[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
G06F 19/00
G06K 19/00

[12] 发明专利说明书

[21] ZL 专利号 98116127.8

[45] 授权公告日 2004 年 7 月 28 日

[11] 授权公告号 CN 1159669C

[22] 申请日 1998.7.17 [21] 申请号 98116127.8

[30] 优先权

[32] 1997.12.10 [33] JP [31] 340382/1997

[71] 专利权人 富士通株式会社

地址 日本神奈川

[72] 发明人 麻生泉 螺良修一

审查员 王京霞

[74] 专利代理机构 中国国际贸易促进委员会专利商标事务所

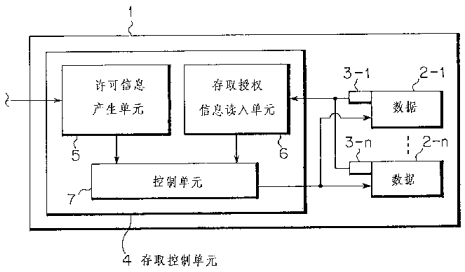
代理人 于 静

权利要求书 3 页 说明书 20 页 附图 40 页

[54] 发明名称 卡式记录媒体和其存取控制方法

[57] 摘要

本发明提供了一种卡式记录媒体，以简化存取授权的设置和更改工作，从而可靠执行安全系统的管理和操作。 包括用来存放数据的存储单元以及存取控制单元。 存取控制单元包括一个存取主体识别信息产生单元，它产生识别存取主体的存取主体识别信息、一个存取授权信息读入单元，它读入与存取主体要求存取的数据对应而设置的存取授权信息、以及一个控制单元，它从存取主体识别信息和存取授权信息获得一个存取授权，并根据所获得的存取授权控制存取主体对数据的存取。



ISSN1008-4274

1、一种卡式记录媒体（1），包括存放作为存取对象的数据的存储单元（2－1到2－n）以及控制一个存取主体对所述数据的存取的存取控制单元（4），该卡式记录媒体中的所述存取控制单元（4）包括：

一个存取主体识别信息产生单元（5），产生用来识别所述存取主体的存取主体识别信息（9），

一个存取授权信息读入单元（6），读取与所述存取主体要求存取的所述数据对应的数学函数定义的存取授权信息（3－1到3－n）来获得与所述存取主体要求存取的所述数据对应而设置的一个存取授权，以及

一个控制单元（7），通过使用存取主体识别信息（9）和存取授权信息（3－1到3－n）执行一个数学函数来获得与所述存取主体识别信息（9）对应的一个存取授权，并根据所获得的所述存取授权控制所述存取主体对所述数据的存取。

2、权利要求1所述的卡式记录媒体，其中所述存取主体识别信息（9）包括涉及至少两种存取条件的一条信息。

3、权利要求1所述的卡式记录媒体，其中所述存取主体识别信息（9）包括用来对照一个操作者的一条对照存取主体识别信息（9A）和用来鉴别一个应用的一条鉴别存取主体识别信息（9B）。

4、权利要求3所述的一种卡式记录媒体，其中所述对照存取主体识别信息（9A）对应于指示操作者身份的一条存取主体对照信息，而所述鉴别存取主体识别信息（9B）对应于识别应用的一条存取主体对照信息。

5、权利要求3所述的卡式记录媒体，其中对照存取主体识别信息（9A）和鉴别存取主体识别信息（9B）都是通过包括至少一类信息和具有分级结构的分级信息的一个矩阵来表示的。

6、权利要求5所述的卡式记录媒体，其中所述存取授权信息（3－1到3－n）包括对于所述矩阵的每个元件以对照存取主体识别信息

（9A）和鉴别存取主体识别信息（9B）为条件确定的存取授权元素以及使用所述存取授权元素的一个数学函数。

7、权利要求1所述的卡式记录媒体，其中所述存取主体识别信息产生单元（5）保持:

默认的对照存取主体识别信息，用于对照一个操作者;

默认的鉴别存取主体识别信息，用于鉴别一个应用;

用于参考的存取主体对照信息，用于指示操作者身份;

用于参考的存取主体识别信息，用于识别应用;

存取主体识别信息生成信息，用于生成用于对照与作为参考的存取主体对照信息相对应的操作者的一条对照存取主体识别信息，及生成用于鉴别与作为参考的存取主体鉴别信息相对应的应用的一条鉴别存取主体识别信息;

数学函数，用于将生成的对照存取主体识别信息反映为所述默认的对照存取主体识别信息，将生成的鉴别存取主体识别信息反映为所述默认的鉴别存取主体识别信息。

8、权利要求1所述的卡式记录媒体，其中卡式记录媒体包括多个逻辑通道（13），通过它们所述存取主体可以存取所述数据，而所述存取控制单元（4）对每个所述逻辑通道（13）相互独立地控制所述存取主体对所述数据的存取。

9、权利要求8所述的卡式记录媒体，其中存取控制单元（4）对所述逻辑通道（13）的每个通道产生所述存取主体识别信息（9）。

10、权利要求1所述的卡式记录媒体，其中卡式记录媒体包含一个审计记录（8），其内容为对所述存取控制单元（4）的操作进行的审计。

11、一种卡式记录媒体（1）的存取控制方法，用来控制存取主体对包含存放作为存取对象的数据的存储单元（2－1到2－n）的卡式记录媒体（1）中的所述数据的存取，它包括:

一个存取主体识别信息产生步骤，用来产生识别所述存取主体的存取主体识别信息（9），

一个存取授权信息读入步骤，读入与所述存取主体要求存取的所述数据对应的数学函数定义的存取授权信息（3－1到3－n），来获得与所述存取主体要求存取的所述数据对应而设置的一个存取授权，以及

一个控制步骤，通过使用存取主体识别信息（9）和存取授权信息（3－1到3－n)执行一个数学函数来获得与所述存取主体识别信息(9）对应的一个存取授权，并根据所获得的所述存取授权控制所述存取主体对所述数据的存取。

12、权利要求11所述的卡式记录媒体的存取控制方法，其中，当存取主体输入一条指示操作者的身份的存取主体对照信息和识别一个应用的存取主体鉴别信息时，存取主体识别信息产生步骤将把输入的存取主体对照信息和输入的存取主体鉴别信息与作为参考的一条存取主体对照信息和作为参考的一条存取主体鉴别信息进行对照，且如果两者都一致，存取主体识别信息产生步骤产生与作为参考的存取主体对照信息和作为参考的存取主体鉴别信息对应的对照操作者的对照存取主体识别信息和鉴别应用的鉴别存取主体识别信息，并将所产生的对照存取主体识别信息和所产生的鉴别存取主体识别信息反映为一条默认的用于对照操作者的对照存取主体识别信息，和一条默认的用于鉴别应用的鉴别存取主体识别信息。

13、权利要求11所述的卡式记录媒体的存取控制方法，其中：

所述存取主体识别信息（9）包括一条对照一个操作者的对照存取主体识别信息（9A）和鉴别一个应用的一条鉴别存取主体识别信息（9B），以及

所述控制步骤在对照存取主体识别信息（9A）和鉴别存取主体识别信息（9B）的条件下确定存取授权元素，并通过使用所述存取授权元素的一项数学操作获得与所述存取主体识别信息（9）对应的存取授权。

卡式记录媒体和其存取控制方法

技术领域

本发明涉及卡式记录媒体，例如所用IC卡、电子货币载体、信用卡、ID卡、自备卡等，还涉及这些卡式记录媒体的存取控制方法，以及上面记录有卡式记录媒体的存取控制程序的计算机可读记录媒体。

背景技术

近年来，随着IC卡的广泛应用，需要安全性的信息，如电子货币信息、信用卡信息、医疗图表信息等都已经被存放在IC卡上。因而，IC卡需要安全地存放这些信息。为了满足这种需要，迫切需要在通过符合国际标准（ISO 7816）的命令来加强执行存取控制时的安全性。

执行卡式记录媒体的存取控制的技术在日本专利申请公开号(以下将其简称为JP－A）60－160491（IC卡）、JP－A－60－205688（便携媒体）、JP－A－60－205689（便携媒体）、JP－A－60－205690（便携媒体）、JP－A－60－207939（通过电子装置的记录系统）等中公开过，它们被认为是加强卡式记录媒体安全性的有效方法。

下面将在JP－A－60－160491（IC卡）中公开的技术作为一个例子，参考图46（a）、46（b）和图47对其进行描述。

如图46（a）中所示，IC卡100包括文件101－1和101－2，用来存放作为存取对象的数据。文件101－1、101－2分别被赋予一个存取授权信息（安全管理信息）102－1、102－2。

另外，客户机103A被赋予一个口令密码号：“a”，客户机103B被赋予一个口令密码号：“a，c”，而客户机103C被赋予一个口令密码号：“a，b”。在此，赋予文件101－1、101－2的存取授权信息102－1，102－2都是“a，b”。因此，只有具有口令“a，b”的客户机可以读取文件101－1，101－2。

在这种假设下，我们考虑一种方法来向客户机103A新赋授权来读取文件101－1。但是，客户机103A没有赋予授权来存取文件101－2，

而客户机 103B 没有赋予授权来存取文件 101－1。另外，假定对客户机 103C 没有任何影响。

在此情况下，如图 46（b）中所示，还赋予了客户机 103A 一个口令“d”来将客户机 103A 的口令改变为“a，d”，而赋予文件 101－1 的存取授权信息 102－1 的设置向用符号 102－1’所表示的设置的改变将能够新赋予客户机 103A 一个读取文件 101－1 的授权。

另外，我们考虑一种方法来向具有口令“b，c”的客户机 103D 新赋予读取文件 101－1 的授权。

在此情况下，如图 47 中所示，还赋予客户机 103D 一个口令“d”来将客户机 103D 的口令改变为“b，c，d”，而将赋予文件 101－1 的存取授权信息 102－1’的设置改变为用符号 102－1’’所表示的设置将能够新赋予客户机 103D 一个读取文件 101－1 的授权。

有时，文件 101－2 和存取授权信息 102－2 并没有表示在图 46（b）和图 47 中。

但是，在前面的控制对卡式记录媒体的存取的方法中，设置和更改存取授权的方法以及使用和维护/管理安全系统的方法对用户来说不容易理解；设置和更改存取授权的工作以及使用和维护/管理安全系统的工作对安全系统的设计者来说是一件很麻烦的事，这是一个问题。

换句话说，当扩展或压缩客户机 103A 到 103D 的存取授权时，必须再检查赋予文件 101－1、101－2 的存取授权信息 102－1、102－2，而设置和更改存取授权的工作将会对整个系统产生影响。也就是说，在定义了上述的安全系统之后要改变存取授权将需要事先检查整个安全系统，这使得设置和更改存取授权的工作变得极端复杂。

在公开的其它授权中的技术具有同样的问题。

另外，当考虑到将电子货币信息、信用卡信息、自备信息等存放在一块卡式记录媒体上的多目的应用时，对安全系统的操作来说，就有必要在某个地方能够控制安全性，而在应用中要能够保持信息的独立性。

发明内容

本发明是考虑到前面的问题而设计的，本发明的一个目的是提供一种卡式记录媒体和卡式记录媒体的一种存取控制方法，其中可以可靠执行安全系统的管理和操作，而设置和更改存取授权的工作甚至在多目的

应用中也可以被简化，以及一种计算机可读记录媒体，它上面记录了卡式记录媒体的存取控制程序，此程序控制存取主体对数据的存取。

为了达到前面的目的，本发明所涉及的一种卡式记录媒体，包括存放作为存取对象的数据的存储单元以及控制一个存取主体对所述数据的存取的存取控制单元，该卡式记录媒体中的所述存取控制单元包括：一个存取主体识别信息产生单元，产生用来识别所述存取主体的存取主体识别信息，一个存取授权信息读入单元，读取与所述存取主体要求存取的所述数据对应的数学函数定义的存取授权信息来获得与所述存取主体要求存取的所述数据对应而设置的一个存取授权，以及一个控制单元，通过使用存取主体识别信息和存取授权信息执行一个数学函数来获得与所述存取主体识别信息对应的一个存取授权，并根据所获得的所述存取授权控制所述存取主体对所述数据的存取。

另外，在涉及本发明的卡式记录媒体中，存取主体识别信息包括涉及至少两个以上的存取条件的信息。

此外，在涉及本发明的卡式记录媒体中，存取主体识别信息包括对照存取主体识别信息，用来将一个操作者和鉴别一个应用的鉴别存取主体识别信息进行对照。

另外，在涉及本发明的卡式记录媒体中，对照存取主体识别信息对应于指示操作者身份的一个存取主体对照信息，而鉴别存取主体识别信息对应于识别应用的一个存取主体鉴别信息。

另外，在涉及本发明的卡式记录媒体中，对照存取主体识别信息和鉴别存取主体识别信息是通过至少一类信息和具有分级结构的级别信息的一个矩阵表达的。

另外，在涉及本发明的卡式记录媒体中，存取授权信息包括用于每个矩阵元素和使用存取授权元素的一个数学函数的对照存取主体识别信息和鉴别存取主体识别信息的条件所确定的存取授权元素。

另外，在涉及本发明的卡式记录媒体中，存取主体识别信息产生单元保持：（1）默认的对照存取主体识别信息，（2）默认的鉴别存取主体识别信息，（3）用于参考的存取主体对照信息，（4）用于参考的存取主体识别信息，（5）存取主体识别信息生成信息，及（6）一个数学函数。其中，（1）默认的对照存取主体识别信息是用于对照一个操作者的信息，（2）默认的鉴别存取主体识别信息是用于鉴别一个

应用的信息，（3）用于参考的存取主体对照信息是用于指示操作者身份的信息，（4）用于参考的存取主体识别信息是用于识别应用的信息，（5）存取主体识别信息生成信息用于生成用于对照与作为参考的存取主体对照信息相对应的操作者的一条对照存取主体识别信息，及用于生成用于鉴别与作为参考的存取主体鉴别信息相对应的应用的一条鉴别存取主体识别信息，（6）数学函数用于将生成的对照存取主体识别信息反映为默认的对照存取主体识别信息，将生成的鉴别存取主体识别信息反映为默认的鉴别存取主体识别信息。

另外，涉及本发明的卡式记录媒体包括多个逻辑通道，通过它们对数据进行存取，而存取控制单元对每个逻辑通道相互独立地控制存取主体对数据的存取。

另外，在涉及本发明的卡式记录媒体中，存取控制单元产生每个逻辑通道的存取主体识别信息。

另外，涉及本发明的卡式记录媒体还包括一个审计记录，这是一条对存取控制单元的操作进行审计的信息。

另一方面，涉及本发明的卡式记录媒体的一种存取控制方法是通过存取主体对涉及的存取进行控制，在卡式记录媒体中包含有存放作为存取对象的数据的存储单元。一种卡式记录媒体的存取控制方法，用来控制存取主体对包含存放作为存取对象的数据的存储单元的卡式记录媒体中的所述数据的存取，它包括：一个存取主体识别信息产生步骤，用来产生识别所述存取主体的存取主体识别信息，一个存取授权信息读入步骤，读入与所述存取主体要求存取的所述数据对应的数学函数定义的存取授权信息，来获得与所述存取主体要求存取的所述数据对应而设置的一个存取授权，以及一个控制步骤，通过使用存取主体识别信息和存取授权信息执行一个数学函数来获得与所述存取主体识别信息对应的一个存取授权，并根据所获得的所述存取授权控制所述存取主体对所述数据的存取。

在涉及本发明的卡式记录媒体的存取控制方法中，当存取主体输入存取主体对照信息来指示操作者的身份和识别应用的存取主体鉴别信息时，存取主体识别信息产生步骤将所输入的存取主体对照信息和所输入的具有作为参考的存取主体对照信息和作为参考的存取主体鉴别信息的存取主体鉴别信息进行对照。如果两者一致，存取主体识别信

息产生步骤产生一个对照存取主体识别信息，用来对照与作为参考的存取主体对照信息对应的操作者和一个鉴别存取主体识别信息，用来鉴别和作为参考的存取主体鉴别信息对应的应用，并把所产生的对照存取主体识别信息和所产生的鉴别存取主体识别信息反映为用来对照操作者的默认的对照存取主体识别信息和用来鉴别应用的默认鉴别存取主体识别信息上。

另外，在涉及本发明的卡式记录媒体的存取控制方法中，存取主体识别信息被设计为包含用来对照操作者的对照存取主体识别信息和用来鉴别应用的鉴别存取主体识别信息；而控制步骤在对照存取主体识别信息和鉴别存取主体识别信息的条件下确定存取授权元素，并通过使用存取授权元素的数学操作获得与存取主体识别信息对应的存取授权。

另外，涉及本发明的计算机可读记录媒体具有所记录的卡式记录媒体的一个存取控制程序，而存取控制程序通过计算机和包含存放作为存取对象的数据的存储单元来控制对数据的存取。在计算机可读记录媒体中，卡式记录媒体的存取控制程序通过存取主体识别信息产生单元产生识别存取主体的存取主体识别信息、通过存取授权信息读入单元来读取用来获得与存取主体需要存取的数据对应而设置的存取授权的存取授权信息、以及通过一个控制单元获得与来自存取主体识别信息和存取授权信息的存取主体识别信息对应的存取授权使计算机发生作用，并根据所获得的存取授权控制存取主体对数据的存取。

根据在此所述的本发明，即便在卡式记录媒体的多目的应用的情况下，也可以简化设置和更改工作，而安全系统的管理和操作也可以可靠地执行，这是其优点。

从后面的详细描述中可以明显地看到本发明的适应范围。但是，应该了解，在表示本发明的最佳实施例时所用的详细描述和专门的例子仅仅是为了举例而给出的，因为从这些详细描述中熟练的技术人员可以很明白地了解在本发明的精神和范围之内的各种变化和修改。

