[19]中华人民共和国专利局

[51]Int.Cl[6]
G06F 13/14

[12] 发明专利申请公开说明书

[21] 申请号 97110316.X

[43]公开日 1998 年 2 月 25 日

[11] 公开号 CN 1174355A

[22]申请日 97.3.31

[30]优先权

[32]96.3.29 [33]JP[31]076200/96

[32]96.9.30 [33]JP[31]278877/96

[71]申请人 东芝株式会社

地址 日本神奈川

[72]发明人 饭岛康雄

[74]专利代理机构 上海专利商标事务所

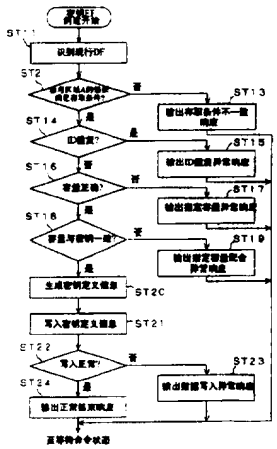
代理人 方晓虹

权利要求书 4 页 说明书 13 页 附图页数 13 页

[54]发明名称 文件管理方法

[57]摘要

一种文件管理方法，包括：设定具有多个存储区域的可携带存储媒体的口令的工序、判断口令是否已变更的判断工序、当判断口令未变更时禁止对所述多个存储区域进行处理的工序、当判断口令发生变更时能够根据给出的命令对所述多个存储区域进行处理的工序。采用本发明，在媒体的口令由上级向下级移交后，只要下级不变更该口令，其效力便不能发挥，故安全性好。



权　利　要　求　书

1.一种文件管理方法，其特征在于，包括:

设定具有多个存储区域(12)的可携带存储媒体(1)的密钥数据的工序(11 、 S103);

判断所述存储媒体的密钥数据是否已变更的判断工序(11 、 S109);

当所述判断工序判断密钥数据未变更时，禁止对所述多个存储区域进行处理的工序(11 、 S113);

当所述判断工序判断密钥数据发生变更时，能够根据给出的命令对所述多个存储区域进行处理的工序(11 、 S111)。

2.根据权利要求 1 所述的文件管理方法，其特征在于，还包括，

当所述判断工序判断密钥数据未变更时，根据给出的命令把所述密钥数据变更为新密钥数据的工序(11 、 S107)。

3.根据权利要求 1 所述的文件管理方法，其特征在于，还包括，

无论所述判断工序判断如何、根据给出的命令对所述多个存储区域实行处理的、切换成通常工作模式的工序(11)。

4.根据权利要求 1 所述的文件管理方法，其特征在于，还包括，

在密钥数据中设定表示通常工作模式的属性信息的工序(11);

当所述密钥数据含有所述属性信息时，无论所述判断工序的判断如何、根据给出的命令对所述多个存储区域实行处理的工序(11)。

5.根据权利要求 1 所述的文件管理方法，其特征在于，

所述实行工序是根据给出的命令在所述存储区域创建数据文件的工序（图 7），且在密钥变更前通过禁止工序而实行禁止。

6.根据权利要求 1 所述的文件管理方法，其特征在于，

所述实行工序是根据给出的命令在所述存储区域创建密钥数据文件的工序（图 8），且在密钥变更前通过禁止工序而实行禁止。

7.根据权利要求 6 所述的文件管理方法，其特征在于，

所述实行工序是根据给出的命令在所述存储区域的密钥数据文件中设定密钥数据的工序（图 9），且在密钥变更前通过禁止工序而实行禁止。

8.一种具有多个存储区域的可携带存储媒体，其特征在于，包括:

在多个存储区域(12)存储密钥数据和数据的手段(11 、 12);

判断所述存储手段存储的所述密钥数据是否已变更的手段(11 、 S109);

当所述判断手段判断密钥数据未变更时，禁止对所述多个存储区域进行处理的手段(11 、 S113);

当所述判断手段判断密钥数据发生变更时，能够根据给出的命令对所述多个

存储区域进行处理的手段(11 、 S111)。

9.根据权利要求 8 所述的可携带存储媒体，其特征在于，还包括，

当所述判断手段判断密钥数据未变更时，根据给出的命令把所述密钥数据变更为新密钥数据的手段(11 、 S107)。

10.根据权利要求 8 所述的可携带存储媒体，其特征在于，还包括，

无论所述判断手段的判断如何、根据给出的命令对所述多个存储区域实行处理的、切换成通常工作模式的手段(11)。

11.根据权利要求 8 所述的可携带存储媒体，其特征在于，还包括，

把具有表示通常工作模式的属性信息的密钥数据进行存储的手段(11 、12);

当所述密钥数据含有所述属性信息时，无论所述判断手段的判断如何、根据给出的命令对所述多个存储区域实行处理的手段(11)。

12.根据权利要求 8 所述的可携带存储媒体，其特征在于，

所述实行手段是根据给出的命令在所述存储区域创建数据文件的手段（ 11 、图 7 ），且在密钥变更前通过禁止手段而禁止数据文件的创建。

13.根据权利要求 8 所述的可携带存储媒体，其特征在于，

所述实行手段是根据给出的命令在所述存储区域创建密钥数据文件的手段（ 11 、图 8 ），且在密钥变更前通过禁止手段而禁止密钥数据文件的创建。

14.根据权利要求 13 所述的可携带存储媒体，其特征在于，

所述实行手段是根据给出的命令在所述存储区域的密钥数据文件中设定密钥数据的手段（ 11 、图 9 ），且在密钥变更前通过禁止手段而禁止密钥数据的设定。

15.一种存储器的存取管理方法，是把存储器划分为多个文件，并分别对该划分的多个文件的存取进行管理，由使用该存储器的系统的上级在文件属下预先设定第 1 密钥，使用该存储器的系统的下级可重新设定密钥，且通过这些密钥的对照使能够向所述文件进行存取，

其特征在于，参考在所述第 1 密钥中设定的密钥变更用存取条件，把所述上级设定的第 1 密钥变更为只有下级可知的第 2 密钥，在变更为该第 2 密钥后，拒绝所述上级在文件属下创建密钥。

16.一种文件存取管理方法，对由上级文件和下级文件构成的树结构文件的存取进行管理，其特征在于，

对上级管理者对管理的上级文件设定存取条件，

在从上级管理者向下级管理者提供的文件中设定存取条件，

当在下级文件中设定从上级管理者向下级管理者移交用的移交密钥的场合，参考该文件的上级文件的存取条件，

在满足该上级文件的存取条件的场合，在下级文件中设定移交密钥，

当在下级文件的属下设定文件的场合，参考该下级文件的存取条件，在满足该存取条件的场合，进行文件的设定。

17.根据权利要求 16 所述的文件存取管理方法，其特征在于，对所述下级文件给与表示可否设定移交密钥的识别信息，根据该识别信息禁止设定针对该文件的移交密钥。

18.根据权利要求 17 所述的文件存取管理方法，其特征在于，在针对所述下级文件的移交密钥变更的场合，更新所述识别信息，以便以后禁止设定针对该文件的移交密钥。

19.根据权利要求 17 所述的文件存取管理方法，其特征在于，表示可否在所述下级文件中设定移交密钥的识别信息根据特殊命令更新。

20.根据权利要求 16 所述的文件存取管理方法，其特征在于，对所述下级文件设定移交密钥是根据移交密钥设定用命令进行，当在所述下级文件的属下设定文件的场合，根据与移交密钥设定用命令不同的命令进行。

21.一种可携带信息处理装置，具有由上级文件和下级文件构成的树结构文件，其特征在于，具有:

设定存取条件、由上级管理者利用的上级文件，

设定存取条件、由上级管理者提供、下级管理者利用的下级文件，

当参考上级文件的存取条件且满足该上级文件的存取条件的场合，在下级文件中设定从上级管理者向下级管理者移交用的移交密钥的第 1 手段，

当参考该下级文件的存取条件且满足该存取条件的场合，在下级文件的属下设定文件的第 2 手段。

22.根据权利要求 21 所述的可携带信息处理装置，其特征在于，在所述下级文件中具有表示可否设定移交密钥的识别信息的存储区域，且具有根据该识别信息禁止设定针对该文件的移交密钥的手段。

23.根据权利要求 21 所述的可携带信息处理装置，其特征在于，具有在针对所述下级文件的移交密钥变更的场合更新所述识别信息、以便以后禁止设定针对该文件的移交密钥的手段。

24.根据权利要求 21 所述的可携带信息处理装置，其特征在于，所述可携带信息存储媒体根据从外部装置供给的命令工作，

表示可否在所述下级文件中设定移交密钥的识别信息具有根据外部装置供给的特殊命令进行更新的手段。

25.根据权利要求 21 所述的可携带信息处理装置，其特征在于，所述可携带信息存储媒体根据从外部装置供给的命令工作，

用所述第 1 手段对所述下级文件设定移交密钥是根据移交密钥设定用的命令进行工作，用所述第 2 手段在所述下级文件的属下设定文件是根据与移交密钥设定用的命令不同的命令进行工作。

26.一种存储信息处理装置用控制程序的媒体，是创建由上级文件和下级文件构成的树结构文件、存储通过控制手段进行各文件存取管理的信息处理装置用控制程序的、计算机可读出的存储媒体，其特征在于，

所述控制程序使所述控制手段进行以下步骤：

创建由上级管理者设定存取条件的上级文件的步骤，

创建由上级管理者提供、为下级管理者利用而设定存取条件的下级文件的步骤，

在参考上级文件的存取条件且满足该上级文件存取条件的场合、在下级文件中设定从上级管理者向下级管理者移交用的移交密钥的步骤，

在参考下级文件的存取条件且满足该存取条件的场合、在下级文件的属下设定文件的步骤。

27.根据权利要求 26 所述的存储媒体，其特征在于，存储所述信息处理装置用控制程序的程序存储器、被分配了所述文件的数据存储器、对该文件进行存取管理的控制电路、及与外部装置之间的接口在 1 个模块中构成。

说　明　书

文件管理方法

本发明涉及在内装具有譬如非易失性存储器、及对其进行控制的 CPU 等控制元件的 IC 芯片的 IC 卡中，对上述存储器内划分设定的多个文件进行管理的文件管理方法。

最近，作为可携带的存储媒体，内装具有非易失性存储器、及对其进行控制的 CPU（中央处理单元）等控制元件的 IC 芯片的 IC 卡倍受注目。

这种 IC 卡把内装的数据存储器划分为多个文件，且各个文件中存储着用户应用时所必要的数据等，通过从外部装置输入应用识别名等，使只有所选择的对应文件能够使用。因此，通过把多个应用数据进行文件划分，并存储于 1 片 IC 卡上，即可用于多个目的。

这些应用文件可以包括用于交易数据等数据存储的多个数据文件和用于密钥数据存储的密钥文件。

另外，在最新的 IC 卡中，对各文件附加了称为存取条件的信息，通过对照该信息所指示的卡内密钥（口令）而判定可否进行命令存取。

这类 IC 卡在从制造者转移到用户的过程中，可以想象有卡片的发行处理/卡内的系统基本信息存储等各种工序。并且可以想象与各工序有关的当事人也不一样。

譬如，前者是卡片发行者（上级），后者是使用者（下级）。在卡片发行者向使用者移交卡片存取的权限时，一般是在 IC 卡上设定称为“移交密钥”的临时密钥（口令），使用者与其进行对照，以后，使用者便可对 IC 卡进行存取。

在这种场合，一旦为了只使使用者进行文件内的管理而设定该文件的存取条件，由于为发行者设定使用者用移交密钥所必须满足的使用者密钥不存在，故发行者不能永久设定该移交密钥。

为了避免这一点，作为给予该文件的存取条件，考虑设定使用者密钥或发行者密钥。

即，只要按以下状态设定存取条件即可：当发行者在该文件上设定使用者用移交密钥的场合，通过对照发行者密钥来满足存取条件，另一方面，在使用者进行该文件内的其他管理行为的场合，通过对照自身的使用者密钥而满足存取条件。

