[19] 中华人民共和国国家知识产权局

[12] 发明专利说明书

专利号 ZL 00819883.7

[51] Int. Cl[7]
G06F 12/14
G06K 19/07
G06K 19/077
G06K 19/10
H04L 9/32

[45] 授权公告日 2005 年 11 月 16 日

[11] 授权公告号 CN 1227595C

[22] 申请日 2000.9.18 [21] 申请号 00819883.7
[86] 国际申请 PCT/JP2000/006348 2000.9.18
[87] 国际公布 WO2002/023349 日 2002.3.21
[85] 进入国家阶段日期 2003.3.12
[71] 专利权人 株式会社东芝
地址 日本东京都
[72] 发明人 池田英贵
审查员 张 妍

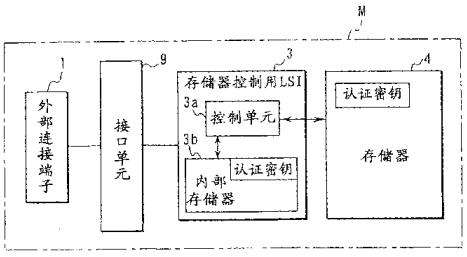
[74] 专利代理机构 中国国际贸易促进委员会专利商标事务所
代理人 吴丽丽

权利要求书 1 页 说明书 14 页 附图 14 页

[54] 发明名称 便携式电子介质的认证方法

[57] 摘要

一种便携式电子介质，包括：施加有配线的基板(2)；焊接到基板(2)存储数据与认证密钥的存储器(4)；以及包括包含存储数据与认证密钥的内部存储器(3b)，和控制向存储器(4)进行数据记录或者从存储器(4)的数据再现的控制单元(3a)的由裸芯片所构成，且安装在基板(2)上，用封装树脂进行封装并通过金丝键合连接到基板(2)的存储器控制用 LSI。 上述控制单元(3a)，通过匹配记录在上述存储器(4)中的认证密钥和记录在上述内部存储器(3b)中的认证密钥，来判断上述存储器(4)是否正确。



ISSN1008-4274

1. 一种便携式电子介质的认证方法， 该便携式电子介质由以下部分构成：通过软质镀金被实施布线的基板；通过焊料安装在该基板上，记录数据的第一存储器；由一个裸芯片构成，用封装树脂覆盖每个裸芯片而安装在上述基板上，并通过金丝键合与上述基板连接的控制电路，该裸芯片内置了以下部分：在记录数据的同时，记录作为上述第一存储器的状态信息在上次处理时使用了的上述第一存储器的记录开始地址、记录信息的长度、从记录开始地址的对记录信息的长度的信息的校验和的第二存储器；控制向上述第一存储器记录数据，或控制重放记录在上述第一存储器中的数据的控制部件，其中上述第一存储器和第二存储器的一部分为非易失性存储器，该便携式电子介质的认证方法的特征在于：

上述控制部件在对上述第一存储器进行访问时，判断上述第一存储器的上次处理时使用了的记录开始地址和记录信息的长度，从该判断出的记录开始地址开始计算对记录信息的长度的信息的校验和，根据上述判断出的记录开始地址、记录信息的长度、计算出的校验和与记录在上述第二存储器中的上次处理时使用了的上述第一存储器的记录开始地址、记录信息的长度、校验和是否一致，判断上述第一存储器是否正确。

2. 根据权利要求 1 所述的便携式电子介质的认证方法，其特征在于：第二存储器的非易失性的存储器中记录着上述第一存储器的状态信息。

3. 根据权利要求 1 所述的便携式电子介质的认证方法，其特征在于：

在上述第二存储器中记录有上述控制部件的控制程序。

便携式电子介质的认证方法

技术领域

本发明涉及作为分别将记录数据的存储器和控制此存储器的控制电路安装在一个卡上的存储卡的便携式电子介质。

背景技术

一般，在分别将记录数据的存储器和控制此存储器的控制电路（控制用 LSI）安装在一个卡（基板）上的情况下，存储器和控制用 LSI 分别对应于基板通过焊料来进行连接。

因此，在能够容易地更换存储器的同时，拆下控制用 LSI 来进行解析就成为可能。

由此，仅更换存储器来进行使用，或者增加存储器容量的伪造就成为可能。

发明内容

本发明考虑到上述的情况，目的是通过禁止与控制电路有对应关系的存储器以外的存储器的安装，来防止利用安装不同的存储器所进行的伪造。

本发明目的是能够使对控制存储器的控制电路的解析变得困难。

为了达到上述目的，本发明提供一种便携式电子介质，包括：施加有配线的基板；安装在此基板上，记录数据并记录有认证密钥的第一存储器；以及包括记录数据并记录有认证密钥的第二存储器，和控制向上述第一存储器进行数据的记录、或者控制对记录在上述第一存储器中的数据进行再现的控制单元，由芯片所构成，且安装在上述基板上并连接到上述基板的控制电路；上述控制单元，根据记录在上述第一存储器中的认证密钥与记录在上述第二存储器中的认证密钥是否

一致，来判断上述第一存储器是否正确。

为此，本发明还提供一种便携式电子介质，包括：施加有配线的基板；安装在此基板上，记录数据的第一存储器；以及包括记录数据并记录着上述第一存储器的状态信息的第二存储器，和控制向上述第一存储器进行数据的记录、或者控制对记录在上述第一存储器中的数据进行再现的控制单元的，由芯片所构成，安装在上述基板上并连接到上述基板的控制电路；上述控制单元，根据上述第一存储器的状态是否与记录在上述第二存储器中上述第一存储器的状态信息一致，来判断上述第一存储器是否正确。

为此，本发明进而提供一种便携式电子介质，包括：施加有配线的基板；安装在此基板上，记录数据并记录有对认证密钥进行加密后的加密数据的第一存储器；以及包括记录数据并记录有认证密钥、加密密钥以及解码程序的第二存储器，和控制向上述第一存储器进行数据的记录、或者控制对记录在上述第一存储器中的数据进行再现的控制单元，由芯片所构成，且安装在上述基板上并连接到上述基板的控制电路；上述控制单元，通过记录在上述第二存储器中的加密密钥和解码程序将记录在上述第一存储器中的加密数据解码成认证密钥，根据此认证密钥与记录在上述第二存储器中的认证密钥是否一致，来判断上述第一存储器是否正确。

附图说明

图 1 是表示本发明存储卡的内部结构的图。

图 2 是表示存储卡的内部结构的图。

图 3 是表示存储卡的内部的断面结构的图。

图 4 是表示存储卡的内部结构的图。

图 5 是表示存储卡的控制块的图。

图 6、8 是用于说明第一实施形式中的认证密钥的记录例的图。

图 7 是用于说明第一实施形式中的存储卡的启动时的处理或者电源电压供给时的处理的流程图。

图 9 是用于说明第二实施形式中的存储器的状态信息的记录例的图。

图 10 是用于说明第二实施形式中的认证处理的流程图。

图 11 是表示第二实施形式中的存储卡的存储器中的上次处理的最后的音乐信息的记录状态的图。

图 12 是用于说明第二实施形式中的存储器状态信息的记录处理和认证处理的流程图。

图 13 是表示第二实施形式中的内部存储器的存储器状态信息的记录例的图。

图 14、16 是用于说明第三实施形式中的加密数据、认证密钥、加密密钥和解码程序的记录例的图。

图 15 是用于说明第三实施形式中的认证处理的流程图。

图 17、19 是用于说明第四实施形式中的加密数据、认证密钥、加密密钥、解码程序和加密程序的记录例的图。

图 18 是用于说明第四实施形式中的认证处理的流程图。

图 20 是表示第五实施形式中的因特网连接系统的整体结构的图。

图 21 是用于说明向第五实施形式中的因特网连接系统中的批发销售店中的存储卡的因特网连接信息登录服务的图。

具体实施方式

下面，对本发明的实施形式进行说明。

首先，从图 1 到图 3 表示作为便携式电子介质的存储卡（SD 卡）M 的结构。图 1 是表示本发明存储卡 M 的内部结构的图，图 2 是表示存储卡 M 的内部结构的图，图 3 是表示存储卡 M 的内部的断面结构的图。

即，存储卡 M，在持有外部连接端子 1 的基板 2 上安装存储器控制用 LSI（控制电路、控制器）3、存储器（外部存储器、第一存储器）4、芯片部件 5 和其他的 IC6，并且如图 4 所示那样，收纳在外壳 7 内。

上述基板 2 的外部连接端子 1，为了提高接触持久性而采用硬质

镀金。

在上述基本 2 的具有外部连接端子 1 的面的相反侧的面 2a 中，施加适用于金丝键合的软质镀金。

在此面 2a 中，管芯键合作为裸芯片的存储器控制用芯片的上述存储器控制用 LSI3，金丝键合连接基板 2 和裸芯片（存储器控制用 LSI3），并用封装树脂 8 来封装。然后，焊接安装 TSOP 类型的存储器 4、芯片部件 5 和其他的 IC6。

这样，通过对基板 2 裸芯片地安装上述存储器控制用 LSI3，就会有使密钥数据的解析困难的效果。

接着，对上述存储卡 M 的控制电路，使用图 5 进行说明。

此存储卡 M，如图 5 所示那样，包括作为进行与外部装置（没有图示）的数据交换的联系单元的外部连接端子 1、连接到此外部连接端子 1 的接口单元 9、连接到此接口单元 9 的存储器控制用 LSI3 和控制连接到此存储器控制用 LSI3 的数据的记录再现的存储器 4。上述接口单元 9 由芯片部件 5 和其他的 IC6 构成。

存储器控制用 LSI3，包括对整体进行控制的控制单元 3a，和记录此控制单元 3a 用的控制程序并记录数据的内部存储器（第二存储器）3b。

上述存储卡 M，在与外部装置（没有图示）的连接时被供给电源电压。

[第一实施形式]

接着，对在上述这样的结构中，使用在对上述内部存储器 3b、上述存储器 4 不能改写的状态下所记录的认证密钥，来进行上述存储器 4 的认证的实施形式进行说明。

在此情况下，在上述内部存储器 3b 中，如图 6 所示那样，预先记录作为认证密钥的唯一值，而且是不能改写地进行记录。

另外，在上述存储器 4 中，也如图 6 所示那样，不能改写地记录与在上述内部存储器 3b 中所记录的认证密钥相同的认证密钥。

上述存储器 4 和内部存储器 3b，由不可改写的 ROM 单元和可改

写的 ROM 单元组成，在此不可改写的 ROM 单元中记录有上述认证密钥。

接着，对在上述这样的结构中，上述存储卡 M 启动时或者来自上述外部装置的电源电压供给时的处理，参照图 7 所示的流程图进行说明。

即，在存储卡启动时或者来自上述外部装置的电源电压供给时，控制单元 3a 进行自诊断（ST1）。此自诊断的结果，控制单元 3a 在诊断结果为确认的情况下（ST2），读出记录在存储器 4 中的认证密钥（ST3），读出记录在内部存储器 3 中的认证密钥（ST4），比较它们是否一致（ST5）。

