I772747

(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 I772747 B**

(45)公告日： 中華民國 111 (2022) 年 08 月 01 日

(21)申請案號：109104690 (22)申請日： 中華民國 109 (2020) 年 02 月 14 日

(51)Int. Cl.： ***G06F9/455 (2006.01)***

(30)優先權：2019/03/08 美國 16/296,332

(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：尹布蘭達 克勞迪亞 IMBRENDA, CLAUDIO (IT)；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	I453672B	TW	201710912A
US	9792143B1	US	2018/0247082A1
US	2018/0330081A1		

審查人員：高元良

申請專利範圍項數：25 項 圖式數：6 共 47 頁

(54)名稱

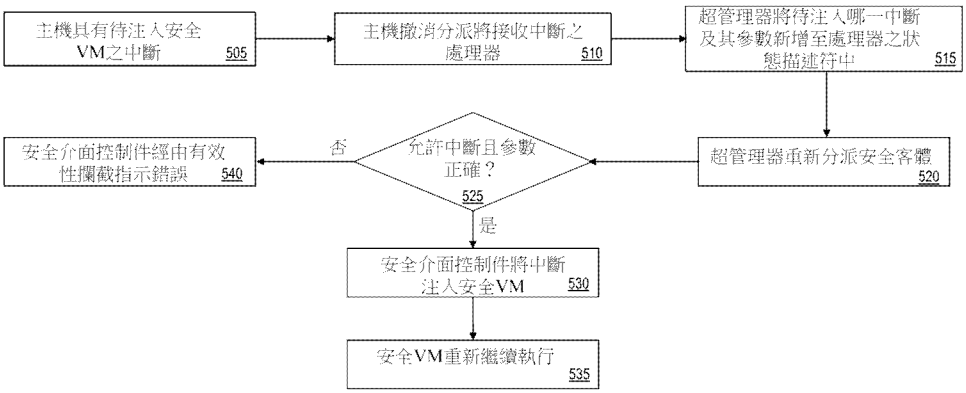
用於將中斷及例外注入安全虛擬機器之電腦實施方法、電腦系統及電腦程式產品

(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藉由在一主機伺服器上執行之一非安全實體起始一安全實體，該非安全實體被禁止直接存取該安全實體之任何資料。該方法進一步包括將由該主機伺服器產生之一中斷注入該安全實體。該注入包括藉由該非安全實體將關於該中斷之資訊新增至接著與該安全實體相關聯之非安全儲存器之一部分中。該注入進一步包括藉由該主機伺服器之一安全介面控制件將該中斷注入該安全實體。

According to one or more embodiments of the present invention, a computer implemented method includes initiating, by a non-secure entity that is executing on a host server, a secure entity, the non-secure entity prohibited from directly accessing any data of the secure entity. The method further includes injecting, into the secure entity, an interrupt that is generated by the host server. The injecting includes adding, by the non-secure entity, information about the interrupt into a portion of non-secure storage, which is then associated with the secure entity. The injecting further includes injecting, by a secure interface control of the host server, the interrupt into the secure entity.

指定代表圖：


主機具有待注入安全VM之中斷 505
主機撤消分派將接收中斷之處理器 510
超管理器將待注入哪一中斷及其參數新增至處理器之狀態描述符中 515
超管理器重新分派安全客體 520
允許中斷且參數正確？ 525
否
安全介面控制件經由有效性攔截指示錯誤 540
是
安全介面控制件將中斷注入安全VM 530
安全VM重新繼續執行 535

【圖5】

I772747

【發明摘要】

公告本

【中文發明名稱】

用於將中斷及例外注入安全虛擬機器之電腦實施方法、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 INJECTING INTERRUPTS AND EXCEPTIONS INTO SECURE VIRTUAL MACHINE

【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藉由在一主機伺服器上執行之一非安全實體起始一安全實體，該非安全實體被禁止直接存取該安全實體之任何資料。該方法進一步包括將由該主機伺服器產生之一中斷注入該安全實體。該注入包括藉由該非安全實體將關於該中斷之資訊新增至接著與該安全實體相關聯之非安全儲存器之一部分中。該注入進一步包括藉由該主機伺服器之一安全介面控制件將該中斷注入該安全實體。

【英文】

According to one or more embodiments of the present invention, a computer implemented method includes initiating, by a non-secure entity that is executing on a host server, a secure entity, the non-secure entity prohibited from directly accessing any data of the secure entity. The method further includes injecting, into the secure entity, an interrupt that is generated by the host server. The injecting includes adding, by the non-secure entity, information about the interrupt into a portion of non-secure storage, which is then associated with the secure entity. The injecting

further includes injecting, by a secure interface control of the host server, the interrupt into the secure entity.

【指定代表圖】

圖5

【代表圖之符號簡單說明】

無

【發明說明書】

【中文發明名稱】

用於將中斷及例外注入安全虛擬機器之電腦實施方法、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 INJECTING INTERRUPTS AND EXCEPTIONS INTO SECURE VIRTUAL MACHINE

【技術領域】

【先前技術】

【0001】本申請案係關於電腦技術，且更具體而言，係關於虛擬機器或容器。

【0002】雲端計算促進能夠快速且容易地為客戶佈建虛擬機器，而不需要客戶購買硬體或為實體伺服器提供佔用面積。客戶可根據改變的偏好來擴展或收縮虛擬機器。通常，雲端計算提供者佈建虛擬機器，其實體上駐留於提供者之資料中心處。在此環境中，客戶之虛擬機器作為客體執行且雲端提供者使用作為主機執行之超管理器程式碼，以虛擬化可能屬於不同客戶之多個虛擬機器之間的伺服器資源。

【0003】客戶常常關注虛擬機器中之資料的安全性。客戶可能希望其程式碼及資料與雲端計算提供者之間或其資料之間以及其程式碼與資料之間及來自在提供者站點處執行之其他VM的安全性。客戶可能希望提供者之管理員提供安全性以及防止在機器上執行之其他程式碼(包括超管理器程式碼)中的潛在安全漏洞。此等管理員及其他程式碼可能出於惡意而行事。

【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。

【發明內容】

【0005】根據本發明之一或多個實施例，一種電腦實施方法包括藉由在主機伺服器上執行之非安全實體起始安全實體，該非安全實體被禁止直接存取安全實體尚未明確共用之安全實體的任何資料。該方法進一步包括將由主機伺服器產生之中斷注入安全實體。該注入包括藉由非安全實體將關於中斷之資訊新增至與安全實體相關聯之非安全儲存器之一部分中。該注入進一步包括藉由主機伺服器之安全介面控制件將中斷注入安全實體。在一或多個實例中，安全實體為安全虛擬機器、容器或客體。在一或多個實例中，非安全實體為超管理器、OS或主機。

【0006】根據本發明之一或多個實施例，該方法進一步包括在注入之前，藉由安全介面控制件判定是否准許將中斷注入安全實體，其中該注入係基於判定准許將中斷注入安全實體而執行。在一或多個實例中，安全介面控制件基於針對安全實體之准許中斷的清單而判定准許將中斷注入安全實體。准許中斷之清單特定於該安全實體。

【0007】根據本發明之一或多個實施例，關於中斷之資訊包含待注入之中斷的識別符及與中斷相關聯之一或多個參數。在一或多個實例中，該方法進一步包括在注入之前，藉由安全介面控制件判定是否准許將中斷及一或多個參數注入安全實體，其中該注入係基於判定准許將中斷及一或多個參數注入安全實體而執行。

【0008】在一或多個實例中，該方法進一步包括在藉由非安全實體注入之前，撤消分派與安全實體相關聯之處理器。另外，在藉由非安全實

體新增關於中斷之資訊之後，重新分派虛擬處理器以重新繼續安全實體之操作。

【0009】根據本發明之一或多個實施例，該方法進一步包括回應於判定不准許將中斷注入安全實體而藉由安全介面控制件向非安全實體指示錯誤。

【0010】根據本發明之一或多個實施例，該安全介面控制件包含硬體、微碼及其他受信任韌體。

【0011】另外，根據本發明之一或多個實施例，一種電腦實施方法包括藉由在主機伺服器上之非安全實體上執行的安全實體執行指令，該指令產生待轉遞至非安全實體之條件，該非安全實體被禁止直接存取安全實體尚未明確共用之安全實體的任何資料。該方法進一步包括撤消分派與執行指令之安全實體相關聯的處理器，該非安全實體接著仿真指令。該方法進一步包括藉由非安全實體判定是否應將中斷或程式例外遞送至安全實體，且基於此判定，藉由非安全實體，將中斷或程式例外注入安全實體。注入中斷包括基於由指令之仿真引發的中斷或程式例外，藉由非安全實體將關於中斷或程式例外之資訊新增至與安全實體相關聯之非安全儲存器之一部分。注入中斷進一步包括重新繼續與安全實體相關聯之處理器以重新繼續安全實體之操作。

