

發明專利說明書

(本申請書格式、順序及粗體字，請勿任意更動，※記號部分請勿填寫)

※申請案號：97100819

※申請日期：97 年 01 月 09 日

※IPC 分類：G06A 7/00 (2006.01)

一、發明名稱：

G07F 7/00 (2006.01)

(中) 結帳用終端機及積體電路 (I C) 卡
(英) Settlement terminal and IC card

G06F 21/00 (2006.01)

二、申請人：(共 1 人)

1. 姓 名：(中) 日立製作所股份有限公司
(英) HITACHI, LTD.

代表人：(中) 1. 古川一夫
(英) 1. FURUKAWA, KAZUO

地 址：(中) 日本國東京都千代田區丸之內一丁目六番六號
(英) 6-6, Marunouchi 1-chome, Chiyoda-ku, Tokyo, Japan

國籍：(中英) 日本 JAPAN

三、發明人：(共 4 人)

1. 姓 名：(中) 相川慎
(英) AIKAWA, MAKOTO

國 籍：(中) 日本
(英) JAPAN

2. 姓 名：(中) 高見穰
(英) TAKAMI, YUTAKA

國 籍：(中) 日本
(英) JAPAN

3. 姓 名：(中) 伊藤滋行
(英) ITO, SHIGEYUKI

國 籍：(中) 日本
(英) JAPAN

4. 姓 名：(中) 橋本和則
(英) HASHIMOTO, KAZUNORI

國 籍：(中) 日本

(英) JAPAN

四、聲明事項：

◎本案申請前已向下列國家（地區）申請專利 ☐ 主張國際優先權：

【格式請依：受理國家（地區）；申請日；申請案號數 順序註記】

1. 日本 ; 2007/01/17 ; 2007-007602 ☒ 有主張優先權

(英) JAPAN

四、聲明事項：

◎本案申請前已向下列國家（地區）申請專利 ☐ 主張國際優先權：

【格式請依：受理國家（地區）；申請日；申請案號數 順序註記】

1. 日本 ; 2007/01/17 ; 2007-007602 ☒ 有主張優先權

九、發明說明

【發明所屬之技術領域】

本發明關於積體電路卡（IC卡）。

【先前技術】

習知金融交易使用之現金卡或信用卡雖以使用磁帶方式之卡片為主流，但近年來使用偽造卡之不當使用急增之故，IC卡之替換被急速進展。其中，IC卡可以使用埋入卡片中之IC晶片，主動進行資料之保護，和磁帶方式之卡片比較偽造極為困難。現在使用IC卡之現金卡或信用卡之卡片以EMV規格為業界標準（*defacto standard*）。

於EMV規格，採用PIN比對方式作為IC卡持有者之本人確認方式。其中，PIN（*Personal Identification Number*）為現金卡或信用卡之密碼。但是，PIN比對（*verification*）方式有如下問題，亦即IC卡持有者本身有可能忘掉PIN之值的問題，及無法充分防止盜用造成之偽裝問題。因此，近年來，利用指紋、靜脈、虹膜等他人難以盜取、而且因個人而異之生體資訊而成的生體認證方式被注目。使用IC卡之生體（*biometrics*）認證方式被揭示於專利文獻1。

於專利文獻1（特開2001-344213號公報）揭示：事先將本人之生體資訊保存於IC卡（以下稱保存於IC卡之生體資訊為生體登錄資料），本人確認時，將使用生體資訊感測器進行生體資訊之檢測而獲得的生體資訊（以下稱

爲生體比對資料)，輸入至 IC 卡。於 IC 卡，則於內部進行生體登錄資料與生體比對資料之比對處理，而確認是否爲本人。

【發明內容】

（發明所欲解決之課題）

但是，現金卡或信用卡採用之 PIN 比對方式，爲防止不當使用者重複輸入適當之 PIN，而找出之 PIN，大多設定 PIN 比對之失敗次數，在設定次數範圍內 PIN 比對失敗時，成爲無法使用金融交易。但是，正當使用者忘掉 PIN 之值而錯誤輸入之情況下，亦成爲無法使用金融交易此點就便利性而言乃爲需要解決之問題。

另外，於生體認證方式，例如登錄於 IC 卡之生體登錄資料之精確度不良、或生體之隨時間變化導致登錄於 IC 卡之生體登錄資料於現在之生體資訊間之差異變大情況下，即使本人亦被判定爲他人之可能性變大。因此，使用 IC 卡之生體認證方式，其被使用於現金卡或信用卡等金融交易時，若發生此一現象則會產生即使本人亦無法進行金融交易之問題。

因此，組合 PIN 比對與生體認證方式，而進行能兼顧安全與便利性之本人確認的結帳用終端機及 IC 卡之實現成爲一大課題。

（用以解決課題的手段）

為解決上述問題，本發明之結帳用終端機，係具有：密碼輸入部，用於輸入該使用者之密碼；及生體資訊取得部，依據特定之生體認證方式來取得該使用者之生體資訊；該結帳用終端機，在進行該使用者之本人確認之前，係由該 IC 卡接收：本人確認方式清單、亦即可使用之本人確認方式之清單；及本人確認方式優先度，其表示本人確認方式之優先度；依據該本人確認方式清單及該本人確認方式優先度，來判斷進行使用該密碼輸入部之密碼比對，或進行使用該生體資訊取得部之生體認證。

又，本發明之 IC 卡，係具有：密碼比對功能，其藉由比對密碼而進行使用者之本人確認；及生體認證功能，係使用生體認證來進行使用者之本人確認；係管理：本人確認方式優先度，其表示本人確認方式之優先度；密碼比對殘餘次數，用於表示該密碼比對功能之殘餘試行次數；及生體認證殘餘次數，用於表示該生體認證功能之殘餘試行次數。

又，本發明之 IC 卡，係於記憶體儲存有第 1 應用（application）、第 2 應用及作業系統（operating system）者，該作業系統具有：應用間通信功能，於該第 1 應用與第 2 應用之間進行資料通信；及應用雜湊（hash）值產生功能，用於產生該第 2 應用之雜湊值；該第 1 應用，係使用該雜湊值產生功能取得對該第 2 應用之第 1 雜湊值加以保持，之後，使用該應用間通信功能進行和該第 2 應用間之資料通信時，係使用該雜湊值產生功能

取得對該第 2 應用之第 2 雜湊值，藉由比較該第 1 雜湊值與該第 2 雜湊值，而判斷是否進行和該第 2 應用間之資料通信。

如上述說明，組合 PIN 比對與生體認證方式，可以實現能兼顧安全與便利性之本人確認的結帳用終端機及 IC 卡。

【實施方式】

以下依據圖面說明本發明之實施形態。

（第 1 實施形態）

依據圖 1～9 說明本發明第 1 實施形態。圖 1 為第 1 實施形態之結帳系統之構成方塊圖，其構成包含：IC 卡 100，結帳用終端機 200，網路 220，及結帳中心 230。

IC 卡 100，係由結帳用終端機 200 之使用者持有，使用於進行本人確認及結帳交易處理。結帳中心 230，係由主機電腦（host computer）等構成，介由網路（network）220 連接於結帳用終端機 200，進行結帳交易處理之集中管理。

又，本實施形態中，結帳用終端機 200 假設為例如銀行之 ATM 或信用卡結帳用終端機。或者是行動電話或 PDA 等之行動終端機亦可。又，結帳用終端機 200 之使用者，雖假設為例如持有 IC 卡 100、亦即現金卡或信用卡等金融卡者，但不限定於結帳交易處理，例如使用 IC 卡 100

進行之本人確認，其被利用於出入場或網路使用之取用管理等情況下亦可適用本實施形態。

以下說明 IC 卡 100 之內部構成。IC 卡 100 具有通信部 101，記憶體 102，及運算處理部 103。通信部 101，係使用於 IC 卡 100 和外部間之通信，例如可考慮為依據國際標準規格之 ISO/IEC 7816 規定之接觸通信，或者可考慮為依據國際標準規格之 ISO/IEC 14443 規定之非接觸通信，或者依據其他規格之通信亦可適用本實施形態。

記憶體 102，具有儲存 IC 卡 100 保持之程式或資料的功能，由 ROM（唯獨記憶體）或 EEPROM（電氣抹除可程式化唯獨記憶體）或 RAM（隨機存取記憶體）等半導體記憶體構成。運算處理部 103，負責 IC 卡 100 全體之控制，可經由通信部 101 接收指令，依據記憶體 102 儲存之程式進行對應於指令之處理，進行將對應之回復經由通信部 101 傳送至外部的控制。

以下說明結帳用終端機 200 之內部構成。結帳用終端機 200 具有：IC 卡通信部 201，PIN 輸入部 202，生體資訊感測器 203，記憶體 204，中心通信部 205，使用者介面部 206，及運算處理部 207。IC 卡通信部 201，係使用於控制 IC 卡 100，例如可考慮為依據國際標準規格之 ISO/IEC 7816 規定之接觸通信，或者可考慮為依據國際標準規格之 ISO/IEC 14443 規定之非接觸通信，或者依據其他規格之通信亦可適用本實施形態。

PIN 輸入部 202，具有輸入使用者之 PIN 的功能，例

如可考慮為數字輸入專用之小型鍵盤、亦即數字鍵盤（ten-key）。感測器通信部 205，具有讀取生體資訊的功能，例如可考慮為讀取指紋或指靜脈（finger vein）等，或者具有讀取其他生體資訊的功能者亦適用本實施形態。

記憶體 204，具有儲存結帳用終端機 200 使用之程式 210 或關連資料的功能，可由硬碟或半導體記憶體等構成。中心通信部 205，係使用於和結帳中心 230 進行資料通信，具有連接於電話或網際網路等共用線路網或專用線路網的功能。

使用者介面部 206，具有對結帳用終端機 200 之使用者輸出、提示影像資料或文字等視覺資訊或聲音資訊的顯示功能，及輸入結帳用終端機 200 之使用者必要之資訊的功能。顯示功能，可考慮使用影像管顯示器或液晶顯示器。輸入功能，可考慮使用鍵盤或觸控面板。運算處理部 207，負責結帳用終端機 200 全體之控制，可依據記憶體 204 儲存之結帳程式 210 進行使用 IC 卡 100 之結帳處理。

以下說明 IC 卡 100 之記憶體 102 儲存之程式及資料之構成。於記憶體 102 儲存有：結帳應用 110，生體認證應用 130，作業系統 140，及共用緩衝區 150。

結帳應用 110 為，執行使用 IC 卡 100 之結帳處理時被使用之 IC 卡應用程式。生體認證應用 130 為，執行使用 IC 卡 100 之生體認證處理時被使用之 IC 卡應用程式。

作業系統 140 為系統程式，用於提供執行結帳應用 110、生體認證應用 130 之必要之基本功能，具有選擇、

執行由外部指定之 IC 卡應用之功能。又，具有防火牆功能，可保護各 IC 卡應用所管理之程式或資料免受其他 IC 卡應用之影響。作業系統 140 之具體例可為例如 IC 卡之作業系統、亦即 MULTOS 或 Java（登記商標）Card。或者使用其他作業系統亦適用本實施形態。

共用緩衝區 150 為，儲存經由通信部 101 接收之指令或對應之回復的緩衝區。共用緩衝區 150 用於儲存：在結帳應用 110 與生體認證應用 130 之間接收／傳送之資料。結帳應用 110 具有藉由 PIN 比對進行本人確認的功能，但不具有藉由生體認證進行本人確認的功能。因此，結帳應用 110 執行藉由生體認證之本人確認時，係使生體認證應用 130 經由共用緩衝區 150 執行生體認證處理。

以下說明結帳應用 110 之資料構成。結帳應用 110 所管理之資料包含：結帳 AID111，生體 AID 清單 112，結帳 AP 鍵 113，生體 AP 雜湊（hash）值 114，本人確認方式清單 115，本人確認方式優先度 116、登錄 PIN117，生體認證殘餘次數 118，PIN 比對殘餘次數 119，本人確認結果 120，及使用者辨識號碼 121。

