I751492

(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 I751492 B**

(45)公告日： 中華民國 111 (2022) 年 01 月 01 日

(21)申請案號：109104693 (22)申請日： 中華民國 109 (2020) 年 02 月 14 日

(51)Int. Cl.： ***G06F12/14 (2006.01)*** ***G06F21/78 (2013.01)***

(30)優先權：2019/03/08 美國 16/296,306

(71)申請人：美商萬國商業機器公司 (美國) INTERNATIONAL BUSINESS MACHINES CORPORATION (US)
美國

(72)發明人：布撒巴 法迪 Y BUSABA, FADI Y. (US)；海勒 麗莎 克蘭頓 HELLER, LISA CRANTON (US)；布萊德貝瑞 強納生 D BRADBURY, JONATHAN D. (US)

(74)代理人：陳長文

(56)參考文獻：

TW	200412105A	US	2016/0299851A1
US	2017/0357592A1	US	2018/0373895
US	2019/0042463A1		

審查人員：詹効儒

申請專利範圍項數：25 項 圖式數：22 共 86 頁

(54)名稱

用於跨多個安全網域共用安全記憶體之電腦實施之方法、電腦系統及電腦程式產品

(57)摘要

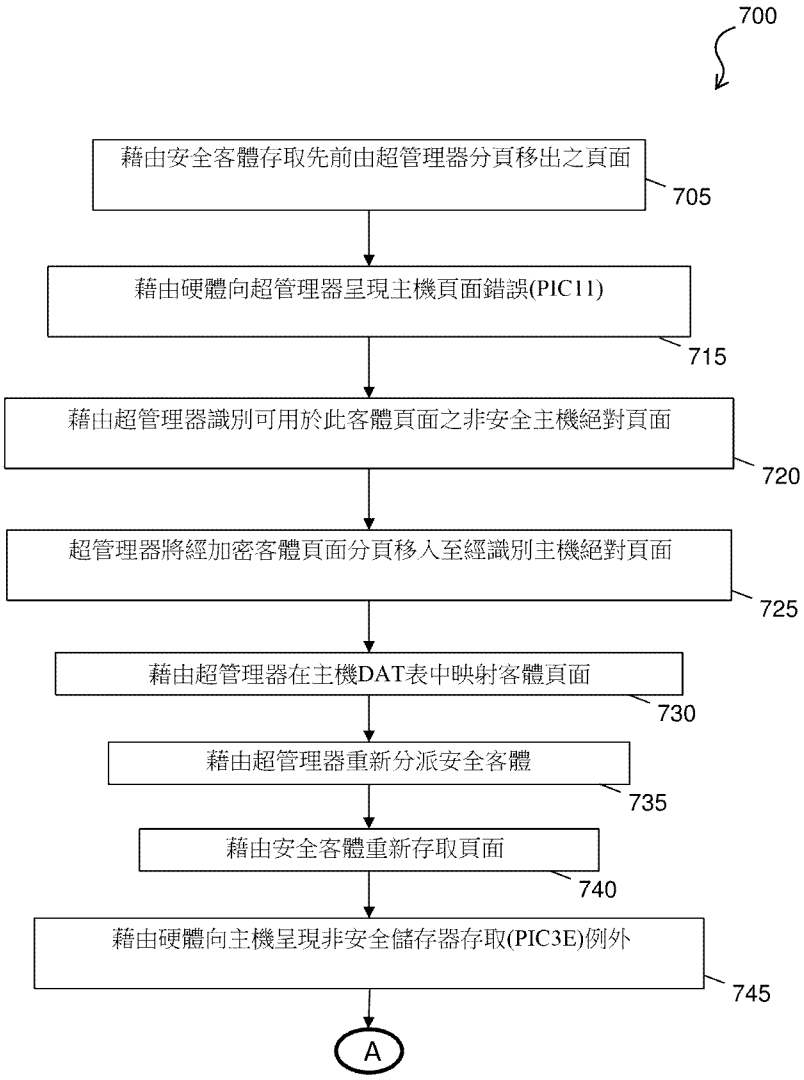
根據本發明之一或多個實施例，一種電腦實施方法包括在一電腦系統之一安全介面控制件處接收對記憶體之一安全頁面的一安全存取請求。該安全介面控制件可檢查與該安全頁面相關聯之一停用虛擬位址比較狀態。該安全介面控制件可基於該停用虛擬位址比較狀態經設定而在存取該安全頁面時停用一虛擬位址檢查以支援將複數個虛擬位址映射至該安全頁面之同一絕對位址，及/或支援使用一絕對位址存取且不具有一相關聯之虛擬位址的安全頁面。

According to one or more embodiments of the present invention, a computer implemented method includes receiving a secure access request for a secure page of memory at a secure interface control of a computer system. The secure interface control can check a disable virtual address compare state associated with the secure page. The secure interface control can disable a virtual address check in accessing the secure page to support mapping of a plurality of virtual addresses to a same absolute address to the secure page based on the disable virtual address compare state being set and/or to support secure pages that are accessed using an absolute address and do not have an associated virtual address.

指定代表圖：

符號簡單說明：

700:用於匯入操作之程序流程



【圖7】

110年11月16日 所提修正替換頁

公告本

I751492

【發明摘要】

【中文發明名稱】

用於跨多個安全網域共用安全記憶體之電腦實施之方法、電腦系統及電腦程式產品

【英文發明名稱】

COMPUTER IMPLEMENT METHOD, COMPUTER SYSTEM AND COMPUTER PROGRAM PRODUCT FOR SHARING SECURE MEMORY ACROSS MULTIPLE SECURITY DOMAINS

【中文】

根據本發明之一或多個實施例，一種電腦實施方法包括在一電腦系統之一安全介面控制件處接收對記憶體之一安全頁面的一安全存取請求。該安全介面控制件可檢查與該安全頁面相關聯之一停用虛擬位址比較狀態。該安全介面控制件可基於該停用虛擬位址比較狀態經設定而在存取該安全頁面時停用一虛擬位址檢查以支援將複數個虛擬位址映射至該安全頁面之同一絕對位址，及/或支援使用一絕對位址存取且不具有一相關聯之虛擬位址的安全頁面。

【英文】

According to one or more embodiments of the present invention, a computer implemented method includes receiving a secure access request for a secure page of memory at a secure interface control of a computer system. The secure interface control can check a disable virtual address compare state associated with the secure page. The secure interface control can disable a virtual address check in accessing the secure page to support mapping of a plurality of virtual addresses to a same absolute address to the secure page based on the disable virtual address compare

state being set and/or to support secure pages that are accessed using an absolute address and do not have an associated virtual address.

【指定代表圖】

圖7

【代表圖之符號簡單說明】

700: 用於匯入操作之程序流程

【發明說明書】

【中文發明名稱】

用於跨多個安全網域共用安全記憶體之電腦實施之方法、電腦系統及電腦程式產品

【英文發明名稱】

COMPUTER IMPLEMENT METHOD, COMPUTER SYSTEM AND COMPUTER PROGRAM PRODUCT FOR SHARING SECURE MEMORY ACROSS MULTIPLE SECURITY DOMAINS

【技術領域】

【先前技術】

【0001】 本發明大體上係關於電腦技術，且更具體而言，係關於跨多個安全網域共用安全記憶體。

【0002】 雲端運算及雲端儲存向使用者提供了在第三方資料中心中儲存及處理其資料之能力。雲端運算促進能夠快速且容易地為客戶佈建VM，而不需要客戶購買硬體或為實體伺服器提供佔用面積。客戶可根據改變之客戶偏好或要求來容易地擴展或收縮VM。通常，雲端運算提供者佈建VM，其實體上駐留於提供者之資料中心處的伺服器上。客戶常常擔心VM中之資料的安全性，此尤其係因為運算提供者常常在同一伺服器上儲存多於一個客戶之資料。客戶可能需要其自身程式碼/資料與雲端運算提供者之程式碼/資料之間以及其自身程式碼/資料與在提供者之站台處執行的其他VM之自身程式碼/資料之間的安全性。此外，客戶可能希望提供者之管理員提供安全性以及希望避免由在機器上執行之其他程式碼可能造成的安全漏洞。

【0003】 為了處置此等敏感情形，雲端服務提供者可實施安全控制以確保適當的資料隔離及邏輯儲存分隔。虛擬化在實施雲端基礎架構中之

廣泛使用為雲端服務之客戶帶來獨特的安全性問題，此係因為虛擬化更改作業系統(OS)與基礎硬體(無論為運算、儲存或甚至網路連接硬體)之間的關係。此引入虛擬化作為額外層，其自身必須經適當地組態、管理及保證安全。

【0004】 一般而言，在主機超管理器之控制下作為客體執行的VM依賴於彼超管理器為彼客體透明地提供虛擬化服務。此等服務包括記憶體管理、指令仿真及中斷處理。

【0005】 在記憶體管理之狀況下，VM可將其資料自磁碟移動(分頁移入)以駐留於記憶體中，且VM亦可將其資料移回(分頁移出)至磁碟。在頁面駐留於記憶體中時，VM (客體)使用動態位址轉譯(DAT)以將記憶體中之頁面自客體虛擬位址映射至客體絕對位址。此外，主機超管理器對於記憶體中之客體頁面具有其自身的DAT映射(自主機虛擬位址至主機絕對位址)，且其可獨立地且對客體透明地將客體頁面分頁移入及移出記憶體。超管理器經由主機DAT表在兩個分開的客體VM之間提供記憶體隔離或客體記憶體共用。主機亦能夠在必要時代表客體存取客體記憶體以模擬客體操作。

【發明內容】

【0006】 根據本發明之一或多個實施例，一種電腦實施方法包括在電腦系統之安全介面控制件處接收對記憶體之安全頁面的安全存取請求。安全介面控制件可檢查與安全頁面相關聯之停用虛擬位址比較狀態。安全介面控制件可基於停用虛擬位址比較狀態經設定而在存取安全頁面時停用虛擬位址檢查，以支援將複數個虛擬位址映射至安全頁面之同一絕對位址。優點可包括跨多個安全網域共用安全記憶體。

【0007】 根據本發明之額外或替代實施例，安全介面控制件可基於網域識別符驗證複數個安全網域中之一安全網域經授權以存取共用頁面。優點可包括基於網域識別符限制共用。

【0008】 根據本發明之額外或替代實施例，可比較該安全網域之該網域識別符與識別為允許共用之該等安全網域的複數個網域識別符，以確認對存取共用頁面之授權。優點可包括將共用限於網域識別符之清單中的成員。

【0009】 根據本發明之額外或替代實施例，安全介面控制件可確認，對於可存取安全頁面之多個安全網域中之任一者，將虛擬位址映射至絕對位址之動態位址轉譯表之複數個群組藉由經組態以管理動態位址轉譯表之群組中之一或多者的不安全主機保持不變，其中用於虛擬位址之每一表映射包括動態位址轉譯表之一或多個群組中的多個相關聯表。安全存取請求可基於偵測到動態位址轉譯表之一或多個群組中之改變而終止。優點可包括確認不安全主機不會修改用以存取安全頁面之位址映射。

【0010】 根據本發明之額外或替代實施例，停用虛擬位址比較狀態可經由區域安全性表儲存及更新，該區域安全性表包括與安全頁面相關聯之安全網域識別符、與安全頁面相關聯之虛擬位址映射資料以及停用虛擬位址比較狀態。優點可包括追蹤及組態每個安全網域及/或記憶體頁面之選項。

【0011】 根據本發明之額外或替代實施例，安全介面控制件可為韌體、硬體、受信任軟體或韌體、硬體及受信任軟體之組合。安全頁面可經指派給由超管理器或作業系統管理之安全虛擬機器或安全容器。優點可包括以對整個系統效能具有低的相關聯操作影響來實施安全介面控制件。

【0012】 根據本發明之一或多個實施例，一種電腦實施方法包括在電腦系統之安全介面控制件處接收對記憶體之安全頁面的安全存取請求。安全介面控制件可檢查與安全頁面相關聯之停用虛擬位址比較狀態。安全介面控制件可基於進行安全存取請求之實體的授權狀態及停用虛擬位址比較狀態經設定而啟用對未指定虛擬位址之安全頁面的絕對位址存取。優點可包括支援絕對位址存取以用於共用安全頁面。

【0013】 本發明之其他實施例在電腦系統及電腦程式產品中實施上述方法之特徵。

【0014】 額外特徵及優點經由本發明之技術實現。本文中詳細描述本發明之其他實施例及態樣且將其視為本發明之一部分。為更好地理解具有該等優點及特徵的本發明，參考描述及圖式。

【圖式簡單說明】

【0015】 在本說明書之結尾處的申請專利範圍中特別地指出且清楚地主張本文中所描述之排他性權利的細節。本發明之實施例的前述以及其他特徵及優點自結合隨附圖式進行之以下詳細描述顯而易見，在隨附圖式中：

【0016】 圖1描繪根據本發明之一或多個實施例的區域安全性表；

【0017】 圖2描繪根據本發明之一或多個實施例的用於執行DAT之虛擬及絕對位址空間；

【0018】 圖3描繪根據本發明之一或多個實施例的支援在超管理器下執行之虛擬機器(VM)的巢套之多部分DAT；

【0019】 圖4描繪根據本發明之一或多個實施例的安全客體儲存之映射；

【0020】 圖5描繪根據本發明之一或多個實施例的動態位址轉譯(DAT)操作之系統示意圖；

【0021】 圖6描繪根據本發明之一或多個實施例的安全介面控制件記憶體之系統示意圖；

【0022】 圖7描繪根據本發明之一或多個實施例的匯入操作之程序流程；

【0023】 圖8描繪根據本發明之一或多個實施例的匯入操作之程序流程；

【0024】 圖9描繪根據本發明之一或多個實施例的所供給記憶體操作之程序；

【0025】 圖10描繪根據本發明之一或多個實施例的非安全超管理器頁面至安全介面控制件之安全頁面的轉變之程序流程；

【0026】 圖11描繪根據本發明之一或多個實施例的由安全介面控制件進行之安全儲存器存取的程序流程；

【0027】 圖12描繪根據本發明之一或多個實施例的藉由安全介面控制件及硬體進行存取標示的程序流程；

【0028】 圖13描繪根據本發明之一或多個實施例的藉由程式及安全介面控制件進行之支援安全存取及非安全存取的轉譯之程序流程；

【0029】 圖14描繪根據本發明之一或多個實施例的藉由程式及安全介面控制件進行之具有安全儲存保護的DAT之程序流程；

【0030】 圖15描繪根據本發明之一或多個實施例的用於虛擬位址模式檢查之程序流程；

【0031】 圖16描繪根據本發明之一或多個實施例的經由位址轉譯之

頁面共用的方塊圖；

【0032】 圖17描繪根據本發明之一或多個實施例的經由位址轉譯及頁面複製之頁面共用的方塊圖；

【0033】 圖18描繪根據本發明之一或多個實施例的用於跨多個安全網域共用安全記憶體之程序流程；

【0034】 圖19說明根據本發明之一或多個實施例的雲端運算環境；

【0035】 圖20描繪根據本發明之一或多個實施例的抽象模型層；

【0036】 圖21描繪根據本發明之一或多個實施例的系統；及

【0037】 圖22描繪根據本發明之一或多個實施例的處理系統。

【0038】 本文中所描繪之圖式為說明性的。在不背離本發明之精神的情況下，所描述之圖式或操作可存在許多變化。舉例而言，可以不同次序執行動作或可添加、刪除或修改動作。又，術語「耦接」及其變化描述在兩個元件之間具有通信路徑且並不暗示元件之間的直接連接且其間不具有插入元件/連接。所有此等變體視為本說明書之一部分。

【實施方式】

【0039】 本發明之一或多個實施例利用軟體與機器之間的高效輕量安全介面控制件以提供額外安全性。

【0040】 在主機超管理器之控制下作為客體執行的虛擬機器(VM)依賴於彼超管理器為彼客體透明地提供虛擬化服務。此等服務可應用於安全實體與另一不受信任實體之間的任何介面，其在傳統上允許此另一實體存取安全資源。如先前所提及，此等服務可包括但不限於記憶體管理、指令仿真及中斷處理。舉例而言，對於中斷及例外注入，超管理器通常讀取及/或寫入至客體之前置詞區(prefix area)(低核心)中。如本文中所使用之術

語「虛擬機器」或「VM」係指實體機器(運算裝置、處理器等)及其處理環境(作業系統(OS)、軟體資源等)之邏輯表示。VM維持為在基礎主機機器(實體處理器或處理器集合)上執行之軟體。自使用者或軟體資源之視角，VM呈現為其自身的獨立實體機器。如本文中所使用之術語「超管理器」及「VM監視器(VMM)」係指管理及准許多個VM在同一主機機器上使用多個(且有時不同的) OS執行的處理環境或平台服務。應瞭解，部署VM包括VM之安裝程序及VM之起動(或啟動)程序。在另一實例中，部署VM包括VM之起動(或啟動)程序(例如，在VM先前已安裝或已存在之狀況下)。

【0041】 為了促進及支援安全客體，存在技術挑戰：超管理器與安全客體之間需要額外安全性而不依賴於超管理器，使得超管理器無法存取來自的VM資料且因此無法以上文所描述之方式提供服務。

【0042】 本文中所描述之安全執行提供保證安全儲存與非安全儲存之間以及屬於不同安全使用者之安全儲存之間的隔離的硬體機構。對於安全客體，在「不受信任」之非安全超管理器與安全客體之間提供額外安全性。為進行此操作，超管理器通常代表客體執行之許多功能需要併入至機器中。本文中描述新的安全介面控制件，在本文中亦被稱作「UV」，以在超管理器與安全客體之間提供安全介面。術語安全介面控制件與UV在本文中可互換使用。安全介面控制件與硬體協作以提供此額外安全性。此外，較低層級超管理器可為此不受信任超管理器提供虛擬化，且若此較低層級超管理器以受信任程式碼(例如，受信任軟體)實施，則其亦可為安全介面控制件之部分。

【0043】 在一個實例中，安全介面控制件實施於內部、安全且受信

任的硬體及/或韌體中。此受信任韌體可包括例如處理器微碼或PR/SM邏輯分割程式碼。對於安全客體或實體，安全介面控制件提供安全環境之初始化及維護以及此等安全實體之分派在硬體上的協調。在安全客體主動地使用資料且資料駐留於主機儲存器中時，其「以純文字(in the clear)」保存在安全儲存器中。安全客體儲存器可由彼單一安全客體存取，該安全客體嚴格地由硬體執行。亦即，硬體防止任何非安全實體(包括超管理器或其他非安全客體)或不同安全客體存取彼資料。在此實例中，安全介面控制件作為韌體之最低層級的受信任部分而執行。最低層級或微碼實際上為硬體之擴充且用以實施例如在來自IBM之zArchitecture®中定義的複雜指令及功能。微碼可存取儲存器之所有部分，該儲存器在安全執行之情況下包括其自身的安全UV儲存器、非安全超管理器儲存器、安全客體儲存器及共用儲存器。此允許其提供安全客體或支援彼客體之超管理器所需的任何功能。安全介面控制件亦可直接存取硬體，此允許硬體在由安全介面控制件建立之條件的控制下高效地提供安全性檢查。

【0044】 根據本發明之一或多個實施例，軟體使用UV呼叫(UVC)指令以請求安全介面控制件執行特定動作。舉例而言，UVC指令可由超管理器使用以初始化安全介面控制件，建立安全客體網域(例如，安全客體組態)且在彼安全組態內建立虛擬CPU。其亦可用以匯入(解密且指派給安全客體網域)及匯出(加密且允許主機存取)安全客體頁面，作為超管理器分頁移入或分頁移出操作之部分。此外，安全客體能夠定義與超管理器共用之儲存器，使安全儲存器共用且使共用儲存器安全。

【0045】 類似於許多其他架構化指令，此等UVC命令可由機器韌體執行。機器不進入安全介面控制模式，而是機器在其當前正執行之模式中

執行安全介面控制功能。硬體維持韌體狀態及軟體狀態兩者，因此不切換內容脈絡以便處置此等操作。此低額外負荷允許軟體、受信任韌體及硬體之不同層之間的緊密合作，其方式為最小化及降低安全介面控制件之複雜度，同時仍提供必要的安全等級。

【0046】 根據本發明之一或多個實施例，為支援安全介面控制件及硬體所需之控制區塊結構以適當地維護安全客體且支援超管理器環境，超管理器將儲存器供給至安全介面控制件，同時初始化安全客體環境。結果，為準備1)初始化區域以執行安全客體，2)建立安全客體網域及3)建立在該等域中之每一者中執行的安全CPU，超管理器發出查詢UVC指令以尤其判定供給所需之儲存器量。一旦已供給儲存器，則將其標記為安全且註冊為屬於安全介面控制件；且禁止任何非安全或安全客體實體之存取。此狀況保持，直至相關聯實體(例如，安全客體CPU、安全客體網域或區域)被毀壞時。

【0047】 在一個實例中，為支援區域特定UV控制區塊，作為初始化UVC之部分，UV儲存器之第一區段經供給至安全介面控制件且駐留於在本文中所稱的UV2儲存器中。為支援基本及可變安全客體組態控制區塊(對於每一安全客體網域)，作為建立安全客體組態UVC之部分，UV儲存器之第二區段及第三區段經供給且分別駐留於UVS及UVV儲存器中。為支援安全CPU控制區塊，UV儲存器之第四及最終區段亦駐留於UVS空間中且作為建立安全客體CPU UVC之部分而供給。在此等區域中之每一者經供給時，安全控制介面將其標記為安全(以防止其被任何非安全實體存取)，且亦在區域安全性表中將其註冊為屬於安全介面控制件(以防止其被任何安全客體實體存取)。為了在UV空間內提供進一步隔離，UV2空間

(其不與任何特定安全客體網域相關聯)亦使用唯一UV2安全網域來標示，而UVS及UVV空間均進一步使用相關聯之特定安全客體網域來標示。在此實例中，UVV空間駐留於主機虛擬空間中，且因此，可進一步使用主機虛擬至主機絕對映射來識別。

【0048】 儘管安全介面控制件可存取所有儲存器(非安全儲存器、安全客體儲存器及UV儲存器)，但本發明之一或多個實施例提供允許安全介面控制件非常特定地存取UV儲存器之機制。使用在安全客體網域之間提供隔離的相同硬體機構，本發明之實施例可在UV儲存器內提供類似隔離。此保證安全介面控制件僅在預期且指定時存取UV儲存器；僅存取用於所要的指定安全客體之安全客體儲存器；且僅在指定時存取非安全儲存器。亦即，安全介面控制件可非常明確地指定其意欲存取的儲存器，使得硬體可保證其實際上確實存取彼儲存器。此外，可進一步指定其僅意欲存取與指定安全客體網域相關聯之UV儲存器。

【0049】 為提供安全性，當超管理器透明地分頁移入及分頁移出安全客體資料時，與硬體一起工作之安全介面控制件提供及保證資料之解密及加密。為實現此，需要超管理器在分頁移入及分頁移出客體安全資料時發出新的UVC。基於由安全介面控制件在此等新UVC期間設置之控制，硬體將保證此等UVC實際上由超管理器發出。

【0050】 在此新的安全環境中，每當超管理器分頁移出安全頁面時，需要其發出新的自安全儲存器轉換(匯出) UVC。回應於此匯出UVC，安全介面控制件將1)指示頁面由UV「鎖定」，2)對頁面加密，3)將頁面設定為非安全且4)重設UV鎖定。一旦匯出UVC完成，超管理器現便可分頁移出經加密之客體頁面。

【0051】 此外，每當超管理器分頁移入安全頁面時，其必須發出新的至安全儲存器轉換(匯入) UVC。回應於此匯入UVC，UV或安全介面控制件將1)在硬體中將頁面標記為安全，2)指示頁面由UV「鎖定」，3)對頁面解密，4)向特定安全客體網域設定授權且5)重設UV鎖定。每當安全實體進行存取時，硬體便在轉譯期間執行關於彼頁面之授權檢查。此等檢查包括1)驗證頁面實際上確實屬於正試圖存取其之安全客體網域的檢查，及2)確保在此頁面已駐留於客體記憶體中時超管理器未改變此頁面之主機映射的檢查。一旦頁面標記為安全，硬體便防止超管理器或非安全客體VM存取任何安全頁面。額外轉譯步驟防止另一安全VM進行存取且防止超管理器進行重新映射。

【0052】 對於諸如安全VM或容器之安全實體，記憶體之每一絕對頁面通常經指派給一個安全VM (或容器)且不允許其他VM/容器或超管理器/OS進行存取或與其他VM/容器或超管理器/OS共用。在某些執行環境中，可存在邏輯上在各種安全VM/容器間共用之共同安全記憶體(例如，OS內核中之安全資料庫或安全共用區)。管理不同VM (或容器)之超管理器(或OS)可為執行VM (或容器)中之每一者指派不同記憶體位址空間，以達成所需記憶體隔離。每一執行VM (或容器)可呈現為具有其自身的與任何其他執行VM (或容器)不同的位址空間。為了在此等VM間共用共同儲存器，超管理器可經由位址轉譯將來自各種執行VM之虛擬位址映射至同一實體記憶體中。對於安全VM/容器，超管理器/OS可能不受信任且通常可能禁止將來自各種VM之不同虛擬位址映射至單一絕對位址。安全介面控制件可負責驗證虛擬至實體位址之映射未被非安全超管理器/OS篡改。用於頁面共用而不複製映射之可能暫時解決方案可包括使用複製複本，一個複本經