【0012】根據本發明之一或多個實施例，該方法進一步包括在注入之前，藉由安全介面控制件判定程式例外對注入安全實體是否有效，其中注入係基於判定程式例外對注入安全實體有效而執行。在一或多個實例中，安全介面控制件基於對應於指令之例外的預定清單而判定程式例外有效。在一或多個實例中，關於程式例外之資訊包含待注入之程式例外的識

別符及與程式例外相關聯之一或多個參數。

【0013】上述特徵亦可至少由系統、電腦程式產品及機器提供。

【0014】額外技術特徵及益處經由本發明之技術實現。本發明之實施例及態樣在本文中經詳細描述且視為所主張主題之一部分。為了更好地理解，參考實施方式及圖式。

【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描繪根據本發明之實施例的雲端計算環境；

【0017】圖2描繪根據本發明之實施例的抽象模型層；

【0018】圖3說明根據實施例之用於代管系統的實例系統；

【0019】圖4說明根據實施例之代管系統的實例方塊圖；

【0020】圖5說明根據本發明之一或多個實施例的用於安全介面控制件將中斷之通知提供至安全VM的實例方法之流程圖；及

【0021】圖6說明根據本發明之一或多個實施例的用於安全VM在非安全實體中引發例外的實例方法之流程圖。

【實施方式】

【0022】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處理程序或程序中。

【0023】以下定義及縮寫將用於解譯申請專利範圍及說明書。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獨占式包括。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。

【0024】另外，術語「例示性」在本文中用以意謂「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解釋為比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個，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個，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。

【0025】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裝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。

【0026】出於簡潔起見，本文中可能或可能不詳細描述與進行及使用本發明之態樣有關的習知技術。特定而言，用以實施本文中所描述之各

種技術特徵的計算系統及特定電腦程式之各種態樣為熟知的。因此，為簡潔起見，許多習知實施細節在本文中僅簡要提及或完全省略而不提供熟知系統及/或程序細節。

【0027】關於典型雲端環境之技術挑戰為對VM資料及演算法之潛在不安全且不想要的存取(例如，藉由雲端提供者或雲端管理員)。雲端提供者通常將超管理器程式碼作為主機執行，且將客戶之VM作為客體執行。此超管理器程式碼提供允許多個VM在單一實體機器上執行所需之虛擬化功能。在現有系統中，超管理器(且常常擴展為雲端管理員)可存取客戶之資料及演算法，以應對其必須存取彼資料之有限部分以提供虛擬化功能的情形。一個虛擬化實例為藉由超管理器處置I/O操作。由於針對大量經虛擬化客體虛擬化I/O操作之複雜度，因此需要此處置。當客體發出I/O指令以起始例如I/O請求x之請求時，此虛擬化之第一部分開始。此需要超管理器存取I/O指令之客體運算元(暫存器及儲存器兩者)。回應於此指令，超管理器更新適當的控制區塊結構以追蹤彼請求，且在硬體中起始I/O請求。彼等控制區塊結構可由硬體/韌體使用以在客體經分派時直接向客體呈現相關聯之I/O中斷x。然而，若在等待此I/O請求完成時，客體進入啟用等待狀態，則由於此客體不進行任何工作，因此超管理器可在硬體上分派有工作要進行之另一客體。為進行此操作，超管理器(藉助於硬體/韌體)監視I/O中斷x何時變成待處理，且自虛擬化視角，在適當時向客體呈現此情況且重新分派客體。為進行此操作，超管理器用I/O中斷資訊更新客體預先指定(prefix)頁面且在分派客體I/O中斷處理常式之前更新客體指令位址以指向該處理常式。此需要存取客體儲存器及客體狀態兩者(指令位址)。為了提供此功能及類似功能，超管理器通常具有存取機器中之客體

(VM)狀態及儲存器的無限權限，如本文中所描述，此可能不安全且不受信任，且因此為客戶不希望的。然而，超管理器可為非安全實體且VM為安全實體。在一或多個實例中，安全實體可進一步包括虛擬器或客體。在一或多個實例中，非安全實體可進一步包括在VM中執行個體化之作業系統。在一或多個實例中，主機10亦可被視為非安全實體。因此，本發明之一或多個實施例提供對超管理器之權限的限制且另外促進待由超管理器處置之操作的完成，諸如在I/O操作之狀況下，而無需授予對安全客體設施之存取。

【0028】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。此等服務可包括但不限於記憶體管理、指令仿真及中斷處理。由本發明之一或多個實施例提供的技術解決方案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。舉例而言，對於中斷及例外仿真，超管理器通常讀取及/或寫入至客體之預先指定區(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(計算裝置、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。虛擬機器狀態由在底層主機機器(實體處理器或處理器集合)上執行之超管理器維持。自使用者或軟體資源之視角，虛擬機器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)。

【0029】在目前可用之技術解決方案中，超管理器(例如，IBM®之z/VM®，或基於內核之虛擬機器(KVM)的開放原始碼軟體)藉由發出開始解譯性執行(Start-Interpretive-Execution；SIE)指令來在實體處理單元或主機伺服器上分派新VM虛擬CPU (vCPU)，該指令導致調用SIE進入微碼。SIE指令之運算元為被稱作狀態描述(SD)之控制區塊，其含有客體狀態。在現有實施方案中，此狀態描述駐留於超管理器儲存器中。在SIE進入期間，此客體狀態(包括通用及控制暫存器、客體指令位址及客體程式狀態字(PSW))由微碼載入至硬體中。此允許客體vCPU在實體處理器上執行。當vCPU在硬體上執行時，客體狀態在硬體中維持。在某一時刻，硬體/微碼必須將控制傳回至超管理器。此常常被稱作SIE退出。舉例而言，若此vCPU執行需要超管理器進行仿真之指令或若vCPU時間配量(亦即，為此vCPU在實體處理器上執行所分配的時間)到期，則可能需要此傳回。在SIE退出期間，由於硬體在任何給定時間皆具有資源以僅支援單一vCPU且其現時必須將超管理器狀態載入至硬體中，因此微碼將當前客體狀態儲存於狀態描述中。雖然未分派此vCPU，但其狀態維持於狀態描述中。由於此狀態描述處於超管理器儲存器內，因此超管理器在此類狀況下控制VM之資料，且在一些狀況下，需要此控制來仿真在VM執行之指令。現有超管理器依賴於經由SIE指令使用此介面以分派vCPU。

【0030】然而，為促進安全客體，存在諸如代管節點之電腦伺服器必須在超管理器與安全客體之間提供額外安全性的技術挑戰，使得超管理器無法存取來自VM的資料且因此無法以上文所描述之方式提供服務。

【0031】一些指令(例如，輸入/輸出(I/O)操作)經委派給超管理器。因此，超管理器必須執行彼等指令之解譯，其在許多狀況下可導致客體例

外(程式中斷)，例如在指定無效參數或運算元時。此導致以下情形：其中超管理器僅知曉哪些參數或運算元有效，而不能夠直接向安全客體(亦即，安全VM)呈現例外(程式中斷)，因此提供新介面，其允許藉由超管理器經由安全介面控制件將中斷注入客體。此外，在超管理器代表安全VM監視外部或I/O中斷之一些情況下，其亦必須能夠向VM呈現外部或I/O中斷。

【0032】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實施，則其亦可為安全介面控制件之部分。

【0033】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。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zAarchitecture®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內容脈絡中包括其自身的安全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。術語儲存器與記憶體在本文中可互換地使用。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。

