(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 101504785 B
(45)授权公告日 2013.01.02

(21)申请号 200910008210.4
(22)申请日 2006.10.19
(30)优先权数据
303838/2005 2005.10.19 JP
(62)分案原申请数据
200610136086.6 2006.10.19
(73)专利权人 日立欧姆龙金融系统有限公司
地址 日本东京都
(72)发明人 今井启允 佐川大介 山口章
(74)专利代理机构 永新专利商标代理有限公司 72002
代理人 杨谦 胡建新
(51)Int.Cl.
G07F 7/12(2006.01)
G07F 19/00(2006.01)

(56)对比文件
JP 特开平10-312459 A,1998.11.24, 全文.
JP 特开2001-168855 A,2001.06.22, 全文.
CN 1272188 A,2000.11.01, 全文.

审查员 王立升

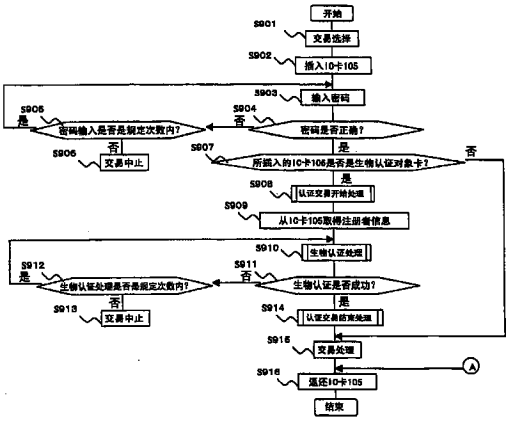
权利要求书 3 页 说明书 14 页 附图 12 页

(54)发明名称

生物体认证控制方法及现金自动交易装置

(57)摘要

本发明的目的为,在使用IC卡的生物体认证系统及其方法中,实现生物体信息的高隐秘性。本发明的生物体认证控制方法对生物体认证进行控制,从便携式电子装置接收预处理数据并发送给生物体认证机构部,使生物体认证机构部组合第2生物体信息和预处理数据制成认证数据,接收认证数据,将认证数据发送给便携式电子装置,使注册数据和认证数据在上述便携式电子装置内进行比对,从便携式电子装置接收表示注册数据和认证数据之间的认证结果的认证结果数据,将认证结果数据发送给生物体认证机构部,使生物体认证机构部根据认证结果数据制成与生物体认证是否成功有关的信息,从生物体认证机构部接收与生物体认证是否成功有关的信息。



CN 101504785 B

1. 一种生物体认证控制方法，对生物体认证进行控制，其特征在于，

控制部从便携式电子装置接收预处理数据，该预处理数据是从第 1 生物体信息获得且预先存储在上述便携式电子装置内的信息，

上述控制部将所接收的上述预处理数据发送给生物体认证机构部，

上述控制部使上述生物体认证机构部组合由上述生物体认证机构部取得的第 2 生物体信息和上述预处理数据，制成认证数据，

上述控制部从上述生物体认证机构部接收上述认证数据，

上述控制部将所接收到的上述认证数据发送给上述便携式电子装置，

上述控制部使注册数据和上述认证数据在上述便携式电子装置内进行比对，该注册数据是组合上述第 1 生物体信息和上述预处理数据而制成的信息，且是预先存储在上述便携式电子装置内的信息，

上述控制部从上述便携式电子装置接收表示上述注册数据和上述认证数据之间的认证结果的认证结果数据，

上述控制部将所接收的上述认证结果数据发送给上述生物体认证机构部，

上述控制部使上述生物体认证机构部根据上述认证结果数据制成与生物体认证是否成功有关的信息，

上述控制部从上述生物体认证机构部接收上述与生物体认证是否成功有关的信息。

2. 根据权利要求 1 所述的生物体认证控制方法，其特征在于，

上述预处理数据包含不能确定个人的信息，上述认证数据包含能够确定个人的信息。

3. 根据权利要求 1 所述的生物体认证控制方法，其特征在于，

上述认证数据包含以上述预处理数据作为加密密钥对第 2 生物体信息加密后的信息。

4. 根据权利要求 1 所述的生物体认证控制方法，其特征在于，

判断上述便携式电子装置中所存储的辅助认证方式是否是便携式电子装置内认证方式，如果是便携式电子装置内认证方式，则使上述注册数据和上述认证数据进行比对。

5. 根据权利要求 1 所述的生物体认证控制方法，其特征在于，

判断上述生物体认证机构部上所放置的手指是否是生物体，如果是生物体，则使上述注册数据和上述认证数据进行比对。

6. 根据权利要求 1 所述的生物体认证控制方法，其特征在于，

上述预处理数据包含使用不可逆转换处理的算法根据上述第 1 生物体信息所制成的信息，上述认证数据包含使用不可逆转换处理的算法根据上述第 2 生物体信息所制成的信息。

7. 根据权利要求 1 所述的生物体认证控制方法，其特征在于，

上述预处理数据包含不能从上述预处理数据本身还原上述第 1 生物体信息的信息，上述认证数据包含不能从上述认证数据本身还原上述第 2 生物体信息的信息。

8. 一种现金自动交易装置，自动进行现金的交易，其特征在于，

具有：

卡机构部，读取 IC 卡的信息；

生物体认证机构部，取得利用上述现金自动交易装置的使用者的生物体特征量；以及

控制部，上述控制部从上述卡机构部接收预处理数据，该预处理数据是从第 1 生物体

信息获得且预先存储在 IC 卡内的信息，并且上述控制部将所接收的上述预处理数据发送给上述生物体认证机构部，使上述生物体认证机构部组合由上述生物体认证机构部取得的第 2 生物体信息和上述预处理数据，制成认证数据，上述控制部从上述生物体认证机构部接收上述认证数据，将所接收到的上述认证数据发送给上述 IC 卡，使注册数据和上述认证数据在上述 IC 卡内进行比对，该注册数据是组合上述第 1 生物体信息和上述预处理数据而制成的信息，且是预先存储在上述 IC 卡内的信息，上述控制部从上述 IC 卡接收表示上述注册数据和上述认证数据之间的认证结果的认证结果数据，将所接收的上述认证结果数据发送给上述生物体认证机构部，使上述生物体认证机构部根据上述认证结果数据制成与生物体认证是否成功有关的信息，上述控制部从上述生物体认证机构部接收上述与生物体认证是否成功有关的信息。

9. 根据权利要求 8 所述的现金自动交易装置，其特征在于，

上述生物体认证机构部具有 ：生物体照射部，对该生物体认证机构部上所放置的生物体照射光 ；以及图像取得部，取得由上述生物体照射部照射的上述生物体的图像 ；

根据由上述图像取得部所取得的上述生物体特征量、和从上述 IC 卡经由上述控制部所接收到的上述预处理数据，按照不可逆转换处理的算法生成上述认证数据。

10. 根据权利要求 9 所述的现金自动交易装置，其特征在于，

上述控制部存储执行生物体信息认证处理的认证控制中间件，根据所存储的上述认证控制中间件，按照指示在上述生物体认证机构部生成上述认证数据，将所生成的上述认证数据发送给上述 IC 卡。

11. 根据权利要求 8 所述的现金自动交易装置，其特征在于，

上述控制部还从上述生物体认证机构部接收在生物体的哪个部位上生物体认证成功与否的信息，输出认证失败时的原因。

12. 根据权利要求 8 所述的现金自动交易装置，其特征在于，

上述卡机构部建立和上述 IC 卡之间的连接，并且从上述 IC 卡读出生物体认证中的辅助信息，发送给上述控制部，

上述控制部根据所接收到的上述辅助信息，在 IC 卡内认证处理时继续上述认证处理，在装置内认证处理时从上述卡机构部吐出上述 IC 卡。

13. 根据权利要求 8 所述的现金自动交易装置，其特征在于，

上述控制部响应上述 IC 卡的认证处理，执行使用者所选择的交易，在上述认证处理的结果为失败时，将从上述 IC 卡所接收到的上述预处理数据再次发送给上述生物体认证机构部，再次执行认证处理。

14. 根据权利要求 8 所述的现金自动交易装置，其特征为，

具有 ：

纸币存取部，进行纸币存取 ；以及

操作部，向使用者显示操作内容，受理来自使用者的输入 ；

上述控制部通过上述操作部受理使用者所希望的支付交易，在响应上述 IC 卡的认证处理并且其结果为成功时，从上述纸币存取部吐出纸币。

15. 根据权利要求 8 所述的现金自动交易装置，其特征在于，

具有操作部，显示与交易相关的操作内容，检测来自使用者的输入，

上述控制部通过上述操作部检测使用者所希望的余额查询，在响应上述 IC 卡的认证处理并且其结果为上述比对结果已成功时，在上述操作部上显示存款或借款余额，随后，若由上述操作部受理了需要认证的交易，则将从上述 IC 卡接收且存储的上述预处理数据再次发送给上述生物体认证机构部，根据从生物体认证机构部新输入的生物体特征量、和再次输出的上述预处理数据，生成认证数据。

16. 根据权利要求 8 所述的现金自动交易装置，其特征在于，

上述控制部在使用者所选择的交易结束之前暂时存储上述预处理数据，随着交易结束，对上述预处理数据进行删除处理。

生物体认证控制方法及现金自动交易装置

[0001] 本发明为下述申请的分案申请，原申请信息如下：

[0002] 申请日：2006 年 10 月 19 日

[0003] 申请号：200610136086.6

[0004] 发明名称：IC 卡内认证系统

技术领域

[0005] 本发明涉及在现金自动出纳装置 (ATM) 等中使用的生物体认证系统。

背景技术

[0006] 以往，在由现金自动出纳装置 (ATM) 等进行的生物体认证系统中，有如下系统。

[0007] 在专利文献 1（日本特开 2000-215294 号公报）中，记述了生物体识别信息内置型 IC 卡及其本人认证方法。该技术为，在使用 IC 卡的本人认证方法中，在 IC 卡中内置生物体识别信息，由 IC 卡内的生物识别比对处理部对该生物体识别信息和本人原有的生物体信息识别信息进行处理，进行本人认证。

[0008] 在专利文献 2（日本特开 2005-115800 号公报）中，记述了使用生物体信息的个人认证方法。该技术为，分割从使用者所取得的生物体信息，分别把一部分存储于电子卡中，把另一部分存储于数据库中，当进行认证时，从电子卡使用者取得生物体信息，从上述电子卡读出一部分生物体信息，随后检索和该一部分生物体信息相关的另一部分生物体信息是否存在于上述数据库中，存在时结合这些生物体信息，和前面所取得的电子卡使用者的生物体信息进行比较，进行认证判断。

[0009] 在专利文献 3（日本特开平 10-312459 号公报）中，记述了使用便携式电子装置及生物体信息的个人认证方法。该技术为，事先在 IC 卡等便携式电子装置中存储注册数据（生物体信息的特征量），通过在 IC 卡内比对认证时得到的特征数据（生物体信息的特征量）和注册数据，来实施认证。

[0010] 在专利文献 1 中，虽然在存储有生物体信息的 IC 卡内进行生物体认证，但是因为在 IC 卡内按原状存储生物体信息，所以存在因 IC 卡的失窃・遗失而使生物体信息泄漏的可能性。

[0011] 在专利文献 2 中，虽然将生物体信息分开到电子卡和数据库这 2 个中进行存储（注册），在认证时将它们 2 个结合，但是还需要在数据库中存储很多使用者的数据并且始终进行管理，处理较为麻烦。

[0012] 在专利文献 3 中，在从生物体信息提取生物体特征量并作为注册数据进行存储的 IC 卡内，对认证时新得到的生物体特征量和注册数据进行比对，并用其进行生物体认证，但是因为在便携式电子装置（IC 卡）和数据处理装置（IC 卡终端）之间传输了生物体特征量，所以在该传输过程中存在作为个人信息的生物体特征量泄漏的可能性。

发明内容

[0013] 本发明的目的为，在使用 IC 卡的生物体认证系统及其方法中，实现生物体信息的高隐秘性。

[0014] 为了解决上述课题，实施 IC 卡内认证方式，该 IC 卡内认证方式通过便携式电子装置（IC 卡）内的认证程序来进行生物体认证处理。本发明的生物体认证控制方法进行如下动作，从便携式电子装置接收由生物体信息得到的预处理数据，将上述预处理数据发送给生物体认证机构部，从上述生物体认证机构部接收将通过上述生物体认证机构部所取得的生物体信息和上述预处理数据组合制成的认证数据，将所接收到的上述认证数据发送给上述便携式电子装置，使预先存储在上述便携式电子装置内的注册数据和上述认证数据，在上述便携式电子装置内进行比对。