附图说明

从下面所给的详细描述和仅仅通过举例而非作为本发明的限制所给出的附图中可以更加全面地了解本发明，其中：

图 1 是一个举例表示涉及本发明的一个实施例的卡式记录媒体的

结构的功能框图；

图 2 是一个举例表示涉及本发明的一个实施例的卡式记录媒体的结构的功能框图；

图 3 是一个举例表示涉及本发明的一个实施例的卡式记录媒体的结构的功能框图；

图 4 是解释涉及本发明的一个实施例的卡式记录媒体的操作的一个图；

图 5 是解释许可信息的一个图；

图 6 是举例表示一个状态的图，在此状态下，在多个客户机应用和一个存取控制单元之间提供了多个逻辑通道；

图 7 是举例表示审计记录的一个例子的图；

图 8（a）、图 8（b）的每个图都举例表示了其中的安全系统将 IC 卡作为卡式记录媒体而构造的一个例子；

图 9（a）到图 9（c）的每个图都举例表示了一个状态，在此状态下对对照许可信息进行了修改；

图 10（a）到图 10（c）的每个图都解释了一条许可信息；

图 11 是解释存取授权信息的一个图；

图 12 是举例表示默认许可信息的一个图；

图 13（a）、图 13（b）的每个图都举例表示了一条对照许可信息；

图 14（a）、图 14（b）的每个图都举例表示了一条鉴别许可信息；

图 15 是举例表示赋予人事信息的存取授权信息的一个图；

图 16 是举例表示赋予帐目信息的存取授权信息的一个图；

图 17 是举例表示涉及存取授权的条件的定义的一个图；

图 18 是举例表示涉及存取授权的条件的定义的一个图；

图 19 是举例表示在 IC 卡中的永久性存储器的区域分配的一个图；

图 20 是举例表示图 19 中所示的数据区的详细文件结构的一个图；

图 21（a）、图 21（b）的每个图都是举例表示了 IC 卡中的永久性存储器的文件结构的图；

图 22（a）到图 22（d）的每个图都举例表示了图 21 中所示的详细的文件结构；

图 23（a）、图 23（b）的每个图都举例表示了图 21 中所述的详细的文件结构；

图 24 到图 30 的每个图都解释了涉及本发明的一个实施例的卡式记录媒体的操作;

图 31 是解释默认许可信息的产生的一个图;

图 32 到图 34 的每个图都解释了许可信息的更改;

图 35、图 36 的每个图都解释了存取授权的计算;

图 37 到图 45 的每个图都是解释涉及本发明的记录媒体的一个实施例的操作的流程图;

图 46（a）、图 46（b）的每个图都解释了在卡式记录媒体中的常规的存取控制方法; 以及

图 47 是解释在卡式记录媒体中的常规存取控制方法的一个图;

具体实施方式

下面将参考附图对本发明的最佳实施例进行详细描述。

（a）一个实施例的描述

图 1 到图 3 是举例表示涉及本发明的一个实施例的卡式记录媒体的结构的功能框图。例如，图 1 到图 3 中所示的卡式记录媒体 1 可以是作为电子货币载体的 IC 卡、信用卡、ID 卡、自备卡等。卡式记录媒体 1 包含有存放作为存取对象的数据的文件（存储单元）2－i（i＝1～n，n: 可选择的自然数），以及通过存取主体[此后的卡式记录媒体 1 的主人、在存取过程中由此主人所用的一个终端、以及执行实际的存取的一个应用（客户机应用）作为一个通用的名字都指的是存取主体]控制数据存取的一个存取控制单元 4。

在此，向文件 2－i 中的数据提供了一个存取授权信息 3－i（i＝1－n，n: 可选择的自然数）用来获得指示一个存取主体是否可以存取数据的存取授权。

另外，如图 1 中所示，向存取控制单元 4 提供了一个许可信息产生单元（存取主体识别信息产生单元）5 来产生许可信息（存取主体识别信息，由图 2 中的符号 9 指示），用来识别一个存取主体，一个存取授权信息读入单元 6，用来读入与存取主体需要存取的数据对应而设置的存取授权信息 3－i，以及一个控制单元，用来获得与来自前面的许可信息 9 和存取授权信息 3－i 的存取主体识别信息对应的存取授权，并根据所获得的存取授权控制存取主体对数据的存取。

另外，如图2、图3所示，向卡式记录媒体1提供了一个客户机应用12来实际执行存取。并在这一客户机应用12和存取控制单元4之间提供了一个逻辑通道。

另外，如图2中所示，卡式记录媒体1被设计为包含一个审计记录8用来作为控制单元4中的操作的审计内容。另外，图7举例表示了审计记录的一个例子。审计记录存放在审计记录IEF（内部基本文件；见后面所用的图19）中。在此，IEF被按前面的记录结构进行配置，审计记录按命令接收/处理的顺序被连续存放。

另外，符号11指示了利用卡式记录媒体1中的数据执行各种处理的一个终端，而符号10指示了用来从终端11传送读/写指令的一个卡接口装置，其中插入并连接了卡式记录媒体1。

另外，客户机应用12可以安装到卡接口装置10中；在图2中，每种卡式记录媒体1、卡接口装置10以及终端11都包含客户机应用12。

另外，如图3中所示，卡式记录媒体1被提供了一个通信控制单元14作为与卡接口装置10之间的一个接口单元。后面将对图3进行详细描述。

现在将详细描述前面的许可信息9和存取授权信息3－i。

许可信息9是识别一个存取主体的一条信息。但是，在涉及本实施例的卡式记录媒体1中，许可信息9包括涉及至少两个以上的存取条件的一条信息。

具体的，如图5中所示，许可信息9包括一条对照许可信息9A和一条鉴别许可信息9B。

在此，对照许可信息9A是为了鉴别操作者是否是卡式记录媒体1的主人而对操作者进行对照的一条信息，它与指示操作者的身份的一条存取主体对照信息[口令]相对应。

另外，鉴别许可信息9B是为了鉴别所执行的存取是否是通过可存取的终端11进行的而对客户机应用12进行鉴别的一条信息，它与用来识别客户机应用12的一条存取主体鉴别信息（鉴别从终端11传送的关键字信息）相对应。

另外，如图10（a）、图10（b）所示，对照许可信息9A和鉴别

许可信息9B是通过一个矩阵来表示的，此矩阵包括至少一类信息和具有分级结构的一个级别信息。另外，在图10（a）、图10（b）中，在一个公司中的部门的名称（人员、帐目、一般事件、开发、购买）被用作信息种类的一个例子，而在一个公司中的管理职位的名称（部门管理员、部门主管管理员、分部管理员、一般职务级别）被用作具有分级结构的级别信息的一个例子。另外，图10（c）实际表示了一个状态，在此状态下对对照许可信息9A和鉴别许可信息9B进行了合并。

另外，在此实施例中，为了产生对照许可信息9A和鉴别许可信息9B，许可信息产生单元5产生了一条默认的对照许可信息、一条默认的鉴别许可信息、作为参考的一个口令（作为参考的存取主体对照信息）、作为参考的一条鉴别关键字信息（作为参考的存取主体鉴别信息）、以及与所参考的口令对应的一条对照许可信息。另外，许可信息产生单元5包含了一个数学函数，用来将产生与作为参考的鉴别关键字信息对应的一条鉴别许可信息的存取主体识别信息产生信息反映为默认的对照许可信息，并将所产生的鉴别许可信息反映为默认的鉴别许可信息。另外，对照许可信息9A的产生和使用这些信息的鉴别许可信息9B将在以后进行描述。

另外，存取授权信息3－i是其中的一个存取主体具有一个存取授权的信息。在涉及本实施例的卡式记录媒体1中，存取授权信息3－i用在对照许可信息9A和鉴别许可信息9B、以及采用这些存取授权元素的一个数学函数（见图11中的公式（1））的条件下对每一个矩阵元素确定的存取授权元素[见图11中的符号Q]进行配置。另外，存取授权信息3－i由安全系统的设计者适当进行设置。

另外，在涉及本实施例的卡式记录媒体1中，实际上在卡式记录媒体1中的ROM（没有画出）上以及在磁盘驱动器的记录媒体（没有画出）等上面、以及在图2中所示的终端11的计算机中等记录的一个程序（在此和下面指的是卡式记录媒体的存取控制程序）被读出到卡式记录媒体1中和图2中所示的终端11的计算机等中的存储器（RAM；没有画出）上，且此程序由一个处理电路（卡式记录媒体1中的MPU或图2中所示的终端11的计算机等中）启动并执行；因此，在处理电路的操作中实现了与前面的存取控制单元4（即与许可信息产生单元5、存取授权信息读入单元6、

以及控制单元7对应的功能）对应的功能。

在此，卡式记录媒体的存取控制程序通过产生许可信息9（对照许可信息9A、鉴别许可信息9B）的许可信息产生单元用来识别一个存取主体，存取授权信息读入单元6读入与存取主体需要存取的数据对应而设置的存取授权信息3－i、以及根据与来自前面的许可信息9和存取授权信息3－i的许可信息9对应而获得的存取授权的存取主体来控制对数据的存取的控制单元7使卡式记录媒体1发生作用。

在此，将通过一个公司中的人事和帐目部门管理员和帐目分部管理员存取存放在卡式记录媒体1中的人事信息这种情况来描述涉及本实施例的卡式记录媒体1的存取控制。

在图8（a）、图8（b）中举例表示了将IC卡用作卡式记录媒体1的一个安全系统的结构。

在此，我们假定人事和帐目部门管理员（用符号A表示）拥有一个证明其人事和帐目部门管理员身份的口令，而帐目分部管理员（用符号B表示）拥有一个证明其帐目分部管理员身份的口令。

另外，符号11A表示能够执行IC卡1A中的涉及人事的事务的一个终端，而符号11B表示能够执行IC卡1B中涉及帐目的事务的一个终端。另外，符号10A、10B表示前面的卡接口装置。

另外，IC卡1A、1B具有前面图3中所示的结构。在图3中，符号14表示利用卡接口单元执行指令的传送/通知处理的一个通信控制单元，符号12表示执行人事处理或帐目处理的一个客户机应用，符号4表示前面的存取控制单元，符号2－1和2－2分别表示存放人事信息和帐目信息的文件，符号3－1和3－2分别表示赋予文件2－1中的人事信息和文件2－2中的帐目信息的存取授权信息。

另外，当通过图8（a）、图8（b）中所示的终端11A和11B执行人事处理或帐目处理时，这些从IC卡1A、1B中的人事信息或帐目信息读取或写入到这些个人信息等存取的主体，即人事和帐目部门管理员A、帐目分部管理员B、终端11A、终端11B、IC卡1A、1B中实际执行存取的客户机应用12、或在终端11A、11B中没有画出的一个客户机应用一般都被称为一个存取主体。

IC卡1A、1B拥有这样一个结构，涉及一个存取主体的信息在存取人事信息或帐目信息时需要通过存取控制单元4。也就是说，在本实施例中的IC卡1A、1B具有图4中所示的结构.

为了表示存取主体本身具有存取IC卡1A、1B中的人事信息或帐目信息的适当授权，存取主体被设计为从图12中所示的存取控制单元4中获得一条默认的许可信息（存取主体的默认许可信息）。另外，提供了两种默认的许可信息，即鉴别默认许可信息和对照默认许可信息，每一种信息都在初始化过程中作为许可信息的初始值被装入。

在本实施例中，符合国际标准（ISO 7816－4）的主要的对照（检验）命令是被用来鉴别存取的人就是被承认进行存取的人的。另外，符合国际标准（ISO 7816－4）的“外部鉴别”命令是被用来鉴别终端11A、11B就是被承认进行存取的终端的。

另外，在主要的对照命令中的口令和在“外部鉴别”命令中的密码关键字信息（鉴别关键字信息）分别通过对照许可信息9A和鉴别许可信息9B被连接在一起。

另外，通过实施例中的对照所获得的对照许可信息被举例表示在图13（a）、图13（b）中、而通过实施例中的鉴别所获得的鉴别许可信息被举例表示在图14（a）、图14（b）中。另外，图13（a）中所示的对照许可信息9Aa和图14（a）中所示的鉴别信息9By与人事和帐目部门管理员A对应，而图13（b）中所示的对照许可信息9Ab和图14（b）中所示的鉴别信息9Bz与人事和帐目分部管理员B对应。

另外，如上所述，产生与许可信息9A、9B对应的存取授权的存取授权信息3－1、3－2分别是与在IC卡1A、1B中的人事信息和帐目信息相对应而定义的。

在此，图15举例表示了赋予人事信息的一部分存取授权信息3－1，而图16举例表示了赋予帐目信息的一部分存取授权信息3－2。

另外，为了通过数学操作获得存取的存取授权，存取授权审定操作者Fo1、Fo2[见图15、图16和下面的公式（2）、（3）]以及审定存取授权的条件（见存取授权元素fo11－fo29；图17、图18）是与存取授权信息3－1、3－2相对应而进行定义的。另外，图17举例表示了赋予人事

信息的一部分存取授权信息3－1、而图18举例表示了赋予帐目信息的一部分存取授权信息3－2。

Fo1 = fo11 + fo14 + fo17 …（2）

Fo2 = fo22 + fo25 + fo28 …（3）

例如，在赋予图17中所示的人事信息的存取授权信息3－1的情况下，存取授权元素fo11与具有“部门管理员/人事（即人事部门管理员）”的许可信息的存取主体相对应对存取授权进行了定义。

另外，在存取授权信息3－1、3－2中，所有的存取授权（R：读授权，W：写授权，X：删除授权）都被设置为允许面对已经获得对照许可信息9A和鉴别许可信息9B的存取主体。而且，只获得对照许可信息9A的存取授权被设置为只允许读，而其它的则被设置为不允许存取人事信息2－1。

另外，通过对照和鉴别所获得的存取主体的许可信息9A、9B被包含在存取控制单元4中，直到存取主体结束存取为止。

另外，在IC卡1（1A、1B）中的数据具有如图19所示的结构。

图19举例表示了IC卡1中的永久性存储器的区域分割，而前面的鉴别默认许可信息和对照默认许可信息被存放在系统区域中。

另外，图20举例表示了图19所示的数据区的一个详细的文件结构。另外，在图19、图20中，MF（主文件）是DF（专用文件）的基础。而且，EF（基本文件）包括IEF（内部基本文件）和WEF（工作基本文件）。IEF是用于存放IC卡1中除客户机应用之外的鉴别关键字、对照关键字和程序用来执行管理和控制目的数据的区域。WEF是存放IC卡1中不是程序、但由外部装置（例如，终端11、11A、11B等）使用（另外，数据的内容由外部装置随意定义）的数据的区域。

另外，涉及本实施例的卡式记录媒体1的存取控制的描述预先假定了图21（a）、图21（b）、图22（a）~图22（d）、图23（a）和图23（b）中所示的文件结构。这些附图仅仅举例表示了描述所必需的数据。

根据前面的结构，在涉及本发明的一个实施例的卡式记录媒体1中，当一个存取主体请求存取卡式记录媒体1中的一个数据时，存取控制单元4

将执行对存取请求的存取控制。

此时，在存取控制单元4中，首先，许可信息产生单元5产生许可信息9（对照许可信息9A，鉴别许可信息9B），用来根据已经从存取主体（许可信息产生步骤；图37中的步骤S1）发送的一个口令和一条密码关键字信息（鉴别关键字信息）识别存取主体。

为了加入详细信息，当存取主体输入表示操作者的身份的口令和识别应用的密码关键字信息时，许可信息产生单元5将输入的口令和密码关键字信息与用于参考的口令和用于参考的密码关键字信息进行对照。如果它们是一致的，那么许可信息产生单元5将利用前面的许可信息产生信息产生与所参考的口令和所参考的密码关键字信息对应的对照许可信息和鉴别许可信息；且许可信息产生单元5利用前面的数学函数将所产生的对照许可信息和鉴别许可信息反映为默认的对照许可信息和默认的鉴别许可信息上（即，对许可信息进行修改），因而产生对照许可信息9A和鉴别许可信息9B。

另外，将参考图31对默认的许可信息的产生进行描述。如图31中所示，当卡式记录媒体（IC卡）1加电时，卡式记录媒体1中的MPU被复位为开始初始化。且在初始化过程中，存取控制单元4从前面的系统区中装入默认的鉴别许可信息和默认的对照许可信息，从而产生默认的许可信息。

另外，将参考图32到图34对许可信息的修改进行描述。

首先对鉴别许可信息的修改进行描述。如图32中所示，当鉴别关键字（这一鉴别关键字被存放在IEF区“1”中）被装入到MF中时，就获得了一条默认的鉴别许可信息。且如果鉴别关键字正确，将根据前面所产生的鉴别许可信息对鉴别许可信息进行修改。另外，如图33中所示，当鉴别关键字（这一鉴别关键字被存放在IEF区“3”中）被装入到DF“1”中时，就获得了已经修改过的一条鉴别许可信息。且如果鉴别关键字正确，将根据前面所产生的鉴别许可信息对鉴别许可信息进行进一步的修改。

接下来，将对对照许可信息的修改进行描述。当对照密码号（对照关键字；这一对照关键字被存放在IEF区“2”中）被装入到MF中时，就获得了一条默认的对照许可信息。且如果对照关键字正确，将根据前面所

产生的对照许可信息（见图34）对对照许可信息进行修改。图9（a）到图9（c）还顺便举例表示了被修改的对照许可信息的状态。

接下来，在存取控制单元4中，存取授权信息读入单元6读入与存取主体请求存取（存取授权信息读入步骤；图37中的步骤S2）的数据对应而设置的存取授权信息3－i。

另外，控制单元7获得与来自前面的许可信息9对应的一个存取授权和存取授权信息3－i，并根据所获得的存取授权（控制步骤；图37中步骤S3）控制存取主体对数据的存取。

为进入详细信息，控制单元7在对照许可信息9A和鉴别许可信息9B的条件下确定存取授权元素（例如，图11、图18中的fo11到fo29），并通过采用了存取授权元素的数学操作获得与许可信息9对应的存取授权。

另外，将参考图35、图36对存取授权的计算进行描述。如图35中所示，在由许可信息产生单元5所产生的对照许可信息9A和鉴别许可信息9B的基础上，在WEF“1”区中执行记录读取并将存取授权元素读出。随后，通过使用存取授权元素的数学操作获得与许可信息9对应的存取授权（见图36）。

另外，图38到图45举例表示了实际的卡式记录媒体1的操作。图38举例表示了卡式记录媒体1的操作的总流程。而图39举例表示了图38中所示的步骤A1的细节，而图40举例表示了图38中所示的步骤A4的细节。图41到图44举例表示了图40中所示的步骤B4到B7的细节，而图45举例表示了图43中所示的步骤B19的细节和图44中所示的步骤B24的细节。