【0034】本發明之一或多個實施例藉由提供新介面來解決此等技術挑戰，該新介面允許藉由硬體或韌體將中斷注入VM。另外，本發明之一或多個實施例提供此額外安全性，同時仍允許超管理器將服務提供至VM。此藉由將存取安全客體設施且通常由超管理器代表客體進行之功能或功能之部分併入至新「安全介面控制件」中來實現。由本發明之一或多個實施例使用的注入方法可應用於超管理器可能需要注入之任何中斷類型。在一或多個實例中，此功能性可藉由使用微碼及/或其他硬體模組來提供，且在本說明書中，統稱為由安全介面控制件提供。微碼為充當處理器硬體之擴展的受信任韌體。因此，本發明之一或多個實施例促進超管理器將中斷安全且可靠地注入安全客體，且經由安全介面控制件傳達已發生必須由此客體處置之中斷條件。

【0035】現對背景技術進行簡要描述，此後描述由本發明之一或多個實施例用於藉由超管理器將中斷及/或例外注入安全VM之特定特徵。預先應理解，儘管本發明包括關於雲端計算之詳細描述，但本文中所敘述之教示的實施不限於雲端計算環境。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計算環境來實施。

【0036】雲端計算為用於使得能夠對可組態計算資源(例如，網路、網路頻寬、伺服器、處理、記憶體、儲存器、應用程式、虛擬機器及服務)之共用集區進行便利之按需網路存取的服務遞送之模型，可組態計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。

【0037】特性如下：

【0038】隨選自助服務：雲端客戶可視需要自動地單向佈建計算能力(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。

【0039】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。

【0040】資源集用：提供者之計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。

【0041】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。

【0042】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。

【0043】服務模型如下：

【0044】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底層雲端基礎架構，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。

【0045】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底層雲端基礎架構，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。

【0046】基礎架構即服務(IaaS)：提供給客戶之能力係佈建處理、儲存、網絡及其他基礎計算資源，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底層雲端基礎架構，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)。

【0047】部署模型如下：

【0048】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。

【0049】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。

【0050】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。

【0051】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。

【0052】藉由集中於無國界、低耦合、模組化及語義互操作性對雲端計算環境進行服務定向。雲端計算之關鍵為包括互連節點之網路的基礎架構。

【0053】現參看圖1，描繪說明性雲端計算環境50。如所展示，雲端計算環境50包含一或多個雲端計算節點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的本端計算裝置可與該一或多個雲端計算節點通信。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)。此允許雲端計算環境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計算裝置上維持資源。應理解，圖1中所展示之計算裝置54A至54N之類型意欲僅為說明性的，且計算節點10及雲端計算環境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。

【0054】現參看圖2，展示藉由雲端計算環境50 (圖1)所提供之功能

抽象層之集合。事先應理解，圖2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：

【0055】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。

【0056】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：虛擬機器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。

【0057】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提供計算資源及用以執行雲端計算環境內之任務之其他資源的動態採購。當在雲端計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，此等資源可包含應用程式軟體授權。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計算環境之存取。服務等級管理84提供雲端計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提供雲端計算資源之預先配置及採購，針對雲端計算資源之未來要求係根據SLA來預期。

【0058】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計算環境。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；及原始程式碼版本設定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。

【0059】圖3說明根據本發明之一或多個實施例的實例代管節點10。代管節點10與一或多個用戶端裝置20A至20C直接通信或經由網路165間接通信。代管節點10可為雲端計算提供者之資料中心或主機伺服器。代管節點10執行超管理器12，其促進部署一或多個虛擬機器15 (15A至15N)。代管節點10進一步包括硬體層13，其包括促進超管理器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微碼，包括安全介面控制件11。在現有技術解決方案中，在超管理器12與硬體/微碼13之間、硬體/微碼13與一或多個VM 15之間、超管理器12與一或多個VM 15之間及經由硬體/微碼13在超管理器12至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，且替代地經由安全介面控制件11提供通信。

【0060】舉例而言，代管節點10可促進用戶端裝置20A部署虛擬機器15A至15N中之一或多者。可回應於來自相異用戶端裝置20A至20C之各別請求而部署虛擬機器15A至15N。舉例而言，虛擬機器15A可由用戶端裝置20A部署，虛擬機器15B可由用戶端裝置20B部署且虛擬機器15C可由用戶端裝置20C部署。代管節點10亦可促進用戶端佈建實體伺服器(不作為虛擬機器執行)。本文中所描述之實例將代管節點10中之資源的佈建作為虛擬機器之部分來體現，然而，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。

【0061】在一實例中，用戶端裝置20A至20C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，且代管節點10可作為實體之私用雲端操作。在此狀況下，代管節點10僅代管由屬於該實體

之用戶端裝置20A至20C部署的虛擬機器15A至15N。在另一實例中，用戶端裝置20A至20C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，代管節點10可作為代管來自不同實體之虛擬機器的公用雲端操作。舉例而言，可按遮蔽方式部署虛擬機器15A至15N，其中虛擬機器15A不便於存取虛擬機器15B。舉例而言，代管節點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)特徵來遮蔽虛擬機器15A至15N。諸如PR/SM LPAR之此等特徵提供分割區之間的隔離，因此促進代管節點10在不同邏輯分割區中部署同一實體代管節點10上之不同實體的兩個或多於兩個虛擬機器15A至15N。

【0062】來自用戶端裝置20A至20C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、伺服器電腦或請求代管節點10之超管理器12部署虛擬機器的任何其他通信設備。用戶端裝置20A可經由網路165或直接發送供超管理器接收之請求。來自虛擬機器15A至15N之虛擬機器15A為超管理器12回應於來自用戶端裝置20A至20C中之用戶端裝置20A的請求而部署的虛擬機器映像。超管理器12為虛擬機器監視器(VMM)，其可為建立及執行虛擬機器之軟體、韌體或硬體。超管理器12促進虛擬機器15A使用代管節點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 VM SERVER™、CITRIX XENSERVER™、VMWARE ESX™、MICROSOFT HYPER-V™、KVM或任何其他超管理器。超管理器12可為直接在代管節點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。

【0063】圖4說明根據本發明之一或多個實施例的實例代管節點之組件。代管節點10可為電腦，諸如伺服器電腦、桌上型電腦、平板電腦、智慧型手機或執行超管理器12之任何其他電腦，該超管理器又部署虛擬機器15A至15N。代管節點10包括組件，其包括諸如電子電路系統之硬體。除其他組件以外，代管節點10亦包括處理器105、耦接至記憶體控制器115之記憶體110，及一或多個輸入裝置145及/或輸出裝置140，諸如經由本端I/O控制器135通信耦接之周邊或控制裝置。此等裝置140及145可包括例如電池感測器、位置感測器(高度計40、加速度計42、GPS 44)、指示器/識別燈及其類似者。諸如習知鍵盤150及滑鼠155之輸入裝置可耦接至I/O控制器135。I/O控制器135可為例如一或多個匯流排或其他有線或無線連接，如此項技術中已知的。I/O控制器135可具有用以實現通信之額外元件，諸如控制器、緩衝器(快取記憶體)、驅動器、中繼器及接收器，為簡單起見省略額外元件。

【0064】I/O裝置140、145可進一步包括傳達輸入及輸出兩者的裝置，例如磁碟及磁帶儲存器、網路介面卡(NIC)或調變器/解調變器(用於存取其他檔案、裝置、系統或網路)、射頻(RF)或其他收發器、電話介面、橋接器、路由器及其類似者。

【0065】處理器105為用於執行硬體指令或軟體(特定而言，儲存於記憶體110中之彼等指令或軟體)之硬體裝置。處理器105可為常規製造或市售之處理器、中央處理單元(CPU)、與代管節點10相關聯之若干處理器當中的輔助處理器、基於半導體之微處理器(呈微晶片或晶片組形式)、巨集處理器或用於執行指令之其他裝置。處理器105包括快取記憶體170，其可包括但不限於用以加速可執行指令提取之指令快取記憶體、用以加速

資料提取及儲存之資料快取記憶體及用以加速可執行指令及資料兩者之虛擬至實體位址轉譯的轉譯後備緩衝器(TLB)。快取記憶體170可組織為更多快取記憶體層級(L1、L2等)之階層。

