I451245

(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 I451245 B**

(45)公告日： 中華民國 103 (2014) 年 09 月 01 日

(21)申請案號：100133035 (22)申請日： 中華民國 100 (2011) 年 09 月 14 日

(51)Int. Cl.： *G06F11/34 (2006.01)* *G06F9/455 (2006.01)*

(71)申請人：財團法人資訊工業策進會 (中華民國) INSTITUTE FOR INFORMATION INDUSTRY (TW)

臺北市大安區和平東路 2 段 106 號 11 樓

(72)發明人：陳智偉 CHEN, ZHIWEI (TW) ；田家瑋 TIEN, CHIAWEI (TW) ；田謹維 TIEN, CHINWEI (TW) ；林志鴻 LIN, CHIHHUNG (TW)

(74)代理人：蔡坤財；李世章

(56)參考文獻：

TW 201117100A CN 101452397A

US 7996836B1

審查人員：謝進忠

申請專利範圍項數：27 項 圖式數：2 共 0 頁

(54)名稱

虛擬機器監控方法、系統及儲存其之電腦可讀取紀錄媒體

VIRTUAL MACHINE MONITORING METHOD, SYSTEM AND COMPUTER READABLE STORAGE MEDIUM FOR STORING THEREOF

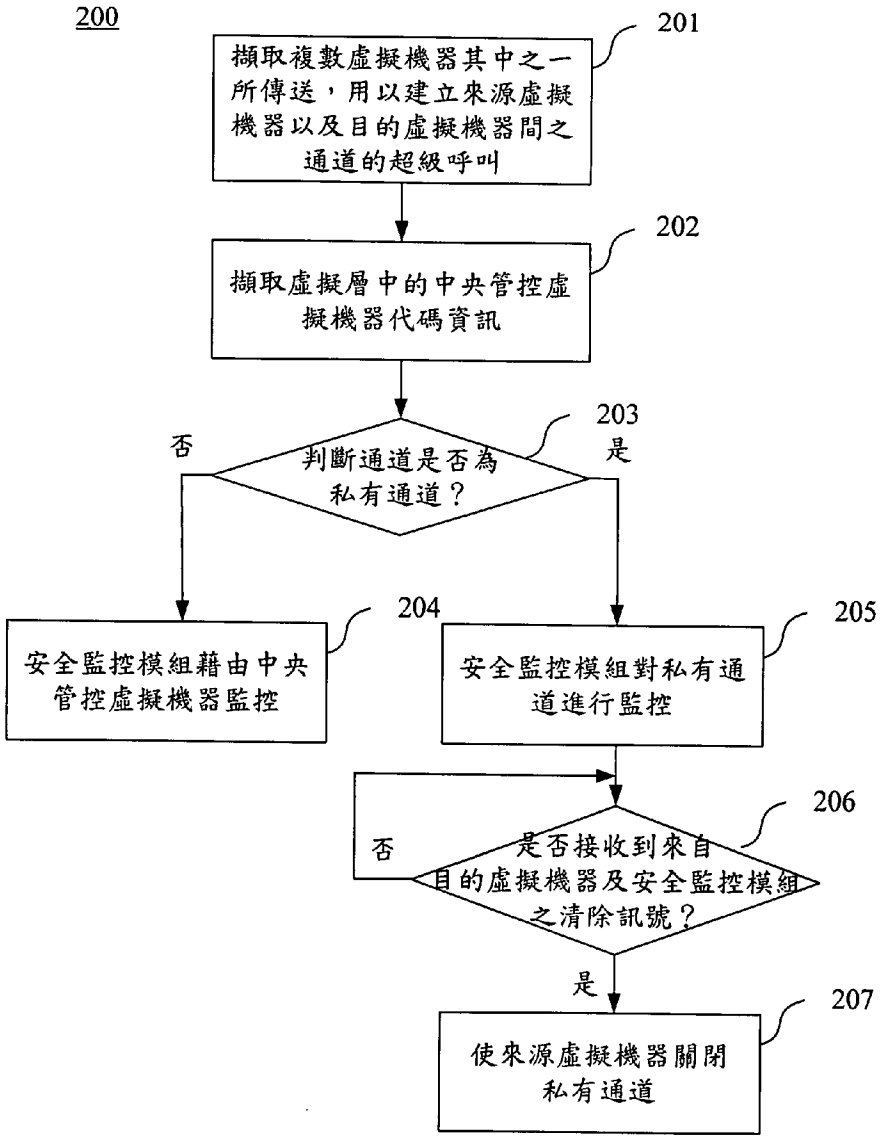
(57)摘要

一種虛擬機器監控方法，應用於虛擬機器監控系統中。虛擬機器監控方法包含下列步驟：於虛擬機器監控系統之虛擬層中擷取複數虛擬機器其中之一所傳送之超級呼叫，其中超級呼叫用以建立來源虛擬機器以及目的虛擬機器間之通道。擷取虛擬層中之中央管控虛擬機器代碼資訊。依據中央管控虛擬機器代碼資訊及對應超級呼叫之通道建立資訊判斷通道之類型。當通道為不透過虛擬機器中之中央管控虛擬機器所建立之私有通道時，使安全監控模組監控私有通道。

A virtual machine monitoring method used in a virtual machine monitoring system is provided. The virtual machine monitoring method includes retrieving a hypercall transmitted from one of a plurality of virtual machines to a hypervisor of a virtual machine monitoring system, in which the hypercall is for establishing a channel between a source virtual machine and a target virtual machine. A central control virtual machine ID information in the hypervisor is retrieved. A type of the channel established by the hypercall is determined according to the central control virtual machine ID information and channel-establishing information corresponding to the hypercall. When the channel is a private channel that is not related to a central control virtual machine of the virtual machines, a security module is used to monitor the private channel.