在卡式记录媒体1的存取控制单元4中，首先，许可信息产生单元5从前面的系统区（见图19、图21（a））中装入鉴别默认许可信息和对照默认许可信息，并产生默认的许可信息（图38中步骤A1，图39中步骤B1、B2）。

接下来，存取控制单元4判断存取主体是否发送了命令（存取控制单元4是否从存取主体中接收到了命令）（图38中步骤A2）。如果存取控制单元4没有接收到命令，它将在步骤A2重复进行操作，直到接收到一条命令为止。且如果它接收到一条命令，存取控制单元4将按它接收命令（图

38 中步骤 A3 ）的顺序记录审计记录 8（见图 2 ）。

另外，存取控制单元 4 执行与接收到的命令有关的处理（图 38 中步骤 A4 ）。即，首先存取控制单元 4 判断所接收到的命令的种类（图 40 中步骤 B3 ），并执行与命令种类对应的处理（图 40 中的步骤 B4 到 B7 ）。即，如果接收到的命令是主要的对照命令，控制单元 4 将执行与主要的对照命令所对应的处理（图 40 中步骤 B4 ）；如果接收到的命令是外部鉴别命令，它将执行与外部鉴别命令对应的处理（图 40 中步骤 B5 ）；如果接收到的命令是读记录命令，它将执行与读记录命令对应的处理（图 40 中步骤 B6 ）；如果接收到的命令是写记录命令，它将执行与写记录命令对应的处理（图 40 中步骤 B7 ）。

另外，在控制单元 4 执行完与接收到的命令对应的处理之后，它响应处理的结果（图 38 中步骤 A5 ），并按它处理命令的顺序记录审计记录 8（图 38 中步骤 A6 ）。

在此，将参考图 41 对与图 40 的步骤 B4 中的主要对照命令对应的处理进行描述。

如果接收到的命令是主要的对照命令，在存取控制单元 4 中的许可信息产生单元 5 将装入对前述数据区的当前 DF 中的口令（密码号）存放在 IEF 中的口令[见图 19、图 20、图 21（ b ）]（图 41 中步骤 B8 ）。

另外，许可信息产生单元 5 判断与主要的对照命令一起传送的口令是否与装入的口令相同（图 41 中步骤 B9 ）。如果传送的口令被判断为与装入的口令相同，那么许可信息产生单元 5 将产生对照许可信息 9A （图 41 中步骤 B10 ），并产生被称为“正常结束”的一条响应信息（图 41 中步骤 B11 ）。另外，如果传送的口令被判断为与装入的口令不同，那么许可信息产生单元 5 将产生一条称为“口令对照错误”的响应信息（图 41 中步骤 B12 ）。

另外，将参考图 42 对与图 40 中步骤 B5 中的外部鉴别命令对应的处理进行描述。

如果接收到的命令是外部鉴别命令，在存取控制单元 4 中的许可信息产生单元 5 将装入对前述数据区的当前 DF 中的鉴别关键字信息（关键字）所存放在 IEF 中的鉴别关键字信息[见图 19、图 20、图 21（ b ）]（图 42

中步骤 B13），并利用装入关键字对与外部鉴别命令一起传送的鉴别关键字信息（输入数据）进行解码（图 42 中步骤 B14）。

另外，许可信息产生单元 5 判断装入的鉴别关键字信息（普通文本）是否与解码的鉴别关键字信息（解码文本）相同（图 42 中步骤 B15）。如果普通文本被判断为与解码文本相同，那么许可信息产生单元 5 将产生鉴别许可信息 9B（图 42 中步骤 B16），并产生称为“正常结束”的一条响应信息（图 42 中步骤 B17）。另外，如果普通文本被判断为与解码文本不同，那么许可信息产生单元 5 将产生一条称为“关键字鉴别错误”的响应信息（图 42 中步骤 B18）。

另外，将参考图 43 对与图 40 中的步骤 B6 中的读记录命令对应的处理进行描述。

如果接收到的命令是读记录命令，存取控制单元 4 将执行与存取请求（读请求）有关的存取控制。

即，在存取控制单元 4 中的控制单元 7 根据对照许可信息 9A、所产生的鉴别许可信息 9B、和存取主体请求存取的与存取授权信息读入单元 6 读入的数据对应的存取授权信息 3 - i，执行存取授权的数学操作（图 43 中步骤 B19）。

另外，存取控制单元 4 判断所获得的存取授权是否允许读取授权（图 43 中步骤 B20）。如果允许读取授权，那么存取控制单元 4 将读出存取主体请求存取的数据（相关的记录）（图 43 中步骤 B21），并产生一条称为“正常结束”的响应信息（图 43 中步骤 B22）。另外，如果不允许读取授权，那么存取控制单元 4 将产生一条称为“安全故障”的响应信息（图 43 中步骤 B23）。

另外，将参考图 44 对与图 40 中步骤 B7 中的写记录命令对应的处理进行描述。

如果接收到的命令是写记录命令，存取控制单元 4 将执行与存取请求（写请求）有关的存取控制。

即，在存取控制单元 4 中的控制单元 7 根据对照许可信息 9A、所产生的鉴别许可信息 9B、和存取主体请求存取的与存取授权信息读入单元 6 读入的数据对应的存取授权信息 3 - i，执行存取授权的数学操作（图 44

中步骤B24）。

另外，存取控制单元 4 判断所获得的存取授权是否允许写授权（图44中步骤B25）。如果允许写授权，那么存取控制单元4将写入存取主体请求存取的数据（相关的记录）（图44中步骤B26），并产生一条称为“正常结束”的响应信息（图44中步骤B27）。另外，如果不允许写授权，那么存取控制单元4将产生一条称为“安全故障”的响应信息（图44中步骤B28）。

最后，将参考图45对图44中步骤B24和图43中步骤B19中的存取授权的数学处理进行描述。

存取授权信息读入单元6读入与在存取控制单元4的控制单元7中的存取主体请求存取的数据对应的存取授权信息（对象标签）3 - i（图45中步骤B29），而控制单元7判断是否存在一个数学对象的标签信息（图45中步骤B30）。如果存在一个数学对象的标签信息，控制单元7将获得存取主体（对象）的存取授权信息（图45中步骤B31），并重复前述步骤B30的操作。且如果不存在一个数学对象的标签信息，控制单元7将如上所述根据对照许可信息9A、鉴别许可信息9B、以及存取授权信息3 - i执行存取授权的数学操作（图45中步骤B32）。控制单元7判断所获得的存取授权的存取种类（图45中步骤B33），并控制允许或禁止与存取请求命令（读记录命令或写记录命令）对应的存取。

另外，前述的许可信息产生步骤（图37中步骤S1）对应于图38中所示步骤A1（即图39中所示步骤B1、B2）、以及图40中所示步骤B4、B5（即图41中步骤B8到B12，以及图42中步骤B13到B18）。另外，前面的存取授权信息读入步骤（图37中步骤S2）和控制步骤（图37中步骤S3）对应于图40中所示步骤B6、B7（即图43中步骤B19到B23，图44中步骤B24到B28，图45中步骤B29到B33）。

另外，将引用一个公司中的人事和帐目部门管理员存取存放在卡式记录媒体1中的文件2 - 1和2 - 2中的人事信息和帐目信息（见图3）的例子，对涉及本实施例的卡式记录媒体1的存取控制进行描述。

首先，将描述一下人事和帐目部门管理员对人事信息的存取，将其分成如下的步骤（1）到（3）。

（1）主要对照

如图24中所示，当人事和帐目部门管理员A利用图24中没有画出的一个终端的键盘输入一个口令“a”时，[例如，图8（a）中所示终端11A]，此终端将利用主要的对照命令将口令“a”传送到IC卡1A。

一旦主要的对照命令被传送，IC卡1A中的存取控制单元（图24中没有画出）将对照口令“a”；且如果对照正确，存取控制单元将产生对照许可信息9Aa。另外，图25举例表示了确认人事和帐目部门管理员的许可信息已经产生的一个状态。

（2）终端的鉴别

接下来，为了确认在存取中所用的终端是被授权为存取的正确终端，利用文本鉴别命令执行了终端的鉴别（外部鉴别）。在图26中，终端11A将一个鉴别数据和密码关键字的一个签字（密码关键字信息）“y”传送到IC卡1A。

一旦外部鉴别命令被传送，IC卡1A中的存取控制单元（图26中没有画出）将判断所签的数据是否被正确解码，并随后执行终端11A的鉴别（通过密码关键字“y”的鉴别）。另外，如果鉴别正确，控制单元将产生鉴别许可信息9By。另外，图27举例表示了确认人事信息终端的许可信息已经产生的一个状态。

（3）人事信息的存取

拥有对照许可信息9Aa和鉴别许可信息9By的存取主体（人事和帐目部门管理员A）试图存取人事信息。在此和下面将解释当信息被存取时，由存取控制单元所执行的存取授权的数学操作。

将利用图28对要实际表达的在对照和鉴别中所获得的许可信息9Aa、9By的合成进行解释。

关于前面的存取主体所拥有的许可信息9Aa、9By，作为存取对象赋予人事信息的存取授权信息3－1（见图3）具有如图29中所示的对存取授权元素fo11、fo14、fo17的逻辑求和操作符。即，存取授权是通过以下的公式（4）所获得的。

存取授权＝（fo11）或（fo14）或（fo17）

…（4）

另外，根据存取授权的这种数学操作，存取控制单元允许存取主体的“RWX”存取（见图29）。

因此，人事和帐目部门管理员能够存取存放在卡式记录媒体1中的人事信息。当存取主体读入人事信息时，例如，图4所示的读过程被正确执行时，存取主体就能够读入人事信息。

接下来，将描述人事和帐目部门管理员对帐目信息的存取。

当存取主体获得如图28所示的许可信息9Aa、9By时，在前面（1）中，并试图存取帐目信息时，图30中所示的存取授权的数学操作将被执行。

涉及图28所示的存取主体（人事和帐目部门管理员）所具有的许可信息9Aa、9By，赋予作为存取对象的帐目信息的存取授权信息3－2（见图3）具有对存取授权元素fo22、fo25、fo28的逻辑求和操作符。即，存取授权是通过以下的公式（5）所获得的。

存取授权＝（fo22）或（fo25）或（fo28）

（5）

另外，根据存取授权的这种数学操作，存取控制单元允许存取主体的“R－－”存取（见图30）。

因此，人事和帐目部门管理员能够存取存放在卡式管理员媒体1中的帐目信息，但只能进行读入存取操作。当存取主体读入帐目信息时，例如，图4所示的读过程被正确执行时，存取主体能够读入帐目信息。但是，当存取主体试图写帐目信息时，因为存取主体不具有写存取授权，存取控制单元将拒绝写操作，并将错误通知给存取主体。

因而，根据涉及本发明的实施例的卡式记录媒体1，由于存取控制单元4被构造为控制存取主体对卡式记录媒体1中的数据的存取，所以在多目的应用的情况下，存取授权的设置和更改工作被简化，而安全系统的管理和操作可以可靠地执行。

也就是说，当执行对卡式记录媒体1中的数据的存取授权的设置和更改时，只需要更改获得被赋予数据的存取授权信息3－i中的存取授权的函数即可，而存取授权的设置和更改工作则可以简化。

另外，由于许可信息9可以被赋予与来自存取主体的所有存取请求对

应的每个存取主体，所以可以根据许可信息9来可靠地执行安全性的审计，这也加强了安全系统的性能。因此，安全系统的管理和操作可以可靠地被执行。

另外，考虑到多目的应用，安全系统可以被设计为只将注意力集中到相关的许可信息9和存取授权信息3－i，并可保持多个数据的独立性。

另外，由于可以执行对许可信息9的数学操作，因此可对所有商业目的提供许可信息9。因此，当业务从一项往另一项转变时，例如，在一项业务中所获得的商业信息9可能被删除时，它可避免许可信息9在业务之间产生混淆。反过来，则可设置许可信息9在业务之间产生混淆。

（b）其它

在涉及前述实施例的卡式记录媒体1中，在客户机应用12和存取控制单元4之间仅提供了一个逻辑通道13，通过它存取主体可以存取数据。但是，本发明并不仅限于此，如图6中所示，在多个客户机应用12A、12B和控制单元4之间可以提供多个逻辑通道13－1、13－2。另外，尽管附图中没有表示，但在一个客户机应用和控制单元4之间可以提供多个逻辑通道13－1、13－2（即，它对应于图6中所示的客户机应用12A、12B相同的情况）。

在这些情况下，存取控制单元4通过对每个逻辑通道13－1、13－2独立的客户机应用12A、12B控制对数据的存取。而且，在此情况下，存取控制单元4对逻辑通道13－1产生一条许可信息15a，而对逻辑通道13－2产生一条许可信息15b。

本发明虽然是这样进行描述的，但很明显可以通过许多方法对其进行变化。这种变化并不被认为是偏离了本发明的范围和精神，而对本领域技术人员来说，很明显，所有这些变化都将包括在下面的权利要求范围之内。

图1

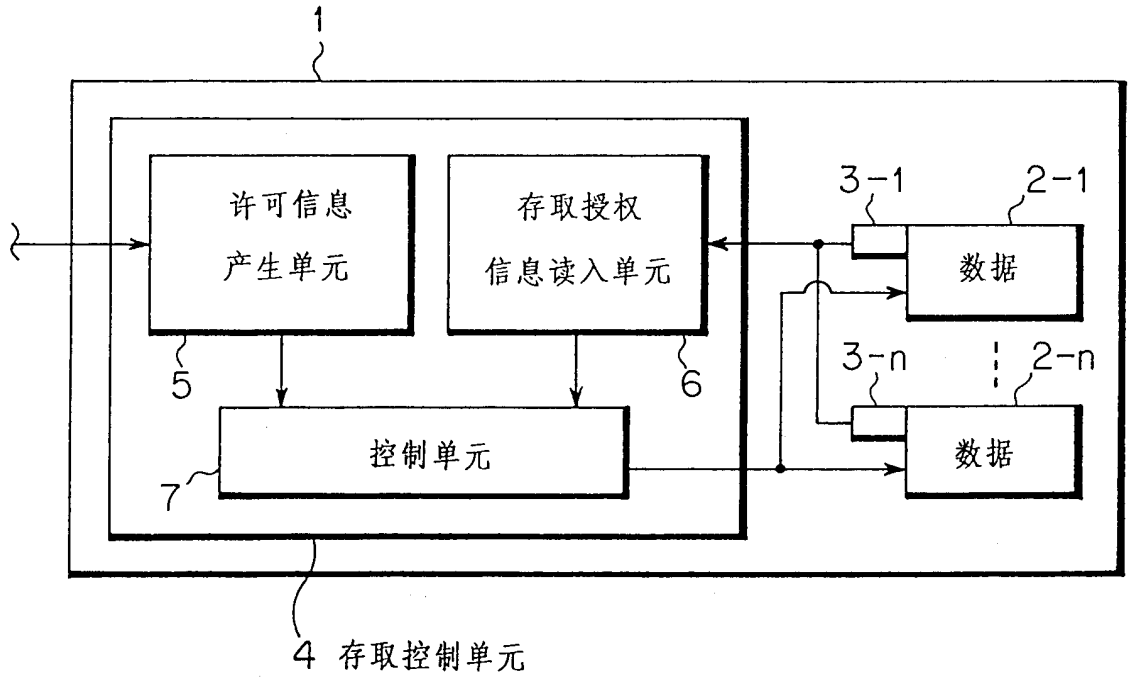


图2

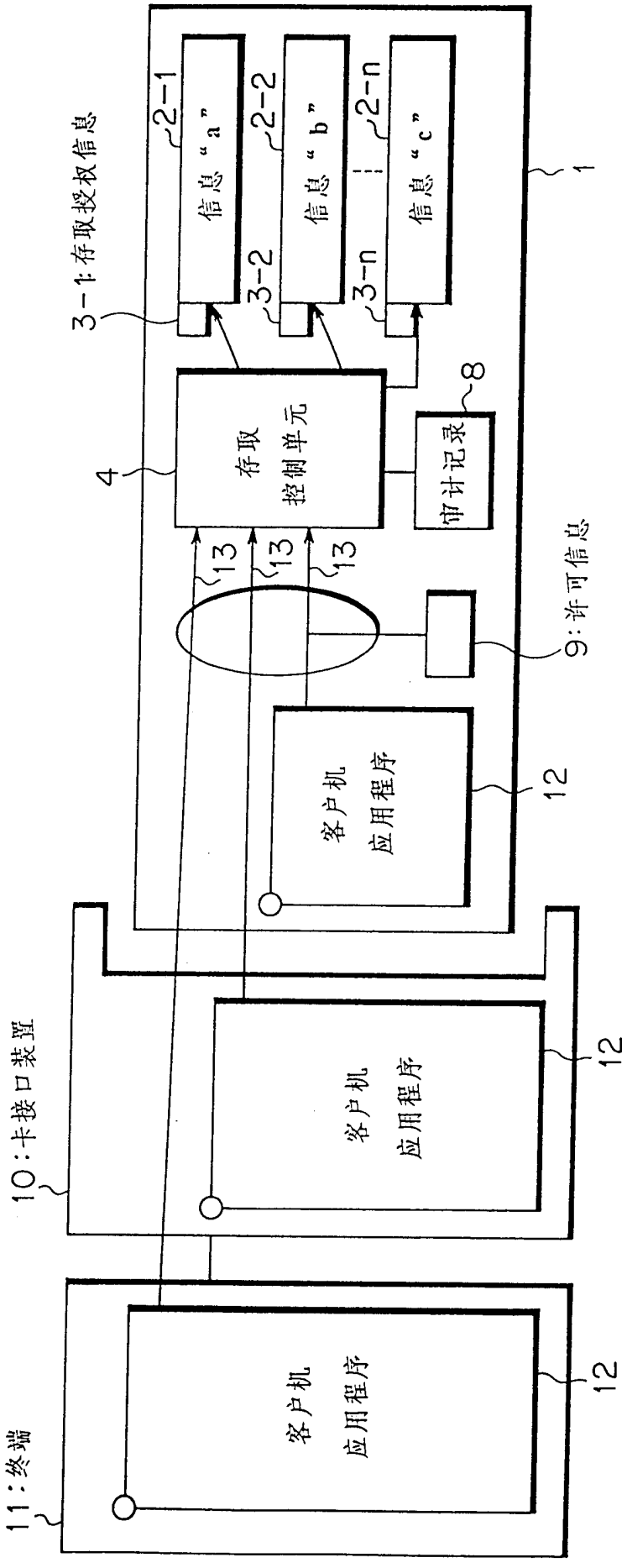

1
2-1
信息“a”
2-2
信息“b”
2-n
信息“c”
3-1:存取授权信息
3-2
3-n
4
存取
控制单元
8
审计记录
9:许可信息
13
13
13
12
客户机
应用程序
10:卡接口装置
12
客户机
应用程序
11:终端
12
客户机
应用程序

