發明專利說明書 200422833

（本說明書格式、順序及粗體字，請勿任意更動，※記號部分請勿填寫）

※ 申請案號：92135525

※ 申請日期：92/12/16　　※IPC 分類：G06F 12/14
G06K 19/073

壹、發明名稱：（中文/英文）

（中文）記憶裝置及使用其之電子機器

（英文）

貳、申 請 人：（共 1 人）

姓名或名稱：（中文/英文）

（中文）松下電器產業股份有限公司

（英文）MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.（松下電器產業株式会社）

代表人：（中文/英文）

中村邦夫 / Kunio NAKAMURA

住居所或營業所地址：（中文/英文）

（中文）日本國大阪府門真市大字門真 1006 番地

（英文）1006, Oaza Kadoma, Kadoma-shi, Osaka, 571-8501, Japan

國　籍：（中文）日本　（英文）Japan

參、發明人：（共 4 人）

姓　名：（中文/英文）

(1)高木佳彥 / Yoshihiko TAKAGI

(2)中西良明 / Yoshiaki NAKANISHI

(3)佐佐木理 / Osamu SASAKI（佐々木理）

(4)菊地隆文 / Takafumi KIKUCHI（菊地隆文）

住居所地址：（中文/英文）

(1)日本國東京都大田區東六鄉 2-20-5-506

2-20-5-506, Higashirokugou, Ota-ku, Tokyo 144-0046 Japan

(2)日本國東京都杉並區松ノ木 2-4-10-305

2-4-10-305, Matsunoki Suginami-ku, Tokyo 166-0014 Japan

(3)日本國東京都大田區東六鄉 2-20-5-620

2-20-5-620, Higashirokugou, Ota-ku, Tokyo 144-0046 Japan

(4)日本國東京都大田區東六鄉 2-20-5-718

2-20-5-718, Higashirokugou, Ota-ku, Tokyo 144-0046 Japan

國　籍：（中文）日本　（英文）Japanese

肆、聲明事項：

☐ 本案係符合專利法第二十條第一項☐第一款但書或☐第二款但書規定之期間，其日期為：　年　月　日。

◎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；2002/12/16；2002-363597
2.
3.
4.
5.

☐ 主張國內優先權(專利法第二十五條之一)：

【格式請依：申請日；申請案號數　順序註記】

1.
2.

☐ 主張專利法第二十六條微生物：

☐ 國內微生物 【格式請依：寄存機構；日期；號碼　順序註記】

☐ 國外微生物 【格式請依：寄存國名；機構；日期；號碼　順序註記】

☐ 熟習該項技術者易於獲得，不須寄存。

(3)日本國東京都大田區東六鄉 2-20-5-620

2-20-5-620, Higashirokugou, Ota-ku, Tokyo 144-0046 Japan

(4)日本國東京都大田區東六鄉 2-20-5-718

2-20-5-718, Higashirokugou, Ota-ku, Tokyo 144-0046 Japan

國　籍：（中文）日本　（英文）Japanese

肆、聲明事項：

☐ 本案係符合專利法第二十條第一項☐第一款但書或☐第二款但書規定之期間，其日期為：　年　月　日。

◎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；2002/12/16；2002-363597
2.
3.
4.
5.

☐ 主張國內優先權(專利法第二十五條之一)：

【格式請依：申請日；申請案號數　順序註記】

1.
2.

☐ 主張專利法第二十六條微生物：

☐ 國內微生物 【格式請依：寄存機構；日期；號碼　順序註記】

☐ 國外微生物 【格式請依：寄存國名；機構；日期；號碼　順序註記】

☐ 熟習該項技術者易於獲得，不須寄存。

玖、發明說明：

【發明所屬之技術領域】

本發明係關於半導體記憶卡等的記憶裝置，及對該記憶裝置執行資料的寫入/讀出的電子機器，尤其是關於實現保全等級高、且具有大記憶容量的記憶媒體。

【先前技術】

具備將非揮發性半導體記憶體作為記憶媒體的半導體記憶卡（以下，稱為「記憶卡」），與DVD等的磁碟狀記憶媒體比較，其記憶容量雖小，但因其不需要大的機構部，而可以小型地使用，具有優良的耐震性，因此作為適宜移動用的記憶媒體，最近其利用範圍正擴大中。

記憶卡具有內建CPU(微電腦)者及未內建CPU者。內建CPU的記憶卡內的CPU的動作，係由外部機器所要求，進行對非揮發性記憶體的讀出/寫入處理。

另外，在記憶卡的非揮發性記憶體設置保全區域，在提高保全等級方面也花費一番功夫。在下述專利文獻1記載有一記憶卡，其在非揮發性記憶體內設置可存取僅獲得認證成功的外部機器的認證區域；及還可存取外部機器的任一者的非認證區域。使用該記憶卡將密碼化的音樂內容儲存於非認證區域，將該音樂內容解碼的解碼鍵儲存於認證區域，藉以可保護音樂內容的著作權。

如此之記憶卡內的CPU的動作，除資料的讀出·寫入處理外，還有允許外部機器對認證區域的存取用的外部機器的認證處理。

無論如何，記憶卡內的CPU的動作，限定於記憶體的讀寫及依據此者，而記錄於記憶體的資料的控制係由外部機器所執行。

另一方面，同樣地內建CPU的IC卡，在耐干擾性的模組內具有CPU，同時還具有記憶區域。因耐干擾性的緣故，外部機器無法於該記憶區域直接存取。因此，IC卡對複製或偽造具有高保密性，而廣泛應用於要求高保全性的數位現金的服務等。

IC卡內的CPU的動作，不僅進行記憶體的讀出·寫入，還執行外部輸入的資料的密碼化、署名生成、署名驗證、所輸入的密碼的認證等而有各種的用途。另外，記錄於IC卡的記憶體內的資料的控制係由IC卡內部的CPU來執行。

如此般，IC卡的CPU與習知內建於記憶卡內的CPU相比，具有多功能且高保全性。

(專利文獻1)

日本專利特開2001-14441號公報

但是，IC卡受所記憶的資訊容量所限，與數位現金的服務的多樣化一起，均受到來自服務業者對記憶容量的擴大要求。例如，為避免數位現金的2度提取等的故障的發生，若欲實施記錄電子發票或交易記錄的服務，為記憶累積的電子發票等，與習知的IC卡的容量比較，有確保大的資訊容量的必要。

另一方面，因為上述專利文獻1所記載的記憶卡可將認證區域設定為可變，因此可具有某種程度的大的資訊容

量。但是，該認證區域為可由外部機器直接控制的區域，因此與IC卡相比較，其保全等級低。

【發明內容】

本發明係用以解決上述習知問題者，其目的在於提供記憶容量大且具備有與IC卡同等保全等級的記憶區域的記憶裝置，還提供使用該記憶裝置的電子機器。

在此，本發明中係在固定或可裝卸地連接於電子機器的記憶裝置中設置：非耐干擾性的第1記憶體，其具有可從電子機器存取的正常區域、和無法從電子機器直接存取的保全區域；及耐干擾性的第2記憶體，其無法從電子機器直接存取，而對第1記憶體的保全區域的存取，僅介由管理對第2記憶體的存取的保全控制部才可進行。

因為該保全區域無法由外部機器直接存取，因此，其保全性較習知的認證區域高。另外，該保全區域係設於非耐干擾性的記憶體，因此可以低成本獲得大的記憶容量。

另外，本發明中，對具有第1區域、第2區域及第3區域作為記憶區域的記憶裝置進行存取的電子機器，係在接受對記憶裝置的存取要求時，在記憶裝置之作為非耐干擾性之記憶區域的第1區域，介由控制對記憶裝置之存取的記憶裝置的全體控制部進行存取，在第1區域以外之作為非耐干擾性之記憶區域的第2區域，介由全體控制部及控制對第2區域及第3區域的存取的記憶裝置的保全控制部，經由與保全控制部的認證後進行存取，另外，在記憶裝置之作為耐干擾性之記憶區域的第3區域，介由全體控

制部及保全控制部，經由與保全控制部的認證後進行存取。

該電子機器運用該半導體記憶卡等的記憶裝置，實現多樣化的服務。

【實施方式】

本發明之實施形態之半導體記憶卡（在此稱為「保全記憶卡」），如圖1之概念圖所示，具備：備有內部非揮發性記憶體41的耐干擾性模組（tamper resistant module：TRM）40；備有非認證區域53、認證區域52及保全區域51的大容量非揮發性記憶體50；對內部非揮發性記憶體41及保全區域51進行存取的內部CPU30；及與電子機器（讀出/寫入（R/W）裝置）的外部CPU60通信而進行認證處理，允許對受到認證的外部CPU60的認證區域52進行存取的控制部20。

TRM40的非揮發性記憶體41，例如，由16位元組單位組成可刪除、寫入的EEPROM，另外，大容量非揮發性記憶體50，例如，可進行在512位元組等的塊單位的刪除及可進行在1位元組單位的寫入的快閃記憶體所組成。

外部CPU60可在非認證區域53無條件進行存取，另外，認證區域52可在控制部20的認證完成的情況進行存取。但是，外部CPU60無法知道保全區域51及內部非揮發性記憶體41的存在，無法直接對此等進行存取。

對於保全區域51及內部非揮發性記憶體41，僅可由內部CPU30進行存取。保全區域51和內部非揮發性記憶體41的差異在於，內部非揮發性記憶體41設於TRM40，而相

對於此，保全區域51設於不具耐干擾性的大容量非揮發性記憶體50。因此，保全區域51與內部非揮發性記憶體41比較，可具有大的記憶容量。相反，保全等級較設於TRM40的內部非揮發性記憶體41要低。該4個區域的保全等級以非認證區域53最低，然後為認證區域52、保全區域51、內部非揮發性記憶體41順序增高。

保全記憶卡10的詳細構成容待後述，關於其使用形態說明如下。

例如、保全記憶卡可使用於圖3所示的音樂配信系統等。該系統中，保全記憶卡10安裝於屬R/W裝置的行動電話61上。另外，在該系統存在有介由網絡95傳送音樂的配信伺服器94；進行結帳處理的結帳伺服器93；將數位現金充值於記憶卡10的充值伺服器92；及數位現金的充值用終端91。

行動電話61如圖4的方塊圖所示，具備相當於圖1的外部CPU的CPU60；預先記憶用於認證的認證鍵群622或指令生成程式621的ROM62；作為CPU60的作業區域使用的RAM63；構成顯示畫面的液晶顯示部64；介由網絡進行無線通信的無線通信部65；使用者操作用的操作鍵66；將保全記憶卡10連接於內部匯流排70的卡I/F部67；及進行與保全記憶卡10的相互認證的認證電路68，此等各部均由內部匯流排70連接。

使用者首先將數位現金充值於保全記憶卡10。為此，使用者將保全記憶卡10安裝於充值用終端91，根據所顯示

的指示操作充值用終端91。此時，充值用終端91對保全記憶卡10的內部CPU30要求進款操作的起動。進款操作起動的內部CPU30，當從充值用終端91接收到數位現金的進款處理要求時，從該要求的指令將資料的寫入處判斷為內部非揮發性記憶體41，於是將從充值用終端91傳達來的金額寫入內部非揮發性記憶體41。如此般便可將數位化資訊記憶於內部非揮發性記憶體41。

