I750184

(19)中華民國智慧財產局

(12)發明說明書公告本　**(11)證書號數：TW I750184 B**

(45)公告日： 中華民國 110 (2021) 年 12 月 21 日

(21)申請案號：106118774　(22)申請日： 中華民國 106 (2017) 年 06 月 07 日

(51)Int. Cl.：　*G06F12/14　(2006.01)*

(30)優先權：2016/08/02　美國　62/370,230

2016/09/23　美國　15/275,337

(71)申請人：南韓商三星電子股份有限公司 (南韓) SAMSUNG ELECTRONICS CO., LTD.　(KR) 南韓

(72)發明人：歐拉利格　桑龐　保羅 OLARIG, SOMPONG PAUL (US)；張牧天 CHANG, MU-TIEN (TW)

(74)代理人：林孟閱；盧姵君；陳怡如

(56)參考文獻：

TW	I507876	TW	201346545A
US	2008/0195830A1	US	2010/0024028A1
US	2014/0289488A1	US	2015/0121537A1
US	2015/0294698A1		

審查人員：詹効儒

申請專利範圍項數：20 項　圖式數：10　共 59 頁

(54)名稱

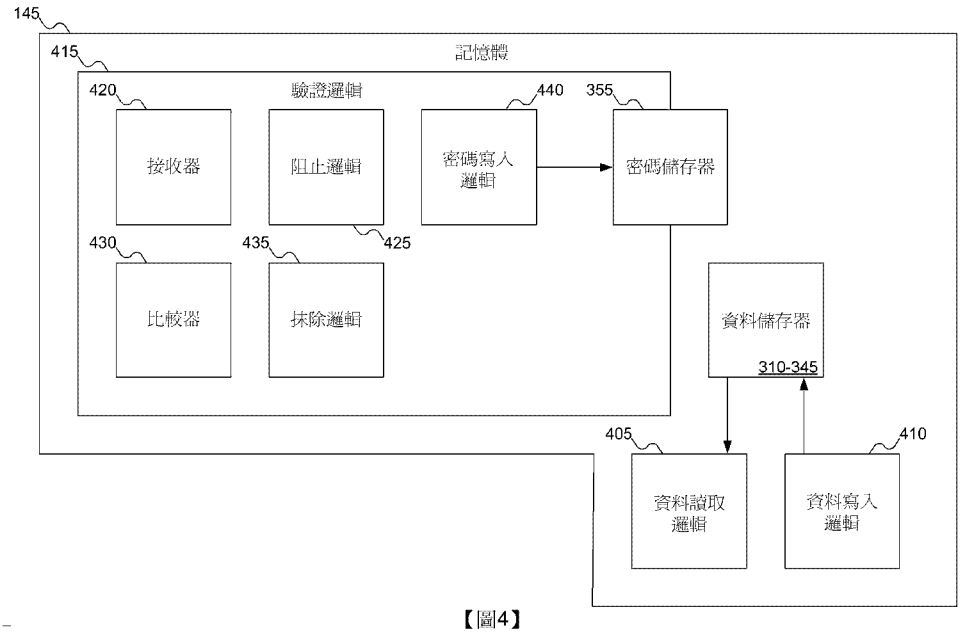
安全記憶體與智慧儲存裝置內執行資料擦除之方法

(57)摘要

揭露一種安全記憶體。所述記憶體可包括用於資料的資料儲存器、以及用於自所述資料儲存器讀取及寫入資料的資料讀取邏輯及資料寫入邏輯。密碼儲存器可所儲存密碼。接收器可自記憶體控制器接收所接收密碼。比較器可將所述所接收密碼與所述所儲存密碼進行比較。若所述所接收密碼不與所述所儲存密碼匹配，則抹除邏輯可抹除所述資料儲存器中的所述資料。最後，阻止邏輯可阻止自所述記憶體控制器存取所述記憶體，直至所述比較器完成自身的操作之後為止。

A secure memory is disclosed. The memory may include data storage for data, along with a data read logic and a data write logic to read and write data from the data storage. A password storage may store a stored password. A receiver may receive a received password from a memory controller. A comparator may compare the received password with the stored password. An erase logic may erase data in the data storage if the received password does not match the stored password. Finally, a block logic may block access to the memory from the memory controller until after the comparator completes its operation.

指定代表圖：



【圖4】

符號簡單說明：

145:記憶體

310-345:記憶體晶片/資料儲存器

355:儲存器/密碼儲存器

405:資料讀取邏輯

410:資料寫入邏輯

415:驗證邏輯

420:接收器

425:阻止邏輯

430:比較器

435:抹除邏輯

440:密碼寫入邏輯

專利案號：106118774

106年08月16日 修正

申請日：106年6月7日

I750184

公告本

IPC分類：G06F 12/14 (2006.01)

【發明摘要】

【中文發明名稱】安全記憶體與智慧儲存裝置內執行資料擦除之方法

【英文發明名稱】SECURED MEMORY AND METHOD OF EXECUTING DATA SCRUBBING INSIDE A SMART STORAGE DEVICE

【中文】揭露一種安全記憶體。所述記憶體可包括用於資料的資料儲存器、以及用於自所述資料儲存器讀取及寫入資料的資料讀取邏輯及資料寫入邏輯。密碼儲存器可所儲存密碼。接收器可自記憶體控制器接收所接收密碼。比較器可將所述所接收密碼與所述所儲存密碼進行比較。若所述所接收密碼不與所述所儲存密碼匹配，則抹除邏輯可抹除所述資料儲存器中的所述資料。最後，阻止邏輯可阻止自所述記憶體控制器存取所述記憶體，直至所述比較器完成自身的操作之後為止。

【英文】A secure memory is disclosed. The memory may include data storage for data, along with a data read logic and a data write logic to read and write data from the data storage. A password storage may store a stored password. A receiver may receive a received password from a memory controller. A comparator may compare the received password with the stored password. An erase logic may erase data in the data storage if the received

password does not match the stored password. Finally, a block logic may block access to the memory from the memory controller until after the comparator completes its operation.

【指定代表圖】圖4。

【代表圖之符號簡單說明】

145：記憶體

310-345：記憶體晶片/資料儲存器

355：儲存器/密碼儲存器

405：資料讀取邏輯

410：資料寫入邏輯

415：驗證邏輯

420：接收器

425：阻止邏輯

430：比較器

435：抹除邏輯

440：密碼寫入邏輯

【特徵化學式】

無

106-08-16

【發明說明書】

【中文發明名稱】安全記憶體與智慧儲存裝置內執行資料擦除之方法

【英文發明名稱】SECURED MEMORY AND METHOD OF EXECUTING DATA SCRUBBING INSIDE A SMART STORAGE DEVICE

[相關申請案資料]

本申請案主張於2016年8月2日提出申請的序列號為62/370,230的美國臨時專利申請案的權利，所述美國臨時專利申請案出於所有目的而併入本案供參考。

【技術領域】

【0001】 本發明概念大體而言是有關於記憶體，且更具體而言是有關於可得到保全以防止對儲存於記憶體中的資料的未授權存取的記憶體。

【先前技術】

【0002】 非揮發性記憶體（non-volatile memory，NVM）的內容是持久性的。當用作長期儲存器裝置時，預期且期望存在以下行為：需要保存資料。

【0003】 但在記憶體空間中使用非揮發性記憶體可能造成問題。經常出於安全原因，保持於記憶體空間中的諸多形式的資料傾向為暫態的。非揮發性記憶體打破了此假設且會在非揮發性記憶體

被偷走或非揮發性記憶體的資源被重新指配時造成風險。舉例而言，當資料實際上儲存於非揮發性記憶體上時，基於雲端的網頁服務可在被所述服務假設為揮發性記憶體的元件上儲存客戶資料。若在未明確清除記憶體內容的同時終止網頁服務，則就像例如非揮發性記憶體被偷走、或非揮發性記憶體的資源被給予另一雲使用者一樣，此資料可能被另一使用者獲得。

【0004】 仍需一種使記憶體得到保全以防止對記憶體模組、尤其是利用非揮發性記憶體的記憶體模組的未授權存取的方式。

【發明內容】

【0005】 本發明的記憶體，包括資料儲存器、資料讀取邏輯、資料寫入邏輯、密碼儲存器、接收器、比較器、抹除邏輯及阻止邏輯。資料儲存器，用於第一使用者的資料。資料讀取邏輯自所述資料儲存器讀取資料。資料寫入邏輯向所述資料儲存器寫入資料。密碼儲存器用於所儲存密碼。接收器自記憶體控制器接收所接收密碼。比較器將所述所接收密碼與所述所儲存密碼進行比較。若所述所接收密碼不同於所述所儲存密碼，則抹除邏輯抹除所述資料儲存器中的所述資料。阻止邏輯阻止自所述記憶體控制器存取所述資料儲存器，直至所述比較器完成操作之後為止。其中，所述所接收密碼或所述所儲存密碼不用於對儲存於所述記憶體中的資料進行加密。

【0006】 本發明的方法，包括下列步驟。確定記憶體已被重設。判斷所述記憶體正在以安全模式還是非安全模式運作。若所述記

憶體正在以所述安全模式運作，則選擇使用者的密碼、將所述密碼發送至所述記憶體、以及接收對所述記憶體的存取。其中，所述密碼不用於對儲存於所述記憶體中的資料進行加密。

【0007】 本發明的方法，包括下列步驟。自記憶體向記憶體控制器發送表示所述記憶體正在以安全模式運作的訊號。自所述記憶體控制器接收所接收密碼。將所述所接收密碼與所儲存密碼進行比較。若所述所接收密碼不與所述所儲存密碼匹配，則抹除所述記憶體、以及提供所述記憶體控制器對所述記憶體的存取。其中，所述所接收密碼或所述所儲存密碼不用於對儲存於所述記憶體中的資料進行加密。

【圖式簡單說明】

【0008】

圖 1 示出根據本發明概念的實施例的具有使用安全記憶體的各種主機（host machine）的資料中心。

圖 2 示出圖 1 所示主機的其他細節。

圖 3 示出圖 1 所示記憶體的細節。

圖 4 示出圖 1 所示記憶體的替代圖。

圖 5 示出圖 3 至圖 4 所示記憶體使用自圖 3 所示記憶體控制器接收的密碼來判斷準許存取儲存於圖 3 至圖 4 所示記憶體中的資料還是抹除儲存於圖 3 至圖 4 所示記憶體中的資料。

圖 6 示出根據本發明概念實施例的圖 1 所示可在兩個使用者之間共享資源的記憶體的例子。

圖 7A 至圖 7C 示出根據本發明概念實施例的圖 3 所示記憶體控制器請求對圖 1 所示記憶體的存取的示例性過程的流程圖。

圖 8 示出根據本發明概念實施例的圖 3 所示記憶體控制器選擇密碼來請求對圖 1 所示記憶體的存取的示例性過程的流程圖。

圖 9A 至圖 9C 示出根據本發明概念實施例的圖 1 所示記憶體判斷準許圖 3 所示記憶體控制器存取資料還是抹除資料的示例性過程的流程圖。

圖 10 示出根據本發明概念實施例的圖 4 所示抹除邏輯自圖 1 所示記憶體抹除資料的示例性過程的流程圖。

【實施方式】

【0009】 現將詳細參照本發明概念的實施例，所述實施例的例子示於附圖中。在以下詳細說明中，提出諸多具體細節以使得能夠達成對本發明概念的透徹理解。然而，應理解，此項技術中具有通常知識者可在不使用該些具體細節的條件下實踐本發明概念。在其他實例中，未對眾所習知的方法、過程、組件、電路、及網路予以詳細闡述，以避免使所述實施例的各個態樣不必要地模糊。

【0010】 應理解，儘管本文中可能使用用語「第一」、「第二」等來闡述各種元件，然而該些元件不應受該些用語限制。該些用語僅用於區分各個元件。舉例而言，在不背離本發明概念的範圍的條件下，可將第一模組稱為第二模組，且相似地，可將第二模組稱為第一模組。

【0011】 本文中在對本發明概念的說明中使用的術語僅用於闡述

具體實施例而非旨在限制本發明概念。除非上下文中清楚地另外指示，否則在對本發明概念及隨附申請專利範圍的說明中使用的單數形式「一（a、an）」及「所述（the）」旨在亦包含複數形式。亦應理解，本文所用用語「及/或（and/or）」指代且囊括相關所列項中一或多個項的任意及全部可能組合。更應理解，當在本說明書中使用用語「包括（comprises 及/或 comprising）」時，是指明所陳述特徵、整數、步驟、操作、元件、及/或組件的存在，但不排除一或多個其他特徵、整數、步驟、操作、元件、組件、及/或其群組的存在或添加。所述圖式的組件及特徵未必按比例繪製。

【0012】 安全非揮發性記憶體（NVM）模組可用於記憶體空間中。非揮發性記憶體可配備有密碼及驗證邏輯（authentication logic）：來自非揮發性記憶體的資料可僅當使用者具有匹配密鑰時被存取。

【0013】 安全模組的控制流程可按照以下進行：

1）記憶體控制器在重設（例如加電（power-up）等由硬體引發的重設、或由軟體引發的重設）時讀取雙列直插記憶體模組（Dual In-Line Memory Module，DIMM）的串列存在偵測（Serial Presence Detect，SPD），以判斷所述雙列直插記憶體模組是否具有安全模式。

【0014】 2）若雙列直插記憶體模組不具有安全模式，則系統正常運作。

【0015】 3）否則，記憶體控制器藉由新定義的模式暫存器設定

（Mode Register Set，MRS）命令將密碼發送至雙列直插記憶體模組。

【0016】 4）若密碼被識別，則雙列直插記憶體模組被解鎖且所述雙列直插記憶體模組作為常規雙列直插記憶體模組而運作。雙列直插記憶體模組可將表示準許對記憶體控制器的存取的訊號發送至所述記憶體控制器。「驗證」訊號可經由 DQ 匯流排（DQ bus）來遞送。所述系統可接著正常運作。

【0017】 5）若密碼未被識別，則雙列直插記憶體模組可要求記憶體控制器進行重試。重試訊號亦可經由 DQ 匯流排來發送。記憶體控制器可接著亦藉由模式暫存器設定命令來重新發送所述密鑰。

【0018】 6）若重試次數超過臨限值，則雙列直插記憶體模組可停止允許記憶體控制器進行重試。相反，雙列直插記憶體模組可經由 DQ 匯流排而將「未授權」訊號發送至記憶體控制器。雙列直插記憶體模組可接著在準許記憶體控制器對所述雙列直插記憶體模組的存取之前抹除自身的內容。

【0019】 圖 1 示出根據本發明概念實施例的具有使用安全記憶體的各種主機的資料中心。在圖 1 中，資料中心 105 可包括各種主機（其亦可被稱作伺服器），例如主機 110、115、120、及 125。資料中心 105 可支援可由任意使用者使用的客戶機（client machine），例如客戶機 130。客戶機 130 的使用者可有效地自資料中心 105「租賃（lease）」資源來達成任意所需服務。舉例而言，

資料中心 105 可使得使用者能夠購買可遞送至他或她家中的產品；資料中心 105 可將記憶體「租賃」給使用者以在選擇使用者的購買項並完成支付的同時儲存使用者的購物車。儘管圖 1 示出包括四個主機 110、115、120 及 125、以及一個客戶機 130 的資料中心 105，本發明概念的實施例可支援任意數目的主機及/或客戶機。由於出於本發明的目的主機 110、115、120、及 125 是可互換的，因此進一步提及主機 110 旨在亦包括提及主機 115、120、及 125。