图3

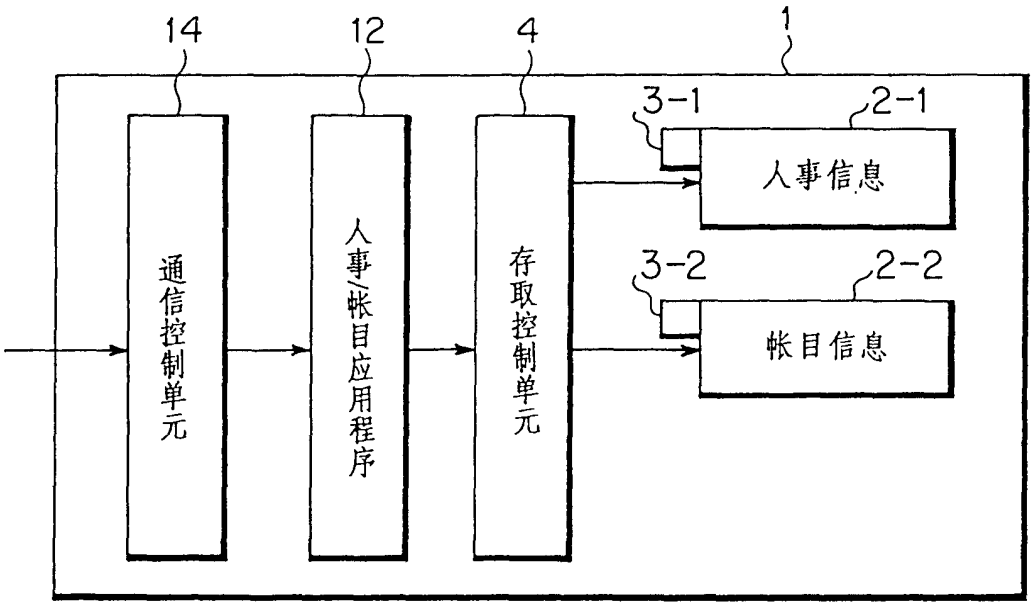

14
12
4
1
3-1
2-1
人事信息
3-2
2-2
帐目信息
通信控制单元
人事/帐目应用程序
存取控制单元

图4

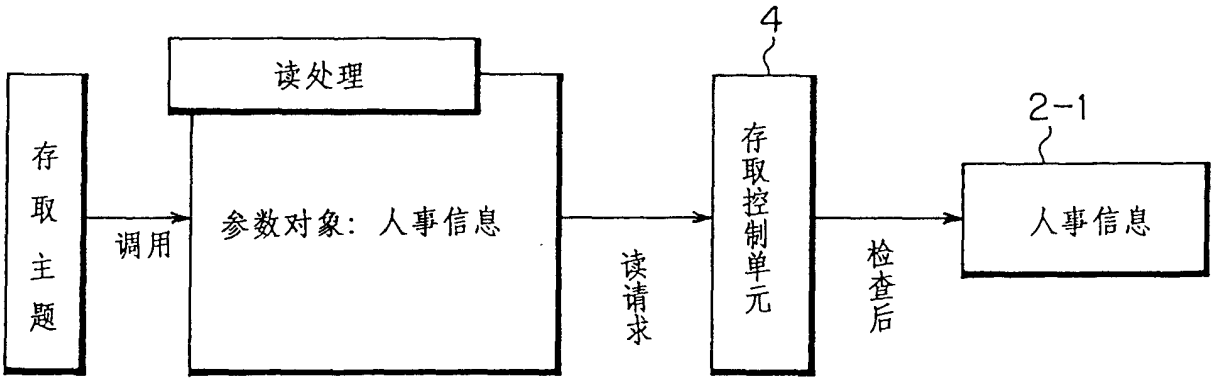

存取主题
调用
读处理
参数对象：人事信息
读请求
4
存取控制单元
检查后
2-1
人事信息

图5

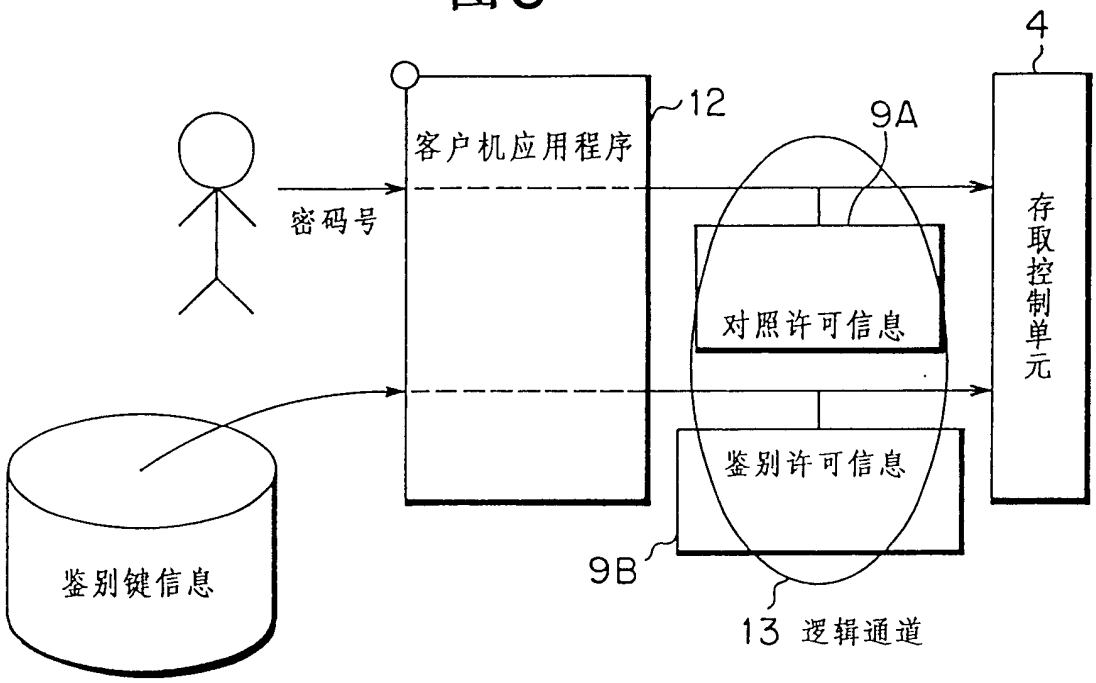

4
客户机应用程序
12
9A
密码号
对照许可信息
存取控制单元
鉴别许可信息
鉴别键信息
9B
13 逻辑通道

图6

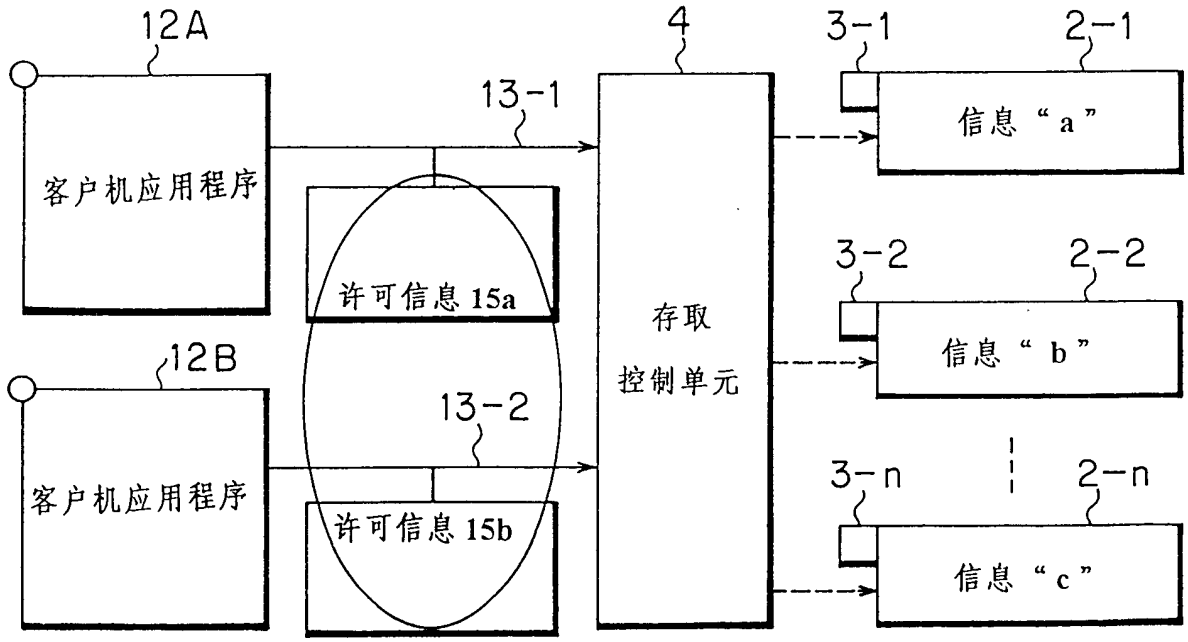

12A
4
3-1
2-1
13-1
客户机应用程序
信息“a”
许可信息 15a
存取
控制单元
3-2
2-2
12B
信息“b”
13-2
客户机应用程序
3-n
2-n
许可信息 15b
信息“c”

图7

审计计录文件（IEF）

记录号	记录
1	命令接收（第1次）
2	命令结果（第1次）
3	命令接收（第2次）
4	命令结果（第2次）
5	命令接收（第3次）
.	
n	命令结果（第m次）

命令接收记录的详细内容
以下信息存放在接收记录中
－接收计数（对卡OS中的每次命令接收计数）
－接收命令
－在接收前鉴别许可信息（在命令处理前鉴别许可信息）
－在接收前对照许可信息（在命令处理前对照许可信息）
命令接收记录的详细内容
以下信息存放在接收记录中
－接收计数（对卡OS中的每次命令接收计数）
－处理后的响应信息
－在处理后鉴别许可信息（在命令处理后鉴别许可信息）
－在处理后对照许可信息（在命令处理后对照许可信息）

图8(a)

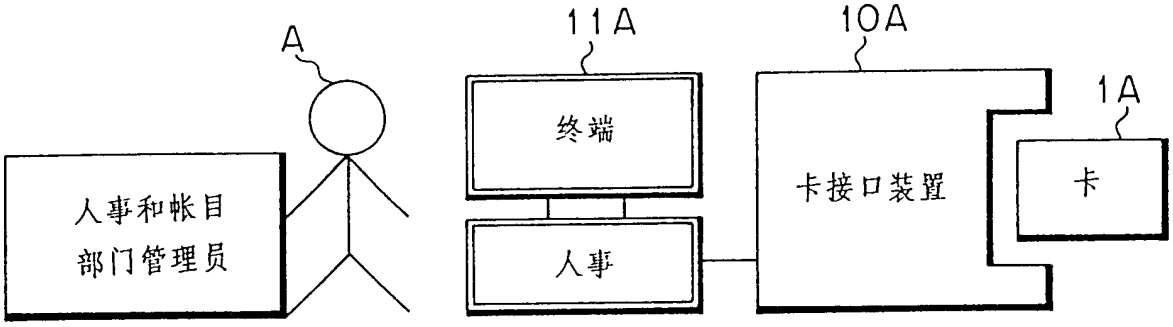

A
11A
10A
1A
终端
卡接口装置
卡
人事和帐目
部门管理员
人事

图8(b)

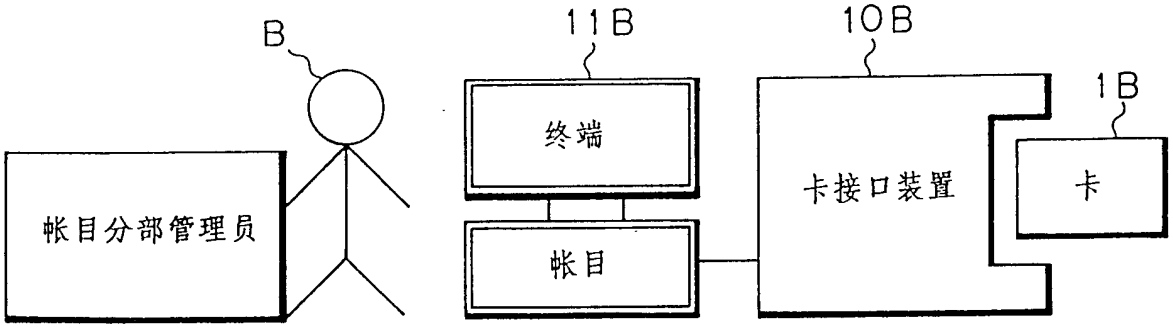

B
11B
10B
1B
终端
卡接口装置
卡
帐目分部管理员
帐目

图9(a)

具有帐目部门管理员和帐目分部管理员的许可

许可信息		分类				
		人事	帐目	一般事件	开发	购买
级别	部门管理员		○			
	部门主管管理员					
	分部管理员		○			
	一般级别					

图9(b)

新获得的一般事件的部门主管管理员的许可

许可信息		分类				
		人事	帐目	一般事件	开发	购买
级别	部门管理员					
	部门主管管理员			○		
	分部管理员					
	一般级别					

图9(c)

当许可的数学函数被定义为与以前的信息逻辑求和时

许可信息		分类				
		人事	帐目	一般事件	开发	购买
级别	部门管理员		○			
	部门主管管理员			○		
	分部管理员		○			
	一般级别					

图10(a)

对照许可信息		分类				
		人事	帐目	一般事件	开发	购买
级别	部门管理员		○			
	部门主管管理员			○		
	分部管理员		○			
	一般级别					

图 10(b)

鉴别许可信息		分类				
		人事	帐目	一般事件	开发	购买
级别	部门管理员					
	部门主管管理员			○		○
	分部管理员		○			
	一般级别					

图10(c)

对照/鉴别许可信息		分类				
		人事	帐目	一般事件	开发	购买
级别	部门管理员		○ —			
	部门主管管理员			○ ○		— ○
	分部管理员		○ ○			
	一般级别					

图11

存取授权信息

Fo：合成的逻辑函数						
鉴别许可信息		分类				
		人事	帐目	一般事件	开发	购买
	部门管理员	fo 11	fo 12	fo 13	fo 14	fo 15
	部门主管管理员	fo 21	fo 22	fo 23	fo 24	fo 25
	分部管理员	fo 31	fo 32	fo 33	fo 34	fo 35
	一般级别	fo 41	fo 42	fo 43	fo 44	fo 45

fo12：

对照	鉴别	存取授权
O	O	=RWX
O	—	=RW-
—	O	=RW-
—	—	=---

fo23：

对照	鉴别	存取授权
O	O	=RW-
O	—	=R--
—	O	=R--
—	—	=---

fo25：

对照	鉴别	存取授权
O	O	=---
O	—	=---
—	O	=---
—	—	=---

fo32：

对照	鉴别	存取授权
O	O	=RWX
O	—	=R-X
—	O	=R-X
—	—	=---

} Q

在以下假设下所获得的存取授权

若 Fo=(fo12 OR fo23) AND (fo32)---(1)

Fo=(RW- OR RW-) AND (RWX)=RW-

图12

许可信息		分类		
		人事	帐目	其它
级别	部门管理员			
	分部管理员			
	其它			

图13(a)

对照（口令“a”：人事和帐目部门管理员）

对照许可信息 9Aa		分类		
		人事	帐目	其它
级别	部门管理员	○	○	
	分部管理员			
	其它			

图13(b)

对照（口令“b”：帐目分部管理员）

对照许可信息 9Ab		分类		
		人事	帐目	其它
级别	部门管理员			
	分部管理员		○	
	其它			

图14(a)

鉴别（密码键“y”：人事终端）

对照许可信息 9By		分类		
		人事	帐目	其它
级别	部门管理员	○		
	分部管理员	○		
	其它	○		

图14(b)

鉴别（密码键“z”：帐目终端）

对照许可信息 9Bz		分类		
		人事	帐目	其它
级别	部门管理员		○	
	分部管理员		○	
	其它		○	

图15

操作者：Fo1

人事信息标签信息		分类		
		人事	帐目	其它
级别	部门管理员	fo11	fo12	fo13
	分部管理员	fo14	fo15	fo16
	其它	fo17	fo18	fo19

图16

操作者: Fo2				
帐目信息 标签信息		分类		
		人事	帐目	其它
级别	部门管理员	fo21	fo22	fo23
	分部管理员	fo24	fo25	fo26
	其它	fo27	fo28	fo29

图17

存取授权的条件定义

R: 读授权　　W: 写授权　　X: 删除授权

fo11:			fo12: (没定义)			fo13: (没定义)		
对照	鉴别	存取授权	对照	鉴别	存取授权	对照	鉴别	存取授权
○	○	=RWX	○	○	=---	○	○	=---
○	—	=R--	○	—	=---	○	—	=---
—	○	=---	—	○	=---	—	○	=---
—	—	=---	—	—	=---	—	—	=---
fo14:			**fo15: (没定义)**			**fo16: (没定义)**		
对照	鉴别	存取授权	对照	鉴别	存取授权	对照	鉴别	存取授权
○	○	=RW-	○	○	=---	○	○	=---
○	—	=R--	○	—	=---	○	—	=---
—	○	=---	—	○	=---	—	○	=---
—	—	=---	—	—	=---	—	—	=---
fo17:			**fo18: (没定义)**			**fo19: (没定义)**		
对照	鉴别	存取授权	对照	鉴别	存取授权	对照	鉴别	存取授权
○	○	=R--	○	○	=---	○	○	=---
○	—	=---	○	—	=---	○	—	=---
—	○	=---	—	○	=---	—	○	=---
—	—	=---	—	—	=---	—	—	=---

