

[19] 中华人民共和国国家知识产权局



[12] 发明专利申请公布说明书

[21] 申请号 200580007957.8

[51] Int. Cl.

G06F 12/14 (2006.01)

G06K 17/00 (2006.01)

H04M 1/725 (2006.01)

H04M 11/00 (2006.01)

H04Q 7/38 (2006.01)

[43] 公开日 2007 年 3 月 14 日

[11] 公开号 CN 1930557A

[22] 申请日 2005.6.6

[21] 申请号 200580007957.8

[30] 优先权

[32] 2004. 6. 11 [33] JP [31] 174625/2004

[86] 国际申请 PCT/JP2005/010363 2005.6.6

[87] 国际公布 WO2005/121974 日 2005.12.22

[85] 进入国家阶段日期 2006.9.12

[71] 申请人 株式会社 NTT 都科摩

地址 日本东京

[72] 发明人 服部易宪

[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 曲 瑞

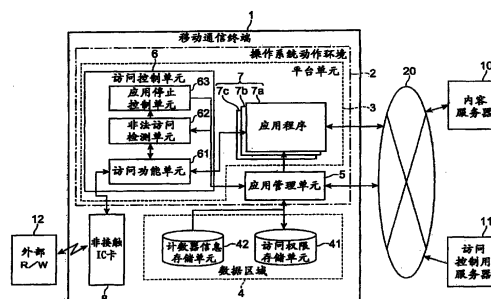
权利要求书 2 页 说明书 11 页 附图 5 页

[54] 发明名称

移动通信终端以及数据访问控制方法

[57] 摘要

该移动通信终端(1)具备:非接触 IC 卡(8);
作为用于使应用程序(7)动作的应用程序接口的平台单元(3);控制应用程序(7)的起动以及停止的应用管理单元(5);以及在平台单元(3)内动作,对从应用程序(7)向非接触 IC 卡(8)的访问进行中继的访问控制单元(6),其中访问控制单元(6)在检测出从应用程序(7)向非接触 IC 卡(8)的非法访问的情况下,向应用管理单元(5)指示停止应用程序(7)。



1.一种移动通信终端，其特征在于，具备：

非接触 IC 卡；

平台单元，作为用于使应用程序动作的应用程序接口；

应用管理单元，控制应用程序的起动以及停止；以及

访问控制单元，在上述平台单元内动作，对从应用程序向上述非接触 IC 卡的访问进行中继，

其中，上述访问控制单元在检测出从应用程序向上述非接触 IC 卡的非法访问的情况下，向上述应用管理单元指示停止上述应用程序。

2.根据权利要求 1 所述的移动通信终端，其特征在于，

还具备：访问权限存储单元，存储表示应用程序对上述非接触 IC 卡的访问权限的访问权限信息，

上述访问控制单元根据在存储于上述访问权限存储单元内的上述访问权限信息中是否允许应用程序对上述非接触 IC 卡的访问，来进行上述非法访问的检测。

3.根据权利要求 1 或 2 所述的移动通信终端，其特征在于，

上述访问控制单元在从应用程序接收到包含用于确定非接触 IC 卡中的数据存储区域的数据存储区域信息的访问请求后，从上述非接触 IC 卡接收针对上述访问请求的应答，

根据在该接收到的应答中是否包含表示访问失败的信息，来进行上述非法访问的检测。

4.根据权利要求 1~3 中任意一项所述的移动通信终端，其特征在于，

上述访问控制单元在从应用程序接收到包含用于访问非接触 IC 卡的认证代码的访问请求后，从上述非接触 IC 卡接收针对上述访问请求的应答，

根据在该接收到的应答中是否包含表示访问失败的信息，来进行上述非法访问的检测。

5.一种数据访问控制方法，控制在内置有非接触 IC 卡的移动通信终端内的平台上动作的应用程序的数据访问，其特征在于，具备：

访问控制步骤，在上述平台单元内动作的访问控制单元对从应用程序向上述非接触 IC 卡的访问进行中继；以及

程序停止步骤，在上述访问控制单元检测来自应用程序的非法访问的情况下，向控制应用程序的起动以及停止的应用管理单元指示停止上述应用程序。

移动通信终端以及数据访问控制方法

技术领域

本发明涉及移动通信终端以及数据访问控制方法。

背景技术

目前,由便携电话机等移动通信终端下载并执行在游戏或电子商务交易等中使用的应用程序。这时,应用程序与设置在内容提供方等处的外部服务器进行数据通信。作为用于提高由这种应用程序进行通信时的安全性的技术,例如包括在下述专利文献1中记载的对计算机的非法入侵的应对方法。在该非法入侵应对方法中,在检测出对在计算机上公开的Web文件的非法入侵的情况下,通过强制结束操作系统来禁止非法访问。