【0020】 圖 1 示出包括網路 135 的資料中心 105。網路 135 可採取任意所需形式，包括區域網路（Local Area Network，LAN）、廣域網路（Wide Area Network，WAN）、例如網際網路等的全域網路、及有線網路或無線網路。另外，網路 135 可為該些網路中的任意者的組合，以容許資料中心 105 進行分散而非位於單一地理位置。

【0021】 圖 1 亦示出主機 110 的細節，儘管相同的細節亦可在資料中心 105 內的主機 110、115、120、及 125 中的任意者內找到。主機 110 被示出為包括處理器 140、記憶體 145、電子可抹除可程式化唯讀記憶體（Electronically Erasable Programmable Read Only Memory，EEPROM）150、及儲存裝置 155。處理器 140 可為任一種處理器：例如，英特爾至強（Intel Xeon）、賽揚（Celeron）、安騰（Itanium）或淩動（Atom）處理器、或者 AMD 皓龍（Opteron）處理器、ARM 處理器等。記憶體 145 可為任一種記憶體，例如動態隨機存取記憶體（Dynamic Random Access Memory，DRAM）、

持續隨機存取記憶體（Persistent Random Access Memory，PRAM）、靜態隨機存取記憶體（Static Random Access Memory，SRAM）、鐵電式隨機存取記憶體（Ferroelectric Random Access Memory，FRAM）、或例如磁阻式隨機存取記憶體（Magnetoresistive Random Access Memory，MRAM）等非揮發性隨機存取記憶體（Non-Volatile Random Access memory，NVRAM）。另外，記憶體145可為混合記憶體，包括單一記憶體模組中的揮發性記憶體裝置與非揮發性記憶體裝置的任意所需組合。但與傳統記憶體模組相比，記憶體 145 可為如下所述的安全記憶體模組。儲存裝置 155 在其他可能性中可為任一種儲存裝置，包括傳統硬碟驅動機或快閃記憶體。

【0022】 電子可抹除可程式化唯讀記憶體 150 可儲存重要產品資料（Vital Product Data，VPD）160。儘管如下所述的記憶體 145 可自身指明記憶體 145 是否是安全記憶體，然而重要產品資料 160 可提供此資訊的替代來源。儘管圖 1 示出重要產品資料 160 被儲存於電子可抹除可程式化唯讀記憶體 150 中，然而本發明概念的實施例可使用任意替代性儲存媒體來進行支援。舉例而言，電子可抹除可程式化唯讀記憶體 150 可被例如可抹除可程式化唯讀記憶體（Erasable Programmable Read Only Memory，EPROM）或快閃記憶體等替代品取代。

【0023】 圖 2 示出圖 1 所示主機 110、115、120、及 125 的其他細節。參照圖 2，通常，主機 110、115、120、及 125 包括一或多個

處理器 140，所述一或多個處理器 140 可包括記憶體控制器 205 及時鐘 210，記憶體控制器 205 及時鐘 210 可用於協調主機 110、115、120、及 125 的各組件的運作。處理器 140 亦可耦合至記憶體 145，記憶體 145 可包括例如隨機存取記憶體（random access memory，RAM）、唯讀記憶體（read-only memory，ROM）、或其他狀態保存媒體。處理器 140 亦可耦合至儲存裝置 155 且耦合至網路連接器 215，網路連接器 215 可為例如乙太網路連接器（Ethernet connector）或無線連接器。處理器 140 亦可在其他組件間亦連接至匯流排 220，可使用輸入/輸出引擎 230 來管理的使用者介面 225 及輸入/輸出介面埠可附接至匯流排 220。

【0024】 圖 3 示出圖 1 所示記憶體 145 的細節。在圖 3 中，記憶體 145 可包括暫存器時脈驅動器（register clock driver，RCD）305 以及記憶體晶片 310、315、320、325、330、335、340、及 345。儘管圖 3 示出以八個晶片來儲存資料的典型動態隨機存取記憶體模組，然而本發明概念的實施例可包括其他類型的記憶體模組且包括任意所需數目的晶片或晶片替代品。

【0025】 記憶體控制器 205 可與記憶體 145 介接。記憶體控制器 205 可發送命令以對記憶體晶片 310-345 直接讀取及寫入資料。記憶體控制器 205 亦可介接暫存器時脈驅動器 305 以使用命令/位址訊號及時脈訊號來與。

【0026】 在記憶體 145 已執行重設操作之後，記憶體控制器 205 可判斷記憶體 145 是否正在以安全模式運作。所述重設操作可為

由硬體引發的重設（例如，當圖 1 所示主機 110 最初加電時）、或由軟體引發的重設（例如，當記憶體控制器 205 通知記憶體 145 使用者對資源的租賃已結束時（以下所進一步闡述））。記憶體控制器 205 可藉由詢問串列存在偵測（SPD）350 來判斷記憶體 145 是否正在以安全模式運作。作為另一選擇，如以上參照圖 1 所述，記憶體控制器 205 可自電子可抹除可程式化唯讀記憶體 150 存取圖 1 所示重要產品資料 160，重要產品資料 160 可指示記憶體 145 是否正在以安全模式運作。

【0027】 若記憶體 145 未正在以安全模式運作，則記憶體控制器 205 可按照傳統慣例來存取記憶體 145。但若記憶體 145 正在以安全模式運作，則記憶體控制器 205 可嘗試驗證至記憶體 145 以得到存取權限。（應注意，在此上下文中，「驗證以得到存取權限」並非暗示可拒絕記憶體控制器 205 對記憶體 145 的存取，而是如下所述暗示記憶體控制器 205 可僅在記憶體 145 已抹除任意之前的資料之後得到對記憶體 145 存取的權限）。記憶體控制器 205 可藉由模式暫存器設定（MRS）命令將密碼發送至暫存器時脈驅動器 305。暫存器時脈驅動器 305 可接著將所接收密碼與儲存於儲存器 355 中的密碼進行比較。若所接收密碼匹配所儲存密碼，則可準許記憶體控制器 205 對記憶體 145 的存取：此訊號可經由 DQ 匯流排來發送。否則，記憶體 145 可抹除儲存於記憶體晶片 310-345 中的任意資料，在此之後，可準許記憶體控制器 205 對記憶體 145 的存取。

【0028】 為方便將來的存取，暫存器時脈驅動器 305 亦可將所接收密碼儲存於儲存器 355 中，進而使得記憶體控制器 205 能夠在將來使用所接收密碼來驗證至記憶體 145。暫存器時脈驅動器 305 亦可將現有密碼覆蓋寫入儲存器 355 中，進而防止在將來接受較舊的所儲存密碼。抹除所儲存密碼亦可作為抹除儲存於記憶體 145 中的資料的一部分，進而再次防止在將來接受較舊的所儲存密碼。

【0029】 記憶體控制器 205 可以任意所需方式產生密碼。示例性方式可為產生隨機密碼、自預定密碼清單選擇密碼、產生使用者 ID 的雜湊、或使用可信賴平台模組（Trusted Platform Module，TPM）來產生密碼。本發明概念的實施例亦可支援其他技術來產生密碼。

【0030】 本發明概念的實施例相較於傳統系統而言具有若干優點。藉由提供用於保全記憶體 145 的機制，一個使用者可能讀取另一使用者的資料的危險顯著降低。但由於使用者的資料並非在儲存於記憶體中時被加密，因此無需包括加密邏輯來管理所加密資料。無需對資料進行加密亦會減少自記憶體 145 存取資料所需的時間，乃因無需為執行加密/解密而花費任何時間。

【0031】 傳統系統的一個有用的類比可為將記憶體與銀行的保險箱系統相比。為自銀行中的保險箱存取東西，必須呈現此箱的鑰匙。若使用者此時需要對不同箱中的資料進行存取，則必須關閉第一箱並打開下一箱。此與對資料進行加密的傳統系統相似：要存取任意特定片段資料，則必須對此資料進行解密，此會減慢存

取速度。

【0032】 相比之下，可將記憶體 145 與房屋相比，且將用於存取記憶體 145 的密碼與門的鑰匙相比。在將門解鎖之前，房屋中的內容物是受保護的。一旦門被解鎖，則資料可被無延遲地自由存取：由於所述資料未被加密，因此不會引起進一步的延遲。

【0033】 圖 4 示出圖 1 所示記憶體 145 的替代圖。與示出記憶體 145 的具體實施例的圖 3 相比，圖 4 示出記憶體 145 的更抽象表示形式。記憶體 145 可包括可儲存實際使用者資料的資料儲存器 310-345、以及可自資料儲存器 310-345 讀取及寫入資料的資料讀取邏輯 405 及資料寫入邏輯 410。

【0034】 記憶體 145 亦可包括驗證邏輯 415，驗證邏輯 415 可判斷是否將準許使用者對記憶體 145 進行存取。如上所述，「被準許的存取（granted access）」並非意指存在可能不容許使用者使用記憶體 145 的可能性，而是意指記憶體 145 可在準許使用者進行存取之前抹除資料儲存器 310-345 中的任意資料。驗證邏輯 415 可包括接收器 420、阻止邏輯 425、比較器 430、及抹除邏輯 435。接收器 420 可自圖 3 所示記憶體控制器 205 接收密碼。在驗證邏輯 415 判斷是否在準許圖 3 所示記憶體控制器 205 準許存取之前應對資料儲存器 310-345 進行抹除的同時，阻止邏輯 425 可阻止自圖 3 所示記憶體控制器 205 對記憶體 145 進行存取。比較器 430 可將自圖 3 所示記憶體控制器 205 接收的密碼與儲存於密碼儲存器 355 中的密碼進行比較以查看所述密碼是否匹配。若所述密碼不匹

配，則抹除邏輯 435 可在準許圖 3 所示記憶體控制器 205 對記憶體 145 進行存取之前抹除資料儲存器 310-345 的內容。

【0035】 抹除邏輯 435 可以對於記憶體 145 所採用的形式而言適宜的任意方式運作。舉例而言，若記憶體 145 僅使用揮發性記憶體，則抹除邏輯 435 可藉由以下來有效地對記憶體 145 進行抹除：防止資料儲存器 310-345 中的值再新直至儲存於資料儲存器 310-345 中的所有值皆丟失，即不再儲存儲存於資料儲存器 310-345 中任意值。（此將耗時多久可相依於資料儲存器 310-345 的具體類型及形式、以及例如與資料儲存器 310-345 的製造相關聯的偏心率（eccentricity）等其他因素。舉例而言，若記憶體 145 使用揮發性記憶體且處於冷環境中，則抹除邏輯 435 可能需要向記憶體 145 寫入值以抹除記憶體 145，乃因記憶體 145 的內容可能無法在合理時間量內被破解）。在本發明概念的其他實施例中，抹除邏輯 435 可視需要使用例如 0 或 1 等常數值對儲存於資料儲存器 310-345 中的所有者進行覆蓋寫入。在本發明概念的再一實施例中，抹除邏輯 435 可執行所設計的寫入序列以抹除任意值。此種序列的例子可包括由美國國防部（Department of Defense，DoD）或其他政府機構及非政府組織設計的序列。舉例而言，此序列可包括寫入所有零、接著寫入所有一、再接著將隨機圖案寫入記憶體中。在本發明概念的可與快閃記憶體一起使用的再一實施例中，記憶體 145 中的所有資料區塊（或至少含有有效資料的區塊）可在可準許圖 3 所示記憶體控制器 205 對記憶體 145 進行存取之

前立即經歷垃圾收集（garbage collection）。

【0036】 驗證邏輯 415 亦可包括密碼寫入邏輯 440。密碼寫入邏輯 440 可將密碼寫入至密碼儲存器 355。舉例而言，若自圖 3 所示記憶體控制器 205 接收的密碼不與儲存於密碼儲存器 355 中的密碼匹配，則在抹除邏輯 435 抹除資料儲存器 310-345 的內容之後，密碼寫入邏輯 440 可將自圖 3 所示記憶體控制器 205 接收的密碼寫入至密碼儲存器 355。以此種方式，圖 3 所示記憶體控制器 205 可隨後使用相同的密碼來驗證至記憶體 145，任何其他記憶體控制器將不能夠進行驗證（不包括其他記憶體控制器設法生成相同的密碼的不可能事件），藉此保護使用者的資料免於未授權存取。

【0037】 在圖 3 至圖 4 中，確定何時重設記憶體 145 取決於所述系統。亦即，記憶體 145 不知道任意特定使用者已租賃記憶體 145 達多久。因此，圖 3 所示記憶體控制器 205（或圖 1 所示資料中心 105 的服務提供者）可藉由計時器來跟蹤使用者已對記憶體 145 進行存取達多久。一旦使用者的租賃已過期，則圖 3 所示記憶體控制器 205（或圖 1 所示主機 110 的任意其他所需組件）可發出由軟體引發的重設指令至記憶體 145（或更大體而言，發出至圖所示伺服器 110），此可保護使用者的資料免於被另一使用者讀取。

【0038】 在圖 3 至圖 4 中，密碼儲存器 355 被示出為與串列存在偵測 350 分離。但本發明概念的一些實施例可視需要將密碼儲存於串列存在偵測 350 的未使用部分或供應商專用區域中。此種方式可使得避免僅為密碼而引入新的儲存器。

【0039】 圖 5 示出圖 3 至圖 4 所示記憶體 145 使用自圖 3 所示記憶體控制器 205 接收的密碼來判斷準許存取儲存於圖 3 至圖 4 所示記憶體 145 中的資料還是抹除儲存於圖 3 至圖 4 所示記憶體 145 中的資料。在圖 4 中，接收器 420 可自圖 3 所示記憶體控制器 205 接收密碼 505。比較器 430 可接著將所接收密碼 505 與可自密碼儲存器 355 擷取的所儲存密碼 510 進行比較。若所接收密碼 505 與所儲存密碼 510 匹配，則比較結果 515 可指示可準許圖 3 所示記憶體控制器 205 立即對圖 4 所示記憶體 145 進行存取；否則，比較結果 515 可指示應阻止圖 3 所示記憶體控制器 205 直至圖 3 至圖 4 所示資料儲存器 310-345 中的資料已被圖 4 所示抹除邏輯 435 抹除之後為止。

【0040】 圖 5 亦示出臨限值 520 的使用。在本發明概念的一些實施例中，比較器 430 可執行對所接收密碼 505 與所儲存密碼 510 的單一比較以判斷是否準許圖 3 所示記憶體控制器 205 對圖 3 至圖 4 所示記憶體 145 的存取。但本發明概念的其他實施例可允許圖 3 所示記憶體控制器 205 提供多個所接收密碼 505。舉例而言，在比較器 430 確定所接收密碼 505 不與所儲存密碼 510 匹配之後，圖 4 所示驗證邏輯 415 可經由 DQ 匯流排將訊號發送至圖 3 所示記憶體控制器 205，進而請求圖 3 所示記憶體控制器 205 重新發送所接收密碼 505。容許重試可防止資料的非預期變化：例如，因在發送所接收密碼 505 時存在干擾而造成的變化。比較器 430 可接著測試所接收密碼 505 達與由臨限值 520 指明的次數一樣多的次

數，在此之後，若尚未找到匹配，則比較結果 515 可指明在圖 3 至圖 4 所示記憶體 145 中自圖 3 至圖 4 所示資料儲存器 310-345 抹除資料。臨限值 520 可被設定成任意所需整數值；但由於圖 3 所示記憶體控制器 205 被臨時阻止對圖 3 至圖 4 所示記憶體 145 進行存取直至本發明概念的實施例已判斷是否抹除圖 3 至圖 4 所示資料儲存器 310-345 中的資料（且視需要執行此抹除）為止，因此將臨限值 520 保持為較低整數值可有利於減少阻止圖 3 至圖 4 所示記憶體控制器 205 的持續時間。