然而，在这种场合，在该文件中设定的存取条件可由发行者与使用者双方进行存取，不能说对该文件的管理权限已从发行者（上级）移交给了使用者（下级）。

而且，对于该移交密钥（口令），卡片发行者是已知的，故为了做到只有使

用者自身知道该密钥，一般是通过对照该移交密钥而将其进行重写。

然而，采用上述现有技术，在更改 IC 卡内的数据时，会使其问题的解决复杂化。譬如，考虑到 IC 卡内的应用的有效期限一般是通过对照使用者的密钥（口令）而变更的，在临时更改该数据时，就会追究使用者的责任。

然而，如果该使用者不变更前述的移交密钥即加以利用，则卡片发行者即可进行与使用者同等的处理。即，数据的更改虽然是由于使用者的不注意引起的，却会使卡片发行者同时受到怀疑。

从而，运用移交密钥的本来目的、即“对 IC 卡管理权限的移交”不能完全实现。

另一方面，附加了重写移交密钥义务，且使其在 IC 卡内进行一义性检验的方法对于只要求 IC 卡便利性的应用是不现实的方法。

本发明的目的在于提供一种在把媒体等的移交密钥（口令）从上级移交到下级后，只要下级不变更该密钥，其效力便不会发挥，安全性好的文件管理方法及使用该方法的媒体。

本发明的技术方案是一种文件管理方法，包括：设定具有多个存储区域 12 的、可携带存储媒体 1 的口令的工序 11 、 S103；把所述存储媒体现在的口令与在所述设定工序中设定的所述口令进行比较、判断口令是否已变更的判断工序 11 、 S109；当所述判断工序判断口令未变更时，禁止对所述多个存储区域进行处理的工序 11 、 S113；当所述判断工序判断口令发生变更时，根据给出的命令对所述多个存储区域实行处理的工序 11 、 S111 。

本发明的再一技术方案是一种具有多个存储区域的可携带存储媒体，使用上述的方法，其包括：在多个存储区域 12 存储口令和数据的手段 11 、 12；把给出的起始口令与所述存储手段存储的所述口令进行比较并判断口令是否变更的手段 11 、 S109；当所述判断手段判断口令未变更时，禁止对所述多个存储区域进行处理的手段 11 、 S113；当所述判断手段判断口令发生变更时，根据对所述多个存储区域给出的命令实行处理的工序 11 、 S111 。

本发明通过上述顺序，只要不变更 IC 发行者（上级）所定的密钥（口令），IC 卡的使用者（下级）就不能在存储区域进行写入应用等处理。

因而，由于使用者必定要在密钥变更后进行处理，故可以完全实现管理权限的移交，因此可提供提高安全性的文件管理方法及其媒体装置。

对附图的简单说明

图 1 是表示使用本发明实施形态的 IC 卡的卡片处理装置构成示例的方框图。

图 1B 是表示本发明动作特征的流程图。

图 2 是表示 IC 卡构成示例的方框图。

图 3 是表示数据存储器构成示例的存储空间分配图。

图 4 表示各种定义信息的格式示例。

图 5 表示在数据存储器内设定的文件构造示例。

图 6 表示在数据存储器内设定的目录构造示例。

图 7 是说明创建数据文件的动作的流程图。

图 8 是说明创建密钥基本文件的动作的流程图。

图 9 是说明设定密钥数据的动作的流程图。

图 10 是说明变更密钥数据的动作的流程图。

图 11 是说明对照密钥的动作的流程图。

图 12 是说明对数据基本文件进行存取的动作的流程图。

以下结合附图说明本发明的实施形态。

图 1 表示使用本实施形态的可携带电子装置、即 IC 卡的譬如作为金融系统或购物系统等的终端装置使用的卡片处理装置的构成示例。即，该装置可经过卡片读写机 2 把 IC 卡 1 与由 CPU 等构成的控制部 3 连接，同时把键盘 4 、 CRT 显示装置 5 、打印机 6 及软盘装置 7 与控制部 3 连接。

图 2 表示 IC 卡 1 的构成示例，由作为控制部的控制元件（譬如 CPU ） 11 、可消除存储内容的非易失性数据存储器 12 、工作存储器 13 、程序存储器 14 、及为得到与卡片读写机 2 间的电气接触用的接触部 15 构成。其中，虚线内部分（控制元件 11 、数据存储器 12 、工作存储器 13 、程序存储器 14 ）用 1 个（或多个） IC 芯片构成，且如日本实用新型公开 1990-17381 号公报所公开的， IC 芯片 10 与接触部 15 被制成一体化 IC 模块后设置在 IC 卡本体内部。

数据存储器 12 用于各种数据的存储，譬如用 EEPROM 等构成。工作存储器 13 是将控制元件 11 进行处理时的处理数据加以临时保存用的存储器，譬如用 RAM 等构成。程序存储器 14 譬如用屏蔽 ROM 构成，是用于存储控制元件 11 的程序等的。

执行后述图 7 至图 13 各子程序的程序存储在程序存储器 14 内。

数据存储器 12 ，如图 3 所示，划分成控制区域 120 、目录 121 、空白区域 122 、及区域群 123 。区域群 123 可以具有多个数据区域及密钥区域，且可用称为数据文件（ DF ）的概念组合化。另外，后述的主文件（ MF ）作为数据文件的 1 个形态被统一管理。

数据文件是对对应的应用所用的数据区域及密钥区域进行汇总管理用的文件。

数据区域，是将譬如交易数据一类根据需要而进行读写用的数据进行存储的区域。

密钥区域是用于存储譬如密码等的区域，成为写入/重写/对照的对象，不能读出。

另外，这些区域如图 3 所示，作为区域群 123 而被统一分配。又，这些文件

或区域通过使用数据存储器 12 内的目录 121，使控制元件 11 识别各自的物理位置。

以下用图 1B 的表示本发明动作特征的流程图说明本发明的文件管理方法的概要。

在图 1B 的流程图中，使用该方法的譬如 IC 卡等媒体由 IC 卡发行者作成文件(S101)，而且 IC 卡发行者在该媒体上设定移交密钥（口令）(S103)。

而且该 IC 卡被移交给在 IC 卡的文件上作成应用并加以存储的使用者。

使用者在 IC 阅读机上安装 IC 卡并输入移交密钥进行对照(S105)，对 IC 卡进行存取。接着把移交密钥（口令）变更为使用者专用的(S107)。这样，用以前的移交密钥便不能进行存取，管理权限便从 IC 卡发行者完全地移交给使用者。一旦确认移交密钥已变更(S109)，即可根据给出的命令进行数据文件创建处理（图 7）、密钥基本文件创建处理（图 8）、密钥数据设定处理（图 9）、对基本文件的存取（图 12）等处理。

另一方面，如果移交密钥未变更，即使输入原来的 IC 卡发行者设定的移交密钥，与命令对应的上述各项处理也不会执行。从而，一旦发生移交密钥变更后的文件重写等的故障，其责任在于将移交密钥重写的使用者。

不过，即使在移交密钥变更以前，也只可执行变更移交密钥的处理。

通过使用这种方法，可以完全妥善地实现 IC 卡等文件的管理权限在 IC 卡发行者（上级）和使用者（下级）之间的移交。

在图 3 的控制区域 120，存储着区域群 123 的起始地址信息及空白区域 122 的起始地址信息。

图 3 的目录 121 如图 4 所示，存储着与各数据文件及区域对应的各种定义信息。

图 4 的信息 201 是对数据文件的名称定义的信息。该定义信息由在目录 121 内识别数据文件名定义信息用的数据 PTN、分配给本数据文件的文件序列号 DFSN、本数据文件的主文件的序列号 PFSN、对本数据文件给出的文件名 DFname 及表示其长度的数据 NL、及对这些数据的正确性进行检验用的数据 BCC 构成。

图 4 的信息 202 是对数据文件的管理信息定义的信息。该定义信息由在目录 121 内识别数据文件名定义信息用的数据 PTN、分配给本数据文件的文件序列号 DFSN、本数据文件的主文件的序列号 PFSN、数据文件容量 DFS、对识别存储本数据文件附加信息的数据区域用的 AAID 附加信息是否输出等作规定的 TYPE、禁止密钥的分类的 UCF、表示数据文件的存取条件的 DFAC、保持本数据文件状态用的 DFST、被位于本数据文件属下的数据文件及区域所用的字节数 US、以及检验这些数据正确性用的数据 BCC 构成。

这里，DFST 的特定位（例如第 8 位）作为表示该 DF 的移交密钥是否变更的移交位使用。

另外，特别是 AAID，在用后述的数据文件选择命令选择了数据文件时，根据需要而输出其中表示的数据区域的内容。

图 4 的信息 203 是对存储各种交易数据等的区域定义的信息。该定义信息由在目录 121 内识别区域定义信息用的数据 PTN、本区域所属的数据文件的序列号 DFSN、对区域进行存取时的识别号 AID、表示区域起始地址的 ATOP、表示区域容量的 ASIZ、表示区域存取条件的 AAC、保持区域状态的 AST、以及检验这些数据正确性用的数据 BCC 构成。

图 4 的信息 204 是对存储各种密钥数据的区域定义的信息。该定义信息由在目录 121 内识别密钥区域定义信息用的数据 PTN、本区域所属的数据文件的序列号 DFSN、对区域进行存取时的识别号 KID、表示区域起始地址的 KTOP、表示区域容量的 KSIZ、表示密钥的分类的 CF、表示密钥的存取条件的 KAC、保持密钥状态的 KST、以及检验这些数据正确性用的数据 BCC 构成。

其中所用的识别信息 PTN 用譬如 1 字节构成，对给数据文件名称定义的信息 201 用 '00'，对给数据文件的管理信息定义的信息 202 用 '01'，对给数据区域定义的信息 203 用 '02'，对给密钥区域定义的信息 204 用 '03'。

图 5 表示文件的构造示例。在该图中，DFnn 表示数据文件，Dnn 表示数据区域，Knn 表示密钥区域。

如图所示，在 IC 卡 1 内的存储器 12 中，在主文件（MF）的属下，分别设定数据文件 DF1、DF2 及密钥区域 K00、K01、数据区域 D00、D01。

在数据文件 DF1 的属下，分别设定数据文件 DF1 - 1、DF1 - 2 及密钥区域 K11、K12、数据区域 D11、D12。

在数据文件 DF1 - 1 的属下，分别设定密钥区域 K111、K112、数据区域 D111/D112，在数据文件 DF1 - 2 的属下，分别设定密钥区域 K121、K122、数据区域 D121、D122。

在数据文件 DF2 的属下，分别设定数据文件 DF2 - 1、DF2 - 2 及密钥区域 K21、K22、数据区域 D21、D22。

在数据文件 DF2 - 1 的属下，设定密钥区域 K211、K212、数据区域 D211、D212，在数据文件 DF2 - 2 的属下，设定密钥区域 K221、K222、数据区域 D221、D222。

上述各种定义信息如图 6 所示，成批存储于目录 121 中。如图所示，在各定义信息中，DFSN（文件序列号）在文件创建时即自动给出。根据该 DFSN 及存储在数据文件定义信息中的主文件序列号，控制元件 11 识别各文件的相关状态。

譬如，数据文件 DF1 - 1 的定义信息（序列号 # 13）为：DFSN 是 '03'，PFSN 是 '01'。即，本数据文件的文件序列号 '03' 是在创建时给出，同时知道本数据文件创建于 DF1 的属下，并把数据文件 DF1 的 DFSN（'01'）作为 PFSN 给出。

图 7 是说明创建数据文件（ DF ）用的动作的流程图，以下就该图进行说明。IC 卡 1 一旦收到从外部输入的数据文件创建命令，首先识别可使用状态、即成为现行状态的数据文件（以下称现行 DF ）（ ST1 ）。特别是在对 IC 卡 1 作电激活后，现行 DF 立即成为主文件（ MF ）。