专利文献1:特开2003-263413号公报

发明内容

发明所要解决的技术问题

然而,在上述的非法入侵应对方法中,虽然能够检测出经由网络的来自外部的非法访问,但是难以检测出内部的Web服务器等的应用程序中的非法访问。特别是,在内置有用于存储交易数据或余额数据等的IC卡的移动通信终端中,该倾向更为显著。即,即使由具有恶意的内容提供方生成的应用程序进行对IC卡的非法访问,在其痕迹没有流露到外部的情况下也无法检测出该状态。

另一方面,还考虑监视访问前后的IC卡内的数据一致性的方法,但是在这种情况下,即使能够防止数据的篡改,也不足以防止数据的非法取得。

因此,本发明是鉴于这样的问题而完成的,目的在于提供一种能

够充分防止从应用程序向内部的 IC 卡的非法访问的移动通信终端以及数据访问控制方法。

解决技术问题的手段

为了解决上述问题，本发明的移动通信终端的特征是具备：非接触 IC 卡；平台单元，作为用于使应用程序动作的应用程序接口；应用管理单元，控制应用程序的起动以及停止；以及访问控制单元，在上述平台单元内动作，对从应用程序向上述非接触 IC 卡的访问进行中继，其中，上述访问控制单元在检测出从应用程序向上述非接触 IC 卡的非法访问的情况下，向上述应用管理单元指示停止上述应用程序。

或者，本发明的数据访问控制方法控制在内置有非接触 IC 卡的移动通信终端内的平台上动作的应用程序的数据访问，其特征在于，具备：访问控制步骤，在上述平台单元内动作的访问控制单元对从应用程序向上述非接触 IC 卡的访问进行中继；以及程序停止步骤，在上述访问控制单元检测出来自应用程序的非法访问的情况下，向控制应用程序的起动以及停止的应用管理单元指示停止上述应用程序。

在这样的移动通信终端以及数据控制方法中，独立于应用程序的访问控制单元对应用程序向非接触 IC 卡的访问进行中继，这时在检测出非法访问的情况下，控制该应用程序的停止。这样，通过使与应用程序不同的部分、特别是通常不容易篡改的平台具有数据访问功能，即使在应用程序自身包含非法数据的情况下，也能够更可靠地检测出非法访问。

发明的效果

依据本发明的移动通信终端，能够充分地防止从应用程序对内部的 IC 卡的非法访问。

附图说明

图 1 是表示本发明的移动通信终端的一个最佳实施方式的概略结构图。

图 2 是存储在图 1 的访问权限存储单元中的数据的一个

例子。

图3是存储在图1的计数器信息存储单元中的数据的数据的结构图的一个例子。

图4是表示利用访问权限信息的数据访问控制时的移动通信终端的动作的流程图。

图5是表示利用来自非接触IC卡的应答内容的数据访问控制时的移动通信终端的动作的流程图。

符号的说明

1: 移动通信终端; 2: 操作系统动作环境; 3: 平台单元; 4: 数据区域; 5: 应用管理单元; 6: 访问控制单元; 7a、7b、7c(7): 应用程序; 8: 非接触IC卡; 10: 内容服务器; 11: 访问控制用服务器; 20: 通信网络

具体实施方式

以下, 根据附图详细地说明本发明的移动通信终端的最佳实施方式。在附图的说明中, 在相同的要素上标注相同的符号, 并省略重复说明。

图1是本发明的移动通信终端的一个最佳实施方式的概略结构图。该图所示的移动通信终端1是具有用于实现游戏功能、电子商务交易功能、等待图像显示功能等的应用程序能够动作的环境的通信终端。作为这种通信终端的例子, 可以举出便携电话机、PHS(个人手持电话系统)、PDA(个人数字助理)这样的可进行经由网络的信息通信的设备。如图1所示, 作为功能性结构要素, 移动通信终端1构成为包括操作系统动作环境2、构筑在该操作系统动作环境2上的平台单元3、在操作系统动作环境2上动作的应用管理单元5和数据区域4, 并且在内部具备非接触IC卡8。