[0015] 本发明为了对 IC 卡、认证装置进行数据的传输和认证处理指示而采用了认证控制软件，由此可以提供一种安全性较高的生物体认证方式。再者，通过使构成认证控制软件的认证控制应用程序和认证控制中间件制成可以适应不同的多种认证方式，因而在多个认证中，在终端中装载有对多个生物体的认证装置时，可以实现适应多个各种认证装置的控制。

附图说明

[0016] 图 1 是本发明生物体信息注册处理系统的概要图例。

[0017] 图 2 是本发明生物体信息注册处理系统的框图例。

[0018] 图 3 是生物体信息注册处理的说明图。

[0019] 图 4 是生物体信息注册处理的流程图例。

[0020] 图 5 是生物体认证处理系统的概要图例。

[0021] 图 6 是生物体认证处理系统的框图例。

[0022] 图 7 是认证控制软件的结构图例。

[0023] 图 8 是生物体认证处理的说明图。

[0024] 图 9 是包括使用 IC 卡内认证方式的生物体认证处理在内的交易流程图例。

[0025] 图 10 是认证交易开始处理的流程图例。

[0026] 图 11 是生物体认证处理的流程图例。

[0027] 图 12 是认证交易结束处理的流程图例。

[0028] 具体实施方式

[0029] 下面，对于使用本发明的一个实施方式进行说明。

[0030] （实施例 1）

[0031] 在本实施方式中，大致分为生物体信息注册处理和生物体认证处理这 2 个进行说明，该生物体信息注册处理为，在金融机构的营业所中，在操作员（窗口营业员）和使用者间，对使用者持有的便携式电子装置、特别是 IC 卡，注册使用者的生物体信息（例如，手指静脉）；该生物体认证处理为，使用设置于金融机构、便利店等中的主要自动进行涉及现金的交易的现金自动交易装置、现金自动出纳机 (ATM)，并使用使用者的生物体信息进行认证。用图 1 ～ 4 来说明生物体信息注册处理，用图 5 ～ 12 来说明生物体认证处理。

[0032] 首先，简单说明生物体信息的注册处理和认证处理的概要。

[0033] 在生物体信息注册处理中，从使用者的手指静脉提取特征量，生成预处理数据，并

且还生成注册数据，注册在 IC 卡中。在该处理的过程中使用的窗口终端和附带 IC 卡装置的生物体信息注册装置连接，注册用的生物体信息（预处理数据、注册数据）被加密，并且不经由窗口终端而从生物体信息注册装置直接向 IC 卡传送，并执行写入。

[0034] 另一方面，在生物体认证处理中，将来自使用者手指静脉的特征量和 IC 卡中所注册的预处理数据、注册数据，基于特有的认证、比对技术来执行其处理。在该处理的过程中以 ATM 为中心，利用通过与 ATM 连接的生物体认证机构部新取得的生物体信息和从 IC 卡所读出的预处理数据，生成认证数据，将其传输给 IC 卡，并在 IC 卡内进行认证处理。

[0035] 在本发明的说明中，虽然采用生物体信息的注册处理使用营业所系统并且认证处理使用 ATM 的方式，来进行说明，但是也可以采用在营业所系统中还进行认证处理并且在 ATM 中还进行注册处理的方式。但是，生物体信息的注册处理即使在明确是本人的基础上，也最好在操作员在场的营业所系统中执行。另外，虽然作为预先注册生物体信息的媒体，以 IC 卡为例进行了说明，但是不限于此，也可以是移动电话或 RFID(Radio-Frequency-Identification :无线射频识别）标签等可携带的电子媒体（便携式电子装置），而目前最好是在对使用者最为普及的提款卡中装载了 IC 芯片的 IC 卡，可以限制系统的变更。

[0036] 图 1 是在金融机构的营业所内操作员使用的营业所系统之中特别选出与生物体信息注册有关的生物体信息注册处理系统的概要图。将具备生物体信息读取装置 102 的下述生物体信息注册装置 101 和控制该生物体信息注册装置 101 的注册用终端装置 104 连接来构成该生物体信息注册系统。该系统由金融机构的操作员（窗口营业员）来操作注册用终端装置 104，在 IC 卡 105 中注册使用者的生物体信息。具体而言，由窗口营业员对操作部 107 进行操作，通过显示于显示部 106 上的各种菜单进行选择，并且除了生物体信息的注册之外，还可以进行金融机构中各种各样的交易。

[0037] 窗口营业员将 IC 卡 105 插入作为生物体信息注册装置 101 的一个结构的 IC 卡装置 103 中，使 IC 卡 105 成为可写入的状态。另一方面，使用者将使用者自己的手指沿着图示的形状放置于生物体信息读取装置 102 上。通过窗口营业员的操作，生物体信息读取装置 102 使近红外线透过所放置的手指，并由摄像机对手指的静脉图案进行拍摄，获得其图像。从该图像提取生物体特征量，对所提取的生物体特征量施以下述的处理，由 IC 卡装置 103 对 IC 卡 105 执行记录、写入的处理。还有，生物体特征量是从手指静脉数据（静脉图案）所得到的可以确定个人的数据。

[0038] IC 卡装置 103 具有除了如上所述在 IC 卡 105 中写入信息的功能之外，还具有对存储在 IC 卡 105 中的信息进行读取的功能。也就是说，具有读取或写入功能，但是在下面将采用向 IC 卡 105 内写入生物体信息的例子，来进行说明。

[0039] 图 2 是表示图 1 中所说明的生物体信息注册处理系统的一个实施例的结构的框图。

[0040] 生物体信息注册装置 101 包括 :CPU21，控制生物体信息注册装置 101 整体 ;主存储部 202，存储各种各样的信息 ;生物体信息读取装置 102，读取生物体信息 IC 卡装置 103，在 IC 卡 105 中写入生物体信息 ;通信部 215，和注册用终端装置 104 连接。

[0041] 主存储部 202 分为存储各种程序的 ROM203 和主要存储数据并且可重写所存储的数据的 RAM204。这里，虽然作为由 ROM203、RAM204 组成的主存储部（也简单称为存储部）202 进行了说明，但是也可以是分别由硬盘、各种半导体存储器构成的结构。ROM203 具

备：注册处理程序 205，用来进行生物体信息的注册处理；注册数据制作程序 206，用来制作认证时使用的注册数据；生物体信息读取装置控制程序 207，用来控制生物体信息读取装置 102；IC 卡装置控制程序 208，用来对 IC 卡 105 进行信息的写入处理；通信控制程序 209，用来控制通信部 215。

[0042] 生物体信息读取装置 102 具备：图像传感器（图像取得部）210，取得生物体图像（手指静脉图案），由 CCD 摄像机等构成；生物体有无检测用照明 LED211，检测是否在图像传感器 210 的图像可取得区域上放置了手指；生物体取得用照明 LED（生物体照射部）212，在取得生物体图像（手指静脉图案）时对手指照射近红外线。IC 卡装置 103 具备：IC 卡写入部 213，在 IC 卡 105 中写入信息；触点端子 214，用来和 IC 卡 105 进行连接。

[0043] IC 卡 105 具备：CPU221，控制 IC 卡 105 整体；存储部 222，存储与生物体信息相关的数据和涉及金融交易的程序等；触点端子 223，用来和生物体信息注册装置 101 连接。还有，IC 卡装置 103 和 IC 卡 105 并不限定于利用触点端子的接触式，也可以采用非接触式的结构。

[0044] 注册用终端装置 104 包括：CPU231，控制注册用终端装置 104 整体；主存储部 232，存储有数据和程序；显示部 106，由 CRT 或液晶显示器等构成，显示操作指导；操作部 107，由受理窗口营业员的输入操作的键盘、鼠标等构成；通信部 235，连接生物体信息注册装置 101 和生物体注册用终端装置 104。而且，主存储部 232 除了存储有用来控制生物体信息注册装置 101 的生物体信息注册装置控制程序 233 之外，还存储有在窗口交易的各种金融交易用的程序。

[0045] 利用图 3，说明在生物体信息注册处理中在 IC 卡 105 中注册的注册数据的制作过程。其中，制作过程中的算法等的阐述由于安全方面、即为了防止因信息泄漏等引起的伪造的关系，将其说明予以省略。在生物体信息的认证处理中也相同。

[0046] 首先，根据由图像传感器 210 所得到的生物体图像（手指静脉图案），使用某种算法来提取表现其特征的生物体特征量（步骤 301）。然后，根据该生物体特征量，再使用某种算法来制作预处理数据。接着，将生物体特征量和预处理数据组合，来制作注册数据（步骤 302）。

[0047] 这里，所谓的预处理数据，也可以解释为制作注册数据所使用的加密密钥。另外，注册数据如上面及附图所明确的那样，是不能从生物体特征量直接制作的数据。另外，虽然预处理数据和注册数据是从明确表现使用者本身的特征的生物体特征量制作出的数据，但是在该制作过程中要使用不可逆转换处理的算法。因而，作为利用逆转换的制作处理，不能根据注册数据制作生物体特征量或预处理数据，并且不能根据预处理数据和注册数据这 2 个数据制作生物体特征量。还有，预处理数据的形式最好是提取出不能确定使用者个人的部分后所制作出的信息，并且注册数据的形式最好是提取出能确定个人的部分后所制作出的信息。另外，预处理数据、注册数据都是只能由卡持有者获得的专用信息。

[0048] 最后，将所制作出的预处理数据和注册数据存储于 IC 卡 105 中（步骤 303）。IC 卡 105 中所存储的这些数据在被加密的状态下存储，并且如上所述，在无法进行利用逆转换的制作处理的状态下存储。因而，假设预处理数据、注册数据被有恶意的人读出，且两个数据被译码，也不可能生成生物体特征量。这样，其特征之一为，通过数据的加密、生成无法逆转换的数据这样的双重安全化，来保护 IC 卡内的数据。

[0049] 下面，用数学公式来表达上述的数据制作算法。

[0050] 假设生物体特征量为 x，则预处理数据 y 使用某个函数 f（相当于算法），作为“y = f(x)”来表达。

[0051] 由于注册数据 z 是通过组合生物体特征量 x 和预处理数据 y 而制成的，因而使用某个函数 g 表达为“x+y → z = g(x, y)”。

[0052] 而且，因为该制作过程是不可逆的，所以不能象 z = g(x,y) → x、z = g(x,y) → y、z = g(x, y) → x+y 那样，从注册数据还原生物体特征量和预处理数据。

[0053] 图 4 是生物体信息注册装置 101 的 CPU201 或者根据来自 CPU201 的指示由各机构、各单元（也包括程序）所执行的生物体信息注册处理的流程图例。

[0054] 在 IC 卡装置 103 中插入 IC 卡 105，成为 IC 卡连接状态（可向 IC 卡 105 写入数据的状态）。为了使 IC 卡连接成立，需要使 IC 卡 105 的触点端子 223 接触 IC 卡装置 103 的触点端子 214。下面，说明窗口营业员操作注册用终端装置 104 将使用者的生物体信息注册于 IC 卡 105 内的过程，并且说明基于该操作的由各机构等执行的处理、控制。另外，图 2 中所说明的通信控制程序 209 是特别在生物体信息注册装置 101 和生物体注册用终端装置 104 之间控制数据收发的程序，而在下面进行省略说明。

[0055] 注册用终端装置 104 在显示部 106 上显示菜单画面（对选择注册、认证、变更、结束等处理进行指导的画面），通过操作部 107 来受理窗口营业员的输入操作。若从所显示的交易项目之中通过操作部 107 选择注册处理，则注册用终端装置 104 的 CPU231 执行注册处理程序 205、生物体信息注册装置控制程序 233，向生物体信息注册装置 101 发出注册处理开始的指示。收到注册处理开始指示后的生物体信息注册装置 101 的 CPU201 执行注册处理程序 205，并且作为系统整体实施注册处理。