指派給每一執行VM或容器。當共用共同安全資料庫之複雜度增加至管理複製影像之複雜度時，此方法對於執行數千個VM或容器影像之系統可能為不可行的。

【0053】 如上文所提及，除了其他以外，安全介面控制件亦可負責保證位址轉譯完整度。除安全客體儲存器以外，亦可存在自超管理器儲存器供給且給予安全介面控制件之記憶體區。此等區可能僅可由安全介面控制件存取。此等區可作為絕對記憶體進行維護及參考且通常不經受動態位址轉譯。此等安全絕對頁面可能不具有與其相關聯之虛擬位址映射。本發明之實施例可應用於執行中安全容器或安全VM，且允許在安全OS與安全容器之間或在超管理器與安全VM之間共用安全共同區。如本文中進一步所描述，亦可支援多個執行中安全容器/VM間的共用。

【0054】 現轉向圖1，總體上展示根據本發明之一或多個實施例的區域安全性表100。圖1中所展示之區域安全性表100由安全介面控制件維持，且由安全介面控制件及硬體使用以保證對由安全實體存取之任何頁面的安全存取。區域安全性表100藉由主機絕對位址110編索引。亦即，對於主機絕對儲存器之每一頁面，皆存在一個項目。每一項目包括用以驗證該項目屬於進行存取之安全實體的資訊。

【0055】 另外，如圖1中所展示，區域安全性表100包括安全網域ID 120 (識別與此頁面相關聯之安全網域)；UV位元130 (指示此頁面被供給安全介面控制件且由安全介面控制件擁有)；停用位址比較(DA)位元140 (用以在某些情形中，諸如在定義為主機絕對之安全介面控制件頁面不具有相關聯之主機虛擬位址時，停用主機位址對比較)；共用(SH)位元150 (指示與非安全超管理器共用頁面)；及主機虛擬位址160 (指示針對此主機

絕對位址註冊之主機虛擬位址，其被稱作主機位址對)。應注意，主機位址對指示主機絕對位址及相關聯之所註冊主機虛擬位址。主機位址對表示此頁面(一旦由超管理器匯入)之映射，且比較保證在彼頁面正由客體使用時主機不重新映射該頁面。

【0056】 動態位址轉譯(DAT)用以將虛擬儲存器映射至真實儲存器。當客體VM在超管理器之控制下作為可分頁客體執行時，客體使用DAT來管理駐留於其記憶體中之頁面。此外，主機在客體頁面駐留於其記憶體中時獨立地使用DAT來管理彼等頁面(連同其自身頁面)。超管理器使用DAT來提供不同VM之間的儲存隔離及/或共用以及防止客體存取超管理器儲存器。當客體正以非安全模式執行時，超管理器可存取所有客體儲存器。

【0057】 DAT使得能夠隔離一個應用程式與另一應用程式，同時仍准許該等應用程式共用共同資源。又，DAT准許實施VM，其可用於設計及測試OS之新版本連同並行處理應用程式。虛擬位址識別虛擬儲存器中之位置。位址空間為虛擬位址之連續序列連同特定變換參數(包括DAT表)，其允許每一虛擬位址轉譯成相關聯之絕對位址，該絕對位址藉由儲存器中之位元組位置識別彼位址。

【0058】 DAT使用多表查找(例如，每轉譯查找DAT表之群組)以將虛擬位址轉譯成相關聯之絕對位址。此表結構通常由儲存管理器定義及維持。此儲存管理器藉由分頁移出一個頁面例如以調入另一頁面來在多個程式之間透明地共用絕對儲存器。舉例而言，當頁面被分頁移出時，儲存管理器將在相關聯之頁表中設定無效位元。當程式試圖存取被分頁移出之頁面時，硬體將向儲存管理器呈現程式中斷，其常常被稱作頁面錯誤。作為

回應，儲存管理器將分頁移入所請求頁面且重設無效位元。此皆透明於程式而進行，且允許儲存管理器虛擬化儲存器並在各種不同使用者間共用該儲存器。

【0059】 當虛擬位址由CPU使用以存取主儲存器時，其首先藉助於DAT轉換成真實位址且接著藉助於前置詞轉換成絕對位址。用於特定位址空間之最高層級表的指定項(起點及長度)被稱作位址空間控制元素(ASCE)且定義相關聯之位址空間。

【0060】 根據本發明之一或多個實施例，圖1之區域安全性表100中的DA位元140可與每一安全頁面相關聯，以停用由安全介面控制件進行之虛擬位址檢查，以存取安全頁面。DA位元140可為在安全介面控制件之控制下的欄位。當安全頁面註冊於區域安全性表中且指派給安全網域時，可適當地設定DA位元140。當存取安全頁面時，可將DA位元用作由安全介面控制件進行之安全性檢查的一部分，以判定是否允許存取。當DA位元為零時，在對安全頁面進行存取時由安全介面控制件進行之安全性檢查的部分為確保在不瞭解安全介面控制件之情況下，不會修改安全頁面之DAT轉譯表。一旦向安全網域給定頁面，主機虛擬位址160 (與主機絕對位址組合以建立主機位址對)便連同相關聯之安全網域ID 120及圖1中所展示之與彼安全頁面相關聯的其他屬性一起註冊於圖1之用於彼頁面的區域安全性表100中。對於對頁面之每一存取，安全介面控制件可藉由比較存取虛擬/絕對主機位址對及存取安全網域ID與先前所註冊之位址對及域ID來驗證存取。若存在比較錯誤，則安全介面控制件可報告例外。因此，當DA=0時，僅一個主機虛擬位址可映射至任何給定主機絕對位址。

【0061】 如描述於本發明之一或多個實施例中，DA位元標記在經

設定時可允許將許多主機虛擬位址映射至同一主機絕對位址。DA位元標記可在安全介面控制件之控制下，且可僅針對經授權以與其他域共用頁面之域及標記為安全共同頁面中主機虛擬頁面而設定。因此，當DA=1時，可存在跨各種安全網域之唯一或相同的一對一虛擬至絕對位址映射，且每一一對一映射可由一個安全網域擁有。DA位元亦可針對由超管理器供給至安全介面控制件且定義為絕對位址之主機絕對頁面(例如，未指定虛擬位址之頁面)而設定。為支援兩種用途，安全介面控制件及/或其他系統組件可忽略對使用DA=1標記之頁面的虛擬位址檢查。標記可與特定頁面相關聯且未必適用於整個安全網域。此外，當頁面為安全頁面時，系統可驗證僅經授權容器/VM可存取共用安全頁面。

【0062】 現轉向圖2，總體上展示根據本發明之一或多個實施例的用於執行DAT之實例虛擬位址空間202及204以及絕對位址空間206。在圖2中所展示之實例中，存在兩個虛擬位址空間：虛擬位址空間202 (由位址空間控制元素(ASCE) A 208定義)及虛擬位址空間204 (由ASCE B 210定義)。虛擬頁面A1.V 212a1、A2.V 212a2及A3.V 212a3藉由儲存管理器使用ASCE A 208在多表(區段230及頁表232a、232b)查找中映射至絕對頁面A1.A 220a1、A2.A 220a2及A3.A 220a3。類似地，虛擬頁面B1.V 214b1及B2.V 214b2係使用ASCE B 210分別在兩表234及236查找中映射至絕對頁面B1.A 222b1 及B2.A 222b2。

【0063】 現轉向圖3，總體上展示根據本發明之一或多個實施例的用以支援在超管理器下執行之VM的巢套之多部分DAT轉譯之實例。在圖3中所展示之實例中，客體A虛擬位址空間A 302 (由客體ASCE (GASCE) A 304定義)及客體B虛擬位址空間B 306 (由GASCEB 308定義)兩者駐留於

共用主機(超管理器)虛擬位址空間325中。如所展示，屬於客體A之虛擬頁面A1.GV 310a1、A2.GV 310a2及A3.GV 310a3分別藉由客體A儲存管理器使用GASCEA 304映射至客體絕對頁面A1.HV 340a1、A2.HV 340a2及A3.HV 340a3；屬於客體B之虛擬頁面B1.GV 320b1及B2.GV 320b2分別獨立地藉由客體B儲存管理器使用GASCEB 308映射至客體絕對頁面B1.HV 360b1及B2.HV 360b2。在此實例中，此等客體絕對頁面直接映射至共用主機虛擬位址空間325中，且隨後經歷至主機絕對位址空間330之額外主機DAT轉譯映射。如所展示，主機虛擬位址A1.HV 340a1、A3.HV 340a3及B1.HV 360b1藉由主機儲存管理器使用主機ASCE (HASCE) 350映射至A1.HA 370a1、A3.HA 370a3及B1.HA 370b1。屬於客體A之主機虛擬位址A2.HV 340a2及屬於客體B之B2.HV 360b2兩者映射至同一主機絕對頁面AB2.HA 380。此使得能夠在此等兩個客體之間共用資料。在客體DAT轉譯期間，客體表位址中之每一者被視為客體絕對位址且經歷額外巢套之主機DAT轉譯。

【0064】 本文中所描述之本發明之實施例提供安全客體及UV儲存保護。禁止非安全客體及超管理器存取安全儲存器。超管理器規定，對於給定駐留的安全客體頁面，以下情況發生。相關聯之主機絕對位址僅可經由單一超管理器(主機) DAT映射存取。亦即，存在映射至指派給安全客體之任何給定主機絕對位址的單一主機虛擬位址。與給定安全客體頁面相關聯之超管理器DAT映射(主機虛擬至主機絕對)在頁面被分頁移入時不改變。對於單一安全客體，映射與安全客體頁面相關聯之主機絕對頁面。

【0065】 根據本發明之一或多個實施例，亦禁止在安全客體之間共用儲存器。儲存器在安全客體之控制下在單一安全客體與超管理器之間共

用。UV儲存器為安全儲存器且可由安全介面控制件存取但不可由客體/主機存取。儲存器藉由超管理器分配至安全介面控制件。根據本發明之一或多個實施例，硬體及安全介面控制件禁止任何嘗試違反此等規則之行為。

【0066】 現轉向圖4，總體上展示根據本發明之一或多個實施例的安全客體儲存器之映射的實例。圖4類似於圖3，除了圖4之實例不允許在安全客體A與安全客體B之間共用儲存器以外。在圖3之非安全實例中，屬於客體A之主機虛擬位址A2.HV 340a2及屬於客體B之B2.HV 360b2兩者映射至同一主機絕對頁面AB2.HA 380。在圖4之安全客體儲存實例中，屬於客體A之主機虛擬位址A2.HV 340a2映射至主機絕對位址A2.HA 490a，而屬於客體B之B2.HV 360b2映射至其自身的B2.HA 490b。在此實例中，安全客體之間不存在共用。

【0067】 在安全客體頁面駐留於磁碟上時，其經加密。當超管理器分頁移入安全客體頁面時，其發出UV呼叫(UVC)，該呼叫使安全介面控制件將頁面標記為安全(除非共用)，對其解密(除非共用)且將其註冊(在區域安全性表中)為屬於適當安全客體(例如，客體A)。此外，其將相關聯之主機虛擬位址(例如，A3.HV 340a3)註冊至彼主機絕對頁面(被稱作主機位址對)。若超管理器未能發出正確UVC，則其在試圖存取安全客體頁面時接收例外。當超管理器分頁移出客體頁面時，發出類似UVC，其對客體頁面(除非共用)加密，之後將客體頁面標記為非安全且在區域安全性表中將其註冊為非安全。

【0068】 在具有五個給定主機絕對頁面K、P、L、M及N之實例中，當超管理器分頁移入該等主機絕對頁面時，其中之每一者由安全介面控制件標記為安全。此防止非安全客體及超管理器存取該等頁面。當超管

理器分頁移入主機絕對頁面K、P及M時，將其註冊為屬於客體A；當主機絕對頁面L及N由超管理器分頁移入時，將其註冊至客體B。在分頁期間不對共用頁面(在單一安全客體與超管理器之間共用的頁面)加密或解密。共用頁面未標記為安全(允許由超管理器存取)，但在區域安全性表中向單一安全客體網域註冊。

【0069】 根據本發明之一或多個實施例，當非安全客體或超管理器試圖存取由安全客體擁有之頁面時，超管理器接收安全儲存器存取(PIC3D)例外。不需要額外轉譯步驟來判定此情形。

【0070】 根據一或多個實施例，當安全實體試圖存取頁面時，硬體執行額外轉譯檢查，其驗證儲存器實際上確實屬於彼特定安全客體。若並非如此，則向超管理器呈現非安全存取(PIC3E)例外。此外，若正被轉譯之主機虛擬位址不匹配來自區域安全性表中之所註冊主機位址對的主機虛擬位址，則辨識到安全儲存違反(「3F」x)例外。為了使得能夠與超管理器共用，只要轉譯檢查允許存取，安全客體便可存取未標記為安全的儲存器。

【0071】 現轉向圖5，總體上展示根據本發明之一或多個實施例的DAT操作之系統示意圖500。系統示意圖500包括主機主要虛擬位址空間510及主機本籍虛擬位址空間520，頁面係自該等空間轉譯(例如，參見主機DAT轉譯525；應注意，虛線表示經由DAT轉譯525進行之映射)至超管理器(主機)絕對位址空間530。舉例而言，圖5說明主機絕對儲存器由兩個不同的主機虛擬位址空間共用以及彼等主機虛擬位址中之一者不僅在兩個客體之間共用而且另外與主機本身共用。就此而言，主機主要虛擬位址空間510及主機本籍虛擬位址空間520為兩個主機虛擬位址空間之實例，其

中之每一者分別由分開的ASCE (主機主要ASCE (HPASCE) 591及主機本籍ASCE (HHASCE) 592)定址。應注意，所有安全介面控制件儲存器(虛擬及真實兩者)皆由超管理器供給且標記為安全。一旦經供給，只要相關聯之安全實體存在，安全介面控制件儲存器便僅可由安全介面控制件存取。

【0072】 如所說明，主機主要虛擬位址空間510包括客體A絕對頁面A1.HV、客體A絕對頁面A2.HV、客體B絕對頁面B1.HV及主機虛擬頁面H3.HV。主機本籍虛擬位址空間520包括安全介面控制件虛擬頁面U1.HV、主機虛擬頁面H1.HV及主機虛擬頁面H2.HV。

【0073】 根據本發明之一或多個實施例，在本文中所描述之區域安全性表中，所有安全客體(例如，安全客體A及安全客體B)儲存器經註冊為屬於安全客體組態，且相關聯之主機虛擬位址(例如，A1.HV、A2.HV、B1.HV)亦註冊為主機位址對之部分。在一或多個實施例中，所有安全客體儲存器皆映射於主機主要虛擬空間中。此外，亦在區域安全性表中，所有安全介面控制件儲存器經註冊為屬於安全介面控制件，且可基於相關聯之安全客體網域在區域安全性表中進一步區分。根據本發明之一或多個實施例，將UV虛擬儲存器映射於主機本籍虛擬空間中，且將相關聯之主機虛擬位址註冊為主機位址對之部分。根據一或多個實施例，UV真實儲存器不具有相關聯之主機虛擬映射，且區域安全性表中之DA位元(其指示停用虛擬位址比較)經設定以指示此情形。將主機儲存器標記為非安全且在區域安全性表中亦註冊為非安全。

【0074】 因此，在「客體絕對=主機虛擬」之狀況下，超管理器(主機)主要DAT表(由HPASCE 591定義)如下轉譯主機主要虛擬位址空間510

之頁面：將客體A絕對頁面A1.HV映射至屬於安全客體A之主機絕對A1.HA；將客體A絕對頁面A2.HV映射至屬於安全客體A之主機絕對A2.HA；將客體B絕對頁面B1.HV映射至屬於安全客體B之主機絕對B1.HA；且將主機虛擬頁面H3.HV映射至主機絕對頁面H3.HA非安全主機(且由於其非安全，因此不存在主機位址對)。另外，超管理器(主機)本籍DAT表(由HHASCE 592定義)如下轉譯主機本籍虛擬位址空間520之頁面：將安全介面控制件虛擬頁面U1.HV映射至定義為安全UV虛擬之主機絕對頁面U1.HA；將主機虛擬頁面H1.HV映射至定義為非安全之主機絕對頁面H1.HA且將主機虛擬頁面H2.HV映射至定義為非安全之主機絕對頁面H2.HA。不存在與H1.HA或H2.HA相關聯之主機位址對，此係因為其非安全。

【0075】 在操作中，若安全客體試圖存取指派給安全介面控制件之安全頁面，則硬體向超管理器呈現安全儲存違反(「3F」X)例外。若非安全客體或超管理器試圖存取任何安全頁面(包括指派給安全介面控制件之彼等頁面)，則硬體向超管理器呈現安全儲存器存取(「3D」X)例外。替代地，對於嘗試存取安全介面控制件空間，可呈現錯誤條件。若硬體偵測到對安全介面控制件存取之安全指派的失配(例如，儲存器在區域安全性表中註冊為屬於安全客體而非屬於安全介面控制件，或所使用的主機位址與所註冊對存在失配)，則呈現檢查。

【0076】 換言之，主機主要虛擬位址空間510包括主機虛擬頁面A1.HV及A2.HV (屬於安全客體A)及B1.HV (屬於安全客體B)，其分別映射至主機絕對A1.HA、A2.HA及B1.HA。此外，主機主要虛擬位址空間510包括主機(超管理器)頁面H3.HV，其映射至主機絕對H3.HA。主機本

籍虛擬空間520包括兩個主機虛擬頁面H1.HV及H2.HV，其映射至主機絕對頁面H1.HA及H2.HA中。主機主要虛擬位址空間510及主機本籍虛擬位址空間520兩者映射至單一主機絕對530中。將屬於安全客體A及安全客體B之儲存頁面標記為安全且在圖1中所展示之區域安全性表100中向其安全網域註冊且具有相關聯之主機虛擬位址。另一方面，將主機儲存器標記為非安全。當超管理器正定義安全客體時，其必須將主機儲存器供給至安全介面控制件以用於支援此等安全客體所需的安全控制區塊。此儲存器可定義於主機絕對或主機虛擬空間中且在一個實例中，具體而言定義於主機本籍虛擬空間中。返回圖5，主機絕對頁面U1.HA及U2.HA安全UV絕對為安全介面控制件儲存器，其定義為主機絕對儲存器。結果，此等頁面標記為安全且在圖1中所展示之區域安全性表100中註冊為屬於安全介面控制件且向相關聯之安全網域註冊。由於頁面定義為主機絕對位址，因此不存在相關聯之主機虛擬位址，由此在區域安全性表100中設定DA位元。

【0077】 在轉譯之後，超管理器(主機)絕對位址空間530之實例可見於圖6中。圖6描繪根據本發明之一或多個實施例的關於安全介面控制件記憶體之系統示意圖600。系統示意圖600說明超管理器(主機)絕對位址空間630，其包括主機絕對頁面A2.HA安全客體A (用於A2.HV)；主機絕對頁面B1.HA安全客體B (用於B1.HV)；主機絕對頁面H1.HA非安全(主機)；主機絕對頁面H2.HA非安全(主機)；主機絕對頁面U3.HA安全UV真實(無HV映射)；主機絕對頁面U1.HA安全UV虛擬(用於U1.HV)；及主機絕對頁面A1.HA安全客體A (用於A1.HV)。

【0078】 現轉向圖7，總體上展示根據本發明之一或多個實施例的用於匯入操作之程序流程700。當安全客體存取由超管理器分頁移出之頁

面時，會發生一系列事件，諸如程序流程700中所展示之事件，以便安全地將彼頁面調回。程序流程700在區塊705處開始，其中安全客體存取客體虛擬頁面。由於該頁面例如無效，因此硬體向超管理器呈現由程式中斷碼11 (PIC11)指示之主機頁面錯誤(參見區塊715)。超管理器又識別可用於此客體頁面之非安全主機絕對頁面(參見區塊720)，且將經加密客體頁面分頁移入至識別出的主機絕對頁面(參見區塊725)。

【0079】 在區塊730處，接著在適當(基於主機虛擬位址)的主機DAT表中映射主機絕對頁面。在區塊735處，超管理器主機接著重新分派安全客體。在區塊740處，安全客體重新存取客體安全頁面。不再存在頁面錯誤，但由於此為安全客體存取且頁面未在圖1之區域安全性表100中標記為安全，因此在區塊745處，硬體向超管理器呈現非安全儲存例外(PIC3E)。此PIC3E防止客體存取此安全頁面，直至已發出必要匯入。接下來，程序流程700繼續進行至「A」，其連接至圖8。

【0080】 現轉向圖8，總體上展示根據本發明之一或多個實施例的用於執行匯入操作之程序流程800。回應於PIC3E，正常執行之超管理器(例如，以預期方式執行而無錯誤)將發出匯入UVC (參見區塊805)。應注意，此時，待匯入之頁面標記為非安全且僅可由超管理器、其他非安全實體及安全介面控制件存取。其無法由安全客體存取。

【0081】 作為匯入UVC之部分，充當安全介面控制件之受信任韌體檢查以查看此頁面是否已由安全介面控制件鎖定(參見決策區塊810)。若由安全介面控制件鎖定，則程序流程800繼續進行至區塊820。在區塊820處，將「忙碌」傳回碼傳回至超管理器，作為回應，超管理器將延遲(參見區塊825)且重新發出匯入UVC (程序流程800返回至區塊805)。若頁面

尚未被鎖定，則程序流程800繼續進行至決策區塊822。

【0082】 在決策區塊822處，安全介面控制件檢查以查看該頁面是否為與非安全超管理器共用之頁面。若該頁面被共用(程序流程800繼續進行至決策區塊824)，則安全介面控制件在區域安全性表中將主機絕對位址向相關聯之安全客體網域註冊，具有主機虛擬位址且註冊為共用的。此頁面保持標記為非安全。此完成匯入UVC且頁面現可由客體存取。處理以超管理器重新分派客體(區塊830)且安全客體成功地存取頁面(區塊835)繼續。

【0083】 若待匯入之主機虛擬頁面不與超管理器共用(程序流程800繼續進行至區塊840)，則安全介面控制件將標記頁面為安全，使得超管理器不再能夠存取頁面。在區塊845處，安全介面控制件鎖定該頁面，使得其他UVC無法修改頁面狀態。一旦設定了鎖定(在區塊850處)，安全介面控制件便將驗證在客體頁面經加密時其內容未改變。若內容確有改變，則將錯誤傳回碼傳回至超管理器，否則，安全介面控制件將對安全頁面解密。

【0084】 在區塊855處，安全介面控制件解鎖頁面，從而允許其他UVC進行存取，在區域安全性表中將頁面註冊為安全且與適當的客體網域及主機虛擬位址相關聯，以完成主機位址HV->HA對。此允許客體進行存取且完成UVC。

【0085】 現轉向圖9，總體上展示根據本發明之一或多個實施例的關於所供給記憶體操作之程序流程900。程序流程900在區塊905處開始，其中超管理器將查詢UVC發出至安全介面控制件。在區塊910處，安全介面控制件傳回資料(例如，查詢UVC)。此資料可包括所需之基本區域特定

主機絕對儲存器的量；所需之基本安全客體網域特定主機絕對儲存器的量；每MB所需之可變安全客體網域特定主機虛擬儲存器的量；及/或所需之基本安全客體CPU特定主機絕對儲存器的量。

【0086】 在區塊915處，超管理器保留基本主機絕對區域特定儲存器(例如，基於由查詢UVC傳回之大小)。在區塊920處，超管理器將初始化發出至安全介面控制件。就此而言，超管理器可發出初始化UVC，其為在整個區域之安全客體組態之間進行協調所需的UV控制區塊提供所供給儲存器。初始化UVC指定基本區域特定儲存器起點。

【0087】 在區塊925處，安全介面控制件藉由將所供給儲存器註冊至UV及標記為安全來實施初始化(例如，初始化UVC)。對於初始化UVC，安全介面控制件可將所供給儲存器標記為安全；為區域安全性表指派所供給儲存器中之一些；且在區域安全性表中向唯一安全網域註冊但不向相關聯之安全客體網域註冊所供給儲存器以供UV使用且將其註冊為不具有相關聯之主機虛擬位址對。

【0088】 在區塊930處，超管理器保留儲存器(例如，基本及可變安全客體網域特定儲存器)。舉例而言，超管理器保留基本及可變(例如，基於安全客體網域儲存器之大小)安全客體網域特定儲存器(例如，由查詢UVC傳回之大小)。在區塊935處，超管理器將建立組態發出至安全介面控制件。就此而言，超管理器可發出建立安全客體組態UVC，其指定基本及可變安全客體網域特定儲存器起點。另外，建立安全客體組態UVC為支援此安全客體組態所需之UV控制區塊提供所供給儲存器。

【0089】 在區塊940處，安全介面控制件實施建立組態(例如，建立安全客體組態UVC)。對於建立安全客體組態UVC，安全介面控制件可將

所供給儲存器標記為安全；將所供給儲存器註冊於區域安全性表中以供UV使用；且向相關聯之安全客體網域註冊所供給儲存器。將所供給基本(主機絕對)儲存器註冊為不具有相關聯之主機虛擬位址對。將所供給可變(主機虛擬)儲存器註冊為具有相關聯之主機虛擬位址對。