非接触IC(集成电路)卡8在内部具有天线、IC芯片、存储器, 构成为可以与外部R/W(读出器/写入器)12之间通过电波非接触地进行数据通信。在该数据通信中, 能够从外部R/W12访问非接触

IC 卡 8 的存储器（读出 / 写入）。同时，非接触 IC 卡 8 与移动通信终端 1 的内部电路（未图示）有线连接，还可以与在移动通信终端 1 上动作的应用程序进行数据通信（详细情况后述）。

另外，内置于该非接触 IC 卡 8 内的存储器被细分成多个分层区域，以该细分后的区域为单位从外部进行访问。更详细地说，将该存储器划分成被称为系统的多个区域，进而，将系统细分成被称为分区的多个区域。根据这样的存储器的分层构造，例如按照电子商务交易服务等服务提供商的不同分开使用系统的区域、按照服务种类的不同分开使用分区的区域。

并且，非接触 IC 卡 8 针对来自外部的访问具有认证功能。该认证通过接收密码等认证代码或用于确定上述系统和分区的数据存储区域信息来进行。非接触 IC 卡还针对外部的访问源回答认证结果。

操作系统动作环境 2 在 CPU（中央处理单元）、RAM（随机存取存储器）等硬件上构成，是进行文件管理、存储器管理，数据输入输出管理、用户接口提供等的 OS（操作系统）等系统程序常驻的动作环境。另外，在操作系统动作环境 2 上，还执行用于实现作为移动通信终端 1 的基本功能的通话功能、电子邮件收发功能以及互联网连接功能等的基本程序。

数据区域 4 构筑在 RAM（随机存取存储器）、ROM（只读存储器）、磁盘等存储器上，是存储 OS 等系统程序所利用的系统数据、基本程序所利用的电话簿数据等基本数据、各种程序文件以及后述的应用管理单元 5 所参照的数据等的数据区域。

平台单元 3 是用于执行以 JAVA（注册商标）语言记述的应用程序的 JAVA（注册商标）虚拟机器程序（未图示）所常驻的程序执行环境。以下，在称为“应用程序”的情况下是指系统程序或基本程序以外的程序，是指从 WWW 服务器等的外部下载并执行的程序。该 JAVA（注册商标）虚拟机器程序具有下述功能：在执行应用程序时，将应用程序的代码转换为可在操作系统动作环境 2 中解释的代码，并传送给操作系统动作环境 2。并且，在平台单元 3 中，具备多个作为

可从应用程序调用的函数的 API（应用程序接口）。

在这样的平台单元 3 上，执行应用程序 7a、7b、7c。应用程序 7a、7b、7c 在由应用管理单元 5 从内容服务器 10 暂时下载到数据区域 4 以后，根据来自用户的指示在平台单元 3 上起动。另外，应用程序 7a、7b、7c 构成为可以经由通信网络 20 与内容服务器 10 进行 HTTP（超文本传输协议）通信。

应用管理单元 5 在操作系统动作环境 2 上动作，是进行应用程序 7 的下载以及应用程序 7 的起动和停止的控制的部分。

更具体地讲，应用管理单元 5 根据来自移动通信终端 1 的用户的指示，从内容服务器 10 取得存储了应用程序 7 的代码的 JAR（Java（注册商标）ARchiver）文件，并下载到数据区域 4 内的预定区域中。另外，应用管理单元 5 根据来自用户的指示，读出 JAR 文件来控制应用程序 7 的起动。并且，应用管理单元 5 还具有根据来自用户的指示以及来自访问控制单元 6 的指示（具体情况后述），控制应用程序 7 的停止的功能。该应用程序 7 的停止既可以通过结束应用程序 7 的进程来进行，也可以通过删除或变更应用程序 7 的程序文件、参数文件等进行。

