[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06K 19/07 (2006.01)
G06K 7/00 (2006.01)

[12] 发明专利说明书

专利号 ZL 200510007966.9

[45] 授权公告日 2009 年 3 月 4 日

[11] 授权公告号 CN 100465991C

[22] 申请日 2005.2.4
[21] 申请号 200510007966.9
[30] 优先权
[32] 2004. 2. 4 [33] JP [31] 27573/04
[73] 专利权人 夏普株式会社
地址 日本大阪市
[72] 发明人 小川龙一 若林正树
[56] 参考文献
CN1298519A 2001.6.6
CN1304116A 2001.7.18
CN1397055A 2003.2.12
US20020166075A1 2002.11.7
US6597285B2 2003.7.22
US5666537A 1997.9.9
EP0446519A2 1991.9.18
CN1413389A 2003.4.23
CN1172541A 1998.2.4
一种非接触式 IC 卡控制器的设计. 肖斌，秦东，徐志伟，孙承绶. 半导体技术，第 25 卷第 2 期. 2004
审查员 赵云峰
[74] 专利代理机构 中国专利代理(香港)有限公司
代理人 浦柏明 刘宗杰

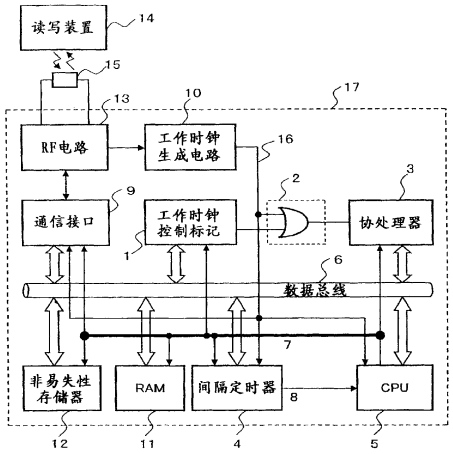
权利要求书 2 页 说明书 14 页 附图 11 页

[54] 发明名称

辅助运算用协处理器内置型 IC 卡及其控制方法

[57] 摘要

本发明的课题是一种 IC 卡(17)，在主运算处理装置(5)以外内置辅助运算用协处理器(3)，配备：在经过比帧等待时间短的设定时间后，输出中断要求信号(8)的间隔定时器(4)；以及根据中断要求信号(8)的输出，停止向协处理器(3)供给工作时钟(16)，根据来自外部装置(14)的规定的响应输入，恢复工作时钟(16)的供给，控制协处理器(3)的工作的协处理器控制装置(1、2、5)。 当接收来自外部装置(14)的指令时，判定指令的内容，将比帧等待时间短的设定时间设定在间隔定时器(4)中，启动间隔定时器(4)。



1. 一种 IC 卡，它是在主运算处理装置以外内置辅助运算用协处理器的 IC 卡，其特征在于：

配备：

在经过比帧等待时间短的设定时间后，输出中断要求信号的间隔定时器；以及

根据上述中断要求信号的输出，停止向上述协处理器供给工作时钟，根据来自外部装置的规定的响应输入恢复上述工作时钟的供给，控制上述协处理器的工作的协处理器控制装置，配备当接收来自上述外部装置的指令时，判定上述指令的内容，将比上述帧等待时间短的设定时间设定在上述间隔定时器中，启动上述间隔定时器的间隔定时器设定装置，上述间隔定时器设定装置的处理通过上述主运算处理装置执行。

2. 如权利要求 1 所述的 IC 卡，其特征在于：

上述协处理器控制装置配备：

用于控制停止及恢复向上述协处理器供给工作时钟的控制标记；

根据上述控制标记的状态，控制停止及恢复向上述协处理器供给工作时钟的工作时钟控制装置；以及

接收上述中断要求信号的输出，将上述控制标记的状态设定在工作停止状态，接受上述响应输入，将上述控制标记的状态设定在工作恢复状态的控制标记设定装置，上述控制标记设定装置的处理通过上述主运算处理装置执行。

3. 如权利要求 2 所述的 IC 卡，其特征在于：

当停止向上述协处理器供给工作时钟时，上述主运算处理装置向上述外部装置输出帧等待时间延长要求，当从上述外部装置接受该响应输入时，将上述控制标记的状态设定在工作恢复状态。

4. 如权利要求 1 所述的 IC 卡，其特征在于：

配备存储通常处理用的程序的非易失性存储器和比上述非易失性存储器工作功耗更低的第 2 存储器，

至少在上述协处理器工作时，上述协处理器所处理的程序存储在上述第 2 存储器中。

5. 如权利要求 4 所述的 IC 卡，其特征在于：

在上述协处理器工作时，禁止对上述非易失性存储器进行存取。

6. 如权利要求 1 所述的 IC 卡，其特征在于：

在与上述外部装置的通信应用中，配备非接触接口及接触接口的至少某一方。

7. 一种 IC 卡的控制方法，上述 IC 卡在主运算处理装置以外内置辅助运算用协处理器，其特征在于：

上述控制方法包含下述事项：

上述主运算处理装置，进行中断许可的设定，使得在经过比帧等待时间短的设定时间后，输出中断要求信号；

在上述中断许可的设定后，开始上述协处理器的运算处理；

上述主运算处理装置，在上述协处理器的运算处理中，当输出上述中断要求信号时，分支到中断处理；以及

控制停止及恢复向上述协处理器的工作时钟的供给的工作时钟控制装置，在上述中断处理中，停止向上述协处理器供给工作时钟，当接受来自外部装置的规定的响应输入时，恢复上述工作时钟的供给，

包含下述事项：

在上述中断处理中，在停止向上述协处理器供给工作时钟后，向上述外部装置输出帧等待时间延长要求，当从上述外部装置接受该响应输入时，恢复上述工作时钟的供给。

8. 如权利要求 7 所述的 IC 卡控制方法，其特征在于：

当接收来自上述外部装置的指令时，判定上述指令是否是上述协处理器的执行指令，在是上述协处理器的执行指令的情况下，进行上述中断许可的设定。

辅助运算用协处理器内置型 IC 卡及其控制方法

技术领域

本发明涉及内置了密码处理等辅助运算用协处理器的 IC 卡，更详细地说，涉及用于改善 IC 卡与外部装置间的通信协议的效率的也能够在非接触型、接触型及组合型的任何一种 IC 卡中应用的技术。

背景技术

由于在塑料制的卡上安装了非易失性存储器、CPU、密码用协处理器等的 IC 芯片（半导体集成电路器件）的 IC 卡与现在广泛使用的磁卡相比，能够处理更大量的数据、安全性优越，故开始在各种各样的用途中普及。IC 卡具有：通过将在其表面上设置了金属制端子的 IC 卡插入外部读写装置，通过该端子进行供电和数据授受的接触型 IC 卡；使用电磁感应技术，通过使天线线圈进入读写装置所发生的磁场中，用读写装置和电波（例如，数 MHz～数十 MHz 程度的载波频率）进行供电和数据授受的非接触型 IC 卡；以及具备了接触型和非接触型两者的接口的组合型 IC 卡等。近年来，非接触型 IC 卡由于其操作的便利性而开始得到普及。

（非接触型 IC 卡在供电上存在的问题）

但是，在非接触型 IC 卡或者组合型 IC 卡的非接触通信中，为了通过电磁感应从读写装置进行馈电，对 IC 卡不能以大容量的电力驱动，而应成为小容量的电源。因此，非接触型 IC 卡需要竭力抑制电流消耗。在现在的 IC 卡中，由于非易失性存储器的读出、写入、擦除以及在上述密码运算用的协处理器中消耗的电流大，在非接触中的供电方面存在问题。

（非接触 IC 卡在通信方面存在的问题）

接近型非接触型 IC 卡的通信方式例如是用 ISO14443 型 B 规格（ASK10%）进行规格化的、低深度调制方式。这里，所谓低深度调制是指，将从在通信中使用的信号的最大振幅 Amax 和最小振幅 Amin 以下述式（1）定义的比率称为调制率，将 10%那样低的调制率的通信称为低深度调制。

调制率=（Amax-Amin）/（Amax+Amin） （1）

在低深度调制中，很微小的电压变动对通信品质产生影响。因此，在通信中，必须抑制消耗电流，迄今在通信中进行运算用协处理器的工作、非易失性存储器的写入、擦除、读出等工作是困难的。