另外，數位現金的充值，也可從安裝著保全記憶卡10的行動電話61，於充值伺服器92作存取，而在線上進行。

其次，使用者從行動電話61進入配信伺服器94，委託音樂內容的購入。配信伺服器94要求音樂內容的價款的結帳。接受此要求，行動電話61的CPU60在保全記憶卡10的內部CPU30要求結帳應用的起動。起動結帳應用的內部CPU30，在認證了行動電話61後，從記錄於內部非揮發性記憶體41的數位現金的餘額減去從行動電話61傳達來的支付款項。藉由此，配信伺服器94將電子發票傳送給行動電話61，行動電話61的CPU60將該電子發票接收要求傳送給保全記憶卡10的內部CPU30。內部CPU30係從其要求的指令將資料的寫入處判斷為保全區域51，將電子發票記憶於保全區域51。

又，結帳處理係將儲存於內部非揮發性記憶體41的信用號碼提示於結帳伺服器93，也可在與結帳伺服器93間進行。

結帳結束後，配信伺服器94將密碼化的音樂內容和其

解碼鍵傳送給行動電話61。行動電話61的CPU60，判斷受信資料，將內容的解碼鍵儲存於保全記憶卡10的認證區域52，另外，將密碼化的內容儲存於保全記憶卡10的非認證區域53。

如此般，在該系統中，在保全記憶卡10的內部非揮發性記憶體41儲存有現金資訊，在保全區域51儲存電子發票，在認證區域52儲存解碼鍵，另外在非認證區域53儲存被密碼化的內容。

圖2的方塊圖顯示保全記憶卡10的構成。保全記憶卡10大致由控制部20、大容量非揮發性記憶體50及相當於圖1的TRM40的IC部11所構成。大容量非揮發性記憶體50具有非認證區域53、認證區域52、保全區域51及儲存於此等的區域的位址資訊的位址資訊管理區域54。

控制部20具備：在與R/W裝置69間進行資料的授受的資料I/F部21；在與R/W裝置69間進行指令的授受的指令I/F部22；認證R/W裝置69的控制認證部23；解釋已受理的指令而進行響應該指令的處理的控制指令處理部24；控制對大容量非揮發性記憶體50的存取，同時成為與IC部11的資料的交接窗口的存取控制部25；及在與大容量非揮發性記憶體50間交接資料的大容量非揮發性記憶體I/F部26。

另外，耐干擾性的IC部11具備：內部非揮發性記憶體41；在與控制部20之間進行資料和指令的授受的I/F部12；解釋指令進行響應指令的處理的IC指令處理部13；

在內部非揮發性記憶體41及保全區域51管理由檔案形式所儲存的資料的檔案管理部14；認證R/W裝置69，對認證的R/W裝置69允許對內部非揮發性記憶體41及保全區域51的資料存取的IC認證部15；對內部非揮發性記憶體41及保全區域51的寫入/讀出資料使用儲存於內部非揮發性記憶體41的鍵進行密碼化/解碼化的密碼/解碼電路17；進行內部非揮發性記憶體41及保全區域51的管理的記憶體管理部16；及進行內部非揮發性記憶體41的資料的授受的內部非揮發性記憶體I/F部18。在申請專利範圍所稱的保全控制部對應於IC部11的IC指令處理部13、IC認證部15、密碼/解碼電路17、檔案管理部14及記憶體管理部16。

控制部20的控制指令處理部24係解釋從R/W裝置69接收的指令，該指令判斷為：

・是否要求對大容量非揮發性記憶體50的認證區域52或非認證區域53的存取者？

・是否要求認證？

・是否要求依IC部11的處理？

在要求大容量非揮發性記憶體50的認證區域52或非認證區域53的存取時，於存取控制部25指示對大容量非揮發性記憶體50的存取控制，在要求依IC部11的處理時，於存取控制部25指示對IC部11的指令的傳送，另外，在要求認證時，於控制認證部23指示認證處理。

對認證區域52的存取僅在對其終端的控制認證部23的

認證完成的情況被接受。

存取控制部25在對大容量非揮發性記憶體50的存取控制時，參照記錄於大容量非揮發性記憶體50的位址資訊管理區域54的位址資訊。在終端(R/W裝置69)指定大容量非揮發性記憶體50的邏輯位址而要求存取時，從位址資訊管理區域54的記錄判斷指定的位址是否屬於大容量非揮發性記憶體50的任一區域，對認證區域52的存取要求，限於認證完成的終端才允許進行。

另外，IC部11的IC指令處理部13，解釋從控制部20所送信的指令，其處理要求判斷

·是否要求對內部非揮發性記憶體41的資料寫入/讀出者？

·是否要求對保全區域51的資料寫入/讀出者？

·是否要求其他處理？

IC指令處理部13在指令要求操作的起動時，在內部起動其操作。

操作係指從R/W裝置69受取的指令的解釋形態，在操作起動後從R/W裝置69受取IC指令處理部13的指令，在該操作與R/W裝置69之間取決的解釋係藉由IC指令處理部13所進行。

操作起動後受取的指令，在要求認證時，IC指令處理部13於IC認證部15指示R/W裝置69的認證處理。

另外，IC指令處理部13，在指令為由內部起動的操作與R/W裝置69之間所取決的對內部非揮發性記憶體41的

資料的寫入/讀出，或要求對保全區域51的資料的寫入/讀出的指令時，在IC認證部15確認是否完成認證處理的事項。

在完成認證處理的情況，允許其要求，在要求寫入該要求時，將寫入的資料並附上儲存處的資訊傳送給記憶體管理部16。

管理內部非揮發性記憶體41及保全區域51的記憶體管理部16，係由密碼/解碼電路17將寫入資料密碼化（此時密碼/解碼電路17係使用儲存於內部非揮發性記憶體41的密碼鍵予以密碼化）後，介由內部非揮發性記憶體I/F部18，將應寫入內部非揮發性記憶體41的資料寫入內部非揮發性記憶體41，將寫入位置的資訊傳輸給檔案管理部14。另外，介由大容量非揮發性記憶體I/F部26，將應寫入保全區域51的資料寫入大容量非揮發性記憶體50的保全區域51，將寫入位置的資訊傳輸給檔案管理部14。

檔案管理部14基於從記憶體管理部16傳輸來的資訊，管理儲存於內部非揮發性記憶體41及保全區域51的檔案。

另外，IC指令處理部13在其要求為讀出要求時，於檔案管理部14求取應欲讀出的資料的檔案位置，於記憶體管理部16要求該檔案的讀出。

記憶體管理部16，當記憶體管理部16從內部非揮發性記憶體41或保全區域51讀出該檔案時，由密碼/解碼電路17將資料解碼（此時密碼/解碼電路17係使用儲存於內部非揮發性記憶體41的鍵予以解碼），傳送給IC指令處理部

13。

被解碼的資料係傳送給控制部20，從資料I/F部21傳送給R/W裝置69。

在此，若整理對大容量非揮發性記憶體50的非認證區域53、認證區域52、保全區域51及內部非揮發性記憶體41的寫入/讀出條件，其內容成為如下。

・非認證區域：可無條件進行存取。可以對非認證區域進行存取用的正常指令進行資料的寫入/讀出。

・認證區域：有完成與控制部20的控制認證部23的認證的必要。藉由控制認證部23的認證，使用認證區域52的邏輯位址可進行存取。

・保全區域：有完成與IC部11的IC認證部15(=IC部操作)的認證的必要。藉由在IC部操作與終端間取決的指令可進行資料的寫入/讀出(或作為IC部操作的部分處理可進行資料的寫入/讀出)。因從終端無法看見保全區域，故終端無法使用保全區域的邏輯位址進行存取。

・內部非揮發性記憶體：與保全區域的寫入/讀出完全相同。又，也可使對保全區域作存取用的認證和對內部非揮發性記憶體作存取用的認證各異。

圖8顯示大容量非揮發性記憶體50的內部構造。在此，大容量非揮發性記憶體50的物理位址上的配置，顯示非認證區域53為0000~(XXXX-1)，認證區域52為XXXX~(ZZZZ-1)，保全區域51為ZZZZ~(YYYY)的情況。顯示保全區域51與認證區域52的境界的第1位址資訊為

ZZZZ，顯示認證區域52與非認證區域53的境界的第2位址資訊為XXXX。另外，非認證區域53的尺寸為XXXX，認證區域52的尺寸為ZZZZ- XXXX，保全區域51的尺寸為YYYY-ZZZZ+1。

圖9顯示表示各區域的物理位址及邏輯位址的對應關係的「邏輯-物理位址變換表」。非認證區域53的邏輯位址為0000~(XXXX-1)，認證區域52的邏輯位址為0000~(ZZZZ-XXXX-1)、保全區域51的邏輯位址為0000~(YYYY- ZZZZ)。

在位址資訊管理區域54保持有第1位址資訊、第2位址資訊及各區域的邏輯-物理位址變換表。關於非認證區域53、認證區域52及保全區域51的任一者，也無法越過所分配的邏輯位址的境界以指定邏輯位址，但可移動於各區域的境界，以擴張或縮小各區域。

保全區域51的擴張或縮小可藉由改變第1位址資訊來實現。圖9的邏輯-物理位址變換表中，因為將非認證區域53及認證區域52的邏輯位址的順序作為物理位址的順序的正順序，將保全區域51之邏輯位址的順序作為物理位址的順序的逆順序，在改變認證區域52與保全區域51的境界時，只要同時修正邏輯塊的末尾位址側即足夠，因此可減少伴隨著境界改變的表的改寫負擔，而可高速處理。

關於該境界改變的操作步驟容待後述。

再者，說明有關該保全記憶卡的資料的儲存步驟。

圖5及圖6顯示從安裝著保全記憶卡的終端，於配信伺服器委託內容購入，進行價款的結帳處理，直到將該電子

發票儲存於保全區域，將密碼化的內容儲存於非認證區域，另外將內容的解碼鍵儲存於認證區域的步驟。

如圖5所示，終端於配信伺服器委託內容購入(1)。配信伺服器要求內容之價款的結帳(2)。終端將要求結帳應用的起動的指令傳送給保全記憶卡10的IC部11(3)。控制部20的控制指令處理部24係將該指令認識為對IC部的指令，並傳送給IC部11(4)。IC部11起動結帳應用，使IC認證部15開始，將回答返回終端(5)、(6)。終端將認證要求指令傳送給保全記憶卡10(7)，控制部20的控制指令處理部24將該指令認識為對IC部的指令傳輸給IC部11(8)。IC認證部15認證終端(或配信伺服器)，回答認證結果(9)、(10)。完成認證的終端係於保全記憶卡10顯示支付額，傳送給結帳要求的指令(11)。控制部20的控制指令處理部24將該指令認識為對IC部的指令，傳輸給IC部11(12)。IC認證部15係藉由所謂「結帳要求」的指令判斷為寫入內部非揮發性記憶體41的資料，進行將記錄於內部非揮發性記憶體41的餘額，改寫為減去支付額的金額的處理，回答處理結束(13)、(14)(又，終端拒絕未完成(9)的認證的狀態下的結帳要求)。