200・・・虛擬機器監控方法

201-207・・・步驟



第2圖

I451245

公告本

發明專利說明書

（本說明書格式、順序，請勿任意更動，※記號部分請勿填寫）

※申請案號：100133035

※申請日：100.9.14　※IPC分類：G06F 11/34 2006.01
G06F 9/455 2006.01

一、發明名稱：（中文/英文）

虛擬機器監控方法、系統及儲存其之電腦可讀取紀錄媒體

VIRTUAL MACHINE MONITORING METHOD, SYSTEM AND COMPUTER READABLE STORAGE MEDIUM FOR STORING THEREOF

二、中文發明摘要：

一種虛擬機器監控方法，應用於虛擬機器監控系統中。虛擬機器監控方法包含下列步驟：於虛擬機器監控系統之虛擬層中擷取複數虛擬機器其中之一所傳送之超級呼叫，其中超級呼叫用以建立來源虛擬機器以及目的虛擬機器間之通道。擷取虛擬層中之中央管控虛擬機器代碼資訊。依據中央管控虛擬機器代碼資訊及對應超級呼叫之通道建立資訊判斷通道之類型。當通道為不透過虛擬機器中之中央管控虛擬機器所建立之私有通道時，使安全監控模組監控私有通道。

三、英文發明摘要：

A virtual machine monitoring method used in a virtual machine monitoring system is provided. The virtual machine

monitoring method includes retrieving a hypercall transmitted from one of a plurality of virtual machines to a hypervisor of a virtual machine monitoring system, in which the hypercall is for establishing a channel between a source virtual machine and a target virtual machine. A central control virtual machine ID information in the hypervisor is retrieved. A type of the channel established by the hypercall is determined according to the central control virtual machine ID information and channel-establishing information corresponding to the hypercall. When the channel is a private channel that is not related to a central control virtual machine of the virtual machines, a security module is used to monitor the private channel.

四、指定代表圖：

(一)本案指定代表圖為：第（　2　）圖。

(二)本代表圖之元件符號簡單說明：

200：虛擬機器監控方法

201-207：步驟

五、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

無

六、發明說明：

【發明所屬之技術領域】

本揭示內容是有關於一種資訊監控技術，且特別是有關於一種虛擬機器監控方法、系統及儲存其電腦可讀取紀錄媒體。

【先前技術】

在現代電腦技術的進步下，軟體常常無法對過多的硬體資源做有效的利用。藉由在硬體上建立虛擬環境以執行數個虛擬機器，將可以使硬體資源獲得最有效的利用。

在虛擬環境的虛擬機器中，常會設置一個中央管控的虛擬機器，以將虛擬機器資源進行集中管理。虛擬機器間的溝通需要經過中央管控的虛擬機器進行。因此，在習知的技術中，要判斷系統是否有異常的資料傳輸，只需要對中央管控的虛擬機器進行監控即可。然而為了加速虛擬機器間的溝通，在新近的技術中也允許虛擬機器間在不透過中央管控的虛擬機器的情形下，直接建立私有的通道。因此，習知的監控技術，將難以對這樣的私有通道進行監控，容易產生資訊安全上的漏洞。

因此，如何設計一個新的虛擬機器監控方法、系統及儲存其電腦可讀取紀錄媒體，以克服上述之問題，乃為此一業界亟待解決的問題。

【發明內容】

因此，本揭示內容之一態樣是在提供一種虛擬機器監控系統，包含：虛擬層（hypervisor）、複數虛擬機器、安全監控模組以及超級呼叫（hypercall）攔截模組。虛擬機器藉由虛擬層存取至少一實體運算裝置之硬體資源，其中虛擬機器包含中央管控虛擬機器，以對虛擬機器進行管控。超級呼叫攔截模組位於虛擬層中，以擷取虛擬層中之中央管控虛擬機器代碼資訊以及擷取虛擬機器其中之一所傳送之超級呼叫，其中超級呼叫用以建立來源虛擬機器以及目的虛擬機器間之通道，超級呼叫攔截模組進一步依據中央管控虛擬機器代碼資訊及對應超級呼叫之通道建立資訊判斷通道之類型，以於通道為不透過中央管控虛擬機器所建立之私有通道時，使安全監控模組監控私有通道。

依據本揭示內容一實施例，其中通道建立資訊包含對應來源虛擬機器之來源虛擬機器代碼以及對應目的虛擬機器之目的虛擬機器代碼。中央管控虛擬機器代碼資訊包含中央管控虛擬機器之中央管控虛擬機器代碼，超級呼叫攔截模組擷取中央管控虛擬機器代碼資訊，俾判斷來源虛擬機器代碼以及目的虛擬機器代碼是否包含中央管控虛擬機器代碼，以判斷通道之類型。當來源虛擬機器代碼以及目的虛擬機器代碼不包含中央管控虛擬機器代碼，超級呼叫攔截模組判斷通道之類型為私有通道。當來源虛擬機器代碼以及目的虛擬機器代碼其中之一為中央管控虛擬機器代碼，超級呼叫攔截模組判斷通道之類型為中央管控通道。

