

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：96116285

※申請日期：96年05月08日

※IPC分類：G06K9/00 (2006.01)

一、發明名稱：

(中) 生物認證裝置與生物認證系統以及 I C 卡片和生物認證方法
(英)

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 5 人)

1. 姓 名：(中) 相川慎
(英)
國 籍：(中) 日本
(英) JAPAN

2. 姓 名：(中) 畠中祥子
(英)
國 籍：(中) 日本
(英) JAPAN

3. 姓 名：(中) 橋本和則
(英)
國 籍：(中) 日本
(英) JAPAN

4. 姓 名：(中) 伊藤滋行
(英)
國 籍：(中) 日本

(英) JAPAN

5.姓 名：(中) 高見穰
(英)
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 ; 2006/06/05 ; 2006-155852 ☒ 有主張優先權

(英) JAPAN

5.姓 名：(中) 高見穰
(英)
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 ; 2006/06/05 ; 2006-155852 ☒ 有主張優先權

(1)

九、發明說明

【發明所屬之技術領域】

本發明，係特別有關於使用 IC 卡而進行以生物認證所致之本人確認的生物認證系統。

【先前技術】

先前，作為利用電腦等資訊機器而進行金融交易或是出入室管理時的本人確認之手段，一般係為採用對暗號或是密碼等之只有本人方能知悉的資訊作確認的方法。但是，暗號或是密碼，係有一旦被他人所得知，則他人即可容易地偽裝成本人的缺點。因此，在近年來，利用有指紋或是虹彩等之他人難以盜取且係為因人而異的生物資訊之生物認證係被注目。

作為利用有生物認證之個人確認方法，係有如下所述者。於專利文獻 1 中，係預先將本人之生物資訊保存於 IC 卡中（以下，將保存在 IC 卡中之生物資訊稱為「登錄資料」），並在本人確認時，將使用生物資訊感測器所取得之生物資訊（以下，稱為「對照資料」），輸入至 IC 卡中。而，IC 卡，係藉由於內部進行登錄資料與對照資料的對照處理，而確認其是否為本人。於此，由於在生物認證中係無法進行根據登錄資料與對照資料是否完全一致的二值判定，因此係使用特定之演算法來計算登錄資料與對照資料的類似度或不一致度，並藉由將計算結果與預先所設定之基準值（臨界值）作比較，而進行判定。

(2)

作為其中一例，於圖 18 中展示登錄資料與對照資料之不一致度的分布。在圖 18 中，橫軸係顯示對照之不一致度，而縱軸係顯示出現之頻度。又，顯示出當將本人之登錄資料與本人之對照資料相對照時之頻度曲線 901，以及將本人之登錄資料與他人之登錄資料相對照時的頻度曲線 902。通常，由於曲線 901 係成為較曲線 902 更靠左邊（不一致度小），因此藉由設定生物認證臨界值 903，而當不一致度較認證臨界值 903 為更小時，判斷係為本人，而當不一致度較認證臨界值 903 為更大時，判斷係為他人。

[專利文獻 1]日本特開 2001-344213 號公報

【發明內容】

[發明所欲解決之課題]

於此，如圖 18 所示，一般而言，頻度曲線 901 與頻度曲線 902 係具有重疊部，而就算是本人，若是不一致度係被包含於區域 910 內，則亦會被判定為他人。若是在被登錄於 IC 卡中之生物資訊的精確度並不佳的情況下，或是由於生物之經年變化、測定時之誤差等而使得被登錄在 IC 卡中之生物資訊與現在之生物資訊的不一致度變大的情況時，則就算是本人亦會被判定為他人之可能性便會變大。

例如，在將使用有 IC 卡之生物認證使用在金融卡或是信用卡等之金融交易時，若是發生此種現象，則會產生

(3)

雖然是本人但卻無法進行金融交易的問題。又，亦可想見有預先在 IC 卡中登錄生物認證之嘗試次數（表示就算生物認證失敗亦能反覆進行認證的可能次數），而若是生物認證失敗，則每一次失敗便在 IC 卡內將嘗試次數扣除 1 的方式。藉由此種構成，若是嘗試次數成為 0，則可想見會有 IC 卡之生物認證功能係成為無法利用，而使得其後之生物認證成為無法進行的情況。在被登錄於具備有此種功能之 IC 卡中的生物資訊與現在的生物資訊之不一致度變大時，則 IC 卡之生物認證功能係容易變為無法使用。

[用以解決課題之手段]

本發明，係為一種生物認證裝置，係為使用利用者之生物資訊而進行本人確認之生物認證裝置，並具備有：檢測出生物資訊之生物資訊感測器；和進行生物認證之演算處理部；和儲存資料之記憶體，其特徵為：前述記憶體，係儲存有當每次在前述演算處理部所進行之生物認證失敗時，使其值減少之殘餘嘗試次數，前述演算處理部，係產生為較生物認證開始時之殘餘嘗試次數更小之值的下限值，並實行生物認證，直到減少後之殘餘嘗試次數成為前述下限值以下為止，當減少後之殘餘嘗試次數為前述下限值以下時，作成對前述利用者進行警告之警告資料。

又，本發明，係為一種生物認證裝置，係為經由使用有利用者之生物認證資訊，來進行本人確認的生物認證裝置，其特徵為，具備有：儲存資料的記憶體；和進行生物

(4)

認證之演算處理部，前述記憶體，係儲存：前述利用者之第 1 生物資訊；和身為在以值之大小來判斷生物認證的成功與否時的基準值之生物認證臨界值；和身為在以值之大小來判斷前述利用者之第 1 生物資訊的變化檢測之有無時的基準值之變化檢測臨界值，前述演算處理部，係從外部取得前述利用者之第 2 生物資訊，並將前述第 1 生物資訊與所取得之第 2 生物資訊作比較，而計算出將兩者之相異以定量來作表示之不一致度，當所計算出之不一致度為較前述生物認證臨界值小且較前述變化檢測臨界值大的情況時，作成將對於第 1 生物資訊之變化檢測通知給前述利用者之通知資料。

而，本發明，係為一種生物認證裝置，其中，前述記憶體，係儲存：前述利用者之過去的生物認證之履歷；和身為在以值之大小來判斷前述利用者之第 1 生物資訊的經年變化檢測之有無時的基準值之經年變化檢測臨界值，前述演算處理部，係當所計算之不一致度為較前述經年變化臨界值更大時，作成將對於第 1 生物資訊之經年變化檢測通知給前述利用者之通知資料。

進而，本發明，係為一種生物認證系統，係具備有 IC 卡，和與該 IC 卡作通訊，經由使用利用者之生物資訊的生物認證，來進行本人確認的生物認證裝置，其特徵為：前述 IC 卡，係具備有：與前述生物認證裝置進行通訊之第 1 通訊部；和儲存資料之第 1 記憶體；和進行生物認證之第 1 演算處理部，前述第 1 記憶體，係儲存當每次

(5)

在前述第 1 演算處理部所進行之生物認證失敗時，使其值減少之殘餘嘗試次數，前述生物認證裝置，係具備有：與前述 IC 卡進行通訊之第 2 通訊部；和儲存資料之第 2 記憶體；和進行生物認證之第 2 演算處理部，該第 2 演算處理部，係產生為較生物認證開始時之殘餘嘗試次數更小之值的下限值，並實行生物認證，直到減少後之殘餘嘗試次數成為前述下限值以下為止，當減少後之殘餘嘗試次數為前述下限值以下時，作成對前述利用者進行警告之警告資料。

又，本發明，係為一種具備有 IC 卡、和與該 IC 卡進行通訊，而經由使用有利用者之生物資訊的生物認證，來進行本人確認之生物認證裝置的生物認證系統，其特徵為，前述 IC 卡，係具備有：與前述生物認證裝置進行通訊之第 1 通訊部；和儲存前述利用者之第 1 生物資訊之第 1 記憶體；和進行生物認證之第 1 演算處理部，該第 1 演算處理部，係從外部取得前述利用者之第 2 生物資訊，並將前述第 1 生物資訊與所取得之第 2 生物資訊作比較，而計算出將兩者之相異以定量來作表示之不一致度，前述生物認證裝置，係具備有：與前述 IC 卡進行通訊之第 2 通訊部；和儲存資料之第 2 記憶體；和進行生物認證之第 2 演算處理部，前述第 2 記憶體，係儲存：身為在以值之大小來判斷前述利用者之第 1 生物資訊的變化檢測之有無時的基準值之變化檢測臨界值，前述第 2 演算處理部，係取得前述 IC 卡所計算之不一致度，並將所取得之不一致

(6)

度與前述變化檢測臨界值作比較，當前述不一致度為較前述變化檢測臨界值更大時，作成將對於第 1 生物資訊之變化檢測通知給前述利用者之通知資料。

而，本發明，係為一種 IC 卡，係為經由使用有利用者之生物認證資訊，來進行本人確認的 IC 卡，其特徵為，具備有：與外部進行通訊之通訊部；和儲存相關於生物認證之資料的記憶體；和進行生物認證之演算處理部，前述記憶體，係儲存：前述利用者之第 1 生物資訊；和身為在以值之大小來判斷生物認證的成功與否時的基準值之生物認證臨界值；和身為在以值之大小來判斷前述利用者之第 1 生物資訊的變化檢測之有無時的基準值之變化檢測臨界值，前述演算處理部，係從外部取得前述利用者之第 2 生物資訊，並將前述第 1 生物資訊與所取得之第 2 生物資訊作比較，而計算出將兩者之相異以定量來作表示之不一致度，當所計算出之不一致度為較前述生物認證臨界值小且較前述變化檢測臨界值大的情況時，作成將對於第 1 生物資訊之變化檢測通知給前述利用者之通知資料。

進而，本發明，係為一種生物認證方法，係為使用 IC 卡與和該 IC 卡進行通訊之生物認證裝置，而藉由利用者之生物資訊來進行生物認證的生物認證方法，其特徵為：藉由前述 IC 卡，而記錄在每次生物認證失敗時減少其值之殘餘嘗試次數，並藉由前述生物認證裝置，而產生為較生物認證開始時之殘餘嘗試次數更小之值的下限值，並使生物認證成為可被實行，直到減少後之殘餘嘗試次數

(7)

成爲前述下限值以下爲止，當減少後之殘餘嘗試次數爲前述下限值以下時，作成對前述利用者進行警告之警告資料。

又，本發明，係爲一種生物認證方法，係爲使用 IC 卡、和與該 IC 卡作通訊之生物認證裝置，而藉由利用者之生物資訊來進行生物認證的生物認證方法，其特徵爲，藉由前述 IC 卡，記錄前述利用者之第 1 生物資訊，並從外部取得前述利用者之第 2 生物資訊，將前述第 1 生物資訊與所取得之第 2 生物資訊作比較，並計算將兩者之相異以定量來表示之不一致度，而藉由前述生物認證裝置，來儲存身爲在以值之大小來判斷前述利用者之第 1 生物資訊的變化檢測有無時的基準值之變化檢測臨界值，並取得前述 IC 卡所計算之不一致度，而將所取得之不一致度與前述經年變化檢測臨界值作比較，當前述不一致度爲較前述經年變化檢測臨界值大的情況時，檢測出相對於前述利用者的第 1 生物資訊之變化。

而，本發明，係爲一種生物認證方法，係爲使用 IC 卡，而藉由利用者之生物資訊來進行生物認證的生物認證方法，其特徵爲，藉由前述 IC 卡，記錄前述利用者之第 1 生物資訊；和身爲判斷生物認證之成功與否的基準值之生物認證臨界值；和身爲在以值之大小來判斷有無檢測出前述利用者之第 1 生物資訊的變化時的基準值之變化檢測臨界值，並從外部取得前述利用者之第 2 生物資訊，將前述第 1 生物資訊與所取得之第 2 生物資訊作比較，並計算

(8)

將兩者之相異以定量來表示之不一致度，若是該不一致度為較前述生物認證臨界值小且較前述變化檢測臨界值大，則檢測出相對於前述利用者的第 1 生物資訊之變化。

[發明之效果]

藉由使用本發明，則就算是在被登陸於 IC 卡中之生物資訊與現在的生物資訊間之不一致度變大，而使得就算係為本人，以生物認證所致之本人認證也成為失敗的情況中，亦能夠不使利用者的便利性降低，而提供適當的服務之 IC 卡、生物認證裝置、以及生物認證方法。

【實施方式】

對本發明之實施方式作說明。

針對本發明之生物認證裝置與生物認證系統以及 IC 卡還有生物認證方法之實施例，使用圖面來作說明。

[實施例 1]

對實施例 1 作說明。圖 1，係為展示本發明之第 1 實施例的構成之構成圖。於圖 1 中，100 係為 IC 卡，200 係為金融交易終端，300 係為網路，400 係為中心。IC 卡 100，係被金融交易終端 200 之使用者所保有，並為了安全的進行使用有生物認證之本人確認與金融交易處理而被使用。於此，在本實施例中，係使用現金卡或是信用卡等之金融卡片作為 IC 卡 100 之例來作說明，但是，並不限

(9)

定為金融交易處理，就算是將 IC 卡 100 所進行之生物認證，使用於出入室或是網路利用之存取（access）管理時的情況，亦包含於本發明的適用範圍之內。又，雖係以使用有現金卡或是信用卡而進行金融交易之例如窗口終端或是 ATM（自動現金存款裝置）等的金融交易終端 200 作為例子而說明，但是，並不限定於金融交易處理，只要是使用 IC 卡 100 而進行生物認證處理的終端，則均包含於本發明的適用範圍內。同時，就算是不間斷地將金融交易終端 200 與 IC 卡 100 作連接並成為可作通訊的一體型之構成，亦被包含於本發明的適用範圍之內。又，IC 卡 100，並非限定為通常之 IC 卡的形狀，就算是記憶卡或是系統 LSI 等之硬體，亦包含於本發明之適用範圍。例如，亦可為具備有 IC 卡之功能的 IC 晶片、系統 LSI 等。故而，亦可為與具備有 IC 卡之功能的 IC 晶片、系統 LSI 等相連接，並成為一體化的行動終端。此種情況下之所謂連接，係指互相具備有接點者、相接觸者、直接被固定於基板等，而流動有電性訊號者，或者是，亦包含有以電磁感應、無線等之非接觸式所致者。