終端將回答返回配信伺服器(15)。配信伺服器將電子發票傳送給終端(16)。終端將電子發票的儲存要求指令傳送給保全記憶卡10(17)。控制部20的控制指令處理部24將該指令認識為對IC部的指令，傳輸給IC部11。IC認證部15係藉由所謂「電子發票儲存要求」的指令判斷為應儲存

於保全區域51的資料，由密碼/解碼電路17將電子發票密碼化後，儲存於保全區域51(18)（又，終端拒絕未完成(9)的認證的狀態下的電子發票儲存要求）。

又，依IC認證部15的(9)的認證可為將允許「結帳要求」用的認證及允許「電子發票儲存要求」用的認證分開進行（亦即，有使用不同的鍵進行認證的必要）。

如圖6所示，當將電子發票的儲存完成的回答從IC部11傳送給終端時(19)、(20)，終端便於配信伺服器要求內容的傳送(21)。配信伺服器將密碼化的內容及將此解碼的內容鍵傳送給終端(22)。終端判斷在從配信伺服器所受取的資料內包含有應寫入認證區域52的內容鍵的事項，對保全記憶卡10的控制部20要求認證(23)。控制部20的控制指令處理部24解釋該指令，由控制認證部23進行終端的認證，並回答認證結果(24)。終端發出對認證區域52的內容鍵的寫入要求(25)。控制部20的存取控制部25，因已完成終端的認證，因此允許為認證區域52的存取，將內容鍵寫入認證區域52。當有寫入結束的回答時(26)，終端將密碼化的內容判斷為應對非認證區域53寫入的事項，於保全記憶卡10要求對非認證區域53的寫入(27)。當密碼化的內容被寫入非認證區域53，其回答返回終端時(28)，終端將完成通知傳送給配信伺服器(29)。

如此之後，將電子發票密碼化後寫入保全區域51，將內容鍵寫入認證區域52，將被密碼化的內容寫入非認證區域53。

又，在將圖5之步驟中記錄於內部非揮發性記憶體41的餘額改寫為減去支付額的金額時(13)，如圖7所示，也可將該支付額寫入保全區域51(13')。利用如此的步驟，可將結帳記錄記錄於保全區域51。

另外，在進行依結帳應用的認證(3)前或後，也可進行確認利用者用的密碼認證。

再者，說明有關大容量非揮發性記憶體50的各區域間的境界改變的步驟。在此，顯示改變圖8的第1位址資訊以擴張或縮小保全區域51的情況。

該境界改變係由來自安裝著保全記憶卡10的終端的要求所進行。

(1)終端對保全記憶卡10要求境界改變操作的起動，起動該操作的保全記憶卡10的IC部11，起動IC指令處理部13及IC認證部15。終端對IC部11要求認證，於是IC認證部15認證終端。又，該認證也可為與需要對內部非揮發性記憶體41或保全區域51的存取的認證不同的認證，僅由部分的特定終端進行保全區域51的擴張/縮小。

(2)受到認證的終端對IC部操作(IC指令處理部13)通知改變後的第1位址資訊(新的ZZZZ)。

(3)IC指令處理部13係於記憶體管理部16傳達新的ZZZZ，以指示保全區域51的境界改變。記憶體管理部16係以對應於ZZZZ的值的方式修正保全區域51與認證區域52的邏輯-物理位址變換表，於位址資訊管理區域54儲存新的ZZZZ的值及修正後的邏輯-物理位址變換表。此時，

只要在圖9的保全區域及認證區域的表上同時修正邏輯塊的末尾位址側。

(4)記憶體管理部16在擴張保全區域51的情況，刪除新成為保全區域的部分的資料，在縮小保全區域51的情況，刪除新成為認證區域52的部分的資料。此時，也可刪除保全區域及/或認證區域的所有資料。

(5)IC指令處理部13在終端通知境界改變完成。

另外，此時基於IC部的要求，保全記憶卡10的控制部20，也可進行境界改變的處理。該情況的操作步驟成為如下。

(1)與上述(1)相同，終端接受IC認證部15的認證。

(1')終端對保全記憶卡10的控制部20要求認證，藉由控制指令處理部24的指示，控制認證部23進行允許認證區域的尺寸改變用的認證。

(2)與上述(2)相同，終端對IC指令處理部13通知改變後的第1位址資訊(新的ZZZZ)。

(3)IC指令處理部13係經由存取控制部25而於控制指令處理部24要求境界位址變更。

(3')控制指令處理部24係於位址資訊管理區域54保存ZZZZ的值，且一併以對應ZZZZ的值的方式修正保全區域與認證區域的邏輯-物理位址變換表。(只是，在未進行(1')的認證的情況拒絕境界位址的改變，並將拒絕之事通知IC指令處理部13)。

(4)控制指令處理部24在擴張保全區域的情況，刪除新

成為保全區域的部分的資料，在縮小保全區域的情況，刪除新成為認證區域的部分的資料。另外，也可刪除保全區域及/或認證區域的所有資料。

(5)控制指令處理部24係將境界改變完成傳達給IC指令處理部13，IC指令處理部13在終端通知境界改變完成(只是，在(3')中拒絕境界位址的改變的情況，於終端通知境界改變的拒絕)。

另外，認證區域的擴張/縮小，係藉由改變認證區域與非認證區域的境界的第2位址資訊來進行。該情況的操作步驟成為如下。

(1)終端對保全記憶卡10的控制部20要求認證，藉由控制指令處理部24的指示，控制認證部23進行允許認證區域的尺寸改變用的認證。

(2)接受認證的終端，對控制部20通知改變後的第2位址資訊(新的XXXX)。

(3)控制指令處理部24係於位址資訊管理區域54保存XXXX的值，且一併以對應XXXX的值的方式修正非認證區域與認證區域的邏輯-物理位址變換表。(只是，在未進行(1)的認證的情況拒絕境界位址的改變，並將拒絕之事通知終端)。

(4)控制指令處理部24在擴張保全區域的情況，刪除新成為認證區域的部分的資料，在縮小認證區域的情況，刪除新成為非認證區域的部分的資料。另外，也可刪除非認證區域及/或認證區域的所有資料。

(5)控制指令處理部24在終端通知境界改變完成。

又，該情況，如圖10所示，若邏輯-物理位址變換表的非認證區域53的邏輯位址的序號為物理位址的順序的正順序，認證區域52的邏輯位址的序號為物理位址的順序的逆順序，因為在境界改變時，只要同時修正邏輯塊的末尾位址側即足夠，因此伴隨境界改變的表的改寫負擔的減少，高速處理變得可能。

非認證區域的擴張或縮小，可藉由認證區域的擴張或縮小處理來實現。

另外，如圖11所示，也可在大容量非揮發性記憶體50，以保全區域51、非認證區域53、認證區域52的順序配置各區域。圖12顯示此時的邏輯-物理位址變換表的一例。

另外，該情況，為了將保全區域51設為從終端無法看見的區域，或是為了保持與未具有保全區域的記憶卡的互換性，如圖11所示，也可設置與實際的境界位址不同的「虛設終端的位址」。在該虛設終端的位址中，省略保全區域，將虛設非認證區域53的前頭的物理位址設為0000(實際為XXXX')，將虛設非認證區域53與認證區域52的境界的物理位址設為ZZZZ''(實際為ZZZZ')，將虛設認證區域終端的前頭的物理位址設為YYYY''(實際為YYYY')。在終端將境界位址認識為ZZZZ''，要求區域的擴張/縮小時，要求該ZZZZ''的改變，但控制指令處理部認識ZZZZ''與ZZZZ'的關係，轉換為實際的物理位址ZZZZ'，進行境界的改變。

又，在本發明之實施形態中，說明了有關在大容量非揮

發性記憶體50設置非認證區域、認證區域及保全區域的3區域作為記憶區域的情況，也可在大容量非揮發性記憶體50除保全區域外設置非認證區域或認證區域的其中一區域作為正常區域。

另外，在此只要說明了在保全記憶卡的IC部搭載結帳用操作的情況，但是其他還可搭載生成署名的操作。

該情況，在對資料的保全區域的寫入時計算寫入資料的雜湊值，將此儲存於IC部的內部非揮發性記憶體內，對該雜湊值生成電子署名。在從資料的保全區域讀出時(解碼後)，再度計算雜湊值，在寫入時利用與儲存於IC部的內部非揮發性記憶體內的雜湊值作比較，以檢測資料的缺損、改善等。

利用搭載如此的功能，該保全記憶卡也可利用於結帳時，也可利用於對某一資料提供電子署名時。

另外，作為使用該保全記憶卡的R/W裝置，說明了搭載數位內容配信服務用操作，具有結帳功能和內容的下載及對記憶卡的儲存功能的情況，但在運用該記憶卡的基礎上，R/W裝置還要求具有如下的功能。

・可生成讀寫保全記憶卡的正常區域用的指令。

・可於保全記憶卡的IC部生成要求處理用的IC指令。

・取得與IC部操作(IC認證部)進行認證用的認證鍵，使用此可生成認證所必要的資料(對從IC部操作提供的亂數提供密碼或署名的資料)。

另外，在將保全記憶卡作為正常區域，具有非認證區域

及認證區域的情況，除此之外，

・可生成讀寫認證區域用的指令。

・取得與保全記憶卡的控制認證部進行認證用的認證鍵，使用此可生成認證所必要的資料。

又，認證鍵的取得係在R/W裝置(電子機器)由ROM等保持認證鍵的情況，從此處著手。另外，在電子機器未保持認證鍵的情況，則從外部機器(伺服器、可拆媒體等)接收。

另外，也可將本發明的保全記憶卡10具有的大容量非揮發性記憶體50，換為其他的記憶媒體，例如硬碟、光碟、光磁碟等的非揮發媒體，當然也可與本發相同可實現大容量・高保全性的記憶裝置。

另外，本發明之保全記憶卡10無須對電子機器可裝卸，例如，如將IC晶片埋入電子機器的一體型機器等，也可與電子機器固定連接。另外，也無須如卡/晶片的形狀，即使為磁碟或磁帶等的形態亦無妨。另外，本發明之電子機器(60、61、69)只要為固定裝置終端、行動終端、行動電話等可連接記憶裝置者，為任何裝置均無妨。

也就是說，除本發明之實施形態中說明的裝置外，還可依其用途考慮將IC晶片埋入行動電話者、將硬碟安裝於固定設置終端者等的各種各樣的形態。

雖參照特定的實施形態詳細說明了本發明，但只要未超出本發明之實質範圍，即可作種種的變化或修正。

本申請案係基於2002年12月16日提出申請的日本專利申請(特願2002-363597號)，其內容係參照該案而得者。

（產業上的可利用性）

從上述說明可知，本發明之記憶體裝置，其保全性與IC卡相同，可具有記憶容量遠大於IC卡的記憶區域。

另外，該記憶裝置具備複數的保全等級的記憶體，可由1個裝置對應數位現金或音樂配信等的多功能服務。另外，該複數的記憶區域的大小可依據需要改變。

另外，本發明之電子機器（R/W裝置）可運用該記憶裝置，實現多樣化的服務。

【圖式簡單說明】

圖1為本發明之實施形態之保全記憶卡的概念圖。

圖2為顯示本發明之實施形態之保全記憶卡的構成的方塊圖。

圖3為使用本發明之實施形態之保全記憶卡的系統的概念圖。

圖4為顯示本發明之實施形態之R/W裝置的構成的方塊圖。

圖5為顯示本發明之實施形態之保全記憶卡的寫入步驟的序列圖。

圖6為顯示本發明之實施形態之保全記憶卡的寫入步驟的序列圖。

圖7為顯示本發明之實施形態之保全記憶卡的其他寫入步驟的序列圖。

圖8為顯示本發明之實施形態之保全記憶卡的大容量非揮發性記憶體的構造圖。

圖 9 為顯示本發明之實施形態之邏輯-物理位址變換表的圖。

圖 10 為顯示本發明之實施形態之邏輯-物理位址變換表的其他例的圖。

圖 11 為顯示本發明之實施形態之保全記憶卡的大容量非揮發性記憶體的不同構造圖。

圖 12 為顯示本發明之實施形態之邏輯-物理位址變換表的不同例的圖。

(元件符號說明)