依據本揭示內容另一實施例，通道為虛擬層之共享記憶體（share memory）。

依據本揭示內容又一實施例，中央管控虛擬機器代碼資訊係藉由核心地圖（kernel map）查詢。

依據本揭示內容再一實施例，當通道之類型為私有通道時，超級呼叫攔截模組將超級呼叫發佈至目的虛擬機器以及安全監控模組，俾使安全監控模組存取私有通道之資訊。超級呼叫攔截模組更用以於接收到目的虛擬機器以及安全監控模組分別傳送之清除訊號後，使來源虛擬機器關閉私有通道。

本揭示內容之一態樣是在提供一種虛擬機器監控方法，應用於虛擬機器監控系統中。虛擬機器監控方法包含下列步驟：於虛擬機器監控系統之虛擬層中擷取複數虛擬機器其中之一所傳送之超級呼叫，其中超級呼叫用以建立來源虛擬機器以及目的虛擬機器間之通道。擷取虛擬層中之中央管控虛擬機器代碼資訊。依據中央管控虛擬機器代碼資訊及對應超級呼叫之通道建立資訊判斷通道之類型。當通道為不透過虛擬機器中之中央管控虛擬機器所建立之私有通道時，使安全監控模組監控私有通道。

依據本揭示內容一實施例，其中通道建立資訊包含對應來源虛擬機器之來源虛擬機器代碼以及對應目的虛擬機器之目的虛擬機器代碼。中央管控虛擬機器代碼資訊包含中央管控虛擬機器之中央管控虛擬機器代碼，依據中央管控虛擬機器代碼資訊判斷通道之類型之步驟更包含判斷來源虛擬機器代碼以及目的虛擬機器代碼是否包含中央管控虛擬機器代碼，以判斷通道之類型。當來源虛擬機器代碼以及目的虛擬機器代碼不包含中央管控虛擬機器代碼，通

道之類型為私有通道。當來源虛擬機器代碼以及目的虛擬機器代碼其中之一為中央管控虛擬機器代碼，通道之類型為中央管控通道。

依據本揭示內容另一實施例，通道為虛擬層之共享記憶體。

依據本揭示內容又一實施例，中央管控虛擬機器代碼資訊係藉由核心地圖查詢。

依據本揭示內容再一實施例，當通道之類型為私有通道時，使安全監控模組監控私有通道之步驟更包含：將超級呼叫發佈至目的虛擬機器以及安全監控模組以及使安全監控模組存取私有通道之資訊。

依據本揭示內容更具有之一實施例，虛擬機器監控方法更包含：判斷目的虛擬機器以及安全監控模組是否分別傳送清除訊號以及當目的虛擬機器以及安全監控模組分別傳送清除訊號，使來源虛擬機器關閉私有通道。

本揭示內容之一態樣是在提供一種電腦可讀取紀錄媒體，儲存一電腦程式，用以執行一種虛擬機器監控方法，其中虛擬機器監控方法包含：於虛擬機器監控系統之虛擬層中擷取複數虛擬機器其中之一所傳送之超級呼叫，其中超級呼叫用以建立來源虛擬機器以及目的虛擬機器間之通道。擷取虛擬層中之中央管控虛擬機器代碼資訊。依據中央管控虛擬機器代碼資訊及對應超級呼叫之通道建立資訊判斷通道之類型。當通道為不透過虛擬機器中之中央管控虛擬機器所建立之私有通道時，使安全監控模組監控私有通道。

依據本揭示內容一實施例，其中通道建立資訊包含對應來源虛擬機器之來源虛擬機器代碼以及對應目的虛擬機器之目的虛擬機器代碼。中央管控虛擬機器代碼資訊包含中央管控虛擬機器之中央管控虛擬機器代碼，依據中央管控虛擬機器代碼資訊判斷通道之類型之步驟更包含判斷來源虛擬機器代碼以及目的虛擬機器代碼是否包含中央管控虛擬機器代碼，以判斷通道之類型。當來源虛擬機器代碼以及目的虛擬機器代碼不包含中央管控虛擬機器代碼，通道之類型為私有通道。當來源虛擬機器代碼以及目的虛擬機器代碼其中之一為中央管控虛擬機器代碼，通道之類型為中央管控通道。

依據本揭示內容另一實施例，通道為虛擬層之共享記憶體。

依據本揭示內容又一實施例，中央管控虛擬機器代碼資訊係藉由核心地圖查詢。

依據本揭示內容再一實施例，當通道之類型為私有通道時，使安全監控模組監控私有通道之步驟更包含：將超級呼叫發佈至目的虛擬機器以及安全監控模組以及使安全監控模組存取私有通道之資訊。

依據本揭示內容更具有之一實施例，虛擬機器監控方法更包含：判斷目的虛擬機器以及安全監控模組是否分別傳送清除訊號以及當目的虛擬機器以及安全監控模組分別傳送清除訊號，使來源虛擬機器關閉私有通道。

應用本揭示內容之優點係在於藉由擷取用以建立來源虛擬機器以及目的虛擬機器間之通道的超級呼叫，並於判

斷為此通道為一私有通道時進行監控，可以偵測虛擬機器間未經過中央控管虛擬機器的溝通行為，避免資安漏洞，而輕易地達到上述之目的。

【實施方式】

請參照第 1 圖。第 1 圖為本揭示內容一實施例中，虛擬機器監控系統 1 之方塊圖。虛擬機器監控系統 1 包含：虛擬層（hypervisor）10、複數虛擬機器 120、122 及 124、安全監控模組 14 以及超級呼叫（hypercall）攔截模組 16。

