID “C003” 构成的使用者履历信息。因而，在此情况下，该其他存储卡的使用者履历信息列表包括由 “ID-A”、再现顺序号 “1” 和 “C003” 构成的使用者履历信息。

在这样的情况下，由管理服务器装置 100 存储的集合 β 不是从存储卡 200e 发送的集合 α 的子集，此外，集合 α 也不是集合 β 的子集。但是，在这样的情况下也可以将由上述设备 ID 识别的设备看作是正当的。

这里，最初在存储卡 200e 的使用者履历信息列表 231f 中不包含使用者履历信息的状态、接着追加写入了由 “ID-A”、“1” 和 “C001” 构成的使用者履历信息的状态、再追加写入了由 “ID-A”、“2” 和 “C002” 构成的使用者履历信息的状态、然后追加写入了由 “ID-A”、再现顺序号和其他内容 ID 构成的使用者履历信息的状态、还包括然后的同样的状态，将这些多个状态称作属于相同的 1 个视听

履历系列（第1视听履历系列）。

此外，在其他存储卡的使用者履历信息列表中写入了由“ID-A”、再现顺序号“1”和内容ID“C003”构成的使用者履历信息的状态、接着写入了由“ID-A”、再现顺序号和其他内容ID构成的使用者履历信息的状态、还包括然后的同样的状态，将这些多个状态称作属于相同的1个视听履历系列（第2视听履历系列）。

第1视听履历系列与第2视听履历系列是对应于相同的设备ID的，但第1视听履历系列与第2视听履历系列是不同的。

（1）不正当设备检测系统1g的结构

不正当设备检测系统1g的管理服务器装置100利用存储在内部的服务器履历信息列表120f（与不正当设备检测系统1f所具有的服务器履历信息列表120f相同），从存储卡200f提取对应于与经由登记装置300接收到的设备ID相同的设备ID的、1个以上的视听履历系列，判断接收到的使用者履历信息列表所属于的视听履历系列是否与所提取的视听履历系列的任一个相同，如果相同，则计算表示所提取的视听履历系列的数量的系列数，如果不同，则对所提取的视听履历系列的数量加上“1”而计算系列数，将计算出的系列数与规定的阈值、例如“100”比较，如果计算出的系列数比“100”大，则将由接收到的设备ID识别的设备推测为不正当的设备，如果计算出的系列数比“100”小或相等，则将由接收到的设备ID识别的设备推测为正当的设备。

不正当设备检测系统1g具有与不正当设备检测系统1f相同的结构。这里，以与不正当设备检测系统1f的不同点为中心进行说明。

在不正当设备检测系统1g中，使用具有与不正当设备检测系统1f相同的结构的存储卡200e。存储卡200e具有图28所示的使用者履历信息列表231f。

（2）管理服务器装置100的结构

不正当设备检测系统1g的管理服务器装置100具有与不正当设备检测系统1f的管理服务器装置100同样的结构。这里，以与不正当设备检测系统1f的管理服务器装置100的不同点为中心进行说明。

管理服务器装置 100 在管理表存储部 103 中具有图 29 所示的服务器履历信息列表 120f。

关于服务器履历信息列表 120f 如上所述。另外，在服务器履历信息列表 120f 中，属于相同的视听履历系列的服务器履历信息相邻地配置，按再现顺序号的升序排列。

控制部 102 从存储卡 200e 经由登记装置 300 及因特网 10 接收使用者履历信息列表，从接收到的使用者履历信息列表中提取设备 ID。这里，设提取出 1 个设备 ID。

控制部 102 从服务器履历信息列表 120f 中提取全部包含所提取的设备 ID 的服务器履历信息。将所提取的全部的服务器履历信息称作服务器履历信息群。将服务器履历信息群的一例在图 34 中表示为服务器履历信息群 621。

接着，将所提取的所有的服务器履历信息如以下所示那样分类为 1 个以上的视听履历系列。

在服务器履历信息列表 120f 中，由于属于相同的视听履历系列的服务器履历信息相邻地配置，按再现顺序号的升序排列，所以将所提取的所有的服务器履历信息依次 1 个个地读出，将包含在所读出的服务器履历信息中的再现顺序号、和包含在前 1 个读出的服务器履历信息中的再现顺序号比较，如果该再现顺序号比前 1 个的再现顺序号小，则将前 1 个读出的服务器履历信息与该读出的服务器履历信息看作表示视听履历系列的边界，将到前 1 个为止读出的服务器履历信息作为 1 个视听履历系列，将该读出的服务器履历信息以后作为另一个视听履历系列。

在图 34 所示的服务器履历信息群 621 中，多个服务器履历信息的集合 631 属于 1 个视听履历系列，另外的多个服务器履历信息的集合 632 属于另 1 个视听履历系列，再另外的多个服务器履历信息的集合 633 属于再另 1 个视听履历系列。如该图所示，在集合 631 与集合 632 的边界上，再现顺序号的值从“3”减少为“1”。

这样，控制部 102 将所提取的所有的服务器履历信息分类为 1 个以上的视听履历系列。

接着，控制部 102 判断接收到的使用者履历信息列表所属于的视听履历系列，是否是与其所提取的视听履历系列的任一个相同的。如果相同，则计算表示其所提取的视听履历系列的数量的系列数，如果不同，则对所提取的视听履历系列的数目加上“1”而计算系列数。

接着，控制部 102 将计算出的系列数与规定的阈值、例如“100”比较，如果计算出的系列数比“100”大，则将由接收到的设备 ID 识别的设备推测为不正当的设备，将设备判断等级设为“3”，将所提取的设备 ID 向不正当设备列表追加写入，将接收到的使用者履历信息列表追加写入到服务器履历信息列表 120f 中，将设备判断等级经由因特网 10 向登记装置 300 发送。

如果计算出的系列数比“100”小或相等，则控制部 102 将由接收到的设备 ID 识别的设备推测为正当的设备，将设备判断等级设为“0”，将接收到的使用者履历信息列表追加写入到服务器履历信息列表 120f 中，将设备判断等级经由因特网 10 向登记装置 300 发送。

(3) DVD 购入时的动作

利用图 33 所示的流程图，对 DVD 购入时的管理服务器装置 100 的动作进行说明。

登记装置对安装的存储卡 200e 输出表示读出使用者履历信息列表的读出指示（步骤 S431），存储卡 200e 从一般区域 205e 中读出使用者履历信息列表 231f（步骤 S432），将读出的使用者履历信息列表 231f 向登记装置 300 输出（步骤 S433）。

登记装置 300 将所获取的使用者履历信息列表经由因特网 10 向管理服务器装置 100 发送（步骤 S434）。

管理服务器装置 100 的控制部 102 经由登记装置 300 及因特网 10 从存储卡 200e 接收使用者履历信息列表（步骤 S433～S434），从所接收到的使用者履历信息列表中提取设备 ID（步骤 S435）。

接着，控制部 102 从服务器履历信息列表 120f 中提取包含有所提取的设备 ID 的所有服务器履历信息（步骤 S436）。

接着，控制部 102 利用接收到的使用者履历信息列表及提取出的所有的服务器履历信息，提取视听履历系列，计算所提取的视听履历

系列的系列数，将计算出的系列数暂时存储在内部中（步骤 S461）。

接着，控制部 102 将计算并存储的系列数与“100”比较，如果计算并存储的系列数比“100”大（步骤 S462），则将设备判断等级设为“3”（步骤 S439），将所提取的设备 ID 向不正当设备列表追加写入（步骤 S440）。

如果计算并存储的系列数比“100”小或相等（步骤 S462），则控制部 102 将设备判断等级设为“0”（步骤 S438）。

接着，控制部 102 将接收到的使用者履历信息列表追加写入到服务器履历信息列表 120f 中（步骤 S441），将设备判断等级经由因特网 10 向登记装置 300 发送（步骤 S442）。

5、其他变形例

另外，根据上述实施方式对本发明进行了说明，但本发明当然并不限于上述的实施方式。以下这样的情况也包含在本发明中。

(1) 在上述的实施方式中，DVD 播放器将记录在 DVD 中的加密内容解密并再现，但并不限于此。也可以代替 DVD 播放器、由内容再现装置经由因特网取得加密内容而进行解密并再现。此外，也可以将加密内容通过数字广播而广播、数字广播接收装置接收广播波、从接收到的广播波中提取加密内容、将提取的加密内容解密并再现。

此外，也可以是，在可移动型的存储卡中与加密内容密钥一起记录加密内容，内容再现装置从存储卡读出加密内容、将读出的加密内容解密并再现。

(2) 在上述的实施方式中，对 DVD 播放器分配了 1 个设备密钥，但，分配给 1 个再现装置的设备密钥的个数并不一定是 1 个，也可以是多个。进而，也可以由多个设备 ID 共用相同的设备密钥。

(3) 在上述的实施方式中，将内容通过内容密钥加密、将内容密钥通过设备密钥加密，但本发明并不限于该结构。

例如，也可以在密钥层级中再追加一层，成为将内容通过内容密钥加密、将内容密钥通过媒体密钥加密、将媒体密钥通过设备密钥加密那样的密钥层级。密钥层级的层数中并不需要特别的限制。

(4) 在上述的实施方式中，管理服务器装置判断是使用内容的

正规设备还是不正当设备，来检测不正当设备，但本发明并不限于该结构。

例如，也可以代替将本发明应用到内容使用系统中、而应用到电车等的定期票使用系统中，管理设备判断其使用是正规使用还是不正当使用，来检测不正当使用。

例如，定期票使用系统由具有设备 ID 的便携终端、以及记录有定期票信息并具有媒体 ID 的可移动媒体的对、和设置在车站中的检票机构成。可移动媒体插入在便携终端中使用。检票机与上述实施方式的管理服务器装置同样地动作。检票机管理设备 ID 与媒体 ID 的组，例如在某可移动媒体插入在他人的便携终端中使用的情况下，管理设备能够判断该媒体 ID 以与不同的设备 ID 构成的组使用，所以能够检测可移动媒体的不正当利用。

进而，在此情况下，也可以是设置阈值、能够设定 1 个可移动媒体能够使用的设备的数量（设备 ID 的数量）的结构。

此外，只要是利用设备 ID 与媒体 ID 检测不正当设备、或不正当使用的系统，在上述以外的系统中也能够应用本发明。

(5) 在上述的实施方式中，为使用者保持可移动媒体而使用店铺设备的形态，但本发明并不限于该结构。

例如，也可以使用 MAC 地址来代替媒体 ID。经由网络将设备 ID 以及 MAC 地址发送给管理设备，管理设备利用 MAC 地址进行不正当设备的判断，如果不是不正当设备，则发送加密内容密钥。

此外，在 MAC 地址以外，也可以是使用具有不能改写的固有信息的、例如 IC 卡的形态。本发明只要是利用不能改写或变更的固有信息的形态，也可以是任何的结构来代替媒体 ID。

(6) 在本发明的实施方式中，为可移动媒体保持固有的媒体 ID 的形态，但本发明并不限于该结构。例如，也可以是设定的（可管理的）多个可移动媒体具有相同的媒体 ID 的结构。

(7) 在本发明的实施方式中，存在多个阈值，在超过了第 1 个阈值的情况下在判断为不正当设备之前发出警告，在超过了第 2 个阈值的情况下判断为不正当设备，但也可以使用 1 个阈值。如果比阈值