結帳 AID111，係提供給予結帳應用 110 的應用辨識子（AID：Application Identifier）。其中，AID，係為辨識 IC 卡用的辨識子，用於作業系統 140 進行應用之選擇時。國際流通之 IC 卡應用之 AID 附加編號方法被規定於國際規格之 ISO／IEC7816－5。

生體 AID 清單 112，係結帳應用 110 可使用之生體認

證應用之 AID 之清單。假設結帳應用 110 僅對應 1 種類之生體認證應用時，於生體 AID 清單 112 僅儲存對應之生體認證應用之 AID。結帳 AP 鍵 113，係結帳應用 110 於結帳處理時執行之各種密碼運算處理使用之鍵資料。

生體 AP 雜湊值 114，係結帳應用 110 可使用之生體認證應用之雜湊值。其中，雜湊值，係使對象之資料或程式，藉由稱為雜湊函數之函數加以運算之結果值。雜湊值，其由不同資料獲得同一雜湊值之頻度非常小，具有由雜湊值無法推定基礎資料的特徵。因此，結帳應用 110 事先取得生體 AP 雜湊值 114，對生體認證應用委託生體認證時，藉由再度取得生體 AP 雜湊值 114 加以比較，即可檢測出生體認證應用之資料或程式被破壞、篡改而被變更。當結帳應用 110 檢測出生體認證應用之破壞、篡改時，可進行判斷而取消生體認證應用之委託。

其中，產生生體 AP 雜湊值 114 之雜湊函數，可考慮例如 SHA-1 雜湊函數，或其他雜湊函數亦可適用本實施形態。藉由使用可信賴性之雜湊函數，無法由生體 AP 雜湊值 114 推定出生體應用之內容，不必擔心生體應用之內容洩漏。

本人確認方式清單 115，係結帳應用 110 可執行之本人確認方式之清單。本人確認方式優先度 116，係表示生體認證之本人確認與 PIN 比對之本人確認之其中一方之優先度較高。例如本人確認方式優先度 116 之值為「0」時，表示生體認證之優先度較高，「1」時表示 PIN 比對

之優先度較高，「2」時表示兩者之優先度相等而加以編碼化。或以其他編碼化而表示優先度之情況亦適用本實施形態之範圍。又，結帳應用 110 對應之生體認證方式有多數種類時，分別表示各個生體認證方式之優先順位亦可。

登錄 PIN117 為 IC 卡 100 之使用者之 PIN，生體認證殘餘次數 118，係設定經由結帳應用 110 執行之生體認證處理之殘餘試行次數。PIN 比對殘餘次數 119，係設定經由結帳應用 110 執行之 PIN 比對處理之殘餘試行次數。生體認證殘餘次數 118 和 PIN 比對殘餘次數 119，係設定特定之正整數之值作為初期值，本人確認失敗之每一次被減少。生體認證殘餘次數 118 為「0」時，設為結帳應用 110 不可執行生體認證。又，PIN 比對殘餘次數 119 為「0」時，設為結帳應用 110 不可執行 PIN 比對。

於本實施形態之說明中，雖然結帳應用 110 使用生體認證殘餘次數 118 進行可否執行生體認證之管理，但結帳應用 110，不保持生體認證之殘餘試行次數，而是保持生體認證失敗之次數，據以進行可否執行生體認證之管理，亦為本實施形態之範圍。

又，於本實施形態之說明中，雖然結帳應用 110 使用 PIN 比對殘餘次數 119 進行可否執行 PIN 比對之管理，但結帳應用 110，不保持 PIN 比對之殘餘試行次數，而是保持 PIN 比對失敗之次數，據以進行可否執行 PIN 比對之管理，亦為本實施形態之範圍。

本人確認結果 120，係設定結帳應用 110 進行本人確

認之結果。使用者辨識號碼 121，係辨識 IC 卡 100 之使用者的編號。例如信用卡結帳時設定為信用卡編號，現金卡交易時設定為銀行負帳戶編號，或者以其他編號來辨識使用者亦可。

以下說明生體認證應用 130 之資料構成。生體認證應用 130 所管理之資料包含：生體 AID131，生體登錄資料 132，結帳 AP 雜湊值 133。

生體 AID131，係提供給予生體認證應用 130 的應用辨識子，和上述結帳 AID111 同樣，係為辨識 IC 卡應用，而作為作業系統 140 選擇 IC 卡應用時被使用。生體登錄資料 132，係 IC 卡 100 之使用者登錄的生體資訊。生體登錄資料 132，可考慮使用指紋圖案或指靜脈圖案等，或者使用其他之生體資訊者亦為本實施形態之範圍。

結帳 AP 雜湊值 133，係結帳應用 110 之雜湊值。被使用於檢測結帳應用 110 之破壞、或篡改。

以下說明作業系統 140 管理之資料及功能。作業系統 140，係保持應用管理表格 141。又，具有：外部通信功能 142，應用追加刪除功能 143，應用執行功能 144，應用間通信功能 145，及應用雜湊值產生功能 146。

應用管理表格 141，係作業系統 140 管理 IC 卡應用時使用之表格。

外部通信功能 142，係控制通信部 101 由 IC 卡 100 外部接收指令之同時，傳送對應之回復的功能。應用追加刪除功能 143，係使 IC 卡應用由 IC 卡 100 外部下載，將下

載之 IC 卡應用登錄於應用管理表格 141 而設為可執行的功能，及將登錄於應用管理表格 141 之 IC 卡應用加以刪除的功能。

應用執行功能 144，係依據來自於 IC 卡 100 外部之指令，選擇登錄於應用管理表格 141 之任一 IC 卡應用，之後，由 IC 卡 100 外部接收指令之後，執行所選擇之 IC 卡應用而進行和指令對應之處理的功能。

其中，IC 卡應用，係依據不依存於 IC 卡硬體的專用指令集被作成的程式，應用執行功能 144 係進行，讀取依據專用指令集被作成的程式而執行的解譯器（interpreter）（或虛擬機器）處理。

應用執行功能 144 具有防火牆功能，可保護 IC 卡應用之程式或資料，免於 IC 卡 100 外部及 IC 卡 100 內部登錄之其他 IC 卡應用之不正當存取。應用執行功能 144 之具體例可為例如 IC 卡之作業系統、亦即 MULTOS 或 Java（登記商標）Card 具備的功能。

應用間通信功能 145，係設定現在執行中之 IC 卡應用 A 可對指定之 IC 卡應用 B 傳送信息，可由 IC 卡應用 B 接收和信息對應之處理結果的功能。

具體言之為，現在執行中之 IC 卡應用 A 將信息儲存於共用緩衝區 150 之同時，指定 IC 卡應用 B 之 AID，呼叫應用間通信功能 145 時，應用間通信功能 145 將現在執行中之 IC 卡應用 A 設為暫時停止狀態之後，設定 AID 所指定之 IC 卡應用 B 為可執行狀態。IC 卡應用 B 則進行信

息對應之處理，將處理結果儲存於共用緩衝區 150 之後結束處理。

之後，應用間通信功能 145 設定 IC 卡應用 A 回復可執行狀態。IC 卡應用 A 由共用緩衝區 150 取得和信息對應之處理結果。和信息對應之處理結果，係被儲存於共用緩衝區 150，因此可於 IC 卡應用間被共用，但和信息對應之處理，係於 IC 卡應用之內部被執行，因此處理內容可隱蔽，不會暴露於其他 IC 卡應用。

如上述說明，應用間通信功能 145，係在結帳應用 110 對生體認證應用 130 委託生體認證處理時被使用。應用間通信功能 145 之具體例可為例如 IC 卡之作業系統、亦即 MULTOS 具備的委派（delegation）功能或 Java（登記商標）Card 具備的 SIO（Shareable Interface Object）功能。

應用雜湊值產生功能 146，係針對登錄於應用管理表格 141 之 IC 卡應用之資料或程式，藉由雜湊函數之使用而產生其之雜湊值的功能。其中，產生雜湊值之雜湊函數，可考慮例如 SHA-1 雜湊函數，或其他雜湊函數亦可適用本實施形態。

又，執行中之 IC 卡應用，可以指定其他之 IC 卡應用之 AID，呼叫應用雜湊值產生功能 146 而取得指定之 IC 卡應用之雜湊值。其中，產生雜湊值用之原資料，不論是構成 IC 卡應用之資料或程式全體，或者程式之全體或一部分，或資料之全體或一部分之任一情況均為本實施形態

之適用範圍。

圖 2 為應用管理表格 (table) 141 之構成例。於圖 2，應用管理表格 141，係依據登錄之 IC 卡應用之每一個，記錄著 AID161，應用參照位址 162，應用容量之大小 163，選擇旗標 164，呼叫順序 165，以及應用雜湊值 166 的表格。其中，AID161，係辨識對應之 IC 卡應用，作業系統 140 進行應用之選擇時被使用的辨識子。

應用參照位址 162，係保持對應之 IC 卡應用的記憶體之先頭位址。於圖 2，對各 IC 卡應用僅設定 1 個位址，但亦可設定編碼 (code) 部之先頭位址及資料部之先頭位址等多數個位址。

應用容量之大小 163，係對應之 IC 卡應用容量之大小 (size)。於圖 2，對各 IC 卡應用容量僅設定 1 個大小，但亦可設定編碼 (code) 部之容量大小及資料部之容量大小等多數個容量大小。選擇旗標 164 係表示對應之 IC 卡應用現在是否被選擇。於圖 2 之例，IC 卡應用被選擇時設為「1」，未被選擇時設為「0」，但亦可為其他表示法。呼叫順序 165 係表示藉由應用間通信功能 145 被呼叫之 IC 卡應用之順序。於圖 2 之例，呼叫之順序以數字之大小表示，但亦可為其他表示法。

應用雜湊值 166，係設定對應之 IC 卡應用之雜湊值。於圖 2，對各 IC 卡應用僅設定 1 個雜湊值，但亦可設定編碼部全體或一部分之雜湊值、資料部全體或一部分之雜湊值。又，上述應用雜湊值產生功能 146，於每一次接受雜

湊值之產生要求時，再度計算對應之 IC 卡應用之雜湊值亦可，或者不進行雜湊值之再度計算，而參照應用管理表格 141 登錄之應用雜湊值 166 之情況亦為本實施形態之適用範圍。

以下說明本人確認方式清單 115 之內部構成。於圖 3，本人確認方式清單 115 之構成包含多數個本人確認方式 170。本人確認方式 170 為，辨識本人確認方式用的編號。於圖 3 之例，本人確認方式 170 為「1」時表示離線（off line）PIN 比對之本人確認，「2」時表示線上（on line）PIN 比對之本人確認，「3」時表示指靜脈認證之本人確認，「4」時表示指紋（finger print）認證之本人確認，「5」時表示虹膜（iris）認證之本人確認。又，「0」表示不需要本人確認。

其中，離線 PIN 比對係於 IC 卡 100 內部進行 PIN 比對的方式，線上 PIN 比對係於結帳中心 230 進行 PIN 比對的方式。本人確認方式清單 115，只要能辨識本人確認方式，就算是圖 3 以外之標記方法，亦屬於本實施形態之適用範圍。

圖 4 為在 IC 卡 100 與結帳用終端機 200 之間進行的結帳處理順序（Sequence）圖。於圖 4 之結帳處理順序，係進行生體認證之本人確認。

於步驟 S1001，結帳用終端機 200 為選擇 IC 卡 100 內部之結帳應用 110，而將結帳應用 110 之 AID、亦即結帳 AID 傳送至 IC 卡 100，由結帳應用 110 接收生體 AID

清單。於本處理步驟，於結帳用終端機 200 與 IC 卡 100 間之通信，可考慮使用例如 ISO/IEC7816 及 EMV 規格規定之 SELECT FILE 指令。