一旦识别了现行 DF，接着参考现行 DF 定义信息的存取条件信息中有关文件创建的信息。把该条件只与后述的 RAM 上的对照状态保持区域 A 进行比较，判断是否确立了存取条件所要求的密钥（口令）的对照状态（ ST2 ）。

如果没有确立，即输出表示存取条件不一致的响应显示信息，并返回到等待命令状态（ ST3 ）。如果确立了，接着把设定在命令内的数据文件的文件名（ DF - ID ）抽出，主 FSN 拥有与现行 DF 具有的 FSN 相同的值，进而确认是否存在文件名与抽出的文件名相同的数据文件定义信息（ ST4 ）。

如果存在，即输出表示 ID 重复异常的响应显示信息，并返回到等待命令状态（ ST5 ）。如果不存在，则根据命令所给出的创建数据文件用的数据，生成图 4 所示的数据文件定义信息（ ST6 ），并将其写入规定区域（ ST7 ）。

在该写入中，当写入未正常结束时（ ST8 ），输出表示数据写入异常的响应显示信息，并返回到等待命令状态（ ST9 ）。而当写入正常结束时（ ST8 ），输出表示正常结束的响应显示信息，并返回到等待命令状态（ ST10 ）。

图 8 是说明创建密钥基本文件（ EF ）的动作的流程图，以下就该图进行说明。 IC 卡 1 一旦收到从外部输入的密钥 EF 创建命令，首先识别现行 DF （ ST11 ）。

一旦识别了现行 DF，接着参考现行 DF 定义信息的存取条件信息中有关文件创建的信息。把该条件只与后述的 RAM 上的对照状态保持区域 A 进行比较，判断是否确立了存取条件所要求的密钥（口令）的对照状态（ ST12 ）。

如果没有确立，即输出表示存取条件不一致的响应显示信息，并返回到等待命令状态（ ST13 ）。如果确立了，即参考命令显示信息指示的基本文件名（ EF - ID ），在成为存取对象的现行 DF 内，检验该基本文件名是否存在（ ST14 ）。如果存在，即输出表示 ID 重复异常的响应显示信息，并返回到等待命令状态（ ST15 ）。

如果不存在，则参考命令显示信息所指定的密钥 EF 的容量数据，与成为存取对象的现行 DF 内的空白区域容量进行比较（ ST16 ）。在该比较中，在指定的密钥 EF 容量上加上创建该密钥 EF 时使用的目录信息的容量，然后检验前述空白区域容量是否超过该值。在前者大于后者的场合，输出表示指定容量异常的响应显示信息，并返回到等待命令状态（ ST17 ）。

如果不是那样，接着检验命令显示信息指定的密钥类型和容量的正确性（ ST18 ）。这时，当密钥类型成为“认证相关密钥”时容量譬如是 10 字节时，或是当密钥类型成为“对照密钥”时容量譬如是 3 ~ 18 字节时，则判断容量为

正确。在判断为不正确的场合，输出表示指定容量配合异常的响应显示信息，并返回到等待命令状态（ ST19 ）。

这里，当判断容量为正确时，根据收到的命令，生成应存储于目录中的密钥 EF 定义信息（ ST20 ），并把其写入规定区域（ ST21 ）。这时，状态信息的第 8 位根据命令显示信息所指定的密钥类型信息中的第 1 位而决定其值。即，在前者的位中设定与后者的位值同样的值。

该状态信息的第 8 位是表示密钥数据是否已变更的位，当该位为“ 1 ”时，表示变更行为未实施，而当其为“ 0 ”时则表示该行为已实施。

从而，当上述密钥类型信息的第 1 位为“ 1 ”时，只要密钥变更未进行，则状态信息的第 8 位不会成为“ 0 ”，另外，在“ 0 ”的场合，无论密钥变更是否进行，状态信息的第 8 位都变成“ 0 ”（即，与重写行为在暗中进行相同）。

在上述密钥 EF 信息的写入中，当写入未正常结束时（ ST22 ），输出表示数据写入异常的响应显示信息，并返回到等待命令状态（ ST23 ）。而当写入正常结束时（ ST22 ），输出表示正常结束的响应显示信息，并返回到等待命令状态（ ST24 ）。

图 9 是说明设定密钥数据的动作的流程图，以下就该图进行说明。 IC 卡 1 一旦收到从外部输入的密钥数据设定命令，首先识别现行 DF （ ST31 ）。

一旦识别了现行 DF ，接着参考命令显示信息所指示的基本文件名（ EF - ID ），并在成为存取对象的现行 DF 内检验该基本文件名是否存在（ ST32 ），如果不存在，则输出表示该密钥 ID 不存在的响应显示信息，并返回到等待命令状态（ ST33 ）。

如果存在，接着参考该密钥 EF 定义信息的存取条件信息中有关密钥数据设定的信息。把该条件只与后述的 RAM 上的对照状态保持区域 A 进行比较，判断是否确立了存取条件所要求的密钥的对照状态（ ST34 ）。

如果没有确立，即输出表示存取条件不一致的响应显示信息，并返回到等待命令状态（ ST35 ）。如果确立了，接着在对应的密钥 EF 区域内确认密钥数据是否存在（ ST36 ）。如果存在，即输出表示已有密钥数据存在的响应显示信息，并返回到等待命令状态（ ST37 ）。

如果不存在，则检验命令显示信息指定的密钥类型和输入密钥数据容量的正确性（ ST38 ）。这时，当密钥类型成为“认证相关密钥”时容量譬如是 8 字节时，或是当密钥类型成为“对照密钥”时容量譬如是 1 ~ 16 字节时，判断容量为正确。在判断为不正确的场合时，输出表示密钥数据容量异常的响应显示信息，并返回到等待命令状态（ ST39 ）。

这里，在判断容量为正确的场合，接着把该密钥 EF 定义信息中所定义的容量与输入的密钥数据的容量进行比较（ ST40 ）。当在后者的容量中譬如加上“ 2 ”后大于前者容量时，输出表示区域容量不足的响应显示信息，并返回到等

待命令状态（ ST41 ）。

如果不是那样，则在用收到的命令输入的密钥数据中加上 1 字节长的信息及 1 字节的 BCC，将其存入该密钥 EF 区域（ ST42 ），用响应显示信息输出其处理结果，并返回到等待命令状态（ ST43 ）。

图 10 是说明变更密钥数据的动作的流程图，以下就该图进行说明。IC 卡 1 一旦收到从外部输入的密钥数据变更命令，首先识别现行 DF （ ST51 ）。

一旦识别了现行 DF，接着参考命令显示信息所指示的基本文件名（ EF - ID ），并在成为存取对象的现行 DF 内检验该基本文件名是否存在（ ST52 ），如果不存在，则输出表示该密钥 ID 不存在的响应显示信息，并返回到等待命令状态（ ST53 ）。

如果存在，接着参考该密钥 EF 定义信息的存取条件信息中有关密钥变更的信息。把该条件只与后述的 RAM 上的对照状态保持区域 A 和 B 进行比较，判断是否确立了存取条件所要求的密钥的对照状态（ ST54 ）。

如果没有确立，即输出表示存取条件不一致的响应显示信息，并返回到等待命令状态（ ST55 ）。如果确立了，接着在对应的密钥 EF 区域内确认密钥数据是否存在（ ST56 ）。如果不存在，即输出表示已有密钥数据不存在的响应显示信息，并返回到等待命令状态（ ST57 ）。

如果存在，则检验命令显示信息指定的密钥类型和输入密钥数据容量的正确性（ ST58 ）。这时，当密钥类型成为“认证相关密钥”时容量譬如是 8 字节时，或是当密钥类型成为“对照密钥”时容量譬如是 1 ~ 16 字节时，判断容量为正确。在判断为不正确的场合，输出表示密钥数据容量异常的响应显示信息，并返回到等待命令状态（ ST59 ）。

这里，在判断容量为正确的场合，接着把该密钥 EF 定义信息中所定义的容量与输入的密钥数据的容量进行比较（ ST60 ）。当在后者的容量中譬如加上“ 2 ”后大于前者容量时，输出表示区域容量不足的响应显示信息，并返回到等待命令状态（ ST61 ）。

如果不是那样，则在用收到的命令输入的密钥数据中加上 1 字节长的信息及 1 字节的 BCC，将其存入该密钥 EF 区域（ ST62 ），用响应显示信息输出其处理结果，并返回到等待命令状态（ ST63 ）。另外，这时把处于密钥 EF 定义信息中的状态信息第 8 位置为“ 0 ”（ ST64 ）。

图 11 是说明对照密钥的动作的流程图，以下就该图进行说明。IC 卡 1 一旦收到从外部输入的密钥对照命令，首先识别现行 DF （ ST71 ）。

一旦识别了现行 DF，接着通过对目录 121 进行检索，在现行 DF 内确认具有指定的文件名（ ID ）的密钥 EF 定义信息是否存在（ ST72 ）。如果不存在，则输出表示该密钥 ID 不存在的响应显示信息，并返回到等待命令状态（ ST73 ）。

如果存在，即确认该密钥是否成为锁定状态（ ST74 ）。这时，在判断为锁定

状态的场合，即输出表示密钥锁定的响应显示信息，并返回到等待命令状态（ST75）。

如果不是那样，即把命令显示信息内的密钥数据与该密钥 EF 内存储的密钥数据进行对照（ST76）。这时，在两者一致的场合（ST77），参考该密钥 DF 定义信息中的对照位指定信息，在位变更前把 B 区域的、在位变更后把 A 区域的由该信息指定的位置为“1”（ST78）。接着，把该密钥 EF 定义信息中的密钥固有的对照不一致计数器清零（ST79），输出表示正常结束的响应显示信息，并返回到等待命令状态（ST80）。

另外规定的 RAM 区域被划分成对照状态保持区域 A 及 B。把哪个区域的对应位置为“1”取决于该密钥 EF 定义信息中密钥状态信息的第 8 位的值。该位表示是否对根据该密钥 EF 信息定义的密钥进行过变更处理，如后所述，它表示如果成为“0”就是变更后的密钥，如果成为“1”就是未经变更处理的密钥。当其成为“0”时，即设定前述对照状态保持区域 A 的对应位，如果成为“1”，则设定前述对照状态保持区域 B 的对应位。

另外，在密钥对照处理中，在判断为不一致的场合（ST77），首先参考该密钥 EF 定义信息中的对照位指定信息及状态信息，按照与上述相同的顺序把对照状态保持区域 A 或 B 中任一区域的规定位置为“0”（ST81）。

接着，将密钥固有的对照不一致计数器只增值 1（ST82）。这时，当未达到密钥 EF 定义信息中的计数器最大值时（ST83），输出表示对照不一致的响应显示信息，并返回到等待命令状态（ST84）。当达到最大值时，输出表示密钥锁定完毕的响应显示信息，并返回到等待命令状态（ST85）。

文件创建时、密钥 EF 创建时、密钥数据创建时、密钥数据变更时参考对照状态保持区域 A，对照状态保持区域 B 则在密钥数据变更时被参考。

如上所述，在密钥变更完毕的场合，如果对照状态保持区域 A 未变更，则对照状态保持区域 B 的位置 1，故在文件创建时，密钥 EF 创建时及密钥数据创建时，密钥必须变更完毕。另外，在密钥变更时要参考对照状态保持区域 A 及 B，故无论密钥变更完毕或是未变更，都可进行密钥的变更。

图 12 是说明对数据基本文件进行存取的动作的流程图。以下就该图进行说明。IC 卡 1 一旦收到从外部输入的数据 EF 存取命令，首先识别现行 DF（ST91）。