大则推测为不正当的设备，如果为阈值以下则推测为正当的设备。

(8) 在上述实施方式及变形例中，也可以使用 IC 卡来代替存储卡。

(9) 在上述实施方式及变形例中，也可以将管理服务器装置 100 与登记装置 300 结合、作为一体的装置来实现。

(10) 上述的各装置具体而言是由微处理器、ROM、RAM、硬盘单元、显示器单元、键盘、鼠标等构成的计算机系统。在上述 RAM 或上述硬盘单元中存储有计算机程序。这里，计算机程序是为了实现规定的功能而组合多个表示对计算机的指令的命令代码而构成的。通过上述微处理器按照上述计算机程序动作，各装置实现其功能。即，上述微处理器将包含在上述计算机程序中的各命令 1 个个地读出，将读出的命令解读，按照解读结果动作。

(11) 构成上述各装置的结构要素的一部分或全部也可以由 1 个系统 LSI (Large Scale Integration: 大规模集成电路) 构成。系统 LSI 是将多个结构部集成在 1 个芯片上而制造的超多功能 LSI，具体而言是包括微处理器、ROM、RAM 等而构成的计算机系统。在上述 RAM 中存储有计算机程序。通过上述微处理器按照上述计算机程序动作，系统 LSI 实现其功能。

此外，构成上述各装置的结构要素的各部可以单独地单芯片化，也可以包含一部分或全部而单芯片化。此外，这里设为 LSI，但根据集成度的不同，有时也称作 IC、系统 LSI、超 (super) LSI、甚 (ultra) LSI。

此外，集成电路化的方法并不限于 LSI，也可以通过专用电路或通用处理器实现。在 LSI 制造后，也可以使用可编程的 FPGA (Field Programmable Gate Array: 现场可编程门阵列) 及能够再构成 LSI 内部的电路单元的连接及设定的可重构处理器。

(12) 构成上述的各装置的结构要素的一部分或全部也可以在各装置中可装拆的 IC 卡或单体的模块构成。上述 IC 卡或上述模块是由微处理器、ROM、RAM 等而构成的计算机系统。上述 IC 卡或上述模块也可以包括上述超多功能 LSI。通过微处理器按照计算机程序动

作，上述 IC 卡或上述模块实现其功能。该 IC 卡或该模块也可以具有防篡改性。

(13) 本发明也可以是上述所示的方法。此外，也可以是通过计算机实现这些方法的计算机程序，也可以是由上述计算机程序构成的数字信号。

此外，本发明也可以是将上述计算机程序或上述数字信号记录在计算机可读的记录媒体、例如软盘、硬盘、CD-ROM、MO、DVD、DVD-ROM、DVD-RAM、BD (Blu-ray Disc: 蓝光光盘)、半导体存储器等中而成的产品。此外，也可以是记录在这些记录媒体中的上述计算机程序或上述数字信号。

此外，本发明也可以是将上述计算机程序或上述数字信号经由电气通信线路、无线或有线通信线路、以因特网为代表的网络、数据广播等传送的结构。

此外，本发明也可以是具备微处理器和存储器的计算机系统，上述存储器存储有上述计算机程序，上述微处理器按照上述计算机程序动作。

此外，也可以通过将上述程序或上述数字信号记录在上述记录媒体中并移送，或者将上述程序或上述数字信号经由网络等移送，由独立的其他计算机系统实施。

(14) 也可以将上述实施方式及上述变形例分别组合。

(15) 总结

如以上说明，本发明是由利用内容的利用设备、管理利用设备的不正当的管理设备、和记录数据的可移动媒体构成的不正当设备检测系统。上述利用设备具备存储能够识别该设备的设备识别信息的存储部。上述可移动媒体具备存储上述设备识别信息的第 1 存储区域、以及存储能够识别该可移动媒体的媒体识别信息的第 2 存储区域。上述管理设备具备从上述可移动媒体的第 1 存储区域及第 2 存储区域分别读出设备识别信息及媒体识别信息的读出部、和根据上述读出的设备识别信息及媒体识别信息判断保有上述设备识别信息的利用设备是否是不正当设备的判断部。

这里，上述管理设备也可以具备基于上述设备识别信息来生成管理媒体识别信息的管理表的表生成部。

这里，也可以是，上述管理设备具备存储用来判断是否是不正当设备的阈值的阈值存储部，上述管理设备的表生成部基于设备识别信息而计数媒体识别信息，生成存储上述计数的总数的管理表，上述管理设备的判断部在上述计数的总数超过存储在上述阈值存储部中的阈值的情况下判断为不正当设备。

这里，也可以是，上述管理设备的阈值存储部对每个设备识别信息存储1个以上的阈值。

这里，也可以是，上述管理设备具备：与设备识别信息相对应地存储设备密钥的设备密钥存储部、选择内容的利用所需的内容密钥的选择部、将由上述选择部选择的内容密钥通过对应于上述设备识别信息的设备密钥加密的加密部、和将上述加密的内容密钥写入到上述可移动媒体中的写入部，上述可移动媒体具备存储上述加密内容密钥的第3存储区域。

这里，也可以是，上述利用设备具备判断自身存储的设备识别信息是否存储在上述可移动媒体中的判断部、和在由判断部判断为没有存储的情况下将上述设备识别信息写入到上述可移动媒体的上述第1存储区域中的写入部。

这里，也可以是，上述可移动媒体具备存储内容的利用所需的加密的内容密钥的第3存储区域，上述利用设备具备从上述可移动媒体存储的第3存储区域中读出对应于该设备的加密内容的读出部。

这里，也可以是，上述可移动媒体具备存储内容的利用所需的加密的内容密钥的第3存储区域、和存储由上述内容密钥加密的内容的第4存储区域，上述利用设备具备从上述可移动媒体存储的第4存储区域中读出加密的内容的读出部。

这里，也可以是，上述可移动媒体具备存储内容的利用所需的加密的内容密钥的第3存储区域，上述利用设备具备从上述可移动媒体存储的第3存储区域判断是否存在该设备所需的加密内容密钥的判断部。

这里，上述可移动媒体也可以是存储卡。

这里，上述可移动媒体也可以是 IC 卡。

此外，本发明是管理利用内容的利用设备的不正当的管理设备，记录数据的可移动媒体具备存储能够识别上述利用设备的设备识别信息的第 1 存储区域、以及存储能够识别该可移动媒体的媒体识别信息的第 2 存储区域，上述管理设备具备从上述可移动媒体的第 1 存储区域及第 2 存储区域分别读出设备识别信息及媒体识别信息的读出部、和根据上述读出的设备识别信息及媒体识别信息判断保有上述设备识别信息的利用设备是否是不正当设备的判断部。

这里，也可以是，上述管理设备具备基于上述设备识别信息生成管理媒体识别信息的管理表的表生成部。

这里，也可以是，上述管理设备具备存储用来判断是否是不正当设备的阈值的阈值存储部，上述管理设备的表生成部基于设备识别信息而计数媒体识别信息，生成存储上述计数的总数的管理表，上述管理设备的判断部在上述计数的总数超过存储在上述阈值存储部中的阈值的情况下判断为不正当设备。

这里，也可以是，上述管理设备的阈值存储部对每个设备识别信息存储 1 个以上的阈值。

这里，也可以是，上述管理设备具备与设备识别信息相对应地存储设备密钥的设备密钥存储部、选择内容的利用所需的内容密钥的选择部、将由上述选择部选择的内容密钥通过对应于上述设备识别信息的设备密钥加密的加密部、和将上述加密的内容密钥写入到上述可移动媒体中的写入部。

此外，本发明是利用内容的利用设备，记录数据的可移动媒体具备存储能够识别上述利用设备的设备识别信息的第 1 存储区域、以及存储能够识别该可移动媒体的媒体识别信息的第 2 存储区域，上述利用设备具备存储能够识别该设备的设备识别信息的存储部。

这里，也可以是，上述利用设备具备判断自身存储的设备识别信息是否存储在上述可移动媒体中的判断部、和在由判断部判断为没有存储的情况下将上述设备识别信息写入到上述可移动媒体的上述第 1

存储区域中的写入部。

这里，也可以是，上述可移动媒体具备存储内容的利用所需的加密的内容密钥的第3存储区域，上述利用设备具备从上述可移动媒体存储的第3存储区域中读出对应于该设备的加密内容的读出部。

这里，也可以是，上述可移动媒体具备存储内容的利用所需的加密的内容密钥的第3存储区域、和存储由上述内容密钥加密的内容的第4存储区域，上述利用设备具备从上述可移动媒体存储的第4存储区域中读出加密的内容的读出部。

这里，也可以是，上述可移动媒体具备存储内容的利用所需的加密的内容密钥的第3存储区域，上述利用设备具备从上述可移动媒体存储的第3存储区域判断是否存在该设备所需的加密内容密钥的判断部。

此外，本发明也可是记录数据的可移动媒体，上述可移动媒体具备存储可识别利用内容的利用设备的设备识别信息的第1存储区域、以及存储可识别该可移动媒体的媒体识别信息的第2存储区域。

这里，也可以是，上述可移动媒体具备存储内容的利用所需的加密的内容密钥的第3存储区域。

这里，上述可移动媒体也可以是存储卡。

这里，上述可移动媒体也可以是IC卡。

此外，本发明是由管理不正当利用的管理设备、和记录数据的可移动媒体构成的不正当利用检测系统。上述可移动媒体具备存储能够识别利用设备的设备识别信息的第1存储区域、以及存储能够识别该可移动媒体的媒体识别信息的第2存储区域。上述管理设备具备从上述可移动媒体的第1存储区域及第2存储区域分别读出设备识别信息及媒体识别信息的读出部、和根据上述读出的设备识别信息及媒体识别信息判断保有上述设备识别信息的利用设备是否是不正当设备的判断部。

这里，也可以是，上述管理设备具备生成管理上述设备识别信息与上述媒体识别信息的组的管理表的表生成部、和基于上述媒体识别信息、在得到不同的设备识别信息的情况下将该利用判断为不正当的

判断部。

这里，也可以是，上述管理设备具备对每个上述媒体固有信息设置不同的阈值而存储的存储部。

此外，本发明是管理不正当利用的管理设备，记录数据的可移动媒体具备存储能够识别利用设备的设备识别信息的第1存储区域、以及存储能够识别该可移动媒体的媒体识别信息的第2存储区域。上述管理设备具备从上述可移动媒体的第1存储区域及第2存储区域分别读出设备识别信息及媒体识别信息的读出部、和根据上述读出的设备识别信息及媒体识别信息判断保有上述设备识别信息的利用设备是否是不正当设备的判断部。

这里，也可以是，上述管理设备具备生成管理上述设备识别信息与上述媒体识别信息的组的管理表的表生成部、和基于上述媒体识别信息、在得到不同的设备识别信息的情况下将该利用判断为不正当的判断部。

这里，也可以是，上述管理设备具备对每个上述媒体固有信息设置不同的阈值而存储的存储部。

此外，本发明是在利用内容的利用设备、管理利用设备的不正当的管理设备、和记录数据的可移动媒体中使用的不正当设备检测方法，其特征在于，包括：存储步骤，在上述利用设备中存储能够识别该设备的设备识别信息；第1存储步骤，在上述可移动媒体中存储上述设备识别信息；第2存储步骤，存储能够识别该可移动媒体的媒体识别信息；读出步骤，在上述管理设备中从上述可移动媒体的第1存储区域及第2存储区域分别读出设备识别信息及媒体识别信息；判断步骤，根据上述读出的设备识别信息及媒体识别信息判断保有上述设备识别信息的使用设备是否是不正当设备。

工业实用性

构成本发明的各装置及存储媒体在需要检测不正当的设备的所有的产业中，特别是在制作并分发内容的内容分发产业中，能够经营性地并持续及反复地使用。此外，构成本发明的各装置及记录媒体在电器设备制造产业中能够经营性地并持续及反复地制造、销售。