接下來，針對 IC 卡 100 之內部構成作說明。IC 卡 100，係具備有：通訊部 101、和程式儲存記憶體 102、和不揮發性資料儲存記憶體 103、和揮發性資料儲存記憶體 104、和演算處理部 105。通訊部 101，係用於使 IC 卡 100 與外部作通訊，而可考慮有例如根據身為國際標準規格之 ISO/IEC7816 所規定的接觸通訊。或者是，亦可考

慮採用身為國際標準規格之 ISO / IEC 14443 所規定的非接觸通訊。或是，就算是根據其他之規格來進行通訊的情況，亦係包含於本發明之適用範圍內。程式儲存記憶體 102，係具有將 IC 卡 100 所保持之程式永久性地作儲存的功能，而係由例如 ROM (Read Only Memory) 或是 EEPROM (Electrical Erasable Programmable Read Only Memory) 等之不揮發性半導體記憶體所構成。不揮發性資料儲存記憶體 103，係為就算是對 IC 卡之電力供給被中斷，亦會繼續對任意之資料作保持的記憶體，而係為由 EEPROM 等之不揮發性半導體記憶體所構成。揮發性資料儲存記憶體 104，係為儲存有就算是一旦對 IC 卡之電力供給被中斷即會被消除亦為無妨之一時的資料之記憶體，而係為由 RAM (Random Access Memory) 等之揮發性半導體記憶體所構成。演算處理部，係負責對 IC 卡 100 全體之控制，若是經由通訊部 101 而受訊有控制指令，則根據被儲存於程式儲存記憶體 102 之程式，來進行因應於所受訊之控制指令的處理，並實行將相對應之回應 (response) 經由通訊部 101 來送訊至外部的處理。

接下來，針對金融交易終端 200 之內部構成作說明。金融交易終端 200，係具備有：IC 卡通訊部 201、和程式儲存記憶體 202、和不揮發性資料儲存記憶體 203、和揮發性資料儲存記憶體 204、和生物資訊感測器 205、和使用者界面部 206、和中心通訊部 207、和演算處理部 208。IC 卡通訊部 201，係用於對 IC 卡 100 作控制，而可

考慮有例如根據身為國際標準規格之 ISO/IEC7816 所規定的接觸通訊。或者是，亦可考慮採用身為國際標準規格之 ISO/IEC14443 所規定的非接觸通訊。或是，就算是根據其他之規格來進行通訊的情況，亦係包含於本發明之適用範圍內。程式儲存記憶體 102，係具有將金融交易終端 200 所保持之程式永久性地作儲存的功能，而係由例如硬碟或是半導體記憶體等所構成。不揮發性資料儲存記憶體 203，係具有將金融交易終端 200 所使用之永久性的資料作儲存的功能，而係由例如硬碟或是半導體記憶體等所構成。揮發性資料儲存記憶體 204，係具有將金融交易終端 200 所使用之暫時性的資料作儲存的功能，而係由例如硬碟或是半導體記憶體等所構成。生物資訊感測器 205，係具備有對利用者之生物資訊作讀取的功能。在本實施例中，作為生物資訊，雖係想定為對指紋圖案或是指靜脈圖案作讀取的情況，但是，就算是對其他之生物資訊作讀取的情況，亦包含於本發明之適用範圍內。使用者界面部 206，係具備有：用以對於金融交易終端 200 之利用者，輸出畫像或文字等之視覺資訊或是聲音資訊並作提示的顯示功能；和使 IC 卡決算終端 300 之利用者能夠輸入必要之資訊的輸入功能。作為顯示功能，係可考慮使用映像管顯示器或是液晶顯示器。作為輸入功能，係可考慮使用鍵盤或是觸控是面板。中心通訊部 207，係為用以與中心 400 作通訊，而具備有能與例如電話或是網際網路等之公眾線路網或是專用線路網之網路 300 作連接的功能。演算

(12)

處理部 208，係負責金融交易終端 200 全體之控制，並實施使用有 IC 卡 100 之生物認證處理，和使用有 IC 卡 100 之金融交易處理。

接下來，針對 IC 卡 100 所保持之程式以及資料的構成，使用圖 2 來作說明。於圖 2 中，係詳細展示有被儲存於 IC 卡 100 之程式儲存記憶體 102 中之程式、被儲存於不揮發性資料儲存記憶體 103 中之資料、以及被儲存於揮發性資料儲存記憶體 104 中之資料的詳細內容。首先，在程式儲存記憶體 102 中，係被儲存有：生物認證程式 121、和金融交易程式 122、和 IC 卡作業系統 123。生物認證程式 121，係為用以實行使用有 IC 卡 100 之生物認證處理的應用程式。金融交易程式 122，係為用以實行使用有 IC 卡 100 之金融交易處理的應用程式。IC 卡作業系統 123，係為提供在實行生物認證程式 121 和金融交易程式 122 時所必要之基本功能的系統程式。作為 IC 卡作業系統 123，例如係可考慮採用 MULTOS（商標）。或者是，就算係使用其他之作業系統，亦包含於本發明之適用範圍內。

在不揮發性資料儲存記憶體 103 中，係被儲存有：生物認證程式管理不揮發性資料 130，和金融交易程式管理不揮發性資料 140。生物認證程式管理不揮發性資料 130，係為生物認證程式 121 所管理之不揮發性資料，並以無法從其他之程式來作存取的方式，經由 IC 卡作業系統 123 而被管理。同樣的，金融交易程式管理不揮發性資

料 140，係為金融交易程式 122 所管理之不揮發性資料，並以無法從其他之程式來作存取的方式，經由 IC 卡作業系統 123 而被管理。

在揮發性資料儲存記憶體 104 中，係被儲存有：生物認證程式管理揮發性資料 150，和金融交易程式管理揮發性資料 160。生物認證程式管理揮發性資料 150，係為生物認證程式 121 所管理之揮發性資料，並以無法從其他之程式來作存取的方式，經由 IC 卡作業系統 123 而被管理。同樣的，金融交易程式管理揮發性資料 160，係為金融交易程式 122 所管理之揮發性資料，並以無法從其他之程式來作存取的方式，經由 IC 卡作業系統 123 而被管理。

接下來，針對構成生物認證程式管理不揮發性資料 130 之資料作說明。在生物認證程式管理不揮發性資料 130 中，係包含有：暗號金鑰資料 131、和生物資訊登錄資料 132、和生物資訊相關資料 133、和生物認證臨界值 134、和使用者的資訊 135、和生物認證履歷 136、和嘗試次數上限值 137、殘餘嘗試次數 138。暗號金鑰資料 131，係為用以在 IC 卡 100 與金融交易終端 200 之間，進行機器認證以及暗號通訊的金鑰資料。在本實施例中，暗號金鑰資料 131，係可為 DES 或 AES 之類的共通鍵暗號方式之金鑰資料，亦可為 RSA 或橢圓曲線之類的公開鍵暗號方式的資料。生物資訊登錄資料 132，係為在將 IC 卡 100 使用於金融交易前，利用者在金融機關之專用窗口

等處所登錄在 IC 卡 100 中之利用者本人的生物資訊，並以不會洩漏至 IC 卡 100 之外部的方式而被管理。在本實施例中，作為生物資訊登錄資料 132，雖係想定為對指紋圖案或是指靜脈圖案作處理的情況，但是，就算是對其他之生物資訊作處理的情況，亦包含於本發明之適用範圍內。又，在圖 2 中，雖係僅存在有 1 個的生物資訊登錄資料 132，但是，就算是在 IC 卡 100 中被登錄有複數之生物資訊登錄資料的情況，亦包含於本發明之適用範圍內。生物資訊相關資料 133，係為生物資訊登錄資料 132 之附屬資訊，在將對生物資訊登錄資料 132 作登錄的同時，被登錄於 IC 卡 100 內。

生物資訊相關資料 133，例如係為顯示被作為生物資訊登錄資料 132 而被保持的指紋圖案之中心座標值。生物資訊相關資料 133，係為可從 IC 卡 100 所讀出的資料，並被使用於將金融交易終端 200 在生物認證處理中所使用的生物資訊對照資料以高精確度來產生之。生物認證臨界值 134，係為從生物認證登錄資料 132 與生物資訊對照資料 151 所算出之不一致度的基準值，若是不一致度為較生物認證臨界值小，則判定生物認證登錄資料 132 與生物資訊對照資料 151 係為同一人物之生物資訊。使用者資訊 135，係為相關於將生物資訊登錄資料 132 作登錄的人之資訊，而包含有姓名或是金融交易用之帳戶號碼之類的資訊。使用者資訊 135，係可考慮在與登錄生物資訊登錄資料 132 之相同時間點，來登錄於 IC 卡 100 內。生物認證

履歷 136，係為過去所進行之生物認證的履歷資料，而包含有：生物認證係為成功或是失敗之類的資訊，或是從生物認證登錄資料與生物認證對照資料所算出之不一致度之類的資訊。嘗試次數上限值 137，係為顯示使用 IC 卡 100 所實行之生物認證處理的最大失敗次數。殘餘嘗試次數 138，係為顯示使用 IC 卡 100 所實行之生物認證處理的尚可容許之失敗次數。殘餘嘗試次數 138，最初係被設定為與嘗試次數上限值相同的值，並在每一次之生物認證失敗時被減去 1。藉由此，若是殘餘嘗試次數 138 之值成為 0，則 IC 卡 100 係成為能夠以不對其後之生物認證處理作許可的方式來作控制。

接下來，針對構成生物認證程式管理揮發性資料 150 之資料作說明。在構成生物認證程式管理揮發性資料之資料 150 中，係包含有生物資訊對照資料 151、和不一致度 152、和生物認證結果 153。生物資訊對照資料 151，係為從金融交易終端 200 所取得之利用者的對照資料。不一致度 152，係為將生物資訊登錄資料 133 與生物資訊對照資料 152 之差異以定量來作表示者，係在 IC 卡 100 之內部，根據特定之演算法來計算。生物認證結果 153，係為將不一致度 152 與生物認證臨界值 134 作比較後之結果，而表示是否經由生物認證而能確認利用者係為本人。

接下來，針對金融交易終端 200 所保持之程式以及資料的構成，使用圖 3 來作說明。於圖 3 中，係詳細展示有被儲存於金融交易終端 200 之程式儲存記憶體 202 中之程

式、被儲存於不揮發性資料儲存記憶體 203 中之資料、以及被儲存於揮發性資料儲存記憶體 204 中之資料的詳細內容。首先，在程式儲存記憶體 202 中，係被儲存有：生物認證程式 221、和金融交易程式 222、和金融交易終端作業系統 223。生物認證程式 221，係為用以控制 IC 卡 100 而實行生物認證處理的應用程式。金融交易程式 222，係為用以控制 IC 卡 100 而實行金融交易處理的應用程式。金融交易終端作業系統 223，係為提供在安裝生物認證程式 221 和金融交易程式 222 時所必要之基本功能的系統程式。在本實施例中，作為金融交易終端作業系統 223，係可使用任意種類的作業系統。

在不揮發性資料儲存記憶體 203 中，係被儲存有：暗號金鑰資料 231、和經年變化檢測臨界值 232、和第 1 利用限度額 233、和第 2 利用限度額 234。暗號金鑰資料 231，係為用以在 IC 卡 100 與金融交易終端 200 之間，進行機器認證以及暗號通訊的金鑰資料。在本實施例中，暗號金鑰資料 231，係可為 DES 或 AES 之類的共通金鑰暗號方式之金鑰資料，亦可為 RSA 或橢圓曲線之類的公開金鑰暗號方式的金鑰資料。經年變化檢測臨界值 232，係為用以檢測出：被登錄於 IC 卡 100 之生物資訊登錄資料 133，是否由於經年之變化等的理由，而變得與現在之利用者的生物資訊有很大差異的基準值。第 1 利用限度額 233，係為表示當生物認證成功時在金融交易中所可利用之金額的上限。第 2 利用限度額 234，係為表示當生物認

證不成功時在金融交易所可利用之金額的上限。

在揮發性資料儲存記憶體 204 中，係包含有：使用者資訊 241、和生物資訊相關資料 242、和生物資訊對照資料 243、和生物認證結果 244、和不一致度 245、和生物認證履歷 246、和殘餘嘗試次數 247、和經年變化檢測結果 248、和嘗試次數下限值 249。使用者資訊 241，係為將保持於 IC 卡 100 中之使用者資訊 135，從 IC 卡 100 所讀取出者。生物資訊相關資料 242，係為將保持於 IC 卡 100 中之生物資訊相關資料 132，從 IC 卡 100 所讀取出者。生物認證結果 244，係為將 IC 卡 100 在生物認證處理中所產生之生物認證結果 153，從 IC 卡 100 所取得者。不一致度 245，係為將 IC 卡 100 在生物認證處理中所產生之不一致度 152，從 IC 卡 100 所取得者。

生物認證履歷 246，係為將保持於 IC 卡 100 中之生物認證履歷 136，從 IC 卡 100 所讀取出者。殘餘嘗試次數 247，係為將 IC 卡 100 所保持之殘餘嘗試次數 138，從 IC 卡 100 所取得者。經年變化檢測結果 248，係為儲存：被登錄於 IC 卡 100 之生物資訊登錄資料 133，是否被檢測出為變得與現在之利用者的生物資訊有很大差異的結果。嘗試次數下限值 249，係為當金融交易終端 200 與 IC 卡 100 通訊時所產生之值。

接下來，針對 IC 卡 100 所實行之生物認證的處理流程之其中一例，使用圖 4 來作說明。首先，開始處理，並判斷 IC 卡 100 之殘餘嘗試次數 138 是否在 0 以下

(18)