【0090】 在區塊945處，超管理器保留基本安全客體CPU特定儲存器(例如，由查詢UVC傳回之大小)。在區塊950處，超管理器指定儲存器起點。舉例而言，超管理器將指定基本安全客體CPU特定儲存器起點之建立安全客體CPU發出至UV。在區塊955處，安全介面控制件實施建立CPU(例如，建立安全客體CPU UVC)。對於建立安全客體CPU UVC，安全介面控制件可將所供給儲存器標記為安全，且在區域安全性表中註冊所供給儲存器以供UV使用，但不向相關聯之安全客體網域註冊且註冊為不具有相關聯之主機虛擬位址對。

【0091】 現轉向圖10，總體上展示根據本發明之一或多個實施例的關於非安全超管理器頁面至安全介面控制件之安全頁面的轉變之程序流程1000。在程序流程1000中，展示三個超管理器頁面(例如，非安全超管理器頁面A、非安全超管理器頁面B及非安全超管理器頁面C)。

【0092】 超管理器(非安全)頁面A、B及C可由非安全實體(包括超管理器)存取。另外，將超管理器(非安全)頁面A、B及C標記為非安全(NS)以及在區域安全性表(例如，圖1中所展示之區域安全性表100)中註冊為非安全且不共用。在箭頭1005處，發出初始化UVC，其將客體頁面A轉變至與整個區域相關聯之安全介面控制件真實儲存器頁面1010 (UV2)。可將安全介面控制件真實儲存器1010標記為安全以及在區域安全性表(例如，圖1中所展示之區域安全性表100)中註冊為不具有安全客體網域且不具有

超管理器至主機絕對(HV->HA)映射的UV。實情為，向唯一UV2安全網域註冊其且將DA位元設定為1。應注意，安全介面控制件真實儲存器1010可由安全介面控制件作為真實來存取。

【0093】 自超管理器(非安全)頁面B，在箭頭1025處，發出建立SG組態或建立SG CPU UVC，其將此頁面轉變至與安全客體網域相關聯之安全介面控制件真實儲存器1030 (UVS)。可將安全介面控制件真實儲存器1030標記為安全以及在區域安全性表(例如，圖1中所展示之區域安全性表100)中註冊為具有相關聯之安全客體網域且不具有超管理器至主機絕對(HV->HA)映射(亦即，DA位元=1)的UV。應注意，安全介面控制件真實儲存器1010可由安全介面控制件代表安全客體網域作為真實來存取。

【0094】 自超管理器(非安全)頁面C，在箭頭1045處，發出建立SG組態UVC，其將此頁面轉變至與安全客體網域相關聯之安全介面控制件虛擬儲存器1050 (UVV)。可將安全介面控制件虛擬儲存器1050標記為安全以及在區域安全性表(例如，圖1中所展示之區域安全性表100)中註冊為具有安全客體網域且具有超管理器至主機絕對(HV->HA)映射的UV。應注意，安全介面控制件虛擬儲存器1050可代表安全客體網域作為UV虛擬來存取。

【0095】 現轉向圖11，描繪根據一或多個實施例之關於由程式或安全介面控制件進行之安全儲存器存取的程序流程1100。此表示以下情形：安全介面控制件將存取客體儲存器或安全介面控制件儲存器，且必須正確地標示彼存取以便允許硬體驗證彼存取之安全性。1100描述安全介面控制件進行之儲存器存取的此標示。程序流程1100在區塊1110處開始，其中安全介面控制件判定是否正存取安全介面控制件儲存器。

【0096】若此並非對安全介面控制件儲存器之存取，則程序流程1100繼續進行至決策區塊1112 (如由否箭頭所展示)。在決策區塊1112處，安全介面控制件判定其是否正存取安全客體儲存器。若此並非對安全客體儲存器之存取，則程序流程1100繼續進行至「B」(其連接至圖12之程序流程1200)，其將使用預設設定用於非安全存取。若此為對安全客體儲存器之存取，則程序流程1100繼續進行決策區塊1113，其中安全介面控制件判定是否正使用預設安全客體網域。若是，則程序流程1100繼續進行至「B」(其連接至圖12之程序流程1200)，其將使用預設設定用於安全客體存取。若否，則程序流程1100繼續進行至區塊1114。在區塊1114處，將適當安全客體網域載入至SG安全網域暫存器中(且繼續進行至「B」，其連接至圖12之程序流程1200)。

【0097】若此為對安全介面控制件儲存器之存取，則程序流程1100繼續進行至區塊1120 (如由是箭頭所展示)。在區塊1120處，將存取標示為安全UV (例如，使用UV安全網域暫存器)。

【0098】程序流程1100接著繼續進行至決策區塊1130，其中安全介面控制件判定此是否為對UVV空間(例如，SG組態變數表)之存取。若其為對UVV空間之存取，則程序流程1100繼續進行至區塊1134 (如由是箭頭所展示)。在區塊1134處，將存取標示為虛擬。在區塊1136處，將適用的安全客體網域載入至UV安全網域暫存器中。在區塊1138處，準備開始DAT轉譯及存取儲存器。返回至決策區塊1130，若此並非對UVV空間之存取，則程序流程1100繼續進行至區塊1140 (如由否箭頭所展示)。在區塊1140處，將存取標示為真實。

【0099】在決策區塊1150處，安全介面控制件判定此是否為對UVS

空間(例如，SG組態或CPU表)之存取。若此為對UVS空間之存取，則程序流程1100繼續進行至區塊1136 (如由是箭頭所展示)。若此並非對UVS空間之存取，則程序流程1100繼續進行至區塊1170 (如由否箭頭所展示)。此存取將接著為對UV2空間(例如，區域安全性表)之存取。在區塊1170處，將唯一UV2安全網域載入至UV安全網域暫存器中。

【0100】 圖12描繪根據本發明之一或多個實施例的程序流程1200。當客體經分派時，SIE進入韌體可向硬體指示客體正執行(例如，客體模式在作用中)且可指示客體是否安全。若客體安全，則可將相關聯之安全客體網域載入至硬體中(例如，載入SG安全網域暫存器中)。當程式正存取儲存器時，硬體可在存取時基於程式之當前狀態來標示存取。圖12說明處理流程1200中之此程序的實例。在區塊1205處，硬體可判定機器當前是否正在客體模式中執行，且若否，則可在區塊1210處將存取標示為主機存取且在區塊1215處將存取標示為非安全存取。若在區塊1205處，機器正在客體模式中執行，則可在區塊1220處將存取標示為客體存取，且進一步在區塊1225處判定當前客體是否為安全客體。若客體非安全，則可在區塊1215處將存取標示為非安全。若客體安全，則硬體可在區塊1230處將客體標示為安全，其可使安全客體與在分派安全客體時載入之SG安全網域暫存器相關聯。對於非安全客體及安全客體兩者，可在區塊1235處檢查DAT狀態。若DAT關閉，則可在區塊1240處將存取標示為真實。若DAT開啟，則可在區塊1245處將存取標示為虛擬。一旦存取由於DAT關閉在區塊1240處標示為真實或由於DAT開啟在區塊1245處標示為虛擬，硬體便在區塊1250處準備好開始轉譯且存取儲存器，如圖13中進一步所描述。

【0101】 圖13描繪根據本發明之一或多個實施例的程序流程1300中之藉由硬體進行以支援安全存取及非安全存取兩者的轉譯之實例。在區塊1305處，硬體可判定存取是否標示為客體轉譯，且若如此且存取在區塊1310處為虛擬的，則可在區塊1315處執行客體DAT。在客體DAT轉譯期間，可對客體DAT表進行巢套之中間提取。可將表提取標示為客體真實且在原始轉譯標示為安全的情況下標示為安全。表提取亦可遵循程序流程1300之轉譯程序。在於區塊1315處針對標示為客體虛擬之存取執行客體DAT之後且對於在區塊1310處標示為客體真實(虛擬=否)之任何存取，可在區塊1320處應用客體前置詞及客體記憶體位移。在客體轉譯程序完成時，在區塊1325處所得位址可標示為主機虛擬且在原始客體轉譯標示為安全的情況下標示為安全。對於標示為主機虛擬之任何存取，程序1300可繼續。若原始存取在區塊1305處為主機存取(客體=否)且在區塊1330處為虛擬存取，則可執行主機DAT (區塊1335)。在區塊1335處，可將主機表提取標記為非安全。在於區塊1335處執行主機DAT之後或若原始主機存取在區塊1330處標示為真實(虛擬=否)，則可在區塊1340處應用主機前置詞。在區塊1345處，所得位址可為主機絕對位址。

【0102】 圖14描繪根據本發明之一或多個實施例的可由硬體在程序流程1400中執行之具有安全儲存保護的DAT轉譯之實例。自圖13之區塊1345繼續，若在區塊1405處識別安全UV存取，則硬體可在區塊1410處驗證儲存器是否註冊為安全UV儲存器，且若否，則在區塊1415處呈現錯誤。當存取UV儲存器時，可由安全介面控制件進行安全UV存取。若儲存器在區塊1410處註冊為安全UV儲存器，則保護檢查可如可針對任何安全存取執行而繼續，除了UV安全網域暫存器(由安全介面控制件在進行安全

UV存取之前設置)可用作處理繼續之區塊1420處的域檢查之指定安全網域以外。此外，在區塊1425處針對UV存取偵測到的任何違反(項目點D)可在區塊1430處呈現為錯誤，而非在區塊1435處向超管理器呈現例外，如針對區塊1425處之安全客體違反(安全UV=否)所進行。

【0103】 對於在區塊1405處未標示為安全UV存取之存取，硬體在區塊1440處判定存取是否為安全客體存取，且若否且若頁面在區塊1445處標記為安全，則可在區塊1435處向超管理器呈現例外。否則，若在區塊1440處存取並非安全客體存取且在區塊1445處頁面未標記為安全，則在區塊1450處，轉譯成功。

【0104】 若在區塊1440處存取為安全客體存取或在區塊1410處對儲存器之安全UV存取註冊為安全UV儲存器，則硬體可在區塊1420處檢查以確保儲存器註冊至與存取相關聯之安全實體。若此為安全UV存取，則可自UV安全網域暫存器(由安全介面控制件基於正被存取之安全UV儲存器而載入)獲得指定安全網域，且對於安全客體存取，自SG安全網域暫存器(在分派安全實體時載入)獲得指定安全網域。若在區塊1420處正被存取之儲存器未註冊至指定安全網域，則如圖15中所描繪，相對於區域安全性表介面1485執行子程序1500。

【0105】 在子程序1500中，在區塊1510處，執行檢查以判定是否允許跨安全網域之虛擬位址共用。可基於與區域或分割區相關聯之暫存器值執行檢查。在區塊1520處，若允許跨安全網域之共用且允許由當前安全網域共用，則可在區塊1530處執行是否停用虛擬位址檢查之檢查。可經由區域安全性表中對安全網域之暫存器存取或表查找來執行是否允許由當前安全網域共用之檢查，該暫存器存取或表查找可特定於此主機絕對頁

面。可藉由查驗停用虛擬位址比較狀態(DA)來執行是否停用虛擬位址檢查之檢查，其中經標記頁面(例如，DA=1)導致停用虛擬位址檢查。若在區塊1510處不允許跨安全網域之虛擬位址共用，在區塊1520處不允許由當前安全網域共用或在區塊1530處不停用虛擬位址檢查(例如，DA=0)，則可在區塊1435處向超管理器呈現例外。替代地，若在區塊1520處不停用虛擬位址檢查(DA=0)，則對於此主機絕對頁面及安全客體網域，安全介面控制件可檢查所註冊之主機虛擬位址，且若存取主機位址對匹配所註冊之主機位址對，則在區塊1450處，轉譯將成功地完成，且若該等對不匹配，則將向超管理器呈現例外(1435)。否則，若在區塊1530處停用虛擬位址檢查，則子程序1500可在區塊1450處以成功轉譯結束。

【0106】返回至圖14之程序1400，對於在區塊1440及區塊1410處的對在區塊1420處註冊至指定安全網域之儲存器的安全存取，若在區塊1455處停用虛擬位址檢查，亦即，DA位元=1且在區塊1460處，存取真實，則在區塊1450處，轉譯完成。然而，若在區塊1455處DA位元=1但在區塊1460處存取虛擬(真實=否)，則若在區塊1465處允許虛擬化位址(VA)共用，則在區塊1450處轉譯亦完成。然而，若在區塊1455處DA位元=1，存取在區塊1460處為虛擬的(真實=否)且在區塊1465處不允許VA共用，則可發生兩個選項中之一者。選項1以在區塊1470處主機虛擬至主機絕對匹配繼續。選項2為對於區塊1425處之安全UV存取，在區塊1430處發生錯誤，且對於區塊1425處之安全客體存取(安全UV=否)，在區塊1435處向超管理器呈現例外。若在區塊1455處DA位元=0且在區塊1475處存取為虛擬存取，則硬體可在區塊1470處判定存取之主機虛擬至主機絕對映射是否匹配針對此主機絕對位址而註冊的映射。若匹配，則在區塊1450處，轉

譯成功地完成。若在區塊1470處映射並不匹配，則對於區塊1425處之安全UV存取，在區塊1430處發生錯誤，且對於區塊1425處之安全客體存取(安全UV=否)，在區塊1435處向超管理器呈現例外。若DA位元=0且在區塊1475處存取為真實存取(虛擬=否)，則對於區塊1425處之安全UV存取，在區塊1430處發生錯誤，且對於區塊1425處之安全客體存取(安全UV=否)，在區塊1435處向超管理器呈現例外(選項2)；替代地，在區塊1450處，轉譯可成功地完成(選項1)。在區塊1480處之藉由I/O子系統進行的任何存取可檢查以在區塊1445處查看頁面是否標記為安全，且若頁面安全，則可在區塊1435處向超管理器呈現例外；若頁面未標記為安全，則在區塊1450處，轉譯成功。

【0107】 可經由區域安全性表介面1485共同地管理儲存器註冊及映射之各種檢查。舉例而言，區塊1410、1420、1455、1470及1475可與相關聯於同一區域之區域安全性表介接，以管理各種存取。類似地，圖15之區塊1510、1520及1530可與區域安全性表介接以管理各種存取，該區域安全性表與同一區域相關聯。

【0108】 作為其他實例，圖16及圖17說明映射程序選項。如先前所描述，來自安全網域或安全介面控制之每一記憶體存取可用安全網域、主機位址對及DA標記來標示。主機位址對可包括虛擬位址及相關聯之絕對位址。每一實體(例如，安全容器或VM)可具有其自身的安全網域ID。在以下實例中，定義數個術語。V=記憶體存取之虛擬位址。A=記憶體存取之絕對位址。D=安全網域ID。DA=停用虛擬位址比較位元。對於正常操作之安全網域，可在分頁移入時註冊所有記憶體存取且在存取時驗證該等記憶體存取。作為實例，安全網域X可在記憶體中擁有三個頁面，其具有

以下所註冊之主機位址對及相關聯資訊：一個頁面為(V1x,A1x)，DA=0 (不共用)，D=X；另一頁面為(V2x,A2x)，DA=0 (不共用)，D=X；第三頁面為(V3x,A3x)，DA=0 (不共用)，D=X。除非例如經由圖1之區域安全性表100在主機位址對及安全客體網域上發生匹配，否則不允許存取此等頁面。另一安全網域Y亦可在執行且在記憶體中擁有使用兩個主機位址對及相關聯資訊註冊之兩個頁面：一個頁面為(V1y,A1y)，DA=0 (不共用)，D=Y；且另一頁面為(V2y,A2y)，DA=0 (不共用)，D=Y。除非用於存取之主機位址對及安全客體網域匹配為此頁面註冊之彼等主機位址對及安全客體網域，否則可能不允許存取此等頁面。只要對應絕對位址為唯一的，安全網域X及Y便均可使用同一虛擬位址值映射頁面。舉例而言，由於對於所有此等頁面，DA=0，因此V1x可等於V2y，但A1x不得等於A2x、A3x、A1y或A2y中之任一者。為允許共用使用虛擬位址註冊之絕對頁面或允許絕對(相較於虛擬)存取，設定圖1之DA位元140。

【0109】 以下實例說明兩個安全網域之間的頁面共用。對於相同的兩個安全網域X及Y，可共用A1x及A1y，因此A1x=A1y=A1。對於安全實體X及Y，所註冊之主機位址對及相關聯資訊可為(V1x,A1)，DA=1 (共用頁面)，D=X；(V2x,A2x)，DA=0 (不共用)，D=X；(V3x,A3x)，DA=0 (不共用)，D=X；(V1y,A1)，DA=1 (共用頁面)，D=Y；且(V2y,A2y)，DA=0 (不共用)，D=Y。對於域X及Y，可僅允許對共用絕對頁面A1之存取，且在一個實例中，由於DA=1，因此跳過對虛擬位址之匹配檢查。在另一狀況下，每一域X及Y可針對每一共用頁面註冊一單獨(唯一或匹配)之虛擬位址。頁面請求在安全網域間之共用可由一或多個安全網域開始且由其餘域驗證。

【0110】 作為另一實例，若頁面使用指示不進行虛擬位址檢查之DA=1來註冊，則安全介面控制件可使用絕對位址存取安全UV頁面。在此狀況下，頁面使用主機位址對(--,A1as)來註冊，其中主機虛擬位址無關緊要，DA=1且D=AS (輔助安全(aux-secure)，其指示頁面屬於安全介面控制件)。安全介面控制件可比較安全網域以保證僅安全介面控制件允許存取此頁面。由於DA=1，因此不進行虛擬位址檢查。

【0111】 圖16描繪兩個安全網域之間的頁面共用之實施的實例作為DA=1 (共用)之一個實例。在該實例中，自虛擬位址空間1602至絕對位址空間1604之主機位址對為：(V1,A2)、(V2,A1)、(V3,A2)、(V4,A3)、(V5,A2)。絕對位址A2可在三個不同虛擬位址間共用1606：來自同一安全客體網域1608之V1及V5以及來自另一安全網域1610之V3。自虛擬位址空間1602至絕對位址空間1604之轉譯可由非受信任超管理器或OS擁有。此共用在某些情形下可為有益的；然而，若域1608、1610兩者均能夠存取與共用1606相同的絕對位址A2，則在域1608、1610之間共用同一絕對位址A2可引發安全問題。

【0112】 根據本發明之一或多個實施例，作為DA=1 (共用)之另一實例，圖17說明對圖16之實例的修改，其中主機位址對為：(V1,A2)、(V2,A1)、(V4,A3)、(V5,A2)。值得注意地，位址轉譯對(V3,A2)在自虛擬位址空間1602至絕對位址空間1704之映射中並不直接可用。對於安全容器/VM，可能不允許頁面共用。(V3,A2)改變為(V3,A2')，其可包括複製實體A2頁面以針對每一容器/VM具有一個唯一複本。因此，藉由域1608、1610進行之存取可皆觀察到A2之分開複本，但將對不同絕對頁面A2、A2'執行改變A2之內容的任何嘗試。圖1之DA位元140可用以允許使

用兩個不同虛擬位址(例如，域1608之V1及域1610之V3)在兩個不同安全網域1608、1610之間共用一個絕對頁面。

【0113】 現轉向圖18，總體上展示根據本發明之一或多個實施例的用於跨多個安全網域共用安全記憶體的程序流程1800。在區塊1805處，電腦系統之安全介面控制件可接收對記憶體之安全頁面的安全存取請求。在區塊1810處，安全介面控制件可檢查與安全頁面相關聯之停用虛擬位址(例如，DA位元140)比較狀態。在區塊1815處，安全介面控制件可基於停用虛擬位址比較狀態經設定(例如，DA=1)而在存取安全頁面時停用虛擬位址檢查，以支援將複數個虛擬位址映射至安全頁面之同一絕對位址。可基於進行安全存取請求之實體的授權狀態及停用虛擬位址比較狀態經設定(例如，DA=1)而啟用對未指定虛擬位址之安全頁面的絕對位址存取。安全介面控制件可基於網域識別符而驗證複數個安全網域中之一安全網域經授權以存取共用頁面。可比較該安全網域之該識別符與識別為允許共用之該等安全網域之複數個網域識別符，以確認對存取共用頁面之授權。

【0114】 安全介面控制件可檢查安全頁面關於安全網域之註冊狀態。安全介面控制件可基於判定安全頁面未向安全網域註冊而判定安全網域是否允許共用。可基於判定安全網域允許共用而檢查停用虛擬位址比較狀態。安全介面控制件可確認允許跨複數個安全網域共用虛擬位址。舉例而言，安全介面控制件可確認，對於可存取安全頁面之多個安全網域中之任一者，將虛擬位址映射至絕對位址之DAT表的複數個群組藉由經組態以管理DAT表之群組中之一或多者的不安全主機保持不變。用於虛擬位址之每一表映射可包括DAT表之一或多個群組中的多個相關聯表。可基於偵測到DAT表之一或多個群組中的改變而終止安全存取請求。

【0115】 安全頁面之虛擬絕對位址對可與安全網域識別符一起註冊於例如圖1之區域安全性表100中。回應於安全存取請求，可驗證與安全存取請求相關聯之位址且可驗證具有虛擬絕對位址對及安全網域識別符之存取安全網域。停用虛擬位址比較狀態可經由區域安全性表100儲存及更新，該區域安全性表包括與安全頁面相關聯之安全網域識別符、與安全頁面相關聯之虛擬位址映射資料以及停用虛擬位址比較狀態。安全頁面可經指派給由超管理器或作業系統管理之安全虛擬機器或安全容器。

【0116】 應理解，儘管本發明包括關於雲端運算之詳細描述，但本文中所敍述之教示的實施不限於雲端運算環境。更確切而言，本發明之實施例能夠結合現在已知或稍後開發之任何其他類型之運算環境來實施。

【0117】 雲端運算為用於使得能夠對可組態運算資源(例如，網路、網路頻寬、伺服器、處理、記憶體、儲存器、應用程式、VM及服務)之共用集區進行便利之按需網路存取的服務遞送之模型，可組態運算資源可藉由最少的管理工作或與服務提供者之互動而快速地佈建及釋放。此雲端模型可包括至少五個特性、至少三個服務模型及至少四個部署模型。

【0118】 特性如下：

【0119】 隨選自助服務：雲端客戶可視需要自動地單向佈建運算能力(諸如，伺服器時間及網路儲存器)，而無需與服務提供者之人為互動。

【0120】 寬頻網路存取：可經由網路獲得能力及經由標準機制存取能力，該等標準機制藉由異質精簡型或複雜型用戶端平台(例如，行動電話、膝上型電腦及PDA)促進使用。

【0121】 資源集用：提供者之運算資源經集用以使用多租戶模型為多個客戶服務，其中根據需要動態指派及重新指派不同實體及虛擬資源。

位置獨立性之意義在於，客戶通常不具有對所提供資源之確切位置的控制或瞭解，但可能能夠按較高抽象等級(例如，國家、州或資料中心)指定位置。

【0122】 快速彈性：可快速且彈性地佈建能力(在一些狀況下，自動地)以迅速地向外延展，且可快速地釋放能力以迅速地向內延展。在客戶看來，可用於佈建之能力常常看起來為無限的且可在任何時間以任何量來購買。

【0123】 所量測服務：雲端系統藉由在適於服務類型(例如，儲存、處理、頻寬及作用中使用者帳戶)之某一抽象等級下充分利用計量能力而自動控制及最佳化資源使用。可監視、控制及報告資源使用狀況，從而為所利用服務之提供者及客戶兩者提供透明度。

【0124】 服務模型如下：

【0125】 軟體即服務(SaaS)：提供給客戶之能力係使用在雲端基礎架構上執行之提供者之應用程式。可經由諸如網頁瀏覽器(例如，基於網路之電子郵件)之精簡型用戶端介面自各種用戶端裝置存取應用程式。客戶並不管理或控制包括網路、伺服器、作業系統、儲存器或甚至個別應用程式能力之基礎雲端基礎架構，其中可能的例外狀況為有限的使用者特定應用程式組態設置。

【0126】 平台即服務(PaaS)：提供給客戶之能力係將使用由提供者所支援之程式設計語言及工具建立的客戶建立或獲取之應用程式部署至雲端基礎架構上。客戶並不管理或控制包括網路、伺服器、作業系統或儲存器之基礎雲端基礎架構，但控制所部署之應用程式及可能的代管環境組態之應用程式。

【0127】 基礎架構即服務(IaaS)：提供給客戶之能力係佈建處理、儲存、網絡及其他基礎運算資源，其中客戶能夠部署及執行可包括作業系統及應用程式之任意軟體。客戶並不管理或控制基礎雲端基礎架構，但控制作業系統、儲存器、所部署應用程式，及可能有限地控制選擇網路連接組件(例如，主機防火牆)。

【0128】 部署模型如下：

【0129】 私用雲端：僅為組織操作雲端基礎架構。私用雲端可由組織或第三方來管理且可存在內部部署或外部部署。

【0130】 社群雲端：雲端基礎架構由若干組織共用且支援分擔問題(例如，任務、安全要求、策略及順應性考量)的特定社群。社群雲端可由組織或第三方來管理且可存在內部部署或外部部署。