[0056] 在注册用终端装置 104 的显示部 106 上显示指导，指导在生物体信息注册装置 101 中插入 IC 卡 105。若 IC 卡 105 插入到了 IC 卡装置 103 中（步骤 401），则使 IC 卡 105 的触点端子 223 和 IC 卡装置 103 的触点端子 214 接触，连接生物体信息注册装置 101 和 IC 卡 105（步骤 402）。此时，判断所插入的 IC 卡 105 的存储部 222 中是否有与生物体信息相关的程序（步骤 403），在没有程序时（不能注册数据的卡时），返还 IC 卡 105（步骤 411）。另一方面，在所插入的 IC 卡 105 的存储部 222 中存在与生物体信息相关的程序时（能注册数据的卡时），在显示部 106 上显示指导，指导将要注册的手指放置于生物体信息读取装置 102 上。与其相应，使用者把要注册的手指放置于生物体信息读取装置 102 上。生物体信息注册装置 101 的 CPU201 执行生物体信息读取装置控制程序 207，向生物体信息读取装置 102 发出生物体信息读取开始的指示。若在图像传感器 210 的图像可取得区域上放置了物体（手指），则生物体信息读取装置 102 通过生物体有无检测用照明 LED211 检测到物体（手指）的进入（步骤 404），并调查物体（手指）是否是生物体（步骤 405）。在所插入的物体（手指）不是生物体时，在 IC 卡 105 中不写入任何信息，将 IC 卡 105 返还（步骤 411）。在所插入的物体（手指）是生物体时，由生物体取得用照明 LED212 对物体（手指）照射近红外线，并由图像传感器 210 取得生物体图像（手指静脉图案），存储于 RAM204 中（步骤 406）。接着，从生物体图像（手指静脉图案）提取生物体特征量（步骤 407）。然后，在通过执行注册数据制作程序 206，如图 3 所示根据生物体特征量制作出预处理数据之后（步骤 408），根据生物体特征量和预处理数据来制作注册数据（步骤 409）。接着，执行 IC 卡装置控制程

序 208，由 IC 卡写入部 213 以及 IC 卡 105 内的 CPU221，将所制作出的 RAM204 内的预处理数据和认证数据存储于 IC 卡 105 的存储部 222 中，生物体信息注册结束（步骤 410），返还 IC 卡 105（步骤 411）。

[0057] 以上，虽然基于各 CPU201、221、231 和存储部中所存储的各程序的处理、控制，说明了生物体信息的注册处理、控制，但是不言而喻，各程序也可以在转移到注册处理的最初阶段就已经启动，并且将这些硬件及软件的结构作为控制部来掌握，上述的各种控制、处理是该控制部的功能、单元。另外，对于下面说明的生物体信息认证处理来说也相同。

[0058] 在执行生物体信息的认证处理时，使用上述通过注册处理所注册的信息，也就是 IC 卡 105 中所存储、注册及写入的预处理数据和注册数据，将进行认证处理作为前提来进行说明。

[0059] 图 5 是生物体认证处理系统的概要图。连接现金自动交易或出纳装置 (ATM)501 和服务器 502 来构成生物体认证系统，该现金自动交易或出纳装置 501 具备读取生物体信息的功能和读取（或写入）IC 卡 105 的信息的功能，该服务器 502 存储有与金融商品有关的交易所需要的信息。ATM501 是自动执行存款、支付及转帐等使用者希望的各种交易的装置，使用者可以在卡 / 明细单机构部 504 中插入 IC 卡 105，通过操作部 503 输入所希望的交易或金额等，通过生物体认证机构 508 而成功认证，从而进行交易。特别是，在现金交易中，由纸币存取机构部 506 执行纸币存款或取款，由硬币存取机构部 507 执行硬币存款或取款，ATM501 进行使用者所希望的现金交换。另外，当使用者希望填写存折时，可以通过存折机构部 505 在存折中填写交易内容，进行打印。

[0060] 图 6 是表示生物体认证处理系统的一个实施例结构的框图。ATM501 具有 ：CPU601，控制 ATM 整体 ；操作部 503，进行交易项目的画面显示和按键输入检测，具体来说，受理使用者的操作或用手指所按下的按键输入，并且由接触式面板等构成 ；卡 / 明细单机构部 504，具有卡的插入及吐出动作、对卡磁条或 IC 卡 105 的读 / 写动作、卡凹凸部分的图像读取以及将所交易的内容打印在明细单上并将其从装置内吐出的功能 ；存折机构部 505，具有使用者的存折的插入 / 吐出动作、磁条的读 / 写动作以及利用打印部对存折打印的功能等。

[0061] 再者，还包括 ：纸币存取机构部 506，具有纸币的鉴别、运送及收纳功能等，进行纸币的存款或取款处理 ；硬币存取机构部 507，具有硬币的鉴别、运送及收纳功能等，进行硬币的存款或取款处理 ；生物体认证机构部 508，取得生物体信息，支持其认证 ；主存储部（也简单称为存储部）602，存储有数据和程序 ；通信部 610，和服务器 502 连接。

[0062] 还有，图 1、2 中所说明的注册用终端装置 104 的操作部 107 用来在窗口营业员将使用者的生物体信息向 IC 卡 105 注册时进行输入操作，由键盘或鼠标等构成，另一方面，图 5、6 的 ATM501 的操作部 503 用来在使用者通过 ATM501 进行交易时进行输入操作，由接触式面板等构成，虽然着两个都是操作部，但是结构、用途不同。

[0063] 卡 / 明细单机构部 504 具备 ：IC 卡读取部 603，读取 IC 卡 105 的信息 ；明细单打印部 604，在明细单上打印交易内容 ；触点端子 605，用来和 IC 卡 105 连接。

[0064] 生物体认证机构部 508 具备 ：存储部 606，存储有各种数据等 ；图像传感器（图像取得部）607，取得使用者的生物体图像（手指静脉图案），由 CCD 摄像机等构成 ；生物体有无检测用照明 LED608，检测是否在图像传感器 607 的图像可取得区域上放置了手指 ；照明 LED（生物体照射部）609，在取得生物体图像（手指静脉图案）时对手指照射近红外线。也

就是说，生物体认证机构部 508 具有和图 1、2 所示的生物体信息读取装置 102 大致相同的取得生物体信息的功能。

[0065] 主存储部（也简单称为存储部）602 在硬件上包括：ROM620，存储有各种程序；RAM621，主要存储有数据，并且可重写所存储的数据。如同上述注册处理中所说明的那样，也可以分别由硬盘或各种半导体存储器构成，并且还称为第 1、2 存储部。另外，ROM620 具备认证控制软件 622，该认证控制软件 622 用来按照 CPU601 等的指示，进行下面说明的生物体图像取得、认证等处理，控制生物体认证机构部 508。此外，虽然没有图示，但是还存储有对 ATM501 的操作部 503 的画面数据以及 ATM501 中现金交易、转帐交易等所需的程序、软件。经由通信网和 ATM501 连接的服务器 502 包括：CPU611，控制服务器 502 整体；存储部 612；通信部 613，和 ATM501 连接。

[0066] 图 7 图示出，ATM501 中的生物体信息的认证所涉及的控制、特别是以用于控制生物体认证机构部 508 的认证控制软件 622 为中心的与主存储部 602、生物体认证机构部 508、卡 / 明细单机构部 504 内的 IC 卡 105 相关的控制块（软件结构）。

[0067] 认证控制软件 622 可以大致分为认证控制应用程序 701 和认证控制中间件 702，并且分别将软件称为软件、应用程序称为应用程序，中间件称为中间件。所谓的认证控制应用程序 701 指的是，具有将装载有生物体认证机构部 508 的 ATM501 导入的金融机构等的个别功能的程序，并且对每个金融机构制作或变更其认证的顺序或方式、认证时的画面显示等其规格。特别是，本认证控制应用程序 701 对认证中间件 702 进行认证处理开始指示等。

[0068] 所谓认证控制中间件 702 指的是，具有即使金融机构不同并且生物体信息不同而认证处理所需的通用功能的程序，是如控制生物体认证机构部 508 的生物体认证机构部控制程序 703、以及从 IC 卡 105 对与卡交换数据、执行 IC 卡 105 内的程序进行控制的 IC 卡控制程序 704 那样的、负责控制、处理生物体信息认证所涉及的各种程序的程序。

[0069] 另外，由认证控制中间件 701 执行并获得的数据暂时存储于 RAM621 中。RAM621 具有用于在生物体认证机构部 508 和 IC 卡 105 之间交换数据的缓存区域即认证结果数据缓存器 705、认证数据缓存器 706 及预处理数据缓存器 707 之类的各数据缓存器。这些数据虽然在硬件上存储于 RAM621 中，但是在软件上还能认为存储于认证控制软件 622 中，特别是认证控制中间件 702 中。

[0070] 另外，认证控制中间件 702 根据来自认证控制应用程序 701 的指示，经由驱动器（未图示）使卡 / 明细单机构部 504 和生物体认证机构部 508 动作。而且，如上所述，这些各部位由 ATM501 的 CPU601 来控制其处理。还有，所谓驱动器指的是，用来利用计算机外围设备・装置（设备）的控制用软件。

[0071] 由认证控制软件 622 控制的生物体认证机构部 508 的存储部 606 具有：认证数据制作程序 709，用来制作认证数据；认证结果判断程序 710，用来根据认证结果数据判断认证成功与否。另外，卡 / 明细单机构部 504 具有用来实施认证处理的认证程序 711。

[0072] 利用图 8，说明生物体认证处理中认证的构成、数据的交换。也用于作为对下述图 11 的生物体认证流程的说明的补充。以下的动作主体是从认证控制应用程序 701 接收执行指令的认证控制中间件 702，但是因为认证控制应用程序 701 和认证控制中间件 702 共同执行，所以还能认为通过认证控制软件 622 进行动作。另外，还能将接收、发送分别称为输入、输出。

[0073] 若在ATM501的交易中执行生物体信息的认证，则向认证控制中间件702发送预先存储在IC卡105中的预处理数据、注册数据之中的预处理数据。认证控制中间件702从IC卡105接收预处理数据，暂时存储于RAM621（包括认证控制软件622、认证控制中间件702）的预处理数据缓存器707中，之后发送给生物体认证机构部508（步骤801）。另一方面，生物体认证机构部508从认证控制软件622接收预处理数据，随后或者并行地，取得使用者的生物体信息，从生物体信息提取生物体特征量。然后，将所接收到的预处理数据和所取得并提取的生物体特征量组合，来制作认证数据（步骤802）。

[0074] 这样，在生物体信息的认证处理中，预处理数据还具有作为用于制作认证数据加密密钥的功能。另外，假使取得了该认证数据，也不能根据该数据直接制作生物体特征量。虽然认证数据是从生物体特征量制作出的数据，但是因为在其制作过程中使用了不可逆转换处理的算法，所以不能反向地从认证数据制作生物体特征量，并且不能根据预处理数据和认证数据这2个数据制作生物体特征量。预处理数据是将不能确定个人的部分提取后所制作出的信息，认证数据是将能确定个人的部分提取后所制作出的信息。

[0075] 这里，和生物体信息注册时相同，用数学公式来表达上述数据制作算法。

[0076] 将通过生物体认证机构部508在认证时得到的信息，也就是新得到的生物体特征量设为x′。而且，由于预处理数据y和注册时没有变化，因而是“y＝f(x)”。

[0077] 由于认证数据z′是利用生物体特征量x′和预处理数据y的组合制成的，因而使用某个函数g表达为“x′+y→z′＝g(x′，y)”。而且，由于该制作过程是不可逆过程，因而不能象z′→x′、z′→y、z′→x′+y那样从注册数据还原生物体特征量和预处理数据。

[0078] 在S802的认证数据制作之后，根据认证控制软件622的指示、控制，将由生物体认证机构部508所制作出的认证数据暂时存储于认证数据缓存器706中，之后发送给IC卡105（步骤803）。IC卡105接收认证数据，并使用某个算法对预先存储在IC卡105中的注册数据和认证数据进行比对（也称为生物体认证处理），来制作认证结果数据（步骤804）。再将所制作出的认证结果数据发送给认证控制中间件702。认证控制中间件702从IC卡105接收认证结果数据，暂时存储在认证控制软件622的认证结果数据缓存器705中，之后发送给生物体认证机构部508。然后，生物体认证机构部508在生物体认证机构部508内进行认证结果数据的判断（分析）（步骤805），将认证结果数据和认证成功部位·认证失败原因通知给认证控制中间件702（步骤806），生物体认证处理结束。

[0079] 这样，在生物体认证处理中，虽然与使用者的生物体信息本身最为接近的生物体特征量没有存储于IC卡105内，而通过生物体认证机构部508来取得并提取生物体特征量，但是具有不会从生物体认证机构部泄露到外面的特征。

[0080] 另外，通过认证控制软件622并且在其控制之下在IC卡105和生物体认证机构部508之间所交换的数据是预处理数据、认证数据及认证结果数据这3个，但具有无论怎样如上所述组合这些数据都不能制作出生物体特征量的特征。