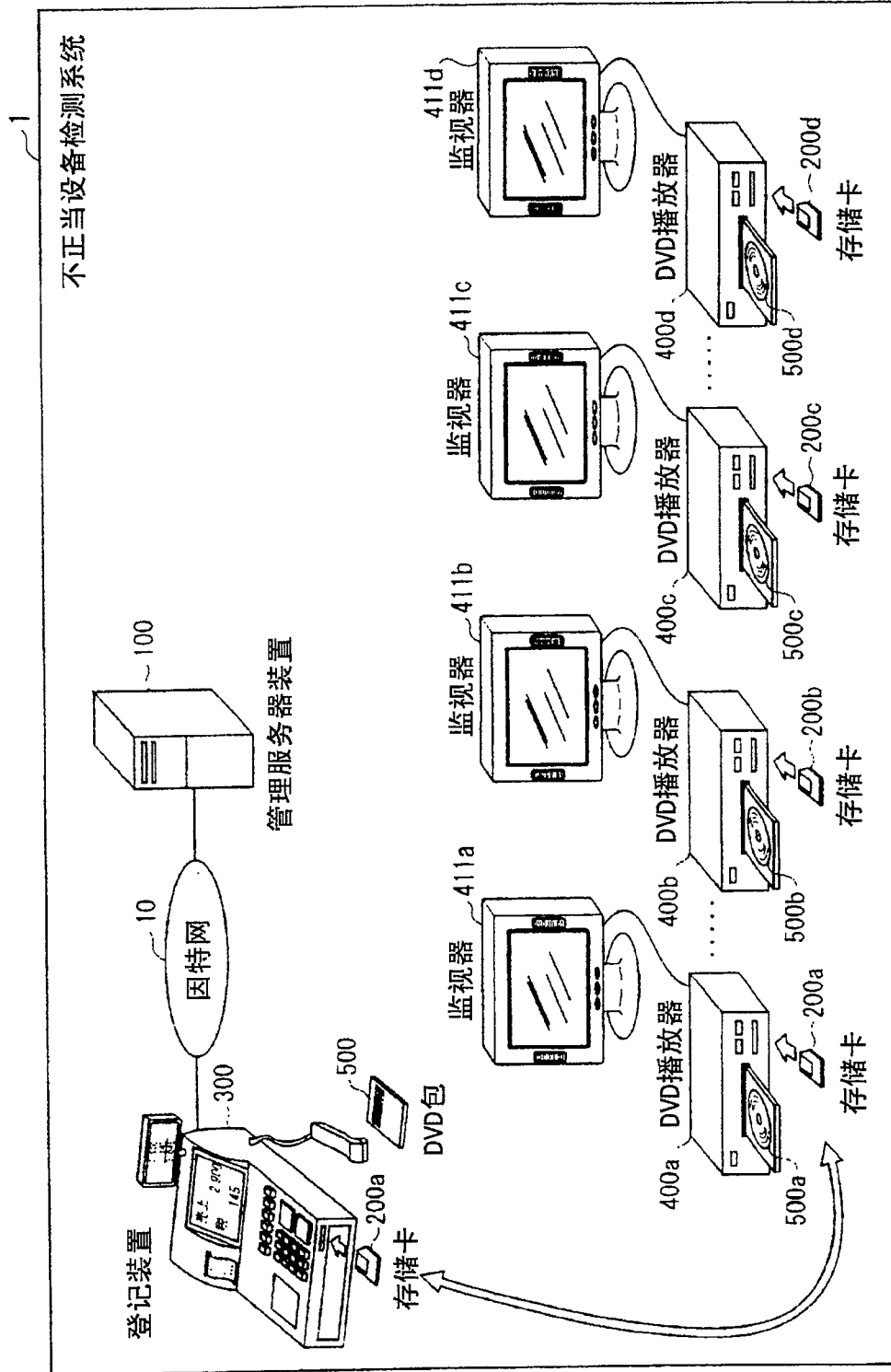


图1

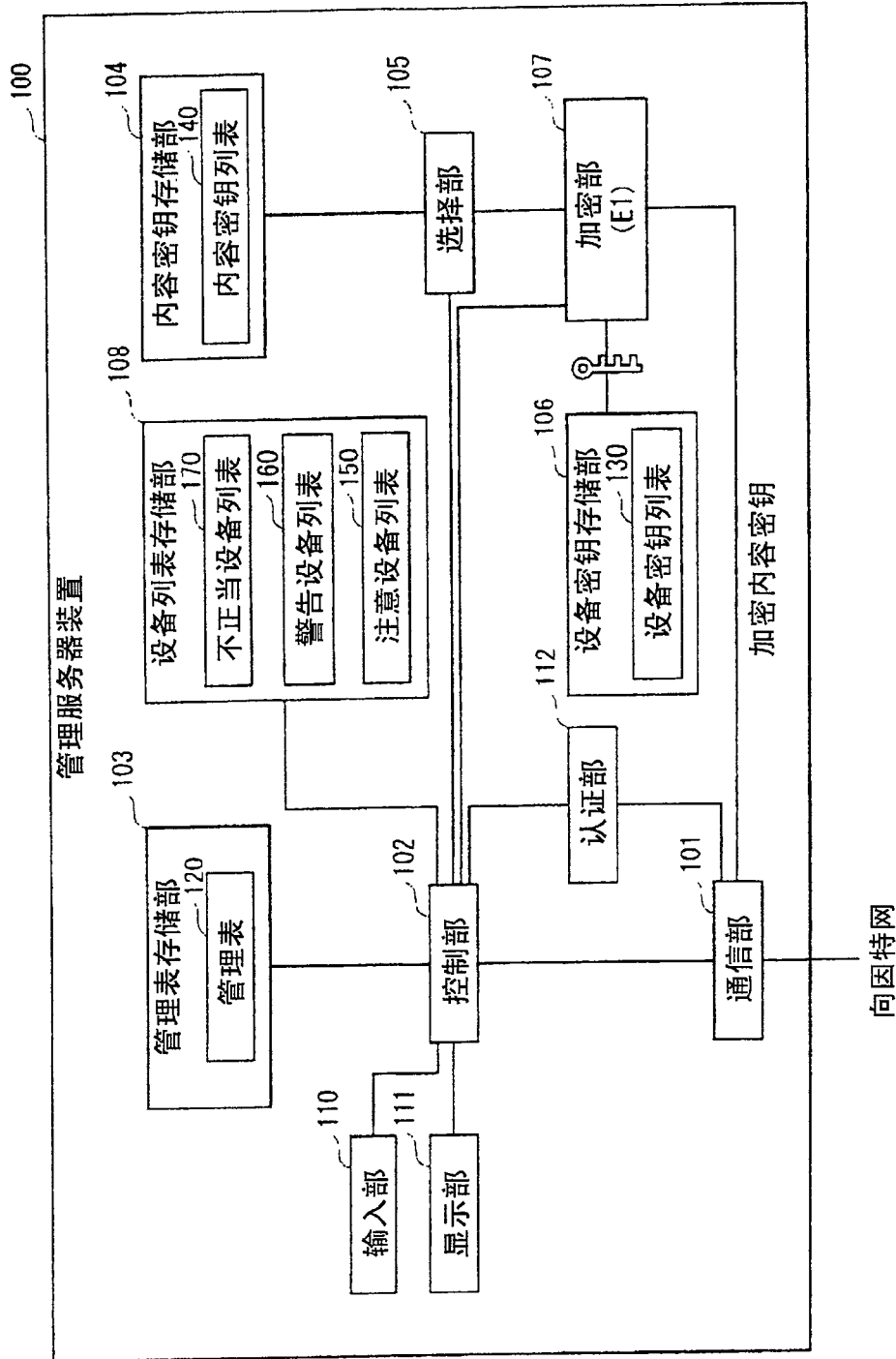


图2

120

126 管理表 122 123

媒体ID信息		
设备ID	媒体ID	媒体ID总数
ID-A	MID-1	2
	MID-5	
ID-B	MID-2	1
ID-C	MID-11	3
	MID-12	
	MID-13	
⋮	⋮	⋮

121 125 128 124 127 129

图3

设备密钥列表

设备密钥信息

设备ID	设备密钥
ID-A	DK-A
ID-B	DK-B
⋮	⋮

130

131

132

133

134

图4

140 ↙

内容密钥列表

内容密钥信息	
内容ID	内容密钥
C001	CK-1
C002	CK-2
C003	CK-3
⋮	⋮

141 — (points to the table)

143 — (points to the '内容密钥' header)

142 — (points to 'CK-1')

144 — (points to 'CK-2')

145 — (points to 'CK-3')

图5

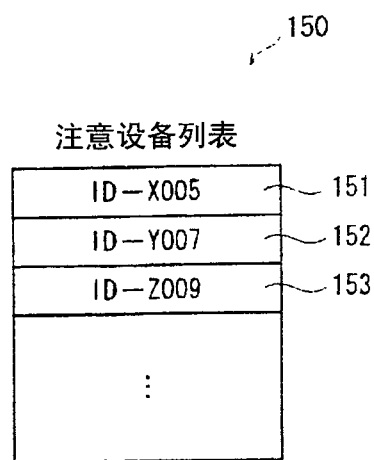


图6

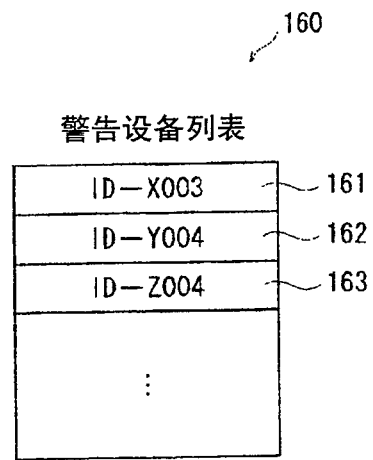


图7

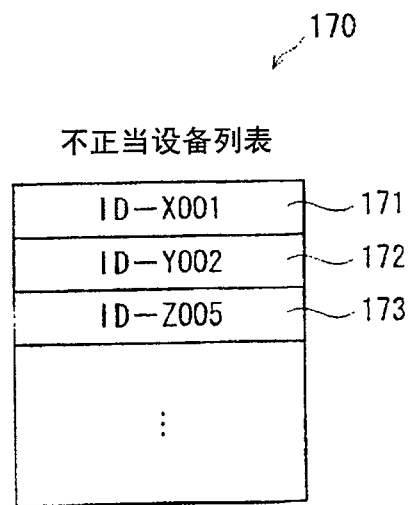


图8

媒体ID总数	~100	101~150	151~199	200~
登记装置的显示	允许显示	注意显示	警告显示	不允许显示
加密内容密钥的输出	有	有	以登记装置的操作者 的批准为条件而有	无
管理服务器装置中的登录	—	向注意设备列表登录	向警告设备列表登录	向不正当设备 列表登录