控制单元 3a 在此比较的结果为两者的认证密钥相一致时，进行称为存储器 4 为正确的认证（认证确认）（ST6），并成为待机状态（ST7）。

另外，在上述步骤 2 中诊断为 NG 的情况下，或者在通过上述步骤 6 的认证为 NG 的情况下，控制单元 3a 中止处理（ST8）。

通过上述步骤 6 的认证为 NG 的情况是说，上述步骤 5 的比较结果为，由于认证密钥为不一致而存储器 4 为不正确的情况。

尽管上述例子中，对在存储卡启动时或者来自上述外部装置的电源电压供给时，进行存储器 4 的认证的情况进行了说明，但在每当进行存储器 4 的访问就进行存储器 4 的认证的情况下也可以与上述同样地进行实施。

作为向上述存储器 4 进行的访问处理，在进行从外部供给的音乐信息或程序的记录，或者进行所记录的音乐信息或程序的再现时执行。

另外，也可以将为了用于与存储器 4 进行认证而记录在内部存储器 3b 中的认证密钥用于外部装置和卡 M 间的认证。进而，如图 8 所示那样，也可以在卡 M 的内部存储器 3b 中，存储用于与存储器 4 进行认证的内部认证密钥 K1，和用于与外部装置进行认证的外部认证密钥 K2。

[第二实施形式]

接着，对在上述这样的结构中，上述存储器控制用 LSI3 记录上次的上述存储器 4 的状态（处理的形态）信息，并在下回进行存储器 4 的访问时，通过与记录有存储器 4 的状态的存储器 4 的状态信息是否相同，来进行上述存储器 4 的认证的实施形式进行说明。

在此情况下，控制单元 3a，在上述存储卡 M 中的处理结束时，如图 9 所示那样，在内部存储器 3b 中记录上述存储器 4 的状态信息。上述存储器 4 的状态信息是，上次处理时所利用的区域（FAT：文件分配表）、上述存储器 4 的整体的校验和（验算值）、在上次处理结束时在存储器 4 中所记录的内容的校验和（验算值）等。由此，在内部存储器 3b 中，就记录上次处理时所利用的区域（FAT：文件分配表），或者上述存储器 4 的整体的校验和，或者在上次处理的最后在存储器 4 中所记录的内容的校验和等。

另外，上述存储器 4，由非易失性的存储器所构成，保持上次已处理的存储器的状态。上述内部存储器 3b，由非易失性的存储器所构成，保持存储器 4 的状态信息。

接着，对在上述这样的结构中，进行向上述存储器 4 的访问处理时的认证处理，参照图 10 所示的流程图进行说明。

向上述存储器 4 进行的访问处理是，对从外部供给的音乐信息或程序进行记录，或者对所记录的音乐信息或程序进行再现等。

即，控制单元 3a 在向存储器 4 进行访问时，确认存储器 4 的记录状态（ST11），并判断上次处理时所利用的区域（FAT）（ST12）。接着，控制单元 3a 对此所判断出的上次处理时所利用的区域（FAT）与记录在上述内部存储器 3b 中的上次处理时所利用的区域（FAT）是否一致（ST13）进行比较。

控制单元 3a 在此比较的结果为两者相一致时，进行称为存储器 4 为正确的认证（认证确认）（ST14），并执行向上述存储器 4 的访问处理（ST15）。作为此访问处理，例如，进行数据的记录（写入），或者所记录的数据的再现（读出）。

在执行此访问处理后，控制单元 3a 将由此访问处理所利用的区

域（FAT）记录到（重写）上述内部存储器3b（ST16）。

另外，控制单元3a在通过上述步骤13的比较的结果为两者不一致时，设认证为NG并中止访问处理（ST17）。

尽管在上述例子中，作为存储器4的状态信息，以FAT为例进行了说明，但在上述存储器4的整体的校验和（验算值）、或者在上次处理的最后在存储器4中所记录的内容的校验和（验算值）等的情况下也可以同样地进行实施。

对在上述上次处理的最后，如图11所示那样，将音乐信息“A”以长度“BB”记录到存储器4的地址“AAAA”的情况中的存储器状态信息的记录处理和认证处理，参照图12所示的流程图进行说明。

即，控制单元3a，计算出对于上述音乐信息“A”的校验和（验算值）“CC”（ST21）。

接着，控制单元3a，通过将上述存储器4的记录开始地址“AAAA”、记录信息的长度“BB”和上述所计算出的校验和（验算值）“CC”附加给预先赋予上述音乐信息“A”的信息ID，生成存储器状态信息（ST22），如图13所示那样，记录在内部存储器3b中（ST23）。

然后，控制单元3a接着在向存储器4进行访问时（ST24），确认存储器4的记录状态（ST25），判断在上次处理的最后从存储器4的地址“AAAA”记录了长度为“BB”的信息（ST26）。

接着，控制单元3a计算对于从存储器4的地址“AAAA”得到的长度“BB”的信息的校验和（验算值）“CC”（ST27）。

然后，控制单元3a通过上述所判断的地址“AAAA”、长度“BB”和所计算出的校验和（验算值）“CC”判断为存储器状态信息（ST28），比较此存储器状态信息与从内部存储器3b读出的上次处理时的存储器状态信息是否一致（ST29）。

控制单元3a在此比较的结果为两者相一致时，进行称为存储器4为正确的认证（认证确认）（ST30），并执行向上述存储器4的访问

处理（ST31）。

另外，控制单元3a在通过上述步骤29的比较结果为两者不一致时，设认证为NG并中止访问处理（ST32）。

[第三实施形式]

接着，对在上述这样的结构中，使用在不可改写的状态下记录到上述存储器4中的认证密钥的加密数据，和在不可改写的状态下记录到上述内部存储器3b中的认证密钥部、解码程序和加密密钥，来进行上述存储器4的认证的实施形式进行说明。

在此情况下，在上述存储器4中，如图14所示那样，预先记录用唯一的加密密钥对认证密钥进行加密后的加密数据，而且是不能改写地进行记录。

另外，在上述内部存储器3b中，如图14所示那样，不能改写地记录与在上述存储器4中所记录的加密数据的加密前的认证密钥相同的认证密钥，对在上述存储器4中所记录的加密数据进行解码的解码程序，以及在由此解码程序对加密数据进行解码时的加密密钥。

上述存储器4和内部存储器3b，由不可改写的ROM单元和可改写的ROM单元组成，在此不可改写的ROM单元中记录有上述认证密钥。

接着，对在上述这样的结构中，上述存储器4的认证处理，参照图15所示的流程图进行说明。

即，控制单元3a读出记录在存储器4中的加密数据（ST41）。接着，控制单元3a通过基于记录在内部存储器3b中的解码程序，用记录在内部存储器3b中的加密密钥对上述所读出的加密数据进行解码，得到认证密钥（ST42）。进而，控制单元3a比较此所得到的认证密钥与记录在内部存储器3b中的认证密钥是否一致（ST43）。

控制单元3a在此比较的结果为两者的认证密钥相一致时，进行称为存储器4为正确的认证（认证确认）（ST44）。

另外，控制单元3a在通过上述步骤43的比较的结果为两者不一致时，设认证为NG（ST45）。

另外，也可以将为了用于与存储器 4 进行认证而记录在内部存储器 3b 中的认证密钥用于外部装置和存储卡 M 间的认证。进而，如图 16 所示那样，也可以在存储卡 M 的内部存储器 3b 中，存储用于与存储器 4 的认证的内部认证密钥 K1，和用于与外部装置的认证的外部认证密钥 K2。

[第四实施形式]

接着，对在上述这样的结构中，在对来自外部装置的接收数据进行加密并记录到上述存储器 4 时，使用通过上述第三实施形式的认证处理（步骤 41～45），和通过上述第二实施形式的认证处理（步骤 11～14），来进行上述存储器 4 的认证的实施形式进行说明。

在此情况下，在上述存储器 4 中，如图 17 所示那样，预先记录用唯一的加密密钥对认证密钥进行了加密的加密数据，而且是不能改写地进行记录。

另外，在上述内部存储器 3b 中，如图 17 所示那样，不能改写地记录与在上述存储器 4 中所记录的加密数据的加密前的认证密钥相同的认证密钥，对来自上述外部装置的接收数据进行加密的加密程序，对在上述存储器 4 中所记录的加密数据进行解码的解码程序，以及在由上述加密码程序对接收数据进行加密时和在由上述解码程序对加密数据进行解码时的加密密钥。

另外，在内部存储器 3b 中，如图 17 所示那样，记录上次处理时所利用的区域（FAT：文件分配表），或者上述存储器 4 的整体的校验和，或者在上次处理的最后在存储器 4 中所记录的内容的校验和等。

上述存储器 4 和内部存储器 3b，由不可改写的 ROM 单元和可改写的 ROM 单元组成，在此不可改写的 ROM 单元中记录有上述认证密钥。可改写的 ROM 单元，由非易失性的存储器所构成，保持上次已处理的存储器的状态。

接着，对在上述这样的结构中，来自上述外部装置的数据接收时的认证处理，参照图 18 所示的流程图进行说明。

即，控制单元 3a 在从外部装置接收到数据时（ST51），进行通

过上述第三实施形式的认证处理（ST52），进而进行通过上述第二实施形式的认证处理（ST53）。

控制单元 3a 在此结果为各认证处理是确认时（ST54），基于记录在内部存储器 3b 中的加密程序，用记录在内部存储器 3b 中的加密密钥对上述所接收的数据进行加密（ST55）。

接着，控制单元 3a 将此所加密的数据记录到存储器 4（ST56）。

在此记录结束后，控制单元 3a 将存储器 4 的状态记录到（重写）上述内部存储器 3b（ST57）。

另外，控制单元 3a 在任一个的认证处理是 NG 时，中止处理（ST58）。

此外，在对记录在上述存储器 4 中的被加密的数据进行解码再现的情况下也与上述同样地进行动作。

作为向上述存储器 4 所记录的数据，可以是音乐信息或程序等。

另外，也可以将为了用于与存储器 4 进行认证而记录在内部存储器 3b 中的认证密钥用于外部装置和存储卡 M 间的认证。进而，如图 19 所示那样，也可以在存储卡 M 的内部存储器 3b 中，存储用于与存储器 4 的认证的内部认证密钥 K1，和用于与外部装置的认证的外部认证密钥 K2。