（帧等待时间设定方面存在的问题）

在非接触型 IC 卡与读写装置间的通信中，初始响应通过 ISO14443-3 进行规格化。该非接触型 IC 卡的处理流程图示于图 1。

另外，在初始响应后的非接触型 IC 卡与读写装置之间的通信中的协议通过 ISO14443-4 进行规格化。

当电源处于关断状态的非接触型 IC 卡从读写装置中接受能量时，电源上升，通过从读写装置向 IC 卡发送 REQB 指令，开始初始响应。REQB 指令是非接触型 IC 卡的准备要求指令，在该指令内包含用途领域标识符（AFI）、属性信息参数（PARM）、循环冗余检验符（CRC）等信息。

接收了准备要求 REQB 指令的非接触型 IC 卡经过 REQB 指令中的用途领域标识符（AFI）的一致检测、从属性信息（PARM）判断非接触型 IC 卡的枚数的上限值（在实施例中，N=1 枚），使 ATQB 响应返回到读写装置中。ATQB 响应是对 REQB 指令的请求响应信号，包含伪固有标识符（PUPI）、应用信息（Application data）、协议信息（Protocol information）、循环冗余检验符（CRC）等信息。通过读写装置接收 ATQB 响应，读写装置得到上述信息。

非接触型 IC 卡返回 ATQB 响应，进而，当进行 ATTRIB 指令的接收和 ATTRIB 的响应时，初始响应结束，非接触型 IC 卡转移到激活状态。

然后，非接触型 IC 卡与读写装置按 ISO14443-4 规格化了的协议实施通信。

通常，读写装置与非接触型 IC 卡使用上述协议从读写装置向非接触型 IC 卡发送指令，非接触型 IC 卡执行与接收的指令相应的处理，将指令的执行结果发送到读写装置。当非接触型 IC 卡从读写装置接收 S 块的 DESELECT 指令时，非接触型 IC 卡转移到停止状态（HALT）。当非接触型 IC 卡处于停止状态时，仅仅能够接收来自读写装置的 WUPB 指令。通过 WUPB 指令，非接触型 IC 卡再次从初始响应工作中的 AFI 的一致检测进行工作。

在包含在对初始响应时的 REQB 指令的 ATQB 响应内的协议信息（Protocol information）中，作为非接触型 IC 卡通信中所需的参数，包含位传输速度、最大帧尺寸等，其中有用于读写装置设定帧等待时间的参数 FWI。读写装置接收 FWI 后，进行下式（2）所示的计算，设定帧等待时间 FWT。

$$FWT=(256\times16/fc)\times2^{FWI} \qquad (2)$$

在上述式（2）中，fc 是读写装置所发生的载波频率，在规格中为 13.56MHz。在规格中，将 0～14 的值（与约 302μs～约 4949ms 的 FWT 对应）分配给 FWI。在 FWI 中采用哪个值，由非接触型 IC 卡侧决定，非接触型 IC 卡需要在与向读写装置发送的 FWI 对应的时间内，结束非接触型 IC 卡内的处理。当在该时间内没有结束 IC 卡内的处理的情况下，读写装置也可以作为超时错误处理。在 ISO14443-4 的协议通信应用中，在读写装置的帧等待时间内没有结束非接触型 IC 卡侧的处理的情况下，需要非接触型 IC 卡向读写装置进行延长帧等待时间的要求，以延长读写装置侧的超时错误判断时间。用于帧等待时间延长的读写装置与非接触型 IC 卡的通信指令用 ISO14443-4 的协议规格规定。现在，需要在非接触型 IC 卡内进行长时间处理的处理有用于进行协处理器运算所需的各种加密/解密的算术运算等。

在初始响应中，例如在将 FWI 设定在 FWI=14 那样大的值的情况下，在读写装置侧，总是将超时错误判定的时间设定得很长。因此，在没有必要延长时间的其他的指令中，在非接触型 IC 卡内的处理和通信中发生异常，在读写装置不能正确地接收对来自读写装置的指令的非接触型 IC 卡的响应的情况下，存在读写装置对超时错误的异常判定要花必要以上的时间、性能降低的问题。在初始响应中的 FWI 设定希望设定为考虑了 IC 卡系统整体性能的尽可能小的值。

但是，考虑到 IC 卡系统的性能，例如当将 FWI 设定为 FWI=4 那样小的值时，在一部分的协处理器运算中，往往需要超过了读写装置的帧等待时间的运算时间。

为了解决这种帧等待时间设定方面的问题，也考虑过在协处理器运算中利用时间中断功能，进行用于延长帧等待时间的读写装置与非接触型 IC 卡之间的通信的方法，在协处理器运算中进行帧等待时间延长要求（通信）的情况由于通信处理被加在原来运算处理上，在与功

耗的增大相联系、非接触型 IC 卡的通信中，会造成通信距离缩短或者通信的稳定性降低等，使利用该方法提高效率变得困难。

另外，在协处理器运算中，处理时间随运算用协处理器所实施的运算种类及给予运算用协处理器的参数不同而不同。现在，即使在多个密码处理、或者一个密码处理内，也需要处理多个参数，难以事前将处理时间图表化，预测是否需要延长帧等待时间。因此，在现状的非接触型 IC 卡中，在实施所有的协处理器运算前，进行用于帧等待时间延长的通信，对读写装置进行帧等待时间的延长设定的处理。对读写装置的帧等待时间延长是暂时的处理，在非接触型 IC 卡的一次的指令处理结束（将对指令的响应发送到读写装置）后，读写装置的帧等待时间返回到初始值。

其次，图 2 表示与现有的帧等待时间的设定相关的实施例。根据图 2 所示的现有的实施例，读写装置与非接触型 IC 卡根据 ISO14443-4 协议，进行下述工作。此外，图 2 中的 R/W 表示读写装置，ICC 表示非接触型 IC 卡。

（1）读写装置通过 I 块向非接触型 IC 卡发送指令。非接触型 IC 卡接收该指令，判定指令的类别。

（2）如果在（1）中接收的指令是伴随运算用协处理器工作的指令，则非接触型 IC 卡在协处理器运算开始前，向读写装置发送帧等待时间延长要求（S 块的 WTX 要求）。

（3）读写装置按照 S 块的 WTX 要求，延长帧等待时间。读写装置向非接触型 IC 卡发送帧等待时间延长响应（S 块的 WTX 响应）。

（4）非接触型 IC 卡进行指令的执行处理（协处理器运算处理）。

（5）当指令的执行处理结束时，非接触型 IC 卡通过 I 块向读写装置发送对向读写装置的指令的执行结果。

但是，上述现有例中的帧等待时间设定方式至少存在以下 2 个课题。即，第 1，即使在不需要帧等待时间延长（处理时间短）的协处理器运算中，由于进行用于帧等待时间延长的通信，发生用于该发送接收的时间的浪费，使读写装置与非接触型 IC 卡的通信效率降低。第 2，由于在协处理器运算处理前进行用于帧等待时间延长的通信，将该通信作为引发剂，对攻击者告知加密运算和解密运算的关键信息等的解析点，有可能成为安全性方面的问题。

发明内容

因此，本发明是鉴于上述问题而进行的，其目的在于：主要解决在非接触型 IC 卡中存在的供电方面的问题、通信方面的问题以及帧等待时间设定方面的问题，提供能够以低功耗进行高效通信的 IC 卡及其控制方法。

用于达到上述目的的本发明的 IC 卡是在主运算处理装置以外内置了辅助运算用的协处理器的 IC 卡，其第 1 特征在于，配备：在经过比帧等待时间短的设定时间后，输出中断要求信号的间隔定时器；以及根据上述中断要求信号的输出，停止向上述协处理器供给工作时钟，根据来自外部装置的规定的响应输入，恢复上述工作时钟的供给，控制上述协处理器工作的协处理器控制装置。

根据上述第 1 特征的本发明的 IC 卡，在协处理器的运算处理超过比帧等待时间更短的设定时间的情况下，中断协处理器的运算处理，例如对读写装置等外部装置，能够通过发送变更通信条件的要求（例如，帧等待时间延长要求），变更外部装置的通信条件，等待该变更确认响应输入的接收，恢复中断了的协处理器的运算处理。其结果是，能够避免由于协处理器的运算处理与外部装置间的通信同时进行引起的非接触型 IC 卡中的供电方面的问题及通信方面的问题，避免在协处理器的运算处理中，因对外部装置进行帧等待时间延长要求而发生没有准备的超时错误。另外，在协处理器的运算处理在经过上述设定时间之前结束的情况下，可节省对外部装置进行通信条件的变更要求的浪费，谋求提高通信效率及处理效率。另外，由于对外部装置通信条件的变更要求是在协处理器的运算处理开始后经过上述设定时间后进行的，可提高对将该通信作为引发剂的攻击者的安全性。