[S2000]，若是殘餘嘗試次數為 0 以下，則前進至步驟 S2004。

若是殘餘嘗試次數不為 0 以下，則 IC 卡 100，係將 IC 卡 100 所預先保持之生物資訊登錄資料 132，與從金融交易終端 200 所取得之生物資訊對照資料 151，使用圖案比對等之演算法來作比較，並計算不一致度 [S2001]。於此，不一致度 152 之計算，係不論是使用何種之演算法，均包含於本發明之適用範圍內。接下來，IC 卡 100，係將在步驟 S2001 中所計算之不一致度 152 與與生物認證臨界值 134 作比較 [S2002]，若是不一致度 152 並不小於生物認證臨界值 134，則 IC 卡 100 係將殘餘嘗試次數 138 減去 1 [S2003]，而 IC 卡 100 係將生物認證結果 153 設定為「失敗」 [S2004]。若是不一致度 152 為較生物認證臨界值 134 更小，則 IC 卡 100 係將生物認證結果 153 設定為「成功」 [S2005]。

接下來，針對金融交易終端 200 所實行之經年變化檢測的處理流程之其中一例，使用圖 5 來作說明。開始處理，金融交易終端 200，係將從 IC 卡 100 所取得之不一致度 245 與經年變化檢測臨界值 232 作比較 [S3000]，若是不一致度 245 為較經年變化檢測臨界值 232 大，則金融交易終端 200，係將經年變化檢測結果 248 設定為「有經年變化」 [S3001]。若是不一致度 245 並不為較經年變化檢測臨界值 232 更大，則金融交易終端 200 係將經年變化檢測結果 248 設定為「無經年變化」 [S3002]。

於此，在圖 5 中係藉由將不一致度 245 與經年變化檢測臨界值 232 作比較，而進行經年變化之檢測，但是，就算是未發生有經年變化，若是不一致度變為較經年變化檢測臨界值 232 更大，則會有被判定為「有經年變化」的可能性。例如，亦可考慮有：當因為外部環境等之影響，而使得以生物資訊感測器 205 所致之利用者的生物資訊對照資料之取得並未被正常實行，而使不一致度 245 成為較通常為大的情況。為了盡可能的減低此種可能性，亦可參考從 IC 卡 100 所取得之生物認證履歷 246，以提升經年變化檢測之精確性。例如，可考慮：若是被包含於生物認證履歷 246 中之過去的不一致度，亦成為較經年變化檢測臨界值 232 大，則判定為「有經年變化」。

接下來，針對在 IC 卡 100 與金融交易終端 200 之間進行送收訊的指令以及回應之其中一例作說明。圖 6 (a)、(b)，係為應用程式選擇指令 500 與應用程式選擇回應 501 之格式圖。應用程式選擇指令 500，係為為了對被儲存在 IC 卡 100 內之應用程式作選擇，而從金融交易終端 200 對 IC 卡 100 所送訊的指令，並被儲存有：用以識別本指令之指令碼、和參數、和指令資料長度、和用以識別應用程式之程式識別子、和回應資料長度。應用程式選擇回應 501，係為將 IC 卡 100 對應用程式選擇指令 500 作處理的結果回送至金融交易終端 200 的回應，而被儲存有：程式相關資訊，和回應碼。

圖 7 (a)、(b) 係為機器認證開始指令 510 與機器

認證開始回應 511 之格式圖。機器認證開始指令 510，係為為了開始機器認證，而從金融交易終端 200 對 IC 卡 100 所送訊的指令，並被儲存有：用以識別本指令之指令碼、和參數、和指令資料長度、和終端亂數、和回應資料長度。機器認證開始回應 511，係為將 IC 卡 100 對機器認證開始指令 510 作處理的結果回送至金融交易終端 200 的回應，而被儲存有：卡片檢証資料，和回應碼。

圖 8 (a) 、 (b) 係為機器認證實行指令 520 與機器認證實行回應 521 之格式圖。機器認證實行指令 520，係為為了實行機器認證，而從金融交易終端 200 對 IC 卡 100 所送訊的指令，並被儲存有：用以識別本指令之指令碼、和參數、和指令資料長度、和終端檢証資料。機器認證實行回應 521，係為將 IC 卡 100 對機器認證實行指令 520 作處理的結果回送至金融交易終端 200 的回應，而被儲存有：回應碼。

圖 9 (a) 、 (b) ，係為使用者資訊讀取指令 530 與使用者資訊讀取回應 531 之格式圖。使用者資訊讀取指令 530，係為金融交易終端 200 為了將使用者資訊從 IC 卡 100 中讀取出，而對 IC 卡 100 所送訊的指令，並被儲存有：用以識別本指令之指令碼、和參數、和回應資料長度。使用者資訊讀取回應 531，係為將 IC 卡 100 對使用者資訊讀取指令 530 作處理的結果回送至金融交易終端 200 的回應，而被儲存有：使用者資訊，和回應碼。

圖 10 (a) 、 (b) ，係為生物資訊相關資料讀取指

(21)

令 540 與生物資訊相關資料讀取回應 541 之格式圖。生物資訊相關資料讀取指令 540，係為金融交易終端 200 為了讀取出被儲存在 IC 卡 100 中的生物資訊相關資料，而對 IC 卡 100 所送訊的指令，並被儲存有：用以識別本指令之指令碼、和參數、和回應資料長度。生物資訊相關資料讀取回應 541，係為將 IC 卡 100 對生物資訊相關資料讀取指令 540 作處理的結果回送至金融交易終端 200 的回應，而被儲存有：生物資訊相關資料，和回應碼。

圖 11 (a) 、 (b) 係為生物認證履歷讀取指令 550 與生物認證履歷讀取回應 551 之格式圖。生物認證履歷讀取指令 550，係為金融交易終端 200 為了讀取出被儲存在 IC 卡 100 中的生物認證履歷，而對 IC 卡 100 所送訊的指令，並被儲存有：用以識別本指令之指令碼、和參數、和回應資料長度。生物認證履歷讀取回應 541，係為將 IC 卡 100 對物認證履歷讀取指令 540 作處理的結果回送至金融交易終端 200 的回應，而被儲存有：生物認證履歷，和回應碼。

圖 12 (a) 、 (b) 係為生物認證實行指令 560 與生物認證實行回應 561 之格式圖。生物認證實行指令 560，係為為了實行生物認證，而從金融交易終端 200 對 IC 卡 100 所送訊的指令，並被儲存有：用以識別本指令之指令碼、和參數、和指令資料長度、和生物資訊對照資料。生物認證實行回應 561，係為將 IC 卡 100 對生物認證實行指令 560 作處理的結果回送至金融交易終端 200 的回應，

而被儲存有：生物認證結果、和不一致度、和殘餘嘗試次數、和回應碼。

接下來，針對在 IC 卡 100 與金融交易終端 200 之間的處理流程，使用圖 13 來作說明。於圖 13 所示之處理流程，係成為從 IC 卡 100 與金融交易終端 200 已成為可相互通訊的狀態起的處理流程。首先，金融交易終端 200 係為了選擇 IC 卡 100 之生物認證程式 121 的啟動，而送訊被設定有生物認證程式 121 之程式識別碼的應用程式選擇指令 500[S1000]。IC 卡 100，若是接收有被設定了生物認證程式 121 之程式識別碼的應用程式選擇指令 500，則係選擇生物認證程式 121 之啟動，並回送應用程式選擇回應 501[S1100]。接下來，金融交易終端 200，係將機器認證開始指令 510 以及機器認證實行指令 520，送訊至 IC 卡 100，並進行與 IC 卡 100 間之機器認證 [S1001]。IC 卡 100，係藉由接收有機器認證開始指令 510 以及機器認證實行指令 520，而進行機器認證，並回送機器認證開始回應 511 以及機器認證實行回應 521[S1101]。機器認證處理，係藉由進行使用有 IC 卡 100 所保持之暗號金鑰資料 131 和金融交易終端 200 所保持之暗號金鑰資料 231 的暗號處理，而相互確認對方係為正當的機器。進而，亦可藉由進行機器認證，而對用以將在之後的 IC 卡通訊中所送收訊的資料作編碼化之金鑰資料作共同保有。在本發明中，對於使用於機器認證中之編碼演算法、以及金鑰資料之共有演算法，係並不作特定，不論使用何種之演算法，

均為在本發明之適用範圍內。

接下來，金融交易終端 200，係送訊使用者資訊讀取指令 530，並取得 IC 卡 100 所保持之使用者資訊 135[S1002]。IC 卡 100，若是收訊到使用者資訊讀取指令 530，則讀取出設定有使用者資訊 135 之使用者資訊，並回送回應 531[S1102]。藉由此，金融交易終端 200 係將從 IC 卡 100 所取得之使用者資訊，作為使用者資訊 241 而暫時保存。

金融交易終端 200，係送訊生物資訊相關資料讀取指令 540，並取得 IC 卡 100 所保持之生物資訊相關資料 133[S1003]。IC 卡 100，若是收訊有生物資訊相關資料讀取指令 540，則將被設定有生物資訊相關資料 133 之生物資訊相關資料讀取出，並回送生物資訊相關資料讀取回應 541[S1103]。藉由此，金融交易終端 200 係將從 IC 卡 100 所取得之生物資訊相關資料，作為生物資訊相關資料 242 而暫時保存。

金融交易終端 200，係將生物認證履歷讀取指令 550 送訊至 IC 卡 100，並取得 IC 卡 100 所保持之生物認證履歷 136[S1004]。IC 卡 100，若是收訊有生物認證履歷讀取指令 550，則讀取出被設定有生物認證履歷 136 之認證履歷，並回送回應 551[S1104]。藉由此，金融交易終端 200，係將從 IC 卡 100 所取得之生物認證履歷，作為生物認證履歷 246 而作暫時保存。

金融交易終端 200，係使用生物資訊感測器 205，而

(24)

讀取利用者之生物資訊，並產生生物資訊對照資料 243[S1005]。金融交易終端 200，爲了高精確度地產生生物資訊對照資料 243，係亦可事先參考從 IC 卡 100 所讀取出之生物資訊相關資料 242。接下來，金融交易終端 200，係將設定有在步驟 S1005 中所產生之生物資訊對照資料 243 的生物認證實行指令 560，送訊至 IC 卡 100 並實行生物認證處理[S1006]。IC 卡 100，若是收訊有生物認證實行指令 560，則係將生物資訊對照資料，作爲生物資訊對照資料 152 而暫時保存，並計算出不一致度 152 與生物認證結果 153。不一致度 152 與生物認證結果 153 之計算方法，係已使用圖 4 而作了說明。而後，IC 卡 100，係將設定有不一致度 152 和生物認證結果 153 和殘餘嘗試次數 138 之生物認證實行回應 561 回送至金融交易終端 200。金融交易終端 200 係將被設定於生物認證實行回應 561 中的生物認證結果和不一致度與殘餘嘗試次數，分別作爲生物認證結果 244 和不一致度 245 以及殘餘嘗試次數 247 而暫時作保存[S1106]。

金融交易終端 200，係判定生物認證結果 244 的本人確認係爲成功或是失敗[S1007]，若是本人確認係爲成功，則前進至步驟 S1012。若是本人確認失敗，則前進至步驟 S1008 中，而金融交易終端 200，當嘗試次數下限值在步驟 S1000 之實行後爲尙未被產生時，則將嘗試次數下限值 249，在 1 以上且未滿殘餘嘗試次數 247 的範圍內作隨機產生[S1008]。接下來，金融交易終端 200，係判斷殘

(25)

餘嘗試次數 247 是否在嘗試次數下限值 249 以下 [S1009]，若是殘餘嘗試次數 247 為嘗試次數下限值 249 以下，則前進至步驟 S1011。若是殘餘嘗試次數 247 超過嘗試次數 249，則金融交易終端 200，係確認利用者是否要再度進行生物認證所致的本人確認 [S1010]。對利用者之確認，係使用金融交易終端 200 之使用者界面部 206 所提供的顯示功能與輸入功能。在步驟 S1010 中，若是利用者承諾再度進行生物認證，則前進至步驟 S1005，而若是利用者拒絕再度進行生物認證，則金融交易終端 200，係與利用者確認是否可將金融交易之使用額度降低 [S1011]。對利用者之確認，係使用金融交易終端 200 之使用者界面部 206 所提供的顯示功能與輸入功能。

若是利用者判斷降低使用額度也沒關係，則前進至步驟 S1013。如果利用者並不願意，則前進至 S1015。

在步驟 S1012 中，金融交易終端 200，係進行經年變化的檢測處理。關於經年變化之檢測處理的詳細內容，係已使用圖 5 而作了說明。而，當經年變化檢測結果係成為「檢測有經年變化」時，則使用金融交易終端 200 之使用者界面部 206 所提供的顯示功能與輸入功能，而對利用者提出警告。而後，前進至步驟 S1013。

在步驟 S1013 中，金融交易終端 200 係為了選擇 IC 卡 100 之金融交易程式 122 的啓動，而送訊被設定有金融交易程式 122 之程式識別碼的應用程式選擇指令 500。IC 卡 100，若是接收有被設定了金融交易程式 122 之程式識

別碼的應用程式選擇指令 500，則係選擇金融交易程式 122 之啟動，並回送應用程式選擇回應 501[S1113]。接下來，IC 卡 100 與金融交易終端 200，係在作為之前所實施的生物認證結果而被設定之使用額度的範圍內，進行金融交易處理[S1014、S1114]。

金融交易終端 200，係在步驟 S1011 中，當利用者拒絕金融交易之使用額度的降低時，使用金融交易終端 200 之使用者界面 206 所提供之顯示功能與輸入功能，對利用者顯示不可進行金融交易的事態[S1015]。

最後，金融交易終端 200，係將生物認證結果與金融交易結果，通知至中心 300[S1016]。中心 300，係保持過去之利用者的生物認證之履歷。

接下來，於圖 14，展示在金融交易終端 200 之使用者界面 206 所顯示之畫面的其中一例。圖 14，係為當進行了生物認證所致的本人確認後，其結果係在成功地作了本人確認的同時，亦檢測出有經年變化的情況時之畫面的遷移。首先，在畫面 700 中，金融交易終端 200，係為了進行生物認證，而顯示有用以將利用者之手指導引至金融交易終端 200 之生物資訊感測器 205 並放置的文章、聲音、圖形。接下來，在畫面 701 中，金融交易終端 200，係顯示用以告知利用者目前係正在進行生物認證的文章、聲音、圖形。接下來，在畫面 702 中，金融交易終端 200，係顯示用以告知利用者使用有生物認證之本人確認係為成功的文章、聲音、圖形。接下來，在畫面 703 中，