[0081] 另外，在生成生物体信息所涉及的各数据等的生物体认证处理中，具有分别由IC卡105、生物体认证机构部508进行分担来取得认证结果的特征。因此，其设计为，即使IC卡或生物体认证机构部被盗并且对其内部进行了译码，也不能执行生物体认证处理。也就是说，虽然在理论上，也可以在认证时从由生物体认证机构部508所取得的生物体特征量

新制作预处理数据，并且根据该预处理数据和生物体特征量制作认证数据，但是在本实施方式中，由于没有那样做，而是利用预先存储在 IC 卡 105 中的预处理数据和生物体特征量来制作认证数据，因而安全性提高。

[0082] 另外，最好是，认证控制中间件 702 将预处理数据存储于生物体认证机构部 508 内，并且在制作认证数据后将其删除，优选的是，当需要认证时，随时从预处理数据缓存器 707 发送给生物体认证机构部 508。也就是说，在利用 ATM501 的交易结束之前，在认证控制软件 622 内的预处理数据缓存器 707 中预先存储预处理数据。这样一来，有下述效果，即与从 IC 卡 105 发送预处理数据相比，如果从认证控制软件 622 内的预处理数据缓存器 707 发送，则可以实现更快的处理。

[0083] 利用图 9 ～ 12，说明在现金自动交易装置、现金自动出纳装置 (ATM)501 上使用 IC 卡 105 来实施包含利用 IC 卡内认证方式的生物体认证处理的支付交易时的处理。

[0084] 图 9 是表示由 ATM501 的 CPU601、认证控制软件 622 等（控制部）所执行的、特别是使用 IC 卡内认证方式的生物体认证处理中的 ATM 上的交易的流程图例。

[0085] 在进行生物体认证处理之前，进行交易选择或密码输入、卡插入等执行 ATM501 上的交易所需的处理。从 ROM620 读取存款、支付、余额查询及转帐等交易选择指导，显示于操作部 503 上，从使用者受理交易的选择（步骤 901）。在选择出需要生物体认证的交易如支付交易等时，在操作部 503 上显示将 IC 卡插入的指导，催促插入 IC 卡 105。若由使用者在卡 / 明细单机构部 504 中插入了 IC 卡 105，则对其进行检测（步骤 902），由卡 / 明细单机构部 504 的 IC 卡读取部 603 从 IC 卡 105 读取帐号。还有，IC 卡 105 也可以是具备磁条的卡，此时，也可以从 IC 卡 105 的磁条读取除生物体信息之外的帐号等数据。

[0086] 接着，将输入密码的指导显示于操作部 503 上。若由使用者在操作部 503 上输入了密码，则对其进行检测（步骤 903），将所读取的帐号和所输入的密码经由通信部 610、613 发送给服务器 502。另一方面，服务器 502 的 CPU611 经由通信部 610、613 接收所输入的密码，对所输入的密码和预先注册在存储部 612 中的与帐号对应的密码进行比对，将该比对结果经由通信部 610、613 发送给 ATM501。ATM501 经由通信部 610、613 接收比对结果，并检查密码正确与否（步骤 904），在所输入的密码不正确时，对密码的输入次数进行计数（步骤 905）。如果此时密码的输入次数在规定次数以内，则对使用者催促再次输入密码。如果密码的输入次数超过了规定次数，则中止交易（步骤 906）。

[0087] 在 S904 中所输入的密码正确时，判断所插入的 IC 卡 105 是否是生物体认证对象卡（步骤 907）。此时生物体认证对象卡指的是，具有实施生物体认证所需的信息和程序的卡。

[0088] 然后，在所插入的 IC 卡 105 不是生物体认证对象卡时，不进行生物体认证处理，而接着执行支付等交易（步骤 915）。在所插入的 IC 卡 105 是生物体认证对象卡时，作为生物体认证处理的事前准备，进行认证交易开始处理（步骤 908）。有关认证交易开始处理，利用下述的图 10 详细说明。

[0089] 认证交易开始处理结束后，ATM501 的 CPU601 在 RAM621 中取得并展开认证控制软件 622。接着，ATM501 的 CPU601 执行认证控制应用程序 701。接收该情况，认证控制应用程序 701 对认证控制中间件 702 发出注册信息取得指示。收到注册信息取得指示后的认证控制中间件 702 执行 IC 卡控制程序 704，从 IC 卡 105 取得由认证控制应用程序 701 所指

示的处理所需的信息（注册者信息）（步骤909）。在处理所需的信息中，包含帐号、营业所号码、项目等交易信息以及使用者姓名、有无驾驶证或保险证等可确认本人的证明书之类的使用者信息等。另外，此时认证控制中间件702除了取得被认证控制应用程序701指示取得的信息之外，还取得预先注册在IC卡105中的预处理数据，存储于预处理数据缓存器707中。原因是，通过和认证控制应用程序701所指定的信息一起取得预处理数据，可以减少访问IC卡105的次数，加快处理时间。该数据发送给认证控制中间件702，并存储于预处理数据缓存器707中。这样，虽然ATM501的CPU501成为主体，执行认证控制软件622内的各种程序，并进行各自的处理，以下，为了简化说明而将该过程省略，以认证控制中间件702为主体进行说明。另外，如上所述，还将这些总体称为由控制部（单元）进行的控制、处理。

[0090] 在从IC卡105取得注册信息后，认证控制中间件702执行生物体认证机构部控制程序703，进行生物体认证处理（步骤910）。也就是说，将预处理数据缓存器707中所存储的预处理数据发送给生物体认证机构部508，并且对生物体认证机构部508指示取得生物体信息。对于该生物体认证处理，虽然利用图8进行了说明，但是在下述的图11中也进行详细说明。

[0091] 接着，检查生物体认证成功与否（步骤911），在此，在生物体认证失败时，对生物体认证的实施次数进行计数（步骤912）。如果此时生物体认证的实施次数在规定次数以内，则将在RAM621或程序中存储、保存的预处理数据再次发送给生物体认证机构部508，对使用者催促生物体认证的再次实施。如果生物体认证的实施次数超过了规定次数，则中止交易（步骤913）。还有，此时，为了提高安全性，将RAM621中所存储的预处理数据等删除。并且，在S911中，在生物体认证成功时，作为生物体认证处理的事后处理，进行认证交易结束处理（步骤914）。对于该认证交易结束处理，将利用下述的图12进行详细说明。

[0092] 认证交易结束处理结束后，执行使用者所希望的交易，也就是执行在S901中进行过交易选择的交易（步骤915）。具体而言，如果使用者所希望的交易是支付交易，则通过操作部503受理支付金额的输入。若由使用者进行了支付金额输入，则在操作部503上显示所输入的金额以及按下催促金额是否正确的确认按键的消息。若按下了操作部503的确认按键，则和服务器502进行交易数据的相互通信。在相互通信后，ATM501的CPU601将所要求的金额量的纸币、硬币从纸币存取机构部506、硬币存取机构部507分别吐出，并使卡/明细单机构部504的明细单打印部604打印交易数据。然后，从卡/明细单机构部504返还IC卡105，并将交易数据打印于明细单上并送出，交易得以结束（步骤916）。

[0093] 另外，如果使用者所希望的交易是余额查询，则和服务器502进行交易数据的相互通信，相互通信后，在操作部503上显示存款或借款余额。在显示后，对使用者指导是想结束交易还是想继续实施其他交易。在想结束交易时，从卡/明细单机构部504返还IC卡105，并且按照使用者的要求将交易数据打印于明细单上并送出，交易得以结束（步骤916）。在使用者希望进行其他交易实施时，进行以下处理。

[0094] 在余额查询后接着希望进行上述支付交易等需要生物体认证的交易时，再次实施生物体认证，并且只在生物体认证成功时执行交易。由于考虑到在使用者通过余额查询确认了存款·借款余额后没有收取IC卡105而离开了ATM时由第3人执行交易的情形，通过在每次交易都实施生物体认证，可以消除这样的危险，实现安全性较高的ATM系统。

[0095] 还有，在该流程中，虽然在密码输入之后，实施了生物体认证，但是也可以使该顺

序相反，在生物体认证实施之后输入密码。在先实施密码输入时存在下述优点，即由于和一般的交易相同，使用者插入卡后，在最初的交易选择后立刻输入密码，因而即便随后进行生物体认证，操作流程也易于处理接近现状的装置。另一方面，在与利用密码进行认证相比、先实施生物体认证时，存在下述优点，即，由于如果在本人以外的人进行生物体认证并且生物体认证失败而拒绝交易时，不经过密码输入就结束交易，因而不用为了无用的密码比对而与服务器进行通信即可，可以减轻对服务器的负担。

[0096] 利用图 10，说明图 9 的 S908 中的认证交易开始处理。从认证控制应用程序 701 收到认证交易开始指示后的认证控制中间件 702 执行 IC 卡控制程序 704，进行和 IC 卡 105 之间的连接（步骤 1001）。这形成如上所述可从 IC 卡 105 读取数据的状态。但是，在 IC 卡 105 中没有与生物体认证有关的数据并且是不适应 IC 卡内认证的 IC 卡时，例如希望即使只通过上述利用密码的认证处理也可以进行 ATM 上所希望的交易，并且最好在和图 9 的 S902 等卡插入大致相同的定时，利用认证控制中间件 702 之外的其他 ATM 软件，来执行 IC 卡控制程序 704，至少在 S908 的处理前完成与 IC 卡 105 的连接。

[0097] 另外，在插入到卡 / 明细单机构部 504 中的 IC 卡 105 内，通过图 1 的生物体信息注册装置 101 预先注册有使用者固有的注册数据及预处理数据，并且装载、存储有用来在 IC 卡 105 内进行认证的认证程序 711。该认证程序 711 是在 IC 卡 105 中预先或者以不可重写的形式写入的应用程序，是用来根据特定的算法对 IC 卡中预先注册的注册数据和由 ATM 的控制部所得到的认证数据进行匹配及比对的程序。

[0098] 若在 S1001 中卡 / 明细单机构部 504 和 IC 卡 105 之间的连接成功，则认证控制中间件 702 取得注册在 IC 卡 105 中的支持认证方式（或是支持认证信息）（步骤 1002）。所谓支持认证方式指的是，预先注册在 IC 卡 105 中的方式，是可以唯一决定能将认证数据或生物体特征量等的息按哪种控制顺序实施认证处理的信息。例如，在手指静脉认证中，支持在生物体认证机构部 508 内进行认证（比对）的装置内认证处理和在 IC 卡 105 内进行认证的 IC 卡内认证处理，通过从 IC 卡 105 取得支持认证方式，能够切换认证控制顺序，用 1 个认证控制程序来实现 2 种认证方式。

[0099] 使用该支持认证方式取得那样的、使用 IC 卡等中所注册认证方式、唯一决定认证控制顺序的信息来切换认证控制顺序或方式的方法，在 ATM 等生物体认证装置装载终端中装载了多个认证装置（例如，手指、手掌之类的静脉认证装置或眼睛的虹膜认证装置等）时，可以通过切换认证控制程序的控制方式，来适应多个生物体认证装置的控制。

[0100] 接着，判断在步骤 1002 中所得到的认证方式是否是 IC 卡内认证（步骤 1003），在不是 IC 卡内认证时不进行交易处理，返还 IC 卡 105（步骤 916）。另一方面，在是 IC 卡内认证方式时，进行 ATM501 和 IC 卡 105 之间的相互认证，并且认证交易开始处理结束（步骤 1004）。所谓相互认证指的是下述处理，即，用来确认在生物体认证机构部 508 中的认证数据制作程序 709 和装载于 IC 卡 105 中的认证程序 711 等是否已被篡改成非法的程序，或者在 ATM501 和 IC 卡 105 之间确认相互程序合法性。

[0101] 利用图 11，对于图 9 的 S908 的生物体认证处理进行说明。如同图 8 中所说明的那样，该生物体认证处理是最终进行预先记录在 IC 卡 105 内的注册数据和生物体认证处理时新制作的认证数据之间的认证（比对）并获得其比对结果的处理，其特征为，在 IC 卡 105 内进行认证本身的实质所涉及的处理。

[0102] 虽然在图9的S909中通过IC卡105接收数据，但是与此同时，在该生物体认证时，从IC卡105将预先存储的预处理数据发送给认证控制中间件702。认证控制中间件702接收存储在IC卡105中的预处理数据，存储于预处理数据缓存器707中。再者，将预处理数据缓存器707中所存储的该预处理数据发送给生物体认证机构部508（步骤1101）。生物体认证机构部508若接收到预处理数据，则作为下来的处理或并行处理，读取使用者的生物体信息。