一旦识别了现行 DF，接着参考命令显示信息所指示的基本文件名（EF－ID），并在成为存取对象的现行 DF 内检验该基本文件名是否存在（ST92），如果不存在，则输出表示该密钥 ID 不存在的响应显示信息，并返回到等待命令状态（ST93）。

如果存在，接着参考数据 EF 定义信息的存取条件信息中与存取的类型（数据读出/写入/变更）对应的存取条件信息。把该条件只与后述的 RAM 上的对照状

态保持区域 A 进行比较，判断是否确立了存取条件所要求的密钥的对照状态（ ST94 ）。

如果没有确立，即输出表示存取条件不一致的响应显示信息，并返回到等待命令状态（ ST95 ）。如果确立了，接着对对应的数据 EF 区域内进行存取（ ST96 ），并用响应显示信息输出其处理结果，并返回到等待命令状态（ ST97 ）。

这样，譬如作为设定使用者密钥（移交密钥）的存取条件，需要作为其上级的发行者的密钥，而且使用者移交密钥的变更预先设定为可根据该密钥的对照而进行，并且设定为在执行其他存取命令时，必须要有使用者的密钥对照。

在这种场合，变更前的使用者移交密钥的对照结果存储在对照状态保持区域 B 。因而，即使其他存取需要对照使用者密钥，在用于这些存取的对照状态保持 A 区域也不反映对照结果，从而可以做到不发挥该密钥的效果。

另外，唯有在该密钥变更的场合，因参考对照状态保持区域 A 及 B ，故在变更前也可参考确立了的对照状态，从而允许密钥变更行为。

又，通过密钥变更后的密钥的对照，在对照状态保持区域 A 反映对照状态，故就以后的其他存取已发挥出效果。

另外，如本实施形态那样，根据密钥 EF 创建时输入的密钥的类型信息，可设定是否模拟地在这一时刻进行变更，故可根据使用者的各种要求，由作为上级的卡片发行者有选择地设定各种类型。

在前述的实施形态中，作为从密钥的类型信息中预先设定表示密钥变更是否已进行的状态信息的时间，是在密钥 EF 创建命令处理中进行，当然也可以是在设置密钥的命令处理中进行。

图 13 是说明创建移交密钥基本文件（ EF ）的动作的流程图，以下就该图进行说明。 IC 卡 1 一旦收到从外部输入的移交 EF 创建命令，首先识别现行 DF （ ST101 ）。

一旦识别了现行 DF ，接着检验该数据文件（ DF ）内设定的状态信息 DFST 中的移交位是否置 1 （ ST102 ）。

如果移交位置 1 ，则该命令被拒绝，输出表示不可移交的响应显示信息，并返回到等待命令状态（ ST103 ）。而如果移交位置 0 ，该移交密钥 EF 创建命令则被允许。另外，该移交位在数据文件创建时置 0 ，且在移交密钥自身根据密钥变更命令变更时置 1 。

一旦移交密钥 EF 创建命令被允许，接着就参考该现行 DF 的主数据文件（ DF ）的存取条件。把该条件只与后述的 RAM 上的对照状态保持区域 A 进行比较，判断是否确立了存取条件所要求的密钥（口令）的对照状态（ ST104 ）。

如果没有确立，即输出表示存取条件不一致的响应显示信息，并返回到等待命令状态（ ST105 ）。如果确立了，接着参考命令显示信息指示的基本文件名（ EF - ID ），在成为存取对象的现行 DF 内，检验该基本文件名是否存在（ ST106 ）。

如果存在，即输出表示 ID 重复异常的响应显示信息，并返回到等待命令状态（ ST107 ）。

如果不存在，接着参考命令显示信息所指定的密钥 EF 的容量数据，与成为存取对象的现行 DF 内的空白区域容量进行比较（ ST108 ）。在该比较中，在指定的密钥 EF 容量上加上创建该密钥 EF 时使用的目录信息的容量，然后检验前述空白区域容量是否超过该值。如果前者大于后者，则输出表示指定容量配合异常的响应显示信息，并返回到等待命令状态（ ST109 ）。

如果不是那样，则检验命令显示信息指定的密钥类型和容量的正确性（ ST110 ）。这时，当密钥类型成为“认证相关密钥”时容量譬如是 10 字节时，或是当密钥类型成为“对照密钥”时容量譬如是 3 ~ 18 字节时，则判断容量为正确。在判断为不正确的场合，输出表示指定容量异常的响应显示信息，并返回到等待命令状态（ ST111 ）。

这里，当判断容量为正确时，根据收到的命令，生成应存储于目录中的密钥 EF 定义信息（ ST112 ），并将其写入规定区域（ ST113 ）。这时，状态信息的第 8 位根据命令显示信息所指定的密钥类型信息中的第 1 位而决定其值。即，在前者的位中设定与后者的位值同样的值。

该状态信息的第 8 位是表示密钥数据是否已变更的位，当该位为“ 1 ”时，表示变更行为未实施，而当其为“ 0 ”时则表示该行为已实施。

从而，当上述密钥类型信息的第 1 位为“ 1 ”时，只要密钥变更未进行，状态信息的第 8 位就不会成为“ 0 ”，另外，在“ 0 ”的场合，无论是否进行密钥变更，状态信息的第 8 位都变成“ 0 ”（即，等于是重写行为在暗中进行）。

在上述密钥 EF 定义信息的写入中，在写入未正常结束的场合（ ST114 ），输出表示数据写入异常的响应显示信息，并返回到等待命令状态（ ST115 ）。而在写入正常结束的场合（ ST114 ），输出表示正常结束的响应显示信息，并返回到等待命令状态（ ST116 ）。

以下说明在上述构造中对 IC 卡创建各文件的顺序。

首先，在制造 IC 卡时，为了设定（创建）应向卡片发行者移交的移交密钥的基本文件，按照图 9 的流程图并如图 14 所示，在主文件（ MF ）属下创建密钥“ EF - a ”，并在此处设定移交密钥。

接着按照图 10 的流程图进行针对该密钥基本文件 EF - a 的设定，在进行密钥的设定时，参考对该密钥 EF - a 给出的密钥设定用存取条件。

在此状态下，一旦发行者接受卡片，即按照图 11 的流程图变更移交密钥。即如图 15 所示，发行者把制造者设定的移交密钥变更为只有其自身知道的密钥（ a’）。在该变更中，参考在该密钥 EF 中设定的密钥变更用存取条件。在此时刻，对主文件（ MF ）给出的移交位置 1，以后，由制造者进行的主文件（ MF ）属下的密钥的创建即被拒绝。

接着，发行者在主文件（ MF ）属下创建自身需要的数据 EF － a 。在这种场合，参考在主文件（ MF ）中设定的 EF 创建用存取条件。

另外，发行者在主文件（ MF)属下创建对使用者开放用的数据文件（ DF)。DF 的设定按照图 7 的流程图进行，在这种场合，参考在主文件（ MF ）中设定的数据文件（ DF ）创建用存取条件。

接着，发行者在该数据文件（ DF ）属下创建应向使用者移交的移交密钥 EF － b 。移交密钥 EF － b 的创建按照图 9 的流程图进行，在这种场合，参考的存取条件不是对该数据文件（ DF ）给出的，而是参考对其主文件、即（ MF ）给出的存取条件。

接着，发行者在该移交密钥 EF － b 内设定移交密钥。移交密钥的设定按照图 10 的流程图进行，在这种场合，参考成为对象的密钥 EF － b 给出的、设定密钥用的存取条件。

在此状态下，一旦使用者接受卡片，即如图 16 所示，使用者把发行者设定的移交密钥变更为只有其自身知道的密钥（ b’）。在该变更中，参考在该密钥 EF 中设定的密钥变更用存取条件。在此时刻，对数据文件（ DF)给出的移交位置 1，以后，由发行者进行的数据文件（ DF ）属下的密钥的创建即被拒绝。

接着，使用者在数据文件（ DF ）属下创建自身需要的数据 EF － b 。数据 EF － b 的创建按照图 7 的流程图进行，在这种场合，参考在数据文件（ DF ）中设定的 EF 创建用存取条件。

另外，，使用者在数据文件（ DF ）属下创建自身需要的密钥 EF － c 。密钥 EF － c 的创建按照图 8 的流程图进行，在这种场合，也是参考在数据文件（ DF ）中设定的 EF 创建用存取条件。

命令形成如下形式，特别是，通常的密钥 EF 创建命令和移交密钥 EF 创建命令形成不同的命令码形式， IC 卡根据该命令码识别命令的内容。

即，对通常的密钥 EF 创建命令与移交密钥 EF 创建命令加以识别，是移交密钥 EF 创建命令时根据图 9 的流程进行处理，而是通常的密钥 EF 创建命令时则根据图 8 的流程进行处理。

区域（基本文件）创建命令

命令码 A/AID(EF-ID)/ASIZ/AAC

密钥 EF 创建命令

命令码 B/KID/KSIZ/CF/AAC

移交密钥 EF 创建命令

命令码 C/KID/KSIZ/CF/AAC

当在上述的现行 DF 属下创建移交密钥 EF 的场合，参考现行 DF 的主 DF 的存取条件。主 DF 的存取条件是上级设定的。移交密钥 EF 的创建可以由上级进行。

另外，对移交密钥 EF 设定移交密钥时参考该 EF 的存取条件，而该 EF 的存

取条件是在移交 EF 创建时由上级设定的，上级设定该 EF 存取条件，以便能够对移交密钥 EF 设定移交密钥。

当使用者在现行 DF 属下设定密钥 EF 的场合，参考现行 DF 的密钥 EF 创建用存取条件，而 DF 的存取条件是在 DF 创建时由上级设定。

然而，在移交密钥变更后，使用该 DF 存取条件的处理（数据 EF 、密钥 EF 的创建）只能是使用者进行，故存取权的区分是明确的。

还有，作为密钥 EF 创建用存取条件，由于上级预先设定移交密钥变更后的密钥，使用者在变更了移交密钥后设定自身使用的密钥 EF ，并根据该自身使用的密钥 EF 的密钥定义信息中的对照位指定信息准备可满足 DF 存取条件的环境，并且做到一旦对照自身的密钥，即可满足创建数据 EF 用的 DF 存取条件，使数据 EF 的创建成为可能。

这样一来，上级虽然是设定 DF 存取条件的，却不知道其内容，而只有使用者才能满足 DF 的存取条件。

如上所述，采用上述发明的实施形态，为在数据文件（ DF ）属下创建 EF （或 DF ）所必要的密钥取决于对该数据文件（ DF ）给出的存取条件，而且该存取条件可在不指定上级密钥（在本实施例中，发行者成为使用者的上级）的情况下实现。

从而，使用者欲由自身管理的文件（或存储区域）可只用自身的密钥保护。

这样，就不会形成发行者对该数据文件（ DF ）的干预，从而可以从发行者向使用者移交对该文件（或存储区域）进行存取的权限。

还有，本实施例中的移交位在数据文件（ DF ）创建时置 0，在移交密钥自身根据密钥变更命令而变更的时刻置 1，当然也可以不与密钥变更命令连动，而是用移交位置 1 的命令实施。在这种场合，执行该命令时使用的存取条件参考在作为对象的文件中所设定的内容。