【0066】記憶體110可包括揮發性記憶體元件(例如，隨機存取記憶體(RAM)，諸如DRAM、SRAM、SDRAM等))及非揮發性記憶體元件(例如，快閃記憶體、ROM、可抹除可程式化唯讀記憶體(EPROM)、電可抹除可程式化唯讀記憶體(EEPROM)、可程式化唯讀記憶體(PROM)、磁帶、光碟唯讀記憶體(CD-ROM)、磁碟、磁片 、卡匣、盒或其類似者等)中之一者或組合。此外，記憶體110可併有電子、磁性、光學及/或其他類型之儲存媒體。應注意，記憶體110可具有分散式架構，其中各個組件彼此遠離而定位，但可由處理器105存取。

【0067】記憶體110中之指令可包括一或多個分開程式，該程式中之每一者包含用於實施邏輯功能之可執行指令的有序清單。在圖2之實例中，記憶體110中之指令包括執行超管理器12之合適作業系統(OS)。作業系統可控制其他電腦程式之執行，且提供排程、輸入輸出控制、檔案及資料管理、記憶體管理以及通信控制及相關服務。在諸如z System™之實例中，代管節點10之製造商可提供超管理器12。在結構不同於z System之結構的系統之狀況下，其中超管理器12不由硬體製造商提供，所提供之雲端計算可使用諸如來自VMWARE™、KVM或其他超管理器提供者之超管理器12。在一實例中，實體代管節點10之管理員不能修改超管理器12，除了需要修改以便應用由製造商提供之服務時以外。舉例而言，超管理器12可提供為代管節點10之「已獲授權內部碼(LIC)」及/或微碼的部分。

【0068】包括例如用於處理器105之指令或其他可擷取資訊的額外資

料可儲存於儲存器120中，該儲存器可為諸如硬碟機或固態磁碟機之儲存裝置。儲存於記憶體110或儲存器120中之指令可包括使得處理器能夠執行本發明之系統及方法之一或多個態樣的彼等指令。

【0069】代管節點10可進一步包括耦接至使用者介面或顯示器130之顯示控制器125。在一些實施例中，顯示器130可為LCD螢幕。在其他實施例中，顯示器130可包括複數個LED狀態燈。在一些實施例中，代管節點10可進一步包括用於耦接至網路165之網路介面160。網路165可為用於經由寬頻連接在代管節點10與外部伺服器、用戶端及其類似者之間進行通信的基於IP之網路。在一實施例中，網路165可為衛星網路。網路165在代管節點10與外部系統之間傳輸及接收資料。在一些實施例中，網路165可為藉由服務提供者進行系統管理之經管理IP網路。網路165可以無線方式實施，例如使用無線協定及技術，諸如WiFi、WiMax、衛星或任何其他協定及技術。網路165亦可為封包交換式網路，諸如區域網路、廣域網路、都會區域網路、網際網路或其他類似類型之網路環境。網路165可為固定無線網路、無線區域網路(LAN)、無線廣域網路(WAN)、個人區域網路(PAN)、虛擬私人網路(VPN)、企業內部網路或其他合適網路系統，且可包括用於接收及傳輸信號之裝備。

【0070】用戶端裝置20A可請求超管理器12部署可存取代管節點10之特定硬體及/或軟體組件的對應虛擬機器15A。舉例而言，用戶端裝置20A可請求虛擬機器15A存取預定數目個處理器、預定量之揮發性記憶體(諸如，隨機存取記憶體(RAM))、預定量之非揮發性記憶體(諸如，儲存空間)或任何其他硬體組件。替代地或另外，用戶端裝置20A可請求虛擬機器15A存取諸如由對應唯一識別符識別之電子電路系統的特定硬體組

件。舉例而言，用戶端裝置20A可請求虛擬機器15A存取特定類型之處理器、共處理器、網路卡或任何其他晶片或電子電路系統。在一實例中，用戶端裝置20A可使用由電子電路系統之製造商提供的識別符來識別電子電路系統。在一實例中，該識別符可結合版本識別符來使用。替代地或另外，用戶端裝置20A可請求虛擬機器15A存取特定軟體組件，諸如作業系統、應用程式、基本輸入/輸出系統(BIOS)、開機映像或任何其他軟體組件。所請求之軟體組件可包括代管節點10之硬體組件中的韌體及嵌入程式。用戶端裝置20A可使用由各別軟體組件之開發者/製造商提供的各別唯一識別符識來別所請求之軟體組件。在一實例中，該等識別符可結合軟體組件之版本識別符來使用。

【0071】圖5說明根據本發明之一或多個實施例的用於超管理器經由安全介面控制件將中斷之通知提供至安全VM的實例方法之流程圖。該方法包括藉由執行開始解譯性執行(SIE)指令來分派安全VM 15A vCPU及將處理器105及其他計算資源分配給安全VM 15A。SIE指令將處理器105置於定義於記憶體110中之控制區塊中的仿真狀態中，該仿真狀態通常被稱作狀態描述符(SD)。通常，SIE指令具有定址SD之一個運算元。亦即，SD含有定義待在處理器105上仿真之硬體狀態的欄位，如可由用戶端裝置20為安全VM 15A所請求的。在一或多個實例中，處理器105可被視為虛擬處理器，此係因為處理器105可應起始安全VM 15A之用戶端20的請求而受到指令以仿真另一處理器架構之行為。

【0072】根據本發明之一或多個實施例，SD欄位包括：(1)含有絕對記憶體位址之起源欄位，安全VM (亦即，客體)之真實位址零指派於該絕對記憶體位址處，該絕對記憶體位址定位客體之頁面零；(2)用於安全VM

15A之當前程式狀態字(PSW)的欄位；(3)用於安全VM 15A之通用暫存器(GR)及控制暫存器(CR)的儲存區；及(4)用於其他客體狀態之其他雜項欄位。

【0073】該方法包括在505處，主機10判定應注入中斷且建立彼中斷使得可將其注入安全VM 15A。中斷可為I/O外部中斷或任何其他類型之中斷。如早前所提及，超管理器12不可直接存取記憶體、暫存器或安全VM 15A之任何其他資料，從而藉由在重新分派之前將客體中斷資訊直接儲存至VM預先指定頁面中及將中斷新PSW載入至當前VM狀態(亦即，SD)中來防止超管理器12將中斷直接注入安全VM 15A，此直接注入係如可在現有技術解決方案中所進行的。

【0074】在需要時，在510處，主機10撤消分派安全VM 15A之待接收中斷的虛擬處理器。另外，在515處，超管理器12將待注入之中斷及與中斷相關聯之一或多個參數新增至虛擬處理器之SD中。在一或多個實例中，此新增可替代地由超管理器12以典型方式發出注入指令來執行，該注入指令由安全介面控制件實施。在識別出由超管理器12請求之指令後，安全介面控制件可將中斷條件注入安全VM 15A抑或將中斷資訊安全地新增至相關聯之SD中以供在下一次分派時進行處理。在520處，超管理器12進一步藉由重新分派安全虛擬機器來重新繼續指派給安全VM 15A之處理器105的操作。

【0075】此時，當超管理器12為安全VM 15A重新分派虛擬處理器時，在SIE進入以重新分派此vCPU期間，在525處，安全介面控制件11檢查所注入中斷及其參數是否有效且針對所注入之中斷的類型是否啟用處理器105。當安全VM 15A經起始時，用戶端20或預設設定可提供安全VM

15A可接收之中斷的清單。在一或多個實例中，例如出於安全性原因，可限制例如I/O中斷之特定類型的中斷到達安全VM 15A。此外，可限制與I/O中斷相關聯之一或多種類型的參數到達安全VM 15A。舉例而言，可限制包括文字、記憶體指標或待由安全VM 15A執行之指令碼的參數或任何其他類型之參數。在一或多個實例中，安全介面控制件11可存取針對安全VM 15A而限制(或允許)之中斷類型及/或參數類型的清單。舉例而言，此清單可儲存於分配給安全介面控制件11之記憶體的安全部分中。在一或多個實例中，不同清單可應用於不同安全VM。