10 半導體記憶卡(保全記憶卡)

11 TRM40 的 IC 部

12 I/F 部

13 IC 指令處理部

14 檔案管理部

15 IC 認證部

16 記憶體管理部

17 密碼/解碼電路

18 內部非揮發性記憶體 I/F 部

20 控制部

21 資料 I/F 部

22 指令 I/F 部

23 控制認證部

24 控制指令處理部

25 存取控制部

26　大容量非揮發性記憶體 I/F 部

30　內部 CPU

40　耐干擾性模組（TRM）

41　內部非揮發性記憶體

50　大容量非揮發性記憶體

51　保全區域

52　認證區域

53　非認證區域

54　位址資訊管理區域

60　外部 CPU

61　行動電話

62　ROM

63　RAM

64　液晶顯示部

65　無線通信部

66　操作鍵

67　卡 I/F 部

68　認證電路

69　R/W 裝置

70　內部匯流排

91　充值用終端

92　充值伺服器

93　結帳伺服器

94　配信伺服器

95　網絡

621　指令生成程式

622　認證鍵群

伍、中文發明摘要：

本發明之目的在於，提供記憶容量大且具備有與IC卡同等保全等級之記憶區域的記憶卡。

在可裝卸於電子機器的半導體記憶卡10，設置具有可從電子機器進行存取的正常區域52、53和無法從電子機器直接存取的保全區域51的非耐干擾性的第1記憶體50；及無法從電子機器直接存取的耐干擾性的第2記憶體41；而對第1記憶體50的保全區域51的存取，僅介由管理對第2記憶體41的存取的保全控制部30才可進行。該保全區域51因為外部機器無法直接存取，因此較認證區域52的保全等級高。另外，由於該保全區域51係設於非耐干擾性的記憶體50，因此可取得大的記憶容量。

陸、英文發明摘要：

拾、申請專利範圍：

1.一種記憶裝置，其係固定或可裝卸地連接於電子機器者，其特徵為具備：

非耐干擾性的第1記憶體，其具有可從上述電子機器存取的正常區域、和無法從上述電子機器直接存取的保全區域；

耐干擾性的第2記憶體，其無法從上述電子機器直接存取；及

保全控制部，其管理對上述第2記憶體的存取；且

從上述電子機器對上述第1記憶體的保全區域的存取，僅介由上述保全控制部才可進行。

2.如申請專利範圍第1項之記憶裝置，其中，上述保全控制部接受上述保全控制部認證的電子機器的指令，對上述保全區域或第2記憶體作存取，進行資料的寫入或讀出。

3.如申請專利範圍第1項之記憶裝置，其中，上述第2記憶體內儲存有密碼鍵，

上述保全控制部係使用上述密碼鍵以將寫入上述保全區域的資料密碼化後予以寫入，並且，使用上述密碼鍵將從上述保全區域讀出的資料解碼。

4.如申請專利範圍第1項之記憶裝置，其中，上述保全控制部係計算寫入上述保全區域的資料的雜湊值，將上述雜湊值儲存於上述第2記憶體，並計算從上述保全區域讀出的資料的雜湊值，與儲存於上述第2記憶體的雜湊值核對。

5.如申請專利範圍第1項之記憶裝置，其中，上述第1記憶體的正常區域包含僅藉由控制記憶裝置的全體控制部所認證的電子機器可存取的認證區域；及連未受到認證的電子機器也可存取的非認證區域。

6.如申請專利範圍第1項之記憶裝置，其中，顯示上述正常區域與上述保全區域之境界的境界位址資訊；和敘述上述正常區域及保全區域之各個邏輯位址與物理位址關係的邏輯-物理位址變換表，係作為上述第1記憶體的位址資訊而被管理。

7.如申請專利範圍第6項之記憶裝置，其中，上述第1記憶體的位址資訊包含有：顯示上述認證區域與上述非認證區域之境界的境界位址資訊；及上述認證區域與上述非認證區域的各個邏輯-物理位址變換表。

8.如申請專利範圍第6項之記憶裝置，其中，上述境界位址資訊及邏輯-物理位址變換表，係記錄於上述第1記憶體的位址資訊管理區域。

9.如申請專利範圍第6項之記憶裝置，其中，由上述境界位址資訊所表示之上述正常區域與上述保全區域的境界，係由接受上述保全控制部之認證的電子機器的指令來變更。

10.如申請專利範圍第7項之記憶裝置，其中，由上述境界位址資訊所表示的上述認證區域與上述非認證區域的境界，係由接受上述全體控制部之認證的電子機器的指令來變更。

11.如申請專利範圍第10項之記憶裝置，其中，上述認證區域與上述非認證區域之境界的境界位址資訊，係由實際境界位址及除保全區域外所設定的虛設境界位址所構成，

依接受上述全體控制部之認證的電子機器的指令所指定的上述虛設境界位址，藉以改變上述實際境界位址。

12.一種電子機器，其係對具有第1區域、第2區域及第3區域作為記憶區域的記憶裝置進行存取者，其特徵為：

當上述電子機器接受對記憶裝置的存取要求時，

在記憶裝置之作為非耐干擾性之記憶區域的第1區域，介由控制對記憶裝置之存取的記憶裝置的全體控制部進行存取；

在接受上述全體控制部及控制對第2區域和第3區域之存取的記憶裝置的保全控制部的認證後，在第1區域以外之作為非耐干擾性之記憶區域的上述第2區域，介由保全控制部進行存取；

經由與上述保全控制部的認證後，在記憶裝置之作為耐干擾性之記憶區域的上述第3區域，介由上述全體控制部及上述保全控制部進行存取。

13.如申請專利範圍第12項之電子機器，其具備有：

第1指令生成機構，其生成對第1區域寫入或讀出資料的指令；

第2指令生成機構，其生成對保全控制部要求處理的指令；及

第 1 認證處理機構，其取得用於和上述保全控制部之認證的認證鍵，進行和上述保全控制部的認證處理。

14. 如申請專利範圍第 12 項之電子機器，其中，在作為第 1 區域之部分區域的非認證區域，進行不經由與全體控制部之認證的存取，在非認證區域以外之作為第 1 區域之部分或全部區域的認證區域，進行經由與全體控制部之認證後的存取。

15. 如申請專利範圍第 14 項之電子機器，其具備：

第 3 指令生成機構，其生成對認證區域寫入或讀出資料的指令；及

第 2 認證處理機構，其取得用於和全體控制部之認證的認證鍵，進行和上述全體控制部的認證處理。

拾壹、圖式：

圖 1

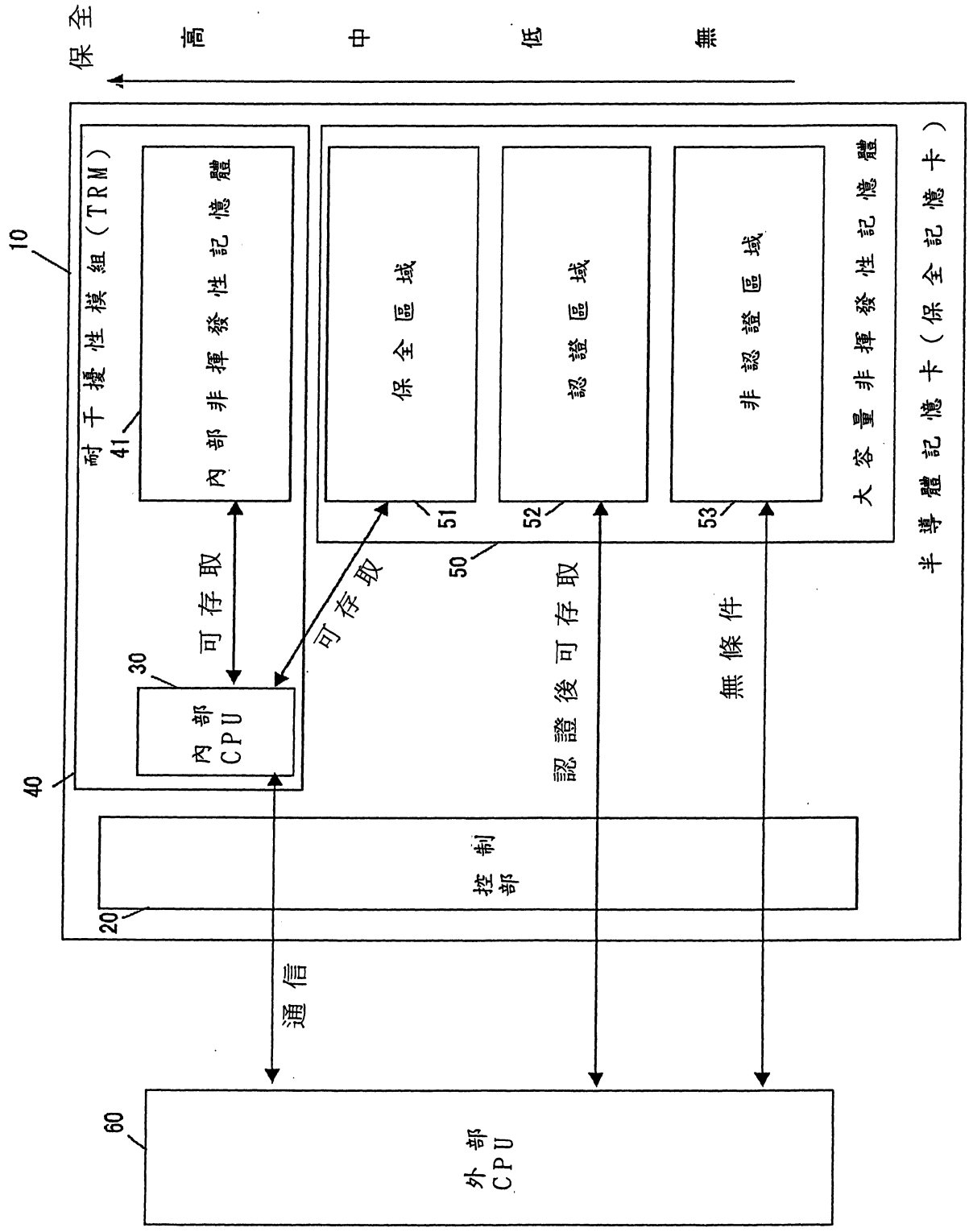

保全
高
中
低
無
10
耐干擾性模組（TRM）
41
內部非揮發性記憶體
30
內部CPU
40
可存取
可存取
50
保全區域
51
認證區域
52
非認證區域
53
大容量非揮發性記憶體
半導體記憶卡（保全記憶卡）
認證後可存取
無條件
控制部
20
通信
60
外部CPU