於步驟 S1002，結帳應用 110 經由作業系統 140 之應用執行功能 144 被選擇，將結帳應用 110 保持之生體 AID 清單回送至結帳用終端機 200。

於步驟 S1003，結帳用終端機 200 由結帳應用 110 取得之生體 AID 清單，選擇可執行之生體認證之生體 AID，為進行結帳處理之初期化，將選擇之生體 AID 傳送結帳應用 110。於本處理步驟，於結帳用終端機 200 與 IC 卡 100 間之通信，可考慮使用例如 EMV 規格規定之 GET PROCESSING OPTIONS 指令。

於步驟 S1004，結帳應用 110，在指定之生體 AID 不包含於生體 AID 清單 112 時判斷為不進行生體認證。或者，在指定之生體 AID 包含於生體 AID 清單 112 時，為確認指定之生體 AID 所對應之生體認證應用 130 是否被不當篡改，而對作業系統 140 委託生體認證應用 130 之雜湊值之產生。

於步驟 S1005，作業系統 140 使用應用管理表格 141，進行指定之生體 AID 所對應之生體認證應用 130 之檢索，使用應用雜湊值產生功能 146 產生生體認證應用 130 之雜湊值。

於步驟 S1006，結帳應用 110 進行取得之雜湊值與事先取得之生體 AP 雜湊值 114 之比較。比較結果一致時判

斷生體認證應用 130 可被利用，不一致時判斷為生體認證應用 130 被不當篡改。

於步驟 S1007，結帳用終端機 200，係由結帳應用 110 傳送本人確認方式清單及本人確認方式優先度之取得要求。於本處理步驟，於結帳用終端機 200 與 IC 卡 100 間之通信，可考慮使用例如 EMV 規格規定之 READ RECORD 指令。

於步驟 S1008，若結帳應用 110 於步驟 S1004 及步驟 S1006 判斷生體認證應用 130 可被利用時，追加本人確認方式清單 115 對應之生體認證方式及 PIN 比對方式。或者，判斷生體認證應用 130 不可被利用時，僅將 PIN 比對方式追加於本人確認方式清單 115。將本人確認方式清單 115 與本人確認方式優先度 116 送回結帳用終端機 200。

於步驟 S1009，結帳用終端機 200 由本人確認方式清單 115 與本人確認方式優先度 116 確認可執行生體認證時，係使用生體資訊感測器 203 取得使用者之生體比對資料。

於步驟 S1010，結帳用終端機 200 為進行生體認證之本人確認，而將使用者之生體比對資料傳送至結帳應用 110。於本處理步驟，於結帳用終端機 200 與 IC 卡 100 間之通信，可考慮使用例如 EMV 規格規定之 VERIFY 指令。

於步驟 S1011，結帳應用 110，係將取得之生體比對資料傳送至生體認證應用 130，將生體認證處理委由生體

認證應用 130 進行。該委託處理，係介由作業系統 140 之應用間通信功能 145 進行。之後，由生體認證應用 130 取得本人確認結果，將本人確認結果 120 保存之同時，傳送至結帳用終端機 200。

於步驟 S1012，生體認證應用 130，為確認結帳應用 110 是否被不當篡改，而對作業系統 140 委託結帳應用 110 之雜湊值之產生。

於步驟 S1005，作業系統 140，係使用應用雜湊值產生功能 146 產生結帳應用 110 之雜湊值。

於步驟 S1014，生體認證應用 130 係進行取得之雜湊值與事先取得之結帳 AP 雜湊值 133 之比較。比較結果不一致時判斷為結帳應用 110 被不當篡改，而中斷生體認證處理。

於步驟 S1015，生體認證應用 130，係使用由結帳應用 110 取得之生體比對資料與事先保持之使用者生體登錄資料，進行生體認證處理。之後，以生體認證結果作為將本人確認結果回送至結帳應用 110。

於步驟 S1016，結帳用終端機 200，在由結帳應用 110 取得之本人確認結果為「成功」隨進行結帳處理，而將交易關連資料傳送結帳應用 110。其中，交易關連資料係包含交易金額、交易日期、認證用亂數等的資料。之後，結帳用終端機 200，由結帳應用 110 取得交易承認資料。其中，交易承認資料，係表示結帳應用 110 承認結帳處理的資料，使用密碼處理而產生。

由結帳應用 110 取得之交易承認資料，係被傳送至結帳中心 230 而進行結帳處理之最終確認亦可。於本處理步驟，於結帳用終端機 200 與 IC 卡 100 間之通信，可考慮使用例如 EMV 規格規定之 GENERATE APPLICATION CRYPTOGRAM 指令。

於步驟 S1017，結帳應用 110，由結帳用終端機取得交易關連資料之後，進行本人確認結果 120 之確認。本人確認結果 120 之確認成功時，判斷交易內容正確之後，使用結帳 AP 鍵 113 進行密碼處理，產生交易承認資料。其中，產生交易承認資料用的密碼處理，不論使用 DES 密碼等之共通鍵密碼方式，或使用 RSA 密碼等之公開鍵密碼方式，均屬於本實施形態之適用範圍。

於使用圖 4 說明之結帳處理順序中，在 IC 卡 100 與生體認證應用 130 之間，互相之雜湊值係介由作業系統 140 取得，而檢測出不正當之篡改，因此可安全進行 IC 卡應用間之通信。又，結帳用終端機 200 傳送至 IC 卡 100 的生體比對資料，為防止盜聽或篡改而進行密碼處理亦可。此情況下，進行生體比對資料之密碼處理時使用的鍵資料，可以事前使用特定之鍵共用協定，而於結帳用終端機 200 與生體認證應用 130 之間被共用。

圖 5 為結帳用終端機 200 進行之本人確認處理流程圖。本處理，係於如 4 所示結帳處理順序之步驟 S1001、步驟 S1003 及步驟 S1007 進行。

於步驟 S5000，結帳用終端機 200，由 IC 卡 100 取得

被儲存於 IC 卡 100 之生體認證應用之 AID 清單、亦即生體 AID 清單。

於步驟 S5001，結帳用終端機 200，係由 IC 卡 100 取得之生體 AID 清單之中，選擇可於結帳用終端機 200 利用之生體認證方式所對應之生體 AID，將選擇之生體 AID 傳送 IC 卡 100。其中若由 IC 卡 100 未取得生體 AID 清單，或者 IC 卡 100 中之生體 AID 清單為空白，或者結帳用終端機 200 可利用之生體認證方式不存在時，亦可不必將生體 AID 傳送 IC 卡 100。之後，由 IC 卡 100 取得本人確認方式清單及本人確認方式優先度。

於步驟 S5002，若由 IC 卡 100 取得之本人確認方式清單之中被記載為本人確認不必要時，不執行本人確認處理，移至步驟 S5005。若未記載為本人確認不必要時，則移至步驟 S5003。

於步驟 S5003，若由 IC 卡 100 取得之本人確認方式清單之中，被記載為結帳用終端機 200 所選擇之生體認證方式時，移至步驟 S5005。若非如此，則移至步驟 S5004。

於步驟 S5004，若由 IC 卡 100 取得之本人確認方式清單之中，被記載為 PIN 比對時，移至步驟 S5007。若非如此，則本人確認失敗，移至步驟 S5011。

於步驟 S5005，若由 IC 卡 100 取得之本人確認方式清單之中，被記載為 PIN 比對時，移至步驟 S5006。若非如此，則移至步驟 S5008。

於步驟 S5006，確認由 IC 卡 100 取得之本人確認方式優先度若 PIN 比對之優先度高於生體認證時，移至步驟 S5007。若生體認證之優先度高於 PIN 比對時，則移至步驟 S5008。若生體認證之優先度等於 PIN 比對之優先度時，則移至步驟 S5009。

於步驟 S5007，結帳用終端機 200 係藉由使用者介面部 206 對使用者提示導引而使進行 PIN 比對之本人確認。之後，使用 PIN 輸入部 202，由使用者輸入 PIN，進行 PIN 比對。PIN 比對，不論是於 IC 卡 100 內部進行之離線 PIN 比對，或者於結帳中心 230 進行之線上 PIN 比對，均適用於本實施形態之範圍。

於步驟 S5008，結帳用終端機 200 係藉由使用者介面部 206 對使用者提示導引而使進行生體認證之本人確認。之後，使用生體資訊感測器 203 產生使用者之生體比對資料，進行生體認證。生體認證，係藉由將生體比對資料傳送至 IC 卡 100 而進行。

於步驟 S5009，結帳用終端機 200 係藉由使用者介面部 206 對使用者提示導引，而使進行 PIN 比對或生體認證之其中任一之本人確認。若使用者選擇 PIN 比對時，則使用 PIN 輸入部 202，由使用者輸入 PIN 而進行 PIN 比對。PIN 比對，不論是於 IC 卡 100 內部進行之離線 PIN 比對，或者於結帳中心 230 進行之線上 PIN 比對，均適用於本實施形態之範圍。若使用者選擇生體認證時，則使用生體資訊感測器 203 產生使用者之生體比對資料，進行生體

認證。

於步驟 S5010，若 PIN 比對或生體認證之本人確認結果成功時，移至步驟 S5012。若非如此，則移至步驟 S5011。

於步驟 S5011，結帳用終端機 200，因使用者之本人確認失敗，而中止結帳處理。

於步驟 S5012，結帳用終端機 200，因使用者之本人確認成功，而繼續結帳處理。

於使用圖 5 說明之結帳用終端機 200 所進行本人確認處理流程中，結帳用終端機 200，可依據由 IC 卡 100 取得之本人確認方式清單及本人確認方式優先度，而適當選擇 PIN 比對或生體認證之其中任一之本人確認方式。因此，IC 卡 100 未對應於生體認證，而對使用者提示進行生體認證之導引等之舉動可以被防止。

又，於步驟 S5011，選擇之本人確認方式失敗時，若和失敗之本人確認方式不同的未實施之本人確認方式，被記載於本人確認方式清單時，追加實施該未實施之本人確認方式亦可。又，追加實施之本人確認方式成功時，不中斷結帳處理而繼續亦可。此情況下，因最初實施之本人確認方式失敗之故，可考慮課以減少結帳處理之限度額等之任何條件。

圖 6 為 IC 卡 100 內部之結帳應用 110 所進行之本人確認方式清單 115 之設定處理流程圖。本處理，係於圖 4 之結帳處理順序之步驟 S1008 進行。

於步驟 S2000，結帳應用 110，係將結帳應用 110 對應之本人確認方式全部追加於本人確認方式清單 115。

於步驟 S2001，在結帳用終端機 200 以生體 AID 指定特定之生體認證方式時，移至步驟 S2002。若未指定生體認證方式，則移至步驟 S2006。

於步驟 S2002，若結帳應用 110 可支援，結帳用終端機 200 指定之生體 AID 所對應之生體認證方式時，移至步驟 S2003。若非如此，則移至步驟 S2005。

於步驟 S2003，結帳應用 110 係檢測生體認證應用之雜湊值，確認有否被進行不正當之篡改之後，移至步驟 S2004。若非如此，則移至步驟 S2005。

於步驟 S2004，結帳應用 110 係確認生體認證殘餘次數 118，若非「0」則移至步驟 S2007。「0」則移至步驟 S2005。

於步驟 S2005，結帳應用 110，係由本人確認方式清單 115 刪除結帳用終端機 200 所指定之生體認證方式。

於步驟 S2006，結帳應用 110，係由本人確認方式清單 115 刪除全部之生體認證方式。

於步驟 S2007，結帳應用 110 係確認 PIN 比對殘餘次數 119，若非「0」則移至步驟 S2009。「0」則移至步驟 S2008。

於步驟 S2008，結帳應用 110，係由本人確認方式清單 115 刪除 PIN 比對。

於步驟 S2009，結帳應用 110，係將本人確認方式清

單 115 及本人確認方式優先度 116 傳送至結帳用終端機 200。

藉由使用圖 6 說明之本人確認方式清單 115 之設定處理流程，結帳應用 110 可將，在結帳應用 110 於結帳用終端機 200 之間可以處理的、設定有本人確認方式之本人確認方式清單 115，傳送至結帳用終端機 200。