另外，理想的情况是，本发明的第 2 特征在于，配备：在上述第 1 特征的本发明的 IC 卡中，当接收来自上述外部装置的指令时，判定上述指令的内容，将比上述帧等待时间短的设定时间设定在上述间隔定时器中，启动上述间隔定时器的间隔定时器设定装置。 这里，上述间隔定时器设定装置的处理最好是通过上述运算处理装置执行。根据该第 2 特征，由于能够根据来自外部装置的接收指令的内容来调整设定时间，能够谋求更有效地提高通信效率和处理效率。

更理想的情况是，本发明的第 3 特征在于，在上述任一特征的本发明的 IC 卡中，上述协处理器控制装置配备：用于控制停止及恢复向上述协处理器的工作时钟的供给的控制标记；根据上述控制标记的状态，控制向上述协处理器的工作时钟供给的停止及恢复的工作时钟控制装置；接受上述中断要求信号的输出，将上述控制标记的状态设定在工作停止状态，接受上述响应输入，将上述控制标记的状态设定在工作恢复状态的控制标记设定装置。这里，上述控制标记设定装置的处理最好通过上述运算处理装置执行。根据该第 3 特征，上述协处理器控制装置能够具体地得到实现，起到上述第 1 或者第 2 特征 IC 卡的作用效果。

更理想的情况是，本发明的第 4 特征在于，在上述第 3 特征的本发明的 IC 卡中，当上述运算处理装置停止向上述协处理器供给工作时钟时，向上述外部装置输出帧等待时间延长要求，当从上述外部装置接受该响应输入时，将上述控制标记的状态设定在工作恢复状态。这里，上述控制标记设定装置的处理通过上述运算处理装置执行。根据该第 4 特征，由于在上述协处理器的运算处理中断中，执行用于帧等待时间延长要求的与外部装置的通信，能够避免成为供电不足的情况，使帧等待时间延长成为可能，起到上述第 1 或者第 2 特征的 IC 卡的作用效果。

更理想的情况是，本发明的第 5 特征在于，在上述任一特征的本发明的 IC 卡中，配备存储通常处理用的程序的非易失性存储器和比上述非易失性存储器工作功耗低的第 2 存储器，至少在上述协处理器工作时，上述协处理器所处理的程序存储在上述第 2 存储器中。进而，在上述协处理器工作时，最好禁止对上述非易失性存储器进行存取。根据该第 5 特征，可谋求降低上述协处理器的运算处理时的功耗，特别是更有效地谋求解决非接触型 IC 卡中的供电方面的问题。

更理想的情况是，本发明的特征在于：在上述任一特征的本发明的 IC 卡中，在与上述外部装置的通信应用中，配备非接触接口及接触接口的至少某一方。也就是说，不管通信接口是非接触、接触中的某一方，能够起到上述各特征的 IC 卡的作用效果。

用于达到上述目的的本发明的 IC 卡的控制方法是在主运算处理装置以外，内置辅助运算用协处理器的 IC 卡的控制方法，其特征在于：

进行中断许可的设定，使得在经过比帧等待时间短的设定时间后输出中断要求信号；在上述中断许可设定后，开始上述协处理器的运算处理；在上述协处理器的运算处理中，当输出上述中断要求信号时，分支到中断处理，在上述中断处理中，停止向上述协处理器的工作时钟供给，当接受来自外部装置的规定的响应输入时，恢复上述工作时钟的供给。

另外，在上述特征的本发明的IC卡控制方法中，最好是当接收来自上述外部装置的指令时，判定上述指令是否是上述协处理器的执行指令，在是上述协处理器的执行指令的情况下，进行上述中断许可的设定。进而，在上述中断处理中，最好是在停止向上述协处理器的工作时钟供给后，向上述外部装置输出帧等待时间延长要求，当从上述外部装置接受该响应输入时，恢复上述工作时钟的供给。

附图说明

图1是表示被ISO14443规定的非接触型IC卡或者组合型IC卡的非接触工作时的初始响应例的流程图。

图2是表示在现有的LC卡中在协处理器运算前进行帧等待时间延长处理的情况下的处理顺序的说明图。

图3是表示本发明的IC卡的硬件结构的一例的系统结构图。

图4是表示在本发明的LC卡中发生帧等待时间延长用中断、进行帧等待时间延长处理的情况下的处理顺序的说明图。

图5是表示在本发明的IC卡中不发生帧等待时间延长用中断、不进行帧等待时间延长处理的情况下的处理顺序的说明图。

图6是表示本发明的IC卡的控制处理顺序的一例的流程图。

图7是表示图6所示的流程图的初始化处理（步骤S2）的子程序的流程图。

图8是表示图6所示的流程图的协处理器运算处理（步骤S8）的子程序的流程图。

图9是表示图6所示的流程图的步骤S8内的中断处理的子程序的流程图。

图10是表示图9所示的流程图的S-WTX要求发送接收处理（步骤SInt3）的子程序的流程图。

图 11 是表示被 ISO7816-3 规定的接触型 IC 卡的接触工作时的初始响应例的流程图。

具体实施方式

现参照附图说明本发明的 IC 卡的一个实施例。

（第 1 实施例）

首先，参照图 3 的系统结构图说明本发明的 IC 卡的硬件结构。在本第 1 实施例中，假想是非接触型 IC 卡并进行说明。

本发明的非接触型 IC 卡 17 是内置了作为主运算处理装置的 CPU5 和 CPU5 以外的密码处理等辅助运算用的协处理器 3 的 IC 卡，配备：进行向协处理器 3 供给协处理器工作时钟的供给停止及供给恢复的工作时钟控制标记 1；控制协处理器 3 的工作时钟的供给停止及供给恢复的工作时钟控制电路 2；以及间隔定时器 4。另外，还配备：用于发送/接收从作为外部装置的读写装置 14 发生的信号的天线 15；连接在天线 15 上的 RF 电路 13；连接在 RF 电路 13 上的通信接口 9；以及连接在 RF 电路 13 上的工作时钟生成电路 10。进而，为了存储用于通过 CPU5 的处理而执行对本结构的 IC 卡的控制的控制用程序，还配备闪速存储器等非易失性存储器 12 及静态 RAM 等 RAM11。

RF 电路 13 解调从读写装置 14 接收到的信号，将数据传送给通信接口 9。另外，通过天线 15 将从通信接口 9 传送来的数据发送到读写装置 14。进而，从读写装置 14 接收到的信号中抽出时钟，将时钟供给工作时钟生成电路 10。

在工作时钟生成电路 10 中，为了使非接触型 IC 卡 17 内的各种电路工作，生成工作时钟 16，将工作时钟 16 供给工作时钟控制电路 2、CPU5、间隔定时器 4、通信接口 9 等。

工作时钟控制标记 1、协处理器 3、间隔定时器 4、CPU5、通信接口 9、非易失性存储器 12 及 RAM11 用数据总线 6 相互连接构成，同时，从 CPU5 输出的控制信号组 7 被输入到工作时钟控制标记 1、协处理器 3、间隔定时器 4、通信接口 9、非易失性存储器 12 及 RAM11 中。该控制信号组 7 例如用地址信号、读出信号、写入信号等构成。另外，从间隔定时器 4 输出的中断要求信号 8 被输入到 CPU5 中。

CPU5 使用数据总线 6 和控制信号组 7，通过执行上述控制用程序，

能够控制工作时钟控制标记 1、协处理器 3、间隔定时器 4、通信接口 9、非易失性存储器 12 及 RAM11 的工作。例如，CPU5 能够通过数据总线 6，用由任意的地址信号和写入信号构成的控制信号组 7，对间隔定时器 4 写入任意的数据，使之进行任意的计数工作。通过 CPU5，启动了的间隔定时器 4 经过所指定的设定时间后，能够向 CPU5 输出中断要求信号 8，CPU5 通过接收该中断要求信号 8，进行中断处理，识别帧等待时间经过的情况。中断处理用的程序被存储在非易失性存储器 12 或者 RAM11 内，在该处理中，能够使用通信接口 9，在与读写装置 14 之间执行用于帧等待时间延长的发送接收处理。

另外，能够用由任意的地址信号和写入信号构成的控制信号组 7，通过数据总线 6，对工作时钟控制标记 1 写入数据“0”或者数据“1”，也能够用由任意的地址信号和读出信号构成的控制信号组 7，通过数据总线 6 读出工作时钟控制标记 1 的内容。