虛擬機器監控系統 1 是建立於實體運算裝置 18 上的虛擬環境，以藉由虛擬環境技術在虛擬層 10 上虛擬出數個虛擬機器，可以達到同時對實體運算裝置 18 的硬體資源進行存取的功效。舉例來說，虛擬機器監控系統 1 可建立於一個個人電腦中，並藉由虛擬環境技術在虛擬層 10 上虛擬出各執行不同的作業系統的數個虛擬機器。因此，在現代電腦硬體技術愈來愈進步的情形下，虛擬機器將可使硬體資源獲得最大的使用率。於不同實施例中，虛擬機器之數目可依需求調整，不為第 1 圖中繪示所限。

虛擬機器各包含一個虛擬機器代碼。於一實施例中，虛擬機器代碼是以網域（domain）編碼表示。舉例來說，虛擬機器 122 之虛擬機器代碼可為網域 1（domain 1），而虛擬機器 124 之虛擬機器代碼可為網域 2（domain 2）。於本實施例中，虛擬機器 120 為一個中央管控虛擬機器。中央管控虛擬機器在不同之實施例中，可以是虛擬機器代碼為網域 0（domain 0）的管控虛擬機器，或是具有其他虛擬

機器代碼之一驅動網域（driver domain）虛擬機器，以對其他虛擬機器 122、124 間的溝通進行管控。

虛擬機器 122、124 間常見的的溝通方式，是透過中央管控虛擬機器 120 所進行。亦即，虛擬機器 122、124 間進行溝通時，是在虛擬層 10 中建立一個共享記憶體，並經由中央管控虛擬機器 120 來對共享記憶體進行資料的傳輸。因此，藉由這樣的中央管控通道，其傳輸的資料均會經由中央管控虛擬機器 120 的轉發。在這樣的情形下，安全監控模組 14 可直接在中央管控虛擬機器 120 進行資料的攔截，以監控是否有危及資訊安全的事情發生。需注意的是，上述之安全監控模組 14 於一實施例中，可為一獨立於中央管控虛擬機器 120 之安全監控虛擬機器。於其他實施例中，安全監控模組 14 亦可設置於中央管控虛擬機器 120 之中，而不需獨立設置。

然而，不透過中央管控虛擬機器 120 而直接藉由超級呼叫所建立在虛擬機器 122、124 間的私有通道，雖然可以加快虛擬機器 122、124 間的資料傳遞，但也使得安全監控模組 14 無法藉由在中央管控虛擬機器 120 進行資料攔截的方式來監控，因此容易造成資訊安全上的漏洞。

本揭示內容之虛擬機器監控系統 1 中的超級呼叫攔截模組 16 位於虛擬層 10，可用以擷取虛擬機器其中之一所傳送之超級呼叫。舉例來說，虛擬機器 122 在欲與虛擬機器 124 進行溝通時，將藉由第 1 圖中所繪示之實線路徑傳送超級呼叫至虛擬層 10 中。於本實施例中，超級呼叫之來源為虛擬機器 122，而目的則是虛擬機器 124。在虛擬層

10 中，將產生對應此超級呼叫的通道建立資訊（未繪示）。於一實施例中，通道建立資訊包含事件（event）相關資料結構及網域相關資料結構，分別記錄有來源虛擬機器代碼及目的虛擬機器代碼。

表 1

	資料結構名稱	資料結構參數
事件相關資料結構	struct evtchn	Struct { domain *remote_dom }interdomain
網域相關資料結構	struct domain	current->domain

請參照表 1。表 1 為本揭示內容一實施例中，通道建立資訊中的事件相關資料結構及網域相關資料結構之內容。其中，參數「domain *remote_dom」即對應至來源虛擬機器代碼，而參數「current->domain」即對應至目的虛擬機器代碼。因此，位於虛擬層 10 中的超級呼叫攔截模組 16 將可根據通道建立資訊擷取來源虛擬機器代碼以及目的虛擬機器代碼。於本實施例中，來源虛擬機器代碼即為網域 1，而目的虛擬機器代碼即為網域 2。

需注意的是，於其他實施例中，來源虛擬機器代碼及目的虛擬機器代碼亦可能以其他的型式儲存，不為本實施例中的實施方式所限。

超級呼叫攔截模組 16 進一步可擷取虛擬層 10 中之中央管控虛擬機器代碼資訊（未繪示）。於一實施例中，中央管控虛擬機器代碼資訊是記錄於核心地圖（kernel map）中，因此可藉由查詢核心地圖得知虛擬機器代碼資訊。於

一實施例中，中央管控虛擬機器代碼資訊即為中央管控虛擬機器之虛擬機器代碼（於本實施例中為網域 0）。因此，在將來源虛擬機器代碼及目的虛擬機器代碼與虛擬機器代碼資訊中的中央管控虛擬機器代碼相比對後，可以得知來源虛擬機器與目的虛擬機器是否其中一者為中央管控虛擬機器 120。