图9

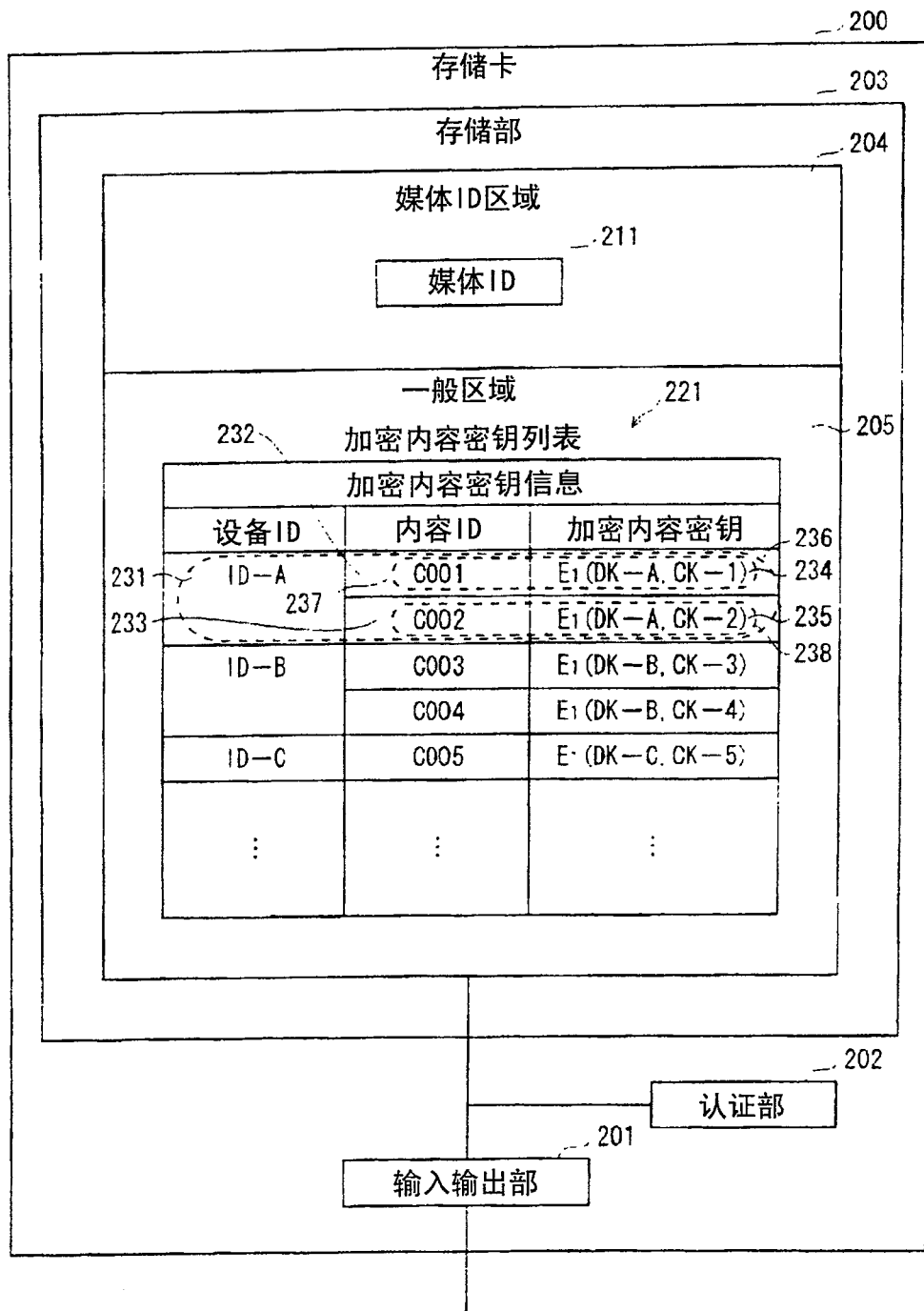


图10

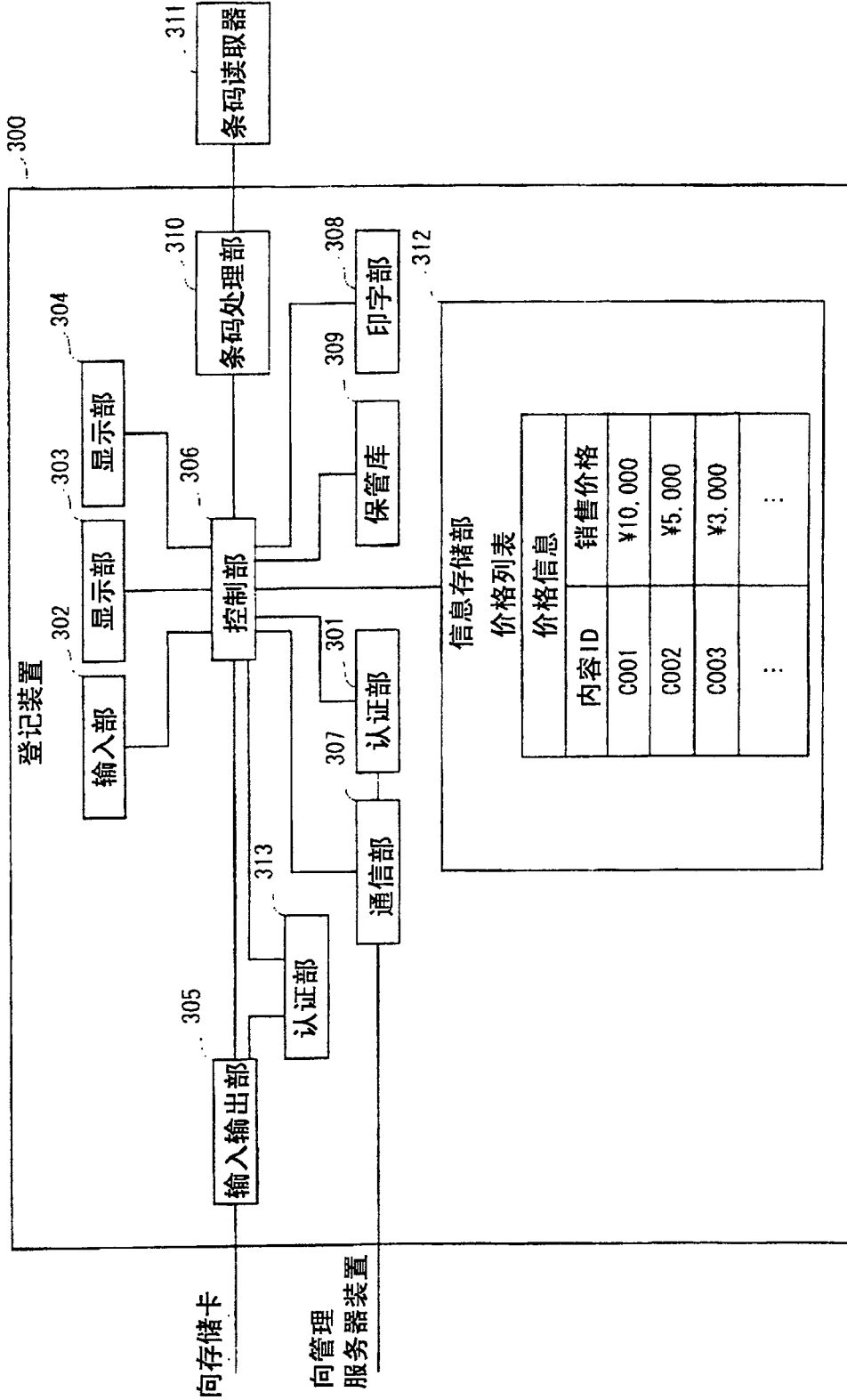


图11

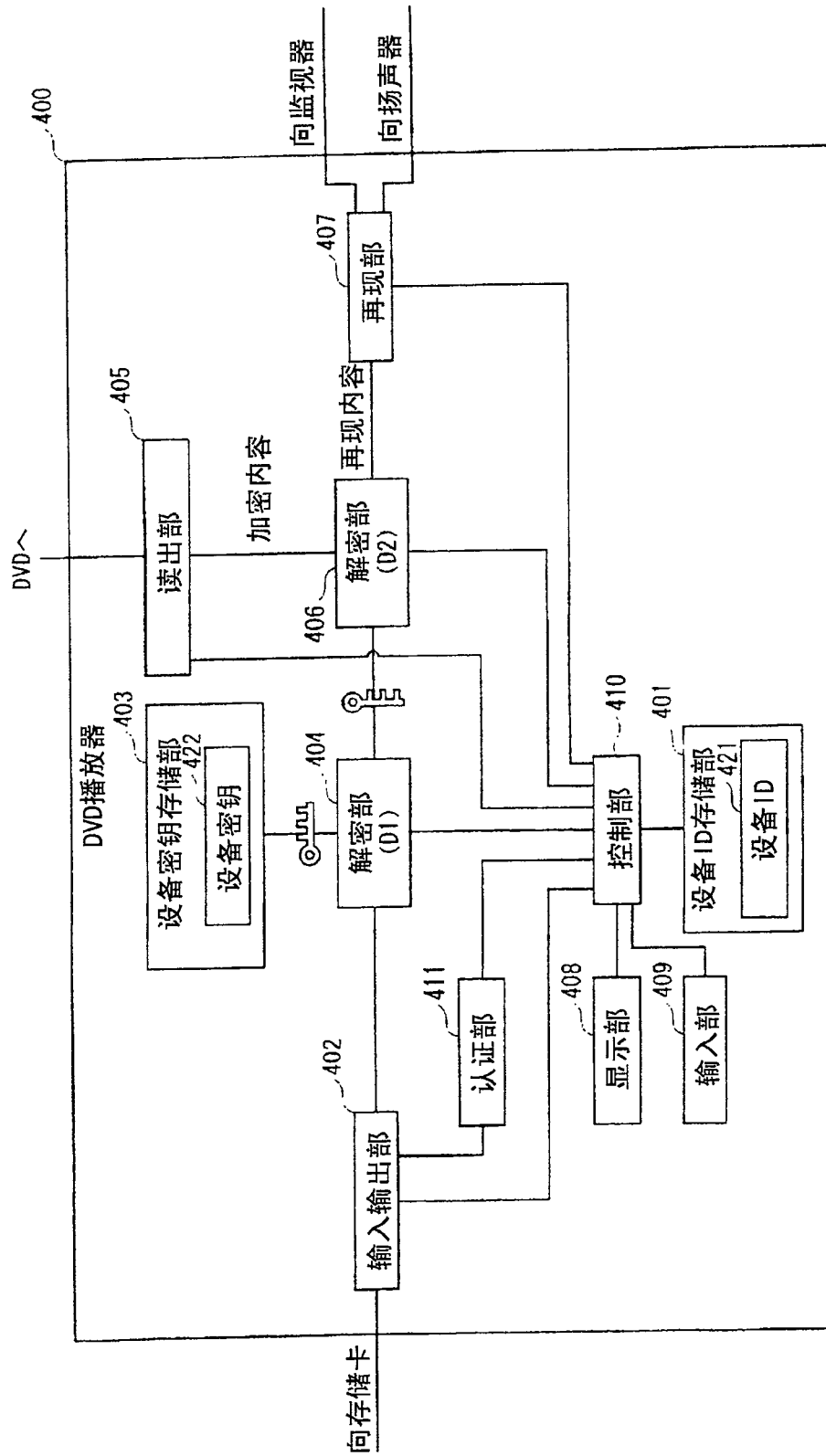


图12

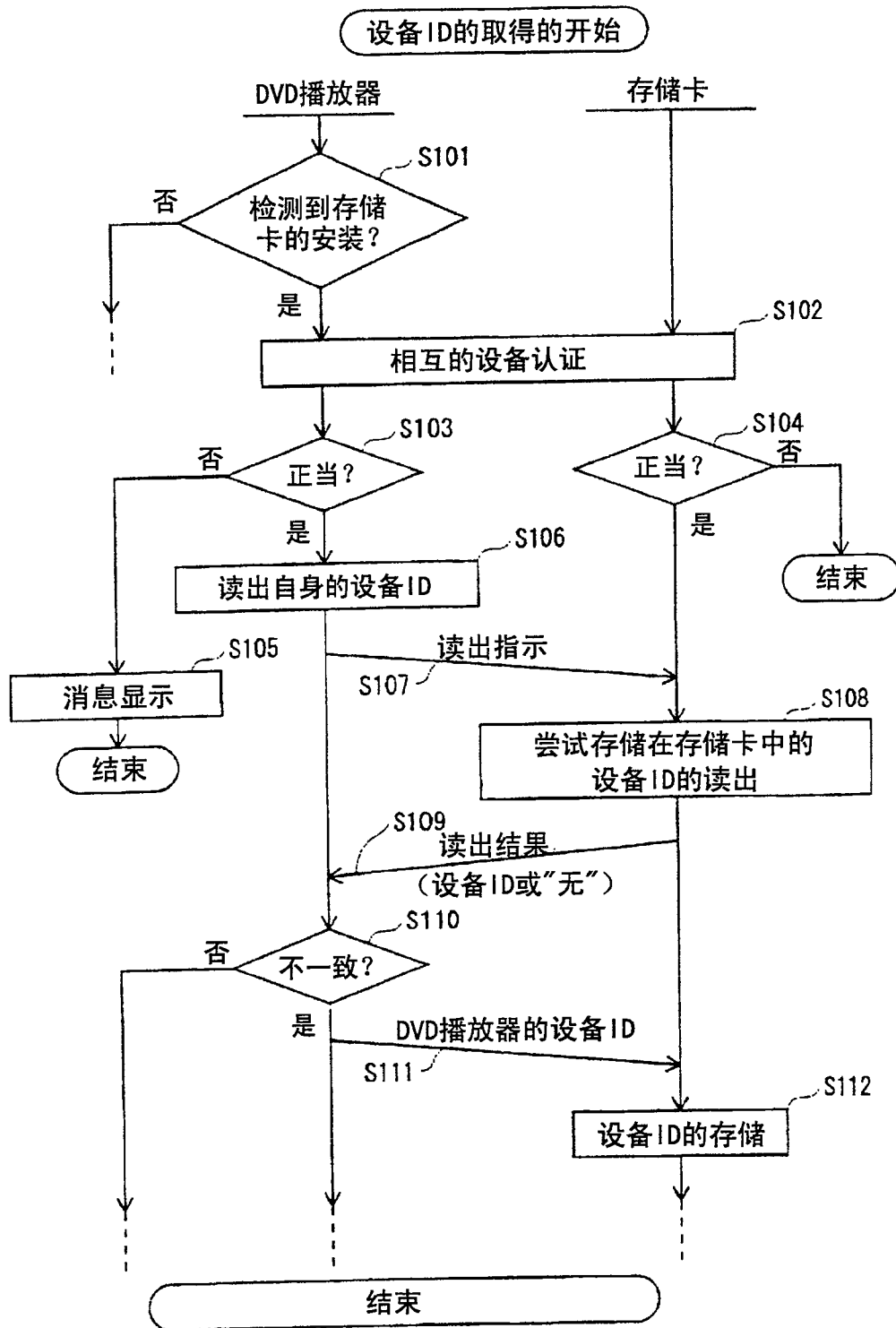


图13

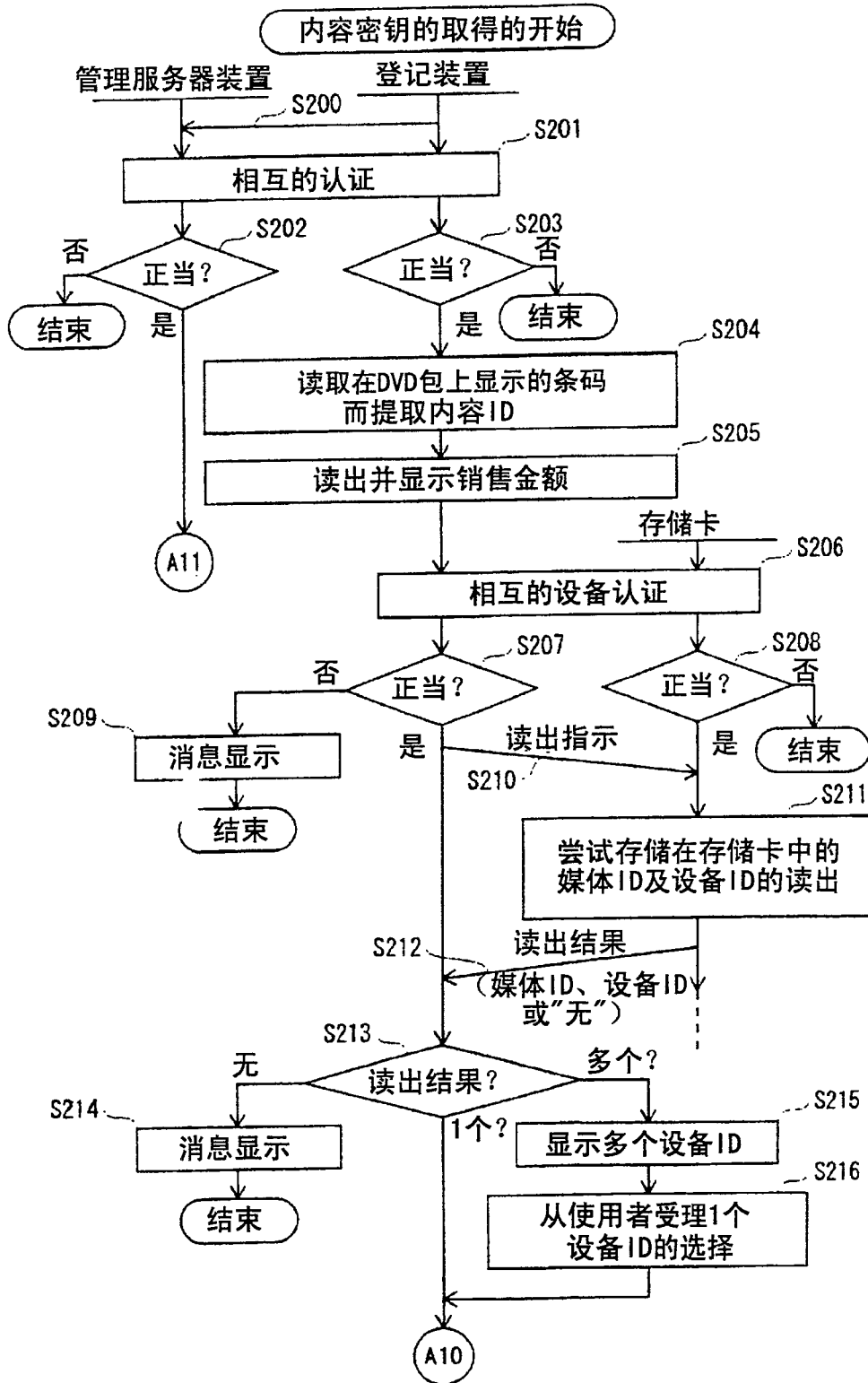