圖 7 為 IC 卡 100 內部之結帳應用 110 所進行之 PIN 比對之處理流程圖。

於步驟 S3001，結帳應用 110，在接收來自結帳用終端機 200 之 PIN 比對要求時，係確認 PIN 比對殘餘次數 119，若為「0」則移至步驟 S3011。若非「0」則移至步驟 S3002。

於步驟 S3002，結帳應用 110，係進行 PIN 比對處理，而確認來自結帳用終端機 200 之 PIN 與結帳應用 110 保持之登錄 PIN117 是否一致。

於步驟 S3003，結帳應用 110，若於步驟 S3002 進行之 PIN 比對處理結果成功，則移至步驟 S3004。若失敗則移至步驟 S3008。

於步驟 S3004，結帳應用 110，因為 PIN 比對處理成功之故，而使 PIN 比對殘餘次數 119 回復為初期設定值。例如若 PIN 比對殘餘次數 119 最初設為「5」，則初期設定值為「5」。又，將 PIN 比對殘餘次數 119 僅加上特定值時，亦為本實施形態之適用範圍。

於步驟 S3005，結帳應用 110，係參照本人確認方式

優先度 116，若 PIN 比對之優先度為生體認證之優先度以上時，移至步驟 S3006。若非如此則移至步驟 S3007。

於步驟 S3006，結帳應用 110，係使生體認證殘餘次數 118 回復為初期設定值。例如若生體認證殘餘次數 118 最初設為「10」，則初期設定值為「10」。又，將生體認證殘餘次數 118 僅加上特定值時，亦為本實施形態之適用範圍。

於步驟 S3007，結帳應用 110，係將本人確認結果 120 設定為「成功」。

於步驟 S3008，結帳應用 110，因為 PIN 比對處理失敗之故，而使 PIN 比對殘餘次數 119 僅減少特定之值。

於步驟 S3009，結帳應用 110，係參照本人確認方式優先度 116，若 PIN 比對之優先度為生體認證之優先度以上時，移至步驟 S3010。若非如此則移至步驟 S3011。

於步驟 S3010，結帳應用 110，係使生體認證殘餘次數 118 僅減少特定之值。

於步驟 S3011，結帳應用 110，係將本人確認結果 120 設定為「失敗」。

於步驟 S3012，結帳應用 110，係將本人確認結果 120 傳送至結帳用終端機 200。

於使用圖 7 說明之結帳應用 110 所進行之 PIN 比對之處理流程中，若 PIN 比對之優先度為生體認證之優先度以上時，PIN 比對成功時，使生體認證殘餘次數 118 及 PIN 比對殘餘次數 119 同時進行初期化，PIN 比對失敗時，使

生體認證殘餘次數 118 及 PIN 比對殘餘次數 119 僅減掉特定值。如此則，即使生體認證殘餘次數 118 為「0」無法進行生體認證之情況下，藉由 PIN 比對之成功，則下次可以再度執行生體認證。其中，PIN 比對之優先度小於生體認證之優先度時，生體認證殘餘次數 118 不受 PIN 比對結果而變動，因此生體認證不影響 PIN 比對之成功否。

圖 8 為 IC 卡 100 內部之結帳應用 110 進行之生體認證之處理流程圖。

於步驟 S4001，結帳應用 110 接收來自結帳用終端機 200 之生體認證要求後，確認生體認證殘餘次數 118，若為「0」則移至步驟 S4011。若不是則移至步驟 S4002。

於步驟 S4002，結帳應用 11 係將接收來自結帳用終端機 200 之生體比對資料，傳送至生體認證應用 130 要求執行生體認證，由生體認證應用 130 取得生體認證結果。

於步驟 S4003，結帳應用 110，在步驟 S4002 由生體認證應用 130 取得之生體認證結果為成功時，移至步驟 S4004。若不是則移至步驟 S4008。

於步驟 S4004，結帳應用 110，因為生體認證成功之故，而使生體認證殘餘次數 118 回復為初期設定值。又，將生體認證殘餘次數 118 僅加上特定值時，亦為本實施形態之適用範圍。

於步驟 S4005，結帳應用 110，係參照本人確認方式優先度 116，若生體認證之優先度為 PIN 比對之優先度以上時，移至步驟 S4006。若非如此則移至步驟 S4007。

於步驟 S4006，結帳應用 110，係使 PIN 比對殘餘次數 119 回復為初期設定值。又，將 PIN 比對殘餘次數 119 僅加上特定值時，亦為本實施形態之適用範圍。

於步驟 S4007，結帳應用 110，係將本人確認結果 120 設為「成功」。

於步驟 S4008，結帳應用 110，因為生體認證失敗之故，而使生體認證殘餘次數 118 減掉特定之值。

於步驟 S4009，結帳應用 110，係參照本人確認方式優先度 116，若生體認證之優先度為 PIN 比對之優先度以上時，移至步驟 S4010。若非如此則移至步驟 S4011。

於步驟 S4010，結帳應用 110，係使 PIN 比對殘餘次數 119 僅減掉特定之值。其中，設定生體認證殘餘次數 118 之值為 N，僅於 N 成為特定整數 M 之倍數時，進行減掉 PIN 比對殘餘次數 119 之值的處理亦可。例如設定 M 為 5，生體認證失敗 5 次時減去 PIN 比對殘餘次數 119 之值。

於步驟 S4011，結帳應用 110，係將本人確認結果 120 設為「失敗」。

於步驟 S4012，結帳應用 110，係將本人確認結果 120 傳送至結帳用終端機 200。

於使用圖 8 說明之結帳應用 110 所進行之生體認證之處理流程中，若生體認證之優先度為 PIN 比對之優先度以上時，生體認證成功時，使生體認證殘餘次數 118 及 PIN 比對殘餘次數 119 同時進行初期化，PIN 比對失敗時，使

生體認證殘餘次數 118 及 PIN 比對殘餘次數 119 同時僅減掉特定值。如此則，即使 PIN 比對殘餘次數 119 為「0」無法進行 PIN 比對之情況下，藉由生體認證之成功，則下次可以再度執行 PIN 比對。其中，生體認證之優先度小於 PIN 比對之優先度時，PIN 比對殘餘次數 119 不受生體認證結果而變動，因此 PIN 比對不會影響生體認證之成否。

圖 9 為 IC 卡 100 內部之結帳應用 110 之 PIN 比對無法利用時，回復為使用生體認證而可利用 PIN 比對之同時，更新為新的 PIN 之處理順序圖。

於步驟 S3501，結帳用終端機 200，係使用生體資訊感測器 203 取得使用者之生體比對資料之同時，使用 PIN 輸入部 202 由使用者輸入新的 PIN。

於步驟 S3502，結帳用終端機 200，係將步驟 S3501 取得之使用者之生體比對資料及新的 PIN 傳送至結帳應用 110。於本處理步驟，於結帳用終端機 200 與 IC 卡 100 間之通信，可考慮使用例如 EMV 規格規定之 PIN CHANGE / UNBLOCK 指令。

於步驟 S3503，結帳應用 110，係將取得之生體比對資料傳送至生體認證應用 130，委由生體認證應用 130 進行生體認證處理。之後，由生體認證應用 130 取得本人確認結果。

於步驟 S3504，生體認證應用 130，係使用由結帳應用 110 取得之生體比對資料，及事先保持之使用者生體登錄資料進行生體認證處理。以該生體認證之結果作為本人

確認結果，而回送至結帳應用 110。

於步驟 S3505，結帳應用 110，在生體認證之本人確認成功時，進行本人確認方式優先度 116 之確認。若生體認證之優先度為 PIN 比對之優先度以上時，藉由變更 PIN 比對殘餘次數 119 成為初期值，而使 PIN 比對回復成為可以利用。又，使登錄 PIN117 之值，更新為由結帳用終端機取得增新的 PIN 之值。

於使用圖 9 說明之處理順序中，結帳用終端機 200 傳送至 IC 卡 100 的 PIN 及生體比對資料，為防止盜聽或篡改而進行密碼處理加以保護亦可。此情況下，進行密碼處理時使用的鍵資料，可以使用事前特定之鍵共用協定，關於 PIN 可於結帳用終端機 200 與結帳應用 110 之間被共用，關於生體比對資料可於結帳用終端機 200 與生體認證應用 130 之間被共用。

（第 2 實施形態）

以下使用圖 10－11 說明本發明第 2 實施形態。圖 10 為第 2 實施形態之結帳系統之構成方塊圖，其構成包含：IC 卡 100，結帳用終端機 200，網路 220，及結帳中心 230。

IC 卡 100，係由結帳用終端機 200 之使用者持有，使用於進行本人確認及結帳交易處理。結帳中心 230，係由主機電腦（host computer）等構成，介由網路 220 連接於結帳用終端機 200，進行結帳交易處理之集中管理。

又，本第 2 實施形態中，和第 1 實施形態同樣，結帳用終端機 200 假設為例如銀行之 ATM 或信用卡結帳用終端機。或者是行動電話或 PDA 等之行動終端機亦可。又，結帳用終端機 200 之使用者，雖假設為例如持有 IC 卡 100、亦即現金卡或信用卡等金融卡者，但不限定於結帳交易處理，例如使用 IC 卡 100 進行之本人確認，其被利用於出入場或網路使用之取用管理等情況下亦可適用本實施形態。

圖 10 所示 IC 卡 100 及結帳用終端機 200 之內部構成，係和圖 1 所示 IC 卡 100 及結帳用終端機 200 之內部構成同樣，假設為作為本人確認被進行之 PIN 比對，係於結帳中心被進行。

以下說明圖 10 所示結帳中心 230 之內部構成。結帳中心 230 具有：結帳用終端機通信部 301，記憶體 302，及運算處理部 303。結帳用終端機通信部 301，係使用於和結帳用終端機 200 之間之通信，具有連接於電話、網際網路等公用線路網、或專用線路網之功能。

記憶體 302，具有儲存控制程式 310 及使用者管理表格 320 的功能，由硬碟或半導體記憶體等構成。其中，使用者管理表格 320，係進行本結帳系統之全部使用者之本人確認時被使用的表格。

運算處理部 303，係負責結帳中心 230 全體之控制，可依據記憶體 302 儲存之控制程式 310 進行結帳處理之集中管理。

以下說明使用者管理表格 320 之內部構成。使用者管理表格 320，係依據登錄之使用者之每一個記錄著使用者辨識號碼 321，登錄 PIN322，PIN 比對殘餘次數 323。其中，使用者辨識號碼 321，係用於辨識使用者的編號，和各使用者之 IC 卡 100 內部之結帳應用 110 管理的使用者辨識號碼 121 為同一之值。例如信用卡結帳時設定為信用卡編號，現金卡交易時設定為銀行負帳戶編號，或者以其他編號來辨識使用者亦可。

登錄 PIN322，係 IC 卡 100 之使用者之 PIN，PIN 比對殘餘次數 323，係設定為結帳中心 230 執行之 PIN 比對處理之殘餘試行次數。PIN 比對殘餘次數 323，係設定特定之正整數之值作為初期值，本人確認失敗之每一次被減少。PIN 比對殘餘次數 323 為「0」時，設為結帳中心 230 不可執行 PIN 比對。

圖 11，係結帳中心 230 執行之 PIN 比對失敗，結帳中心 230 設為不可執行 PIN 比對的處理順序圖。

於步驟 S6001，結帳用終端機 200，係使用 PIN 輸入部 202 由使用者輸入 PIN。

於步驟 S6002，結帳用終端機 200，係將使用者輸入之 PIN 傳送至結帳中心 230，委由進行 PIN 比對之本人確認。

於步驟 S6003，結帳中心 230，係利用使用者輸入之 PIN 與使用者管理表格 320，進行 PIN 比對。於本處理順序中，假設 PIN 比對失敗之同時，PIN 比對殘餘次數 323