【0131】 公開雲端：該雲端基礎架構可用於公眾或大型工業集團且為出售雲端服務之組織所擁有。

【0132】 混合雲端：該雲端基礎架構為兩個或多於兩個雲端(私用、社群或公開)之組合物，其保持獨特實體但藉由實現資料及應用程式攜帶性(例如，用於在雲端之間實現負載平衡之雲端叢發)之標準化或專屬技術繫結在一起。

【0133】 藉由集中於無國界、低耦合、模組化及語義互操作性對雲端運算環境進行服務定向。雲端運算之關鍵為包括互連節點之網路的基礎架構。

【0134】 現參看圖19，描繪說明性雲端運算環境50。如所展示，雲端運算環境50包括一或多個雲端運算節點10，雲端客戶所使用之諸如個人數位助理(PDA)或蜂巢式電話54A、桌上型電腦54B、膝上型電腦54C

及/或汽車電腦系統54N的本端運算裝置可與該一或多個雲端運算節點通信。節點10可彼此通信。可在一或多個網路(諸如，如上文所描述之私用、社群、公開或混合雲端或其組合)中將該等節點實體地或虛擬地分組(未展示)。此允許雲端運算環境50供應基礎架構、平台及/或軟體作為服務，針對該等服務，雲端客戶不需要在本端運算裝置上維持資源。應理解，圖19中所展示之運算裝置54A至54N之類型意欲僅為說明性的，且運算節點10及雲端運算環境50可經由任何類型之網路及/或網路可定址連接(例如，使用網頁瀏覽器)與任何類型之電腦化裝置通信。

【0135】 現參看圖20，展示藉由雲端運算環境50 (圖19)所提供之功能抽象層之集合。事先應理解，圖20中所展示之組件、層及功能意欲僅為說明性的且本發明之實施例不限於此。如所描繪，提供以下層及對應功能：

【0136】 硬體及軟體層60包括硬體及軟體組件。硬體組件之實例包括：大型電腦61；基於精簡指令集電腦(RISC)架構之伺服器62；伺服器63；刀鋒伺服器64；儲存裝置65；以及網路及網路連接組件66。在一些實施例中，軟體組件包括網路應用程式伺服器軟體67及資料庫軟體68。

【0137】 虛擬化層70提供抽象層，可自該抽象層提供虛擬實體之以下實例：虛擬伺服器71；虛擬儲存器72；虛擬網路73，包括虛擬私用網路；虛擬應用程式及作業系統74；以及虛擬用戶端75。

【0138】 在一個實例中，管理層80可提供下文所描述之功能。資源佈建81提供運算資源及用以執行雲端運算環境內之任務之其他資源的動態採購。當在雲端運算環境內利用資源時，計量及定價82提供成本追蹤，及對此等資源之消耗之帳務處理及發票開立。在一個實例中，此等資源可包

括應用程式軟體授權。安全性提供針對雲端客戶及任務之身分識別驗證，以及對資料及其他資源之保護。使用者入口網站83為客戶及系統管理器提供對雲端運算環境之存取。服務等級管理84提供雲端運算資源分配及管理使得滿足所需服務等級。服務等級協議(SLA)規劃及實現85提供雲端運算資源之預先配置及採購，針對雲端運算資源之未來要求係根據SLA來預期。

【0139】 工作負載層90提供功能性之實例，可針對該功能性利用雲端運算環境。可自此層提供之工作負載及功能的實例包括：地圖測繪及導航91；軟體開發及生命週期管理92；虛擬教室教育遞送93；資料分析處理94；異動處理95；及控制對與虛擬機器相關聯之安全儲存器的存取96。應理解，此等僅為一些實例且在其他實施例中，該等層可包括不同服務。

【0140】 現轉向圖21，描繪根據本發明之一或多個實施例的系統2100。系統2100包括與一或多個用戶端裝置20A至20E直接或間接通信(諸如，經由網路165)之實例節點10 (例如，代管節點)。節點10可為雲端運算提供者之資料中心或主機伺服器。節點10執行超管理器12，其促進部署一或多個VM 15 (15A至15N)。節點10進一步包括硬體/韌體層13，其包括安全介面控制件11。安全介面控制件11包括促進超管理器12將一或多個服務提供至虛擬機器15之一或多個硬體模組及韌體。在現有技術解決方案中，在超管理器12與安全介面控制件11之間、安全介面控制件11與一或多個VM 15之間、超管理器12與一或多個VM 15之間及經由安全介面控制件11在超管理器12與VM 15之間存在通信。為促進安全VM環境，根據本發明之一或多個實施例的代管節點10不包括超管理器12與一或多個

VM 15之間的任何直接通信。

【0141】舉例而言，代管節點10可促進用戶端裝置20A部署VM 15A至15N中之一或多者。可回應於來自相異用戶端裝置20A至20E之各別請求而部署VM 15A至15N。舉例而言，VM 15A可由用戶端裝置20A部署，VM 15B可由用戶端裝置20B部署且VM 15C可由用戶端裝置20C部署。節點10亦可促進用戶端佈建實體伺服器(不作為VM執行)。本文中所描述之實例將節點10中之資源的佈建作為VM之部分來體現，然而，亦可應用所描述之技術解決方案以作為實體伺服器之部分來佈建資源。

【0142】在一實例中，用戶端裝置20A至20E可屬於同一實體，諸如個人、企業、政府機構、公司內的部門或任何其他實體，且節點10可作為實體之私用雲端操作。在此狀況下，節點10僅代管由屬於該實體之用戶端裝置20A至20E部署的VM 15A至15N。在另一實例中，用戶端裝置20A至20E可屬於相異實體。舉例而言，第一實體可擁有用戶端裝置20A，而第二實體可擁有用戶端裝置20B。在此狀況下，節點10可作為代管來自不同實體之VM的公用雲端操作。舉例而言，可按遮蔽方式部署VM 15A至15N，其中VM 15A不便於存取VM 15B。舉例而言，節點10可使用IBM z Systems®處理器資源/系統管理器(PR/SM)邏輯分割區(LPAR)特徵來遮蔽VM 15A至15N。諸如PR/SM LPAR之此等特徵提供分割區之間的隔離，因此促進節點10在不同邏輯分割區中部署同一實體節點10上之不同實體的兩個或多於兩個VM 15A至15N。PR/SM LPAR超管理器實施於具有特定硬體之受信任內部韌體中以提供此隔離。

【0143】來自用戶端裝置20A至20E之用戶端裝置20A為通信設備，諸如電腦、智慧型手機、平板電腦、桌上型電腦、膝上型電腦、伺服器電

腦或請求節點10之超管理器12部署VM的任何其他通信設備。用戶端裝置20A可經由網路165發送供超管理器接收之請求。來自VM 15A至15N之VM 15A為超管理器12回應於來自用戶端裝置20A至20E中之用戶端裝置20A的請求而部署的VM影像。超管理器12為VM監視器(VMM)，其可為建立及執行VM之軟體、韌體或硬體。超管理器12促進VM 15A使用節點10之硬體組件以執行程式及/或儲存資料。藉由適當特徵及修改，超管理器12可為IBM z Systems®、Oracle's VM Server, Citrix's XenServer, Vmware's ESX, Microsoft Hyper-V超管理器或任何其他超管理器。超管理器12可為直接在節點10上執行之原生超管理器或在另一超管理器上執行之代管超管理器。

【0144】 現轉向圖22，展示根據本發明之一或多個實施例的用於實施本文中之教示的節點10。節點10可為電子電腦架構，其包含及/或使用利用各種通信技術之任何數目個運算裝置及網路以及其組合，如本文中所描述。節點10可為易於可調、可擴充及模組化的，能夠改變至不同服務或獨立於其他特徵而重新組態一些特徵。

【0145】 在此實施例中，節點10具有處理器2201，其可包括一或多個中央處理單元(CPU) 2201a、2201b、2201c等。亦被稱作處理電路、微處理器、運算單元之處理器2201經由系統匯流排2202耦接至系統記憶體2203及各種其他組件。系統記憶體2203包括唯讀記憶體(ROM) 2204及隨機存取記憶體(RAM) 2205。ROM 2204耦接至系統匯流排2202，且可包括控制節點10之某些基本功能的基本輸入/輸出系統(BIOS)。RAM為耦接至系統匯流排2202以供處理器2201使用之讀取-寫入記憶體。

【0146】 圖22之節點10包括硬碟2207，其為可由處理器2201執行之

可讀取的有形儲存媒體之實例。硬碟2207儲存軟體2208及資料2209。軟體2208儲存為指令以在節點10上由處理器2201執行(以執行程序，諸如參看圖1至圖21所描述之程序)。資料2209包括組織於各種資料結構中之定性或定量變數的值之集合以支援軟體2208之操作且由該等操作使用。

【0147】 圖22之節點10包括一或多個配接器(例如，硬碟控制器、網路配接器、圖形配接器等)，其互連處理器2201、系統記憶體2203、硬碟2207以及節點10之其他組件(例如，周邊及外部裝置)且支援其間的通信。在本發明之一或多個實施例中，一或多個配接器可連接至一或多個I/O匯流排，其經由中間匯流排橋接器連接至系統匯流排2202，且一或多個I/O匯流排可利用共同協定，諸如周邊組件互連(PCI)。

【0148】 如所展示，節點10包括將鍵盤2221、滑鼠2222、揚聲器2223及麥克風2224互連至系統匯流排2202之介面配接器2220。節點10包括將系統匯流排2202互連至顯示器2231之顯示配接器2230。顯示配接器2230 (及/或處理器2201)可包括圖形控制器以提供圖形效能，諸如GUI 2232之顯示及管理。通信配接器2241將系統匯流排2202與網路2250互連，從而使得節點10能夠與其他系統、裝置、資料及軟體(諸如，伺服器2251及資料庫2252)通信。在本發明之一或多個實施例中，軟體2208及資料2209之操作可藉由伺服器2251及資料庫2252在網路2250上實施。舉例而言，網路2250、伺服器2251及資料庫2252可組合以提供軟體2208及資料2209之內部反覆，作為平台即服務、軟體即服務及/或基礎架構即服務(例如，作為分散式系統中之網路應用程式)。

【0149】 本文中所描述之實施例必定植根於電腦技術，且特定而言為代管VM之電腦伺服器。另外，本發明之一或多個實施例藉由促進代管

VM之電腦伺服器代管安全VM來促進改良運算技術本身，特定而言為代管VM之電腦伺服器的操作，其中甚至禁止超管理器存取記憶體、暫存器及與安全VM相關聯之其他此資料。此外，本發明之一或多個實施例藉由使用安全介面控制件(在本文中亦被稱作「UV」)來提供朝向改良代管運算伺服器之VM的重要步驟，以促進安全VM與超管理器之分離且因此維持由運算伺服器代管之VM的安全性，該安全介面控制件包括硬體、韌體(例如，微碼)或其組合。安全介面控制件提供輕型中間操作以促進安全性，而不會在VM之初始化/退出期間添加確保VM狀態安全的大量額外負荷，如本文中所描述。

【0150】 本文中所揭示之本發明之實施例可包括控制對VM之安全儲存器之存取的系統、方法及/或電腦程式產品(本文中為系統)。應注意，對於每種解釋，用於元件之識別符重新用於不同圖式之其他類似元件。

【0151】 本文中參看相關圖式描述本發明之各種實施例。可在不脫離本發明之範疇的情況下設計本發明之替代實施例。在以下描述及圖式中，闡述元件之間的各種連接及位置關係(例如，上方、下方、鄰近等)。除非另外規定，否則此等連接及/或位置關係可為直接或間接的，且本發明在此方面不意欲為限制性的。相應地，實體之耦接可指直接抑或間接耦接，且實體之間之位置關係可為直接或間接位置關係。此外，本文中所描述之各種任務及程序步驟可併入至具有未詳細地描述於本文中之額外步驟或功能性的更全面程序或處理程序中。

【0152】 以下定義及縮寫將用於解譯申請專利範圍及本說明書。如本文中所使用，術語「包含(comprises/comprising)」、「包括(includes/including)」、「具有(has/having)」、「含有(contains或

containing)」或其任何其他變體意欲涵蓋非排他性包括。舉例而言，包含一系列元件之組合物、混合物、程序、方法、物品或設備未必僅限於彼等元件，而是可包括未明確地列出或此類組合物、混合物、程序、方法、物品或設備所固有的其他元件。

【0153】 另外，術語「例示性」在本文中用於意謂「充當實例、例子或說明」。不必將本文中描述為「例示性」之任何實施例或設計理解為比本發明之其他實施例或設計較佳或有利。術語「至少一個」及「一或多個」可理解為包括大於或等於一個之任何整數數目，亦即，一個、兩個、三個、四個等。術語「複數個」可理解為包括大於或等於兩個之任何整數數目，亦即，兩個、三個、四個、五個等。術語「連接」可包括間接「連接」及直接「連接」兩者。

【0154】 術語「約」、「大體上」、「大約」及其變體意欲包括與基於在申請本申請案時可用的設備之特定量的量測相關聯之誤差度。舉例而言，「約」可包括給定值之±8%或5%或2%的範圍。

【0155】 本發明可為在任何可能之技術細節整合層級處的系統、方法及/或電腦程式產品。該電腦程式產品可包括一(或多個)電腦可讀儲存媒體，其上具有電腦可讀程式指令以使處理器進行本發明之態樣。

【0156】 電腦可讀儲存媒體可為有形裝置，其可持留及儲存指令以供指令執行裝置使用。電腦可讀儲存媒體可為例如但不限於電子儲存裝置、磁性儲存裝置、光學儲存裝置、電磁儲存裝置、半導體儲存裝置或前述各者之任何合適組合。電腦可讀儲存媒體之更特定實例的非窮盡性清單包括以下各者：攜帶型電腦磁片、硬碟、隨機存取記憶體(RAM)、唯讀記憶體(ROM)、可抹除可程式化唯讀記憶體(EPROM或快閃記憶體)、靜態

隨機存取記憶體(SRAM)、攜帶型光碟唯讀記憶體(CD-ROM)、數位多功能光碟(DVD)、記憶棒、軟碟、機械編碼裝置(諸如，上面記錄有指令之凹槽中之打孔卡片或凸起結構)及前述各者之任何合適組合。如本文中所使用，不應將電腦可讀儲存媒體本身解釋為暫時性信號，諸如無線電波或其他自由傳播之電磁波、經由波導或其他傳輸媒體傳播之電磁波(例如，經由光纖纜線傳遞之光脈衝)，或經由導線傳輸之電信號。

【0157】 本文中所描述之電腦可讀程式指令可自電腦可讀儲存媒體下載至各別運算/處理裝置或經由網路(例如，網際網路、區域網路、廣域網路及/或無線網路)下載至外部電腦或外部儲存裝置。網路可包含銅傳輸纜線、光學傳輸光纖、無線傳輸、路由器、防火牆、交換器、閘道器電腦及/或邊緣伺服器。每一運算/處理裝置中之網路配接卡或網路介面自網路接收電腦可讀程式指令且轉遞電腦可讀程式指令以用於儲存於各別運算/處理裝置內之電腦可讀儲存媒體中。

【0158】 用於進行本發明之操作之電腦可讀程式指令可為以一或多種程式設計語言之任何組合編寫之組譯器指令、指令集架構(ISA)指令、機器指令、機器相關指令、微碼、韌體指令、狀態設置資料、用於積體電路系統之組態資料，或原始程式碼或目標程式碼，該一或多種程式設計語言包括諸如Smalltalk、C++或其類似者之物件導向式程式設計語言，及程序性程式設計語言，諸如「C」程式設計語言或類似程式設計語言。電腦可讀程式指令可完全在使用者電腦上執行，作為單獨套裝軟體部分地在使用者之電腦上執行，部分地在使用者之電腦上及部分地在遠端電腦上執行或完全在遠端電腦或伺服器上執行。在後一情形中，遠端電腦可經由任何類型之網路(包括區域網路(LAN)或廣域網路(WAN))連接至使用者之電

腦，或可連接至外部電腦(例如，使用網際網路服務提供者經由網際網路)。在一些實施例中，電子電路系統(包括例如可程式化邏輯電路系統、場可程式化閘陣列(FPGA)或可程式化邏輯陣列(PLA))可藉由利用電腦可讀程式指令之狀態資訊來個人化電子電路系統而執行電腦可讀程式指令，以便執行本發明之態樣。

【0159】 本文參考根據本發明之實施例之方法、設備(系統)及電腦程式產品之流程圖說明及/或方塊圖來描述本發明之態樣。應理解，可藉由電腦可讀程式指令實施流程圖說明及/或方塊圖中之每一區塊，及流程圖說明及/或方塊圖中的區塊之組合。

【0160】 可將此等電腦可讀程式指令提供至通用電腦、專用電腦或其他可程式化資料處理設備之處理器以產生機器，使得經由該電腦或其他可程式化資料處理設備之處理器執行之指令建立用於實施該一或多個流程圖及/或方塊圖區塊中所指定之功能/動作之構件。亦可將此等電腦可讀程式指令儲存於電腦可讀儲存媒體中，該等指令可指導電腦、可程式化資料處理設備及/或其他裝置以特定方式起作用，使得儲存有指令之電腦可讀儲存媒體包含製品，該製品包括實施在該一或多個流程圖及/或方塊圖區塊中指定之功能/動作之態樣的指令。

【0161】 電腦可讀程式指令亦可載入至電腦、其他可程式化資料處理設備或其他裝置上，以使一系列操作步驟在該電腦、其他可程式化設備或其他裝置上執行以產生電腦實施之程序，使得在該電腦、其他可程式化設備或其他裝置上執行之指令實施在該一或多個流程圖及/或方塊圖區塊中所指定之功能/動作。

【0162】 諸圖中之流程圖及方塊圖說明根據本發明之各種實施例的

系統、方法及電腦程式產品之可能實施之架構、功能性及操作。就此而言，流程圖或方塊圖中之每一區塊可表示指令之模組、區段或部分，其包含用於實施指定邏輯功能之一或多個可執行指令。在一些替代實施中，區塊中所提及之功能可不按諸圖中所提及之次序發生。舉例而言，以連續方式展示的兩個區塊實際上可實質上同時執行，或該等區塊有時可以相反次序執行，此取決於所涉及的功能性。亦應注意，可由執行指定功能或動作或進行專用硬體及電腦指令之組合的基於專用硬體之系統實施方塊圖及/或流程圖說明之每一區塊及方塊圖及/或流程圖說明中之區塊的組合。

【0163】 本文中所使用之術語僅出於描述特定實施例之目的，且並不意欲為限制性的。如本文中所使用，除非上下文另外明確地指示，否則單數形式「一(a、an)」及「該」意欲亦包括複數形式。應進一步理解，術語「包含(comprises及/或comprising)」在用於本說明書中時指定所陳述特徵、整體、步驟、操作、元件及/或組件之存在，但不排除一或多個其他特徵、整體、步驟、操作、元件、組件及/或其群組之存在或添加。

【0164】 各種實施例之描述在本文中已出於說明的目的呈現，但不意欲為詳盡的或限於所揭示之實施例。在不脫離所描述實施例之範疇及精神的情況下，一般熟習此項技術者將顯而易見許多修改及變化。本文中所使用之術語經選擇以最佳解釋實施例之原理、實際應用或對市場中發現的技術之技術改良，或使得其他一般熟習此項技術者能夠理解本文中所揭示之實施例。

【符號說明】

【0165】

10: 雲端運算節點

11: 安全介面控制件

12: 超管理器

13: 硬體/韌體層

15: VM

15A: VM

15B: VM

15C: VM

15D: VM

15N: VM

20A: 用戶端裝置

20B: 用戶端裝置

20C: 用戶端裝置

20D: 用戶端裝置

20E: 用戶端裝置

50: 雲端運算環境

54A: 個人數位助理(PDA)或蜂巢式電話/運算裝置

54B: 桌上型電腦/運算裝置

54C: 膝上型電腦/運算裝置

54N: 汽車電腦系統/運算裝置

60: 硬體及軟體層

61: 大型電腦

62: 基於精簡指令集電腦(RISC)架構之伺服器

63: 伺服器

64: 刀鋒伺服器

65: 儲存裝置

66: 網路及網路連接組件

67: 網路應用程式伺服器軟體

68: 資料庫軟體

70: 虛擬化層

71: 虛擬伺服器

72: 虛擬儲存器

73: 虛擬網路

74: 虛擬應用程式及作業系統

75: 虛擬用戶端

80: 管理層

81: 資源佈建

82: 計量及定價

83: 使用者入口網站

84: 服務等級管理

85: 服務等級協議(SLA)規劃及實現

90: 工作負載層

91: 地圖測繪及導航

92: 軟體開發及生命週期管理

93: 虛擬教室教育遞送

94: 資料分析處理

95: 異動處理

96: 控制對與虛擬機器相關聯之安全儲存器的存取

100: 區域安全性表

110: 主機絕對位址

120: 安全網域ID

130: UV位元

140: 停用位址比較(DA)位元

150: 共用(SH)位元

160: 主機虛擬位址

165: 網路

202: 虛擬位址空間

204: 虛擬位址空間

206: 絕對位址空間

208: 位址空間控制元素(ASCE) A

210: ASCE B

212a1: 虛擬頁面A1.V

212a2: 虛擬頁面A2.V

212a3: 虛擬頁面A3.V

214b1: 虛擬頁面B1.V

214b2: 虛擬頁面B2.V

220a1: 絕對頁面A1.A

220a2: 絕對頁面A2.A

220a3: 絕對頁面A3.A

222b1: 絕對頁面B1.A

222b2: 絕對頁面B2.A

230: 區段

232a: 頁表

232b: 頁表

234: 表

236: 表

302: 客體A虛擬位址空間A

304: 客體ASCE (GASCE) A

306: 客體B虛擬位址空間B

308: GASCEB

310a1: 虛擬頁面A1.GV

310a2: 虛擬頁面A2.GV

310a3: 虛擬頁面A3.GV

320b1: 虛擬頁面B1.GV

320b2: 虛擬頁面B2.GV

325: 共用主機(超管理器)虛擬位址空間

330: 主機絕對位址空間

340a1: 客體絕對頁面A1.HV

340a2: 客體絕對頁A2.HV/主機虛擬位址

340a3: 客體絕對頁A3.HV/主機虛擬位址

350: 主機ASCE (HASCE)

360b1: 客體絕對頁面B1.HV/主機虛擬位址

360b2: 客體絕對頁面B2.HV/主機虛擬位址

370a1: 主機絕對頁面A1.HV

370a3: 主機絕對頁面A3.HV

370b1: 主機虛擬位址B1.HV

380: 主機絕對頁面AB2.HA

490a: 主機絕對位址A2.HA

490b: 主機絕對位址B2.HA

500: DAT操作之系統示意圖

510: 主機主要虛擬位址空間

520: 主機本籍虛擬位址空間

525: 主機DAT轉譯

530: 超管理器(主機)絕對位址空間

591: 主機主要ASCE (HPASCE)

592: 主機本籍ASCE (HHASCE)

600: 關於安全介面控制件記憶體之系統示意圖

630: 超管理器(主機)絕對位址空間

700: 用於匯入操作之程序流程

800: 用於執行匯入操作之程序流程

900: 關於所供給記憶體操作之程序流程

1000: 關於非安全超管理器頁面至安全介面控制件之安全頁面的程序流程

1005: 箭頭

1010: 安全介面控制件真實儲存器頁面/安全介面控制件真實儲存器

1025: 箭頭

1030: 安全介面控制件真實儲存器

1045: 箭頭

1050: 安全介面控制件虛擬儲存器

1100: 關於由程式或安全介面控制件進行之安全儲存器存取的程序流程

1200: 程序流程

1300: 程序流程

1400: 程序流程

1485: 區域安全性表介面

1500: 子程序

1602: 虛擬位址空間

1604: 絕對位址空間

1606: 共用

1608: 安全客體網域

1610: 安全網域

1704: 絕對位址空間

1800: 用於跨多個安全網域共用安全記憶體的程序流程

2100: 系統

2201: 處理器

2201a: 中央處理單元(CPU)

2201b: 中央處理單元(CPU)

2201c: 中央處理單元(CPU)

2202: 系統匯流排

2203: 系統記憶體

2204: 唯讀記憶體(ROM)

2205: 隨機存取記憶體(RAM)

2207: 硬碟

2208: 軟體

2209: 資料

2220: 介面配接器

2221: 鍵盤

2222: 滑鼠

2223: 揚聲器

2224: 麥克風

2230: 顯示配接器

2231: 顯示器

2232: GUI

2241: 通信配接器

2250: 網路

2251: 伺服器

2252: 資料庫

【發明申請專利範圍】

【請求項1】

一種電腦實施之方法，其包含：

在一電腦系統之一安全介面控制件處接收對記憶體之一安全頁面的一安全存取請求；

藉由該安全介面控制件檢查與該安全頁面相關聯之一停用虛擬位址比較狀態；及

基於該停用虛擬位址比較狀態經設定，藉由該安全介面控制件在存取該安全頁面時停用一虛擬位址檢查以支援將複數個虛擬位址映射至該安全頁面之同一絕對位址。

【請求項2】

如請求項1之方法，其進一步包含：

藉由該安全介面控制件基於一網域識別符而驗證複數個安全網域中之一安全網域經授權以存取一共用頁面。

【請求項3】

如請求項2之方法，其中比較該安全網域之該網域識別符與識別為允許共用之該等安全網域之複數個網域識別符，以確認對存取該共用頁面之授權。

【請求項4】

如請求項2之方法，其進一步包含：

確認對於可存取該安全頁面之多個安全網域中之任一者，將虛擬位址映射至絕對位址之動態位址轉譯表的複數個群組藉由經組態以管理動態位址轉譯表之該等群組中之一或多者的一不安全主機保持不變，其中用於