图14

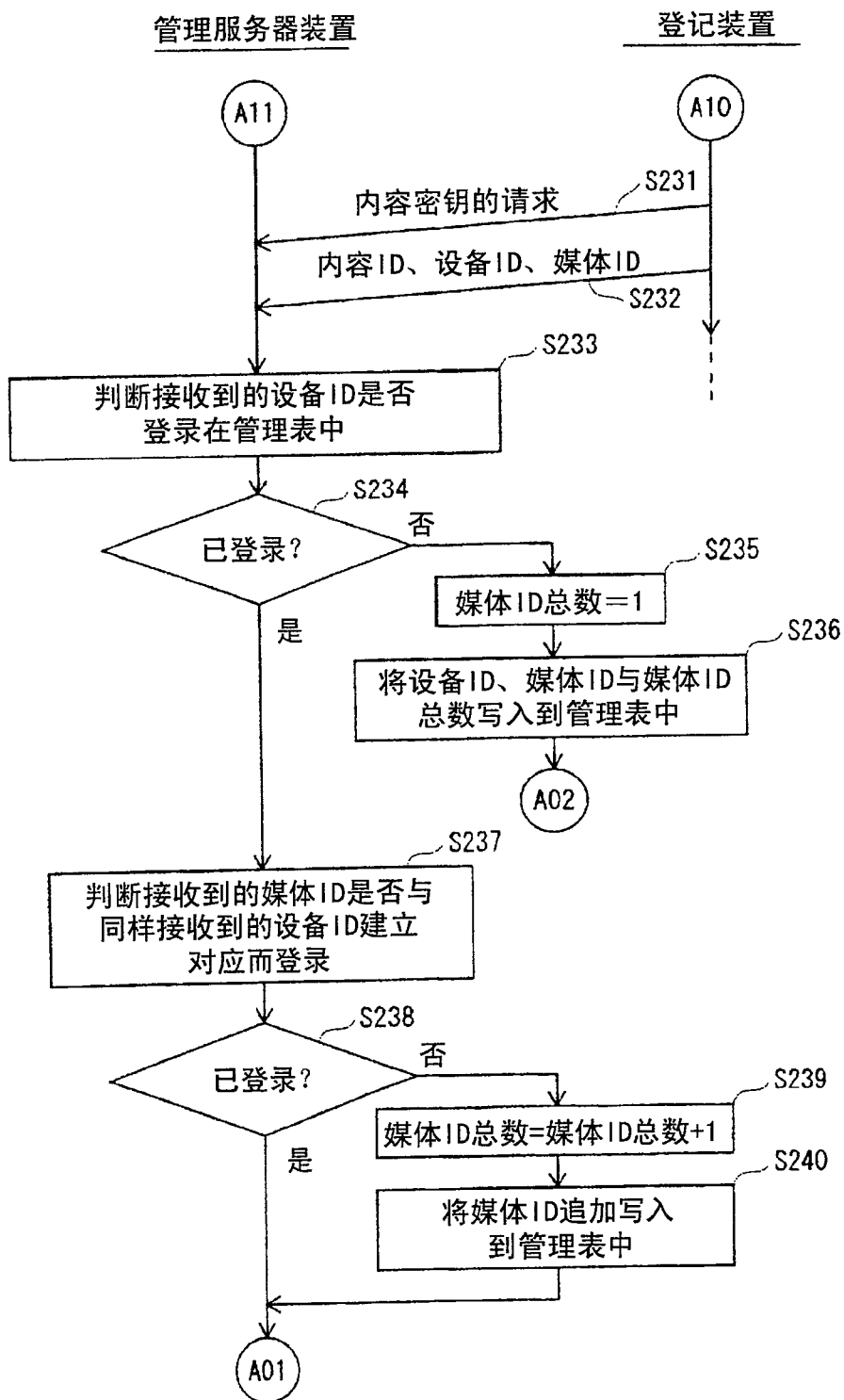


图15

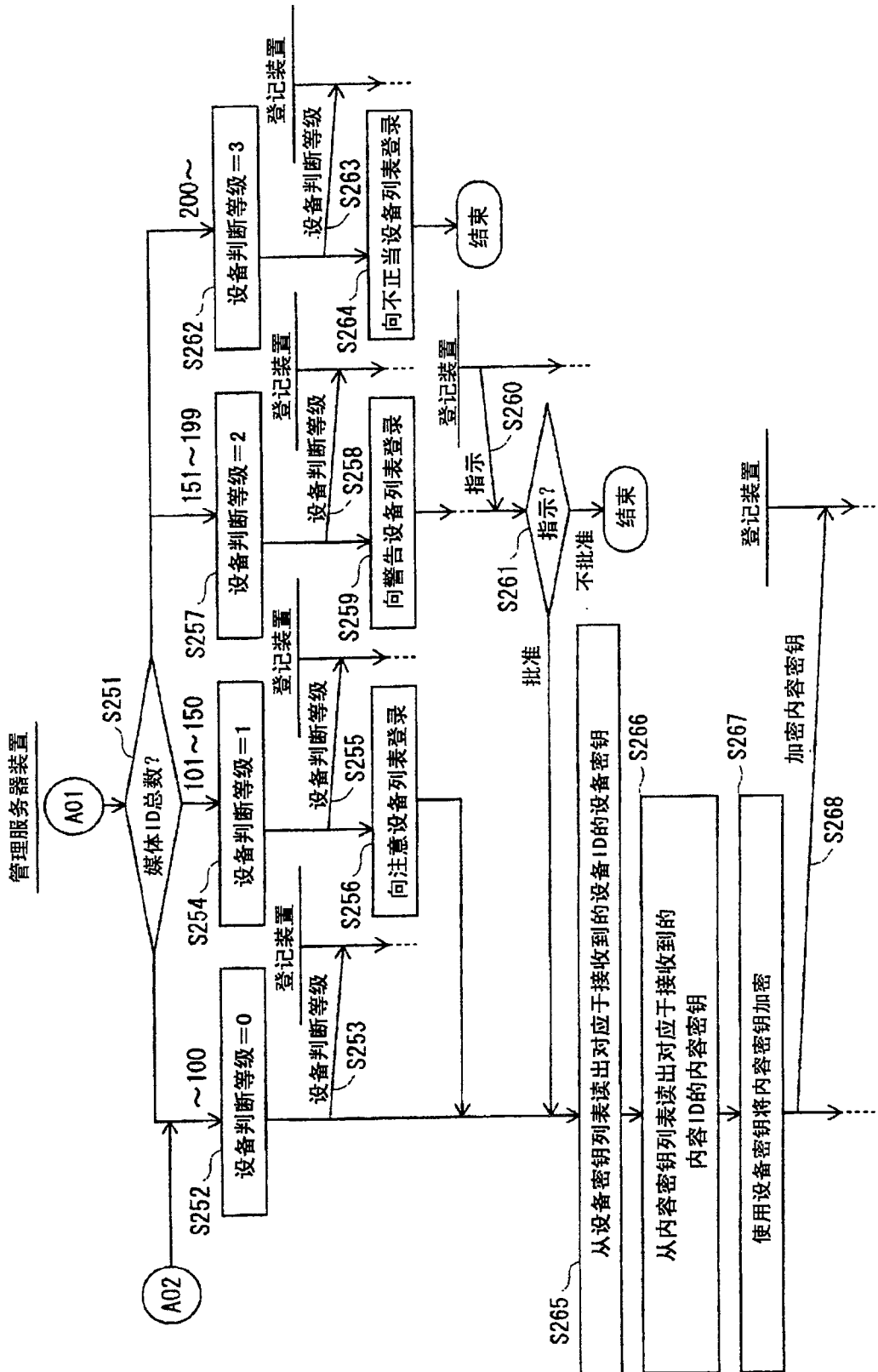


图16

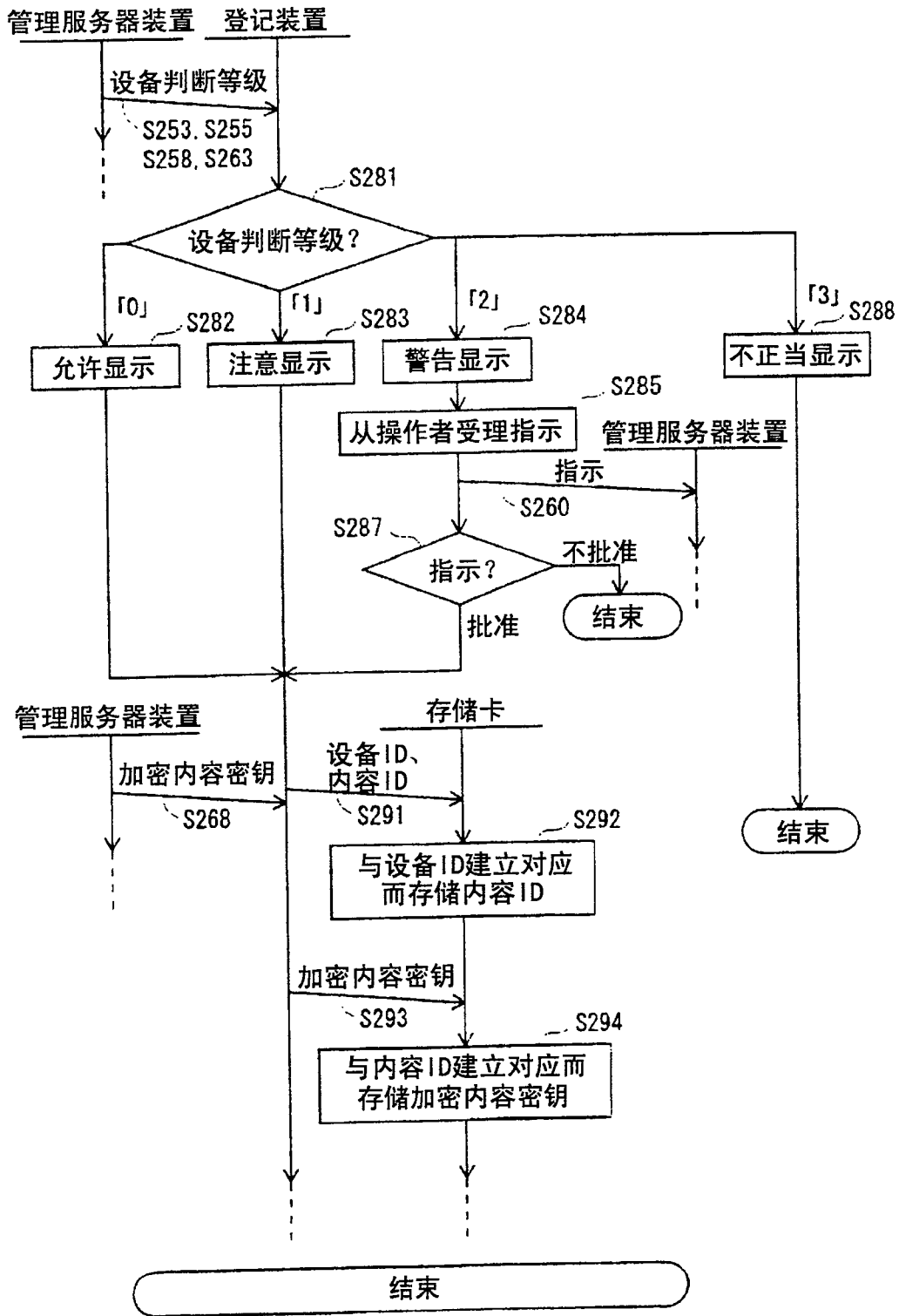


图17

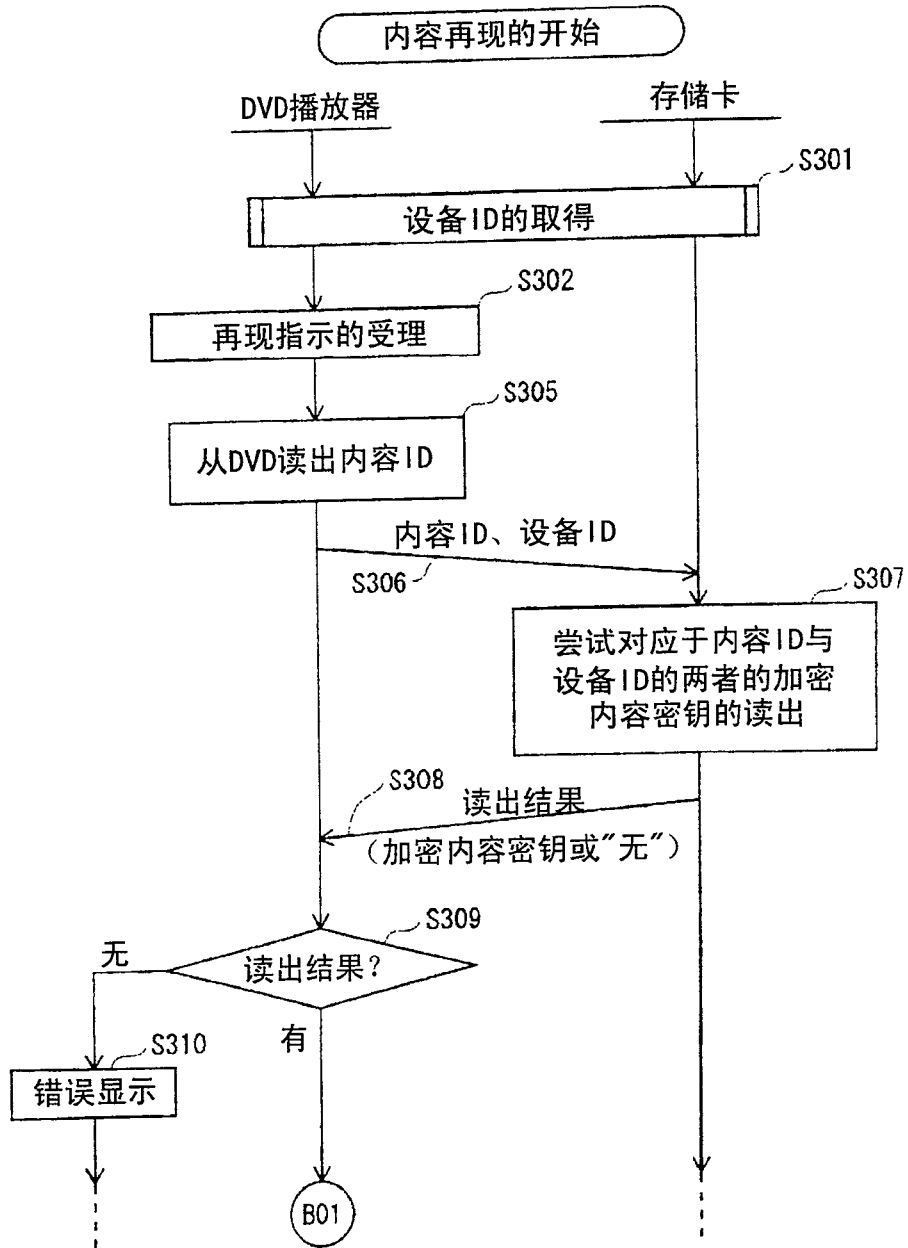


图18

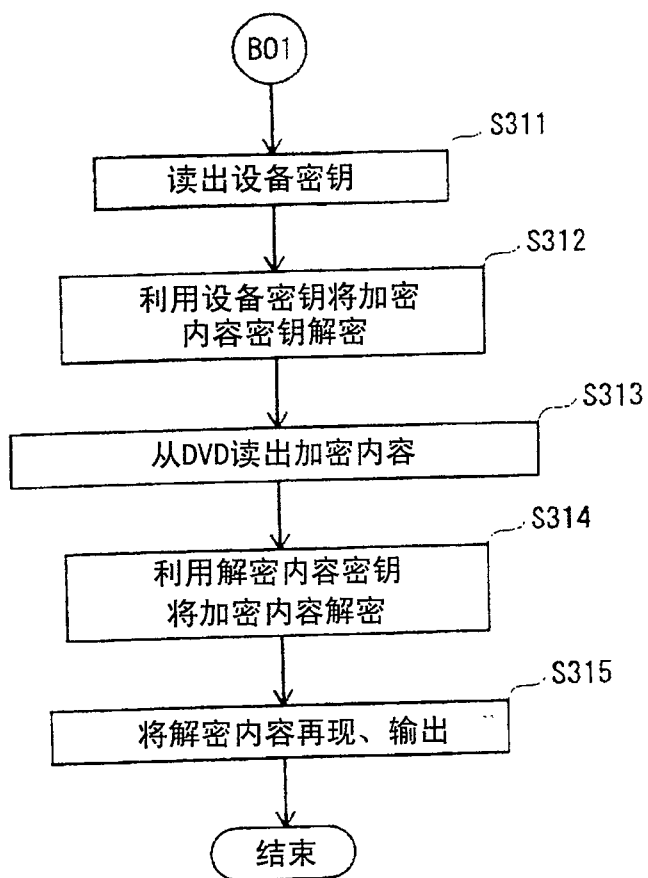