[第五实施形式]

接着，说明具有上述认证功能的存储卡 M 的利用例。

参照图 20、图 21 来说明，例如将存储卡 M 使用于因特网连接系统的情况的例子。

即，图 20 是表示利用了具有上述内置的存储器确认用的认证功能的存储卡 M 的因特网连接系统的整体结构的图。

在该图中，PC（个人计算机）11、作为移动电话的例如便携电话 12、电子照相机 13 以及 TV 装置（电视装置）14 的各电子设备，不管怎样都备有可以安装预定的可移式记录介质，例如具有不能从外部直接访问被隐藏的存储区域的邮票大小的存储卡 M 的卡槽，和对向因特网 15 等进行连接所必要的调制解调器等的通信接口（没有图示）。

在本实施形式中，在存储卡 M 的存储器 4 中，为了可以从该存储卡 M（在卡槽中）所安装的电子设备（通过因特网供应商的服务器，也就是通过供应商方）连接到因特网 15，登录有用户 ID、用户密码、邮件帐户、邮件密码、DNS（DNS 服务器地址）、访问接口（连接对象的电话号码）等组成的因特网连接信息 150。在此存储卡 M 的存储器 4 中所登录的因特网连接信息 150 的数据格式，统一成与上述 PC11、便携电话 12、电子照相机 13 以及 TV 装置等各种电子设备（装置）无关的预定格式。

另外，在 PC11 中搭载有记录了用于在存储卡 M 安装在自身的卡槽时自动地启动，从该存储卡 M 的存储器 4 读出预定格式的因特网连接信息 150 并自动连接到因特网 15 的特定的应用程序（因特网连接设定应用程序）110 的（可计算机读取的）上述存储器 4。在此进行存储卡 M 的启动时，进行利用上述第一、第二、第三实施形式的内置的存储器确认用的认证处理。另外，在存储器的认证为确认的情况下，进而可以使用存储在存储卡 M 内的内部存储器 3b 的认证密钥在与作为外部装置的 PC11 之间进行识别。然后，在这些认证为确认时，启动上述特定的应用程序。

另外，在便携电话 12、电子照相机 13 以及 TV 装置 14 等其他种类的电子设备中也搭载有记录了因特网连接设定应用程序（下面，称为应用）110 的记录介质。此记录介质是 ROM、磁盘装置、闪存等。此外，应用 110 也可以通过通信线路来进行下载。

这样，通过设为在 PC11、便携电话 12、电子照相机 13 以及 TV 装置 14 等电子设备中搭载应用（因特网连接设定应用）110 的结构，用户仅通过携带在存储器 4 中登录有因特网连接信息 150 的存储卡 M，并将该存储卡 M 适宜地安装到上述电子设备（PC11、便携电话 12、电子照相机 13 以及 TV 装置 14 等电子设备）的卡槽，就能够简单地从该设备连接到因特网 15。在这里，由于并不依存于使用的电子设备，故用户通过交替使用一张存储卡 M，也能够从任何的设备连接到因特网 15。

于是在本实施形式中，就存在向存储卡 M 的存储器 4 进行因特网连接信息 150 的登录服务的商店。顾客将存储卡 M 带到此种商店，或者在该商店购买存储卡 M，在该商店向此存储卡 M 的存储器 4 进行因特网连接信息 150 的登录。在图 20 中，是在批发销售店 16 和便利店 17 中进行因特网连接信息登录服务的。为此，在批发销售店 16 中，就准备有搭载着记录了因特网连接信息登录用的应用（因特网连接信息登录应用程序）180 的（可计算机读取的）存储介质的 PC160。另外，在便利店 17 中，准备有搭载着不仅记录了向存储卡 M 的存储器 4 进行因特网连接信息登录用的应用（因特网连接信息登录应用）180，还记录了向存储卡 M、MD（微型磁盘）等进行数字内容下载用的应用的（可计算机读取的）存储介质的信息写入终端 170。

在批发销售店 16、便利店 17 等的因特网连接信息登录服务店中的登录服务的结果，与因特网供应商（下面，略称为供应商）18 签约的用户数（入会者数），可以按不同该供应商 18 并且按每个因特网连接信息登录服务店进行统计。于是各供应商 18，以预定的期间为单位，例如以月为单位，对本系统（可移式记录介质用因特网连接系统）的提供公司，因特网连接信息登录服务店（批发销售店 16、便利店 17 等）进行现金返还 19。

接着，参照图 21 对向图 20 的系统中的因特网连接信息登录服务店、例如批发销售店 16 中的存储卡 M 的存储器 4 进行因特网连接信息登录（写入）的服务进行说明。

首先，当在 PC160 的卡槽中，如箭头 a 所示那样安装用户的存储卡 M 后，因特网连接信息登录应用 180 就启动。于是，就在 PC160 的显示器上（与提供图 20 的系统的公司缔结有合同）显示供应商的一览画面（供应商一览画面）201。

当用户在供应商一览画面上选择所希望的供应商后，或者当批发销售店 16 的店员选择用户要求的供应商后，PC160 就按照应用 180 显示表示与此所选择的供应商间的会员合同内容的画面 202。在此画面 202 上设置有确认按钮 202a，当按下（选择）该确认按钮 202a 后，

就切换到支付方法的选择画面 203。这里当选择支付方法后，就切换到邮件帐户生成画面 204。这里，当设定用户希望的邮件帐户的候补后，PC160 通过与用户所指定的供应商服务器 210 进行线路（因特网）连接，将用户所指定的支付方法、邮件帐户发送给该服务器 210，就如箭头 b 所示那样委托确认，并切换到正在在线确认的画面 205。

用户指定的供应商的服务器 210，对用户所希望的邮件帐户从第一候补依次检查是否已经给予其他用户，如果没有给予就决定将该帐户给予用户。如果所有的候补都给予完时，就在批发销售店 16 的 PC160 从服务器 210 请求再次生成邮件帐户。

当决定用户所希望的邮件帐户的给予后，服务器 210 进而决定给予该用户的用户 ID、用户密码、邮件密码，并将包含这些信息和 DNS、访问接点，对因特网的连接所必要的信息发送给批发销售店 16 的 PC160。

于是批发销售店 16 的 PC160，基于从供应商的服务器 210 发送的信息，生成包含用户 ID、用户密码、邮件密码、DNS、访问接点的预定格式的因特网连接信息 150，按照预定的算法用后面说明的介质密钥 Km 对该因特网连接信息 150 进行加密，开始向安装在该 PC160 的卡槽的存储卡 M 的存储器 4 进行写入的动作，并切换到正在信息写入的画面 206。

在向上述的存储卡 M 的存储器 4 进行写入操作时，进行上述第四实施形式的认证处理。另外，在存储器的认证为确认的情况下进而可以使用存储在存储卡 M 内的内部存储器 3b 中的认证密钥在与作为外部装置的 PC11 之间进行认证。然后，在这些认证为确认时，就开始写入动作。

当 PC160 结束向存储卡 M 的存储器 4 进行的因特网连接信息 150 的写入后，就切换到向用户询问是否用密码保护存储卡 M 的信息的询问画面 207。

如果在请求用密码进行保护的情况下，PC160 就使用户指定密码。PC160 按照预定的算法对用户指定的密码进行加密并作为密码写

入到存储卡 M。该所加密的密码，就成为用于从存储卡 M 取出介质密钥的密钥。当 PC160 将密码 311 写入存储卡 15 后，就完成一系列的因特网连接信息写入处理，也就是用户登录处理。在此情况下，PC160 在切换到表示用户登录完毕的画面 208 的同时，例如经由因特网如箭头 c 所示那样将用户登录完毕，通知给开发本系统的公司（系统提供公司）所有的合同计数服务器 211。另一方面，在没有请求用密码进行包含的情况下，PC160 在直接切换到用户登录完毕画面 208 的同时，如箭头 c 所示那样将用户登录完毕通知给合同计数服务器 211。在此用户登录完毕通知中，包含有用户所签约的供应商的信息。

合同计数服务器 211，按各供应商并且按每个批发销售店 16 等的因特网连接信息登录服务店来计数（统计）与各供应商签约的用户数（入会者数）。于是，当从批发销售店 16 的 PC160 通知用户登录完毕后，合同计数服务器 211，就使所通知的供应商的入会者数计数加 1，使进行连接到该供应商用的因特网连接信息的登录服务的商店（批发销售店 16）所接待的入会者数计数加 1。

如上述那样，作为防止伪造存储卡的技术向存储器的某区域写入成为密钥的数据，在存储器控制用 LSI 中对该密钥数据进行认证，仅在一致的情况下进行向存储器的访问就成为可能。

为此，例如既便替换成存储器容量大的存储器，由于存储器控制用 LSI 的认证不一致故也不能对存储器进行访问。

同样，既便欲对于一个存储器控制用 LSI，使用好几个存储器，由于认证不一致故也不能对存储器进行访问。

另外，对密钥数据进行加密以使不能解析存储器内的密钥数据也是有效的。

本发明，提供一种由包括记录数据的存储器，控制向此存储器进行数据的记录或者控制在上述存储器中所记录的数据的再现的控制单元，此控制单元所使用的内置内部存储器的存储器控制用 LSI 所构成的存储卡，上述控制单元，根据记录在上述存储器中的认证密钥与记录在上述内部存储器中的认证密钥是否一致，来判断上述存储器是否正确。