【0076】若中斷類型及參數類型之驗證成功，則在530及535處，安全介面控制件11將中斷注入安全VM 15A且安全VM 15A之執行重新繼續。安全介面控制件11藉由將關於中斷之資訊及對應參數新增至安全VM 15A之記憶體(預先指定頁面)及暫存器來注入中斷。另外，在535處，安全VM 15A執行重新繼續，其中引發中斷。

【0077】在由安全介面控制件11驗證到中斷及/或參數之不當值的狀況下，在540處，安全介面控制件11例如經由有效性攔截向超管理器12指示錯誤，且安全VM 15A之執行不重新繼續。在接收到有效性攔截後，安全介面控制件11或超管理器12可引發指示可能安全漏洞之警報，如本文中所描述。

【0078】因此，當超管理器12不可直接存取與安全VM 15A相關聯之記憶體/暫存器空間時，上文所描述之方法促進超管理器12將中斷注入安全VM 15A。

【0079】另外，本發明之一或多個實施例促進安全VM 15A在超管理器12中引發中斷或程式例外。

【0080】當安全VM 15A執行程式指令例如作為由在安全VM 15A中執行之應用程式所執行的操作之部分時且在程式指令需要攔截於超管理器12之情況下，存在技術挑戰。作為彼客體程式指令之仿真的部分，超管理器12判定存在與程式指令相關聯之客體例外，但不能存取與安全VM 15A相關聯之向VM呈現例外所必要的任何暫存器/記憶體。本文中所描述之本發明之一或多個實施例促進將例外注入VM 15A。

【0081】圖6說明根據本發明之一或多個實施例的用於超管理器回應於客體指令之仿真而在安全VM中引發例外的實例方法之流程圖。該方法包括在605處，安全VM 15A發出需要超管理器介入之指令。舉例而言，該指令可為對主機10之I/O通道的請求、針對非同步中斷啟用之指令或需要超管理器12服務之任何其他此類指令。

【0082】實情為，在本發明之一或多個實施例中，在610處，安全介面控制件11例如經由狀態描述符向超管理器12呈現指令及其他有限客體狀態資訊。在一或多個實例中，硬體或安全介面控制件識別出，由安全VM 15A執行之指令需要超管理器介入，且作為回應，攔截指令。亦即，其停止由VM執行指令且將當前客體狀態儲存於安全儲存器中。安全介面控制件11例如藉由將資訊複製至狀態描述符中來向超管理器12安全地公開指令仿真所需之客體狀態的部分(諸如，運算元及作業碼)，且開始執行處置客體攔截之超管理器程式碼。應注意，因此傳遞該指令以供超管理器12在無來自安全VM 15A之任何內容脈絡的情況下執行。安全介面控制件11基於待以此方式攔截之預定指令(指令類型)之清單而識別待攔截之指令。在615處，超管理器12仿真指令。

【0083】在620處，超管理器12判定在指令之仿真期間是否遇到例

外。若未遇到例外，則在625處，超管理器12重新繼續安全VM 15A之執行。因此，在630處，安全VM 15A根據與安全VM 15A相關聯之狀態描述符使用客體狀態來重新繼續操作。

【0084】實情為，若在客體指令之仿真期間遇到例外，則在635處，超管理器12判定將向安全VM 15A呈現哪一例外。因此，超管理器12將關於待報告給安全VM 15A之例外的資訊包括於例如狀態描述符中。該資訊可包括待報告之例外的識別符連同對應於待報告之例外的一或多個參數。在一或多個實例中，所報告例外可不同於在指令之執行期間實際上遇到的例外。在完成狀態描述符更新後，在640處，超管理器12使用SIE指令重新分派安全VM 15A。替代地，超管理器12可經由指令調用安全介面控制件11，以指示在下一次分派時應向安全VM 15A呈現例外，且安全介面控制件可對狀態描述符或類似控制區塊進行適當更新。

【0085】在SIE進入期間，安全介面控制件11檢查安全VM 15A之狀態描述符且識別由超管理器12新增之例外資訊。在645處，安全介面控制件11判定是否將例外傳遞至安全VM 15A。安全介面控制件11基於允許傳遞至安全VM 15A之例外的清單而進行判定。例外之清單可特定於安全VM 15A，且可為預定清單或由起始安全VM 15A之用戶端提供的清單，及其類似者。

【0086】此外，在一或多個實例中，安全介面控制件11基於傳遞至超管理器12以供執行之指令而檢查傳遞至安全VM 15A之例外是否適當。舉例而言，安全介面控制件11可具有可攔截於超管理器12之客體指令的清單，且對於每一指令，具有可由超管理器12傳遞回至安全VM 15A之一或多個例外的集合。若所傳遞之例外並非來自對應於由安全VM 15A執行之

指令的例外之集合，則在650處，安全介面控制件11藉由引發警報經由例如有效性攔截來指示錯誤，如本文中所描述。

【0087】另外，在645處，安全介面控制件11藉由檢查與例外一起傳遞之參數來判定傳遞至安全VM 15A之例外的適當性。若該等參數不匹配一或多個所允許之參數類型，則在650處，安全介面控制件11引發錯誤條件或警報。

【0088】實情為，若藉由超管理器12傳遞至安全VM 15A之例外及參數有效，則在655處，安全介面控制件11將例外注入安全VM 15A。舉例而言，將例外注入安全VM 15A包括改變安全VM 15A之一或多個暫存器值及記憶體(低核心)值，其向安全VM 15A之作業系統指示已發生例外。在630處，進一步重新繼續安全VM執行。重新繼續包括安全VM 15A處置因為指令在被攔截之前執行而已引發的例外。

【0089】因此，本發明之一或多個實施例促進藉由超管理器12將例外注入安全VM 15A。

【0090】根據本發明之一或多個實施例，電腦伺服器可代管主機安全VM，該等安全VM禁止超管理器存取與其相關聯之記憶體、暫存器及其他資料，而不必改變超管理器及/或安全VM程式碼/架構以將中斷注入超管理器及/或將例外注入安全VM。實情為，根據本發明之一或多個實施例，包括微碼之安全介面控制件使用狀態描述符及儲存器/記憶體之安全部分來傳達中斷/例外資訊，從而促進此類注入。此外，安全介面控制件對中斷/例外資訊執行有效性檢查以防止在安全VM與超管理器之間傳遞惡意資訊，且繼續以此方式維持安全VM之安全性。

【0091】本發明之一或多個實施例植根於電腦技術，特定而言為代

管電腦伺服器之虛擬機器。另外，本發明之一或多個實施例藉由促進代管電腦伺服器代管安全VM來促進改良計算技術本身，特定而言為代管電腦伺服器之虛擬機器的操作，其中甚至禁止超管理器存取與安全VM相關聯之記憶體、暫存器及其他此類資料。此外，本發明之一或多個實施例藉由使用硬體層及/或包括微碼之安全介面控制件來提供朝向改良代管計算伺服器之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計算伺服器代管之VM的安全性。硬體層提供輕型中間操作以促進安全性，而不會添加注入中斷及/或例外之大量額外負荷，如本文中所描述。

【0092】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。

【0093】電腦可讀儲存媒體可為有形裝置，其可持留及儲存指令以用於指令執行裝置使用。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。

【0094】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計算/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。每一計算/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計算/處理裝置內之電腦可讀儲存媒體中。