图18

存取授权的条件定义　　R：读授权　　W：写授权　　X：删除授权

fo21：（没定义）

对照	鉴别	存取授权
○	○	=---
○	—	=---
—	○	=---
—	—	=---

fo22：

对照	鉴别	存取授权
○	○	=RWX
○	—	=R--
—	○	=---
—	—	=---

fo23：（没定义）

对照	鉴别	存取授权
○	○	=---
○	—	=---
—	○	=---
—	—	=---

fo24：（没定义）

对照	鉴别	存取授权
○	○	=---
○	—	=---
—	○	=---
—	—	=---

fo25：

对照	鉴别	存取授权
○	○	=RW-
○	—	=R--
—	○	=---
—	—	=---

fo26：（没定义）

对照	鉴别	存取授权
○	○	=---
○	—	=---
—	○	=---
—	—	=---

fo27：（没定义）

对照	鉴别	存取授权
○	○	=---
○	—	=---
—	○	=---
—	—	=---

fo28：

对照	鉴别	存取授权
○	○	=R--
○	—	=---
—	○	=---
—	—	=---

fo29：（没定义）

对照	鉴别	存取授权
○	○	=---
○	—	=---
—	○	=---
—	—	=---

图19

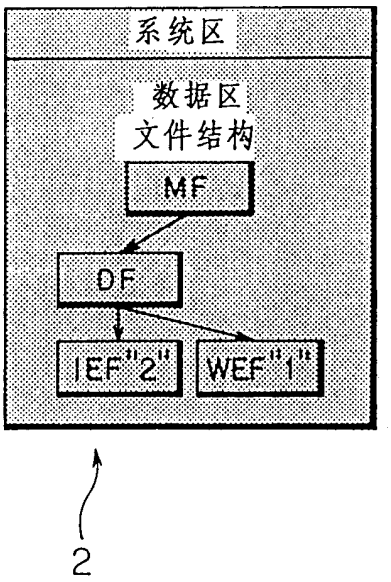


图20

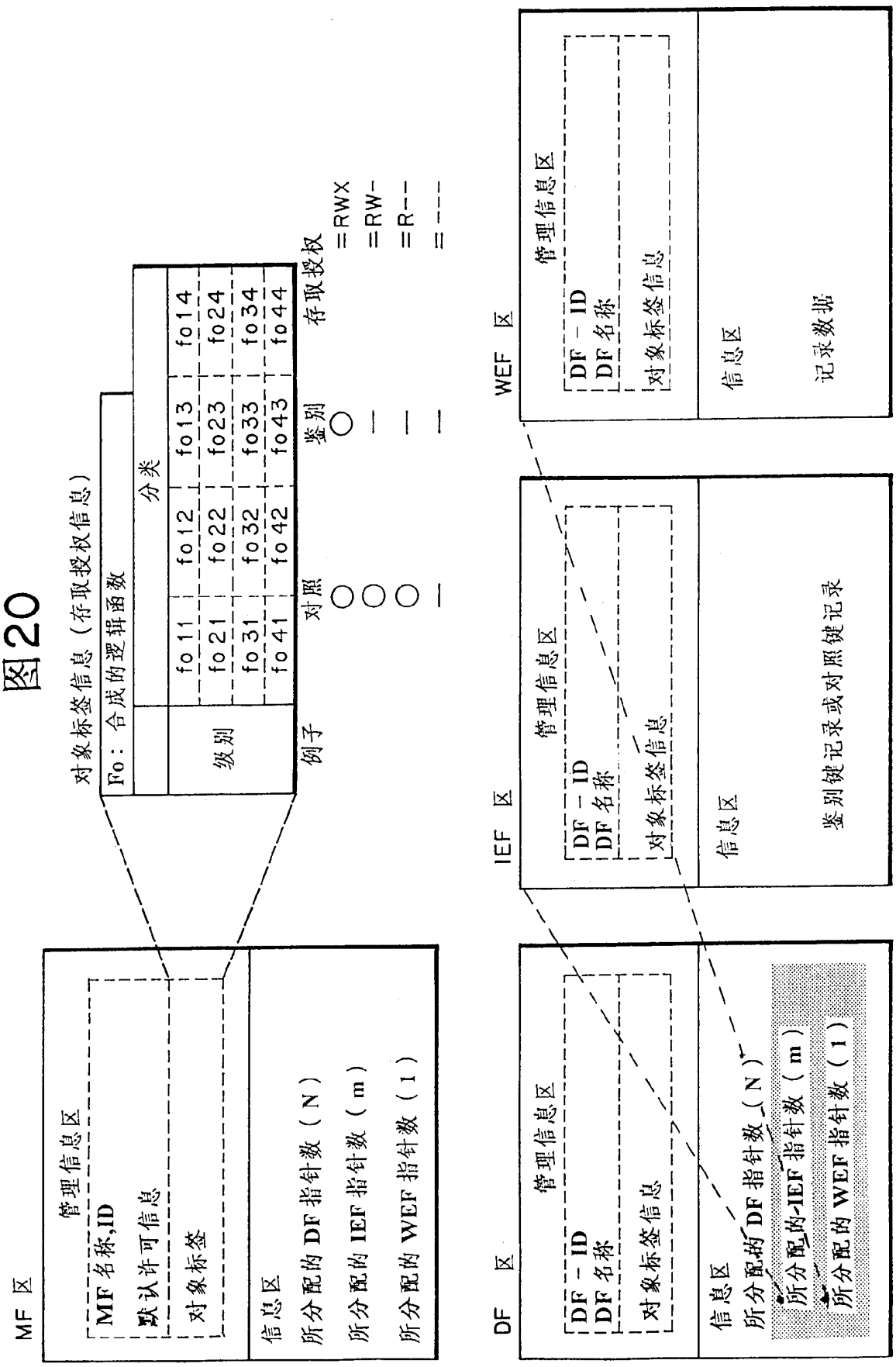

MF 区
管理信息区
MF 名称,ID
缺认许可信息
对象标签
信息区
所分配的 DF 指针数（N）
所分配的 IEF 指针数（m）
所分配的 WEF 指针数（1）
对象标签信息（存取授权信息）
Fo：合成的逻辑函数
分类
级别
fo11 fo12 fo13 fo14
fo21 fo22 fo23 fo24
fo31 fo32 fo33 fo34
fo41 fo42 fo43 fo44
例子
对照
鉴别
存取授权
○ ○ ○ —
○ — — —
○ — — —
— — — —
=RWX
=RW-
=R--
=----
DF 区
管理信息区
DF－ID
DF 名称
对象标签信息
信息区
所分配的 DF 指针数（N）
所分配的 IEF 指针数（m）
所分配的 WEF 指针数（1）
IEF 区
管理信息区
DF－ID
DF 名称
对象标签信息
信息区
鉴别键记录或对照键记录
WEF 区
管理信息区
DF－ID
DF 名称
对象标签信息
信息区
记录数据

图21(b)

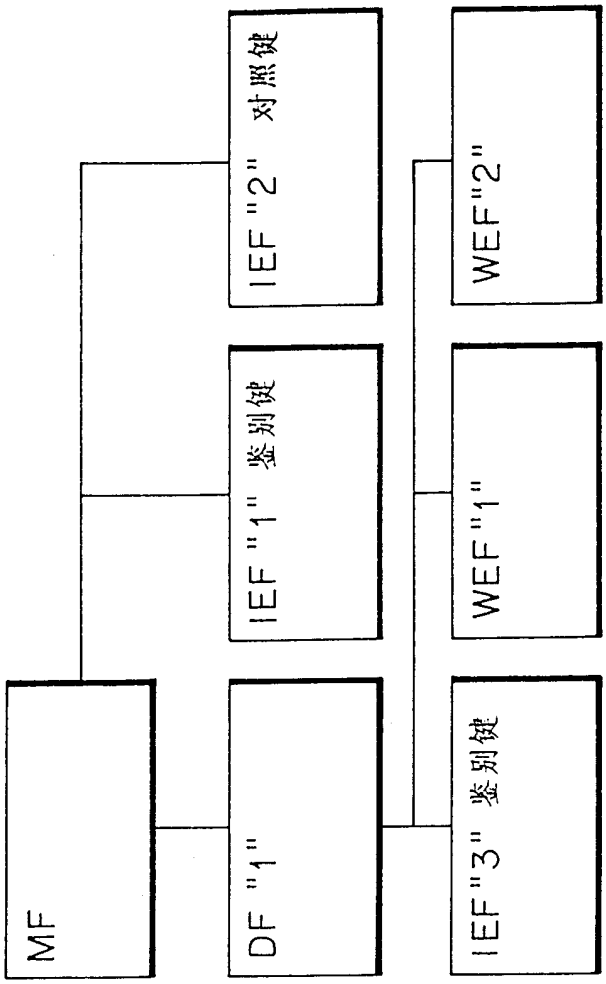

MF
DF "1"
IEF "1" 鉴别键
IEF "2" 对照键
IEF "3" 鉴别键
WEF "1"
WEF "2"

图21(a)

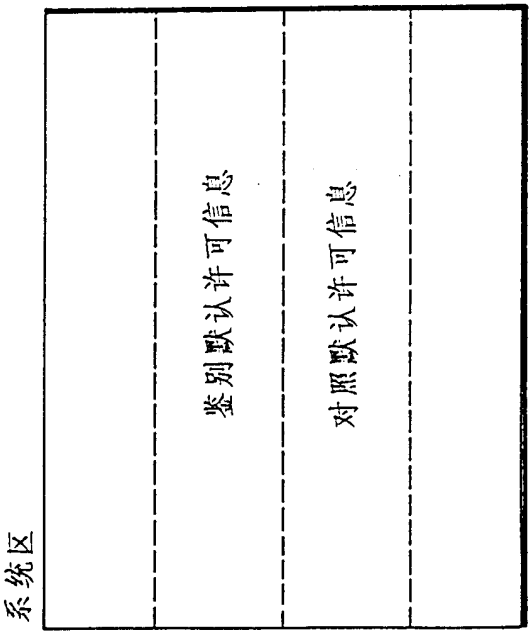

系统区
鉴别默认许可信息
对照默认许可信息

图22(a)

鉴别默认许可信息

F0	分类			
级别	○			

F0: 新许可＝所获得的许可

图22(b)

对照默认许可信息

F0	分类			
级别	○			

F0: 新许可＝所获得的许可

图22(c)

鉴别所获得的许可信息（存放在IEF “1”）

F1	分类			
级别	○			
		○	○	

F1: 新许可＝当前许可和所获得的许可的逻辑和

图22(d)

对照所获得的许可信息（存放在IEF “2”中）

F2	分类			
级别	○			
		○		
		○		

F2: 新许可＝当前许可和所获得的许可的逻辑和

图23(a)

鉴别所获得的许可信息（存放在IEF “3”中）

F3	分类			
级别	○			
		○	○	
		○	○	

F3 新许可＝当前许可和所获得的许可的逻辑和

图23(b)

WEF “1”的对象标签信息

Fo：合成的逻辑函数

	分类			
级别	fo11	—	—	—
	—	fo22	fo23	—
	—	fo32	—	—
	—	—	—	—

Fo

	鉴别	对照	存取授权
fo11	○	○	–––
fo22	○	○	R––
fo23	○	○	–W–
fo32	○	○	––X

存取授权的定义

R：读授权　　W：写授权　　X：删除授权

图24

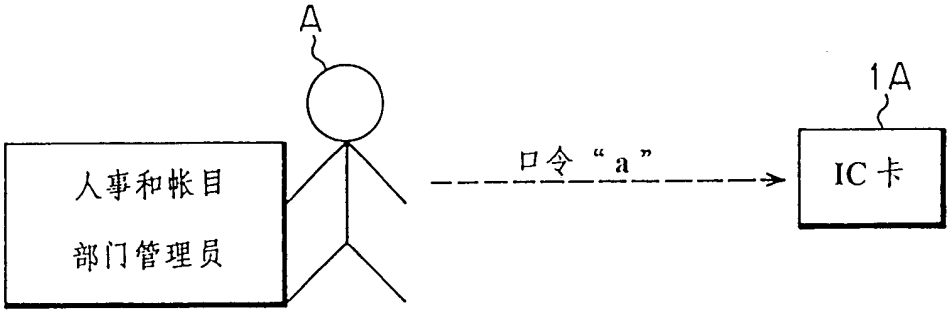


图25

对照许可信息9Aa		分类		
		人事	帐目	其它
级别	部门管理员	○	○	
	分部管理员			
	其它			

图26

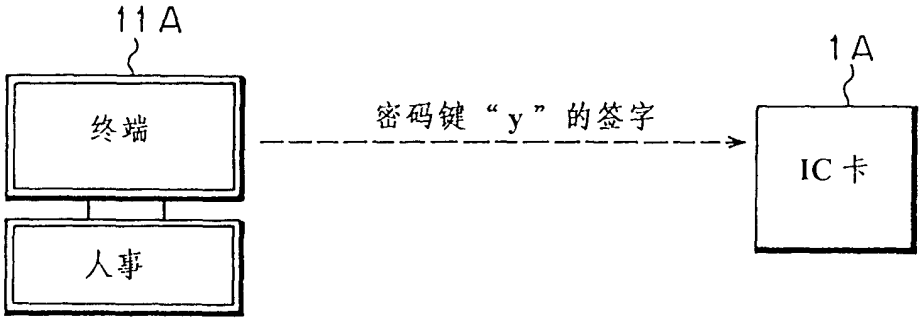


图27

鉴别许可信息 9By		分类		
		人事	帐目	其它
级别	部门管理员	○		
	分部管理员	○		
	其它	○		

图 28

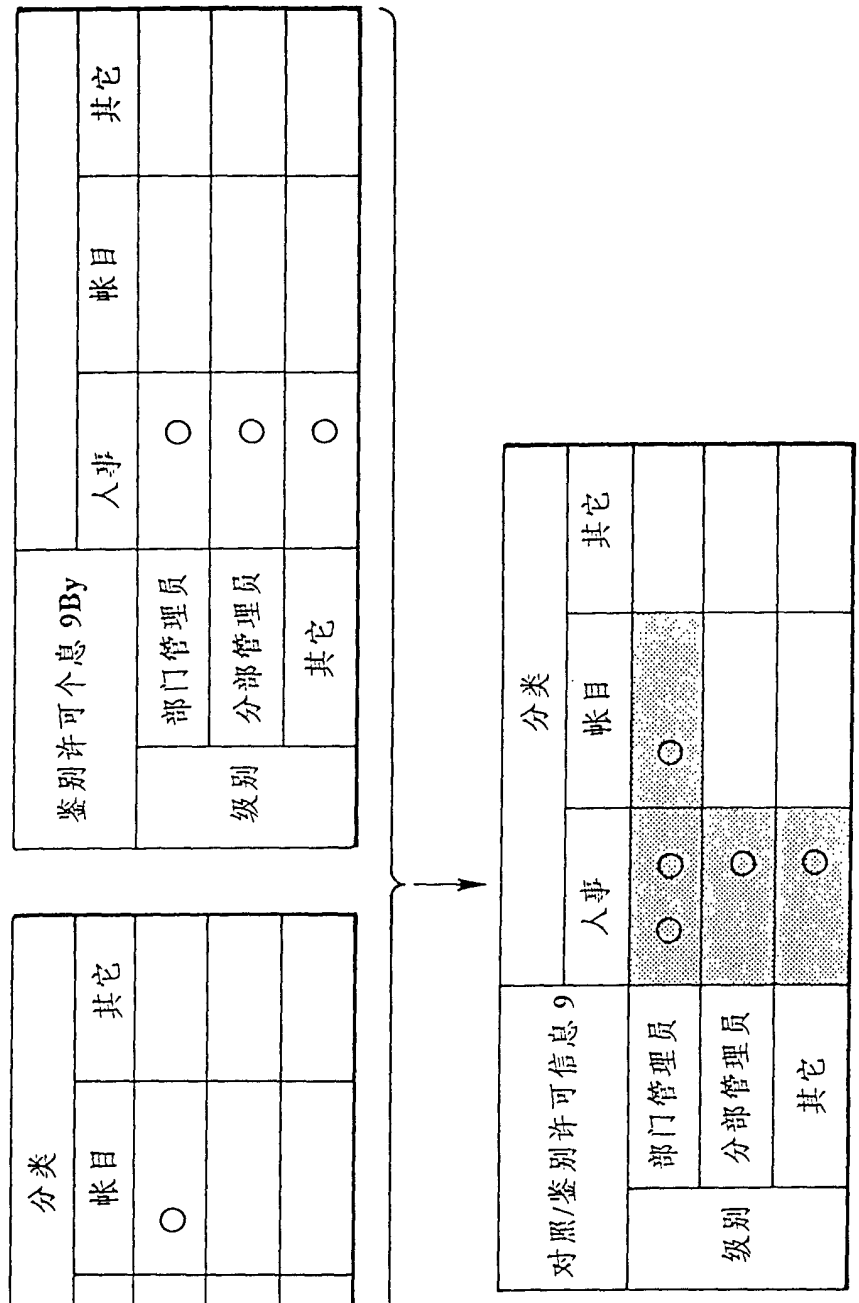

对照许可信息 9Aa
分类
人事
帐目
其它
级别
部门管理员
分部管理员
其它
○
鉴别许可个息 9By
分类
人事
帐目
其它
级别
部门管理员
分部管理员
其它
○
对照/鉴别许可信息 9
分类
人事
帐目
其它
级别
部门管理员
分部管理员
其它
○