金融交易終端 200，係在顯示畫面 702 之後，在金融交易中，或者是結束了金融交易時，將：由於被登錄在 IC 卡 100 之生物資訊登錄資料 133，係因為經年變化等之理由，而與現在的利用者之生物資訊有很大的差異一事，通知給利用者，並顯示將利用者導引至金融機構之窗口的文章、聲音、圖形。

接下來，作為在金融交易終端 200 之使用者界面部 206 所顯示之畫面的其他例子，於圖 15 中，展示當進行了生物認證所致的本人確認後，其結果本人確認係為失敗的情況時之畫面的遷移。首先，在畫面 710 中，金融交易終端 200，係為了進行生物認證，而顯示有用以將利用者之手指導引至金融交易終端 200 之生物資訊感測器 205 並放置的文章、聲音、圖形。接下來，在畫面 711 中，金融交易終端 200，係顯示用以告知利用者目前係正在進行生物認證的文章、聲音、圖形。接下來，在畫面 712 中，金融交易終端 200，係顯示：當生物認證失敗，且在圖 13 之步驟 S1009 中，殘餘嘗試次數 247 並非為嘗試次數下限值 249 以下的情況時，由於本人確認係為失敗，因此確認是否要再度進行生物認證所致的本人確認的畫面。若是利用者選擇再度進行本人確認，則金融交易終端 200 係顯示畫面 710 並再度進行生物認證。若是利用者選擇不再進行本人確認，則金融交易終端 200 係顯示畫面 713。接下來，在畫面 713 中，金融交易終端 200，係顯示：當生物認證失敗，且在圖 13 之步驟 S1009 中，殘餘嘗試次數

247 為嘗試次數下限值 249 以下的情況時，由於生物認證所致之本人確認係為失敗，因此確認是否可以將其後之金融交易的使用額度降低的畫面。接下來，在畫面 714 中，金融交易終端 200，係在金融交易中，或者是結束了金融交易時，由於被登錄在 IC 卡 100 之生物資訊登錄資料 133，係因為經年變化等之理由，而與現在的利用者之生物資訊有很大的差異，因此以將利用者導引至金融機構之窗口的的方式，而顯示文章、聲音、圖形。

圖 14 以及圖 15 所展示之畫面，係為其中一例，就算是能得到相同效果之顯示文章或圖形的畫面構成，則亦包含於本發明之適用範圍內。

[實施例 2]

針對本發明之第 2 實施例，使用圖面來作說明。本實施例，雖係成為與在實施例 1 中使用圖 1 所說明的構成圖為相同構成，但是 IC 卡 100 所保持的內部資料的一部份係為相異。圖 16，係為 IC 卡 100 所保持之程式以及資料的構成圖。實施例 2，係在 IC 卡 100 之生物認證程式管理不揮發性資料 130 中，保持有經年變化檢測臨界值 139，此點係與實施例 1 相異。

接下來，針對在實施例 2 中之 IC 卡 100 所實行之生物認證的處理流程之其中一例，使用圖 17 來作說明。首先，開始處理，並判斷 IC 卡 100 之殘餘嘗試次數 138 是否在 0 以下[S4000]，若是殘餘嘗試次數 138 為 0 以下，

則前進至步驟 S4004。若是殘餘嘗試次數 138 超過 0，則 IC 卡 100，係將 IC 卡 100 所預先保持之生物資訊登錄資料 132，與從金融交易終端 200 所取得之生物資訊對照資料 151，使用特定之演算法來作比較，並計算不一致度 152[S4001]。於此，不一致度 152 之計算，係不論是使用何種之演算法，均包含於本發明之適用範圍內。接下來，IC 卡 100，係將在步驟 S2001 中所計算之不一致度 152 與生物認證臨界值 134 作比較[S4002]，若是不一致度 152 並不小於生物認證臨界值 134，則 IC 卡 100 係將殘餘嘗試次數 138 減去 1[S4003]。接下來，IC 卡 100 係將生物認證結果 153 設定為「失敗」[S4003]。

在步驟 S4002 中，若是不一致度 152 為較生物認證臨界值 134 小，則 IC 卡 100，係將不一致度 245 與經年變化檢測臨界值 139 作比較，若是不一致度 245 為較經年變化檢測臨界值 139 大，則 IC 卡 100，係將生物認證結果 153 設定為「生物認證成功，有經年變化」[S4006]。

在步驟 S4005 中，若是不一致度 152 並不為較經年變化檢測臨界值 139 更大，則 IC 卡 100，係將生物認證結果 153 設定為「生物認證成功，無經年變化」[S4007]。

以上，雖係使用圖 17 而針對 IC 卡 100 所實行之生物認證的處理流程作了說明，但是當在步驟 S4006 中被判斷為「生物認證成功，有經年變化」的情況時，亦可將生物資訊登錄資料 132 更新為生物資訊對照資料 151。在此情況下，於之後的生物認證中，生物資訊對照資料 151，係

成爲代替生物資訊登錄資料 132 而被作爲登錄資料來被參考。或者是，亦可將生物資訊對照資料 151 作爲新的登錄資料，而永遠的保存於 IC 卡 100 中。在此情況下，於之後的生物認證中，除了生物資訊登錄資料 132 之外，生物資訊對照資料 151，亦成爲被作爲登錄資料來被參考。

【圖式簡單說明】

[圖 1]實施例 1 中之生物認證系統的構成圖。

[圖 2]IC 卡 100 所保持之程式以及資料的構成圖。

[圖 3]金融交易終端 200 所保持之程式以及資料的構成圖。

[圖 4]IC 卡 100 所實行之生物認證的處理流程圖。

[圖 5]金融交易終端 200 所實行之經年變化檢測的處理流程圖。

[圖 6]應用程式選擇指令 500 與應用程式選擇回應 501 之格式圖。

[圖 7]機器認證開始指令 510 與機器認證開始回應 511 之格式圖。

[圖 8]機器認證實行指令 520 與機器認證實行回應 521 之格式圖。

[圖 9]使用者資訊讀取指令 530 與使用者資訊讀取回應 531 之格式圖。

[圖 10]生物資訊相關資料讀取指令 540 與生物資訊相關資料讀取回應 541 之格式圖。

(31)

[圖 11]生物認證履歷讀取指令 550 與生物認證履歷讀取回應 551 之格式圖。

[圖 12]生物認證實行指令 560 與生物認證實行回應 561 之格式圖。

[圖 13]IC 卡 100 與金融交易終端 200 間之處理流程圖。

[圖 14]金融交易終端 200 所顯示之畫面變遷的一例（其之 1）之說明圖。

[圖 15]金融交易終端 200 所顯示之畫面變遷的一例（其之 2）之說明圖。

[圖 16]在實施例 2 中之 IC 卡 100 所保持之程式以及資料的構成圖。

[圖 17]在實施例 2 中之 IC 卡 100 所實行之生物認證的處理流程圖。

[圖 18]登錄資料與對照資料之不一致度的分布圖。

【主要元件對照表】

- 10：手指
- 100：IC 卡
- 101：通訊部
- 102：程式儲存記憶體
- 103：不揮發性資料儲存記憶體
- 104：揮發性資料儲存記憶體
- 105：演算處理部
- 121：生物認證程式

(32)

- 122：金融交易程式
- 123：IC卡作業系統
- 130：生物認證程式管理不揮發性資料
- 131：暗號金鑰資料
- 132：生物資訊登錄資料
- 133：生物資訊相關資料
- 134：生物認證臨界值
- 135：使用者資訊
- 136：生物認證履歷
- 137：嘗試次數上限值
- 138：殘餘嘗試次數
- 140：金融交易程式管理不揮發性資料
- 150：生物認證程式管理揮發性資料
- 151：生物資訊對照資料
- 152：不一致度
- 153：生物認證結果
- 160：金融交易程式管理揮發性資料
- 200：金融交易終端
- 201：IC卡通訊部
- 202：程式儲存記憶體
- 203：非揮發性資料儲存記憶體
- 204：揮發性資料儲存記憶體
- 205：生物資訊感測器
- 206：使用者介面部

(33)

207：中心通訊部

208：演算處理部

221：生物認證程式

222：金融交易程式

223：金融交易終端作業系統

231：暗號金鑰資料

232：經年變化檢測臨界值

233：第1利用限度額

234：第2利用限度額

241：使用者資訊

242：生物資訊相關資料

243：生物資訊對照資料

244：生物認證結果

245：不一致度

246：生物認證履歷

247：殘餘嘗試次數

248：經年變化檢測結果

249：嘗試次數下限值

300：網路

400：中心

500：應用程式選擇指令

501：應用程式選擇回應

510：機器認證開始指令

511：機器認證開始回應

(34)

520：機器認證實行指令
521：機器認證實行回應
530：使用者資訊讀取指令
531：使用者資訊讀取回應
540：生物資訊相關資料讀取指令
541：生物資訊相關資料讀取回應
550：生物認證履歷讀取指令
551：生物認證履歷讀取回應
560：生物認證實行指令
561：生物認證實行回應
700：畫面
701：畫面
702：畫面
703：畫面
710：畫面
711：畫面
712：畫面
713：畫面
714：畫面
901：頻度曲線
902：頻度曲線
903：生物認證臨界值
910：區域
920：區域

五、中文發明摘要

發明之名稱：生物認證裝置與生物認證系統以及 IC 卡片和生物認證方法

[課題]提供一種：在就算是因為登錄於 IC 卡之生物資訊與現在的生物資訊之不一致度變大，而使得即使是本人，生物認證所致之本人確認也成為失敗的情況下，亦能不使利用者之便利性降低，而能提供適當之服務的 IC 卡、生物認證裝置、以及生物認證方法。

[解決手段]一種使用利用者之生物資訊而進行本人確認之生物認證裝置 200，並具備有：儲存資料之記憶體 203、204；和進行生物認證之演算處理部 208，其特徵為：記憶體 203、204，係儲存有當每次生物認證失敗時使其值減少之殘餘嘗試次數，演算處理部 208，係產生為較生物認證開始時之殘餘嘗試次數更小之值的下限值，並使生物認證成為可實行，直到減少後之殘餘嘗試次數成為下限值以下為止，當減少後之殘餘嘗試次數為前述下限值以下時，作成對前述利用者進行警告之警告資料。

六、英文發明摘要

發明之名稱：

(1)

十、申請專利範圍

1. 一種生物認證裝置，係為使用利用者之生物資訊而進行本人確認之生物認證裝置，並具備有：

檢測出生物資訊之生物資訊感測器；和

進行生物認證之演算處理部；和

儲存資料之記憶體，

其特徵為：

前述記憶體，係儲存有當每次在前述演算處理部所進行之生物認證失敗時，使其值減少之殘餘嘗試次數，

前述演算處理部，係產生為較生物認證開始時之殘餘嘗試次數更小之值的下限值，並實行生物認證，直到減少後之殘餘嘗試次數成為前述下限值以下為止，

當減少後之殘餘嘗試次數為前述下限值以下時，作成對前述利用者進行警告之警告資料。

2. 如申請專利範圍第 1 項所記載之生物認證裝置，其中，前述記憶體，係儲存：前述利用者之第 1 生物資訊；和身為在以值之大小來判斷前述利用者之生物認證的成功與否時的基準值之生物認證臨界值；和身為在以值之大小來判斷有無檢測出前述利用者之第 1 生物資訊的變化時的基準值之變化檢測臨界值，

前述演算處理部，係取得前述利用者之第 2 生物資訊，並將前述第 1 生物資訊與所取得之第 2 生物資訊作比較，而計算出將兩者之相異以定量來作表示之不一致度，當所計算出之不一致度為較前述生物認證臨界值小且較前

(2)

述變化檢測臨界值大的情況時，作成將對於第 1 生物資訊之變化檢測通知給前述利用者之通知資料。

3. 如申請專利範圍第 1 項所記載之生物認證裝置，其中，前述記憶體，係儲存：前述利用者之過去的生物認證之履歷；和身為在以值之大小來判斷前述利用者之第 1 生物資訊的經年變化檢測之有無時的基準值之經年變化檢測臨界值，

前述演算處理部，係當所計算之不一致度為較前述經年變化臨界值更大時，作成將對於第 1 生物資訊之經年變化檢測通知給前述利用者之通知資料。

4. 如申請專利範圍第 1 項所記載之生物認證裝置，其中，在前述演算處理部所演算之生物資訊，係為相關於指紋的資訊，或是相關於指靜脈的資訊。

5. 一種生物認證系統，係具備有：

IC 卡；和

與該 IC 卡通訊，並經由使用利用者之生物資訊的生物認證，來進行本人確認的生物認證裝置，

其特徵為：

前述 IC 卡，係具備有：與前述生物認證裝置進行通訊之第 1 通訊部；和儲存資料之第 1 記憶體；和進行生物認證之第 1 演算處理部，前述第 1 記憶體，係儲存當每次在前述第 1 演算處理部所進行之生物認證失敗時，使其值減少之殘餘嘗試次數，

前述生物認證裝置，係具備有：與前述 IC 卡進行通

(3)

訊之第 2 通訊部；和進行生物認證之第 2 演算處理部，該第 2 演算處理部，係產生為較生物認證開始時之殘餘嘗試次數更小之值的下限值，並可實行生物認證，直到減少後之殘餘嘗試次數成為前述下限值以下為止，當減少後之殘餘嘗試次數為前述下限值以下時，作成對前述利用者進行警告之警告資料。

6. 如申請專利範圍第 5 項所記載之生物認證系統，其中，

前述 IC 卡，係具備有：與前述生物認證裝置進行通訊之第 1 通訊部；和儲存前述利用者之第 1 生物資訊的第 1 記憶體；和進行生物認證之第 1 演算處理部，該第 1 演算處理部，係從外部取得前述利用者之第 2 生物資訊，並將前述第 1 生物資訊與所取得之第 2 生物資訊作比較，而計算出將兩者之相異以定量來作表示之不一致度，