【0095】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。

【0096】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。

【0097】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。

【0098】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。

【0099】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。

【0100】本發明之各種實施例之描述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】

【0101】

10: 主機/雲端計算節點/代管節點

11: 安全介面控制件

12: 超管理器

13: 硬體層/硬體/微碼

15: 虛擬機器

15A: 安全虛擬機器

15B: 虛擬機器

15C: 虛擬機器

15D: 虛擬機器

15N: 虛擬機器

20A: 用戶端裝置

20B: 用戶端裝置

20C: 用戶端裝置

40: 高度計

42: 加速度計

44: GPS

50: 雲端計算環境

54A: 個人數位助理(PDA)或蜂巢式電話/計算裝置

54B: 桌上型電腦/計算裝置

54C: 膝上型電腦/計算裝置

54N: 汽車電腦系統/計算裝置

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: 虛擬機器

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: 原始程式碼版本設定

105: 處理器

110: 記憶體

115: 記憶體控制器

120: 儲存器

125: 顯示控制器

130: 顯示器

135: 本端I/O控制器

140: 輸出裝置/I/O裝置

145: 輸入裝置/I/O裝置

150: 鍵盤

155: 滑鼠

160: 網路介面

165: 網路

170: 快取記憶體

【發明申請專利範圍】

【請求項1】

一種電腦實施方法，其包含：

藉由在一主機伺服器上執行之一非安全實體起始一安全實體，該非安全實體被禁止直接存取該安全實體之任何資料；及

將由該主機伺服器或由該非安全實體產生之一中斷注入該安全實體，該注入包含：

藉由該非安全實體將關於該中斷之資訊新增至與該安全實體相關聯之非安全儲存器之一部分中；及

藉由該主機伺服器之一安全介面控制件將該中斷注入該安全實體。

【請求項2】

如請求項1之電腦實施方法，其中該非安全實體為一超管理器，且該安全實體為一安全虛擬機器。

【請求項3】

如請求項1之電腦實施方法，其中該安全實體為一容器且該非安全實體為一作業系統。

【請求項4】

如請求項1之電腦實施方法，其進一步包含：

在該注入之前，藉由該安全介面控制件判定是否准許將該中斷注入該安全實體，其中該注入係基於判定准許將該中斷注入該安全實體而執行。

【請求項5】

如請求項4之電腦實施方法，其中該安全介面控制件基於針對該安全實體之准許中斷的一預定清單而判定准許將該中斷注入該安全實體。

【請求項6】

如請求項5之電腦實施方法，其中准許中斷之該清單特定於該安全實體。

【請求項7】

如請求項4之電腦實施方法，其中該方法進一步包括回應於判定不准許將該中斷注入該安全實體而藉由該安全介面控制件向該非安全實體指示一錯誤。

【請求項8】

如請求項1之電腦實施方法，其進一步包含在藉由該非安全實體注入之前，撤消分派與該安全實體相關聯之一虛擬處理器。

【請求項9】

如請求項1之電腦實施方法，其進一步包含：在該注入之前，藉由該安全介面控制件判定是否准許將該中斷及一或多個參數注入該安全實體，其中該注入係基於判定准許將該中斷及該一或多個參數注入該安全實體而執行。

【請求項10】

如請求項1之電腦實施方法，其中新增關於該中斷之該資訊包含以下操作中之一者：

藉由該非安全實體將關於該中斷之該資訊儲存至與該安全實體相關聯之一狀態描述符中；及

藉由該非安全實體發出一指令以用於一安全控制介面將關於該中斷

之該資訊儲存至與該安全實體相關聯之一狀態描述符中。

【請求項11】

一種電腦系統，其包含：

一記憶體；

一安全介面控制件；及

一處理單元，其與該記憶體及該安全介面控制件耦接，該處理單元經組態以執行代管一或多個安全實體之一非安全實體，該非安全實體被禁止直接存取一安全實體之任何資料，且其中將由該非安全實體產生之一中斷注入該等安全實體的一方法包含：

藉由該非安全實體將關於該中斷之資訊新增至與該安全實體相關聯之非安全儲存器之一部分中；及

藉由該安全介面控制件將該中斷注入該安全實體。

【請求項12】

如請求項11之系統，其中該方法進一步包含：

在藉由該非安全實體注入之前，撤消分派與該安全實體相關聯之一處理器。

【請求項13】

如請求項12之系統，其中在藉由該非安全實體新增關於該中斷之該資訊之後，重新分派一虛擬處理器以重新繼續該安全實體之操作。

【請求項14】

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執行時使該處理單元執行一方法，該方法包含：

藉由在一主機伺服器上執行之一非安全實體起始一安全實體，該非安全實體被禁止直接存取該安全實體之任何資料；及

藉由該非安全實體將由該主機伺服器產生之一中斷注入該安全實體，該注入包含：

藉由該非安全實體將關於該中斷之資訊新增至與該安全實體相關聯之非安全儲存器之一部分中；

藉由該非安全實體重新繼續與該安全實體相關聯之一處理器以重新繼續該安全實體之操作；及

藉由一安全介面控制件將該中斷注入該安全實體。

【請求項15】

如請求項14之電腦程式產品，其中該方法進一步包含：

在藉由該非安全實體注入之前，撤消分派與該安全實體相關聯之該處理器。

【請求項16】

如請求項15之電腦程式產品，其中該安全介面控制件基於針對該安全實體之准許中斷的一預定清單而判定准許將該中斷注入該安全實體。

【請求項17】

如請求項15之電腦程式產品，其中該方法進一步包含：

在藉由該非安全實體新增關於該中斷之該資訊之後，重新分派一虛擬處理器以重新繼續該安全實體之操作。

【請求項18】

如請求項14之電腦程式產品，其中關於該中斷之該資訊包含待注入之該中斷的一識別符及與該中斷相關聯之一或多個參數。

【請求項19】

一種電腦實施方法，其包含：

藉由在一主機伺服器上之一非安全實體上執行的一安全實體執行產生一程式例外之一指令，該程式例外待轉遞至該非安全實體，該非安全實體被禁止直接存取該安全實體之任何資料；及

藉由一安全介面控制件向該非安全實體呈現該指令；

藉由該非安全實體執行該指令；及

將來自該非安全實體之該程式例外注入該安全實體，該注入包含：

基於由該指令之仿真引發的該程式例外，藉由該非安全實體將關於該程式例外之資訊新增至與該安全實體相關聯之非安全儲存器之一部分中；及

藉由該非安全實體重新繼續與該安全實體相關聯之一處理器以重新繼續該安全實體之操作。

【請求項20】

如請求項19之電腦實施方法，其進一步包含：

在藉由該安全介面控制件向該非安全實體呈現該指令之前，撤消分派與該安全實體相關聯之該處理器。

【請求項21】

如請求項20之電腦實施方法，在藉由該非安全實體新增關於該程式例外之該資訊之後，重新分派一虛擬處理器以重新繼續該安全實體之操作。

【請求項22】

如請求項19之電腦實施方法，其中關於該程式例外之該資訊包含待

注入之該程式例外的一識別符及與該程式例外相關聯之一或多個參數。

【請求項23】

一種電腦系統，其包含：

一記憶體；

一安全介面控制件；及

一處理單元，其與該記憶體及該安全介面控制件耦接，該處理單元經組態以執行代管複數個安全實體之一非安全實體，該非安全實體被禁止直接存取一安全實體之任何資料，且其中該系統經組態以執行用以將來自該非安全實體之一程式例外注入該等安全實體之一方法，該方法包含：