访问控制单元 6 在平台单元 3 内动作，是用于对从应用程序 7 向非接触 IC 卡 8 的访问（读出/写入）进行中继的部分。作为功能性构成要素，访问控制单元 6 具备访问功能单元 61、非法访问检测单元 62、应用停止控制单元 63。以下，详细地说明各构成要素。

访问功能单元 61 是包括用于访问非接触 IC 卡 8 的多个 API 的部分。访问功能单元 61 在接收到来自应用程序 7 的 API 调用（访问请求）后，向非接触 IC 卡 8 发送出访问请求信号。该 API 调用通过指定用于确定对象的 API 的 API 名、以及访问所必需的认证用参数来进行。进而，将非接触 IC 卡 8 针对访问请求信号所发送出的应答以及参照数据中继到应用程序 7。所谓参照数据，是指伴随访问请求从非接触 IC 卡 8 内的存储器读出的数据。

另外，访问功能单元 61 在从应用程序 7 接收到 API 调用的情况

下，还向非法访问检测单元 62 输出该被调用的 API 名以及来自非接触 IC 卡 8 的应答。

非法访问检测单元 62 是在检测出来自应用程序 7 的非法访问的情况下、向应用管理单元 5 指示停止应用程序 7 的部分。以下，说明由非法访问检测单元 62 进行的非法访问检测。

（基于访问权限信息的非法访问检测）

非法访问检测单元 62 将与应用程序 7 所调用的 API 有关的 API 名输出到应用管理单元 5。对此，应用管理单元 5 参照存储在设置于数据区域 4 内的访问权限存储单元 41 中的访问权限信息，向非法访问检测单元 62 返送允许标志。该访问权限信息是表示应用程序 7 对非接触 IC 卡 8 的访问权限的信息，由应用管理单元 5 预先从访问控制用服务器 11 取得。

图 2 中示出在这种情况下存储在访问权限存储单元 41 中的数据的结构图的一个例子。如该图所示，在访问权限存储单元 41 中，与允许标志（0/1）相关联地存储有助于确定应用程序的应用程序 ID 和用于确定 API 的 API 名。依据该访问权限信息的例子，意味着允许标志“1”允许由应用程序 ID “APID1” 确定的应用程序 7a 进行 API “数据读出” 的调用。另一方面，表示允许标志“0”不允许应用程序 7a 进行 API “数据写入” 的调用。另外，为了提高安全性，存储在访问权限存储单元 41 中的数据最好是仅能从应用管理单元 5 参照以及写入。

因此，依据图 2 的例子，应用管理单元 5 在应用程序 7a 调用了 API “数据写入” 的情况下，向非法访问检测单元 62 返送与应用程序 7a 的应用程序 ID “APID1” 以及 API 名 “数据写入” 相对应的允许标志“0”。

返回到图 1，非法访问检测单元 62 在应用管理单元 5 返送的允许标志是表示不允许的“0”的情况下，检测出来自应用程序 7 的非法访问，并将该信息通知给应用停止控制单元 63。

（基于来自非接触 IC 卡的应答内容的非法访问检测）

非法访问检测单元 62 在进行上述的基于访问权限信息的非法访问检测的同时，如下进行基于来自非接触 IC 卡 8 的应答内容的非法访问检测。

即，非法访问检测单元 62 在来自非接触 IC 卡 8 的应答内容中包含表示访问失败的信息的情况下，向应用管理单元 5 输出与应用程序 7 所调用的 API 有关的 API 名。

作为来自非接触 IC 卡 8 的应答表示访问失败的情况，可以举出以下情况：在应用程序 7 要调用必须进行基于密码（认证代码）的认证的 API 的情况下，指定了错误的密码作为认证用参数的情况；以及在应用程序 7 要调用必须进行基于数据存储区域信息的认证的 API 的情况下，指定了不存在的数据存储区域信息作为认证用参数的情况。这里，数据存储区域信息是指定非接触 IC 卡 8 内的存储器中的访问目的地数据存储区域的信息，由用于确定系统的系统代码以及用于确定分区的分区代码构成。

对此，应用管理单元 5 参照存储在设置于数据区域 4 中的计数器信息存储单元 42 中的失败计数器，向非法访问检测单元 62 返送表示访问失败是否在容许次数以内的容许标志。该失败计数器既可以在移动通信终端 1 内预先设定，也可以从访问控制用服务器 11 等取得。