[0103] 图11的步骤1102～步骤1105的处理执行和图4的步骤404～步骤407大致相同的处理，获得生物体特征量。若在图像传感器607的图像可取得区域上放置了手指，则由生物体有无检测用照明LED608检测放置了物体（手指）的情况（步骤1102），检查物体（手指）是否是生物体（步骤1103）。在所插入的物体（手指）不是生物体时，生物体认证失败（步骤1104）。在所插入的物体（手指）是生物体时，由生物体取得用照明LED609对生物体照射近红外线，由图像传感器607取得生物体图像（手指静脉图案），存储于存储部606中（步骤1105）。

[0104] 接着，从生物体图像（手指静脉图案）提取表现特征数据的生物体特征量（步骤1106）。然后，在认证控制中间件702的指示下执行认证数据制作程序709，由此来制作图8中所说明的认证数据（步骤1107）。然后，将所制作出的认证数据发送给认证控制中间件702，存储于认证数据缓存器706中。

[0105] 认证控制中间件702执行IC卡控制程序704，将认证数据缓存器706中所存储的认证数据发送给IC卡105，并且对IC卡105内的认证程序711发出生物体认证指示（步骤1108）。另一方面，IC卡105执行卡内所存储的认证程序711，对IC卡105中预先注册的注册数据和上述认证控制中间件702的认证数据缓存器706中所存储的认证数据进行比对，进行生物体认证处理，并制作认证结果数据。

[0106] 然后，IC卡105将认证结果数据发送给认证控制中间件702，认证控制中间件702将其存储于认证控制中间件701内（作为硬件是RAM内）的认证结果数据缓存器705中。这样，在认证控制中间件702所实施的生物体认证机构部508和IC卡105之间的数据的收发控制过程中，从生物体图像（手指静脉图案）所取得的生物体特征量不会到生物体认证机构部508的外部，并且注册在IC卡105中的认证数据也不到外部。因而，可以防止个人信息泄漏到装置的外部，因此使个人信息的隐秘性得到保护，提高安全性。

[0107] 认证控制中间件702执行生物体认证机构部控制程序703，将认证结果数据缓存器705中所存储的认证结果数据发送给生物体认证机构部508，并且对认证结果判断程序710发出认证结果判断指示。接着，执行认证结果判断程序710，根据在IC卡105内所进行的认证结果即存储于认证结果数据缓存器705中的认证结果数据，判断生物体认证是成功还是失败。这里作为输出，生物体认证机构部508在认证成功时，将在生物体的哪个部位上认证成功通知给认证控制中间件702（步骤1109）。例如，如果生物体认证的部位是手指静脉或指纹等，则将在哪个手指（如右手、中指等）上认证成功通知给认证控制中间件702，如果是手掌的静脉，则将是右手还是左手通知给认证控制中间件702，如果是眼睛的虹膜，则将是右眼还是左眼上认证成功通知给认证控制中间件702。

[0108] 在认证结果失败时，由认证结果判断程序710判断IC卡内认证失败的原因，将其通知给认证控制中间件702。作为原因，最好例如附带有是手指的放置方法不对或者放置了

与注册过的手指不同的其他手指等信息，通知给认证控制中间件 702，据此由认证控制应用程序 701 在操作部 503 上显示该原因，因此可以提供操作性优良的装置。这样，以生物体认证机构部 508 判别认证结果为例，进行了说明，但是也可以是下述方式，该方式为，可以通过 IC 卡内的认证程序 711 或取得认证结果数据后的认证控制中间件 702 判断认证处理的成功与否和认证成功部位、认证失败原因等认证结果。

[0109] 认证控制中间件 702 将注册数据和认证数据的匹配、比对结果即判断结果数据发送给认证控制应用程序 701。如果判断结果数据是认证失败，则认证控制应用程序 701 使 ATM501 的操作部 503 显示出认证再次开始画面等，让使用者再次实施认证。此时，认证控制中间件 702 最好将通过 IC 卡 105 的注册信息取得处理所取得的预处理数据持续保持于预处理数据缓存器 707 中，由于可以省略 IC 卡 105 的注册信息取得处理，因而加快认证处理时间。这还可以在为了进行余额查询到支付交易这类在 1 次光顾中连续的需要本人确认的交易而执行多次认证处理时，也同样通过不从预处理数据缓存器 707 将由 IC 卡 105 所取得的预处理数据删除，来省略 IC 卡 105 的注册信息取得处理，执行连续交易中的认证处理。

[0110] 利用图 12，来说明图 9 的 S914 所示的认证交易结束处理。

[0111] 如果判断结果数据是认证成功，则认证控制应用程序 701 对认证控制中间件 702 发出认证交易结束指示。认证控制中间件 702 执行 IC 卡控制程序 704，并执行和 IC 卡 105 之间的断开处理。所谓和 IC 卡 105 之间的断开指的是不能访问 IC 卡 105 的状态。在和 IC 卡 105 断开后，按照来自认证控制中间件 702 的指示，生物体认证装置控制程序 703 将在生物体认证机构部 508 中的生物体特征量等生物体认证中所使用的个人信息及据此所制作出的认证所涉及的信息，从存储部全部删除。

[0112] 这是防止个人信息等泄漏到外部使安全性得到提高的有效特征。在将生物体认证机构部 508 内的数据清除之后，认证控制中间件 702 将本身具有的认证结果数据缓存器 705、认证数据缓存器 706 及预处理数据缓存器 707 中所存储的信息删除（连续交易除外），防止了信息泄漏。认证交易结束处理结束后，进行支付金额的输入、与服务器 502 之间的相互通信等，支付交易结束。

[0113] 上面，如同利用图 1 ～图 4 说明生物体信息的注册处理并利用图 5 ～图 12 说明生物体信息的认证处理那样，例如在硬件上通过 CPU601、主存储部 602 的控制、处理来进行，在软件上通过认证控制软件 622、认证控制应用程序 701、认证控制中间件 702 的控制、处理来执行生物体信息的认证。因而，如上所述，既可以将它们总称为由控制部、控制机构进行的控制、处理，也可以在 LSI 等硬件上实现各程序的功能。另外，图 7 的各种程序不仅仅是在其处理中需要时首次启动、执行，如果在 ATM 启动时使各程序预先启动，来执行各处理中需要的程序，则可以缩短处理时间。

[0114] 另外，虽然在图 3 中，说明了根据生物体特征量制作预处理数据并从该所制作出的预处理数据和生物体特征量制作认证时使用的注册数据的方式，但是有关预处理数据的制作，也可以和生物体特征量完全无关，并且独立进行制作。如上所述，在注册生物体信息时预处理数据具有用来制作注册数据的加密密钥（或算法）的功能，在生物体认证时具有用来制作认证数据的加密密钥的功能、作用。因而，如果根据生物体特征量来制作预处理数据，则可以成为与使用者分别对应的数据，构成安全性较高的数据制作算法，另一方面，如果和生物体特征量相独立的制作预处理数据，也可以预先制作作为加密密钥发挥作用的预

处理数据本身，并且在整体上成为简单的程序结构，所以节省人工和时间，注册、认证的处理时间变短。

[0115] 另外，虽然根据生物体特征量一步制作出预处理数据，但是也可以分几步进行制作。据此，存在下述这样的效果，也就是假使第 3 人想要解析预处理数据制作过程，也因制作过程较为复杂，而难以解析，并且解析需要时间。

[0116] 另外，因为预处理数据、注册数据、认证数据（包括在认证失败时或连续交易时制作的认证数据）原本是根据使用者的手指等生物体特征量（包括图像图案）所制作、生成的信息，所以能够称为第 1、2、・・・（生物）信息。也就是说，也可以认为这些第 1、2、・・・（生物体信息）是从包含生物体特征量在内的概念及生物体信息中得到的信息。

[0117] 上面，由于不用在认证装置装载终端中装入在本发明的 IC 卡内认证方式中可以对 IC 卡内所注册的个人进行确定的信息和由认证装置所取得的生物体信息（生物体特征量）其本身，因而能够保护个人信息的隐秘性，实现安全性较高的生物体认证。