藉由一安全介面控制件向該非安全實體呈現一指令；

藉由該非安全實體執行該指令；及

將來自該非安全實體之該程式例外注入該安全實體，該注入包含：

基於由該指令之仿真引發的該程式例外，藉由該非安全實體將關於該程式例外之資訊新增至與該安全實體相關聯之非安全儲存器之一部分中；及

藉由該非安全實體重新繼續與該安全實體相關聯之一處理器以重新繼續該安全實體之操作。

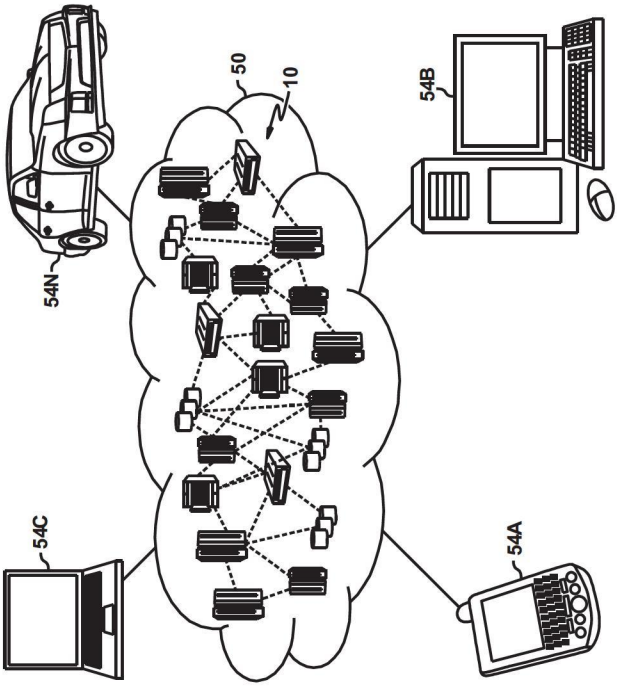
【請求項24】

如請求項23之系統，其中該方法進一步包含在藉由該安全介面控制件向該非安全實體呈現該指令之前，撤消分派與該安全實體相關聯之該處理器。

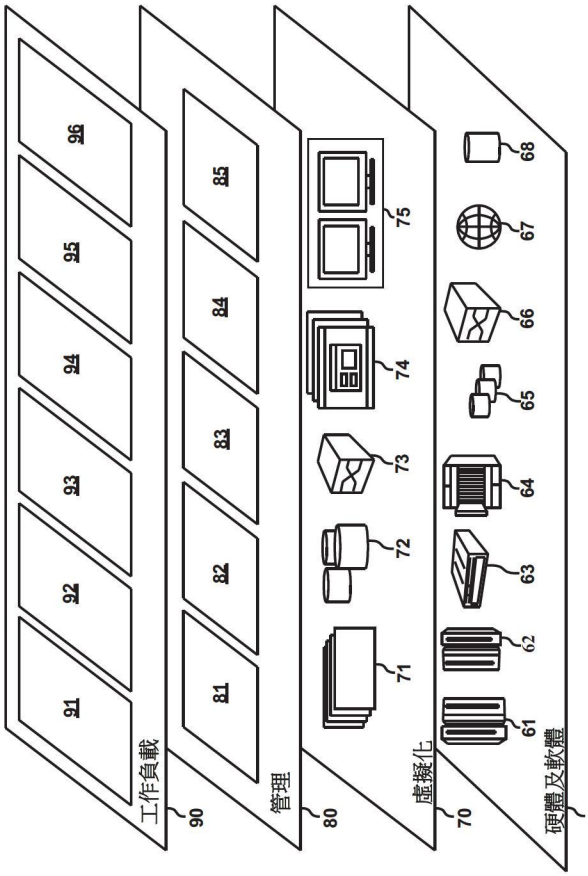
【請求項25】

如請求項23之系統，其中該方法進一步包含在藉由該非安全實體新增關於該程式例外之該資訊之後，重新分派一虛擬處理器以重新繼續該安全實體之操作。

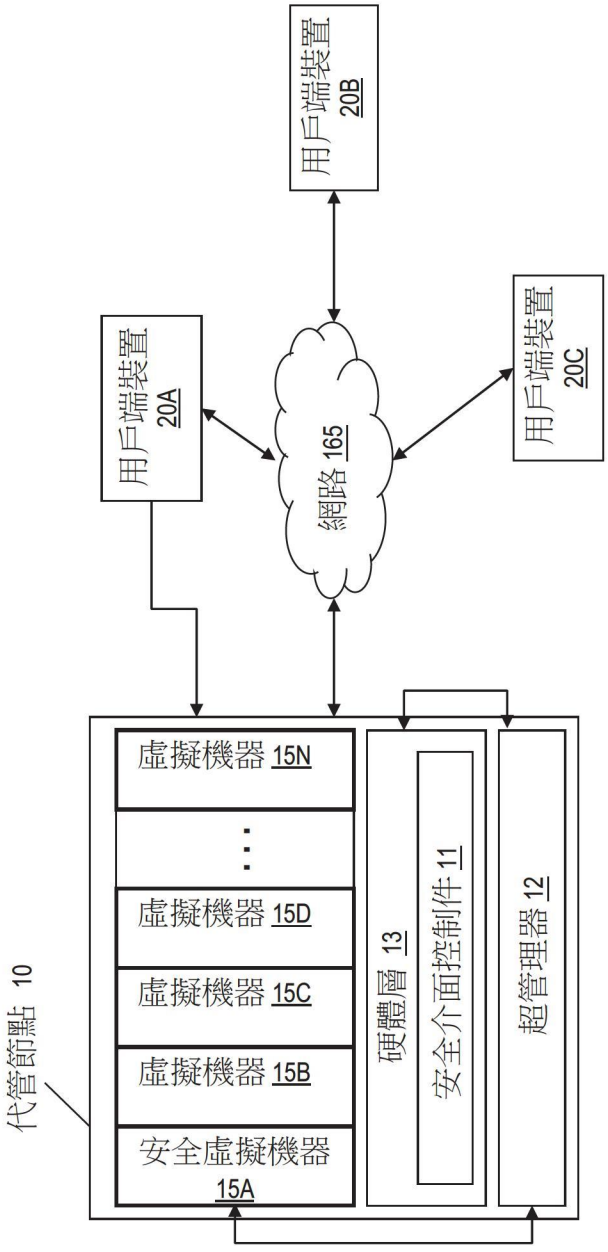
【發明圖式】



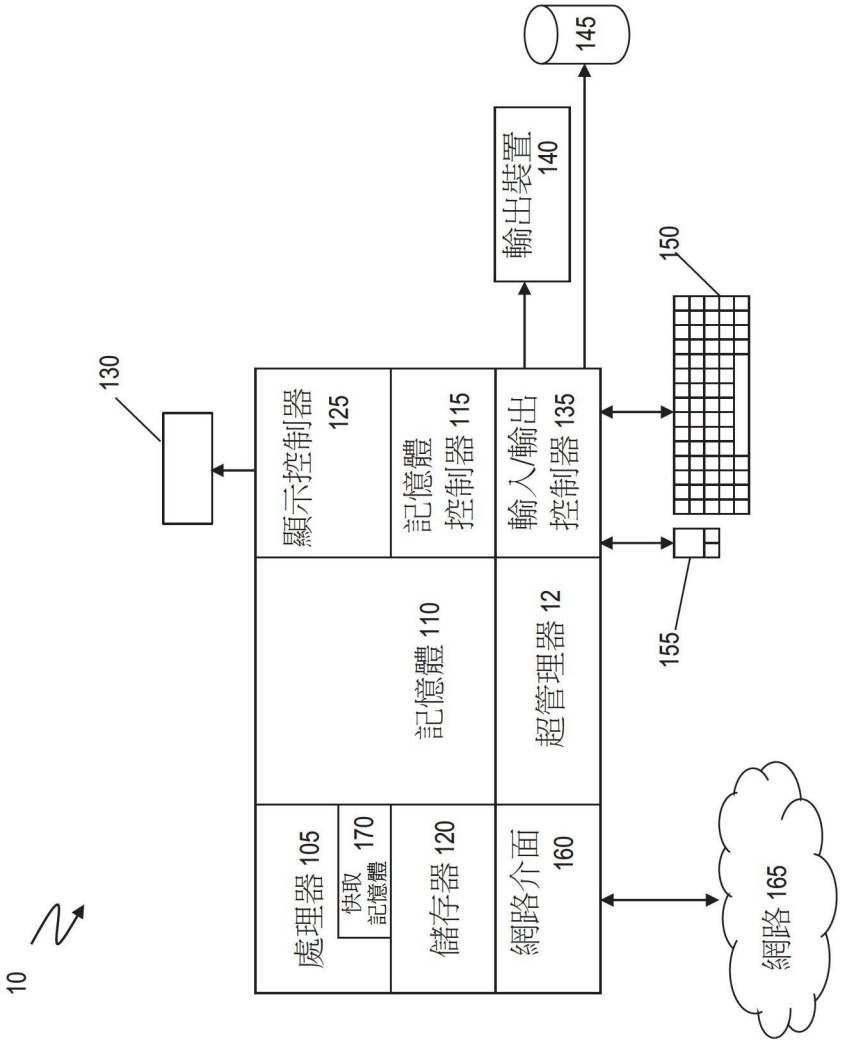
【圖1】


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

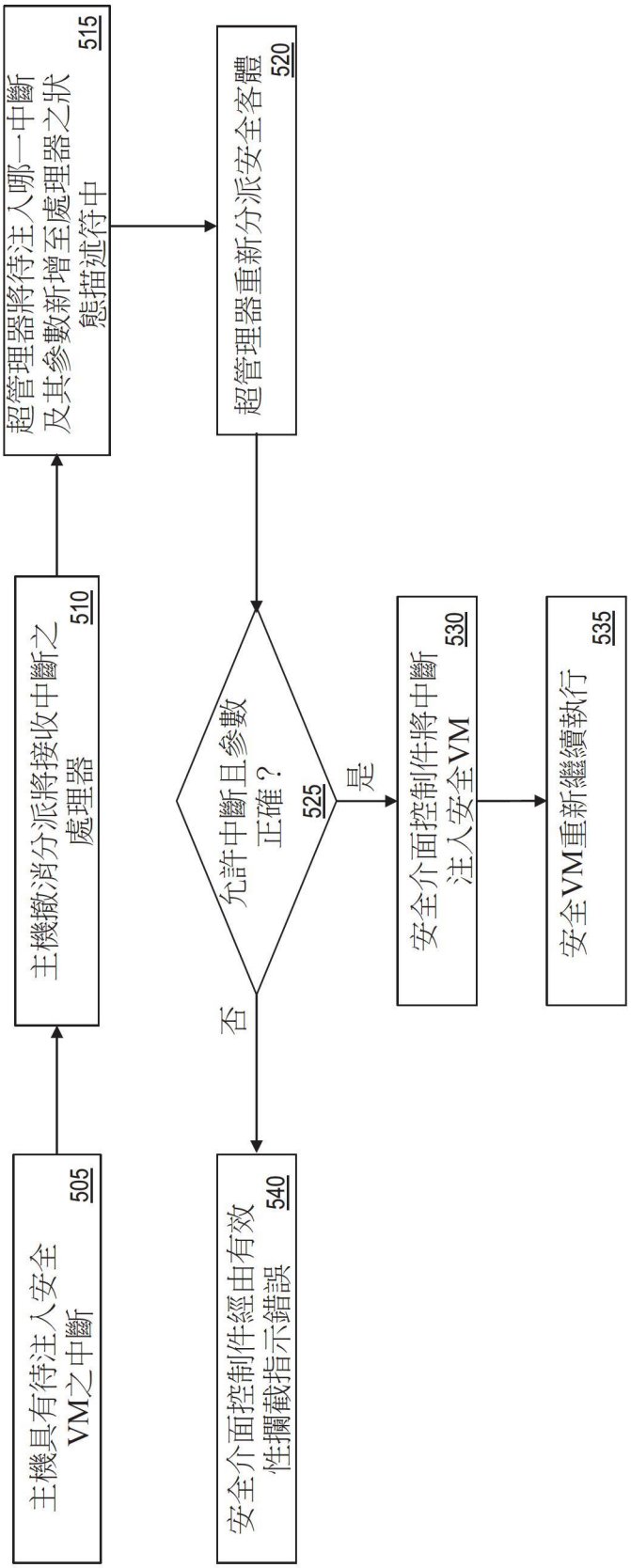
【圖2】


用戶端裝置 20B
用戶端裝置 20A
網路 165
用戶端裝置 20C