图 3 中示出在这种情况下存储在计数器信息存储单元 42 中的失败计数器的结构图的一个例子。如该图所示，在计数器信息存储单元 42 中，与计数器以及容许次数相关联地存储有用于确定应用程序的应用程序 ID 和用于确定 API 的 API 名。依据该失败计数器的例子，意味着由应用程序 ID “APID1” 确定的应用程序 7a 所进行的 API “数据读出” 的调用至此已经检测出 “4” 次访问失败，而访问失败容许到 “4” 次。另一方面，意味着由应用程序 7a 进行的 API “PIN 解除指令” 的调用没有检测到访问失败，而访问失败容许到 “5” 次。为了进一步提高安全性，存储在计数器信息存储单元 42 中的数据最好是仅能从应用管理单元 5 参照以及写入。

因此，应用管理单元 5 使与返回了访问失败的对象应用程序以及

API 相对应的计数器加 1。然后，在进行加法运算后的计数器在容许次数以内的情况下，向非法访问检测单元 62 返送容许标志“1”，在计数器超过了容许次数的情况下，向非法访问检测单元 62 返送容许标志“0”。

返回到图 1，非法访问检测单元 62 在从应用管理单元 5 返送的容许标志是表示不容许的“0”的情况下，检测来自应用程序 7 的非法访问，并将该信息通知给应用停止控制单元 63。

应用停止控制单元 63 是在从非法访问检测单元 62 接收到非法访问检出通知后、向应用管理单元 5 指示停止检测出非法访问的应用程序 7 的部分。对此，应用管理单元 5 通过控制相应的应用程序 7 的停止，来停止应用程序 7。

下面，参照图 4～图 5 说明移动通信终端 1 的动作，同时对移动通信终端 1 中的数据访问控制方法进行详述。图 4 是表示利用访问权限信息的数据访问控制时的移动通信终端 1 的动作的流程图，图 5 是表示利用来自非接触 IC 卡的应答内容的数据访问控制时的移动通信终端 1 的动作的流程图。

首先，参照图 4，说明利用访问权限信息的数据访问控制时的移动通信终端 1 的动作。

首先，以用户操作等为契机，从应用程序 7a 向访问功能单元 61 调用用于访问非接触 IC 卡 8 的 API（步骤 S101）。对此，访问功能单元 61 在向非法访问检测单元 62 输出了所调用的 API 名后，非法访问检测单元 62 向应用管理单元 5 查询应用程序 7a 的与该 API 有关的访问权限信息（步骤 S102）。

接着，应用管理单元 5 根据该 API 的 API 名以及调用了该 API 的应用程序 7a 的应用程序 ID，参照存储在访问权限存储单元 41 中的访问权限信息（步骤 S103）。然后，非法访问检测单元 62 判定包含在访问权限信息中的允许标志是否是表示允许的“1”（步骤 S104）。

上述判定的结果是允许标志为“1”的情况下（步骤 S104；是），非法访问检测单元 62 向访问功能单元 61 通知允许访问非接触 IC 卡 8

(步骤 S105)。然后,访问功能单元 61 向非接触 IC 卡 8 发送出与应用程序 7a 所调用的 API 相对应的访问请求信号(步骤 S106)。然后,访问功能单元 61 将从非接触 IC 卡 8 返送的应答以及参照数据中继到应用程序 7a(步骤 S107)。

另一方面,在允许标志为“0”的情况下(步骤 S104;否),应用停止控制单元 63 向应用管理单元 5 指示应用程序 7a 的停止(步骤 S108)。对此,应用管理单元 5 控制应用程序 7a 的停止(步骤 S109)。

其次,参照图 5,说明利用来自非接触 IC 卡 8 的应答内容的数据访问控制时的移动通信终端 1 的动作。以下说明的处理是应用程序 7a 在附加访问非接触 IC 卡 8 所必要的密码或数据存储区域信息等认证用参数后调用 API 的情况下的处理。

首先,以用户操作等为契机,从应用程序 7a 向访问功能单元 61 调用用于访问非接触 IC 卡 8 的 API(步骤 S201)。该 API 的调用通过指定 API 名和认证用参数来进行。对此,访问功能单元 61 在向与 API 名对应的访问请求信号附加了认证用参数后,向非接触 IC 卡 8 送出(步骤 S202)。然后,访问功能单元 61 在接收到从非接触 IC 卡 8 返送的应答后,向非法访问检测单元 62 输出该应答和 API 名(步骤 S203)。