圖 2

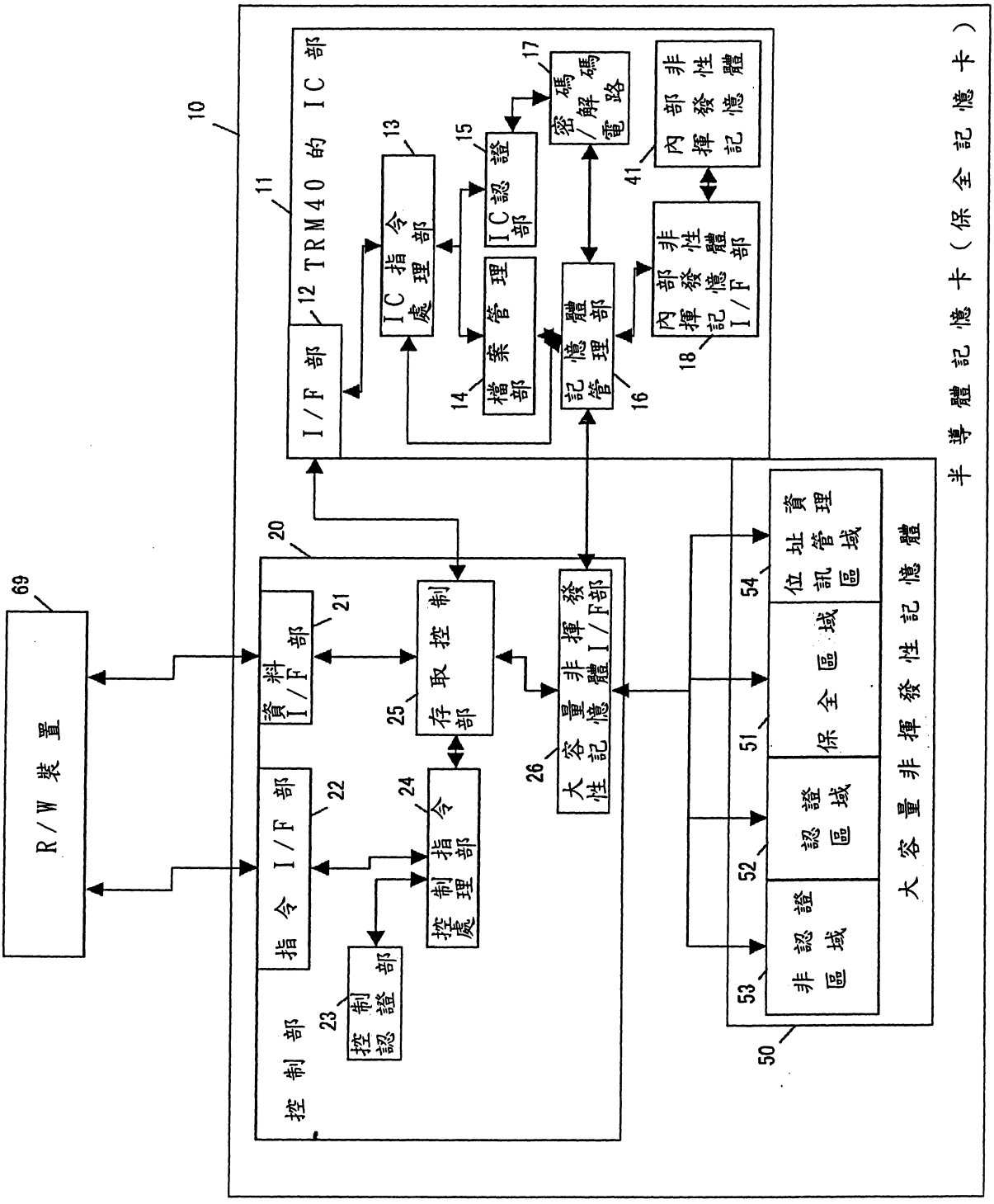

半導體記憶卡（保全記憶卡）
10
11 TRM40的IC部
12 I/F部
13 IC指令處理部
14 檔案管理部
15 IC認證部
16 記憶體管理部
17 密碼解電路
18 內部發憶非性體I/F部
41 內部非性體揮發憶記
20 控制部
21 資料I/F部
22 指令I/F部
23 控制認證部
24 控制指令處理部
25 控制取存部
26 大容量非揮發性記憶體I/F部
50 大容量非揮發性記憶體
51 保全區域
52 認證區域
53 非認證區域
54 位址資訊管理區域
69 R/W裝置

圖 3

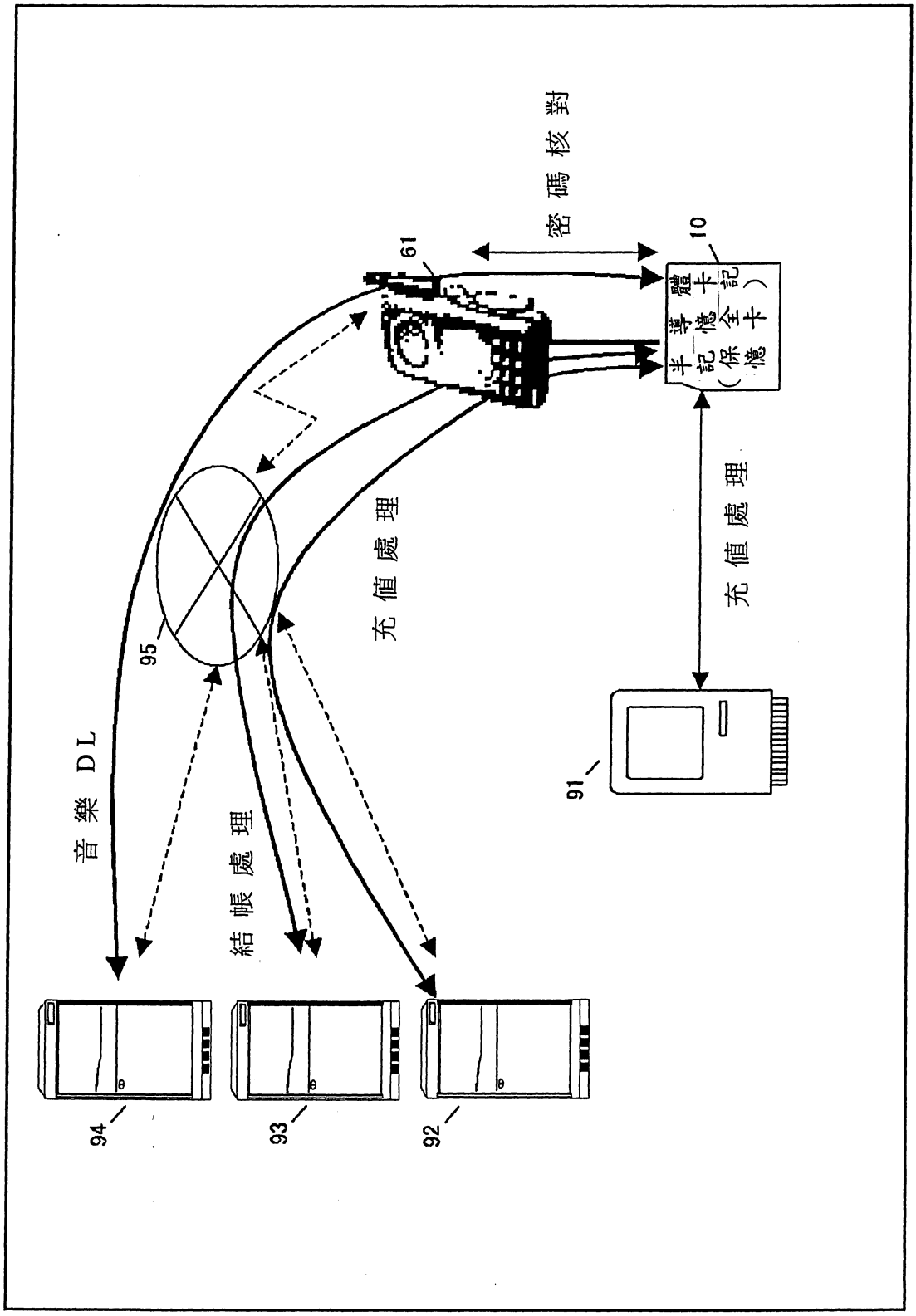


圖 4

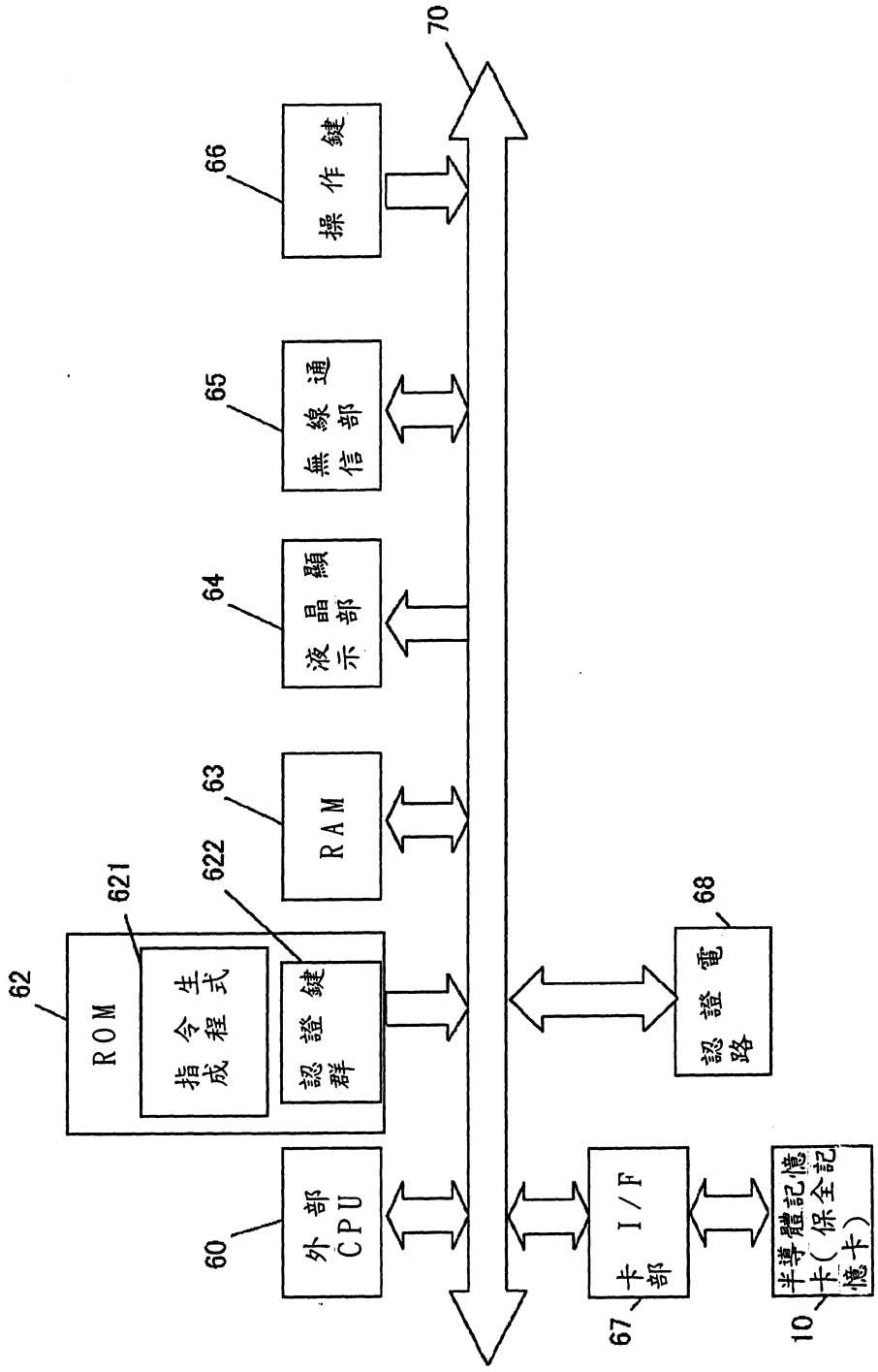

70
66
操作鍵
65
無線通信部
64
液晶顯示部
63
RAM
62
ROM
621
指令生成程式
622
認證鍵群
68
電認路
60
外部CPU
卡I/F部
67
半導體記憶卡(保全記憶卡)
10