另外，CPU5 能够用由任意的地址信号和写入信号构成的控制信号组 7，通过数据总线 6，对协处理器 3 进行任意数据的写入，进行任意的运算。协处理器 3 仅仅在从工作时钟生成电路 10 供给工作时钟 16 时才能够工作，当不从工作时钟生成电路 10 供给工作时钟时，停止运算处理。

控制协处理器 3 的工作时钟的停止及恢复的工作时钟控制电路 2 输入在工作时钟生成电路 10 中所生成的工作时钟 16 和工作时钟控制标记 1 的状态。工作时钟控制电路 2 例如用“或”电路构成，控制是否对协处理器 3 供给工作时钟。在这种情况下，在工作时钟控制标记 1 的内容为数据“0”的情况下，工作时钟控制电路 2 对协处理器 3 供给从工作时钟生成电路 10 所供给的工作时钟 16。在工作时钟控制电路 1 的内容为数据“1”的情况下，工作时钟控制电路 2 不对协处理器 3 供给从工作时钟生成电路 10 所供给的工作时钟 16。

在上述硬件结构中，通过用工作时钟控制标记 1、工作时钟控制电路 2 及 CPU5 对工作时钟控制标记 1 设定数据“0”或者“1”的方法，提供根据来自间隔定时器 4 的中断要求信号 8 的输出，停止向协处理器 3 的工作时钟的供给，根据来自外部装置的规定的响应输入，恢复工作时钟的供给，控制协处理器的工作的协处理器控制方法。

根据上述硬件结构，CPU5 通过控制工作时钟控制标记 1，能够控

制协处理器 3 的工作的中断、恢复。

接着，利用上述硬件结构，参照图 3、图 4 及图 5，说明非接触型 IC 卡 17 与读写装置 14 之间的帧等待时间延长的一系列控制顺序。此外，非接触型 IC 卡 17 与读写装置 14 之间的通信协议遵照 ISO14443-3 及 ISO14443-4。

上述帧等待时间延长的控制方法作为 CPU5 所执行的控制用程序，被存储在非易失性存储器 12 中。上述控制顺序由 CPU5 利用上述外围硬件用软件进行处理。

图 4 是在非接触型 IC 卡 17 的指令执行中（协处理器 3 的运算处理执行中），由于作为帧等待时间延长用定时器而利用的间隔定时器 4 溢出，发生 S-WTX 要求发送接收情况的工作实例。现实施以下（1）~（9）的处理。

图 5 是在非接触型 IC 卡 17 的指令执行中（协处理器 3 的运算处理执行中），作为帧等待时间延长用定时器而利用的间隔定时器 4 不溢出，不发生 S-WTX 要求发送接收情况的工作实例。在这种情况下，实施以下（1）~（3）及（9）的处理。

在本实施例中，被构成为使得协处理器 3 的工作和读写装置 14 与非接触型 IC 卡 17 的通信不同时进行。

处理（1）：读写装置 14 通过 I 块向 IC 卡发送任意的指令。在非接触型 IC 卡 17 中内置的 CPU5 接收该指令，判定指令的内容。而且，在间隔定时器 4 中设定帧等待时间经过前发生定时器中断的计数值后，允许定时器中断，启动帧等待时间延长用的间隔定时器 4。

处理（2）：CPU5 进行指令的执行处理（协处理器运算处理）。

处理（3）：CPU5 监视协处理器 3 的运算处理结束，如果检测出运算处理结束，执行下述的处理（9）。

处理（4）：在上述处理（3）中，在检测出运算处理结束之前，帧等待时间延长用的间隔定时器 4 溢出的情况下，通过发生中断要求信号 8，向非接触型 IC 卡 17 的中断启动程序分支，执行处理（5）~（8）。

处理（5）：CPU5 将数据“1”设置在工作时钟控制标记 1 上，通过工作时钟控制电路 2 停止向协处理器 3 供给工作时钟 16。据此，协处理器 3 的工作成为暂时停止（Suspend）状态。

处理（6）：CPU5 调用 S-WTX 要求发送接收处理。在该处理中，CPU5 向读写装置 14 发送帧等待时间延长要求（S-WTX 要求）。此外，S-WTX 要求是根据 S 块（ISO14443-4 协议的管理块）的指令的帧等待时间延长要求。

处理（7）：读写装置 14 根据 S-WTX 要求，使超时时间延长。读写装置 14 将帧等待时间延长响应（S-WTX 响应）发送到非接触型 IC 卡 17。此外，S-WTX 响应是根据对 S-WTX 要求的 S 块指令的读写装置 14 的响应。

处理（8）：CPU5 将数据“0”设置到工作时钟控制标记 1 上，通过工作时钟控制电路 2 恢复向协处理器 3 供给工作时钟 16。据此，协处理器 3 的工作成为恢复（Resume）状态。非接触型 IC 卡 17 进行中断返回，返回到处理（3）。

处理（9）：当指令的执行处理结束时，CPU5 通过 I 块（ISO14443-4 协议的信息块）将指令执行结果发送到读写装置 14。

通过上述控制顺序，在协处理器 3 的运算处理执行中，仅仅在通过间隔定时器 4 发生中断要求信号 8 时，启动通过 CPU5 的中断处理，暂时停止协处理器 3 的工作（运算处理），由于能够在延长了帧等待时间的基础上对读写装置 14 恢复协处理器 3 的工作，能够不将帧等待时间的发送接收作为引发剂对攻击者告知解析点而付诸实施，在安全性方面有利。另外，在通过间隔定时器 4 发生中断要求前，协处理器 3 的运算结束的情况下，由于能够不发生用于帧等待时间延长的通信，结束指令处理，从而能够改善通信的效率。

（第 2 实施例）

在上述第 1 实施例中，表示了协处理器 3 在工作中，构成为读写装置 14 与非接触型 IC 卡 17 的通信不同时进行的实例。这里，协处理器 3 所处理的程序例示了存储在非易失性存储器 12 内的情况。但是，协处理器 3 的工作与其执行存储在非易失性存储器 12 内的程序，不如在 RAM11 等功率消耗较少的存储器上执行，中断发生时的处理直到协处理器 3 的工作暂时停止为止，也在 RAM11 上执行，禁止向非易失性存储器 12 的存取，反倒更能降低在协处理器 3 的工作时的功耗。

另外，在帧等待时间延长时所发生的读写装置 14 与非接触型 IC 卡 17 的通信处理程序同样也是配置在 RAM11 上的一方能够谋求降低功

耗。

以下，参照图 3 的硬件结构图及图 6～图 10 的流程图，说明在 RAM11 上执行协处理器处理程序及在帧等待时间延长时所发生的读写装置 14 与非接触型 IC 之间的通信处理程序，在协处理器处理程序执行中禁止向非易失性存储器 12 存取的第 2 实施例。此外，假想非接触型 IC 卡 17 的硬件结构与第 1 实施例相同。另外，非接触型 IC 卡 17 的控制方法作为 CPU5 所执行的控制用程序存储在非易失性存储器 12 中。

首先，如图 6 所示，当从读写装置 14 通过电波开始向非接触型 IC 卡供给电力时，非接触型 IC 卡 17 开始工作（步骤 S1）。

接着，非接触型 IC 卡 17 执行初始化处理（步骤 S2）。步骤 S2 的初始化处理例如如图 7 所示，作为初始化处理的子程序构成，在该处理中，将数据发送/接收处理（步骤 S21）、中断处理（步骤 S22）、协处理器运算处理（步骤 S23）的各程序从非易失性存储器 12 传送到 RAM11。

接着，在步骤 S3 中，在非接触型 IC 卡 17 与读写装置 14 之间进行图 1 所示的初始响应工作，在 ISO14443-4 协议中，非接触型 IC 卡 17 成为能够通信的状态（激活状态）。

在步骤 S4 中，非接触型 IC 卡 17 分支到在步骤 S2 中传送到 RAM11 上的数据接收处理，等待从读写装置 14 发送来的指令（I 块指令）。

当在步骤 S4 中，非接触型 IC 卡 17 接收了来自读写装置 14 的指令（I 块指令）时，转移到步骤 S5，判定指令是否是包含协处理器 3 的执行的指令。当判定为接收的指令是包含协处理器 3 的执行的指令时，转移到步骤 S6，在间隔定时器 4 中设定在帧等待时间经过前发生定时器中断的计数值后，允许定时器中断，启动间隔定时器 4。当判定为接收指令是不包含协处理器的执行的指令的情况下，转移到步骤 S7，执行其他的处理。