图19

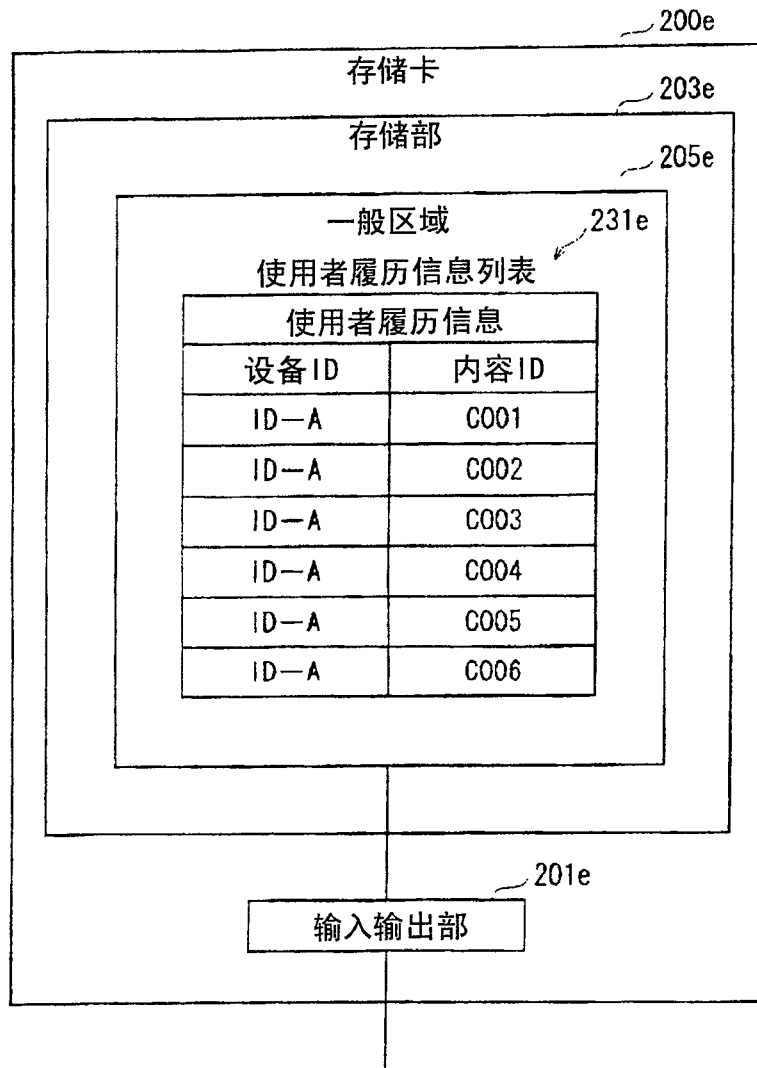


图20

120e

服务器履历信息列表

服务器履历信息	
设备ID	内容ID
ID-A	C001
ID-A	C002
⋮	⋮
ID-A	C005
⋮	⋮
ID-X	M001
ID-X	M002
ID-X	N001
ID-X	N002
ID-X	X001
ID-X	X002
ID-X	Y001
ID-X	Y002
⋮	⋮