圖 5

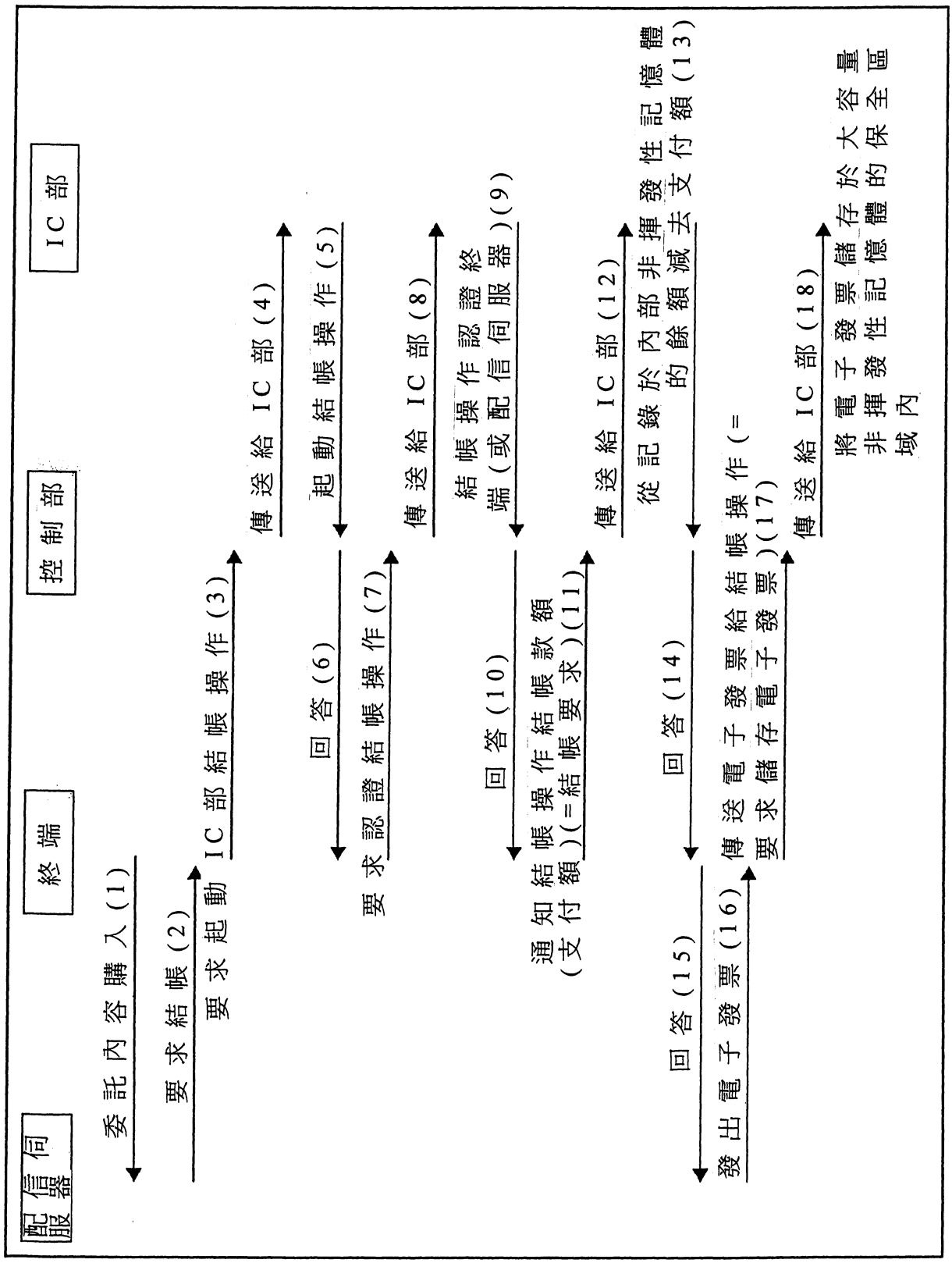

配信伺服器
終端
控制部
IC部
委託內容購入(1)
要求結帳(2)
IC部結帳操作(3)
傳送給IC部(4)
起動結帳操作(5)
回答(6)
要求認證結帳操作(7)
傳送給IC部(8)
結帳操作認證終端(或配信伺服器)(9)
回答(10)
通知結帳操作結帳款額(支付額)(=結帳要求)(11)
傳送給IC部(12)
從記錄於內部非揮發性記憶體的餘額減去支付額(13)
回答(14)
回答(15)
發出電子發票(16)
傳送電子發票給結帳操作(=要求儲存電子發票)(17)
傳送給IC部(18)
將電子發票儲存於大容量非揮發性記憶體的保全區域內

圖 6

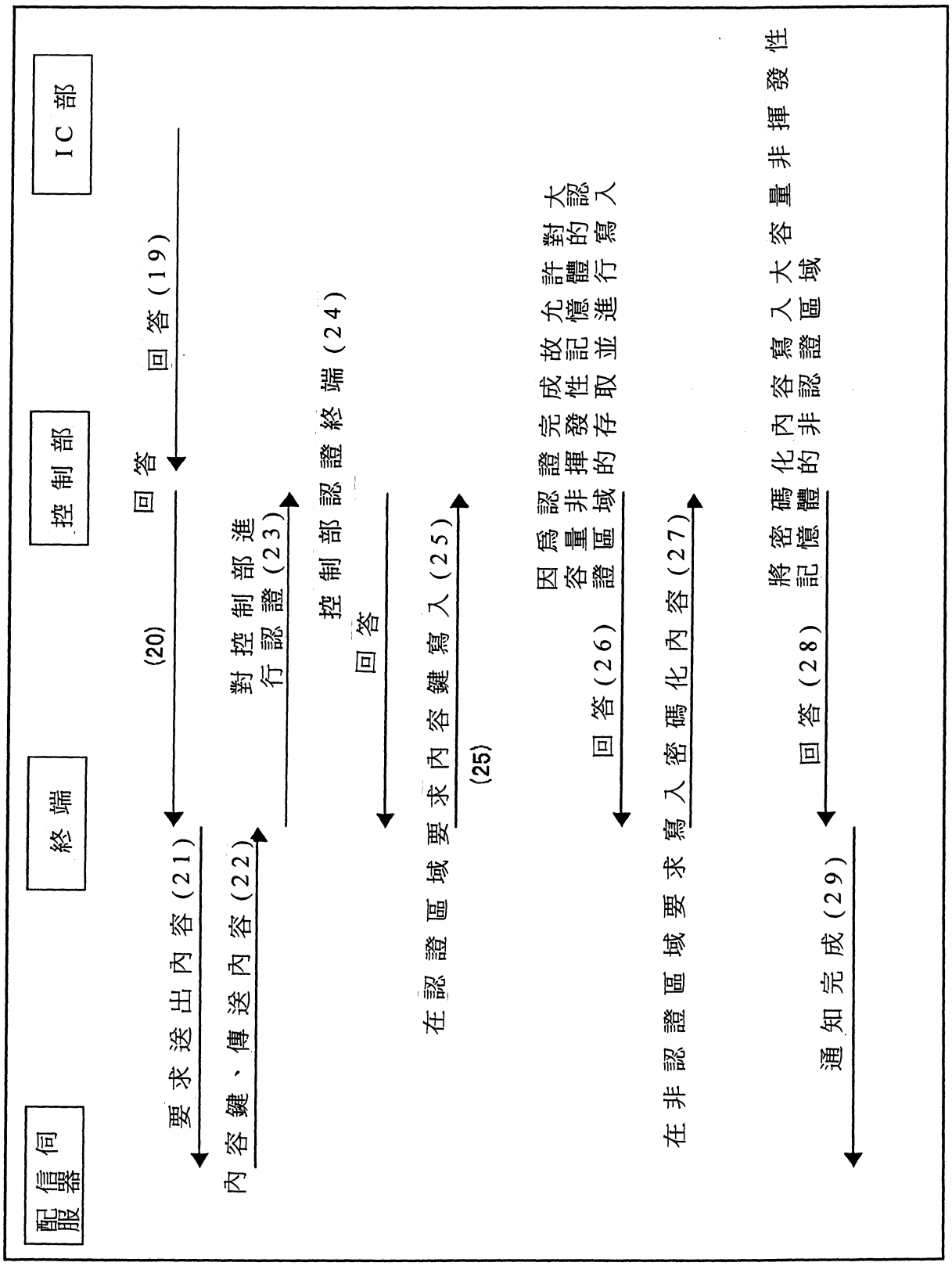

配信伺服器
終端
控制部
IC部
要求送出內容(21)
回答
回答(19)
(20)
內容鍵、傳送內容(22)
對控制部進行認證(23)
控制部認證終端(24)
回答
在認證區域要求內容鍵寫入(25)
(25)
因爲認證完成性故允許體對的認容量非揮發性記憶體並進行寫入
回答(26)
證區域的存取
在非認證區域要求寫入密碼化內容(27)
將密碼化內容寫入大容量非揮發性
回答(28)
記憶體的非認證區域
通知完成(29)