图1

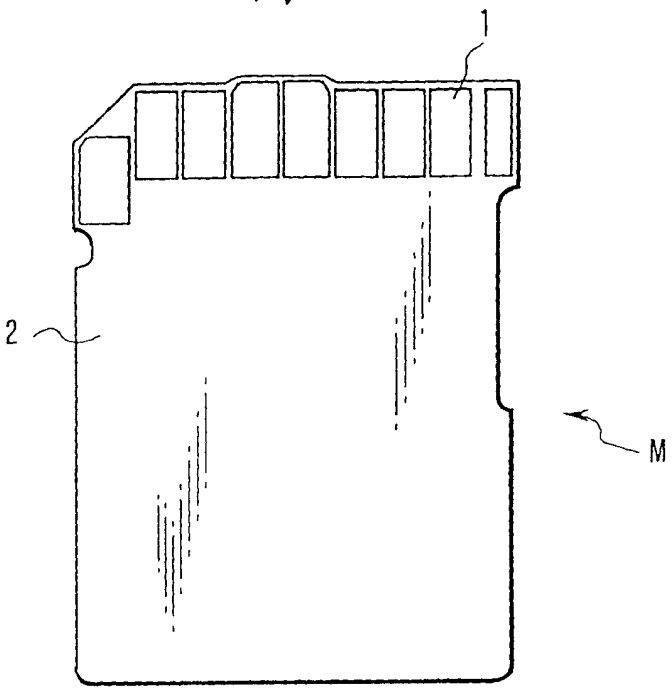


图2

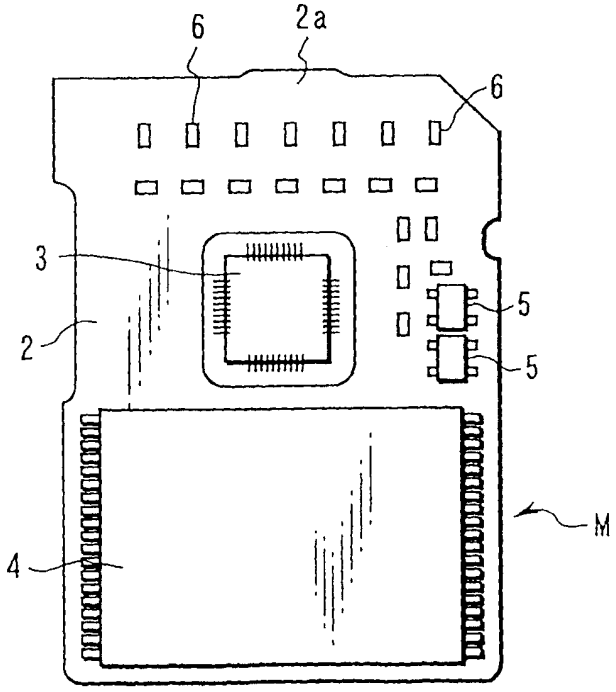


图3

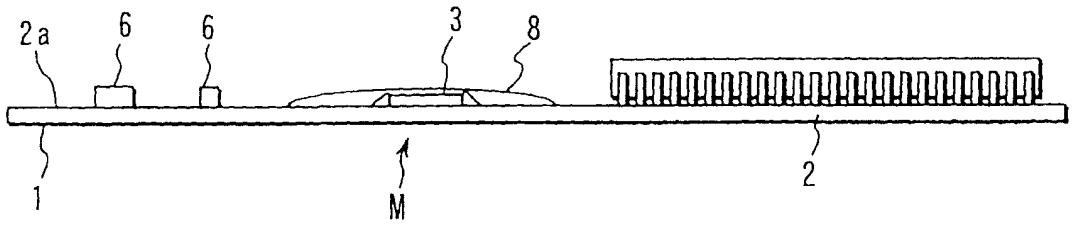


图4

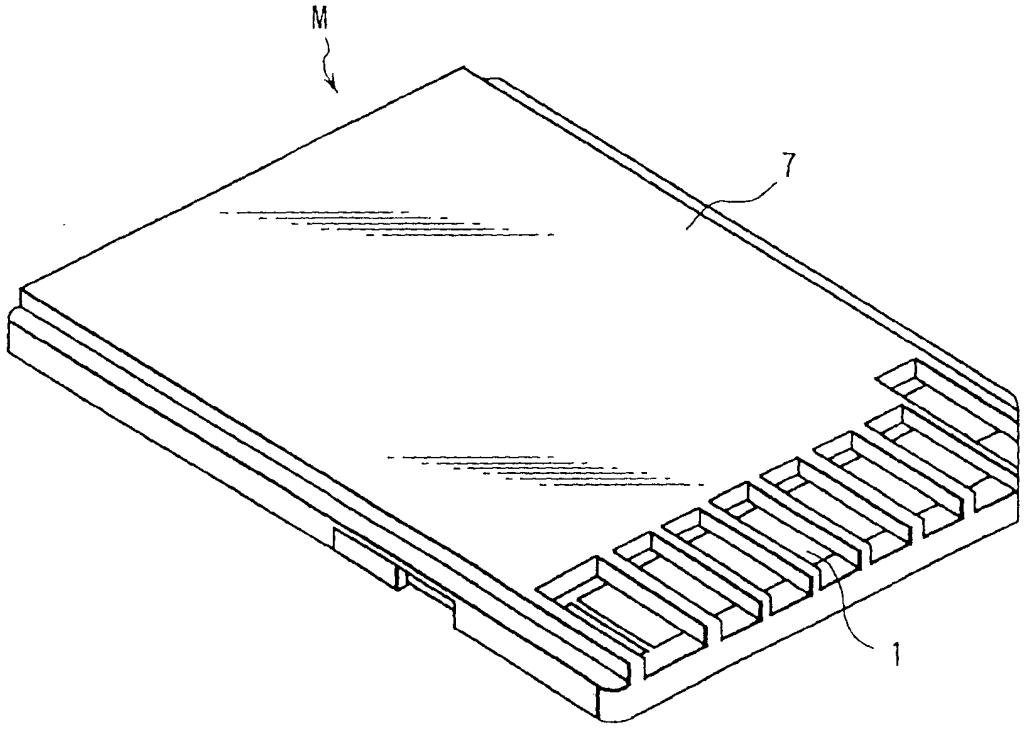


图5

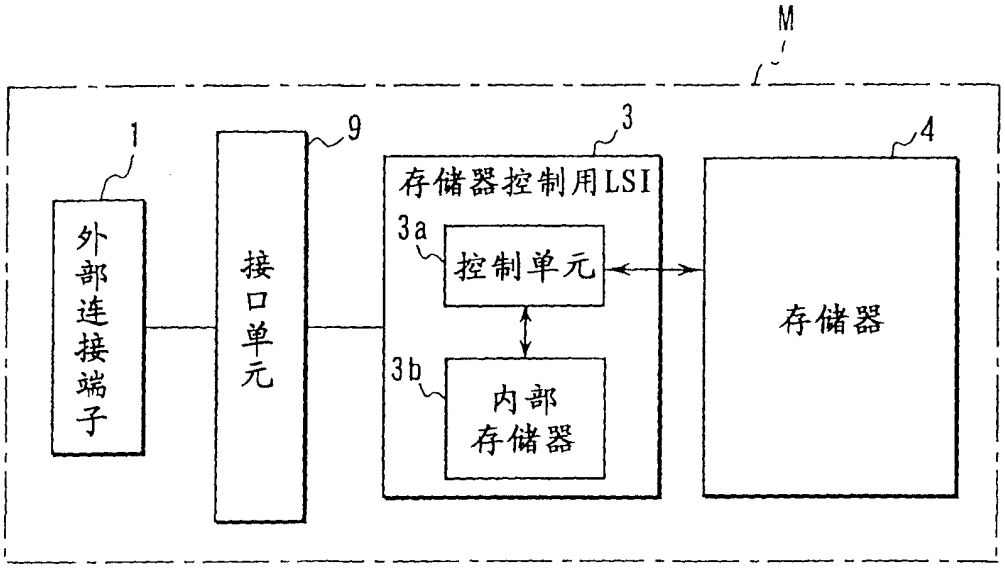

M
1
外部连接端子
9
接口单元
3
存储器控制用LSI
3a
控制单元
3b
内部存储器
4
存储器

图6

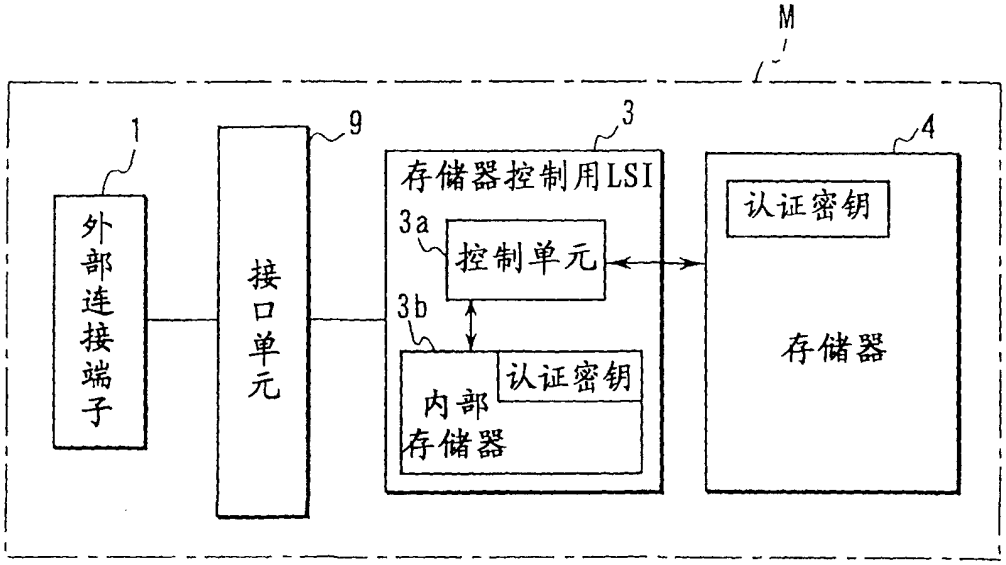

M
1
外部连接端子
9
接口单元
3
存储器控制用LSI
3a
控制单元
3b
认证密钥
内部存储器
4
认证密钥
存储器

图7

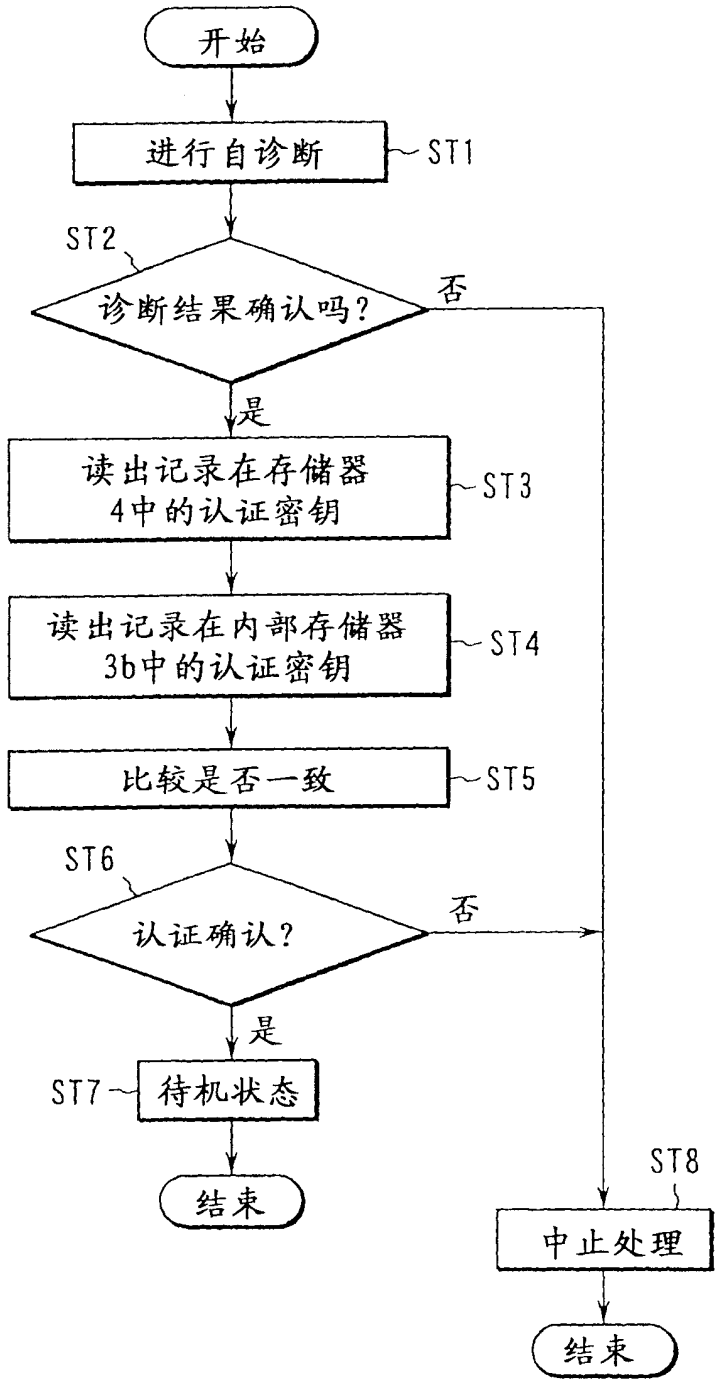

开始
进行自诊断
ST1
ST2
诊断结果确认吗?
否
是
读出记录在存储器4中的认证密钥
ST3
读出记录在内部存储器3b中的认证密钥
ST4
比较是否一致
ST5
ST6
认证确认?
否
是
ST7
待机状态
结束
ST8
中止处理
结束