減掉後之結果成爲「0」。因此，結帳中心 230 對結帳用終端機 200 傳送不可利用 PIN 比對之指令。

於步驟 S6004，結帳用終端機 200，係將接收來自結帳中心 230 的不可利用 PIN 比對之指令，傳送至結帳應用 110。

於步驟 S6005，結帳應用 110，係設定 PIN 比對殘餘次數 119 爲「0」，設爲不可進行 PIN 比對。

於步驟 S6006，結帳應用 110，係參照本人確認方式優先度 116，若 PIN 比對之優先度爲生體認證之優先度以上時，設定生體認證殘餘次數 118 爲「0」，設爲不可進行生體認證。

於使用圖 11 說明之處理流程中，若 PIN 比對之優先度爲生體認證之優先度以上時，使生體認證殘餘次數 118 及 PIN 比對殘餘次數 119 同時設爲「0」，設爲不可進行 PIN 比對與生體認證之雙方。若生體認證之優先度爲 PIN 比對之優先度以上時，設爲僅不可進行 PIN 比對，可以執行生體認證。

又，若生體認證之優先度爲 PIN 比對之優先度以上時，即使設爲無法進行 PIN 比對之情況下，如圖 8 之說明，藉由生體認證之成功，則下次可以再度執行 PIN 比對。

（發明效果）

藉由使用本發明，可實現較習知更能提升信賴性的結

帳用終端機及 IC 卡。

【圖式簡單說明】

圖 1 為第 1 實施形態之結帳系統之構成方塊圖。

圖 2 為應用管理表格 (table) 141 之構成例。

圖 3 為本人確認方式清單 (list) 115 之內部構成例。

圖 4 為在 IC 卡 100 與結帳用終端機 200 之間進行的結帳處理順序圖。

圖 5 為結帳用終端機 200 進行之本人確認處理流程圖。

圖 6 為結帳應用 110 進行之本人確認方式清單 115 之設定處理流程圖。

圖 7 為結帳應用 110 進行之 PIN 比對之處理流程圖。

圖 8 為結帳應用 110 進行之生體認證之處理流程圖。

圖 9 為生體認證引起之 PIN 比對解除及 PIN 更新處理順序圖。

圖 10 為第 2 實施形態之結帳系統之構成方塊圖。

圖 11 為設定為不可執行結帳中心 230 之 PIN 比對的處理順序圖。

【主要元件符號說明】

100：IC 卡；101：通信部；102：記憶體；103：運算處理部；110：結帳應用；111：結帳 AID；112：生體 AID 清單；113：結帳 AP 鍵；114：生體 AP 雜湊值；

115：本人確認方式清單；116：本人確認方式優先度；
117：登錄 PIN；118：生體認證殘餘次數；119：PIN 比對
殘餘次數；120：本人確認結果；121：使用者辨識號碼；
130：生體認證應用；131：生體 AID；132：生體登錄資
料；133：結帳 AP 雜湊值；140：作業系統；141：應用管
理表格；142：外部通信功能；143：應用追加刪除功能；
144：應用執行功能；145：應用間通信功能；146：應用
雜湊值產生功能；150：共用緩衝區；200：結帳用終端
機；201：IC 卡通信部；202：PIN 輸入部；203：生體資
訊感測器；204：記憶體；205：中心通信部；206：使用
者介面部；207：運算處理部；210：結帳程式；220：網
路；230：結帳中心；161：AID；162：應用參照位址；
163：應用容量之大小；164：選擇旗標；165：呼叫順
序；166：應用雜湊值；170：本人確認方式；301：結帳
用終端機通信部；302：記憶體；303：運算處理部；
310：控制程式；320：使用者管理表格；321：使用者辨
識號碼；322：登錄 PIN；323：PIN 比對殘餘次數。

五、中文發明摘要

發明之名稱：結帳用終端機及積體電路（IC）卡

結帳用終端機，係具有：密碼輸入部，用於輸入該使用者之密碼（password）；及生體資訊（biometrics）取得部，依據特定之生體認證（biometrics authentication）方式來取得該使用者之生體資訊；該結帳用終端機，在進行該使用者之本人確認（personal identification）之前，係由該 IC 卡接收本人確認方式清單（list），亦即可使用之本人確認方式之清單；及本人確認方式優先度，其表示本人確認方式之優先度；依據該本人確認方式清單及該本人確認方式優先度，來判斷進行使用該密碼輸入部之密碼比對，或進行使用該生體資訊取得部之生體認證。

六、英文發明摘要

發明之名稱：

十、申請專利範圍

1.一種結帳用終端機，係藉由和 IC 卡之通信而進行使用者之本人確認者；其特徵為：

該結帳用終端機具有：密碼輸入部，用於輸入該使用者之密碼；及生體資訊取得部，依據特定之生體認證方式來取得該使用者之生體資訊；

該結帳用終端機，在進行該使用者之本人確認之前，係由該 IC 卡接收本人確認方式清單，亦即可使用之本人確認方式之清單；及本人確認方式優先度，其表示本人確認方式之優先度；依據該本人確認方式清單及該本人確認方式優先度，來判斷進行使用該密碼輸入部之密碼比對，或進行使用該生體資訊取得部之生體認證。

2.如申請專利範圍第 1 項之結帳用終端機，其中，

該結帳用終端機，係於該本人確認方式清單，記載著該密碼比對與該生體認證之雙方之本人確認方式，

該本人確認方式優先度，被設定為該密碼比對之優先度高於該生體認證之優先度時，係優先執行該密碼比對。

3.如申請專利範圍第 1 項之結帳用終端機，其中，

該結帳用終端機，係於該本人確認方式清單，記載著該密碼比對與該生體認證之雙方之本人確認方式，

該本人確認方式優先度，被設定為該生體認證之優先度高於該密碼比對之優先度時，係優先執行該生體認證。

4.如申請專利範圍第 1 項之結帳用終端機，其中，

該結帳用終端機，係於該本人確認方式清單，記載著

該密碼比對與該生體認證之雙方之本人確認方式，

該本人確認方式優先度，被設定為該生體認證之優先度相等於該密碼比對之優先度時，係由該使用者選擇執行該密碼比對與該生體認證之其中任一。

5.一種 IC 卡，係進行使用者之本人確認者，其特徵為：

該 IC 卡具有：

密碼比對功能，係藉由比對密碼而進行使用者之本人確認；及

生體認證功能，係使用生體認證來進行使用者之本人確認；

係管理：本人確認方式優先度，其表示本人確認方式之優先度；密碼比對殘餘次數，用於表示該密碼比對功能之殘餘試行次數；及生體認證殘餘次數，用於表示該生體認證功能之殘餘試行次數。

6.如申請專利範圍第 5 項之 IC 卡，其中，

該 IC 卡，在使用該密碼比對功能之本人確認成功時，該本人確認方式優先度被設定成，PIN 比對之優先度為生體認證之優先度以上時，係將該生體認證殘餘次數僅加上特定之值。

7.如申請專利範圍第 5 項之 IC 卡，其中，

該 IC 卡，在使用該生體認證功能之本人確認成功時，該本人確認方式優先度被設定成，生體認證之優先度為密碼比對之優先度以上時，係將該密碼比對殘餘次數僅

加上特定之值。

8.如申請專利範圍第 5 項之 IC 卡，其中，

該 IC 卡，在使用該密碼比對功能之本人確認失敗時，該本人確認方式優先度之設定值被設定成，密碼比對之優先度為生體認證之優先度以上時，係將該生體認證殘餘次數僅減掉特定之值。

9.如申請專利範圍第 5 項之 IC 卡，其中，

該 IC 卡，在使用該生體認證功能之本人確認失敗時，該本人確認方式優先度被設定成，生體認證之優先度為密碼比對之優先度以上時，係將該密碼比對殘餘次數僅減掉特定之值。

10.一種 IC 卡，係進行使用者之本人確認者，其特徵為：

該 IC 卡具有：

密碼比對功能，係藉由比對密碼而進行使用者之本人確認；及

生體認證功能，係使用生體認證來進行使用者之本人確認；

係管理：本人確認方式優先度，其表示本人確認方式之優先度；及事前登錄之第 1 密碼；

由該 IC 卡外部接收第 2 密碼之後，該生體認證功能之執行結果成功時，該本人確認方式優先度被設定成，生體認證之優先度為密碼比對之優先度以上時，係將該第 1 密碼之值更新為該第 2 密碼之值。

11.一種 IC 卡，係和結帳用終端機通信而進行使用者之本人確認者，其特徵為：

該 IC 卡具有：

密碼比對功能，係藉由比對密碼而進行使用者之本人確認；及

生體認證功能，係使用生體認證來進行使用者之本人確認；

係保持：本人確認方式清單，其表示可使用之本人確認方式之清單；密碼比對殘餘次數，用於表示該密碼比對功能之殘餘試行次數；及生體認證殘餘次數，用於表示該生體認證功能之殘餘試行次數；

使該本人確認方式清單之內容，依據該密碼比對殘餘次數及該生體認證殘餘次數加以決定之後，將該本人確認方式清單傳送至該結帳用終端機。

12.如申請專利範圍第 11 項之 IC 卡，其中，

該 IC 卡，在該密碼比對殘餘次數成為特定值以下，判斷其以上之密碼比對無法進行時，係將未包含該密碼比對引起之本人確認方式的該本人確認方式清單傳送至該結帳用終端機。

13.如申請專利範圍第 11 項之 IC 卡，其中，

該 IC 卡，在該生體認證殘餘次數成為特定值以下，判斷其以上之生體認證無法進行時，係將未包含該生體認證引起之本人確認方式的該本人確認方式清單傳送至該結帳用終端機。

14、一種 IC 卡，係於記憶體儲存有第 1 應用、第 2 應用及作業系統者，其特徵為：

該作業系統具有：應用間通信功能，於該第 1 應用與第 2 應用之間進行資料通信；及應用雜湊（hash）值產生功能，用於產生該第 2 應用之雜湊值；

該第 1 應用，係使用該雜湊值產生功能取得對該第 2 應用之第 1 雜湊值加以保持，之後，使用該應用間通信功能進行和該第 2 應用間之資料通信時，係使用該雜湊值產生功能取得對該第 2 應用之第 2 雜湊值，藉由比較該第 1 雜湊值與該第 2 雜湊值，而判斷是否進行和該第 2 應用間之資料通信。