如上所述，采用前述实施形态时，可提供一种譬如没有上级对数据文件的干预、可从上级向下级移交向该数据文件或存储区域进行存取的权限的存储器存取管理方法。

另外，在前述实施形态中，作为进行文件管理的电子设备，例举了 IC 卡，当然并不限于此，只要是具备需要进行文件管理的存储器的电子设备都适用。

如上所述，本发明可以提供一种在把移交密钥（口令）从上级移交给下级后、只要下级不变更该密钥（口令）、其效力便不会发挥的、安全性好的文件管理方法及使用该方法的媒体。

说 明 书 附 图

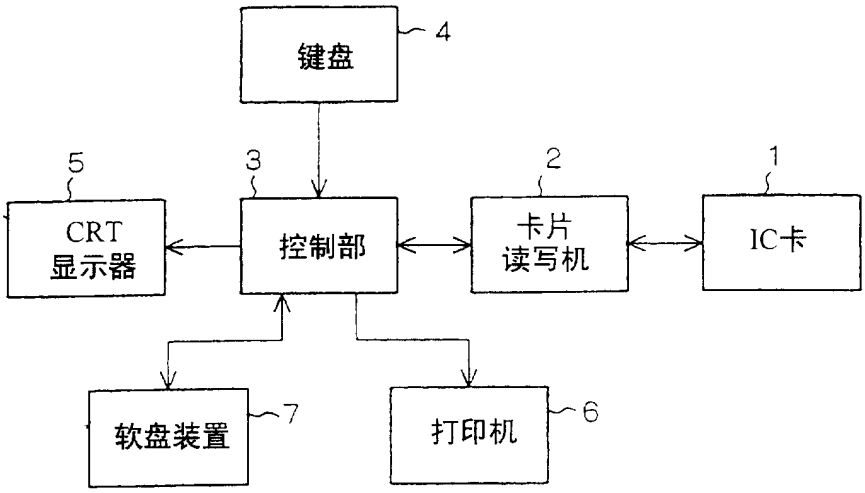

键盘
4
5
3
2
1
CRT
显示器
控制部
卡片
读写机
IC卡
软盘装置
7
打印机
6

图 1A

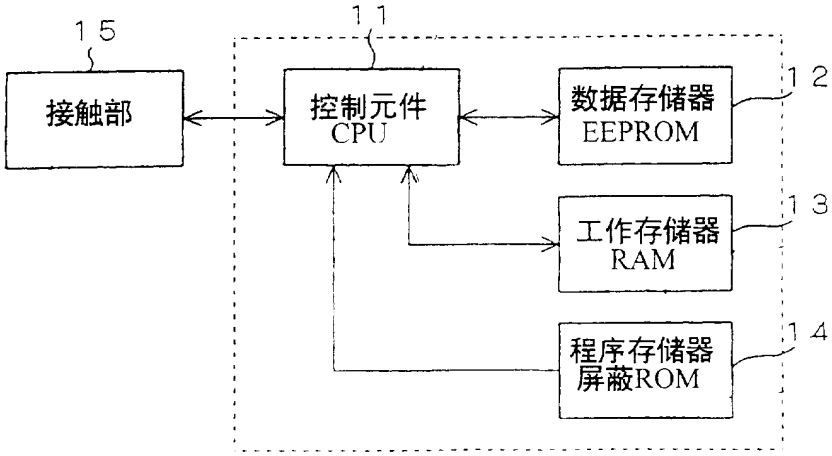

15
11
接触部
控制元件
CPU
数据存储器
EEPROM
12
工作存储器
RAM
13
程序存储器
屏蔽ROM
14

图 2

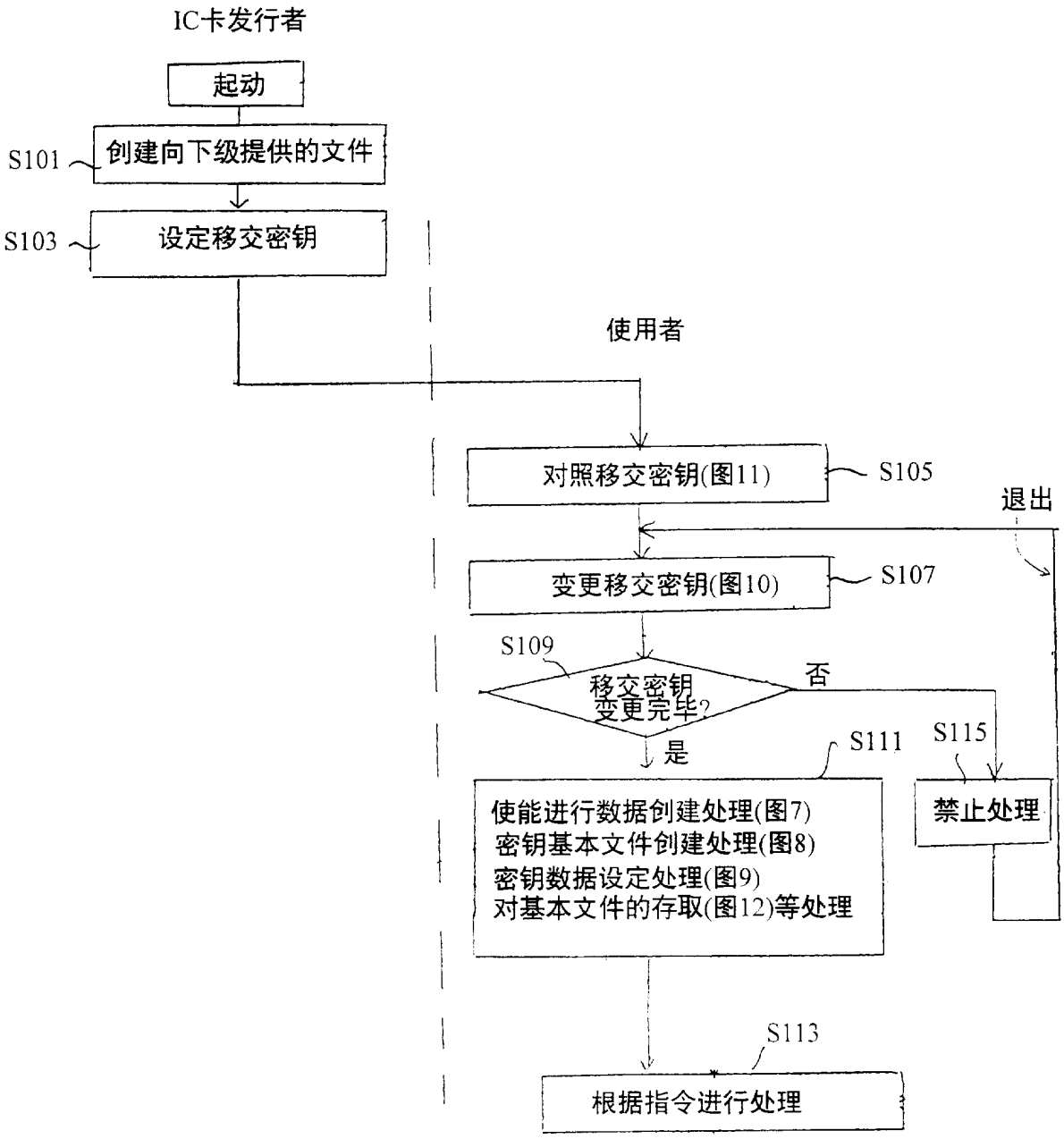

IC卡发行者
起动
S101
创建向下级提供的文件
S103
设定移交密钥
使用者
对照移交密钥(图11)
S105
退出
变更移交密钥(图10)
S107
S109
移交密钥
变更完毕?
否
是
S111
S115
使能进行数据创建处理(图7)
密钥基本文件创建处理(图8)
密钥数据设定处理(图9)
对基本文件的存取(图12)等处理
禁止处理
S113
根据指令进行处理

图 1B

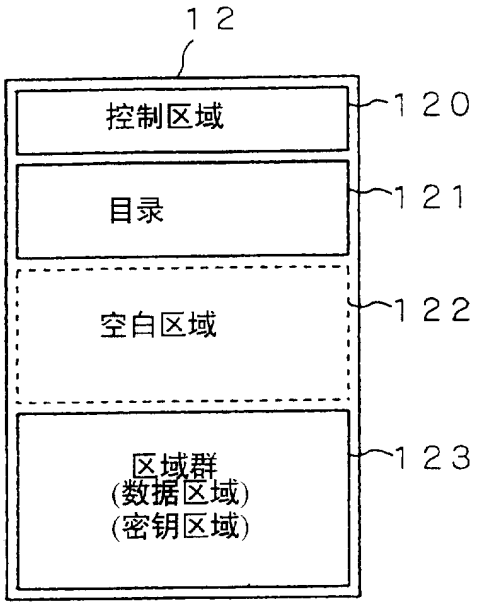

12
控制区域
120
目录
121
空白区域
122
区域群
(数据区域)
(密钥区域)
123

图 3

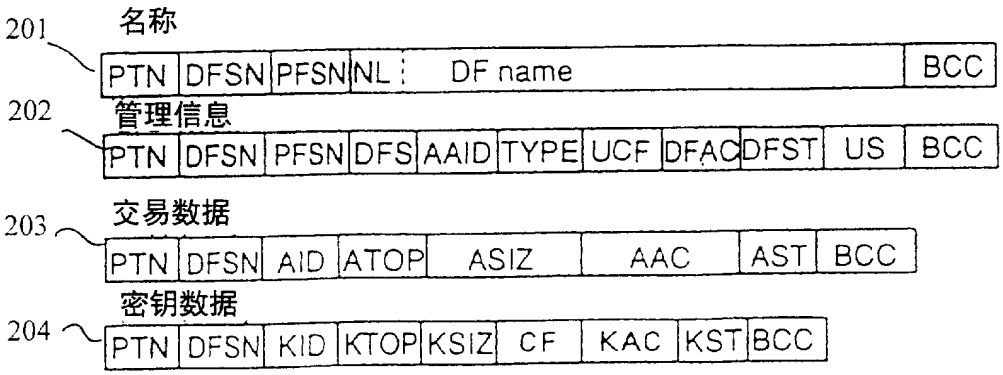

201
名称
PTN
DFSN
PFSN
NL
DF name
BCC
202
管理信息
PTN
DFSN
PFSN
DFS
AAID
TYPE
UCF
DFAC
DFST
US
BCC
203
交易数据
PTN
DFSN
AID
ATOP
ASIZ
AAC
AST
BCC
204
密钥数据
PTN
DFSN
KID
KTOP
KSIZ
CF
KAC
KST
BCC