图8

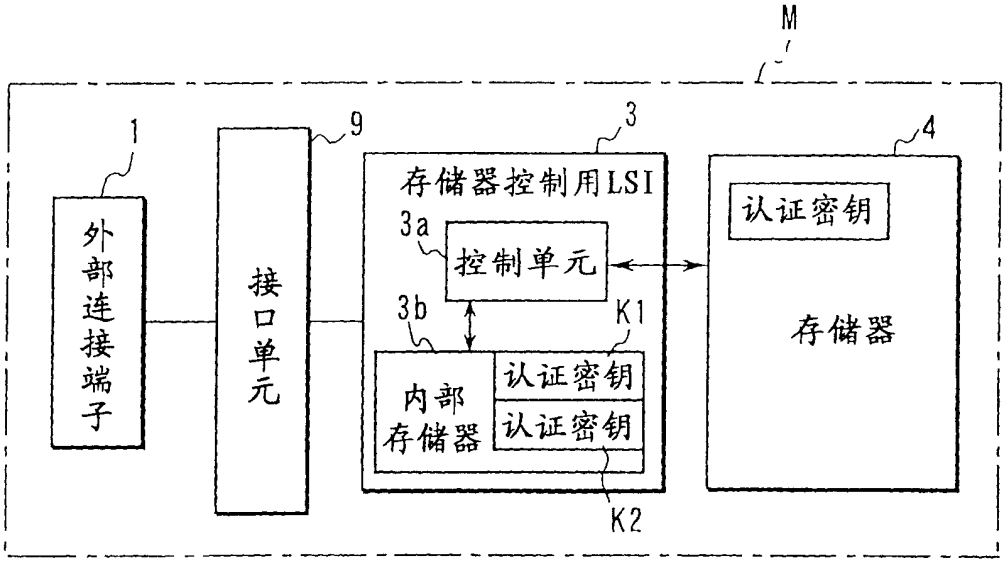

M
1
外部连接端子
9
接口单元
3
存储器控制用LSI
3a
控制单元
3b
K1
内部存储器
认证密钥
认证密钥
K2
4
认证密钥
存储器

图9

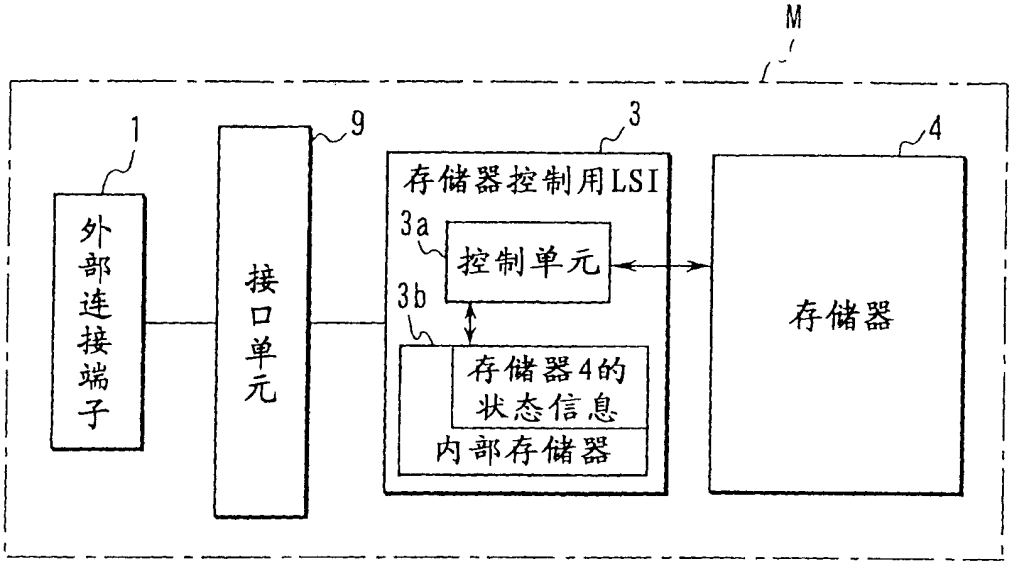

M
1
外部连接端子
9
接口单元
3
存储器控制用LSI
3a
控制单元
3b
存储器4的状态信息
内部存储器
4
存储器

图11

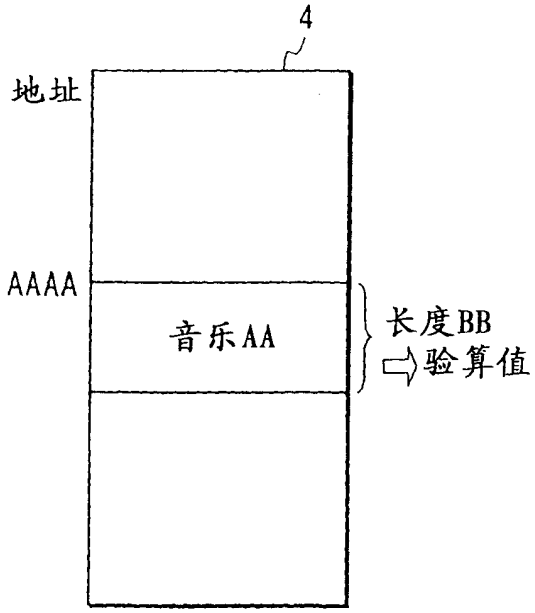

4
地址
AAAA
音乐AA
长度BB
验算值

图13

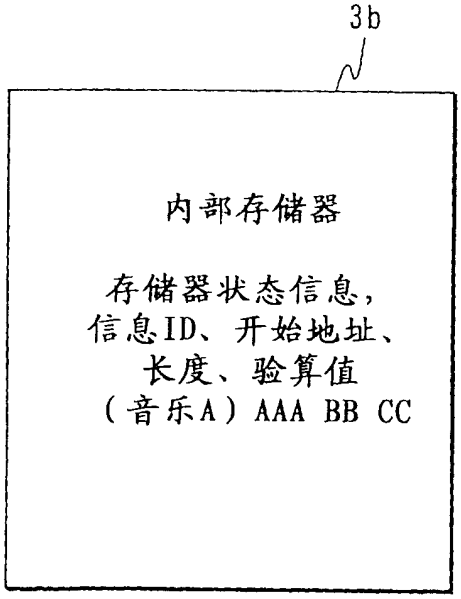

3b
内部存储器
存储器状态信息，
信息ID、开始地址、
长度、验算值
（音乐A）AAA BB CC

图10

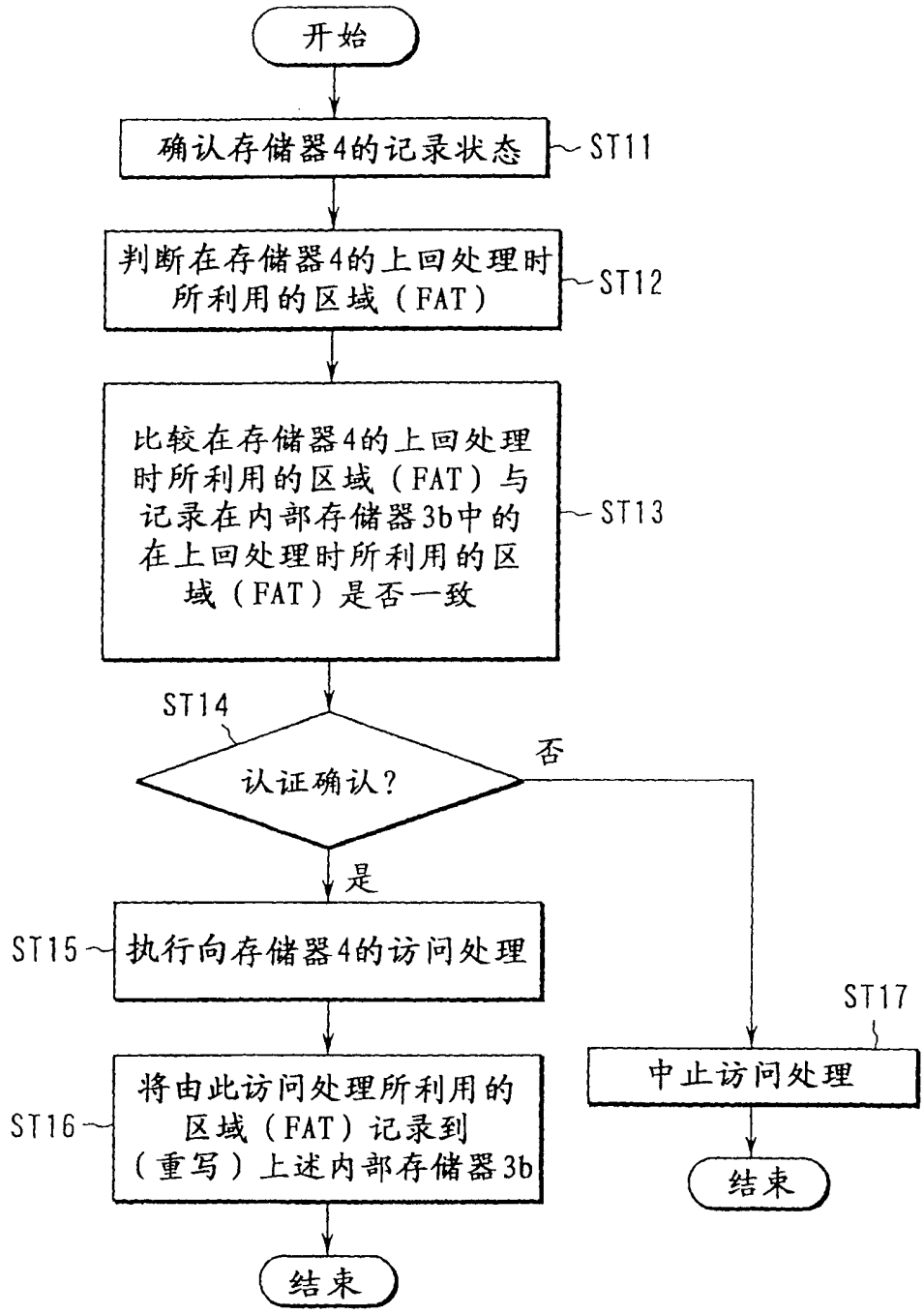

开始
确认存储器4的记录状态
ST11
判断在存储器4的上回处理时所利用的区域（FAT）
ST12
比较在存储器4的上回处理时所利用的区域（FAT）与记录在内部存储器3b中的在上回处理时所利用的区域（FAT）是否一致
ST13
ST14
认证确认？
否
是
ST15
执行向存储器4的访问处理
ST16
将由此访问处理所利用的区域（FAT）记录到（重写）上述内部存储器3b
结束
ST17
中止访问处理
结束

图12

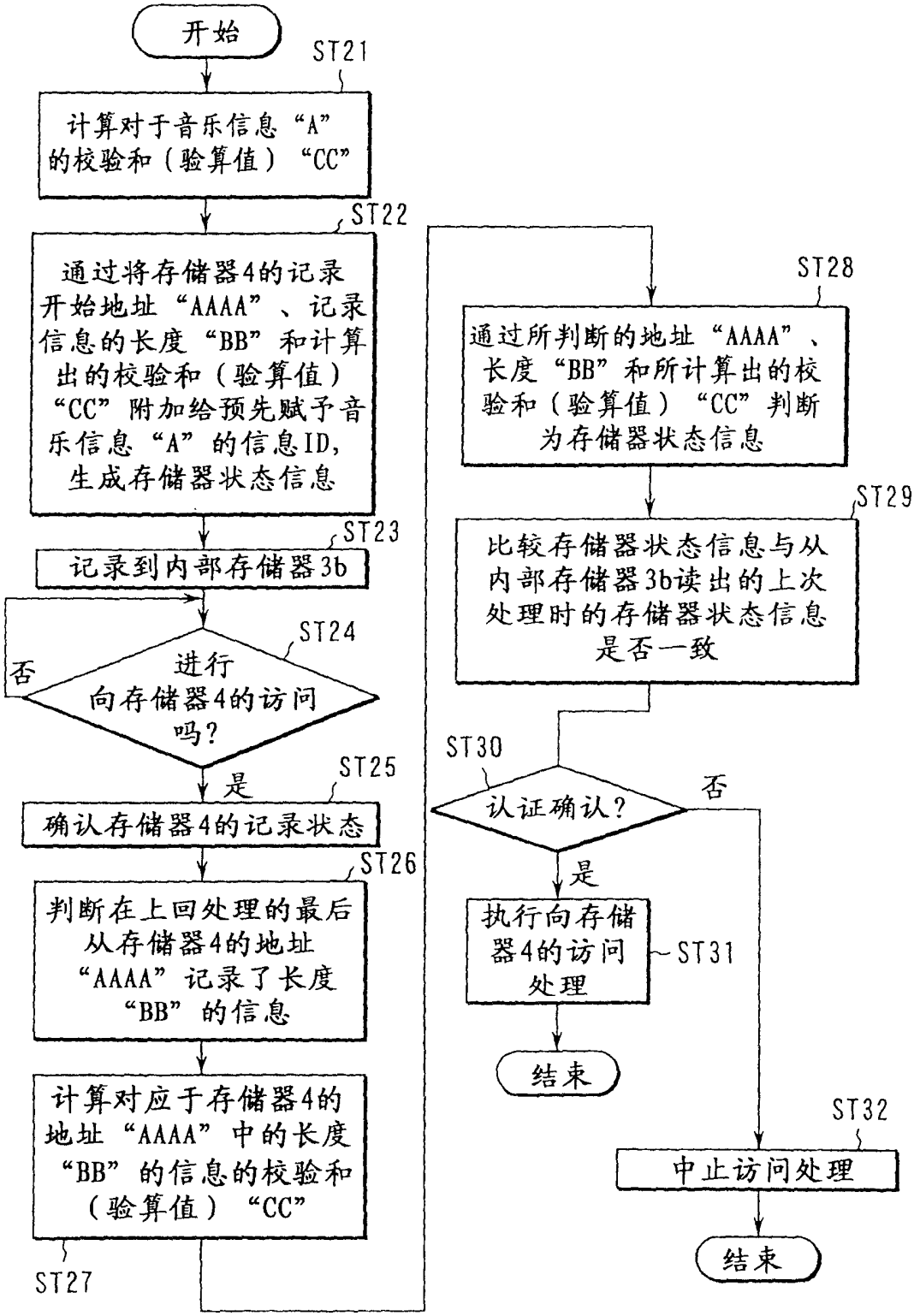

开始
ST21
计算对于音乐信息“A”的校验和（验算值）“CC”
ST22
通过将存储器4的记录开始地址“AAAA”、记录信息的长度“BB”和计算出的校验和（验算值）“CC”附加给预先赋予音乐信息“A”的信息ID，生成存储器状态信息
ST23
记录到内部存储器3b
ST24
进行向存储器4的访问吗？
否
是
ST25
确认存储器4的记录状态
ST26
判断在上回处理的最后从存储器4的地址“AAAA”记录了长度“BB”的信息
计算对应于存储器4的地址“AAAA”中的长度“BB”的信息的校验和（验算值）“CC”
ST27
ST28
通过所判断的地址“AAAA”、长度“BB”和所计算出的校验和（验算值）“CC”判断为存储器状态信息
ST29
比较存储器状态信息与从内部存储器3b读出的上次处理时的存储器状态信息是否一致
ST30
认证确认？
否
是
执行向存储器4的访问处理
ST31
结束
ST32
中止访问处理
结束