一虛擬位址之每一表映射包含動態位址轉譯表之該一或多個群組中的多個相關聯表；及

基於偵測到該等動態位址轉譯表之該一或多個群組中的一改變而終止該安全存取請求。

【請求項5】

如請求項1之方法，其中該停用虛擬位址比較狀態係經由一區域安全性表儲存及更新，該區域安全性表包含與該安全頁面相關聯之一安全網域識別符、與該安全頁面相關聯之虛擬位址映射資料以及該停用虛擬位址比較狀態。

【請求項6】

如請求項1之方法，其中該安全介面控制件包含韌體、硬體、受信任軟體或韌體、硬體及受信任軟體之一組合，且該安全頁面經指派給由一超管理器或作業系統管理之一安全虛擬機器或一安全容器。

【請求項7】

一種電腦系統，其包含：

一記憶體；

一處理單元；及

一安全介面控制件，其經組態以執行包含以下各者之複數個操作：

檢查與來自在該處理單元上執行之一實體的對該記憶體之一安全頁面之一安全存取請求相關聯的一停用虛擬位址比較狀態；及

基於該停用虛擬位址比較狀態經設定，在存取該安全頁面時停用一虛擬位址檢查以支援將複數個虛擬位址映射至該安全頁面之同一絕對位址。

【請求項8】

如請求項7之系統，其中該安全介面控制件經組態以執行包含以下者之操作：

基於一網域識別符而驗證複數個安全網域中之一安全網域經授權以存取一共用頁面。

【請求項9】

如請求項8之系統，其中比較該安全網域之該網域識別符與識別為允許共用之該等安全網域之複數個網域識別符，以確認對存取該共用頁面之授權。

【請求項10】

如請求項8之系統，其中該安全介面控制件經組態以執行包含以下各者之操作：

確認對於可存取該安全頁面之多個安全網域中之任一者，將虛擬位址映射至絕對位址之動態位址轉譯表的複數個群組藉由經組態以管理動態位址轉譯表之該等群組中之一或多者的一不安全主機保持不變，其中用於一虛擬位址之每一表映射包含動態位址轉譯表之該一或多個群組中的多個相關聯表；及

基於偵測到該等動態位址轉譯表之該一或多個群組中的一改變而終止該安全存取請求。

【請求項11】

如請求項7之系統，其中該停用虛擬位址比較狀態係經由一區域安全性表儲存及更新，該區域安全性表包含與該安全頁面相關聯之一安全網域識別符、與該安全頁面相關聯之虛擬位址映射資料以及該停用虛擬位址比

較狀態。

【請求項12】

如請求項7之系統，其中該安全介面控制件包含韌體、硬體、受信任軟體或韌體、硬體及受信任軟體之一組合，且該安全頁面經指派給由一超管理器或作業系統管理之一安全虛擬機器或一安全容器。

【請求項13】

一種電腦程式產品，其包含一電腦可讀儲存媒體，該電腦可讀儲存媒體包含電腦可執行指令，該等電腦可執行指令在由一處理單元之一安全介面控制件執行時使該處理單元執行一方法，該方法包含：

檢查與來自在該處理單元上執行之一實體的對記憶體之一安全頁面之一安全存取請求相關聯的一停用虛擬位址比較狀態；及

基於該停用虛擬位址比較狀態經設定，在存取該安全頁面時停用一虛擬位址檢查以支援將複數個虛擬位址映射至該安全頁面之同一絕對位址。

【請求項14】

如請求項13之電腦程式產品，其中該等可執行指令進一步使該處理單元執行：

藉由該安全介面控制件基於一網域識別符而驗證複數個安全網域中之一安全網域經授權以存取一共用頁面。

【請求項15】

如請求項14之電腦程式產品，其中比較該安全網域之該網域識別符與識別為允許共用之該等安全網域之複數個網域識別符，以確認對存取該共用頁面之授權。

【請求項16】

如請求項14之電腦程式產品，其中該等可執行指令進一步使該處理單元執行：

確認對於可存取該安全頁面之多個安全網域中之任一者，將虛擬位址映射至絕對位址之動態位址轉譯表的複數個群組藉由經組態以管理動態位址轉譯表之該等群組中之一或多者的一不安全主機保持不變，其中用於一虛擬位址之每一表映射包含動態位址轉譯表之該一或多個群組中的多個相關聯表；及

基於偵測到該等動態位址轉譯表之該一或多個群組中的一改變而終止該安全存取請求。

【請求項17】

如請求項13之電腦程式產品，其中該停用虛擬位址比較狀態係經由一區域安全性表儲存及更新，該區域安全性表包含與該安全頁面相關聯之一安全網域識別符、與該安全頁面相關聯之虛擬位址映射資料以及該停用虛擬位址比較狀態。

【請求項18】

如請求項13之電腦程式產品，其中該安全頁面經指派給由一超管理器或作業系統管理之一安全虛擬機器或一安全容器。

【請求項19】

一種電腦實施之方法，其包含：

在一電腦系統之一安全介面控制件處接收對記憶體之一安全頁面的一安全存取請求；

藉由該安全介面控制件檢查與該安全頁面相關聯之一停用虛擬位址

比較狀態；及

基於進行該安全存取請求之一實體的一授權狀態及該停用虛擬位址比較狀態經設定，啟用對未指定虛擬位址之該安全頁面的絕對位址存取。

【請求項20】

如請求項19之方法，其進一步包含：

藉由該安全介面控制件基於一網域識別符而驗證複數個安全網域中之一安全網域經授權以存取一共用頁面。

【請求項21】

如請求項20之方法，其中比較該安全網域之該網域識別符與識別為允許共用之該等安全網域之複數個網域識別符，以確認對存取該共用頁面之授權。

【請求項22】

如請求項19之方法，其中該安全介面控制件包含韌體、硬體或韌體及硬體之一組合，且該安全頁面經指派給由一超管理器或作業系統管理之一安全容器或一安全虛擬機器。

【請求項23】

一種電腦系統，其包含：

一記憶體；

一處理單元；及

一安全介面控制件，其經組態以執行包含以下各者之複數個操作：

檢查與來自在該處理單元上執行之一實體的對該記憶體之一安全頁面之一安全存取請求相關聯的一停用虛擬位址比較狀態；及

基於進行該安全存取請求之一實體的一授權狀態及該停用虛擬位

址比較狀態經設定，啟用對未指定虛擬位址之該安全頁面的絕對位址存取。

【請求項24】

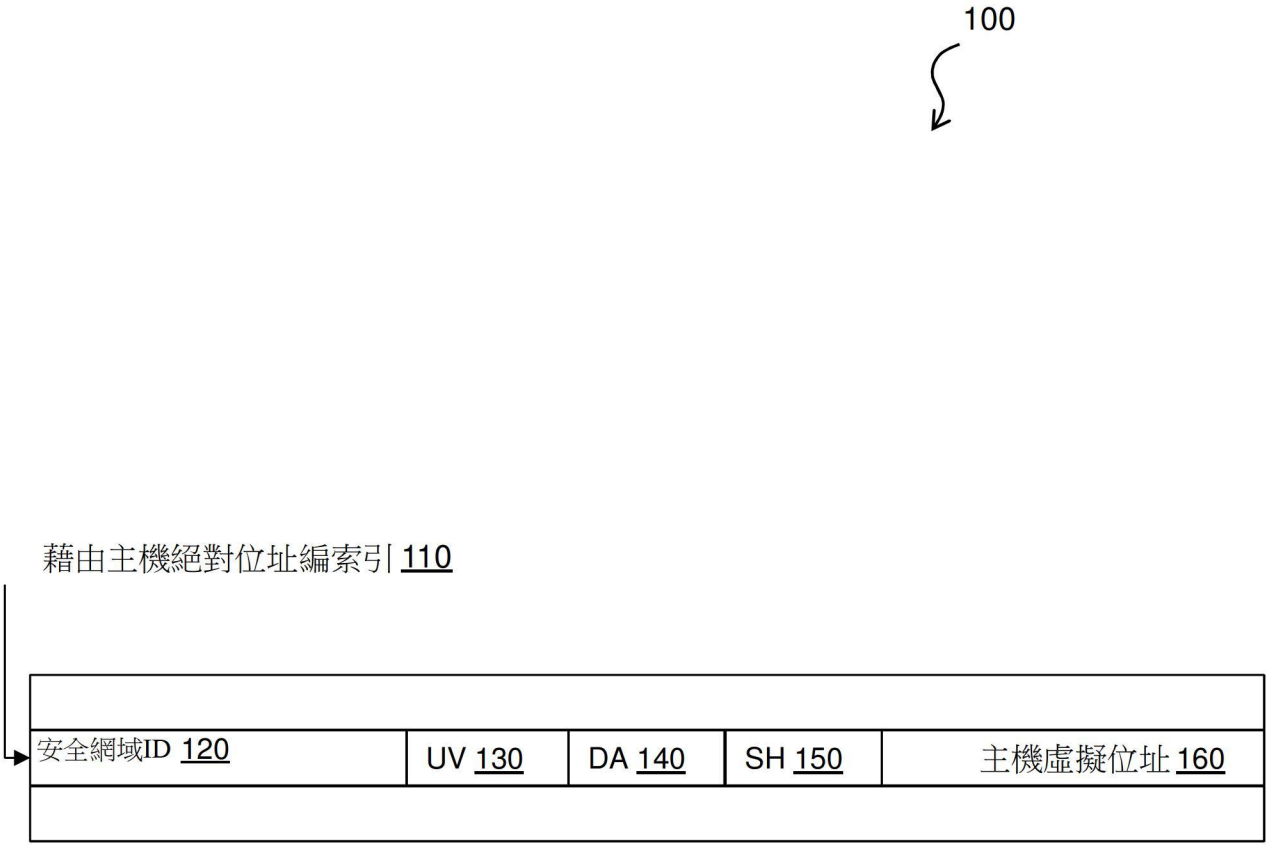
如請求項23之系統，其中該安全介面控制件經組態以執行包含以下者之操作：

基於一網域識別符而驗證複數個安全網域中之一安全網域經授權以存取一共用頁面。

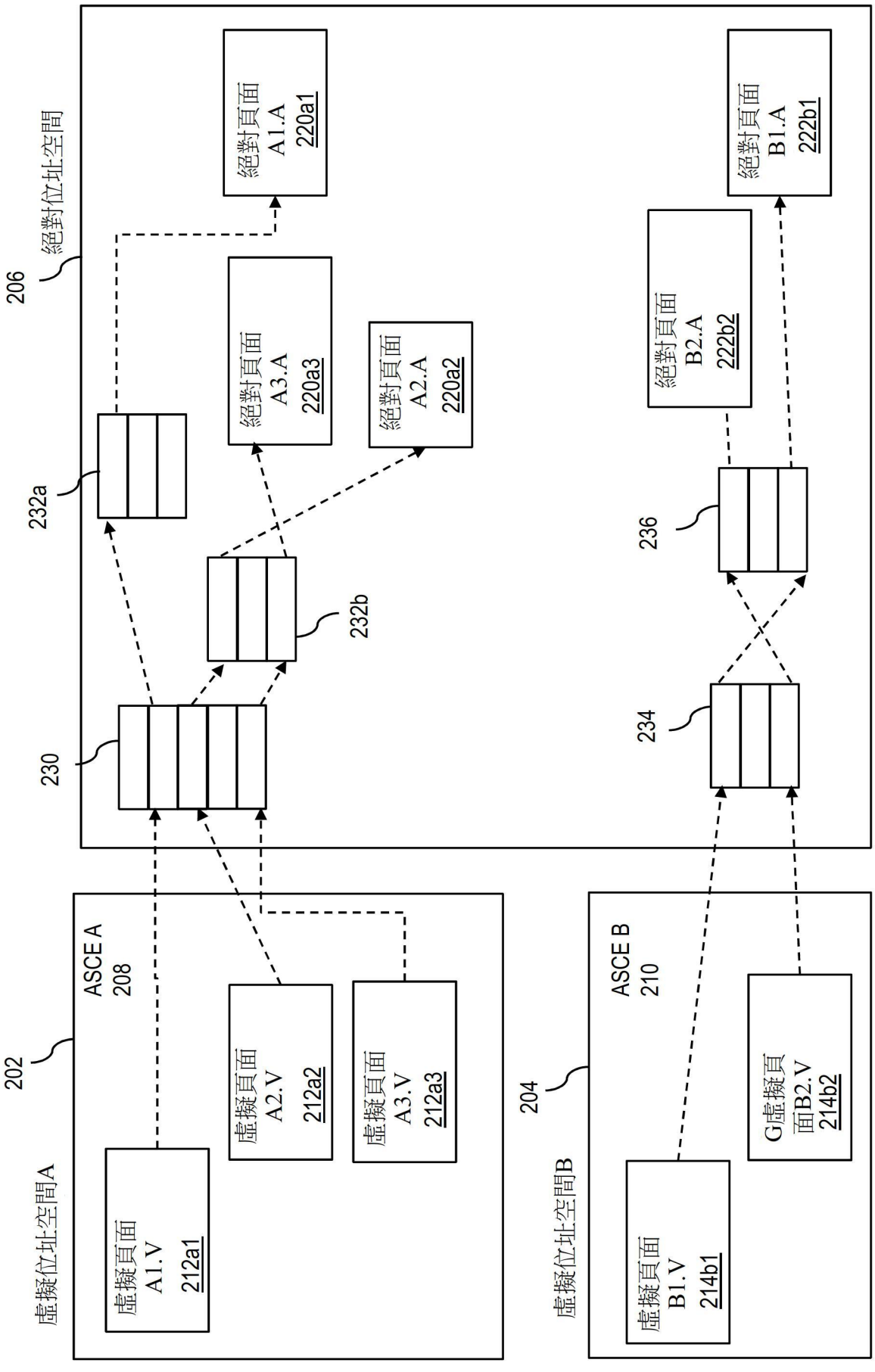
【請求項25】

如請求項24之系統，其中比較該安全網域之該網域識別符與識別為允許共用之該等安全網域之複數個網域識別符，以確認對存取該共用頁面之授權。

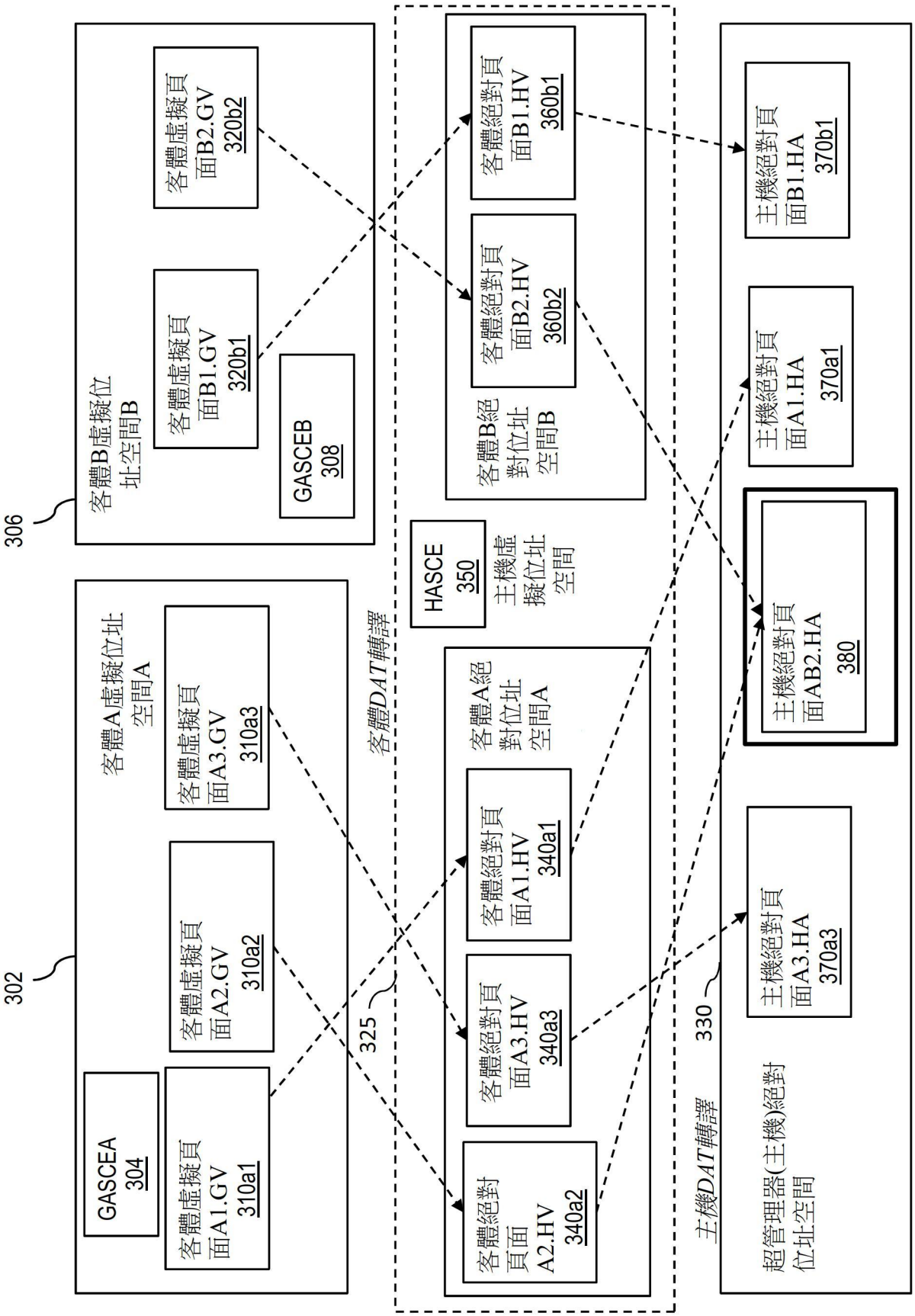
【發明圖式】


100
藉由主機絕對位址編索引 110
安全網域ID 120
UV 130
DA 140
SH 150
主機虛擬位址 160

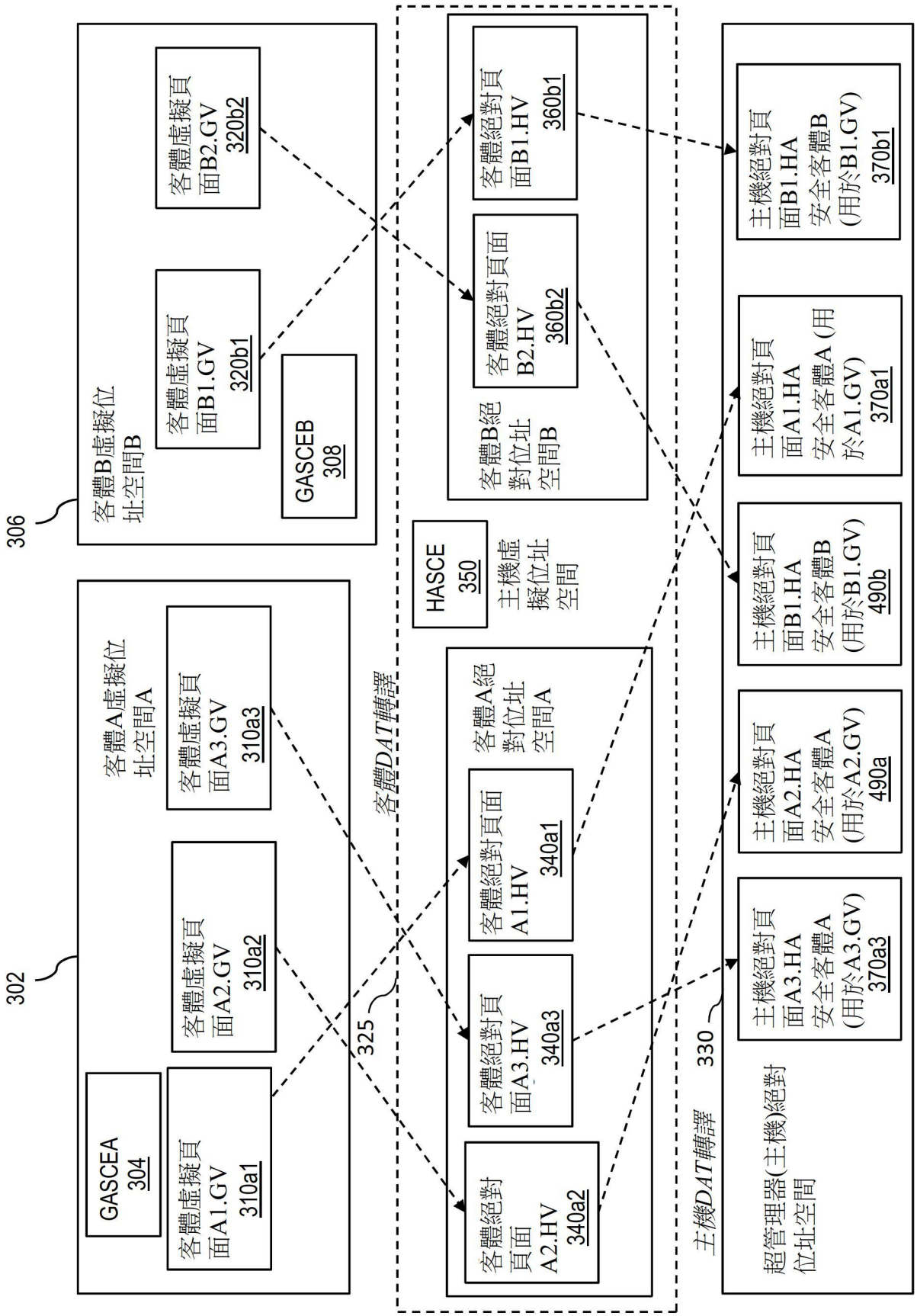
【圖1】


虛擬位址空間A
202
ASCE A
208
虛擬頁面
A1.V
212a1
虛擬頁面
A2.V
212a2
虛擬頁面
A3.V
212a3
虛擬位址空間B
204
ASCE B
210
虛擬頁面
B1.V
214b1
G虛擬頁
面B2.V
214b2
絕對位址空間
206
絕對頁面
A1.A
220a1
絕對頁面
A3.A
220a3
絕對頁面
A2.A
220a2
絕對頁面
B2.A
222b2
絕對頁面
B1.A
222b1
230
232a
232b
234
236