前述生物認證裝置，係具備有：與前述 IC 卡進行通訊之第 2 通訊部；和儲存資料之第 2 記憶體；和進行生物認證之第 2 演算處理部，前述第 2 記憶體，係儲存：身為在以值之大小來判斷前述利用者之第 1 生物資訊的變化檢測之有無時的基準值之變化檢測臨界值，前述第 2 演算處理部，係取得前述 IC 卡所計算之不一致度，並將所取得之不一致度與前述變化檢測臨界值作比較，當前述不一致度為較前述變化檢測臨界值更大時，作成將對於第 1 生物資訊之變化檢測通知給前述利用者之通知資料。

7. 一種 IC 卡，係為經由使用有利用者之生物資訊的

(4)

生物認證，來進行本人確認的 IC 卡，其特徵為，具備有：

與外部進行通訊之通訊部；和儲存相關於生物認證之資料的記憶體；和進行生物認證之演算處理部，

前述記憶體，係儲存：前述利用者之第 1 生物資訊；和身為在以值之大小來判斷生物認證的成功與否時的基準值之生物認證臨界值；和身為在以值之大小來判斷前述利用者之第 1 生物資訊的變化檢測之有無時的基準值之變化檢測臨界值，

前述演算處理部，係從外部取得前述利用者之第 2 生物資訊，並將前述第 1 生物資訊與所取得之第 2 生物資訊作比較，而計算出將兩者之相異以定量來作表示之不一致度，當所計算出之不一致度為較前述生物認證臨界值小且較前述變化檢測臨界值大的情況時，作成將對於第 1 生物資訊之變化檢測通知給前述利用者之通知資料。

8. 一種具備有 IC 卡之功能的 IC 晶片，係為具備有經由使用有利用者之生物資訊之生物認證，來進行本人確認的 IC 卡之功能的 IC 晶片，其特徵為，具備有：

與外部進行通訊之通訊部；和儲存相關於生物認證之資料的記憶體；和進行生物認證之演算處理部，

前述記憶體，係儲存：前述利用者之第 1 生物資訊；和身為在以值之大小來判斷生物認證的成功與否時的基準值之生物認證臨界值；和身為在以值之大小來判斷前述利用者之第 1 生物資訊的變化檢測之有無時的基準值之變化

(5)

檢測臨界值，

前述演算處理部，係從外部取得前述利用者之第 2 生物資訊，並將前述第 1 生物資訊與所取得之第 2 生物資訊作比較，而計算出將兩者之相異以定量來作表示之不一致度，當所計算出之不一致度為較前述生物認證臨界值小且較前述變化檢測臨界值大的情況時，作成將對於第 1 生物資訊之變化檢測通知給前述利用者之通知資料。

9. 一種生物認證方法，係為使用 IC 卡與和該 IC 卡進行通訊之生物認證裝置，而藉由利用者之生物資訊來進行生物認證的生物認證方法，其特徵為：

藉由前述 IC 卡，而記錄在每次生物認證失敗時減少其值之殘餘嘗試次數，並藉由前述生物認證裝置，而產生為較生物認證開始時之殘餘嘗試次數更小之值的下限值，並使生物認證成為可被實行，直到減少後之殘餘嘗試次數成為前述下限值以下為止，當減少後之殘餘嘗試次數為前述下限值以下時，作成對前述利用者進行警告之警告資料。

10. 如申請專利範圍第 9 項所記載之生物認證方法，其中，藉由前述 IC 卡，記錄前述利用者之第 1 生物資訊，並從外部取得前述利用者之第 2 生物資訊，將前述第 1 生物資訊與所取得之第 2 生物資訊作比較，並計算將兩者之相異以定量來表示之不一致度，而藉由前述生物認證裝置，來儲存身為在以值之大小來判斷前述利用者之第 1 生物資訊的變化檢測有無時的基準值之變化檢測臨界值，

(6)

並取得前述 IC 卡所計算之不一致度，而將所取得之不一致度與前述經年變化檢測臨界值作比較，當前述不一致度為較前述經年變化檢測臨界值大的情況時，檢測出相對於前述利用者的第 1 生物資訊之變化。

11. 如申請專利範圍第 9 項所記載之生物認證方法，其中，藉由前述 IC 卡，記錄前述利用者之第 1 生物資訊；和身為判斷生物認證之成功與否的基準值之生物認證臨界值；和身為檢測出前述利用者之生物資訊的變化的基準值之變化檢測臨界值，並從外部取得前述利用者之第 2 生物資訊，將前述第 1 生物資訊與所取得之第 2 生物資訊作比較，並計算將兩者之相異以定量來表示之不一致度，若是該不一致度為較前述生物認證臨界值小且較前述變化檢測臨界值大，則檢測出相對於前述利用者的第 1 生物資訊之變化。