虛擬機器 15N
虛擬機器 15D
虛擬機器 15C
虛擬機器 15B
安全虛擬機器 15A
硬體層 13
安全介面控制件 11
超管理器 12
代管節點 10

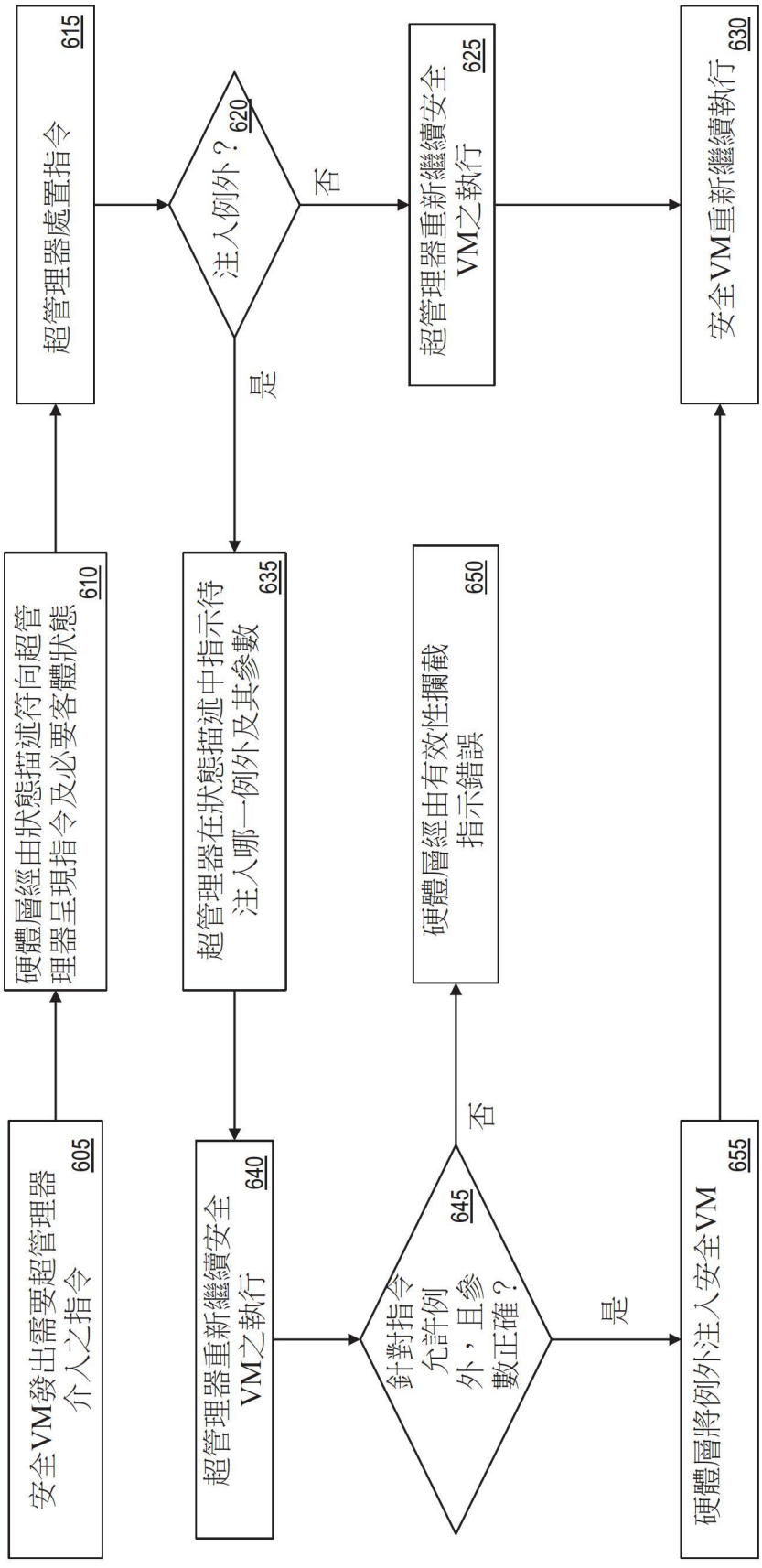
【圖3】


10
處理器 105
快取記憶體 170
儲存器 120
記憶體 110
網路介面 160
超管理器 12
顯示控制器 125
記憶體控制器 115
輸入/輸出控制器 135
130
輸出裝置 140
145
150
155
網路 165

【圖4】


主機具有待注入安全VM之中斷
505
主機撤消分派將接收中斷之處理器
510
超管理器將待注入哪一中斷及其參數新增至處理器之狀態描述符中
515
超管理器重新分派安全客體
520
允許中斷且參數正確？
525
否
是
安全介面控制件經由有效性攔截指示錯誤
540
安全介面控制件將中斷注入安全VM
530
安全VM重新繼續執行
535

【圖5】


安全VM發出需要超管理器介入之指令
605
硬體層經由狀態描述符向超管理器呈現指令及必要客體狀態
610
超管理器處置指令
615
注入例外？
620
否
超管理器重新繼續安全VM之執行
625
安全VM重新繼續執行
630
是
超管理器在狀態描述中指示待注入哪一例外及其參數
635
超管理器重新繼續安全VM之執行
640
針對指令允許例外，且參數正確？
645
否
硬體層經由有效性攔截指示錯誤
650
是
硬體層將例外注入安全VM
655

【圖6】