非法访问检测单元 62 判定来自非接触 IC 卡 8 的应答内容是否包含表示访问失败的信息(步骤 S204)。在判定的结果是应答内容不表示访问失败的情况下(步骤 S204;否),访问功能单元 61 将该应答以及从非接触 IC 卡 8 返送的参照数据中继到应用程序 7a(步骤 S205)。

另一方面,在上述判定的结果是应答内容表示访问失败的情况下(步骤 S204;是),访问功能单元 61 向应用管理单元 5 输出与应用程序 7a 所调用的 API 有关的 API 名(步骤 S206)。对此,应用管理单元 5 在从访问权限存储单元 41 读出了与该 API 名和应用程序 7a 的应用程序 ID 相对应的计数器和容许次数后,通过使该计数器加 1 来进行更新(步骤 S207)。

然后,应用管理单元 5 判定进行了加法运算后的计数器是否在容

许次数以内（步骤 S208）。在判定的结果是在容许次数以内的情况下（步骤 S208；是），从应用管理单元 5 向非法访问检测单元 62 通知该信息（步骤 S212）。然后，访问功能单元 61 接收到该通知后，向应用程序 7a 返送表示访问失败的应答（步骤 S213）。

另一方面，在超过了容许次数的情况下（步骤 S207；否），应用管理单元 5 向非法访问检测单元 62 通知容许次数溢出（步骤 S209）。非法访问检测单元 62 在接收到容许次数溢出通知后，判断为从应用程序 7a 进行了非法访问，应用停止控制单元 63 向应用管理单元 5 指示停止应用程序 7a（步骤 S210）。对此，应用管理单元 5 控制应用程序 7a 的停止（步骤 S211）。

依据以上说明的移动通信终端 1，独立于应用程序 7 的访问控制单元 6 对应用程序 7 向非接触 IC 卡 8 的访问进行中继，此时在检测出非法访问的情况下，控制该应用程序 7 的停止。这样，通过使与应用程序 7 不同的部分、特别是通常不容易篡改的平台单元 3 具有数据访问功能，即使在应用程序 7 自身包含非法代码的情况下，也能够更可靠地检测出非法访问。从而，能够抑制例如有恶意的内容提供方利用应用程序使存储在非接触 IC 卡 8 中的个人信息外流。

另外，根据与各个应用程序 7 和访问种类相对应地管理的访问权限信息来进行应用程序 7 的非法访问检测。由此，能够更为柔性地实现每个应用程序对非接触 IC 卡的访问的控制。

而且，由于根据来自非接触 IC 卡 8 的应答内容来判断应用程序 7 的非法访问检测，因此在利用数据存储空间信息或认证代码来进行非接触 IC 卡 8 中的访问允许的情况下，可以防止由没有得到允许的应用程序进行的非法访问。其结果，例如可以排除对用于访问非接触 IC 卡 8 的密码进行分析并使之外流这样的非法攻击。

另外，在本发明中，还具备用于存储表示应用程序对非接触 IC 卡的访问权限的访问权限信息的访问权限存储单元，访问控制单元最好根据在存储于访问权限存储单元内的访问权限信息中是否允许应用程序对非接触 IC 卡的访问，来进行非法访问的检测。这种情况下，

可以更柔性地实现每个应用程序对非接触 IC 卡的访问的控制。

而且，访问控制单元最好在从应用程序接收到包含用于确定非接触 IC 卡中的数据存储区域的数据存储区域信息的访问请求以后，从非接触 IC 卡接收针对访问请求的应答，根据在该接收到的应答中是否包含表示访问失败的信息，来进行非法访问的检测。依据这样的结构，例如在利用表示数据区域的代码来进行非接触 IC 卡中的访问允许的情况下，能够防止由没有得到允许的应用程序进行的非法访问。

进而，访问控制单元最好在从应用程序接收到包含用于访问非接触 IC 卡的认证代码的访问请求以后，从非接触 IC 卡接收针对访问请求的应答，根据在该接收到的应答中是否包含表示访问失败的信息，来进行非法访问的检测。如果具备这样的访问控制单元，则例如在利用密码等认证代码来进行非接触 IC 卡中的访问允许的情况下，能够防止没有得到允许的应用程序进行的非法访问。