圖 7

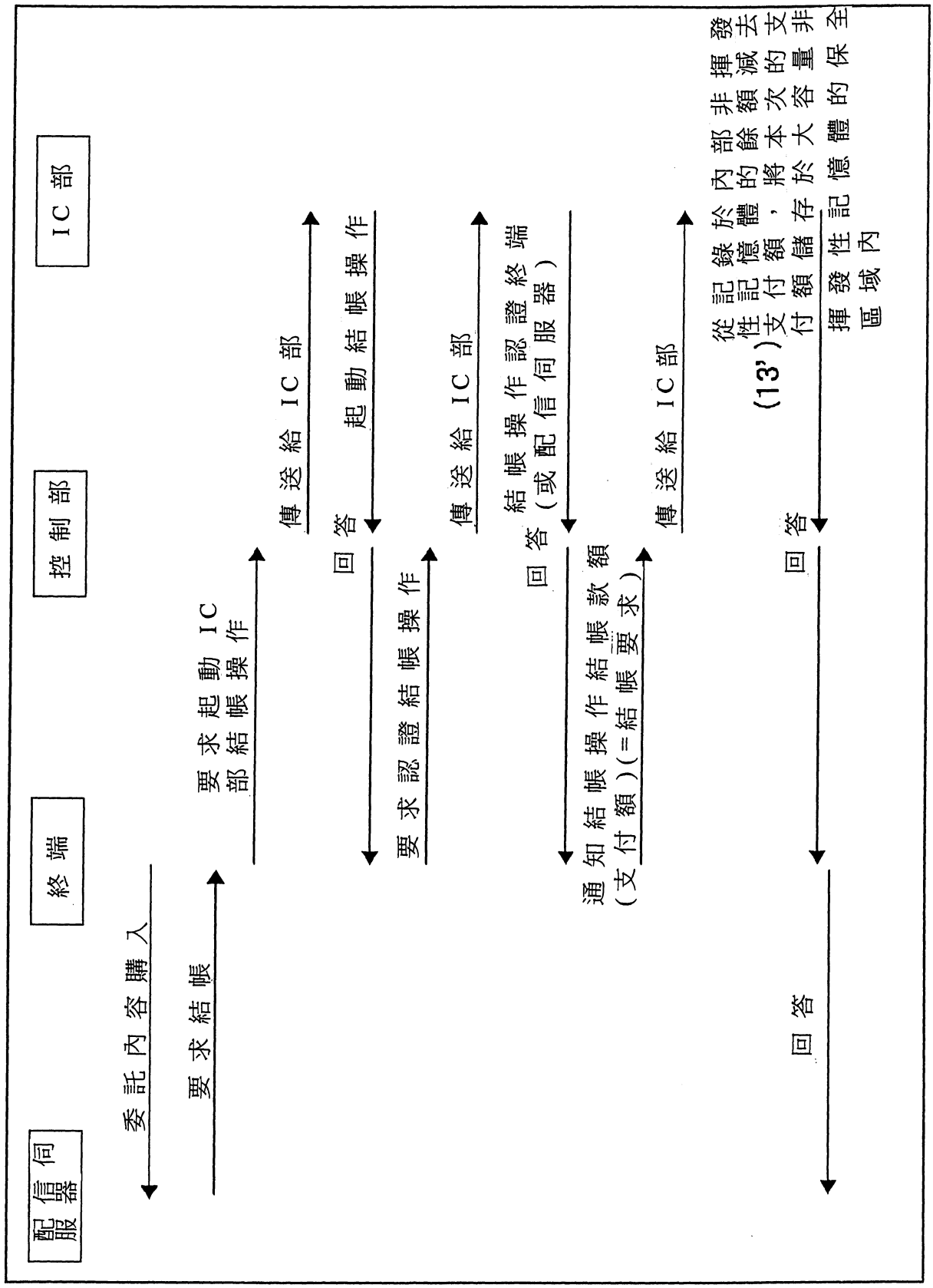

配信伺服器
終端
控制部
IC部
委託內容購入
要求結帳
要求起動IC部結帳操作
傳送給IC部
回答 起動結帳操作
要求認證結帳操作
傳送給IC部
結帳操作認證終端
回答(或配信伺服器)
通知結帳操作結帳款額(支付額)(=結帳要求)
傳送給IC部
回答
(13')從記錄於內部非揮發性記憶體的餘額減去支付額，將本次容量非揮發性記憶體的保全區域內支付額儲存於大
回答

圖 8

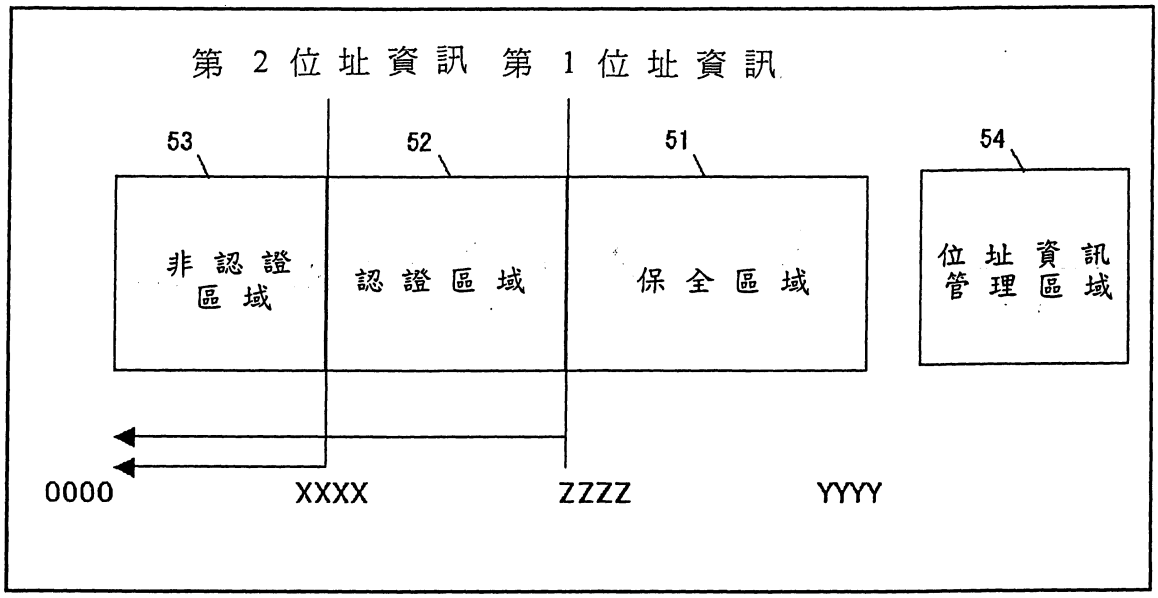

第 2 位址資訊
第 1 位址資訊
53
52
51
54
非認證區域
認證區域
保全區域
位址資訊管理區域
0000
XXXX
ZZZZ
YYYY

圖 9

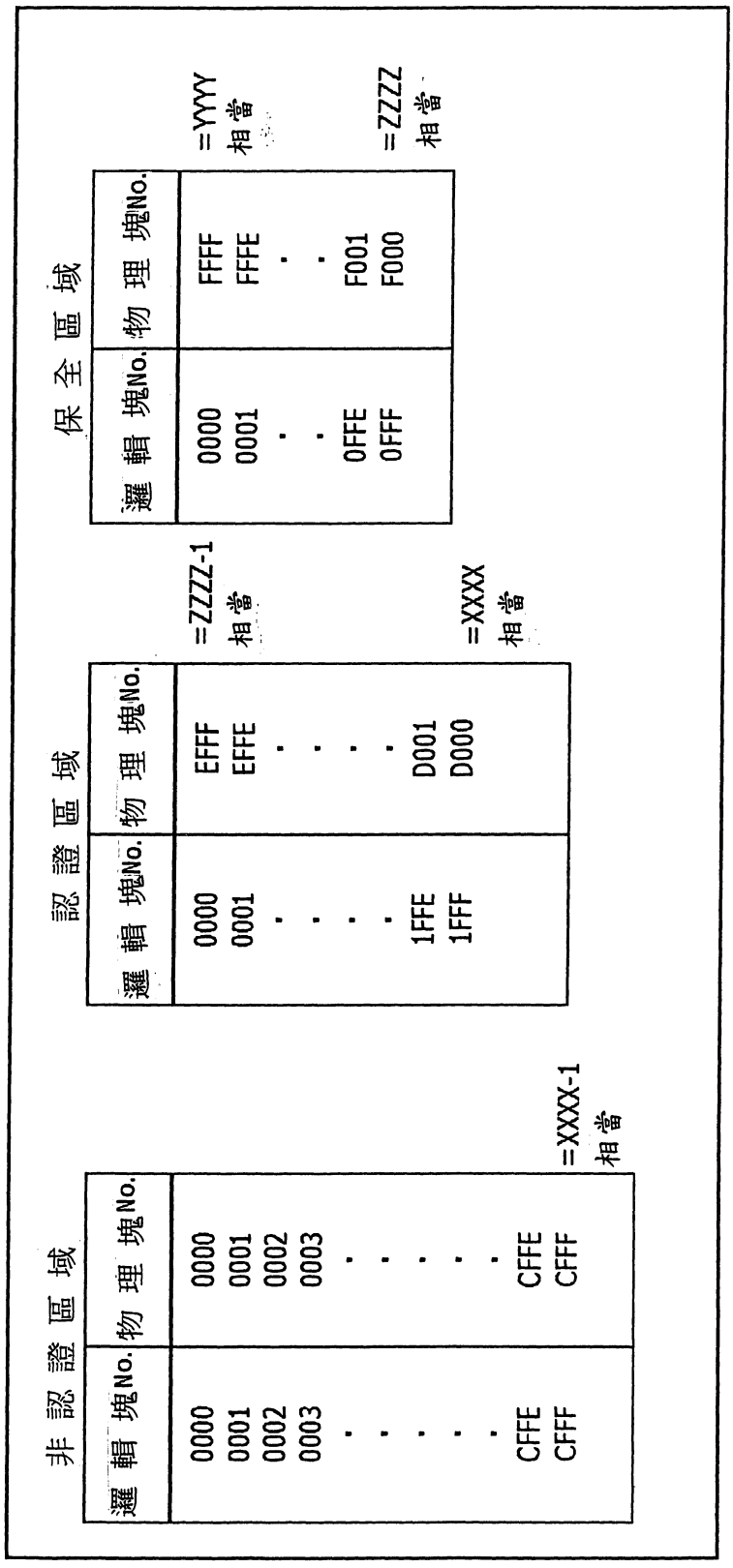

非認證區域
邏輯塊No.
物理塊No.
0000 0000
0001 0001
0002 0002
0003 0003
CFFE CFFE
CFFF CFFF
=XXXX-1 相當
認證區域
邏輯塊No.
物理塊No.
0000 EFFF
0001 EFFE
1FFE D001
1FFF D000
=ZZZZ-1 相當
=XXXX 相當
保全區域
邏輯塊No.
物理塊No.
0000 FFFF
0001 FFFE
OFFE F001
OFFF F000
=YYYY 相當
=ZZZZ 相當