在步骤 S6 中，间隔定时器 4 启动后，非接触型 IC 卡 17 分支到在步骤 S2 中存储在 RAM11 上的协处理器运算处理（步骤 S8）。

当分支到步骤 S8 时，如图 8 所示，非接触型 IC 卡 17 从 RAM11 内开始进行协处理器运算（步骤 S81），在步骤 S82 中等待协处理器 3 的运算处理结束。如果在步骤 S82 中间隔定时器 4 溢出时，发生中断

要求信号 8，启动中断处理。当中断处理启动时，非接触型 IC 卡分支到在步骤 S2 中存储到 RAM11 上的步骤 S8 内的中断处理。在步骤 S82 中间隔定时器 4 不是溢出，协处理器 3 的运算处理结束的情况下，非接触型 IC 卡 17 结束步骤 S8 的协处理器运算处理。

如图 9 所示，步骤 S8 内的中断处理在步骤 SInt1 中非接触型 IC 卡 17 停止间隔定时器 4 的工作。接着，在步骤 SInt2 中，将数据“1”设置在工作时钟控制标记 1 上，通过工作时钟控制电路 2 停止向协处理器 3 供给工作时钟 16。据此，协处理器 3 的工作成为暂时停止（Suspend）状态。接着，如图 10 所示，在步骤 SInt3 中，为了对读写装置 14 延长帧等待时间，非接触型 IC 卡 17 在步骤 SInt31 中向读写装置 14 发送 S-WTX 要求。而且，在步骤 SInt32 中等待从读写装置 14 发送 S-WTX 响应。这时，读写装置 14 延长帧等待的超时时间。当非接触型 IC 卡 17 从读写装置接收 S-WYX 响应时，转移到步骤 SInt4。

如图 9 所示，在步骤 SInt4 中，非接触型 IC 卡 17 将数据“0”设置在工作时钟控制标记 1 上，通过工作时钟控制电路 2 恢复向协处理器 3 供给工作时钟 16。据此，协处理器 3 的工作成为恢复（Resume）状态。接着，在步骤 SInt5 中，恢复间隔定时器 4 的工作，结束中断处理。

中断处理结束后，非接触型 IC 卡 17 再次返回到步骤 S82（参照图 8），等待协处理器 3 的运算处理的结束。当协处理器运算结束时，步骤 S8 的运算处理结束，在步骤 S9 中，非接触型 IC 卡 17 禁止停止间隔定时器 4 的工作和定时器中断。

当包含协处理器 3 的运算处理的指令的处理全部结束时，在步骤 S10 中，非接触型 IC 卡 17 通过 I 块将指令执行结果发送到读写装置 14。在步骤 S10 中，这分支到在步骤 S2 中传送到 RAM11 上的数据发送处理上，并被执行。

通过上述控制顺序，不同时执行协处理器 3 的工作和读写装置 14 与非接触型 IC 卡 17 的通信，在 RAM11 上执行协处理器处理程序，执行禁止向非易失性存储器 12 存取的非接触型 IC 卡的控制。

（其他实施例）

在上述各实施例中，就配备了非接触接口的非接触型 IC 卡的情况进行了说明，本发明的控制顺序及其装置也能够应用于配备了接触接

口的接触型 IC 卡。

在这种情况下，IC 卡用图 6 所示的流程图的步骤 S3 的初始响应程序，按照图 11 所示的接触型 IC 卡的初始响应处理而工作。从电源关断状态（步骤 S100）通过读写装置的 IC 卡激活工作，接触型 IC 卡进行电源接通、时钟供给、复位（步骤 S101）。接着，接触型 IC 卡向读写装置发送复位响应（步骤 S102）。然后，进行用带外部端子的 IC 卡的电信号及传输协议规格 ISO7816-3 所规定的，例如用 T=1 协议进行读写装置与接触型 IC 卡的通信（步骤 S103）。

在图 6 所示的流程图中，步骤 S3 以下的工作与配备了非接触接口的非接触型 IC 卡相同。

虽然已通过优选实施例对本发明进行了描述，但显然可知，在不背离本发明的宗旨与范围的情况下，可以由专业技术人员作各种修改和变更。因此，本发明仅仅用所附权利要求来量度。

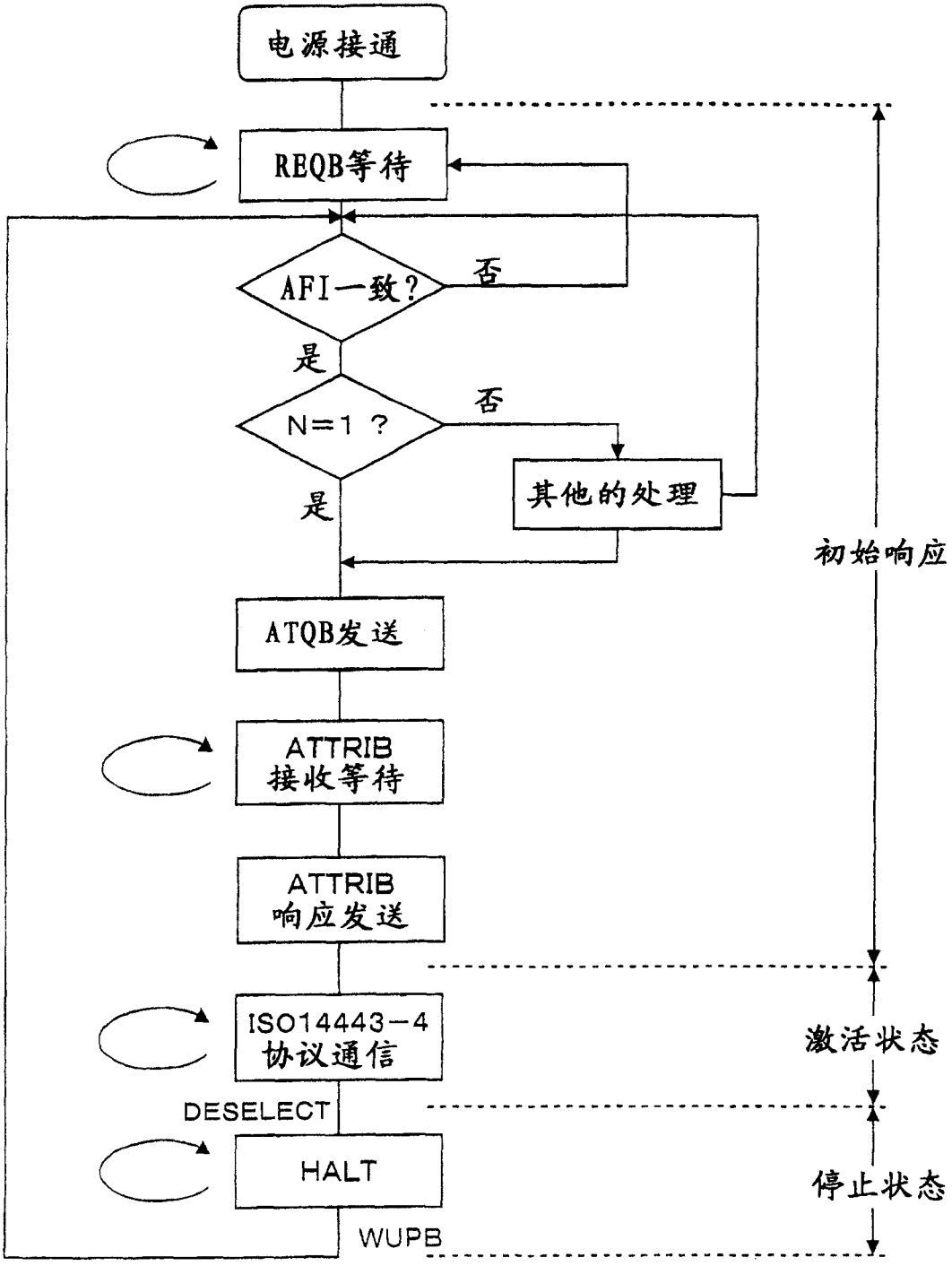

电源接通
REQB等待
AFI一致?
否
是
N=1 ?
否
是
其他的处理
ATQB发送
ATTRIB
接收等待
ATTRIB
响应发送
ISO14443-4
协议通信
DESELECT
HALT
WUPB
初始响应
激活状态
停止状态