图14

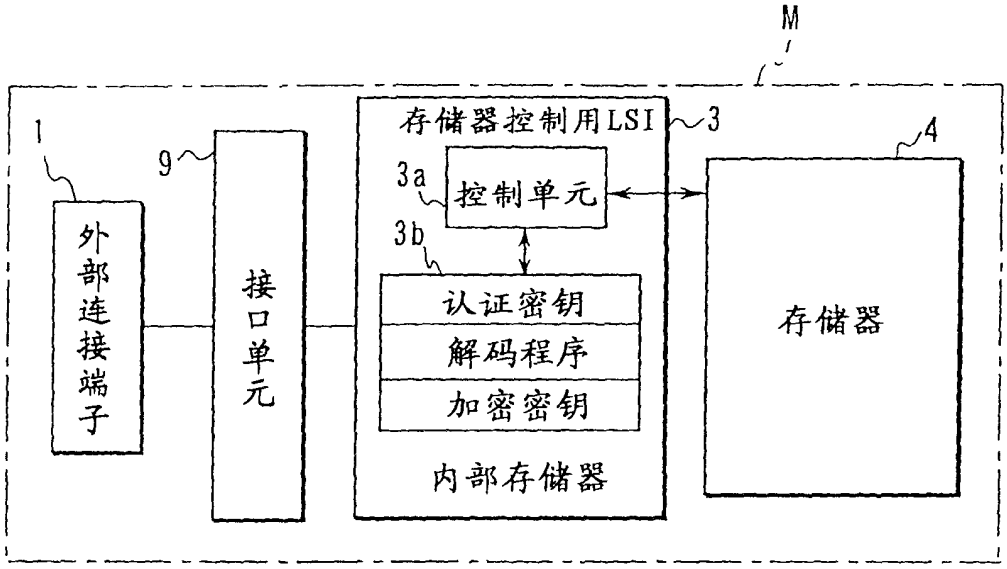

M
1
外部连接端子
9
接口单元
存储器控制用LSI
3
3a
控制单元
3b
认证密钥
解码程序
加密密钥
内部存储器
4
存储器

图17

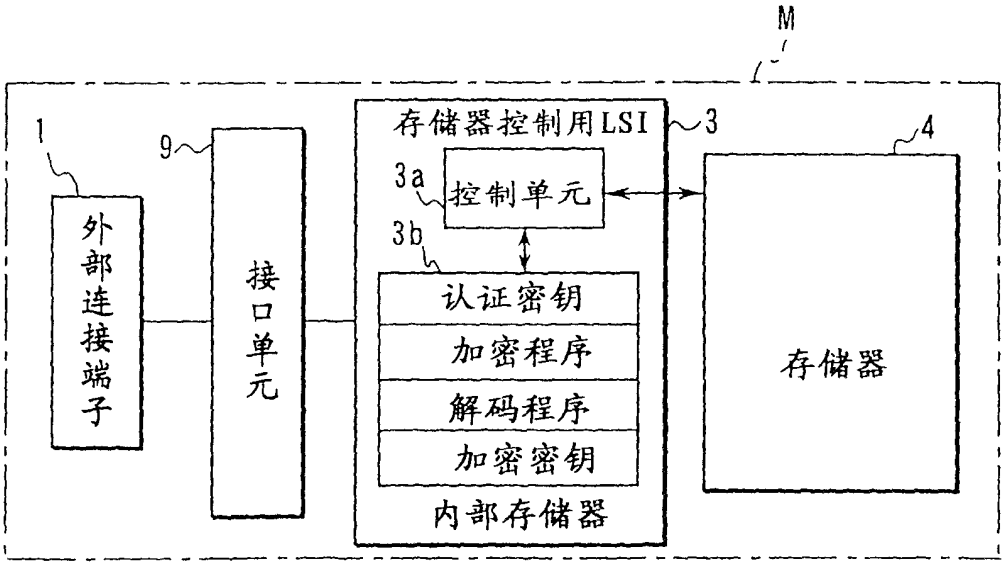

M
1
外部连接端子
9
接口单元
存储器控制用LSI
3
3a
控制单元
3b
认证密钥
加密程序
解码程序
加密密钥
内部存储器
4
存储器

图15

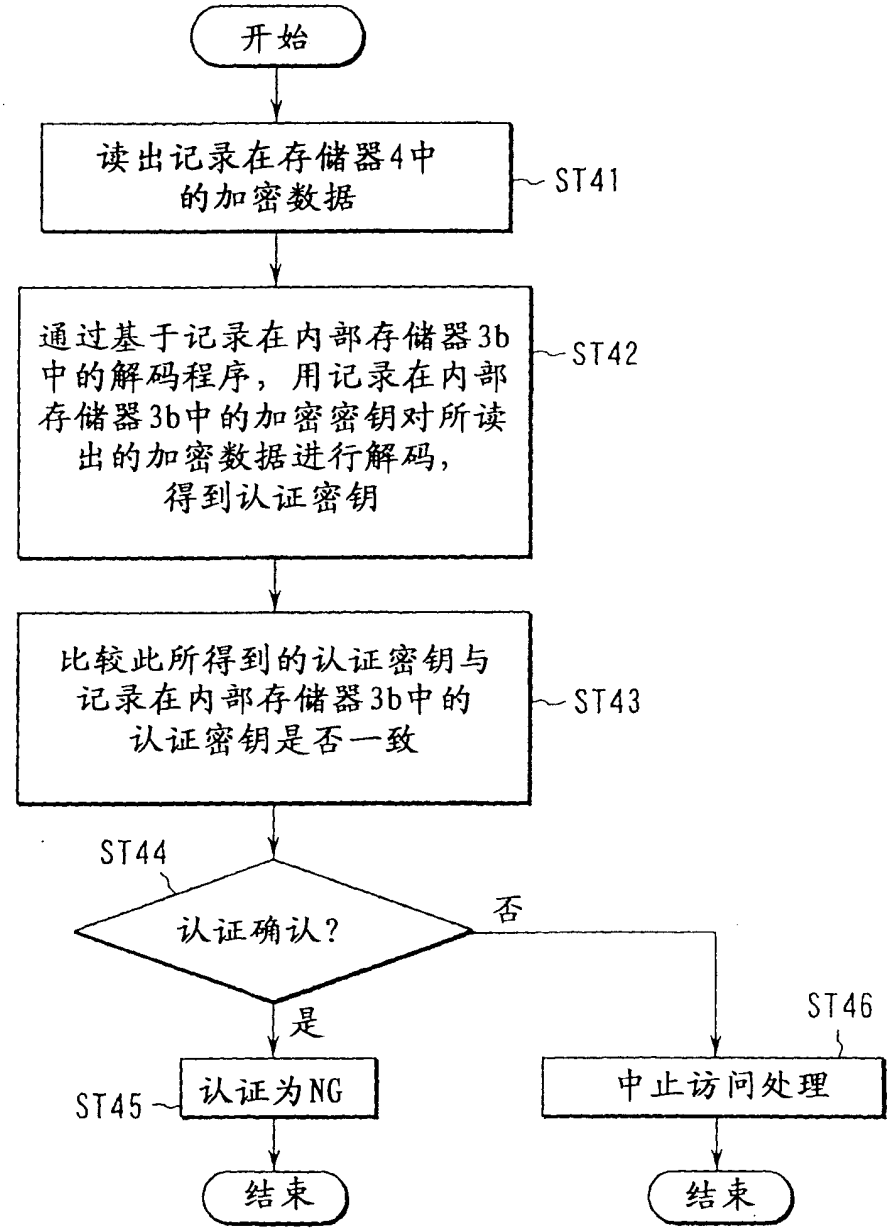

开始
读出记录在存储器4中的加密数据
ST41
通过基于记录在内部存储器3b中的解码程序，用记录在内部存储器3b中的加密密钥对所读出的加密数据进行解码，得到认证密钥
ST42
比较此所得到的认证密钥与记录在内部存储器3b中的认证密钥是否一致
ST43
ST44
认证确认?
否
是
ST46
ST45
认证为NG
中止访问处理
结束
结束