图21

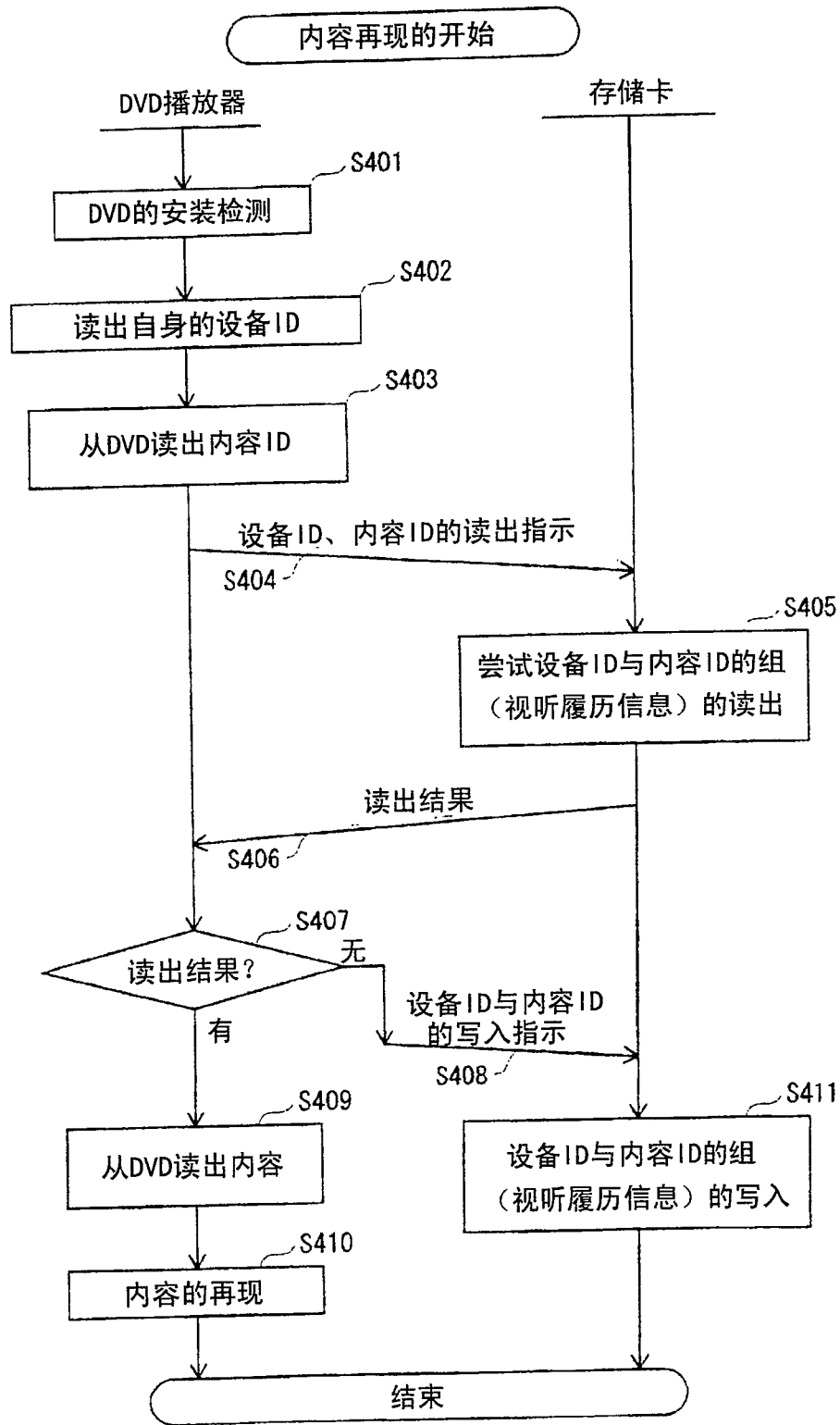


图22

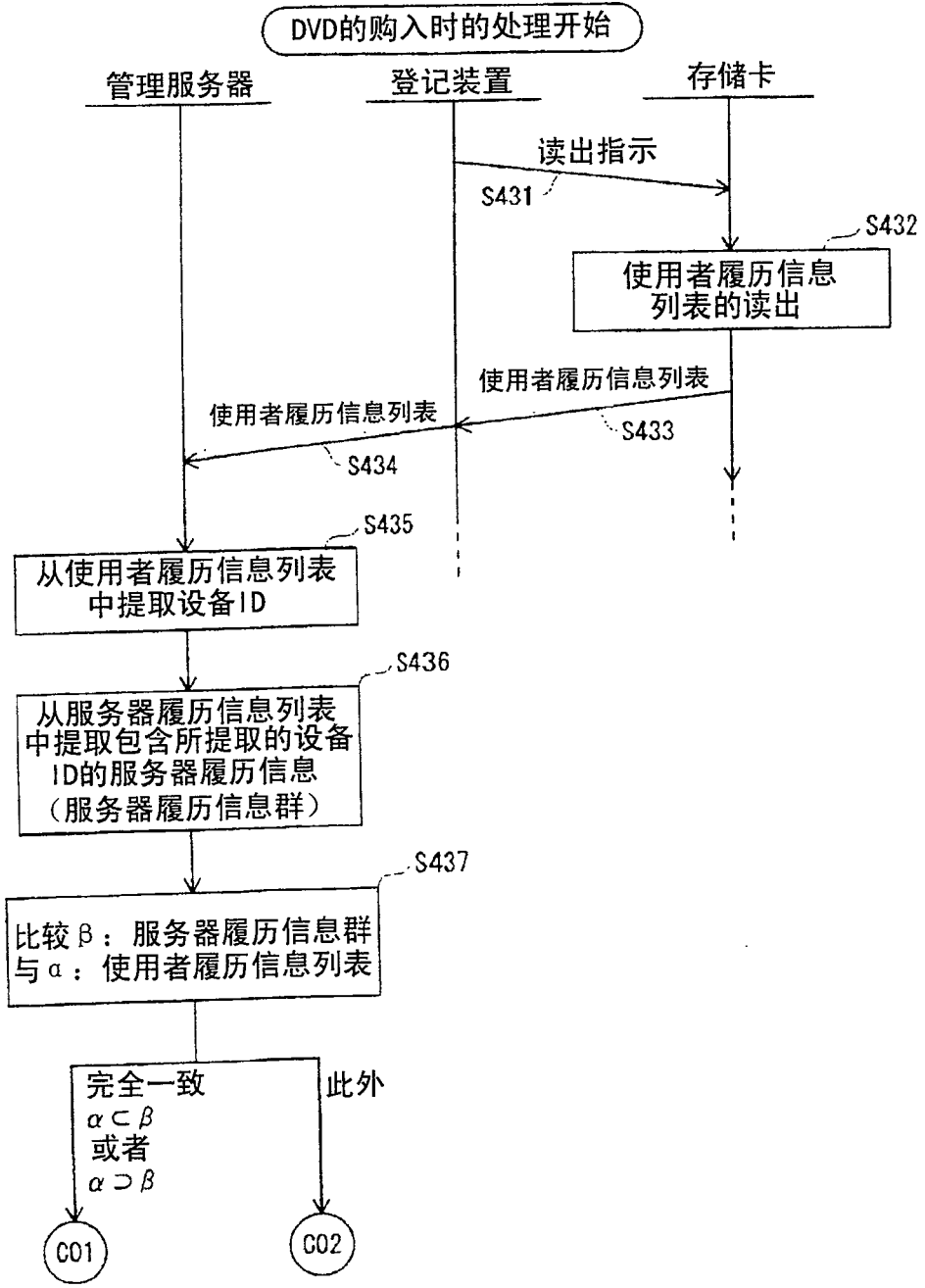


图23

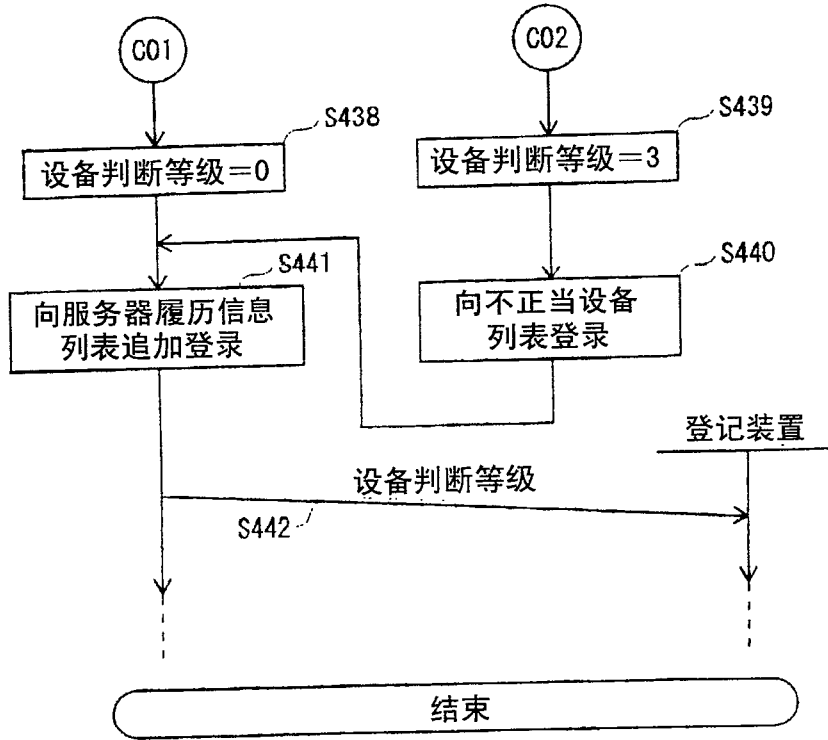


图24

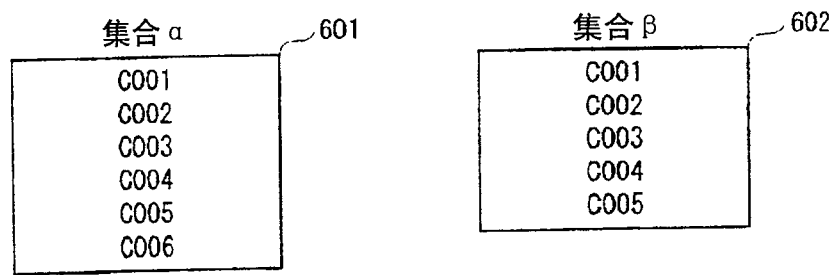


图25

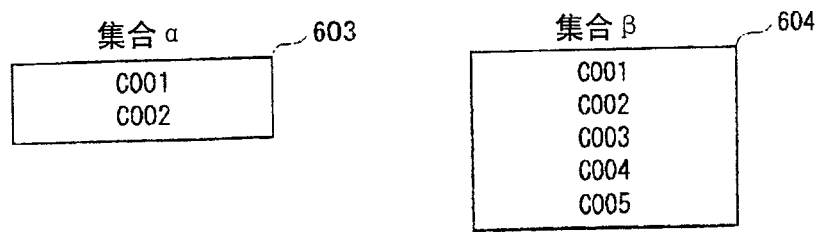


图26

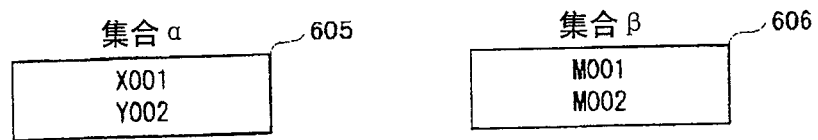


图27

231f

使用者履历信息列表

使用者履历信息		
设备ID	再现顺序号	内容ID
ID-A	1	C001
ID-A	2	C002
ID-A	3	C003
ID-A	4	C004
ID-A	5	C005
ID-A	6	C006

图28

120f

服务器履历信息列表

服务器履历信息		
设备ID	再现顺序号	内容ID
ID-A	1	C001
ID-A	2	C002
⋮	⋮	⋮
ID-A	5	C005
ID-X	1	M001
ID-X	2	M002