图 1

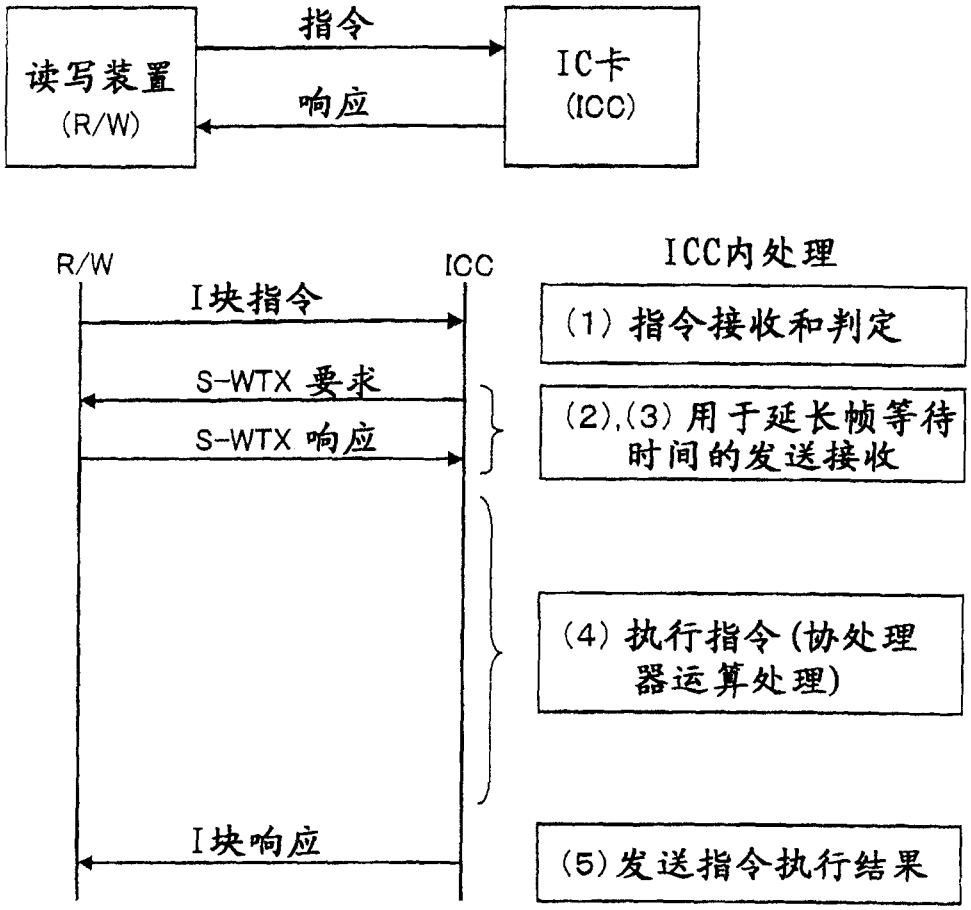

读写装置
(R/W)
指令
响应
IC卡
(ICC)
R/W
ICC
ICC内处理
I块指令
(1) 指令接收和判定
S-WTX 要求
S-WTX 响应
(2),(3) 用于延长帧等待时间的发送接收
(4) 执行指令(协处理器运算处理)
I块响应
(5)发送指令执行结果

图 2

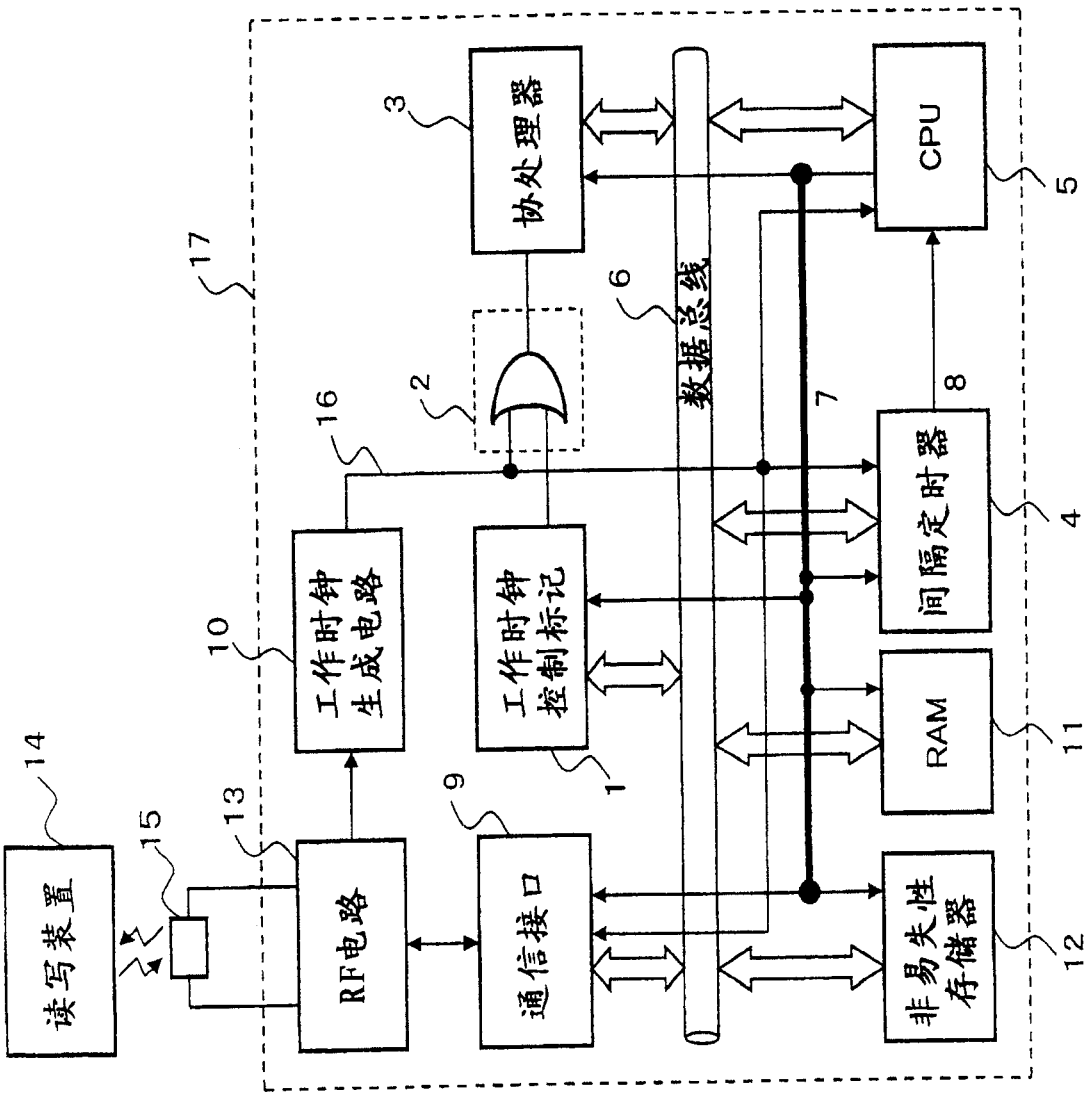

读写装置
14
15
13
RF电路
9
通信接口
工作时钟
生成电路
10
工作时钟
控制标记
1
16
2
协处理器
3
17
数据总线
6
CPU
5
间隔定时器
4
8
7
RAM
11
非易失性
存储器
12