图16

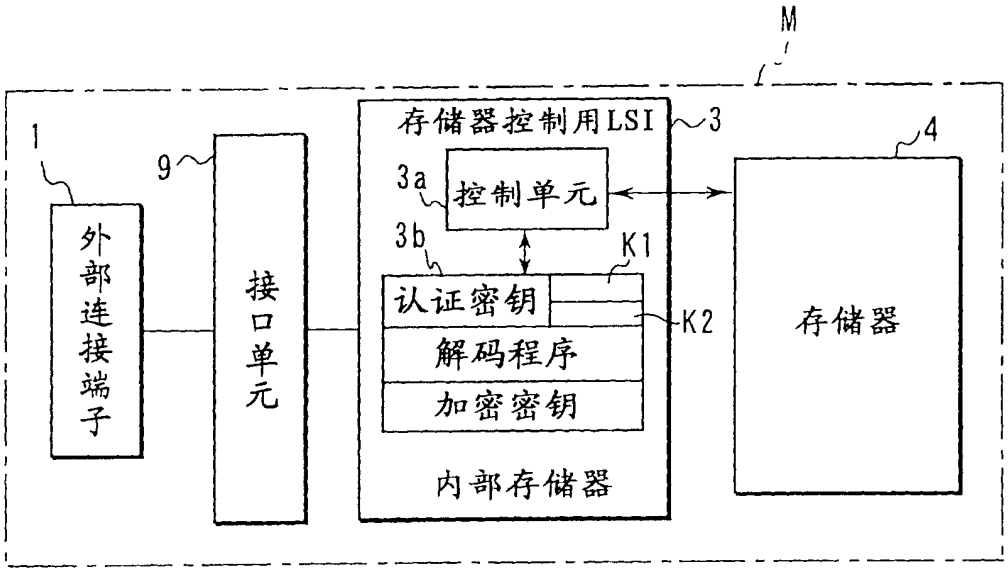

M
存储器控制用LSI
3
1
9
4
3a
控制单元
3b
K1
外部连接端子
接口单元
认证密钥
K2
存储器
解码程序
加密密钥
内部存储器

图19

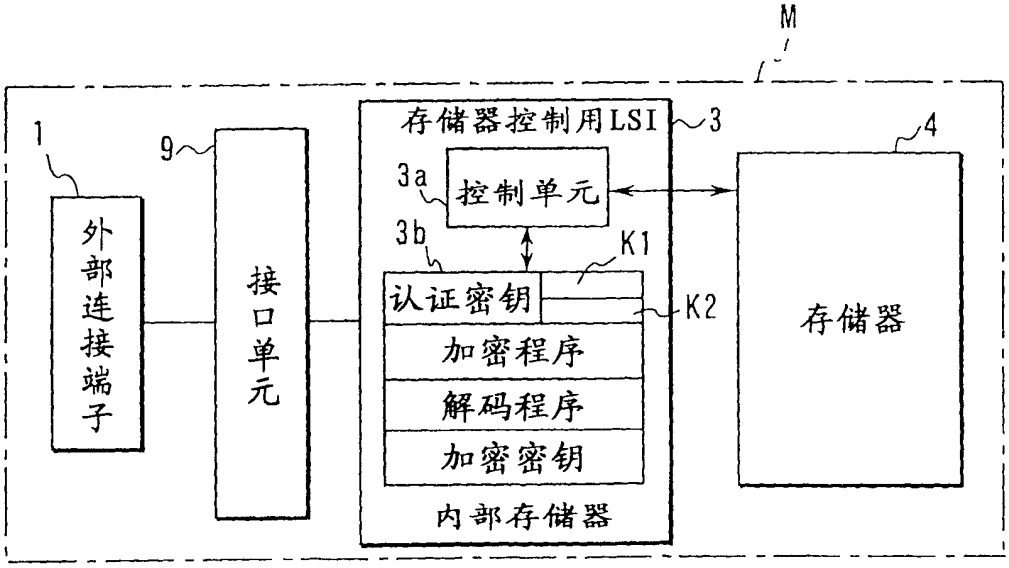

M
存储器控制用LSI
3
1
9
4
3a
控制单元
3b
K1
外部连接端子
接口单元
认证密钥
K2
存储器
加密程序
解码程序
加密密钥
内部存储器

图18

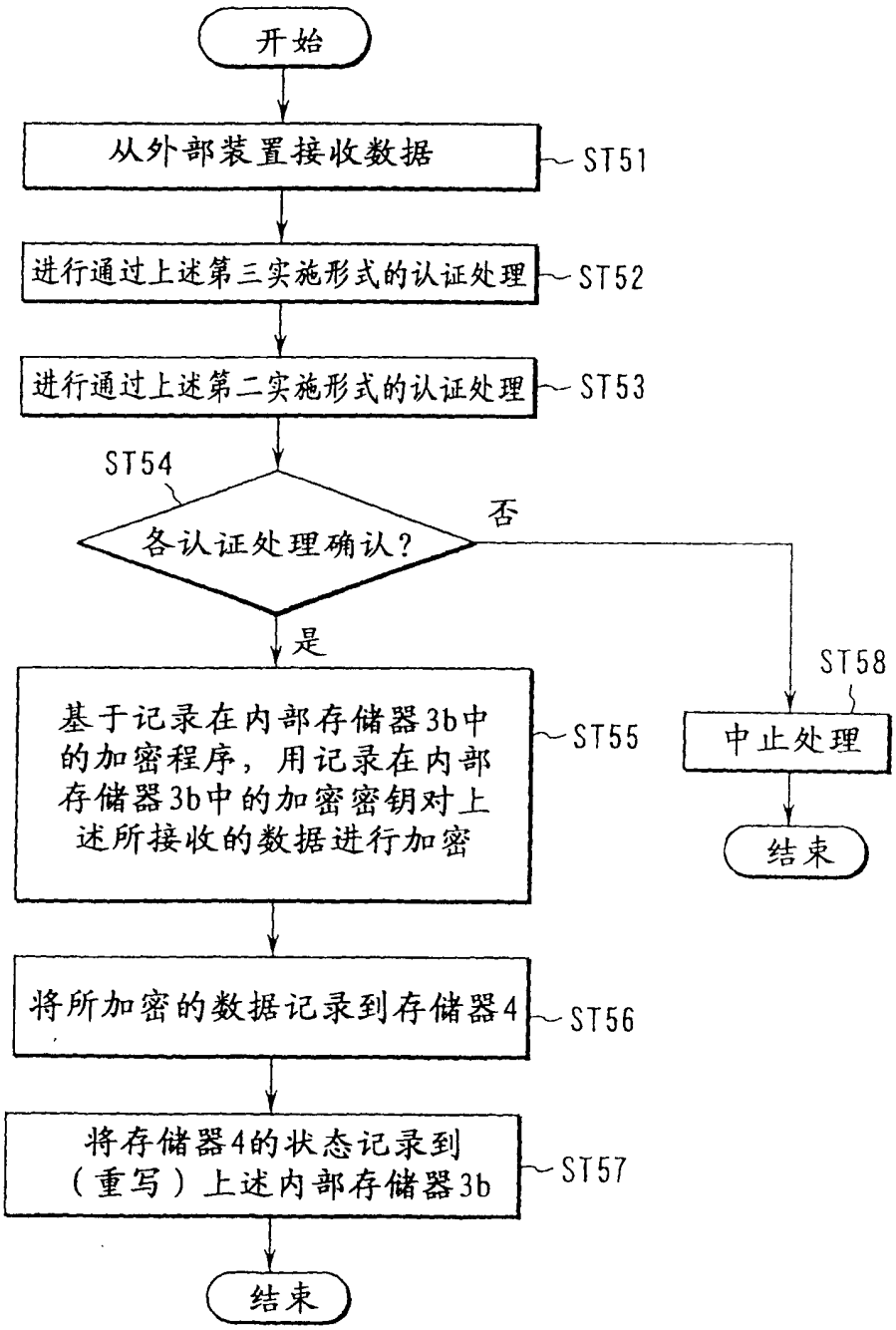

开始
从外部装置接收数据
ST51
进行通过上述第三实施形式的认证处理
ST52
进行通过上述第二实施形式的认证处理
ST53
ST54
各认证处理确认？
否
是
基于记录在内部存储器3b中的加密程序，用记录在内部存储器3b中的加密密钥对上述所接收的数据进行加密
ST55
ST58
中止处理
结束
将所加密的数据记录到存储器4
ST56
将存储器4的状态记录到（重写）上述内部存储器3b
ST57
结束

图20

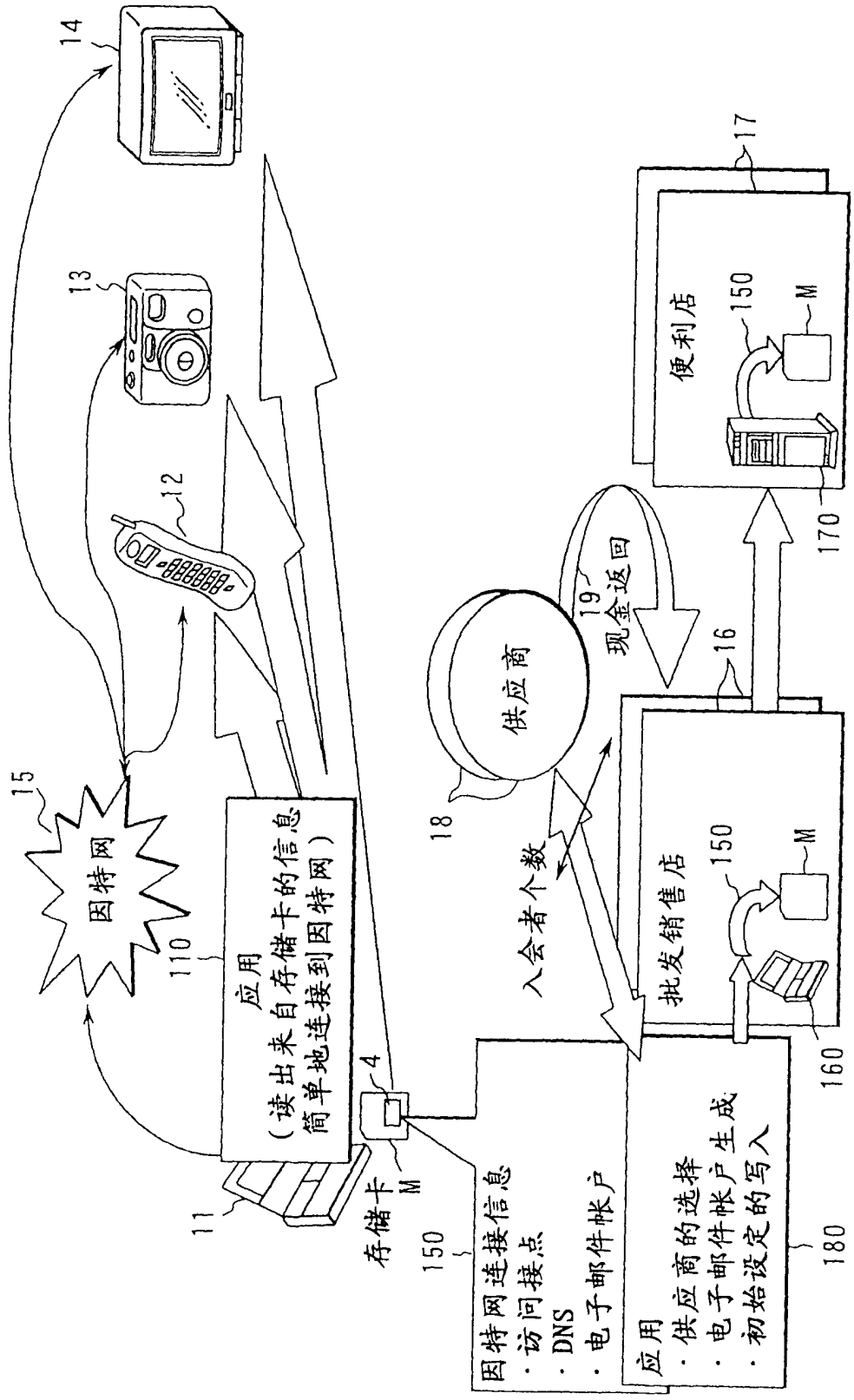