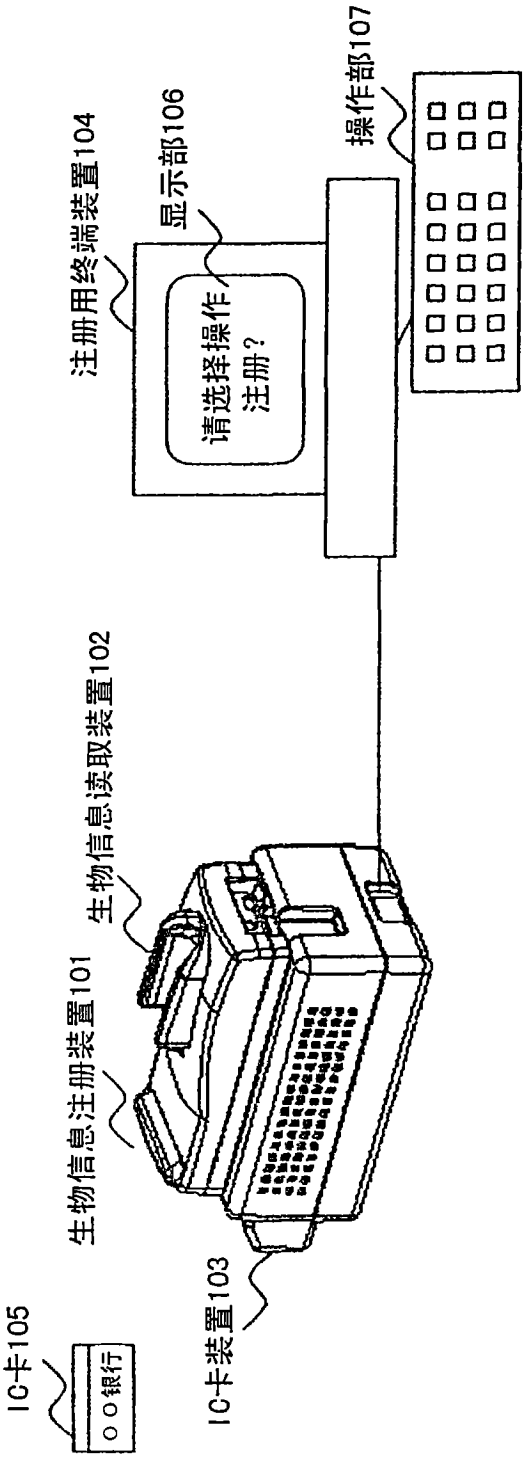

注册用终端装置104
显示部106
请选择操作
注册？
操作部107
生物信息读取装置102
生物信息注册装置101
IC卡105
○○银行
IC卡装置103

图1

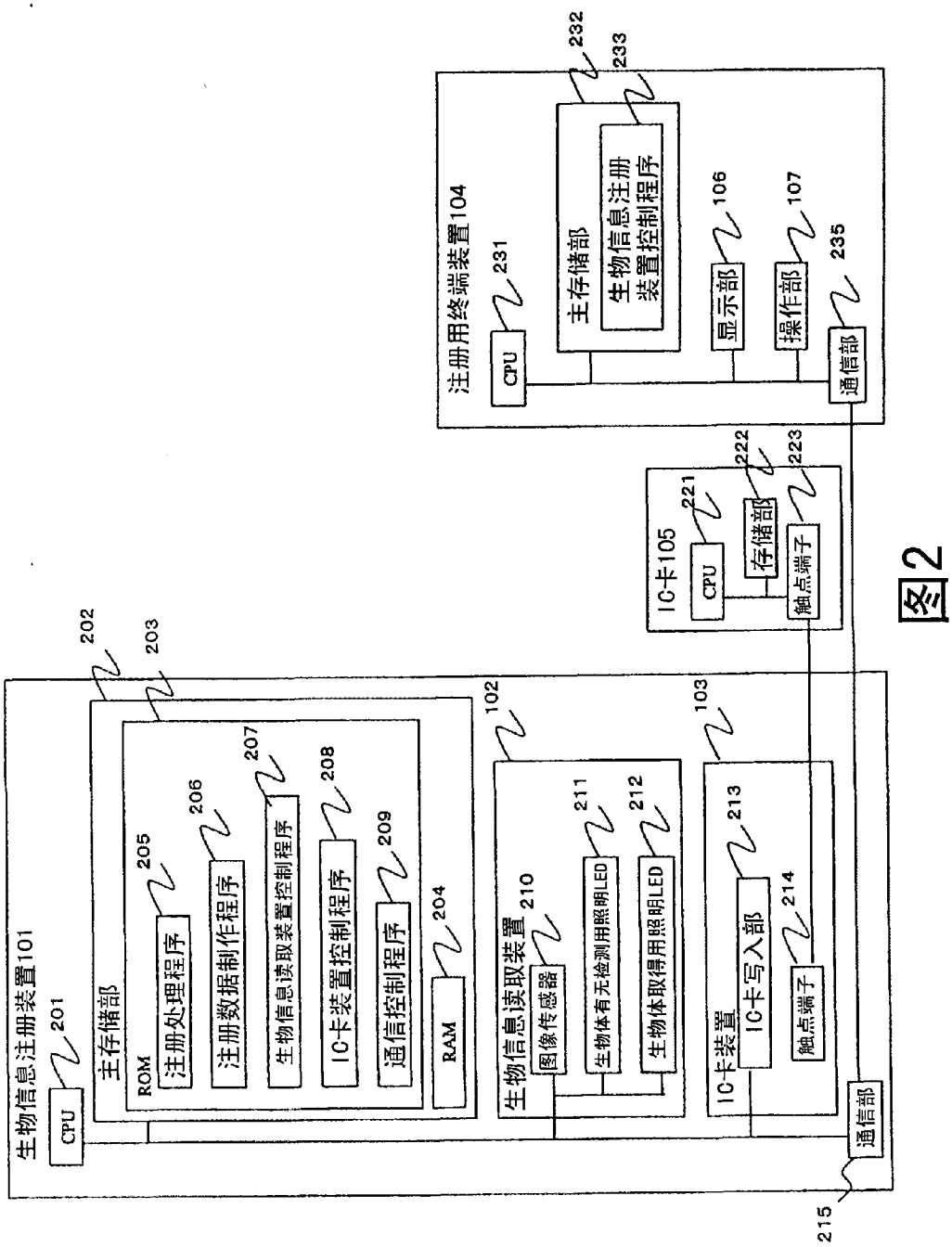

生物信息注册装置101
CPU
201
主存储部
202
ROM
203
注册处理程序
205
注册数据制作程序
206
生物信息读取装置控制程序
207
IC卡装置控制程序
208
通信控制程序
209
RAM
204
生物信息读取装置
102
图像传感器
210
生物体有无检测用照明LED
211
生物体取得用照明LED
212
IC卡装置
103
IC卡写入部
213
触点端子
214
通信部
215
IC卡105
CPU
221
存储部
222
触点端子
223
注册用终端装置104
CPU
231
主存储部
232
生物信息注册装置控制程序
233
显示部
106
操作部
107
通信部
235

图2

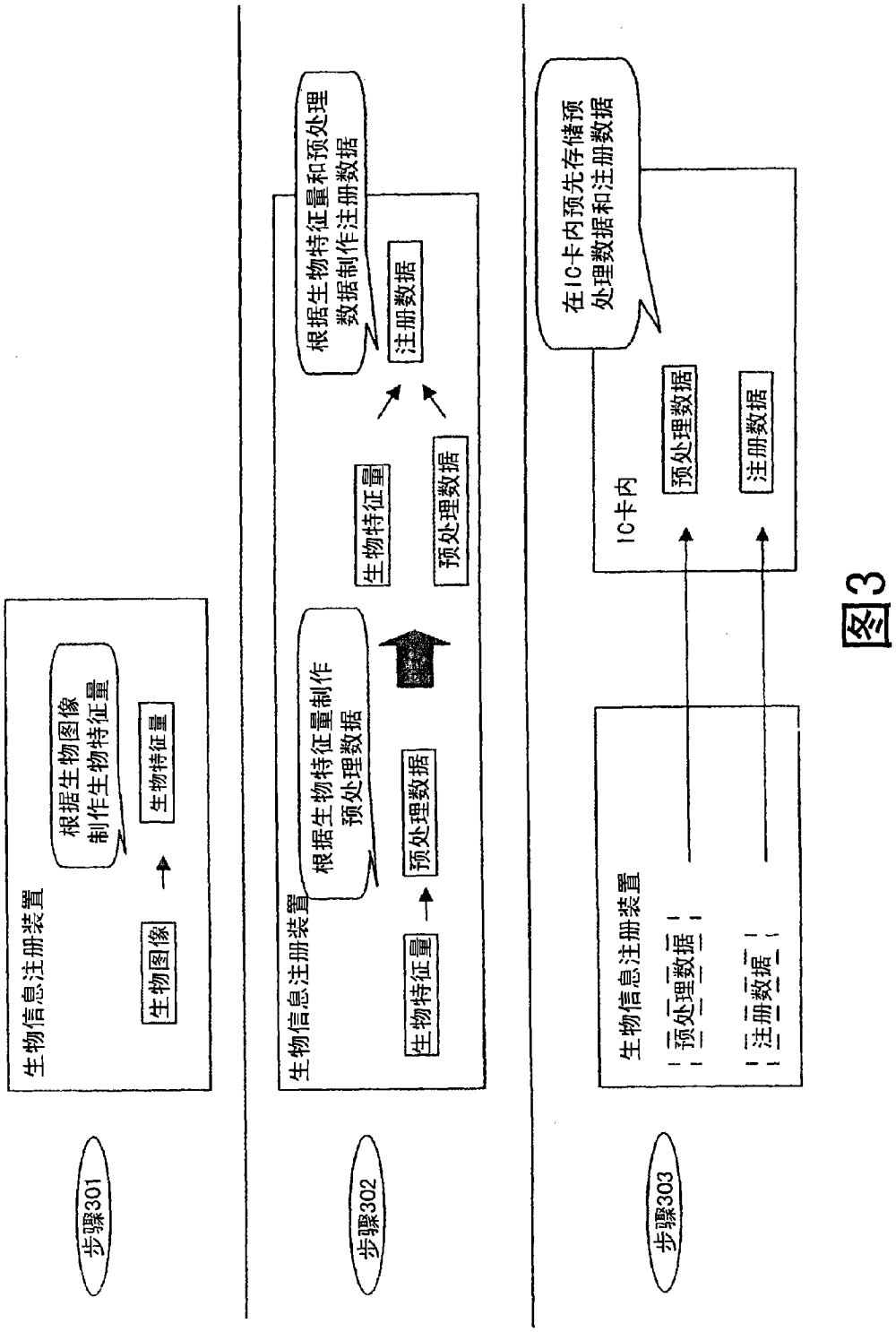

步骤301
生物信息注册装置
根据生物图像制作生物特征量
生物图像
生物特征量
步骤302
生物信息注册装置
根据生物特征量制作预处理数据
生物特征量
预处理数据
生物特征量
预处理数据
根据生物特征量和预处理数据制作注册数据
注册数据
步骤303
生物信息注册装置
预处理数据
注册数据
IC卡内
预处理数据
注册数据
在IC卡内预先存储预处理数据和注册数据

图3

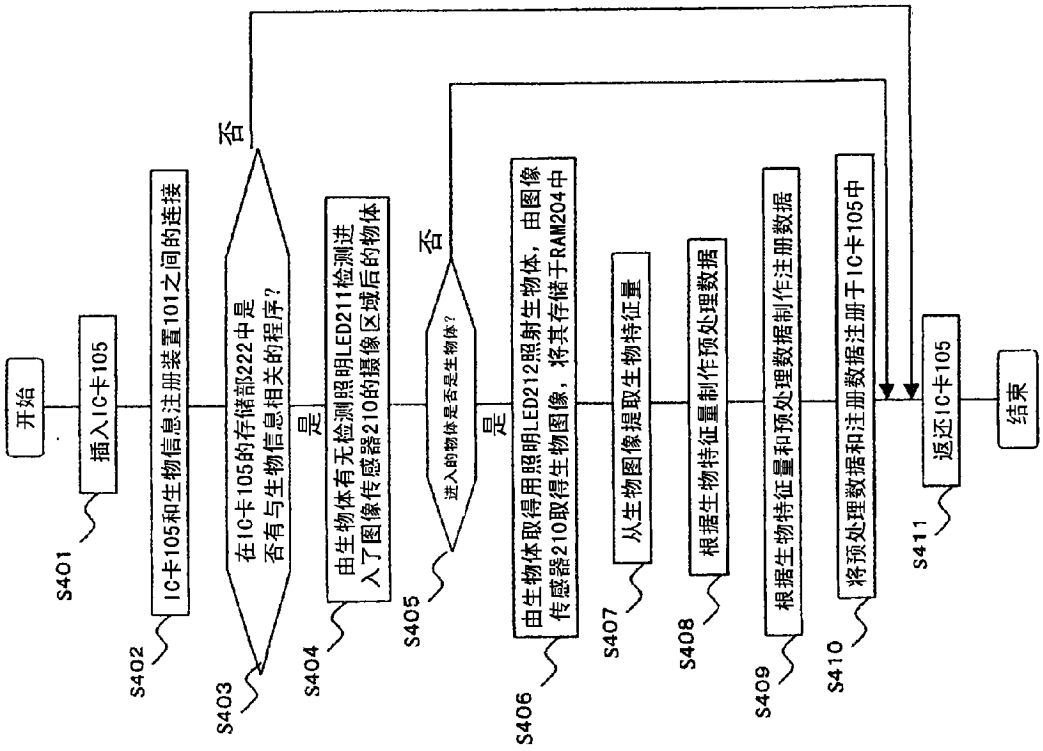

开始
插入IC卡105
S401
IC卡105和生物信息注册装置101之间的连接
S402
在IC卡105的存储部222中是否有与生物信息相关的程序？
S403
否
是
由生物体有无检测照明LED211检测进入了图像传感器210的摄像区域后的物体
S404
进入的物体是否是生物体？
S405
否
是
由生物体取得用照明LED212照射生物体，由图像传感器210取得生物图像，将其存储于RAM204中
S406
从生物图像提取生物特征量
S407
根据生物特征量制作预处理数据
S408
根据生物特征量和预处理数据制作注册数据
S409
将预处理数据和注册数据注册于IC卡105中
S410
返还IC卡105
S411
结束