图29

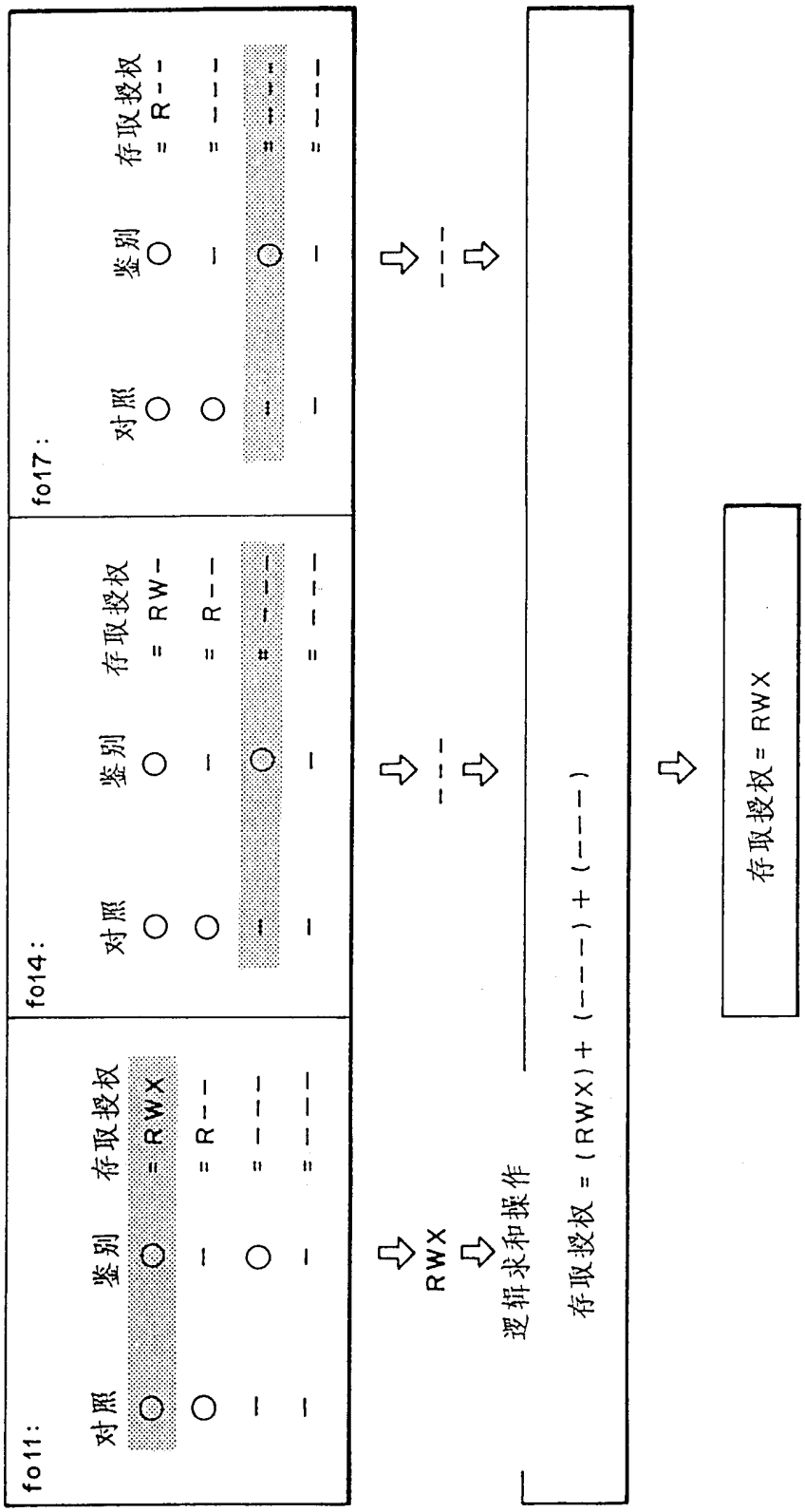
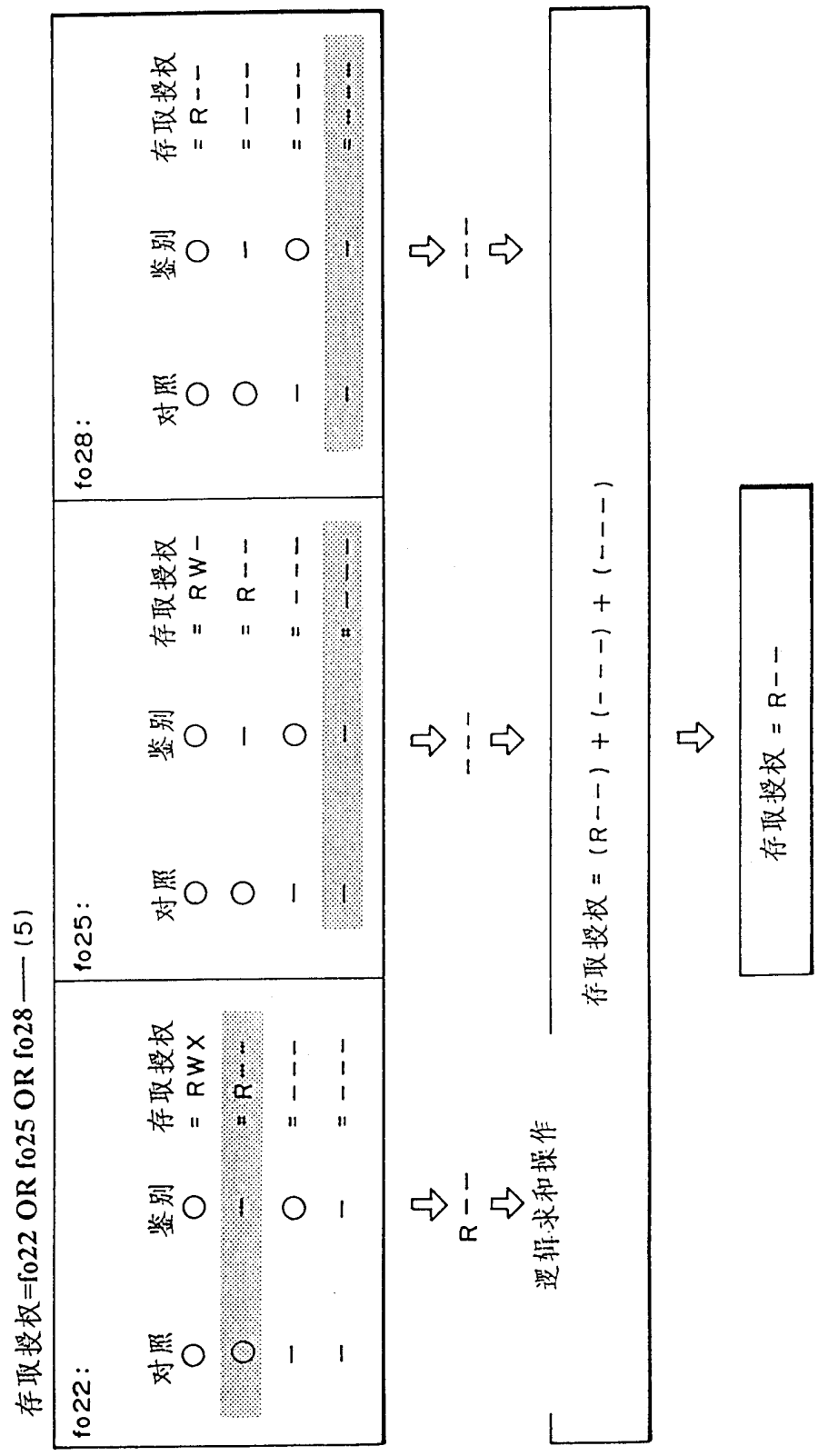

存取授权 = fo11 OR fo14 OR fo17 —— (4)
fo11:
对照 鉴别 存取授权
○ ○ = RWX
○ – = R– –
– ○ = – – –
– – = – – –
fo14:
对照 鉴别 存取授权
○ ○ = RW–
○ – = R– –
– ○ = – – –
– – = – – –
fo17:
对照 鉴别 存取授权
○ ○ = R– –
○ – = – – –
– ○ = – – –
– – = – – –
RWX
– – –
逻辑求和操作
存取授权 = (RWX) + (– – –) + (– – –)
存取授权 = RWX

图30


存取授权=fo22 OR fo25 OR fo28——(5)
fo22:
对照 ○ 鉴别 ○ 存取授权 = RWX
○ — = R--
— ○ = ----
— — = ----
fo25:
对照 ○ 鉴别 ○ 存取授权 = RW-
○ — = R--
— ○ = ----
— — = ----
fo28:
对照 ○ 鉴别 ○ 存取授权 = R--
○ — = ----
— ○ = ----
— — = ----
R--

逻辑求和操作
存取授权 = (R--) + (---) + (----)
存取授权 = R--

图 31

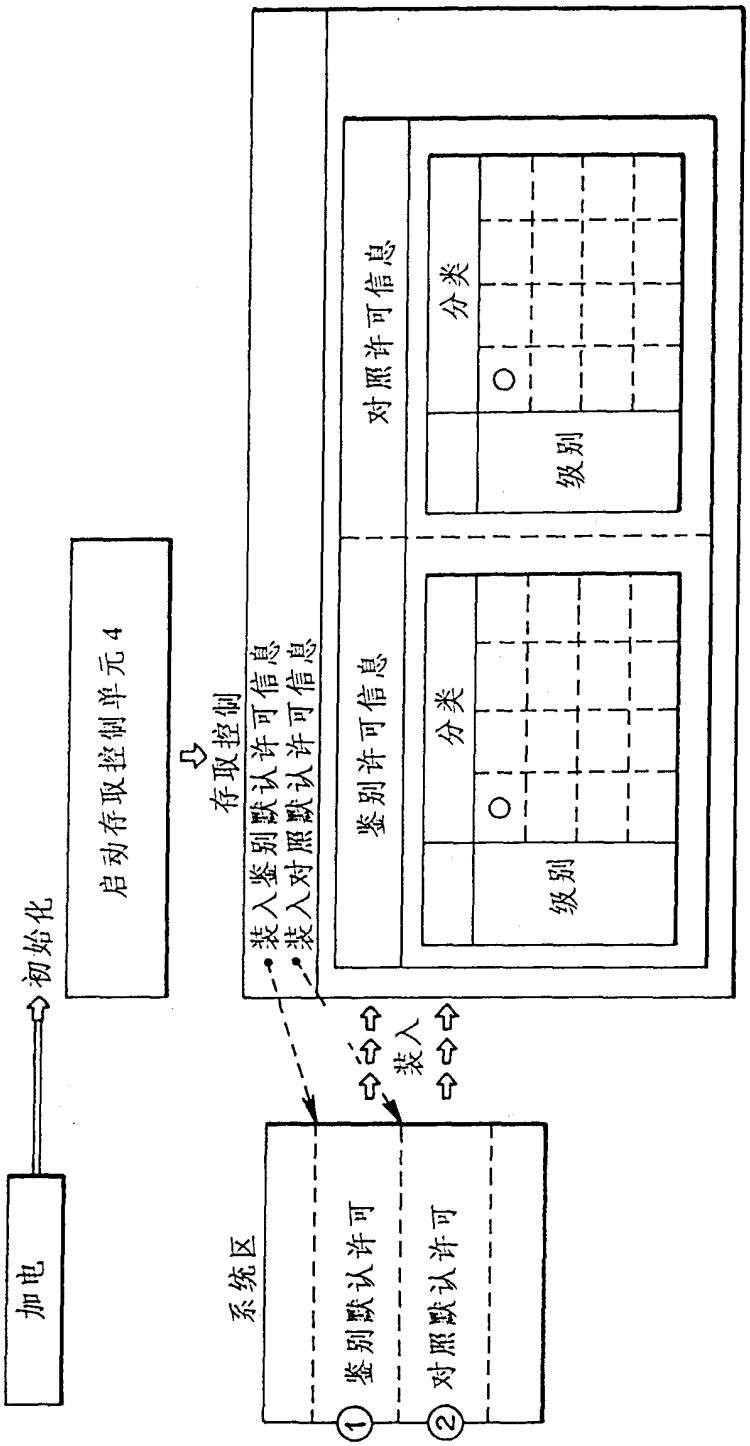

加电
初始化
启动存取控制单元 4
存取控制侧
装入鉴别默认许可信息
装入对照默认许可信息
鉴别许可信息
对照许可信息
分类
级别
分类
级别
装入
系统区
① 鉴别默认许可
② 对照默认许可

图32

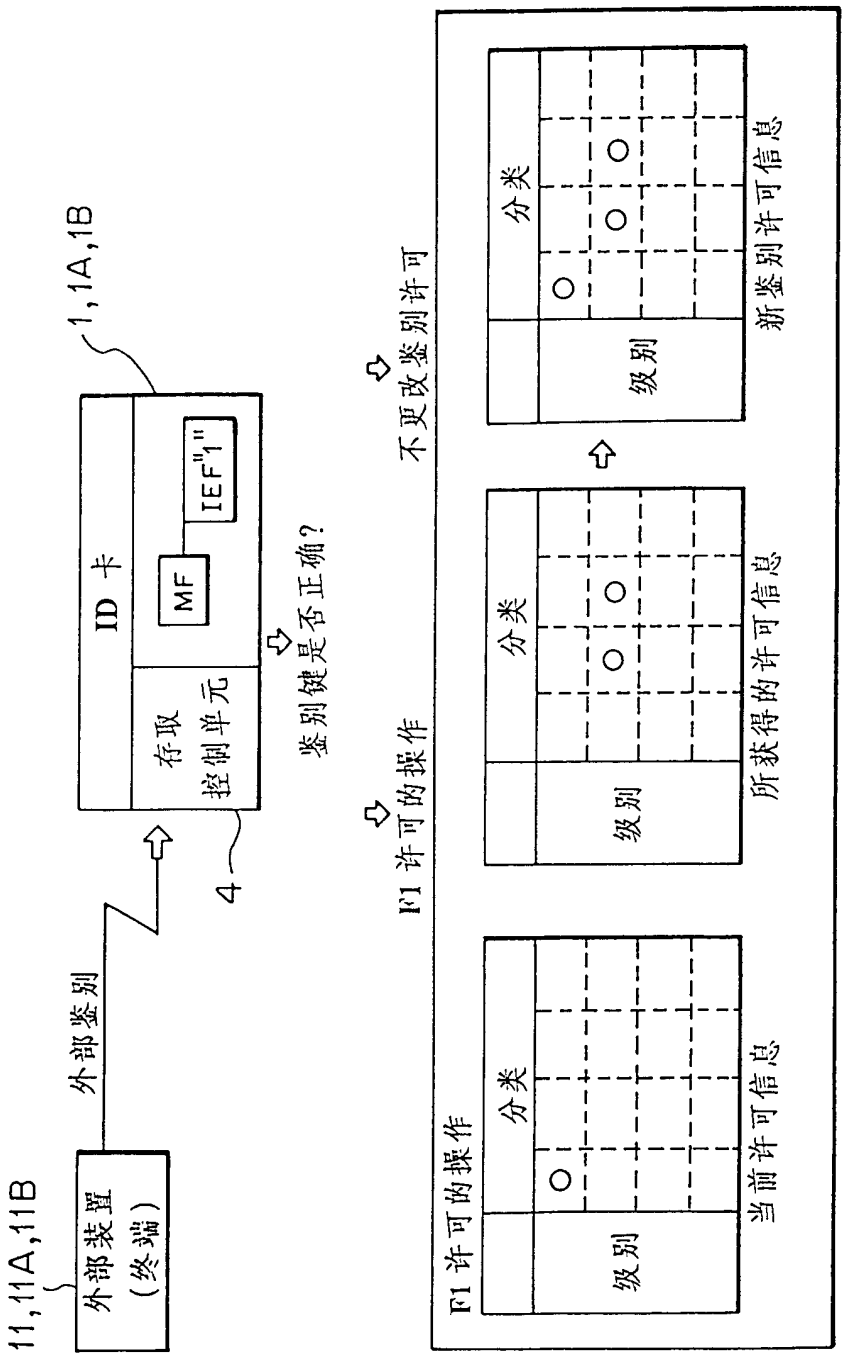

11,11A,11B
外部装置
(终端)
外部鉴别
1,1A,1B
ID 卡
存取
控制单元
MF
IEF"1"
4
鉴别键是否正确?
不更改鉴别许可
F1 许可的操作
分类
级别
当前许可信息
所获得的许可信息
新鉴别许可信息

图 33

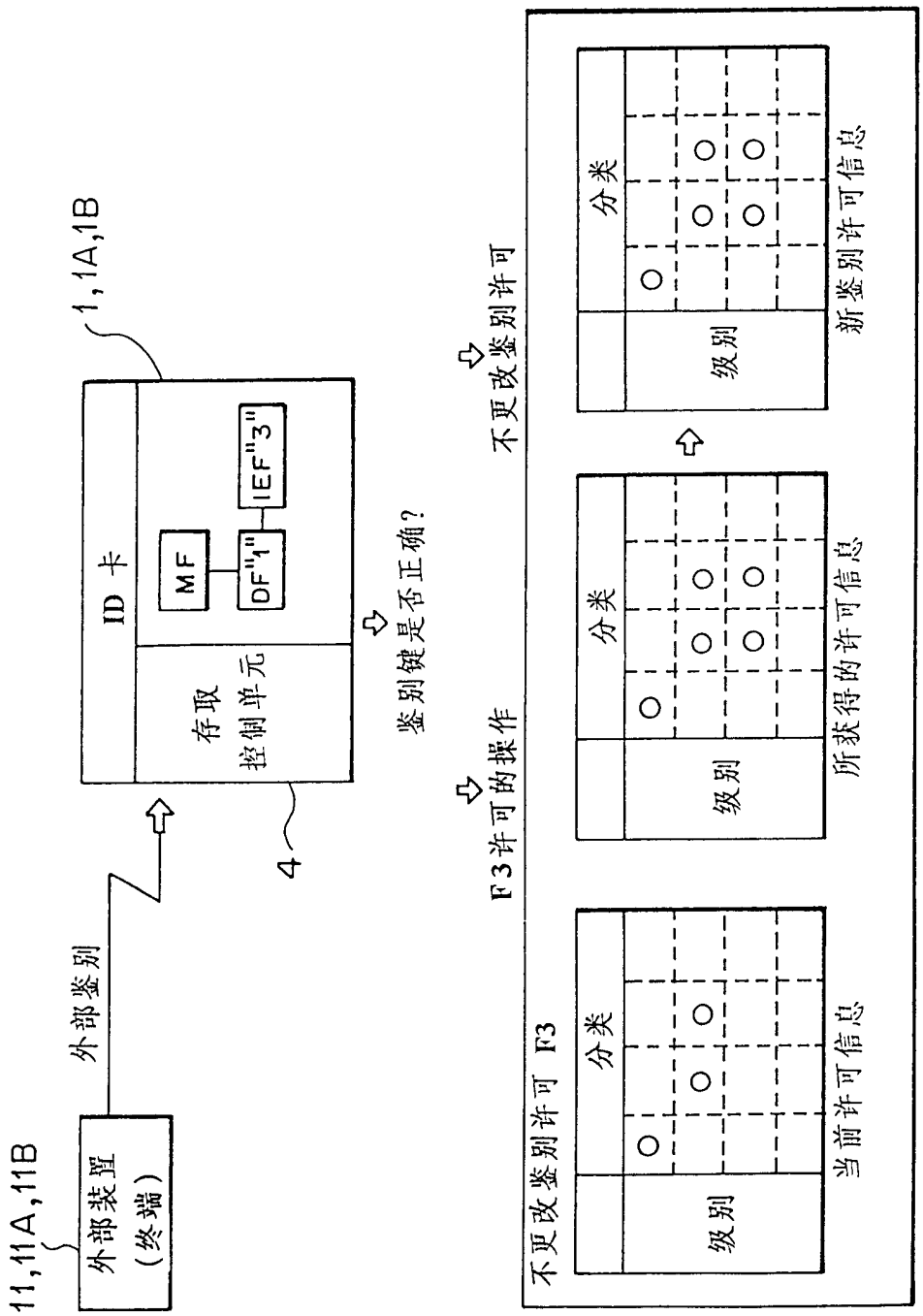

11,11A,11B
外部装置
（终端）
外部鉴别
1,1A,1B
ID 卡
存取
控制单元
MF
DF"1"
IEF"3"
4
鉴别键是否正确？
不更改鉴别许可
F3许可的操作
不更改鉴别许可 F3
分类
级别
当前许可信息
分类
级别
所获得的许可信息
分类
级别
新鉴别许可信息