如其中一者為中央管控虛擬機器 120，超級呼叫攔截模組 16 將判斷據此超級呼叫所建立的通道為中央管控通道。根據前述，由於來源虛擬機器代碼為網域 1，而目的虛擬機器代碼為網域 2，均非中央管控虛擬機器 120 之中央管控虛擬機器代碼。因此，超級呼叫攔截模組 16 將判斷據此超級呼叫所建立的通道為不透過中央管控虛擬機器 120 所建立之私有通道。

超級呼叫攔截模組 16 進一步將超級呼叫發佈至目的虛擬機器 124 及安全監控模組 14。超級呼叫將接著於虛擬層 10 中建立共享記憶體 100，以建立虛擬機器 122 與虛擬機器 124 溝通的通道。此時，目的虛擬機器 124 及安全監控模組 14 將均具有對共享記憶體 100 進行存取的權限。安全監控模組 14 將可對虛擬機器 122 與虛擬機器 124 經由私有通道所傳輸的資料，即第 1 圖中以虛線繪示之部份進行監控。

於一實施例中，超級呼叫攔截模組 16 將擷取目的虛擬機器 124 在處理完來源虛擬機器 122 的要求後，傳送至虛擬層 10 中欲關閉私有通道的清除訊號（未繪示）。而安全監控模組 14 在讀取完共享記憶體 100 的資料後，也將傳送

其對應的清除訊號至超級呼叫攔截模組 16。超級呼叫攔截模組 16 將在均接收到來自目的虛擬機器 124 及安全監控模組 14 的清除訊號後，才將清除訊號傳送至來源虛擬機器 122，使來源虛擬機器 122 將共享記憶體 100 移除以關閉私有通道，以避免此私有通道在安全監控模組 14 尚未存取完即為目的虛擬機器 124 的清除訊號所清除。

因此，本揭示內容之虛擬機器監控系統 1 藉由超級呼叫攔截模組 16 之設置，可以在擷取虛擬機器代碼資訊以及用以建立通道之超級呼叫後進一步根據其對應的通道建立資訊判斷此通道是否為私有通道，並在判斷為私有通道後，使安全監控模組 14 具有存取通道的權限，以進行資安監控。

請參照第 2 圖。第 2 圖為本揭示內容一實施例中，一種虛擬機器監控方法 200 之流程圖。虛擬機器監控方法可應用於如第 1 圖所示之虛擬機器監控系統 1 中。此虛擬機器監控方法可實作為一電腦程式，並儲存於一電腦可讀取記錄媒體中，而使電腦讀取此記錄媒體後執行即時地點推薦方法。電腦可讀取記錄媒體可為唯讀記憶體、快閃記憶體、軟碟、硬碟、光碟、隨身碟、磁帶、可由網路存取之資料庫或熟悉此技藝者可輕易思及具有相同功能之電腦可讀取紀錄媒體。

虛擬機器監控方法 200 包含下列步驟：

於步驟 201，藉由虛擬機器監控系統 1 之超級呼叫攔截模組 16，在虛擬層 10 中擷取複數虛擬機器 120、122 及 124 其中之一所傳送之超級呼叫，其中超級呼叫用以建立

來源虛擬機器以及目的虛擬機器間之通道。

於步驟 202，超級呼叫攔截模組 16 擷取虛擬層 10 中的虛擬機器代碼資訊。接著於步驟 203，超級呼叫攔截模組 16 依據虛擬機器代碼資訊及對應超級呼叫之通道建立資訊判斷通道是否為私有通道。舉例來說，上述之虛擬機器中，虛擬機器 120 為一個中央管控虛擬機器 120。在通道建立資訊中將記錄有來源虛擬機器代碼以及目的虛擬機器代碼，而透過前述之核心地圖，則可得知中央管控虛擬機器 120 的代碼。因此，超級呼叫攔截模組 16 可據以判斷來源虛擬機器代碼以及目的虛擬機器代碼是否其中一者為中央管控虛擬機器 120 之代碼。

如果兩者其中之一為中央管控虛擬機器 120 的代碼，則將於步驟 204 判斷據此超級呼叫所建立者為中央管控通道，安全監控模組 14 將藉由中央管控虛擬機器 120 監控。如果兩者均不為中央管控虛擬機器 120 的代碼，則將於步驟 205 判斷據此超級呼叫所建立者為私有通道，且超級呼叫攔截模組 16 將使安全監控模組 14 監控私有通道。於一實施例中，超級呼叫攔截模組 16 是藉由將超級呼叫發佈至安全監控模組 14 及目的虛擬機器，以使安全監控模組 14 及目的虛擬機器均對於此私有通道具有存取的權限。因此安全監控模組 14 將可對於私有通道內的資訊進行監控。

接著於步驟 206，超級呼叫攔截模組 16 判斷是否接收到目的虛擬機器及安全監控模組 14 的清除訊號。如果至少其中之一的清除訊號尚未接收到，則超級呼叫攔截模組 16 將回到步驟 206 繼續等待。如果兩者的清除訊號均已接收

到，則將於步驟 207 中使來源虛擬機器關閉此私有通道。

雖然本揭示內容已以實施方式揭露如上，然其並非用以限定本揭示內容，任何熟習此技藝者，在不脫離本揭示內容之精神和範圍內，當可作各種之更動與潤飾，因此本揭示內容之保護範圍當視後附之申請專利範圍所界定者為準。