【0041】 圖 6 示出根據本發明概念實施例的圖 1 所示可在兩個使用者之間共享資源的記憶體 145 的例子。在圖 6 中，記憶體 145 可包括兩個記憶體部分 605 及 610，所述兩個部分中的每一者可被視作單獨的記憶體模組。舉例而言，記憶體 145 可為具有以太位元組（terabyte）或更大單位量測的容量的雙列直插記憶體模組。由於記憶體的此種量可大於單一使用者所需，因此將整個記憶體 145 指配給單一使用者將造成浪費。相反，可將記憶體 145 的一部分（例如，部分 605）指配給使用者，使得部分 610 可用於其他用途（包括另一使用者）。

【0042】 使用介面 615 使得兩個記憶體控制器 205 及 620 可與記憶體 145 介接。舉例而言，記憶體控制器 205 可與記憶體 145 的部分 605 介接，且記憶體控制器 620 可與記憶體 145 的部分 610 介接。藉由此種方式，儘管記憶體 145 可儲存兩個不同使用者的資料，然而每一使用者可僅存取自己的資料而不是另一使用者的

資料。此機制會保護每一者的資料。

【0043】 當一個使用者結束租賃記憶體 145 中為自己所用的一部分時，可啟動記憶體 145 的由軟體引發的重設。舉例而言，假定租賃部分 605 的使用者已結束自己的租賃。記憶體 145 可接著被重設。當記憶體 145 的由軟體引發的重設完成時，記憶體控制器 602 可向記憶體 145 呈現自身的密碼。記憶體控制器 620 可因此使自身重新驗證至記憶體 145，以重新得到對儲存於部分 610 中的使用者的資料的存取的權限。儘管由軟體引發的重設及驗證過程確實可能延遲對部分 610 中的使用者的資料的存取，然而此延遲並不顯著，且將可能甚至不會被使用者注意到。

【0044】 另一方面，記憶體控制器 205 可向記憶體 145 呈現新密碼。由於此密碼將（可能）不會被識別，因此記憶體控制器 205 將不可能驗證至記憶體 145。因此，可在另一使用者可租賃 605 之前抹除部分 605，進而保護其資料之前已被儲存於部分 605 中的使用者。

【0045】 儘管圖 6 示出本發明概念實施例的被劃分成兩個部分 605 及 610 的記憶體 145 可支援記憶體 145 中的任意數目的部分。圖 6 中的使用兩個部分僅為例子。另外，根據記憶體 145 的實施例，記憶體 145 可對於記憶體 145 的每一部分包括一個暫存器時脈驅動器、對於記憶體 145 的所有部分包括一個暫存器時脈驅動器、或根本不包括暫存器時脈驅動器。

【0046】 圖 7A 至圖 7C 示出根據本發明概念實施例的圖 3 所示記

憶體控制器 205 請求對圖 1 所示記憶體 145 的存取的示例性過程的流程圖。在圖 7A 中，在方塊 705 處，圖 3 所示記憶體控制器 205 可確定圖 1 所示記憶體 145 已被重設（藉由由硬體引發的重設或由軟體引發的重設）。在方塊 710 處，記憶體控制器 205 可判斷圖 1 所示記憶體 145 是否正處於安全模式：例如，藉由自圖 3 所示串列存在偵測 350 讀取相關資料。在方塊 715 處，若圖 1 所示記憶體 145 未正在以安全模式運作，則圖 3 所示記憶體控制器 205 可接收對圖 1 所示記憶體 145 的存取。

【0047】 另一方面，若圖 1 所示記憶體 145 正在以安全模式運作，則在方塊 720 處，圖 3 所示記憶體控制器 205 可選擇用於與圖 1 所示記憶體 145 一起使用的密碼。在方塊 725 處，因應於來自圖 1 所示記憶體 145 的請求，圖 3 所示記憶體控制器 205 可將所述密碼發送至圖 1 所示記憶體 145。

【0048】 在方塊 730 處（圖 7B），圖 3 所示記憶體控制器 205 可判斷密碼是否已被接受。如上所述，圖 1 所示記憶體 145 可經由 DQ 匯流排來發送指示所述密碼是否已被接受且圖 3 所示記憶體控制器 205 是否已被授權的訊號。若所述密碼未被接受，則在方塊 735 處，圖 3 所示記憶體控制器 205 可接收要求重新發送密碼的請求，且控制可返回至圖 7A 所示方塊 720。作為另一選擇，在方塊 740 處，圖 3 所示記憶體控制器 205 可僅在圖 1 所示記憶體 145 已抹除圖 3 至圖 4 所示資料儲存器 310-345 中的所有資料之後接收對圖 1 所示記憶體 145 的存取。方塊 735 與方塊 740 之間的不

同代表記憶體 145 是否已執行臨限數目的密碼比較：由於圖 3 所示記憶體控制器 205 可能不知道臨限值，因此圖 3 所示記憶體控制器 205 可僅能夠因應於由圖 1 所示記憶體 145 所作出的其他密碼請求。

【0049】 另一方面，若密碼被接受，則在方塊 745 處，圖 3 所示記憶體控制器 205 可接收對圖 1 所示記憶體 145 的存取，而不首先抹除圖 3 至圖 4 所示資料儲存器 310-345 中的資料。

【0050】 在方塊 750 處（圖 7C），圖 3 所示記憶體控制器 205 可量測自已準許圖 3 所示記憶體控制器 205 對圖 1 所示記憶體 145 進行存取時起已達多久。在方塊 755 處，圖 3 所示記憶體控制器 205 可判斷是否已經過臨限時間量—使用者租賃圖 1 所示記憶體 145 的時間量。若否，則圖 3 所示記憶體控制器 205 可稍等片刻再重新量測已經過多少時間。一旦租賃時間已過，則在方塊 760 處，圖 3 所示記憶體控制器 205 可指令圖 1 所示記憶體 145 執行由軟體引發的重設，處理在此之後結束。

【0051】 圖 8 示出根據本發明概念實施例的圖 3 所示記憶體控制器 205 選擇密碼來請求對圖 1 所示記憶體 145 的存取的示例性過程的流程圖。在圖 8 中，在方塊 805 處，圖 3 所示記憶體控制器 205 可產生隨機密碼以用於驗證至圖 1 所示記憶體 145。作為另一選擇，在方塊 810 處，圖 3 所示記憶體控制器 205 可自密碼清單選擇密碼以用於驗證至圖 1 所示記憶體 145。作為另一選擇，在方塊 815 處，圖 3 所示記憶體控制器 205 可對使用者 ID 進行雜湊以

產生密碼以用於驗證至圖 1 所示記憶體 145。作為另一選擇，在方塊 820 處，圖 3 所示記憶體控制器 205 可自可信賴平台模組存取密碼以用於驗證至圖 1 所示記憶體 145。

【0052】 圖 9A 至圖 9C 示出根據本發明概念實施例的圖 1 所示記憶體 145 判斷準許圖 3 所示記憶體控制器 205 存取資料還是抹除資料的示例性過程的流程圖。在圖 9A 中，在方塊 905 處，圖 1 所示記憶體 145 可接收要求知道圖 1 所示記憶體 145 是否正在以安全模式運作的請求。在方塊 910 處，圖 1 所示記憶體 145 可將指示圖 1 所示記憶體 145 是否正在以安全模式運作的訊號發送至圖 3 所示記憶體控制器 205。在方塊 915 處，圖 1 所示記憶體 145 可自圖 3 所示記憶體控制器 205 接收要求對圖 1 所示記憶體 145 進行存取的請求。

【0053】 在方塊 920 處，圖 1 所示記憶體 145 可判斷自身是否正在以安全模式運作。若圖 1 所示記憶體 145 未正在以安全模式運作，則在方塊 925 處，圖 1 所示記憶體 145 可準許對圖 3 所示記憶體控制器 205 的存取。否則，在方塊 930 處，驗證邏輯 415 可自圖 3 所示密碼儲存器 355 存取圖 5 所示所儲存密碼 510。

【0054】 在方塊 935 處（圖 9B），圖 1 所示記憶體 145 可自圖 3 所示記憶體控制器 205 請求圖 5 所示密碼 505。在方塊 940 處，圖 1 所示記憶體 145 可自圖 3 所示記憶體控制器 205 接收圖 5 所示密碼 505。在方塊 945 處，圖 4 所示比較器 430 可將圖 5 所示所接收密碼 505 與圖 5 所示所儲存密碼 510 進行比較。

【0055】 在方塊 950 處，圖 4 所示驗證邏輯 415 可確定圖 5 所示指示圖 5 所示所接收密碼 505 與圖 5 所示所儲存密碼 510 的比較是否指示匹配的比較結果 515。若是，則在方塊 955 處，圖 1 所示記憶體 145 可準許圖 3 所示記憶體控制器 205 對圖 1 所示記憶體 145 的存取。

【0056】 在方塊 960 處（圖 9C），假定圖 5 所示所接收密碼 505 不與圖 5 所示所儲存密碼 510 匹配，則圖 4 所示驗證邏輯 415 可判斷是否已發生密碼比較的臨限數目。若否，則控制返回至圖 9B 所示方塊 935 以使圖 1 所示記憶體 145 自圖 3 所示記憶體控制器 205 請求新密碼。否則，在方塊 965 處，圖 4 所示抹除邏輯 435 可自圖 3 至圖 4 所示資料儲存器 310-345 抹除資料。接著，在方塊 970 處，圖 4 所示密碼寫入邏輯 440 可將圖 5 所示所接收密碼 505 寫入至圖 3 所示密碼儲存器 355 中，在此之後，在方塊 975 處，圖 1 所示記憶體 145 可準許圖 3 所示記憶體控制器 205 對圖 1 所示記憶體 145 的存取。

【0057】 在方塊 980 處，無論圖 1 所示記憶體 145 在抹除圖 3 至圖 4 所示資料儲存器 310-345 中的資料的條件下還是在不進行所述抹除的條件下準許圖 3 所示記憶體控制器 205 對圖 1 所示記憶體 145 的存取，在方塊 980 處，圖 1 所示記憶體 145 均可自圖 3 所示記憶體控制器 205 接收用於執行由軟體引發的重設的訊號，且在方塊 985 處，圖 1 所示記憶體 145 可執行由軟體引發的重設，處理在此之後結束。

【0058】 圖 10 示出根據本發明概念實施例的圖 4 所示抹除邏輯 435 自圖 1 所示記憶體 145 抹除資料的示例性過程的流程圖。在圖 10 中，在方塊 1005 處，圖 4 所示抹除邏輯 435 可對被使用者使用過的記憶體區塊執行垃圾收集。作為另一選擇，在方塊 1010 處，圖 4 所示抹除邏輯 435 可使用常數值對圖 1 所示記憶體 145 中的所有資料進行覆蓋寫入。作為另一選擇，在方塊 1015 處，圖 4 所示抹除邏輯 435 可對圖 1 所示記憶體 145 中的所有資料執行覆蓋寫入序列，例如寫入所有零、接著寫入所有一、再接著寫入隨機圖案。作為另一選擇，在方塊 1020 處，圖 4 所示抹除邏輯 435 可防止圖 1 所示記憶體 145 中的胞元被再新，直至當圖 1 所示記憶體 145 可保證所有所儲存資料值皆已丟失時為止。

【0059】 在圖 7A 至圖 10 中，示出了本發明概念的一些實施例。但熟習此項技術者應認識到，藉由改變所述方塊的次序、藉由省略方塊、或藉由包括未在圖式中示出的環節，本發明概念亦可具有其他實施例。無論是否明確闡述，流程圖的所有此類變型均被視為本發明概念的實施例。

【0060】 以下論述旨在提供對其中可實作有本發明概念的一些態樣的適合的一或多個機器的簡要大體說明。所述一或多個機器可至少部分地藉由以下來控制：來自例如鍵盤、滑鼠等傳統輸入裝置的輸入；以及自另一機器接收的指示、與虛擬實境（virtual reality，VR）環境的交互、生物劑量學回饋（biometric feedback）、或另一種輸入訊號。本文中所用用語「機器」旨在廣泛地囊括單

片機（single machine）、虛擬機（virtual machine）、或通訊地耦合的一起運作的機器、虛擬機、或裝置的系統。示例性機器包括：計算裝置，例如個人電腦、工作站、伺服器、可攜式電腦、手持式裝置、電話機、平板電腦（tablet）等；以及運輸裝置，例如私人或公共運輸工具（例如，汽車、火車、計程車等）。

【0061】 所述一或多個機器可包括例如可程式化或非可程式化邏輯裝置或陣列、應用專用積體電路（Application Specific Integrated Circuit，ASIC）、嵌式電腦、智慧卡等嵌式控制器。所述一或多個機器可使用一或多個連接（例如經由網路介面、數據機、或其他通訊耦合進行的連接）而連接至一或多個遠端機器。各機器可藉由例如內部網路、網際網路、區域網路、廣域網路等實體網路及/或邏輯網路而互連。熟習此項技術者應知，網路通訊可使用包括射頻（radio frequency，RF）、衛星、微波、電氣及電子工程師學會（Institute of Electrical and Electronics Engineers，IEEE）802.11、藍芽®、光學裝置、紅外裝置、纜線、雷射等各種有線及/或無線短程或長程載體及協定。

【0062】 本發明概念的實施例可藉由參照或結合包括功能、過程、資料結構、應用程式等的相關聯資料來闡述，所述相關聯資料當由機器存取時會使得所述機器執行任務或定義抽象資料類型或低層級硬體上下文。相關聯資料可儲存於例如以下等裝置中：揮發性及/或非揮發性記憶體，例如隨機存取記憶體、唯讀記憶體等；或者其他儲存裝置及其相關聯的儲存媒體，包括硬驅動機、

軟碟、光學儲存器、磁帶、快閃記憶體、記憶條、數位視訊光碟、生物邏輯儲存器等。相關聯資料可以封包、串列資料、並列資料、傳播訊號等形式藉由包括實體網路及/或邏輯網路的傳輸環境而進行傳遞且可以壓縮或加密格式使用。相關聯資料可用於分佈式環境中，且在本地及/或遠端地儲存以供機器存取。

【0063】 本發明概念的實施例可包括包含能夠由一或多個處理器執行的指令的有形非暫時性機器可讀取媒體，所述指令包括執行本文所述本發明概念的元件的指令。

【0064】 由於已參照所示實施例闡述並說明瞭本發明概念的原理，因此應認識到，在不背離此類原理的條件下可在佈置及細節上對所示實施例加以修改且可以任何所需方式將所示實施例加以組合。而且，儘管前面的論述已著重於具體實施例，然而亦慮及其他配置。具體而言，儘管本文中使用例如「根據本發明概念的實施例」等表達，然而該些片語意欲大體引用實施例可能性，且並非旨在將本發明概念限制為具體實施例配置。本文中所使用的該些用語可引用能夠組合成其他實施例的相同的或不同的實施例。

【0065】 前面的說明性實施例不應被視作限制其發明概念。儘管已闡述了若干實施例，然而熟習此項技術者將易知，在不本質上背離本發明的新穎教示內容及優點的條件下可對該些實施例作出諸多潤飾。因此，所有此類潤飾皆旨在包含於如申請專利範圍中所界定的此發明概念的範圍內。