图34

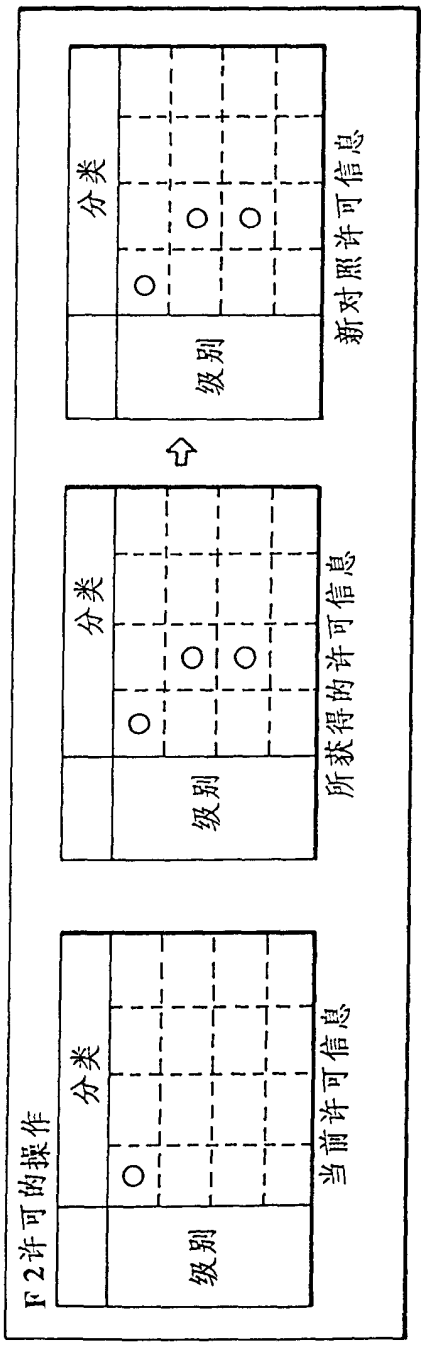


图35

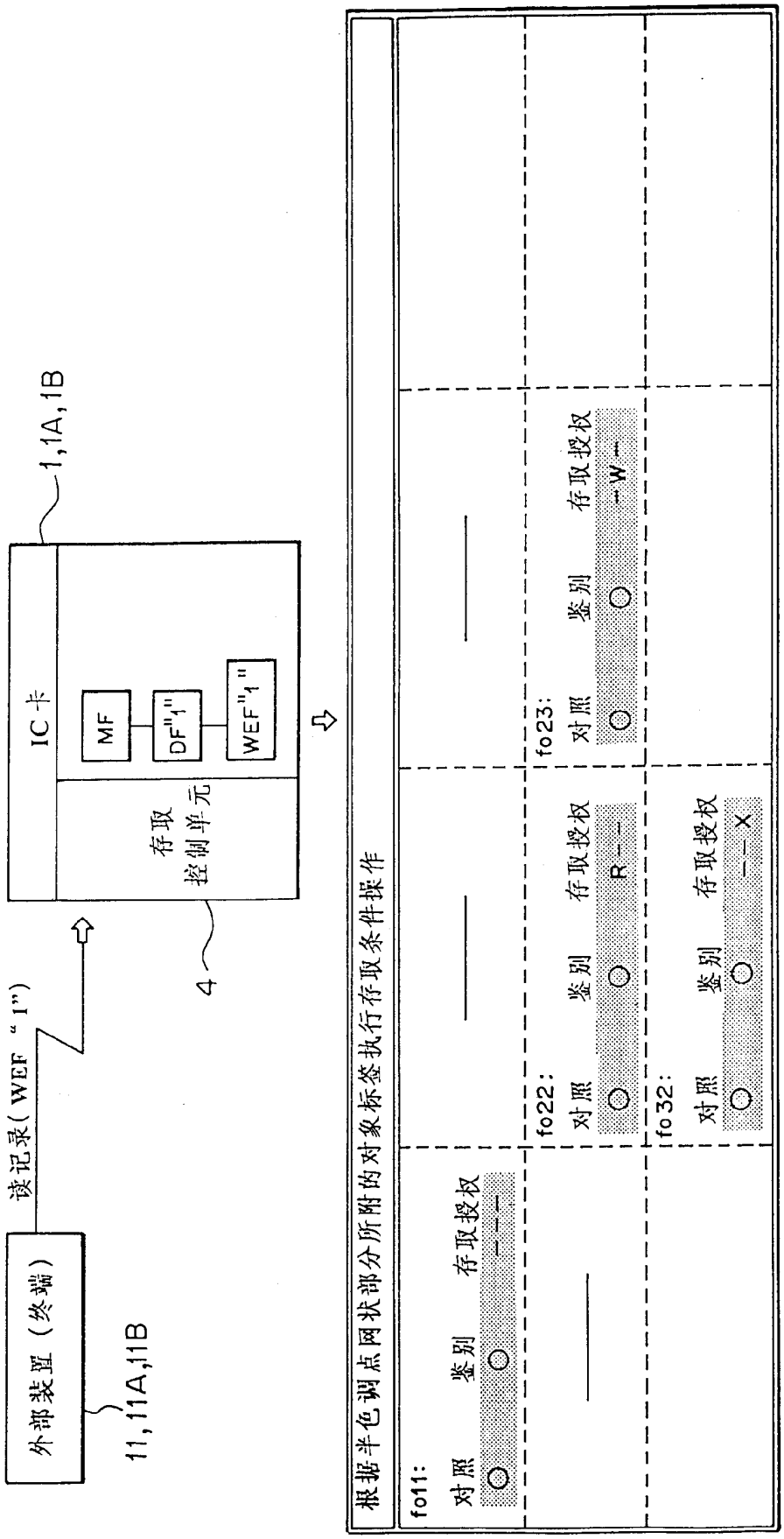

外部装置（终端）
11,11A,11B
读记录(WEF "1")
IC卡
1,1A,1B
存取
控制单元
MF
DF"1"
WEF"1"
4
根据半色调点网状部分所附的对象标签执行存取条件操作
fo11:
对照
鉴别
存取授权
O
O
---
fo22:
对照
鉴别
存取授权
O
O
R--
fo23:
对照
鉴别
存取授权
O
O
-W-
fo32:
对照
鉴别
存取授权
O
O
--X

图 36

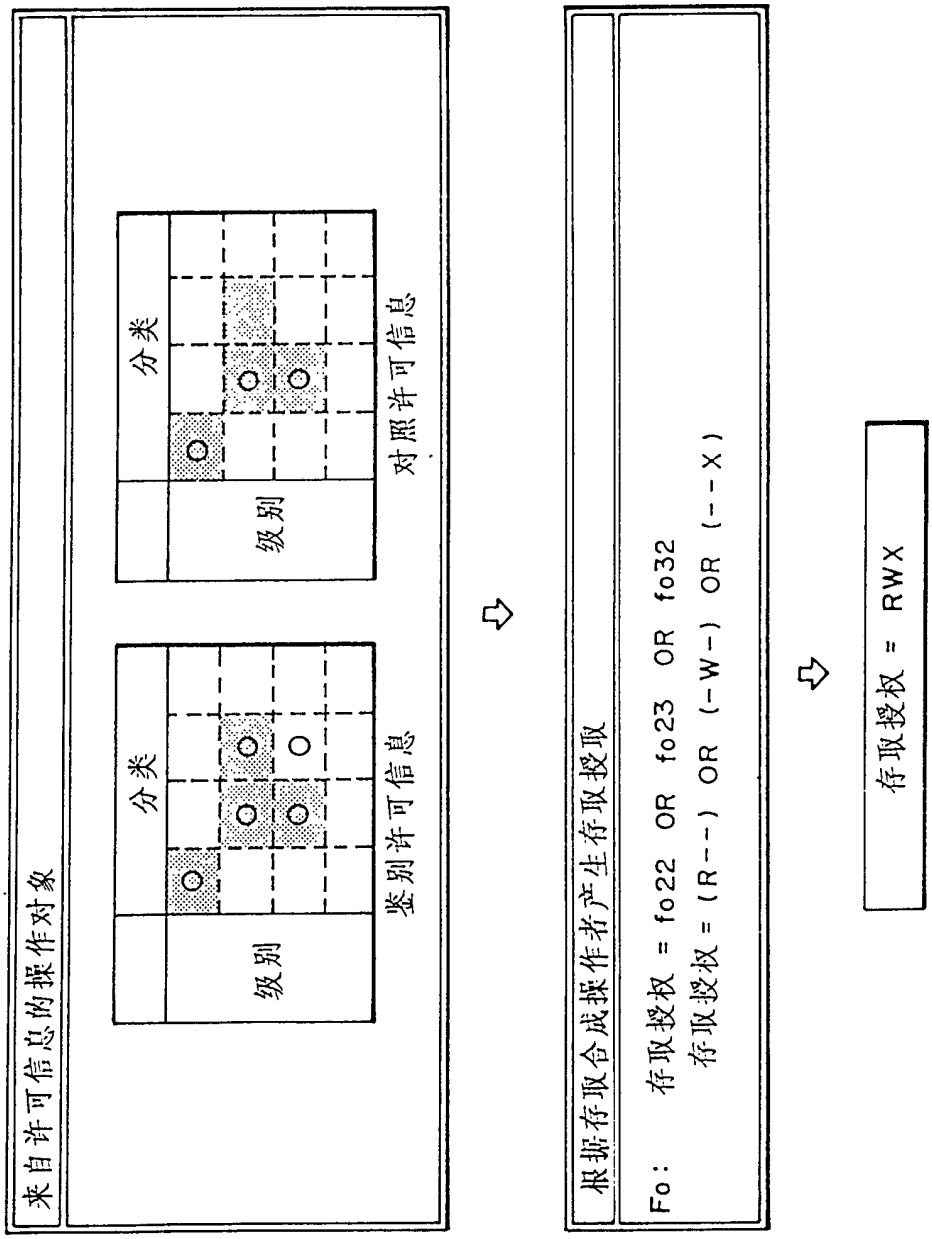

来自许可信息的操作对象
分类
级别
鉴别许可信息
分类
级别
对照许可信息
根据存取合成操作者产生存取授取
Fo: 存取授权 = fo22 OR fo23 OR fo32
存取授权 = (R--) OR (-W-) OR (--X)
存取授权 = RWX

图 37

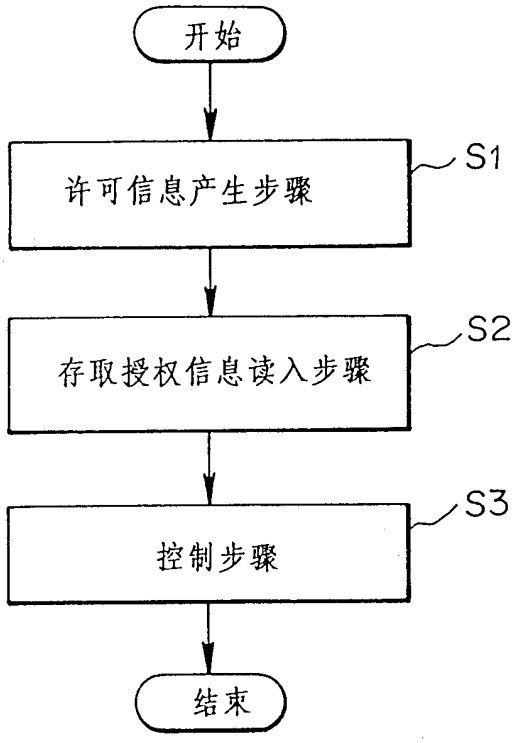


图38

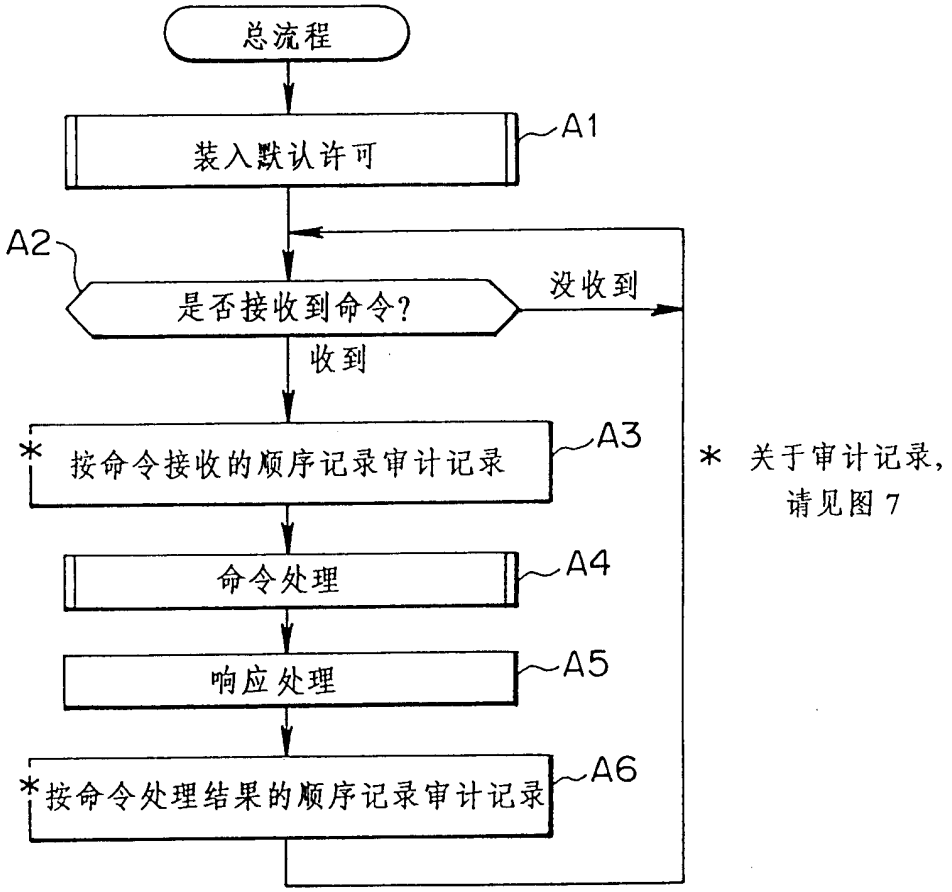

总流程
装入默认许可
A1
A2
是否接收到命令?
没收到
收到
*按命令接收的顺序记录审计记录
A3
命令处理
A4
响应处理
A5
*按命令处理结果的顺序记录审计记录
A6
* 关于审计记录，
请见图7

图 39

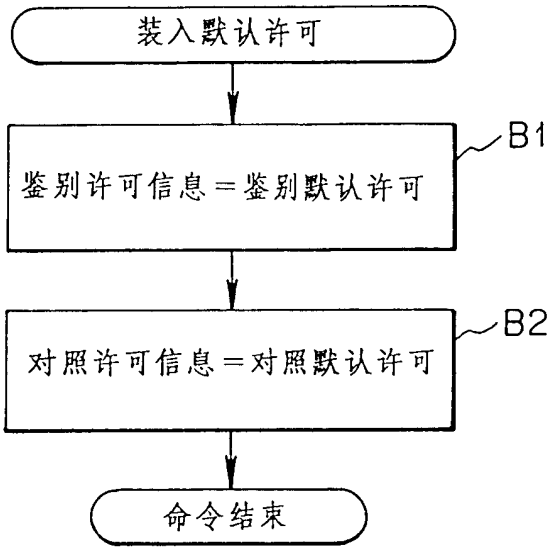


图 40

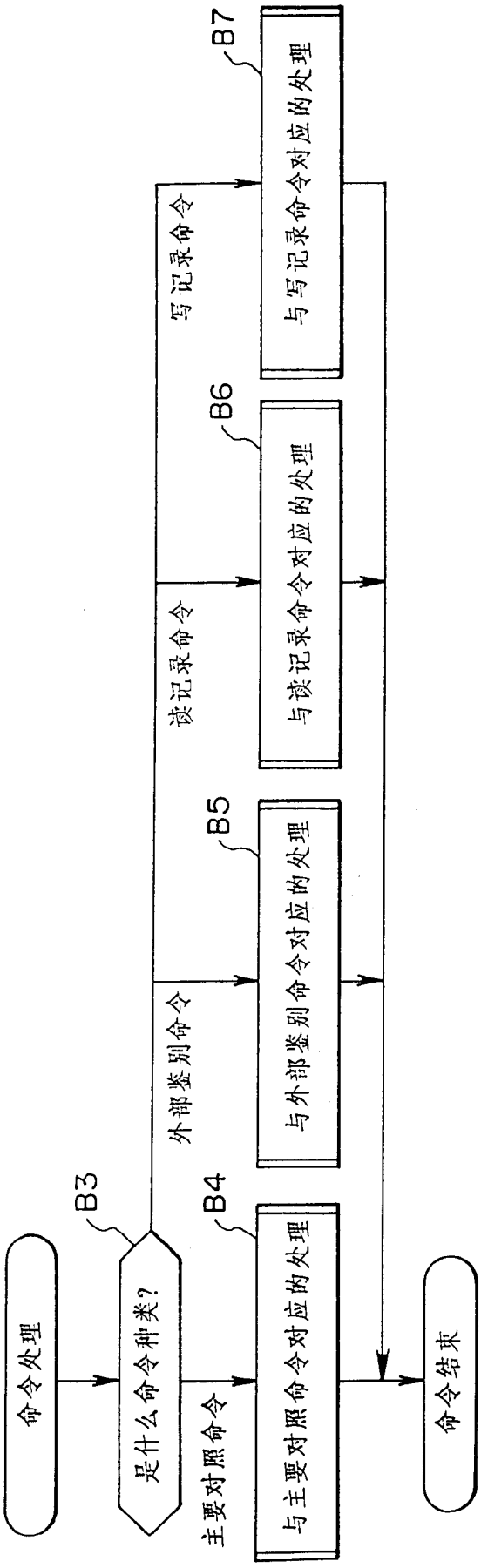

命令处理
是什么命令种类?
主要对照命令
与主要对照命令对应的处理
外部鉴别命令
与外部鉴别命令对应的处理
读记录命令
与读记录命令对应的处理
写记录命令
与写记录命令对应的处理
命令结束
B3
B4
B5
B6
B7