【圖式簡單說明】

為讓本揭示內容之上述和其他目的、特徵、優點與實施例能更明顯易懂，所附圖式之說明如下：

第 1 圖為本揭示內容一實施例中，虛擬機器監控系統之方塊圖；以及

第 2 圖為本揭示內容一實施例中，一種虛擬機器監控方法之流程圖。

【主要元件符號說明】

1：虛擬機器監控系統
10：虛擬層
100：共享記憶體
120、122、124：虛擬機器
14：安全監控模組
16：超級呼叫攔截模組
18：實體運算裝置
200：虛擬機器監控方法
201-207：步驟

七、申請專利範圍：

1. 一種虛擬機器監控系統，包含：

一虛擬層（hypervisor）；

複數虛擬機器，藉由該虛擬層存取至少一實體運算裝置之一硬體資源，其中該等虛擬機器包含一中央管控虛擬機器，以對該等虛擬機器進行管控；

一安全監控模組；以及

一超級呼叫（hypercall）攔截模組，位於該虛擬層中，以擷取該虛擬層中之一中央管控虛擬機器代碼資訊以及擷取該等虛擬機器其中之一所傳送之一超級呼叫，其中該超級呼叫用以建立一來源虛擬機器以及一目的虛擬機器間之一通道，該超級呼叫攔截模組進一步依據該中央管控虛擬機器代碼資訊及對應該超級呼叫之一通道建立資訊判斷該通道之類型，以於該通道為不透過該中央管控虛擬機器所建立之一私有通道時，使該安全監控模組監控該私有通道。

2. 如請求項1所述之虛擬機器監控系統，其中該通道建立資訊包含對應該來源虛擬機器之一來源虛擬機器代碼以及對應該目的虛擬機器之一目的虛擬機器代碼。

3. 如請求項2所述之虛擬機器監控系統，其中該中央管控虛擬機器代碼資訊包含該中央管控虛擬機器之一中央管控虛擬機器代碼，該超級呼叫攔截模組擷取該中央管控虛擬機器代碼資訊，俾判斷該來源虛擬機器代碼以及該目的虛擬機器代碼是否包含該中央管控虛擬機器代碼，以

判斷該通道之類型。

4. 如請求項3所述之虛擬機器監控系統，當該來源虛擬機器代碼以及該目的虛擬機器代碼不包含該中央管控虛擬機器代碼，該超級呼叫攔截模組判斷該通道之類型係為該私有通道。

5. 如請求項3所述之虛擬機器監控系統，當該來源虛擬機器代碼以及該目的虛擬機器代碼其中之一為該中央管控虛擬機器代碼，該超級呼叫攔截模組判斷該通道之類型係為一中央管控通道。

6. 如請求項1所述之虛擬機器監控系統，該通道為該虛擬層之一共享記憶體（share memory）。

7. 如請求項1所述之虛擬機器監控系統，其中該虛擬機器代碼資訊係藉由一核心地圖（kernel map）查詢。

8. 如請求項1所述之虛擬機器監控系統，其中當該通道之類型係為該私有通道時，該超級呼叫攔截模組將該超級呼叫發佈至該目的虛擬機器以及該安全監控模組，俾使該安全監控模組存取該私有通道之資訊。

9. 如請求項8所述之虛擬機器監控系統，該超級呼

叫攔截模組更用以於接收到該目的虛擬機器以及該安全監控模組分別傳送之一清除訊號後，使該來源虛擬機器關閉該私有通道。

10. 一種虛擬機器監控方法，應用於一虛擬機器監控系統中，該虛擬機器監控方法包含下列步驟：

於該虛擬機器監控系統之一虛擬層中擷取複數虛擬機器其中之一所傳送之一超級呼叫，其中該超級呼叫用以建立一來源虛擬機器以及一目的虛擬機器間之一通道；

擷取該虛擬層中之一中央管控虛擬機器代碼資訊；

依據該中央管控虛擬機器代碼資訊及對應該超級呼叫之一通道建立資訊判斷該通道之類型；以及

當該通道為不透過該等虛擬機器中之一中央管控虛擬機器所建立之一私有通道時，使一安全監控模組監控該私有通道。

11. 如請求項10所述之虛擬機器監控方法，其中該通道建立資訊包含對應該來源虛擬機器之一來源虛擬機器代碼以及對應該目的虛擬機器之一目的虛擬機器代碼。

12. 如請求項11所述之虛擬機器監控方法，其中該中央管控虛擬機器代碼資訊包含該中央管控虛擬機器之一中央管控虛擬機器代碼，依據該中央管控虛擬機器代碼資訊及該超級呼叫之該通道建立資訊判斷該通道之類型之步驟更包含判斷該來源虛擬機器代碼以及該目的虛擬機器代碼