图4

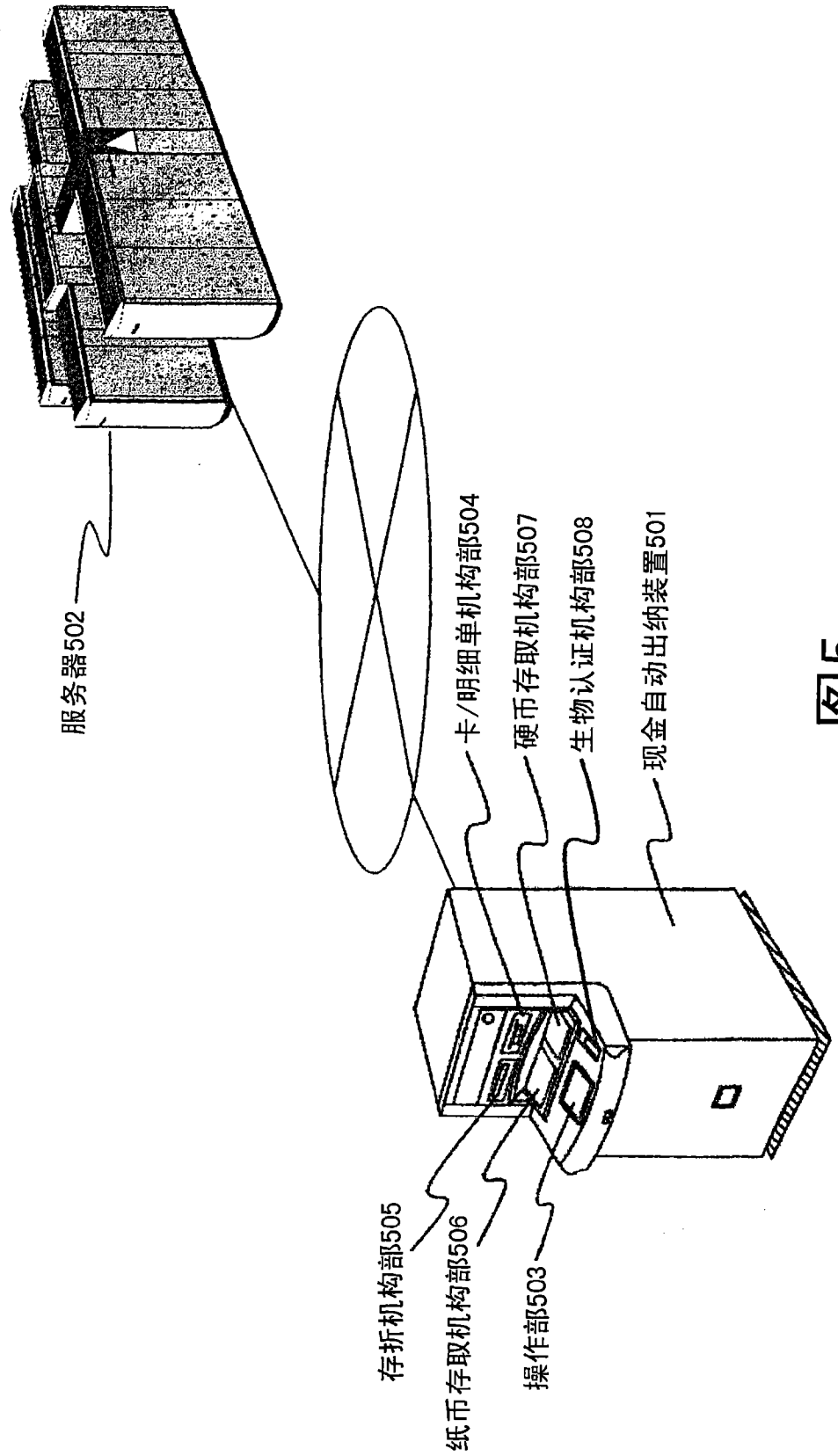

服务器502
卡/明细单机构部504
硬币存取机构部507
生物认证机构部508
现金自动出纳装置501
存折机构部505
纸币存取机构部506
操作部503

图5

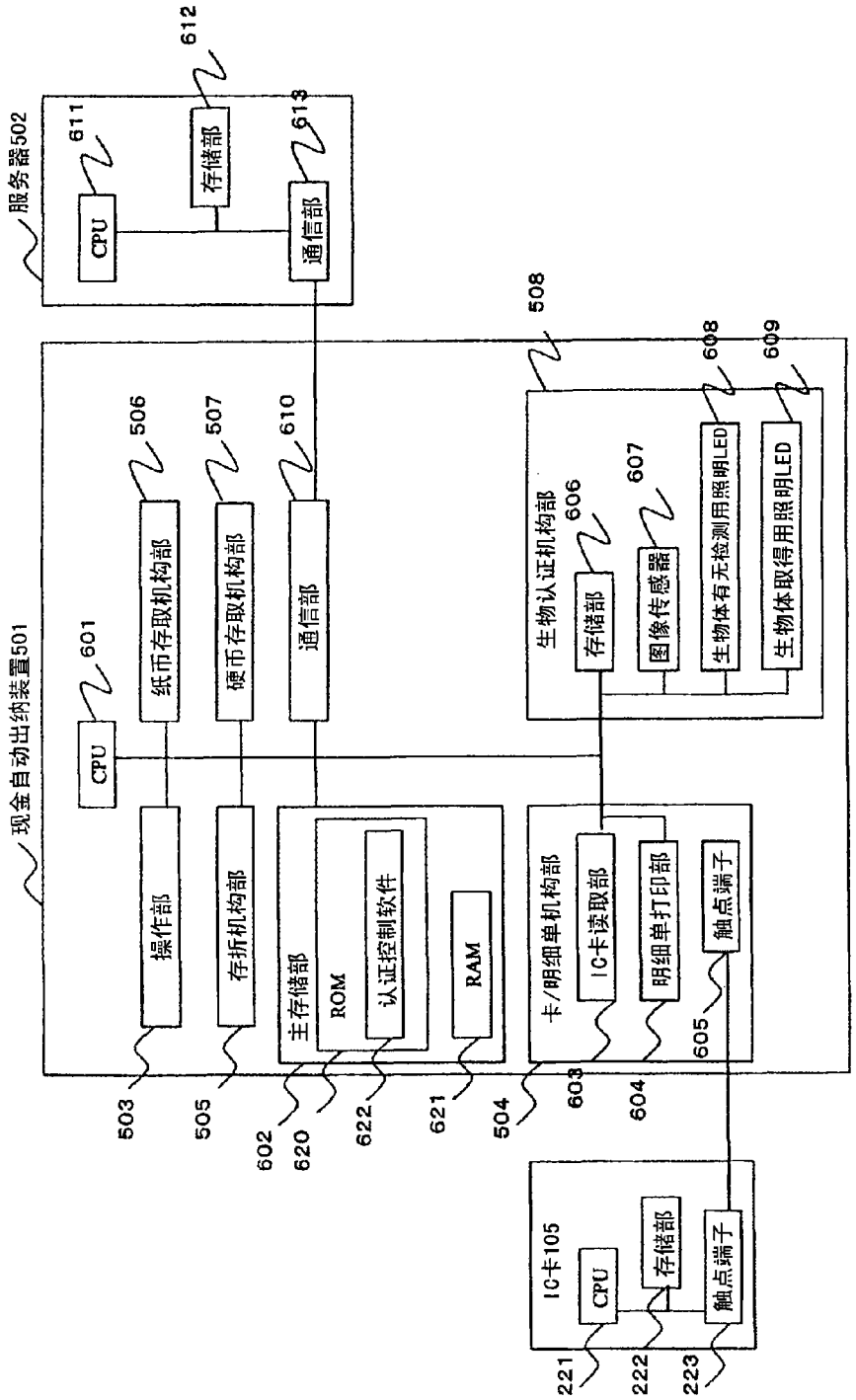

服务器502
CPU
611
存储部
612
通信部
613
现金自动出纳装置501
CPU
601
纸币存取机构部
506
硬币存取机构部
507
通信部
610
508
生物认证机构部
存储部
606
图像传感器
607
生物体有无检测用照明LED
608
生物体取得用照明LED
609
操作部
存折机构部
主存储部
ROM
认证控制软件
RAM
卡/明细单机构部
IC卡读取部
明细单打印部
触点端子
605
503
505
602
620
622
621
504
603
604
IC卡105
CPU
存储部
触点端子
221
222
223

图6

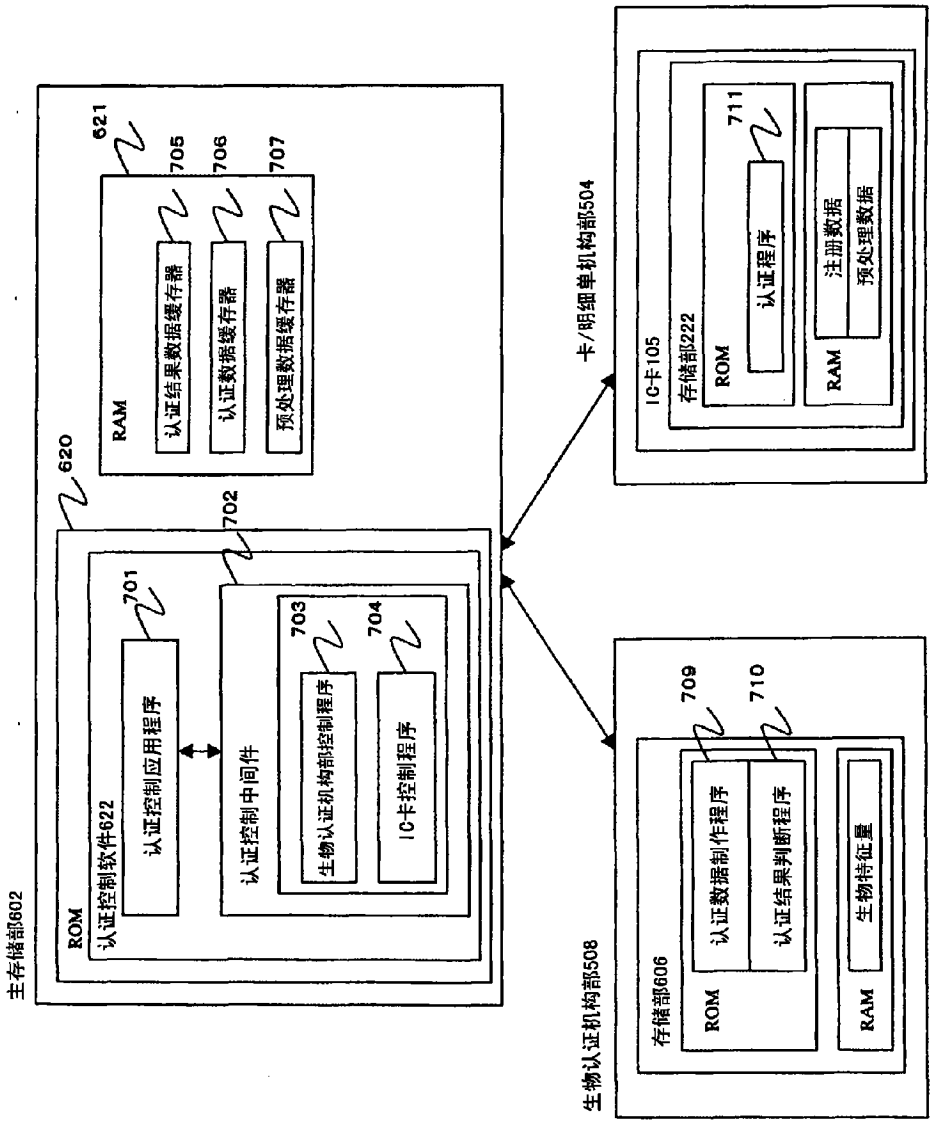

主存储部602
ROM
620
认证控制软件622
701
认证控制应用程序
702
认证控制中间件
703
生物认证机构部控制程序
704
IC卡控制程序
RAM
621
705
认证结果数据缓存器
706
认证数据缓存器
707
预处理数据缓存器
卡/明细单机构部504
IC卡105
存储部222
ROM
711
认证程序
RAM
注册数据
预处理数据
生物认证机构部508
存储部606
ROM
709
认证数据制作程序
710
认证结果判断程序
RAM
生物特征量

图7

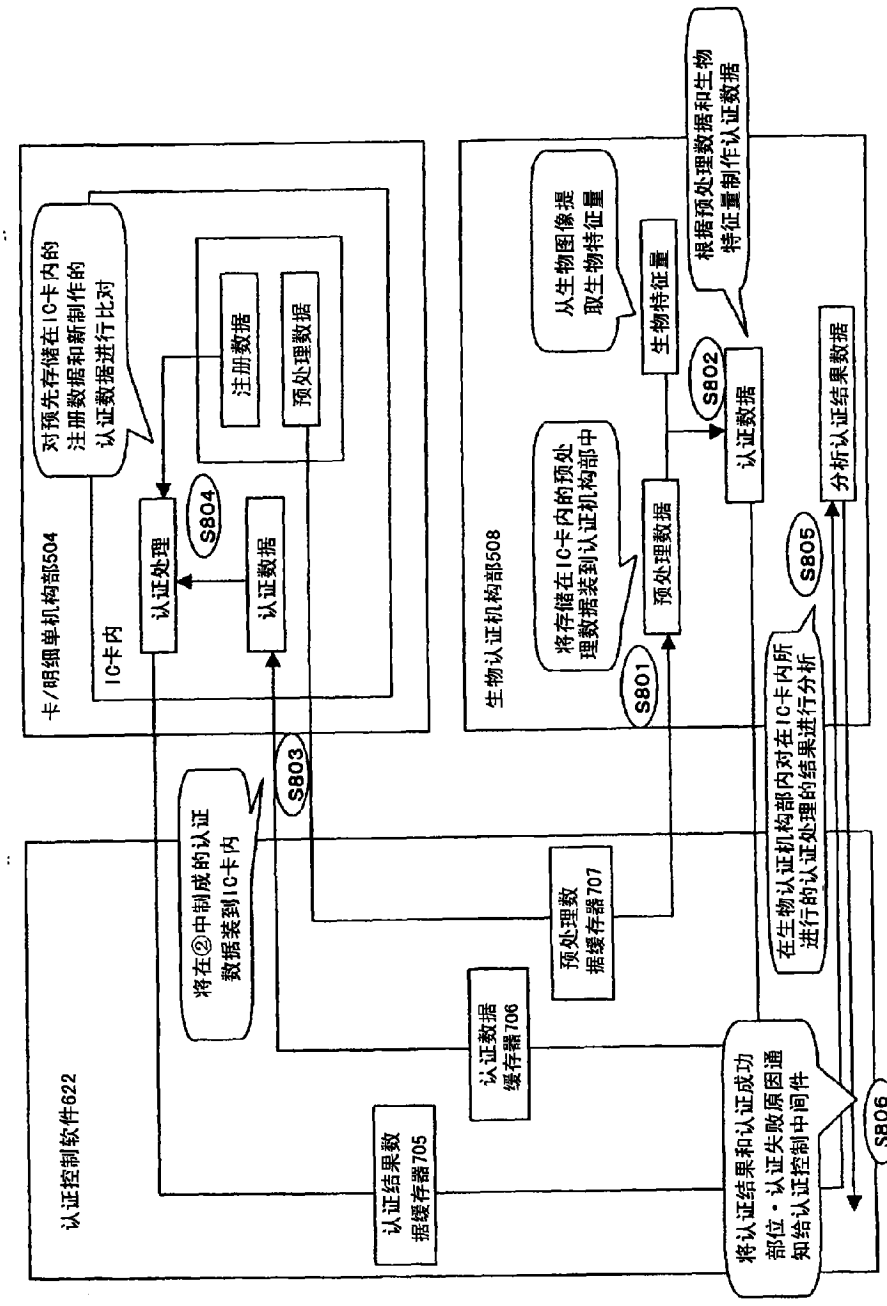

认证控制软件622
卡/明细单机构部504
IC卡内
认证处理
认证数据
注册数据
预处理数据
对预先存储在IC卡内的注册数据和新制作的认证数据进行比对
S804
S803
将在②中制成的认证数据装到IC卡内
生物认证机构部508
从生物图像提取生物特征量
生物特征量
根据预处理数据和生物特征量制作认证数据
S802
认证数据
将存储在IC卡内的预处理数据装到认证机构部中
预处理数据
S801
S805
分析认证结果数据
在生物认证机构部内对在IC卡内所进行的认证处理的结果进行分析
认证结果数据缓存器705
认证数据缓存器706
预处理数据缓存器707
将认证结果和认证成功部位·认证失败原因通知给认证控制中间件
S806