图41

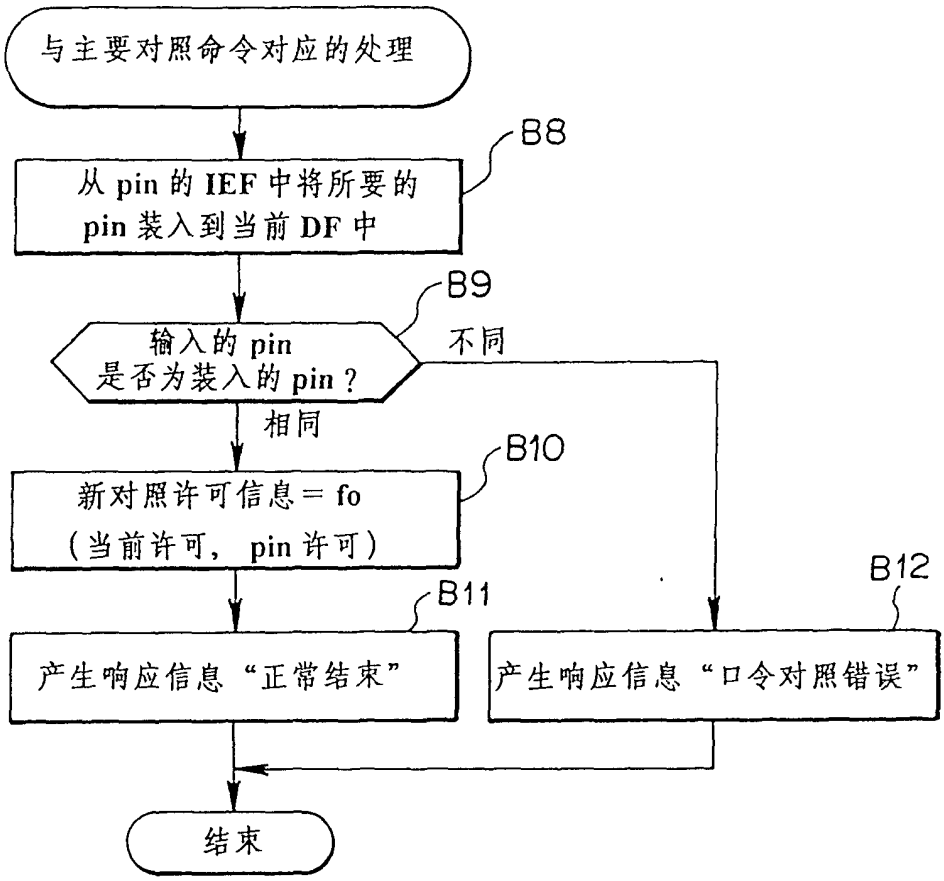
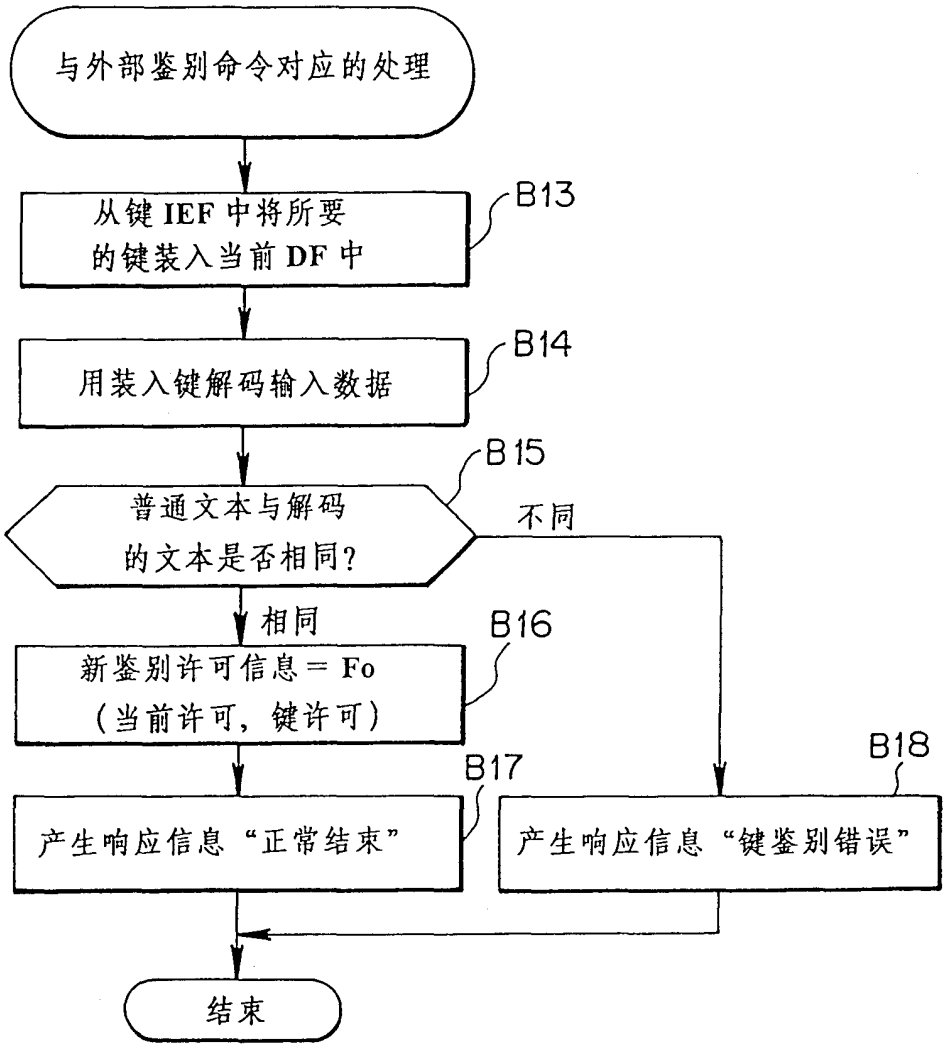

与主要对照命令对应的处理
B8
从 pin 的 IEF 中将所要的 pin 装入到当前 DF 中
B9
输入的 pin 是否为装入的 pin？
不同
相同
B10
新对照许可信息＝ fo
（当前许可， pin 许可）
B11
产生响应信息“正常结束”
B12
产生响应信息“口令对照错误”
结束

图 42



※ 在“外部”命令之前 IC 卡需要拥有鉴别数据

图 43

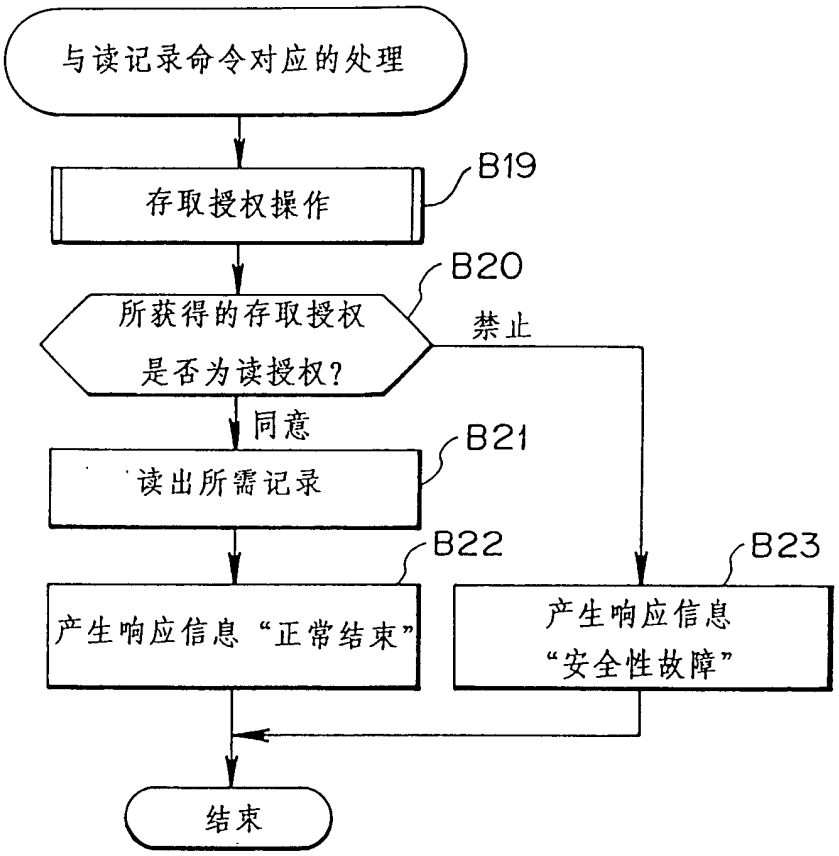

与读记录命令对应的处理
存取授权操作
B19
所获得的存取授权
是否为读授权?
B20
禁止
同意
读出所需记录
B21
产生响应信息“正常结束”
B22
产生响应信息
“安全性故障”
B23
结束

图44

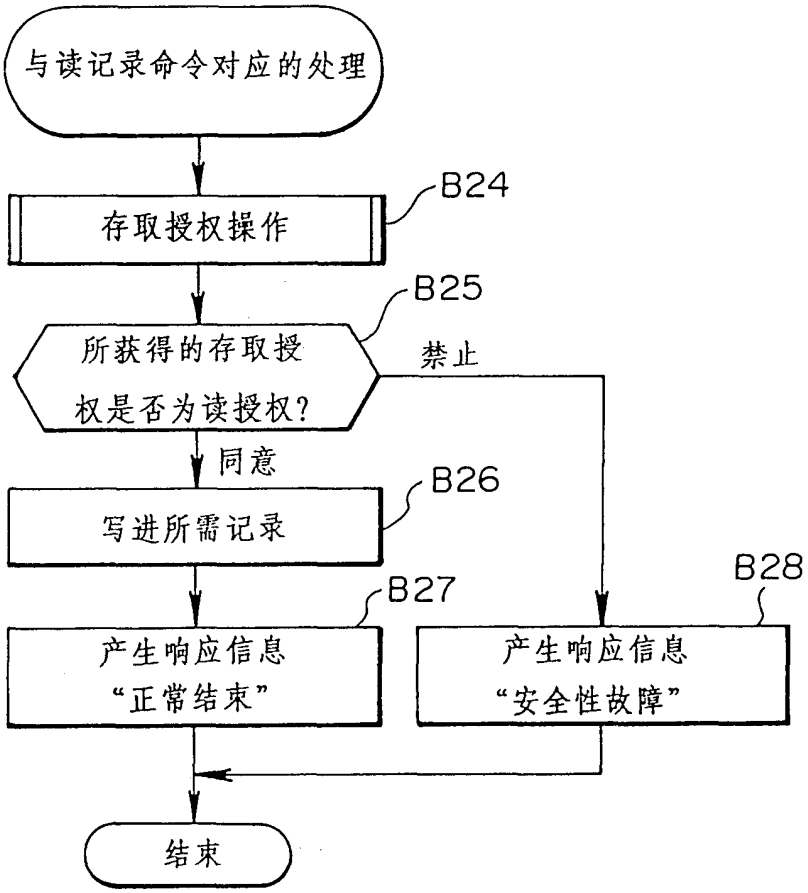
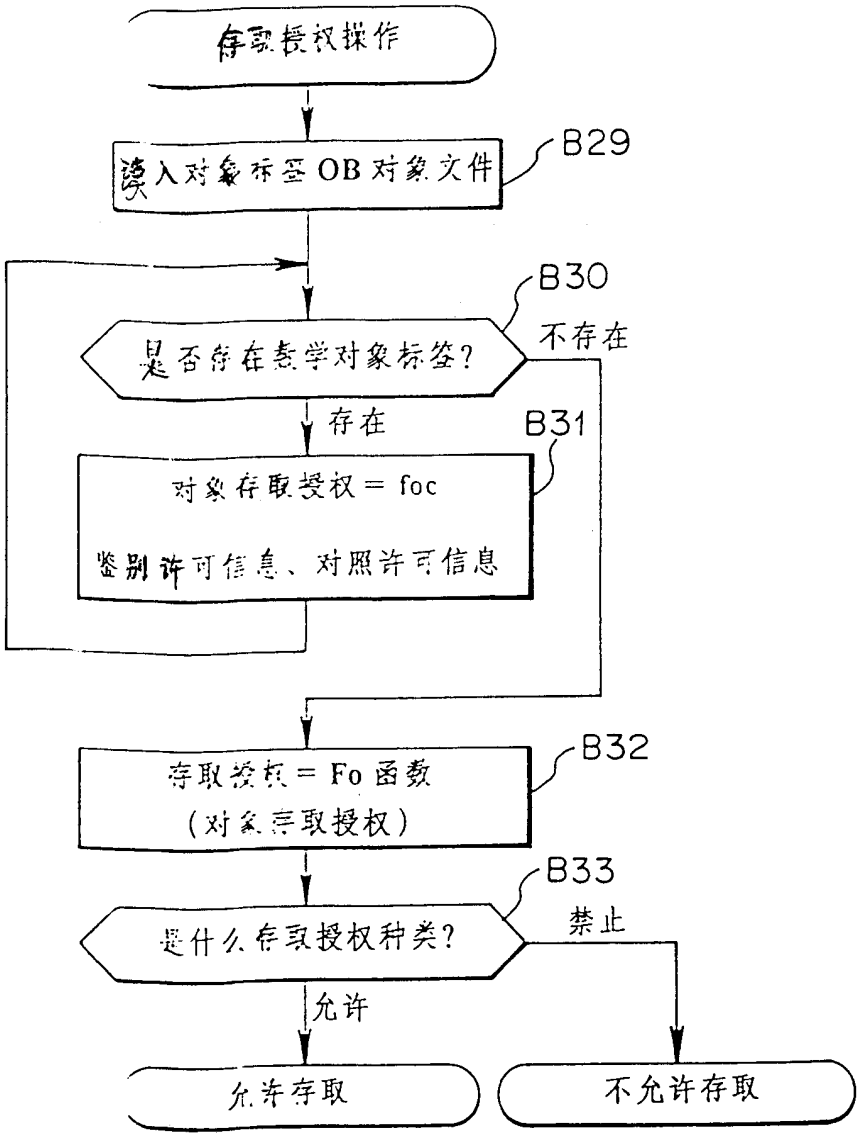

与读记录命令对应的处理
B24
存取授权操作
B25
所获得的存取授权是否为读授权?
禁止
同意
B26
写进所需记录
B27
产生响应信息“正常结束”
B28
产生响应信息“安全性故障”
结束

图 45


存取授权操作
读入对象标签 OB 对象文件
B29
是否存在该学对象标签?
B30
不存在
存在
B31
对象存取授权 = foc
鉴别许可信息、对照许可信息
存取授权 = Fo 函数
(对象存取授权)
B32
是什么存取授权种类?
B33
禁止
允许
允许存取
不允许存取

客户机 103A
密码号“ a ”

客户机 103B
密码号“ a,c ”

客户机 103C
密码号“ a,b ”

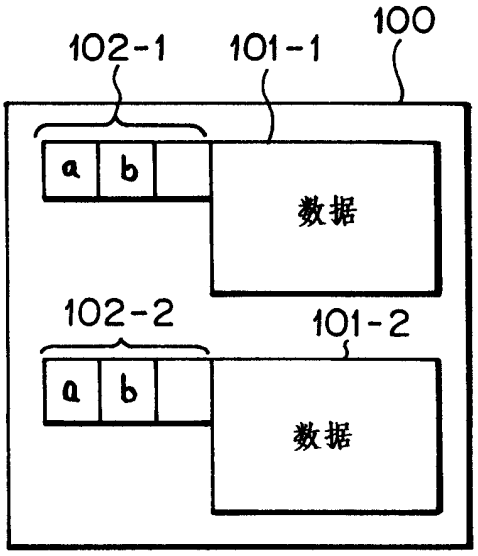


图46(a)
现有技术

客户机 103A
密码号“ a,d ”

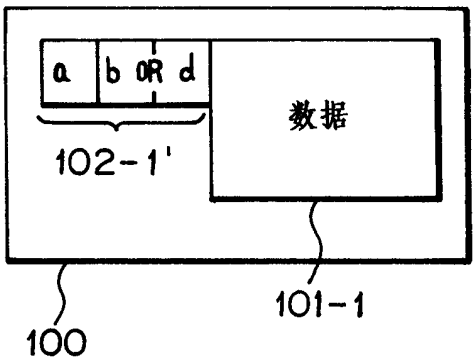


图46(b)
现有技术

图 47

现有技术