是否包含該中央管控虛擬機器代碼，以判斷該通道之類型。

13. 如請求項12所述之虛擬機器監控方法，當該來源虛擬機器代碼以及該目的虛擬機器代碼不包含該中央管控虛擬機器代碼，該通道之類型係為該私有通道。

14. 如請求項12所述之虛擬機器監控方法，當該來源虛擬機器代碼以及該目的虛擬機器代碼其中之一為該中央管控虛擬機器代碼，該通道之類型係為一中央管控通道。

15. 如請求項10所述之虛擬機器監控方法，該通道為該虛擬層之一共享記憶體。

16. 如請求項10所述之虛擬機器監控方法，其中該中央管控虛擬機器代碼資訊係藉由一核心地圖查詢。

17. 如請求項10所述之虛擬機器監控方法，其中當該通道之類型係為該私有通道時，使該安全監控模組監控該私有通道之步驟更包含：

將該超級呼叫發佈至該目的虛擬機器以及該安全監控模組；以及

使該安全監控模組存取該私有通道之資訊。

18. 如請求項17所述之虛擬機器監控方法，更包含：

判斷該目的虛擬機器以及該安全監控模組是否分別傳送一清除訊號；以及

當該目的虛擬機器以及該安全監控模組分別傳送該清除訊號，使該來源虛擬機器關閉該私有通道。

19. 一種電腦可讀取紀錄媒體，儲存一電腦程式，用以執行一種虛擬機器監控方法，其中該虛擬機器監控方法包含：

於一虛擬機器監控系統之一虛擬層中擷取複數虛擬機器其中之一所傳送之一超級呼叫，其中該超級呼叫用以建立一來源虛擬機器以及一目的虛擬機器間之一通道；

擷取該虛擬層中之一中央管控虛擬機器代碼資訊；

依據該中央管控虛擬機器代碼資訊及對應該超級呼叫之一通道建立資訊判斷該通道之類型；以及

當該通道為不透過該等虛擬機器中之一中央管控虛擬機器所建立之一私有通道時，使一安全監控模組監控該私有通道。

20. 如請求項19所述之電腦可讀取紀錄媒體，其中該超級呼叫包含一通道建立資訊，該通道建立資訊包含對應該來源虛擬機器之一來源虛擬機器代碼以及對應該目的虛擬機器之一目的虛擬機器代碼。

21. 如請求項20所述之電腦可讀取紀錄媒體，其中該中央管控虛擬機器代碼資訊包含該中央管控虛擬機器之一

中央管控虛擬機器代碼，依據該中央管控虛擬機器代碼資訊及該超級呼叫之該通道建立資訊判斷該通道之類型之步驟更包含判斷該來源虛擬機器代碼以及該目的虛擬機器代碼是否包含該中央管控虛擬機器代碼，以判斷該通道之類型。