【0066】 本發明概念的實施例可擴展至以下聲明且並無限制：

聲明 1. 本發明概念的實施例包括一種記憶體，所述記憶體包括：

資料儲存器，用於第一使用者的資料；

資料讀取邏輯，自所述資料儲存器讀取資料；

資料寫入邏輯，向所述資料儲存器寫入資料；

密碼儲存器，用於所儲存密碼；

接收器，自記憶體控制器接收所接收密碼；

比較器，將所述所接收密碼與所述所儲存密碼進行比較；

抹除邏輯，若所述所接收密碼不同於所述所儲存密碼，則抹除所述資料儲存器中的所述資料；以及

阻止邏輯，阻止自所述記憶體控制器存取所述資料儲存器，直至所述比較器完成操作之後為止，

其中所述所接收密碼或所述所儲存密碼不用於對儲存於所述記憶體中的資料進行加密。

【0067】 聲明 2. 本發明概念的實施例包括根據聲明 1 的記憶體，其中所述阻止邏輯能夠操作以阻止自所述記憶體控制器存取所述資料儲存器，直至所述抹除邏輯完成操作之後為止。

【0068】 聲明 3. 本發明概念的實施例包括根據聲明 1 的記憶體，所述記憶體更包括將所述所接收密碼寫入至所述密碼儲存器的密碼寫入邏輯。

【0069】 聲明 4. 本發明概念的實施例包括根據聲明 1 的記憶體，

所述記憶體更包括用以指明所述記憶體是否正在以安全模式運作的串列存在偵測（SPD）。

【0070】 聲明 5. 本發明概念的實施例包括根據聲明 4 的記憶體，其中若所述串列存在偵測指明所述記憶體未正在以所述安全模式運作，則所述阻止邏輯容許所述記憶體控制器存取所述資料儲存器而不調用所述比較器。

【0071】 聲明 6. 本發明概念的實施例包括根據聲明 1 的記憶體，所述記憶體更包括用以指明所述記憶體是否正在以安全模式運作的重要產品資料（VPD）。

【0072】 聲明 7. 本發明概念的實施例包括根據聲明 6 的記憶體，所述記憶體更包括用於儲存所述重要產品資料的電子可抹除可程式化唯讀記憶體（EEPROM）。

【0073】 聲明 8. 本發明概念的實施例包括根據聲明 6 的記憶體，其中若所述重要產品資料指明所述記憶體未正在以所述安全模式運作，則所述阻止邏輯容許所述記憶體控制器存取所述資料儲存器而不調用所述比較器。

【0074】 聲明 9. 本發明概念的實施例包括根據聲明 1 的記憶體，其中所述抹除邏輯能夠操作以在臨限數目的所接收密碼均不同於所述所儲存密碼時抹除所述資料儲存器中的所述資料。

【0075】 聲明 10. 本發明概念的實施例包括根據聲明 1 的記憶體，其中：

所述記憶體更包括第二資料儲存器，所述第二資料儲存器儲

存第二使用者的第二資料；

所述資料讀取邏輯能夠操作以自所述第二資料儲存器讀取所述第二資料；

所述資料寫入邏輯能夠操作以將所述第二資料寫入至所述第二資料儲存器；

所述密碼儲存器能夠操作以儲存第二所儲存密碼；

所述接收器能夠操作以自第二記憶體控制器接收第二所接收密碼；

所述比較器能夠操作以將所述第二所接收密碼與所述第二所儲存密碼進行比較；

所述抹除邏輯能夠操作以在所述第二所接收密碼不同於所述第二所儲存密碼時抹除所述第二資料儲存器中的所述第二資料；且

所述阻止邏輯能夠操作以阻止自所述第二記憶體控制器存取所述第二資料儲存器，直至所述比較器完成操作之後為止。

【0076】 聲明 11. 本發明概念的實施例包括根據聲明 10 的記憶體，其中所述記憶體控制器是所述第二記憶體控制器。

【0077】 聲明 12. 本發明概念的實施例包括根據聲明 1 的記憶體，其中所述記憶體取自包括以下的集合：揮發性記憶體模組、非揮發性記憶體模組、及揮發性記憶體裝置與非揮發性記憶體裝置的任意組合。

【0078】 聲明 13. 本發明概念的實施例包括根據聲明 1 的記憶

體，所述記憶體包括暫存器時脈驅動器（RCD），所述暫存器時脈驅動器包括所述接收器、所述比較器、所述抹除邏輯、及所述阻止邏輯。

【0079】 聲明 14. 根據本發明概念的實施例包括根據聲明 13 的記憶體，其中所述暫存器時脈驅動器更包括所述資料讀取邏輯及所述資料寫入邏輯。

【0080】 聲明 15. 本發明概念的實施例包括一種方法，所述方法包括：

確定記憶體已被重設；

判斷所述記憶體正在以安全模式還是非安全模式運作；以及

若所述記憶體正在以所述安全模式運作，則：

選擇使用者的密碼；

將所述密碼發送至所述記憶體；以及

接收對所述記憶體的存取，

其中所述密碼不用於對儲存於所述記憶體中的資料進行加密。

【0081】 聲明 16. 本發明概念的實施例包括根據聲明 15 的方法，所述方法更包括：若所述記憶體正在以所述非安全模式運作，則不使用密碼接收對所述記憶體的存取。

【0082】 聲明 17. 本發明概念的實施例包括根據聲明 15 的方法，其中將所述密碼發送至所述記憶體包括將所述密碼發送至所述記憶體達臨限數目的次數。

【0083】 聲明 18. 本發明概念的實施例包括根據聲明 15 的方法，其中接收對所述記憶體的存取包括接收對被抹除記憶體的存取。

【0084】 聲明 19. 本發明概念的實施例包括根據聲明 15 的方法，其中接收對所述記憶體的存取包括接收對儲存於所述記憶體中的所述資料的存取。

【0085】 聲明 20. 本發明概念的實施例包括根據聲明 15 的方法，所述方法更包括：

量測自所述記憶體被重設時起的時間量；以及

若自所述記憶體被重設時起的所述時間量大於臨限值，則將由軟體引發的重設發送至所述記憶體。

【0086】 聲明 21. 本發明概念的實施例包括根據聲明 15 的方法，其中所述記憶體取自包括以下的集合：揮發性記憶體模組、非揮發性記憶體模組、及揮發性記憶體裝置與非揮發性記憶體裝置的任意組合。

【0087】 聲明 22. 本發明概念的實施例包括根據聲明 15 的方法，其中所述記憶體包括被指配給第一使用者的第一部分及被指配給第二使用者的第二部分。

【0088】 聲明 23. 本發明概念的實施例包括根據聲明 15 的方法，其中選擇所述使用者的所述密碼包括產生隨機密碼。

【0089】 聲明 24. 本發明概念的實施例包括根據聲明 15 的方法，其中選擇所述使用者的所述密碼包括自可用密碼清單選擇所述密碼。

【0090】 聲明 25. 本發明概念的實施例包括根據聲明 15 的方法，其中選擇所述使用者的所述密碼包括依照所述使用者的辨識符的雜湊產生所述密碼。

【0091】 聲明 26. 本發明概念的實施例包括根據聲明 15 的方法，其中選擇所述使用者的所述密碼包括自可信賴平台模組存取所述密碼。

【0092】 聲明 27. 本發明概念的實施例包括一種方法，所述方法包括：

自記憶體向記憶體控制器發送表示所述記憶體正在以安全模式運作的訊號；

自所述記憶體控制器接收所接收密碼；

將所述所接收密碼與所儲存密碼進行比較；以及

若所述所接收密碼不與所述所儲存密碼匹配，則：

抹除所述記憶體；以及

提供所述記憶體控制器對所述記憶體的存取，

其中所述所接收密碼或所述所儲存密碼不用於對儲存於所述記憶體中的資料進行加密。

【0093】 聲明 28. 本發明概念的實施例包括根據聲明 27 的方法，所述方法更包括：若所述所接收密碼不與所述所儲存密碼匹配，則將所述所接收密碼儲存於所述記憶體中。

【0094】 聲明 29. 本發明概念的實施例包括根據聲明 27 的方法，所述方法更包括：若所述所接收密碼與所述所儲存密碼匹配，則

提供所述記憶體控制器對所述記憶體的存取。

【0095】 聲明 30. 本發明概念的實施例包括根據聲明 27 的方法，所述方法更包括：在抹除所述記憶體之前，將所述所接收密碼與所述所儲存密碼比較達臨限數目的次數。

【0096】 聲明 31. 本發明概念的實施例包括根據聲明 27 的方法，所述方法更包括：

自所述記憶體控制器接收重設命令；以及

因應於所述重設命令而重設所述記憶體。

【0097】 聲明 32. 本發明概念的實施例包括根據聲明 31 的方法，其中因應於所述重設命令而重設所述記憶體包括對所述記憶體中的所有資料執行垃圾收集。

【0098】 聲明 33. 本發明概念的實施例包括根據聲明 31 的方法，其中因應於所述重設命令而重設所述記憶體包括對所述記憶體中的所有資料執行覆蓋寫入序列。

【0099】 聲明 34. 本發明概念的實施例包括根據聲明 31 的方法，其中因應於所述重設命令而重設所述記憶體包括使用常數值對所述記憶體中的所有資料進行覆蓋寫入。

【0100】 聲明 35. 本發明概念的實施例包括根據聲明 31 的方法，其中因應於所述重設命令而重設所述記憶體包括防止對所述記憶體中的所有資料的再新，直至所述記憶體中的所有資料不再儲存於所述記憶體中為止。

【0101】 聲明 36. 本發明概念的實施例包括根據聲明 27 的方法，

其中自所述記憶體向所述記憶體控制器發送表示所述記憶體正在以所述安全模式運作的所述訊號包括自所述記憶體控制器接收請求以判斷所述記憶體是否正在以所述安全模式運作。

【0102】 聲明 37. 本發明概念的實施例包括根據聲明 27 的方法，其中自所述記憶體控制器接收所述所接收密碼包括自所述記憶體控制器請求所述密碼。

【0103】 聲明 38. 本發明概念的實施例包括根據聲明 27 的方法，其中所述記憶體取自包括以下的集合：揮發性記憶體模組、非揮發性記憶體模組、及揮發性記憶體裝置與非揮發性記憶體裝置的任意組合。

【0104】 聲明 39. 本發明概念的實施例包括根據聲明 27 的方法，其中所述記憶體是被指配給第一使用者的第一部分及被指配給第二使用者的第二部分。

【0105】 聲明 40. 本發明概念的實施例包括一種製品，所述製品包括有形儲存媒體，所述有形儲存媒體上儲存有非暫時性指令，所述非暫時性指令當由機器執行時使得：

確定記憶體已被重設；

判斷所述記憶體正在以安全模式還是非安全模式運作；以及

若所述記憶體正在以所述安全模式運作，則：

選擇使用者的密碼；

將所述密碼發送至所述記憶體；以及

接收對所述記憶體的存取，

其中所述密碼不用於對儲存於所述記憶體中的資料進行加密。

【0106】 聲明 41. 本發明概念的實施例包括根據聲明 40 的製品，所述有形儲存媒體上儲存有進一步的非暫時性指令，所述進一步的非暫時性指令當由所述機器執行時使得，若所述記憶體正在以所述非安全模式運作，則不使用密碼接收對所述記憶體的的存取。

【0107】 聲明 42. 本發明概念的實施例包括根據聲明 40 的製品，其中將所述密碼發送至所述記憶體包括將所述密碼發送至所述記憶體達臨限數目的次數。

【0108】 聲明 43. 本發明概念的實施例包括根據聲明 40 的製品，其中接收對所述記憶體的存取包括接收對被抹除記憶體的存取。

【0109】 聲明 44. 本發明概念的實施例包括根據聲明 40 的製品，其中接收對所述記憶體的存取包括接收對儲存於所述記憶體中的資料的存取。

【0110】 聲明 45. 本發明概念的實施例包括根據聲明 40 的製品，所述有形儲存媒體上儲存有進一步的非暫時性指令，所述進一步的非暫時性指令當由所述機器執行時使得：

量測自所述記憶體被重設時起的時間量；以及

若自所述記憶體被重設時起的所述時間量大於臨限值，則將由軟體引發的重設發送至所述記憶體。

【0111】 聲明 46. 本發明概念的實施例包括根據聲明 40 的製品，其中所述記憶體取自包括以下的集合：揮發性記憶體模組、非揮

發性記憶體模組、及揮發性記憶體裝置與非揮發性記憶體裝置的任意組合。

【0112】 聲明 47. 本發明概念的實施例包括根據聲明 40 的製品，其中所述記憶體是被指配給第一使用者的第一部分及被指配給第二使用者的第二部分。

【0113】 聲明 48. 本發明概念的實施例包括根據聲明 40 的製品，其中選擇所述使用者的所述密碼包括產生隨機密碼。

【0114】 聲明 49. 本發明概念的實施例包括根據聲明 40 的製品，其中選擇所述使用者的所述密碼包括自可用密碼清單選擇所述密碼。

【0115】 聲明 50. 本發明概念的實施例包括根據聲明 40 的製品，其中選擇所述使用者的所述密碼包括依照所述使用者的辨識符的雜湊產生所述密碼。

【0116】 聲明 51. 本發明概念的實施例包括根據聲明 40 的製品，其中選擇所述使用者的所述密碼包括自可信賴平台模組存取所述密碼。

【0117】 聲明 52. 本發明概念的實施例包括一種製品，所述製品包括有形儲存媒體，所述有形儲存媒體上儲存有非暫時性指令，所述非暫時性指令當由機器執行時使得：

將表示所述記憶體正在以安全模式運作的訊號自記憶體發送至記憶體控制器；

自所述記憶體控制器接收所接收密碼；

將所述所接收密碼與所儲存密碼進行比較；以及

若所述所接收密碼不與所述所儲存密碼匹配，則：

抹除所述記憶體；以及

提供所述記憶體控制器對所述記憶體的存取，

其中所述所接收密碼或所述所儲存密碼不用於對儲存於所述記憶體中的資料進行加密。

【0118】 聲明 53. 本發明概念的實施例包括根據聲明 52 的製品，所述有形儲存媒體上儲存有進一步的非暫時性指令，所述進一步的非暫時性指令當由所述機器執行時使得，若所述所接收密碼不與所述所儲存密碼匹配，則將所述所接收密碼儲存於所述記憶體中。

【0119】 聲明 54. 本發明概念的實施例包括根據聲明 52 的製品，其中若所述所接收密碼與所述所儲存密碼匹配，則提供所述記憶體控制器對所述記憶體的存取。

【0120】 聲明 55. 本發明概念的實施例包括根據聲明 52 的製品，所述有形儲存媒體上儲存有進一步的非暫時性指令，所述進一步的非暫時性指令當由所述機器執行時使得，在抹除所述記憶體之前對所述所接收密碼與所儲存密碼進行比較達臨限數目的次數。

【0121】 聲明 56. 本發明概念的實施例包括根據聲明 52 的製品，所述有形儲存媒體上儲存有進一步的非暫時性指令，所述進一步的非暫時性指令當由所述機器執行時使得：

自所述記憶體控制器接收重設命令；以及

因應於所述重設命令而重設所述記憶體。

【0122】 聲明 57. 本發明概念的實施例包括根據聲明 56 的製品，其中因應於所述重設命令而重設所述記憶體包括對所述記憶體中的所有資料執行垃圾收集。

【0123】 聲明 58. 本發明概念的實施例包括根據聲明 56 的製品，其中因應於所述重設命令而重設所述記憶體包括對所述記憶體中的所有資料執行覆蓋寫入序列。

【0124】 聲明 59. 本發明概念的實施例包括根據聲明 56 的製品，其中因應於所述重設命令而重設所述記憶體包括使用常數值對所述記憶體中的所有資料進行覆蓋寫入。