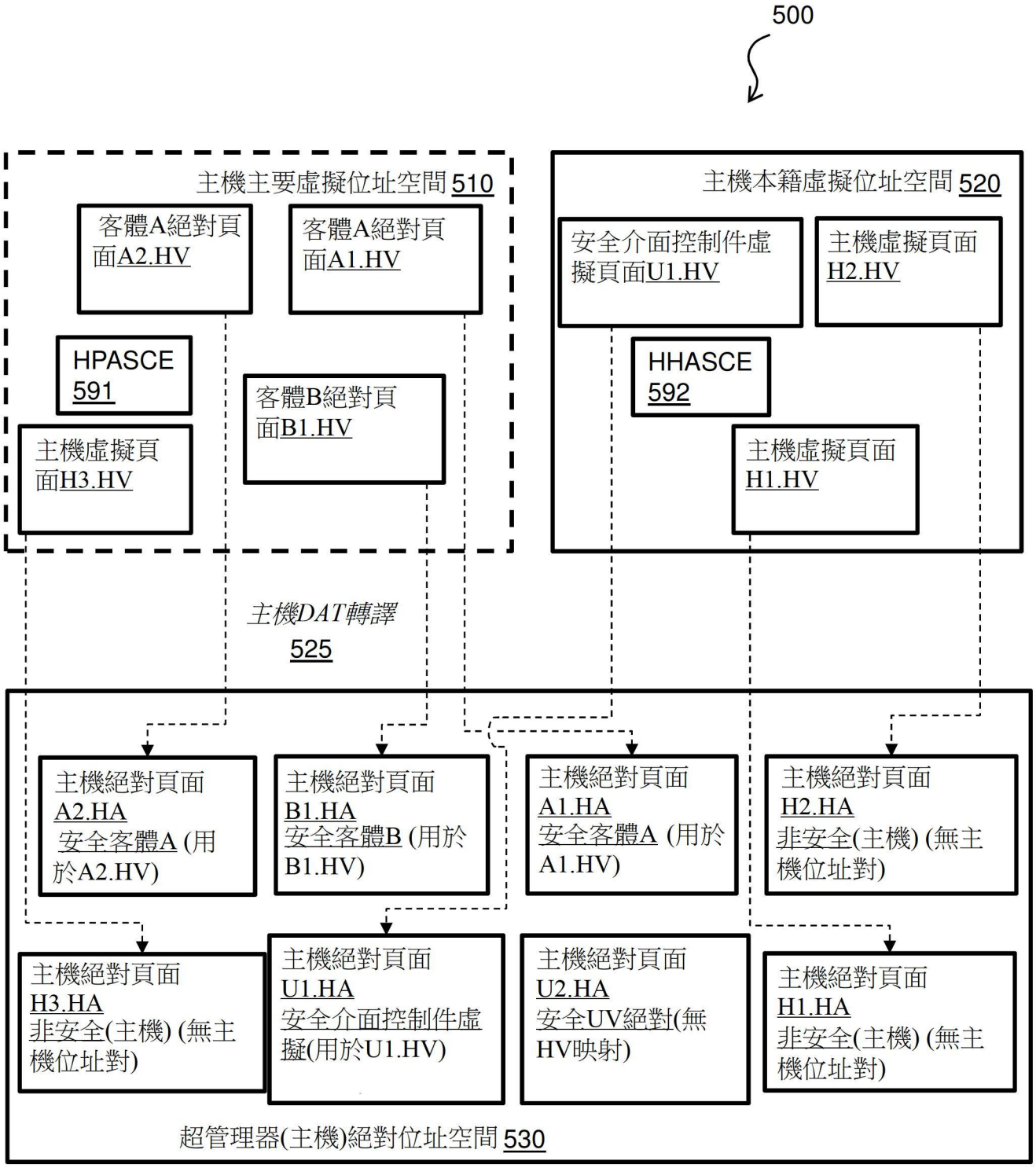
【圖2】


302
客體A虛擬位址空間A
GASCEA 304
客體虛擬頁面A1.GV 310a1
客體虛擬頁面A2.GV 310a2
客體虛擬頁面A3.GV 310a3
306
客體B虛擬位址空間B
GASCEB 308
客體虛擬頁面B1.GV 320b1
客體虛擬頁面B2.GV 320b2
325
客體DAT轉譯
HASCE 350
主機虛擬位址空間
客體A絕對位址空間A
客體絕對頁面A1.HV 340a1
客體絕對頁面A3.HV 340a3
客體絕對頁面A2.HV 340a2
客體B絕對位址空間B
客體絕對頁面B1.HV 360b1
客體絕對頁面B2.HV 360b2
330
主機DAT轉譯
超管理器(主機)絕對位址空間
主機絕對頁面A3.HA 370a3
主機絕對頁面A1.HA 370a1
主機絕對頁面B1.HA 370b1
主機絕對頁面AB2.HA 380

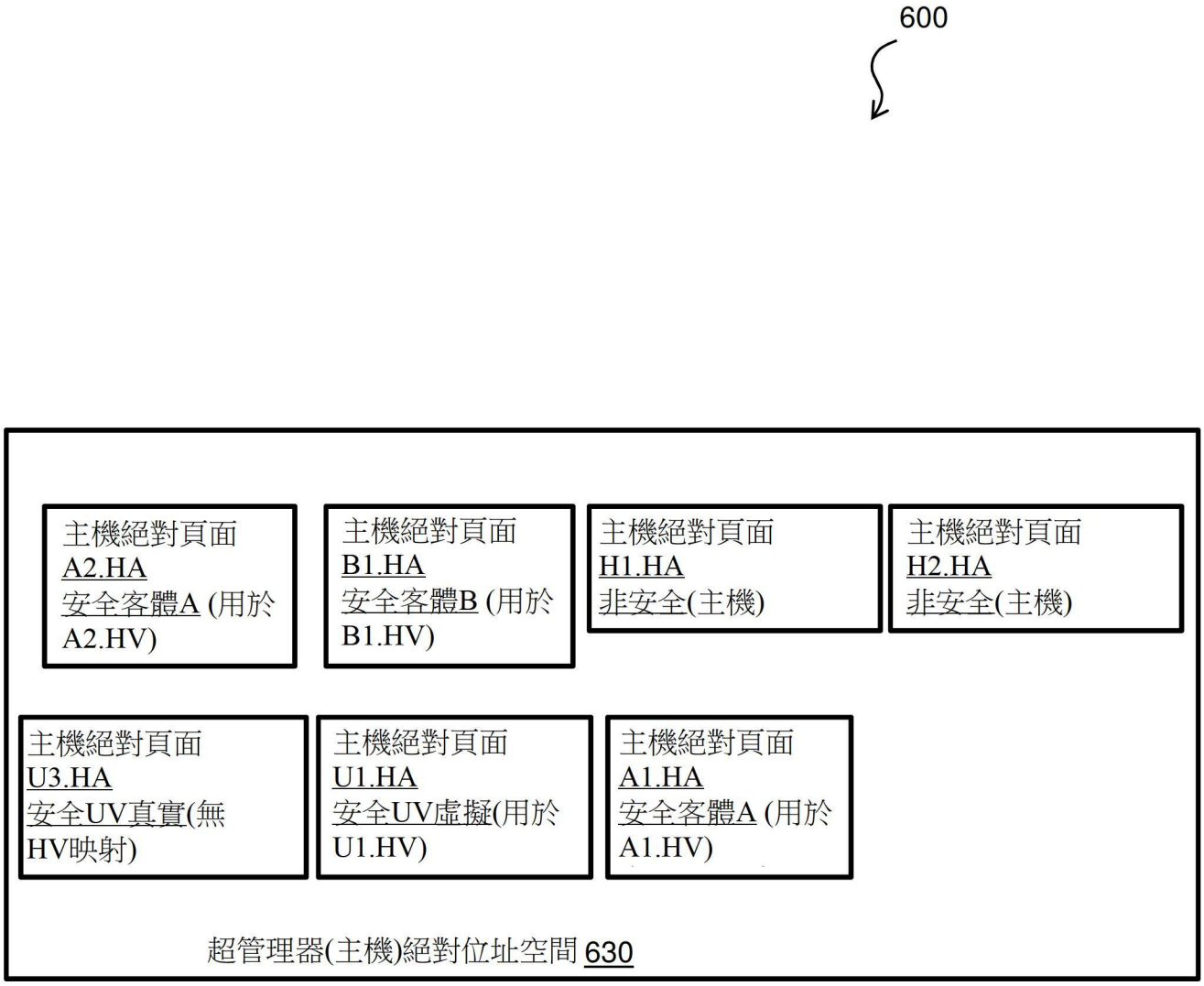
【圖3】


302
306
325
330
客體A虛擬位址空間A
客體B虛擬位址空間B
GASCEA 304
GASCEB 308
HASCE 350
客體虛擬頁面A1.GV 310a1
客體虛擬頁面A2.GV 310a2
客體虛擬頁面A3.GV 310a3
客體虛擬頁面B1.GV 320b1
客體虛擬頁面B2.GV 320b2
客體DAT轉譯
主機虛擬位址空間
客體A絕對位址空間A
客體絕對頁面A1.HV 340a1
客體絕對頁面A3.HV 340a3
客體絕對頁A2.HV 340a2
客體B絕對位址空間B
客體絕對頁面B2.HV 360b2
客體絕對頁面B1.HV 360b1
主機DAT轉譯
超管理器(主機)絕對位址空間
主機絕對頁面A3.HA 安全客體A (用於A3.GV) 370a3
主機絕對頁面A2.HA 安全客體A (用於A2.GV) 490a
主機絕對頁面B1.HA 安全客體B (用於B1.GV) 490b
主機絕對頁面A1.HA 安全客體A (用於A1.GV) 370a1
主機絕對頁面B1.HA 安全客體B (用於B1.GV) 370b1

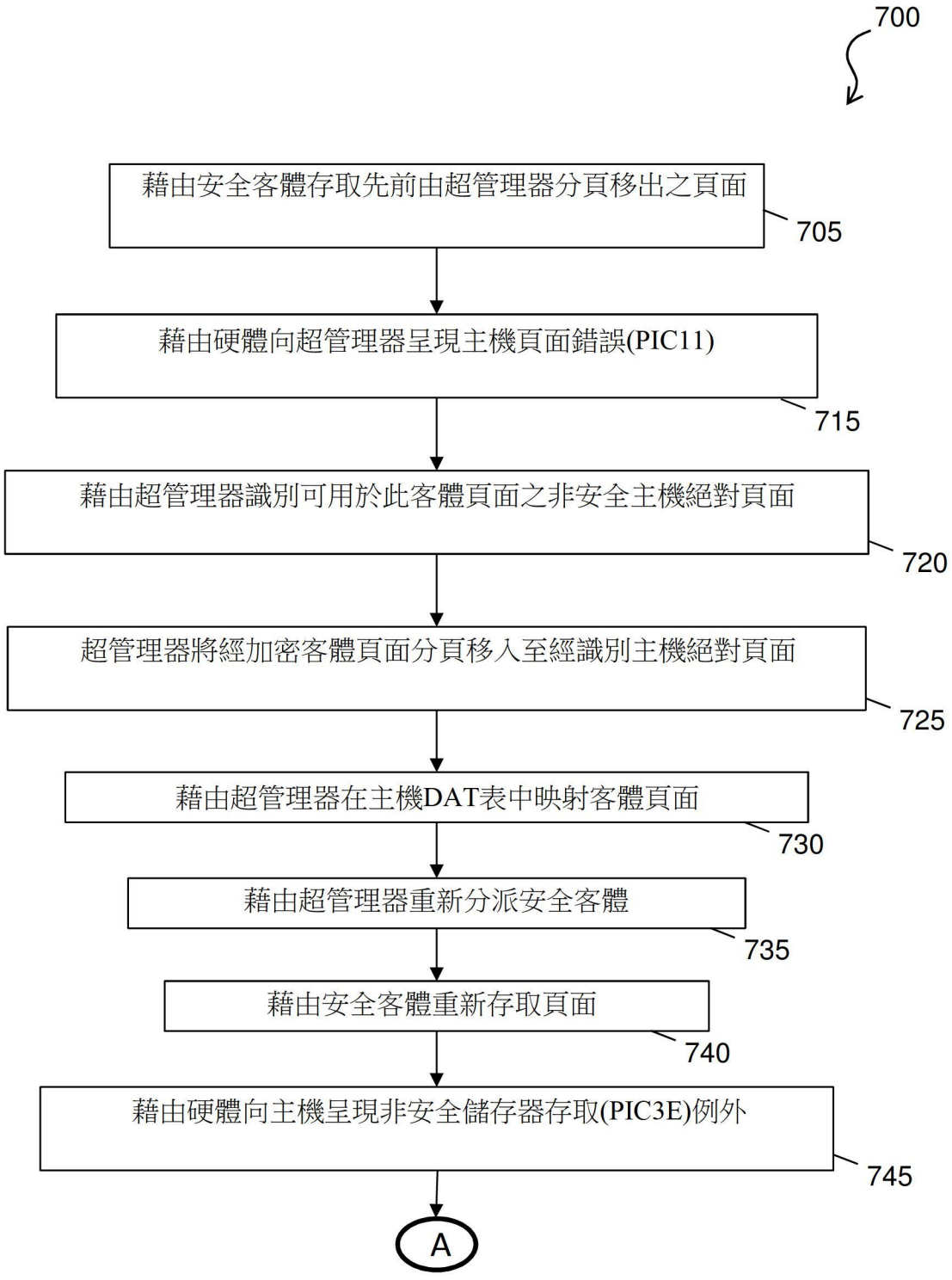
【圖4】


500
主機主要虛擬位址空間 510
客體A絕對頁面A2.HV
客體A絕對頁面A1.HV
HPASCE 591
客體B絕對頁面B1.HV
主機虛擬頁面H3.HV
主機本籍虛擬位址空間 520
安全介面控制件虛擬頁面U1.HV
主機虛擬頁面H2.HV
HHASCE 592
主機虛擬頁面H1.HV
主機DAT轉譯 525
主機絕對頁面A2.HA 安全客體A (用於A2.HV)
主機絕對頁面B1.HA 安全客體B (用於B1.HV)
主機絕對頁面A1.HA 安全客體A (用於A1.HV)
主機絕對頁面H2.HA 非安全(主機) (無主機位址對)
主機絕對頁面H3.HA 非安全(主機) (無主機位址對)
主機絕對頁面U1.HA 安全介面控制件虛擬(用於U1.HV)
主機絕對頁面U2.HA 安全UV絕對(無HV映射)
主機絕對頁面H1.HA 非安全(主機) (無主機位址對)
超管理器(主機)絕對位址空間 530

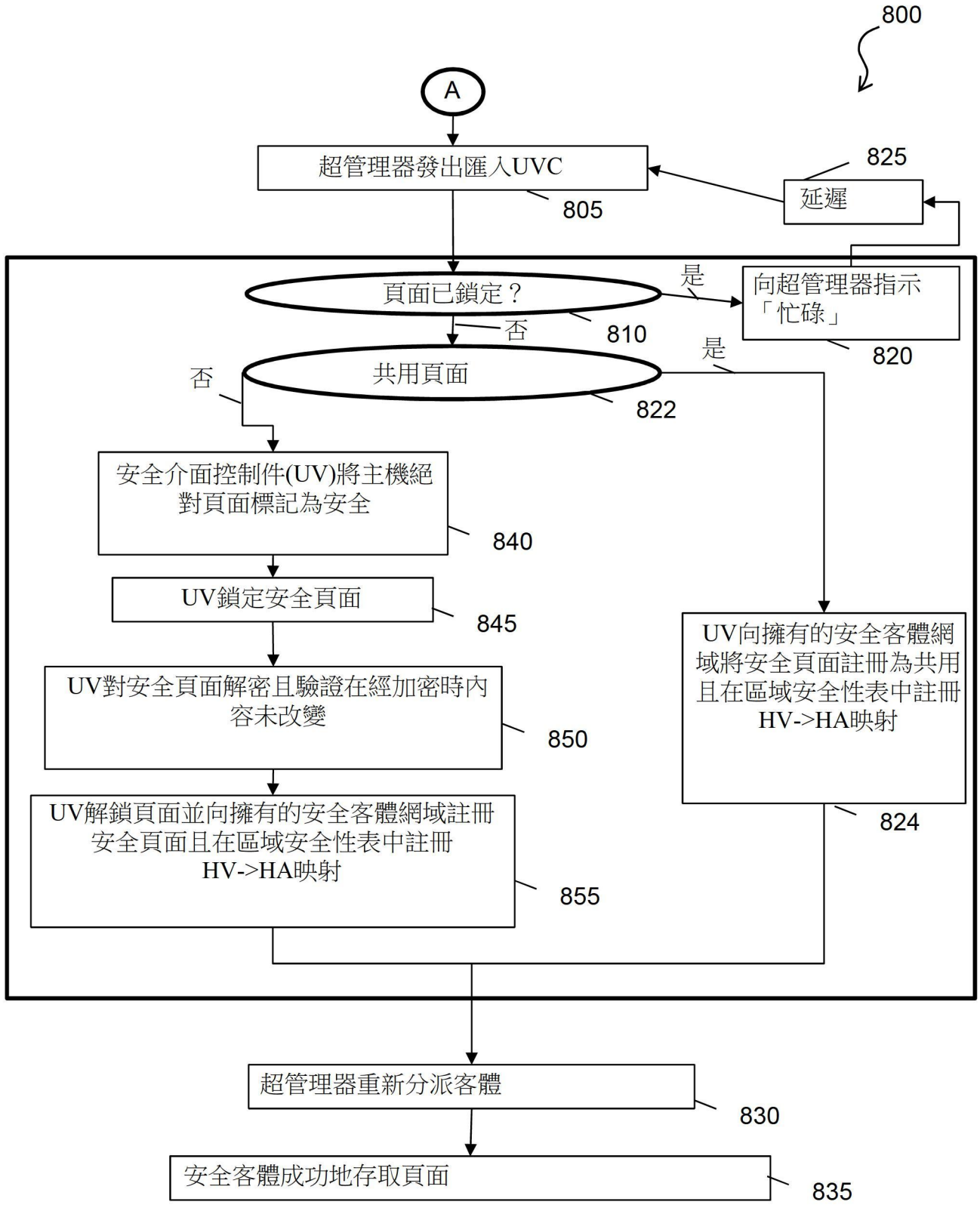
【圖5】


600
主機絕對頁面
A2.HA
安全客體A (用於A2.HV)
主機絕對頁面
B1.HA
安全客體B (用於B1.HV)
主機絕對頁面
H1.HA
非安全(主機)
主機絕對頁面
H2.HA
非安全(主機)
主機絕對頁面
U3.HA
安全UV真實(無HV映射)
主機絕對頁面
U1.HA
安全UV虛擬(用於U1.HV)
主機絕對頁面
A1.HA
安全客體A (用於A1.HV)
超管理器(主機)絕對位址空間 630

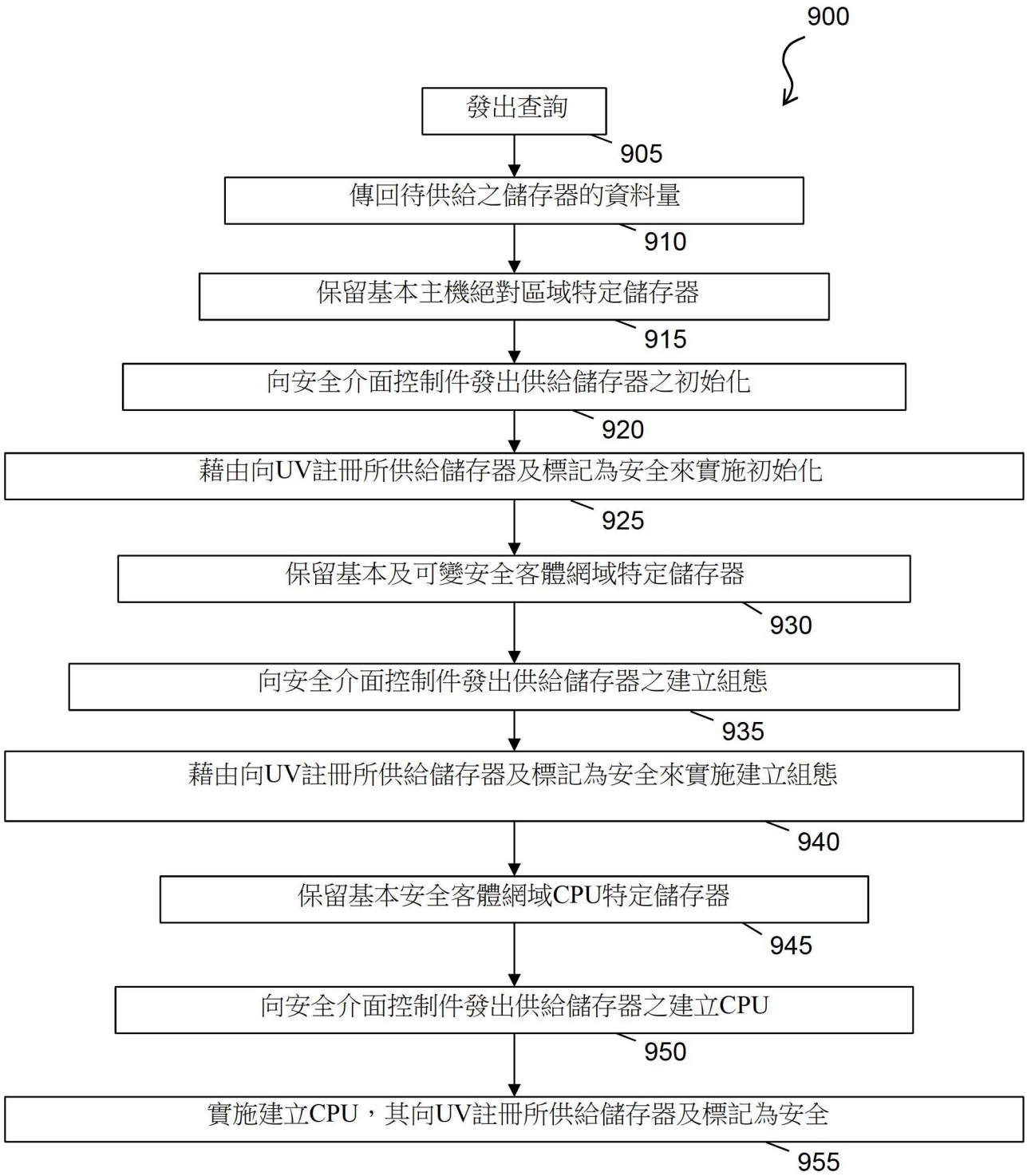
【圖6】


700
藉由安全客體存取先前由超管理器分頁移出之頁面
705
藉由硬體向超管理器呈現主機頁面錯誤(PIC11)
715
藉由超管理器識別可用於此客體頁面之非安全主機絕對頁面
720
超管理器將經加密客體頁面分頁移入至經識別主機絕對頁面
725
藉由超管理器在主機DAT表中映射客體頁面
730
藉由超管理器重新分派安全客體
735
藉由安全客體重新存取頁面
740
藉由硬體向主機呈現非安全儲存器存取(PIC3E)例外
745
A

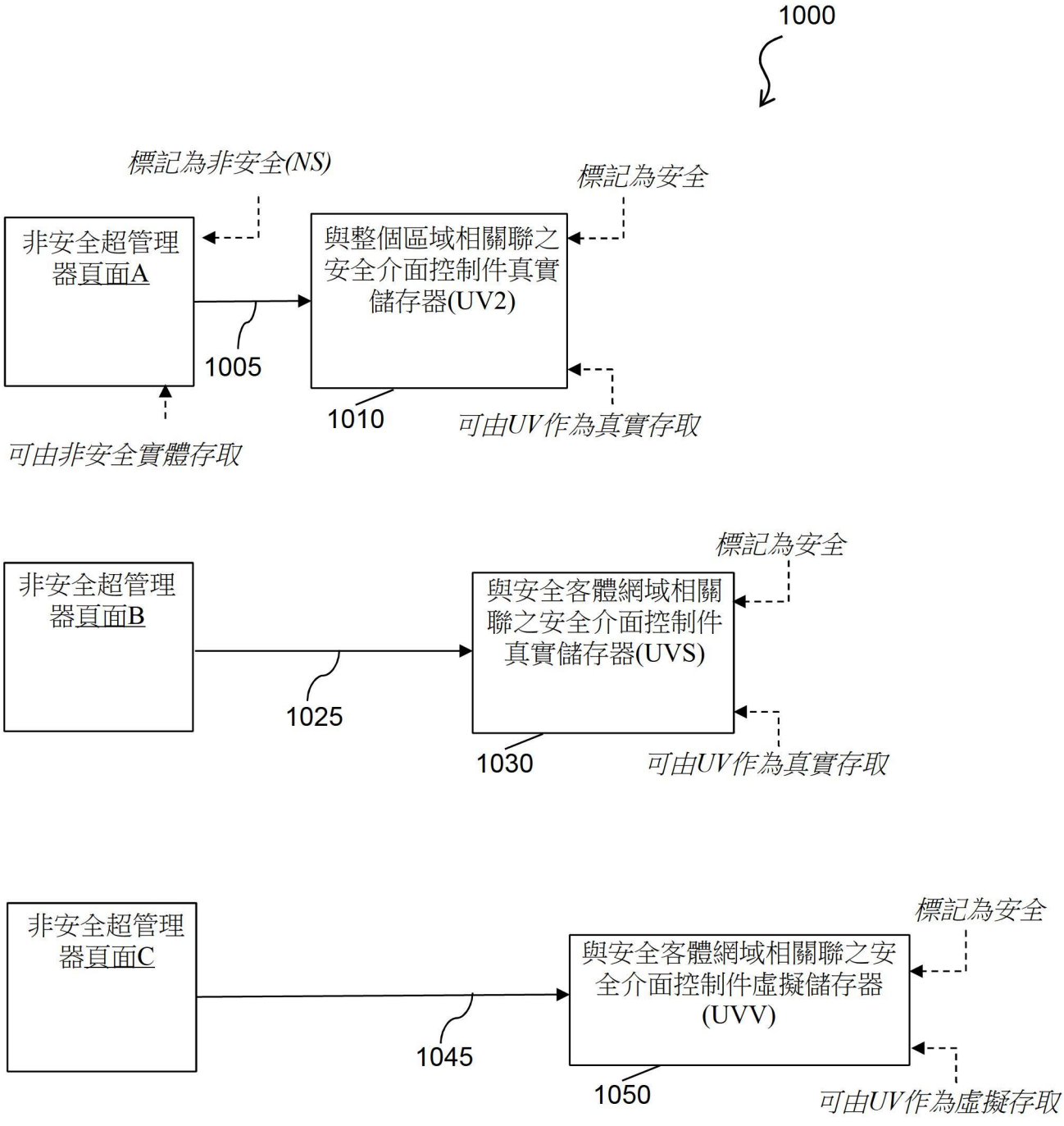
【圖7】


800
A
超管理器發出匯入UVC
805
825
延遲
頁面已鎖定？
是
向超管理器指示「忙碌」
820
否
810
是
否
共用頁面
822
安全介面控制件(UV)將主機絕對頁面標記為安全
840
UV鎖定安全頁面
845
UV對安全頁面解密且驗證在經加密時內容未改變
850
UV向擁有的安全客體網域將安全頁面註冊為共用且在區域安全性表中註冊HV->HA映射
824
UV解鎖頁面並向擁有的安全客體網域註冊安全頁面且在區域安全性表中註冊HV->HA映射
855
超管理器重新分派客體
830
安全客體成功地存取頁面
835