图8

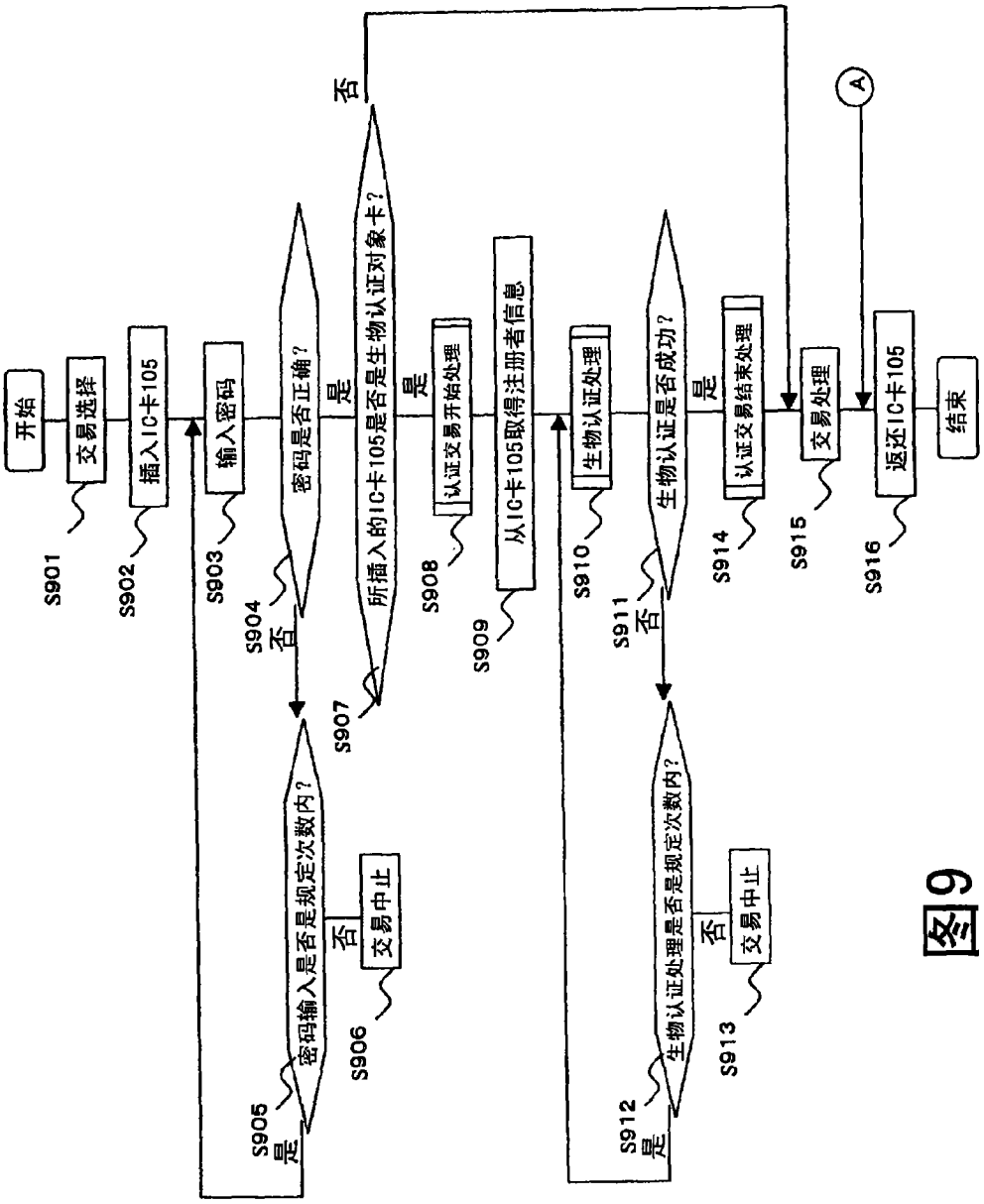

开始
交易选择
插入IC卡105
输入密码
密码是否正确?
否
是
所插入的IC卡105是否是生物认证对象卡?
否
是
认证交易开始处理
从IC卡105取得注册者信息
生物认证处理
生物认证是否成功?
否
是
认证交易结束处理
交易处理
返还IC卡105
结束
密码输入是否是规定次数内?
否
是
交易中止
生物认证处理是否是规定次数内?
否
是
交易中止
S901
S902
S903
S904
S905
S906
S907
S908
S909
S910
S911
S912
S913
S914
S915
S916
A

图9

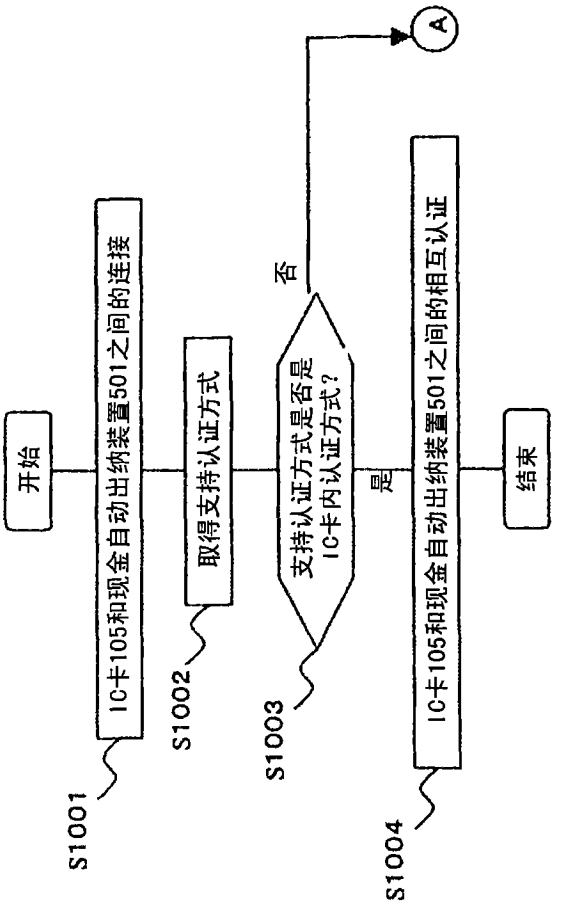

开始
IC卡105和现金自动出纳装置501之间的连接
S1001
取得支持认证方式
S1002
支持认证方式是否是IC卡内认证方式？
S1003
否
A
是
IC卡105和现金自动出纳装置501之间的相互认证
S1004
结束

图10

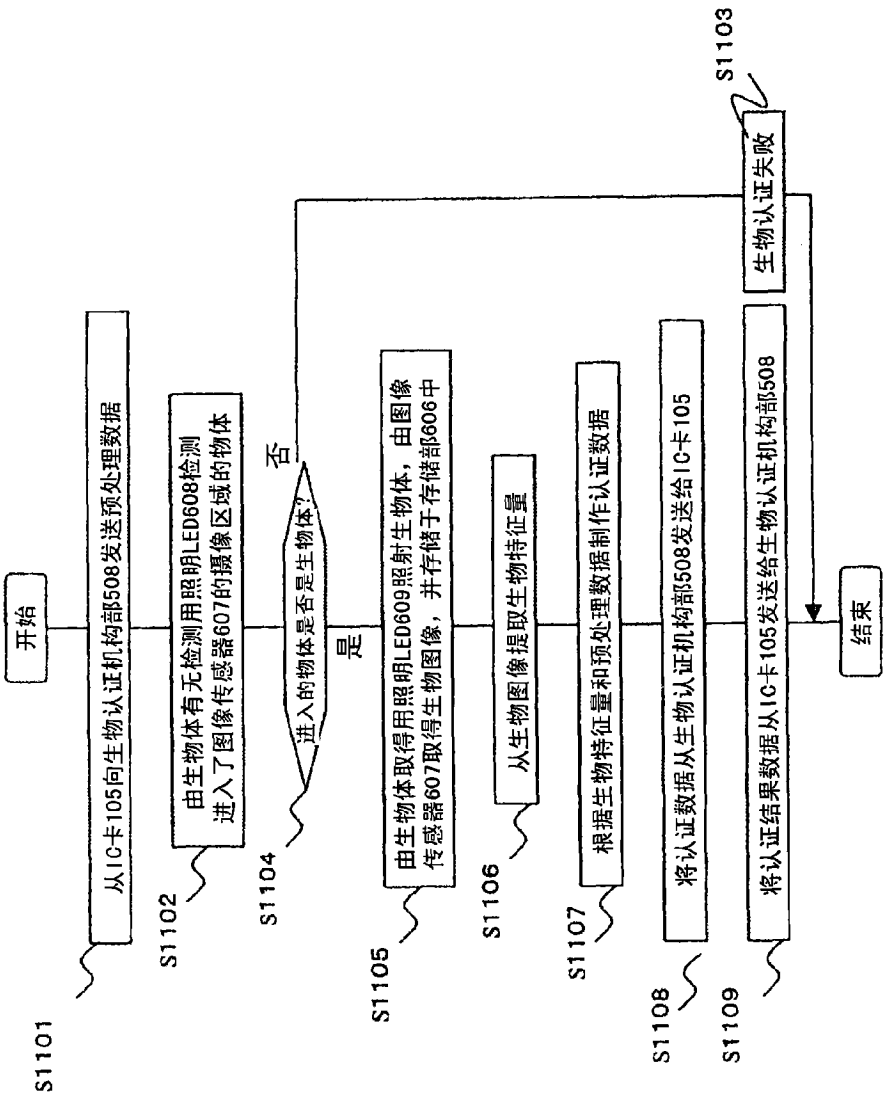

开始
从IC卡105向生物认证机构部508发送预处理数据
S1101
由生物体有无检测用照明LED608检测进入了图像传感器607的摄像区域的物体
S1102
进入的物体是否是生物体?
S1104
否
是
S1103
生物认证失败
由生物体取得用照明LED609照射生物体，由图像传感器607取得生物图像，并存储于存储部606中
S1105
从生物图像提取生物特征量
S1106
根据生物特征量和预处理数据制作认证数据
S1107
将认证数据从生物认证机构部508发送给IC卡105
S1108
将认证结果数据从IC卡105发送给生物认证机构部508
S1109
结束

图11

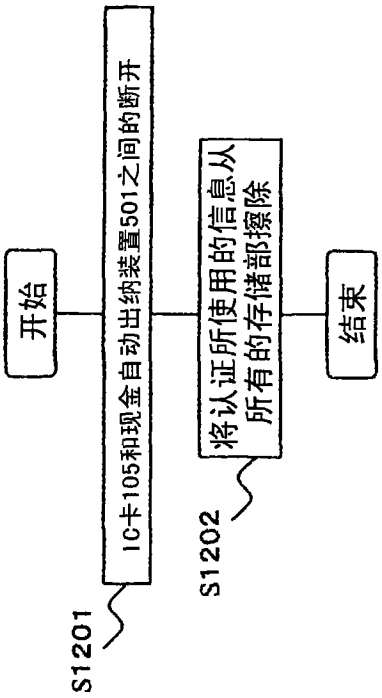

开始
IC卡105和现金自动出纳装置501之间的断开
将认证所使用的信息从所有的存储部擦除
结束
S1201
S1202

图12