【0125】 聲明 60. 本發明概念的實施例包括根據聲明 56 的製品，其中因應於所述重設命令而重設所述記憶體包括，防止對所述記憶體中的所有資料的再新，直至所述記憶體中的所有資料不再儲存於所述記憶體中為止。

【0126】 聲明 61. 本發明概念的實施例包括根據聲明 52 的製品，其中自所述記憶體向所述記憶體控制器發送表示所述記憶體正在以所述安全模式運作的訊號包括自所述記憶體控制器接收請求以判斷所述記憶體是否正在以所述安全模式運作。

【0127】 聲明 62. 本發明概念的實施例包括根據聲明 52 的製品，其中自所述記憶體控制器接收所述所接收密碼包括自所述記憶體控制器請求所述密碼。

【0128】 聲明 63. 本發明概念的實施例包括根據聲明 52 的製品，

其中所述記憶體取自包括以下的集合：揮發性記憶體模組、非揮發性記憶體模組、及揮發性記憶體裝置與非揮發性記憶體裝置的任意組合。

【0129】 聲明 64. 本發明概念的實施例包括根據聲明 52 的製品，其中所述記憶體是被指配給第一使用者的第一部分及被指配給第二使用者的第二部分。

【0130】 因此，考慮到本文所述實施例的眾多種排列形式，此詳細說明及附帶材料僅旨在為說明性的，且不應被視作限制本發明概念的範圍。因此，本發明概念所主張的是所有此類潤飾皆可處於以下申請專利範圍及其等效範圍的範圍及精神內。

【符號說明】

【0131】

105：資料中心

110：主機/伺服器

115、120、125：主機

130：客戶機

135：網路

140：處理器

145：記憶體

150：電子可抹除可程式化唯讀記憶體

155：儲存裝置

160：重要產品資料

205、620：記憶體控制器

210：時鐘

215：網路連接器

220：匯流排

225：使用者介面

230：輸入/輸出引擎

305：暫存器時脈驅動器

310、315、320、325、330、335、340、345：記憶體晶片/資料儲存器

350：串列存在偵測

355：儲存器/密碼儲存器

405：資料讀取邏輯

410：資料寫入邏輯

415：驗證邏輯

420：接收器

425：阻止邏輯

430：比較器

435：抹除邏輯

440：密碼寫入邏輯

505：密碼/所接收密碼

510：所儲存密碼

515：比較結果

520：臨限值

605、610：部分

615：介面

705、710、715、720、725、730、735、740、745、750、755、760、805、810、815、820、905、910、915、920、925、930、935、940、945、950、955、960、965、970、975、980、985、1005、1010、1015、1020：步驟

【發明申請專利範圍】

【第1項】 一種記憶體，包括：

資料儲存器，用於第一使用者的資料；

資料讀取邏輯，自所述資料儲存器讀取資料；

資料寫入邏輯，向所述資料儲存器寫入資料；

密碼儲存器，用於所儲存密碼；

接收器，自記憶體控制器接收所接收密碼；

比較器，將所述所接收密碼與所述所儲存密碼進行比較；

抹除邏輯，若所述所接收密碼不同於所述所儲存密碼，則抹除所述資料儲存器中的所述資料；以及

阻止邏輯，阻止自所述記憶體控制器存取所述資料儲存器，直至所述比較器完成操作之後為止，

其中所述所接收密碼或所述所儲存密碼不用於對儲存於所述記憶體中的資料進行加密。

【第2項】 如申請專利範圍第1項所述的記憶體，其中所述阻止邏輯操作以阻止自所述記憶體控制器存取所述資料儲存器，直至所述抹除邏輯完成操作之後為止。

【第3項】 如申請專利範圍第1項所述的記憶體，更包括密碼寫入邏輯，用以將所述所接收密碼寫入至所述密碼儲存器。

【第4項】 如申請專利範圍第1項所述的記憶體，更包括串列存在偵測（SPD），用以指明所述記憶體是否正在以安全模式運作。

【第5項】 如申請專利範圍第4項所述的記憶體，其中若所述串列

存在偵測指明所述記憶體未正在以所述安全模式運作，則所述阻止邏輯容許所述記憶體控制器存取所述資料儲存器而不調用所述比較器。

【第6項】 如申請專利範圍第1項所述的記憶體，其中在臨限數目的所接收密碼均不同於所述所儲存密碼時，所述抹除邏輯運作以抹除所述資料儲存器中的所述資料。

【第7項】 如申請專利範圍第1項所述的記憶體，其中所述記憶體取自包括以下的集合：揮發性記憶體模組、非揮發性記憶體模組、及揮發性記憶體裝置與非揮發性記憶體裝置的組合。

【第8項】 如申請專利範圍第1項所述的記憶體，更包括暫存器時脈驅動器（RCD），所述暫存器時脈驅動器包括所述接收器、所述比較器、所述抹除邏輯、及所述阻止邏輯。

【第9項】 一種用於記憶體的方法，包括：

確定記憶體已被重設；

判斷所述記憶體正在以安全模式還是非安全模式運作；以及

若所述記憶體正在以所述安全模式運作，則：

選擇使用者的密碼；

將所述密碼發送至所述記憶體；以及

接收對所述記憶體的存取，

其中所述密碼不用於對儲存於所述記憶體中的資料進行加密。

【第10項】 如申請專利範圍第9項所述的方法，更包括：若所述記

憶體正在以所述非安全模式運作，則接收不使用密碼對所述記憶體進行的存取。

【第11項】 如申請專利範圍第9項所述的方法，其中將所述密碼發送至所述記憶體包括將所述密碼發送至所述記憶體達臨限數目的次數。

【第12項】 如申請專利範圍第9項所述的方法，其中接收對所述記憶體的存取包括接收對被抹除記憶體的存取。

【第13項】 如申請專利範圍第9項所述的方法，更包括：

量測自所述記憶體被重設時起的時間量；以及

若自所述記憶體被重設時起的所述時間量大於臨限值，則將由軟體引發的重設發送至所述記憶體。

【第14項】 一種用於記憶體的方法，包括：

自記憶體向記憶體控制器發送表示所述記憶體正在以安全模式運作的訊號；

自所述記憶體控制器接收所接收密碼；

將所述所接收密碼與所儲存密碼進行比較；以及

若所述所接收密碼不與所述所儲存密碼匹配，則：

抹除所述記憶體；以及

提供所述記憶體控制器對所述記憶體的存取，

其中所述所接收密碼或所述所儲存密碼不用於對儲存於所述記憶體中的資料進行加密。

【第15項】 如申請專利範圍第14項所述的方法，更包括：若所述

所接收密碼不與所述所儲存密碼匹配，則將所述所接收密碼儲存於所述記憶體中。

【第16項】 如申請專利範圍第14項所述的方法，更包括：若所述所接收密碼與所述所儲存密碼匹配，則提供所述記憶體控制器對所述記憶體的存取。

【第17項】 如申請專利範圍第14項所述的方法，更包括：在抹除所述記憶體之前，將所述所接收密碼與所述所儲存密碼比較達臨限數目的次數。

【第18項】 如申請專利範圍第14項所述的方法，更包括：

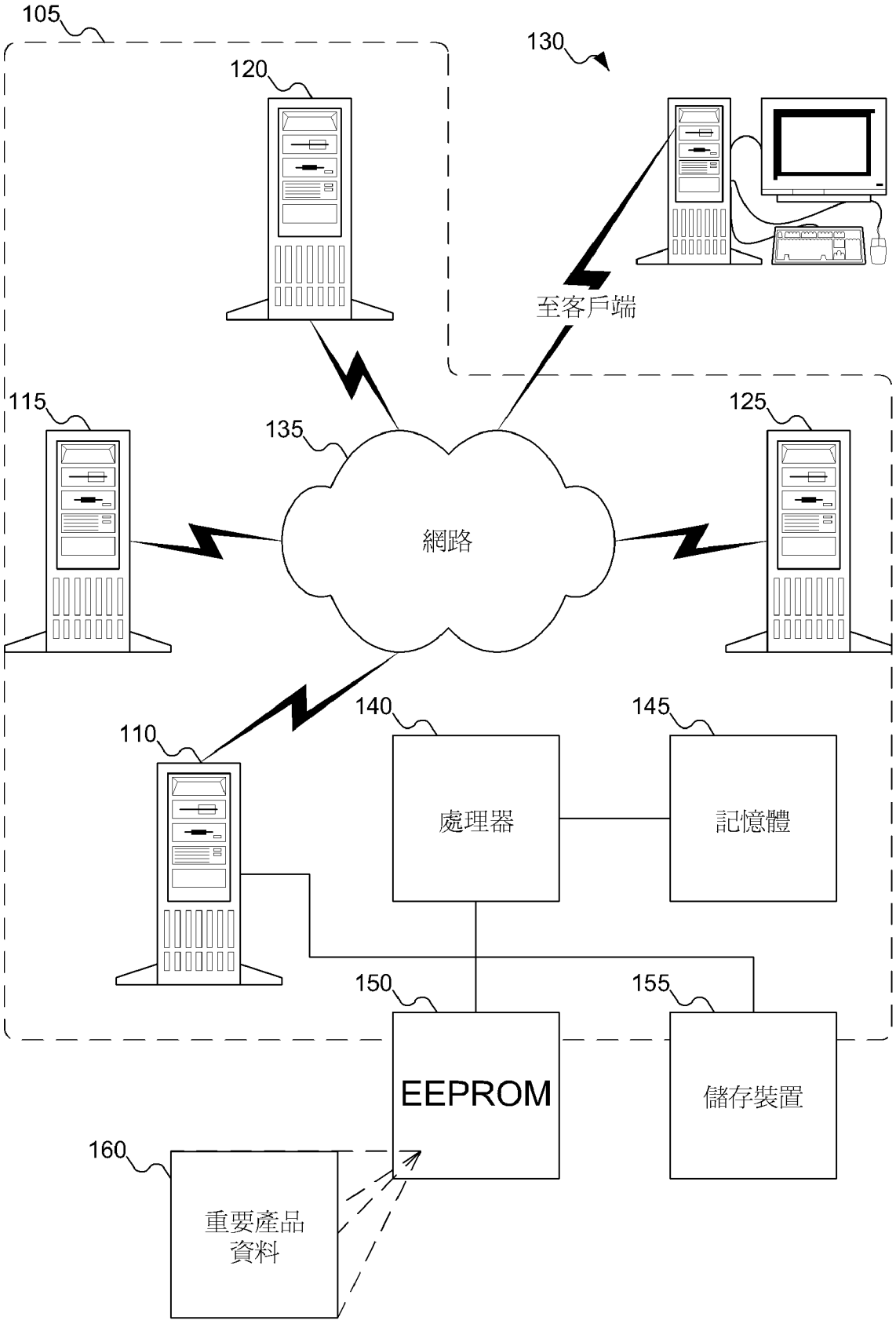
自所述記憶體控制器接收重設命令；以及

因應於所述重設命令而重設所述記憶體。

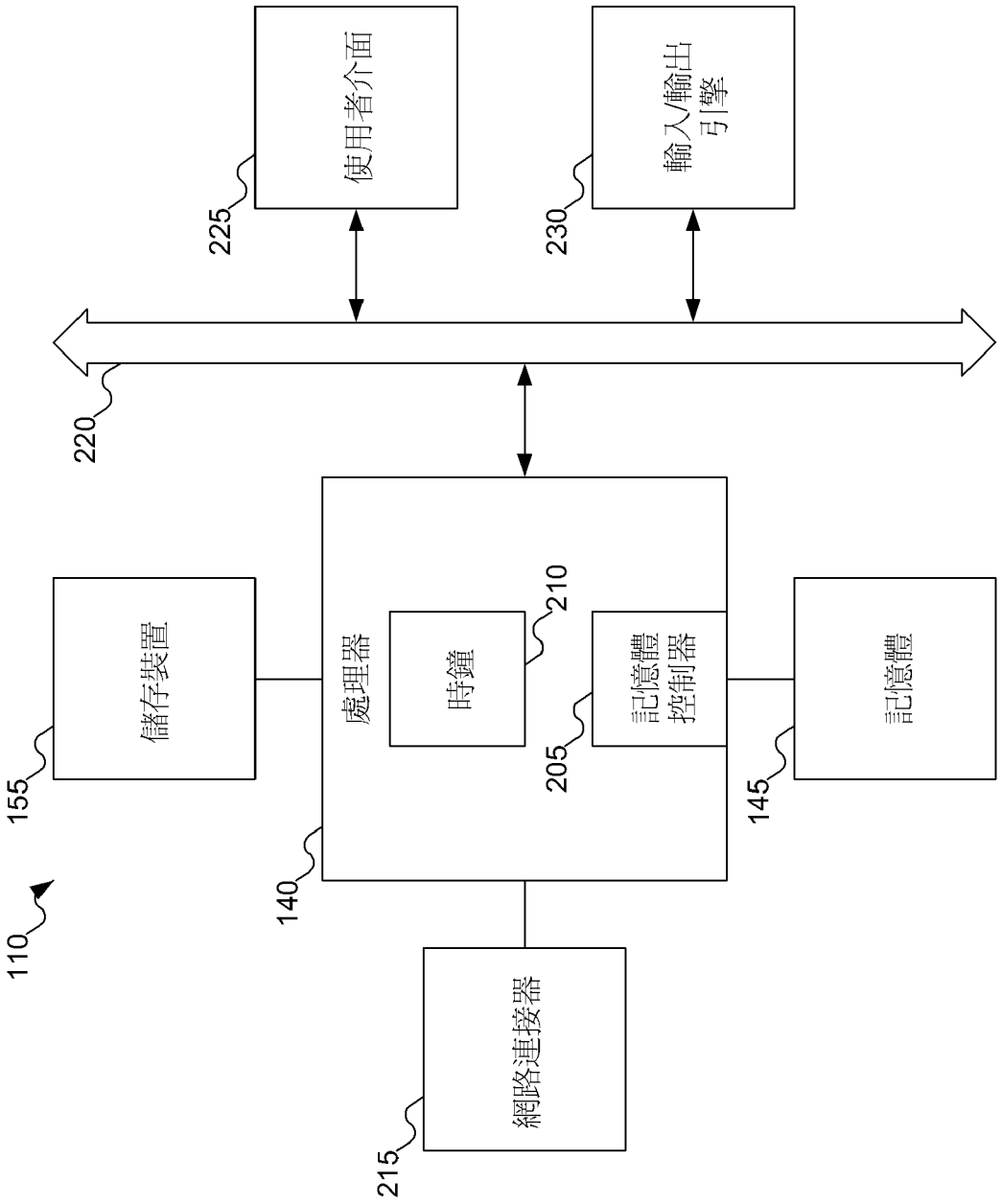
【第19項】 如申請專利範圍第14項所述的方法，其中自所述記憶體向所述記憶體控制器發送表示所述記憶體正在以所述安全模式運作的所述訊號包括自所述記憶體控制器接收請求以判斷所述記憶體是否正在以所述安全模式運作。