另外，本发明并不限于上述的各实施方式。例如，应用程序 7 并不限于用 JAVA（注册商标）语言记述的程序，也可以用 C 语言等其它语言来记述。

产业上的可利用性

本发明以具有控制由应用程序进行的数据访问的功能的无线通信终端以及数据访问控制方法为使用用途，可充分地防止对内部数据的非法访问。

图1

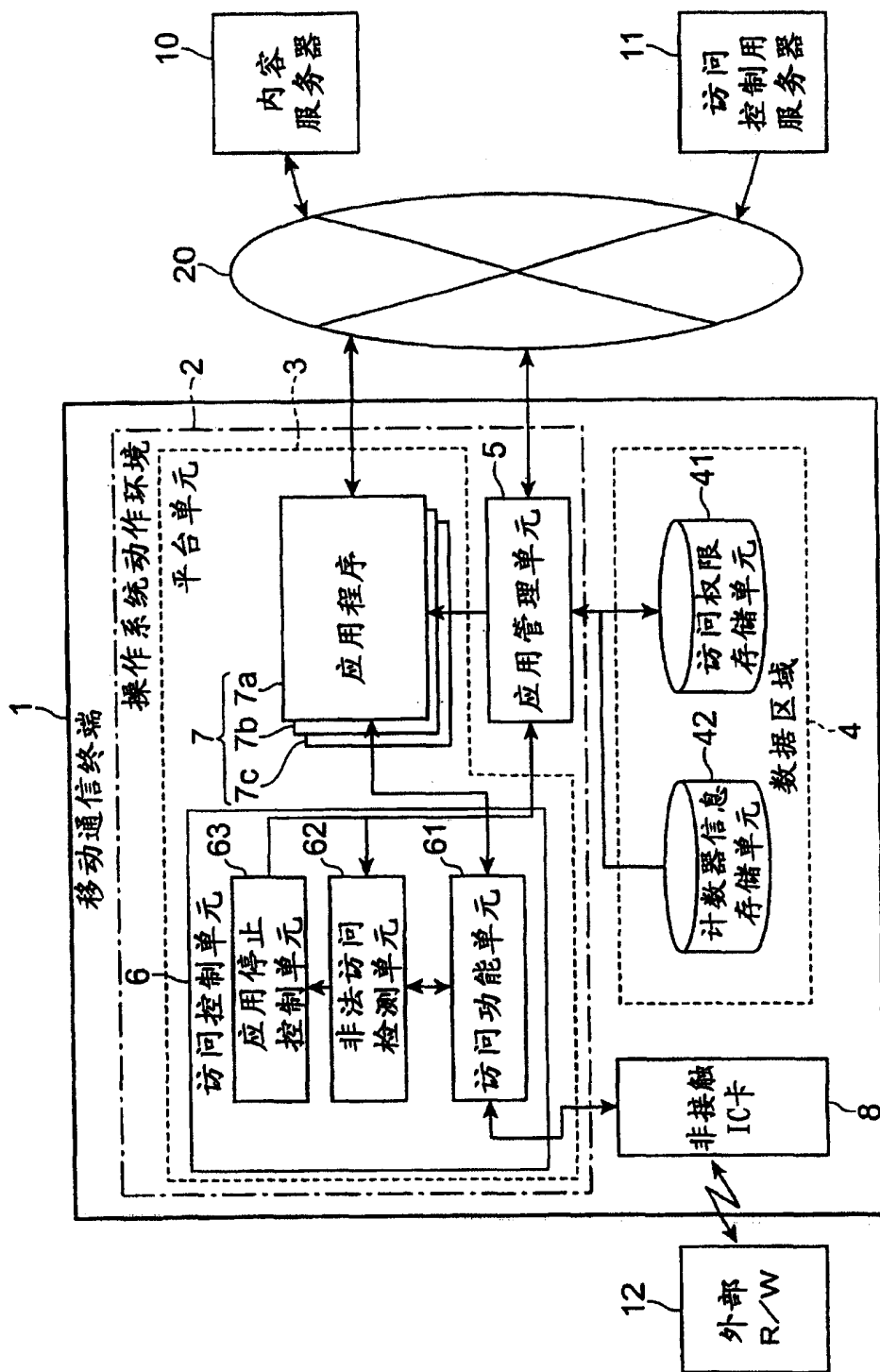


图 2

应用程序ID	对象API名	允许标志
⋮	⋮	⋮
APID1	PIN解除指令	1
APID1	PIN变更指令	0
APID1	数据读出	1
APID1	数据写入	0
⋮	⋮	⋮