22. 如請求項21所述之電腦可讀取紀錄媒體，當該來源虛擬機器代碼以及該目的虛擬機器代碼不包含該中央管控虛擬機器代碼，該通道之類型係為該私有通道。

23. 如請求項21所述之電腦可讀取紀錄媒體，當該來源虛擬機器代碼以及該目的虛擬機器代碼其中之一為該中央管控虛擬機器代碼，該通道之類型係為一中央管控通道。

24. 如請求項19所述之電腦可讀取紀錄媒體，該通道為該虛擬層之一共享記憶體。

25. 如請求項19所述之電腦可讀取紀錄媒體，其中該中央管控虛擬機器代碼資訊係藉由一核心地圖查詢。

26. 如請求項19所述之電腦可讀取紀錄媒體，其中當該通道之類型係為該私有通道時，使該安全監控模組監控該私有通道之步驟更包含：

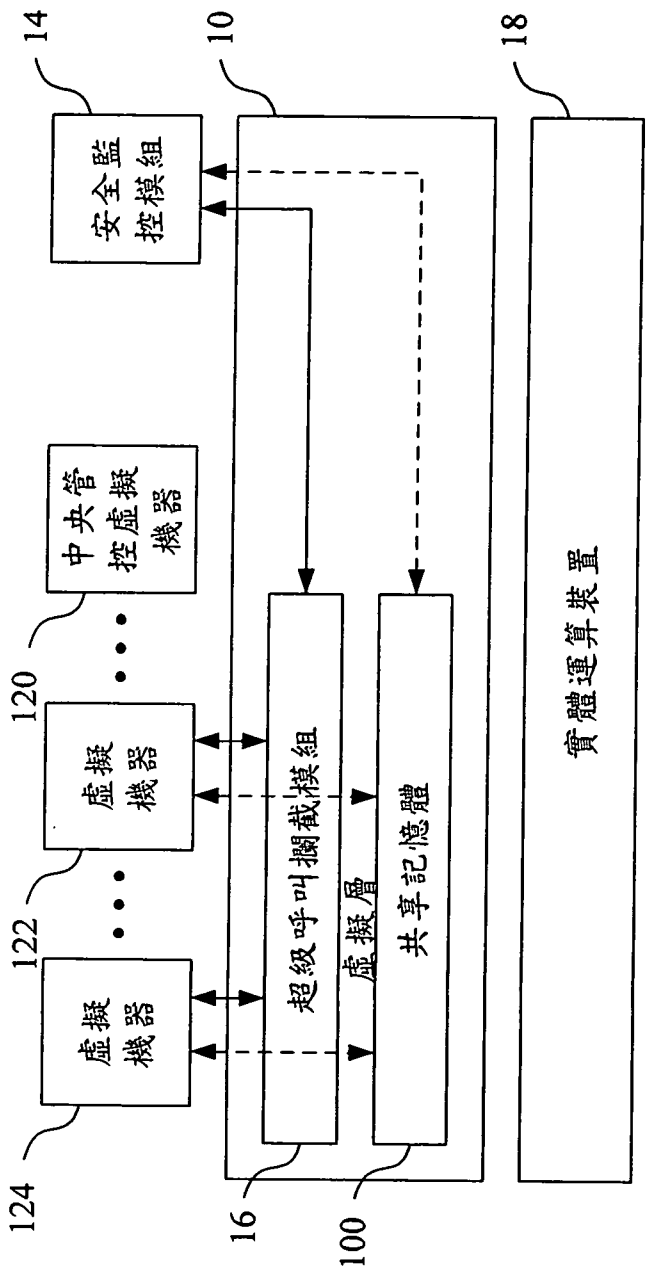
將該超級呼叫發佈至該目的虛擬機器以及該安全監控模組；以及

使該安全監控模組存取該私有通道之資訊。

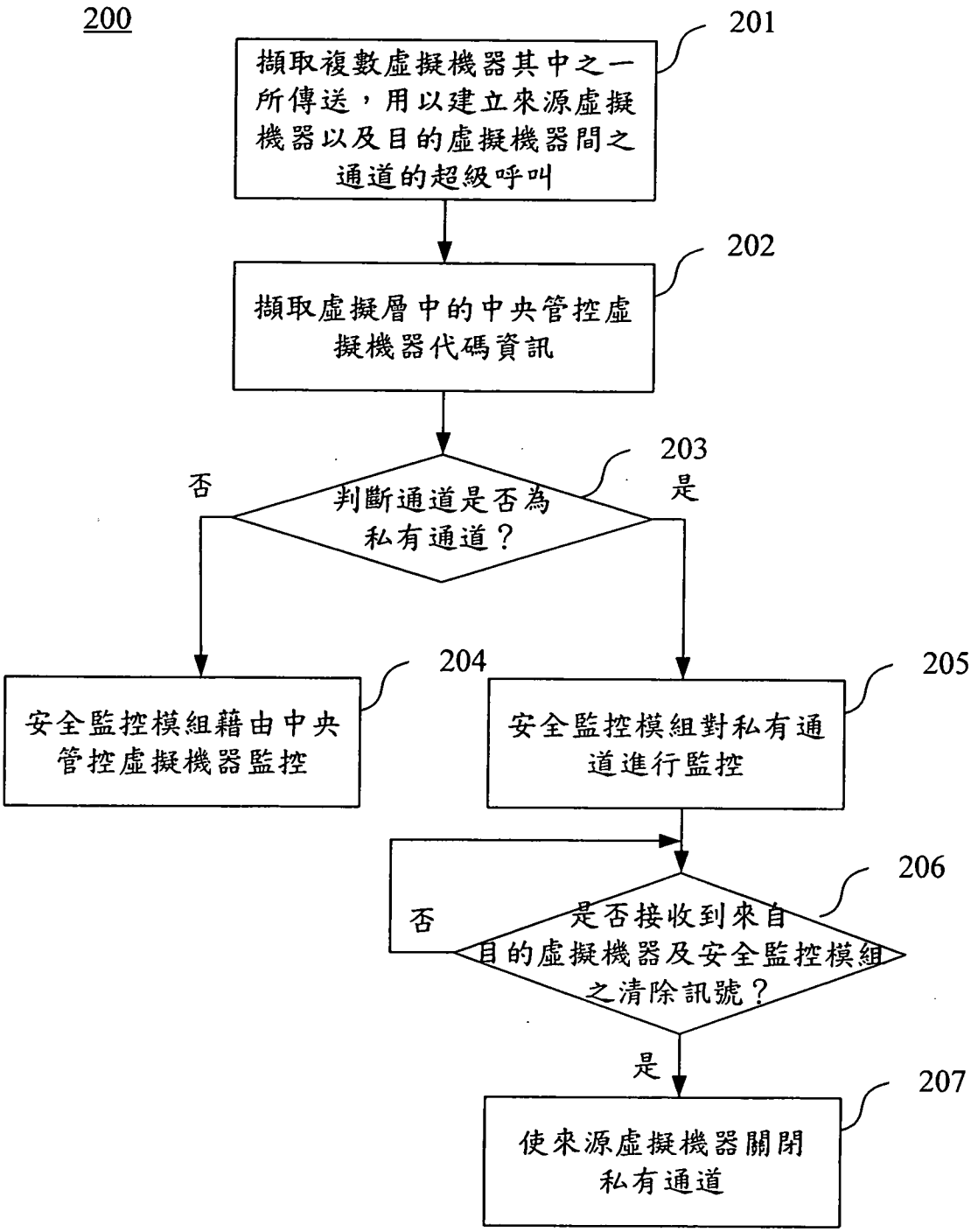
27. 如請求項26所述之電腦可讀取紀錄媒體，該虛擬機器監控方法更包含：

判斷該目的虛擬機器以及該安全監控模組是否分別傳送一清除訊號；以及

當該目的虛擬機器以及該安全監控模組分別傳送該清除訊號，使該來源虛擬機器關閉該私有通道。


1
14
安全監控模組
10
18
中央管控虛擬機器
120
虛擬機器
122
虛擬機器
124
超級呼叫攔截模組
虛擬層
共享記憶體
實體運算裝置
16
100

第1圖


200
201
擷取複數虛擬機器其中之一所傳送，用以建立來源虛擬機器以及目的虛擬機器間之通道的超級呼叫
202
擷取虛擬層中的中央管控虛擬機器代碼資訊
203
判斷通道是否為私有通道？
否
是
204
安全監控模組藉由中央管控虛擬機器監控
205
安全監控模組對私有通道進行監控
206
是否接收到來自目的虛擬機器及安全監控模組之清除訊號？
否
是
207
使來源虛擬機器關閉私有通道

第2圖