【第20項】 如申請專利範圍第14項所述的方法，其中自所述記憶體控制器接收所述所接收密碼包括自所述記憶體控制器請求所述密碼。

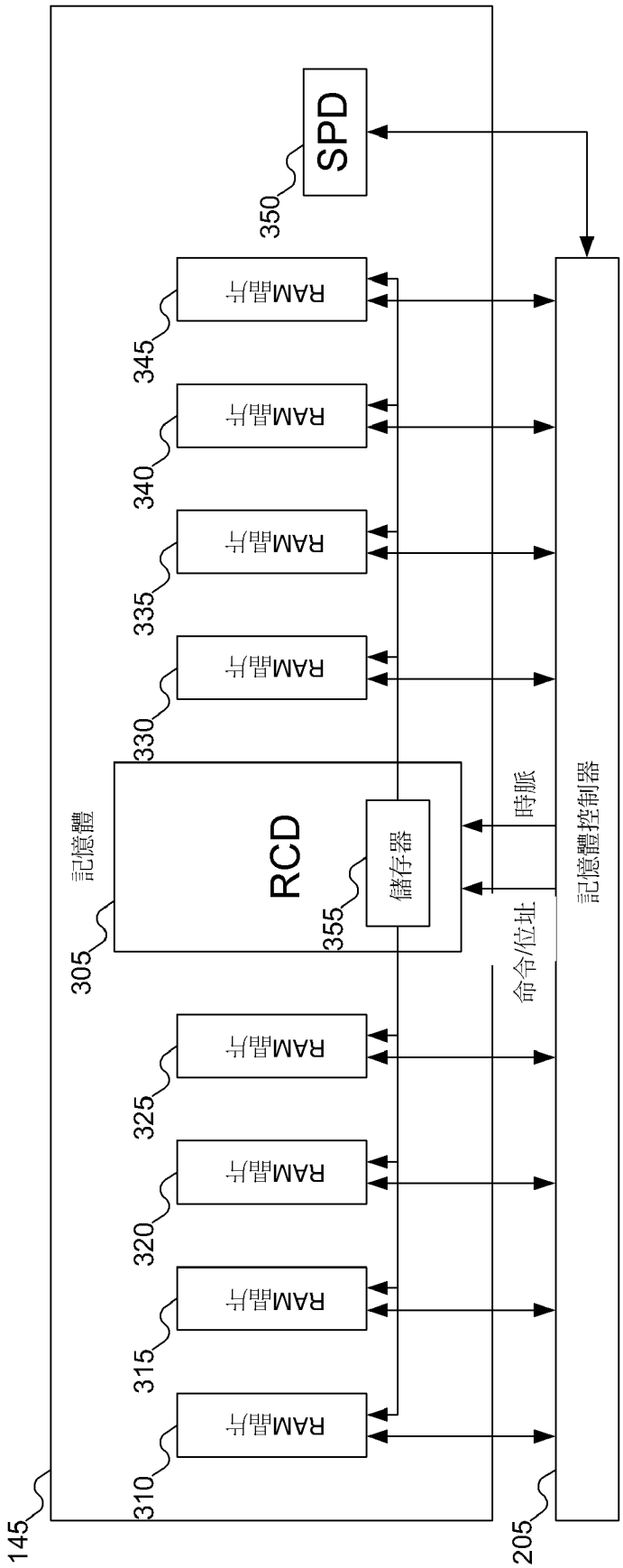
【發明圖式】


105
130
120
至客戶端
115
135
125
網路
110
140
145
處理器
記憶體
150
155
EEPROM
儲存裝置
160
重要產品
資料

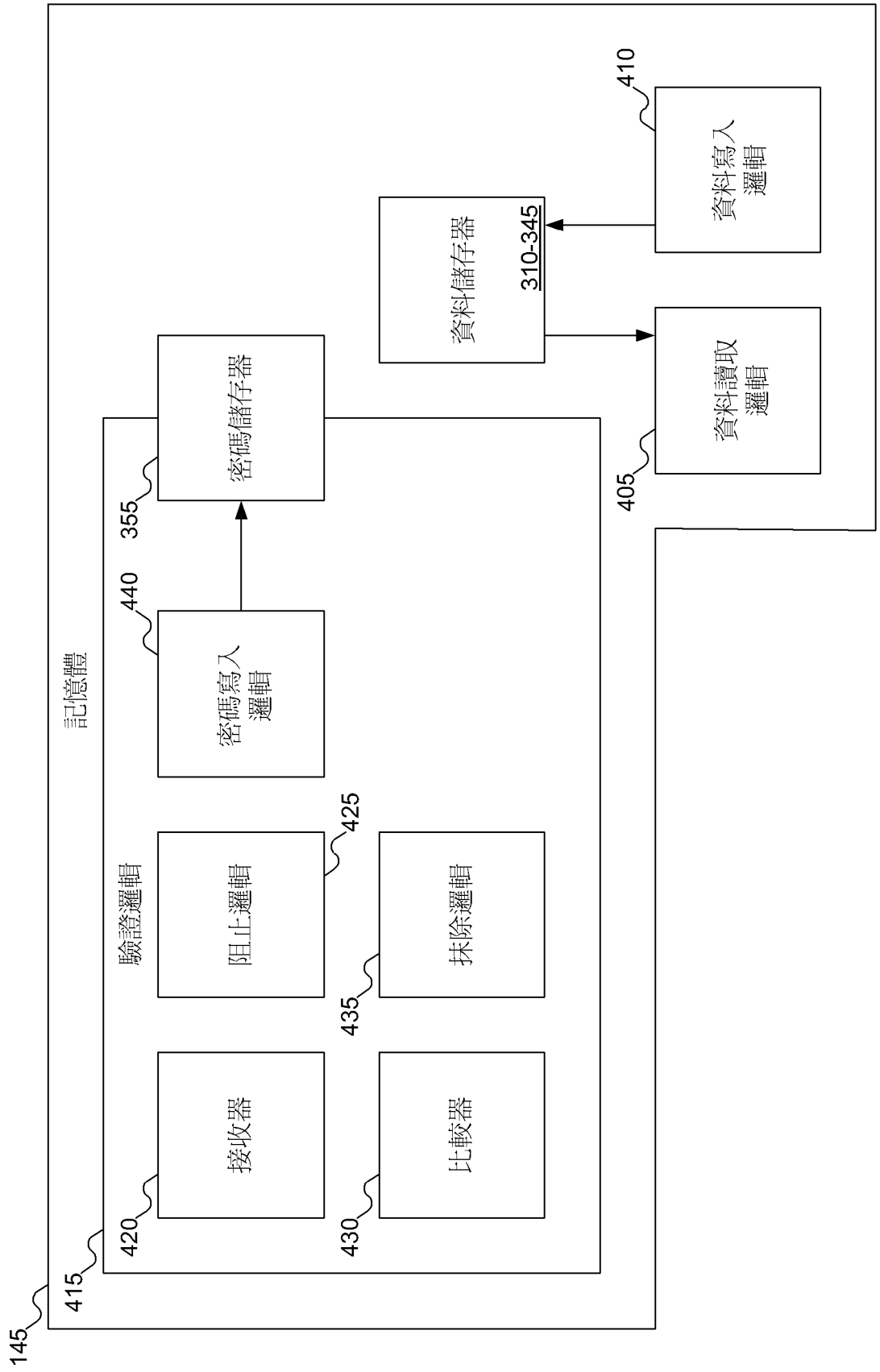
【圖1】


使用者介面
225
輸入/輸出
引擎
230
220
儲存裝置
155
處理器
時鐘
210
記憶體
控制器
205
記憶體
145
140
110
網路連接器
215

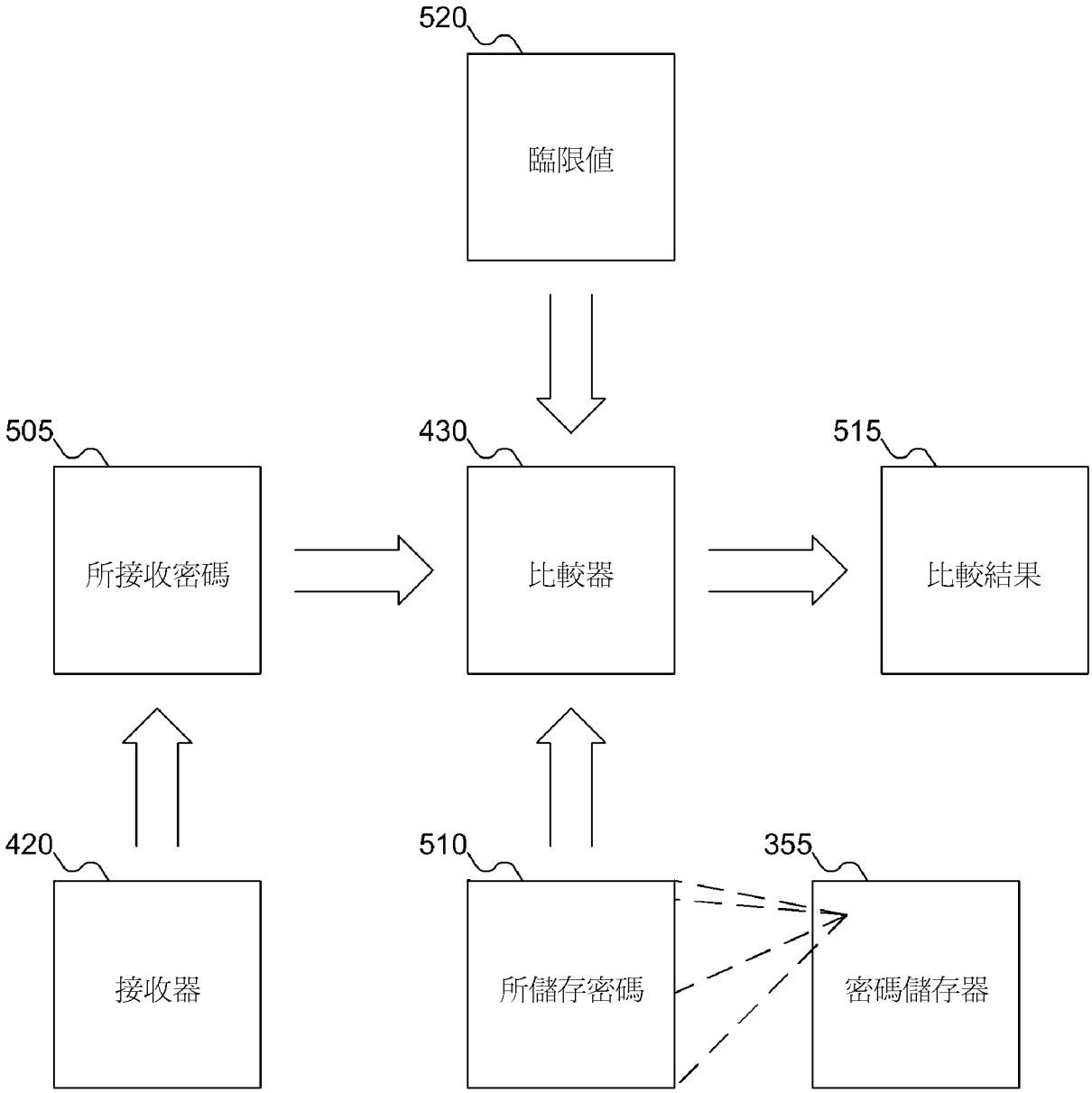
【圖2】


SPD
350
RAM晶片
345
RAM晶片
340
RAM晶片
335
RAM晶片
330
記憶體
305
RCD
儲存器
355
時脈
命令/位址
記憶體控制器
RAM晶片
325
RAM晶片
320
RAM晶片
315
RAM晶片
310
145
205

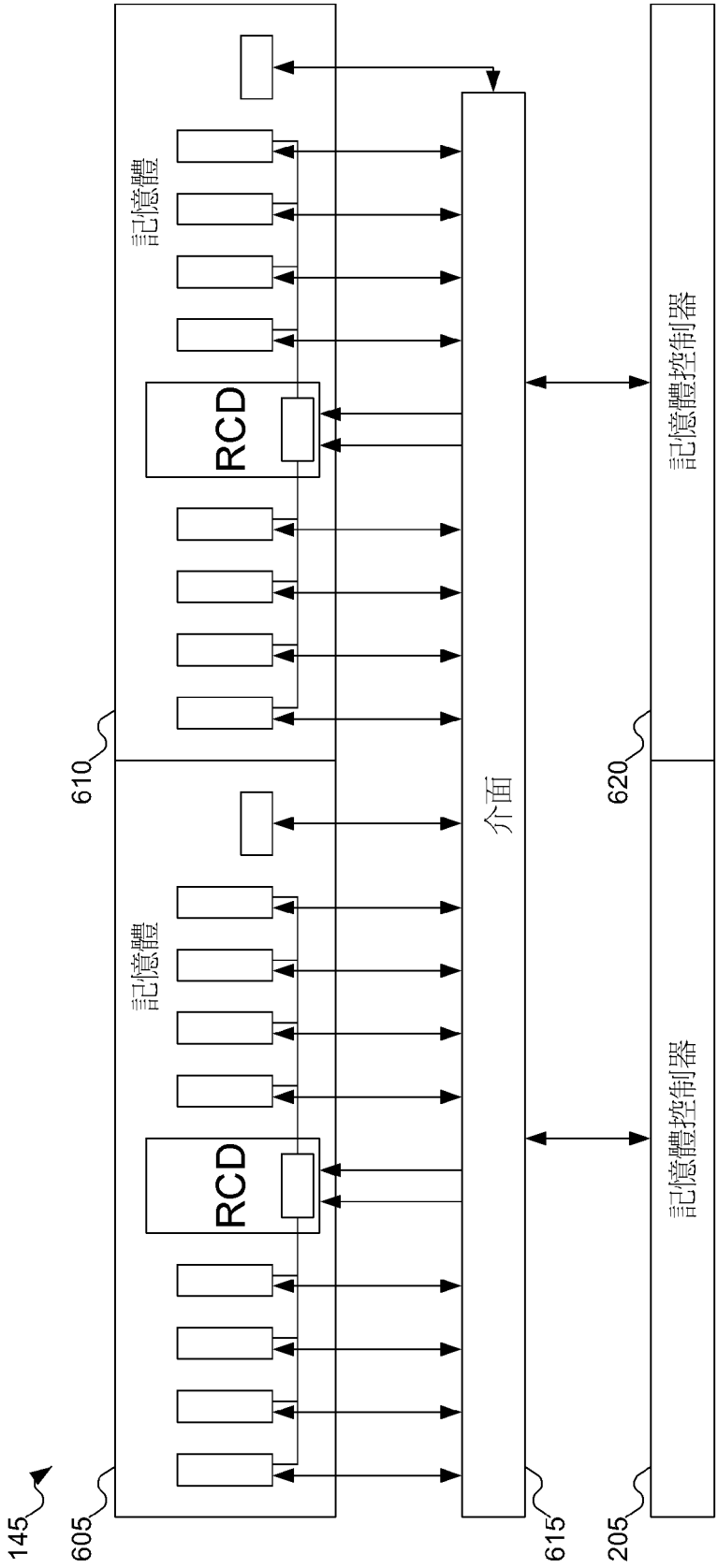
【圖3】


145
記憶體
415
驗證邏輯
420
接收器
430
比較器
435
抹除邏輯
425
阻止邏輯
440
密碼寫入邏輯
355
密碼儲存器
310-345
資料儲存器
405
資料讀取邏輯
410
資料寫入邏輯