图 3

应用程序 ID	对象API名	计数器	容许次数
⋮	⋮	⋮	⋮
APID1	PIN解除指令	0	5
APID1	PIN变更指令	0	3
APID1	数据读出	4	4
APID1	数据写入	0	4
⋮	⋮	⋮	⋮

图 4

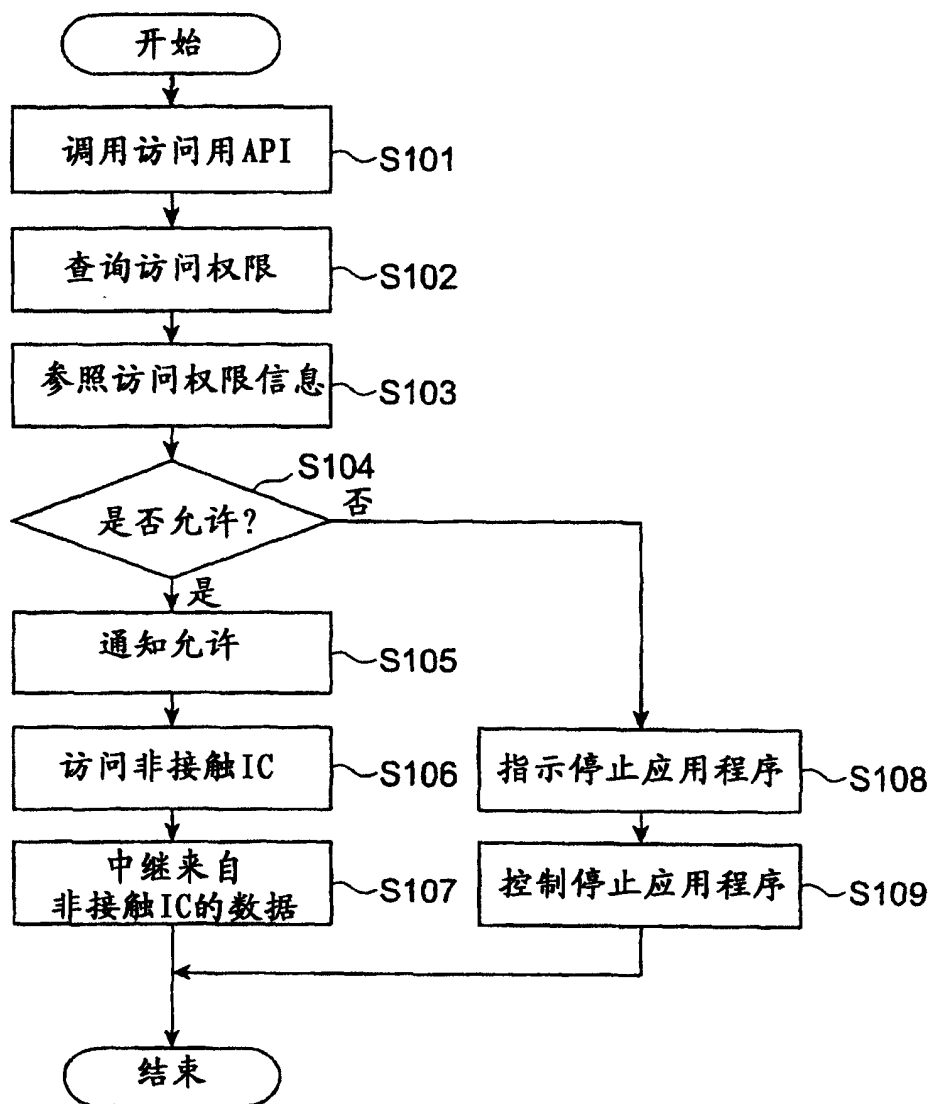


图5