图 4

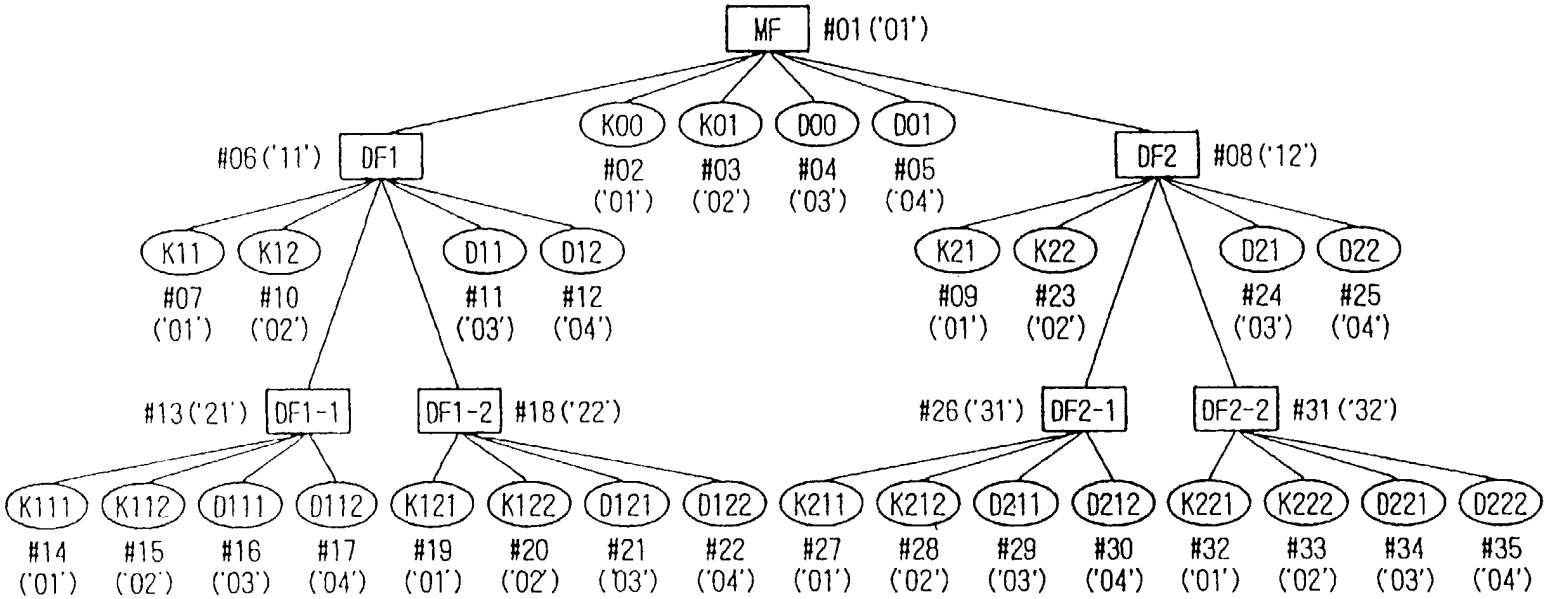

MF
#01 ('01')
K00
K01
D00
D01
#02 ('01')
#03 ('02')
#04 ('03')
#05 ('04')
#06 ('11')
DF1
DF2
#08 ('12')
K11
K12
D11
D12
#07 ('01')
#10 ('02')
#11 ('03')
#12 ('04')
K21
K22
D21
D22
#09 ('01')
#23 ('02')
#24 ('03')
#25 ('04')
#13 ('21')
DF1-1
DF1-2
#18 ('22')
#26 ('31')
DF2-1
DF2-2
#31 ('32')
K111
K112
D111
D112
K121
K122
D121
D122
K211
K212
D211
D212
K221
K222
D221
D222
#14 ('01')
#15 ('02')
#16 ('03')
#17 ('04')
#19 ('01')
#20 ('02')
#21 ('03')
#22 ('04')
#27 ('01')
#28 ('02')
#29 ('03')
#30 ('04')
#32 ('01')
#33 ('02')
#34 ('03')
#35 ('04')

图 5

序列号	DFSN	PFSN	FID	
#01	00	00	00	MF 定义信息
#02	00	-	01	K00 定义信息
#03	00	-	02	K01 定义信息
#04	00	-	03	D00 定义信息
#05	00	-	04	D01 定义信息
#06	01	00	11	DF1 定义信息
#07	01	-	01	K11 定义信息
#08	02	00	12	DF2 定义信息
#09	02	-	01	K21 定义信息
#10	01	-	02	K12 定义信息
#11	01	-	03	D11 定义信息
#12	01	-	04	D12 定义信息
#13	03	01	21	DF1-1 定义信息
#14	03	-	01	K111 定义信息
#15	03	-	02	K112 定义信息
#16	03	-	03	D111 定义信息
#17	03	-	04	D112 定义信息
#18	04	01	22	DF1-2 定义信息
#19	04	-	01	K121 定义信息
#20	04	-	02	K122 定义信息
#21	04	-	03	D121 定义信息
#22	04	-	04	D122 定义信息
#23	02	-	02	K22 定义信息
#24	02	-	03	D21 定义信息
#25	02	-	04	D22 定义信息
#26	05	02	31	DF2-1 定义信息
#27	05	-	01	K211 定义信息
#28	05	-	02	K212 定义信息
#29	05	-	03	D211 定义信息
#30	05	-	04	D212 定义信息
#31	06	02	32	DF2-2 定义信息
#32	06	-	01	K221 定义信息
#33	06	-	02	K222 定义信息
#34	06	-	03	D221 定义信息
#35	06	-	04	D222 定义信息

图 6

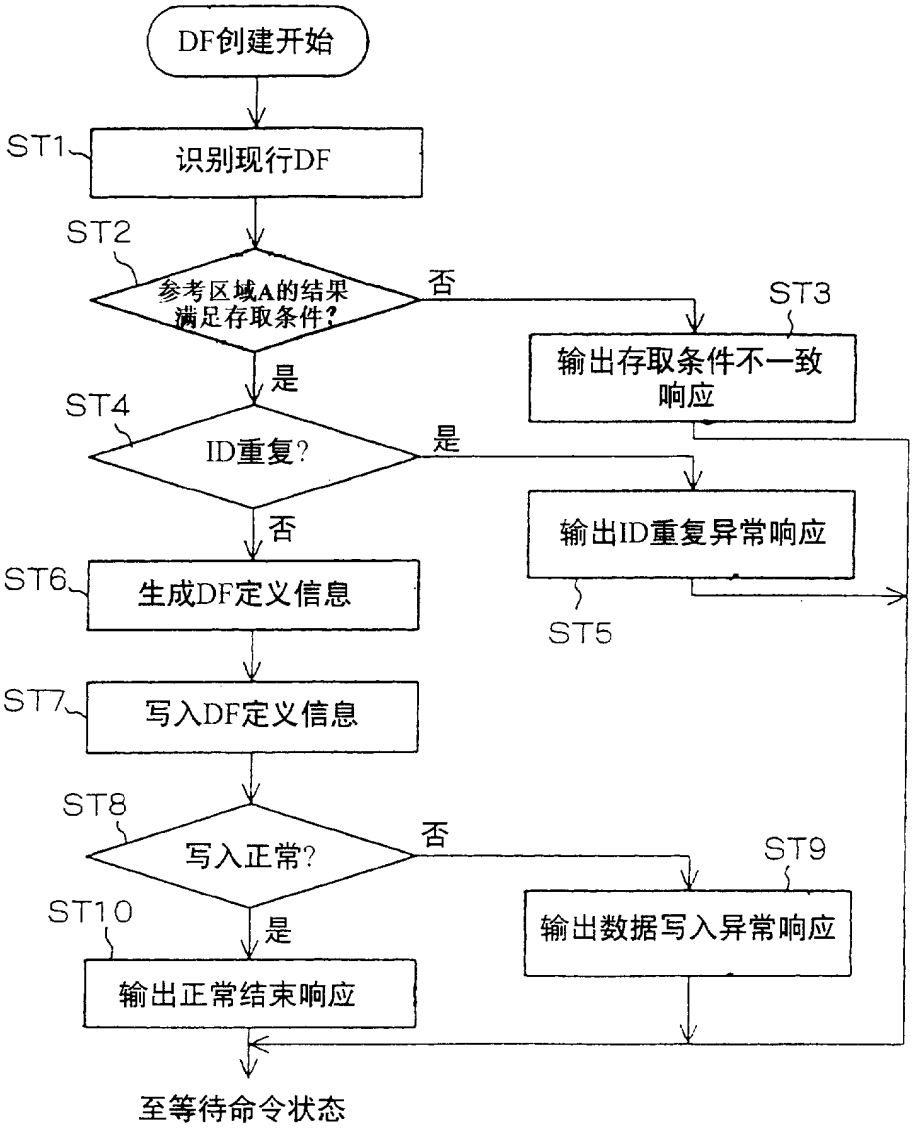

DF创建开始
ST1
识别现行DF
ST2
参考区域A的结果
满足存取条件?
否
ST3
输出存取条件不一致
响应
是
ST4
ID重复?
是
输出ID重复异常响应
ST5
否
ST6
生成DF定义信息
ST7
写入DF定义信息
ST8
写入正常?
否
ST9
输出数据写入异常响应
ST10
是
输出正常结束响应
至等待命令状态

图 7

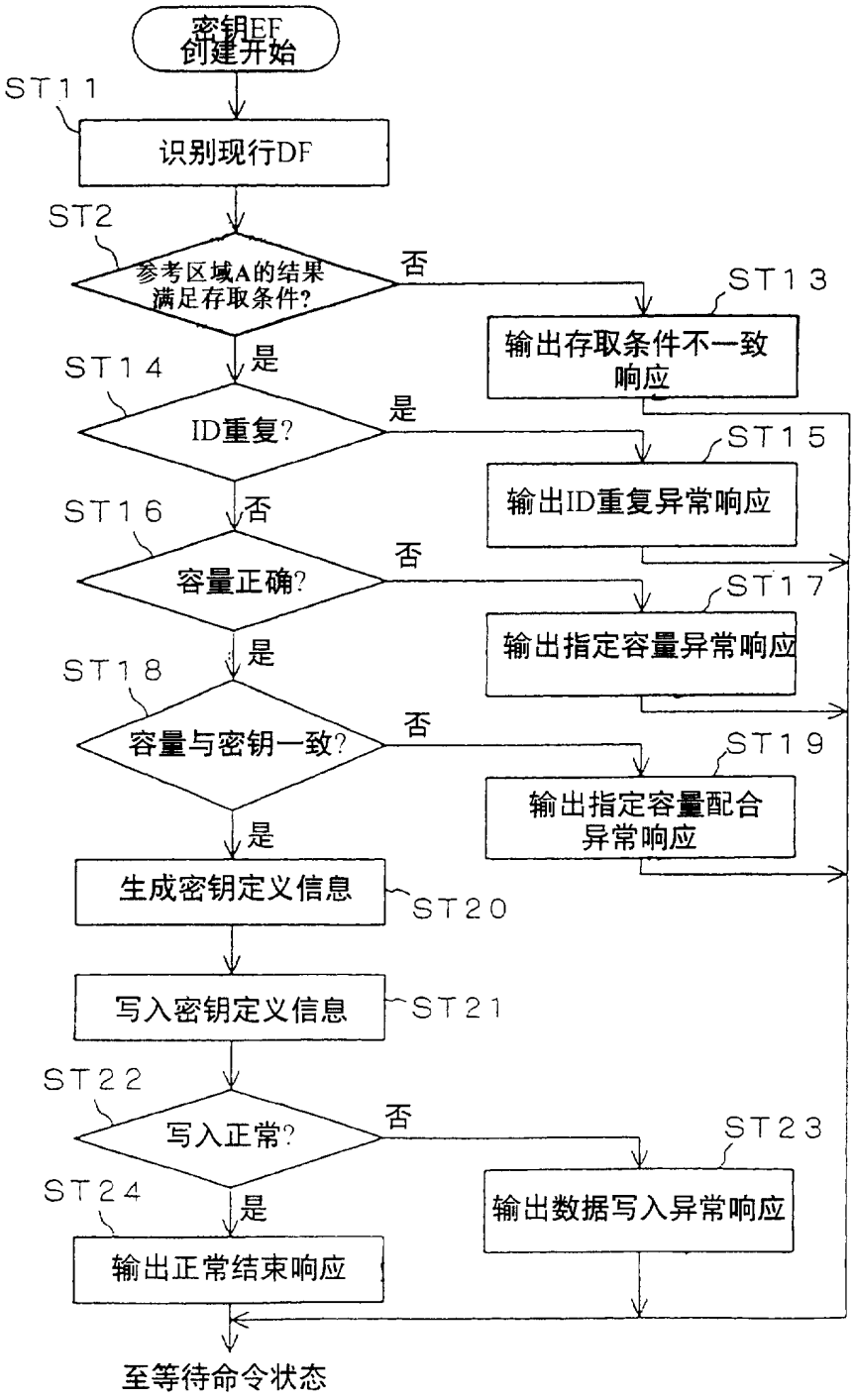

密钥EF
创建开始
ST11
识别现行DF
ST2
参考区域A的结果
满足存取条件?
否
ST13
输出存取条件不一致
响应
是
ST14
ID重复?
是
ST15
输出ID重复异常响应
否
ST16
容量正确?
否
ST17
输出指定容量异常响应
是
ST18
容量与密钥一致?
否
ST19
输出指定容量配合
异常响应
是
生成密钥定义信息
ST20
写入密钥定义信息
ST21
ST22
写入正常?
否
ST23
输出数据写入异常响应
ST24
是
输出正常结束响应
至等待命令状态