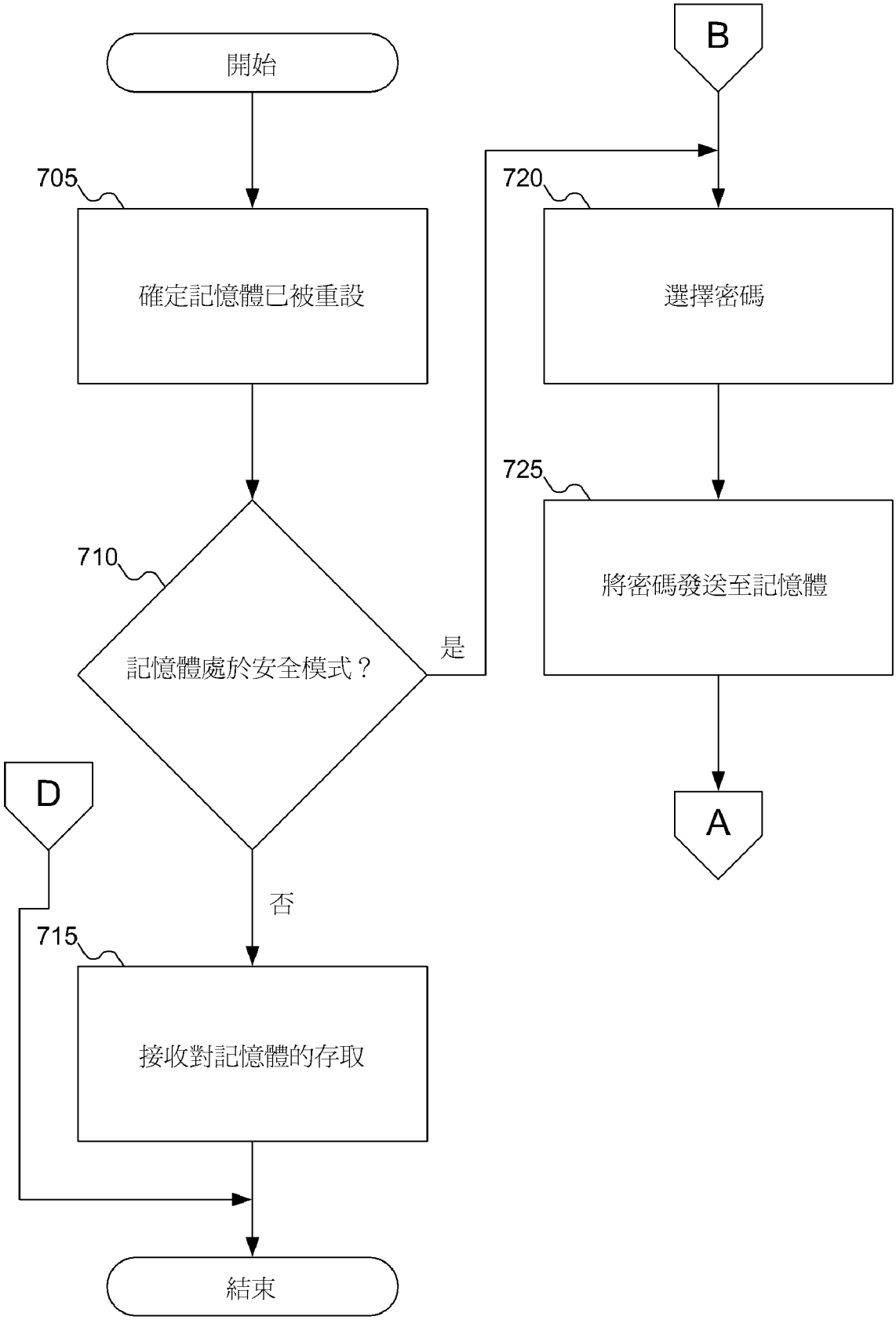
【圖4】



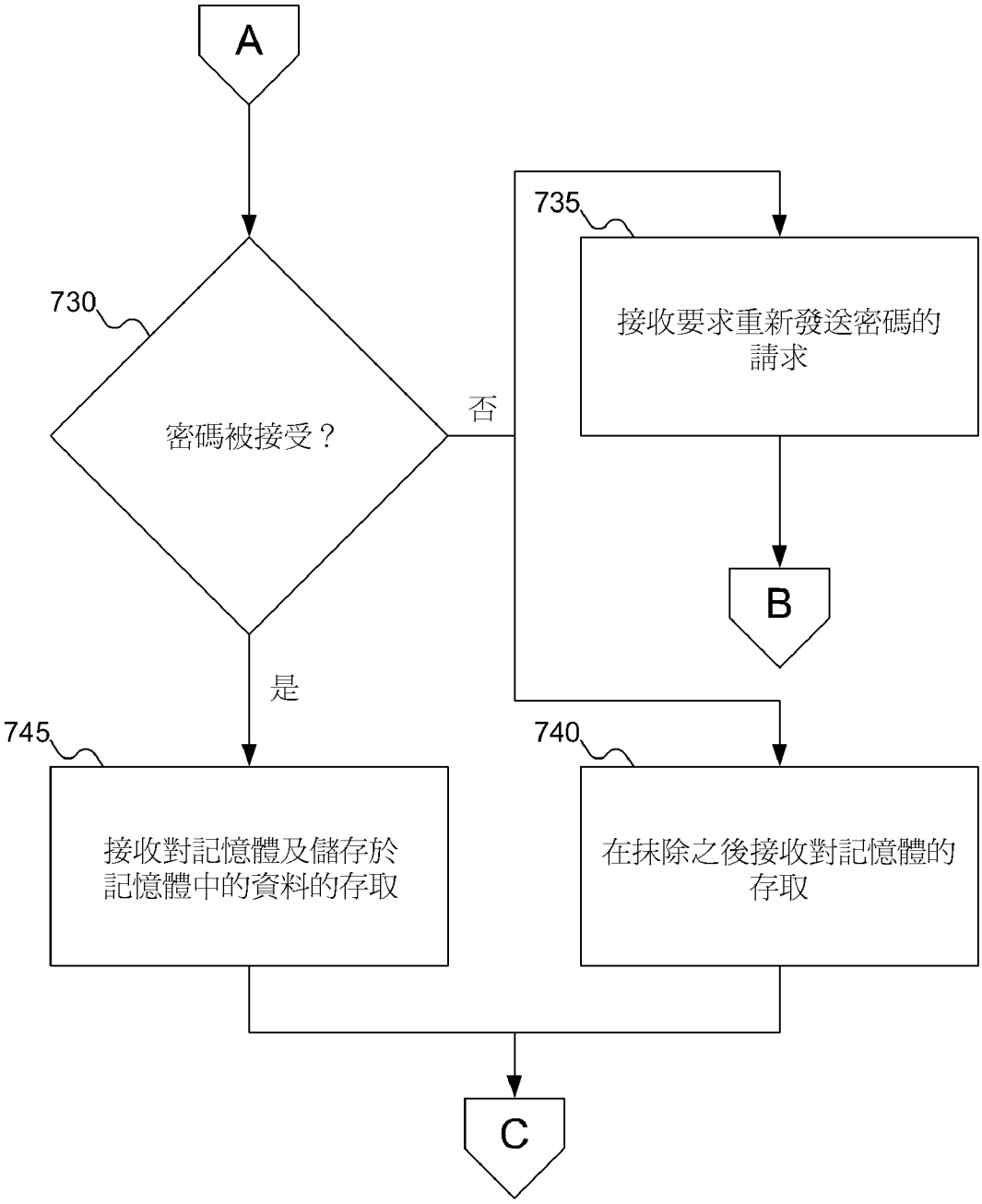
【圖5】



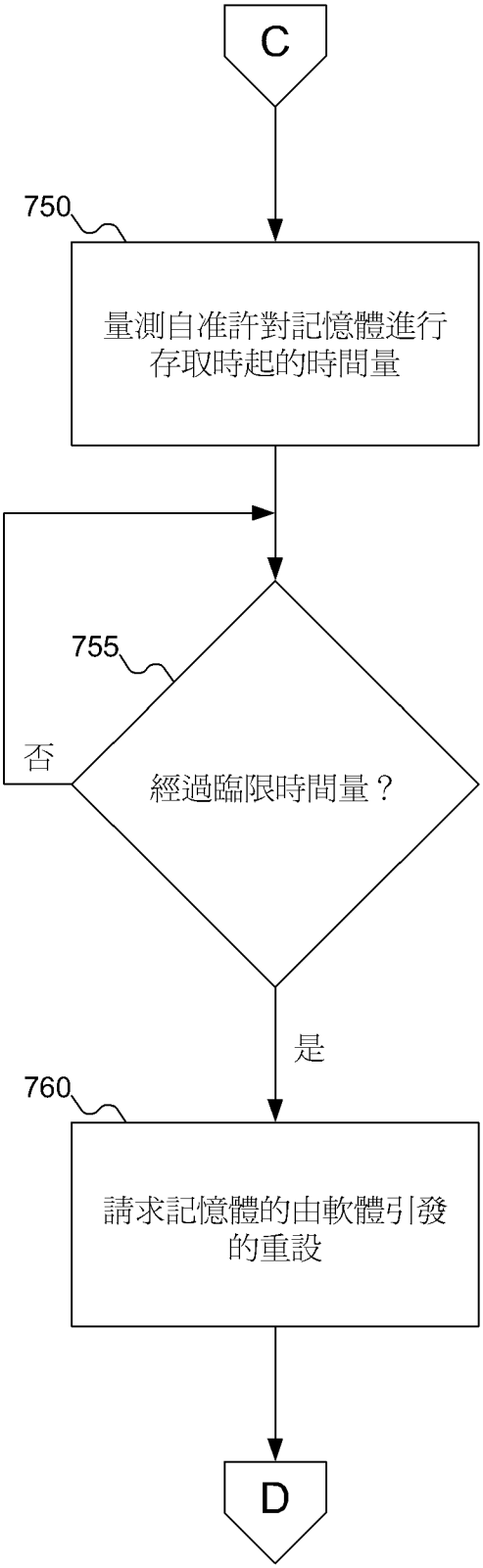
【圖6】


開始
705
確定記憶體已被重設
710
記憶體處於安全模式？
是
否
B
720
選擇密碼
725
將密碼發送至記憶體
A
D
715
接收對記憶體的存取
結束

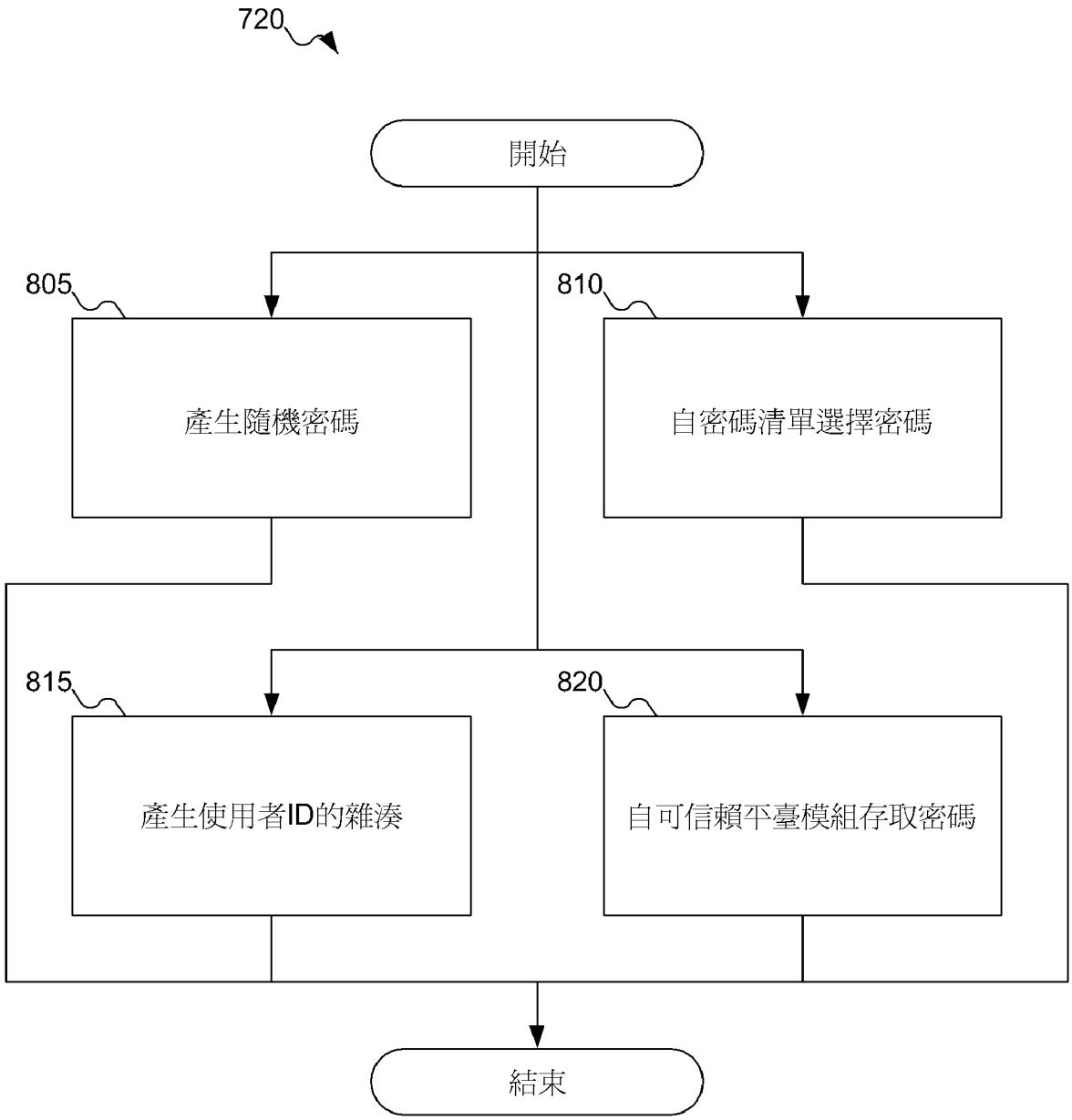
【圖7A】


A
735
接收要求重新發送密碼的請求
730
密碼被接受？
否
B
是
745
接收對記憶體及儲存於記憶體中的資料的存取
740
在抹除之後接收對記憶體的存取
C