15.一種 IC 卡，係於記憶體儲存有第 1 應用、第 2 應用及作業系統者，其特徵為：

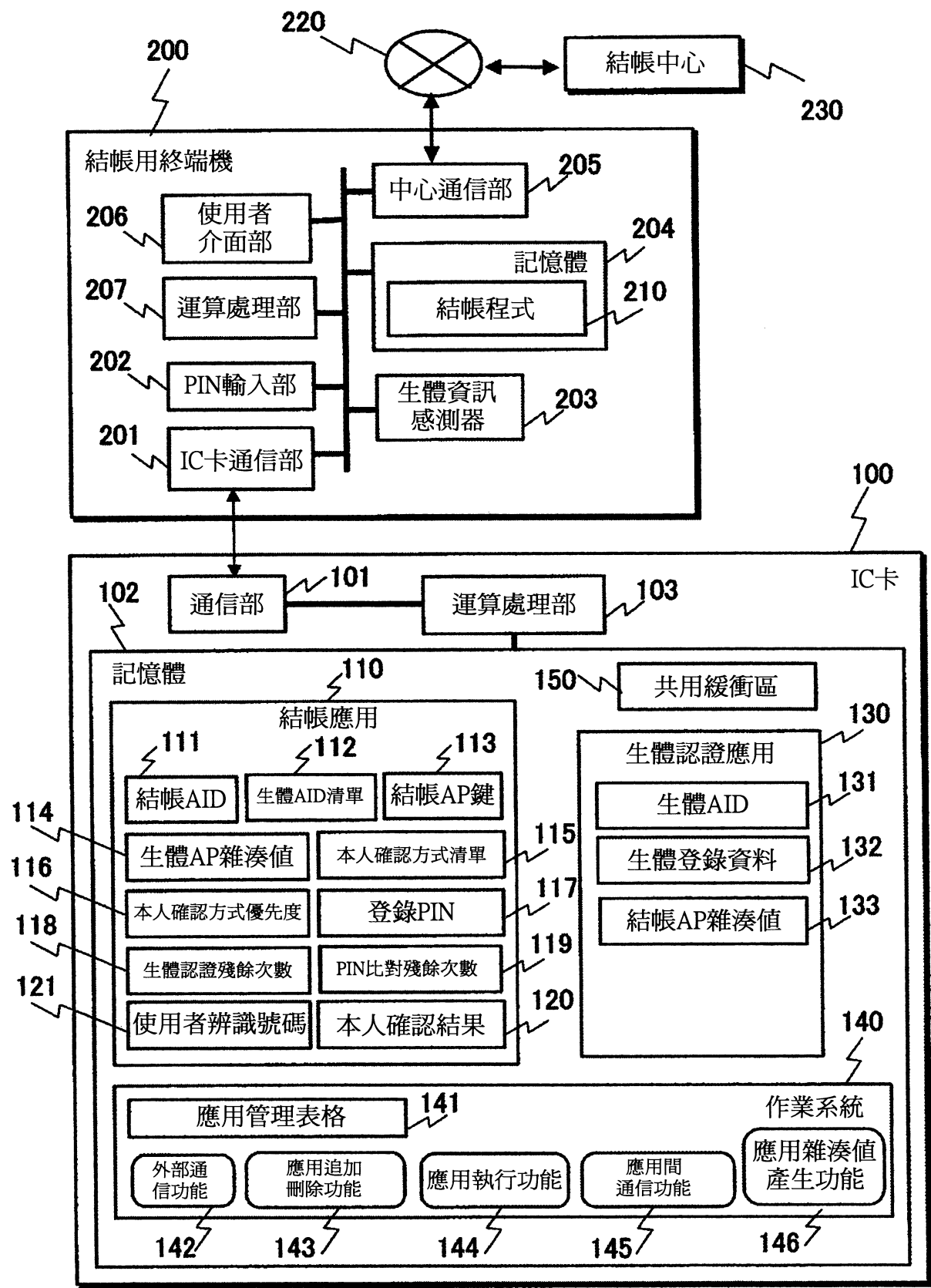
該作業系統具有：應用間通信功能，於該第 1 應用與第 2 應用之間進行資料通信；

該第 1 應用具有：簽名作成功能，用於管理密碼鍵，在使用該密碼鍵之密碼處理產生結帳交易之簽名資料；

該第 2 應用具有：生體認證功能，用於使用生體認證進行使用者之本人確認；

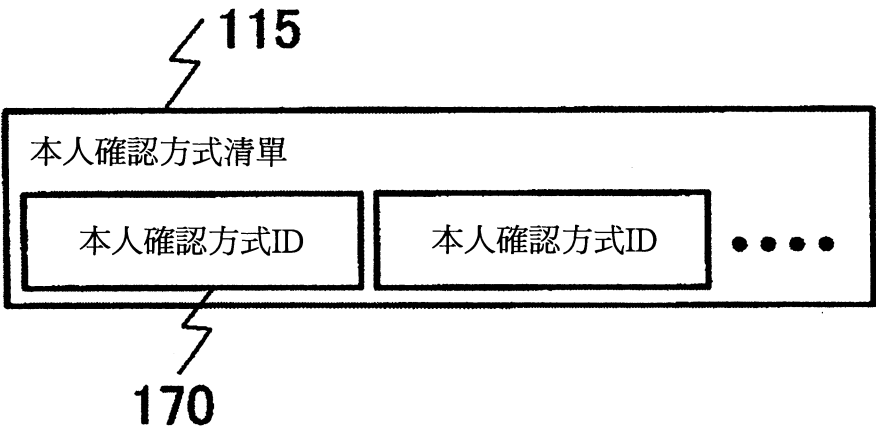
該第 1 應用，係使用該應用間通信功能呼叫該第 2 應用具有之該生體認證功能進行本人確認，由該第 2 應用取得之本人確認結果成功時，係使用該簽名作成功能產生獲知結帳交易之簽名資料。

圖 1



141

圖 3



本人確認方式ID	意味
0	本人確認不要
1	離線PIN比對之本人確認
2	線上PIN比對之本人確認
3	指靜脈認證之本人確認
4	指紋認證之本人確認
5	虹彩認證之本人確認