图 8

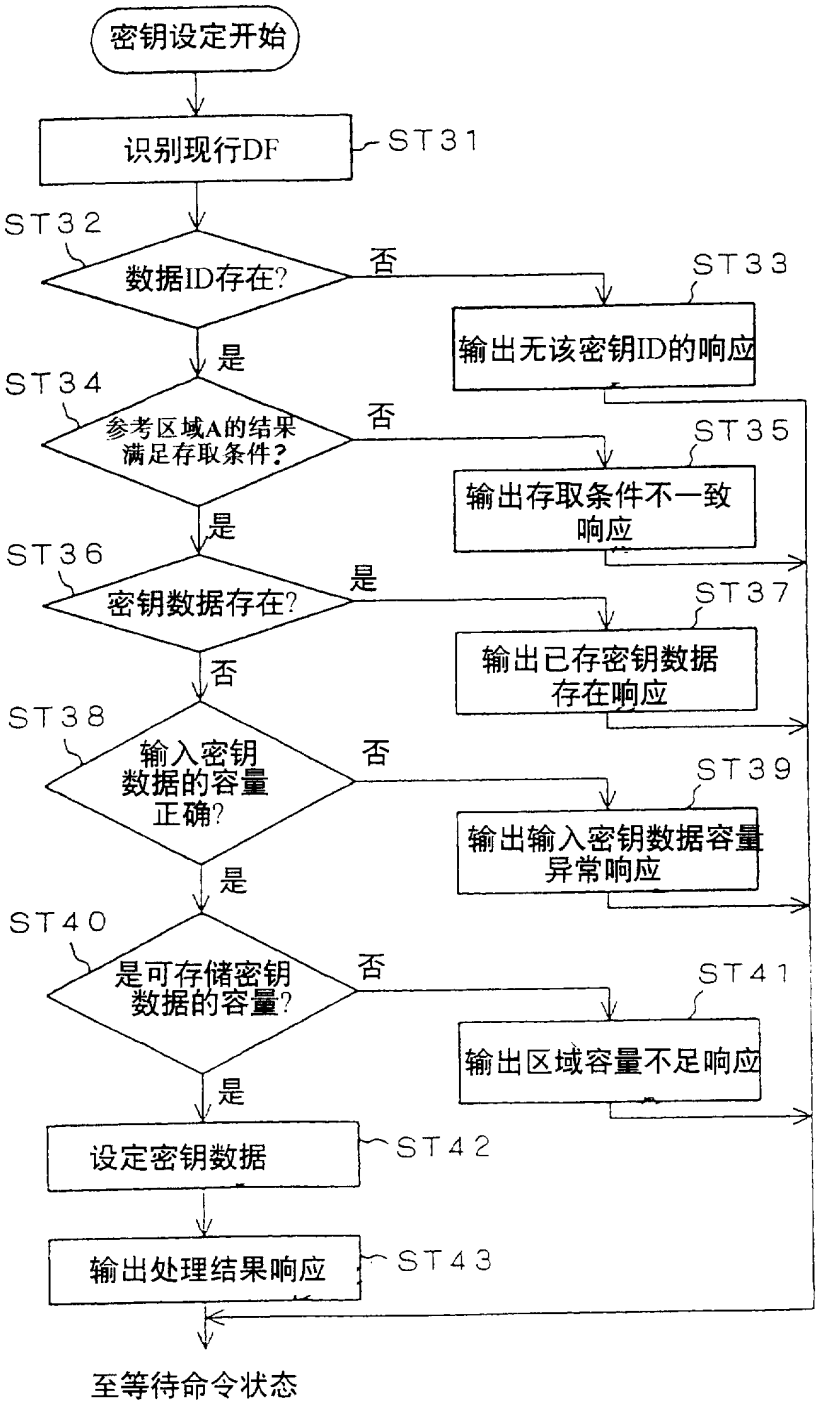

密钥设定开始
识别现行DF
ST31
ST32
数据ID存在?
否
ST33
输出无该密钥ID的响应
是
ST34
参考区域A的结果满足存取条件?
否
ST35
输出存取条件不一致响应
是
ST36
密钥数据存在?
是
ST37
输出已存密钥数据存在响应
否
ST38
输入密钥数据的容量正确?
否
ST39
输出输入密钥数据容量异常响应
是
ST40
是可存储密钥数据的容量?
否
ST41
输出区域容量不足响应
是
设定密钥数据
ST42
输出处理结果响应
ST43
至等待命令状态

图 9

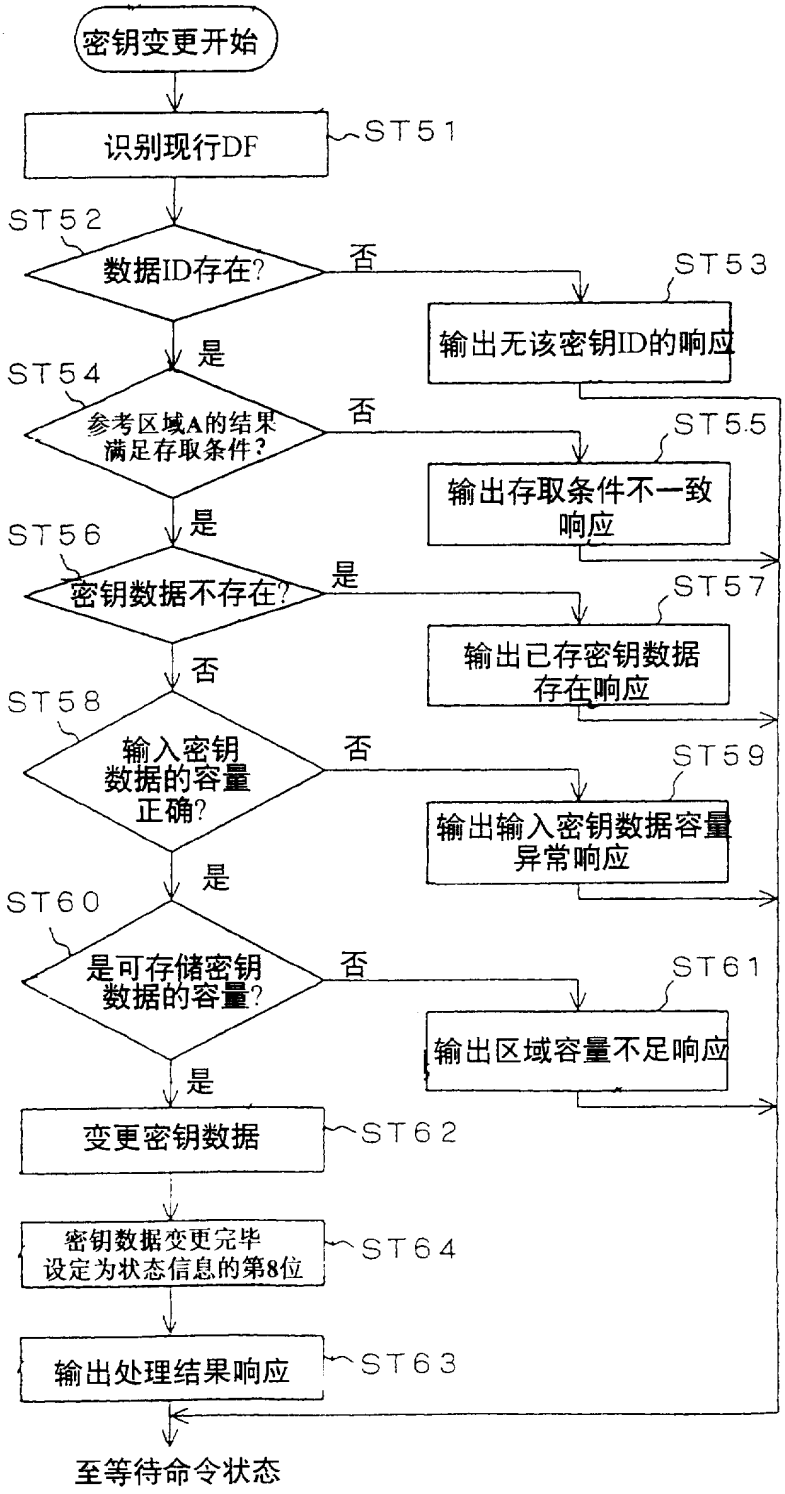

密钥变更开始
识别现行DF
ST51
ST52
数据ID存在?
否
ST53
输出无该密钥ID的响应
是
ST54
参考区域A的结果满足存取条件?
否
ST55
输出存取条件不一致响应
是
ST56
密钥数据不存在?
是
ST57
输出已存密钥数据存在响应
否
ST58
输入密钥数据的容量正确?
否
ST59
输出输入密钥数据容量异常响应
是
ST60
是可存储密钥数据的容量?
否
ST61
输出区域容量不足响应
是
变更密钥数据
ST62
密钥数据变更完毕设定为状态信息的第8位
ST64
输出处理结果响应
ST63
至等待命令状态

图 10

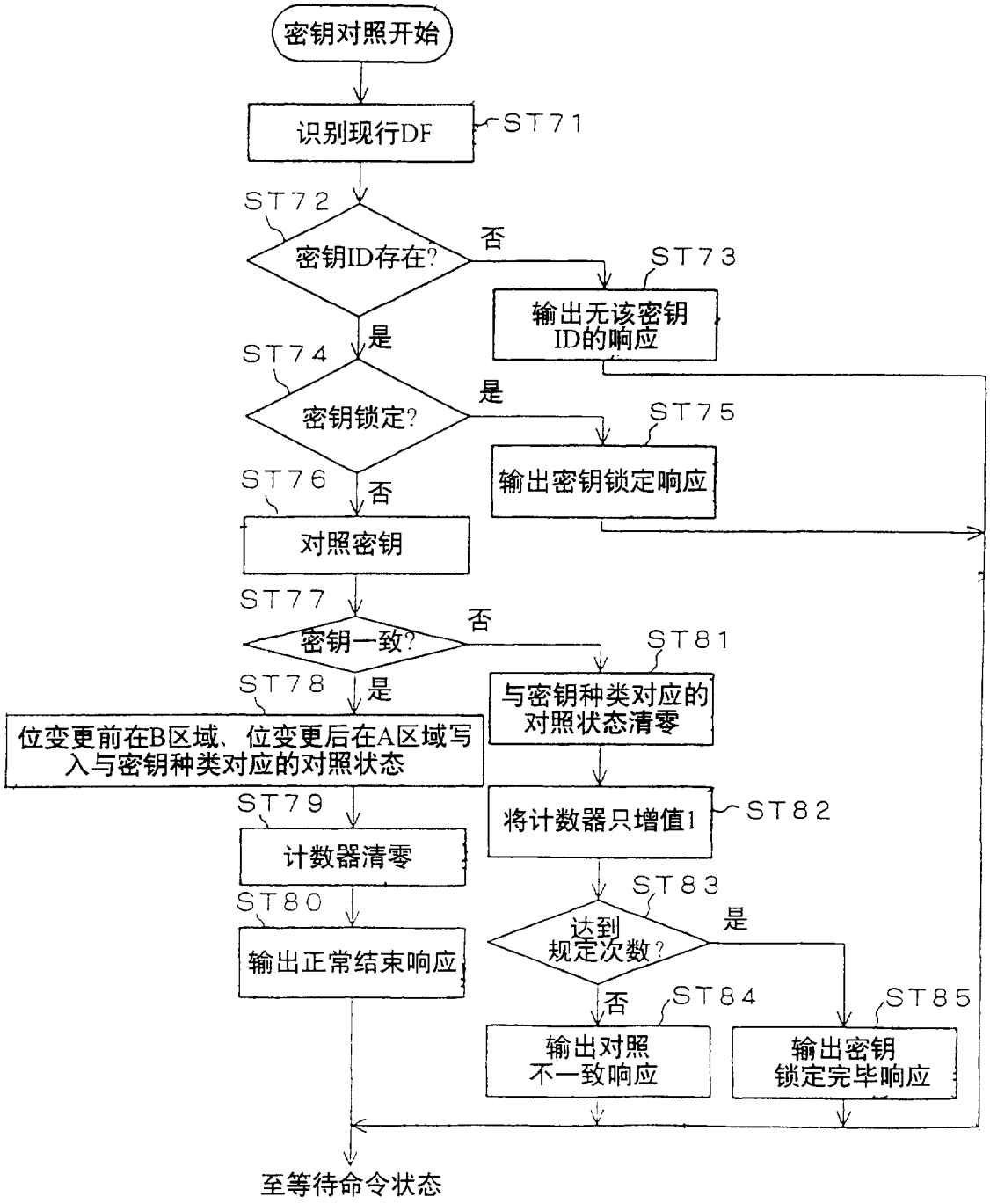

密钥对照开始
识别现行DF
ST71
ST72
密钥ID存在?
否
ST73
输出无该密钥ID的响应
是
ST74
密钥锁定?
是
ST75
输出密钥锁定响应
ST76
否
对照密钥
ST77
密钥一致?
否
ST81
ST78
是
位变更前在B区域、位变更后在A区域写入与密钥种类对应的对照状态
与密钥种类对应的对照状态清零
ST79
计数器清零
将计数器只增值1
ST82
ST83
ST80
输出正常结束响应
达到规定次数?
是
否
ST84
ST85
输出对照不一致响应
输出密钥锁定完毕响应
至等待命令状态