图 3

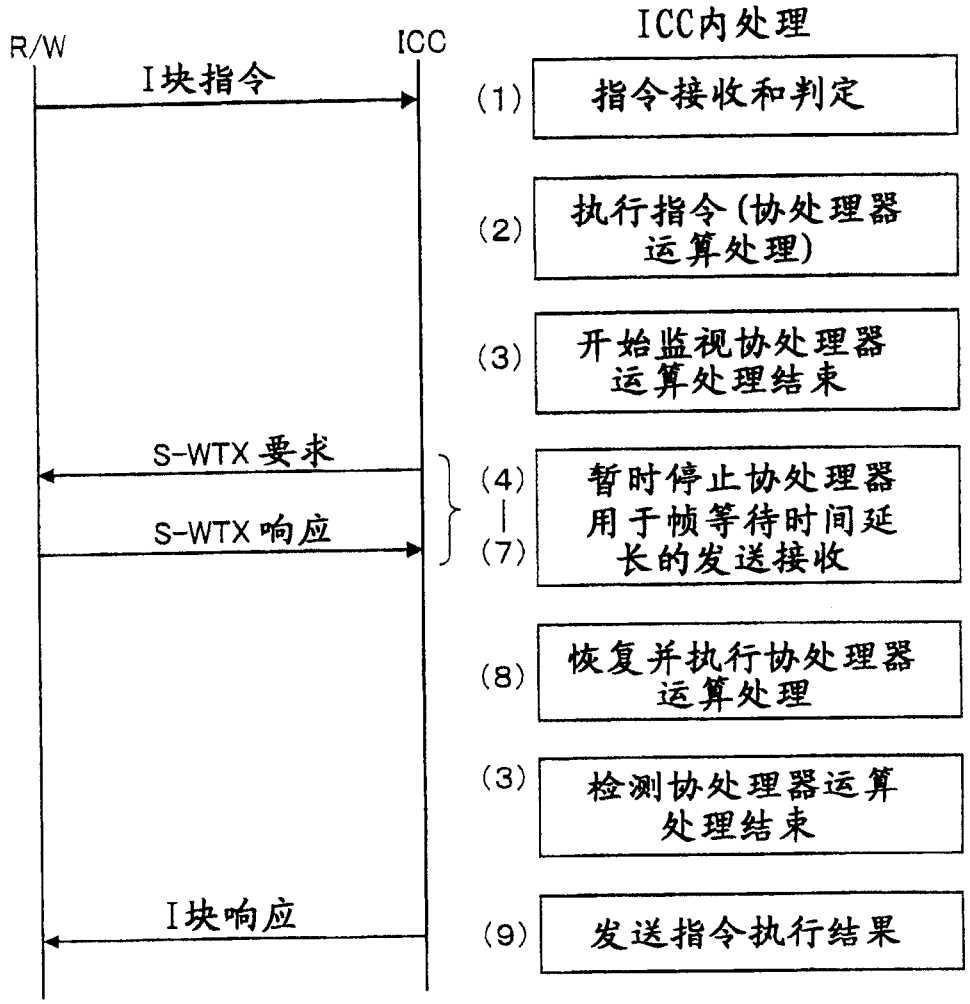

R/W
ICC
ICC内处理
I块指令
(1)
指令接收和判定
(2)
执行指令(协处理器运算处理)
(3)
开始监视协处理器运算处理结束
S-WTX 要求
S-WTX 响应
(4)
|
(7)
暂时停止协处理器用于帧等待时间延长的发送接收
(8)
恢复并执行协处理器运算处理
(3)
检测协处理器运算处理结束
I块响应
(9)
发送指令执行结果

图 4

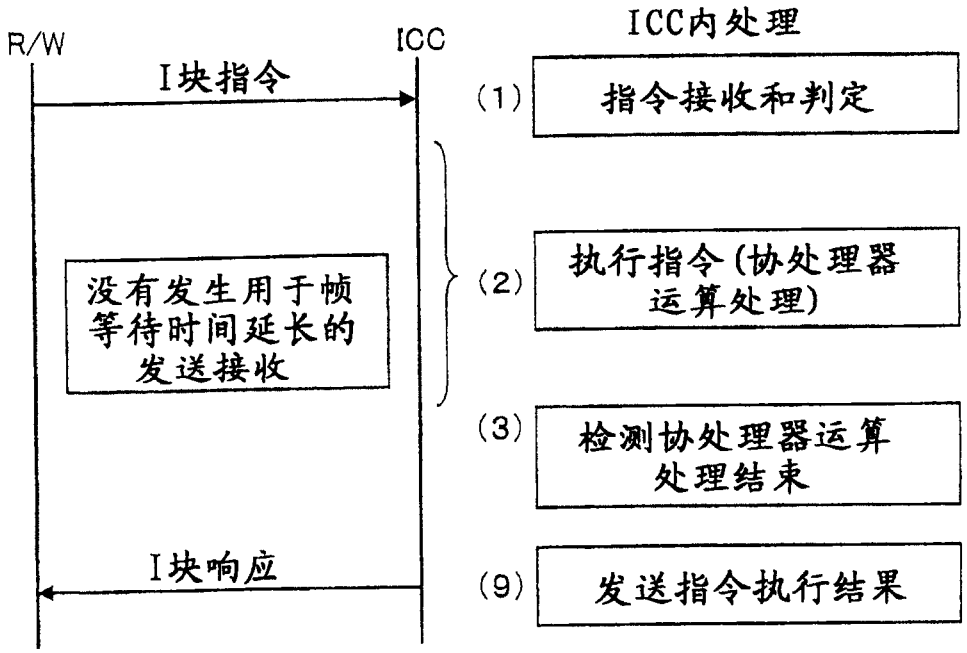

R/W
ICC
ICC内处理
I块指令
(1)
指令接收和判定
没有发生用于帧等待时间延长的发送接收
(2)
执行指令(协处理器运算处理)
(3)
检测协处理器运算处理结束
I块响应
(9)
发送指令执行结果

图 5

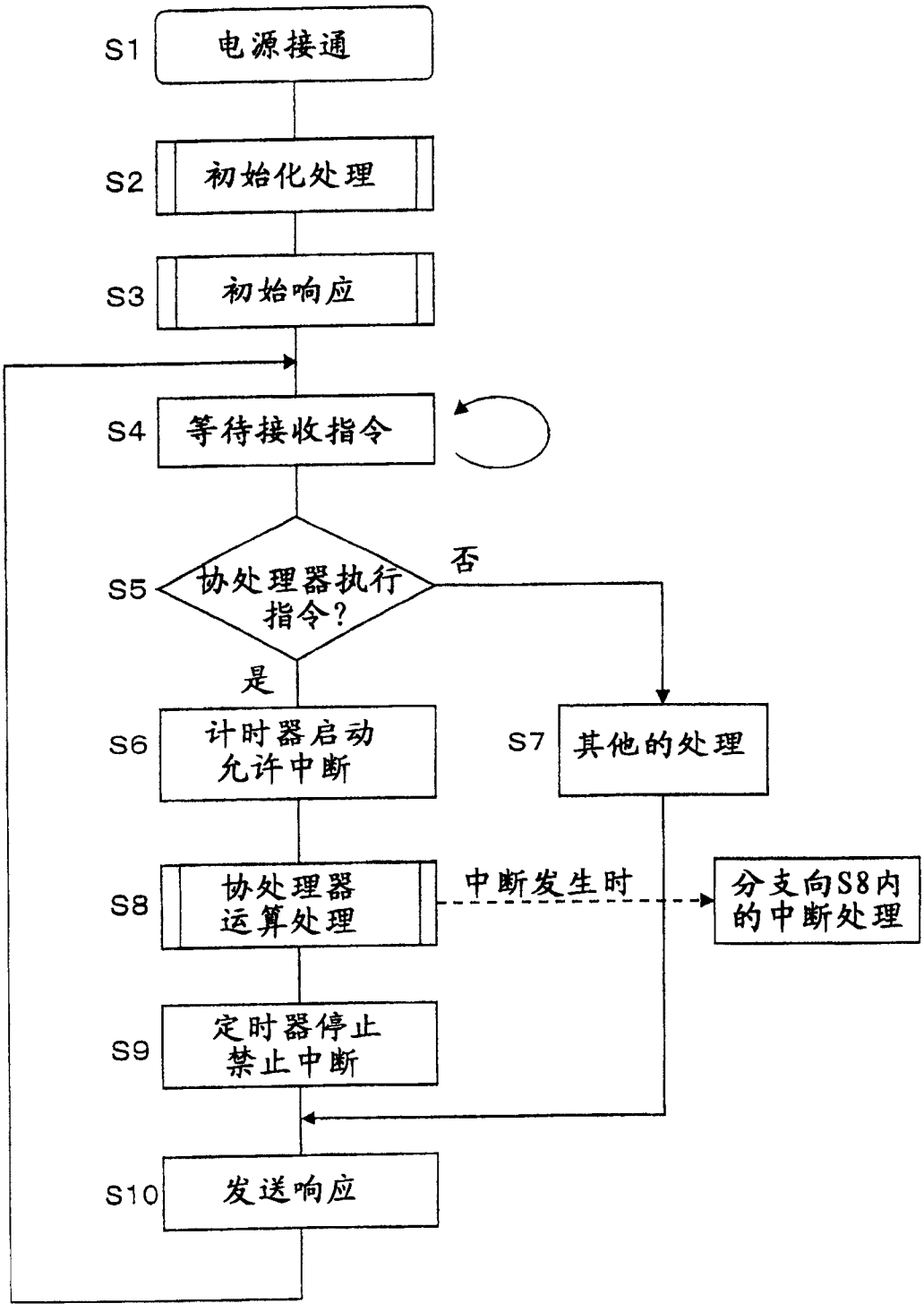

S1
电源接通
S2
初始化处理
S3
初始响应
S4
等待接收指令
S5
协处理器执行指令?
否
是
S6
计时器启动
允许中断
S7
其他的处理
S8
协处理器
运算处理
中断发生时
分支向S8内的中断处理
S9
定时器停止
禁止中断
S10
发送响应