圖 4

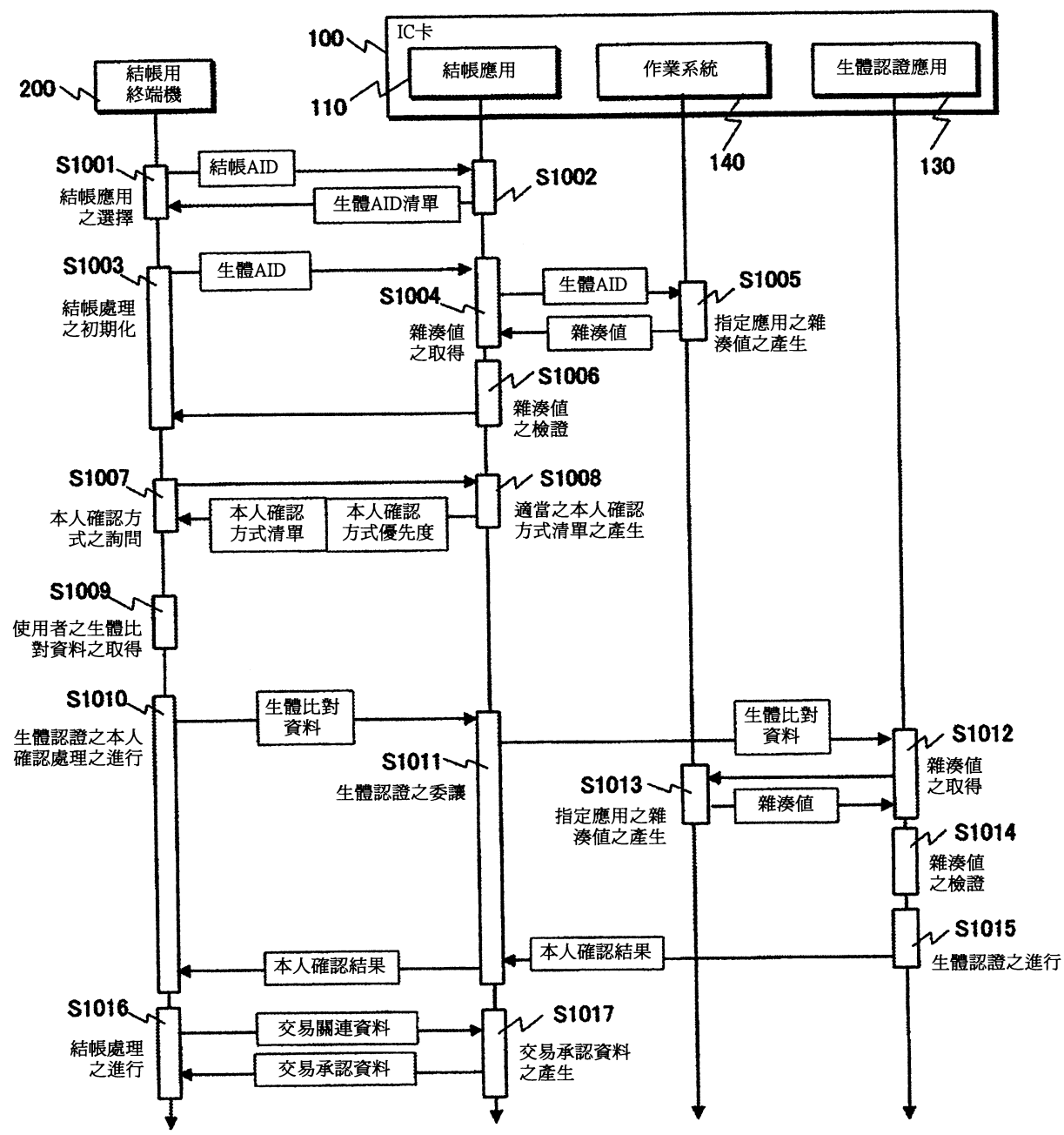


圖5

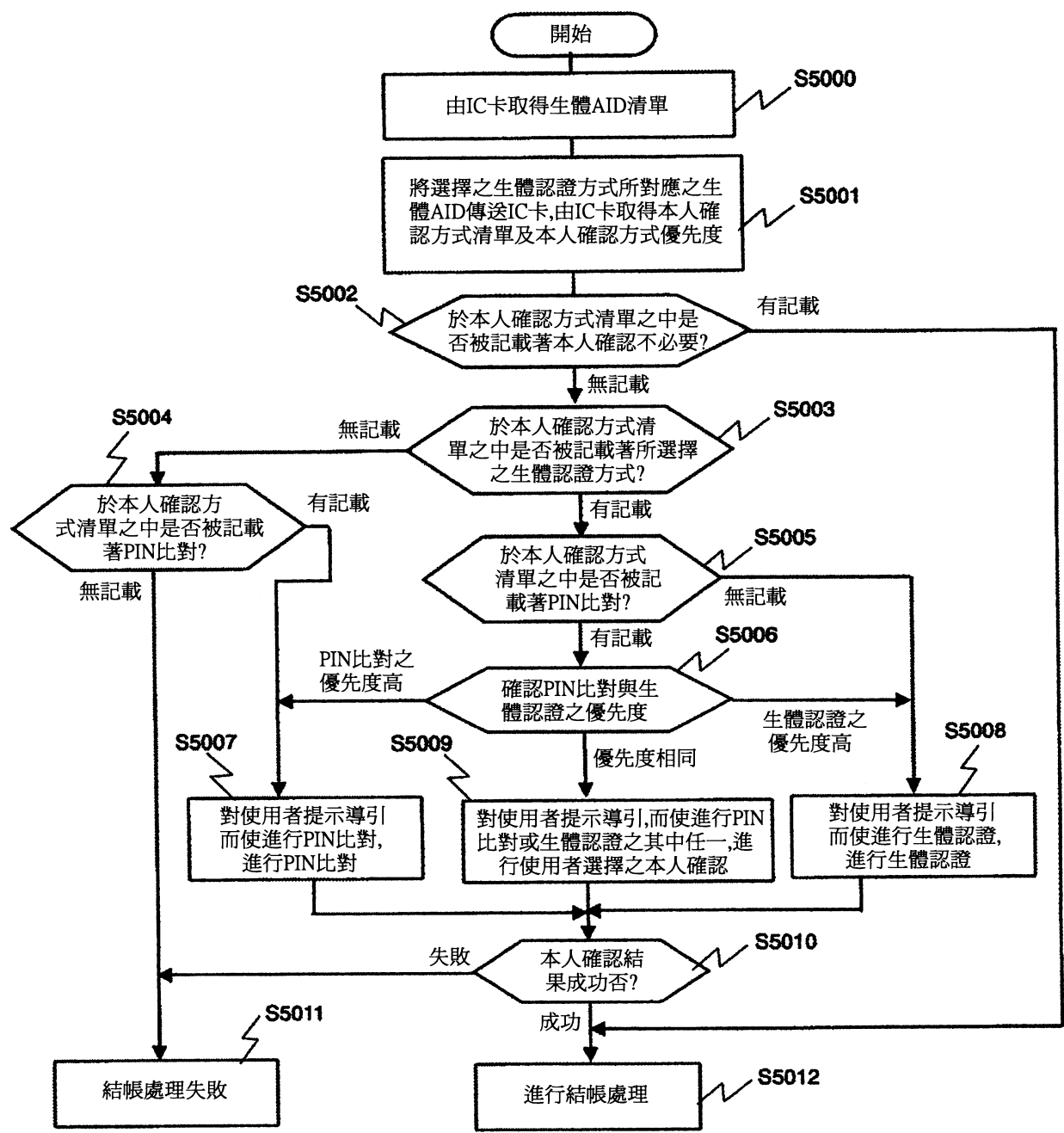


圖6

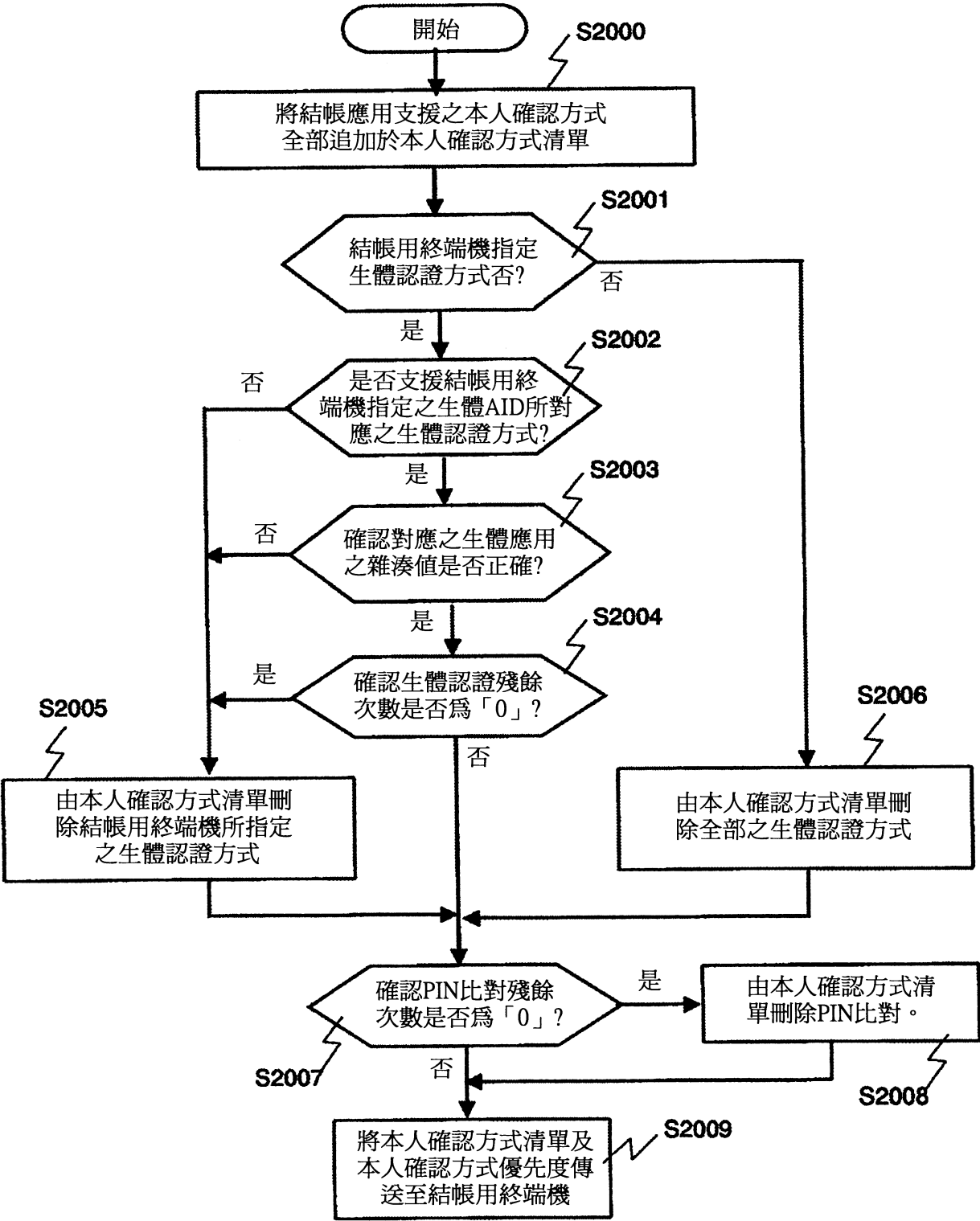


圖 7

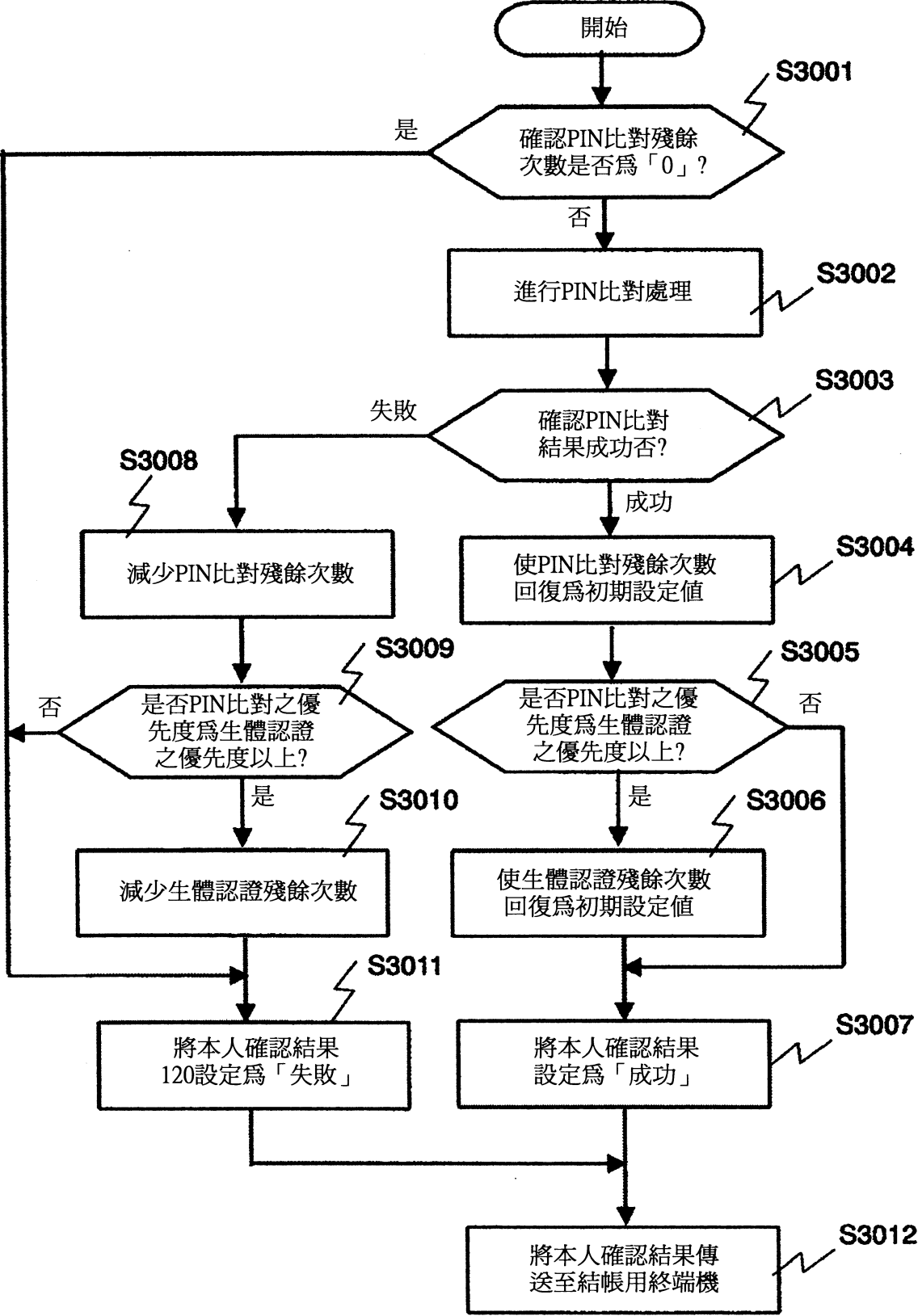


圖 8

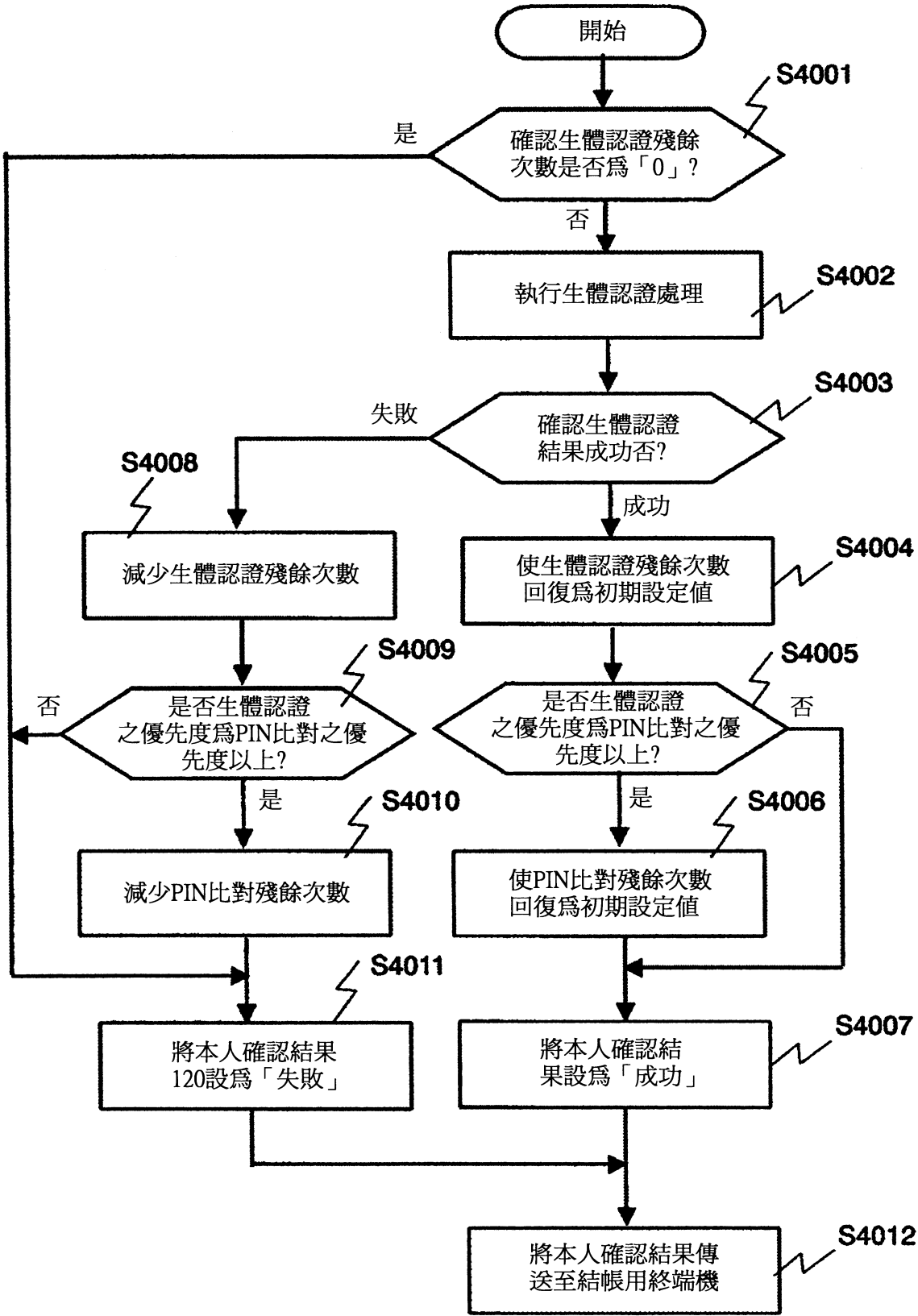


圖 9

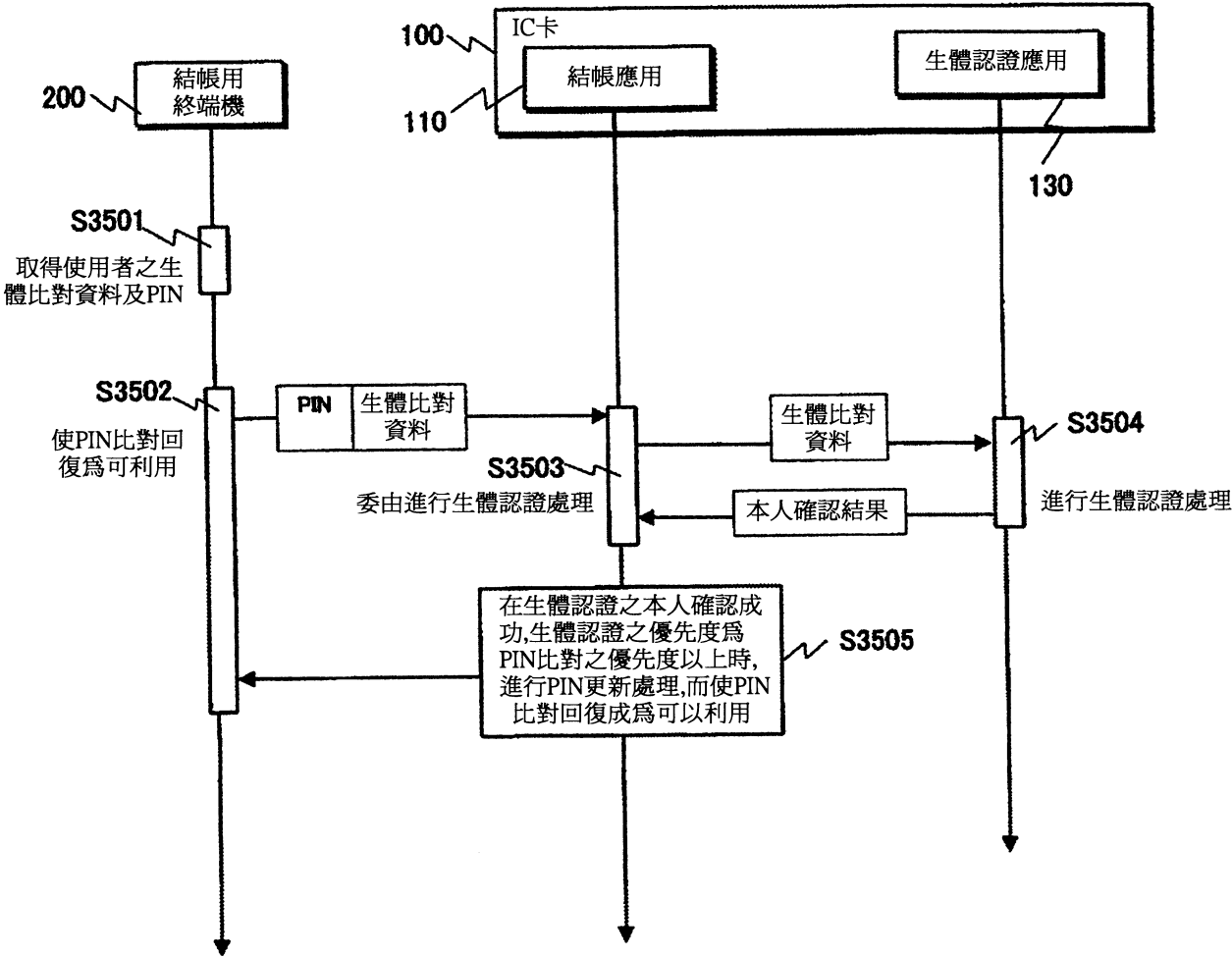


圖 10

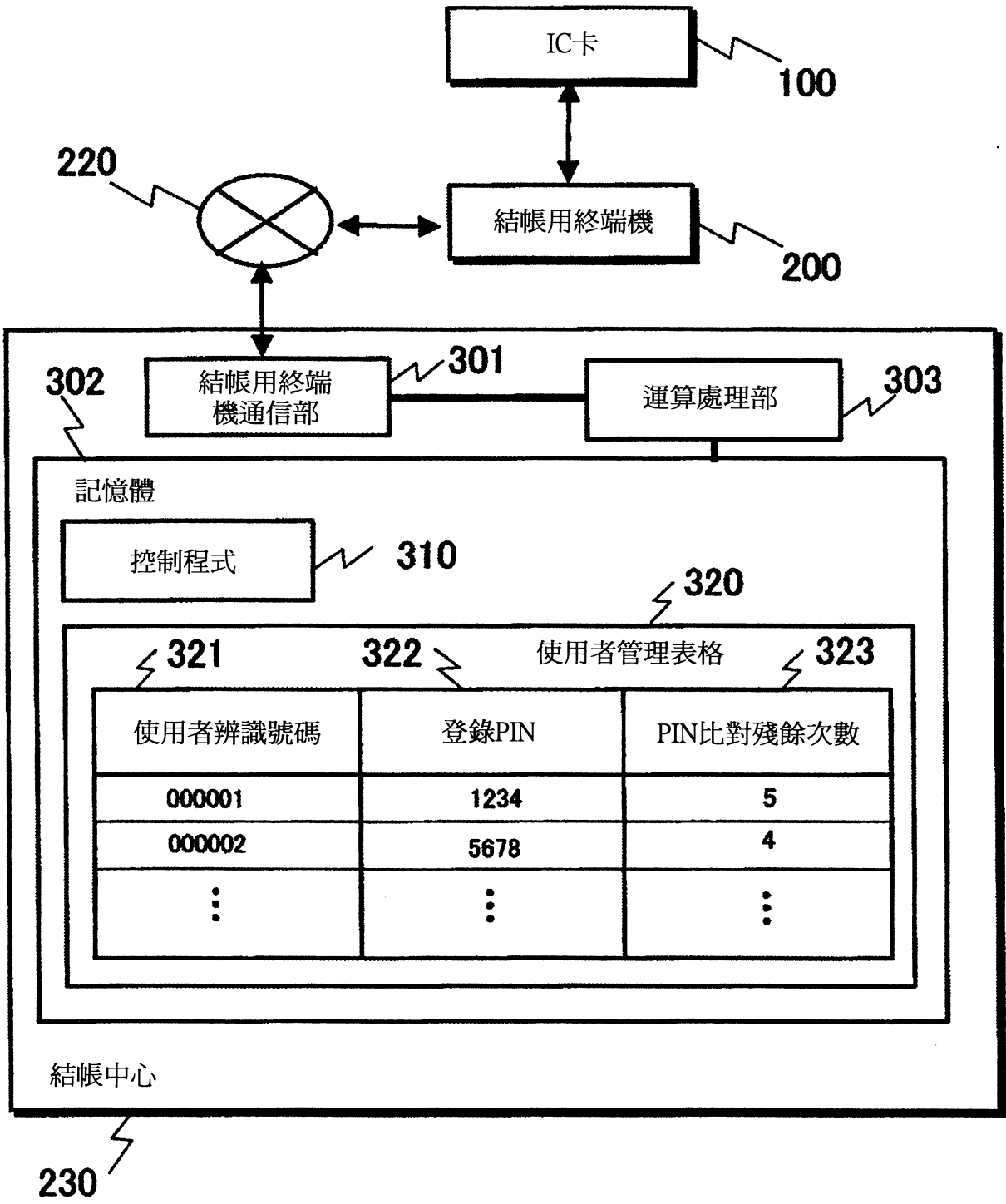
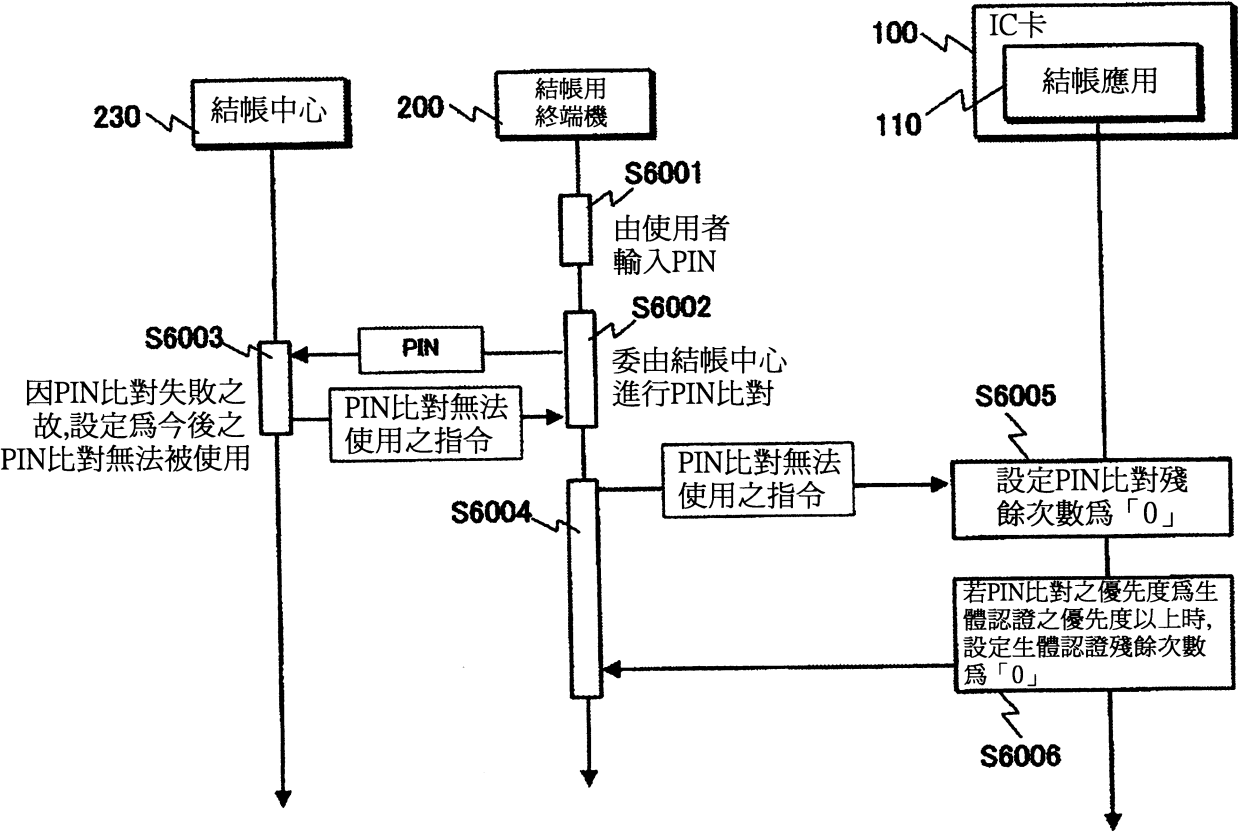


圖 11



七、指定代表圖：

(一)、本案指定代表圖為：第(1)圖

(二)、本代表圖之元件代表符號簡單說明：

100：IC卡；101：通信部；102：記憶體；
103：運算處理部；110：結帳應用；111：結帳 AID；
112：生體 AID 清單；113：結帳 AP 鍵；
114：生體 AP 雜湊值；115：本人確認方式清單；
116：本人確認方式優先度；117：登錄 PIN；
118：生體認證殘餘次數；119：PIN 比對殘餘次數；
120：本人確認結果；121：使用者辨識號碼；
130：生體認證應用；131：生體 AID；
132：生體登錄資料；133：結帳 AP 雜湊值；
140：作業系統；141：應用管理表格；
142：外部通信功能；143：應用追加刪除功能；
144：應用執行功能；145：應用間通信功能；
146：應用雜湊值產生功能；150：共用緩衝區；
200：結帳用終端機；201：IC卡通信部；
202：PIN輸入部；203：生體資訊感測器；
204：記憶體；205：中心通信部；206：使用者介面部；
207：運算處理部；210：結帳程式；220：網路；
230：結帳中心

八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：