图 11

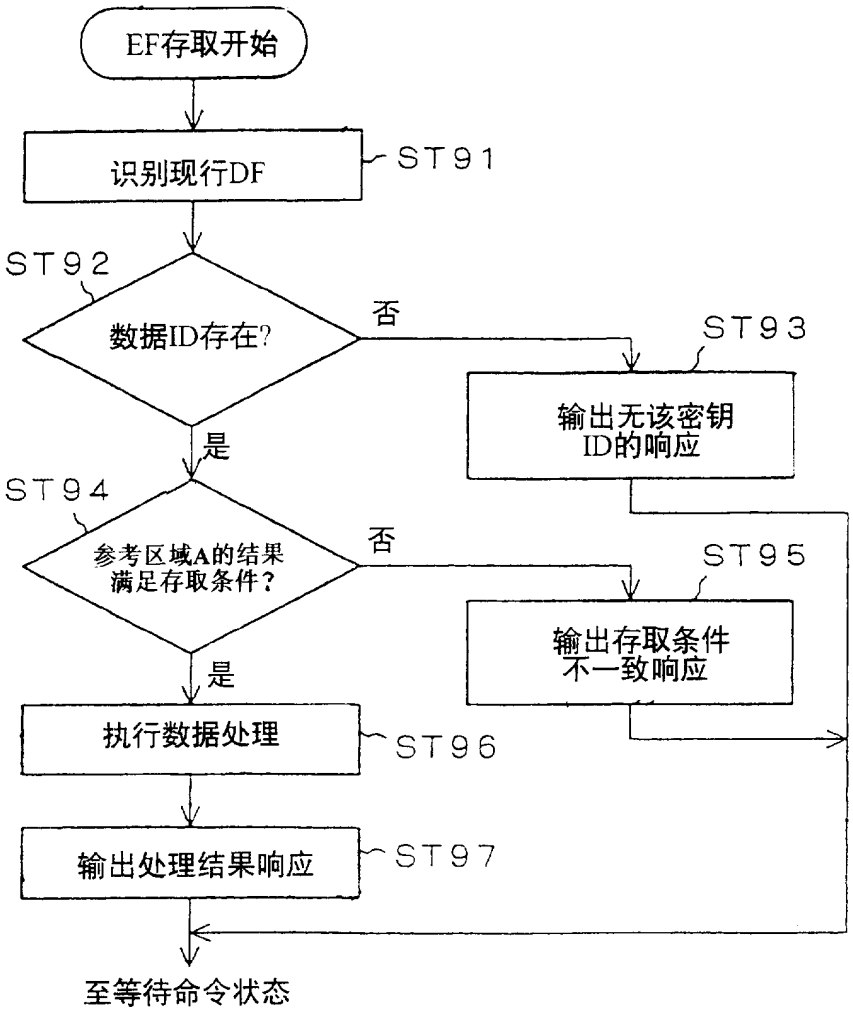

EF存取开始
识别现行DF
ST91
ST92
数据ID存在?
否
ST93
输出无该密钥
ID的响应
是
ST94
参考区域A的结果
满足存取条件?
否
ST95
输出存取条件
不一致响应
是
执行数据处理
ST96
输出处理结果响应
ST97
至等待命令状态

图 12

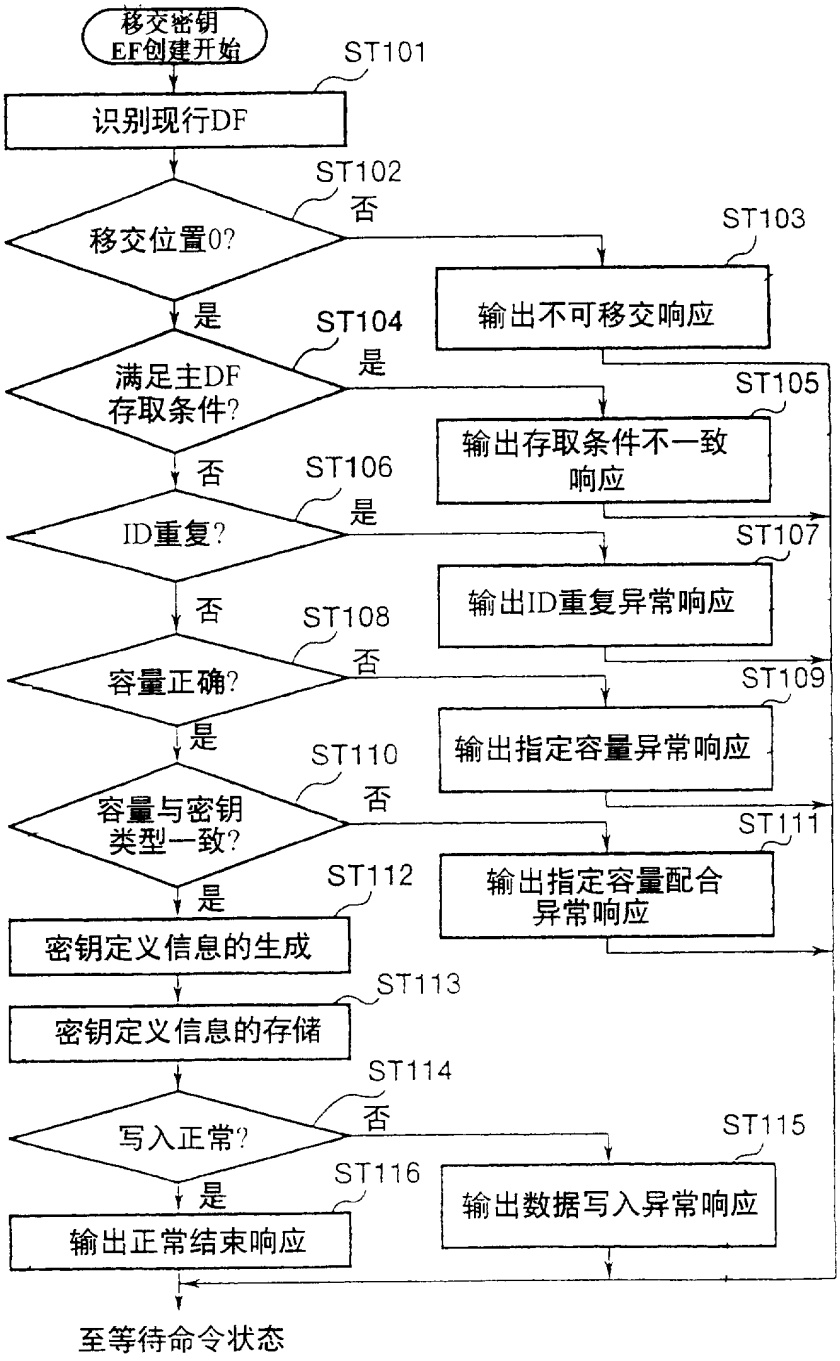

移交密钥
EF创建开始
ST101
识别现行DF
ST102
移交位置0?
否
ST103
输出不可移交响应
是
ST104
满足主DF
存取条件?
是
ST105
输出存取条件不一致
响应
否
ST106
ID重复?
是
ST107
输出ID重复异常响应
否
ST108
容量正确?
否
ST109
输出指定容量异常响应
是
ST110
容量与密钥
类型一致?
否
ST111
输出指定容量配合
异常响应
是
ST112
密钥定义信息的生成
ST113
密钥定义信息的存储
ST114
写入正常?
否
ST115
输出数据写入异常响应
是
ST116
输出正常结束响应
至等待命令状态

图 13

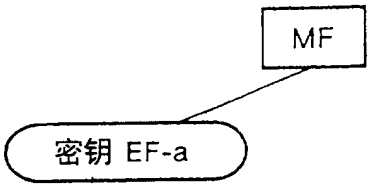

MF
密钥 EF-a

图 14

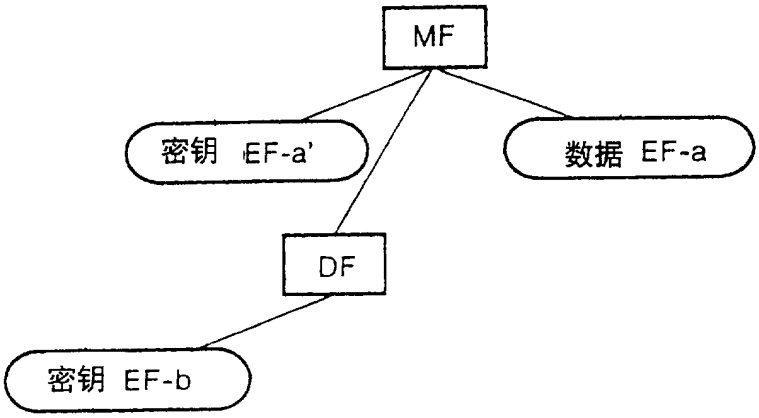

MF
密钥 EF-a'
数据 EF-a
DF
密钥 EF-b

图 15

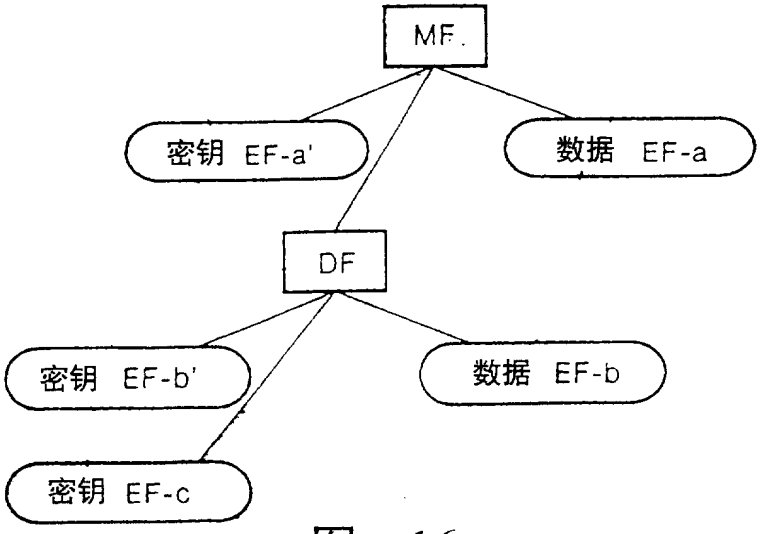

MF
密钥 EF-a'
数据 EF-a
DF
密钥 EF-b'
数据 EF-b
密钥 EF-c

图 16