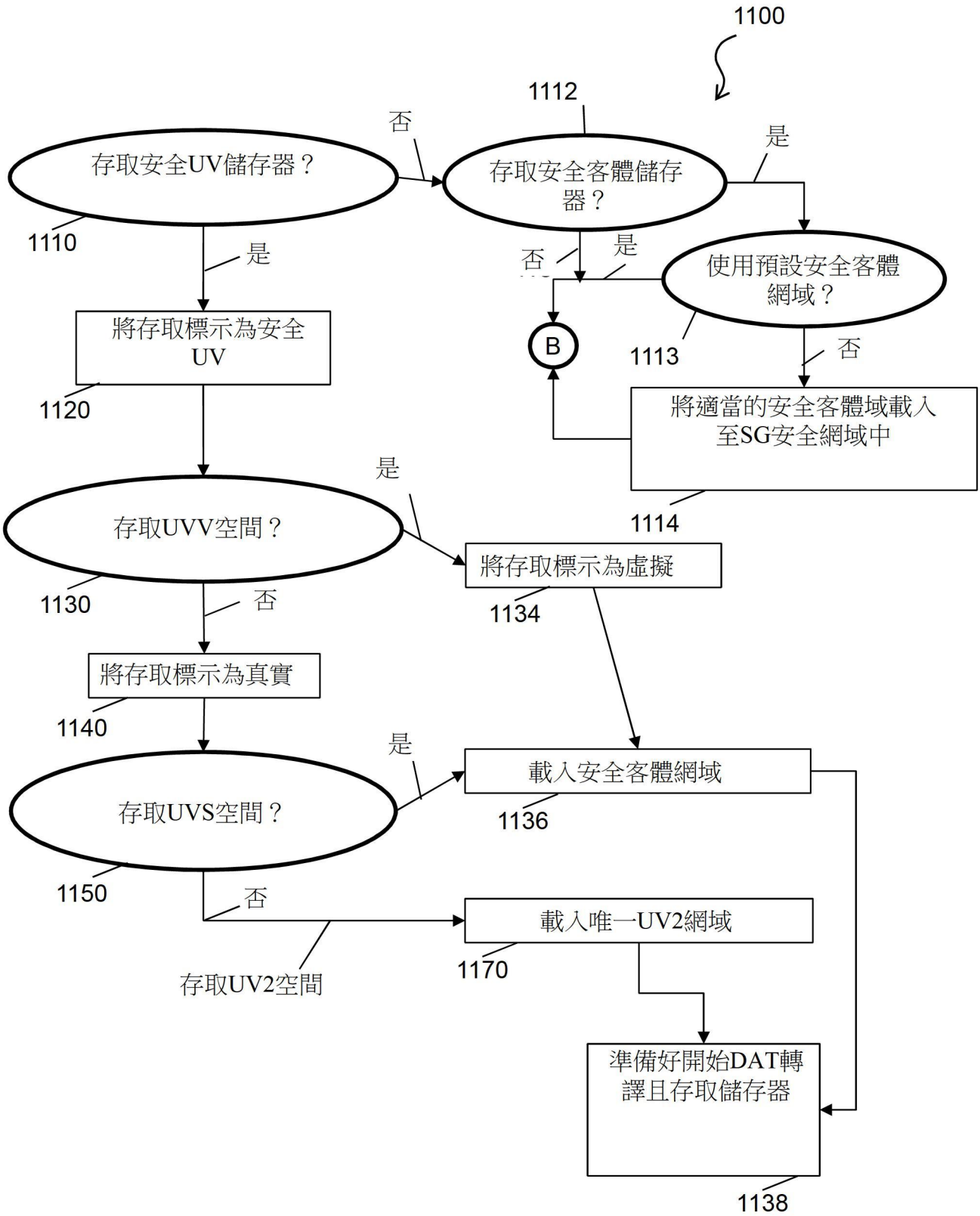
【圖8】


900
發出查詢
905
傳回待供給之儲存器的資料量
910
保留基本主機絕對區域特定儲存器
915
向安全介面控制件發出供給儲存器之初始化
920
藉由向UV註冊所供給儲存器及標記為安全來實施初始化
925
保留基本及可變安全客體網域特定儲存器
930
向安全介面控制件發出供給儲存器之建立組態
935
藉由向UV註冊所供給儲存器及標記為安全來實施建立組態
940
保留基本安全客體網域CPU特定儲存器
945
向安全介面控制件發出供給儲存器之建立CPU
950
實施建立CPU，其向UV註冊所供給儲存器及標記為安全
955

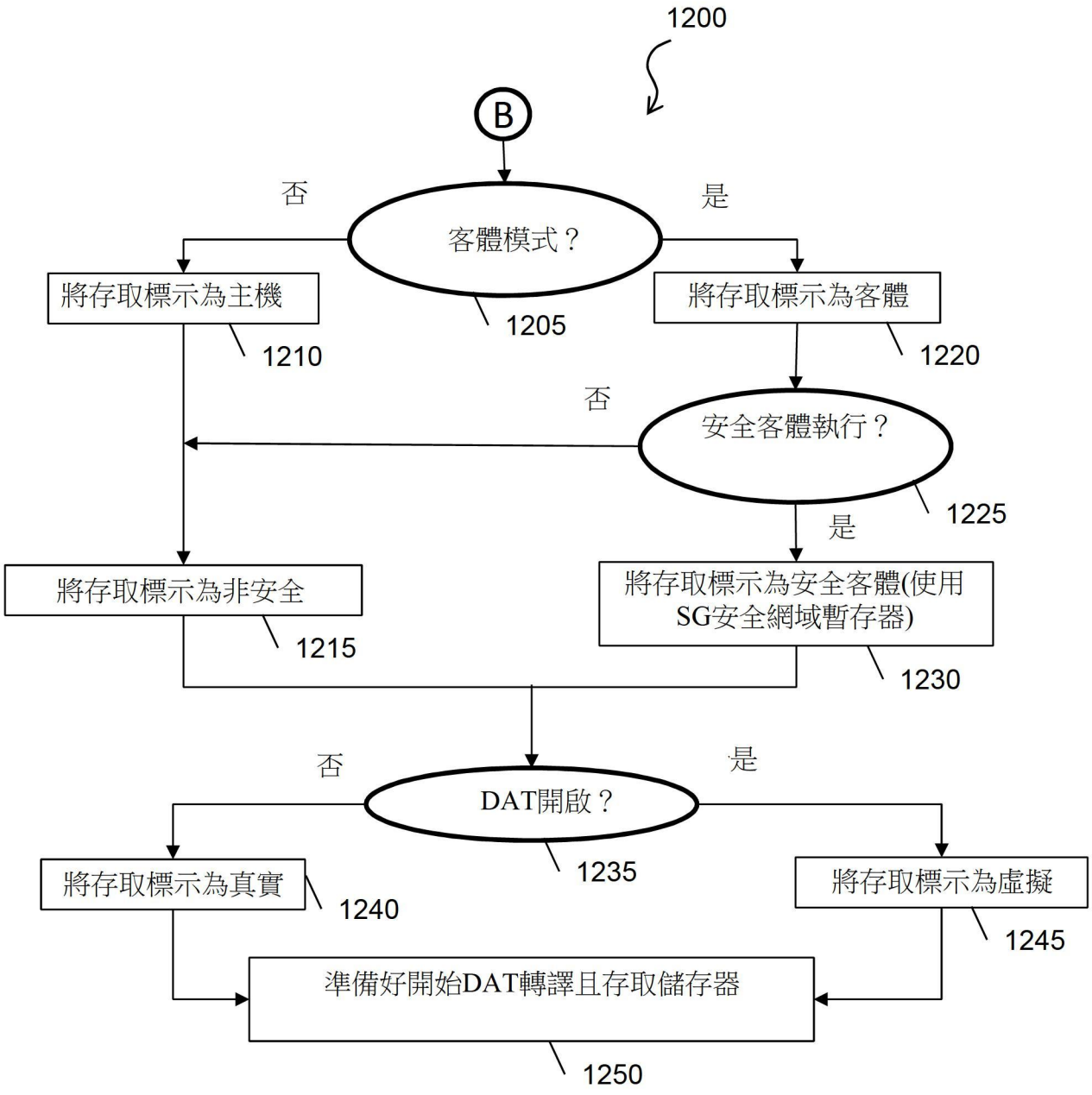
【圖9】


1000
標記為非安全(NS)
標記為安全
非安全超管理器頁面A
與整個區域相關聯之安全介面控制件真實儲存器(UV2)
1005
1010
可由UV作為真實存取
可由非安全實體存取
標記為安全
非安全超管理器頁面B
與安全客體網域相關聯之安全介面控制件真實儲存器(UVS)
1025
1030
可由UV作為真實存取
標記為安全
非安全超管理器頁面C
與安全客體網域相關聯之安全介面控制件虛擬儲存器(UVV)
1045
1050
可由UV作為虛擬存取

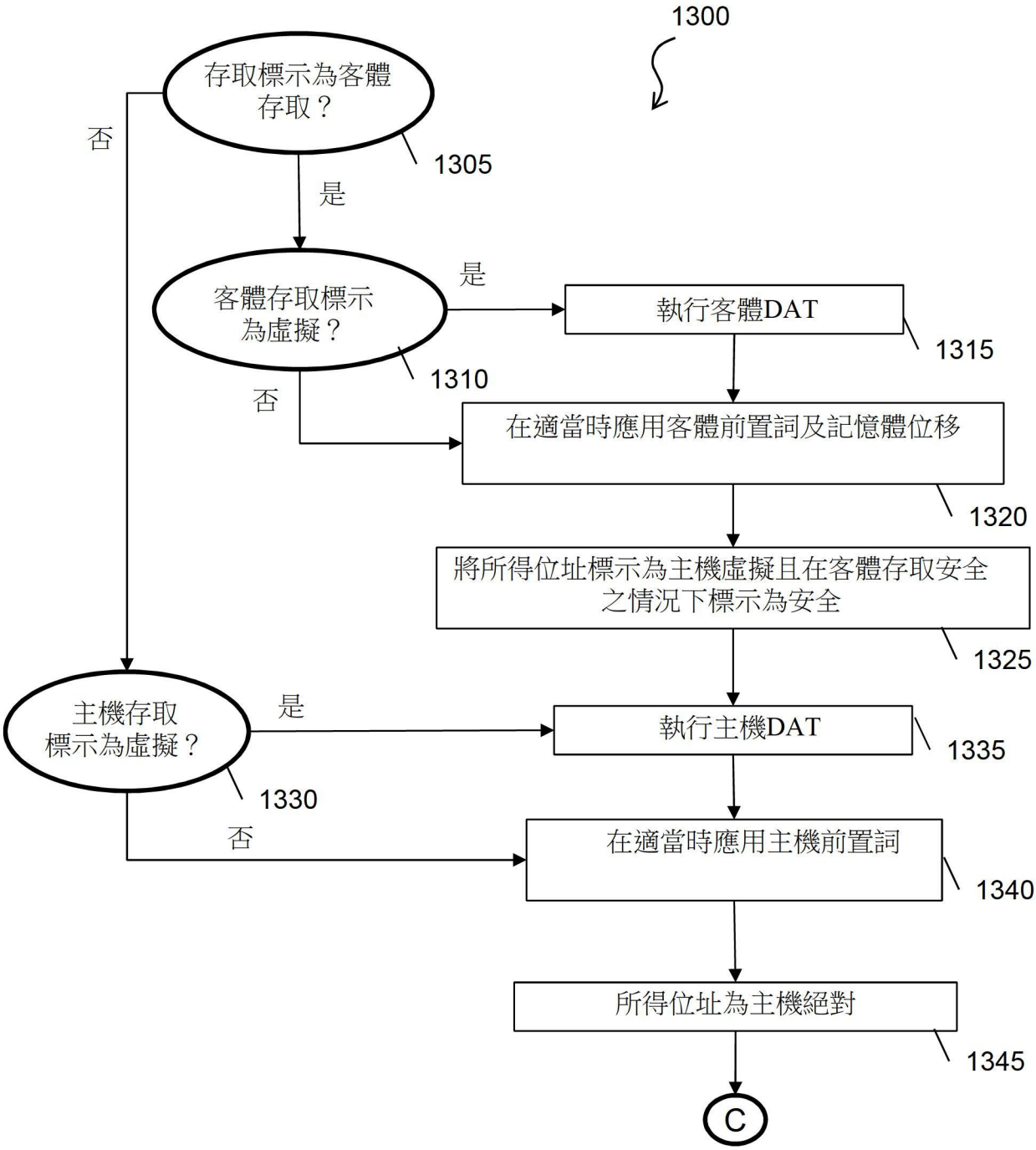
【圖10】


1100
1112
否
存取安全UV儲存器？
存取安全客體儲存器？
是
1110
是
否
是
使用預設安全客體網域？
將存取標示為安全UV
B
1113
否
1120
將適當的安全客體域載入至SG安全網域中
1114
是
存取UVV空間？
將存取標示為虛擬
1130
否
1134
將存取標示為真實
1140
是
存取UVS空間？
載入安全客體網域
1136
1150
否
載入唯一UV2網域
存取UV2空間
1170
準備好開始DAT轉譯且存取儲存器
1138

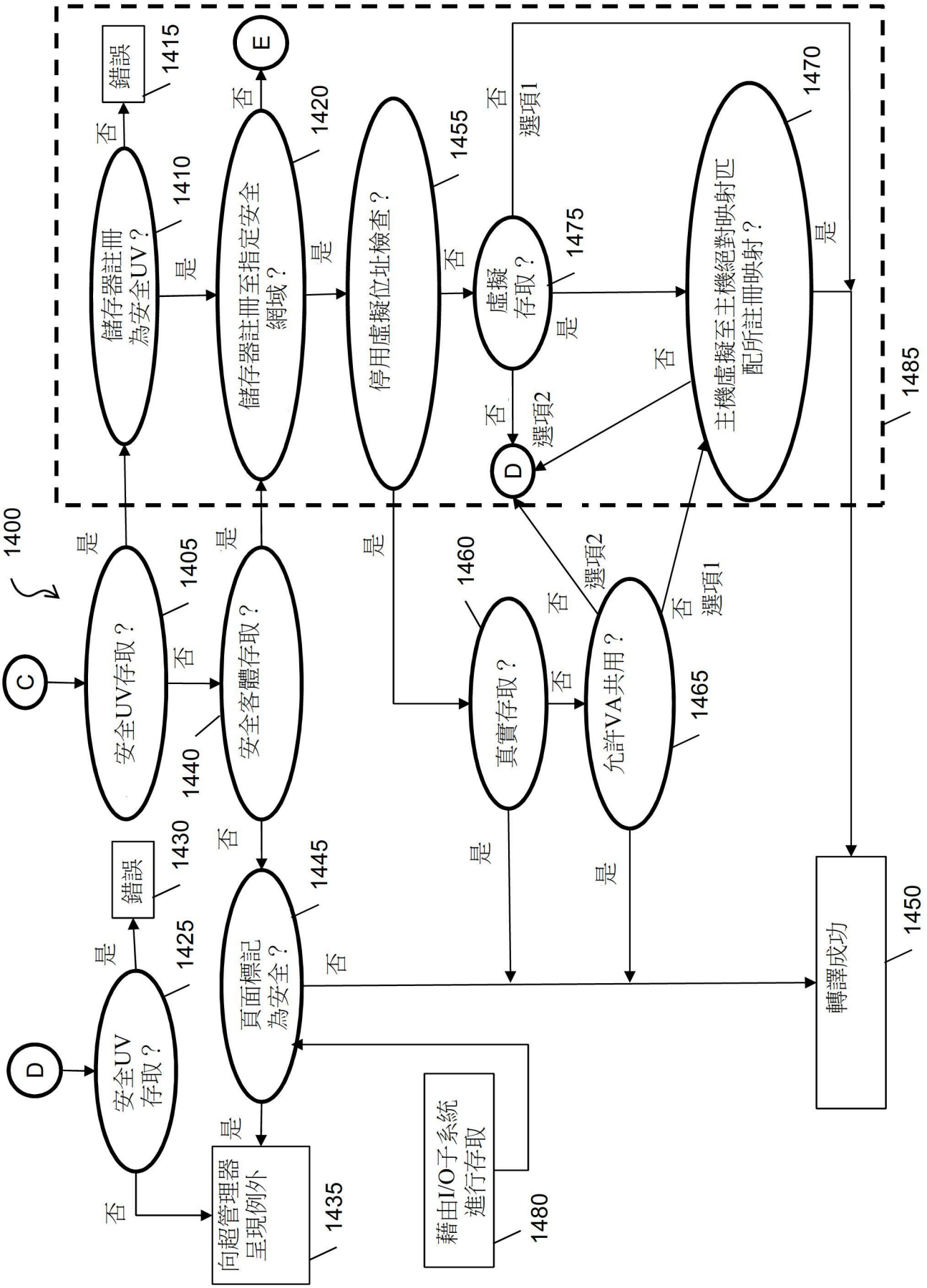
【圖11】


1200
B
否
客體模式？
是
1205
將存取標示為主機
1210
將存取標示為客體
1220
否
安全客體執行？
1225
是
將存取標示為非安全
1215
將存取標示為安全客體(使用SG安全網域暫存器)
1230
否
DAT開啟？
是
1235
將存取標示為真實
1240
將存取標示為虛擬
1245
準備好開始DAT轉譯且存取儲存器
1250

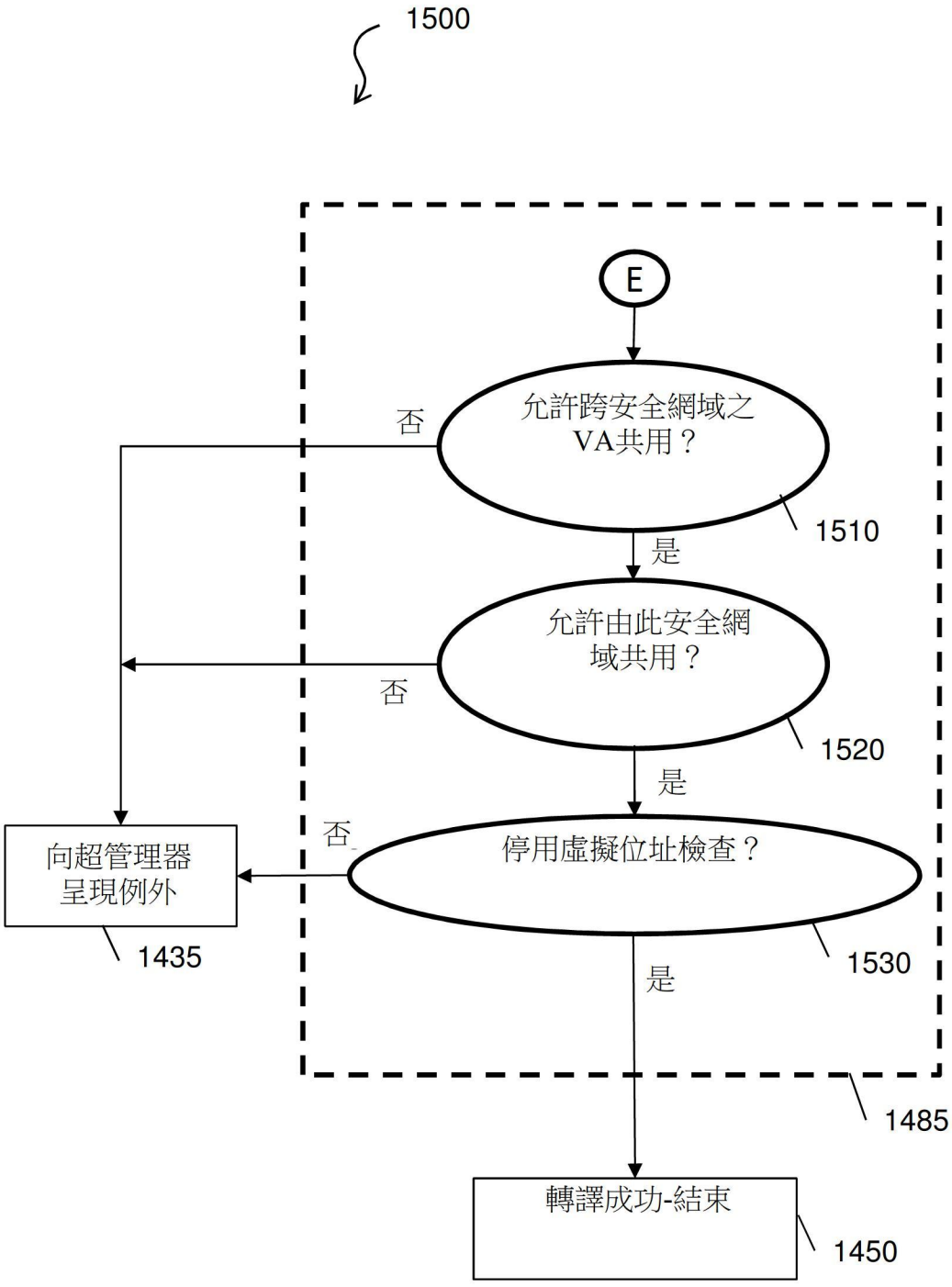
【圖12】


1300
存取標示為客體存取？
1305
否
是
客體存取標示為虛擬？
1310
是
執行客體DAT
1315
否
在適當時應用客體前置詞及記憶體位移
1320
將所得位址標示為主機虛擬且在客體存取安全之情況下標示為安全
1325
主機存取標示為虛擬？
1330
是
執行主機DAT
1335
否
在適當時應用主機前置詞
1340
所得位址為主機絕對
1345
C

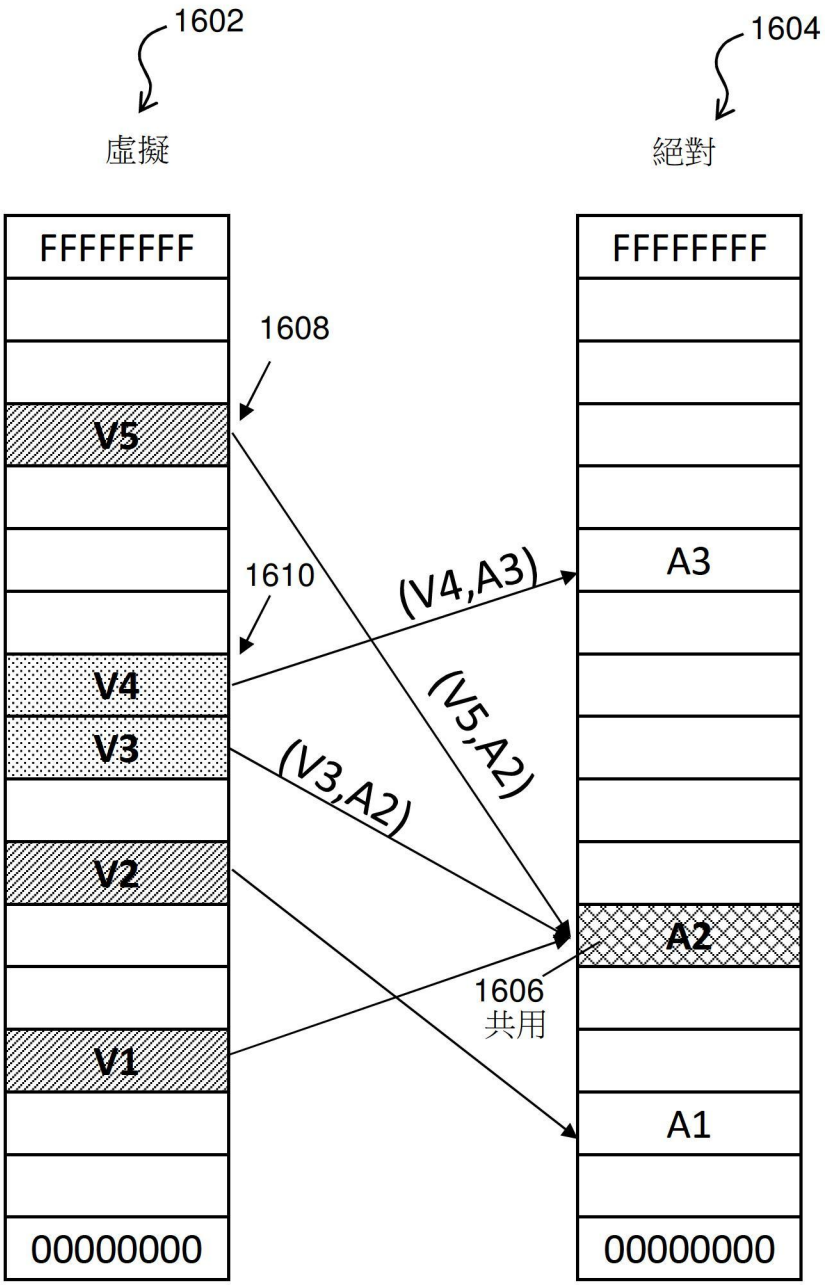
【圖13】


1400
C
D
E
安全UV存取？
1405
是
否
安全客體存取？
1440
是
否
安全UV
存取？
1425
是
否
錯誤
1430
向超管理器
呈現例外
1435
頁面標記
為安全？
1445
是
否
儲存器註冊
為安全UV？
1410
是
否
錯誤
1415
儲存器註冊至指定安全
網域？
1420
是
否
停用虛擬位址檢查？
1455
是
否
真實存取？
1460
是
否
允許VA共用？
1465
是
否
虛擬
存取？
1475
是
否
選項1
選項2
主機虛擬至主機絕對映射匹
配所註冊映射？
1470
是
否
選項1
選項2
1485
轉譯成功
1450
藉由I/O子系統
進行存取
1480