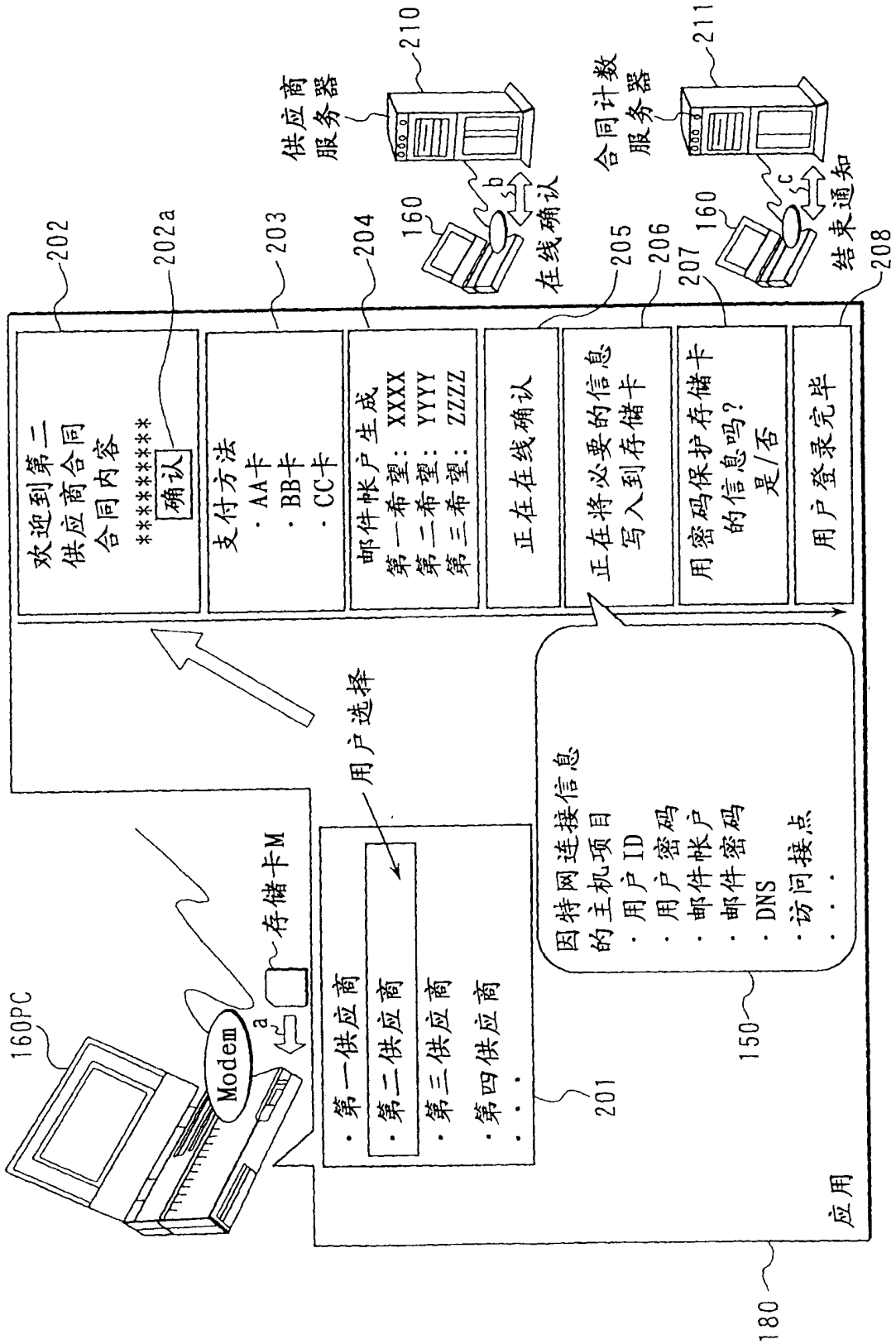

14
13
12
15
因特网
110
应用
（读出来自存储卡的信息
简单地连接到因特网）
11
4
存储卡
M
150
因特网连接信息
·访问接点
·DNS
·电子邮件帐户
应用
·供应商的选择
·电子邮件帐户生成
·初始设定的写入
180
入会者个数
18
供应商
19
现金返回
16
批发销售店
150
M
160
17
便利店
150
M
170

图21


160PC
Modem
a
存储卡M
用户选择
·第一供应商
·第二供应商
·第三供应商
·第四供应商
·
·
·
201
因特网连接信息
的主机项目
·用户ID
·用户密码
·邮件帐户
·邮件密码
·DNS
·访问接点
·
·
·
150
应用
180
欢迎到第二
供应商合同
合同内容
****
确认
202
202a
支付方法
·AA卡
·BB卡
·CC卡
203
邮件帐户生成
第一希望：XXXX
第二希望：YYYY
第三希望：ZZZZ
204
正在在线确认
205
正在将必要的信息
写入到存储卡
206
用密码保护存储卡
的信息吗？
是/否
207
用户登录完毕
208
供应商
服务器
210
b
在线确认
160
合同计数
服务器
211
c
结束通知
160