ID-X	3	M003
⋮	⋮	⋮

图29

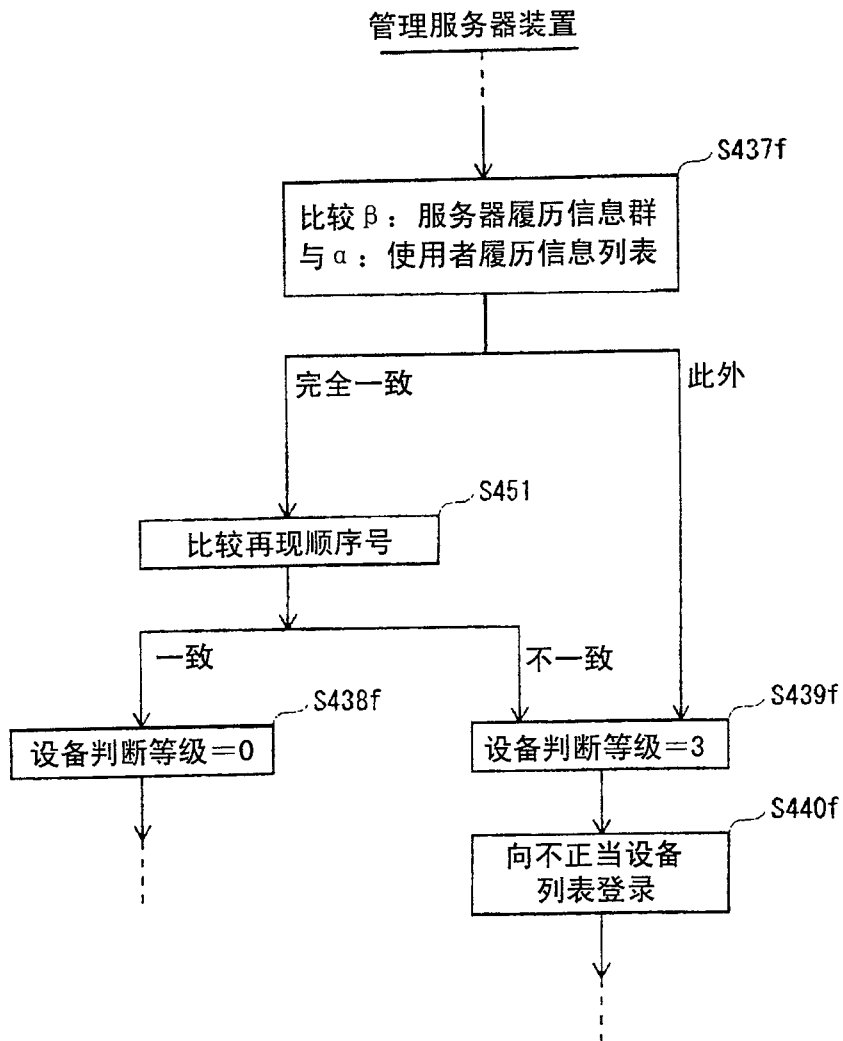


图30

集合 α 611

再现顺序号	内容ID
1	C001
2	C002
3	C003
4	C004
5	C005

集合 β 612

再现顺序号	内容ID
1	C001
2	C002
3	C003
4	C004
5	C005

图31

集合 α 613

再现顺序号	内容ID
2	C001
1	C002
3	C003
4	C004
5	C005

集合 β 614

再现顺序号	内容ID
1	C001
2	C002
3	C003
4	C004
5	C005

图32

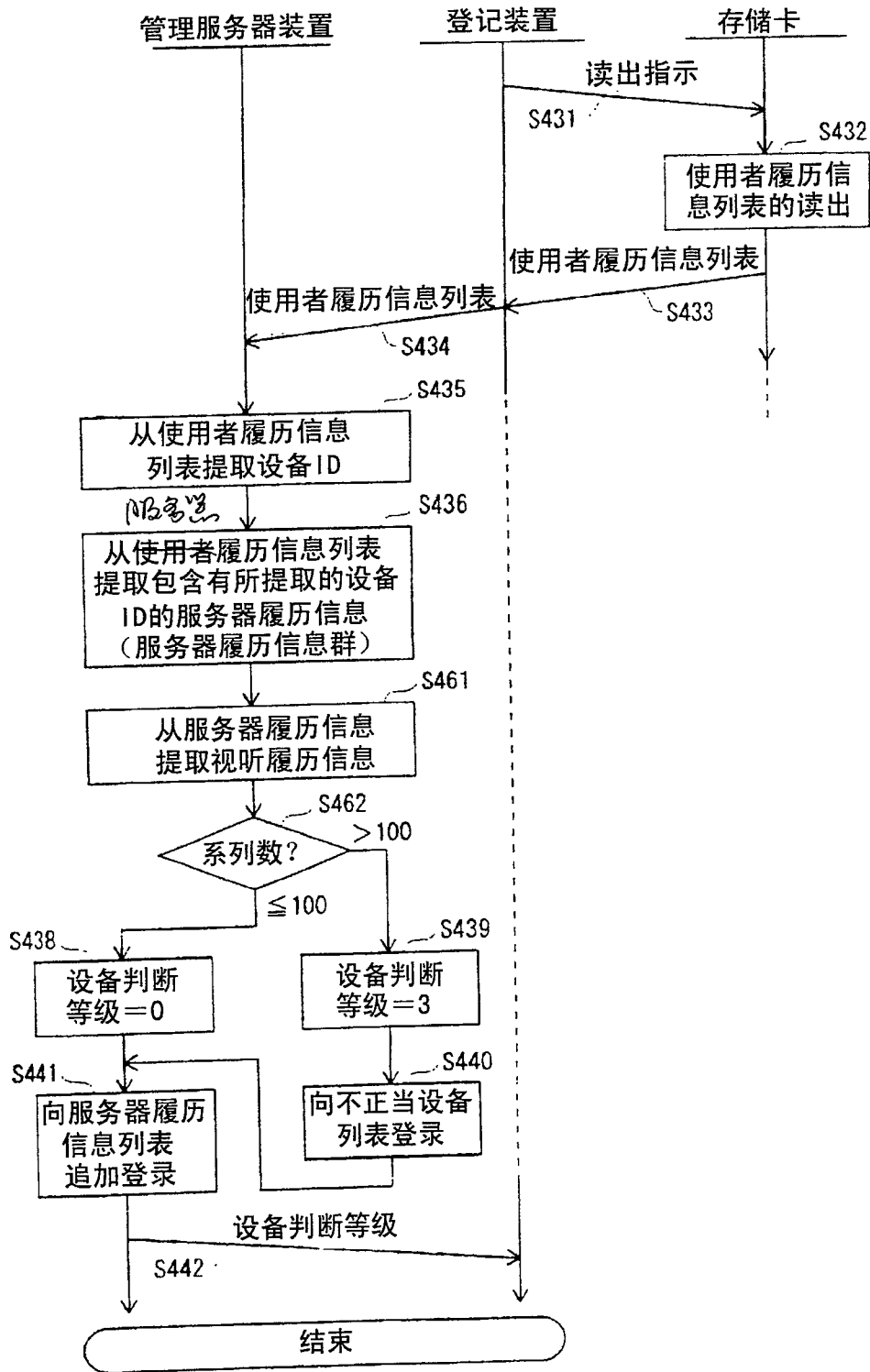


图33

服务器履历信息群

设备ID	再现顺序号	内容ID
ID-A	1	X001
ID-A	2	X002
ID-A	3	X003
ID-A	1	M001
ID-A	2	M002
ID-A	3	M003
ID-A	1	Y001
ID-A	3	Y002
ID-A	3	Y003

621

631

632

633

图34