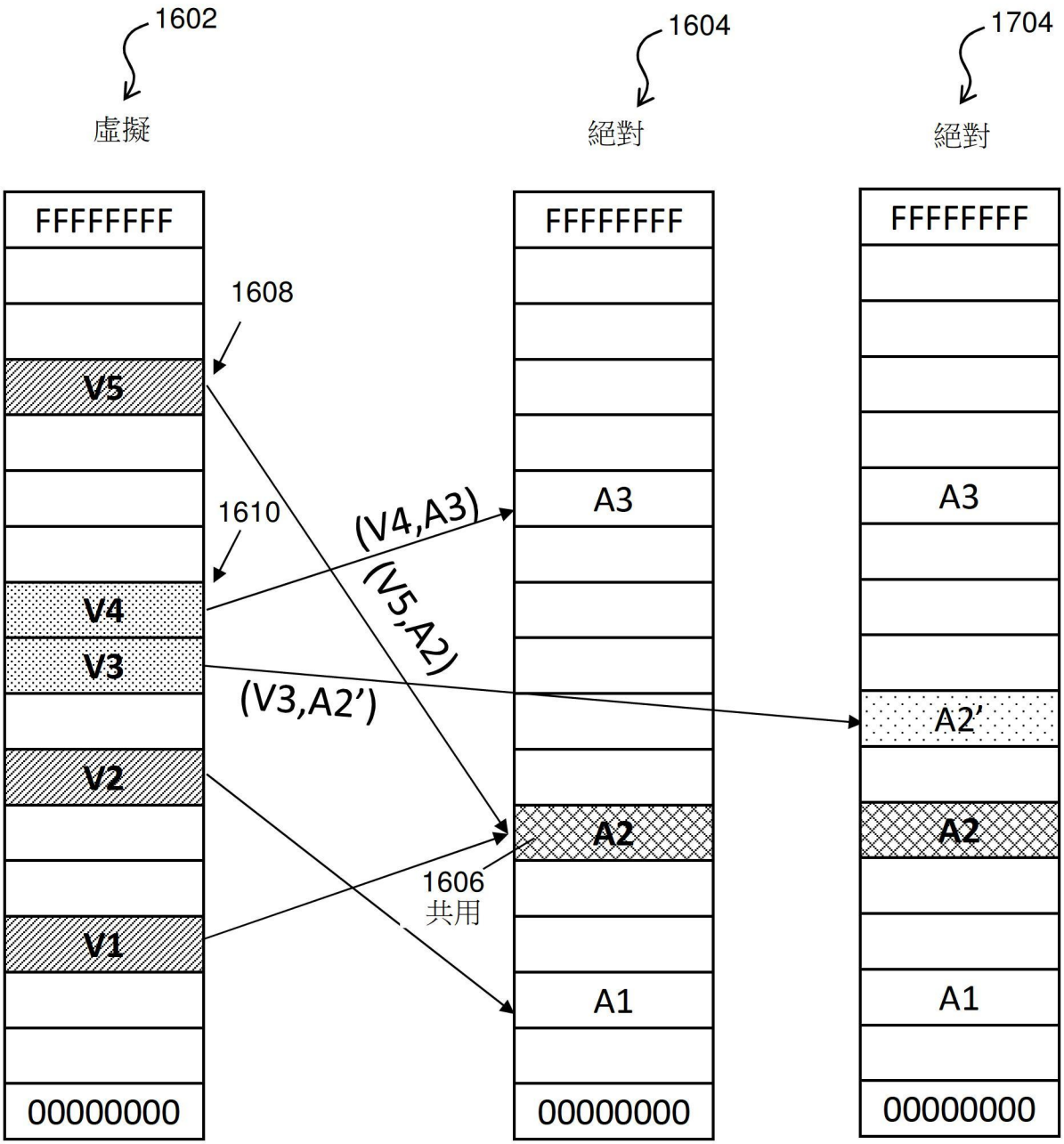
【圖14】


1500
E
允許跨安全網域之VA共用？
否
是
1510
允許由此安全網域共用？
否
是
1520
停用虛擬位址檢查？
否
是
1530
向超管理器呈現例外
1435
1485
轉譯成功-結束
1450

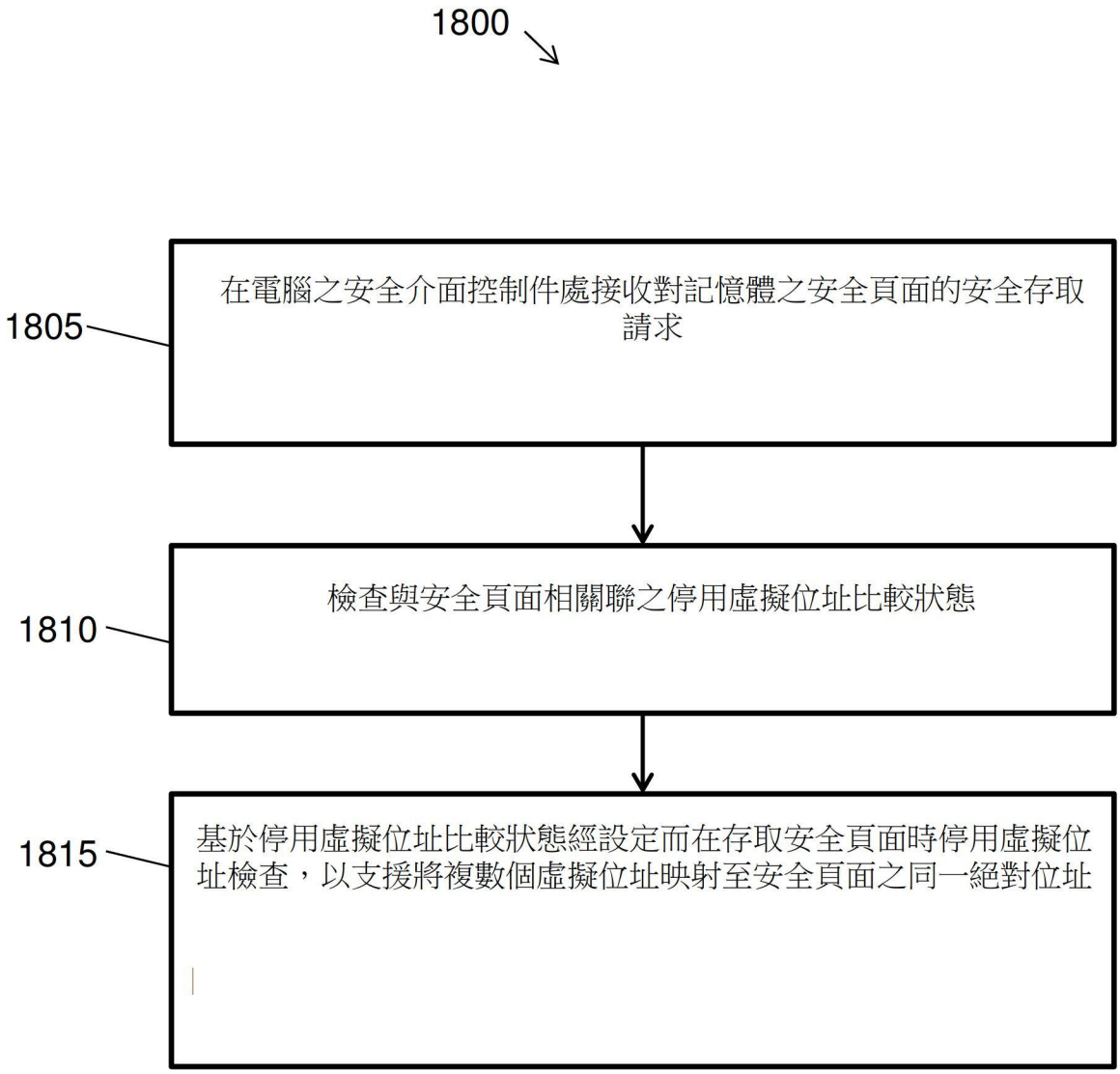
【圖15】


1602
虛擬
1604
絕對
FFFFFFFF
1608
V5
1610
(V4,A3)
A3
V4
(V5,A2)
V3
(V3,A2)
V2
A2
1606
共用
V1
A1
00000000
FFFFFFFF
00000000

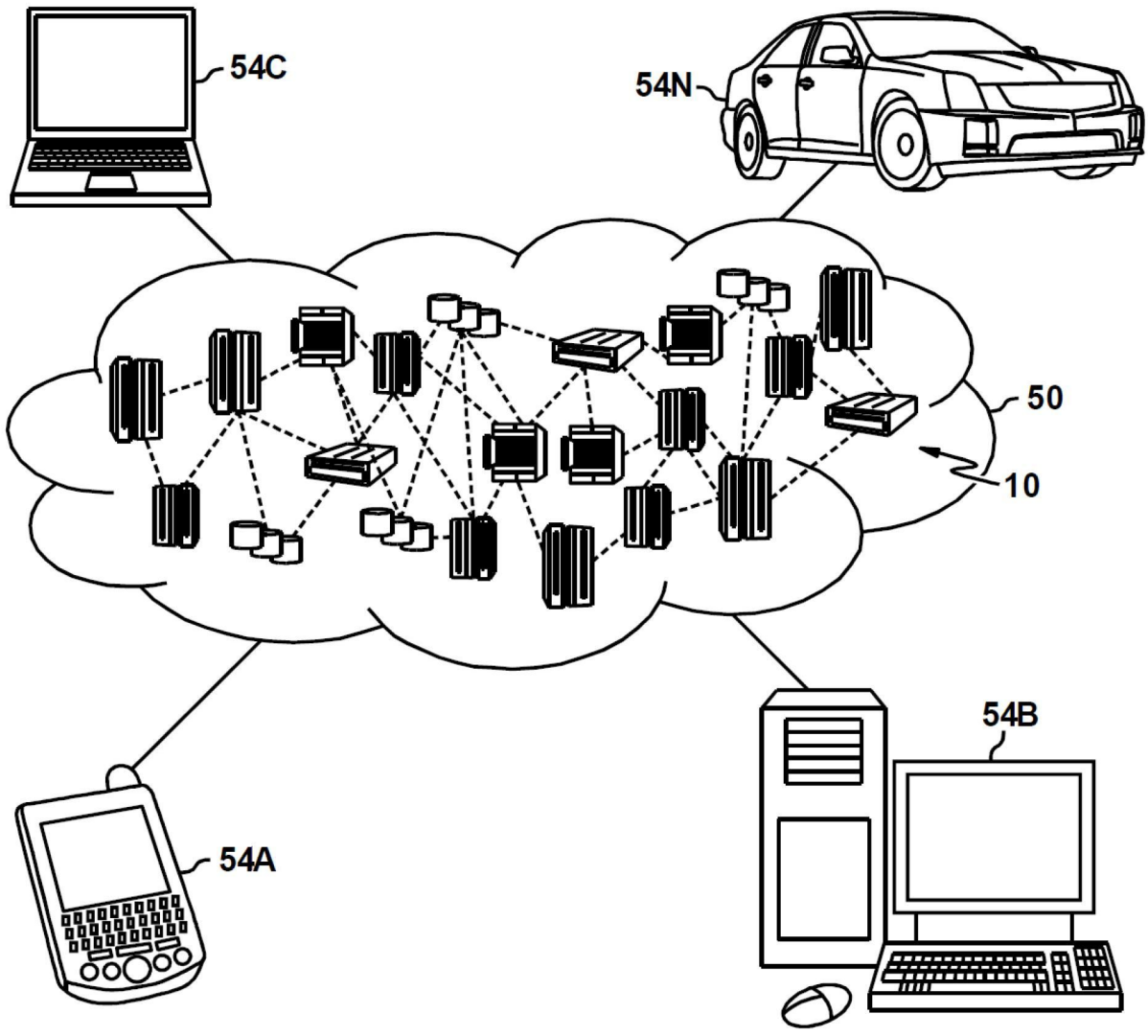
【圖16】


1602
虛擬
1604
絕對
1704
絕對
FFFFFFFF
V5
V4
V3
V2
V1
00000000
1608
1610
(V4,A3)
(V5,A2)
(V3,A2')
1606
共用
A3
A2
A1
00000000
FFFFFFFF
A3
A2'
A2
A1
00000000
FFFFFFFF

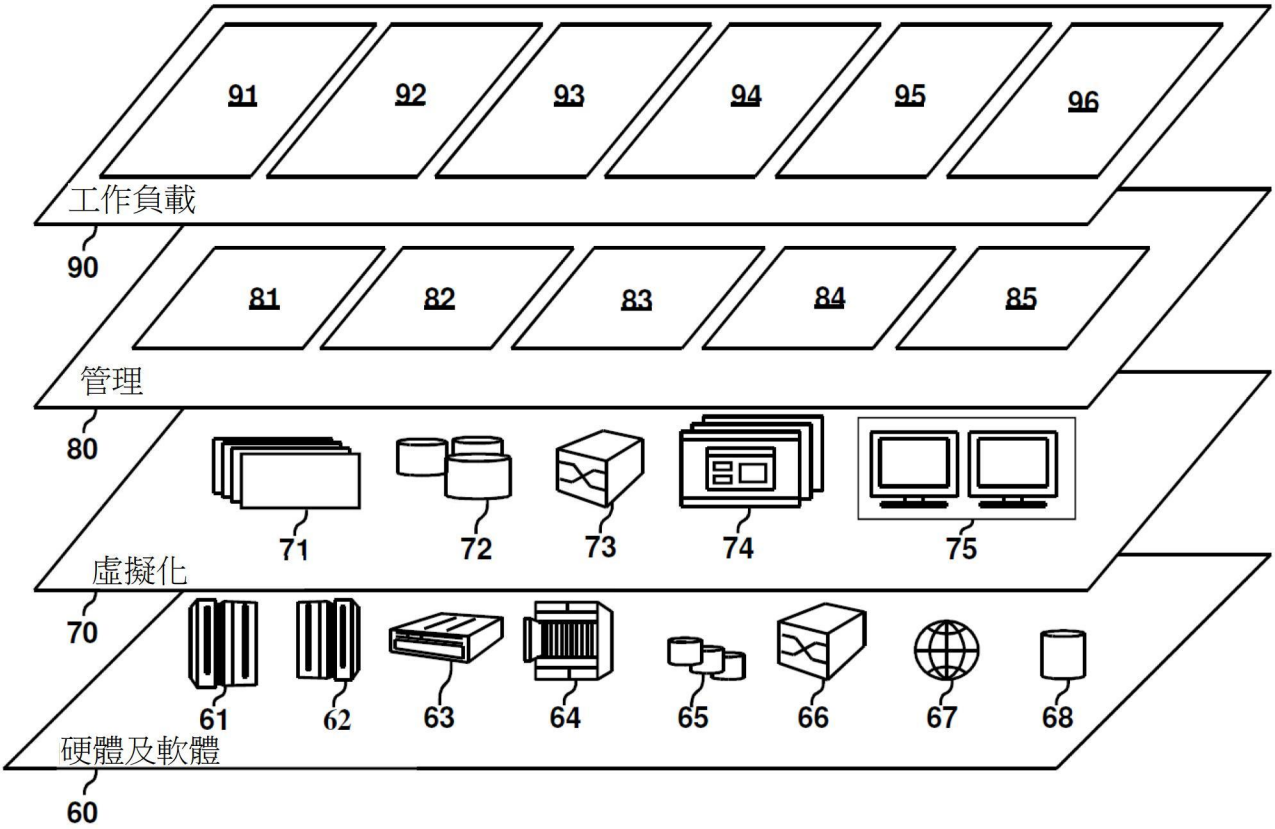
【圖17】


1800
1805
在電腦之安全介面控制件處接收對記憶體之安全頁面的安全存取請求
1810
檢查與安全頁面相關聯之停用虛擬位址比較狀態
1815
基於停用虛擬位址比較狀態經設定而在存取安全頁面時停用虛擬位址檢查，以支援將複數個虛擬位址映射至安全頁面之同一絕對位址

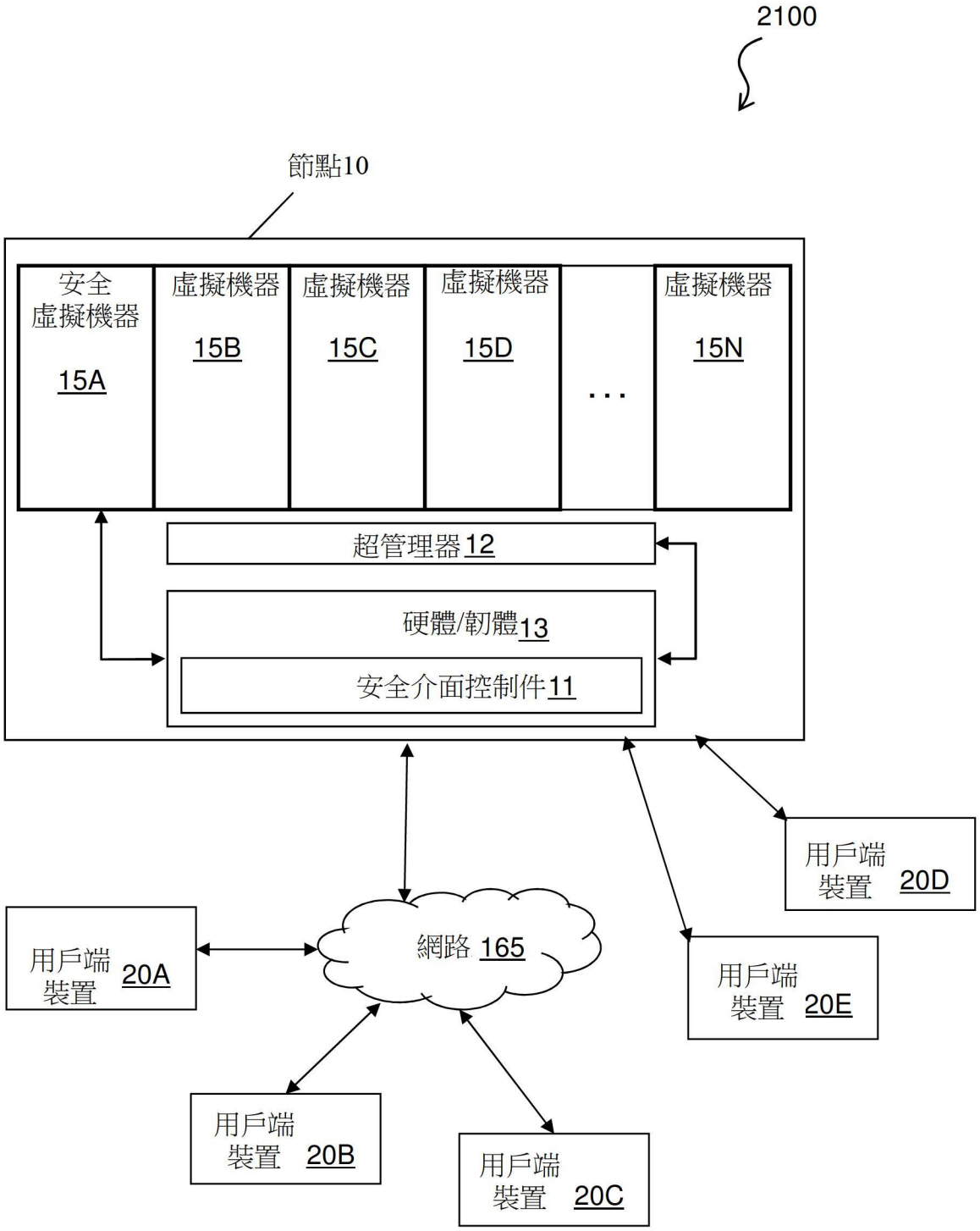
【圖18】



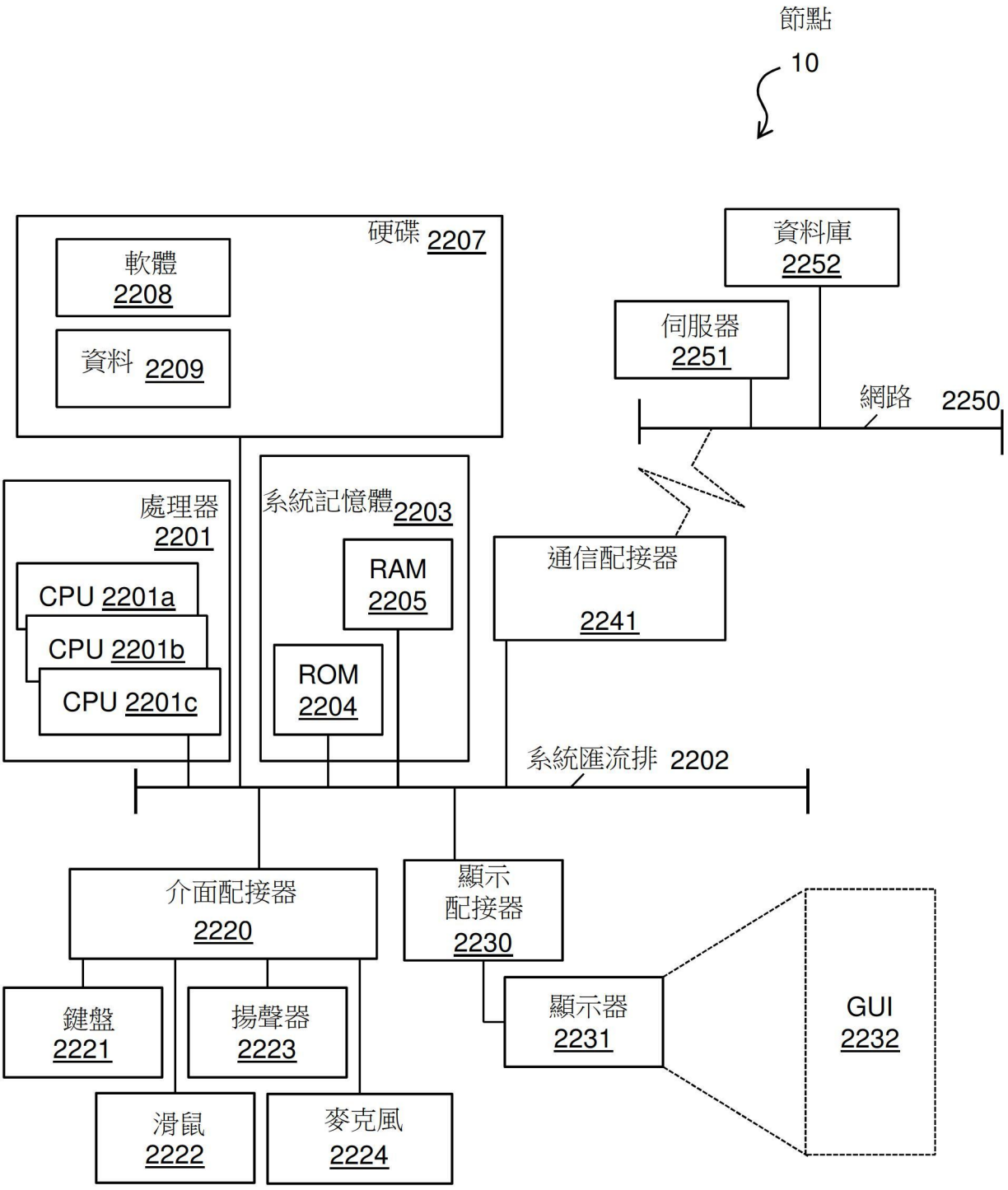
【圖19】


91
92
93
94
95
96
工作負載
90
81
82
83
84
85
管理
80
71
72
73
74
75
虛擬化
70
61
62
63
64
65
66
67
68
硬體及軟體
60

【圖20】


2100
節點10
安全
虛擬機器
15A
虛擬機器
15B
虛擬機器
15C
虛擬機器
15D
...
虛擬機器
15N
超管理器12
硬體/韌體13
安全介面控制件11
用戶端
裝置 20D
用戶端
裝置 20A
網路 165
用戶端
裝置 20E
用戶端
裝置 20B
用戶端
裝置 20C

【圖21】


節點
10
硬碟 2207
軟體
2208
資料 2209
資料庫
2252
伺服器
2251
網路 2250
處理器
2201
CPU 2201a
CPU 2201b
CPU 2201c
系統記憶體2203
RAM
2205
ROM
2204
通信配接器
2241
系統匯流排 2202
介面配接器
2220
顯示
配接器
2230
鍵盤
2221
揚聲器
2223
顯示器
2231
GUI
2232
滑鼠
2222
麥克風
2224

【圖22】