圖 1

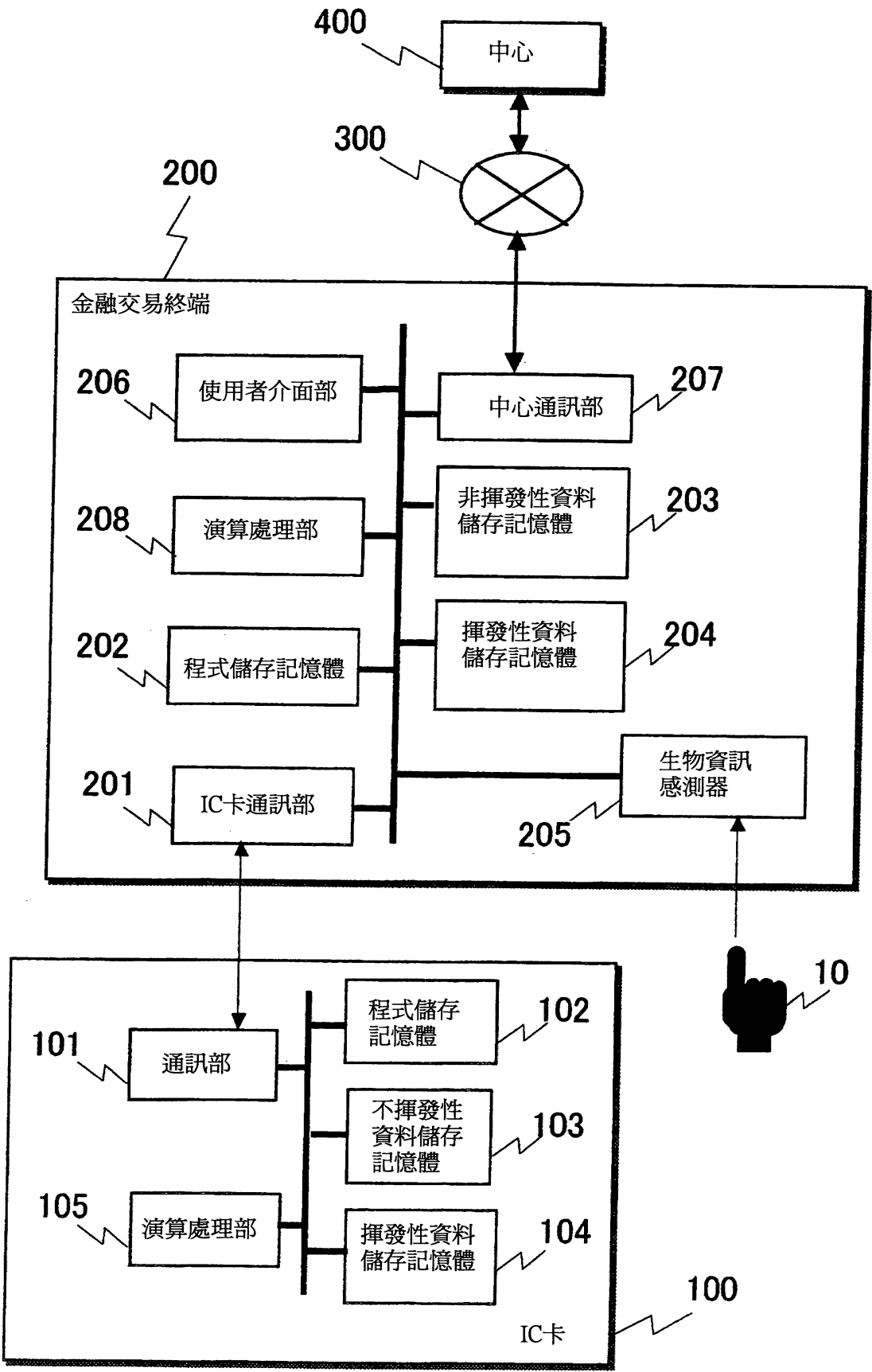


圖2

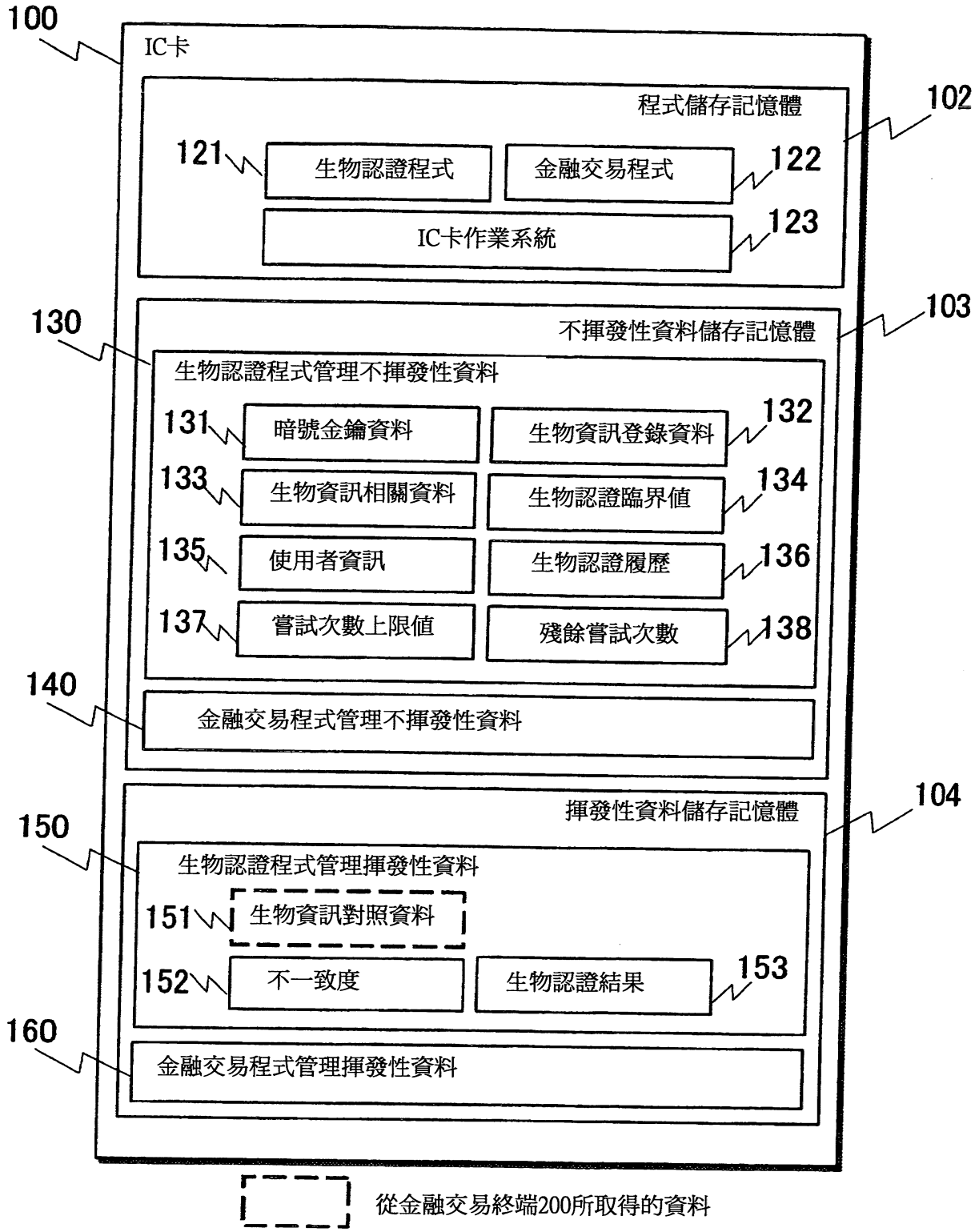


圖3

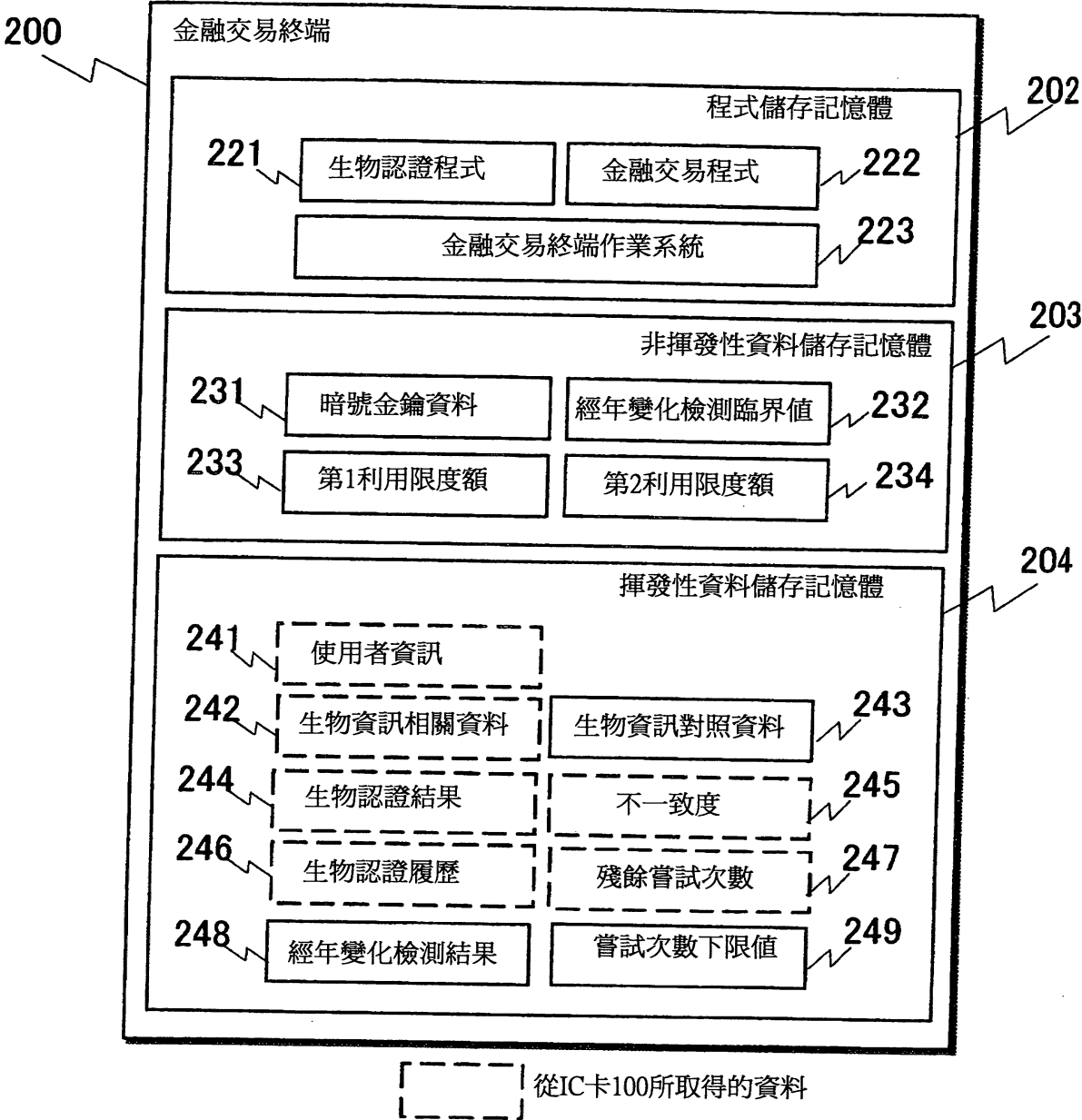


圖4

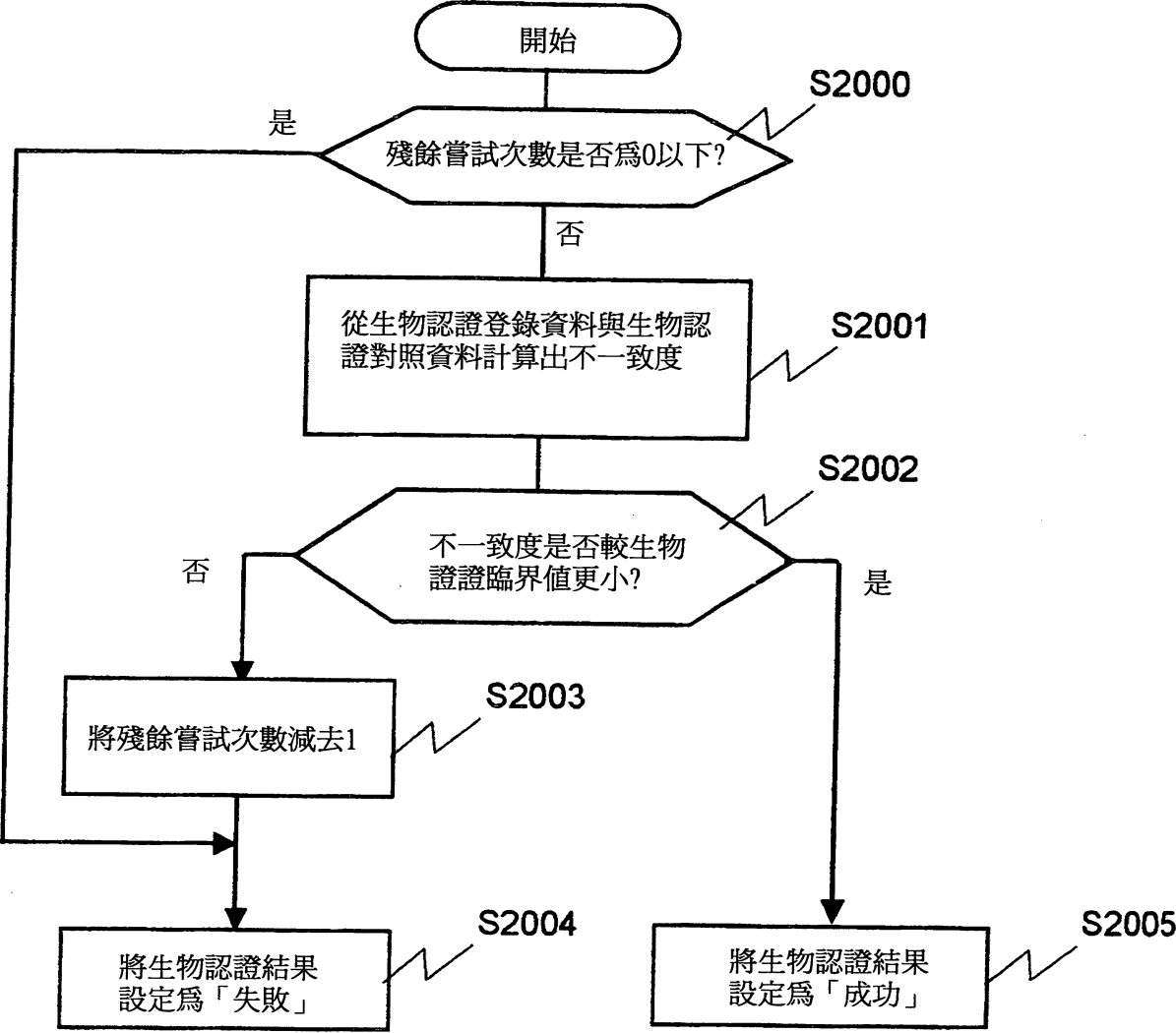


圖5

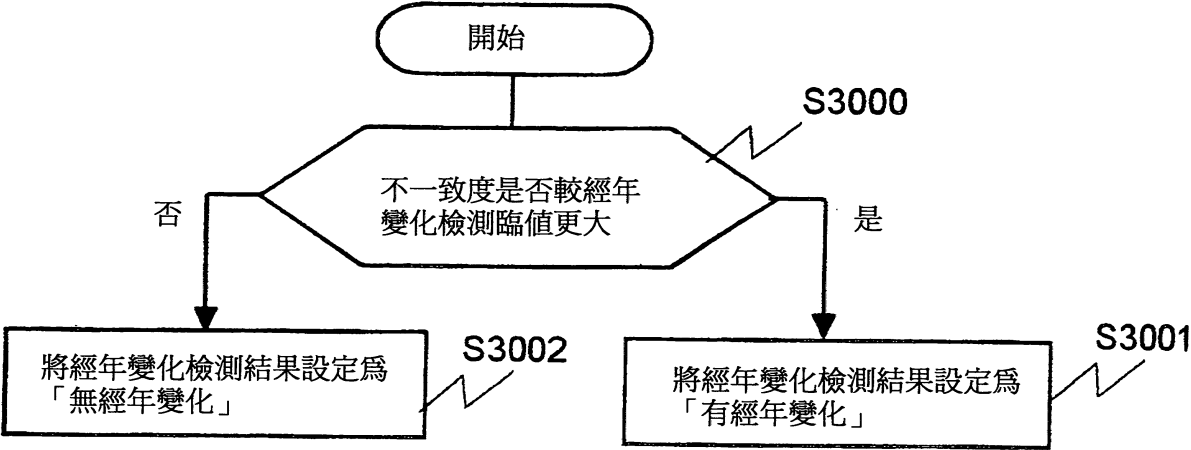


圖 6

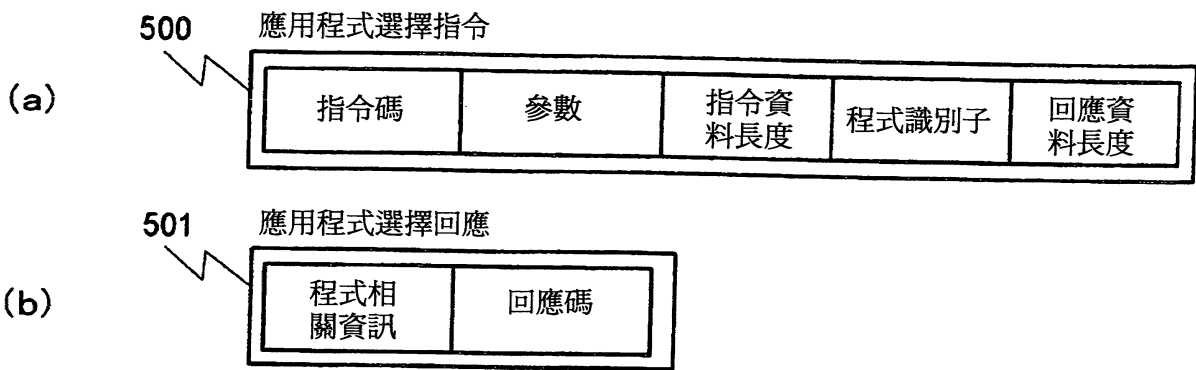