圖１０

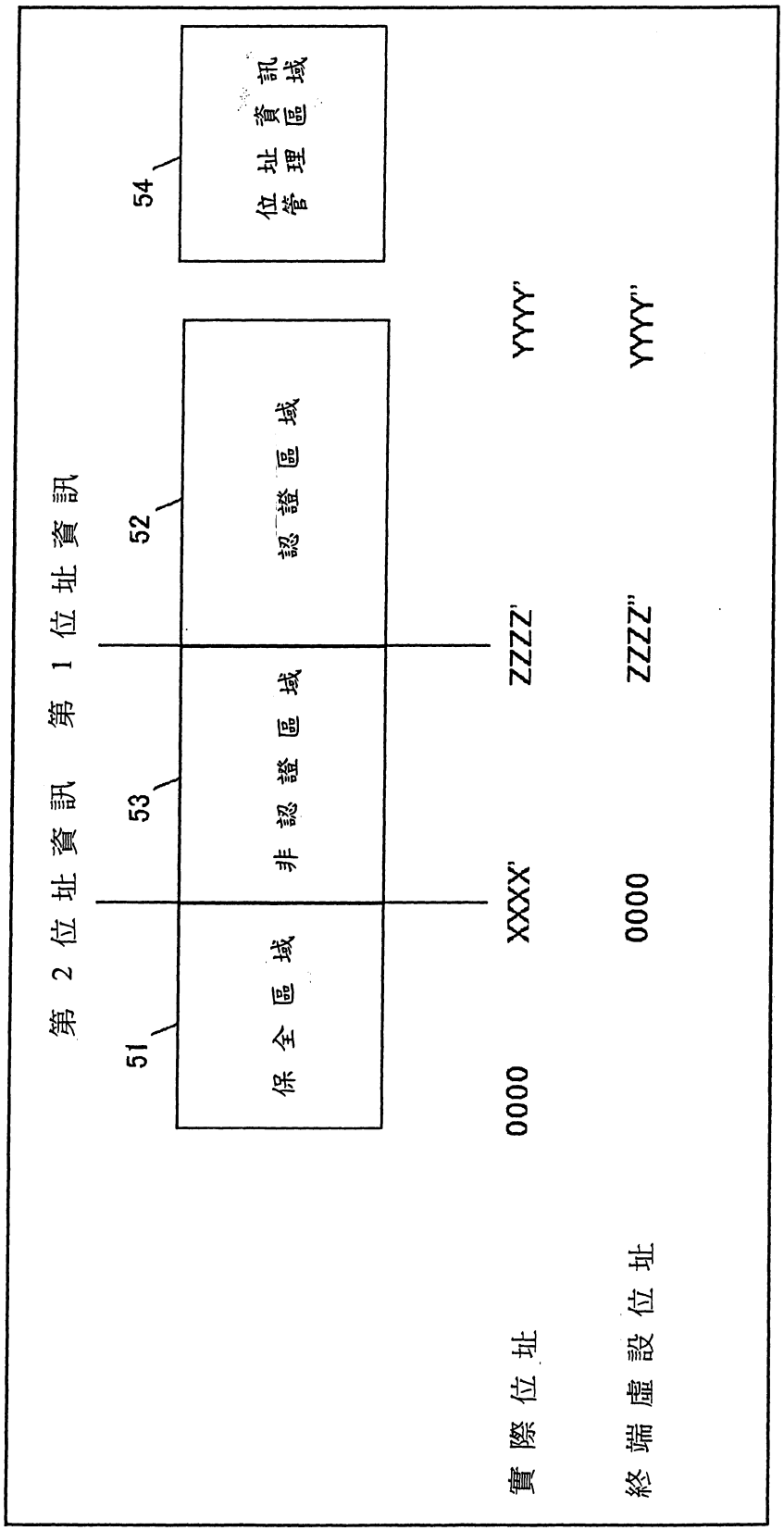

第２位址資訊
第１位址資訊
保全區域
51
非認證區域
53
認證區域
52
位址資訊管理區域
54
實際位址
0000
XXXX'
ZZZZ'
YYYY'
終端虛設位址
0000
ZZZZ''
YYYY''

圖11

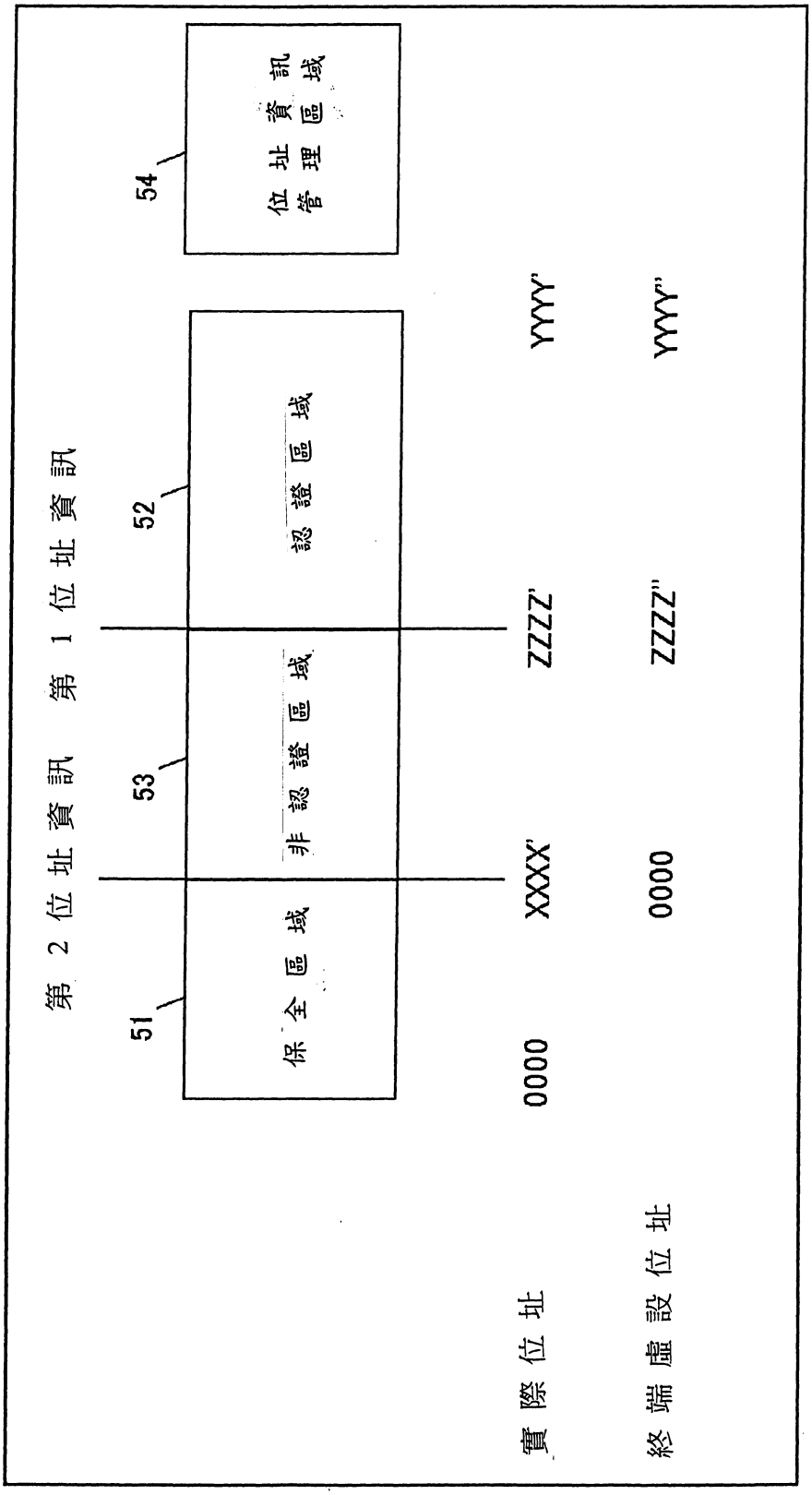
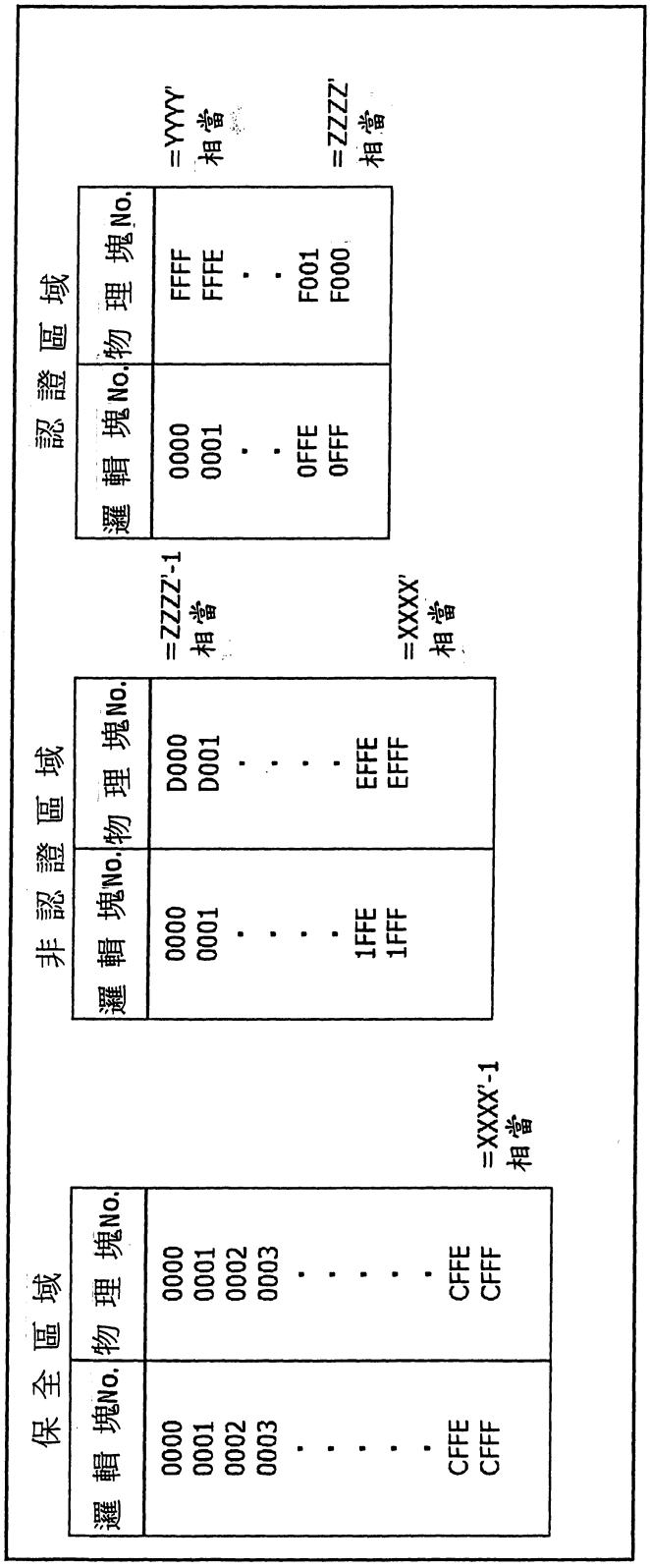

第2位址資訊
第1位址資訊
51
保全區域
53
非認證區域
52
認證區域
54
位址資訊管理區域
實際位址
0000
XXXX'
ZZZZ'
YYYY'
終端虛設位址
0000
ZZZZ''
YYYY''

圖12


保全區域
邏輯塊No.
物理塊No.
0000 0000
0001 0001
0002 0002
0003 0003
CFFE CFFE
CFFF CFFF
=XXXX'-1 相當
非認證區域
邏輯塊No.
物理塊No.
0000 D000
0001 D001
1FFE EFFE
1FFF EFFF
=ZZZZ'-1 相當
=XXXX' 相當
認證區域
邏輯塊No.
物理塊No.
0000 FFFF
0001 FFFE
0FFE F001
0FFF F000
=YYYY' 相當
=ZZZZ' 相當

柒、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 半導體記憶卡(保全記憶卡)
20 控制部
30 內部 CPU
40 耐干擾性模組(TRM)
41 內部非揮發性記憶體
50 大容量非揮發性記憶體
51 保全區域
52 認證區域
53 非認證區域
60 外部 CPU

捌、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

無