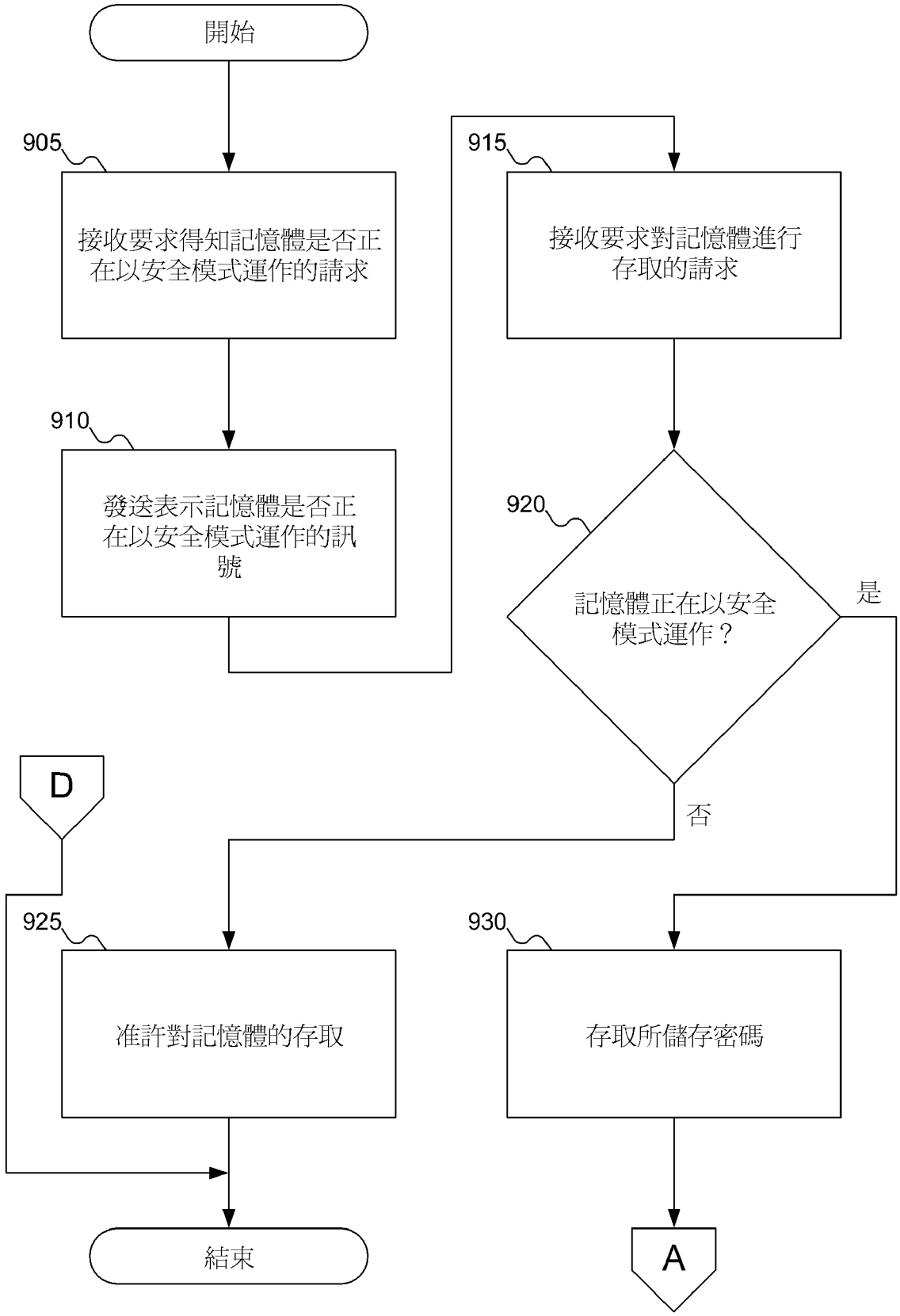
【圖7B】


C
750
量測自准許對記憶體進行存取時起的時間量
755
否
經過臨限時間量？
是
760
請求記憶體的由軟體引發的重設
D

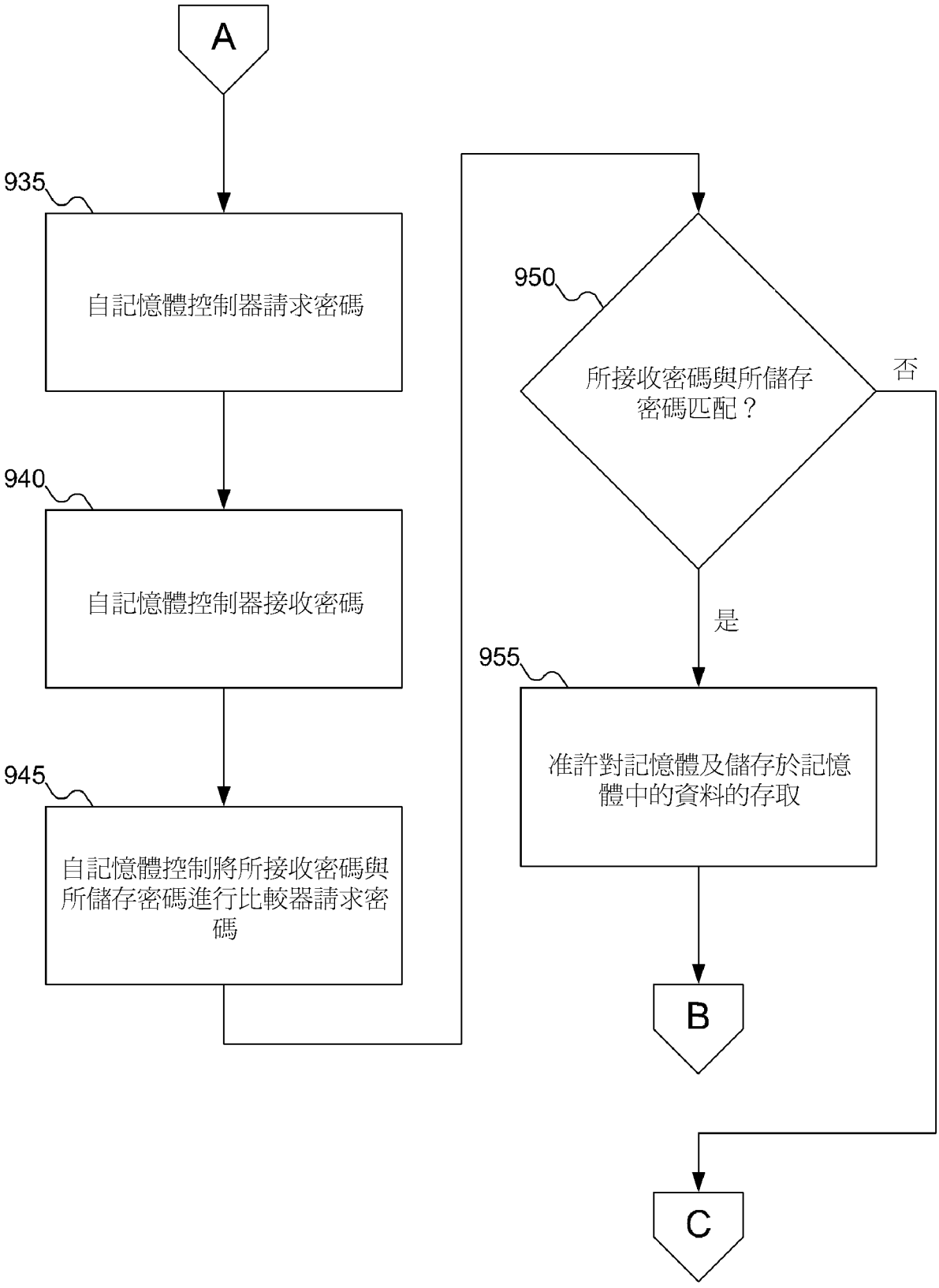
【圖7C】


720
開始
805
產生隨機密碼
810
自密碼清單選擇密碼
815
產生使用者ID的雜湊
820
自可信賴平臺模組存取密碼
結束

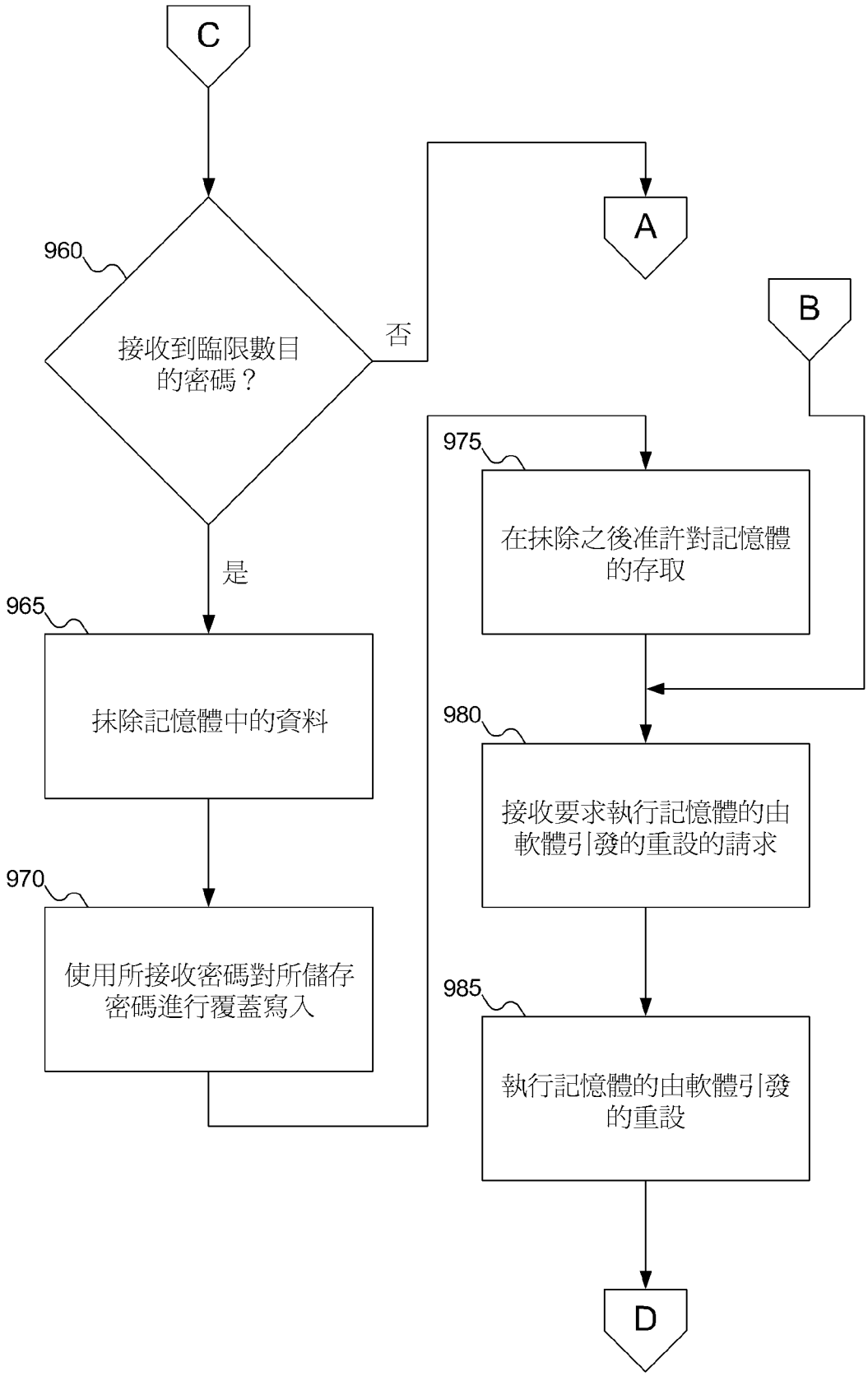
【圖8】


開始
905
接收要求得知記憶體是否正在以安全模式運作的請求
910
發送表示記憶體是否正在以安全模式運作的訊號
915
接收要求對記憶體進行存取的請求
920
記憶體正在以安全模式運作？
是
否
D
925
准許對記憶體的存取
930
存取所儲存密碼
結束
A

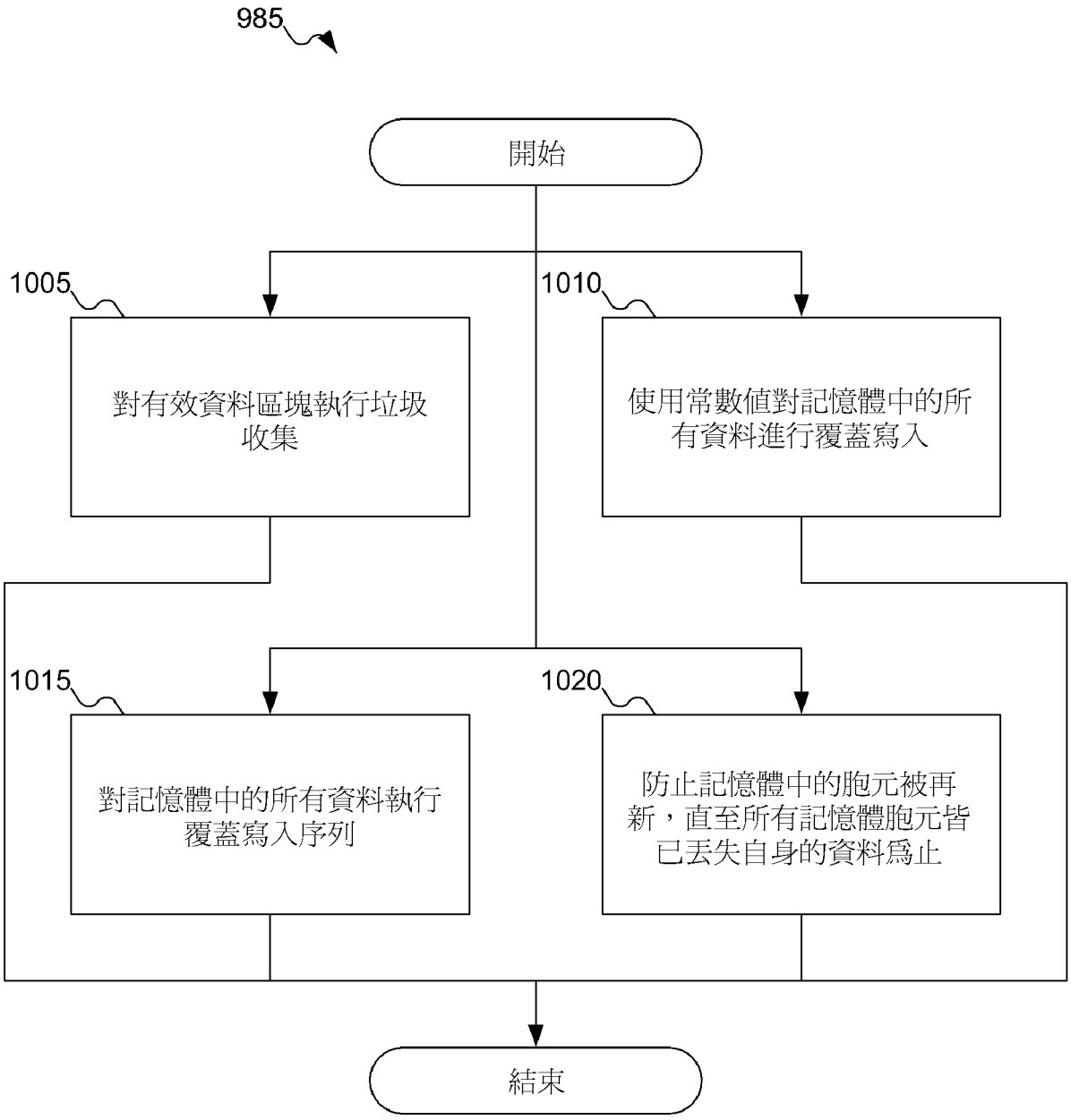
【圖9A】


A
935
自記憶體控制器請求密碼
940
自記憶體控制器接收密碼
945
自記憶體控制將所接收密碼與所儲存密碼進行比較器請求密碼
950
所接收密碼與所儲存密碼匹配？
否
是
955
准許對記憶體及儲存於記憶體中的資料的存取
B
C

【圖9B】


C
960
接收到臨限數目的密碼？
否
A
B
是
965
抹除記憶體中的資料
970
使用所接收密碼對所儲存密碼進行覆蓋寫入
975
在抹除之後准許對記憶體的存取
980
接收要求執行記憶體的由軟體引發的重設的請求
985
執行記憶體的由軟體引發的重設
D

【圖9C】


985
開始
1005
對有效資料區塊執行垃圾收集
1010
使用常數值對記憶體中的所有資料進行覆蓋寫入
1015
對記憶體中的所有資料執行覆蓋寫入序列
1020
防止記憶體中的胞元被再新，直至所有記憶體胞元皆已丟失自身的資料爲止
結束

【圖10】