圖 7

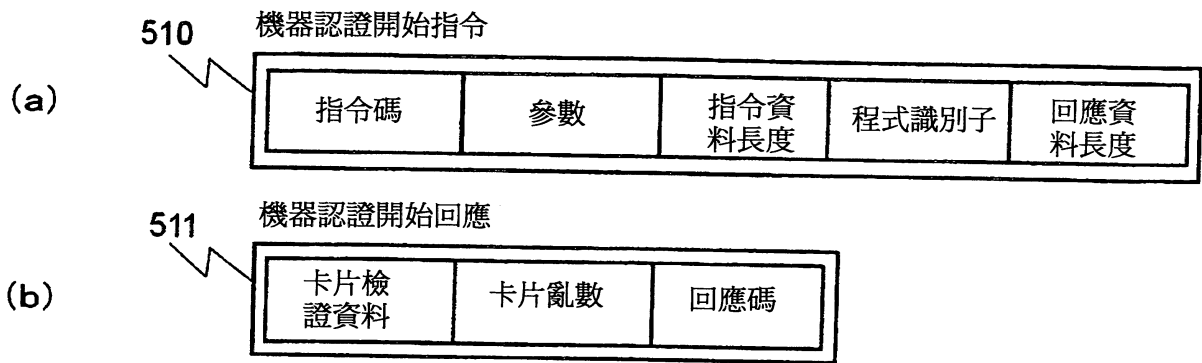


圖 8

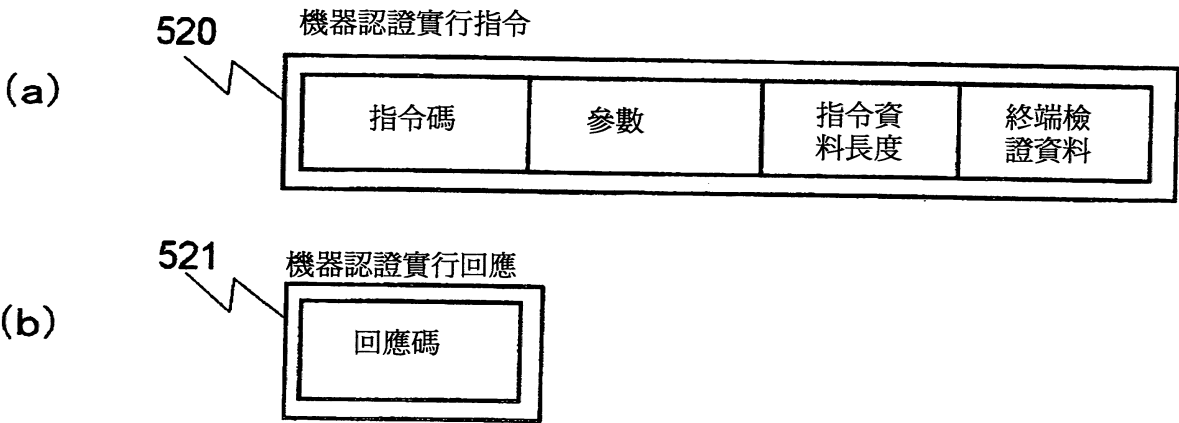


圖 9

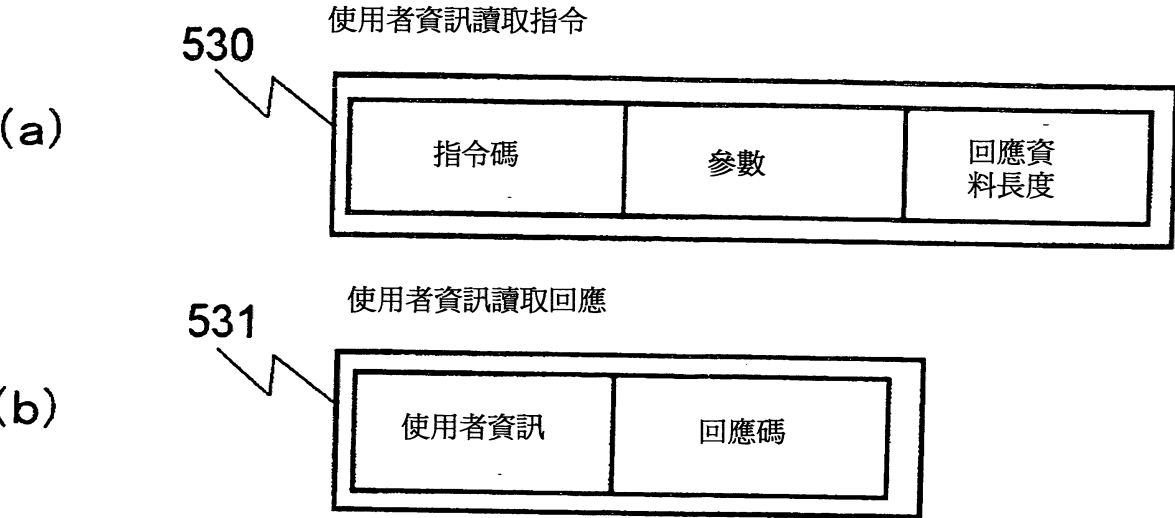


圖 10

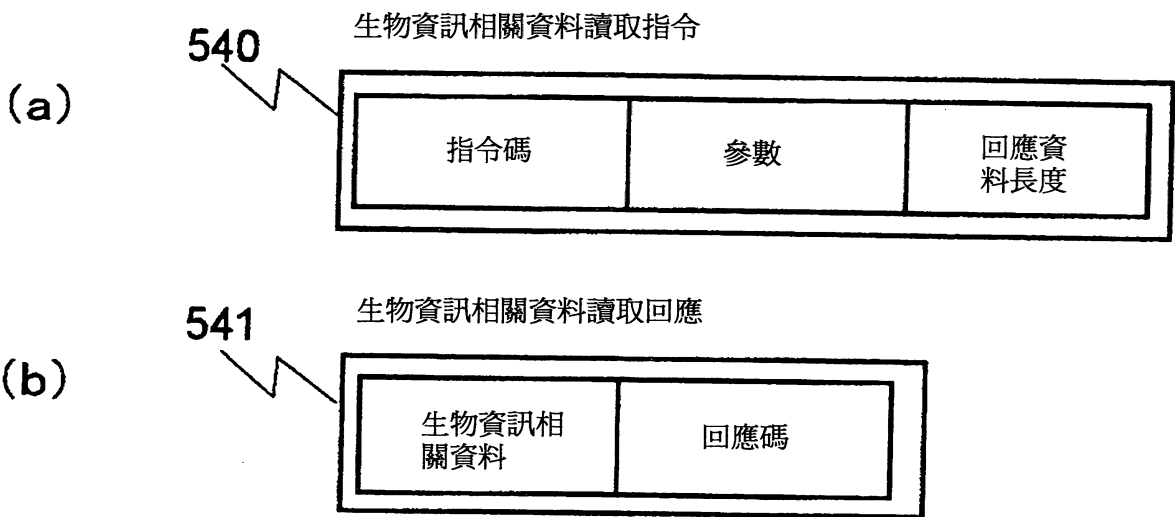


圖 11

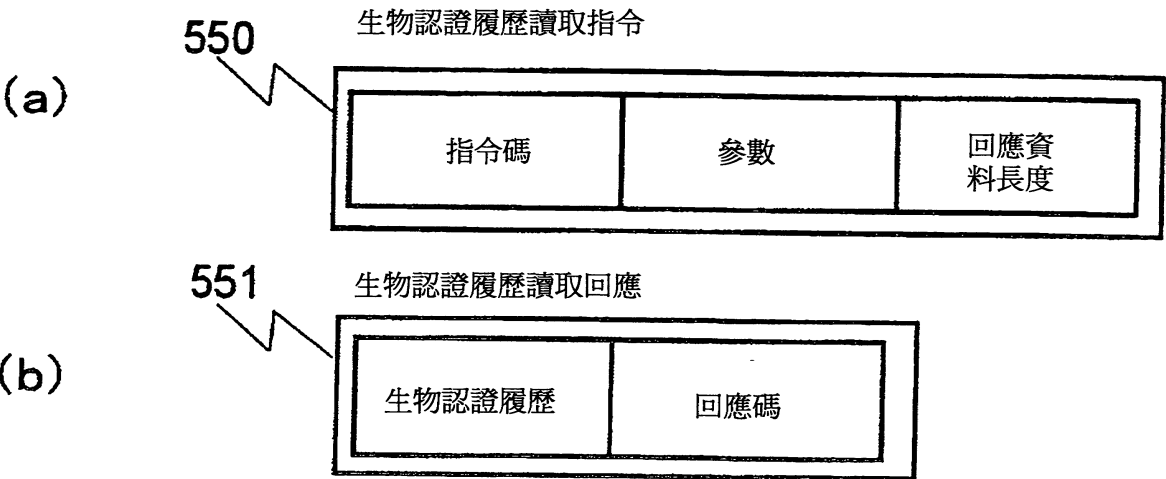
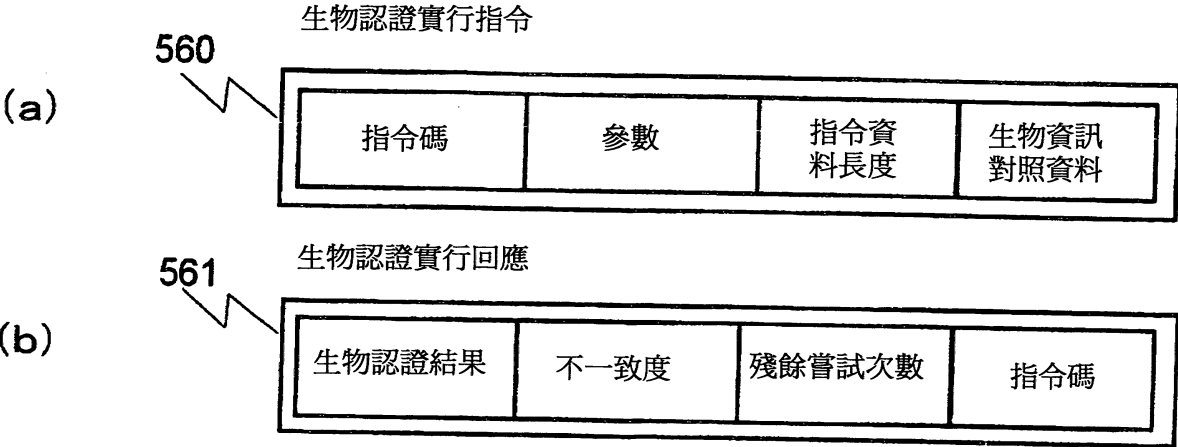