图 6

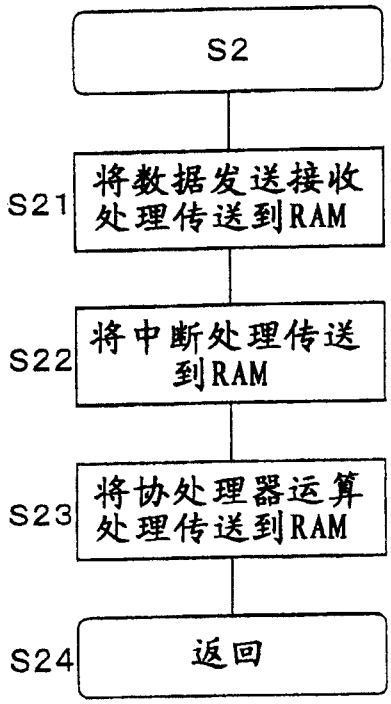

S2
S21
将数据发送接收处理传送到RAM
S22
将中断处理传送到RAM
S23
将协处理器运算处理传送到RAM
S24
返回

图 7

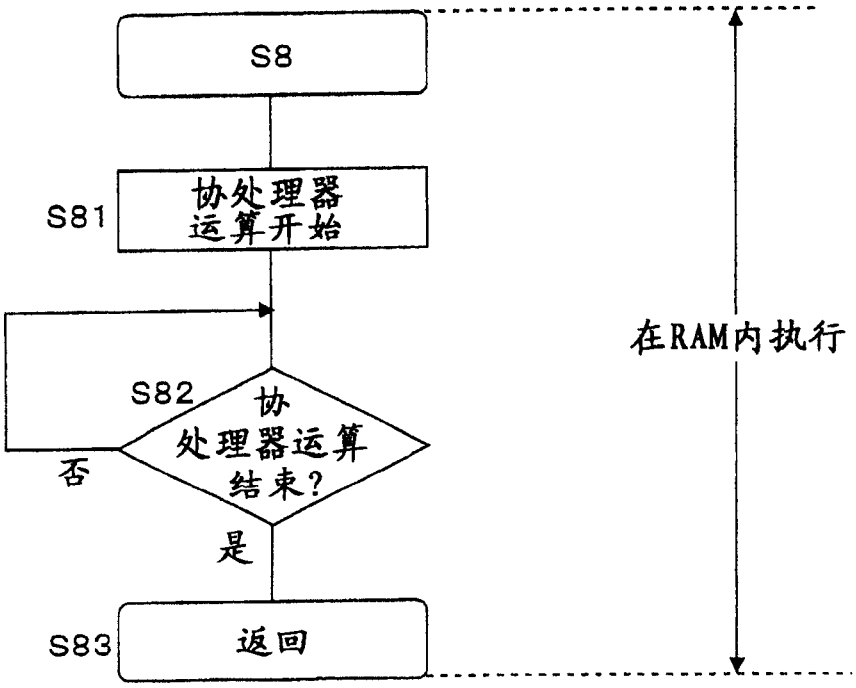


图 8

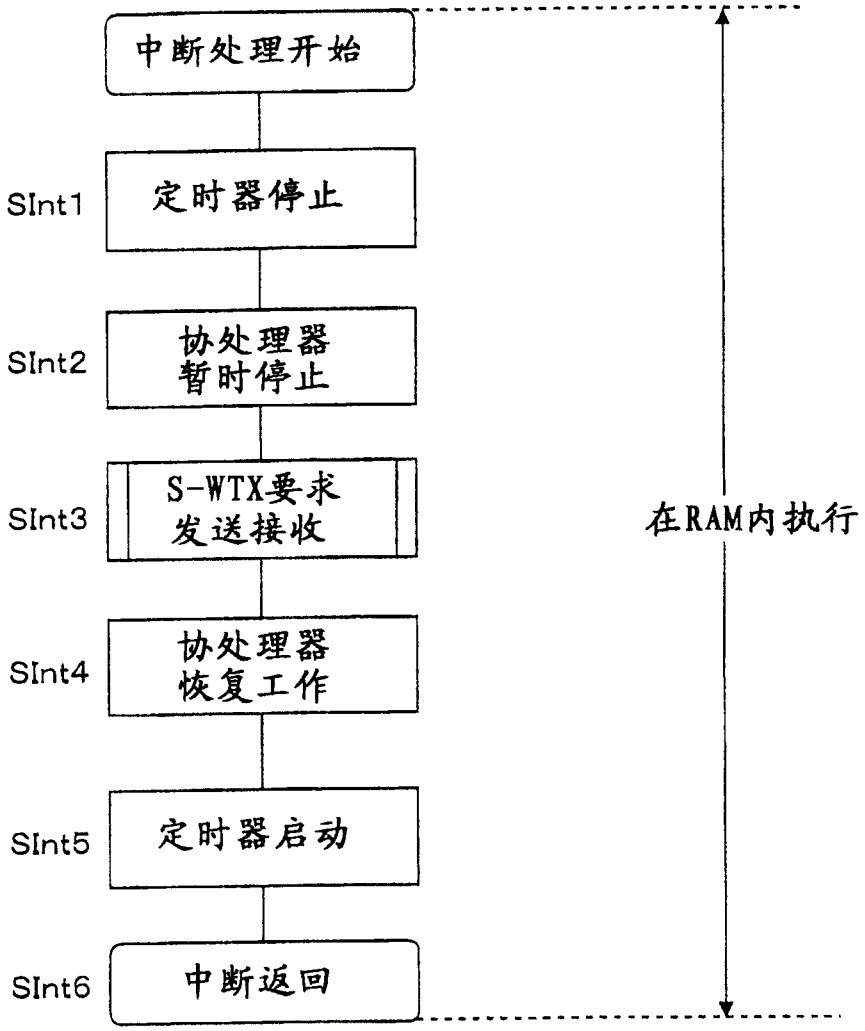

中断处理开始
SInt1
定时器停止
SInt2
协处理器
暂时停止
SInt3
S-WTX要求
发送接收
SInt4
协处理器
恢复工作
SInt5
定时器启动
SInt6
中断返回
在RAM内执行

图 9

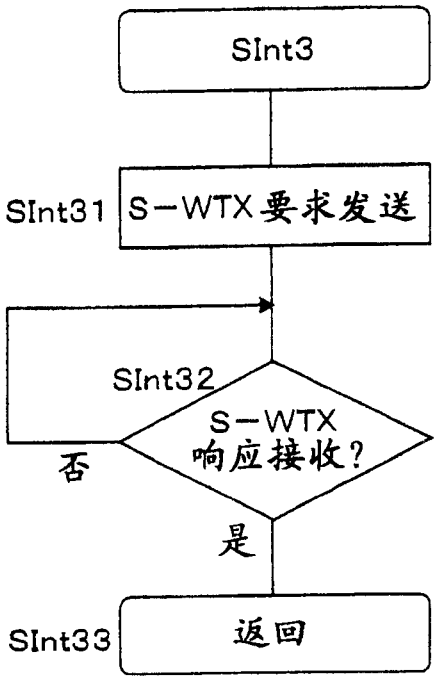


图 10

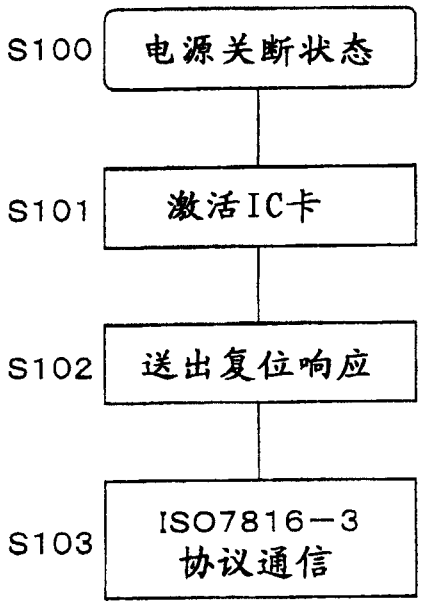


图 11