圖 12



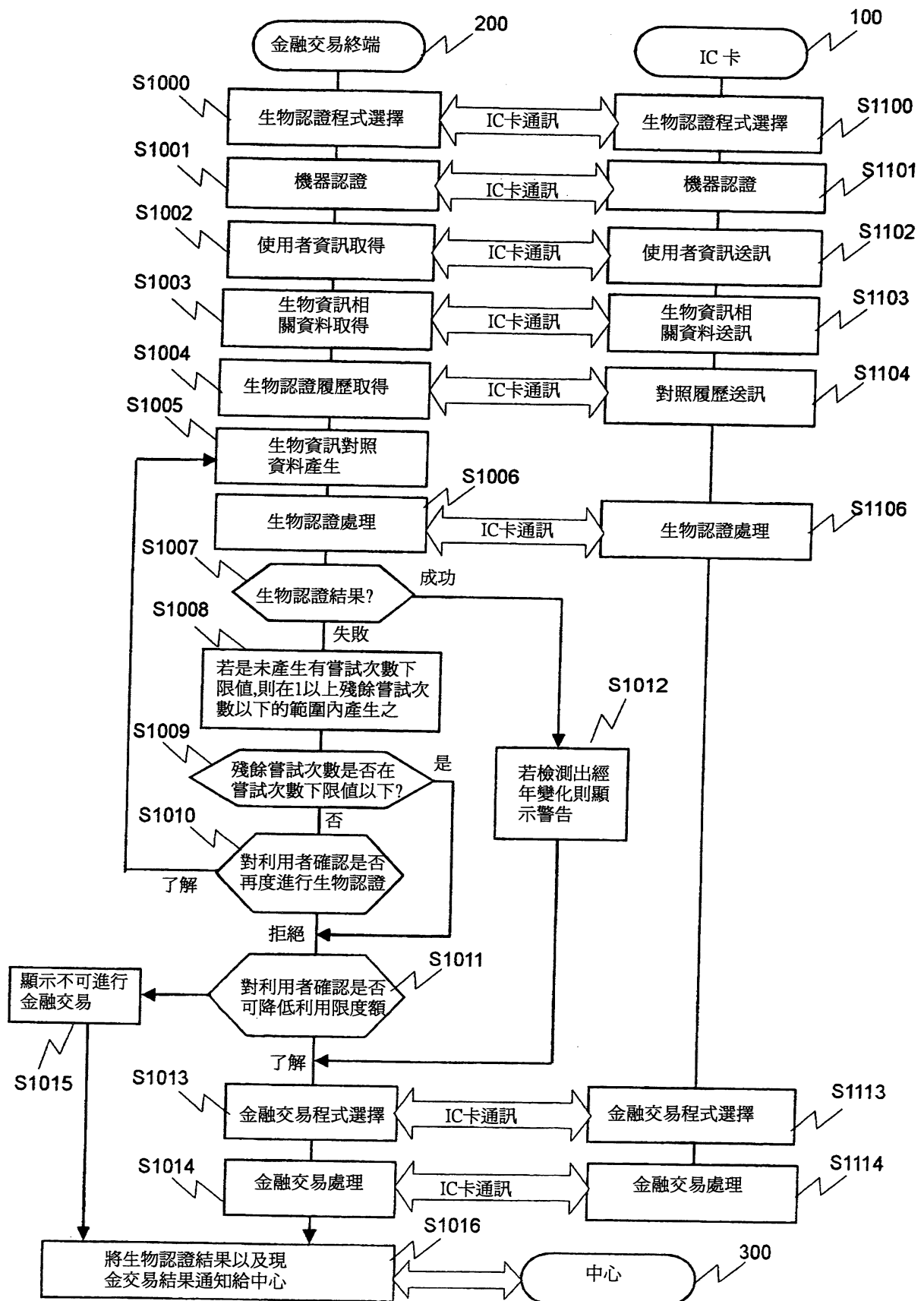


圖 14

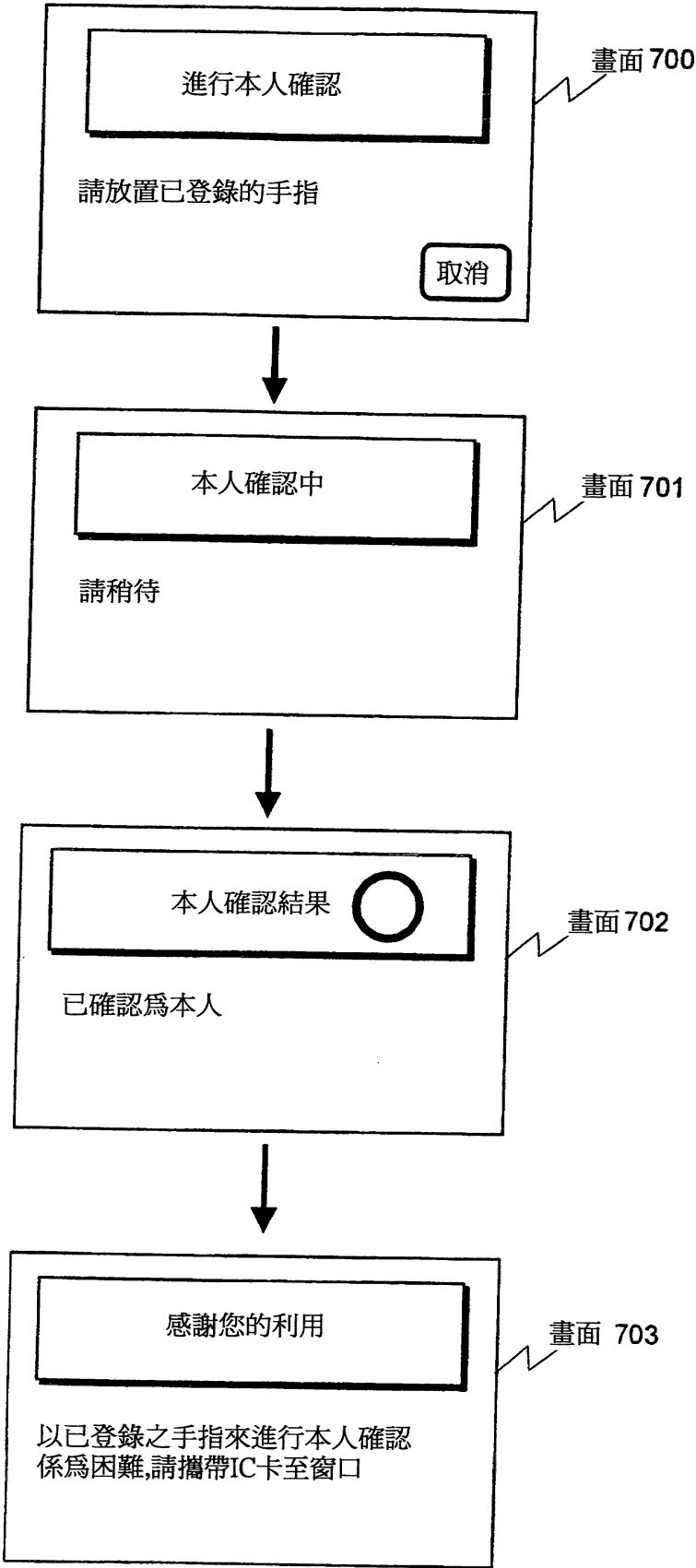


圖 15

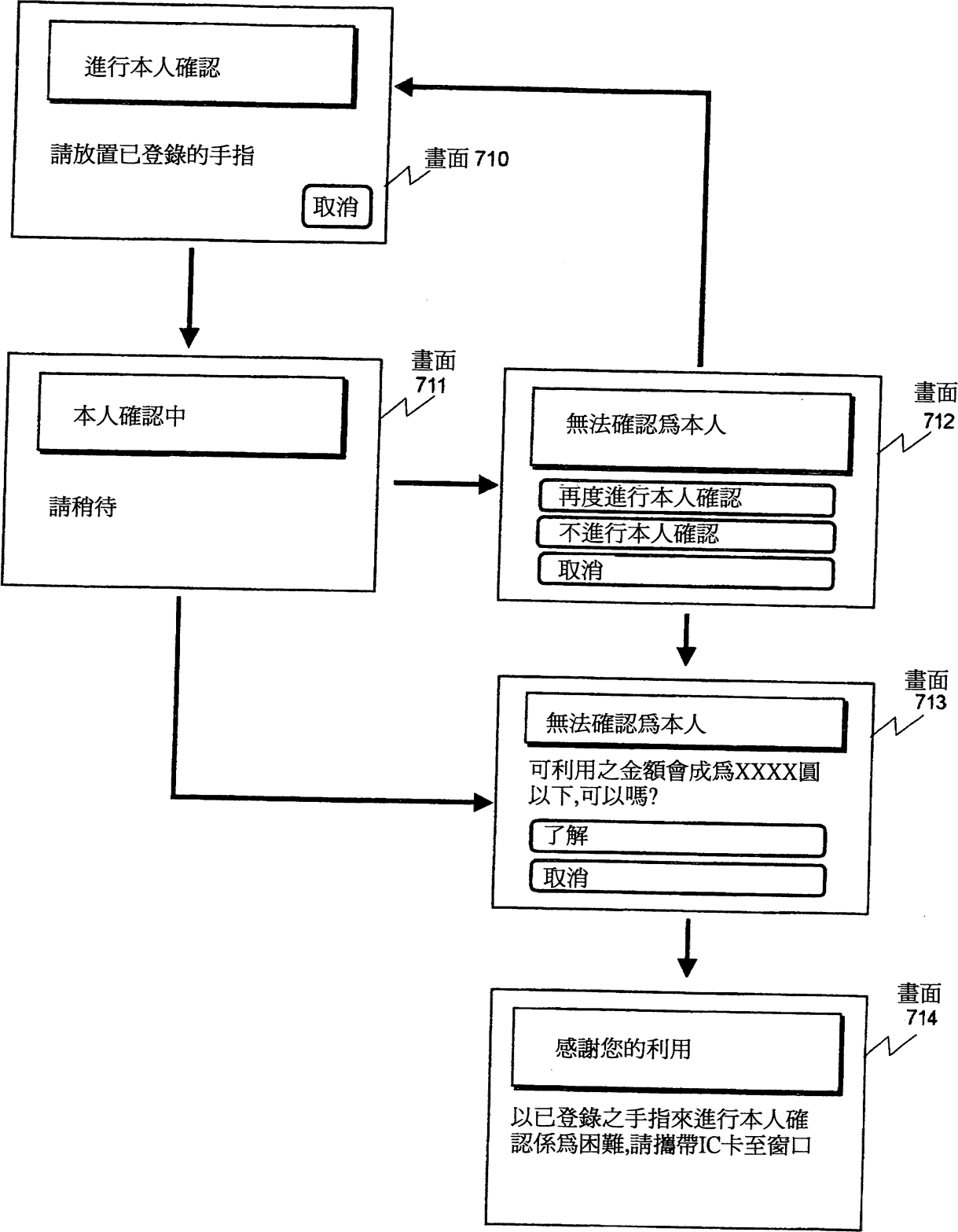


圖 16

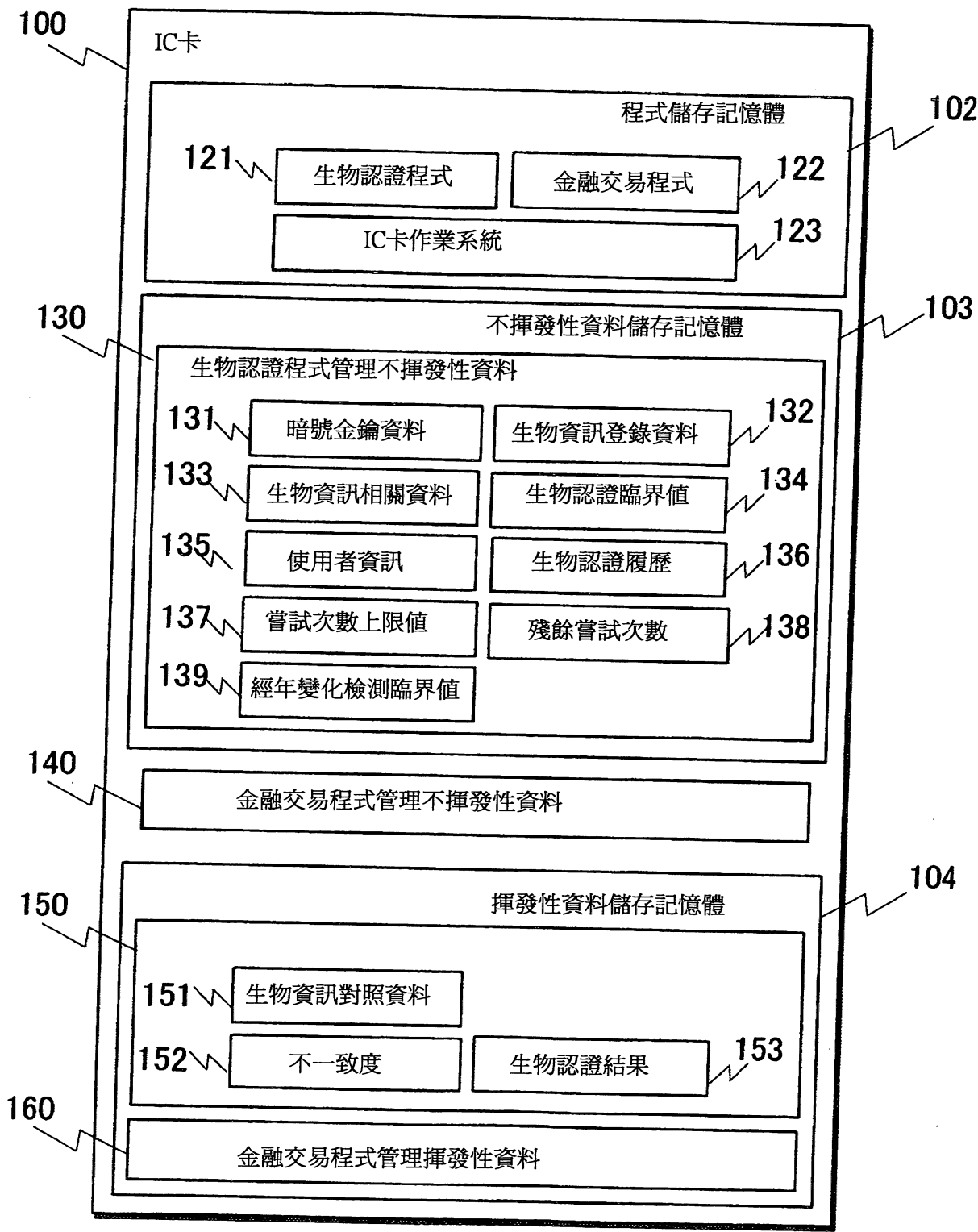


圖 17

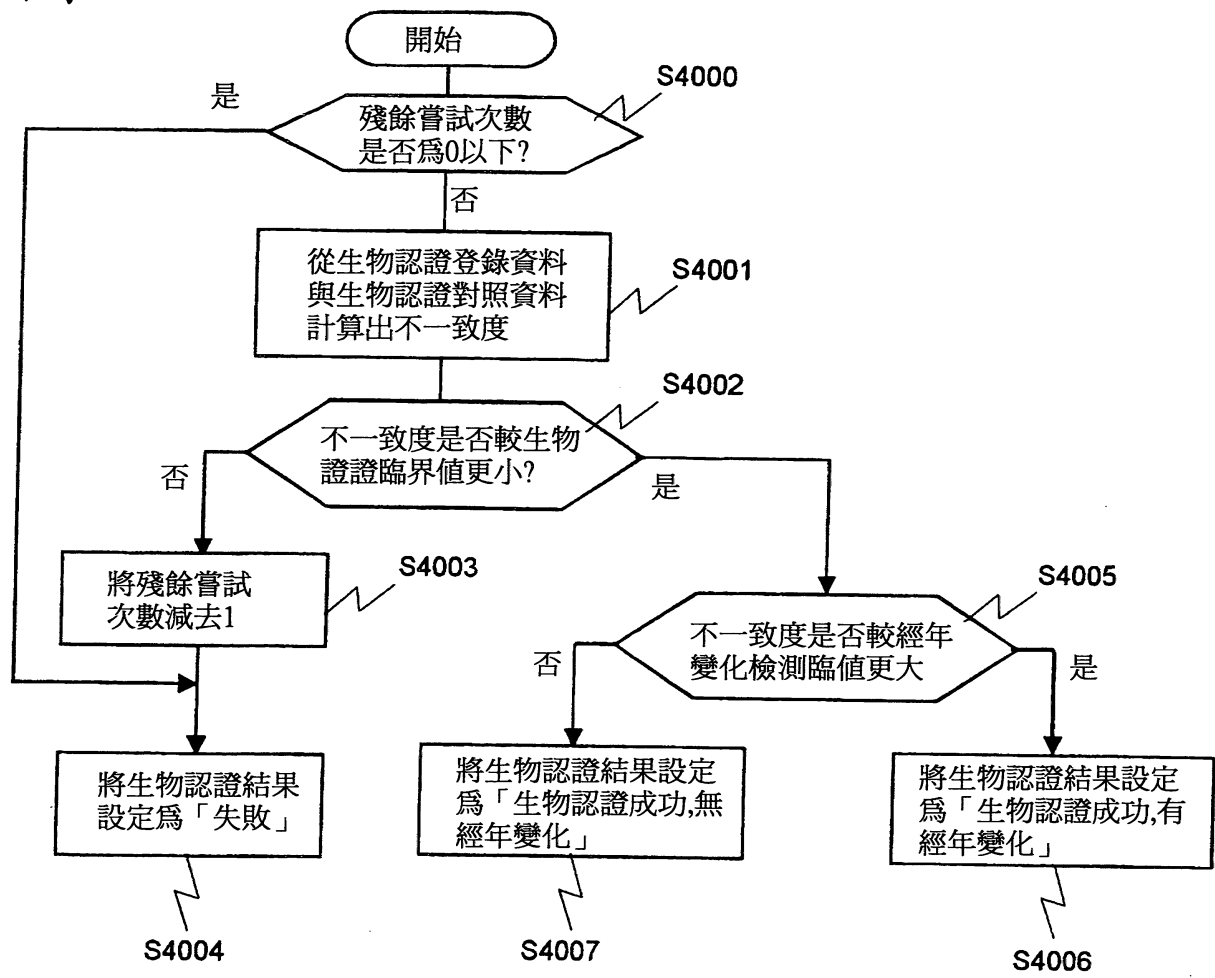
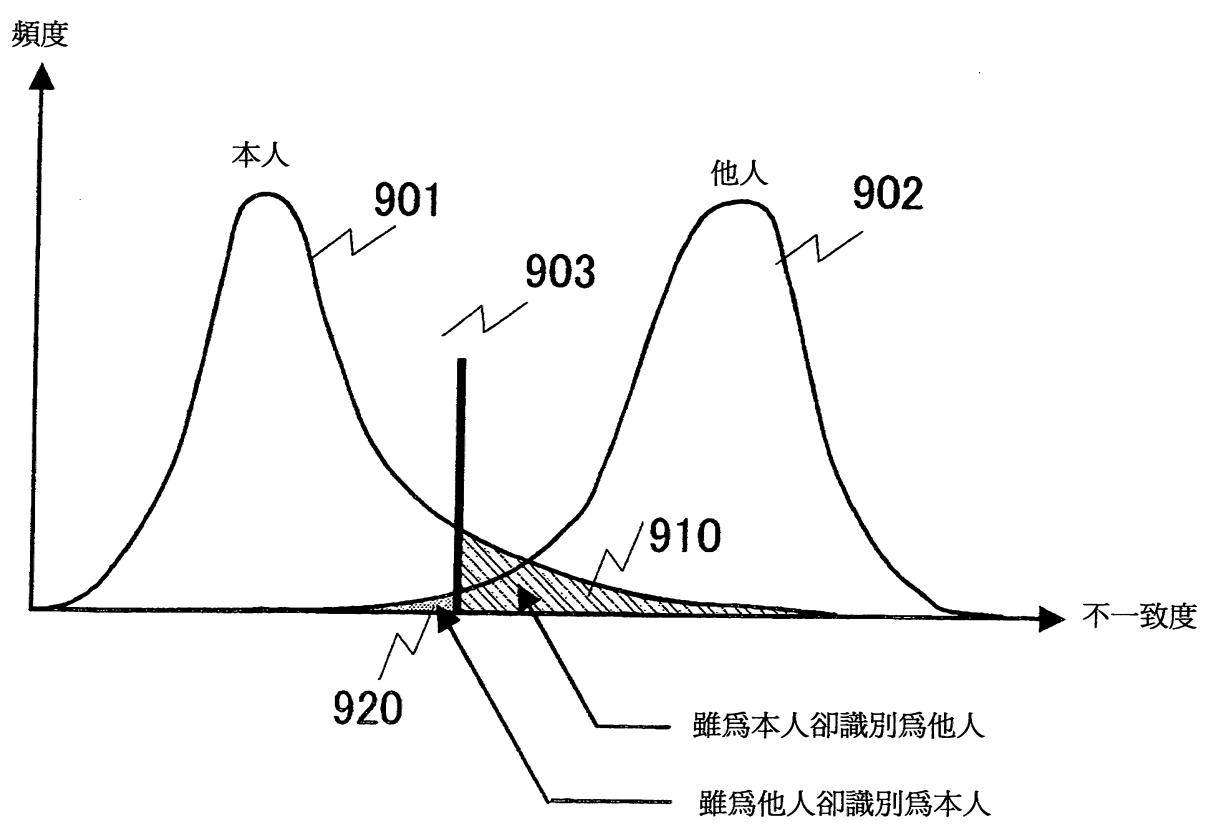


圖 18



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：

- 10：手指
- 100：IC 卡
- 101：通訊部
- 102：程式儲存記憶體
- 103：不揮發性資料儲存記憶體
- 104：揮發性資料儲存記憶體
- 105：演算處理部
- 200：金融交易終端
- 201：IC 卡通訊部
- 202：程式儲存記憶體
- 203：不揮發性資料儲存記憶體
- 204：揮發性資料儲存記憶體
- 205：生物資訊感測器
- 206：使用者介面部
- 207：中心通訊部
- 208：演算處理部
- 300：網路
- 400：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：無